GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA FILE

Sécurisation de fichiers et dossiers

Version 10.1

Dernière mise à jour du document : 29 mars 2022

Référence : sds-fr-sd_file-guide_d_utilisation-v10

Table des matières

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

Préface

Ce document fournit les informations essentielles à l'utilisation de Stormshield Data File. Il décrit les fonctions de Stormshield Data File dans sa configuration par défaut. Vous pouvez personnaliser l'installation de ce composant à l'aide de Stormshield Data Authority Manager. Les options de personnalisation les plus importantes sont données dans ce guide. Ce guide s'adresse :

1. aux administrateurs système qui souhaitent installer Stormshield Data Security ;
2. aux utilisateurs du logiciel qui souhaitent protéger des fichiers confidentiels.

1. Introduction

Cette section décrit les caractéristiques et fonctionnalités de Stormshield Data File.

1.1 Protéger la confidentialité de vos données

Stormshield Data File est un logiciel de sécurité informatique. Il est destiné à garantir la confidentialité des données que vous manipulez tous les jours. Stormshield Data File offre les services de sécurité suivants :

- La confidentialité des fichiers dont seules les personnes autorisées pourront lire le contenu chiffré.
- L'automatisation des tâches de chiffrement et de déchiffrement sur des événements définis par l'utilisateur.
- La suppression sécurisée et définitive des fichiers d'origine, ne laissant ainsi aucune trace des ces fichiers sur votre disque.

Outre le chiffrement, Stormshield Data File permet la compression les fichiers avant leur chiffrement, ceci afin de réduire leur encombrement.

1.2 Méthodes de chiffrement complémentaires

Stormshield Data File comprend plusieurs méthodes complémentaires pour la protection des fichiers :

- Les fichiers peuvent être chiffrés pour vous-même ou un groupe de correspondants grâce à l'utilisation de votre clé publique. Les correspondants utilisent leur clé privée pour déchiffrer les fichiers.
- Les fichiers peuvent être chiffrés sous la forme d'un fichier auto-déchiffrable ou au format SmartFILE.

Le produit de base Stormshield Data File sécurise des fichiers et gère des listes de fichiers à protéger, ceux-ci pouvant être situés sur l'ensemble des volumes disques accessibles en local, ou en réseau. Les listes sont utilisées pour le chiffrement ou le déchiffrement de fichier(s) lors de la survenue d'événements prédéterminés.

1.3 Intégration dans Stormshield Data Security

Stormshield Data File s'intègre dans la gamme Stormshield Data Security Enterprise (solutions à clés publiques). L'utilisation d'un compte existant ainsi que les clés et certificats déjà installés permettent de se connecter de manière unique à tous les composants de Stormshield Data Security Enterprise installés sur votre poste de travail.

Pour plus d'informations, consultez le *Guide d'installation et de mise en œuvre*.

1.4 Cryptographie à clé publique

Stormshield Data File met en œuvre des moyens de cryptologie dits "à clé publique".

Chaque correspondant possède un couple de clés : une clé privée et une clé publique. La clé privée doit être conservée de façon confidentielle par son propriétaire. En revanche, la clé publique est destinée à être distribuée.

Ce couple de clés est utilisé pour le chiffrement et le partage de documents confidentiels, comme cela est expliqué ci-dessous.

Stormshield Data File peut mettre en œuvre :

- Soit un couple unique de clés pour le chiffrement et la signature ;
- Soit deux couples de clés, différents l'un pour le chiffrement, l'autre pour la signature ;
- Soit un couple de clés pour le chiffrement seul ou la signature seule.

1.4.1 Le chiffrement

Le chiffrement est une technique mathématique permettant de transformer des informations numériques (message, fichier) compréhensibles (en clair) en informations numériques (chiffrées). Une fois les données chiffrées, seuls les correspondants, possédant la clé, peuvent les décoder et les lire ; elles sont inintelligibles pour toute autre personne.

L'utilisateur initialise le chiffrement d'un fichier en utilisant sa clé publique ou la clé publique des correspondants si ce fichier est destiné à être transmis.

Le correspondant utilise sa clé privée pour initialiser le déchiffrement du fichier. L'utilisateur et le correspondant sont les seuls à posséder leur clé privée et sont donc assurés que les informations ne peuvent pas être lues par un tiers.

Pour déchiffrer un fichier transmis, le correspondant doit être équipé de Stormshield Data File ou de Security BOX SmartFILE. Cependant, si Stormshield Data Security peut déchiffrer indifféremment les fichiers au format Stormshield Data Security ou Security BOX SmartFILE, Security BOX SmartFILE ne peut déchiffrer que les fichiers qui lui sont destinés.

1.4.2 Certificats

Pour envoyer des messages chiffrés à des correspondants, vous devez connaître la clé publique de chiffrement de vos correspondants.

Les clés publiques sont distribuées sous forme de certificat. Un certificat est un document électronique qui associe une clé publique à son propriétaire. Stormshield Data Security supporte le format de certificat X.509 V3.

IMPORTANT
En cas de renouvellement de la clé de chiffrement ou de certificats, les certificats (ainsi que la clé associée) utilisés pour le chiffrement antérieur de données doivent être conservés afin de pouvoir déchiffrer ultérieurement ces données.

Pour plus d'informations sur l'export et l'import de certificats, consultez le *Guide d'installation et de mise en œuvre*.

1.4.3 Confiance

Un certificat établit un lien entre une clé publique et une identité. Vous ne pouvez utiliser un certificat que si vous faites confiance à ce lien.

En effet, si par exemple vous voulez envoyer un fichier chiffré à Alice, vous devez être certain que le certificat qui se prétend être celui d'Alice est effectivement bien celui d'Alice ; sinon vous prenez le risque que votre fichier soit chiffré non pas avec la véritable clé d'Alice, mais avec la clé d'un imposteur qui pourra déchiffrer votre fichier destiné à Alice.

Deux techniques permettent d'accorder sa confiance à un certificat :

- La confiance par héritage adopte le principe que si vous faites confiance à une autorité dans son rôle de certification, vous faites implicitement confiance aux certificats qu'elle délivre.
- La confiance explicite impose que vous vérifiez vous-même l'origine du certificat. Une technique usuelle consiste à en vérifier l'empreinte à partir d'une source parallèle d'information (téléphone, publication, courrier, site web, etc.).

1.4.4 Annuaires de confiance

Stormshield Data Security permet de gérer un annuaire de confiance : vous y insérez les certificats des correspondants et des autorités auxquels vous faites confiance.

La gestion des annuaires de confiance et des certificats est décrite dans le *Guide d'installation et de mise en œuvre*.

1.5 Connexion sécurisée

L'accès à vos clés est protégé : pour pouvoir les utiliser, vous devez vous connecter à Stormshield Data Security, processus qui consiste à vous authentifier et à vérifier que vous êtes bien le propriétaire des clés.

Stormshield Data Security propose deux méthodes d'authentification :

- par mot de passe : vous saisissez un identifiant et un mot de passe ;
- par carte à puce ou clé USB : vous saisissez le code secret de la carte (en anglais, “PIN” Personal Identification Number).

Stormshield Data Security supporte différents types de cartes à puces et de clés USB.

Pour plus d'informations, reportez-vous au *Guide d'installation et de mise en œuvre*.

1.6 Compatibilité avec Security BOX SmartFILE

Stormshield Data File comprend le composant Security BOX SmartFILE. Vous pouvez donc utiliser toutes les fonctions de ce composant lorsque que vous installez Stormshield Data File. Vous pouvez notamment générer :

- Des fichiers chiffrés au format Security BOX SmartFILE afin de les partager avec des correspondants ne disposant que de l'application Security BOX SmartFILE
- Des fichiers chiffrés sous une forme auto-déchiffrable afin de les partager avec des correspondants ne disposant pas de Stormshield Data File ni de Security BOX SmartFILE.

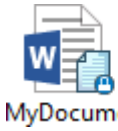
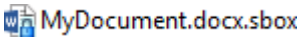
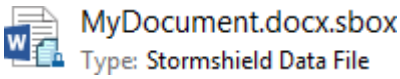
Les fonctions Security BOX SmartFILE sont sélectionnées de manière transparente à partir du menu contextuel Stormshield Data File via le choix **Stormshield Data Security > Chiffrer vers**.

NOTE
Stormshield Data File détecte automatiquement la présence de Security BOX SmartFILE sur votre poste de travail et la désactive de façon à ce que vous n'utilisiez que Stormshield Data File.

1.7 Pictogrammes de chiffrement

Dans l'explorateur de Windows, un dossier sécurisé et un fichier chiffré se reconnaissent par le pictogramme 

.

 MyDocument.docx.sbox	Ces pictogrammes indiquent que le fichier est chiffré. Si vous n'êtes pas autorisé à voir ou modifier ce fichier, vous ne pourrez pas l'ouvrir.
 MyDocument.docx.sbox	
 MyDocument.docx.sbox Type: Stormshield Data File	

2. Installation de Stormshield Data File

Cette section présente la configuration requise par Stormshield Data File et l'installation de l'application.

2.1 Configuration requise

Pour connaître la configuration requise sur les systèmes d'exploitation Microsoft, reportez-vous à la section **Compatibilité** de la note de version de Stormshield Data Security 10.1.

200 Mo d'espace disque sont requis pour l'installation de tous les composants de Stormshield Data Security.

IMPORTANT
Stormshield Data Security n'est pas compatible avec la fonction **Changement Rapide d'Utilisateur**.

2.2 Installation de Stormshield Data File

Stormshield Data File est un composant de Stormshield Data Security Enterprise.

Une clé de licence est communiquée en fonction des droits d'usage que vous avez acquis lors de la commande du produit. Cette clé de licence est demandée à l'installation.

La procédure d'installation est détaillée dans le *Guide d'installation et de mise en œuvre*.

3. Comment dialoguer avec Stormshield Data File

A partir de l'Explorateur Windows, cliquer sur le bouton droit de la souris après avoir sélectionné un fichier et/ou un dossier permet d'accéder aux fonctions de chiffrement et de déchiffrement de Stormshield Data File.

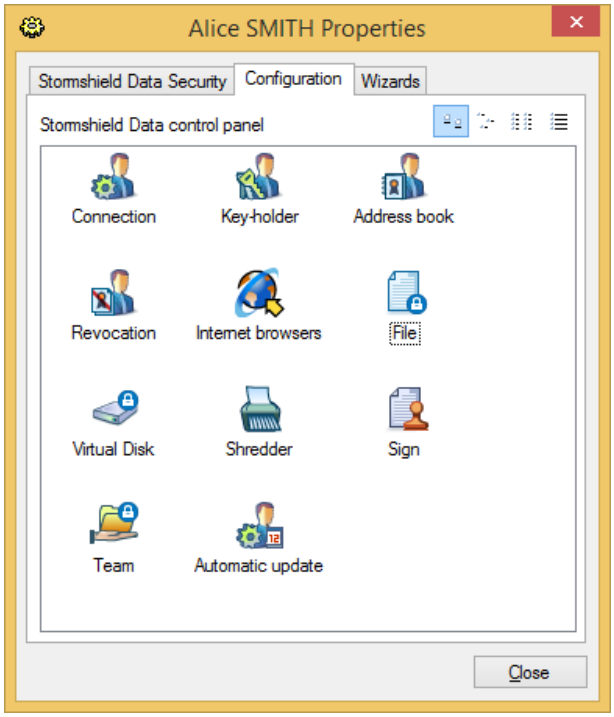
4. Configuration des options

Cette section décrit comment configurer les options générales et avancées de Stormshield Data File.

4.1 Accéder à la fenêtre de configuration

Pour accéder au menu de configuration des options:

1. Effectuez un clic droit sur l'icône Stormshield Data File pour sélectionner **Propriétés** dans le menu contextuel.
2. De la fenêtre **Propriétés**, sélectionnez l'onglet *Configuration*, puis double cliquez sur l'icône **File**.

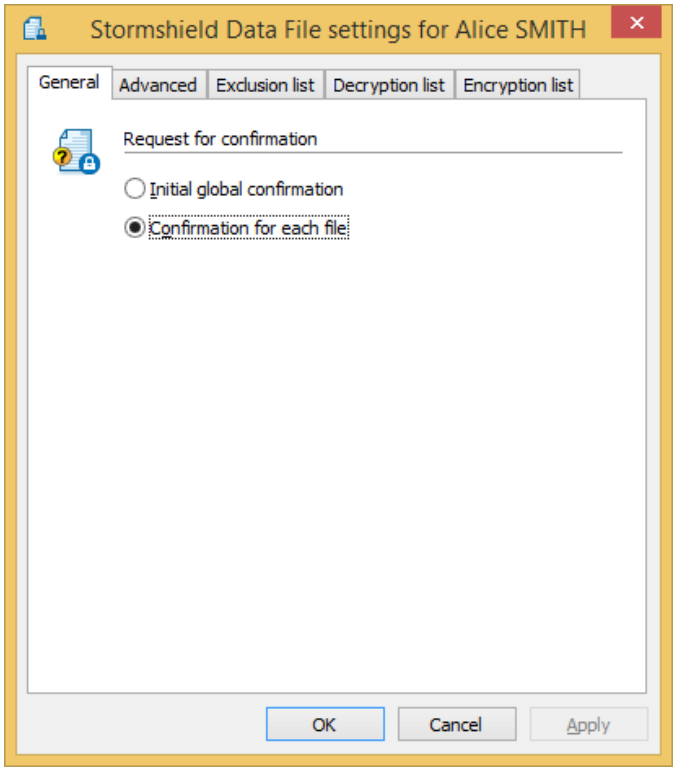


3. Sélectionnez l'onglet *Général* ou *Avancé* selon vos besoins.

Les onglets *Liste de chiffrement*, *Liste de déchiffrement*, et *Liste d'exclusion* ne sont pas décrits dans cette section.

4.2 Options générales

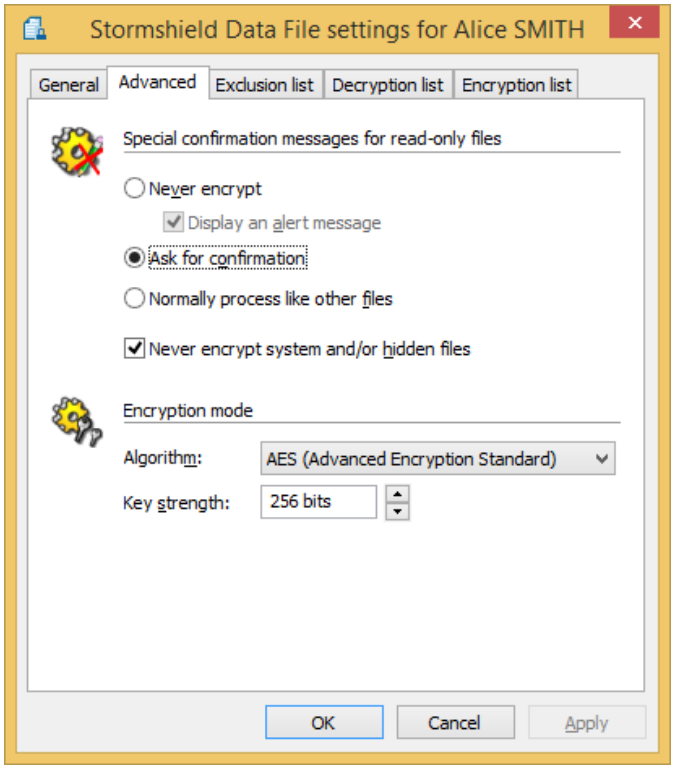
Les options générales sont affichées ci-dessous :



L'onglet *Général* permet de paramétrer les demandes de confirmation. Sélectionner **Confirmation globale initiale** si vous prévoyez de chiffrer de manière fréquente un nombre important de fichiers. Si vous prévoyez de chiffrer des fichiers de manière occasionnelle, conservez **Confirmation pour chaque fichier**, l'option par défaut.

4.3 Options avancées

L'onglet *Avancé* définit la façon de traiter les fichiers en lecture seule et les fichiers cachés. Il permet aussi de choisir l'algorithme et la force de la clé.



Le groupe d'options **Confirmations spéciales de fichiers en lecture seule** vous permet de définir le message de confirmation qui sera affiché en cas de tentative de chiffrement de fichiers en lecture seule, fichiers cachés ou fichiers système. La nature du fichier est spécifiée par les attributs système de chaque fichier.

Sélectionner l'un des boutons pour spécifier l'une des options suivantes :

- **Ne jamais chiffrer** : les fichiers en lecture seule ne seront jamais chiffrés. Pour recevoir un avertissement en cas de tentative de chiffrement d'un fichier en lecture seule, cocher **Signaler ces fichiers**.
- **Demander une confirmation** : une confirmation sera nécessaire avant tout chiffrement d'un fichier en lecture seule.
- **Traiter normalement comme les autres fichiers**: Les fichiers en lecture seule seront traités comme des fichiers ordinaires.

Si vous cochez **Ne jamais chiffrer les fichiers systèmes et/ou cachés**, aucun avertissement n'indiquera que les fichiers systèmes ou cachés ne seront pas chiffrés. Cette option prévaut sur l'option **Demander une confirmation** concernant les fichiers en lecture seule.

Si vous ne cochez pas **Ne jamais chiffrer les fichiers systèmes et/ou cachés**, le chiffrement des fichiers cachés ou systèmes peut être autorisé. Les options définies pour les fichiers en lecture seule prévalent. Si le chiffrement est autorisé pour les fichiers systèmes mais non pour les fichiers en lecture seule, alors aucun fichier en lecture seule ne sera chiffré.

Le mode de chiffrement est défini par :

- l'algorithme de chiffrement
- la force de la clé.

Pour des raisons de sécurité, il est recommandé d'utiliser l'algorithme AES et 256 bits pour la force de la clé.

5. Comment chiffrer et déchiffrer

Cette section décrit comment :

- Chiffrer des fichiers pour soi-même
- Chiffrer des fichiers pour un ou plusieurs correspondants
- Déchiffrer des fichiers
- Générer des fichiers auto-déchiffrables ou chiffrés au format Security BOX SmartFILE

Cette section décrit également comment récupérer un mot de passe utilisé pour la génération de fichiers auto-déchiffrables ou le chiffrement de fichiers au format Security BOX SmartFILE.

5.1 Chiffrer un ou plusieurs fichiers ou dossiers

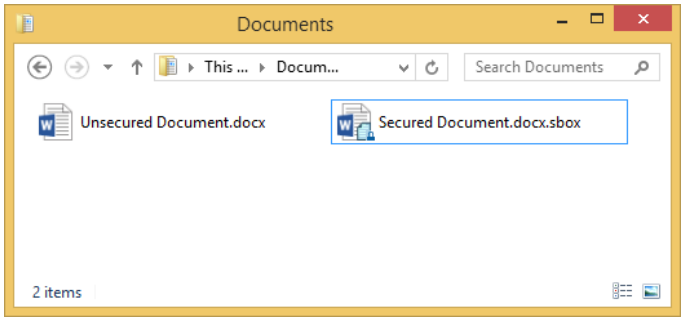
Cette section décrit comment chiffrer des fichiers que :

- vous serez seul à utiliser
- vous allez partager avec un ou plusieurs correspondants.

Les fichiers chiffrés par Stormshield Data File se repèrent :

- par la petite icône en sur-impression apposée à l'icône d'origine
- par l'extension *.SBOX*

Ci-dessous les icônes d'un fichier source et d'un fichier chiffré.

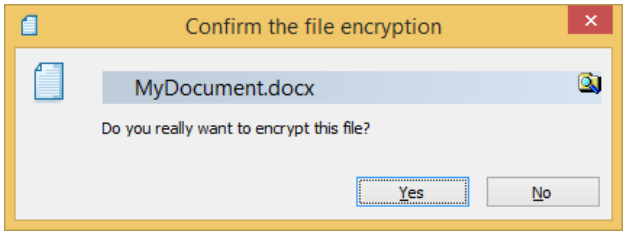


Les procédures décrites dans les sections suivantes s'appliquent aux fichiers et aux dossiers. Il est possible de sélectionner et chiffrer simultanément des fichiers et dossiers.

5.1.1 Chiffrer uniquement pour soi

1. Sélectionnez le(s) fichier(s) à l'aide de la souris puis effectuer un clic droit et choisissez **Stormshield Data Security** > **Chiffrer les fichiers** (ou **Chiffrer le fichier**) dans le menu contextuel :

Le fenêtre suivante s'affiche :



2. Confirmez votre choix. En cas de sélection multiple et selon les options choisies précédemment (voir la section Options générales), Stormshield Data File vous demande de donner :

- une confirmation initiale et globale ; tous les fichiers seront traités et il ne vous sera plus demandé de confirmer.
- une confirmation pour chaque fichier. Pour désactiver temporairement la demande de confirmation pour chaque fichier, désélectionnez l'option dans la fenêtre de confirmation. Il s'agit d'une désactivation temporaire qui n'affecte pas la configuration des options; celle-ci s'appliquera pour la prochaine opération de chiffrement.
- Si vous avez sélectionné un fichier déjà chiffré, Stormshield Data File ignorera ce fichier et traitera les autres fichiers.
- Il est impossible de chiffrer des fichiers vides. Toute tentative de chiffrement d'un fichier vide génère un message d'erreur dans la fenêtre de résumé.

3. La fenêtre de progression de l'opération de chiffrement s'affiche. Au terme de celle-ci un résumé des opérations effectuées s'affiche.

Cliquez sur **Détails**.

Pour fermer automatiquement la fenêtre après un chiffrement réussi, cocher l'option **Fermer la fenêtre automatiquement**. Cette option s'appliquera à toute autre opération de chiffrement et de déchiffrement. Cependant, cette option sera ignorée en cas d'erreurs pendant le chiffrement.

Pour fermer manuellement la fenêtre, attendre que le chiffrement soit terminé et cliquer **Fermer**.

> **NOTE**
> Une fois le chiffrement terminé, le fichier d'origine (en clair) est supprimé de façon sécurisée. La sécurisation est apportée par trois passes d'écriture en surcharge de la totalité du fichier (comme avec le Stormshield Data Shredder.

5.1.2 Chiffrer pour un ou plusieurs correspondants

Utilisez la procédure ci-dessous pour chiffrer des fichiers qui seront partagés avec un ou plusieurs de vos correspondants.

1. Sélectionnez le fichier à l'aide de la souris puis effectuez un clic droit pour choisir **Stormshield Data Security > Chiffrer le fichier vers > Correspondants** dans le menu contextuel.
2. La liste des utilisateurs qui seront à même de déchiffrer votre document s'affiche. Recherchez les utilisateurs ou groupes auxquels vous souhaitez donner le droit d'accès au document. La recherche peut afficher les utilisateurs présents dans l'annuaire de confiance ou dans l'annuaire LDAP dans le cas où il est configuré.

5.2 Déchiffrer un fichier, un dossier ou un ensemble de fichiers

Cette section décrit comment déchiffrer un ou plusieurs fichiers chiffrés.

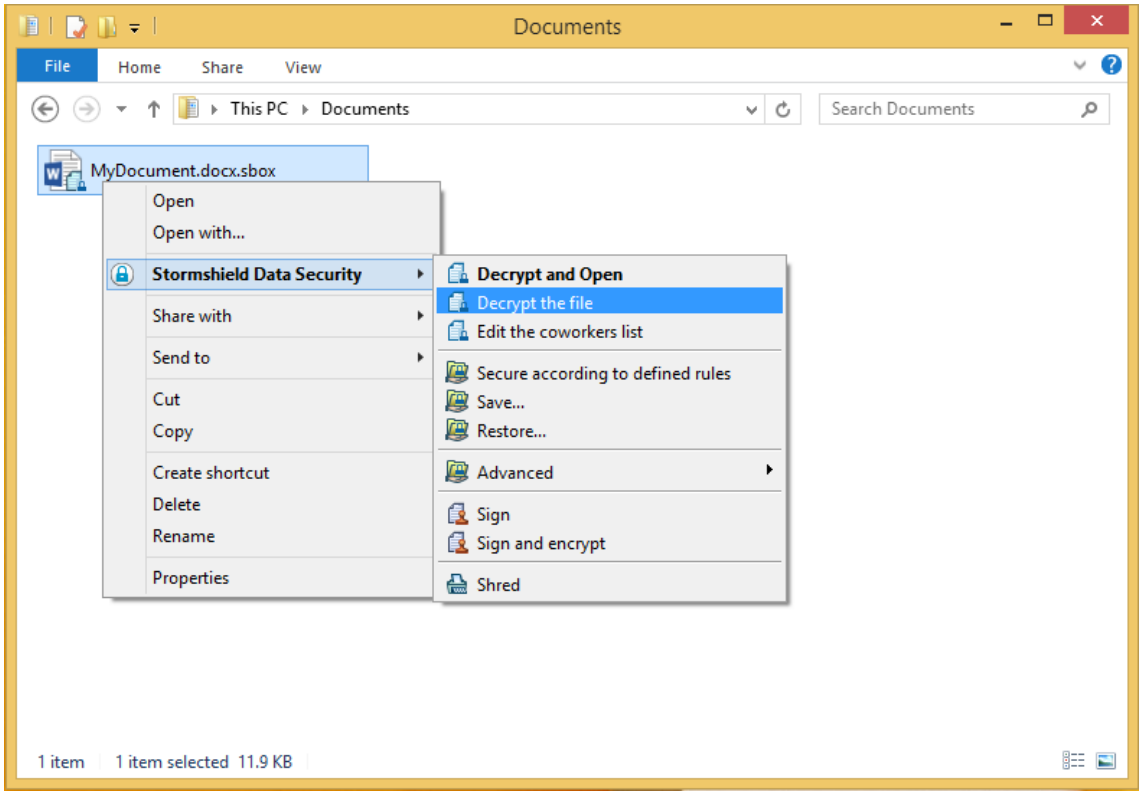
Les fichiers portant l'extension *.sdsx*, *.sbo* ou *.sbox* peuvent être simultanément sélectionnés et traités de la même manière.

Lorsque vous sélectionnez un dossier, Stormshield Data File déchiffre les fichiers que vous avez personnellement chiffrés ou les fichiers chiffrés qui vous ont été envoyés.

Pour déchiffrer un seul fichier, double-cliquez dessus. Le fichier sera automatiquement déchiffré et ouvert par l'application par défaut. Pour déchiffrer un fichier sans l'ouvrir, utilisez la procédure décrite ci-dessous (cette procédure s'applique également pour le déchiffrement de plusieurs fichiers).
Pour déchiffrer un dossier complet, sélectionnez ce dossier et faites un clic droit pour sélectionner **Déchiffrer** dans le menu contextuel.

Pour déchiffrer plusieurs fichiers chiffrés, suivez la procédure décrite ci-dessous.

1. Sélectionnez les fichier(s) et dossier(s) et choisissez **Stormshield Data Security > Déchiffrer** ou **Stormshield Data Security > Déchiffrer et ouvrir** dans le menu déroulant.



La prochaine fenêtre indique la progression de l'opération de chiffrement puis au terme de celle-ci un résumé des opérations effectuées.

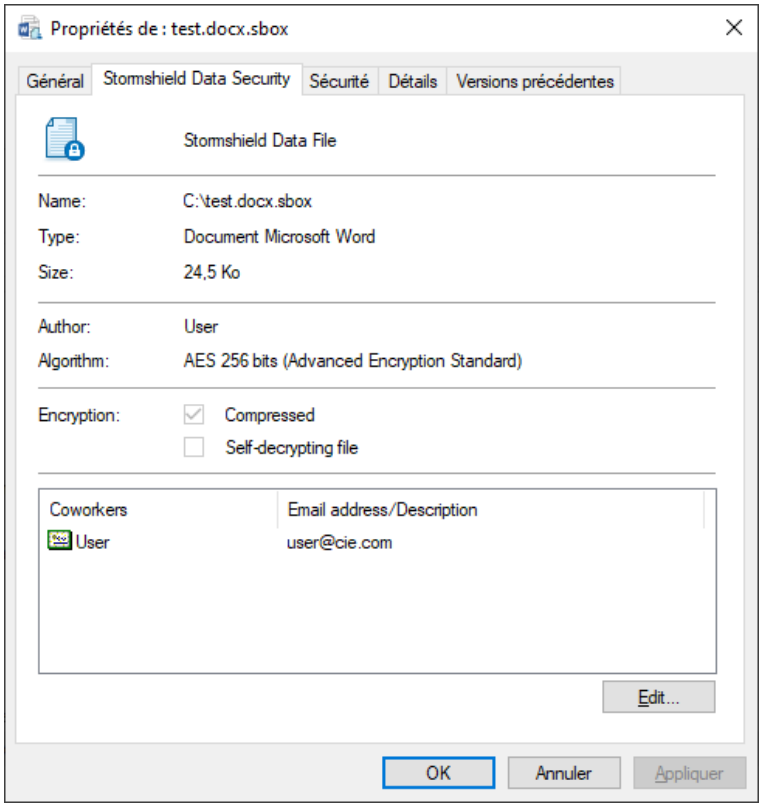
NOTE
Pour des raisons ergonomiques et techniques, il est déconseillé de lancer la commande **Déchiffrer et ouvrir** sur un grand nombre de fichiers.

2. Pour automatiquement fermer la fenêtre après un chiffrement réussi, cocher l'option **Fermer la fenêtre automatiquement**. Cette option s'appliquera à toute autre opération de déchiffrement. Cependant, cette option sera ignorée en cas de survenue d'erreurs pendant le déchiffrement.

Pour fermer manuellement la fenêtre, attendre que le chiffrement soit terminé et cliquer **Fermer**.

5.3 Afficher les propriétés d'un fichier chiffré

Les propriétés d'un fichier chiffré affichent la liste des utilisateurs pour lesquels le fichier a été chiffré, et qui peuvent le déchiffrer.



Aux données habituelles (nom de fichier, type et taille) s'ajoutent :

- le nom de l'utilisateur ayant chiffré le fichier
- l'algorithme utilisé pour le chiffrement
- les attributs du fichier :
- **Compression** indique si le fichier à été compressé par Stormshield Data File (sans rapport avec le fanion similaire des propriétés standards d'un fichier sous Windows). Cette propriété concerne uniquement le format *.sbox*.
- **Auto-déchiffrable** indique si c'est un auto-déchiffrable (voir la section Créer un auto-déchiffrable).
- le nom et l'adresse e-mail des correspondants qui peuvent déchiffrer le fichier (uniquement si vous êtes connecté).

5.4 Gérer les collaborateurs d'un fichier chiffré

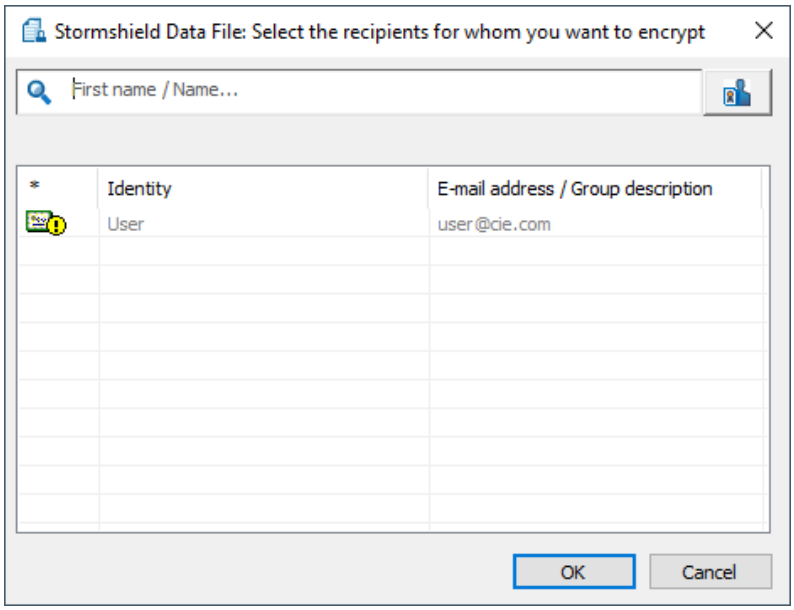
Il est possible de gérer les collaborateurs associés à un fichier chiffré depuis la fenêtre des propriétés de ce fichier. Vous pouvez :

- Ajouter un ou plusieurs collaborateurs depuis votre annuaire.
- Supprimer un ou plusieurs collaborateurs associés au fichier chiffré.

Pour ajouter un ou plusieurs collaborateurs :

1. Ouvrez les **Propriétés** d'un fichier chiffré et sélectionnez l'onglet *Stormshield Data Security* ou bien faites un clic droit sur le fichier chiffré et sélectionnez **Stormshield Data Security > Modifier la liste des collaborateurs**.

   Le sous menu **Stormshield Data Security > Modifier la liste des collaborateurs** n'est plus présent à partir de Windows 10.
2. Cliquez sur le bouton **Modifier**. La fenêtre suivante s'affiche :



3. Recherchez le ou les collaborateurs ou groupes à ajouter et cliquez sur **OK**.
4. Cliquez sur **Appliquer** puis **OK** dans la fenêtre des **Propriétés** pour appliquer les changements. Si vous cliquez sur **Annuler**, les changements ne sont pas pris en compte.

Pour supprimer un ou plusieurs collaborateurs :

1. Dans la fenêtre des **Propriétés**, sélectionnez le ou les collaborateurs voulus et cliquez sur **Supprimer**.
2. Confirmez puis cliquez sur **Appliquer** et **OK** dans la fenêtre des **Propriétés** pour appliquer les changements. Si vous cliquez sur **Annuler**, les changements ne sont pas pris en compte.

NOTE
Il faut être connecté ou disposer des droits sur le fichier pour que les options de gestion des utilisateurs soient disponibles.

Vous pouvez afficher votre annuaire de confiance depuis la liste des collaborateurs afin de mettre à jour les certificats.

5.5 Créer un auto-déchiffrable

Les auto-déchiffrables sont des fichiers de type exécutable (Windows 32 bits) qui contiennent à la fois la forme chiffrée du fichier à protéger et le programme permettant de le déchiffrer. La protection repose sur un mot de passe que les correspondants doivent s'échanger par un

moyen sûr. Ce mot de passe est demandé par le programme contenu dans l'auto-déchiffrable car il sert de clé pour le déchiffrement.

Lorsqu'un fichier de type auto-déchiffrable est reçu sur un poste de travail disposant de Stormshield Data File, le lancement de cet auto-déchiffrable n'active pas réellement le programme contenu mais active la fonction de Stormshield Data File sachant directement décoder le fichier (après fourniture du mot de passe) sans utiliser le code présent à l'intérieur de celui-ci.

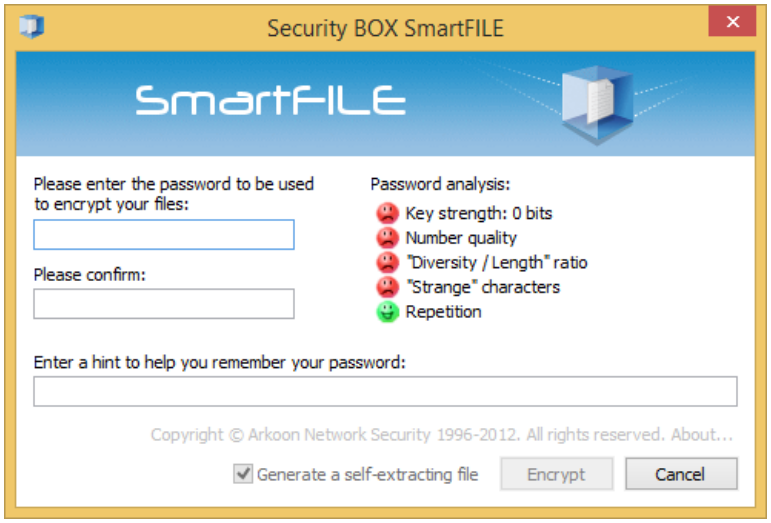
NOTE
Certaines passerelles d'entreprises ne laissent pas passer des exécutables et donc filtrent les fichiers auto-déchiffrables de Stormshield Data File. De même, certains logiciels clients de messagerie refusent l'accès aux exécutables contenus dans les messages.

Les règles suivantes s'appliquent :

- Lorsqu'un fichier est chiffré sous la forme d'un auto-déchiffrable, le fichier source (en clair) n'est pas supprimé.
- Vous pouvez chiffrer plusieurs fichiers et dossiers simultanément. Un fichier auto-déchiffrable sera généré pour chaque fichier.

Pour créer un auto-déchiffrable :

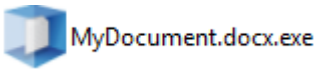
1. Sélectionnez le fichier puis effectuez un clic droit pour sélectionnez **Stormshield Data Security > Chiffrer vers > Auto-déchiffrable** dans le menu contextuel.
2. Entrez le mot de passe et le mnémonique pour vous en souvenir.



Par défaut, la saisie du mot de passe est masquée et nécessite la saisie en double pour confirmation. Il est possible de demander une saisie en clair (qui dispense de la double saisie) en faisant un clic droit dans la zone de saisie du mot de passe et en sélectionnant **Afficher le mot de passe**. Il est possible de revenir à la double saisie masquée de la même façon.

3. Cliquez sur **Chiffrer**. Le fichier est chiffré avec le mot de passe spécifié.

Les fichiers auto-déchiffrables sont identifiés par l'extension *.exe* comme ci-dessous.



5.6 Créer un fichier compatible Security BOX SmartFILE

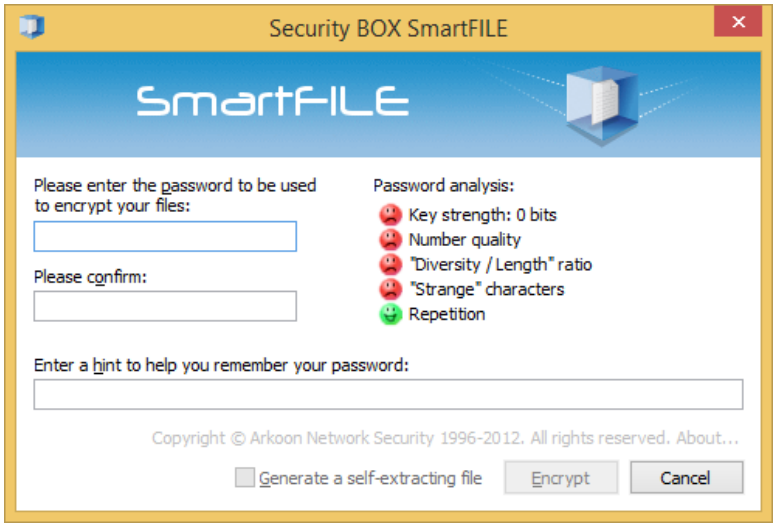
Si vous souhaitez partager des fichiers chiffrés avec des correspondants ne disposant pas de Stormshield Data File mais de Security BOX SmartFILE, Stormshield Data File vous permet de générer des fichiers chiffrés au format Security BOX SmartFILE.

Les règles suivantes s'appliquent :

- Lorsqu'un fichier est chiffré sous la forme d'un auto-déchiffrable, le fichier source (en clair) n'est pas supprimé.
- Vous pouvez chiffrer plusieurs fichiers et dossiers simultanément. Un fichier chiffré au format Security BOX SmartFILE sera créé pour chaque fichier.
- Les noms des fichiers chiffrés ne doivent pas comporter de caractères Unicode.

Pour chiffrer un fichier en utilisant le format Security BOX SmartFILE :

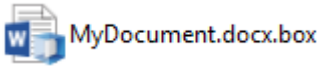
1. Sélectionnez le fichier puis effectuez un clic droit pour sélectionner **Stormshield Data Security > Chiffrer vers > SmartFile**.
2. Entrez le mot de passe et le mnémonique pour vous en souvenir.



Par défaut, la saisie du mot de passe est masquée et nécessite la saisie en double pour confirmation. Il est possible de demander une saisie en clair (qui dispense de la double saisie) en faisant un clic droit dans la zone de saisie du mot de passe et en sélectionnant **Afficher le mot de passe**. Il est possible de revenir à la double saisie masquée de la même façon.

3. Cliquez **Chiffrer**. Le fichier est chiffré avec le mot de passe spécifié.

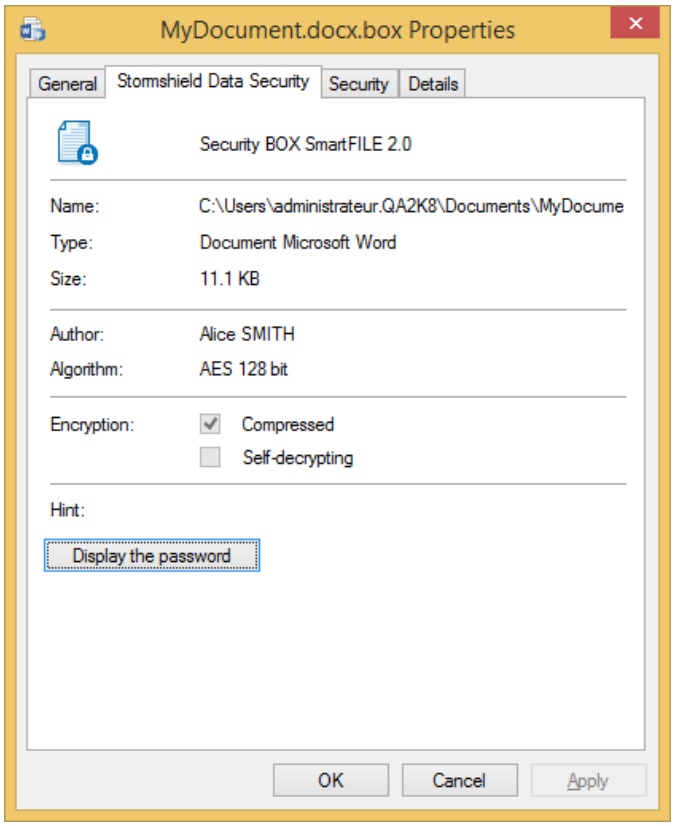
Les fichiers chiffrés au format Security BOX SmartFILE disposent d'une petite icône et d'une extension spécifique comme ci-dessous :



5.7 Récupération du mot de passe

Si vous avez besoin de récupérer le mot de passe utilisé pour la génération d'un auto-déchiffrable ou d'un fichier chiffré au format Security BOX SmartFILE, il est possible d'afficher le mot de passe à partir des propriétés du fichier (onglet *Stormshield Data Security*). Pour lancer cette fonction, vous devez :

- disposer de Stormshield Data File et de Security BOX SmartFILE
- être connecté sur Stormshield Data Security avec le compte utilisateur qui a servi au chiffrement du fichier Il n'est pas possible de récupérer le mot de passe à partir d'un autre compte Stormshield Data Security (y compris les comptes de récupération) ou en utilisant Security BOX SmartFILE.



Cliquez **Afficher le mot de passe** pour visualiser le mot de passe.

5.8 Déchiffrer un fichier Security BOX SmartFILE avec un compte de recouvrement

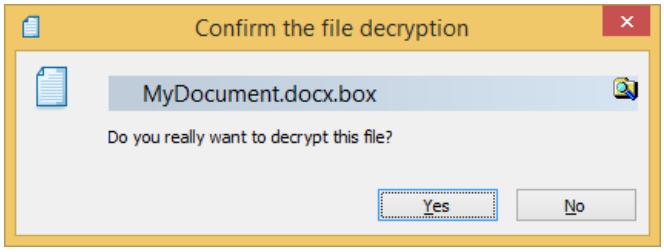
Si vous avez besoin de déchiffrer un fichier Security BOX SmartFILE en utilisant un compte de recouvrement :

1. Connectez-vous au compte de recouvrement.
2. Appuyez et maintenez simultanément enfoncées les touches CTRL+SHIFT puis double-cliquez sur le fichier à déchiffrer.

OU

Appuyez et maintenez simultanément enfoncées les touches CTRL+SHIFT puis effectuez un clic-droit puis sélectionnez **SecurityBOX > Déchiffrer**.

3. Relâchez les touches CTRL+SHIFT. La fenêtre de confirmation s'affiche :



4. Cliquez sur **Oui** si vous souhaitez déchiffrer le fichier.

Le fichier est déchiffré sans mot de passe.

6. Utilisation de listes

Les listes de chiffrement et déchiffrement permettent l'automatisation du chiffrement et du déchiffrement des fichiers pour un fonctionnement plus simple et sans erreur. Il est également possible de créer une liste de fichiers protégés afin de protéger ces fichiers du chiffrement.

6.1 Listes de chiffrement et déchiffrement

Les fichiers inclus dans les listes de chiffrement et déchiffrement sont automatiquement chiffrés ou déchiffrés à des moments prédéfinis. Ainsi, vous pouvez décider de chiffrer automatiquement à la fermeture de votre session, au verrouillage de votre session utilisateur ou à intervalles fixés (par exemple toutes les 15 minutes) en tâche de fond.

NOTE
La liste de déchiffrement doit rester courte pour des raisons de temps de réponse. Bien que Stormshield Data File soit fortement optimisé, le déchiffrement d'un très grand nombre de fichiers reste nécessairement long.

Les listes de chiffrement et déchiffrement peuvent également être utilisées pour lancer le chiffrement ou déchiffrement groupé de tout ou partie de liste.

6.1.1 A propos de la récursivité

La récursivité du chiffrement ou déchiffrement des listes de fichiers permet de l'étendre aux sous-dossiers. Elle est appelée par l'option **Inclure les sous-dossiers** et peut prendre deux valeurs (oui/non). Elle s'applique de diverses façons :

- En tant que mode, elle s'applique à tous les items et peut être activée et répétée dans plusieurs écrans.
- En tant que propriété de dossier, elle définit si seulement le dossier indiqué sera chiffré ou déchiffré ou si ses sous-dossiers le seront aussi.
- En tant que propriété de fichier, elle définit si seulement le fichier indiqué sera chiffré ou déchiffré ou si les fichiers de même nom, mais situés dans d'autres dossiers, le seront aussi.
- En tant que propriété d'une collection de fichiers définie par une expression qui utilise des jokers (* et ?), elle définit si seulement la collection de fichiers sera chiffrée ou déchiffrée ou si les fichiers de même nom, mais situés dans d'autres dossiers, le seront aussi.

6.1.2 Gérer les listes

Pour gérer votre liste de fichiers à chiffrer ou déchiffrer automatiquement :

1. Sélectionnez l'icône Stormshield Data File et effectuez un clic droit pour sélectionner **Propriétés** du menu contextuel
2. Dans la fenêtre de propriétés, sélectionnez l'onglet *Configuration*, cliquez sur l'icône Stormshield Data File puis sélectionnez l'onglet *Liste de chiffrement* ou *Liste de déchiffrement*.

Au centre de la fenêtre se trouve la liste des fichiers et dossiers à chiffrer automatiquement. Vous pouvez en ajouter ou en retirer à l'aide des boutons du même nom au milieu de la fenêtre.

Le signe + sur l'icône symbolise un dossier et indique que les sous-dossiers font également partie de la liste de chiffrement. Cette propriété du dossier est modifiable en cliquant sur le bouton Propriétés (voir étape 4).

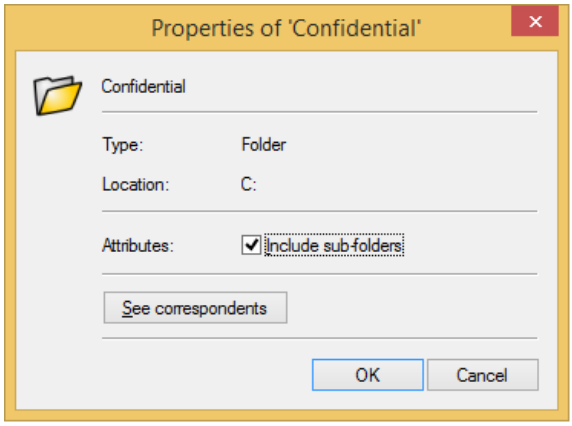
3. Pour activer ou désactiver par défaut le mode récursif, cliquez sur **Ajouter** puis sélectionnez **Inclure les sous-dossiers**. Si le mode récursif est le mode par défaut, sélectionner cette option vous permet de désactiver ce mode.

Le nouveau mode par défaut s'appliquera aux prochaines entrées de la liste. Les fichiers ou dossiers présents ne sont pas affectés par le changement et doivent être individuellement modifiés comme expliqué en étape 4.

4. Pour modifier la récursivité d'une entrée :

a. Sélectionnez l'entrée.

b. Cliquez sur **Propriétés**. Une nouvelle fenêtre s'affiche :



c. Modifiez la valeur de l'option et cliquez sur **OK**.

5. Pour ajouter une entrée à la liste, cliquez sur **Ajouter** puis sélectionnez l'une des options suivantes :

- pour ajouter un fichier, cliquez **Ajouter fichiers**
- pour ajouter un dossier, cliquez **Ajouter dossiers**
- pour sélectionner les fichiers à l'aide des caractères spéciaux * et ?, cliquez sur **Ajouter masque** puis entrez le chemin ou parcourez les dossiers.

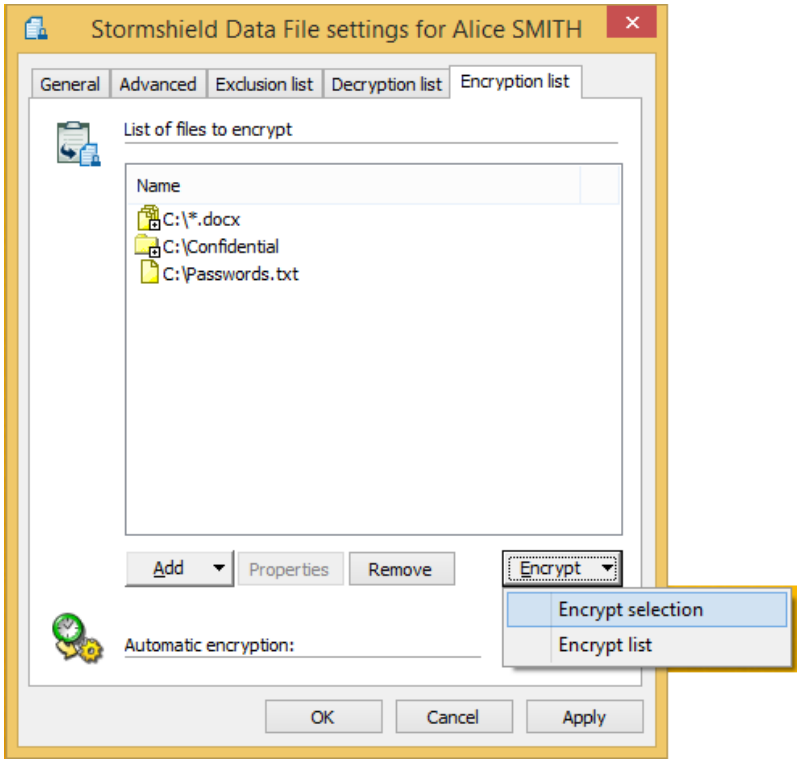
6. Pour retirer un ou plusieurs articles de la liste, sélectionnez les articles puis cliquez **Retirer**.

Pour spécifier les événements qui déclencheront le chiffrement ou déchiffrement automatique ou démarrer immédiatement le chiffrement ou déchiffrement des fichiers et dossiers des listes, référez-vous à la section Chiffrer et déchiffrer.

6.1.3 Chiffrer et déchiffrer

Le chiffrement ou déchiffrement des listes de fichiers peut être déclenché par l'utilisateur ou à l'apparition d'un événement (système ou programmé) :

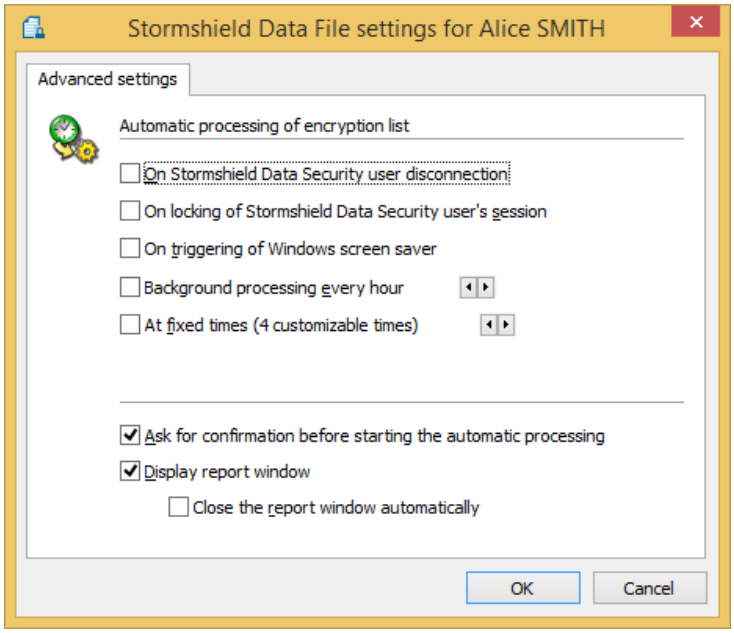
- Déclenché par l'utilisateur : pour chiffrer ou déchiffrer immédiatement tous les items sélectionnés, cliquez dans le bouton combo **Chiffrer** ou **Déchiffrer** puis le choix **Chiffrer la sélection** ou **Déchiffrer la sélection**.



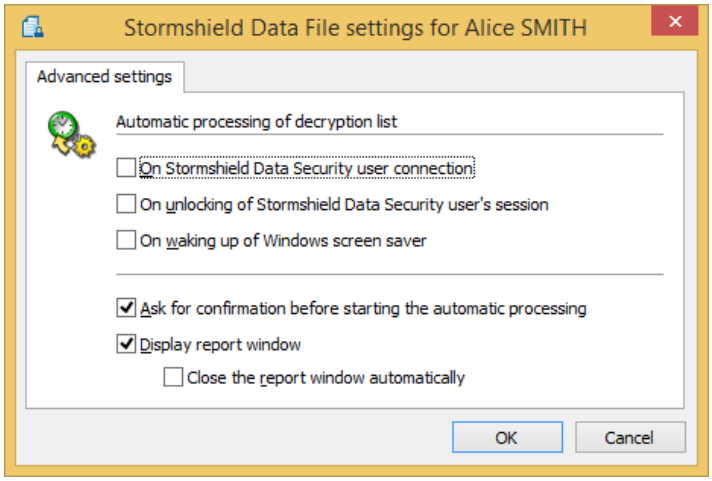
- A l'apparition d'un événement :

1. Pour sélectionner les événements qui doivent déclencher le chiffrement ou déchiffrement de tous les items satisfaisant aux critères de liste, cliquez sur le bouton **Définir**.

La fenêtre suivante affiche les événements qui peuvent être sélectionnés pour déclencher le chiffrement automatique :



La fenêtre suivante affiche les événements qui peuvent être sélectionnés pour déclencher le déchiffrement automatique :



2. Sélectionnez les événements déclencheurs, la fréquence ou les heures de la journée :

- Pour le chiffrement :
- Chaque fois que l'utilisateur Stormshield Data Security se déconnecte, que ce soit manuellement via le menu Stormshield Data Security de la barre des tâches ou automatiquement au moment de la fermeture de la session Windows (ou lors d'événements analogues : retrait de carte à puce, lancement de l'économiseur d'écran....)
- Chaque fois que la session Stormshield Data Security est verrouillée
- Chaque fois que l'économiseur d'écran de Windows se met en route
- En tâche de fond, à une fréquence choisie par l'utilisateur (de 5 minutes à huit heures)
- A heures fixes (résolution : 1 minute).
- Pour le déchiffrement :
- Chaque fois que l'utilisateur Stormshield Data Security se connecte
- Chaque fois que la session Stormshield Data Security est déverrouillée
- Chaque fois que l'économiseur d'écran de Windows est désactivé.

3. Demandez éventuellement :

- une confirmation avant l'exécution automatique. Cochez l'option **Demander confirmation avant une exécution automatique**.

> **NOTE**
> La demande de confirmation est temporisée. Si l'utilisateur n'a pas répondu dans les 10 secondes, le traitement est lancé. Cela permet d'effectuer les traitements automatiques même lorsque l'utilisateur s'est absenté de son poste. Lorsqu'une confirmation est demandée, l'utilisateur a donc 10 secondes pour annuler le traitement.

- l'affichage d'un compte-rendu. Cochez la case **Afficher la fenêtre de compte-rendu**. La case **Fermer automatiquement la fenêtre de compte-rendu** reprend exactement la valeur de la case affichée dans le compte-rendu. La fermeture automatique de la fenêtre de compte-rendu ne s'applique que s'il n'y a pas eu d'erreur.

6.2 Liste d'exclusion (fichiers protégés)

Pour des raisons de sécurité, il peut être important de ne pas autoriser le chiffrement de certains fichiers pour éviter qu'ils ne soient pas chiffrés par erreur. Afin d'empêcher le

chiffrement accidentel de fichiers, il vous faut créer une liste d'exclusion, qui va contenir la liste des fichiers ne devant pas être chiffrés.

Les principes de récursivité expliqués à la section A propos de la récursivité s'appliquent à la liste d'exclusion.

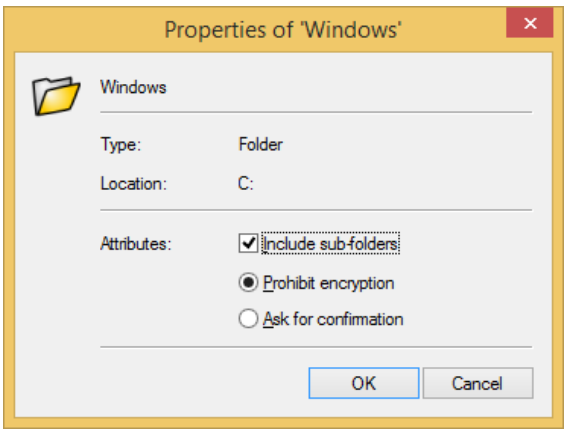
Pour éviter le chiffrement du dossier système (C:\WINDOWS\ par défaut) et le dossier d'installation de Stormshield Data File (C:\Program Files\MSI\Security BOX\ par défaut), il est recommandé d'inclure ces dossiers dans la liste d'exclusion.

Pour créer la liste d'exclusion :

1. Sélectionnez l'icône Stormshield Data File et effectuez un clic droit pour sélectionner **Propriétés** du menu contextuel.
2. Dans la fenêtre de propriétés, sélectionnez l'onglet *Configuration* ; cliquez sur l'icône Stormshield Data File.
3. Sélectionnez l'onglet *Liste d'exclusion*. Au centre de la fenêtre se trouve la liste de fichiers et dossiers à ne pas chiffrer.
   Vous pouvez en ajouter ou en retirer à l'aide des boutons du même nom au milieu de la fenêtre.
   L'icône indique que le fichier ou dossier ne doivent pas être chiffrés.
   L'icône indique qu'une confirmation doit être obtenue avant de chiffrer le fichier ou dossier.
4. Pour activer ou désactiver par défaut le mode récursif, cliquez sur **Ajouter** et sélectionnez **Inclure les sous-dossiers**. Si le mode récursif est le mode par défaut, sélectionner cette option vous permet de désactiver ce mode.

Le nouveau mode par défaut s'appliquera aux prochaines entrées de la liste. Les fichiers ou dossiers déjà présents ne sont pas affectés par le changement et doivent être individuellement modifiés comme expliqué en étape 5.

5. Pour modifier la récursivité d'une entrée :
   a. Sélectionnez l'entrée.
   b. Cliquez **Propriétés**. Une nouvelle fenêtre s'affiche :



   c. Modifiez la valeur de l'option et cliquez **OK**.
6. Pour ajouter une entrée à la liste, cliquez **Ajouter** puis sélectionnez l'une des options suivantes :

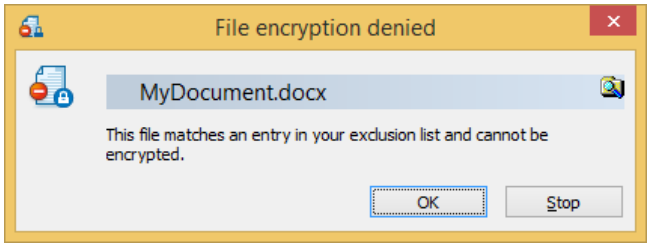
- Pour ajouter un fichier et empêcher le chiffrement de manière inconditionnelle, sélectionnez **Ajouter des fichiers > Interdire le chiffrement**.
- Pour ajouter un fichier et demander une confirmation avant le chiffrement, sélectionnez **Ajouter des fichiers > Demander une confirmation**.

- Pour ajouter un dossier et empêcher le chiffrement de manière inconditionnelle, sélectionnez **Ajouter un dossier > Interdire le chiffrement**.
- Pour ajouter un dossier et demander une confirmation avant le chiffrement, sélectionnez **Ajouter un dossier > Demander une confirmation**.
- Pour sélectionner automatiquement, en particulier à l'aide de jokers (* et ?), les types de fichiers à protéger, cliquez sur **Ajouter une expression** et saisissez le chemin de fichier ou parcourez les disques.

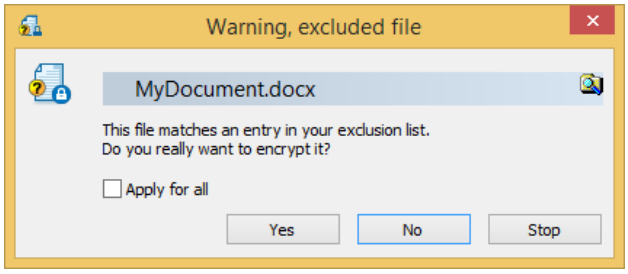
Pour protéger tous les fichiers définissant les comptes Stormshield Data Security, utilisez une expression du type *:*.usr. Ceci interdira le chiffrement de tous les fichiers avec l'extension *.usr*, sur tous les disques du système. Ceci est un exemple. En fait il est recommandé d'interdire le chiffrement de dossier complet.

7. Pour ôter une ou plusieurs entrées de la liste, sélectionnez les articles et cliquez sur **Retirer**.

En cas de tentative de chiffrement d'un dossier protégé, la fenêtre suivante est affichée (si l'affichage de la notification n'a pas été désactivée, voir la fenêtre précédente) :



Ou :



Dans la dernière fenêtre, cliquez sur **Appliquer à tous** pour appliquer votre choix (oui ou non) à tous les fichiers.

6.2.1 Règles d'exclusion

1. Si un fichier/dossier appartient aux deux listes (chiffrement et exclusion), celle des fichiers protégés est prioritaire sur la première. Par suite, il ne sera pas effacé.
2. Quand plusieurs règles d'exclusion s'appliquent à un fichier (par exemple l'une s'appliquant à c:\tmp et l'autre à c:\tmp\folder1), la plus restrictive s'applique : si l'une nécessite une confirmation et l'autre exclut immédiatement, le fichier sera exclu sans confirmation.
3. Les règles d'exclusion sont en vigueur entre la vérification de l'attribut "caché/système" des fichiers et celle de l'attribut "en lecture seule". En d'autres termes, si les règles sont les suivantes :

a. les fichiers cachés/système ne doivent pas être chiffrés

b. une demande de confirmation est nécessaire pour les fichiers verrouillés.

Un fichier pour lequel ces deux règles s'appliquent ne sera pas chiffré sans une demande de confirmation.

7. Transchiffrer des fichiers chiffrés

Cette section décrit comment transchiffrer des fichiers chiffrés.

7.1 Présentation

Stormshield Data File permet de mettre à jour les listes des utilisateurs pouvant accéder à vos fichiers chiffrés par Stormshield Data File. Vous pouvez ajouter ou retirer des utilisateurs. Lors de la mise à jour de la liste des utilisateurs, Stormshield Data File re-chiffre le ou les fichiers avec une nouvelle clé de chiffrement : cette opération est appelée "transchiffrement".

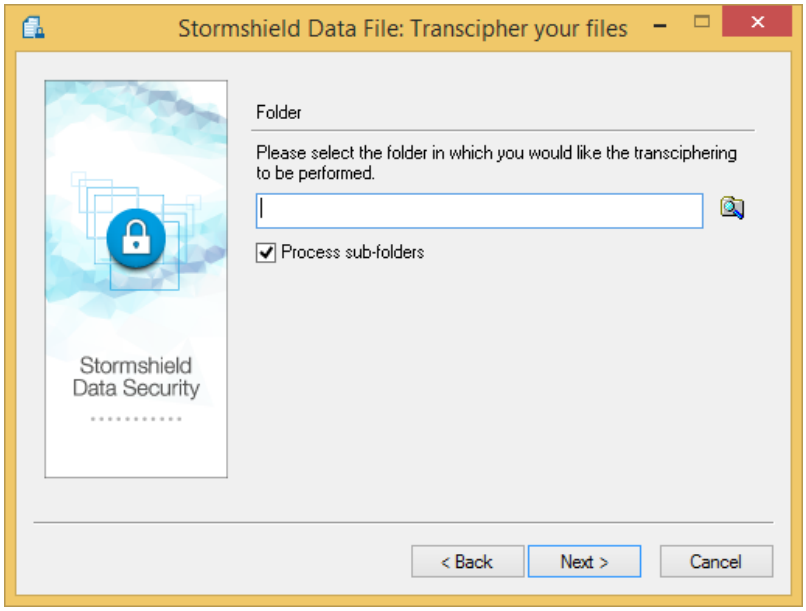
Un fichier chiffré est transchiffré dans son format d'origine : s'il est au format .sbox, il reste au format .sbox après transchiffrement.

7.2 Transchiffrement de fichiers

Avant toute opération de transchiffrement, vous devez vous munir du certificat de l'utilisateur que vous allez ajouter (fichier *.cer* ou *.crt*). Ce certificat peut vous être transmis directement ou être obtenu à partir de votre annuaire de confiance ou d'un annuaire LDAP (consultez le *Guide d'installation et de mise en œuvre*).

Pour lancer l'assistant de transchiffrement de fichiers :

1. Ouvrez le menu **Démarrer** de Windows et choisissez **Programmes > Stormshield Data Security**.
2. Choisissez **Stormshield Data File – Transchiffrer vos fichiers**. L'écran de bienvenue s'affiche :



3. Sélectionnez le dossier contenant les fichiers à transchiffrer. Si vous souhaitez également transchiffrer les sous-dossiers, cochez la case **Appliquer aux sous-dossiers**. Cliquez sur **Suivant**. La liste affichée est issue de votre annuaire de confiance et ne propose que les certificats valides pour l'opération (certificat en cours de validité et dont les usages autorisent le chiffrement).
4. Sélectionnez le certificat des utilisateurs que vous voulez ajouter aux fichiers Stormshield Data File.

Si des utilisateurs ne sont pas présents dans la liste, cliquez sur pour importer dans votre annuaire de confiance leur certificat à partir d'un fichier ou d'un annuaire LDAP.

Cliquez sur **Suivant** .

5. Cliquez **Oui, je reste utilisateur des fichiers traités**, si vous souhaitez continuer à pouvoir lire les fichiers qui vont être transchiffrés.

Autrement, cliquez sur **Non, je me retire de la liste des utilisateurs**, si vous pensez ne plus être amené à lire ces fichiers. Le choix de l'option n'a aucune incidence si vous transchiffrez un fichier :

- avec une clé de délégation. Vous ne serez pas ajouté à la liste des utilisateurs mais vous pourrez toujours y accéder tant que vous serez en possession de la clé de délégation.
- avec une clé privée pour votre usage personnel (suite à un renouvellement de clé ou de compte par exemple). Vous serez ajouté à la liste des utilisateurs autorisés à accéder au fichier.

Cliquez sur **Suivant**.

6. Vérifiez le récapitulatif et cliquez sur **Terminer** : l'assistant recherche alors dans le dossier spécifié tous les fichiers chiffrés avec votre clé, et les transchiffre. Une fois l'opération terminée, un compte-rendu fournit des statistiques en indiquant :

- le nombre de fichiers à traiter
- le nombre de fichiers traités
- le nombre de fichiers pour lesquels l'opération a échoué

Pour chaque fichier/dossier transchiffré, une icône indique le résultat de l'opération :

- : Dossier transchiffré avec succès.
- : Dossier traité avec succès, mais contenant des fichiers n'ayant pas pu être transchiffrés pour l'une des raisons suivantes :
- clé non trouvée (vous n'êtes pas utilisateur de ce fichier) ;
- fichier chiffré avec une clé de déchiffrement.
- : Dossier ne contenant aucun fichier chiffré.
- : Dossier contenant un fichier en erreur.
- : Fichier transchiffré avec succès.
- : Fichier chiffré non transchiffré pour l'une des raisons suivantes :
- clé non trouvée (vous n'êtes pas utilisateur de ce fichier).
- fichier chiffré avec une clé de déchiffrement (délégation).
- : Fichier en erreur.

STORMSHIELD

documentation@stormshield.eu