GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA TEAM

Chiffrement transparent et partagé

Version 10.1

Dernière mise à jour du document : 29 mars 2022

Référence : sds-fr-sd_team-guide_d_utilisation-v10

Table des matières

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

Préface

A propos de ce guide

Ce document fournit les informations essentielles à l'utilisation de Stormshield Data Security Enterprise.

Audience

Ce guide s'adresse :

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

1. Environnement d'utilisation

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

1.1 Recommandations sur la veille sécurité

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

1.2 Recommandations sur les clés et les certificats

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

1.3 Recommandations sur les algorithmes

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

1.4 Recommandations sur les comptes utilisateurs

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

1.5 Recommandations sur les postes de travail

1. Le poste de travail sur lequel Stormshield Data Security est installé doit être sain. Il doit pour cela exister dans l'organisation une politique de sécurité du système d'information dont les exigences sont respectées sur les postes de travail. Cette politique doit notamment prévoir que les logiciels installés soient régulièrement mis à jour et que le système soit protégé contre les virus et autres logiciels espion ou malveillant (pare-feu correctement paramétré, antivirus à jour, etc).

2. La politique de sécurité doit également prévoir que les postes non équipés de Stormshield Data Security n'aient pas accès aux dossiers confidentiels partagés sur un serveur, afin qu'un utilisateur ne puisse pas provoquer un déni de service en altérant ou en supprimant, par inadvertance ou par malveillance, les fichiers protégés par le produit.
3. L'accès aux fonctions d'administration du système du poste est restreint aux seuls administrateurs système.
4. Le système d'exploitation doit gérer les journaux d'événements générés par le produit en conformité avec la politique de sécurité de l'organisation. Il doit par exemple restreindre l'accès en lecture à ces journaux aux seules personnes explicitement autorisées.
5. L'utilisateur doit veiller à ce qu'un attaquant potentiel ne puisse pas observer voire accéder au poste lorsque la session Stormshield Data Security est ouverte.

1.6 Recommandations sur les intervenants

1. L'administrateur de la sécurité est considéré de confiance. Il définit la politique de sécurité de Stormshield Data Security en respectant l'état de l'art, et éventuellement crée les comptes des utilisateurs via l'application Stormshield Data Authority Manager.
2. L'administrateur système est également considéré de confiance. Il est en charge de l'installation et de la maintenance de l'application et du poste de travail (système d'exploitation, logiciels de protection, librairie *PKCS#11* d'interface avec une carte à puce, applications bureautiques et métier, etc). Il applique la politique de sécurité définie par l'administrateur de la sécurité.
3. L'utilisateur du produit doit respecter la politique de sécurité en vigueur dans son organisme.

1.7 Recommandation sur le chiffrement des fichiers

1. L'algorithme de chiffrement des fichiers doit être l'AES.
2. Il n'est pas recommandé de chiffrer un fichier de plus de 2 tera-octets (au-delà de cette taille, le fichier chiffré pourrait présenter des vulnérabilités).

1.8 Environnement de certification et de qualification

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

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

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

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

2. Présentation

Stormshield Data Security Enterprise est une solution de sécurité pour poste de travail sous Microsoft Windows préservant la confidentialité des données partagées, stockées ou échangées par voie de messagerie.

Stormshield Data Security Enterprise offre les fonctions de sécurité suivantes :

- le chiffrement transparent et en temps réel des fichiers ;
- le chiffrement et la signature des courriers électroniques ;
- le chiffrement à la demande des fichiers, en vue d'un transfert par mail ou d'une sauvegarde sécurisée ;
- l'effacement sécurisé et irréversible des données ;
- la signature électronique de fichiers et de dossiers ;
- le chiffrement de disques virtuels.

La solution intègre un outil permettant le paramétrage des fonctions de sécurité et l'administration des utilisateurs et de leurs clés cryptographiques. Stormshield Data Team assure le chiffrement transparent de vos fichiers confidentiels : les fichiers sont chiffrés là où ils se trouvent, en temps réel et de façon transparente pour vos applications bureautiques ou métier.

La protection est assurée selon des règles définies par dossier : tout fichier créé ou déposé dans un “dossier sécurisé” est automatiquement chiffré sans la moindre interaction utilisateur. L'emplacement, le nom et l'extension du fichier restent inchangés.

Stormshield Data Security permet également le partage de données confidentielles entre plusieurs collaborateurs. La “règle de sécurité” spécifiée sur le dossier définit alors les collaborateurs autorisés à lire et modifier les fichiers stockés dans le dossier. La non-révocation d’un collaborateur est vérifiée conformément à la politique de sécurité définie.

Stormshield Data Security peut sécuriser :

- un dossier local à l'ordinateur personnel du collaborateur ;
- un support amovible (une clé USB) en totalité ou partiellement (un ou plusieurs sous-dossiers) ;
- un dossier partagé sur un serveur de fichiers.

Quand une règle de sécurité est définie sur un dossier, elle est appliquée de façon récursive à tous ses éventuels sous-dossiers. Il est néanmoins possible de définir une règle différente sur un sous-dossier bien déterminé. Si aucune règle n’est appliquée sur un fichier ou un dossier avec Stormshield Data Security, le fichier ou le dossier sont créés et s'ouvrent en clair.

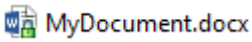
Une fois chiffré, un fichier ne peut être lu, modifié voire effacé que par l'un des collaborateurs autorisés par la règle de sécurité. Toutes les lectures/écritures et chiffrements/déchiffrements de donnée s'effectuent au “fil de l'eau” et en mémoire : aucune copie en clair du fichier n'est créée.

Techniquement, chaque fichier est chiffré à l'aide d'une clé de chiffrement symétrique (AES) qui est propre au fichier. Cette clé est elle-même chiffrée avec la clé publique de chiffrement (RSA) de chaque collaborateur autorisé.

Stormshield Data Security assure également le chiffrement du fichier d'échange du système (le swap ou la mémoire paginée) dans lequel peuvent persister des résidus de données confidentielles.

2.1 Pictogrammes de chiffrement

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

 Confidential	Le pictogramme indique qu'une règle de Stormshield Data Team s'applique sur le dossier. Si le collaborateur fait partie de la liste des personnes autorisées, les fichiers créés, déplacés ou copiés dans ce dossier seront automatiquement chiffrés. Vous pourrez voir le contenu de ce dossier, mais vous ne pourrez pas ouvrir les fichiers chiffrés, sauf si vous en avez la permission. Vous ne pourrez pas non plus créer de fichiers chiffrés dans ce dossier. Si Stormshield Data Team n'est pas installé, vous pouvez accéder normalement à des dossiers et des fichiers sécurisés, mais leur contenu restera chiffré.
 MyDocument Microsoft Word Document 11.8 KB	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	
 MyDocument	

2.2 Mécanismes cryptographiques

Stormshield Data Team met en œuvre des algorithmes et mécanismes cryptographiques standards pour les opérations élémentaires suivantes :

- chiffrement symétrique des données (AES) ;
- chiffrement asymétrique des clés de chiffrement (PKCS#1) ;
- dérivation de clé à partir d'un mot de passe (PKCS#5, PKCS#12) ;
- calcul d'empreinte (SHA-256, SHA-1).

Stormshield Data Team prend en compte les systèmes de gestion de fichiers suivants :

- NTFS ;
- FAT32 ;
- CIFS ;
- DFS ;

Stormshield Data Team supporte les algorithmes suivants :

- AES 256, 192, 128 bits ;
- DES 192, 128, 64 bits.

Les algorithmes supportés et la taille des clés peuvent être restreints en utilisant Stormshield Data Authority Manager.

3. Installation

3.1 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 la suite Stormshield Data Security.

Pour que l'utilisation du module Stormshield Data Team soit la plus performante possible, nous vous recommandons d'organiser le classement de vos fichiers dans une arborescence de dossiers. Moins il y a de fichiers et de sous-dossiers dans un dossier, plus les performances sont optimales.

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

Stormshield Data Team ne fonctionne pas avec un serveur Microsoft Windows utilisant Citrix Server ou Terminal Server.

3.2 Installer Stormshield Data Team

Stormshield Data Team est un composant de Stormshield Data Security, et il est installé avec la Suite.

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

Pour installer Stormshield Data Team, vous devez avoir les droits administrateur et une clé de licence.

Les procédures d'installation et de désinstallation sont détaillées dans le *Guide d'installation et de mise en œuvre*.

3.3 Limitations connues

Le tableau suivant liste les limitations connues pour Stormshield Data Security :

Fonctionnalité	Description
NFS	Les partitions de type NFS ne sont pas supportées.
CSC + DFS	Un dossier disponible hors connexion ne peut pas être sécurisé.
Samba + DFS	Un partage Samba défini comme une racine DFS ne peut pas être sécurisé.
Gestion des versions \ Shadow Copy	Ce système de sauvegarde de volumes, sur lequel repose notamment la gestion des versions sous Windows Explorer, n'est pas supporté par Stormshield Data Team.
FUS	En cas d'utilisation de plusieurs sessions Windows en parallèle, un seul utilisateur peut se connecter à Stormshield Data Security à un instant donné.
Partage d'un répertoire local sécurisé	Le partage en local d'un répertoire chiffré par le module Team n'est pas possible.

Fonctionnalité	Description
Connexion au bureau à distance	En connexion au bureau à distance, l'affichage des propriétés Team via le menu contextuel (Stormshield Data Security > Propriétés) d'un fichier sécurisé dans un dossier sécurisé d'une clé USB engendre une erreur.
Répertoires synchronisés	Les répertoires synchronisés de type SharePoint, Dropbox, Office 365, etc. ne sont pas supportés par Stormshield Data Team et ne peuvent donc pas être sécurisés par le module. Nous vous recommandons d'exclure ces répertoires des dossiers analysés par Stormshield Data Team. Vous pouvez exclure des répertoires grâce à la variable Skipfolder qui contient la liste des dossiers exclus.

4. Utilisation courante

4.1 Sécuriser un dossier

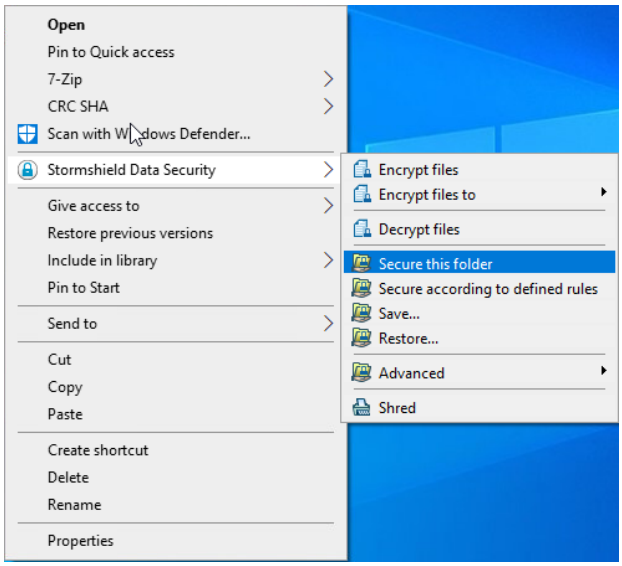
Lorsque vous sécurisez un dossier, vous définissez implicitement ou explicitement une règle de sécurité. Celle-ci est stockée dans les propriétés du dossier concerné. Cela permet, en cas de partage du dossier avec vos collaborateurs, de faciliter la gestion de la liste des collaborateurs autorisés.

NOTE
Les administrateurs doivent noter que les règles de sécurité sont stockées dans un fichier caché (*sboxteam.sbt*). Ce fichier est visible sur une machine sur laquelle Stormshield Data Team n'est pas installé. Ce fichier ne doit pas être supprimé, et il doit être enregistré avec le reste des fichiers Stormshield Data Security.

4.1.1 Sécuriser un dossier en trois clics

Pour sécuriser rapidement un dossier, sans définir de règle de sécurité :

1. Sélectionnez le dossier à l'aide de la souris puis effectuez un clic droit et choisissez **Stormshield Data Security > Sécuriser le dossier** dans le menu contextuel :



2. Confirmez votre choix.

NOTE
Si le collaborateur n'est pas connecté, ou si la session Stormshield Data Security est verrouillée, la fenêtre de connexion/déverrouillage s'affiche. Le collaborateur doit s'authentifier correctement pour continuer l'opération.

Le dossier est sécurisé par une règle ne contenant que le collaborateur connecté en cours. Les fichiers du dossier sont mis à jour et chiffrés.

4.1.2 Sécuriser un dossier en définissant une règle de sécurité

Sécuriser un dossier

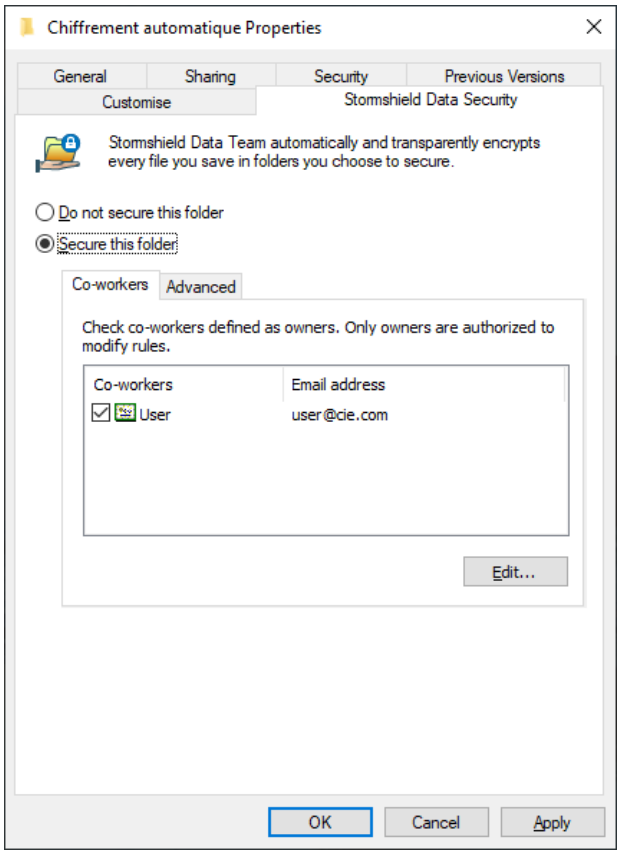
Pour sécuriser un dossier et définir une règle de sécurité :

1. Connectez-vous à Stormshield Data Security.

Pour plus d'informations sur la connexion à Stormshield Data Security, reportez-vous au *Guide d'installation et de mise en œuvre*.

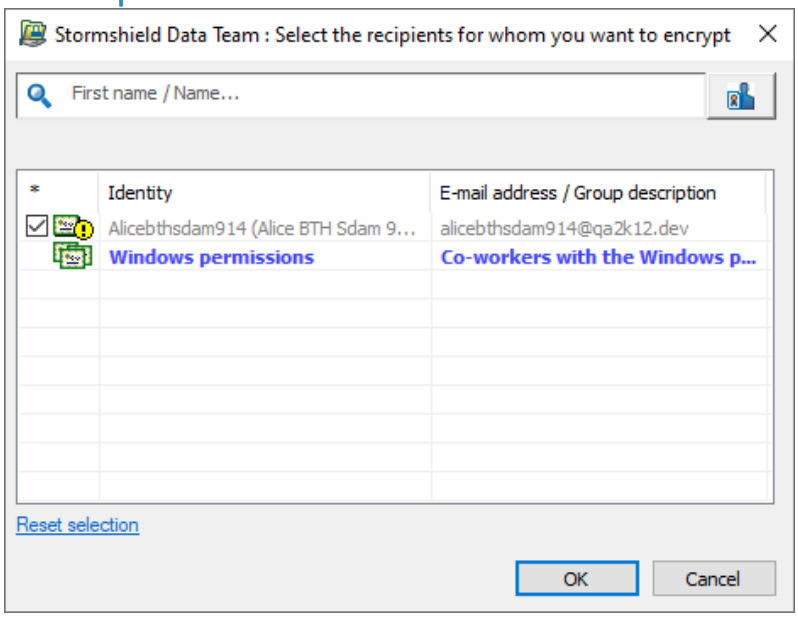
Si Stormshield Data Team est installé mais que vous n'êtes pas connecté à Stormshield Data Security, vous ne pouvez pas créer un nouveau fichier dans un dossier protégé par une règle.

2. Sélectionnez le dossier que vous désirez sécuriser.
3. Cliquez sur le bouton droit puis sélectionnez **Propriétés**.
4. Sélectionnez l'onglet *Stormshield Data Security*.



5. Sélectionnez l'option **Sécuriser ce dossier** pour chiffrer ce dossier (les sous-dossiers sont automatiquement sécurisés).

6. Si vous souhaitez partager votre dossier, cliquez sur le bouton **Modifier** et recherchez les collaborateurs ou les groupes autorisés.
   Les collaborateurs possédant les autorisations Windows sur le dossier concerné sont automatiquement suggérés dans le groupe **Autorisations Windows** si l'option est activée. Vous pouvez cliquer sur le nom du groupe pour supprimer certains collaborateurs du groupe si nécessaire. Pour plus d'informations, reportez-vous à la section Gérer la suggestion automatique de collaborateurs.



7. Cliquez sur **OK** pour fermer la fenêtre de recherche de collaborateurs.
8. Dans la liste des collaborateurs, cochez les propriétaires de la règle. Ce sont les seules personnes autorisées à modifier les accès à ce dossier. Il doit toujours y avoir au moins un propriétaire de règle. Par défaut, la personne qui crée la règle est propriétaire de la règle, mais elle pourra ensuite être définie comme collaborateur autorisé.
9. Cliquez sur **OK** pour enregistrer et appliquer votre règle.

Vous pouvez désormais créer ou déposer des fichiers confidentiels dans ce dossier sécurisé : ils seront automatiquement chiffrés.

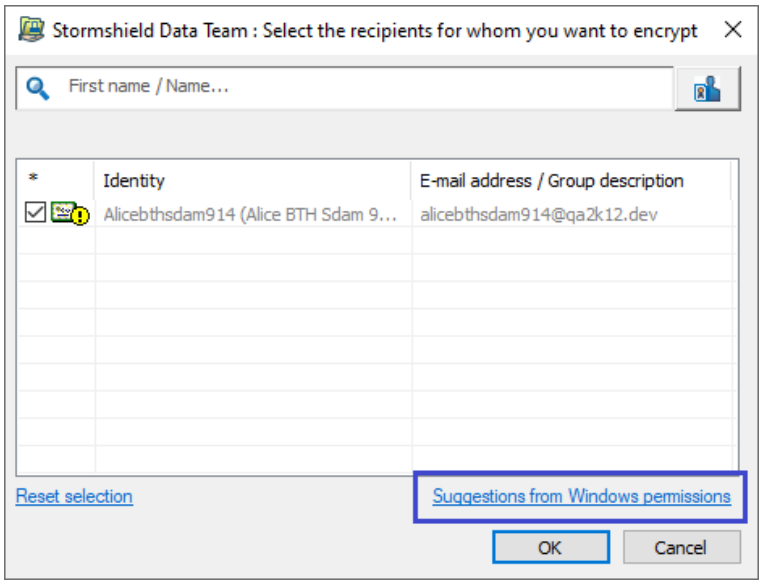
> **NOTE**
> Pour pouvoir sécuriser un dossier ou modifier la liste des collaborateurs autorisés, un collaborateur doit avoir dans son annuaire de confiance les certificats de tous les autres collaborateurs autorisés.

Ajouter ou supprimer des collaborateurs de la règle de sécurité

Pour ajouter ou supprimer des collaborateurs dans une règle de sécurité s'appliquant à un dossier déjà sécurisé :

1. Faites un clic droit sur le dossier concerné.
2. Sélectionnez **Propriétés**.
3. Sélectionnez l'onglet *Stormshield Data Security*.
4. Dans l'onglet **Collaborateurs**, cliquez sur **Modifier**.

5. Recherchez les collaborateurs ou groupes autorisés pour en ajouter de nouveaux ou bien supprimez des collaborateurs de la liste en survolant la ligne du collaborateur et en cliquant sur la croix rouge.
   Cliquez sur le lien **Suggestions via les autorisations Windows** en bas de la fenêtre pour ajouter automatiquement les collaborateurs possédant les autorisations Windows sur le dossier concerné. Vous pouvez cliquer sur le nom du groupe pour supprimer certains collaborateurs du groupe si nécessaire. Ce lien n'est visible que si l'option est activée. Pour plus d'informations, reportez-vous à la section Gérer la suggestion automatique de collaborateurs.

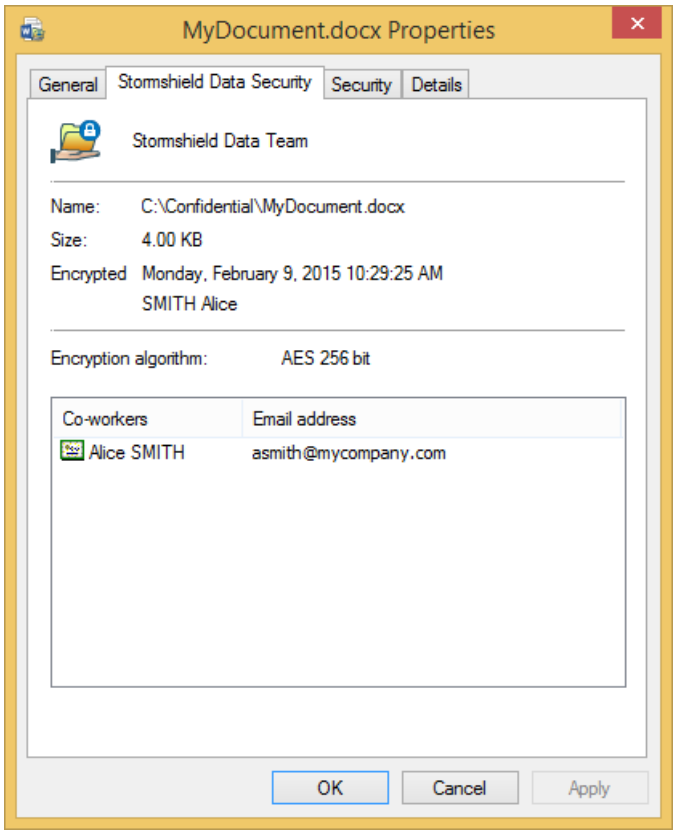


6. Cliquez sur **OK** pour fermer la fenêtre de recherche de collaborateurs.
7. Cliquez sur **OK** pour enregistrer et appliquer votre règle.

4.1.3 Propriétés d'un fichier chiffré

Pour afficher les propriétés d'un fichier chiffré avec une règle de sécurité, dans l'explorateur Windows, sélectionnez le fichier avec le bouton droit de votre souris, et choisissez **Stormshield Data Security** puis **Propriétés** ou bien ouvrez les **Propriétés** du fichier et sélectionnez l'onglet *Stormshield Data Security*.

NOTE
Le sous-menu **Stormshield Data Security** > **Propriétés** n'est plus présent à partir de Windows 10.



Dans l'onglet *Stormshield Data Security*, la taille indiquée inclut les données de sécurité propres à Stormshield Data Security (alors que la taille indiquée dans l'onglet *Général* n'inclut pas ces données de sécurité).

La liste des collaborateurs n'est affichée que si :

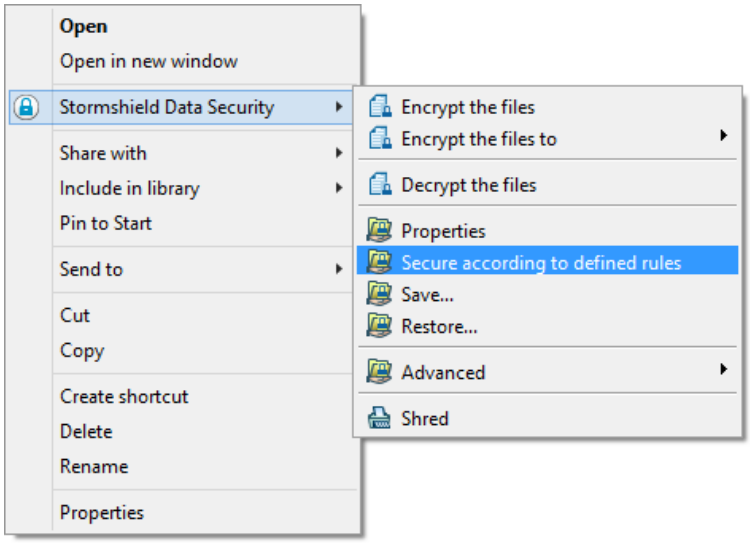
- vous êtes connecté à Stormshield Data Security ;
- vous faites partie de cette liste de collaborateurs.

4.2 Mettre à jour la sécurité d'un dossier

Quand vous définissez ou modifiez une règle de sécurité sur un dossier, vous devez appliquer cette nouvelle règle au dossier afin que tous les fichiers qu'il contient soient chiffrés conformément à cette règle. Stormshield Data Team propose systématiquement d'effectuer cette opération au moment où vous validez la création/modification d'une règle. Cependant, si vous déclinez cette offre, il est toujours possible de le faire plus tard.

Pour appliquer une nouvelle règle ou modifier une règle :

1. Fermez tous les fichiers contenus dans le dossier.
2. Dans l'explorateur, sélectionnez le dossier ou les fichiers à mettre à jour avec le bouton droit de votre souris, et choisissez **Stormshield Data Security**, puis **Sécuriser selon les règles définies**.



NOTE
La mise à jour des fichiers s'interrompt si vous verrouillez ou fermez votre session Stormshield Data Security ou votre session Windows. Cette mise à jour reprend automatiquement quand vous vous reconnectez à Stormshield Data Security. Cette reprise vous est signalée par une info-bulle.

Une fenêtre d'avancement affiche le fichier en cours de traitement et la liste des fichiers en erreur. Les erreurs possibles sont les suivantes :

Libellé	Description
Vous ne faites pas partie des collaborateurs autorisés.	Vous ne pouvez donc pas accéder au fichier.
Accès refusé.	Le fichier est protégé par des permissions Windows, ou bien le fichier est déjà ouvert par un autre logiciel.
Traitement annulé.	Vous avez annulé l'opération.

4.3 Règles et précautions d'usage

4.3.1 Ouvrir un fichier chiffré

Pour voir ou accéder à des fichiers ou des dossiers sécurisés, vous devez d'abord vous connecter à Stormshield Data Security.

NOTE
Pour accéder à un fichier chiffré par une autre personne, vous devez être sur la liste des utilisateurs autorisés.
Selon la politique de sécurité définie par votre administrateur, si votre clé de chiffrement est révoquée, l'accès aux fichiers chiffrés vous est interdit, même si vous faites partie des collaborateurs autorisés.

Une fois connecté à Stormshield Data Security, vous pouvez ouvrir et enregistrer les fichiers chiffrés avec les applications habituelles.

NOTE
Si vous tentez d'ouvrir un fichier chiffré alors que vous n'en avez pas la permission, un message d'avertissement s'affiche. Contactez le propriétaire du fichier ou du dossier.

4.3.2 Créer un fichier dans un dossier sécurisé

Vous devez être connecté à Stormshield Data Security et faire partie de la liste des utilisateurs autorisés pour pouvoir créer un fichier chiffré dans un dossier sécurisé. Pour plus d'informations sur la façon de se connecter à Stormshield Data Security, reportez-vous au *Guide d'installation et de mise en œuvre*.

4.3.3 Copier ou déplacer un fichier

IMPORTANT
Ne copiez jamais ou ne déplacez jamais un fichier chiffré vers un dossier non sécurisé, sinon votre fichier sera enregistré en clair. Si vous voulez déplacer le fichier et conserver son chiffrement, ou bien créer une copie de sauvegarde chiffrée elle aussi, reportez-vous à la section Sauvegarder un fichier chiffré.

Il est également possible de chiffrer le fichier en utilisant Stormshield Data File directement dans le dossier sécurisé par Stormshield Data Team, avant de copier ou de déplacer le fichier.

4.3.4 Supprimer un fichier

Pour pouvoir supprimer un fichier chiffré, il faut faire partie de ses utilisateurs autorisés.

Quand vous supprimez un fichier chiffré sous Windows, il reste chiffré dans la corbeille.

4.3.5 Fichiers disponibles hors connexion

Si vous sécurisez un dossier “disponible hors connexion”, les fichiers du dossier sont chiffrés au niveau du dossier partagé sur le réseau mais également sur votre poste, dans le dossier local dans lequel ils sont recopiés.

4.3.6 Verrouiller la session

Quand la session de Stormshield Data Security est verrouillée, les instances des fichiers ouverts restent accessibles pour les applications. Cependant, les applications ne peuvent pas ouvrir d'autres fichiers protégés même si elles accèdent déjà à des fichiers protégés. Cela permet aux applications (Microsoft Outlook par exemple) de rester actives même si la session de Stormshield Data Security est verrouillée.

Pour plus d'informations sur le verrouillage d'une session de Stormshield Data Security, reportez-vous au *Guide d'installation et de mise en œuvre*.

4.3.7 Se déconnecter de Stormshield Data Security

Quand vous vous déconnectez de Stormshield Data Security, les instances des fichiers ouverts deviennent inaccessibles pour les applications. Toutes les tentatives pour accéder aux fichiers protégés aboutiront à un message d'erreur. Il est recommandé de fermer toutes les applications faisant appel à des fichiers protégés avant de fermer la session de Stormshield Data Security.

4.3.8 Cas particuliers

Il est possible d'avoir des fichiers chiffrés dans un dossier non sécurisé, ou d'avoir des fichiers non chiffrés dans un répertoire sécurisé. Ce cas se produit notamment dans les cas suivants :

- en cas de déplacement de dossiers ;
- si le chiffrement initial est interrompu ;
- en cas de sauvegarde (avec le menu Stormshield Data Security) de fichier chiffré/non chiffré.

4.4 Visualiser les règles connues

Vous pouvez à tout moment visualiser l'ensemble des règles Team connues de l'utilisateur Stormshield Data Security.

Dans la barre des tâches, cliquez avec le bouton droit de la souris sur l'icône de Stormshield Data Security.

1. Cliquez sur *Propriétés*.
2. Dans l'onglet **Configuration**, double-cliquez sur l'icône Stormshield Data Team.
3. Cliquez sur l'onglet **Règles de sécurité**.
4. La liste des règles connues s'affiche dans la partie supérieure de la fenêtre. Sélectionnez une règle pour voir la liste des collaborateurs et propriétaires de la règle.

   NOTE
   Si le nombre de collaborateurs présents sur un règle est élevé (supérieur à 100), l'affichage de la liste des collaborateurs peut être long (entre cinq et dix secondes selon le système).

5. Utilisation avancée

5.1 Sauvegarder un fichier chiffré

Si vous souhaitez faire une sauvegarde d'un fichier chiffré ou d'un dossier sécurisé, vous NE devez surtout PAS utiliser la fonction Enregistrer de Windows ou glisser et déposer votre fichier sur votre support de sauvegarde non sécurisé (clé USB ou CD ou DVD réinscriptible) : votre fichier confidentiel serait alors copié en clair.

Pour copier un fichier chiffré et garder le chiffrement, procédez comme suit :

1. Dans l'explorateur Windows, sélectionnez le fichier ou dossier à archiver avec le bouton droit de votre souris, et choisissez **Stormshield Data Security**, puis **Sauvegarder**.

Vous pouvez sélectionner plusieurs fichiers ou dossiers en même temps.

2. Sélectionnez le dossier destination de la sauvegarde.
3. Cliquez sur **OK** : le fichier sélectionné est copié chiffré dans le dossier de destination. La hiérarchie dans l'arborescence des dossiers est maintenue.

Il n'est pas nécessaire que vous soyez connecté à Stormshield Data Security pour effectuer une sauvegarde.

> **NOTE**
> Par défaut, Stormshield Data Security est configuré pour refuser l'ouverture d'un fichier chiffré stocké dans un dossier non sécurisé (reportez-vous à la section Configurer Stormshield Data Team).

5.2 Restaurer un fichier chiffré

Pour pouvoir récupérer un fichier sauvegardé chiffré, vous devez le restaurer sur un dossier sécurisé :

1. Sélectionnez le dossier ou les fichiers à restaurer avec le bouton droit de votre souris, et choisissez **Stormshield Data Security**, puis **Restaurer**.
2. Sélectionnez le dossier destination de la restauration : vous ne pouvez sélectionner qu'un dossier sécurisé.
3. Cliquez sur **OK** : le fichier sélectionné est copié chiffré dans le dossier sécurisé saisi.

5.3 Désécuriser un dossier (déchiffrer)

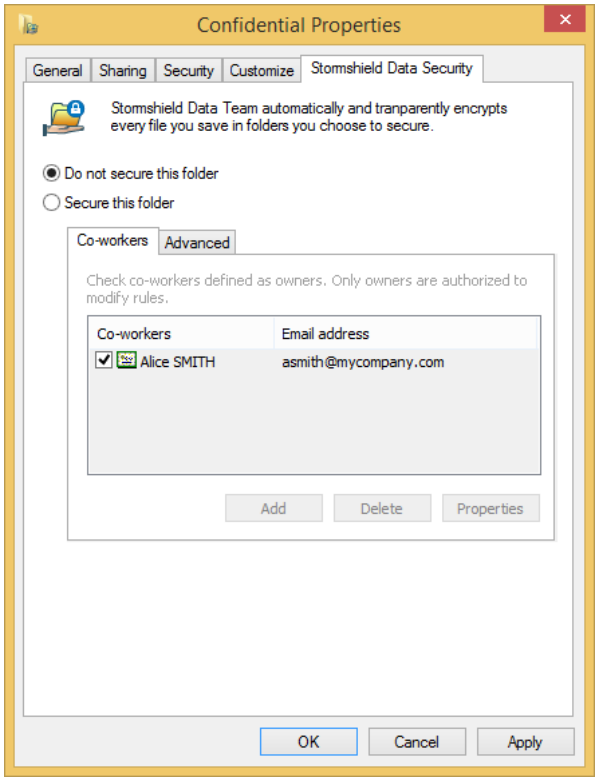
Pour désécuriser un dossier, suivez la procédure suivante :

1. Il s'agit d'abord de supprimer la règle indiquant que le dossier contient des documents chiffrés. Pour cela, faites un clic droit sur le dossier sécurisé (signalé par l'icône Stormshield Data Security), puis sélectionnez les menus **Stormshield Data Security** et **Propriétés**.

La page de propriétés apparaît indiquant l'état de sécurisation du dossier, les personnes ayant accès à ce dossier (les collaborateurs) et les personnes ayant l'autorisation de modifier les options de sécurité (les propriétaires).

2. Pour désécuriser le dossier, cliquez sur **Ne pas sécuriser ce dossier** puis sur **OK**.

Seuls les propriétaires d'une règle sont autorisés à la supprimer.



3. La fenêtre suivante vous invite à confirmer la désécurisation. Cliquez sur **Oui**.
4. Commence alors le déchiffrement des fichiers contenus dans le dossier. Une barre de progression s'affiche.

Si des fichiers sont en erreur, c'est-à-dire qu'ils n'ont pas été déchiffrés (par exemple en raison d'un accès refusé), ils sont listés dans la partie Détail (cliquez sur **Détail**).

5. Cliquez sur **Fermer**. La règle de sécurité a été supprimée et les fichiers contenus dans le dossier sont maintenant en clair.

5.4 Désécuriser des fichiers (déchiffrer)

Il n'est pas possible de désécuriser des fichiers dans un dossier sécurisé. En revanche, dans les cas suivants, des fichiers chiffrés peuvent se trouver dans un dossier non sécurisé et vous pouvez avoir besoin de les déchiffrer :

- Après une désécurisation d'un dossier (décrit dans la section précédente) sans déchiffrement des fichiers. C'est le cas lorsque l'administrateur a répondu **Non** à la question **Voulez-vous désécuriser, c'est à dire remettre en clair les fichiers chiffrés de ce dossier ?**.
- Après une sauvegarde de fichier effectuée par le menu Stormshield Data Security.

1. Pour désécuriser un fichier ou un ensemble de fichiers, sélectionnez-les dans l'explorateur.
2. Cliquez avec le bouton droit et choisissez : **Stormshield Data Security**, puis **Avancé**, puis **Désécuriser**.

Une fenêtre d'avancement affiche alors la liste des fichiers désécurisés (déchiffrés).

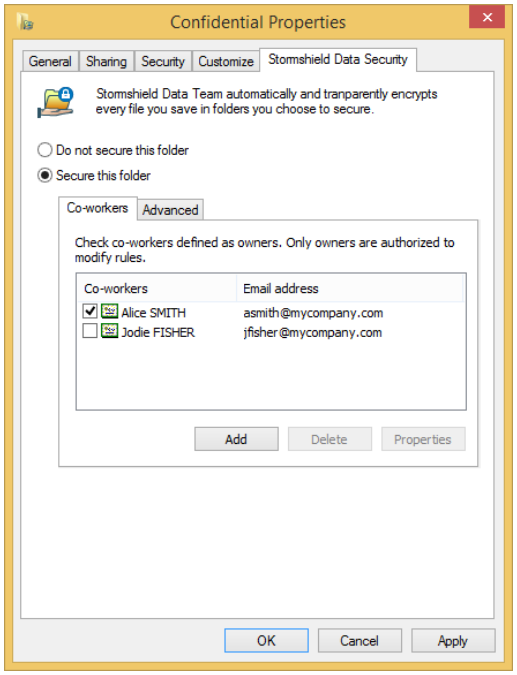
Une fois désécurisé, le contenu du fichier apparaît en clair et tout le monde peut y accéder, le lire, le modifier et supprimer ce fichier.

5.5 Définir une règle de sécurité différente sur un sous-dossier

Lorsqu'un dossier est sécurisé, tous ses sous-dossiers sont également sécurisés par défaut, en utilisant la même règle. Cependant, vous pouvez définir des règles spécifiques pour un sous-dossier qui l'emporteront sur les règles de sécurité du dossier parent.

Procédez comme suit :

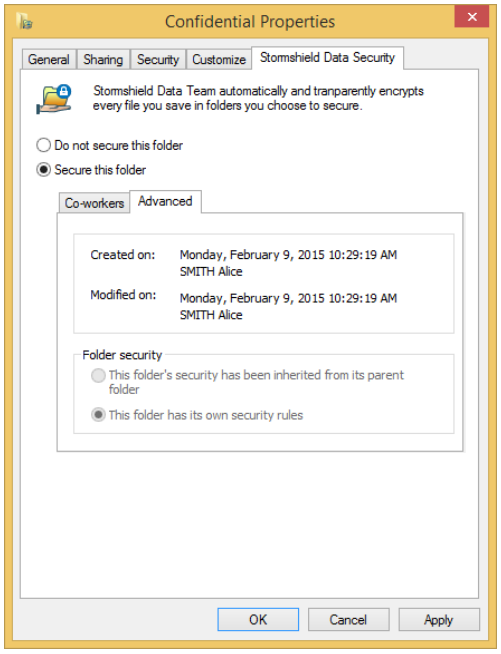
1. Dans l'Explorateur Windows, cliquez avec le bouton droit de votre souris sur le dossier et sélectionnez **Propriétés**.
2. Cliquez sur l'onglet *Stormshield Data Security*.



Vous pouvez voir les utilisateurs autorisés dans la liste des collaborateurs. Le nom des propriétaires est coché.

3. Si vous sélectionnez l'onglet *Avancé*, vous verrez des informations sur la personne qui a créé la règle sur ce dossier.

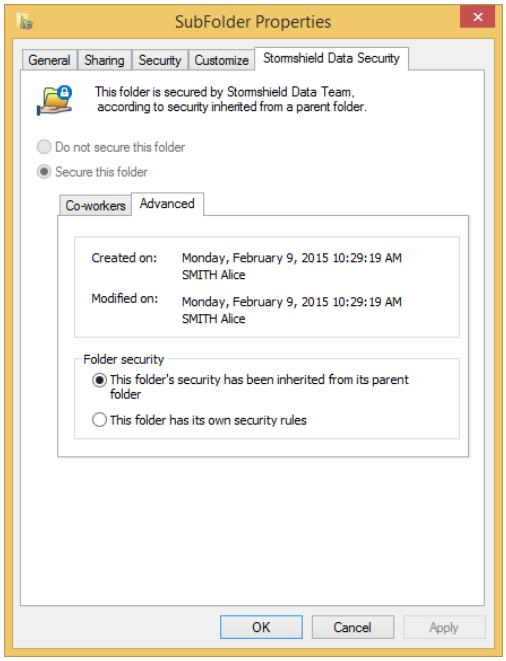
- Pour un dossier racine sur lequel une règle de sécurité est explicitement définie, la page suivante est affichée :



NOTE

Si vous êtes répertorié comme propriétaire, vous pouvez désécuriser le dossier depuis cette fenêtre de propriétés, en sélectionnant **Ne pas sécuriser ce dossier**. Pour plus d'informations, reportez-vous à la section Désécuriser un dossier (déchiffrer).

- Pour un sous-dossier, la page suivante est affichée :



En utilisant les boutons radio de la section **Sécurité du dossier**, vous pouvez indiquer si le sous-dossier hérite des règles de son dossier parent, ou s'il a ses propres règles.

- Quand des règles de sécurité sont définies pour un dossier, les nouveaux fichiers créés dans ce dossier sont chiffrés automatiquement, sans nécessiter d'action supplémentaire.
- Quand un dossier est sécurisé, tous ses sous-dossiers sont également sécurisés par défaut, en utilisant la même règle. Cependant vous pouvez définir des règles spécifiques pour un sous- dossier qui l'emporteront sur les règles de sécurité du dossier parent.

- Si un dossier sécurisé est déplacé, les règles de sécurité restent les mêmes. Cependant, si le sous-dossier est chiffré grâce à une règle de sécurité héritée d'un dossier parent, dans ce cas il n'héritera pas de la règle dans sa nouvelle localisation ; par contre, les fichiers existants gardent leur chiffrement courant (même si les utilisateurs autorisés du dossier cible sont différents). S'il est déplacé en un lieu non sécurisé, le dossier sera non sécurisé, mais les fichiers déplacés restent chiffrés.
- Si vous déplacez un dossier dans un dossier déjà sécurisé, les fichiers contenus dans le dossier d'origine ne seront pas chiffrés automatiquement.
- Il n'est pas possible d'avoir un dossier non sécurisé à l'intérieur d'un dossier sécurisé.
- Vous ne pouvez pas chiffrer le contenu des dossiers suivants ainsi que leurs sous-dossiers :
- le dossier de Windows (par exemple **c:\windows**) ;
- le dossier système (par exemple **c:\windows\system32**) ;
- le dossier des logiciels (par exemple **c:\program_files**).
- Si vous copiez ou déplacez un fichier chiffré vers un dossier non sécurisé, votre fichier est copié en clair. Si vous souhaitez faire une sauvegarde sécurisée de votre fichier, reportez-vous à la section Sauvegarder un fichier chiffré.
- Les fichiers peuvent avoir des règles différentes de celles du dossier qui les contient. Par exemple Franck, Diane et Alice peuvent avoir accès au dossier X, mais seuls Franck et Diane peuvent accéder à un fichier contenu dans ce dossier. Ceci se produit quand la modification d'une règle n'est pas appliquée.
- Si des fichiers sont déjà stockés dans un dossier avant qu'une règle ne soit définie (ou bien si vous modifiez la règle déjà établie), vous devez mettre à jour la sécurité des fichiers déjà stockés dans ce dossier comme indiqué dans la section Sécuriser un dossier en trois clics.

5.6 Supprimer des fichiers chiffrés

Seuls des utilisateurs autorisés peuvent supprimer des fichiers chiffrés. Les fichiers chiffrés que vous supprimez par la commande Windows **Supprimer**, ou par la touche **Supprimer** du clavier, sont déposés dans la corbeille, mais sont toujours chiffrés.

Si vous n'êtes pas un collaborateur autorisé et que vous souhaitez supprimer complètement des fichiers chiffrés, vous devez utiliser la fonction de suppression Stormshield Data Security.

1. Cliquez avec le bouton droit sur le fichier ou dossier dans l'explorateur.
2. Choisissez **Stormshield Data Security**, puis **Avancé**, puis **Supprimer**.

Une fenêtre d'avancement affiche alors la liste des fichiers traités.

Un fichier ainsi supprimé n'est pas déposé dans la corbeille : il est définitivement supprimé.

5.7 Réparer une règle

Une règle de sécurité est techniquement stockée dans un fichier privé caché dans le dossier en question. Quand vous accédez à un dossier sécurisé par une règle, Stormshield Data Security stocke dans votre compte le contenu de ce fichier technique afin de pouvoir détecter les attaques suivantes :

- effacement du fichier technique ;
- modification par un tiers non autorisé de la règle (ajout, suppression d'un collaborateur) ;
- remplacement du fichier technique par celui d'une une autre règle valide, mais prévue pour un autre dossier

Certains de ces événements peuvent également être la conséquence, non pas d'une attaque, mais d'un cas d'usage exceptionnel tel que le suivant :

- suppression du dossier ;
- création d'un nouveau dossier portant le même nom ;
- éventuellement définition d'une nouvelle règle.

En cas de suspicion d'attaque, Stormshield Data Security interdit tout accès au dossier concerné. Pour rétablir l'accès au dossier :

1. Dans l'Explorateur Windows, cliquez avec le bouton droit sur le fichier et sélectionnez Propriétés.
2. Cliquez sur l'onglet *Stormshield Data Security*.
3. Cliquez sur **Restaurer** pour recopier dans le dossier la règle stockée dans votre compte.
4. Ou cliquez sur **Actualiser** pour accepter la règle définie sur le dossier et la recopier dans votre compte.

5.8 Configurer Stormshield Data Team

Une fois installé, vous pouvez modifier la configuration de Stormshield Data Team :

1. Dans la barre de tâches, cliquez avec le bouton droit sur l'icône de Stormshield Data Security.
2. Cliquez sur l'onglet *Configuration*.
3. Double-cliquez sur l'icône Team.
4. Ouvrez l'onglet *Avancé*.

Les options de configuration avancées sont décrites dans les sections suivantes.

> **NOTE**
> Les options de configuration avancées peuvent être renforcées en utilisant la console d'administration Stormshield Data Authority Manager. Pour plus d'informations, reportez-vous à la documentation de Stormshield Data Authority Manager.

5.8.1 Fermer la fenêtre de compte-rendu

Quand vous appliquez la sécurité d'un dossier (reportez-vous à la section Mettre à jour la sécurité d'un dossier) ou quand vous sauvegardez ou restaurez des fichiers (reportez-vous à la section Sauvegarder un fichier chiffré), une fenêtre de compte-rendu affiche la liste des fichiers traités :

- choisissez **Jamais** pour que cette fenêtre ne se ferme pas automatiquement : vous devez vous-même la fermer ;
- choisissez **Toujours** pour que cette fenêtre se ferme automatiquement ;
- choisissez **Si aucun avertissement** pour que cette fenêtre se ferme automatiquement uniquement si aucune erreur n'est intervenue. Au moindre avertissement ou à la moindre erreur, la fenêtre reste affichée : vous devez vous-même la fermer.

5.8.2 Ouverture/suppression d'un fichier chiffré dans un dossier non sécurisé

Certaines applications telles que Microsoft Word ou Excel crée un fichier temporaire dans le même dossier que le fichier chiffré déjà ouvert.

IMPORTANT
Si vous ouvrez un fichier chiffré dans un dossier non sécurisé, des fichiers temporaires en clair seront créés dans ce dossier. Quand vous enregistrez et fermez le fichier, le fichier temporaire en clair remplace le fichier chiffré original. De plus, même si vous n'enregistrez pas le fichier, le fichier temporaire en clair qui a été supprimé reste sur votre ordinateur et peut être récupéré à l'aide d'outils spécialisés.

C'est pourquoi il est fortement recommandé de choisir l'option **Refuser** afin d'interdire l'ouverture ou la suppression d'un fichier chiffré dans un dossier non sécurisé.

Si vous choisissez **Autoriser en lecture seule**, un fichier chiffré peut être lu, mais pas modifié. Mais il n'est pas exclu que des fichiers temporaires soient quand même créés, et que vous deviez les supprimer vous-même.

Si vous choisissez **Autoriser**, un fichier chiffré dans un dossier non sécurisé peut être lu et modifié. Des fichiers temporaires peuvent être également créés, et vous devrez les supprimer vous-même.

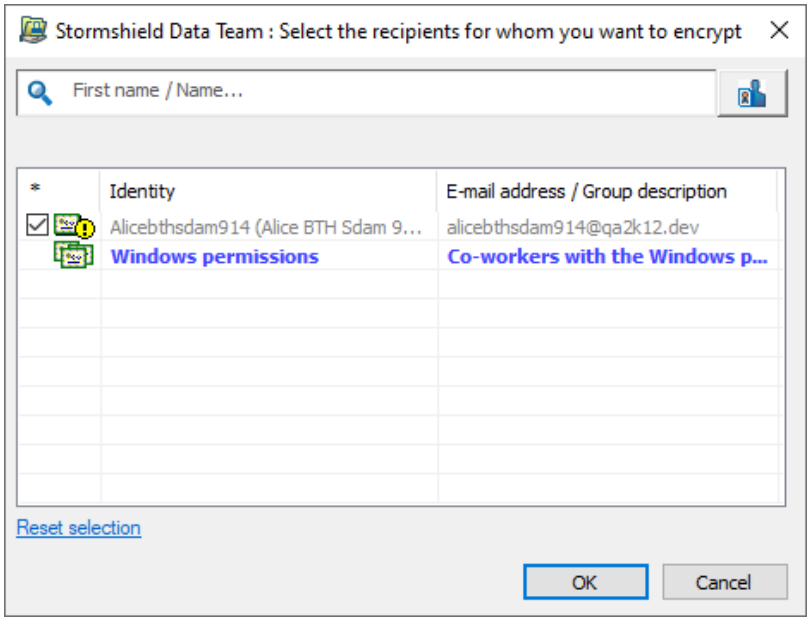
NOTE
La prise en compte de l'option sélectionnée (**Refuser**, **Autoriser en lecture seule** ou **Autoriser**) nécessite une déconnexion puis une reconnexion à Stormshield Data Security.

5.9 Mise à jour automatique des règles

Lorsque qu'un collaborateur change de clé de chiffrement, toutes les règles Team dans lesquelles se trouve son certificat de chiffrement doivent être mises à jour. Il est possible de mettre à jour toutes les règles connues par un utilisateur avec Stormshield Data Authority Manager (consultez le guide d'utilisation de Stormshield Data Authority Manager). Cette mise à jour des règles n'est possible que si l'utilisateur fait partie des propriétaires de la règle.

5.10 Gérer 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**.



Cette suggestion automatique fonctionne si les deux conditions suivantes sont réunies :

- l'annuaire LDAP est correctement configuré. Pour plus d'informations, reportez-vous au guide de Stormshield Data Authority Manager.
- les utilisateurs retrouvés via les autorisations Windows possèdent un certificat valide dans l'annuaire Active Directory.

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

HKEY_LOCAL_MACHINE\SOFTWARE\Arkoon\Security BOX Enterprise\Kernel\SuggestCoworkersThroughACL

Choisissez le type DWORD et la valeur "0".

6. Cas d'erreurs fonctionnelles

Ce chapitre liste les cas d'erreurs fonctionnelles rencontrés lors de l'utilisation de Stormshield Data Security Enterprise.

NOTE
Dans les tableaux suivants, le terme **Journalisation** signifie qu'un événement a été enregistré dans l'observateur d'événements de Microsoft Windows.

Création d'un fichier refusée	
Circonstance	Vous tentez de créer un fichier dans un dossier sur lequel une règle de sécurité est définie, dans un des cas suivants : • vous n'êtes pas connecté à Stormshield Data Security ; • vous êtes révoqué ; • vous ne faites pas partie des utilisateurs autorisés par la règle de sécurité.
Effet	L'application se voit refuser la création du fichier (“Accès refusé”). Le message d'erreur dépend de l'application.
Journalisation	Non

Ouverture d'un fichier refusée	
Circonstance	Vous tentez d'ouvrir un fichier dans un des cas suivants : • le fichier est dans un dossier sur lequel une règle de sécurité est définie et : • vous n'êtes pas connecté à Stormshield Data Security ; • vous êtes révoqué ; • vous ne faites pas partie des utilisateurs autorisés par la règle de sécurité. • Le fichier est chiffré et : • vous n'êtes pas connecté à Stormshield Data Security ; • vous êtes révoqué ; • vous ne faites pas partie des utilisateurs autorisés par la règle de sécurité ; • le fichier est dans un dossier non sécurisé et la politique de sécurité interdit l'ouverture d'un fichier chiffré dans un dossier non sécurisé.
Effet	L'application se voit refuser l'ouverture du fichier (“Accès refusé”). Le message d'erreur dépend de l'application.
Journalisation	Non

Sauvegarde ou Restauration d'un fichier refusée	
Circonstance	Vous sauvegardez ou restaurez un ou plusieurs fichiers dans un dossier sur lequel il n'a pas les permissions (gérées par le système de fichier natif).
Effet	La copie est en échec. Dans le compte-rendu, le ou les fichiers en échec apparaissent avec l'erreur “Accès refusé” et une icône d'erreur.

Sauvegarde ou Restauration d'un fichier refusée	
Journalisation	Oui

documentation@stormshield.eu