

# Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy Guide de démonstration

Version du produit : 5.60

Date du document : avril 2011



## Table des matières

1	Introduction.....	3
2	Configuration requise.....	4
3	Le package de configuration de démonstration .....	5
4	Installation du logiciel de démonstration.....	5
5	Qu'attendre une fois que le logiciel a été installé.....	5
6	Qu'attendre de la version complète.....	14
7	Mise à niveau vers la version complète.....	17
8	Désinstallation du logiciel de démonstration.....	19
9	Support technique.....	19
10	Mentions légales.....	19

# 1 Introduction

Ce document vous guide tout au long de la version de démonstration du client SafeGuard Disk Encryption. La version de démonstration vous permet de tester le processus de chiffrement de l'intégralité du disque de SafeGuard, y compris l'installation et l'utilisation de l'authentification au démarrage (POA, Power-on Authentication) dans la phase de pré-initialisation.

Il s'agit d'une démonstration destinée aux clients standard pour les produits suivants utilisant le même moteur de client SafeGuard :

## ■ Sophos SafeGuard Disk Encryption (SDE)

Solution de chiffrement du disque complet pour les disques durs locaux. Solution faisant partie intégrante de la licence Sophos Endpoint Security and Data Protection (ESDP). La configuration des stratégies de chiffrement s'effectue à l'aide du SafeGuard Policy Editor. Pour déployer les stratégies sur les ordinateurs d'extrémité, un SafeGuard Policy Editor sous licence est nécessaire.

Pour plus d'informations, voir

<http://www.sophos.fr/products/enterprise/endpoint/security-and-control/>.

## ■ SafeGuard Easy (SGE)

Semblable à SDE, avec en plus, la prise en charge pour l'authentification par empreinte digitale Lenovo, les clés non cryptographiques et les disques durs externes ainsi que la prise en charge d'un environnement runtime afin d'avoir deux installations Windows chiffrées en parallèle sur le même ordinateur. La configuration des stratégies de chiffrement s'effectue à l'aide du SafeGuard Policy Editor. Pour déployer les stratégies sur les ordinateurs d'extrémité, un SafeGuard Policy Editor concédé en licence est nécessaire.

Pour plus d'informations, voir

<http://www.sophos.fr/products/enterprise/encryption/safeguard-easy/>.

Afin d'évaluer le client SafeGuard Disk Encryption, un package de configuration de démonstration avec des paramètres de stratégie préconfigurés est fourni, voir [Le package de configuration de démonstration](#) à la page 5. Ces paramètres de stratégie ne peuvent pas être modifiés dans cette version de démonstration. Le package de configuration de démonstration doit être déployé sur un ordinateur de test avec une installation cliente SDE/SGE 5.60, voir [Installation du logiciel de démonstration](#) à la page 5.

Le package de configuration de démonstration SGNDemoClientConfig.msi est disponible dans le dossier d'installation du produit Sophos SafeGuard Disk Encryption/SafeGuard Easy livré. Ce package est également prêt au téléchargement sur la page <https://secure.sophos.com/products/enterprise/free-trials/safeguard-easy/>.

Si la sécurité vous intéresse au-delà du chiffrement des disques locaux, **SafeGuard Enterprise** est le produit qu'il vous faut. Produit de chiffrement phare de Sophos, SafeGuard Enterprise comporte la gestion centralisée en ligne intégrée avec Active Directory, la création de rapports, l'authentification multiples facteurs (à travers les empreintes digitales Lenovo, les cartes à puce ou les clés cryptographiques) et la gestion étendue des clés pour le chiffrement des supports amovibles et le contrôle des ports. Une version de démonstration distincte est disponible pour SafeGuard Enterprise avec le SafeGuard Management Center et tous les modules. Pour obtenir cette démonstration, veuillez contacter un interlocuteur commercial Sophos. Pour plus

d'informations sur SafeGuard Enterprise, voir <http://www.sophos.fr/products/enterprise/encryption/safeguard-enterprise/>.

Une fois que vous aurez terminé votre évaluation, vous pourrez passer à une version complète de la solution de chiffrement SafeGuard. Vous pouvez mettre à niveau le client de démonstration vers Sophos SafeGuard Disk Encryption, SafeGuard Easy ou SafeGuard Enterprise. Pour obtenir un court aperçu de ce que vous pouvez attendre des versions sous licence, voir [Qu'attendre de la version complète](#) à la page 14.

## 2 Configuration requise

Pour installer SGNDemoClientConfig.msi, le package de configuration de démonstration de SafeGuard Disk Encryption, sur un ordinateur de test, les conditions préalables requises suivantes s'appliquent :

- Le client Sophos SafeGuard Disk Encryption (SDE)/SafeGuard Easy (SGE) est installé avec le chiffrement des périphériques (Device Encryption).
- Le client SDE/SGE ne doit pas avoir été configuré à l'aide d'un package de configuration client créé avec un SafeGuard Policy Editor sous licence.

Pour installer les clients SDE/SGE avec Device Encryption, les configurations système requises suivantes s'appliquent :

- Windows XP SP2 ou version ultérieure (32 bits)
- Windows Vista SP1 (32 bits)
- Windows Vista SP1 (64 bits)
- Windows 7 (32 ou 64 bits)
- Minimum 1 Go de RAM
- Minimum 1 Go d'espace disque
- Lecteur IDE ou SATA (non pas SCSI). Pour plus d'informations sur la compatibilité des matériels, voir <http://www.sophos.fr/support/knowledgebase/article/107781.html>
- Si vous utilisez Lenovo Rescue and Recovery, assurez-vous que la version 4.21 ou une version ultérieure est utilisée.

En cas de doute concernant la plate-forme prise en charge, vous pouvez installer le logiciel. Le processus d'installation vous fera savoir si un problème est rencontré et quittera l'opération.

### Remarque :

Le programme d'installation 64 bits est un téléchargement distinct depuis [sophos.com](http://sophos.com).

Avant d'installer le logiciel, assurez-vous d'avoir les droits d'administrateur pour la machine cliente sur laquelle vous voulez l'installer.

### Remarque :

Ce logiciel est fourni à des fins d'évaluation seulement et ne doit pas être utilisé sur des ordinateurs en production. Pour passer de la démonstration à la version complète, des licences valides sont nécessaires. Pour plus d'informations, voir [Mise à niveau vers la version complète](#) à la page 17.

### 3 Le package de configuration de démonstration

Afin d'évaluer le client SafeGuard Disk Encryption, un package de configuration de démonstration avec des paramètres de stratégie préconfigurés est fourni. Ce package de configuration doit être déployé sur un ordinateur de test avec une installation cliente SDE/SGE 5.60 comprenant Device Encryption, voir [Installation du logiciel de démonstration](#) à la page 5.

Le package de configuration de démonstration SGNDemoClientConfig.msi est disponible dans le dossier d'installation du produit Sophos SafeGuard Disk Encryption/SafeGuard Easy livré. Ce package est également prêt au téléchargement sur la page <https://secure.sophos.com/products/enterprise/free-trials/safeguard-easy/>.

Le package de configuration de démonstration inclut la configuration cliente suivante :

- Tous les lecteurs internes sont chiffrés.
- Tout utilisateur possédant les droits d'administrateur Windows peut désinstaller le logiciel.
- Le mécanisme de récupération Local Self Help est activé et préconfiguré pour la récupération de connexion en cas de mots de passe oubliés.
- La connexion par carte à puce/clé cryptographique est désactivée.
- Tout utilisateur peut importer d'autres utilisateurs SafeGuard pour leur permettre de se connecter à l'authentification au démarrage.

**Remarque :**

Ces paramètres préconfigurés ne peuvent pas être modifiés dans cette version de démonstration.

### 4 Installation du logiciel de démonstration

1. Installez le client Sophos SafeGuard Disk Encryption/SafeGuard Easy avec Device Encryption sur l'ordinateur de test. Pour plus d'informations, reportez-vous au guide de démarrage de Sophos SafeGuard Disk Encryption/SafeGuard Easy.
2. Installez le package de configuration de démonstration SGNDemoClientConfig.msi sur l'ordinateur de test.

Si vous essayez d'installer le package de configuration de démonstration sans avoir installé en premier le client Sophos SafeGuard Disk Encryption/SafeGuard Easy, un message d'erreur apparaît. Un message d'erreur apparaît également si le client a déjà été configuré avec un package de configuration de démonstration créé avec un SafeGuard Policy Editor sous licence.

3. Redémarrez l'ordinateur de test.

### 5 Qu'attendre une fois que le logiciel a été installé

Après que vous avez redémarré l'ordinateur de test, le premier écran que vous apercevez est celui de la mention légale. Il s'agit d'une fonctionnalité de stratégie facultative que vous pouvez activer lorsque vous déployez SafeGuard Disk Encryption sur votre environnement. Dans la version complète du produit, le texte est complètement personnalisable. Pour l'instant, lisez la mention légale et cliquez sur **OK**.



## 5.1 Windows XP

### 5.1.1 Si vous avez déjà un mot de passe Windows défini

1. L'écran de connexion Windows apparaît.
2. Saisissez vos codes d'accès Windows et connectez-vous à Windows.

À ce stade, SafeGuard Disk Encryption synchronise vos codes d'accès Windows avec son système d'authentification au démarrage (POA, Power-on Authentication).

**Remarque :**

SafeGuard Disk Encryption utilise vos codes d'accès Windows pour son authentification au démarrage.

Activez Local Self Help maintenant afin d'avoir un mécanisme de récupération au cas où vous oublieriez vos codes d'accès, [voir Activation de Local Self Help](#) à la page 9.

### 5.1.2 Si vous n'avez pas de mot de passe Windows défini

Si vous n'avez pas configuré de mot de passe Windows, vous êtes maintenant invité à le faire.

1. Un message **Mot de passe non valide** apparaît suivi par la boîte de dialogue **Changer** pour définir un mot de passe.
2. Comme vous n'avez pas de mot de passe, laissez le champ **Ancien mot de passe** vide.
3. Dans le champ **Nouveau mot de passe**, saisissez un mot ou une phrase dont vous vous souviendrez. Répétez-le dans le champ **Confirmation**.

Vous devez vous souvenir du mot de passe afin d'accéder au lecteur chiffré et de démarrer l'ordinateur.

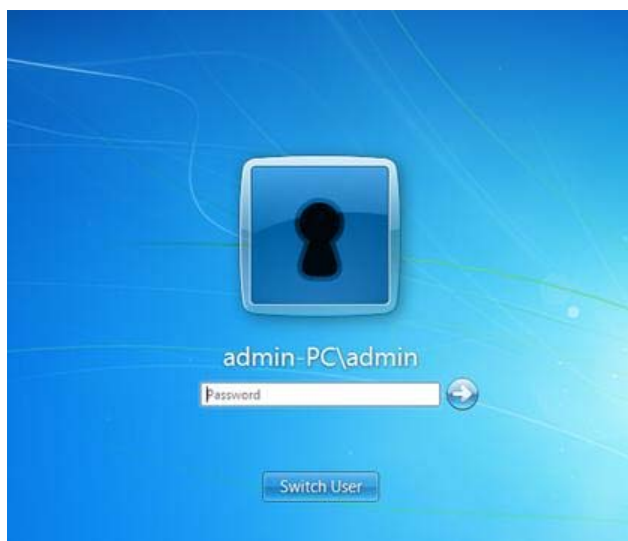
Activez Local Self Help maintenant afin d'avoir un mécanisme de récupération au cas où vous oublieriez vos codes d'accès, [voir Activation de Local Self Help](#) à la page 9.

## 5.2 Windows Vista et Windows 7

Windows Vista et Windows 7 ont un mécanisme d'authentification différent de Windows XP. Si vous utilisez ces systèmes d'exploitation, le comportement suivant est prévisible.

### 5.2.1 Si vous avez déjà un mot de passe Windows défini

1. Après le chargement du système d'exploitation, vous passez directement au bureau, comme auparavant. Cette fois, par contre, la boîte de dialogue apparaît :



2. Saisissez votre mot de passe.

Le bureau se charge et SafeGuard Disk Encryption synchronise vos codes d'accès. Au prochain redémarrage de l'ordinateur, vous pouvez vous connecter à l'authentification au démarrage avec ces codes d'accès.

Si, pour une quelconque raison, vous ne voyez pas l'icône du trou de serrure, sélectionnez **Changer d'utilisateur** et sélectionnez cette icône avant de vous connecter.

Activez Local Self Help maintenant afin d'avoir un mécanisme de récupération au cas où vous oublieriez vos codes d'accès, [voir Activation de Local Self Help](#) à la page 9.

### 5.2.2 Si vous n'avez pas de mot de passe Windows défini

Après avoir sélectionné **OK** dans la boîte de dialogue de la mention légale, Windows se charge et vous vous retrouvez directement sur le bureau comme d'habitude. À cause de la configuration de démonstration, vos codes d'accès Windows doivent être synchronisés avec le mécanisme d'authentification au démarrage.

**Remarque :**

SafeGuard Disk Encryption utilise vos codes d'accès Windows pour son authentification au démarrage.

1. Pour la synchronisation, la boîte de dialogue **Connexion à Sophos SafeGuard** apparaît.
2. Comme vous n'avez pas de mot de passe, cliquez simplement sur **OK**.

Un message **Changement du mot de passe Sophos SafeGuard** apparaît.

Ceci se produit car SafeGuard Disk Encryption n'accepte pas de mot de passe sans caractères.

3. Cliquez sur **OK**.

Vous êtes maintenant invité à changer votre mot de passe. La boîte de dialogue **Changement** pour définir un mot de passe apparaît.

Comme vous n'avez pas de mot de passe, laissez le champ **Ancien mot de passe** vide.

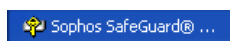
4. Dans le champ **Nouveau mot de passe**, saisissez un mot ou une phrase dont vous vous souviendrez. Répétez-le dans le champ **Confirmation**.

Vous devez vous souvenir du mot de passe afin d'accéder au lecteur chiffré et de démarrer l'ordinateur.

Activez Local Self Help maintenant afin d'avoir un mécanisme de récupération au cas où vous oublieriez vos codes d'accès, [voir Activation de Local Self Help](#) à la page 9.

## 5.3 Processus de chiffrement du disque dur

Lorsque vous vous êtes connecté à Windows, un onglet apparaît dans la barre des tâches :



Cliquez sur cet onglet pour voir les progrès du chiffrement initial.

**Remarque :**

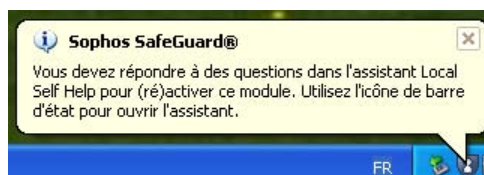
Lors du chiffrement initial, il est possible que vous ayez affaire à un ralentissement des performances du système.



A ce stade, vous pouvez continuer à travailler ou mettre l'ordinateur hors tension. Si vous le mettez hors tension, le processus de chiffrement initial reprendra au redémarrage où il s'est arrêté.

## 5.4 Activation de Local Self Help

Après vous être connecté à votre bureau, un message apparaît :



Il s'agit d'un message d'avertissement pour vous signaler que vous pouvez maintenant activer Local Self Help. Local Self Help vous permet de récupérer vos codes d'accès de connexion oubliés en répondant à des questions auxquelles vous avez préalablement répondu lors de l'activation de Local Self Help.

Pour activer Local Self Help :

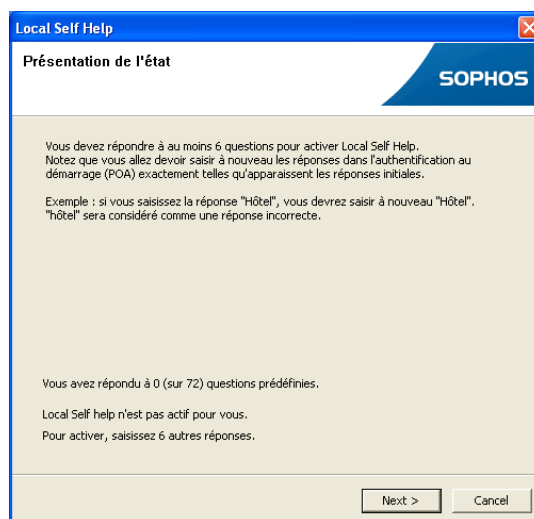
1. Cliquez avec le bouton droit de la souris sur l'icône du bouclier dans votre barre des tâches et sélectionnez **Local Self Help**.



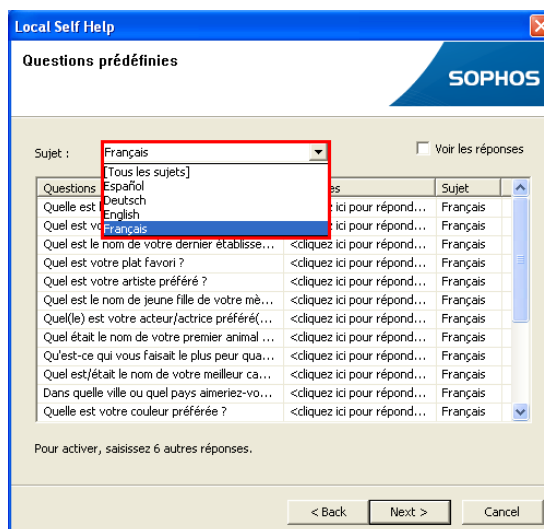
2. Vous êtes invité à saisir de nouveau vos codes d'accès :



3. Saisissez votre nom d'utilisateur et votre mot de passe Windows et cliquez sur **Suivant**.



4. Cette page fournit un statut. Cliquez sur **Suivant**.



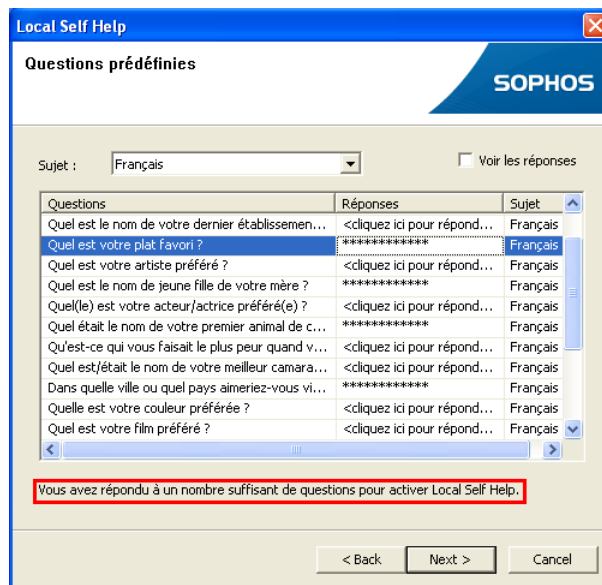
5. Dans la boîte de dialogue **Questions prédéfinies**, sélectionnez une langue dans la liste déroulante **Thème**. Vous pouvez maintenant commencer à répondre aux questions.

N'oubliez pas que les réponses sont sensibles aux majuscules.

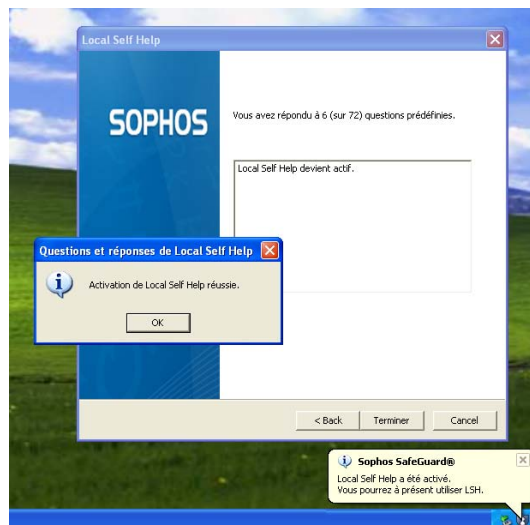
**Remarque :**

Pour le japonais, sa prise en charge appropriée doit être installée sous Windows XP. Sinon, les questions japonaises peuvent ne pas apparaître correctement.

Une fois que vous avez répondu aux six questions, le statut change en bas de la boîte de dialogue.



6. Cliquez sur **Suivant**, puis sur **Terminer**.



Local Self Help est activé.

## 5.5 Au prochain redémarrage

Au prochain redémarrage de l'ordinateur, l'authentification au démarrage est activée. Le premier écran est la mention légale.

1. Cliquez sur **Accepter** pour continuer.

Dans la version complète du produit, la boîte de dialogue de la mention légale et les suivantes sont personnalisées vous permettant ainsi de minimiser l'impact visuel sur vos utilisateurs finaux. Naturellement, dans cette version de démonstration, l'impact est fortement visible et non configurable.



2. Une fois que vous avez passé la mention légale, vous pouvez vous connecter à l'authentification au démarrage. Saisissez vos codes d'accès dans les champs fournis et cliquez sur **OK**.



SafeGuard Disk Encryption valide les codes d'accès, puis permet à Windows de se charger. Tant que vous ne saisissez pas une série valide de codes d'accès, les données présentes sur le lecteur seront accessibles à personne.

À ce stade, il n'y a rien d'autre à faire pour configurer le logiciel. La fonctionnalité exacte disponible dans la version complète dépend de la version du produit (Sophos SafeGuard Disk Encryption (offre groupée ESDP)/SafeGuard Easy ou SafeGuard Enterprise) que vous achetez. Vous pouvez trouver des détails complets sur le site Web de Sophos.

## 5.6 Récupération du mot de passe avec Local Self Help

Si vous avez oublié le mot de passe que vous utilisiez pour accéder à Windows lors de la configuration de SafeGuard Disk Encryption, vous pouvez récupérer votre mot de passe avec Local Self Help. Si vous avez suivi les étapes décrites dans ce guide, vous aurez activé Local Self Help pour la récupération de connexion, [voir Activation de Local Self Help](#) à la page 9.

Pour récupérer votre système si vous avez oublié votre mot de passe :

1. Saisissez votre nom d'utilisateur et sélectionnez **Récupération**.



2. La boîte de dialogue de bienvenue Local Self Help apparaît. Cette boîte de dialogue affiche une brève description des étapes suivantes. Cliquez sur **Suivant**.
3. Il vous est maintenant demandé de répondre à trois des six questions auxquelles vous avez répondu lors de la configuration. Les réponses sont sensibles aux majuscules. Pour continuer, vous devez répondre correctement aux trois. Si une réponse est fautive, SafeGuard considère cela comme une tentative de connexion échouée. Pour des raisons de sécurité, le système n'indique pas quelle question a fait l'objet d'une réponse incorrecte.
4. Après avoir répondu correctement à toutes les questions, vous pouvez cliquer sur la boîte bleue pour que votre mot de passe vous soit rappelé ou simplement cliquer sur **OK** pour être autorisé à accéder à Windows.

## 6 Qu'attendre de la version complète

Les sections suivantes constituent un court aperçu des fonctionnalités et des avantages des versions complètes de Sophos SafeGuard Disk Encryption, SafeGuard Easy et SafeGuard Enterprise.

Si vous souhaitez en savoir plus sur le portefeuille de produits SafeGuard ou commander la version sous licence, veuillez utiliser [sophos.com](http://sophos.com) ou contacter votre interlocuteur commercial local.

### 6.1 Principaux avantages à posséder une version complète sous licence

Cette version de démonstration vous donne un simple aperçu des fonctionnalités de chiffrement du disque complet de la gamme de produits SafeGuard.

La mise à niveau vers une version complète du produit vous permet :

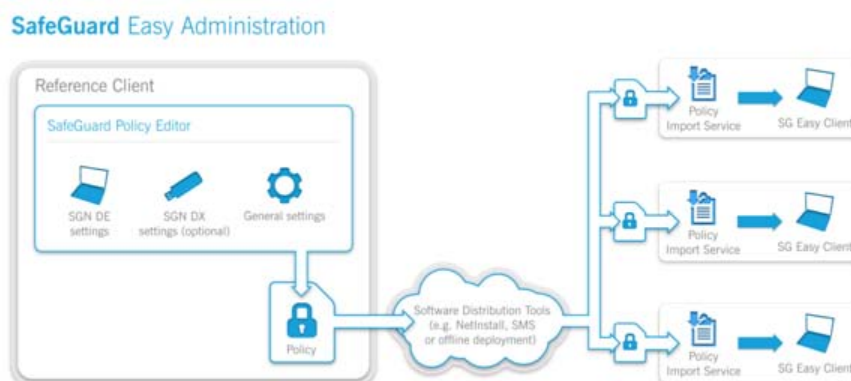
- d'avoir le contrôle complet des stratégies de chiffrement y compris le chiffrement des lecteurs supplémentaires et la configuration du bitmap d'arrière-plan ainsi que les notifications utilisateur.

- d'utiliser des méthodes de récupération supplémentaires en cas de mots de passe oubliés (Challenge/Réponse) et d'être aidé lors de la restauration d'installations de systèmes d'exploitation endommagées même sur des lecteurs chiffrés avec l'image de récupération amorçable pour client virtuel de type Windows PE.
- d'utiliser en option des disques durs à chiffrement automatique compatibles Opal gérés par SafeGuard avec toutes les options de pré-initialisation et de gestion proposées par la solution logicielle SafeGuard.
- d'avoir des options d'authentification par carte à puce, par clé cryptographique et/ou biométrique (SafeGuard Easy ou SafeGuard Enterprise).
- d'avoir la gestion en ligne, notamment la synchronisation Active Directory, une API de gestion, la journalisation centralisée, la création de rapports et la gestion des clés (SafeGuard Enterprise).
- d'ajouter en option des modules fonctionnels supplémentaires pour le chiffrement des supports amovibles y compris les supports optiques (SafeGuard Data Exchange), le contrôle des ports et des périphériques (SafeGuard Configuration Protection) ou la gestion de BitLocker (SafeGuard PartnerConnect) lorsque vous choisissez d'effectuer une mise à niveau vers SafeGuard Enterprise.
- de recevoir des mises à jour de produits et d'obtenir du support technique dans le monde entier de Sophos et des partenaires Sophos.

## 6.2 Variantes de gestion parmi lesquelles choisir

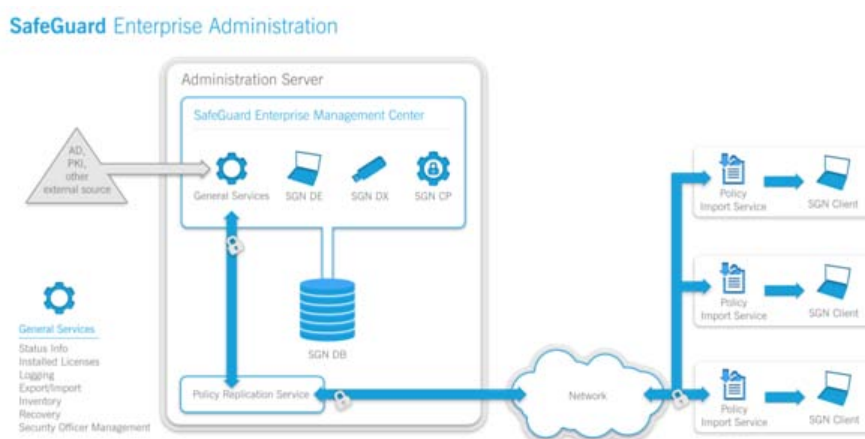
SafeGuard Easy (SGE) et Sophos SafeGuard Disk Encryption (SDE) sont gérés en mode dit autonome, où les stratégies sont créées sur un client de référence et déployées via un mécanisme de déploiement tiers quelconque. Avec cette version de démonstration, vous pouvez évaluer un client SGE/SDE. La mise à niveau vers la version complète nécessite l'installation du SafeGuard Policy Editor et l'importation d'une licence valide. Ensuite, vous pouvez créer un package de configuration sous licence et le déployer sur les clients de démonstration.

Le schéma suivant illustre le mode de gestion SafeGuard Easy/Sophos SafeGuard Disk Encryption :



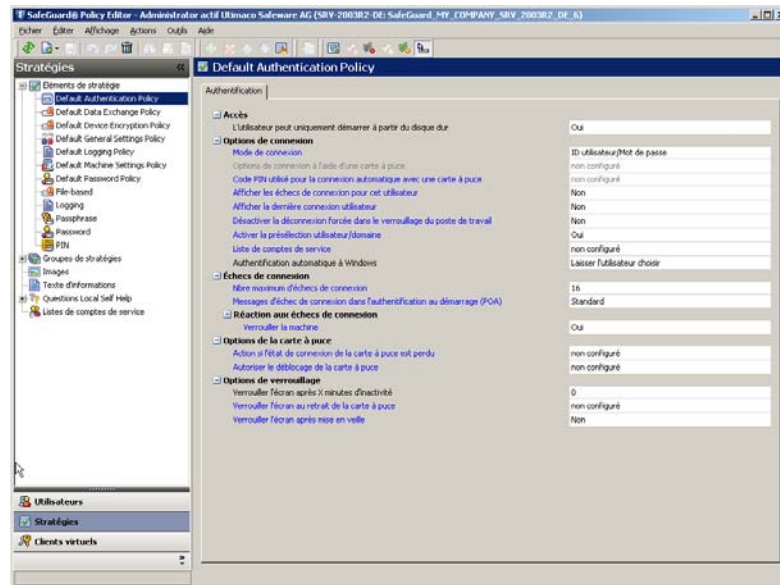
SafeGuard Enterprise est géré en ligne via un mécanisme de service web qui autorise aussi l'importation depuis Active Directory, la journalisation centralisée et la création de rapports de statuts ainsi que d'autres modules de sécurité comme SafeGuard Data Exchange pour le chiffrement des supports amovibles à base de groupes et SafeGuard Configuration Protection pour le contrôle des ports et des périphériques. La mise à niveau depuis cette version de démonstration nécessite l'installation du serveur d'administration SGN et du SafeGuard Management Center et le déploiement d'un package de configuration sous licence pour les clients de démonstration. Ces derniers deviennent alors des clients administrés qui se connectent au serveur SGN.

Le schéma suivant illustre la gestion en ligne SafeGuard Enterprise. En outre, dans un scénario SGN géré, un sous-ensemble des clients peut aussi être géré dans le mode dit hors ligne qui est alors identique au scénario SafeGuard Easy du schéma précédent.



### 6.3 Exemples d'écrans des variantes de gestion

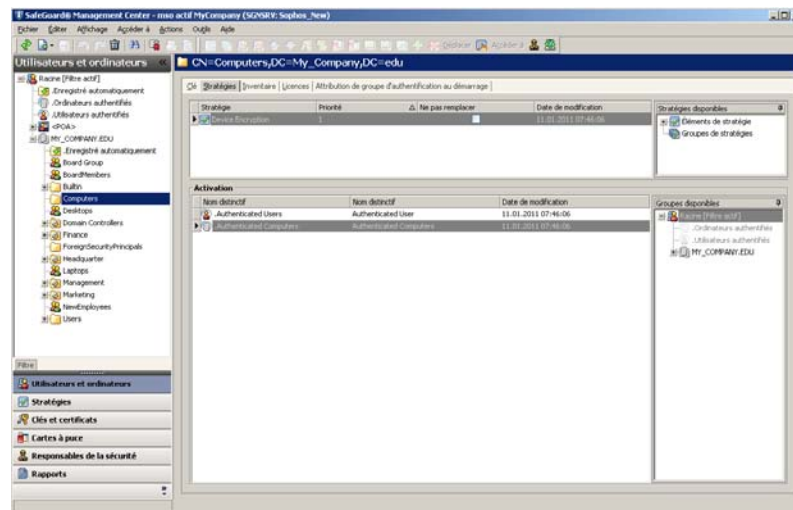
L'écran suivant montre le SafeGuard Policy Editor pour SafeGuard Easy. Le SafeGuard Policy Editor pour Sophos SafeGuard Disk Encryption (SDE) est presque le même. Il a simplement moins d'options de stratégie avancées, par exemple pas de stratégies Data Exchange et pas de stratégies pour la connexion par empreinte digitale.



**Remarque :**

Les éléments d'interface pour Active Directory, la gestion des responsables de la sécurité, les rapports, les clés et les certificats, etc. ne sont pas nécessaires donc absents du mode autonome (SGE/SDE), contrairement au SafeGuard Enterprise Management Center.

La capture d'écran suivante indique la gestion **Utilisateurs et ordinateurs** du SafeGuard Management Center.



## 7 Mise à niveau vers la version complète

Une fois que vous aurez terminé votre évaluation, vous pouvez, si vous le voulez, passer à une version complète de la solution de chiffrement SafeGuard.

Vous pouvez mettre à niveau le client de démonstration vers

- Sophos SafeGuard Disk Encryption/SafeGuard Easy, voir [Mise à niveau vers un client Sophos SafeGuard](#) à la page 18.
- SafeGuard Enterprise, voir [Mise à niveau vers un client SafeGuard Enterprise](#) à la page 18.

Pour la mise à niveau, vous avez besoin de licences valides. Pour les obtenir, veuillez contacter votre interlocuteur commercial local.

Pour mettre à niveau, créez un nouveau package de configuration avec l'outil de gestion sous licence correspondant et déployez-le sur l'ordinateur.

**Remarque :**

Il n'est pas nécessaire de supprimer la version de démonstration.

**Remarque :**

Vous ne pouvez pas mettre à niveau un client de démonstration vers une version complète plus récente. Vous devez tout d'abord mettre à niveau le client de démonstration vers un client sous licence de la même version, puis le mettre à jour vers la nouvelle version.

## 7.1 Mise à niveau vers un client Sophos SafeGuard

1. Assurez-vous qu'un SafeGuard Policy Editor sous licence est disponible.

Pour obtenir des informations détaillées sur comment installer et configurer un SafeGuard Policy Editor sous licence, reportez-vous au guide de démarrage de Sophos SafeGuard Disk Encryption/SafeGuard Easy.

2. Dans le SafeGuard Policy Editor, créez un nouveau package de configuration.

Pour obtenir des informations détaillées, reportez-vous au guide de démarrage de Sophos SafeGuard Disk Encryption/SafeGuard Easy.

3. Déployez le nouveau package de configuration sur l'ordinateur de test.

Après avoir effectué une mise à niveau vers la version complète, une sauvegarde de clé automatique est initialisée. Les utilisateurs importés lors de l'évaluation ne sont pas supprimés et auront quand même accès à l'ordinateur. Pour plus d'informations, reportez-vous à l'aide de l'administrateur Sophos SafeGuard Disk Encryption/SafeGuard Easy et l'aide utilisateur.

## 7.2 Mise à niveau vers un client SafeGuard Enterprise

1. Assurez-vous qu'un SafeGuard Management Center sous licence est disponible.

Pour obtenir des informations détaillées sur comment installer et configurer SafeGuard Enterprise et un SafeGuard Management Center sous licence, reportez-vous au manuel d'installation de SafeGuard Enterprise.

2. Dans le SafeGuard Management Center, créez un nouveau package de configuration.

Pour obtenir des informations détaillées, reportez-vous au manuel d'installation de SafeGuard Enterprise.

3. Déployez le nouveau package de configuration sur l'ordinateur de test.

Après avoir effectué une mise à niveau vers la version complète, une sauvegarde de clé automatique est initialisée. L'authentification au démarrage repasse à la connexion automatique et le premier utilisateur Windows qui se connecte devient le propriétaire de la machine. Pour plus d'informations, reportez-vous à l'aide de l'administrateur SafeGuard Enterprise et l'aide utilisateur.

## 8 Désinstallation du logiciel de démonstration

Si vous choisissez de ne pas mettre à niveau la configuration du client vers une version complète, vous pouvez supprimer le logiciel de démonstration depuis l'ordinateur de test comme suit.

### Remarque :

Pour mettre à niveau vers une version complète, il n'est pas nécessaire de désinstaller en premier le logiciel de démonstration, voir [Mise à niveau vers la version complète](#) à la page 17. Si vous souhaitez en savoir plus sur le portefeuille de produits SafeGuard ou commander la version sous licence, veuillez utiliser [sophos.com](http://sophos.com) ou contacter votre interlocuteur commercial local.

1. Ouvrez **Ajout/Suppression de programmes**.
2. Supprimez "Sophos SafeGuard 5.60 Client Configuration", puis supprimez "Sophos SafeGuard 5.60 Client".

Lorsque vous supprimez le client, vous voyez le lecteur commencer à déchiffrer. Nous vous conseillons de désinstaller les deux packages et de permettre au lecteur de terminer le déchiffrement avant de redémarrer.

Si le système fait l'objet d'un redémarrage au cours de ce processus, la désinstallation est annulée, mais le déchiffrement continue lorsque le système est redémarré. Une fois que le déchiffrement est terminé, vous pouvez réinitialiser la suppression du client de chiffrement SafeGuard.

## 9 Support technique

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

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

## 10 Mentions légales

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

Sophos est une marque déposée de Sophos Limited, Sophos Group et Utimaco Safeware AG, selon le cas. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées de leurs propriétaires respectifs.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

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