

# SOPHOS

## Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Aide administrateur

Date du document : Novembre 2010



# Table des matières

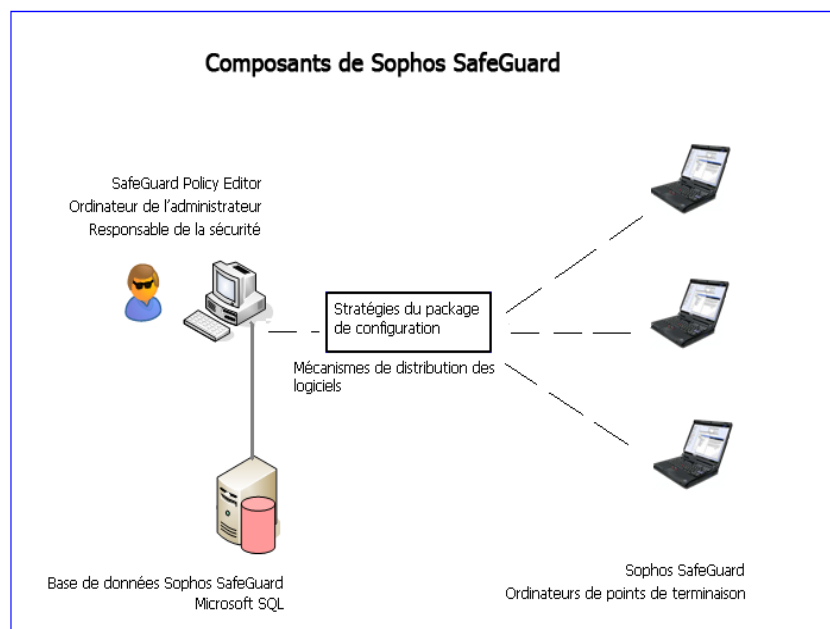
1	À propos de Sophos SafeGuard.....	3
2	SafeGuard Policy Editor.....	5
3	Sophos SafeGuard sur les ordinateurs finaux.....	8
4	Chiffrement de données.....	9
5	Mise en route.....	13
6	Installation.....	20
7	Installation du Sophos SafeGuard sur les ordinateurs disposant de plusieurs systèmes d'exploitation.....	40
8	Connexion à SafeGuard Policy Editor.....	43
9	Utilisation de stratégies.....	44
10	Utilisation de packages de configuration.....	50
11	Exportation des certificats de l'entreprise et du responsable principal de la sécurité.....	52
12	Restauration d'une installation corrompue de SafeGuard Policy Editor.....	54
13	Restauration d'une configuration corrompue de base de données.....	55
14	Options d'accès administratif sur les ordinateurs finaux.....	57
15	Stratégies par défaut.....	70
16	Paramètres de stratégie.....	80
17	SafeGuard Data Exchange.....	120
18	Authentification au démarrage (POA).....	123

19 Options de récupération .....	133
20 Récupération via Local Self Help .....	134
21 Récupération par Challenge/Réponse .....	140
22 Récupération du système .....	156
23 Empêcher la désinstallation sur les ordinateurs finaux .....	159
24 Mise à jour de Sophos SafeGuard .....	160
25 Mise à niveau de Sophos SafeGuard 5.5x vers SafeGuard Enterprise.....	164
26 Mise à niveau de SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x vers Sophos SafeGuard 5.5x .....	167
27 Support technique.....	176
28 Copyright .....	177

# 1 À propos de Sophos SafeGuard

Sophos SafeGuard est une solution de sécurité des données à la pointe de la technologie qui utilise un chiffrement basé sur une stratégie pour protéger efficacement les informations sur les ordinateurs finaux.

L'administration s'effectue via SafeGuard Policy Editor utilisé pour créer et gérer les stratégies de sécurité et qui propose des fonctions de récupération. Les stratégies sont déployées sur les ordinateurs finaux via des packages de configuration. Côté utilisateur, le chiffrement de données et la protection contre des accès non autorisés sont les principales fonctions de sécurité de Sophos SafeGuard. Sophos SafeGuard est un outil convivial, facile à utiliser et qui s'intègre en toute transparence dans l'environnement normal de l'utilisateur. Le système d'authentification de Sophos SafeGuard, l'authentification au démarrage (POA, Power-On Authentication), fournit une protection efficace des accès et offre une prise en charge conviviale lors de la récupération des informations d'identification.



## 1.1 Ensembles de produits

Sophos SafeGuard est disponible avec différents ensembles de produits : SGE (SafeGuard Easy) et ESDP (Endpoint Security and Data Protection). À partir de la version 5.50, SGE est le nouveau nom de produit de SafeGuard Enterprise autonome. Pour chaque ensemble de produits, différents modules et fonctions sont disponibles. Les modules et fonctions non disponibles pour ESDP sont annotés dans ce manuel.

## 1.2 Composants Sophos SafeGuard

Sophos SafeGuard est constitué des composants suivants :

Composant	Description
SafeGuard Policy Editor	L'outil de gestion Sophos SafeGuard permet de créer des stratégies de chiffrement et d'authentification. Un ensemble de stratégies par défaut et un package de configuration par défaut pour les ordinateurs finaux peuvent être créés au moment de la configuration initiale. SafeGuard Policy Editor propose également des fonctions de récupération pour accéder de nouveau aux ordinateurs finaux, en cas d'oubli de mot de passe, par exemple.
Base de données de Sophos SafeGuard	La base de données Sophos SafeGuard contient toutes les données pertinentes relatives aux paramètres de stratégie des ordinateurs finaux.
Logiciel Sophos SafeGuard sur les ordinateurs finaux	Logiciel de chiffrement sur les ordinateurs finaux

## 2 SafeGuard Policy Editor

SafeGuard Policy Editor est l'outil de gestion des ordinateurs protégés par Sophos SafeGuard et qui sont gérés localement.

SafeGuard Policy Editor est installé sur l'ordinateur que vous utilisez pour réaliser des tâches administratives. En tant que responsable de la sécurité, vous utilisez SafeGuard Policy Editor pour gérer les stratégies Sophos SafeGuard et créer des paramètres de configuration pour les ordinateurs finaux. Les stratégies et paramètres sont exportés vers des packages de configuration et déployés sur les ordinateurs finaux. Vous pouvez créer plusieurs packages de configuration et les distribuer via des mécanismes tiers. Les packages peuvent être distribués lors de l'installation du logiciel de chiffrement Sophos SafeGuard. Vous pouvez modifier les paramètres des ordinateurs finaux par la suite, en déployant d'autres packages de configuration.

SafeGuard Policy Editor propose également des fonctions de récupération pour accéder aux ordinateurs finaux, lorsqu'un utilisateur oublie son mot de passe, par exemple.

### 2.1 Fonctions

Pour plus de convivialité et pour faciliter l'administration, SafeGuard Policy Editor propose les fonctions suivantes :

- **Configuration par défaut** : un package de configuration, avec des stratégies recommandées préconfigurées pour les ordinateurs finaux, peut être créé par défaut lors de la configuration initiale de SafeGuard Policy Editor. Si les stratégies par défaut ne suffisent pas à satisfaire vos exigences particulières, vous pouvez définir vos propres stratégies dans SafeGuard Policy Editor.
- **Options d'accès administratif** : Pour fournir un accès spécial destiné à la post-installation et aux tâches administratives sur les ordinateurs finaux, Sophos SafeGuard propose des comptes de services pour les options d'accès administratif et des comptes d'accès à l'authentification au démarrage.
- **Clés de chiffrement** : Une clé machine générée automatiquement est utilisée pour SafeGuard Device Encryption (chiffrement basé sur volume). Pour SafeGuard Data Exchange (chiffrement basé sur fichier), ce sont les clés générées localement sur l'ordinateur final qui seront utilisées. SafeGuard Data Exchange n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

- **Local Self Help** : Pour récupérer les mots de passe oubliés, Sophos SafeGuard propose l'option de récupération appropriée, Local Self Help. Local Self Help permet aux utilisateurs de récupérer leur mot de passe, sans recourir à l'aide du support.

- **Challenge/Réponse avec aide du support** :

Une procédure Challenge/Réponse avec aide du support peut être demandée par un utilisateur qui a oublié son mot de passe ou qui l'a saisi de façon incorrecte un trop grand nombre de fois. Elle peut également s'appliquer pour récupérer des données en cas de corruption de l'authentification au démarrage. La procédure Challenge/Réponse repose sur des fichiers de récupération de clé qui sont générés automatiquement lors du déploiement de l'ordinateur final Sophos SafeGuard.

## 2.2 Base de données

Les stratégies Sophos SafeGuard sont stockées dans une base de données SQL sur l'ordinateur de l'administrateur. Vous êtes invité à installer Microsoft SQL Server 2005 Express lors de l'installation de Sophos SafeGuard Policy Editor si aucune instance existante du serveur SQL n'est disponible. Microsoft SQL 2005 Express est donc fourni avec le produit.

## 2.3 Mise à niveau

Vous pouvez facilement effectuer une mise à niveau vers la suite SafeGuard Enterprise via la gestion centralisée, afin d'utiliser l'ensemble des fonctions de SafeGuard Enterprise.

## 2.4 Consignation

Les événements des ordinateurs protégés par Sophos SafeGuard sont consignés dans la visionneuse des événements Windows.

## 2.5 Différences par rapport à SafeGuard Management Center

En raison de la présence d'un serveur de gestion central, SafeGuard Management Center propose des fonctionnalités de gestion améliorées, par exemple :

- Importation d'Active Directory avec gestion utilisateur et domaine.
- Consignation centrale.
- Rôle administratif pouvant être défini.

SafeGuard Management Center est disponible avec SafeGuard Enterprise.

**Remarque:** Vous pouvez également définir des paramètres et créer des packages de configuration pour les ordinateurs Sophos SafeGuard qui ne disposent d'aucune connexion avec le serveur SafeGuard Enterprise dans SafeGuard Management Center.

## 3 Sophos SafeGuard sur les ordinateurs finaux

Le chiffrement de données et la protection contre les accès non autorisés sont les principales fonctions de sécurité de Sophos SafeGuard. Sophos SafeGuard est un outil facile à utiliser et convivial qui s'intègre en toute transparence dans l'environnement normal de l'utilisateur. Le système d'authentification de Sophos SafeGuard, l'authentification au démarrage (POA), fournit la protection des accès nécessaire et offre une prise en charge conviviale lors de la récupération des informations d'identification.

### 3.1 Modules pris en charge

Les modules suivants sont fournis pour les ordinateurs finaux :

#### ■ SafeGuard Device Encryption

- **Chiffrement basé sur volume** : Garantit que toutes les données des volumes spécifiés (volume d'initialisation, disque dur, partitions) sont chiffrées de manière transparente (y compris les fichiers d'initialisation, les fichiers d'échange, les fichiers inactifs/d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sans que l'utilisateur doive modifier ses habitudes de travail ou tenir compte de problèmes de sécurité.
- **Authentification au démarrage** : La connexion de l'utilisateur se fait immédiatement après la mise sous tension de l'ordinateur. Une fois l'authentification au démarrage réussie, l'utilisateur est connecté automatiquement au système d'exploitation.

#### ■ SafeGuard Data Exchange

L'échange de données est facilité avec les supports amovibles de toutes les plates-formes sans rechiffrement.

- **Chiffrement basé sur fichier** : Tous les supports inscriptibles mobiles, disques durs externes et cartes mémoire USB inclus, sont chiffrés de manière transparente.

**Remarque:** Ce module n'est pas pris en charge avec ESDP (Endpoint Security and Data Protection).

## 4 Chiffrement de données

La fonction principale de Sophos SafeGuard est le chiffrement des données sur des périphériques de stockage de données différents. Le chiffrement peut être basé sur volume ou sur fichier avec des clés et des algorithmes différents.

**Remarque:** Le chiffrement basé sur fichier n'est pas pris en charge par ESDP (Endpoint Security and Data Protection).

Les fichiers sont chiffrés de manière transparente. Lorsqu'un utilisateur ouvre, modifie et enregistre un fichier, il n'est pas invité à le chiffrer ou déchiffrer.

Lors de la première configuration dans SafeGuard Policy Editor, une stratégie par défaut avec des paramètres de chiffrement prédéfinis est créée automatiquement, voir [Stratégies par défaut](#), à la page 70.

Vous pouvez définir des paramètres de chiffrement dans une stratégie de sécurité du type **Protection du périphérique**. Pour plus d'informations, voir [Utilisation de stratégies](#), à la page 44 et voir [Protection du périphérique](#), à la page 102.

### 4.1 Chiffrement basé sur volume

Grâce au chiffrement basé sur volume, toutes les données d'un volume (y compris les fichiers d'initialisation, les fichiers paginés, les fichiers d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sont chiffrées. L'utilisateur n'a pas à modifier ses habitudes de travail ni tenir compte de problèmes de sécurité.

**Remarque:** Si une stratégie de chiffrement existe pour un volume ou un type de volume et que le chiffrement du volume échoue, l'utilisateur n'est pas autorisé à y accéder.

#### 4.1.1 Chiffrement initial rapide

Le chiffrement initial rapide est un mode spécial du chiffrement basé sur volume. Il permet de réduire la durée nécessaire au chiffrement initial (ou final) de volumes sur des ordinateurs de points de terminaison en accédant uniquement à l'espace disque en cours d'utilisation.

Les conditions préalables suivantes s'appliquent au chiffrement initial rapide :

- Le chiffrement initial rapide s'applique aux volumes au format NTFS uniquement.
- Les volumes au format NTFS dont la taille de cluster est de 64 Ko ne peuvent pas être chiffrés en mode de chiffrement initial rapide.

**Remarque:** Ce mode se traduit par une sécurité inférieure si un disque a déjà été utilisé précédemment. Les secteurs inutilisés peuvent contenir des données. Le mode de chiffrement initial rapide est donc désactivé par défaut.

Pour activer le chiffrement initial rapide, sélectionnez le paramètre basé sur volume **Chiffrement initial rapide** dans une stratégie du type **Protection du périphérique**.

**Remarque:** Pour le déchiffrement d'un volume, le mode de chiffrement initial rapide est toujours utilisé quel que soit le paramètre de stratégie défini. Les conditions préalables indiquées s'appliquent également au déchiffrement.

### 4.1.2 Chiffrement basé sur volume et partition système Windows 7

Pour Windows 7 Professionnel, Entreprise et Édition Intégrale, une partition système est créée sur les ordinateurs de points de terminaison sans assignation de lettre de lecteur. Cette partition système ne peut pas être chiffrée par Sophos SafeGuard.

### 4.1.3 Chiffrement basé sur volume et objets du système de fichiers non identifiés

Les objets du système de fichiers non identifiés sont des volumes qui ne peuvent pas être clairement identifiés comme texte brut ou chiffrés par SafeGuard Enterprise. L'accès au volume est refusé s'il existe une stratégie de chiffrement définie pour un objet du système de fichiers non identifié. Si aucune stratégie de chiffrement n'existe, l'utilisateur peut accéder au volume.

**Remarque:** Si une stratégie de chiffrement, dont le paramètre **Clé à utiliser pour le chiffrement** est défini de sorte à permettre la sélection de clé (par exemple, **Toute clé du jeu de clés utilisateur**), existe pour un volume d'objets du système de fichiers non identifiés, un intervalle de temps s'écoule entre l'affichage de la boîte de dialogue de sélection de la clé et le refus de l'accès. Pendant cet intervalle, le volume reste accessible. Le volume est accessible tant que la boîte de dialogue de sélection de clé n'est pas confirmée. Pour éviter ceci, indiquez une clé présélectionnée pour le chiffrement. Pour plus d'informations sur les paramètres de stratégie appropriés, voir [Protection du périphérique](#), à la page 102. Cet intervalle de temps existe également pour les volumes d'objets du système de fichiers non identifiés qui sont connectés à un ordinateur de point de terminaison, notamment lorsque l'utilisateur a déjà ouvert des fichiers sur le volume lorsque la stratégie de chiffrement prend effet. Dans ce cas, il n'est pas garanti que l'accès au volume sera refusé car cela risque de provoquer une perte de données.

#### 4.1.4 Chiffrement de volumes avec fonctionnalité d'exécution automatique activée

Si vous appliquez une stratégie de chiffrement aux volumes pour lesquels l'exécution automatique est activée, les problèmes suivants peuvent se produire :

- Le volume n'est pas chiffré.
- Si le volume est un objet du système de fichiers non identifié (voir [Chiffrement basé sur volume et objets du système de fichiers non identifiés](#), à la page 10), l'accès n'est pas refusé.

## 4.2 Chiffrement basé sur fichier

**Remarque:** Le chiffrement basé sur fichier n'est pas pris en charge par ESDP (Endpoint Security and Data Protection).

Le chiffrement basé sur fichier garantit que toutes les données sont chiffrées (à l'exception du support d'initialisation et des informations de répertoire). Grâce au chiffrement basé sur fichier, même les supports optiques tels que les CD/DVD peuvent être chiffrés. De plus, les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard n'est pas installé (si les stratégies l'autorisent).

**Remarque:** Les données chiffrées selon la méthode de chiffrement basé sur fichier ne peuvent pas être compressées. De même, les données compressées ne peuvent pas être chiffrées selon la méthode basée sur fichier.

**Remarque:** Les volumes d'initialisation ne sont jamais chiffrés selon la méthode basée sur fichier. Ils sont automatiquement exclus du chiffrement basé sur fichier, même si une règle correspondante est définie.

Pour appliquer le chiffrement basé sur fichier à des ordinateurs de points de terminaison, créez une stratégie du type **Protection du périphérique** et définissez le **Mode de chiffrement du support** sur **Sur fichier**. Pour plus d'informations, voir [Protection du périphérique](#), à la page 102.

### 4.2.1 Exclusion d'applications du chiffrement

Vous pouvez définir des applications devant être ignorées par le pilote du filtre Sophos SafeGuard et devant être exclues du chiffrement/déchiffrement transparent.

Un exemple est un programme de sauvegarde. Pour garantir que ces données ne sont pas déchiffrées lors de la création d'une sauvegarde, cette application peut être exclue du processus de chiffrement/déchiffrement. Les données sont sauvegardées sous forme chiffrée.

Un exemple type consiste à définir des programmes de sauvegarde comme exemptés afin qu'ils puissent toujours lire et enregistrer les données chiffrées.

Les applications susceptibles de déclencher des dysfonctionnements lorsqu'elles sont utilisées avec Sophos SafeGuard mais qui ne nécessitent pas de chiffrement peuvent généralement être exemptées de chiffrement.

Vous pouvez définir des applications devant être exclues du déchiffrement dans une stratégie du type **Protection du périphérique** avec la cible **Périphériques de stockage locaux**. Le nom complet du fichier exécutable (contenant éventuellement les informations du chemin d'accès) est utilisé pour spécifier les **Applications non gérées**.

Pour plus d'informations, voir [Protection du périphérique](#), à la page 102.

## 5 Mise en route

Ce chapitre explique comment préparer l'installation de Sophos SafeGuard.

### 5.1 Stratégie de déploiement

Avant de procéder au déploiement de Sophos SafeGuard sur les ordinateurs finaux, il est recommandé de définir une stratégie de déploiement qui tienne compte des exigences spécifiques et des options disponibles.

Lorsque vous définissez une stratégie de déploiement pour Sophos SafeGuard, vous devez tenir compte des options suivantes :

#### 5.1.1 Stratégies

Sophos SafeGuard propose les options de stratégie suivantes :

##### ■ Stratégies par défaut

Sophos SafeGuard propose des stratégies prédéfinies par défaut pour un déploiement de stratégies rapide et facile. Lors de la configuration initiale de SafeGuard Policy Editor, un groupe de stratégies avec des paramètres de chiffrement et d'authentification prédéfinis est créé par défaut. Un package de configuration contenant ces stratégies par défaut est automatiquement créé pour configurer les ordinateurs finaux.

Pour en savoir plus sur les stratégies par défaut et sur leurs paramètres, voir [Stratégies par défaut](#), à la page 70.

##### ■ Définition de vos propres stratégies

Si les stratégies par défaut ne suffisent pas à satisfaire vos exigences particulières, vous pouvez définir vos propres stratégies dans SafeGuard Policy Editor.

Pour en savoir plus sur la création de stratégies, voir [Utilisation de stratégies](#), à la page 44. Pour en savoir plus sur le déploiement de stratégies sur les ordinateurs finaux, voir [Utilisation de packages de configuration](#), à la page 50.

Pour obtenir une description détaillée de toutes les stratégies disponibles et de leurs paramètres, voir [Paramètres de stratégie](#), à la page 80.

## 5.1.2 Options d'accès administratif

Afin de fournir un accès destiné aux tâches administratives après l'installation de Sophos SafeGuard sur les ordinateurs finaux, Sophos SafeGuard propose des options d'accès administratif pour les deux scénarios suivants :

### ■ 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, sans avoir à activer l'authentification au démarrage et sans être ajoutés en tant qu'utilisateurs sur les ordinateurs.

Les listes de comptes de service sont affectées aux ordinateurs finaux via des stratégies. Elles doivent être affectées dans le premier package de configuration Sophos SafeGuard, créé pour la configuration des ordinateurs finaux. Vous pouvez mettre à jour les listes de comptes de service en créant un nouveau package de configuration et en le déployant sur les ordinateurs finaux.

Pour en savoir plus sur les listes de comptes de service, voir [Listes de comptes de service pour la connexion Windows](#), à la page 57.

### ■ Comptes d'accès POA pour connexion POA

Les comptes d'accès POA sont des comptes locaux prédéfinis qui permettent aux utilisateurs (membres de l'équipe informatique, par exemple) de se connecter à des ordinateurs finaux pour effectuer des tâches administratives après activation de l'authentification au démarrage. Les comptes d'accès POA permettent les connexions à partir de l'authentification au démarrage. Il n'y a pas de connexion automatique à Windows.

Vous pouvez créer des comptes d'accès POA dans Sophos SafeGuard Policy Editor, les regrouper dans des groupes de comptes d'accès POA et affecter ces groupes à des ordinateurs finaux via les packages de configuration Sophos SafeGuard.

Pour en savoir plus sur les comptes d'accès POA, voir [Comptes d'accès POA pour connexion POA](#), à la page 63.

### 5.1.3 Options de récupération

Pour les situations nécessitant une procédure de récupération (en cas d'oubli du mot de passe, par exemple), Sophos SafeGuard propose deux options 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. Pour accéder de nouveau à leur ordinateur, il leur suffit de répondre à un certain nombre de questions prédéfinies dans l'authentification au démarrage.

Dans les stratégies par défaut, Local Self Help est activé et configuré par défaut. Si vous n'utilisez pas la configuration par défaut, vous devez activer Local Self Help via une stratégie et définir les questions auxquelles l'utilisateur final doit répondre.

Pour plus d'informations, voir [Récupération via Local Self Help](#), à la page 134.

#### ■ 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. Pour lancer une procédure Challenge/Réponse, vous aurez besoin de l'aide du support.

Dans les stratégies par défaut, la procédure Challenge/Réponse est activée par défaut. Si vous n'utilisez pas la configuration par défaut, vous devez utiliser une stratégie pour activer la procédure Challenge/Réponse. Pour récupérer des données via une procédure Challenge/Réponse, vous devez commencer par créer des fichiers spécifiques appelés clients virtuels dans SafeGuard Policy Editor.

Pour plus d'informations, voir [Récupération par Challenge/Réponse](#), à la page 140 et voir [Création d'un client virtuel](#), à la page 148.

## 5.2 Configuration minimale du système

Reportez-vous au Guide de Démarrage pour connaître les détails relatifs à la configuration requise pour le matériel et le logiciel, les service packs et l'espace disque requis lors de l'installation et pour garantir un bon fonctionnement.

### **5.2.1 Configuration minimale du système spécifique pour les ordinateurs finaux**

- 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.

## **5.3 Préparation pour l'installation**

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

### **5.3.1 Préparation générale**

- Pour installer le logiciel et utiliser SafeGuard Policy Editor, vous devez disposer des droits d'administrateur Windows.
- Fermez toutes les applications ouvertes.
- Vérifiez que l'espace disque disponible est suffisant. Les informations afférentes se trouvent dans le Guide de Démarrage.
- Lisez attentivement les Notes de version.

### **5.3.2 Préparation au chiffrement**

- Un compte utilisateur doit être configuré et actif sur les ordinateurs finaux.
- Créez une sauvegarde complète des données sur l'ordinateur final.
- 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. Le fichier est mis à jour tous les mois et est téléchargeable à l'adresse suivante : <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

Pour en savoir plus, voir voir [Raccourcis clavier pris en charge dans l'authentification au démarrage](#), à la page 130 dans 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.de/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. 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 irréprochable. L'utilisation de programmes d'imagerie ou de clonage peut affecter l'état de cet enregistrement.

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.

## 5.4 Paramètres de langue

Les paramètres de langue pour les assistants de configuration, SafeGuard Policy Editor et Sophos SafeGuard sur les ordinateurs finaux sont les suivants :

### 5.4.1 Langue de l'assistant de configuration

Les assistants d'installation et de configuration utilisent le paramètre de langue du système d'exploitation. L'anglais, l'allemand, le français et le japonais sont les langues prises en charge. Si la langue du système d'exploitation n'est pas disponible pour les assistants de configuration, la langue par défaut est l'anglais.

## 5.4.2 Langue de SafeGuard Policy Editor

Vous pouvez définir la langue de SafeGuard Policy Editor dans SafeGuard Policy Editor :

- Ouvrez le menu Outils > Options > Général. Activez l'option **Utiliser la langue définie par l'utilisateur** et sélectionnez une langue. L'anglais, l'allemand, le français et le japonais sont les langues prises en charge.
- Redémarrez SafeGuard Policy Editor pour qu'il s'affiche dans la langue sélectionnée.

## 5.4.3 Langue de Sophos SafeGuard sur les ordinateurs finaux

Pour définir la langue de Sophos SafeGuard sur l'ordinateur final, vous devez utiliser une stratégie de type Général dans les paramètres de SafeGuard Policy Editor Personnalisation > Langue du client :

- La langue du produit Sophos SafeGuard est identique à la langue du système d'exploitation, si celle-ci est définie. Si la langue du système d'exploitation n'est pas disponible pour Sophos SafeGuard, la langue par défaut est l'anglais.
- Les composants du produit Sophos SafeGuard s'affichent sur l'ordinateur final dans la langue sélectionnée.

## 5.5 Interaction avec les autres produits SafeGuard

Notez les interactions suivantes :

### 5.5.1 Interaction avec SafeGuard LAN Crypt

Notez les éléments suivants :

- SafeGuard LAN Crypt 3.7x et Sophos SafeGuard 5.50 peuvent coexister sur le même ordinateur et sont entièrement compatibles.
- Les versions de SafeGuard LAN Crypt antérieures à 3.7x et Sophos SafeGuard 5.5x ne peuvent pas coexister sur un même ordinateur.

Si vous essayez d'installer Sophos SafeGuard 5.50 sur un ordinateur où SafeGuard LAN Crypt 3.6x ou version antérieure est déjà installé, l'installation est annulée et un message d'erreur s'affiche.

### 5.5.2 Interaction avec SafeGuard PrivateCrypto et SafeGuard PrivateDisk

Sophos SafeGuard 5.5x et les produits autonomes SafeGuard PrivateCrypto, ainsi que SafeGuard PrivateDisk à partir de la version 2.30, peuvent coexister sur le même ordinateur.

### **5.5.3 Interaction avec SafeGuard Removable Media**

Le module SafeGuard Data Exchange et SafeGuard Removable Media ne peuvent pas coexister sur le même ordinateur. Avant d'installer le module SafeGuard Data Exchange sur un ordinateur final, vérifiez si SafeGuard Removable Media est déjà installé. Si oui, vous devez désinstaller SafeGuard Removable Media avant d'installer SafeGuard Data Exchange sur l'ordinateur final.

**Remarque:** SafeGuard DataExchange n'est pas disponible avec ESDP.

## 6 Installation

La configuration de Sophos SafeGuard implique ce qui suit :

	Tâche	Package/outil d'installation	
		ESDP	SGE
1	<b>Configurez l'ordinateur qui est utilisé pour l'administration de Sophos SafeGuard.</b>		
	Installez SafeGuard Policy Editor.	SDEPolicyEditor.msi	SGNPolicyEditor.msi
	Pour effectuer une configuration initiale dans SafeGuard Policy Editor, créez une configuration par défaut pour le logiciel de chiffrement.	Assistant de configuration SafeGuard Policy Editor	
2	<b>Personnalisez le logiciel de chiffrement Sophos SafeGuard (facultatif)</b>		
	Créez d'autres paramètres de configuration via des stratégies prédéfinies (listes de comptes de service, par exemple).	Zone de stratégies SafeGuard Policy Editor	
	Générez d'autres packages de configuration (MSI) contenant des stratégies définies par l'utilisateur.	Outil de package de configuration SafeGuard Policy Editor	
3	<b>Configurez le logiciel de chiffrement Sophos SafeGuard sur les ordinateurs finaux.</b>		
	Afin de garantir la réussite de l'installation du logiciel de chiffrement Sophos SafeGuard, vous devez fournir aux ordinateurs finaux la configuration requise.	SGxClientPreinstall.msi	SGxClientPreinstall.msi
	Pour mettre en place Sophos SafeGuard Device Encryption (chiffrement basé sur volume), installez les éléments suivants :	SDEClient.msi ou	SGNClient.msi <b>Remarque:</b> Par ailleurs, dans ce package, Sophos SafeGuard Data Exchange (chiffrement basé sur fichier) peut être activé manuellement.
	Pour mettre en place Sophos SafeGuard Data Exchange (chiffrement basé sur fichier) uniquement, installez les éléments suivants :	non disponible avec ESDP	SGNClient_withoutDE.msi
	Déployez les packages de configuration sur les ordinateurs finaux.	<Packageconfig>.msi généré	

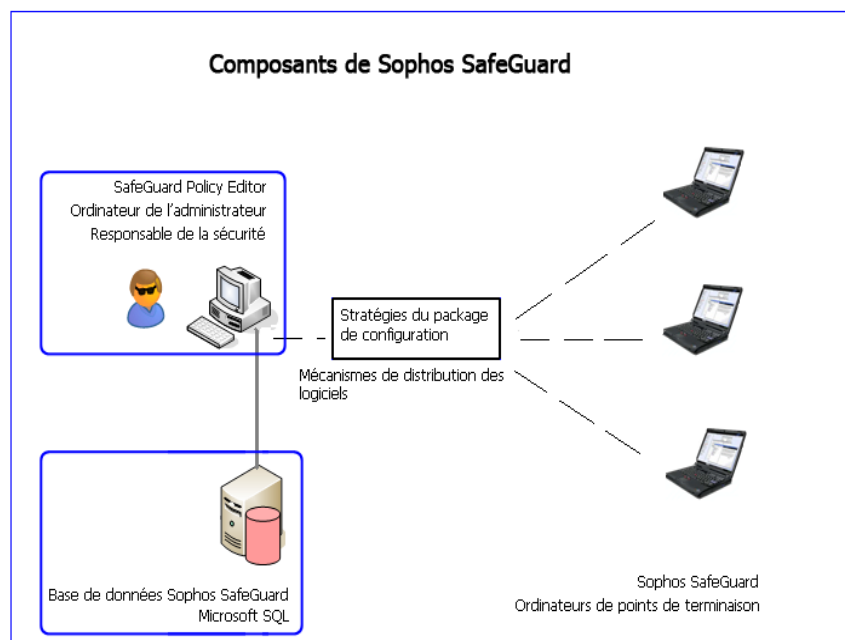
**Remarque:** Si le système d'exploitation des ordinateurs finaux est Windows 7 64 bits ou Windows Vista 64 bits, vous pouvez installer la variante 64 bits du package .msi « client », s'il existe (<nom package>\_64.msi).

## 6.1 Installation de SafeGuard Policy Editor

### Conditions préalables :

Les conditions préalables suivantes doivent être remplies :

- Vous devez disposer de droits d'administrateur Windows.
- Pour utiliser un serveur de base de données Microsoft SQL déjà installé, vous devez disposer des droits d'accès et des données de compte SQL nécessaires.
- .NET Framework 3.0 Service Pack 1 doit être installé sur l'ordinateur de l'administrateur. Vous pouvez le télécharger gratuitement sur le site <http://www.microsoft.com/fr/fr>.



Avant de déployer le logiciel de chiffrement sur les ordinateurs finaux, vous devez d'abord installer SafeGuard Policy Editor sur un ordinateur d'administrateur. Vous pouvez également effectuer la première installation de 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.

1. Si vous êtes client ESDP, double-cliquez sur le fichier SDEPolicyEditor.msi. Si vous êtes client SGE, double-cliquez sur le fichier SGNPolicyEditor.msi. Un assistant vous guidera tout au long des étapes nécessaires.
2. Cliquez sur **Suivant** dans la fenêtre de bienvenue.
3. Acceptez le contrat de licence.
4. Confirmez le chemin d'installation par défaut.  

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

SafeGuard Policy Editor est désormais installé sur l'ordinateur de l'administrateur. Ensuite, vous pouvez effectuer la configuration initiale de SafeGuard Policy Editor.

## **6.2 Réalisation de la configuration initiale dans l'assistant de configuration SafeGuard Policy Editor**

Vous devez disposer des droits d'administrateur Windows.

1. Après l'installation, 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**.

### **6.2.1 Configuration de la base de données**

Les stratégies et les paramètres du chiffrement Sophos SafeGuard sont stockés dans une base de données. Le flux de travail varie selon que vous créez une nouvelle base de données dans le cadre d'une première installation ou que vous utilisez une base de données existante. Si vous souhaitez installer des instances supplémentaires de SafeGuard Policy Editor, mieux vaut utiliser une base de données existante. Le personnel du support peut ainsi exécuter des procédures Challenge/Réponse.

1. Sur la page **Base de données**, exécutez l'une des actions suivantes :
  - Si vous effectuez l'installation pour la première fois, activez l'option **Créer une base de données**.
  - S'il ne s'agit pas d'une première installation ou si vous souhaitez réutiliser une base de données créée précédemment, activez l'option **Utiliser une base de données existante**. Sous **Nom de la base de données**, sélectionnez, dans la liste, le nom de la base de données.
2. Sous **Paramètres de base de données**, exécutez l'une des actions suivantes :
  - Si seule la base de données Microsoft SQL Express préinstallée est accessible, l'instance sera affichée dans **Instance de serveur SQL**. Vos informations d'identification Windows seront utilisées comme compte d'accès SQL. Cliquez sur **Suivant**.
  - Si vous utilisez une base de données existante ou si plusieurs instances de serveur SQL sont installées, cliquez sur **Modifier** pour sélectionner celle que vous souhaitez utiliser. Une boîte de dialogue dans laquelle vous pouvez configurer la connexion au serveur sélectionné s'affiche. Une fois que vous avez terminé, les paramètres sélectionnés s'affichent. Cliquez sur **Suivant**.

La connexion au serveur de base de données a été établie.

### **6.2.1.1 Réalisation d'une configuration supplémentaire pour la connexion à une base de données**

Procédez comme suit :

1. Dans **Connexion à la base de données**, sous **Serveur de base de données**, sélectionnez, dans la liste, le serveur de base de données SQL souhaité. Tous les serveurs de base de données disponibles sur votre ordinateur ou sur votre réseau s'affichent. (La liste est actualisée toutes les 12 minutes). Activez l'option **Utiliser SSL** pour protéger la connexion à ce serveur de base de données avec SSL.
2. Sous **Authentification**, sélectionnez le type d'authentification à utiliser pour accéder à la base de données :
  - Activez l'option **Utiliser l'authentification Windows NT** pour utiliser vos informations d'identification Windows.

**Remarque:** Utilisez ce type d'authentification si votre ordinateur appartient à un domaine. Une configuration supplémentaire peut cependant vous être demandée. L'utilisateur doit en effet être autorisé à accéder à la base de données.

- Activez l'option **Utiliser l'authentification SQL Server** pour accéder à la base de données avec vos informations d'identification SQL. Vous serez invité à saisir vos informations d'identification et à les confirmer. Si nécessaire, vous pouvez les obtenir auprès de votre administrateur SQL.

**Remarque:** Utilisez ce type d'authentification si votre ordinateur n'appartient à aucun domaine. Activez ensuite l'option **Utiliser SSL** pour sécuriser la connexion au/du serveur de base de données. Le chiffrement SSL requiert cependant un environnement SSL sur l'ordinateur sur lequel se trouve la base de données SQL que vous avez préalablement configurée. Pour plus d'informations, reportez-vous à : <http://www.sophos.com/support/knowledgebase/article/108339.html>. Grâce à l'authentification SQL, vous pouvez facilement effectuer la mise à niveau vers SafeGuard Management Center, ultérieurement.

3. Cliquez sur **Vérifier la connexion**. Si la connexion à la base de données SQL a été établie, un message de réussite correspondant s'affiche.
4. Cliquez deux fois sur **OK** pour confirmer.

## 6.2.2 Création du certificat du responsable de la sécurité (nouvelle base de données)

Si vous effectuez l'installation pour la première fois ou que vous créez une nouvelle base de données, un certificat pour le responsable de la sécurité est créé à des fins d'authentification. Un seul compte est créé pour chaque installation. En tant que responsable de la sécurité, vous pouvez accéder à SafeGuard Policy Editor pour créer des stratégies Sophos SafeGuard et configurer le logiciel de chiffrement pour les utilisateurs finaux. Pour récupérer une configuration de base de données endommagée, voir [Restauration d'une configuration corrompue de base de données](#), à la page 55.

1. Dans la page **Responsable de la sécurité**, le nom de ce dernier est déjà affiché.  
Pour les installations avec ESDP, le responsable de la sécurité s'appelle systématiquement Administrateur. Pour les autres installations, le nom de l'utilisateur actuel est affiché.
2. Saisissez et confirmez le mot de passe que vous utiliserez pour accéder à SafeGuard Policy Editor.  
Conservez le mot de passe en lieu sûr. Si vous le perdez, vous ne pourrez plus accéder à SafeGuard Policy Editor. Le support informatique doit disposer d'un accès au compte afin de pouvoir exécuter les tâches de récupération.
3. Cliquez sur **Suivant** pour confirmer les valeurs par défaut.

Le nouveau certificat du responsable de la sécurité est stocké dans le magasin de certificats. Un certificat d'entreprise sera ensuite créé.

### 6.2.3 Importation du certificat du responsable de la sécurité (si utilisation d'une base de données existante)

Si vous utilisez une base de données existante, vous devez importer le certificat du responsable de la sécurité. Seuls les certificats générés par SafeGuard Policy Editor peuvent être importés. Les certificats créés par une infrastructure de clé publique (par exemple, Verisign) ne sont pas autorisés.

1. Sur la page **Responsable de la sécurité**, cliquez sur **Importer** pour importer le certificat du responsable de la sécurité.
2. Recherchez le certificat en question, puis cliquez sur **Ouvrir**.
3. Saisissez le mot passe du fichier de récupération de clé que vous avez utilisé pour vous authentifier pour SafeGuard Policy Editor.
4. Cliquez sur **Oui** pour confirmer le certificat.
5. Saisissez et confirmez un mot de passe pour l'authentification pour Sophos SafeGuard Policy Editor.
6. Cliquez sur **Suivant**, puis sur **Terminer** pour terminer la configuration initiale.

La configuration initiale de SafeGuard Policy Editor est terminée.

### 6.2.4 Création du certificat d'entreprise

Le certificat d'entreprise est utilisé pour sécuriser les paramètres de stratégie de la base de données et des ordinateurs protégés par Sophos SafeGuard. Pour récupérer une configuration de base de données endommagée, voir [Restauration d'une configuration corrompue de base de données](#), à la page 55.

1. Dans la page **Entreprise**, saisissez le **Nom de l'entreprise**. Vérifiez que l'option **Créer automatiquement un certificat** est activée.

Si vous effectuez l'installation pour la première fois et que vous avez créé une nouvelle base de données, l'option **Créer automatiquement un certificat** est déjà activée. Le nom ne doit pas dépasser 64 caractères.

2. Cliquez sur **Suivant**.

Le nouveau certificat d'entreprise est stocké dans la base de données.

## 6.2.5 Sauvegarde de certificat

À des fins de récupération, les certificats du responsable de la sécurité et les certificats d'entreprise créés doivent être sauvegardés dans un emplacement sécurisé.

1. Sur la page **Sauvegarde de certificat**, définissez un emplacement pour stocker les sauvegardes de certificats.
2. Cliquez sur **Suivant** pour confirmer l'emplacement de stockage.

Les certificats sont sauvegardés à l'emplacement indiqué.

**Remarque:** 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. Vous en aurez besoin pour restaurer une installation endommagée ou une base de données corrompue,

**Remarque:** voir [Exportation des certificats de l'entreprise et du responsable principal de la sécurité](#), à la page 52.

## 6.2.6 Création de stratégies par défaut

Afin de faciliter l'administration, des stratégies par défaut qui couvrent un ensemble de paramètres de configuration recommandés sont fournies. Un package de configuration (MSI) contenant ces stratégies par défaut sera créé au cours de la configuration initiale. Pour en savoir plus sur les stratégies par défaut, voir [Stratégies par défaut](#), à la page 70.

**Remarque:** 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.

1. Sur la page **Stratégie par défaut**, vérifiez que l'option **Créer une stratégie par défaut** est activée.
2. Indiquez ou confirmez un emplacement pour stocker le package de configuration (MSI) qui sera créé et qui contient les stratégies par défaut.
3. Cliquez sur **Suivant** pour confirmer.

Le groupe de stratégies s'affiche dans la zone de navigation **Stratégies** de SafeGuard Policy Editor. Le package de configuration contenant ces stratégies s'affiche dans l'**Outil de package de configuration** de SafeGuard Policy Editor. Déployez le package de configuration sur les ordinateurs finaux lors de l'installation du logiciel de chiffrement. Si la configuration par défaut ne répond pas à vos besoins, vous pouvez créer des stratégies supplémentaires, les publier dans un package de configuration et les déployer sur les ordinateurs finaux.

## 6.2.7 Création d'un magasin de clés de récupération

Pour permettre une procédure Challenge/Réponse sur les ordinateurs protégés par Sophos SafeGuard, en cas d'oubli du mot de passe par exemple, des fichiers de récupération de clé spécifiques sont requis. Sur chaque ordinateur final, un fichier de récupération de clé de ce type est généré lors du déploiement de Sophos SafeGuard.

Pour terminer la procédure Challenge/Réponse, il est essentiel de stocker ces fichiers sur un partage réseau. Vous devez également fournir les droits d'accès au support afin qu'il puisse y accéder. Ce fichier de récupération de clé est chiffré par le certificat d'entreprise. Vous pouvez donc l'enregistrer en toute sécurité sur le réseau ou sur un support externe.

1. Sur la page **Clés de récupération**, activez l'option par défaut **Paramètres du partage réseau**.

Cette opération permet de créer un partage réseau SafeGuardRecoveryKeys\$ et un répertoire sur l'ordinateur local sur lequel seront automatiquement enregistrées les clés de récupération. Le partage est configuré pour n'autoriser que l'écriture des nouveaux fichiers à l'emplacement de partage. Vous pouvez modifier le chemin local si nécessaire. Le partage réseau doit se trouver sur un lecteur formaté avec NTFS. NTFS permet de paramétrer les autorisations d'accès. Si l'option **Paramètres du 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.

2. Dans la page **Clés de récupération**, fournissez au support les droits d'accès appropriés au partage de clés de récupération : cliquez sur **Suivant** pour accepter les autorisations par défaut. L'accès au partage de clés de récupération est géré via un nouveau groupe Windows nommé « SafeGuardRecoveryKeyAccess ». Par défaut, tous les membres du groupe d'administrateurs locaux y sont ajoutés. **Remarque :** dans un environnement de domaine, cela inclut également le groupe d'administrateurs de domaines qui est également membre du groupe d'administrateurs locaux. Cliquez sur **Autorisations** pour afficher ou modifier les membres du groupe.

**Remarque :**

Dans SafeGuard Policy Editor, il est possible de créer plusieurs packages de configuration de stratégies : par exemple un package pour les ordinateurs dans un environnement de domaine et un autre pour les ordinateurs autonomes.

3. Cliquez sur **Suivant**.

Les autorisations du partage réseau seront définies. Pour plus d'informations sur les autorisations, voir [Définitions des autorisations du partage réseau](#), à la page 28.

## 6.2.8 Définitions des autorisations du partage réseau

1. Dans **Autorisations du partage réseau**, exécutez l'une des actions suivantes :

- Cliquez sur **Ajouter des membres locaux** pour ajouter des membres locaux disposant des droits d'administration pour exécuter des actions de récupération.
- Cliquez sur **Ajouter des membres globaux** pour ajouter des membres globaux disposant des droits d'administration pour exécuter des actions de récupération.

2. Cliquez sur **OK**

Le groupe « SafeGuardRecoveryKeyAccess » créé sur l'ordinateur contient les membres affichés dans les **Autorisations du partage réseau**.

Les autorisations NTFS suivantes sont automatiquement définies sur le répertoire local spécifié :

- **Tout le monde** : Créer des fichiers - Les utilisateurs connectés à l'ordinateur Sophos SafeGuard sont autorisés à ajouter des fichiers mais ne peuvent pas rechercher de répertoire, ni supprimer ou lire de fichiers. **L'autorisation « Créer des fichiers » est disponible dans les Paramètres de sécurité avancés d'un répertoire.**
- **SafeGuardRecoveryKeyAccess** : Modifier - Tous les utilisateurs qui figurent dans la boîte de dialogue **Autorisations** sont autorisés à lire, supprimer ou ajouter des fichiers.
- **Administrateurs** : contrôle total

Sophos SafeGuard supprime également l'héritage des autorisations sur le répertoire afin de garantir que les autorisations ci-dessus ne seront pas accidentellement remplacées.

Le partage réseau SafeGuardRecoveryKeys\$ sera créé avec la permission suivante :

- **Tout le monde** : contrôle total

**Remarque:** Les autorisations obtenues regroupent les autorisations NTFS et les autorisations de partage. Les autorisations NTFS étant plus restrictives, ce sont elles qui s'appliquent.

Si vous souhaitez configurer manuellement un partage réseau, nous vous suggérons d'utiliser les mêmes paramètres d'autorisation que ceux qui sont décrits ci-dessus. Dans ce cas, vérifiez que vous avez manuellement désactivé l'héritage des autorisations sur le répertoire.

### 6.2.9 Finalisation de la configuration initiale

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

La configuration initiale de SafeGuard Policy Editor est terminée. Les fichiers Networkshare.xml et ConfigurationOutput.xml sont enregistrés dans le chemin temporaire. Le fichier Networkshare.xml contient les paramètres de configuration qui figurent dans l'assistant. Le fichier ConfigurationOutput.xml consigne tous les événements qui ont eu lieu pendant le traitement des paramètres de configuration. Les événements s'affichent sur la dernière page de l'assistant de configuration SafeGuard Policy Editor.

## 6.3 Configuration d'instances supplémentaires de SafeGuard Policy Editor

Vous pouvez configurer d'autres instances de SafeGuard Policy Editor afin de fournir un accès à l'équipe du support de Sophos SafeGuard pour qu'elle puisse effectuer les tâches de récupération.

1. Démarrez SafeGuard Policy Editor sur l'ordinateur correspondant. 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**, activez l'option **Utiliser une base de données existante**. Sous **Paramètres de base de données**, sélectionnez le nom de la base de données concernée dans la liste. Cliquez sur **Changer** pour sélectionner l'instance SQL Server à utiliser. Une boîte de dialogue dans laquelle vous pouvez configurer la connexion à l'instance sélectionnée s'affiche.
4. Dans la boîte de dialogue **Connexion à la base de données**, sous **Serveur de base de données**, sélectionnez, dans la liste, l'instance de base de données SQL souhaitée. Tous les serveurs de base de données disponibles sur votre ordinateur ou sur votre réseau s'affichent. (La liste est actualisée toutes les 12 minutes). Activez **Utiliser SSL** pour protéger la connexion avec cette base de données serveur via SSL. Cela peut s'avérer utile lorsque les certificats de la machine sont implémentés sur le serveur de base de données avant l'installation de Sophos SafeGuard.

5. Sous **Authentification**, sélectionnez le type d'authentification à utiliser pour accéder à la base de données :

- Activez l'option **Utiliser l'authentification Windows NT** pour utiliser vos informations d'identification Windows.

**Remarque:** Utilisez ce type d'authentification si votre ordinateur appartient à un domaine. Une configuration supplémentaire peut cependant vous être demandée. L'utilisateur doit en effet être autorisé à accéder à la base de données.

- Activez l'option **Utiliser l'authentification SQL Server** pour accéder à la base de données avec vos informations d'identification SQL. Vous serez invité à saisir vos informations d'identification et à les confirmer. Si nécessaire, vous pouvez les obtenir auprès de votre administrateur SQL.

**Remarque:** Utilisez ce type d'authentification si votre ordinateur n'appartient à aucun domaine. Activez ensuite l'option **Utiliser SSL** pour sécuriser la connexion au/du serveur de base de données. Le chiffrement SSL requiert cependant un environnement SSL sur l'ordinateur sur lequel se trouve la base de données SQL que vous avez préalablement configurée. Pour plus d'informations, reportez-vous à : <http://www.sophos.com/support/knowledgebase/article/108339.html>.

6. Cliquez sur **Vérifier la connexion**. Si la connexion à la base de données SQL a été établie, un message de réussite correspondant s'affiche.

7. Cliquez deux fois sur **OK** pour revenir à la page **Base de données**. Puis cliquez sur **Suivant**.

8. Dans la page **Responsable de la sécurité**, cliquez sur **Importer** pour importer le certificat du responsable de la sécurité associé à la base de données sélectionnée. Recherchez le certificat en question, puis cliquez sur **Ouvrir**.

Seuls les certificats générés par SafeGuard Policy Editor peuvent être importés. Les certificats créés par une infrastructure de clé publique (par exemple, Verisign) ne sont pas autorisés.

9. Saisissez le mot de passe du magasin de certificats.

10. Cliquez sur **Suivant**, puis sur **Terminer** pour terminer l'assistant de configuration de SafeGuard Policy Editor.

## 6.4 Configuration de Sophos SafeGuard sur les ordinateurs finaux

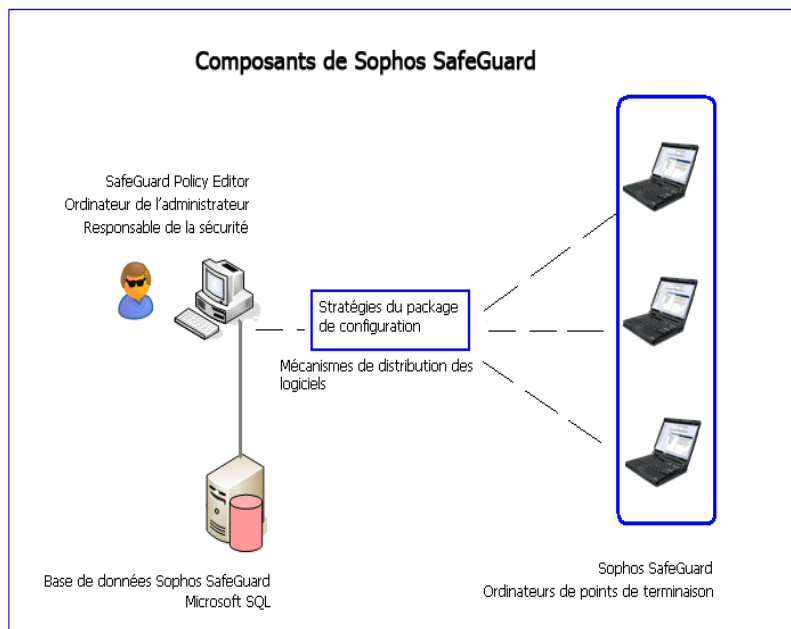
Selon l'installation, les ordinateurs finaux peuvent être équipés de plusieurs modules Sophos SafeGuard, voir [Sophos SafeGuard sur les ordinateurs finaux](#), à la page 8.

Il existe plusieurs méthodes pour déployer Sophos SafeGuard sur les ordinateurs finaux :

Les responsables de la sécurité peuvent effectuer la configuration des ordinateurs finaux localement ou lancer l'installation et la configuration initiale des ordinateurs finaux dans le cadre de la distribution centralisée des logiciels. L'installation standardisée sur plusieurs ordinateurs est ainsi garantie.

Les différentes options de déploiement sont également décrites dans l'article suivant : <http://www.sophos.de/support/knowledgebase/article/108426.html>

Pour en savoir plus sur le comportement de l'ordinateur après l'installation de Sophos SafeGuard, consultez le Guide de démarrage (chapitre *Première connexion après l'installation de Sophos SafeGuard*) et 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*).



### 6.4.1 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.

### 6.4.2 Configuration locale des ordinateurs finaux

Si vous souhaitez installer une version d'évaluation sur un ordinateur final, installez d'abord Sophos SafeGuard en local.

Avant d'installer le logiciel de chiffrement, préparez l'installation sur l'ordinateur final, voir [Préparation pour l'installation](#), à la page 16.

1. Connectez-vous à l'ordinateur en tant qu'administrateur.
2. Installez le package MSI de préparation, 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 appropriés.

**Remarque :** vous pouvez également installer vcredist\_x86.exe, téléchargeable sur le site suivant : <http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2> ou vérifier que le fichier MSVCR80.dll, version 8.0.50727.4053 se trouve sur l'ordinateur, dans le dossier Windows\WinSxS.

3. Double-cliquez sur le package d'installation (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	Sophos SafeGuard Easy
SDEClient.msi pour la variante 32 bits. SDEClient_x64.msi pour la variante 64 bits.	SGNClient.msi pour la variante 32 bits. SGNClient_x64.msi pour la variante 64 bits. SGNClient_withoutDE.msi pour SafeGuard Data Exchange uniquement. SGNClient_withoutDE_x64.msi pour SafeGuard Data Exchange uniquement, variante 64 bits.

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 et Data Exchange.
  - 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 ESDP.

6. Acceptez les valeurs par défaut dans les boîtes de dialogue suivantes.

Sophos SafeGuard est installé sur l'ordinateur final.

7. Dans SafeGuard Policy Editor, configurez le logiciel de chiffrement selon vos besoins :
  - Utilisez les stratégies prédéfinies créées par défaut lors de la configuration initiale de SafeGuard Policy Editor pour garantir un déploiement de stratégies rapide et facile.
  - Si les stratégies par défaut ne suffisent pas à satisfaire vos exigences particulières, vous pouvez définir vos propres stratégies dans SafeGuard Policy Editor (voir [Utilisation de stratégies](#), à la page 44). Pour en savoir plus sur le déploiement de stratégies sur les ordinateurs finaux, voir [Utilisation de packages de configuration](#), à la page 50.

Par exemple, votre stratégie de déploiement peut nécessiter la configuration d'un accès administratif à l'ordinateur pour le personnel de maintenance. Dans ce cas, vous devez définir une stratégie spécifique et créer un package de configuration contenant ces stratégies.

8. Installez le package de configuration (MSI) correspondant sur l'ordinateur.

Sophos SafeGuard a été configuré sur l'ordinateur final. Pour en savoir plus 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*).

### 6.4.3 Configuration centralisée des ordinateurs finaux

La configuration centralisée des ordinateurs finaux permet de garantir une installation standardisée sur plusieurs ordinateurs. Avant de déployer le logiciel de chiffrement, préparez l'installation sur les ordinateurs finaux, voir [Préparation pour l'installation](#), à la page 16.

1. Utilisez vos propres outils pour créer le package que vous souhaitez installer sur les ordinateurs finaux. Le package doit contenir les éléments suivants :

- **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.

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

Vous le trouverez dans le programme d'installation du produit que vous avez téléchargé sur le site Web de Sophos ou sur le CD du produit.

Pour les packages disponibles, voir [Installation](#), à la page 20.

**Remarque:** Si le système d'exploitation des ordinateurs finaux est Windows 7 64 bits ou Windows Vista 64 bits, vous pouvez installer la variante 64 bits du package .msi « client », s'il existe (<nom package>\_64.msi).

- **Package(s) de configuration**

Configurez le logiciel de chiffrement selon vos besoins :

Utilisez le package de configuration avec les stratégies prédéfinies par défaut créées lors de la configuration initiale de SafeGuard Policy Editor.

Si les stratégies par défaut ne suffisent pas à satisfaire vos exigences particulières, vous pouvez créer vos propres stratégies et les publier dans un package de configuration dans SafeGuard Policy Editor (voir *Utilisation de stratégies*, à la page 44). Pour en savoir plus sur le déploiement de stratégies sur les ordinateurs finaux, voir *Utilisation de packages de configuration*, à la page 50.

Par exemple, votre stratégie de déploiement peut nécessiter la configuration d'un accès administratif à l'ordinateur pour le personnel de maintenance. Dans ce cas, vous devez définir une stratégie spécifique et la déployer sur l'ordinateur via un package de configuration.

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

Nous recommandons d'utiliser msixec, l'outil de ligne de commande de Windows Installer, pour créer le script. Pour en savoir plus sur msixec, reportez-vous à voir *Commande pour l'installation centralisée*, à la page 35 ou [http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx)

2. Créez un dossier Logiciels pour centraliser toutes les applications.
3. Créez le script. Dans l'invite de commande, entrez la commande de Windows Installer msixec avec les paramètres appropriés.
4. À l'aide des mécanismes de distribution de logiciels de l'entreprise, distribuez ce package sur les ordinateurs finaux.

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 msixec de Windows Installer. Pour en savoir plus, voir voir *Raccourcis clavier pris en charge dans l'authentification au démarrage*, à la page 130, ainsi que les articles suivants :

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

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

### 6.4.3.1 Commande pour l'installation centralisée

Lorsque vous installez Sophos SafeGuard de manière centralisée sur les ordinateurs finaux, utilisez le composant Windows Installer « msixec ». Le composant « msixec » fait déjà partie de Windows XP, Vista et de Windows 7, et exécute automatiquement une installation préconfigurée de Sophos SafeGuard. Comme la source et la destination du programme d'installation peuvent également être spécifiées, l'installation standard sur plusieurs ordinateurs finaux existe.

Pour en savoir plus sur msiexec, consultez :[http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

## Syntaxe de la ligne de commande

```
msiexec /i <chemin+nom du package msi> /qn ADDLOCAL=ALL | <Fonctions>
<paramètre>
```

La syntaxe de la ligne de commande est constituée des éléments suivants:

- paramètres de Windows Installer, par exemple, les avertissements des journaux et les messages d'erreur envoyés dans un fichier lors de l'installation ;
- fonctions de Sophos SafeGuard à installer, par exemple, le chiffrement basé sur volume ;
- paramètres de Sophos SafeGuard, par exemple, pour spécifier le répertoire d'installation.

## Options de commande

Vous pouvez sélectionner toutes les options disponibles en utilisant msiexec.exe dans l'invite. Les principales options sont décrites ci-dessous.

Option	Description
/i	Spécifie qu'il s'agit d'une installation.
/qn	Exécute une installation sans interaction de l'utilisateur et n'affiche pas d'interface utilisateur.
ADDLOCAL=	Répertorie les fonctions à installer. Si aucune option n'est définie, toutes les fonctions de l'installation standard sont installées. Lorsque vous dressez la liste des fonctions sous ADDLOCAL, séparez les éléments par une virgule et non par un espace. - Respectez la casse. - Si vous sélectionnez une fonction, vous devez également ajouter toutes les fonctions parentes à la ligne de commande.
ADDLOCAL=ALL	Installe toutes les fonctions disponibles.
REBOOT=Force   ReallySuppress	Force ou supprime une réinitialisation après l'installation. Si rien n'est spécifié, la réinitialisation est forcée après l'installation.
/L* <chemin + nom de fichier>	Consigne tous les avertissements et messages d'erreur dans le fichier journal spécifié. Le paramètre /Le <chemin + nom de fichier> consigne uniquement les messages d'erreur.
InstallDir= <répertoire>	Spécifie le répertoire dans lequel installer le client Sophos SafeGuard. Si aucune valeur n'est spécifiée, le répertoire d'installation par défaut est <SYSTEM>:\PROGRAM FILES\SOPHOS.

### 6.4.3.2 Fonctions Sophos SafeGuard (ADDLOCAL)

Pour procéder à une installation centralisée, vous devez définir en amont quelles fonctions de Sophos SafeGuard sont à installer sur les ordinateurs finaux. Une liste des fonctions s'affiche après avoir indiqué ADDLOCAL dans la commande.

Le tableau ci-dessous dresse la liste des fonctions Sophos SafeGuard qui peuvent être installées sur les ordinateurs finaux.

#### Fonctions pour SafeGuard Device Encryption

SGNClient.msi, SDEClient.msi ou la variante respective 64 bits.

**Remarque:** Les fonctions **Client** et **Authentification** doivent être installées par défaut. Si vous sélectionnez une fonction, vous devez également ajouter les fonctions parentes à la ligne de commande !

Fonctions parentes	Fonction
<b>Client</b>	<b>Authentification</b> La fonction <b>Authentification</b> et sa fonction parente <b>Client</b> doivent être installées par défaut.
<b>Client, Authentification</b>	<b>CredentialProvider</b> Vous devez sélectionner cette fonction pour les ordinateurs dotés de Windows Vista. Elle permet d'activer la connexion à l'aide du fournisseur d'informations d'identification.
<b>Client, BaseEncryption</b>	<b>SectorBasedEncryption</b> Installe le chiffrement basé sur volume de Sophos SafeGuard avec les fonctions suivantes : Tous les volumes, supports amovibles inclus, peuvent être chiffrés via le chiffrement basé sur volume de Sophos SafeGuard. Authentification au démarrage (POA) de Sophos SafeGuard, récupération de Sophos SafeGuard avec procédure Challenge/Réponse
<b>Client</b>	<b>SecureDataExchange</b> <b>Remarque:</b> Cette fonction n'est pas prise en charge avec ESDP. SafeGuard Data Exchange avec chiffrement basé sur fichier est toujours installé localement et pour les supports amovibles. SafeGuard Data Exchange fournit le chiffrement sécurisé pour les supports amovibles. Les données peuvent être partagées avec d'autres utilisateurs en toute sécurité et facilement. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale. Si vous avez installé SafeGuard Data Exchange sur votre ordinateur, SafeGuard Portable l'est également. SafeGuard Portable permet aux données d'être partagées en toute sécurité avec les ordinateurs sur lesquels SafeGuard Data Exchange n'est pas installé.

## Fonctions pour SafeGuard Data Exchange

SGNClient\_withoutDE..msi ou la variante respective 64 bits.

**Remarque:** Ces packages d'installation ne sont pas prises en charge avec ESDP.

**Remarque:** Les fonctions **Client** et **Authentification** doivent être installées par défaut. Si vous sélectionnez une fonction, vous devez également ajouter les fonctions parentes à la ligne de commande !

Fonctions parentes	Fonction
<b>Client</b>	<b>Authentification</b> La fonction <b>Authentification</b> et sa fonction parente <b>Client</b> doivent être installées par défaut.
<b>Client</b>	<b>SecureDataExchange</b> <b>Remarque:</b> Cette fonction n'est pas prise en charge avec ESDP. SafeGuard Data Exchange avec chiffrement basé sur fichier est toujours installé localement et pour les supports amovibles. SafeGuard Data Exchange fournit le chiffrement sécurisé pour les supports amovibles. Les données peuvent être partagées avec d'autres utilisateurs en toute sécurité et facilement. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale. Si vous avez installé SafeGuard Data Exchange sur votre ordinateur, SafeGuard Portable l'est également. SafeGuard Portable permet aux données d'être partagées en toute sécurité avec les clients sur lesquels SafeGuard Data Exchange n'est pas installé.

## Exemple de commande pour le chiffrement basé sur volume

Une fois la commande indiquée ci-dessous exécutée :

- Les ordinateurs finaux sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
- L'authentification au démarrage Sophos SafeGuard pour l'authentification aux ordinateurs finaux Sophos SafeGuard est installée.
- Le chiffrement basé sur volume de Sophos SafeGuard est installé.
- Un fichier journal est créé.
- Le package de configuration par défaut est exécuté.

**Exemple :**

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log  
I:\Temp\SGxClientPreinstall.log  
  
msiexec /i F:\Software\SGNClient.msi /qn /log I:\Temp\SGNClient.log  
  
ADDLOCAL=Client,Authentication,BaseEncryption,SectorBasedEncryption  
  
InstallDir=C:\Program Files\Sophos\Sophos SafeGuard  
  
msiexec /i F:\Software\StandardConfig.msi /qn /log  
I:\Temp\StandardConfig.log
```

#### **6.4.4 Installation conforme à FIPS**

La certification FIPS décrit les conditions de sécurité requises des modules de chiffrement. Par exemple, les organismes publics aux États-Unis et au Canada doivent utiliser des logiciels certifiés conformes à FIPS 140-2 pour les informations de sécurité particulièrement sensibles.

Sophos SafeGuard utilise des algorithmes AES certifiés conformes à FIPS. Une nouvelle mise en œuvre et plus rapide des algorithmes AES est installée par défaut s'ils ne sont pas certifiés conformes à FIPS.

Pour utiliser la variante certifiée conforme à FIPS d'un algorithme AES, définissez la propriété FIPS\_AES sur 1 lors de l'installation du logiciel de chiffrement Sophos SafeGuard.

Deux méthodes sont possibles :

- Ajoutez la propriété au script de ligne de commande :  

```
msiexec /i F:\Software\SGNClient.msi FIPS_AES=1
```
- Procédez à une transformation.

## 7 Installation du Sophos SafeGuard sur les ordinateurs disposant de plusieurs systèmes d'exploitation

**Remarque:** Cette fonction n'est pas prise en charge avec ESDP (Endpoint Security and Data Protection).

Le client Sophos SafeGuard peut être installé sur un ordinateur afin d'en protéger les données si plusieurs systèmes d'exploitation sont installés sur différents volumes du disque dur. Sophos SafeGuard propose un système d'exécution. Le client d'exécution Sophos SafeGuard permet les opérations suivantes lorsqu'il est installé sur des volumes disposant d'une installation supplémentaire de Windows :

- L'installation Windows résidant sur ces volumes peut être initialisée correctement via un gestionnaire d'initialisation.
- Vous pouvez accéder aux partitions des volumes chiffrés avec une clé machine définie lors d'une installation complète du client Sophos SafeGuard.

### 7.1 Conditions requises et restrictions

Notez les éléments suivants :

- Le client d'exécution Sophos SafeGuard ne fournit aucune fonction ou fonctionnalité spécifique au client Sophos SafeGuard.
- Le client d'exécution SafeGuard Enterprise prend en charge uniquement les systèmes d'exploitation également pris en charge par le client SafeGuard Enterprise.
- Le bon fonctionnement des claviers USB peut être limité.
- Seuls les gestionnaires d'initialisation actifs à la suite d'une authentification au démarrage sont pris en charge.
- La prise en charge des gestionnaires d'amorçage tiers n'est pas garantie. Nous recommandons d'utiliser les gestionnaires d'initialisation de Windows.
- Le client d'exécution Sophos SafeGuard ne peut pas être mis à jour vers un client Sophos SafeGuard complet.
- Le package d'installation du client d'exécution doit être installé avant la version complète du package d'installation du client Sophos SafeGuard.
- Seuls les volumes chiffrés avec la clé machine définie de Sophos SafeGuard sont accessibles.

## **7.2 Préparations**

Pour configurer le client d'exécution Sophos SafeGuard, effectuez les préparatifs suivants dans l'ordre indiqué :

1. Assurez-vous que les volumes sur lesquels le client d'exécution Sophos SafeGuard est exécuté sont visibles au moment de l'installation et peuvent porter leur nom Windows (par exemple C:).
2. Choisissez les volumes du disque dur sur lesquels installer le client d'exécution Sophos SafeGuard. Dans Sophos SafeGuard, ces volumes sont définis en tant qu'installations secondaires de Windows. Il peut exister plusieurs installations secondaires de Windows. Installez le package SGNClientRuntime.msi (ou SGNClientRuntime\_x64.msi sur les systèmes d'exploitation Windows 7 64 bit or Windows Vista 64 bit).
3. Choisissez le volume du disque dur sur lequel installer la version complète du client Sophos SafeGuard. Dans Sophos SafeGuard, ce volume est défini en tant qu'installation primaire de Windows. Il ne peut exister qu'une seule installation primaire de Windows. Installez le package SGNClient.msi (ou SGNClient\_x64.msi sur les systèmes d'exploitation Windows 7 64 bit or Windows Vista 64 bit).

## **7.3 Configuration du client d'exécution Sophos SafeGuard**

Veillez procéder comme suit :

1. Sélectionnez les volumes secondaires requis du disque dur sur lesquels installer le client d'exécution Sophos SafeGuard.
2. Initialisez l'installation secondaire de Windows sur le volume sélectionné.
3. Installez le package d'installation d'exécution sur le volume sélectionné.
4. Confirmez les valeurs par défaut de la boîte de dialogue suivante du programme d'installation. Aucune sélection de fonction en particulier n'est nécessaire.
5. Sélectionnez un dossier d'installation du client d'exécution.
6. Confirmez pour terminer l'installation du client d'exécution.
7. Sélectionnez le volume primaire du disque dur sur lequel installer le client Sophos SafeGuard.
8. Initialisez l'installation primaire de Windows sur le volume sélectionné.

9. Installez le package d'installation préparatoire SGxClientPreinstall.msi pour fournir aux ordinateurs finaux les conditions requises pour un déploiement réussi du logiciel de chiffrement.
10. Installez le package d'installation du client Sophos SafeGuard sur le volume sélectionné
11. Créez le package de configuration et déployez le package de configuration sur l'ordinateur final.
12. Chiffrez les deux volumes à l'aide de la clé machine définie.

## **7.4 Initialisation à partir d'un volume secondaire via un gestionnaire d'initialisation**

Veillez procéder comme suit :

1. Démarrez l'ordinateur.
2. Connectez-vous à l'authentification au démarrage avec vos informations d'identification.
3. Démarrez le gestionnaire d'initialisation et sélectionnez le volume secondaire requis en tant que volume d'initialisation.
4. Réinitialisez l'ordinateur à partir de ce volume.

Vous pouvez accéder à chacun des volumes chiffrés avec la clé machine définie.

## **8 Connexion à SafeGuard Policy Editor**

Pour vous connecter à SafeGuard Policy Editor, procédez comme suit :

1. Démarrez SafeGuard Policy Editor. Une boîte de dialogue de connexion apparaît.
2. Saisissez le mot de passe du responsable de la sécurité spécifié lors de la configuration initiale, puis confirmez-le en cliquant sur **OK**.

SafeGuard Policy Editor s'ouvre.

## 9 Utilisation de stratégies

Les sections suivantes décrivent les tâches administratives relatives aux stratégies, par exemple la création, le regroupement et la sauvegarde.

Un ensemble de stratégies recommandées par défaut est déjà créé lors de la configuration initiale de SafeGuard Policy Editor, voir [Réalisation de la configuration initiale dans l'assistant de configuration SafeGuard Policy Editor](#), à la page 22. Pour obtenir une description détaillée de la stratégie par défaut, voir [Stratégies par défaut](#), à la page 70.

Par ailleurs, pour une description de tous les paramètres de stratégie disponibles avec Sophos SafeGuard, voir [Paramètres de stratégie](#), à la page 80.

### 9.1 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.






## 9.2 Édition de paramètres de stratégie

Lors de la sélection d'une stratégie dans la fenêtre de navigation, vous pouvez éditer les paramètres de la stratégie dans la zone d'action.

	<p>Une icône rouge en regard d'un paramètre « non configuré » indique qu'une valeur doit être définie pour ce paramètre de stratégie. Pour enregistrer la stratégie, vous devez tout d'abord sélectionner un paramètre autre que non configuré.</p>
---	---

### 9.2.1 Restauration des valeurs par défaut de paramètres de stratégie

Dans la barre d'outils, les icônes suivantes servent à la configuration des paramètres de stratégie :

	<p>Affiche les valeurs par défaut des paramètres de stratégie non configurés.</p>
	<p>Définit le paramètre de stratégie marqué comme « non configuré ».</p>
	<p>Définit tous les paramètres de stratégie d'une zone sur « non configuré ».</p>
	<p>Définit la valeur par défaut de la stratégie marquée.</p>
	<p>Définit tous les paramètres de stratégie d'une zone sur la valeur par défaut.</p>

## 9.2.2 Différences entre les stratégies spécifiques d'une machine et les stratégies spécifiques d'un utilisateur

Stratégie de couleur bleue	La stratégie s'applique uniquement aux machines et non aux utilisateurs.
Stratégie de couleur noire	La stratégie s'applique aux machines et aux utilisateurs.

## 9.3 Groupes de stratégies

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.

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.

### 9.3.1 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.

### 9.3.2 Résultats du regroupement de stratégies

Le résultat du regroupement de stratégies s'affiche séparément.

Pour afficher le résultat, cliquez sur l'onglet **Résultat**.

- Un onglet distinct s'affiche pour chaque type de stratégie.  
Les paramètres obtenus de la combinaison des stratégies individuelles dans un groupe s'affichent.
- Pour les stratégies de protection du périphérique, un onglet s'affiche pour chaque cible de stratégie (volumes d'initialisation, lecteur X, etc.).

## 9.4 Sauvegarde de stratégies et de groupes de stratégies

Vous pouvez créer des sauvegardes de stratégies et de groupes de stratégies dans des fichiers XML. Si nécessaire, les stratégies/groupes de stratégies correspondants peuvent ensuite être restaurés à partir de ces fichiers XML.

Pour créer une sauvegarde d'une stratégie/d'un groupe de stratégies :

1. Sélectionnez la stratégie/le groupe de stratégies dans la fenêtre de navigation sous **Éléments de stratégie** ou **Groupes de stratégies**.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Sauvegarder la stratégie**.  
La commande **Sauvegarder la stratégie** est également accessible dans le menu **Actions**.
3. Dans la boîte de dialogue **Enregistrer sous**, entrez le nom du fichier XML, puis sélectionnez un emplacement de stockage. Cliquez sur **Enregistrer**.

La sauvegarde de la stratégie/du groupe de stratégies est stockée sous forme de fichier XML dans le répertoire spécifié.

## 9.5 Restauration de stratégies et de groupes de stratégies

Pour restaurer une stratégie/un groupe de stratégies à partir d'un fichier XML, procédez comme suit :

1. Sélectionnez les **Éléments de stratégie/Groupes de stratégies** dans la fenêtre de navigation.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Restaurer une stratégie**.

La commande **Restaurer une stratégie** est également accessible depuis le menu **Actions**.

3. Sélectionnez le fichier XML à partir duquel la stratégie/le groupe de stratégies doit être restauré, puis cliquez sur **Ouvrir**.

La stratégie/le groupe de stratégies est restauré(e).

## 10 Utilisation de packages de configuration

Les ordinateurs protégés par Sophos SafeGuard reçoivent leurs stratégies de chiffrement via des packages de configuration créés dans SafeGuard Policy Editor. Afin que Sophos SafeGuard fonctionne correctement sur les ordinateurs finaux, vous devez créer un package de configuration contenant les groupes de stratégies appropriés et le distribuer sur les ordinateurs finaux.

Lors de la configuration initiale dans l'assistant de configuration de SafeGuard Policy Editor, un package de configurations par défaut et des stratégies par défaut peuvent déjà être créés.

Dès que vous modifiez des paramètres de stratégie, vous devez créer de nouveaux packages de configuration et les distribuer sur les ordinateurs finaux.

Les sections suivantes expliquent comment créer des packages de configuration et les distribuer sur les ordinateurs finaux.

**Remarque:** Vérifiez votre réseau et vos ordinateurs à intervalles réguliers pour détecter les packages de configuration obsolètes ou non utilisés. De même, pour des raisons de sécurité, n'oubliez pas de les supprimer.

### 10.1 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.

Après

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.

## 10.2 Distribution de packages de configuration

Les packages de configuration doivent être installés sur les ordinateurs finaux après l'installation du logiciel de chiffrement Sophos SafeGuard ou après toute modification apportée aux paramètres de configuration.

Distribuez le package de configuration sur les ordinateurs finaux via les mécanismes de distribution de logiciels de votre entreprise ou installez-le manuellement.

**Remarque:** Pour modifier les paramètres de stratégie d'un ordinateur protégé par Sophos SafeGuard, créez un nouveau package de configuration en incluant les stratégies modifiées, puis distribuez-le à l'ordinateur.

**Remarque:** Si vous tentez de remplacer un package de configuration récent par un plus ancien, l'installation échoue et un message d'erreur s'affiche.

## 11 Exportation des certificats de l'entreprise et du responsable principal de la sécurité

Lors d'une installation de Sophos SafeGuard, les deux éléments suivants sont essentiels et nécessitent une sauvegarde approfondie dans un emplacement sûr :

- le certificat de la société enregistré dans la base de données SafeGuard ;
- le certificat du responsable principal de la sécurité (MSO) se trouvant dans le magasin de certificats de l'ordinateur sur lequel SafeGuard Policy Editor est installé.

**Remarque:** Dans SafeGuard Policy Editor, le MSO correspond au responsable défini durant la configuration initiale. Avec l'ESDP, ce responsable est toujours appelé Administrateur.

Ces deux certificats peuvent être exportés sous la forme de fichiers .p12 à des fins de sauvegarde. Pour restaurer une installation de SafeGuard Policy Editor ou une base de données corrompue, importez le certificat approprié

**Remarque:** Nous conseillons de réaliser cette tâche immédiatement après la configuration initiale de SafeGuard Policy Editor.

### 11.1 Exportation des certificats d'entreprise

1. Dans la barre de menus de SafeGuard Policy Editor, sélectionnez **Outils > Options**.
2. Cliquez dans l'onglet **Certificats**, puis sur le bouton **Exporter** dans la section **Certificat d'entreprise**.
3. Vous êtes invité à saisir un mot de passe pour sécuriser le fichier exporté. Entrez un mot de passe, confirmez-le, puis cliquez sur **OK**.
4. Saisissez un nom et un emplacement de stockage pour le fichier, puis cliquez sur **OK**.

Le certificat de la société est exporté sous la forme d'un fichier .p12 à l'emplacement désigné et peut être utilisé à des fins de récupération.

## 11.2 Exportation du certificat du responsable principal de la sécurité

Pour sauvegarder le certificat du responsable principal de la sécurité connecté à SafeGuard Policy Editor, procédez comme suit :

1. Dans la barre de menus de SafeGuard Policy Editor, sélectionnez **Outils > Options**.
2. Cliquez dans l'onglet **Certificats**, puis sur le bouton **Exporter** dans la section **Certificat <Administrateur>**.
3. Vous êtes invité à saisir un mot de passe pour sécuriser le fichier exporté. Entrez un mot de passe, confirmez-le, puis cliquez sur **OK**.
4. Saisissez un nom et un emplacement de stockage pour le fichier à exporter, puis cliquez sur **OK** pour confirmer.

Le certificat du responsable principal de la sécurité actuellement connecté est exporté sous la forme d'un fichier .p12 à l'emplacement défini et peut être utilisé à des fins de récupération.

## 12 Restauration d'une installation corrompue de SafeGuard Policy Editor

Si l'installation de SafeGuard Policy Editor est corrompue mais que la base de données est intacte, l'installation peut facilement être restaurée en réinstallant SafeGuard Policy Editor et en utilisant la base de données existante ainsi que le certificat du responsable de la sécurité sauvegardé.

Procédez comme suit :

1. Réinstallez le package d'installation de Policy Editor. Ouvrez SafeGuard Policy Editor. L'assistant de configuration démarre automatiquement.
2. Dans **Base de données**, activez l'option **Utiliser une base de données existante**. Sous **Nom de la base de données**, sélectionnez, dans la liste, le nom de la base de données. Sous **Paramètres de base de données**, configurez la connexion à la base de données. Cliquez sur **Suivant**.
3. Dans **Responsable de la sécurité**, exécutez l'une des actions suivantes :
  - Si le fichier de certificat sauvegardé se trouve sur l'ordinateur, il s'affiche. Saisissez le mot de passe que vous utilisez pour vous authentifier pour Sophos SafeGuard Policy Editor.
  - Si le fichier de certificat sauvegardé est introuvable sur l'ordinateur, cliquez sur **Importer**. Recherchez le fichier de certificat sauvegardé et cliquez sur **Ouvrir** pour confirmer. Saisissez le mot de passe du fichier de certificat sélectionné. Cliquez sur **Oui** pour confirmer. Saisissez et confirmez un mot de passe pour l'authentification pour SafeGuard Policy Editor.
4. Cliquez sur **Suivant**, puis sur **Terminer** pour terminer la configuration de SafeGuard Policy Editor.

L'installation corrompue de SafeGuard Policy Editor est restaurée.

## 13 Restauration d'une configuration corrompue de base de données

La configuration corrompue d'une base de données peut être restaurée en réinstallant SafeGuard Policy Editor pour créer une nouvelle instance de la base de données, d'après les fichiers de certificat sauvegardés. Vous garantissez ainsi que tous les ordinateurs finaux Sophos SafeGuard existants acceptent les stratégies de la nouvelle installation. Cette procédure évite de devoir configurer et restaurer de zéro l'intégralité de la base de données.

- Les certificats de l'entreprise et du responsable principal de la sécurité pour la configuration de la base de données correspondante doivent avoir été exportés sous la forme de fichiers .p12, ainsi qu'être disponibles et valides.
- Vous devez également connaître les mots de passe de ces deux fichiers .p12, ainsi que du magasin de certificats.

Procédez comme suit :

1. Réinstallez le package d'installation de Policy Editor. Ouvrez SafeGuard Policy Editor. L'assistant de configuration démarre automatiquement.
2. Dans **Base de données**, sélectionnez **Créer une base de données**. Sous **Paramètres de base de données**, configurez la connexion à la base de données. Cliquez sur **Suivant**.
3. Dans **Responsable de la sécurité**, sélectionnez le responsable de la sécurité approprié. Désactivez l'option **Créer automatiquement un certificat**. Cliquez sur **Importer** pour rechercher le fichier de certificat sauvegardé. Saisissez et confirmez le mot de passe du responsable de la sécurité pour le magasin de certificats. Le certificat est alors importé. Cliquez sur **Suivant**.
4. Dans **Informations sur l'entreprise**, désactivez l'option **Créer automatiquement un certificat**. Cliquez sur **Importer** pour rechercher le fichier de certificat sauvegardé qui contient le certificat d'entreprise valide. Vous êtes invité à saisir le mot de passe défini pour le magasin de certificats. Entrez le mot de passe, puis cliquez sur **OK** pour confirmer. Cliquez sur **Oui** pour confirmer le message. Le certificat d'entreprise est alors importé.
5. Dans **Sauvegarde de certificat**, définissez un emplacement pour stocker les sauvegardes de certificats. Cliquez sur **Suivant** pour confirmer l'emplacement de stockage.

6. Dans **Stratégie par défaut**, désactivez l'option **Créer une stratégie par défaut**, puis cliquez sur **Suivant**.
7. Dans **Clés de récupération**, désactivez l'option **Créer un partage réseau**, puis cliquez sur **Suivant** et sur **Terminer**.

La configuration de la base de données est restaurée.

## 14 Options d'accès administratif sur les ordinateurs finaux

Afin de fournir un accès destiné aux tâches administratives après l'installation de Sophos SafeGuard sur les ordinateurs finaux, Sophos SafeGuard propose 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, sans avoir à activer l'authentification au démarrage et sans être ajoutés en tant qu'utilisateurs sur les ordinateurs. Les listes de comptes de service sont définies dans la zone **Stratégies** de Sophos SafeGuard Policy Editor et affectées aux ordinateurs finaux via des stratégies intégrées aux packages de configuration Sophos SafeGuard. Les utilisateurs figurant sur une liste de compte de service sont considérés comme des utilisateurs invités lorsqu'ils se connectent à l'ordinateur final.

**Remarque:** Les listes de comptes de service sont affectées aux ordinateurs finaux via des stratégies. Elles doivent être affectées dans le premier package de configuration Sophos SafeGuard, créé pour la configuration des ordinateurs finaux. Vous pouvez mettre à jour les listes de comptes de service en créant un nouveau package de configuration et en le déployant sur les ordinateurs finaux.

### ■ Comptes d'accès POA pour connexion POA

Les comptes d'accès POA sont des comptes locaux prédéfinis qui permettent aux utilisateurs (membres de l'équipe informatique, par exemple) de se connecter à des ordinateurs finaux pour effectuer des tâches administratives après activation de l'authentification au démarrage. Les comptes d'accès POA permettent les connexions à partir de l'authentification au démarrage. Il n'y a pas de connexion automatique à Windows. Il s'agit de comptes d'accès définis dans la zone **Utilisateurs** de Sophos SafeGuard Policy Editor (ID utilisateur et mot de passe) et affectés aux ordinateurs finaux via des groupes d'accès POA inclus dans des packages de configuration Sophos SafeGuard.

### 14.1 Listes de comptes de service pour la connexion Windows

Exemple de scénario type pour la plupart des mises en œuvre : une équipe de déploiement installe de nouveaux ordinateurs dans un environnement sur lequel Sophos SafeGuard est installé. Pour des raisons d'installation ou de vérification, les opérateurs en charge du déploiement peuvent se connecter à leur ordinateur respectif avant que l'utilisateur final ne reçoive sa nouvelle machine et n'active l'authentification au démarrage.

Le scénario peut ainsi être le suivant :

1. Sophos SafeGuard est installé sur un ordinateur final.
2. Après le redémarrage de l'ordinateur, l'opérateur en charge du déploiement se connecte.
3. L'opérateur en charge du déploiement est ajouté à l'authentification au démarrage, qui devient active.

À la réception de son ordinateur, l'utilisateur final ne pourra pas se connecter au POA et doit effectuer une procédure Challenge/Réponse.

Pour éviter que ces opérations d'administration sur un ordinateur protégé par Sophos SafeGuard n'activent l'authentification au démarrage et n'entraînent l'ajout des opérateurs en charge du déploiement comme autant d'utilisateurs possibles de l'ordinateur, Sophos SafeGuard offre la possibilité de créer des listes de comptes de service pour les ordinateurs protégés par Sophos SafeGuard. Les utilisateurs figurant dans ces listes sont ainsi traités comme des utilisateurs invités de Sophos SafeGuard.

Avec les comptes de service, le scénario est le suivant :

1. Sophos SafeGuard est installé sur un ordinateur final.
2. Après le redémarrage de l'ordinateur, un opérateur en charge du déploiement et figurant sur une liste de comptes de service se connecte (connexion Windows).
3. D'après la liste de comptes de service appliquée à l'ordinateur, l'utilisateur est identifié comme un compte de service et traité comme utilisateur invité.

L'opérateur en charge du déploiement ne sera pas ajouté à POA et l'authentification au démarrage ne sera pas active. L'utilisateur final peut se connecter et activer le POA.

**Remarque:** Vous devez affecter des listes de comptes de service dans le premier package de configuration Sophos SafeGuard, créé pour configurer les ordinateurs finaux. Vous pouvez mettre à jour les listes de comptes de service en créant un nouveau package de configuration avec des paramètres modifiés et en le déployant sur les ordinateurs finaux.

### **14.1.1 Création de listes de comptes de service et ajout d'utilisateurs**

Pour créer des listes de comptes de service et ajouter des utilisateurs, procédez comme suit :

1. Cliquez sur **Stratégies** dans la zone de navigation.
2. Sélectionnez **Listes de comptes de service** dans la fenêtre de navigation de la stratégie.
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 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 respectives, 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 à présent enregistrée et peut être sélectionnée dès lors que vous créez une stratégie.

#### **14.1.1.1 Informations supplémentaires pour la saisie de noms d'utilisateur et de domaine**

Il existe plusieurs méthodes servant à spécifier des utilisateurs dans les listes de comptes de service. Deux champs sont alors utilisés : **Nom d'utilisateur** et **Nom du domaine** (voir [Présentation des différentes combinaisons de connexion](#), à la page 59). Par ailleurs, certaines restrictions s'appliquent concernant la saisie de ces champs (voir [Restrictions](#), à la page 60).

##### **Présentation des différentes combinaisons de connexion**

Les deux champs séparés **Nom d'utilisateur** et **Nom du domaine** par entrée de liste offrent la souplesse nécessaire pour couvrir toutes les combinaisons disponibles de connexion, par exemple utilisateur@domaine ou domaine\utilisateur.

Pour gérer plusieurs combinaisons nom d'utilisateur/nom de domaine, vous pouvez utiliser les astérisques (\*) comme caractères génériques. Une astérisque peut remplacer le premier signe, le dernier signe ou être le seul signe autorisé.

Par exemple :

- **Nom d'utilisateur** : Administrateur
- **Nom du domaine** : \*

Cette combinaison indique tous les utilisateurs ayant pour nom d'utilisateur Administrateur et se connectant à un poste en local ou en réseau quel qu'il soit.

Le nom du domaine prédéfini [LOCALHOST] disponible dans la liste déroulante du champ **Nom du domaine** indique une connexion à n'importe quel poste de travail en local.

Par exemple :

- **Nom d'utilisateur** : "\*admin"
- **Nom du domaine** : [LOCALHOST]

Cette combinaison indique tous les utilisateurs dont le nom d'utilisateur se termine par « admin » et se connectant à un poste en local quel qu'il soit.

En outre, les utilisateurs ont la possibilité de se connecter de plusieurs manières différentes, par exemple :

- utilisateur : test, domaine : masociété ou
- utilisateur : test, domaine : masociété.com.

Étant donné que les spécifications de domaine dans les listes de comptes de service ne sont pas automatiquement résolues, trois méthodes sont disponibles qui servent à indiquer correctement le domaine :

- Vous savez exactement comment l'utilisateur va se connecter et saisir le domaine en conséquence.
- Vous créez plusieurs entrées de liste de comptes de service.
- Vous utilisez les caractères génériques pour couvrir l'ensemble des cas (utilisateur : test, domaine : masociété\*).

**Remarque:** Afin d'éviter les problèmes liés au fait que Windows peut utiliser des noms tronqués et non la même séquence de caractères, il est recommandé de saisir le NomComplet ou le nom Netbios, voire d'utiliser des caractères génériques.

## **Restrictions**

Un astérisque ne peut remplacer que le premier signe, le dernier signe ou être le seul signe autorisé. Voici quelques exemples de chaînes valides et non valides concernant l'utilisation des astérisques :

- Exemples de chaînes valides : admin\*, \*, \*strator, \*minis\*.
- Exemple de chaînes non valides : \*\*, Admin\*trator, Ad\*minst\*.

En outre, les restrictions suivantes s'appliquent :

- Le caractère ? n'est pas autorisé dans les noms de connexion utilisateur.
- Les caractères / \ [ ] : ; | = , + \* ? < > " ne sont pas autorisés dans les noms de domaine.

### 14.1.2 Modification et suppression des listes de comptes de service

En tant que responsable de la sécurité possédant le droit **Modifier les listes de comptes de service**, vous pouvez modifier ou supprimer les listes de comptes de service à tout moment :

- Pour modifier une liste de comptes de service, double-cliquez dans la fenêtre de navigation de la stratégie. La liste de comptes de service s'ouvre et vous pouvez alors ajouter, supprimer ou modifier les noms d'utilisateur dans la liste.
- Pour supprimer une liste de comptes de service, sélectionnez-la dans la fenêtre de navigation de stratégie, ouvrez le menu contextuel, puis sélectionnez **Supprimer**.

### 14.1.3 Affectation d'une liste de comptes de service via une stratégie

Pour sélectionner et affecter une liste de comptes de services, procédez comme suit :

1. Créez une nouvelle stratégie du type **Authentification** ou sélectionnez-en une existante.
2. Sous **Options de connexion**, sélectionnez la liste de comptes de service requise dans la liste déroulante du champ **Liste de comptes de service**.

**Remarque :** Le paramètre par défaut de ce champ est [**Aucune liste**], c'est-à-dire qu'aucune liste de comptes de service ne s'applique. Les opérateurs en charge du déploiement se connectant à l'ordinateur après l'installation de Sophos SafeGuard ne seront ainsi pas traités comme des utilisateurs invités. Ils pourront activer l'authentification au démarrage et être ajoutés à l'ordinateur. Pour annuler l'affectation d'une liste de comptes de service, sélectionnez l'option [**Aucune liste**].

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

Vous pouvez à présent transférer la stratégie sur l'ordinateur concerné et rendre les comptes de service disponibles sur l'ordinateur.

**Remarque:** Si vous sélectionnez des listes de comptes de service différentes dans des stratégies qui le sont tout autant et qui correspondent toutes au RSOP (Resulting Set of Policies, paramètre valide pour un ordinateur/groupe spécifique), la liste de comptes de service affectée à la dernière stratégie appliquée prendra le dessus sur toutes les listes de comptes de service précédemment assignées. Les listes de comptes de service ne seront pas fusionnées.

#### **14.1.4 Transfert de la stratégie à l'ordinateur de l'utilisateur**

Les ordinateurs protégés par Sophos SafeGuard reçoivent des stratégies via des packages de configuration créés dans SafeGuard Policy Editor, à partir du menu **Outils > Outil de package de configuration**.

Soit le fichier de configuration est distribué via les mécanismes de distribution de logiciels de l'entreprise, soit le package de configuration est installé manuellement sur les ordinateurs finaux.

**Remarque:** Étant donné que la fonctionnalité de liste de comptes de service se révèle tout particulièrement utile et importante durant l'installation initiale, au cours de la phase de déploiement d'une mise en œuvre, nous recommandons d'inclure une stratégie **Authentification** avec les paramètres de liste de comptes de service requis dans le groupe de stratégies transféré avec le package de configuration Sophos SafeGuard initial créé dans SafeGuard Policy Editor pour aider à la configuration de l'ordinateur final après l'installation.

**Remarque:** Pour modifier les paramètres de stratégie d'un ordinateur protégé par Sophos SafeGuard, créez un nouveau package de configuration en incluant les stratégies modifiées, puis distribuez-le à l'ordinateur.

#### **14.1.5 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.

##### **14.1.5.1 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).

### 14.1.6 Consignation des événements

Les actions accomplies concernant les listes de comptes de service sont signalées par les événements du journal suivants :

#### **SafeGuard Policy Editor**

- Liste de comptes de service <nom> créée
- Liste de comptes de service <nom> modifiée
- Liste de comptes de service <nom> supprimée

#### **Sophos SafeGuard ordinateur final**

- Utilisateur Windows <nom domaine/utilisateur> connecté à <horodatage> sur le poste <nom domaine/poste de travail> avec un compte de service SGN.
- Nouvelle liste de comptes de service <nom> importée.
- Liste de comptes de service <nom> supprimée.

## 14.2 Comptes d'accès POA pour connexion POA

Une fois Sophos SafeGuard installé et l'authentification au démarrage (POA) activée, vous devez pouvoir accéder aux ordinateurs finaux pour exécuter des tâches administratives. Grâce aux comptes d'accès POA, les utilisateurs (notamment des membres de l'équipe informatique) peuvent se connecter aux ordinateurs finaux à partir de l'authentification au démarrage, pour exécuter des tâches administratives, sans avoir à lancer de procédure Challenge/Réponse. Il n'y a pas de connexion automatique à Windows. Les utilisateurs doivent se connecter avec leurs comptes Windows existants.

Vous pouvez créer des comptes d'accès POA dans Sophos SafeGuard Policy Editor, les regrouper dans des groupes de comptes d'accès POA et affecter ces groupes à des ordinateurs finaux via les packages de configuration Sophos SafeGuard. Les utilisateurs, par exemple les comptes d'accès POA, inclus dans le groupe de comptes d'accès POA affecté, seront ajoutés au POA et pourront se connecter à l'aide de leur nom d'utilisateur et de leur mot de passe prédéfinis.

### 14.2.1 Création de comptes d'accès POA

Pour créer 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.
5. Vous pouvez également entrer une description pour le nouvel utilisateur POA.
6. Saisissez un mot de passe pour le nouveau compte d'accès POA et confirmez-le.

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.

7. 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**.

### 14.2.2 Modification du mot de passe d'un compte d'accès POA

Pour modifier le mot de passe d'un compte 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**, **Utilisateurs POA**, sélectionnez un utilisateur POA.
3. Dans le menu contextuel de cet utilisateur POA, sélectionnez **Propriétés**.

La boîte de dialogue **Propriétés de l'utilisateur POA** s'affiche.

4. Dans l'onglet **Général**, sous **Mot de passe utilisateur**, saisissez le nouveau mot de passe et confirmez-le.
5. Cliquez sur **OK**.

Le nouveau mot de passe est attribué au compte d'accès POA correspondant.

### 14.2.3 Suppression de comptes d'accès POA

Pour supprimer 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, Utilisateurs POA**, sélectionnez un compte d'accès POA.
3. Cliquez avec le bouton droit de la souris sur le compte d'accès POA et sélectionnez **Supprimer** dans le menu contextuel.

Le compte d'accès POA (utilisateur POA) est supprimé et n'apparaît plus dans la fenêtre de navigation **Utilisateurs**.

**Remarque:** Si l'utilisateur appartient à un ou plusieurs groupes POA, le compte d'accès POA sera également supprimé de ces groupes. Le compte d'accès POA reste cependant disponible sur l'ordinateur final jusqu'à ce qu'un nouveau package de configuration soit créé et attribué. Pour en savoir plus sur les groupes POA, voir [Création de groupes de comptes d'accès POA](#), à la page 65. Pour en savoir plus sur la modification des attributions des comptes d'accès POA, voir [Modification des attributions de comptes d'accès POA sur les ordinateurs finaux](#), à la page 68

### 14.2.4 Création de groupes de comptes d'accès POA

Pour pouvoir attribuer des comptes d'accès POA aux ordinateurs finaux via des packages de configuration, les comptes doivent être organisés par groupes. Lors de la création de packages de configuration, vous pouvez sélectionner un groupe de comptes d'accès POA à attribuer.

Pour créer des groupes de 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 **Groupes POA**.
3. Dans le menu contextuel des **Groupes POA**, cliquez sur **Nouveau > Créer un groupe**.

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

4. Dans le champ **Nom complet**, saisissez le nom du nouveau groupe POA.
5. Vous pouvez également entrer une description pour le nouveau groupe POA.
6. Cliquez sur **OK**.

Le nouveau groupe de comptes d'accès POA a été créé et est affiché sous **Groupes POA** dans la zone de navigation **Utilisateurs**. Vous pouvez maintenant ajouter des utilisateurs (comptes d'accès POA) au groupe de comptes d'accès POA.

### 14.2.5 Ajout de comptes aux groupes de comptes d'accès POA

Pour ajouter des utilisateurs (comptes d'accès POA) aux groupes de 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, Groupe POA**, sélectionnez un groupe POA.

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

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

La boîte de dialogue **Sélectionner un objet membre** s'affiche.

4. Sélectionnez l'utilisateur (compte d'accès POA) que vous souhaitez ajouter au groupe.
5. Cliquez sur **OK**.

Le compte d'accès POA est ajouté au groupe, puis affiché dans l'onglet **Membres**.

**Remarque:** Vous pouvez également ajouter des comptes aux groupes en sélectionnant l'utilisateur POA (compte d'accès POA) dans la fenêtre de navigation et en exécutant les étapes décrites ci-dessus. Avec cette approche, l'onglet **Membre de** s'affiche dans la zone d'action une fois l'utilisateur sélectionné. Cet onglet affiche les groupes auxquels l'utilisateur a été attribué. Le flux de travail de base reste le même.

### 14.2.5.1 Suppression de membres des groupes de comptes d'accès POA

Pour supprimer des membres (comptes d'accès POA) des groupes de 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, Groupe POA**, sélectionnez un groupe POA.

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

3. Sélectionnez l'utilisateur que vous souhaitez supprimer du groupe.
4. Dans la barre d'outils de SafeGuard Policy Editor, cliquez sur l'icône **Supprimer** (croix rouge).

L'utilisateur est supprimé du groupe.

**Remarque:** Vous pouvez également supprimer des membres des groupes en sélectionnant l'utilisateur POA (compte d'accès POA) dans la fenêtre de navigation et en exécutant les étapes décrites ci-dessus. Avec cette approche, l'onglet **Membre de** s'affiche dans la zone d'action une fois l'utilisateur sélectionné. Cet onglet affiche les groupes auxquels l'utilisateur a été attribué. Le flux de travail de base reste le même.

### 14.2.6 Attribution de comptes d'accès POA aux ordinateurs finaux

Pour attribuer des groupes de comptes d'accès POA à des ordinateurs finaux via des packages de configuration, procédez comme suit :

1. Dans SafeGuard Policy Editor, sélectionnez **Outil de package de configuration** dans le menu **Outils**.
2. Sélectionnez un package de configuration existant ou créez-en un nouveau.  
Pour en savoir plus sur la création d'un nouveau package de configuration, voir [Création d'un package de configuration Sophos SafeGuard](#), à la page 50.
3. Spécifiez un **Groupe POA** préalablement créé dans la zone **Utilisateurs** de SafeGuard Policy Editor qui sera appliqué aux ordinateurs.

Le paramètre par défaut pour le groupe POA est **Aucun groupe**.

Vous pouvez également sélectionner un groupe vide par défaut. Ce groupe peut être utilisé pour supprimer les attributions de groupes de comptes d'accès POA sur les ordinateurs finaux. Pour plus d'informations, voir [Suppression de comptes d'accès POA des ordinateurs finaux](#), à la page 68.

4. Spécifiez un chemin de sortie pour le fichier MSI.
5. Cliquez sur **Créer un MSI client autonome**.
6. Déployez le fichier MSI sur les ordinateurs finaux.

L'installation du fichier MSI entraîne l'ajout des utilisateurs (comptes d'accès POA) inclus dans le groupe au POA sur les ordinateurs finaux. Les comptes d'accès POA sont disponibles pour la connexion POA.

### **14.2.7 Modification des attributions de comptes d'accès POA sur les ordinateurs finaux**

Pour modifier l'attribution des comptes d'accès POA sur les ordinateurs finaux, procédez comme suit :

1. Créez un nouveau groupe de comptes d'accès POA ou modifiez-en un existant.
2. Créez un nouveau package de configuration, puis sélectionnez un groupe de comptes d'accès POA existant ou celui que vous venez de créer.

Le nouveau groupe de comptes d'accès POA est disponible sur l'ordinateur final. Tous les utilisateurs inclus sont ajoutés à l'authentification au démarrage. Le nouveau groupe remplace le précédent. Les groupes de comptes d'accès POA ne sont pas fusionnés.

### **14.2.8 Suppression de comptes d'accès POA des ordinateurs finaux**

Les comptes d'accès POA peuvent être supprimés des ordinateurs finaux en leur attribuant un groupe de comptes d'accès POA vide. Procédez comme suit :

1. Dans SafeGuard Policy Editor, sélectionnez **Outil de package de configuration** dans le menu **Outils**.
2. Sélectionnez un package de configuration existant ou créez-en un nouveau.  
Pour en savoir plus sur la création d'un nouveau package de configuration, voir [Création d'un package de configuration Sophos SafeGuard](#), à la page 50.
3. Spécifiez un **Groupe POA** vide créé préalablement dans la zone **Utilisateurs** de SafeGuard Policy Editor, ou sélectionnez le groupe POA vide fourni dans l'**Outil de package de configuration**.
4. Spécifiez un chemin de sortie pour le fichier MSI.

5. Cliquez sur **Créer un MSI client**.
6. Déployez le fichier MSI sur les ordinateurs finaux.

L'installation du fichier MSI entraîne la suppression de tous les comptes d'accès POA des ordinateurs finaux. Tous les utilisateurs concernés sont donc supprimés de l'authentification au démarrage.

### **14.2.9 Connexion à un ordinateur final à l'aide d'un compte d'accès POA**

Pour vous connecter à l'aide d'un compte d'accès POA, procédez comme suit :

1. Mettez l'ordinateur sous tension.

La boîte de dialogue de connexion de l'authentification au démarrage s'affiche.

2. Saisissez le **Nom d'utilisateur** et le **Mot de passe** du compte d'accès POA prédéfini.

Vous n'êtes pas connecté à Windows automatiquement. Par conséquent, la boîte de dialogue de connexion Windows s'affiche.

3. Dans le champ **Domaine**, sélectionnez le domaine <**POA**>.
4. Connectez-vous à Windows à l'aide de votre compte utilisateur Windows existant.

## 15 Stratégies par défaut

Lors de la configuration initiale de SafeGuard Policy Editor, un groupe de stratégies avec des paramètres de chiffrement et d'authentification prédéfinis est créé par défaut. Un package de configuration (.msi) contenant ces stratégies par défaut est créé automatiquement.

Après l'installation les éléments de la stratégie et le groupe sont affichés dans la zone de navigation **Stratégies** de SafeGuard Policy Editor. Le package de configuration par défaut créé automatiquement s'affiche et peut être sélectionné dans l'**Outil de package de configuration** de SafeGuard Policy Editor.

**Remarque:** Les stratégies par défaut ne peuvent être créées que lors de la configuration initiale de SafeGuard Policy Editor, dans l'assistant de configuration de SafeGuard Policy Editor.

Les deux sections suivantes dressent la liste des stratégies par défaut disponibles avec SGE (SafeGuard Easy) et ESDP (Endpoint Security and Data Protection).

Pour obtenir une description détaillée des paramètres de stratégie, voir [Paramètres de stratégie](#), à la page 80.

## 15.1 Stratégies par défaut disponibles avec SGE

Les valeurs par défaut s'appliquent automatiquement aux options dont les paramètres sont définis sur non configuré, dans le tableau ci-dessous. Les valeurs par défaut correspondantes sont indiquées entre parenthèses.

**Remarque:** Pour obtenir une description détaillée des paramètres de stratégie, voir [Paramètres de stratégie](#), à la page 80.

Stratégie	Paramètres
<p><b>Stratégie de paramètres généraux par défaut</b> Type de stratégie : Paramètres généraux</p>	<p><b>Personnalisation :</b></p> <ul style="list-style-type: none"> <li>■ Langue utilisée sur le client : Utiliser les paramètres de langue du SE</li> </ul> <p><b>Récupération de connexion :</b></p> <ul style="list-style-type: none"> <li>■ Activer la récupération de connexion après la corruption du cache local Windows : Non</li> </ul> <p><b>Local Self Help :</b></p> <ul style="list-style-type: none"> <li>■ Activer Local Self Help : Oui</li> <li>■ Longueur minimale des réponses : 3</li> <li>■ L'utilisateur peut définir des questions personnalisées : Oui</li> </ul> <p><b>Challenge/Réponse (C/R) :</b></p> <ul style="list-style-type: none"> <li>■ Activer la récupération de la connexion (via C/R) : Oui</li> <li>■ Autoriser la connexion automatique à Windows : Oui</li> </ul>

Stratégie	Paramètres
<p><b>Stratégie d'authentification par défaut</b>                      Type de stratégie : <b>Authentification</b></p>	<p><b>Accès :</b></p> <ul style="list-style-type: none"> <li>■ <b>L'utilisateur peut uniquement booter à partir du disque dur : Oui</b></li> </ul> <p><b>Options de connexion :</b></p> <ul style="list-style-type: none"> <li>■ <b>Mode de connexion : ID utilisateur/Mot de passe</b></li> <li>■ <b>Afficher les échecs de connexion pour cet utilisateur : Non</b></li> <li>■ <b>Afficher la dernière connexion utilisateur : Non</b></li> <li>■ <b>Désactiver la déconnexion forcée dans le verrouillage du poste de travail : Non</b></li> <li>■ <b>Activer la présélection utilisateur/domaine : Oui</b></li> <li>■ <b>Authentification automatique à Windows : Laisser l'utilisateur choisir</b></li> </ul> <p><b>Échecs de connexion :</b></p> <ul style="list-style-type: none"> <li>■ <b>Nbre maximum d'échecs de connexion : 16</b></li> <li>■ <b>Messages d'échec de connexion dans l'authentification au démarrage (POA) : Standard</b></li> </ul> <p><b>Réaction aux échecs de connexion :</b></p> <ul style="list-style-type: none"> <li>■ <b>Verrouiller la machine : Oui</b></li> </ul>

Stratégie	Paramètres
<p><b>Stratégie de mot de passe par défaut</b> Type de stratégie : <b>Mot de passe</b></p>	<p><b>Mot de passe :</b></p> <ul style="list-style-type: none"> <li>■ <b>Longueur min. du mot de passe : 4</b></li> <li>■ <b>Longueur max. du mot de passe : 128</b></li> <li>■ <b>Nombre min. de lettres : 0</b></li> <li>■ <b>Nombre min. de chiffres : 0</b></li> <li>■ <b>Nombre min. de caractères spéciaux : 0</b></li> <li>■ <b>Respecter la casse : Non</b></li> <li>■ <b>Interdire la succession de touches horizontales : Non</b></li> <li>■ <b>Interdire la succession de touches verticales : Non</b></li> <li>■ <b>Utilisation interdite de 3 caractères consécutifs ou plus : Non</b></li> <li>■ <b>Utilisation interdite du nom d'utilisateur en tant que mot de passe : Non</b></li> <li>■ <b>Utiliser la liste des mots de passe interdits : Non</b></li> </ul> <p><b>Modifications :</b></p> <ul style="list-style-type: none"> <li>■ <b>Modification du mot de passe autorisée après un min. de (jours) : non configuré</b> (la valeur par défaut 0 s'applique)</li> <li>■ <b>Expiration du mot de passe après (jours) : non configuré</b> (la valeur par défaut 999 s'applique)</li> <li>■ <b>Avertir d'un changement obligatoire avant (jours) : non configuré</b> (la valeur par défaut 10 s'applique)</li> </ul> <p><b>Général :</b></p> <ul style="list-style-type: none"> <li>■ <b>Longueur de l'historique de mot de passe : 0</b></li> </ul>

Stratégie	Paramètres
<p><b>Stratégie de chiffrement de périphérique par défaut</b> Type de stratégie : <b>Protection du périphérique</b></p>	<p>Chiffre tous les disques internes.</p> <ul style="list-style-type: none"> <li>■ <b>Mode de chiffrement du support : Basé sur le volume</b></li> </ul> <p>Paramètres généraux :</p> <ul style="list-style-type: none"> <li>■ <b>Algorithme à utiliser pour le chiffrement : AES256</b></li> <li>■ <b>Clé à utiliser pour le chiffrement : Clé machine définie</b></li> <li>■ <b>L'utilisateur est autorisé à créer une clé locale : non configuré</b> (la valeur par défaut <b>Oui</b> s'applique)</li> </ul> <p>Paramètres basés sur le volume :</p> <ul style="list-style-type: none"> <li>■ <b>L'utilisateur peut ajouter ou supprimer des clés d'un volume chiffré : non configuré</b> (la valeur par défaut <b>Non</b> s'applique)</li> <li>■ <b>Réaction aux volumes non chiffrés : Accepter tous les supports et chiffrer</b></li> <li>■ <b>L'utilisateur peut déchiffrer le volume : Non</b></li> <li>■ <b>Poursuivre sur les secteurs incorrects : Oui</b></li> </ul>
<p><b>Stratégie d'échange de données par défaut</b> Type de stratégie : <b>Protection du périphérique</b></p>	<p>Chiffre les supports amovibles</p> <ul style="list-style-type: none"> <li>■ <b>Mode de chiffrement du support : Basé sur fichier</b></li> </ul> <p>Paramètres généraux :</p> <ul style="list-style-type: none"> <li>■ <b>Algorithme à utiliser pour le chiffrement : AES256</b></li> <li>■ <b>Clé à utiliser pour le chiffrement : Toute clé du jeu de clés utilisateur</b></li> </ul> <p>Paramètres basés sur le fichier :</p> <ul style="list-style-type: none"> <li>■ <b>Copier portable SG vers support amovible : Oui</b></li> <li>■ <b>L'utilisateur peut définir une passphrase de support pour les périphériques : Oui</b></li> </ul>

Stratégie	Paramètres
<p><b>Stratégie de réglages machine par défaut</b>                      Type de stratégie : <b>Paramètres machine spécifiques</b></p>	<p><b>Authentification au démarrage (POA) :</b></p> <ul style="list-style-type: none"> <li>■ Activer l'authentification au démarrage : <b>Oui</b></li> </ul> <p><b>Éveil par appel réseau (WOL) sécurisé :</b></p> <ul style="list-style-type: none"> <li>■ Nombre de connexions automatiques : <b>0</b></li> <li>■ Connexion à Windows autorisée pendant le WOL : <b>Non</b></li> </ul> <p><b>Options d'affichage :</b></p> <ul style="list-style-type: none"> <li>■ Afficher l'identification de la machine : <b>Nom du poste de travail</b></li> <li>■ Afficher la mention légale : <b>Non</b></li> <li>■ Afficher des infos supplémentaires : <b>Jamais</b></li> <li>■ Activer et afficher l'icône de la barre d'état système : <b>Oui</b></li> <li>■ Afficher les icônes en chevauchement dans l'Explorateur : <b>Oui</b></li> <li>■ Clavier virtuel en POA : <b>Oui</b></li> </ul> <p><b>Options d'installation :</b></p> <ul style="list-style-type: none"> <li>■ Désinstallation autorisée : <b>Oui</b></li> <li>■ Activer la protection anti-sabotage Sophos : <b>Oui</b></li> </ul> <p><b>Remarque:</b> Ce paramètre ne s'applique qu'aux ordinateurs finaux sur lesquels Sophos Endpoint Security and Control version 9.5 ou ultérieure est installé.</p>
<p><b>Stratégie de consignation par défaut</b>                      Type de stratégie : <b>Consignation</b></p>	<p>Consigne uniquement les erreurs dans le journal d'événements, ignore les autres.</p>

## 15.2 Stratégies par défaut disponibles avec ESDP

Les valeurs par défaut s'appliquent automatiquement aux options dont les paramètres sont définis sur non configuré, dans le tableau ci-dessous. Les valeurs par défaut correspondantes sont indiquées entre parenthèses.

**Remarque:** Pour obtenir une description détaillée des paramètres de stratégie, voir [Paramètres de stratégie](#), à la page 80.

Stratégie	Paramètres
<p><b>Stratégie de paramètres généraux par défaut</b> Type de stratégie : Paramètres généraux</p>	<p><b>Personnalisation :</b></p> <ul style="list-style-type: none"> <li>■ <b>Langue utilisée sur le client : Utiliser les paramètres de langue du SE</b></li> </ul> <p><b>Récupération de connexion :</b></p> <ul style="list-style-type: none"> <li>■ <b>Activer la récupération de connexion après la corruption du cache local Windows : Non</b></li> </ul> <p><b>Local Self Help :</b></p> <ul style="list-style-type: none"> <li>■ <b>Activer Local Self Help : Oui</b></li> <li>■ <b>Longueur minimale des réponses : 3</b></li> <li>■ <b>L'utilisateur peut définir des questions personnalisées : Oui</b></li> </ul> <p><b>Challenge/Réponse (C/R) :</b></p> <ul style="list-style-type: none"> <li>■ <b>Activer la récupération de la connexion (via C/R) : Oui</b></li> <li>■ <b>Autoriser la connexion automatique à Windows : Oui</b></li> </ul>

Stratégie	Paramètres
<p><b>Stratégie d'authentification par défaut</b> Type de stratégie : <b>Authentification</b></p>	<p>Accès :</p> <ul style="list-style-type: none"><li>■ L'utilisateur peut uniquement booter à partir du disque dur : <b>Oui</b></li></ul> <p>Options de connexion :</p> <ul style="list-style-type: none"><li>■ Mode de connexion : <b>ID utilisateur/Mot de passe</b></li><li>■ Afficher les échecs de connexion pour cet utilisateur : <b>Non</b></li><li>■ Afficher la dernière connexion utilisateur : <b>Non</b></li><li>■ Désactiver la déconnexion forcée dans le verrouillage du poste de travail : <b>Non</b></li><li>■ Activer la présélection utilisateur/domaine : <b>Oui</b></li><li>■ Authentification automatique à Windows : <b>Laisser l'utilisateur choisir</b></li></ul> <p>Échecs de connexion :</p> <ul style="list-style-type: none"><li>■ Nbre maximum d'échecs de connexion : <b>16</b></li><li>■ Messages d'échec de connexion dans l'authentification au démarrage (POA) : <b>Standard</b></li></ul> <p>Réaction aux échecs de connexion :</p> <ul style="list-style-type: none"><li>■ Verrouiller la machine : <b>Oui</b></li></ul>

Stratégie	Paramètres
<p><b>Stratégie de mot de passe par défaut</b> Type de stratégie : <b>Mot de passe</b></p>	<p><b>Mot de passe :</b></p> <ul style="list-style-type: none"> <li>■ <b>Longueur min. du mot de passe : 4</b></li> <li>■ <b>Longueur max. du mot de passe : 128</b></li> <li>■ <b>Nombre min. de lettres : 0</b></li> <li>■ <b>Nombre min. de chiffres : 0</b></li> <li>■ <b>Nombre min. de caractères spéciaux : 0</b></li> <li>■ <b>Respecter la casse : Non</b></li> <li>■ <b>Interdire la succession de touches horizontales : Non</b></li> <li>■ <b>Interdire la succession de touches verticales : Non</b></li> <li>■ <b>Utilisation interdite de 3 caractères consécutifs ou plus : Non</b></li> <li>■ <b>Utilisation interdite du nom d'utilisateur en tant que mot de passe : Non</b></li> <li>■ <b>Utiliser la liste des mots de passe interdits : Non</b></li> </ul> <p><b>Modifications :</b></p> <ul style="list-style-type: none"> <li>■ <b>Modification du mot de passe autorisée après un min. de (jours) : non configuré</b> (la valeur par défaut 0 s'applique)</li> <li>■ <b>Expiration du mot de passe après (jours) : non configuré</b> (la valeur par défaut 999 s'applique)</li> <li>■ <b>Avertir d'un changement obligatoire avant (jours) : non configuré</b> (la valeur par défaut 10 s'applique)</li> </ul> <p><b>Général :</b></p> <ul style="list-style-type: none"> <li>■ <b>Longueur de l'historique de mot de passe : 0</b></li> </ul>

Stratégie	Paramètres
<p><b>Stratégie de chiffrement de périphérique par défaut</b> Type de stratégie : <b>Protection du périphérique</b></p>	<p>Chiffre tous les disques internes.</p> <ul style="list-style-type: none"> <li>■ <b>Mode de chiffrement du support : Basé sur le volume</b></li> </ul> <p>Paramètres généraux :</p> <ul style="list-style-type: none"> <li>■ <b>Algorithme à utiliser pour le chiffrement : AES256</b></li> <li>■ <b>Clé à utiliser pour le chiffrement : Clé machine définie</b></li> </ul> <p>Paramètres basés sur le volume :</p> <ul style="list-style-type: none"> <li>■ <b>Réaction aux volumes non chiffrés : Accepter tous les supports et chiffrer</b></li> <li>■ <b>L'utilisateur peut déchiffrer le volume : Non</b></li> <li>■ <b>Poursuivre sur les secteurs incorrects : Oui</b></li> </ul>
<p><b>Stratégie de réglages machine par défaut</b> Type de stratégie : <b>Paramètres machine spécifiques</b></p>	<p>Authentification au démarrage (POA) :</p> <ul style="list-style-type: none"> <li>■ <b>Activer l'authentification au démarrage : Oui</b></li> </ul> <p>Éveil par appel réseau (WOL) sécurisé :</p> <ul style="list-style-type: none"> <li>■ <b>Nombre de connexions automatiques : 0</b></li> <li>■ <b>Connexion à Windows autorisée pendant le WOL : Non</b></li> </ul> <p>Options d'affichage :</p> <ul style="list-style-type: none"> <li>■ <b>Afficher l'identification de la machine : Nom du poste de travail</b></li> <li>■ <b>Afficher la mention légale : Non</b></li> <li>■ <b>Afficher des infos supplémentaires : Jamais</b></li> <li>■ <b>Activer et afficher l'icône de la barre d'état système : Oui</b></li> <li>■ <b>Afficher les icônes en chevauchement dans l'Explorateur : Oui</b></li> <li>■ <b>Clavier virtuel en POA : Oui</b></li> </ul> <p>Options d'installation :</p> <ul style="list-style-type: none"> <li>■ <b>Désinstallation autorisée : Oui</b></li> <li>■ <b>Activer la protection anti-sabotage Sophos : Oui</b></li> </ul> <p><b>Remarque:</b> Ce paramètre ne s'applique qu'aux ordinateurs finaux sur lesquels Sophos Endpoint Security and Control version 9.5 ou ultérieure est installé.</p>
<p><b>Stratégie de consignation par défaut</b> Type de stratégie : <b>Consignation</b></p>	<p>Consigne uniquement les erreurs dans le journal d'événements, ignore les autres.</p>

## 16 Paramètres de stratégie

Les stratégies de Sophos SafeGuard comportent tous les paramètres devant être actifs pour mettre en œuvre une stratégie de sécurité à l'échelle de l'entreprise sur les ordinateurs des utilisateurs.

Les stratégies de SafeGuard Enterprise peuvent comporter des paramètres pour les domaines suivants (types de stratégies) :

- **Paramètres généraux**

Contient, par exemple, des paramètres de taux de transfert, d'images d'arrière-plan, etc.

- **Authentification**

Contient des paramètres de mode de connexion, verrouillage de périphérique, etc.

- **Mots de passe**

Définit la configuration minimale des mots de passe des utilisateurs.

- **Passphrases pour SafeGuard Data Exchange**

**Remarque:** Ces paramètres ne sont pas pris en charge avec ESDP (Endpoint Security and Data Protection).

Définit la configuration minimale des passphrases. Les passphrases sont utilisées pour un échange de données sécurisé avec SafeGuard Data Exchange lors de la génération d'une clé.

- **Protection du périphérique**

Contient les paramètres de chiffrement basé sur volume ou sur fichier (notamment les paramètres de SafeGuard Data Exchange et de SafeGuard Portable) : algorithmes, clés, lecteurs sur lesquels les données doivent être chiffrées, etc.

- **Paramètres machine spécifiques**

Contient les paramètres d'authentification au démarrage (activer/désactiver), d'éveil par appel réseau sécurisé, d'options d'affichage, etc.







- **Consignation**

Définit les événements à consigner.





Les sections suivantes fournissent une description détaillée de tous les paramètres de stratégie disponibles dans SafeGuard Policy Editor.



Différents paramètres sont disponibles avec SGE (SafeGuard Easy) et ESDP (Endpoint Security and Data Protection). Pour ESDP, les paramètres de stratégie basés sur fichier et les paramètres relatifs à SafeGuard Data Exchange ne sont pas disponibles. Dans les sections suivantes, les paramètres disponibles pour SGE et ESDP sont marqués d'une coche dans la colonne correspondante.





## 16.1 Paramètres généraux

Paramètre de stratégie	SGE	ESDP	Explication
<b>PERSONNALISATION</b>			
<b>Langue utilisée sur le client</b>			Détermine la langue d'affichage des paramètres de Sophos SafeGuard sur l'ordinateur final. Outre les langues prises en charge, les utilisateurs peuvent sélectionner le paramètre de langue du système d'exploitation de l'ordinateur final.
<b>RÉCUPÉRATION DE LA CONNEXION</b>			
<b>Activer la récupération de connexion après la corruption du cache local Windows</b>			Le cache local Windows stocke toutes les clés et stratégie ainsi que les fichiers certifiés par l'utilisateur et les fichiers d'audit. Les données stockées dans le cache local sont signées et ne peuvent pas être modifiées manuellement. Lorsque le cache local Windows est corrompu, la récupération de connexion est désactivée par défaut, c'est-à-dire que sa restauration s'effectue automatiquement à partir de la sauvegarde. Aucune procédure Challenge/Réponse n'est donc requise pour réparer le cache local Windows. Si le cache local Windows doit être réparé expressément via une procédure Challenge/Réponse, définissez ce champ sur « OUI ».
<b>Activer Local Self Help</b>			
<b>Activer Local Self Help</b>			Détermine si un utilisateur Sophos SafeGuard est autorisé à se connecter à son ordinateur via Local Self Help en cas d'oubli de son mot de passe. Grâce à Local Self Help, il peut se connecter en répondant à un nombre spécifique de questions prédéfinies dans l'authentification au démarrage.

Paramètre de stratégie	SGE	ESDP	Explication
			<p>Ainsi, l'utilisateur peut de nouveau accéder à son ordinateur même si aucune connexion téléphonique ou Internet n'est disponible.</p> <p>Une procédure Challenge/Réponse n'est pas nécessaire dans ce cas. Local Self Help permet de réduire les interventions et les coûts relatifs au support. La connexion automatique à Windows doit être activée pour que l'utilisateur puisse utiliser Local Self Help. Dans le cas contraire, Local Self Help ne fonctionne pas.</p>
<b>Longueur minimale des réponses</b>	✔	✔	Dans ce champ, définissez la longueur minimale (en caractères) des réponses à enregistrer pour Local Self Help sur l'ordinateur final.
<b>Texte de bienvenue sous Windows</b>	✔	✔	Dans ce champ, vous pouvez spécifier le texte d'informations à afficher dans la première boîte de dialogue au démarrage de l'assistant de Local Self Help sur l'ordinateur final. Avant de pouvoir spécifier le texte ici, il doit être créé et enregistré.
<b>L'utilisateur peut définir des questions personnalisées</b>	✔	✔	<p>En tant que responsable de la sécurité, vous pouvez définir de manière centralisée les questions auxquelles répondre et les distribuer sur l'ordinateur final à l'aide de la stratégie. Toutefois, vous pouvez également accorder aux utilisateurs le droit de définir des questions personnalisées. Pour autoriser les utilisateurs à définir des questions personnalisées, sélectionnez <b>Oui</b> dans ce champ.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<b>Challenge / Réponse (CR)</b>			
<b>Activer la récupération de la connexion (via C/R)</b>			<p>Détermine si, dans le cadre d'une récupération de connexion, un utilisateur est autorisé à générer un challenge dans l'authentification au démarrage (POA) afin de pouvoir accéder de nouveau à son ordinateur via une procédure Challenge/Réponse.</p> <ul style="list-style-type: none"> <li>■ <b>OUI</b> : l'utilisateur peut générer un challenge et le bouton <b>Challenge</b> du POA est actif. Dans ce cas, l'utilisateur peut de nouveau accéder à son ordinateur via une procédure C/R.</li> <li>■ <b>NON</b> : l'utilisateur n'est pas autorisé à générer un challenge et le bouton <b>Challenge</b> du POA est inactif. Dans ce cas, l'utilisateur ne peut pas lancer de procédure C/R pour accéder de nouveau à son ordinateur.</li> </ul> <p>Sophos SafeGuard propose également la méthode de récupération de connexion Local Self Help. Elle peut être activée via le paramètre de stratégie <b>Activer Local Self Help</b>.</p>
<b>Texte d'informations</b>			<p>Affiche un texte d'informations lorsqu'une procédure Challenge/Réponse est lancée dans l'authentification au démarrage. Les textes d'informations peuvent inclure, par exemple « Veuillez contacter le bureau de support en appelant au 01234-56789. ». Avant d'indiquer un texte ici, vous devez le créer sous forme de fichier texte dans la zone de navigation <b>Stratégies</b> sous <b>Texte d'informations</b>.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<p><b>Autoriser la connexion Windows automatique</b></p>			<p>Permet à l'utilisateur de se connecter automatiquement à Windows après s'être authentifié, en utilisant la procédure Challenge/Réponse.</p> <ul style="list-style-type: none"> <li>■ <b>OUI</b> : l'utilisateur est automatiquement connecté à Windows.</li> <li>■ <b>NON</b> : l'écran de connexion Windows apparaît.</li> </ul> <p><b>Cas d'application</b> : Un utilisateur a oublié son mot de passe. Après la procédure Challenge/Réponse, Sophos SafeGuard connecte l'utilisateur à l'ordinateur sans mot de passe Sophos SafeGuard. Dans ce cas, la connexion automatique à Windows est désactivée et l'écran de connexion Windows s'affiche. L'utilisateur ne peut pas se connecter car il ne connaît pas le mot de passe Sophos SafeGuard (= mot de passe Windows). <b>OUI</b> autorise la connexion automatique ; l'utilisateur n'est pas bloqué au niveau de l'écran de connexion de Windows.</p>
<p><b>IMAGES</b></p>			<p>Condition préalable : Les nouvelles images doivent être enregistrées dans la <b>zone de navigation de stratégie</b> de Sophos SafeGuard Policy Editor, sous <b>Images</b>. Les images ne sont disponibles qu'une fois enregistrées. Formats pris en charge : .BMP, PNG, JPEG.</p>





Paramètre de stratégie	SGE	ESDP	Explication
<p><b>Image d'arrière-plan dans POA</b></p> <p><b>Image d'arrière-plan dans POA (basse résolution)</b></p>			<p>Remplace l'image bitmap bleue d'arrière-plan par l'écran SafeGuard pour l'arrière-plan que vous avez sélectionné. Par exemple, les clients peuvent utiliser le logo de l'entreprise dans POA et lors de la connexion de Windows. Taille de fichier maximale pour toutes les images bitmap d'arrière-plan : 500 Ko</p> <p>Normal :</p> <ul style="list-style-type: none"> <li>■ Résolution : 1024 x 768 (mode VESA)</li> <li>■ Couleurs : illimitées</li> </ul> <p>Basse :</p> <ul style="list-style-type: none"> <li>■ Résolution : 640 x 480 (mode VGA)</li> <li>■ Couleurs : 16 couleurs</li> </ul>
<p><b>Image de connexion dans POA</b></p> <p><b>Image de connexion dans POA (basse résolution)</b></p>			<p>Change l'image bitmap Sophos SafeGuard affichée dans la boîte de dialogue de connexion à POA. Par exemple, le logo de l'entreprise peut être affiché dans cette boîte de dialogue.</p> <p>Normal :</p> <ul style="list-style-type: none"> <li>■ Résolution : 413 x 140 pixels</li> <li>■ Couleurs : illimitées</li> </ul> <p>Basse :</p> <ul style="list-style-type: none"> <li>■ Résolution : 413 x 140 pixels</li> <li>■ Couleurs : 16 couleurs</li> </ul>




## 16.2 Authentification

La manière dont les utilisateurs se connectent à leur ordinateur est déterminée par une stratégie du type **Authentification**.

Paramètre de stratégie	SGE	ESDP	Explication
<b>ACCÈS</b>			
<b>Les utilisateurs peuvent booter à partir du disque dur uniquement</b>	✔	✔	Détermine si les utilisateurs peuvent démarrer leur PC à partir du disque dur et/ou d'un autre support. <b>OUI</b> : les utilisateurs peuvent booter à partir du disque dur uniquement. L'Authentification au démarrage (POA) n'offre pas la possibilité de démarrer le PC avec une disquette ou un autre support externe. <b>NON</b> : les utilisateurs peuvent démarrer le PC à partir du disque dur, d'une disquette ou d'un support externe (USB, CD, etc.).
<b>OPTIONS DE CONNEXION</b>			
<b>Mode de connexion</b>	✔	✔ Options disponibles pour ce paramètre : <b>ID utilisateur/Mot de passe</b> <b>Remarque:</b> La connexion par empreinte digitale n'est pas disponible avec ESDP.	Détermine comment un utilisateur doit s'authentifier dans POA. <ul style="list-style-type: none"> <li>■ <b>ID utilisateur/Mot de passe</b> : La connexion doit s'effectuer par l'intermédiaire du nom d'utilisateur et du mot de passe dans POA.</li> <li>■ <b>Empreinte digitale</b> : Sélectionnez ce paramètre pour permettre la connexion à l'aide du lecteur d'empreintes digitales Lenovo. Les utilisateurs auxquels cette stratégie s'applique peuvent alors se connecter à l'aide d'une empreinte digitale ou d'un nom d'utilisateur et d'un mot de passe. Cette procédure offre le niveau de sécurité maximum. Lors de la connexion, l'utilisateur fait glisser son doigt sur le lecteur d'empreintes digitales..</li> </ul>

Paramètre de stratégie	SGE	ESDP	Explication
			<p>Lorsque l'empreinte digitale est correctement reconnue, le processus d'authentification au démarrage lit les informations d'identification de l'utilisateur et connecte l'utilisateur à l'authentification au démarrage. Le système transfère alors les informations d'identification vers Windows et connecte l'utilisateur à l'ordinateur</p> <p><b>Remarque:</b> Après avoir sélectionné cette procédure de connexion, l'utilisateur peut se connecter uniquement à l'aide d'une empreinte digitale préenregistrée ou d'un nom d'utilisateur et d'un mot de passe.</p>
<b>Afficher les échecs de connexion pour cet utilisateur</b>	✔	✔	<p>Affiche (paramètre : <b>OUI</b>) après la connexion à POA et Windows une boîte de dialogue indiquant des informations relatives au dernier échec de connexion (nom d'utilisateur/date/heure).</p>
<b>Afficher la dernière connexion utilisateur</b>	✔	✔	<p>Affiche (paramètre : <b>OUI</b>) après la connexion à partir de l'authentification au démarrage ou la connexion à Windows, une boîte de dialogue s'affiche contenant des informations concernant</p> <ul style="list-style-type: none"> <li>■ la dernière connexion (nom d'utilisateur/date/heure) ;</li> <li>■ les dernières informations d'identification de l'utilisateur connecté.</li> </ul>

Paramètre de stratégie	SGE	ESDP	Explication
<b>Désactiver la déconnexion forcée dans le verrouillage du poste de travail</b>			<p>Si un utilisateur souhaite quitter l'ordinateur final pendant une courte durée, il peut cliquer sur <b>Verrouiller le poste de travail</b> pour empêcher d'autres utilisateurs de l'utiliser et le déverrouiller avec le mot de passe utilisateur.</p> <p>Si cette option est définie sur NON, l'utilisateur qui a verrouillé l'ordinateur, ainsi qu'un administrateur, peuvent le déverrouiller. Si un administrateur déverrouille l'ordinateur, l'utilisateur connecté est automatiquement déconnecté. La définition de ce champ sur OUI change ce comportement. Dans ce cas, seul l'utilisateur peut déverrouiller l'ordinateur. L'administrateur ne pourra pas le déverrouiller et l'utilisateur ne sera pas déconnecté automatiquement.</p> <p>Remarque : ce paramètre ne prend effet que sous Windows XP.</p>
<b>Activer la présélection utilisateur/domaine</b>			<p><b>Oui</b> : POA enregistre les nom d'utilisateur et domaine du dernier utilisateur connecté. Il n'est donc pas nécessaire que les utilisateurs saisissent leur nom d'utilisateur chaque fois qu'ils se connectent.</p> <p><b>Non</b> : POA <u>n'enregistre pas</u> les nom d'utilisateur et domaine du dernier utilisateur connecté.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<b>Authentification automatique à Windows</b>			<p><b>Remarque:</b> Pour que l'utilisateur puisse autoriser d'autres utilisateurs à accéder à son ordinateur, il doit pouvoir désactiver la connexion automatique vers Windows.</p> <ul style="list-style-type: none"> <li>■ <b>Laisser l'utilisateur choisir</b> L'utilisateur peut choisir en activant/désactivant cette option dans la boîte de dialogue de connexion POA d'exécuter ou non la connexion automatique à Windows.</li> <li>■ <b>Appliquer l'authentification automatique à Windows</b> L'utilisateur se connecte toujours automatiquement à Windows.</li> <li>■ <b>Désactiver l'authentification automatique à Windows</b> Après la connexion POA, la boîte de dialogue de connexion Windows s'affiche. L'utilisateur doit se connecter manuellement à Windows.</li> </ul>
<b>Liste de comptes de service</b>			<p>Pour éviter que les opérations d'administration sur un ordinateur protégé par Sophos SafeGuard n'activent l'authentification au démarrage et n'entraînent l'ajout des opérateurs en charge du déploiement comme autant d'utilisateurs possibles de l'ordinateur, Sophos SafeGuard offre la possibilité de créer des listes de comptes de service pour les ordinateurs finaux Sophos SafeGuard. Les utilisateurs figurant dans ces listes sont ainsi traités comme des utilisateurs invités de Sophos SafeGuard.</p> <p>Avant de sélectionner une liste, vous devez créer les listes dans la zone de navigation <b>Stratégies</b> sous <b>Listes de comptes de service</b>.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<b>ÉCHECS DE CONNEXION</b>			
<b>Nbre maximum d'échecs de connexion</b>	✓	✓	Détermine le nombre de tentatives de connexion d'un utilisateur avec un nom d'utilisateur ou un mot de passe non valide. Par exemple, après trois tentatives successives de saisie d'un nom d'utilisateur ou d'un mot de passe incorrect, une quatrième tentative déclenche le paramètre « Réaction aux échecs de connexion ».
<b>Réaction aux échecs de connexion</b>			
<b>Verrouiller la machine</b>	✓	✓	Détermine si le PC est verrouillé après plusieurs échecs de connexion. Le verrouillage de l'ordinateur peut être levé par un administrateur qui doit réinitialiser le PC et se connecter. Tenez également compte du verrouillage utilisateur Windows dans ce contexte.
<b>OPTIONS DE VERROUILLAGE</b>			
<b>Verrouiller l'écran après X minutes d'inactivité</b>	✓	✓	Détermine le délai à l'issue duquel un bureau inutilisé est automatiquement verrouillé. La valeur par défaut est de 0 minute, auquel cas le bureau n'est pas verrouillé.
<b>Verrouiller l'écran après mise en veille</b>	✓	✓	Détermine si l'écran est verrouillé si l'ordinateur est réactivé du mode veille.

## 16.3 Création d'une liste de mots de passe interdits à utiliser dans les stratégies

Pour les stratégies de type **Mot de passe** une liste de mots de passe peut être créée afin de définir quelles sont les séquences de caractères qui ne doivent pas être utilisées dans les mots de passe :

**Remarque:** Dans les listes, les mots de passe non autorisés sont séparés par un saut de ligne.

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans SafeGuard Policy Editor. La taille maximale de ces fichiers texte est de **50 Ko**. Sophos SafeGuard n'utilise que des textes codés en Unicode UTF-16. Si vous ne créez pas les fichiers texte dans ce format, ils sont convertis automatiquement lors de l'enregistrement.

Si une conversion s'impose, un message s'affiche et indique que le fichier est en cours de conversion.

Pour enregistrer des fichiers texte, procédez comme suit :

1. Dans la zone de navigation de stratégie, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau > Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur [...] pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation de stratégie. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.


**Remarque:** Grâce au bouton **Modifier le texte**, vous pouvez ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.







## 16.4 Règles de syntaxe des mots de passe



Les mots de passe peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau mot de passe, n'utilisez pas de caractère avec la combinaison ALT + < caractère > car ce mode de saisie n'est pas disponible dans l'authentification au démarrage (POA). Les règles relatives aux mots de passe utilisés pour se connecter au système sont définies dans des stratégies du type **Mot de passe**.

**Remarque:** Si des règles de mot de passe ont été définies dans SafeGuard Policy Editor, aucune règle ne doit être définie dans Active Directory.

Paramètre de stratégie	SGE	ESDP	Explication
<b>RÈGLES</b>			
<b>Longueur min. du mot de passe</b>	✓	✓	Affiche le nombre de caractères que doit contenir un mot de passe lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
<b>Longueur max. du mot de passe</b>	✓	✓	Affiche le nombre maximum de caractères que doit contenir un mot de passe lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
<b>Nombre min. de lettres</b> <b>Nombre min. de chiffres</b> <b>Nombre min. de caractères spéciaux</b>	✓	✓	Ce paramètre ne s'applique qu'avec Utiliser la liste des mots de passe interdits et Utilisation interdite du nom d'utilisateur en tant que mot de passe.

Paramètre de stratégie	SGE	ESDP	Explication
<b>Respecter la casse</b>			<p>Ce paramètre ne s'applique qu'avec <b>Utiliser la liste des mots de passe interdits</b> et <b>Utilisation interdite du nom d'utilisateur en tant que mot de passe</b>.</p> <p><b>Cas 1 :</b> Vous avez saisi « tableau » dans la liste des mots de passe interdits. Si l'option <b>Respecter la casse</b> est définie sur <b>OUI</b>, les variantes supplémentaires du mot de passe telles que TABLEAU ou TABLEAU ne seront pas acceptées et la connexion sera refusée.</p> <p><b>Cas 2 :</b> « EMaier » est saisi comme nom d'utilisateur. Si l'option <b>Respecter la casse</b> est définie sur <b>OUI</b> et si <b>Utilisation interdite du nom d'utilisateur en tant que mot de passe</b> est définie sur <b>NON</b>, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple emaiier ou eMaiER) comme mot de passe.</p>
<b>Interdire la succession de touches horizontales</b>			<p>Les séquences de touches consécutives sont, par exemple « 123 » ou « aze ». Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.</p>
<b>Interdire la succession de touches verticales</b>			<p>Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple « wqal », « xsz2 » ou « 3edc » (mais pas « wse4 », « xdr5 » ou « cft6 »). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mot de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<b>Au moins 3 caractères consécutifs non autorisés</b>			<p>L'activation de cette option interdit les séquences de touches.</p> <ul style="list-style-type: none"> <li>■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant (« abc » ; « cba » ; « ; » , etc.).</li> <li>■ constituées de trois symboles identiques ou plus (« aaa » ou « 111 »).</li> </ul>
<b>Utilisation interdite du nom d'utilisateur en tant que mot de passe</b>			<p>Détermine si le nom d'utilisateur et le mot de passe peuvent être identiques.</p> <p><b>Oui</b> : l'utilisateur peut utiliser son nom d'utilisateur Windows comme mot de passe.</p> <p><b>Non</b> : le nom d'utilisateur Windows et le mot de passe doivent être différents.</p>
<b>Utiliser la liste de mots de passe interdits</b>			<p>Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les mots de passe. Les séquences de caractères sont stockées dans la liste des mots de passe interdits (par ex. un fichier .txt).</p>

Paramètre de stratégie	SGE	ESDP	Explication
<p><b>Liste de mots de passe interdits</b></p>	<p style="text-align: center;"></p>	<p style="text-align: center;"></p>	<p>Définit les séquences de caractères à ne pas utiliser pour les mots de passe. Si un utilisateur utilise un mot de passe non autorisé, un message d'erreur s'affiche.</p> <p><b>Conditions préalables importantes :</b></p> <p>Une liste (fichier) de mots de passe non autorisés doit être enregistrée dans SafeGuard Policy Editor, dans la zone de navigation de stratégie sous <b>Texte d'informations</b>. La liste n'est disponible qu'après l'enregistrement.</p> <p>Taille de fichier maximale : 50 Ko Format pris en charge : Unicode</p> <p><b>Définition de mots de passe interdits</b></p> <p>Dans la liste, les mots de passe non autorisés sont séparés par un saut de ligne. Le caractère générique : Le caractère générique « * » peut représenter tout caractère et tout nombre de caractères dans un mot de passe. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme mot de passe.</p> <p>Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe.</p> <p>Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier.</p> <p>L'option <b>Utiliser la liste des mots de passe interdits</b> doit être activée.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<b>MODIFICATIONS</b>			
<b>Modification du mot de passe autorisée après un min. de (jours)</b>	✔	✔	Détermine la période pendant laquelle un mot de passe ne peut être modifié. Ce paramètre empêche l'utilisateur de changer trop souvent de mot de passe au cours d'une période donnée. <b>Exemple :</b> L'utilisateur Miller définit un nouveau mot de passe (par ex. « 13jk56 »). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de changer le mot de passe par « 74jk56 ». Le changement de code PIN est refusé car Mme Miller ne peut définir un nouveau mot de passe qu'après un délai de cinq jours.
<b>Expiration du mot de passe après (jours)</b>	✔	✔	Si la période de validité maximum est activée, l'utilisateur doit définir un nouveau mot de passe une fois la période définie expirée.
<b>Avertir d'un changement obligatoire avant (jours)</b>	✔	✔	Un message d'avertissement s'affiche « n » jours avant l'expiration du mot de passe pour rappeler à l'utilisateur de changer son mot de passe dans « n » jours. L'utilisateur peut également le changer immédiatement.
<b>GÉNÉRAL</b>			
<b>Longueur de l'historique de mot de passe</b>	✔	✔	Détermine le moment où les mots de passe précédemment utilisés peuvent être réutilisés. Il convient de définir la longueur d'historique avec le paramètre Expiration du mot de passe après (jours).





Paramètre de stratégie	SGE	ESDP	Explication
			<p><b>Exemple :</b></p> <p>La longueur de l'historique de mot de passe pour l'utilisateur Miller est définie sur 4 et le nombre de jours après lequel l'utilisateur peut modifier son mot de passe est de 30. M. Miller se connecte actuellement à l'aide du code PIN « Informatik ». Lorsque la période de 30 jours expire, il est invité à modifier son mot de passe. M. Miller saisit « Informatik » comme nouveau mot de passe et reçoit un message d'erreur indiquant que ce mot de passe a déjà été utilisé et qu'il doit en sélectionner un nouveau. M. Miller ne peut pas utiliser le mot de passe « Informatik » avant la quatrième invitation de changement du mot de passe (en d'autres termes, longueur d'historique du mot de passe = 4).</p>


## 16.5 Règles de passphrase pour SafeGuard Data Exchange

**Remarque:** Ces paramètres ne sont pas pris en charge avec ESDP (Endpoint Security and Data Protection). Pour une description de SafeGuard Data Exchange, voir [SafeGuard Data Exchange](#), à la page 120.

L'utilisateur doit saisir une passphrase pour l'échange de données sécurisé via SafeGuard Data Exchange qui est utilisé pour générer des clés locales. La configuration minimale est définie dans les stratégies du type **Passphrase**. Pour plus d'informations sur SafeGuard Data Exchange et sur SafeGuard Portable, consultez l'aide de l'utilisateur de Sophos SafeGuard, chapitre *SafeGuard Data Exchange*.

Paramètre de stratégie	SGE	ESDP	Explication
<b>Longueur min. du passphrase</b>	✔		Définit le nombre minimum de caractères de la passphrase à partir de laquelle la clé est générée. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
<b>Longueur max. du passphrase</b>	✔		Définit le nombre maximum de caractères de la passphrase. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
<b>Nombre min. de lettres Nombre min. de chiffres Nombre min. de caractères spéciaux</b>	✔		Ce paramètre spécifie qu'une passphrase ne peut pas contenir seulement des lettres, des nombres ou des symboles mais doit comporter une combinaison de ces 2 au moins (par ex. 15 fleur etc.). Ce paramètre n'est pratique que si vous avez défini une longueur minimum de passphrase supérieure à 2.

Paramètre de stratégie	SGE	ESDP	Explication
<b>Respecter la casse</b>			<p>Ce paramètre est effectif lorsque l'option <b>Utilisation interdite du nom d'utilisateur en tant que passphrase</b> est active.</p> <p><b>Exemple :</b> « EMaier » est saisi comme nom d'utilisateur. Si l'option <b>Respecter la casse</b> est définie sur <b>OUI</b> et si <b>Utilisation interdite du nom d'utilisateur en tant que passphrase</b> est définie sur <b>NON</b>, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple emaiER ou eMaiER) comme passphrase.</p>
<b>Interdire la succession de touches horizontales</b>			<p>Les séquences de touches consécutives sont, par exemple « 123 » ou « aze ». Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.</p>
<b>Interdire la succession de touches verticales</b>			<p>Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple « wqa1 », « xsz2 » ou « 3edc » (mais pas « wse4 », « xdr5 » ou « cft6 »). Un maximum de deux caractères adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mots de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.</p>
<b>Au moins 3 caractères consécutifs non autorisés</b>			<p>L'activation de cette option interdit les séquences de touches</p> <ul style="list-style-type: none"> <li>■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant (« abc » ; « cba » ; « ; » , etc.).</li> <li>■ constituées de trois symboles identiques ou plus (« aaa » ou « 111 »).</li> </ul>

Paramètre de stratégie	SGE	ESDP	Explication
<b>Utilisation interdite du nom d'utilisateur en tant que passphrase</b>			Détermine si le nom d'utilisateur et la passphrase peuvent être identiques. <b>OUI</b> : l'utilisateur peut utiliser son nom d'utilisateur Windows comme passphrase. <b>NON</b> : le nom d'utilisateur Windows et la passphrase doivent être différents.

## 16.6 Protection du périphérique

La fonction principale de Sophos SafeGuard est le chiffrement des données sur des périphériques de stockage de données différents. Le chiffrement peut être basé sur volume ou sur fichier avec des clés et des algorithmes différents. Les stratégies du type Protection du périphérique incluent également des paramètres pour SafeGuard Data Exchange et SafeGuard Portable.

**Remarque:** Pour plus d'informations sur SafeGuard Data Exchange et sur SafeGuard Portable, consultez l'aide de l'utilisateur de Sophos SafeGuard, chapitre *SafeGuard Data Exchange*.

**Remarque:** SafeGuard Data Exchange, SafeGuard Portable et le chiffrement basé sur fichier ne sont pas pris en charge avec ESDP.

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



- stockage de masse (volumes d'initialisation/autres volumes) ;
- Supports amovibles (non pris en charge par les installations avec ESDP).
- Lecteurs optiques (non pris en charge par les installations avec ESDP).





Une stratégie distincte doit être créée pour chaque cible.

Paramètre de stratégie	SGE	ESDP	Description
<b>Mode de chiffrement du support</b>	✔	✔ Options disponibles pour ce paramètre : <ul style="list-style-type: none"> <li>■ <b>Aucun chiffrement</b></li> <li>■ <b>basé sur le volume</b></li> </ul> <b>Remarque:</b> Les paramètres basés sur le fichier ne sont pas disponibles avec ESDP.	Permet de protéger les périphériques (PC, ordinateurs portables) ainsi que tous types de supports amovibles. L'objectif essentiel consiste à chiffrer toutes les données stockées sur des périphériques de stockage locaux ou externes. Cette méthode transparente permet aux utilisateurs de continuer à utiliser leurs applications courantes, par exemple Microsoft Office. Le chiffrement transparent signifie que toutes les données chiffrées (dans des répertoires ou dans des volumes chiffrés) sont automatiquement déchiffrées dans la mémoire principale dès qu'elles sont ouvertes dans un programme. Un fichier est automatiquement chiffré de nouveau lorsqu'il est enregistré.

Paramètre de stratégie	SGE	ESDP	Description
			<p>Les options suivantes sont disponibles :</p> <ul style="list-style-type: none"> <li>■ <b>Aucun chiffrement</b></li> <li>■ <b>Basé sur volume (= chiffrement transparent basé sur secteur)</b></li> </ul> <p>Garantit que toutes les données sont chiffrées (y compris les fichiers d'initialisation, les fichiers d'échange, les fichiers inactifs/d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sans que l'utilisateur doive modifier ses habitudes de travail ou tenir compte de problèmes de sécurité.</p> <p><b>Remarque:</b> Si une stratégie de chiffrement existe pour un volume ou un type de volume et que le chiffrement du volume échoue, l'utilisateur n'est pas autorisé à y accéder.</p> <p><b>Partition système de Windows 7 :</b>                      Notez que, pour Windows 7 Professionnel, Entreprise et Édition Intégrale, une partition système est créée sur les ordinateurs de points de terminaison sans assignation de lettre de lecteur. Cette partition système ne peut pas être chiffrée par Sophos SafeGuard.</p> <p><b>Accès aux objets du système de fichiers non identifiés :</b>                      Les objets du système de fichiers non identifiés sont des volumes qui ne peuvent pas être clairement identifiés comme texte brut ou chiffrés par Sophos SafeGuard. L'accès au volume est refusé s'il existe une stratégie de chiffrement définie pour un objet du système de fichiers non identifiés. Si aucune stratégie de chiffrement n'existe, l'utilisateur peut accéder au volume.</p>

Paramètre de stratégie	SGE	ESDP	Description
			<p><b>Remarque:</b> Si une stratégie de chiffrement, dont le paramètre <b>Clé à utiliser pour le chiffrement</b> est défini de sorte à permettre la sélection de clé (par exemple, <b>Toute clé du jeu de clés utilisateur</b>), existe pour un volume d'objets du système de fichiers non identifiés, un intervalle de temps s'écoule entre l'affichage de la boîte de dialogue de sélection de la clé et le refus de l'accès. Pendant cet intervalle, le volume reste accessible. Le volume est accessible tant que la boîte de dialogue de sélection de clé n'est pas confirmée. Pour éviter ceci, indiquez une clé présélectionnée pour le chiffrement (voir la description du paramètre de stratégie <b>Clé à utiliser pour le chiffrement</b>). De plus, cet intervalle de temps existe également pour les volumes d'objets du système de fichiers non identifiés qui sont connectés à un ordinateur final, notamment lorsque l'utilisateur a déjà ouvert des fichiers sur le volume lorsque la stratégie de chiffrement prend effet ou si l'exécution automatique est activée. Dans ce cas, il n'est pas garanti que l'accès au volume sera refusé car cela risque de provoquer une perte de données.</p> <p><b>Volumes avec fonctionnalité d'exécution automatique activée :</b></p> <p>Si l'exécution automatique est activée sur un volume pour lequel une stratégie de chiffrement existe, les problèmes suivants peuvent se produire :</p> <ul style="list-style-type: none"> <li>■ Le volume n'est pas chiffré.</li> <li>■ Si le volume est un UFO (objet fichier non identifié), l'accès n'est pas refusé.</li> </ul>



Paramètre de stratégie	SGE	ESDP	Description
			<p><b>Basé sur fichier (= chiffrement transparent basé sur fichier (Chiffrement Smart Media))</b></p> <p>Garantit que toutes les données sont chiffrées (à l'exception du support d'initialisation et des informations de répertoire) avec l'avantage que même les supports optiques tels que les CD/DVD peuvent être chiffrés et que les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard n'est pas installé (si les stratégies l'autorisent).</p> <p><b>Remarque:</b> Les données chiffrées en utilisant le chiffrement basé sur fichier ne peuvent pas être compressées. De même, les données compressées ne peuvent pas être chiffrées en utilisant le chiffrement basé sur fichier. Les volumes d'initialisation ne sont jamais chiffrés selon la méthode basée sur fichier. Ils sont automatiquement exclus du chiffrement basé sur fichier, même si une règle correspondante est définie.</p>
<b>PARAMÈTRES GÉNÉRAUX</b>			
<b>Algorithmes à utiliser pour le chiffrement</b>			<p>Définit l'algorithme de chiffrement.</p> <p>Liste des algorithmes utilisables avec les normes respectives :</p> <p>AES256 : 32 octets (256 bits)</p> <p>AES128 : 16 octets (128 bits)</p>

Paramètre de stratégie	SGE	ESDP	Description
<b>Clé à utiliser pour le chiffrement</b>			Définit la clé utilisée pour le chiffrement. Pour le chiffrement par Sophos SafeGuard, seule une clé machine générée automatiquement est utilisée pour le chiffrement basé sur volume. Pour le chiffrement basé sur fichier, seules les clés locales créées par l'utilisateur peuvent être utilisées. L'option suivante est disponible : <b>Clé machine définie :</b> la clé de la machine est utilisée ; l'utilisateur ne peut PAS sélectionner de clé.
<b>L'utilisateur est autorisé à créer une clé locale</b>			Ce paramètre détermine si l'utilisateur peut générer ou non une clé locale sur son ordinateur. Les clés locales sont générées sur l'ordinateur final selon une passphrase saisie par l'utilisateur. La configuration minimale de la passphrase est définie dans des stratégies du type <b>Passphrase</b> . <b>Remarque:</b> Dans la mesure où seules les clés locales étant utilisées pour le chiffrement basé sur fichier, l'utilisateur doit pouvoir créer des clés locales si des stratégies de chiffrement basé sur fichier s'appliquent. Le paramètre par défaut de ce champ (non configuré) permet à l'utilisateur de créer des clés locales.
<b>PARAMÈTRES BASÉS SUR VOLUME</b>			
<b>L'utilisateur peut ajouter des clés au volume chiffré ou en supprimer</b>			<b>OUI :</b> les utilisateurs de Sophos SafeGuard peuvent ajouter des clés à un jeu de clés ou en supprimer. La boîte de dialogue s'affiche via la commande du menu contextuel <b>Chiffrement / onglet Chiffrement</b> . <b>NON :</b> les utilisateurs de Sophos SafeGuard ne peuvent pas ajouter de clés.





Paramètre de stratégie	SGE	ESDP	Description
<b>Réaction aux volumes non chiffrés</b>	✔	✔	Définit comment Sophos SafeGuard gère les supports non chiffrés. Les options suivantes sont disponibles : <ul style="list-style-type: none"> <li>■ <b>Rejeter</b> (= le support en texte n'est pas chiffré)</li> <li>■ <b>N'accepter que les supports vierges et chiffrer</b></li> <li>■ <b>Accepter tous les supports et chiffrer</b></li> </ul>
<b>L'utilisateur peut déchiffrer un volume</b>	✔	✔	Permet à l'utilisateur de Sophos SafeGuard de déchiffrer le volume par l'intermédiaire d'une commande du menu contextuel dans l'Explorateur Windows.
<b>Chiffrement initial rapide</b>	✔	✔	Sélectionnez ce paramètre pour activer le mode de chiffrement initial rapide pour le chiffrement basé sur fichier. Ce mode permet de réduire la durée nécessaire au chiffrement initial sur des ordinateurs de points de terminaison. <b>Remarque:</b> ce mode peut se traduire par une sécurité inférieure. Pour plus d'informations, voir <a href="#">Chiffrement initial rapide</a> , à la page 9.
<b>Poursuivre sur les secteurs incorrects</b>	✔	✔	Indique si le chiffrement doit se poursuivre ou être arrêté si des secteurs incorrects sont détectés. Le paramètre par défaut est <b>OUI</b> .
<b>PARAMÈTRES BASÉS SUR FICHER</b>			
<b>Chiffrement initial de tous les fichiers</b>	✔		Démarre automatiquement le chiffrement initial d'un volume après la connexion de l'utilisateur. Il se peut que l'utilisateur doive sélectionner une clé du jeu de clés au préalable.
<b>L'utilisateur peut annuler le chiffrement initial</b>	✔		Permet à l'utilisateur d'annuler le chiffrement initial.



Paramètre de stratégie	SGE	ESDP	Description
L'utilisateur n'est pas autorisé à accéder aux fichiers non chiffrés	✔		Définit si un utilisateur peut accéder aux données non chiffrées d'un volume.
L'utilisateur peut déchiffrer des fichiers	✔		Permet à un utilisateur de déchiffrer des fichiers individuels ou des répertoires entiers (en utilisant l'extension de l'Explorateur Windows <clic droit>).
L'utilisateur peut définir une passphrase de support pour les périphériques	✔		Permet à l'utilisateur de définir une passphrase de support sur son ordinateur. La passphrase de support permet d'accéder facilement via SafeGuard Portable à toutes les clés locales utilisées sur des ordinateurs sur lesquels SafeGuard Data Exchange n'est pas installé.
Applications non gérées	✔		<p>Permet de définir d'autres applications devant être ignorées par le pilote du filtre Sophos SafeGuard et devant être exclues du chiffrement/déchiffrement transparent. Le séparateur à utiliser pour ces applications est « ; ».</p> <p>Un exemple d'application non gérée est un programme de sauvegarde. Pour garantir que ces données ne sont pas déchiffrées lors de la création d'une sauvegarde, cette application peut être exclue du processus de chiffrement/déchiffrement. Les données sont sauvegardées sous forme chiffrée.</p> <p><b>Remarque:</b> Comme il s'agit de paramètres spécifiques à la machine, ils ne sont appliqués que lorsque l'ordinateur final est réinitialisé.</p>

Paramètre de stratégie	SGE	ESDP	Description
			<p><b>Définition des applications non gérées</b></p> <p>Utilisation générale :</p> <p>Les programmes de sauvegarde peuvent être définis comme exemptés afin qu'ils puissent toujours lire et enregistrer les données chiffrées.</p> <p>Les applications susceptibles de déclencher des dysfonctionnements lorsqu'elles sont utilisées avec Sophos SafeGuard mais qui ne nécessitent pas de chiffrement peuvent généralement être exemptées de chiffrement.</p> <p>Le nom complet du fichier exécutable (contenant éventuellement les informations du chemin d'accès) est utilisé pour spécifier une application exemptée.</p> <p><b>Remarque:</b> Des applications non gérées ne peuvent être définies que pour des périphériques de stockage locaux. Pour une stratégie globale du type <b>Protection du périphérique</b>, la cible <b>Périphériques de stockage locaux</b> doit être sélectionnée. Pour toutes les autres cibles, l'option Applications non gérées n'est pas disponible.</p>

Paramètre de stratégie	SGE	ESDP	Description
<b>Supports amovibles uniquement</b> <b>Copier portable SG vers support amovible</b>			<p>Si cette option est activée, SafeGuard Portable est copié sur tous les supports amovibles connectés à l'ordinateur final.</p> <p>SafeGuard Portable permet l'échange de données chiffrées avec le support amovible sans que Sophos SafeGuard soit installé au niveau du destinataire. Le destinataire peut déchiffrer et rechiffrer les fichiers chiffrés en utilisant SafeGuard Portable et le mot de passe correspondant. Le destinataire peut rechiffrer les fichiers avec SafeGuard Portable ou utiliser la clé d'origine pour le chiffrement.</p> <p>Il n'est pas nécessaire que SafeGuard Portable soit installé ou copié sur l'ordinateur du destinataire, il peut être utilisé directement à partir du support amovible.</p>
<b>Dossier en texte brut</b>			<p>Le dossier spécifié ici sera créé sur chaque support amovible. Les fichiers copiés dans ce dossier restent au format brut.</p>

## 16.7 Paramètres spécifiques de la machine - Paramètres de base







Paramètre de stratégie	SGE	ESDP	Explication
<b>AUTHENTIFICATION AU DÉMARRAGE (POA)</b>			
<b>Activer l'authentification au démarrage</b>			Définit si POA est activé ou désactivé en permanence. <b>Remarque:</b> Pour des raisons de sécurité, il est fortement recommandé que l'authentification au démarrage reste activée. La désactivation de l'authentification au démarrage réduit la sécurité du système lors des connexions Windows et accroît le risque d'accès non autorisés aux données chiffrées.
<b>Interdire l'utilisateur invité</b>			Définit si un utilisateur est autorisé à se connecter à Windows.
<b>Éveil par appel réseau sécurisé (WOL)</b>			La stratégie « Éveil par appel réseau sécurisé » permet à l'ordinateur final de se préparer aux déploiements de logiciels dans lesquels les paramètres nécessaires tels que la désactivation temporaire de POA et un intervalle d'éveil par appel réseau peuvent être importés directement dans l'ordinateur final et analysés par celui-ci. L'équipe de déploiement peut concevoir un script de programmation en utilisant les commandes fournies pour garantir la protection maximale par Sophos SafeGuard bien que l'authentification au démarrage soit désactivée. N'oubliez pas que la désactivation du POA (même pour un nombre limité de processus d'initialisation) réduit le niveau de sécurité de votre système.









Paramètre de stratégie	SGE	ESDP	Explication
			<p><b>EXEMPLE :</b> L'équipe de déploiement des logiciels notifie le responsable de la sécurité de Sophos SafeGuard d'un déploiement de logiciel prévu le 25 septembre 2009 entre 03:00 et 06:00 le matin. 2 réinitialisations sont requises. L'agent local en charge du déploiement des logiciels doit être en mesure de se connecter à Windows. Le responsable de la sécurité crée la stratégie suivante et l'attribue aux ordinateurs finaux correspondants :</p> <p><b>Nombre de connexions automatiques (0 = pas de WOL) : 5</b></p> <p><b>Connexion Windows autorisée pendant l'éveil par appel réseau : Oui</b></p> <p><b>Début de la plage horaire pour le lancement du WOL externe : 24 sept. 2009, 12:00</b></p> <p><b>Fin de la plage horaire pour le lancement du WOL externe : 25 sept. 2009, 06:00</b></p> <p>Le responsable de la sécurité fournit un tampon de 3 pour les connexions automatiques.</p> <p>Il définit l'intervalle à 12 heures le jour précédant le déploiement pour permettre au script de programmation SGMCMDDIntn.exe de démarrer rapidement et que l'éveil par appel réseau ne démarre pas après le 25 septembre à 3 heures du matin.</p> <p>L'équipe de déploiement des logiciels produit deux commandes pour le script de programmation :</p> <ul style="list-style-type: none"> <li>■ démarrage 24 sept.2009, 12:15, SGMCMDDIntn.exe /WOLstart</li> <li>■ démarrage 26 sept.2009, 09:00 SGMCMDDIntn.exe /WOLstop</li> </ul>



Paramètre de stratégie	SGE	ESDP	Explication
			<p>Le script de déploiement est daté du 25.09.2009, 03:00. L'éveil par appel réseau peut être à nouveau explicitement désactivé à la fin du script en utilisant SGMCMDDIntn.exe / WOLstop.</p> <p>Tous les ordinateurs finaux qui se connectent avant le 24 septembre 2009 et qui se connectent aux serveurs de déploiement recevront la nouvelle stratégie et les commandes de programmation.</p> <p>Tout ordinateur final sur lequel la programmation déclenche la commande SGMCMDDIntn/WOLstart entre le 24 sept. 2009 à midi et le 25 sept. 2009, à 6 heures du matin se trouve dans l'intervalle de l'éveil par appel réseau et ce dernier sera par conséquent activé.</p>
<p><b>Nombre de connexions automatiques</b></p>	<p style="text-align: center;"></p>	<p style="text-align: center;"></p>	<p>Définit le nombre de réinitialisations lorsque l'authentification au démarrage est inactive pour l'éveil par appel réseau.</p> <p>Ce paramètre remplace temporairement le paramètre <b>Activer l'authentification au démarrage</b> jusqu'à ce que le nombre prédéfini de connexions automatiques soit atteint. L'authentification au démarrage est ensuite réactivée. Exemple : le nombre de connexions automatiques est défini sur 2, « Activer l'authentification au démarrage » est activé. Le PC s'initialise deux fois sans authentification au démarrage via POA.</p> <p>Pour le mode Éveil par appel réseau, nous recommandons de toujours autoriser <b>trois réinitialisations de plus que nécessaire</b> pour faire face aux problèmes imprévus.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<b>Connexion à Windows autorisée pendant le WOL</b>	✔	✔	Détermine si la connexion Windows est autorisée pendant l'éveil par appel réseau, par ex. pour une mise à jour de logiciel. Ce paramètre est analysé par POA.
<b>Début de la plage horaire pour le lancement du WOL externe</b> <b>Fin de la plage horaire pour le lancement du WOL externe</b>	✔	✔	<p>La date et l'heure peuvent être sélectionnées ou saisies pour le début et la fin de l'éveil par appel réseau (WOL). Format de date : <i>MM/JJ/AAAA</i> Format d'heure : <i>HH:MM</i></p> <p>Les combinaisons suivantes de saisie sont possibles :</p> <ul style="list-style-type: none"> <li>■ début et fin de l'éveil par appel réseau définis ;</li> <li>■ fin de l'éveil par appel réseau définie, début ouvert ;</li> <li>■ pas de saisie : aucun intervalle n'a été défini pour l'ordinateur final.</li> </ul> <p>En cas de déploiement planifié de logiciels, le responsable de la sécurité doit définir la plage de l'éveil par appel réseau de sorte que le script de programmation puisse démarrer suffisamment tôt pour que les ordinateurs finaux aient le temps de s'initialiser.</p> <p>WOLstart (Début WOL) : Le point de départ de l'éveil par appel réseau dans le script de programmation doit se trouver dans l'intervalle défini dans la stratégie. Si aucun intervalle n'est défini, l'éveil par appel réseau n'est pas activé localement sur l'ordinateur final Sophos SafeGuard.</p> <p>WOLstop (Fin WOL) : Cette commande s'effectue quel que soit le point final défini pour l'éveil par appel réseau.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<b>OPTIONS D'AFFICHAGE</b>			
<b>Afficher l'identification de la machine</b>	✔	✔	Affiche le nom de l'ordinateur ou un texte défini dans la barre de titre du POA.  Si les paramètres réseau de Windows incluent le nom de la machine, ce dernier est automatiquement intégré aux paramètres de base.
<b>Texte d'identification de la machine</b>	✔	✔	Le texte à afficher dans la barre de titre du POA.  Si vous avez sélectionné <b>Nom défini</b> dans le champ <b>Afficher l'identification de la machine</b> , vous pouvez entrer le texte dans ce champ de saisie.
<b>Afficher la mention légale</b>	✔	✔	Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît avant l'authentification dans POA. Dans certains pays, la loi exige l'affichage d'une zone de texte ayant un certain contenu.  L'utilisateur doit confirmer la zone de texte avant que le système ne continue.  Avant de spécifier un texte, ce dernier doit être enregistré en tant qu'élément de texte dans la <b>zone de navigation de stratégie</b> sous <b>Texte d'informations</b> .
<b>Texte de la mention légale</b>	✔	✔	Le texte à afficher en tant que mention légale.  Dans ce champ, vous pouvez sélectionner un élément de texte enregistré dans <b>Texte d'informations</b> dans la <b>zone de navigation de stratégie</b> .

Paramètre de stratégie	SGE	ESDP	Explication
<b>Afficher des infos supplémentaires</b>			<p>Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît après la mention légale (si elle est activée).</p> <p>Vous pouvez définir si les informations supplémentaires doivent être affichées:</p> <ul style="list-style-type: none"> <li>■ <b>Jamais</b></li> <li>■ <b>À chaque démarrage système</b></li> <li>■ <b>À chaque connexion</b></li> </ul>
<b>Texte des informations supplémentaires</b>			<p>Le texte à afficher en tant qu'informations supplémentaires.</p> <p>Dans ce champ, vous pouvez sélectionner un élément de texte enregistré dans <b>Texte d'informations</b> dans la <b>zone de navigation de stratégie</b>.</p>
<b>Afficher pendant (s)</b>			<p>Dans ce champ, vous pouvez définir la durée (en secondes) pendant laquelle les informations supplémentaires doivent être affichées.</p> <p>Vous pouvez spécifier le nombre de secondes après lesquelles la zone de texte d'informations supplémentaires est fermée automatiquement.</p> <p>L'utilisateur peut fermer la zone de texte à tout moment en cliquant sur <b>OK</b>.</p>

Paramètre de stratégie	SGE	ESDP	Explication
<b>Activer et afficher l'icône de la barre d'état système</b>			<p>Grâce à l'icône de la barre d'état système de Sophos SafeGuard, l'utilisateur peut accéder rapidement et facilement à l'ensemble des fonctions de son ordinateur. En outre, des informations concernant le statut de Sophos SafeGuard (nouvelles stratégies reçues, ...) peuvent être affichées dans des infobulles.</p> <p><b>Oui :</b> l'icône de barre d'état système est affichée dans la zone d'information de barre des tâches et l'utilisateur est continuellement informé du statut de Sophos SafeGuard via l'infobulle.</p> <p><b>Non :</b> <b>Muet :</b> l'icône de barre d'état système est affichée dans la zone d'information de barre des tâches mais aucune information d'état n'est affichée via l'infobulle.</p>
<b>Afficher les icônes en chevauchement dans l'Explorateur</b>			Définit si des symboles de clé Windows s'affichent pour indiquer l'état de chiffrement des volumes, périphériques, dossiers et fichiers.
<b>Clavier virtuel en POA</b>			Définit si un clavier virtuel peut être affiché sur demande dans la boîte de dialogue de POA pour la saisie du mot de passe.
<b>OPTIONS D'INSTALLATION</b>			
<b>Désinstallation autorisée</b>			Détermine si la désinstallation de Sophos SafeGuard est autorisée sur les ordinateurs finaux. Lorsque l'option <b>Désinstallation autorisée</b> est définie sur <b>Non</b> , Sophos SafeGuard ne peut pas être désinstallé, même par quelqu'un ayant des droits d'administrateur, lorsque ce paramètre est actif au sein d'une stratégie.

Paramètre de stratégie	SGE	ESDP	Explication
<p><b>Activer la protection anti-sabotage Sophos</b></p>			<p>Cette option permet d'activer et de désactiver la protection anti-sabotage Sophos pour les installations avec ESDP. Si vous avez autorisé la désinstallation de Sophos SafeGuard via le paramètre de stratégie <b>Désinstallation autorisée</b>, vous pouvez définir ce paramètre de stratégie sur <b>Oui</b>, pour garantir que les tentatives de désinstallation sont vérifiées par la protection anti-sabotage Sophos et éviter la suppression accidentelle du logiciel.</p> <p>Si la protection anti-sabotage Sophos n'autorise pas la désinstallation, les tentatives de désinstallation seront annulées.</p> <p>Si vous définissez l'option <b>Activer la protection anti-sabotage Sophos</b> sur <b>Non</b>, la protection anti-sabotage Sophos ne pourra ni vérifier ni empêcher la désinstallation de Sophos SafeGuard.</p> <p><b>Remarque:</b> Ce paramètre ne s'applique qu'aux ordinateurs finaux utilisant Sophos Endpoint Security and Control version 9.5 ou ultérieure.</p>

## 16.8 Consignation

Les événements Sophos SafeGuard sont consignés dans la visionneuse des événements Windows. Pour indiquer les événements à consigner dans la visionneuse des événements Windows, créez une stratégie du type **Consignation**, puis sélectionnez les événements souhaités d'un simple clic.

Vous pouvez sélectionner plusieurs types d'événements, de catégories différentes (par exemple Authentification, Chiffrement, etc.). Il est recommandé de définir une stratégie pour la consignation et de déterminer quels sont les événements nécessaires, en fonction de vos exigences en matière de rapports et d'audits.

## 17 SafeGuard Data Exchange

**Remarque:** SafeGuard Data Exchange et SafeGuard Portable ne sont pas pris en charge avec ESDP (Endpoint Security and Data Protection).

SafeGuard Data Exchange est utilisé pour chiffrer des données stockées sur des supports amovibles connectés à un ordinateur final Sophos SafeGuard afin d'échanger ces données avec d'autres utilisateurs. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale.

Seuls les utilisateurs disposant des clés appropriées peuvent lire le contenu des données chiffrées. Tout processus de chiffrement ultérieur est exécuté de manière transparente.

En tant que responsable de la sécurité, vous définissez les paramètres spécifiques dans une stratégie du type **Protection du périphérique** avec **Cible de protection de périphérique : Supports amovibles**.

### 17.1 Clés locales

SafeGuard Data Exchange prend en charge le chiffrement à l'aide de clés locales. Des clés locales sont créées sur les ordinateurs finaux et peuvent être utilisées pour chiffrer des données de supports amovibles. Pour les créer, il faut saisir une passphrase.

**Remarque:** SafeGuard Data Exchange n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

Si des clés locales sont utilisées pour chiffrer des fichiers sur des supports amovibles, ces fichiers peuvent être déchiffrés à l'aide de SafeGuard Portable sur un ordinateur sur lequel SafeGuard Data Exchange n'est pas installé. À l'ouverture des fichiers avec SafeGuard Portable, l'utilisateur est invité à saisir la passphrase spécifiée lors de la création de la clé. L'utilisateur peut ouvrir le fichier s'il connaît la passphrase.

Grâce à SafeGuard Portable, chaque utilisateur connaissant la passphrase peut accéder à un fichier chiffré sur un support amovible. Ainsi, il est également possible de partager des données chiffrées avec des partenaires qui ne possèdent pas Sophos SafeGuard. SafeGuard Portable et la passphrase des fichiers auxquels ils doivent accéder doivent leur être fournis.

Si différentes clés locales sont utilisées pour chiffrer des fichiers de supports amovibles, vous pouvez également restreindre l'accès aux fichiers. Par exemple : Vous chiffrez les fichiers contenus sur une carte mémoire USB à l'aide d'une clé avec la passphrase `my_localkey` et vous chiffrez un fichier nommé `ForMyPartner.doc` à l'aide de la passphrase `partner_localkey`. Si vous donnez la carte mémoire USB à un partenaire et que vous lui fournissez la passphrase `partner_localkey`, il n'aura accès qu'au fichier `ForMyPartner.doc`.

**Remarque:** Par défaut, SafeGuard Portable est copié automatiquement sur tous les supports amovibles connectés au système. Si vous ne souhaitez pas que SafeGuard Portable soit copié automatiquement sur les supports amovibles, désactivez l'option Copier portable SG vers support amovible dans une stratégie du type Chiffrement de périphérique.

## 17.2 Passphrase du support

SafeGuard Data Exchange permet également de spécifier qu'une seule passphrase de support pour tous les supports amovibles (sauf les supports optiques) doit être créée sur l'ordinateur final. La passphrase du support permet d'accéder à toutes les clés locales utilisées dans SafeGuard Portable. L'utilisateur ne saisit qu'une seule passphrase et peut accéder à tous les fichiers chiffrés dans SafeGuard Portable, quelle que soit la clé locale utilisée pour le chiffrement.

Sur chaque ordinateur et pour chaque périphérique, une clé de chiffrement de support unique pour le chiffrement de données est créée automatiquement. La clé est protégée par la passphrase du support. Sur un ordinateur sur lequel SafeGuard Data Exchange est installé, il n'est donc pas nécessaire de saisir la passphrase de support pour accéder aux fichiers chiffrés contenus sur le support amovible. L'accès est accordé automatiquement si la clé appropriée se trouve dans le jeu de clés de l'utilisateur.

La fonction de passphrase de support est disponible lorsque l'option **L'utilisateur peut définir une passphrase de support pour les périphériques** est activée dans une stratégie du type **Protection du périphérique**.

Lorsque ce paramètre est activé sur l'ordinateur, l'utilisateur est invité automatiquement à saisir une passphrase de support lors de la première connexion au support amovible. L'utilisateur peut également changer la passphrase de support. La synchronisation est alors automatique lorsque la passphrase reconnue sur l'ordinateur et la passphrase de support amovible ne correspondent pas.

En cas d'oubli de la passphrase de support, l'utilisateur peut la récupérer sans recourir au support.

**Remarque:** Pour activer la passphrase de support, activez l'option **L'utilisateur peut définir une passphrase de support pour les périphériques** dans une stratégie du type Chiffrement de périphérique.

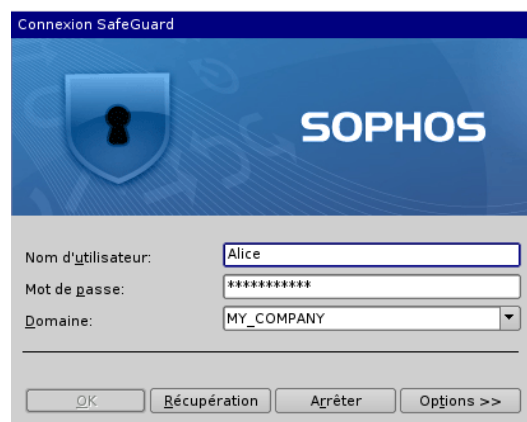
Sur un ordinateur protégé par Sophos SafeGuard et sur lequel la fonction de passphrase de support est désactivée, aucune clé n'est disponible une fois l'installation terminée, car les clients autonomes utilisent des clés locales uniquement. Avant de pouvoir utiliser le chiffrement, l'utilisateur doit créer une clé.

Si la fonction de passphrase de support est activée dans une stratégie de support amovible pour des ordinateurs protégés par Sophos SafeGuard, la clé de chiffrement de support est créée automatiquement sur l'ordinateur client et peut être utilisée pour un chiffrement immédiatement après l'installation. Il s'agit d'une clé prédéfinie du jeu de clés de l'utilisateur et elle s'affiche sous la forme <nom utilisateur> dans les boîtes de dialogue de sélection de clés.

Le cas échéant, les clés de chiffrement de support sont également utilisées pour toutes les tâches de chiffrement initial.

## 18 Authentification au démarrage (POA)

Sophos SafeGuard identifie l'utilisateur avant même le démarrage du système d'exploitation. Pour cela, le noyau du système de Sophos SafeGuard démarre en amont. Il est protégé contre toute modification puis il est enregistré et masqué sur le disque dur. Ce n'est que lorsque l'utilisateur s'est correctement authentifié à partir de l'authentification au démarrage que le système d'exploitation (Windows) réel démarre à partir de la partition chiffrée. L'utilisateur est ensuite automatiquement connecté à Windows. La procédure est identique lorsque l'ordinateur final revient du mode hibernation.



Les avantages de l'authentification au démarrage de Sophos SafeGuard sont les suivants :

- une interface utilisateur graphique, avec prise en charge de la souris et des fenêtres pouvant être déplacées, pour plus de facilité et de lisibilité ;
- une présentation graphique qui, en suivant les instructions, peut être personnalisée pour les ordinateurs d'entreprise (image d'arrière-plan, image de connexion, message d'accueil, etc.) ;
- la prise en charge des comptes utilisateur Windows et des mots de passe dès l'étape de préinitialisation, ce qui évite à l'utilisateur de devoir mémoriser des informations d'identification distinctes ;
- la prise en charge de format Unicode et par conséquent des mots de passe et des interfaces utilisateur en langue étrangère.

## 18.1 Retard de connexion

Sur un ordinateur protégé par Sophos SafeGuard, un retard de connexion s'applique si un utilisateur fournit des informations d'identification incorrectes pendant l'authentification Windows ou l'authentification au démarrage. Le retard de connexion augmente à chaque échec de tentative de connexion. Après un échec de connexion, une boîte de dialogue apparaît et affiche le délai restant.

**Remarque:** Si un utilisateur saisit un code PIN incorrect lors de la connexion sur la carte à puce, il n'y aura aucun retard de connexion.

Vous pouvez indiquer le nombre de tentatives de connexion autorisées dans une stratégie du type **Authentification** en vous aidant pour cela de l'option **Nbre maximum d'échecs de connexion**.

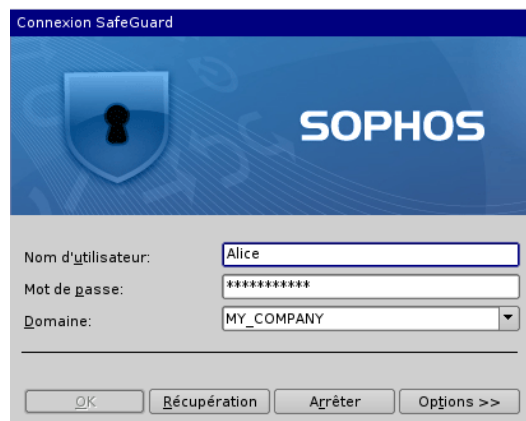
## 18.2 Verrouillage de la machine

Dans une stratégie du type **Authentification**, vous pouvez également spécifier le verrouillage de l'ordinateur après un certain nombre d'échecs de tentatives de connexion en définissant l'option **Verrouiller la machine** sur **Oui**. Pour déverrouiller leur ordinateur, les utilisateurs doivent lancer une procédure Challenge/Réponse.

## 18.3 Configuration de l'authentification au démarrage

La boîte de dialogue POA comporte les composants suivants :

- Image de connexion
- Texte des boîtes de dialogue
- Langue de la disposition du clavier



Vous pouvez modifier l'apparence de la boîte de dialogue de l'authentification au démarrage selon vos préférences, grâce notamment aux paramètres de stratégie de SafeGuard Policy Editor.

### **18.3.1 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. Toutefois, il est possible d'afficher des images différentes telles que le logo de l'entreprise.

Les images d'arrière-plan et de connexion sont définies via une stratégie du type **Paramètres généraux**.

Utilisées dans Sophos SafeGuard, les images d'arrière-plan et de connexion doivent respecter certaines conditions :

#### **Image d'arrière-plan**

Taille de fichier maximale pour toutes les images d'arrière-plan : **500 Ko**

Sophos SafeGuard prend en charge deux variantes d'images d'arrière-plan :

- **1024 x 768** (mode VESA)

Couleurs : aucune restriction

Option dans le type de stratégie **Paramètres généraux : Image d'arrière-plan dans POA**

- **640 x 480** (mode VGA)

Couleurs : 16

Option dans le type de stratégie **Paramètres généraux : Image d'arrière-plan dans POA (basse résolution)**

#### **Image de connexion**

Taille de fichier maximale pour toutes les images de connexion : **100 Ko**

Sophos SafeGuard prend en charge deux variantes d'images de connexion :

- **413 x 140**

Couleurs : aucune restriction

Option dans le type de stratégie **Paramètres généraux : Image de connexion dans POA**

■ **413 x 140**

Couleurs : 16

Option dans le type de stratégie **Paramètres généraux : Image de connexion dans POA (basse résolution)**

Les images, les textes d'informations et les listes doivent être créés en premier sous la forme de fichiers (fichiers BMP, PNG, JPG ou texte), puis enregistrés dans la fenêtre de navigation.

### **18.3.1.1 Enregistrement d'images**

Pour enregistrer des images, procédez comme suit :

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Images** et sélectionnez **Nouveau > Image**.
2. Entrez le nom de l'image dans le champ **Nom de l'image**.
3. Cliquez sur [...] pour sélectionner l'image préalablement créée.
4. Cliquez sur **OK**.

La nouvelle image apparaît en tant que nœud secondaire de **Images** dans la zone de navigation de stratégie. Si vous sélectionnez l'image, elle s'affiche dans la zone d'action. L'image peut désormais être sélectionnée lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres images. Toutes les images enregistrées s'affichent en tant que nœuds secondaires.

**Remarque:** Grâce au bouton **Modifier l'image**, vous pouvez changer l'image attribuée. Une boîte de dialogue de sélection d'une autre image s'affiche lorsque vous cliquez sur ce bouton.

## 18.3.2 Texte des informations défini par l'utilisateur dans l'authentification au démarrage (POA)

Vous pouvez personnaliser l'authentification au démarrage (POA) en affichant les **textes d'informations définis par l'utilisateur** :

- Texte d'informations affiché lors du lancement d'une procédure de Challenge/Réponse pour la récupération de connexion (p. ex. : « Contactez le bureau de support en appelant au 01234-56789. »)

Option dans le type de stratégie **Paramètres généraux : Texte d'informations**

- Mentions légales affichées après la connexion à POA

Option dans le type de stratégie **Paramètres de machine spécifiques : Texte de la mention légale**

- Texte d'informations supplémentaires affiché après la connexion à POA

Option dans le type de stratégie **Paramètres de machine spécifiques : Texte des informations supplémentaires**

### 18.3.2.1 Enregistrement de textes d'informations

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans SafeGuard Policy Editor. La taille maximale de ces fichiers pour les textes d'informations est de **50 Ko**. Sophos SafeGuard n'utilise que des textes codés en Unicode UTF-16. Si vous ne créez pas les fichiers texte dans ce format, ils sont convertis automatiquement lors de l'enregistrement.

Si une conversion s'impose, un message s'affiche et indique que le fichier est en cours de conversion.

Pour enregistrer des textes d'informations :

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau > Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur [...] pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation de stratégie. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

**Remarque:** Grâce au bouton **Modifier le texte**, vous pouvez ajouter du texte au texte existant. Une boîte de dialogue de sélection d'un autre fichier texte s'affiche lorsque vous cliquez sur ce bouton. Le texte contenu dans ce fichier est ajouté à la fin du texte existant.

### **18.3.3 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.

Après l'installation, la langue dans laquelle le texte de la boîte de dialogue d'authentification au démarrage s'affiche ne peut être modifiée que via une stratégie définie dans SafeGuard Policy Editor. Le changement de la langue par défaut sous Windows n'affecte pas celle du texte de la boîte de dialogue d'authentification au démarrage.

La langue du texte de la boîte de dialogue d'authentification au démarrage est définie via une stratégie du type **Paramètres généraux** (option **Langue utilisée sur le client**).

### **18.3.4 Disposition du clavier**

Chaque pays ou presque a une disposition de clavier qui lui est propre, c'est-à-dire une répartition différente des touches. La disposition du clavier dans POA est importante lorsque vous saisissez des noms d'utilisateur, des mots de passe et des codes de réponse.

Par défaut, pour l'authentification au démarrage, Sophos SafeGuard adopte la disposition du clavier qui a été définie dans les Options régionales et linguistiques de Windows pour l'utilisateur Windows par défaut, au moment de l'installation de Sophos SafeGuard. Si « Allemand » est la disposition de clavier définie sous Windows, la disposition allemande du clavier sera utilisée dans POA.

La langue de la disposition du clavier utilisée est affichée dans POA, par exemple « FR » pour le français. Outre la disposition du clavier par défaut, la disposition du clavier américain (anglais) peut également être utilisée.

Il existe un certain nombre d'exceptions :

- La disposition du clavier est effectivement prise en charge, mais la police requise est manquante (Bulgare, par exemple). Par conséquent, seuls les caractères spéciaux sont affichés dans le champ **Nom d'utilisateur**.
- Aucune disposition du clavier n'est disponible (par exemple pour la République Dominicaine). Dans ces situations, POA revient à la disposition de clavier d'origine. Pour la République Dominicaine, il s'agit de l'« espagnol ».

**Remarque:** Toutes les dispositions de clavier non prises en charge utilisent la disposition de clavier américain par défaut. Cela signifie également que les seuls caractères reconnus et pouvant être saisis au clavier sont ceux qui sont pris en charge dans la disposition de clavier américain. De la sorte, les utilisateurs ne peuvent se connecter lors de l'authentification au démarrage que si leur nom d'utilisateur et leur mot de passe sont composés de caractères pris en charge dans la disposition de clavier de la langue correspondante.

#### **18.3.4.1 Clavier virtuel**

Sophos SafeGuard propose aux utilisateurs un clavier virtuel qu'ils peuvent afficher/masquer dans l'authentification au démarrage et sur les touches à l'écran duquel ils peuvent cliquer pour entrer des informations d'identification, etc.

En tant que responsable de la sécurité, vous pouvez activer/désactiver l'affichage du clavier virtuel à l'aide d'une stratégie du type **Paramètres de machine spécifiques** avec l'option **Clavier virtuel**.

La prise en charge du clavier virtuel doit être activée/désactivée via un paramètre de stratégie.

Le clavier virtuel accepte différentes dispositions et il est possible de changer la disposition à l'aide des mêmes options que pour la disposition du clavier de l'authentification au démarrage.

#### **18.3.4.2 Modification de la disposition du clavier**

La disposition du clavier pour l'authentification au démarrage, clavier virtuel inclus, peut être modifiée rétrospectivement.

Pour modifier la langue de la disposition du clavier, procédez comme suit :

1. Sélectionnez **Démarrer > Panneau de configuration > Options régionales et linguistiques > Options avancées**.
2. Dans l'onglet **Options régionales**, sélectionnez la langue souhaitée.

3. Dans l'onglet **Options avancées**, activez l'option **Appliquer tous les paramètres au compte d'utilisateur actuel et au profil utilisateur par défaut** sous **Paramètres par défaut du compte d'utilisateur**.
4. Cliquez sur **OK** pour confirmer vos paramètres.

POA mémorise la disposition du clavier utilisée au cours de la dernière connexion et l'active automatiquement à la connexion suivante. Cette opération nécessite que vous réinitialisiez l'ordinateur final deux fois. Si la disposition du clavier mémorisée est désactivée via les **Options régionales et linguistiques**, elle est conservée jusqu'à ce que l'utilisateur en sélectionne une autre.

**Remarque:** Par ailleurs, vous devez modifier la langue de la disposition du clavier pour les programmes non-unicode.

Si la langue souhaitée n'est pas disponible sur le système, Windows peut vous inviter à l'installer. Après l'avoir fait, vous devez réinitialiser l'ordinateur deux fois de sorte que, en premier lieu, la nouvelle disposition du clavier puisse être lue par l'authentification au démarrage et, en second lieu, que l'authentification au démarrage puisse définir la nouvelle disposition.

Vous pouvez changer la disposition du clavier requise pour l'authentification au démarrage à l'aide de la souris ou du clavier (**Alt+Maj**).

Vous pouvez voir les langues installées et disponibles sur le système via Démarrer > Exécuter > regedit > HKEY\_USERS\DEFAULT\Keyboard Layout\Preload.

## 18.4 Raccourcis clavier pris en charge dans l'authentification au démarrage

Certains paramètres et fonctionnalités matériels peuvent générer des problèmes lors du démarrage des ordinateurs finaux et provoquer le blocage du système. L'authentification au démarrage prend en charge plusieurs raccourcis clavier pour modifier les paramètres matériels et désactiver des fonctionnalités. De plus, des listes « grise » et « noire » contenant les fonctions connues pour provoquer des problèmes sont intégrées au fichier .msi installé sur l'ordinateur.

Nous vous recommandons d'installer une version mise à jour du fichier de configuration POA avant tout déploiement important de Sophos SafeGuard. Le fichier est mis à jour tous les mois et est téléchargeable à l'adresse suivante : <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

Vous pouvez personnaliser ce fichier en fonction du matériel d'un environnement spécifique.

**Remarque:** Lorsqu'un fichier personnalisé est utilisé, celui-ci remplace le fichier intégré au fichier .msi. Le fichier par défaut est utilisé uniquement lorsqu'aucun fichier de configuration POA n'a été défini ou trouvé.

Pour installer le fichier de configuration POA, entrez la commande suivante :

MSIEXEC /i <package MSI client> POACFG=<chemin du fichier de configuration POA>

Pour en savoir plus, consultez la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/65700.html>.

**Les raccourcis clavier suivants sont pris en charge dans POA :**

- **Maj F3** = support patrimonial USB (actif/inactif)
- **Maj F4** = mode graphique VESA (actif/inactif)
- **Maj F5** = support USB 1.x et 2.0 (actif/inactif)
- **Maj F6** = contrôleur ATA (actif/inactif)
- **Maj F7** = support USB 2.0 seulement (actif/inactif)

Le support USB 1.x reste tel qu'il est défini par Maj F5.

- **Maj F9** = ACPI/APIC (actif/inactif)

**Matrice de dépendance des raccourcis clavier USB**

Maj F3	Maj F5	Maj F7	Patrimonial	USB 1.x	USB 2.0	Commentaire
désactivé	désactivé	désactivé	activé	activé	activé	3.
activé	désactivé	désactivé	désactivé	activé	activé	Par défaut
désactivé	activé	désactivé	activé	désactivé	désactivé	1., 2.
activé	activé	désactivé	activé	désactivé	désactivé	1., 2.
désactivé	désactivé	activé	activé	activé	désactivé	3.
activé	désactivé	activé	désactivé	activé	désactivé	
désactivé	activé	activé	activé	désactivé	désactivé	
activé	activé	activé	activé	désactivé	désactivé	2.

1. Maj F5 désactive USB 1.x et USB 2.0.

**Remarque:** Le fait d'appuyer sur Maj F5 pendant la période d'initialisation réduit considérablement la durée de lancement de l'authentification au démarrage. Gardez cependant en mémoire que si l'ordinateur est équipé d'un clavier USB ou d'une souris USB, ces derniers peuvent être désactivés si vous appuyez sur **Maj F5**.

2. Si aucun support USB n'est actif, l'authentification au démarrage tente d'utiliser BIOS SMM au lieu de sauvegarder et de restaurer le contrôleur USB. Le mode patrimonial peut fonctionner dans ce scénario.
3. Le support patrimonial est actif, USB est actif. L'authentification au démarrage tente de sauvegarder et de restaurer le contrôleur USB. Il se peut que le système se bloque selon la version du BIOS utilisée.

Vous pouvez spécifier les modifications pouvant être effectuées en utilisant des raccourcis clavier lors de l'installation du logiciel de chiffrement Sophos SafeGuard à l'aide d'un fichier .mst. Pour ce faire, utilisez l'appel approprié avec msiexec.

NOVESA	Définit si le mode VESA ou VGA est utilisé.0 = mode VESA (standard)1 = mode VGA
NOLEGACY	Définit si le support patrimonial est activé après connexion à l'authentification au démarrage.0 = support patrimonial activé 1 = le support patrimonial non activé (standard)
ALTERNATE	Définit si les périphériques USB sont pris en charge par POA. 0 = support USB activé (standard)1 = aucun support USB
NOATA	Définit si un pilote de périphérique int13 est utilisé.0 = pilote de périphérique ATA standard (par défaut)1 = pilote de périphérique int13
ACPIAPIC	Définit si le support ACPI/APIC est utilisé.0 = aucun support ACPI/APIC (par défaut)1 = support ACPI/APIC actif
NOVESA	Définit si le mode VESA ou VGA est utilisé.0 = mode VESA (standard)1 = mode VGA

## 18.5 POA désactivé et Lenovo Rescue and Recovery

Si l'authentification au démarrage est désactivée sur l'ordinateur, l'authentification Rescue and Recovery doit être activée pour la protection contre l'accès aux fichiers chiffrés à partir de l'environnement Rescue and Recovery.

Pour plus de détails sur l'activation de l'authentification Rescue and Recovery, veuillez vous reporter à la documentation Lenovo Rescue and Recovery.

## 19 Options de récupération

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

### ■ 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, et ainsi les tâches de routine des membres du support en leur permettant de se concentrer sur des demandes plus complexes.

Pour en savoir plus voir [Récupération via Local Self Help](#), à la page 134.

### ■ 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.

Pour en savoir plus voir [Récupération par Challenge/Réponse](#), à la page 140.

### ■ Récupération du système

Sophos SafeGuard propose plusieurs méthodes et outils de récupération relatifs à des composants du système essentiels ainsi qu'à des composants Sophos SafeGuard, par exemple :

- MBR (Master Boot Record) corrompu
- Problèmes du noyau Sophos SafeGuard
- Problèmes d'accès aux volumes
- Problèmes d'initialisation Windows

Pour en savoir plus voir [Récupération du système](#), à la page 156.

## 20 Récupération via Local Self Help

Sophos SafeGuard propose Local Self Help pour les ordinateurs protégés par Sophos SafeGuard afin de permettre aux utilisateurs ayant oublié leur mot de passe de se connecter à leur ordinateur sans recourir à l'aide du support.

Grâce à Local Self Help, les utilisateurs peuvent accéder de nouveau à leur ordinateur portable dans les situations où aucune connexion par téléphone ou réseau n'est disponible et où ils ne peuvent donc pas utiliser de procédure Challenge/Réponse (par exemple à bord d'un avion). L'utilisateur peut se connecter à son ordinateur en répondant à un nombre prédéfini de questions dans l'authentification au démarrage (POA).

En tant que responsable de la sécurité, vous pouvez définir de manière centralisée les questions auxquelles il faudra répondre et les distribuer sur l'ordinateur à l'aide d'une stratégie. À titre d'exemple, nous vous proposons un sujet de question prédéfini. Vous pouvez utiliser ce sujet tel quel ou le modifier. Dans la stratégie correspondante, vous pouvez également accorder aux utilisateurs le droit de définir des questions personnalisées.

Pour proposer les réponses initiales et modifier les questions, l'assistant de Local Self Help est disponible sur l'ordinateur final une fois que la fonction est activée à l'aide d'une stratégie. Pour obtenir une description détaillée de Local Self Help sur l'ordinateur final, consultez l'aide de l'utilisateur de Sophos SafeGuard, chapitre *Récupération via Local Self Help*.

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

### 20.1 Définition des paramètres de Local Self Help à l'aide d'une stratégie

Vous définissez les paramètres de Local Self Help dans une stratégie du type **Paramètres généraux** sous **Récupération de connexion - Activer Local Self Help**. Vous pouvez activer ici la fonction à utiliser sur l'ordinateur final et définir d'autres droits et paramètres.

### 20.1.1 Activation de Local Self Help

Pour activer Local Self Help et l'utiliser sur l'ordinateur final, sélectionnez **Oui** dans le champ **Activer Local Self Help**.

Une fois la stratégie appliquée à l'ordinateur, ce paramètre permet à l'utilisateur d'exploiter Local Self Help pour récupérer la connexion. Pour pouvoir utiliser Local Self Help, l'utilisateur doit alors activer cette méthode de récupération en répondant à un nombre de questions spécifié parmi les questions reçues ou en créant et en répondant à des questions personnalisées (en fonction de ses autorisations).

À cet effet, l'assistant de Local Self Help est disponible via une icône dans la barre des tâches Windows une fois la stratégie appliquée et l'ordinateur redémarré.

### 20.1.2 Définition de paramètres supplémentaires

Outre l'activation de Local Self Help, vous pouvez définir les paramètres suivants pour cette fonction dans une stratégie du type **Paramètres généraux** :

#### ■ **Longueur minimale des réponses**

Dans ce champ, définissez la longueur minimale (en caractères) des réponses. Le nombre par défaut est **1**.

#### ■ **Texte de bienvenue sous Windows**

Dans ce champ, vous pouvez spécifier le texte d'informations à afficher dans la première boîte de dialogue au démarrage de l'assistant de Local Self Help sur l'ordinateur. Avant de pouvoir spécifier le texte ici, il doit être créé et enregistré.

#### ■ **L'utilisateur peut définir des questions personnalisées**

Les scénarios suivants sont possibles concernant la définition de questions pour Local Self Help :

- En tant que responsable de la sécurité, définissez les questions et distribuez-les aux utilisateurs. Les utilisateurs ne sont pas autorisés à définir des questions personnalisées.
- En tant que responsable de la sécurité, définissez les questions et distribuez-les aux utilisateurs. Les utilisateurs sont également autorisés à définir des questions personnalisées. Lorsqu'ils répondent au nombre minimum de questions nécessaire pour activer Local Self Help, les utilisateurs peuvent choisir entre des questions prédéfinies et des questions personnalisées ou une combinaison des deux.

- Vous autorisez les utilisateurs à définir des questions personnalisées. Les utilisateurs activent Local Self Help sur leurs ordinateurs en définissant des questions personnalisées et en y répondant.

Pour autoriser les utilisateurs à définir des questions personnalisées, sélectionnez l'option **Oui** dans le champ **L'utilisateur peut définir des questions personnalisées**.

## 20.2 Définition de questions

Pour pouvoir utiliser Local Self Help sur un ordinateur final, l'utilisateur doit répondre à dix questions minimum et les enregistrer. Pour se connecter à partir de l'authentification au démarrage via Local Self Help, l'utilisateur doit répondre à cinq questions sélectionnées de façon aléatoire parmi ces dix questions.

Si l'utilisateur n'est pas autorisé à définir des questions personnalisées, vous devez transférer dix questions prédéfinies au minimum vers l'ordinateur au moyen de la stratégie pour permettre à l'utilisateur d'activer Local Self Help.

Pour enregistrer et modifier des questions Local Self Help, en tant que responsable de la sécurité, vous devez disposer du droit **Modifier les questions Local Self Help**.

### 20.2.1 Utilisation du modèle

Un sujet de question prédéfini est proposé pour Local Self Help. Par défaut, ce sujet de question est disponible en allemand et en anglais sous **Questions Local Self Help** dans la zone de navigation de stratégie.

Le sujet de question est aussi éventuellement disponible en français, italien, espagnol et japonais. Vous pouvez également importer ces versions de langue dans la zone de navigation de stratégie.

**Remarque:** Lors de la saisie des réponses en japonais pour activer Local Self Help sur les ordinateurs finaux, l'utilisateur doit utiliser les caractères Romaji (Roman). Sinon, les réponses ne correspondent pas lorsque l'utilisateur les saisit dans l'authentification au démarrage.

Vous pouvez utiliser le sujet de question prédéfini tel quel, le modifier ou le supprimer.

Si vous conservez les deux versions de langue du sujet de question prédéfini en l'état et que vous activez Local Self Help à l'aide d'une stratégie du type **Paramètres généraux**, les deux sujets de question prédéfinis sont transférés automatiquement vers l'ordinateur final avec la stratégie.

## 20.3 Importation de sujets de question

Grâce à la procédure d'importation, vous pouvez importer d'autres versions de langue du sujet de question prédéfini ou de vos listes de questions personnalisées créées sous la forme de fichiers .XML.

Pour importer un ensemble de questions,

1. Créez un sujet de question.
2. Dans la zone de navigation **Stratégies**, sélectionnez le nouveau sujet de question sous **Questions Local Self Help**.
3. 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 **Importer**.
4. Sélectionnez le répertoire et le sujet de question, puis cliquez sur **Ouvrir**.

Les questions importées s'affichent dans la zone d'action. Vous pouvez maintenant enregistrer le sujet de question tel quel ou le modifier.

## 20.4 Création d'un sujet de question et ajout de questions

Vous pouvez non seulement utiliser des sujets de questions dans plusieurs langues mais également créer de nouveaux sujets de questions à propos de thèmes différents. Vous pouvez ainsi proposer aux utilisateurs un choix de sujets de questions qui pourraient leur convenir.

Pour créer un sujet de question et ajouter des questions, procédez comme suit :

1. Dans la zone de navigation **Stratégies**, sélectionnez **Questions Local Self Help**.
2. Cliquez avec le bouton droit de la souris sur **Questions Local Self Help**, puis sélectionnez **Nouveau > Sujet de la question**.
3. Saisissez un nom pour le sujet de question et cliquez sur **OK**.
4. Dans la zone de navigation **Stratégies**, sélectionnez le nouveau sujet de question sous **Questions Local Self Help**.
5. 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**.

6. Une nouvelle ligne de question est ajoutée. Saisissez votre question et appuyez sur **Entrée**. Répétez cette étape pour ajouter d'autres questions.
7. Pour enregistrer vos modifications, cliquez sur l'icône **Enregistrer** dans la barre d'outils.

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

## 20.5 Modification de sujets de question

Pour modifier des sujets de questions existants, procédez comme suit :

1. Dans la zone de navigation **Stratégies**, sélectionnez le sujet de question souhaité sous **Questions Local Self Help**.
2. Vous pouvez maintenant ajouter, modifier ou supprimer des questions.
  - Pour ajouter des questions, cliquez avec le bouton droit de la souris dans la zone d'action pour afficher le menu contextuel. Dans le menu contextuel, cliquez sur **Ajouter**. Une nouvelle ligne est ajoutée à la liste de questions. Entrez votre question sur la ligne.
  - Pour modifier des questions, cliquez sur le texte de la question souhaitée dans la zone d'action. La question est marquée d'une icône en forme de crayon. Entrez vos modifications sur la ligne de la question.
  - Pour supprimer des questions, sélectionnez la question souhaitée en cliquant sur la case grise située au début de la ligne de la question dans la zone d'action, puis cliquez sur **Supprimer** dans le menu contextuel de la question.
3. Pour enregistrer vos modifications, cliquez sur l'icône **Enregistrer** dans la barre d'outils.

Le sujet de question modifié est enregistré et transféré avec la stratégie du type **Paramètres généraux** qui active Local Self Help sur les ordinateurs finaux.

## 20.6 Suppression de sujets de question

Pour supprimer intégralement un sujet de question, cliquez avec le bouton droit de la souris sur le sujet concerné **Questions Local Self Help** dans la zone de navigation **Stratégies**, puis sélectionnez **Supprimer**.

**Remarque:** Si vous supprimez un sujet de question alors que des utilisateurs ont déjà répondu à certaines questions pour activer Local Self Help sur leurs ordinateurs, leurs réponses ne sont plus valides car les questions n'existent plus.

## 20.7 Enregistrement de textes de bienvenue

Vous pouvez enregistrer un texte de bienvenue à afficher dans la première boîte de dialogue de l'assistant de Local Self Help dans la zone de navigation Stratégies de SafeGuard Policy Editor.

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans SafeGuard Policy Editor. La taille maximale de ces fichiers pour les textes d'informations est de 50 Ko. Sophos SafeGuard n'utilise que des textes codés en Unicode UTF-16. Si vous ne créez pas les fichiers texte dans ce format, ils sont convertis automatiquement lors de l'enregistrement.

Si une conversion s'impose, un message s'affiche et indique que le fichier est en cours de conversion.

Pour enregistrer des textes d'informations :

1. Dans la zone de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Texte d'informations** et sélectionnez **Nouveau > Texte**.
2. Entrez le nom du texte à afficher dans le champ **Nom de l'élément de texte**.
3. Cliquez sur [...] pour sélectionner le fichier texte préalablement créé. Un message s'affiche si le fichier doit être converti.
4. Cliquez sur **OK**.

Le nouvel élément de texte s'affiche en tant que nœud secondaire sous **Texte d'informations** dans la zone de navigation **Stratégies**. Si vous sélectionnez un élément de texte, son contenu s'affiche dans la fenêtre de droite. L'élément de texte peut désormais être sélectionné lors de la création de stratégies.

Répétez la procédure pour enregistrer d'autres éléments de texte. Tous les éléments de texte enregistrés s'affichent en tant que nœuds secondaires.

## 21 Récupération par Challenge/Réponse

Pour simplifier le flux de travail et réduire les coûts du support, Sophos SafeGuard fournit une solution de récupération Challenge/Réponse. Sophos SafeGuard aide les utilisateurs qui ne parviennent pas à se connecter à leur ordinateur ou qui ne peuvent pas accéder aux données chiffrées en leur proposant un mécanisme de Challenge/Réponse convivial.

Cette fonctionnalité est intégrée à SafeGuard Policy Editor sous la forme d'un assistant de récupération.

### 21.1 Avantages de la procédure Challenge/Réponse

Le mécanisme Challenge/Réponse est un système de récupération sécurisé et fiable.

- Tout au long du processus, aucune donnée confidentielle n'est échangée sous une forme autre que chiffrée.
- Cette procédure ne contient aucun point d'écoute électronique de tiers, car les données espionnées ne peuvent pas être utilisées ultérieurement ni sur d'autres périphériques.
- L'utilisateur peut commencer à retravailler rapidement. L'oubli du mot de passe n'entraîne aucune perte de données chiffrées.

### 21.2 Situations classiques nécessitant l'aide du support

- Un utilisateur a oublié le mot de passe au niveau de l'authentification et l'ordinateur a été verrouillé.

**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 peut être affiché et l'utilisateur peut continuer à l'utiliser. Cela évitera la réinitialisation du mot de passe et le recours à l'assistance du support. Pour plus d'informations, voir [Récupération via Local Self Help](#), à la page 134.

- Le cache local de l'authentification au démarrage est partiellement endommagé.

Sophos SafeGuard propose différents flux de travail de récupération pour ces scénarios classiques, ce qui permet aux utilisateurs d'accéder de nouveau à leur ordinateur.

## 21.3 Flux de travail de challenge/réponse

La procédure Challenge/Réponse repose sur les deux composants suivants :

- l'ordinateur final sur lequel le code de challenge sera généré ;
- SafeGuard Policy Editor où, en tant que responsable du support possédant les droits correspondants, vous créez un code de réponse qui autorisera l'utilisateur à effectuer l'action requise sur l'ordinateur.

1. Sur l'ordinateur final, l'utilisateur demande le code de challenge. En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage, soit via l'outil de récupération de clé KeyRecovery.

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

2. L'utilisateur contacte le support. Il lui fournit les données d'identification nécessaires, ainsi que le code de challenge.

3. Le support lance l'assistant de récupération dans SafeGuard Policy Editor.

4. Le support sélectionne le type de récupération approprié, confirme les données d'identification et le code de challenge, puis sélectionne l'action de récupération souhaitée.

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

5. Le support transmet le code de réponse à l'utilisateur, par exemple par téléphone ou message texte.

6. L'utilisateur saisit le code de réponse, En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage, soit via l'outil de récupération de clé KeyRecovery.

L'utilisateur est ensuite autorisé à effectuer l'action convenue, par exemple à réinitialiser le mot de passe et à reprendre son travail.

## 21.4 Ouverture de l'assistant de récupération

Pour pouvoir effectuer une procédure de récupération, assurez-vous de disposer des droits et des autorisations requis.

1. Connectez-vous à SafeGuard Policy Editor.
2. Cliquez sur **Outils > Récupération** dans la barre de menus.

L'assistant de récupération SafeGuard démarre. Vous pouvez sélectionner le type de récupération demandé.

## 21.5 Types de récupération

Sélectionnez le type de récupération que vous souhaitez utiliser. Les types de récupération suivants sont fournis :

### ■ Challenge/Réponse pour l'authentification au démarrage

Sophos SafeGuard propose une procédure Challenge/Réponse pour l'authentification au démarrage si l'utilisateur a oublié son mot de passe ou s'il l'a saisi de manière incorrecte un trop grand nombre de fois.

**Remarque:** Par ailleurs, la méthode de récupération de connexion Local Self Help ne requiert aucune assistance du support.

### ■ Challenge/Réponse à l'aide de clients virtuels

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.

## 21.6 Challenge/Réponse pour l'authentification au démarrage

Sophos SafeGuard propose une procédure Challenge/Réponse pour l'authentification au démarrage si l'utilisateur a oublié le mot de passe ou s'il l'a saisi de manière incorrecte un trop grand nombre de fois. Dans ce cas, les informations de récupération nécessaires à la procédure Challenge/Réponse sont basées sur le fichier de récupération des clés. Sur chaque ordinateur final Sophos SafeGuard, un fichier de récupération de clé de ce type est généré lors du déploiement de Sophos SafeGuard.

Si ce fichier de récupération de clés est accessible au support Sophos SafeGuard, par exemple par l'intermédiaire d'un chemin réseau partagé, une procédure Challenge/Réponse pour l'authentification au démarrage pour un ordinateur protégé par Sophos SafeGuard peut être fournie.

Afin de faciliter la recherche et le regroupement des fichiers de récupération de clés, ils portent le nom de l'ordinateur : nomordinateur.GUID.xml dans le nom du fichier. Vous pouvez ainsi effectuer des recherches de caractères génériques avec des astérisques (\*), par exemple : \*.GUID.xml.

**Remarque:** Lorsqu'un ordinateur est renommé, le cache local de l'ordinateur n'applique pas le changement de nom. Le cache local stocke toutes les clés et stratégies ainsi que les certificats utilisateur et les fichiers d'audit. Le nouveau nom de l'ordinateur doit donc être supprimé du cache local afin de ne conserver que le nom précédent, bien que l'ordinateur ait été renommé sous Windows.

### **21.6.1 Actions de récupération de l'authentification au démarrage**

La procédure Challenge/Réponse pour l'authentification au démarrage d'un ordinateur final intervient dans les configurations suivantes :

- L'utilisateur a entré un mot de passe incorrect un trop grand nombre de fois au niveau de l'authentification au démarrage et l'ordinateur est verrouillé.
- L'utilisateur a oublié le mot de passe.
- Un cache local endommagé doit être réparé.

Pour un ordinateur protégé par Sophos SafeGuard, aucune clé utilisateur n'est disponible dans la base de données. La clé machine définie est, quant à elle, disponible. Par conséquent, la seule action de récupération possible dans une session de Challenge/Réponse est **Initialisation du client SGN sans connexion utilisateur**.

La procédure Challenge/Réponse permet à l'ordinateur de démarrer à partir de l'authentification au démarrage. L'utilisateur pourra alors se connecter à Windows.

Études de cas de récupération potentiels :

**L'utilisateur a entré un mot de passe incorrect un trop grand nombre de fois au niveau de l'authentification au démarrage et l'ordinateur est verrouillé.**

L'ordinateur est verrouillé et l'utilisateur est invité à lancer une procédure Challenge/Réponse pour le déverrouiller. Comme dans ce cas, la réinitialisation du mot de passe n'est pas nécessaire car l'utilisateur n'a pas oublié le mot de passe. La procédure Challenge/Réponse permet à l'ordinateur de s'initialiser en passant par l'authentification au démarrage. L'utilisateur peut ensuite saisir le mot de passe approprié au niveau Windows et réutiliser l'ordinateur.

**L'utilisateur a oublié le mot de passe.**

**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. Pour plus d'informations, voir [Récupération via Local Self Help](#), à la page 134.

Lors de la récupération d'un mot de passe oublié via la procédure Challenge/Réponse, une réinitialisation de mot de passe est requise.

1. La procédure Challenge/Réponse permet à l'ordinateur de démarrer à partir de l'authentification au démarrage.
2. 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.
3. 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.
4. 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.
5. Sophos SafeGuard détecte que le nouveau choix de mot de passe ne correspond pas au mot de passe Sophos SafeGuard actuel utilisé dans 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**.

6. 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.
7. 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.

### **Clés pour SafeGuard Data Exchange**

**Remarque:** Lorsque l'utilisateur a oublié le mot de passe Windows et doit en saisir un nouveau, un nouveau certificat utilisateur est également créé. L'utilisateur ne pourra donc plus utiliser les clés déjà créées pour SafeGuard Data Exchange. Pour continuer à utiliser les clés utilisateur déjà générées pour SafeGuard Data Exchange, l'utilisateur doit se souvenir des passphrases SafeGuard Data Exchange afin de les réactiver.

**Remarque:** SafeGuard Data Exchange n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

### **Le cache local doit être réparé.**

Le cache local stocke toutes les clés et stratégies ainsi que les certificats utilisateur et les fichiers d'audit. Lorsque le cache local est corrompu, la récupération de connexion est désactivée par défaut, c'est-à-dire que sa restauration s'effectue automatiquement à partir de la sauvegarde. Aucune procédure Challenge/Réponse n'est donc requise pour réparer le cache local. Cependant, la récupération de connexion peut être activée par stratégie, si le cache local doit effectivement être réparé via une procédure Challenge/Réponse. Dans ce cas, l'utilisateur est automatiquement invité à lancer une procédure Challenge/Réponse, si le cache local est corrompu.

## **21.6.2 Génération d'une réponse à l'aide du fichier de récupération de clé**

Le fichier de récupération de clé généré durant l'installation du logiciel de chiffrement Sophos SafeGuard doit être stocké dans un emplacement accessible au responsable support et son nom doit être connu.

Pour générer une réponse, procédez comme suit :

1. Pour ouvrir l'assistant de récupération dans SafeGuard Policy Editor, sélectionnez **Outils > Récupération** dans la barre de menus.
2. Dans **Type de récupération**, sélectionnez **Client Sophos SafeGuard**.
3. Cliquez sur **Parcourir** pour localiser le fichier de récupération de clé requis. Pour faciliter l'identification des fichiers de récupération, leur nom est identique à celui de l'ordinateur : nomordinateur.GUID.xml.

4. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié.

Si le code de challenge a été saisi correctement, l'action de récupération demandée par l'ordinateur Sophos SafeGuard, ainsi que les actions de récupération possibles s'affichent. S'il a été saisi de façon incorrecte, le terme **Non valide** s'affiche au-dessous du bloc contenant l'erreur.

5. Sélectionnez l'action que l'utilisateur doit entreprendre, puis cliquez sur **Suivant**.
6. Un code de réponse est généré. Communiquez-le à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

L'utilisateur peut saisir le code de réponse, exécuter l'action requise, puis reprendre son travail.

## 21.7 Challenge/Réponse à l'aide de clients virtuels

La procédure Challenge/Réponse utilisant les clients virtuels dépend des éléments suivants :

- **Fichier de récupération de clé**

Il est créé durant la configuration du logiciel de chiffrement Sophos SafeGuard et contient la clé de chiffrement de l'ordinateur final. Ce fichier de récupération de clé est généré pour chaque ordinateur protégé par Sophos SafeGuard et contient la clé machine définie, qui est chiffrée à l'aide du certificat de l'entreprise. Le support doit pouvoir y accéder, par exemple sur une carte mémoire ou via un chemin réseau partagé.

- **Fichier du client virtuel**

Il s'agit de fichiers spécifiques appelés clients virtuels qui sont créés dans SafeGuard Policy Editor et utilisés comme informations de référence dans la base de données.

- **Disque de récupération Windows PE modifié par Sophos SafeGuard**

Le disque de récupération sert à initialiser l'ordinateur final à partir du BIOS.

- **Outil de récupération de clé KeyRecovery**

Cet outil sert à lancer la procédure Challenge/Réponse. Il est déjà disponible sur le disque de récupération Windows PE modifié par Sophos SafeGuard. Vous le trouverez également dans le répertoire Outils du logiciel Sophos SafeGuard.

### **21.7.1 Clients virtuels**

Les clients virtuels sont des fichiers de clés spécifiques pouvant être utilisés pour récupérer un volume chiffré lorsqu'aucune information de référence sur l'ordinateur n'est disponible dans la base de données et que la procédure Challenge/Réponse habituelle n'est pas prise en charge. Le client virtuel fait office d'informations d'identification et de référence durant la procédure Challenge/Réponse et est stocké dans la base de données.

Pour permettre l'exécution d'une procédure Challenge/Réponse dans des situations d'urgence complexes, vous devez créer des fichiers spécifiques, appelés clients virtuels, et les distribuer à l'utilisateur avant de lancer la procédure elle-même. L'ordinateur redevient accessible grâce à ces clients virtuels, à un outil de récupération de clé (KeyRecovery) et à un disque de récupération Windows PE modifié par SafeGuard, fourni avec votre produit.

### **21.7.2 Flux de travail de récupération à l'aide de clients virtuels**

Pour accéder à l'ordinateur chiffré, voici le flux de travail général qui s'applique :

1. Demandez au support technique de vous fournir le disque de récupération Sophos SafeGuard.
2. 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>.
3. Créez le client virtuel dans SafeGuard Policy Editor.
4. Exportez le client virtuel dans un fichier.
5. Démarrez l'ordinateur depuis le disque de récupération.
6. Importez le fichier du client virtuel dans l'outil de récupération de clé KeyRecovery.
7. Initialisez le challenge dans l'outil de récupération de clé KeyRecovery.
8. Confirmez le client virtuel dans SafeGuard Policy Editor.
9. Sélectionnez l'action de récupération requise.
10. Saisissez le code de challenge dans SafeGuard Policy Editor.
11. Générez le code de réponse dans SafeGuard Policy Editor.
12. Saisissez le code de réponse dans l'outil de récupération de clé KeyRecovery.

L'ordinateur est accessible à nouveau.

### 21.7.3 Création d'un client virtuel

Les clients virtuels sont des fichiers de clés chiffrés pouvant être utilisés dans le cadre d'une récupération par procédure Challenge/Réponse à titre d'informations de référence sur l'ordinateur.

Les fichiers du client virtuel peuvent être utilisés par différents ordinateurs et pour plusieurs sessions de 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.

Le nouveau client virtuel s'affiche dans la zone d'action. Exportez-le ensuite dans un fichier.

### 21.7.4 Exportation d'un client virtuel

Les clients virtuels doivent être exportés dans des fichiers pour être distribués sur les ordinateurs finaux et utilisés à des fins de récupération. Ces fichiers sont toujours appelés recoverytoken.tok.

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 zone d'action, recherchez le client virtuel concerné en cliquant sur la loupe. Les clients virtuels disponibles s'affichent.
4. Sélectionnez l'entrée requise dans la zone d'action et cliquez sur **Exporter le client virtuel** dans la barre d'outils.
5. Sélectionnez un emplacement de stockage pour le fichier du client virtuel recoverytoken.tok, puis cliquez sur **OK** pour confirmer.

Enregistrez le fichier dans un emplacement sécurisé.

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

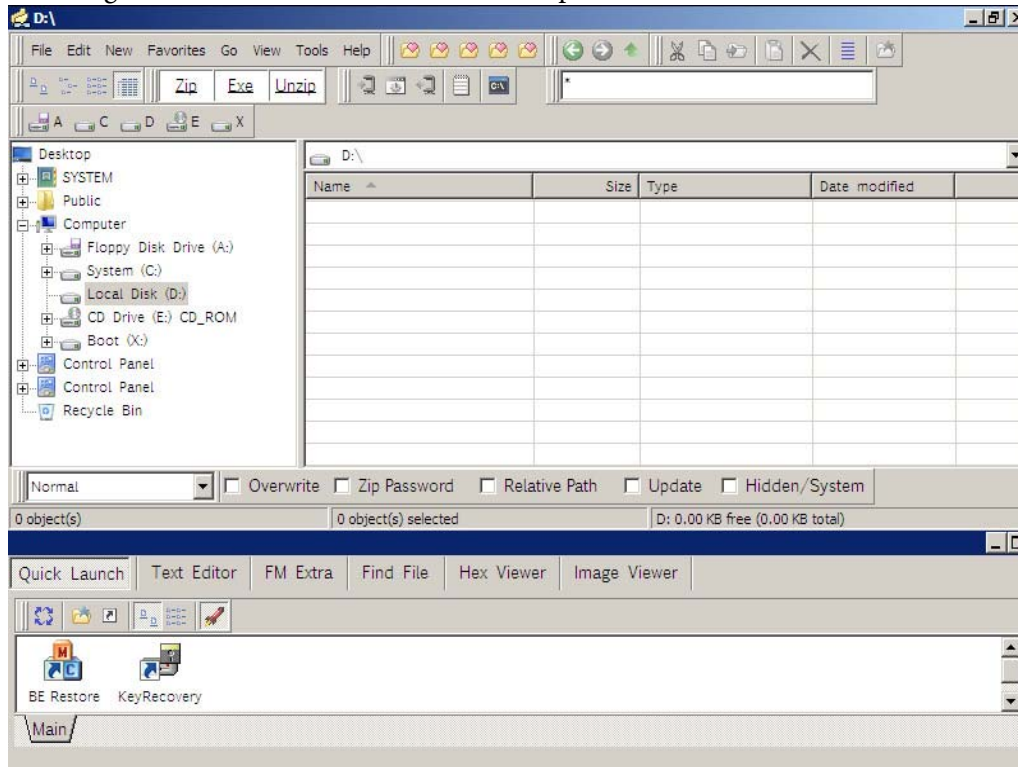
6. Copiez le fichier du client virtuel recoverytoken.tok sur un support amovible. Nous recommandons d'utiliser une carte mémoire.

Veillez à conserver ce support de stockage en lieu sûr. Rendez-le accessible côté utilisateur car il servira à lancer une procédure Challenge/Réponse avec les clients virtuels.

### 21.7.5 Initialisation de l'ordinateur depuis le disque de récupération

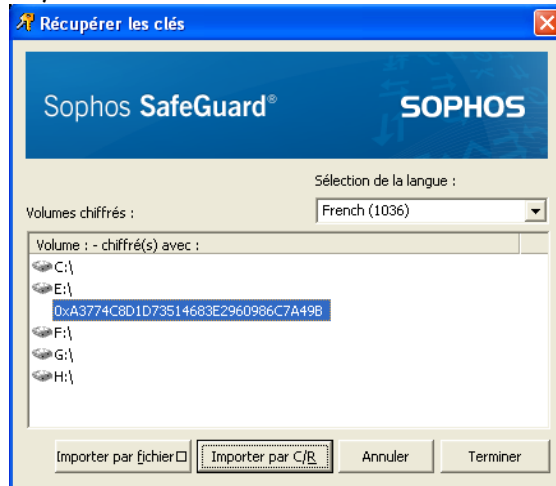
Vérifiez que la séquence d'initialisation dans les paramètres du BIOS permet de démarrer à partir du CD.

1. Insérez le disque de récupération, puis démarrez l'ordinateur final. Le gestionnaire de fichiers intégré s'ouvre. Les volumes et les lecteurs présents s'affichent immédiatement.



Le contenu du lecteur chiffré ne s'affiche pas dans le gestionnaire de fichiers. Ni le système de fichiers, ni la capacité et l'espace utilisé/libre ne figurent dans les propriétés du lecteur chiffré.

2. Au bas du gestionnaire de fichiers, dans la section **Lancement rapide**, cliquez sur l'icône KeyRecovery pour ouvrir l'outil de récupération de clé KeyRecovery. L'outil de récupération de clé KeyRecovery affiche les ID de clé des lecteurs chiffrés.

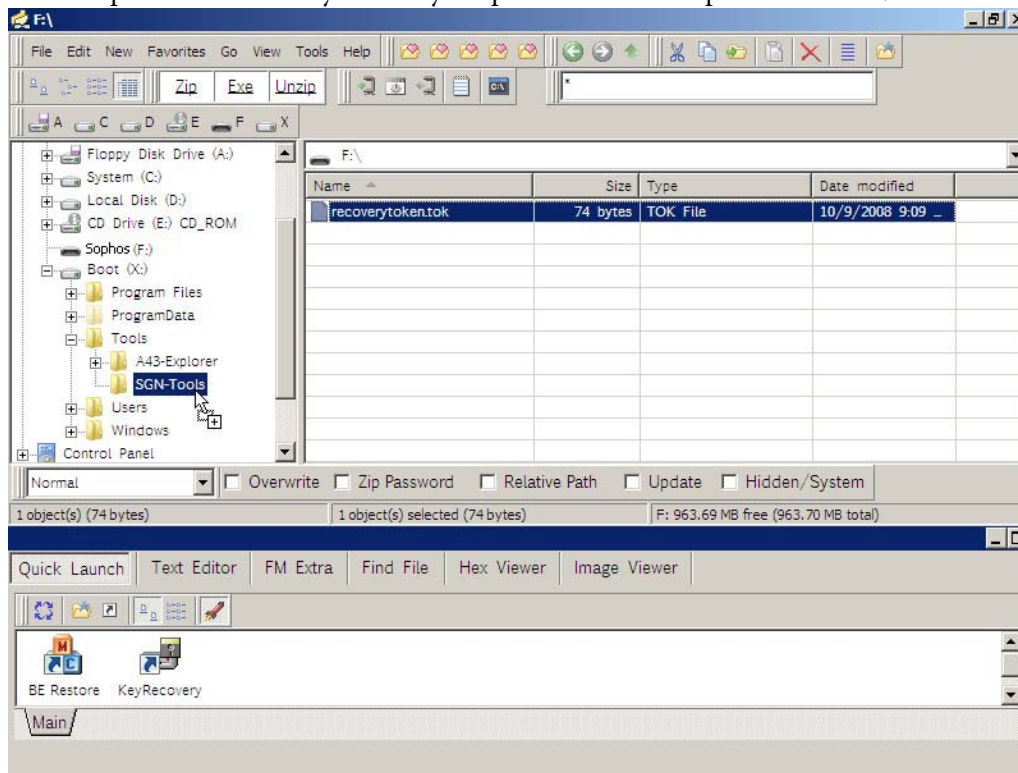


3. Recherchez les ID de clé des lecteurs auxquels vous souhaitez accéder. Vous devrez fournir cet ID de clé ultérieurement.

Importez ensuite le client virtuel dans l'outil de récupération de clé.

## 21.7.6 Importation du client virtuel dans l'outil de récupération de clé KeyRecovery

- L'ordinateur a été initialisé depuis le disque de récupération.
  - Vérifiez que le lecteur USB, sur lequel est enregistré le fichier du client virtuel recoverytoken.tok, a été correctement monté.
1. Dans le gestionnaire de fichiers Windows PE, sélectionnez le lecteur sur lequel est enregistré le client virtuel. Le fichier recoverytoken.tok s'affiche sur la droite.
  2. Sélectionnez le fichier recoverytoken.tok et faites-le glisser sur le lecteur où se trouve l'outil de récupération de clé KeyRecovery. Déposez-le dans le répertoire Outils\Outils-SGN.



### 21.7.7 Lancement d'une procédure Challenge dans l'outil Recover Keys

1. Au bas du gestionnaire de fichiers Windows PE, dans la section **Lancement rapide**, cliquez sur l'icône KeyRecovery pour ouvrir l'outil de récupération de clé KeyRecovery. L'outil de récupération de clé KeyRecovery affiche les ID de clé des lecteurs chiffrés.

Cet outil démarre et affiche une liste de tous les volumes, ainsi que des informations de chiffrement correspondantes (ID de clé).



2. Sélectionnez le volume à déchiffrer, puis cliquez sur Importer par C/R pour générer le code de challenge.

À titre de référence dans la base de données Sophos SafeGuard, le fichier client virtuel est utilisé et mentionné dans la procédure Challenge. Le code de challenge est alors généré et s'affiche.

3. Communiquez le nom du client virtuel et le code de challenge au support, par exemple par téléphone ou en envoyant un message texte. Une aide à l'épellation est fournie.

## 21.7.8 Génération d'une réponse à l'aide de clients virtuels

Pour accéder à un ordinateur protégé par Sophos SafeGuard et générer une réponse à l'aide de clients virtuels, deux actions sont requises :

1. Confirmez le client virtuel dans la base de données de SafeGuard Policy Editor.
2. Sélectionnez l'action de récupération requise. Étant donné que seul le fichier de récupération de clé peut être déchiffré, il doit être sélectionné pour générer un code de réponse.

### 21.7.8.1 Confirmation du client virtuel

Le client virtuel doit avoir été créé dans SafeGuard Policy Editor sous **Clients virtuels** ainsi qu'être disponible dans la base de données.

1. Dans SafeGuard Policy Editor, cliquez sur **Outils > Récupération** pour ouvrir l'assistant de récupération.
2. Dans **Type de récupération**, sélectionnez **Client virtuel**.
3. Saisissez le nom du client virtuel que l'utilisateur vous a indiqué. Pour ce faire, vous pouvez procéder de plusieurs façons :
  - Saisissez directement le nom unique.
  - Sélectionnez un nom en cliquant sur [...] dans la section **Client virtuel** de la boîte de dialogue **Type de récupération**. Cliquez ensuite sur **Rechercher maintenant**. La liste des clients virtuels s'affiche. Sélectionnez le client virtuel requis, puis cliquez sur **OK**. Le nom du client virtuel s'affiche alors dans la fenêtre **Type de récupération** sous **Client virtuel**.
4. Cliquez sur **Suivant** pour confirmer le nom du fichier du client virtuel.

Ensuite, sélectionnez l'action de récupération requise.

### 21.7.8.2 Sélection du fichier de récupération de clé

Sélectionnez au préalable le client virtuel requis dans l'assistant de récupération SafeGuard Policy Editor.

Le support doit pouvoir accéder au fichier de récupération de clé nécessaire pour récupérer l'accès à l'ordinateur. Ce fichier peut par exemple se trouver sur un partage réseau

1. Dans l'assistant de récupération, dans le client virtuel, sélectionnez l'action de récupération **Clé requise**, puis cliquez sur **Suivant**.
2. Activez l'option **Sélectionner un fichier de récupération de clé contenant une clé de récupération**.

3. Cliquez sur [...] en regard de cette option pour rechercher le fichier. Pour faciliter l'identification des fichiers de récupération, leur nom est identique à celui de l'ordinateur : nomordinateur.GUID.xml.
4. Cliquez sur **Suivant** pour confirmer. La fenêtre dans laquelle vous devez saisir le code de challenge s'affiche.
5. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié.

Si le code de challenge a été saisi correctement, le code de réponse est généré. S'il a été saisi de façon incorrecte, le terme **Non valide** s'affiche au-dessous du bloc contenant l'erreur.

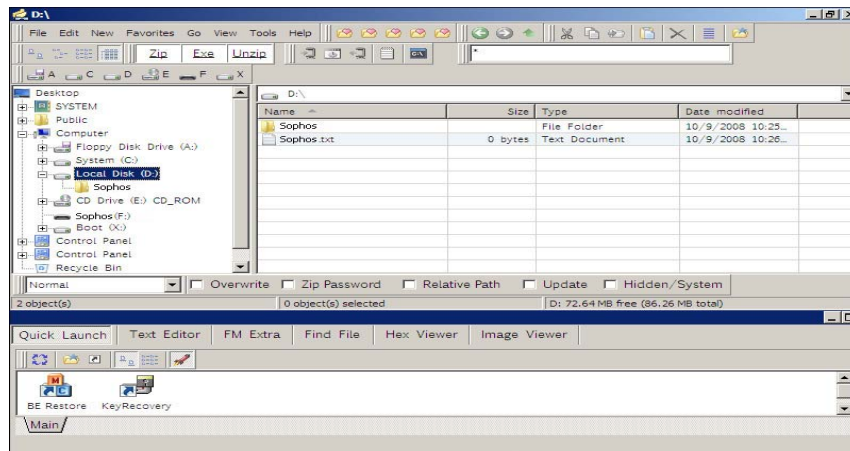
6. Lisez alors le code de réponse à l'utilisateur. Une aide à l'épellation est fournie. Vous pouvez également copier le code de réponse dans le Presse-papiers.

### 21.7.9 Saisie du code de réponse dans l'outil de récupération de clé KeyRecovery

1. Sur l'ordinateur final, dans l'outil de récupération de clé KeyRecovery, entrez le code de réponse fourni par le support.  
La clé de récupération requise figure dans ce code de réponse.
2. Cliquez sur OK. Le disque sélectionné pour la procédure Challenge/Réponse a été déchiffré.



3. Pour vérifier si le déchiffrement a réussi, sélectionnez le lecteur déchiffré dans le gestionnaire de fichiers Windows PE :



Le contenu du lecteur déchiffré s'affiche dans le gestionnaire de fichiers. Le système de fichiers, ainsi que la capacité et l'espace utilisé/libre, figurent dans les propriétés du lecteur déchiffré.

L'accès aux données stockées sur cette partition est récupéré. Suite à ce déchiffrement réussi, vous pouvez lire, écrire et copier des données à partir du disque indiqué et/ou vers celui-ci.

### 21.7.10 Suppression de clients virtuels

Les clients virtuels désormais inutiles peuvent être supprimés de la base de données Sophos SafeGuard.

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 zone d'action, cliquez avec le bouton droit de la souris sur l'icône en forme de loupe pour rechercher le client virtuel concerné. Les clients virtuels disponibles s'affichent.
4. Validez l'entrée souhaitée, puis cliquez sur **Supprimer le client virtuel** dans la barre d'outils.
5. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

Le client virtuel est alors supprimé de la base de données et ne peut plus être utilisé dans une procédure Challenge/Réponse.

## 22 Récupération du système

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.

Les sections suivantes couvrent les sources d'erreur et les méthodes de récupération envisageables.

### 22.1 Récupération de 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, vous pouvez récupérer l'accès aux données chiffrées en initialisant l'ordinateur via un disque de récupération Windows PE personnalisé pour Sophos SafeGuard.

Conditions préalables :

- L'utilisateur exécutant 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 de connexion de l'authentification au démarrage, sous **Poursuivre l'initialisation à partir de :**, sélectionnez **support externe**. L'ordinateur démarre.

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

## 22.2 MBR (Master Boot Record) corrompu

Pour résoudre les problèmes de MBR corrompu, Sophos SafeGuard propose l'utilitaire BE\_Restore.exe.

Pour une description détaillée de la façon de restaurer un MBR corrompu au moyen de cet utilitaire, reportez-vous au guide des outils SafeGuard.

## 22.3 Volumes

Sophos SafeGuard permet le chiffrement basé sur lecteur. Cela inclut les informations de chiffrement de l'enregistrement constituées du secteur d'initialisation, de la KSA principale et de sauvegarde, ainsi que du secteur d'initialisation original sur chaque lecteur.

Dès que l'une des unités ci-dessous est endommagée, le volume ne peut plus accéder :

- à l'une des deux zones de stockage des clés (KSA) ;
- au MBR original.

### 22.3.1 Secteur d'initialisation

Au cours du processus de chiffrement, le secteur d'initialisation d'un volume est remplacé par le secteur d'initialisation de Sophos SafeGuard.

Le secteur d'initialisation de Sophos SafeGuard contient des informations sur :

- l'emplacement de la KSA principale et de sauvegarde dans les clusters et les secteurs en relation au début de la partition ;
- la taille de la KSA.

Même si le secteur d'initialisation de Sophos SafeGuard est endommagé, les volumes chiffrés restent inaccessibles.

L'utilitaire BE\_Restore peut restaurer le secteur d'initialisation endommagé. Pour une description détaillée de cet utilitaire, reportez-vous au guide des outils SafeGuard.

### 22.3.2 Secteur d'initialisation original

Le secteur d'initialisation original est celui qui est exécuté après le déchiffrement du DEK (clé de chiffrement de données) et après que l'algorithme et la clé ont été chargés dans le pilote du filtre BE.

Si ce secteur d'initialisation est défectueux, Windows n'a pas accès au volume. Normalement le message d'erreur habituel « Le disque n'est pas formaté. Voulez-vous le formater maintenant ? Oui/Non » est affiché.

Néanmoins, Sophos SafeGuard charge le DEK pour ce volume. L'outil utilisé pour réparer le secteur d'initialisation doit être compatible avec le filtre de volume supérieur de Sophos SafeGuard.

## 22.4 Configuration de WinPE pour Sophos SafeGuard

Pour accéder aux lecteurs chiffrés avec le BOOTKEY d'un ordinateur dans un environnement WinPE, Sophos SafeGuard propose Win PE avec les modules de fonction et les pilotes Sophos SafeGuard appropriés. Pour lancer SetupWinPE, entrez la commande suivante :

```
SetupWinPE -pe2 <fichier d'image WinPE>
```

fichier d'image WinPE étant le nom de chemin complet d'un fichier d'image WinPE.

SetupWinPE effectue toutes les modifications nécessaires.

**Remarque:** Notez que, dans ce type d'environnement WinPE, seuls les lecteurs chiffrés avec le BOOTKEY sont accessibles. Les lecteurs chiffrés avec une clé utilisateur sont inaccessibles car les clés ne sont pas disponibles dans cet environnement.

## 23 Empêcher la désinstallation sur les ordinateurs finaux

Pour renforcer la protection des ordinateurs finaux, vous pouvez empêcher la désinstallation locale de Sophos SafeGuard à l'aide d'une stratégie du type **Paramètres spécifiques à la machine**. Pour empêcher la désinstallation locale, définissez l'option **Désinstallation autorisée** de la stratégie **Paramètres spécifiques à la machine** sur **Non** et déployez cette stratégie sur les ordinateurs finaux. Une fois ce type de stratégie appliqué à l'ordinateur final, les tentatives de désinstallation seront annulées et les tentatives non autorisées seront consignées.

**Remarque:** Si vous utilisez une version de démonstration, vous ne devez pas activer ce paramètre de stratégie ni le désactiver avant l'expiration de cette version afin de garantir une désinstallation facile.

### 23.1 Protection anti-sabotage Sophos

La protection anti-sabotage Sophos permet d'éviter la suppression accidentelle de Sophos SafeGuard si l'option **Désinstallation autorisée** dans la stratégie **Paramètres spécifiques à la machine** qui s'applique à l'ordinateur final est définie sur **Oui** ou sur **non configuré**.

**Remarque:** La protection anti-sabotage Sophos ne s'applique qu'aux ordinateurs finaux dotés de Sophos Endpoint Security and Control version 9.5 ou version ultérieure.

Vous pouvez activer la protection anti-sabotage Sophos dans une stratégie du type **Paramètres spécifiques à la machine**. Si l'option **Désinstallation autorisée** de cette stratégie est définie sur **Oui** ou sur **Non configuré**, l'option **Activer la protection anti-sabotage Sophos** devient active et peut être sélectionnée.

Si vous définissez l'option **Activer la protection anti-sabotage Sophos** sur **Oui**, toute tentative de désinstallation sera expressément vérifiée par la protection anti-sabotage Sophos. Si la protection anti-sabotage Sophos n'autorise pas la désinstallation, le processus est annulé.

Si vous définissez l'option **Activer la protection anti-sabotage Sophos** sur **Non**, vous ne pourrez pas empêcher la désinstallation de Sophos SafeGuard.

Si l'option **Activer la protection anti-sabotage Sophos** est définie sur **non configuré**, la valeur par défaut **Oui**, s'applique.

## 24 Mise à jour de Sophos SafeGuard

Une mise à jour de Sophos SafeGuard comprend la mise à jour des composants suivants dans l'ordre indiqué :

1. Base de données de Sophos SafeGuard
2. SafeGuard Policy Editor
3. Ordinateur protégé par Sophos SafeGuard

Sophos SafeGuard 5.50 est directement mis à jour à partir de SafeGuard Enterprise autonome 5.35 ou version ultérieure, sans aucune modification des paramètres précédemment définis. Si vous souhaitez mettre à jour des versions antérieures, vous devez d'abord effectuer une mise à jour vers 5.40.

### 24.1 Mise à jour de la base de données

#### Conditions préalables

- Une base de données Sophos SafeGuard version 5.35 ou ultérieure doit être installée (nom de produit précédent jusqu'à la version 5.40 : SafeGuard Enterprise autonome). Les versions antérieures doivent d'abord être mises à jour vers la version 5.40.
- Les scripts SQL à exécuter doivent être présents sur l'ordinateur hébergeant la base de données.
- .NET Framework 3.0 Service Pack 1 doit être installé pour la mise à jour vers la dernière version.
- Vous devez disposer de droits d'administrateur Windows.
- Sauvegardez la base de données avant de procéder à la mise à jour.

Dans le répertoire Outils de votre logiciel, vous trouverez plusieurs scripts SQL pour la mise à jour de la base de données.

Pour mettre à jour la base de données, procédez comme suit :

1. Fermez SafeGuard Policy Editor.
2. Définissez la base de données correspondante en mode SINGLE\_USER pour exécuter les scripts SQL.

3. La base de données doit être convertie version par version dans la version actuelle. En fonction de la version installée, démarrez les scripts SQL suivants dans cet ordre :
  - a) 5.35 > 5.40: Exécutez MigrateSGN530\_SGN535.sql.
  - b) 5.4x > 5.50 : Exécutez MigrateSGN540\_SGN550.sql.
4. Redéfinissez la base de données correspondante en mode MULTI\_USER.

Les sommes de contrôle cryptographiques de certains tableaux peuvent ne plus être correctes après la mise à jour de la base de données. Des messages d'erreur s'affichent alors au démarrage de SafeGuard Policy Editor. Vous pouvez réparer les tableaux dans la boîte de dialogue correspondante.

La dernière version de la base de données Sophos SafeGuard peut ensuite être utilisée.

## 24.2 Mise à jour de SafeGuard Policy Editor

### Conditions préalables

- La version 5.35 de SafeGuard Policy Editor ou une version ultérieure doit être installée. Les versions antérieures doivent d'abord être mises à jour vers la version 5.40.
- SafeGuard Policy Editor ne doit pas être désinstallé.
- La base de données Sophos SafeGuard a déjà été mise à jour vers la dernière version.
- NET Framework 3.0 Service Pack 1 doit être installé pour la mise à jour vers la dernière version. Vous pouvez le télécharger gratuitement sur le site <http://www.microsoft.com/downloads/en/default.aspx>.
- Vous devez avoir mis à niveau ASP.NET vers la version 2.0.
- Vous devez disposer de droits d'administrateur Windows.

Procédez comme suit :

1. Installez la dernière version du package d'installation SafeGuard Policy Editor. Vous n'avez pas besoin de réexécuter l'assistant de configuration.

SafeGuard Policy Editor a été mis à jour vers la dernière version.

## 24.3 Mise à jour des ordinateurs protégés par Sophos SafeGuard

SafeGuard Policy Editor version 5.5x peut gérer des ordinateurs protégés par Sophos SafeGuard version 5.35 ou ultérieure.

### Conditions préalables

- La version 5.35 ou ultérieure du package d'installation du « client » Sophos SafeGuard doit être installée. Les versions antérieures doivent d'abord être mises à jour vers la version 5.40.
- La base de données Sophos SafeGuard et SafeGuard Policy Editor ont déjà été mis à jour vers la dernière version.
- Vous devez disposer de droits d'administrateur Windows.

Procédez comme suit :

1. Installez le package MSI de préparation, SGxClientPreinstall.msi, qui fournit à l'ordinateur final la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement actuel, et notamment les fichiers DLL requis.

**Remarque :** vous pouvez également installer vcredist\_x86.exe, téléchargeable sur le site suivant : <http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2> ou vérifier que le fichier MSVCR80.dll, version 8.0.50727.4053 se trouve sur l'ordinateur, dans le dossier Windows\WinSxS.

2. Installez la dernière version du package d'installation du client correspondant.

Windows Installer reconnaît les modules déjà installés et n'installe que ces modules. Si l'authentification au démarrage est installée, un noyau POA mis à jour sera également disponible après la mise à jour (stratégies, clés, etc.). Sophos SafeGuard redémarrera automatiquement sur votre ordinateur.

- Si la configuration de Sophos SafeGuard est restée inchangée, vous n'avez pas besoin de créer ni d'installer un nouveau package de configuration Sophos SafeGuard. Toutefois, pour des raisons de sécurité, nous vous recommandons de supprimer tous les packages de configuration obsolètes ou non utilisés.
- Vous ne devez créer et réinstaller un nouveau package de configuration Sophos SafeGuard que si des modifications sont intervenues dans la configuration, par exemple lorsque les paramètres de stratégie ont été modifiés. Si vous créez un nouveau package de configuration Sophos SafeGuard, assurez-vous de supprimer le package obsolète.

**Remarque:** Si vous tentez de remplacer un package de configuration Sophos SafeGuard récent par un plus ancien, l'installation échoue et un message d'erreur s'affiche.

## 24.4 Optimisation de Sophos SafeGuard avec le chiffrement basé sur volume

**Remarque:** Cette description ne s'applique pas à Sophos SafeGuard avec ESDP (Endpoint Security and Data Protection).

Pour faire d'un ordinateur protégé par Sophos SafeGuard, sur lequel est installé le module SafeGuard Data Exchange avec chiffrement basé sur fichier, un client Sophos SafeGuard avec chiffrement basé sur volume et SafeGuard Data Exchange avec chiffrement basé sur fichier, vous devez procéder comme suit. Ces étapes sont nécessaires pour garantir une authentification au démarrage sécurisée et correcte.

1. Désinstallez le package d'installation de SafeGuard Data Exchange (SGNClient\_withoutDE.msi/SGNClient\_withoutDE-x64.msi).
2. Désinstallez le package de configuration de Sophos SafeGuard.
3. Installez le package Sophos SafeGuard Device Encryption avec chiffrement basé sur volume en sélectionnant les fonctions Device Encryption et Data Exchange SGNClient.msi/SGNClient\_x64.msi).
4. Générez et installez un nouveau package de configuration Sophos SafeGuard sur l'ordinateur.

Le fichier de récupération de clé ainsi que les clés locales créées lors de l'installation du package Data Exchange ne seront pas supprimés et resteront disponibles.

## 25 Mise à niveau de Sophos SafeGuard 5.5x vers SafeGuard Enterprise

Vous pouvez facilement effectuer une mise à niveau de Sophos SafeGuard 5.5.x vers la suite SafeGuard Enterprise via la gestion centralisée, afin d'utiliser l'ensemble des fonctions de SafeGuard Enterprise.

Pour ce faire, procédez comme suit :

- SafeGuard Policy Editor doit être mis à niveau vers SafeGuard Management Center.
- Les ordinateurs finaux chiffrés par Sophos SafeGuard doivent être mis à niveau pour devenir des ordinateurs protégés par SafeGuard Enterprise.

### 25.1 Mise à niveau de SafeGuard Policy Editor vers SafeGuard Management Center

Vous pouvez migrer SafeGuard Policy Editor vers SafeGuard Management Center afin d'utiliser les fonctions de gestion complètes, par exemple, la gestion des utilisateurs et des ordinateurs, ainsi que la consignation.

#### Conditions préalables

- La désinstallation de SafeGuard Policy Editor n'est pas nécessaire.
- Avant de procéder à la migration, configurez le serveur SafeGuard Enterprise.

#### Mise à niveau SafeGuard Policy Editor

Pour la mise à niveau, installez simplement le package SGNManagementCenter.msi sur l'ordinateur sur lequel SafeGuard Policy Editor est configuré.

1. Démarrez SGNManagementCenter.msi à partir du dossier d'installation du produit.
2. Cliquez sur **Suivant** dans la fenêtre de bienvenue.
3. Acceptez le contrat de licence.
4. Sélectionnez un chemin d'installation.
5. Confirmez la réussite de l'installation.

6. Si nécessaire, redémarrez votre ordinateur.
7. Configurez SafeGuard Management Center.

SafeGuard Policy Editor a été mis à niveau vers SafeGuard Management Center.

## **25.2 Mise à niveau des configurations Sophos SafeGuard vers SafeGuard Enterprise**

Vous pouvez mettre à niveau la configuration Sophos SafeGuard d'un ordinateur final vers une configuration SafeGuard Enterprise. Les ordinateurs sont ainsi définis dans SafeGuard Management Center en tant qu'objets pouvant être gérés et disposant d'une connexion avec le serveur SafeGuard Enterprise.

**Remarque:** Il n'est pas conseillé d'effectuer la procédure inverse, c'est-à-dire de mettre à niveau la configuration SafeGuard Enterprise vers la configuration antérieure Sophos SafeGuard. Pour ce faire, vous devez réinstaller complètement le logiciel de chiffrement Sophos SafeGuard sur le PC de l'utilisateur.

### **Conditions préalables**

- SafeGuard Policy Editor a été mis à niveau vers SafeGuard Management Center.
- Il n'est pas nécessaire que le logiciel de chiffrement Sophos SafeGuard soit installé sur l'ordinateur final.
- Veillez à sauvegarder l'ordinateur final avant d'effectuer la mise à niveau.
- Vous devez disposer de droits d'administrateur Windows.

### **Mise à niveau des configurations Sophos SafeGuard vers SafeGuard Enterprise.**

Pour effectuer la mise à niveau, il vous suffit de créer un autre package de configuration dans SafeGuard Management Center et de le déployer sur les ordinateurs concernés.

1. Créez le package de configuration pour le client SafeGuard Enterprise géré dans SafeGuard Management Center via **Outils > Outil de package de configuration > Créer un package client Enterprise (géré)**.
2. Attribuez ce package aux ordinateurs Sophos SafeGuard via une stratégie de groupe.  
Lors de la mise à niveau, tous les utilisateurs et certificats sont supprimés et l'authentification au démarrage est désactivée, car l'attribution utilisateur-ordinateur n'est pas mise à niveau. Après la mise à niveau, les ordinateurs finaux ne sont donc plus protégés !

3. Réinitialisez deux fois votre ordinateur après la mise à niveau : la première connexion est toujours effectuée via l'ouverture de session automatique de Windows. De nouvelles clés et de nouveaux certificats sont attribués à l'utilisateur. Par conséquent, il ne peut se connecter à l'authentification au démarrage que lors de la seconde réinitialisation. Les ordinateurs ne sont protégés à nouveau qu'après la seconde réinitialisation.

Sur l'ordinateur final, la configuration Sophos SafeGuard est désormais une configuration SafeGuard Enterprise.

## **26 Mise à niveau de SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x vers Sophos SafeGuard 5.5x**

Pour effectuer la mise à niveau de SafeGuard Easy version 4.5x et de Sophos SafeGuard Disk Encryption version 4.6 vers Sophos SafeGuard 5.5, installez simplement le package d'installation du client SafeGuard Device Encryption sur l'ordinateur.

La mise à niveau directe a été testée. Elle est prise en charge pour SafeGuard Easy 4.5x. La mise à niveau directe doit également fonctionner pour les versions qui se trouvent entre la version 4.3x et la version 4.4x. La mise à niveau des versions antérieures à la version 4.3x n'est pas prise en charge. Ces versions doivent d'abord être mises à niveau vers SafeGuard Easy 4.5.

Le chiffrement des disques durs est conservé ; vous n'avez donc pas besoin de les déchiffrer et de les chiffrer à nouveau. Il n'est pas non plus nécessaire de désinstaller SafeGuard Easy ou Sophos SafeGuard Disk Encryption.

Ce chapitre décrit la mise à niveau vers Sophos SafeGuard, explique les fonctions qui peuvent être migrées et détaille les restrictions.

### **26.1 Conditions préalables**

Les conditions préalables suivantes doivent être remplies :

- La mise à niveau directe a été testée. Elle est prise en charge pour SafeGuard Easy 4.5x. La mise à niveau directe doit également fonctionner pour les versions qui se trouvent entre la version 4.3x et la version 4.4x. La mise à niveau des versions antérieures à la version 4.3x n'est pas prise en charge. Ces versions doivent d'abord être mises à niveau vers SafeGuard Easy 4.5.
- Vous pouvez effectuer une mise à niveau directe vers Sophos SafeGuard Disk Encryption version 4.6x.
- SafeGuard Easy/Sophos SafeGuard Disk Encryption doivent être exécutés sur le système d'exploitation suivant :
  - Windows XP Professionnel Service Pack 2 et 3
- La version 3.01 ou ultérieure de Windows Installer doit être installée.
- Le matériel doit respecter la configuration minimale du système pour Sophos SafeGuard 5.50.

- Si vous utilisez un logiciel spécifique, par exemple un middleware Lenovo, il doit respecter la configuration minimale du système pour Sophos SafeGuard 5.50.
- La mise à niveau peut être effectuée uniquement si les disques durs sont chiffrés à l'aide des algorithmes suivants : AES128, AES256, 3DES et IDEA.

### 26.1.1 Restrictions

La mise à niveau est soumise aux restrictions suivantes :

- Seul le package d'installation de SafeGuard Device Encryption, avec les fonctions standard, peut être installé (SGNClient.msi/SDEClient.msi). Si le module SafeGuard Data Exchange doit également être installé, cette installation doit s'effectuer dans une étape séparée. (Notez que SafeGuard Data Exchange n'est pas pris en charge avec ESDP.)
- Le package d'installation sans chiffrement basé sur volume (SGNClient\_sansDE.msi) n'est pas pris en charge pour la mise à niveau vers Sophos SafeGuard.
- Les installations suivantes ne peuvent pas être mises à niveau vers Sophos SafeGuard. Par ailleurs, n'essayez pas d'installer Sophos SafeGuard.

**Remarque:** Si vous démarrez une mise à niveau dans les cas énoncés ci-dessous, un message d'erreur s'affichera. (numéro d'erreur 5006).

- Installations à double initialisation
- Installations avec commutateur Compaq actif
- Installations Lenovo Computrace
- Disques durs partiellement chiffrés, un secteur d'initialisation chiffré par exemple
- Disques durs avec des partitions masquées
- Disques durs chiffrés avec l'un des algorithmes suivants: XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16
- Scénarios à plusieurs initialisations avec une seconde partition Windows ou Linux
- Les supports amovibles qui ont été chiffrés avec les algorithmes XOR, STEALTH, DES, RIJNDAEL, Blowfish-8 ou Blowfish-16 ne peuvent pas être mis à niveau.

**Remarque:** Des données risquent d'être perdues si un périphérique amovible est chiffré avec les algorithmes XOR, STEALTH, DES, RIJNDAEL, Blowfish-8 ou Blowfish-16. Les données du support amovible ne sont pas accessibles dans Sophos SafeGuard après la mise à niveau.

- Les supports amovibles avec des volumes Super Floppy ne peuvent pas être transformés après la migration.
- Les supports amovibles peuvent être convertis dans un format compatible avec Sophos SafeGuard. Après la conversion, un support de données chiffrées ne peut être lu que par Sophos SafeGuard et uniquement sur l'ordinateur final sur lequel il a été converti.

**Remarque:** Le chiffrement et la migration des supports amovibles ne sont pas pris en charge avec ESDP.

## 26.2 Fonctionnalités mises à niveau

Le tableau ci-dessous indique les fonctionnalités mises à niveau et comment elles sont mappées dans Sophos SafeGuard.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Mise à niveau	Sophos SafeGuard
Disques durs chiffrés	Oui	Les clés des disques durs sont protégées par l'authentification au démarrage de Sophos SafeGuard. Elles ne sont donc jamais exposées. Si le mode de protection à l'initialisation est sélectionné dans SafeGuard Easy, vous devez désinstaller la version actuelle. L'algorithme de chiffrement du disque dur n'est pas modifié par la mise à niveau. En conséquence, l'algorithme réel de ce type de disque dur mis à niveau peut différer de la stratégie générale de Sophos SafeGuard.
Support amovible chiffré (ne concerne pas Sophos SafeGuard Disk Encryption avec ESDP)	Oui	Les supports de données chiffrés, par exemple les cartes mémoire USB, peuvent être convertis au format Sophos SafeGuard. Remarque : après la conversion, un support de données chiffrées ne peut être lu que par SafeGuard Enterprise et uniquement sur l'ordinateur final sur lequel il a été converti. La conversion doit être confirmée cas par cas.
Algorithmes de chiffrement	Dans une certaine mesure	Les algorithmes AES128, AES256, 3DES et IDEA peuvent être migrés. AES-128 et 3-DES ne peuvent néanmoins pas être sélectionnés dans SafeGuard Policy Editor pour les supports à chiffrer.
de SafeGuard Enterprise basée sur le Web	Dans une certaine mesure	La procédure challenge/réponse est conservée.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Mise à niveau	Sophos SafeGuard
Noms d'utilisateur	Non	<p>Étant donné que les noms d'utilisateur Windows sont utilisés dans Sophos SafeGuard, vous n'avez pas besoin de réutiliser les noms d'utilisateur SafeGuard Easy/Sophos SafeGuard Disk Encryption spécifiques. L'enregistrement des ordinateurs mis à niveau s'effectue donc de la même manière que pour une nouvelle installation de Sophos SafeGuard : en attribuant de façon centralisée ou en enregistrant localement les utilisateurs de l'ordinateur.</p> <p><b>Remarque:</b> Après la mise à niveau, le premier utilisateur qui se connecte à Windows est défini comme utilisateur principal au sein de l'authentification au démarrage (sauf s'il est indiqué sur la liste de comptes de service).</p>
Mots de passe utilisateur	Non	<p>Étant donné que les mots de passe utilisateur Windows sont utilisés dans Sophos SafeGuard, vous n'avez pas besoin de réutiliser les mots de passe SafeGuard Easy/Sophos SafeGuard Disk Encryption spécifiques. Les mots de passe SafeGuard Easy/Sophos SafeGuard Disk Encryption ne seront donc pas mis à niveau.</p>
Stratégies, paramètres (par exemple, longueur minimum de mot de passe)	Non	<p>Pour garantir la cohérence de tous les paramètres, aucune mise à niveau automatique n'est exécutée. Les stratégies doivent être réinitialisées dans SafeGuard Policy Editor.</p>
Authentification de préinitialisation	Non	<p>L'authentification de préinitialisation (PBA) est remplacée par l'authentification au démarrage (POA) de Sophos SafeGuard.</p>
Installations sans GINA	Oui	<p>Les installations sans GINA sont mises à niveau vers Sophos SafeGuard avec installation de SGNGINA.</p>
Clés cryptographiques/Cartes à puce	Non	<p>L'authentification des clés cryptographiques/cartes à puce n'est pas prise en charge avec Sophos SafeGuard. Si vous souhaitez utiliser des clés cryptographiques/cartes à puce, nous vous recommandons de migrer vers SafeGuard Enterprise.</p>

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Mise à niveau	Sophos SafeGuard
Connexion avec le lecteur d'empreintes digitales Lenovo	Dans une certaine mesure <b>Remarque:</b> La connexion par empreinte digitale n'est pas disponible avec ESDP.	Vous pouvez continuer à utiliser la connexion par empreinte digitale dans Sophos SafeGuard. Le matériel et le logiciel du lecteur d'empreintes digitales doivent être pris en charge par Sophos SafeGuard et les données d'empreintes digitales de l'utilisateur doivent être réenregistrées. Pour plus d'informations sur la connexion par empreinte digitale, reportez-vous à l'aide de l'utilisateur.

## 26.3 Préparation à la mise à niveau

Vous devez prendre les mesures suivantes avant de démarrer l'installation de Sophos SafeGuard :

- Avant d'effectuer la mise à niveau des ordinateurs finaux, préparez un package de configuration Sophos SafeGuard à l'aide de SafeGuard Policy Editor. Une fois que le logiciel de chiffrement est installé sur les ordinateurs finaux, vous pouvez y déployer le package de configuration. Les stratégies transférées avec le premier package de configuration doivent correspondre à la configuration précédente de l'ordinateur doté de SafeGuard Easy/Sophos SafeGuard Disk Encryption.

Si aucun package de configuration n'est installé avec la mise à niveau, tous les lecteurs qui ont été chiffrés par SafeGuard Easy/Sophos SafeGuard Disk Encryption restent chiffrés.

- Pour réduire le risque de perte de données, nous vous recommandons de créer une sauvegarde complète des ordinateurs que vous souhaitez mettre à niveau.

Réalisez les étapes recommandées avant de procéder à l'installation de Sophos SafeGuard. Utilisez notamment les commandes « chkdsk » et « defrag ». Pour plus d'informations sur les commandes « chkdsk » et « defrag », reportez-vous à notre base de connaissances :

- chkdsk : <http://www.sophos.de/support/knowledgebase/article/107081.html>
- defrag : <http://www.sophos.de/support/knowledgebase/article/109226.html>
- Nous vous recommandons de créer une sauvegarde valide du noyau et de l'enregistrer dans un emplacement toujours accessible (par exemple, un chemin d'accès au réseau). Pour plus d'informations, reportez-vous aux manuels ou aux aides de SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.60, chapitre *Enregistrement du noyau système et création d'un support d'urgence*.

- Pour réduire le risque de perte de données, nous vous recommandons de créer un environnement de test pour la première mise à niveau.
- Si vous effectuez une mise à niveau de versions antérieures de SafeGuard Easy, vous devez d'abord mettre à niveau vers la version 4.50.
- Laissez les ordinateurs allumés tout au long du processus de mise à niveau.
- Le responsable de la sécurité doit conserver les informations d'identification Windows des utilisateurs au cas où les utilisateurs perdraient leur mot de passe Windows après la migration. Cela peut se produire si les utilisateurs se sont connectés auparavant via l'authentification de préinitialisation et se connectent ensuite via la connexion sécurisée Windows (SAL). Les utilisateurs n'utilisent donc jamais leurs informations d'identification Windows.

**Remarque:** Les utilisateurs doivent connaître leur mot de passe de connexion à Windows avant de procéder à la mise à niveau. Cette étape est essentielle car il est impossible de définir un mot de passe Windows après la mise à niveau et l'installation de Sophos SafeGuard. Si les utilisateurs ne le connaissent pas car ils ont utilisé la connexion automatique sécurisée de SafeGuard Easy/Sophos Disk Encryption, ils ne pourront pas se connecter à Sophos SafeGuard, puisque la connexion automatique vers Windows sera refusée. Les utilisateurs ne pourront donc plus se connecter à Sophos SafeGuard. Il existe donc un risque de perte de données car les utilisateurs ne peuvent plus accéder à leurs ordinateurs.

## 26.4 Démarrage de la mise à niveau

**Remarque:** L'installation peut être effectuée sur un système exécutant SafeGuard Easy /Sophos SafeGuard Disk Encryption. Aucun déchiffrement de disques durs ou de volumes chiffrés n'est nécessaire.

**Remarque:** Utilisez le package du client SafeGuard Device Encryption (SGNClient.msi/SDEClient.msi) depuis le dossier d'installation, avec la fonction standard définie. Vous ne pouvez pas utiliser le package client SGNClient\_withoutDE.msi pour effectuer la mise à niveau. Pour une mise à niveau réussie, l'installation doit être exécutée de manière centralisée en mode sans surveillance. L'installation via le dossier de configuration n'est pas recommandée.

Procédez comme suit :

1. Double-cliquez sur le fichier WIZLDR.exe dans le dossier de programme de SafeGuard Easy/Sophos SafeGuard Disk Encryption de l'ordinateur final que vous souhaitez mettre à niveau. Cette opération démarre l'assistant de migration.
2. Dans l'assistant de migration, entrez le mot de passe SYSTEM et confirmez en cliquant sur **Suivant**. Dans **Dossier de destination**, cliquez sur **Suivant** pour confirmer les paramètres par défaut, puis sur **Terminer** pour terminer l'action. Un fichier de configuration de migration SGEMIG.cfg est créé.

3. Dans l'Explorateur Windows, modifiez le nom du fichier SGEMIG.cfg en SGE2SGN.cfg.

**Remarque :** les droits du propriétaire/de l'auteur doivent être définis pour ce fichier et pour le chemin d'accès au dossier dans lequel il est stocké pendant la mise à niveau. Autrement, la mise à niveau risque d'échouer et un message indiquant que le fichier SGE2SGN.cfg est introuvable s'affiche.

4. Entrez la commande « msiexec » dans l'invite de commande pour installer le package de préinstallation Sophos SafeGuard, ainsi que le package d'installation du « client » sur l'ordinateur doté de SafeGuard Easy/Sophos SafeGuard Disk Encryption. Ajoutez le paramètre MIGFILE qui indique le chemin d'accès au fichier de configuration de migration SGE2SGN.cfg :

**Exemple :**

```
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
```

```
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SDEClient.msi
```

```
/L*VX“\Distributionserver\Software\Sophos\SafeGuard\%Nomordinateur%.log“
```

```
MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg
```

- Une fois la mise à niveau effectuée, vous pouvez utiliser Sophos SafeGuard sur l'ordinateur.
- Même si la mise à niveau échoue, SafeGuard Easy/Sophos SafeGuard Disk Encryption restent disponibles sur l'ordinateur. Dans ce cas, Sophos SafeGuard est automatiquement supprimé.

## 26.5 Configuration des ordinateurs finaux mis à niveau

Les ordinateurs finaux sont initialement configurés par des packages de configuration qui permettent, entre autres, d'activer l'authentification au démarrage.

Par conséquent, lors de la mise à niveau, le package de préinstallation et le package d'installation de Sophos SafeGuard, contenant le logiciel de chiffrement, doivent être installés en premier. Ce n'est qu'une fois l'authentification au démarrage activée et l'utilisateur connecté à Windows que l'ordinateur final peut être configuré.

1. Créez le package de configuration initiale dans SafeGuard Policy Editor via **Outils > Outil de package de configuration** et définissez les paramètres de stratégie appropriés.
2. Installez le package de configuration sur les ordinateurs finaux.

**Remarque :** les stratégies transférées avec le premier package de configuration Sophos SafeGuard doivent correspondre à la configuration précédente de l'ordinateur doté de SafeGuard Easy/Sophos SafeGuard Disk Encryption.

## 26.6 Après la mise à niveau

Après une mise à niveau réussie, les éléments suivants sont disponibles dans Sophos SafeGuard après la connexion depuis l'authentification au démarrage :

- les clés et algorithmes des volumes chiffrés ;
- les clés et algorithmes des supports amovibles chiffrés (uniquement applicable lors d'une mise à niveau vers SafeGuard Easy).

Les volumes chiffrés restent inchangés et les clés de chiffrement sont automatiquement converties dans un format compatible avec Sophos SafeGuard.

**Remarque:** Pour déchiffrer le disque dur ou ajouter et supprimer des clés de chiffrement du disque dur, l'utilisateur doit d'abord redémarrer l'ordinateur.

Les stratégies doivent être réinitialisées dans SafeGuard Policy Editor afin de correspondre à la configuration précédente de l'ordinateur doté de SafeGuard Easy/Sophos SafeGuard Disk Encryption.

### 26.6.1 Migration du support amovible

**Remarque:** La migration des supports amovibles ne concerne pas Sophos SafeGuard Disk Encryption avec ESDP.

Le support amovible chiffré reste également inchangé, mais les clés doivent être converties dans un format compatible avec Sophos SafeGuard.

**Remarque:** Par conséquent, après la conversion, un support de données chiffrées ne peut être lu que par SafeGuard Enterprise et uniquement sur l'ordinateur final sur lequel il a été converti pendant la migration.

Pour déchiffrer le support amovible ou ajouter et supprimer des clés de chiffrement du disque dur, l'utilisateur doit d'abord retirer le support de l'ordinateur, puis le réinsérer.

Pour accéder à un support amovible après migration, l'utilisateur doit confirmer explicitement la conversion des clés de chiffrement dans un format compatible avec Sophos SafeGuard. La stratégie appropriée de chiffrement basé sur volume doit être présente sur l'ordinateur avant la conversion, faute de quoi les clés ne sont pas converties.

L'utilisateur est invité à confirmer la conversion pour chaque support amovible. Un message approprié s'affiche.

- Si l'utilisateur confirme la conversion, il bénéficie d'un accès complet aux données migrées.
- Si l'utilisateur refuse la conversion, les données migrées peuvent tout de même être lues et modifiées.

Les supports amovibles récemment ajoutés sont chiffrés, comme sur tout ordinateur Sophos SafeGuard, si la configuration de stratégie appropriée est présente sur l'ordinateur final.

## 27 Support technique

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

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

## **28 Copyright**

Copyright © 1996 - 2010 Sophos Group et Utimaco Safeware AG. 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.