GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

GUIDE DE CONFIGURATION AVANCÉE

Version 11.3

Dernière mise à jour du document : 16 décembre 2024

Référence : sds-fr-sdse-guide_de_configuration_avancée-v11.3

Table des matières

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

1. Avant de commencer

Ce guide décrit l'utilisation de fichiers de configuration et de la base de registre Windows pour configurer les politiques de sécurité SDS Enterprise.

Les paramètres des politiques Stormshield Data Security Enterprise sont configurables de plusieurs façons :

- Dans la **console d'administration SDMC** accessible à l'adresse https://sds.stormshieldcs.eu/admin. Elle vous permet de créer et de configurer des politiques de sécurité via une interface graphique qui alimente un fichier de configuration *.json*. Pour plus d'informations, reportez-vous à la section *Gérer les politiques de sécurité dans SDMC* du Guide d'administration.
  Un certain nombre de paramètres avancés ne sont pas disponibles dans SDMC mais uniquement dans les différents fichiers de configuration ci-dessous.
- Directement dans les **fichiers de configuration *.json*** qui contiennent la grande majorité des paramètres de configuration des politiques de sécurité. Il existe un fichier par politique de sécurité. Pour plus d'informations, reportez-vous à la section Configurer une politique de sécurité dans un fichier .json.
  Tous les paramètres présents dans la console d'administration SDMC sont aussi configurables dans le fichier *.json*.
- Dans un **fichier de configuration *SBox.ini*** qui contient uniquement quelques paramètres avancés. Pour plus d'informations, reportez-vous à la section Configurer les paramètres avancés dans le fichier SBox.ini.
- Dans la base de registre Windows pour la fonctionnalité Stormshield Data Team. Pour plus d'informations, reportez-vous à la section Configurer les paramètres avancés dans la base de registre.

2. Configurer une politique de sécurité dans un fichier *.json*

1. Créez et configurez une politique de sécurité dans la console d'administration SDMC. Cela génère un fichier au format JSON du nom la politique de sécurité, par exemple *politiquedéfaut.json*.
   Pour plus d'informations, reportez-vous à la section *Gérer les politiques de sécurité dans SDMC* du Guide d'administration.
2. Téléchargez ce fichier.
   Pour plus d'informations, reportez-vous à la section *Installer les agents SDS Enterprise sur les postes des utilisateurs* du Guide d'administration.
3. Éditez le fichier *.json* et modifiez ses paramètres manuellement. Le fichier est divisé en plusieurs sections qui correspondent chacune à une fonctionnalité SDS Enterprise. Au sein de ces sections se trouvent les différents paramètres.
   Les tableaux ci-après contiennent la description des paramètres classés par fonctionnalité. La présence des paramètres dans le fichier est obligatoire, sauf indication contraire. Les tableaux mentionnent également si le paramètre existe dans la console d'administration SDMC et où le trouver.

2.1 Compte

La configuration de comptes utilisateurs est effectuée dans la section *accountPolicy* du fichier *.json*, elle-même divisée en plusieurs sous-sections : *parameters*, *creation* et *recovery*.

2.1.1 parameters

Les paramètres de fonctionnement des comptes utilisateurs sont configurés dans la section *parameters* décrite dans le tableau ci-dessous. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques** > **Comptes** > **Paramètres**.

Pour plus d'informations, reportez-vous à la section *Définir les paramètres génériques des comptes* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
cryptography	Indique comment sont effectuées les opérations cryptographiques au cours de l'utilisation du compte. Ce paramètre affecte toutes les fonctionnalités de SDS Enterprise, sauf Data Disk.		Chiffrement et signature
	encryptionAlgorithm : Algorithme à utiliser lors des opérations de chiffrement.	AES-256	Algorithme de chiffrement
	hashAlgorithm : Algorithme à utiliser lors des opérations de signature.	SHA-256, SHA-512	Algorithme de signature

Paramètre	Description	Valeurs possibles	SDMC
	keyEncryptionMethod : Optionnel. Algorithme à utiliser lors du chiffrement des clés. Les valeurs sont : • "RSA-OAEP-SHA-256", valeur par défaut, • "RSA-OAEP-SHA-1", valeur de compatibilité pour d'anciennes cartes	RSA-OAEP-SHA-256, RSA-OAEP-SHA-1	N/A
cardAccount	Optionnel. Indique le fonctionnement des comptes carte à puce. Ce champ est présent uniquement si la politique autorise la connexion à des comptes carte à puce.		Comptes carte ou token USB
cardMiddlewares	Liste des middleware dont l'utilisation est rendue possible sur le poste de travail. Le middleware permet à SDS Enterprise de communiquer avec tous types de carte à puce ou token USB.		Middleware
	name : Nom affiché pour cette configuration de middleware.	Chaîne de caractères	
	dllname : Nom de la DLL contenant le middleware. La valeur est un chemin absolu vers la DLL sur le poste de l'utilisateur. Si la DLL se trouve dans un dossier de la variable Windows PATH, le nom de la DLL est suffisant.	Chaîne de caractères	
	disablePKCS11Label, disablePKCS11Extractable, disablePKCS11Modifiable et disablePKCS11ModulusBits : Paramètres contrôlant l'utilisation de divers attributs PKCS#11 lors de la communication avec les cartes à puce / tokens USB. Ils proviennent de la base de middleware connus sur SDMC, et sont renseignés afin d'accroître la compatibilité de l'agent avec les middleware de différents constructeurs. Il est contre-indiqué de modifier les valeurs fournies par défaut.	true, false	
	showAllSlots : Indique si la fenêtre "Informations" dans le configurateur de carte affiche des informations sur tous les slots logiques gérés par le middleware (true), ou seulement les slots avec une carte / token branché (false).	true, false	
cardFilter	Optionnel. Filtres à appliquer pour sélectionner le bon lecteur de carte à puce lors de l'affichage de la mire de connexion.		Filtrage de lecteurs de cartes

Paramètre	Description	Valeurs possibles	SDMC
	manufacturer : Chaîne à utiliser pour filtrer les lecteurs de carte à puce selon le nom de leur fabricant. Les caractères * et ? sont autorisés.	Chaîne de caractères	Nom du fabricant
	description : Chaîne à utiliser pour filtrer les lecteurs de carte à puce selon leur description.	Chaîne de caractères	Description
accountMode	Indique quel type de compte utilisateur peut être connecté. Les valeurs sont : • "password" pour le mode *mot de passe*. Les clés sont stockées dans le fichier keystore.usr et sont protégées par un mot de passe. • "smartcard" pour le mode *carte à puce*. Les clés sont stockées dans une carte à puce ou un token USB et protégées par un code PIN. • "SSO" pour le mode *single sign-on* où les clés du compte sont issues du keystore Windows. Ce mode ne requiert pas d'authentification. • "passwordAndSmartcard" pour les modes *mot de passe* et *carte à puce*.	password, smartcard, SSO, passwordAnd Smartcard	Type de compte

2.1.2 creation

Les paramètres de création des comptes utilisateurs sont configurés dans la section *creation* décrite dans le tableau ci-dessous. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques** > **Comptes** > **Création**.

Pour plus d'informations, reportez-vous à la section *Définir les paramètres de création de comptes* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
accountKeyMode	Indique le type de fonctionnement des comptes à la création des comptes. Ce paramètre n'affecte pas le fonctionnement des comptes existants. Les valeurs sont : • "singleKeyEncryption" pour un compte avec une clé de chiffrement, • "singleKeySignature" pour un compte avec une clé de signature, • "dualKey" pour un compte avec une clé de chiffrement et une clé de signature.	singleKey Encryption, singleKey Signature, dualKey	Gestion des clés
passwordAccountMethod	Indique s'il est possible de créer des comptes mot de passe et comment. Les valeurs sont : • "forbidden" pour interdire la création de comptes mot de passe, • "manual" pour autoriser l'utilisateur à créer un compte manuellement.	forbidden, manual	Paramètres généraux Comptes Mot de passe
cardAccountMethod	Indique s'il est possible de créer des comptes carte à puce ou token USB et comment. Les valeurs sont : • "forbidden" pour interdire la création de comptes carte ou token, • "manual" pour autoriser l'utilisateur à créer un compte manuellement, • "automatic" pour pouvoir lancer une création de compte automatique, • "manualAndAutomatic" pour combiner la création de compte manuelle et automatique.	forbidden, manual, automatic, manualAnd Automatic	Paramètres généraux Comptes Carte ou token USB
passwordAccount	Optionnel. Indique les paramètres de création des comptes mot de passe. Ce champ est absent si la création de comptes mot de passe est interdite.		Création des comptes mot de passe
passwordStrength	Indique la force du mot de passe choisi par l'utilisateur pour son nouveau compte.		Force du mot de passe

Paramètre	Description	Valeurs possibles	SDMC
	alphabeticCharMinCount : Nombre minimum de caractères alphabétiques que doit contenir le mot de passe de l'utilisateur.	Entier positif	Nombre minimum de caractères alphabétiques
	numericCharMinCount : Nombre minimum de caractères numériques que doit contenir le mot de passe de l'utilisateur.	Entier positif	Nombre minimum de caractères numériques
	specialCharMinCount : Nombre minimum de caractères spéciaux que doit contenir le mot de passe de l'utilisateur.	Entier positif	Nombre minimum de caractères spéciaux
	totalCharMinCount : Nombre minimum de caractères que doit contenir le mot de passe de l'utilisateur.	Entier positif	Nombre minimum de caractères
	allowedKeySources : Liste des sources parmi lesquelles l'utilisateur peut choisir les clés pour son compte. Les valeurs sont : • "p12File" pour que l'utilisateur sélectionne un fichier P12 dans lequel se trouvent des clés de son compte, • "selfSignedP12" pour que l'utilisateur demande à SDS Enterprisede lui générer des clés auto-certifiées pour son compte.	p12File, selfSignedP12	Importer des certificats .p12 Générer localement des certificats .p12
	selfSignedOptions : Optionnel. Paramètres spécifiques à la génération de clés auto-certifiées. Ce champ est absent si la création manuelle de comptes mot de passe ne permet pas d'utiliser des clés auto-certifiées.		Certificats auto-certifiés
	baseLifetimeYears : Validité des certificats en nombre d'années à leur création.	Entier positif	Période de validité des certificats auto-certifiés générés par SDS lors d'une création de compte

Paramètre	Description	Valeurs possibles	SDMC
	renewalPeriodYears : Validité des certificats en nombre d'années à leur renouvellement.	Entier positif	Période de validité des certificats auto-certifiés générés par SDS lors d'un renouvellement de clé
	keyType : Taille des clés générées par SDS Enterprise à la création du compte.	RSA-2048, RSA-4096	Taille de la clé
automatic	Optionnel. Paramètres concernant la création automatique de comptes. Ce champ peut être absent si la création automatique de comptes est interdite.		Filtrer les autorités lors de la création automatique
	encryptionKeyAuthorityId : Optionnel. Identifiant unique de l'autorité dont est issue les clés de chiffrement à utiliser pour créer le compte. Vous trouverez l'identifiant dans la liste des autorités dans la section certificateData du fichier *.json*.	Chaîne de caractères unique	Nom de l'autorité pour le déchiffrement
	signatureKeyAuthorityId : Optionnel. Identifiant unique de l'autorité dont est issue la clé de signature à utiliser pour créer le compte. Vous trouverez l'identifiant dans la liste des autorités dans la section certificateData du fichier *.json*.	Chaîne de caractères unique	Nom de l'autorité pour la signature

2.1.3 recovery

Les paramètres de recouvrement des comptes utilisateurs sont configurés dans la section *recovery* décrite dans le tableau ci-dessous. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques** > **Comptes** > **Recouvrement de données**.

Pour plus d'informations, reportez-vous à la section *Permettre le recouvrement de données* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
certificateIds	Identifiant unique du certificat de recouvrements à ajouter aux utilisateurs pour toute opération de chiffrement de l'Agent SDS Enterprise. Vous trouverez l'identifiant dans la liste des certificats dans la section certificateData du fichier *.json*.	Chaîne de caractères unique	Gestion des clés

2.2 Certificats de la politique

La liste des certificats utilisés dans la politique est spécifiée dans la section *certificateData* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Bibliothèque de certificats**.

Pour plus d'informations sur les certificats, reportez-vous à la section *Gérer les certificats des autorités de certification et les certificats de recouvrement dans SDMC* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
certificateData	Liste des certificats utilisés dans la politique.		
	id : Identifiant unique du certificat dans la politique. Il est utilisé dans d'autres sections du fichier *.json* pour identifier le certificat. Voir l'exemple ci-dessous.	Chaîne de caractères unique	N/A
	data : Valeur du certificat, encodée en base64.	Chaîne de caractères	N/A

Exemple d'une liste de deux certificats. Le premier représente le certificat de l'autorité émettrice des clés à utiliser pour une création de compte automatique.

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

L'ID du premier certificat "0123456789ab-cdef-0123-4567-89abcdef" est donc utilisé comme valeur des paramètres `encryptionKeyAuthorityId` et `signatureKeyAuthorityId` de la politique de création de compte automatique (section accountPolicy) :

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

2.3 Annuaires de la politique

La liste des annuaires LDAP utilisés dans la politique est spécifiée dans la section *ldapData* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Bibliothèque LDAP**.

Pour plus d'informations sur les certificats, reportez-vous à la section *Gérer les annuaires LDAP dans SDMC* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
id	Identifiant unique de l'annuaire LDAP dans la politique. Il est utilisé dans d'autres sections du fichier *.json* pour identifier l'annuaire.	Chaîne de caractères unique	N/A
configuration	Configuration de l'annuaire LDAP		
name	Nom de la configuration.	Chaîne de caractères	Nom du serveur
access	Paramètres de contact du serveur LDAP.		N/A
	address : Adresse du serveur.	Chaîne de caractères	Adresse
	port : Port à utiliser.	Entier entre 0 et 65536	Port de connexion
	protocol : Protocole à utiliser. Les valeurs sont : • "ldap" pour le protocole LDAP standard, • "ldaps" pour le protocole LDAP sécurisé, • "ldapsWithFallbackToLdap" pour tenter une connexion LDAP si la connexion LDAPS échoue.	ldap ldaps, ldapsWith Fallback ToLdap	Utiliser une connexion LDAPS Tenter une connexion LDAP en cas d'échec de connexion LDAPS
credentials	Identifiants de connexion.		Contrôle d'accès
	username : Nom d'utilisateur. La valeur "<Myself>" permet d'utiliser les identifiants de la session Windows.	Chaîne de caractères	Identifiant
	password : Mot de passe. La valeur "<Myself>" permet d'utiliser les identifiants de la session Windows.	Chaîne de caractères	Mot de passe
advanced	Paramètres de recherche.		Recherche
	base : Base d'une requête LDAP.	Chaîne de caractères	Base
	depth : Profondeur de la recherche. Les valeurs sont : • "minimum" pour effectuer la recherche au niveau immédiat dans l'arborescence, • "oneLevel" pour effectuer la recherche au niveau immédiat et sur un niveau inférieur seulement, • "maximum" pour effectuer la recherche de façon récursive dans l'arborescence.	mimimum, oneLevel, maximum	Profondeur

Paramètre	Description	Valeurs possibles	SDMC
	timeoutSeconds : Délai d'aboutissement de la requête avant abandon en secondes.	Entier positif >= 10	Délai avant abandon de la requête de connexion en secondes
searchAttributeNames	Noms à utiliser pour demander différents attributs lors de la recherche.		Nom des attributs de recherche
	emailAddress : Nom de l'attribut contenant l'adresse e-mail. La valeur par défaut est "mail".	Chaîne de caractères	Adresse e-mail
	commonName : Nom de l'attribut contenant le nom usuel. La valeur par défaut est "cn".	Chaîne de caractères	Nom usuel
	certificate : Nom de l'attribut contenant le certificat. La valeur par défaut est "usercertificate;binary".	Chaîne de caractères	Certificat

2.4 Stormshield Data File

La fonctionnalité Stormshield Data File est configurée dans la section *filePolicy* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Fonctionnalités > File**.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer Stormshield Data File* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
allowEncryptSmartFile	Indique si l'utilisateur est autorisé à créer des fichiers smartFILE.	true, false	Autoriser la création de fichiers smartFILE
allowEncryptionForRecipient	Indique si l'utilisateur est autorisé à chiffrer des fichiers pour lui-même ou pour un destinataire.	true, false	Autoriser le chiffrement de fichiers pour un destinataire
allowFileDecryption	Indique si l'utilisateur est autorisé à déchiffrer des fichiers.	true, false	Autoriser le déchiffrement de fichiers
allowFolderDecryption	Indique si l'utilisateur est autorisé à déchiffrer des dossiers.	true, false	Autoriser le déchiffrement de dossiers

Paramètre	Description	Valeurs possibles	SDMC
allowFolderEncryption	Indique si l'utilisateur est autorisé à chiffrer des dossiers.	true, false	Autoriser le chiffrement de dossiers
allowNetworkDecryption	Indique si l'utilisateur est autorisé à déchiffrer des fichiers réseau.	true, false	Autorise le déchiffrement de fichiers réseau
allowNetworkEncryption	Indique si l'utilisateur est autorisé à chiffrer des fichiers réseau.	true, false	Autorise le chiffrement de fichiers réseau
allowSelfDecryptableFilesCreation	Indique si l'utilisateur est autorisé à créer des fichiers auto-déchiffrables.	true, false	Autoriser la création de fichiers auto-déchiffrables
blockedExtensionsOnOpening	Types de fichiers qu'il faudra d'abord déchiffrer avant d'ouvrir.	Liste d'extensions sous le format *.ext*	N/A
confirmForEachFile	En cas de chiffrement de plusieurs fichiers, indique si une confirmation est requise pour chaque fichier.	true, false	Confirmer le chiffrement de chaque fichier
decryptionList	Spécifie des paramètres de la liste de déchiffrement automatique de fichiers. Pour utiliser cette liste, voir Section decryptionList.		Liste de déchiffrement
encryptHiddenFiles	Indique si les fichiers cachés doivent être chiffrés.	true, false	Chiffrer les fichiers cachés
encryptionList	Spécifie des paramètres de la liste de chiffrement automatique de fichiers. Pour utiliser cette liste, voir Section encryptionList.		Liste de chiffrement
exclusionList	Spécifie des paramètres de la liste d'exclusion. Pour utiliser cette liste, voir Section exclusionList.		Liste d'exclusion
fileFormat	Format du fichier chiffré.	sdsx, sbox	Format de chiffrement

Paramètre	Description	Valeurs possibles	SDMC
readOnlyFilesEncryption	Indique comment traiter les fichiers en lecture seule.	treatAsUsual, askConfirmation, doNotEncryptBut Notify, neitherEncryptNorNotify	Traiter normalement comme les autres fichiers, Demander une confirmation, Signaler mais ne pas chiffrer, Ne pas signaler et ne pas chiffrer
autoEncryptDecryptedFolder	Permet d'activer le chiffrement Windows automatique sur le répertoire temporaire de déchiffrement des fichiers *.sdsx* (répertoire C:\Users\[user]\AppData\LocalLow\Stormshield\Stormshield Data Security\Decrypted).	true, false	

2.4.1 Section decryptionList

Les fichiers inclus dans les listes de déchiffrement sont automatiquement déchiffrés à certains moments prédéfinis. Les paramètres suivants sont spécifiés dans la section *filePolicy.decryptionList* du fichier *.json*.

Paramètre	Description	Valeurs possibles	SDMC
askConfirmation	Indique si une confirmation est requise avant le déchiffrement automatique.	true, false	Demander une confirmation avant le déchiffrement automatique
displayReport	Indique si un compte-rendu doit être affiché après le déchiffrement automatique.	true, false	Afficher un compte-rendu après le déchiffrement automatique
files	Liste de fichiers à déchiffrer automatiquement.		Fichiers déchiffrés automatiquement

Paramètre	Description	Valeurs possibles	SDMC

	path : Chemin d'un fichier. Pour indiquer plusieurs fichiers, la liste "files" doit contenir plusieurs objets avec chacun une propriété "path" différente. Par exemple :
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		Chaîne de caractères	Chemin du fichier

folders	Liste de dossiers à déchiffrer automatiquement.		
	path : Chemin d'un dossier. Pour indiquer plusieurs dossiers, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	Chemin du dossier ou masque
	recursive : Indique si les sous-dossiers sont compris dans la liste de déchiffrement.	true, false	Inclure les sous-dossiers
masks	Liste de masques à déchiffrer automatiquement. Pour indiquer plusieurs masques, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files"		
	path : Chemin d'un masque. Pour indiquer plusieurs masques, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	Chemin du dossier ou masque
	recursive : Indique si les sous-dossiers sont compris dans la liste de déchiffrement.	true, false	Inclure les sous-dossiers
onConnection	Déchiffre la liste de fichiers à la connexion à SDS Enterprise .	true, false	Déchiffrer automatiquement à la connexion au compte SDS Enterprise
onScreenSaverOver	Déchiffre la liste de fichiers à l'arrêt de l'économiseur d'écran.	true, false	Déchiffrer automatiquement à l'arrêt de l'économiseur d'écran
onSessionUnlock	Déchiffre la liste de fichiers au déverrouillage de la session.	true, false	Déchiffrer automatiquement au déverrouillage de la session

2.4.2 Section encryptionList

Les fichiers inclus dans les listes chiffrement sont automatiquement chiffrés à des moments prédéfinis. Les paramètres suivants sont spécifiés dans la section *filePolicy.encryptionList* du fichier *.json*.

Paramètre	Description	Valeurs possibles	SDMC
askConfirmation	Indique si une confirmation est requise avant le chiffrement automatique.	true, false	Demander une confirmation avant le chiffrement automatique
displayReport	Indique si un compte-rendu doit être affiché après le chiffrement automatique.	true, false	Afficher un compte-rendu après le chiffrement automatique
files	Liste de fichiers à chiffrer automatiquement.		Fichiers chiffrés automatiquement

	path : Chemin d'un fichier. Pour indiquer plusieurs fichiers, la liste "files" doit contenir plusieurs objets avec chacun une propriété "path" différente. Par exemple :
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		Chaîne de caractères	Chemin du fichier

fixedTimesInSeconds	Liste d'horaires auxquels les fichiers sont chiffrées automatiquement. En nombre de secondes depuis 00:00. Par exemple 1h30 du matin est représenté par la valeur "5400".	Liste d'entiers positifs	N/A
folders	Liste de dossiers à chiffrer automatiquement.		
	path : Chemin d'un dossier. Pour indiquer plusieurs dossiers, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	Chemin du dossier
	recursive : Indique si les sous-dossiers sont compris dans la liste de chiffrement.	true, false	Inclure les sous-dossiers
intervalMinutes	Fréquence à laquelle les fichiers sont chiffrées automatiquement. En minutes.	Entier positif	Fréquence du chiffrement automatique
masks	Liste de masques à chiffrer automatiquement.		

Paramètre	Description	Valeurs possibles	SDMC
	path : Chemin d'un masque. Pour indiquer plusieurs masques, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	Chemin du dossier ou masque
	recursive : Indique si les sous-dossiers sont compris dans la liste de chiffrement.	true, false	Inclure les sous-dossiers
onDisconnection	Active la liste à la déconnexion de SDS Enterprise.	true, false	Chiffrer automatiquement à la déconnexion du compte SDS Enterprise
onScreenSaverStarted	Active la liste au démarrage de l'économiseur d'écran.	true, false	Chiffrer automatiquement au démarrage de l'économiseur d'écran
onSessionLock	Active la liste au verrouillage de la session SDS Enterprise.	true, false	Déchiffrer automatiquement au verrouillage de la session

2.4.3 Section exclusionList

Par l'intermédiaire d'une liste d'exclusion, vous pouvez exclure certains fichiers pour éviter qu'ils ne soient chiffrés par erreur. Les paramètres suivants sont spécifiés dans la section *filePolicy.exclusionList* du fichier *.json*.

Paramètre	Description	Valeurs possibles	SDMC
displayWarning	Indique si une fenêtre d'avertissement doit être affichée si une opération n'aboutit pas à cause de la liste d'exclusion.	true, false	Afficher un avertissement en cas de refus de chiffrement
files	Liste de fichiers à exclure du chiffrement.		Fichiers exclus du chiffrement
	askForConfirmation : Indique si une confirmation doit être demandée pour le chiffrement de fichiers exclus.	true, false	N/A

Paramètre	Description	Valeurs possibles	SDMC

	path : Chemin du fichier. Pour indiquer plusieurs fichiers, la liste "files" doit contenir plusieurs objets avec chacun une propriété "path" différente. Par exemple :
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		Chaîne de caractères	Chemin du fichier

folders	Liste de dossiers à exclure du chiffrement.		Dossiers ou masques exclus du chiffrement
	askForConfirmation : Indique si une confirmation doit être demandée pour le chiffrement de dossiers exclus.	true, false	N/A
	path : Chemin du dossier. Pour indiquer plusieurs dossiers, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	Chemin du fichier
	recursive : Indique si les sous-dossiers sont compris dans la liste d'exclusion.	true, false	Inclure les sous-dossiers
masks	Liste de masques à exclure du chiffrement.		Dossiers ou masques exclus du chiffrement
	askForConfirmation : Indique si une confirmation doit être demandée pour le chiffrement des fichiers exclus.	true, false	N/A
	path : Chemin du masque avec l'extension "*.ext" pour appliquer le masque. Pour indiquer plusieurs masques, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	Chemin du fichier
	recursive : Indique si les sous-dossiers sont compris dans la liste d'exclusion.	true, false	Inclure les sous-dossiers

2.5 Stormshield Data Team

La fonctionnalité Stormshield Data Team est configurée dans la section *teamPolicy* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Fonctionnalités > Team**.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer Stormshield Data Team* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
accessToEncryptedFile	Indique l'accessibilité à un fichier chiffré. Les valeurs sont : • "always" pour y accéder quel que soit l'état du certificat, • "notIfRevokedOrCrlExpired" pour refuser l'accès si la clé de chiffrement est révoquée ou la CRL indisponible, • "notIfCertificateHasAnIssue" pour refuser l'accès si le certificat a un avertissement ou une erreur.	always, notIfRevokedOrCrlExpired, notIfCertificateHasAnIssue	L'utilisateur peut accéder à un fichier chiffré quel que soit l'état de son certificat, L'utilisateur ne peut pas accéder à un fichier chiffré si le certificat de sa clé de chiffrement est révoqué ou lorsque la liste de révocation n'est pas disponible, L'utilisateur ne peut pas accéder à un fichier chiffré si son certificat présente un avertissement ou une erreur.
allowDecryption	Indique si le déchiffrement de fichiers est autorisé.	true, false	Autoriser le chiffrement
allowDeletion	Indique si la suppression de fichiers est autorisée.	true, false	Autoriser la suppression
allowEncryptionAccordingToDefinedRules	Indique si le chiffrement selon les règles définies est autorisé.	true, false	Autoriser le chiffrement selon les règles définies
allowSaveAndRestore	Indique si la sauvegarde et la restauration sont autorisées.	true, false	Autoriser la sauvegarde et la restauration

Paramètre	Description	Valeurs possibles	SDMC
closeReportWindow	Indique dans quel cas fermer la fenêtre de compte-rendu. Les valeurs sont : • "always" pour que la fenêtre se ferme après le chiffrement, • "ifNoWarning" pour que la fenêtre reste affichée en cas d'avertissement, • "never"pour que la fenêtre reste affichée après le chiffrement.	always, ifNoWarning, never	Fermeture de la fenêtre de compte-rendu
excludedFolders	Optionnel. Liste des dossiers à exclure. Cette liste est récursive.	Chaînes de caractères	N/A
openEncryptedFileInUnsecuredFolder	Définit le comportement lors de l'ouverture d'un fichier chiffré dans un dossier non sécurisé. Les valeurs sont : • "allow" pour l'autoriser, • "deny" pour l'interdire, • "readonly" pour l'autoriser en lecture seule uniquement.	allow, deny, readOnly	Ouverture de fichiers chiffrés dans un dossier non sécurisé
reencryptFilesWhenRemovingCoworkers	Indique si les fichiers sont re-chiffrés si l'on retire un collaborateur de la règle.	true, false	Chiffrer les fichiers de nouveau lorsqu'un collaborateur est supprimé d'une règle

Paramètre	Description	Valeurs possibles	SDMC
secureDragAndDrop	Définit le comportement lors d'une copie ou déplacement de dossiers/fichiers couverts par une règle Data Team vers un dossier non sécurisé. Les valeurs sont : • "keepCurrentRule" pour appliquer la règle du dossier de destination après déplacement ou copie, • "forbidden" pour interdire le déplacement ou la copie, • "noDecryption" pour ne pas déchiffrer le fichier après déplacement ou copie.	keepCurrentRule, forbidden, noDecryption	Déchiffrer pendant le déplacement ou la copie, Interdire le déplacement ou la copie, Conserver le chiffrement pendant le déplacement ou la copie
setCreationDateToCurrentDate	Indique si la date de création doit être la date du jour.	true, false	Indiquer la date du jour comme date de création
setModificationDateToCurrentDate	Indique si la date de modification doit être la date du jour.	true, false	Indiquer la date du jour comme date de modification
showCoworkers	Indique dans quel cas la règle est affichée. Les valeurs sont : • "always" pour que tous les utilisateurs puissent afficher la règle, • " onlyIfUserIsACoworker" pour que seuls les collaborateurs de la règle puissent afficher la règle.	always, onlyIfUserIsACoworker	Affichage des collaborateurs
showSuccessfullyProcessedFiles	Indique si les fichiers correctement chiffrés sont affichés dans la fenêtre de progression.	true, false	Voir les fichiers chiffrés dans la fenêtre de progression
updateCoworkerKeyInKnownRules	Indique si la clé du collaborateur est mise à jour dans les règles connues après un renouvellement de clé.	true, false	Mettre à jour la clé d'un collaborateur dans les règles connues si sa clé est renouvelée

Paramètre	Description	Valeurs possibles	SDMC
useLocalCertificateState	Indique si l'état du certificat local présent dans le cache doit être utilisé si la CRL ne peut être téléchargé, ou si elle a expiré.	true, false	Utiliser l'état du certificat local dans le cache si la liste de révocation ne peut pas être téléchargée ou si elle a expiré

2.6 Stormshield Data Disk

La fonctionnalité Stormshield Data Disk est configurée dans la section *diskPolicy* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Fonctionnalités > Disk**.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer Stormshield Data Disk* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
allocationUnitKB	Taille des clusters NTFS utilisés dans le disque virtuel.	0, 512, 1024, 4096	N/A
automaticCreation	Optionnel. Permet de créer automatiquement un volume pour un utilisateur se connectant pour la première fois.		
	autoMount : Permet ou non de monter automatiquement le volume à chaque connexion de l'utilisateur.	true, false	Monter automatiquement le volume lorsque l'utilisateur se connecte à SDS
	mountLetter : Lettre utilisée pour le disque monté. Si la lettre est indisponible, la première lettre disponible dans l'ordre alphabétique inverse est prise (en partant de Z).	lettre entre D et Z	Lettre du lecteur
	showFinalReport : Permet ou non d'afficher un rapport de fin.	true, false	Afficher un compte-rendu à la fin de la création
	sizeMB : Optionnel. Taille en Mo à allouer au volume à créer. Si cette valeur n'est pas renseignée, la taille sera 10% de la taille disponible sur le poste de travail client.	Entier positif	Taille du volume

Paramètre	Description	Valeurs possibles	SDMC
	vboxFullPath : Nom et emplacement du fichier spécial et chiffré .vbox sur lequel repose le volume.	Chemin	Chemin complet du fichier .vbox associé au volume
enableCompression	Indique si la compression du volume est autorisée.	true, false	N/A
enableQuickCreation	Indique si la création rapide est autorisée.	true, false	N/A
enableQuickFormat	Indique si le formatage rapide est autorisé.	true, false	N/A
enableRescueFileModification	Indique si la modification des fichiers de sauvegarde vboxsave est autorisée.	true, false	N/A
enableExpertMode	Indique si la modification des fichiers de sauvegarde vboxsave est autorisée dans le répertoire du vbox associé.	true, false	N/A
fileSystem	Système de fichier utilisé pour les volumes montés.	NTFS, FAT32, FAT	Système de fichiers
maxSizeMB	Taille maximale autorisée pour la création d'un volume en Mo.	Entier positif	Taille maximale autorisée
mountAsNonRemovable	Indique si le disque monté sera amovible ou non.	true, false	Monter les volumes en tant que disques non amovibles
volumeName	Nom donné aux volumes créés. Par défaut "SDSDiskVolume".	Chaîne	Nom des volumes
encryptionAlgorithm	Indique le mode de chiffrement utilisé pour le volume. Les valeurs sont : • "AES-256" pour le mode de chiffrement AES CBC (valeur par défaut), • "AES-XTS-256" pour le mode de chiffrement AES-XTS qui offre une meilleure protection des données et est recommandé par l'ANSSI.	[AES-256], AES-XTS-256	N/A

2.7 Stormshield Data Mail

La fonctionnalité Stormshield Data Mail est configurée dans la section *mailPolicy* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Fonctionnalités > Mail**.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer Stormshield Data Mail* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
enableSMime	Indique si l'envoi et la réception de messages chiffrés avec S/MIME sont autorisés. Ce paramètre n'a actuellement aucun effet et sera fonctionnel dans une version future.	true, false	N/A
enablePGP	Indique si l'envoi et la réception de messages chiffrés avec PGP sont autorisés.	true, false	Autoriser le chiffrement/déchiffrement des messages en PGP
encryptByDefault	Indique si le chiffrement doit être automatiquement activé lors de la composition de nouveaux messages.	true, false	Activer le chiffrement des messages par défaut
signByDefault	Indique si la signature doit être automatiquement activée lors de la composition de nouveaux messages.	true, false	Activer la signature des messages par défaut
signatureType	Type de signature à utiliser lors de la composition de messages signés.	clear, opaque	Type de signature pour signer les messages (S/MIME uniquement)
updateAddressBookWithSignedMailCertificates	Indique si le certificat de signature associé à l'adresse e-mail est importé dans l'annuaire de confiance de l'utilisateur, et si l'import est automatique ou effectué manuellement par l'utilisateur.		
	automatic Les valeurs sont : • "trustedAuthorities"pour importer les certificats dont l'émetteur est de confiance, • "no" pour ne pas importer de certificats.	trusted Authorities, no	Autoriser la mise à jour automatique de l'annuaire de confiance : • Uniquement pour les autorités connues • Non

Paramètre	Description	Valeurs possibles	SDMC
	manual Les valeurs sont : • "anyAuthority" pour autoriser l'import de certificats de toutes origines, • "trustedAuthorities"pour importer les certificats dont l'émetteur est de confiance, • "no" pour ne pas importer de certificats.	anyAuthority, trustedAuthorities, no	Autoriser la mise à jour manuelle de l'annuaire de confiance : • Pour toutes les autorités, • Uniquement pour les autorités connues, • Non
keepSignatureOnSecurityDeletion	Indique si la signature d'un message doit être conservée lorsque l'on désécurise ce dernier.	true, false	N/A
showOperationInProgressDialog	Indique si une fenêtre de chargement doit être affichée lorsqu'une opération dure plus de trois secondes.	true, false	N/A
sensitivityLabelsBehaviour	Optionnel. Lorsqu'un utilisateur envoie un message avec une étiquette de confidentialité Microsoft Purview Information Protection, SDS Enterprise vérifie la présence de l'étiquette dans cette liste et l'action de sécurisation associée à l'étiquette (en anglais, sensitivity labels).		Chiffrement et signature automatiques avec Microsoft Purview
	labelID : nom de l'étiquette tel que paramétré dans la console d'administration Microsoft Purview Information Protection.	chaîne de caractères	
	behaviour : configuration de sécurisation minimale à appliquer sur le message.	sign, encrypt, signAndEncrypt	

2.8 Stormshield Data Sign

La fonctionnalité Stormshield Data Sign est configurée dans la section *signPolicy* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Fonctionnalités > Sign**.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer Stormshield Data Sign* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
allowCoSigning	Indique si l'utilisateur est autorisé à co-signer des documents.	true, false	Autoriser la co-signature d'un fichier
allowCounterSigning	Indique si l'utilisateur est autorisé à contre-signer des documents.	true, false	Autoriser la contre-signature d'un fichier
allowOverSigning	Indique si l'utilisateur est autorisé à sur-signer des documents.	true, false	Autoriser la sur-signature d'un fichier
allowSigning	Indique si l'utilisateur est autorisé à signer des documents.	true, false	Autoriser la signature d'un fichier
allowSigningOnActiveContent	Indique si l'utilisateur est autorisé à signer des documents contenant du contenu actif.	true, false	Autoriser la signature de fichiers lorsque du contenu actif est détecté
defaultSignExtension	Extension de fichier par défaut pour les documents signés.	".p7f", ".p7m"	Extension de fichier par défaut
displayDocumentBeforeSigning	Indique si l'utilisateur est obligé de visualiser un document avant de le signer.	true, false	Toujours afficher le fichier avant de le signer
informUserAboutActiveContentInWordFiles	Indique si l'utilisateur doit être informé qu'un document Word contient du contenu actif avant de pouvoir le signer. Ce paramètre n'est pris en compte que pour les documents Microsoft Word 2000 ou supérieur.	true, false	Informer l'utilisateur de la présence de contenu actif dans le fichier Microsoft Word avant de signer
informUserAboutMacrosInPdfFiles	Indique si l'utilisateur doit être informé qu'un document PDF contient des macros avant de pouvoir le signer.	true, false	Informer l'utilisateur de la présence de macros dans le fichier PDF avant de signer
informUserAboutMacrosInWordFiles	Indique si l'utilisateur doit être informé qu'un document Word contient des macros avant de pouvoir le signer. Ce paramètre n'est pris en compte que pour les documents Microsoft Word 97 à 2003.	true, false	Informer l'utilisateur de la présence de macros dans le fichier Microsoft Word avant de signer
preselectMailToAskForSignature	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.	true, false	N/A

Paramètre	Description	Valeurs possibles	SDMC
preselectMailToNotifyCoWorkers	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.	true, false	N/A

2.9 Stormshield Data Shredder

La fonctionnalité Stormshield Data Shredder est configurée dans la section *shredderPolicy* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Fonctionnalités > Shredder**.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer Stormshield Data Shredder* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
addDesktopIcon	Indique si un raccourci Stormshield Data Shredder est ajouté sur le bureau Windows pour effectuer des glisser-déposer.	true, false	Ajouter un raccourci sur le bureau
allowBinShredding	Indique si l'utilisateur est autorisé à broyer des fichiers de la corbeille.	true, false	N/A
allowDragAndDropOnShredderIcon	Indique si l'utilisateur est autorisé à broyer des fichiers via un glisser-déposer sur l'icône du Shredder.	true, false	Activer le glisser-déplacer d'éléments sur l'icône de SD Shredder
allowFileShredding	Indique si l'utilisateur est autorisé à broyer des fichiers.	true, false	Autoriser le broyage de fichiers
allowFolderShredding	Indique si l'utilisateur est autorisé à broyer des dossiers.	true, false	Autoriser le broyage de dossiers
allowShreddingInterruption	Indique si l'utilisateur est autorisé à interrompre une opération de broyage.	true, false	Autoriser l'interruption d'une opération de broyage

Paramètre	Description	Valeurs possibles	SDMC
confirmForEachFile	En cas de broyage de plusieurs fichiers, indique si une confirmation de l'utilisateur est requise pour chaque fichier.	true, false	Confirmer pour chaque fichier Confirmer une fois pour tous les fichiers
exclusionList	Spécifie des paramètres de la liste d'exclusion. Pour utiliser cette liste, voir Section exclusionList.		N/A
readOnlyFilesShredding	Indique comment traiter les fichiers en lecture seule. Les valeurs sont : • "neitherShredNorNotify" pour ne pas broyer le fichier et ne pas informer l'utilisateur, • "doNotShredButNotify" pour ne pas broyer le fichier et informer l'utilisateur, • "askConfirmation" pour demander une confirmation avant de broyer, • "treatAsUsual" pour broyer selon les mêmes règles que les autres fichiers.	neitherShred NorNotify, doNotShred ButNotify, askConfirmation, treatAsUsual	Ne jamais broyer Signaler les fichiers Demander confirmation Traiter comme les autres fichiers
shredHiddenFiles	Indique si l'utilisateur est autorisé à broyer les fichiers cachés.	true, false	N/A
shreddingPatternBytes	Bits utilisés pour remplacer le contenu des fichiers broyés	Liste d'entiers positifs compris entre 0 et 255	N/A

2.9.1 Section exclusionList

Par l'intermédiaire d'une liste d'exclusion, vous pouvez exclure certains fichiers pour éviter qu'ils ne soient broyés par erreur. Les paramètres suivants sont spécifiés dans la section *shredderPolicy.exclusionList* du fichier *.json*. Cette liste est optionnelle.

Paramètre	Description	Valeurs possibles	SDMC
displayWarning	Indique si une fenêtre d'avertissement doit être affichée si une opération n'aboutit pas à cause de la liste d'exclusion.	true, false	N/A
files	Optionnel. Liste de fichiers à exclure du broyage.		N/A

Paramètre	Description	Valeurs possibles	SDMC
	askForConfirmation : Indique si une confirmation doit être demandée pour le broyage de fichiers exclus.	true, false	N/A
	path : Chemin d'un fichier. Pour indiquer plusieurs fichiers, la liste "files" doit contenir plusieurs objets avec chacun une propriété "path" différente. Par exemple : `"files": [ { "path": "path1" }, { "path": "path2" } ]`	Chaîne de caractères	N/A
folders	Optionnel. Liste de dossiers à exclure du broyage.		N/A
	askForConfirmation : Indique si une confirmation doit être demandée pour le broyage de dossiers exclus.	true, false	N/A
	path : Chemin d'un dossier. Pour indiquer plusieurs dossiers, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	N/A
	recursive : Indique si les sous-dossiers sont compris dans la liste d'exclusion.	true, false	N/A
masks	Optionnel. Liste de masques à exclure du broyage.		N/A
	askForConfirmation : Indique si une confirmation doit être demandée pour le broyage des fichiers exclus.	true, false	N/A
	path : Chemin du masque avec l'extention "*.ext" pour appliquer le masque. Pour indiquer plusieurs masques, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	N/A
	recursive : Indique si les sous-dossiers sont compris dans la liste d'exclusion.	true, false	N/A

2.9.2 Section shreddingList

Les fichiers inclus dans les listes de broyage sont automatiquement broyés à des moments prédéfinis. Les paramètres suivants sont spécifiés dans la section *shredderPolicy.shreddingList* du fichier *.json*.

Paramètre	Description	Valeurs possibles	SDMC
askConfirmation	Indique si une confirmation est requise avant le broyage automatique.	true, false	N/A
displayReport	Indique si un compte-rendu doit être affiché après le broyage automatique.	true, false	N/A
files	Optionnel. Liste de fichiers à broyer automatiquement.		N/A

	path : Chemin d'un fichier. Pour indiquer plusieurs fichiers , la liste "files" doit contenir plusieurs objets avec chacun une propriété "path" différente. Par exemple :
	`"files": [`
	`{`
	`"path": "path1"`
	`},`
	`{`
	`"path": "path2"`
	`}`
	`]`
		Chaîne de caractères	N/A

fixedTimesInSeconds	Liste d'horaires auxquels les fichiers sont broyés automatiquement. En nombre de secondes depuis 00:00. Par exemple 1h30 du matin est représenté par la valeur "5400"	Liste d'entiers positifs	N/A
folders	Optionnel. Liste de dossiers à broyer automatiquement		N/A
	path : Chemin d'un dossier. Pour indiquer plusieurs dossiers, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	N/A
	recursive : Indique si les sous-dossiers sont compris dans la liste de broyage.	true, false	N/A
intervalMinutes	Optionnel. Fréquence à laquelle les fichiers sont broyés automatiquement. En minutes.	Entier positif	N/A
masks	Optionnel. Liste de masques à broyer automatiquement.		N/A
	path : Chemin du masque avec l'extention "*.ext" pour appliquer le masque. Pour indiquer plusieurs masques, ce paramètre doit être utilisé plusieurs fois. Voir le paramètre "files".	Chaîne de caractères	N/A

Paramètre	Description	Valeurs possibles	SDMC
	recursive : Indique si les sous-dossiers sont compris dans la liste des éléments à broyer.	true, false	N/A
onDisconnection	Active le broyage automatique à la déconnexion de SDS Enterprise	true, false	N/A
onScreenSaverStarted	Active le broyage automatique au démarrage de l'économiseur d'écran.	true, false	N/A
onSessionLock	Active le broyage automatique au verrouillage de la session SDS Enterprise.	true, false	N/A

2.10 Stormshield Data Share

La fonctionnalité Stormshield Data Share est configurée dans la section *sharePolicy* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Fonctionnalités > Share**.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer Stormshield Data Share* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
• dropboxPolicy • oodrivePolicy • oneDrivePolicy • oneDriveForBusinessPolicy • sharepointPolicy	Indique comment SDS Enterprise doit protéger les espaces collaboratifs de type Dropbox, Oodrive, OneDrive, OneDrive for Business et SharePoint. Chacun de ces paramètres est un objet à part entière dont les propriétés individuelles sont détaillées dans les lignes ci-après.		• Dropbox • OneDrive • OneDrive for Business • SharePoint • OoDrive
	protect : Indique si l'espace synchronisé doit être protégé automatiquement.	true, false	Activer/désactiver le bouton
	subfoldersToProtect : Spécifie la liste des sous-dossiers à protéger dans l'espace collaboratif. Ne s'applique que si `"protect" : true`. Une liste vide signifie que la totalité de l'espace collaboratif est protégé. Exemples : • `[ "Documents" ]` • `[ "Folder1", "Folder2\\SubFolder" ]`	Liste de chaînes de caractères	Avancé

Paramètre	Description	Valeurs possibles	SDMC
ruleCreation	Optionnel. À la création d'une règle de protection automatique d'un dossier, permet de forcer la création d'une règle partagée ou locale ou de laisser le choix à l'utilisateur. Les valeurs possibles sont : • "forceSharedRule" pour toujours créer les règles de protection comme des règles partagées. • "forceLocalRule" pour toujours créer les règles de protection comme des règles locales. • "userChoice" pour permettre à l'utilisateur de choisir de partager ou non la règle.	forceSharedRule, forceLocalRule, userChoice	Toujours créer les règles de protection comme règles partagées Toujours créer les règles de protection comme règles non partagées Permettre de choisir le type de règles de protection lors de la création

2.11 Annuaires

Les annuaires à utiliser pour fournir les certificats des utilisateurs sont définis dans la section *directories* du fichier *.json*, elle-même divisée en plusieurs sous-sections : *ldap* et *pgp*.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer les annuaires d'entreprise* du Guide d'administration.

2.11.1 Section ldap

Les annuaires LDAP sont configurés dans la section *ldap* décrite dans le tableau ci-dessous. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques** > **Annuaires** > **LDAP**.

Paramètre	Description	Valeurs possibles	SDMC
addWildcardSuffixInFilter	Indique s'il faut suffixer les critères de recherche par "*".	true, false	Suffixer les critères de recherche par "*"
addWildcardPrefixInFilter	Indique s'il faut préfixer les critères de recherche par "*"	true, false	N/A
addUserCertificateBinaryFilter	Indique s'il faut ajouter "usercertificate;binary=*" au filtre de recherche, afin de retourner uniquement les entités LDAP disposant d'un certificat.	true, false	N/A

Paramètre	Description	Valeurs possibles	SDMC
ldapAddressBookList	Liste des identifiants uniques des annuaires LDAP accessibles pour les utilisateurs. Vous trouverez les identifiants dans la liste des annuaires LDAP dans la section ldapData du fichier *.json*.	Liste de chaînes de caractères uniques	Ajouter depuis la bibliothèque
automaticUpdate	Optionnel. Indique comment gérer la mise à jour automatique de l'annuaire de confiance et donc des certificats. La mise à jour automatique est appliquée seulement si tous les paramètres sont remplis.		Mettre à jour l'annuaire automatiquement
	downloadCrlsUponVerification : Indique s'il faut télécharger la CRL lors de la vérification du certificat.	true, false	N/A
	onPeriodicHours : Fréquence à laquelle la mise à jour est effectuée (en heures).	Entier positif entre 1 et 24	Fréquence de la mise à jour
	onUserConnection : Indique si la mise à jour démarre à la connexion de l'utilisateur.	true, false	Démarrer la mise à jour de l'annuaire lorsque l'utilisateur se connecte à son compte SDS
	updateValidCertificatesWithNewerOnes : Indique s'il faut mettre à jour les certificats valides avec des certificats plus récents.	true, false	Mettre à jour les certificats stockés dans l'annuaire de confiance à partir de certificats plus récents d'un annuaire LDAP
	updateOnlyFromCAs : Optionnel. Liste des identifiants uniques des autorités à partir desquelles appliquer la mise à jour. Vous trouverez les identifiants dans la liste des autorités dans la section certificateData du fichier *.json*. Si ce champ n'est pas renseigné, toutes les autorités sont prises en compte.	Liste de chaînes de caractères dont chacune correspond au champ "id" d'un objet dans la liste "certificateData" de la politique.	N/A
	expiredCertificates : Indique comment gérer la suppression des certificats expirés.		Suppression des certificats expirés
	updateWithNewerOnes : Indique s'il faut mettre à jour avec des certificats plus récents. Se base sur la liste fournie par le paramètre "updateOnlyFromCAs".	true, false	Mettre à jour les certificats expirés

Paramètre	Description	Valeurs possibles	SDMC
	removeFromLocalDirectory : Indique s'il faut supprimer le certificat de l'annuaire local.	true, false	Supprimer automatiquement
	removeOnlyFromCAs : Optionnel. Liste des identifiants uniques des autorités à partir desquelles appliquer la suppression. Vous trouverez les identifiants dans la liste des autorités dans la section certificateData du fichier *.json*. Si ce champ n'est pas renseigné, toutes les autorités sont prises en compte.	Liste de chaînes de caractères dont chacune correspond au champ "id" d'un objet dans la liste "certificateData" de la politique.	Sélection des CA émettrices des certificats à supprimer automatiquement lorsqu'ils expirent
	revokedCertificates : Indique comment gérer la suppression des certificats révoqués.		Suppression des certificats révoqués
	updateWithNewerOnes : Indique s'il faut mettre à jour avec des certificats plus récents. Se base sur la liste fournie par le paramètre "updateOnlyFromCAs".	true, false	Mettre à jour les certificats révoqués
	removeFromLocalDirectory : Indique s'il faut supprimer le certificat de l'annuaire local.	true, false	Supprimer automatiquement
	removeOnlyFromCAs : Optionnel. Liste des identifiants uniques des autorités à partir desquelles appliquer la suppression. Vous trouverez les identifiants dans la liste des autorités dans la section certificateData du fichier *.json*. Si ce champ n'est pas renseigné, toutes les autorités sont prises en compte.	Liste de chaînes de caractères dont chacune correspond au champ "id" d'un objet dans la liste "certificateData" de la politique.	Sélection des CA émettrices des certificats à supprimer automatiquement lorsqu'ils sont révoqués
	missingCertificates : Indique comment gérer la suppression des certificats absents. Les paramètres sont les mêmes que pour "expiredCertificates" (voir ci-dessus).		Suppression des certificats retirés de l'annuaire LDAP
	updateWithNewerOnes : Indique s'il faut mettre à jour avec des certificats plus récents. Se base sur la liste fournie par le paramètre "updateOnlyFromCAs".	true, false	Mettre à jour les certificats manquants lors de la recherche de collaborateurs
	removeFromLocalDirectory : Indique s'il faut supprimer le certificat de l'annuaire local.	true, false	Supprimer automatiquement

Paramètre	Description	Valeurs possibles	SDMC
	removeOnlyFromCAs : Optionnel. Liste des identifiants uniques des autorités à partir desquelles appliquer la suppression. Vous trouverez les identifiants dans la liste des autorités dans la section certificateData du fichier *.json*. Si ce champ n'est pas renseigné, toutes les autorités sont prises en compte.	Liste de chaînes de caractères	Sélection des CA émettrices des certificats à supprimer automatiquement lorsqu'ils sont retirés de l'annuaire LDAP

2.11.2 Section pgp

Les fichiers inclus dans les listes de déchiffrement sont automatiquement déchiffrés à certains moments prédéfinis. Les paramètres suivants sont spécifiés dans la section *directories.pgp* du fichier *.json*.

Paramètre	Description		SDMC
wkdServers	URLs paramétriques vers des serveurs hébergeant des clés publiques accessibles par le schéma WKD (Web Key Directory). Elles doivent être de la forme suivante, les parties en gras étant conservées telles quelles : • WKD "advanced" : **https://openpgpkey**.sous-domaines-optionnels.domaine.toplevel**/.well-known/openpgpkey/<d>/hu/<k>** ?parametres_get=optionnels • WKD "direct" : **https://**sous-domaines-optionnels.domaine.toplevel**/.well-known/openpgpkey/hu/<k>** ?parametres_get=optionnels	Liste de chaînes de caractères	Serveurs WKD

2.12 Révocation de certificats

La fonctionnalité de révocation est configurée dans la section *revocationPolicy* du fichier *.json*. Le tableau ci-dessous décrit ses paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Autorités**.

Pour plus d'informations sur la configuration de la fonctionnalité, reportez-vous à la section *Configurer le contrôle de révocation des certificats* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
checkCertificateRevocation	Optionnel. Indique s'il faut vérifier la révocation du certificat.	true, false	N/A

Paramètre	Description	Valeurs possibles	SDMC
displayWarningDBCorrupted	Affiche un message d'avertissement quand la base de données locale des CRL est corrompue.	true, false	N/A
displayWarningDBDeleted	Affiche un message d'avertissement quand la base de données locale des CRL est effacée.	true, false	N/A
fileTimeOutInSeconds	Temps maximum alloué pour le téléchargement de la CRL à partir d'un fichier en secondes.	Entier positif	N/A
httpTimeOutInSeconds	Temps maximum alloué pour le téléchargement de la CRL à partir d'un lien HTTP en secondes.	Entier positif	N/A
issuers	Liste des certificats d'autorité et de recouvrement à utiliser dans vos politiques.		
	certificateID : Identifiant unique du certificat dans la politique. Vous trouverez l'identifiant dans la liste des certificats dans la section certificateData du fichier *.json*.	Chaîne de caractères unique	
	crlDownloadFrequency : Fréquence de téléchargement de la CRL. Les valeurs sont : • "onFirstCryptoOperation" (valeur par défaut) lorsqu'un chiffrement ou déchiffrement est effectué pour la première fois, • "whenExpired" à l'expiration d'un certificat, • "always" à chaque utilisation d'un certificat, • "never" ne jamais télécharger la CRL.	OnFirst Crypto Operation, WhenExpired, Always, Never	N/A
	methods : Liste des méthodes de téléchargement de la CRL.		Ajouter depuis la bibliothèque
	type : Type de méthode de révocation.	"CRL" "OCSP"	N/A
	url : URL utilisée pour le téléchargement.	Chaîne de caractères	N/A
ldapTimeOutInSeconds	Temps maximum alloué pour le téléchargement de la CRL à partir d'un lien LDAP en secondes.	Entier positif	N/A
validityDurationInDays	Durée de validité de la CRL en jours.	Entier positif (max 365)	Durée de validité des listes de révocation

2.13 Points de distribution

Les points de distribution des politiques sont configurés dans la section *distributionPointPolicy* du fichier *.json*. Le tableau ci-dessous décrit leurs paramètres. Dans la console d'administration SDMC, les paramètres équivalents se trouvent dans le panneau **Politiques > Diffusion**.

Pour plus d'informations, reportez-vous à la section *Configurer les points de distribution des politiques* du Guide d'administration.

Paramètre	Description	Valeurs possibles	SDMC
urls	Liste des URL indiquant le ou les chemins complets du fichier des politiques *.jwt* de votre choix. SDS Enterprise vérifie la liste des points de distribution dans l'ordre que vous avez déterminé. Il applique la première politique valide qu'il rencontre. Les URL doivent être préfixées par http://, https://, ou file:// et séparées par des virgules. Par exemple : `"http://test.com/file.jwt", "file://10.1.1.1/file.jwt"`	Liste d'URL	Chemin complet du fichier de la politique

3. Configurer les paramètres avancés dans le fichier *SBox.ini*

Certains paramètres avancés sont gérés dans le fichier de configuration *SBox.ini* qui se trouve dans le dossier *Program Files\Arkoon\Security BOX\Kernel*.

Le fichier est divisé en plusieurs sections qui correspondent chacune à une fonctionnalité SDS Enterprise. Au sein de ces sections se trouvent les différents paramètres.

Les tableaux ci-après contiennent la description des paramètres classés par fonctionnalité. Lors de l'édition du fichier, veuillez respecter les conditions suivantes :

- Si une valeur optionnelle du fichier de configuration est invalide, la valeur par défaut est utilisée.
- 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.
- Après avoir modifié le fichier *SBox.ini*, il est recommandé de redémarrer l'ordinateur pour garantir que toutes les modifications seront bien prises en compte.

3.1 Paramétrage via les Group Policy Windows

Vous pouvez aussi définir les paramètres de configuration du fichier *SBox.ini* via les **Group Policy** (GPO) Windows, au niveau “Machine” ou au niveau “Utilisateur”.

> **NOTE**
> Stormshield recommande 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.

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*.

SDS Enterprise 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.

3.2 [Logon]

Paramètre	Description
AllowCard	Autorise une connexion à SDS Enterprise en mode carte à puce ou token USB : • 0 : Non autorisé (par défaut), • 1 : Autorisé.
ConnectOnCard	Affiche la fenêtre de connexion SDS Enterprise avec saisie du code secret sur insertion carte ou token : • 0 : Pas d'affichage (par défaut), • 1 : Affichage. La fenêtre ne s'affiche pas s'il existe déjà un compte SDS Enterprise connecté (mot de passe ou carte/token).
UnfreezeOnCard	Affiche la fenêtre de déverrouillage carte sur insertion carte ou token si la session SDS Enterprise de l'utilisateur est verrouillée : • 0 : Non, • 1 : Oui (par défaut). La fenêtre ne s'active que si l'utilisateur connecté utilise un compte SDS Enterprise en mode carte ou token.
RepairCardAccount	Permet de réparer une carte si seul le certificat est disponible, en renouvelant la clé à partir du CKA_ID connu dans le compte.
UpgradeEncipherCardAccount	Permet l'ajout automatique d'une clé de signature à un compte carte ou token mono-clé chiffrement.
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 SDS Enterprise 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`.
AllowLocalUnblock	Autorise un déblocage local si la session SDS Enterprise de l'utilisateur est bloquée : • 0 : non autorisé, • 1 : autorisé (par défaut).
AllowDistantUnblock	Autorise un déblocage distant si la session SDS Enterprise de l'utilisateur est bloquée : • 0 : non autorisé, • 1 : autorisé (par défaut).

Paramètre	Description
DontShowLicenceKey	Permet de ne pas afficher la valeur de la clé de licence dans la fenêtre **A propos de** SDS Enterprise : • 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.
SlotFilterOn	Si plusieurs lecteurs de carte ou tokens sont connectés au poste de travail (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 SDS Enterprise. Pour plus d'informations, reportez-vous à la section [SlotFilter]).
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.
ExternalCardAuthent	Permet d'activer la mire de connexion de SDS Enterprise 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)
GUILog	Permet d'interdire la saisie d'un mot de passe en ligne de commande au moment de la connexion et du déverrouillage de l'utilisateur par l'outil en ligne de commande *SBCMD.exe*. • 0 : Saisie du mot de passe autorisée, • 1 : Saisie du mot de passe interdite.

3.3 [UpgradeEncipherCardAccount_CertificateTemplate]

Paramètre	Description

[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>`

3.4 [SlotFilter]

Paramètre	Description
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.

Paramètre	Description
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.

3.5 [KeyRenewal]

Les sections [KeyRenewal] et [SBox.KeyRenewalWizardYYY] concernent le renouvellement de clés pour des comptes SDS Enterprise 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	Active ou désactive la fonctionnalité du choix de répertoire cible dans lequel est réalisé le déchiffrement. Les valeurs sont : • 0 : Désactivé (valeur par défaut), • 1 : Activé. Si la fonctionnalité est désactivée, les trois paramètres suivants ne seront pas pris en compte et le comportement adopté sera celui par défaut.
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 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

3.5.1 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.

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

Types de compte

Le tableau suivant liste les types de compte disponibles dans SDS 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.

3.6.1 Paramètres

Le tableau suivant décrit le contenu de chaque section en fonction du type de compte XXX :

Paramètre	KS	GP	Description
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 SDS Enterprise, 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*.
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.
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.
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.
ExportKeys		#	Si une clé n'a pas été tirée par la carte ou le token (si <InternalKeys> = 0), SDS Enterprise 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.

Paramètre	KS	GP	Description
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).
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.
AutomaticRenewFromCard			Pour [SBox.KeyRenewalWizardGP] Avec un compte Carte ou SSO, lorsque la nouvelle clé de chiffrement ou de signature est déjà dans la carte ou dans le Magasin de certificats Windows de l'utilisateur, cette option permet de renouveler automatiquement la clé quand la précédente expire : • 0 : pas de renouvellement automatique (par défaut) , • 1 : renouvellement automatique avec message de confirmation pour l'utilisateur, • 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.

3.7 [External PKCS11 Policy]

Paramètre	Description
CPLCanChangePKCS11	Permet ou non à l'utilisateur de modifier le type de carte ou token défini dans le **configurateur de l'extension carte**. • 0 : non, • 1 : oui (par défaut)

3.8 [File]

Paramètre	Description
ExeActivate	Active ou désactive la fonctionnalité du choix de répertoire cible dans lequel est réalisé le déchiffrement. Les valeurs sont : • 0 : Désactivé (valeur par défaut), • 1 : Activé. Si la fonctionnalité est désactivée, les trois paramètres suivants ne seront pas pris en compte et le comportement adopté sera celui par défaut.
ExeToCheck	Permet de configurer une liste d'exécutables pour lesquels SDS Enterprise doit contrôler les répertoires d'ouverture où sont déchiffrés les fichiers FILE. Si ce paramètre n'est pas présent, la fonctionnalité s'active alors pour tous les exécutables appelants. La syntaxe est la suivante : `ExeToCheck = nom_exe_1 [, nom_exe_n]`

ExeTargetDirectory	Spécifie le chemin du répertoire dans lequel s'effectue 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 : Dossier contenant les données d'applications de tous les utilisateurs, C:\Program Data.
	• COMMON_DOCUMENTS : Dossier contenant les fichiers communs à tous les utilisateurs, C:\Users\Public\Documents.
	• USERNAME : Nom d'utilisateur Windows.
	• LOCAL_APPDATA : Dossier contenant les données des applications locales, C:\Users\username\AppData\Local.
	• DESKTOP : Dossier contenant les fichiers sur le bureau, C:\Users\username\Desktop.
	• PROFILE : Dossier du profil de l'utilisateur, 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.

AllowOverwriteFile	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.

Paramètre	Description
AllowTransciphering WithDecipheredKeys	Autorise à transchiffrer avec une clé de déchiffrement. Les valeurs sont : • 0 : Valeur par défaut : transchiffrement avec une clé de déchiffrement non autorisé, • 1 : Transchiffrement avec une clé de déchiffrement autorisé.

3.9 [Team]

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

4. Configurer les paramètres avancés dans la base de registre

Certains paramètres avancés de SDS Enterprise doivent être configurés dans la base de registre Windows.

Pour modifier la base de registre :

1. Accédez à la base de registre en lançant **regedit.exe**.
2. Dans l'arborescence, atteignez la clé indiquée.
3. Modifiez la valeur de la clé.
4. Quittez la base de registre.
5. Redémarrez la machine.

4.1 Modifier les dates de dernier accès

Lorsque Stormshield Data Team est installé sur un poste de travail, la date de dernier accès d'un fichier est modifiée lors d'un parcours de répertoire. Le paramètre `AccessTimeAction` permet de restaurer la véritable date de dernier accès sur les fichiers.

Clé	`AccessTimeAction (DWORD)`
Emplacement	**HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SBoxTeamDrv\Parameters**
Valeurs	• `0x00000000` : La date d'accès modifiée par Stormshield Data Team est conservée (valeur par défaut), • `0x00000001` : La date d'accès est restaurée sur les systèmes de fichiers standard, • `0x00000002` : La date d'accès est restaurée sur les systèmes de fichiers NFS, • `0x00000008` : La date d'accès est restaurée sur les systèmes de fichiers standard avec une baisse potentielle de performances. Cette option permet la compatibilité avec les systèmes de fichiers "vus comme standard" tels que NAS EMC ou des serveurs CIFS non usuels. En règle générale, la valeur par défaut `0x00000000` est préconisée. Néanmoins, lors de l'utilisation d'une solution d'archivage basée sur un NAS EMC, la valeur `0x00000008` est préconisée.

4.2 Déplacer les 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 de la façon suivante :

Clé	`SkipFolderR(DWORD)`
Emplacement	**HKLM\SYSTEM\CURRENTCONTROLSET\Services\SBoxTeamDrv\Parameters**
Valeur	Ajouter le dossier contenant la base CSC.

4.3 Maintenir les 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 conserver les performances habituelles, il est possible d'appliquer les clés de registre suivantes :

4.3.1 Améliorer les performances lors du parcours d'arborescences chiffrées

Pour diminuer 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 », vous pouvez modifier la valeur du paramètre `OverlayIconAccuracy`.

Clé	`OverlayIconAccuracy (DWORD)`
Emplacement	**HKEY_LOCAL_MACHINE\SOFTWARE\ARKOON\Security BOX Enterprise\Properties\Team**
Valeur	• `0x40` : Diminue sensiblement le temps de détermination de l'état chiffré ou non d'un dossier en mode carte ou token.

4.3.2 Exclure les 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. Si la clé `SkipApp` n'existe pas, vous pouvez la créer en choisissant une valeur de type REG_MULTI_SZ.

Clé	`SkipApp (MULTI_SZ)`
Emplacement	**HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\SboxTeamDrv\Parameters**
Valeur	Ajouter un processus à exclure par ligne. Il est recommandé 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 Ainsi que les processus spécifiques Dell : HostStorageService.exe HostControlService.exe

4.3.3 Exclure des extensions et des 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 :

Clé	`Extensions (DWORD)`
Emplacement	**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions**
Valeur	Ajouter la liste des extensions à exclure. Il est recommadé d'exclure les extensions suivantes : *.box*, *.sbox*, *.sbt*, *.sdsx*, *.usi*, *.usr*.
Clé	`Processes (DWORD)`
Emplacement	**HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows Defender\Exclusions**
Valeur	Ajouter la liste des processus à exclure. Il est recommandé d'exclure les processus suivants : *SBDSRV*, *SBoxDiskSrv* ainsi que les processus des antivirus et autres EDR.

4.4 Désactiver la suggestion automatique de collaborateurs

Lors de la sélection des collaborateurs autorisés à accéder à un dossier sécurisé, les collaborateurs possédant les autorisations Windows sur le dossier concerné sont automatiquement suggérés dans un groupe qui s'appelle **Autorisations Windows**.

Vous pouvez désactiver cette fonctionnalité en créant la clé de registre suivante :

Clé	`SuggestCoworkersThroughACL (DWORD)`
Emplacement	**HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel**
Valeur	• 0

4.5 Configurer le filtre pour la recherche de collaborateurs dans l'annuaire LDAP

Lors de la sélection des collaborateurs autorisés à accéder à un dossier sécurisé, la recherche dans l'annuaire LDAP se base par défaut sur le nom commun (Common name).

Si le nom commun ne suffit pas, vous pouvez configurer un filtre de recherche personnalisé pour rechercher dans plusieurs attributs LDAP, grâce aux clés de registre suivantes :

Clé	`SearchFilter (REG_SZ)`
Emplacement	**HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Properties\CoworkerSelector**
Valeur	Indiquez le filtre que vous souhaitez appliquer lors d'une recherche LDAP. Utilisez les connecteurs logiques "&" (et) et "|" (ou). Par exemple : • `(|(cn=?)(mail=?))` permet de rechercher la chaîne de caractères entrée par l'utilisateur dans le nom commun OU dans l'adresse e-mail. • `(&(|(cn=?)(mail=?))(usercertificate;binary=*))` permet de rechercher la chaîne de caractères entrée par l'utilisateur dans le nom commun OU dans l'adresse e-mail ET l'utilisateur doit posséder un certificat dans l'annuaire LDAP. Le caractère "?" est remplacé par la chaîne de caractères entrée par l'utilisateur dans le champ de recherche.
Clé	`SearchPattern (REG_SZ)`
Emplacement	**HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Properties\CoworkerSelector**

Valeur	Clé optionnelle. Permet de remplacer si besoin le caractère par défaut "?" utilisé dans le filtre.

5. Pour aller plus loin

Des informations complémentaires et réponses à vos éventuelles questions sont disponibles dans la base de connaissances Stormshield (authentification nécessaire).

documentation@stormshield.eu