GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

GUIDE D'UTILISATION AVANCÉE

Version 11.1

Dernière mise à jour du document : 4 avril 2024

Référence : sds-fr-sdse-guide_d_utilisation_avancée-v11.1

Table des matières

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

1. Avant de commencer

Ce guide, à destination des administrateurs, contient les informations nécessaires à l'utilisation de la solution SDS Enterprise sur les postes de travail des utilisateurs. Il décrit l'utilisation simple et avancée des fonctionnalités de SDS Enterprise.

SDS Enterprise assure la protection et la confidentialité des données stockées sur les répertoires locaux, partagés, ou dans le Cloud, en s'appuyant sur le chiffrement de bout en bout transparent et intégré aux outils de communication et de collaboration. Il permet également de maîtriser l'accès aux données protégées selon les groupes et les profils des utilisateurs.

L'agent SDS Enterprise installé sur les postes des utilisateurs fournit les fonctionnalités suivantes :

- le chiffrement transparent et en temps réel des fichiers, en vue d'un transfert par mail ou d'une sauvegarde sécurisée,
- le chiffrement automatique de fichiers stockés dans des dossiers locaux ou dans des dossiers d'espaces synchronisés avec les hébergeurs en ligne OneDrive, DropBox, SharePoint et Oodrive,
- le chiffrement et la signature des courriers électroniques permettant de protéger les données qu'ils contiennent et de garantir leur provenance et l'intégrité de leur contenu,
- le partage des dossiers chiffrés sur le réseau de l'entreprise avec des collaborateurs,
- l'effacement sécurisé et irréversible des données,
- la signature électronique de fichiers et de dossiers, permettant de garantir leur provenance et l'intégrité de leur contenu,
- le chiffrement de disques virtuels, permettant de stocker des documents protégés. Ces disques virtuels peuvent être partagés entre collaborateurs.

La console d'administration SDMC permet de paramétrer l'utilisation des fonctionnalités sur les postes de travail. Pour plus d'informations, reportez-vous au *Guide d'administration SDS Enterprise*.

2. Se connecter à SDS Enterprise

Après avoir été installé, l'agent SDS Enterprise démarre chaque fois que l'utilisateur démarre Windows.

Afin d'utiliser les fonctionnalités de SDS Enterprise, l'utilisateur doit se connecter à SDS Enterprise. Pour cela, il doit disposer d'un compte utilisateur correctement configuré. Pour plus d'informations sur la création de compte, reportez-vous au *Guide d'administration SDS Enterprise*.

Plusieurs utilisateurs peuvent partager le même poste de travail, mais un seul utilisateur à la fois peut être connecté et peut utiliser SDS Enterprise. Une politique de sécurité SDS Enterprise s'applique à tous les utilisateurs du poste.

Lorsque l'utilisateur se connecte à SDS Enterprise, son identité est vérifiée et ses clés et paramètres sont accessibles.

En mode carte ou token, l'utilisateur insère simplement sa carte ou token pour ouvrir le menu SDS Enterprise. La fenêtre de connexion s'ouvre directement si la carte ou token est déjà inséré dans le lecteur. Si vous utilisez une carte à puce virtuelle, connectez-vous comme décrit ci-dessous.

Pour se connecter à SDS Enterprise :

1. Double-cliquez sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Entrez le mot de passe ou le code confidentiel, en fonction du type de compte.
3. Cliquez sur **Valider**.

ATTENTION
Si vous saisissez consécutivement trop de codes erronés (par défaut : 3), votre compte se bloque. Pour le débloquer, reportez-vous au reportez-vous au *Guide d'administration SDS Enterprise*.

Si vous utilisez le type de compte Single Sign-on (SSO), la connexion de l'utilisateur est automatique et transparente.

3. Verrouiller le compte SDS Enterprise ou se déconnecter

Par mesure de sécurité, l'utilisateur doit verrouiller ou se déconnecter de son compte SDS Enterprise lorsqu'il s'éloigne du poste de travail afin de bloquer l'accès aux fonctionnalités SDS Enterprise.

Lorsque l'utilisateur verrouille sa session Windows ou met son poste de travail en veille, le compte SDS Enterprise peut être automatiquement verrouillé ou déconnecté selon les paramètres choisis dans SDMC. Pour plus d'informations, reportez-vous au *Guide d'administration SDS Enterprise*.

3.1 Verrouiller le compte SDS Enterprise

Le verrouillage du compte interdit l'accès aux clés. L'utilisateur ne peut donc plus accéder aux données chiffrées, mais il peut continuer d'utiliser les fichiers déjà ouverts par Stormshield Data Team par exemple.

La procédure de verrouillage est la même pour le mode mot de passe ou le mode carte ou token. Le retrait de la carte ou token du lecteur permet également le verrouillage de la session. En réinsérant la carte ou le token, vous accédez directement à l'écran de déverrouillage.

Pour verrouiller le compte :

1. Faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Cliquez sur **Verrouiller**. L'icône SDS Enterprise devient rouge  et l'accès au compte n'est plus possible.

Lorsque le compte est verrouillé, accédez au déverrouillage par le même menu.

3.2 Se déconnecter du compte SDS Enterprise

La déconnexion ne peut se faire que lorsque l'utilisateur est connecté (icône verte) ou le compte verrouillé (icône rouge).

La déconnexion correspond à la fermeture du compte SDS Enterprise. Les fonctionnalités de SDS Enterprise sont inutilisables. Nous vous recommandons de fermer les fichiers et applications concernés avant la déconnexion.

La procédure de déconnexion est la même pour le mode mot de passe ou le mode carte ou token. Après déconnexion, si vous réinsérez la carte ou le token, vous accédez à l'écran de connexion.

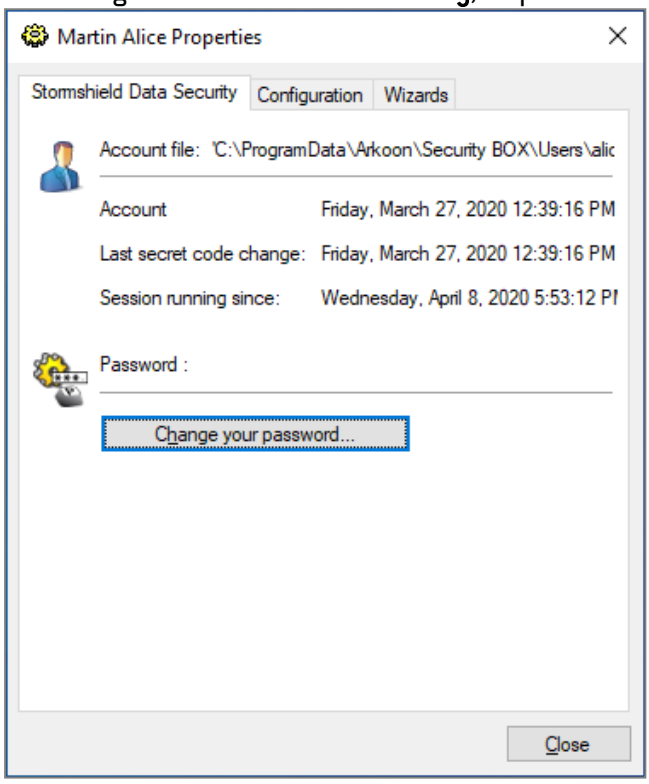
Pour vous déconnecter :

1. Faites un clic droit sur l'icône SDS Enterprise  depuis la barre des tâches Windows.
2. Cliquez sur **Déconnecter**. L'icône SDS Enterprise devient grise  .

4. Modifier le mot de passe du compte SDS Enterprise

Pour les comptes de type Mot de passe, l'utilisateur peut modifier manuellement son mot de passe.

1. Faites un clic droit sur l'icône SDS Enterprise depuis la barre des tâches Windows.
2. Choisissez **Propriétés**.
3. Dans l'onglet **Stormshield Data Security**, cliquez sur **Changer votre mot de passe**.



4. Saisissez votre mot de passe actuel puis deux fois votre nouveau mot de passe.

SDS Enterprise différencie les majuscules des minuscules. Par exemple, le mot de passe Dupont-1 est différent du mot de passe dupont-1. SDS Enterprise analyse le mot de passe et en évalue la force.

5. Sécuriser des fichiers

La fonctionnalité Stormshield Data File permet de garantir la confidentialité des données que vos utilisateurs manipulent tous les jours. Il 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 le disque.

Outre le chiffrement, la fonctionnalité Stormshield Data File permet la compression des fichiers avant leur chiffrement.

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

- Les fichiers peuvent être chiffrés par l'utilisateur pour lui-même ou un groupe de correspondants grâce à l'utilisation de clés publiques. 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.

Pour des informations sur le paramétrage de Stormshield Data File dans SDMC, reportez-vous au *Guide d'administration SDS Enterprise*.

5.1 Connaître le composant Security BOX SmartFILE

La fonctionnalité Stormshield Data File comprend le composant Security BOX SmartFILE qui permet de chiffrer des fichiers au format Security BOX SmartFILE afin de les partager avec des correspondants ne disposant que de l'application Security BOX SmartFILE.

L'opération est accessible dans le menu contextuel SDS Enterprise: **Stormshield Data Security** > **Security BOX SmartFILE**.

5.2 Chiffrer et déchiffrer des fichiers

Cette section décrit comment :

- Chiffrer des fichiers pour l'utilisateur lui-même
- Chiffrer des fichiers pour un ou plusieurs correspondants
- Déchiffrer des fichiers
- Générer des fichiers chiffrés au format Security BOX SmartFILE

Cette section décrit également comment récupérer un mot de passe utilisé pour le chiffrement de fichiers au format Security BOX SmartFILE.

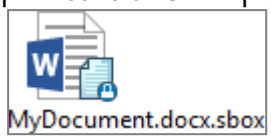
5.2.1 Chiffrer un ou plusieurs fichiers

Cette section décrit comment chiffrer des fichiers que :

- l'utilisateur sera seul à utiliser
- l'utilisateur partagera avec un ou plusieurs correspondants.

Les fichiers chiffrés par Stormshield Data File se repèrent :

- par l'icône en sur-impression apposée à l'icône d'origine :



- par les extensions *.sdsx* ou *.sbox*.

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.

Pour chiffrer un ou plusieurs fichiers :

1. Sélectionnez le ou les fichiers puis faites un clic droit et sélectionnez le menu **Stormshield Data Security** > **Protéger** ou **Protéger les fichiers**.
   La fenêtre **Choix de vos correspondants** s'affiche avec votre nom seul car par défaut vous êtes la seule personne autorisée à déchiffrer les fichiers.
2. Si vous souhaitez partager le ou les fichiers protégés avec d'autres utilisateurs ou groupes d'utilisateurs, saisissez leur nom dans le champ de recherche. La recherche peut afficher les utilisateurs et groupes présents dans l'annuaire de confiance ou dans l'annuaire LDAP s'il est configuré. Elle affiche les utilisateurs ou membres de groupes dont le certificat est valide ou révoqué (l'état de révocation est vérifié en arrière-plan).
   - Les groupes provenant de l'annuaire local affichent une icône verte,
   - Les groupes provenant de l'annuaire LDAP affichent une icône jaune,
   - Un appui sur la touche Entrée dans le champ de recherche lance directement une recherche dans l'annuaire LDAP.
3. Confirmez votre choix. En cas de sélection multiple, Stormshield Data File 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 au format *.sbox* vides. Toute tentative de chiffrement d'un fichier vide génère un message d'erreur dans la fenêtre de résumé.
4. La fenêtre de progression des opérations de chiffrement s'affiche. Au terme de celle-ci un résumé des opérations effectuées s'affiche.
   Cliquez sur **Détails**.
5. Pour fermer automatiquement la fenêtre après un chiffrement réussi, cochez l'option **Fermer la fenêtre automatiquement**. Cette option s'appliquera à toute autre opération de chiffrement et de déchiffrement. Cependant, cette option est ignorée en cas d'erreurs pendant le chiffrement.

Si vous avez chiffré pour un groupe, le groupe ne s'affiche ensuite plus dans la liste des utilisateurs sélectionnés lorsque vous modifiez la règle. Il est remplacé par les noms des utilisateurs concernés.

5.2.2 Déchiffrer un fichier ou un ensemble de fichiers

Pour déchiffrer un fichier, l'utilisateur doit être équipé de Stormshield Data File ou de Security BOX SmartFILE. Cependant, si SDS Enterprise peut déchiffrer indifféremment les fichiers au format SDS Enterprise ou Security BOX SmartFILE, Security BOX SmartFILE ne peut déchiffrer que les fichiers qui lui sont destinés.

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

Lorsque l'utilisateur sélectionne un dossier, Stormshield Data File déchiffre les fichiers qu'il a personnellement chiffrés ou les fichiers chiffrés qui lui ont été adressés.

Pour déchiffrer un dossier complet :

- Sélectionnez ce dossier puis sélectionnez **Stormshield Data Security > Retirer la protection** dans le menu contextuel.

Pour déchiffrer un ou plusieurs fichiers chiffrés :

1. Sélectionnez les fichiers, faites un clic droit, puis sélectionnez le menu **Stormshield Data Security > Retirer la protection**.
   La prochaine fenêtre indique la progression des opérations de déchiffrement puis au terme de celle-ci affiche un résumé des opérations effectuées.
2. Pour automatiquement fermer la fenêtre après un déchiffrement réussi, cochez 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.

5.2.3 Ouvrir un ou plusieurs fichiers chiffrés

Pour ouvrir un ou plusieurs fichiers chiffrés :

- Sélectionnez les fichiers puis appuyez sur la touche **Entrée**,

- ou -

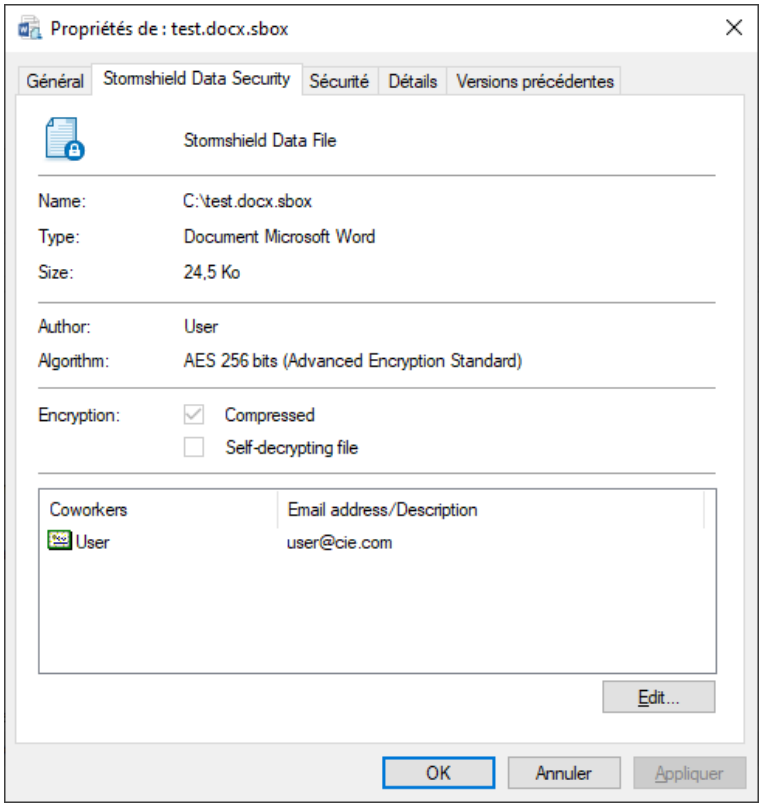
- Sélectionnez les fichiers puis sélectionnez **Stormshield Data Security > Ouvrir** dans le menu contextuel.

Selon le format des fichiers chiffrés (extensions *.sdsx* ou *.sbox*) le comportement diffère :

- Dans le cas des fichiers portant l'extension *.sdsx*, le contenu des fichiers chiffrés s'affiche dans l'application correspondante. Les fichiers restent chiffrés.
- Dans le cas des fichiers portant l'extension *.sbox*, la protection est retirée des fichiers puis les fichiers sont ouverts dans l'application correspondante. Il faudra les chiffrer à nouveau après leur fermeture.

5.2.4 Afficher les propriétés d'un fichier chiffré

Les propriétés d'un fichier chiffré affichent la liste des utilisateurs en mesure de 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*.
- le nom et l'adresse e-mail des correspondants qui peuvent déchiffrer le fichier (uniquement si l'utilisateur est connecté).

5.2.5 Gérer les collaborateurs d'un fichier chiffré

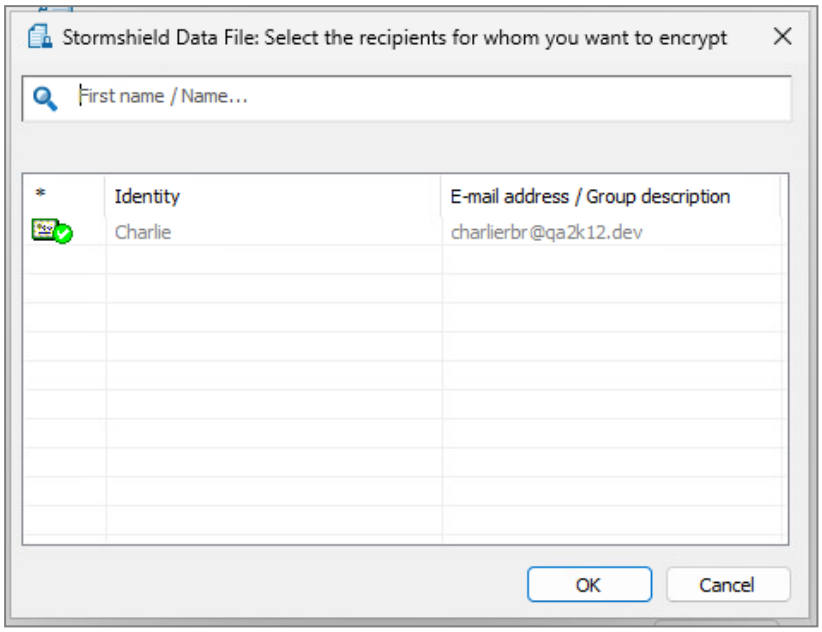
Il est possible de gérer les collaborateurs associés à un fichier chiffré depuis la fenêtre des propriétés de ce fichier. Vous pouvez :

- Ajouter un ou plusieurs collaborateurs depuis l'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**. Vous pouvez presser la touche Entrée pour lancer directement une recherche dans l'annuaire LDAP. Si vous recherchez un groupe :
   - Les groupes provenant de l'annuaire local affichent une icône verte,
   - Les groupes provenant de l'annuaire LDAP affichent une icône jaune.
4. Cliquez sur **Appliquer** puis **OK** dans la fenêtre des **Propriétés** pour appliquer les changements.

Pour supprimer un ou plusieurs collaborateurs :

1. Dans la fenêtre des **Propriétés**, sélectionnez l'onglet **Stormshield Data Security** et cliquez sur **Modifier**.
2. La fenêtre de sélection des correspondants s'ouvre. Survolez la ligne d'un collaborateur et cliquez sur la corbeille rouge pour le supprimer. Cliquez sur **OK**.
3. Cliquez sur **Appliquer** puis **OK** dans la fenêtre des **Propriétés** pour appliquer les changements.

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

5.2.6 Créer un fichier compatible Security BOX SmartFILE

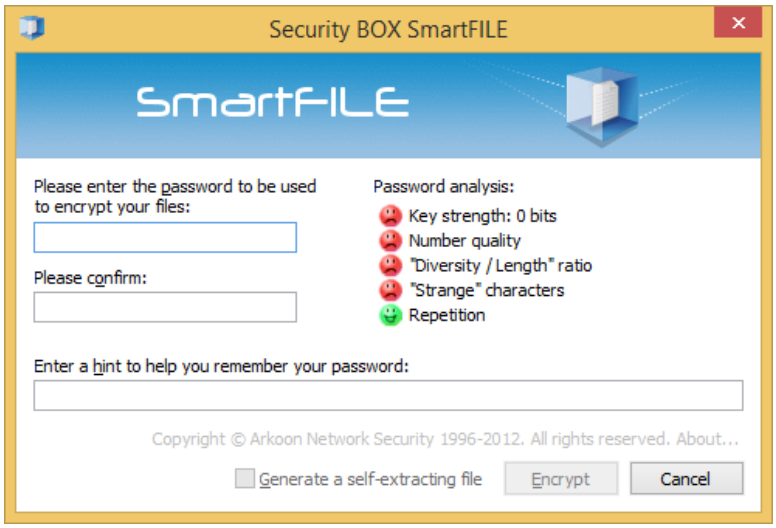
Si l'utilisateur souhaite partager des fichiers chiffrés avec des correspondants ne disposant pas de Stormshield Data File mais de Security BOX SmartFILE, Stormshield Data File permet de générer des fichiers chiffrés au format Security BOX SmartFILE.

Les règles suivantes s'appliquent :

- L'utilisateur peut chiffrer plusieurs fichiers simultanément. Un fichier chiffré au format Security BOX SmartFILE est créé pour chaque fichier.
- Les noms des fichiers chiffrés ne doivent pas comporter de caractères au format Unicode.

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

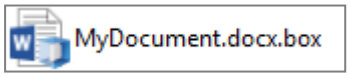
1. Sélectionnez le fichier puis effectuez un clic droit pour sélectionner **Stormshield Data Security > Security BOX SmartFile**.
2. Entrez le mot de passe et le mnémonique.



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**. Revenez à la double saisie masquée de la même façon.

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

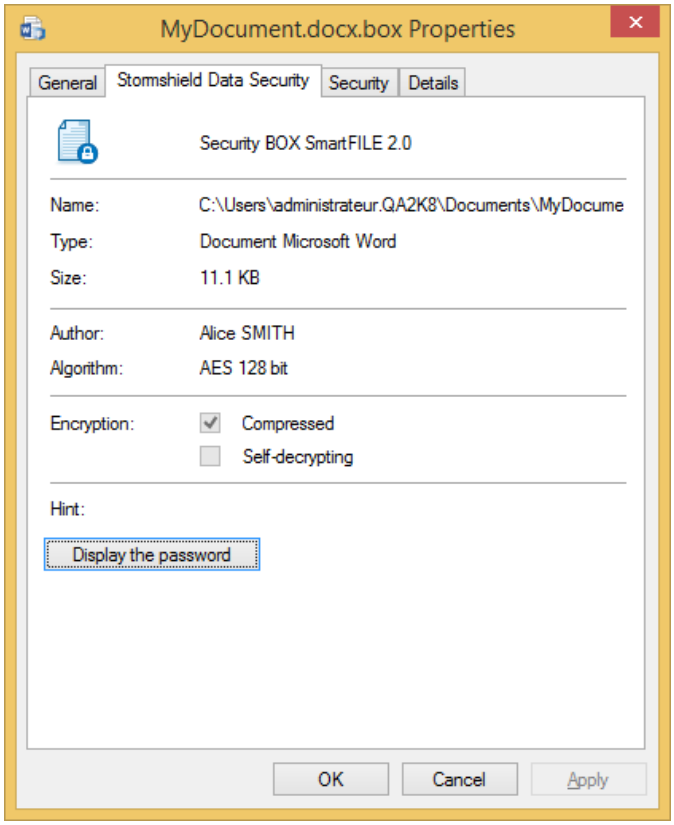
Les fichiers chiffrés au format Security BOX SmartFILE disposent d'une petite icône et d'une extension spécifique :



5.2.7 Récupérer le mot de passe

Si l'utilisateur a besoin de récupérer le mot de passe utilisé pour la génération 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 à SDS Enterprise 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 SDS Enterprise (y compris les comptes de récupération) ou en utilisant Security BOX SmartFILE.



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

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

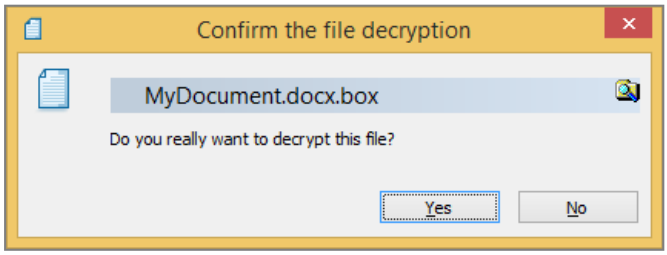
Si l'utilisateur a besoin de déchiffrer un fichier Security BOX SmartFILE en utilisant un compte de recouvrement :

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. Confirmez le déchiffrement.

Le fichier est déchiffré sans mot de passe.

5.3 Transchiffrer des fichiers

SDS Enterprise permet de mettre à jour les listes des utilisateurs pouvant accéder à des 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 *.sdsx*, il reste au format *.sdsx* après transchiffrement.

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 l'annuaire de confiance ou d'un annuaire LDAP (consultez le *Guide d'administration SDS Enterprise*).

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 l'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 l'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 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.

6. Protéger automatiquement des dossiers

Stormshield Data Share permet de protéger automatiquement le contenu de dossiers confidentiels, et éventuellement d'en partager l'accès avec d'autres collaborateurs. Lorsque cette fonctionnalité est activée, chaque nouveau document ou sous-dossier placé dans ce dossier est chiffré et accessible seulement par les utilisateurs autorisés. Vous pouvez protéger le contenu des types de dossiers suivants :

- Dossiers standard Windows se trouvant sur votre poste de travail,
- Dossiers issus d'un espace collaboratif synchronisé.

Pour sécuriser automatiquement un dossier sur un partage réseau, un serveur de fichiers ou un lecteur externe (e.g., clé USB), utilisez la fonctionnalité Stormshield Data Team.

6.1 Protéger automatiquement le contenu d'un dossier local

Vous pouvez activer la protection automatique d'un dossier se trouvant sur votre poste de travail afin que tous les sous-dossiers et documents que vous y déposez soient systématiquement protégés.

Cette fonctionnalité est dépendante de la fonctionnalité File et ne peut pas fonctionner sans cette dernière.

6.1.1 Protéger automatiquement l'accès à un dossier

1. Dans l'explorateur Windows, faites un clic droit sur le dossier local que vous souhaitez protéger et sélectionnez **Stormshield Data Security** > **Protéger automatiquement le dossier**. La fenêtre **Choix de vos correspondants** s'affiche avec votre nom seul car par défaut vous êtes la seule personne autorisée à déchiffrer le contenu du dossier.
2. Si vous souhaitez partager le contenu du dossier protégé avec d'autres utilisateurs, saisissez leur nom dans le champ de recherche. La recherche peut afficher les utilisateurs présents dans l'annuaire de confiance ou dans l'annuaire LDAP s'il est configuré.
3. Cliquez sur **OK**.
   Une règle de protection est créée qui contient le chemin vers le dossier ainsi que l'utilisateur ou la liste des utilisateurs autorisés à déchiffrer son contenu.
   Tous les nouveaux dossiers et fichiers déplacés dans ce dossier sont désormais chiffrés automatiquement. Leur icône affiche un petit cadenas bleu.
4. Si vous souhaitez chiffrer également tous les dossiers et fichiers déjà présents avant l'activation de la protection automatique, faites un clic droit sur le dossier protégé et sélectionnez **Stormshield Data Security** > **Avancé** > **Appliquer les modifications à tout le dossier**.

Si dans le dossier, certains fichiers avaient déjà été protégés précédemment, les comportements suivants s'appliquent :

- Les utilisateurs qui étaient autorisés à accéder à ces fichiers seront remplacés par ceux spécifiés par la nouvelle règle de protection.
- Les fichiers déjà chiffrés auxquels vous n'avez pas l'autorisation d'accéder ne seront pas traités.
- Les fichiers chiffrés au format *.sbox* ne seront pas traités.

Si vous déplacez le dossier et son contenu, la règle de protection se met à jour. Tout le contenu reste protégé et la protection automatique du dossier reste activée.

6.1.2 Modifier les collaborateurs autorisés à accéder au contenu du dossier

1. Dans l'explorateur Windows, faites un clic droit sur le dossier dont vous souhaitez modifier les collaborateurs autorisés.
2. Sélectionnez **Stormshield Data Security** > **Modifier la règle de protection automatique**.
3. Dans la fenêtre **Choix de vos correspondants**, ajoutez ou retirez des utilisateurs autorisés à déchiffrer le contenu du dossier. Saisissez leur nom dans le champ de recherche.
4. Cliquez sur **OK**.
   Le dossier et les documents qu'il contient sont désormais accessibles par tous les utilisateurs que vous avez autorisés.
5. Si vous souhaitez appliquer ce changement également pour tous les dossiers et fichiers déjà présents au préalable, faites un clic droit sur le dossier protégé et sélectionnez **Stormshield Data Security** > **Avancé** > **Appliquer les modifications à tout le dossier**.

6.1.3 Désactiver la protection automatique d'un dossier

1. Dans l'explorateur Windows, faites un clic droit sur le dossier dont vous souhaitez désactiver la protection automatique. Ce dossier ne doit pas se trouver dans un espace synchronisé protégé automatiquement par l'administrateur et vous devez être autorisé à y accéder.
2. Sélectionnez **Stormshield Data Security** > **Avancé** > **Désactiver la protection du dossier**.

Lorsque vous retirez la protection d'undossier, les documents qu'il contient restent chiffrés. En revanche, tous les nouveaux documents que vous y ajoutez ne sont plus automatiquement chiffrés.

6.2 Protéger automatiquement des dossiers d'espaces collaboratifs synchronisés

Vous pouvez chiffrer des documents stockés sur des espaces collaboratifs synchronisés avec les hébergeurs en ligne OneDrive, DropBox, SharePoint et Oodrive.

6.2.1 Connaître les prérequis

- La fonctionnalité Stormshield Data File doit être installée pour que Stormshield Data Share fonctionne.
- L'administrateur doit avoir préalablement activé la protection automatique des dossiers d'un ou plusieurs types d'espaces collaboratifs synchronisés dans SDMC. Pour plus d'informations, reportez-vous à la section *Configurer Stormshield Data Share* du *Guide d'administration SDS Enterprise*.

6.2.2 Protéger un document dans votre espace collaboratif synchronisé

1. Connectez-vous à SDS Enterprise.
2. Déplacez votre document dans le dossier synchronisé de votre choix (e.g., OneDrive, Dropbox).
   Il est automatiquement protégé : il comporte désormais une extension *.sdsx* et son icône affiche un petit cadenas. Vous êtes la seule personne à pouvoir le consulter.

Vous pouvez ensuite autoriser d'autres utilisateurs à accéder à votre document protégé. Pour plus d'informations, reportez-vous à la section Gérer les collaborateurs d'un fichier chiffré.

Si par la suite vous déplacez votre document protégé hors de l'espace synchronisé, il reste protégé. Dans ce cas, vous pouvez néanmoins retirer sa protection. Pour plus d'informations, reportez-vous à la section Déchiffrer un fichier ou un ensemble de fichiers.

7. Sécuriser le contenu d'un dossier

La fonctionnalité Stormshield Data Team assure le chiffrement automatique des fichiers confidentiels : les fichiers sont chiffrés là où ils se trouvent, en temps réel et de façon transparente.

La protection est assurée selon des règles de sécurité 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 Team 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 utilisateur est vérifiée conformément à la politique de sécurité définie.

Stormshield Data Team peut sécuriser :

- Un support amovible (une clé USB) en totalité ou partiellement (un ou plusieurs sous-dossiers),
- Un dossier partagé sur un serveur de fichiers.

Pour protéger automatiquement un dossier local au poste de travail de l'utilisateur ou un espace collaboratif synchronisé, utilisez la fonctionnalité Stormshield Data Share.

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 Team, le fichier ou le dossier sont créés et sont lus 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.

Les menus contextuels de Stormshield Data Team visibles lorsque l'utilisateur fait un clic droit sur un dossier dépendent des paramètres sélectionnés dans la console d'administration SDMC. Pour plus d'informations, reportez-vous à la section *Configurer Stormshield Data Team* du *Guide d'administration*.

7.1 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 des collaborateurs, de faciliter la gestion de la liste des collaborateurs autorisés.

NOTE
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 modifié ni supprimé.

7.1.1 Comprendre les icônes Stormshield Data Team

Dans l'explorateur Windows, un dossier sécurisé et un fichier chiffré se reconnaissent par l'icône

 Confidential	L'icône indique qu'une règle de Stormshield Data Team s'applique sur le dossier. Si l'utilisateur 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 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 reste chiffré. Dans ce cas, nous vous recommandons de ne pas modifier ces fichiers. Ils pourraient alors être corrompus de façon irrémédiable.
 MyDocument Microsoft Word Document 11.8 KB	Ces icônes 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	

7.1.2 Sécuriser un dossier sans définir de partage

Pour sécuriser rapidement un dossier sans le partager avec d'autres utilisateurs, c'est-à-dire sans définir de règle de sécurité :

1. Sélectionnez le dossier à l'aide de la souris puis effectuez un clic droit et sélectionnez le menu **Stormshield Data Security > Sécuriser le dossier**.
2. Confirmez votre choix.
   Le dossier est alors sécurisé par une règle ne contenant que l'utilisateur connecté en cours. Les fichiers du dossier sont mis à jour et chiffrés.

7.1.3 Sécuriser un dossier en définissant un partage

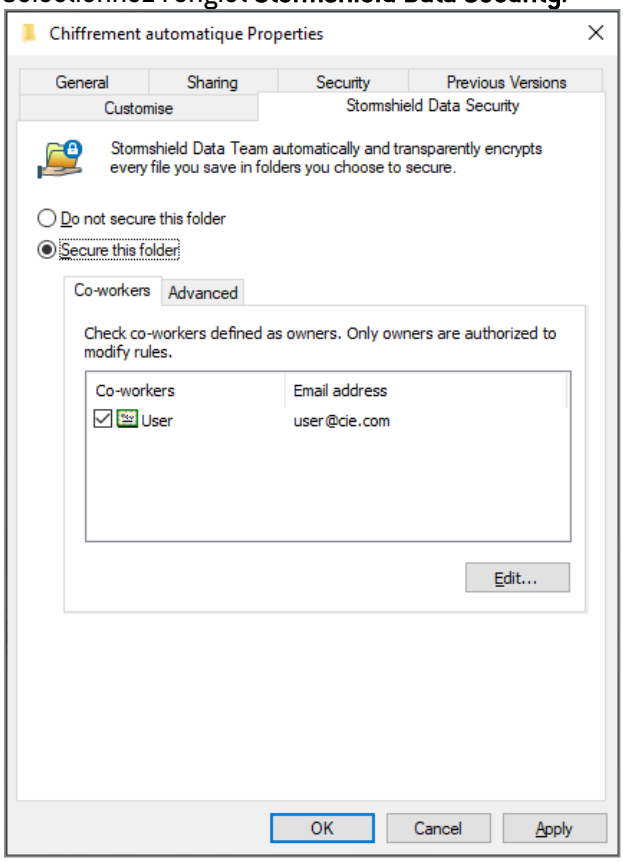
Pour sécuriser un dossier en donnant accès à d'autres utilisateurs à ce dossier, c'est-à-dire en définissant une règle de sécurité, suivez les procédures suivantes.

Sécuriser un dossier

Pour sécuriser un dossier et définir une règle de sécurité :

1. Sélectionnez le dossier que vous souhaitez sécuriser.
2. Cliquez sur le bouton droit puis sélectionnez **Propriétés**.

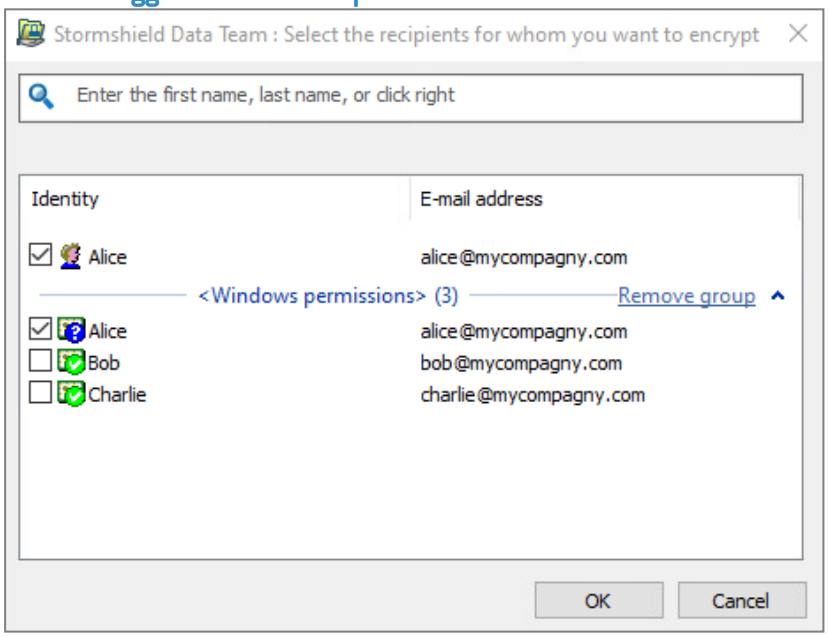
3. Sélectionnez l'onglet **Stormshield Data Security**.



4. Sélectionnez l'option **Sécuriser ce dossier** pour chiffrer le dossier. Les sous-dossiers sont automatiquement sécurisés.

5. Si vous souhaitez partager votre dossier, cliquez sur le bouton **Modifier** et recherchez les collaborateurs ou les groupes autorisés. La recherche peut afficher les collaborateurs et groupes présents dans l'annuaire de confiance ou dans l'annuaire LDAP s'il est configuré. Elle affiche les collaborateurs ou membres de groupes dont le certificat est valide ou révoqué (l'état de révocation est vérifié en arrière-plan).
   - Les groupes provenant de l'annuaire local affichent une icône verte,
   - Les groupes provenant de l'annuaire LDAP affichent une icône jaune,
   - Un appui sur la touche Entrée dans le champ de recherche lance directement une recherche dans l'annuaire LDAP.

   Les collaborateurs possédant les autorisations Windows sur le dossier concerné peuvent être automatiquement suggérés dans le groupe **Autorisations Windows** si l'option est activée (icône bleue). Vous pouvez cliquer sur le nom du groupe pour supprimer certains collaborateurs du groupe si nécessaire. Si l'option n'est pas activée, vous pouvez ajouter le groupe depuis la liste de suggestions. 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. 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 simple collaborateur autorisé.
8. 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.

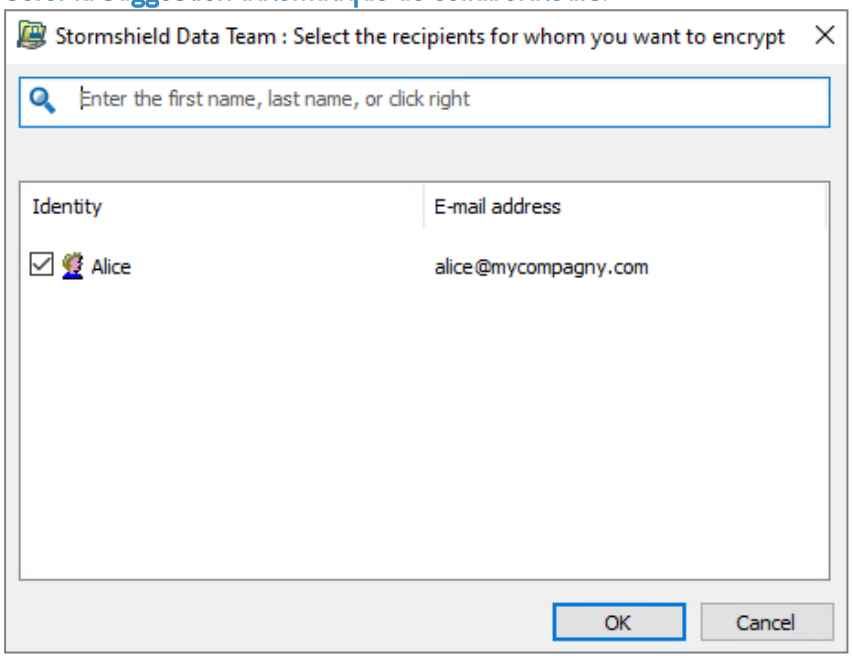
Si vous avez chiffré pour un groupe, le groupe ne s'affiche ensuite plus dans la liste des collaborateurs sélectionnés. Il est remplacé par les noms des collaborateurs concernés.

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 corbeille rouge.
   Un clic droit dans le champ de recherche permet de sélectionner 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.



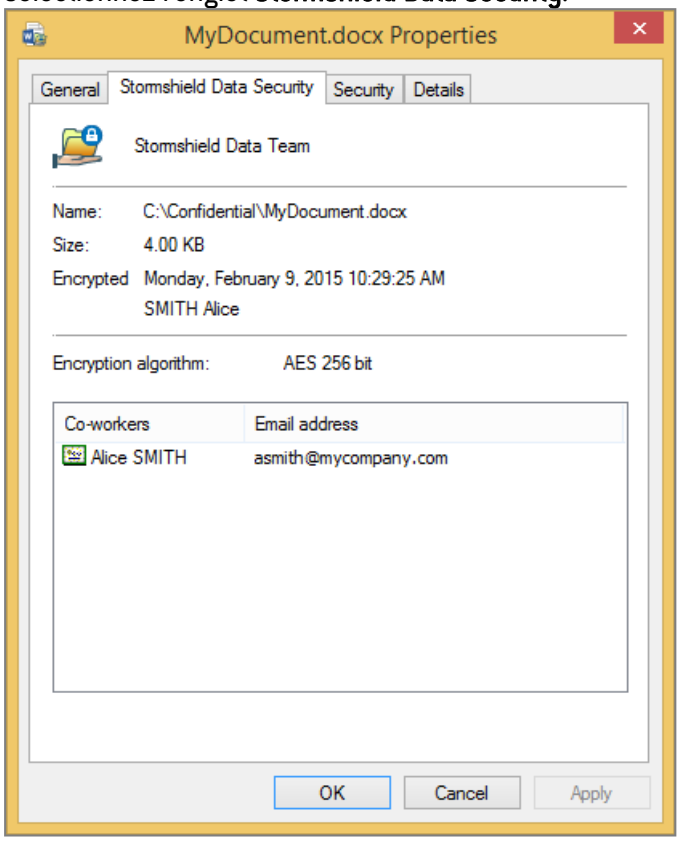
6. Cliquez sur **OK** pour fermer la fenêtre de recherche de collaborateurs.
7. Cliquez sur **OK** pour enregistrer et appliquer votre règle.

7.1.4 Gérer les dossiers sécurisés

Vous pouvez réaliser les actions suivantes sur les dossiers sécurisés.

Afficher les 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 sélectionnez **Stormshield Data Security** puis **Propriétés** ou bien ouvrez les **Propriétés** du fichier et sélectionnez l'onglet **Stormshield Data Security**.



Dans l'onglet **Stormshield Data Security**, la taille indiquée inclut les données de sécurité propres à SDS Enterprise (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 SDS Enterprise,
- vous faites partie de cette liste de collaborateurs.

Copier ou déplacer un fichier ou un dossier couverts par une règle Team vers un dossier non sécurisé

Vous pouvez choisir le comportement par défaut en cas de copie ou de déplacement de fichiers ou dossiers chiffrés vers un dossier non sécurisé dans les paramètres avancés de la fonctionnalité Team dans SDMC. Vous pouvez interdire le déplacement ou la copie, ou bien vous pouvez les autoriser en choisissant de déchiffrer ou de conserver le chiffrement.

Pour paramétrer ces options, reportez-vous au *Guide d'administration de SDS Enterprise*, section *Configurer Stormshield Data Team*.

Quel que soit le comportement choisi, le menu contextuel **Sauvegarder** permet de créer une copie de fichier ou dossier tout en gardant le chiffrement. Pour plus d'informations, reportez-vous à la section Sauvegarder un fichier chiffré.

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

Sécuriser des 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.

Visualiser les règles connues

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

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
La durée de traitement dépend directement du nombre de collaborateurs présents dans la règle et des performances du système.

7.2 Mettre à jour la sécurité d'un dossier

Vous pouvez mettre à jour la sécurité d'un dossier, c'est-à-dire la règle de sécurité qui s'applique à lui, à n'importe quel moment.

Pour appliquer une nouvelle règle ou modifier une règle de sécurité sur un dossier :

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 sélectionnez le menu **Stormshield Data Security** > **Sécuriser selon les règles définies**.

NOTE
La mise à jour des fichiers s'interrompt si vous verrouillez ou fermez votre session SDS Enterprise ou votre session Windows. Cette mise à jour reprend automatiquement quand vous vous reconnectez à SDS Enterprise. 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.

7.3 Sauvegarder un fichier chiffré

Pour copier un fichier chiffré ou un dossier sécurisé 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 sélectionnez **Stormshield Data Security** > **Avancé** > **Sauvegarder**. Vous pouvez sélectionner plusieurs fichiers ou dossiers en même temps.
2. Sélectionnez le dossier de 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 SDS Enterprise pour effectuer une sauvegarde.

NOTE
Par défaut, SDS Enterprise est configuré pour autoriser l'ouverture d'un fichier chiffré stocké dans un dossier non sécurisé.

ATTENTION
Il ne faut surtout pas utiliser la fonction Enregistrer de Windows ou glisser et déposer le fichier sur un support de sauvegarde non sécurisé : le fichier confidentiel serait alors copié en clair.

7.4 Restaurer un fichier chiffré

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

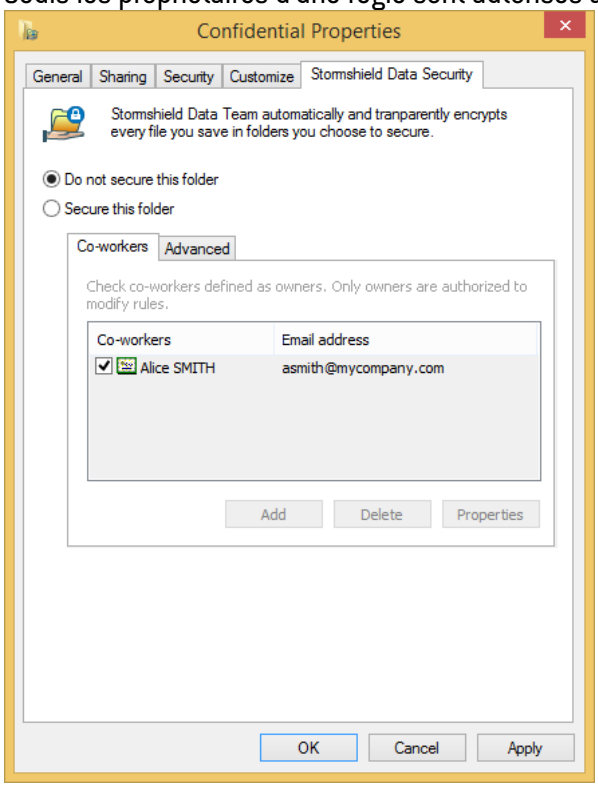
1. Sélectionnez le dossier ou les fichiers à restaurer avec le bouton droit de votre souris, et sélectionnez **Stormshield Data Security** > **Avancé** > **Restaurer**.
2. Sélectionnez le dossier de destination de la restauration : vous ne pouvez sélectionner qu'un dossier sécurisé.
3. Cliquez sur **OK**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

7.5 Retirer la sécurité d'un dossier

Pour retirer la sécurité d'un dossier et déchiffrer les fichiers qu'il contient, suivez la procédure suivante :

1. Faites un clic droit sur le dossier sécurisé, puis sélectionnez les menus **Stormshield Data Security** et **Propriétés**.
   La page de propriétés s'affiche 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 retirer la sécurité du 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**.
5. Cliquez sur **Fermer**. La règle de sécurité a été supprimée et les fichiers contenus dans le dossier sont maintenant en clair.

7.6 Déchiffrer des fichiers

Il n'est pas possible de déchiffrer 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.

Pour déchiffrer un fichier ou un ensemble de fichiers :

1. 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 déchiffrés.

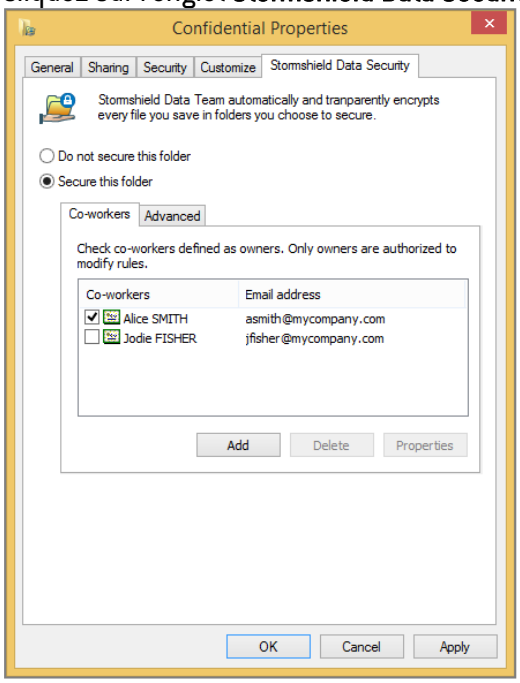
Une fois l'opération terminée, le dossier est accessible sans restriction et tous les fichiers qu'il contient sont enregistrés en clair.

7.7 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.

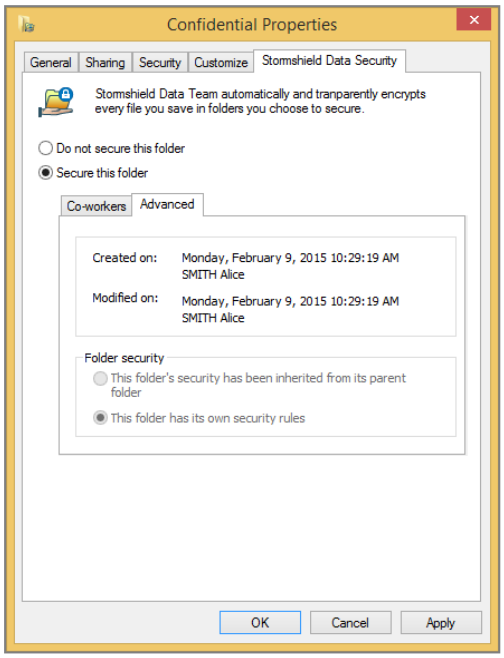
Procédez comme suit :

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**.



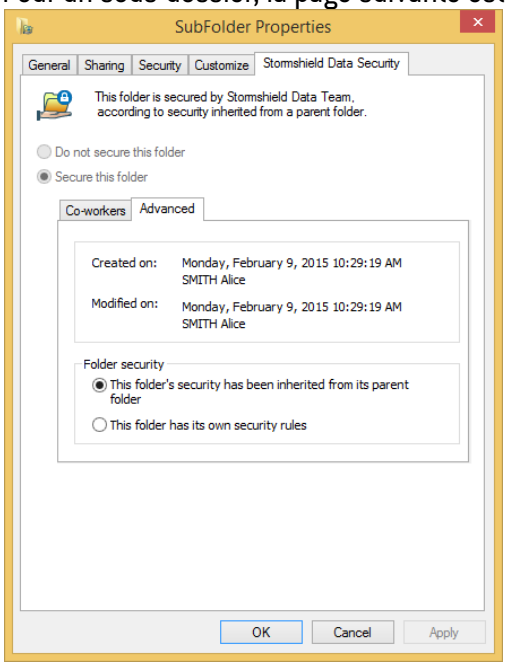
Vous pouvez voir les utilisateurs autorisés dans la liste des collaborateurs. Le nom des propriétaires est coché.

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 Retirer la sécurité d'un dossier.

- 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.
- Le déplacement d'un dossier sécurisé conserve la règle de sécurité à la condition que celle-ci soit portée par le dossier lui-même. Si cette règle était portée par son parent, alors le dossier perd sa sécurité après son déplacement. Toutefois, les fichiers qu'il contient 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 sans définir de partage.

7.8 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 l'utilisateur n'est pas un collaborateur autorisé et qu'il souhaite supprimer complètement des fichiers chiffrés, il doit utiliser la fonction de suppression SDS Enterprise.

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

7.9 Réparer une règle

Une règle de sécurité est techniquement stockée dans un fichier privé caché dans le dossier en question. Quand un utilisateur accède à un dossier sécurisé par une règle, SDS Enterprise stocke dans son 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 :

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

En cas de suspicion d'attaque, SDS Enterprise interdit tout accès au dossier concerné. Pour rétablir l'accès au dossier :

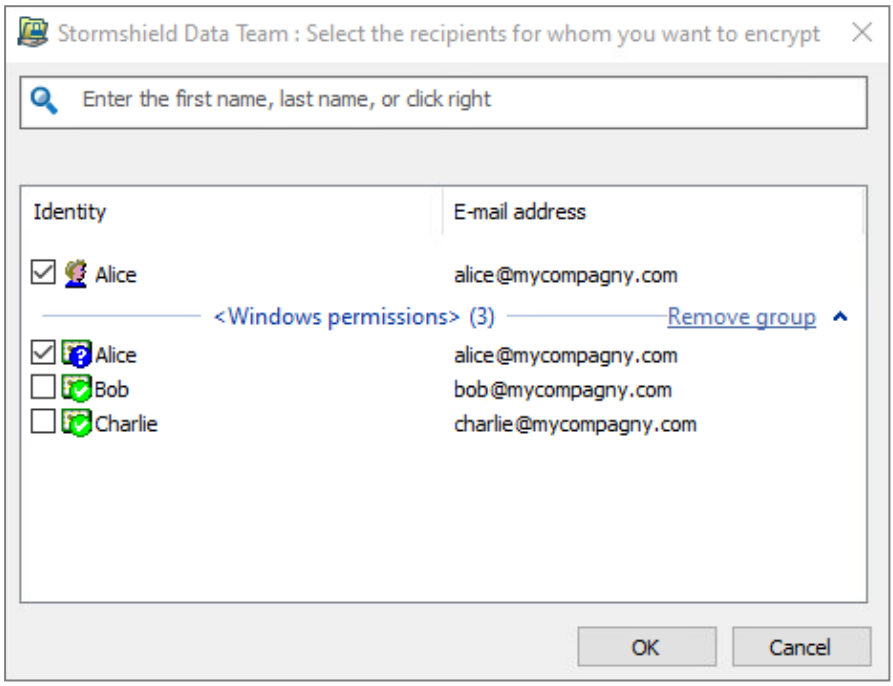
1. Dans l'Explorateur Windows, cliquez avec le bouton droit sur le fichier et sélectionnez **Propriétés**.
2. Cliquez sur l'onglet **Stormshield Data Security**.
3. Cliquez sur **Restaurer** pour recopier dans le dossier la règle stockée dans le compte.
4. Ou cliquez sur **Actualiser** pour accepter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

7.10 Mettre à jour automatiquement 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 automatiquement toutes les règles connues par un utilisateur. Pour en savoir plus, consultez la section *Configurer Stormshield Data Team* du *Guide d'administration*. Cette mise à jour des règles n'est possible que si l'utilisateur fait partie des propriétaires de la règle.

7.11 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**, accompagné d'une icône bleue dans le champ de recherche.



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 d'administration SDS Enterprise*.
- les utilisateurs retrouvés via les autorisations Windows possèdent un certificat valide dans l'annuaire Active Directory.

Vous pouvez désactiver cette fonctionnalité en créant une clé de registre. Pour plus d'informations, reportez-vous à la section *Désactiver la suggestion automatique de collaborateurs* du *Guide de configuration avancée* SDS Enterprise.

7.12 Connaître les limitations connues

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

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.
Partage d'un répertoire local sécurisé	Le partage en local d'un répertoire chiffré par Stormshield Data 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.
Espaces collaboratifs synchronisés	Les espaces collaboratifs synchronisés de type SharePoint, Dropbox, Office 365, etc. ne sont pas supportés par Stormshield Data Team. Nous vous recommandons d'exclure ces répertoires des dossiers analysés par Stormshield Data Team. Vous pouvez exclure des répertoires grâce au paramètre `excludedFolders`dans le fichier *.json* de la politique de sécurité. Pour plus d'informations, reportez-vous à la section *Stormshield Data Team* du Guide de configuration avancée. Pour sécuriser des espaces collaboratifs synchronisés, reportez-vous à la section Protéger automatiquement des dossiers.

8. Créer des volumes virtuels sécurisés

La fonctionnalité Stormshield Data Virtual Disk permet de garantir la confidentialité des données que l'utilisateur stocke sur son disque dur en créant des volumes virtuels chiffrés : seuls le propriétaire et les personnes autorisées pourront accéder aux volumes sécurisés.

Stormshield Data Virtual Disk utilise peu de ressources (mémoire et CPU) et les fichiers sont chiffrés en temps réel au moment de leur écriture et déchiffrés à la lecture. Les applications peuvent accéder directement aux informations protégées d'un fichier situé sur un volume virtuel.

Stormshield Data Virtual Disk permet de :

- Créer un volume virtuel sécurisé sur lequel l'utilisateur souhaite sauvegarder des données confidentielles. Reportez-vous à la section Créer un volume sécurisé.
- Monter un volume sécurisé sur le poste de travail, c'est-à-dire connecter un volume virtuel sur lequel l'utilisateur sauvegarde des données confidentielles. Reportez-vous à la section Monter un volume sécurisé.
- Démonter un volume sécurisé du poste de travail, c'est-à-dire déconnecter le volume virtuel. Reportez-vous à la section Démonter un volume sécurisé.

Lorsque l'utilisateur crée un volume virtuel sécurisé, il définit une liste d'utilisateurs autorisés. Ces utilisateurs autorisés sont les utilisateurs qui peuvent monter et démonter le volume sécurisé et par conséquent accéder au contenu du volume. Reportez-vous à la section Modifier la liste des utilisateurs.

Le fichier container (extension *.vbox*) représente le volume chiffré à partir de l'Explorateur Windows. Le volume chiffré correspond au contenu du fichier container.

Pour des informations sur le paramétrage de Stormshield Data Virtual Disk dans SDMC, reportez-vous au *Guide d'administration SDS Enterprise*.

8.1 Créer un volume sécurisé

La fonctionnalité Stormshield Data Virtual Disk permet de créer des volumes virtuels sécurisés. Tous les fichiers placés sur ces volumes seront chiffrés puis stockés de manière sécurisée.

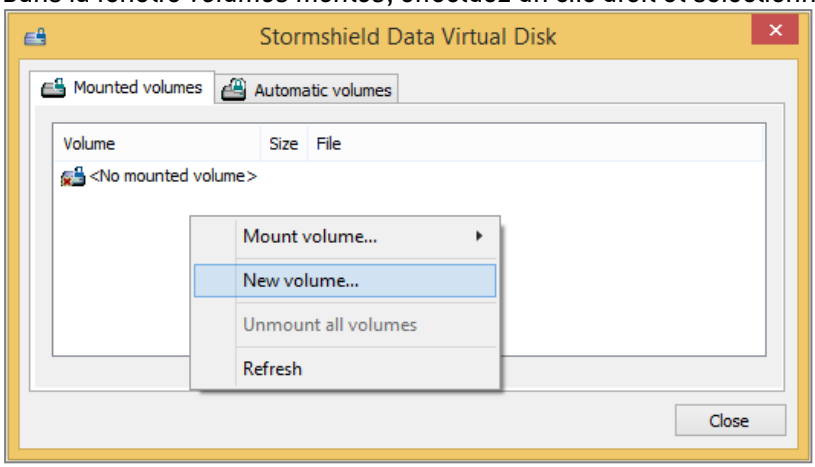
L'utilisation d'un volume virtuel sécurisé est identique à celle d'un disque dur. Vous pouvez y copier des fichiers et lancer des applications qui utilisent des fichiers sauvegardés sur ce volume. Il est également possible d'installer des applications sur des volumes sécurisés.

Comme un volume disque physique, un volume disque virtuel peut être endommagé ou détruit, entraînant la perte des informations qu'il contient. Vous devez donc conserver une copie de sauvegarde des fichiers stockés sur le volume virtuel ou du fichier hébergeant le contenu du volume virtuel. Il est également conseillé d'administrer les volumes virtuels de la même manière que les volumes physiques en effectuant des opérations telles que formatage, vérification des erreurs, fragmentation, gestion des sauvegardes.

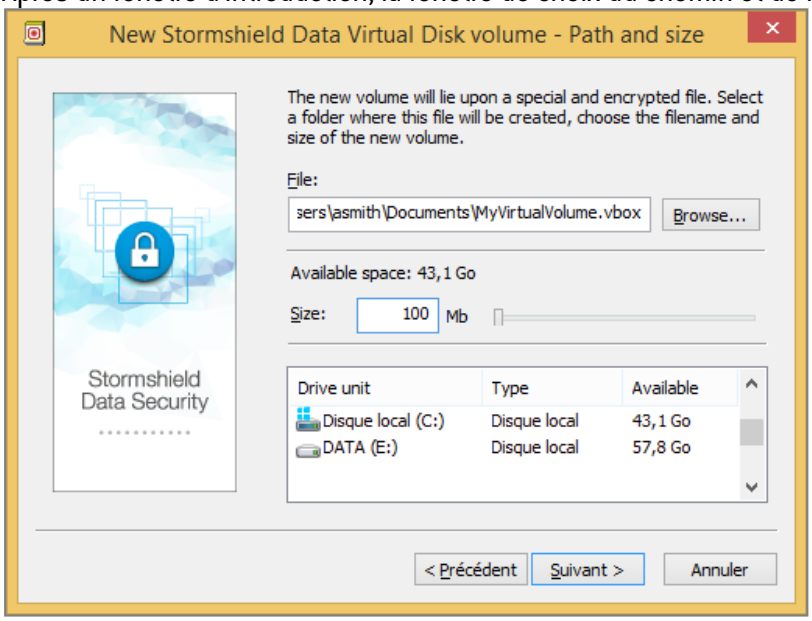
Pour créer un volume sécurisé :

1. Dans la barre de recherche Windows, recherchez Stormshield Data Virtual Disk.
2. À partir du panneau de contrôle de Stormshield Data Virtual Disk, sélectionnez l'onglet *Volume montés*.

3. Dans la fenêtre *Volumes montés*, effectuez un clic droit et sélectionnez **Nouveau volume**.



4. Après un fenêtre d'introduction, la fenêtre de choix du chemin et de la taille s'affiche :



a. Dans le champ **Fichier**, spécifiez le nom du volume et son emplacement. L'extension *.vbox* sera automatiquement ajoutée au nom du volume.

> **IMPORTANT**
> Dans le cas où un volume chiffré est monté localement dans une session Windows, tous les utilisateurs pouvant ouvrir une session locale sur le poste de travail auront accès au contenu du volume chiffré. Pour plus d'informations, reportez-vous à la section *Configurer et utiliser les fonctionnalités avancées de l'agent* du *Guide d'administration SDS Enterprise*.

b. Dans le champ **Taille**, spécifiez la taille du volume. Celle-ci peut être comprise entre 1 MB et la taille maximum disponible. Par défaut, la taille est égale à 10% de l'espace disponible du répertoire.

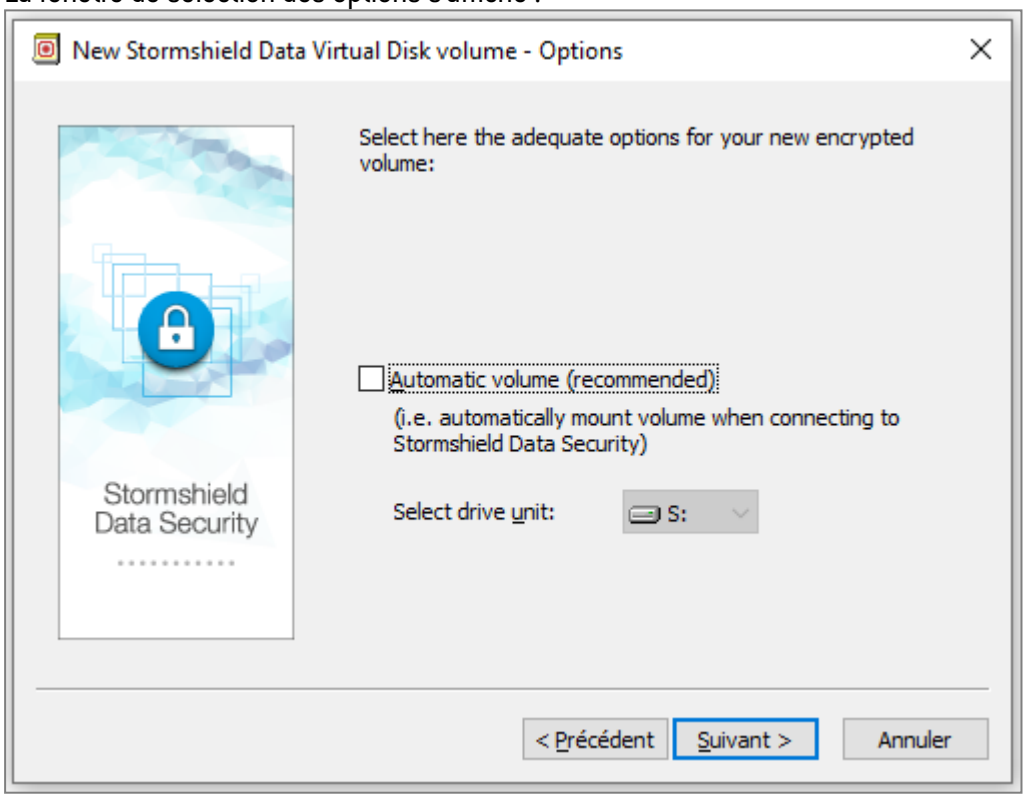
> **IMPORTANT**
> La taille maximale d'un volume Stormshield Data Virtual Disk est 2048 Go (2 To).

5. Cliquez sur **Suivant**.

6. Vous pouvez permettre à d'autres personnes d'utiliser le volume créé. Saisissez leur nom dans le champ de recherche. La recherche peut afficher les utilisateurs ou groupes présents dans l'annuaire de confiance ou dans l'annuaire LDAP dans le cas où il est configuré. Elle affiche les utilisateurs ou membres de groupes dont le certificat est valide ou révoqué (l'état de révocation est vérifié en arrière-plan).
   - Les groupes provenant de l'annuaire local affichent une icône verte,
   - Les groupes provenant de l'annuaire LDAP affichent une icône jaune,
   - Un appui sur la touche Entrée dans le champ de recherche lance directement une recherche dans l'annuaire LDAP.

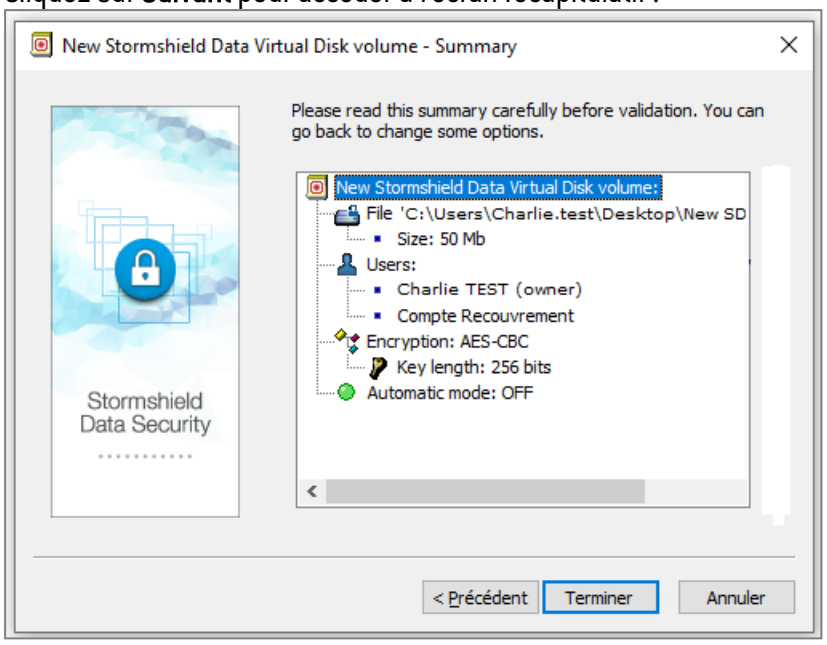
> **NOTE**
> L'utilisation simultanée du volume par plusieurs utilisateurs n'est pas possible. Chaque utilisateur autorisé accède au volume de façon alternée.

   Une fois la liste des utilisateurs complète, cliquez sur **Suivant**.
7. La fenêtre de sélection des options s'affiche :



   Vous devez indiquer :
   - Si le volume doit être automatiquement monté chaque fois que vous vous connectez à SDS Enterprise,
   - La lettre du lecteur sur lequel monter le volume et si celui-ci doit être monté automatiquement à chacune de vos connexions à SDS Enterprise. Aucun lecteur réseau ou aucune clé USB ne doit utiliser la même lettre de lecteur.

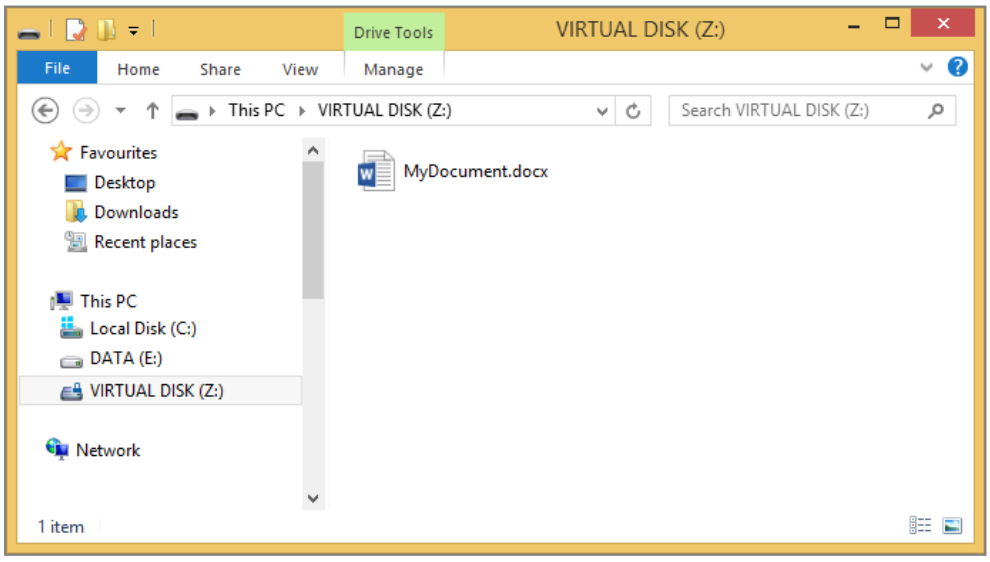
8. Cliquez sur **Suivant** pour accéder à l'écran récapitulatif :



Par défaut, l'algorithme et la force de la clé utilisés pour chiffrer les fichiers sur votre volume sécurisé sont AES-CBC et 256 bits. Vous pouvez modifier ces valeurs dans le fichier JSON de configuration de la politique. Pour plus d'informations, reportez-vous au *Guide de configuration avancée*.

9. Cliquez sur **Terminer**.
Le volume s'affiche désormais dans l'Explorateur Windows. Tous les fichiers placés sur ce volume sont chiffrés et accessibles pour tout utilisateur autorisé.

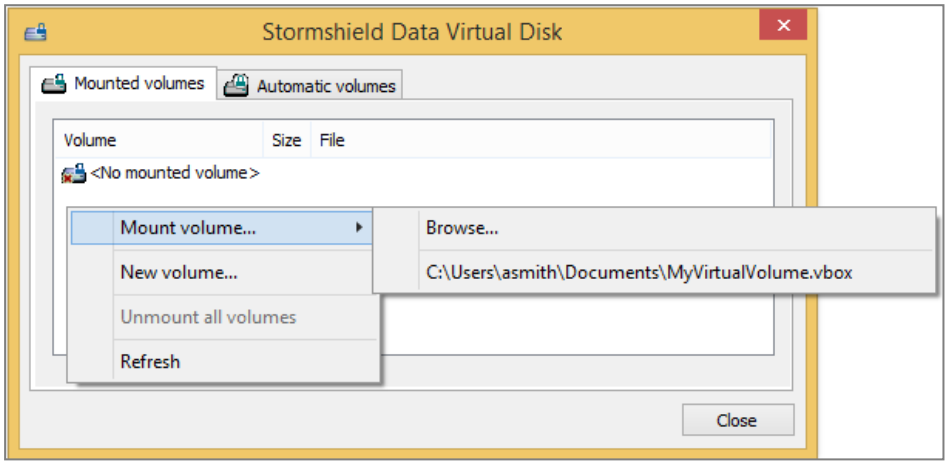
NOTE
Le fichier de secours *.vboxsave* est créé dans le même répertoire que le fichier container *.vbox*.



8.2 Monter un volume sécurisé

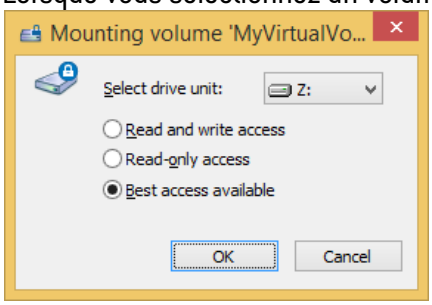
Pour monter un volume existant :

1. Dans la barre de recherche Windows, recherchez Stormshield Data Virtual Disk.
2. À partir du panneau de contrôle de Stormshield Data Virtual Disk, sélectionnez l'onglet *Volume montés*.
3. Par un clic droit, choisissez **Monter un volume** puis **Parcourir** pour sélectionner le volume à monter. Les volumes récemment créés sont listés sous l'option **Parcourir** et peuvent être directement sélectionnés.



> **NOTE**
> L'onglet *Volumes Automatiques* permet de monter un volume automatique s'il a été démonté ou n'a pas été monté avec succès.

4. Lorsque vous sélectionnez un volume à monter, la boite de dialogue suivante s'affiche :



Sélectionnez l'unité et le type d'accès :

- **Accès en lecture et écriture** : uniquement possible si le volume n'a pas encore été monté.
- **Lecture seulement** : le volume est en accès lecture seulement. Possible uniquement si le volume n'a pas été déjà monté en accès lecture et écriture.
- **Meilleur accès disponible** :
  - le volume sera monté en accès lecture/écriture s'il n'a pas encore été monté ;
  - le volume sera monté en accès lecture seule s'il a déjà été monté en accès lecture seule ;
  - un message d'erreur sera affiché si le volume a déjà été monté en accès lecture et écriture.

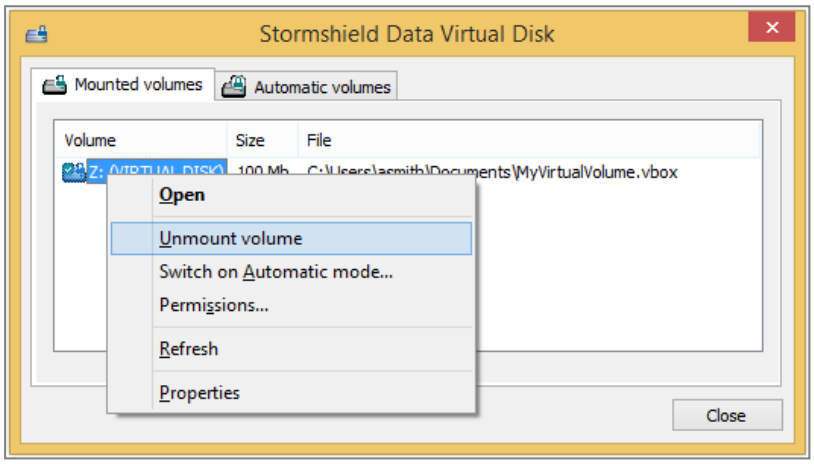
Aucun lecteur réseau ou aucune clé USB ne doit utiliser la même lettre de lecteur. Si la lettre pour monter le lecteur sélectionné est déjà prise, un message d'erreur s'affiche.

Généralement, un volume chiffré est monté en local sur votre poste.

Un volume peut également être monté sur un serveur de fichiers depuis votre poste. Dans ce cas, les échanges de données entre le serveur et votre poste sont chiffrés. Le déchiffrement se fait en local.

8.3 Démonter un volume sécurisé

- Pour démonter un volume sécurisé, sélectionnez ce volume à partir du panneau de contrôle Stormshield Data Virtual Disk et choisissez **Démonter le volume** à partir du menu contextuel.



NOTE
La liste montre également les volumes automatiques. Démonter un volume automatique peut donc se faire à partir de cette fenêtre mais également en sélectionnant l'onglet *Volumes automatiques*.

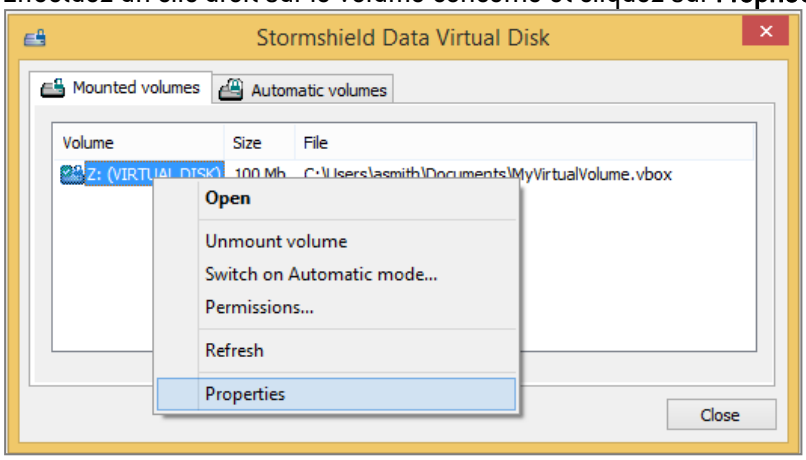
8.4 Accéder aux propriétés d'un volume sécurisé

Stormshield Data Virtual Disk permet d'accéder aux propriétés à partir :

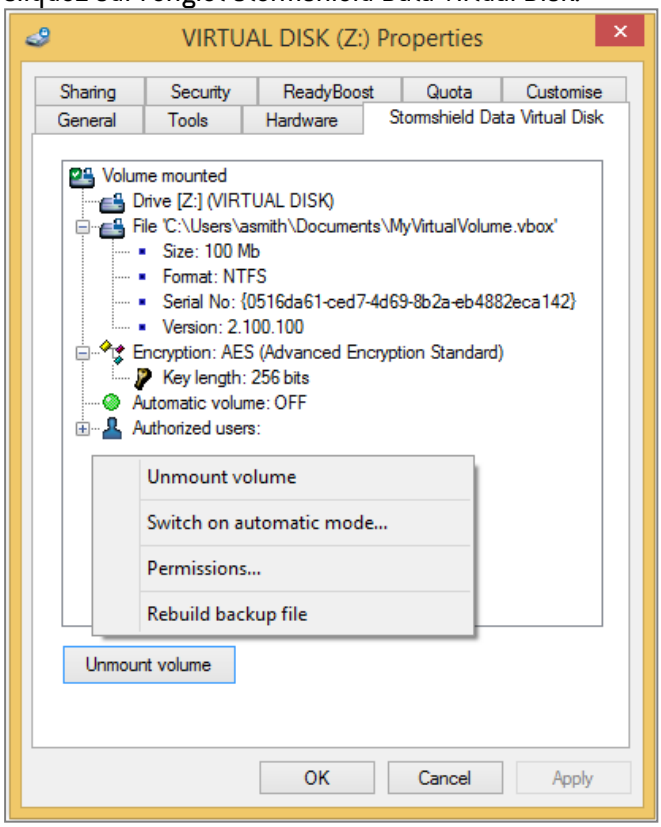
- du panneau de contrôle de Stormshield Data Virtual Disk pour les volumes montés et volumes automatiques,
- du fichier container pour les volumes non montés.

8.4.1 À partir du panneau de contrôle Stormshield Data Virtual Disk

1. Effectuez un clic droit sur le volume concerné et cliquez sur **Propriétés**.



2. Cliquez sur l'onglet Stormshield Data Virtual Disk.

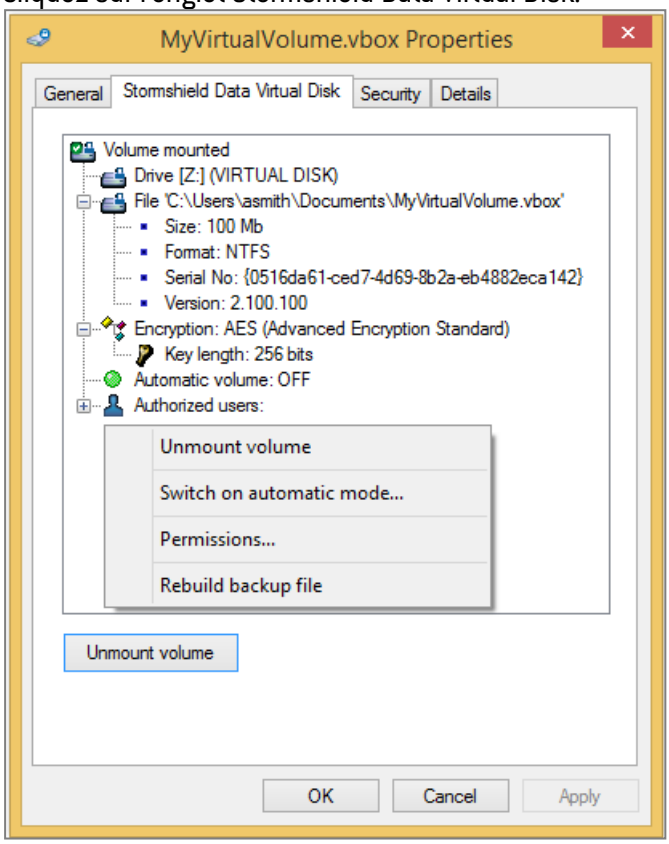


3. En effectuant un clic droit dans la fenêtre de l'onglet, vous pouvez :
   - Démonter le volume (le bouton **Démonter** permet également cette opération),
   - Modifier le mode du volume (manuel ou automatique),
   - Modifier les droits d'accès des utilisateurs,
   - Régénérer un fichier de secours.

> **NOTE**
> Le fichier de secours *.vboxsave* est créé dans le même répertoire que le fichier container *.vbox*.

8.4.2 À partir du fichier container

1. À partir de l'Explorateur Windows, effectuez un clic droit sur le fichier container et cliquez sur **Propriétés**.
2. Cliquez sur l'onglet Stormshield Data Virtual Disk.



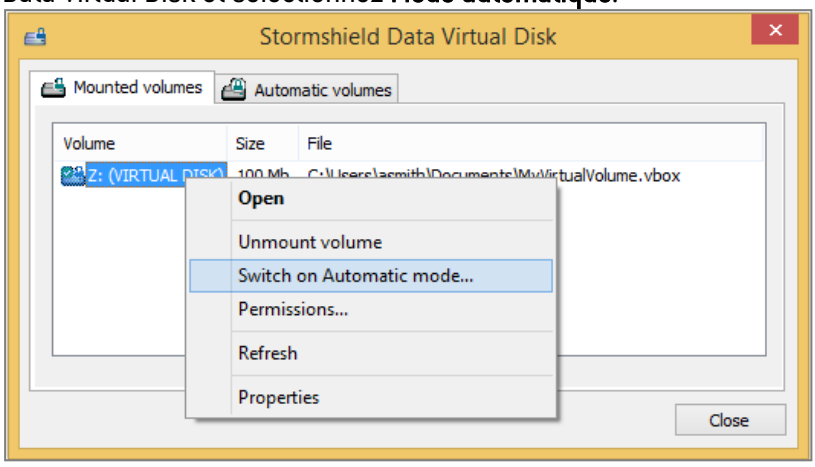
3. En effectuant un clic droit dans la fenêtre de l'onglet, vous pouvez :
   - Démonter le volume (le bouton **Démonter** permet également cette opération),
   - Modifier le mode du volume (manuel ou automatique),
   - Modifier les droits d'accès des utilisateurs,
   - Régénérer un fichier de secours.

8.5 Monter automatiquement un volume sécurisé

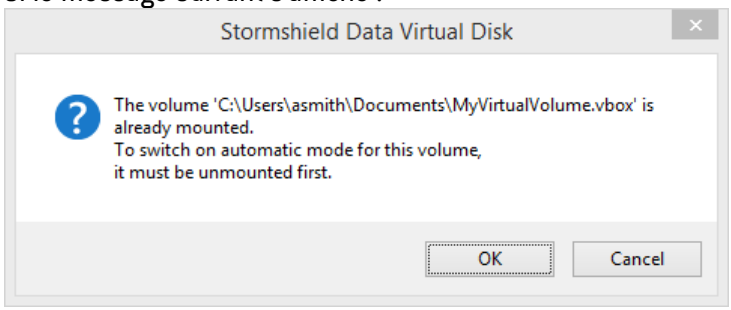
Si vous choisissez l'option montage automatique des volumes, Stormshield Data Virtual Disk monte automatiquement les volumes sécurisés lors de la connexion à SDS Enterprise.

8.5.1 Passer en mode automatique

1. Effectuez un clic droit sur le volume sécurisé depuis le panneau de contrôle de Stormshield Data Virtual Disk et sélectionnez **Mode automatique**.

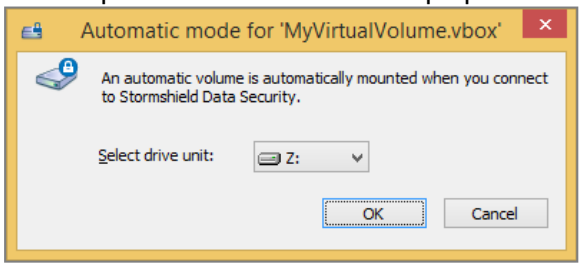


Si le message suivant s'affiche :



Le volume doit d'abord être démonté. Vérifiez qu'aucune application en cours n'utilise de fichiers sur ce volume et cliquez sur **OK**.

2. Sélectionnez la lettre (du lecteur de montage) à utiliser pour monter le volume. Par défaut, la lettre précédemment utilisée est proposée.

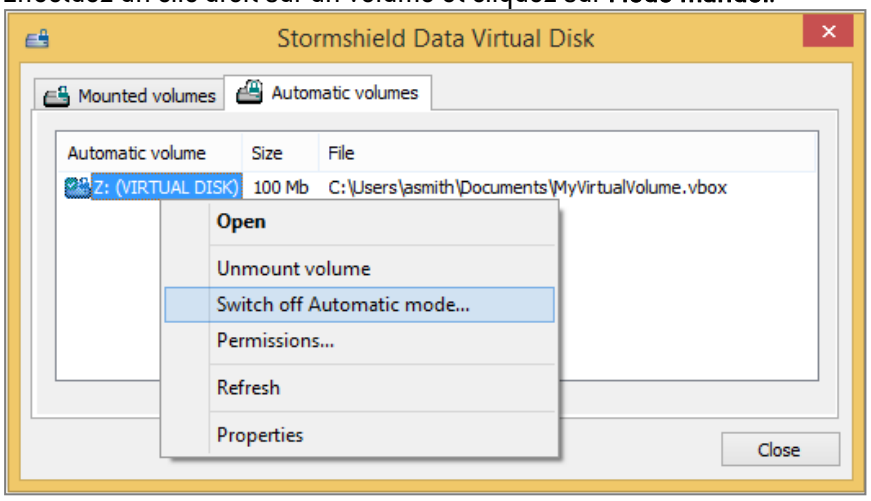


Aucun lecteur réseau ou aucune clé USB ne doit utiliser la même lettre de lecteur.

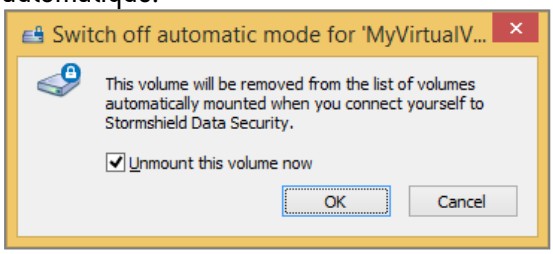
8.5.2 Passer en mode manuel

1. Sélectionnez l'onglet **Volumes automatiques** à partir du panneau de contrôle de Stormshield Data Virtual Disk.

2. Effectuez un clic droit sur un volume et cliquez sur **Mode manuel**.



3. Une fenêtre de confirmation s'affiche. Avant de cliquer sur **OK** vous pouvez demander de démonter le volume en cochant l'option **Démonter le volume maintenant**. Contrairement à ce qui se passe lors du passage en mode automatique, il n'y a pas de démontage automatique.



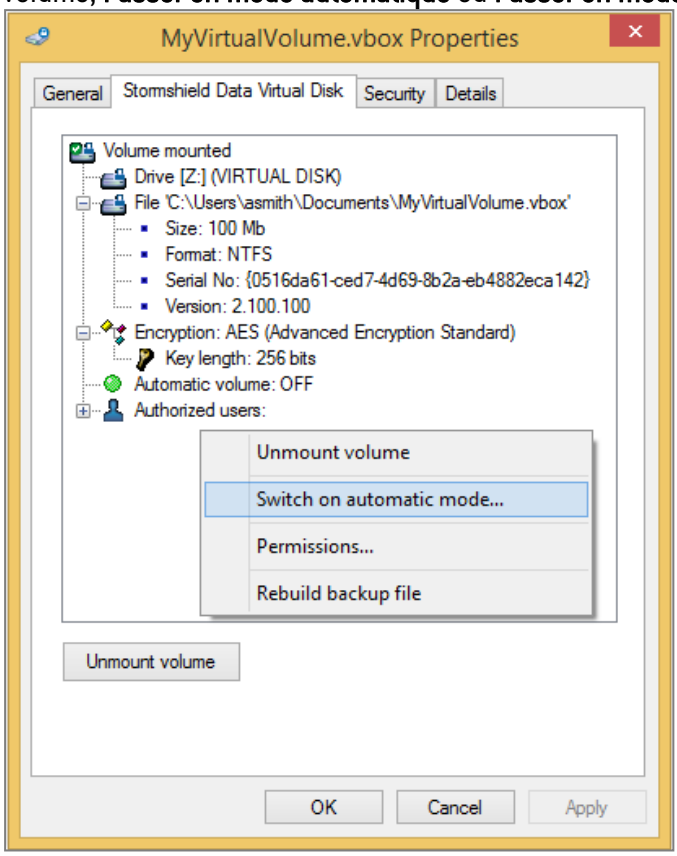
4. Cliquez sur **OK** pour valider votre choix.

8.5.3 Activer et désactiver le mode automatique à partir du fichier container

Il est possible d'activer ou désactiver le mode automatique à partir du fichier container. Dans ce cas, il n'est pas nécessaire d'avoir monté le volume pour activer le mode automatique.

1. A partir de l'Explorateur Windows, effectuez un clic droit sur le fichier container et sélectionnez **Propriétés**.
2. Sélectionnez l'onglet Stormshield Data Virtual Disk.

3. Effectuez un clic droit dans la fenêtre et sélectionnez, en fonction du mode courant du volume, **Passer en mode automatique** ou **Passer en mode manuel**.



8.6 Modifier la liste des utilisateurs

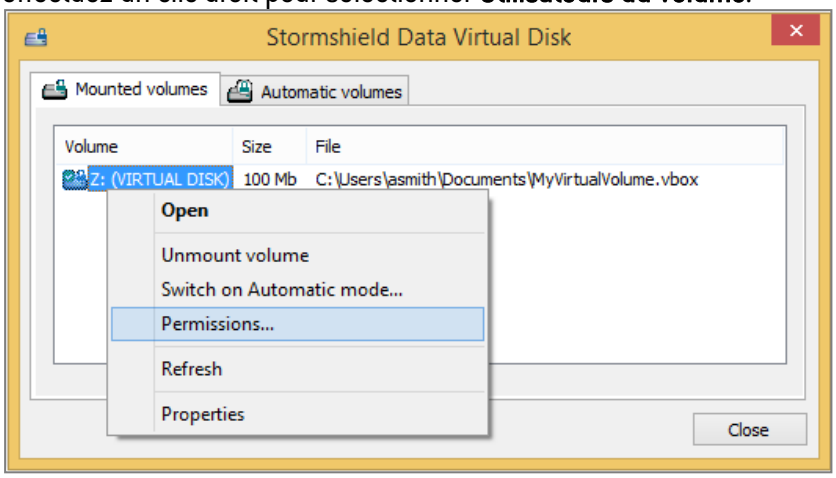
La modification de la liste des utilisateurs requiert que le volume soit déjà monté ou soit en mode automatique.

Seul le propriétaire d'un volume est autorisé à en modifier la liste des utilisateurs autorisés. Cette modification peut se faire à partir :

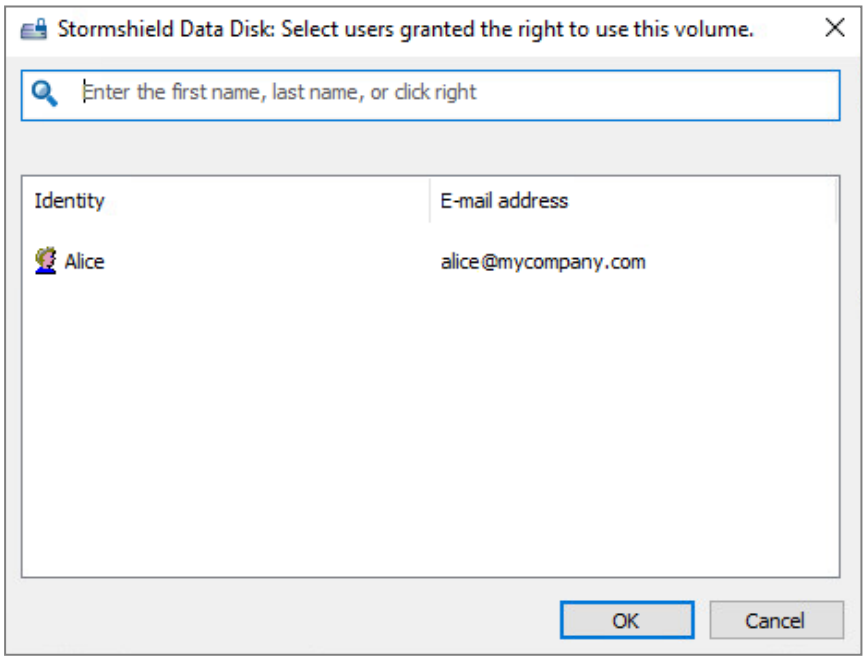
- du panneau de contrôle de Stormshield Data Virtual Disk pour les volumes montés et automatiques,
- du fichier container.

8.6.1 À partir du panneau de contrôle Stormshield Data Virtual Disk

1. À partir de l'onglet **Volumes montés** ou **Volumes automatiques**, sélectionnez un volume et effectuez un clic droit pour sélectionner **Utilisateurs du volume**.



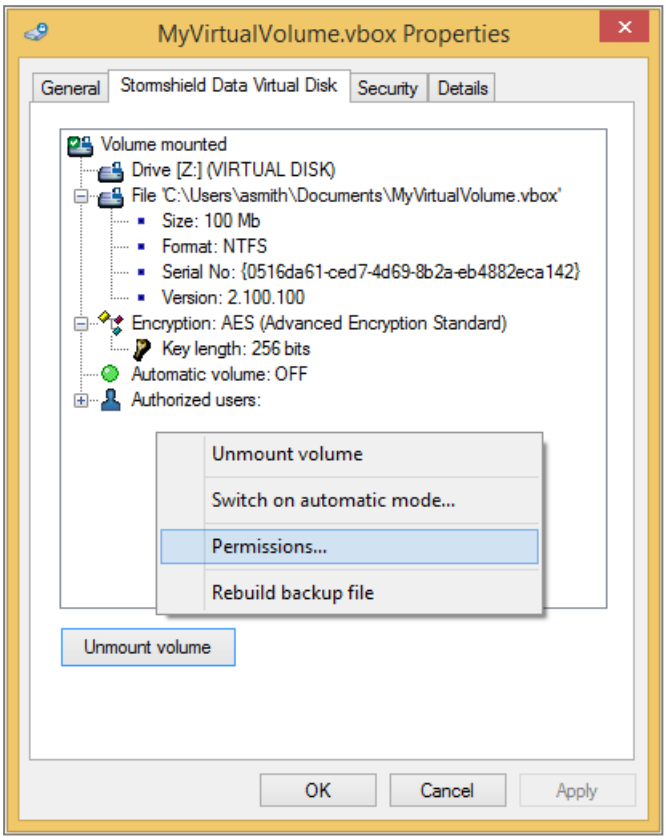
2. La liste des utilisateurs qui ont accès au volume s'affiche. Recherchez les utilisateurs ou groupes auxquels vous souhaitez donner le droit d'accès au volume. La recherche peut afficher les utilisateurs présents dans l'annuaire de confiance ou dans l'annuaire LDAP dans le cas où il est configuré. Elle affiche les utilisateurs ou membres de groupe dont le certificat est valide ou révoqué.
   - Les groupes provenant de l'annuaire local affichent une icône verte,
   - Les groupes provenant de l'annuaire LDAP affichent une icône jaune,
   - Un appui sur la touche Entrée dans le champ de recherche lance directement une recherche dans l'annuaire LDAP.



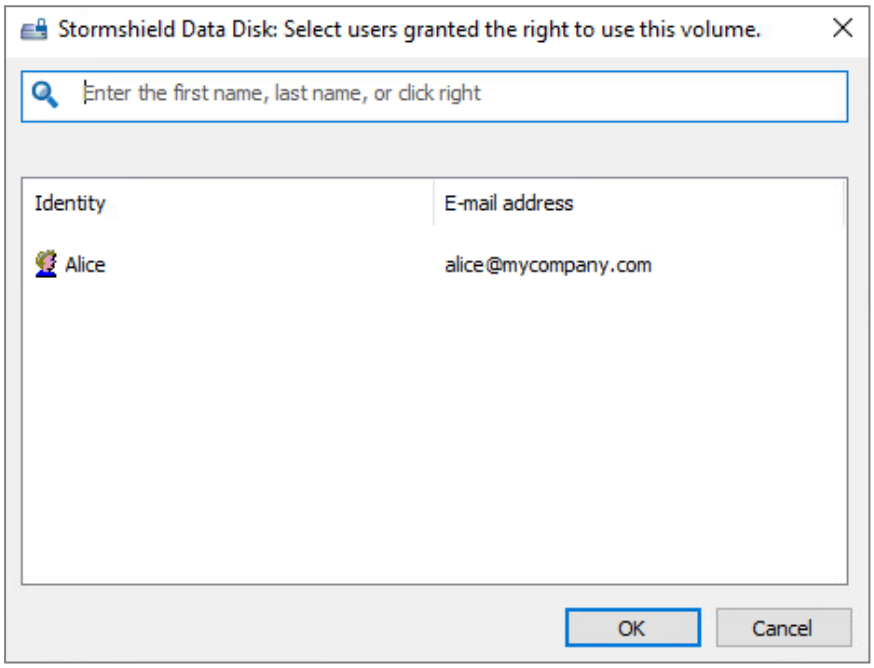
8.6.2 À partir du fichier container

1. À partir de l'Explorateur Windows, effectuez un clic droit sur le fichier container et cliquez sur **Propriétés**.
2. Cliquez sur l'onglet Stormshield Data Virtual Disk.

3. Dans la fenêtre de l'onglet, effectuez un clic droit et sélectionnez **Modifier la liste des utilisateurs**.



4. La liste des utilisateurs qui ont accès au volume s'affiche. Recherchez les utilisateurs ou groupes auxquels vous souhaitez donner le droit d'accès au volume. La recherche peut afficher les utilisateurs présents dans l'annuaire de confiance ou dans l'annuaire LDAP dans le cas où il est configuré. Elle affiche les utilisateurs ou membres de groupe dont le certificat est valide ou révoqué.
   - Les groupes provenant de l'annuaire local affichent une icône verte,
   - Les groupes provenant de l'annuaire LDAP affichent une icône jaune,
   - Un appui sur la touche Entrée dans le champ de recherche lance directement une recherche dans l'annuaire LDAP.



8.7 Modifier le propriétaire d'un volume

Cette fonction est une fonction avancée qui doit être utilisée avec précaution et qui nécessite l'application d'une politique de sécurité spécifique.

Le nouveau propriétaire doit faire partie de la liste des utilisateurs autorisés. Pour l'ajouter, reportez-vous à la section Modifier la liste des utilisateurs.

1. Dans les paramètres du fichier de configuration *.json* de la politique appliquée au poste de travail de l'utilisateur concerné, indiquez les paramètres suivants :

```
"diskPolicy" : {
 "enableRescueFileModification": true,
 "enableExpertMode": true
},
```

   Pour plus d'informations sur la modification de la politique de sécurité, reportez-vous au *Guide de configuration avancée*.
2. Redéployez le fichier de la politique mise à jour sur le poste de l'utilisateur concerné.
3. Sur le poste de l'utilisateur, assurez-vous que l'utilisateur connecté est le propriétaire du volume puis ouvrez le répertoire qui contient le fichier container dans l'Explorateur Windows. Ce répertoire contient le fichier container (extension *.vbox*) et un autre fichier portant le même nom mais suivi de l'extension *.vboxsave* (il s'agit du fichier de secours).
4. Effectuez un clic droit sur le fichier *.vboxsave* et sélectionnez **Propriétés**.

5. Sélectionnez l'onglet Stormshield Data Virtual Disk et cliquez sur le signe + à gauche des utilisateurs autorisés pour en voir la liste complète.
6. Effectuez un clic droit sur le nom du nouveau propriétaire et sélectionnez **Sélectionner comme nouveau propriétaire**.

> **NOTE**
> Si le choix **Sélectionner comme nouveau propriétaire** n'est pas proposé, le fichier *.json* n'a pas été correctement modifié ou déployé sur le poste ; il se peut également que l'utilisateur actuellement connecté ne soit pas le propriétaire du volume.

Une fois le nouveau propriétaire sélectionné, un message d'avertissement s'affiche au bas de la fenêtre pour vous informer que la liste des utilisateurs autorisés du fichier *.vboxsave* est différente de celle du fichier *.vbox*.

7. Cliquez sur **Mettre à jour le volume** pour synchroniser les deux listes.

> **NOTE**
> Si vous modifiez le propriétaire d'un volume alors que vous n'êtes pas le propriétaire de ce volume, il est nécessaire d'effectuer un recouvrement du volume. Pour cela, vous devez être autorisé à effectuer l'opération de recouvrement. Consultez le *Guide d'administration SDS Enterprise* pour plus d'informations.

9. Sécuriser des messages électroniques

La fonctionnalité Stormshield Data Mail est une extension qui s'intègre dans votre client de messagerie Outlook pour ajouter à vos messages les services de sécurité suivants :

- **La confidentialité** du message : seuls les destinataires pourront lire le message transmis. Elle est assurée par le chiffrement du message.
- **L'intégrité** du message : il ne peut pas être modifié en cours de transfert sans que cela ne soit détecté.
- **L'authentification de l'émetteur** : le destinataire du message est certain de l'identité de l'émetteur.
  L'intégrité du message et l'authentification de l'émetteur sont garanties par une signature électronique.

Les messages sécurisés sont conservés sous cette forme dans votre base de messages.

Stormshield Data Mail implémente la norme S/MIME V3 : vous pouvez échanger des messages sécurisés avec tout correspondant possédant un logiciel de messagerie supportant la norme S/MIME V2 ou V3.

Stormshield Data Mail ne peut pas s'ajouter aux fonctions de sécurité natives d'Outlook. Un message doublement sécurisé ne pourra être lu par son destinataire.

Stormshield Data Mail est disponible sous forme d'add-in pour les clients de messagerie Microsoft Outlook 2019 et 365 Professional.

Elle est compatible avec les serveurs de messagerie suivants :

- Microsoft Exchange Server 2010 SP1/SP2/SP3
- Microsoft Exchange Server 2013 SP1
- Microsoft Exchange Server 365
- Microsoft Exchange Server 2019

Pour des informations sur le paramétrage de Stormshield Data Mail dans SDMC, reportez-vous au *Guide d'administration SDS Enterprise*.

9.1 Envoyer un message sécurisé

Votre message n'est sécurisé qu'à son envoi. Lorsqu'il est sauvegardé en tant que brouillon, il n'est pas sécurisé.

1. Connectez-vous à SDS Enterprise.
2. Écrivez le message comme vous le faites d'habitude avec votre client de messagerie. Utilisez le format HTML pour la rédaction de votre message. Le format Texte enrichi (RTF) n'est pas supporté par Stormshield Data Mail car il présente un risque de perte d'informations.
3. Si vous souhaitez signer le message, dans la zone **Sécurité** de l'onglet *Message*, cliquez sur l'icône . La signature d'e-mails au format PGP n'est pas supportée.
   - ou -
   Si vous souhaitez chiffrer le message, dans la zone **Sécurité** de l'onglet *Message*, cliquez sur l'icône .

   Le bandeau inférieur Stormshield Data Security s'affiche dans la fenêtre du message et indique les options de sécurité sélectionnées.

4. Dans le bandeau inférieur, cliquez sur le lien **Modifier...** pour choisir le format d'émission des messages sécurisés, S/MIME ou PGP. Ce choix n'est offert que si le format PGP a été configuré dans la politique. Pour plus d'informations, reportez-vous au Guide d'administration *SDS Enterprise*, sections *Configurer Stormshield Data Mail* et *Configurer les annuaires d'entreprise*.
5. Cliquez sur **Envoyer**.

Le message envoyé est placé dans le dossier approprié (**Éléments envoyés** par défaut), sécurisé avec les options de sécurité sélectionnées. Si vous avez choisi le chiffrement, le message est automatiquement chiffré avec votre clé publique. Il sera déchiffré quand vous l'ouvrirez.

NOTE
L'édition d'un message sécurisé directement dans la boite d'envoi n'est pas supportée.

9.2 Lire un message sécurisé

Cette section vous explique comment consulter un message sécurisé et y répondre.

9.2.1 Ouvrir un message sécurisé

Vous recevez et lisez vos messages comme vous avez l'habitude de le faire avec votre client de messagerie. Si un message a été chiffré par son émetteur, Stormshield Data Mail se charge de le déchiffrer au moment où vous l'ouvrez. Si le message comporte une signature, Stormshield Data Mail la vérifie et signale les éventuelles anomalies détectées.

Si vous n'êtes pas connecté à SDS Enterprise, une fenêtre vous invite à vous connecter pour pouvoir lire le message ou vérifier la signature.

NOTE
Un fichier *.msg* chiffré et/ou signé ne peut être ouvert depuis l'Explorateur Windows. Reportez-vous à l'article à ce sujet dans la Base de connaissancesStormshield (anglais uniquement).

IMPORTANT
Il est interdit de modifier un message sécurisé reçu avec le menu Outlook **Actions > Modifier le message** car cette opération pourrait désactiver la sécurité du message.

9.2.2 Consulter le compte-rendu de sécurité

A l'ouverture d'un message sécurisé, vous pouvez consulter le compte-rendu de sécurité en cliquant sur le lien dans le bandeau inférieur Stormshield Data Security.

Une icône est visible à côté du lien **Compte-rendu de sécurité** pour signaler une erreur ou un avertissement consultables dans le compte-rendu. En cas d'erreur, le bandeau de sécurité apparaît en rouge.

Le compte-rendu de sécurité indique le détail des algorithmes employés pour le chiffrement et la signature du message.

Si le message est signé, le compte-rendu comprend également :

- L'identité de l'émetteur signataire du message,
- Un indicateur de confiance à accorder au certificat de l'émetteur dans le bandeau supérieur de la fenêtre du compte-rendu qui indique :
  - Le résultat de la vérification cryptographique de la signature. La signature est alors considérée comme correcte ou incorrecte,
  - Le résultat des contrôles effectués sur le certificat de l'émetteur : Stormshield Data Mail vérifie que le certificat est valide, qu'il est autorisé à signer et qu'il ne présente aucune extension critique non supportée. S'il en comporte une, la règle de sécurité l'oblige à rejeter le certificat.

NOTE
La vérification de la signature de messages signés au format PGP n'est pas supportée par Stormshield Data Mail. Un message indiquant que la signature n'a pas pu être vérifiée est affiché dans le bandeau de sécurité pour les messages de ce type.

9.2.3 Répondre ou transférer un message chiffré

Lorsque vous répondez à un ou plusieurs destinataires d'un message chiffré, l'option de chiffrement est automatiquement sélectionnée dans votre message de réponse.

Ce mécanisme s'applique également lors du transfert des messages chiffrés.

9.2.4 Lire un message sécurisé attaché en pièce jointe

Pour lire un message sécurisé qui se trouve en pièce jointe d'un autre message (sécurisé ou non), glissez-déposez le dans un des dossiers de votre boîte de réception.

Lorsque des messages comportant des pièces jointes sont réceptionnés, Outlook indique la taille de ces pièces jointes. Dans le cas de messages chiffrés, Outlook indique systématiquement "0 octet".

9.2.5 Lire un message sécurisé au format OpenPGP

Stormshield Data Mail est capable de déchiffrer les messages sécurisés par un client de messagerie supportant le protocole OpenPGP (format PGP/MIME). Il faut au préalable avoir importé les clés de déchiffrement au format OpenPGP dans votre porte-clés.

Pour plus d'informations, reportez-vous au *Guide d'administration SDS Enterprise*.

Importer un porte-clés OpenPGP

1. Faites un clic droit sur l'icône SDS Enterprise et choisissez **Propriétés**.
2. Dans l'onglet *Configuration*, double-cliquez sur **Porte-clés**.
3. Sélectionnez l'onglet **Porte-clés OpenPGP**.
4. Cliquez sur **Opérations** puis **Importer un porte-clés**.
5. Sélectionnez un fichier au format OpenPGP (*.gpg*, *.pgp*ou *.asc*). Le fichier peut contenir plusieurs clés.
6. Saisissez le mot de passe protégeant le fichier.

Pour supprimer ou remplacer le porte-clés, sélectionnez les menus **Supprimer le porte-clés** ou **Remplacer le porte-clés** dans le menu **Opérations**.

Le remplacement du porte-clés écrase le porte-clés déjà présent.

Lire un message sécurisé au format OpenPGP

Vous recevez et lisez vos messages comme vous avez l'habitude de le faire avec votre client de messagerie. Si un message a été chiffré par son émetteur, Stormshield Data Mail se charge de le déchiffrer au moment où vous l'ouvrez.

Si vous n'êtes pas connecté à SDS Enterprise, une fenêtre vous invite à vous connecter pour pouvoir lire le message.

La sécurité d'un message chiffré et signé ou seulement signé au format OpenPGP ne peut pas être désactivée.

NOTE
La vérification de la signature de messages signés au format PGP n'est pas supportée par Stormshield Data Mail. Un message indiquant que la signature n'a pas pu être vérifiée est affiché dans le bandeau de sécurité pour les messages de ce type.

Lire un message sécurisé au format PGP Partitionné

Le format PGP Partitionné est le prédécesseur du format PGP/MIME. Les deux formats s'appuient sur les mêmes mécanismes de sécurité et le format de porte-clés est donc le même.

La lecture d'un message sécurisé au format PGP Partitionné s'effectue de la même façon que la lecture d'un message au format PGP/MIME.

9.3 Transchiffrer les messages sécurisés

Le transchiffrement est une opération qui permet de mettre à jour le niveau de protection des messages sécurisés en re-chiffrant avec une nouvelle clé les messages ayant été sécurisés avec une ancienne clé de chiffrement et en utilisant l'algorithme de chiffrement configuré par défaut dans le compte utilisateur.

L'ancienne clé de chiffrement peut devenir obsolète pour les raisons suivantes :

- La clé de chiffrement a été renouvelée,
- Le compte utilisateur a été mis à jour et la clé de chiffrement est devenue inutilisable. Par exemple lors du passage d'un compte mot de passe à un compte carte, d'une révocation de clé, clé provenant d'un autre système de chiffrement, etc,
- La clé de chiffrement a été transmise par un tiers, par exemple lors d'une passation de pouvoir dans le cadre d'un changement de poste.

Pour transchiffrer un message sécurisé, l'ancienne clé de chiffrement est nécessaire afin de le déchiffrer au préalable. Elle doit donc être présente dans le porte-clés en tant que clé de déchiffrement.

Une fois transchiffré, le message est alors déchiffrable uniquement avec la nouvelle clé.

Un message ou une pièce jointe est transchiffré dans son format d'origine : s'il est au format .sbox, il reste au format .sbox après transchiffrement.

NOTE
Une clé de délégation ne peut pas être utilisée pour transchiffrer car elle donne uniquement le droit de lire des messages sécurisés.

9.3.1 Transchiffrement et gestion des collaborateurs

Le comportement du processus de transchiffrement vis-à-vis des collaborateurs est le suivant dans ces deux cas :

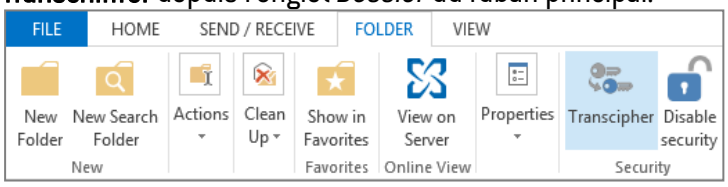
- Lorsqu'un message sécurisé au format S/MIME reçu par plusieurs destinataires est transchiffré, il est alors sécurisé uniquement pour l'utilisateur courant. Les collaborateurs ne sont pas impactés car seule la copie personnelle locale du message est transchiffrée.
- Lorsqu'un message en clair avec une pièce jointe sécurisée est transchiffré, seul le niveau de sécurité de la pièce jointe est mis à jour. Si cette pièce jointe est transférée aux collaborateurs déclarés dans le fichier *.sbox* original et si leurs certificats sont toujours valides, ceux-ci pourront toujours accéder à la pièce jointe.

Les comptes de recouvrement associés aux comptes utilisateur sont quant à eux toujours intégrés aux messages transchiffrés.

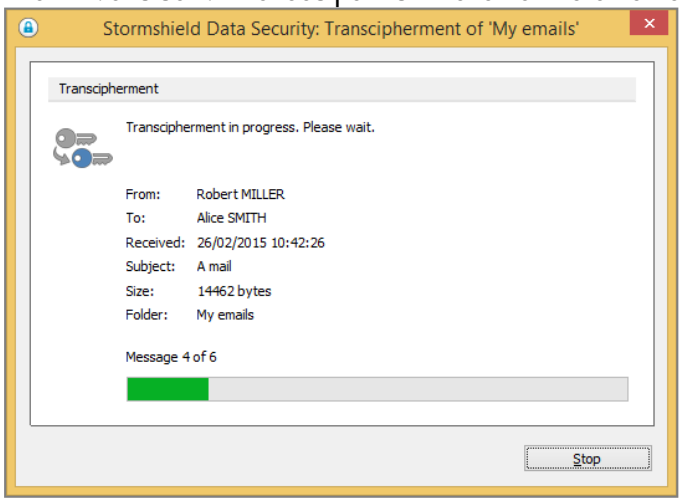
9.3.2 Utiliser le transchiffrement

Le transchiffrement est une opération qui s'effectue sur un dossier de votre messagerie Outlook et l'ensemble de ses sous-dossiers.

1. Sélectionnez le dossier à transchiffrer.
2. Faites un clic droit sur le dossier et sélectionnez **Transchiffrer** ou bien cliquez sur **Transchiffrer** depuis l'onglet *Dossier* du ruban principal.



3. Dans la fenêtre de transchiffrement, cliquez sur **Transchiffrer**. Au cours du traitement, des informations sont affichées pour suivre le bon déroulement des opérations.



4. A la fin du processus, un rapport affiche le nombre de messages transchiffrés et le nombre d'erreurs rencontrées. En cas d'erreur, cliquez sur le bouton **Voir le compte-rendu**.

Le compte-rendu détaille le type d'erreur pour chaque message concerné :

- L'utilisateur ne possède pas de clé de chiffrement valide,
- L'utilisateur ne possède qu'une clé de délégation,
- Le traitement du message a provoqué une erreur,

- La fonctionnalité File n'est pas installée (dans le cas où le message contient une pièce jointe sécurisée).

Le fichier de compte-rendu est intitulé *SBoxTransciphermentReport-<utilisateur>-<horodatage>.txt* et se trouve dans le dossier temporaire de l'utilisateur. Ce fichier est conservé dans ce dossier.

NOTE
L'accès aux clés privées de l'utilisateur pendant le transchiffrement nécessite d'être connecté au compte SDS Enterprise.

La fenêtre de progression empêche toute interaction avec Outlook pendant la durée du processus. Si malgré cela, le transchiffrement est interrompu, il faut le relancer manuellement.

9.3.3 Limitations du transchiffrement

Certaines configurations de messages transchiffrés ne sont pas prises en charge par le processus de transchiffrement :

- Une pièce jointe sécurisée contenue dans un message sécurisé S/MIME n'est pas transchiffrée,
- Un message sécurisé transmis en tant que pièce jointe *.MSG* dans un message en clair n'est pas transchiffré.

Le transchiffrement des messages chiffrés à l'aide du protocole OpenPGP n'est pas possible.

9.4 Désactiver la sécurité

Par défaut, les messages sécurisés reçus sont conservés sécurisés dans la base de messages d'Outlook.

Il peut arriver que vous ne souhaitiez pas conserver la sécurité d'un message sécurisé, par exemple si vous voulez le déposer dans un dossier public.

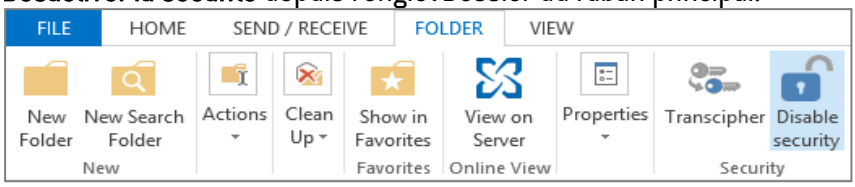
Lors de la désactivation de la sécurité, les messages chiffrés et/ou signés seront stockés en clair, sans chiffrement ni signature.

NOTE
Une clé de délégation ne peut pas être utilisée pour désactiver la sécurité.

La désactivation de la sécurité est une opération qui peut s'effectuer sur un dossier de votre messagerie Outlook et l'ensemble de ses sous-dossiers ou sur une sélection de messages électroniques.

9.4.1 Désactiver la sécurité d'un dossier

1. Faites un clic droit sur un dossier et sélectionnez **Désactiver la sécurité** ou bien cliquez sur **Désactiver la sécurité** depuis l'onglet *Dossier* du ruban principal.



2. Dans la fenêtre de désactivation de la sécurité, cliquez sur **Désactiver la sécurité**. Au cours du traitement, des informations sont affichées pour suivre le bon déroulement des opérations.
3. A la fin du processus, un rapport affiche le nombre de messages désécurisés et le nombre d'erreurs rencontrées. En cas d'erreur, cliquez sur le bouton **Voir le compte-rendu**.

La fenêtre de progression empêche toute interaction avec Outlook pendant la durée du processus. Si malgré cela, la désactivation de la sécurité est interrompue, il faut la relancer manuellement.

9.4.2 Désactiver la sécurité d'une sélection de messages

1. Sélectionnez un ou plusieurs messages.
2. Effectuez un clic droit sur la sélection pour faire apparaître le menu contextuel et sélectionnez **Désactiver la sécurité** ou bien cliquez sur **Désactiver la sécurité** depuis l'onglet *Accueil* du ruban principal.
3. Le reste de la procédure est identique à la désactivation de la sécurité d'un dossier.

9.4.3 Consulter le compte-rendu

Le compte-rendu détaille le type d'erreur pour chaque message concerné :

- L'utilisateur ne possède pas de clé de chiffrement valide,
- L'utilisateur ne possède qu'une clé de délégation,
- Le traitement du message a provoqué une erreur,
- L'utilisateur ne possède pas de clé de chiffrement valide,
- L'utilisateur ne possède qu'une clé de délégation,
- Le traitement du message a provoqué une erreur.

Le fichier de compte-rendu est intitulé *SBoxDeleteSecurityReport-<horodatage>.txt* et se trouve dans le dossier temporaire de l'utilisateur. Ce fichier est conservé dans ce dossier.

Généralement les messages erronés sont des messages chiffrés qui utilisent une clé inconnue. Par exemple, une ancienne clé, qui n'a pas été importée comme clé de déchiffrement dans votre compte.

> **NOTE**
> L'accès aux clés privées de l'utilisateur pendant la désactivation de la sécurité nécessite d'être connecté au compte SDS Enterprise.

9.4.4 Limitations de la désactivation de la sécurité

Certaines configurations de messages ne sont pas prises en charge par le processus de désactivation de la sécurité :

- Un message sécurisé transmis en tant que pièce jointe *.msg* d'un message en clair ou d'un message sécurisé ne peut pas être désécurisé.
- Un message chiffré et signé ou seulement signé au format OpenPGP ne peut pas être désécurisé.

9.5 Interagir avec Stormshield Data Connector

Si le module Stormshield Data Connector est installé sur la machine, vous pouvez envoyer des messages chiffrés et/ou signés depuis un script PowerShell ou un programme .NET.

Pour plus d'informations, consultez le *Guide d'utilisation* de Stormshield Data Connector.

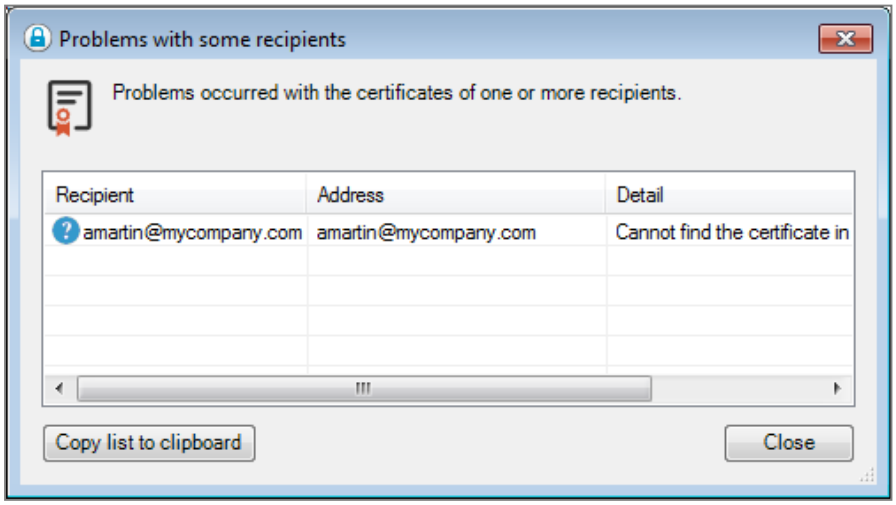
9.6 Résoudre les problèmes

9.6.1 Certificat non trouvé, en erreur ou non valide

Si vous chiffrez votre message, Stormshield Data Mail recherche dans votre annuaire de confiance et éventuellement dans vos annuaires LDAP le certificat de chaque destinataire. Il vérifie aussi que chaque certificat est valide, permet le chiffrement, ne présente aucune extension critique non supportée.

NOTE
Il n'est pas possible de rechercher les certificats des destinataires lors de l'envoi d'un message à un groupe de distribution dynamique. En effet, l'adresse e-mail des membres de ce type de groupes n'est pas accessible par SDS Enterprise.

Si lors de l'envoi, au moins un certificat est absent ou introuvable, Stormshield Data Mail indique les destinataires concernés par un signe ?.



Vous devez résoudre les problèmes de certificats avant de pouvoir envoyer votre message. S'ils sont absents de votre annuaire, vous devez les importer au préalable. Si les destinataires font

partie d'un groupe de contacts, vous pouvez retirer les destinataires dont le certificat pose problème.

Stormshield Data Mail indique les certificats en avertissement (certificat auto-certifié, liste de révocation périmée, etc…) par un signe  . Si, lors de l'envoi, tous les certificats sont en avertissement, vous pouvez poursuivre quand même l'envoi avec le bouton **Continuer** ou résoudre les problèmes soulevés par les certificats après annulation de l'envoi.

Si, lors de l'envoi, au moins un certificat est en erreur (périmé, révoqué, etc…), Stormshield Data Mail indique les certificats incriminés par un signe  . Vous devez résoudre les problèmes de certificats avant de pouvoir envoyer votre message.

IMPORTANT
En cas de changement d'adresse e-mail d'un collaborateur de l'entreprise, il est impératif de renouveler le certificat utilisateur et de le republier sur l'annuaire LDAP le cas échéant. En effet, si l'adresse e-mail du collaborateur n'est pas identique à celle indiquée sur ses certificats, le collaborateur ne pourra plus envoyer de message sécurisé.

10. Signer des documents

La fonctionnalité Stormshield Data Sign permet de signer électroniquement des documents. Les signatures électroniques sont basées sur une infrastructure à clé publique (PKI). Elles résultent d'une opération cryptographique.

Stormshield Data Sign permet donc de garantir l'authenticité des signataires et l'intégrité du contenu d'un fichier.

En outre, signer un document avec Stormshield Data Sign peut être considéré comme un engagement au même titre qu'une signature manuscrite peut le faire.

Lorsqu'un utilisateur signe un document avec Stormshield Data Sign :

- L'empreinte unique du document est créée à l'aide d'un algorithme mathématique.
- L'empreinte du document est signée avec sa clé privée puis est combinée avec sa clé publique et son certificat pour créer une signature électronique unique qui sera ajoutée au document.

Stormshield Data Sign place le document signé dans un nouveau fichier qui porte le même nom de fichier que le fichier original mais a une extension différente. Le document signé est scellé et tout changement apporté au document après la signature invalide la signature. C'est une façon de protéger le document contre toute falsification des données et de signature.

Lorsque vous vérifiez un document signé avec Stormshield Data Sign :

- La signature de l'expéditeur est vérifiée à l'aide de la clé publique de l'expéditeur et l'empreinte du document original est extraite. Stormshield Data Sign calcule à son tour l'empreinte du document signé et compare le résultat à l'empreinte originale extraite. Si les empreintes sont identiques, l'authenticité du document est validée.
- L'authenticité et la validité du certificat de l'expéditeur, et donc de sa signature, sont vérifiées à l'aide de la liste de révocation.

Pour des informations sur le paramétrage de Stormshield Data Sign dans SDMC, reportez-vous au *Guide d'administration SDS Enterprise*.

10.1 Connaître les caractéristiques de Stormshield Data Sign

10.1.1 Différents types de signatures

Stormshield Data Sign permet d'apposer différents types de signatures sur un document. Il est possible de :

- **co-signer** un document en ajoutant votre propre signature à un document déjà signé, indépendamment des autres signatures déjà présentes.
  Par exemple, un contrat entre deux parties requiert la signature des deux parties pour être valide. Stormshield Data Sign permet à chaque partie de signer le document indépendamment l'une de l'autre et, ce, dans n'importe quel ordre.
- **contre-signer** un document signé en ajoutant votre propre signature sur une autre signature.
  Par exemple, pour être payée, une facture doit être d'abord signée par le commanditaire qui valide la facture, puis contre-signée par le comptable. Le paiement nécessite les deux signatures : le comptable doit attendre la validation du commanditaire et contre-signe cette validation.

- **sur-signer** un document en apposant votre signature sur l'enveloppe qui contient le document signé.
  Par exemple, un transporteur garantit l'intégrité du document qui lui est confié en le mettant sous enveloppe et en signant cette enveloppe. Aucune co- ou contre-signature ne peut alors être ajoutée ou retirée du document transporté.

10.1.2 Compatibilité

Stormshield Data Sign permet la sauvegarde des documents signés dans deux types de fichiers distincts : les fichiers de type *.p7f* ou *.p7m*.

Les fichiers de type *.p7m* peuvent être expédiés vers et validés par des correspondants qui n'utilisent pas Stormshield Data Sign, mais utilisent un autre logiciel conforme à la norme RFC 2630, qui spécifie les règles de format de la signature électronique.

10.2 Signer un fichier

Si vous êtes sur le point de signer un document Microsoft Word, ou un document PDF, Stormshield Data Sign peut l'analyser et informer de la présence de macros ou de contenu actif pouvant modifier dynamiquement l'apparence du document lors de son affichage. Ces contrôles sont activables dans la configuration de la fonctionnalité Sign. Il vous appartient ensuite de signer ou non le document. Pour plus d'informations, reportez-vous à la section *Configurer Stormshield Data Sign* dans le *Guide d'administration*.

Il existe deux méthodes pour signer un fichier.

10.2.1 Signer depuis le menu contextuel

Pour signer un fichier :

1. Sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Stormshield Data Security > Signer** à partir du menu contextuel.
2. Suivez ensuite les instructions de l'assistant, qui demande systématiquement votre code confidentiel ou votre mot de passe, puis cliquez sur **Quitter** pour terminer la procédure.

Après avoir signé un document avec succès, Stormshield Data Sign ne modifie pas le fichier original. Il génère un nouveau fichier portant le même nom mais avec une extension *.p7f* ou *.p7m*.

Pour signer et chiffrer un fichier :

1. Sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Stormshield Data Security > Signer et chiffrer** à partir du menu contextuel.

   > **NOTE**
   > Ce menu n'est présent que si la fonctionnalité Stormshield Data File est installée.

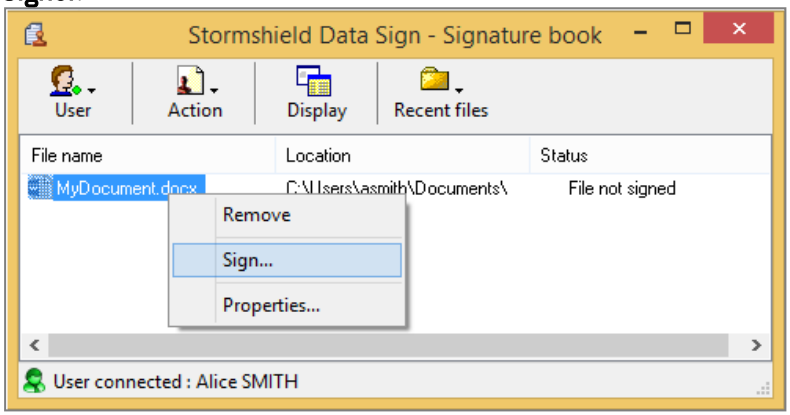
2. Suivez ensuite les instructions de l'assistant, qui demande systématiquement votre code confidentiel ou votre mot de passe, puis cliquez sur **Quitter**.
3. A l'ouverture de la fenêtre **Choix de vos correspondants**, sélectionnez les correspondants pour lesquels vous voulez effectuer le chiffrement puis cliquez sur **OK**.

10.2.2 Signer depuis le parapheur Stormshield Data Sign

1. Sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Envoyer vers > Stormshield Data Sign** à partir du menu contextuel. Le fichier est alors déposé dans le parapheur.

> **NOTE**
> Si le parapheur est déjà ouvert, sélectionnez le fichier désiré pour le déplacer et le déposer dans le Parapheur

2. Dans le parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Signer**.



3. Suivez les instructions de l'assistant, qui demande systématiquement votre code confidentiel ou votre mot de passe.

Après avoir signé un document avec succès, Stormshield Data Sign ne modifie pas le fichier original. Il génère un nouveau fichier portant le même nom mais avec une extension *.p7f* ou *.p7m*.

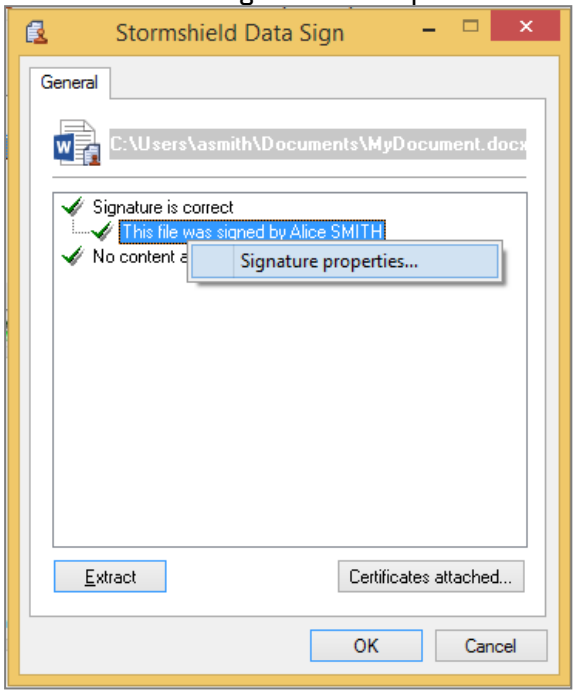
10.3 Vérifier un fichier signé

Utilisez la procédure ci-dessous pour vérifier un fichier signé. Ce dernier doit être un fichier avec une extension de type *.p7f* ou *.p7m*.

1. Dans l'Explorateur Windows, double-cliquez sur le fichier ou faites un clic droit pour sélectionner à partir du menu contextuel **Envoyer vers > Stormshield Data Sign**. La fenêtre du parapheur s'ouvre et le fichier y est déposé.

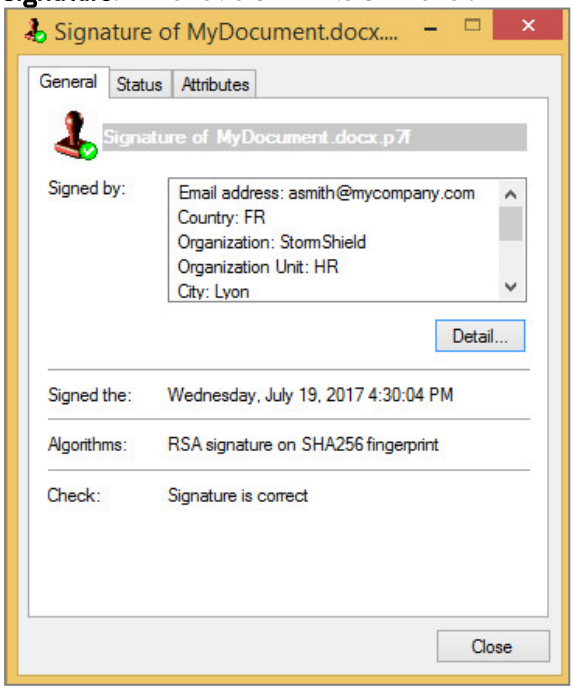
> **NOTE**
> Si la fenêtre du Parapheur est déjà ouverte, vous pouvez utiliser le glisser-déposer pour y placer le fichier.

2. A l'intérieur du parapheur, effectuez un clic droit sur le fichier et sélectionnez **Signatures**. Le certificat du signataire s'affiche (voir ci-dessous). Seul le premier niveau de signatures est affiché. Il inclue la signature, puis les éventuelles co-signatures et contre-signatures. Le second niveau de signature correspondant à la sur-signature n'est pas montré.

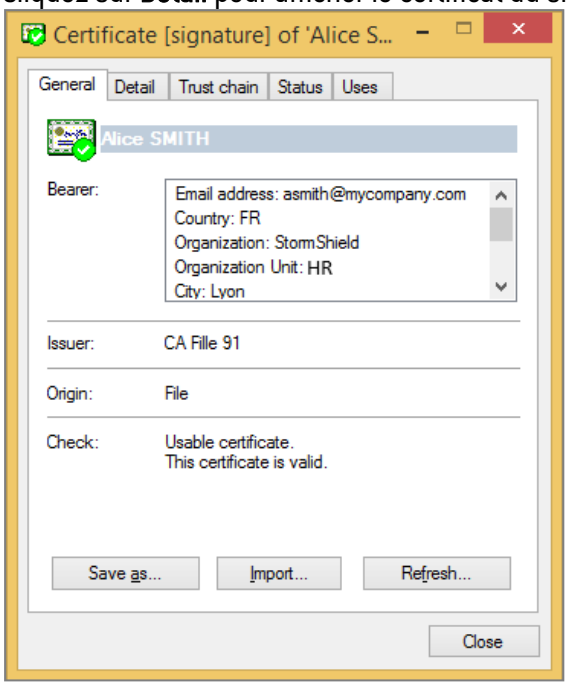


Si vous cliquez sur **Certificats joints**, Stormshield Data Sign affiche les certificats joints au fichier lors de la signature. Ces certificats ne peuvent cependant pas être considérés comme valides tant qu'ils n'ont pas été vérifiés à l'aide de votre annuaire de confiance.

3. Cliquez sur la signature avec le bouton droit de votre souris et choisissez **Propriété de la signature**. La fenêtre suivante s'affiche :



4. Cliquez sur **Détail** pour afficher le certificat du signataire :



Stormshield Data Sign vérifie :

- L'authenticité du contenu du document et de la signature : Stormshield Data Sign vérifie la signature et obtient l'empreinte originale du document. Puis Stormshield Data Sign calcule l'empreinte du document signé pour la comparer à l'empreinte originale. Si les empreintes sont identiques, cela signifie que le document n'a pas été modifié et Stormshield Data Sign en garantit l'authenticité.
- La validité du certificat de la signature : Stormshield Data Sign vérifie la validité du certificat pour garantir l'authenticité du signataire. En cas de signatures multiples, chaque signature est vérifiée : tous les certificats requis pour valider la signature numérique sont vérifiés.

Pour valider un certificat, Stormshield Data Sign consulte la liste de révocation. Cette liste étant régulièrement mise à jour, les résultats sont susceptibles d'être différents à chaque demande de vérification.

Cliquez sur **Importer** pour importer le certificat du signataire dans votre annuaire de confiance.

Cliquez sur **Rafraîchir** pour dynamiquement mettre à jour les données de la signature avec le ou les nouveaux certificats ou les informations de la liste de révocation.

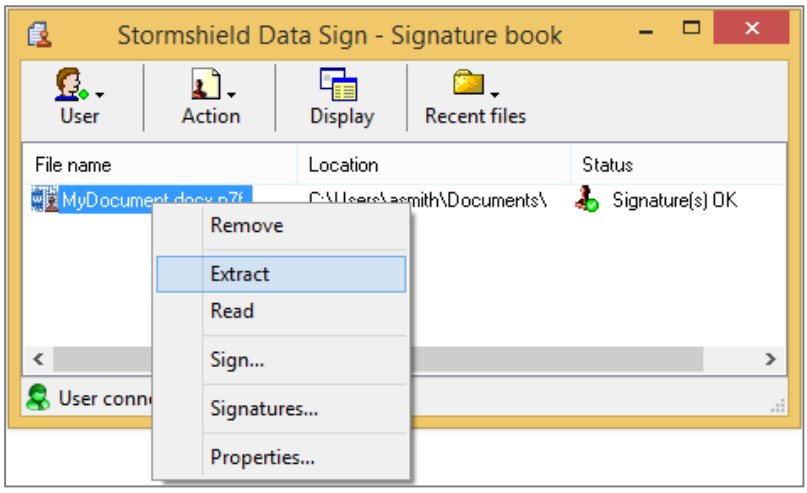
Une fois la vérification achevée, Stormshield Data Sign affiche une icône résumant le résultat des vérifications effectuées :

 La signature est correcte et le certificat du signataire est valide.
 Une anomalie a été détectée.
 Une erreur grave a été détectée.

10.4 Extraire le fichier d'origine

Utilisez la procédure ci-dessous pour extraire d'un fichier signé le fichier d'origine et le sauvegarder dans un nouveau fichier :

1. Effectuez l'une des deux actions possibles :
   - A partir du parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Extraire** :



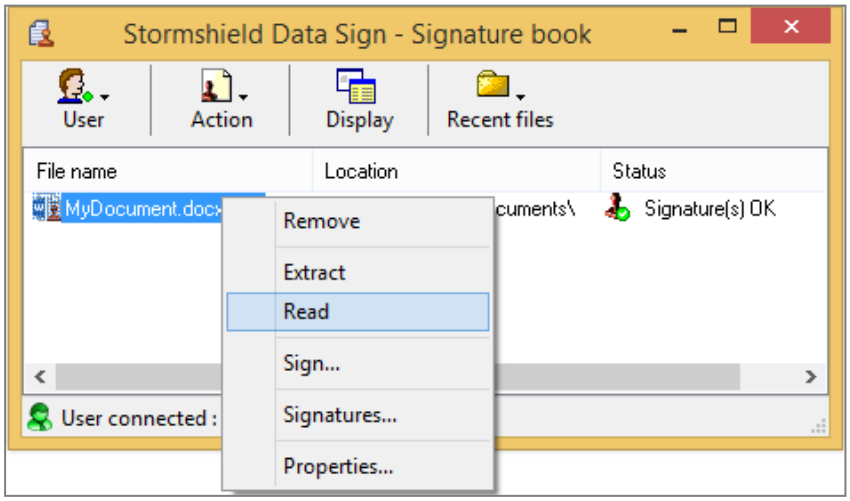
   - A partir de la fenêtre affichant la signature d'un fichier, cliquez sur **Extraire**.
2. Saisissez le nom du fichier sous lequel le fichier d'origine va être enregistré.

> **NOTE**
> Si vous extrayez le contenu d'un fichier sur-signé, le résultat de l'extraction contient le premier niveau de signature mais ne contient aucune sur-signature.

10.5 Lire le contenu d'un fichier signé

Pour lire le contenu d'un fichier signé avec l'application associée sans pour autant extraire le fichier d'origine :

1. Dans le parapheur, cliquez sur le fichier signé avec le bouton droit de votre souris et choisissez **Lire** :



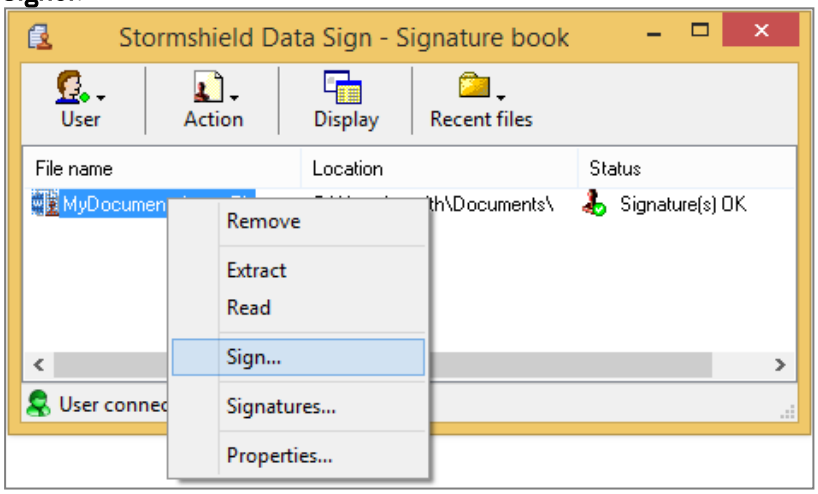
2. Attendez que le compte rendu de la signature s'affiche.

3. Cliquez sur **Lire**. L'action associée par défaut en fonction du type du fichier s'exécute. Généralement le fichier est ouvert dans l'application appropriée.

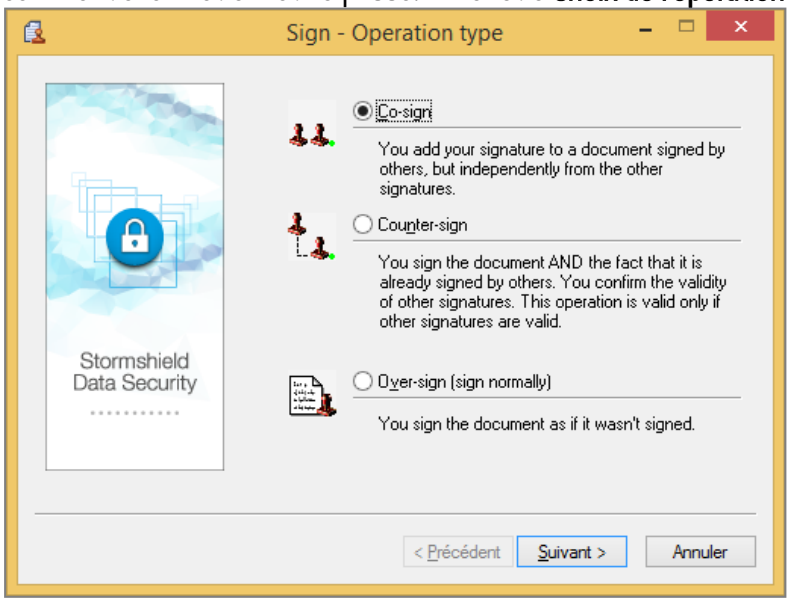
10.6 Signer un fichier déjà signé

Pour signer un fichier déjà signé :

1. Dans l'Explorateur Windows, sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Envoyer vers > Stormshield Data Sign** à partir du menu contextuel : le fichier est alors déposé dans le parapheur.
   - Si le parapheur est déjà ouvert, y déplacer et déposer le fichier sélectionné.
   - Vous pouvez également double-cliquer sur un fichier *.p7f* ou .p7m. Le parapheur s'ouvre alors automatiquement et le fichier y est déposé.
2. Dans le parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Signer**.



3. Suivez les instructions de l'assistant, qui vous demande systématiquement votre code confidentiel ou votre mot de passe. La fenêtre **Choix de l'opération** s'affiche :



4. Sélectionnez l'une des options en fonction de ce que vous souhaitez faire :
   - **Co-signer** pour ajouter votre propre signature au fichier, indépendamment des autres signatures déjà présentes, qu'elles soient correctes ou non.
   - **Contre-signer** pour ajouter signature et contre-signer toutes les autres signatures déjà présentes (y compris les contre-signatures). Cette opération n'est disponible que si toutes les signatures ont déjà été vérifiées et validées.

     > **NOTE**
     > Vous pouvez contre-signer :
     > - toutes les signatures (comme décrit ci-dessous)
     > - une seule signature (voir la section Contre-signer une signature précise)

   - **Sur-signer**. Lorsque vous sur-signez un document, le fichier signé d'origine n'est pas modifié : l'assistant propose de générer un nouveau fichier portant par défaut le même nom auquel est ajoutée l'extension *.p7f*.

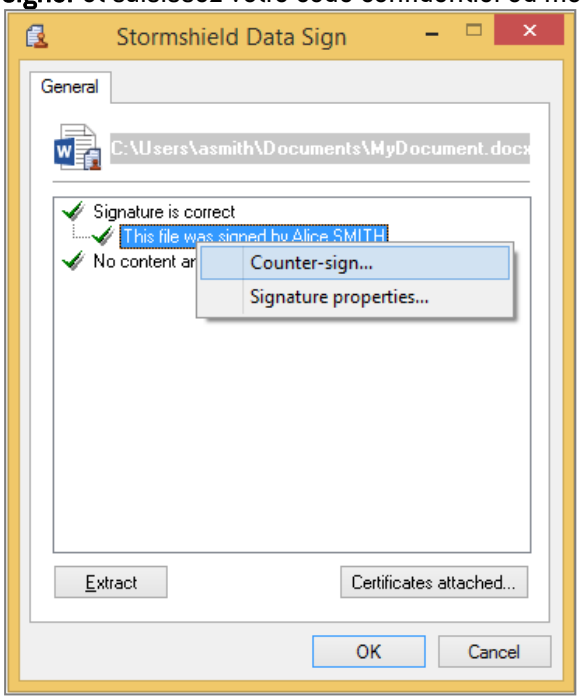
> **NOTE**
> Chaque fois qu'un fichier est sur-signé, l'extension *.p7f* est ajoutée au nouveau fichier généré. Il est donc possible de rencontrer des fichiers avec de multiples extensions *.p7f*.

10.7 Contre-signer une signature précise

Pour contre-signer une signature précise dans un fichier déjà signé :

1. Dans l'Explorateur Windows, sélectionnez le fichier à signer et cliquez sur le bouton droit de la souris pour choisir **Envoyer vers > Stormshield Data Sign** à partir du menu contextuel : le fichier est alors déposé dans le parapheur.
2. Dans le parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Signatures**. Stormshield Data Sign affiche sous forme arborescente les signatures et contre-signatures éventuelles contenues dans le fichier.

3. Cliquez sur la signature concernée avec le bouton droit de votre souris, choisissez **Contre-signer** et saisissez votre code confidentiel ou mot de passe.



Votre contre-signature est ajoutée au fichier signé d'origine. Cette modification sera effective lors de la fermeture de la fenêtre.

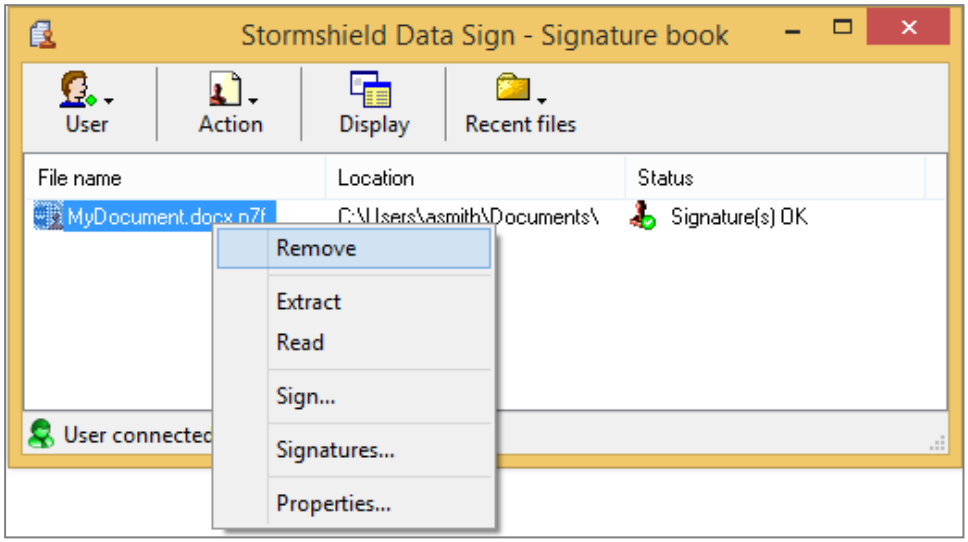
10.8 Notifier par e-mail

Sur la dernière fenêtre de l'assistant, deux options de notification par e-mail sont proposées :

- **Notifier les collaborateurs par e-mail** : Stormshield Data Sign prépare un courrier électronique à destination de collaborateurs afin que ceux-ci soient avertis de la signature du document. Si le document avait été précédemment signé, la liste des destinataires est pré-remplie avec les adresses e-mail des co-signataires,
- **Demander une signature par e-mail** : Stormshield Data Sign prépare un courrier électronique à destination des collaborateurs afin que ceux-ci apposent également leur signature sur le document.

10.9 Enlever un fichier du parapheur

1. Pour enlever un fichier du parapheur, cliquez sur le fichier avec le bouton droit de votre souris et choisissez **Enlever** :



2. Confirmez votre choix.

Le fichier est retiré de la liste du parapheur mais n'est pas physiquement supprimé.

11. Supprimer définitivement des fichiers

La fonctionnalité Stormshield Data Shredder permet de garantir un effacement irréversible des données que les utilisateurs souhaitent supprimer. Cette procédure a pour objet d'éviter qu'une tierce personne ne puisse récupérer une information que l'utilisateur pensait avoir supprimée et en prendre connaissance à son insu.

Un procédé d'effacement conventionnel sous Microsoft Windows n'efface pas réellement les données. Des outils peuvent analyser les fragments de fichiers sur le disque dur et reconstituer les fichiers supprimés.

Stormshield Data Shredder écrit en plusieurs passes une série de caractères en octets (00;FF;55 par défaut) à la place du contenu du fichier. Le fichier initial est alors totalement modifié et même une analyse complète du disque dur, secteur par secteur, ne permet pas de récupérer l'information effacée.

Selon les paramètres définis par l'administrateur dans la politique, la fonctionnalité Stormshield Data Shredder peut être lancée :

- par clic droit sur le fichier ou dossier à supprimer pour afficher le menu contextuel,
- par glisser-déposer depuis le bureau de Windows.

Pour des informations sur le paramétrage de Stormshield Data Shredder dans SDMC, reportez-vous au *Guide d'administration SDS Enterprise*.

11.1 Supprimer des fichiers en utilisant le clic droit

1. Dans l'Explorateur Windows, sélectionnez le fichier ou dossier à supprimer, puis effectuez un clic droit pour sélectionner **Stormshield Data Security > Broyer** dans le menu contextuel.
2. Pour supprimer plusieurs fichiers ou dossiers à la fois, procédez à une sélection multiple et lancez la suppression. Lorsqu'un dossier est supprimé par Stormshield Data Shredder, l'ensemble des fichiers et dossiers qu'il contient sont supprimés de manière sécurisée. Pour arrêter les demandes de confirmation, décochez la case **Demandez une confirmation pour chaque fichier**.

   > **IMPORTANT**
   > Si vous arrêtez le broyage en cliquant sur **Arrêter**, le fichier ne sera pas supprimé, mais les fichiers déjà supprimés ne pourront plus être récupérés.

3. Durant le traitement, un compte rendu est affiché avec le résultat individuel de chaque fichier.
   Pour demander la fermeture automatique du compte rendu à la fin du traitement, cochez la case **Fermer automatiquement la fenêtre**. La fermeture n'a lieu que si le traitement s'est déroulé sans erreur.

11.2 Supprimer des fichiers en utilisant le glisser-déposer

Stormshield Data Shredder supporte le glisser/déposer sur le bureau ou dans l'Explorateur Windows.

- Sélectionnez le ou les fichiers à supprimer dans l'Explorateur Windows. Maintenez le bouton gauche de la souris enfoncé, déplacez l'icône des fichiers jusqu'à l'icône de Stormshield Data Shredder présente sur le bureau et relâchez le bouton :

Vous pouvez aussi sélectionner un ou plusieurs dossiers à supprimer et procéder de la même façon.

Stormshield Data Shredder procède alors à l'effacement définitif et irréversible des données. Le traitement est strictement identique à celui lancé par un clic droit dans l'Explorateur Windows.

12. Pour aller plus loin

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

documentation@stormshield.eu