GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

USER GUIDE

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-user_guide-v10

Table of contents

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

1. Getting started

Welcome to the help center for the Stormshield Data Security Enterprise (SDS Enterprise) suite.

If you are a user of the suite and need help on the various modules that protect your files and e-mails, use this help center to get started quickly with Virtual Disk, Mail, Team, File, Shredder and Sign.

I'd like to:	I need to use:	
Create an encrypted virtual disk to store files safely on my workstation.	Stormshield Data Virtual Disk	 Virtual Disk
Encrypt e-mails and sign them to guarantee the authenticity of their sender's identity and the integrity of their contents	Stormshield Data Mail	
Share encrypted files with coworkers on my company's network	Stormshield Data Team	 Team
Encrypt files or folders on demand	Stormshield Data File	 File
Permanently delete files from my hard disk	Stormshield Data Shredder	 Shredder
Sign files to guarantee the authenticity of their sender's identity and the integrity of their contents	Stormshield Data Sign	 Sign
Add the certificates of my contacts to an address book so that I can encrypt files or folders for these contacts	SDS Enterprise Address book	 Address book

Depending on your company's security policy, some of these SDS Enterprise modules may not be installed on your workstation.

All documentation for the SDS Enterprise suite is available on the Stormshield technical documentation website.

2. Stormshield Data Virtual Disk

2.1 What is a virtual disk?

A virtual disk that is secured with Virtual Disk is a storage area that you can create on your workstation or on a removable device. It appears in Windows Explorer as a standard disk drive (e.g., K:) when you log in to your SDS Enterprise account.

2.2 What is the purpose of a virtual disk?

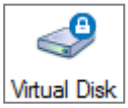
A virtual disk that is secured with Virtual Disk enables you to store all your sensitive data in it, and acts as a safe that effectively protects all the files you put into it. You can allow other users to access it if necessary, and you can share it easily via a file server or removable device because there is only one file to send.

NOTE
This encryption method is able to protect data up to the Restricted Distribution level.

2.3 How does a virtual disk work?

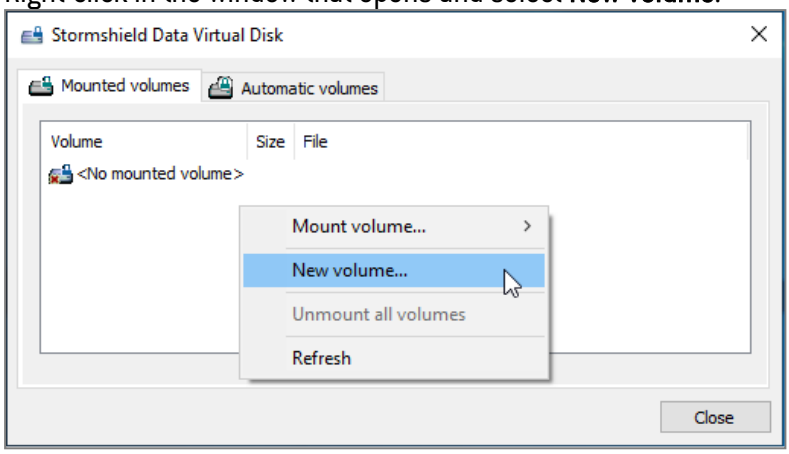
- Stormshield Data Virtual Disk automatically encrypts files placed on the virtual disk,
- Stormshield Data Virtual Disk automatically decrypts files in the virtual disk when an authorized user needs to read it,
- These encryption and decryption operations are transparent.

2.4 Creating and using an encrypted virtual disk

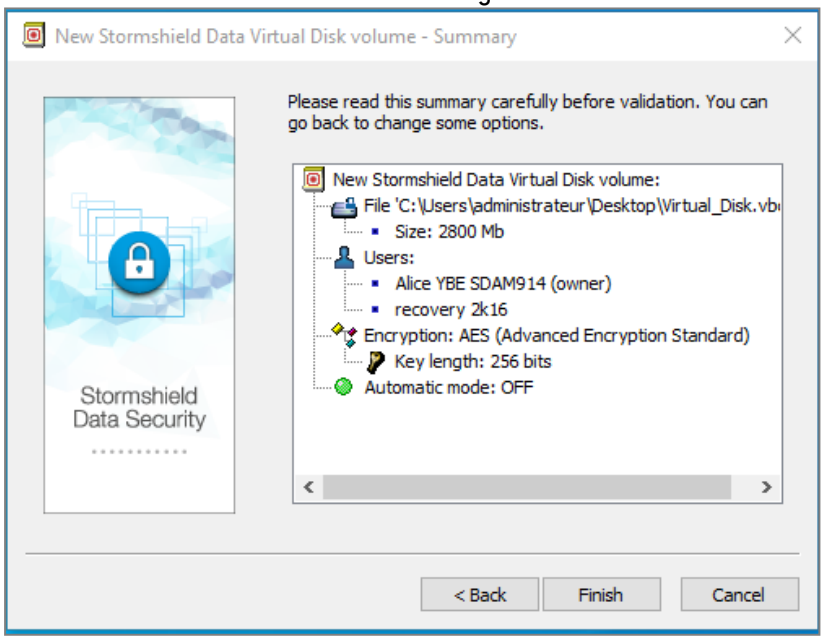
1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Open the **Properties** menu by double-clicking on the SDS Enterprise icon again.
3. Double-click on the 

icon. There may be a shortcut to this module on your desktop.

4. Right-click in the window that opens and select **New volume**.



5. Click on **Browse** to name the file that will contain the virtual disk and choose its location.
6. Define the size of the disk. Do note that the size of the disk cannot be changed once it is created, so make sure that you choose the appropriate size.
7. If necessary, select the coworkers who will be able to access the virtual disk. The list of coworkers is taken from your SDS Enterprise address book. For more information, see the section Managing the user address book.
8. You can select the **Automatic volume** checkbox, which allows you to automatically show the virtual disk in the file explorer when you log in to your SDS Enterprise account.
9. Click on **Next,** then on **Finish**. The virtual disk is now ready to be used in your file explorer like a standard disk. All documents that you send to it will be automatically encrypted



If you move a file from an encrypted virtual disk to a standard folder, it will no longer be protected and can be accessed even when you are not logged in to your SDS Enterprise account.

For more information on how to use Stormshield Data Virtual Disk, refer to the User Guide.

3. Stormshield Data Mail

3.1 What does Stormshield Data Mail do?

Stormshield Data Mail makes it possible to encrypt and/or sign your e-mails in Microsoft Outlook before you send them. This guarantees their confidentiality and integrity, and confirms your identity.

> **NOTE**
> This encryption method is able to protect data up to the Restricted Distribution level.

3.2 What is e-mail encryption?

- With Stormshield Data Mail, the body of an e-mail and its attachments can be encrypted,
- Only the recipients of the e-mail will be able to decrypt the e-mail and its attachments,
- E-mails encrypted with Stormshield Data Mail can be decrypted with any e-mail client that follows the S/MIME standard.

3.3 What is an e-mail signature?

- The signature proves to your recipients that you, and no one else, sent the e-mail,
- It prevents other users from assuming the identity of the sender because the **From:** field in mail clients can be easily falsified,
- It proves to your recipients that the contents of the e-mail were not changed between the moment you sent it and when the recipient read it,
- E-mails signed with Stormshield Data Mail can be verified with any e-mail client that follows the S/MIME standard.

3.4 Encrypting and signing an e-mail

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Write an e-mail as you normally would in Microsoft Outlook.
3. In the **Security** area in the **Message** tab, click on to encrypt your e-mail, and/or on to sign it.
4. The Stormshield Data Security Enterprise banner will appear at the bottom of the e-mail window.
5. Click on **Send**.

Your recipients must already be in your SDS Enterprise address book before these operations can be performed. For more information, see the section Managing the user address book.

When you are the recipient of a secure message, it will contain a banner at the bottom of the window:

For more information on how to use Stormshield Data Mail, refer to the **User Guide**.

4. Stormshield Data Team

4.1 What is a Stormshield Data Team-encrypted shared folder?

An encrypted shared folder:

- Can be used only with SDS Enterprise,
- Looks like a standard folder,
- Can be accessed only by people that the owner(s) of the folder has/have specifically allowed, for example, members of the same team.

4.2 What is the purpose of an encrypted shared folder?

A shared folder encrypted with Team allows members of a team to work together securely in the same folder. The information stored in such a folder cannot be accessed by any unauthorized user. Folders are usually shared on a file server, but they can also be local or on a removable medium.

NOTE
This encryption method is able to protect data up to the Restricted Distribution level.

4.3 How does an encrypted shared folder work?

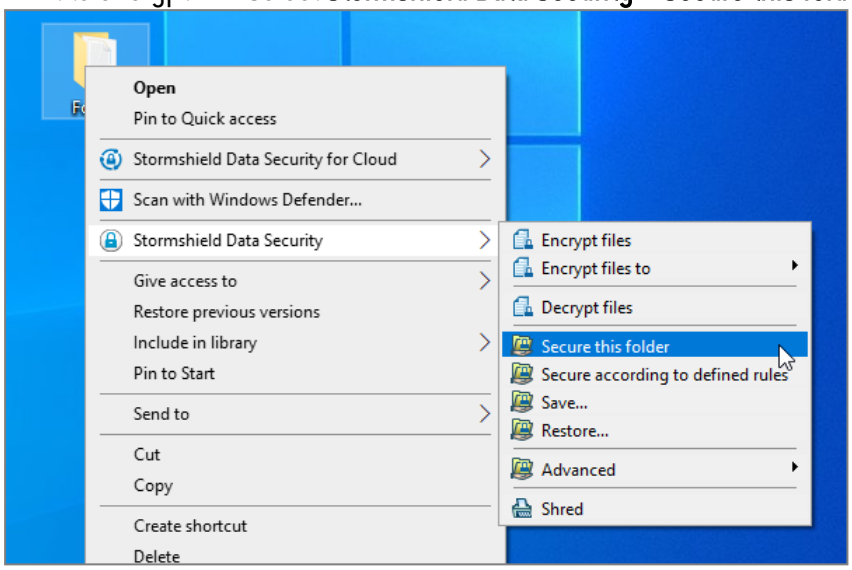
- Stormshield Data Team automatically encrypts files that are placed in the encrypted shared folder,
- Stormshield Data Team automatically decrypts files in the encrypted shared folder when an authorized user needs to read it,
- These encryption and decryption operations are transparent.

4.4 Creating and using an encrypted shared folder

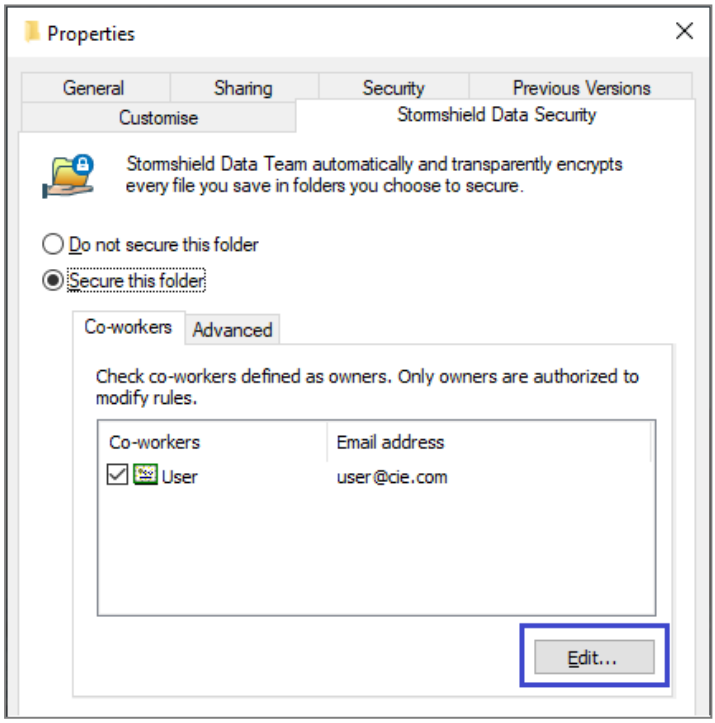
NOTE
Stormshield Data Team cannot secure synchronized directories such as SharePoint, Dropbox, Office 365, etc.

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the  taskbar.

2. Once you choose a location, such as a file server for example, right-click on the folder you want to encrypt and select **Stormshield Data Security** > **Secure this folder**.



3. Confirm. The contents of the entire folder will now be encrypted. Encryption may take a while depending on the volume of files and the quality of your network connection if the folder is located on a file server.
4. To add coworkers, right-click on the encrypted folder and select **Properties**.
5. In the **Co-workers** tab, click on **Edit**.



6. Select the coworkers who will be able to access the folder. The list of coworkers is taken from your SDS Enterprise address book. For more information, see the section Managing the user address book.
7. If necessary, select the checkbox in the **Co-workers** column to allow a user to add other coworkers.
8. Click on **OK** then on **Yes** to confirm the addition of coworkers. The contents of the folder are encrypted again, to take into account the added coworkers.

You and your team members can now use this folder in the same way you would use a standard folder. If a coworker adds new files, they will be automatically encrypted.

4.5 Modifying Team settings

You can check and modify the advanced settings of Stormshield Data Team:

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Open the **Properties** menu by double-clicking on the SDS Enterprise icon again in the taskbar.
3. Click on the 

icon.

For more information on how to use Stormshield Data Team, refer to the User Guide.

5. Stormshield Data File

5.1 What does Stormshield Data File do?

With Stormshield Data File, you can:

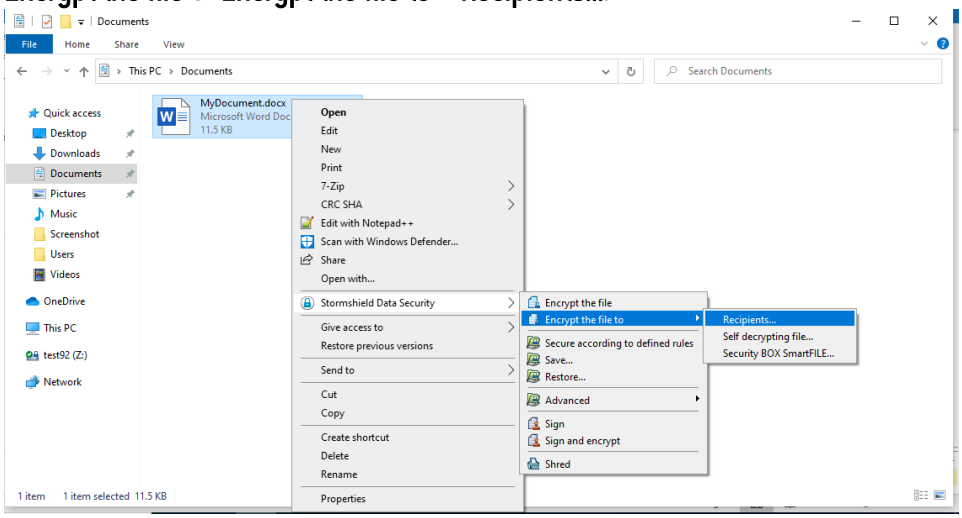
- Manually encrypt files or folders on your workstation,
- Manually encrypt files to send them to recipients who also have SDS Enterprise,
- Create encrypted files that can be automatically decrypted for recipients who do not have SDS Enterprise. Warning: this encryption mode relies only on a password exchange and is not suitable for the protection of sensitive data.

5.2 How does Stormshield Data File work?

Unlike Disk or Team, in which encryption and decryption operations are automatic, files or folders encrypted with Stormshield Data File must be manually decrypted in order to be used, and manually encrypted again to continue protecting them.

5.3 Encrypting for yourself or for recipients who have Stormshield Data File

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Right-click on the file or folder you want to encrypt and select **Stormshield Data Security** > **Encrypt the file** or **Encrypt the file to** > **Recipients...**.



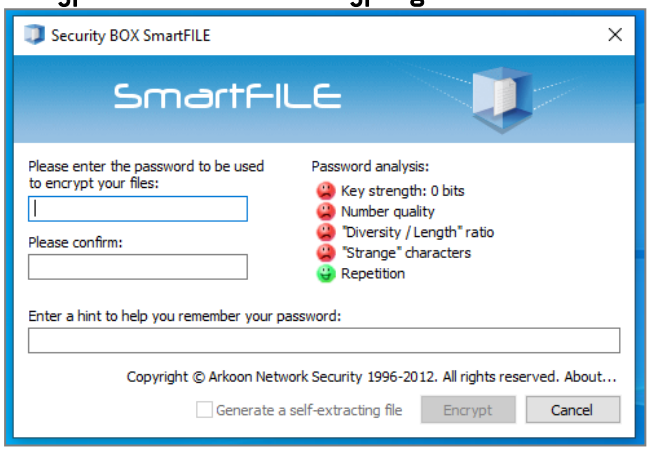
3. Where necessary, select internal recipients who will be able to decrypt the file or folder. The list of recipients is taken from your SDS Enterprise address book. For more information, see the section Managing the user address book.
4. Confirm the encryption. An *.sbox* file will be created.
5. If you have encrypted the file for recipients, send them the *.sbox* file.

This encryption mode is able to protect data up to the Restricted Distribution level.

WARNING
Ensure that you do not encrypt system files or directories.

5.4 Encrypting for recipients who do not have Stormshield Data File

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Right-click on the file or folder you want to encrypt and select **Stormshield Data Security** > **Encrypt the file to** > **Self-decrypting file**....



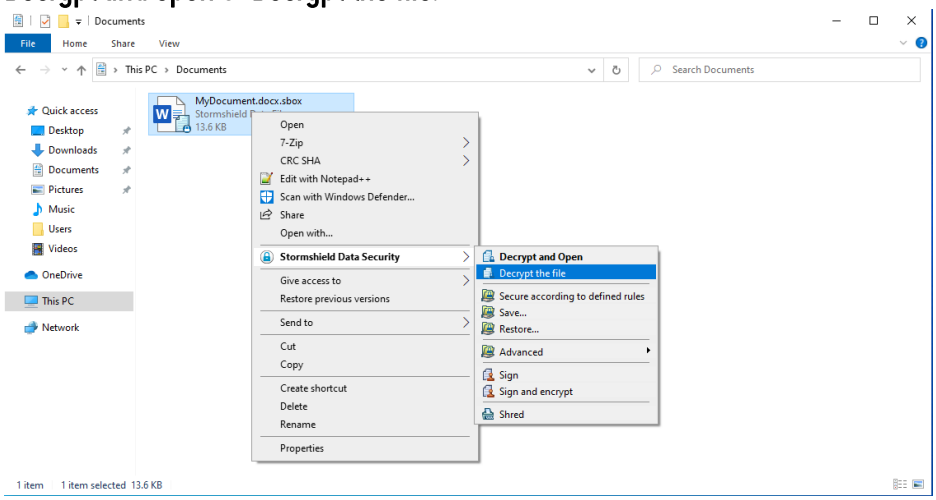
3. Enter a password in the **Security BOX SmartFILE** window, then confirm it.
4. Confirm the encryption.
5. The original file remains in plaintext and an *.exe* file will be created at the same location. Send the *.exe* file and the password to your recipients. You do not need any decryption software to open the file. However, your recipients will not be able to encrypt the file again.

This encryption mode is not suitable for protecting Restricted Distribution level data.

5.5 Decrypting files or folders

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.

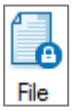
2. Right-click on the file or folder you want to decrypt and select **Stormshield Data Security** > **Decrypt and open** or **Decrypt the file**.



3. Confirm the decryption.

5.6 Modifying File settings

You can check and modify the general and advanced settings of Stormshield Data File:

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Open the **Properties** menu by double-clicking on the SDS Enterprise icon again in the taskbar.
3. Click on the 

icon.

For more information on how to use Stormshield Data File, refer to the User Guide.

6. Stormshield Data Shredder

6.1 What does Stormshield Data Shredder do?

- When you move files to the Windows recycle bin, and when you empty it, files are not really deleted from the hard disk. Stormshield Data Shredder makes it possible to permanently delete files and folders. This is an irreversible operation, the equivalent of a paper shredder.
- No IT maintenance tools will be able to retrieve deleted data.

6.2 How does Stormshield Data Shredder work?

Stormshield Data Shredder rewrites several times over the sectors of the hard disk on which deleted files are stored.

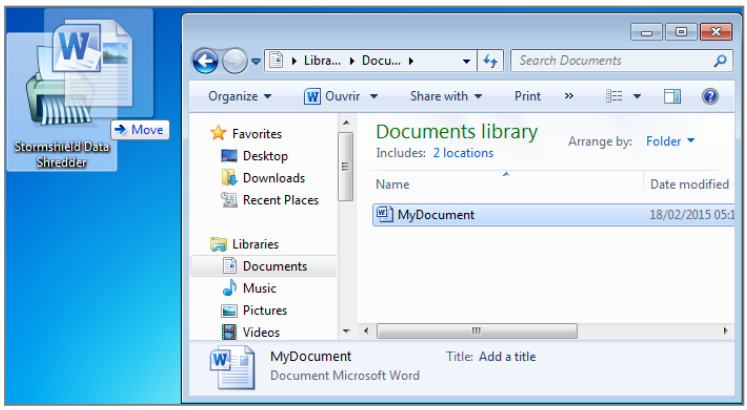
6.3 Deleting files or folders

WARNING
Stormshield Data Shredder must be used carefully, as shredded files will be irretrievably deleted from your workstation.

To irreversibly delete files or folders:

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Right-click on the file or folder you wish to delete and select **Stormshield Data Security** > **Shred**.
3. Confirm shredding.

You can also drag the files you want to delete and drop them on the Stormshield Data Shredder icon on your desktop.



6.4 Modifying Shredder settings

You can check and modify the general and advanced settings of Stormshield Data Shredder:

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Open the **Properties** menu by double-clicking on the SDS Enterprise icon again in the taskbar.
3. Click on the 

icon.

For more information on how to use Stormshield Data Shredder, refer to the User Guide.

7. Stormshield Data Sign

7.1 What does Stormshield Data Sign do?

Stormshield Data Sign makes it possible for one or several coworkers to electronically sign all types of files:

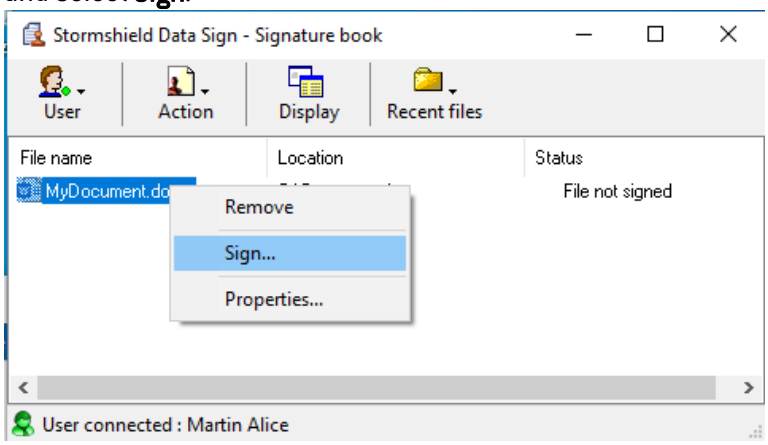
- the signature guarantees the authenticity of signers' identities and the integrity of what these files contain,
- the electronic signature can be considered as binding as a handwritten signature.

7.2 How does Stormshield Data Sign work?

- Your electronic signature is unique, as it is the combination of your private signature key and your certificate,
- 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 file is sealed, and any changes made to it after it has been signed will render the signature invalid.

7.3 Signing a file

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Right-click on the file you want to sign and select **Send to** > **Stormshield Data Sign**.
3. The Stormshield Data Sign signature book opens. In the signature book, right-click on the file and select **Sign**.

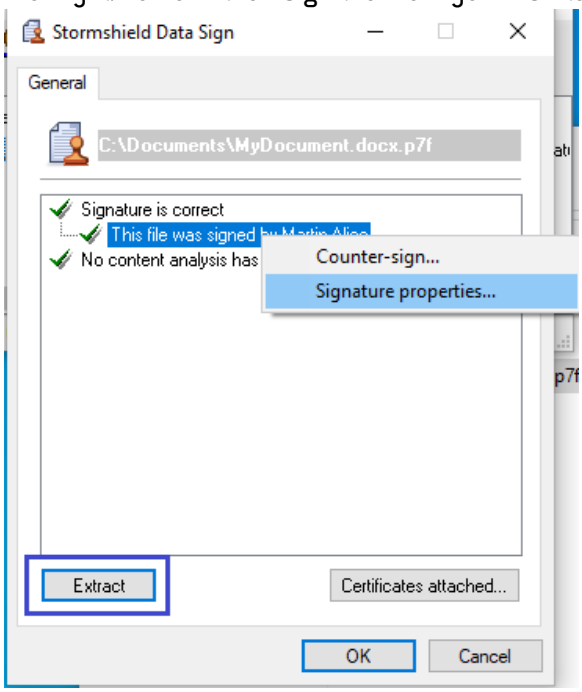


4. Complete the next few steps and click on **Finish**.
5. Enter your secret code and quit.
6. A file with the same name as the original file but with a *.p7f* or *.p7m* extension will be created at the same location. This is the file that you can send to your recipients.

7.4 Checking a signed file

When you receive a signed file from a coworker, you can check who signed the file:

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Double-click on the signed file that has a *.p7f* or *.p7m* extension.
3. The Stormshield Data Sign signature book opens. In the signature book, right-click on the file and select **Signatures**.
4. In the window that opens, you can extract the file by clicking on **Extract** if you wish to modify it. You can then sign the file if you wish to send it signed to your recipients.

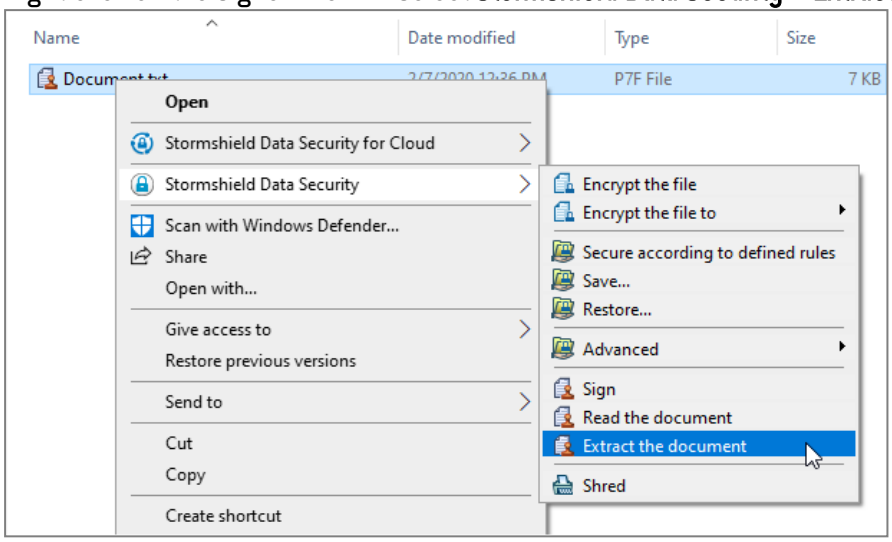


7.5 Modifying a file signed by coworkers

When you receive a *.p7f* or *.p7m* file that your coworkers signed, you must extract it before you can modify it. Then follow the procedure below:

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.

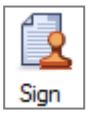
2. Right-click on the signed file and select **Stormshield Data Security** > **Extract the document**.



3. Select the location to save the document, which will be saved in its original format. You can now open and modify it, and then sign it if necessary.

7.6 Modifying Sign settings

You can check and modify the general settings of Stormshield Data Sign:

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Open the **Properties** menu by double-clicking on the SDS Enterprise icon again in the taskbar.
3. Click on the 

icon.

For more information on how to use Stormshield Data Sign, refer to the User Guide.

8. Managing the user address book

SDS Enterprise provides an address book that contains the users with whom you are likely to share confidential information.

This address book is personal and SDS Enterprise considers it trustworthy. It contains your coworkers' encryption and/or signature certificates, which are needed when secure data is exchanged.

The SDS Enterprise address book can be associated with your company's address book if it has one. In this case, it will automatically contain the list of all your coworkers.

You can also add external users to your address book.

8.1 Looking up the SDS Enterprise address book

To look up the address book and the coworkers with whom you might exchange secure files:

1. Log in to your SDS Enterprise account by double-clicking on the SDS icon in the taskbar.
2. Open the **Properties** menu by double-clicking on the SDS Enterprise icon again in the taskbar.
3. Click on the 

icon.

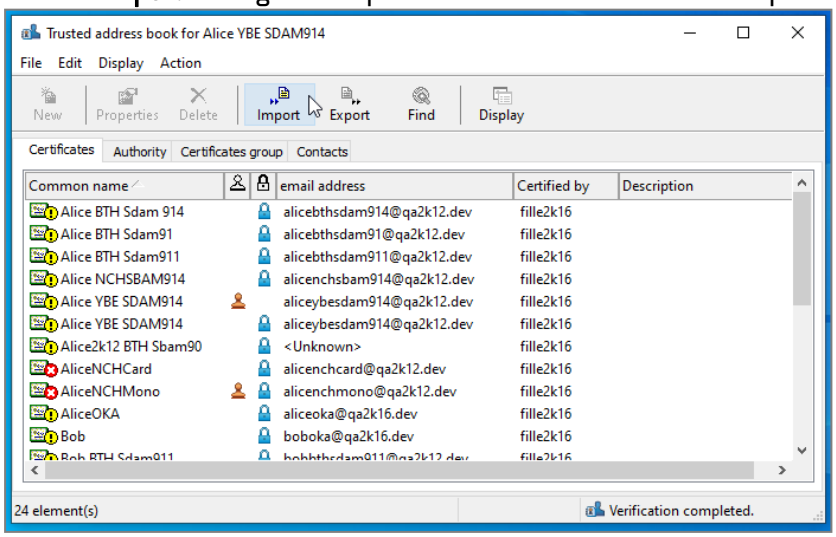
8.2 Adding external users to the address book

If you need to exchange confidential information with partners or other users who are not in your company, ask your contacts to provide you with their certificates (*.p7b*, *.p7c*, *.cer* or *.crt* file).

Ensure beforehand that the person sending you the certificate is trustworthy.

To import certificates into your address book:

1. Open your address book as shown above.
2. Click on **Import** or drag and drop the certificate and follow the steps indicated.



documentation@stormshield.eu