GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA TEAM

Transparent and shared encryption

Version 10.1

Document last update: March 29, 2022

Reference: sds-en-sd_team-user_guide-v10

Table of contents

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

Preface

About this guide

This document provides essential information on the use of Stormshield Data Security Enterprise.

Audience

This guide is intended for:

- system administrators who want to install Stormshield Data Security Enterprise
- software users who wish to protect confidential files

1. Use environment

To use Stormshield Data Security Enterprise under the conditions of the Common Criteria evaluation and of the french qualification at standard level, it is essential to observe the following guidelines.

1.1 Recommendations on security watch

1. Regularly check security alerts provided on https://advisories.stormshield.eu/.
2. Always apply the software update if it contains a security breach correction. These updates are available on your customer area MyStormshield.

1.2 Recommendations on keys and certificates

1. RSA keys of users and certification authorities must be a minimum size of 4096 bits, with a public exponent strictly greater than 65536.
2. The certificates and CRLs must be signed with the SHA-512 algorithm.

1.3 Recommendations on algorithms

1. Stormshield Data Security supports several algorithms but recommends using AES 256, RSA 2048 and SHA 512.
2. Triple DES, RC4 and RC5 algorithms are supported too.
3. RC2 and DES algorithms are supported for compatibility but we recommend not using them because of known weaknesses.

1.4 Recommendations on user accounts

1. The user accounts must be protected by the AES encryption algorithm and SHA-256 cryptographic hash standard.
2. Passwords should be subject to a security policy preventing weak passwords.
3. Appropriate organizational measures must ensure the authenticity of templates from which the user accounts are created.
4. In case of using a hardware key ring (smart card or hardware token), this device protects the confidentiality and integrity of keys and certificates that it contains.

1.5 Recommendations on workstations

1. The workstation on which Stormshield Data Security is installed must be healthy. There must be an information system security policy whose requirements are met on the workstations. This policy shall verify the installed software is regularly updated and the system is protected against viruses and spyware or malware (firewall properly configured, antivirus updates, etc.).

2. The security policy should also consider that the workstations not equipped with Stormshield Data Security do not have access to shared confidential files on a server, so that a user can not cause a denial of service by altering or removing inadvertently or maliciously, files protected by the product.
3. Access to administrative functions of the workstation system is restricted only to system administrators.
4. The operating system must manage the event logs generated by the product in accordance with the security policy of the company. It must for example restrict read access to these logs to only those explicitly permitted.
5. The user must ensure that a potential attacker can not see or access the workstation when the Stormshield Data Security session is open.

1.6 Recommendations on administrators

1. The security administrator responsible for defining the security policy on the workstation or via Stormshield Data Authority Manager is considered as trusted.
2. The system administrator responsible is considered as trusted. He/She is responsible for the installation and maintenance of the application and workstation (operating system, protection software, PKCS#11 interface library with a smart card, desktop and engineering software. He/She applies the security policy defined by the security administrator.
3. The product user must respect the company's security policy.

1.7 Recommendations on files encryption

1. The files encryption algorithm must be AES.
2. Encrypting a file of more than 2 terabytes is not recommended. The encrypted file could be vulnerable.

1.8 Certification and qualification environment

The software modules evaluated in the context of the EAL 3+ Common Criteria Certification and of the qualification of Stormshield Data Security are:

1. The component "Transparent encryption" (Stormshield Data Team), including the definition of security rules, the encryption of files according to these rules, and the encryption of the system exchange file (swap).
2. The "Stormshield Data kernel", common to all Stormshield Data Security modules, including the authentication of the user, monitoring the inactivity of the workstation, managing a reliable certificates directory and controlling the non-recovation of used certificates.
3. The internal software cryptographic module (Stormshield Data Crypto), managing the user keys which are stored in a file (software implementation) or on a smart card.

However the following modules are beyond the evaluation scope:

1. Stormshield Data Authority Manager administration tool.
2. The possible smart card and its middleware PKCS#11.

2. Presentation

Stormshield Data Security Enterprise is a security solution for workstations running Microsoft Windows. It maintains confidentiality of data shared, stored or exchanged via email.

Stormshield Data Security Enterprise has the following security features:

- transparent encryption and real-time files
- encryption and signature of emails
- encryption of files on demand, for a transfer by mail or a secured backup
- secured and irreversible erasure of data
- electronic signature of files and folders
- encryption of virtual disks

The solution provides a tool for setting security and administration features for users and their cryptographic keys. Stormshield Data Team provides transparent encryption of your confidential files: the files are encrypted wherever they are, in real time and transparent for your business or office applications.

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

Stormshield Data Security also allows the sharing of confidential data between several co-workers. The "safety rule" specified on the folder defines the co-workers authorized to read and modify the files stored in the folder. The non-revocation of a co-worker is checked according to the defined security policy.

Stormshield Data Security can secure:

- a local folder to the personal computer of the co-worker
- removable media (USB stick) in whole or partially (one or more sub-folders)
- a shared folder on a files server

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 Security, the file or folder is created and opened in clear text.

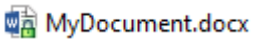
Once encrypted, a file can be read, modified or deleted only by a co-worker authorized by the security rule. All reading / writing and encryption / decryption for data are operated “on the fly” and in memory: no clear copy of the file is created.

Technically, each file is encrypted using a symmetric encryption key (AES) specific to the file. This key is encrypted with the encryption public key (RSA) of each authorized co-worker.

Stormshield Data Security also provides encryption of the swap file system in which can persist residues of confidential data.

2.1 Encryption pictograms

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

 Confidential	This indicates that a Stormshield Data Team security rule has been applied to the folder. If you are part of 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 encrypted files in this folder either. If Stormshield Data Team is not installed, you can access normally secured files and folders but existing file content is encrypted.
 MyDocument Microsoft Word Document 11.8 KB	These indicate that the file is encrypted. If you are not authorized to view or modify this file, you will not be able to open it.
 MyDocument.docx	
 MyDocument	

2.2 Cryptographic mechanisms

Stormshield Data Team implements standard cryptographic algorithms and mechanisms for the following basic operations:

- symmetric data encryption (AES)
- asymmetric encryption of encryption keys (PKCS # 1)
- key derivation from a password (PKCS # 5, PKCS # 12)
- footprint calculation (SHA-256, SHA-1)

Stormshield Data Team handles the following files management systems:

- NTFS
- FAT32
- CIFS
- DFS

Stormshield Data Team supports the following algorithms:

- AES 256, 192, 128 bits
- DES 192, 128, 64 bits

The supported algorithms and the keys size can be restricted by using Stormshield Data Authority Manager.

3. Installing Stormshield Data Team

3.1 Required configuration

For information on the required configuration of Microsoft Windows systems, refer to the section **Compatibility** of the 10.1 Stormshield Data Security Release Notes.

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

To use the Stormshield Data Team module in the most effective way, we recommend you to classify your files within a folder tree. Performance will be optimal when there are fewer files and subfolders in a folder.

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

NOTE
Stormshield Data Team does not run on a Microsoft Windows server using Citrix or Terminal Server.

3.2 Installing Stormshield Data Team

Stormshield Data Team is a Stormshield Data Security component, and as such is installed with the Stormshield Data Security suite.

To install Stormshield Data Team, you must have administrator rights and a license key, which was provided with the product purchase.

The complete install and uninstall procedures are detailed in the *Installation and Implementation guide*.

3.3 Known limitations

The following table describes the known limitations of Stormshield Data Security:

Functionalities	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, enabling version management in Windows Explorer among other things, is not supported by Stormshield Data Team.
FUS	If several Windows sessions are opened at the same time, only one user can connect to Stormshield Data Security.
Sharing a local secured directory	It is not possible to share locally a directory encrypted with the module Team.
Connection to the remote desktop	In remote desktop connection, displaying the Team properties through the contextual menu (Stormshield Data Security > Properties) of a secured file in a secured folder on a USB key generates an error.

Functionalities	Description
Synchronized directories	Stormshield Data Team cannot support synchronized directories such as SharePoint, Dropbox, Office 365, etc. and thus cannot encrypt them. We recommend you to exclude these directories form the folders analyzed by Stormshield Data Team. To exclude directories, use the variable Skipfolder which contains the list of excluded folders.

4. Common usage

4.1 Securing a folder

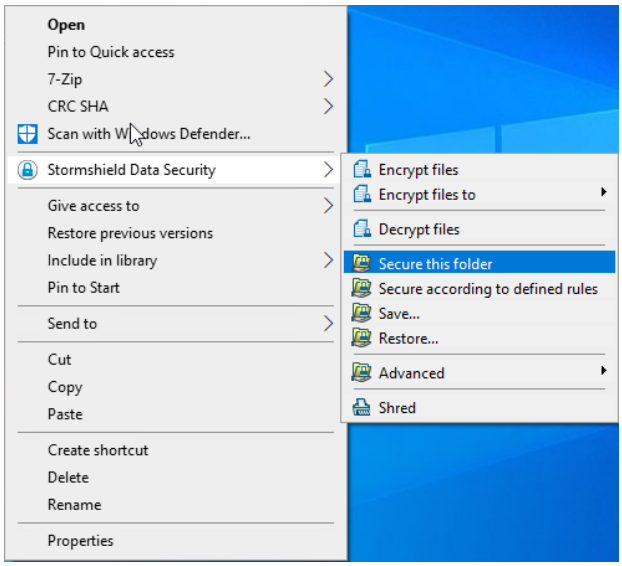
Each time you secure a folder, you define implicitly or explicitly a security rule. It is saved as part of the folder's properties. It allows making it easier to manage lists of authorized users of shared folders.

NOTE
Administrators should note that the security rules are stored in a hidden file (sboxteam.sbt). This file is visible on a machine where Stormshield Data Team is not installed. This file should not be deleted, and should be saved with the rest of the Stormshield Data Security files.

4.1.1 Securing a folder in three steps

To quickly secure a folder, without defining a security rule:

1. Select the folder to encrypt and right-click and select the Stormshield Data Security > Secure according to defined rules option as shown below.



2. Confirm your choice.

NOTE
f the user is not connected, or if the Stormshield Data Security session is locked, the connection/unlocking window is displayed. The user must identify correctly to carry on.

The folder is secured by a rule that contains only the current connected user. The files are updated and encrypted.

4.1.2 Securing a folder with a security rule

Securing a folder

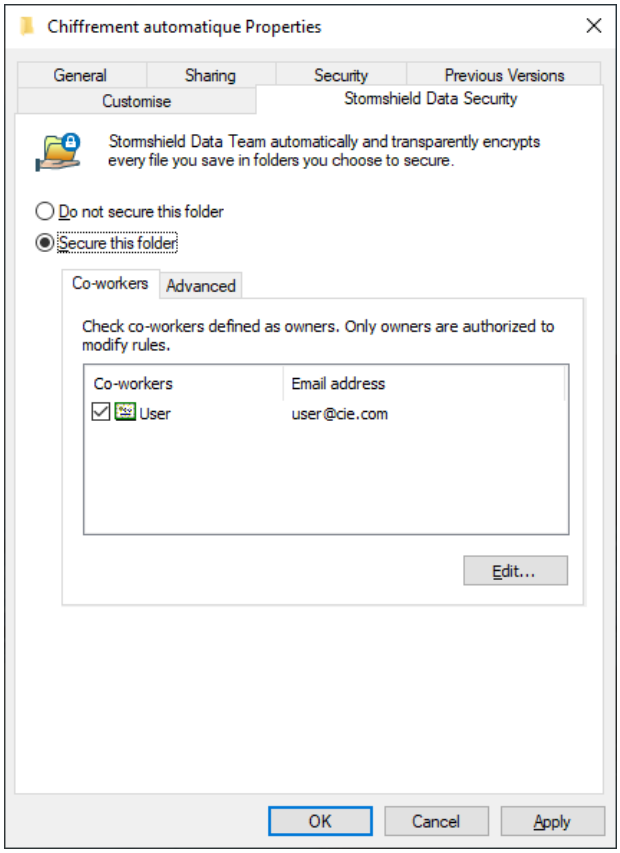
To secure a folder and define a security rule:

1. Log on to Stormshield Data Security.

For more information on logging on to Stormshield Data Security, see the *Installation and Implementation guide*.

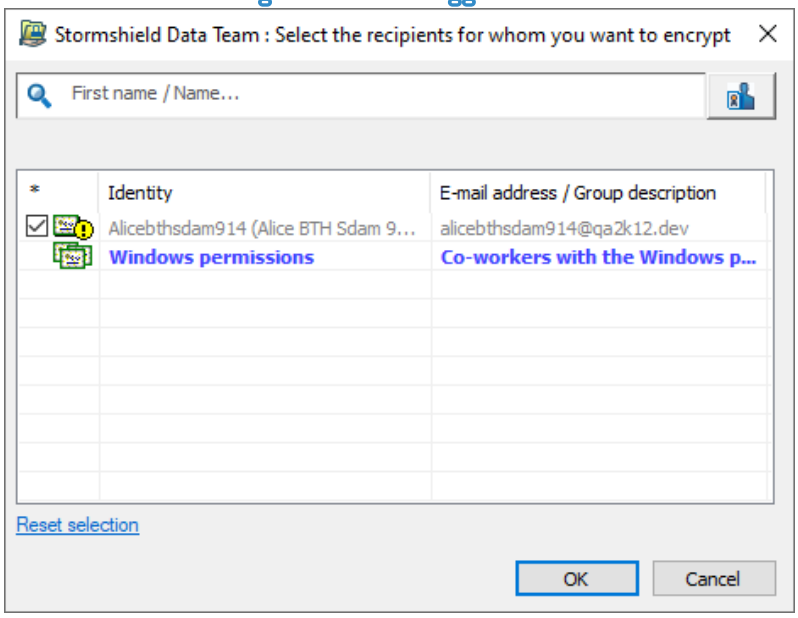
If Stormshield Data Team is installed but you are not logged on to Stormshield Data Security, you cannot create a new file in a folder protected by a rule.

2. Select the folder to be secured.
3. Right-click on the folder, and select Properties.
4. Select the *Stormshield Data Security* tab.



5. Check the option Secure this folder to encrypt this folder. All sub-folders and files in the folder will also be encrypted automatically.

6. If you need to share the folder with other users, click Edit and search for users or groups. Co-workers holding the Windows permissions on the folder concerned are automatically suggested in the Windows permissions group if the option is enabled. You can click on the group name to remove some co-workers from the group if necessary. For more information, see the section Manage automatic suggestion of co-workers.



7. Click **OK** to close the co-worker search window.
8. In the co-workers 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 authorized co-workers afterwards.
9. 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.

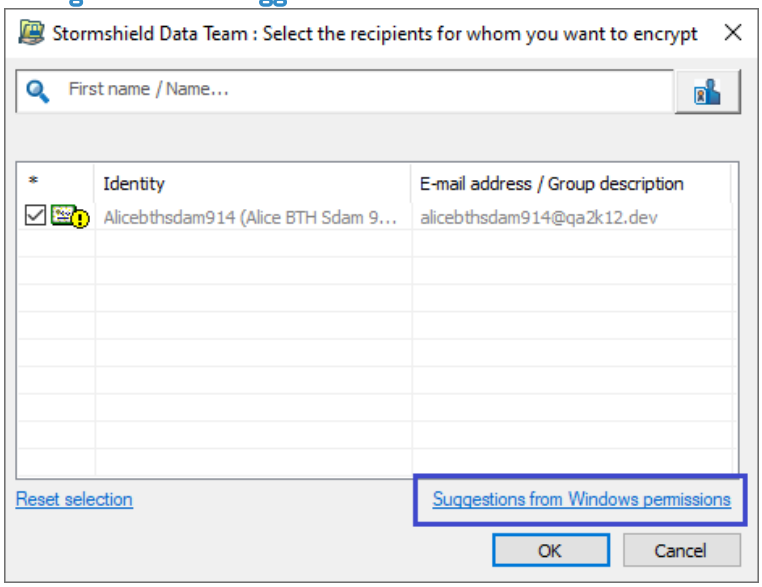
> **NOTE**
> In order to secure a folder or edit a list of authorized co-workers, users must have the certificates of all other authorized co-workers in their trusted address books.

Adding or removing co-workers from the security rule

To add or remove co-workers 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 **Co-workers** tab, click on **Edit**.

5. Search for co-workers or groups to add or remove co-workers from the list by scrolling your mouse over the line of the co-worker and clicking on the red cross.
   Click on the link **Suggestions from Windows permissions** at the bottom of the window to automatically add co-workers who hold the Windows permissions on the folder in question.
   You can click on the group name to remove some co-workers from the group if necessary.
   You will see this link only if the option is enabled. For more information, see the section Manage automatic suggestion of co-workers.



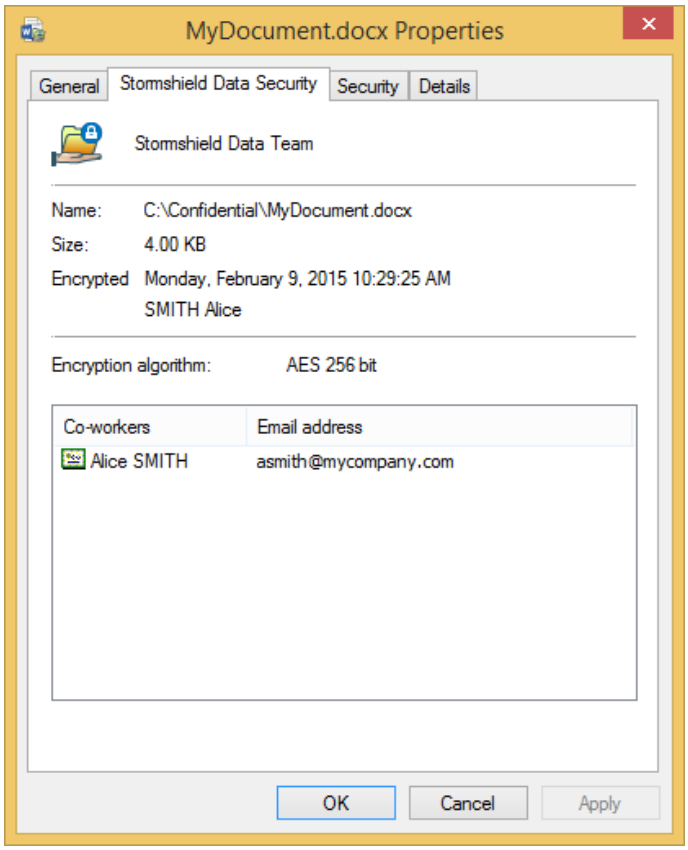
6. Click **OK** to close the co-worker search window.
7. Click OK to save and apply the rule.

4.1.3 Viewing encrypted file properties

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

NOTE

The submenu Stormshield Data Security > Properties is no longer available from Windows 10.



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

The list of authorized users is displayed only if:

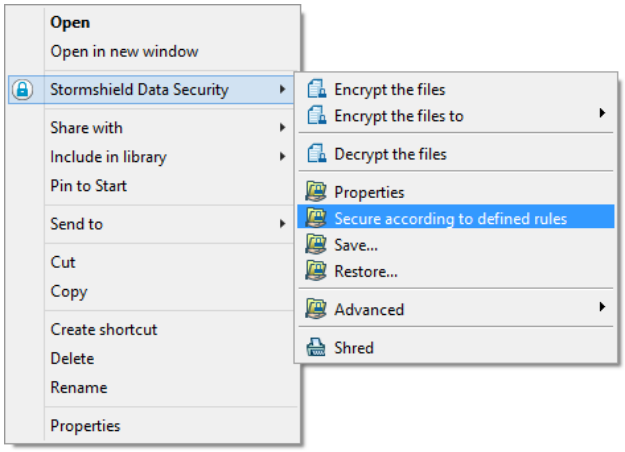
- you are connected to Stormshield Data Security.
- you are part of the authorized users' list.

4.2 Updating folder security

When you define or modify a security rule in a folder, you should apply this new rule to the folder in order to apply this new or modified rule to all the files included in the folder. Automatically, Stormshield Data Team suggests you perform this operation when you validate a rule creation/modification. However, if you reject this proposal, it is always possible to do it later.

To apply a new rule or modify 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 choose Stormshield Data Security.
3. Then select Secure according to defined rules.



NOTE

The files update will stop if you log off or lock Stormshield Data Security or your Windows session. This update automatically resumes when you reconnect to Stormshield Data Security. 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 part of the authorized co-workers	You are not allowed to access the file.
Access denied	The file is protected by Windows security rights, or the file is currently open in another program.
Process cancelled	You have stopped the current operation.

4.3 Rules and usage precautions

4.3.1 Opening an encrypted file

To view or access encrypted files in folders that have been secured, you must first log on to Stormshield Data Security.

NOTE

To access files secured by someone else, you must be part of the authorized co-workers of the rule protecting the Stormshield Data Team encrypted files. Depending on the security policy defined by your administrator, if your encryption key is revoked, the access to encrypted files is not allowed, even if you are among the authorized co-workers.

Once logged on to Stormshield Data Security (and the personal rule defined if needed) you can open and save the encrypted files with the usual applications.

NOTE
If you have not been given Windows permissions on the folder, you will get an error message when you try to open an encrypted file in a secured folder. Contact the file/folder owner.

4.3.2 Creating a new file in a secured folder

You must be logged on to Stormshield Data Security and be part of the list of authorized users in order to create an encrypted file in a secured folder. For more information on logging on to Stormshield Data Security, see the *Installation and Implementation guide*.

4.3.3 Copying or moving a file

CAUTION
Never copy or move an encrypted file into a non-secured folder, otherwise your file will be stored in clear text. If you want to move the file and keep encryption, or create an encrypted copy for backup, see section Saving an encrypted file.

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

4.3.4 Deleting an encrypted file

Only authorized users can delete an encrypted file using Windows Explorer.

When deleting a file with Windows Explorer, the encrypted file is placed in the recycle bin but remains encrypted.

4.3.5 Offline files

If you secure a folder available offline, the files are encrypted at the shared folder level on the network but also on your workstation, in the local folder in which they are copied.

4.3.6 Locking the Stormshield Data Security session

When the Stormshield Data Security session is locked, the instances of opened files remain accessible by the applications. However, the application cannot open other protected files even if other protected files are already opened. This enables applications (Microsoft Outlook for example) to remain active although the Stormshield Data Security session is locked.

For the procedure to lock the Stormshield Data Security session, see the *Installation and Implementation guide*.

4.3.7 Disconnecting the Stormshield Data Security session

When the Stormshield Data Security session is closed, the instances of opened files become inaccessible by the applications. All attempts to access protected files will return an error message. It is recommended to close all applications using protected files before closing the Stormshield Data Security session.

4.3.8 Particular cases

It is possible to have encrypted files in a folder which is not secured, or have files that are not encrypted in a secured directory. This occurs particularly in the following cases:

- when moving folders
- if the initial encryption is interrupted
- in case of backup (with the Stormshield Data Security menu) of encrypted / not encrypted file

4.4 Viewing known rules

It is possible to view all Team rules known by the Stormshield Data Security user at any time.

1. In the systray, right-click on the Stormshield Data Security icon and select Properties.
2. Select the Configuration tab.
3. Double-click the Stormshield Data Team icon.
4. Select the Security Rules tab:

The known rules list displays in the upper part of the window. Select a rule to view the list of co-workers and owners of the rule.

NOTE
If the number of co-workers on a rule is high (more than 100), displaying the co-workers list can take between five and ten seconds according to the system.

5. Advanced use

5.1 Saving an encrypted file

If you want to save an encrypted file or secured folder to a non-secured folder or on a non-protected removable storage device (USB key, CD/DVD RW), never use the Windows save or drag-and-drop feature. If you do so, your file will be stored in clear text.

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

1. With Windows Explorer, right-click on the encrypted file/folder to be saved and choose Stormshield Data Security and then Save.

It is possible to select several files or folders at once.

2. Select the destination folder. This folder must not be secured by a Stormshield Data Team rule.
3. Click OK. The selected file/folder is copied, with encryption, into the destination folder. The folder hierarchy is kept.

You do not need to be logged on to Stormshield Data Security to execute the above procedure.

NOTE
By default, Stormshield Data Security refuses to open an encrypted file stored in a non-secured folder (see Configuring Stormshield Data Team).

5.2 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 choose Stormshield Data Security and then Restore.
2. Select the destination folder; it must be a secured folder.
3. Click OK. The selected encrypted file(s) are copied into the secured folder, and remain encrypted.

5.3 De-securing a folder (decrypting)

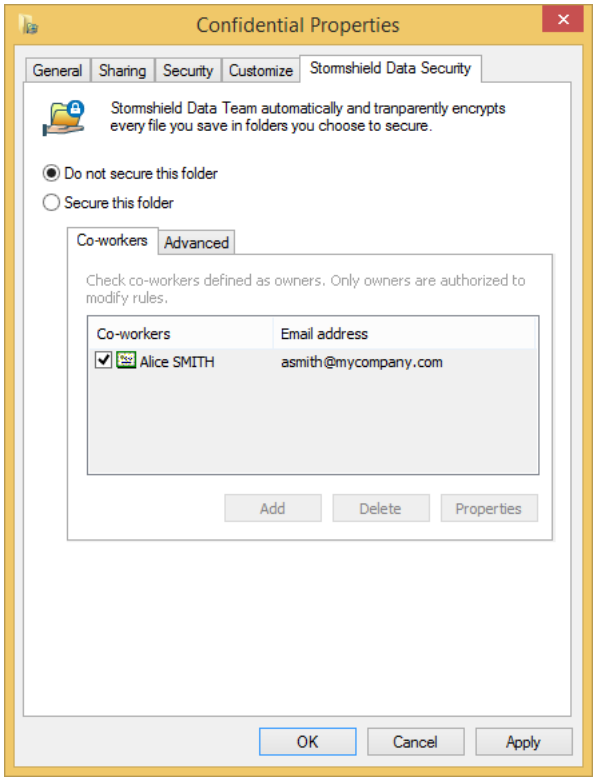
To remove the security of a folder, follow the procedure below:

1. The rule specifying that the folder contains encrypted files must first be deleted. To do so, right-click the secure folder (with the Stormshield Data Security icon), and then select Stormshield Data Security and Properties.

The properties page indicates the secure state of the folder, the co-workers allowed to access the folder and the users allowed the modify the security options (the rule owners)

2. Click Do not secure this folder and then OK.

Rule owners only are allowed to delete a rule.



3. The following window ask you to confirm. Click Yes.
4. A progress bar shows the decryption of the files being processed.

If some files have not been decrypted (for example because of an access denied), they are listed in the Details section (click Details).

5. Click Close. The security rule has been deleted and the files contained in the folder are now in plain-text mode.

5.4 De-securing files (decrypting)

It is not possible to remove the security on files contained in a secure folder. 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.

1. To remove security, in Windows Explorer, select a file or a group of files.
2. Right-click and choose Stormshield Data Security, then Advanced and then Remove security.

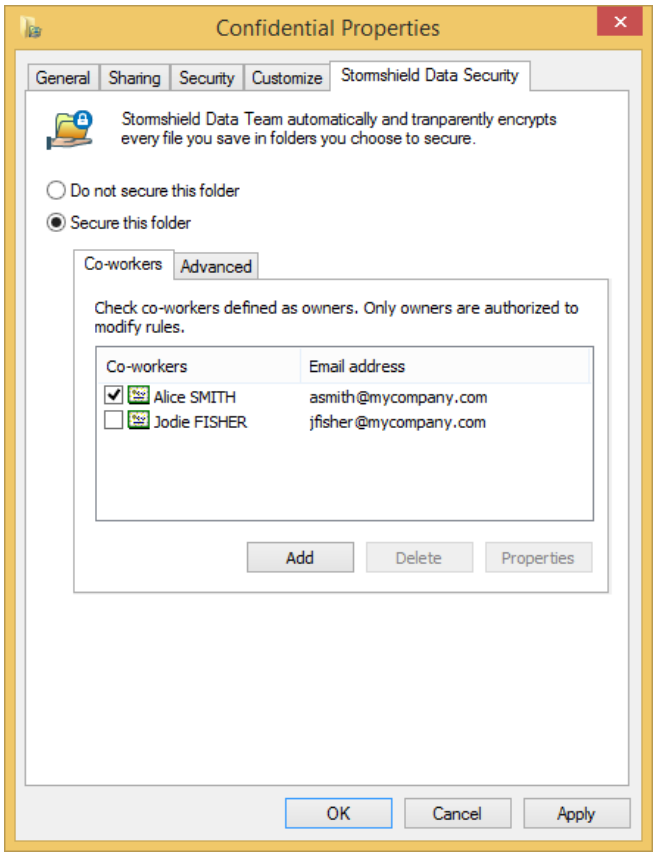
A status window displays the list of de-secured (decrypted) files.

Once a file is decrypted, its content becomes clear text, and everybody can access, read, update and delete the files.

5.5 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 outweigh the safety rules of the parent folder.

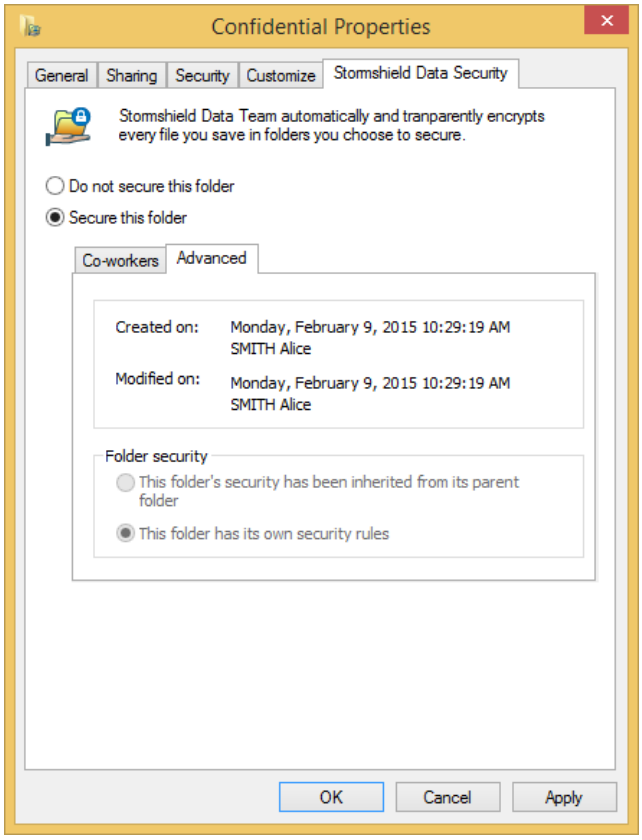
1. In Windows explorer, right click on the folder and select Properties.
2. Click on the Stormshield Data Security tab.



The list of authorized co-workers appears. The name of owners is selected.

3. If you select the Advanced tab, you will have information on the co-worker who created the rule on the folder.

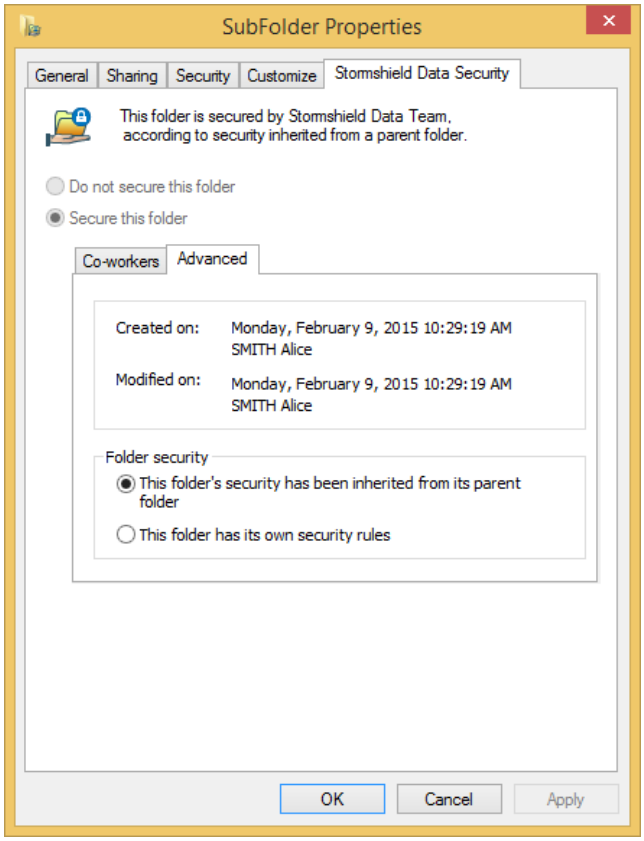
- For a root folder on which a security rule is explicitly defined, the following page is displayed:



NOTE

If you are defined as owner, you can unsecure the folder from the properties window, by selecting Do no secure this folder. For more information, see Section 5.3, "De-securing a folder (decrypting)".

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



Use the buttons of the Folder security section, you can precise if the sub-folder inherits the rules of its parent folder, or if it has its rules.

NOTE

It is impossible to have an unsecure folder within a secured folder.

- When encryption rules are defined on a folder and you are listed as an authorized user, new files you create in the encrypted folder are automatically secured, without any additional action.
- When a folder is secured, all sub-folders are by default also encrypted using the same rule. However, you can define specific rules on a sub-folder that override the security rules of the parent folder. You can also select an option so that sub-folders do not inherit the parent folder rules.
- If a secured folder is moved, the encryption rules on the folder remain the same. However, if the sub- folder is encrypted because of a parent rule, then it will not inherit the rule in the new location; rather, the existing file keeps their current encryption (even if the authorized users of the target folder are different).
- If it is moved to an un-secured location, the folder will be un-secured but the moved files will remain encrypted. If you move a non-secured folder into a secured folder, the files in the original folder will not be encrypted automatically.
- It is not possible to have a non-secured folder within a secured folder.
- You cannot encrypt the content of the following folders and their sub-folders:
- Windows folder (typicallyc:\windows) ;
- system folder (typically c:\windows\system32) ;
- program folder (typically c:\program_files).

- If you copy or move an encrypted file into a non secured folder, the file is copied in clear text. To make a secured copy of the file, see Section 4.2, "Updating folder security".
- Files can have different rules than the folder they are in. For example, Frank, Diane and Alice can have access to folder X, but only Frank and Diane can have access to a file in this folder. This happens when a modification to a rule is not applied.
- If files are already stored into a folder before a rule is defined (or if later you modify the rule) you must update the security of the files previously stored into the folder as described in Section 4.2, "Updating folder security".

5.6 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 you are not an authorized user of an encrypted file and want to delete the file, you must use the dedicated Stormshield Data Security function.

The use of this function must be allowed by the system administrator, according to security policies set when installing and configuring Stormshield Data Authority Manager

NOTE
Files deleted with the Stormshield Data Security Delete function are definitively deleted. They are not placed in the recycle bin.

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

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

5.7 Repairing a rule

A security rule is stored in a private file hidden in the folder. When you access a folder secured by a security rule, Stormshield Data Security stores in your account the content of this technical file to detect the following attacks:

- deletion of the technical file
- modification of the rule by an unauthorized third party (adding, deleting a co-worker)
- replacement of the technical file by the file of another valid rule, but provided for another folder

Some of these events can also be the consequence of an exceptional use case as the following:

- deletion of the folder
- creation of a new folder with the same name
- optionally definition of a new rule

In case of suspicion of an attack, Stormshield Data Security prohibits access to the folder concerned. To restore the 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 recopy in the folder the rule stored in your account.
4. Or click on Refresh to accept the rule set on the folder and copy it into your account.

5.8 Configuring Stormshield Data Team

Once you have installed Stormshield Data Team, you can configure some of the rule elements.

1. In the systray, right-click on the Stormshield Data Security icon and select Properties.
2. Select the Configuration tab.
3. Double-click Team icon.
4. Select the Advanced tab.

The advanced configuration options are described in the following sections.

> **NOTE**
> The advanced configuration options can be reinforced using the Stormshield Data Authority Manager administration console. For more information, refer to the documentation.

5.8.1 Close the report window

When you secure a folder (see Section 4.2, "Updating folder security") or when you save or restore files (see Section 4.2, "Updating folder security"), a list of encrypted files is displayed in a report window:

- If you choose Never, the report window will stay open; you must close it manually each time.
- If you choose Always, the report window will be displayed during processing. It will be closed automatically.
- If you choose No warning, the window will be closed automatically if no error occurs. If an error or warning occurs then it will stay open and you must close it manually.

5.8.2 Open/delete an encrypted file in a non-secured folder

Note that some applications such as Microsoft Word or Excel create a temporary file in the same folder containing the encrypted file that is opened.

> **WARNING**
> If you open an encrypted file in a non-secured folder, a temporary clear text file will be created in the folder. When you save and close the file, the temporary clear text file replaces the original encrypted file. Moreover, even if you do not save the file, the deleted temporary clear text file remains on your PC and can be recovered using specialized tools, which is a security risk.

We recommend you use Deny to ensure that encrypted files are not opened/deleted in a non-secured folder. This ensures that no temporary clear text copies are created.

If you choose Allow Read only, an encrypted file may be read and remains encrypted. Temporary files are generated and must be deleted separately.

If you choose Allow, an encrypted file in a non-secured folder can be read and updated. Temporary files are generated and must be deleted separately.

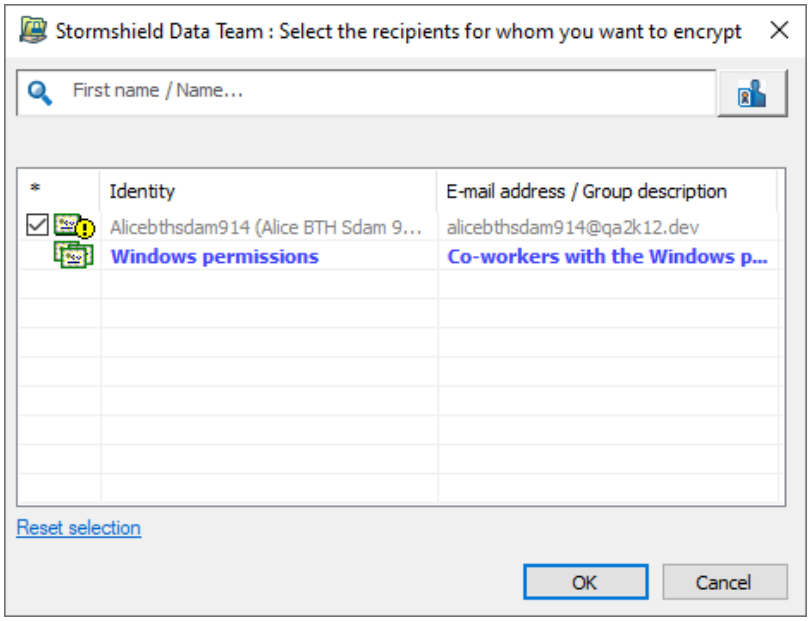
WARNING
For the selected option (Deny, Allow Read only or Allow) to be taken into account, the user must close and relaunch Stormshield Data Security.

5.9 Rules automatic update

When a co-worker's encryption key changes, all the Team rules which include their encryption certificate need to be updated. All the rules known by a user can be updated with Stormshield Data Authority Manager (refer to the Stormshield Data Authority Manager user guide). It is possible to update rules only if the user is one of the owners of the rule.

5.10 Manage automatic suggestion of co-workers

When selecting the co-workers you want to share the folder with, co-workers who hold the Windows permissions that enable accessing the folder concerned are automatically suggested in a group which name is Windows permissions.



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

- the LDAP directory must be properly configured. For more information, refer to the Stormshield Data Authority Manager guide.
- users suggested via Windows permissions must have a valid certificate in the Active Directory.

However you may want to disable this feature. You must then create the following registry key:

HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel\SuggestCoworkersThroughACL

Select the DWORD type and the “0” value.

6. Functional errors

NOTE
In the following tables, the term Log means an event has been saved in Microsoft Windows Event Logs.

Creating a file is denied	
Circumstance	You attempt to create a file in a folder on which a security rule has been defined, in one of the following cases: • you are not logged to Stormshield Data Security • you are revoked • you are not among the users authorized by the security rule
Consequence	The application is not authorized to create the file (“Access denied”). The error message depends on the application.
Log	No

Opening a file is denied	
Circumstance	You attempt to open a file in one of the following cases: • the file is in a folder on which a security rule is defined and: • you are not logged to Stormshield Data Security • you are revoked • you are not among the users authorized by the security rule • the file is encrypted and • you are not logged to Stormshield Data Security • you are revoked • you are not among the users authorized by the security rule • the file is in a non-secured folder and the security policy does not allow the opening of an encrypted file in a non-secured folder
Consequence	The application is not authorized to open a file (“Access denied”). The error message depends on the application
Log	No

Saving or restoring a file denied	
Circumstance	You save or restore one or several files in a folder on which there is no permission (managed by the system of native file).
Consequence	Copy is unsuccessful. In the report, the file appears in failure with error "Access Denied " and an error icon.
Log	Yes

documentation@stormshield.eu