Security BOX Suite

Administration Guide

English | Version 8.0 for Windows® | March 2012

Security BOX

ARKOON NETWORK SECURITY

Security BOX Suite

Administration Guide

Version 8.0 for Windows®

Published March 2012

Contacts.

Arkoon Network Security
1 Place Verrazzano
69009 Lyon
France

Tel: +33 (0)4 72 53 01 01
Fax: +33 (0)4 72 53 12 60
Email: commercial@arkoon.net
Website: http://www.arkoon.net

Registering your software. Any Security BOX user benefits from our support, provided that your maintenance contract is valid. Our support can be easily reached:

Website: http://www.arkoon.net

Product support is restricted to software that is properly registered. The list of Security BOX users is confidential, and is used internally only for the purpose of updates and product support.

Note on encryption. The law defines the conditions governing the authorized use and sale of encryption tools. Encryption is the use of cryptographic tools. Cryptography (or encryption) is a mathematical technique that allows legible messages (plaintext) to be transformed into messages which cannot be read by third parties (ciphertext). This technique guarantees the security of confidential data or files.

Security BOX implements long key encryption technology based on standard and reputable algorithms (RSA, RC2, RC4, DES, 3DES, AES, etc.)

Security BOX fully complies with French and European legislation governing encryption.

Table of Contents

Preface

This guide provides technical information for the deployment and administration of Security BOX. It supplements the individual user manuals for the various components within the application suite. It applies to version 8.0 of Security BOX Suite.

1. Known limitations

The following table lists the known limitations for Security BOX:

Feature	Description
NFS	NFS partitions are not supported.
DFS + CSC	A DFS folder available offline cannot be secure.
Samba + DFS	A Samba share set as a DFS root cannot be secured.
Versions management \ Shadow Copy	This backup mechanism is not supported by Security BOX Team. Therefore, such features as Windows Explorer version control which rely on the shadow copy mechanism, will not work.
FUS	The FUS (Fast User Switching) feature of Windows Vista is not supported by Security BOX Enterprise.
ExcludedPath	With Microsoft Windows XP, to exclude a DFS network folder, the option is not functional when `ExcludedPath` specifies a DFS network path DFS: • either directly (logical path) • or by specifying a drive letter mapped to a network path To ensure proper use of `ExcludedPath`, it is necessary to define the physical path(s) to this folder. E.g. the following architecture: • a logical path (IDFS link) `\\MyDFSRoot\MySharedFolder` like `MySharedFolder` goes to the physical path `\\MyPhysicalServer\RepA`. • a network drive `R:` mounted on `\\MyDFSRoot\MySharedFolder`. It is essential to specify `\\MyPhysicalServer\RepA` in `ExcludedPath` and not `R:` nor `\\MyDFSRoot\ MySharedFolder`.
Installing Security BOX while logged on to Windows with a domain user account (on Vista and 7)	You cannot installl Security BOX for a domain user if the UAC (User Account Control) is enabled because the privilege evolution does not work.

2. Abbreviations

2.1. Types of accounts

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

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.

2.2. Folders

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

ProgDir	Standard installation folder of applications. By default: `C:\Program Files`
InstallDir	Security BOX installation folder. By default `<ProgDir>\Arkoon\Security BOX`

WinDir	Windows root folder:
	
	`C:\WINDOWS`
	
	or
	
	`C:\WINNT`

SysDir	Windows system folder. By default (with Microsoft ® Windows ® XP, Vista, 7): `<WinDir>\System32`
DrivDir	Windows drivers folder. By default (with Microsoft ® Windows ® XP, Vista, 7): `<SysDir>\Drivers`
CommonFilesDi	Folder containing the common files. For example: `C:\Program Files\Fichiers Communs`
InfDir	Folder containing the installation and description files for drivers with Microsoft ® Windows ®. For example: `<WinDir>\Inf`

2.3. Windows ® registry root keys

The following table lists Windows registry root keys:

HKCR	HKEY_CLASSES_ROOT
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE

Chapter 1. Use environment

To use Security BOX under the conditions of its Common Criteria evaluation and its qualification to a standard level, it is essential to observe the following guidelines.

1.1. Recommendations on security watch

1. Regularly check security alerts provided on https://support-https.arkoon.net/security/advisories.php.
2. Always apply the software update if it contains a security breach correction. These updates are available on https://support-https.arkoon.net.

1.2. Recommendations on keys and certificates

1. RSA keys of users and certification authorities must be a minimum size of 2048 bits, with a public exponent strictly greater than 65536, for a use not exceeding the year 2020.
2. The certificates and CRLs must be signed with the SHA-256 algorithm.
3. For a use beyond the year 2020, the minimum size of an RSA key is 4096 bits.

1.3. 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.

1.4. Recommendations on administrators

1. The security administrator responsible for defining the security policy on the workstation or via Security BOX 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.

1.5. Recommendations on workstations

1. The workstation on which Security BOX 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 Security BOX 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 Security BOX session is open.

1.6. Certification and qualification environment

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

1. The component "Transparent encryption" (Security BOX 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 "Security BOX kernel", common to all Security BOX 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 (Security BOX 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. Security BOX Manager or Authority Manager administration tools.
2. The possible smart card and its middeware PKCS#11.
3. “Security BOX Unified Logon" module to combine Windows session opening and the connection to Security BOX.

Chapter 2. User accounts

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

2.1. Location

When connecting, Security BOX looks for the user accounts in the folder defined in the `Sbox.ini` file, usually `RootPath1` folder, as described in Section 3.3.3, “Section [User]”.

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

By default, the following folders are blank: `RootPath1 = <COMMON_APPDATA >\Arkoon\Security BOX \users`

and `RootPath2`

`RootPath1` is the folder in which Security BOX 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.

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 files make up a user account:

`<Username>.usr` — The main file, also called KeyStore. This file contains:

- the user's private keys (in password mode)
- current and past certificates
- kernel configuration data and configuration data for the Security BOX Suite applications
- data for protecting other account files (encryption keys, authenticators)

Note
If this file is corrupt, the connection fails and returns the following error message: "`Your user file is not accessible`"

`<Username>.usd` — The user's `local` folder. This file contains the certificates for the correspondents and authorities who are 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.ust` — A history of consulted files that are protected by Security BOX Team.

This history stores the elements that make it possible to detect a fraudulent change to a security rule.

`SBoxFileList.dec` — Security BOX File decryption list. See Note below.

`SBoxFileList.efp` — Security BOX File exclusion list. See Note below.

`SBoxFileList.enc` — Security BOX File encryption list. See Note below.

`SBoxShrdList.cfp` — Security BOX Shredder exclusion list. See Note below.

`SBoxShrdList.cln` — Security BOX Shredder cleaning list. See Note below.

Note

- 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 Security BOX

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

- Clé privée :
  - CKA_DECRYPT
  - CKA_SIGN
  - CKA_SIGN_RECOVER
  - CKA_UNWRAP
- Clé publique :
  - CKA_ENCRYPT
  - CKA_VERIFY
  - CKA_VERIFY_RECOVER
  - CKA_WRAP

Chapter 3. Local policies

Local policies are the manageable 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

This file is installed in the `<InstallDir>\Kernel` folder by default.

However, it may be stored in another folder, as defined by the registry key:

`HKLM\Software\Arkoon\Security BOX\Kernel\PathIni`

This folder cannot be a network folder. It must be located on a local workstation.

Permissions:

The `Sbox.ini` file must be "readable" by everyone.

However, it may be set up with write protection.

3.2. Configuring using Windows group policy

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.

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

3.2.1. Reading priorities

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

1. `HKCU\Software\Policies\Arkoon\Security BOX Suite\<`*`Section`*`>\<`*`Item`*`>` key

   (The item is always in REG_SZ format.)
2. `HKLM\Software\Policies\Arkoon\Security BOX Suite\<`*`Section`*`>\<`*`Item`*`>` key

   (The item is always in REG_SZ format.)
3. `Sbox.ini` file

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 rebooting the computer to ensure that all of the changes are taken into account.

3.3.1. Section [Logon]

[Logon]		GPO	Available from patch
AllowPassword	Authorizes a connection to Security BOX in "password" mode: • 0: not authorized (default) • 1: authorized	Machine/User	-
AllowCard	Authorizes a connection to Security BOX in "USB key or card" mode: • 0: not authorized (default) • 1: authorized	Machine/User	-
AllowLocalUnblock	Authorizes a local unlock if the user's session is blocked: • 0: not allowed • 1: allowed (by default)		-
AllowDistantUnbloc	Authorizes a distant unlock if the user's session is blocked: • 0: not allowed • 1: allowed (by default)		-
ConnectOnCard	Displays the Security BOX 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 Security BOX account logged in (password or card).	Machine/User	-
UnFreezeOnCard		Machine/User	-

[Logon]		GPO	Available from patch
	Displays the card unlocking window when a card is inserted and the user's Security BOX session is locked. • 0: No • 1: Yes (by default) The window is applicable only if the user logged on has a Security BOX account in card mode.		
NoShutdown	Shuts down Windows if a user is logged into Security BOX: • 0: authorized (by default) • 1: denied This parameter is particularly useful when there is a lot of processing to be executed when disconnecting from Security BOX, such as encrypting a list with Security BOX File. This avoids the problem of Windows automatically stopping processing upon a timeout.	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 used only for non-CPS2 (Healthcare Professional Card) Security BOX accounts
	This parameter is optional. If it is blank, the user must enter the information manually.
		Machine/User	-

P10RequestEmailCPS	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>]`
		Machine/User	-

[Logon]		GPO	Available from patch
	More detailed information on the syntax can be found in the documentation for "mailto" links This parameter is used only for CPS2 (Healthcare Professional Card) Security BOX accounts This parameter is optional. By default, it contains only the e-mail address `inscription@certif.gip-cp.fr`, without a subject.		
DontShowLicenceKey	Keeps the license key value from displaying in the **About Security BOX** 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 Security BOX 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	-
GUILog	Prohibits a password from being passed via the command line (SBCMD tool): • 0: Accepts the password in the command line (default) • 1: Rejects it, causing a connection failure	Machine/User	-
On	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 Security BOX (see Section 3.3.2, "Section [SlotFilter]").	Machine	-

[Logon]		GPO	Available from patch
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>		-
ExternalCardAuthen	Enables to activate Security BOX logon window to use an external PIN-PAD when entering a PIN (card or token mode).		-

[Logon]		GPO	Available from patch
	• 0: no authentication by external PIN-PAD (value by default) ; • 1: authentication by external PIN-PAD		

3.3.2. Section (SlotFilter)

Caution
This section should only be filled in when `SlotFilterOn` in the `[Logon]` section equals `1`. Otherwise, its content is ignored.

[SlotFilter]		GPO	Available from patch
SlotInfoDescription Prefix	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. **Caution** This item is case sensitive. If this field is blank, the data is not filtered.	MACHINE	-
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. **Caution** This item is case sensitive. If this field is blank, the data is not filtered.	MACHINE	-

3.3.3. Section [User]

[User]		GPO	Available from patch
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.). Section 2.2, "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 Security BOX. It is possible to use keywords for this parameter; see the section called "Using keywords in RootPathN parameters " page 25.	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.	MACHINE / USER	-

[User]		GPO	Available from patch
	This option is convenient when there are several Security BOX users sharing a single workstation so that they can more easily access their Security BOX account.		
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, Security BOX 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 enabled (default) • 1: automatic completion disabled	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:

COMMON_APPDATA	The file system folder containing application data for all users. A typical path is: • Vista: `C:\ProgramData` • XP: `C:\Documents and Settings\All Users\Application Data`
COMMON_DOCUMENTS	The file system folder that contains documents that are common to all users. A typical path is: • Vista: `C:\Users\Public\Documents` • XP: `C:\Documents and Settings\All Users\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: • Vista: `C:\Users\username\Desktop` • XP: `C:\Documents and Settings\username\Desktop`
LOCAL_APPDATA	The file system folder that serves as a data repository for local (nonroaming) applications. A typical path is: • Vista: `C:\Users\username\AppData\Local` • XP: `C:\Documents and Settings\username\Local Settings\Application Data`
MYDOCUMENTS	The file system folder used to physically store a user's common repository of documents. A typical path is: • Vista: `C:\Users\username\Documents` • XP: `C:\Documents and Settings\username\My Documents`
PROFILE	The user's profile folder. A typical path is: • Vista: `C:\Users\username` • XP: `C:\Documents and Settings\username`
PROFILES	The file system folder containing user profile folders. A typical path is: • Vista: `C:\Users` • XP: `C:\Documents and Settings`
USERNAME	Windows username. (username)

3.3.4. Section [NewUser]

The `[NewUser]` and `[SBox.NewUserWizardExXXX]` sections are for creating 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, GP2, CPS2 . See Section 2, “Abbreviations”.

AllowNewUser	Creating an account: • 0: not authorized (default) • 1: authorized
CertLife	Term of validity, in years, for certificates self-generated by Security BOX. 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: KS1, KS2, GP1, GP2, RFU (not used, but this column is required), CPS2
<Algorithm to be applied>	Algorithms for protecting the user’s keystore. See the section called “User key types”.

The next two sections provide information on the types of keys and algorithms that are available or implemented when creating an account.

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

KS1, KS2, GP1, GP2, RFU (not used, but this column is required), CPS2

User key types

The supported key types (the user’s private keys) are:

A key type can be:

```
KEY_RSA_512BITS
KEY_RSA_768BITS
KEY_RSA_1024BITS
KEY_RSA_2048BITS
```

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

There must therefore be only one “`2`” per account type, or column.

So, if RSA 1024 bits is the default value and RSA 2048 is prohibited, then it must be set up as:

```
KEY_RSA_512BITS  = 111111
KEY_RSA_768BITS  = 111111
KEY_RSA_1024BITS = 222222
KEY_RSA_2048BITS = 000000
```

To avoid not being able 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.

Note
The 512 and 768 key sizes are currently considered to be low. We therefore recommend no longer using them except when imposed by the environment.

Keystore protection algorithms

Supported protection algorithms for protecting a keystore are:

Encryption		Hash
CRYPTO_AES_256BITS CRYPTO_AES_192BITS CRYPTO_AES_128BITS CRYPTO_DES_128BITS CRYPTO_DES_64BITS	CRYPTO_RC5_128BITS CRYPTO_RC5_64BITS CRYPTO_RC5_40BITS CRYPTO_RC4_128BITS CRYPTO_RC4_64BITS CRYPTO_RC4_40BITS CRYPTO_RC2_128BITS CRYPTO_RC2_64BITS CRYPTO_RC2_40BITS	HASH_SHA1 HASH_MD5 HASH_MD2

For account types whose order number is N, the protected algorithm integrated is the one whose Nth digit is "`1`".

For example, to implement AES 256 + SHA 1 for KS1 and KS2 and DES 128 + MD5 for GP1 and GP2, it must be set up as follows:

```
CRYPTO_AES_256BITS= 110000
CRYPTO_DES_128BITS= 001111
HASH_SHA1= 110000
HASH_MD5 = 001111
```

There must therefore be only one per account type (and therefore one per column) for the encryption algorithm and the hash algorithm.

To avoid not being able to create an account if there is a configuration error in the `Sbox.ini` file, the following behavior is adopted:

- If there are several authorized encryption algorithms for an account type, the algorithm used will be based first on the algorithm's function (in the order AES, DES, RC5, RC4, RC2) and then on the largest authorized key size.
- If there are several authorized hash algorithms for an account type, the algorithm used will be the first one authorized from (in order) SHA1, MD5 and MD2.

- If an unexpected character is entered as the value for one of the algorithms, the algorithm is not authorized for the account type. The value 0 [not authorized] is assumed.
- 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 there is no authorized encryption or hash algorithm, an account cannot be created.

Except in a very specific case, we recommend leaving the predefined value for these two algorithms (AES 256 bits and SHA-1) by putting the following lines:

```
CRYPTO_AES_256BITS= 111111
HASH_SHA1= 111111
```

3.3.5. Section [NewUserCard]

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

[NewUserCard]		GPO	Available from patch
AllowNewUserAuto	This parameter authorizes card accounts to be created automatically when first used on a workstation. Section 4.4, “Interoperability with other cards/tokens”. • 0: Automatic creation not authorized (default) • 1: Automatic creation authorized	-	-

3.3.6. Sections [SBox.NewUserWizardExXXX]

Parameters

The following table details the content for each section based on the account type `XXX`, see Section 2, “Abbreviations”.

Parameter	KS1	KS2	GP1	GP2	CPS2	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 model to be used for the creation. The model 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 model 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 models can be found in the *Security BOX Manager/Security BOX Authority Manager* manual.
MasterKeystore	•	•	•	•	•	If the *<MasterPath>* item is set, this item designates the name of the file containing the account

Parameter	KS1	KS2	GP1	GP2	CPS2	Description
						model 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 model 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, KS2, CPS2 modes • the card in GP1, GP2 modes • 0: No (default for KS1, KS2, CPS2 modes) • 1: Yes (default for GP1, GP2 modes)
NoExtractableKeystoreKeys				•		The keys stored in a keystore for a card account cannot be exported: • 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, Security BOX automatically imports the certificates

Parameter	KS1	KS2	GP1	GP2	CPS2	Description
						(for the correspondents or authorities) indicated by the *<DirectoryModel>* • 0: *<DirectoryModel>* is a file (default). The extensions supported are .cer, .crt, .p7b, .p7c, and .sbc. 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, .p7c, and .sbc 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 model, Security BOX copies the list files from Security BOX File and Security BOX Shredder. The integrity of these files is verified against the model 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 model • 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:

Parameter	KS1	KS2	GP1	GP2	CPS2	Description
						• 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.
ChangePINSO	•	•				When creating an account, Security BOX 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, GP2, and CPS2 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

Parameter	KS1	KS2	GP1	GP2	CPS2	Description
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 Security BOX, 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), Security BOX 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: • 11: box checked and accessible • 10: box checked and uneditable • 01: box unchecked and accessible

Parameter	KS1	KS2	GP1	GP2	CPS2	Description
						• 00: box unchecked and uneditable (default)
EncipherментKey InCard				•		**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
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

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	CPS2	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: • 00 = check box unchecked and uneditable • 01 = check box unchecked and editable (default) • 10 = check box checked and uneditable • 11 = check box checked and editable This parameter is recognized only if *<ExportKeys>* is set to 1. If the *<ShowSaveKeyPage>* parameter is set to 1, there is no user interaction, and the save then depends on what is indicated as the default value for "checking" the check box (the digit on the left).

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
- *[Sbox.NewUserWizardExCPS2.Encryption]*: CPS2 card account for the encryption key
- *[Sbox.NewUserWizardExCPS2.Signature]*: CPS2 card account for the signature key

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

Parameter	KS1	KS2	GP1	GP2	CPS2	CPS2. Sig.	Description
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, GP2,and CPS2) • 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

Parameter	KS1	KS2	GP1	GP2	CPS2	CPS2. Sig.	Description
							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)

Parameter	KS1	KS2	GP1	GP2	CPS2	CPS2. Sig.	Description
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

Parameter	KS1	KS2	GP1	GP2	CPS2	CPS2. Sig.	Description
							• 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

Parameter	KS1	KS2	GP1	GP2	CPS2	CPS2. Sig.	Description
							editable (default)

Note
The “CPS2 Enc” and “CPS2 Sig” columns distinguish between what is customizable for the two types of CPS2 card keys, which are systematically customized with the signature key when they are issued.

3.3.7. Section (KeyRenewal)

The *[KeyRenewal]* and *[SBox.KeyRenewalWizardYYY]* sections are for renewing keys for existing Security BOX 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

CertLife — Term of validity, in years, for certificates self-generated by Security BOX. 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 below.

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

KS, GP

The types of keys supported and the management rules for configuration errors are the same as for an account creation, defined in the section called “User key types” page 26.

So, if RSA 1024 bits is the default value and RSA 2048 is prohibited, then it must be set up as:

```
KEY_RSA_512BITS  = 111
KEY_RSA_768BITS  = 111
KEY_RSA_1024BITS = 222
KEY_RSA_2048BITS = 000
```

3.3.8. Sections (SBox.KeyRenewalWizardYYY)

The following table details the content for each section based on the account type YYY (defined in Section 3.3.7, “Section [KeyRenewal]”).

Parameter	KS	GP	CPS	Description
NoExtractableK	•	•	•	See the parameter by this name in Section 3.3.6, “Sections [SBox.NewUserWizardExXXX]”.
Pkcs12Import	•	•	•	See the parameter by this name in Section 3.3.6, “Sections [SBox.NewUserWizardExXXX]”.
InternalKeys		•		See the parameter by this name in Section 3.3.6, “Sections [SBox.NewUserWizardExXXX]”.
ExportKeys		•		See the parameter by this name in Section 3.3.6, “Sections [SBox.NewUserWizardExXXX]”.
KeepCardObjects		•		See the parameter by this name in Section 3.3.6, “Sections [SBox.NewUserWizardExXXX]”.
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

3.3.9. Section (Mail)

[NewUserCard]		GPO	Available from patch
DisplayComlogWindow	Allows the Security BOX 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 Security BOX connection window appears systematically (default). This parameter does not affect whether a user is locked.	-	-
DisplayComlogWindowUserLocked	Allows the Security BOX connection window to display	-	-

[NewUserCard]		GPO	Available from patch
	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 Security BOX connection window appears systematically (default). This parameter does not affect whether a user is locked.		
AllowSendClearIfEncryptAskUn	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).	-	-

Outlook Edition

AttachmentsScanningTimeout

When sending a secure message, the Outlook edition waits as long as indicated in ms. The special value -1 indicates that there is no waiting period.

Using this parameter allows time for an antivirus server to analyze the message.

Default: 5000 (5 seconds).

Notes Edition

When the user sends a message, the Notes Edition of Security BOX Mail uses the “sign” and “encrypt” check boxes in the standard 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 Security BOX, use the following parameter to tell Security BOX to ignore the check boxes that are native to Lotus Notes:

DoNotCheckNativeCheckBox

Ignores the check boxes native to 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 Notes Edition of Security BOX Mail looks at the extra check boxes on the new message form.

- `SecurityBOXMailSignOption`: Indicates that Security BOX Mail must sign the e-mail message.
- `SecurityBOXMailEncryptOption`: Indicates that Security BOX Mail must encrypt the e-mail message for each recipients.

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

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

3.3.10. Section [CRL]

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

[CRL]		GPO	Available from patch
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.
		-	-

3.3.11. Section (external PKCS11 policy)

The `[external PKCS11 policy]` section is for configuring the type of USB token or smart card (Security BOX Card Extension) in Windows Control Panel.

[CRL]		GPO	Available from patch
CPLShowExtension	Indicates whether the configurator appears in Windows Control Panel. • 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 Security BOX 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 enabled:	-	-

[CRL]		GPO	Available from patch
	• 0: No • 1: Yes (default)		
CPLPKCS11InfosSaveAsEnabled	The **Save As** button is enabled: • 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.

3.3.12. Section [File]

The `[File]` section contains the Security BOX File parameters.

CanEncryptNetFile The user can encrypt a file located on the network:

- 0: No
- 1: Yes (default)

CanDecryptNetFile The user can decrypt a file located on the network:

- 0: No
- 1: Yes (default)

Note
If the network folder is protected by Security BOX Team, then Security BOX File can always decrypt an encrypted file, regardless of this parameter.

Note
Encryption over a network is secure because plain text data is converted into encrypted data. However, decryption can cause security issues because previously protected data becomes unencrypted. For this reason, when encrypting a file on a network to protect shared files, decryption over the network must be prohibited. This forces the user to make a copy to their workstation to decrypt the file locally.

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

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

Parameter	Description	GPO	Available from patch
ExeActivate	This parameter activates the feature to choose the target directory in which the encryption will be done. Allowed values: • 0: the feature is disabled (default) • 1: the feature is enabled If the ExeActivate option is set to 0, the parameters below will be ignored and Security BOX 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 yo 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 Security BOX tags or Microsoft Windows environment variables between < >. The list below shows sample tags on Windows XP: • COMMON_APPDATA : `C:\Documents and settings\All Users\Application Data` • COMMON_DOCUMENTS : `C:\Documents and settings\All Users\Documents` • USERNAME : nom d'utilisateur Windows connecté.		

	• LOCAL_APPDATA : `C:\Documents and settings\<username>\Local settings\Application Data` • DESKTOP : `C:\Documents and settings\<username>\desktop` • PROFILE :`C:\Documents and settings\<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 Security BOX FILE file is opened several times. Allowed values are: : • 0: overwriting is disabled. 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 enabled (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 Security BOX 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.		

3.3.13. Section (DirectoryUpdate)

Automatically updating the folder

The following updates may be performed automatically to the user's local folder:

- Deleting expired certificates
- Deleting revoked certificates
- Replacing certificates in the local folder with more recent certificates found on an LDAP server

Each of these three certificate-related updates may be restricted by issuing authority.

Activate

Enables automatic folder updates.

- 1: automatic updates enabled
- 0: automatic updates disabled (default)

AllowManualUpdate

Allow manual updates

- 0: not allowed (by default)
- 1: allowed

Note
This parameter is taken into account only if the *Directory Update* feature is activated.

Timer

This parameter is the activation frequency of treatment expressed in hours. It is possible to execute it twice a day or once a week. The value by default is 24.

StartOnConnection

- 0: (value by default): treatment is not forced for Security BOX user's connection.
- 1 : treatment of folder update is launched during Security BOX user's connection.

ReplaceFromLDAP

Enables the replacement of certificates in the local folder with more recent certificates found on an LDAP server:

- 1: automatic replacement enabled
- 0: automatic replacement disabled (default)

This parameter is recognized only if `Activate`=1.

Note
The replacement only works if the certificate has a correct validity status.

55CompatibilityMode=1

This parameter allows to modify display for security folder in order to control validity dates for certificates (Security BOX Suite 5.5).

- 0 : automatic replacement disabled (default)
- 1 : automatic replacement enabled

ReplaceFromLDAPOnValidCert

This parameter monitors the treatment on valid certificates.

2 possible values:

- 0: the certificate is ignored

- 1: (value by default): the treatment is executed on this certificate.

ReplaceFromLDAPOnOutOfDateCert

This parameter monitors the treatment on obsolete certificates.

2 possible values:

- 0: the certificate is ignored
- 1: (value by default): the treatment is executed on this certificate.

ReplaceFromLDAPOnRevokedCert

This parameter monitors the treatment on revoked certificates.

2 possible values

- 0: the certificate is ignored
- 1: (value by default): the treatment is executed on this certificate.

CommonNameReplace

This parameter makes it possible to flag certificate-issuing authorities by which ones to replace automatically.

The value of this parameter indicates:

- The "`CommonName`" for authorities issuing certificates affected by the processing, separated by semicolons, or
- The `keyword` "All", meaning that all of the certificates are affected (default).

This parameter is recognized only if `ReplaceFromLDAP`=1 and `Activate`=1.

DeleteIfOutOfDate

Enables the removal of expired certificates:

- 1: removal enabled
- 0: removal disabled (default)

This parameter is recognized only if `Activate`=1.

CommonNameOutOfDate

This parameter makes it possible to flag certificate-issuing authorities by which ones to delete automatically upon expiration.

The syntax for the value is identical to the syntax for the `CommonNameReplace` parameter.

This parameter is recognized only if `DeleteIfOutOfDate`=1 and `Activate`=1.

DeleteIfRevoke

Enables the removal of revoked certificates:

- 1: removal enabled
- 0: removal disabled (default)

This parameter is recognized only if `Activate`=1.

CommonNameRevoke

This parameter makes it possible to flag certificate-issuing authorities by which ones to delete automatically upon revocation.

The syntax for the value is identical to the syntax for the `CommonNameReplace` parameter.

This parameter is recognized only if `DeleteIfRevoke`=1 and `Activate`=1.

Other parameters

`AddCertAttrInLdapFilter`

This parameter makes it possible to automatically add criteria (`usercertificate;binary=*`) to the LDAP search filter:

- 1: add the criteria (default)
- 0: add nothing

Adding this criteria makes it possible to focus only on entries containing a certificate, which is consistent with normal use of the Security BOX folder.

`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

3.3.14. Section (Disk)

The `[Disk]` section is for configuring Security BOX Disk.

General parameters (Disk)

`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.

Volume formatting data (Disk)

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:

`FileSytem`

File system used for the formatting:

- NTFS
- FAT32 (default)
- FAT

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:
- 1: Yes (default)
- 0: No

Compression
Enable compression:
- 1: Yes
- 0: No (default)

This parameter may or may not be recognized, depending on the file system used for formatting (only NTFS uses it).

Volume automatic creation data (Disk)

In addition to interactive mode, a volume may be created using the command line tool (see the *Security BOX Disk* guide) or automatically at the time of the user's first connection. This section describes the creation parameters used in these two cases. Information on formatting the volume was provided earlier.

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.
- 1: Automatic mode (default)
- 0: Manual mode

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 Security BOX username (UserId) and some Windows CSIDL values.

UserId	The user's Security BOX 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:\Documents and Settings\All Users\Application Data`.
COMMON_DOCUMENTS	The file system folder that contains documents that are common to all users. A typical path is `C:\Documents and Settings\All Users\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:\Documents and Settings\username\Desktop`.
LOCAL_APPDATA	The file system folder that serves as a data repository for local (nonroaming) applications. A typical path is `C:\Documents and Settings\username\Local Settings\Application Data`.
MYDOCUMENTS	The file system folder used to physically store a user's common repository of documents. A typical path is `C:\Documents and Settings\username\My Documents`
PROFILE	The user's profile folder. A typical path is `C:\Documents and Settings\username`.
PROFILES	The file system folder containing user profile folders. A typical path is `C:\Documents and Settings`.
USERNAME	Windows username (username).

Volume data created on the first connection (Disk)

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

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 *Security BOX Disk manual*) and to perform recovery operations (described in Section 6.4, "Security BOX Disk").

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)

DfsSupport

Enables file encryption on a DFS share

- 0: No (default)
- 1: Yes

If this option is not enabled and DFS files are accessed in secure mode, they can remain unencrypted even if the product indicates otherwise.

Enabling this option can cause workstations to operate more slowly. These slowdowns are based on the network configuration and the DFS servers on the network.

3.3.15. Section (Team)

DFS support

Parameter	Description	GPO
DfsSupport	Activates files encryption on a DFS sharing: • 0 : no (by default) • 1 : yes If this option is not activated and files on DFS are accessed in secured mode, they can remain uncrypted even if the product indicates the contrary.	-

Parameter	Description	GPO
	Activating this option can slow down some machines. The slowdown depends on the network configuration as well as installed DFS servers. **Note** DFS on Samba is not supported. To deactivate it, you must modify the `sbm.conf` file (on Samba server) and indicate *`host msdfs = no`* parameter in section [global]. Refer to Samba documentation for more details.	

Saving the internal cache file

Parameter	Description	GPO
`TeamCachePath`	This parameter determines the directory where Team saves its internal cache file. It is automatically added by the installer according to platform (XP or VISTA). Its value can still be customized by the administrator with the following restrictions: • The folder specified must be a local directory accessible by all users. • The file must be part of folders excluded from encryption (Section 6.8.7, "Folder exclusion").	-

Managing shared rules

Shared security rules in Security BOX Team can be disabled or combined with personal user account rules, depending on the values of *`AllowDetachRules`* and *`Rule`*, defined below.

Parameter	Description	GPO	Available from patch
`AllowDetachRules`	Indicates if the rules stored directly into the folder are taken into account • 0: the rules stored at folders level are not taken into account. • 1 (by default) : the rules stored at folders level are taken into account.	-	-
`Rule`	Indicates the mode for whether rules stored directly in folders are taken into account: • `DetachOnly`: Possible user account rules are not taken into account. In the Team configuration panel in Security BOX, the **Security Rules** tab is hidden.	-	-

Parameter	Description	GPO	Available from patch
	• `PathInProfil` If a personal rule is defined in the user's Security BOX account, then only the name of the folder on which the rule applies is taken into account. This is defined in the sharing rule, that is to say on the folder. This option allows to forcer folder to be secured without modifying the employees list. • `ProfilFirst`: The user account rules are taken into account. If a rule stored at the folder level and a rule stored at the Security BOX account level are defined in the same folder, the rule at the Security BOX account level is used. This parameter applies only if the rules stored at the folder level are taken into account (`AllowDetachRules=1`)		

Modifying Security BOX tab

It is possible to grey out Security BOX tab in the properties window to prevent a user from modifying or deleting the existing detached rules or creating new ones.

Parameter	Description	GPO	Available from patch
HideDetachRules	• 0 (value by default): any allowed user can modify the content of the Security BOX tab for the folder's properties window • 1: the content of the Security BOX tab for the folder's properties window is greyed out for any user **Note** This parameter is taken into account only if the *AllowDetachRules* parameter is 1.	-	-

Opening an encrypted file not allowed if encryption key is revoked

It is possible to check the certificate of an encryption key. To do so, you must use the following parameter in the [Team] section into the `Sbox.ini` file :

Warning
This verification can take some time, in particular when network time-outs are at stake if the Certificate Revocation List (CRL) cannot be downloaded (for example if the host server cannot be accessed).

Parameter	Description	GPO	Available from patch
DenyAccessOn BadCertificate	• 0 (value by default): the user can access the encrypted files even if the certificate of the encryption key is revoked. • 0x00900090 : the user cannot access the encrypted files if the certificate of the encryption key is revoked.	-	-
CheckCertificate Timeout	• 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.	-	-
AllowLocal CertificateStore=1	• 0 (value by default): if the CRL cannot be downloaded, the certificate is considered as revoked. • 1: if the CRL cannot be downloaded and the certificate is in the local cache, the state of the local certificate is used.	-	-

The parameters are taken into account when the user connects on the account.

Configuring copy or movement for a folder/file

Parameter	Description	GPO	Available from patch
SecureDrag AndDrop	The *SecureDragAndDrop* parameter enables to limit the copy or movement for folders and files with a Security BOX 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: same behaviour as current one. The parameter has the three following values: • 0: (by default) the behaviour remains identical to the current one. • 1: the action is not allowed. • 2: moving or copying does not decrypt the files.	-	-

Parameter	Description	GPO	Available from patch
	Note The *SecureDragAndDrop=2* parameter corresponds to the implementation on the **Drag and Drop** of the **Save** feature from Security BOX contextual menu.		

Chapter 4. Managing smart cards and USB tokens

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

4.1. Type of USB token or smart card used

Security BOX can use any USB token or smart card as long as its manufacturer provides a PKCS#11 cryptographic module (standard interface) that has been reasonably implemented.

The name of the DLL for the cryptographic module to be implemented can be specified in the **USB key or card type configurator** (in Windows control panel).

This configurator knows the DLL name for some manufacturers. These names are defined in the `CardChoice.ini` file (see Section 4.2, "CardChoice.ini file"). This file can be completed to take into account any cards or tokens that were not initially expected.

To enable a cryptographic module within Security BOX, you must:

1. Launch the configurator (from Windows Control Panel).
2. Select a predefined card type.

   Or define a new one (manufacturer name and the name of the DLL for its PKCS#11 interface).
3. Possibly test the module by clicking on the **Information** button: The number of visible drives (at least 1) is shown.
4. Confirm your selection by clicking on **Apply** or **OK**.
5. Close the Windows session and open a new one to apply the changes.

You can now create or use a card account.

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**
> To take changes into account that were made for a card or token type and to apply them to the Security BOX 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.

[Manufacturer name or card type]	This name identifies the type of USB token or smart card and is displayed by the configurator.
dllname	Name (and possibly the path) for the manufacturer's DLL PKCS#11 DLL This parameter is required.
eCKA_MODIFIABLE	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.
eCKA_EXTRACTABLE	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.
eCKA_LABEL	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.
eCKA_MODULUS_BITS	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.
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. Directly enabling a cryptographic module

The standard procedure for enabling a cryptographic module involves using the "USB key or card configurator", as described in Chapter 4, *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.

4.4. Interoperability with other cards/tokens

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 3.3.2, "Section [SlotFilter]", indicates which PKCS#11 slots to check to filter for parasitic slots.

```
[Logon]
SlotFilterOn=1
[SlotFilter]
SlotInfoDescriptionPrefix =    ; "description" field prefix
SlotInfoManufacturerIdPrefix = ; "ManufacturerId" field prefix
```

4.5. Automatically creating a card account

4.5.1. Description

To make it easier to deploy card accounts and to minimize actions required by the user, Security BOX Suite 8.0 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. Security BOX 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 Security BOX account is then created.

4.5.2. 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 3.3.5, “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

If the configuration is invalid, the account will not be automatically created. Only traditional creation will be available.

4.6. Using the card’s keys

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

Security BOX 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 Security BOX 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 therefore 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.

4.7. Renewing card data

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

4.7.1. Renewing certificates

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

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 Security BOX has correctly recognized the new one. You can verify whether the new certificate is recognized by using the key holder on the Security BOX configuration panel.

4.7.2. 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 Security BOX has correctly recognized the new ones. You can verify whether the new certificates are recognized by using the key-holder on the Security BOX configuration panel.

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

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

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

4.7.3. Reinitializing keys

It is now possible to reset a card (using a tool other than Security BOX) 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
```

4.8. Polling the card

Security BOX card extension periodically polls the card to detect the user card (or token) insertions/retrievals. It is now possible to suspend and resume the poll using the sbcmd tool.

The syntax:

- `sbcmd /P -stop`: to stop polling.
- `sbcmd /P -start`: to resume polling .

Chapter 5. Customizing the installation

This chapter explains how to do the following:

- **administer a centralized installation procedure**
- **generate a specific installation packet, such as:**
  - **accounts centralized on a server**
  - **accounts created from a specific "master"**
  - **any other special case affecting the `Sbox.ini` see Section 2.3, "User account files" and `CardChoice.ini` Chapter 4,** *Managing smart cards and USB tokens*.

5.1. Basic files for the installation procedure

The basic installation procedure includes the following files:

`setup.exe`	Entry point for the installation procedure: • installs Microsoft Installer, if necessary • installs the InstallShield runtime, if necessary • launches the Security BOX Suite installation This file does not contain any files or scripts specific to Security BOX.
`setup.ini`	Configuration file for `setup.exe`
`instmsiw.exe`	Microsoft Installer. This program is required if it is not already present.
`ISScript9.Msi`	Runtime for InstallShield. This runtime is required for the Security BOX Suite installation procedure.
`Security BOX Suite 8.0.msi`	Full installation procedure for Security BOX. This file contains all of the files and scripts necessary to install Security BOX. We recommend not using the MSI file directly to carry out the installation, but to use the program `setup.exe`. If this file is used directly, Windows Installer (version >= 2.0) must already be installed, and the InstallShield runtime must also already be installed. In addition, with Vista, the MSI file must be run in a command line window opened by an administrator.
`<CodePage>.ini`	Resource file identified within `setup.exe` where *<CodePage>* is: • `0x0409` for the English version • `0x040c` for the French version

5.2. Installing with user interaction

This is the default installation mode for Security BOX Suite 8.0.

After entering a license key and accepting the license agreement, the installation procedure offers to install all of the components for the software suite that are authorized under the license key. These two components require the user to manually select them for installation.

To install these modules without explicitly asking the user, the `USERMUSTSELECTGINA` property in the installation package's "Property" table must be set to `NO`.

5.3. Administered installation

The centralized administration and/or customization of the installation procedure requires a "server image" of the `.MSI` (Microsoft Installer) file.

5.3.1. Generating a server image (administered installation)

To generate a server image of an `.MSI`, run:

```
msiexec /a "<full path>\Security BOX Suite 8.0.msi".
```

Note
With Vista, a security confirmation may be requested. The user must then authorize the procedure to continue.

The procedure asks the user to specify the folder (called `<ImageDir>`) containing:

- a file `Security BOX Suite 8.0.msi` which contains only the installation rules and scripts
- all of the files (binary files, `.ini`) to be installed, in a relative tree structure matching the final tree structure.

5.3.2. Updating the server image

If a patch is available, then the server image can be updated with the following command (on a single line):

```
msiexec /p "<full path> >\Security BOX Suite 8.0.msp" /a "<ImageDir>\Security BOX Suite 8.0.msi"
```

This command applies to the `.MSI` of the server image (located under `<ImageDir>`).

Note
With Vista, a security confirmation may be requested. The user must then authorize the procedure to continue.

The order of the `/p` and `/a` parameters must absolutely be respected. The msiexec command `/p … /a` is not the same as the msiexec command `/a … /p` (which makes no sense).

Caution
If a new patch is delivered, then it should not be applied to a server image that has already been patched. It is then necessary to:

1. Generate a new unpatched image:

   ```
   msiexec /a <official .msi>
   ```

2. Update this image with the latest patch:

   ```
   msiexec /p <last .msp> /a <msi image>
   ```

3. Install the updated image, see Section 5.3.3, “Installing on a workstation”:

5.3.3. Installing on a workstation

Using the server image, Security BOX is installed on a workstation by running:

```
msiexec /i <ImageDir>\Security BOX Suite 8.0.msi
```

Note
With Vista, this command must be run in a command line window opened by an administrator.

To install Security BOX using the `setup.exe` file, you must then recopy the five `<ImageDir>` files: `setup.exe`, `setup.ini`, `0x0409.ini` (for the English version, or `0x040c.ini` for the French version), `instmsiw.exe` and `ISScript.msi` for the basic procedure (located in the same folder as `Security BOX Suite 8.0.msi`).

5.3.4. Updating on a workstation

If Security BOX is already installed on a workstation, then updating it from the patched server image is done by running:

```
msiexec /fvamus <ImageDir>\Security BOX Suite 8.0.msi
```

Note
With Vista, this command must be run in a command line window opened by an administrator.

5.4. Installing without user interaction

To install Security BOX Suite without user interaction, run:

```
msiexec /qn /i "<path>\Security BOX Suite 8.0" LICENCENUM=<license number>
```

where `<license number>` must be written as `ABCDEFGH-ABCDEFGH` (with the dash).

Note
With Vista, this command must be run in a command line window opened by an administrator.

Possible variations are:

- `/qn`: installation without any screens
- `/qn+`: same as `/qn`, but with a final confirmation screen
- `/qb`: installation with a screen showing a progress bar and estimated time remaining
- `/qb+`: same as `/qb`, but with a final confirmation screen

Caution

- The `/qr` switch does not work. It only installs the Security BOX.
- The version update (5.X, 6.X => 8.0) does not work in silent mode. In this case, you must first uninstall the old version in silent mode and then reinstall the new one.

Note
In silent mode, the procedure installs all of the applications authorized by the license. Using the private SBREMOVE property (see Section 5.8, “Additional customizations”) you can limit the applications installed.

To uninstall the suite, run:

```
msiexec /x "<path>\Security BOX Suite 8.0.msi"
```

Note
With Vista, this command must be run in a command line window opened by an administrator.

5.5. Customizing the Sbox.ini and CardChoice.ini files

The `Sbox.ini` and `CardChoice.ini` files (described in Section 2.3, “User account files” and Chapter 4, *Managing smart cards and USB tokens*, respectively) can be customized.

5.5.1. For a standard installation

The Security BOX Suite installation program allows the two configuration files, `sbox.ini` and `cardchoice.ini`, to be customized at the end of the installation, just before launching the application.

The adjustments to be made are written to a file called `sboxsetup.ini`, which is located in the same folder as `Security BOX Suite 8.0.msi`.

Important
This only updates the `sbox.ini` file after installation. The information within the `sboxsetup.ini` file are not taken into account for the installation.
Therefore, when the *DefaultPath1* parameter (indicating the folder path *default* which contains the default user account) is specified into`sboxsetup.ini`, the *default* folder must be moved from the installation folder (`C:\Documents and Settings\All Users\Application Data\Arkoon\Security BOX\Users` under Windows XP and `C:\programdata\arkoon\security BOX\Users` under Windows Vista) to the folder specified in `sboxsetup.ini`.

A `[patchini]` section needs to be created in this file with the following syntax for each line:

```
<ini name> = <section>;<item>;<operation>[;<value>]
```

ini name	"SB" for `sbox.ini`
	"CC" for `cardchoice.ini`
section	Name of the relevant section (without brackets)
Item	Name of the entry to be modified
Operation	"`D`" delete: deletes the key (value is then optional and ignored).
	"`W`" write: writes the key.
	"`R`" replace: writes the key if it already exists (does nothing if it no longer exists).
	"`A`" add: writes the key if it no longer exists (does nothing if it already exists).
Value	Value to be assigned to the item (all operations except "`D`").

Note
For the "`W`", "`R`" and "`A`" operations, if the value field is not supplied, the corresponding item is deleted. It is not possible to set a value to blank.

5.5.2. For an administered installation

For this, the relevant files must be modified directly on the server image in the following folder:

```
<ImageDir>\Program Files\Arkoon\Security BOX\Kernel\
```

For example:

- All of the user accounts can be centralized on a server by including `RootPath2 = \\ <server name>\<folder>` in the [User] section of `Sbox.ini`.
- You can prohibit new accounts from being created by putting `AllowNewUser = 0` in the *[NewUser]* section.
- A specific type of cart can be offered by default in the “card type configurator” using the `CPLForcePKCS11Label` item in Section 3.3.11, “Section [external PKCS11 policy]”.
- The other types of cards can be deleted from the `CardChoice.ini` file.

Warning
It is impossible to customize the following items in the `Sbox.ini` file. They are automatically set by the installation procedure.

- `[User]` section: *RootPath1*

5.5.3. Creating registry keys during the installation

Security BOX Suite installation program allows you to configure a number of registry keys at the end of installation, just before launching the application. To do this, the registry keys to manipulate, create, add, change or delete, are placed in a the `sboxregistry.ini` file placed in the same folder than `Security BOX Suite 8.0.msi`.

Important
This mechanism only allows you to create chain value registry keys or `DWORD` value after the installation. The information provided in the registry base are not taken into account. Consequently, writing in the registry settings such as the access path configuration, cannot guarantee the compliance or the validity of the target parameter. This will require the intervention of a user (e.g. to move a file to the right place in a tree). Also, some configuration settings written in the registry will always require a system reboot to be taken into account.

The `[patchregistry]` section must be created in this file with the following syntax for each line:

```
<operation>;<key>;[<item<];[<type>];[<value>]
```

With

- operation:
  - "D" (delete) to delete the key (the value is optional and is ignored)
  - "W" (write) to write the key
  - "R" (replace) to replace the key if it already exists (do not operate this action if it does not exist)
  - "A" (add) to write the key if it does not exist yet (do not operate this action if it exists)
- key: registry key
- item: entry name
- type: entry type ("SZ" for a chain value and "DW" for a DWORD
- value: value for the item

"W" allows you yo create registry rules or modify the value of an existing key. This operation does not require the value field and a key is simply create without a value.

"R" and "A" require the value field. The item, type and value fields are required.

"D" allows you to delete either only the key registry value (if it specified in the item, type and value fields), or a registry key (if the item, type and value fields are not present).

5.6. Creating an account from an account model

Security BOX Suite can create accounts from a model, automatically integrating:

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

An account model 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`, `.sbc`).
- the file lists (encryption, decryption, exclusion) for Security BOX File
- the file lists (cleaning, exclusion) for Security BOX Shredder

If these file lists 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.

Whatever is not stored in a `.usr` file will not be copied when creating an account:

- Security BOX: The list of recently connected users and the network connection mode.
- Security BOX Disk: the automatically mounted volumes.

It is possible to define a different account model for each type of account: KS1, KS2, GP1, GP2; seeSection 2, “Abbreviations”.

Warning
Security BOX Suite 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|sbc)>`*
- The file indicated by *`DirectoryModel`* does not exist or cannot be accessed.

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

5.6.1. The account model is located on a server

If the account model is located on a server, the file, `<ImageDir>\Program Files\ARKOON\Security BOX\Kernel\sbox.ini`

must contain the following items in Section 3.3.6, “Sections [SBox.NewUserWizardExXXX]”:

- `MasterPath` and `MasterKeystore` for the `.usr` file containing the account model

- `DirModelIsFolder` and `DirectoryModel` for the certificate file(s) to be integrated in the folder

5.6.2. The account model must be installed on the workstations

Implementation basics

If the account model must be installed on the workstations (for example, if there are isolated workstations where Security BOX was installed from a custom CD), a "masters" subfolder containing the model accounts must be created in the same folder as `Security BOX Suite 8.0.msi` (`<ImageDir>`).

For Windows XP, this subfolder is copied into `C:\Documents and Settings\All Users\Application Data\Arkoon\Security BOX\`

For Windows Vista, this subfolder is copied into `C:\programData\Arkoon\Security BOX`

At the time of installation, the models and associated file are automatically installed, and the Security BOX product and `Sbox.ini` file are updated to make them effective.

Installing the model from a “masters” folder also works with an administered installation procedure.

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 models.

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`: model keystore

  `ks1.p7c`: list of certificates to be imported
- for a password account with two keys for signing and encryption:

  `ks2.usr`: model keystore

  `ks2.p7c`: list of certificates to be imported
- for a card account with only one key for signing and encryption:

  `gp1.usr`: model keystore

  `gp1.p7c`: list of certificates to be imported
- for a card account with two keys for signing and encryption:

  `gp2.usr`: model keystore

  `gp2.p7c`: list of certificates to be imported

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

The model folders can also include the Security BOX File and Security BOX Shredder list files. Each of the folders must have the following files:

- `SBoxFileList.dec`: Security BOX File decryption list
- `SBoxFileList.efp`: Security BOX File exclusion list
- `SBoxFileList.enc`: Security BOX File encryption list
- `SBoxShrdList.cfp`: Security BOX Shredder exclusion list
- `SBoxShrdList.cln`: Security BOX Shredder cleaning list

5.7. Volume automatically created upon the first connection

It is possible to automatically create a Security BOX Disk volume when the user first connects, using the following principles:

- The user is asked no questions, apart from a possible initial confirmation.
- The creation parameters are read from the `[Disk]` section in `Sbox.ini`.
- The process integrates the (silent) formatting for the created volume.

Because the creation may take a significant amount of time, a progress bar is displayed.

Information on creating this volume at the time of the first connection is provided in the section called “Volume data created on the first connection [Disk]” page 52.

5.8. Additional customizations

5.8.1. External files, customizing connection and “About” windows

For customization purposes, Security BOX Suite can use external files to modify the background image in the connection window or to modify the “About” window.

To use this functionality, you must create a subfolder called External in the same folder that contains the file `Security BOX Suite 8.0.msi` (in administered mode or not).

The files directly contained in this folder (possible sub-trees are not taken into account) will be recopied at the end of the installation to the External subfolder from the installation folder.

Note
These image files may be copied to the External folder (possibly creating the folder, if necessary) after the installation.

To customize the connection and “About” windows, the following image files must be in the External folder:

- `brand.bmp`: Top banner in the connection window (dimensions: 408x63)

- `line.bmp`: Separation line (dimensions: 410x2). The separate line is recognized only if there is a custom banner (`brand.bmp`).

These files must be in true-color BMP format (24-bit encoding for each pixel).

Warning
Deploying Security BOX with modified windows is subject to agreement with Arkoon Network Security.

5.8.2. Application preselection settings

Using the *SBREMOVE* property, it is possible to limit which application the user can install, even if the license authorizes others.

A practical use for this property is the ability to have different installation profiles while having a single license key and a single installation package.

Below is a list of possible values:

Code	Suppressed Product
SBoxFile	Security BOX File
SBoxDisk	Security BOX Disk
SBoxBroyeur	Security BOX Shredder
SBoxMailOutlook	Security BOX Mail Outlook Edition
SBoxMailNotes	Security BOX Mail Notes Edition
SBoxSign	Security BOX Sign
SBoxTeam	Security BOX Team
SBoxGina	Security BOX Gina on Windows XP or Security BOX Credential Provider on Windows Vista
SBoxExtCarteGen	Security BOX Card Extension
SBoxCSP	Security BOX Extension for Internet browsers

In the value for the SBREMOVE property, the different components whose installation is prohibited must be separated by a comma, without spaces.

Example: The <SBOXLICENCENUM> license key allows all of the Security BOX Suite components to be installed. The following command line deletes Security BOX File, and the Internet browser application extensions can be installed.

```
msiexec /i "<path>\Security BOX Suite 8.0" LICENCENUM=<SBOXLICENSENUM> SBREMOVE=SBoxFile,SBoxCSP
```

Note
With Vista, this command must be run in a command line window opened by an administrator.

Chapter 6. Advanced features

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

6.1. Installation procedure

6.1.1. Version updates

Security BOX Suite 8.0 can be installed directly onto a workstation equipped with Security BOX Suite 5.01 to 6.5. However, the update cannot be applied in silent mode.

If silent mode must absolutely be used, then the old version of the Security BOX Suite must be uninstalled silently, and then version 8.0 can be installed.

To migrate from an older version, you must:

1. Migrate from the original version to an intermediate version, making it possible to migrate to version 8.0.
2. Connect once to each Security BOX account that must be migrated. The format of Security BOX accounts changes between the different versions, and a migration takes place at the time of the first connection with a new version of the product.

6.1.2. Modifications

On a workstation where Security BOX Suite 8.0 is installed, access to the initial installation support is required only when adding a component.

When deleting a component or even when completely uninstalling the product, the initial source of the installation is no longer necessary. However, in some conditions, access to this source may be requested.

6.1.3. Patches

It is not possible to run a Security BOX Suite 8.0 patch directly from removable media (CD-ROM, etc.). You must first copy the `Security BOX Suite 8.0.msp` file to a local folder, and execute the local copy.

Unlike previous versions of Security BOX Suite, it is no longer necessary to have the initial installation source to be able to install a patch. However, in some conditions, access to this source may be requested.

Note
The product must never be updated by a user who is connected with unique authentication or when the temporary file folder is secured by Security BOX Team.

6.1.4. Installing using the command line

Windows Installs allows the user to specify elements to be installed or deleted in the command line using the *ADDLOCAL* and *REMOVE* properties.

However, we recommend that you avoid this method of installation for Security BOX Suite 8.0 because some of the applications's elements are hidden but required for the application to work. In addition, there are dependencies between some elements that will keep the applications from running properly if they are not respected.

6.2. General information for all Security BOX applications

6.2.1. Fast User Switching

The following Security BOX components are compatible with the Fast User Switching feature in Windows XP and Vista.

- Security BOX Disk
- Security BOX File
- Security BOX Mail Notes Edition
- Security BOX Mail Outlook Edition
- Security BOX Shredder
- Security BOX Sign
- Card extension (as long as a PKCS#11 interface is available).

6.2.2. Automatic backup copies

With each successful connection, Security BOX 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.

6.3. Events log

6.3.1. Introduction

Security BOX Suite has an events log mechanism enabling the administrators to monitor the defined security environnement and identify incidents taking place while the product is used. All the events related to Security BOX Suite can be accessed via Windows event viewer. Data can be read and analyzed and once the problem has been found, a solution ca 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 the section called “Types 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**: Security BOX Suite user name.
- **Computer**: computer name (NetBIOS).

6.3.2. Configuring the events log

During a new installation of Security BOX Suite, 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.

Configuring Group Policy Object with Windows XP

To configure the GPO (Group Policy Object), you must first upload the logs administration file in the group policy client (**GPEdit**).

Microsoft Windows XP® GPO uses `.adm` files to implement the group policies. The installation of Security BOX Suite places the `Sbsuite.adm` components configuration file in the `%SystemRoot%\inf` folder. This

file is not automatically uploaded when launching **GPEdit**, and it is then necessary to launch it the first time. To do so:

1. Launch **GPEdit** (**Start** > **Execute** > then enter **gpedit.msc**).
2. In **Computer configuration** > **Administrative templates**, right-click and select **Add/Remove templates...**.
3. Click on **Add**, then select the `Sbsuite.adm` file (in `%SystemRoot%\inf`).
4. Click on **Close**. The `Sbsuite.adm` file is then copied in `%SystemRoot%\system32\GroupPolicy\Adm` and uploaded in the GPO. From now, it will be uploaded when launching **GPEdit**.

   The **Security BOX components** folder has been created under **Administrative templates**. The **All modules: Activation [...]** entry enables to start the events generation once it has been activated.

   Note
   The other entries enable to configure the events generation more precisely.

A direct modification of the group policy modifies the corresponding values in the registry database. For example, activating the information and error messages for the TEAM module and deactivating the warning messages done from the GPO, implies the creation/modification of the corresponding registry keys.

Configuring Group Policy Object with Windows Vista

Microsoft Windows Vista ® 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 Security BOX Suite 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. The end of the procedure is equivalent to Microsoft Windows XP® procedure.

6.3.3. Using the events log

Any action done by Security BOX Suite 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.

6.4. Security BOX Disk

6.4.1. 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 Security BOX 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 called "Modifying a volume's users list via the .VBOXSAVE file [Disk]" page 53.

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 wanting a recovery must 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.

6.4.2. Unmounting by force

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

6.4.3. 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.

6.4.4. Limitations

- The maximum size of a Security BOX 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 Security BOX Disk volume may be incorrect in Explorer (either a normal disk icon or a document icon).

6.4.5. Windows XP

Some successive mounting or unmounting changes to the same volumes with different unit letters can cause the volume labels to be reversed in Explorer.

This is not a product anomaly but a reaction from a Windows XP component (MountManager).

6.5. Security BOX File

6.5.1. File permissions

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

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

6.5.2. Windows shutdown and long automatic processing

By default, Security BOX disconnects the Security BOX 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 Security BOX to not allow Windows to close a session if a Security BOX user is connected. To do this, put `NoShutDown`=1 in the `[Logon]` section of the `sbox.ini` file. See Section 3.3, “References”.

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

6.5.3. Syntax of the Security BOX 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
Security BOX Encryption List	*.enc
Security BOX Decryption List	*.dec
Security BOX 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	Note
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
```

6.5.4. Keywords for the Security BOX File file lists

Security BOX File file lists take the following keywords into account:

- *AppData*: a typical path is `C:\Documents and Settings\username\Application Data`
- *CommonDocuments*: a typical path is `C:\Documents and Settings\All Users\Documents`
- *Cookies*: a typical path is `C:\Documents and Settings\username\Cookies`
- *History*: file system folder used as a common folder for Internet history.
- *InternetCache*: a typical path is `C:\Documents and Settings\username\Local Settings\Temporary Internet Files`
- *Personal*: a virtual folder which represents the `My Documents` desktop item .
- *ProgramFiles*: a typical path is `C:\Program Files`
- *ProgramFilesCommon*: a typical path is `C:\Program Files\Common`
- *Recent*: a typical path is `C:\Documents and Settings\username\My Recent Documents`
- *System*: system folder Windows ®. A typical path is `C:\Windows\System32`
- *Windows*: Windows folder ® or SYSROOT. It corresponds to `%windir%` environment variables or `%SYSTEMROOT%`

  A typical path is `C:\Windows`

6.6. Security BOX Shredder

6.6.1. Syntax of the Security BOX 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
Security BOX Clean List	`*.cln`
Security BOX 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	Note
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

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

6.6.2. Windows shutdown and long automatic processing

By default, Security BOX disconnects the Security BOX user when the Windows session is closed (or 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 Security BOX to not allow Windows to close a session if a Security BOX user is connected. To do this, put `NoShutDown=1` in the `[Logon]` section of the `sbox.ini` file. See Section 3.3, “References”.

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

6.6.3. Keywords for the Security BOX Shredder file lists

Security BOX Shredder file lists take the following keywords into account:

- *AppData*: a typical path is `C:\Documents and Settings\username\Application Data`
- *CommonDocuments*: a typical path is `C:\Documents and Settings\All Users\Documents`
- *Cookies*: a typical path is `C:\Documents and Settings\username\Cookies`
- *History*: file system folder used as a common folder for Internet history.
- *InternetCache*: a typical path is `C:\Documents and Settings\username\Local Settings\Temporary Internet Files`

- *Personal*: a virtual folder which represents the `My Documents` desktop item .
- *ProgramFiles*: a typical path is `C:\Program Files`
- *ProgramFilesCommon*: a typical path is `C:\Program Files\Common`
- *Recent*: a typical path is `C:\Documents and Settings\username\My Recent Documents`
- *System*: system folder Windows. A typical path is `C:\Windows\System32`
- *Windows*: Windows folder or SYSROOT. It corresponds to `%windir%` environment variables or `%SYSTEMROOT%`

  A typical path is `C:\Windows`
- *BitBucket*: virtual folder which 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:\Documents and Settings\username\Application Data %temp%` -> `C:\Documents and Settings\username\Local Settings\Temp`
Then `<"Appdata"\..\local settings\temp>` is equivalent to `%temp%`
You must enter `%AppData%\..\local settings\temp\` in the list.

6.7. Security BOX Mail

6.7.1. Outlook Edition

Do not use Word as a message editor

For versions of Outlook prior to 2007, Microsoft Word should NOT be set up as a message editor.

To disable Word as a message editor, select **Options** in Outlook's **Tools** menu.

For XP and Outlook 2003, go to the **Mail Format** tab and uncheck the **Use Word to edit e-mail messages** check box.

Forcing Outlook to enable Security BOX Mail

Sometimes after installing Security BOX Mail – Outlook Edition, Outlook does not enable the Security BOX Mail extension. There is no Security BOX menu in the **Tools** menu, no security options available when sending a message, etc.

You must then:

1. Exit Outlook.
2. Search for the file `extend.dat` on your workstation and delete it. This file is typically in:
   - `C:\Documents and Settings\USERNAME\Local Settings\Application Data\Microsoft\Outlook` on XP
   - `C:\Users\USERNAME\AppData\Local\Microsoft\Outlook` on Vista
3. Restart Outlook.

This deletion forces Outlook to reread the registry key containing its extensions.

> **Note**
> All of the listed extensions are then re-enabled. If one of them was disabled before, you must disable it again.

To disable an extension from Outlook's main window:

For Outlook XP and 2003:

1. Select the **Tools/Options** menu.
2. Open the **Other**.
3. Click on **Advanced Options**.
4. Then click on **Add-In Manager**.

For Outlook 2007:

1. Select the **Tools/Trust Center** menu.
2. Select **Add-Ins** from the list on the left.
3. Select **Exchange Client Extensions** in the combo box at the bottom.
4. Click on **OK**.

6.7.2. Notes Edition not enabled

The installation procedure for Security BOX 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 Security BOX extension has not been enabled.

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), Security BOX 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 Security BOX Mail information to the end of the line.

6.8. Security BOX Team

6.8.1. DFS environment restriction

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

6.8.2. 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.

6.8.3. 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 Security BOX Team.

6.8.4. 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.

Security BOX 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.

6.8.5. Optimizing access on slow networks

To know if a file is really encrypted or not, Security BOX 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, Security BOX 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\SYSTEM\CurrentControlSet\Services\SboxTeamDrv\Parameters`, the key `CacheActivate (DWORD) = 1`
- 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 an secured folder, an unencrypted file appears as encrypted.

6.8.6. Improving performances when browinsg encrypted trees

This improvement reduces significantly the time for determining the status of an unencrypted or encrypted folder (determination of the icon of a folder) in "Smart Card" mode. This option is set through the `OverlayIconAccuracy` in the registry:

```
HKEY_LOCAL_MACHINE\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Team

OverlayIconAccuracy = 0x40
```

This value can be combined with other current values.

6.8.7. Folder exclusion

Security BOX Team provides the **ExcludedPath** feature, which enables to exclude folders from Security BOX 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.

- La gestion de l'**OverlayIcon** : l'overlayIcon Team n'est pas affiché sur un dossier d'une arborescence exclue du chiffrement.

If you want to exclude a folder fromSecurity BOX TEAM analysis , you must add it to **ExcludedPath**into 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 `< >`

Important
You must 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:\Documents and settings\All Users\Application Data`
- `COMMON_DOCUMENTS`: `C:\Documents and settings\All Users\Documents`
- `USERNAME`: `<username>` Windows user's name .
- `LOCAL_APPDATA`: `C:\Documents and settings\<username>\Local settings\Application Data`
- `DESKTOP`: `C:\Documents and settings\<username>\desktop`
- `MYDOCUMENTS`: `C:\Documents and settings\<username>\My Documents`
- `PROFILE`: `C:\Documents and settings\<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.

6.8.8. 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.

There are some restrictions to these rules:

- If Security BOX user is not connected, it is allowed to move a folder which has a personal rule.

- If the user is not connected, moving is not allowed but ONLY IF the source folder and/or the destination folder have a personal rule. If both directories have a rule, the ban takes effect when the rules are different.
- If moving a folder is allowed, the files of subdirectories which possibly have a private rule keep their security (there is neither encryption nor decyphering).

6.8.9. Mobile profiles support

During files synchronization for a mobile device, Windows uses the files modification date to find out if the files need to be synchronized. By default, Security BOX Team keeps the files modification date when their security has changed (first encryption, adding a new user, desecurization). In this cas, file previously synchronized are not synchronized in their new state.

To ensure files synchronization, you must indicate the *UpdateFileDateOnSecurityUpdate=1* parameter into the `Sbox.ini` file.

6.8.10. Accessing a file is not allowed if the certificate is revoked

Security BOX 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.

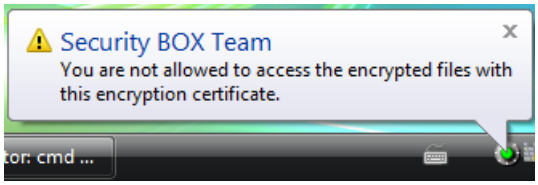
  Note
  These operations fail even if the file is encrypted with an old encryption key.
- Any operation on security rules (personal and shared rules) is impossible. The user interfaces are greyed out and they only allow reading for rules parameters.

Security BOX 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.

6.8.11. Modifying the last access dates

Some solutions (as the archive solutions) are based on last access dates of files to operates treatments. However, when Security BOX 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 Security BOX 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; • `0x00000004`: restoration of access date on Netware 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** The `0x8` value also works with standard FS but with a performance penalty. It can be useful on other unusual CIFS servers.

Also refer to the following parameters:

- `OverlayIconAccuracy`: enables not to change the access dates to files (values: `0x00000020`) ;
- `UpdateFileDateOnSecurityUpdate`: enables to change the dates of creation/modification/last access to files during the change of security.

6.8.12. 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.

6.8.13. Information to provide when reporting a problem

In the event of a problem on a workstation, you must tell Security BOX support the exact environment stored on the workstation:

- The version, the patch number and the language used for Security BOX ;
- The type of version installed: official, evaluation, trace ;
- The Security BOX license number ;
- The list of components installed: Mail Edition, File, 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 Security BOX Outlook Edition is involved: the version and SP for the Outlook client and the Exchange server ;
- If the Security BOX 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 model, the drive type, the name of the PKCS#11 DLL used and its version.

6.9. Information to provide when reporting a problem

In the event of a problem on a workstation, you must tell Security BOX support the exact environment stored on the workstation:

- The version, the patch number and the language used for Security BOX ;
- The type of version installed: official, evaluation, trace ;
- The Security BOX license number ;
- The list of components installed: Mail Edition, File, 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 Security BOX Outlook Edition is involved: the version and SP for the Outlook client and the Exchange server ;
- If the Security BOX 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 model, the drive type, the name of the `PKCS#11 DLL` used and its version.

Glossary

C

Certificate	A certificate is used to encrypt information (files or e-mail messages) before sending it to a correspondent. Certificates include a **public key**.
Certificate authority	When you need a trusted certificate, you can request one from a certificate authority.
Certificate group	A group of certificates created in Security BOX. This allows you to encrypt to a group rather than individually.
Certificate revocation list	A list of certificates that have been revoked or are no longer valid, and therefore should not be relied upon.
CRL	See Certificate revocation list.

D

Distribution point	Provides updates for CRL or user account updates (where USX fields can be found and updated).

E

Encryption	A method used to protect data (files or e-mails) by transforming the information using an algorithm to make it unreadable to anyone except those possessing the necessary decryption key.
Encryption key	If a user has two keys (one for signing and one for encryption), this is the key for encryption. This also refers to the unique key for users who have just one key for encryption.

K

Keystore	An account file with a `.usr` extension, containing: • the user's private keys for a "password" account • configuration data for Security BOX applications.

P

Personal key	If a user has just one key for signing and encryption, it is called a **personal key**.
PKI	Public key infrastructure. It links public keys with users by means of a certificate authority.
Private key	When creating a key, two keys are created: the private key and the public key. The private key is kept secret, while the public key may be widely distributed.

	Incoming messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key.
Public key	When creating a key, two keys are created: the private key and the public key. The private key is kept secret, while the public key may be widely distributed. Incoming messages are encrypted with the recipient's public key and can only be decrypted with the corresponding private key.

R

Recovery certificate	The recovery certificate is linked to a recovery account. When implemented, it is used in all user accounts to encrypt all files, messages, etc.

S

Secret code	When you create a Security BOX user account, you create a “secret code” or password to use the account.
Security Officer	A backup or emergency password to be used when the normal password is forgotten, and the Security BOX account is blocked.
Signature key	If a user has two keys (one for signing and one for encryption), this is the key for signing. This also refers to the unique key for users who have just one key for a signature.

T

Transcyphering	When updating the authorized user list, Security BOX File re-encrypts the file using a new key encryption. This operation is referred to as transciphering.
Trusted address book	List of correspondent contacts created by the user, which includes the correspondent's certificate.

U

User account	A set of user-specific files that allow the user to use Security BOX.

Security BOX

ARKOON

NETWORK SECURITY