GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

ADVANCED CONFIGURATION GUIDE

Version 11.2

Document last updated: July 30, 2024

Reference: sds-en-sdse-advanced_configuration_guide-v11.2

Table of contents

1. Getting started 4

2. Configuring a security policy in a .json file 5

2.1 Account 5
2.1.1 parameters 5
2.1.2 creation 7
2.1.3 recovery 9
2.2 Policy certificates 9
2.3 Policy directories 10
2.4 Stormshield Data File 12
2.4.1 decryptionList section 13
2.4.2 encryptionList section 14
2.4.3 exclusionList section 16
2.5 Stormshield Data Team 17
2.6 Stormshield Data Disk 19
2.7 Stormshield Data Mail 21
2.8 Stormshield Data Sign 22
2.9 Stormshield Data Shredder 23
2.9.1 exclusionList section 25
2.9.2 shreddingList section 26
2.10 Stormshield Data Share 27
2.11 Directories 28
2.11.1 ldap section 28
2.11.2 pgp section 30
2.12 Certificate revocation 31
2.13 Distribution points 32

3. Configuring advanced settings in the Sbox.ini file 33

3.1 Configuration via Windows group policy 33
3.2 [Logon] 33
3.3 [UpgradeEncipherCardAccount_CertificateTemplate] 36
3.4 [SlotFilter] 36
3.5 [KeyRenewal] 37
3.5.1 User key types 37
3.6 [SBox.KeyRenewalWizardKS]/[SBox.KeyRenewalWizardGP] 38
Types of accounts 38
3.6.1 Parameters 38
3.7 [CoworkerSelector] 40
3.8 [External PKCS11 Policy] 40
3.9 [File] 41
3.10 [Team] 42

4. Configuring advanced settings in the registry base 43

4.1 Changing the dates of the last access 43
4.2 Moving folders available offline 43
4.3 Keeping performance optimal on the workstation 43
4.3.1 Improving performance when browsing encrypted trees 44
4.3.2 Excluding Windows processes that access encrypted folders 44
4.3.3 Excluding Windows Defender extensions and scans 44
4.4 Disabling automatic suggestion of co-workers 45

5. Further reading 46

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

1. Getting started

This guide describes the use of configuration files and the Windows registry base to configure SDS Enterprise security policies.

Stormshield Data Security Enterprise policy settings can be configured in several ways:

- In the **SDMC administration console**, which can be accessed at https://sds.stormshieldcs.eu/admin. The console allows you to create and configure security policies via a graphical interface that feeds the *.json* configuration file. For more information, refer to the *Managing security policies in SDMC* in the Administration guide.
  A number of advanced parameters are not available in SDMC, but only in the different configuration files below.
- Directly in ***.json* configuration files** that contain the large majority of the configuration parameters found in security policies. There is one file per security policy. For more information, refer to the section Configuring a security policy in a .json file.
  All settings in the SDMC administration console can also be configured in the *.json* file.
- In an ***SBox.ini* configuration file** that contains only some advanced parameters. For further information, refer to the section Configuring advanced settings in the Sbox.ini file.
- In the Windows registry base for the Stormshield Data Team feature. For further information, refer to the section Configuring advanced settings in the registry base.

2. Configuring a security policy in a *.json* file

1. Create and configure a security policy in the SDMC administration console. This will generate a file in JSON format with the name of the security policy, e.g., *defaultpolicy.json*. For more information, see section *Managing security policies in SDMC* in the Administration guide.
2. Download the file.
   For more information, see section *Installing SDS Enterprise agents on user workstations* in the Administration guide.
3. Edit the *.json* file and manually modify its parameters. The file is divided into several sections, each of which correspond to a feature in SDS Enterprise. Various parameters are found in these sections.
   The tables below contain the descriptions of the parameters, categorized by feature. Unless otherwise indicated, there must be parameters in the file. The tables also mention whether the parameter exists in the SDMC administration console and where to find it.

2.1 Account

User accounts can be configured in the *accountPolicy* section of the *.json* file, which is divided into several sub-sections: *parameters*, *creation* and *recovery*.

2.1.1 parameters

The operating parameters of user accounts can be configured in the *parameters* section described in the table below. In the SDMC administration console, the equivalent parameters are found in **Policies** > **Accounts** > **Parameters**.

For further information, refer to the section *Configuring generic account settings* in the Administration guide.

Parameter	Type Description	Prescribed values	SDMC
cryptography	Indicates how cryptographic operations are performed when the account is in use. This parameter impacts all functions of SDS Enterprise, except Data Disk.		Encryption and signature
	encryptionAlgorithm: Algorithm to use in encryption operations.	AES-256	Encryption algorithm
	hashAlgorithm: Algorithm to use in signature operations.	SHA-256, SHA-512	Signature algorithm
	keyEncryptionMethod: Optional. Algorithm to use in operations encrypting the keys. Allowed values are: • "RSA-OAEP-SHA-256", default value, • "RSA-OAEP-SHA-1", compatibility value for old cards	RSA-OAEP-SHA-256, RSA-OAEP-SHA-1	N/A
cardAccount	Optional. Indicates how smart card accounts operate. This field appears only if the policy allows connections to smart card accounts.		Card or USB token accounts

Parameter	Type Description	Prescribed values	SDMC
cardMiddlewares	List of middleware programs that can be used on the workstation. Middleware allows SDS Enterprise to communicate with all types of smart cards and USB tokens.		Middleware
	name: Name displayed for this middleware configuration.	String of characters	
	dllname: Name of the DLL containing the middleware. The value is an absolute path to the DLL on the user's workstation. If the DLL is in a folder of the Windows PATH variable, the DLL name will suffice.	String of characters	
	disablePKCS11Label, disablePKCS11Extractable, disablePKCS11Modifiable et disablePKCS11ModulusBits: Parameters that monitor the use of various PKCS#11 attributes during communication with smart cards/USB tokens. These parameters come from the database of known middleware programs on SDMC, and are entered to increase the agent's compatibility with middleware from various vendors. You are advised against modifying the default values provided.	true, false	
	showAllSlots: Indicates whether the "Information" window in the smart card configurator displays information about all logical slots managed by the middleware (true), or only slots with a smart card/token inserted (false).	true, false	
cardFilter	Optional. Filters to be applied to select the right smart card drive when the connection window appears.		Card reader filtering
	manufacturer: String to be used to filter smart card drives by vendor name. The characters * and ? are allowed.	String of characters	Vendor name
	description: String to be used to filter smart card drives by description.	String of characters	Type Description

Parameter	Type Description	Prescribed values	SDMC
accountMode	Indicates the user account types that can be connected. Allowed values are: • "password" for the *password* mode. Keys are stored in the keystore.usr file and protected by a password. • "smartcard" for *smart card* mode. Keys are stored on a smart card or USB token and protected by a PIN. • "SSO" for *single sign-on* mode, in which the account's keys are issued by the Windows keystore. This mode does not require authentication. • "passwordAndSmartcard" for *password* and *smart card* modes.	password, smartcard, SSO, passwordAnd Smartcard	Account type

2.1.2 creation

The creation parameters of user accounts can be configured in the *creation* section described in the table below. In the SDMC administration console, the equivalent parameters are found in **Policies** > **Accounts** > **Creation**.

For further information, refer to the section *Setting account creation parameters* in the Advanced configuration guide.

Parameter	Type Description	Prescribed values	SDMC
accountKeyMode	Indicates the operating mode of accounts when they are created. This parameter does not affect how existing accounts function. Allowed values are: • "singleKeyEncryption" for accounts with a single encryption key, • "singleKeySignature" for accounts with a single signature key, • "dualKey" for accounts with an encryption key and a signature key.	singleKey Encryption, singleKey Signature, dualKey	Key management
passwordAccount Method	Indicates whether password accounts can be created, and how. Allowed values are: • "forbidden" to prohibit the creation of password accounts, • "manual" to allow users to create accounts manually.	forbidden, manual	General Settings Password accounts

Parameter	Type Description	Prescribed values	SDMC
cardAccountMethod	Indicates whether smart card or USB token accounts can be created, and how. Allowed values are: • "forbidden" to prohibit the creation of smart card or token accounts, • "manual" to allow users to create accounts manually, • "automatic" to enable launching the creation of automatic accounts, • "manualAndAutomatic" to combine the creation of manual and automatic accounts.	forbidden, manual, automatic, manualAnd Automatic	General Settings Accounts Card or USB token
passwordAccount	Optional. Indicates password creation settings. This field does not appear if password account creation is prohibited.		Password account creation
passwordStrength	Indicating the strength of the password chosen by the user for the new account.		Password strength
	alphabeticCharMinCount: Minimum number of alphabetic characters that the user's password must contain.	Positive integer.	Minimum number of alphabetic characters
	numericCharMinCount: Minimum number of digital characters that the user's password must contain.	Positive integer.	Minimum number of numeric characters
	specialCharMinCount: Minimum number of special characters that the user's password must contain.	Positive integer.	Minimum number of special characters
	totalCharMinCount: Minimum number of characters that the user's password must contain.	Positive integer.	Minimum number of characters
	allowedKeySources: List of sources from which users can choose keys for their accounts. Allowed values are: • "p12File" so that users will select a P12 file in which the keys to their account are saved, • "selfSignedP12" so that users request SDS Enterprise to generate self-certified keys for their accounts.	p12File, selfSignedP12	Import .p12 certificates Generate .p12 certificates locally
	selfSignedOptions: Optional. Specific parameters relating to the generation of self-certified keys. This field does not appear if the manual creation of password accounts does not allow the use of self-certified keys.		Self-certified certificates

Parameter	Type Description	Prescribed values	SDMC
	baseLifetimeYears: Certificate validity in number of years from their creation date.	Positive integer.	Validity period of self-certified certificates issued by SDS upon account creation
	renewalPeriodYears: Certificate validity in number of years from their renewal date.	Positive integer.	Validity period of self-certified certificates issued by SDS upon key renewal
	keyType: Size of keys generated by SDS Enterprise when the account is created.	RSA-2048, RSA-4096	Key size
automatic	Optional. Settings relating to the automatic creation of accounts. This field may not appear if automatic account creation is prohibited.		Filter CAs on automatic creation
	encryptionKeyAuthorityId: Optional. Unique ID of the authority that issued the encryption keys to be used for creating the account. You will find the ID in the list of authorities in the certificateData section of the *.json* file.	Unique character string	Authority name for decryption
	signatureKeyAuthorityId: Optional. Unique ID of the authority that issued the signature key to be used for creating the account. You will find the ID in the list of authorities in the certificateData section of the *.json* file.	Unique character string	Authority name for signature

2.1.3 recovery

The recovery parameters of user accounts can be configured in the *recovery* section described in the table below. In the SDMC administration console, the equivalent parameters are found in **Policies** > **Accounts** > **Data recovery**.

For more information, see the section *Enabling data recovery* in the Administration Guide.

Parameter	Type Description	Prescribed values	SDMC
certificateIds	Unique ID of the recovery certificate to be added to users for the SDS Enterprise agent's encryption operations. You will find the identifier in the list of certificates in the certificateData section of the *.json* file.	Unique character string	Key management

2.2 Policy certificates

The list of certificates used in the policy is specified in the *certificateData* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the

equivalent parameters are found in **Certificate library**.

For more information on certificates, refer to the section *Managing authority certificates and recovery certificates in SDMC* in the Administration guide.

Parameter	Description	Prescribed values	SDMC
certificateData	List of certificates used in the policy.		
	id : Unique ID of the certificate in the policy. Used in other sections of the *.json* file to identify the certificate. See the example below.	Unique character string.	N/A
	data: Value of the certificate encoded in Base64.	Character string	N/A

Example of a list of two certificates. The first represents the certificate of the authority that issues the keys to be used for creating an automatic account.

```
"certificateData": [
        {
                "id": "0123456789ab-cdef-0123-4567-89abcdef",
                "data": "LS0tLS1CRUdJTiBDRVJU..."
        },
        {
                "id": "fedcba987654-3210-fedc-ba98-76543210",
                "data": "UlEWURDQ0FraWdBd0lCQ..."
        },
]
```

The ID of the first certificate "0123456789ab-cdef-0123-4567-89abcdef" is therefore used as the value in the parameters `encryptionKeyAuthorityId` and `signatureKeyAuthorityId` in the automatic account creation policy (accountPolicy section):

```
"automatic": {
  "encryptionKeyAuthorityId": "0123456789ab-cdef-0123-4567-
89abcdef",
  "signatureKeyAuthorityId": "0123456789ab-cdef-0123-4567-89abcdef"
}
```

2.3 Policy directories

The list of LDAP directories used in the policy is specified in the *ldapData* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in the **LDAP library** panel.

For more information on certificates, refer to the section *Managing LDAP directories in SDMC* in the Administration guide.

Parameter	Description	Prescribed values	SDMC
id	Unique ID of the LDAP directory in the policy. Used in other sections of the *.json* file to identify the directory.	Unique character string.	N/A
configuration	LDAP directory configuration		

Parameter	Description	Prescribed values	SDMC
name	Configuration name.	Character string	Server name
access	LDAP server contact settings.		N/A
	address: Server address.	Character string	Address
	port: Port to use.	Integer between 0 and 65536	Connection port
	protocol: Protocol to use. Allowed values are: • "ldap" for the standard LDAP protocol, • "ldaps" for the secure LDAP protocol, • "ldapsWithFallbackToLdap" to attempt an LDAP connection if the LDAPS connection fails.	ldap ldaps, ldapsWith Fallback ToLdap	Use an LDAPS connection Try to connect with LDAP if LAPS connection fails
credentials	Connection ID.		Access control
	username: User name. The "<Myself>" value makes it possible to use the Windows session identifiers.	Character string	ID
	password: Password. The "<Myself>" value makes it possible to use the Windows session identifiers.	Character string	Password
advanced	Search settings.		Search
	base: Base of an LDAP request.	Character string	Base
	depth: Search depth. Allowed values are: • "minimum" to perform the search on the immediate level in the tree, • "oneLevel" to perform the search on the immediate level and on a lower level only, • "maximum" to perform the search recursively in the tree.	minimum, oneLevel, maximum	Depth
	timeoutSeconds: Timeout of the request before canceling (in seconds).	Positive integer >= 10	Timeout before canceling connection request (in seconds)
searchAttributeNames	Names to use to request various attributes during the search.		Search attribute names

Parameter	Description	Prescribed values	SDMC
	emailAddress: Name of the attribute containing the e-mail address. The default value is "mail".	Character string	E-mail address
	commonName: Name of the attribute containing the common name. The default value is "cn".	Character string	Common name
	certificate: Name of the attribute containing the certificate. The value by default is "usercertificate;binary".	Character string	Certificate

2.4 Stormshield Data File

Stormshield Data File can be configured in the *filePolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > File**.

For more information on configuring this feature, refer to the section *ConfiguringStormshield Data File*in the Administration guide.

Parameter	Type Description	Prescribed values	SDMC
allowEncryptSmart File	Indicates whether the user is allowed to create smartFILE files.	true, false	Allow creation of smartFILE files
allowEncryptionFor Recipient	Indicates whether the user is allowed to encrypt for a recipient.	true, false	Enable file encryption for a recipient
allowFileDecryption	Indicates whether the user is allowed to decrypt files.	true, false	Enable file decryption
allowFileEncryption	Indicates whether the user is allowed to encrypt files.	true, false	Enable file encryption
allowFolderDecryption	Indicates whether the user is allowed to decrypt folders.	true, false	Enable folder decryption
allowFolderEncryption	Indicates whether the user is allowed to encrypt folders.	true, false	Enable folder encryption
allowNetworkDecryption	Indicates whether the user is allowed to decrypt network files.	true, false	Enable network file decryption
allowNetworkEncryption	Indicates whether the user is allowed to encrypt network files.	true, false	Enable network file encryption
allowSelfDecryptable FilesCreation	Indicates whether the user is allowed to create self-decryptable files.	true, false	Enable creation of self-decryptable files
blockedExtensionsOn Opening	Types of files that must first be decrypted before opening.	List of extensions in *.ext* format	N/A

Parameter	Type Description	Prescribed values	SDMC
confirmForEachFile	If several files are being encrypted, indicates whether a confirmation is required for each file.	true, false	Confirm encryption for each file
decryptionList	Specifies the parameters of the automatic file decryption list. To use this list, refer to decryptionList section.		Decryption list
encryptHiddenFiles	Indicates whether hidden files must be encrypted.	true, false	Encrypt hidden files
encryptionList	Specifies the parameters of the automatic file encryption list. To use this list, refer to encryptionList section.		Encryption list
exclusionList	Specifies the parameters of the exclusion list. To use this list, refer to exclusionList section.		Exclude list
fileFormat	Format of the encrypted file.	sdsx, sbox	Encryption format
readOnlyFilesEncryption	Indicates how to process read-only files.	treatAsUsual, askConfirmation, doNotEncryptBut Notify, neitherEncrypt NorNotify	Process normally like standard files, Request confirmation, Notify but do not encrypt, Neither notify nor encrypt

2.4.1 decryptionList section

Files included in decryption lists are automatically decrypted at a predetermined time or when a predetermined event takes place. The following parameters are specified in the *filePolicy.decryptionList* section of the *.json* file.

Parameter	Type Description	Prescribed values	SDMC
askConfirmation	Indicates whether a confirmation is required before automatic decryption.	true, false	Ask confirmation before performing automatic decryption
displayReport	Indicates whether to display a report after automatic decryption.	true, false	Display report after performing automatic decryption
files	List of files to decrypt automatically.		Files decrypted automatically

Parameter	Type Description	Prescribed values	SDMC

	path: File path. To indicate several files, the “files” list must contain several objects, each with a different “path” property. For example:
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		String	File path

folders	List of folders to decrypt automatically.		
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	Folder path or mask
	recursive: Indicates whether sub-folders are included in the decryption list.	true, false	Include sub-folders
masks	List of masks to decrypt automatically. To indicate several masks, this parameter must be used several times. See the "files" parameter.		
	path: Mask path. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	Folder path or mask
	recursive: Indicates whether sub-folders are included in the decryption list.	true, false	Include sub-folders
onConnection	Decrypts the list of files upon connection to SDS Enterprise.	true, false	Decrypts automatically upon connection to the SDS Enterprise account
onScreenSaverOver	Decrypts the list of files when screensaver stops.	true, false	Decrypt automatically when screensaver stops
onSessionUnlock	Decrypt the list of files when unlocking session.	true, false	Decrypt automatically when unlocking session

2.4.2 encryptionList section

Files included in encryption lists are automatically encrypted at a predetermined time or when a predetermined event takes place. The following parameters are specified in the *filePolicy.encryptionList* section of the *.json* file.

Parameter	Type Description	Prescribed values	SDMC
askConfirmation	Indicates whether a confirmation is required before automatic encryption.	true, false	Ask confirmation before performing automatic encryption
displayReport	Indicates whether to display a report after automatic encryption.	true, false	Display report after performing automatic encryption
files	List of files to encrypt automatically.		Files encrypted automatically

	path: File path. To indicate several files, the “files” list must contain several objects, each with a different “path” property. For example:
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		String	File path

fixedTimesInSeconds	List of times at which files are automatically encrypted. Expressed in number of seconds from 00:00. For example, 1:30 a.m. is represented by a value of 5400.	List of positive whole integers	N/A
folders	List of folders to encrypt automatically.		
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	Folder path
	recursive: Indicates whether sub-folders are included in the encryption list.	true, false	Include sub-folders
intervalMinutes	Frequency with which files are automatically encrypted. Expressed in minutes.	Positive integer.	Automatic encryption frequency
masks	List of masks to encrypt automatically.		
	path: Mask path. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	Folder path or mask
	recursive: Indicates whether sub-folders are included in the encryption list.	true, false	Include sub-folders

Parameter	Type Description	Prescribed values	SDMC
onDisconnection	Enables list when disconnecting from SDS Enterprise.	true, false	Encrypt automatically when disconnecting from the SDS Enterprise account
onScreenSaverStarted	Enables the list when screensaver starts.	true, false	Encrypt automatically when screensaver starts
onSessionLock	Enables the list when locking the SDS Enterprise session.	true, false	Decrypt automatically when locking session

2.4.3 exclusionList section

Using an exclusion list, you can exclude some files to prevent them from being encrypted by mistake. The following parameters are specified in the *filePolicy.exclusionList* section of the *.json* file.

Parameter	Type Description	Prescribed values	SDMC
displayWarning	Indicates whether a warning window must be displayed if an operation could not be completed because of the exclusion list.	true, false	Display warning when encryption is rejected
files	List of files to be excluded from encryption.		Files excluded from encryption
	askForConfirmation: Indicates whether confirmation must be requested for the encryption of excluded files.	true, false	N/A

	path: File path. To indicate several files, the “files” list must contain several objects, each with a different “path” property. For example:
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		String	File path

folders	List of folders to be excluded from encryption.		Folders or masks excluded from encryption
	askForConfirmation: Indicates whether confirmation must be requested for the encryption of excluded folders.	true, false	N/A
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	File path

Parameter	Type Description	Prescribed values	SDMC
	recursive: Indicates whether sub-folders are included in the exclusion list.	true, false	Include sub-folders
masks	List of masks to be excluded from encryption.		Folders or masks excluded from encryption
	askForConfirmation: Indicates whether confirmation must be requested for the encryption of excluded files.	true, false	N/A
	path: Path of the mask with the "*.ext" extension to apply the mask. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	File path
	recursive: Indicates whether sub-folders are included in the exclusion list.	true, false	Include sub-folders

2.5 Stormshield Data Team

Stormshield Data Team can be configured in the *teamPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Team**.

For more information on configuring this feature, refer to the section *Configuring Stormshield Data Team* in the Administration guide.

Parameter	Description	Prescribed values	SDMC
accessToEncryptedFile	Indicates the accessibility of an encrypted file. Allowed values are: • "always" to access it regardless of the certificate status, • "notIfRevokedOrCrlExpired" to deny access if the encryption key is revoked or the CRL is not available, • "notIfCertificateHasAnIssue" to deny access if the certificate has a warning or error.	always, notIfRevokedOrCrlExpired, notIfCertificateHasAnIssue	Users can access an encrypted file regardless of the status of their certificate, Users cannot access an encrypted file if the certificate of their encryption key is revoked or if the revocation list is not available, Users cannot access an encrypted file if their certificate displays a warning or an error.

Parameter	Description	Prescribed values	SDMC
allowDecryption	Indicates whether file decryption is allowed.	true, false	Allow encryption
allowDeletion	Indicates whether file deletion is allowed.	true, false	Allow deletion
allowEncryptionAccordingToDefinedRules	Indicates whether encryption is allowed according to the rules defined.	true, false	Allow encryption according to the rules defined
allowSaveAndRestore	Indicates whether backups and restorations are allowed.	true, false	Allow save and restore
closeReportWindow	Indicates when to close the report window. Allowed values are: • "always" for the window to close after encryption, • "ifNoWarning" for the window to remain displayed when there is a warning, • "never" for the window to remain displayed after encryption.	always, ifNoWarning, never	Closing the report window
excludedFolders	Optional. List of folders to be excluded. This list is recursive.	Character string	N/A
ignoredApplications	Optional. List of applications to be ignored.	Character string	N/A
openEncryptedFileInUnsecuredFolder	Defines the behavior when opening an encrypted file in a non-secure folder. Allowed values are: • "allow" to allow it, • "deny" to prohibit it, • "readonly" to allow it in read-only mode.	allow, deny, readOnly	Opening encrypted files in a non-secured folder
reencryptFilesWhenRemovingCoworkers	Indicates whether files will be encrypted again if a co-worker is removed from the rule.	true, false	Encrypt again files when removing coworkers from a rule

Parameter	Description	Prescribed values	SDMC
secureDragAndDrop	Defines the behavior when files or folders covered by a Data Team rule are copied or moved to a non-secure folder. Allowed values are: • "keepCurrentRule" to apply the rule of the destination folder after moving or copying, • "forbidden" to prohibit copying or moving, • "noDecryption" to not decrypt the file after moving or copying.	keepCurrentRule, forbidden, noDecryption	Decrypt when copying or moving, Prohibit copying or moving, Keep encryption when copying or moving
setCreationDateToCurrentDate	Indicates whether the creation date must be the current date.	true, false	Set creation date to current date
setModificationDateToCurrentDate	Indicates whether the modification date must be the current date.	true, false	Set modification date to current date
showCoworkers	Indicates when the rule is displayed. Allowed values are: • "always" so that all users can display the rule, • "onlyIfUserIsACoworker" so that only co-workers in the rule can show the rule,	always, onlyIfUserIsACoworker	Show co-workers
showSuccessfullyProcessedFiles	Indicates whether correctly encrypted files are shown in the progress window.	true, false	Show encrypted files in the progress window
updateCoworkerKeyInKnownRules	Indicates whether the co-worker's key is updated in the known rules after a key renewal.	true, false	Update a coworker's key in the known rules if the key has been renewed
useLocalCertificateState	Indicates whether the status of the local certificate in the cache must be used if the CRL cannot be downloaded, or if it has expired.	true, false	Use local certificate state in cache if the revocation list cannot be downloaded or if it is expired

2.6 Stormshield Data Disk

Stormshield Data Disk can be configured in the *diskPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Disk**.

For more information on configuring this feature, refer to the section *Configuring Stormshield Data Disk* in the Administration guide.

Parameter	Type Description	Prescribed values	SDMC
allocationUnitKB	Size of the NTFS clusters used in the virtual disk.	0, 512, 1024 and 4096	N/A
automaticCreation	Optional. Makes it possible to automatically create a volume for a user who connects for the first time.		
	autoMount: Enables or disables the automatic mounting of the volume every time the user connects.	true, false	Mount the volume automatically when the user connects to SDS
	mountLetter: Letter used for the mounted disk. If the letter is not available, the first letter available in reverse alphabetical order will be taken (starting with Z).	letter between D and Z	Drive letter
	showFinalReport: Enables or disables the display of a final report.	true, false	Display a report after the creation
	sizeMB: Optional. Size in MB to allocate to the volume to be created. If no value is entered, the size will amount to 10% of the available size on the client workstation.	Positive integer.	Volume size
	vboxFullPath: Name and location of the special encrypted .vbox file on which the volume relies.	Path	Full path to the .vbox file associated with the volume
enableCompression	Indicates whether compression of the volume is allowed.	true, false	N/A
enableQuickCreation	Indicates whether quick creation is allowed.	true, false	N/A
enableQuickFormat	Indicates whether quick format is allowed.	true, false	N/A
enableRescueFileModification	Indicates whether modification of vboxsave backup files is allowed.	true, false	N/A
enableExpertMode	Indicates whether modification of vboxsave backup files is allowed in the associated vbox directory.	true, false	N/A
fileSystem	File system used for mounted volumes.	NTFS, FAT32, FAT	File system
maxSizeMB	Maximum size allowed for the creation of a volume in MB.	Positive integer.	Maximum size allowed

Parameter	Type Description	Prescribed values	SDMC
mountAsNonRemovable	Indicates whether the mounted disk will be removable.	true, false	Mount volumes as non removable disks
volumeName	Name given to created volumes. By default "SDSDiskVolume".	String	Volume name
encryptionAlgorithm	Indicates the encryption mode used for the volume. Allowed values are: • "AES-256" for the AES CBC encryption mode (default value), • "AES-XTS-256" for the AES-XTS encryption mode offering a better data protection and recommended by the ANSSI.	[AES-256], AES-XTS-256	N/A

2.7 Stormshield Data Mail

Stormshield Data Mail can be configured in the *mailPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies** > **Features** > **Mail**.

For more information on configuring this feature, refer to the section *ConfiguringStormshield Data Mail* in the Administration guide.

Parameter	Type Description	Prescribed values	SDMC
enableSMime	Indicates whether messages encrypted with S/MIME can be sent and received. Currently, this parameter has no effect and will be operational in a future version.	true, false	N/A
enablePGP	Indicates whether messages encrypted with PGP can be sent and received.	true, false	Allow PGP messages encryption/decryption
encryptByDefault	Indicates whether encryption must be automatically enabled when new messages are being composed.	true, false	Enable messages encryption by default
signByDefault	Indicates whether signing must be automatically enabled when new messages are being composed.	true, false	Enable messages signature by default
signatureType	Type of signature to use when composing signed messages.	clear, opaque	Type of signature to sign messages (S/MIME only)

Parameter	Type Description	Prescribed values	SDMC
updateAddressBookWithSignedMailCertificates	Indicates whether the signature certificate associated with the e-mail address is imported into the user's trusted address book, and whether it is imported automatically or manually by the user.		
	automatic Allowed values are: • "trustedAuthorities" to import certificates with a trusted issuer, • "no" to not import certificates.	trusted Authorities, no	Allow automatic updates of the trusted address book: • Only for known authorities • No
	manual Allowed values are: • "anyAuthority" to allow the import of certificates from any source, • "trustedAuthorities" to import certificates with a trusted issuer, • "no" to not import certificates.	anyAuthority, trustedAuthorities, no	Allow manual update of the trusted address book: • For all authorities, • Only for known authorities, • No
keepSignatureOnSecurityDeletion	Indicates whether the signature of a message must be kept when its protection is lifted.	true, false	N/A
showOperationInProgressDialog	Indicates whether a loading window must be shown whenever an operation lasts longer than three seconds.	true, false	N/A

2.8 Stormshield Data Sign

Stormshield Data Sign can be configured in the *signPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Sign**.

For more information on configuring this feature, refer to the section *Configuring Stormshield Data Sign* in the Administration guide.

Parameter	Description	Prescribed values	SDMC
allowCoSigning	Indicates whether the user is allowed to co-sign files.	true, false	Allow file co-signature
allowCounterSigning	Indicates whether the user is allowed to counter-sign files.	true, false	Allow file counter-signature
allowOverSigning	Indicates whether the user is allowed to over-sign files.	true, false	Allow file over-signature

Parameter	Description	Prescribed values	SDMC
allowSigning	Indicates whether the user is allowed to sign files.	true, false	Allow file signature
allowSigningOnActive Content	Indicates whether the user is allowed to sign files containing active content.	true, false	Allow file signature when active content is detected
defaultSignExtension	Default file extension for signed files.	".p7f", ".p7m"	Default file extension
displayDocument BeforeSigning	Indicates whether the user must view a file before signing it.	true, false	Always show file before signing
informUserAboutActive ContentInWordFiles	Indicates whether the user must be informed that a Word file contains active content before being able to sign it. This parameter applies only to files in Microsoft Word version 2000 and higher.	true, false	Inform user when active content is detected in the Microsoft Word file before signing
informUserAbout MacrosInPdfFiles	Indicates whether the user must be informed that a PDF file contains macros before being able to sign it.	true, false	Inform user when macros are detected in the PDF file before signing
informUserAbout MacrosInWordFiles	Indicates whether the user must be informed that a Word file contains macros before being able to sign it. This parameter applies only to files in Microsoft Word versions 97 to 2003.	true, false	Inform user when macros are detected in the Microsoft Word file before signing
preselectMailToAsk ForSignature	When the document signature process is ended, the user can request the preparation of an e-mail addressed to co-workers 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-signers' email addresses; This option relates to the check box in the signature wizard.	true, false	N/A
preselectMailTo NotifyCoWorkers	When the document signature process is over, the user may request the preparation of an e-mail addressed to co-workers in order to ask them to sign the document. This option relates to the check box in the signature wizard.	true, false	N/A

2.9 Stormshield Data Shredder

Stormshield Data Shredder can be configured in the *shredderPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Shredder**.

For more information on configuring this feature, refer to the section *ConfiguringStormshield Data Shredder* in the Administration guide.

Parameter	Type Description	Prescribed values	SDMC
addDesktopIcon	Indicates whether a Stormshield Data Shredder shortcut will be added to the Windows desktop to enable dragging and dropping.	true, false	Add desktop shortcut
allowBinShredding	Indicates whether the user is allowed to shred files in the bin.	true, false	N/A
allowDragAndDropOn ShredderIcon	Indicates whether the user is allowed to shred files by dragging and dropping on the Shredder icon.	true, false	Enable dragging and dropping items on the SD Shredder icon
allowFileShredding	Indicates whether the user is allowed to shred files.	true, false	Allow file shredding
allowFolderShredding	Indicates whether the user is allowed to shred folders.	true, false	Allow folder shredding
allowShredding Interruption	Indicates whether the user is allowed to interrupt shredding operations.	true, false	Allow the interruption of shredding operations
confirmForEachFile	If several files are being shredded, indicates whether user confirmation is required for each file.	true, false	Confirm for each file Confirm only once for all files
exclusionList	Specifies the parameters of the exclusion list. To use this list, refer to exclusionList section.		N/A
readOnlyFilesShredding	Indicates how to process read-only files. Allowed values are: • "neitherShredNorNotify" to neither shred the file nor notify the user, • "doNotShredButNotify" to not shred the file but notify the user, • "askConfirmation" to request confirmation before shredding, • "treatAsUsual" to shred according to the same rules applied to other files.	neitherShred NorNotify, doNotShred ButNotify, askConfirmation, treatAsUsual	Never shred Report the files Ask confirmation Process like standard files
shredHiddenFiles	Indicates whether the user is allowed to shred hidden files.	true, false	N/A
shreddingPatternBytes	Bits used to replace the content of shredded files	List of positive integers between 0 and 255	N/A

2.9.1 exclusionList section

Using an exclusion list, you can exclude some files to prevent them from being shredded by mistake. The following parameters are specified in the *shredderPolicy.exclusionList* section of the *.json* file. This list is optional.

Parameter	Type Description	Prescribed values	SDMC
displayWarning	Indicates whether a warning window must be displayed if an operation could not be completed because of the exclusion list.	true, false	N/A
files	Optional. List of files to be excluded from shredding.		N/A
	askForConfirmation: Indicates whether confirmation must be requested for the shredding of excluded files.	true, false	N/A

	path: File path. To indicate several files, the “files” list must contain several objects, each with a different “path” property. For example:
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		String	N/A

folders	Optional. List of folders to be excluded from shredding.		N/A
	askForConfirmation: Indicates whether confirmation must be requested for the shredding of excluded folders.	true, false	N/A
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	N/A
	recursive: Indicates whether sub-folders are included in the exclusion list.	true, false	N/A
masks	Optional. List of masks to be excluded from shredding.		N/A
	askForConfirmation: Indicates whether confirmation must be requested for the shredding of excluded files.	true, false	N/A
	path: Path of the mask with the "*.ext" extension to apply the mask. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	N/A

Parameter	Type Description	Prescribed values	SDMC
	recursive: Indicates whether sub-folders are included in the exclusion list.	true, false	N/A

2.9.2 shreddingList section

Files included in shredding lists are automatically shredded at a predetermined time or when a predetermined event takes place. The following parameters are specified in the *shredderPolicy.shreddingList* section of the *.json* file.

Parameter	Type Description	Prescribed values	SDMC
askConfirmation	Indicates whether a confirmation is required before automatic shredding.	true, false	N/A
displayReport	Indicates whether to display a report after automatic shredding.	true, false	N/A
files	Optional. List of files to shred automatically.		N/A

	path: File path. To indicate several files, the “files” list must contain several objects, each with a different “path” property. For example:
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		String	N/A

fixedTimesInSeconds	List of times at which files are automatically shredded. Expressed in number of seconds from 00:00. For example, 1:30 a.m. is represented by a value of 5400.	List of positive whole integers	N/A
folders	Optional. List of folders to shred automatically		N/A
	path: Folder path. To indicate several folders, this parameter must be used several times. See the "files" parameter.	String	N/A
	recursive: Indicates whether sub-folders are included in the shredding list.	true, false	N/A
intervalMinutes	Optional. Frequency with which files are automatically shredded. Expressed in minutes.	Positive integer.	N/A

Parameter	Type Description	Prescribed values	SDMC
masks	Optional. List of masks to shred automatically.		N/A
	path: Path of the mask with the "*.ext" extension to apply the mask. To indicate several masks, this parameter must be used several times. See the "files" parameter.	String	N/A
	recursive: Indicates whether sub-folders are included in the shredding list.	true, false	N/A
onDisconnection	Enables automatic shedding when disconnecting from SDS Enterprise	true, false	N/A
onScreenSaverStarted	Enables automatic shredding when screensaver starts.	true, false	N/A
onSessionLock	Enables automatic shredding when locking SDS Enterprise session.	true, false	N/A

2.10 Stormshield Data Share

Stormshield Data Share can be configured in the *sharePolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Features > Share**.

For more information on configuring this feature, refer to the section *ConfiguringStormshield Data Share* in the Administration guide.

Parameter	Type Description	Prescribed values	SDMC
• dropboxPolicy • oodrivePolicy • oneDrivePolicy • oneDriveForBusinessPolicy • sharepointPolicy	Indicates how SDS Enterprise must protect Dropbox, Oodrive, OneDrive, OneDrive for Business and SharePoint shared spaces. Each of these parameters is a separate object whose individual properties are detailed in the following lines.		• Dropbox • OneDrive • OneDrive for Business • SharePoint • OoDrive
	protect: Indicates whether the synchronized space must be automatically protected.	true, false	Enable/Disable the button 

Parameter	Type Description	Prescribed values	SDMC
	subfoldersToProtect: Specifies the list of sub-folders to be protected in the shared space. Applies only if `"protect" : true`. An empty list means that the entire shared space is protected. Examples: • `[ "Documents" ]` • `[ "Folder1", "Folder2\SubFolder" ]`	List of strings	Advanced

2.11 Directories

The directories to be used to provide user certificates are defined in the *directories* section of the *.json* file, which is divided into several sub-sections: *ldap* and *pgp*.

For more information on configuring this feature, refer to the section *Configuring corporate directories* in the Administration guide.

2.11.1 ldap section

LDAP directories are configured in the *ldap* section described in the table below. In the SDMC administration console, the equivalent parameters are found in **Policies** > **Directories** > **LDAP**.

Parameter	Type Description	Prescribed values	SDMC
addWildcardSuffix InFilter	Indicates whether search criteria must have the suffix "*".	true, false	Suffix search criteria by "*"
addWildcardPrefix InFilter	Indicates whether search criteria must have the prefix "*"	true, false	N/A
addUserCertificate BinaryFilter	Indicates whether "usercertificate;binary=*" must be added to the search filter to return only LDAP entities that have a certificate.	true, false	N/A
ldapAddressBookList	List of unique IDs in LDAP directories accessible to users. You will find the IDs in the list of LDAP directories in the ldapData section of the *.json* file.	List of unique character strings.	Add from library
automaticUpdate	Optional. Indicates how to manage updates of the trusted address book and its certificates. Automatic updates are applied only if all parameters are fulfilled.		Update the directory automatically
	downloadCrlsUponVerification: Indicates whether the CRL must be downloaded when verifying the certificate.	true, false	N/A
	onPeriodicHours: Frequency with which updates are performed (in hours).	Positive integer between 1 and 24	Update frequency

Parameter	Type Description	Prescribed values	SDMC
	onUserConnection: indicates whether the update begins when the user logs in.	true, false	Start the directory update when the user connects to the SDS account
	updateValidCertificatesWithNewerOnes: Indicates whether valid certificates must be updated with more recent certificates.	true, false	Update certificates saved in the trusted directory with most recent certificates from an LDAP directory
	updateOnlyFromCAs: Optional. List of unique IDs of authorities from which updates are to be applied. You will find the IDs in the list of authorities in the certificateData section of the *.json* file. If this field is empty, all authorities will be taken into account.	List of character strings, each of which corresponds to the "id" field of an object in the "certificateData" list of the policy.	N/A
	expiredCertificates: Indicates how to manage the deletion of expired certificates.		Deletion of expired certificates
	updateWithNewerOnes: Indicates whether they must be updated with more recent certificates. This criterion is based on the list provided by the parameter "updateOnlyFromCAs".	true, false	Update expired certificates
	removeFromLocalDirectory: Indicates whether the certificate must be removed from the local directory.	true, false	Delete automatically
	removeOnlyFromCAs: Optional. List of unique IDs of authorities from which deletion will be applied. You will find the IDs in the list of authorities in the certificateData section of the *.json* file. If this field is empty, all authorities will be taken into account.	List of character strings, each of which corresponds to the "id" field of an object in the "certificateData" list of the policy.	Selection of CAs that issue certificates to be deleted automatically when they expire
	revokedCertificates: Indicates how to manage the deletion of expired certificates.		Deletion of certificates revoked

Parameter	Type Description	Prescribed values	SDMC
	updateWithNewerOnes: Indicates whether they must be updated with more recent certificates. This criterion is based on the list provided by the parameter "updateOnlyFromCAs".	true, false	Update revoked certificates
	removeFromLocalDirectory: Indicates whether the certificate must be removed from the local directory.	true, false	Delete automatically
	removeOnlyFromCAs: Optional. List of unique IDs of authorities from which deletion will be applied. You will find the IDs in the list of authorities in the certificateData section of the *.json* file. If this field is empty, all authorities will be taken into account.	List of character strings, each of which corresponds to the "id" field of an object in the "certificateData" list of the policy.	Selection of CAs issuing certificates to delete automatically when they are revoked
	missingCertificates: Indicates how to manage the deletion of absent certificates. The parameters are the same as those for "expiredCertificates" (see above).		Deletion of certificates removed from the LDAP directory
	updateWithNewerOnes: Indicates whether they must be updated with more recent certificates. This criterion is based on the list provided by the parameter "updateOnlyFromCAs".	true, false	Update missing certificates when searching for coworkers
	removeFromLocalDirectory: Indicates whether the certificate must be removed from the local directory.	true, false	Delete automatically
	removeOnlyFromCAs: Optional. List of unique IDs of authorities from which deletion will be applied. You will find the IDs in the list of authorities in the certificateData section of the *.json* file. If this field is empty, all authorities will be taken into account.	List of strings	Selection of CAs issuing certificates to delete automatically when they are removed from the LDAP directory

2.11.2 pgp section

Files included in decryption lists are automatically decrypted at a predetermined time or when a predetermined event takes place. The following parameters are specified in the *directories.pgp* section of the *.json* file.

Parameter	Type Description		SDMC
wkdServers	Parametric URLs to servers hosting public keys that can be accessed by the WKD (Web Key Directory) schema. They must be in the following form, the sections in bold being kept as is: • WKD "advanced": **https://openpgpkey**.optional-sub-domains.domain.toplevel**/.well-known/openpgpkey/<d>/hu/<k>**?get_parameters=optional • WKD "direct": **https://**optional-sub-domains.domain.toplevel**/.well-known/openpgpkey/hu/<k>**?get_parameters=optional	List of strings	WKD servers

2.12 Certificate revocation

Revocation can be configured in the *revocationPolicy* section of the *.json* file. The table below describes its parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Authorities**.

For more information on how to configure the feature, refer to the section *Configuring certificate revocation control* in the Administration guide.

Parameter	Type Description	Prescribed values	SDMC
checkCertificateRevocation	Optional. Indicates whether certificate revocation must be verified.	true, false	N/A
displayWarningDBCorrupted	Shows a warning message when the local CRL database is corrupted.	true, false	N/A
displayWarningDBDeleted	Shows a warning message when the local CRL database has been erased.	true, false	N/A
fileTimeOutInSeconds	Maximum time in seconds allocated to downloading the CRL from a file.	Positive integer.	N/A
httpTimeOutInSeconds	Maximum time in seconds allocated to downloading the CRL from an HTTP link.	Positive integer.	N/A
issuers	List of authority certificates and recovery certificates to be used in your policies.		
	certificateID: Unique ID of the certificate in the policy. You will find the identifier in the list of certificates in the certificateData section of the *.json* file.	Unique character string	

Parameter	Type Description	Prescribed values	SDMC
	crlDownloadFrequency: Frequency with which the CRL is downloaded. Allowed values are: • "onFirstCryptoOperation" (default value) the first time an encryption or decryption operation is conducted, • "WhenExpired" when the certificate expires, • "always" every time a certificate is used, • "never" never download the CRL.	OnFirst Crypto Operation, WhenExpired, Always, Never	N/A
	methods: List of CRL download methods.		Add from library
	type: Type of revocation method.	"CRL" "OCSP"	N/A
	url: URL used for the download.	String	N/A
ldapTimeOutInSeconds	Maximum time in seconds allocated to downloading the CRL from a LDAP link in seconds.	Positive integer.	N/A
validityDurationInDays	CRL validity in days.	Positive integer. (max 365)	Validity period of revocation lists

2.13 Distribution points

Policy distribution points can be configured in the *distributionPointPolicy* section of the *.json* file. The table below describes their parameters. In the SDMC administration console, the equivalent parameters are found in **Policies > Distribution**.

For further information, refer to the section *Configuring policy distribution points* in the Administration guide.

Parameter	Description	Prescribed values	SDMC
urls	List of URLs indicating the full path(s) to the *.jwt* policy file of your choice. SDS Enterprise checks the list of distribution points in the order you have set. It will apply the first valid policy that it detects. URLs must have an http://, https://, or file:// prefix and must be separated by commas. For example: `"http://test.com/file.jwt", "file://10.1.1.1/file.jwt"`	List of URLs	Full path to the policy file

3. Configuring advanced settings in the *Sbox.ini* file

Some advanced parameters are managed in the *SBox.ini* configuration file found in the folder *Program Files\Arkoon\Security BOX\Kernel*.

The file is divided into several sections, each of which correspond to a feature in SDS Enterprise. Various parameters are found in these sections.

The tables below contain the descriptions of the parameters, categorized by feature. When editing the file, please comply with the following conditions:

- If an optional value in the configuration file is invalid, the default value is used.
- The *SBox.ini* file does not support Unicode characters. As a result, the configured paths can contain only ANSI characters, except / * ? < > " | ! # @. However, these characters can be inserted between quotes.
- After you have modified the *SBox.ini* file, we recommend that you reboot the computer to ensure that all of the changes are applied.

3.1 Configuration via Windows group policy

You can also define the configuration settings of the *SBox.ini* file through the Windows **Group Policy** (GPO), in the "Machine" settings, or in the "User" settings.

NOTE
Stormshield recommends setting 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.

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

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

SDS Enterprise 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.

3.2 [Logon]

Parameter	Description
AllowCard	Allows a connection to SDS Enterprise in smart card or USB token mode: • 0: not allowed (default), • 1: allowed.

Parameter	Description
ConnectOnCard	Displays the SDS Enterprise connection window after inserting a smart card or token and entering the PIN: • 0: not displayed (by default), • 1: displayed. The window does not appear when there is already an SDS Enterprise account logged in (password or smart card/token).
UnfreezeOnCard	Displays the card unlocking window when a smart card or token is inserted and the user's SDS Enterprise session is locked. • 0: No, • 1: Yes (default). The window is enabled only if the connected user has an SDS Enterprise account in smart card or token mode.
RepairCardAccount	Makes it possible to repair a smart card if only the certificate is available, by renewing the key based on the known CKA_ID in the account.
UpgradeEncipher CardAccount	Automatically adds a signature key to a smart card or USB token account with a single encryption key.
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 SDS Enterprise 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.
AllowLocal Unblock	Authorizes a local unlock if the user's SDS Enterprise session is blocked: • 0: not allowed, • 1: allowed (by default)
AllowDistant Unblock	Authorizes a distant unlock if the user's SDS Enterprise session is blocked: • 0: not allowed, • 1: allowed (by default)
DontShowLicenceKey	Keeps the license key value from displaying in the **About SDS Enterprise** window: • 0: The license key is displayed normally (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.
SlotFilterOn	If several card or token drives are connected to the workstation (e.g., a standard drive and a 3G network card), this makes it possible to use a specific drive by defining a filter to identify it. • 0: Any drive is recognized (default), • 1: Only the drive indicated in the [SlotFilter] section is recognized by SDS Enterprise. For more information, see the section [SlotFilter].

Parameter	Description
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): <Subject of the message> [&body=<accompanying message>] <Authority email address>?subject= More detailed information on the syntax can be found in the documentation for "mailto" links This is an optional parameter. If it is blank, the user must enter the information manually.
ExternalCard Authent	Enables the SDS Enterprise connection window in order to use an external PIN-PAD to enter a PIN (smart card or token mode). • 0: No authentication by external PIN-PAD (default value), • 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),
GUILog	Prohibits entering a password in command line during connection, and prevents the *SBCMD.exe* tool from unlocking the user in command line. • 0: Password entry allowed, • 1: Password entry not allowed.

3.3 [UpgradeEncipherCardAccount_CertificateTemplate]

Parameter	Description

[UpgradeEncipherCardAccount_CertificateTemplate]	Allows to define account certificate template.
	• `KeyUsage`
	Indicates the list of the 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 by `KeyUsage`
	• `ExtendedKeyUsage`
	`ExtendedKeyUsage = <EkuToken> *(, < EkuToken >)`
	`<EkuToken>= <Oid>| <EKUKeyWord>`
	`<EKUKeyWord>= clientAuth | emailProtection`
	<Oid> is the "String" representation for OID
	(Example: 1.3.6.1.5.5.7.3.2)
	NOTE
	If the item is missing, there is no filtering by `extendedKeyUsage`
	• `AuthorityCommonName`
	This item contains the commonName value for the certificate issuer:
	`AuthorityCommonName=< CN for certificate issuer>`

3.4 [SlotFilter]

Parameter	Type Description
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 item is case sensitive. If this field is blank, the data will not be filtered.

Parameter	Type Description
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.

3.5 [KeyRenewal]

The [KeyRenewal] and [SBox.KeyRenewalWizardYYY] sections are for renewing keys for existing SDS Enterprise 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	Type Description
CertLife	Enables or disables the possibility of choosing the target directory in which the file will be encrypted. Allowed values are: • 0: Disabled (default value), • 1: Enabled. If the feature is disabled, the next three parameters will not be applied and the default behavior will be adopted.
Key types	List of keys (type and length) to offer when creating an account. The types of keys are defined using items with values 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 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 ■ KEY_RSA_4096BITS = 111

3.5.1 User key types

The supported key types (the user's private keys) are KEY_RSA_2048BITS and KEY_RSA_4096BITS.

The key type can be:

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

For any given account type, only one key type can be allowed and offered by default.

The types of keys are defined using items with values 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).

Example of a key type configuration:

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
- KEY_RSA_4096BITS= 111111

To avoid being prevented from creating accounts when there are errors in the configuration of the *Sbox.ini* file, the following preferences are 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.

3.6 [SBox.KeyRenewalWizardKS]/[SBox.KeyRenewalWizardGP]

Types of accounts

The following table lists the types of accounts available in SDS Enterprise:

KS1	Password account with a single key to sign and encrypt.
KS2	Password account with two different keys to sign and encrypt.
GP1	Card account with a single key to sign and encrypt.
GP2	Card account with two different keys to sign and encrypt.

3.6.1 Parameters

The following table details the content for each section based on the account type XXX

Parameter	KS	GP	Type Description
Pkcs12Import	#	#	The new account's key (or keys) can be imported from a PKCS#12 file. • 0: No (default), • 1: Yes.
InternalKeys		#	In smart card or USB token mode (GP1 or GP2), keys are extracted: • 0 = by SDS Enterprise, in memory • 1 = by the card (default) **NOTE** When keys are generated via smart card, they may be created by the smart card itself, or in memory, depending on the vendor's implementation or the configuration of the key's *PKCS#11* layer.
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 value: 000.
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.
KeepCardObjects		#	**Do not destroy non-reused objects** check box: • 00 : check box unchecked and grayed out (default), • 01: box unchecked and accessible, • 10: box checked and uneditable, • 11: box checked and accessible.
ExportKeys		#	If a key was not extracted by the smart card or token (if <InternalKeys> = 0), SDS Enterprise may display a window offering to save this key in a PKCS#12 file (to save it) or to copy it in the user's keystore (to be used later). • 0 : page not displayed (default), • 1 : displayed.
NoExtractableK	#	#	At the time of creation, indicates whether the private keys are marked as not being able to be exported: • From the keystore for KS1 and KS2 modes, • From the smart card in GP1 and GP2 modes. Allowed values are: • 0: No (default for KS1 and KS2 modes), • 1: Yes (default for GP1 and GP2 modes).

Parameter	KS	GP	Type Description
DisableCreateSelf	#	#	Prohibits a self-certified key from being used, whether for creating an account or for renewing a key. • 0: Authorizes the extraction of a self-certified key (default), • 1: Prohibits the use of a self-certified key.
AutomaticRenewFromCard			For [SBox.KeyRenewalWizardGP] With a Card or SSO account, when the new encryption or signature key is already in the card or in the user's Windows certificate store, this option allows automatic renewal of the key when the previous one expires: • 0: no automatic renewal (by default), • 1: automatic renewal with user confirmation message, • 2: automatic renewal without user confirmation message. **IMPORTANT** The value 1 allows the user to refuse renewal. However, after a refusal, the update is not proposed. Therefore, using this value is not recommended.

3.7 [CoworkerSelector]

Parameter	Description
EnableResearchByEmail	Enables or disables searching for peers by certificate e-mail address. • 0: does not allow searching by e-mail address (by default), • 1: allows searching by e-mail address.
EmailSeparatorCharacters	Specifies the characters in the e-mail address which are considered space characters, to enable searching by this field. By default, the characters "-", "." and "_" will be replaced with a space character. For example the address john-mark.doe@domain.com will be considered as john mark doe.

3.8 [External PKCS11 Policy]

Parameter	Type Description
CPLCanChangePKCS11	Enables or disables modification of the smart card or token type defined in the **card extension configurator**. • 0: no, • 1: yes (default).

3.9 [File]

Parameter	Description
ExeActivate	Enables or disables the possibility of choosing the target directory in which the file will be encrypted. Allowed values are: • 0: Disabled (default value), • 1: Enabled. If the feature is disabled, the next three parameters will not be applied and the default behavior will be adopted.
ExeToCheck	Configures a list of executable files for which SDS Enterprise must monitor open directories in which FILE files are decrypted. If this parameter is not present, the feature will be enabled for all caller executable files. The syntax is as follows: `ExeToCheck = name_exe_1 [, name_exe_n]`

ExeTargetDirectory	Specifies the path of the directory where the FILE file will be decrypted then opened. The syntax is as follows:
	`ExeTargetDirectory = path`
	where `path` is the target directory path. This path can contain tags or Microsoft Windows environment variables between < >. These tags can be:
	• COMMON_APPDATA: Folder containing application data for all users, C:\Program Data.
	• COMMON_DOCUMENTS: Folder containing the common files for all users, C:\Users\Public\Documents.
	• USERNAME: Windows username.
	• LOCAL_APPDATA: Folder containing the data of local applications, C:\Users\username\AppData\Local.
	• DESKTOP: Folder containing files on the desktop, C:\Users\username\Desktop.
	• PROFILE: Folder of the user's profile, C:\Users\username.
	• %ENV% where ENV is a system environment variable.
	Examples: `[FILE] ExeTargetDirectory=c:\User`
	`ExeTargetDirectory=<%TMP%>`
	NOTE
	The format must follow the Windows requirements: **C:\xxxx**.
	This path must not be placed between quotes.

AllowOverwriteFile	Specifies whether the file can be overwritten. This requirement may arise when several users open the same file at the same time. Allowed values are: • 0: overwriting is disabled. If a file with the same name as the encrypted and/or decrypted file already exists in the target directory, the decryption operation will fail. • 1: overwriting is enabled (default value). If a file with the same name as the encrypted and/or decrypted file already exists in the target directory, it will be silently overwritten.

Parameter	Description
AllowTransciphering WithDecipheredKeys	Allows cross-encryption with a decryption key. Allowed values are: • 0: default value. Cross-encryption with a decryption key not allowed, • 1: cross-encryption with a decryption key allowed.

3.10 [Team]

Parameter	Description
CheckCertificate Timeout	• 120 (default value): the value indicates the number of minutes between two verifications of the certificate of the user's encryption key. This parameter can take on any positive value, and is applied when the user logs in.

4. Configuring advanced settings in the registry base

Some advanced parameters in SDS Enterprise must be configured in the Windows registry base.

To edit the registry base:

1. Go to the registry database by running **regedit.exe**.
2. In the tree, go to the key indicated.
3. Change the value of the key.
4. Quit the registry database.
5. Restart the machine.

4.1 Changing the dates of the last access

When Stormshield Data Team is installed on a workstation, the date of the last access changes when a folder is browsed. The `AccessTimeAction` parameter makes it possible to restore the actual date on which files were last accessed.

Key	`AccessTimeAction (DWORD)`
Location	**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SBoxTeamDrv\Parameters**
Values	• `0x00000000`: The access date modified by Stormshield Data Team is kept (default value), • `0x00000001`: The access date is restored on standard file systems, • `0x00000002`: The access date is restored on NFS file systems, • `0x00000008`: The access date is restored on standard file systems with a potential slowdown in performance. This option enables compatibility with file systems considered standard, such as NAS EMC or non-standard CIFS servers. In general, the default value `0x00000000` is recommended. However, when using an archive solution based on a NAS EMC, the value `0x00000008` is recommended.

4.2 Moving folders available offline

Using the *cachemov.exe* tool, the system folder - *<%WINDIR%>\CSC* -, which contains the files that are available offline, can be moved.

Stormshield Data Team must be configured as follows to manage this particular environment:

Key	`SkipFolderR(DWORD)`
Location	**HKLM\SYSTEM\CURRENTCONTROLSET\Services\SBoxTeamDrv\Parameters**
Value	Add the folder containing the CSC database.

4.3 Keeping performance optimal on the workstation

When Stormshield Data Team is used, users' workstations may slow down. To keep the usual levels of performance, the following registry keys can be applied:

4.3.1 Improving performance when browsing encrypted trees

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. If the `SkipApp` key does not exist, you can create it by choosing a REG_MULTI_SZ value.

Key	`SkipApp (MULTI_SZ)`
Location	**HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SboxTeamDrv\Parameters**
Value	Add one process to exclude per line. 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 As well as the specific Dell processes: HostStorageService.exe HostControlService.exe

4.3.2 Excluding Windows processes that access encrypted folders

To reduce the time it takes to determine whether a folder is encrypted in “smart card” mode (this determines the icon of the folder), the value of the `OverlayIconAccuracy` parameter can be changed.

Key	`OverlayIconAccuracy (DWORD)`
Location	**HKEY_LOCAL_MACHINE\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Team**
Value	• `0x40`: Greatly reduces the time it takes to determine whether a folder is encrypted in smart card or token mode.

4.3.3 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:

Key	`Extensions (DWORD)`
Location	**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions**
Value	Add the list of extensions to exclude. We recommend that you exclude the following extensions: *.box*, *.sbox*, *.sbt*, *.sdsx*, *.usi*, *.usr*.

Key	`Processes (DWORD)`
Location	**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions**
Value	Add the list of processes to exclude. We recommend that you exclude the following processes: *SBDSRV*, *SBoxDiskSrv* as well as antivirus and other EDR processes.

4.4 Disabling automatic suggestion of co-workers

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

You can disable this feature by creating the following registry key:

Key	`SuggestCoworkersThroughACL (DWORD)`
Location	**HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel**
Value	• 0

5. Further reading

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

documentation@stormshield.eu