GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA FILE

Files and folders encryption

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-sd_file-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 File. It describes the functions of Stormshield Data File 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

This chapter describes the features and characteristics of Stormshield Data File.

1.1 Protecting data confidentiality

Stormshield Data File is a data processing security software, which preserves the confidentiality of your data. Stormshield Data File provides the following security features:

- Confidentiality of files: only authorized users may access the contents of encrypted files.
- Automatic encryption and decryption, based on user-defined event triggers.
- Safe deletion of the original plain file after encryption, leaving no recoverable trace of the original file on your hard disk.

In addition, Stormshield Data File provides file compression. Before encrypting your files, Stormshield Data Security compresses them in order to decrease their size.

1.2 Complementary file protection methods

Stormshield Data File offers several complementary file protection methods:

- Files can be encrypted for your personal use or for a correspondent or a group of correspondents using your public key. Correspondents can decrypt the files using their private key
- Files can also be encrypted in order to be self-decryptable using a password or encrypted using Security BOX SmartFILE format

Stormshield Data File secures individual files, or files contained in folders and managed lists of files which may be located on the local workstation or available over the network. Lists are used to encrypt and decrypt files when predetermined events take place.

1.3 Integration into Stormshield Data Security

Stormshield Data File is fully integrated into Stormshield Data Security (public key solutions); this will allow you to use any existing account with previously installed keys and certificates in order to access all the Stormshield Data Security components installed on your computer.

For more information, refer to the *Installation and Implementation guide*.

1.4 Public key encryption

Stormshield Data Security uses the public key encryption technology.

Each correspondent has a pair of keys: a private key and a public key. The private key is carefully kept by its owner. The public key, by contrast, is freely distributed.

This pair of keys is used for encrypting and sharing confidential documents, as explained below.

Stormshield Data Security can use one of the following:

- a unique pair of keys for encrypting and signing
- two different key pairs, one for encrypting, the other for signing
- one key pair for encrypting only or signing only

1.4.1 Encryption

The sender initializes file encryption using either their public key, or the public key of the correspondent(s) if the file is to be sent. The correspondent then uses his private key to decrypt the file. Since the user or correspondent(s) are the only ones who have the private key, they are assured that the data cannot be read by a third party.

To decrypt an encrypted file which has been sent, the correspondent must have either Stormshield Data File or Security BOX SmartFile. However, Stormshield Data File can decrypt any type of encrypted files while Security BOX SmartFile can decrypt only files intended to be read by Security BOX SmartFile.

If the file is a self-decrypting file, no application is required to decrypt the file.

1.4.2 Certificates

In order to share encrypted files with correspondents, you need to know the public key of your correspondents.

Public keys are distributed as certificates. A certificate is an electronic document that links a public key to its owner. Stormshield Data Security manages certificates with the X.509 v3 format.

> **IMPORTANT**
> In case of encryption key or certificate renewal, the previous encryption certificate and associated key must be kept in the Stormshield Data Security user account in order to be able to decrypt previously-encrypted files.

For more information on exporting and importing certificates, see the *Installation and Implementation guide*.

1.4.3 Trust

A certificate links a public key to an identity. You can only use the certificate if you trust this link.

If, for example, you want to send an encrypted message to Alice, you must be sure that the certificate actually belongs to Alice. If not, there is a risk that the message has not been encrypted with Alice's real key, but with the key of an impostor who can then decipher your message.

Two techniques enable the trust of a certificate to be established:

- inherited trust is based on the principle that if you trust a certification authority, you implicitly trust the certificates that it distributes.
- explicit trust means that you need to verify the origin of the certificate yourself. One way to do this is to check a parallel source of information (telephone, publication, mail, website, etc.).

1.4.4 Trusted address books

Stormshield Data Security includes a trusted address book: you can use it to insert the certificates of trusted correspondents and authorities.

The management of trusted address books and certificates is described in the *Installation and Implementation guide*.

1.5 A secured connection to Stormshield Data Security

Access to your keys is protected: to be able to use your keys, you must connect to Stormshield Data Security, a process which involves self-authentication, i.e. proving that you are actually the owner of the keys.

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*.

1.6 Compatibility with Security BOX SmartFile

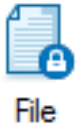
Stormshield Data File includes Security BOX SmartFILE. It is therefore possible to use all the functions provided by Security BOX SmartFILE, when Stormshield Data File is installed. This allows you to generate:

- Security BOX SmartFILE-encrypted documents in order to share them with correspondents who use Security BOX SmartFILE and do not have Stormshield Data File
- self-decrypting files and share them with correspondents who do not have Security BOX SmartFILE nor Stormshield Data File

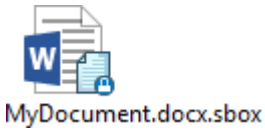
The Security BOX SmartFILE functions are selected in a transparent way from the Stormshield Data File context-sensitive menu via the Stormshield Data Security > Encrypt to choice.

NOTE
The Stormshield Data Security installation program automatically detects if Security BOX SmartFILE is already installed and deactivates it so that Stormshield Data File is used instead.

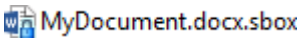
1.7 Encryption pictograms

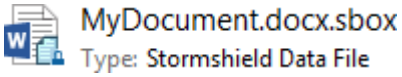


The following pictogram combined with the original Windows icon identifies secured folders or files, as described below.



These indicate that the file is encrypted. If you are not authorized to view or modify this file, you will not be able to open it.





2. Installing Stormshield Data File

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 File

Stormshield Data File 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. Interacting with Stormshield Data File

In Windows Explorer, you can right-click on the file(s) and folder(s) to select Stormshield Data File encryption and decryption functions.

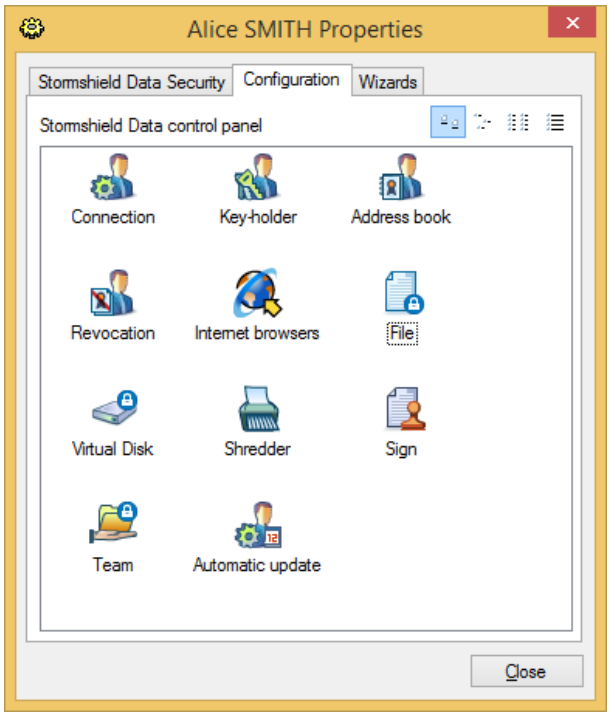
4. Configuring Stormshield Data File

This chapter tells you how to configure general and advanced settings.

4.1 Displaying the option setting window

To access the option setting window:

- from the system tray, right-click the Stormshield Data Security icon and select Properties
- from the Properties window, go to the Configuration tab and double-click the File icon

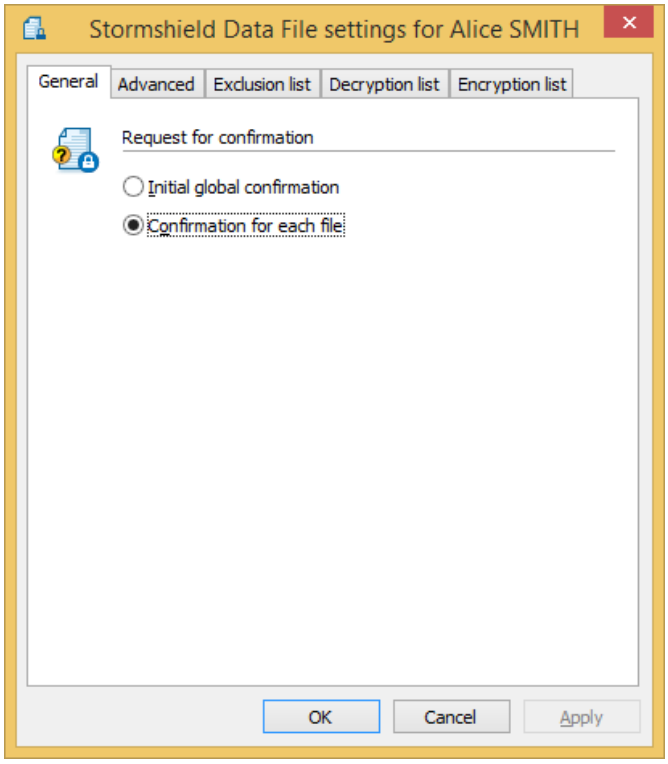


- select the General or Advanced tab according to your needs

> **NOTE**
> The other tabs (Encryption list, Exclusion list, and Decryption list) are not described in this section.

4.2 General configuration

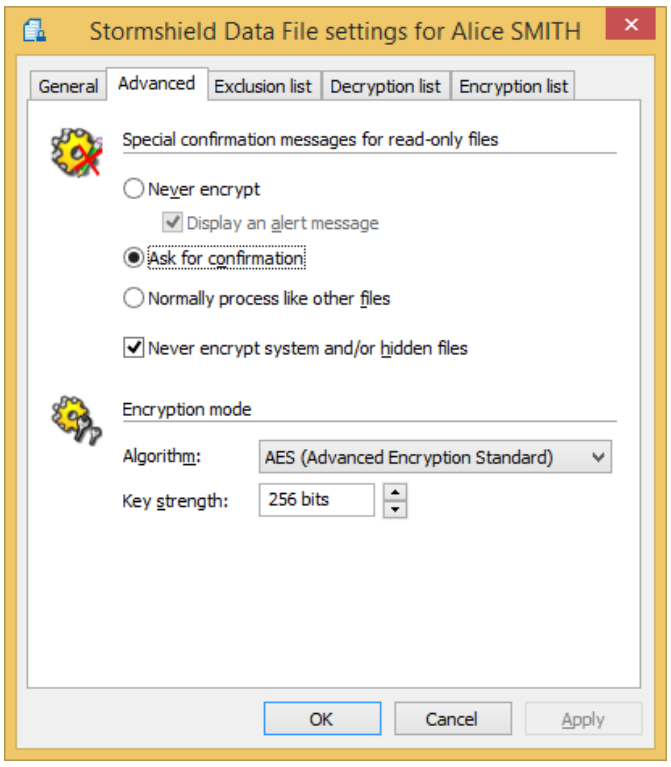
The General options window is shown below:



The General tab is used to configure the confirmation options. Select Initial global confirmation if you plan to frequently encrypt a large number of files. If you plan to encrypt files occasionally, keep Confirmation for each file, which is the default option.

4.3 Advanced configuration

The Advanced settings window, meant for expert users, is shown below:



The Special confirmation messages for read-only files section enables you to define the confirmation message that will be displayed when trying to encrypt read-only, hidden, 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 encrypt read-only files.

You can ensure a notice is sent when attempting to encrypt a read-only file (check the box Display an alert message).

- receive a confirmation request before encryption
- process them as if they are not read-only

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

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

The encryption mode can also be configured by specifying:

- the algorithm used for encryption
- the key strength

> **NOTE**
> For security reasons, it is recommended to use the AES algorithm with 256 bits key strength.

5. Encrypting and decrypting file

This chapter describes how to:

- encrypt files for your personal use or to send to recipients
- decrypt files
- generate a self-decrypting file or a Security BOX SmartFILE-encrypted file

It also describes how to recover a password used for the encryption of a self-decrypting or Security BOX SmartFILE-encrypted file.

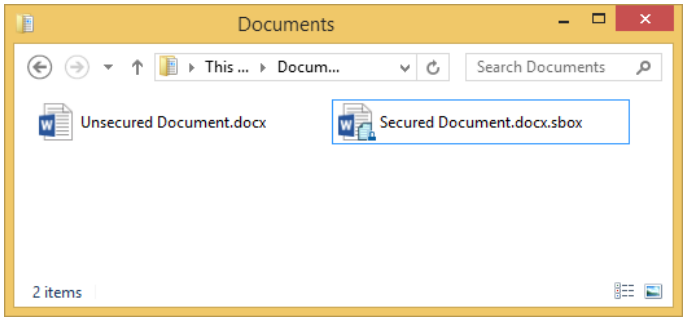
5.1 Encrypting a file or a folder

This section describes how to encrypt files which:

- you will be the only one to use
- you will send to one or several correspondents

Files encrypted using Stormshield Data File are identified as follows:

- by the presence of a small icon appearing over the initial icon image, as shown below
- by the .sbox extension file, as shown below

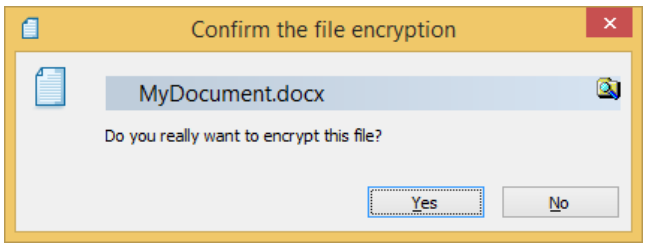


NOTE
The procedures described below use the right-click method and apply to both files and folders. You can also select and encrypt files and folders simultaneously.

5.1.1 Encrypting files for your own use

1. Select the file(s) to encrypt and right-click to select the **Encrypt the files** option (or **Encrypt the file**.

The following window is then displayed:



2. Confirm your choice. In case of a multiple-file selection, and according to the options previously set (refer to Section 5.2, "General configuration"), you will be prompted for one of these:

- an initial and global confirmation; all the files will be processed and you will no longer be asked to confirm the encryption task.
- a confirmation per file; to temporarily deactivate the confirmation for each file, un-check the appropriate checkbox in the confirmation pop-up window. This does not modify the options which were previously configured and will apply the next time an encryption is run.
- If you select a file that has already been encrypted, Stormshield Data File will ignore this file and will process the other ones.
- Empty files cannot be encrypted. Trying to encrypt empty files results in an error displayed in the summary window.

3. An encryption progress window is displayed; once the encryption is completed, a summary window is displayed.

Click **Details**.

To automatically close the window at the end of a successful encryption, check **Close the window automatically**. This option will be kept for any additional encryption to complete and will also apply during the decryption operation. However, this option will be ignored if errors occur during the operation.

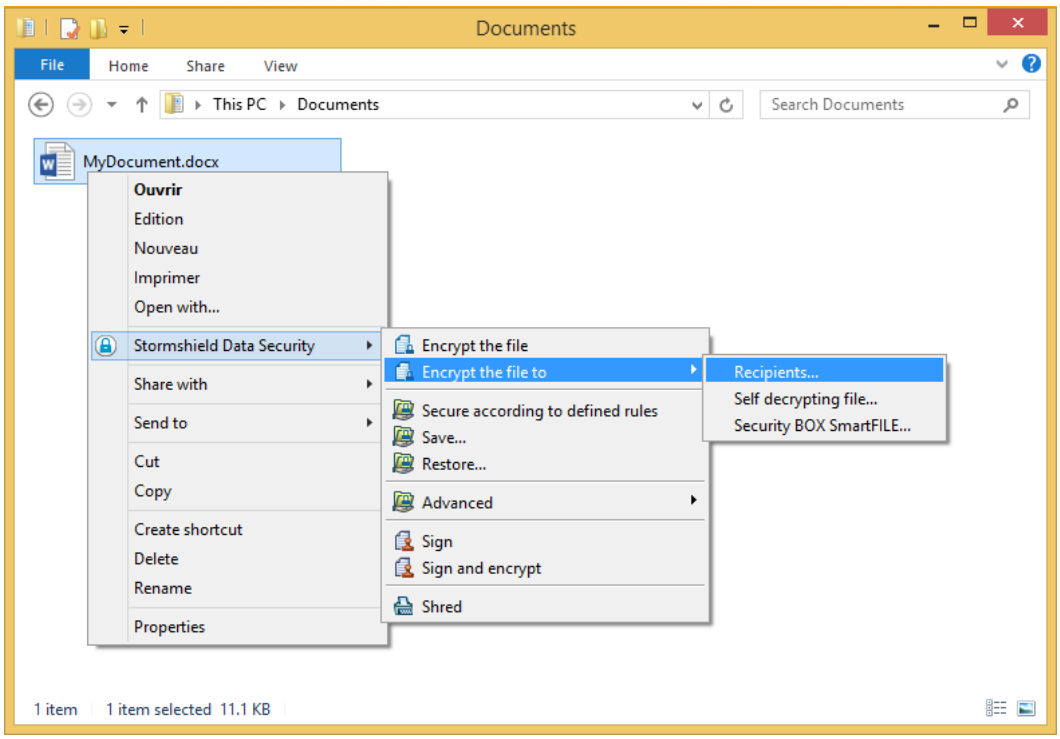
To manually close the window, wait until the encryption completes and click **Close**.

> **NOTE**
> After encryption, the source file (not encrypted) is suppressed in a secured way; three encryption passes are used (as with Stormshield Data Shredder).

5.1.2 Encrypting files to send to a recipient

Use the following procedure to encrypt files to send to a third party.

1. Select the file to encrypt and right-click to select the **Stormshield Data Security** > Encrypt to > Recipients option as shown below.



2. The list of users able to decrypt the file is displayed. Search for users or groups who will be allowed to access the file. The search displays users specified in the trusted address book as well as users from the LDAP directory if it is configured.

5.2 Decrypting a file or group of files

This section explains how to decrypt one or several files encrypted using Stormshield Data File.

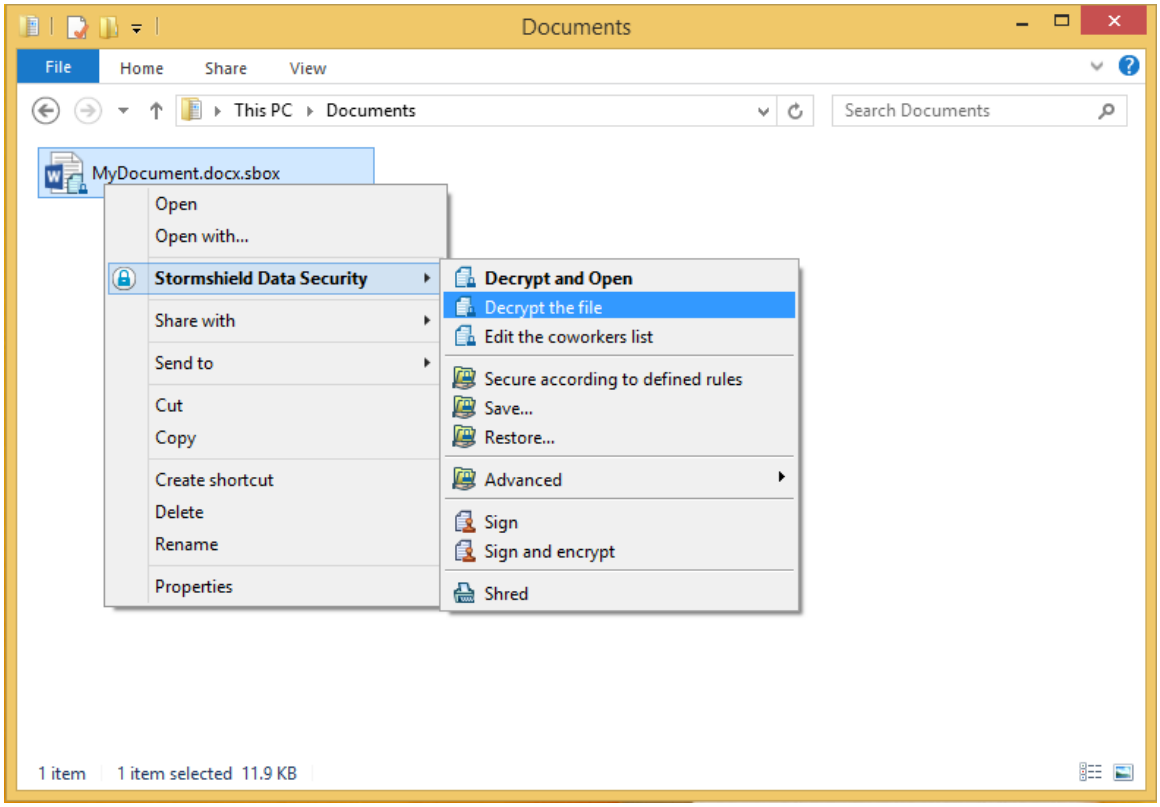
Files with the .sdsx, .sbo or .sbox file extensions can be simultaneously selected and will be processed in the same way.

If you select a folder, Stormshield Data File will decrypt only the files which you have previously encrypted or the encrypted files which had been sent to you. Other files will be ignored and will not be processed.

To decrypt a single file, double-click on it. The file is automatically decrypted and opened with the default application. To decrypt a file without opening it, use the procedure described below.

To decrypt several files, use the following procedure.

1. Select the desired file/folder and right-click to select the Stormshield Data Security > Decrypt or Stormshield Data Security > Decrypt and Open choice as shown below.



An encryption progress window is displayed and shows for each file the result of the task being performed.

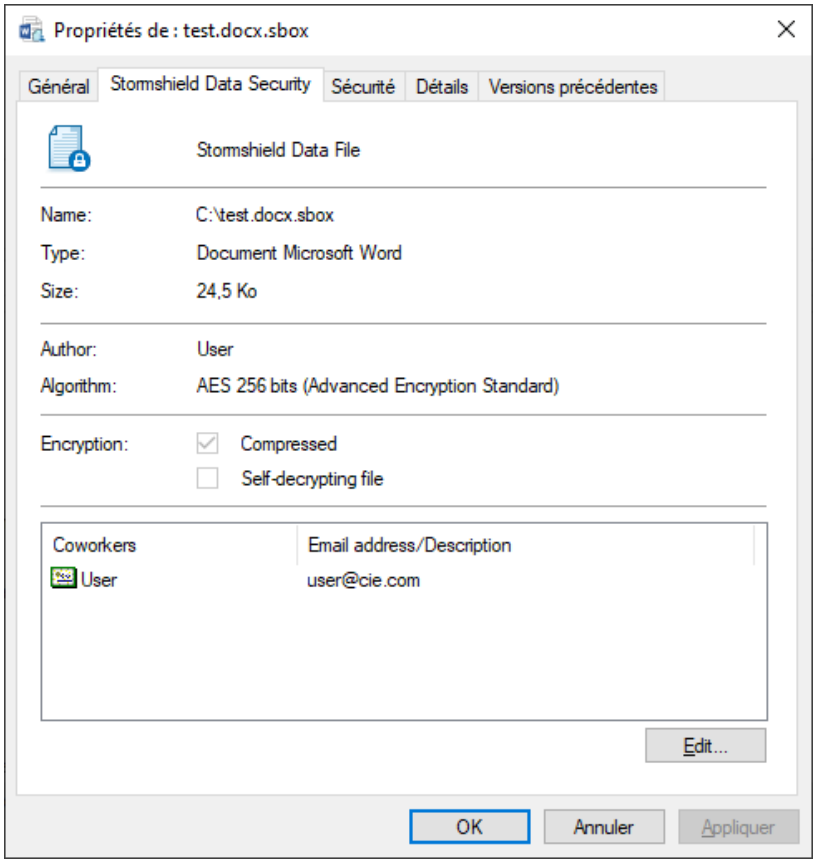
NOTE
For ergonomic and technical reasons, it is not recommended to run the Decrypt and Open function on a large number of files.

2. To automatically close the window at the end of a successful decryption, check Close the window automatically. This option will be kept for any additional decryption to complete. However, this selection will be ignored if errors occur during the decryption process.

To manually close the window, wait until the encryption completes and click Close.

5.3 Displaying encrypted file properties

The properties for encrypted files list the users for whom the file was encrypted and who are therefore able to decrypt it.



In addition to the usual information (file name, type and size), the Properties window indicates:

- the name of the user who has encrypted the file
- the algorithm used for encryption
- the file attributes:
- Compression indicates whether the file has been compressed using Stormshield Data File. This attribute is different from the standard attribute available for a Microsoft Windows file. This property only concerns the *.sbox* format.
- Self-decrypting indicates whether the file is a self-decrypting file. Refer to Section 4.4, "Generating a self-decrypting file" for further information.
- the name and e-mail address of the persons who can decrypt the file (only if you are connected).

5.4 Managing coworkers on an encrypted file

Coworkers associated to an encrypted file can be managed from the properties window of this file. You can:

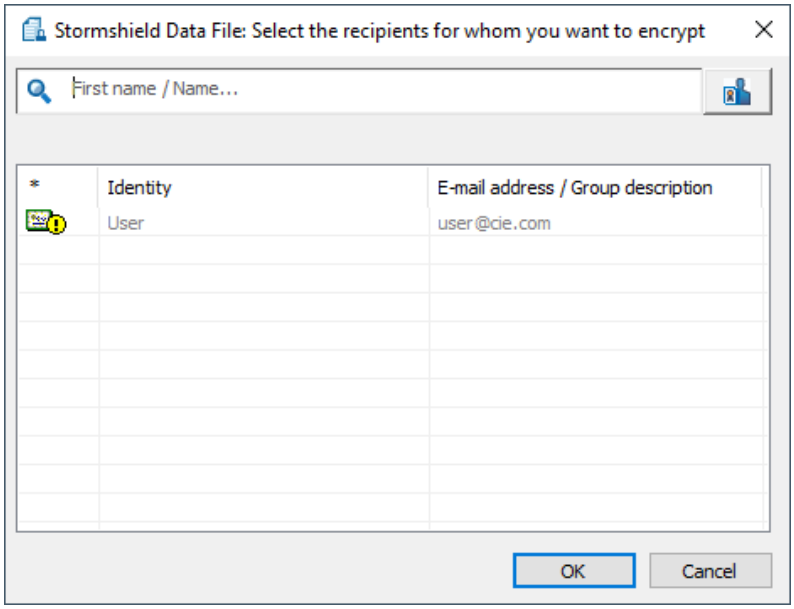
- Add one or more coworkers from your address book.
- Remove one or more coworkers associated to the encrypted file.

To add coworkers:

1. Open the **Properties** of an encrypted file and select the *Stormshield Data Security* tab or right-click the encrypted file and select **Stormshield Data Security > Edit the coworkers list**.

   NOTE
   The submenu **Stormshield Data Security** > **Edit the coworkers list** is no longer available from Microsoft Windows 10.

2. Click on **Edit**. The following window opens:



3. Search the coworkers or groups to add and click **OK**.
4. Click **Apply** and **OK** in the **Properties** window to apply the modifications. If you click **Cancel**, the modifications are not taken into account.

To remove coworkers:

1. In the **Properties** window, select the coworkers and click **Delete**.
2. Confirm and click **Apply** and **OK** in the **Properties** window to apply the modifications. If you click **Cancel**, the modifications are not taken into account.

   CAUTION
   These features are available only if you are connected or if you have rights on the file.

   NOTE
   Your trusted address book can be displayed from the coworkers list in order to update certificates.

5.5 Generating a self-decrypting file

Self-decrypting files are Windows-32 bits executable files which contain both the encrypted data and the decryption program required to decrypt the data. Access to the file is password-

protected. The password must be shared between the correspondents using a secured and confidential communication way and is required to run the decryption program.

When a self-decrypting file is received on a workstation running Stormshield Data File, the file decryption program contained in the self-decrypting file is not actually run to decrypt the program. Instead, a Stormshield Data File function is automatically activated and decrypts the encrypted data.

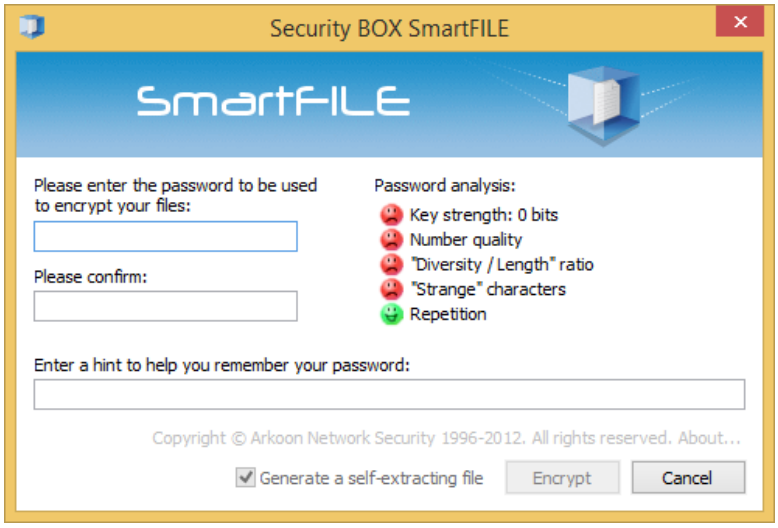
CAUTION
Some gateways prevent executable files from accessing the networks they control and block Stormshield Data File executable files. Similarly, some e-mail systems can block executable files attached to incoming messages.

The following rules apply:

- when you create a self-decrypting file, the source file is not deleted.
- you can encrypt several files and folders simultaneously. A self-decrypting file will be created for each selected file.

To create a self-decrypting file:

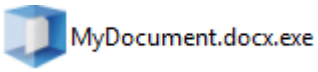
1. Select the desired file and right-click to select Stormshield Data Security > Encrypt to > Self-decrypting file.
2. Enter the password required for the decryption and a hint (optional).



NOTE
By default, the password you are entering is not displayed and must be entered twice for confirmation. To display the password you are entering and avoid re-entering it, right-click in the password field area and select the Display the password choice. Use the same procedure to restore the default setting.

3. Check Generate a self-extracting file.
4. Click on Encrypt. The file is encrypted with the entered password.

Self-decrypting files are identified with the .exe extension file as shown below.



5.6 Generating a Security BOX SmartFILE file

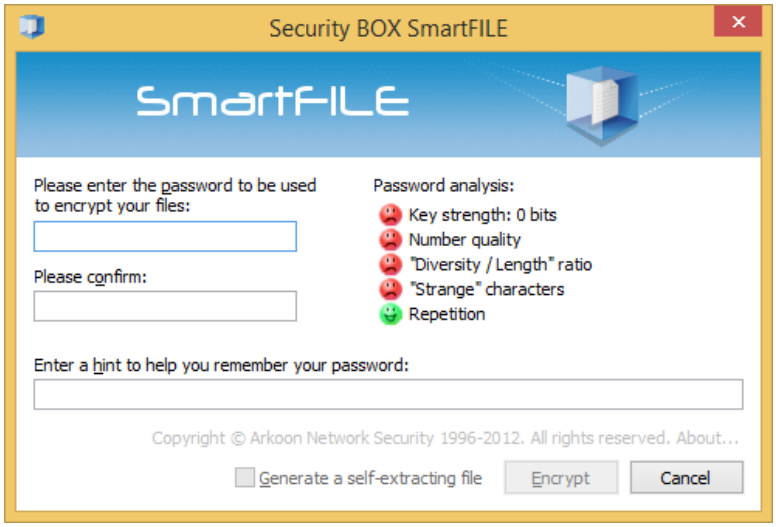
If you need to send encrypted files to recipients who do not have Stormshield Data File but use Security BOX SmartFILE instead, Stormshield Data File allows you to generate Security BOX SmartFILE- encrypted files.

The following rules apply:

- the original files are not deleted after encryption.
- you can encrypt several files or folders. A Security BOX SmartFILE file will be created for each selected file.
- The names of the encrypted files must not contain Unicode characters.

To create a Security BOX SmartFILE-encrypted file:

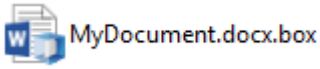
1. Select the file and right-click to select **Stormshield Data Security > Encrypt to > Security BOX SmartFILE**.
2. Enter the password required for the decryption and a hint (optional) to retrieve it later on.



By default, the password you are entering is not displayed and must be entered twice for confirmation. To display the password you are entering and avoid re-entering it, right-click in the password field area and select the **Display the password** choice. Use the same procedure to restore the default setting.

3. Click on **Encrypt**. The file is encrypted with the entered password.

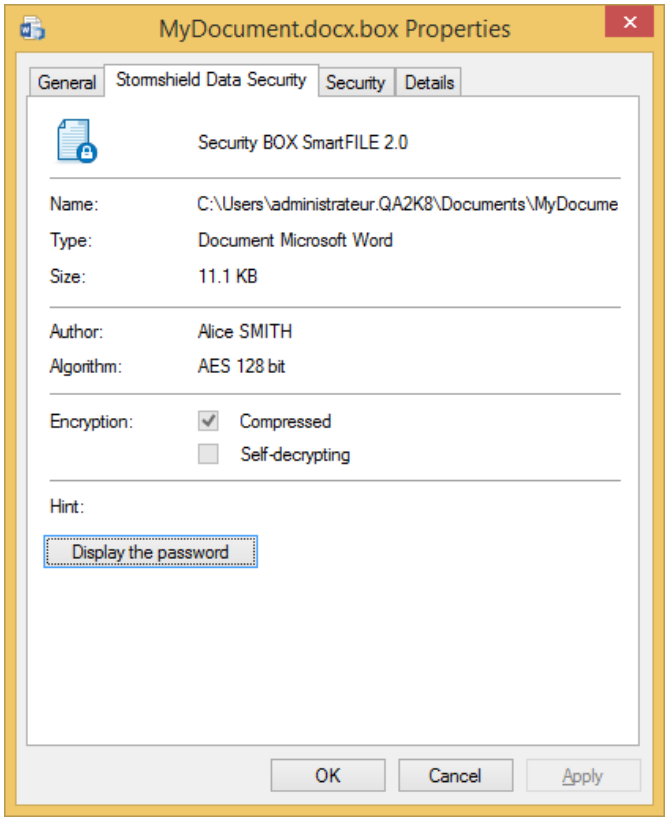
Security BOX SmartFILE-encrypted files are identified by the presence of a small lock icon and the .box extension file:



5.7 Recovering the password

If you need to recover the password used for the encryption of a self-decrypting file or a Security BOX SmartFILE-encrypted file, you can display this password from the file properties (via the Stormshield Data Security tab).

In order to use this function, you must be logged onto Stormshield Data Security using the same account as the one used for the file encryption. You cannot recover the password with another Stormshield Data Security account (including recovery accounts) or using Security BOX SmartFILE.



Click the Display the password button.

5.8 Decrypting a Security BOX SmartFILE file with a recovery account

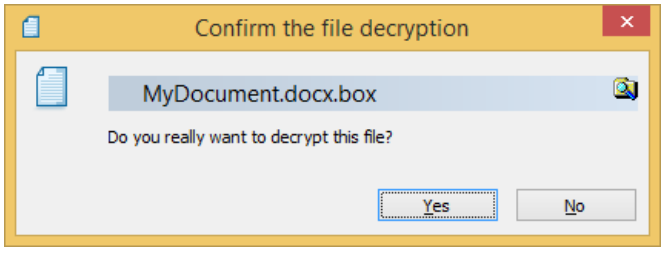
If you need to decrypt a Security BOX SmartFILE file with a recovery account:

1. Log into the recovery account.
2. Press and hold simultaneously CTRL+SHIFT keys and then double-click on the file you wish to decrypt.

OR

Press and hold simultaneously CTRL+SHIFT keys and then right-click and select SecurityBOX > Decrypt.

3. Release the CTRL+SHIFT keys. The confirmation window is displayed.



4. Click on Yes if you wish to decrypt the file.

The file is decrypted without a password.

6. Using lists

Encryption and decryption lists can be used to automate file encryption and decryption in order to make the use of the software easier and avoid file handling errors. A protected file list can also be created to protect pre-selected files from encryption. This chapter describes how to configure such lists.

6.1 Encryption and decryption lists

Files enrolled in encryption or decryption lists are automatically processed at a predetermined time or when a predetermined event takes place. For example, file encryption can be automatically started upon disconnection, at predetermined times or at set intervals.

> **NOTE**
> Try to keep this list as short as possible. Though Stormshield Data Security provides optimized time responses, decrypting a large number of files is time-consuming.

Encryption and decryption lists can also be used to manually launch a batch encryption or decryption of all of the list items or of selected ones only.

6.1.1 About recursion

Recursion of automatic file list encryption or decryption defines the sub-folder inclusion behavior. It is invoked by the **Include sub-folders** option and can take two values (on/off). It applies in various ways :

- as a mode, it applies to all items and can be activated and repeated in various screens
- as a property of a folder, it defines if only the indicated folder will be encrypted or decrypted automatically or if its sub-folders will also be
- as a property of a file, it defines if only the indicated file will be encrypted or decrypted automatically or if files with the same name, but located in other folders, will also be encrypted or decrypted
- 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 automatically encrypted or decrypted or if files with the same name, but located in other folders, will also be encrypted or decrypted

6.1.2 Managing the lists

In order to manage encryption or decryption lists, proceed as follows:

1. Select the Stormshield Data Security icon and right-click to select Properties from the context-sensitive menu.
2. From the Properties window, go to the Configuration tab and double-click on the Stormshield Data File icon; then select the Encryption list or Decryption list tab. The list of files, folders, and wildcard expressions for automatic encryption or decryption is displayed in the main window.

NOTE
The plus sign (+) next to a folder icon indicates that the sub-folders must be also included in the encryption/decryption list. To exclude sub-folders, uncheck the appropriate box in the Properties window, as explained in Step 4.

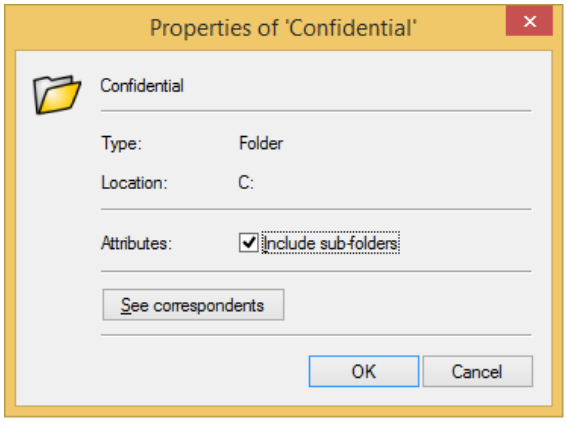
3. To activate or deactivate the default recursive mode, click on Add and select the Include sub-folders option. If the recursive mode is the default mode, selecting this option allows you to deactivate this mode.

NOTE
The new default mode will apply for next items to be added. Items already enrolled in the list are not impacted by the change and must be individually updated as explained in Step 4.

4. To modify the recursion 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 OK to save your changes.

5. To enroll a new list item, click the Add combo button and select one of the options:

- to select other files, click the Add files option
- to select another folder, click the Add folder option
- to automatically select the files you want to process using wild characters (* and ?), click Add mask and enter the path or browse the drives

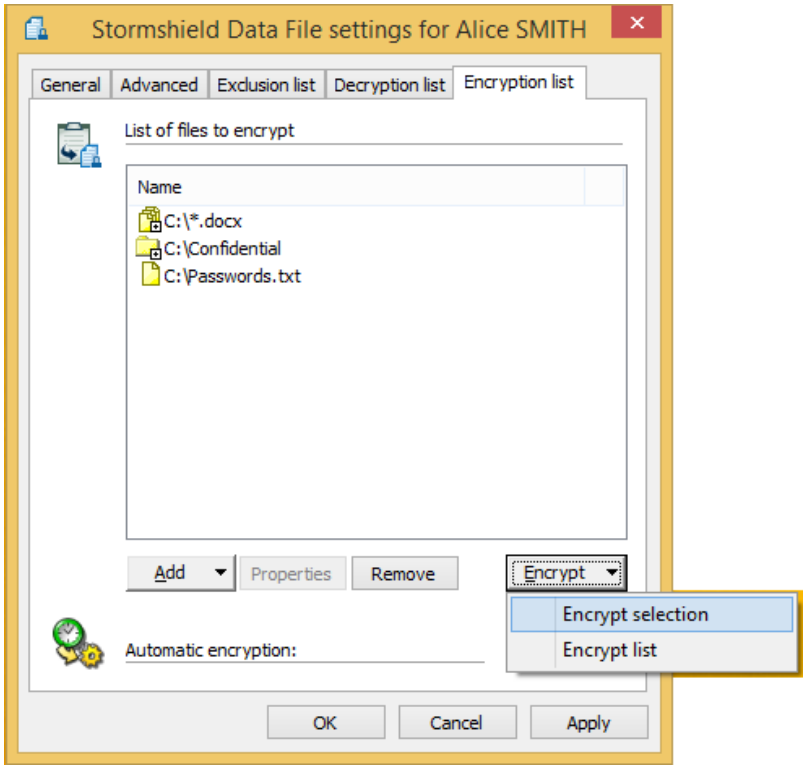
6. To remove one or several items from the list, select the item(s) to be removed and click the Remove button.

To customize the events that will trigger the automatic encryption or encryption, or launch an immediate encryption or decryption of the list items, refer to Section 6.1.3, "Encrypting or decrypting files".

6.1.3 Encrypting or decrypting files

Encrypting or decrypting a list of files can be user-triggered or event-triggered:

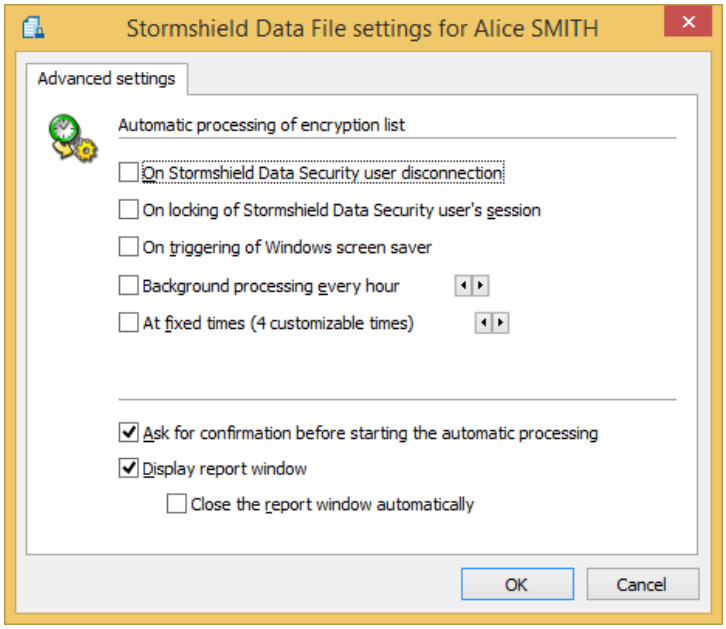
- user-triggered: to immediately encrypt or decrypt the whole list or only the items currently selected, click Encrypt or Decrypt.



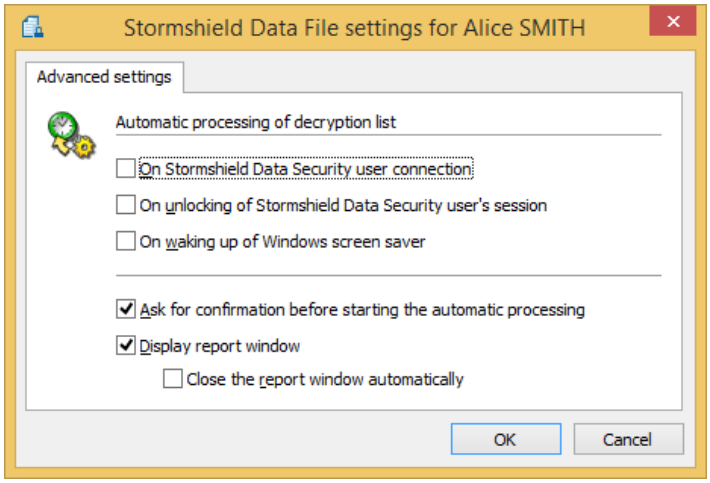
- event-triggered:

1. Select Settings to specify the events required to trigger the encryption or decryption of all items meeting the list criteria.

- the following window shows the events that can be selected to trigger automatic file encryption:



- the following window shows the events that can be selected to trigger automatic file decryption:



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

- for encryption:
- whenever you connect to Stormshield Data Security whether you manually disconnect via the Stormshield Data Security menu in the task bar automatically disconnect when closing your Windows session.
- whenever your Stormshield Data Security session is locked
- whenever the Windows screen saver is triggered
- as a background task at specified intervals of times or at fixed times
- for decryption:
- whenever you connect to Stormshield Data Security
- whenever your Stormshield Data Security session is unlocked
- whenever the Windows screen saver is waken up

3. Optionally, you can also set the following options:

- Ask for confirmation before automatic processing.

  NOTE
  The confirmation request is slightly delayed. If you do not reply within the next 10 seconds, the process is launched. This allows starting the automatic file processing even if you are away from your workstation. When a confirmation is requested, you must reply within the next 10 seconds to cancel the automatic processing.

- Display report window, to display a report upon completion of the task. If you choose to automatically close the report window, the window will close automatically if no error has occurred.

6.2 Protected file list

In order to protect files from encryption, you can lock certain files and folders to make sure that they are not encrypted by mistake. In order to lock specific files and folders, create an exclusion list.

- The recursion principles, explained in Section 6.1.1, "About recursion", apply to the exclusion list. Refer to that section for further information.

- To prevent file encryption in the system folder (C:\WINDOWS\ by default) and the Stormshield Data Security installation folder (C:\Program Files\Arkoon\Security BOX by default), it is recommended to add these folders to the exclusion list.

To create or modify an exclusion list:

1. Select the Stormshield Data Security icon and right-click to select Properties from the context-sensitive menu.
2. From the Properties window, go to Configuration tab and double-click on the Stormshield Data File icon.
3. Select the Exclusion list tab. The list of files, folders, and wildcard expressions for automatic exclusion is displayed in the main window.

The ⛔ icon displayed next to a folder or a file icon indicates that it cannot be encrypted.

The ❓ icon displayed next to a folder or file icon indicates that a confirmation is to be requested before encrypting the file or folder.

4. To activate or deactivate the default recursive mode, click Add and select the Include sub-folders option. If the recursive mode is the default mode, selecting this option allows you to deactivate this mode.

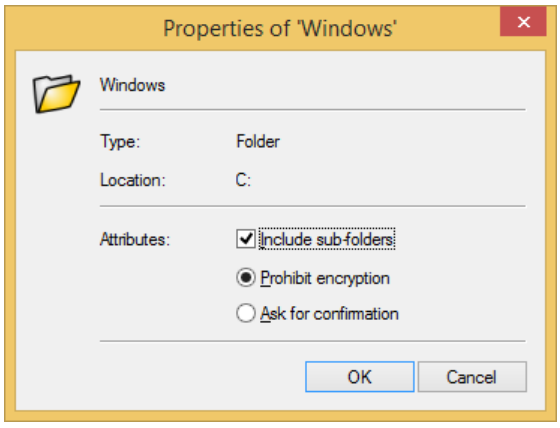
> **NOTE**
> The new default mode will apply for next items to be added. Items already enrolled in the list are not impacted by the change and must be individually updated as explained in Step 4.

The flag used to configure the recursive mode parameter is shared with the encryption and decryption lists. When you modify the option in one tab, it is automatically updated in the other tabs.

5. To modify the recursion 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 OK to save your changes.

6. To enroll a new list item, click the Add combo button and select one of the options:

- to add files and unconditionally prevent encryption, select the Add files > Prohibit Encryption option
- to add files and be notified before file encryption, select Add files > Ask for confirmation. option
- to add folders and unconditionally prevent encryption, select the Add folder > Prohibit Encryption option

- to add folders and be notified before file encryption, select Add folder > Ask for confirmation. option
- to automatically select the files you want to lock using wild characters (* and ?), select Add mask and enter the path or browse the drives

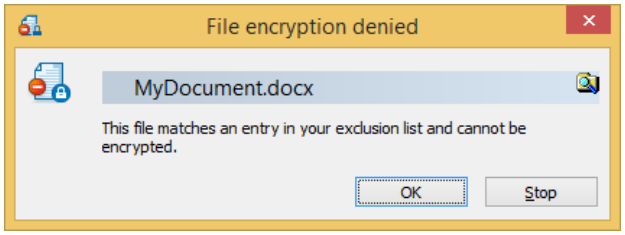
For example, to protect files in the Stormshield Data Security accounts, use wildcard expressions, such as *:*.usr. This will block encryption of all files with the usr extension, on all drives in the system. In fact, it is recommended to prohibit encryption of the C:\Program Files\Arkoon\Security BOX folder.

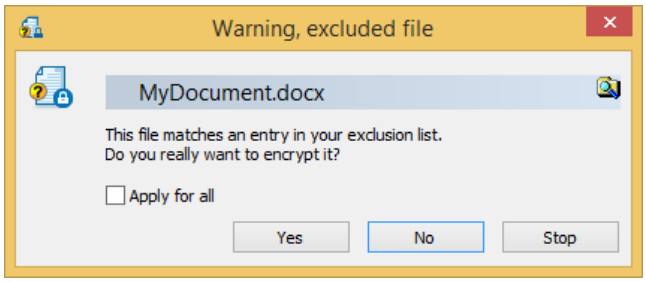
The Browse button enables you to enroll all files in the default C:\WINDOWS\ system folder, or in the default C:\Program Files\Arkoon\Security BOX Stormshield Data Security installation folder.

NOTE
The recursive mode applies not only to the folder but also to the files and wildcard characters. For example, when the recursive mode is enabled, c:\tmp\MyDocument.txt includes all the MyDocument.txt files in the c:\tmp folder and any of its sub-folders. In the same way, c:\tmp*.doc includes all the files with the .doc file extension in the c:\tmp folder and any of its sub-folders.

7. To remove one or several items from the list, select the item(s) to be removed and click the Remove button.

If Stormshield Data File tries to encrypt a protected file, one of the following windows is displayed provided that the appropriate checkbox (Display a warning message for rejected encryptions) has been selected in the Exclusion list window.





In the latter window, check Apply for all to apply your choice (Yes or No) to all files.

6.2.1 About the exclusion rules

1. If a file/folder belongs to both the encryption and exclusion lists, the exclusion overrides the former. Therefore, the file will not be encrypted.
2. When several exclusion rules apply to a file, the most restrictive one applies. If one requires confirmation and the other excludes it unconditionally, the file is excluded without any confirmation request.
3. 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:

a. the hidden/system files must not be encrypted.
b. a confirmation request for the files in the exclusion list is required

A file for which these two rules apply will not be encrypted without a confirmation request.

7. Transciphering encrypted files

This chapter describes how to transcipher encrypted files.

7.1 Introduction

Stormshield Data File allows you to update the list of users authorized to access files encrypted with Stormshield Data File. You can add or remove users. When updating the list of authorized users, Stormshield Data File re-encrypts the file(s) using a new encryption key. This operation is referred to as file “transcipherment”.

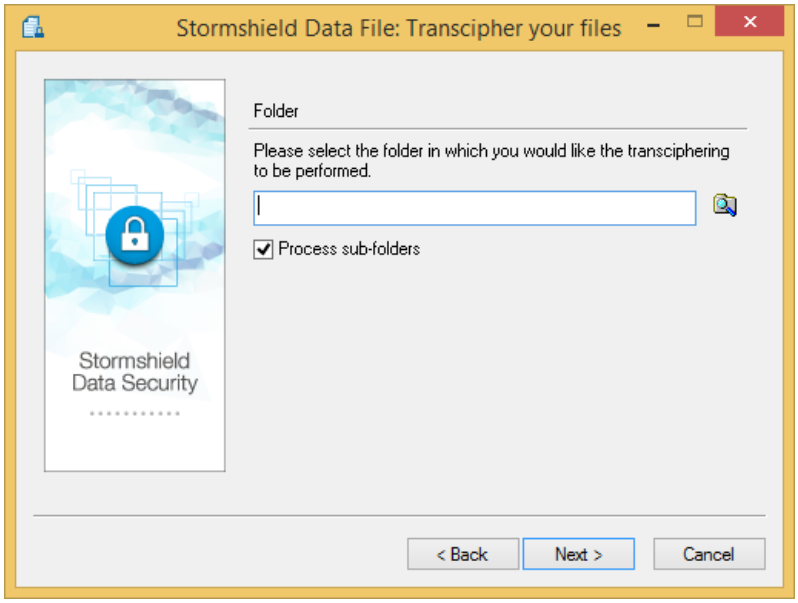
Encrypted files are transciphered to their original formats: if they are in .sbox, they will remain in .sbox after transcipherment.

7.2 Transciphering your files

Before you start, make sure you have the certificates for each new user to be added. This certificate can be directly sent to you or obtained from your trusted address book or an LDAP directory.

To update the authorized user list and re-encrypt your files:

1. From the Start menu, select Programs, then Stormshield Data Security.
2. Select Stormshield Data File > Transcipher your files. A welcome page is displayed. Click Next.



3. Select the folder containing the files to transcipher. In order to include files located in sub-folders, check the Apply to sub-folders box and click Next. Valid user certificates that have been extracted from your trusted address book are displayed.
4. Select the ones to be added to the list. If some are missing from the list, click on the icon in order to update your trusted address book by importing new user certificates directly from files or from an LDAP directory. Click Next.
5. Click YES, I remain a user of these file to continue being able to access the files you are about to re-encrypt. Otherwise, click NO, I am no longer a user of these files. The option you choose has no effect if you transcipher a file:

- with a decryption key (you will not be added to the users allowed to decrypt the file, but will be able to access the file as long as you can use the decryption key).
- with a private key for your personal use. You will be automatically added to the list of users allowed to decrypt the file.

Click Next.

6. Check the information displayed and click on Finish. The assistant looks for the files in the specified folder and transciphers them. When the task has completed, a report displays all the processed files in a tree view. It provides statistics by indicating:

- the number of files to process
- the number of files processed
- the number of files for which the operation failed

For each file/folder, an icon indicates the processing result:

- : The folder has been successfully transciphered.
- : The folder has been successfully processed, but it contains files that could not be transciphered for the following reasons:
- The key was not found – you are not authorized to access the file.
- The file has been encrypted using a decryption key.
- : The folder does not contain any encrypted file.
- : The folder contains a file containing errors.
- : The file has been successfully transciphered.
- : The file has not been transciphered for the following reasons:
- The key was not found – you are not authorized to access the file.
- The file has been encrypted using a decryption key.
- : The file contains errors.

documentation@stormshield.eu