GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

ADMINISTRATION GUIDE

Version 9.3

Document last update: February 4, 2021

Reference: sds-en-sds_suite-administration_guide-v9.3

Table of contents

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

Preface

About this guide

This guide provides technical information for the deployment and administration of Stormshield Data Security. It supplements the individual user manuals for the various components within the application suite. It applies to version 9.3 of Stormshield Data Security.

Audience

This guide is intended for:

- the security administrator who defines the security policy.
- the system administrator in charge of deploying and installing Stormshield Data Security.

Abbreviations

Types of accounts

The following table lists the types of accounts available in Stormshield Data Security:

KS1	password account with one key to sign and encrypt.
KS2	password account with two different keys to sign and encrypt.
GP1	password account with one key to sign and encrypt.
GP2	password account with two different keys to sign and encrypt.

Folders

The following table lists the abbreviations for the folders used in Stormshield Data Security:

ProgDir	Standard installation folder of applications. By default: C:\Program Files
InstallDir	Stormshield Data Security installation folder. By default <ProgDir>\Arkoon\Security BOX
WinDir	Windows root folder: C:\WINDOWS
SysDir	Windows system folder. By default (with Microsoft Vista, 7): <WinDir>\System32
DrivDir	Windows drivers folder. By default (with Microsoft Vista, 7): <SysDir>\Drivers
CommonFilesDir	Folder containing the common files. For example: C:\Program Files\Common Files
InfDir	Folder containing the installation and description files for drivers with Microsoft Windows. For example: <WinDir>\Inf

Windows registry root keys

The following table lists Windows registry root keys:

HKCR	HKEY_CLASSES_ROOT
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE

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 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.

1.6 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.

1.7 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. User accounts

To use Stormshield Data Security, you need user accounts. These must be set up as defined in the following sections.

2.1 Location

When connecting, Stormshield Data Security looks for the user accounts in the folder defined in the *SBox.ini* file, usually `RootPath1` folder, as described in section Section [User].

If the account is not found in RootPath1, Stormshield Data Security then looks in the `RootPath2` folder.

By default, the following folders are blank: `RootPath1 = <COMMON_APPDATA >\Arkoon\Security BOX\Users` and `RootPath2`. Refer to section Using keywords in RootPathN parameters.

`RootPath1` is the folder in which Stormshield Data Security creates new accounts. In the event of a failure, there is no fallback on `RootPath2`.

The `RootPath1` and `RootPath2` folders may be on a server share or even a USB key or any other read/write removable media.

It is therefore possible to:

- centralize the user accounts for a local network on a server
- store a nomadic user to a removable device.

> **NOTE**
> It is possible to customize the `RootPath1` and `RootPath2` parameters. Though, the specified path must match a valid tree on the workstation because the installation package only builds the default path. If the path is customized, the tree must be manually rebuilt (refer to section Naming conventions and permissions).

2.2 Naming conventions and permissions

In the `RootPath1` and `RootPath2` folders, the folder name for a user is:

- Password mode: the username
- USB cryptographic token or card: the number for their USB token or card

If the users create their account themselves, then the `RootPath1` folder must have "Full control" permission for "Everyone", which is applied to the subfolders.

On the user's own folder:

- the user must at least have "Edit" permission
- other users can have "No access"

NOTE
It is strongly recommended to block access from other users if the `RootPath1` or `RootPath2` folders are on a server, or if they are on a machine that is shared by several users.

2.3 User account files

The following table describes the files making up a user account:

<username>.usr	Main file, also called KeyStore. This file contains: • user's private keys (in password mode) • current and past certificates • kernel configuration data and the configuration data for the Stormshield Data Security applications • data for protecting other account files (encryption keys, authenticators) **NOTE** If this file is corrupted, the connection fails and returns the following error message: Your user file is not accessible.
<username>.usd	The user's trusted address book. This file contains the certificates for the correspondents and authorities trusted by the user. **NOTE** If this file is missing or corrupted, the connection fails and returns the following error message: A system component has failed to load.
<username>.bcrl	The revocation controller database, which includes for each CRL transmitter: • management data (issue date, next date, CRLNumber) • the list of revoked certificates. **NOTE** If this file is corrupt, the connection is accepted and returns the following alert message: Your personal revoked certificates database has been illegally altered. If this file is missing, the connection is accepted and returns the following alert message: Your personal revoked certificates database has been illegally deleted. A new database will be created automatically.
SBoxFileList.dec	Stormshield Data File decryption list. (1)
SBoxFileList.efp	Stormshield Data File exclusion list. (1)
SBoxFileList.enc	Stormshield Data File encryption list. (1)
SBoxFileList.cfp	Stormshield Data Shredder exclusion list. (1)
SBoxFileList.cln	Stormshield Data Shredder cleaning list. (1)

(1) For these files:

- If a list file is corrupted, then the connection is accepted, and an alert displays when the list opens: Your encryption/decryption/cleaning/protection list file has been modified without your knowledge. Would you like to load the list anyway?
- If a list file is missing, then the connection is accepted, and an alert displays when the list opens: The encryption/decryption/cleaning/protection list file cannot be found. Your list will be reinitialized.

NOTE
The account export assistant (user/assistant/account export properties) groups these files together in an installation program to enable the entire account to be copied to another workstation. More detailed information about exporting accounts is available in the *Installation and Implementation guide*.

2.4 PKCS#11 attributes for keys provided to Stormshield Data Security

If the keys are drawn by an external PKI, the following PKCS#11 attributes are mandatory:

- Private key:
  - CKA_DECRYPT
  - CKA_SIGN
  - CKA_SIGN_RECOVER
  - CKA_UNWRAP
- Public key:
  - CKA_ENCRYPT
  - CKA_VERIFY
  - CKA_VERIFY_RECOVER
  - CKA_WRAP

3. Local policies

Local policies are the operating parameters that are not specific to a user.

They may be defined in the *SBox.ini* configuration file or by group strategies (GPO).

3.1 *SBox.ini* configuration file

By default, this file is installed in the <InstallDir>\Kernel folder.

> **NOTE**
> Unicode characters are not supported by the *SBox.ini* file. As a result, the paths set up can contain ANSI characters only, except for the characters / * ? < > " | ! # @. These ones can though be used between quotes.

3.2 Configuring using Windows group policy

3.2.1 Overview

The configuration settings in the *SBox.ini* file may also be defined using the system's "Group Policy".

Depending on how it is set up, it may be at the GPO level, in the "Machine" settings, or in the "User" settings.

> **NOTE**
> It is recommended to define the local policy parameters by GPO, rather than via the *SBox.ini* file.

It is possible to generate .adm files that can be integrated into the "Group Strategy" console, making it possible to configure the options.

3.2.2 Reading priorities

Each [Section,Item] parameter is determined in the following reading order:

1. Key `HKCU\Software\Policies\Arkoon\Security BOX Enterprise\<Section>\<Item>` (the item is always in REG_SZ format).
2. Key `HKLM\Software\Policies\Arkoon\Security BOX Enterprise\<Section>\<Item>` (the item is always in REG_SZ format).
3. *SBox.ini* file

Stormshield Data Security will apply the first configuration that it finds and ignore the ones that follow. So if a parameter is configured in the HKCU folder, the HKLM folder and the *SBox.ini* file will be ignored.

3.3 References

The tables below provide information on the manageable policies:

- the third column for each parameter indicates whether it is in GPOs and in which class: MACHINE / USER. If the table cell is blank, this means that the parameter cannot be placed in GPOs.
- if an optional value in the configuration file is invalid, the default value is used.
- when changing the content of the *SBox.ini* file, we recommend you to reboot the computer to ensure that all of the changes are taken into account.

3.3.1 [Logon] section

Parameter	Description	GPO
`AllowPassword`	Authorizes a connection to Stormshield Data Security in "password" mode: • 0: not authorized (default) • 1: authorized	Machine/User
`AllowCard`	Authorizes a connection to Stormshield Data Security in "USB key or card" mode: • 0: not authorized (default) • 1: authorized	Machine/User
`AllowLocal Unblock`	Authorizes a local unlock if the user's session is blocked: • 0: not allowed • 1: allowed (by default)	Machine/User
`AllowDistant Unblock`	Authorizes a distant unlock if the user's session is blocked: • 0: not allowed • 1: allowed (by default)	Machine/User
`ConnectOnCard`	Displays the Stormshield Data Security connection window after inserting a card and entering the PIN: • 0: not displayed (by default) • 1: displayed The window only displays when there is not already a Stormshield Data Security account logged in (password or card).	Machine/User
`UnFreezeOnCard`	Displays the card unlocking window when a card is inserted and the user's Stormshield Data Security session is locked. • 0: No • 1: Yes (by default) The window is applicable only if the user logged on has a Stormshield Data Security account in card mode.	Machine/User

P10RequestEmail	Value of the "mailto:" link used at the end of a certificate request to send the request by e-mail. Basic syntax (on a single line): <Authority email address> ?subject= <Subject of the message> [&body=<accompanying message>] More detailed information on the syntax can be found in the documentation for "mailto" links. This parameter is optional. If it is blank, the user must enter the information manually.	Machine/User
P10RequestEmail CPS	Value of the "mailto:" link used at the end of a confidentiality certificate request to send the request by e-mail. Basic syntax (on a single line): <Authority email address> ?subject= <Subject of the message> [[&body==<accompanying message>] More detailed information on the syntax can be found in the documentation for "mailto" links This parameter is optional. By default, it contains only the e-mail address inscription@certif.gip-cp.fr, without a subject.	Machine/User
DontShowLicenceKey	Keeps the license key value from displaying in the About Stormshield Data Security window. • 0: The license key displays as normal. (default) • 1: The license key is not displayed. For a deployment, we recommend not displaying the license key, which is specific to the user's company.	Machine/User
DontShowPath2	Keeps the path from displaying when the RootPath2 parameter is used: • 0: displays the full account access path (default) • 1: does not display the full account access path Displaying the full path makes it easier to identify the Stormshield Data Security account used for the connection, but it has no real meaning for a standard user. This makes it very easy to distinguish between connections made with RootPath1 from those made with RootPath2.	Machine/User
SlotFilterOn	If several card or token drives are connected to the workstation (ex. a standard drive and a 3G network card), this makes it possible to use a specific drive by defining a filter for identifying it. • 0: Any drive is recognized (default) • 1: Only the drive indicated in the [SlotFilter] section is recognized by Stormshield Data Security (see section Section [SlotFilter]).	Machine/User
UpgradeEncipherCardAccount	Allows adding automatically a signature key to an encryption single-key account • 0: By default • 1: Enables the feature	Machine/User

ExternalCard Authent	Allows activating Stormshield Data Security logon window to use an external PIN-PAD when entering a PIN (card or token mode). • 0: No authentication by external PIN-PAD (value by default) ; • 1: Authentication by external PIN-PAD
LDAPVersion	Allows choosing the LDAP version to be used when connecting to the address book: • 2: version 2 used • 3: version 3 used (default)

3.3.2 [UpgradeEncipherCardAccount_CertificateTemplate] section

Parameter	Description	GPO

`UpgradeEncipherCardAccount_ CertificateTemplate`	Allows to define account certificate template. • KeyUsage Indicates the list of certificate's KeyUsages with the following syntax: KeyUsage = <Value>*(+ <Value>) où <Value> is one of the following keywords: • DS: Usage Digital Signature • NR: Usage Non Repudiation • KE: Usage Key encryption • DE: Usage Data Encryption • KA: Usage Key Agreement • CS: Usage Key Cert Sign • CR: Usage CRL Sign • EO: Usage Encipher Only • DO: Usage Decipher Only **NOTE** If the item is missing, there is no filtering on KeyUsage • ExtendedKeyUsage ExtendedKeyUsage = <EkuToken> *(, < EkuToken >) <EkuToken>= <Oid>| <EKUKeyWord> <EKUKeyWord>= clientAuth | emailProtection <oid> is the "String" representation for OID (ex: 1.3.6.1.5.5.7.3.2) **NOTE** If the item is missing, there is no filtering on extendedKeyUsage • AuthorityCommonName This item contains the commonName value for the certificate issuer: AuthorityCommonName =<CN for certificate issuer>	Machine/User

3.3.3 [SlotFilter] section

This section must be entered only when the value of the item `SlotFilterOn` in the [Logon] section is 1. If this is not the case, its contents will be ignored.

The following table describes the parameters in the [SlotFilter] section:

Parameter	Description	GPO
SlotInfoDescriptionPrefix	Indicates the prefix for the Description field from the drive slotinfo.SlotDescription at the *PKCS#11* level. For example, if the configuration data is set to SER, SERIAL will be accepted whereas USB will not. This parameter is case sensitive. If this field is blank, the data will not be filtered.	Host
SlotInfoManufacturerIdPrefix	Indicates the prefix for the <ManufacturerId> field from the drive slotinfo.ManufacturerId at the *PKCS#11* level. For example, if the configuration data is set to AX, AXALTO will be accepted whereas GEMPLUS will not. This item is case sensitive. If this field is blank, the data will not be filtered.	Host

Special characters "*" and "?" can be used with the filter to obtain more results.

3.3.4 [User] section

Parameter	Description	GPO
RootPath1	The main folder in which to look for a user account during a connection. If the account is not found in the specified folder, the system looks for it in RootPath2 (if configured). This folder can point to removable media (external drive, USB key, etc.). See section Naming conventions and permissions for the naming conventions and file permissions that may be required. This parameter is required. Value set by default at installation: <COMMON_APPDATA>\Arkoon\Security BOX\Users If this parameter is missing or invalid, it is not possible to log on to Stormshield Data Security. It is possible to use keywords for this parameter; see section Using keywords in RootPathN parameters.	MACHINE / USER
RootPath2	An additional folder in which to look for a user account. This parameter is optional. See RootPath1 above.	MACHINE / USER
ConnectPopup	In the connection window, right-clicking on the Username field can display a history of the recently connected users. • 0: The history is not displayed. (default) • 1: The history displays. This option is convenient when there are several Stormshield Data Security users sharing a single workstation so that they can more easily access their Stormshield Data Security account.	MACHINE / USER
ShowBrowse	Displays the Browse item in the history of recently logged on users. • 0: item missing (default) • 1: item present The Browse feature makes it possible to log on to accounts that are not found in RootPath1 or in RootPath2. This feature is useful for administrator workstations that access accounts in different trees. This parameter is recognized only when ConnectPopup is set to 1.	MACHINE / USER

ShowLastUsers	Number of users to display in the history. From 0 (default) to 10. If the value entered is greater than 10, it is automatically set back to 10. This parameter is recognized only when ConnectPopup is set to 1.	MACHINE / USER
HideCompletion	When the user begins to enter their username in the connection window, Stormshield Data Security can automatically complete their input with the first username in the history of connected users that begins with what the user has already entered. • 0: automatic completion activated (default) • 1: automatic completion deactivated	MACHINE / USER

Using keywords in RootPathN parameters

The RootPath1 and RootPath2 parameters can include:

- An environment variable, stated as <%Variable%>
- A keyword, specified as: <KeyWord>

The following are the keywords that are supported:

Keyword	Description
COMMON_APPDATA	The file system folder containing application data for all users. A typical path is:C:\ProgramData.
COMMON_DOCUMENTS	The file system folder that contains documents that are common to all users. A typical path is:C:\Users\Public\Documents.
DESKTOP	The file system folder used to physically store file objects on the desktop (not to be confused with the desktop folder itself). A typical path is:C:\Users\<username>\Desktop.
LOCAL_APPDATA	The file system folder that serves as a data repository for local (nonroaming) applications. A typical path is:C:\Users\<username>\AppData\Local.
MYDOCUMENTS	The file system folder used to physically store a user's common repository of documents. A typical path is:C:\Users\<username>\Documents.
PROFILE	The user's profile folder. A typical path is: C:\Users\<username>.
PROFILES	The file system folder containing user profile folders. A typical path is: C:\Users.
USERNAME	Windows username.(username)

3.3.5 [NewUser] section

The [NewUser] and [SBox.NewUserWizardExXXX] sections are for the creation of an account:

- the [NewUser] section is common to all types of new accounts;
- the [SBox.NewUserWizardExXXX] section is only for creating a XXX account, which may be KS1, KS2, GP1 or GP2 (refer to the section Abbreviations).

The table below describes the parameters of the section [NewUser]:

Parameter	Description
AllowNewUser	Creating an account: • 0: not authorized • 1: authorized (default)
CertLife	Term of validity, in years, for certificates self-generated by Stormshield Data Security. The value must be between 1 and 20. Default value: 20 years.

Key types	List of keys (type and length) to offer when creating an account. See the section called "User key types".

User key types

The supported key type (the user's private keys) is KEY_RSA_2048BITS.

The key type can be:

- 0: unauthorized
- 1: authorized
- 2: authorized and offered by default

There must therefore be only one "2" per account type, or column.

The types of keys are defined using items whose value is made up of an ordered series of 6 digits, with each digit corresponding to a type of account. The order of account types is:

KS1, KS2, GP1, GP2, RFU, CPS2 (RFU and CPS2 are not used, but these columns are required).

So, if KEY_RSA_2048BITS is the default value and KEY_RSA_1024BITS is prohibited, then it must be set up as:

- KEY_RSA_1024BITS = 000000
- KEY_RSA_2048BITS = 222222

To avoid problems to create an account if there is a configuration error in the *SBox.ini* file, the following behavior is adopted:

- If there is no default value, the strongest authorized key size is used as the default value.
- If an unexpected character is entered as the value for one of the key types, the value 0 (not authorized) is used.
- If not all characters have been entered, the missing characters to the right are treated as 0s (not authorized). For example, 111 is recognized as 111000.
- If several default values are given, the default value is the default value with the larger key size.

However, if there is no authorized algorithm for an account type, a key cannot be generated. This makes it possible, for example, to force a key to be imported from a PKCS#12 file.

3.3.6 [NewUserCard] section

This section is used to enable or disable specific functions for creating a card account.

Parameter	Description
`AllowNewUserAuto`	This parameter authorizes card accounts to be created automatically when first used on a workstation. See section Interoperability with other cards/tokens. • 0: Automatic creation not authorized (default) • 1: Automatic creation authorized

3.3.7 [SBox.NewUserWizardExXXX] sections

Parameters

The following table details the content for each section based on the account type XXX, see section Abbreviations.

Parameter	KS1	KS2	GP1	GP2	Description
AllowNewUser	•	•	•	•	Creating an account: • 0 = not authorized (default) • 1 = authorized
AllowNewUserCipher	•		•		Creating an account with a unique key, reserved for encryption: • 0 = not authorized • 1 = authorized (default)
AllowNewUserSign	•		•		Creating an account with a unique key, reserved for the signature: • 0 = not authorized • 1 = authorized (default)
MasterPath	•	•	•	•	If the <MasterKeystore> item is specified, this item contains the file containing the account template to be used for the creation. The template name is then identified by the <MasterKeystore> item below. If the <MasterKeystore> item is not set, this item contains the absolute path to the account template to be used for the account creation. Do not put a \ at the end of the item's value. If this item is missing, the account will be created with the default values (no limitation on access to parameters, no recovery certificate, no pre-set data, etc.) More information on account templates can be found in the Stormshield Data Authority Manager manual.
MasterKeystore	•	•	•	•	If the <MasterPath> item is set, this item designates the name of the file containing the account template to be used for the account creation. If this item is missing but <MasterPath>has a value, then <MasterPath> supplies the full name of the template file (see above).
NoExtractableK	•	•	•	•	At the time of creation, indicates whether the private keys are marked as not being able to be exported: • the keystore for KS1 and KS2 modes • the card in GP1 and GP2 modes • 0: No (default for KS1 and KS2 modes) • 1: Yes (default for GP1 and GP2 modes)

NoExtractableKeystoreKeys				•	This item indicates if the keys stored in a keystore for a card account can be exported or not: • 00: The keys can be exported (default). • 01: The encryption key is exportable. • 10: The signature key is exportable. • 11: No key is exportable. This parameter is useful for GP2 card accounts in which some private keys are stored in the keystore and not in the card itself.
Pkcs12Import	•	•	•	•	The new account's key (or keys) can be imported from a PKCS#12 file. • 0: No (default) • 1: Yes
DirModelIsFolder	•	•	•	•	When creating an account, Stormshield Data Security automatically imports the certificates (for the correspondents or authorities) indicated by the <DirectoryModel> • 0: <DirectoryModel> is a file (default). The extensions supported are *.cer*, *.crt*, *.p7b* and *.p7c*. The *Installation and Implementation guide* provides information about these formats. • 1: <DirectoryModel> is a folder. If so, the content from all of the certificate files (.cer, .crt, .p7b and .p7c extensions) in this folder will be imported. Do not put a \ at the end of the parameter's value.
DirectoryModel	•	•	•	•	See <DirModelIsFolder> above. This parameter is optional. If it has no value, the user's folder will not be pre-filled.

MasterPolicies	•	•	•	•	When creating an account with an account template, Stormshield Data Security copies the list files from Stormshield Data File and Stormshield Data Shredder. The integrity of these files is verified against the template account. This parameter makes it possible to remove this integrity check and then use files coming from other accounts. • 1st: List present and no associated seal in the template • 2nd: Seal present in the profile, but no list • 3rd: Seal and list present, but not matching The behavior to adopt is then defined for each case by one of the following values: • 0: Stop the process. • 1: Continue without copying the list. • 2: Continue and copy the list. Default: 000 **NOTE** The second digit cannot be 2. Example: For the value 012, this means that: • for the first digit, the list is present and the seal is not associated to the template. • for the second digit, the seal is present in the profile but there is no list. • for the third digit, the seal and the list are present but not matching.
ChangePINSO	•	•			When creating an account, Stormshield Data Security asks for a Security Officer password to be entered. This can be set with this parameter: • 0: No backup password displayed on the input page. The backup password is inactive (default for GP1 and GP2 accounts). • 1: Backup password displayed on the input page (default for KS1 and KS2 accounts).
UsrPwdMinLen	•	•			Minimum length for a password (decimal). The value must be between 0 (default) and 64. If the value entered is greater than 64, the maximum value (64) is used.
UsrPwdCharSet	•	•			Syntax: abc where “abc” are 3 uppercase hex digits (0->F), indicating the minimum number of characters in a password: • a: number of alphabetical characters • b: number of numeric characters • c: number of other characters Default: 000

`UserPinLeft`	•	•	•	•	Number of failed connection attempts before blocking an account. The number must be between 1 and 999. If the value is higher, 999 is used. Default: 3
`SOPinLeft`	•	•	•	•	Number of failed Security Officer connection attempts before blocking an account. The number must be an integer greater than 0 (no maximum value). Default: <UserPinLeft>
`InternalKeys`			•	•	In USB token or card mode (GP1 or GP2), the keys are pulled: • 0 = by Stormshield Data Security, in memory (default) • 1 = by the card **NOTE** For a generation by the card, this can be done by the card itself or in memory, depending on the manufacturer's implementation or the configuration of its PKCS#11 layer.
`ExportKeys`			•	•	If a key has not been pulled by the card or token (i.e. if <InternalKeys> = 0), Stormshield Data Security can display a window asking to save the key to a PKCS#12 file (for saving) or copy it to the user's keystore (to be exported later, see InternalKeys): • 0 = page not displayed (default) • 1 = displayed
`KeepCardObjects`			•	•	Do not destroy non-reused objects check box: • 00: box unchecked and uneditable • 01: box unchecked and accessible • 10: box checked and uneditable • 11: box checked and accessible (default)
`EnciphermentKeyInCard`				•	Put the encryption key on the card check box: • 11: box checked and accessible (default) • 10: box checked and uneditable • 01: box unchecked and accessible • 00: box unchecked and uneditable
`SigningKeyInCard`				•	Put the signature key on the card check box: • 11: box checked and accessible (default) • 10: box checked and uneditable • 01: box unchecked and accessible • 00: box unchecked and uneditable

Customizing the account creation pages

The account creation pages can be customized, for example, to automatically pre-select some parameters or even to display only the minimum elements.

This is done in the SBox.NewUserWizardExXXX sections, using the parameters defined in the following table.

Parameter	KS1	KS2	GP1	GP2	Description
ShowSaveKeyPage			•	•	Displays the page for saving keys: • 0 = page not displayed • 1 = page displayed (default) This parameter is recognized only if <ExportKeys> is set to 1.
SaveKeysInProfile			•	•	Allows (or disallows) keys to be saved to the keystore associated with the card: • 0 = check box unchecked (default) • 1 = check box checked This parameter is recognized only if <ExportKeys> is set to 1. If the <ShowSaveKeyPage> parameter is set to 0, there is no user interaction, and the save then depends on the value indicated for the SaveKeysInProfile parameter. If no value is indicated for this parameter, the default value is applied.

Customizing by key type

More advanced customization can be carried out by adding the following sections:

- [Sbox.NewUserWizardExKS1.Personal]: single-key password account
- [Sbox.NewUserWizardExKS2.Encryption]: password account for the encryption key
- [Sbox.NewUserWizardExKS2.Signature]: password account for the signature key
- [Sbox.NewUserWizardExGP1.Personal]: single-key card account
- [Sbox.NewUserWizardExGP2.Encryption]: card account for the encryption key
- [Sbox.NewUserWizardExGP2.Signature]: card account for the signature key

In addition, the parameters associated with each of these sections are:

Parameter	KS1	KS2	GP1	GP2	Description
DisableCreateSelf	•	•	•	•	Prohibits a self-certified key from being used, whether for creating an account or for renewing a key. • 0: Authorizes the use of a self-certified key (default) • 1: Prohibits the use of a self-certified key

KeyPage	•	•	•	•	Indicates whether the page for selecting the origin of the key should be displayed and the default processing to be carried out: • 0 = normal page display (default) • 1 = page not displayed and key reused (only for GP1 and GP2) • 2 = page not displayed and key created (even with the CreateForceKey parameter) • 3 = page not displayed and attached PKCS#12 imported. If importing PKCS#12 is prohibited (Pkcs12Import=0) or if keys are to be generated internally in the card (InternalKeys=1), this value cannot be used, and the page displays, as if KeyPage=0.
CreateForceKey	•	•	•	•	Specifies the key size. This parameter is used only when KeyPage=2. Authorized values are: 512, 768, 1024, and 2048. There is no default value. If KeyPage=2 and the parameter is missing or invalid, then the key origin selection page appears (as if <KeyPage>=0).
P12ImportPath	•	•	•	•	Full access path to the P12 import file. This parameter is read only when KeyPage=3. If the parameter points to a PKCS#12 file, then the specified value is shown but is not editable. Otherwise, the field is pre-populated with the parameter's value. This field is recognized only if Pkcs12Import=1.
ShowKeyCertPage	•	•	•	•	Displays the certificate page when using a PKCS#12 file or when reusing keys from a card. • 0 = not displayed • 1 = page displayed (default)
SelfCertMail	•	•	•	•	Pre-populates the e-mail address field for generating a self-signed certificate. In this field, it is possible to input: • an e-mail address • an e-mail address suffix (ex: @masociete.fr). The user can then edit and complete the value. This parameter is optional. If it is not set, the relevant field initializes as blank.
SelfCertOrganization	•	•	•	•	Pre-populates the **Organization** field for generating a self-signed certificate. This parameter is optional. If it is not set, the relevant field initializes as blank.
SelfCertOrganizationRW	•	•	•	•	**Organization** field can be edited: • 0 = field pre-populated (or blank) and uneditable • 1 = field pre-populated and editable (default)
SelfCertCity	•	•	•	•	Pre-populates the **City** field for generating a self-signed certificate. This parameter is optional. If it is not set, the relevant field initializes as blank.
SelfCertCityRW	•	•	•	•	**City** field can be edited: • 0 = field pre-populated (or blank) and uneditable • 1 = field pre-populated and editable (default)

SelfCertCountry	•	•	•	•	Pre-populates the **Country** field for generating a self-signed certificate. This parameter is optional. If it is not set, the relevant field initializes as blank.
SelfCertCountryRW	•	•	•	•	**Country** field can be edited: • 0 = field pre-populated (or blank) and uneditable • 1 = field pre-populated and editable (default)

3.3.8 [KeyRenewal] section

The [KeyRenewal] and [SBox.KeyRenewalWizardYYY] sections are for renewing keys for existing Stormshield Data Security accounts.

The [KeyRenewal] section is common to all types of accounts.

The [SBox.KeyRenewalWizardYYY] section includes the parameters specific to renewing a YYY, account key, which can be:

- KS: key renewal for a KS1 or KS2 password account
- GP: key renewal for a GP1 or GP2 card account

Parameter	Description
CertLife	Term of validity, in years, for certificates self-generated by Stormshield Data Security. The value must be between 1 and 20. Default value: 20 years.
Key types	List of keys (type and length) to offer when creating an account. The types of keys supported are defined using items whose value is made up of an ordered series of 3 digits, with each digit corresponding to a type of account. The order of account types is: KS, GP, CPS The types of keys supported and the management rules for configuration errors are the same as for an account creation, defined in the section User key types. So, if RSA 2048 bits is the default value and RSA 1024 is prohibited, then it must be set up as: • KEY_RSA_512BITS = 111 • KEY_RSA_768BITS = 111 • KEY_RSA_1024BITS = 000 • KEY_RSA_2048BITS = 222

3.3.9 [SBox.KeyRenewalWizardYYY] section

The following table details the content for each section based on the account type YYY (defined in section Section [KeyRenewal]).

Parameter	KS	GP	Description

NoExtractableK	• This item indicates if the keys stored in a keystore for a card account can be exported or not: • 00: The keys can be exported (default). • 01: The encryption key is exportable. • 10: The signature key is exportable. • 11: No key is exportable. This parameter is useful for GP2 card accounts in which some private keys are stored in the keystore and not in the card itself.
Pkcs12Import	• The new account's key (or keys) can be imported from a PKCS#12 file. • 0: No (default) • 1: Yes
InternalKeys	• In USB token or card mode (GP1 or GP2), the keys are pulled: • 0 = by Stormshield Data Security, in memory • 1 = by the card (default) **NOTE** For a generation by the card, this can be done by the card itself or in memory, depending on the manufacturer's implementation or the configuration of its PKCS#11 layer.
ExportKeys	• If a key has not been pulled by the card or token (i.e. if <InternalKeys> = 0), Stormshield Data Security can display a window asking to save the key to a PKCS#12 file (for saving) or copy it to the user's keystore (to be exported later, see InternalKeys): • 0 = page not displayed (default) • 1 = displayed
KeepCardObjects	• **Do not destroy non-reused objects** check box: • 00: box unchecked and uneditable (default) • 01: box unchecked and accessible • 10: box checked and uneditable • 11: box checked and accessible
AutomaticRenewFromCard	• With a card account, when a user's new encryption or signature key is already on the card, this option makes it possible to automatically renew the key when the previous one expires. • 0: no automatic renewal (value by default) • 1: automatic renewal with a confirmation message • 2: automatic renewal without a confirmation message **WARNING** The value 1 allows the user to decline the renewal. However, after a refusal, the update is no longer proposed. It is thus not recommended to use this value.

3.3.10 [CoworkerSelector] section

In the SD File, SD Virtual Disk and SD Team modules, searches for users in the peer selection window include by default the certificate common name.

This section is for enabling or disabling peer search on the e-mail address field in certificates:

Parameter	Description
EnableResearchByEmail	This parameter makes it possible to enable peer search on the certificate e-mail address. • 0: does not allow search on the e-mail address (by default); • 1: allows search on the e-mail address.
EmailSeparatorCharacters	This parameter specifies the characters in the e-mail address which will be considered as a space character in order to make search on this field possible. By default, the characters "-", "." and "_" will be replace with a space character. For example the address john-mark.doe@domain.com will be considered as john mark doe.

3.3.11 [Mail] section

Common parameters

The table below describes the parameters of the section [Mail] common to the different messaging software:

NOTE
These parameters are supported by Stormshield Data Mail Notes Edition. They are not supported by Stormshield Data Mail Outlook 2010 Edition and higher.

Parameter	Description
DisplayComlogWindow	Allows the Stormshield Data Security connection window to display when sending a message ("Disconnected user" mode). • 0 = The connection window appears only if the user checks the **Sign** or **Encrypt** buttons when composing a message. • 1 = The Stormshield Data Security connection window appears systematically (default). This parameter does not affect whether a user is locked.
DisplayComlogWindow UserLocked	Allows the Stormshield Data Security connection window to display when sending a message ("Locked user" mode). • 0 = The connection window appears only if the user checks the **Sign** or **Encrypt** buttons when composing a message. • 1 = The Stormshield Data Security connection window appears systematically (default). This parameter does not affect whether a user is disconnected.
AllowSendClearIf EncryptAsked	Limits the options offered to the user when a correspondent does not have a valid encryption certificate: • 0 = Prohibits the message from being sent as plain text. • 1 = The user can send the message in plain text (default).

Lotus Notes Edition

When the user sends a message, the Lotus Notes Edition of Stormshield Data Mail uses the **Sign** and **Encrypt** check boxes in the standard Lotus Notes interface to determine which security options to apply to the message. The user can no longer use the native security within Lotus Notes.

To choose between the native security in Lotus Notes and the security in Stormshield Data Security, use the following parameter to tell Stormshield Data Security to ignore the check boxes that are native to Lotus Notes:

Parameter	Description
`DoNotCheckNativeCheckBox`	Ignores the check boxes native to Lotus Notes when making a message secure • 0: Use the Notes check boxes. (default) • 1: Do not use the security check boxes that are native to Lotus Notes.

When this parameter is active, the Lotus Notes Edition of Stormshield Data Mail looks at the extra check boxes on the new message form.

- SecurityBOXMailSignOption: Indicates that Stormshield Data Mail must sign the e-mail message.
- SecurityBOXMailEncryptOption: Indicates that Stormshield Data Mail must encrypt the e-mail message for each recipients.

These new check boxes are optional. If they have not been added to the new message form (which requires a modification to the Lotus Notes database), they are treated as unchecked.

If these check boxes have been added, it is possible to keep Stormshield Data Mail from displaying the send options input window by checking the **Don't display the security options window** option in the settings for the Lotus Notes Edition of Stormshield Data Mail.

3.3.12 [CRL] section

The [CRL] section contains the parameters for the revocation controller.

Parameter	Description
`LDAPTimeOut`	Maximum time, in seconds, for downloading CRL to LDAP. Default: 30 **NOTE** This value is also used as the timeout for downloading account update files (USX file) when a user connects, but the default value for that is 25 seconds.

`HTTPTimeOut`	To define the timeout to download a CRL via HTTP.
	The syntax is:
	`[CRL]`
	`HTTPTimeOut=value in seconds`
	The value by default is: 300.

3.3.13 [external PKCS11 policy] section

The [external PKCS11 policy] section is for configuring the type of USB token or smart card (Stormshield Data Security Card Extension) accessible from menu **Windows/Start/Stormshield Data Security Enterprise**.

Parameter	Description
CPLShowExtension	Blocks the launch of the card configurator: • 0: Not displayed • 1: Displayed (default)
CPLCanChangePKCS11	Indicates whether the user can modify the USB key or card defined in the configurator. • 0: No • 1: Yes (default)
CPLForcePKCS11Label	Initial value for the name of the cryptographic module. Initial value (forced) for the name of the cryptographic module. Positioning this field and making it impossible to be modified (option `CPLCanChangePKCS11 = 0`) allows to freeze the PKCS#11 interface used by Stormshield Data Security on the workstation. Parameter by default: ;CPLForcePKCS11Label= If this parameter is not present (commented with ";"), the field is not initialized. The field must not be blocked (parameter CPLCanChangePKCS11=0) except if you want to prevent the user from accessing a card or a token. Example: `CPLForcePKCS11Label=ALADDIN eToken PRO`.
CPLPKCS11InfosEnabled	The **Information** button is activated: • 0: No • 1: Yes (default)
CPLPKCS11InfosSaveAsEnabled	The **Save As** button is activated: • 0: No • 1: Yes (default)

To be able to analyze an access problem with a user's card or token, it is recommended to leave read access (viewing information) for the parameters.

3.3.14 [File] section

The [File] section contains the Stormshield Data File parameter:

Parameter	Description
AllowTranscipheringWithDecipheredKeys	Allow to transcrypt with a decryption key. • 0: Value by default. Transcryption with a decryption key not allowed • 1: Transcryption with a decryption key allowed

Opening an encrypted FILE (*.sbox) file in a customized folder

New options allow the Stormshield Data Security administrator to configure the target directory that Stormshield Data File must use to store deciphered files when Stormshield Data File is called by other applications (Mail clients, ...).

Parameter	Description

`ExeActivate`	This parameter activates the feature to choose the target directory in which the encryption will be done. Allowed values: • 0: the feature is deactivated (default) • 1: the feature is activated If the ExeActivate option is set to 0, the parameters below will be ignored and Stormshield Data File will decipher files to the default target directory provided by the calling application.
`ExeToCheck`	This parameter allows you to configure a list of calling applications for which the custom target directory must be used to store deciphered files. If this option is not set or the list is empty, the custom target directory will be used to decipher files from any calling application. `ExeToCheck = nom_exe_1 [, nom_exe_n]`

`ExeTargetDirectory`	This parameter allows you to configure the path of the target directory where deciphered files must be stored. This option is set as follows:
	`ExeTargetDirectory = path`
	where path is the target directory path. This path can contain Stormshield Data Security tags or Microsoft Windows environment variables between < >. The list below shows sample tags :
	• COMMON_APPDATA : **C:\ProgramData**
	• COMMON_DOCUMENTS : **C:\Users\Public\Documents**
	• USERNAME : nom d'utilisateur Windows connecté.
	• LOCAL_APPDATA : **C:\Users\<username>\AppData\Local**
	• DESKTOP : **C:\Users\<username>\Desktop**
	• PROFILE : **C:\Users\<username>**
	• %ENV% où ENV est une variable d'environnement système.
	Examples : `[FILE] ExeTargetDirectory=c:\User`
	`ExeTargetDirectory=<%TMP%>`
	NOTE
	The path format must comply with standard Windows path such as: **C:\xxxx**.
	The path must not be surrounded by quotes or double quotes.

`AllowOverwriteFile`	This paramater enables to specify if it is allowed or not to overwrite files. This case can occur when the same Stormshield Data File file is opened several times. Allowed values are: :
	• 0: overwriting is deactivated. If a file, whose name corresponds either to the ciphered file or deciphered file, already exists in the target directory then the deciphering request will fail.
	• 1: overwriting is activated (default). Any file whose name corresponds either to the ciphered file or deciphered file will be transparently overwritten.
	Example of a complete configuration: `[FILE] ExeActivate=1`
	`ExeToCheck=nlnotes.exe`
	`ExeTargetDirectory=<%TMP%>\MonDossierTemporaire`
	`AllowOverwriteFile=1`
	This sample configuration defines where Stormshield Data File files are stored and deciphered when attached to a note and opened from a Lotus Notes client. The behaviour of applications other than Lotus Notes remains unmodified.

3.3.15 [Directory] section

This table describes the parameters of the [Directory] section:

Parameter	Description
`AddCertAttrInLdapFilter`	This parameter makes it possible to automatically add criterion (usercertificate;binary=*) to the LDAP search filter: • 1: adds the criterion (default) • 0: adds nothing Adding this criterion makes it possible to focus only on entries containing a certificate, which is consistent with normal use of the Stormshield Data Security address book.
`AddAsteriskSuffixInLdapFilter`	This parameter allows a '*' to automatically be added to the end of searched values (mail and cn). Therefore, if the user types dup, then the search looks for dup*, returning "dupond" and "dupont": • 1: adds the '*' character (default) • 0: adds nothing
`AddProxyAddressesInLdapFilter`	This parameter makes it possible to automatically add criterion '(proxyAddresses=smtp:xxx@yyy.zzz)' to the LDAP search filter to search by email address. Therefore, searching for a user is performed from the 'mail' field and the 'proxyAddresses' field, instead of the 'mail' field only: • 1 : adds the filter '(proxyAddresses=smtp:xxx@yyy.zzz)' (by default) • 0: adds nothing

3.3.16 [Disk] section

The [Disk] section is for configuring Stormshield Data Virtual Disk.

General parameters

Parameter	Description
`MaxVolumeSize`	Limits the volume size, expressed in MB (*.vbox*), when created by the assistant. = xxx: Size in MB (xxx MB) If blank, it can take up as much space as is available on a drive.
`DefaultVolumeSize`	Default secured volume available in the creation assistant. = xxx: default size (in MB) If missing, then the size is 10% of the volume available on the selected drive.

`MountAsRemovable`	Allows specifying if the secured volume will be considered as a removable device. • 0: no • 1: yes (default) The following limitations apply for this parameter: • If MountAsRemovable=0, images can be lost in PowerPoint 2013 and higher documents in case of disconnection/session locking. • If the volume is used through the Remote Desktop Protocol, the value 0 is mandatory. • MountAsRemovable=1 does not grant access to a recycle bin dedicated to the Virtual Disk volume.

Volume formatting data

After being created, the volumes are automatically formatted so that they may be used directly.

The parameters below represent the formatting characteristics for the volume:

Parameter	Description
`FileSytem`	File system used for the formatting: • NTFS (default) • FAT • FAT32 If the requested file system is FAT32 and the size is less than 32 MB, the formatting will be done using FAT.
`Label`	Label for the volume created. This parameter is optional. Its default value varies according to the language: • FR: "Disque sécurisé" • EN: "Secure disk"
`AllocUnit`	Size of the allocation unit: • 0: Default allocation size (default) • 512 • 1024 • 4096 This parameter may or may not be recognized, depending on the file system used for formatting (only NTFS uses it).
`QuickFormat`	Use quick formatting: • 0: No • 1: Yes (default)
`Compression`	Enable compression: • 0: No (default) • 1: Yes This parameter may or may not be recognized, depending on the file system used for formatting (only NTFS uses it).

Volume automatic creation data

There are three ways to create a volume:

- by the interactive mode
- automatically at the time of the user's first connection

This table describes the volume automatic creation parameters:

Parameter	Description
VboxFullPathName	Full name for the container file associated with the volume. This name can include the keywords specified below. This parameter is required (no value by default).
SilentSize	Size of the volume to be created, in MB. Default: 10% of the available size on the container's target unit (specified by the VboxFullPathName parameter).
AutoMount	Indicates whether the created volume is in automatic or manual mode. • 0: Manual mode • 1: Automatic mode (default)
MountLetter	Mount letter (do not put a ":" after the letter.) This parameter is optional. If this letter is not assigned, the assistant selects the next available letter in reverse alphabetic order (i.e. starting with z:).

The full name of the file associated with a volume may contain:

- An environment variable, stated as <%Path%> or
- A keyword, also expressed as <KeyWord>

The supported keywords, described in the table below, are the Stormshield Data Security username (UserId) and some Windows CSIDL values.

UserId	The user's Stormshield Data Security username
RootPath1	User account folder, specified in the *SBox.ini* file
RootPath2	Second user account folder, specified in the *SBox.ini* file
COMMON_APPDATA	The file system folder containing application data for all users. A typical path is: **C:\ProgramData**.
COMMON_DOCUMENTS	The file system folder that contains documents that are common to all users. A typical path is: **C:\Users\Public\Documents**.
DESKTOP	The file system folder used to physically store file objects on the desktop (not to be confused with the desktop folder itself). A typical path is: **C:\Users\<username>\Desktop**.
LOCAL_APPDATA	The file system folder that serves as a data repository for local (nonroaming) applications. A typical path is: **C:\Users\<username>\AppData\Local**.
MYDOCUMENTS	The file system folder used to physically store a user's common repository of documents. A typical path is: **C:\Users\<username>\Documents**.
PROFILE	The user's profile folder. A typical path is: **C:\Users\<username>**.
PROFILES	The file system folder containing user profile folders. A typical path is: **C:\Users**.
USERNAME	Windows username (username).

Creation data of a volume created at first logon

It is possible to request a volume to be created when a user first connects. The data below is specific to the first connection. The other required data comes from the automatic creation described earlier.

Parameter	Description

`CreateDiskOnFirstConnection`	Automatically creates a disk when the user first connects to their account on a workstation: • 1: Yes • 0: No (default)
`Verbose`	Displays the confirmation and reporting window: • 2: displays both windows • 1: only the reporting window • 0: no window (default) This parameter is used only when creating a volume at the time of the first connection (`CreateDiskOnFirstConnection=1`).
`CloseReportWindow`	Automatically closes the reporting window after creating the drive. • 1: Yes • 0: No (default) This parameter is used only when creating a volume at the time of the first connection (`CreateDiskOnFirstConnection=1`).

Modifying a volume's users list via the .VBOXSAVE file [Disk]

The parameters below enable the feature for modifying a volume's user list from the *.vboxsave* backup file. This feature is used for moving ownership of a volume to another user (described in the Stormshield Data Virtual Disk manual) and to perform recovery operations (see section Stormshield Data Virtual Disk).

Parameter	Description
`ModifyRescueFile`	Allows users to be modified in the backup file: • 1: Yes • 0: No (default) Depending on the value of the ExpertMode parameter, the backup file may need to be in a separate folder from the volume concerned.
`ExpertMode`	Authorizes modifications to the users in the backup file, even if they are in the same folder as the associated *.vbox* file: • 1: Yes • 0: No (default)

3.3.17 [Team] section

Opening an encrypted file not allowed if encryption key is revoked

Both default and secured modes for the access to encrypted files if the certificate of the encryption key is revoked are configured in Stormshield Data Authority Manager except this parameter:

Parameter	Description
`CheckCertificateTimeout`	• 120 (value by default): the value indicates the number of minutes between two verifications of the user's certificate of the encryption key. **NOTE** This parameter can take any positive value.

The parameter is taken into account when the user connects on the account.

Refer to the Stormshield Data Authority Manager user guide for more information.

Configuring copy or movement for a folder/file

Parameter	Description
`SecureDrag AndDrop`	The `SecureDragAndDrop` parameter enables to limit the copy or movement for folders and files with a Stormshield Data Team rule to a non-secure rule and prevents from any accidental copy or movement. It enables to specify the following features: • Blocked movement. • Encrypted movement. • By default: behaviour described in the table below. The parameter has the three following values: • 0: (by default) the behaviour is described in the table below. • 1: the action is not allowed. • 2: moving or copying does not decrypt the files. Default behaviour When dragging and dropping a file or folder from a secure folder to a non-secure folder: • A folder inheritating the parent folder security rule or a file will no longer be secured. • A folder having its own security rule will keep it, except if it is moved to another volume.

	To a non-secure folder, on the same volume	To a non-secure folder, on another volume
Dragging and dropping a file from a secure folder	Decrypted	Decrypted
Dragging and dropping a folder which security rule is inherited	Decrypted	Decrypted
Dragging and dropping a folder having its own security rule	Encrypted	Decrypted

NOTE

The `SecureDragAndDrop=2` parameter corresponds to the implementation on the the **Sign** or **Encrypt** buttons of the the **Sign** or **Encrypt** buttonsfeature from Stormshield Data Security contextual menu.

IMPORTANT

When the user is not connected, the parameter is not effective and the default behaviour is applied.

Displaying files successfully processed

Parameter	Description
`ShowSuccessful Operations`	In the monitoring screen of an encryption operation, this parameter enables to display or hide files successfully processed. In any case, files in error are displayed. • 0: only files in error are displayed (default value) • 1: all files are displayed.

3.3.18 [Sign] section

The [Sign] section contains the Stormshield Data Sign parameters.

Parameter	Description
`MailToNotifyCoworkers`	When the document signature process is ended, the user can ask the preparation of an e-mail intended to coworkers in order to notify them the document has been signed. If the document was previously signed, the recipients list is pre-filled with the co-signatories e-mail addresses. This option takes an action on the check box in the signature wizard: • 0: no (by default), the check box is not selected; • 1: yes, the check box is selected.
`MailToAskForSignature`	When the document signature process is ended, the user can ask the preparation of an e-mail intended to coworkers in order to ask them to sign the document. This option takes an action on the check box in the signature wizard: • 0: no (by default), the check box is not selected; • 1: yes, the check box is selected.
`TmpFolder`	This parameter allows specifying the directory path in which temporary files are created during co-signature and counter-signature processes. The syntax is as follows: `TmpFolder = path` where `path` is the directory path. This path can include tags (SecurityBOX tags or Windows environment variables) by writing them between <>. These tags can be: • COMMON_APPDATA: C:\ProgramData • COMMON_DOCUMENTS: C:\Users\Public\Documents • USERNAME: name of the Windows user connected • LOCAL_APPDATA: C:\Users\<username>\AppData\Local • DESKTOP: C:\Users\<username>\Desktop • PROFILE: C:\Users\<username> • %ENV% where ENV is a system environment variable Examples: [SIGN] TmpFolder=c:\User ; TmpFolder=<%TMP%> **NOTE** The format must follow the Windows requirements: C:\xxxx\. This path must not be enclosed in quotes.

3.4 Common Criteria evaluation environment

The following tables list the values of the parameters in the registry base and in the *sbox.ini* file that correspond to the secure environment which was evaluated for EAL3+ Common Criteria.

3.4.1 Registry base

Parameter	Description
`ForceGenerationKey`	Allows forcing the generation of a new encryption key each time a LibreOffice or OpenOffice file is modified. Key: HKLM\SYSTEM\CurrentControlSet\services\SboxTeamDrv\Parameters Type: DWORD Value: • 0: No new encryption key generation (default value) • 1: New encryption key generation

3.4.2 *sbox.ini* file

Section / Parameter	Objective
[Logon]	
`AllowPassword = 0` `AllowCard = 1`	Only allow card mode logon.
`GUILog = 1`	Does not allow entering a password in command line.
[NewUser]	
`AllowNewUser = 0`	Disables the local account creation when account deployment is made via a user account installation file.
`AllowNewUser = 1`	Enables the local account creation in the case of an account automatic creation in smart card mode.
[SBox.NewUserWizardExKS1] **[SBox.NewUserWizardExKS2]**	
`AllowNewUser = 0`	Disables the account creation in password mode.
[SBox.KeyRenewalWizardGP]	
`AutomaticRenewFromCard = 2`	Forces the keys renewal in smart card mode from the keys present in the card.
[External PKCS11 Policy]	
`CPLCanChangePKCS11 = 0`	Does not allow the user to modify the type of card or token.

NOTE

Parameters of the sections [DirectoryUpdate], [File] and [Team] corresponding to this environment have been moved in version 8.0.2. It is thus necessary to configure the new parameters in the user account or in the associated template to keep the same parameters after migrating in version 9.3. For more information, refer to Appendix B. Migration procedure of Security BOX Suite 6.x, 7.x, 8.0.x and 9.x to 9.3.

The following parameters were removed from the *sbox.ini* file and added to the Stormshield Data Authority Manager parameters from the 8.0.2 version.

Section / Parameter	Objective
[DirectoryUpdate]	These parameters allow to automatically update the user address book.
`Activate`	
`AllowManualUpdate`	
`55CompatibilityMode`	

Section / Parameter	Objective
StartConnection	
ReplaceFromLDAP	
ReplaceFromLDAPOnValidCert	
ReplaceFromLDAPOnOutOfDateCert	
ReplaceFromLDAPOnRevokedCert	
CommonNameRevoke	
CommonNameReplace	
CommonNameOutOfDate	
CommonNameNotOnLDAP	
DeleteIfOutOfDate	
DeleteIfRevoke	
DeleteIfNotOnLDAP	
AllowDownloadCRL	
DisableCheckOnDisplay	
Timer	
[File]	These parameters allow modifying the behavior of Stormshield Data File on files located on the network.
CanEncryptNetFile	
CanDecryptNetFile	
[Team]	These parameters allow modifying the advanced behavior of Stormshield Data Team.
AllowLocalCertificateStore	
DenyAccessOnBadCertificate	
HideDetachRule	
UpdateFileDateOnSecurityUpdate	

3.5 Windows Registry

Stormshield Data Security also supports the following parameters in the Registry:

Parameter	Description
AlternateCheckHolder	Allows taking into account a change in the identity of a certificate's holder when applying a *.usx* update file, for example when the domain name of the e-mail address has changed. The holder's identity is composed of: • Email address • Country • Organization • Organization Unit • City • Given Name • Surname • Common name Key: HKLM\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel Type: DWORD Value: • 0: the new identity is not taken into account, the *.usx* file is not applied (default value). • 1: the new identity is taken into account.
DelayUnfreezeCardMessage	Allows configuring the display time of the information message asking for the card to be inserted when a user tries to perform a cryptographic operation whereas the card account session is locked. The default display time of the message is two seconds. Key: HKLM\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Kernel\DelayUnfreezeCardMessage Type: DWORD 32 bits Value: Time between 2 and 30 seconds. Default value: 2.

4. Managing smart cards and USB tokens

This chapter describes how to set up and manage Stormshield Data Security to use a smart card or USB token.

4.1 Type of USB token or smart card used

Stormshield Data Security can use any smart card or USB token as long as its vendor provides a compatible *PKCS#11* cryptographic module (standard interface). For smart cards and tokens by vendors that have published mini drivers with Microsoft, Stormshield Data Security middleware can be used so that plug-and-play can be supported. For other smart cards, you must manually install compatible middleware.

The **USB key or smart card configurator** (from the **Windows/Start/** menu) makes it possible to define the name of the DLL in the cryptographic module to set up.**Stormshield Data Security**

This configurator knows the names of some vendors' DLLs. These names are defined in the *CardChoice.ini* file (described in the section CardChoice.ini file). This file can be completed to take into account smart cards or tokens that were not initially considered.

To enable a cryptographic module in Stormshield Data Security:

1. Run the configurator from the Windows menu.
2. Choose a type of pre-defined smart card, or define a new one (name of the vendor, and especially the name of the DLL of its *PKCS#11* interface).
3. Test this module if necessary by clicking on the **Information** button: the number of visible drives is indicated (there must be at least one).
4. Confirm your selection by clicking on **Apply** or **OK**.
5. Shut down your Windows session and open a new one to apply the change.

A smart card account can now be created or used.

To use virtual smart cards, this feature must be enabled on workstations that will be deployed with SDS. To allow SDS to use virtual smart cards, you must deploy and populate them with keys, by using an external management tool. You can then create a smart card account as you would for physical media. For more information, refer to the *Installation Guide*.

4.2 *CardChoice.ini* file

The *CardChoice.ini* file is located in the **<InstallDir>\Kernel folder**.

This file is used only by the “USB key or card type configurator”. It contains the list of cryptographic modules that are known and offered by the configurator.

The *CardChoice.ini* file consists of a manufacturer section, including:

- the DLL name for the manufacturer's PKCS#11 interface
- possible attributes for the PKCS#11 object that are not supported by the interface

The following table details the contents of a card or token type section.

NOTE
Unicode characters are not supported by the *SBox.ini* file. As a result, the paths set up can contain ANSI characters only, except for the characters / * ? < > " | ! # @. These ones can though be used between quotes.

CAUTION
To take changes into account that were made for a card or token type and to apply them to the Stormshield Data Security settings, you must do more than simply restart the system. You must:

1. Restart the UBS key or card type configurator.
2. Select the card type, if it is not already selected.
3. Confirm your selection by clicking on **Apply** or **OK**.
4. Restart the system to apply the changes.

dllname	Name (and possibly the path) for the manufacturer's PKCS#11 DLL. This parameter is required.
• `eCKA_MODIFIABLE`: CK_TRUE if the object can be modified (by default) • `eCKA_EXTRACTABLE`: CK_TRUE if the key can be extracts from the smart card • `eCKA_LABEL`: description of the key • `eCKA_MODULUS_BITS`: size of the module	Specifies the attributes not taken into account by the manufacturer's PKCS#11 interface: • 0: This attribute is managed by the manufacturer's PKCS#11 interface (default) • 1: This attribute is not handled. These settings can also be modified through the **Advanced** menu in the **Smart card or USB key configurator**.
AllSlot	Some manufacturers handle logical drives that are not possible to connect to. This parameter makes it possible to not display all of the detected slots. • 0: Only slots with an available USB token or smart card are listed (default) • 1: All of the slots are displayed.

4.3 Using several types of cards or USB tokens on the same workstation

Stormshield Data Security can use several types or cards or USB tokens on the same workstation and on the same Windows session. The contextual menu of the Stormshield Data Security notification icon in the taskbar allows switching from a type of cryptographic module to another without using the card extension configurator.

To display the menu to choose the type of card or USB token, set up first the *SBox.ini* file as follows:

- The [Logon] section must include the parameter `AllowCard=1`,
- The [External PKCS11 Policy] section must include the parameter `CPLCanChangePKCS11=1`. Otherwise, the cryptographic modules will display as grayed out even if they are available on the workstation.

- The [External PKCS11 Policy] section must include the parameter `CPLPKCS11KnownList` indicating the path of a "*CardChoice.ini*" file with read-only access for the current user.

For more information about the *SBox.ini* file sections and the available parameters, refer to the section References.

To choose a type of cryptographic module:

1. Disconnect from Stormshield Data Security.
2. Right-click the notification icon in the taskbar and select the menu **Select smart card or USB token**.
3. The list of devices available on your workstation displays. A check mark shows the *PKCS#11* cryptographic device currently used.
4. Select the module corresponding to the device you want to use in the menu. A dialog box displays. Click **Yes** to restart Stormshield Data Security and apply the changes.
5. After restarting Stormshield Data Security, double-click the notification icon to connect using the new device or right-click and select **Connect...**.

If none of the modules defined in the *CardChoice.ini* file has been detected on the workstation, the notification "No cryptographic module detected " displays when the menu **Select smart card or USB token** is selected.

If a module has been detected but could not be loaded, it will display as grayed out and selection will not be possible.

If the cryptographic module is installed after Stormshield Data Security, you must restart the Windows session to see it in the menu. Similarly, a Windows session must be restarted if a cryptographic module has been uninstalled and still displays in the menu.

4.4 Directly enabling a cryptographic module

The standard procedure for enabling a cryptographic module involves using the “USB key or card configurator”, as described in section Managing smart cards and USB tokens.

It is possible not to use the configurator, but instead to write the name of the cryptographic module DLL directly to the Windows registry (possibly including its path) under the registry key:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ARKOON\Security BOX Enterprise\Kernel\
Components\Pkix\Pkcs11CardDll=<DLL name>>
```

The operating system must then be restarted to take any changes into effect.

4.5 Interoperability with other smart cards/tokens

If several cryptographic media are connected to a workstation, you can choose the one to use when you connect to Stormshield Data Security. Do note that you must use the same reader for the connected medium for the entire duration of your Windows session.

Some peripherals include both a card reader and a smart card, such as a UMTS card with its SIM card.

However, the middleware detects the presence of such a card, even if its driver does not allow it to be used.

The [SlotFilter] section, described in section Section [SlotFilter], indicates to Stormshield Data Security which *PKCS#11* slots to check to filter for parasitic slots.

```
[Logon]
SlotFilterOn=1
```

```
[SlotFilter]
SlotInfoDescriptionPrefix= ; prefix of the "description" field
SlotInfoManufacturerIdPrefix= ; prefix of the "ManufacturerId" field
```

4.6 Automatic creation of a card account

To make it easier to deploy card accounts and to minimize actions required by the user, Stormshield Data Security 9.3 can automatically create the user's card account when the card is used for the first time.

To do this, the user simply inserts a token or smart card. Stormshield Data Security automatically detects that the user does not have an existing account associated with it and offers to create one. To continue, the user only has to enter the PIN for the card, and the Stormshield Data Security account is then created.

4.6.1 Settings

Only one type of card account may be authorized on the workstation.

- A single-key account with signature and encryption use.
- A single-key account with encryption use only.
- A single-key account with signature use only.
- A two-key account, one for encryption and one for signing.

The table below specifies the parameter combinations that are compatible with automatic creation of a card account. This function requires the use of AllowNewUserAuto parameter described in section Section [NewUserCard].

Section	Item	Value
Single-key, dual-use account		
SBox.NewUserWizardExGP1	AllowNewUser	1
SBox.NewUserWizardExGP1	AllowNewUserCipher	0
SBox.NewUserWizardExGP1	AllowNewUserSign	0
SBox.NewUserWizardExGP2	AllowNewUser	0
Single-key, encryption use account		
SBox.NewUserWizardExGP1	AllowNewUser	0
SBox.NewUserWizardExGP1	AllowNewUserCipher	1
SBox.NewUserWizardExGP1	AllowNewUserSign	0
SBox.NewUserWizardExGP2	AllowNewUser	0
Single-key, signature use account		
SBox.NewUserWizardExGP1	AllowNewUser	0
SBox.NewUserWizardExGP1	AllowNewUserCipher	0
SBox.NewUserWizardExGP1	AllowNewUserSign	1
SBox.NewUserWizardExGP2	AllowNewUser	0
Two-key account		
SBox.NewUserWizardExGP1	AllowNewUser	0
SBox.NewUserWizardExGP1	AllowNewUserCipher	0
SBox.NewUserWizardExGP1	AllowNewUserSign	0
SBox.NewUserWizardExGP2	AllowNewUser	1

WARNING
The automatic creation of a card account is not compatible with values different from 10 or 11 for parameter KeepCardObjects.

4.7 Using the card's keys

In addition to the user's current keys, other encryption keys may be placed on the card.

Stormshield Data Security automatically uses these encryption keys to decrypt documents (messages/files) when the current key cannot do it.

These keys can come from several sources:

- The user's old encryption keys. Obsolete keys may be placed on the card (with their associated certificates) to allow the user to decrypt files that were encrypted with old keys. This is particularly useful for files stored in backups.
- External keys. For example, keys for former employees that can be used to retrieve information (files/messages).

Depending on the Stormshield Data Security components, the keys on the card are not identified the same way. For some components, the keys are identified by their CKA_ID attribute (so they must always keep the same CKA_ID value), but for other components, identification is done using information from the certificate (issuer and serial number).

We recommend that keys stored on the cards always have the same CKA_ID PKCS#11 attribute and that all of the associated certificates are also present.

4.8 Renewing card data

This section provides information on renewing card data from outside of Stormshield Data Security. The data is therefore updated by a third party and is intended for use later by Stormshield Data Security.

4.8.1 Renewing certificates

When renewing certificates on the card or token, the new certificates are effective the next time the user connects to Stormshield Data Security.

When a new certificate is added to the card, the certificate object that is created must have the same CKA_ID PKCS#11 attribute as the old one.

The old certificate should not be deleted unless Stormshield Data Security has correctly recognized the new one. You can verify whether the new certificate is recognized by using the key holder on the Stormshield Data Security configuration panel.

4.8.2 Renewing keys

When renewing keys (with the associated certificate) on the card or token, the new keys are used when the old keys become obsolete or, more specifically, when their certificate becomes obsolete.

For an account with several keys (one for encryption and one for signing), the new keys are selected based on the use of the associated certificates.

The old keys (signature and encryption) should not be deleted unless Stormshield Data Security has correctly recognized the new ones. You can verify whether the new certificates are recognized by using the key-holder on the Stormshield Data Security configuration panel.

4.8.3 Reinitializing keys

Once Stormshield Data Security recognizes the new keys, the old ones can be deleted. However, we recommend you to delete only the signature key and keeping the encryption key so that you can decrypt encrypted documents (files/messages) with the old one.

If a key is deleted before Stormshield Data Security recognizes its replacement, the user will no longer be able to connect to their account.

For a single-key account (personal key), we recommend you not to delete the key on the card or token.

It is now possible to reset a card (using a tool other than Stormshield Data Security) with some new signing and encryption keys.

CAUTION
The card must contain the previous encryption private key.

To enable this feature, write the following in *SBox.ini*:

```
[Logon] RepairCardAccount=1
```

5. Creating an account from an account template

5.1 Creating an account from an account template

Stormshield Data Security can create accounts from a template, automatically integrating:

- specific configuration data
- recovery certificates
- a list of certificates preloaded in the folder

An account template consists of:

- a *.usr* file, from which the following information is copied:
- all of the configuration data: Connection, Mail, File, Shredder, LDAP folder list, revocation controller (including CRL transmitters and the custom distribution points), etc.
- all of the possible non-hidden recovery certificates
- one or more certificate files (*.cer*, *.crt*, *.p7c*, *.p7b*).
- the list files (encryption, decryption, exclusion) for Stormshield Data File
- the list files (cleaning, exclusion) for Stormshield Data Shredder

If these list files do not correspond to the "*xxx.usr*" account (which leads to an integrity error), it is possible to invalidate the integrity check by modifying the MasterPolicies parameter.

It is possible to define a different account template for each type of account: KS1, KS2, GP1, GP2; see section Abbreviations.

WARNING

Stormshield Data Security refuses to create an account in the following conditions:

- MasterPath and MasterKeystore filled in *SBox.ini*.
- DirModelIsFolder = 0
- DirectoryModel =<X:\chemin\du\fichier.(cer|crt|p7b|p7c)>
- The file indicated by DirectoryModel does not exist or cannot be accessed.

  Stormshield Data Security displays the red cross and the following message Failed to copy templates instead of the warning message.

5.1.1 The account template is located on a server

If the account template is located on a server, the file, <ImageDir>\Program Files\ARKOON\Security BOX\Kernel*SBox.ini* must contain the following items in section Sections [SBox.NewUserWizardExXXX]:

- MasterPath for the *.usr* file containing the account template
- DirModelIsFolder and DirectoryModel for the certificate file(s) to be integrated in the folder

5.1.2 The account template must be installed on the workstations

Implementation basics

If the account template must be installed on the workstations (for example, if there are isolated workstations where Stormshield Data Security was installed from a custom CD), a "masters"

subfolder containing the template accounts must be created in the same folder as Stormshield Data Security *9.3.1.msi* (<ImageDir>).

This subfolder is copied into **C:\programData\Arkoon\Security BOX**

> **NOTE**
> At the time of installation, the templates and associated file are automatically installed, and the Stormshield Data Security product and *SBox.ini* file are updated to make them effective.

Contents of the "masters" folder

In the "masters" folder, you must create subfolders corresponding to the various types of accounts ks1, ks2, gp1 et gp2 for which there are templates.

These \masters\xxx\ folders (where xxx = ks1, ks2, gp1 or gp2) must contain the following files (nothing is required, only the present files are recognized, the names must be exact):

- for a password account with only one key for signing and encryption:
  - *ks1.usr*: template keystore
  - *ks1.p7c*: list of certificates to be imported
- for a password account with two keys for signing and encryption:
  - *ks2.usr*: template keystore
  - *ks2.p7c*: list of certificates to be imported
- for a card account with only one key for signing and encryption:
  - *gp1.usr*: template keystore
  - *gp1.p7c*: list of certificates to be imported
- for a card account with two keys for signing and encryption:
  - *gp2.usr*: template keystore
  - *gp2.p7c*: list of certificates to be imported

For a given account type, there can be only one account template. If several account templates are required, then it is necessary to generate an image of the installation procedure for each template.

The template folders can also include the Stormshield Data File and Stormshield Data Shredder list files. Each of the folders must have the following files:

- *SBoxFileList.dec*: Stormshield Data File decryption list
- *SBoxFileList.efp*: Stormshield Data File exclusion list
- *SBoxFileList.enc*: Stormshield Data File encryption list
- *SBoxShrdList.cfp*: Stormshield Data Shredder exclusion list
- *SBoxShrdList.cln*: Stormshield Data Shredder cleaning list

> **NOTE**
> This procedure is automatic when using the Stormshield Data Authority Manager customization package.

5.2 Automatic creation of a volume at first logon

It is possible to automatically create a Stormshield Data Virtual Disk volume when the user logs on for the first time, according to the following principles:

- no question is asked to the user, except a confirmation
- the creation parameters are read in *SBox.ini*, section [Disk]
- the process integrates the formatting (silent) of the created volume

The creation can take a considerable time: a progress bar is displayed to make the user wait.

Refer to the section called "Creation data of a volume created at first logon" to find the volume creation data.

6. Advanced features

This chapter contains all of the technical information (tips, limitations, and warnings) about the Stormshield Data Security components.

6.1 General information for all Stormshield Data Security applications

6.1.1 Fast User Switching

Stormshield Data Security 9.3 is not compatible with the Fast User Switching feature.

6.1.2 Automatic backup copies

With each successful connection, Stormshield Data Security makes a backup copy (*.bak*) of the keystore (*.usr*), folder (*.usd*) and revocation database (*.bcrl*) files.

If the user account is blocked (after entering several [3 by default] consecutive incorrect codes) or if the account is corrupted, it must be restored from its last backup copy. Do the following in the folder containing the user account:

1. Rename the *.usr*, *.usd*, and *.brcl* files.
2. Make a backup copy of the files *.usr.bak*, *.usd.bak*, and *.brcl.bak*.
3. Delete the *.bak* extension from the files *.usr.bak*, *.usd.bak*, and *.brcl.bak*.

The user account is then reset to how it was at the time of the last successful connection.

6.2 Events log

Stormshield Data Security has an events log mechanism enabling the administrators to monitor the defined security environment and identify incidents taking place while the product is used.

6.2.1 Introduction

All the events related to Stormshield Data Security can be accessed via Windows event viewer. Data can be read and analyzed and once the problem has been found, a solution can be determined thanks to the provided information.

Types of messages

The error messages generated can be of three different types:

- Information messages: a simple informational message that does not involve security or require corrective action.
- Warnings: an indication that signals a potential problem to the administrator.
- Errors: a serious problem that prevents the configuration from being deployed successfully on the appliance.

Detail of logged information

The logs allow to display the following information:

- Type of message: information, warning or error (see sectionTypes of messages).
- Date: date at the moment the message has been generated.

- Time: time at the moment the message has been generated.
- Source: source from which the event has been generated.
- Category: short description of the event source.
- Event: number corresponding to the type of generated message.
- User: Stormshield Data Security user name.
- Computer: computer name (NetBIOS).

6.2.2 Configuring the events log

During a new installation of Stormshield Data Security, the events logs are deactivated by default. To activate them, it is necessary to modify the registry parameters related to the various categories of events and allow to find or not a type of events.

The procedure is done via the GPO manager (*gpedit.msc*). The logs can be accessed via Windows Event Viewer. Also, they can be sent to a remote server, for example the Stormshield Visibility Center server, the monitoring solution of Stormshield.

Configuring Group Policy Object

Microsoft Windows GPO uses *.admx* files for the configuration parameters and *.adml* language files, where all the texts related to these parameters are referenced.

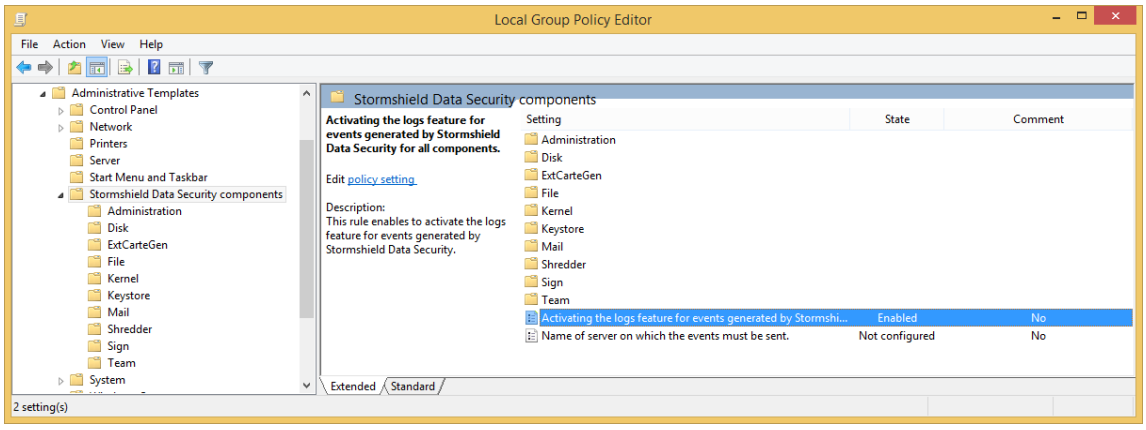
The installation of Stormshield Data Security places:

- the *Sbsuite.admx* file in the *%SystemRoot%\PolicyDefinitions* folder
- the *Sbsuite.adml* language file in the *%SystemRoot%\PolicyDefinitions\en-US* folder.

These files are automatically uploaded when launching gpedit and it is not necessary to upload them.

1. Launch gpedit (**Start > Execute >** then enter *gpedit.msc*).
2. Click on **Administrative Templates > Stormshield Data Security components**. The **Activating the logs feature for events generated by Stormshield Data Security for all modules** entry enables to start the events generation once it has been activated. The other entries allow you to configure more precisely the events generation.

A direct change of the group policy modifies the corresponding values in the registry database. They apply to all users. They can be found under the key HKEY_CURRENT_USER in the registry base. However, a group policy (specified remotely by Active Directory) takes priority over changes made locally.



IMPORTANT

The feature **Activating the events logs for Stormshield Data Security Administration components** is a general parameter: if deactivated, no event will be generated, whatever the parameter for the modules. Moreover, a "non configured" module is active if the general parameter is activated.

For example, if you want to activate the events for the Virtual Disk module only:

1. Activate the events logs feature for all modules.
2. Activate the events logs feature for the Virtual Disk module.
3. Deactivate the feature for all other modules.

Viewing logs in Stormshield Visibility Center

To configure event logging on the Stormshield Visibility Center, refer to the SVC *Administration guide* available on the Stormshield Technical Documentation website.

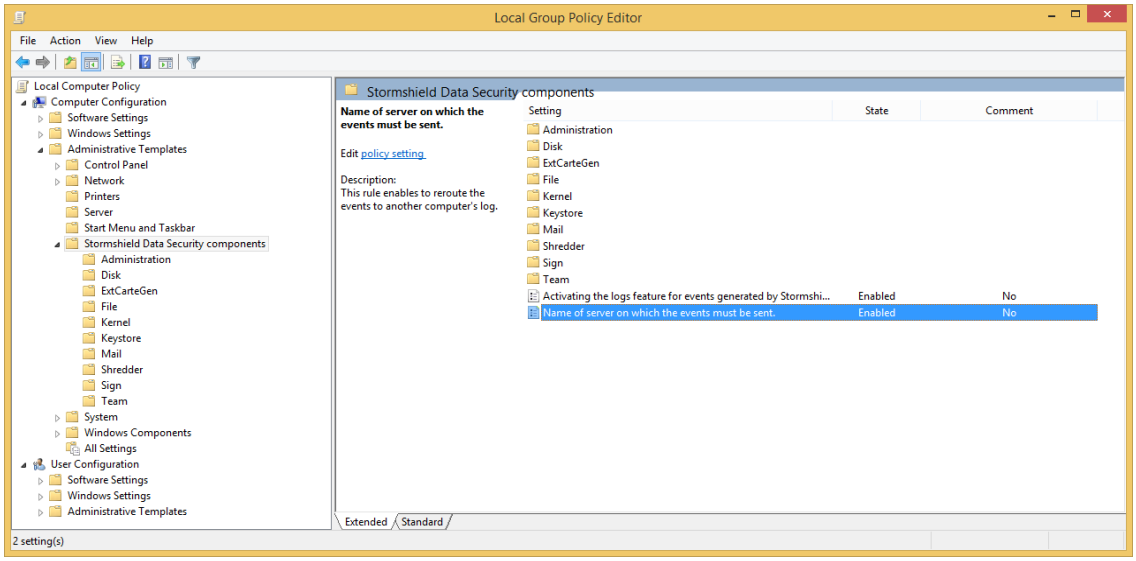
Viewing logs on another remote server

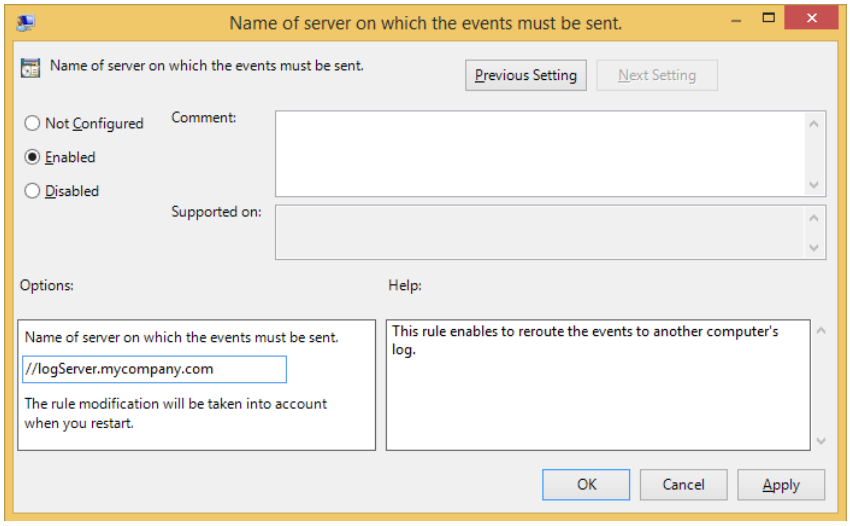
It is possible to configure event logging on a remote server other than SVC in order to centralize logs.

You have to configure the collecting server and the workstations issuing logs to authorize events logging and reception. A detailed description is available on the Microsoft website (https://msdn.microsoft.com/en-us/library/cc748890.aspx).

After configuring the computers, you need to define the remote server to which Stormshield Data Security will send events in the Group Policy Object Editor (*gpedit.msc*):

1. Launch gpedit (**Start** > **Execute** > then enter *gpedit.msc*).
2. Click on **Administrative Templates** > **Stormshield Data Security components**. Enable the option **Name of server on which the events must be sent** and enter the remote collecting server address.





6.2.3 Using the events log

Any action operated by Stormshield Data Security is listed in the events logs following the same criteria (see the section called "Types of messages"). The events can be viewed from Windows Event Viewer.

6.3 Stormshield Data Virtual Disk

6.3.1 Recovery using the .VBOXSAVE file

The physical support for a secure volume is a container file (.vbox extension) that contains:

- the cryptographic elements necessary for mounting the volume (the volume's symmetric encryption key is wrapped with the public key for each authorized user and with each recovery key)
- the content belonging to the volume (files stores in the volume and file system).

The cryptographic elements are systematically saved in a "backup file" (*.vboxsave* extension) when the volume is created and again with each modification to the user list.

Recovering a Stormshield Data Virtual Disk volume is identical to changing the owner, as described in the product user manual. Basically, the user requesting a change in ownership is not the initial owner but the user whose encryption certificate has been defined as the recovery certificate.

Therefore, recovery consists of defining a new user as the owner of the volume. The new owner can then perform all the chosen operations.

The parameters used for modifying a volume's user list from the *.vboxsave* backup file are described in the section Modifying a volume's users list via the .VBOXSAVE file [Disk].

Recovery without the container file

However, for a simple ownership change, it is possible to perform a recovery without having a container file, only with the VBOXSAVE volume.

The user with the container file does not need to send the entire container file so that the recovery can be performed, but only needs to send the *.vboxsave* file.

For this, the user who wants a recovery shall send the *.vboxsave* file to the administrator in charge of recovery. The administrator proceeds as if changing the owner, then sends the *.vboxsave* file to the user who made the request. They only have to update the *.vboxsave* file and continue the ownership change procedure as if they had updated the *.vboxsave* file themselves.

6.3.2 Unmounting by force

We recommend you not to unmount a Stormshield Data Virtual Disk volume "by force" or when there are open files in it. If such an operation is necessary, we strongly recommend you to check the volume (using the Windows tool for checking the disk) the next time it is mounted, before using it.

6.3.3 Copying volumes

If a secure volume is duplicated by copying the .vbox container file, the two copies cannot be mounted simultaneously on a single workstation.

Generally, it is not recommended to duplicate volumes by copying the .vbox container file. This method should be used only for backups.

6.3.4 Using the volume within a Windows multi-session context

For a better integration within Microsoft Windows, a Stormshield Data Virtual Disk volume behaves in the same way than a standard storage volume.

An encrypted volume mounted in a Windows session is thus accessible from other Windows sessions opened on the workstation.

To avoid that, the user must select the Stormshield Data Security account lockout when the Windows session locks. For more information, refer to the section *Setting screen saver options* in the *Stormshield Data Security Installation and implementation guide*.

Locking the account unmounts encrypted volumes mounted in the session. However unmounting by force a volume may damage the files opened on this volume. The user must save modifications before locking the session.

On a Window server, a remote user cannot see the Stormshield Data Virtual Disk volumes mounted by other remote users connected to the same server. We recommend however selecting automatic locking because disk volumes are actually just hidden. Data on the disks may then be accessed.

6.3.5 Limitations

- The maximum size of a Stormshield Data Virtual Disk volume is 2048 GB (2 TB).
- A volume larger than 2 GB cannot be formatted in FAT16 (a limitation of FAT16).
- A volume smaller than 2.5 MB cannot be formatted in NTFS (a limitation of NTFS).
- The icon for a Stormshield Data Virtual Disk volume may be incorrect in Explorer (either a normal disk icon or a document icon).

6.4 Stormshield Data File

6.4.1 File permissions

If permissions (in the NTFS sense) are defined for a file, then they are lost after Stormshield Data File encrypts or decrypts the file.

If Windows permissions must be implemented on confidential files secured by Stormshield Data File, then these permissions must be defined for the directories containing the files, not on the files themselves.

6.4.2 Windows shutdown and long automatic processing

By default, Stormshield Data Security disconnects the Stormshield Data Security user when the Windows session is closed (or the user shuts down the system before the end of the session).

If the user configured a large amount of automatic processing (a large encryption list), this processing might not have enough time to finish.

To mitigate this risk, it is possible to configure Stormshield Data Security to not allow Windows to close a session if a Stormshield Data Security user is connected. To do this, put NoShutDown=1 in the [Logon] section of the *SBox.ini* file. See section Section [Logon].

With this configuration, the user must disconnect from Stormshield Data Security before closing the Windows session.

6.4.3 Syntax of the Stormshield Data File file lists

A file list is a text file whose lines are separated by a CR+LF, without a blank line, along with a three-line header:

```
Security BOX Encryption List
Version=1
===== DO NOT EDIT what you see in these file! ====
```

1st line: defines the file type from among the following types:

Content of the First Line	File Type
Stormshield Data Security Encryption List	*.enc
Stormshield Data Security Decryption List	*.dec
Stormshield Data Security Encryption Protected List	*.efp

2nd line: defines the version of the file. Only version 1 has been implemented so far.

3rd line: constant.

Remaining lines: defines a list element, using the following syntax:

- for an encryption or decryption list:

```
Folder , [File] , dir | file | * [,rec ] [,SO ] [,Hide ]
```

- for an exclusion list:

```
Folder , [File] , dir | file | * , ref | conf [,rec ] [,SO ] [,Hide ]
```

Parameter	Description	
Folder	full path to the folder	no "\" at the end
File	file name by itself	empty for a folder

dir	the line designates a folder	[File] must be blank
file	the line designates a file	[File] must not contain wildcards
*	the line designates a set of files	[File] contains wildcards ("*","?")
rec	recursiveness indicator	the subfolders of Folder are affected
SO	the line is not editable by the user	SO = System Officer
hide	the line is hidden from the user	
ref	the designated files are protected by a rejection	reserved to the list of protected files
conf	the designated files are protected by a confirmation	reserved to the list of protected files

Example:

```
Security BOX Encryption List
Version=1
===== DO NOT EDIT what you see in these file! =====
C:\SECURE,,dir,rec,SO
```

6.4.4 Keywords for the Stormshield Data File file lists

Stormshield Data File file lists take the following keywords into account:

AppData	The typical path is C:\Users\username\AppData\Roaming.
CommonDocuments	The typical path is C:\Users\Public\Documents.
Cookies	The typical path is C:\Users\username\AppData\Roaming\Microsoft\Windows\Cookies.
History	File system folder used as a common folder for Internet history.
InternetCache	The typical path is C:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files.
Personal	The virtual folder represents the C:\Users\username\Documents desktop item.
ProgramFiles	The typical path is C:\Program Files.
ProgramFilesCommon	The typical path is C:\Program Files\Common Files.
Recent	The typical path is C:\Users\username\AppData\Roaming\Microsoft\Windows\Recent.
System	Windows system folder. The typical path is C:\Windows\System32.
Windows	Windows folder or SYSROOT. It corresponds to %windir% environment variables or %SYSTEMROOT% The typical path is C:\Windows

6.5 Stormshield Data Shredder

6.5.1 Windows shutdown and long automatic processing

By default, Stormshield Data Security disconnects the Stormshield Data Security user when the Windows session is closed (or if the user shuts down the system before the end of the session).

If the user is configured for a large amount of automatic processing (a large cleaning list), this processing might not have enough time to finish.

To mitigate this risk, it is possible to configure Stormshield Data Security to not allow Windows to close a session if a Stormshield Data Security user is connected. To do this, put NoShutDown=1 in the [Logon] section of the *SBox.ini* file. See section Section [Logon].

With this configuration, the user must disconnect from Stormshield Data Security before closing the Windows session.

6.5.2 Syntax of the Stormshield Data Shredder file lists

A file list is a text file whose lines are separated by a CR+LF, without blank lines, along with a three-line header:

```
Security BOX Clean List
Version=1
===== DO NOT EDIT what you see in these file! ====
```

1st line: defines the file type from among the following types:

Content of the First Line	File Type
Stormshield Data Security Clean List	*.cln
Stormshield Data Security Clean Protected List	*.cfp

2nd line: defines the version of the file. Only version 1 has been implemented so far.

3rd line: constant.

Remaining lines: defines a list element, using the following syntax:

- for a cleaning list:

```
Folder , [File] , dir | file | * [,rec ] [,SO ] [,Hide ]
```

- for an exclusion list:

```
Folder , [File] , dir | file | * , ref | conf [,rec ] [,SO ] [,Hide ]
```

Parameter	Description	
Folder	full path to the folder	no "\" at the end
File	file name by itself	empty for a folder
dir	the line designates a folder	[File] must be blank
file	the line designates a file	[File] must not contain wildcards
*	the line designates a set of files	[File] contains wildcards ("*","?")
rec	recursiveness indicator	the subfolders of Folder are affected
SO	the line is not editable by the user	SO = System Officer
hide	the line is hidden from the user	
ref	the designated files are protected by a rejection	reserved to the list of protected files
conf	the designated files are protected by a confirmation	reserved to the list of protected files

6.5.3 Keywords for the Stormshield Data Shredder file lists

Stormshield Data Shredder file lists take the following keywords into account:

AppData	The typical path is C:\Users\username\AppData\Roaming.
CommonDocuments	The typical path is C:\Documents and Settings\All Users\Documents.
Cookies	The typical path is C:\Users\username\AppData\Roaming\Microsoft\Windows\Cookies.
History	File system folder used as a common folder for Internet history.

InternetCache	The typical path is C:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files.
Personal	The virtual folder represents the C:\Users\username\Documents desktop item.
ProgramFiles	The typical path is C:\Program Files.
ProgramFilesCommon	The typical path is C:\Program Files\Common Files.
Recent	The typical path is C:\Users\username\AppData\Roaming\Microsoft\Windows\Recent.
System	Windows system folder. The typical path is C:\Windows\System32.
Windows	Windows folder or SYSROOT. It corresponds to %windir% environment variables or %SYSTEMROOT% The typical path is C:\Windows
BitBucket	The virtual folder contains the user's Bin items.

NOTE
The syntax for these keywords is: %keyword%

Example:

To add the bin content to a Shredder list, you must add the %BitBucket% item.

NOTE
%temp% is not handled. However, it is possible to specify it if
%AppData% -> C:\Users\username\AppData\Roaming
%temp% -> C:\Users\username\AppData\Local\Temp

Then <"Appdata"\..\Local\Temp> is equivalent to %temp%.

You must enter %AppData%\..\Local\Temp\ in the list.

6.6 Stormshield Data Mail

6.6.1 Stormshield Data Mail Outlook Edition

RTF format

RTF format is not supported by Stormshield Data Mail Outlook Edition because it does not guarantee a reliable interoperability with the security mechanism of Stormshield Data Security. Using the RTF format could engender a loss of information.

It is thus recommended using the HTML format to write secure messages, because there is no interoperability issue with this format.

Transcipherment

Transcipherment allows updating the protection level of secured messages (S/MIME format messages or plain text messages including an attachment encrypted with the component Stormshield Data File). It consists in 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.

Accessing user's private keys during transcipherment implies to be connected to Stormshield Data Security.

It is thus recommended disabling automatic disconnection and session locking on screen saver options when there are many messages to be transciphered. The processing time is proportional to the number of messages to be processed.

NOTE

A secured message will not be transciphered if the user's current encryption key is the key which encrypted first the message.

A message which has already been transciphered by the current key will not be transciphered again, as long as the user's current key is not updated.

Encryption learning

Encryption learning allows automatic encryption of e-mails sent to a specific recipient. Learning relies on default values of 90 days and three encrypted e-mails sent over that period to enable automatic encryption.

These default values can be modified in the registry base thanks to the following information:

HKEY_CURRENT_USER\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Mail\ AutoSuggestWithinDays =<DWORD : number of days>

HKEY_CURRENT_USER\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Mail \ AutoSuggestUsageCount =<DWORD : number of sent e-mails>

The learning option can also be enabled or disabled by modifying the following key:

HKEY_CURRENT_USER\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Mail \ EnableAutoSuggestEncrypt=<DWORD : 0 to disable, 1 to enable>

6.6.2 Notes Edition not activated

The installation procedure for Stormshield Data Mail - Notes Edition adds its four components to the *notes.ini* file.

If Notes is installed over a network or only for the current user (not for all of the workstation's users = AllUsers), then the *notes.ini* file modified by the installation procedure is not the one that Notes actually uses. The Stormshield Data Security extension has not been activated.

In this case, you must add the following lines to the *notes.ini* file that Notes actually uses:

```
EXTMGR_ADDINS=SBMLNR2,SBMLNW
NSF_HOOKS=SBMLNR
ADDINMENUS=SBMLNM
```

If one of these lines is already present (another extension is already installed), Stormshield Data Mail is added to the end of the line.

Example:

```
ADDINMENUS=<other extension>,SBMLNM
```

If an extension was already present and the updated *notes.ini* file is not the one that is actually used, you should update the relevant lines by adding the Stormshield Data Mail information to the end of the line.

6.6.3 LDAP settings: certificates with several e-mail addresses

If a recipient having several e-mail addresses in his/her certificate is not in your Stormshield Data Security trusted address book but is in your LDAP directory(ies), a dialog box warning that "the certificate has not been found in your trusted address book" can display when sending an encrypted e-mail to this recipient.

In this case, you can set up your LDAP directory in order to retrieve the certificate when sending the encrypted e-mail.

To do so, check that the user attribute "proxyAddresses" in the LDAP directory contains all the user secondary e-mail addresses.

In the attribute, each secondary e-mail address must be preceded by "smtp: ", whereas the main address is preceded by "SMTP: ".

This attribute can be updated via enterprise mail servers such as Exchange.

6.6.4 E-mail addresses coherency check

When sending e-mails, the best available certificate is searched for each recipient. If the certificate comes from the LDAP directory, a coherency check occurred between the recipient's e-mail address and the address specified in this certificate. If they are not the same, the certificate is rejected and the e-mail may not be sent.

If you use internal aliases for users' addresses, this mechanism may not be appropriate.

- To deactivate coherency check on a user's workstation, define the **DWORD CheckLDAPCertificateEmailAddress** value to 0 in the HKLM\SOFTWARE\Arkoon\Security BOX Enterprise\Mail registry key.

NOTE
The e-mail addresses coherency check has been implemented for security reasons. We do recommend not deactivating it, unless specifically required.

6.7 Stormshield Data Team

6.7.1 DFS environment restriction

- A DFS root cannot be encrypted.
- Stormshield Data Security accounts must not be stored on a DFS share.

6.7.2 Managing the user's temporary folder (%TEMP%)

Several employees should not be listed on a rule involving the temporary folder for the Windows profile. Applications use this folder to store temporary files specific to the user.

If this rule is not respected, blockages can occur.

6.7.3 Managing the system's temporary folder

System processes (typically services) use this file to store temporary files, and it is shared with the other users on the system.

This folder is typically c:\windows\temp. The exact location depends on the installation of the operating system.

This folder should not be encrypted with Stormshield Data Team.

6.7.4 Folders available offline

Using the cachemov.exe tool, it is possible to move the system folder <%WINDIR%>CSC which contains the files that are available offline.

Stormshield Data Team must be configured to manage this particular environment.

To do this, follow the procedure below:

1. Run regedit.
2. Go to the key: HKLM\SYSTEM\CURRENTCONTROLSET\Services\SBoxTeamDrv\Parameters
3. Add the SkipFolderR value, the folder containing the CSD database.
4. Restart the machine.

6.7.5 Optimizing access on slow networks

To know if a file is really encrypted or not, Stormshield Data Team must open it. On a low speed network (for example, GPRS), the explorer may become very slow, even appear to be frozen.

In such a case, Stormshield Data Team can be configured to detect if a file is encrypted or not according to the presence of a “local” rule.

To enable this feature, write the following in the registry:

For HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Properties\Team, the key OverlayIconAccuracy (DWORD) = 0x00000005.

CAUTION
In this operating mode:

- In an unsecured folder, an encrypted file appears as unencrypted.
- In a secured folder, an unencrypted file appears as encrypted.

6.7.6 Keeping performance optimal on the workstation

When Stormshield Data Team is used, users's workstation may slow down.Stormshield To guarantee the usual levels of performance, the following settings can be applied to workstations.

Improving performance when browsing encrypted trees

This enhancement greatly reduces the time it takes to determine whether a folder is encrypted in "smart card" mode, this determines the icon of the folder.

This option can be configured in the OverlayIconAccuracy in the registry database:

1. Go to the registry database by running **regedit.exe**.
2. In the tree, go to the key **HKEY_LOCAL_MACHINE\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Team**.
3. Change the value of the key `OverlayIconAccuracy = 0x40`.
4. Quit the registry database.
5. Restart the machine.

This value can be combined with other current values.

Excluding Windows processes that access encrypted folders

Some Windows processes can slow down the workstation by regularly accessing folders that Stormshield Data Team encrypts.

To reduce the frequency of these slowdowns, you can exclude in the registry database the processes that are considered safe and do not cause any file modifications:

1. Go to the registry database by running **regedit.exe**.
2. In the tree, go to the key **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SboxTeamDrv\Parameters**.
3. Change the value of the `SkipApp` key by adding the list of processes to exclude. Add one process per line. If a key does not exist, you can create it by choosing a REG_MULTI_SZ value.
4. Quit the registry database.
5. Restart the machine.

We recommend that you exclude the following processes:

- SearchIndexer.exe
- searchUI.exe
- MsMpEng.exe
- SearchProtocolHost.exe
- SearchFilterHost.exe
- mobsync.exe
- msdtc.exe
- mstsc.exe
- mobsync.exe
- wfica32.exe
- vmtoolsd.exe
- SecurityHealthService.exe
- SearchApp.exe
- NisSrv.exe

Dell processes:

- HostStorageService.exe
- HostControlService.exe

Excluding Windows Defender extensions and scans

To prevent your workstation from slowing down, you can also exclude the extensions and scans that Windows Defender runs:

1. Go to the registry database by running **regedit.exe**.
2. In the tree, go to the key **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions**.
3. In the `Extensions` key, add the list of extensions to exclude. We recommend that you exclude the following extensions: *.box*, *.sbox*, *.sbt*, *.sdsx*, *.usi*, *.usr* (REG_DWORD).
4. In the `Processes` key, add the list of processesto exclude. We recommend that you exclude the following processes: SBDSRV, SBoxDiskSrv (REG_DWORD) as well as antivirus and other EDR processes.
5. Quit the registry database.
6. Restart the machine.

6.7.7 Folder exclusion

Stormshield Data Team provides the ExcludedPath feature, which enables to exclude folders from Stormshield Data Team.

This feature takes in charge:

- Display management for the Team properties tab on folders: the content of the Team tab cannot be accessed for a folder from a tree excluded from encryption.
- Encryption report management for the application of a shared rule: a file from an excluded tree has an Excluded file status during securing and de-securing operations. During the desecuring operation, a file in clear text keeps its File in clear text status.
- Management for OverlayIcon: Team overlayIcon is not displayed on a folder of a tree excluded from encryption.

If you want to exclude a folder from Stormshield Data Team analysis , you must add it to ExcludedPathinto the[TEAM] section of *SBox.ini* file.

Syntax is as follows:

```
[TEAM] ExcludedPath = path * [,path]: where path is the path of the folder to
exclude. This path can be composed with SecurityBOX tags if put into < >
```

The default value is: ExcludedPath = <%APPDATA%>.

IMPORTANT

You shall not add a space between the coma and the path.

The tag can be:

- RootPath1: users' account folder for *SBox.ini*
- RootPath2: second users's account folder
- COMMON_APPDATA: C:\ProgramData
- COMMON_DOCUMENTS: C:\Users\Public\Documents
- USERNAME: <username> Windows user's name .
- LOCAL_APPDATA: C:\Users\username\AppData\Local
- DESKTOP: C:\Users\username\Desktop
- MYDOCUMENTS: C:\Users\username\Documents
- PROFILE: C:\Users\username
- %ENV%: where ENV is a system environment variable.

Example:

```
[TEAM] ExcludedPath=c:\User,<RootPath1>,<%TMP%>
```

NOTE

If RootPath1 or DefaultPath1 parameters for *SBox.ini* are customized, it is necessary to add these specific directories into ExcludedPath.

NOTE

The maximum size for the ExcludedPath parameter is 255 characters.

6.7.8 Moving an intra-volume folder

Moving an intra-volume folder is not allowed when source and destination directories do no have the same security.

NOTE

If the action is executed into Windows explorer, the moving operation is replaced with Copy + Delete the source. In this case, the destination folder's security is applied to the "moved" folder.

6.7.9 Accessing a file is not allowed if the certificate is revoked

Stormshield Data Team prevents a user from accessing an encrypted file if his/her certificate is revoked, even if this user appears in the list of users. This can be done configuring the *SBox.ini* file.

Consequently, when the certificate is checked:

- Any operation on secured files (opening, creating, renaming, moving and deleting) is denied.

  NOTE

  These operations fail even if the file is encrypted with an old encryption key.

- Any operation on security rules is impossible. The user interfaces are greyed out and they only allow reading for rules parameters.

Stormshield Data Team uses the revocation controler configuration defined at the user level. Therefore:

- Do not allow the user to deactivate the revocation control.
- Do not forget to correctly configure the downloading rule for the revocation lists.

See the section called "Opening an encrypted file not allowed if encryption key is revoked" for the parameters to use.

A tooltip is displayed during the first access to an encrypted file after the connection (once per connection) to warn the user his/her encryption certificate does not allow him/her to access the encrypted files.

NOTE

Verifying the certificate is revoked is not a safe way to prevent users from opening a file. Indeed, this verification does not replace files encryption but is only a temporary way. It is also important to prevent from creating a new encryption key or using another certificate.

6.7.10 Modifying the last access dates

Some solutions (as the archive solutions) are based on last access dates of files to operates treatments. However, when Stormshield Data Team is installed on a workstation, the last access date is modified when browsing a folder.

The AccessTimeAction parameter enables to control the restoration of the last access dates on files and suppress the modification of last access dates when opening files with Stormshield Data Team.

Location:	HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SBoxTeamDrv\Parameters
Key:	AccessTimeAction (DWORD)

Values:

- 0x00000000: no attempt to restore the access date (value by default);
- 0x00000001: optimized restoration of access date on standard files systems;
- 0x00000002: restoration of access date on NFS files systems;
- 0x00000008: restoration of access dates on standard files systems. This option enables the compatibility with files systems "considered as standard", such as NAS EMC.

In a general way, the value by default (0) is recommended. However, when using an archive solution based on a NAS EMC, the 0x00000008 value is recommended.

NOTE
The0x8 value also works with standard FS but with a performance penalty. It can be useful on other unusual CIFS servers.

Also refer to the parameter OverlayIconAccuracy which enables not to change the access dates to files (values: 0x00000020).

6.7.11 Using the cache in a network

When using the cache in a network, the files and folders but also the rules may be changed beyond the control of the local file system user. If a change is made by a user on the network, other workstations using the share may have incorrect cache entries for some time and therefore invalid status in Windows Explorer. Consequently, the new states will not take effect immediately.

To reduce these inconsistencies, you can take the following measures:

- Secure a folder from its creation while it is still empty.
- Notify users that they avoid using the share at the critical moment.
- Do not destroy a file and then recreate it with the same name and different characteristics. If this should be done, let pass between the two operations the time required to update the caches (within 15 minutes or restart the user machine for instantaneous effect).
- Perform operations on a consistent tree of files (security / desecuring) at times when no or few users are connected (e.g. during lunch break or end of the day).

NOTE
The addition or deletion of coworkers to an existing rule does not pose a particular problem and there is therefore no precaution.

6.8 Automatic account update on LDAPS

An automatic account update with a *.usx* file is possible from an LDAP server with SSL connection (LDAPS). To establish the SSL connection, Stormshield Data Security requires that:

- the protocol specified in the URL be ldaps://;
- the port used be the port 636.

6.9 Execution traces

In case of any issue occurring when using the software, Stormshield Data Security offers a tracing system. It provides Stormshield Data Security Technical Assistance Center with information useful for the analysis of issues. Restarting the workstation or the Windows session is not required to enable tracing.

6.9.1 How tracing works

To enable Stormshield Data Security tracing, select the Stormshield Data Security folder in the Windows Start menu or double-click the file with the *.sbdiag* extension provided by the Stormshield Data Security Technical Assistance Center.

During a tracing session, the following elements are saved in the folder **C:/ProgramData/Arkoon/Security BOX/Traces**:

- Stormshield Data Security traces (*Trace.etl* file);
- Stormshield Data Security events (*audits.evtx* file): it is possible to configure the generation of this file in the interface or in the *.sbdiag* file. Events logs must be enabled. To enable logs, refer to section Events log;
- A digest of the workstation (*sbdiag.xml* file): information about the system and about the installation of Stormshield Data Security and the Microsoft Office suite;
- A PSR trace (Problem Steps Recorder): this tool is provided with Windows operating systems from Windows 7 and allows recording actions performed when reproducing a problem on the workstation. It is possible to configure the generation of this file in the interface or in the *.sbdiag* file.

On Windows Server 2012 R2 and Windows 7 SP1, you must first install the following Microsoft update to be able to use PSR trace: hotfix package KB3080149 (https://support.microsoft.com/en-us/kb/3080149).

6.9.2 Using tracing system

From a .sbdiag file

1. Double-click the .sbdiag file provided by the Stormshield Data Security Technical Assistance Center to start the tracing interface in pre-configured mode.
2. Click Start tracing.
3. Wait for the Tracing in progress message.
4. Reproduce the actions sequence to be traced.
5. When the sequence is done, click Stop tracing.
6. In the next window, add comments for the Stormshield Data Security Technical Assistance Center if needed. Provide additional information about the method of reproduction, time markers, file names, etc.
7. Wait until the folder containing the tracing session opens. Send the zip file Trace<timestamp>.zip to the Stormshield Data Security Technical Assistance Center.

> **NOTE**
> In pre-configured mode, parameters cannot be modified.

From the tracing interface

If you do not have a .sbdiag file or if you want to customize the tracing session, select Tracing in the Windows Start/Stormshield Data Security menu.

To start the session, first open the settings window by clicking the gear icon and select options. Enabling events logs is required to extract Stormshield Data Security events.

NOTE
If a Stormshield Data Security module is not installed on the workstation, checking or unchecking this module in the settings window has no consequence on tracing.

After clicking OK, a .sbdiag file is automatically created and the tracing session can be started as described in the previous section.

CAUTION
The PSR (Problem Steps Recorder) tool can record screen captures during tracing session.

Appendix A. List of Stormshield Data Security logs

A.1. Administration

Stormshield Data Security Suite installation

Number	Type	Description
300	Information	Stormshield Data Security installation was successful. The configuration parameters are: • Version: %2 (%3) • Patch version: %4 • Installation folder: %5 • Company: %6
301	Information	Stormshield Data Security modification was successful. The configuration parameters are: • Version: %2 (%3) • Patch version: %4 • Installation folder: %5
302	Information	Stormshield Data Security uninstall was successful. The configuration parameters are: • Version: %2 (%3) • Patch version: %4 • Installation folder: %5
303	Information	Stormshield Data Security patch installation was successful. The configuration parameters are: - • Version: %2 (%3) • Patch version: %4 • Installation folder: %5 • Company: %6
304	Information	Stormshield Data Security patch modification was successful. The configuration parameters are: - • Version: %2 (%3) • Patch version: %4 • Installation folder: %5
305	Information	Stormshield Data Security patch uninstall was successful. The configuration parameters are: - • Version: %2 (%3) • Patch version: %4 • Installation folder: %5
306	Error	Stormshield Data Security setup closed unexpectedly.
307	Error	Stormshield Data Security setup closed before it ends up correctly.
308	Error	According to the group policy, events are sent to the '%2' server, but connecting to this address fails with the error code %3: "%4". Please ask your administrator.
1925	Error	You do not have sufficient privileges to run this installation for all users on this computer. Open a session as an administrator, then try to run this installation again.

Directory administration

Number	Type	Description
700	Information	The automatic update of the directory was successful.
701	Error	The automatic update of the directory failed.
702	Information	The manual update of the directory was successful.
703	Error	The update of the directory failed.
704	Information	The update of the directory at logon was successful.
705	Error	The update of the directory at logon failed.
706	Information	The update of the directory after unlock was successful.
707	Error	The update of the directory after unlock failed.
708	Information	The export of certificate(s) %4 of the directory with format '%3' was successful in file '%2'.
709	Error	The export of certificate(s) %4 of the directory with format '%3' in file '%2' failed.
710	Information	The import of certificate(s) %2 in the directory was successful.
711	Error	The import of certificate(s) %2 in the directory failed.
712	Information	COMPATIBILITY_MODE option: Value: %2 Acces %3
713	Information	ALLOW_MANUAL_UPDATE option: Value: %2 Acces %3
714	Information	DISABLE_CHECK_ON_DISPLAY option: Value: %2 Acces %3
715	Information	ACTIVATE option: Value: %2 Acces %3
716	Information	ALLOW_DOWNLOAD_CRL option: Value: %2 Acces %3
717	Information	REPLACE_FROM_LDAP option: Value: %2 Acces %3
718	Information	START_ON_CONNECTION option: Value: %2 Acces %3
719	Information	REPLACE_FROM_LDAP_OUTOFDATE_CERT option: Value: %2 Acces %3
720	Information	REPLACE_FROM_LDAP_REVOKEDCERT option: Value: %2 Acces %3
721	Information	DELETE_IF_OUTOFDATE option: Value: %2 Acces %3
722	Information	DELETE_IF_REVOKE option: Value: %2 Acces %3
723	Information	DELETE_IF_NOT_ON_LDAP option: Value: %2 Acces %3
724	Information	SB_EVT_ADMINISTRATION_INFO_REPLACE_ON_VALID_CERT option: Value: %2 Acces %3
725	Information	TIMER option: Value: %2 Acces %3
726	Information	COMMON_NAME_REPLACE option: Value: %2 Acces %3
727	Information	COMMON_NAME_OUT_OF_DATE option: Value: %2 Acces %3
728	Information	COMMON_NAME_REVOKE option: Value: %2 Acces %3
729	Information	COMMON_NAME_NOT_ON_LDAP option: Value: %2 Acces %3
730	Warning	The LDAP update of the certificate which email is '%2' could not be applied because the revocation list is not available.

Management of the revocation list

Number	Type	Description
1100	Information	The update of the revocation list %2 was successful.
1101	Error	The update of the revocation list %2 failed.
1102	Information	The update of the revocation list %2 from the cache was successful.
1103	Error	The automatic update of the revocation list %2 from the cache failed.

A.2. Virtual Disk

Volumes management

Number	Type	Description
8300	Information	The mounting of the automatic volume '%2' on '%3' in '%4' mode was successful.
8301	Error	The mouting of the automatic volume '%2' on '%3' in '%4' mode failed.
8302	Information	The volume '%2' was successfully mounted on '%3' in '%4' mode.
8303	Error	The mounting of the volume '%2' on '%3' in '%4' mode failed.
8304	Information	The unmounting of the automatic volume '%2' mounted on '%3' was successful.
8305	Error	The unmounting of the automatic volume '%2' mounted on '%3' failed
8306	Information	The volume '%2' mounted on '%3' was successfully unmounted.
8307	Error	The unmounting of volume '%2' mounted on '%3' failed.
8308	Information	The volume '%2' mounted on '%3' was successfully locked.
8309	Error	The unlock of volume '%2' mounted on '%3' failed.
8310	Information	The volume '%2' mounted on r '%3' was successfully unlocked.
8311	Error	The unlock of volume '%2' mounted on '%3' failed.
8312	Information	The volume '%2' was successfully created.
8313	Error	The creation of volume '%2' failed.
8314	Information	The volume '%2' was successfully added to the list of automatic volumes. It will be mounted on '%3'.
8315	Error	The adding of volume '%2' to the list of automatic volumes failed.
8316	Information	The volume '%2' mounted on '%3' was successfully deleted to the list of automatic volumes.
8317	Error	The deletion of volume '%2' (mounted on '%3') from the list of automatic volumes failed.

A.3. File

Encryption /Decryption

Number	Type	Description
18300	Information	The user successfully encrypted the file '%2' in auto-encryptable mode.
18301	Error	The encryption of the file '%2' in auto-encryptable mode failed.
18302	Information	The user successfully encrypted the folder '%2' in auto-encryptable mode.
18303	Error	The encryption of the folder '%2' in auto-encryptable mode failed.
18304	Information	The user successfully encrypted the file '%2' by using SecurityBOX SmartFile.
18305	Error	The encryption of file '%2' by using SecurityBOX SmartFile failed.
18306	Information	The user successfully encrypted the folder '%2' by using SecurityBOX SmartFile.
18307	Error	The encryption of the folder '%2' by using SecurityBOX SmartFile failed.
18308	Information	The user successfully encrypted the file '%2' for the following correspondents: %3.
18309	Error	The encryption of the file '%2' for the following correspondents failed: %3.
18310	Information	The user successfully encrypted the folder '%2' for the following correspondents: %3.
18311	Error	The encryption of the folder '%2' for the following correspondents failed: %3.
18312	Information	These coworkers have been added successfully to the file '%2' :%r%3.
18313	Error	These coworkers could not be added to the file '%2' : %r%3.
18314	Information	These coworkers have been removed successfully from the file '%2':%r%3.
18315	Error	These coworkers could not be removed from the file '%2': %r%3.

Encryption / Decryption

Number	Type	Description
18700	Information	The user successfully encrypted the file '%2'.
18701	Error	The encryption of the file '%2' failed.
18702	Information	The user successfully decrypted the file '%2'.
18703	Error	The decryption of the file '%2' failed.

A.4. Kernel

Start / Stop

Number	Type	Description
25300	Information	The start of the kernel was successful.
25301	Error	The start of the kernel failed
25302	Information	The stop of the kernel was successful.
25303	Error	The stop of the kernel failed.
25304	Error	The value of the paramter %2 present in *SBox.ini* is not valid. %3 Please contact your administrator.
25305	Error	The value of the parameter %2 was not entered in *SBox.ini*. %3 Please contact your administrator.
31725	Error	The 'MasterPolicies' parameter prohibits copying the file '%2'.

LDAPS authentication

Numéro	Type	Description
25700	Warning	SSL security warning: invalid server certificate. %rDelivered to: %2%rDelivered by: %3%rValid from %4 to %5.%rPlease contact your system administrator.
25701	Error	SSL security error: invalid server certificate. %rDelivered to: %2%rDelivered by: %3%rValid from %4 to %5.%rPlease contact your system administrator.
25702	Error	All authentication methods submitted to the LDAP server have failed.
25703	Information	The user is authenticated by the LDAP server with the method: %2

Cryptographic device selection

Numéro	Type	Description
26100	Information	The user selected the '%2' middleware.

A.5. Keystore

Log on / Log off

Number	Type	Description
31300	Information	The user was logged on their Stormshield Data Security keyring.
31301	Error	Stormshield Data Security keyring logon failed.
31302	Information	The user logged off their Stormshield Data Security keyring.

31303	Error	The user could not logged off Stormshield Data Security keyring.
31304	Information	Stormshield Data Security user session was locked.
31305	Error	Stormshield Data Security user session failed to lock.
31306	Information	Stormshield Data Security user session unlock was successful.
31307	Error	Stormshield Data Security user session unlock failed.
31308	Warning	A user was already logged on Stormshield Data Security in another Windows session.
31309	Warning	The secret code is incorrect.
31310	Warning	The identifier '%2' does not correspond to a Stormshield Data Security account.
31311	Warning	Stormshield Data Security session could not be locked because the card in the drive was not the right card.
31312	Error	Stormshield Data Security account or card was blocked.
31313	Information	The card was withdrawn from the drive.
31314	Error	The card is blocked.
31315	Error	Unable to notify a component.
31316	Error	Unable to load a component: '%2'

Account management

Number	Type	Description
31700	Information	The account was successfully created.
31701	Warning	The installation of Stormshield Data Security account encountered a non-blocking error.
31702	Error	The installation of Stormshield Data Security account failed.
31703	Information	The uninstall of Stormshield Data Security account was successful.
31704	Error	The uninstall of Stormshield Data Security account failed.
31705	Information	The security policy was updated.
31706	Error	The security policy update failed with the following error: %2.
31707	Information	The export of Stormshield Data Security account was successful.
31708	Error	The export of Stormshield Data Security account failed.
31709	Information	The change of the secret code associated to the account was successful.
31710	Error	The change of the secret code associated to the account failed.
31711	Error	The number of errors to change the secret code exceeded the authorized limit.
31712	Error	Impossible to create a new Stormshield Data Security account because the card is blocked.
31713	Warning	The entered secret code is incorrect.
31714	Error	The content of the card does not allow automatic account creation. .
31715	Error	Impossible to create a new Stormshield Data Security account because the template is blocked.
31716	Error	Impossible to create a new Stormshield Data Security account because the template cannot be accessed.
31717	Information	A new signatory of security policies was defined.
31718	Warning	The update of the security policy was not taken into account because the new signatory was rejected by the user.
31719	Information	Security policy download from '%2'.
31720	Warning	Error of the security policy download from '%2'.
31721	Information	The security policy update was not taken into account because the account is up-to-date.
31722	Error	The security policy update was not taken into account because the file signature is incorrect.

31723	Error	The security policy update was not taken into account for the following reason: '%2'.
31724	Warning	The security policy update was not taken into account despite the warning: %2.
31725	Error	The 'MasterPolicies' parameter forbids duplication of the file '%2'.
31726	Error	%2 card account automatic creation: %3.

Keys management

Numéro	Type	Description
32100	Information	The export of the encryption key by the user was successful.
32101	Error	The export of the encryption key by the user failed.
32102	Information	The renewal of the encryption key by the user was successful.
32103	Error	The renewal of the encryption key by the user failed.
32104	Information	The export of the signature key by the user was successful.
32105	Error	The export of the signature key by the user failed.
32106	Information	The renewal of the signature key by the user was successful.
32107	Error	The renewal of the signature key by the user failed.
32108	Information	The export of the key by the user was successful
32109	Error	The export of the key by the user failed
32110	Information	The renewal of the key by the user was successful.
32111	Error	The renewal of the key by the user failed.
32112	Information	The export of the encryption key certificate by the user was successful.
32113	Error	The export of the encryption key certificate by the user failed.
32114	Information	The export of the signature key certificate was successful.
32115	Error	The export of the signature key certificate failed.
32116	Information	The export of the key certificate by the user was successful.
32117	Error	The export of the key certificate by the user failed.
32118	Information	A certificate for the %2 has not been imported in the user account because it was out of date.
32119	Information	A certificate for the %2 has not been imported in the user account because its key usages were not sufficient.

Keyring management

Number	Type	Description
32500	Information	The encryption key was succesffully imported.
32501	Error	L'import de la clé de déchiffrement a échoué.
32502	Information	The recovery key was successfully imported.
32503	Error	The import of the recovery key failed.

A.6. Mail

Outgoing/Incoming

Number	Type	Description
39312	Information	The certificate of the user '%2' has not been found in the trusted address book.
39313	Information	The certificate of the user '%2' has been revoked.

Number	Type	Description
39314	Information	The certificate of the user '%2' is no longer valid.
39315	Information	The trust chain of the user '%2' has been revoked.
39316	Information	The trust chain of the user '%2' is no longer valid.
39317	Information	The certificate revocation list is not available for the user '%2'.
39318	Warning	The user received an encrypted e-mail but does not have any decryption key.
39319	Warning	The user received an e-mail with an invalid signature. The e-mail has been signed with the certificate '%2'.
39320	Information	Sending a signed e-mail was successful (Recipient(s): %2).
39321	Information	Sending an encrypted e-mail was successful (Recipient(s): %2).
39322	Information	Sending a signed and encrypted e-mail was successful (Recipient(s): %2).

Transcipherment

Number	Type	Description
39700	Information	The user run transcipherment on the folder '%2'
39701	Warning	Issues occurred with transcipherment.

Disabling security

Number	Type	Description
40100	Information	The security of e-mails in the folder '%2' has been disabled.
40101	Information	The security of some e-mails has been disabled (number: %2).
40102	Warning	Issues occurred when disabling the security of some e-mails.

Administration

Number	Type	Description
40500	Information	The Stormshield Data Mail module has been successfully loaded in Outlook '%2'.
40501	Information	The Stormshield Data Mail module has been disabled in Outlook '%2'.
40502	Information	The following exception has been raised in the Stormshield Data Mail module: %2.
40503	Warning	The following registry key, which is necessary for the Stormshield Data Mail Outlook Edition add-in to work properly, has been modified: '%2'.

A.7. Shredder

Number	Type	Description
46300	Information	The shredding operation was successfully initiated.
46301	Error	The shredding operation failed to start.
46302	Information	The shredding operation was successful.
46303	Error	The shredding operation failed.
46304	Information	The deletion of file '%2' was successful.
46305	Error	The deletion of file "%2' failed.
46306	Information	The deletion of folder '%2' was successful.
46307	Error	The deletion of folder '%2' failed.
46308	Information	Secure emptying of the bin was successful.
46309	Error	Secure emptying of the bin failed.
46310	Information	Secure cleaning of the list of files was successful.
46311	Error	Secure cleaning of the list of files failed.

A.8. Sign

Signature

Number	Type	Description
47300	Information	The file '%2' was successfully signed.
47301	Error	The signature of the file r '%2' failed.
47302	Information	The file '%2' was successfully co-signed.
47303	Error	The co-signature of the file '%2' failed.
47304	Information	The file '%2' was successfully counter-signed.
47305	Error	The counter-signature of the file '%2' failed
47306	Information	The file '%2' was successfully over-signed.
47307	Error	The over-signature of the file r '%2' failed.
47308	Error	File '%2' is corrupted.

A.9. Team

Rules management

Numéro	Type	Description
49300	Information	A security rule has been defined on the folder '%2'.
49301	Error	Configuration of folder '%2' as a secure folder has failed.
49302	Information	The folder '%2' is back to clear mode (not secure).
49303	Error	Configuration of folder '%2' as a non secured folder has failed.
49304	Information	The following co-workers have been successfully added to folder '%2' rule:%r%3.
49305	Error	Addition of the following co-workers to folder '%2' rule has failed:%r%3.
49306	Information	The following co-workers have been successfully removed from folder '%2' rule:%r%3.
49307	Error	Removal of the following co-workers from folder '%2' rule failed: %r%3.
49308	Information	The following owners have been successfully added to folder '%2' rule: %r%3.
49309	Error	Addition of the following owners to folder '%2' rule has failed: %r%3.
49310	Information	The following owners have been successfully removed from folder '%2' rule: %r%3.
49311	Error	Removal of the following owners from folder '%2' rule has failed: %r%3.
49312	Information	Folder '%2' has been successfully configured as a secured folder (profile).
49313	Error	Configuration of folder '%2' as a secure folder has failed (profile).
49314	Information	Folder '%2' has been successfully configured as a non secure folder (profile).
49315	Error	Configuration of folder '%2' as a non secure folder has failed (profile).
49316	Information	The folder '%2' rule has been successfully updated (profile).
49317	Error	Update of the folder '%2' rule has failed (profile).
49318	Information	The following co-workers were successfully added to folder '%2' rule (profile):%r%3.
49319	Error	Addition of the following co-workers to folder '%2' rule failed (profile):%r%3.
49320	Information	The following co-workers have been successfully removed from folder '%2' rule (profile):%r%3.

49321	Error	Removal of the following co-workers from folder '%2' rule has failed (profile): %r%3.
49322	Warning	Update of the rules file (.ust) of the folder '%2' failed: inconsistent header.
49323	Warning	The user is not part of the users allowed for the rule on '%2'.
49324	Warning	The user gets access the rule properties on '%2' whereas the certificate is revoked.
49325	Information	The security rule of folder '%2' has been saved in the user account.
49326	Warning	The certificate '%2' could not be found.
49327	Information	The certificate '%2' is invalid and has been ignored.
49328	Information	The certificate '%2' is invalid, the user interrupted the encryption operation.
49329	Warning	The certificate '%2' could not be completely checked and has been used.
49330	Information	The certificate '%2' could not be completely checked and has been ignored.
49331	Warning	The certificate '%2' is not valid and revoked, and has been deleted from the rule.
49332	Information	The safety rule on '% 2' folder has been restored from the user account.
49333	Warning	Attack suspected: the security rule of '%2' folder has been replaced.
49334	Information	The security rule of '%2' folder has disappeared.
49335	Warning	An illegitimate coworker has been detected and ignored in the security rule of '%2' folder.
49336	Information	The safety rule on '% 2' folder has been restored from the local rule.
49342	Warning	The parent-child relationship or the revocation list cannot be verified.

Team rules update

Numéro	Type	Description
49337	Warning	The new certificate of the co-worker '%2' has not been found. He/she is no longer part of the rule.
49338	Warning	The rule known on the folder '%2' is out of date. The automatic update could not be applied.
49339	Warning	The folder '%2' on which the rule applies cannot be found or is no longer secured.
49340	Error	The encryption key of the co-worker '%2' has not been found.
49341	Warning	The co-worker '%2' has not been found in the rule.

Encryption/decryption

Numéro	Type	Description
49700	Information	File '%2' has been successfully moved from a secure folder to a non secure folder.
49701	Error	Moving file '%2' from a secure folder to a non secure folder has failed.
49702	Information	Folder '%2' has been successfully moved from a secure folder to a non secure folder.
49703	Error	Moving folder '%2' from a secure folder to a non secure folder has failed.
49704	Information	File '%2' has been successfully secured with defined rules.
49705	Error	Securing file '%2' with defined rules has failed.
49706	Information	Folder '%2' has been successfully secured with defined rules.
49707	Error	Securing folder '%2' with defined rules has failed.
49708	Information	File '%2' has been successfully unsecured.
49709	Error	Unsecuring file '%2' has failed.
49710	Information	Folder '%2' has been successfully unsecured.

49711	Error	Unsecuring folder '%2' has failed.
49712	Information	Securing has been cancelled.
49713	Information	Unsecuring has been cancelled.
49714	Error	Impossible to bring into compliance the folder '%2': You do not have the Windows rights.
49715	Warning	Impossible to bring into compliance the hidden folder '%2': You do not have the Windows rights.

Backing up/Restoring

Numéro	Type	Description
50100	Information	The '%2' file backup is finished.
50101	Error	The file '%2' could not be saved.
50102	Information	The '%2' folder backup is finished.
50103	Error	The folder '%2' could not be saved.
50104	Information	The '%2' file restoration is finished.
50105	Error	The file '%2' could not be restored.
50106	Information	The '%2' folder restoration is finished.
50107	Error	The folder '%2' could not be restored.
50108	Information	Saving has been canceled.
50109	Information	Restoring has been cancelled.
50110	Error	Impossible to save in the folder '%2': You do not have the Windows rights.
50111	Error	Impossible to restore in the folder '%2': You do not have the Windows rights.

Driver

Numéro	Type	Description
50100	Warning	File '%2' cannot be opened using '%3'.
50101	Error	A timeout occured while trying to open the file '%2' using '%3'.
50502	Error	Team service request failed: '%2' using '%3'.

Appendix B. Migration procedure of Security BOX Suite 6.x, 7.x, 8.0.x and 9.x to 9.3

It is important to apply the following procedure because the parameters of the sections [DirectoryUpdate], [File] and [Team] which were included in the *SBox.ini* file before the 8.0.2 version are now configured in the user account. If this procedure is not applied, these parameters could be ignored.

To migrate to 9.3 version:

1. Update Security BOX Authority Manager to Stormshield Data Security 9.3 version following the procedure in Stormshield Data Authority Manager guide.
2. Configure the new parameters of the sections [Directory], [File] and [Team] of the template in Stormshield Data Authority Manager.
3. Update Security BOX Suite to Stormshield Data Security 9.3 version on client workstations.

   NOTE
   For versions strictly previous to 8.0.1, you need to uninstall first the version before installing the 9.3 version.
4. Distribute the *.usx* file of the template from Stormshield Data Authority Manager.

   NOTE
   Between steps 3 and 4 of the procedure, migrated parameters are no longer taken into account by Stormshield Data Security because they are no longer read in the *SBox.ini* file and are not yet included in the account parameters. It is thus important to apply these two steps in a row as far as possible.

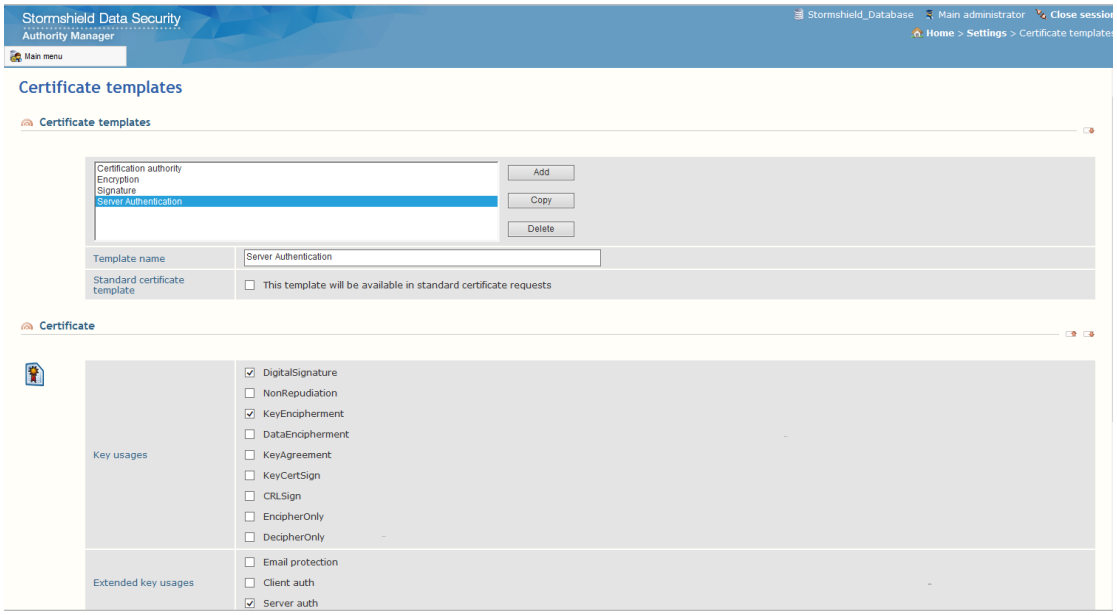
Appendix C. LDAPS configuration

The procedure below applies to Stormshield Data Security as well as to Stormshield Data Security, if the LDAPS protocol is enabled.

C.1. Creating certificates for authentication through Stormshield Data Authority Manager

In order to use the LDAPS protocol with certificates requiring certification authorities external to the Active Directory server, certificates with extended usages must be generated from the Stormshield Data Authority Manager administration interface. For more information about Stormshield Data Authority Manager, refer to the user guide.

1. When connected to Stormshield Data Authority Manager, select **Settings** and **Certificate templates**.
2. Add a new template called "Server authentication".
3. Select the usages **DigitalSignature**, **KeyEncipherment** and **Server auth**.



4. Add another certificate template called "Client authentication" and select the usages **DigitalSignature**, **KeyEncipherment** and **Client auth**.
5. Then go to the section **Users management>Users>Users creation>Advanced creation** in order to create two users.
6. For the first user, in the **Name** field, enter the DNS name of the LDAP server and leave the **Given name** field empty. In the **Keys and certificates** section, select **Server authentication** in the **Key 1** field. Leave the **Key 2** field empty.
7. For the second user, repeat the previous step but select **Client authentication** in the **Key 1** field. The certificate associated to this user will be assigned to client workstations equipped with Stormshield Data Security.
8. Export the keys generated for both users.
9. Export the certificates of all the trust chain of these users from the **Certification authority** section.

C.2. Adding keys and authority certificates in the Windows certificate store

In LDAPS authentication mode, the server provides its certificate to the client in order to be validated. Stormshield Data Security and Stormshield Data Authority Manager use the Windows certificate store to check the parent-child relationship of the server's certificate.

The procedure below allows importing keys and certificates of the trust chain in the Windows store. This procedure must be executed on:

- the Active Directory server
- the Stormshield Data Authority Manager server
- the client workstations equipped with Stormshield Data Security.

1. Open the program Microsoft Management Console (MMC) as an administrator preferably (enter *mmc.exe* in the **Windows Start/Run menu**).
2. Select **File** and **Add/Remove Snap-in** (keyboard shortcut: Ctrl+M).
3. In the left column, select **Certificates** and click **Add**.
4. The Snap-in window opens:

- For the Active Directory server:
  - Select **A service account** and click **Next**.
  - Choose **Local computer (...)** and then click **Next**.
  - Chosse **Active Directory Domain Services** and click **Finish**.
- For the Active Directory server and the Stormshield Data Authority Manager server:
  - Select **Computer account** and click **Next**.
  - Choose **Local computer (...)** and then click **Finish**.
- For client workstations equipped with Stormshield Data Security:
  - Select **My user account** and click **Finish**.

5. Expand the content of **Certificates (local computer)** or **Certificates – Current User**.
6. Import the root authority certificate associated to the LDAP certificates in the **Trusted Root Certification Authorities** store.
7. Import the other parent authority certificates in the **Intermediate Certification Authorities** store.
8. Import the Stormshield Data Authority Manager server key previously saved in the local computer personal certificate store of the Authority Manager server.
9. Import the Stormshield Data Security workstation key previously saved in the workstation personal certificate store.
10. Import the Active Directory server key previously saved in the personal certificate store of the Active Directory server.
11. When you exit MMC, select **No** to answer the console settings saving request.

NOTE

For Stormshield Data Security, it is also possible to add certificates in the local computer store. The checking process of the server's certificate searches the current user's store in a transparent way and then the local computer's store if needed.

C.3. Configuring the SSL protocol for Stormshield Data Security

After importing keys and certificates on workstations and servers, you can set up Stormshield Data Security and Stormshield Data Authority Manager to be able to use the SSL protocol:

1. In Stormshield Data Authority Manager, in **Settings > LDAP synchronization**, enable the option **SSL**.
2. In **User management > Templates > Components > Stormshield Data Kernel > Directory > LDAP directories**, replace 389 by 636 in the **Port** field so that the Stormshield Data Security directory uses this port which will activate the LDAPS over TLS.

Appendix D. Information to provide when reporting a problem

In the event of a problem on a workstation, you must inform Stormshield Data Security Technical Assistance Center of the exact environment stored on the workstation:

- The version and the language used for Stormshield Data Security.
- The type of version installed: official, evaluation.
- The Stormshield Data Security license number.
- The list of components installed: Mail Edition, File, Virtual Disk, Shredder, Card extension, etc..
- The version, the Service Pack (SP) and the language used for Windows.
- The version and Internet Explorer service pack installed.
- If the Stormshield Data Security Outlook Edition is involved: the version and SP for the Outlook client and the Exchange server.
- If the Stormshield Data Security Notes Edition is involved: the 3-digit version (and possibly one letter) for the Notes client and its Domino server.
- If the Card extension is involved: the card template, the drive type, the name of the PKCS#11 DLL used and its version.

STORMSHIELD

documentation@stormshield.eu