

SOPHOS

Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Guide de démarrage

Date du document : Avril 2010



Table des matières

1	À propos de ce guide.....	3
2	Introduction.....	4
3	Mise à niveau de Sophos SafeGuard Disk Encryption 4.60	7
4	Mise à niveau des versions de SafeGuard Easy 4.x.....	8
5	Quelles sont les étapes clés ?	9
6	Vérification de la configuration minimale du système.....	10
7	Préparation de l'installation.....	12
8	Installation de SafeGuard Policy Editor.....	15
9	Réalisation de la configuration initiale.....	16
10	Réalisation d'une configuration supplémentaire pour le logiciel de chiffrement	18
11	Configuration des accès administratifs sur les ordinateurs finaux	28
12	Installation du logiciel de chiffrement et de la configuration de chiffrement sur les ordinateurs finaux.....	31
13	Récupération d'un mot de passe oublié.....	37
14	Récupération de l'accès au système.....	40
15	Aide sur les tâches communes.....	43
16	Support technique.....	44
17	Copyright	45

1 À propos de ce guide

Ce guide vous indique comment configurer Sophos SafeGuard afin de protéger les ordinateurs de votre entreprise contre les accès non autorisés.

Il s'applique aux produits suivants :

- Sophos SafeGuard Disk Encryption (SDE) 5.50 disponible avec l'ensemble Endpoint Security and Data Protection (ESDP).
- Sophos SafeGuard Easy (SGE) 5.50. À partir de la version 5.50, SGE est le nouveau nom de produit de la solution autonome SafeGuard Enterprise.

Dès lors qu'une fonction ou un paramètre diffère entre les deux produits, le guide le mentionne de façon explicite.

Des informations supplémentaires sont disponibles dans les documents de l'aide de l'administrateur et de l'aide de l'utilisateur Sophos SafeGuard qui accompagnent ce Guide de démarrage.

2 Introduction

Sophos SafeGuard permet de chiffrer les données de manière transparente. Les utilisateurs n'ont pas besoin de spécifier les données à chiffrer, si bien que l'opération passe totalement inaperçue. Le chiffrement permet d'éviter la consultation ou la modification des données des personnes non autorisées. Le chiffrement Sophos SafeGuard ne peut pas être contourné, même si vous connectez les supports de stockage à un autre système.

Les avantages de Sophos SafeGuard sont les suivants :

- Système de protection simple, mais efficace de la confidentialité des données
- Mise en œuvre rapide
- Utilisation d'une technologie de chiffrement leader sur le marché et certifiée conforme à FIPS 140

Les ordinateurs protégés par Sophos SafeGuard exécutent l'authentification au démarrage SafeGuard avant le démarrage des systèmes d'exploitation.

Connexion SafeGuard

SOPHOS

Nom d'utilisateur: Alice

Mot de passe: *****

Domaine: MY_COMPANY

OK Récupération Arrêter Options >>

L'authentification au démarrage fournit les fonctions conviviales et hautement sécurisées suivantes :

- Protection contre les modifications non autorisées pour Sophos SafeGuard Disk Encryption
- Délais de connexion en cas de saisies erronées
- Interface utilisateur graphique personnalisable de type Windows
- Connexion automatique à Windows
- Prise en charge de plusieurs langues et de la norme unicode

2.1 Accès pratique pour les opérations informatiques

Sophos SafeGuard propose plusieurs fonctions facilitant les opérations informatiques sur les ordinateurs finaux :

- L'authentification au démarrage peut être configurée afin d'être utilisée avec l'éveil par appel réseau, notamment pour faciliter la gestion des correctifs.
- Les comptes de service permettent aux membres de l'équipe informatique de se connecter aux ordinateurs finaux pour réaliser des tâches de post-installation, et ce, sans activer l'authentification au démarrage.
- Les comptes d'accès POA permettent aux membres de l'équipe informatique de se connecter aux ordinateurs finaux chiffrés pour réaliser des tâches administratives après activation de l'authentification au démarrage.

2.2 Scénarios de récupération dans Sophos SafeGuard

Sophos SafeGuard propose plusieurs options de récupération, adaptées à différents scénarios de récupération :

■ Récupération de connexion via Local Self Help

Local Self Help permet aux utilisateurs ayant oublié leur mot de passe de se connecter à leur ordinateur sans l'aide du support. Les utilisateurs peuvent accéder de nouveau à leur ordinateur même si aucune connexion téléphonique ou réseau n'est disponible (à bord d'un avion, par exemple). Pour se connecter, ils doivent répondre à un certain nombre de questions prédéfinies dans l'authentification au démarrage.

Local Self Help réduit le nombre d'appels de récupération de connexion, réduisant ainsi les tâches de routine du personnel de support et lui permettant de se concentrer sur des demandes plus complexes.

■ **Récupération par Challenge/Réponse**

Le mécanisme Challenge/Réponse est un système de récupération de connexion sécurisé et fiable qui vient en aide aux utilisateurs qui ne peuvent pas se connecter à leur ordinateur ou accéder aux données chiffrées. Lors de la procédure Challenge/Réponse, l'utilisateur communique le code de challenge généré sur l'ordinateur final au responsable du support qui générera à son tour un code de réponse. Ce code autorisera l'utilisateur à exécuter une action spécifique sur l'ordinateur. Grâce à la récupération par Challenge/Réponse, Sophos SafeGuard propose plusieurs flux de travail pour les scénarios de récupération classiques nécessitant l'aide du support.

■ **Récupération du système**

Sophos SafeGuard propose divers outils et méthodes destinés à la récupération du système, notamment Windows PE personnalisé par Sophos SafeGuard ou Lenovo Rescue and Recovery. Grâce à ces outils, les problèmes liés au système Windows et aux composants Sophos SafeGuard peuvent être résolus.

■ **Fichier de récupération de clé**

La récupération par Challenge/Réponse ainsi que la récupération du système reposent sur un fichier de récupération de clé créé pour chaque ordinateur chiffré par Sophos SafeGuard et généralement stocké sur un partage réseau. Cette clé de récupération garantit que le processus de récupération n'est pas utilisé pour contourner la protection des données. Pour davantage de sécurité, cette clé est également chiffrée. Le partage réseau, ainsi que les droits d'accès requis pour ce partage, sont créés automatiquement au cours de la configuration initiale.

3 Mise à niveau de Sophos SafeGuard Disk Encryption 4.60

De nombreuses améliorations ont été apportées à Sophos SafeGuard Disk Encryption (SDE) 5.50. Parmi elles, une aide pour chiffrer les ordinateurs utilisant Windows Vista et Windows 7 (32 et 64 bits).

Les ordinateurs déjà chiffrés à l'aide de SDE 4.60 peuvent être mis à niveau vers SDE 5.50. Les volumes chiffrés restent inchangés et les clés de chiffrement sont automatiquement converties dans un format compatible avec la version 5.50.

Avant de mettre à niveau les ordinateurs chiffrés vers Sophos SafeGuard 5.50, un nouveau package de configuration de stratégie doit être créé à l'aide de SafeGuard Policy Editor et déployé en même temps que le logiciel Sophos SafeGuard 5.50.

Pour plus d'informations, reportez-vous à l'aide de l'administrateur de Sophos SafeGuard, chapitre *Mise à niveau de SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x vers Sophos SafeGuard 5.50* ou <http://www.sophos.com/support/knowledgebase/article/108561.html>.

4 Mise à niveau des versions de SafeGuard Easy 4.x

De nombreuses améliorations ont été apportées à Sophos SafeGuard Easy (SGE) 5.50. Parmi elles, une aide pour chiffrer les ordinateurs utilisant Windows Vista et Windows 7 (32 et 64 bits).

Les ordinateurs déjà chiffrés à l'aide de SGE versions 4.3x à 4.5x peuvent être mis à niveau vers SGE 5.50. Les volumes chiffrés restent inchangés et les clés de chiffrement sont automatiquement converties dans un format compatible avec la version 5.50.

SGE 5.50 utilise par ailleurs SafeGuard Policy Editor, un outil d'administration non compatible avec SGE 4.5x. Avant de mettre à niveau les ordinateurs chiffrés vers Sophos SafeGuard 5.50, un nouveau package de configuration de stratégie doit être créé à l'aide de SafeGuard Policy Editor et déployé en même temps que le logiciel Sophos SafeGuard 5.50.

Pour plus d'informations, reportez-vous à l'aide de l'administrateur de Sophos SafeGuard, chapitre *Mise à niveau de SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x vers Sophos SafeGuard 5.5x*. Pour en savoir plus, voir <http://www.sophos.com/support/knowledgebase/article/108561.html>.

5 Quelles sont les étapes clés ?

Il est recommandé d'installer Sophos SafeGuard Disk Encryption sur un serveur Windows avant de déployer le logiciel de chiffrement sur les ordinateurs à l'aide d'un outil de déploiement de logiciel tel que Microsoft System Center Configuration Manager. Les étapes clés sont les suivantes :

- Vérification de la configuration minimale du système.
- Préparation de l'installation.
- Installation de SafeGuard Policy Editor, utilisé pour la configuration des stratégies et les tâches du support.
- Réalisation de la configuration initiale.
- Réalisation d'une configuration supplémentaire pour le logiciel de chiffrement.
- Installation du logiciel de chiffrement et de la configuration de chiffrement sur les ordinateurs finaux.

6 Vérification de la configuration minimale du système

6.1 Configuration minimale des outils d'administration

Matériel

- Intel ou AMD X86 CPU
- 1 Go de RAM
- 1 Go d'espace disque disponible (recommandé)

Logiciel

Sauf mention contraire, les versions 32 et 64 bits des systèmes d'exploitation suivants sont prises en charge. Il est recommandé d'installer les derniers service packs suivants :

- Microsoft Windows XP Professionnel (32 bits)
- Microsoft Windows 2003 Server
- Microsoft Windows 2003 Server R2
- Microsoft Windows Vista
- Microsoft Windows 2008 Server
- Microsoft Windows 2008 Server R2
- Microsoft Windows 7

Microsoft ASP.net : .NET Framework 3.0 SP1

6.2 Configuration minimale de la base de données

Les versions 32 et 64 bits prises en charge sont les suivantes :

- Microsoft SQL Server 2005 SP2, SP3
- Microsoft SQL Server 2005 Express SP2, SP3
- Microsoft SQL Server 2008
- Microsoft SQL Server 2008 Express

6.3 Configuration minimale des ordinateurs protégés par Sophos SafeGuard

Matériel

- Intel ou AMD X86 CPU
- 512 Mo de RAM (minimum), 1 024 Mo (recommandé pour Windows Vista)
- L'installation requiert au moins 300 Mo d'espace disque disponible dont 100 Mo doivent se trouver sur une zone contiguë. Si vous ne disposez pas de 5 Go d'espace disque disponible ou si votre système d'exploitation n'a pas été installé récemment, défragmentez votre système avant de procéder à l'installation afin de garantir que vous disposez de cette zone contiguë. Le cas échéant, un espace disponible contigu insuffisant risque de provoquer l'échec de l'installation.

Logiciel

Sauf mention contraire, les versions 32 et 64 bits des systèmes d'exploitation suivants sont prises en charge. Il est recommandé d'installer les derniers service packs suivants :

- Microsoft Windows XP Professionnel (32 bits uniquement)
- Microsoft Windows Vista éditions Entreprise, Intégrale, Professionnel ou Familiale Premium (Vista n'est pas pris en charge sans SP1)
- Microsoft Windows 7

Restrictions

- Si vous utilisez le mécanisme Intel Advanced Host Controller Interface (AHCI) sur l'ordinateur, le disque dur d'initialisation doit être installé dans le slot 0 ou le slot 1. Vous pouvez insérer jusqu'à 32 disques durs. Sophos SafeGuard ne s'exécute que sur les deux premiers numéros de slot.
- Les disques dynamiques et les disques de table de partition GUID (GPT) ne sont pas pris en charge. Dans ces cas-là, l'installation est interrompue. Si de tels disques sont trouvés sur l'ordinateur ultérieurement, ils ne sont pas pris en charge.
- Le module Sophos SafeGuard Device Encryption ne prend pas en charge les systèmes équipés de disques durs reliés via un bus SCSI.

7 Préparation de l'installation

Avant de procéder au déploiement de Sophos SafeGuard, il est recommandé d'exécuter les étapes préparatoires suivantes :

7.1 Considérations générales

- Si vous souhaitez installer Sophos SafeGuard via un déploiement centralisé, nous vous recommandons de configurer une liste de comptes de service. Une fois qu'un administrateur informatique a été ajouté à la liste de comptes de service, il peut se connecter aux ordinateurs sur lesquels Sophos SafeGuard est installé, et ce, sans activer l'authentification au démarrage. Cette opération est fortement recommandée car, par défaut, le premier utilisateur qui se connecte à l'ordinateur final après l'installation est considéré, dans l'authentification au démarrage, comme étant le compte principal. Pour plus d'informations, voir [Configuration des listes de comptes de service](#), à la page 27.
- Un déploiement centralisé de Sophos SafeGuard peut être effectué grâce à une vaste gamme d'outils de gestion/déploiement, notamment Microsoft SCCM/SMS, IBM Tivoli ou Enteo Netinstall.
- Vous pouvez ou non utiliser la configuration de stratégie par défaut recommandée et fournie avec Sophos SafeGuard. Pour un récapitulatif des stratégies par défaut, voir [Réalisation d'une configuration supplémentaire pour le logiciel de chiffrement](#), à la page 17. Pour obtenir une analyse détaillée des stratégies par défaut, reportez-vous au chapitre *Stratégies par défaut* de l'aide de l'administrateur.
- Si vous souhaitez utiliser un éveil par appel réseau, vous devez d'abord le configurer via une stratégie du type **Paramètres de machine spécifiques**. Pour plus d'informations, consultez le chapitre *Paramètres de stratégie* de l'aide de l'administrateur.
- Sophos SafeGuard peut être configuré pour enregistrer les journaux de chiffrement et d'installation sur un emplacement du réseau (chemin UNC). L'administrateur peut ainsi analyser le processus de chiffrement depuis un emplacement central. Pour plus d'informations, voir [Installation du logiciel de chiffrement et de la configuration de chiffrement à l'aide d'un script](#), à la page 33.

7.2 Préparation générale

- Pour installer le logiciel de chiffrement et utiliser les outils d'administration Sophos SafeGuard, vous devez disposer des droits d'administrateur Windows.
- Lisez attentivement les Notes de version.

7.3 Préparation des ordinateurs au chiffrement

- Un compte utilisateur doit être configuré et actif sur l'ordinateur. L'utilisateur doit disposer d'un mot de passe.
- Fermez toutes les applications ouvertes.
- Vérifiez que l'espace disque disponible est suffisant.
- Créez une sauvegarde complète des données sur l'ordinateur.
- Sophos fournit une liste des configurations matérielles afin de réduire le risque de conflits entre l'authentification au démarrage et le matériel de votre ordinateur. La liste est fournie avec le package d'installation du logiciel de chiffrement.

Il est recommandé d'installer une version à jour du fichier de configuration matérielle avant de procéder au déploiement de Sophos SafeGuard. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant :

<ftp://POACFG:POACFG@ftp.ou.utimaco.de>

Pour en savoir plus, voir la section *Raccourcis clavier pris en charge dans l'authentification au démarrage* de l'aide de l'administrateur, ainsi que l'article suivant :

<http://www.sophos.com/support/knowledgebase/article/65700.html>.

- Recherchez les erreurs sur le ou les disques durs à l'aide de la commande suivante :

```
chkdsk %drive% /F /V /L /X
```

Dans certains cas, vous pouvez être invité à redémarrer votre ordinateur et à réexécuter la commande chkdsk. Vous trouverez plus d'informations sur ce sujet dans la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/107081.html>.

- Utilisez la fonction de défragmentation de Windows pour localiser et consolider les éléments fragmentés, notamment les fichiers d'initialisation, les fichiers de données et les dossiers sur les volumes locaux.

```
defrag %drive%
```

Vous trouverez plus d'informations sur ce sujet dans la base de connaissances :

<http://www.sophos.com/support/knowledgebase/article/109226.html>

- Désinstallez les gestionnaires d'initialisation tiers, tels que PRONetworks Boot Pro et Boot-US.
- Si vous avez utilisé un outil d'imagerie/de clonage, nous vous recommandons de remplacer le MBR. Pour installer Sophos SafeGuard, votre MBR (Master Boot Record) doit être unique et sain. Il se peut que, suite à l'utilisation d'outils d'image/de clone, le MBR ne soit plus sain.

Vous pouvez nettoyer le MBR (Master Boot Record) en démarrant à partir d'un CD Windows et en exécutant la commande FIXMBR dans la Console de récupération Windows.

Pour en savoir plus, consultez la base de connaissances :

<http://www.sophos.com/support/knowledgebase/article/108088.html>

- Si la partition d'initialisation a été convertie du format FAT au format NTFS, mais que le système n'a pas encore été redémarré, vous ne devez pas installer Sophos SafeGuard. Il se peut que l'installation ne soit pas terminée car le système de fichiers était encore au format FAT lors de l'installation mais que c'est le format NTFS qui a été détecté au moment de l'activation. Dans ce cas, vous devez redémarrer l'ordinateur une fois avant d'installer Sophos SafeGuard.

8 Installation de SafeGuard Policy Editor

Avant de déployer le logiciel de chiffrement sur les ordinateurs finaux, vous devez d'abord installer SafeGuard Policy Editor sur un serveur Windows. Ensuite, vous pourrez l'installer sur plusieurs ordinateurs d'administrateurs connectés à la base de données Sophos SafeGuard centrale du serveur. Le même compte doit être utilisé pour accéder à chaque instance de SafeGuard Policy Editor.

Conditions préalables : .NET Framework 3.0 Service Pack 1 doit être installé sur le serveur Windows. Vous pouvez le télécharger gratuitement sur le site <http://www.microsoft.com/downloads>.

1. Connectez-vous à votre ordinateur en tant qu'administrateur.
2. À partir du dossier d'installation du produit, installez l'un des éléments suivants. Un assistant vous guidera tout au long des étapes nécessaires.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
Double-cliquez sur SDEPolicyEditor.msi.	Double-cliquez sur SGNPolicyEditor.msi.

3. Acceptez les valeurs par défaut dans les boîtes de dialogue qui s'affichent.

Installation de la base de données : Une instance de base de données SQL est utilisée pour stocker les paramètres de stratégie de Sophos SafeGuard. Il se peut que vous soyez invité à installer Microsoft SQL Server 2005 Express lors de l'installation de SafeGuard Policy Editor si aucune instance existante de la base de données SQL n'est disponible. Dans ce cas, vos informations d'identification Windows sont utilisées comme compte utilisateur SQL.

4. Cliquez sur **Terminer** pour terminer l'installation.

SafeGuard Policy Editor est installé. Ensuite, vous pouvez effectuer la configuration initiale dans SafeGuard Policy Editor.

9 Réalisation de la configuration initiale

Vous devez disposer des droits d'administrateur Windows pour réaliser la configuration initiale avec SafeGuard Policy Editor.

1. Démarrez SafeGuard Policy Editor. L'assistant de configuration démarre et vous guide tout au long des étapes nécessaires.
2. Cliquez sur **Suivant** pour confirmer la page de **Bienvenue**.
3. Dans la page **Base de données**, l'instance de base de données SQL sélectionnée ou créée lors de l'installation de SafeGuard Policy Editor s'affiche. Cliquez sur **Suivant** pour confirmer les valeurs par défaut. La base de données est créée.
4. Dans la page **Responsable de la sécurité**, le nom de ce dernier est déjà affiché. Saisissez et confirmez le mot de passe que vous utiliserez pour accéder à SafeGuard Policy Editor. Cliquez sur **Suivant** pour confirmer les valeurs par défaut. Le certificat du responsable de la sécurité est créé.

Conservez le mot de passe en lieu sûr. Si vous le perdez, vous ne pourrez plus accéder à SafeGuard Policy Editor. Le personnel du support informatique doit disposer d'un accès au compte afin de pouvoir exécuter les tâches de récupération.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
Le nom pour le responsable de la sécurité est toujours administrateur.	Le nom de l'utilisateur actuel est affiché.

5. Dans la page **Entreprise**, saisissez le **Nom de l'entreprise**. Cliquez sur **Suivant** pour confirmer la valeur par défaut. Le certificat de l'entreprise est créé.
Vous pouvez également importer le certificat s'il s'agit d'une réinstallation.
6. Cliquez sur **Suivant** pour confirmer la valeur par défaut de la page **Sauvegarde de certificat**. Assurez-vous d'exporter les certificats vers un emplacement accessible à des fins de récupération (sur une carte mémoire par exemple), immédiatement après la configuration initiale. Conservez-les en lieu sûr. Vous en aurez besoin pour restaurer une installation défectueuse ou une base de données corrompue. Pour plus d'informations, consultez l'aide de l'administrateur.
7. Cliquez sur **Suivant** pour confirmer les valeurs par défaut de la page **Stratégie par défaut**. Les stratégies par défaut recommandées, ainsi qu'un package de configuration (standard-packet.msi) contenant ces stratégies par défaut, sont créés.

Les stratégies par défaut recommandées comprennent le chiffrement des volumes de disques durs internes, l'activation de l'authentification au démarrage et les paramètres permettant la récupération locale et à distance. Pour plus de détails, voir [Réalisation d'une configuration supplémentaire pour le logiciel de chiffrement](#), à la page 17 et l'aide de l'administrateur, au chapitre Stratégies par défaut. Les stratégies par défaut ne peuvent être créées que lors de la configuration initiale dans l'assistant de configuration de SafeGuard Policy Editor. Vous pouvez les modifier ultérieurement ou créer de nouvelles stratégies définies par l'utilisateur.

8. Dans la page **Clés de récupération**, activez l'option **Créer un partage réseau**. Cliquez sur **Suivant** pour accepter les autorisations par défaut.

Cette opération permet de créer un partage réseau SafeGuardRecoveryKeys\$ et un répertoire sur le serveur ou l'ordinateur local sur lequel seront automatiquement enregistrées les clés de récupération. Elle permet également de fournir au support les droits d'accès appropriés au partage de clés de récupération. Si l'option **Créer un partage réseau** n'est pas activée, l'utilisateur final sera invité à indiquer un emplacement d'enregistrement des fichiers de clés de récupération à la fin du chiffrement.

Remarque: Le logiciel Sophos SafeGuard tentera de se connecter au partage réseau pendant 4 minutes environ. En cas d'échec, une infobulle s'affichera sur l'ordinateur et une erreur sera consignée dans le journal. D'autres tentatives de connexion au partage réseau seront effectuées après chaque connexion Windows jusqu'à ce que la connexion soit établie ou que les fichiers de clés de récupération soient sauvegardés manuellement sur l'ordinateur.

9. Cliquez sur **Suivant**. Cliquez ensuite sur **Terminer** pour terminer la configuration. SafeGuard Policy Editor se lance à la fermeture de l'assistant de configuration.

La configuration initiale est terminée. Vous avez créé un package de configuration avec un ensemble de stratégies par défaut ainsi qu'un partage de clés de récupération avec les droits d'accès appropriés pour le support. Il est recommandé de consulter les chapitres restants du Guide de démarrage avant le déploiement de Sophos SafeGuard et du package de configuration de stratégies par défaut sur les ordinateurs finaux. Pour obtenir plus d'informations sur le déploiement, reportez-vous au chapitre voir [Installation du logiciel de chiffrement et de la configuration de chiffrement à l'aide d'un script](#), à la page 33.

10 Réalisation d'une configuration supplémentaire pour le logiciel de chiffrement

Les stratégies Sophos SafeGuard incluent tous les paramètres nécessaires pour mettre en œuvre une stratégie de sécurité sur les ordinateurs finaux à l'échelle de l'entreprise. Elles comportent des paramètres pour les zones suivantes (types de stratégie) :

Type de stratégie	Contenu	SDE	SGE
Paramètres généraux	Paramètres de la récupération de connexion, personnalisation de l'authentification au démarrage, etc.	✓	✓
Authentification	Paramètres du mode de connexion, nombre de tentatives de connexion, etc.	✓	✓
Mots de passe	Paramètres des mots de passe utilisateur (longueur, caractères interdits).	✓	✓
Protection du périphérique	Paramètres de chiffrement (sélection de volume).	Paramètres du chiffrement basé sur volume.	Paramètres du chiffrement basé sur volume ou sur fichier (SafeGuard Data Exchange et SafeGuard Portable).
Paramètres machine spécifiques	Paramètres de l'ordinateur, notamment l'authentification au démarrage (activer/désactiver), l'éveil par appel réseau sécurisé, les options d'affichage, etc.	✓	✓
Consignation	Définit les événements à consigner.	✓	✓
Passphrase	Paramètres des passphrases SafeGuardData Exchange.		✓

Grâce aux stratégies de configuration par défaut, vos ordinateurs finaux sont bien protégés :

- L'authentification au démarrage est activée.
- Le chiffrement basé sur volume de tous les disques durs internes est activé.
- La récupération du mot de passe via Local Self Help en cas d'oubli est activée et configurée.
- Par ailleurs, la récupération de mot de passe par Challenge/Réponse avec aide du support est activée.
- Le fichier de récupération de clé requis est généré automatiquement sur chaque ordinateur protégé par Sophos SafeGuard. Il est ensuite stocké dans un partage réseau créé lors de la configuration initiale. Les autorisations d'accès à ce partage sont configurées par défaut.
- pour SafeGuard Easy 5.50 : le chiffrement basé sur fichier des supports amovibles est activé.

La configuration par défaut ne couvre pas les zones suivantes. Vous devez donc les traiter avant de déployer les stratégies.

- Pour fournir un accès spécial destiné à la post-installation et aux tâches administratives sur les ordinateurs finaux, vous pouvez créer des options d'accès administratifs : comptes de service et comptes d'accès POA.
- Définissez des paramètres avancés. Par exemple, définissez vos propres questions pour Local Self Help.
- Pour récupérer les données lorsque l'authentification au démarrage est corrompue, créez des fichiers spéciaux (clients virtuels) requis pour la procédure Challenge/Réponse via un environnement WinPE.
- Personnalisez l'authentification au démarrage selon les préférences de votre entreprise.

10.1 Création de stratégies

Pour créer une stratégie, procédez comme suit :

1. Connectez-vous à SafeGuard Policy Editor à l'aide du mot de passe défini lors de la configuration initiale.
2. Cliquez sur **Stratégies** dans la zone de navigation.
3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis sélectionnez **Nouveau**.
4. Sélectionnez le type de stratégie. Une boîte de dialogue pour nommer la stratégie du type de stratégie sélectionné s'affiche.

5. Entrez le nom et éventuellement la description de la nouvelle stratégie.

Stratégies de protection du périphérique :

Lors de la création d'une stratégie de protection du périphérique, vous devez également spécifier la cible de la protection du périphérique dans cette boîte de dialogue. Les cibles possibles sont les suivantes:

- stockage de masse (volumes d'initialisation/autres volumes);
- supports amovibles (uniquement pris en charge pour les installations de SafeGuard Easy) ;
- lecteurs optiques (uniquement pris en charge pour les installations de SafeGuard Easy).

Une stratégie distincte doit être créée pour chaque cible. Vous pouvez ultérieurement combiner les stratégies individuelles dans un groupe de stratégies nommé *Chiffrement* par exemple.

6. Cliquez sur **OK**.

La nouvelle stratégie s'affiche dans la fenêtre de navigation **Stratégies**, sous **Éléments de stratégie**, à gauche. Tous les paramètres du type de stratégie sélectionné s'affichent dans la zone d'action, à droite, et peuvent être modifiés au besoin.

10.2 Combinaison de stratégies dans des groupes

Conditions préalables :

Les stratégies individuelles de différents types doivent être tout d'abord créées.

Les stratégies Sophos SafeGuard doivent être combinées dans des groupes de stratégies afin d'être transférées dans un package de configuration. Un groupe de stratégies peut contenir différents types de stratégies.

Pour grouper des stratégies, procédez comme suit :

1. Cliquez sur **Stratégies** dans la zone de navigation.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Groupes de stratégies** et sélectionnez **Nouveau**.
3. Cliquez sur **Nouveau groupe de stratégies**. Une boîte de dialogue pour nommer le groupe de stratégies s'affiche.
4. Entrez un nom unique et, éventuellement, la description du groupe de stratégies. Cliquez sur **OK**.

5. Le nouveau groupe de stratégies s'affiche dans la **fenêtre de navigation** sous **Groupes de stratégies**.
6. Sélectionnez le groupe de stratégies. La zone d'action indique tous les éléments requis pour regrouper les stratégies.
7. Pour ajouter les stratégies au groupe, glissez-les de la liste de stratégies disponibles dans la zone de stratégies.
8. Vous pouvez définir une **priorité** pour chaque stratégie en les organisant grâce au menu contextuel.

Si vous rassemblez des stratégies du même type dans un groupe, les paramètres sont fusionnés automatiquement. Dans ce cas, vous pouvez définir des priorités d'utilisation des paramètres. Les paramètres d'une stratégie ayant une priorité supérieure remplacent ceux d'une stratégie de priorité inférieure. Si une option est définie sur **non configuré**, le paramètre **ne sera pas remplacé** dans une stratégie de priorité inférieure.

Exception relative à la protection du périphérique:

Les stratégies de protection du périphérique seront fusionnées uniquement si certaines sont définies pour la même cible (volume d'initialisation par exemple). Les paramètres sont ajoutés si elles pointent des cibles différentes.

9. Enregistrez la stratégie via **Fichier > Enregistrer**.

Le groupe de stratégies contient désormais les paramètres de toutes les stratégies individuelles. Ensuite, vous pouvez créer un package de configuration qui inclut le groupe de stratégies.

10.3 Création d'un package de configuration Sophos SafeGuard

Remarque: Les stratégies sont transférées vers les ordinateurs finaux via un package de configuration. Après avoir créé une nouvelle stratégie ou modifié une stratégie existante, assurez-vous de bien exécuter les étapes suivantes. Un package de configuration est créé automatiquement lors de la configuration initiale, uniquement si vous utilisez les stratégies par défaut. Dans ce cas, il n'est pas nécessaire de réaliser les étapes suivantes.

Pour créer un package de configuration, procédez comme suit :

1. Dans SafeGuard Policy Editor, dans le menu **Outils**, sélectionnez l'**Outil de package de configuration**.
2. Cliquez sur **Ajouter un package de configuration**.
3. Donnez un nom au package de configuration.

4. Spécifiez le **Groupe de stratégies** préalablement créé dans SafeGuard Policy Editor et que vous souhaitez appliquer aux ordinateurs.
5. Sous **Emplacement de la sauvegarde de la clé**, spécifiez un chemin réseau partagé pour le stockage du fichier de récupération de clé. Entrez le chemin de partage sous la forme suivante : \\networkcomputer\, par exemple « \\mycompany.edu\ ». Si vous ne spécifiez pas de chemin ici, l'utilisateur final sera invité à indiquer l'emplacement de stockage de ce fichier lors de sa première connexion à l'ordinateur final, suite à l'installation.

Le fichier de récupération de clé est requis pour activer la récupération des ordinateurs protégés par Sophos SafeGuard. Il est généré sur chaque ordinateur protégé par Sophos SafeGuard.

Veillez à enregistrer le fichier de récupération de clé dans un emplacement accessible au support, un chemin réseau partagé par exemple. Les fichiers peuvent également être fournis au support à l'aide de différents mécanismes. Ce fichier est chiffré par le certificat d'entreprise. Il peut donc être enregistré sur un support externe ou sur le réseau pour être fourni au support à des fins de récupération. Il peut également être envoyé par e-mail.
6. Sous **Groupe POA**, vous pouvez sélectionner le groupe de comptes d'accès POA que vous souhaitez affecter à l'ordinateur final. Une fois l'authentification au démarrage activée, les comptes d'accès POA fournissent un accès à l'ordinateur final pour effectuer des tâches administratives. Pour attribuer des comptes d'accès POA, le groupe POA doit avoir été préalablement créé dans la zone **Utilisateurs** de SafeGuard Policy Editor.
7. Spécifiez un chemin de sortie pour le package de configuration (MSI).
8. Cliquez sur **Créer un package de configuration**.

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer ce package aux ordinateurs finaux Sophos SafeGuard et le déployer sur ceux-ci.

10.4 Configuration de Local Self Help

Local Self Help permet aux utilisateurs ayant oublié leur mot de passe de le récupérer, sans recourir à un quelconque support. Pour ce faire, ils doivent simplement répondre à un nombre prédéfini de questions dans l'authentification au démarrage. Vous pouvez définir l'ensemble des questions qui attendent une réponse dans SafeGuard Policy Editor. Un sujet de question prédéfini est également proposé. Vous pouvez aussi accorder aux utilisateurs le droit de définir des questions personnalisées.

Remarque: Local Self Help est déjà configuré avec les questions prédéfinies dans les stratégies par défaut. Si vous utilisez les stratégies par défaut, les étapes de configuration suivantes ne sont pas requises.

Pour configurer des paramètres Local Self Help spécifiques, effectuez la procédure suivante :

1. Dans la zone de navigation de SafeGuard Policy Editor, cliquez sur **Stratégies**.
2. Créez une nouvelle stratégie du type **Paramètres généraux**.
3. Définissez les paramètres de Local Self Help sous **Local Self Help (LSH)** :
 - a) Dans le champ **Activer Local Self Help**, sélectionnez **Oui**.
 - b) Dans le champ **Longueur minimale des réponses**, définissez le nombre minimal de caractères que l'utilisateur doit saisir lorsqu'il répond pour la première fois aux questions.
 - c) Dans le champ **Texte de bienvenue sous Windows**, vous pouvez spécifier le texte d'information à afficher dans la première boîte de dialogue au démarrage de l'assistant de Local Self Help sur l'ordinateur final. Avant de pouvoir sélectionner le texte ici, il doit être créé et enregistré. Pour obtenir une description détaillée de la création et de l'enregistrement de textes d'information, reportez-vous à la section *Enregistrement de textes de bienvenue* de l'aide de l'administrateur.
 - d) Pour autoriser les utilisateurs à définir des questions personnalisées, sélectionnez l'option **Oui** dans le champ **L'utilisateur peut définir des questions personnalisées**.

Après avoir défini les paramètres de stratégie pour l'activation de Local Self Help sur les ordinateurs finaux, définissez un sujet de question à déployer avec la stratégie.

Dans la zone de navigation **Stratégies**, un sujet de question prédéfini est proposé sous **Questions Local Self Help**. Vous pouvez l'utiliser tel quel, le modifier ou le supprimer. Les étapes suivantes décrivent les procédures de création d'un sujet de question et d'ajout de questions.

4. Dans la zone de navigation **Stratégies**, sélectionnez **Questions Local Self Help**.
5. Cliquez avec le bouton droit de la souris sur **Questions Local Self Help**, puis sélectionnez **Nouveau > Sujet de la question**.
6. Saisissez un nom pour le sujet de question et cliquez sur **OK**.
7. Dans la zone de navigation **Stratégies**, sélectionnez le nouveau sujet de question sous **Questions Local Self Help**.
8. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel du sujet de question. Dans le menu contextuel, sélectionnez **Ajouter**.

Une nouvelle ligne de question est ajoutée.

9. Saisissez votre question et appuyez sur **Entrée**. Répétez cette étape pour ajouter d'autres questions.

Le sujet de la question doit contenir au moins 10 questions.

10. Pour enregistrer vos modifications, cliquez sur l'icône **Enregistrer** dans la barre d'outils.

Votre sujet de question est enregistré et est automatiquement déployé avec la stratégie du type **Paramètres généraux**, activant Local Self Help sur les ordinateurs finaux.

11. Ajoutez la stratégie au groupe de stratégies à déployer sur les ordinateurs finaux dans le package de configuration.

Le groupe de stratégies contenant la stratégie de type **Paramètres généraux** peut être sélectionné lors de la création d'un package de configuration (via **Outils > Outil de package de configuration**), pour déploiement sur les ordinateurs finaux. Local Self Help est activé sur l'ordinateur final via ce groupe de stratégies. Pour pouvoir utiliser Local Self Help, l'utilisateur doit d'abord activer cette fonction en répondant à dix questions minimum (voir [Activation de Local Self Help sur l'ordinateur final](#), à la page 23).

10.4.1 Activation de Local Self Help sur l'ordinateur final

Pour activer Local Self Help sur les ordinateurs finaux, l'utilisateur doit répondre à dix questions minimum et les stocker.

1. Une fois la stratégie devenue effective sur l'ordinateur final, une infobulle indique qu'il existe des questions Local Self Help sans réponse. L'utilisateur redémarre l'ordinateur.

La commande **Local Self Help** est ajoutée au menu contextuel de l'icône de la barre d'état système dans la barre des tâches Windows.

2. L'utilisateur effectue un clic droit sur l'icône de la barre d'état système de Sophos SafeGuard et sélectionne **Local Self Help**.

La boîte de dialogue **Bienvenue dans l'assistant Local Self Help** s'affiche. L'assistant de Local Self Help guide l'utilisateur dans les étapes du processus de réponse aux questions et de stockage de ces dernières.

Local Self Help est activé sur l'ordinateur final à la fin du processus de l'assistant.

10.5 Configuration de la procédure Challenge/Réponse pour la récupération des données

Les volumes chiffrés peuvent être récupérés facilement grâce à des fichiers spécifiques appelés clients virtuels, dans les cas où la procédure Challenge/Réponse n'est pas prise en charge, par exemple lorsque l'authentification au démarrage est corrompue. Ils peuvent être utilisés par différents ordinateurs et pour plusieurs sessions de challenge/réponse.

Les fichiers du client virtuel doivent être créés et mis à disposition du support avant la réalisation de la procédure Challenge/Réponse.

1. Dans SafeGuard Policy Editor, sélectionnez la zone **Clients virtuels**.
2. Dans la fenêtre de navigation située à gauche, cliquez sur **Clients virtuels**.
3. Dans la barre d'outils, cliquez sur **Ajouter un client virtuel**.
4. Entrez un nom unique pour le client virtuel et cliquez sur **OK**. Les clients virtuels sont identifiés dans la base de données par ces noms.
5. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.
6. Sélectionnez le client virtuel correspondant dans la zone d'action et cliquez sur **Exporter le client virtuel** dans la barre d'outils. Sélectionnez un emplacement de stockage pour le fichier du client virtuel `recoverytoken.tok`, puis cliquez sur **OK** pour confirmer.

Le client virtuel a été exporté vers le fichier `recoverytoken.tok`.

7. Copiez le fichier du client virtuel `recoverytoken.tok` sur un support amovible. Nous recommandons d'utiliser une carte mémoire.

Veillez à conserver ce support de stockage en lieu sûr. Mettez les fichiers à disposition du support et rendez-les accessibles dans l'environnement de l'ordinateur final puisqu'ils sont requis pour une procédure Challenge/Réponse avec des clients virtuels.

10.6 Personnalisation de l'authentification au démarrage

Vous pouvez personnaliser l'apparence de l'authentification au démarrage selon vos préférences, notamment les images d'arrière-plan/de connexion, le texte d'information, le clavier ou la langue utilisée. Créez préalablement des images et des textes et enregistrez-les dans SafeGuard Policy Editor. Le reste de la configuration est effectué via les stratégies.

Vous pouvez configurer l'authentification au démarrage comme suit :

■ Image d'arrière-plan et de connexion

Par défaut, les images d'arrière-plan et de connexion qui s'affichent dans l'authentification au démarrage sont conçues selon SafeGuard. Ces images peuvent être personnalisées pour afficher le logo de votre entreprise, par exemple.

Les images d'arrière-plan et de connexion sont configurées via une stratégie du type

Paramètres généraux.

Pour obtenir une description détaillée, reportez-vous à la section *Image d'arrière-plan et de connexion* de l'aide de l'administrateur.

■ Textes d'information personnalisés

Vous pouvez définir des textes d'information personnalisés à afficher dans l'authentification au démarrage, notamment les informations que vous souhaitez afficher lors du lancement d'une procédure Challenge/Réponse dans le cadre de la récupération de connexion, les mentions légales ou les informations supplémentaires à afficher après la connexion à partir de l'authentification au démarrage.

Ces textes sont configurés via des stratégies de type **Paramètres généraux** ou **Paramètres de machine spécifiques**.

Pour obtenir une description détaillée, reportez-vous à la section *Texte des informations défini par l'utilisateur dans l'authentification au démarrage (POA)* de l'aide de l'administrateur.

■ Langue du texte de la boîte de dialogue d'authentification au démarrage

Après l'installation du logiciel de chiffrement Sophos SafeGuard, le texte de la boîte de dialogue d'authentification au démarrage est affiché dans la langue par défaut, celle qui a été définie dans les Options régionales et linguistiques de Windows sur l'ordinateur final, lors de l'installation de Sophos SafeGuard.

Vous pouvez modifier le texte de la boîte de dialogue d'authentification au démarrage via une stratégie du type **Paramètres généraux**.

Pour obtenir une description détaillée, reportez-vous à la section *Langue du texte de la boîte de dialogue d'authentification au démarrage* de l'aide de l'administrateur.

■ **Disposition du clavier**

Par défaut, Sophos SafeGuard adopte la disposition du clavier de l'authentification au démarrage qui a été définie dans les **Options régionales et linguistiques** de Windows lors de l'installation.

Vous pouvez modifier la disposition du clavier dans les **Options régionales et linguistiques**.

Pour obtenir une description détaillée, reportez-vous à la section *Disposition du clavier* de l'aide de l'administrateur.

■ **Clavier virtuel**

Sophos SafeGuard propose un clavier virtuel qui permet de saisir les informations d'identification en cliquant sur les touches à l'écran.

Vous pouvez définir si vous souhaitez que le clavier virtuel soit disponible via une stratégie du type **Paramètres de machine spécifiques**.

Pour obtenir une description détaillée, reportez-vous à la section *Clavier virtuel* de l'aide de l'administrateur.

11 Configuration des accès administratifs sur les ordinateurs finaux

Afin de fournir l'accès nécessaire pour les tâches administratives après avoir installé Sophos SafeGuard sur les ordinateurs finaux, vous pouvez configurer les options d'accès administratif suivantes :

■ Comptes de service pour la connexion Windows

Grâce aux comptes de service, les utilisateurs (opérateurs chargés du déploiement ou membres de l'équipe informatique) peuvent se connecter (connexion Windows) aux ordinateurs finaux après l'installation de Sophos SafeGuard, et ce, sans avoir à activer l'authentification au démarrage et sans être ajoutés en tant qu'utilisateurs sur les ordinateurs.

■ Comptes d'accès POA pour connexion POA

Les comptes d'accès POA sont des comptes prédéfinis qui permettent aux utilisateurs (membres de l'équipe informatique, par exemple) de se connecter (connexion POA) à des ordinateurs finaux pour effectuer des tâches administratives après activation de l'authentification au démarrage.

Pour en savoir plus sur ces options, reportez-vous à l'aide de l'administrateur de Sophos SafeGuard, sections *Comptes de service pour la connexion Windows* et *Comptes d'accès POA pour la connexion POA*.

11.1 Configuration des listes de comptes de service

Procédez comme suit:

1. Dans la zone de navigation de SafeGuard Policy Editor, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation de la stratégie, sélectionnez **Listes de comptes de service**.
3. Dans le menu contextuel de l'option **Listes de comptes de service**, cliquez sur **Nouveau > Liste de comptes de service**.
4. Entrez un nom pour la liste de comptes de service, puis cliquez sur **OK**.
5. Sélectionnez la nouvelle liste sous **Listes de comptes de service** dans la fenêtre de navigation de la stratégie.
6. Cliquez avec le bouton droit de la souris dans la zone d'action, à droite, pour ouvrir le menu contextuel de la liste de comptes de service. Dans le menu contextuel, sélectionnez **Ajouter**.

7. Une nouvelle ligne utilisateur est ajoutée. Entrez le **Nom d'utilisateur** et le **Nom du domaine** dans les colonnes correspondantes, puis appuyez sur **Entrée**. Répétez cette étape pour ajouter d'autres utilisateurs.

8. Enregistrez vos modifications en cliquant sur l'icône **Enregistrer** de la barre d'outils.

La liste de comptes de service est désormais enregistrée. Dans les étapes suivantes, vous pouvez la sélectionner pour l'affecter via une stratégie.

9. Créez une stratégie du type **Authentification**.

10. Sous **Options de connexion**, sélectionnez la liste de comptes de service dans la liste déroulante du champ **Liste de comptes de service**.

11. Enregistrez vos modifications en cliquant sur l'icône **Enregistrer** de la barre d'outils.

12. Ajoutez la stratégie au groupe de stratégies à déployer sur les ordinateurs finaux dans le package de configuration.

Le groupe de stratégies contenant la stratégie **Authentification** peut être sélectionné lors de la création d'un package de configuration (via **Outils > Outil de package de configuration**), pour déploiement sur les ordinateurs finaux. Via ce groupe de stratégies, la liste de comptes de service est affectée à l'ordinateur final.

11.2 Configuration des comptes d'accès POA

Procédez comme suit:

1. Dans la zone de navigation de SafeGuard Policy Editor, cliquez sur **Utilisateurs**.
2. Dans la fenêtre de navigation **Utilisateurs**, sous **POA**, sélectionnez **Utilisateurs POA**.
3. Dans le menu contextuel des **Utilisateurs POA**, cliquez sur **Nouveau > Créer un utilisateur**.

La boîte de dialogue **Créer un utilisateur** s'affiche.

4. Dans le champ **Nom complet**, saisissez un nom, par exemple le nom de connexion du nouvel utilisateur POA. Vous pouvez également entrer une description pour le nouvel utilisateur POA.

5. Saisissez un mot de passe pour le nouveau compte d'accès POA et confirmez-le.

Remarque: Pour renforcer la sécurité, le mot de passe doit respecter des exigences de complexité minimales, à savoir une longueur minimale de 8 caractères, un mélange de caractères numériques et alphanumériques, etc. Si le mot de passe que vous avez entré est trop court, un message d'avertissement s'affichera.

6. Cliquez sur **OK**.

Le nouveau compte d'accès POA a été créé et l'utilisateur POA (compte d'accès POA) s'affiche sous **Utilisateurs POA** dans la zone de navigation **Utilisateurs**.

Répétez ces étapes pour créer d'autres utilisateurs POA.

Au cours des étapes suivantes, vous allez créer un groupe POA à sélectionner lors de la création de packages de configuration et ajouter les utilisateurs à ce groupe.

7. Dans la fenêtre de navigation **Utilisateurs**, sous **POA**, sélectionnez **Groupes POA**.

8. Dans le menu contextuel des **Groupes POA**, cliquez sur **Nouveau > Créer un groupe**.

La boîte de dialogue **Créer un groupe** s'affiche.

9. Dans le champ **Nom complet**, saisissez le nom du nouveau groupe POA. Vous pouvez également entrer une description pour le nouveau groupe POA.

10. Cliquez sur **OK**.

11. Dans la fenêtre de navigation **Utilisateurs**, sous **POA**, **Groupe POA**, sélectionnez le nouveau groupe POA.

Dans la zone d'action de SafeGuard Policy Editor, sur la droite, l'onglet **Membres** s'affiche.

12. Dans la barre d'outils de SafeGuard Policy Editor, cliquez sur l'icône **Ajouter** (signe « + » vert).

13. Sélectionnez l'utilisateur (compte d'accès POA) que vous souhaitez ajouter au groupe, puis cliquez sur **OK**. Répétez ces étapes pour ajouter d'autres utilisateurs.

Le groupe POA peut être sélectionné lors de la création du package de configuration (via **Outils > Outil de package de configuration**) à déployer sur les ordinateurs finaux.

12 Installation du logiciel de chiffrement et de la configuration de chiffrement sur les ordinateurs finaux

Procédez comme suit:

1. Avant d'installer le logiciel de chiffrement, préparez l'installation sur l'ordinateur final, voir [Préparation de l'installation](#), à la page 11.
2. Pour vous familiariser avec Sophos SafeGuard, commencez par installer le logiciel de chiffrement sur un ordinateur réservé à l'évaluation.
3. Connectez-vous une première fois.
4. Ensuite, utilisez vos propres outils pour créer et distribuer le package d'installation afin de configurer de manière centralisée le logiciel de chiffrement sur les ordinateurs finaux.

12.1 Installation d'une version d'évaluation

Avant d'installer le logiciel de chiffrement, préparez l'installation sur l'ordinateur final, voir [Préparation de l'installation](#), à la page 11.

1. Connectez-vous à l'ordinateur en tant qu'administrateur.
2. Installez le package MSI SGxClientPreinstall.msi qui fournit à l'ordinateur final la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement, et notamment les fichiers DLL requis.
3. Double-cliquez sur le package MSI « client » correspondant pour démarrer l'assistant d'installation du logiciel de chiffrement. Il vous guidera tout au long des étapes nécessaires. Installez l'un des produits suivants :

Sophos SafeGuard Disk Encryption	SafeGuard Easy
SDEClient.msi pour la variante 32 bits ou SDEClient_x64.msi pour la variante 64 bits.	SGNClient.msi pour la variante 32 bits. SGNClient_x64.msi pour la variante 64 bits. Pour plus de packages MSI client, consultez le chapitre <i>Installation</i> de l'aide de l'administrateur.

4. Acceptez les valeurs par défaut dans les boîtes de dialogue qui s'affichent.

5. Si vous y êtes invité, sélectionnez le type d'installation. Les clients installant SGNClient.msi ou SGNClient_x64.msi doivent exécuter l'une des actions suivantes :

- Sélectionnez **Complète** pour installer les composants Device Protection (chiffrement basé sur volume) et Data Exchange (chiffrement basé sur fichier).
- Sélectionnez **Standard** pour installer Device Protection uniquement.
- Sélectionnez **Personnalisée** pour activer les fonctions selon vos besoins.

La fonction **Data Exchange** n'est pas disponible avec SDE.

6. Acceptez les valeurs par défaut dans les boîtes de dialogue suivantes pour terminer l'assistant d'installation.

7. Accédez à l'emplacement d'enregistrement du package de configuration par défaut (MSI) créé lors de la configuration initiale dans SafeGuard Policy Editor.

8. Installez ce package de configuration sur l'ordinateur.

Sophos SafeGuard est installé sur l'ordinateur final avec une configuration par défaut. Effectuez ensuite votre première connexion à l'ordinateur après l'installation.

Une configuration supplémentaire peut être requise pour garantir que l'authentification au démarrage fonctionne correctement sur chaque plate-forme matérielle. La plupart des conflits matériels peuvent être résolus à l'aide de la fonctionnalité « Raccourcis clavier », intégrée à l'authentification au démarrage. Les raccourcis clavier peuvent être configurés après l'installation, depuis l'authentification au démarrage, ou via un paramètre de configuration supplémentaire transmis à l'outil de déploiement msiexec. Pour en savoir plus, voir la section *Raccourcis clavier pris en charge dans l'authentification au démarrage* de l'aide de l'administrateur, ainsi que les articles suivants :

<http://www.sophos.com/support/knowledgebase/article/107781.html>

<http://www.sophos.com/support/knowledgebase/article/107785.html>

12.2 Première connexion à un ordinateur final (sans compte de service)

1. Redémarrez l'ordinateur. La boîte de dialogue de connexion automatique Sophos SafeGuard s'affiche. La boîte de dialogue de connexion Windows s'affiche ensuite.

Sous Windows Vista et Windows 7, vous devez tout d'abord appuyer sur CTRL+ALT+SUPPR pour démarrer la connexion automatique et vous connecter. L'administrateur peut désactiver ce paramètre dans la console MMC de l'éditeur d'objet de stratégie de groupe sous Paramètres Windows > Paramètres de sécurité > Stratégies locales > Désactiver les options de sécurité (Enregistrement interactif : CTRL+ ALT+ SUPPR non nécessaire).
2. Saisissez votre nom d'utilisateur et votre mot de passe Windows.
3. Redémarrez de nouveau l'ordinateur. L'authentification au démarrage de Sophos SafeGuard est activée.
4. Saisissez votre nom d'utilisateur et votre mot de passe Windows. Vous êtes automatiquement connecté à Windows.

L'authentification au démarrage est maintenant activée. Vous êtes enregistré en tant qu'utilisateur Sophos SafeGuard. Une infobulle de confirmation s'affiche. À votre prochaine connexion, vous devrez uniquement entrer vos informations d'identification Windows à l'authentification au démarrage.

Le chiffrement initial démarrera automatiquement. Avec les stratégies par défaut, tous les disques internes seront chiffrés. Vous pouvez continuer à travailler et il n'est pas nécessaire de redémarrer l'ordinateur à la fin du chiffrement. Les disques seront chiffrés et déchiffrés en toute transparence pour des modifications sans interaction avec l'utilisateur. Pour obtenir plus d'informations sur le comportement de l'ordinateur après l'installation de Sophos SafeGuard, reportez-vous à l'aide de l'utilisateur (chapitres *Première connexion après l'installation de Sophos SafeGuard*, *Exemple de première connexion utilisateur à partir de l'authentification au démarrage* et *Chiffrement de données*).

12.3 Connexion à un ordinateur final à l'aide d'un compte de service

Lors de la première connexion à Windows après réinitialisation de l'ordinateur, un utilisateur figurant sur une liste de comptes de service se connecte à la machine concernée en tant qu'utilisateur invité Sophos SafeGuard. Cette première connexion Windows à la machine ne déclenche pas de procédure d'authentification au démarrage, de même qu'elle n'ajoute pas l'utilisateur à l'ordinateur. L'infobulle de l'icône de la barre d'état système de Sophos SafeGuard « Synchronisation utilisateur initiale terminée » ne s'affiche pas.

12.3.1 Affichage du statut du compte de service sur l'ordinateur final

Le statut de connexion de l'utilisateur invité est également disponible via l'icône de la barre d'état système. Pour en savoir plus sur l'icône de la barre d'état système, reportez-vous au chapitre *Icône de barre d'état et infobulle* de l'aide de l'utilisateur Sophos SafeGuard, (description du champ relatif à l'état de l'utilisateur).

12.4 Installation du logiciel de chiffrement et de la configuration de chiffrement à l'aide d'un script

Avant de déployer le logiciel de chiffrement, préparez l'installation sur les ordinateurs finaux, voir [Préparation pour l'installation](#), à la page 4.

Utilisez vos propres outils pour créer un package à installer sur les ordinateurs finaux. Le package doit contenir les éléments suivants :

- **Script avec les commandes de l'installation préconfigurée**

Nous recommandons d'utiliser msiexec, l'outil de ligne de commande de Windows Installer, pour créer le script. Pour en savoir plus sur msiexec, reportez-vous au chapitre *Commande pour l'installation centralisée* de l'aide de l'administrateur ou à [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

- **Package d'installation de préparation de Sophos SafeGuard**

Utilisez SGxClientPreinstall.msi. Le package fournit aux ordinateurs finaux la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement, notamment le fichier DLL MSVCR80.dll, version 8.0.50727.4053.

Remarque: Si ce package n'est pas installé, l'installation du logiciel de chiffrement échouera.

- **Sophos SafeGuard Package d'installation du logiciel de chiffrement Sophos SafeGuard**

Vous le trouverez dans le dossier du produit que vous avez téléchargé sur le site Web de Sophos ou sur le CD du produit.

- **Package(s) de configuration**

Il s'agit du ou des package(s) de configuration créé(s) préalablement dans SafeGuard Policy Editor. Ils contiennent les stratégies avec la configuration de chiffrement des ordinateurs finaux. Pour garantir un déploiement de stratégies rapide et facile, utilisez le package de configuration et les stratégies prédéfinies par défaut créées lors de la configuration initiale ou utilisez les stratégies que vous avez vous-même créées.

1. Sur l'ordinateur de l'administrateur, créez un dossier Logiciels pour centraliser toutes les applications.
2. Pour créer le script, entrez les commandes dans l'invite de commande avec les paramètres de ligne de commande, comme indiqué dans l'exemple suivant.

Exemple de script :

```
msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi /qn
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi /qn
/L*VX G:\Temp\Sophos\SafeGuard\%computername%\SDEClient_inst.log
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard
msiexec /i F:\Software\Sophos\SafeGuard\SDEClientConfig.msi /qn
```

■ **msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi**
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard

Cette commande installe, à partir de l'emplacement de stockage spécifié, le package d'installation de préparation de Sophos SafeGuard et le logiciel de chiffrement dans le répertoire d'installation par défaut (C:\Program Files\Sophos\Sophos SafeGuard). Cette commande installe Sophos SafeGuard Device Encryption (chiffrement basé sur volume) ainsi que l'authentification au démarrage.

■ **msiexec /i F:\Software\Sophos\SafeGuard\SDEClientConfig.msi**

Cette commande installe le package de configuration Sophos SafeGuard dans le répertoire d'installation par défaut, à partir de l'emplacement de stockage spécifié.

■ **/L*VX**

G:\Temp\Sophos\SafeGuard\%nomordinateur%\SDEClient_inst.log

Cette commande consigne tous les avertissements et messages d'erreur dans le fichier journal spécifié stocké sur le réseau et crée un fichier journal pouvant être analysé automatiquement à l'aide de l'outil de Windows Installer wilogutl.exe.

■ **/qn**

Cette commande exécute une installation sans interaction de l'utilisateur et n'affiche pas d'interface utilisateur.

3. À l'aide des mécanismes de distribution de logiciels de l'entreprise, distribuez le package d'installation et de configuration sur les ordinateurs finaux.

Le logiciel de chiffrement et les packages de configuration sont installés sur les ordinateurs finaux et ces derniers sont alors chiffrés.

Une configuration supplémentaire peut être requise pour garantir que l'authentification au démarrage fonctionne correctement sur chaque plate-forme matérielle. La plupart des conflits matériels peuvent être résolus à l'aide de la fonctionnalité « Raccourcis clavier », intégrée à l'authentification au démarrage. Les raccourcis clavier peuvent être configurés après l'installation, depuis l'authentification au démarrage, ou via un paramètre de configuration supplémentaire passé à la commande msiexec de Windows Installer. Pour en savoir plus, reportez-vous au chapitre *Raccourcis clavier pris en charge dans l'authentification au démarrage* de l'aide de l'administrateur, ainsi qu'aux articles suivants :

<http://www.sophos.com/support/knowledgebase/article/107781.html>

<http://www.sophos.com/support/knowledgebase/article/107785.html>

13 Récupération d'un mot de passe oublié

Si l'utilisateur a oublié son mot de passe, il existe deux manières de le récupérer :

- l'utilisateur peut le récupérer via Local Self Help (recommandé) ;
- le support peut le récupérer via une procédure Challenge/Réponse.

13.1 Récupération d'un mot de passe oublié via Local Self Help

1. L'utilisateur saisit son nom d'utilisateur dans l'authentification au démarrage, sur l'ordinateur final.

Le bouton **Récupération** devient actif.

2. L'utilisateur clique sur **Récupération**.

- Si seule la méthode Local Self Help est activée sur l'ordinateur final pour la récupération de la connexion, Local Self Help démarre.
- Si les méthodes Local Self Help et Challenge/Réponse sont activées pour la récupération de la connexion, une boîte de dialogue permettant de sélectionner ces deux méthodes s'affiche. L'utilisateur clique sur **Local Self Help**.

La boîte de dialogue de bienvenue dans Local Self Help s'affiche.

3. Dans les cinq boîtes de dialogue suivantes, l'utilisateur répond à cinq questions sélectionnées aléatoirement parmi les questions stockées sur l'ordinateur final. Après avoir répondu à la dernière, l'utilisateur confirme ses réponses en cliquant sur **OK**.

4. Dans la boîte de dialogue suivante, l'utilisateur peut afficher le mot de passe en appuyant sur la touche Entrée, sur la barre d'espace ou en cliquant sur la case bleue.

Le mot de passe ne s'affiche que pendant 5 secondes maximum. Le processus d'initialisation continue ensuite automatiquement. L'utilisateur peut immédiatement masquer le mot de passe en appuyant de nouveau sur la touche Entrée, sur la barre d'espace ou en cliquant de nouveau sur la case bleue.

5. Après avoir lu le mot de passe, l'utilisateur clique sur **OK**.

L'utilisateur est connecté à l'authentification au démarrage et à Windows et pourra utiliser le mot de passe pour se connecter ultérieurement.

13.2 Récupération d'un mot de passe oublié via Challenge/Réponse

Conditions préalables :

Le fichier de récupération de clé créé pour chaque ordinateur final lors de l'installation du logiciel de chiffrement Sophos SafeGuard doit être accessible au support et son nom doit être connu. Le support doit disposer des autorisations nécessaires pour effectuer les actions de récupération. La méthode Challenge/Réponse doit être activée sur l'ordinateur final, via une stratégie.

Remarque: Nous vous recommandons d'utiliser en priorité Local Self Help pour récupérer un mot de passe oublié. Avec la récupération via Local Self Help, le mot de passe actuel de l'utilisateur peut être affiché de manière confidentielle dans l'authentification au démarrage et l'utilisateur peut continuer d'utiliser ce mot de passe. Cela évitera la réinitialisation du mot de passe et le recours à l'assistance du support.

1. L'utilisateur saisit son nom d'utilisateur dans l'authentification au démarrage, sur l'ordinateur final. Le bouton **Récupération** devient actif.
2. L'utilisateur clique sur **Récupération**.
 - Si seule la méthode Challenge/Réponse est activée pour la récupération de la connexion, elle démarre automatiquement.
 - Si les méthodes Challenge/Réponse et Local Self Help sont disponibles pour la récupération de la connexion, l'utilisateur sélectionne **Challenge/Réponse**.

Une boîte de dialogue indiquant le nom du fichier de récupération de clé requis s'affiche.

3. L'utilisateur clique sur **Suivant**. Un code de challenge généré de manière aléatoire s'affiche.
4. L'utilisateur contacte le support. Il lui fournit le nom du fichier de récupération de clé requis ainsi que le code de challenge.
5. Le support lance l'assistant de récupération dans SafeGuard Policy Editor.
6. Le support sélectionne le type de récupération **Challenge/Réponse pour l'authentification au démarrage**, confirme la clé et le code de challenge, puis sélectionne l'action de récupération souhaitée : **Initialisation sans connexion utilisateur**.

Un code de réponse sous la forme d'une chaîne de caractères ASCII est généré et s'affiche.

7. Le support transmet le code de réponse à l'utilisateur, par exemple par téléphone ou message texte.
8. Sur l'ordinateur final, dans l'assistant Challenge/Réponse, l'utilisateur clique sur **Suivant** pour entrer le code de réponse fourni. L'ordinateur peut démarrer à partir de l'authentification au démarrage.

9. Dans la boîte de dialogue de connexion Windows, l'utilisateur ne connaît pas davantage le mot de passe correct et doit par conséquent le modifier au niveau Windows. Cela nécessite d'autres actions de récupération sortant du périmètre de Sophos SafeGuard, via des moyens Windows standard. Nous recommandons l'utilisation des méthodes de réinitialisation de mot de passe Windows suivantes.
 - via un compte de service ou administrateur disponible sur l'ordinateur final avec les droits Windows requis ;
 - via un disque de réinitialisation de mot de passe Windows sur l'ordinateur final.
10. L'utilisateur saisit le nouveau mot de passe Windows fourni par le support. L'utilisateur modifie ensuite ce mot de passe immédiatement en choisissant une valeur connue de lui seul.
11. Sophos SafeGuard détecte que le nouveau choix de mot de passe ne correspond pas au mot de passe Sophos SafeGuard utilisé actuellement au niveau de l'authentification au démarrage. L'utilisateur est alors invité à saisir son ancien mot de passe Sophos SafeGuard et, puisqu'il a oublié son mot de passe, il doit cliquer sur **Annuler**.
12. Dans Sophos SafeGuard, la définition d'un nouveau mot de passe sans donner l'ancien requiert un nouveau certificat. L'utilisateur doit confirmer cette procédure.
13. Un nouveau certificat utilisateur sera créé en fonction du nouveau choix de mot de passe Windows. Cela permet à l'utilisateur de se reconnecter à l'ordinateur ainsi qu'à l'authentification au démarrage à l'aide du nouveau mot de passe.

L'utilisateur peut reprendre ses activités.

14 Récupération de l'accès au système

Sophos SafeGuard propose plusieurs options de récupération dans les situations critiques, notamment lorsque l'authentification au démarrage est corrompue et que l'utilisateur ne peut plus accéder aux données chiffrées, ou lorsque le MBR (Master Boot Record) est endommagé.

14.1 Récupération de données par Challenge/Réponse à l'aide de clients virtuels

La récupération de données à l'aide de clients virtuels repose sur une procédure Challenge/Réponse. Ce type de récupération s'applique si, dans des circonstances particulières, le système d'exploitation ne démarre plus, à cause, notamment, d'une configuration de pilote corrompue.

Dans ce cas, l'accès aux données chiffrées peut être récupéré en démarrant l'ordinateur à partir d'un disque de récupération Windows PE personnalisé pour Sophos SafeGuard et en lançant une procédure Challenge/Réponse à l'aide de clients virtuels. Pour plus d'informations, consultez le chapitre *Récupération de l'accès au système* de l'aide de l'administrateur.

Pour récupérer l'accès aux données chiffrées sur l'ordinateur, procédez comme suit :

1. Demandez au support technique de vous fournir le disque de récupération Sophos SafeGuard.
Le support peut télécharger le disque de récupération Windows PE avec les derniers pilotes du filtre Sophos SafeGuard sur le site du support Sophos. Pour en savoir plus, consultez la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/108805.html>.
2. Configurez le client virtuel dans SafeGuard Policy Editor.
3. Démarrez l'ordinateur depuis le disque de récupération.
4. Importez le fichier du client virtuel dans l'outil de récupération de clé KeyRecovery.
5. Initialisez le challenge dans l'outil de récupération de clé KeyRecovery.
6. Confirmez le client virtuel dans SafeGuard Policy Editor.
7. Saisissez le code de challenge dans SafeGuard Policy Editor.
8. Générez le code de réponse dans SafeGuard Policy Editor.
9. Saisissez le code de réponse dans l'outil de récupération de clé KeyRecovery.

L'accès aux données stockées sur cette partition est récupéré.

14.2 Récupération des données via l'initialisation à partir d'un support externe

Ce type de récupération s'applique lorsque l'utilisateur peut toujours se connecter à partir de l'authentification au démarrage mais ne peut plus accéder au volume chiffré. Dans ce cas, l'accès aux données chiffrées peut être récupéré en démarrant l'ordinateur à partir d'un disque de récupération Windows PE personnalisé pour Sophos SafeGuard.

Conditions préalables :

- L'utilisateur qui exécute l'initialisation à partir d'un support externe doit disposer de l'autorisation appropriée. Ce droit peut être soit configuré dans SafeGuard Policy Editor via une stratégie de type **Authentification (l'utilisateur peut déchiffrer le volume défini sur Oui)**, soit obtenu, pour une utilisation unique, via une procédure Challenge/Réponse.
- L'ordinateur doit prendre en charge l'initialisation à partir de supports autres qu'un disque dur fixe.

Pour récupérer l'accès aux données chiffrées sur l'ordinateur, procédez comme suit :

1. Demandez au support technique de vous fournir le disque Sophos SafeGuard Windows PE.
Le support peut télécharger le disque de récupération Windows PE avec les derniers pilotes du filtre Sophos SafeGuard sur le site du support Sophos. Pour en savoir plus, consultez la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/108805.html>.
2. Connectez-vous à l'authentification au démarrage avec vos informations d'identification.
3. Insérez le disque de récupération Windows PE dans l'ordinateur.
4. Dans la boîte de dialogue Connexion POA, cliquez sur **Poursuivre l'installation à partir de :**, puis sélectionnez **support externe**. L'ordinateur démarre.

L'accès aux données stockées sur cette partition est récupéré.

14.3 Récupération d'un ordinateur dont le Master Boot Record est corrompu

Une fois Sophos SafeGuard installé sur l'ordinateur final, une copie du Master Boot Record (MBR) original est enregistrée et stockée sur le noyau système de l'ordinateur. Si le MBR est corrompu, le système ne peut pas démarrer. Pour récupérer les systèmes dont le MBR est corrompu, Sophos SafeGuard propose l'utilitaire de récupération approprié : BE_Restore.exe. Vous pouvez ainsi exécuter l'une des actions suivantes :

- restauration du MBR à partir d'une sauvegarde ;
- réparation du MBR.

Pour obtenir une description détaillée de ce type de récupération, reportez-vous au chapitre *Restauration d'un MBR corrompu* du guide des outils Sophos SafeGuard.

15 Aide sur les tâches communes

Cette section vous indique où trouver les informations relatives à la réalisation des tâches communes. Pour en savoir plus, reportez-vous à l'aide de l'administrateur ou à l'aide de l'utilisateur Sophos SafeGuard.

Tâche	Manuel/Chapitre
Connexion à SafeGuard Policy Editor	Aide de l'administrateur, Connexion à SafeGuard Policy Editor
Connexion à l'ordinateur protégé par Sophos SafeGuard	Aide de l'utilisateur, Authentification au démarrage
Garantie du bon fonctionnement de l'authentification au démarrage	Aide de l'administrateur/aide de l'utilisateur, Raccourcis clavier pris en charge dans l'authentification au démarrage
Affichage des informations spécifiques à Sophos SafeGuard sur l'ordinateur final	Aide de l'utilisateur, Icône de la barre d'état système et info-bulle
Création et regroupement des stratégies	Aide de l'administrateur, Utilisation de stratégies
Export des certificats	Aide de l'administrateur, Exportation des certificats de l'entreprise et du responsable principal de la sécurité
Création des accès administratifs aux ordinateurs finaux	Aide de l'administrateur, Options d'accès administratifs sur les ordinateurs finaux
Récupération d'un mot de passe via Local Self Help	Aide de l'administrateur, aide de l'utilisateur : Récupération via Local Self Help
Récupération d'un mot de passe via Challenge/Réponse	Aide de l'administrateur, aide de l'utilisateur : Récupération par Challenge/Réponse
Récupération des données sur les ordinateurs finaux	Aide de l'administrateur, Challenge/Réponse à l'aide de clients virtuels
Récupération d'un Master Boot Record corrompu	Guide des outils, Restauration d'un Master Boot Record corrompu
Mise à niveau de SDE 4.60 ou SGE 4.3x - 4.5x vers Sophos SafeGuard	Aide de l'administrateur, mise à niveau de SafeGuard Easy 4.x/SophosDisk Encryption 4.x vers Sophos SafeGuard 5.5x

16 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, 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.

17 Copyright

Copyright © 1996 - 2009 Sophos Plc

Tous droits réservés. 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.

Sophos est une marque déposée de Sophos Plc et de Sophos Group. SafeGuard est une marque déposée de Utimaco Safeware AG - a member of the Sophos Group. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Tous les produits SafeGuard sont sous le copyright d'Utimaco Safeware AG- a member of the Sophos Group, ou, le cas échéant, des concédants de la licence. Tous les autres produits Sophos sont sous copyright de Sophos Plc, ou, le cas échéant, des concédants de la licence.

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.