GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

GUIDE D'ADMINISTRATION

Version 10.1.1

Dernière mise à jour du document : 8 février 2023

Référence : sds-fr-sds_suite-guide_d_administration-v10

Table des matières

Dans la documentation, Stormshield Data Security Enterprise est désigné sous la forme abrégée : SDS.

Préface

A propos de ce guide

Ce guide fournit les informations techniques nécessaires au déploiement et à l'administration de Stormshield Data Security Enterprise. Il complète les manuels d'utilisation des différents composants de la suite Stormshield Data Security. Il s'applique à la version 10.1.1 de Stormshield Data Security Enterprise.

Audience

Ce guide s'adresse

- à l'administrateur de la sécurité qui définit la politique de sécurité.
- à l'administrateur système en charge du déploiement et de l'installation de Stormshield Data Security Enterprise.

Abréviations

Types de compte

Le tableau suivant liste les types de compte disponibles dans Stormshield Data Security Enterprise :

KS1	Compte mot de passe avec une seule clé pour signer et/ou chiffrer.
KS2	Compte mot de passe avec deux clés différentes pour signer et chiffrer.
GP1	Compte carte avec une seule clé pour signer et/ou chiffrer.
GP2	Compte carte avec deux clés différentes pour signer et chiffrer.

Dossiers

Le tableau suivant regroupe les abréviations des dossiers utilisés dans Stormshield Data Security Enterprise :

ProgDir	Dossier standard d'installation des applications. Par défaut : **C:\Program Files**
InstallDir	Dossier d'installation de Stormshield Data Security. Par défaut : **<ProgDir>\Arkoon\Security BOX**
WinDir	Dossier racine de Windows : **C:\WINDOWS**
SysDir	Dossier système de Windows. Par défaut : **<WinDir>\System32**

DrivDir	Dossier des pilotes Windows. Par défaut : **<SysDir>\Drivers**
CommonFilesDir	Dossier contenant les fichiers communs. Par exemple : **C:\Program Files\Fichiers Communs**
InfDir	Dossier contenant les fichiers d'installation et de description de pilotes sous Microsoft Windows. Par exemple : **<WinDir>\Inf**

Clés racine du registre de Windows

Clés racine du registre de Windows

Le tableau suivant liste les clés racine du registre de Microsoft Windows :

HKCR	HKEY_CLASSES_ROOT
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE

1. Environnement d'utilisation

Pour utiliser Stormshield Data Security Enterprise dans les conditions de son évaluation Critères Communs et de sa qualification au niveau standard, il est impératif de respecter les recommandations suivantes.

1.1 Recommandations sur la veille sécurité

1. Consultez régulièrement les alertes de sécurité diffusées sur https://advisories.stormshield.eu/.
2. Appliquez systématiquement une mise à jour du logiciel si elle contient la correction d'une faille de sécurité. Ces mises à jour sont disponibles sur votre espace client MyStormshield.

1.2 Recommandations sur les clés et les certificats

1. Les clés RSA des utilisateurs et des autorités de certification doivent être d'une taille minimale de 4096 bits, avec un exposant public strictement supérieur à 65536.
2. Les certificats et les CRL doivent être signés avec l'algorithme d'empreinte SHA-512.

1.3 Recommandations sur les algorithmes

1. Stormshield Data Security supporte différents algorithmes mais préconise l'utilisation de AES 256, RSA 2048, SHA 512.
2. Les algorithmes Triple DES, RC4 et RC5 sont également supportés.
3. Les mécanismes RC2 et DES sont supportés pour compatibilité mais il est déconseillé de les utiliser car ils comportent des faiblesses connues.

1.4 Recommandations sur les comptes utilisateurs

1. Les comptes utilisateurs doivent être protégés par l'algorithme de chiffrement AES et le standard de hachage cryptographique SHA-256.
2. Les mots de passe doivent être soumis à une politique de sécurité empêchant les mots de passe faibles.
3. Des mesures organisationnelles adaptées doivent assurer l'authenticité des modèles à partir desquels les comptes utilisateurs sont créés.
4. En cas d'utilisation d'un porte-clés matériel (carte à puce ou token matériel), ce dispositif assure la protection en confidentialité et en intégrité des clés et des certificats qu'il contient.

1.5 Recommandations sur les intervenants

1. L'administrateur de la sécurité est considéré de confiance. Il définit la politique de sécurité de Stormshield Data Security en respectant l'état de l'art, et éventuellement crée les comptes des utilisateurs via l'application Stormshield Data Authority Manager.

2. L'administrateur système est également considéré de confiance. Il est en charge de l'installation et de la maintenance de l'application et du poste de travail (système d'exploitation, logiciels de protection, librairie *PKCS#11* d'interface avec une carte à puce, applications bureautiques et métier, etc). Il applique la politique de sécurité définie par l'administrateur de la sécurité.
3. L'utilisateur du produit doit respecter la politique de sécurité en vigueur dans son organisme.

1.6 Recommandations sur les postes de travail

1. Le poste de travail sur lequel Stormshield Data Security est installé doit être sain. Il doit pour cela exister dans l'organisation une politique de sécurité du système d'information dont les exigences sont respectées sur les postes de travail. Cette politique doit notamment prévoir que les logiciels installés soient régulièrement mis à jour et que le système soit protégé contre les virus et autres logiciels espion ou malveillant (pare-feu correctement paramétré, antivirus à jour, etc).
2. La politique de sécurité doit également prévoir que les postes non équipés de Stormshield Data Security n'aient pas accès aux dossiers confidentiels partagés sur un serveur, afin qu'un utilisateur ne puisse pas provoquer un déni de service en altérant ou en supprimant, par inadvertance ou par malveillance, les fichiers protégés par le produit.
3. L'accès aux fonctions d'administration du système du poste est restreint aux seuls administrateurs système.
4. Le système d'exploitation doit gérer les journaux d'événements générés par le produit en conformité avec la politique de sécurité de l'organisation. Il doit par exemple restreindre l'accès en lecture à ces journaux aux seules personnes explicitement autorisées.
5. L'utilisateur doit veiller à ce qu'un attaquant potentiel ne puisse pas observer voire accéder au poste lorsque la session Stormshield Data Security est ouverte.

1.7 Environnement de certification et de qualification

Les modules logiciels évalués dans le cadre de la certification Critères Communs EAL3+ et de la qualification de Stormshield Data Security sont :

1. Le composant "Chiffrement transparent" (Stormshield Data Team), qui assure la définition des règles de sécurité, le chiffrement des fichiers conformément à ces règles, et le chiffrement du fichier d'échange du système (mémoire paginée ou swap).
2. Le "noyau Stormshield Data Kernel", commun à tous les produits de la gamme, qui assure l'authentification de l'utilisateur, surveille l'inactivité du poste, gère un annuaire de certificats de confiance, et contrôle la non-révocation des certificats utilisés.
3. Le module cryptographique logiciel interne (Stormshield Data Crypto), qui gère les clés de l'utilisateur, qu'elles soient stockées dans un fichier (implémentation logicielle) ou dans une carte à puce.

En revanche, les modules suivants sont en dehors du périmètre de l'évaluation :

1. L'outil d'administration Stormshield Data Authority Manager.
2. L'éventuelle carte à puce et son middleware *PKCS#11*.

2. Comptes utilisateurs

Des comptes utilisateurs sont nécessaires pour utiliser Stormshield Data Security. Ils doivent être installés comme décrit dans les sections suivantes.

2.1 Localisation

Lors d'une connexion, Stormshield Data Security recherche par défaut le compte d'un utilisateur dans le dossier défini dans le fichier *SBox.ini*, section `[User]`, item `RootPath1` (reportez-vous à la section Section [User]).

Si le compte n'est pas trouvé dans ce dossier, Stormshield Data Security le recherche dans le dossier `RootPath2`.

Par défaut, `RootPath1 = COMMON_APPDATA\Arkoon\Security BOX\Users` et `RootPath2` ne sont pas renseignés (reportez-vous à la section Utilisation de mots-clés dans les paramètres RootPath).

`RootPath1` est également le dossier dans lequel Stormshield Data Security crée un nouveau compte. En cas d'échec, il n'y a pas de repli sur `RootPath2`.

Les dossiers `RootPath1` et `RootPath2` peuvent être sur un serveur partagé, une disquette, une clé USB ou tout autre support amovible en lecture-écriture.

Il est ainsi possible de :

- centraliser les comptes des utilisateurs d'un réseau local sur un serveur ;
- stocker sur une unité amovible le compte d'un utilisateur nomade.

NOTE
Les paramètres `RootPath1` et `RootPath2` peuvent être personnalisés. Le chemin indiqué doit néanmoins correspondre à une arborescence valide sur le poste de travail. En effet, le package d'installation ne construit que le chemin par défaut. Si le chemin est personnalisé, l'arborescence doit être reconstruite manuellement (voir la section Nommage et permissions).

2.2 Nommage et permissions

Dans les dossiers `RootPath1` et `RootPath2`, le nom du dossier utilisateur dépend du type de compte :

- si le compte est de type mot de passe, le nom du dossier est l'identifiant de l'utilisateur ;
- si le compte est de type carte ou token USB, le nom du dossier est le numéro de la carte ou du token USB.

Si l'utilisateur crée lui-même son compte, le dossier `RootPath1` doit avoir la permission **Contrôle total** pour **Tout le monde**, laquelle s'applique aux sous-dossiers.

Sur un dossier donné :

- l'utilisateur doit avoir au minimum la permission de **Modifier** ;
- les autres utilisateurs peuvent avoir **Aucun accès**. Cette interdiction d'accès aux autres utilisateurs est fortement recommandée si les dossiers `RootPath1` ou `RootPath2` sont sur un serveur ou s'ils sont sur une machine partagée par plusieurs utilisateurs.

2.3 Fichiers constituant un compte utilisateur

Le tableau suivant liste les fichiers constituant un compte utilisateur :

<identifiant>.usr	Fichier principal, également appelé KeyStore. Il contient : • les clés privées de l'utilisateur (en mode mot de passe) ; • les certificats actuels et passés ; • les données de configuration du noyau et des applications de Stormshield Data Security ; • les données de protection des autres fichiers du compte (clés de chiffrement et sceaux). Si ce fichier est corrompu, la connexion échoue. Le message d'erreur suivant s'affiche : **Votre fichier utilisateur est inaccessible**.
<identifiant>.usd	Annuaire de confiance de l'utilisateur. Il contient les certificats des correspondants et des autorités auxquels l'utilisateur fait confiance. Si ce fichier est effacé ou corrompu, la connexion échoue. Le message d'erreur suivant s'affiche : **Le chargement d'un composant système a échoué**.
<identifiant>.bcrl	Base de données du contrôleur de révocation, incluant pour chaque émetteur de CRL : • des données de gestion ; • la liste des certificats révoqués. Si ce fichier est corrompu, la connexion est acceptée. Le message d'alerte suivant s'affiche : **Votre base personnelle de certificats révoqués a été illégalement altérée**. Si ce fichier est effacé, la connexion est acceptée. Le message d'alerte suivant s'affiche : **Votre base personnelle de certificats révoqués a été illégalement supprimée. Une nouvelle base va être automatiquement reconstruite**.
SBoxFileList.dec	Liste de déchiffrement de Stormshield Data File. (1)
SBoxFileList.efp	Liste d'exclusion de Stormshield Data File. (1)
SBoxFileList.enc	Liste de chiffrement de Stormshield Data File. (1)
SBoxFileList.cfp	Liste d'exclusion de Stormshield Data Shredder. (1)
SBoxFileList.cln	Liste de nettoyage de Stormshield Data Shredder. (1)

(1) Pour ces fichiers :

- Si un fichier liste est corrompu, la connexion est acceptée et une alerte est affichée à l'ouverture de la liste. Le message suivant s'affiche : **Votre fichier liste de chiffrement/déchiffrement/nettoyage/protection a été modifié à votre insu. Voulez-vous quand même charger cette liste ?**
- Si un fichier liste est effacé, la connexion est acceptée et une alerte est affichée à l'ouverture de la liste. Le message suivant s'affiche : **Le fichier liste de chiffrement/dechiffrement/nettoyage/protection est introuvable. Votre liste va être réinitialisée.**

L'assistant d'exportation du compte (**propriétés de l'utilisateur/assistants/export de compte**) permet de regrouper ces fichiers dans un programme d'installation qui va permettre de copier le compte complet sur un autre poste de travail. De plus amples informations sur l'exportation de compte sont disponibles dans le *Guide d'installation et de mise en œuvre*.

2.4 Attributs *PKCS#11* des clés fournies à Stormshield Data Security

Si les clés sont tirées par une PKI externe, les attributs *PKCS#11* suivants sont nécessaires :

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

3. Politiques locales

Les politiques locales rassemblent tous les paramètres de fonctionnement administrables qui sont indépendants d'un utilisateur.

Elles peuvent être définies dans le fichier de configuration *SBox.ini* ou par des stratégies de groupes (GPO).

3.1 Fichier de configuration *SBox.ini*

Ce fichier est installé par défaut dans le dossier **<InstallDir>\Kernel**.

Les caractères Unicode ne sont pas supportés par le fichier *SBox.ini*. Par conséquent, les chemins paramétrés ne doivent contenir que des caractères ANSI, excepté les caractères / * ? < > " | ! # @. Néanmoins, ces caractères peuvent être insérés entourés de guillemets.

3.2 Paramétrage via les Group Policy Windows

3.2.1 Généralités

Les paramètres de configuration du fichier *SBox.ini* peuvent également être définis via les **Group Policy** (GPO) du système.

Chaque paramètre peut être défini au niveau “Machine” ou au niveau “Utilisateur”.

> **NOTE**
> Il est recommandé de définir les paramètres de politique locale par GPO plutôt que via le fichier *SBox.ini*.

Il est possible de générer des fichiers *.adm* intégrables dans la console **Stratégie de Groupe**, lesquels permettent de paramétrer les options.

3.2.2 Priorités de lecture

La détermination d'un paramètre [Section,Item] s'effectue dans l'ordre de lecture suivant :

1. Clé `HKCU\Software\Policies\Arkoon\Security BOX Suite\<Section>\<Item>` (l'item est toujours au format REG_SZ).
2. Clé `HKLM\Software\Policies\Arkoon\Security BOX Suite\<Section>\<Item>` (l'item est toujours au format REG_SZ).
3. Fichier *SBox.ini*.

Stormshield Data Security prend en compte la première configuration trouvée et ignore les suivantes. Ainsi, si un paramètre est configuré dans le répertoire HKCU, le répertoire HKLM et le fichier *SBox.ini* sont ignorés.

3.3 Références

Les tableaux ci-dessous spécifient les politiques administrables :

- la troisième colonne indique pour chaque paramètre s'il peut être présent dans une GPO et dans quelle classe : Machine/User. Si la cellule du tableau n'est pas renseignée, c'est que le paramètre ne peut pas être placé dans une GPO ;
- si une valeur optionnelle du fichier de configuration est invalide, la valeur par défaut est utilisée ;
- en cas de modification du contenu du fichier *SBox.ini*, il est recommandé de redémarrer l'ordinateur pour garantir que toutes les modifications seront bien prises en compte.

3.3.1 Section [Logon]

Le tableau suivant décrit les paramètres de la section [Logon] :

Paramètre	Description	GPO
`AllowPassword`	Autorise une connexion à Stormshield Data Security en mode mot de passe : • 0 : non autorisé (par défaut) ; • 1 : autorisé.	Machine/User
`AllowCard`	Autorise une connexion à Stormshield Data Security en mode carte ou clé USB : • 0 : non autorisé (par défaut) ; • 1 : autorisé.	Machine/User
`AllowLocalUnblock`	Autorise un déblocage local si la session Stormshield Data Security de l'utilisateur est bloquée : • 0 : non autorisé ; • 1 : autorisé (par défaut).	Machine/User
`AllowDistantUnblock`	Autorise un déblocage distant si la session Stormshield Data Security de l'utilisateur est bloquée : • 0 : non autorisé ; • 1 : autorisé (par défaut).	Machine/User
`ConnectOnCard`	Affichage de la fenêtre de connexion Stormshield Data Security avec saisie du code secret sur insertion carte : • 0 : pas d'affichage (par défaut) ; • 1 : affichage. La fenêtre s'affiche seulement s'il n'y a pas déjà un compte Stormshield Data Security connecté (mot de passe ou carte).	Machine/User
`UnFreezeOnCard`	Affiche la fenêtre de déverrouillage carte sur insertion carte si la session Stormshield Data Security de l'utilisateur est verrouillée : • 0 : non ; • 1 : oui (par défaut). La fenêtre ne s'active que si l'utilisateur connecté utilise un compte Stormshield Data Security en mode carte.	Machine/User

Paramètre	Description	GPO
`P10RequestEmail`	Valeur du lien **mailto** utilisé en fin de demande de certificat pour envoyer la demande par mail. Syntaxe de base (sur une seule ligne) : `<Adresse e-mail de l'autorité>?subject=<Objet du message> [&body=<message d'accompagnement>]`. Des informations plus détaillées sur la syntaxe peuvent être trouvées au niveau de la documentation des liens **mailto**. Ce paramètre est optionnel. S'il n'est pas présent, les informations seront à entrer manuellement par l'utilisateur.	Machine/User
`DontShowLicenceKey`	Permet de ne pas afficher la valeur de la clé de licence dans la fenêtre **A propos de Stormshield Data Security** : • 0 : la clé de licence est affichée normalement (par défaut) ; • 1 : la clé de licence n'est pas affichée. Il est recommandé dans le cadre d'un déploiement de ne pas afficher la clé de licence qui est spécifique à l'entreprise utilisatrice.	Machine/User
`DontShowPath2`	Désactive l'affichage du chemin quand le paramètre `RootPath2` est utilisé : • 0 : affichage du chemin complet d'accès au compte (par défaut) ; • 1 : pas d'affichage du chemin complet d'accès au compte. L'affichage du chemin complet permet de bien identifier le compte Stormshield Data Security utilisé pour la connexion mais il n'a pas de signification réelle pour un utilisateur standard. Cela permet d'identifier très facilement les connexions faites sur le `RootPath1` de celles effectuées sur le `RootPath2`.	Machine/User
`SlotFilterOn`	Si plusieurs lecteurs de carte ou tokens sont connectés au poste (par exemple un lecteur standard et une carte réseau 3G), cet item permet de prendre en compte un lecteur précis en définissant un filtre permettant de l'identifier. • 0 : tout lecteur est pris en compte (par défaut) ; • 1 : seul le lecteur indiqué à la section [SlotFilter] est pris en compte par Stormshield Data Security (reportez-vous à la section Section [SlotFilter]).	Machine/User
`UpgradeEncipher CardAccount`	Permet l'ajout automatique d'une clé de signature à un compte mono-clé chiffrement • 0 : (par défaut) ; • 1 : activation de la fonctionnalité.	Machine/User

Paramètre	Description	GPO
ExternalCardAuthent	Permet d'activer la mire de connexion de Stormshield Data Security pour l'utilisation d'un PIN-PAD externe lors de la saisie d'un code PIN (mode carte ou token). • 0 : pas d'authentification par PIN-PAD externe (valeur par défaut) ; • 1 : authentification par PIN-PAD externe.	
LDAPVersion	Permet de choisir la version de LDAP à utiliser lors de la connexion à l'annuaire, parmi les valeurs suivantes : • 2 : utilisation de la version 2 • 3 : utilisation de la version 3 (par défaut)	

3.3.2 Section [UpgradeEncipherCardAccount_CertificateTemplate]

Paramètre	Description	GPO
`UpgradeEncipherCardAccount_CertificateTemplate`	Permet de définir le gabarit du certificat de signature présent sur la carte. • `KeyUsage` Précise la liste des `KeyUsages` du certificat selon la syntaxe suivante : `KeyUsage = <Valeur>*(+ <Valeur>)` où `<Valeur>` est l'un des mots-clés suivants : • 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** En cas d'absence de l'item, il n'y a pas de filtrage sur le `KeyUsage`. • `ExtendedKeyUsage` `ExtendedKeyUsage = <EkuToken> *(, <EkuToken >)` `<EkuToken>= <Oid>| <EKUKeyWord>` `<EKUKeyWord>= clientAuth	emailProtection` <Oid> est la représentation "String" de l'OID (Exemple : 1.3.6.1.5.5.7.3.2). **NOTE** En cas d'absence de l'item, il n'y a pas de filtrage sur `extendedKeyUsage`. • `AuthorityCommonName` Cet item contient la valeur du `commonName` de l'émetteur du certificat : `AuthorityCommonName =<CN de l'émetteur du certificat>`	Machine/User

3.3.3 Section [SlotFilter]

Cette section doit être renseignée uniquement dans le cas où l'item `SlotFilterOn` de la section [Logon] vaut 1. Si ce n'est pas le cas, son contenu est ignoré.

Le tableau suivant décrit les paramètres de la section [SlotFilter] :

Paramètre	Description	GPO
`SlotInfoDescriptionPrefix`	Indique le préfixe du champ description remonté par le lecteur (`slotinfo.SlotDescription` au niveau *PKCS#11*). Par exemple, si la donnée de configuration est positionnée à SER, SERIAL sera accepté tandis que USB ne le sera pas. Ce paramètre est sensible à la casse. Si ce champ n'est pas présent, aucun filtrage n'est effectué sur les données.	Machine
`SlotInfoManufacturerIdPrefix`	Indique le préfixe du champ <ManufacturerId> remonté par le lecteur (`slotinfo.ManufacturerId` au niveau *PKCS#11*). Par exemple, si la donnée de configuration est positionnée à AX, AXALTO sera accepté tandis que GEMPLUS ne le sera pas. Ce paramètre est sensible à la casse. Si ce champ n'est pas présent, aucun filtrage n'est effectué sur les données.	Machine

Vous pouvez utiliser les caractères spéciaux "*" et "?" pour élargir le périmètre du filtre.

3.3.4 Section [User]

Le tableau suivant décrit les paramètres de la section [User] :

Paramètre	Description	GPO
`RootPath1`	Dossier principal de recherche du compte d'un utilisateur lors de sa connexion. Si le compte n'est pas trouvé dans le dossier indiqué, il est recherché dans `RootPath2` (si positionné). Ce dossier peut désigner un support amovible (disquette, clé USB…). Reportez-vous à la section Nommage et permissions pour les règles de nommage et les permissions nécessaires. Ce paramètre est obligatoire. Valeur fixée par défaut à l'installation : `<COMMON_APPDATA>\Arkoon\Security BOX\Users` Si ce paramètre est absent ou invalide, il n'est pas possible de se connecter à Stormshield Data Security. L'utilisation de mots-clés dans ce paramètre est autorisé, reportez-vous à la section Utilisation de mots-clés dans les paramètres RootPath.	Machine/User
`RootPath2`	Dossier complémentaire pour la recherche du compte d'un utilisateur. Ce paramètre est facultatif.	Machine/User

Paramètre	Description	GPO
ConnectPopup	Dans la fenêtre de connexion, un clic droit sur le champ **Identifiant** peut afficher l'historique des derniers utilisateurs qui se sont connectés : • 0 : l'historique n'est pas affiché (par défaut) ; • 1 : l'historique est affiché. Cette option est utile lorsque plusieurs utilisateurs Stormshield Data Security utilisent un même poste afin qu'ils puissent facilement accéder à leur compte Stormshield Data Security.	Machine/User
ShowBrowse	Affichage de l'item **Parcourir** dans l'historique des derniers utilisateurs connectés : • 0 : item absent (par défaut) ; • 1 : item présent. La fonction **Parcourir** permet de se connecter à des comptes qui ne sont ni dans RootPath1, ni dans RootPath2. Cette fonction est utile pour des postes d'administrateurs accédant à des comptes dans différentes arborescences. La prise en compte de ce paramètre nécessite que ConnectPopup soit positionné sur 1.	Machine/User
ShowLastUsers	Nombre d'utilisateurs à afficher dans l'historique : de 0 (par défaut) à 10. Si la valeur saisie est supérieure à 10, celle-ci est ramenée automatiquement à 10. La prise en compte de ce paramètre nécessite que ConnectPopup soit positionné sur 1.	Machine/User
HideCompletion	Dans la fenêtre de connexion, quand l'utilisateur saisit son identifiant, Stormshield Data Security peut compléter automatiquement la saisie avec le premier identifiant trouvé dans l'historique des utilisateurs connectés et commençant par ce que l'utilisateur a déjà saisi : • 0 : complétion automatique activée (par défaut) ; • 1 : complétion automatique désactivée.	Machine/User

Utilisation de mots-clés dans les paramètres RootPath

Les paramètres RootPath1 et RootPath2 peuvent inclure :

- une variable d'environnement, indiquée sous la forme <%variable%> ;
- un mot-clé, indiqué sous la forme <KeyWord>.

Le tableau suivant décrit les mots-clés supportés :

Mot-clé	Description
COMMON_APPDATA	Répertoire contenant les données d'application de tous les utilisateurs. Le chemin type est **C:\ProgramData**.
COMMON_DOCUMENTS	Répertoire contenant les fichiers communs à tous les utilisateurs. Le chemin type est **C:\Users\Public\Documents**.

Mot-clé	Description
DESKTOP	Répertoire utilisé pour le stockage de fichiers sur le bureau. Le chemin type est **C:\Users\<username>\Desktop**.
LOCAL_APPDATA	Répertoire utilisé pour les données des applications locales. Le chemin type est **C:\Users\<username>\AppData\Local**.
MYDOCUMENTS	Répertoire utilisé pour le stockage des documents de l'utilisateur. Le chemin type est **C:\Users\<username>\Documents**.
PROFILE	Le dossier du profil de l'utilisateur. Le chemin type est **C:\Users\<username>**.
PROFILES	Le dossier des profils des utilisateurs. Le chemin type est **C:\Users**.
USERNAME	Nom d'utilisateur Windows.

3.3.5 Section [NewUser]

Les sections [NewUser] et [SBox.NewUserWizardExXXX] concernent la création de compte :

- la section [NewUser] est commune à tous les types de création de compte ;
- la section [SBox.NewUserWizardExXXX] concerne uniquement la création de compte de type XXX, qui peut être KS1, KS2, GP1, ou GP2 (reportez-vous à la section Types de compte).

Le tableau suivant décrit les paramètres de la section [NewUser] :

Paramètre	Description
`AllowNewUser`	Création de compte : • 0 : non autorisée ; • 1 : autorisée (par défaut).
`CertLife`	Durée de validité, en années, des certificats auto-générés par Stormshield Data Security : • La valeur doit être entre 1 et 20 ; • Valeur par défaut = 20 ans.
Type de clé	Liste des clés (type et longueur) à proposer pour la création de compte. Voir la section Types de clé de l'utilisateur.

Types de clé de l'utilisateur

Les types de clés supportés (clés privées de l'utilisateur) sont KEY_RSA_2048BITS et KEY_RSA_4096BITS.

Un type de clé peut être :

- 0 : non autorisé ;
- 1 : autorisé ;
- 2 : autorisé et proposé par défaut.

Pour un type de compte, un seul type de clé peut être autorisé et proposé par défaut.

Les types de clés supportés sont définis à l'aide d'items dont la valeur est constituée d'une suite ordonnée de 6 chiffres, chaque chiffre correspondant à un type de compte. L'ordre des types de comptes est le suivant :

KS1, KS2, GP1, GP2, RFU, CPS2 (RFU et CPS2 ne sont pas utilisés, mais ces colonnes sont nécessaires).

Exemple de paramétrage des types de clés :

Si KEY_RSA_2048BITS est la valeur par défaut, et si KEY_RSA_1024BITS est interdit, il faut paramétrer de la façon suivante :

- KEY_RSA_1024BITS = 000000
- KEY_RSA_2048BITS = 222222
- KEY_RSA_4096BITS =111111

Afin d'éviter l'impossibilité de création d'un compte en cas d'erreur de paramétrage du fichier *SBox.ini*, les comportements suivants sont adoptés :

- si aucune valeur par défaut n'est indiquée, la taille de clé la plus forte autorisée est utilisée comme valeur par défaut ;
- si un caractère non prévu est saisi comme valeur d'un des types de clé, la valeur 0 (valeur non autorisée) est utilisée ;
- si tous les caractères ne sont pas saisis, les caractères manquants à droite sont considérés comme des 0 (valeur non autorisée). Par exemple, 111 est compris comme étant 111000 ;
- si plusieurs valeurs par défaut sont indiquées, la valeur par défaut proposée est celle indiquée par défaut et ayant la plus grande taille de clé.

Cependant, si aucun algorithme n'est autorisé pour un type de compte, la génération de clé ne sera pas possible. Cela permet, par exemple, de forcer l'importation de la clé à partir d'un fichier PKCS#12.

3.3.6 Section [NewUserCard]

Cette section est utilisée pour activer ou désactiver des fonctions spécifiques aux créations de compte carte :

Paramètre	Description
`AllowNewUserAuto`	Ce paramètre permet d'autoriser la création automatique de comptes cartes lors de leur première utilisation sur un poste (reportez-vous à la section Création automatique de compte carte dès la première utilisation d'une carte). • 0 : n'autorise pas la création automatique (par défaut) ; • 1 : autorise la création automatique.

3.3.7 Section [SBox.NewUserWizardExXXX]

Paramètres

Le tableau suivant décrit le contenu de chaque section en fonction du type de compte XXX (reportez-vous à la section Types de compte) :

Paramètre	KS1	KS2	GP1	GP2	Description
AllowNewUser	#	#	#	#	Création de compte : • 0 : non autorisée (par défaut) ; • 1 : autorisée.
AllowNewUserCipher	#		#		Création de compte avec une clé unique réservée au chiffrement : • 0 : non autorisée ; • 1 : autorisée (par défaut).
AllowNewUserSign	#		#		Création de compte avec une clé unique réservée à la signature : • 0 : non autorisée ; • 1 : autorisée (par défaut).
MasterPath	#	#	#	#	Ce paramètre contient le chemin absolu vers le modèle de compte à utiliser pour la création de compte. De plus amples informations sur les modèles de comptes peuvent être trouvées dans le manuel de Stormshield Data Authority Manager.
NoExtractableK	#	#	#	#	Lors de sa création, cet item indique si les clés privées sont marquées comme ne pouvant pas être exportées : • du keystore en mode KS1, KS2 ; • de la carte en mode GP1, GP2. Les valeurs sont : • 0 : non (par défaut en mode KS1, KS2) ; • 1 : oui (par défaut en mode GP1, GP2).

Paramètre	KS1	KS2	GP1	GP2	Description
`NoExtractableKeystoreKeys`				#	Cet item indique si les clés d'un compte carte stockées dans un keystore peuvent être exportées ou non : • 00 : les clés peuvent être exportées (par défaut) ; • 01 : la clé de chiffrement est exportable ; • 10 : la clé de signature est exportable ; • 11 : aucune clé n'est exportable. Ce paramètre est utile pour les comptes carte GP2 dont certaines clés privées sont stockées dans le keystore et non pas dans la carte elle-même.
`Pkcs12Import`	#	#	#	#	La clé (ou les clés) du nouveau compte peut être importée depuis un fichier *PKCS#12* : • 0 : non (par défaut) ; • 1 : oui.
`DirModelIsFolder`	#	#	#	#	Lors de la création d'un compte, Stormshield Data Security importe automatiquement dans l'annuaire les certificats (de correspondants ou d'autorités) indiqués par le paramètre `DirectoryModel`. • 0 : `<DirectoryModel>` est un fichier (par défaut). Les extensions supportées sont .cer, .crt, .p7b, .p7c (les formats correspondants sont indiqués dans le *Guide d'installation et de mise en œuvre*) ; • 1 : `<DirectoryModel>` est un dossier. Dans ce cas, le contenu de tous les fichiers de certificats (extension *.cer*, *.crt*, *.p7b*, .p7c) contenus dans ce dossier sera importé. Il ne faut pas mettre de \ à la fin de la valeur du paramètre.

Paramètre	KS1	KS2	GP1	GP2	Description
`DirectoryModel`	#	#	#	#	Voir `<DirModelIsFolder>`. Ce paramètre est facultatif. S'il n'est pas présent, l'annuaire de l'utilisateur n'est pas pré-rempli.

Paramètre	KS1	KS2	GP1	GP2	Description
MasterPolicies	#	#	#	#	Lors de la création d'un compte avec un modèle de compte, Stormshield Data Security copie les fichiers liste de Stormshield Data File et Stormshield Data Shredder. L'intégrité de ces fichiers est vérifiée par rapport au compte modèle. Ce paramètre permet de supprimer ce contrôle d'intégrité et donc d'utiliser des fichiers provenant d'autres comptes. Ce paramètre est constitué de 3 chiffres qui définissent, dans l'ordre, le comportement à adopter dans les 3 cas d'erreur suivants : • liste présente et pas de sceau associé dans le modèle ; • sceau présent dans le profil mais pas de liste ; • sceau et liste présents mais non concordants. Le comportement à adopter est alors défini pour chaque cas par une des valeurs suivantes : • 0 : arrêter le processus ; • 1 : continuer sans copier la liste ; • 2 : continuer en copiant la liste. Valeur par défaut : 000. **NOTE** Le 2ème chiffre ne peut pas prendre la valeur 2. Exemple : Pour la valeur 012, cela signifie que :

Paramètre	KS1	KS2	GP1	GP2	Description
					• action 0 pour le premier cas de figure : si la liste est présente et qu'il n'y a pas de sceau associé dans le modèle, on arrête le processus ; • action 1 pour le second cas de figure: Si le sceau est présent dans le profil mais qu'il n'y a pas de liste, on continue le processus sans copier la liste ; • action 2 pour le dernier cas de figure : si le sceau et la liste sont présents mais non concordants, on continue en copiant la liste.
ChangePINSO	#	#			Lors de la création de compte, Stormshield Data Security propose l'entrée d'un mot de passe Security Officer. Ceci peut être conditionné avec ce paramètre : • 0 : pas d'affichage de la page de saisie d'un mot de passe de secours – le mot de passe de secours est désactivé (par défaut pour les compte GP1 et GP2) ; • 1 : affichage de la page de saisie d'un mot de passe de secours (par défaut pour les comptes KS1 et KS2).
UsrPwdMinLen	#	#			Longueur minimale du mot de passe (en décimal). La valeur doit être entre 0 (par défaut) et 64. Si la valeur saisie est supérieure à 64, la valeur maximale (64) est utilisée.

Paramètre	KS1	KS2	GP1	GP2	Description
`UsrPwdCharSet`	#	#			Syntaxe : abc où abc sont 3 digits HEXA (0->F) obligatoirement en majuscules indiquant le nombre de caractères minimum dans un mot de passe : • a : nombre de caractères alphabétiques ; • b : nombre de caractères numériques ; • c : nombre de caractères autres. Valeur par défaut : 000.
`UserPinLeft`	#	#	#	#	Nombre de tentatives de connexion en échec avant blocage d'un compte. Le nombre doit être compris entre 1 et 999. Si la valeur est supérieure, la valeur maximale (999) est utilisée. Valeur par défaut : 3.
`SOPinLeft`	#	#	#	#	Nombre de tentatives de connexion en échec en mode Security Officer avant blocage d'un compte. Le nombre doit être un entier supérieur à 0 (pas de valeur maximale). Valeur par défaut : `<UserPinLeft>`.
`InternalKeys`			#	#	En mode carte/clé USB (GP1 ou GP2), les clés sont tirées : • 0 : par Stormshield Data Security, en mémoire (par défaut) ; • 1 : par la carte. **NOTE** Dans le cas d'une génération par la carte, celle-ci peut être faite par la carte elle-même ou en mémoire selon l'implémentation du constructeur ou la configuration de sa couche *PKCS#11*.

Paramètre	KS1	KS2	GP1	GP2	Description
`ExportKeys`			#	#	Si une clé n'a pas été tirée par la carte ou le token (si `<InternalKeys> = 0`), Stormshield Data Security peut afficher une fenêtre proposant de sauvegarder cette clé dans un fichier PKCS#12 (pour sauvegarde) ou de la copier dans le keystore de l'utilisateur (pour exportation ultérieure). • 0 : page non affichée (par défaut) ; • 1 : affichage normal de la page.
`KeepCardObjects`			#	#	Une case à cocher permet de **Ne pas détruire les objets non réutilisés** : • 00 : case non cochée et grisée ; • 01 : case non cochée et accessible ; • 10 : case cochée et grisée ; • 11 : case cochée et accessible (par défaut).
`EnciphermentKeyInCard`				#	Une case à cocher permet de **Mettre la clé de chiffrement dans la carte** : • 00 : case non cochée et grisée ; • 01 : case non cochée et accessible ; • 10 : case cochée et grisée ; • 11 : case cochée et accessible (par défaut).
`SigningKeyInCard`				#	Une case à cocher permet de **Mettre la clé de signature dans la carte** : • 00 : case non cochée et grisée ; • 01 : case non cochée et accessible ; • 10 : case cochée et grisée ; • 11 : case cochée et accessible (par défaut).

Personnalisation des pages de création de compte

La création de compte peut être personnalisée par exemple pour présélectionner automatiquement certains paramètres, voire même n'afficher que le minimum d'informations.

Cette opération s'effectue dans les sections [SBox.NewUserWizardExXXX] en utilisant les paramètres définis dans le tableau suivant.

Paramètre	KS1	KS2	GP1	GP2	Description
`ShowSaveKeyPage`			#	#	Affiche la page de sauvegarde des clés : • 0 = page non affichée ; • 1 = affichage normal de la page (par défaut). Ce paramètre n'est reconnu que si la valeur associée à `<ExportKeys>` est 1.
`SaveKeysInProfile`			#	#	Permet ou non la sauvegarde des clés dans le keystore associé à la carte : • 0 = case non cochée (par défaut) • 1 = case cochée Ce paramètre n'est reconnu que si la valeur associée à `<ExportKeys>` est 1. Si la valeur associée au paramètre `<ShowSaveKeyPage>` est 0, l'utilisateur ne peut pas agir sur la case à cocher et la sauvegarde des clés dépend alors de la valeur indiquée pour le paramètre `SaveKeysInProfile`. Si aucune valeur n'est précisée, la valeur par défaut est appliquée.

Personnalisation par type de clé

Une personnalisation plus avancée peut être effectuée en ajoutant les sections suivantes :

- [Sbox.NewUserWizardExKS1.Personal] : compte mot de passe mono-clé ;
- [Sbox.NewUserWizardExKS2.Encryption] : compte mot de passe pour la clé de chiffrement ;
- [Sbox.NewUserWizardExKS2.Signature] : compte mot de passe pour la clé de signature ;
- [Sbox.NewUserWizardExGP1.Personal] : compte carte mono-clé ;
- [Sbox.NewUserWizardExGP2.Encryption] : compte carte pour la clé de chiffrement ;
- [Sbox.NewUserWizardExGP2.Signature] : compte carte pour la clé de signature.

Par ailleurs, les paramètres associés à chacune de ces sections sont :

Paramètre	KS1	KS2	GP1	GP2	Description
DisableCreateSelf	#	#	#	#	Permet d'interdire le tirage d'une clé auto-certifiée, tant à la création de compte qu'au renouvellement de clé : • 0 : autorise le tirage d'une clé auto-certifiée (par défaut) ; • 1 : interdit le tirage d'une clé auto-certifiée.
KeyPage	#	#	#	#	Indique si la page de sélection de l'origine de la clé doit être affichée ou non et le traitement par défaut qui doit être effectué : • 0 : affichage normal de la page (par défaut) ; • 1 : page non affichée et réutilisation de la clé (uniquement pour GP1 et GP2) ; • 2 : page non affichée et création de la clé (ne pas oublier le paramètre <CreateForceKey>) ; • 3 : page non affichée et importation PKCS#12 affichée. Si l'importation PKCS#12 est interdite (<Pkcs12Import> = 0) ou que les clés sont à générer en interne dans la carte (<InternalKeys> = 1), l'utilisation de cette valeur est interdite et entraîne l'affichage de la page comme si <KeyPage> = 0.
CreateForceKey	#	#	#	#	Spécification de la taille de clé. Ce paramètre n'est utilisé que lorsque le paramètre <KeyPage> = 2. Les valeurs autorisées sont : 512, 768, 1024, 2048 et 4096. Il n'y a pas de valeur par défaut. Si <KeyPage> = 2 et que le paramètre n'est pas présent ou invalide, alors la page de sélection de l'origine de la clé apparaît (comme si <KeyPage>=0).

Paramètre	KS1	KS2	GP1	GP2	Description
P12ImportPath	#	#	#	#	Chemin d'accès complet au fichier d'import P12. Ce paramètre n'est lu que lorsque le paramètre <KeyPage> = 3. Si le paramètre pointe sur un fichier PKCS#12 alors la valeur précisée est présentée de manière non modifiable. Dans le cas contraire, le champ est pré-rempli avec la valeur du paramètre. Ce champ n'est remplacé que si le paramètre <Pkcs12Import> = 1.
ShowKeyCertPage	#	#	#	#	Permettre l'affichage de la page des certificats lors de l'utilisation d'un fichier PKCS#12 ou de la réutilisation des clés d'une carte : • 0 : pas d'affichage ; • 1 : affichage de la page (par défaut).
SelfCertMail	#	#	#	#	Pré-renseigner le champ adresse e-mail pour la génération d'un certificat auto-signé. Il est possible de saisir dans ce champ : • une adresse e-mail ; • un suffixe d'adresse e-mail (ex : @masociete.fr). La valeur peut ensuite être modifiée et complétée par l'utilisateur. Ce paramètre est optionnel. S'il n'est pas positionné, le champ concerné est initialisé à vide.
SelfCertOrganization	#	#	#	#	Pré-renseigner le champ **Société** pour la génération d'un certificat auto-signé. Ce paramètre est optionnel. S'il n'est pas positionné, le champ concerné est initialisé à vide.
SelfCertOrganizationRW	#	#	#	#	Modification possible du champ **Société** : • 0 : champ pré-renseigné (ou vide) et non modifiable ; • 1 : champ pré-renseigné et modifiable (par défaut).
SelfCertCity	#	#	#	#	Pré-renseigner le champ **Ville** pour la génération d'un certificat auto-signé. Ce paramètre est optionnel. S'il n'est pas positionné, le champ concerné est initialisé à vide.

Paramètre	KS1	KS2	GP1	GP2	Description
SelfCertCityRW	#	#	#	#	Modification possible du champ **Ville** : • 0 : champ pré-renseigné (ou vide) et non modifiable ; • 1 : champ pré-renseigné et modifiable (par défaut).
SelfCertCountry	#	#	#	#	Pré-renseigner le champ **Pays** pour la génération d'un certificat auto-signé. Ce paramètre est optionnel. S'il n'est pas positionné, le champ concerné est initialisé à vide.
SelfCertCountryRW	#	#	#	#	Modification possible du champ **Pays** : • 0 : champ pré-renseigné (ou vide) et non modifiable ; • 1 : champ pré-renseigné et modifiable (par défaut).

3.3.8 Section [KeyRenewal]

Les sections [KeyRenewal] et [SBox.KeyRenewalWizardYYY] concernent le renouvellement de clés pour des comptes Stormshield Data Security existants.

La section [KeyRenewal] est commune à tous les types de compte.

La section [SBox.KeyRenewalWizardYYY] comporte les paramètres spécifiques au renouvellement de clé d'un compte de type YYY, qui peut être :

- KS : renouvellement d'une clé d'un compte mot de passe KS1 ou KS2 ;
- GP : renouvellement d'une clé d'un compte carte GP1 ou GP2.

Paramètre	Description
CertLife	Durée de validité, en années, des certificats auto-générés par Stormshield Data Security. La valeur doit être comprise entre 1 et 20. Valeur par défaut : 20 ans.

Paramètre	Description
Types de clé	Liste des clés (type et longueur) à proposer pour la création de compte. Les types de clés supportés sont définis à l'aide d'items dont la valeur est constituée d'une suite ordonnée de 3 chiffres, chaque chiffre correspondant à un type de compte. L'ordre des types de compte est : KS, GP, CPS. Les types de clés supportés et les règles de gestion sur les erreurs de configuration sont les mêmes que ceux de la création de compte, définis dans la section Types de clé de l'utilisateur. Ainsi, si RSA 2048 bits est la valeur par défaut, et si RSA 1024 est interdit, il faut paramétrer : • KEY_RSA_512BITS = 111 • KEY_RSA_768BITS = 111 • KEY_RSA_1024BITS = 000 • KEY_RSA_2048BITS = 222 • KEY_RSA_4096BITS = 111

3.3.9 Section [SBox.KeyRenewalWizardYYY]

Le tableau suivant présente le contenu de chaque section en fonction du type de compte YYY défini dans la section Section [KeyRenewal].

Paramètre	KS	GP	Description
NoExtractableK	#	#	Cet item indique si les clés d'un compte carte stockées dans un keystore peuvent être exportées ou non : • 00 : les clés peuvent être exportées (par défaut) ; • 01 : la clé de chiffrement est exportable ; • 10 : la clé de signature est exportable ; • 11 : aucune clé n'est exportable. Ce paramètre est utile pour les comptes carte GP2 dont certaines clés privées sont stockées dans le keystore et non pas dans la carte elle-même.
Pkcs12Import	#	#	La clé (ou les clés) du nouveau compte peut être importée depuis un fichier PKCS#12 : • 0 : non (par défaut) ; • 1 : oui.
InternalKeys		#	En mode carte/token USB (GP1 ou GP2), les clés sont tirées : • 0 : par Stormshield Data Security, en mémoire ; • 1 : par la carte (par défaut). **NOTE** Dans le cas d'une génération par la carte, celle-ci peut être faite par la carte elle-même ou en mémoire selon l'implémentation du constructeur ou la configuration de sa couche *PKCS#11*.

Paramètre	KS	GP	Description
ExportKeys		#	Si une clé n'a pas été tirée par la carte ou le token (si <InternalKeys> = 0), Stormshield Data Security peut afficher une fenêtre proposant de sauvegarder cette clé dans un fichier PKCS#12 (pour sauvegarde) ou de la copier dans le keystore de l'utilisateur (pour exportation ultérieure). • 0 : page non affichée (par défaut) ; • 1 : affichage normal de la page.
KeepCardObjects		#	Une case à cocher permet de **Ne pas détruire les objets non réutilisés** : • 00 : case non cochée et grisée (par défaut) ; • 01 : case non cochée et accessible ; • 10 : case cochée et grisée ; • 11 : case cochée et accessible.
AutomaticRenew FromCard		#	Avec un compte carte, quand la nouvelle clé de chiffrement ou de signature d'un utilisateur est déjà dans la carte, cette option permet de renouveler automatiquement la clé quand la précédente expire : • 0 : pas de renouvellement automatique (valeur par défaut) ; • 1 : renouvellement automatique avec message de confirmation ; • 2 : renouvellement automatique sans message de confirmation. **IMPORTANT** La valeur 1 peut permettre à l'utilisateur de refuser le renouvellement. Cependant, après un refus, la mise à jour n'est plus proposée. Il est donc déconseillé d'utiliser cette valeur.

3.3.10 Section [CoworkerSelector]

Dans les modules SD File, SD Virtual Disk et SD Team, la recherche dans la fenêtre de sélection des correspondants fonctionne par défaut sur le nom commun (*Common name*) et l'adresse e-mail du certificat.

Cette section est utilisée pour activer ou désactiver la recherche de correspondant sur le champ Adresse e-mail des certificats :

Paramètre	Description
EnableResearchByEmail	Ce paramètre permet d'activer la recherche de correspondant sur l'adresse e-mail du certificat. • 0 : n'autorise pas la recherche sur l'adresse e-mail (par défaut) ; • 1 : autorise la recherche sur l'adresse e-mail.
EmailSeparatorCharacters	Ce paramètre définit les caractères de l'adresse e-mail qui seront considérés comme un espace afin que la recherche sur ce champ fonctionne. Par défaut les caractères "-", "." et "_" seront remplacés par un espace. Par exemple l'adresse jean-philippe.dupont@domain.com sera vue comme jean philippe dupont.

3.3.11 Section [Mail]

Paramètres communs

Le tableau suivant décrit les paramètres communs aux différents clients de messagerie de la section [Mail].

Ces paramètres concernent Stormshield Data Mail Édition Notes. Ils ne sont pas pris en charge par Stormshield Data Mail Édition Outlook.

Paramètre	Description
DisplayComlogWindow	Permet d'afficher ou non la fenêtre de connexion à Stormshield Data Security lors de l'émission d'un message (Mode "Utilisateur déconnecté") : • 0 : affichage de la fenêtre de connexion uniquement si l'utilisateur coche les boutons **Signer** ou **Chiffrer** lors de la composition du message ; • 1 : affichage systématique de la fenêtre de connexion à Stormshield Data Security (par défaut). Ce paramètre ne concerne pas l'état verrouillé d'un utilisateur.
DisplayComlogWindow UserLocked	Permet d'afficher ou non la fenêtre de connexion à Stormshield Data Security lors de l'émission d'un message (Mode "Utilisateur verrouillé") : • 0 : affichage de la fenêtre de connexion uniquement si l'utilisateur coche les boutons **Signer** ou **Chiffrer** lors de la composition du message ; • 1 : affichage systématique de la fenêtre de connexion à Stormshield Data Security (par défaut). Ce paramètre ne concerne pas l'état déconnecté d'un utilisateur.

Paramètre	Description
AllowSendClearIfEncryptAsked	Permet de limiter les options proposées à l'utilisateur lorsqu'un correspondant ne possède pas de certificat de chiffrement valide : • 0 : interdiction d'envoyer en clair le message ; • 1 : l'utilisateur peut envoyer le message en clair (par défaut).

Édition Lotus Notes

Quand l'utilisateur envoie un message, Stormshield Data Mail Édition Notes utilise les cases à cocher **Signer** et **Chiffrer** de l'interface Lotus Notes standard pour déterminer les options de sécurité à appliquer au message. L'utilisateur ne peut dès lors plus mettre en œuvre la sécurité native de Lotus Notes.

Pour pouvoir choisir entre la sécurité native de Lotus Notes et la sécurité de Stormshield Data Security, il faut désactiver la lecture des cases à cocher natives de Lotus Notes par Stormshield Data Security à l'aide du paramètre suivant :

Paramètre	Description
DoNotCheckNativeCheckBox	Permet de ne pas prendre en compte les cases à cocher natives de Lotus Notes pour la sécurisation du message • 0 : utilisation des cases à cocher de Lotus Notes (par défaut) ; • 1 : non utilisation des cases à cocher natives de sécurité de Lotus Notes.

Lorsque ce paramètre est activé, Stormshield Data Mail Édition Notes prend en compte des cases à cocher supplémentaires au niveau du formulaire de création de message :

- SecurityBOXMailSignOption : indique que Stormshield Data Mail doit signer le message électronique ;
- SecurityBOXMailEncryptOption : indique que Stormshield Data Mail doit chiffrer le message électronique pour les différents destinataires.

Ces nouvelles cases à cocher sont optionnelles. Si elles ne sont pas ajoutées au formulaire de création du message (cela nécessite de modifier la base de données Lotus Notes), elles sont considérées comme n'étant pas cochées.

Lorsque ces cases à cocher ont été ajoutées, il est possible de désactiver l'affichage de la fenêtre de saisie des options d'envoi par Stormshield Data Mail en cochant l'option **Ne pas afficher la fenêtre de choix des options de sécurité** dans la configuration de Stormshield Data Mail Édition Notes.

3.3.12 Section [CRL]

La section [CRL] comporte les paramètres du contrôleur de révocation.

Paramètre	Description
`LDAPTimeOut`	Délai maximal, en secondes, d'un téléchargement de CRL en LDAP. Valeur par défaut : 30. **NOTE** Cette valeur est également utilisée comme timeout pour le téléchargement des fichiers de mise à jour de compte (fichier *USX*) lors de la connexion d'un utilisateur mais dans ce cas, la valeur par défaut est 25 secondes.

`HTTPTimeOut`	Délai maximal, en secondes, d'un téléchargement de CRL en HTTP.
	Valeur par défaut : 300.
	La syntaxe est la suivante :
	`[CRL]`
	`HTTPTimeOut=valeur en secondes`

`DontDisplayWrnMsgDBDeleted`	Le message d'avertissement concernant la suppression de la base de CRL peut être masqué. • 0 : non (par défaut), le message s'affiche ; • 1 : oui, le message est masqué.
`DontDisplayWrnMsgDBCorrupted`	Le message d'avertissement concernant la possible corruption de la base de CRL peut être masqué. • 0 : non (par défaut), le message s'affiche ; • 1 : oui, le message est masqué.

3.3.13 Section [External PKCS11 Policy]

La section [external PKCS11 policy] concerne la configuration de type de carte ou clé USB (Stormshield Data Security Card Extension) accessible depuis le menu **Windows/Démarrer/Stormshield Data Security**.

Le tableau suivant décrit les paramètres de la section [External PKCS11 Policy] :

Paramètre	Description
`CPLShowExtension`	Bloque le lancement du configurateur de carte. • 0 : pas d'affichage ; • 1 : affichage (par défaut).
`CPLCanChangePKCS11`	L'utilisateur peut modifier le type de carte ou token USB défini dans le configurateur. • 0 : non ; • 1 : oui (par défaut).

Paramètre	Description
`CPLForcePKCS11Label`	Valeur initiale (forcée) du nom du module cryptographique. Le fait de positionner ce champ et de le rendre non modifiable (option `CPLCanChangePKCS11 = 0`) permet de figer l'interface *PKCS#11* utilisée par Stormshield Data Security sur le poste. Paramétrage par défaut : CPLForcePKCS11Label= Si ce paramètre n'est pas présent (commenté en début de ligne avec ";"), le champ n'est pas initialisé. Il ne faut pas bloquer le champ (paramètre `CPLCanChangePKCS11=0`) sauf pour empêcher l'utilisateur d'accéder à une carte ou un token. Exemple d'appel d'option : `CPLForcePKCS11Label=ALADDIN eToken PRO`.
`CPLPKCS11InfosEnabled`	Le bouton **Informations** est accessible. • 0 : non ; • 1 : oui (par défaut).
`CPLPKCS11Infos SaveAsEnabled`	Le bouton **Enregistrer sous** est accessible. • 0 : non ; • 1 : oui (par défaut).

Afin de permettre l'analyse de problème d'accès à la carte ou au token de l'utilisateur, il est souhaitable de laisser l'accès en lecture (consultation des informations) pour les paramètres.

3.3.14 Section [File]

La section [File] comporte les paramètres de Stormshield Data File.

Le tableau suivant décrit le paramètre de la section [File] :

Paramètre	Description
`AllowTranscipheringWithDecipheredKeys`	Autorise à transchiffrer avec une clé de déchiffrement • 0 : valeur par défaut : transchiffrement avec une clé de déchiffrement non autorisé ; • 1 : transchiffrement avec une clé de déchiffrement autorisé.

Ouverture d'un fichier chiffré FILE dans un répertoire personnalisé

Il est possible de définir le répertoire cible pour le déchiffrement d'un fichier FILE ouvert depuis une autre application (par exemple Lotus Notes).

Paramètre	Description
`ExeActivate`	Ce paramètre actionne la fonctionnalité du choix de répertoire cible dans lequel sera réalisé le déchiffrement. Les valeurs sont : • 0 : interrupteur désactivé (valeur par défaut) ; • 1 : interrupteur activé. Si l'interrupteur est désactivé (valeur 0), les trois paramètres suivants ne seront pas pris en compte et le comportement adopté sera celui par défaut.
`ExeToCheck`	Ce paramètre permet de configurer une liste d'exécutables pour lesquels Stormshield Data Security devra contrôler les répertoires d'ouverture où seront déchiffrés les fichiers FILE. Si ce paramètre n'est pas présent, la fonctionnalité s'activera alors pour tous les exécutables appelants. La syntaxe est la suivante : `ExeToCheck = nom_exe_1 [, nom_exe_n]`

`ExeTargetDirectory`	Ce paramètre permet de spécifier le chemin du répertoire dans lequel s'effectuera le déchiffrement puis l'ouverture du fichier FILE. La syntaxe est la suivante :
	`ExeTargetDirectory = path`
	où path est le chemin du répertoire. Ce chemin peut être composé de tags (tags SecurityBOX ou variables d'environnement Windows) en mettant ceux-ci entre < >. Ces tags peuvent être les suivants :
	• COMMON_APPDATA : **C:\ProgramData**
	• COMMON_DOCUMENTS : **C:\Users\Public\Documents**
	• USERNAME : nom d'utilisateur Windows connecté.
	• LOCAL_APPDATA : **C:\Users\<username>\AppData\Local**
	• DESKTOP : **C:\Users\<username>\Desktop**
	• PROFILE : **C:\Users\<username>**
	• %ENV% où ENV est une variable d'environnement système.
	Exemples : `[FILE] ExeTargetDirectory=c:\User`
	`ExeTargetDirectory=<%TMP%>`
	NOTE
	Le format à utiliser doit respecter les conventions Windows : **C:\xxxx**.
	Ce chemin ne doit pas être encadré par des guillemets.

Paramètre	Description
`AllowOverwriteFile`	Ce paramètre permet de spécifier si l'écrasement de fichier est autorisé. Ce cas peut par exemple se présenter lors d'une ouverture multiple d'un même document. Les valeurs sont : • 0 : écrasement interdit. Si un fichier avec le même nom que le fichier chiffré et/ou déchiffré existe déjà dans le répertoire cible, l'opération de déchiffrement échouera ; • 1 : écrasement autorisé (valeur par défaut). Si un fichier avec le même nom que le fichier chiffré et/ou déchiffré existe déjà dans le répertoire cible, il sera écrasé de manière silencieuse. Exemple de paramétrage complet : `[FILE] ExeActivate=1 ExeToCheck=nlnotes.exe ExeTargetDirectory=<%TMP%>\MonDossierTemporaire AllowOverwriteFile=1`. Ce paramétrage permet de définir le répertoire cible des fichiers FILE ouverts en pièces jointes dans l'application Lotus Notes. Le comportement des autres applications reste inchangé.

3.3.15 Section [Directory]

Le tableau suivant décrit les paramètres de la section [Directory] :

Paramètre	Description
`AddCertAttrInLdapFilter`	Ce paramètre permet d'ajouter automatiquement le critère (usercertificate;binary=*) au filtre d'une recherche LDAP : • 1 : ajoute le critère (par défaut) ; • 0 : n'ajoute rien. L'ajout de ce critère permet de ne remonter que les entrées contenant un certificat, ce qui correspond aux utilisations normales de l'annuaire Stormshield Data Security.
`AddAsteriskSuffixInLdapFilter`	Ce paramètre permet d'ajouter automatiquement '*' à la fin des valeurs recherchées (mail et cn). Ainsi, si l'utilisateur tape "dup", la recherche porte sur "dup*" et on obtient "dupond" et "dupont" : • 1 : ajoute le caractère '*' (par défaut) ; • 0 : n'ajoute rien.
`AddAsteriskPrefixInLdapFilter`	Ce paramètre permet d'ajouter automatiquement '*' au début des valeurs recherchées (cn). Ainsi, si l'utilisateur tape "dupont", la recherche porte sur "*dupont" et on obtient "pierre dupont" et "marie dupont" : • 1 : ajoute le caractère '*' ; • 0 : n'ajoute rien (par défaut).

Paramètre	Description
`AddProxyAddressesInLdapFilter`	Ce paramètre permet d'ajouter automatiquement le critère '(proxyAddresses=smtp:xxx@yyy.zzz)' au filtre de recherche LDAP pour les recherches par adresse e-mail. Ainsi, la recherche d'un utilisateur s'effectue à partir de son champ 'mail' et de son champ 'proxyAddresses' , au lieu d'uniquement le champ 'mail': • 1 : ajoute le filtre '(proxyAddresses=smtp:xxx@yyy.zzz)' (par défaut) ; • 0 : n'ajoute rien.
`LdapConfig`	Ce paramètre permet de choisir le moteur de recherche LDAP utilisé par la fenêtre de sélection des correspondants (composants Disk, File et Team) et par le composant Stormshield Data Mail : • Legacy (valeur par défaut) : Utilise le moteur de recherche de l'annuaire de confiance Stormshield Data Security pour effectuer les recherches sur l'annuaire LDAP. • User : Utilise le moteur de recherche dédié LDAP en se basant sur la configuration définie dans l'annuaire de confiance de l'utilisateur SDS connecté. Pour plus d'informations sur l'utilisation des moteurs de recherche LDAP, reportez-vous à la section Mise en oeuvre d'annuaire LDAP dans le *Guide d'installation Stormshield Data Security*.

3.3.16 Section [Disk]

La section [Disk] concerne le paramétrage de Stormshield Data Virtual Disk.

Paramètres généraux

Le tableau suivant décrit les paramètres généraux de la section [Disk] :

Paramètre	Description
`MaxVolumeSize`	Permet de maximiser la taille d'un volume exprimée en Mo (*.vbox*) lors de sa création par l'assistant. Si ce paramètre n'est pas renseigné, on peut prendre la totalité de la taille disponible sur un lecteur.
`DefaultVolumeSize`	L'assistant de création d'un volume sécurisé propose une taille par défaut (en Mo). Si ce paramètre n'est pas renseigné, on propose une taille valant 10% de la taille disponible sur le lecteur sélectionné.

Paramètre	Description
`MountAsRemovable`	Permet de spécifier si le volume sécurisé sera considéré comme un périphérique amovible. • 0 : non • 1 : oui (par défaut) Ce paramètre comporte les limitations suivantes : • MountAsRemovable=0 peut provoquer une perte d'image dans des documents PowerPoint à partir de Microsoft Office 2013 en cas de déconnexion/verrouillage. • Pour une utilisation du volume à distance (Remote Desktop Protocol), la valeur 0 est obligatoire. • MountAsRemovable=1 ne permet pas d'avoir accès à une corbeille dédiée au volume Virtual Disk.
`QuickCreate`	Permet de créer un volume sécurisé sur un disque local de manière plus rapide que sur un disque réseau. • 0 : non (par défaut) • 1 : oui

Données de formatage d'un volume

Après création, les volumes sont automatiquement formatés pour être directement utilisables.

Le tableau suivant décrit les paramètres de formatage d'un volume :

Paramètre	Description
`FileSytem`	Système de fichiers utilisés pour le formatage : • NTFS (par défaut) ; • FAT ; • FAT32. Si le système de fichiers demandé est FAT32 et que la taille est inférieure à 32 Mo, le formatage est effectué en FAT.
`Label`	Label du volume créé. Ce paramètre est optionnel. La valeur par défaut est fonction de la langue : • Version française : "Disque sécurisé" ; • Version anglaise : "Secure disk".
`AllocUnit`	Taille d'unité d'allocation : • 0 : Taille d'allocation par défaut ; • 512 ; • 1024 ; • 4096. La prise en compte de ce paramètre dépend du système de fichiers utilisé pour le formatage (seul NTFS l'utilise).

Paramètre	Description
`QuickFormat`	Adopter un formatage rapide : • 0 : non ; • 1 : oui (par défaut).
`Compression`	Activer la compression. La prise en compte de ce paramètre dépend du système de fichiers utilisé pour le formatage (seul NTFS l'utilise) : • 0 : non (par défaut) ; • 1 : oui.

Données de création automatique d'un volume

La création d'un volume peut se faire de deux façons :

- en mode interactif ;
- automatiquement lors de la première connexion de l'utilisateur.

Le tableau suivant décrit les paramètres de création automatique d'un volume :

Paramètre	Description
`VboxFullPathName`	Nom complet du fichier container associé au volume. Ce nom peut comporter les mots-clés spécifiés ci-dessous. Ce paramètre est obligatoire (aucune valeur par défaut).
`SilentSize`	Taille du volume en Mo pour le volume à créer. Par défaut : 10% de la taille disponible sur l'unité cible du container spécifié par le paramètre `VboxFullPathName`.
`AutoMount`	Indique si le volume créé est en mode automatique ou manuel : • 0 : mode manuel ; • 1 : mode automatique (par défaut).
`MountLetter`	Lettre de montage (Ne pas ajouter ':' après la lettre saisie). Si cette lettre n'est pas renseignée, l'assistant choisit dans l'ordre alphabétique inverse (c'est-à-dire à partir de z) la première lettre disponible. Ce paramètre est optionnel.

Le nom complet du fichier associé à un volume peut comporter :

- soit une variable d'environnement, indiquée sous la forme <%Path%> ;
- soit un mot-clé, indiqué sous la forme <KeyWord>.

Les mots-clés supportés, décrits dans le tableau ci-dessous, sont l'identifiant Stormshield Data Security de l'utilisateur (UserId) et certains CSIDL de Windows :

Mot-clé	Description
UserId	Identifiant Stormshield Data Security de l'utilisateur.
RootPath1	Dossier des comptes utilisateurs, spécifié dans le fichier *SBox.ini*.
RootPath2	Second dossier des comptes utilisateurs, spécifié dans le fichier *SBox.ini*.

Mot-clé	Description
COMMON_APPDATA	Répertoire contenant les données d'application de tous les utilisateurs. Le chemin type est **C:\ProgramData**.
COMMON_DOCUMENTS	Répertoire contenant les fichiers communs à tous les utilisateurs. Le chemin type est **C:\Users\Public\Documents**.
DESKTOP	Répertoire utilisé pour le stockage de fichiers sur le bureau. Le chemin type est **C:\Users\<username>\Desktop**.
LOCAL_APPDATA	Répertoire utilisé pour les données des applications locales. Le chemin type est **C:\Users\<username>\AppData\Local**.
MYDOCUMENTS	Répertoire utilisé pour le stockage des documents de l'utilisateur. Le chemin type est **C:\Users\<username>\Documents**.
PROFILE	Le dossier du profil de l'utilisateur. Le chemin type est **C:\Users\<username>**.
PROFILES	Le dossier des profils des utilisateurs. Le chemin type est **C:\Users**.
USERNAME	Nom d'utilisateur Windows.

Données de création d'un volume à la première connexion

Il est possible de demander la création d'un volume à la première connexion d'un utilisateur. Les données sont celles qui sont spécifiques à la première connexion. Les autres données nécessaires à l'opération sont celles issues de la création en mode automatique décrites précédemment.

Paramètre	Description
`CreateDiskOnFirstConnection`	Crée automatiquement sur le poste un disque lors de la première connexion de l'utilisateur à son compte : • 0 : non (par défaut) ; • 1 : oui.
`Verbose`	Affiche la fenêtre de confirmation et de compte-rendu : • 0 : aucune fenêtre (par défaut) ; • 1 : uniquement la fenêtre de compte-rendu ; • 2 : les deux fenêtres. Ce paramètre n'est utilisé que pour la création à la première connexion (`CreateDiskOnFirstConnection = 1`)
`CloseReportWindow`	Ferme automatiquement la fenêtre de compte-rendu après la création du disque : • 0 : non (par défaut) ; • 1 : oui. Ce paramètre n'est utilisé que pour la création à la première connexion (`CreateDiskOnFirstConnection = 1`).

Modification des utilisateurs d'un volume via le fichier *.VBOXSAVE*

Les paramètres ci-dessous activent la fonction qui permet de modifier la liste des utilisateurs d'un volume à partir du fichier de secours *.vboxsave*. Cette fonction est utilisée pour transmettre la propriété d'un volume à un autre utilisateur (reportez-vous au manuel Stormshield Data Virtual Disk) et pour effectuer des opérations de recouvrement à la section Stormshield Data Virtual Disk :

Paramètre	Description
`ModifyRescueFile`	Autorise la modification des utilisateurs dans le fichier de secours : • 0 : non (par défaut) ; • 1 : oui Selon la valeur du paramètre `ExpertMode`, il faut ou non que le fichier de secours soit dans un dossier distinct du volume concerné.
`ExpertMode`	Autorise la modification des utilisateurs dans le fichier de secours même s'il est dans le même dossier que le fichier *.vbox* associé : • 0 : non (par défaut) ; • 1 : oui.

3.3.17 Section [Team]

La section [Team] concerne le paramétrage de Stormshield Data Team.

Interdiction d'accéder à un fichier chiffré si le certificat est révoqué

Le mode par défaut et le mode sécurisé d'accès aux fichiers chiffrés si le certificat de la clé de chiffrement de l'utilisateur est révoqué se configurent dans Stormshield Data Authority Manager à l'exception de ce paramètre :

Paramètre	Description
`CheckCertificateTimeout`	• 120 (valeur par défaut) : la valeur indique le nombre de minutes entre deux vérifications du certificat de la clé de chiffrement de l'utilisateur. Ce paramètre peut prendre toute valeur positive.

Le paramètre est pris en compte à la connexion de l'utilisateur.

Veuillez consulter le *Guide d'utilisation de Stormshield Data Authority Manager* pour plus d'informations.

Configuration de copie ou déplacement d'un dossier /fichier

Paramètre	Description
`SecureDragAndDrop`	Le paramètre `SecureDragAndDrop` permet de limiter le déplacement ou la copie de dossiers et de fichiers couverts par une règle Stormshield Data Team vers un dossier non sécurisé et prévient une action de déplacement ou de copie accidentelle de la part de l'utilisateur. Il permet de spécifier les fonctionnements suivants : • déplacement bloqué ; • déplacement chiffré ; • par défaut : comportement indiqué dans le tableau ci-dessous. Le paramètre peut prendre 3 valeurs : • 0 : (par défaut) le comportement est celui indiqué dans le tableau ci-dessous ; • 1 : l'action est interdite ; • 2 : le déplacement ou la copie ne déchiffre pas les fichiers. **Comportement par défaut** Lors d'une opération de glisser-déposer d'un dossier sécurisé vers un dossier non sécurisé : • Un dossier héritant de la règle de sécurité du dossier parent ou un fichier ne seront plus sécurisés ; • Un dossier ayant sa propre règle de sécurité la conservera, sauf si il est déplacé sur un autre volume.

	Vers un dossier non sécurisé, dans le même volume	Vers un dossier non sécurisé, dans un autre volume
Glisser-déposer d'un fichier depuis un dossier sécurisé	Clair	Clair
Glisser-déposer d'un dossier dont la règle de sécurité est héritée	Clair	Clair
Glisser-déposer d'un dossier qui a sa propre règle de sécurité	Sécurisé	Clair

Le paramètre `SecureDragAndDrop=2` correspond à l'application sur le **Glisser-Déposer** de la fonctionnalité **Sauvegarder** présente dans le menu contextuel de Stormshield Data Security.

IMPORTANT
Lorsque l'utilisateur est déconnecté, le paramètre n'est pas effectif et le comportement par défaut est appliqué.

Affichage des fichiers traités avec succès

Paramètre	Description
`ShowSuccessfulOperations`	Dans l'écran de suivi d'une opération de chiffrement, ce paramètre permet d'afficher ou de cacher les fichiers traités avec succès. Dans tous les cas, les fichiers en erreur sont affichés. • 0 : seuls les fichiers en erreurs sont affichés (valeur par défaut). • 1 : tous les fichiers traités, avec succès et en erreur, sont affichés.

3.3.18 Section [Sign]

La section [Sign] concerne le paramétrage de Stormshield Data Sign.

Paramètre	Description
`MailToNotifyCoworkers`	Lorsque le processus de signature d'un document est terminé, l'utilisateur peut demander la préparation d'un courrier électronique à destination de collaborateurs afin que ceux-ci soient avertis de cette signature. Si le document avait été précédemment signé, la liste des destinataires est pré-remplie avec les adresses e-mail des co-signataires. Cette option agit sur la case à cocher dans l'assistant de signature : • 0 : non (par défaut), la case n'est pas cochée ; • 1 : oui, la case est cochée.
`MailToAskForSignature`	Lorsque le processus de signature d'un document est terminé, l'utilisateur peut demander la préparation d'un courrier électronique à destination des collaborateurs pour que ceux-ci apposent aussi leur signature. Cette option agit sur la case à cocher dans l'assistant de signature : • 0 : non (par défaut), la case n'est pas cochée ; • 1 : oui, la case est cochée.

Paramètre	Description
`TmpFolder`	Ce paramètre permet de spécifier le chemin du répertoire dans lequel s'effectue la création de fichiers temporaires lors des opérations de co-signature et contre-signature. La syntaxe est la suivante : `TmpFolder = path` où `path` est le chemin du répertoire. Ce chemin peut être composé de tags (tags SecurityBOX ou variables d'environnement Windows) en mettant ceux-ci entre <>. Ces tags peuvent être les suivants : • COMMON_APPDATA : C:\ProgramData • COMMON_DOCUMENTS : C:\Users\Public\Documents • USERNAME : nom d'utilisateur Windows connecté • LOCAL_APPDATA : C:\Users\<username>\AppData\Local • DESKTOP : C:\Users\<username>\Desktop • PROFILE : C:\Users\<username> • %ENV% où ENV est une variable d'environnement système Exemples : [SIGN] TmpFolder=c:\User ; TmpFolder=<%TMP%> **NOTE** Le format à utiliser doit respecter les conventions Windows : C:\xxxx\. Ce chemin ne doit pas être encadré par des guillemets.

3.3.19 Section [PGP]

La section [PGP] concerne le paramétrage PGP de Stormshield Data Mail.

Paramètre	Description
`WKDServers`	Pour envoyer et recevoir des e-mails chiffrés au format PGP dans Outlook, vous devez spécifier quels serveurs WKD (Web Key Directories) consulter. Ces annuaires de clés publiques permettent à Stormshield Data Mail de récupérer les clés publiques PGP des destinataires d'e-mails chiffrés. La valeur de ce paramètre est une ou plusieurs URL de serveurs WKD, correspondant à l'un des deux formats suivants : • **https://openpgpkey.**domaine.org**/.well-known/openpgpkey/<d>/hu/<k>**? • **https://**sous-domaines-optionnels.domain.org**/.well-known/openpgpkey/hu/<k>**? Les parties en gras de l'URL doivent être conservées telles quelles. Les autres parties doivent être remplacées par les domaines ou sous-domaines du serveur. Après le point d'interrogation ?, vous pouvez ajouter des paramètres GET aux URL sous la forme *paramètre=valeur* et séparés par le caractère &. Une fois le paramètre `WKDServers` configuré, redémarrez Outlook afin que les options PGP apparaissent dans la fenêtre de configuration des options de sécurité de Stormshield Data Mail. Pour plus d'informations, reportez-vous au Guide *Stormshield Data Mail Édition Outlook*. **NOTE** SDS communique avec les WKD en HTTPS. Tous les ordinateurs hébergeant Stormshield Data Mail doivent donc disposer du certificat de l'autorité ayant émis le certificat SSL du serveur WKD.
`Disable`	Permet de désactiver le support du format PGP par Stormshield Data Mail : • 1 : le support est désactivé. Par défaut, le support de PGP est activé si ce paramètre est absent ou si sa valeur ne correspond pas exactement à 1 sans espace (Disable=1). Lorsque le support de PGP est désactivé, les messages chiffrés avec PGP s'ouvrent dans Outlook au format brut.

3.4 Environnement d'évaluation Critères Communs

Les tableaux suivants recensent les valeurs des différents paramètres en base de registre et dans le fichier *sbox.ini* correspondant à l'environnement sécurisé ayant fait l'objet de l'évaluation Critères Communs EAL3+.

3.4.1 Base de registre

Paramètre	Description
`ForceGenerationKey`	Permet de forcer la génération d'une nouvelle clé de chiffrement à chaque modification de fichier LibreOffice et OpenOffice. Clé : HKLM\SYSTEM\CurrentControlSet\services\SboxTeamDrv\Parameters Type : DWORD Valeur : • 0 : Pas de génération d'une nouvelle clé de chiffrement (valeur par défaut) • 1 : Génération d'une nouvelle clé de chiffrement

3.4.2 Fichier *sbox.ini*

Section / Paramètre	Objectif
[Logon]	
`AllowPassword = 0` `AllowCard = 1`	N'autoriser que la connexion en mode en carte.
`GUILog = 1`	Interdire la saisie d'un mot de passe en ligne de commande.
[NewUser]	
`AllowNewUser = 0`	Désactiver la création de compte en local dans le cas d'un déploiement de compte via un fichier d'installation de compte utilisateur.
`AllowNewUser = 1`	Activer la création de compte en local dans le cas d'une création automatique du compte en mode carte à puce.
[SBox.NewUserWizardExKS1] **[SBox.NewUserWizardExKS2]**	
`AllowNewUser = 0`	Désactiver la création de compte en mode mot de passe.
[SBox.KeyRenewalWizardGP]	
`AutomaticRenewFromCard = 2`	Forcer le renouvellement des clés en mode carte à puce à partir des clés présentes dans la carte.
[External PKCS11 Policy]	
`CPLCanChangePKCS11 = 0`	Ne pas autoriser l'utilisateur à modifier le type de carte ou token.

Les paramètres des sections [DirectoryUpdate], [File] et [Team] correspondant à cet environnement ayant été déplacés en version 8.0.2, si l'utilisateur veut conserver un paramétrage équivalent à la suite d'une migration vers la version 10.1.1, il faut renseigner les nouveaux paramètres dans le compte utilisateur ou le modèle associé. Pour connaître la procédure à suivre, référez-vous à l'Annexe B. Procédure de migration d'un parc Security BOX Suite 8.0.x et 9.x vers la version Stormshield Data Security 10.1.1.

Voici la liste des paramètres qui ont été supprimés du fichier *sbox.ini* et rajoutés dans les paramètres de Stormshield Data Authority Manager depuis la version 8.0.2.

Section / Paramètre	Objectif
[DirectoryUpdate]	Ces paramètres permettent de mettre à jour automatiquement l'annuaire de l'utilisateur.
`Activate`	
`AllowManualUpdate`	
`55CompatibilityModes`	
`StartConnection`	
`ReplaceFromLDAP`	
`ReplaceFromLDAPOnValidCert`	
`ReplaceFromLDAPOnOutOfDateCert`	

Section / Paramètre	Objectif
ReplaceFromLDAPOnRevokedCert	
CommonNameRevoke	
CommonNameReplace	
CommonNameOutofDate	
CommonNameNotOnLDAP	
DeleteIfOutOfDate	
DeleteIfRevoke	
DeleteIfNotOnLDAP	
AllowDownloadCRL	
DisableCheckOnDisplay	
Timer	
[File]	Ces paramètres permettent de modifier le comportement du module Stormshield Data File sur les fichiers situés sur le réseau.
CanEncryptNetFile	
CanDecryptNetFile	
[Team]	Ces paramètres permettent de modifier le comportement avancé du module Stormshield Data Team.
AllowLocalCertificateStore	
DenyAccessOnBadCertificate	
HideDetachRule	
UpdateFileDateOnSecurityUpdate	

3.5 Base de registre

Stormshield Data Security accepte également les paramètres suivants en base de registre :

Paramètre	Description
`AlternateCheckHolder`	Permet la prise en compte d'un changement de l'identité du titulaire d'un certificat lors de l'application d'un fichier de mise à jour (*.usx*), par exemple lorsque le nom de domaine de l'adresse e-mail a changé. L'identité du titulaire comprend : • Email • Pays • Organisation/Société • Département/Unité • Localité • Prénom • Nom de famille • Nom usuel Clé : HKLM\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel Type : DWORD Valeur : • 0 : Pas de prise en compte de la nouvelle identité, le fichier *.usx* ne s'applique pas (valeur par défaut). • 1 : Prise en compte de la nouvelle identité.
`DelayUnfreezeCardMessage`	Permet de régler la durée d'affichage du message d'information demandant l'insertion de la carte, lors d'une tentative d'opération cryptographique alors que la session d'un compte carte est verrouillée. Le message a par défaut une durée d'affichage de deux secondes. Clé : HKLM\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Kernel\DelayUnfreezeCardMessage Type : DWORD 32 bits Valeur : Temps compris entre 2 et 30 secondes. Valeur par défaut :2.

4. Gestion des cartes et tokens USB

Vous pouvez configurer la suite Stormshield Data Security afin d'utiliser une carte à puce ou un token USB. Cette section décrit comment installer et gérer ce type de compte utilisateur.

4.1 Type de carte ou token USB utilisé

Stormshield Data Security peut utiliser toute carte ou token USB dès lors que son constructeur fournit un module cryptographique *PKCS#11* (interface standard) compatible. Pour les cartes ou tokens dont le fabricant a publié ses minidrivers auprès de Microsoft, vous pouvez utiliser le middleware Stormshield Data Security afin de bénéficier d'un fonctionnement Plug-and-Play. Pour les autres cartes vous devez installer manuellement le middleware compatible.

Le **Configurateur de type de carte ou clé USB** (depuis le menu **Windows/Démarrer/Stormshield Data Security**) permet de définir le nom de la DLL du module cryptographique à mettre en œuvre.

Ce configurateur connaît le nom des DLL de certains constructeurs. Ces noms sont définis dans le fichier *CardChoice.ini* (décrit à la section Fichier CardChoice.ini). Ce fichier peut être complété pour prendre en compte des cartes ou des tokens non prévus initialement.

Pour activer un module cryptographique au sein de Stormshield Data Security :

1. Lancez le configurateur depuis le menu Windows.
2. Choisissez un type de carte pré-défini, ou définissez-en un nouveau (nom du constructeur et surtout nom de la DLL de son interface *PKCS#11*).
3. Éventuellement testez ce module en cliquant sur le bouton **Informations** : le nombre de lecteurs visibles est indiqué (il doit être au moins 1).
4. Validez votre choix en cliquant sur **Appliquer** ou **OK**.
5. Fermez la session Windows et ouvrez en une nouvelle pour prendre en compte la modification.

Il est désormais possible de créer ou d'utiliser un compte carte.

Pour pouvoir utiliser les cartes à puce virtuelles, cette fonctionnalité doit être activée sur les postes qui seront déployés avec SDS. Afin que SDS puisse utiliser les cartes à puces virtuelles, vous devez les déployer et les peupler avec des clés à l'aide d'un outil de gestion externe. Ensuite vous pouvez créer un compte carte comme pour les supports cryptographiques physiques. Reportez-vous au *Guide d'installation* pour plus d'informations.

4.2 Fichier *CardChoice.ini*

Le fichier *CardChoice.ini* se trouve dans le dossier *<InstallDir>\Kernel*.

Ce fichier est utilisé uniquement par le configurateur de type de carte ou clé USB (il n'est pas utilisé par le noyau de Stormshield Data Security). Il contient la liste de modules cryptographiques connus et proposés par ce configurateur.

Le fichier *CardChoice.ini* est composé d'une section par constructeur, laquelle comprend :

- le nom de la DLL de l'interface *PKCS#11* du constructeur ;
- les éventuels attributs d'objet *PKCS#11* non supportés par cette interface.

Le tableau suivant détaille le contenu d'une section relative à un type de carte ou token.

NOTE
Les caractères Unicode ne sont pas supportés par le fichier *cardchoice.ini*. Par conséquent, les chemins paramétrés ne doivent contenir que des caractères ANSI, excepté les caractères / * ? < > " | ! # @. Néanmoins, ces caractères peuvent être insérés entourés de guillemets.

Pour prendre en compte les modifications effectuées pour un type de carte ou token et les appliquer à la configuration de Stormshield Data Security, relancez le système et effectuez les opérations suivantes :

1. relancez le configurateur de type de carte ou token USB ;
2. sélectionnez le type de carte si cela n'est pas déjà fait ;
3. validez le choix en cliquant sur **Appliquer** ou **OK** ;
4. relancez le système pour prendre en compte la modification.

`dllname`	Nom (et éventuellement chemin) de la DLL *PKCS#11* du constructeur. Ce paramètre est obligatoire.
• `eCKA_MODIFIABLE`: CK_TRUE si l'objet peut être modifié (par défaut) • `eCKA_EXTRACTABLE`: CK_TRUE si la clé peut être extraite de la carte • `eCKA_LABEL`: description de la clé • `eCKA_MODULUS_BITS`: taille du module	Permet de spécifier des attributs non pris en compte par l'interface *PKCS#11* du constructeur : • 0 : cet attribut est géré par l'interface *PKCS#11* du constructeur (par défaut) ; • 1 : cet attribut n'est pas géré. Ces paramètres sont également modifiables via le menu **Avancé** du **Configurateur de carte ou de clé USB**.
`AllSlot`	Certains constructeurs gèrent des lecteurs logiques sur lesquels il est impossible de se connecter. Ce paramètre permet de ne pas afficher tous les slots détectés. • 0 : l'affichage est limité aux slots avec une carte ou une clé USB présente (par défaut) ; • 1 : tous les slots sont affichés.

4.3 Utilisation de plusieurs types de cartes ou clés USB sur le même poste de travail

Stormshield Data Security peut utiliser plusieurs types de cartes ou clés USB sur la même machine et sur la même session Windows. Le menu contextuel de l'icône de notification Stormshield Data Security dans la barre des tâches permet de passer d'un type de module cryptographique à un autre sans avoir à utiliser le configurateur de l'extension carte.

Pour accéder au menu permettant de choisir le type de carte ou de clé USB, le fichier *sbox.ini* doit être au préalable configuré de la façon suivante :

- La section [Logon] doit comporter le paramètre `AllowCard=1`,
- La section [External PKCS11 Policy] doit comporter le paramètre `CPLCanChangePKCS11=1`. Si ce n'est pas le cas, les modules cryptographiques apparaîtront grisés, même s'ils sont disponibles sur le poste de travail.
- La section [External PKCS11 Policy] doit comporter le paramètre `CPLPKCS11KnownList` indiquant le chemin d'un fichier « *CardChoice.ini* » accessible en lecture par l'utilisateur courant.

Pour plus d'informations sur les sections du fichier *sbox.ini* et les paramètres disponibles, référez-vous à la section Références.

Pour choisir un type de module cryptographique :

1. Déconnectez vous de Stormshield Data Security.
2. Faites un clic-droit sur l'icône de notification dans la barre des tâches, puis accédez au menu **Choisir un type de carte ou de clé USB**.
3. La liste des périphériques disponibles sur votre poste de travail apparaît. Une coche indique le module cryptographique *PKCS#11* en cours d'utilisation.
4. Sélectionnez dans le menu le module qui correspond au modèle du périphérique que vous souhaitez utiliser. Une boîte de dialogue s'ouvre. Cliquez sur **Oui** pour redémarrer Stormshield Data Security et prendre en compte les modifications.
5. Après le redémarrage de Stormshield Data Security, double-cliquez sur l'icône de notification pour vous connecter en utilisant le nouveau périphérique, ou faites un clic droit et sélectionnez **Connecter…**.

Si aucun des modules définis dans le fichier *CardChoice.ini* n'a été détecté sur le poste de travail, le message « Aucun module cryptographique détecté » apparaît lorsque l'on sélectionne le menu **Choisir un type de carte ou de clé USB**.

Si un module a été détecté, mais que son chargement a échoué, alors il apparaîtra grisé et ne pourra pas être sélectionné.

Si le module cryptographique est installé après Stormshield Data Security, le redémarrage de la session Windows est nécessaire pour le voir apparaître dans le menu. De la même manière, il faut redémarrer la session Windows pour ne plus voir apparaître dans le menu un module cryptographique qui a été désinstallé.

4.4 Activation directe d'un module cryptographique

La procédure standard pour activer un module cryptographique consiste à utiliser le **Configurateur de carte ou clé USB** selon le mode opératoire décrit à la section Type de carte ou token USB utilisé.

Il est possible de ne pas utiliser ce configurateur en écrivant directement dans le registre de Windows le nom de la DLL du module cryptographique (avec éventuellement son chemin) sous la clé de registre :

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

Il faut ensuite relancer le système d'exploitation pour prendre en compte toute modification.

4.5 Cohabitation avec d'autres cartes ou tokens

Si plusieurs supports cryptographiques sont connectés à un poste, vous pouvez choisir lequel vous souhaitez utiliser lors de la connexion à Stormshield Data Security. Notez que vous devez

utiliser le même lecteur pour le support cryptographique physique connecté tout au long de votre session Windows.

Certains périphériques embarquent un lecteur de carte et une carte à puce, comme par exemple, une carte UMTS avec sa carte SIM.

Or, des middlewares signalent la présence d'une telle carte, même si son pilote ne permet pas de l'exploiter.

La section [SlotFilter], décrite à la section Section [SlotFilter], permet d'indiquer à Stormshield Data Security les "slots" *PKCS#11* à interroger afin de filtrer les "slots" parasites.

```
[Logon]
SlotFilterOn=1

[SlotFilter]
SlotInfoDescriptionPrefix=    ; préfixe du champ "description"
SlotInfoManufacturerIdPrefix= ; préfixe du champ "ManufacturerId"
```

4.6 Création automatique de compte carte dès la première utilisation d'une carte

Pour faciliter le déploiement des comptes carte, et minimiser les actions de l'utilisateur, Stormshield Data Security 10.1.1 peut créer automatiquement le compte carte d'un utilisateur lors de la première introduction de celle-ci.

Pour cela, l'utilisateur introduit simplement sa carte à puce ou token. Stormshield Data Security détecte automatiquement qu'il n'y a pas de compte existant associé et propose d'en créer un. Pour effectuer cette opération, l'utilisateur n'a qu'à saisir le code confidentiel de la carte et le compte Stormshield Data Security est ainsi créé.

4.6.1 Paramétrage

Un seul type de compte carte doit être autorisé sur le poste :

- compte mono-clé avec double usage signature et chiffrement ;
- compte mono-clé avec l'usage chiffrement seul ;
- compte mono-clé avec l'usage signature seule ;
- compte avec deux clés, l'une de chiffrement, l'autre de signature.

Le tableau ci-dessous indique les combinaisons de paramètres compatibles avec la création automatique de compte carte. Cette fonction nécessite l'utilisation du paramètre AllowNewUserAuto décrit section Section [NewUserCard].

Section	Item	Valeur
Compte mono-clé bi-usage		
SBox.NewUserWizardExGP1	AllowNewUser	1
SBox.NewUserWizardExGP1	AllowNewUserCipher	0
SBox.NewUserWizardExGP1	AllowNewUserSign	0
SBox.NewUserWizardExGP2	AllowNewUser	0
Compte mono clé usage chiffrement		

Section	Item	Valeur
SBox.NewUserWizardExGP1	AllowNewUser	0
SBox.NewUserWizardExGP1	AllowNewUserCipher	1
SBox.NewUserWizardExGP1	AllowNewUserSign	0
SBox.NewUserWizardExGP2	AllowNewUser	0
Compte mono clé usage signature		
SBox.NewUserWizardExGP1	AllowNewUser	0
SBox.NewUserWizardExGP1	AllowNewUserCipher	0
SBox.NewUserWizardExGP1	AllowNewUserSign	1
SBox.NewUserWizardExGP2	AllowNewUser	0
Compte bi-clé		
SBox.NewUserWizardExGP1	AllowNewUser	0
SBox.NewUserWizardExGP1	AllowNewUserCipher	0
SBox.NewUserWizardExGP1	AllowNewUserSign	0
SBox.NewUserWizardExGP2	AllowNewUser	1

NOTE
La création automatique de compte carte est incompatible avec des valeurs différentes de 10 ou 11 pour le paramètre `KeepCardObjects`.

4.7 Utilisation des clés de la carte

Indépendamment des clés courantes de l'utilisateur, il est possible de placer dans la carte d'autres clés de chiffrement.

Ces clés de chiffrement sont automatiquement utilisées par Stormshield Data Security pour déchiffrer des documents (messages/fichiers) lorsque la clé courante ne peut pas y parvenir.

Ces clés peuvent avoir plusieurs provenances :

- anciennes clés de chiffrement de l'utilisateur. Il est possible de placer dans la carte des clés obsolètes (avec les certificats associés) afin de permettre à l'utilisateur de déchiffrer des fichiers chiffrés avec d'anciennes clés (cela sert notamment pour les fichiers stockés dans des sauvegardes) ;
- clés externes. Par exemple, des clés d'anciens collaborateurs dont on veut pouvoir récupérer les informations (fichiers/messages).

Selon les composants Stormshield Data Security, les clés de la carte ne sont pas identifiées de la même façon. Pour certains composants, les clés sont identifiées à partir de leur attribut CKA_ID (il faut donc que la clé garde toujours la même valeur de CKA_ID) tandis que pour d'autres composants, l'identification est faite à partir des informations du certificat (émetteur et numéro de série).

Il est donc recommandé que les clés stockées dans les cartes le soient toujours avec le même attribut *PKCS#11* CKA_ID et que tous les certificats associés soient également présents.

4.8 Renouvellement des données de la carte

Cette section décrit le renouvellement de données de la carte effectué avec des moyens externes à Stormshield Data Security. Ces données sont donc mises à jour par un produit tiers et sont destinées à être utilisées par la suite par Stormshield Data Security.

4.8.1 Renouvellement des certificats

En cas de renouvellement de certificats dans la carte ou token, les nouveaux certificats sont pris en compte lors de la prochaine connexion de l'utilisateur à Stormshield Data Security.

Lorsqu'un nouveau certificat est ajouté à la carte, il faut que l'objet certificat créé ait bien le même attribut *PKCS#11* CKA_ID que l'ancien.

L'ancien certificat ne doit pas être supprimé tant que le nouveau n'a pas été pris en compte correctement par Stormshield Data Security. Il est possible de vérifier que le nouveau certificat a bien été pris en compte en utilisant le porte-clés du panneau de configuration Stormshield Data Security.

4.8.2 Renouvellement des clés

En cas de renouvellement de clés (avec le certificat associé) dans la carte ou le token, les nouvelles clés sont prises en compte lorsque les anciennes clés deviennent obsolètes ou, plus précisément, lorsque leur certificat devient obsolète.

Dans le cas de compte avec plusieurs clés (une de chiffrement et une de signature), le choix des nouvelles clés s'effectue en fonction des usages des certificats associés.

Les anciennes clés (signature et chiffrement) ne doivent pas être supprimées tant que les nouvelles n'ont pas été prises en compte correctement par Stormshield Data Security. Il est possible de vérifier que les nouvelles clés ont bien été prises en compte en utilisant le porte-clés du panneau de configuration Stormshield Data Security.

4.8.3 Réinitialisation des clés

Lorsque les clés ont été prises en compte par Stormshield Data Security, il est possible de supprimer les anciennes clés. Cependant, il est recommandé de ne supprimer que la clé de signature et de garder la clé de chiffrement afin de pouvoir déchiffrer des documents (fichiers/messages) chiffrés avec l'ancienne.

Si une clé est supprimée avant que sa remplaçante ait été prise en compte par Stormshield Data Security, l'utilisateur ne pourra plus se connecter à son compte.

Dans le cas d'un compte mono-clé (clé personnelle), il est recommandé de ne pas supprimer de clé dans la carte ou le token.

Il est possible de réinitialiser (par un outil autre que Stormshield Data Security) une carte avec des nouvelles clés de signature et de chiffrement.

IMPORTANT
Il est impératif que l'ancienne clé de chiffrement reste bien dans la carte.

Pour activer cette fonction, il faut écrire dans le fichier *SBox.ini* :

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

5. Création de compte à partir d'un modèle de compte

5.1 Création de compte à partir d'un modèle de compte

Stormshield Data Security peut créer des comptes à partir d'un modèle, afin qu'ils intègrent automatiquement :

- des données de configuration spécifiques ;
- des certificats de recouvrement ;
- une liste de certificats préchargés dans l'annuaire.

Un modèle de compte se compose :

- d'un fichier *.usr* à partir duquel sont copiés :
- toutes les données de configuration : Connexion, Mail, File, Shredder, liste des annuaires LDAP, Contrôleur de révocation (dont émetteurs de CRL et les points de distribution personnalisés, etc...) ;
- tous les éventuels certificats de recouvrement non "cachés".
- d'un ou plusieurs fichiers de certificats (*.cer*, *.crt*, *.p7c*, *.p7b*) ;
- des fichiers liste (chiffrement, déchiffrement, exclusion) pour Stormshield Data File ;
- des fichiers liste (nettoyage, exclusion) pour Stormshield Data Shredder ;

Si ces fichiers liste ne correspondent pas au compte *xxx.usr* (ce qui entraîne une erreur dans le contrôle d'intégrité), il est possible d'invalider le contrôle d'intégrité en modifiant le paramètre MasterPolicies.

Il est possible de définir un modèle de compte différent pour chaque type de compte : KS1, KS2, GP1, GP2 (voir la section Types de compte).

NOTE
Stormshield Data Security refuse la création de compte dans les conditions suivantes :

- `MasterPath` renseigné dans le fichier *SBox.ini* ;
- `DirModelIsFolder = 0` ;
- `DirectoryModel =<X:\chemin\du\fichier.(cer|crt|p7b|p7c)>` ;
- le fichier pointé par `DirectoryModel` n'existe pas ou n'est pas accessible.

Stormshield Data Security affiche l'icône croix rouge et le message **Échec de la copie des modèles** en lieu et place d'un message d'avertissement.

5.1.1 Le modèle de compte est localisé sur un serveur

Si le modèle de compte est localisé sur un serveur, le fichier, **<ImageDir>\Program Files\ARKOON\Security BOX\Kernel\sbox.ini** doit contenir les items suivants (voir la section Section [SBox.NewUserWizardExXXX]) :

- `MasterPath` pour le fichier *.usr* contenant le modèle de compte ;
- `DirModelIsFolder` et `DirectoryModel` pour le(s) fichier(s) de certificats à intégrer dans l'annuaire.

5.1.2 Le modèle de compte doit être installé sur les postes

Principes de mise en œuvre

Si le modèle de compte doit être installé sur les postes de travail (par exemple, dans le cas de postes isolés sur lesquels Stormshield Data Security est installé à partir d'un CD personnalisé), il faut créer un dossier masters contenant les comptes modèles.

Ce sous-dossier est copié dans **C:\programData\Arkoon\Security BOX**.

> **NOTE**
> Lors de l'installation, les modèles et les fichiers associés sont automatiquement installés en même temps que le produit Stormshield Data Security et le fichier *SBox.ini* est mis à jour pour en tenir compte.

Contenu du dossier "masters"

Dans le dossier "masters", il faut créer des sous-dossiers correspondant aux différents types de comptes ks1, ks2, gp1 et gp2, pour lesquels il existe des modèles.

Dans ces dossiers **\masters\xxx** (où xxx = ks1, ks2, gp1 ou gp2), il faut déposer les fichiers suivants (aucun n'est obligatoire, seuls les fichiers présents sont pris en compte, les noms doivent impérativement être respectés) :

- pour un compte mot de passe avec une seule clé pour signer et chiffrer :
  - *ks1.usr* : keystore modèle ;
  - *ks1.p7c* : liste des certificats à importer.
- pour un compte mot de passe avec deux clés différentes pour signer et chiffrer :
  - *ks2.usr* : keystore modèle ;
  - *ks2.p7c* : liste des certificats à importer.
- pour un compte carte avec une seule clé pour signer et chiffrer :
  - *gp1.usr* : keystore modèle ;
  - *gp1.p7c* : liste des certificats à importer.
- pour un compte carte avec deux clés différentes pour signer et chiffrer :
  - *gp2.usr* : keystore modèle ;
  - *gp2.p7c* : liste des certificats à importer.

Pour un type de compte donné, un seul modèle de compte est possible. Si plusieurs modèles de compte doivent être mis en place, il faut générer une image de la procédure d'installation par modèle.

Les dossiers modèles peuvent également inclure des fichiers listes de Stormshield Data File et de Stormshield Data Shredder. Déposez dans chacun des dossiers les fichiers suivants :

- *SBoxFileList.dec* : liste de déchiffrement de Stormshield Data File ;
- *SBoxFileList.efp* : liste d'exclusion de Stormshield Data File ;
- *SBoxFileList.enc* : liste de chiffrement de Stormshield Data File ;
- *SBoxShrdList.cfp* : liste d'exclusion de Stormshield Data Shredder ;
- *SBoxShrdList.cln* : liste de nettoyage de Stormshield Data Shredder.

Cette procédure est automatique en utilisant la personnalisation de package de Stormshield Data Authority Manager.

5.2 Création automatique d'un volume à la première connexion

Il est possible de créer automatiquement un volume Stormshield Data Virtual Disk à la première connexion de l'utilisateur selon les principes suivants :

- aucune question n'est posée à l'utilisateur, mise à part une éventuelle confirmation préalable ;
- les paramètres de création sont lus dans le *SBox.ini*, section [Disk] ;
- le processus intègre le formatage (silencieux) du volume créé.

La création pouvant prendre un temps non négligeable, une barre de progression est affichée afin de faire patienter l'utilisateur.

Les informations de création de ce volume à la première connexion sont fournies à la section Données de création d'un volume à la première connexion.

6. Fonctionnalités avancées

Cette section regroupe un ensemble d'informations techniques (astuces, limites, précaution à prendre) sur les composants de la suite Stormshield Data Security.

6.1 Fonctions génériques pour toutes les applications Stormshield Data Security

6.1.1 Changement rapide d'utilisateur

Stormshield Data Security 10.1.1 n'est pas compatible avec la fonctionnalité de changement rapide d'utilisateur Windows (Fast User Switching).

6.1.2 Copies de sauvegarde automatiques

A chaque connexion réussie, Stormshield Data Security effectue une copie de sauvegarde (*.bak*) des fichiers keystore (*.usr*), annuaire (*.usd*) et base de révocation (*.bcrl*).

Si le compte de l'utilisateur est bloqué (après la saisie simultanée de plusieurs [3 par défaut] codes faux), ou s'il est corrompu, il faut restaurer le compte à partir de sa dernière copie de sauvegarde.

Pour cela, dans le dossier contenant le compte de l'utilisateur :

- renommer au cas où les 3 fichiers *.usr*, *.usd*, *.brcl* ;
- faire une copie de sauvegarde des 3 fichiers *.usr.bak*, *.usd.bak*, *.brcl.bak* ;
- supprimer l'extension *.bak* des 3 fichiers *.usr.bak*, *.usd.bak*, *.brcl.bak*.

L'utilisateur est ainsi remis dans l'état de sa dernière connexion réussie.

6.2 Journalisation des événements

Stormshield Data Security possède un mécanisme de journalisation des événements permettant aux administrateurs de surveiller l'environnement de sécurité défini et d'identifier un incident survenant au cours de l'utilisation de la solution.

6.2.1 Introduction

Tous les événements liés à Stormshield Data Security sont accessibles par l'intermédiaire de l'observateur d'événements Windows. Les données stockées peuvent être lues et analysées puis, une fois le problème identifié, l'action à mener peut être formulée de façon précise à partir des informations remontées.

Types de messages

Les messages d'erreur générés par Stormshield Data Security peuvent être de trois types différents :

- messages d'information : il s'agit d'une simple information qui ne met pas en jeu la sécurité ;
- messages d'avertissement : il s'agit d'une indication qui signale un problème potentiel à l'administrateur ;
- messages d'erreur : il s'agit d'un réel problème qui empêche l'installation de la configuration.

Détail des informations journalisées

Les journaux permettent de visualiser les informations suivantes :

- **Type de message** : information, avertissement ou erreur (voir la section Types de messages) ;
- **Date** : date à laquelle le message a été généré ;
- **Heure** : heure à laquelle le message a été généré ;
- **Source** : source à partir de laquelle l'événement a été généré ;
- **Catégorie** : brève description de la source de l'événement ;
- **Événement** : numéro correspondant au type du message généré ;
- **Utilisateur** : nom de l'utilisateur de Stormshield Data Security ;
- **Ordinateur** : nom (NetBIOS) de l'ordinateur.

6.2.2 Configuration

Lors d'une nouvelle installation de Stormshield Data Security, les journaux d'événements sont désactivés par défaut. Pour les activer, il est nécessaire de modifier les paramètres de la base de registre relatifs aux différentes catégories d'événements et permettre ainsi de remonter ou pas un type particulier d'événements.

La procédure s'effectue par le biais du gestionnaire de Group Policy Object (*gpedit.msc*). Les journaux sont ensuite accessibles par l'intermédiaire de l'observateur d'événements Windows. Ils peuvent également être envoyés sur un serveur distant.

Configuration par Group Policy Object

La GPO de Microsoft Windows utilise des fichiers *.admx* pour les paramètres de configuration, et des fichiers de langue *.adml*, où tous les textes relatifs à ces paramètres, sont référencés.

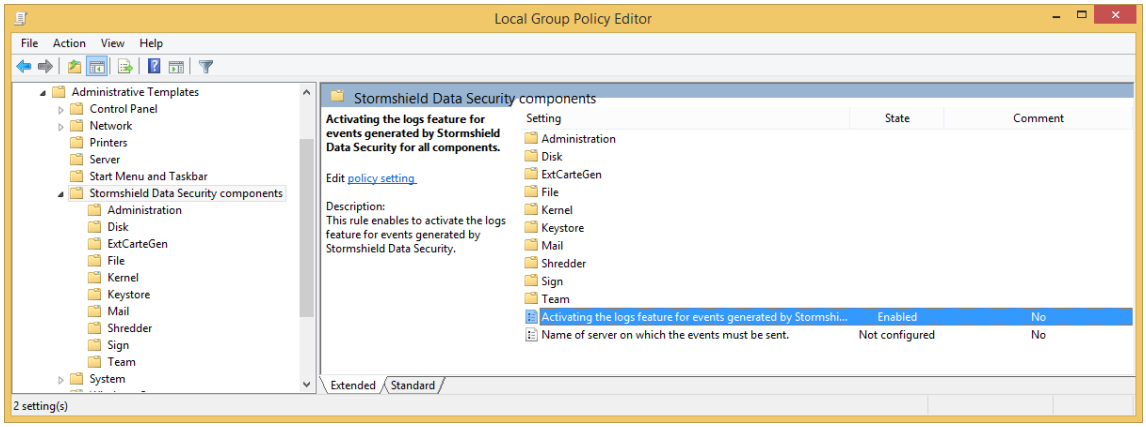
L'installation de Stormshield Data Security place :

- le fichier *Sbsuite.admx* dans le dossier *%SystemRoot%\PolicyDefinitions*
- le fichier de langue *Sbsuite.adml* dans le dossier *%SystemRoot%\PolicyDefinitions\en-US*

Ces fichiers sont chargés automatiquement lors du lancement de gpedit et il n'est pas nécessaire de les charger.

1. Lancez gpedit (**Démarrer** > **Exécuter** > puis tapez *gpedit.msc*).
2. Cliquez sur **Modèles d'administration** > **Composants Stormshield Data Security**. Une fois activée, l'entrée **Activer la fonctionnalité de journalisation des événements générés par Stormshield Data Security pour tous les modules** permet de démarrer la génération des événements. Les autres entrées permettent de configurer la génération des événements de façon plus précise.

Un changement de la stratégie de groupe modifie directement les valeurs correspondantes en base de registre. Celles-ci s'appliquent pour chaque utilisateur. Elles sont présentes sous la clé HKEY_CURRENT_USER de la base de registre. En revanche, une stratégie de groupe (spécifiée à distance par Active Directory) est prioritaire sur les changements effectués localement.



NOTE

La fonctionnalité **Activer la fonctionnalité de journalisation des événements générés par Stormshield Data Security pour tous les modules** est un interrupteur général : s'il est désactivé, aucun événement ne sera généré, quel que soit le réglage effectué pour les modules. De plus, un module “Non configuré” est actif si l'interrupteur global est activé.

Par exemple, si vous souhaitez n'activer que les événements du module Virtual Disk :

1. Activez la fonctionnalité de journalisation des événements générés par Stormshield Data Security pour tous les modules.
2. Activez la journalisation d'événements du module Virtual Disk de Stormshield Data Security.
3. Désactivez la journalisation d'événements pour tous les autres modules.

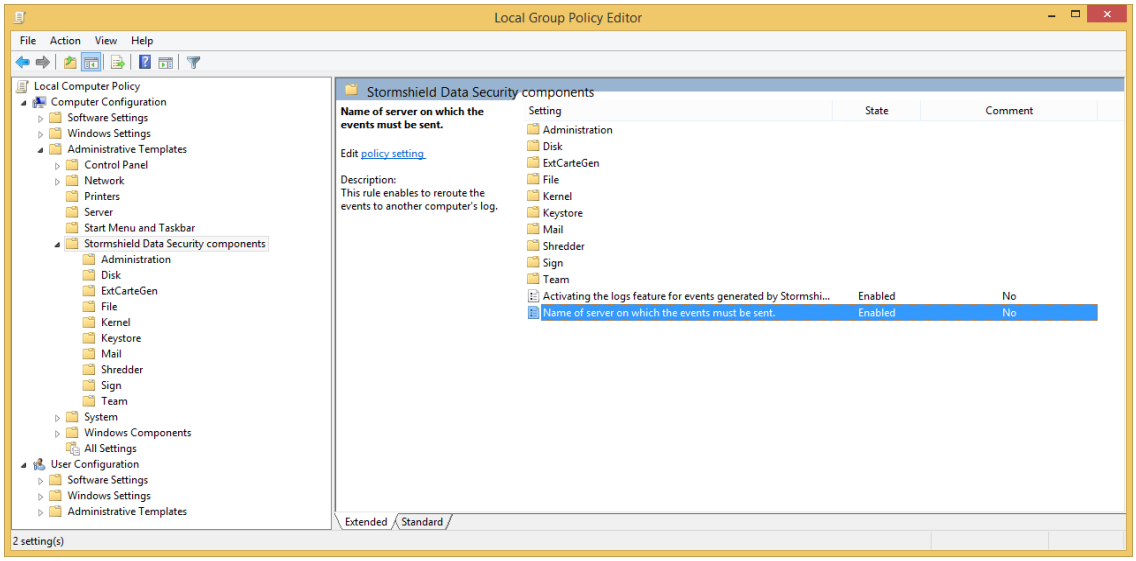
Journalisation sur un autre serveur distant

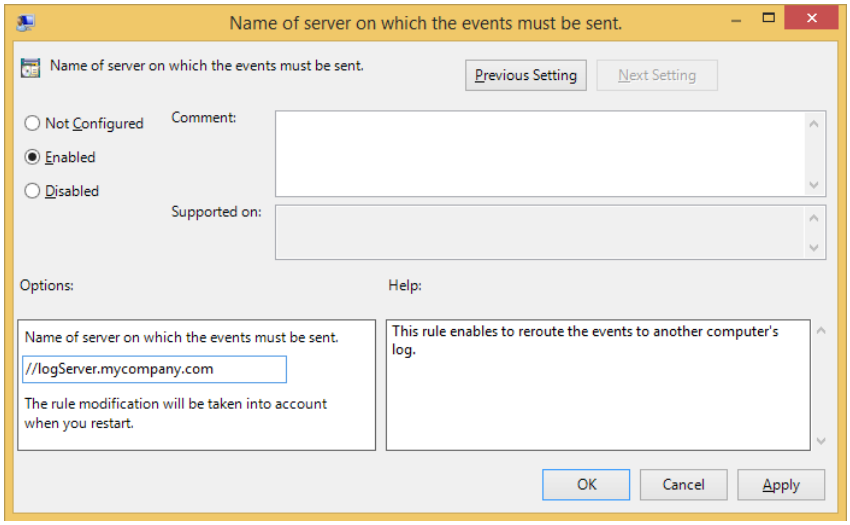
Il est possible de configurer la journalisation des événements vers un serveur distant afin de centraliser la collecte de ces derniers.

Le serveur de collecte des événements, ainsi que tous les postes émetteurs doivent être configurés pour autoriser respectivement la collecte et l'envoi de ces événements. Une description détaillée de cette configuration est disponible sur le site de Microsoft (https://msdn.microsoft.com/en-us/library/cc748890.aspx).

Une fois les machines configurées, indiquez à Stormshield Data Security vers quel serveur distant envoyer les événements, à l'aide du gestionnaire de Group Policy Object (*gpedit.msc*) :

1. Lancez gpedit (**Démarrer** > **Exécuter** > puis tapez *gpedit.msc*).
2. Cliquez sur **Modèles d'administration** > **Composants Stormshield Data Security**. Activez l'option **Nom du serveur vers lequel envoyer les événements**, et saisissez l'adresse du serveur distant de collecte.





6.2.3 Utilisation

Toutes les actions effectuées par Stormshield Data Security sont inscrites dans le journal des événements selon les mêmes critères (reportez-vous à la section Types de messages). Tous les événements sont consultables par l'intermédiaire de l'observateur d'événements Windows.

6.3 Stormshield Data Virtual Disk

6.3.1 Recouvrement via le fichier *.vboxsave*

Le support physique d'un volume sécurisé est un fichier container (extension *.vbox*) qui contient :

- les éléments cryptographiques nécessaires au montage du volume (la clé symétrique de chiffrement du volume est fournie avec la clé publique de chacun des utilisateurs autorisés et avec chaque clé de recouvrement) ;
- le contenu proprement dit du volume (fichiers stockés dans le volume et système de fichier).

Les éléments cryptographiques sont systématiquement sauvegardés dans un "fichier de secours" (extension *.vboxsave*) à la création du volume, puis à chaque modification de la liste des utilisateurs.

Le recouvrement d'un volume Stormshield Data Virtual Disk est identique au changement de propriétaire décrit dans le manuel d'utilisation du produit. Simplement, l'utilisateur effectuant la demande de changement de propriétaire n'est pas le propriétaire initial mais l'utilisateur dont le certificat de chiffrement a été défini comme certificat de recouvrement.

Le recouvrement consiste donc à définir un nouvel utilisateur comme étant le propriétaire du volume. Ce nouveau propriétaire peut ensuite faire toutes les opérations qu'il souhaite.

Les paramètres permettant de modifier la liste des utilisateurs d'un volume à partir du fichier de secours .vboxsave sont décrits à la section Modification des utilisateurs d'un volume via le fichier .VBOXSAVE.

Recouvrement sans le fichier container

Cependant, par rapport au changement simple de propriétaire, il est possible d'effectuer un recouvrement sans disposer du fichier container mais uniquement avec le volume VBOXSAVE.

Cette procédure est notamment utile pour effectuer des recouvrements à distance. L'utilisateur disposant du fichier container n'a pas besoin de le transmettre dans sa totalité pour que le recouvrement soit effectué mais ne transmet que le fichier *.vboxsave*.

Pour cela, il faut que l'utilisateur désirant un recouvrement transmette le fichier *.vboxsave* à l'administrateur chargé du recouvrement. Celui-ci procède comme pour un changement de propriétaire puis transmet le fichier *.vboxsave* à l'utilisateur ayant effectué la demande. Celui-ci n'a plus qu'à mettre à jour le fichier *.vboxsave* et continuer la procédure de changement de propriétaire comme si c'était lui qui avait mis à jour le fichier *.vboxsave*.

6.3.2 Démontage en force

Il n'est pas conseillé de démonter un volume Stormshield Data Virtual Disk "en force", c'est-à-dire quand il y a des fichiers ouverts dessus. Si une telle opération s'avère cependant nécessaire, il est fortement recommandé de vérifier le volume (en utilisant l'outil Windows de vérification de disque) lors de son prochain montage, avant toute utilisation.

6.3.3 Copie de volumes

Si un volume sécurisé est dupliqué en copiant le fichier container .vbox, les deux exemplaires résultant ne peuvent pas être montés simultanément sur un même poste.

De façon générale, il n'est pas recommandé de dupliquer des volumes par copie du fichier container .vbox ; cela ne doit être utilisé que pour des sauvegardes.

6.3.4 Utilisation dans un contexte multi-sessions Windows

Pour faciliter son intégration au sein de Microsoft Windows, un volume Stormshield Data Virtual Disk se comporte comme un volume de stockage standard.

Par conséquent, un volume chiffré monté dans une session Windows est accessible depuis les autres sessions Windows ouvertes en parallèle sur le poste de travail.

Afin d'éviter ceci, l'utilisateur doit définir le verrouillage de son compte Stormshield Data Security lors du verrouillage de sa session Windows. Pour plus d'informations, reportez-vous à la section *Paramétrage sur mise en veille et verrouillage Windows* du *Guide d'installation et de mise en œuvre* de Stormshield Data Security Enterprise.

Le verrouillage a pour effet de démonter les volumes chiffrés montés dans la session. Cependant le démontage forcé peut avoir des conséquences sur les fichiers ouverts sur ce volume. L'utilisateur doit veiller à enregistrer ses modifications avant tout verrouillage de session.

Sur une version serveur de Windows, un utilisateur distant ne voit pas les volumes Stormshield Data Virtual Disk montés par les autres utilisateurs distants connectés au même serveur. Il est néanmoins conseillé d'appliquer le verrouillage automatique car les volumes disques sont simplement masqués. Les données qu'ils contiennent sont donc potentiellement accessibles.

6.3.5 Limites

- La taille maximale d'un volume Stormshield Data Virtual Disk est 2048 Go (2 To).
- Un volume de plus de 2 Go ne peut pas être formaté en FAT16 (c'est une limitation de FAT16).
- Un volume de moins de 2.5 Mo ne peut pas être formaté NTFS (c'est une limitation de NTFS).
- Il peut arriver que l'icône d'un volume Stormshield Data Virtual Disk dans l'explorateur soit incorrecte (soit une icône de disque normal, soit une icône de document).

6.4 Stormshield Data File

6.4.1 Permissions fichier

Si des permissions (au sens NTFS) sont définies sur un fichier, elles sont perdues après chiffrement ou déchiffrement par Stormshield Data File.

Si les permissions de Windows doivent être mises en œuvre sur des fichiers confidentiels sécurisés par Stormshield Data File, il faut définir ces permissions au niveau des dossiers contenant ces fichiers, et non sur les fichiers eux-mêmes.

6.4.2 Arrêt de Windows et traitements automatiques longs

Par défaut, Stormshield Data Security déconnecte l'utilisateur Stormshield Data Security quand la session de Windows est fermée (ou que l'utilisateur demande l'arrêt du système car cela effectue préalablement une fermeture de session).

Si l'utilisateur a paramétré un traitement automatique trop important (grande liste de nettoyage), il se peut que ce traitement n'ait pas le temps de se terminer.

Pour pallier ce risque, il est possible de configurer Stormshield Data Security afin qu'il interdise à Windows de fermer une session si un utilisateur Stormshield Data Security est connecté. Pour cela, indiquer dans le fichier *sbox.ini*, section [Logon], item NoShutDown=1 (section Section [Logon]).

Dans une telle configuration, l'utilisateur doit se déconnecter de Stormshield Data Security avant de fermer sa session Windows.

6.4.3 Syntaxe des fichiers liste de Stormshield Data File

Un fichier liste est un fichier texte, dont les lignes sont séparées par un CR+LF, sans ligne vide, et comportant trois lignes d'en-tête :

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

La 1ère ligne définit le type du fichier parmi les types suivants :

Contenu de la première ligne	Type de fichier
Stormshield Data Security Encryption List	*.enc
Stormshield Data Security Decryption List	*.dec
Stormshield Data Security Encryption Protected List	*.efp

La 2ème ligne définit la version du fichier : seule la version 1 est aujourd'hui implémentée.

La 3ème ligne : constante.

Les ligne(s) suivante(s) définissent un élément de la liste, selon la syntaxe :

- pour une liste de chiffrement, déchiffrement :

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

- pour une liste d'exclusion :

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

Notations :

Paramètre	Description	Remarque
Folder	Chemin complet du dossier.	Pas de "\" à la fin.
File	Nom du fichier seul.	Vide dans le cas d'un dossier.
dir	La ligne désigne un dossier.	`[File]` doit être vide.
file	La ligne désigne un fichier.	`[File]` ne doit pas contenir de "wildcards".
*	La ligne désigne un ensemble de fichiers.	`[File]` contient des wildcards ("*","?").
rec	Indicateur de récursivité.	Les sous-dossiers de Folder sont concernés.
SO	La ligne n'est pas modifiable par l'utilisateur.	`SO = System Officer`
hide	La ligne est cachée à l'utilisateur.	
ref	Les fichiers désignés sont protégés par un refus.	Réservé aux listes de protection.
conf	Les fichiers désignés sont protégés par une confirmation.	Réservé aux listes de protection.

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

6.4.4 Mots-clés des fichiers listes de Stormshield Data File

Les fichiers listes de Stormshield Data File prennent en compte les mots-clés suivants :

`AppData`	Le chemin type est **C:\Users\username\AppData\Roaming**.
`CommonDocuments`	Le chemin type est **C:\Users\Public\Documents**.
`Cookies`	Le chemin type est **C:\Users\username\AppData\Roaming\Microsoft\Windows\Cookies**.
`History`	Le dossier du système de fichier servant de dossier commun pour l'historique Internet.
`InternetCache`	Le chemin type est **C:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files**.
`Personal`	Le dossier virtuel représente l'objet bureau **C:\Users\username\Documents**.
`ProgramFiles`	Le chemin type est **C:\Program Files**.
`ProgramFilesCommon`	Le chemin type est **C:\Program Files\Common Files**.
`Recent`	Le chemin type est **C:\Users\username\AppData\Roaming\Microsoft\Windows\Recent**.
`System`	Le dossier du système Windows. Le chemin type est **C:\Windows\System32**.
`Windows`	Le dossier Windows ou SYSROOT. Il correspond aux variables d'environnement `%windir%` ou `%SYSTEMROOT%`. Le chemin type est **C:\Windows**.

6.5 Stormshield Data Shredder

6.5.1 Arrêt de Windows et traitements automatiques longs

Par défaut, Stormshield Data Security déconnecte l'utilisateur Stormshield Data Security quand la session de Windows est fermée (ou que l'utilisateur demande l'arrêt du système car cela effectue préalablement une fermeture de session).

Si l'utilisateur a paramétré un traitement automatique trop important (grande liste de nettoyage), il se peut que ce traitement n'ait pas le temps de se terminer.

Pour pallier ce risque, il est possible de configurer Stormshield Data Security afin qu'il interdise à Windows de fermer une session si un utilisateur Stormshield Data Security est connecté. Pour cela, indiquer dans le fichier *sbox.ini*, section [Logon], item NoShutDown=1 (section Section [Logon]).

Dans une telle configuration, l'utilisateur doit se déconnecter de Stormshield Data Security avant de fermer sa session Windows.

6.5.2 Syntaxe des fichiers listes de Stormshield Data Shredder

Un fichier liste est un fichier texte, dont les lignes sont séparées par un CR+LF, sans ligne vide, et comportant trois lignes d'en-tête :

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

La 1ère ligne définit le type du fichier parmi les types suivants :

Contenu de la première ligne	Type de fichier
Stormshield Data Security Clean List	*.cln
Stormshield Data Security Clean Protected List	*.cfp

La 2ème ligne définit la version du fichier : seule la version 1 est aujourd'hui implémentée.

La 3ème ligne : constante.

Les ligne(s) suivante(s) définissent un élément de la liste, selon la syntaxe :

- pour une liste de nettoyage :

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

- pour une liste d'exclusion :

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

Notations :

Paramètre	Description	Remarque
`Folder`	Chemin complet du dossier.	Pas de "\" à la fin.
`File`	Nom du fichier seul.	Vide dans le cas d'un dossier.
`dir`	La ligne désigne un dossier.	`[File]` doit être vide.
`file`	La ligne désigne un fichier.	`[File]` ne doit pas contenir de "wildcards".
`*`	La ligne désigne un ensemble de fichiers.	`[File]` contient des wildcards ("*","?").
`rec`	Indicateur de récursivité.	Les sous-dossiers de Folder sont concernés.
`SO`	La ligne n'est pas modifiable par l'utilisateur.	`SO = System Officer`
`hide`	La ligne est cachée à l'utilisateur.	
`ref`	Les fichiers désignés sont protégés par un refus.	Réservé aux listes de protection.
`conf`	Les fichiers désignés sont protégés par une confirmation.	Réservé aux listes de protection.

6.5.3 Mots-clés des fichiers listes de Stormshield Data Shredder

Les fichiers listes de Stormshield Data Shredder prennent en compte les mots-clés suivants:

`AppData`	Le chemin type est **C:\Users\username\AppData\Roaming**.
`CommonDocuments`	Le chemin type est **C:\Users\Public\Documents**.
`Cookies`	Le chemin type est **C:\Users\username\AppData\Roaming\Microsoft\Windows\Cookies**.
`History`	Le dossier du système de fichier servant de dossier commun pour l'historique Internet.
`InternetCache`	Le chemin type est **C:\Users\username\AppData\Local\Microsoft\Windows\Temporary Internet Files**.
`Personal`	Le dossier virtuel représente l'item bureau **C:\Users\username\Documents**.
`ProgramFiles`	Le chemin type est **C:\Program Files**.
`ProgramFilesCommon`	Le chemin type est **C:\Program Files\Common Files**.
`Recent`	Le chemin type est **C:\Users\username\AppData\Roaming\Microsoft\Windows\Recent**.
`System`	Le dossier du système Windows. Le chemin type est **C:\Windows\System32**.
`Windows`	Le dossier Windows ou SYSROOT. Il correspond aux variables d'environnement `%windir%` ou `%SYSTEMROOT%`. Le chemin type est **C:\Windows**.
`BitBucket`	Le dossier virtuel contient les items de la corbeille de l'utilisateur.

NOTE
La syntaxe d'utilisation de ces mots-clés est la suivante : `%mot-clé%`

Pour ajouter le contenu de la corbeille à une liste du Shredder, il faut ajouter l'item : `%BitBucket%`.

`%temp%` n'est pas géré. Il est néanmoins possible de le spécifier en considérant que

```
%AppData% -> C:\Users\username\AppData\Roaming
%temp% -> C:\Users\username\AppData\Local\Temp
```

Il en est déduit que `<"Appdata"\..\Local\Temp>` revient à travailler dans le `%temp%`.

Il faut donc saisir dans la liste : `%AppData%\..\Local\Temp\`.

6.6 Stormshield Data Mail

6.6.1 Stormshield Data Mail Édition Outlook

Format RTF

Le format RTF n'est pas supporté par Stormshield Data Mail Édition Outlook car il ne permet pas d'assurer une interopérabilité fiable avec le mécanisme de sécurisation de Stormshield Data Security. Utiliser le format RTF présente un risque de perte d'informations.

Par conséquent, il est recommandé d'utiliser le format HTML pour la rédaction de votre message sécurisé, car ce format ne présente pas de souci d'interopérabilité.

Transchiffrement

Le transchiffrement est une opération qui permet de mettre à jour le niveau de protection des messages sécurisés (messages au format S/MIME ou messages en clair contenant une pièce jointe chiffrée avec le composant Stormshield Data File) en re-chiffrant avec une nouvelle clé les messages sécurisés avec une ancienne clé de chiffrement et en utilisant l'algorithme de chiffrement configuré par défaut dans le compte utilisateur.

L'accès aux clés privées de l'utilisateur pendant le transchiffrement nécessite d'être connecté à Stormshield Data Security.

Il est donc recommandé de désactiver les options de déconnexion automatique et de verrouillage de session sur écran de veille lorsque le nombre de messages à transchiffrer est important, la durée de traitement étant proportionnelle au nombre de messages à traiter.

NOTE
Un message sécurisé ne sera pas transchiffré si la clé courante de chiffrement de l'utilisateur est celle qui a servi à chiffrer originellement le message.

De même, un message qui a déjà été transchiffré par la clé courante ne sera pas transchiffré à nouveau, tant que la clé courante de l'utilisateur n'est pas mise à jour.

Apprentissage de chiffrement

L'apprentissage de chiffrement permet le chiffrement automatique de messages envoyés à un destinataire spécifique. L'apprentissage s'appuie sur des valeurs par défaut de 90 jours et trois messages chiffrés envoyés sur cette période pour activer le chiffrement automatique.

Ces valeurs par défaut peuvent être modifiées grâce aux informations suivantes dans la base de registre :

HKEY_CURRENT_USER\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Mail\
AutoSuggestWithinDays =<DWORD : nombre de jours>

HKEY_CURRENT_USER\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Mail \
AutoSuggestUsageCount =<DWORD : nombre de messages envoyés>

L'option d'apprentissage peut également être activée ou désactivée en modifiant la clé suivante :

HKEY_CURRENT_USER\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Mail \
EnableAutoSuggestEncrypt=<DWORD : 0 pour désactiver, 1 pour activer>

6.6.2 Édition Lotus Notes non activée

La procédure d'installation de Stormshield Data Mail Édition Notes ajoute au fichier *notes.ini* ses quatre composants.

Si Édition Notes a été installée en réseau ou pour l'utilisateur courant uniquement (pas pour tous les utilisateurs du poste = AllUsers), le fichier *notes.ini* modifié par la procédure d'installation n'est pas celui réellement utilisé par Notes : l'extension Stormshield Data Security n'est alors pas activée.

Dans ce cas, il faut ajouter les lignes suivantes au fichier *notes.ini* réellement utilisé par Lotus Notes :

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

Si l'une de ces lignes est déjà présente (une autre extension est déjà installée), Stormshield Data Mail s'ajoute en fin de ligne.

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

Dans le cas où une extension était déjà présente et que le fichier *notes.ini* mis à jour n'est pas celui réellement utilisé, il convient de mettre à jour les lignes concernées en ajoutant les informations de Stormshield Data Security en fin de ligne.

6.6.3 Paramétrage LDAP : certificats comportant plusieurs adresses e-mail

Si un destinataire possédant plusieurs adresses e-mail dans son certificat est absent de l'annuaire de confiance Stormshield Data Security mais est présent sur votre (vos) annuaire(s) LDAP, une boite de dialogue indiquant que "le certificat n'a pas été trouvé dans votre annuaire de confiance" peut s'ouvrir à l'envoi d'un message chiffré vers ce destinataire.

Dans cette situation spécifique, vous pouvez paramétrer votre annuaire LDAP pour faire en sorte de retrouver le certificat à l'envoi du message chiffré.

Pour cela, vérifiez que l'attribut « proxyAddresses » de l'utilisateur dans l'annuaire LDAP contient bien toutes les adresses e-mail secondaires de l'utilisateur.

Dans cet attribut, chaque adresse e-mail secondaire doit être précédée de « smtp: », alors que l'adresse principale est précédée de « SMTP: ».

Cet attribut peut être mis à jour via des serveurs de messagerie d'entreprise de type Exchange.

6.6.4 Vérification de cohérence des adresses e-mail

Lors de l'envoi de message, le meilleur certificat disponible pour chaque destinataire est recherché. Si ce certificat provient de l'annuaire LDAP, une vérification de cohérence est effectuée entre l'adresse e-mail du destinataire et celle contenue dans ce certificat. En cas de différence, le certificat est rejeté, et l'envoi du message peut être annulé.

Si vous utilisez des alias internes pour les adresses des utilisateurs, ce mécanisme peut devenir inopportun.

- Pour désactiver ce mécanisme de vérification de cohérence des adresses e-mail sur un poste utilisateur, positionnez la valeur **DWORD CheckLDAPCertificateEmailAddress** à 0 dans la clé de registre HKLM\SOFTWARE\Arkoon\Security BOX Enterprise\Mail.

> **NOTE**
> La vérification de cohérence d'adresses e-mail a été implémentée pour des raisons de sécurité. Il est donc recommandé de ne pas la désactiver si ce n'est pas absolument nécessaire.

6.7 Stormshield Data Team

6.7.1 Restriction en environnement DFS

- Une racine DFS ne peut pas être chiffrée.
- Les comptes Stormshield Data Security ne doivent pas être hébergés sur un partage DFS.

6.7.2 Gestion du dossier temporaire utilisateur (%TEMP%)

Il ne faut pas indiquer plusieurs collaborateurs sur une règle affectant le dossier temporaire du profil Windows. Ce dossier est utilisé par les applications pour stocker des fichiers temporaires propres à l'utilisateur.

Si cette règle n'est pas respectée, des blocages peuvent se produire.

6.7.3 Gestion du dossier temporaire du système

Ce dossier est utilisé par les processus système (typiquement les services) pour stocker des fichiers temporaires et il est partagé avec les autres utilisateurs du système.

Ce dossier est typiquement **C:\windows\temp**. La localisation exacte dépend de l'installation du système d'exploitation.

Ce dossier ne doit pas être chiffré avec Stormshield Data Team.

6.7.4 Dossiers disponibles hors connexion

Il est possible via l'utilitaire *cachemov.exe* de déplacer le dossier système - *<%WINDIR%>\CSC* - qui contient les fichiers disponibles hors connexion.

La prise en charge de cet environnement particulier nécessite de paramétrer Stormshield Data Team.

Pour cela, suivre la procédure suivante :

1. Lancez **regedit**.
2. Atteignez la clé **HKLM\SYSTEM\CURRENTCONTROLSET\Services\SBoxTeamDrv\Parameters**.
3. Ajoutez à la valeur de `SkipFolderR`, le dossier contenant la base CSC.
4. Redémarrez la machine.

6.7.5 Optimisation des accès sur réseau lent

Pour savoir si un fichier est réellement chiffré ou non, Stormshield Data Team doit l'ouvrir. Sur un réseau à bas débit (par exemple GPRS), l'explorateur peut alors devenir extrêmement lent, voire sembler bloqué.

Stormshield Data Team peut dans ce cas être paramétré de manière à se fier à la présence d'une règle partagée stockée au niveau d'un dossier pour déterminer si un fichier est chiffré ou non.

Pour activer ce fonctionnement, écrivez dans la base de registre :

Sous **HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Properties\Team** : la clé `OverlayIconAccuracy (DWORD) = 0x00000005`.

IMPORTANT
Dans ce mode de fonctionnement :

- dans un dossier non sécurisé, un fichier chiffré apparaît en clair ;
- dans un dossier sécurisé, un fichier en clair apparaît chiffré.

6.7.6 Maintien des performances du poste de travail

L'utilisation de Stormshield Data Team peut provoquer un ralentissement du fonctionnement des postes de travail des utilisateurs. Afin de garantir les performances habituelles, il est possible d'appliquer les paramétrages suivants sur les postes.

Amélioration des performances lors du parcours d'arborescences chiffrées

Cette amélioration permet de diminuer sensiblement le temps de détermination de l'état chiffré ou non d'un dossier (détermination de l'icône d'un dossier) en mode « Carte à puce ».

Cette option se paramètre par l'intermédiaire de l'OverlayIconAccuracy dans la base de registre :

1. Accédez à la base de registre en lançant **regedit.exe**.
2. Dans l'arborescence, atteignez la clé **HKEY_LOCAL_MACHINE\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Team**.
3. Modifiez la valeur de la clé `OverlayIconAccuracy = 0x40`.
4. Quittez la base de registre.
5. Redémarrez la machine.

Cette valeur peut être combinée aux autres valeurs actuelles.

Exclusion de processus Windows accédant aux dossiers chiffrés

Certains processus Windows peuvent ralentir le fonctionnement du poste de travail en accédant régulièrement à des dossiers chiffrés par Stormshield Data Team.

Pour limiter ces ralentissements, vous pouvez exclure dans la base de registre les processus considérés sûrs et qui n'engendrent pas de modification des fichiers :

1. Accédez à la base de registre en lançant **regedit.exe**.
2. Dans l'arborescence, atteignez la clé **HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SboxTeamDrv\Parameters**.
3. Modifiez la valeur de la clé `SkipApp` en ajoutant la liste des processus à exclure. Ajoutez un processus par ligne. Si la clé n'existe pas, vous pouvez la créer en choisissant une valeur de type REG_MULTI_SZ.
4. Quittez la base de registre.
5. Redémarrez la machine.

Nous vous conseillons d'exclure les processus suivants :

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

- SearchApp.exe
- NisSrv.exe

Processus spécifiques Dell :

- HostStorageService.exe
- HostControlService.exe

Exclusion d'extensions et de processus de l'analyse de Windows Defender

Pour éviter des ralentissements du fonctionnement du poste de travail, vous pouvez également exclure des extensions et processus de l'analyse du logiciel Windows Defender :

1. Accédez à la base de registre en lançant **regedit.exe**.
2. Dans l'arborescence, atteignez la clé **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions**.
3. Dans la clé `Extensions`, ajoutez la liste des extensions à exclure. Nous vous recommandons d'exclure les extensions suivantes : *.box*, *.sbox*, *.sbt*, *.sdsx*, *.usi*, *.usr* (type REG_DWORD).
4. Dans la clé `Processes`, ajoutez la liste des processus à exclure. Nous vous recommandons d'exclure les processus suivants : SBDSRV, SBoxDiskSrv (type REG_DWORD) ainsi que les processus des antivirus et d'autres EDR.
5. Quittez la base de registre.
6. Redémarrez la machine.

6.7.7 Exclusion de dossier

Stormshield Data Team dispose de la fonctionnalité `ExcludedPath`, qui permet d'exclure des dossiers du champ d'action de Stormshield Data Team.

Cette fonctionnalité prend en compte :

- la gestion de l'affichage de l'onglet *Propriétés Team* sur les dossiers : le contenu de l'onglet *Team* n'est plus accessible pour un dossier d'une arborescence exclue du chiffrement ;
- la gestion du rapport de chiffrement de l'application d'une règle partagée : un fichier d'une arborescence exclue a un statut **Fichier exclu** lors d'une opération de sécurisation ou de désécurisation. Lors d'une opération de désécurisation, un fichier en clair conserve son statut Fichier en clair ;
- la gestion du pictogramme : le pictogramme Team n'est pas affiché sur un dossier d'une arborescence exclue du chiffrement.

Pour qu'un dossier ne soit pas analysé par Stormshield Data Team, vous devez l'ajouter à la rubrique `ExcludedPath` de la section [TEAM] du fichier *SBox.ini*.

La syntaxe est la suivante :

```
[TEAM]
ExcludedPath = path * [,path]
```

Où `path` est le chemin du dossier à exclure.

Ce chemin peut être composé de balises Stormshield Data Security en mettant ceux-ci entre < >

La valeur par défaut est : `ExcludedPath = <%APPDATA%>`.

NOTE
Il est important de ne pas mettre d'espace entre la virgule et le chemin.

La balise peut être :

- `RootPath1`: dossier des comptes utilisateurs du *SBox.ini* ;
- `RootPath2`: second dossier des comptes utilisateurs ;
- `COMMON_APPDATA: C:\ProgramData` ;
- `COMMON_DOCUMENTS: C:\Users\Public\Documents` ;
- `USERNAME : <username>` le nom d'utilisateur Windows connecté ;
- `LOCAL_APPDATA: C:\Users\username\AppData\Local` ;
- `DESKTOP: C:\Users\username\Desktop` ;
- `MYDOCUMENTS: C:\Users\username\Documents` ;
- `PROFILE: C:\Users\username` ;
- `%ENV%`: où `ENV` est une variable d'environnement système.

Exemple :

```
[TEAM]
```

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

Si les paramètres `RootPath1` ou `DefaultPath1` de *SBox.ini* sont personnalisés, il devient nécessaire d'ajouter ces dossiers spécifiques en `ExcludedPath`.

La taille maximale du paramètre `ExcludedPath` est de 255 caractères.

6.7.8 Déplacement de dossier intra-volume

Le déplacement de dossier intra-volume est interdit lorsque les dossiers source et destination n'ont pas la même sécurité.

Si l'opération est effectuée dans l'explorateur Windows, celui-ci remplace l'opération de déplacement par l'enchaînement `Copie + Suppression de la source`. Dans ce cas, le dossier "déplacé" se verra appliquer la sécurité du dossier destination.

6.7.9 Interdiction d'accéder à un fichier chiffré si le certificat est révoqué

Stormshield Data Team permet l'interdiction d'accéder à un fichier chiffré à un utilisateur dont le certificat de la clé de chiffrement est révoqué.

Dans ce cas :

- toute opération sur les fichiers sécurisés par Stormshield Data Team (ouverture, création, renommage, déplacement et suppression) est refusée.

Ces opérations échouent même si le fichier est chiffré avec une ancienne clé de chiffrement de l'utilisateur.

- toute opération sur les règles Team est impossible. Les interfaces utilisateurs sont grisées et permettent uniquement la consultation des paramètres des règles.

Stormshield Data Team utilise la configuration du contrôleur de révocation définie au niveau du compte de l'utilisateur. Veillez en particulier :

- à ne pas autoriser l'utilisateur à désactiver le contrôle de révocation ;
- à configurer correctement la règle de téléchargement des listes de révocation.

Reportez-vous à la section Section [Team] pour paramétrer cette interdiction.

Une info-bulle s'affiche au premier accès à un fichier chiffré après la connexion (1 seule fois par connexion) pour avertir l'utilisateur que son certificat de chiffrement ne lui permet pas d'accéder aux fichiers chiffrés :

IMPORTANT
La vérification de la révocation du certificat ne représente pas un moyen sûr d'interdire l'accès à un fichier. En effet, cette vérification ne remplace pas le transchiffrement des fichiers en enlevant le collaborateur qui ne doit plus y avoir accès. Il faut donc la considérer comme un moyen temporaire.

Il est également important que le compte Stormshield Data Security de l'utilisateur soit paramétré correctement pour interdire la création d'une nouvelle clé de chiffrement ou l'utilisation d'un autre certificat.

6.7.10 Modification des dates de derniers accès

Certaines solutions (comme les solutions d'archivages) se basent sur les dates de derniers accès de fichiers pour effectuer leurs traitements. Toutefois, lorsque Stormshield Data Team est installé sur un poste, la date de dernier accès d'un fichier est modifiée lors d'un parcours de répertoire.

Le paramètre `AccessTimeAction` permet de maîtriser la restauration des dates de dernier accès sur les fichiers et de supprimer ainsi la modification de la date de dernier accès des ouvertures de fichiers par Stormshield Data Team.

Emplacement :	**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SBoxTeamDrv\Parameters**
Clé :	`AccessTimeAction (DWORD)`
Valeurs :	• `0x00000000` : pas de tentative de restauration de la date d'accès (valeur par défaut) ; • `0x00000001` : restauration optimisée de la date d'accès sur les systèmes de fichiers standards ; • `0x00000002` : restauration de la date d'accès sur les systèmes de fichiers NFS ; • `0x00000008` : restauration de la date d'accès sur les systèmes de fichiers standards. Cette option permet la compatibilité avec les systèmes de fichiers "vus comme standards" tels que NAS EMC. En règle générale, la valeur par défaut (0) est préconisée. Néanmoins, lors de l'utilisation d'une solution d'archivage basée sur un NAS EMC, la valeur `0x00000008` est préconisée. **NOTE** La valeur `0x8` fonctionne aussi sur les FS standards, mais avec une pénalité de performance. Elle peut être utile sur d'autres serveurs CIFS non usuels.

Référez-vous également au paramètre `OverlayIconAccuracy` qui permet de ne pas changer les dates d'accès aux fichiers (valeur : `0x00000020`).

6.7.11 Utilisation du cache en réseau

Lors d'une utilisation du cache en réseau, les fichiers et répertoires mais également les règles, peuvent être changées hors du contrôle du système de fichiers local de l'utilisateur. Si une modification est effectuée par un utilisateur sur le réseau, les autres postes qui utilisent le partage peuvent avoir pendant un certain temps des entrées de cache incorrectes et donc des statuts incorrects dans l'explorateur Windows. En conséquence, les nouveaux états ne seront pas pris en compte immédiatement.

Pour limiter ces incohérences, vous pouvez prendre les mesures suivantes :

- Sécurisez un dossier dès sa création lorsqu'il est encore vide ;
- Prévenez les utilisateurs pour qu'ils évitent de se servir du partage au moment critique ;
- Evitez de détruire un dossier puis de le recréer avec le même nom et des caractéristiques différentes. Si cette opération doit être effectuée, laissez passer entre les deux opérations le temps nécessaire à la mise à jour des caches (délai de 15 minutes ou redémarrage de la machine de l'utilisateur pour prise en compte instantanée) ;
- Effectuez les opérations conséquentes sur une arborescence de fichiers (sécurisation/désécurisation) à des heures où pas ou peu d'utilisateurs sont connectés (par exemple pendant la pause déjeuner ou en fin de journée).

L'ajout ou la suppression de collaborateurs à une règle existante ne pose pas de problème particulier et il n'y a donc pas de précaution à prendre.

6.8 Mise à jour automatique de compte sur LDAPS

Il est possible d'effectuer une mise à jour de compte automatique par fichier USX depuis un serveur LDAP avec connexion SSL (LDAPS). Pour que la connexion SSL soit mise en œuvre par Stormshield Data Security, il faut :

- Soit que le protocole indiqué dans l'URL soit ldaps://;
- Soit que le port utilisé soit le port 636.

6.9 Prise de traces d'exécution

En cas de problèmes rencontrés lors de l'utilisation du produit, Stormshield Data Security possède un système de prise de traces. Il permet ainsi de fournir au Technical Assistance Center Stormshield Data Security des informations utiles à l'analyse des problèmes. Ces traces sont activables « à chaud », c'est-à-dire sans redémarrer la machine, ni la session Windows.

6.9.1 Fonctionnement de la prise de traces

Pour activer la prise de traces Stormshield Data Security, vous pouvez sélectionner le dossier Stormshield Data Security dans le menu **Démarrer** de Windows ou bien double-cliquer sur un fichier portant l'extension *.sbdiag* et fourni par le Technical Assistance Center Stormshield Data Security.

Lors d'une session de trace, les éléments suivants sont enregistrés dans le dossier **C:/ProgramData/Arkoon/Security BOX/Traces** :

- Les traces Stormshield Data Security produites (fichier *Trace.etl*) ;
- Les événements Stormshield Data Security (fichier *audits.evtx*) : la génération de ce fichier est paramétrable dans l'interface ou dans le fichier d'extension *.sbdiag*. L'activation des journaux d'événements est nécessaire. Pour activer les journaux, reportez-vous à la section Journalisation des événements ;
- Une empreinte de la machine (fichier *sbdiag.xml*) : informations sur le système et sur l'installation de Stormshield Data Security et de la suite Office ;
- Une trace PSR (Problem Steps Recorder) : cet outil, livré avec les systèmes d'exploitation Windows à partir de Windows 7, permet de visualiser les actions effectuées lors de la reproduction d'un problème sur la machine. La génération de ce fichier est paramétrable dans l'interface ou dans le fichier d'extension *.sbdiag*.

6.9.2 Utilisation du système de traces

Depuis un fichier *.sbdiag*

1. Double-cliquez sur le fichier *.sbdiag* fourni par le Technical Assistance Center Stormshield Data Security pour démarrer l'interface de prise de traces en mode préconfiguré.
2. Cliquez sur le bouton **Démarrer la session de trace**.
3. Attendez que le message **Session de trace en cours** s'affiche.
4. Reproduisez la séquence d'actions à tracer.
5. Une fois la reproduction terminée, cliquez sur le bouton **Arrêter la session de trace**.
6. Dans la fenêtre suivante, ajoutez si besoin des commentaires à l'attention du Technical Assistance Center Stormshield Data Security. Donnez des informations supplémentaires sur la méthode de reproduction, des repères temporels, des noms de fichiers, etc.
7. Patientez jusqu'à ce que le dossier contenant la session de trace s'ouvre. Le fichier zip *Trace <horodatage>.zip* doit être envoyé au Technical Assistance Center Stormshield Data Security.

En mode préconfiguré, les paramètres ne sont pas modifiables.

Depuis l'interface de prise de traces

Si vous ne possédez pas de fichier *.sbdiag* ou si vous souhaitez personnaliser la session de trace, sélectionnez l'élément **Prise de traces** dans le menu Windows **Démarrer/Stormshield Data Security**:

1. Pour démarrer la session, ouvrez la boîte de dialogue des paramètres en cliquant sur l'icône de l'engrenage.
2. Il est recommandé de cocher les deux options du panneau supérieur des paramètres. L'activation des journaux d'événements est nécessaire pour l'extraction des événements Stormshield Data Security.

> **NOTE**
> L'outil PSR (Problem Steps Recorder) peut enregistrer des captures d'écran lors de la prise de traces.

3. Sélectionnez le module Kernel et le module impacté par la prise de traces uniquement.
4. Après avoir cliqué sur **OK** dans cette boite de dialogue, un fichier d'extension *.sbdiag* est automatiquement créé et la session de trace peut être démarrée comme décrit dans la section ci-dessus.

Annexe A. Liste des journaux de Stormshield Data Security

A.1. Administration

Installation de la Suite Stormshield Data Security

Numéro	Type	Description
300	Information	L'installation de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5 • Société : %6
301	Information	La modification de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5
302	Information	La désinstallation de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5
303	Information	L'installation du patch de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : - • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5 • Société : %6
304	Information	La modification du patch de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : - • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5
305	Information	La désinstallation du patch de la suite Stormshield Data Security s'est effectuée avec succès. Les paramètres de configuration sont les suivants : - • Version : %2 (%3) • Version de Patch : %4 • Répertoire d'installation : %5
306	Erreur	Le setup deStormshield Data Security s'est interrompu de façon inattendue.

Numéro	Type	Description
307	Erreur	Le setup de Stormshield Data Security a été arrêté avant qu'il ne se termine correctement.
308	Erreur	La politique de groupe définit l'envoi des événements vers le serveur '%2', mais l'utilisation de cette adresse échoue avec le code d'erreur %3 : "%4". Veuillez contacter votre administrateur.
1925	Erreur	Vous ne disposez pas de privilèges suffisants pour exécuter cette installation pour tous les utilisateurs de cet ordinateur. Ouvrez une session en tant qu'administrateur, puis réessayez d'exécuter cette installation.

Administration de l'annuaire

Numéro	Type	Description
700	Information	La mise à jour automatique de l'annuaire s'est effectuée avec succès.
701	Erreur	La mise à jour automatique de l'annuaire a échoué.
702	Information	La mise à jour manuelle de l'annuaire s'est effectuée avec succès.
703	Erreur	La mise à jour de l'annuaire a échoué.
704	Information	La mise à jour de l'annuaire à la connexion s'est effectuée avec succès.
705	Erreur	La mise à jour de l'annuaire à la connexion a échoué.
706	Information	La mise à jour de l'annuaire après déverrouillage s'est effectuée avec succès.
707	Erreur	La mise à jour de l'annuaire après déverrouillage a échoué.
708	Information	L'exportation de %4 certificat(s) de l'annuaire au format '%3' a été réalisée avec succès dans le fichier '%2'.
709	Erreur	L'exportation de %4 certificat(s) de l'annuaire au format '%3' dans le fichier '%2' a échoué.
710	Information	L'importation de %2 certificat(s) dans l'annuaire a été réalisée avec succès.
711	Erreur	L'importation de %2 certificat(s) dans l'annuaire a échoué.
712	Information	Option COMPATIBILITY_MODE : Valeur: %2 Acces %3
713	Information	Option ALLOW_MANUAL_UPDATE : Valeur : %2 Acces %3
714	Information	Option DISABLE_CHECK_ON_DISPLAY: Valeur: %2 Acces %3
715	Information	Option ACTIVATE : Valeur: %2 Acces %3
716	Information	Option ALLOW_DOWNLOAD_CRL : Valeur: %2 Acces %3
717	Information	Option REPLACE_FROM_LDAP : Valeur: %2 Acces %3
718	Information	Option START_ON_CONNECTION : Valeur: %2 Acces %3
719	Information	Option REPLACE_FROM_LDAP_OUTOFDATE_CERT : Valeur: %2 Acces %3
720	Information	Option REPLACE_FROM_LDAP_REVOKEDCERT : Valeur: %2 Acces %3

Numéro	Type	Description
721	Information	Option DELETE_IF_OUTOFDATE : Valeur: %2 Acces %3
722	Information	Option DELETE_IF_REVOKE : Valeur: %2 Acces %3
723	Information	Option DELETE_IF_NOT_ON_LDAP : Valeur: %2 Acces %3
724	Information	Option SB_EVT_ADMINISTRATION_INFO_REPLACE_ON_VALID_CERT : Valeur: %2 Acces %3
725	Information	Option TIMER : Valeur: %2 Acces %3
726	Information	Option COMMON_NAME_REPLACE : Valeur: %2 Acces %3
727	Information	Option COMMON_NAME_OUT_OF_DATE : Valeur: %2 Acces %3
728	Information	Option COMMON_NAME_REVOKE : Valeur: %2 Acces %3
729	Information	Option COMMON_NAME_NOT_ON_LDAP: Valeur: %2 Acces %3
730	Avertissement	La mise à jour LDAP du certificat dont l'e-mail est '%2' n'a pas été effectuée car la liste de révocation n'est pas disponible.

Administration de la liste de révocation

Numéro	Type	Description
1100	Information	La mise à jour de la liste de révocation %2 a été effectuée avec succès.
1101	Erreur	La mise à jour de la liste de révocation %2 a échoué.
1102	Information	La mise à jour de la liste de révocation %2 à partir du cache a été effectuée avec succès.
1103	Erreur	La mise à jour automatique de la liste de révocation %2 à partir du cache a échoué.

A.2. Virtual Disk

Gestion des volumes

Numéro	Type	Description
8300	Information	Le montage du volume automatique '%2' sur '%3' en mode '%4' s'est déroulé avec succès.
8301	Erreur	Le montage du volume automatique '%2' sur '%3' en mode '%4' a échoué.
8302	Information	Le volume '%2' a été monté avec succès sur '%3' en mode '%4'.
8303	Erreur	Le montage du volume '%2' sur '%3' en mode '%4' a échoué.
8304	Information	Le démontage du volume automatique '%2' monté sur '%3' a été un succès.
8305	Erreur	Le démontage du volume automatique '%2' monté sur '%3' a échoué.

Numéro	Type	Description
8306	Information	Le volume '%2' monté sur '%3' a été démonté avec succès.
8307	Erreur	Le démontage du volume '%2' monté sur '%3' a échoué.
8308	Information	Le volume '%2' monté sur '%3' a été verrouillé avec succès.
8309	Erreur	Le verrouillage du volume '%2' monté sur '%3' a échoué.
8310	Information	Le volume '%2' monté sur '%3' a été déverrouillé avec succès.
8311	Erreur	Le déverrouillage du volume '%2' monté sur '%3' a échoué.
8312	Information	Le volume '%2' a été créé avec succès.
8313	Erreur	La création du volume '%2' a échoué.
8314	Information	Le volume '%2' a été ajouté avec succès à la liste des volumes automatiques. Il sera monté sur '%3'.
8315	Erreur	L'ajout du volume '%2' à la liste des volumes automatiques a échoué.
8316	Information	Le volume '%2' monté sur '%3' a été supprimé avec succès de la liste des volumes automatiques.
8317	Erreur	La suppression du volume '%2' (monté sur '%3') de la liste des volumes automatiques a échoué.

A.3. File

Chiffrement / Déchiffrement vers

Numéro	Type	Description
18300	Information	L'utilisateur a chiffré avec succès le fichier '%2' en mode auto-déchiffrable.
18301	Erreur	Le chiffrement du fichier '%2' en mode auto-déchiffrable a échoué.
18302	Information	L'utilisateur a chiffré avec succès le dossier '%2' en mode auto-déchiffrable.
18303	Erreur	Le chiffrement du dossier '%2' en mode auto-déchiffrable a échoué.
18304	Information	L'utilisateur a chiffré avec succès le fichier '%2' en utilisant SecurityBOX SmartFile.
18305	Erreur	Le chiffrement du fichier '%2' en utilisant SecurityBOX SmartFile a échoué.
18306	Information	L'utilisateur a chiffré avec succès le dossier '%2' en utilisant SecurityBOX SmartFile.
18307	Erreur	Le chiffrement du dossier '%2' en utilisant SecurityBOX SmartFile a échoué.
18308	Information	L'utilisateur a chiffré avec succès le fichier '%2' pour les correspondants suivants : %3.
18309	Erreur	Le chiffrement du fichier '%2' pour les correspondants suivants a échoué : %3.

Numéro	Type	Description
18310	Information	L'utilisateur a chiffré avec succès le dossier '%2' pour les correspondants suivants : %3.
18311	Erreur	Le chiffrement du dossier '%2' pour les correspondants suivants a échoué : %3.
18312	Information	Les collaborateurs suivants ont été ajoutés avec succès au fichier '%2' : %r%3.
18313	Erreur	L'ajout des collaborateurs suivants au fichier '%2' a échoué : %r%3.
18314	Information	Les collaborateurs suivants ont été supprimés avec succès du fichier '%2' : %r%3.
18315	Erreur	La suppression des collaborateurs suivants du fichier '%2' a échoué : %r%3.

Chiffrement / Déchiffrement

Numéro	Type	Description
18700	Information	L'utilisateur a chiffré le fichier '%2' avec succès.
18701	Erreur	Le chiffrement du fichier '%2' a échoué.
18702	Information	L'utilisateur a déchiffré le fichier '%2' avec succès.
18703	Erreur	Le déchiffrement du fichier '%2' a échoué.

A.4. Kernel

Démarrage / Arrêt

Numéro	Type	Description
25300	Information	Le démarrage du kernel a été effectué avec succès.
25301	Erreur	Le démarrage du kernel a échoué.
25302	Information	L'arrêt du kernel a été effectué avec succès.
25303	Erreur	L'arrêt du kernel a échoué.
25304	Erreur	La valeur du paramètre %2 présent dans *SBox.ini* est invalide. %3 Veuillez contacter votre administrateur.
25305	Erreur	La valeur du paramètre %2 n'a pas été saisie dans *SBox.ini*. %3 Veuillez contacter votre administrateur.

Authentification LDAPS

Numéro	Type	Description
25700	Avertissement	Avertissement de sécurité SSL : certificat serveur invalide. Délivré à : %2 Délivré par : %3 Valide du %4 au %5. Veuillez contacter votre administrateur.

Numéro	Type	Description
25701	Erreur	Erreur de sécurité SSL : certificat serveur invalide. Délivré à : %2 Délivré par : %3 Valide du %4 au %5. Veuillez contacter votre administrateur.
25702	Erreur	Toutes les méthodes d'authentification soumises au serveur LDAP %2 ont échoué.
25703	Information	L'utilisateur est authentifié auprès du serveur LDAP %2 avec la méthode : %3.

Sélection du composant cryptographique

Numéro	Type	Description
26100	Information	L'utilisateur a sélectionné le middleware '%2'.

A.5. Keystore

Connexion / Déconnexion

Numéro	Type	Description
31300	Information	L'utilisateur s'est connecté à son porte-clé Stormshield Data Security.
31301	Erreur	La connexion au porte-clé Stormshield Data Security a échoué.
31302	Information	L'utilisateur s'est déconnecté de son porte-clé Stormshield Data Security.
31303	Erreur	L'utilisateur n'a pas pu se déconnecter de son porte-clé Stormshield Data Security.
31304	Information	La session Stormshield Data Security de l'utilisateur a été verrouillée.
31305	Erreur	Le verrouillage de la session Stormshield Data Security de l'utilisateur a échoué.
31306	Information	Le déverrouillage de la session Stormshield Data Security de l'utilisateur s'est déroulé normalement.
31307	Erreur	Le déverrouillage de la session Stormshield Data Security de l'utilisateur a échoué.
31308	Avertissement	Un utilisateur est déjà connecté à Stormshield Data Security dans une autre session Windows.
31309	Avertissement	Le code secret saisi est incorrect.
31310	Avertissement	L'identifiant '%2' ne correspond à aucun compte Stormshield Data Security.
31311	Avertissement	La session Stormshield Data Security ne peut pas être déverrouillée car la carte présente dans le lecteur n'est pas la bonne carte.
31312	Erreur	Le compte Stormshield Data Security ou la carte est bloqué.
31313	Information	La carte a été retirée du lecteur.
31314	Erreur	La carte est bloquée.

Numéro	Type	Description
31315	Erreur	Impossible de notifier un composant.
31316	Erreur	Impossible de charger un composant: '%2'.

Administration de compte

Numéro	Type	Description
31700	Information	Le compte a été créé avec succès
31701	Avertissement	L'installation du compte Stormshield Data Security a rencontré une erreur non bloquante.
31702	Erreur	L'installation du compte Stormshield Data Security a échoué.
31703	Information	La désinstallation du compte Stormshield Data Security s'est terminée normalement.
31704	Erreur	La désinstallation du compte Stormshield Data Security a échoué.
31705	Information	La politique de sécurité a été mise à jour.
31706	Erreur	La mise à jour de la politique de sécurité a échoué avec l'erreur suivante : %2.
31707	Information	L'export du compte Stormshield Data Security s'est terminé normalement.
31708	Erreur	L'export du compte Stormshield Data Security a échoué.
31709	Information	Le changement du code secret associé au compte s'est terminé normalement.
31710	Erreur	Le changement du code secret associé au compte a échoué.
31711	Erreur	Le nombre d'erreurs dans le changement du code secret associé au compte a dépassé la limite autorisée.
31712	Erreur	Impossible de créer un nouveau compte Stormshield Data Security parce que la carte est bloquée.
31713	Avertissement	Le code secret saisi est incorrect.
31714	Erreur	Le contenu de la carte ne permet pas la création de compte automatique.
31715	Erreur	Impossible de créer un nouveau compte Stormshield Data Security parce que le modèle est bloqué.
31716	Erreur	Impossible de créer un nouveau compte Stormshield Data Security parce que le modèle est inaccessible.
31717	Information	Un nouveau signataire des politiques de sécurité a été défini.
31718	Avertissement	La mise à jour de la politique de sécurité n'a pas été prise en compte parce que le nouveau signataire a été rejeté par l'utilisateur.
31719	Information	Téléchargement de la politique de sécurité depuis '%2'.
31720	Avertissement	Erreur de téléchargement de la politique de sécurité depuis '%2'.

Numéro	Type	Description
31721	Information	La mise à jour de la politique de sécurité n'a pas été prise en compte parce que le compte est à jour.
31722	Erreur	La mise à jour de la politique de sécurité n'a pas été prise en compte parce que la signature du fichier est incorrecte.
31723	Erreur	La mise à jour de la politique de sécurité n'a pas été prise en compte pour la raison suivante : '%2'.
31724	Avertissement	La mise à jour de la politique de sécurité a été prise en compte malgré l'avertissement : %2.
31725	Erreur	Le paramètre 'MasterPolicies' interdit la copie du fichier '%2'.
31726	Erreur	Création automatique de compte carte %2 : %3.

Administration des clés

Numéro	Type	Description
32100	Information	L'exportation de la clé de chiffrement par l'utilisateur s'est terminée normalement.
32101	Erreur	L'exportation de la clé de chiffrement par l'utilisateur a échoué.
32102	Information	Le renouvellement de la clé de chiffrement par l'utilisateur s'est terminé normalement.
32103	Erreur	Le renouvellement de la clé de chiffrement par l'utilisateur a échoué.
32104	Information	L'exportation de la clé de signature par l'utilisateur s'est terminée normalement.
32105	Erreur	L'exportation de la clé de signature par l'utilisateur a échoué.
32106	Information	Le renouvellement de la clé de signature par l'utilisateur s'est terminé normalement.
32107	Erreur	Le renouvellement de la clé de signature par l'utilisateur a échoué.
32108	Information	L'exportation de la clé par l'utilisateur s'est terminée normalement.
32109	Erreur	L'exportation de la clé par l'utilisateur a échoué.
32110	Information	Le renouvellement de la clé par l'utilisateur s'est terminé normalement.
32111	Erreur	Le renouvellement de la clé par l'utilisateur a échoué.
32112	Information	L'exportation du certificat de la clé de chiffrement par l'utilisateur s'est terminée normalement.
32113	Erreur	L'exportation du certificat de la clé de chiffrement par l'utilisateur a échoué.
32114	Information	L'exportation du certificat de la clé de signature par l'utilisateur s'est terminée normalement.
32115	Erreur	L'exportation du certificat de la clé de signature par l'utilisateur a échoué.

Numéro	Type	Description
32116	Information	L'exportation du certificat de la clé par l'utilisateur s'est terminée normalement.
32117	Erreur	L'exportation du certificat de la clé par l'utilisateur a échoué.
32118	Information	Un certificat pour la %2 n'a pas été importé dans le compte de l'utilisateur car il était périmé.
32119	Information	Un certificat pour la %2 n'a pas été importé dans le compte de l'utilisateur car ses usages étaient insuffisants.

Administration du porte-clés

Numéro	Type	Description
32500	Information	La clé de déchiffrement a été importée avec succès.
32501	Erreur	L'import de la clé de déchiffrement a échoué.
32502	Information	La clé de recouvrement a été importée avec succès.
32503	Erreur	L'import de la clé de recouvrement a échoué.

A.6. Mail

Envoi/Réception

Numéro	Type	Description
39312	Information	Le certificat de l'utilisateur '%2' n'a pas été trouvé dans l'annuaire de confiance.
39313	Information	Le certificat de l'utilisateur '%2' est révoqué.
39314	Information	Le certificat de l'utilisateur '%2' n'est plus valide.
39315	Information	La chaîne de parenté de l'utilisateur '%2' est révoquée.
39316	Information	La chaîne de parenté de l'utilisateur '%2' n'est plus valide.
39317	Information	La liste de révocation du certificat de l'utilisateur '%2' n'est pas disponible.
39318	Avertissement	L'utilisateur a reçu un mail chiffré mais ne possède pas la clé de déchiffrement.
39319	Avertissement	L'utilisateur a reçu un message dont la signature est incorrecte. Le message a été signé avec le certificat '%2'.
39320	Information	L'envoi d'un e-mail signé a été effectué avec succès (Destinataire(s): %2).
39321	Information	L'envoi d'un e-mail chiffré a été effectué avec succès (Destinataire(s): %2).
39322	Information	L'envoi d'un e-mail signé et chiffré a été effectué avec succès (Destinataire(s): %2).

Transchiffrement

Numéro	Type	Description
39700	Information	L'utilisateur a lancé le transchiffrement sur le dossier '%2'.
39701	Avertissement	Le transchiffrement des messages a rencontré des problèmes.

Désactivation de la sécurité

Numéro	Type	Description
40100	Information	La sécurité des messages du dossier '%2' a été désactivée.
40101	Information	La sécurité de certains messages a été désactivée (quantité: %2).
40102	Avertissement	La désactivation de la sécurité des messages a rencontré des problèmes.

Administration

Numéro	Type	Description
40500	Information	Le module Stormshield Data Mail est chargé avec succès dans Outlook '%2'.
40501	Information	Le module Stormshield Data Mail est désactivé dans Outlook '%2'.
40502	Information	L'exception suivante a été levée dans le module Stormshield Data Mail : '%2'.
40503	Avertissement	La clé de registre suivante, nécessaire au bon fonctionnement de l'add-in Stormshield Data Mail Édition Outlook, a été modifiée : '%2'.

A.7. Shredder

Numéro	Type	Description
46300	Information	L'opération de broyage a été initiée avec succès.
46301	Erreur	Echec de démarrage de l'opération de broyage.
46302	Information	L'opération de broyage a été terminée avec succès.
46303	Erreur	L'opération de broyage a échoué.
46304	Information	La suppression du fichier '%2' a été effectuée avec succès.
46305	Erreur	La suppression du fichier '%2' a échoué.
46306	Information	La suppression du dossier '%2' a été effectuée avec succès.
46307	Erreur	La suppression du dossier '%2' a échoué.
46308	Information	Le vidage sécurisé de la corbeille a été effectué avec succès.
46309	Erreur	Le vidage sécurisé de la corbeille a échoué.
46310	Information	Le nettoyage de la liste des fichiers a été effectué avec succès.

Numéro	Type	Description
46311	Erreur	Le nettoyage de la liste des fichiers a échoué.

A.8. Sign

Signature

Numéro	Type	Description
47300	Information	Le fichier '%2' a été signé avec succès.
47301	Erreur	La signature du fichier '%2' a échoué.
47302	Information	Le fichier '%2' a été co-signé avec succès.
47303	Erreur	La co-signature du fichier '%2' a échoué.
47304	Information	Le fichier '%2' a été contre-signé avec succès.
47305	Erreur	La contre-signature du fichier '%2' a échoué.
47306	Information	Le fichier '%2' a été sur-signé avec succès.
47307	Erreur	La sur-signature du fichier '%2' a échoué.
47308	Erreur	Le fichier '%2' est corrompu.

A.9. Team

Gestion des règles

Numéro	Type	Description
49300	Information	Une règle de sécurité a été définie sur le dossier '%2'.
49301	Erreur	Une tentative de sécurisation du dossier '%2' a échoué.
49302	Information	Le dossier '%2' a été remis en clair (non sécurisé).
49303	Erreur	Une tentative de désécurisation du dossier '%2' a échoué.
49304	Information	Les collaborateurs suivants ont été ajoutés avec succès dans la règle du dossier '%2' :%r%3.
49305	Erreur	L'ajout des collaborateurs suivants pour la règle du dossier '%2' a échoué :%r%3.
49306	Information	Les collaborateurs suivants ont été supprimés avec succès de la règle du dossier '%2' :%r%3.
49307	Erreur	La suppression des collaborateurs suivants de la règle du dossier '%2' a échoué : %r%3.
49308	Information	Les propriétaires suivants ont été ajoutés avec succès à la règle du dossier '%2' : %r%3.

Numéro	Type	Description
49309	Erreur	L'ajout de propriétaires pour la règle du dossier '%2' a échoué : %r%3.
49310	Information	Les propriétaires suivants ont été supprimés avec succès de la règle du dossier '%2' : %r%3.
49311	Erreur	La suppression de propriétaires de la règle du dossier '%2' a échoué : %r%3.
49312	Information	Le dossier '%2' a été configuré avec succès en dossier sécurisé (profil).
49313	Erreur	Une tentative de sécurisation du dossier '%2' a échoué (profil).
49314	Information	Le dossier '%2' a été configuré avec succès en dossier non sécurisé (profil).
49315	Erreur	Une tentative de désécurisation du dossier '%2' a échoué (profil).
49316	Information	La règle du dossier '%2' a été modifiée avec succès (profil).
49317	Erreur	La modification de la règle du dossier '%2' a échoué (profil).
49318	Information	Les collaborateurs suivants ont été ajoutés avec succès dans la règle du dossier '%2' (profil) :%r%3.
49319	Erreur	L'ajout des collaborateurs suivants pour la règle du dossier '%2' a échoué (profil) :%r%3.
49320	Information	Les collaborateurs suivants ont été supprimés avec succès de la règle du dossier '%2' (profil) :%r%3.
49321	Erreur	La suppression des collaborateurs suivants de la règle du dossier '%2' a échoué (profil) : %r%3.
49322	Avertissement	La mise à jour du fichier de règles (*.ust*) du dossier '%2' a échoué : en-tête inconsistant.
49323	Avertissement	L'utilisateur ne fait pas partie des utilisateurs autorisés pour la règle sur '%2'.
49324	Avertissement	L'utilisateur accède aux propriétés de la règle sur '%2' alors que son certificat est révoqué.
49325	Information	La règle de sécurité du dossier '%2' a été sauvegardée dans le compte de l'utilisateur.
49326	Avertissement	Le certificat de '%2' n'a pas été trouvé.
49327	Information	Le certificat de '%2' est invalide et a été ignoré.
49328	Information	Le certificat de '%2' est invalide, l'opération de chiffrement a été arrêtée par l'utilisateur.
49329	Avertissement	Le certificat de '%2' n'a pas pu être entièrement vérifié et a été utilisé.
49330	Information	Le certificat de '%2' n'a pas pu être entièrement vérifié et a été ignoré.
49331	Avertissement	Le certificat de '%2' est non valide et révoqué, et a été supprimé de la règle.
49332	Information	La règle de sécurité du dossier '%2' a été restaurée depuis le compte de l'utilisateur.
49333	Avertissement	Suspicion d'attaque : la règle de sécurité du dossier '%2' a été remplacée.

Numéro	Type	Description
49334	Information	La règle de sécurité du dossier '%2' a disparu.
49335	Avertissement	Un collaborateur illégitime a été détecté et ignoré dans la règle de sécurité du dossier '%2'.
49336	Information	La règle de sécurité du dossier '%2' a été restaurée depuis la règle locale.
49342	Avertissement	Impossible de vérifier la chaîne de parenté ou la liste de révocation.

Mise à jour des règles Team

Numéro	Type	Description
49337	Avertissement	Le nouveau certificat du collaborateur '%2' n'a pas été trouvé. Ce dernier ne fait plus partie de la règle.
49338	Avertissement	La règle connue sur le dossier '%2' n'est pas à jour. La mise à jour automatique n'a pas pu être effectuée.
49339	Avertissement	Le dossier '%2' sur lequel s'applique la règle est introuvable ou n'est plus sécurisé.
49340	Erreur	La clé de chiffrement du collaborateur '%2' n'a pas été trouvée.
49341	Avertissement	Le collaborateur '%2' n'a pas été trouvé dans la règle.

Chiffrement/Déchiffrement

Numéro	Type	Description
49700	Information	L'utilisateur a sorti le fichier '%2' d'une zone sécurisée avec succès.
49701	Erreur	La sortie du fichier '%2' d'une zone sécurisée a échoué.
49702	Information	L'utilisateur a sorti le dossier '%2' d'une zone sécurisée avec succès.
49703	Erreur	La sortie du dossier '%2' d'une zone sécurisée a échoué.
49704	Information	L'utilisateur a sécurisé le fichier '%2' selon les règles définies.
49705	Erreur	La sécurisation du fichier '%2' selon les règles définies a échoué.
49706	Information	L'utilisateur a sécurisé le dossier '%2' selon les règles définies.
49707	Erreur	La sécurisation du dossier '%2' selon les règles définies a échoué.
49708	Information	L'utilisateur a désécurisé le fichier '%2' avec succès.
49709	Erreur	La désécurisation du fichier '%2' a échoué.
49710	Information	L'utilisateur a désécurisé le dossier '%2' avec succès.
49711	Erreur	La désécurisation du dossier '%2' a échoué.
49712	Information	La sécurisation a été annulée.
49713	Information	La désécurisation a été annulée.

Numéro	Type	Description
49714	Erreur	Impossible de mettre en conformité le dossier '%2' : vous n'avez pas les autorisations Windows.
49715	Avertissement	Impossible de mettre en conformité le dossier caché '%2' : vous n'avez pas les autorisations Windows.

Sauvegarde/Restauration

Numéro	Type	Description
50100	Information	La sauvegarde du fichier '%2' est terminée.
50101	Erreur	La sauvegarde du fichier '%2' a échoué.
50102	Information	La sauvegarde du dossier '%2' est terminée.
50103	Erreur	La sauvegarde du dossier '%2' a échoué.
50104	Information	La restauration du fichier '%2' est terminée.
50105	Erreur	La restauration du fichier '%2' a échoué.
50106	Information	La restauration du dossier '%2' est terminée.
50107	Erreur	La restauration du dossier '%2' a échoué.
50108	Information	La sauvegarde a été annulée.
50109	Information	La restauration a été annulée.
50110	Erreur	Impossible de sauvegarder dans le dossier '%2' : vous n'avez pas les autorisations Windows.
50111	Erreur	Impossible de restaurer dans le dossier '%2' : vous n'avez pas les autorisations Windows.

Driver

Numéro	Type	Description
50500	Avertissement	Le fichier '%2' ne peut pas être ouvert par '%3'.
50501	Erreur	Délai dépassé lors de la tentative d'ouverture du fichier '%2' par '%3'.
50502	Erreur	La demande au service Team a échoué : '%2' par '%3'.

Annexe B. Procédure de migration d'un parc Security BOX Suite 8.0.x et 9.x vers la version Stormshield Data Security 10.1.1

Il est important de respecter la procédure suivante car les paramètres des sections [DirectoryUpdate], [File] et [Team], auparavant inclus dans le fichier *SBox.ini* (avant la version 8.0.2), se configurent désormais dans le compte utilisateur. Si cette procédure n'est pas respectée, ces paramètres pourraient être ignorés.

Pour effectuer la migration vers la version Stormshield Data Security 10.1.1 :

1. Procédez à la mise à jour de Security BOX Authority Manager vers Stormshield Data Authority Manager 10.1.1 en suivant la procédure indiquée dans le guide de Stormshield Data Authority Manager.
2. Configurez les nouveaux paramètres des sections [Directory], [File] et [Team] du modèle dans l'application Stormshield Data Authority Manager.
3. Procédez à la mise à jour de Security BOX Suite vers Stormshield Data Security 10.1.1 sur les postes clients.

Pour les versions strictement inférieures à 8.0.1, la désinstallation de cette version est nécessaire avant d'installer la version 10.1.1.

4. Diffusez le fichier *.usx* du modèle depuis Stormshield Data Authority Manager.

NOTE
Entre les étapes 3 et 4 de la procédure de migration, les paramètres migrés ne sont plus pris en compte par Stormshield Data Security car ils ne sont plus lus dans le fichier *SBox.ini* et ne sont pas encore présents dans les paramètres du compte. Il est donc important d'effectuer ces deux étapes aussi rapprochées dans le temps que possible.

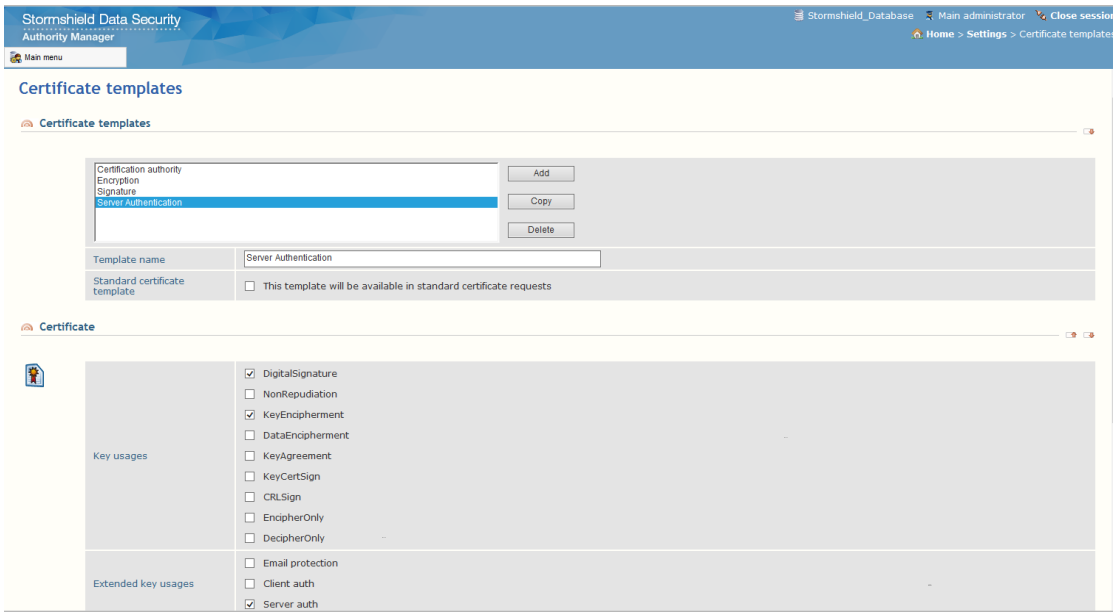
Annexe C. Configuration LDAPS

La procédure ci-dessous s'applique aussi bien à Stormshield Data Security qu'à Stormshield Data Authority Manager, lorsque le protocole LDAPS est activé sur le serveur LDAP.

C.1. Création des certificats pour l'authentification via Stormshield Data Authority Manager

Afin d'utiliser le protocole LDAPS avec des certificats nécessitant des autorités de certification externes au serveur Active Directory, il faut générer des certificats avec des utilisations étendues depuis l'interface d'administration Stormshield Data Authority Manager. Pour plus d'informations sur Stormshield Data Authority Manager, référez-vous à son guide d'utilisation.

1. Une fois connecté à Stormshield Data Authority Manager, sélectionnez la section **Paramètres**, puis **Modèles de certificats**.
2. Ajoutez un nouveau modèle que vous nommez "Authentification Serveur".
3. Sélectionnez les usages **DigitalSignature**, **KeyEncipherment** et **Server auth**.



4. Ajoutez un autre modèle de certificat nommé "Authentification Client" et sélectionnez les usages **DigitalSignature**, **KeyEncipherment** et **Client auth**.
5. Rendez vous ensuite dans la section **Gestion des utilisateurs>Utilisateurs>Création d'utilisateurs>Création avancée** afin de créer deux utilisateurs.
6. Pour le premier utilisateur, dans le champ **Nom**, entrez le nom DNS du serveur LDAP et laissez le champ **Prénom** vide. Dans la section **Clés et certificats**, sélectionnez **Authentification Serveur** dans le champ **Clé 1**. Laissez le champ **Clé 2** vide.
7. Pour le second utilisateur, répétez l'étape précédente mais sélectionnez **Authentification Client** dans le champ **Clé 1**. Le certificat associé à cet utilisateur sera destiné aux postes clients équipés de Stormshield Data Security.
8. Exportez les clés générées pour ces deux utilisateurs.
9. Exportez les certificats de toute la parenté de ces utilisateurs depuis la section **Autorité de certification**.

C.2. Ajout des clés et certificats d'autorité dans le magasin de certificats Windows

En mode d'authentification LDAPS, le serveur présente son certificat au client afin que ce dernier puisse le valider. Stormshield Data Security et Stormshield Data Authority Manager utilisent le magasin de certificats intégré à Windows pour vérifier la parenté du certificat du serveur.

La procédure suivante décrit comment importer les clés et certificats de la chaîne de parenté dans le magasin Windows. Cette procédure est à exécuter sur :

- le serveur Active Directory
- le serveur Stormshield Data Authority Manager
- les postes clients équipés de Stormshield Data Security.

1. Ouvrez le programme Microsoft Management Console (MMC), de préférence en tant qu'administrateur (tapez *mmc.exe* dans le menu Windows **Démarrer/Exécuter**).
2. Sélectionnez le menu **Fichier**, puis **Ajouter/Supprimer un composant logiciel enfichable** (raccourci : Ctrl+M).
3. Dans la colonne de gauche, sélectionnez **Certificats** puis cliquez sur **Ajouter**.
4. La fenêtre **Composant logiciel enfichable** s'ouvre :

- Pour le serveur Active Directory :
  - Choisissez **Un compte de service**, puis cliquez sur **Suivant**.
  - Choisissez **L'ordinateur local (...)**, puis cliquez sur **Suivant**.
  - Choisissez **Services de domaine Active Directory**, puis cliquez sur **Terminer**.
- Pour le serveur Active Directory et le serveur Stormshield Data Authority Manager :
  - Choisissez **Un compte d'ordinateur**, puis cliquez sur **Suivant**.
  - Choisissez **L'ordinateur local (...)**, puis cliquez sur **Terminer**.
- Pour les postes clients équipés de Stormshield Data Security :
  - Choisissez **Mon compte d'utilisateur**, puis cliquez sur **Terminer**.

5. Déroulez le contenu de **Certificats (ordinateur local)** ou **Certificats – Utilisateur actuel**.
6. Importez le certificat d'autorité racine associé aux certificats LDAP dans le magasin **Autorités de certification racines de confiance**.
7. Importez les autres certificats d'autorité parents dans **Autorités de certification intermédiaires**.
8. Importez la clé de serveur Stormshield Data Authority Manager précédemment sauvegardée dans le magasin personnel de certificats de l'ordinateur local du serveur Authority Manager.
9. Importez la clé du poste client Stormshield Data Security précédemment sauvegardée dans le magasin personnel de certificats du poste de travail.
10. Importez la clé du serveur Active Directory précédemment sauvegardée dans le magasin personnel de certificats du serveur Active Directory.
11. En quittant MMC, sélectionnez **Non** pour répondre à la demande d'enregistrement des paramètres de la console.

NOTE
Pour Stormshield Data Security, il est également possible d'ajouter les certificats dans le magasin de l'ordinateur local. La procédure de vérification du certificat du serveur cherche de façon transparente dans le magasin de l'utilisateur courant puis dans celui de l'ordinateur local le cas échéant.

C.3. Configuration du protocole SSL pour Stormshield Data Security

Une fois que les clés et certificats ont été renseignés sur les postes et les serveurs, il est possible de configurer Stormshield Data Security et Stormshield Data Authority Manager pour l'utilisation du protocole SSL :

1. Dans Stormshield Data Authority Manager, dans la section **Paramètres > Synchronisation LDAP**, activez la case **SSL**.
2. Dans la section **Gestion des utilisateurs > Modèles > Composants > Stormshield Data Kernel > Annuaire > Annuaires LDAP**, remplacez 389 par 636 dans le champ **Port** afin que l'annuaire Stormshield Data Security utilise ce port qui activera le LDAPS over TLS.

Annexe D. Informations à fournir pour signaler un problème

En cas de problème sur un poste, il faut indiquer au Technical Assistance Center Stormshield Data Security l'environnement précis installé sur le poste :

- la version + la langue de Stormshield Data Security ;
- le type de version installé : officielle, évaluation ;
- le numéro de licence Stormshield Data Security ;
- la liste des applications installées : Mail Édition XX, File, Virtual Disk, Shredder, Extension carte, etc. ;
- la version + le Service Pack (SP) éventuel + la langue de Windows ;
- la version + SP d'Internet Explorer installé ;
- si l'édition Outlook est concernée : la version + SP du client Outlook et du serveur Exchange ;
- si l'édition Notes est concernée : la version à 3 numéros (+ éventuellement une lettre) du client Notes et du serveur Domino.

documentation@stormshield.eu

Les images de ce document ne sont pas contractuelles, l'aspect des produits présentés peut éventuellement varier.

Copyright © Stormshield 2023. Tous droits réservés. Tous les autres produits et sociétés cités dans ce document sont des marques ou des marques déposées de leur détenteur respectif.