STORMSHIELD

GUIDE
STORMSHIELD DATA SECURITY ENTERPRISE

USER GUIDE

Version 11.3

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

Welcome to the SDS Enterprise help.

If you are an SDS Enterprise user and need help on the various features that protect your files and e-mails, refer to this help file to get started quickly with Virtual Disk, Mail, Team, File, Share, Shredder and Sign.

I'd like to:	I need to use:	
Create an encrypted virtual disk to store files safely on my workstation.	**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	**Data Mail**	
Share encrypted files with coworkers on my company's network	**Data Team**	Team
Encrypt files or folders on demand	**Data File**	File
Automatically encrypt files stored in local folders or in synchronized shared spaces	**Data Share**	
Permanently delete files from my hard disk	**Data Shredder**	Shredder
Sign files to guarantee the authenticity of their sender's identity and the integrity of their contents	**Data Sign**	Sign
Store the certificates of my contacts in an address book. These certificates make it possible to encrypt files or folders for them.	**SDS Enterprise Directory**	Address book

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

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. It 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.

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. In the Windows taskbar, search for Stormshield Data Virtual Disk.
2. Right-click in the window that opens and select **New volume**.
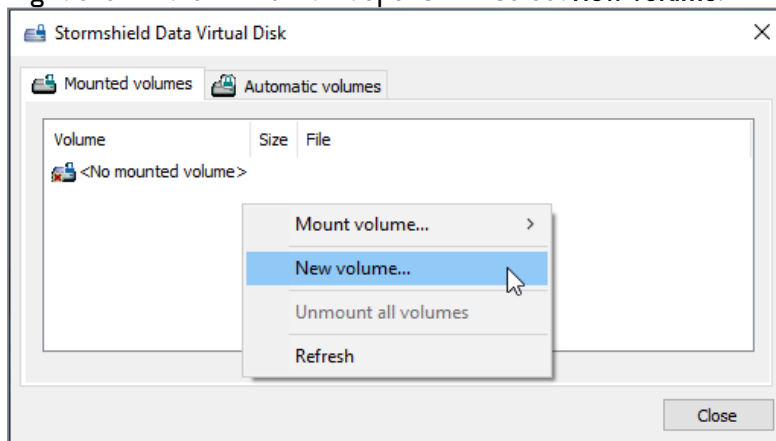
3. Click on **Browse** to name the file that will contain the virtual disk and choose its location.
4. Define the size of the disk. Do note that the size of the disk cannot be changed once it is created, so make sure that you choose the appropriate size.
5. If necessary, select the coworkers who will 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**.

6. 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.

7. 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
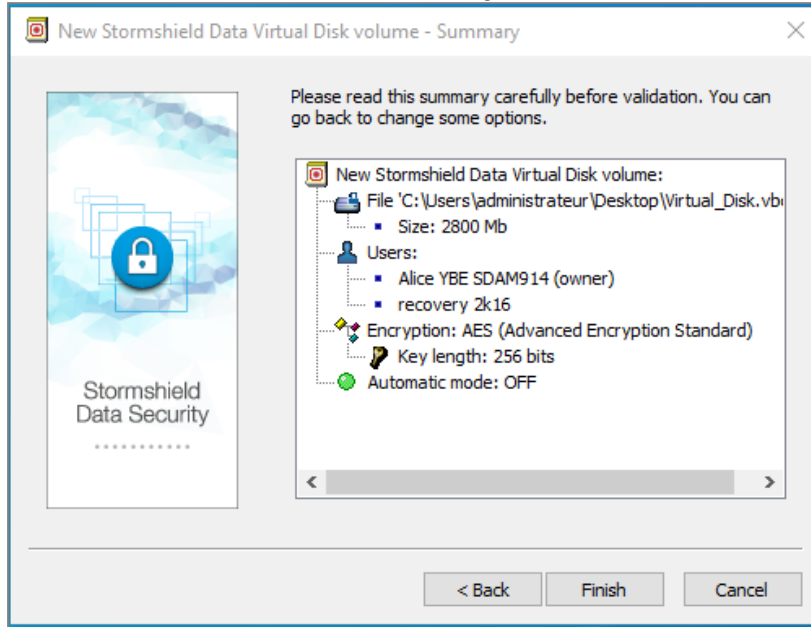
If you move a file from an encrypted virtual disk to a standard folder, it will no longer be protected and can be accessed even when you are not logged in to your SDS Enterprise account.

For more information on how to use Stormshield Data Virtual Disk, refer to the *SDS Enterprise Advanced 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.

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 Enterprise account by double-clicking on the SDS Enterprise 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. We do not support PGP e-mail signature.
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 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:
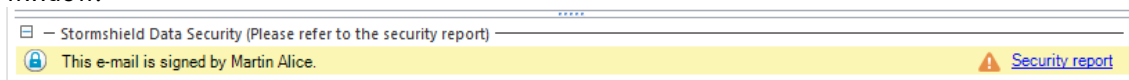
For more information on how to use Stormshield Data Mail, refer to the *SDS Enterprise Advanced User Guide*.

4. Stormshield Data Team

> ⚠️ **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.

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 stored on a removable medium.

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

> ℹ️ **NOTE**
> Stormshield Data Team cannot secure synchronized folders such as SharePoint, Dropbox, Office 365, etc.
> Use Stormshield Data Share instead to security local folders.

1. Log in to your SDS Enterprise account by double-clicking on the SDS Enterprise 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**.
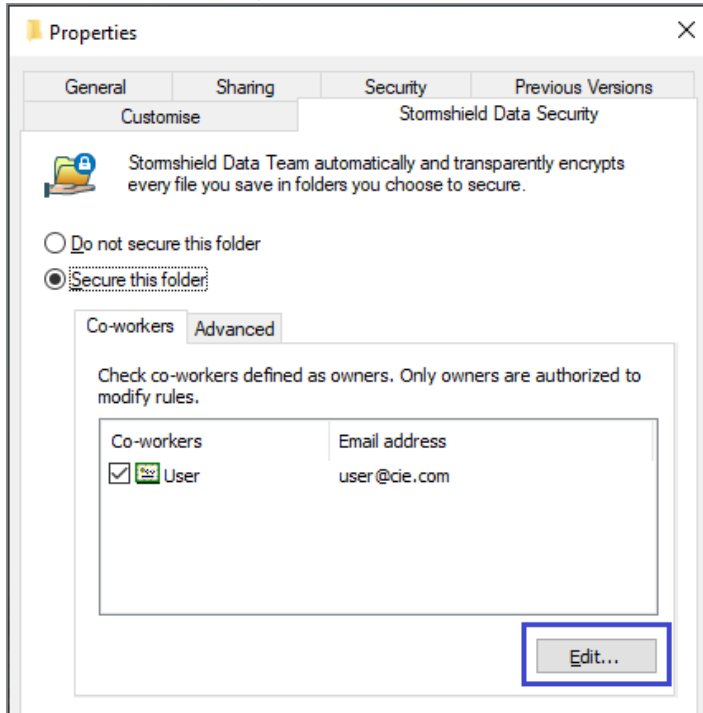
6. Select the coworkers or groups that will be able to access the folder. The list of coworkers and groups is taken from your SDS Enterprise address book. For more information, see the section Managing the user address book.

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.

For more information on how to use Stormshield Data Team, refer to the *SDS Enterprise Advanced 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?

Files or folders encrypted with Stormshield Data File in the default format *.sdsx* can be modified without being manually decrypted or encrypted. Operations are automatic and transparent.

Files or folders encrypted with Stormshield Data File in the *.sbox* format must be manually decrypted in order to be used and manually encrypted again to continue protecting them. They are then encrypted again with the default format *.sdsx*.

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 Enterprise icon in the taskbar.
2. Right-click on the file or folder you want to encrypt and select **Stormshield Data Security** > **Protect** or **Protect files**.
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 Enterprise address book. For more information, see the section Managing the user address book.
4. Confirm the encryption. By default, an *.sdsx* file will be created. According to the configuration defined by your administrator, an *.sbox* file can be created.
5. If you have encrypted the file for recipients, send them the *.sdsx* or *.sbox* file.
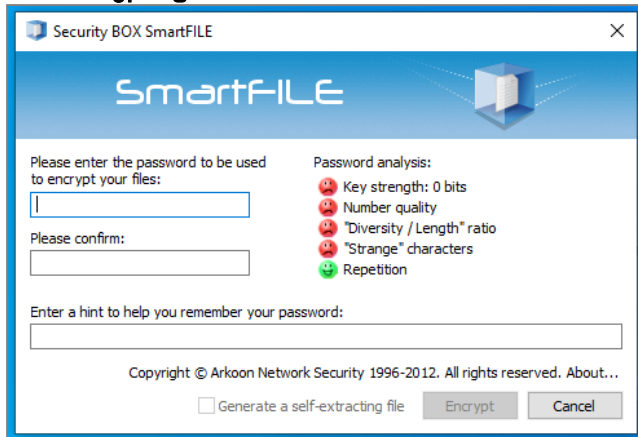
> ⚠ **IMPORTANT**
> Ensure that you do not encrypt system files or directories.

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 Enterprise icon in the taskbar.

2. Right-click on the file or folder you wish to encrypt and select **Stormshield Data Security** > **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.

5.5 Decrypting files or folders

1. Log in to your SDS Enterprise account by double-clicking on the SDS Enterprise icon in the taskbar.
2. Right-click on the file or folder you want to decrypt and select **Stormshield Data Security** > **Remove protection**.
3. Confirm the decryption.

5.6 Opening an encrypted file

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

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

6. Stormshield Data Share

6.1 What does Stormshield Data Share do?

Stormshield Data Share makes it possible to automatically encrypt files and folders saved in these folder

Folder type	Use case
Local folders on your workstation	When you regularly send encrypted files to the same group of coworkers. Stormshield Data Share makes it possible to automate encryption: all files saved in the protected folder will be encrypted for you and the coworker group without the need for any action on your part.
Collaborative workspace folders synchronized with online hosting providers OneDrive, OneDrive for Business, DropBox, SharePoint and Oodrive.	Confidential documents must be stored in synchronized shared workspaces. Stormshield Data Share makes it possible to automatically encrypt all files that you place in such spaces. You can also allow other coworkers to decrypt these files.

> **ℹ NOTE**
> Stormshield Data Share cannot automatically protect folders in shared spaces, on file servers or on removable storage media.
> Use Stormshield Data Team to secure such folders.

6.2 How does Stormshield Data Share work?

- To protect local folders:
  - Stormshield Data Share automatically encrypts files that are placed in the protected folder,
  - Stormshield Data Share automatically decrypts files in the protected folder when an authorized user needs to read it,
  - These encryption and decryption operations are transparent.
- To protect synchronized shared spaces:
  If your administrator has enabled the feature, Stormshield Data Share will detect synchronization applications installed on your workstation and automatically encrypt files that you drop there.

6.3 Automatic protection of local folders

1. Log in to your SDS Enterprise account by double-clicking on the SDS Enterprise icon in the 🔒 taskbar.
2. Right-click on the local folder that you wish to protect and select **Stormshield Data Security** > **Automatically protect folder**.
3. Where necessary, select internal recipients who will be able to decrypt the content of the folder. For more information, see the section Managing the user address book.

4. Confirm automatic protection.
   All new files and folders that are moved to this folder will now be automatically encrypted. They have the extension *.sdsx* and their icon shows a small padlock.

5. To encrypt all existing files and folders as well before enabling automatic protection, right-click on the protected folder and select **Stormshield Data Security** > **Advanced** > **Apply changes to the entire folder**.

6. If you later wish to modify the list of coworkers authorized to decrypt the folder's contents, right-click on the folder and select **Stormshield Data Security** > **Edit access**.

6.4 Encrypting files in a synchronized folder

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

2. Move your files or folder to the synchronized folder of your choice (e.g., OneDrive or 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.

3. To share access to the encrypted file with other coworkers:
   a. Right-click on the encrypted file and select **Stormshield Data Security**> **Edit access**.
   b. Search for the coworkers or groups to add and click on **OK**.
   c. Click on **OK**.

6.5 Reading or editing an encrypted file

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

2. Double-click on the file you want to decrypt.
   The file will open in plaintext.

3. If necessary, make changes to the file and save it.
   The file will automatically be saved encrypted in the folder.

6.6 Removing protection from encrypted files

1. Move the encrypted file outside the synchronized shared space or the local folder.

2. Log in to your SDS Enterprise account by double-clicking on the SDS Enterprise icon in the ![taskbar icon] taskbar.

3. Right-click on the file and select **Stormshield Data Security** > **Remove protection**.

For more information on how to use Stormshield Data Share, refer to the *SDS Enterprise Advanced User Guide*.

7. Stormshield Data Shredder

7.1 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.

7.2 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.

7.3 Deleting files or folders

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

You can also drag the files you want to delete and drop them on the Stormshield Data Shredder icon on your desktop.
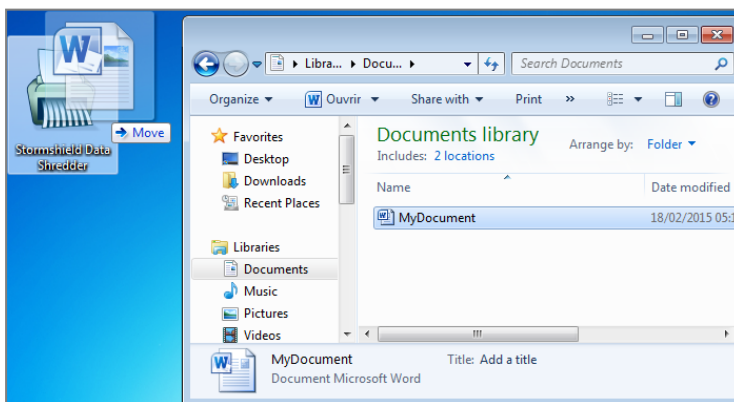
For more information on how to use Stormshield Data Shredder, refer to the *SDS Enterprise Advanced User Guide*.

8. Stormshield Data Sign

8.1 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.

8.2 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.

8.3 Signing a file

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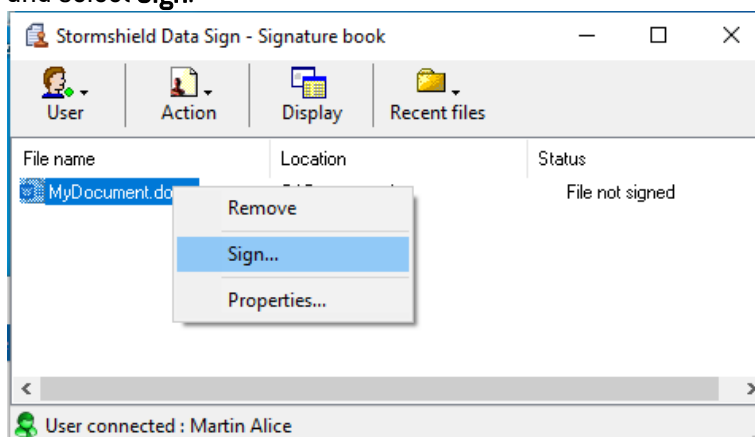

4. Complete the next few steps and click on **Finish**.
5. Enter your secret code and quit.
6. A file with the same name as the original file but with a *.p7f* or *.p7m* extension will be created at the same location. This is the file that you can send to your recipients.

8.4 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 Enterprise account by double-clicking on the SDS Enterprise icon in the ![icon] 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.
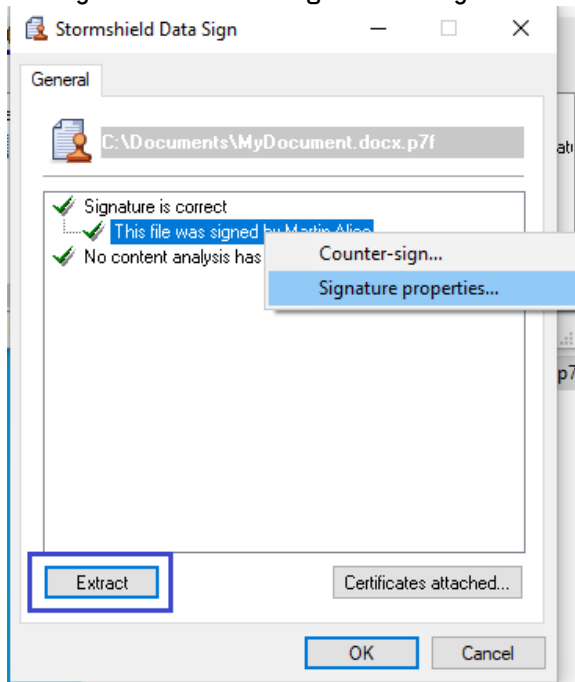
8.5 Modifying a file signed by coworkers

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 Enterprise account by double-clicking on the SDS Enterprise icon in the ![icon] taskbar.

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

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

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

9. 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.
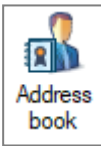
You can also add users from outside your company to your directory.

9.1 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 Enterprise icon in the taskbar.

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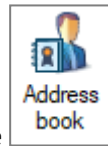
3. Click on the icon.

9.2 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.
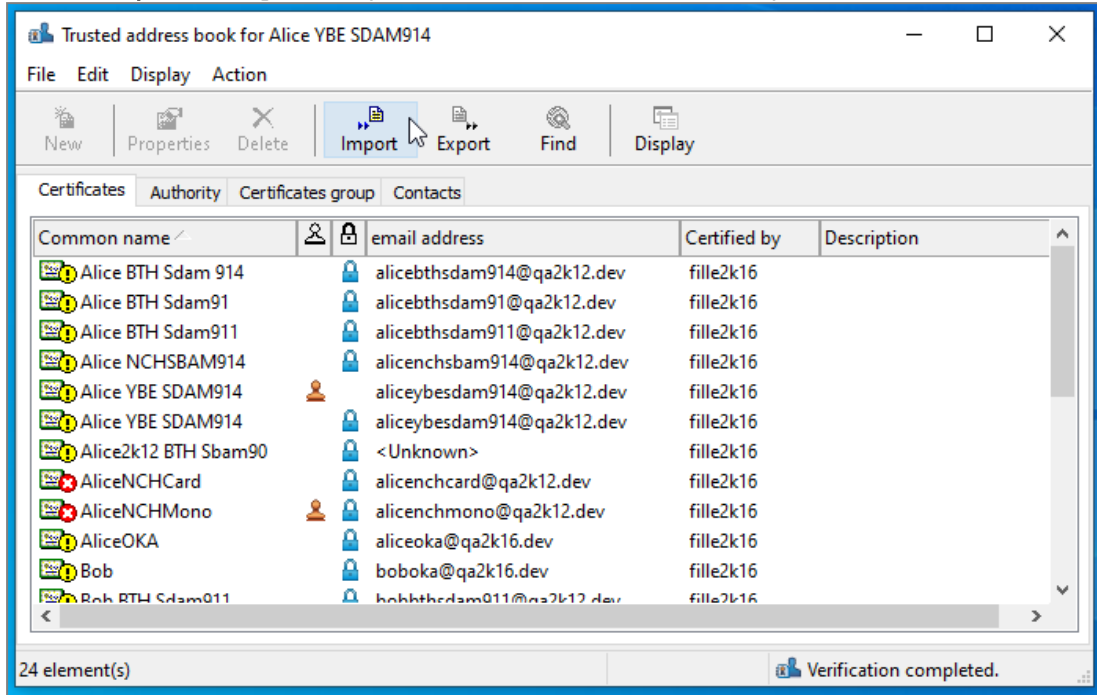
STORMSHIELD

documentation@stormshield.eu

All images in this document are for representational purposes only, actual products may differ.

Copyright © Stormshield 2025. All rights reserved. All other company and product names contained in this document are trademarks or registered trademarks of their respective companies.