

# SOPHOS

## Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Guide des outils

Date du document : Avril 2010



# Table des matières

1	À propos de ce guide.....	2
2	Affichage de l'état du système avec SGNState .....	3
3	Annulation d'une installation en échec avec SGNRollback .....	5
4	Récupération système et outil de récupération BE_Restore.exe.....	9
5	Mise hors service des volumes chiffrés avec BEInvVol.exe.....	14

# 1 À propos de ce guide

Ce guide explique l'utilisation des outils Sophos SafeGuard proposés dans le répertoire des outils du logiciel Sophos SafeGuard de sorte à répondre aux différents scénarios et procédures décrits.

Dans le présent document, vous trouverez les outils suivants :

- SGNState
- SGNRollback
- BEInvVol.exe
- BE\_Restore.exe

**Remarque:** En outre, vous trouverez l'outil Recover Keys (RecoverKeys.exe) dans le répertoire des outils de votre logiciel client Sophos SafeGuard. L'outil Recover Keys sert à lancer une procédure Challenge/Réponse et à ainsi permettre l'accès à l'ordinateur dans des situations complexes d'urgence, par exemple lorsque POA est corrompu et que l'ordinateur doit être initialisé à partir du disque de récupération SafeGuard. Cet outil figure déjà sur le disque de récupération et est également proposé dans le répertoire des outils. Vous trouverez une description détaillée de cet outil ainsi que d'un cas d'urgence dans l'aide de l'administrateur SafeGuard, dans la rubrique Challenge/Réponse à l'aide de clients virtuels.

## 1.1 Public visé

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

## 2 Affichage de l'état du système avec SGNState

Sophos SafeGuard propose l'outil de ligne de commande SGNState qui affiche des informations sur l'état actuel (état du chiffrement et autres informations détaillées connexes) de l'installation Sophos SafeGuard, sur le PC de l'utilisateur.

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

### 2.1 Rapports

SGNState peut également être utilisé pour les rapports :

- 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.

### 2.2 Paramètres

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

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

- Paramètre /? renvoie des informations d'aide sur les paramètres de ligne de commande SGNState disponibles.
- Paramètre /L affiche les informations suivantes :
  - Système d'exploitation
  - Version de Sophos SafeGuard installée
  - Type de POA (Sophos SafeGuard)
  - État du POA (activé/désactivé)
  - 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

- Paramètre /LD renvoie ces informations formatées pour LANDesk

## 3 Annulation d'une installation en échec avec SGNRollback

Dans le cas d'un échec d'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.

Pour des urgences de ce type, Sophos SafeGuard propose l'outil SGNRollback.

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

- permettant l'initialisation de l'ordinateur bloqué ;
- supprimant Sophos SafeGuard ;
- annulant toutes les modifications effectuées dans GINA et les autres composants de système d'exploitation.

SGNRollback est disponible sous forme de fichier exécutable dans le répertoire Outils du dossier logiciel Sophos SafeGuard Admin. Il s'exécute depuis un système de récupération Windows, plus exactement Windows PE ou BartPE.

### 3.1 Scénario d'utilisation

SGNRollback peut réparer une installation Sophos SafeGuard en échec sur un ordinateur client si les conditions suivantes s'appliquent :

- L'authentification au démarrage se fige durant la première initialisation et l'utilisateur ne peut plus démarrer son ordinateur.
- Le disque dur n'est pas chiffré.

**Remarque:** Un scénario de migration de SafeGuard Easy vers Sophos SafeGuard n'est pas pris en charge.

### **3.1.1 Autres conditions préalables**

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

- SGNRollback fonctionne avec les systèmes de récupération WinPE 2.0, WinPE 3.0 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 via le programme de démarrage automatique, l'administrateur utilisant SGNRollback doit définir les paramètres correspondants dans WinPE (voir [Lancement du programme de démarrage automatique de SGNRollback pour Windows PE](#), à la page 6) ou BartPE (voir [Lancement du programme de démarrage automatique de SGNRollback pour BartPE](#), à la page 7).

- Le chiffrement de périphérique Sophos SafeGuard est installé.

### **3.1.2 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 Lancement du programme de démarrage automatique de SGNRollback pour Windows PE**

Pour lancer 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 Lancement du programme de démarrage automatique de SGNRollback pour BartPE**

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

1. Utilisez BartPEBuilder version 3.1.3 ou supérieure pour créer une image PE. Pour des informations plus détaillées, 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 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 en échec

Pour annuler les effets d'une installation Sophos SafeGuard en échec sur un ordinateur client, 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

### Procédure 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 de chiffrement doivent être disponibles très tôt au cours 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 BE\_Restore.exe de Sophos SafeGuard. Cet outil est une application Win32 qui doit être exécutée sous Windows et non sous DOS.

Un chargeur MBR défectueux se traduit par un système qui 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, des étapes préalables sont nécessaires :

1. Nous vous recommandons de créer un CD d'initialisation Windows PE (Environnement préinstallé).
2. Pour utiliser l'outil de récupération de client BE\_Restore.exe, plusieurs fichiers supplémentaires sont nécessaires. Vous trouverez cet outil et les fichiers requis dans le dossier du logiciel client SafeGuard sous tools\KeyRecovery and Restore. Copiez tous les fichiers de ce dossier sur une carte mémoire. Veillez à enregistrer tous les fichiers dans **le même dossier** de 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 ne peut récupérer ou réparer le MBR que 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 ni réparé. Cette condition s'applique également à l'utilisation d'un disque dur amovible.

#### 4.1.1 Restauration d'une sauvegarde MBR précédemment enregistrée

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

1. Après l'installation de Sophos SafeGuard sur l'ordinateur final, vous êtes invité à indiquer un emplacement de fichier pour enregistrer la sauvegarde 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 fichiers Sophos SafeGuard supplémentaires.
3. Insérez à présent le CD d'initialisation Windows PE dans le lecteur, branchez la carte mémoire contenant les fichiers Sophos SafeGuard et initialisez l'ordinateur à partir du CD.
4. Lorsque l'ordinateur est prêt, lancez cmd-box, accédez 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.

#### 4.1.2 Réparation du MBR sans sauvegarde

Même si aucun fichier de sauvegarde MBR n'est disponible en local, 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, en particulier du fait qu'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.

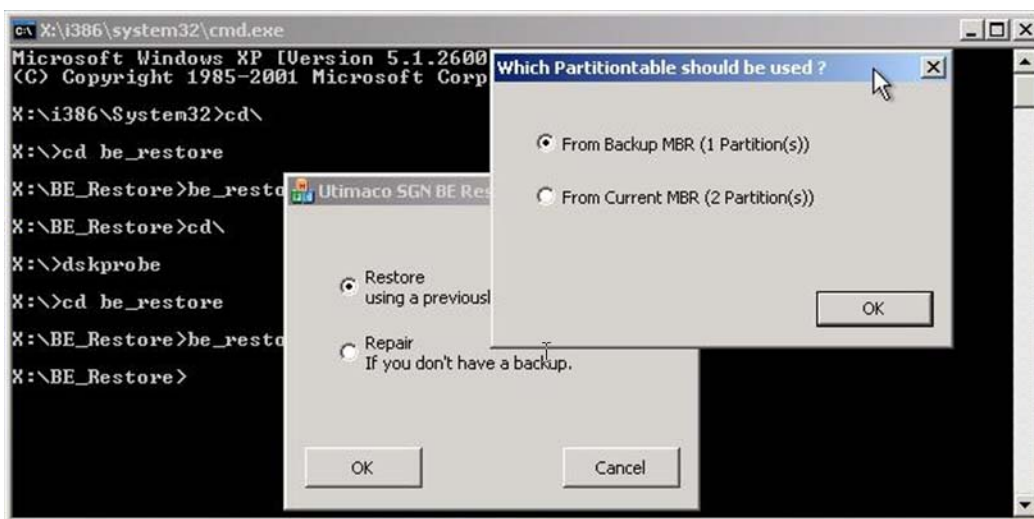
Pour utiliser la fonction de réparation, procédez comme décrit, mais sélectionnez **Réparer le MBR** à l'exécution de BE\_Restore.exe.

Si plusieurs noyaux existent, BE\_Restore.exe – **Réparer le MBR** utilise celui dont l'horodatage est le plus récent.

### 4.1.3 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.



#### 4.1.3.1 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 possédez une sauvegarde, procédez tel que décrit pour l'option **Restaurer le MBR**.

Si vous ne possédez pas de sauvegarde, procédez comme suit :

1. Insérez le CD d'initialisation Windows PE dans le lecteur, branchez la carte mémoire contenant les fichiers Sophos SafeGuard et initialisez l'ordinateur à partir du CD.
2. Lorsque l'ordinateur est prêt, lancez cmd-box, accédez 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, la 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 à des fins de restauration, c'est-à-dire 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**.

Si vous sélectionnez **Depuis le MBR actuel**, la table de partition du MBR actuel sera utilisée, c'est-à-dire dans le cas ci-présent, 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.

#### **4.1.4 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 des unités logiques des disques C:, D: et E: en C:, F: et Q:. Cette action supprime la signature de disque Windows du MBR du disque dur. Après la procédure d'initialisation suivante, Windows passe dans un mode d'analyse de disque dur qui prend du temps et 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.

C'est justement ce que permet de faire l'utilitaire BE\_Restore.exe.

**Remarque:** Soyez très prudent si 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 de disque dur couramment utilisées aujourd'hui. Il est recommandé de toujours utiliser les versions les plus récentes des outils de réparation.

## 5 Mise hors service des volumes chiffrés avec BEInvVol.exe

Pour 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.), particulièrement dans le cas de deux magasins de clés créés et gérés par Sophos SafeGuard. Cet outil de ligne de commande permet de mettre facilement hors service tous les volumes chiffrés. 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 ne peut être utilisé que sur un ordinateur client sur lequel Sophos SafeGuard est installé. Lorsque le volume souhaité a été trouvé, un message d'avertissement s'affiche pour demander à l'utilisateur de confirmer la demande. Tous les magasins de clés (primaires et secondaires) sont ensuite supprimés. Le volume n'est, à ce stade, plus lisible.

Conformément à la norme DoD 5220.22-M, l'outil de ligne de commande purge en permanence les zones de stockage des clés de Sophos SafeGuard (anciennement KSA 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 le processus de suppression. Ceci inclut par exemple le nom du volume, la taille du volume, les informations de magasin de clés telles que le nom symbolique de la clé, la date et l'heure de la suppression, l'utilisateur ayant effectué la suppression et le nom de l'ordinateur sur lequel la suppression a été effectuée. Ces informations peuvent être stockées sur n'importe quel périphérique de stockage, clé USB ou sur le serveur du réseau.

**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/des volume(s) cible(s). Si aucun volume cible n'est spécifié, répertorie les informations concernant tous les volumes.

- xi<volume>

Invalide le(s) volume(s) cible(s), en cas de chiffrement 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.

- ?, h

Affiche l'aide.

### Options

- -g0

Désactive le mécanisme de consignation

- -ga[file]

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

- -gt[file]

Mode consignation -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*`