GUIDE

STORMSHIELD DATA SECURITY ENTERPRISE

STORMSHIELD DATA VIRTUAL DISK

Disque virtuel chiffré

Version 10.1

Dernière mise à jour du document : 29 mars 2022

Référence : sds-fr-sd_virtual_disk-guide_d_utilisation-v10

Table des matières

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

Préface

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

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

1. Introduction

Cette section décrit les caractéristiques et fonctionnalités de Stormshield Data Virtual Disk.

1.1 Présentation

Stormshield Data Virtual Disk est un logiciel de sécurité informatique. Il est destiné à garantir la confidentialité des données que vous stockez sur votre disque dur : seuls le propriétaire et les éventuelles personnes autorisées pourront accéder au volume sécurisé Stormshield Data Virtual Disk.

Le logiciel Stormshield Data Virtual Disk sécurise les fichiers créés ou déposés sur un volume disque virtuel. Les applications peuvent accéder directement aux informations protégées d'un fichier situé sur un volume virtuel.

Un volume disque virtuel est un fichier créé et géré par Stormshield Data Virtual Disk.

Stormshield Data Virtual Disk utilise peu de ressources (mémoire et CPU) et les fichiers sont chiffrés en temps réel au moment de leur sauvegarde et déchiffrés à la lecture.

Une licence du logiciel Stormshield Data Virtual Disk est nécessaire pour pouvoir utiliser celui-ci.

1.2 Concepts clés

Dans ce guide, les termes et concepts suivants sont utilisés :

- Créer un volume chiffré consiste à créer un disque virtuel sur lequel vous souhaitez sauvegarder des données confidentielles. Reportez-vous à la section Création d'un volume sécurisé.
- Monter un volume chiffré consiste à connecter un disque virtuel sur votre poste de travail, disque virtuel sur lequel vous pouvez sauvegarder des données confidentielles. Reportez-vous à la section Montage d'un volume sécurisé.
- Démonter un volume chiffré consiste à déconnecter de votre poste de travail un disque virtuel. Reportez-vous à la section Démontage un volume sécurisé.

A titre de comparaison, la création d'une volume chiffré correspond à l'achat d'une clé USB. Le montage/démontage du volume chiffré correspond au branchement/débranchement de la clé sur votre poste de travail.

- Lorsque vous créez un volume chiffré, vous définissez une liste des utilisateurs autorisés. Ces utilisateurs autorisés sont les utilisateurs qui peuvent monter et démonter le volume chiffré et par conséquent accéder au contenu de ce volume. Reportez-vous à la section Modification de la liste des utilisateurs.

A titre de comparaison, les utilisateurs autorisés sont les personnes auxquelles vous faites confiance et prêtez votre clé USB.

- Le fichier container représente le volume chiffré à partir de l'Explorateur Windows. Le volume chiffré correspond au contenu du fichier container.

A titre de comparaison, le fichier container est votre clé USB telle qu'elle apparaît dans l'Explorateur Windows tandis que le volume chiffré correspond au contenu de votre clé USB.

1.3 Intégration dans Stormshield Data Security

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

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

1.4 Cryptographie à clé publique

Stormshield Data Virtual Disk met en œuvre des moyens de cryptologie dits “à clé publique”.

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

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

Stormshield Data Virtual Disk peut mettre en œuvre :

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

1.4.1 Le chiffrement

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

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

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

1.4.2 Certificats

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

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

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

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

1.4.3 Confiance

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

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

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

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

1.4.4 Annuaires de confiance

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

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

1.5 Connexion sécurisée

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

Stormshield Data Security propose deux méthodes d'authentification :

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

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

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

2. Installation de Stormshield Data Virtual Disk

2.1 Configuration requise

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

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

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

2.2 Installation de Stormshield Data Virtual Disk

Stormshield Data Virtual Disk est un composant de Stormshield Data Security Enterprise.

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

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

3. Utilisation de Stormshield Data Virtual Disk

Cette section décrit l'utilisation de Stormshield Data Virtual Disk.

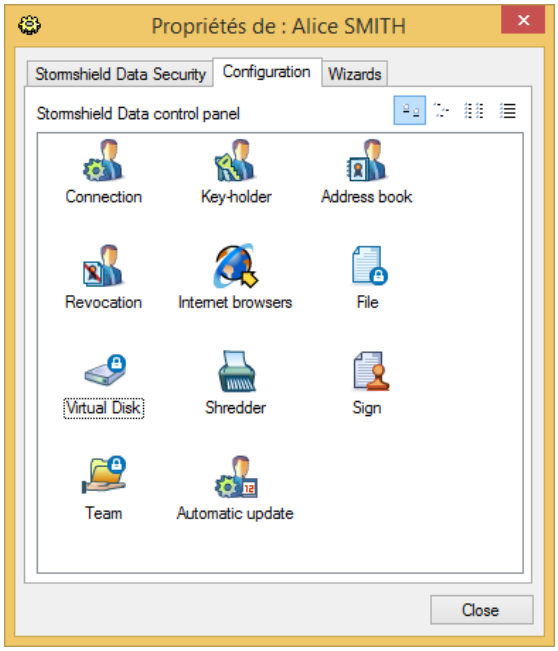
3.1 Création d'un volume sécurisé

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.

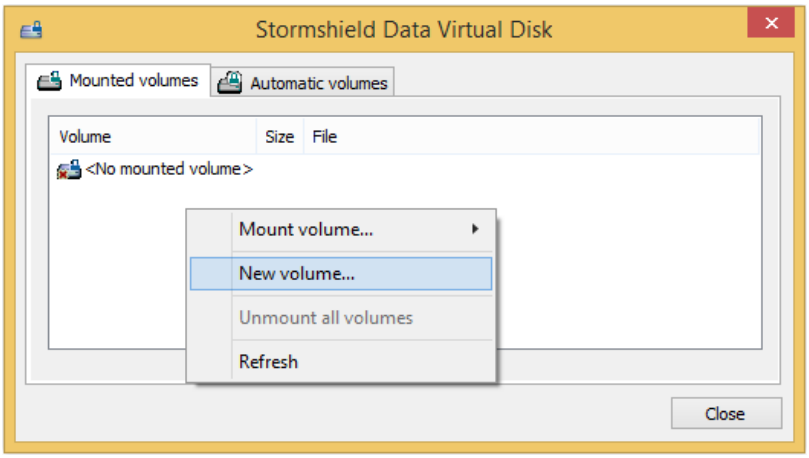
L'utilisation d'un volume virtuel sécurisé est identique à celle d'un disque dur. Vous pouvez y copier des fichiers et lancer des applications qui utilisent des fichiers sauvegardés sur ce volume. Il est également possible d'installer des applications sur des volumes sécurisés.

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.

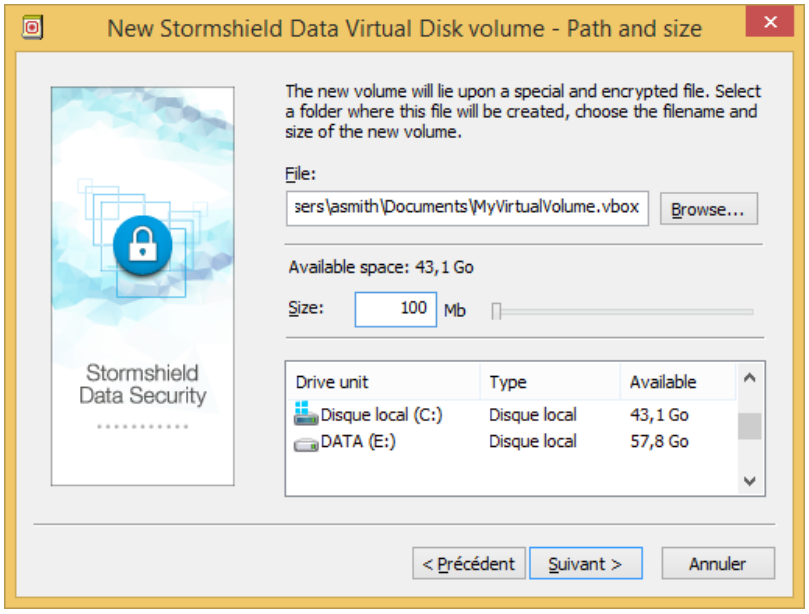
1. Ouvrez la fenêtre de **Propriétés** à partir du menu **Stormshield Data Security** dans la barre de tâches.
2. A partir de cette fenêtre de **Propriétés**, sélectionnez l'onglet *Configuration*.
3. Double-cliquez sur l'icône Virtual Disk.



4. A partir du panneau de contrôle de Stormshield Data Virtual Disk, sélectionnez l'onglet *Volume montés*.
5. Dans la fenêtre *Volume montés*, effectuez un clic droit et sélectionnez **Nouveau volume**.



6. Après un fenêtre d'introduction, la fenêtre suivante s'affiche :



- Dans le champ **Fichier**, spécifiez le nom du volume et son emplacement :
  - Le bouton **Parcourir** permet de sélectionner l'emplacement du volume. Le répertoire, dans lequel le volume sera créé, doit avoir été créé au préalable.
  - 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 *Utilisation dans un contexte multi-sessions Windows* du *Guide d'administration* Stormshield Data Security.

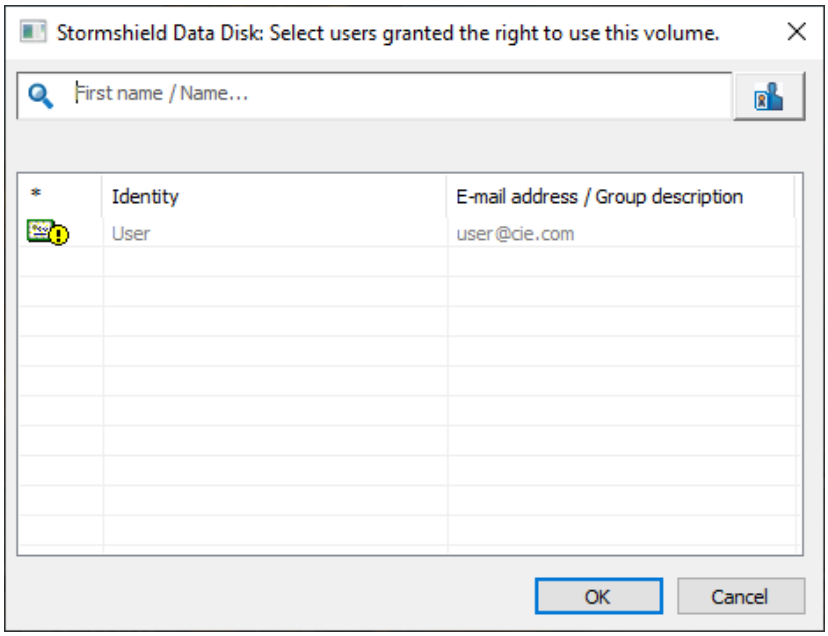
- Dans le champ **Taille**, spécifiez la taille du volume. Celle-ci peut être comprise entre 1 MB et la taille maximum disponible. Par défaut, la taille est égale à 10% de l'espace disponible du répertoire.

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

NOTE
La taille réelle du volume est légèrement inférieure à celle spécifiée, un espace minimum étant réservé pour les fichiers systèmes.

7. Cliquez sur **Suivant**.
8. 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.

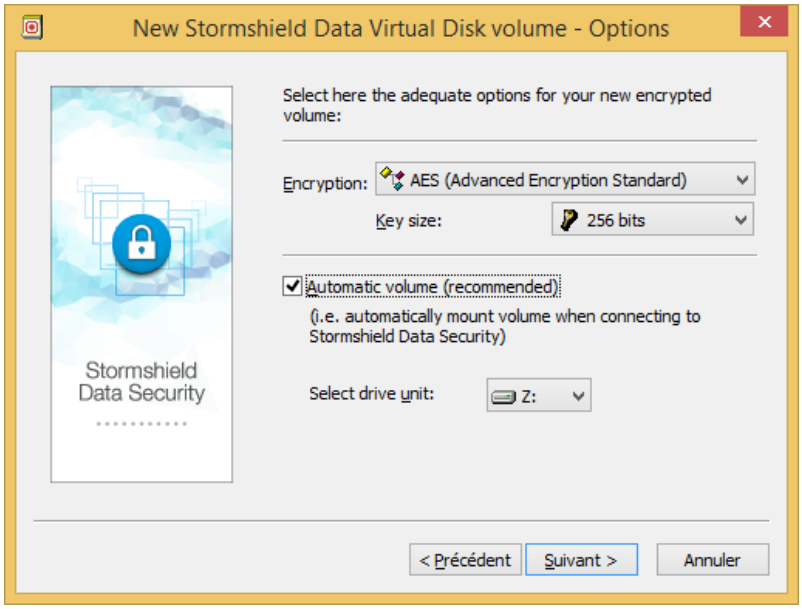
NOTE
L'utilisation simultanée du volume par plusieurs utilisateurs n'est pas possible. Chaque utilisateur autorisé accède au volume de façon alternée.



NOTE

Une fois la liste des utilisateurs complète, cliquez sur **Suivant**.

9. L'écran suivant s'affiche :



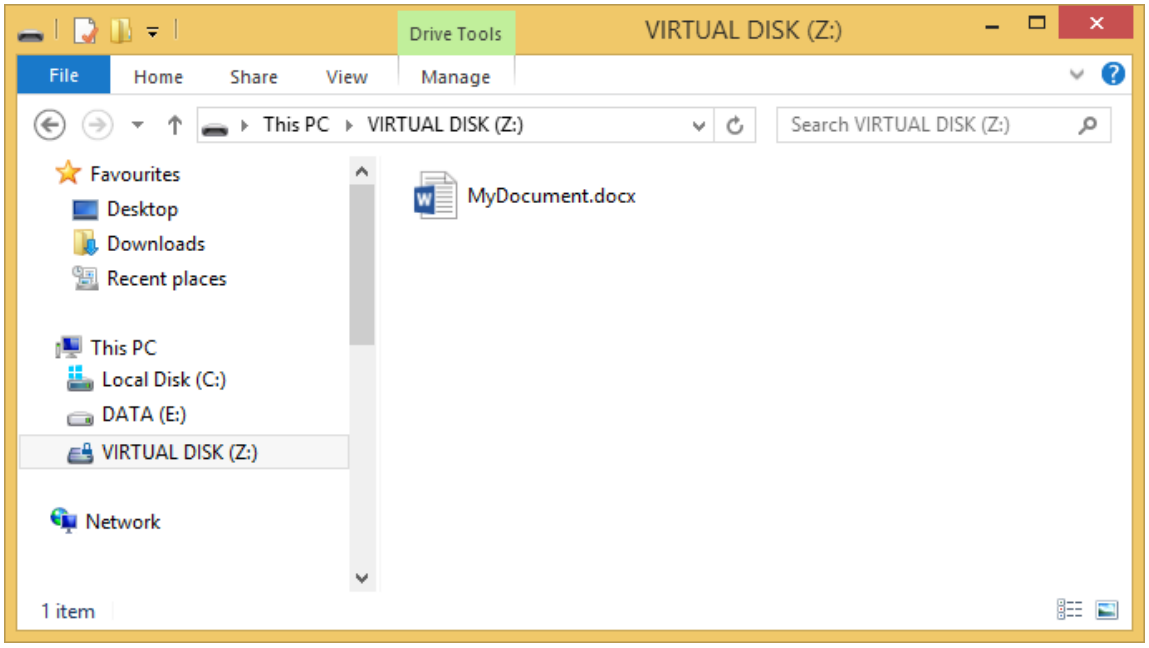
Vous devez indiquer :

- l'algorithme et la force de la clé utilisée pour chiffrer les fichiers sur votre volume sécurisé. L'algorithme AES associé à une clé de 256 bits offre la meilleure protection ;
- si le volume doit être automatiquement monté chaque fois que vous vous connectez à Stormshield Data Security ;
- la lettre du lecteur sur lequel monter le volume et si celui-ci doit être monté automatiquement à chacune de vos connexions à Stormshield Data Security. Aucun lecteur réseau ou aucune clé USB ne doit utiliser la même lettre de lecteur.

10. Cliquez sur **Suivant** pour accéder à l'écran récapitulatif de tous vos choix.

- Pour effectuer la modification, cliquez sur **Précédent**.
- Pour créer votre volume sécurisé, cliquez sur **Terminer**.

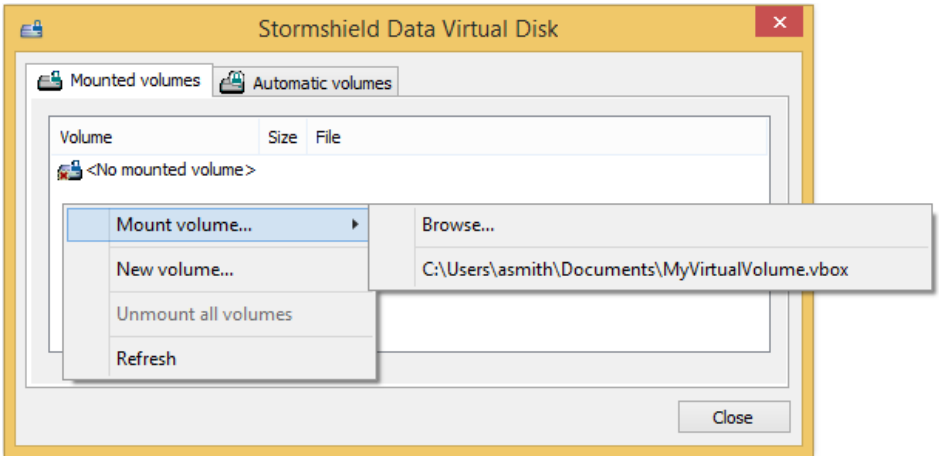
L'opération de création de volume sécurisé étant terminée, le volume apparaît désormais dans l'Explorateur Windows. Tous les fichiers placés sur ce volume seront chiffrés et accessibles pour tout utilisateur autorisé.



3.2 Montage d'un volume sécurisé

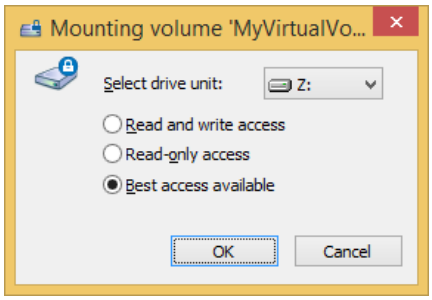
Pour monter un volume existant :

1. Double-cliquez sur le fichier container du volume à partir de l'Explorateur Windows ou bien effectuez un clic droit dans le menu **Stormshield Data Security** et sélectionnez **Propriétés**.
2. A partir de la fenêtre **Propriétés**, sélectionnez l'onglet *Configuration* et double-cliquez sur l'icône Virtual Disk.
3. Dans la fenêtre suivante, 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 :



Sélectionner 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.

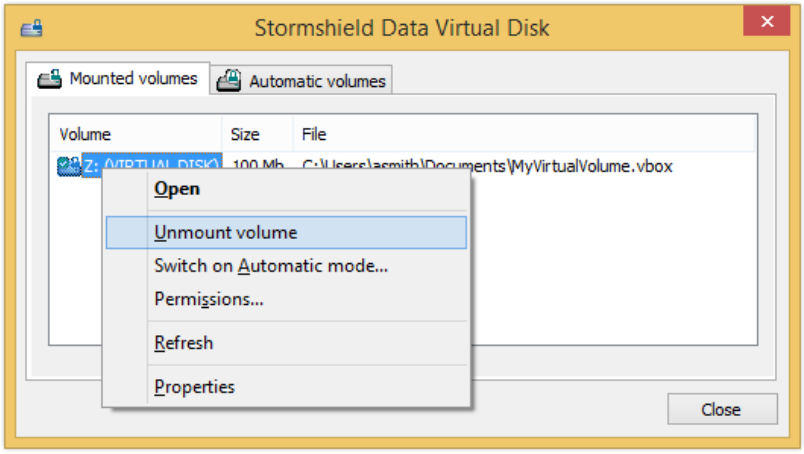
Aucun lecteur réseau ou aucune clé USB ne doit utiliser la même lettre de lecteur. Si la lettre pour monter le lecteur sélectionné est déjà prise, un message d'erreur s'affiche.

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.

3.3 Démontage un volume sécurisé

Pour démonter un volume sécurisé, sélectionnez ce volume à partir de la fenêtre 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*.

3.4 Accès aux propriétés d'un volume chiffré

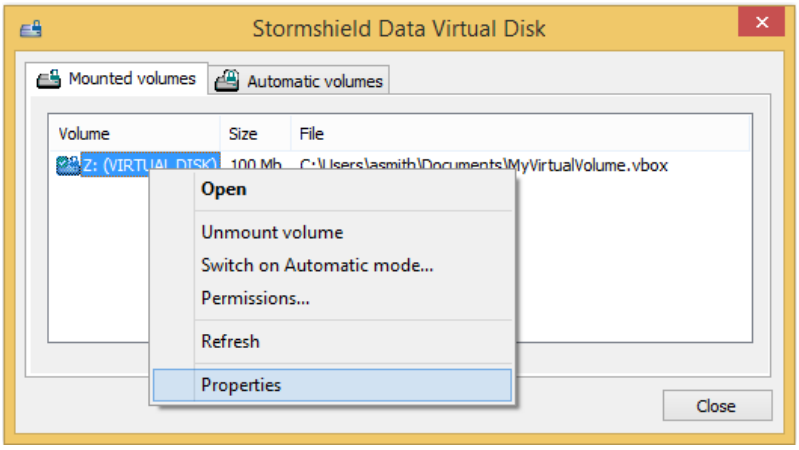
Stormshield Data Virtual Disk permet d'accéder aux propriétés à partir :

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

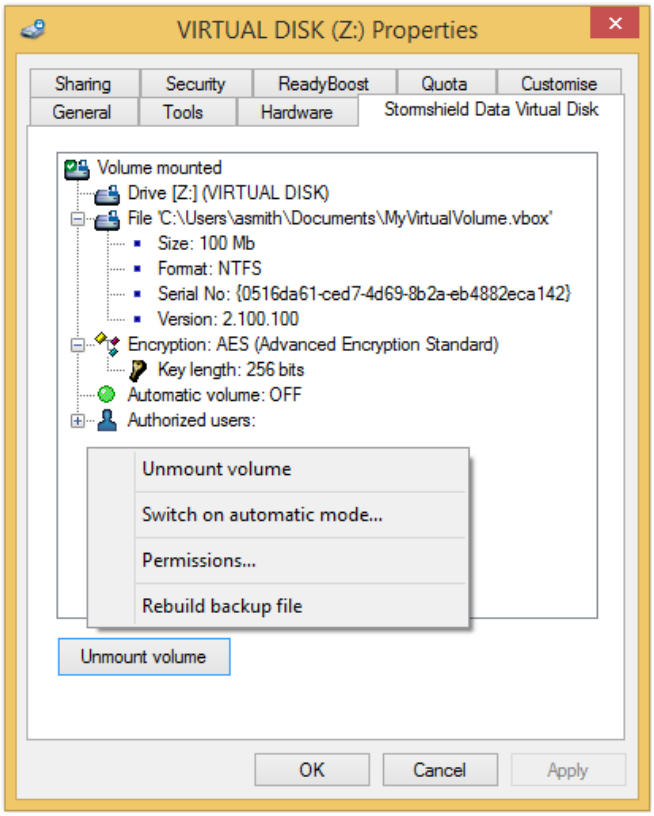
NOTE
Il est impossible d'accéder aux propriétés d'un volume non monté à partir du panneau de contrôle de Stormshield Data Virtual Disk.

3.4.1 A 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*.



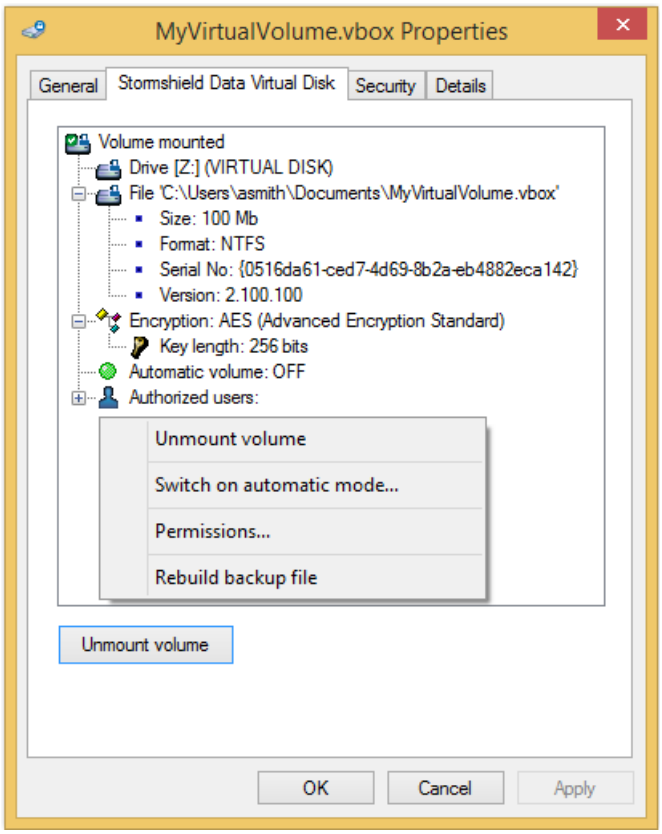
3. En effectuant un clic droit dans la fenêtre de l'onglet *Stormshield Data Virtual Disk*, vous pouvez :

- **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 compte de secours**.

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

3.4.2 A partir du fichier container

1. A 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 *Stormshield Data Virtual Disk*, vous pouvez :

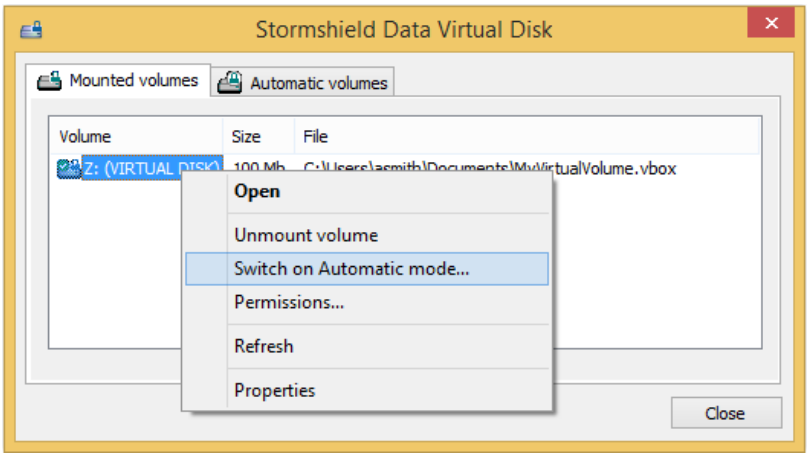
- **Monter** le volume (le bouton **Démonter** permet également cette opération) ;
- Modifier le **mode** du volume (manuel ou automatique) ;
- Modifier les **droits d'accès** des utilisateurs ;
- **Régénérer un fichier de secours**.

3.5 Montage automatique d'un volume sécurisé

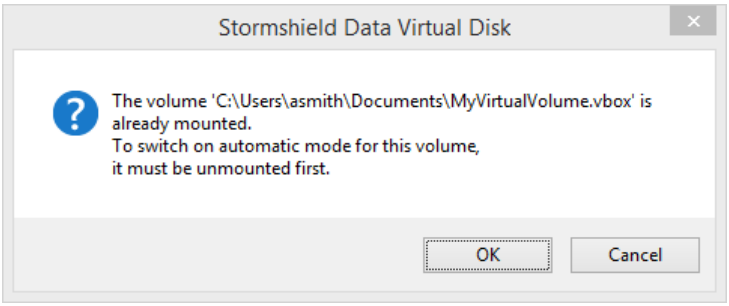
Si vous choisissez l'option montage automatique des volumes, Stormshield Data Virtual Disk monte automatiquement vos volumes sécurisés lors de votre connexion à Stormshield Data Security.

3.5.1 Passage en mode automatique

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

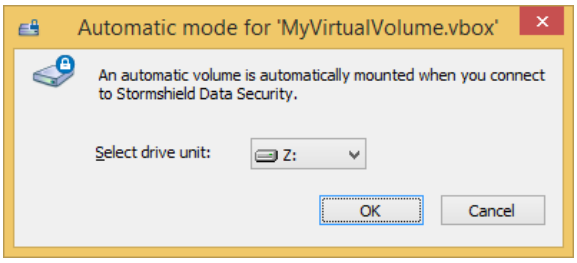


Si le message suivant s'affiche :



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

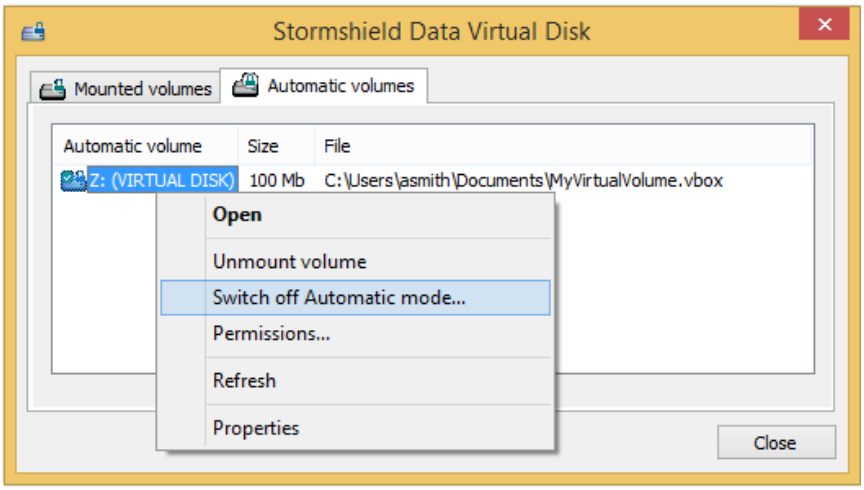
2. Sélectionnez la lettre (du lecteur de montage) à utiliser pour monter le volume. Par défaut, la lettre précédemment utilisée est proposée.



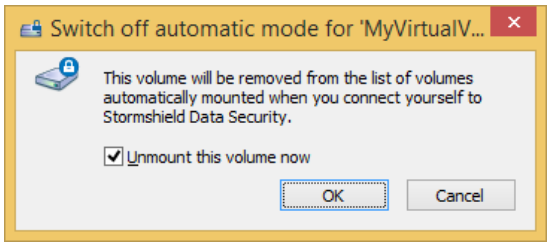
Aucun lecteur réseau ou aucune clé USB ne doit utiliser la même lettre de lecteur.

3.5.2 Passage en mode manuel

1. Sélectionnez **Volumes automatiques** à partir du panneau Stormshield Data Virtual Disk.
2. Effectuez un clic droit et cliquez **Mode manuel**.



3. Une fenêtre de confirmation s'affiche. Avant de cliquer **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.

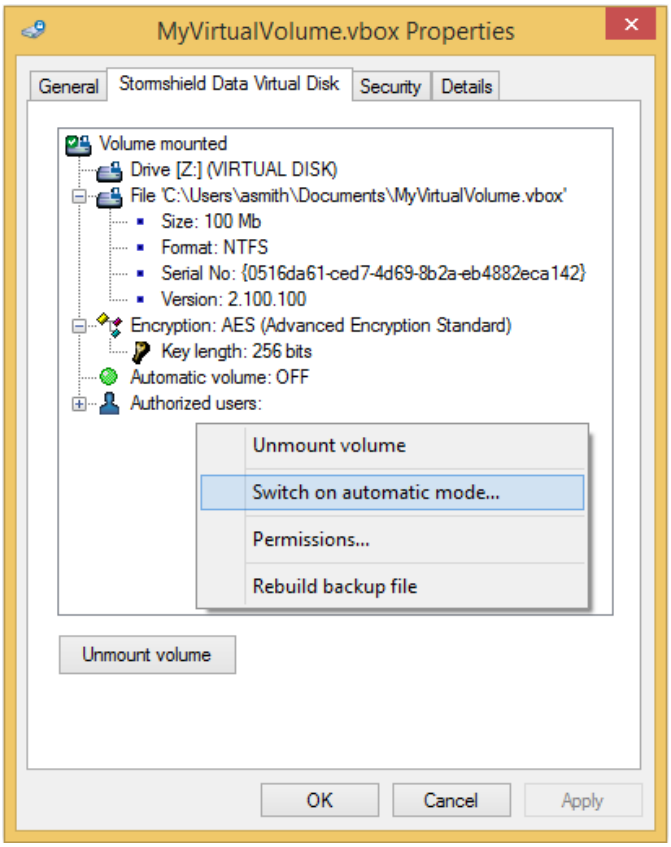


Cliquez **OK** pour valider votre choix.

3.5.3 Activation/désactivation du 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 Stormshield Data Virtual Disk et sélectionnez, en fonction du mode courant du volume, **Passer en mode automatique** ou **Passer en mode manuel**.



3.6 Modification de la liste des utilisateurs

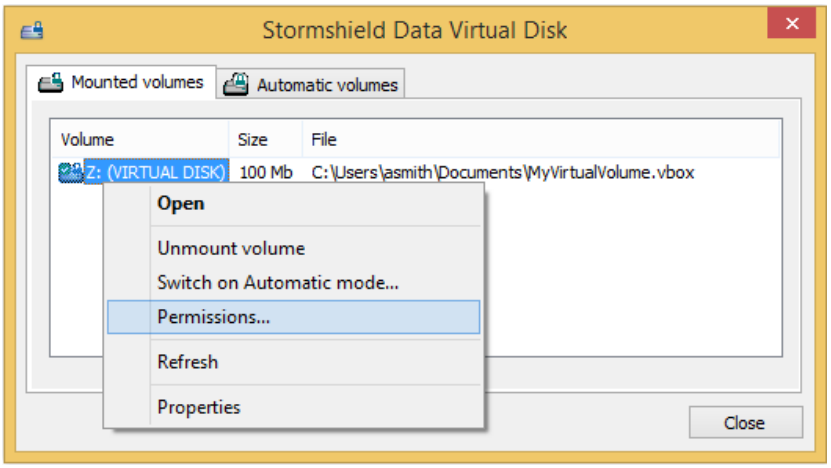
La modification de la liste des utilisateurs requiert que le volume soit déjà monté ou soit en mode automatique.

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

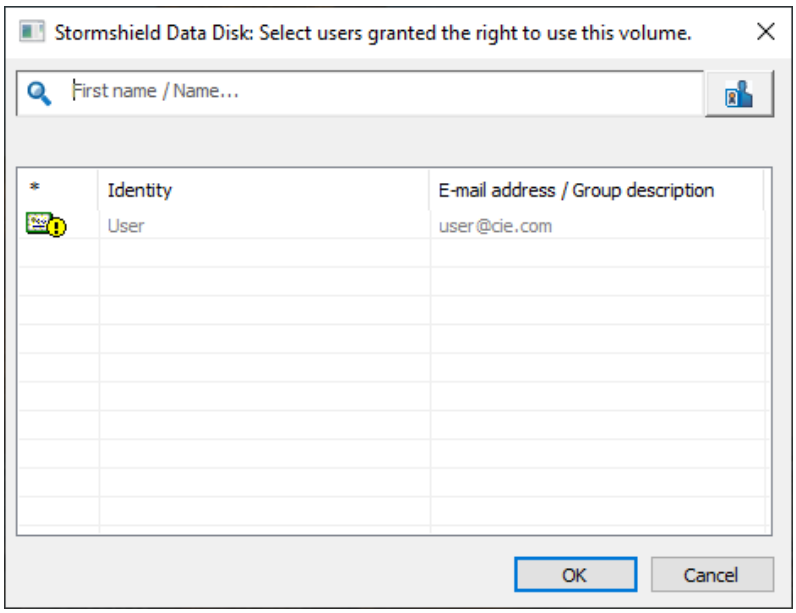
- du panneau Stormshield Data Virtual Disk pour les volumes montés et automatiques ;
- du fichier container.

3.6.1 A partir du panneau 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 **Modifier la liste des utilisateurs**.

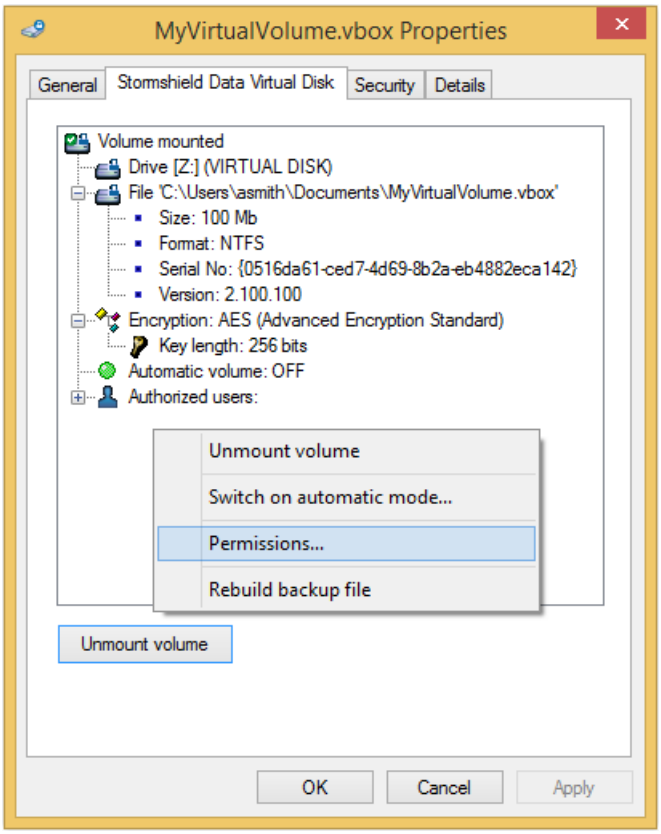


2. La liste des utilisateurs qui ont accès au volume s'affiche. Recherchez les utilisateurs ou groupes auxquels vous souhaitez donner le droit d'accès au volume. La recherche peut afficher les utilisateurs présents dans l'annuaire de confiance ou dans l'annuaire LDAP dans le cas où il est configuré.

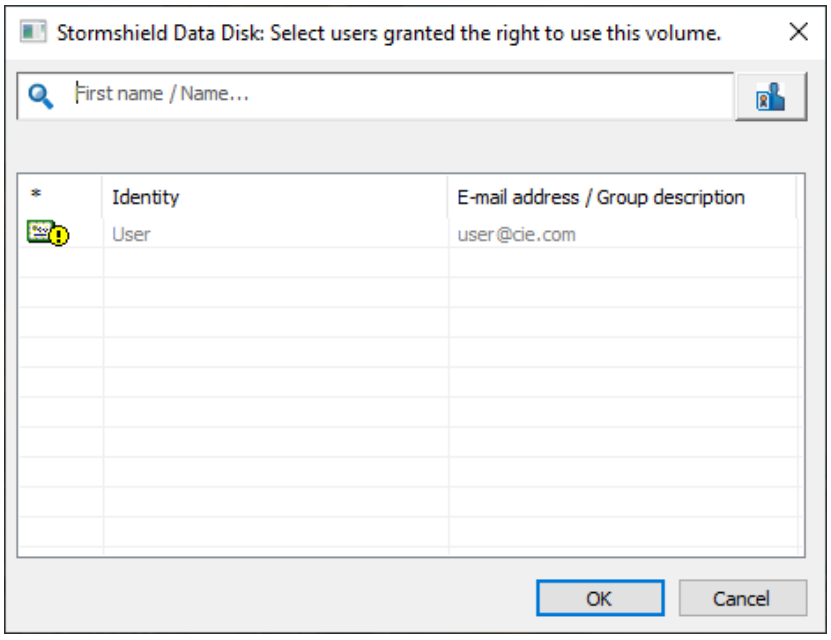


3.6.2 A partir du fichier container

1. A 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 *Stormshield Data Virtual Disk*, 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.



3.7 Déconnexion de Stormshield Data Virtual Disk

Lors de votre déconnexion de Stormshield Data Security, les volumes chiffrés sont démontés, qu'ils soient ou non en cours d'utilisation par des applications ou que certains des fichiers

contenus dans ce volume soient ouverts ou non.

Il est donc recommandé de fermer fichiers et applications avant de se déconnecter de Stormshield Data Security.

Lors de la prochaine connexion, seuls les volumes automatiques seront automatiquement montés.

3.8 Verrouillage de Stormshield Data Security

Lorsque vous verrouillez votre compte utilisateur, les volumes chiffrés montés ne sont plus accessibles en lecture ni écriture, qu'ils soient ou non en cours d'utilisation par des applications ou que certains des fichiers contenus dans ce volume soient ouverts ou non.

Il est donc recommandé de fermer fichiers et applications avant de verrouiller votre compte.

3.9 Modification du propriétaire d'un volume

Cette fonction est une fonction avancée qui doit être utilisée avec précaution.

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

Assurez-vous que l'utilisateur connecté est le propriétaire du volume et suivez la procédure ci-dessous :

1. Ouvrez le fichier *sbox.ini* qui se trouve dans :

C:\Program Files\Arkoon\Security BOX\kernel

Modifiez la section [Disk] de la manière suivante :

```
[Disk]
ModifyRescueFile = 1
ExpertMode=1
```

Pour une description détaillée des paramètres du fichier *sbox.ini*, consultez le *Guide d'administration*.

> **NOTE**
> Il n'est pas nécessaire de redémarrer votre ordinateur ou de vous déconnecter/re-connecter pour prendre en compte ces modifications.

2. 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).
3. Effectuez un clic droit sur le fichier *.vboxsave* et sélectionnez **Propriétés**.
4. Sélectionnez l'onglet *Stormshield Data Virtual Disk* et cliquez sur le signe + à gauche des utilisateurs autorisés pour en voir la liste complète.
5. 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 *sbox.ini* n'a pas été correctement modifié ou sauvegardé ; 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*.

6. Cliquez sur **Mettre à jour le volume** pour synchroniser les deux listes.
7. Rétablissez les valeurs initiales des paramètres de la section `[Disk]` dans le fichier *sbox.ini*.

> **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'installation et de mise en œuvre* pour plus d'informations.

Consultez également le *Guide d'administration* pour l'opération de recouvrement d'un volume.

documentation@stormshield.eu