

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy Guide des outils

Version du produit : 5.60

Date du document : avril 2011



Table des matières

1	À propos de ce guide.....	3
2	Affichage de l'état du système avec SGNState.....	3
3	Annulation d'une installation en échec avec SGNRollback.....	4
4	Récupération système et outil de récupération BE_Restore.exe.....	7
5	Mise hors service des volumes chiffrés avec BEInvVol.exe.....	10
6	Mise hors service de disques durs à chiffrement automatique compatibles Opal.....	12
7	Support technique.....	13
8	Mentions légales.....	13

1 À propos de ce guide

Ce guide vous explique comment utiliser les outils Sophos SafeGuard disponibles dans le répertoire des outils de votre logiciel Sophos SafeGuard.

Dans le présent document, vous trouverez les outils suivants :

- SGNState
- SGNRollback
- BE_Restore.exe
- BEInvVol.exe
- opalinvdisk.exe

Remarque :

En outre, vous trouverez l'outil Recover Keys (RecoverKeys.exe) dans le répertoire des outils de votre logiciel client. Cet outil sert à lancer une procédure Challenge/Réponse pour récupérer l'accès à l'ordinateur dans des situations complexes de récupération d'urgence, par exemple lorsque l'authentification au démarrage est corrompue et que l'ordinateur doit être initialisé à partir du disque de récupération SafeGuard. Cet outil figure déjà sur le disque de récupération et il est également disponible dans le répertoire des outils. Vous trouverez une description détaillée de cet outil dans l'aide de l'administrateur SafeGuard, dans la rubrique Challenge/Réponse à l'aide de clients virtuels.

À qui s'adresse ce guide ?

Ce guide s'adresse aux administrateurs utilisant Sophos SafeGuard et agissant en tant que responsables de la sécurité.

2 Affichage de l'état du système avec SGNState

Sophos SafeGuard offre l'outil de ligne de commande SGNState pour afficher des informations sur l'état actuel (état du chiffrement et d'autres informations détaillées sur l'état) de l'installation Sophos SafeGuard sur un ordinateur d'extrémité.

Vous trouverez cet outil dans le répertoire Outils du dossier de votre logiciel client Sophos SafeGuard.

Rapports

SGNState peut également être utilisé comme suit :

- Le code renvoyé de SGNState peut être évalué sur le serveur à l'aide d'outils de gestion tiers.
- SGNState /LD renvoie un résultat formaté pour LANDesk et pouvant être inscrit dans un fichier.

Paramètres

Vous pouvez appeler l'outil SGNState avec les paramètres suivants :

SGNSTATE [/?] [/L] [/LD]

- Le paramètre `/?` renvoie des informations d'aide sur les paramètres de ligne de commande SGNState disponibles.
- Le paramètre `/L` affiche les informations suivantes :
 - Système d'exploitation
 - Version installée de Sophos SafeGuard
 - Type d'authentification au démarrage (BitLocker ou Sophos SafeGuard)
 - État de l'authentification au démarrage (activée/désactivée)
 - État de l'éveil par appel réseau (activé/désactivé)
 - Nom du serveur
 - Mode de connexion
 - État d'activation du client
 - Date (et heure) de la dernière duplication de données
 - Dernière stratégie reçue
 - État du chiffrement (chiffré/non chiffré), algorithme utilisé pour les volumes individuels
- Le paramètre `/LD` renvoie ces informations formatées pour LANDesk

3 Annulation d'une installation en échec avec SGNRollback

En cas d'échec de l'installation de Sophos SafeGuard sur un ordinateur client, l'initialisation de l'ordinateur est parfois impossible et aucune administration à distance ne peut être effectuée.

Dans ce genre de situations, Sophos SafeGuard propose l'outil SGNRollback.

SGNRollback permet d'annuler automatiquement les effets de l'échec d'une installation de Sophos SafeGuard en :

- Permettant l'initialisation de l'ordinateur bloqué
- Supprimant Sophos SafeGuard,
- Annulant toutes les modifications effectuées dans GINA et dans les autres composants de système d'exploitation.

SGNRollback est un programme disponible dans le répertoire Outils du dossier de votre logiciel Sophos SafeGuard Admin. Il s'exécute depuis un système de récupération Windows, plus exactement WindowsPE ou BartPE.

3.1 Scénario d'utilisation

SGNRollback peut réparer une installation Sophos SafeGuard infructueuse sur un ordinateur d'extrémité si les conditions suivantes s'appliquent :

- L'authentification au démarrage se bloque au premier démarrage et l'ordinateur ne peut plus être initialisé.
- Le disque dur n'est pas chiffré.

Remarque :

La migration à partir de SafeGuard Easy vers Sophos SafeGuard n'est pas prise en charge.

Autres conditions préalables

Pour utiliser SGNRollback, d'autres conditions préalables s'appliquent :

- SGNRollback fonctionne avec les systèmes de récupération WinPE et BartPE. Pour pouvoir utiliser SGNRollback à des fins de récupération, vous devez l'intégrer au système de récupération requis. Pour plus d'informations, consultez la documentation du système de récupération correspondant.

Si SGNRollback doit être exécuté par le programme de démarrage automatique, l'administrateur utilisant SGNRollback doit définir les paramètres correspondants dans WinPE ([voir la section Activation du programme de démarrage automatique de SGNRollback pour WindowsPE à la page 5](#)) ou BartPE ([voir la section Activation du programme de démarrage automatique de SGNRollback pour BartPE à la page 5](#)).

- Sophos SafeGuard Device Encryption est installé.

Systèmes d'exploitation pris en charge

SGNRollback prend en charge les systèmes d'exploitation suivants :

- Windows XP
- Windows Vista
- Windows 7

3.2 Démarrage de SGNRollback dans le système de récupération

Vous pouvez démarrer SGNRollback manuellement ou l'ajouter au programme de démarrage automatique du système de récupération.

3.2.1 Activation du programme de démarrage automatique de SGNRollback pour Windows PE

Pour activer le programme de démarrage automatique de SGNRollback pour Windows PE, installez le kit d'installation automatisée (Windows AIK). Vous trouverez des informations sur la façon de concevoir un environnement Windows PE et d'exécuter automatiquement une application dans le guide de l'utilisateur de l'environnement de préinstallation Windows.

3.2.2 Activation du programme de démarrage automatique de SGNRollback pour BartPE

Pour activer le programme de démarrage automatique de SGNRollback pour BartPE, procédez comme suit :

1. Utilisez la version 3.1.3 ou supérieure de BartPEBuilder pour créer une image PE. Pour plus d'informations, reportez-vous à la documentation BartPE.

2. Dans BartPE Builder, ajoutez le dossier de l'outil de récupération dans le champ **Personnaliser**.
 3. Créez l'image.
 4. Copiez le fichier AutoRun0Recovery.cmd à partir du support Sophos SafeGuard dans le dossier i386 de la version BartPE pour Windows.
 5. Créez une commande AutoRun0Recovery.cmd à l'aide des deux lignes de texte suivantes :

```
\Recovery\recovery.exe  
exit
```
 6. Exécutez l'outil PEBuilder depuis la ligne de commande :

```
Pebuilder -buildis
```

Une nouvelle image iso est créée qui intègre le fichier de démarrage automatique.
 7. Enregistrez l'image obtenue sur un support de récupération.
- Au moment d'initialiser cette image, SGNRollback démarre automatiquement.

3.3 Paramètres

SGNRollback peut être démarré à l'aide du paramètre suivant :

-drv WinDrive	Indique la lettre du lecteur sur lequel l'installation Sophos SafeGuard devant faire l'objet d'une réparation est installée. Ce paramètre ne peut être utilisé qu'en mode récupération. Il doit être utilisé dans des environnements à démarrage multiple pour signaler le lecteur correct.
----------------------	---

3.4 Annulation d'une installation non réussie

Pour annuler les effets d'une installation non réussie de Sophos SafeGuard sur un ordinateur d'extrémité, procédez comme suit :

1. Initialisez l'ordinateur à partir du support de récupération contenant le système de récupération, notamment SGNRollback.
2. Démarrez SGNRollback dans le système de récupération. Si le programme de démarrage automatique est présent, SGNRollback démarrera automatiquement. SGNRollback prépare le système d'exploitation pour la désinstallation de Sophos SafeGuard.
3. Le système vous demande à présent de retirer le support de récupération. Après avoir retiré le support, l'ordinateur est réinitialisé en mode sans échec.

Toutes les modifications effectuées sont supprimées et Sophos SafeGuard est désinstallé.

4 Récupération système et outil de récupération BE_Restore.exe

Processus d'initialisation de Sophos SafeGuard

Sophos SafeGuard chiffre les fichiers et les lecteurs de façon transparente. Les lecteurs d'initialisation peuvent également être chiffrés et les fonctions de déchiffrement telles que le code, les algorithmes de chiffrement et la clé USB de chiffrement doivent être disponibles très tôt au cours de la phase d'initialisation. C'est la raison pour laquelle les informations chiffrées ne sont pas accessibles si les modules essentiels de Sophos SafeGuard ne sont pas disponibles ou ne fonctionnent pas.

4.1 Restauration d'un MBR corrompu

La fonction d'authentification au démarrage de Sophos SafeGuard est chargée à partir du MBR sur le disque dur de l'ordinateur. Lorsque l'installation est terminée, Sophos SafeGuard enregistre une copie de l'original (tel qu'il était avant l'installation de Sophos SafeGuard) dans son noyau, et modifie le chargeur de BPR à partir de LBA 0. Dans son LBA 0, le MBR modifié contient l'adresse du premier secteur du noyau Sophos SafeGuard et sa taille totale.

Les problèmes associés au MBR peuvent être résolus avec l'outil de récupération de Sophos SafeGuard, **BE_Restore.exe**. Cet outil est une application Win32 qui doit être exécutée sous Windows et non sous DOS.

Un chargeur MBR défectueux signifie que le système ne peut pas être initialisé. Il existe deux manières de le restaurer :

- Restauration du MBR à partir d'une sauvegarde.
- Réparation du MBR.

Pour restaurer un MBR corrompu, procédez comme suit :

1. Nous vous conseillons de créer un CD-ROM d'initialisation Windows PE (Environnement préinstallé).
2. Pour utiliser l'outil de récupération de client **BE_Restore.exe**, plusieurs fichiers supplémentaires sont nécessaires. L'outil et les fichiers nécessaires sont disponibles dans le dossier **tools\KeyRecovery and Restore** de votre logiciel client. Copiez tous les fichiers de ce dossier sur une carte mémoire. Veillez à enregistrer tous les fichiers dans **le même** dossier sur votre carte mémoire. Cette condition est nécessaire au démarrage correct de l'outil de récupération.
3. Si nécessaire, modifiez la séquence d'initialisation dans le BIOS et sélectionnez le CD-ROM pour qu'il soit le premier.

Remarque :

BERestore peut uniquement restaurer ou réparer le MBR sur le disque 0. Si vous utilisez deux disques durs et que le système est initialisé à partir de l'autre disque dur, le MBR ne pourra pas être récupéré ou réparé. Cette condition s'applique également à l'utilisation d'un disque dur amovible.

4.2 Restauration d'une sauvegarde MBR précédemment enregistrée

Pour restaurer une sauvegarde MBR précédemment enregistrée, procédez comme suit :

1. Suite à l'installation de Sophos SafeGuard sur l'ordinateur d'extrémité, vous êtes invité à spécifier un emplacement de fichier dans lequel vous allez enregistrer la sauvegarde du MBR. Cette action produit un fichier de 512 octets portant l'extension .BKN, qui contient le MBR.
2. Copiez ce fichier dans le dossier de la carte mémoire dans lequel se trouvent les autres fichiers Sophos SafeGuard.
3. Insérez maintenant le CD-ROM de démarrage Windows PE dans le lecteur, connectez la carte mémoire contenant les fichiers Sophos SafeGuard sur l'ordinateur et démarrez celui-ci à partir du CD-ROM.
4. Lorsque l'ordinateur est prêt, lancez cmd-box, naviguez jusqu'au répertoire de la carte mémoire contenant les fichiers Sophos SafeGuard et exécutez **BE_Restore.exe**.
5. Sélectionnez **Restaurer le MBR** pour effectuer une restauration à partir d'une sauvegarde et sélectionnez le fichier .BKN.

BE_Restore.exe vérifie alors si le fichier .BKN sélectionné correspond à l'ordinateur, puis restaure le MBR sauvegardé.

4.3 Réparation du MBR sans sauvegarde

Même si aucun fichier de sauvegarde MBR n'est disponible localement, BE_Restore.exe peut réparer un chargeur MBR corrompu. **BE_Restore.exe - Réparer le MBR** recherche le noyau Sophos SafeGuard sur le disque dur, utilise son adresse et recrée le chargeur MBR.

Cette procédure présente de très grands avantages, car aucun fichier de sauvegarde MBR spécifique à l'ordinateur n'a besoin d'être disponible en local. Cependant, elle prend un peu plus de temps car **BE_Restore.exe - Réparer le MBR** doit effectuer la recherche complète du disque dur pour trouver le noyau Sophos SafeGuard.

Pour utiliser la fonction de réparation, procédez selon les instructions, mais sélectionnez **Réparer le MBR** à l'exécution de **BE_Restore.exe**.

Si plusieurs noyaux existent, **BE_Restore.exe – Réparer le MBR** utilise celui dont l'estampille temporelle est la plus récente.

4.4 Table de partition

Sophos SafeGuard permet de créer de nouvelles partitions principales ou étendues. Cette action modifie la table de partition du disque dur sur lequel se trouve la partition.

Lors de la restauration d'une sauvegarde MBR, BE_Restore voit que le MBR actuel contient des tables de partition différentes pour le LBA 0 et le fichier de sauvegarde MBR (*.BKN) à restaurer. Dans une boîte de dialogue, l'utilisateur peut indiquer la procédure.

4.4.1 Réparation d'un MBR avec une table de partition corrompue

Une table de partition corrompue peut empêcher l'initialisation du système d'exploitation après une connexion POA réussie.

Vous pouvez résoudre ce problème en utilisant `BE_Restore.exe` pour restaurer un MBR précédemment enregistré ou réparer le MBR sans sauvegarde MBR.

Si vous avez une sauvegarde, procédez tel que décrit pour l'option **Restaurer le MBR**.

Si vous n'avez pas de sauvegarde, procédez comme suit :

1. Insérez le CD-ROM de démarrage Windows PE dans le lecteur, connectez la carte mémoire contenant les fichiers Sophos SafeGuard sur l'ordinateur et démarrez celui-ci à partir du CD-ROM.
2. Lorsque l'ordinateur est prêt, à partir de la ligne de commande, naviguez jusqu'au répertoire de la carte mémoire contenant les fichiers Sophos SafeGuard et exécutez **BE_Restore.exe**.
3. Sélectionnez **Réparer le MBR**. Si `BE_Restore.exe` détecte une différence entre la table de partition du MBR actuel et celle du MBR en miroir, une boîte de dialogue permettant de sélectionner la table de partition à utiliser s'affiche.

Le MBR en miroir correspond au MBR Microsoft d'origine enregistré durant la configuration du client Sophos SafeGuard afin de vous permettre de le restaurer, par exemple, en cas de désinstallation du client. La table de partition de ce MBR en miroir est mise à jour par Sophos SafeGuard si un changement survient dans Windows au niveau de la partition.

4. Sélectionnez **À partir du MBR en miroir**.

Remarque :

Si vous sélectionnez **Depuis le MBR actuel**, la table de partition du MBR actuel sera utilisée, (dans ce cas, une table de partition corrompue). Non seulement le système ne pourra toujours pas être initialisé, mais le MBR en miroir sera mis à jour et par conséquent corrompu.

4.5 Signature de disque Windows

Chaque fois que Windows crée un système de fichiers pour la première fois sur un disque dur, il l'associe à une signature. Cette signature est enregistrée dans le MBR du disque dur (offsets 0x01B – 0x01BB). Notez que, par exemple, les lettres d'unités logiques du disque dur dépendent de la signature de disque Windows.

Exemple : l'administrateur Windows utilise le gestionnaire de disque dur Windows pour changer les lettres d'unités logiques des disques C:, D: et E: sur les lettres C:, F: et Q: afin de supprimer la signature du disque Windows du MBR du disque dur. Au prochain démarrage, Windows passe en mode de contrôle du disque dur et après un long moment restaure la liste des lecteurs. De ce fait, les trois lecteurs ont de nouveau leurs lettres d'unités d'origine C:, D: et E:.

Chaque fois que cela se produit sous Sophos SafeGuard, le pilote du filtre Sophos SafeGuard "BEFLT.sys" n'est pas chargé. L'initialisation du système est ainsi impossible : l'ordinateur affiche un écran bleu « STOP 0xED "Unmountable Boot Volume" ».

Pour réparer cela sous Sophos SafeGuard, la signature de disque Windows originale doit être restaurée sur le MBR du disque dur.

L'utilitaire **BE_Restore.exe** effectue également cette tâche.

Remarque :

Soyez très prudent lorsque vous utilisez un autre outil pour réparer le MBR. Par exemple, un ancien MS DOS **FDISK.exe** que vous utilisez pour réécrire le chargeur MBR («**FDISK /MBR**») peut créer un autre chargeur MBR sans signature de disque Windows. De même qu'un ancien outil peut supprimer la signature de disque Windows, le «nouveau» chargeur MBR peut être incompatible avec les tailles des disques durs fréquemment utilisés aujourd'hui. Utilisez toujours les versions les plus récentes des outils de réparation.

5 Mise hors service des volumes chiffrés avec BEInvVol.exe

Pour les ordinateurs protégés par Sophos SafeGuard, nous proposons un outil de ligne de commande **BEInvVol.exe** pouvant être utilisé pour mettre hors service en toute sécurité les volumes chiffrés (disques durs, clés USB, etc.). Cet outil de ligne de commande est basé sur la norme DoD 5220.22-M et peut être utilisé pour supprimer des magasins de clés en toute sécurité. Cette norme comporte sept cycles de remplacement avec des modèles aléatoires et alternatifs.

Cet outil de ligne de commande est conçu pour être utilisé sur des ordinateurs sur lesquels s'appliquent les événements suivants :

- Sophos SafeGuard est installé.
- Certains volumes de disque dur ont été chiffrés.

Vous devez exécuter cet outil au sein d'un système où le pilote de chiffrement Sophos SafeGuard n'est pas actif. Ceci afin d'empêcher que des données soient mises hors service par accident. Sinon, l'outil ne fonctionne pas et un message d'erreur apparaît.

Remarque :

Nous vous conseillons de démarrer votre système à partir d'un support externe comme un CD-ROM Windows PE et d'utiliser l'outil en fonction des instructions disponibles dans l'aide de la ligne de commande.

Une fois que les volumes cibles correspondants ont été mis hors service, ils ne sont plus lisibles.

Conformément à la norme DoD 5220.22-M, l'outil de ligne de commande purge en permanence les secteurs de démarrage et les zones de stockage des clés de Sophos SafeGuard (KSA d'origine et sauvegarde) de chaque volume chiffré en les remplaçant sept fois. Les clés de chiffrement de données (DEK) aléatoires de chaque volume n'étant pas sauvegardées dans la base de données centrale des clients Sophos SafeGuard, les volumes sont alors parfaitement hermétiques. Même un responsable de sécurité ne peut y accéder.

L'outil de ligne de commande affiche également des informations à l'écran concernant les volumes disponibles. Ceci inclut par exemple le nom du volume, la taille du volume et les informations concernant les secteurs de démarrage et les KSA. Ces informations peuvent en option être stockées dans un fichier. Le chemin de ce fichier doit bien évidemment désigner un volume non mis hors service.

Remarque :

Les données ne peuvent pas être récupérées après suppression.

5.1 Démarrage de l'outil de ligne de commande

Syntaxe

■ **xl[volume]**

Répertorie les informations du ou des volumes cibles. Répertorie les informations concernant tous les volumes si aucun volume cible n'est spécifié.

■ **xi<volume>**

Invalide le ou les volumes cibles, en cas de chiffrage complet. Le <volume> cible doit être spécifié pour cette commande.

■ **<volume>**

Indique le volume cible = {a, b, c, ..., z, *}, <*> correspondant à l'ensemble des volumes.

Options

■ **-g0**

Désactive le mécanisme de journalisation.

■ **-ga[file]**

Mode journalisation -append. Ajoute les entrées du journal à la fin du fichier journal cible ou le crée s'il n'existe pas.

■ **-gt[file]**

Mode journalisation -truncate. Tronque le fichier journal cible s'il existe ou le crée s'il n'existe pas.

■ **[file]**

Spécifie le fichier journal cible. S'il n'est pas spécifié, le fichier journal cible par défaut est "BEInvVol.log" dans le chemin en cours. Ne définissez pas ce fichier sur le volume devant être invalidé.

■ **-?, -h**

Affiche l'aide.

Exemples

```
> beinvvol -h
```

```
> beinvvol xld
```

```
> beinvvol xle -gac:\subdir\file.log
> beinvvol xl* -gtc:\subdir\file.log
> beinvvol xif -gt"c:\my subdir\file.log"
> beinvvol xig -g0
> beinvvol xi*
```

6 Mise hors service de disques durs à chiffrement automatique compatibles Opal

Les disques durs à chiffrement automatique offrent un chiffrement de type matériel des données lorsqu'ils sont écrits sur le disque dur. Le Trusted Computing Group (TCG) a publié la norme Opal indépendante des fournisseurs pour les disques durs à chiffrement automatique. Sophos SafeGuard prend en charge la norme Opal et permet la gestion des ordinateurs d'extrémité avec disques durs à chiffrement automatique compatibles Opal.

Pour plus d'informations sur les disques durs compatibles Opal, reportez-vous à l'aide administrateur de Sophos SafeGuard, chapitre *Sophos SafeGuard et disques durs compatibles Opal à chiffrement automatique*.

Pour les ordinateurs protégés par Sophos SafeGuard, nous proposons l'outil de ligne de commande **opalinvdisk.exe** qui lance un service facultatif de lecteurs de disque dur compatibles Opal (**RevertSP** avec le paramètre **KeepGlobalRangeKey** défini sur **False**). **RevertSP** met en toute sécurité hors service les disques durs compatibles Opal en leur rétablissant leurs valeurs par défaut et en supprimant les clés. Pour plus d'informations sur **RevertSP**, reportez-vous à la section 5.2.3 du document Opal standard TCG Storage Security Subsystem Class : Opal, Specification Version 1.00, Revision 3.00 (disponible dans www.trustedcomputinggroup.org).

6.1 Conditions préalables et recommandations

Pour l'utilisation de **opalinvdisk.exe**, les conditions préalables et les recommandations suivantes s'appliquent :

- Avant que vous n'utilisiez **opalinvdisk.exe**, le disque dur compatible Opal doit être déchiffré avec la commande **Decrypt** de Sophos SafeGuard disponible dans le menu contextuel de l'Explorateur Windows sur l'ordinateur d'extrémité. Pour plus d'informations, reportez-vous à l'aide administrateur de Sophos SafeGuard, section *Permettre aux utilisateurs de déverrouiller les disques durs compatibles Opal* et à l'aide utilisateur de Sophos SafeGuard, section *Extensions des icônes de la barre d'état et de l'Explorateur sur les ordinateurs d'extrémité avec disques durs compatibles Opal*.
- Vous avez besoin des droits d'administrateur.
- Nous vous conseillons d'utiliser **opalinvdisk.exe** dans un environnement Windows PE.
- L'outil **opalinvdisk.exe** lance le service facultatif **RevertSP** avec le paramètre **KeepGlobalRangeKey** défini sur **False**. La véritable procédure de mise hors service exécutée par **RevertSP** dépend du lecteur de disque dur spécifique. Pour plus d'informations, reportez-vous à la section 5.2.3 du document Opal standard TCG Storage Security Subsystem Class : Opal, Specification Version 1.00, Revision 3.00 (disponible dans www.trustedcomputinggroup.org).

6.2 Exécution de opalinvdisk.exe

1. Ouvrez une invite de commande et démarrez **opalinvdisk.exe avec les droits administrateur**.

Des informations sur les outils et sur son utilisation apparaissent.

2. Sur la ligne de commande, entrez **opalinvdisk.exe <TargetDevice>**.

Par exemple : **opalinvdisk.exe PhysicalDrive0**

Si les conditions préalables nécessaires sont remplies, RevertSP est lancé sur le disque dur spécifié dans <TargetDevice>. Si les conditions préalables ne sont pas remplies ou si le disque dur ne prend pas en charge RevertSP, un message d'erreur apparaît.

7 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 du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

8 Mentions légales

Copyright © 1996 - 2011 Sophos Group. Tous droits réservés. SafeGuard est une marque déposée de Sophos Group.

Sophos est une marque déposée de Sophos Limited, Sophos Group et Utimaco Safeware AG, selon le cas. 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.

Les informations de copyright des fournisseurs tiers sont disponibles dans le fichier appelé Disclaimer and Copyright for 3rd Party Software.rtf dans votre répertoire des produits.