

# SOPHOS

## SafeGuard® Private Disk 2.50 Aide

Date du document: mars 2011



# Sommaire

- 1 Aperçu ..... 2
- 2 Premières étapes..... 6
- 3 Application principale SafeGuard PrivateDisk® ..... 15
- 4 SafeGuard PrivateDisk Portable..... 33
- 5 Exemples de cas d'utilisation..... 35
- 6 Administration centralisée ..... 40
- 7 L'interface d'automation OLE de SafeGuard PrivateDisk ..... 46
- 8 Support technique..... 49
- 9 Mentions légales ..... 50

# 1 Aperçu

## 1.1 En quoi consiste SafeGuard® PrivateDisk?

SafeGuard PrivateDisk permet de protéger de manière transparente des fichiers sensibles stockés sur votre ordinateur, indépendamment de leur emplacement (disque dur local, disques amovibles, fichiers sur serveur). Il suffit de créer ou copier votre fichier sur le disque virtuel et il est chiffré automatiquement.

### **La Technologie de Disque Virtuel Sécurisé : Le coffre-fort électronique**

Un tel résultat est rendu possible par l'utilisation de disques virtuels, sortes de disques logiques permettant le stockage de données dans de grands fichiers chiffrés. Notre solution combine le chiffrement avec la protection simultanée de différents fichiers en un disque virtuel. La technologie du disque virtuel crée une sorte de coffre-fort électronique dans l'ordinateur).

Comme tout coffre-fort, l'utilisateur doit s'identifier pour l'ouvrir, pouvant ainsi travailler avec ses données chiffrées. Les données sont chiffrées automatiquement lorsqu'elles sont enregistrées sur ce disque virtuel. Ces fichiers sont également déchiffrés en mémoire automatiquement lors de leur ouverture. L'utilisateur n'a plus à se soucier des opérations de chiffrement.

## 1.2 Avantages

Cette technologie combine les avantages du chiffrement de fichiers à la technologie du chiffrement de disque :

- Le chiffrement est réalisé automatiquement.
- Les fichiers de données et les métadonnées (répertoire) sont chiffrés.
- Pour le travail sur un fichier chiffré, les données sont déchiffrées en mémoire, et non sur le disque.
- Seule une partie des données d'un disque doivent être chiffrés.

### 1.2.1 Disques virtuels

Un disque virtuel consiste à simuler l'existence de disques additionnels sur l'ordinateur, mais contrairement aux disques physiques, un disque virtuel stocke ses données à l'intérieur d'un seul et unique fichier. Pour un disque virtuel de 100 Mo, on a besoin d'un fichier de 100 Mo (appelé fichier volume) sur un des disques physiques.

Ces fichiers peuvent se trouver sur toutes les unités de disque disponibles. Ils peuvent être sur des supports amovibles comme des disquettes, CD-ROM, DVD, ZIP, les mémoires USB, carte de mémoire flash ou alors des unités fixes ou même des unités en réseaux.

Tous les secteurs sont chiffrés. Ainsi, tous les fichiers et répertoires d'un même disque virtuel sont chiffrés avec la même clé de chiffrement, utilisant l'algorithme AES 128 bits.

La sécurité réside dans le mode de protection du disque. Même sans détenir des droits d'accès, les utilisateurs pourraient effacer l'ensemble des fichiers du disque (si l'accès n'était pas refusé) et pourraient lire les données, mais ils ne pourraient pas lire les données non chiffrées ou la structure du répertoire stockées dans le fichier volume.

SafeGuard PrivateDisk protège la clé de chiffrement du disque par le biais d'un mot de passe (PKC 5) ou une paire de clés RSA liées à un certificat. Les utilisateurs peuvent ouvrir les disques virtuels soient en connaissant le mot de passe du disque ou en possédant la clé privée des certificats (stockés dans un fichier ou sur une carte à puce) associés au disque.

### 1.3 Clés du jeu de clés SafeGuard Enterprise

Outre les mots de passe et les certificats, SafeGuard PrivateDisk vous permet d'utiliser des clés du jeu de clés SafeGuard Enterprise pour accéder aux lecteurs PrivateDisk. Si vous avez installé SafeGuard Enterprise sur l'ordinateur, vous pouvez utiliser la totalité des clés contenues dans le jeu de clés de l'utilisateur (clés créées au niveau central par SafeGuard Enterprise ou au niveau local sur le client SafeGuard Enterprise).

Plusieurs utilisateurs peuvent alors accéder au même lecteur PrivateDisk (sur un partage réseau par exemple). Pour permettre l'accès au lecteur PrivateDisk, seule la clé utilisée pour la création de ce lecteur doit être disponible sur l'ordinateur des utilisateurs. Toutefois, ceci n'est possible qu'en cas d'utilisation de la version 2.30 ou d'une version plus récente de SafeGuard PrivateDisk sur les deux ordinateurs.

**Remarque :** Notez que la même clé (par exemple, clé de groupe SafeGuard Enterprise) doit être disponible sur les deux ordinateurs. Si vous utilisez une clé SafeGuard Enterprise non incluse dans le jeu de clés de l'utilisateur, ce dernier ne pourra pas accéder au lecteur PrivateDisk.

Si vous utilisez une clé SafeGuard Enterprise créée localement, vous devez fournir à l'utilisateur souhaitant accéder au lecteur PrivateDisk la passphrase correspondant à la clé. Lors de l'ouverture de l'archive, le destinataire sera automatiquement invité à entrer la passphrase.

## 1.4 Plates-formes supportées

SafeGuard PrivateDisk est disponible pour les systèmes d'exploitation suivants :

- Windows XP 32 bits
- Windows Vista 32 bits
- Windows Vista 64 bits
- Windows 7 32 bits
- Windows 7 64 bits

## 1.5 Versions

### Personal Edition

Cette version est idéale pour les utilisateurs privés ainsi que pour les petites entreprises. Il n'y a pas d'administration centralisée.

### Enterprise Edition

Outre cette version pour utilisateurs privés et petites entreprises, il existe également une version optimisée de SafeGuard PrivateDisk appelée Enterprise Edition, idéale pour les entreprises plus grandes souhaitant déployer et administrer le logiciel. L'édition Enterprise contient toutes les fonctionnalités de la Personal Edition avec en plus:

- Configuration centrale et simple via des stratégies Windows similaires aux autres Produits SafeGuard et Windows.
- Vérification des CRL (Certificate Revocation Lists, listes de révocation de certificats) lors de l'évaluation des certificats.

Comme l'installation de SafeGuard PrivateDisk est faite par Windows Installer, une installation silencieuse peut être réalisée en utilisant tous les mécanismes standard de Windows.

Il est possible de réaliser une mise à jour de la version " Personal Edition " vers la version " Enterprise Edition " du logiciel. La réciproque n'est pas possible.

## Version de démonstration

Une version de démonstration est disponible sur <http://www.sophos.com/products/enterprise/encryption/safeguard-privatedisk/>. Cette version peut être téléchargée gratuitement.

Il s'agit d'une version Personal Edition pleinement opérationnelle conçue à des fins d'évaluation qui fonctionne pendant 30 jours sans limitation. Après ce délai, les disques ne pourront être montés qu'en lecture seule jusqu'à l'achat du produit par le biais de la boutique en ligne Sophos. En outre, vous obtiendrez un écran de démarrage jusqu'à ce que vous achetiez le produit.

## Mise à jour de la version de démonstration

Si vous souhaitez mettre à jour la version de démonstration vers une version complète de SafeGuard PrivateDisk, vous devez simplement installer la nouvelle version sur la précédente. Une version de démonstration peut être mise à jour vers toutes les autres versions.

**Remarque :** Il n'y a pas de fonctions permettant d'augmenter la taille des disques virtuels, qui ont une taille maximale de 20 Mo avec la version de démonstration.

### 1.5.1 Mise à jour vers la version 2.40

Vous n'aurez aucun problème à passer de votre version existante à la version 2.40. Vous pourrez continuer d'utiliser la nouvelle version (pour les fichiers volume) sur les lecteurs PrivateDisk existants.

**Remarque :** À partir de la version 2.00 SafeGuard PrivateDisk utilise par défaut l'algorithme AES-256, tandis que les versions antérieures utilisaient AES-128 (et ne prenaient pas en charge AES-256). Si vous souhaitez utiliser la version 2.40 pour générer des fichiers de volume également exploitables par les versions antérieures de SafeGuard PrivateDisk, vous devez sélectionner l'algorithme de chiffrement AES-128, et aucun autre lorsque vous configurez PrivateDisk. Il est impossible d'utiliser les lecteurs PrivateDisk faisant appel à AES-256 avec les versions antérieures.

## 2 Premières étapes

### 2.1 Certificats - Généralités

SafeGuard PrivateDisk autorise l'utilisation de certificats, y compris des paires de clés publiques/privées, à la place de mots de passe pour authentifier l'utilisateur d'un disque virtuel chiffré. Seul le propriétaire du certificat a accès à la clé privée du certificat et peut l'utiliser pour se connecter. De façon similaire aux mots de passe, les certificats permettent d'accorder des accès de type utilisateur ou administrateur.

Informations importantes concernant l'utilisation de certificats :

SafeGuard PrivateDisk utilise le Microsoft Crypto API uniquement pour l'utilisation des certificats. Le chiffrement des disques virtuels est réalisé avec les algorithmes AES et SHA-1.

SafeGuard PrivateDisk supporte les CSP tiers (Cryptographic Service Providers, Fournisseurs de services cryptographiques), par exemple Microsoft Enhanced CSP.

Afin de garantir le meilleur niveau de sécurité, nous recommandons l'utilisation de CSP robustes comme Microsoft Strong Cryptographic Service Provider (nécessite Windows XP ou Microsoft High Encryption Pack). Ces CSP permettent d'utiliser des clés RSA de 4096 bits et fournissent des algorithmes robustes (comme 3DES).

#### **Quelques pré-requis pour l'utilisation de certificats avec SafeGuard PrivateDisk:**

- Le certificat doit contenir une clé publique.
- Pour accéder à un disque virtuel par le biais de certificats, la clé privée du certificat assigné doit être disponible.
- Seuls apparaissent les certificats des dépôts Personnel, Carnet d'Adresses et Autres Personnes de l'Utilisateur actuel et ceux du dépôt Personnel de l'Ordinateur local. Les certificats stockés dans d'autres dépôts ne sont pas reconnus par SafeGuard PrivateDisk! Les certificats peuvent être importés et organisés en utilisant la console MMC et le composant enfichable Certificats.
- Pour ajouter un certificat à un disque virtuel, seule la clé publique est nécessaire. La clé privée reste la possession du propriétaire du certificat et seul lui est capable d'ouvrir le disque virtuel.

Nous recommandons d'avoir des certificats disponibles dans les dépôts avant de démarrer l'installation de SafeGuard PrivateDisk. Ainsi ils apparaîtront dans la boîte de dialogue *Ajouter des certificats* et pourront être associés à un disque virtuel.

**Remarque :** La gestion des certificats n'est pas prise en charge par SafeGuard PrivateDisk, cela peut être fait par le biais d'une infrastructure PKI interne ou par une autorité de certification tierce.

### 2.1.1 Vérification des Certificats

Pour pouvoir utiliser les certificats avec SafeGuard PrivateDisk, ils doivent remplir certains critères :

- SafeGuard PrivateDisk contrôle la période de validité du certificat. Il est possible d'utiliser un certificat arrivé à expiration pour monter les disques virtuels PrivateDisks, mais il est impossible de les assigner à ces disques.
- SafeGuard PrivateDisk contrôle les extensions critiques des certificats. Il est impossible d'assigner aux disques virtuels des certificats accompagnés d'extensions critiques inconnues. La version Enterprise Edition permet de modifier cette réaction par défaut au sein du modèle d'administration.
- Il est impossible d'assigner des certificats de signature aux disques virtuels. La version Enterprise Edition permet de modifier cette réaction par défaut au sein du modèle d'administration.

#### Enterprise Edition

- La version " Enterprise Edition " de SafeGuard PrivateDisk permet de faire une vérification complète des certificats. Les certificats ne sont acceptés qu'après un contrôle complet de leur chemin de certification. En cas de nécessité, la liste de révocation des certificats (CRL) est téléchargée depuis l'autorité de certification. Si le certificat ne peut être vérifié, l'accès à PrivateDisk sera refusé. L'option de vérification étendue des certificats est désactivée par défaut.

**Remarque :** Pour l'évaluation d'une CRL une connexion réseau peut être nécessaire. Si la connexion ne peut être établie, l'accès sera refusé, même si le certificat est valable.

- La version Enterprise Edition permet de définir un CSP préféré dans le modèle d'administration. Chaque fois qu'un utilisateur essaie de s'authentifier avec un mot de passe ou un certificat d'un CSP différent, un message s'affichera pour indiquer que le CSP préféré offre une meilleure sécurité.

### 2.1.2 Lecteur de carte à puce

Étant donné que les fournisseurs de services cryptographiques (CSP) peuvent activer les certificats à utiliser, les cartes à puce sont automatiquement prises en charge lorsque vous utilisez un CSP de carte à puce. Il est par conséquent possible de se connecter à des disques virtuels à l'aide de certificats sur des cartes à puce.

Si vous souhaitez utiliser des certificats sur des cartes à puce pour vous connecter à un disque virtuel, assurez-vous d'avoir correctement installé le lecteur de carte à puce et le fournisseur de services cryptographiques approprié.

## 2.2 Installation

**Remarque :** L'installation de SafeGuard PrivateDisk n'est possible que si vous êtes connecté au système d'exploitation avec des droits d'administrateur.

Si vous avez téléchargé le programme à partir d'Internet, exécutez le fichier téléchargé.

Si vous avez reçu le programme sous la forme d'un CD, insérez ce dernier dans votre lecteur de CD-ROM. Généralement, l'installation démarre automatiquement (dans le cas contraire, exécutez le fichier .exe ou .msi situé dans le répertoire `Install` de votre CD d'installation).

Un assistant d'installation vous guide tout au long de la procédure d'installation extrêmement simple de SafeGuard PrivateDisk.

Sélectionnez **J'accepte le contrat de licence** dans la boîte de dialogue *Droit de licence*. Dans le cas contraire, vous ne pourrez pas installer SafeGuard PrivateCrypto.

SafeGuard PrivateDisk est prêt à l'emploi immédiatement après l'installation.

### 2.2.1 Icône de la barre d'état système

SafeGuard PrivateDisk place une icône dans la barre des tâches Windows. Lorsque vous cliquez sur cette icône avec le bouton droit de la souris, vous obtenez un menu vous permettant d'effectuer les opérations suivantes :

- démarrage de l'application principale (**PrivateDisk**)
- démarrage de l'Assistant pour le nouveau PrivateDisk (**Nouveau**)
- importation de disques existants (**Importer**)
- montage et démontage de disques (**Monter ou Démont**)
- définition de certains paramètres pour SafeGuard PrivateDisk (**Options**).  
Cette opération n'est possible que si vous êtes connecté au système en tant qu'administrateur.

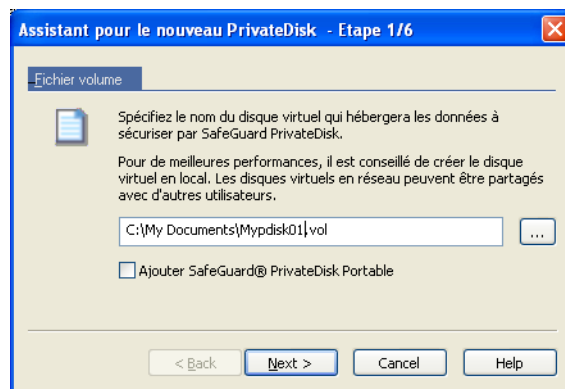
Vous pouvez également démarrer l'application principale SafeGuard PrivateDisk en sélectionnant **Démarrer/Programmes/Sophos/SafeGuard PrivateDisk**.

## 2.3 Démarrage rapide

Après l'installation, utilisez l'assistant de SafeGuard PrivateDisk pour créer simplement en 6 étapes un disque virtuel chiffré.

Par la suite, le nouveau disque virtuel chiffré peut être utilisé comme n'importe quelle unité de disque additionnelle à votre système. Les données stockées sur ce disque virtuel sont chiffrées et déchiffrées automatiquement.

Pour créer un disque virtuel, cliquez droit sur l'icône de SafeGuard PrivateDisk dans la barre de tâches, cliquez sur **Nouveau** et ensuite suivez l'assistant.



1. Spécifiez l'emplacement et le nom du fichier devant contenir les données de votre nouvelle unité de disque chiffrée. L'extension du fichier .vol indique qu'il s'agit d'un disque virtuel exploitable par SafeGuard PrivateDisk.

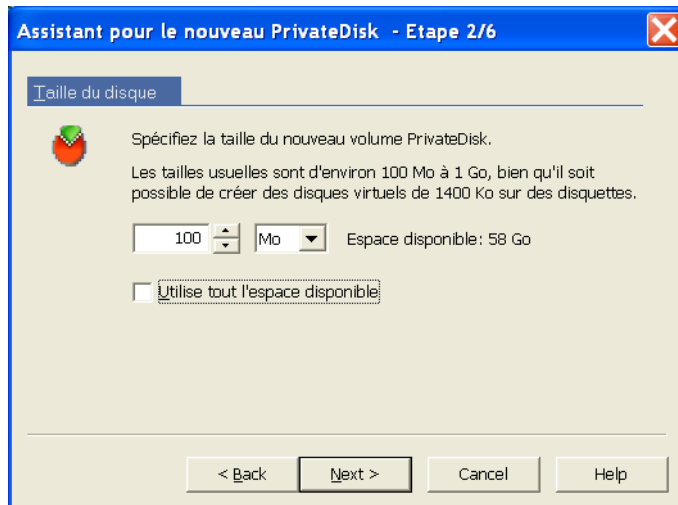
Les chemins de création des lecteurs PrivateDisk peuvent être restreints par des paramètres centralisés. Si vous tentez de créer un lecteur à un emplacement restreint, vous recevrez un message vous indiquant les chemins autorisés.

### ■ Ajouter SafeGuard PrivateDisk Portable

Si vous activez cette option, SafeGuard PrivateDisk Portable sera copié sur le support en même temps que le fichier .vol.

Vous pouvez ouvrir des lecteurs PrivateDisk SafeGuard PrivateDisk Portable sur des ordinateurs non équipés de SafeGuard PrivateDisk.

Cliquez sur **Suivant**.



2. Spécifiez la taille de votre nouvelle unité de disque SafeGuard PrivateDisk. Les tailles typiques vont de 100 Mo à 1 Go.

■ **Utilise tout l'espace disponible**

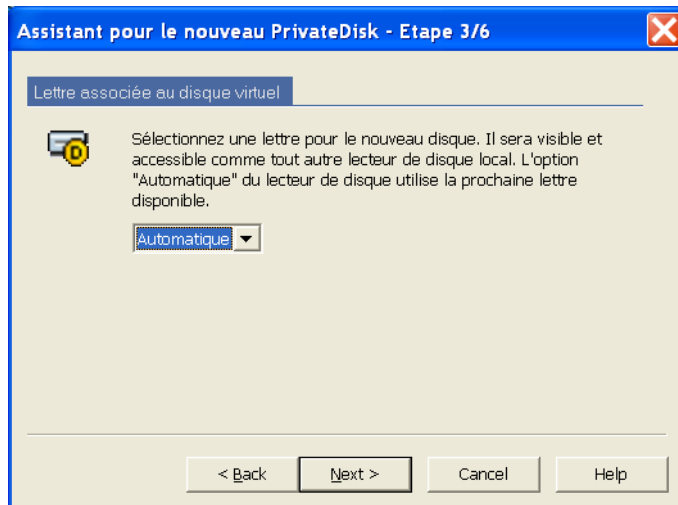
Si vous sélectionnez cette option, SafeGuard PrivateDisk utilise la totalité de l'espace disque disponible sur le lecteur sélectionné pour le nouveau lecteur PrivateDisk.

L'espace disque disponible est indiqué en regard du champ *Espace disponible*

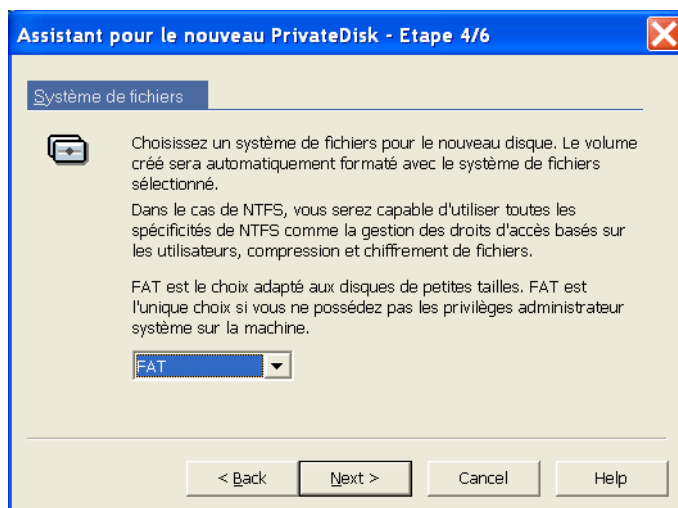
La taille maximale d'un lecteur PrivateDisk peut être restreinte par un paramètre centralisé. Si vous tentez de créer un lecteur plus volumineux, vous recevrez un message vous indiquant la taille maximale des lecteurs PrivateDisk.

Cliquez sur **Suivant**.

**Remarque :** La taille d'un disque virtuel ne peut plus être changée après la création. Pour avoir plus de place, vous devrez créer un nouveau disque virtuel et les données du disque initial doivent être copiées dans le nouveau disque.

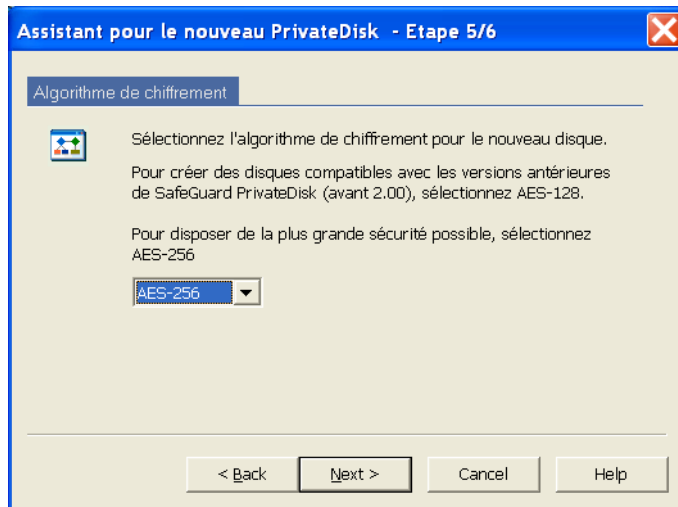


3. Sélectionnez la lettre du lecteur pour votre nouveau disque virtuel. L'unité de disque sera visible comme tout autre disque local. L'option **Automatique** permet d'attribuer automatiquement la prochaine lettre disponible. Cliquez sur **Suivant**.



4. Choisissez le système de fichiers pour votre unité de disque SafeGuard PrivateDisk. Le disque virtuel sera automatiquement formaté. Cliquez sur **Suivant**.

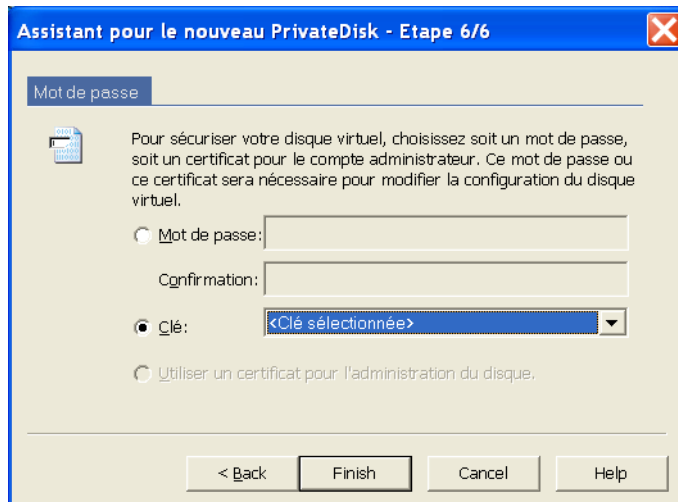
**Remarque :** Les utilisateurs s'identifiant au système n'ayant pas de droit administrateur, ne peuvent choisir que FAT comme système de fichiers pour le disque virtuel.



5. Sélectionnez un algorithme de chiffrement pour le nouveau lecteur. Vous avez le choix entre AES-128 et AES-256.

**Remarque :** À partir de la version 2.00 SafeGuard PrivateDisk utilise par défaut l'algorithme AES-256, tandis que les versions antérieures utilisaient AES-128 (et ne prenaient pas en charge AES-256). Si vous souhaitez utiliser la version 2.00 pour générer des fichiers de volume également exploitables par les versions antérieures de SafeGuard PrivateDisk, vous devez sélectionner l'algorithme de chiffrement AES-128, et aucun autre lorsque vous configurez PrivateDisk. Il est impossible d'utiliser les lecteurs PrivateDisk faisant appel à AES-256 avec les versions antérieures.

Cliquez sur **Suivant**.

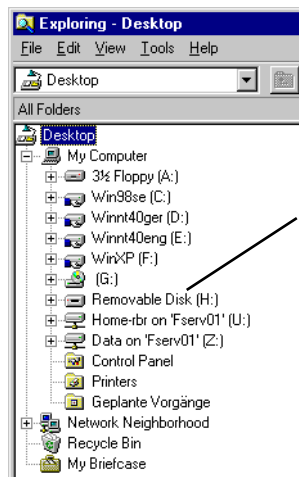


6. Choisissez :

- Un mot de passe pour l'administrateur et confirmez-le. Ce mot de passe sera vérifié chaque fois que vous montez un disque.
- **Une clé du jeu de clés SafeGuard Enterprise**  
Si votre ordinateur est équipé de SafeGuard Enterprise ou de SafeGuard RemovableMedia, vous pouvez utiliser l'une des clés du jeu de clés approprié. Cette clé sera utilisée pour la création d'un volume PrivateDisk et pour la connexion à ce dernier. Aucun mot de passe supplémentaire n'est requis.
- **Utiliser un certificat pour l'administration du disque**  
Si cette option est activée, le programme ajoute le certificat de l'utilisateur au lieu du mot de passe administrateur. Cette option n'edialogue vous invitant à sélectionner un certificat s'affiche.

7. Cliquez sur **Fin**.

Le système crée le nouveau disque virtuel sécurisé sur votre disque dur.



Une fois monté, le nouveau disque virtuel sécurisé est visible comme tout autre disque de votre système et s'utilise de la même façon. Les données sont chiffrées et déchiffrées automatiquement.

Le démontage du disque (opération accessible par un clic avec le bouton droit de la souris dans l'Explorateur) ferme le disque et le supprime de la liste des lecteurs disponibles.

## 2.4 Installation sans surveillance

Une installation sans surveillance désigne une installation s'effectuant sans aucune intervention de l'utilisateur. Cette méthode vous permet d'installer SafeGuard PrivateDisk sur un grand nombre d'ordinateurs à l'aide d'une procédure automatisée.

Le répertoire `Install` de votre CD d'installation contient le fichier `sgpd100.msi` requis pour toute installation sans surveillance.

## 2.4.1 Syntaxe de la ligne de commande

Pour procéder à une installation sans surveillance, vous devez exécuter la commande `msiexec` avec certains paramètres.

Paramètres obligatoires :

`/I`

Spécifie le package d'installation à installer.

`/QN`

Installation sans interface utilisateur (installation sans surveillance)

Nom du fichier `.msi` : `sgpd100.msi`

Syntaxe :

```
msiexec /i <chemin>\sgpd100.msi /qn
```

Paramètre facultatif :

`/L* <chemin + nom_fichier>`

Consigne tous les avertissements et messages d'erreur à l'emplacement spécifié par `<chemin + nom_fichier>`.

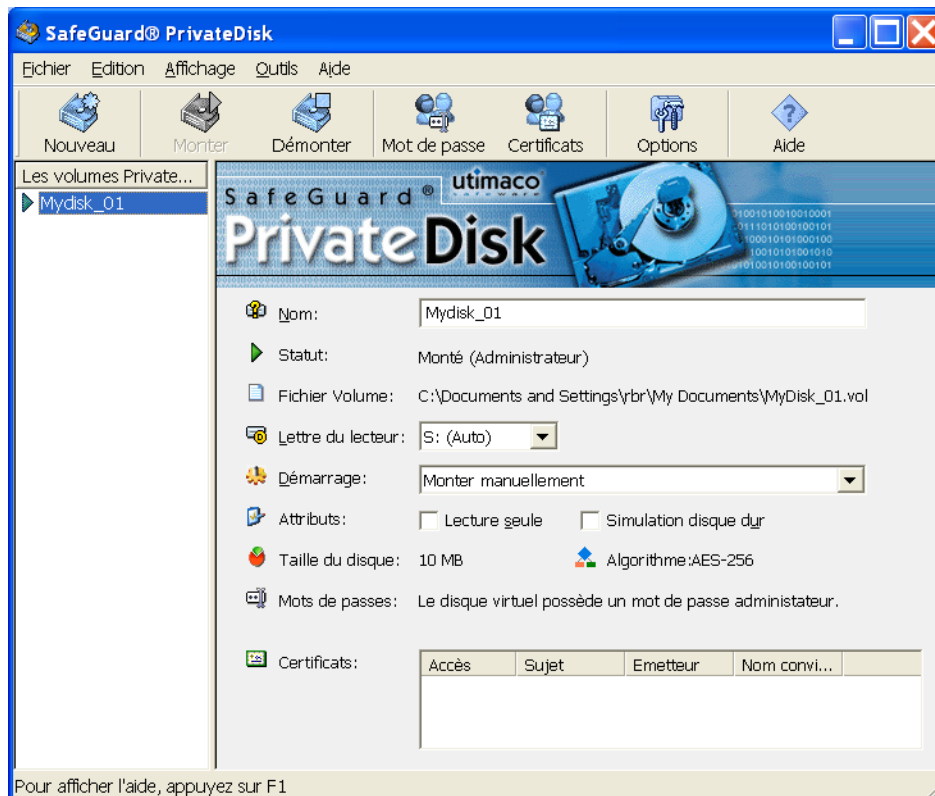
EXEMPLE:

```
msiexec /i C:\Install\sgpd100.msi /qn
```

Le système effectue alors une installation complète de SafeGuard PrivateDisk. Le programme est installé dans le répertoire d'installation par défaut (`<lecteur_système>`: `\Program Files\Sophos`). Le fichier `msi` réside dans le répertoire `Install` du lecteur `C`.

### 3 Application principale SafeGuard PrivateDisk®

Vous pouvez démarrer l'application principale SafeGuard PrivateDisk en cliquant avec le bouton droit de la souris sur l'icône correspondante dans la barre des tâches Windows, puis en cliquant sur **PrivateDisk**, ou en sélectionnant cette application dans le dossier de programmes Windows (Démarrer/Programmes/Sophos/SafeGuard PrivateDisk).



Le volet gauche de la fenêtre de l'application principale présente la liste des disques virtuels sécurisés disponibles.

Si un disque est sélectionné, le volet droit de la fenêtre de l'application principale affiche les détails concernant ce disque. Si aucun disque n'est sélectionné, par exemple au démarrage de l'application, le système affiche un écran de bienvenue fournissant des informations sur l'exécution de tâches élémentaires (telles que la création de disques virtuels sécurisés ou l'importation de disques).

Pour supprimer un disque de la liste des disques disponibles, sélectionnez-le, puis appuyez sur la touche **Suppr** de votre clavier (ou cliquez sur *Edition/Supprimer de la liste*). Le fichier volume reste disponible et peut être réimporté dans la liste des disques disponibles à tout moment.

Pour supprimer réellement un disque (ou, plus exactement, pour supprimer son fichier volume), commencez par le démonter, sélectionnez-le, puis cliquez sur *Edition/Supprimer*. Le système affiche alors une boîte de dialogue vous avertissant que toutes les données stockées sur le disque seront détruites. Si vous confirmez l'opération en cliquant sur **Oui**, le système supprime le fichier volume.

### 3.1 Commandes de barre d'outils et de menu

SafeGuard PrivateDisk comporte une barre d'outils contenant les boutons associés aux commandes essentielles :



- **Nouveau :**  
Démarré l'assistant de création d'un disque virtuel.
- **Monter :**  
Monte le disque virtuel sélectionné.
- **Démonteur :**  
Démonte le disque virtuel sélectionné.
- **Mot de passe :**  
Affiche la boîte de dialogue *Changer le mot de passe d'accès au disque virtuel* vous permettant de modifier/définir les mots de passe (administrateur et utilisateur) des disques virtuels.
- **Certificats :**  
Affiche la boîte de dialogue *Certificats pour les disques virtuels* vous permettant d'assigner et de modifier les certificats associés aux disques virtuels.
- **Options :**  
Permet de modifier les paramètres du programme. Cette option n'est accessible qu'aux administrateurs système.
- **Aide :**  
Ouvre l'aide en ligne de SafeGuard PrivateDisk.
- Toutes ces commandes sont également accessibles dans les différents menus (*Fichier, Edition, Affichage, Outils, Aide*).

Vous pouvez également cliquer sur l'icône SafeGuard PrivateDisk de la barre des tâches Windows pour accéder aux fonctions essentielles (et pour démarrer l'application principale SafeGuard PrivateDisk)

## 3.2 Informations sur le disque sélectionné

Si un disque est sélectionné dans la liste des disques virtuels sécurisés disponibles, le volet droit de la fenêtre principale affiche des informations détaillées concernant ce disque :

- **Nom :**  
Chaque disque virtuel dispose d'un nom symbolique. Le nom par défaut est le nom du fichier du disque sans l'information du chemin. Ce nom peut être changé dans la fenêtre.
- Pour changer le nom d'un disque, saisissez le nouveau nom et validez par la touche Entrée. Le nouveau nom s'affiche dans la liste des fichiers disponibles et ne s'applique qu'à cette liste ! Dans l'explorateur Windows, chaque disque virtuel apparaît de la façon suivante : `Disque amovible (lettre)!`
- **Statut :**  
Donne le statut actuel du disque virtuel sélectionné.
  - **Monté :** Le disque virtuel est monté et disponible.  
Le système affiche également entre parenthèses les droits d'accès associés au montage du disque (Administrateur, Utilisateur, Lecture seule)
  - **Non monté :** Le disque virtuel n'est pas monté
  - **Disque non trouvé :** Le disque spécifié n'existe pas (par exemple, lorsque le fichier a été renommé, déplacé ou effacé).
  - **Disque non PrivateDisk :** Ce disque ne correspond pas à un disque virtuel créé par SafeGuard PrivateDisk.
  - **L'accès est refusé :** L'accès au disque virtuel est refusé (vérifiez vos droits au niveau NTFS).
- **Fichier disque :**  
Montre l'emplacement et le nom du fichier correspondant au disque virtuel.
- **Lettre d'unité de disque :**  
Montre la lettre actuelle du disque virtuel et autorise son changement.  
La lettre peut être fixée (A à Z) ou peut être choisie automatiquement (mode **Automatique**). Dans ce cas, la prochaine lettre disponible est affectée lors du montage du disque.  
Les lettres d'unité de disque peuvent être changées par l'utilisateur à tout instant. Le changement devient effectif lors du prochain montage de disque.  
Par conséquent, à chaque changement de lettre, le système affichera un message vous demandant si vous voulez maintenant remonter le disque. Cliquez sur **Oui** pour valider immédiatement le changement.

■ **Démarrage :**

Précise quand et comment le disque virtuel sélectionné doit être monté. Les options suivantes sont disponibles:

■ **Monter manuellement**

Le disque virtuel n'est pas monté automatiquement. L'utilisateur doit monter le disque virtuel chiffré chaque fois qu'il veut l'utiliser.

■ **Monter après connexion de l'utilisateur au système**

Le disque virtuel chiffré est monté automatiquement après la connexion de l'utilisateur au système d'exploitation.

**Remarque :** Si l'option **Monter après connexion de l'utilisateur au système** est choisie, l'option **Se connecter automatiquement au démarrage** de l'onglet Généralités de la boîte de dialogue Options doit être sélectionnée.

■ **Monter lorsque que le fichier volume est accessible**

Le disque virtuel est monté automatiquement dès que l'unité de disque devient disponible. Cette option est valable pour les disques virtuels installés sur des réseaux et de type périphérique Plug&Play.

■ **Monter lorsque la carte à puce est insérée**

Le disque virtuel est monté automatiquement lors de l'insertion d'une carte à puce.

**Remarque :** Si l'option **Monter lorsque la carte à puce est insérée** est sélectionnée, un lecteur de carte à puce dans l'onglet Carte à puce dans la boîte de dialogue Options doit être sélectionné.

■ **Attributs :**

Permet de spécifier des options de montage pour le disque virtuel :

■ **Lecture seule :**

Le disque virtuel est monté pour un accès en lecture seule, même si l'utilisateur a des droits en lecture/écriture sur le fichier correspondant au disque virtuel.

Avec un accès en lecture/écriture, un disque virtuel ne peut être utilisé que par un seul utilisateur. L'attribut **Lecture seule** permet de partager les données qui sont chiffrées entre plusieurs utilisateurs.

Après un bref instant, les autres utilisateurs peuvent voir les changements opérés par l'utilisateur disposant d'un accès en écriture.

- **Simulation disque dur :**  
Si vous sélectionnez cette option, SafeGuard PrivateDisk simule un nouveau disque local et non un disque amovible. L'icône dans l'explorateur Windows est changée en conséquence. Pour créer un disque virtuel partagé cette option doit être activée. Les disques virtuels sont partagés si vous vous connectez avec les droits administrateur du système.
- **Taille du disque :**  
Indique la taille du disque virtuel sélectionné.  
Outre la taille, le système affiche l'algorithme utilisé pour le chiffrement  
**Remarque :** Il est impossible d'utiliser des lecteurs chiffrés avec AES-256 avec une version de SafeGuard PrivateDisk antérieure à la version 2,00.
- **Mots de passe :**  
La rubrique **Mots de passe** affiche les mots de passe assignés au disque virtuel chiffré. Il peut s'agir d'un mot de passe administrateur, d'un mot de passe administrateur et utilisateur ou seulement d'un mot de passe administrateur si un certificat avec des privilèges d'administrateur est assigné au disque.
- **Certificats :**  
Sous la rubrique **Certificats** apparaît la liste de tous les certificats assignés au disque virtuel. Pour chaque certificat il est possible de voir le type d'accès de celui-ci (utilisateur ou administrateur, lecture ou lecture/écriture).

Il est possible d'éditer une liste de tous les certificats assignés au disque virtuel seulement avec les droits administrateur (voir plus haut).

### 3.3 Création d'un disque virtuel

Vous pouvez créer des disques de différentes façons :

- Cliquez sur le bouton **Nouveau PrivateDisk** de la boîte de dialogue *Bienvenue*.
- Cliquez sur le bouton **Nouveau** de la barre d'outils SafeGuard PrivateDisk.
- Choisissez la commande **Nouveau** du menu *Fichier*.
- Cliquez sur **Nouveau** après avoir cliqué avec le bouton droit de la souris sur l'icône SafeGuard PrivateDisk dans la barre des tâches Windows.

Dans chacun des cas, l'Assistant pour le nouveau PrivateDisk s'exécute et vous guide tout au long de la procédure de création du disque.

### 3.4 Monter et démonter des disques virtuels chiffrés

Pour accéder à un disque virtuel chiffré, le disque doit tout d'abord être monté. Afin de pouvoir monter un disque, l'utilisateur doit être en possession d'un mot de passe ou doit détenir la clé privée d'un certificat assigné au disque virtuel.

Monter/démonter un disque virtuel manuellement :

- Sélectionnez un disque virtuel dans la liste et cliquez sur les boutons **Monter/Démonter** de la barre d'outils de SafeGuard PrivateDisk.
- Sélectionnez le disque virtuel dans la liste et cliquez sur **Monter/Démonter/Démonter tous les disques** dans le menu *Edition*.
- Cliquez sur l'icône SafeGuard PrivateDisk dans la barre de tâches de Windows. Lorsque vous sélectionnez **Monter/Démonter**, le système affiche la liste des disques pour vous permettre de choisir celui que vous souhaitez monter ou démonter.
- Sélectionnez le fichier correspondant au disque virtuel chiffré dans l'explorateur Windows et cliquez sur **Monter/Démonter** dans le menu contextuel de SafeGuard PrivateDisk.

On vous demandera un mot de passe ou un code PIN pour monter le disque.

Si un utilisateur ne peut pas accéder au disque parce qu'un autre utilisateur y est déjà connecté, le nom de l'utilisateur connecté s'affiche à titre d'information.

S'il est impossible de démonter un disque virtuel en raison de la présence d'une application référencée dans le disque, l'utilisateur a le choix entre les options suivantes :

- **Réessayer**  
Déconnecte l'utilisateur lorsque ce dernier a fermé l'application ou le fichier.
- **Forcer le démontage**  
Déconnecte l'utilisateur même si le disque est encore en cours d'utilisation.  
**Avis :**  
Risque de perte des données non enregistrées !
- **Annuler**  
L'utilisateur reste connecté au système.

En dehors du fait de pouvoir monter manuellement un disque virtuel, SafeGuard PrivateDisk offre d'autres méthodes, comme **Monter après connexion de l'utilisateur au système**, **Connexion unique**, **Monter lorsque la carte à puce est insérée**. Veuillez voir les chapitres correspondants pour de plus amples détails.

## 3.5 Importation d'un disque virtuel chiffré dans la liste

Il est possible d'ajouter un disque virtuel chiffré dans la liste des disques virtuels disponibles. Pour cela, utilisez le commande **Importer** du menu *Fichier* pour faire apparaître ce disque virtuel dans la liste.

Une boîte de dialogue apparaît pour sélectionner le disque virtuel recherché. Sélectionnez-le et cliquez sur **Ouvrir**. Le disque est aussitôt ajouté à la liste des disques virtuels disponibles.

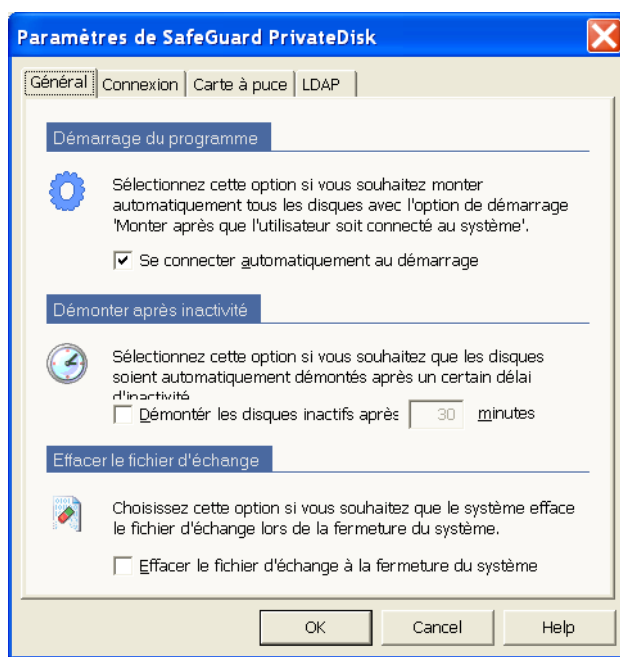
## 3.6 Options du SafeGuard® PrivateDisk

SafeGuard PrivateDisk vous offre certaines options de configuration afin d'adapter le produit à vos besoins personnels. Ces paramètres peuvent être trouvés dans la boîte de dialogue *Options*. Ouvrez la boîte de dialogue en cliquant sur le bouton **Options** dans la barre d'outils de l'application principale SafeGuard PrivateDisk (ou en cliquant sur **Options** dans le menu *Outils*). La boîte de dialogue *Options* est également accessible par un clic droit sur l'icône PrivateDisk dans la barre de tâches, suivi d'un clic sur *Options*.

La boîte de dialogue *Options* vous offre trois onglets différents:

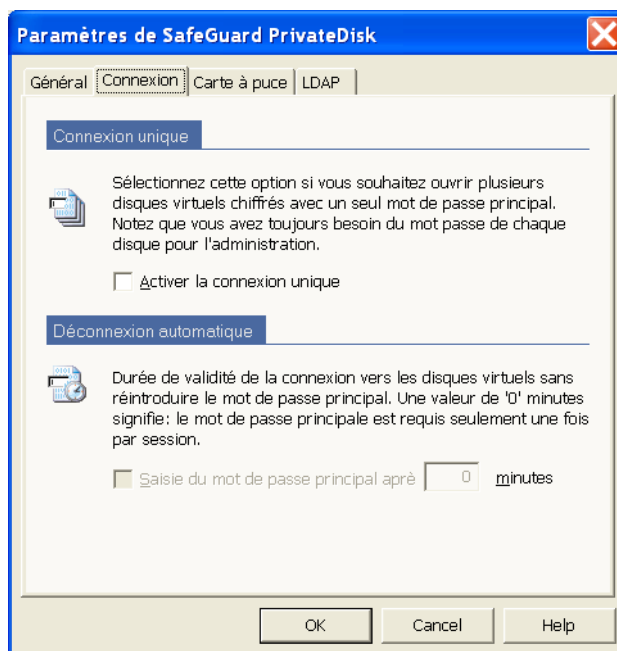
### 3.6.1 L'onglet Généralités

L'onglet *Généralités* contient des options de base déterminant le comportement de SafeGuard PrivateDisk.



- **Se connecter automatiquement au démarrage :**  
Si cette option est activée, tous les disques virtuels créés avec le paramétrage **Monter après connexion de l'utilisateur au système** sont montés automatiquement après l'identification au système. Une boîte de dialogue apparaît à l'écran vous demandant les mots de passe ou le mot de passe principal pour accéder aux disques.
- **Démonter les disques inactifs après :**  
En cas d'activation de cette option, tous les disques montés seront fermés après un certain délai d'inactivité.
- **Effacer le fichier d'échange à la fermeture du système :**  
Le fichier d'échange pouvant contenir des données sensibles, SafeGuard PrivateDisk vous offre la possibilité de le vider à la fermeture du système. Cette option permet de s'assurer que lors de l'arrêt du système, le fichier d'échange de Windows est effacé. Ainsi, aucune information confidentielle ne peut être récupérée.

### 3.6.2 L'onglet Connexion



- **Activer la connexion unique :**  
Si un utilisateur souhaite utiliser plus d'un disque virtuel chiffré, chacun des mots de passe des différents disques lui sera demandé. Afin de simplifier cette procédure, SafeGuard PrivateDisk vous offre la possibilité d'une identification unique en utilisant un seul mot de passe dit principal. En cas d'activation, ce mot de passe principal permet de chiffrer tous les mots de passe des disques virtuels. L'utilisateur doit par la suite entrer uniquement ce mot de passe principal au lieu de chacun des mots de passe.

Lors de l'activation de cette fonction d'identification unique, SafeGuard PrivateDisk est capable de rejouer tous les mots de passe.

Afin de changer ce mot de passe de connexion unique, la commande de menu Outils/Changer le mot de passe principal peut être utilisée.

Pour vous éviter d'avoir à entrer plusieurs fois le mot de passe de connexion unique, ce dernier est enregistré en mémoire pendant une durée configurable.

- **Saisie du mot de passe principal après X minutes**

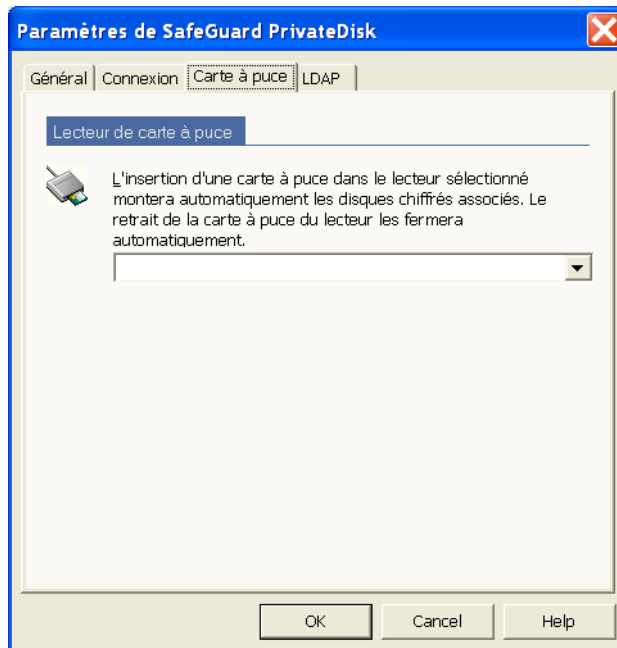
Permet de spécifier une durée au delà de laquelle le mot de passe principal sera à nouveau demandé.

**Remarque :** Cette fonction de connexion unique n'est pas disponible en cas d'identification par le biais de certificats.

### 3.7 L'onglet Carte à puce

Si le paramètre **Monter lorsque la carte à puce est insérée** est spécifié au niveau du disque virtuel, il sera monté automatiquement si la carte à puce est présentée dans le lecteur.

Inversement, il est possible de démonter automatiquement le disque virtuel lorsque la carte à puce est retirée.



Afin d'activer cette fonction, il est nécessaire de préciser le lecteur de carte devant être utilisé. Sélectionnez le lecteur correspondant dans le menu déroulant de l'onglet *Carte à puce*.

### 3.7.1 L'onglet LDAP

Cette boîte de dialogue est disponible uniquement dans l'édition Enterprise.

Lorsque vous assignez des certificats à un lecteur PrivateDisk, SafeGuard PrivateDisk vous permet de faire appel à une recherche LDAP pour trouver des utilisateurs spécifiques.

Les paramètres de cette recherche sont affichés dans cette boîte de dialogue. Il est normalement impossible de les modifier car ils ont été définis via un modèle administratif de l'administration centralisée. Seul un utilisateur détenteur de droits d'administrateur et connecté à SafeGuard PrivateDisk peut modifier les options dans cette boîte de dialogue.

En recherchant un certificat précis (par exemple, à l'aide de l'adresse de messagerie dans le certificat), l'utilisateur de ce certificat peut accéder à un lecteur PrivateDisk puisque ce dernier est assigné au certificat.

Lorsqu'un certificat est assigné, ces paramètres peuvent être définis ou modifiés en local même si l'utilisateur ne détient pas de droits d'administrateur.

## 3.8 Mots de passe et certificats

Un disque virtuel peut avoir exactement un mot de passe administrateur et un mot de passe utilisateur (avec soit un accès en lecture/écriture ou en lecture seule).

De manière additionnelle, des certificats peuvent être assignés aux disques virtuels.

Alors que seulement deux mots de passe peuvent être assignés à un disque virtuel, SafeGuard PrivateDisk vous permet d'assigner jusqu'à 32 certificats.

De manière identique aux mots de passe, les certificats peuvent avoir des droits utilisateur (avec un accès en lecture/écriture ou en lecture seule) ou administrateur.

### 3.8.1 Accès aux disques virtuels chiffrés

#### Connexion avec un mot de passe

L'accès à un disque virtuel chiffré peut être autorisé en spécifiant un mot de passe. SafeGuard PrivateDisk offre trois niveaux de privilège, mais un seul mot de passe utilisateur peut être associé à un disque virtuel en plus du mot de passe administrateur:

- **Mot de passe administrateur :**

C'est le mot de passe initial pour tout nouveau disque virtuel. L'utilisation d'un mot de passe administrateur permet de spécifier un mot de passe utilisateur pour le disque, d'effacer ce mot de passe utilisateur (même s'il n'est pas connu), de modifier le mot de passe administrateur et aussi d'ajouter/d'enlever des certificats (voir ci-après) au disque virtuel.

**Remarque :** Il est également possible d'utiliser un certificat pour authentifier l'administrateur.

Lors de la création d'un nouveau disque virtuel, un certificat peut être associé à l'administrateur au lieu d'un mot de passe !

- **Mot de passe utilisateur avec accès en lecture/écriture :**  
Ce mot de passe utilisateur permet de monter un disque virtuel chiffré et d'y accéder en lecture/écriture.
- **Mot de passe utilisateur avec accès en lecture seule :**  
Ce mot de passe utilisateur permet de monter un disque virtuel chiffré et d'y accéder uniquement en lecture.

### **Connexion avec un certificat**

L'utilisation de mots de passe pour l'accès à un disque virtuel est optionnelle. Des certificats peuvent être utilisés de manière additionnelle ou à la place des mots de passe.

Un certain nombre de certificats (jusqu'à 32) peuvent être associés à chaque disque virtuel. Dans ce cas, la clé publique du certificat est utilisée pour chiffrer la clé de chiffrement du disque (clé AES 128). Seul le propriétaire d'un certificat a accès à la clé privée du certificat et peut l'utiliser pour s'identifier au disque virtuel.

De manière identique aux mots de passe, les certificats peuvent être associés à un privilège (accès en lecture/écriture ou accès en lecture seule ou accès administrateur).

L'identification aux disques virtuels par le biais de certificats offre de nombreux avantages :

- Les administrateurs peuvent facilement assigner des utilisateurs au disque virtuel en utilisant la partie publique disponible du certificat de l'utilisateur.
- Il n'est pas nécessaire de créer et de distribuer des mots de passe initiaux.
- Comme pour les mots de passe, les certificats peuvent être associés soit à des utilisateurs (pour un accès soit en lecture seule soit en lecture/écriture, soit à des administrateurs avec le droit de changer les mots de passe et les certificats assignés).
- Pour ajouter ou enlever des certificats, l'utilisateur doit d'abord s'authentifier au disque comme administrateur (en utilisant soit le mot de passe administrateur ou en possédant un des certificats administrateurs assignés au disque virtuel).

### **Connexion unique**

Lors de l'utilisation de plusieurs disques virtuels, les utilisateurs doivent s'authentifier séparément sur chaque disque. En cas d'utilisation de mots de passe, l'utilisateur doit se rappeler tous les mots de passe pour pouvoir monter tous ses disques virtuels.

Afin de simplifier la procédure d'authentification dans ce cas précis, SafeGuard PrivateDisk propose une fonction de connexion unique qui va rejouer automatiquement tous les mots de passe des disques virtuels. Les mots de passe sont sauvegardés chiffrés dans la base de registres. Pour sécuriser la liste des mots de passe, un mot de passe principal est utilisé. L'utilisateur doit simplement s'en souvenir et le saisir comme mot de passe d'identification unique.

## Démarrage et arrêt automatique

Le disque virtuel chiffré est monté automatiquement après la connexion de l'utilisateur au système d'exploitation, après avoir demandé les mots de passe ou certificats nécessaires.

Les disques virtuels sont démontés automatiquement lors de l'arrêt ou de la fermeture de session. Par ailleurs, les disques virtuels peuvent être démontés après un certain délai d'inactivité.

## Support de cartes à puces

SafeGuard PrivateDisk supporte également l'utilisation de certificats stockés dans des cartes à puce. L'identification à un disque virtuel est réalisée par l'utilisation de la clé privée stockée dans la carte à puce insérée.

SafeGuard PrivateDisk réagit à l'insertion et à l'enlèvement de cartes à puce et est capable de monter et démonter des disques virtuels:

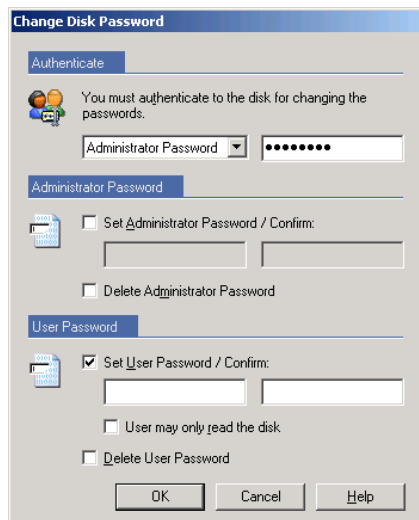
- Lors de l'insertion d'une carte à puce, tous les disques virtuels configurés de la manière **Monter lorsque la carte à puce est insérée** sont automatiquement montés.

Lors de l'enlèvement d'une carte à puce, tous les disques virtuels authentifiés par un certificat sur carte à puce sont démontés.

**Remarque :** La gestion des certificats n'est pas prise en charge par SafeGuard PrivateDisk, cela peut être fait par le biais d'une infrastructure PKI interne ou par une autorité de certification tierce.

### 3.8.2 Edition de mots de passe

Pour modifier les mots de passe, SafeGuard PrivateDisk propose la boîte de dialogue *Changer le mot de passe* d'accès au disque virtuel. Pour ouvrir cette boîte de dialogue, cliquez sur le bouton Mots de Passe dans la barre d'outils ou sur *Changer le mot de passe...* du menu *Edition*.



Cette boîte de dialogue permet :

- **Créer/Changer le mot de passe administrateur**  
Pour changer le mot de passe administrateur, l'utilisateur doit être lui-même administrateur du disque (soit en connaissant l'ancien mot de passe administrateur ou en possédant un des certificats privilégiés de l'administrateur associés au disque)
- **Créer/Changer le mot de passe utilisateur**  
Pour changer le mot de passe utilisateur, l'utilisateur doit être capable de s'identifier au disque virtuel (soit en connaissant l'ancien mot de passe utilisateur ou en ayant le mot de passe actuel de l'administrateur ou en possédant un des certificats privilégiés administrateur associés au disque).
- **Effacer le mot de passe utilisateur**  
Pour effacer le mot de passe utilisateur, l'utilisateur doit être l'administrateur du disque virtuel (soit en connaissant le mot de passe administrateur ou en possédant un des certificats privilégiés de l'administrateur associés au disque)

**Pour changer le mot de passe administrateur**, vous devez vous authentifier au disque en utilisant le mot de passe administrateur:

- Sélectionnez le **Mot de passe administrateur** dans la section Authentification et entrez le mot de passe administrateur.
- Activez l'option **Saisir un mot de passe administrateur**.

- Entrez un nouveau mot de passe administrateur et confirmez le.

**Remarque :** Si un certificat avec des droits administrateur est utilisé (en sélectionnant **Certificat** dans le menu déroulant de la section Authentification), le mot de passe administrateur peut aussi être effacé en choisissant l'option correspondante. Le disque virtuel ne pourra être administré que par un certificat ayant les droits administrateur.

La gestion du mot de passe utilisateur est réalisée de la même manière.

Si vous vous authentifiez au disque virtuel par le biais d'un mot de passe utilisateur, vous ne pourrez changer que le mot de passe utilisateur.

**La création d'un mot de passe utilisateur et son effacement n'est possible qu'en ayant des droits administrateur (soit par le biais du mot de passe administrateur ou en ayant un certificat avec les droits administrateur).**

### 3.8.3 Délai associé à un mot de passe incorrect

Si l'utilisateur entre un mot de passe incorrect, il doit attendre un certain délai avant de pouvoir effectuer une nouvelle tentative de connexion. Ce délai peut être défini sur 2, 5, 10 ou 20 secondes. Le système mémorise le délai réel imposé pour chacun des 10 derniers disques utilisés dans SafeGuard PrivateDisk.

### 3.8.4 Assigner des certificats

L'accès à un disque virtuel peut être également autorisé par le biais de certificats (jusqu'à 32).

**Remarque :** Plusieurs utilisateurs ne peuvent pas accéder à un disque virtuel en lecture/écriture simultanément. Si plusieurs utilisateurs souhaitent accéder à un même disque virtuel chiffré, ils doivent l'ouvrir uniquement en lecture seule.

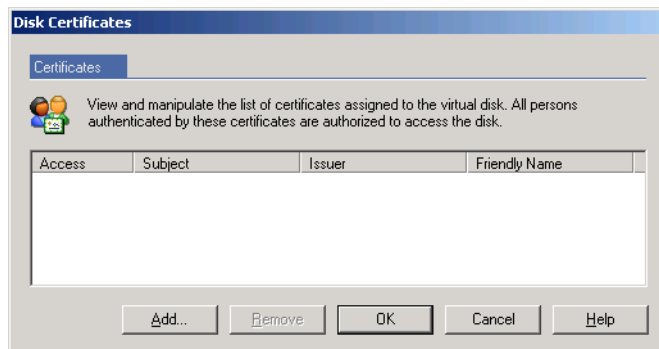
Comme pour les mots de passe, SafeGuard PrivateDisk fait la distinction entre des :

- Certificats administrateur
- Certificats utilisateur
- Certificats utilisateur avec accès en lecture seule

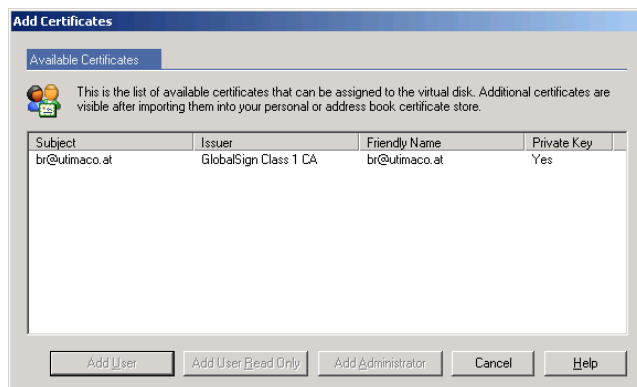
**Remarque :** Pour assigner des certificats à un disque virtuel, vous devez être authentifié en tant qu'administrateur du disque (avec le mot de passe administrateur ou un certificat administrateur).

Pour ajouter des certificats :

1. Cliquez sur le bouton **Certificats** ou choisissez **Certificats...** dans le menu *Edition*.
2. Entrez le mot de passe administrateur et cliquez sur **OK**.  
La boîte de dialogue **Certificats** pour les disques virtuels apparaît.



3. Tous les certificats déjà assignés sont présentés dans cette boîte de dialogue.
4. Pour ajouter des certificats cliquez sur le bouton **Ajouter**.  
La boîte de dialogue *Ajouter des certificats* apparaît.



5. Une liste des certificats disponibles pouvant être assignés au disque apparaît.

**Remarque :** Seuls apparaissent les certificats des dépôts **Personnel**, **Carnet d'Adresses** et **Autres Personnes** de l'Utilisateur actuel et ceux de l'Ordinateur local. Les certificats stockés dans d'autres dépôts ne sont pas reconnus par SafeGuard PrivateDisk!

## Utilisation de LDAP pour chercher un certificat

Si vous voulez assigner un certificat qui n'est pas encore détenu dans ces dépôts de certificats, SafeGuard PrivateDisk vous offre la possibilité d'effectuer une recherche LDAP pour trouver un certificat. Le paramétrage de la recherche LDAP peut être central, dans la rubrique Options de la page LDAP.

- Pour rechercher un certificat, cliquez sur **Chercher le certificat** dans la boîte de dialogue *Ajouter des certificats*. La boîte de dialogue Recherche LDAP s'ouvre.
- Cliquez sur le bouton **Rechercher**. SafeGuard PrivateDisk affiche la liste de tous les certificats qu'il trouve à l'aide des critères de recherche que vous avez définis (données de connexion et filtre de recherche).  
Les filtres sont définis pour permettre la recherche de données spécifiques dans un certificat (par exemple, une adresse de messagerie). Ainsi, si vous vous servez de l'adresse de messagerie pour rechercher un certificat en particulier, le système vous invite à saisir l'adresse de messagerie de la personne pour laquelle vous souhaitez assigner le certificat au disque PrivateDisk.  
Vous pouvez également utiliser des données différentes pour rechercher un certificat. Le système vous invite à entrer les différentes informations requises, en fonction des filtres définis par l'administrateur. Veuillez noter que vous devez saisir ces données (par exemple cn – Common Name) exactement comme elles sont inscrites sur le certificat.
- En bas de la boîte de dialogue, SafeGuard PrivateDisk affiche tous les certificats correspondant à vos critères de recherche. Seuls sont affichés les certificats pouvant être utilisés avec SafeGuard PrivateDisk.
- Marquez le certificat demandé et cliquez sur **Ajouter** pour le transférer vers la liste des certificats disponibles à partir de laquelle vous pouvez l'assigner à un lecteur de disque. La partie publique du certificat est copiée dans le dépôt de certificats.

## Modifier la recherche LDAP

Cliquez sur le bouton Etendu pour afficher les paramètres LDAP et les modifier. Seul un administrateur devrait modifier ces paramètres car cette action exige une connaissance exhaustive de LDAP.

Toutefois, un utilisateur " normal " peut avoir besoin de changer le filtre utilisé. Il est par exemple possible de définir une variété de filtres et de les utiliser pour effectuer une recherche par adresse de messagerie ou Common Name du certificat. Vous pouvez sélectionner un des filtres prédéfinis affichés sous Filtre. Si vous supprimez la ligne Filtre dans cette boîte de dialogue, le système affichera tous les certificats trouvés dans le service d'annuaire LDAP spécifié. Cela peut vous être utile, notamment si vous ne savez pas comment sont écrites les données que vous recherchez (nom d'utilisateur dans le certificat, Common Name, adresse de messagerie, etc.). Vous pouvez ensuite sélectionner le certificat nécessaire dans la liste. Gardez à l'esprit que cette procédure peut générer une très longue liste de certificats !t

## Enregistrer les paramètres

Si vous modifiez les paramètres dans la boîte de dialogue *Recherche LDAP*, vous pouvez les enregistrer et les rétablir en cliquant sur un des boutons placés en haut à droite. Lorsque vous enregistrez les paramètres, vous devez leur donner un nom. Celui-ci vous permettra de les identifier ultérieurement. Vous pouvez sélectionner les paramètres à charger à partir d'une liste.

6. Sélectionnez un certificat dans la liste et suivant les privilèges que vous voulez assigner à l'utilisateur cliquez sur :
  - Ajouter un Utilisateur
  - Ajouter un Utilisateur en Lecture seule
  - Ajouter un Administrateur
7. Le certificat apparaît dans la liste des certificats assignés au disque virtuel. Sous Accès, les droits d'accès respectifs d'un certificat sont visibles.

### 3.8.5 Suppression de certificats assignés à un disque

Pour supprimer des certificats assignés à un disque, procédez comme suit :

1. Cliquez sur **Certificats** dans la barre d'outils ou sélectionnez **Certificats...** dans le menu **Edition**.
2. Entrez le mot de passe administrateur du disque virtuel ou utilisez votre certificat d'authentification, puis cliquez sur **OK**.  
Le système affiche la boîte de dialogue *Certificats pour les disques virtuels*.
3. Pour supprimer un certificat de la liste, sélectionnez-le, puis cliquez sur **Supprimer**.  
Le propriétaire du certificat n'a plus accès à ce disque virtuel.

## 3.9 Clés SafeGuard Enterprise

Vous pouvez monter un lecteur PrivateDisk à l'aide de clés SafeGuard Enterprise. Si un jeu de clés existe, ces clés SafeGuard Enterprise vous sont proposées lorsque vous créez un lecteur par le biais de l'Assistant SafeGuard PrivateDisk.

Si une clé SafeGuard Enterprise est assignée au lecteur, seule cette clé sera utilisée pour le montage du lecteur PrivateDisk. Aucun mot de passe supplémentaire n'est requis. Si la clé existe sur l'ordinateur, elle est automatiquement utilisée pour le montage du lecteur PrivateDisk. Si l'option *Monter après que l'utilisateur est connecté au système* est activée pour le lecteur, la procédure de montage s'effectue de façon transparente. Le lecteur est alors disponible dès que vous ouvrez une session Windows.

## Clés locales

SafeGuard Enterprise distingue les clés créées au niveau central et automatiquement distribuées aux utilisateurs de celles qui ont été créées au niveau local sur les ordinateurs clients. Les clés locales sont accessibles par l'intermédiaire d'une passphrase.

Vous pouvez également monter des lecteurs PrivateDisk à l'aide de clés locales. Si la clé existe sur l'ordinateur, elle est automatiquement utilisée pour le montage du lecteur.

Si la clé locale n'est pas disponible sur l'ordinateur, l'utilisateur est invité à entrer la passphrase.

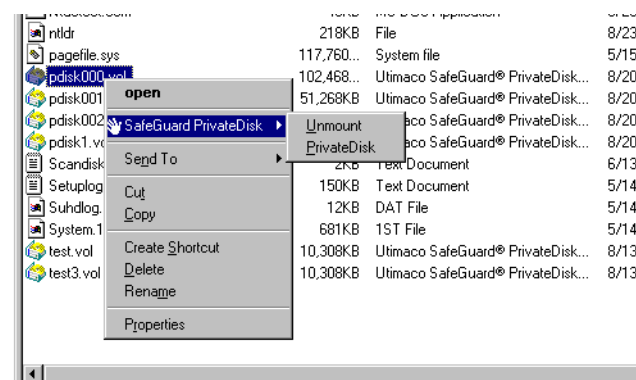
Si un utilisateur est autorisé à accéder au volume alors qu'il ne dispose pas de la clé locale du lecteur PrivateDisk, la passphrase de la clé doit lui être communiquée.

## 3.10 Extensions de l'explorateur Windows

SafeGuard PrivateDisk ajoute l'option de menu *SafeGuard PrivateDisk* au menu contextuel de l'explorateur Windows.

En fonction du fichier ou du disque sélectionné dans l'Explorateur, les commandes suivantes sont disponibles :

- Si vous effectuez un clic droit sur un fichier de volume (.vol), le système affiche l'option de montage ou de démontage du disque virtuel (en fonction de son statut) et l'option de démarrage de l'application principale.
- Si vous effectuez un clic droit sur un fichier de volume (.vol) qui n'a pas encore été ajouté à la liste des disques disponibles dans l'application principale de SafeGuard PrivateDisk, une commande **Importer** s'ajoutera au menu. Cliquez sur **Importer** pour ajouter le disque à la liste des disques virtuels disponibles dans l'application principale de SafeGuard PrivateDisk.



## 4 SafeGuard PrivateDisk Portable

SafeGuard PrivateDisk Portable vous permet d'accéder à des lecteurs PrivateDisk même si votre ordinateur n'est pas équipé de SafeGuard PrivateDisk.

Cette opération est possible grâce à la copie d'un programme spécifique (PDPortable.exe) sur le support amovible. Vous pouvez sélectionner l'option de copie de SafeGuard PrivateDisk Portable sur le support amovible lorsque vous créez un lecteur PrivateDisk.

Lorsque vous connectez le support amovible à un ordinateur non doté de SafeGuard PrivateDisk, vous ne pouvez pas accéder au lecteur PrivateDisk. Mais une fois que vous avez démarré SafeGuard PrivateDisk Portable, vous pouvez sélectionner le lecteur PrivateDisk, puis accéder à ses fichiers chiffrés après avoir entré le mot de passe qui lui est associé.

SafeGuard PrivateDisk Portable ne vous permet pas d'ajouter de fichiers au lecteur PrivateDisk. Vous pouvez cependant enregistrer des fichiers du lecteur PrivateDisk à un autre emplacement. Dans ce cas, les fichiers enregistrés au nouvel emplacement ne sont pas chiffrés.

### 4.1 Ouverture de lecteurs PrivateDisk

Pour ouvrir un lecteur PrivateDisk, procédez comme suit :

1. Pour démarrer SafeGuard PrivateDisk Portable, double-cliquez sur `PDPortable.exe`.
2. Cliquez sur **Fichier > Ouvrir**, puis sélectionnez le lecteur PrivateDisk.
3. Entrez le mot de passe du lecteur PrivateDisk.

**Remarque :** Pour permettre l'échange de données à l'aide de cette méthode, le mot de passe doit être communiqué au destinataire du lecteur SafeGuard PrivateDisk.

4. SafeGuard PrivateDisk Portable présente désormais le lecteur et son contenu. Une fonctionnalité de type Explorateur Windows est alors accessible.
5. Vous pouvez ouvrir des fichiers en double-cliquant sur ces derniers.

## 4.2 Extracting files

Pour extraire des fichiers d'un lecteur PrivateDisk, procédez comme suit :

1. Sélectionnez le ou les fichiers.
2. Cliquez sur **Edition > Extraire**.
3. Sélectionnez un emplacement pour le ou les fichiers.
4. Cliquez sur **Enregistrer**.

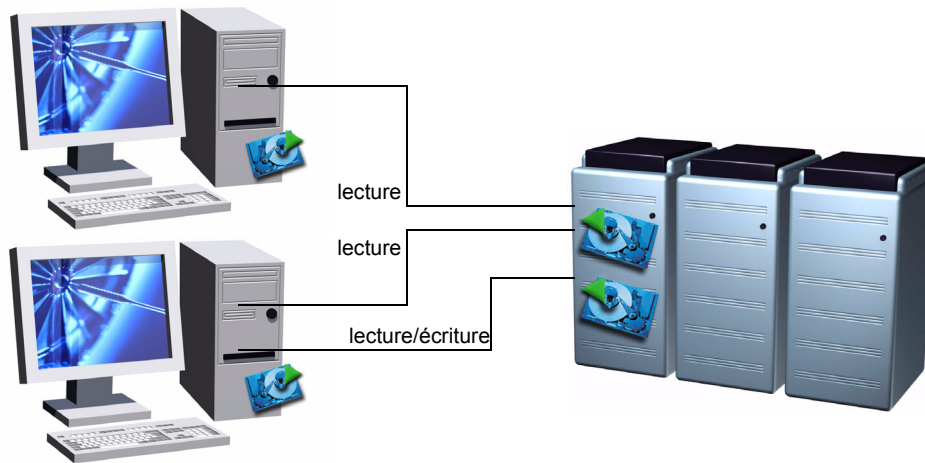
## 5 Exemples de cas d'utilisation

SafeGuard PrivateDisk est une solution intuitive de sécurisation des fichiers stockés sur des postes de travail, ordinateurs portables, serveurs de fichiers et serveurs de terminaux. Les sections qui suivent présentent quelques exemples de scénarios types de protection des données confidentielles avec SafeGuard PrivateDisk.

### 5.1 Utilisateur de poste de travail

Les disques virtuels d'utilisateurs de poste de travail sont généralement créés sur des lecteurs fixes locaux ou sur des emplacements réseau. SafeGuard PrivateDisk garantit la confidentialité des données même lorsque ces dernières sont échangées sur un réseau. Il suffit alors à l'utilisateur d'un poste de travail d'ouvrir le disque virtuel sécurisé sur le serveur de fichiers. SafeGuard PrivateDisk doit simplement être installé sur les postes de travail. Il n'est pas nécessaire de l'installer sur le serveur de fichiers. Le serveur de fichiers stocke uniquement les disques virtuels sécurisés.

Notre exemple comprend deux postes de travail en réseau ainsi qu'un serveur de fichiers. Deux fichiers volume de disque virtuel sécurisé sont stockés sur le serveur de fichiers. L'un des disques virtuels est utilisé par plusieurs postes clients et est donc uniquement accessible en lecture seule. Le second disque virtuel est ouvert par un seul poste client qui dispose donc d'un accès en lecture et en écriture sur ce disque.



Avantages liés à l'utilisation de SafeGuard PrivateDisk :

- Les utilisateurs peuvent stocker des données confidentielles sur les postes serveurs en toute sécurité.
- Les utilisateurs peuvent accéder simultanément en lecture aux disques virtuels.

- Les données transmises entre les clients et les serveurs sont systématiquement chiffrées puisque le chiffrement et le déchiffrement sont effectués par les postes clients.
- Aucune capacité processeur supplémentaire n'est requise sur les postes serveurs puisque le chiffrement est effectué par les postes de travail.
- Les administrateurs des postes serveurs n'ont aucun accès aux données confidentielles s'ils ne sont pas autorisés à ouvrir les disques virtuels. Ceci permet notamment de séparer systématiquement les tâches de l'administrateur de la sécurité de celles de l'administrateur système.
- Un administrateur de sécurité peut créer des fichiers volume de disque virtuel situés au niveau central.
- Les fichiers volume stockés sur les postes serveurs peuvent être aisément inclus dans le plan de sauvegarde des serveurs d'une entreprise.

**Remarque :** L'accès à un disque virtuel sécurisé étant contrôlé de la même façon que l'accès à un fichier unique, plusieurs utilisateurs ne peuvent pas accéder simultanément à un même disque virtuel sécurisé (et l'ouvrir avec un accès en lecture et en écriture).

Si un disque virtuel est monté par un utilisateur avec des droits de lecture/écriture, il ne peut pas être monté par un autre utilisateur. Pour que plusieurs utilisateurs puissent disposer d'un accès simultané à un disque virtuel sécurisé, ils doivent tous monter ce dernier avec un accès en lecture seule.

#### **Accès simultanés en lecture/écriture aux disques virtuels sécurisés**

Les disques chiffrés virtuels peuvent être partagés avec des utilisateurs du réseau comme des lecteurs normaux. Ainsi, si SafeGuard PrivateDisk est installé sur un poste serveur, ce dernier peut partager ses disques virtuels ouverts avec les utilisateurs du réseau. Les postes clients peuvent monter ces disques virtuels partagés comme des ressources réseau standard. Les groupes d'utilisateurs disposent alors d'un accès total (lecture et écriture) simultané aux disques virtuels chiffrés partagés.

#### **Remarques:**

- L'accès aux disques virtuels partagés est uniquement protégé par le biais de fonctions du système d'exploitation (par un mot de passe ou par des informations d'identification utilisateur). Les clients n'ont pas besoin de s'authentifier vis-à-vis des disques virtuels.
- Les données échangées entre les serveurs et les clients sont transmises en texte clair (non chiffré) puisque le déchiffrement est effectué sur le poste serveur. Il est possible d'utiliser un logiciel VPN (réseau privé virtuel) pour sécuriser la connexion.
- Les disques virtuels doivent être ouverts sur le serveur par une personne autorisée.

## 5.2 Utilisateur mobile

La menace la plus importante pour la sécurité des utilisateurs d'ordinateurs portables est le vol. Bien que la solution SafeGuard PrivateDisk ne puisse pas protéger les ordinateurs portables contre le vol, elle permet d'empêcher la lecture des données confidentielles par des étrangers.

Notre exemple comprend un ordinateur portable doté d'un disque virtuel sécurisé local et d'un second disque virtuel sur CD-ROM (contenant par exemple des listes de prix de produits internes, etc.). Les données peuvent être mises à jour entre le siège social et l'utilisateur mobile de façon sécurisée grâce à l'utilisation de fichiers volume virtuels sur CD-ROM. Seuls les utilisateurs autorisés peuvent ouvrir le disque virtuel (à l'aide d'un mot de passe ou en détenant la clé privée d'un certificat assigné) et en lire le contenu.



Avantages liés à l'utilisation de SafeGuard PrivateDisk :

- Les données confidentielles sur le disque dur local sont protégées lorsque l'ordinateur portable est allumé, ainsi qu'en cas de perte ou de vol de ce dernier.
- Pour les personnes non autorisées, le disque virtuel sécurisé ressemble à un fichier normal et la structure des répertoires est masquée.  
Les données confidentielles sont même protégées contre les personnes pouvant accéder physiquement à l'ordinateur portable à condition que ces dernières ne connaissent pas le mot de passe requis pour l'ouverture du disque virtuel sécurisé et que la clé privée des certificats éventuellement assignés soit correctement protégée.
- Il est possible de sécuriser les données confidentielles sans avoir à chiffrer la totalité du disque dur ou des partitions entières.
- Les fichiers volume des disques virtuels sécurisés sont aisément stockables sur des disques durs, des lecteurs réseau et des supports amovibles (disquettes, disques ZIP, CD-ROM, cartes mémoire USB, etc.).
- Les fichiers volume des disques virtuels sécurisés peuvent être échangés en toute sécurité sur des canaux peu sûrs tels qu'une messagerie électronique.

## 5.3 Serveurs de terminaux

SafeGuard PrivateDisk peut être installé sur des serveurs de terminaux. Pour garantir la confidentialité des utilisateurs de serveurs de terminaux, un disque virtuel sécurisé n'est visible que par l'utilisateur l'ayant ouvert.

Avantages liés à l'utilisation de SafeGuard PrivateDisk :

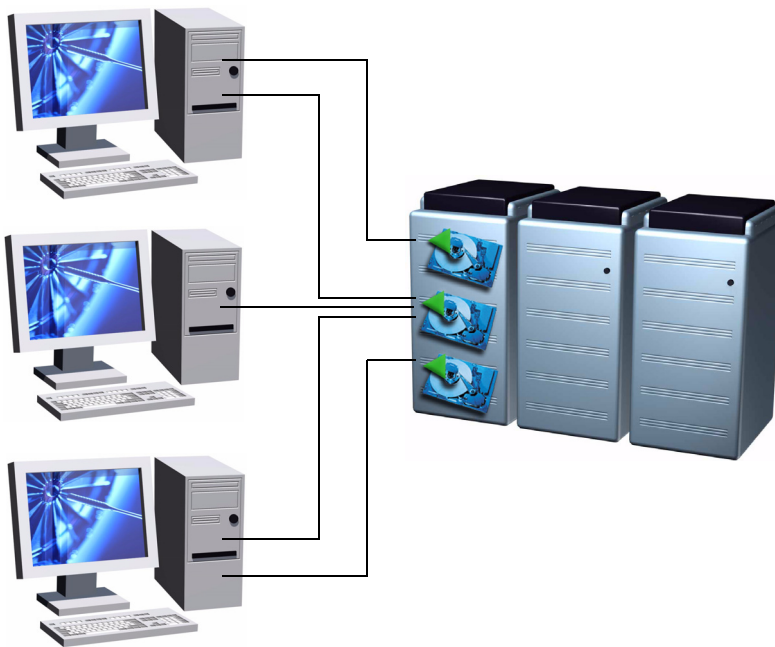
- Les utilisateurs peuvent travailler avec des données confidentielles non accessibles à l'administrateur système du poste serveur de terminaux.
- Les disques virtuels sécurisés ne sont visibles que par les utilisateurs autorisés. Si un utilisateur ouvre un disque virtuel, ce dernier n'est visible par d'autres utilisateurs que si ceux-ci ouvrent également le même disque virtuel.

**Exemple:**

L'UTILISATEUR 1 ouvre un disque virtuel sécurisé en tant que lecteur X

L'UTILISATEUR 2 ne voit pas le lecteur X de l'UTILISATEUR 1 mais peut également ouvrir ce disque virtuel. L'UTILISATEUR 2 peut même ouvrir un autre disque virtuel chiffré en tant que lecteur X.

- Plusieurs utilisateurs peuvent partager un accès en lecture et en écriture à un même disque virtuel sécurisé. **Ceci permet aux groupes d'utilisateurs de travailler simultanément sur les mêmes disques virtuels.**
- Les données transférées entre le serveur de terminaux et ses clients sont sécurisées au moyen du protocole du serveur de terminaux.
- Seuls les postes serveurs de terminaux doivent être administrés (installation des logiciels, etc.).



La figure ci-dessus présente un environnement de serveurs de terminaux dans lequel deux des trois utilisateurs disposent de disques virtuels sécurisés et où tous les utilisateurs partagent également un autre disque virtuel.

**Remarque :** Même si plusieurs utilisateurs d'un serveur de terminaux peuvent utiliser simultanément un même disque virtuel sécurisé, il est possible que ce disque soit associé à une lettre de lecteur différente à chaque session du serveur de terminaux selon la configuration du poste client et de la session. Par exemple, le disque virtuel sécurisé partagé dans cet exemple peut correspondre au lecteur D sur le premier poste et au lecteur E sur le second.

## 5.4 Sauvegardes chiffrées

SafeGuard PrivateDisk peut être utilisé pour les sauvegardes chiffrées.

Vous pouvez effectuer cette opération en copiant les fichiers à sauvegarder sur un disque chiffré virtuel, puis en enregistrant le fichier volume du disque virtuel sur le support de sauvegarde.

Lorsque des fichiers volume de disque virtuel sont en cours d'utilisation sur des réseaux, une sauvegarde des serveurs de réseau inclut automatiquement le contenu des disques virtuels chiffrés.

Avantages liés à l'utilisation de SafeGuard PrivateDisk :

- Les données confidentielles sont sauvegardées sur supports de sauvegarde.
- L'administrateur des sauvegardes n'a pas accès aux données confidentielles.

## 5.5 Changement rapide d'utilisateur

SafeGuard PrivateDisk prend en charge la technologie " Changement rapide d'utilisateur " de Windows XP. Puisque la fonction de changement rapide d'utilisateur de Windows XP repose sur la technologie de serveur de terminaux, l'utilisation de SafeGuard PrivateDisk avec le changement rapide d'utilisateur sous Windows XP est comparable à l'utilisation du logiciel sur un serveur de terminaux. Ceci offre un surcroît de souplesse lorsque plusieurs utilisateurs utilisent simultanément des fichiers et des ordinateurs.

Avantages liés à l'utilisation de SafeGuard PrivateDisk :

- Les disques chiffrés virtuels ne sont visibles et accessibles qu'aux utilisateurs autorisés ; par exemple, si un disque virtuel est ouvert par un utilisateur, il n'est pas visible par les autres utilisateurs.
- Les disques virtuels d'un utilisateur restent ouverts pendant que l'ordinateur est utilisé par un autre utilisateur, mais ne sont pas lisibles par ce dernier. Ceci permet aux applications de continuer à accéder aux données chiffrées en arrière-plan.

## 6 Administration centralisée

### 6.1 Configuration du produit et stratégie

La version Enterprise Edition de SafeGuard PrivateDisk est livrée avec un modèle d'administration (sguard.adm) qui peut servir à créer des fichiers de stratégie (si Active Directory n'est pas disponible ou des objets de stratégie de groupe (pour Active Directory). dans le cadre de la configuration d'un utilisateur ou d'un ordinateur . Le modèle d'administration sguard.adm se trouve dans le sous-répertoire ADM du répertoire d'installation. Ce modèle contient tous les paramètres nécessaires pour configurer SafeGuard PrivateDisk. Il permet également de définir les listes des disques virtuels disponibles pour les utilisateurs et de créer un disque virtuel initial lors de la première ouverture d'une session.

Les politiques spécifiées par l'administrateur sont déployées automatiquement par le système d'exploitation à chaque connexion de l'utilisateur au serveur de domaine ou par Active Directory.

Comme les utilisateurs ne disposent généralement pas des droits administrateurs système), ils ne peuvent pas modifier les paramètres du produit.

#### 6.1.1 Modèle d'administration sguard.adm

Pour utiliser le modèle d'administration de SafeGuard PrivateDisk, ouvrez l'éditeur de stratégie de groupe et ajoutez le modèle d'administration.

Le système affiche ensuite un nœud *SafeGuard* pour la configuration de l'ordinateur et de l'utilisateur contenant un sous-répertoire SafeGuard PrivateDisk.

Les paramètres de configuration de l'ordinateur dans le modèle d'administration sont presque identiques à ceux de la boîte de dialogue *Options* de l'application SafeGuard PrivateDisk, à l'exception des restrictions portant sur les mots de passe :

**Remarque :** Pour obtenir la description des paramètres non détaillés dans ce chapitre, reportez-vous à la boîte de dialogue Propriétés appropriée du modèle d'administration.

##### Éditeur de stratégie système

SafeGuard PrivateDisk

##### Éditeur de stratégie de groupe (Active Directory)

Computer Configuration\  
Administrative Templates\  
SafeGuard\  
PrivateDisk

■ **Généralités**

- Connexion automatique aux disques virtuels
- Démontage automatique des disques virtuels inactifs
- CSP de préférence

En utilisant des certificats pour l'authentification vous pouvez spécifier votre fournisseur de services cryptographiques (CSP) préféré, par exemple un CSP de carte à puce spécifique. Le nom du CSP doit faire partie du nom du CSP dans la base de registres. Le nom convivial est utilisé pour présenter les messages à l'utilisateur et est en option.

■ **Connexion**

- Connexion unique

■ **Cartes à puce**

- Lecteur de carte à puce  
Attention ! Pour le nom du lecteur de carte à puce faites attention à la différence entre minuscule et majuscule !

■ **LDAP**

Dans cet onglet, vous pouvez définir les paramètres à utiliser pour la recherche d'un certificat via LDAP. Le système affiche ces paramètres sur la page LDAP, dans la boîte de dialogue Options, ainsi qu'au début de la recherche visant l'assignation d'un certificat. Il est impossible de modifier ces paramètres dans la boîte de dialogue Options (à moins que l'utilisateur connecté ne détienne des droits d'administrateur), mais il est possible de les modifier au moment de l'assignation du certificat.

- **Hôte**  
Dans le champ Hôte, entrez le nom de domaine ou l'adresse IP du serveur LDAP.
- **Port**  
Dans le champ Port, entrez le port TCP à utiliser pour établir la connexion. Si vous ne renseignez pas ce champ, le port 389 sera utilisé par défaut.
- **Version de protocole**  
Sélectionnez ici la version du protocole à utiliser dans la liste. La version par défaut est 3.
- **Anonyme**  
Si cette option est sélectionnée, le système essaiera d'établir une connexion anonyme avec le serveur.  
Si vous ne souhaitez pas établir une connexion anonyme, saisissez les données d'accès valides pour le serveur LDAP au moment de la connexion.
- **Authentification**  
Vous pouvez définir ici le type requis d'authentification auprès du serveur LDAP. Le paramètre par défaut est GSS (Generic Security Services).

Les paramètres ci-dessous influent sur la recherche dans la structure LDAP.

- **Base**

Vous pouvez définir ci le nœud dans la structure LDAP à partir duquel le système recherche le certificat. Cela vous permet de limiter la recherche à une partie de l'arborescence afin de trouver les certificats plus rapidement (par exemple : recherche limitée à une unité organisationnelle (OU) particulière).

Vous devez spécifier le nœud à partir duquel le système lancera la recherche.

- **Filtre**

Dans le champ de saisie Filtre, vous pouvez définir un filtre de recherche pour un certificat. Lorsque l'utilisateur assigne le certificat, seuls les filtres correspondant au filtre sont affichés. Ce peut être, par exemple, un moyen de rechercher le Common Name ou une adresse de messagerie dans un certificat donné.

**Syntaxe du filtre :**

Un filtre comprend une description (nom du filtre), la définition en cours du filtre (établissant les critères de recherche, par exemple : "cn=") et une liste de paramètres en option. Dans la partie variable de la définition du filtre, entrez "%s" (par exemple : "cn=%s"). La recherche interroge ce paramètre %s. L'utilisateur est invité à saisir les informations appropriées. Dans le filtre, le système remplace le paramètre par la valeur saisie par l'utilisateur.

Dans la liste des paramètres, vous pouvez attribuer un nom à chaque paramètre fictif dans la définition du filtre. Le système affiche le nom du paramètre lorsqu'il invite l'utilisateur à saisir sa valeur afin qu'il puisse voir le type d'informations qu'on lui demande d'entrer.

Lorsque vous saisissez les noms des paramètres, séparez les noms par une virgule.

Entrez le nom du filtre, la définition du filtre et la liste de paramètres entre guillemets et séparez-les par une virgule.

Lorsque vous saisissez plusieurs filtres, séparez-les par un tiret.

Lorsque l'utilisateur assigne un certificat, il peut sélectionner le filtre à utiliser dans la liste des noms de filtres.

**Exemple :**

"Recherche messagerie","mail=%s","Adresse de messagerie".

Si le filtre "Recherche messagerie" est sélectionné pour la recherche d'un certificat, l'utilisateur est invité à saisir l'adresse de messagerie de l'utilisateur recherché (le système affiche l'adresse de messagerie dans la boîte de dialogue). Le système affiche tous les certificats contenant l'adresse de messagerie correspondante.

**Remarque :** L'utilisateur doit saisir les informations requises telles qu'elles sont contenues dans le certificat. L'adresse de messagerie est utile du fait qu'elle est généralement connue et employée par l'utilisateur. Toutefois, dans le cas où cn=%s serait utilisé, par exemple, l'utilisateur doit connaître précisément comment Common Name a été saisi dans le certificat.

- **Attribut**

Vous devez saisir ici l'attribut utilisé pour enregistrer chaque certificat de l'utilisateur dans le service de l'annuaire. Il s'agit généralement de l'attribut LDAP `usercertificates`. L'attribut par défaut est `usercertificates`. Vous ne pouvez définir qu'un seul attribut.
- **Limite de temps**

Limite de temps de recherche exprimée en secondes. La valeur 0 correspond à "aucune limite". Par exemple : 30.
- **Limite de quantité**

Nombre maximal de certificats trouvés que le système affiche et qu'il est donc possible d'assigner. La valeur 0 correspond à "aucune limite". Par exemple : 10.
- **Restrictions des mots de passe**
  - **Longueur minimale**

Vous pouvez définir ici la longueur minimale du mot de passe applicable au nouveau disque virtuel.  
Entrez la longueur minimale souhaitée (entre 1 et 32 caractères). La longueur par défaut est 4 caractères.
- **Vérification du certificat**
  - **Vérification avec la CRL**

Si cette fonction est activée, les certificats seront acceptés après un contrôle complet du chemin de certification. Nota bene : Si nécessaire, la liste de révocation des certificats ( CRL) sera téléchargée depuis l'autorité de certification.
  - **Autoriser les certificats avec des extensions critiques inconnues**

Sélectionnez cette option pour autoriser les certificats même s'ils contiennent une extension critique que le logiciel SafeGuard PrivateDisk ne connaît pas. Vous pourrez ensuite assigner des certificats de ce type.
  - **Autoriser les signatures de certificats**

Sélectionnez cette option pour autoriser les certificats utilisés comme "Signature".

La stratégie applicable à l'utilisateur comporte les entrées suivantes :

```
Configuration utilisateur\  
Modèles d'administration\  
SafeGuard\  
PrivateDisk
```

## ■ Droits utilisateur

- Création de disque  
La création de disques virtuels sur la machine doit être permise de manière explicite. Sélectionnez cette option pour permettre à l'utilisateur de créer ses propres disques virtuels chiffrés.
- Icône de la barre d'état système  
Si cette option est désactivée, l'icône de SafeGuard PrivateDisk ne sera pas présente dans la barre de tâches.

## ■ Les disques virtuels

- Disque virtuel obligatoire  
Il est possible de forcer l'assignation d'un disque virtuel à un utilisateur. Les paramètres de tels disques ne peuvent pas être modifiés par l'utilisateur et ne peuvent pas être enlevés de la liste des disques disponibles. De cette façon, des disques virtuels spécifiques seront toujours disponibles pour certains utilisateurs.

Cette entrée comporte le format suivant:

```
<fichier volume>|<nom>|<lettre>|<options>
```

Si la prochaine lettre inutilisée de l'unité de disque doit être utilisée automatiquement lors du montage du disque (voir paramétrage **Automatique**),

<lettre> doit être laissé en blanc.

Exemple: c:\mandatory001.vol|MandatoryDisk||L)

Options de démarrage (une seule est possible)

L ... Le disque virtuel est monté après l'ouverture de session

P ... Le disque virtuel est monté lorsque le périphérique est disponible (plug and play)

C ... Le disque virtuel est monté lorsqu'une carte à puce est insérée

Options additionnelles :

R ... Montage en lecture seule

S ... Simulation disque dur

Exemple:

```
c:\mandatory001.vol|MandatoryDisk|Z|LR
```

Le fichier mandatory001.vol qui se trouve sur l'unité C correspond au disque virtuel MandatoryDisk. Il s'agit d'un disque virtuel obligatoire. La lettre z est assignée à ce disque virtuel. Le disque est monté lors de l'ouverture de session (L) et est monté pour un accès en lecture seule (R).

Pour la création automatique d'un disque virtuel par l'utilisateur, voir **disque virtuel initial**.

**Remarque :** Si un disque virtuel chiffré est imposé par cette entrée et qu'il n'existe pas encore, il apparaît néanmoins dans la liste des disques disponibles. S'il est créé par la suite, il peut être utilisé comme prévu.

- **Certificat de récupération**

Vous pouvez saisir ici un numéro de série d'un certificat administrateur qui sera assigné automatiquement aux disques virtuels créés par les utilisateurs. Vous avez ainsi la certitude de pouvoir accéder constamment à chaque disque virtuel.

Le numéro de série doit être entré en code hexadécimal.

**Remarque :** La protection des données peut être assurée en gardant la clé privée du certificat Administrateur dans un lieu sécurisé (par exemple sur une carte à puce ou une disquette dans un coffre).

- **Disque virtuel initial**

- **Disque virtuel initial**

Un disque virtuel initial sera créé automatiquement lors de la première ouverture de session si ce disque n'existe pas.

- **Ajouter le certificat de l'utilisateur**

Si cette entrée est activée, le certificat de l'utilisateur est ajouté au disque virtuel créé automatiquement. Par défaut, cette option est désactivée.

**Remarque :** Lors de la création d'un disque virtuel sur l'ordinateur de l'utilisateur, un certificat est ajouté si la clé privée est disponible ! Si plus d'un certificat est disponible, une boîte de dialogue apparaît dans laquelle l'utilisateur pourra choisir un certificat.

- **LDAP**

- **Filtre utilisé**

Vous pouvez ici définir seulement quel filtre de recherche sera proposé par défaut à l'utilisateur s'il recherche un certificat via LDAP. Dans le champ de saisie, vous devez entrer le nom du filtre tel qu'il apparaît dans Configuration Ordinateur.

Vous pouvez choisir uniquement un filtre défini dans Configuration Ordinateur

## 7 L'interface d'automation OLE de SafeGuard PrivateDisk

SafeGuard PrivateDisk exporte un serveur OLE (pdole.exe) qui peut être utilisé pour développer des applications avec des scripts. Cela comprend le Windows Scripting Host (supportant le script de Visual Basic, JavaScript, Perl... ) tout comme les applications MS Office, les pages Web et les environnements de programmation comme Visual Basic, Visual C et beaucoup d'autres...

La classe d'objet COM exportée est appelée PrivateDisk.Application. Pour garantir la compatibilité des scripts, elle exporte une interface IDispatch dotée des propriétés et commandes suivantes.

### 7.1 Propriétés

Le changement des propriétés d'un objet OLE PrivateDisk n'affecte que les opérations ultérieures portant sur cet objet et non l'ensemble des objets.

|               |   |
|---------------|---|
| NoGui Booléen | Cette option doit être fixée à <i>True</i> si aucune boîte de dialogue ou aucun message ne doivent apparaître. Par défaut, cette option est fixée à <i>False</i> , ayant comme conséquence de prompter l'utilisateur pour demander les mots de passe et de faire apparaître des messages d'erreur. Si cette propriété "NoGui" est fixée à <i>True</i> mais qu'une interaction avec l'utilisateur est exigée (par exemple l'entrée d'un mot de passe), toute l'opération est annulée et un code d'erreur approprié est retourné. |
|---------------|---|

## 7.2 Commandes

Voici la liste des commandes pouvant être appelées pour l'objet PrivateDisk.Application. Les paramètres entre parenthèses sont facultatifs. Retrouvez ci-dessous les descriptions des paramètres individuels :

|   |   |
|---|---|
| NewDisk volume, size,<br>(path), (fileSYS),<br>(admpwd), (usrpwd) | Création d'un nouveau disque virtuel. Le disque est monté automatiquement après sa création. Retourne <i>True</i> en cas de succès, <i>False</i> autrement.   |
| MountDisk volume,<br>(pwd), (pwdtype),<br>(readonly)              | Permet de monter un disque virtuel identifié par le fichier correspondant au disque. Le disque virtuel doit déjà être dans la liste des disques de l'utilisateur. Si <i>readonly</i> est fixée à <i>True</i> , le disque virtuel est monté avec un accès en lecture seule. Retourne <i>True</i> en cas de succès, <i>False</i> autrement. |
| ImportDisk volume,<br>(path)                                      | Ajoute un disque virtuel dans la liste de l'utilisateur. Retourne <i>True</i> en cas de succès, <i>False</i> autrement .  |
| UnmountDisk volume<br>(forced)                                    | Démonte un disque virtuel. Si <i>forced</i> est fixée à <i>True</i> , le disque virtuel est démonté même si des applications tournent encore sur le disque. Retourne <i>True</i> en cas de succès, <i>False</i> autrement.  |
| UnmountAllDisks<br>(forced)                                       | Démonte tous les disques actuels déjà montés. Si <i>forced</i> est fixée à <i>True</i> , le disque virtuel est démonté même si des applications tournent encore sur le disque. Retourne <i>True</i> en cas de succès, <i>False</i> autrement.   |
| GetDiskInfo volume,<br>(path), (mounted),<br>(readonly)           | Donne l'état d'un disque virtuel. Seul le paramètre <volume> est utilisé comme information. Toutes les autres valeurs sont des valeurs de sortie renseignées par cette fonction si celle-ci est activée. Retourne <i>True</i> en cas de succès, <i>False</i> autrement.   |
| GetErrorText  | En cas d'erreur, cette fonction peut être appelée pour retourner le message correspondant au code erreur.   |

## 7.2.1 Paramètres

|            |  |
|------------|--|
| volume     | Les disques virtuels sont identifiés par leurs noms de fichier xxxx.vol<br>Le nom symbolique du disque virtuel ne peut pas être utilisé étant donné qu'il n'est pas unique (car personnalisable sur chaque poste).   |
| size       | La taille d'un disque virtuel est exprimée en ko. La valeur est ajustée au prochain multiple de 4 ko, qui est la taille d'un cluster utilisée par SafeGuard PrivateDisk.   |
| path       | Spécifie la lettre associée au disque virtuel. Pour les lettres d'unité de disque, veuillez spécifier une lettre de type "X" or "X:". Pour que le choix soit automatique, laissez ce paramètre à vide.   |
| filesystem | Identifie le système de fichiers du nouveau disque virtuel. Les valeurs possibles sont "FAT" et "NTFS". La valeur par défaut est "FAT".  |
| usrpwd     | Spécifie le mot de passe utilisateur pour un nouveau disque virtuel.   |
| admpwd     | Spécifie le mot de passe administrateur pour un nouveau disque virtuel. Si le paramètre est vide, le mot de passe est demandé lors de la création du disque virtuel.   |
| pwd        | Correspond au mot de passe pour s'identifier au disque virtuel (mot de passe utilisateur ou administrateur ou code PIN pour un CSP - voir le paramètre <pwdtype> plus bas. Si ce paramètre est vide, l'identification à un disque virtuel est faite par le biais de certificats. En cas de nécessité, on demande le mot de passe à l'utilisateur.  |
| pwdtype    | Cette valeur permet de spécifier le type de mot de passe utilisé lors du montage du disque. Elle est utilisée lorsque le paramètre <pwd> est non vide.<br>Valeurs possibles :<br>0 (ou vide) ... le paramètre <pwd> correspond au mot de passe administrateur<br>1 ... le paramètre <pwd> correspond au mot de passe utilisateur<br>2 ... le paramètre <pwd> correspond au code PIN pour une identification par certificat |
| mounted    | Cette valeur est fixée à <i>True</i> si le disque est monté; <i>False</i> autrement.   |
| readonly   | Cette valeur est fixée à <i>True</i> si le disque est monté pour un accès en lecture seule, <i>False</i> autrement (pour un accès en lecture/écriture).  |

## 7.3 Exemple de Script

Un exemple de script en visual basic (`demo.vbs`) se trouve dans le répertoire d'installation de SafeGuard PrivateDisk. Utilisez ce script à des fins de démonstration.

---

## 8 Support technique

Vous pouvez obtenir du support technique pour les produits Sophos de l'une des manières suivantes :

- Visitez le forum SophosTalk à l'adresse <http://community.sophos.com/> et recherchez d'autres utilisateurs qui connaissent le même problème.
- Visitez la base de connaissances du support technique de Sophos à l'adresse <http://www.sophos.fr/support/>
- Téléchargez la documentation des produits à l'adresse <http://www.sophos.fr/support/docs/>
- Envoyez un courriel à [support@sophos.com](mailto:support@sophos.com), y compris le(s) numéro(s) de version du ou des logiciels Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tout message d'erreur.

---

## 9 Mentions légales

Copyright © 2000 - 2011 Sophos Group. Tous droits réservés. SafeGuard est une marque déposée de Sophos Group.

Sophos est une marque déposée de Sophos Limited, Sophos Group ou de Utimaco Safeware AG. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Vous trouverez des informations de copyright des fournisseurs tiers dans le fichier Disclaimer and Copyright for 3rd Party Software.rtf de votre répertoire d'installation.