

SOPHOS

Sophos SafeGuard Disk Encryption Aide utilisateur pour Mac

Date du document : janvier 2011



Table des matières

1	À propos de Sophos SafeGuard Disk Encryption pour Mac.....	3
2	Menu système de Sophos SafeGuard Disk Encryption.....	4
3	Authentification au démarrage.....	5
4	Gestion des utilisateurs.....	8
5	Gestion des disques.....	11
6	Utilisation de Sophos SafeGuard Disk Encryption via le Terminal.....	13
7	Sauvegardes Time Machine.....	20
8	Matériels et configurations pris en charge.....	21
9	Matériels, configurations et opérations non pris en charge.....	23
10	Support technique.....	25
11	Copyright.....	26

1 À propos de Sophos SafeGuard Disk Encryption pour Mac

Sophos SafeGuard Disk Encryption pour Mac est un logiciel qui contient l'authentification au démarrage pour votre Mac et chiffre les disques durs ou les partitions de votre Mac.

Grâce à l'**Authentification au démarrage (POA, Power-on Authentication)**, l'utilisateur s'authentifie pendant la phase de préinitialisation, c'est-à-dire avant le démarrage du système d'exploitation. Une fois que l'utilisateur a été correctement authentifié dans l'authentification au démarrage, le système d'exploitation démarre et l'utilisateur est connecté automatiquement à OS X si la connexion automatique est configurée sur le système.

Sophos SafeGuard Disk Encryption chiffre les données présentes sur un Mac d'après les partitions. L'administrateur SafeGuard définit les disques durs ou les partitions à chiffrer. L'utilisateur SafeGuard n'est pas autorisé à changer ces paramètres.

Les fichiers présents sur une partition chiffrée sont chiffrés de manière transparente. Vous ne serez pas invité à chiffrer ou à déchiffrer les fichiers lors de leur ouverture, modification ou enregistrement. Lorsque vous ouvrez les fichiers, ils sont déchiffrés et vous pouvez les modifier. Ils sont rechiffrés à la fermeture ou à l'enregistrement.

Remarque :

Une fois que Sophos SafeGuard Disk Encryption pour Mac a été installé, la partition système sur laquelle le produit est installé reçoit une nouvelle icône (l'icône de disque avec le bouclier SafeGuard). Cette icône indique seulement que SafeGuard est installé, cette partition n'est pas chiffrée. Les partitions de données obtiennent cette icône lorsqu'elles ont été chiffrées.

2 Menu système de Sophos SafeGuard Disk Encryption

Le menu système de Sophos SafeGuard Disk Encryption est représenté par une icône à droite de la barre de menus. Ce menu vous permet d'accéder rapidement aux fonctions de Sophos SafeGuard Disk Encryption et indique l'état de Sophos SafeGuard Disk Encryption.

Le menu système de Sophos SafeGuard Disk Encryption contient les options de menu suivantes :

- **À propos de SafeGuard** : informations à propos de Sophos SafeGuard Disk Encryption, incluant la version et les informations de copyright.
- **Gestion des disques** : ouvre la gestion des disques. Seuls les administrateurs SafeGuard sont autorisés à changer les paramètres de gestion des disques. Les utilisateurs SafeGuard sont uniquement autorisés à consulter ces paramètres.
- **Gestion des utilisateurs** : ouvre la gestion des utilisateurs. Seuls les administrateurs SafeGuard sont autorisés à changer les paramètres de gestion des utilisateurs. Les utilisateurs SafeGuard sont uniquement autorisés à consulter ces paramètres.
- **Informations d'état** : en cas d'exécution du chiffrement/déchiffrement, les informations d'état incluent le nom de la partition et la progression du chiffrement/déchiffrement.

3 Authentification au démarrage

L'**authentification au démarrage (POA ou Power-on Authentication)** demande à l'utilisateur de s'authentifier pendant la phase de préinitialisation, à savoir avant le démarrage du système d'exploitation. Dès que l'utilisateur a été correctement authentifié dans l'authentification au démarrage, le système d'exploitation démarre et l'utilisateur est connecté automatiquement à OS X si la connexion automatique est configurée.

En l'absence d'utilisateur SafeGuard, l'authentification au démarrage affiche seulement le logo "Sécurisé par SOPHOS" et continue le redémarrage du système d'exploitation après environ une seconde.

Si les utilisateurs SafeGuard sont présents, l'écran d'authentification apparaît. L'authentification au démarrage est toujours activée, qu'il y ait des partitions chiffrées ou non.

Connexion à l'authentification au démarrage

L'authentification au démarrage s'effectue à l'aide des codes d'accès utilisateur Sophos SafeGuard Disk Encryption. Ces codes d'accès doivent être fournis par un administrateur système ou par la personne qui a installé et/ou configuré Sophos SafeGuard Disk Encryption sur votre Mac.

L'authentification s'effectue en saisissant le nom utilisateur et le mot de passe SafeGuard dans les champs de modification.

Si le compte utilisateur Sophos SafeGuard Disk Encryption est accepté, la connexion au système d'exploitation s'effectue automatiquement, si elle est configurée.

3.1 Résolution des problèmes à l'authentification au démarrage

Sophos SafeGuard Disk Encryption propose des options de résolution des problèmes à l'authentification au démarrage :

- Récupération
- Déchiffrement permanent de la partition
- Affichage du journal

Ces options vous assistent en cas de problèmes tels qu'une installation endommagée de Sophos SafeGuard Disk Encryption est endommagée, le non démarrage du système d'exploitation, etc.

La sélection de **Résolution des problèmes** dans la boîte de dialogue d'authentification ouvre un menu avec les options de résolution des problèmes.

3.1.1 Récupération

Outre la récupération de mots de passe oubliés de comptes utilisateur, Sophos SafeGuard Disk Encryption comporte d'autres options de récupération pour faire en sorte que même les systèmes endommagés puissent être récupérés facilement.

Une condition préalable à toute action de récupération exige que les données du noyau et d'authentification soient exportées immédiatement après l'installation du logiciel et la création d'utilisateurs.

Remarque :

Avec les données d'authentification des utilisateurs, exportez ces données à chaque fois que vous ajoutez des utilisateurs ou que vous modifiez leurs codes d'accès afin de conserver vos sauvegardes à jour. Au cas où vous avez mis à jour le logiciel Sophos SafeGuard Disk Encryption sur votre Mac, il est aussi nécessaire d'exporter de nouveau le noyau.

Création de supports de récupération

Pour exporter les données de récupération :

1. Choisissez l'icône Sophos SafeGuard Disk Encryption et cliquez sur **Gestion des utilisateurs**.
2. Saisissez vos codes d'accès SafeGuard (admin, utilisateur, récupération) et cliquez sur **OK**.
3. Le menu **Action** (semblable à un engrenage) contient trois options :

Création de supports de récupération autonomes

Choisissez **Créer un support de récupération autonome...** si vous voulez créer des supports de récupération universels pour vos Macs. Ce support vous permet de récupérer chaque machine à condition que leurs données d'authentification soient OK.

Pour créer le support, cliquez sur **Créer un support de récupération autonome...** Dans la boîte de dialogue qui apparaît, choisissez l'emplacement désiré, laissez l'option **Enregistrer sur l'image disque** cochée et cliquez sur **Créer un support de récupération autonome...**

Remarque :

Quel que soit l'emplacement de stockage que vous avez choisi (déjà sur une clé USB ou temporairement sur le disque dur de votre Mac), vous devez "restaurer" l'image disque sur la racine de la clé USB à l'aide de l'Utilitaire de disque de votre Mac. Ainsi, vous garantissez un fonctionnement correct du support de récupération.

Exportation des données d'authentification

Choisissez **Exporter les données d'authentification** pour sauvegarder tous vos codes d'accès utilisateur. Stockez-les dans un endroit sûr et accessible en cas d'urgence.

Création d'un support de récupération autonome

Choisissez **Créer un support de récupération spécifique** si vous êtes un utilisateur autonome et souhaitez créer un package de récupération contenant toutes les données nécessaires en cas d'urgence. La procédure est identique à la création d'un support de récupération autonome.

Ces actions de récupération peuvent toutes être lancées à l'authentification au démarrage.

Procédure de récupération

En général, la récupération peut être nécessaire pour deux raisons :

- Données d'authentification corrompues. Un message apparaît à l'authentification au démarrage ou à partir du système d'exploitation.
- Problèmes de noyau qui peuvent, par exemple, engendrer des secteurs endommagés sur votre disque dur.

Données d'authentification corrompues

1. Connectez une clé USB contenant les données d'authentification exportées et démarrez votre Mac.

À l'authentification au démarrage, choisissez **Résolution des problèmes** et sélectionnez **Récupérer** dans le menu **Résolution des problèmes**.

Sophos SafeGuard Disk Encryption recherche les données d'authentification et de clé (qui résident en général dans le répertoire racine) sur tous les périphériques amovibles connectés.

2. Si elles sont trouvées, confirmez si vous voulez récupérer les données d'authentification. Après cela, les données d'authentification locales sont remplacées par celles provenant de la clé USB.
3. Après avoir confirmé la récupération réussie, retournez à l'authentification au démarrage et connectez-vous comme d'habitude.

Récupération du noyau

Dans ce cas, lancez l'authentification au démarrage depuis votre support de récupération.

1. Connectez votre support de récupération et démarrez votre Mac depuis ce support.
2. Lorsque le symbole du disque dur avec une croix blanche sur un fond vert apparaît, cliquez dessus.
3. L'authentification au démarrage lancée depuis le support de récupération apparaît.
4. Choisissez **Résolution des problèmes** et sélectionnez l'option **Récupérer** dans le menu **Résolution des problèmes**.
5. Sélectionnez l'option **Partition du noyau** dans le menu **Récupération**. Sélectionner **Données d'authentification** revient à exécuter l'opération décrite sous **Données d'authentification corrompues**.
6. Après avoir confirmé la récupération réussie, retournez à l'authentification au démarrage et connectez-vous comme d'habitude.

3.1.2 Déchiffrement permanent de la partition

Le déchiffrement permanent d'une partition peut être nécessaire, par exemple si le système d'exploitation ne peut plus être démarré et que vous avez besoin d'accéder aux données chiffrées. Ainsi, il est possible de déchiffrer des partitions sans avoir à exécuter le système d'exploitation.

Cette option affiche une liste de toutes les partitions disponibles sur votre Mac.

Vous pouvez sélectionner une partition en appuyant sur la touche ESPACE. Autorisez le déchiffrement en saisissant les codes d'accès admin de SafeGuard dans les champs modifiables.

La sélection de l'option **Déchiffrer** démarre le déchiffrement de la partition sélectionnée.

3.1.3 Affichage du journal

Le choix de cette option affiche le fichier journal, lequel peut vous aider à analyser les problèmes.

Il est possible d'exporter le contenu du journal dans un fichier présent sur une clé USB.

Pour ce faire, connectez une clé USB à votre Mac et sélectionnez **Exporter**. Le fichier journal sera automatiquement stocké dans le répertoire racine de la clé USB.

Remarque :

La clé USB doit avoir une partition FAT.

4 Gestion des utilisateurs

La gestion des utilisateurs de Sophos SafeGuard Disk Encryption est basée sur trois types d'utilisateurs différents.

- Type : **Administrateur**
- Type : **Utilisateur**
- Type : **Récupération**

Ces rôles ne sont pas liés aux comptes système et reflètent un type d'"utilisateur SafeGuard cryptographique".

4.1 Utilisateur admin

L'utilisateur admin est le seul rôle qui peut servir à :

- **Ajouter** des utilisateurs de tout type
- **Supprimer** des utilisateurs de tout type
- **Changer** l'état de chiffrement des partitions

Il doit toujours y avoir un utilisateur admin. Le premier utilisateur créé doit toujours être un utilisateur admin. Ceci est appliqué par la gestion d'utilisateurs SafeGuard et est la condition préalable requise pour toutes les tâches d'administration. Lorsque les utilisateurs sont supprimés, il est impossible de supprimer le dernier utilisateur admin, si plusieurs d'entre-eux ont été créés.

Création du premier utilisateur admin Sophos SafeGuard Disk Encryption

1. Choisissez l'icône Sophos SafeGuard Disk Encryption et cliquez sur **Gestion des utilisateurs**.
2. Saisissez un nom d'utilisateur admin.
3. Saisissez le mot de passe dans les champs **Mot de passe** et **Confirmer le mot de passe**. Sophos SafeGuard Disk Encryption accepte uniquement les mots de passe avec huit caractères ou plus (jusqu'à 127). La sélection de l'option **Afficher le mot de passe** rend le mot de passe saisi visible.
4. Cliquez sur **OK**.

4.2 Utilisateur

Le type **Utilisateur** reflète un utilisateur normal. Les utilisateurs de ce type ne sont pas autorisés à créer/supprimer tout autre utilisateur ou à gérer des disques, mais ils sont autorisés à consulter les paramètres courants sur leurs Mac. Ils sont autorisés à s'authentifier à l'authentification au démarrage.

Création d'un utilisateur SafeGuard

Pour la création d'un utilisateur SafeGuard, vous devez connaître les codes d'accès admin SafeGuard.

1. Choisissez l'icône Sophos SafeGuard Disk Encryption et cliquez sur **Gestion des utilisateurs**.

2. Saisissez vos codes d'accès SafeGuard (admin, utilisateur, récupération) et cliquez sur **OK**.
3. Choisissez **Utilisateurs** dans le volet de gestion.
4. Cliquez sur le bouton **Ajouter** (+) au-dessous de la liste de comptes utilisateur.
5. Choisissez **Utilisateur** dans le menu contextuel **Ajouter un utilisateur**.
6. Saisissez un nom d'utilisateur SafeGuard.
7. Saisissez le mot de passe utilisateur dans les champs **Mot de passe** et **Confirmer le mot de passe**. Sophos SafeGuard Disk Encryption accepte seulement un mot de passe avec huit caractères ou plus (jusqu'à 127). La sélection de l'option **Afficher le mot de passe** rend le mot de passe saisi visible.
8. Saisissez les codes d'accès admin dans les champs **Nom admin** et **Mot de passe admin**.
9. Cliquez sur **OK**.

Le nouvel utilisateur SafeGuard apparaît maintenant dans la liste des comptes et ces codes d'accès lui servent désormais à s'authentifier au démarrage.

4.3 Utilisateur de récupération

L'utilisateur de récupération sert à récupérer le mot de passe oublié d'un utilisateur SafeGuard existant. L'utilisateur de récupération ne peut pas être utilisé pour récupérer un utilisateur admin ou différents utilisateurs de récupération.

Il peut être assimilé à l'utilisateur d'une opération. Chaque utilisateur de récupération est lié à un utilisateur SafeGuard spécifique. Ce qui signifie qu'un utilisateur de récupération peut seulement récupérer un utilisateur SafeGuard spécifique. Si l'utilisateur SafeGuard est supprimé, ses utilisateurs de récupération sont aussi supprimés.

Les utilisateurs de récupération sont autorisés à s'authentifier lors de l'authentification au démarrage mais seront supprimés s'ils sont utilisés pour récupérer le mot de passe d'un utilisateur SafeGuard.

Remarque :

Nous vous conseillons de créer plusieurs utilisateurs de récupération pour chaque utilisateur SafeGuard afin de garantir en permanence la disponibilité d'un utilisateur de récupération en cas d'oubli de mot de passe par l'utilisateur.

Création d'un utilisateur de récupération

Pour la création d'un utilisateur de récupération SafeGuard, vous devez connaître les codes d'accès admin SafeGuard.

1. Choisissez l'icône Sophos SafeGuard Disk Encryption et cliquez sur **Gestion des utilisateurs**.
2. Saisissez vos codes d'accès SafeGuard (admin, utilisateur, récupération) et cliquez sur **OK**.
3. Choisissez **Utilisateurs** dans le volet de gestion.
4. Cliquez sur le bouton **Ajouter** (+) au-dessous de la liste de comptes utilisateur.
5. Choisissez **Récupération** dans le menu contextuel **Ajouter un utilisateur**.
6. Sélectionnez un utilisateur SafeGuard existant dans le menu contextuel. L'utilisateur de récupération sert uniquement à récupérer le mot de passe de cet utilisateur donné.
7. Saisissez un nom d'utilisateur de récupération.
8. Saisissez le mot de passe de l'utilisateur de récupération dans les champs **Mot de passe** et **Confirmer le mot de passe**. Sophos SafeGuard Disk Encryption accepte uniquement des

mots de passe avec huit caractères ou plus. La sélection de l'option **Afficher le mot de passe** rend le mot de passe saisi visible.

9. Saisissez les codes d'accès admin dans les champs **Nom admin** et **Mot de passe admin**.
10. Cliquez sur **OK**.

Le nouvel utilisateur de récupération apparaît maintenant dans la liste des comptes. Cet utilisateur de récupération peut maintenant être utilisé à l'authentification au démarrage et pour la récupération du mot de passe oublié d'un utilisateur.

Récupération du mot de passe oublié d'un utilisateur SafeGuard

1. Connectez-vous à l'authentification au démarrage à l'aide de vos codes d'accès admin SafeGuard ou utilisez les codes d'accès de l'utilisateur de récupération correspondant.

Choisissez l'icône Sophos SafeGuard Disk Encryption et cliquez sur **Gestion des utilisateurs**.

2. Saisissez vos codes d'accès SafeGuard (admin, utilisateur, récupération) et cliquez sur **OK**.
3. Choisissez **Utilisateurs** dans le volet de gestion.
4. Choisissez **Récupérer un utilisateur** à droite du compte utilisateur SafeGuard pour lequel vous voulez récupérer le mot de passe.
5. Saisissez un nouveau mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**.
6. Saisissez le nom et le mot de passe de l'utilisateur de récupération dans les champs **Nom de la récupération** et **Mot de passe de la récupération**.
7. Cliquez sur **OK**.

Le mot de passe de l'utilisateur SafeGuard est réinitialisé. Il peut maintenant être utilisé pour s'authentifier à l'authentification au démarrage.

Remarque : l'utilisateur de récupération est supprimé de la liste des comptes. Veillez à ce qu'il y ait toujours un utilisateur de récupération disponible pour chaque compte. Si nécessaire, créez-en un nouveau. Sans utilisateur de récupération, il est impossible de récupérer un mot de passe oublié.

5 Gestion des disques

Sophos SafeGuard Disk Encryption vous permet de chiffrer le disque dur ou des partitions de votre Mac. Chaque tâche de gestion de disque (chiffrement/déchiffrement/pause/reprise) nécessite une authentification en tant qu'admin SafeGuard.

Le menu système Sophos SafeGuard Disk Encryption à l'extrémité droite de la barre de menus affiche l'état des tâches de chiffrement/déchiffrement en cours d'exécution.

Chiffrement d'une partition

Avant de commencer à chiffrer une partition de données, assurez-vous que tous les fichiers présents sur cette partition sont fermés.

1. Choisissez l'icône Sophos SafeGuard Disk Encryption et cliquez sur **Gestion des disques**.
2. Saisissez vos codes d'accès admin SafeGuard et cliquez sur **OK**.
3. Choisissez **Partitions** dans le volet de gestion. Toutes les partitions disponibles sont affichées.
4. Cliquez sur **Chiffrer** juste à côté de la partition que vous voulez chiffrer.
5. Le chiffrement des partitions sélectionnées démarre immédiatement. Pour améliorer la vitesse de chiffrement, sélectionnez l'option **Mode rapide** en bas à gauche du volet **Gestion des disques**.

Vous pouvez continuer à travailler sur la partition de données au cours du processus de chiffrement.

Remarque :

Nous vous conseillons de ne pas installer de mises à jour et d'effectuer le chiffrement initial et le déchiffrement final d'une machine simultanément car les installations peuvent, dans ce cas, être très lentes.

L'opération de chiffrement/déchiffrement peut faire l'objet d'une pause en cliquant sur le bouton **Pause** à l'extrémité droite de la barre de progression. Pour reprendre le chiffrement, cliquez sur le bouton **Reprendre** qui apparaît lorsque le chiffrement a fait l'objet d'une pause. Pour ces deux actions, authentifiez-vous en tant qu'admin SafeGuard.

Les tâches de chiffrement/déchiffrement ayant fait l'objet d'une pause reprennent automatiquement après redémarrage de votre Mac.

Remarque :

Ne démarrez pas le chiffrement pour les partitions non montées et ne démontez pas de partition lors du chiffrement. Ces deux opérations peuvent entraîner une perte de données.

Déchiffrement d'une partition

Assurez-vous que tous les fichiers présents sur la partition de données à déchiffrer sont fermés pendant le déchiffrement.

1. Choisissez l'icône Sophos SafeGuard Disk Encryption et cliquez sur **Gestion des disques**.
2. Saisissez vos codes d'accès admin SafeGuard et cliquez sur **OK**.
3. Choisissez **Partitions** dans le volet de gestion. Toutes les partitions disponibles sont affichées.
4. Cliquez sur **Déchiffrer** juste à côté de la partition que vous voulez déchiffrer.
5. Le chiffrement de la partition sélectionnée démarre immédiatement.

Le déchiffrement de partitions est possible également à l'authentification au démarrage. Ceci peut être utile par exemple lorsque le système d'exploitation ne peut pas être lancé.

Le choix de **Résolution des problèmes > Déchiffrer la partition en permanence** vous permet de déchiffrer les partitions de votre Mac.

Remarque :

Ne démarrez pas le déchiffrement des partitions non montées et ne démontez pas de partition lors du déchiffrement. Ces deux opérations peuvent entraîner une perte de données.

6 Utilisation de Sophos SafeGuard Disk Encryption via le Terminal

Vous pouvez utiliser Sophos SafeGuard Disk Encryption via le Terminal, l'interface par lignes de commande Mac OS X.

Commandes

Les commandes suivantes sont disponibles via la ligne de commande "sgadmin" :

```
sgadmin --help | -h
```

```
sgadmin --status
```

```
sgadmin --add-user
  --type "user | admin"
  [--user "nom utilisateur"]
  [--password "mot de passe"]
  [--confirm-password "confirmer le mot de passe"]
  [--authenticate-user "nom utilisateur admin"]
  [--authenticate-password "mot de passe admin"]
```

```
sgadmin --add-recovery-user
  --user-to-recover "nom utilisateur"
  [--user "nom utilisateur"]
  [--password "mot de passe"]
  [--confirm-password "confirmer le mot de passe"]
  [--authenticate-user "nom utilisateur admin"]
  [--authenticate-password "mot de passe admin"]
```

```
sgadmin --add-recovery-users
  --user-to-recover "nom utilisateur"
  [--count "nombre d'utilisateurs"]
  [--authenticate-user "nom utilisateur admin"]
  [--authenticate-password "mot de passe admin"]
```

```
sgadmin --remove-user
  [--user "nom utilisateur"]
```

```
[--authenticate-user "nom utilisateur admin "]  
[--authenticate-password "mot de passe admin"]
```

```
sgadmin --list-users  
  [--authenticate-user "nom utilisateur"]  
  [--authenticate-password "mot de passe"]
```

```
sgadmin --change-password  
  [--user "nom utilisateur"]  
  [--old-password "ancien mot de passe"]  
  [--new-password "nouveau mot de passe"]  
  [--confirm-password "confirmer mot de passe"]
```

```
sgadmin --recover-password  
  [--user "nom utilisateur"]  
  [--new-password "nouveau mot de passe"]  
  [--confirm-password "confirmer mot de passe"]  
  [--recovery-user "nom utilisateur de récupération"]  
  [--recovery-password "mot de passe de récupération"]
```

```
sgadmin --backup-authentication  
  --target "/chemin/vers/dossier/cible"
```

```
sgadmin --backup-kernel  
  --target "/chemin/vers/dossier/cible"  
  [--include-authentication]  
  [--create-dmg]
```

```
sgadmin --encrypt "uuid | index | système | tous"  
  [--authenticate-user "nom utilisateur admin"]  
  [--authenticate-password "mot de passe admin"]
```

```
sgadmin --decrypt "uuid | index | système | tous"  
  [--authenticate-user "nom utilisateur admin"]  
  [--authenticate-password "mot de passe admin"]
```

```
sgadmin --pause "uuid | index | tous"
```

```
[--authenticate-user "nom utilisateur admin"]
[--authenticate-password "mot de passe admin"]
```

```
sgadmin --resume "uuid | index | tous"
[--authenticate-user "nom utilisateur admin"]
[--authenticate-password "mot de passe admin"]
```

```
sgadmin --enable-fast
```

```
sgadmin --disable-fast
```

```
sudo sgadmin --set-boot
```

Description des commandes

Le tableau suivant décrit toutes les commandes et options. Tout ce qui figure entre crochets "[...]" est facultatif. S'ils ne sont pas fournis par les options, les noms utilisateur et les mots de passe sont demandés de manière interactive. Les noms utilisateur sont saisis de manière "visible" et les mots de passe de manière "invisible".

Commande	Description
--help -h	Affiche le texte d'aide.
--status	Affiche des informations d'état. Les informations d'index affichées par <code>sgadmin --status</code> sont dynamiques. Ceci signifie qu'en fonction du nombre de partitions montées, les informations d'index peuvent varier.
--add-user	La commande "add-user" sert à ajouter un utilisateur à la machine. Le seul paramètre requis est "type". Le nom utilisateur et le mot de passe ainsi que l'utilisateur et le mot de passe d'authentification peuvent être transmis par des options ou seront demandés de manière interactive. Le premier utilisateur ajouté doit être un Admin. Lorsque le premier utilisateur est ajouté, il n'est pas nécessaire de spécifier <code>auth-user</code> et <code>auth-password</code> . Options : <ul style="list-style-type: none"> ■ --type : type d'utilisateur (Administrateur, Utilisateur) ■ --user : nom de l'utilisateur à ajouter

Commande	Description
	<ul style="list-style-type: none"> ■ --password : mot de passe de l'utilisateur à ajouter ■ --authenticate-user : utilisateur "Admin" requis pour l'authentification (s'il n'est pas le premier utilisateur) ■ --authenticate-password : mot de passe "Admin" requis pour l'authentification (s'il n'est pas le premier utilisateur)
--add-recovery-user	<p>Ajoute un utilisateur de récupération pour un utilisateur donné. Options :</p> <ul style="list-style-type: none"> ■ --user-to-recover : nom de l'utilisateur à récupérer ■ --recovery-user : nom de l'utilisateur de récupération à ajouter ■ --recovery-password : mot de passe de l'utilisateur à ajouter ■ --confirm-password : confirmer le mot de passe. ■ --authenticate-user : utilisateur "Admin" requis pour l'authentification ■ --authenticate-password : mot de passe "Admin" requis pour l'authentification
--add-recovery-users	<p>Le paramètre "count" donne le nombre d'utilisateurs de récupération à créer (nom utilisateur aléatoire et mot de passe aléatoire) et est signalé via "stdout". Options :</p> <ul style="list-style-type: none"> ■ --user-to-recover : nom de l'utilisateur à récupérer ■ --count : nombre d'utilisateurs ■ --authenticate-user : utilisateur "Admin" requis pour l'authentification ■ --authenticate-password : mot de passe "Admin" requis pour l'authentification
--remove-user	<p>Supprime un utilisateur. Options :</p> <ul style="list-style-type: none"> ■ --user : nom de l'utilisateur à supprimer ■ --authenticate-user : utilisateur "Admin" requis pour l'authentification ■ --authenticate-password : mot de passe "Admin" requis pour l'authentification

Commande	Description
--list-users	<p>Dresse la liste de tous les utilisateurs "SafeGuard" sur la machine. Options :</p> <ul style="list-style-type: none"> ■ --authenticate-user : tout utilisateur ayant accès à la machine ■ --authenticate-password : mot de passe de l'utilisateur
--change-password	<p>change le mot de passe d'un utilisateur. Options :</p> <ul style="list-style-type: none"> ■ --recover-password ■ --old-password : ancien mot de passe de l'utilisateur ■ --new-password : nouveau mot de passe de l'utilisateur ■ --confirm-password : confirmation du nouveau mot de passe
--recover-password	<p>Récupère le mot de passe d'un utilisateur. Options :</p> <ul style="list-style-type: none"> ■ --user : nom de l'utilisateur à récupérer ■ --new-password : nouveau mot de passe de l'utilisateur ■ --confirm-password : confirmation du nouveau mot de passe ■ --recovery-user : nom de l'utilisateur de récupération (sera supprimé après une récupération réussie) ■ --recovery-password : mot de passe de l'utilisateur de récupération
--backup-authentication	<p>Sauvegarde les données d'authentification et de clé pour déverrouiller la machine. Options :</p> <ul style="list-style-type: none"> ■ --target : chemin complet vers le dossier cible (doit être un dossier)
--backup-kernel	<p>Sauvegarde du noyau de préinitialisation (POA et chargeur d'initialisation). Options :</p> <ul style="list-style-type: none"> ■ --target : chemin complet vers le dossier cible (doit être un dossier) ■ --include-authentication : inclure aussi les données d'authentification et de clé

Commande	Description
	<ul style="list-style-type: none"> ■ --create-dmg : créer une image disque (.dmg). Elle s'appelle "sgRecoveryMedia.dmg"
--encrypt	<p>Chiffre une partition. Vous pouvez spécifier un identifiant unique universel (uuid) de partition ou un index. Les deux peuvent être récupérés avec la commande --status. Il est aussi possible d'utiliser les mots-clés "système" et "tout". Dans ces cas, soit le système, soit toutes les partitions seront chiffrés. Options :</p> <ul style="list-style-type: none"> ■ --authenticate-user : utilisateur "Admin" requis pour l'authentification ■ --authenticate-password : mot de passe "Admin" requis pour l'authentification
--decrypt	<p>Déchiffre une partition. Vous pouvez spécifier un identifiant unique universel (uuid) de partition ou un index. Les deux peuvent être récupérés avec la commande --status. Il est aussi possible d'utiliser les mots-clés "système" et "tout". Dans ces cas, soit le système, soit toutes les partitions seront déchiffrés. Options :</p> <ul style="list-style-type: none"> ■ --authenticate-user : utilisateur "Admin" requis pour l'authentification ■ --authenticate-password : mot de passe "Admin" requis pour l'authentification
--pause	<p>Met l'opération de chiffrement/déchiffrement sur pause. Vous pouvez spécifier un identifiant unique universel (uuid) de partition ou un index. Les deux peuvent être récupérés avec la commande --status. Il est aussi possible d'utiliser le mot-clé "tout". Dans ces cas, soit les opérations sur le système, soit toutes les partitions feront l'objet d'une pause. Options :</p> <ul style="list-style-type: none"> ■ --authenticate-user : utilisateur "Admin" requis pour l'authentification ■ --authenticate-password : mot de passe "Admin" requis pour l'authentification
--resume	<p>Reprend une opération de chiffrement/déchiffrement. Vous pouvez spécifier un identifiant unique universel (uuid) de partition ou un index. Les deux peuvent être</p>

Commande	Description
	<p>récupérés avec la commande <code>--status</code>. Il est aussi possible d'utiliser le mot-clé "tout". Dans ces cas, soit les opérations sur le système, soit toutes les partitions seront reprises. Options :</p> <ul style="list-style-type: none">■ <code>--authenticate-user</code> : utilisateur "Admin" requis pour l'authentification■ <code>--authenticate-password</code> : mot de passe "Admin" requis pour l'authentification
<code>--enable-fast</code>	Règle toutes les opérations de chiffrement/déchiffrement pour un fonctionnement aussi rapide que possible. Par défaut, la vitesse réelle de ces opérations est restreinte. Si cette commande est exécutée, les opérations ne seront pas restreintes. Ceci devrait augmenter la vitesse globale de 20 % à 30 %.
<code>--disable-fast</code>	Active le comportement par défaut (restriction) des opérations de chiffrement/déchiffrement.
<code>--set-boot</code>	Restaure le système d'exploitation par défaut sur OS X.

7 Sauvegardes Time Machine

Les composants suivants de Sophos SafeGuard Disk Encryption doivent être exclus des sauvegardes Time Machine :

- /.com.sophos
- /System/Library/Extensions/sgbiodrv.kext
- /usr/sbin/sgd
- /usr/bin/sgadmin
- /Library/Sophos SafeGuard
- /Library/LaunchDaemons/com.sophos.sgd.plist
- /Library/LaunchAgents/com.sophos.sguimenu.plist
- /Library/LaunchAgents/com.sophos.sgsynclang.plist
- /Applications/sgui.app

8 Matériels et configurations pris en charge

■ Matériel (type Intel seulement)

- MacBook
- MacBook Pro
- MacBook Air
- iMac
- Mac mini
- Mac Pro

■ EFI

- EFI32 (firmware)
- EFI64 (firmware)

Avec la commande de terminal suivante, le firmware EFI peut être vérifié :

```
"ioreg -l -p IODeviceTree | grep firmware-abi"
```

La valeur renvoyée doit être **"firmware-abi" = <"EFI64">** ou **"firmware-abi" = <"EFI32">**.

■ Système d'exploitation

- Niveau de correctif récent 10.5 (Leopard), noyau 32 bits, mode utilisateur 32 bits/64 bits
- Niveau de correctif récent 10.6 (Snow Leopard), noyau 32 bits/64 bits, mode utilisateur 32 bits/64 bits

■ Mise à jour

Les mises à jour de 5.50 en 5.50.1 sont prises en charge sans déchiffrer le disque dur.

Prise en charge de Bootcamp

Configurez une machine avec une partition Bootcamp avant d'installer Sophos SafeGuard Disk Encryption. La configuration ou la suppression d'une partition Bootcamp suite à l'installation de Sophos SafeGuard Disk Encryption n'est pas prise en charge. Notez que la modification ou le redimensionnement de la disposition de la partition suite à l'installation de SafeGuard n'est pas pris en charge.

Si le système d'exploitation par défaut est changé de OS X à Windows, il ne pourra pas être restauré à OS X ni avec le Panneau de configuration Bootcamp de Windows, ni avec l'utilitaire du disque de démarrage d'OS X. Cette opération devra être effectuée à l'aide de la fonctionnalité fournie par Sophos SafeGuard Disk Encryption.

Vous pouvez définir le système de démarrage d'OS X des manières suivantes :

1. Via l'interface utilisateur :

■ Ouvrez **Gestion de SafeGuard Disk**.

- Ouvrez le menu **Modifier** et sélectionnez **Démarrer ce système d'exploitation par défaut**. Authentifiez-vous en tant qu'administrateur OS X.

2. Via le Terminal :

- Ouvrez un **Terminal** et saisissez “`sudo sgadmin --set-boot`”. Notez que l'authentification en tant qu'administrateur OS X est obligatoire.

9 Matériels, configurations et opérations non pris en charge

■ Matériel

Matériel de type PowerPC

■ Système d'exploitation

10.4 et versions précédentes

■ Bootcamp + SafeGuard Enterprise/SafeGuard Easy pour Windows

SafeGuard Enterprise pour Windows ne prend pas en charge le matériel d'Apple et ne peut pas être installé dans un environnement Bootcamp/Windows. Cette restriction est valable jusqu'à mention contraire dans la documentation de SafeGuard Enterprise pour Windows.

■ Les RESTRICTIONS suivantes s'appliquent au produit :

Sophos SafeGuard Disk Encryption pour Mac ne prend pas en charge les systèmes à double amorçage, c'est-à-dire plusieurs installations d'OS X sur le même Mac.

N'installez pas le logiciel sur des systèmes ayant plus de 50 partitions.

Nous vous conseillons de ne pas chiffrer plus de cinq partitions simultanément.

Clavier : le code de traduction du clavier n'affecte que les touches normales et celles avec une touche de modification. Les touches du pavé non numérique ne sont pas assurées de fournir la même séquence de caractères en cas de modification de la disposition du clavier. Utilisez uniquement "0-9" dans ce bloc. En effet, EFI (Extensible Firmware Interface) ne renvoie qu'un caractère ANSI américain équivalent et aucune touche de modification. Lors de la traduction, la touche du clavier normal a la priorité sur la touche du pavé numérique. Ceci affecte les touches non numériques du pavé numérique comme '=', '/', ", '-', '+'. Ces touches peuvent produire un caractère différent à cause de la disposition du clavier. Par exemple, sur un clavier allemand, la touche " du pavé numérique se transforme en caractère '(' du clavier. Le code a été mis au point et testé avec les claviers suivants : américain, français, allemand. Il n'y a aucune garantie que les autres claviers fonctionnent.

Partitionnement : suite à l'installation de Sophos SafeGuard Disk Encryption pour Mac, la modification de la configuration du partitionnement est impossible ou non prise en charge. Cela signifie qu'aucune modification n'est possible avec "gpt" ou "diskutil". Si la machine est partitionnée à nouveau, cette machine sera perdue et devra faire l'objet d'une nouvelle installation.

Formatage : le formatage des partitions chiffrées n'est pas pris en charge. Si vous voulez supprimer toutes les données, nous vous conseillons de supprimer les fichiers ou de déchiffrer la partition, de la formater et de la chiffrer de nouveau. Sachez que seules les partitions HFS+ sont prises en charge pour le chiffrement.

Mode disque cible : l'utilisation du mode disque cible n'est pas prise en charge, si la machine locale et le disque cible sont tous les deux chiffrés. Elle est prise en charge, si la machine locale n'est pas chiffrée et si le disque cible l'est, ou si la machine locale est chiffrée et que le disque cible ne l'est pas.

Utilisation de diskutil à partir d'un système démarré via l'initialisation du réseau : n'utilisez pas diskutil depuis un système lancé via l'initialisation du réseau lorsque les partitions locales sont chiffrées. Dans ce cas, diskutil ne reconnaît pas les partitions chiffrées et veut les initialiser. Cette opération peut entraîner une perte de données.

Suppression de partitions : la suppression d'une partition n'est pas prise en charge lors d'un chiffrement initial ou d'un déchiffrement final. De même, la suppression des partitions chiffrées n'est pas prise en charge. Les partitions doivent être tout d'abord déchiffrées, puis chiffrées de nouveau.

Partitions démontées et chiffrement/déchiffrement : le chiffrement initial ou le déchiffrement final de partitions non montées n'est pas pris en charge. De même, le démontage d'une partition pendant qu'elle est chiffrée ou déchiffrée n'est pas pris en charge. Cette opération peut entraîner une perte de données.

Mises à niveau du système d'exploitation (par exemple de 10.5 à 10.6) non prises en charge : déchiffrez d'abord les partitions de votre Mac avant de désinstaller Sophos SafeGuard Disk Encryption pour Mac. Procédez ensuite à la mise à niveau du système d'exploitation, installez le produit et chiffrez de nouveau les partitions.

Veille prolongée : lorsque Sophos SafeGuard Disk Encryption pour Mac est installé, la fonction d'hibernation "Deep Sleep" n'est pas prise en charge et elle est désactivée. Certaines applications n'enregistrent pas automatiquement leurs données lorsque le mode veille est activé. Au cas où le mode veille est utilisé pour une période étendue sans connexion au secteur et si une telle application est ouverte avec des données non enregistrées, les données peuvent être perdues.

Mise à niveau à partir d'une installation Beta3 : soit le compte utilisateur qui lance la mise à niveau doit être dans le groupe des administrateurs, soit la commande suivante doit être exécutée avant l'installation : `sudo chmod a+r /.com.sophos`.

Secteurs endommagés : nous vous conseillons de ne pas installer le produit si des secteurs sont endommagés sur votre disque dur. Le chiffrement initial ne s'arrête pas lorsque des secteurs endommagés sont trouvés, mais une entrée est créée dans le journal du noyau.

Chiffrement initial/déchiffrement final sur les partitions de données : avant de commencer à chiffrer une partition de données, assurez-vous que tous les fichiers présents sur cette partition sont fermés. Assurez-vous que tous les fichiers présents sur la partition de données à déchiffrer sont fermés pendant le déchiffrement.

10 Support technique

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

- Rendez-vous sur le forum SophosTalk (anglais) à l'adresse <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support 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.fr, y compris le ou les numéros de version(s) du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte de tout message d'erreur.

11 Copyright

Copyright © 2010 - 2011 Sophos Group. Tous droits réservés. SafeGuard est une marque déposée de Sophos Group.

Tous les autres noms de produits et de sociétés mentionnés 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.

Avis de non-responsabilité et déclaration de copyright pour le logiciel tiers

Des parties de ce logiciel sont sous copyright © 2010 The FreeType Project (www.freetype.org). Tous droits réservés.

Ce produit inclut des logiciels développés par le projet OpenSSL Project à utiliser dans le OpenSSL Toolkit (<http://www.openssl.org/>)

Gladman AES

Copyright (c) 1998-2007, Brian Gladman, Worcester, RU. Tous droits réservés.

TERMES DE LA LICENCE

La distribution gratuite et l'utilisation de ce logiciel sont autorisées (avec ou sans modification) sous les conditions suivantes :

1. les distributions du code source doivent inclure l'avis de copyright ci-dessus, cette liste de conditions et l'avis de non-responsabilité ci-dessous ;
2. les distributions binaires doivent inclure l'avis de copyright ci-dessus, cette liste de conditions et l'avis de non-responsabilité ci-dessous dans leur documentation ;
3. le nom du détenteur des droits de copyright ne doit pas être utilisé pour promouvoir des produits construits en utilisant ce logiciel sans autorisation écrite spécifique.

AVIS DE NON-RESPONSABILITÉ

Ce logiciel est fourni « tel quel » sans aucune garantie explicite ou implicite à l'égard de ses propriétés, y compris, mais sans s'y limiter, à l'exactitude et / ou à l'adéquation.