GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA SHREDDER

Irreversible data deletion

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-sd_shredder-user_guide-v10

Table of contents

In the documentation, Stormshield Data Security Enterprise is referred to in its short form: SDS.

Preface

This document provides essential information on the use of Stormshield Data Shredder. It describes the functions of Stormshield Data Shredder in its default configuration. You can customize the installation of this component using Stormshield Data Authority Manager. The customization options are the most important in this guide. This guide is for

1. system administrators who want to install Stormshield Data Security.
2. users who want to protect confidential files.

1. Introduction

Stormshield Data Shredder is a security component of Stormshield Data Security. This chapter describes the functions and security environment of Stormshield Data Shredder.

1.1 Presentation

Stormshield Data Shredder is a data processing security software. It is intended to provide irreversible deletion of data you wish to remove from your computer. The purpose of this procedure is to prevent third parties from illicitly recovering data deleted from your hard disk.

Stormshield Data Shredder is part of the Stormshield Data Security suite (public key solutions). If you already own one of these software components, you may conveniently access all software functionalities from the Stormshield Data Security interface.

1.2 Deletion principals

This section explains the different types of data deletion.

1.2.1 Classic deletion

When using standard Windows deletion procedures, the content of your data is not completely erased from your disk. Only the physical address or file location of your file on the hard disk is erased from your computer's memory. Some tools, using file fragments present on your disk, are capable of reconstructing files that you thought were erased permanently.

Imagine that in order to remove a page from a book (and thus the data contained on this page) you simply tear out the table of contents and replace it by a new table of contents, which no longer contains a reference to the old page. If you look at the new table of contents, you might imagine that the old data is no longer in the book. However if you leaf through the book page by page the information is still in there.

Your computer works in a similar fashion. The information is never really deleted when you use standard deletion procedures. Only the equivalent of the table of contents in the example above is really updated.

As a result, specific software products may be used to analyze your hard disk and may recover data which you thought you had erased.

1.2.2 Deletion with Stormshield Data Shredder

The solution to the problem of recovery with classic deletion is to use a method which does not merely update the table of contents, but which also tears out the actual page and replaces it with another page containing gibberish. This is exactly how Stormshield Data Shredder works. The product retrieves the physical address (on the hard disk) of the file to be erased, then overwrites this address in several rounds using a series of patterns (00;FF;55 by default). Your initial file is totally modified and even a full analysis of your hard disk, sector by sector, does not allow the data to be recovered.

NOTE
Using several patterns in several rounds suppresses any magnetic remnants. See Section 3.2, "Advanced settings".

1.3 A secured connection to Stormshield Data Security

To use Stormshield Data Shredder you can connect to Stormshield Data Security, a process which involves self-authentication, and enables you to retrieve Stormshield Data Shredder configuration.

Stormshield Data Security provides two authentication methods:

- by password: you enter an identifier and a password,
- by smart card or USB token: you enter the secret code of the card – that is the Personal Identification Number (PIN).

For further information, handling user accounts is described in the *Installation and Implementation guide*.

An alternative is to use the secured erase function which gives you access to your software product without connecting to Stormshield Data Security or if your account is locked. In this case, the default patterns (00;FF;55) are used.

2. Installing Stormshield Data Shredder

This chapter provides information on Stormshield Data Security requirements and installation.

2.1 Required configuration

For the required configuration, refer to the section **Compatibility** of the Stormshield Data Security 10.1 Release Notes.

200 MB of disk space are needed for the installation of all the Stormshield Data Security components.

IMPORTANT
Stormshield Data Security is not compatible with the **Fast User Switching** feature.

2.2 Installing Stormshield Data Shredder

Stormshield Data Shredder is a component of Stormshield Data Security.

Stormshield Data Security installation is global. The delivered product contains all the components of the software suite and allows you to install the applications and components you choose, according to the rights contained in the license key.

The installation procedure is described in the *Installation and Implementation guide*. Refer to this guide for further information.

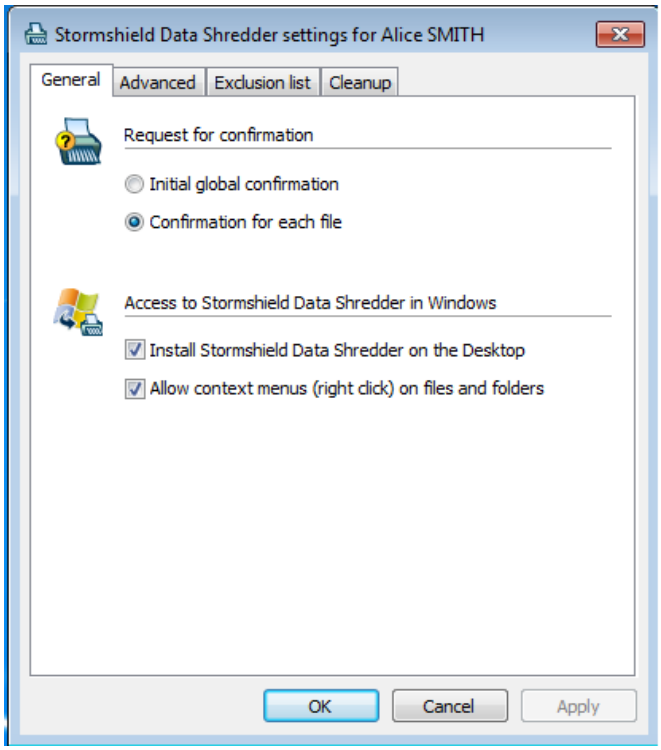
3. Configuring Stormshield Data Shredder

This chapter describes how to configure confirmation requests and access to Stormshield Data Shredder. Advanced settings are also described, but are recommended only for advanced users.

3.1 General configuration

To configure Stormshield Data Shredder, right-click in the Stormshield Data Security menu and select Properties > Configuration tab and double-click the Shredder icon. Your Stormshield Data Shredder settings window is displayed.

The General tab enables you to set the general Stormshield Data Shredder parameters:



Request for confirmation section:

You can request:

- an initial global confirmation, that is a confirmation applicable to every files selected by the erase request
- a confirmation for each file (in addition to the global operation confirmation which will be displayed anyway). During the deletion operation, you can still specify that you do not want any request for the next files; however for a new erase operation, the individual confirmation will still be active.

Access to Stormshield Data Shredder in Windows section:

Both check boxes are selected by default. You can uncheck one or both.

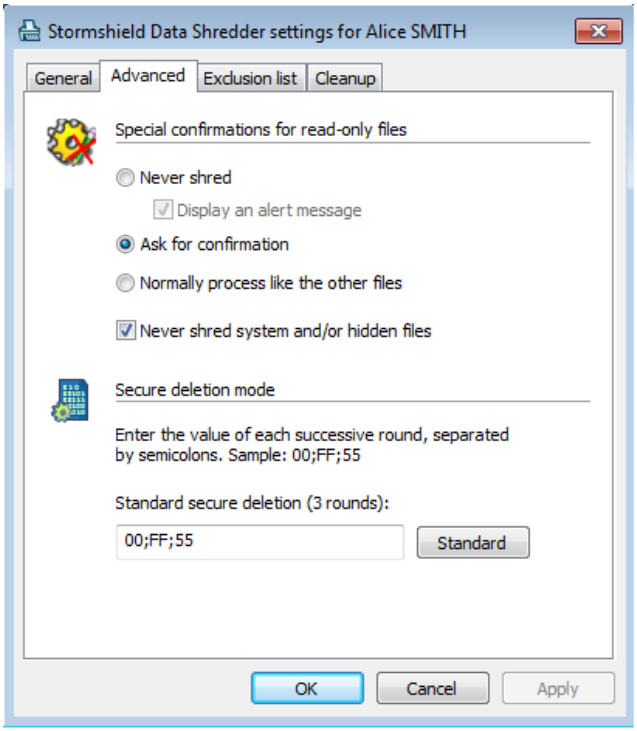
- when the Install Stormshield Data Shredder on the Desktop option is checked, the icon is installed on the desktop: this enables you to use the product by drag and drop.

NOTE
When the desktop icon is activated/deactivated, it is not taken into account immediately when you apply the modification. You must update the desktop (by pressing F5 on the desktop for example) or close/reopen the Windows session.

- when the Allow context menus (right click) on files and folders option is checked, you will be able to right-click in Windows Explorer to access the Stormshield Data Shredder menu options

3.2 Advanced settings

The Advanced tab is meant for advanced users:



The Special confirmations for read-only files section enables you to define the confirmation message that will be displayed when trying to erase read-only files, hidden files, or system files. The type is determined by the system attributes of each file.

Using the radio buttons you can specify one of these options for the read-only files:

- never shred (that is irreversibly erase) read-only files; you can ensure a notice is sent when attempting to delete a read-only file (check the box Display an alert message)
- receive a confirmation request before deletion
- process them as if they are not read-only

If the Never shred system and/or hidden files option is checked, no warning will be displayed to indicate that a system/hidden file is not deleted. This option takes precedence over the second radio button for read-only files.

If the Never shred system and/or hidden files option is NOT checked, the deletion of hidden/system files may be allowed: the rule defined by the radio button for read-only files prevails. If the deletion of system files is allowed, but not that of read-only files (first radio button), a read-only system file will not be deleted.

The Secure deletion mode option defines the level and type of shredding (irreversible erase) to be done, by setting the number of write rounds and the byte values. As many as seven rounds can be set. Every byte value is defined in hexadecimal and is always two digits (the first one may equal 0). The various values are separated by semicolons. The values may be reset to default (00;FF;55) by clicking the Standard button.

CAUTION
The more the rounds that are set, the longer it will take to shred the files.

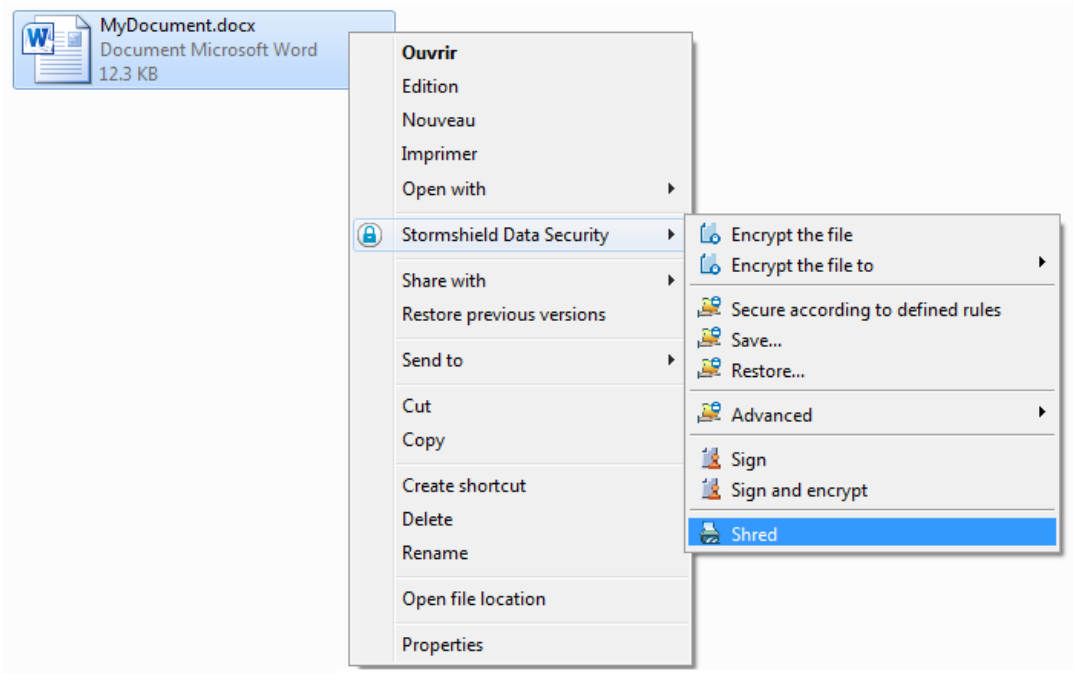
4. Using Stormshield Data Shredder

Stormshield Data Shredder functions can be launched using:

- the right-click after selecting an icon to display the context-sensitive menus in Windows Explorer
- the drag-and-drop feature from the Windows desktop
- automatically, using “Cleanup list”

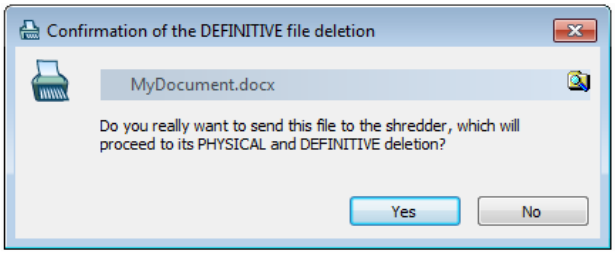
4.1 Using the right-click option

In Windows Explorer right-click the files and/or folders you want to shred, and choose Stormshield Data Security > Shred.

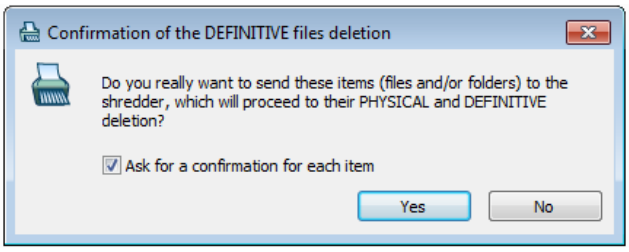


You may select several files to be shredded at the same time. The same applies to folders. When folders are securely erased, every file in the folder is securely erased before the folder is erased. A folder may contain sub-folders, which are processed recursively.

Depending on the configuration, you may be asked to confirm your request before file deletion:



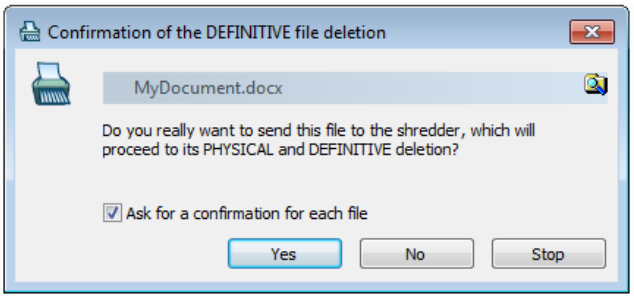
When several items (files or folders) are to be erased, the confirmation will be asked for each item or globally depending whether you select the option Ask for a confirmation for each item, or not.



If you click the No button in the confirmation window, the processing stops immediately.

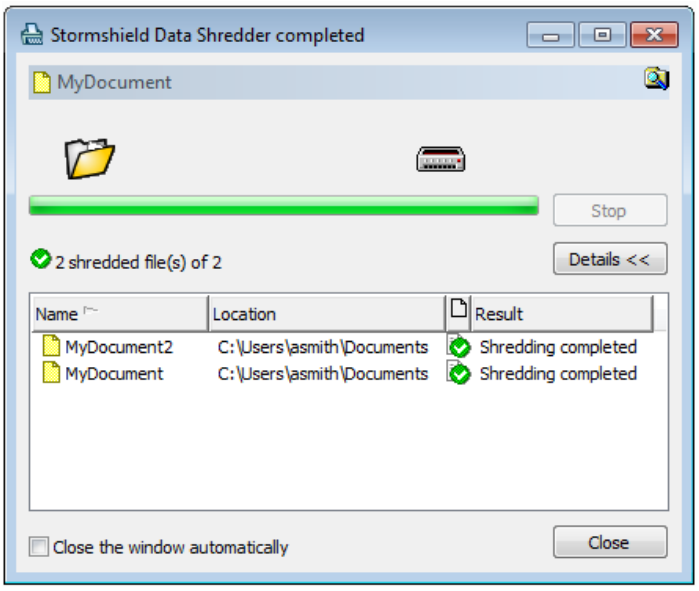
If you click the Yes button with the box checked, a confirmation is asked for each file.

To stop the confirmation requests, uncheck the Ask for a confirmation for each file box. The files will be processed without further confirmation.



CAUTION
If you stop the shredding process by clicking Stop, the file will not be deleted, but the files already erased cannot be retrieved.

As the processing continues, a report showing the result for each file is displayed:

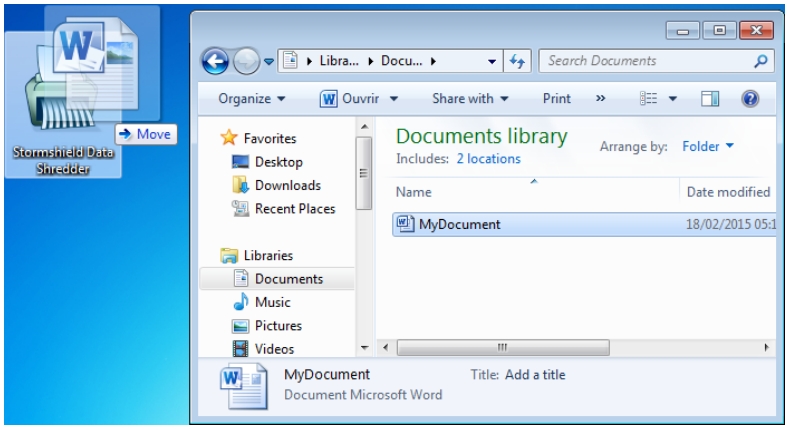


To close the report when the processing ends, check the Close the window automatically box. The window will be closed only if the processing is successful.

4.2 Using drag-and-drop

Stormshield Data Shredder supports drag-and-drop on the Windows desktop or when using Windows Explorer.

Select one or several files from Windows Explorer. Hold down the left mouse button, drag-and-drop the files to the Stormshield Data Shredder icon on the desktop.



You may also select one or more folders for shredding, using the same method.

Stormshield Data Shredder will then destroy the data selected permanently and irreversibly. The processing is strictly the same as that resulting from a right-click in the Windows Explorer.

4.3 Using a "Cleanup list"

A cleanup list lets you automate deletion of files and/or folders in order to facilitate use of Stormshield Data Shredder and avoid errors. Your files are automatically deleted at a predetermined time. You may decide to have your files deleted automatically at one of the following moment:

- at logout
- when a user session is locked
- at fixed intervals (for example every 15 minutes) as a background task

Recursivity of automatic deletion determines if the sub-folder are included in the deletion or not. It is set by the Include sub-folders option and can either be on or off. Recursivity is applied as follows:

- on a folder, it defines if only the indicated folder will be deleted automatically or if its sub-folders will also be deleted
- as a property of a collection of files defined by an expression using wildcard characters (* and ?), it defines if only the collection of files will be deleted automatically or if files with the same name, but located in other sub-folders, will also be deleted

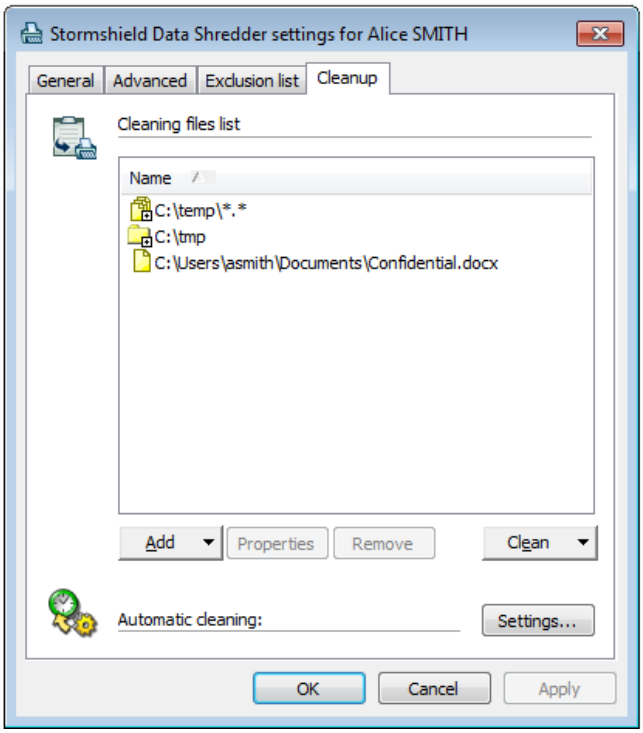
4.3.1 Setting the items for deletion

Select the items you want to include in the Cleanup list:

1. Select Stormshield Data Security systray icon > Properties > Configuration tab > Shredder. Your Stormshield Data Shredder settings window is displayed.

   NOTE
   This is common to any application configuration. You can also double-click the Stormshield Data Shredder icon on the Windows desktop.

2. Select the Cleanup tab. The list of the file(s) and folder(s) for which you want to configure automatic deletion is displayed in the main area.



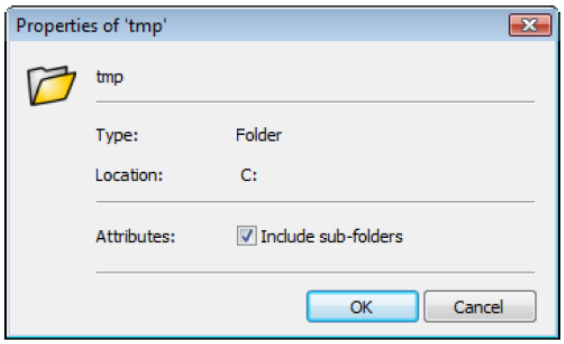
NOTE

The + sign on an icon indicates that the sub-folders are also included in the cleanup.

3. To modify the recursivity of an item (if desired):

a. Select the item.

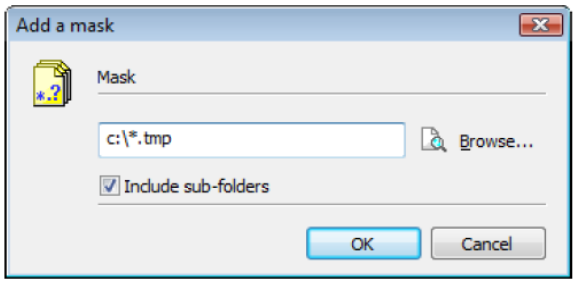
b. Click the Properties button. A new window is displayed.



c. Change the check box value and click the OK button to save the change.

4. To add files to the list in the main area, click the Add combo button and select one of the options:

- To select other files you want to have deleted automatically, click the Add files option.
- To select the folders whose content you want to have deleted automatically, click the Add folder option.
- To select automatically, especially using wildcard characters (* and ?), the types of files you want to delete, click Add mask and enter the file path or browse the drive.



Example: to systematically delete temporary files from your C drive, enter c:*.tmp

NOTE
The Include sub-folders option enables you to define the inclusion behaviour of the next creation. It has no effect to what has already been created.

5. To remove a file or a folder, select the item to be removed and click the Remove button.

4.3.2 Shredding

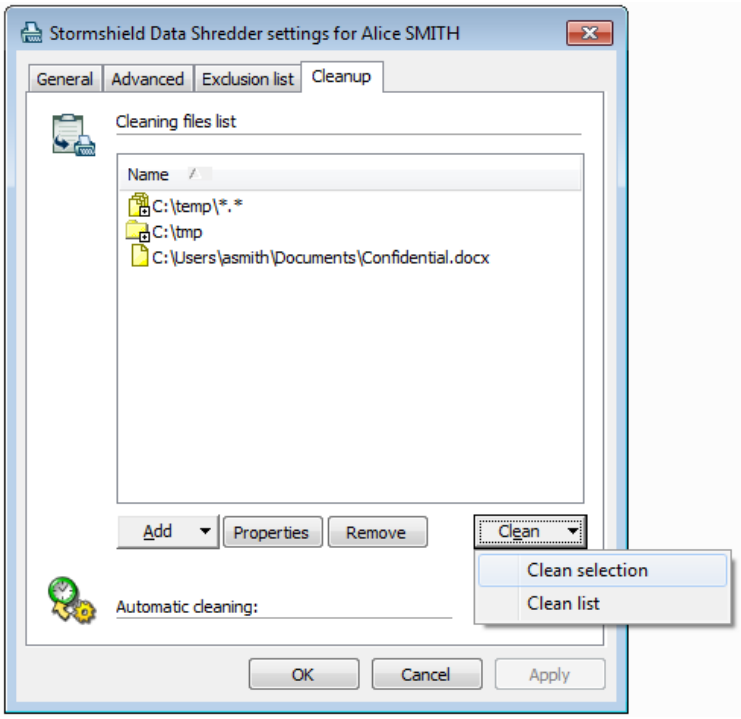
The shredding may be user-triggered or event-triggered, as described in the following sections.

User-triggered

This immediately shreds all items currently selected.

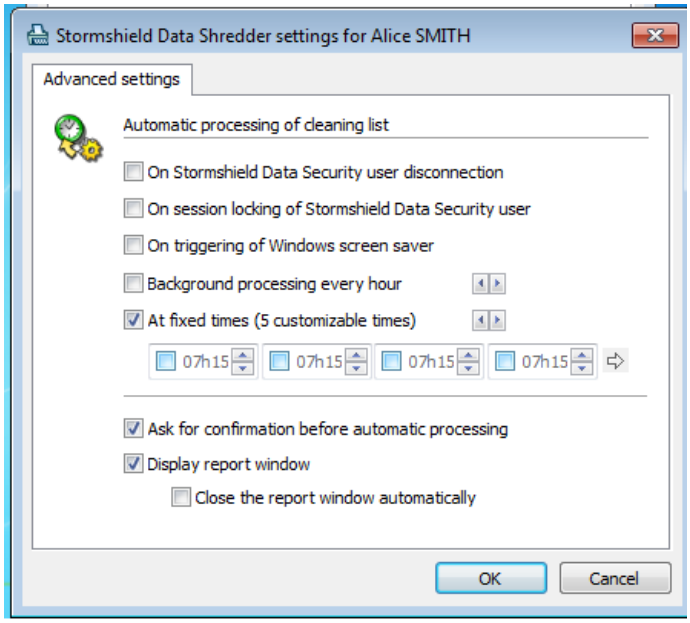
To do so, click in the Clean combo button and select:

- either the Clean selection option to clean all items currently selected
- or the Clean list option to clean all items meeting the list criteria



Event-triggered

1. To select the events required to trigger the shredding of all items meeting the list criteria, click the Settings button; a new window, containing the Advanced settings tab, is displayed.



2. Select the triggering event(s) or periodicity or times within a day:

- whenever the Stormshield Data Security user disconnects, whether it is manually via the Stormshield Data Security menu in the task bar, or automatically at the time the Windows session is closed (or at events producing the same effect: smart card withdrawal, screen savers, ...)
- whenever the Stormshield Data Security session is locked
- whenever the Windows screen saver is triggered
- as a background task, at user-configurable intervals (may be set from five minutes to eight hours)
- at fixed times (step: 1 minute)

3. Optionally ask for confirmation before automatic processing.
4. To set Stormshield Data Shredder so that a confirmation is required prior to automatic shredding and a report is displayed once the deletion is complete, check the Display report window box.

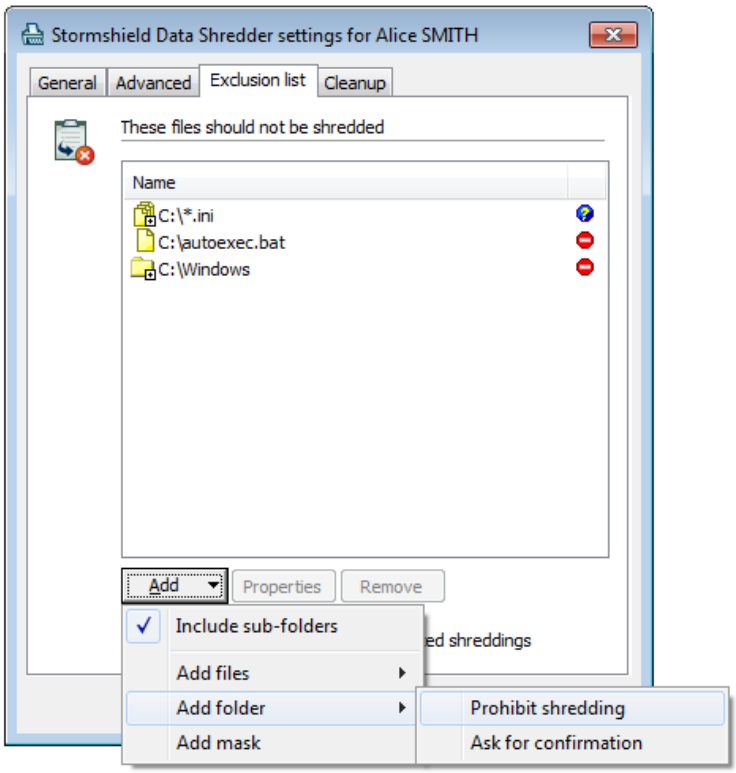
> **NOTE**
> The value of the Close the report window automatically check box repeats exactly that displayed in the report (see Section 4.1, "Using the right-click option").

4.4 Protecting files from deletion

For safety reasons, it may be useful to "lock" certain files to ensure that they will not be shredded by mistake, either during automatic processing, or manual Windows Explorer/drag-and-drop operations. For example, to avoid shredding parameter files for various user accounts, you can protect the folder containing the Stormshield Data Security users accounts (refer to the *Installation and Implementation guide* to locate this folder).

To protect files:

1. Select the Exclusion list tab in the Stormshield Data Shredder settings window. An interface similar to that of automatic cleanup lists is displayed. The files/folders in the exclusion list are marked with a prohibition icon or a question icon on the right of the name according to the exclusion type (see below).



2. You may want to add files or folders to the exclusion list, for unconditional immunization or deletion after confirmation:

- to add files and unconditionally prohibit shredding, click Add > Add files > Prohibit shredding
- to be notified before the file is deleted, click Add > Add files > Ask for confirmation
- to add folder and unconditionally prohibit shredding, click Add > Add folder > Prohibit shredding
- to be notified before the folder is deleted, click Add > Add folder > Ask for confirmation

NOTE
The Include sub-folders option enables you to toggle the mode, just as the similar option in the Cleanup tab does. Changing the mode in either tab updates the display in the other.

- to select automatically, especially using wildcard characters (* and ?), the types of files you want to lock, click Add mask and enter the file path or browse the drives

example 1: Protection of the Stormshield Data Security profile files. To protect files in the Stormshield Data Security profile, use wildcard expressions, such as **.usr. This will block shredding of all files with the usr extension, on all drives in the system.

example 2: Browsing a drive to protect files. The Browse button enables you to enroll all files in the system folder, by default C:\WINDOWS\or in the Stormshield Data Security installation folder, by default C:\Program Files\Arkoon\Security BOX

3. To remove files or folders from the exclusion list, click Remove.

NOTE

If a file/folder is included in both lists (Cleanup and Exclusion lists), the exclusion overrides the former. Therefore it will not be erased.

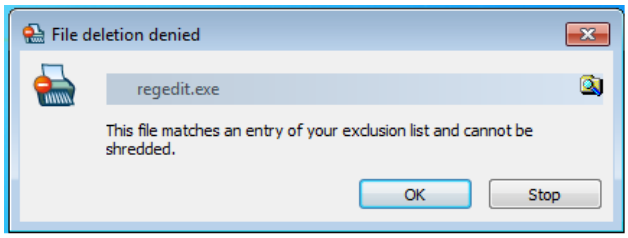
When several exclusion rules apply to a file (for example one covering c:\tmp and the other c:\tmp\folder1), the more restrictive one applies: if one requires confirmation and the other excludes it immediately, the file will be excluded without any confirmation.

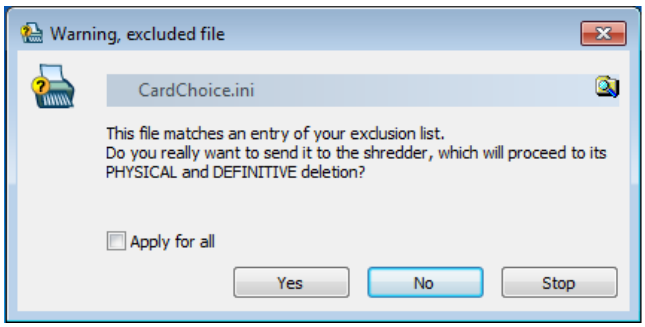
Exclusion rules are enforced between the check of hidden/system files and that of read-only files. In other words, if the rules are as follows:

1. the hidden/system files must not be erased
2. a confirmation request for the files in the exclusion list is required

A file for which these two rules apply will not be erased, and no confirmation request will appear.

If you try to erase a locked file, one of the following windows will be displayed:





In the second window, check the Apply for all box to apply your answer (Yes or No) to all files.

documentation@stormshield.eu