GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

ADVANCED USER GUIDE

Version 11.5

Document last updated: December 23, 2025

Reference: sds-en-sdse-advanced_user_guide-v11.5

Table of contents

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

1. Getting started

This guide is intended for administrators, and contains information that you will need to use the SDS Enterprise solution on user workstations. The guide describes the simple and advanced use of SDS Enterprise features.

SDS Enterprise guarantees the protection and confidentiality of data stored on local, shared or cloud-based folders, by relying on the transparent end-to-end encryption built into communication and collaboration tools. With it, access to protected data can also be restricted to defined groups and user profiles.

The SDS Enterprise agent installed on user workstations provides the following features:

- Real-time transparent file encryption, for transfer by e-mail or secure backup;
- automatic encryption of files stored in local folders or in folders synchronized with online hosts OneDrive, OneDrive for Business, DropBox, SharePoint and Oodrive,
- encryption and signing of e-mails to protect the data they contain and guarantee their origin and the integrity of their content,
- Sharing of encrypted files with coworkers over my company's network;
- Secure and irreversible erasure of data;
- Electronic signature of files and folders, making it possible to guarantee the authenticity of their sender's identity and the integrity of their contents;
- Encryption of virtual disks, making it possible to store protected files; These virtual disks can be shared among coworkers;

The SDMC administration console makes it possible to configure the use of features on workstations. For more information, refer to the *SDS Enterprise Administration guide*.

2. Logging in to SDS Enterprise

After installation, the SDS Enterprise agent will automatically run every time the users start Windows.

Users must log in to SDS Enterprise to use SDS Enterprise features. To do so, they must have a properly configured user account. For more information on how to create accounts, refer to the *SDS Enterprise Administration guide*.

Several users can use the same computer, but only one user per open session may use SDS Enterprise. A SDS Enterprise security policy applies to all users of the workstation.

When users connect to SDS Enterprise, their identities are verified and their keys and settings can be accessed.

In smart card or token mode, users simply need to insert their smart cards or tokens to open the SDS Enterprise menu. The connection window directly opens if the smart card or token is already inserted in the drive. If you are using a virtual smart card, log in as shown below.

To log in to SDS Enterprise:

1. Double-click on the SDS Enterprise icon  in the Windows system tray.
2. Enter the password or confidential code, depending on the account type.
3. Click on **OK**.

WARNING
If you enter your password incorrectly too many times (default is three tries), your account will be blocked. To unlock it, see the *Administration GuideSDS Enterprise*.

If you are using a Single Sign-On (SSO) account, users are connected automatically and transparently.

3. Managing SDS Enterprise account login

To change the SDS Enterprise login management settings:

1. Right-click on the SDS Enterprise icon  in the Windows system tray.
2. Select **Properties**.
3. In the **Configuration** tab, double-click **Connection**.

3.1 Choose when to request password or secret code

In the **Connection** tab, **Ask for secret code** section, choose:

- **At connection time only**: this option is recommended in most cases.
- **On each signature or decryption operation**: to ensure greater security, you can request that the password or secret code be systematically required for each operation involving the user's private key.
- **Every X minute(s)**: if you enable this option, the session will be kept open for the specified time. After this time, the password will be requested if the user performs an operation.

To prevent fraudulent use of the product, we recommend setting the SDS Enterprise account to be locked or automatically logged out when the user is inactive on their workstation. For more information, see the next sections.

3.2 Choose how often to change your password or secret code

This section applies to Password accounts only.

The more regularly you change your secret code (every X days), the less likely it is it will become detected by someone else. You will thus be better protected.

On the **Connection** tab, **Change secret code** section, select an option and use the arrows to indicate the time period:

- **Request change every x day(s).**

A window invites the user to change their password. This option ensures better password confidentiality. By changing it regularly, you limit the risk of it being known to a third party.

- **Impose change every x day(s).**

A window prompts the user to change their password.

- **Inhibit change before x day(s).**

This option stops users from changing their password before a certain period. This prevents users from changing their password once, then changing it again back to their original password. These successive changes would allow users to use the same passwords over and over again, resulting in reduced security.

4. Locking or disconnecting from the SDS Enterprise account

As a security measure, users must lock or disconnect from their SDS Enterprise accounts when they leave their workstations, to prevent access to SDS Enterprise features.

When the user locks their Windows session, removes the smart card or USB token, or the screen saver activates, the SDS Enterprise account can be automatically locked or logged out according to the settings chosen in the security policy. For more information, see the SDS Enterprise *Administration guide*.

4.1 Locking the SDS Enterprise account

Locking the account prevents access to keys. This means that the user can no longer access encrypted data, but can continue to use files that are already open by Stormshield Data Team, for example.

The locking procedure is the same for the password, smart card and token modes. Removing a smart card or token from the drive also makes it possible to lock the session. By reinserting the card or token, you will directly access the unlocking screen.

To lock the account:

1. Right-click on the SDS Enterprise icon  in the Windows system tray.
2. Click on **Lock**. The SDS Enterprise icon turns red  and the account can no longer be accessed.

When the account is locked, go to the same menu to unlock it.

4.2 Disconnecting from the SDS Enterprise account

The account can only be disconnected if the user is connected (green icon) or the account is locked (red icon).

Disconnecting means closing the SDS Enterprise account. As a result, SDS Enterprise features cannot be used. We recommend that you close any open files and running applications before disconnecting.

The disconnection procedure is the same for password, smart card and token modes. After you have disconnected, if you reinsert the smart card or token, you will access the connection screen.

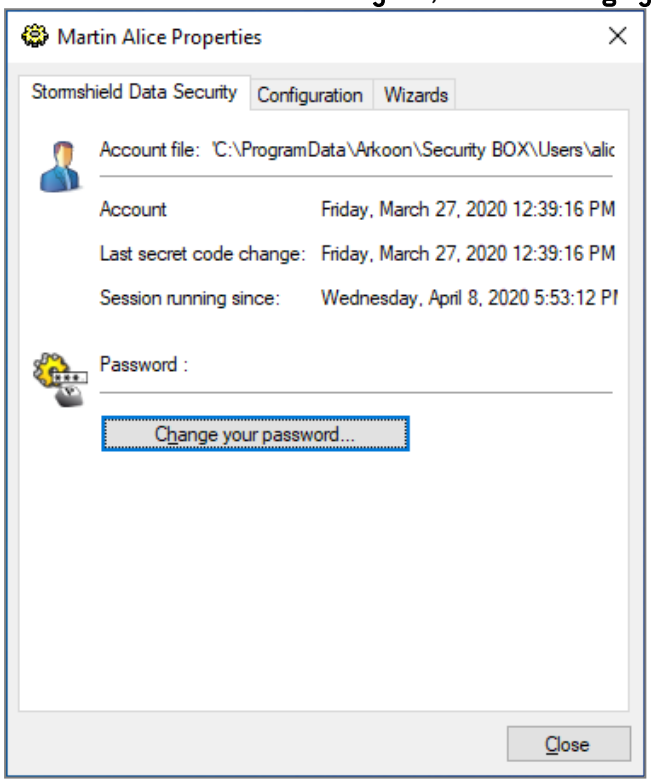
To disconnect:

1. Right-click on the SDS Enterprise icon  in the Windows system tray.
2. Click on **Disconnect**. The SDS Enterprise icon turns gray  .

5. Changing the password of the SDS Enterprise account

In password accounts, users can manually change their passwords.

1. Right-click on the SDS Enterprise icon in the Windows system tray.
2. Select **Properties**.
3. In the **Stormshield Data Security** tab, click on **Change your password**.



4. In the following window, enter your current password and twice your new password.

SDS Enterprise passwords are case sensitive. For example, the secret code Smith-1 is not the same as smith-1. SDS Enterprise analyzes the password and estimates the strength.

6. Securing files

Stormshield Data File makes it possible to guarantee the confidentiality of the data that your users process every day. It provides the following security features:

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

In addition to encryption, Stormshield Data File makes it possible to compress files before encrypting them.

Stormshield Data File offers several complementary file protection methods:

- Files can be encrypted by users themselves or for a recipient group by using public keys. Recipients can decrypt the files using their private keys.
- Files can also be encrypted in order to be self-decryptable using the SmartFILE format.

For more information on how to configure Stormshield Data File in SDMC, refer to the *SDS Enterprise Administration guide*.

6.1 Getting to know the Security BOX SmartFILE component

Stormshield Data File includes the Security BOX SmartFILE component, with which files can be encrypted in Security BOX SmartFILE format so that they can be shared with recipients who do not have the Security BOX SmartFILE application.

The operation can be accessed in the pop-up menu SDS Enterprise: **Stormshield Data Security** > **Security BOX SmartFILE**.

6.2 Encrypting and decrypting files

This chapter describes how to:

- Encrypt files for users themselves,
- Encrypt files for one or several recipients,
- Decrypt files,
- Generate Security BOX SmartFILE-encrypted files.

It also describes how to recover a password used for the encryption of Security BOX SmartFILE-encrypted files.

6.2.1 Encrypting one or several files

This section describes how to encrypt files which:

- The user will be the only one to use,
- The user will share with one or several correspondents.

Files encrypted using Stormshield Data File are identified as follows:

- by the icon superimposed on the original icon:

- by the *.sdsx* or *.sbox* file extensions.

The procedures described below apply to both files and folders. You can also select and encrypt files and folders simultaneously.

To encrypt one or several files:

1. Select the file(s), then right-click and select **Stormshield Data Security** > **Protect** or **Protect files**.
   The **Select recipients** window is displayed with your name only as by default you are the only person authorized to decrypt the files.
2. If you wish to share the protected file(s) with other users or user groups, enter their names in the search field. The search displays users and groups specified in the trusted address book as well as users from the LDAP directory if it is configured. It displays the users or group members whose certificate is valid or revoked (the revocation status is checked in the background).
   - Groups coming from the local directory have a green icon,
   - Groups from the LDAP directory have a yellow icon,
   - Pressing the Enter key in the search field directly launches a search in the LDAP directory.
3. Confirm your choice. If several files are selected, Stormshield Data File will request:
   - An initial and global confirmation; all the files will be processed and you will no longer be asked to confirm the encryption task.
   - Confirmation for each file. To temporarily disable the confirmation request 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 process the others.
   - Empty *.sbox* files cannot be encrypted. Any attempt to encrypt an empty file will generate an error message in the summary window.
4. The progress window for encryption operations appears. When this operation ends, a summary of the operations performed will be shown.
   Click on **Details**.
5. 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.

If you have encrypted for a group, the group is no longer displayed in the list of selected users when you edit the rule. It is replaced by the names of the relevant users.

6.2.2 Decrypting a file or a group of files

To decrypt a file, the user must be equipped with Stormshield Data File or Security BOX SmartFile. However, if SDS Enterprise can decrypt files in SDS Enterprise or Security BOX

SmartFile format, Security BOX SmartFile, Security BOX SmartFile can only decrypt files intended for it.

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

If users select a folder, Stormshield Data File will decrypt only the files that the user has previously encrypted or the encrypted files which had been sent to them.

To decrypt an entire folder:

- Select the folder, then select **Stormshield Data Security> Remove protection** from the pop-up menu.

To decrypt one or several encrypted files:

1. Select the files, right-click and select **Stormshield Data Security > Remove protection**. An encryption progress window will appear, and will show a summary of the operations conducted.
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.

NOTE
If the **Force conversion of .sbox files to .sdsx format** option in the security policy is enabled, the **Remove protection** menu is not visible for files with the *.sbox* extension. For more information on this option, see Configuring Stormshield Data File in the *Administration Guide*.

6.2.3 Opening one or several encrypted files

To open one or several encrypted files:

- Select the file(s) and press **Enter**.

- or -

- Select the file(s), then select **Stormshield Data Security > Open** from the pop-up menu:

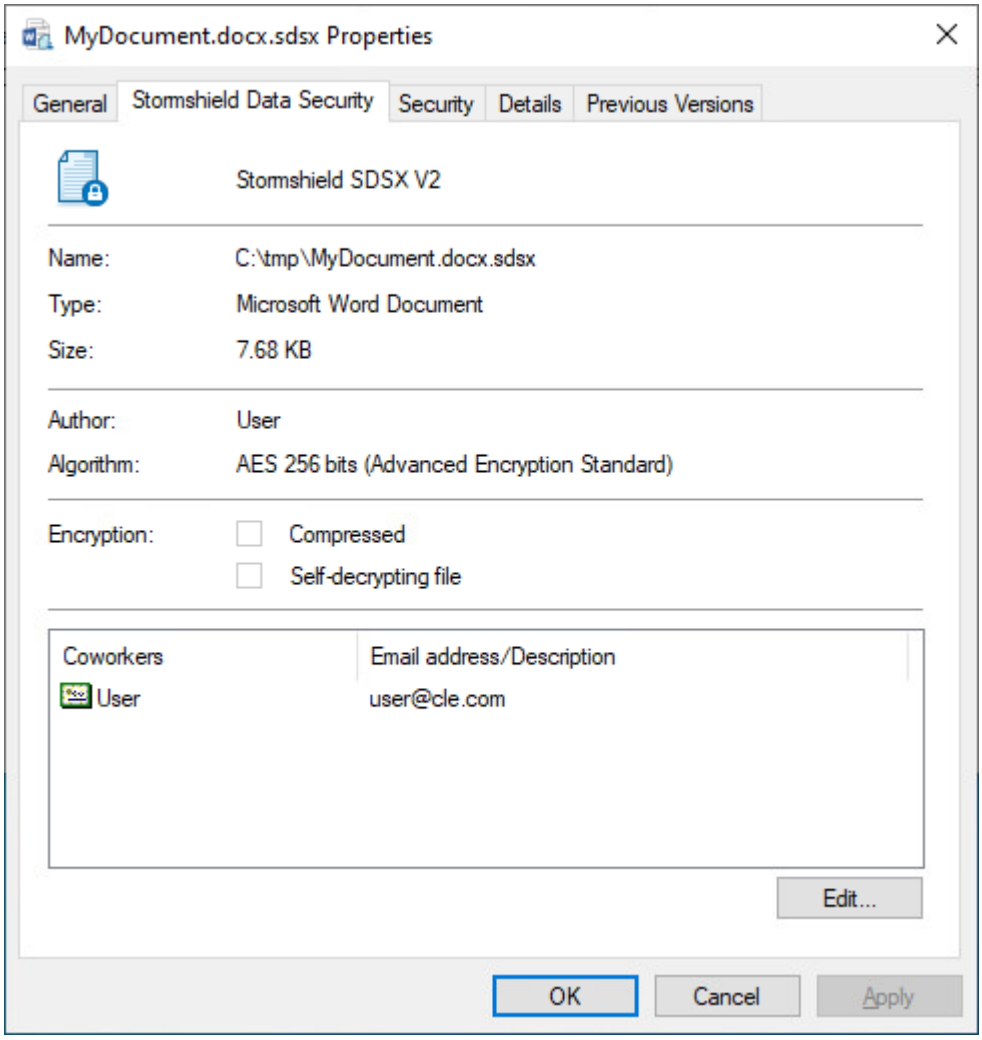
Depending on the format of the encrypted files (extension *.sdsx* or *.sbox*) the next step differs:

- For files with the extension *.sdsx*, the content of the encrypted files appears in the corresponding application. Files remain encrypted.
- For files with the extension *.sbox*, protection has been removed, and files will be opened in the corresponding application. They must be encrypted again after being closed.

NOTE
If the **Force conversion of .sbox files to .sdsx format** option in the security policy is enabled, files with the *.sbox* extension are automatically converted to *.sdsx* format when you open them. For further information, see Configuring Stormshield Data File in the *Administration Guide*. Furthermore, in this case it is not possible to open several files with both extensions simultaneously.

6.2.4 Displaying encrypted file properties

The properties of an encrypted file show the list of users who are 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.
- The name and e-mail address of the persons who can decrypt the file (only if the user is connected).

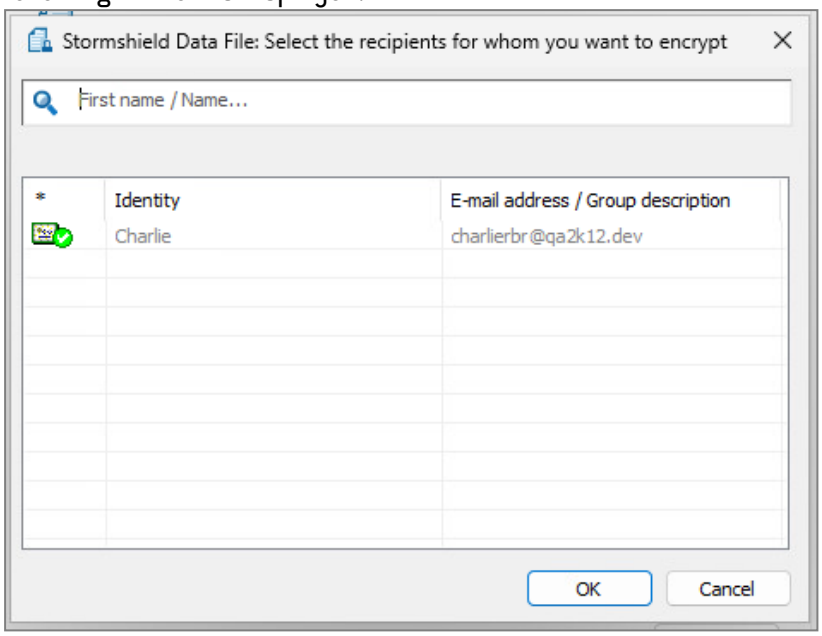
6.2.5 Managing coworkers on an encrypted file

You can manage the coworkers associated with an encrypted file. You can:

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

To add one or more coworkers:

1. Right-click on the encrypted file and select **Stormshield Data Security**> **Edit access**. The following window is displayed:



2. Find the coworker(s) or group(s) you want to add and click on **OK**. You can press the Enter key to start a search directly in the LDAP directory. If you are looking for a group:
   - Groups coming from the local directory have a green icon,
   - Groups coming from the LDAP directory have a yellow icon.
3. Click on **OK** to apply the changes.

To remove one or more coworkers:

1. Right-click on the encrypted file and select **Stormshield Data Security**> **Edit access**.
2. The correspondent selection window opens. Scroll over the line corresponding to a coworker and click on the red bin to delete this coworker.
3. Click on **OK** to apply the changes.

> **NOTE**
> These features are available only if you are connected or if you have rights on the file.

6.2.6 Managing coworkers on multiple encrypted files

You can add or remove coworkers associated with multiple encrypted files in a single action. The operation also works if not all files are protected for the same coworkers.

1. Select the encrypted files.
2. Right-click on the files and select **Stormshield Data Security**> **Edit access**.
3. In the window that appears, choose to add or remove coworkers and confirm.
4. The recipient selection window opens. Select the coworkers to add or remove and confirm.

> **NOTE**
> You must be logged in or have rights to the files for user management options to be available.

6.2.7 Generating a Security BOX SmartFILE file

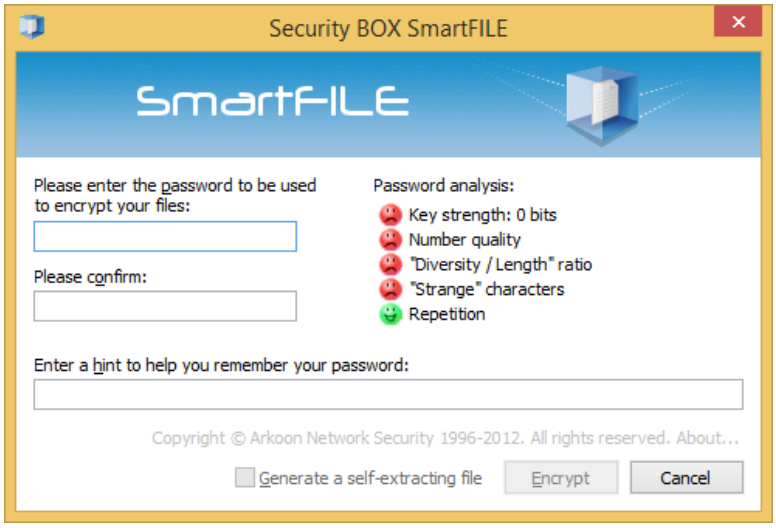
If the user wishes to share encrypted files with recipients who do not have Stormshield Data File, but use Security BOX SmartFILE instead, Stormshield Data File allows you to generate Security BOX SmartFILE-encrypted files.

The following rules apply:

- The user can encrypt several files simultaneously. A Security BOX SmartFILE file is created for each selected file.
- The names of the encrypted files must not contain Unicode characters.

To create a Security BOX SmartFILE-encrypted file:

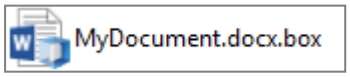
1. Select the file and right-click to select **Stormshield Data Security > Security BOX SmartFILE**.
2. Enter the password and a hint.



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. Return to the hidden double password entry in the same way.

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

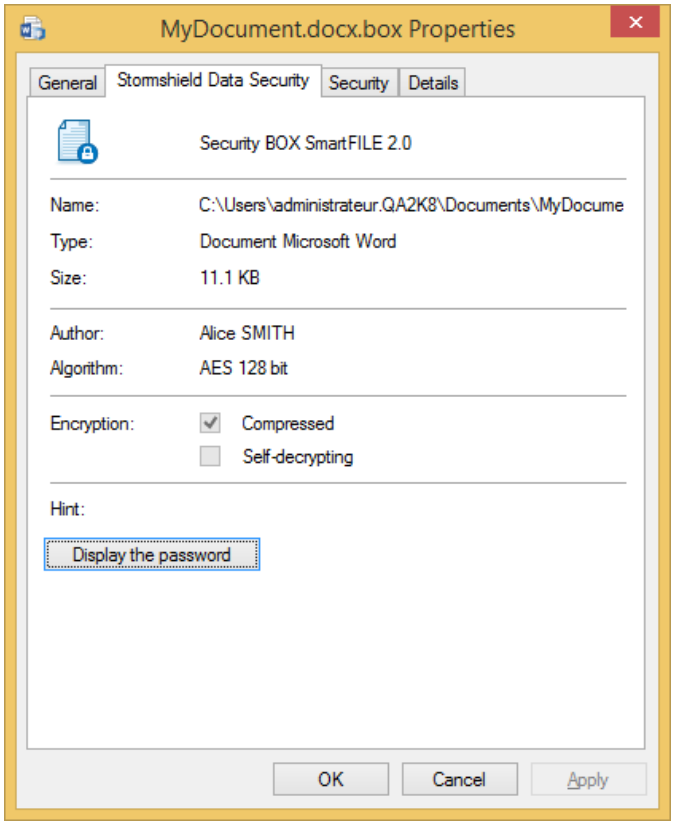
Security BOX SmartFILE-encrypted files are identified by a small icon and a specific extension:



6.2.8 Recovering passwords

If the user needs to recover the password used to generate a Security BOX SmartFILE-encrypted file, this password can be shown in the file properties (via the **Stormshield Data Security** tab). To run this function, you need:

- Stormshield Data File and Security BOX SmartFILE,
- To be logged in to SDS Enterprise using the user account that was used for the file encryption. You cannot recover the password with another SDS Enterprise account (including recovery accounts) or using Security BOX SmartFILE.



- Click on **Show password** to see the password.

6.2.9 Decrypting a Security BOX SmartFILE file with a recovery account

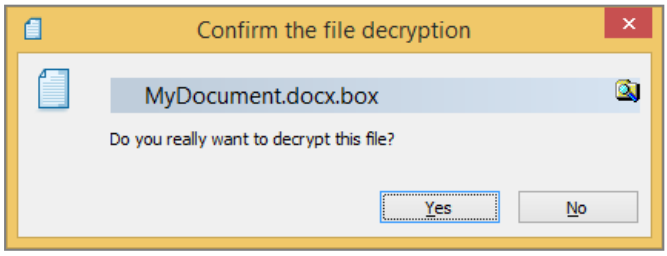
If the user needs to decrypt a Security BOX SmartFILE file with a recovery account:

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 down the CTRL+SHIFT keys simultaneously, then right-click and select SecurityBOX > Decrypt.

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



4. Confirm the decryption.

The file is decrypted without a password.

6.3 Cross-encrypting files

SDS Enterprise 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 "cross-encryption".

Encrypted files are cross-encrypted to their original formats: if they are in *.sdsx*, they will remain in *.sdsx* after cross-encryption.

Before you start, make sure you have the certificates for each new user to be added (*.cer* or *.crt* file). This certificate can be sent to you, obtained from your trusted address book or from an LDAP directory (refer to the SDS Enterprise *Administration guide*).

To launch the file cross-encryption wizard:

1. From the Windows **Start** menu, select **Programs** > **Stormshield Data Security**.
2. Select **Stormshield Data File – Cross-encrypt your files.** A welcome page appears.
3. Select the folder containing the files to cross-encrypt. To include files located in sub-folders, select the **Apply to sub-folders** checkbox. Click on **Next**. The displayed list is from the trusted address book and suggests only certificates valid for the operation (currently valid certificate with which encryption is allowed).
4. Select the certificates of users that you want to add to files in Stormshield Data File.
   If some users are missing from the list, click on to update the trusted address book by importing new user certificates directly from files or from an LDAP directory.
   Click on **Next**.
5. Click on **Yes, I remain a user of these files** to continue being able to access the files you are about to cross-encrypt.
   Otherwise, click on **No, I am no longer a user of these files**. The option you choose has no effect if you cross-encrypt 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 on **Next**.
6. Check the information displayed and click on Finish. The wizard looks for the files in the specified folder and cross-encrypts 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 result of the operation:

- : The folder has been successfully cross-encrypted.
- : The folder has been successfully processed, but it contains files that could not be cross-encrypted 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 cross-encrypted.

-  : The file was not cross-encrypted 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.

7. Automatically protecting folders

Stormshield Data Share makes it possible to automatically protect the content of confidential folders, and share access to them with other coworkers when necessary. When this feature is enabled, each new document or sub-folder placed in a protected folder is encrypted and accessible only by authorized users. You can protect the content of the following folder types:

- Standard Windows folders on your workstation,
- Folders from synchronized shared spaces.

To automatically secure folders on a network share, file server or external drive (e.g., USB drive), use the Stormshield Data Team feature.

7.1 Automatically protecting local folder content

Automatic protection can be enabled on folders on your workstation so that all sub-folders and files that you place there will be systematically protected.

This feature depends on the File feature and cannot run without it.

7.1.1 Automatically protecting access to files

1. In Windows Explorer, right-click on the local folder that you wish to protect and select **Stormshield Data Security > Automatically protect folder.**
   The **Select recipients** window opens with only your name because by default you are the only person allowed to decrypt the folder's content.
2. If you wish to share the contents of the protected folder with other users or groups, enter their name in the search field. The search can display users present in the trusted directory, or in the LDAP directory if configured.
3. Click on **OK**.
4. If you wish, apply the new rule immediately to the entire contents of the folder.
   A protection rule is created containing the path to the folder along with the user or list of users authorized to decrypt its contents.
   All new files and folders that are moved to this folder will now be automatically encrypted. A blue padlock appears on their icons.
5. If you wish to apply the rule later to all folder contents already present before automatic protection was enabled, right-click on the protected folder and select **Stormshield Data Security** > **Advanced** > **Apply changes to the entire folder**.

If some of the files in the folder have already been protected, the following behaviors apply:

- Users who were allowed to access these files will be replaced with those specified by the more recent protection rule.
- Files that are already encrypted, and which you are not allowed to access, will not be processed.
- Files encrypted in *.sbox* format will not be processed.

If you move the folder and its content, the protection rule will be updated. All the content remains protected and automatic protection will remain enabled on the folder.

7.1.2 Editing the list of coworkers allowed to access the content of the folder

1. In Windows Explorer, right-click on the folder for which you wish to manage the list of authorized coworkers.
2. Select **Stormshield Data Security** > **Edit access**.
3. In the **Select recipients** window, add or remove users or groups authorized to decrypt the folder's contents. Enter their name in the search field.
4. Click on **OK**.
5. Apply the change to the entire folder if you wish.
   The folder and its contents are now accessible to all users you have authorized.
6. If you later wish to apply this change to all folders and files already present beforehand, right-click on the protected folder and select **Stormshield Data Security** > **Advanced** > **Apply changes to the entire folder**.

7.1.3 Disabling automatic folder protection

1. From Windows explorer, right-click on the folder on which you wish to disable automatic protection. This folder must not be located in a synchronized space that was automatically protected by the administrator, and you must be authorized to access it.
2. Select **Stormshield Data Security** > **Advanced** > **Disable protection on the folder**.

When you disable folder protection, the documents it contains remain encrypted. However, all new files that you add to it will no longer be automatically encrypted.

7.2 Automatically protecting folders in synchronized shared spaces

To automatically protect the contents of collaborative workspace folders synchronized with online hosts OneDrive, OneDrive for Business, DropBox, SharePoint and Oodrive, two methods are available:

- the administrator sets up automatic protection of a collaborative workspace via the security policy. All content deposited by a user in a collaborative workspace folder is encrypted, and only that user can open their files. Each user can then, from their SDS Enterprise account, give other users access to their documents.
- the user themself can enable automatic protection of a collaborative workspace folder. All the content they place in the folder is then encrypted for themself. They can choose to provide other users with access to their documents.

This Stormshield Data Share feature is dependent on the File feature and cannot function without it.

7.2.1 Protecting a collaborative workspace with a security policy

The administrator must have previously enabled automatic folder protection for one or more types of collaborative workspace synchronized in SDMC. For more information, refer to the section *Configuring Stormshield Data Share* in the *Administration guideSDS Enterprise*.

To automatically protect a new file placed in a synchronized folder:

1. Log in to SDS Enterprise.
2. Move your file to the synchronized folder of your choice (e.g., OneDrive, Dropbox).
   It is automatically protected: it now has a *.sdsx* extension and its icon displays a small padlock. You will be the only person who can view them.

You can then authorize other users to access your protected files in the collaborative workspace.

If you only need a file once, you can share it directly. To do so:

1. Right-click on the file,
2. Select **Stormshield Data Security** > **Edit access**.
3. In the **Select recipients** window, add coworkers or groups as described in Managing coworkers on an encrypted file.

If you need to share files on a recurring basis with the same coworkers, we recommend that you create a sub-folder within the collaborative workspace folder and add a specific protection rule to this folder. To do so:

1. Right-click on the sub-folder and select **Stormshield Data Security** > **Automatically protect folder**.
2. In the **Select recipients** window, enter the names of the coworkers or groups in the search field. The search can display coworkers present in the trusted directory, or in the LDAP directory if configured.
3. Click on **OK**.
4. If you wish, apply the new rule immediately to the entire contents of the folder.
   A protection rule is created containing the path to the folder along with the user or list of users authorized to decrypt its contents.
   All new files and folders that are moved to this folder will now be automatically encrypted. A blue padlock appears on their icons.
5. If you wish to apply the rule later to all folder contents already present before automatic protection was enabled, right-click on the protected folder and select **Stormshield Data Security** > **Advanced** > **Apply changes to the entire folder**.

To edit a protection rule, for example to add coworkers for example, select the **Stormshield Data Security** > **Edit access** menu.

If you subsequently move a protected file out of the synchronized space, it will remain protected. In this case, however, you can remove the protection. For more information, refer to the section Decrypting a file or a group of files.

7.2.2 Protecting a collaborative workspace with a user-defined rule

If a collaborative workspace folder is not already protected by the security policy, you can create an automatic protection rule yourself to protect the files you place in the folder:

1. In Windows Explorer, right-click on the collaborative workspace folder you wish to protect and select **Stormshield Data Security** > **Automatically protect folder**.
   The **Select recipients** window opens with only your name because by default you are the only person allowed to decrypt the folder's content.
2. If you wish to share the contents of the protected folder with other users, enter their name or the name of a group in the search field. The search can display users present in the trusted directory, or in the LDAP directory if configured.
3. Click on **OK**.
4. If you wish, apply the new rule immediately to the entire contents of the folder.
   A protection rule is created containing the path to the folder along with the user or list of users authorized to decrypt its contents.
   All new files and folders that are moved to this folder will now be automatically encrypted. A blue padlock appears on their icons.

5. If you wish to apply the rule later to all folder contents already present before automatic protection was enabled, right-click on the protected folder and select **Stormshield Data Security** > **Advanced** > **Apply changes to the entire folder**.

If some of the files in the folder have already been protected, the following behaviors apply:

- Users who were allowed to access these files will be replaced with those specified by the more recent protection rule.
- Files that are already encrypted, and which you are not allowed to access, will not be processed.
- Files encrypted in *.sbox* format will not be processed.

To edit a protection rule, select the **Stormshield Data Security** > **Edit access** menu.

If you move the folder and its content, the protection rule will be updated. All the content remains protected and automatic protection will remain enabled on the folder.

If you wish to disable automatic folder protection, see Disabling automatic folder protection.

7.2.3 Sharing an automatic protection rule

When you create a rule to protect a collaborative workspace folder, you can not only authorize other users to access the encrypted content, but also share the rule with them. Sharing the rule avoids the need for everyone to create the rule on their own workstation, and enables the same protection rule to be applied to all recipients of the rule.

From the moment the rule is created and shared, all new files placed in the folder by any user listed in the rule are encrypted for all recipients of the rule. If files were already present in the folder before the protection rule was created, it is up to each user with files encrypted for them to apply the changes to their folder, as described below, if they wish to give access to their files.

It is not possible to transform a shared automatic protection rule into a non-shared rule, and vice versa. The choice must be made when the rule is created and this choice is final.

Requirements

For a shared rule to be automatically applied to selected users, each user must already have an automatic protection rule on their collaborative workspace folder:

- If automatic protection is enabled via the security policy, users do not have to do anything.
- If this is not the case, each user must first create an automatic protection rule on the folder so that SDS Enterprise can apply the shared rule.

Sharing the protection rule

1. Right-click on the folder in question and select **Stormshield Data Security**.
2. Select **Automatically protect folder**.
3. In the **Select recipients** window, select the desired coworkers or groups.
4. Check the **Share protection rule** box. A hidden system file *.SDSRULE* containing the rule details will be created in the folder. When the rule's recipients go to the relevant folder on their workstations, the rule will automatically apply to them. New files placed in the folder will be encrypted for them and for all recipients of the rule.
5. Immediately apply the new rule to the entire contents of the folder, if you want all files already in the folder, whether or not they are encrypted for you, to be encrypted for all recipients of the rule.

6. If you wish to subsequently apply the rule to the entire contents of the folder already present before the rule was created, or if a rule recipient wishes to encrypt their files already present for all other recipients, right-click on the protected folder and select **Stormshield Data Security** > **Advanced** > **Apply changes to the entire folder**.

For sharing to work, users must be logged into their SDS Enterprise account.

Editing a shared protection rule

You can edit a shared protection rule to add or remove recipients from the rule. All users sharing a rule can edit it.

To edit a shared rule applied to a collaborative workspace folder:

1. Right-click on the folder in Windows Explorer.
2. Select **Stormshield Data Security** > **Edit access**.
3. Add or remove a coworker from the rule, then confirm.
   The rule is changed for all recipients. For a user removed from the rule, any files they place in the folder in question are now unprotected.

Deleting a shared protection rule

To delete a shared protection rule on a collaborative workspace folder:

1. Right-click on the folder in Windows Explorer.
2. Select **Stormshield Data Security** > **Advanced** > **Disable protection on the folder**.

The rule is then deleted for all recipients of the rule.

Any recipient of a shared rule can delete the rule.

8. Securing folder content

INFORMATION
As of January 2025, Stormshield will no longer offer functional upgrades to the Stormshield Data Team feature. The feature will switch to maintenance mode from this date.

Stormshield Data Team guarantees the automatic encryption of confidential files: the files are encrypted wherever they are, in real time and transparently.

Protection is provided according to security rules defined by folder: any file created or placed in a "secured folder" is automatically encrypted without any user interaction. The location, name and extension of the file remain unchanged.

Stormshield Data Team also makes it possible to share confidential data between several coworkers. The "safety rule" specified on the folder defines the coworkers authorized to read and modify the files stored in the folder. The non-revocation of a user is verified according to the defined security policy.

Stormshield Data Team can secure:

- Removable media (USB stick) entirely or partially (one or more sub-folders),
- A shared folder on a file server.

To automatically protect a local folder on the user's workstation or in a synchronized shared space, use Stormshield Data Share.

When a security rule is set on a folder, it is applied recursively to all its sub-folders. It is nevertheless possible to define a different rule on a well determined sub-folder. If no rule is applied to a file or folder with Stormshield Data Team, the file or folder is created and opened in clear text.

Once encrypted, a file can be read, modified or deleted only by a coworker authorized by the security rule. All reading / writing and encryption / decryption for data are operated “on the fly” and in memory: no clear copy of the file is created.

The pop-up menus shown in Stormshield Data Team when the user right-clicks on a folder depend on the parameters selected in the SDMC administration console. For more information, refer to the section *Configuring Stormshield Data Share* in the *Administration guide.*

8.1 Securing a folder

Every time you secure a folder, you implicitly or explicitly define a security rule. It is saved as part of the folder’s properties. When the folder is shared with coworkers, this makes it easier to manage lists of authorized users.

NOTE
Security rules are saved in an *sboxteam.sbt* hidden file. This file is visible on machines where Stormshield is not installed. This file must neither be modified nor deleted.

8.1.1 Understanding Stormshield Data Team icons

The icon  identifies secured folders and files in Windows Explorer.

 Confidential	The icon indicates that a Stormshield Data Team rule has been applied to the folder. If the user is among the authorized users, files created in, moved or copied to this folder are automatically encrypted. If you are not authorized, you will be able to view the contents of this folder, but not open encrypted files. You will not be able to create files in this folder either. If Stormshield Data Team is not installed, you can access secured files and folders normally, but existing file content remains encrypted. In this case, we advise against modifying these files, as they can be irretrievably corrupted.
 MyDocument Microsoft Word Document 11.8 KB	These icons 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.
 MyDocument.docx	
 MyDocument	

8.1.2 Securing folders without setting shared access

To quickly secure a folder without sharing it with other users, i.e., without setting a security rule:

1. Select the folder to encrypt and right-click to select **Stormshield Data Security** > **Secure the folder**.
2. Confirm your choice.
   The folder is then secured by a rule that contains only the current connected user. The files are updated and encrypted.

8.1.3 Securing folders by setting shared access

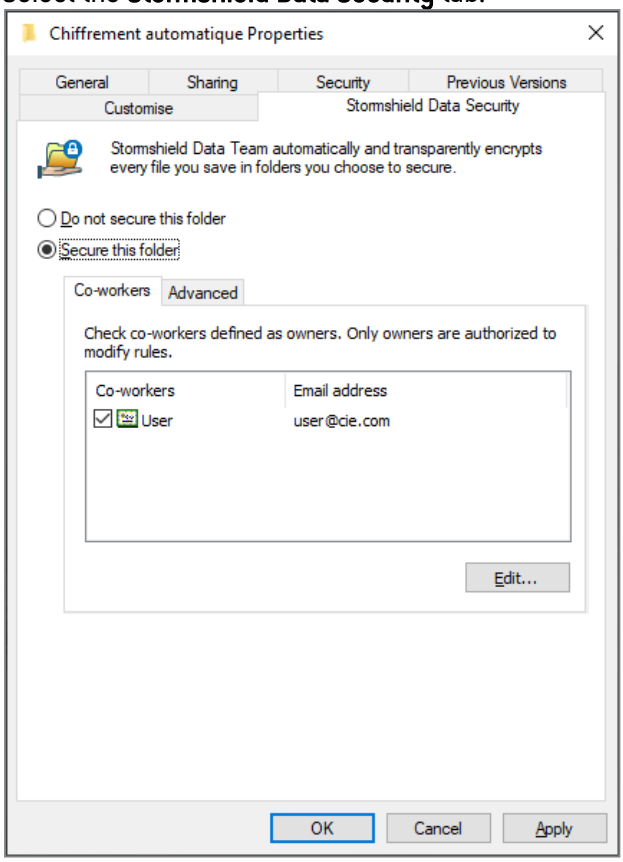
To secure folders by grating other users access to this folder, i.e., by setting a security rule, follow the procedure below.

Securing a folder

To secure a folder and define a security rule:

1. Select the folder to be secured.
2. Right-click on the folder, and select **Properties**.

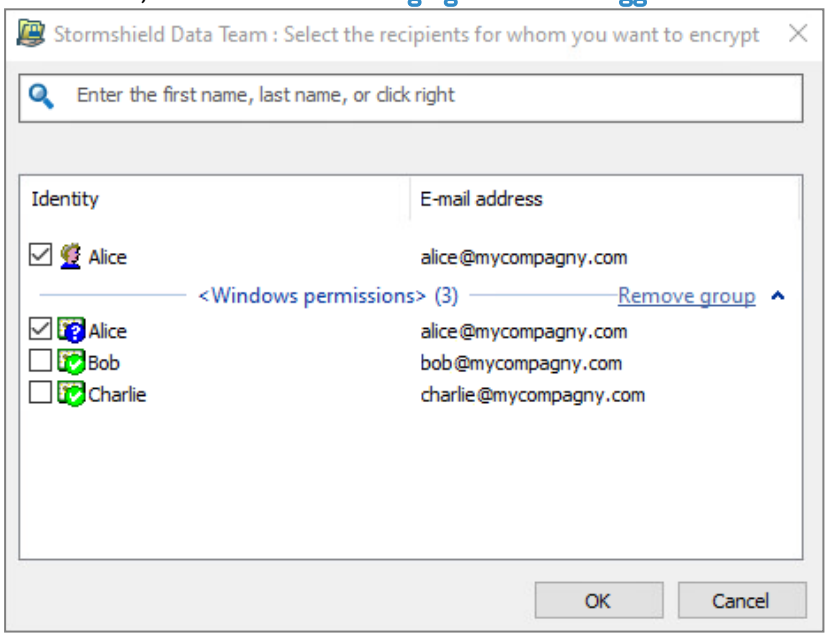
3. Select the **Stormshield Data Security** tab.



4. Select the option **Secure this folder** to encrypt it. All sub-folders and files in the folder will also be encrypted automatically.

5. If you need to share the folder with other users, click **Edit** and search for users or groups. The search displays users and groups specified in the trusted address book as well as users from the LDAP directory if it is configured. It shows coworkers or group members whose certificate is valid or revoked (the revocation status is checked in the background).
   - Groups coming from the local directory have a green icon,
   - Groups from the LDAP directory have a yellow icon,
   - Pressing the Enter key in the search field directly launches a search in the LDAP directory.

   Coworkers holding the Windows permissions on the folder concerned can be automatically suggested in the **Windows permissions** group if the option is enabled (blue icon). You can click on the group name to remove some coworkers from the group if necessary. If the option is not enabled, you can add the group from the list of suggestions. For more information, see the section Managing automatic suggestion of coworkers.



6. Click **OK** to close the coworker search window.
7. In the coworkers list, select the owners of the rule. Only owners are authorized to modify rules. There must always be at least one owner. By default, the user creating the rule is the owner and may be set as a simple authorized coworker later.
8. Click **OK** to save and apply the rule.

You can now create new files or move existing files into this secured folder, where they are automatically encrypted according to the rules on the folder.

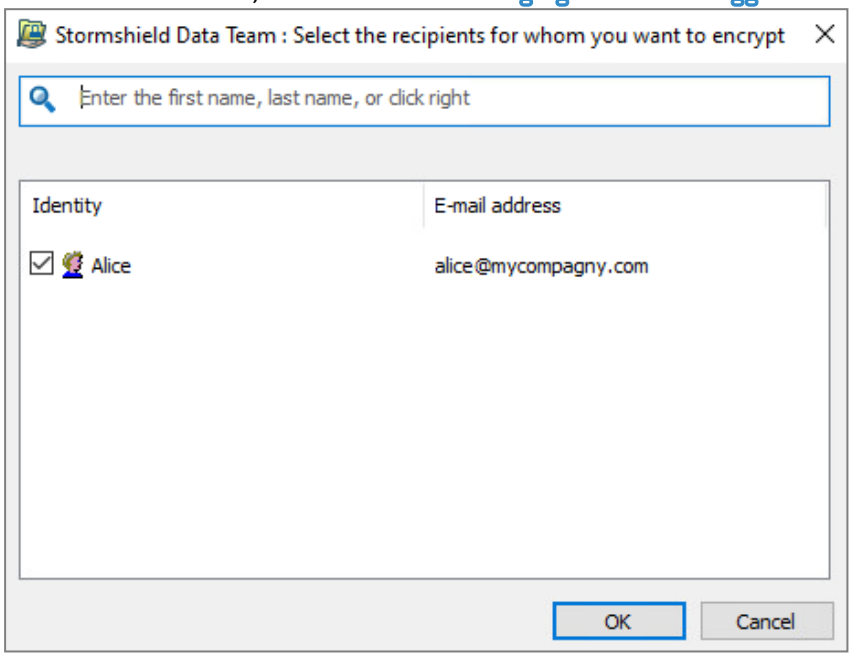
If you have encrypted for a group, the group is no longer displayed in the list of selected coworkers. It is replaced by the names of the coworkers concerned.

Adding or removing coworkers from the security rule

To add or remove coworkers from a security rule applying to a folder already secured:

1. Right-click on the folder in question.
2. Select **Properties**.
3. Select the **Stormshield Data Security** tab.
4. From the **Coworkers** tab, click on **Edit**.

5. Search for coworkers or groups to add or remove coworkers from the list by scrolling your mouse over the line of the coworker and clicking on the red bin.
   By right-clicking in the search field, the coworkers who hold the Windows permissions on the folder in question can be selected. You can click on the group name to remove some coworkers from the group if necessary. You will see this link only if the option is enabled. For more information, see the section Managing automatic suggestion of coworkers.



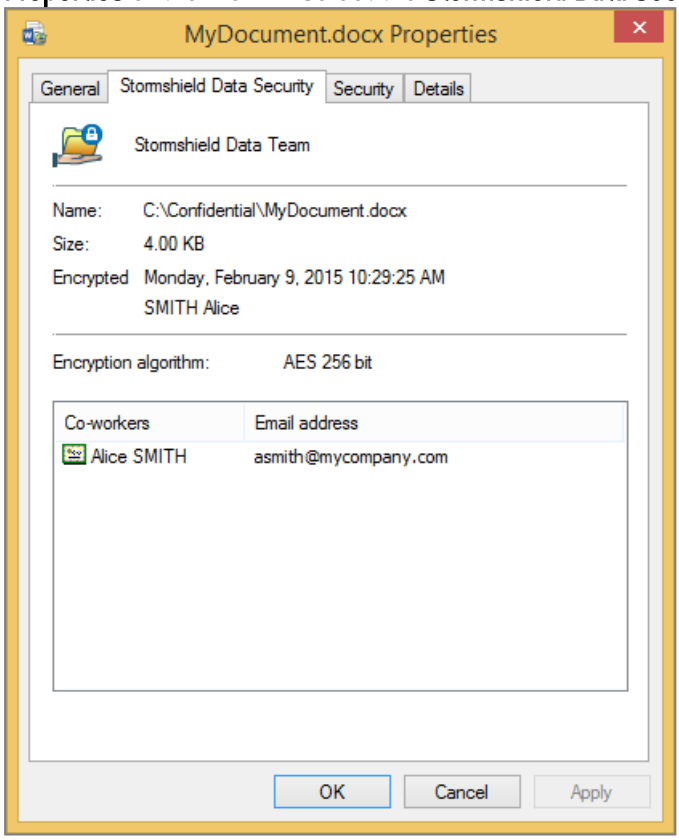
6. Click **OK** to close the coworker search window.
7. Click **OK** to save and apply the rule.

8.1.4 Managing secure folders

You can perform the following operations on secure folders.

Displaying encrypted file properties

- To display properties on a file encrypted with security rules, in Windows Explorer right-click on the file, select **Stormshield Data Security** and then select **Properties** or open the **Properties** of the file and select the **Stormshield Data Security** tab.



In the **Stormshield Data Security** tab, the file size information includes encrypted data and SDS Enterprise security data (the equivalent size information in the **General** tab does not include technical data).

The list of authorized users is displayed only if:

- You are connected to SDS Enterprise.
- You are part of the authorized users' list.

Copying or moving files and folders secured with a Team rule to a non-secure folder

You can choose the default behavior when encrypted files or folders are copied or moved to a non-secure folder, by going to the advanced settings of the Teams feature in SDMC. You can prohibit files and folders from being moved or copied, or you can allow them by choosing to decrypt or keep encryption.

To configure these options, refer to the *SDS Enterprise Administration guide*, under *Configuring Stormshield Data Team.*

Regardless of the behavior chosen, the **Save** pop-up menu makes it possible to create a copy of a file or folder while preserving encryption. For more information, refer to the section Saving an encrypted file.

It is also possible to encrypt the file using Stormshield Data File directly in the folder secured by Stormshield, before copying or moving it.

Securing files available offline

If you secure a folder that can be accessed offline, the files are encrypted at the shared folder level on the network but on your workstation as well, in the local folder in which they are copied.

Viewing known rules

At any time, you can view all Stormshield Data Team rules known to the user.

In the systray, right-click on the Stormshield Data Security icon.

1. Select *Properties*
2. In the **Configuration** tab, double-click on the Stormshield Data Team icon.
3. Select the Security Rules tab:
4. The known rules list appears in the upper part of the window. Select a rule to view the list of coworkers and owners of the rule.

NOTE
Processing time is directly dependent on the number of coworkers in the rule, and system performance.

8.2 Updating folder security

A folder's security, i.e., the security rule that applies to it, can be updated at any time.

To apply a new rule or edit a rule on a folder:

1. Close all the files in this folder.
2. Right-click on the folder or the files to update, and select **Stormshield Data Security** > **Secure according to defined rules**.

NOTE
The file update will be suspended if you lock or close your SDS Enterprise session or Windows session. This update automatically resumes when you reconnect to SDS Enterprise. This recovery is indicated by a tooltip.

A status window displays the list of files, and their current status. The final status shows one of the following results:

Status	Description
You are not an authorized coworker	You are not allowed to access the file.
Access denied.	The file is protected by Windows security permissions, or the file is currently open in another program.
Process cancelled	You have stopped the current operation.

8.3 Saving an encrypted file

To copy an encrypted file or secure folder and keep the encryption, proceed as follows:

1. In Windows Explorer, right-click on the file or folder to be archived and select **Stormshield Data Security > Advanced > Save**.
   Several files or folders can be selected at once.
2. Select the destination folder.
3. Click on **OK**. The selected file will be copied, with encryption, into the destination folder. The folder hierarchy is kept.

You do not need to be logged in to SDS Enterprise to save a file.

NOTE
By default, SDS Enterprise is configured to allow opening encrypted files stored in a non-secure folder.

WARNING
Never use the Windows save function or drag and drop files to a non-secure medium, as confidential files will be copied in plaintext.

8.4 Restoring an encrypted file

To restore a saved encrypted file, you must restore it to a secured folder:

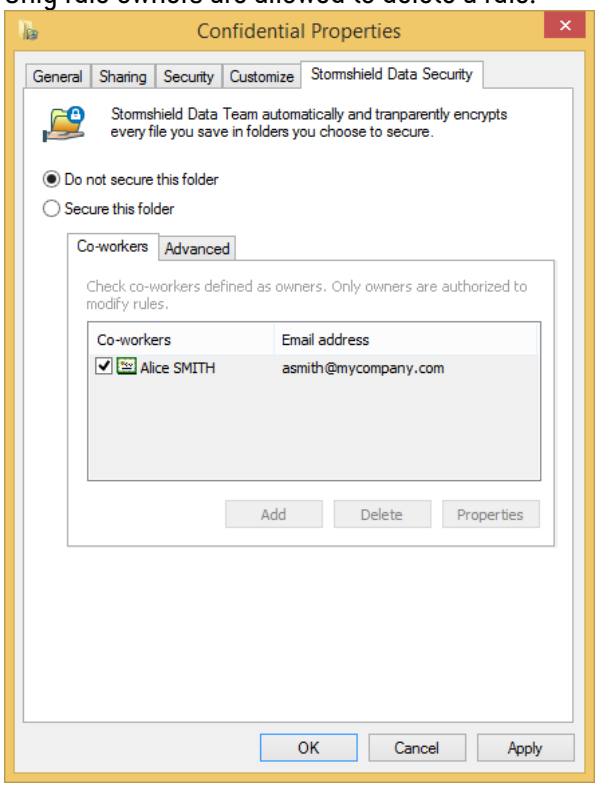
1. Right-click on the folder or the files to be restored, and select **Stormshield Data Security > Advanced > Restore**.
2. Select the destination folder; it must be a secured folder.
3. The selected encrypted file(s) are copied into the secured folder, and remain encrypted. Click on **OK**.

8.5 Removing security on a folder

To remove security on a folder and decrypt the files that it contains:

1. Right-click on the secure folder, then select the **Stormshield Data Security** menus and **Properties**.
   The properties page indicates the secure state of the folder, the coworkers allowed to access the folder and the users allowed to modify the security options (rule owners).

2. Click on **Do not secure this folder** and then **OK**.
   Only rule owners are allowed to delete a rule.



3. The following window will ask you to confirm the operation. Select **Yes** to proceed.
4. A progress bar shows the decryption of the files being processed.
   If some files have not been decrypted (for example, because access was denied), they are listed in the **Details** section.
5. Click on **Close**. The security rule has been deleted and the files contained in the folder are now in plaintext.

8.6 Decrypting files

Files contained in a secure folder cannot be decrypted. However, in the following cases, encrypted files can be in a non-secure folder and may need to be decrypted:

- After a folder has been decrypted (such as described in the previous section) but files inside have not been decrypted. This is the case when the administrator answered No to the question Are you sure you want to remove security of this folder, and save all your files unencrypted?.
- After a file has been saved with the Stormshield Data Security menu.

To decrypt a file or a group of files:

1. Select them in the explorer.
2. Right-click and select: **Stormshield Data Security**, then **Advanced** and then **Remove security**.

A status window will then display the list of decrypted files.

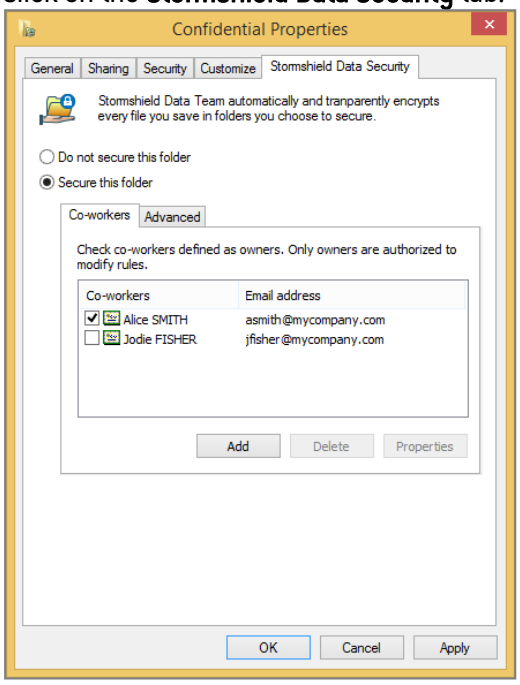
At the end of the operation, the folder will be accessible without restrictions, and all the files it contains will be saved in plaintext.

8.7 Defining a different rule on a sub-folder

When a folder is protected, all its sub-folders are also secured by default, using the same rule. However, you can set specific rules for a sub-folder that will override the safety rules of the parent folder.

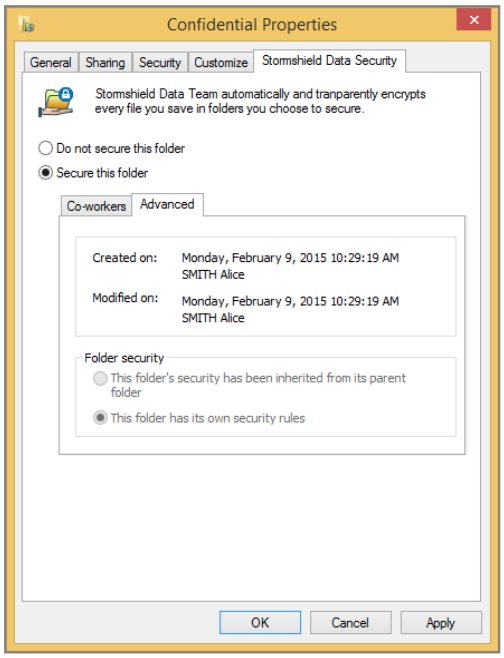
The procedure is as follows:

1. In Windows explorer, right click on the folder and select **Properties**.
2. Click on the **Stormshield Data Security** tab.



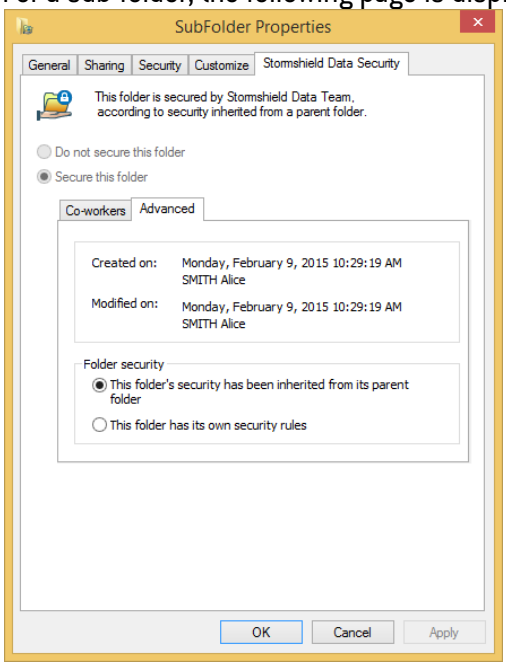
The list of authorized coworkers appears. The name of owners is selected.

3. If you select the Advanced tab, you will see information about the coworker who created the rule on the folder.
   - For a root folder on which a security rule is explicitly defined, the following page is displayed:



> **NOTE**
> If you are identifed as the owner, you can unsecure the folder from the properties window, by selecting **Do not secure this folder**. For more information, please refer to the section Removing security on a folder.

- For a sub-folder, the following page is displayed:



By using the radio buttons in the **Folder security** section, you can indicate whether the sub-folder inherits rules from its parent folder, or whether it has its own rules.

- When encryption rules are defined on a folder, new files created in the encrypted folder are automatically secured.
- When a secure folder is moved, the security rule is kept as long as it is associated with the folder itself. If this rule was associated with its parent, the folder will lose its secure status after it is moved. However, the files that it contains remain encrypted.
- If you move a non-secure folder into a secured folder, the files in the original folder will not be encrypted automatically.
- There cannot be non-secure folders in a secure folder.
- You cannot encrypt the contents of the following folders and their sub-folders:
  - Windows folder (typically **c:\windows**),
  - System folder (typically **c:\windows\system32**),
  - Program folder (typically **c:\program files**).
- If you copy or move an encrypted file into a non-secure folder, the file is copied in plaintext. To make a secure copy of the file, see Saving an encrypted file.
- Files may have different rules from those in the folder that contains them. For example, Franck, Diane and Alice are able to access folder X, but only Franck and Diane can access a file contained in this folder. This happens when a modification to a rule is not applied.
- If files are already stored in a folder before a rule is set (or if you edit a rule that has already been set), you must update the security of files already saved in this folder, as explained in Securing folders without setting shared access.

8.8 Deleting encrypted files

Only authorized users can delete encrypted files with Windows Explorer. Encrypted files that you delete with Windows Explorer Delete command, or with the keyboard Delete key, will be put in the recycle bin, but will still be encrypted.

If a user who is not an authorized coworker wants to fully delete encrypted files, they must use the dedicated SDS Enterprise delete function.

1. In Windows Explorer, right-click on the files or folders you want to delete.
2. Select **Stormshield Data Security** > **Advanced** > **Delete**.

A status window will then display the list of deleted files.

Files deleted in this way will not be placed in the bin; they are permanently deleted.

8.9 Repairing a rule

Security rules are stored in a private file hidden in a folder. When a user accesses a folder secured by a rule, SDS Enterprise stores the content of this technical file in its account so that it can detect the following attacks:

- Deletion of the technical file,
- Modification of the rule by an unauthorized third party (e.g., adding or deleting a coworker),
- Replacement of the technical file with a file from another valid rule, but intended for a different folder.

Some of these events can also be the consequence, not of an attack, but of an exceptional use case such as the:

- Deletion of the folder,
- Creation of a new folder with the same name,
- Definition of a new rule.

If an attack is suspected, SDS Enterprise will prohibit any access to the folder in question. To restore access:

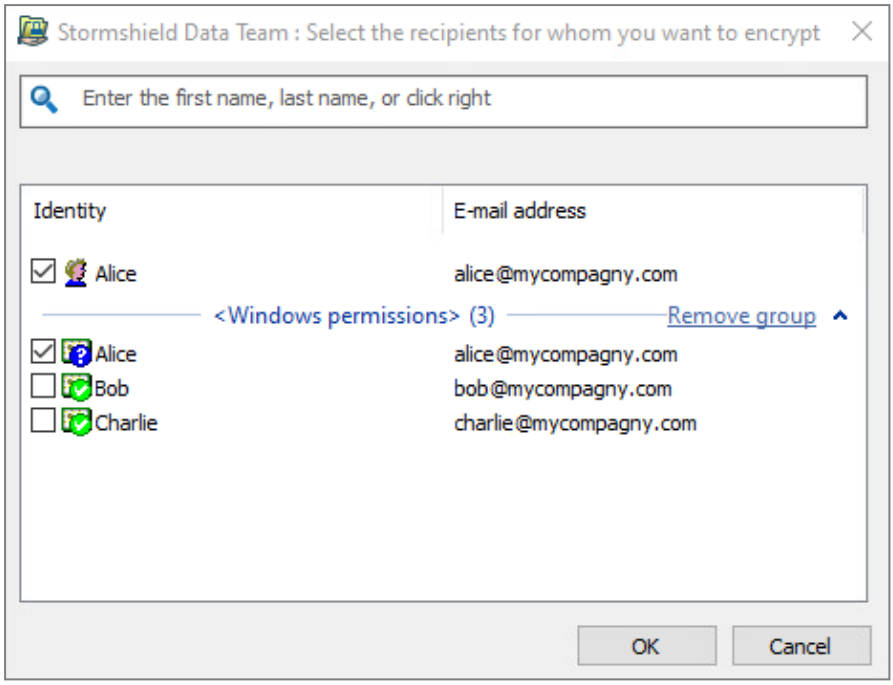
1. In Windows Explorer, right-click on the file and select **Properties**.
2. Click on the **Stormshield Data Security** tab.
3. Click on **Restore** to copy the rule stored in the account into the folder.
4. Or click on **Refresh** to accept the rule set on the folder and copy it into the account.

8.10 Updating rules automatically

When a coworker's encryption key changes, all the Team rules that include their encryption certificate must be updated. All the rules known to a user can be updated automatically. For more information, refer to *Configuring Stormshield Data Team* in the *Administration guide*. These rules can only be updated if the user is a rule owner.

8.11 Managing automatic suggestion of coworkers

When selecting the coworkers you want to share the folder with, coworkers who hold the Windows permissions that enable accessing the folder concerned are automatically suggested in a group which name is **Windows permissions**, together with a blue icon in the search field.



Automatic suggestion will work if the two following conditions are met:

- The LDAP directory must be properly configured. For more information, refer to the *SDS Enterprise Administration guide*.
- Users suggested via Windows permissions must have a valid certificate in the Active Directory.

You can disable this feature by creating a registry key. For more information, refer to the *Deactivating automatic coworker suggestion* in the SDS Enterprise *Advanced configuration guide*.

8.12 Known limitations

The following table lists the known limitations on Stormshield Data Team:

Feature	Description
NFS	NFS-type partitions are not supported.
CSC + DFS	A folder available off line cannot be encrypted.
Samba + DFS	A Samba file share defined as a DFS root cannot be secured.
Versions \ Shadow Copy management	This volume backup system, which is used for version management in Windows Explorer, is not supported by Stormshield Data Team.
Sharing a local secured directory	Stormshield Data Team does not allow encrypted folders to be shared locally.
Connection to the remote desktop	In remote desktop connection, displaying the Team properties of a secure file in a secure folder on a USB drive via the contextual menu (**Stormshield Data Security > Properties**) generates an error.

Feature	Description
Synchronized shared spaces	Stormshield Data Team cannot secure synchronized shared spaces such as SharePoint, Dropbox, Office 365, etc. We recommend that you exclude these directories from the folders analyzed by Stormshield Data Team. Directories can be excluded by using the `excludedFolders` parameter in the security policy's *.json* file. For more information, see section *Stormshield Data Team* in the Advanced configuration guide. To secure synchronized shared spaces, refer to Automatically protecting folders.

9. Creating secure virtual volumes

Stormshield Data Virtual Disk makes it possible to guarantee the confidentiality of the data that users store on their hard disks, by creating encrypted virtual volumes: only the owner and authorized users can access secure volumes.

Stormshield Data Virtual Disk uses a small amount of resources (memory and CPU) and files are encrypted in real time when they are written and decrypted when they are read. Applications can directly access the protected information of files located on a virtual volume.

With Stormshield Data Virtual Disk, you can:

- Create a secure virtual volume on which the user can save confidential data. See section Creating a secure volume.
- Mount a secure volume on the workstation, i.e., connect a virtual volume on which the user can save confidential data. See section Mounting a secure volume.
- Unmount a secure volume on the workstation, i.e., disconnect the virtual volume. See section Unmounting a secure volume.

When users create a secure virtual volume, they define a list of authorized users. These authorized users are users who can mount and unmount the secure volume and access the content of the volume. See the section Editing the list of users.

The container file (*.vbox* extension) represents the volume encrypted from Windows Explorer. The encrypted volume corresponds to the content of the container file.

For more information on how to configure Stormshield Data Virtual Disk in SDMC, refer to the *SDS Enterprise Administration guide*.

9.1 Creating a secure volume

The Stormshield Data Virtual Disk feature makes it possible to create secure virtual volumes. All of the files on these volumes will be stored securely.

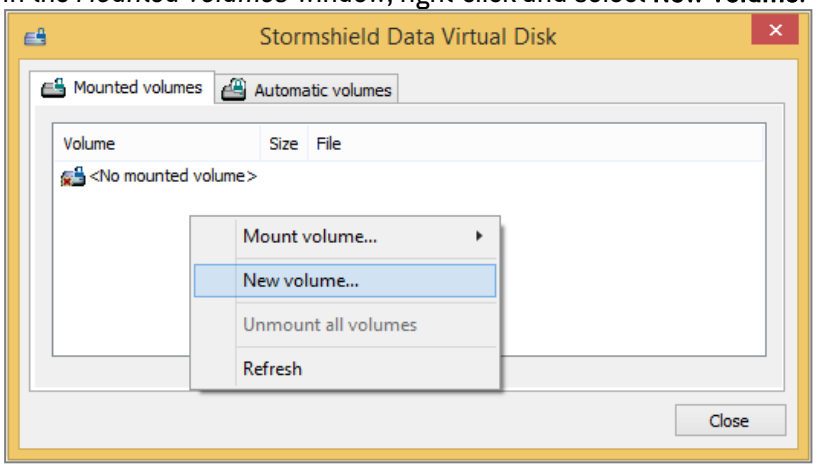
An encrypted volume can be used the same way as a normal hard disk drive. You can copy files on it and start applications that use these files. You can also install software on an encrypted volume.

Similarly to a physical disk volume, a virtual disk volume can be damaged or destroyed, leading to the loss of data contained in it. You must keep a backup copy of the files stored on the virtual volume, or the file hosting the content of the virtual volume. You should take the same precautions with this virtual volume as you would for a normal physical volume (formatting, error checking, fragmentation, and backup management).

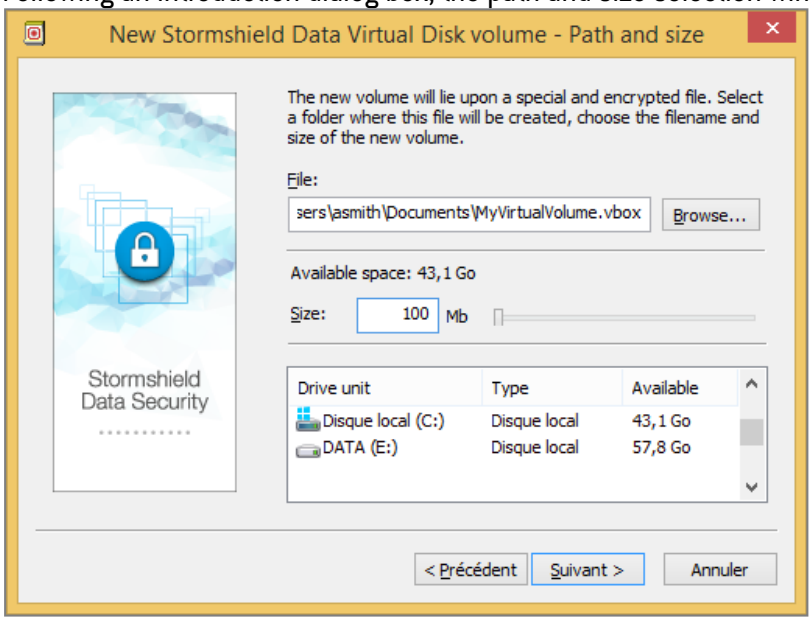
To create a secure volume:

1. In the Windows search bar, look for Stormshield Data Virtual Disk.
2. From the Stormshield Data Virtual Disk control panel, select the *Mounted volumes* tab.

3. In the *Mounted Volumes* window, right-click and select **New Volume**.



4. Following an introduction dialog box, the path and size selection window is displayed:



   a. Specify the volume name and its location in the **File** field. The *.vbox* extension is automatically added to the volume name.

> **IMPORTANT**
> If an encrypted volume is locally mounted in a Windows session, all users allowed to open a local session on the workstation will be able to access the content of the encrypted volume. For further information, refer to the section *Configuring and using the agent's advanced features* in the *SDS Enterprise administration guide*.

   b. Specify the volume size in the **Size** field. You can define the volume size between 1 MB and the maximum available size. The default volume size is 10% of the available space on the drive unit.

> **IMPORTANT**
> The maximum size of a Stormshield Data Virtual Disk volume is 2048 GB (2 TB).

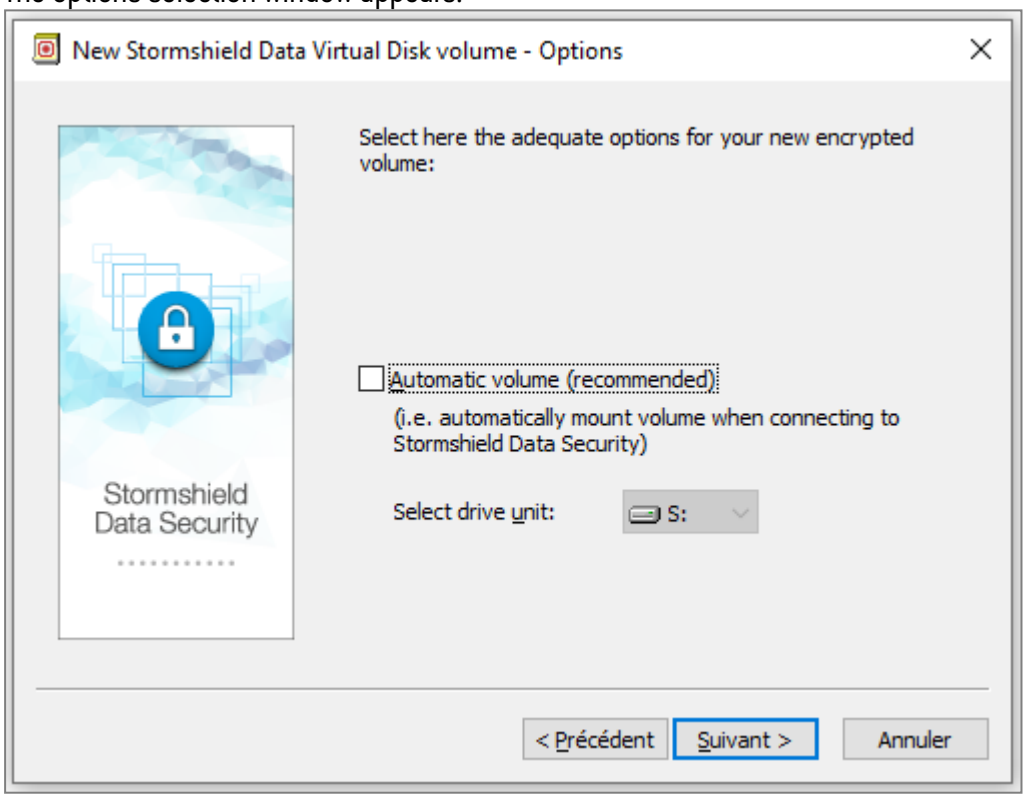
5. Click on **Next**.

6. You may want to authorize other users to use the new volume separately. Enter their name in the search field. The search displays users or groups specified in the trusted address book as well as users from the LDAP directory if it is configured. It displays the users or group members whose certificate is valid or revoked (the revocation status is checked in the background).
   - Groups coming from the local directory have a green icon,
   - Groups from the LDAP directory have a yellow icon,
   - Pressing the Enter key in the search field directly launches a search in the LDAP directory.

> **NOTE**
> Simultaneous use of the volume by different users is not possible. Each allowed user accesses the volume alternately.

When the users list is completed, click **Next**.

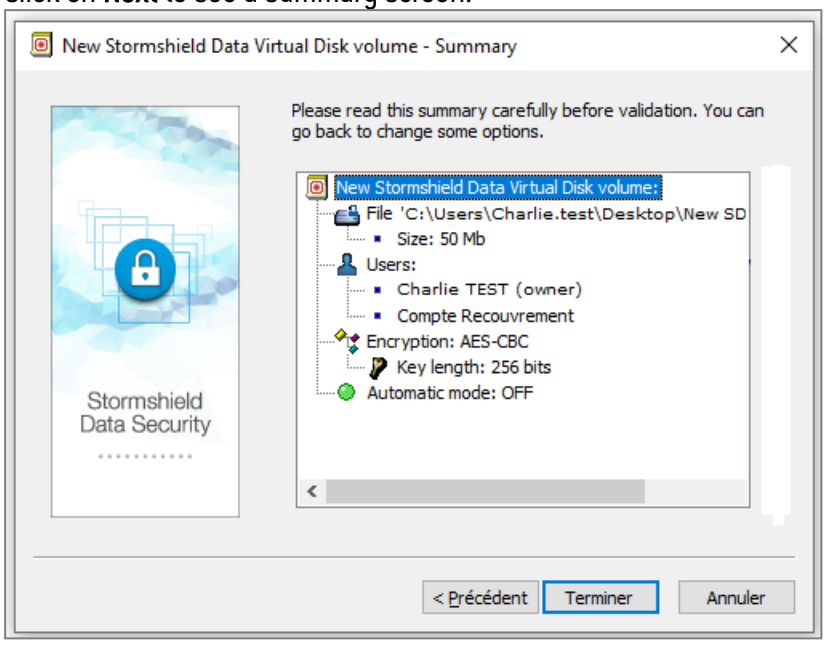
7. The options selection window appears:



In the dialog box displayed above you must:

- indicate if you wish the volume to be mounted automatically each time you connect to SDS Enterprise,
- select the drive unit mount letter to be used and indicate if the volume must be automatically mounted each time you connect to SDS Enterprise. The drive letter must not be used by another network drive or USB drive.

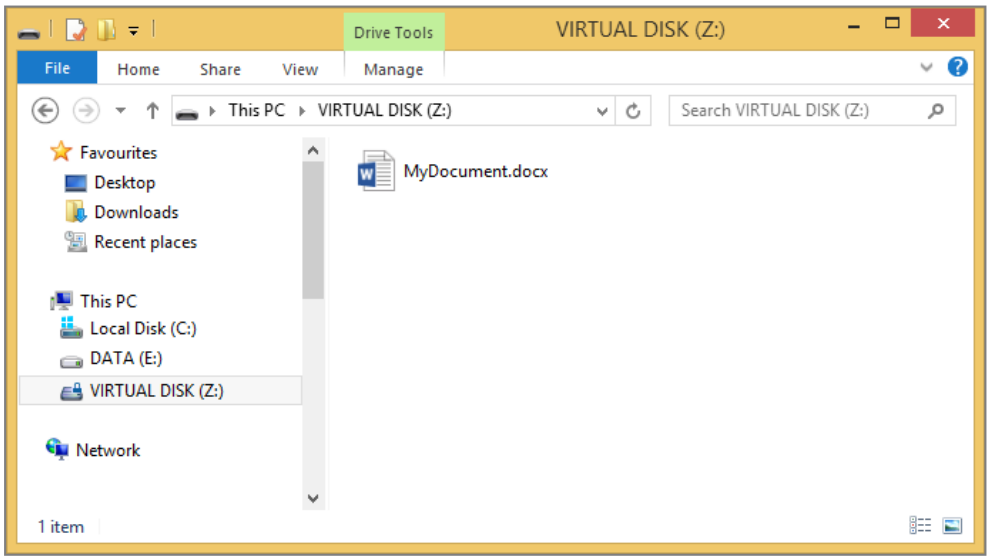
8. Click on **Next** to see a summary screen:



By default, the encryption algorithm and key strength used to encrypt your secured volume are AES-CBC and 256 bits. You can modify these values in the JSON policy configuration file. For more information, refer to the *Advanced configuration guide*.

9. Click on **Finish**.
The volume now appears in the Windows Explorer. All files placed on this volume are encrypted and only authorized users will be able to access the encrypted volume's content.

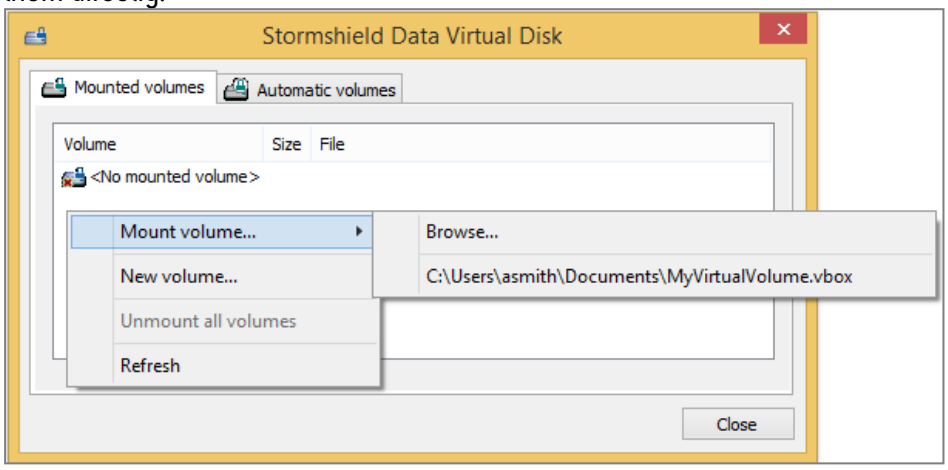
NOTE
The *.vboxsave* backup file is created in the same folder as the *.vbox* container file.



9.2 Mounting a secure volume

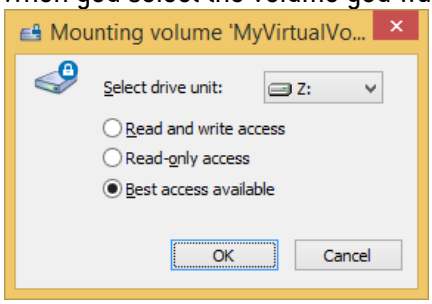
To mount an existing volume:

1. In the Windows search bar, look for Stormshield Data Virtual Disk.
2. From the Stormshield Data Virtual Disk control panel, select the *Mounted volumes* tab.
3. Right-click, then select **Mount volume** and **Browse** to select the volume you want to mount. The recently created volumes are listed below Browse and can be mounted by selecting them directly.



> **NOTE**
> The Automatic volumes tab enables you to mount an automatic volume if it was unmounted or if the mounting failed.

4. When you select the volume you want to mount, the following dialog box is displayed:



Select the drive unit and the access type:

- Read and write access: the volume has read/write access. This is only possible if the volume is not yet mounted.
- Read-only access: the volume has read access. This is only possible if the volume is not yet mounted with read/write access.
- Best access available:
  - The volume will be mounted with read/write access if it is not already mounted.
  - The volume will be mounted with read access if it is already mounted with read access.
  - An error message is displayed if the volume is already mounted with read/write access.

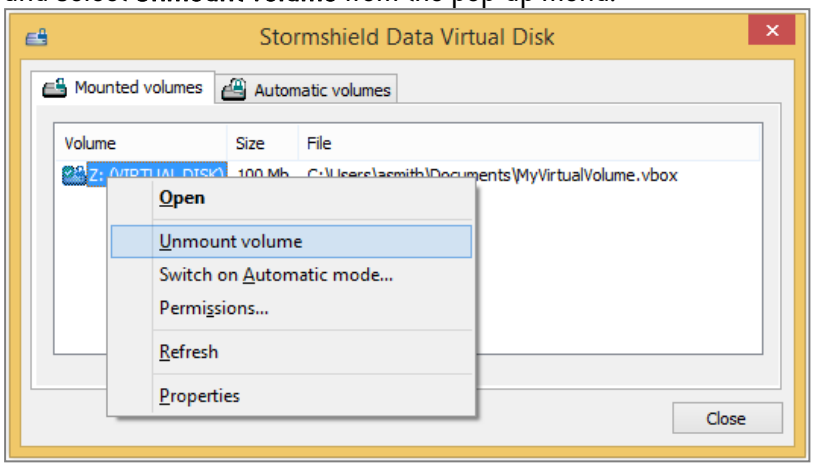
The drive letter must not be used by another network drive or USB drive. If the letter to mount the selected drive is already in use, an error message will appear.

In general, an encrypted volume is mounted to a local workstation.

However, an encrypted volume can be mounted to a file server. In this case, all data exchanged between the server and your workstation will be encrypted. Data will be decrypted on your local workstation.

9.3 Unmounting a secure volume

- To unmount a secure volume, select it from the Stormshield Data Virtual Disk control panel and select **Unmount volume** from the pop-up menu.



NOTE
The list of mounted volumes also includes the automatic volumes. You can also unmount automatic volumes in the Automatic volumes tab.

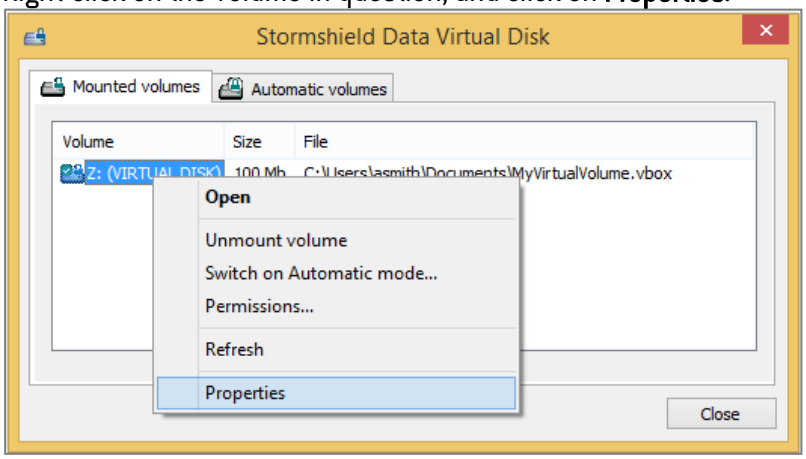
9.4 Accessing secure volume properties

Stormshield Data Virtual Disk offers two ways to access properties from:

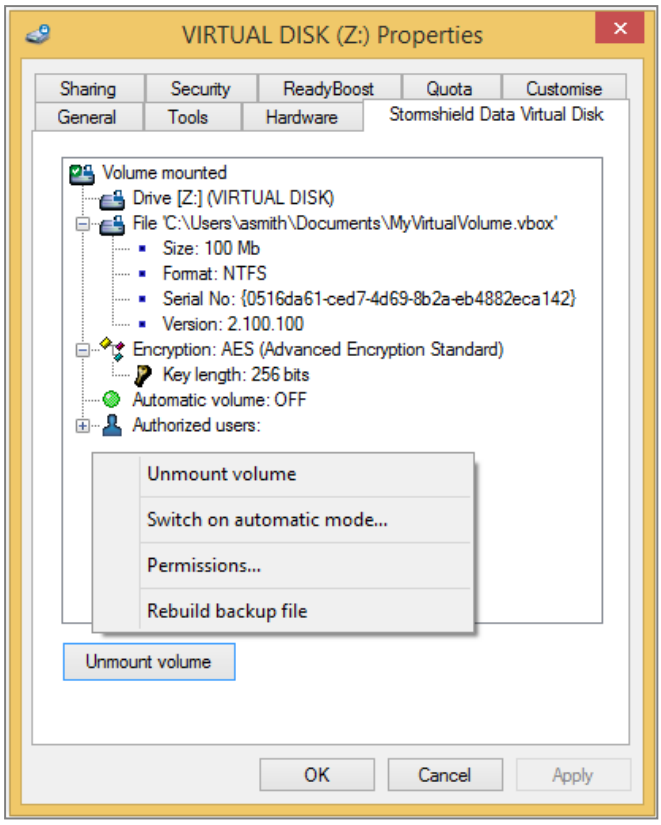
- The Stormshield Data Virtual Disk control panel for mounted volumes and automatic volumes,
- The container file (for unmounted volumes).

9.4.1 From the Stormshield Data Virtual Disk control panel

1. Right-click on the volume in question, and click on **Properties**.



2. Click on the Stormshield Data Virtual Disk tab.

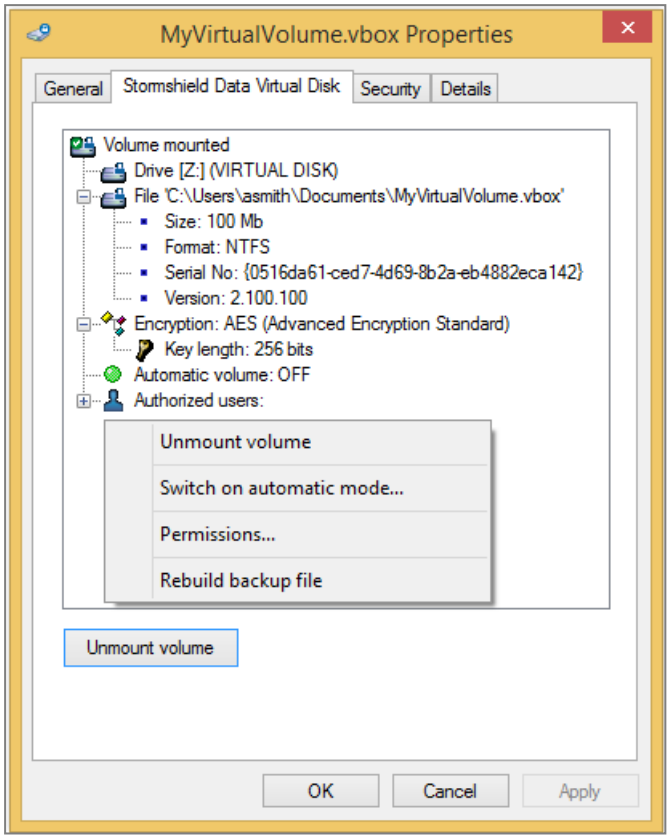


3. By right-clicking in the tab, you can:
   - Unmount the volume (the **Unmount** volume button also enables you to unmount the volume),
   - Switch volume mode (manual/automatic),
   - Modify user access permissions,
   - Rebuild a backup file.

> **NOTE**
> The *.vboxsave* backup file is created in the same folder as the *.vbox* container file.

9.4.2 From the container file

1. In Windows Explorer, right-click on the container file and click on **Properties**.
2. Click on the Stormshield Data Virtual Disk tab.



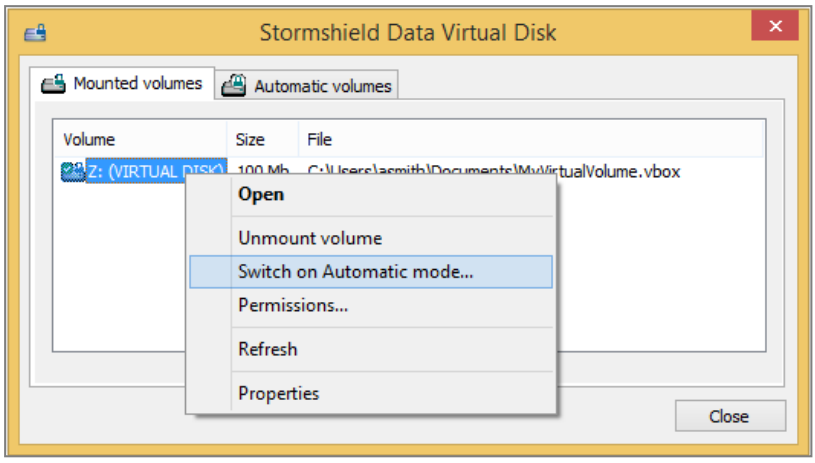
3. By right-clicking in the tab, you can:
   - Unmount the volume (the **Unmount** volume button also enables you to unmount the volume),
   - Switch volume mode (manual/automatic),
   - Modify user access permissions,
   - Rebuild a backup file.

9.5 Automatically mounting a secure volume

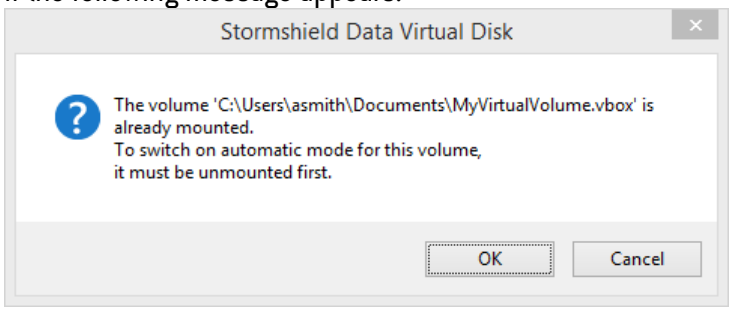
If you select the automatic volume mounting option, Stormshield Data Virtual Disk automatically mounts encrypted volumes whenever you connect to SDS Enterprise.

9.5.1 Switching on automatic mode

1. In the Stormshield Data Virtual Disk control panel, right-click on the encrypted volume and select **Switch on Automatic mode**.

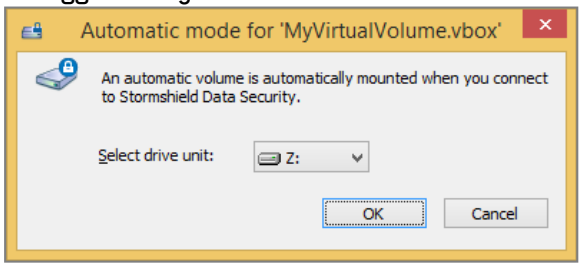


If the following message appears:



The volume must first be unmounted. Make sure there are no running applications using files on the volume, and click on **OK**.

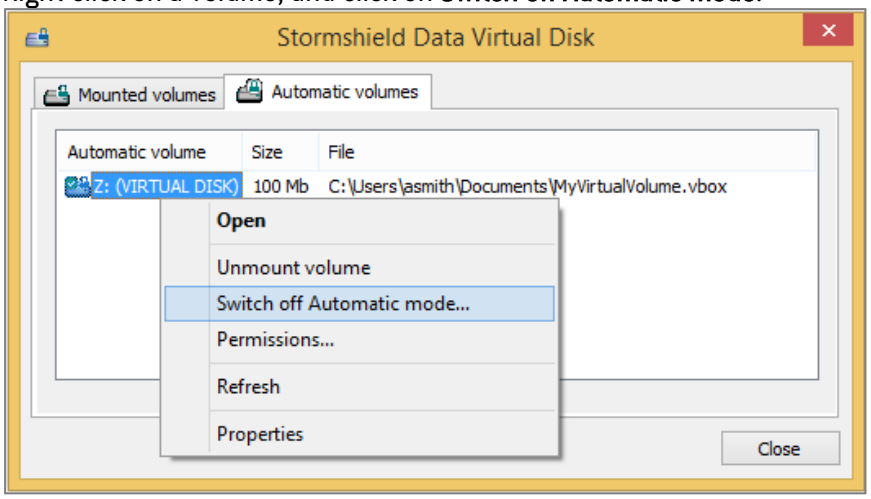
2. Select the drive unit (letter of the drive) to be used to mount the volume. The last unit used is suggested by default.



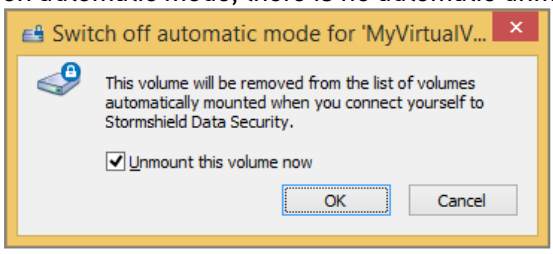
The drive letter must not be used by another network drive or USB drive.

9.5.2 Switching to manual mode

1. Select the **Automatic volumes** tab in the Stormshield Data Virtual Disk control panel.
2. Right-click on a volume, and click on **Switch off Automatic mode**.



3. A confirmation window will appear. Before clicking on **OK**, you can choose to unmount the volume by selecting the option **Unmount this volume now**. Unlike the process of switching on automatic mode, there is no automatic unmounting.



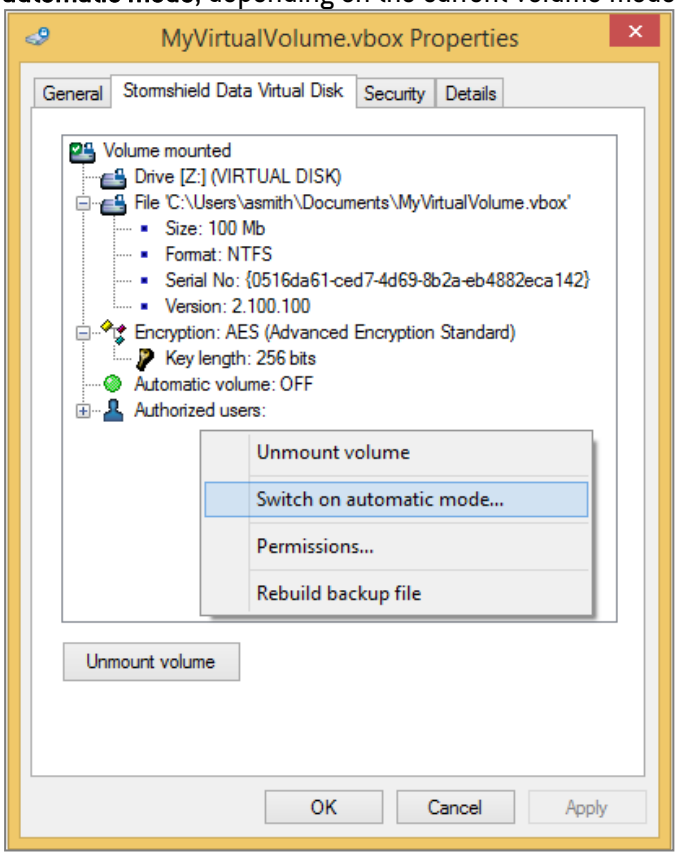
4. Click on **OK** to confirm your choice.

9.5.3 Switching on or off automatic mode from the container file

You can also switch on/off the automatic mode from the container file. In this case, there is no need to mount the volume beforehand to enable automatic mode.

1. In Windows Explorer, right-click on the container file and click on Properties.
2. Select the Stormshield Data Virtual Disk tab.

3. Right-click in the window and select either **Switch on automatic mode** or **Switch off automatic mode**, depending on the current volume mode.



9.6 Editing the list of users

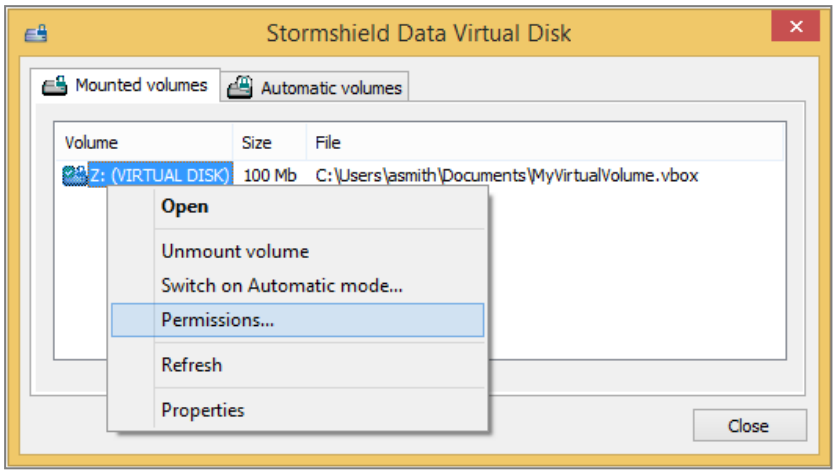
To edit the list of users, the volume must already have been mounted or in automatic mode.

Only the owner of a volume is allowed to edit the list of authorized users. The list can be edited from:

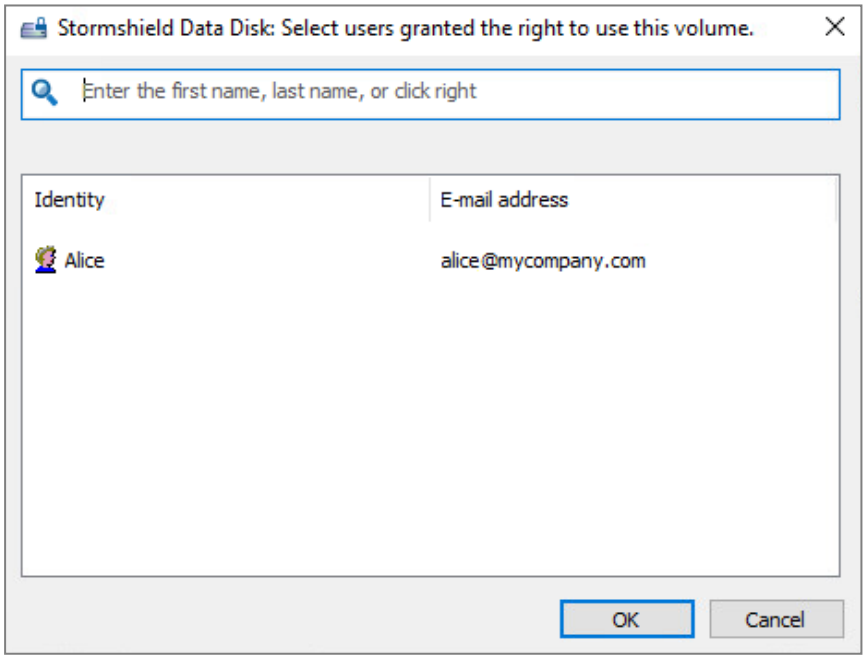
- The Stormshield Data Virtual Disk control panel for mounted volumes and automatic volumes,
- The container file.

9.6.1 From the Stormshield Data Virtual Disk control panel

1. Right-click on the **Mounted volumes** or **Automatic volumes** tab, select a volume and right-click to select **Permissions**.



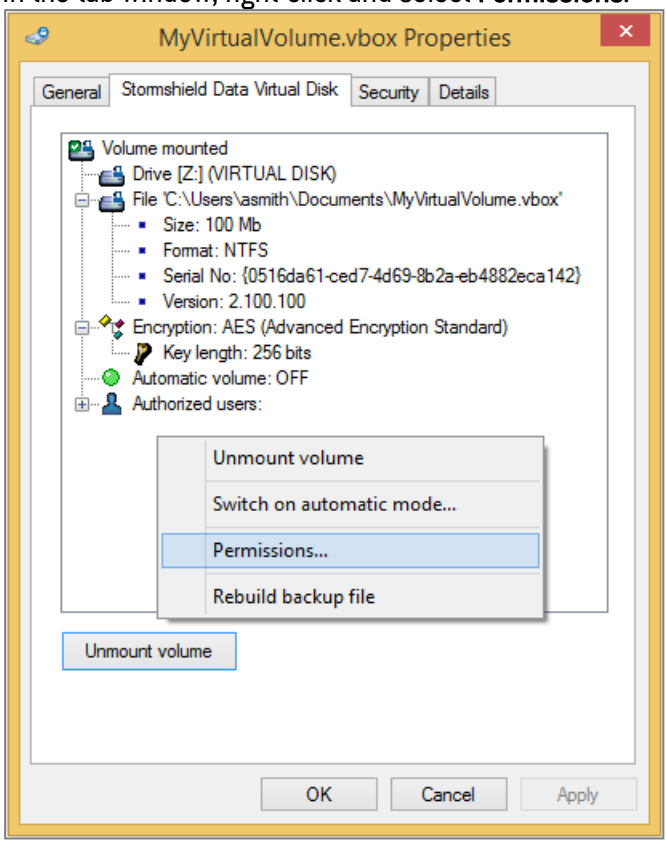
2. You can see the list of users authorized to access the volume. Search for users or groups who will be allowed to access the volume. The search displays users specified in the trusted address book as well as users from the LDAP directory if it is configured. It displays the users or group members whose certificate is valid or revoked.
   - Groups coming from the local directory have a green icon,
   - Groups from the LDAP directory have a yellow icon,
   - Pressing the Enter key in the search field directly launches a search in the LDAP directory.



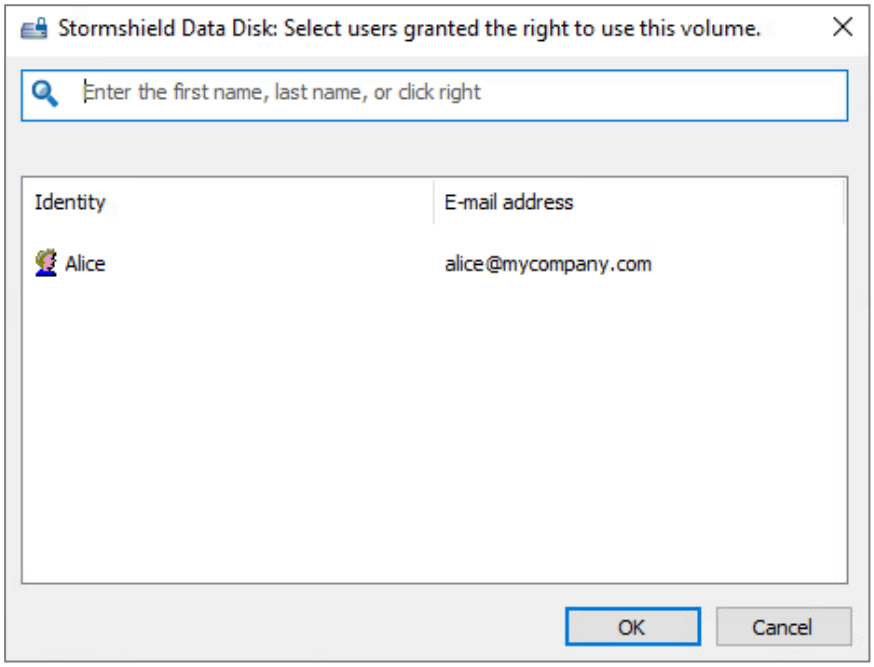
9.6.2 From the container file

1. In Windows Explorer, right-click on the container file and click on **Properties**.
2. Click on the Stormshield Data Virtual Disk tab.

3. In the tab window, right-click and select **Permissions**.



4. You can see the list of users authorized to access the volume. Search for users or groups who will be allowed to access the volume. The search displays users specified in the trusted address book as well as users from the LDAP directory if it is configured. It displays the users or group members whose certificate is valid or revoked.
   - Groups coming from the local directory have a green icon,
   - Groups from the LDAP directory have a yellow icon,
   - Pressing the Enter key in the search field directly launches a search in the LDAP directory.



9.7 Changing the owner of a volume

This function is an advanced feature that must be used with care, and which requires the application of a specific security policy..

The new owner must be from the list of authorized users. To add the new owner, refer to the section Editing the list of users.

1. In the settings of the *.json* configuration file of the policy that is applied to the workstation of the user in question, indicate the following parameters:

```
"diskPolicy": {
 "enableRescueFileModification": true,
 "enableExpertMode": true
},
```

   For more information on how to edit the security policy, refer to the *Advanced configuration guide*.
2. Deploy the updated policy file again on the workstation of the user in question.
3. On the user's workstation, ensure that the connected user is the owner of the volume, then open the folder that contains the container file in Windows Explorer. This folder contains the container file (extension *.vbox*) and another file of the same name but with the extension *.vboxsave* (this is the backup file).
4. Right-click on the *.vboxsave* file and select **Properties**.

5. Select the Stormshield Data Virtual Disk tab and click on the + sign to the left of the authorized users to see the full list.
6. Right-click on the name of the new owner and choose **Select as new owner**.

> **NOTE**
> If the **Select as new owner** option is not offered, this means that the *.json file* file has not been correctly edited or deployed on the workstation. It is also possible that the current connected user is not the owner of the volume.

Once the new owner has been selected, a warning message will appear at the bottom of the window to inform you that the list of users authorized to use the *.vboxsave* file is different from the list for the *.vbox* file.

7. Click on **Update volume** to synchronize both lists.

> **NOTE**
> If you change the owner of the volume when you are not its owner, the volume must be recovered. To do so, you must be authorized to perform a recovery. Refer to the SDS Enterprise *Administration guide* for more information.

10. Securing e-mails

Stormshield Data Mail is an extension that can be integrated with your Outlook mail client to add the following security features to your messages:

- **Confidentiality**: only intended recipients can read sent messages. Confidentiality is guaranteed through the encryption of the message.
- **Integrity**: messages cannot be modified during transfer without changes being detected.
- **Sender authentication**: message recipients can be sure of the identity of the sender. The integrity of the message and the authentication of the sender are guaranteed through a digital signature.

Secure messages are saved in this form in your message database.

Stormshield Data Mail uses the S/MIME V3 standard: you can exchange secure messages with recipients who use messaging software that supports the S/MIME V2 or V3 standard.

Stormshield Data Mail cannot be added to native security functions in Outlook. Messages with double security measures cannot be read by recipients.

Stormshield Data Mail is available as an add-in on Microsoft Outlook 2019 and 365 Professional mail clients.

It is compatible with the following e-mail servers:

- Microsoft Exchange Server 2010 SP1/SP2/SP3
- Microsoft Exchange Server 2013 SP1
- Microsoft Exchange Server 365
- Microsoft Exchange Server 2019

For more information on how to configure Stormshield Data Mail in SDMC, refer to the *SDS Enterprise Administration guide*.

10.1 Sending a secure message

Messages are secured only when they are sent. This means that drafts are not secured.

10.1.1 Using the Agent's features

1. Log in to SDS Enterprise.
2. Write the message as you usually would using your e-mail software.
   Use HTML format to write messages. Stormshield Data Mail does not support rich text format (RTF) as it may cause information loss.
3. If you wish to sign the message, in the **Security** area in the *Message* tab, click on . E-mail signatures in PGP format are not supported.
   - or -
   If you wish to encrypt the message, in the **Security** area in the *Message* tab, click on .

   The lower banner Stormshield Data Security appears in the message window and displays the security options you selected.

4. In the lower banner, click on **Edit...** to select the format in which secured messages will be sent – S/MIME or PGP. This option is only available if PGP was configured in the policy. For more information, see the *SDS Enterprise* Administration Guide, sections *ConfigureStormshield Data Mail* and *Configure Corporate Directories*.
5. Click on **Send**.

Your sent message is stored in your folder (**Sent items** by default), secured with the security options you have selected. If you have selected encryption, the message is automatically encrypted with your own public key. It will be decrypted when you open it.

NOTE
Editing a secure message directly in the outbox is not supported.

10.1.2 Use Microsoft Purview Information Protection sensitivity labels

You can also encrypt and sign your messages by applying Microsoft Purview Information Protection sensitivity labels.

Automatic message encryption and signing can be associated with the use of labels. They are defined in the security policy. For more information about this Microsoft feature, see the Microsoft Purview Information Protection product documentation.

For more information on the use of sensitivity labels in the policy, see the *SDS Enterprise*Administration Guide, section *Configuring Stormshield Data Mail*.

The use of Microsoft labels is complementary to the use of the **Encrypt** and **Sign** options of the SDS Enterprise Agent, described above.

10.2 Reading secure messages

This chapter explains how to read secure messages and reply to them.

10.2.1 Opening secure messages

You receive and read messages as you normally would using your messaging software. If an e-mail has been encrypted by its sender, Stormshield Data Mail will decrypt it when you open the e-mail. If the message contains a signature, Stormshield Data Mail verifies the signature and indicates issues if any.

If you are not connected to SDS Enterprise, a window displays and prompts you to connect to be able to read the message or verify the signature.

NOTE
An encrypted and/or signed *.msg* file cannot be opened from Windows Explorer. For more information, refer to the article in the Stormshield Knowledge Base.

IMPORTANT
You cannot modify a received secured message with the Outlook menu **Actions > Edit Message** because this action could disable the security of the message.

10.2.2 Viewing the security report

When a secure message is opened, you can view the security report by clicking on the link in the upper banner Stormshield Data Security.

An icon next to the **Security report** link may indicate an error or a warning explained in the report, if any. If an error occurs, the security banner will appear in red.

The security report details the algorithms used to encrypt and sign the message.

If the message is signed, the security report also displays:

- The identity of the sender who has signed the message,
- An indication of the level of trust assigned to the sender's certificate in the upper banner of the report window which indicates:
  - The result of the signature's cryptographic verification. The signature is then considered correct or incorrect,
  - The results of checks carried out on the sender's certificate: Stormshield Data Mail checks whether the certificate is valid, is authorized to sign, and does not present any unsupported critical extensions. If it does, the security policy will force the certificate to be rejected.

NOTE
Stormshield Data Mail does not support the verification of the signature of messages signed in PGP format. A message indicating that the signature could not be verified appears in the lower banner.

10.2.3 Replying or forwarding encrypted messages

When you reply one or more recipients of an encrypted message, automatic encryption is automatically selected in the reply message.

This is also the case when forwarding encrypted messages.

10.2.4 Reading secure messages sent as attachments

To be able to read a secure message which is attached to another message (secure or not), you need to drag and drop it to one of the folders of your mailbox.

When receiving e-mails including attachments, Outlook displays the size of the attachments. When the e-mails are encrypted, Outlook always displays "0 bytes".

10.2.5 Reading a message secured in OpenPGP

Stormshield Data Mail can now decrypt e-mails secured by a mail client that supports the OpenPGP protocol (PGP/MIME format). Decryption keys must be imported into your keyring beforehand in OpenPGP format.

For more information, refer to the *SDS Enterprise Administration guide*.

Importing an OpenPGP keyring

1. Right-click on the SDS Enterprise icon and select **Properties**.
2. In the *Configuration* tab, double-click on **Keyring**.
3. Select the **OpenPGP keyring** tab.
4. Click on **Operations** then on **Import a keyring**.
5. Select a file in OpenPGP format (*.gpg*, *.pgp*or *.asc*). The file may contain several keys.
6. Enter the password that protects the file.

To delete or replace the keyring, select the menus **Delete the keyring** or **Replace the keyring** in the **Operations** menu.

Replacing a keyring overwrites the existing keyring.

Reading a message secured in OpenPGP

You receive and read messages as you normally would using your messaging software. If an e-mail has been encrypted by its sender, Stormshield Data Mail will decrypt it when you open the e-mail.

If you are not connected to SDS Enterprise, a window appears and prompts you to connect to be able to read the message.

The security of a message encrypted and signed or only signed with the OpenPGP format cannot be disabled.

NOTE
Stormshield Data Mail does not support the verification of the signature of messages signed in PGP format. A message indicating that the signature could not be verified appears in the lower banner.

Reading a message secured in partitioned PGP

¨The Partitioned PGP format is the predecessor of the PGP/MIME format. Both formats rely on the same security mechanisms so the keyring format is the same.

Messages secured in Partitioned PGP are read in the same way as messages in PGP/MIME format.

10.3 Cross-encrypting secure messages

Cross-encryption makes it possible to update the protection level of secured messages. It consists of re-encrypting with your new key any message encrypted with a former encryption key and by using the default encryption algorithm defined in the user account.

The former encryption key may be out of date for the following reasons:

- The encryption key has been renewed,
- The user account has been updated and the encryption key became unusable, For example, when switching from a password account to a smart card account, or when a key is revoked or comes from another encryption system, etc.,
- The encryption key was sent by a third party, for example when privileges are transferred during the user's transition to a new position.

To cross-encrypt a secured message, the former encryption key is needed in order to decrypt the message first. The key must be in the keycase as a decryption key.

Once the message is cross-encrypted, only the new key is able to decrypt it.

Messages and attachments are cross-encrypted to their original formats: if they are in .sbox, they will remain in .sbox after cross-encryption.

> **NOTE**
> A delegation key cannot be used for cross-encryption because it only allows secured messages to be read.

10.3.1 Cross-encryption and managing coworkers

The way the cross-encryption process behaves with coworkers is as follows in both cases:

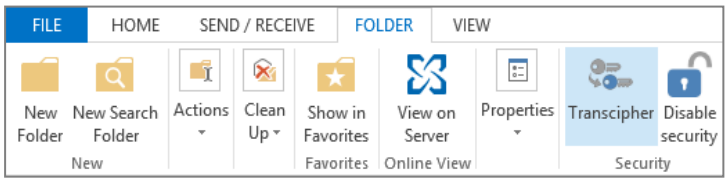
- When a secure S/MIME file sent to several recipients is cross-encrypted, it will be secured only for the current user. Coworkers will not be affected as only the local personal copy of the message is cross-encrypted.
- When a plaintext message with a secure attachment is cross-encrypted, only the security level of the attachment is updated. If this attachment is forwarded to coworkers declared in the original *.sbox* file, and if their certificates are still valid, they will still be able to access the attachment.

As for recovery accounts associated with user accounts, they will still be embedded in cross-encrypted messages.

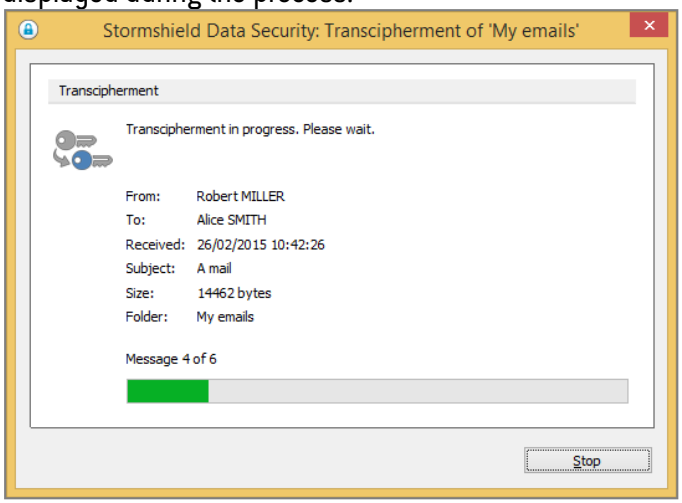
10.3.2 Using cross-encryption

Cross-encryption is an operation that is performed on a folder in your Outlook client and all its sub-folders.

1. Select the folder to cross-encrypt.
2. Right-click on the folder and select **Cross-encrypt** or click on **Cross-encrypt** the *Folder* tab from the main ribbon.



3. In the cross-encryption window, click on **Cross-encrypt**. Information about the operation is displayed during the process.



4. At the end of the process, a report shows the number of cross-encrypted messages and the number of errors. If errors occurred, click **View report**.

The report gives details about the errors for each e-mail impacted:

- The user does not have a valid encryption key,
- The user only has a delegation key,
- An error occurred during the processing of the message,
- The File feature is not installed (in case the message contains a secure attachment).

The report file is named *SBoxTranscipherment Report-<utilisateur>-<horodatage>.txt* and is stored in the user's temporary folder. The file remains in this folder.

NOTE
To access the user's private keys during cross-encryption, you must be connected to the SDS Enterprise account.

The progress window prevents any interaction with Outlook during the process. Despite this, if cross-encryption is disrupted, the user must manually restart the process.

10.3.3 Limitations of cross-encryption

Cross-encryption cannot support some cross-encrypted message configurations:

- Secure attachments contained in secure S/MIME messages are not cross-encrypted,
- Secure messages sent as *.msg* attachments in a plaintext message are not cross-encrypted.

Messages encrypted with OpenPGP cannot be cross-encrypted.

10.4 Disabling security

By default, secure messages that you receive are stored as secure messages in the Outlook message database.

It is possible that you may not want to store messages in a secure format, for example if you want to put the message into a public folder.

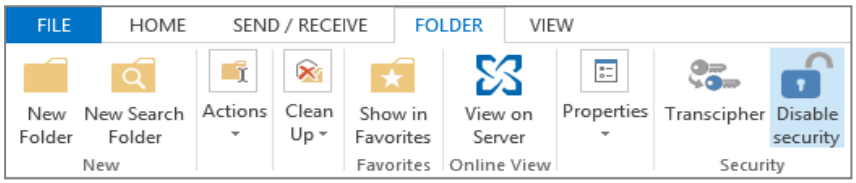
When disabling security, encrypted and/or signed e-mails will be stored in plain- text mode, without encryption or signature.

> **NOTE**
> A delegation key cannot be used to remove security.

The security can be disabled on a folder in your Outlook client and all its sub-folders or on a selection of e-mails.

10.4.1 Disabling security on a folder

1. Right-click on a folder and select **Disable security** or click on **Disable security** in the *Folder* tab from the main ribbon.



2. In the security disabling window, click **Disable security**. Information about the operation is displayed during the process.
3. At the end of the process, a report shows the number of unsecured messages and the number of errors. If errors occurred, click **View report**.

The progress window prevents any interaction with Outlook during the process. If the security disabling process is even though interrupted, the user must manually restart the process.

10.4.2 Disabling security on a selection of e-mails

1. Select one or more e-mails.
2. Right-click the selection to display the contextual menu and select **Disable security** or click **Disable security** on the *Home* tab from the main ribbon.
3. The following steps are the same than in the procedure above.

10.4.3 Reading the security report

The report gives details about the errors for each e-mail impacted:

- The user does not have a valid encryption key,
- The user only has a delegation key,
- An error occurred during the processing of the message,
- The user does not have a valid encryption key,
- The user only has a delegation key,
- An error occurred during the processing of the message.

The report file is named *SBoxDeleteSecurityReport- <timestamp>.txt* and is stored in the temporary folder of the user. The file remains in this folder.

E-mails on which errors occur are usually encrypted e-mails which use an unknown key, for example, an old key which has not been imported as a decryption key in your account.

NOTE
Users need to be connected to their SDS Enterprise account when disabling the security on e-mails so that private keys can be accessed.

10.4.4 Limitations when disabling security

The security cannot be disabled on some e-mail configurations:

- The security of a secured e-mail sent as an attachment *.msg* of a plain-text e-mail or a secured e-mail cannot be disabled.
- The security of an e-mail encrypted and signed or only signed with the OpenPGP format cannot be disabled.

10.5 Interacting with Stormshield Data Connector

If the Stormshield Data Connector module has been installed on the machine, you can send encrypted and/or signed messages from a PowerShell script or a .NET program.

For more information, refer to the Stormshield Data Connector *user guide*.

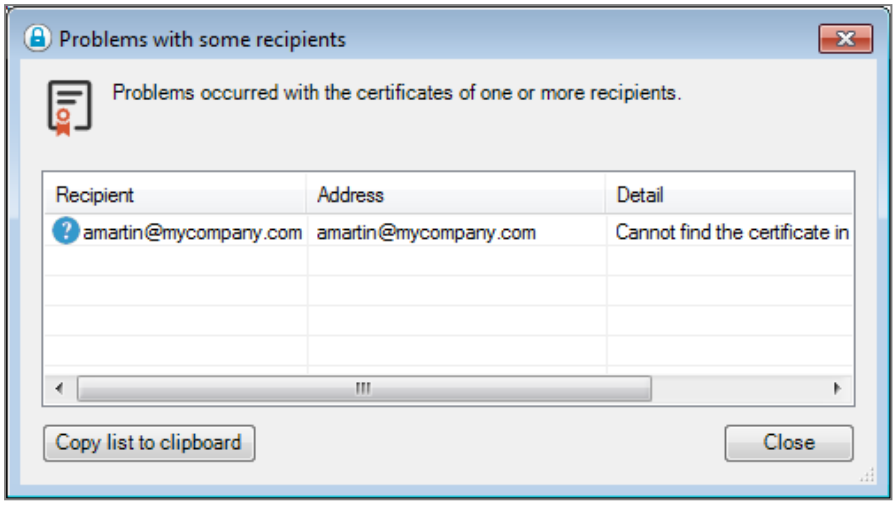
10.6 Troubleshooting

10.6.1 Certificate not found, contains errors or is invalid

If you are encrypting your message, Stormshield Data Mail searches your trusted address book and, if necessary, your LDAP directories for each recipient's certificate. It also verifies whether the certificate is valid, is authorized for encryption, and presents no unsupported critical extensions.

NOTE
When sending a message to a dynamic distribution group, it is not possible to search for recipients' certificates. This is because SDS Enterprise cannot access the e-mail addresses of members of such groups.

If any certificates are not found when sending the e-mail, Stormshield Data Mail displays the recipients in question with a  sign.



Certificate issues must be resolved before your message can be sent. If any certificates are not in your address book, you must import them. If the recipients are part of a contact group, you can remove the recipients whose certificates cause issues.

Stormshield Data Mail displays the certificates which present an issue (self-certified certificate, expired revocation list, etc.) with the warning sign. If, at the time of sending, all certificates are in warning mode, you can still continue sending with the **Continue** button, or resolve the issues raised by the certificates after canceling the send.

If any certificates contain errors when sending the e-mail (expired, revoked, etc.), Stormshield Data Mail displays the affected certificates with a sign. Certificate issues must be resolved before your message can be sent.

IMPORTANT
If a coworker's e-mail address has changed, the user certificate must be renewed and republished in the LDAP directory, if necessary. If the coworker's e-mail address is not the same as the one indicated in their certificate, they will no longer be able to send secure messages.

11. Signing files

Stormshield Data Sign makes it possible to electronically sign documents. Digital signatures are based on a Public Key Infrastructure (PKI) and are the result of a cryptographic operation.

Stormshield Data Sign makes it possible to guarantee the authenticity of signers' identities and the integrity of what these files contain.

In addition, signing a document with Stormshield Data Sign can be considered a commitment, like a written signature does.

When a user signs a file with Stormshield Data Sign:

- The unique fingerprint of the document is created using a mathematical algorithm
- The document fingerprint is signed using the user's private key and is combined with their public key and certificate to create a unique digital signature which is appended to the file.

Stormshield Data Sign puts the signed file in a new file that has the same name as the original file but with a different extension. The signed document is sealed and any changes made to it after it has been signed invalidates the signature, thereby protecting against signature forgery and information tampering.

When you check a signed document using Stormshield Data Sign:

- The signature of the sender is verified using the public key of the sender and the original document fingerprint is extracted. Then Stormshield Data Sign calculates the fingerprint of the received data and compares it to the original one previously extracted. If both fingerprints are the same, the document integrity is validated
- The authenticity and validity of the sender's certificate, and therefore its signature, are validated using the Certificate Revocation List (CRL).

For more information on how to configure Stormshield Data Sign in SDMC, refer to the *SDS Enterprise Administration guide*.

11.1 Stormshield Data Sign characteristics

11.1.1 Various signature types

Stormshield Data Sign allows multiple levels of signatures on the same document. You can therefore:

- **Co-sign** a document by adding your own signature to a document already signed, independently from other signatures (already present)
  For example, a contract between two parties requires both party signatures. Stormshield Data Sign allows each party to sign the contract independently from each other and in any order.
- **Counter-sign** a signed document by adding your own signature on someone else's signature.
  For example, the payment of an invoice must be first be signed by the person who places the order to validate the invoice, then counter-signed by the accountant. Payment requires both signatures; the accountant waits for the validation of the person who places the order, and counter-signs the validation.

- **Over-sign** by signing the envelope containing an already signed file.
  For example, a carrier guarantees the integrity of the document which must be delivered by placing the signed document in an envelope and signing this envelope. No co-signature or counter-signature can then be added or removed from the transported document. The over-signer does not know the content of the envelop.

11.1.2 Compatibility

Stormshield Data Sign allows you to save the signed files using two different file extensions: *.p7f* and *.p7m*.

.p7m signed files can be sent to and validated by recipients who do not use Stormshield Data Sign, but who run another RFC 2630-compliant app that specifies the rules of the digital signature format.

11.2 Signing a file

If you are about to sign a Microsoft Word or a PDF document, Stormshield Data Sign can analyze this document and warn you of the presence of macros or active content which could dynamically modify the appearance of the document. These checks can be enabled in the configuration of the Sign feature. You can then decide whether to sign the document. For more information, refer to the section *Configuring Stormshield Data Sign* in the *Administration guide*.

There are two ways to sign files.

11.2.1 Signing from the pop-up menu

To sign a file:

1. Select the file to sign and right-click to choose **Stormshield Data Security** > **Sign** from the pop-up menu.
2. Follow the instructions shown on the screen. When prompted, enter your password or PIN, then click on **Quit** to end the process.

After successfully signing a file, Stormshield Data Sign does not modify the original file. Instead, it generates a new file with the same file name but with a *.p7f* or *.p7m* extension.

To sign and encrypt a file:

1. Select the file to sign and right-click to choose **Stormshield Data Security** > **Sign and encrypt** from the pop-up menu.

   > **NOTE**
   > This menu is available only if Stormshield Data File has been installed.

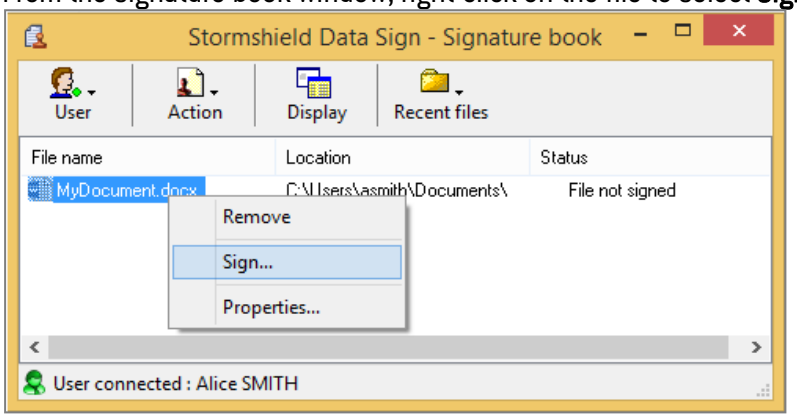
2. Follow the instructions shown on the screen. When prompted, enter your password or PIN (if you use a smart card) and click on Quit.
3. When the **Select recipients** window opens, select the recipients for whom you want to encrypt files, then click on **OK**.

11.2.2 Signing from the Stormshield Data Sign signature book

1. Select the file to sign and right-click to choose **Send to > Stormshield Data Sign** from the pop-up menu: The file is then dropped in the signature book.

> **NOTE**
> If the signature book window is already open, you can select the desired file, and drag and drop it in the Signature book window.

2. From the signature book window, right-click on the file to select **Sign**.



3. Follow the instructions displayed on the screen. When prompted, enter your password or PIN (if you use a smart card).

After successfully signing a file, Stormshield Data Sign does not modify the original file. Instead, it generates a new file with the same file name but with a *.p7f* or *.p7m* extension.

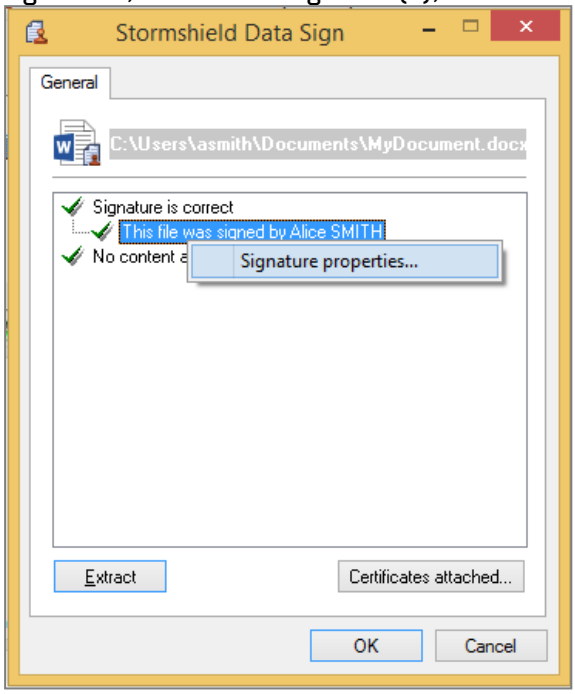
11.3 Checking a signed file

Use the following procedure to check a signed file. The file must have the .p7f or .p7m file extension.

1. In Windows Explorer, double-click or right-click on the desired file and select **Send to > Stormshield Data Sign** from the pop-up menu. The signature book window automatically opens and the file is dropped in it.

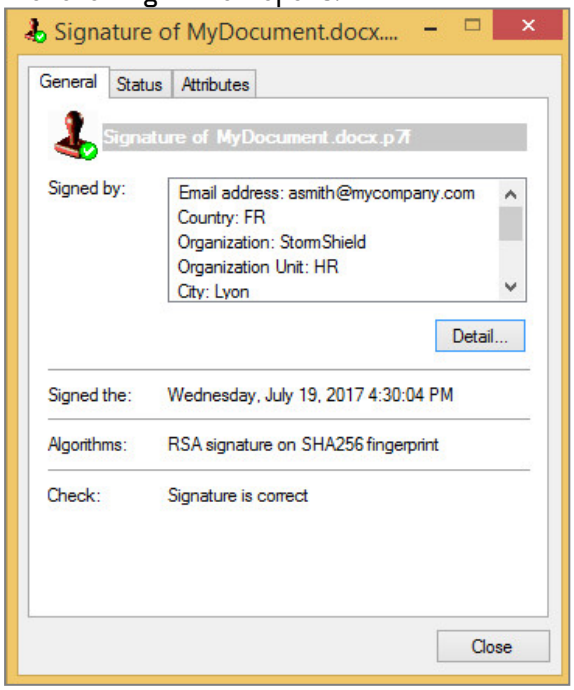
> **NOTE**
> If the signature book window is already open, you can also drag and drop the desired file in the signature book window.

2. Right-click on the file to select **Signatures** from the pop-up menu. The signer's certificate then appears, as shown below. Only the primary level of signatures is displayed. It includes the signature, co-signature(s) and counter-signature(s), if any. The second level of signatures, i.e. the over-signature(s), is not shown.

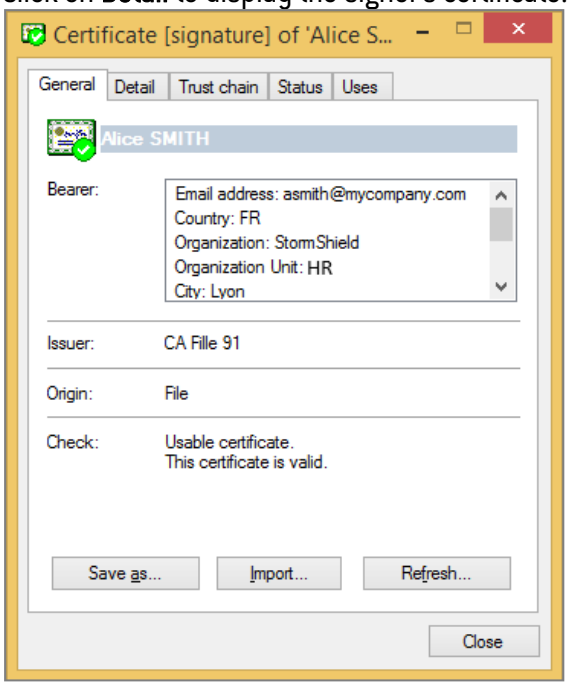


If you click on **Certificates attached**, Stormshield Data Sign displays the certificates attached to the file when it was signed. These certificates cannot be considered reliable and must be checked with your trusted address book or the LDAP directory.

3. Right-click on a signature and select Signature properties from the context-sensitive menu. The following window opens:



4. Click on **Detail** to display the signer's certificate:



Stormshield Data Sign verifies:

- The file content and signature authenticity: Stormshield Data Sign verifies the signature and gets the original document fingerprint. Then Stormshield Data Sign calculates the document fingerprint of the signed document and compares it to the original document fingerprint. If they are the same, this means that the signed document has not been altered and Stormshield Data Sign guarantees its authenticity.
- The signature certificate validity: Stormshield Data Sign checks the validity of the certificate which guarantees the authenticity of the signer. When there are multiple signatures, each individual signature is checked: all of the certificates needed to validate the digital signatures are verified.

In order to validate the certificate, Stormshield Data Sign uses the most recent Control Revocation List (CRL). As the CRLs are regularly updated, the result of the verification may be different each time you request a verification.

Click on Import to import user certificates into your trusted address book.

Click Refresh to dynamically update the signature information with new data including new certificates or CRL input.

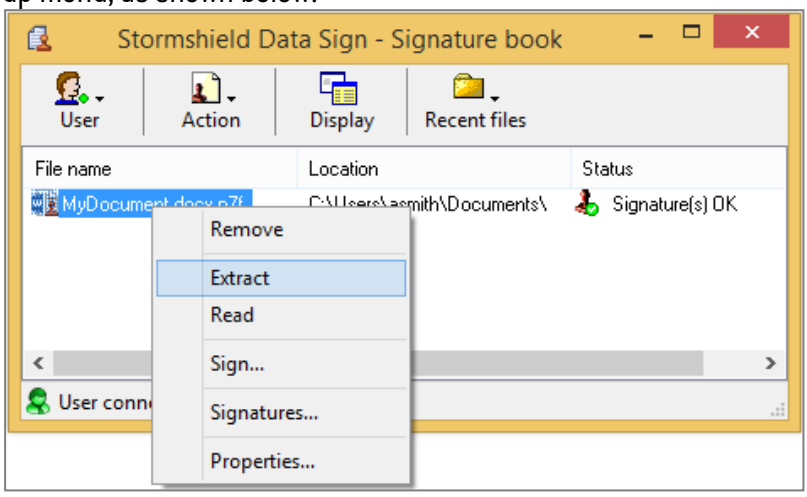
When the verification is complete, Stormshield Data Sign displays, next to the icon of the checked file, an icon that shows the result:

	The signature is correct and the signer's certificate is valid.
	An anomaly was found.
	A serious error was found.

11.4 Extracting the original file

Use the following procedure to extract the original content of the signed file and save it into a new file.

1. Perform one of two possible operations:
   - From the signature book window, right-click on the file and select **Extract** from the pop-up menu, as shown below:



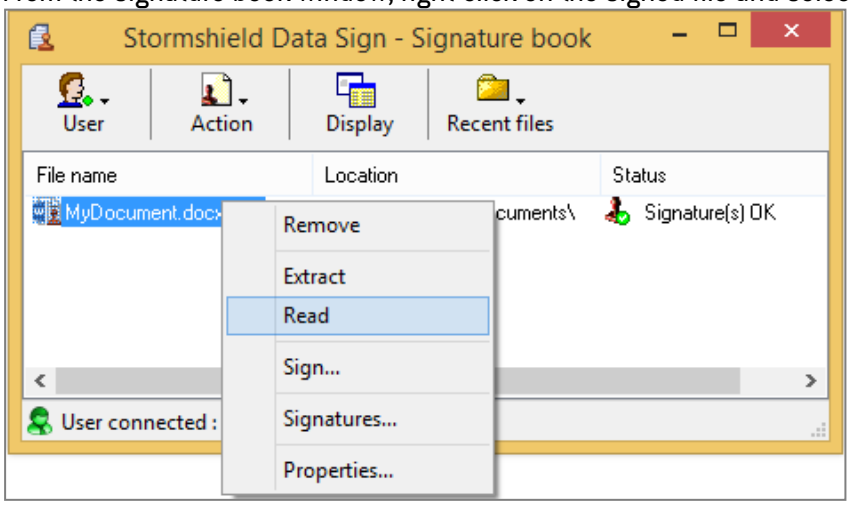
   - From the next window displaying the file signature, click on Extract.
2. Type in the file name under which the extracted and original file will be saved.

> **NOTE**
> If you extract an over-signed file, the resulting extracted file contains the primary signature but does not contain the over signature. The file extraction removes only one level of signatures.

11.5 Reading the contents of a signed file

Use the following procedure to open a signed file without extracting the original file and saving it onto your disk.

1. From the signature book window, right-click on the signed file and select **Read**:



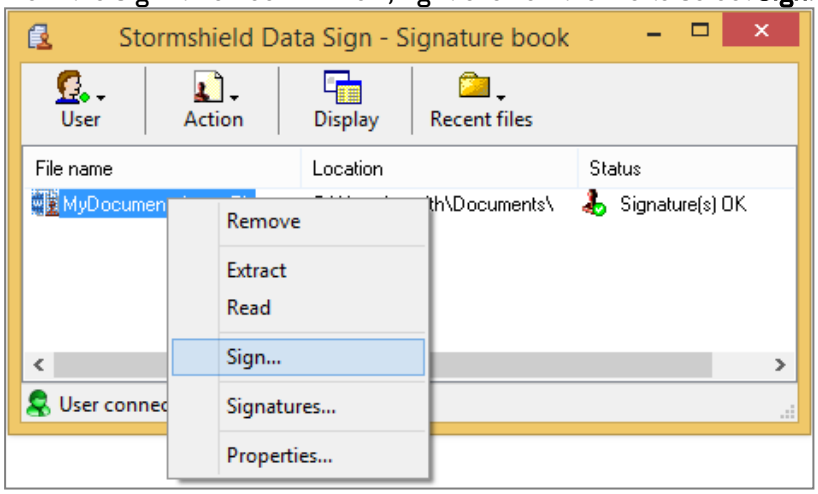
2. The signature report appears.

3. Click on Read. The default action associated with the type of the file is automatically run. Generally, the file is opened by the appropriate application.

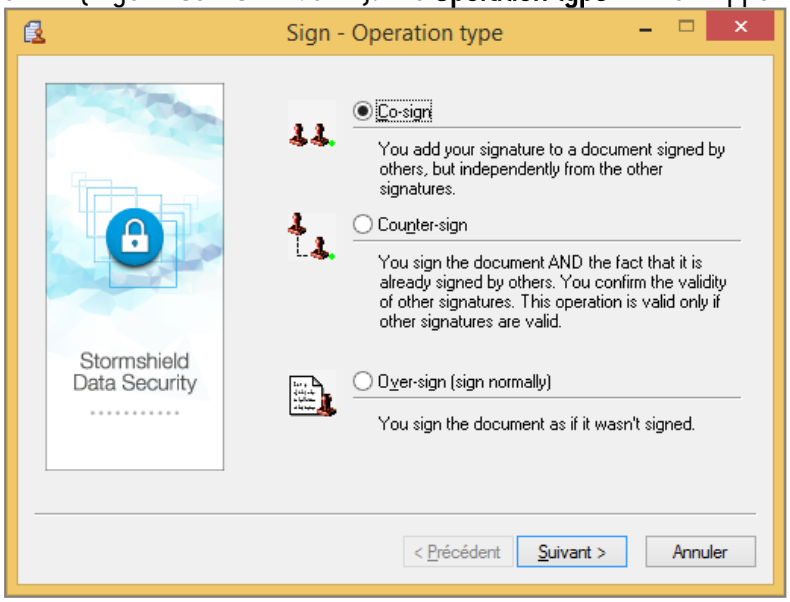
11.6 Signing a file that is already signed

To sign a file which is already signed:

1. In Windows Explorer, select the file to be signed and right-click to choose **Send to >Stormshield Data Sign** from the context menu: the file is then placed in the signature book window.
   - If the signature book window is already open, you can drag and drop the desired file in the Signature book.
   - You can double-click on a *.p7f* or *.p7m* file. The signature book window automatically opens and the file is displayed in it.
2. From the signature book window, right-click on the file to select **Sign**.



3. Follow the instructions displayed on the screen. When prompted for it, enter your password or PIN (if you use a smart card). The **Operation type** window appears:



4. Select one of the options according to your needs:
   - **Co-sign** to add your own signature to the file, independently from any other signature already present and whether they are correct or not.
   - **Counter-sign** to add your signature and counter-sign all the other signatures already included (and possibly other counter-signatures). This operation is only available if all the signatures have already been checked and validated.

     NOTE
     You can either counter-sign:
     - All the signatures of a signed document (as described above) or
     - Only one signature (see Counter-signing a specific signature).
   - **Over-sign**. When you over-sign a document, you actually create a new file using the same fine name and an additional .p7f extension.

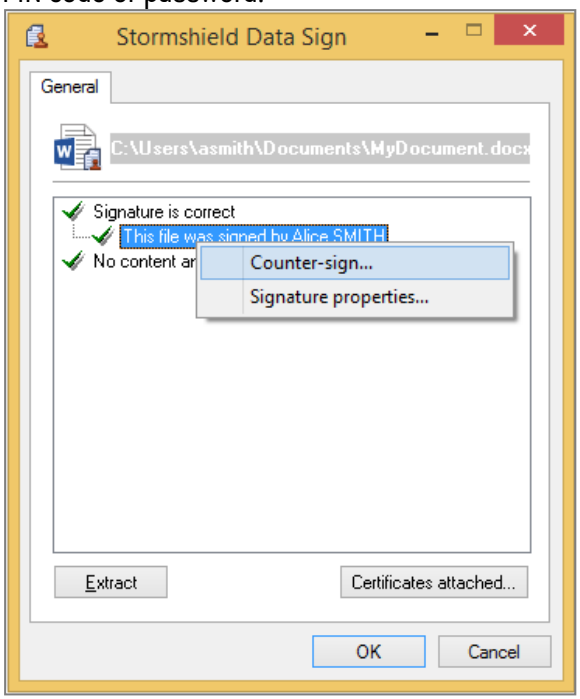
NOTE
Each time a file is over-signed, the .p7f extension is added to the new file generated. It is then possible to find files with several .p7f file type extension.

11.7 Counter-signing a specific signature

To counter-sign a specific signature in an already signed file:

1. In Windows Explorer, select the file you want to sign and right-click to select **Send to > Stormshield Data Sign** from the pop-up menu. The file is then dropped in the signature book window.
2. From the signature book window, right-click on the desired file and select **Signatures** from the pop-up menu. Stormshield Data Sign displays a signature and counter-signature tree contained in the file.

3. Right-click on the signature you want to counter-sign and select Counter-sign. Enter your PIN code or password:



Your counter-signature is added to the original signed file. This change will be applied as soon as you close the window.

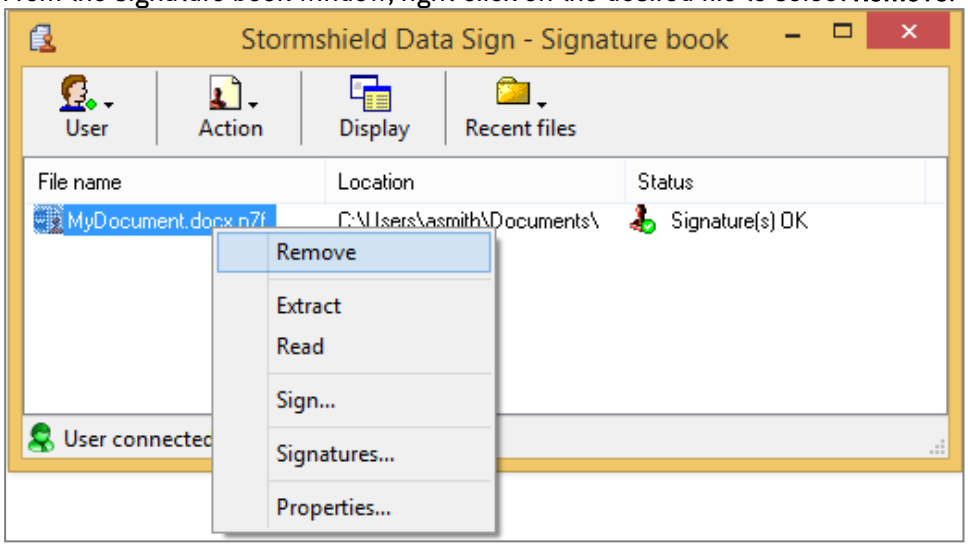
11.8 Notifying by email

On the last window of the wizard, there are two notification options:

- **Notify coworkers by email**: Stormshield Data Sign prepares an e-mail intended for coworkers to notify them that the document has been signed. If the document was previously signed, the recipients list is pre-filled with the co-signers' email addresses;
- **Request for a signature by email**: Stormshield Data Sign prepares an email intended to coworkers to notify them they must sign the document.

11.9 Removing a file from the signature book

1. From the signature book window, right-click on the desired file to select **Remove**:



2. Confirm your choice.

The file is then removed from the signature book list but is not physically deleted.

12. Permanently deleting files

This feature depends on Stormshield Data File and cannot run without it.

Stormshield Data Shredder makes it possible to guarantee the permanent, irreversible erasure of data that users wish to delete. The purpose of this procedure is to prevent third parties from recovering data that users thought had been deleted, without the users' knowledge.

The conventional data erasure procedure in Microsoft Windows does not completely erase data. There are tools that can analyze file fragments on the hard disk and reconstruct deleted files.

Stormshield Data Shredder writes a series of characters in bytes (00;FF;55 by default) in several rounds, replacing the file contents. The initial file is completely modified and even a full analysis of the hard disk, sector by sector, does not allow the data to be recovered.

Depending on the settings configured by the administrator in the policy, Stormshield Data Shredder can be launched:

- By right-clicking on the file or folder to be deleted to display the pop-up menu,
- By dragging and dropping from the Windows desktop.

For more information on how to configure Stormshield Data Shredder in SDMC, see the *SDS Enterprise* Administration guide.

12.1 Deleting files by right-clicking

1. In Windows Explorer, select the file or folder you want to shred, then right-click to select **Stormshield Data Security> Shred** in the pop-up menu.
2. Select several files or folders to be shredded at the same time, then start the shredding process. When a folder is erased by Stormshield Data Shredder, all files and folders in it are securely erased.
   To stop confirmation requests, unselect the checkbox **Request confirmation for each file**.

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

3. As 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.

12.2 Deleting files by dragging and dropping

Stormshield Data Shredder supports dragging and dropping 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 file icons to the Stormshield Data Shredder icon on the desktop, and release the button:

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 right-clickng in Windows Explorer.

13. Further reading

Additional information and answers to questions you may have are available in the Stormshield knowledge base (authentication required).

documentation@stormshield.eu