

# Sophos SafeGuard® Disk Encryption 4.60

## Aide

Date du document: Juin 2009

# Sommaire

|    |  |     |
|----|--|-----|
| 1  | Aperçu .....   | 4   |
| 2  | Mise en route.....   | 12  |
| 3  | Installation locale .....  | 14  |
| 4  | Installation centrale .....  | 22  |
| 5  | Résolution des problème d'une installation avec SGEInteg.....                                    | 29  |
| 6  | Désinstallation.....   | 30  |
| 7  | Démarrage du système et ouverture de session.....  | 34  |
| 8  | Aperçu de l'administration.....  | 40  |
| 9  | Fonction Administration.....   | 42  |
| 10 | L'assistant de configuration pour le déploiement.....  | 45  |
| 11 | Modification des paramètres de registre fréquemment utilisés via le modèle d'administration .... | 58  |
| 12 | Authentification avant l'amorçage (PBA) .....  | 61  |
| 13 | Chiffrement .....  | 65  |
| 14 | Création de profils utilisateur .....  | 70  |
| 15 | Paramètres du mot de passe .....   | 79  |
| 16 | Configuration du mot de passe Windows .....  | 90  |
| 17 | Sophos SafeGuard Disk Encryption Verrouillage du poste.....                                      | 101 |
| 18 | Activation à distance (Wake-On-LAN) sécurisée .....  | 104 |

|    |  |     |
|----|--|-----|
| 19 | Mise en veille prolongée .....   | 107 |
| 20 | Certification FIPS 140-2 (Level 1).....  | 110 |
| 21 | Sophos SafeGuard Disk Encryption et Lenovo Thinkvantage - Rescue and Recovery..... | 112 |
| 22 | Compatibilité avec le logiciel Absolute Computrace .....                           | 121 |
| 23 | Maintenance à distance (Requête/Réponse) .....                                     | 122 |
| 24 | Sauvegarde du noyau du système et création de supports de secours .....            | 130 |
| 25 | Affichage de l'état système de Sophos SafeGuard Disk Encryption .....              | 146 |
| 26 | Audit .....  | 148 |
| 27 | Erreurs .....  | 150 |
| 28 | Support technique.....   | 170 |
| 29 | Copyright.....   | 171 |

# 1 Aperçu

Les ordinateurs individuels contiennent fréquemment des données spécifiques à des personnes, des informations confidentielles relatives à une entreprise ou d'autres données sensibles.

Le vol d'ordinateurs portables, par exemple, est un risque qu'il ne faut pas sous-estimer. Les informations ultra-confidentielles de clients sur l'ordinateur portable de type Notebook d'un collaborateur du service de distribution pourraient, par exemple, tomber entre les mains d'un concurrent et être dommageables à l'entreprise.

Sophos SafeGuard Disk Encryption permet de se protéger contre de tels risques sans avoir à investir un temps considérable dans l'implémentation de mesures de sécurité.

Comment Sophos SafeGuard Disk Encryption protège-t-il les postes de travail contre les interventions non autorisées ? Les fonctions de sécurité principales du programme sont le chiffrement de données et l'authentification avant amorçage pour la protection contre l'accès non autorisé aux ordinateurs ou ordinateurs portables.

Les principaux avantages de Sophos SafeGuard Disk Encryption sont les suivants :

- Sauvegarde simple mais efficace de la confidentialité des données enregistrées ;
- Implémentation rapide du programme ;
- Très grande convivialité.
- Sur la base d'une technologie de chiffrement en tête de marché le produit est compatible avec FIPS 140 certifié.

La table suivante offre un aperçu de Sophos SafeGuard Disk Encryption. Pour augmenter Sophos SafeGuard Disk Encryption nous conseillons d'utiliser SafeGuard Enterprise.

| Sophos SafeGuard Disk Encryption (SDE)   | SafeGuard Enterprise  |
|--|---|
| PME (< 1 000 utilisateurs)   | Moyennes et grandes entreprises (> 1 000 utilisateurs)  |
| Chiffrement total des secteurs du disque uniquement<br>Chiffrement de supports amovibles via SafeGuard PrivateCrypto | Chiffrement total des secteurs du disque, gestion centralisée et exécutable du chiffrement total du disque, chiffrement de supports de stockage amovibles, chiffrement de fichiers et de dossiers |
| Journalisation et établissement de rapports sur l'état de chiffrement via Sophos Compliance and Control              | Piste d'audit complète assurée par des rapports et des fichiers journaux détaillés : garantit la conformité   |

| Sophos SafeGuard Disk Encryption (SDE) | SafeGuard Enterprise  |
|--|---|
| Prise en charge étendue de clavier     | Prise en charge étendue de clavier; Prise en charge étendue des cartes à puce/clés cryptographiques, dispositif biométrique (empreintes Lenovo) |

## 1.1 Fonctions de sécurité centrales

### Chiffrement

Sophos SafeGuard Disk Encryption protège de façon simple et efficace la confidentialité des données lors de leur enregistrement sur disque dur n procédant au chiffrement en ligne. « En ligne », dans ce contexte, signifie que les données sont déchiffrées lors de leur chargement dans la mémoire de travail, puis chiffrées à nouveau lors de leur enregistrement. La clé est déterminée à chaque fois à partir du mot de passe Sophos SafeGuard Disk Encryption de l'utilisateur au moment du démarrage.

Le contenu des disques durs est complètement chiffré par Sophos SafeGuard Disk Encryption encrypts the entire contents of hard disks. Pour le chiffrement, l'algorithme AES-256 est disponible.

Pour disposer d'une solution de sécurité des données encore plus large, nous recommandons la solution de sécurité des données SafeGuard Enterprise, structurée de façon modulaire. SafeGuard Enterprise prend notamment en charge l'administration centrale et le chiffrement de supports amovibles.

### Contrôle d'accès avec l'authentification avant amorçage (PBA)

L'authentification avant amorçage (PBA) est une fonction de sécurité centrale de Sophos SafeGuard Disk Encryption. La PBA n'autorise que l'ouverture de session par les utilisateurs Sophos SafeGuard Disk Encryption enregistrés sur le système.



Lors de la tentative de démarrage d'un poste de travail dont le disque dur est chiffré depuis un support extérieur (par ex. disquette système, CD-ROM ou autre disque dur), le disque dur reste inaccessible. Ceci signifie que le démarrage du système est possible, mais que les données chiffrées sur le disque dur ne peuvent pas être lues.

## 1.2 Autres mécanismes de protection

### Règles de mots de passe

Sophos SafeGuard Disk Encryption offre différentes options d'implémentation de règles de mot de passe dans le module PBA, telles qu'une liste configurable de mots de passe interdits, des règles étendues pour les caractères spéciaux, des codes utilisateur, etc., ce qui permet de s'adapter facilement aux directives de l'entreprise.

### Audit dans la PBA et le système d'exploitation

Sophos SafeGuard Disk Encryption conserve également une trace des problèmes affectant la sécurité, tels que les échecs de connexion, lors de la phase de préparation du démarrage. Ces entrées sont ensuite insérées dans le journal des événements de Windows afin d'être évaluées.

### Administration locale

L'administration de SafeGuard Lite permet de changer les paramètres d'authentification et de chiffrement de votre ordinateur. En tant qu'administrateur, vous pouvez configurer des profils utilisateur.

### Ouverture de session automatique sécurisée (SAL)

L'ouverture de session automatique est une fonction confortable pour la procédure d'ouverture de session. Un utilisateur entre une fois ses données Windows. Pour les autres ouvertures de

session, la connexion à Windows s'effectue automatiquement et l'utilisateur n'a plus à s'authentifier qu'avec les données d'utilisateur Sophos SafeGuard Disk Encryption dans la PBA.

### **Support Wake On LAN sécurisé**

L'authentification avant amorçage de Sophos SafeGuard Disk Encryption offre une protection optimale contre les attaques des pirates informatiques. Cependant, pour garantir le plus sûrement possible la distribution de logiciels via l'activation à distance quand le chiffrement de disque dur est actif, Sophos SafeGuard Disk Encryption propose de nouvelles fonctions.

### **Télé-assistance sûre (Requête/Réponse)**

Le personnel d'assistance aide les utilisateurs quand ceux-ci ont oublié leur mot de passe. La procédure Requête/Réponse est sûre et idéale pour les utilisateurs d'ordinateurs portables, car ces derniers ne requièrent pas de connexion en ligne directe avec le service d'assistance.

### **Installation avec Windows Installer**

L'installation entièrement basée sur le mode Windows Installer (MSI) standard peut être répartie et exécutée de façon simple et effective sur les réseaux Windows.

### **Personnalisation de l'authentification avant amorçage pour demandes juridiques**

Il est notamment possible d'afficher une remarque relative aux droits d'accès, au propriétaire de l'appareil, aux demandes juridiques, etc., prescrits par l'administrateur.

### **Démarrage d'urgence possible à partir d'un CD, une clé USB ou d'une disquette**

Sophos SafeGuard Disk Encryption prend en charge autant que les CD, les disquettes et les clés USB comme supports de secours. Les supports de démarrage sont pris en charge sous MS DOS et Windows PE.

### **Connexion Windows standard sans boîte de dialogue Sophos SafeGuard**

Les clients peuvent personnaliser la connexion par défaut et utiliser une boîte de dialogue de connexion de type Sophos SafeGuard et non plus Windows.

### **Prise en charge de la veille prolongée (Suspendre sur disque)**

La veille prolongée est particulièrement utile pour les utilisateurs de périphériques mobiles qui contournent la procédure de démarrage en mettant leur session sur « pause », puis en la « restaurant », dans la mesure où ces options sont disponibles sur la plupart des systèmes d'exploitation.

Sophos SafeGuard Disk Encryption permet d'utiliser le mode Veille prolongée. La sécurité reste ainsi garantie à tout moment, la consommation est réduite et du temps est gagnée par rapport à la procédure d'amorçage usuelle.

### **Compatibilité avec le logiciel Absolute Computrace**

Computrace permet de rouvrir une session sur un ordinateur volé sur le réseau et de dévoiler son emplacement. Sophos SafeGuard Disk Encryption est compatible avec Computrace. Grâce à la compatibilité, ceci fonctionne à présent aussi avec les disques durs chiffrés.

### **Prise en charge des technologies Thinkvantage de Lenovo - Rescue and Recovery 4.20**

Sophos SafeGuard Disk Encryption, est compatible avec Rescue et Recovery (RnR) de Lenovo.

Sophos SafeGuard Disk Encryption est compatible avec Rescue and Recovery de Lenovo. Ceci permet aux utilisateurs de bénéficier de cette méthode efficace de sauvegarde et de restauration de Lenovo, même si la partition du système d'exploitation est chiffrée avec Sophos SafeGuard Disk Encryption. Sophos SafeGuard Disk Encryption offre ici une fonctionnalité unique en son genre parmi les produits de chiffrement de disques durs. Les sauvegardes de systèmes Sophos SafeGuard Disk Encryption chiffrés peuvent être stockées sur tous les lecteurs proposés par RnR. En cas d'urgence, il est donc possible de restaurer un système endommagé en chargeant une sauvegarde d'un CD/DVD, d'un lecteur réseau, d'un deuxième disque dur interne, ainsi que d'un disque dur ou d'une clé USB.

### **Certification suivant FIPS 140-2 Level 1**

Sophos SafeGuard Disk Encryption satisfait aux directives de la certification FIPS 140-2 Level 1 (FIPS=Federal Information Processing Standard) du National Institute of Standards and Technology américain (NIST). Le NIST définit les critères de sécurité prescrits par le gouvernement des États-unis d'Amérique pour les produits chiffrés.

## **1.3 Configuration système requise**

### **Systèmes d'exploitation**

La configuration minimale requise pour les versions 32 bits des systèmes d'exploitation pris en charge est la suivante (Services Packs testés entre parenthèses) :

- Windows 2000 Professional Service Pack 4 (SP4)
- Windows XP Édition Familiale Service Pack 2 (SP 3)
- Windows XP Édition Professionnelle Service Pack 2 (SP 3)

Les Service Packs actuels sont conseillés.

### **Migration des Service Packs Windows**

Une migration d'un Service Pack est également possible quand Sophos SafeGuard Disk Encryption est installé. Une migration de SP2 vers SP3, par exemple, est également possible quand Sophos SafeGuard Disk Encryption est installé.

### **Systèmes de fichiers pris en charge**

- FAT-32
- NTFS

### **Supports mémoire pris en charge :**

- Disques durs (IDE, SCSI, ATA série, Firewire, USB) ;
- RAID 0 (RAID 0 matériel).  
Sophos SafeGuard Disk Encryption ne prend pas en charge :
  - d'autres classes RAID
  - RAID 0 (logiciel).

### **Supports processeurs**

- AMD
- Intel
- Multiprocesseurs / Hyperthreading

Nous recommandons d'utiliser processeurs AMD ou Intel.

### **Spécifications matérielles**

- **Emplacement mémoire sur le disque dur**  
Selon la méthode d'installation choisie, Sophos SafeGuard Disk Encryption requiert un minimum de 25 Mo d'espace disque. Sophos SafeGuard Disk Encryption requiert les mêmes spécifications que le système d'exploitation.  
  
Bien que Sophos SafeGuard Disk Encryption fonctionne sans problème sur le système décrit, le chiffrement a son prix. Il est donc recommandé d'utiliser un matériel possédant une configuration supérieure au requis.
- **Nombre de disques durs**  
Sophos SafeGuard Disk Encryption prend en charge au maximum 4 disques durs avec au plus 8 partitions par disque dur. Un avertissement est affiché quand un type de partition non pris en charge est décelé.

## **1.4 Documentation**

Sophos SafeGuard Disk Encryption est livré avec un startup guide y avec la présente aide.

## 1.5 Remarques générales

Lors d'une utilisation normale, tenez compte des points suivants :

- La fonction « Changement rapide d'utilisateur » de Windows XP n'est pas prise en charge par Sophos SafeGuard Disk Encryption. Après l'installation de Sophos SafeGuard Disk Encryption, l'écran de bienvenue est automatiquement désactivé.
- Quand l'ordinateur est intégré dans un réseau LAN point à point, certaines parties des disques durs ne doivent pas être affectées à d'autres utilisateurs de ce réseau.
- Le chiffrement et le déchiffrement des disques durs sont automatiquement protégés contre les pannes de courant ou autres perturbations. Lors de la remise en service de l'alimentation électrique, l'opération en cours se poursuit au bon endroit sans intervention de l'utilisateur.

**Remarque :** Le premier chiffrement de disques durs connectables à chaud ne doit pas être interrompu.

Pour plus d'informations aux disques durs connectables à chaud, voir [Configuration du chiffrement](#) sur page 66.

- Si vous faites une pause, activez l'écran de veille de Windows (bouton de **verrouillage de la station de travail**). Si vous devez vous absenter pendant une période prolongée, arrêtez le PC.
- Quand la configuration système conseillée est correcte, l'accès logique aux disques durs est impossible après l'amorçage depuis une disquette. Afin de mieux protéger votre système contre les virus de type cheval de Troie qui pourraient être utilisés pour détecter un mot de passe Sophos SafeGuard Disk Encryption, employez un verrou mécanique ou toute autre mesure interne permettant d'empêcher le démarrage de votre système avec une disquette.

## 1.6 Remarques relatives à la licence

Toute reproduction non autorisée du manuel et du logiciel Sophos SafeGuard Disk Encryption fera l'objet de poursuites judiciaires. Sophos SafeGuard Disk Encryption ne doit être installé que sur un seul ordinateur.

L'utilisation abusive de la copie de sauvegarde pour une installation sur plusieurs ordinateurs est contraire aux dispositions des réglementations régissant les licences et fait l'objet de sanctions pénales. Si vous souhaitez protéger plusieurs ordinateurs, une licence doit être acquise pour chacun d'entre eux.

Les termes et conditions du contrat de licence du logiciel sont applicables.

Droits de brevet d'Ascom Tech Ltd. pour l'Union Européenne, le Japon et les États-Unis. IDEA est une marque commerciale d'Ascom Tech Ltd.

Remerciements:

Un merci tout particulier au Dr. Brian Gladman dont nous avons utilisé l'implémentation AES comme base de notre pilote de chiffrement AES.

## 2 Mise en route

Ce chapitre présente les conditions indispensables à une installation réussie de Sophos SafeGuard Disk Encryption.

### 2.1 Préparation de l'installation

Pour une utilisation la plus efficace possible, certaines mesures de prévention doivent être prises avant l'installation. Veuillez lire avec attention la liste ci-dessous et vous assurer que vous en avez compris tous les points.

#### Préparations générales

- Fermez toutes les applications ouvertes.
- Assurez-vous que l'espace mémoire sur la disque dur est suffisant.

#### Préparations pour le chiffrement

- Avant l'installation de Sophos SafeGuard Disk Encryption, il est conseillé de réaliser une sauvegarde complète de vos supports de données.
- Tous les disques durs qui doivent être chiffrés doivent être connectés à l'ordinateur et activés à l'installation de Sophos SafeGuard Disk Encryption.
- Vérifiez les défauts éventuels de votre ou de vos disques durs avec la commande suivante.  
`chkdsk %systemdrive% /F /V /L /X`

Dans certains cas vous êtes invité à redémarrer l'ordinateur et utiliser `chkdsk` encore une fois.

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

<http://www.sophos.com/support/knowledgebase/article/57554.html>

- Quand la partition d'amorçage est convertie de FAT en NTFS, alors que le système n'a pas encore été réinitialisé avant l'amorçage, Sophos SafeGuard Disk Encryption ne doit pas être installé. Il est possible ce faisant que l'installation ne soit pas terminée, étant donné que le système de fichiers est encore de type FAT au moment de l'installation, alors que NTFS a été détecté au moment de l'activation. Dans ce cas, un redémarrage est nécessaire avant d'installer Sophos SafeGuard Disk Encryption.

### 2.2 Interface utilisateur en plusieurs langues

Si vous lancez l'installation avec « `setup.exe` », la langue de l'interface utilisateur pendant et après l'installation de Sophos SafeGuard Disk Encryption correspond à celle qui est définie dans la section Paramètres régionaux du Panneau de configuration. Sophos SafeGuard Disk Encryption prend en charge l'Anglais, l'Allemand et le Français. Si, par exemple, « Français » est le paramètre

actif, l'interface utilisateur s'affiche en Français. Vous disposez également d'une interface en Anglais (États-Unis) et en Allemand.

L'aide en ligne est toujours disponible dans la langue sélectionnée au moment de l'installation. La modification des paramètres régionaux et linguistiques n'influe en rien sur la langue de l'aide en ligne.

**Si l'installation est lancée via le fichier de « msi »,** la langue de l'interface utilisateur est toujours l'Anglais. Pour activer d'autres langues (Français ou Allemand), des fichiers « Transforms » doivent être exécutés. Le module Windows Installer utilise les fichiers de transformation pour commuter automatiquement le logiciel d'installation sur la nouvelle langue. Les fichiers de transformation suivants sont actuellement disponibles :

`SDE_g.mst` (pour l'Allemand) et `SDE_f.mst` (pour le Français).

Afin d'obtenir des textes transformés pendant l'installation, exécutez la commande suivante :

```
msiexec /I <MSI package> TRANSFORMS=<fichier transform>
```

Une installation en Français requiert l'exécution de cette ligne de commande :

```
msiexec /I SDE.msi TRANSFORMS=SDE_f.mst
```

Veillez noter que le paramètre TRANSFORMS doit toujours être écrit en majuscules.

Pour simplifier l'installation, vous pouvez utiliser le fichier `setup.exe`, qui sélectionne automatiquement la langue de l'Assistant d'installation et exécute `SDE.msi`. `SDE.msi` utilise le fichier `Setup.ini` dans lequel les paramètres suivants peuvent être définis, à condition qu'ils soient présents dans la syntaxe `CmdLine={paramètre1, paramètre2,..}`.

**Remarque:** Quand utiliser `setup.exe` le paramètre TRANSFORMS n'est pas pris en charge.

## 3 Installation locale

Dans le cas d'une installation locale, Sophos SafeGuard Disk Encryption est installé sur un ordinateur autonome. Les étapes suivantes expliquent comment on procède à une installation locale.

L'utilisateur qui doit installer Sophos SafeGuard Disk Encryption doit se connecter avec des **droits d'administration de Windows**, car il doit accéder au disque dur pour installer des pilotes et des services système, qui nécessitent également des droits de niveau administrateur.

### 3.1 Installation de Sophos SafeGuard Disk Encryption

Suivez les étapes ci-dessous :

1. Ouvrez une session en tant qu'administrateur.
2. A l'aide de l'adresse Web et des codes d'accès de téléchargement fournis par votre administrateur système, rendez-vous sur le site Web de Sophos et téléchargez le programme d'installation autonome de votre version de Windows.
3. Recherchez le programme d'installation dans le dossier où il a été téléchargé. Cliquez deux fois sur le programme d'installation. Dans la fenêtre du programme d'installation, cliquez sur **Installer** pour extraire le contenu du programme d'installation sur votre ordinateur et lancer l'assistant d'installation. Les instructions du **Programme d'installation Sophos SafeGuard Disk Encryption** vous guident à travers les étapes nécessaires.
4. Acceptez les propositions par défaut dans les boîtes de dialogue suivantes.
5. Dans **Sélectionner le type d'installation**, choisissez le type d'installation que vous souhaitez exécuter et cliquez sur **Suivant**. Les types d'installation suivants sont disponibles .



■ **Installation distribuée sur les ordinateurs du réseau**

Les outils d'administration permettant d'automatiser l'installation de Sophos SafeGuard Disk Encryption seront installés sur les ordinateurs de votre réseau.

■ **Installation chiffrée sur cet ordinateur**

Installe Sophos SafeGuard Disk Encryption avec l'authentification avant amorçage activée, ouverture de session automatique sécurisée (SAL) et le chiffrement de la partition C: par défaut. L'ordinateur sera soumis à la fonction de chiffrement et vous devrez le redémarrer après l'installation.

■ **Installation distribuée avec chiffrement**

Installe les outils d'administration et Sophos SafeGuard Disk Encryption avec l'authentification avant amorçage, ouverture de session automatique sécurisée (SAL) et le chiffrement de la partition C: par défaut. L'ordinateur sera soumis à la fonction de chiffrement et vous devrez le redémarrer après l'installation.

■ **Installation personnalisée**

Vous permet de sélectionner séparément toutes les fonctions ci-dessus.  
Vous pouvez également installer la fonction Mode FIPS.

Les étapes suivantes dépendent des choix effectués dans **Sélectionner le type d'installation**.

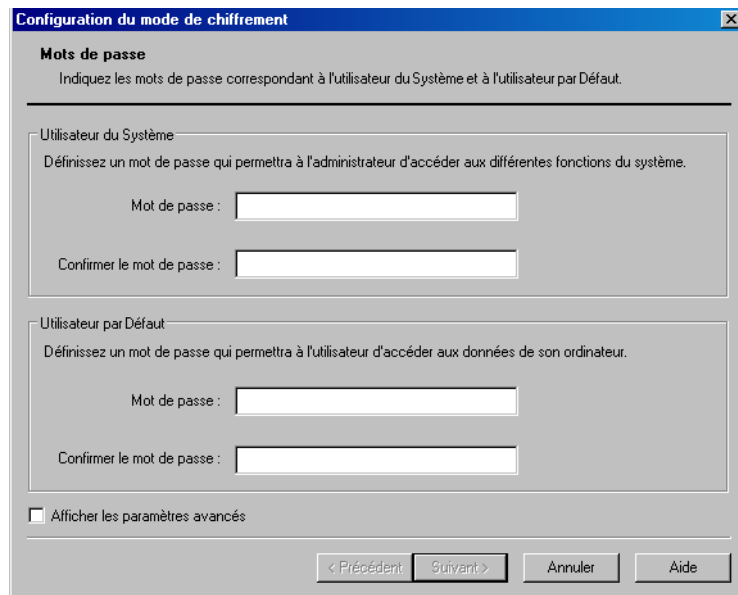
**Si vous avez choisi un type d'installation avec chiffrement ...**

Vous êtes invité à saisir et à confirmer des mots de passe pour les types d'utilisateur prédéfinis d'utilisateur du système (SYSTEM) et d'utilisateur par défaut (USER) de Sophos SafeGuard Disk Encryption. Il s'agit des mots de passe qui permettront d'accéder à votre ordinateur. Ils doivent respecter les règles de définition de mot de passe de Sophos SafeGuard Disk Encryption.

- Le mot de passe pour l'utilisateur par défaut (USER) est le mot de passe initial requis pour la connexion à l'ordinateur après l'installation de Sophos SafeGuard Disk Encryption. A la première ouverture de session de Sophos SafeGuard Disk Encryption l'utilisateur par défaut est invité à changer le mot de passe.
- Le mot de passe SYSTEM est requis par l'utilisateur du système. L'utilisateur du système est l'administrateur avec les droits administratives du niveau hiérarchique le plus élevé. Le mot de passe SYSTEM est requis pour les tâches d'administration et la modification des paramètres utilisateur.

**Remarque :** Veillez à conserver les mots de passe saisis.

Conservez le mot de passe SYSTEM en lieu sûr. En cas de perte de ce mot de passe, vous ne pourrez plus accéder à l'ordinateur.



Le chiffrement par défaut et les paramètres de sécurité (chiffrement de la partition C: et authentification avant amorçage activée et ouverture de session automatique sécurisée) sont définis automatiquement.

- Pour utiliser les paramètres de configuration par défaut, cliquez sur **Suivant** pour terminer l'installation. Vous devez ensuite exécuter des tâches de post-installation (voir [Exécution des tâches de post-installation](#) sur page 18).
- Pour modifier la configuration par défaut pour les paramètres généraux, les paramètres de chiffrement et d'utilisateurs, cochez la case **Afficher les paramètres avancés** et cliquez sur **Suivant**. Puis, effectuez les modifications souhaitées dans les boîtes de dialogue **Configuration du poste de travail**.

### **Si vous avez choisi l' installation du type Distribuée sur les ordinateurs du réseau ...**

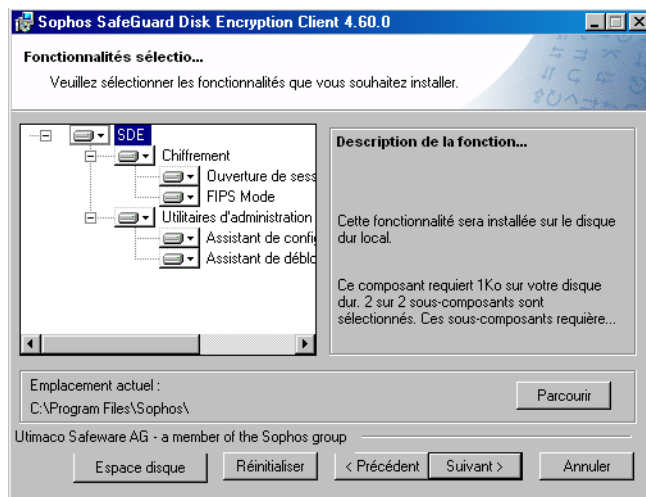
Cliquez sur **Suivant** pour terminer l'installation. Créez ensuite un fichier de configuration pour que l'installation automatisée déploie Sophos SafeGuard Enterprise sur les ordinateurs de votre réseau (voir [L'assistant de configuration pour le déploiement](#) sur page 45).

### **Si vous avez choisi l'installation personnalisée ...**

Sélectionnez les fonctions désirées et cliquez sur **Suivant** pour terminer l'installation.

### 3.1.1 Fonctions installables de Sophos SafeGuard Disk Encryption

Le tableau suivant contient la liste des fonctions disponibles dans Sophos SafeGuard Disk Encryption et précise dans quel type d'installation elles sont incluses. Cette boîte de dialogue est affichée, si vous avez choisi l'installation personnalisée.



| Type d'installation                                   | Fonction   |
|---|--|
| Installation distribuée sur les ordinateurs du réseau | <p><b>Utilitaires d'administration :</b></p> <p><b>Assistant de configuration pour le déploiement</b><br/>Il automatise l'installation, la configuration et la désinstallation de Sophos SafeGuard Disk Encryption. Des tâches d'administration telles que la modification d'une installation existante de Sophos SafeGuard Disk Encryption peuvent être planifiées via les fichiers de configuration (voir <a href="#">Créer un nouveau fichier de configuration</a> sur page 45 ).</p> |
|   | <p><b>Assistant de déblocage à distance</b><br/>Assistant permettant au personnel du support technique d'accorder certaines autorisations aux utilisateurs, pour des actions spécifiques (par exemple, la définition d'un nouveau mot de passe), même si l'administrateur est absent (voir <a href="#">Maintenance à distance (Requête/Réponse)</a> sur page 122).</p>   |

|  |  |
|--|--|
| Installation chiffrée sur cet ordinateur | <p><b>Chiffrement</b></p> <p>Installe Sophos SafeGuard Disk Encryption avec l'authentification avant amorçage activée et le chiffrement de la partition C: par défaut. L'ordinateur sera soumis à la fonction de chiffrement et vous devrez le redémarrer après l'installation.</p>  |
|  | <p><b>Secure Auto Logon (Connexion automatique sécurisée, SAL)</b></p> <p>Se souvient des données d'identification Windows utilisées à la première ouverture de session, afin que vous n'ayez à saisir les identifiants Sophos SafeGuard Disk Encryption qu'au moment de l'authentification avant amorçage pour ouvrir une session sur l'ordinateur (voir <a href="#">Ouverture de session automatique sécurisée (SAL)</a> sur page 90).</p> |
|  | <p><b>Assistant de création d'une disquette de secours</b></p> <p>Vous permet de créer des supports de démarrage de secours contenant la sauvegarde du noyau du système, ainsi que plusieurs fichiers de secours qui vont permettre de résoudre les erreurs Sophos SafeGuard Disk Encryption et d'accéder de nouveau à votre ordinateur.</p> <p>Installé par défaut avec Chiffrement.</p>  |
| Installation distribuée avec chiffrement | Toutes les fonctions ci-dessus   |
| Installation personnalisée               | <p>Sélectionnez l'une des fonctions ci-dessus, et encore :</p> <p><b>FIPS Mode</b></p> <p>Garantit que Sophos SafeGuard Disk Encryption s'exécute en accord avec la norme FIPS 140-2, niveau 1 (voir <a href="#">Certification FIPS 140-2 (Level 1)</a> sur page 110).</p>   |

## 3.2 Exécution des tâches de post-installation

Si vous avez choisi un type d'installation avec chiffrement, effectuez les tâches suivantes sur votre ordinateur à la fin de l'installation.

1. Redémarrez votre ordinateur. La boîte de dialogue d'ouverture de session Windows s'affiche.
2. Saisissez vos données d'identification Windows.
3. Redémarrez l'ordinateur. La boîte de dialogue d'authentification avant amorçage de Sophos SafeGuard Disk Encryption s'affiche.

4. Saisissez le mot de passe utilisateur Sophos SafeGuard Disk Encryption défini au cours de l'installation. Vous êtes invité à modifier ce mot de passe.
5. Modifiez le mot de passe utilisateur Sophos SafeGuard Disk Encryption.
6. Vous êtes de nouveau invité à saisir vos données d'identification Windows.
7. Confirmez d'utiliser l'accès direct automatique à Windows pour la connexion automatique à Windows. Vous êtes connecté à votre ordinateur.

### Et ensuite ?

#### ■ Chiffrement initial

Le chiffrement par défaut de la partition C: du disque dur démarre automatiquement. Cette étape peut prendre un certain temps. Une barre de progression s'affiche. Vous pouvez continuer à travailler sur l'ordinateur.

#### ■ Sauvegarde automatique du noyau

Le noyau du système est sauvegardé automatiquement, voir [Sauvegarde de automatique de noyau du système](#) sur page 130. Il contient les pilotes de Sophos SafeGuard Disk Encryption et le secteur de démarrage principal. Vous pouvez continuer à travailler sur l'ordinateur.

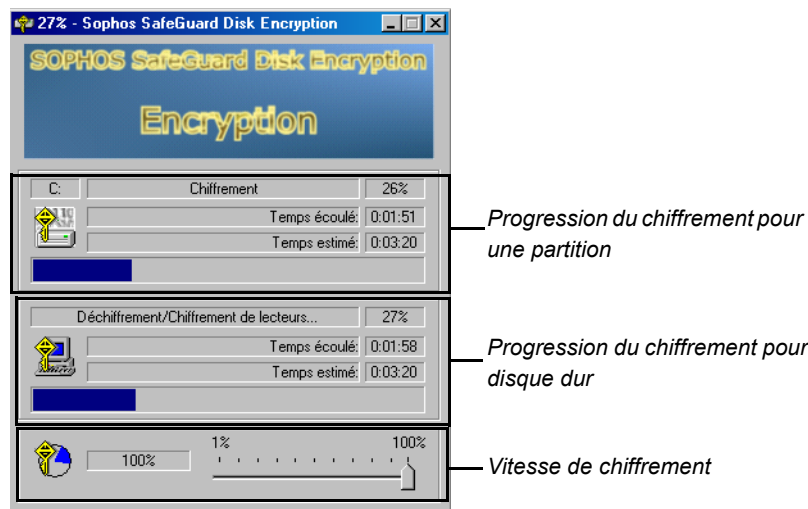
#### ■ Accès direct automatique à Windows

Si vous avez confirmé d'utiliser cette option: La prochaine fois que vous démarrerez l'ordinateur, vous n'aurez qu'à saisir votre mot de passe utilisateur Sophos SafeGuard Disk Encryption au moment de l'authentification avant amorçage et vous serez automatiquement dirigé vers Windows.

## 3.3 Chiffrement initial

En cas d'une installation par défaut avec chiffrement, la partition C: de la disque dur est chiffrée automatiquement. Une fenêtre indiquant la progression du chiffrement est affichée. Le chiffrement se fait en arrière-plan, ce qui permet à l'utilisateur de poursuivre son travail. L'opération de chiffrement initial avec AES-256 par Sophos SafeGuard Disk Encryption nécessite environ 10 Go et dure entre 20 et 30 minutes sur un ordinateur portable de dernière génération.

Une fenêtre indiquant la progression du chiffrement est affichée. Si de très petites partitions sont chiffrées, il peut arriver que la boîte de dialogue ne soit pas visible.



Si l'ordinateur est éteint avant la fin du chiffrement initial, il redémarre toujours DIRECTEMENT à partir du disque dur. Cela s'applique également au premier redémarrage à la fin du chiffrement.

**Ne pas interrompre le chiffrement initial des disques durs « connectables à chaud ».**

Le terme « connectable à chaud » désigne les périphériques USB qui peuvent être connectés et déconnectés sans devoir redémarrer le système. Il ne faut pas interrompre le chiffrement initial des disques durs connectables à chaud.

**Ne plus modifier les partitions**

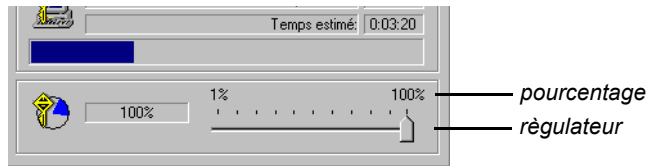
Après le chiffrement de la première partition du disque dur de votre ordinateur, vous ne pourrez plus modifier les partitions. Pour changer les partitions, vous devez commencer par désinstaller Sophos SafeGuard Disk Encryption (= supprimer le chiffrement du premier disque dur), puis créer/supprimer les partitions et réinstaller Sophos SafeGuard Disk Encryption.

**Remarque:** Pour plus d'informations au chiffrement du disque dur, voir [Configuration du chiffrement](#) sur page 66.

**Remarque:** Si le chiffrement initial échoue pour aucune raison et il n'est pas possible de démarrer l'ordinateur, contactez l'assistance technique.

### 3.3.1 Définition de la vitesse de chiffrement

La vitesse à laquelle le chiffrement s'effectue est de 100 % par défaut, mais vous pouvez la modifier avec le régulateur. Plus le pourcentage est élevé, plus le chiffrement est rapide.



Si vous utilisez le régulateur pour réduire la vitesse de chiffrement, Sophos SafeGuard Disk Encryption n'enregistre pas la vitesse de chiffrement réduite. Une fois la station de travail redémarrée, le chiffrement reprend à sa vitesse optimale (100 %).

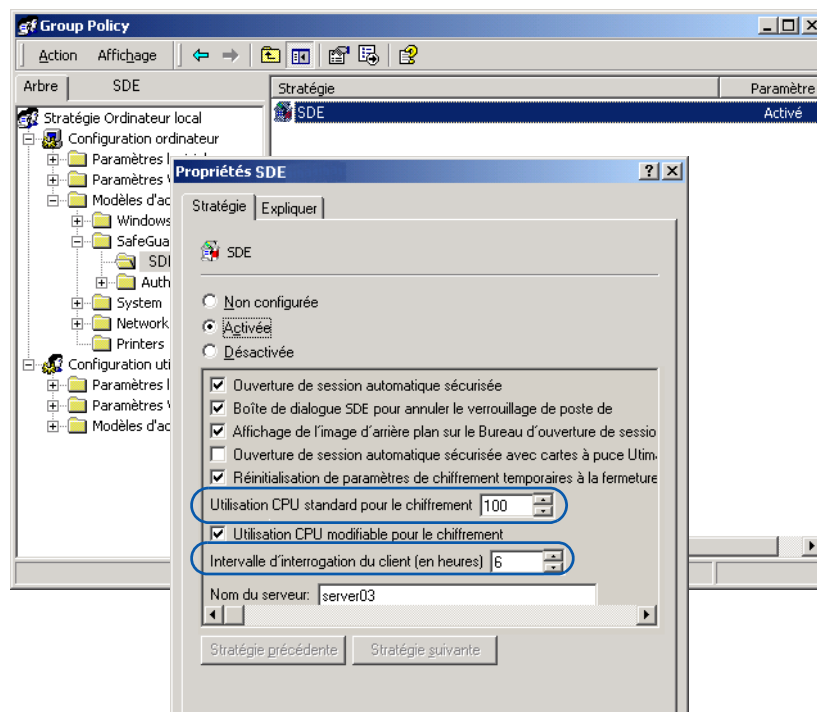
### Modification de la vitesse de chiffrement dans le modèle administratif

Les paramètres de l'unité centrale (CPU) peuvent être également activés ou désactivés à l'aide d'une stratégie du modèle d'administration SafeGuard (voir [Modification des paramètres de registre fréquemment utilisés via le modèle d'administration](#) sur page 58).

La stratégie se trouve sous

**Configuration ordinateur**  
 \Modèles d'administration  
 \SafeGuard  
 \SDE

A la page des propriétés de la stratégie « SDE », vous disposez à cet effet des options « Utilisation CPU standard pour chiffrement » et « Utilisation CPU modifiable pour chiffrement ».



## 4 Installation centrale

Les administrateurs peuvent définir la configuration globale des ordinateurs d'utilisateurs avant de distribuer le logiciel.

À cet effet, l'administrateur crée un fichier sur ordinateur qui contient tous les réglages Sophos SafeGuard Disk Encryption nécessaires aux ordinateurs des utilisateurs. Il s'agit du « fichier de configuration ». Le fichier de configuration permet d'installer Sophos SafeGuard Disk Encryption sur les ordinateurs des utilisateurs. Toute modification ultérieure de la configuration de Sophos SafeGuard Disk Encryption passera par la création d'autres fichiers de configuration. Il est possible d'installer Sophos SafeGuard Disk Encryption dans un environnement avec ou sans Active Directory.

Pour informations à la création des fichiers de configuration, voir [L'assistant de configuration pour le déploiement](#) sur page 45.

### 4.1 Installation avec Active Directory

Sophos SafeGuard Disk Encryption est installé sur les clients dans un environnement Active Directory en ajoutant un programme MSI approprié (`SDE.msi`) à la fonction de distribution de logiciel d'un objet Stratégie de groupe).

Pour adapter le fichier MSI, vous devez disposer d'un éditeur permettant de traiter les fichiers MSI (par ex. ORCA ou NetInstall). ORCA fait partie du PSDK Microsoft (Platform Software Development Kit). Vous pouvez télécharger le PSDK sur le site Web de Microsoft.

#### 4.1.1 Conditions

- Avant un redémarrage, tous les appareils prévus pour l'installation doivent être déplacés également dans l'unité d'organisation pour laquelle l'OSG configuré est utilisé.
- Pour la distribution centralisée du logiciel, les PC clients doivent être reliés au domaine Directory et un compte d'ordinateur doit être défini et actif pour le PC.
- Il doit y avoir suffisamment d'emplacement mémoire sur la partition système.

## 4.1.2 Déploiement des fichiers MSI

Pour ce faire, effectuez la procédure suivante :

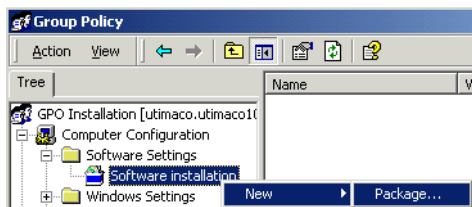
1. Partagez un lecteur local sur le PC de l'administrateur (retirez la protection en écriture) et copiez tous les fichiers .msi requis sur ce lecteur. Assurez-vous que les clients ont accès au lecteur partagé.
2. Dans Windows, cliquez sur **Démarrer\Paramètres\Panneau de configuration\Outils d'administration**. De là, sélectionnez **Utilisateurs et ordinateurs Active Directory**.
3. Cliquez avec le bouton droit de la souris sur un domaine ou une unité d'organisation et sélectionnez **Propriétés**.
4. Sélectionnez l'onglet **Stratégie de groupe** dans la boîte de dialogue **Propriétés**.



5. Créez un objet de stratégie de groupe (par exemple " Installation de GPO ") en cliquant sur **Nouveau**.
6. Cliquez sur **Édition**.
7. Windows affiche alors la stratégie de groupe " Installation de GPO ".
8. Sélectionnez **Configuration ordinateur\Paramètres du logiciel\Installation logicielle**. Dans le menu contextuel **Installation logicielle**, créez un lien vers le serveur de fichiers qui déploiera les packages du logiciel.

**Remarque :** Ajoutez uniquement des packages MSI dans l'installation logicielle de la Configuration ordinateur. Les installations via la Configuration utilisateur ne sont pas prises en charge.

9. Cliquez avec le bouton droit de la souris sur **Installation logicielle**, puis sélectionnez **Nouveau et Package**.



10. Sélectionnez un (ou plusieurs) fichiers .msi dans le répertoire partagé. Chargez les fichiers depuis le véritable chemin réseau (chemin d'accès UNC).
11. Lorsque vous avez accepté toutes les invites, Windows ajoute le fichier .msi à la routine d'installation de l'objet de stratégie de groupe.
12. Fermez la boîte de dialogue.
13. Si vous souhaitez que la langue du système d'exploitation soit ignorée du côté du client, ouvrez le menu contextuel du package MSI installé et sélectionnez Propriétés\Déploiement\Avancé\Ignorer la langue lors du déploiement de ce package.

L'objet de stratégie de groupe " Installation de GPO " sera à présent utilisé pour tous les ordinateurs/utilisateurs présents dans les domaines d'une unité d'organisation. Au prochain redémarrage de ces postes de travail, les packages seront installés sur les ordinateurs cible, de façon automatisée.

Avant de redémarrer les ordinateurs connectés, veillez à ce que :

- les ordinateurs choisis pour l'installation aient été ajoutés à l'unité d'organisation pour laquelle le GPO est configuré ;
- les ordinateurs soient liés au domaine du dossier pour l'exécution de la distribution centralisée du logiciel. De plus, un compte d'ordinateur actif doit être créé sur le domaine pour les PC clients.
- l'espace mémoire sur la partition système est suffisant

## 4.2 Installation sans Active Directory

Pour installer Sophos SafeGuard Disk Encryption sans environnement Active Directory, vous devez avoir des programmes de répartition de logiciel de tiers.

1. Utilisez vos propres outils pour créer et distribuer un package d'installation à installer sur les ordinateurs des utilisateurs finaux. Le package doit contenir :
  - le package d'installation `SDE.msi` disponible dans le dossier de produit téléchargé ;
  - le fichier de configuration généré `Install.cfg` ;
  - un script contenant la ligne de commande pour l'installation préconfigurée.
2. Créez un dossier `Software` sur l'ordinateur de l'administrateur ; il servira d'emplacement de stockage central pour toutes les applications.
3. Créez le script.
4. Distribuez le package d'installation sur les ordinateurs des utilisateurs finaux.

5. Communiquez le mot de passe SDE par défaut aux utilisateurs finaux et informez-les des tâches de post-installation à exécuter.

### 4.2.1 Syntaxe de ligne de commande pour Installation préconfigurée

Quand Sophos SafeGuard Disk Encryption doit être installé avec préconfiguration, utilisez le programme MSIEXEC. MSIEXEC est déjà intégré dans Windows 2000 et dans Windows XP. Ce programme d'installation permet d'exécuter le fichier de configuration créé par l'administrateur. Comme la source et la cible peuvent également être spécifiées, vous avez la possibilité de procéder à une installation unitaire sur plusieurs ordinateurs.

#### Syntaxe de ligne de commande

```
msiexec /i <chemin+msi nom programme> /qn ADDLOCAL=ALL | <fonctionnalités>
<paramètres+fichier de configuration>
```

La syntaxe de la ligne de commande comprend :

- **paramètres Windows Installer**, auditant par ex. les avertissements et les messages d'erreur dans un fichier pendant l'installation.
- **Les composants Sophos SafeGuard Disk Encryption** devant être installés avec un programme Sophos SafeGuard Disk Encryption (par ex. l'assistant de déblocage à distance).
- **propres paramètres Sophos SafeGuard Disk Encryption** via lesquels des fichiers de configuration peuvent par ex. être transmis.
- un fichier de configuration pour une installation avec la propriété « Installer ».

#### Exemple :

```
msiexec /i C:\Software\Sophos\SDE.msi
/L*VX \\%distributionserver%\Sophos\%computername%\SDE_inst.log
CFGFILE=C:\Software\Sophos\Install.cfg/QN
```

Sophos SafeGuard Disk Encryption est installé avec les fonctions par défaut dans le répertoire d'installation par défaut C : \Programs\Sophos\ SafeGuard Disk Encryption et le fichier journal SDE\_inst.log est créé sur le réseau . Les paramètres préconfigurés pour Sophos SafeGuard Disk Encryption se trouvent dans le fichier Install.cfg.

## 4.2.2 Options sélectionnées utilisées par Windows Installer

**Remarque :** Exécutez `msiexec.exe` à partir de l'invite de commande Windows. Le système affiche ensuite toutes les options disponibles du programme d'installation de Windows.

`/i <chemin + nom de fichier>`

Installe (à partir de l'emplacement de stockage spécifié) le package d'installation Sophos SafeGuard Disk Encryption dans le répertoire d'installation par défaut `C:\Program Files\Sophos\SafeGuard Disk Encryption`. L'élément suivant est installé par défaut : chiffrement de la partition C: y compris l'activation de l'authentification avant amorçage et la connexion automatique sécurisée à Windows.

`/qn`

Installation sans intervention de l'utilisateur et affichage d'aucune interface utilisateur.

`ADDLOCAL=`

Liste les composants qui doivent être installés. Si le paramètre n'est pas spécifié, les fonctions par défaut (l'authentification avant amorçage, chiffrement par partition et la connexion automatique sécurisé) sont installés. Pour une liste complète des noms des composants et les composants parents, voir [Composants de Sophos SafeGuard Disk Encryption](#) sur page 27.

**Remarque :** Les différents composants sous sont séparés seulement par une virgule, sans espace supplémentaire. Respectez également la casse (majuscules/minuscules) pour la saisie des différents composants et des paramètres Sophos SafeGuard Disk Encryption.

Lors de la sélection d'un composant, tous les composants parents doivent également être ajoutés à la ligne de commande !

`ALL`

Permet d'installer tous les composants disponibles.

`REBOOT=Forcerestart | NORESTART`

Impose ou neutralise un redémarrage après l'installation. Sans indication, un redémarrage est imposé (défaut: Forcerestart).

`/L* vX <chemin + nom de fichier>`

Consigne tous les messages d'avertissement et d'erreur dans le fichier journal spécifié et crée un fichier journal pouvant être analysé automatiquement sans passer par `wilogutl.exe`.

Pour être toujours en mesure d'accéder au fichier journal d'installation lorsque vous déployez le logiciel de chiffrement sur les ordinateurs des utilisateurs finaux, assurez vous de l'enregistrer sur un chemin UNC sur le réseau.

`v` augmente l'option journal aux mode Verbose.

Le paramètre `/Le <chemin + nom de fichier>` ne consigne que les messages d'erreur.

Installldir= <répertoire>

Indique le répertoire dans lequel Sophos SafeGuard Disk Encryption va être installé.

Sans indication, le répertoire d'installation par défaut <SYSTEM> :\PROGRAMMES\SOPHOS est utilisé.

### 4.2.3 Composants de Sophos SafeGuard Disk Encryption

Dans le table ci-dessous se trouve une liste de tous les composants pouvant être automatiquement installés via le fichier .msi. Elles sont identiques aux fonctionnalités qui peuvent être sélectionnées au cours d'une installation personnalisée autonome.

#### Composants installables avec SDE.msi

| Paramètre  | Composant parent | Description   |
|------------|------------------|---|
| Encryption | SDE              | Installe une version fonctionnelle de Sophos SafeGuard Disk Encryption (ce qui inclut SafeGuard GINA). PBA est installé y la partition C: est chiffré par défaut. |
| SGSAL      | Encryption       | Installe SAL (ouverture de session automatique sécurisée) pour activer la connexion automatique vers Windows.   |
| FIPS       | Encryption       | Installe le mode FIPS.  |
| AdmTools   | SDE              | Installe les utilitaires d'administration (assistant de configuration pour le déploiement, assistant de déblocage à distance).                                    |
| CfgWiz     | AdmTools         | Installe l'assistant de configuration pour le déploiement.  |
| RcWiz      | AdmTools         | Installe l'assistant de déblocage à distance.   |

### 4.2.4 Paramètres Sophos SafeGuard Disk Encryption

**Remarque :** Tous les paramètres doivent être saisis en majuscules dans la syntaxe de ligne de commande.

AUTOBACKUP=0 | 1

Indique si l'assistant de création d'une disquette de secours pour la sauvegarde du noyau système doit être démarré une fois une installation effectuée avec succès. Dans la configuration de base, il démarre automatiquement (AUTOBACKUP=1).

CFGFILE=<fichier de configuration>

Ce paramètre définit le nom complet d'un fichier de configuration Sophos SafeGuard Disk Encryption pour une installation.

PARTCHECK=0 | 1

Détermine si les types de partition existants prennent en charge les systèmes de fichiers connus (FAT 32, NTFS). Si le type de partition est inconnu, l'installation est interrompue. Dans la configuration de base, la vérification est active (PARTCHECK=1).

GINASYS=0 | 1

Indique si le système SafeGuard GINA pour le contrôle de l'ouverture de session Windows doit être installé. SafeGuard GINA (GINASYS=1) est installé dans la configuration par défaut.

**Avis :** Nous conseillons de toujours utiliser SafeGuard GINA. Le système SafeGuard GINA est un composant fonctionnel important de Sophos SafeGuard Disk Encryption. Certaines fonctionnalités ne sont pas disponibles après migration vers une nouvelle version. L'absence du composant GINA peut avoir une incidence sur les migrations ultérieures.

Si vous n'installez pas SafeGuard GINA, certaines fonctions de Sophos SafeGuard Disk Encryption ne seront pas disponibles après l'installation :

- La boîte de dialogue de chiffrement/déchiffrement (ECVIEW) n'est pas affichée quand l'utilisateur n'est pas connecté .
- L'ouverture de session automatique sécurisée ne fonctionne pas.
- L'ouverture de session Windows n'est pas bloquée quand l'activation à distance sécurisée est active.

## 5 Résolution des problème d'une installation avec SGEInteg

Si l'installation a échoué bien qu'ayant fait toutes les préparations vous pouvez utiliser le programme SGEInteg pour la résolution des problèmes de l'installation. SGEInteg indique les erreurs réparables et fatales.

Vous pouvez démarrer le programme SGEInteg du dossier de produit.

### Paramètres du programme de réparation

Vous pouvez lancer SGEInteg avec les paramètres suivants :

```
SGEINTEG [/?] [/c] [/v]
```

- |    |   |
|----|---|
| /? | Aide<br>Affiche tous les paramètres.  |
| /c | Lance l'analyse du système de fichiers.   |
| /v | Active le mode prolix<br>Des messages d'état et d'erreur détaillés s'afficheront à l'écran si vous avez activé ce mode. |

### Exemple

```
sgeinteg.exe /c /v > C:\Software\SGEInteg.log
```

- Le programme SGEInteg est appelé.
- Le système de fichiers est analysé.
- Messages d'erreur et de statut sont enregistrer dans le fichier journal indiqué.

## 6 Désinstallation

Une désinstallation de Sophos SafeGuard Disk Encryption a les conséquences suivantes :

- toutes les zones jusqu'à présent chiffrées du ou des disques durs sont déchiffrées,
- l'authentification avant amorçage (PBA) est supprimée,
- l'ouverture de session Windows initiale est restaurée si la fonction SAL était installée,
- tous les fichiers Sophos SafeGuard Disk Encryption sont effacés,
- toutes les entrées dans la base de registres de Sophos SafeGuard Disk Encryption sont supprimées.

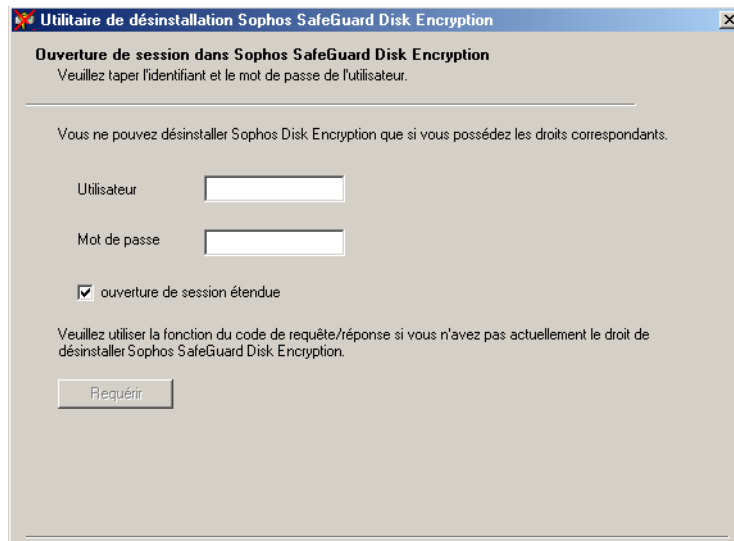
Dans la configuration de base, Sophos SafeGuard Disk Encryption ne peut être désinstallé que par l'utilisateur SYSTEM. En règle générale toutefois, chaque utilisateur Sophos SafeGuard Disk Encryption possédant un droit de désinstallation peut supprimer le programme d'un poste de travail.

**N'essayez pas de supprimer Sophos SafeGuard Disk Encryption en effaçant les fichiers. Si SafeGuard Sophos Disk Encryption n'est pas correctement désinstallé, des entrées demeureront dans la base de registres. Ceci pourrait éventuellement empêcher une nouvelle installation de Sophos SafeGuard Disk Encryption. Dans ce cas, le système d'exploitation de l'ordinateur devra être réinstallé.**

### 6.1 Désinstallation locale

Sélectionnez successivement Démarrer \ Paramètres \ Panneau de configuration \ Ajout \ Suppression de programmes, et enfin « Sophos SafeGuard Disk Encryption ».

Via **Supprimer** et en cliquant sur **Suivant** dans l'écran de bienvenue, vous entrez dans la boîte de dialogue **Ouverture de session Sophos SafeGuard Disk Encryption**.



Tout utilisateur qui souhaite désinstaller le programme, doit entrer son nom d'utilisateur et son mot de passe Sophos SafeGuard Disk Encryption. L'utilisateur doit posséder le droit de désinstaller Sophos SafeGuard Disk Encryption. Après avoir entré les données utilisateur correctes, cliquez sur **Suivant**, ce qui confirme la vérification de sécurité. Entraîne la désinstallation de Sophos SafeGuard Disk Encryption de façon automatique.

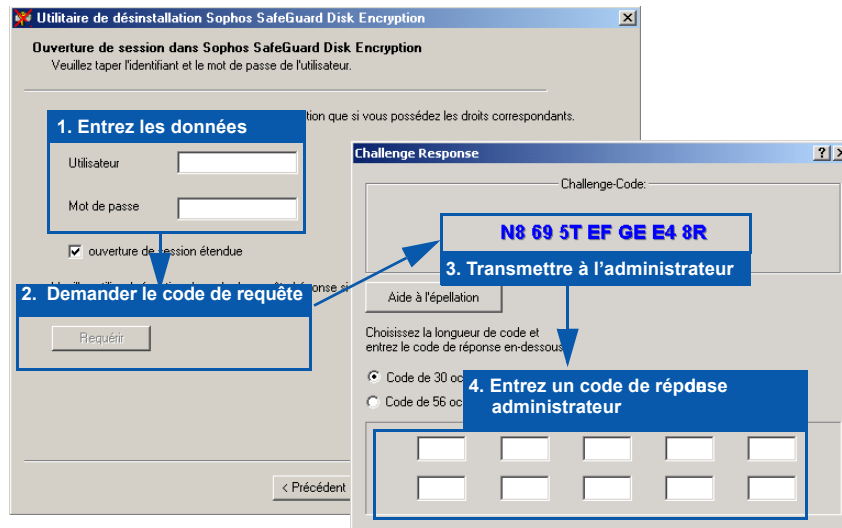
## 6.2 Désinstallation avec Requête/Réponse

Si un utilisateur Sophos SafeGuard Disk Encryption n'est pas autorisé, en raison de son profil, à désinstaller Sophos SafeGuard Disk Encryption, l'administrateur peut lui octroyer ce droit à l'aide de la procédure Requête/Réponse. Dans ce but, l'utilisateur et l'administrateur échangent un code de requête et de réponse.

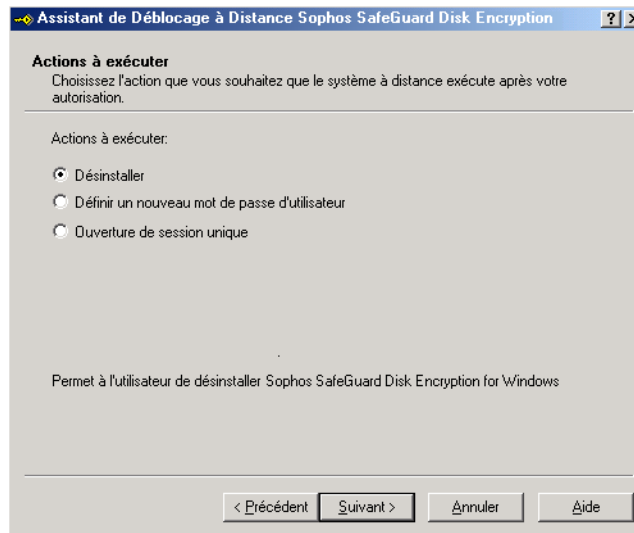
L'utilisateur qui génère le code de réponse (administrateur) doit connaître, sur l'ordinateur de l'utilisateur, un profil disposant d'un droit de désinstallation. Ce profil utilisateur doit en outre toujours avoir *au moins les mêmes droits* que le demandeur sur l'ordinateur de l'utilisateur.

Comment procéder

1. L'utilisateur lance une désinstallation locale (voir [Désinstallation locale](#) sur page 30) et entre dans la boîte de dialogue *Ouverture de session dans Sophos SafeGuard Disk Encryption*.
2. Il tape ses données *Sophos SafeGuard Disk Encryption*, demande le code de requête et le transmet par téléphone, SMS ou courrier électronique à l'administrateur.



3. L'assistant de déblocage à distance permet à l'administrateur de générer un code de réponse avec les données d'accès SafeGuard Sophos Disk Encryption de l'utilisateur. Le droit de désinstallation est fourni avec le code de réponse.



4. Après échange des codes de requête et de réponse, Sophos SafeGuard Disk Encryption est désinstallé.

## 6.3 Désinstallation automatique avec fichier de configuration

La désinstallation de Sophos SafeGuard Disk Encryption est automatisée quand un fichier de configuration avec attribut « Désinstaller » est appelé avec la commande `MSIEXEC`.

Pour informations à la création d'un fichier de configuration du type „Désinstaller“ voir [Création d'un fichier de configuration pour une installation](#) sur page 46 .

### **Syntaxe de ligne de commande**

```
msiexec /x C : \Programs \Sophos \SafeGuard Disk Encryption \SDE.msi  
CFGFILE=D : \Deinstall.cfg /qn
```

## 7 Démarrage du système et ouverture de session

Sophos SafeGuard Disk Encryption remplace le mécanisme d'authentification propre à Windows par une ouverture de session avant le processus d'amorçage, appelée **authentification avant amorçage (PBA)**. L'ouverture de session PBA est la méthode par défaut utilisée après l'installation.

**Quand l'authentification avant amorçage est activée**, une ouverture de session n'est possible qu'avec les données d'accès Sophos SafeGuard Disk Encryption. A partir du mot de passe saisi, la clé de déchiffrement d'un disque dur chiffré, requise pour l'amorçage, est calculée.

**Quand l'authentification avant amorçage est désactivée**, le disque dur reste chiffré. L'ordinateur démarre mais sans interaction de l'utilisateur jusqu'à l'écran de bienvenue de Windows. Dans ce cas, les données de démarrage (Sophos SafeGuard Disk Encryption) sont stockées dans le disque dur sous forme de fichiers cachés. Sans authentification avant amorçage, le niveau de sécurité d'un système est plus faible.

**Remarque:** Pour des raisons de sécurité nous recommandons de ne pas désactiver la PBA. Sinon le système est démarré sans demander un mot de passe.

Selon la méthode d'authentification définie par défaut, l'ouverture de session dans la PBA se fait

- comme utilisateur ordinaire (avec nom d'utilisateur et mot de passe)
- comme utilisateur par défaut (avec mot de passe uniquement)

Indépendamment de la méthode d'authentification, l'écran d'ouverture de session PBA a des caractéristiques et fonctions identiques

- Nom du poste de travail et mentions légales
- Fonction d'aide pour modifier le mot de passe Sophos SafeGuard Disk Encryption
- Fonction d'aide pour réinitialiser des mots de passe oubliés

## 7.1 Ouverture de session comme utilisateur par défaut



Un « Utilisateur par défaut » Sophos SafeGuard Disk Encryption ouvre une session seulement avec son mot de passe Sophos SafeGuard Disk Encryption. Pour les utilisateurs par défaut, la saisie du nom d'utilisateur est inutile.

### 7.1.1 Ouverture de session étendue via [F2]

Si une personne autre que l'utilisateur par défaut doit se connecter, la fonctionnalité de *connexion étendue* doit être activée. Ceci a pour conséquence, qu'en supplément du mot de passe Sophos SafeGuard Disk Encryption ils doivent également entrer leur mot de passe utilisateur.

Au-dessus de la ligne de saisie du mot de passe, vous voyez apparaître le champ de saisie du nom d'utilisateur quand vous appuyez sur F2.

**Avis :** L'utilisateur SYSTEM doit **toujours** ouvrir une session avec le nom d'utilisateur et le mot de passe.

## 7.2 Ouverture de session comme utilisateur régulier



Un utilisateur régulier ouvre une session PBA avec son nom d'utilisateur et son mot de passe Sophos SafeGuard Disk Encryption.

Sous le nom du programme est affiché le nom du poste de travail. Ces données sont reprises des paramètres du système de votre poste de travail.

## 7.3 Modifier le mot de passe Sophos SafeGuard Disk Encryption avec la touche [F10]

Les utilisateurs peuvent modifier eux-mêmes le mot de passe Sophos SafeGuard Disk Encryption avec la touche F10. L'utilisateur entre d'abord dans ce cas ses données Sophos SafeGuard Disk Encryption actuelles et les confirme avec F10. Il est ensuite invité à entrer un nouveau mot de passe.

L'administrateur Sophos SafeGuard Disk Encryption peut toutefois prescrire également la définition d'un nouveau mot de passe après écoulement d'un certain laps de temps.

## 7.4 Fonction d'aide pour réinitialiser les mots de passe oubliés avec la touche [F9]

Sophos SafeGuard Disk Encryption offre un mécanisme Requête/Réponse pour réinitialiser les mots de passe « oubliés ». Si l'utilisateur a besoin d'aide, il doit générer un code de requête dans la PBA en appuyant sur la touche F9.

Ce code de requête est affiché sur l'écran de l'utilisateur sous forme de chaîne de caractères ASCII (14 caractères). L'utilisateur appelle ensuite son administrateur et lui fournit ses informations

personnelles et le code de requête. L'administrateur génère alors un code de réponse. Après saisie de ce code de réponse sur l'ordinateur de l'utilisateur, celui-ci peut redéfinir son mot de passe.

Pour plus de détails sur la procédure Requête/Réponse, voir [Maintenance à distance \(Requête/Réponse\)](#) sur page 122.



## 7.5 Échec d'ouverture de session

L'ouverture de session PBA peut échouer quand

- le nom d'utilisateur Sophos SafeGuard Disk Encryption a été incorrectement entré,
- le mot de passe est incorrect,
- le nom d'utilisateur n'est plus valable.

Quand un utilisateur a entré incorrectement ses données, il doit patienter quelques secondes avant de pouvoir de nouveau ouvrir une session. Pour des raisons de sécurité, le temps d'attente augmente exponentiellement à partir de la seconde tentative. Une seule ouverture de session correcte réinitialise le temps d'attente.

### Réinitialiser une ouverture de session ayant échoué

Vous pouvez réinitialiser de la manière suivante une ouverture de session ayant échoué :

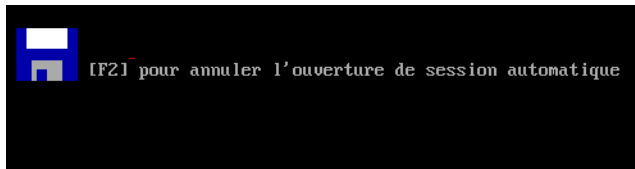
1. Insérez la disquette de secours dans le lecteur et amorcez le système depuis le lecteur A :
2. Appelez le programme `Sgeasy.exe`.
3. Un menu avec les options Désinstaller, Restaurer et Réparer apparaît.
4. Quittez le menu en cliquant sur « Annuler » (Options de désinstallation, Réparer, Restaurer).

5. Redémarrez le système.

Ceci réinitialise la période d'attente.

## 7.6 Imposer l'ouverture de session PBA avec la touche [F2]

Lorsque PBA est désactivé, vous pouvez attendre qu'une icône de disquette s'affiche dans le coin supérieur gauche de l'écran, puis appuyer sur F2 pour activer PBA et vous connecter de la façon habituelle.



## 7.7 Ouverture de session automatique dans le système d'exploitation

Sophos SafeGuard Disk Encryption peut en option exécuter une ouverture de session automatique dans Windows. Dans Sophos SafeGuard Disk Encryption, cette fonction est appelée *Ouverture de session automatique sécurisée* (en abrégé SAL). Après la saisie des données Windows, la SAL les place dans une plage sécurisée et y revient après chaque ouverture de session avec succès par l'utilisateur dans la PBA.

La seule condition est que la PBA soit activée.

Vous aurez à l'avenir uniquement besoin des données Sophos SafeGuard Disk Encryption pour ouvrir la session automatiquement.

Pour plus de détails, voir [Configuration du mot de passe Windows](#) sur page 90.

## 7.8 Compatibilité avec composants d'ouverture de session d'autres concepteurs

Pour toujours garantir la sécurité, les composants Sophos SafeGuard sont toujours appelés en premier par le système d'exploitation.

Une modification de cette séquence d'appel (p.ex. à la suite de l'installation de logiciel d'ouverture de session extérieur) est automatiquement annulée. En cas de réamorçage, si ceci vous empêche d'ouvrir une nouvelle session dans Windows ou si Windows n'est pas correctement disponible après l'ouverture de session, il y a deux possibilités pour annuler cette modification :

- Pour définir manuellement le composant de connexion qui doit être appelé par le composant de connexion Sophos SafeGuard, maintenez enfoncée la touche F8 lorsque le système passe de l'écran au bureau (vide au départ).

- Si vous n'appuyez pas sur F8, une boîte de dialogue s'affiche. Cette boîte de dialogue permet à l'utilisateur de décider si les composants d'ouverture de session Microsoft d'origine ou ceux d'un tiers sont adressés après appel des composants d'ouverture de session Sophos SafeGuard. Cette demande est affichée jusqu'à ce que l'utilisateur décide également de désactiver la demande. Dans ce cas, la dernière sélection effectuée reste valide. L'utilisation de composants Microsoft d'origine garantit un fonctionnement correct de l'ouverture de session, mais désactive le cas échéant certaines fonctions du produit tiers supplémentaire. Le manque d'homogénéité rend parfois difficile l'exécution concomitante de plusieurs composants d'ouverture de session Windows.

## 8 Aperçu de l'administration

Sophos SafeGuard Disk Encryption peut être configuré par le biais du programme de configuration (Assistant de configuration pour le déploiement) ou via l'utilitaire d'administration Sophos SafeGuard Disk Encryption. L'administration permet d'intervenir directement sur la configuration Sophos SafeGuard Disk Encryption de l'ordinateur. Elle sert à l'administration locale sur un ordinateur unique. L'assistant de configuration pour le déploiement ne change rien aux paramètres locaux, mais il réunit les paramètres Sophos SafeGuard Disk Encryption dans un fichier, que vous pouvez distribuer aux ordinateurs.

Les programmes d'administration présentent peu de différence en matière d'options de réglage. Dans les deux programmes, il est prescrit de s'authentifier avec des données Sophos SafeGuard Disk Encryption correctes pour pouvoir procéder à des modifications.

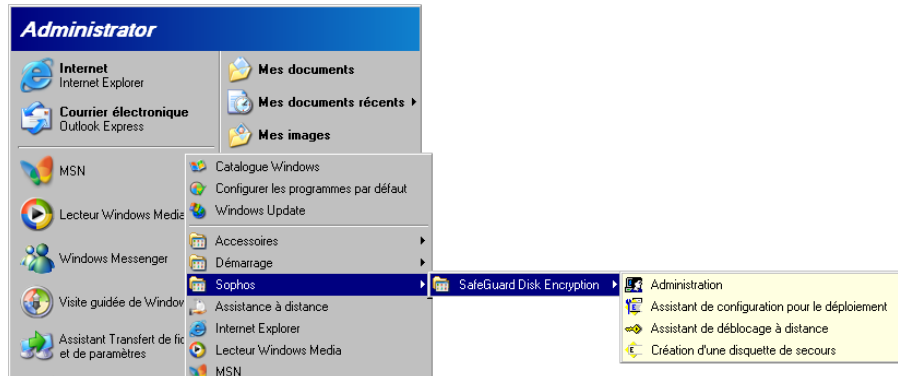
Lequel des deux programmes doit être utilisé dépend du contexte. Vous trouverez plus de détails ci-après.

### 8.1 Distinction des fonctions

Vous devez d'abord déterminer si la fonction de l'administrateur du système (l'utilisateur du système) doit être combinée avec celle du utilisateur, ou si elle doit s'en distinguer. Quand les fonctions sont séparées, il est possible d'intégrer un ou plusieurs assistants d'administration supplémentaires.

- **Fonction combinée** : l'utilisateur est lui-même l'administrateur du système (l'utilisateur du système). Il configure Sophos SafeGuard Disk Encryption sur son ordinateur, pour son usage personnel (une personne). Tous les paramètres sont définis dans l'administration. Le programme de configuration n'est pas requis. Il n'est pas non plus nécessaire de créer un fichier de configuration.
- **Fonctions distinctes sur un PC** : l'administrateur du système (l'utilisateur du système) configure Sophos SafeGuard Disk Encryption sur le PC de l'utilisateur. Si l'administrateur système crée un compte « administrateur » en supplément du compte « utilisateur », trois personnes ont accès au système. La configuration se fait à l'aide de la fonctionnalité d'administration. Le programme de configuration n'est pas requis, étant donné qu'aucun fichier de configuration ne doit être créé.
- **Fonctions distinctes sur plusieurs PC** : l'administrateur du système (l'utilisateur du système) configure Sophos SafeGuard Disk Encryption sur son ordinateur pour les utiliser sur plusieurs postes de travail. Pour ce travail, utilisez l'assistant de configuration pour le déploiement. Vous créez ainsi un fichier dans lequel les définitions sont sauvegardées. Le fichier de configuration est transmis aux utilisateurs via une installation préconfigurée. Pour changer les paramètres sur l'ordinateur de l'administrateur, servez-vous de l'utilitaire d'administration.

## 8.2 Démarrage de l'utilitaire d'administration et de l'assistant de configuration pour le déploiement



Après une installation, Sophos SafeGuard Disk Encryption crée un dossier SafeGuard Disk Encryption dans Programmes \ Sophos. L'utilitaire Administration et l'assistant de configuration pour le déploiement peuvent y être démarrés.

## 9 Fonction Administration

Une fois la fonction Administration exécutée, la boîte de dialogue de connexion s'affiche. Vous pouvez entrer ici les données Sophos SafeGuard Disk Encryption valides avant d'accéder à la fonction Administration.

Pour se connecter comme utilisateur, entrez votre mot de passe utilisateur.

Pour se connecter comme administrateur (l'utilisateur du système), choisissez **ouverture de session étendue**, entrez votre nom de l'utilisateur (SYSTEM) et le mot de passe SYSTEM.

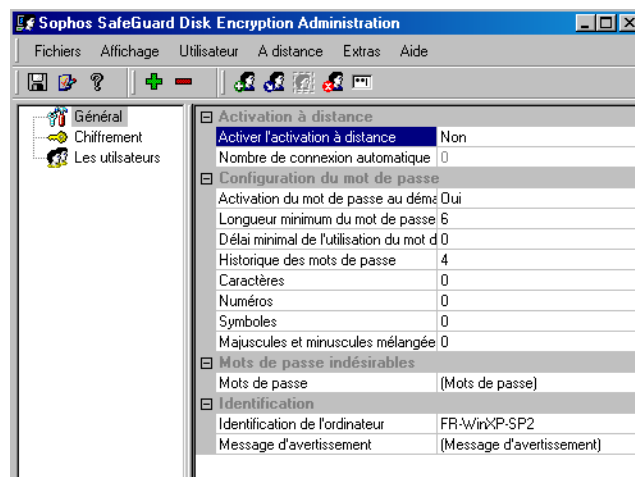


Le nombre de tentatives d'ouverture de session est limité à cinq.

Le système doit ensuite être redémarré pour essayer à nouveau d'ouvrir une session.

### 9.1 Fenêtre d'administration

Après saisie correcte des données d'utilisateur Sophos SafeGuard Disk Encryption, la fenêtre Administration apparaît.



Le volet de gauche présente une liste de toutes les pages de configuration disponibles. Si, dans la fenêtre de gauche, un fichier de configuration est sélectionné, des détails sur les possibilités de réglage sont affichés dans la partie de droite.

Les différentes possibilités de paramétrage correspondent à celles qui sont disponibles lors de l'installation de Sophos SafeGuard Disk Encryption avec les paramètres avancés.

La fenêtre d'administration affiche d'autres informations dans la zone du bas.

- Mode de chiffrement et état de chiffrement des lecteurs.
- État des touches pour le pavé numérique et la touche de mise en exposant.

## 9.2 Barre d'icônes et d'outils

L'utilitaire d'administration comporte une barre d'icônes avec des boutons pour les commandes les plus importantes (de gauche à droite) :



- **Enregistrer**  
Enregistre les nouveaux paramètres. Si des modifications de paramètres requièrent un redémarrage du système, une boîte de dialogue est affichée.
- **Poste de travail**  
Permet de retrouver l'utilitaire d'administration à la prochaine ouverture de session tel qu'il a été quitté (même taille/position de fenêtre, même page de configuration, etc.).
- **Aide**  
Affiche l'aide en ligne.
- **Signe plus/moins**  
Le signe plus affiche dans la fenêtre de droite tous les paramètres subalternes, le signe moins minimise la vue, ne laissant que les titres des rubriques.
- **Créer un utilisateur**  
Ajoute un nouvel utilisateur (affichage dépendant du profil des droits de l'utilisateur ayant ouvert la session).
- **Copier un utilisateur**  
Copie un utilisateur existant (affichage dépendant du profil des droits de l'utilisateur ayant ouvert la session).
- **Supprimer un utilisateur**  
Supprime un utilisateur de la liste (affichage dépendant du profil des droits de l'utilisateur ayant ouvert la session).

- **Modifier le mot de passe**

Permet à l'utilisateur ayant ouvert la session de modifier son mot de passe.

Toutes ces commandes peuvent être également appelées via les différents menus (Fichier, Affichage, Utilisateur, Outils, Aide).

## 10 L'assistant de configuration pour le déploiement

L'assistant de configuration pour le déploiement est utilisé pour créer des fichiers à l'aide desquels l'installation, la configuration et la désinstallation de Sophos SafeGuard Disk Encryption peuvent être automatisées. Des tâches administratives telles que la modification d'une installation Sophos SafeGuard Disk Encryption existante peuvent être résolues également via les fichiers de configuration. Dans les environnements réseau, l'administrateur envoie les fichiers de configuration aux ordinateurs des utilisateurs. Les fichiers sont exécutés sans intervention des utilisateurs. Une fois le même fichier de configuration exécuté sur plusieurs ordinateurs, Sophos SafeGuard Disk Encryption offre à même configurations sur ceux-ci.

Un fichier de configuration ne dépend pas d'un système particulier, c'est-à-dire qu'il peut être utilisé avec des systèmes autres que celui sur lequel il a été créé.

**Remarque :** Il faut que les outils d'administration sont installés pour créer un fichier de configuration. Les fichiers de configuration doivent être protégés contre les accès non autorisés. Les utilisateurs ordinaires ne doivent pas accéder aux fichiers de configuration.

### 10.1 Créer un nouveau fichier de configuration

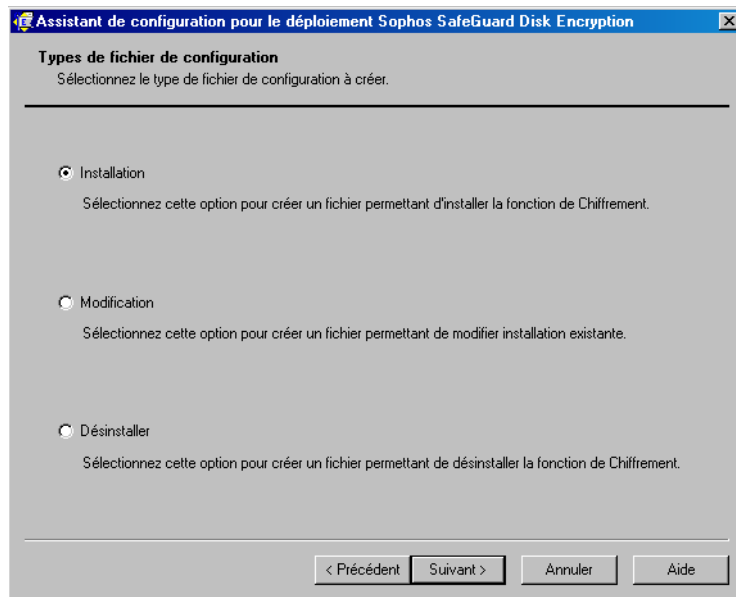
L'assistant de configuration pour le déploiement permet de créer des fichiers pour l'installation, la configuration et la désinstallation sans intervention de l'utilisateur. L'assistant de configuration pour le déploiement saisit successivement les informations nécessaires.

De nouveaux fichiers de configuration sont créés via **Démarrer \ Programmes \ Sophos \ SafeGuard Disk Encryption \ Assistant de configuration pour le déploiement**.

Validez toutes les entrées correctes dans l'assistant avec [Suivant].

Vous déterminez dans quel but le fichier de configuration est créé.

- Pour une installation
- Pour la modification d'une installation Sophos SafeGuard Disk Encryption existante (le dit fichier « Delta »)
- Pour une désinstallation



## 10.2 Création d'un fichier de configuration pour une installation

Le type de fichier « Installer » génère un fichier de configuration avec lequel Sophos SafeGuard Disk Encryption peut être automatiquement installé sur un client (voir [Installation centrale](#) sur page 22).

Une fois que les paramètres souhaités ont été définis dans l'assistant, un fichier de configuration est créé avec par défaut le nom `Install.cfg`.

Le fichier `Install.cfg` contient toutes les indications sur la configuration souhaitée sur l'ordinateur de destination. Il est chiffré et contient la clé (disques durs) et les mots de passe des utilisateurs.

### 10.2.1 Configuration de base

Indiquez si vous souhaitez utiliser une configuration de base pour le nouveau fichier de configuration.

Une configuration de base est un fichier de configuration existant. Il sert de modèle de base pour une nouvelle installation/configuration.

- Si vous voulez créer un fichier de configuration pour la première fois ou si vous voulez créer un nouveau fichier de configuration, simplement cliquez sur **Suivant**. Vous pouvez enregistrer les paramètres de configuration comme une configuration de base plus tard. Pour continuer, voir [Configuration de mots de passe et de chiffrement](#) sur page 47.

- Si un fichier de configuration est déjà disponible, vous pouvez sélectionner ce fichier ici pour l'utiliser comme une configuration de base. Après cliquez sur **Suivant**. Pour continuer, voir [Authentification du fichier de configuration](#) sur page 49.

The screenshot shows a window titled "Assistant de configuration pour le déploiement Sophos SafeGuard Disk Encryption". The main heading is "Fichier de configuration de base (facultatif)". Below it, the text reads: "Choisissez le fichier de configuration qui servira de base à ce fichier-ci." A horizontal line separates this from the next paragraph: "Si vous avez déjà enregistré ou déployé un fichier de configuration, vous pouvez le sélectionner ici et en faire le fichier de configuration de base." The following paragraph states: "Dans le cas contraire, vous pourrez enregistrer le nouveau fichier de configuration en tant que fichier de configuration de base." There is a checkbox labeled "Utiliser un fichier de configuration de base" which is currently unchecked. Below the checkbox is a text input field and a "Parcourir" button. At the bottom of the window, there are four buttons: "< Précédent", "Suivant >", "Annuler", and "Aide".

## 10.2.2 Configuration de mots de passe et de chiffrement

The screenshot shows a window titled "Assistant de configuration pour le déploiement Sophos SafeGuard Disk Encryption". The main heading is "Mots de passe". Below it, the text reads: "Indiquez les mots de passe correspondant à l'utilisateur du Système et à l'utilisateur par Défaut." A horizontal line separates this from the first section: "Utilisateur du Système". Below this, the text reads: "Définissez un mot de passe qui permettra à l'administrateur d'accéder aux différentes fonctions du système." There are two input fields: "Mot de passe :" and "Confirmer le mot de passe :". The second section is "Utilisateur par Défaut". Below this, the text reads: "Définissez un mot de passe qui permettra à l'utilisateur d'accéder aux données de son ordinateur." There are two input fields: "Mot de passe :" and "Confirmer le mot de passe :". At the bottom, there is a checkbox labeled "Afficher les paramètres avancés" which is unchecked. At the very bottom, there are four buttons: "< Précédent", "Suivant >", "Annuler", and "Aide".

Vous êtes invité à saisir et à confirmer des mots de passe pour les types d'utilisateur prédéfinis Sophos SafeGuard Disk Encryption d'utilisateur du système (SYSTEM) et d'utilisateur par défaut


(USER). Il s'agit des mots de passe qui permettront d'accéder l'ordinateur cible. Ils doivent respecter les règles de définition de mot de passe de Sophos SafeGuard Disk Encryption.

- Le mot de passe d'utilisateur par défaut (USER) est le mot de passe initial requis par l'utilisateur par défaut pour la connexion à l'ordinateur après l'installation de Sophos SafeGuard Disk Encryption. A la première ouverture de session l'utilisateur par défaut est invité à modifier ce mot de passe.
- Le mot de passe SYSTEM est requis par l'utilisateur du système. L'utilisateur du système est l'administrateur avec les droits administratives du niveau hiérarchique le plus élevé. Le mot de passe SYSTEM est requis pour les tâches d'administration et la modification des paramètres utilisateur.

**Remarque :** Veillez à conserver les mots de passe saisis.

Conservez le mot de passe SYSTEM en lieu sûr. En cas de perte de ce mot de passe, vous ne pourrez plus accéder aux ordinateurs des utilisateurs finaux.

Vous devez également créer un utilisateur du service d'assistance disposant des droits de réinitialisation des mots de passe. Pour cela, cochez la case **Afficher les paramètres avancés**. Cliquez sur **Suivant**.

Sous **Configuration du poste de travail**, sélectionnez **Utilisateurs**. Cliquez ensuite sur l'icône de création d'un utilisateur .

Dans le champ **Nouveau nom de l'utilisateur** de la boîte de dialogue **Nouvel utilisateur**, entrez le nom `Helpdesk`. Les fonctionnalités attribuées à l'utilisateur « Helpdesk » sont affichées. Définissez les options comme suit :

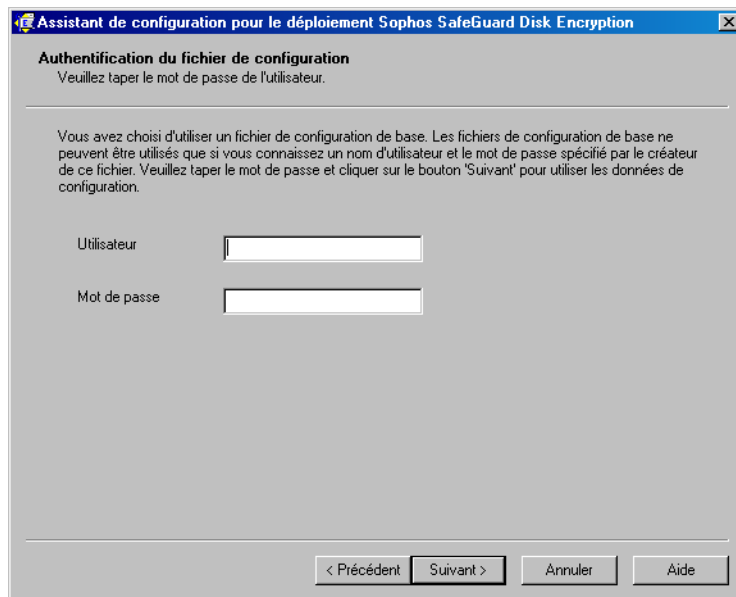
- **Génération d'un code C/R abrégé :** défini sur **Oui**.
- **Changement du mot de passe permis :** défini sur **Non**.
- **Mot de passe :** Cliquez sur **Mot de passe** et ensuite sur [...] pour configurer un mot de passe. Une boîte de dialogue est affichée. Entrez un nouveau mot de passe pour l'utilisateur « Helpdesk », puis confirmez-le.
- **Droits :** Cliquez sur **Droits** et ensuite sur [...]. Dans la boîte de dialogue **Droits de l'utilisateur**, double-cliquez sur la case **Modifier les paramètres d'utilisateurs** de manière à ce que l'utilisateur « Helpdesk » puisse définir un nouveau mot de passe utilisateur et autoriser une ouverture de session unique. Double-cliquez sur la case **Désinstaller** pour permettre à l'utilisateur « Helpdesk » de désinstaller SDE.

La configuration par défaut (chiffrement de la partition C:, l'authentification avant amorçage activée et connexion automatique sécurisé à Windows activée) est spécifié automatiquement. Pour modifier les paramètres de configuration par défaut choisissez **Afficher les paramètres avancés**.

### 10.2.3 Authentification du fichier de configuration

Les paramètres d'un fichier de configuration de base sélectionné ne deviennent pas visibles tant que l'utilisateur du système Sophos SafeGuard Disk Encryption SYSTEM ne s'est pas connecté.

Connectez vous comme l'utilisateur SYSTEM et tapez le mot de passe SYSTEM. La boîte de dialogue **Configuration du poste de travail** est affiché.

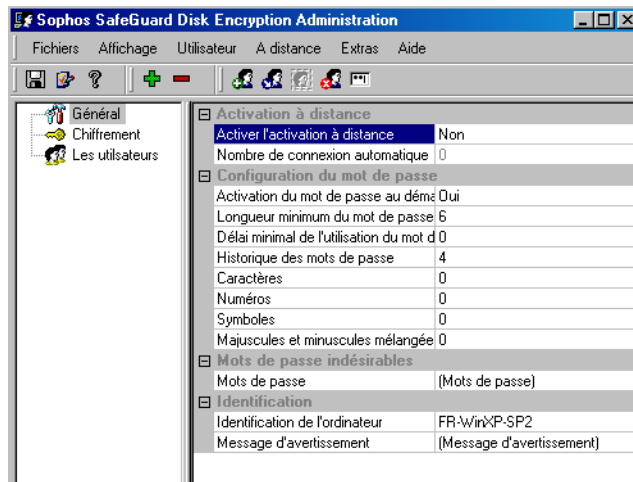


### 10.2.4 Afficher les paramètres avancés

Dans **Configuration du poste de travail** les différentes les pages de configuration sont affichées. Si vous utilisez un fichier de configuration de base, les paramètres sont affichés. Sinon les paramètres par défaut sont affichés.

Vous trouverez des informations plus détaillées sur les différentes pages de configuration dans les chapitres correspondants.

Faites vos changements et cliquez sur **Suivant**.



### 10.2.5 Enregistrer le fichier de configuration

Déterminez le chemin dans lequel vous souhaitez enregistrer le fichier de configuration `Install.cfg` que vous voulez utiliser comme une configuration de base ou acceptez l'emplacement par défaut.

Pour éviter les problèmes, notez toujours les propriétés et paramètres que vous attribuez à un fichier de configuration.

#### Changements du fichier de configuration de base :

Après choisir cette option, vous devrez indiquer si le fichier de configuration de base existant doit être remplacé ou non. Si vous cliquez sur **Oui**, le fichier est écrasé et les modifications seront ajoutées au fichier de configuration de base existant.

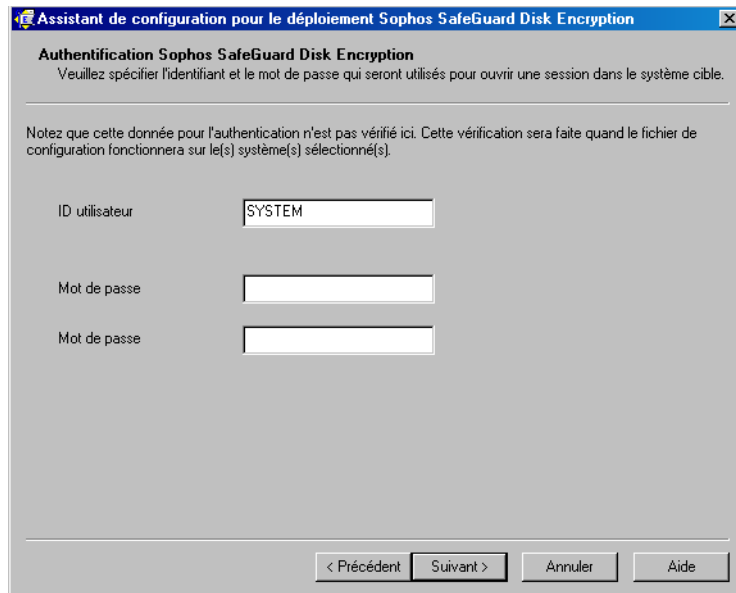
Pour ce faire, il suffit de renommer le fichier de configuration de base et de l'enregistrer sous un autre nom

## 10.3 Création d'un fichier de configuration pour une désinstallation

Choisissez le type de fichier **Désinstaller** pour générer un fichier de configuration avec lequel Sophos SafeGuard Disk Encryption peut être automatiquement désinstallé.

L'utilisateur entré ici doit exister sur le poste de travail et disposer du droit de désinstallation.

Lorsque vous avez entré votre ID utilisateur et le mot de passe, cliquez sur **Suivant**. La boîte de dialogue **Enregistrer les fichiers de configuration** est affichée. Entrez un nom et un emplacement pour le fichier du type **Désinstaller**.

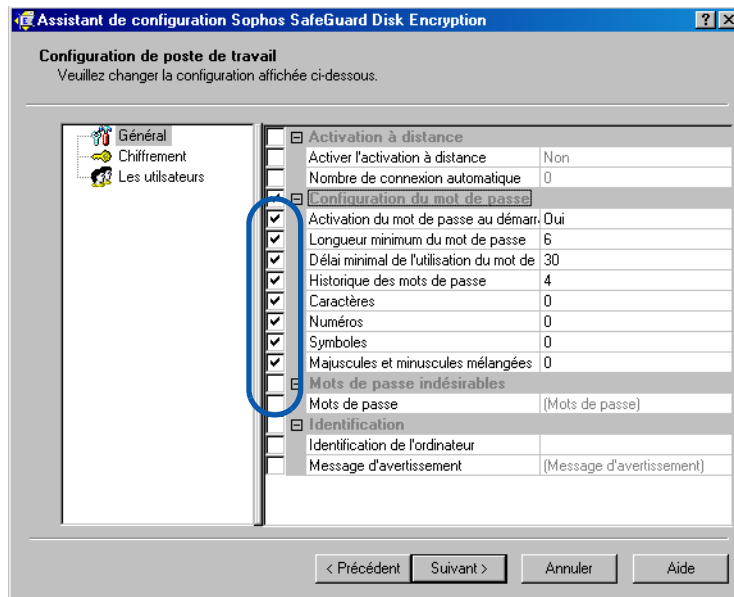


## 10.4 Création d'un fichier de configuration pour la modification (« fichier Delta »)

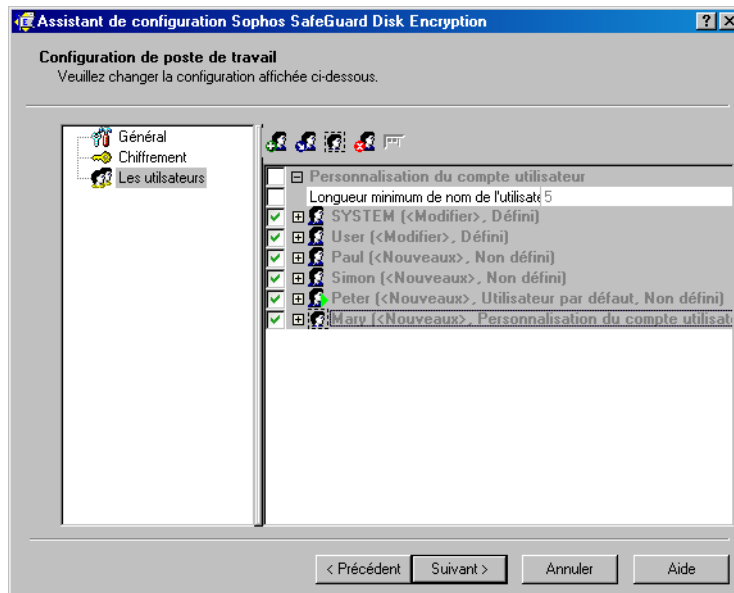
Choisissez le type de fichier **Modifier** pour générer un fichier de configuration avec lequel une configuration Sophos SafeGuard Disk Encryption existante peut être changée.




En bref, un fichier Delta modifie les paramètres d'une installation Sophos SafeGuard Disk Encryption existante. Comme un fichier d'installation, le fichier Delta peut être créé avec ou sans configuration de base.

Les options sur les différentes pages de configuration ne peuvent être traitées dans les fichiers Delta qu'une fois la case correspondante cochée.




A la page de configuration **Les utilisateurs**, veuillez noter les fonctionnalités des boutons de création, copie et suppression d'utilisateur.



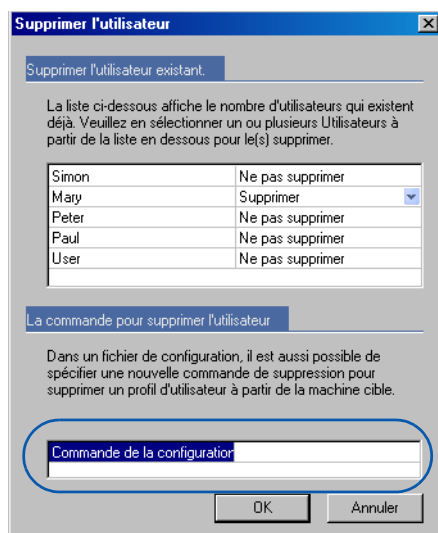
- **Créer un utilisateur**  : à l'exécution du fichier de configuration, crée un nouvel utilisateur Sophos SafeGuard Disk Encryption de ce nom (dans notre exemple *Simon*).
- **Copier un utilisateur**  : Tous les paramètres de l'utilisateur copié sont repris et le nouvel utilisateur de Sophos SafeGuard Disk Encryption reçoit également l'attribut « Créer ».
- **Modifier un utilisateur**  : Crée un utilisateur déjà existant sur un poste de travail lui attribue de nouvelles propriétés (dans notre exemple *User*, *Peter* et *Paul* avec l'attribut

« Modifier »).

Tous les utilisateurs chargés d'une configuration de base reçoivent automatiquement la propriété « Modifier ». Sans configuration de base, les utilisateurs doivent d'abord être créés avec cette propriété.

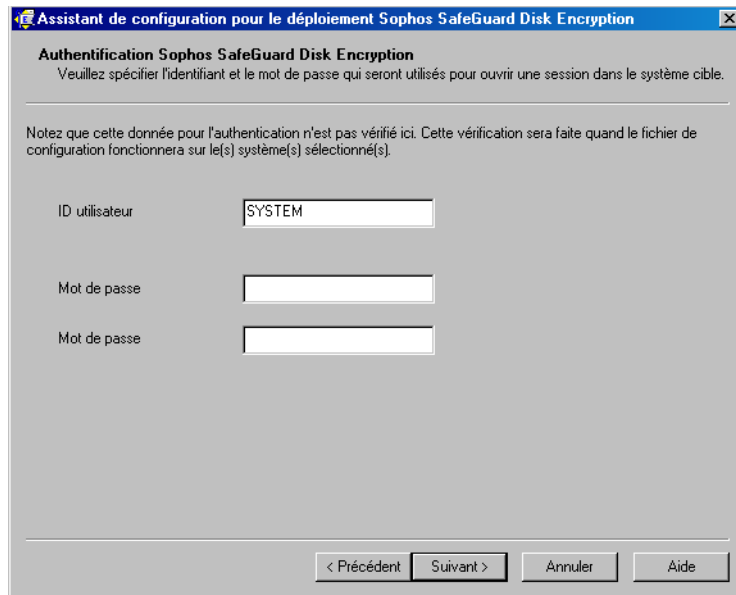
- **Supprimer un utilisateur**  : indique le nom d'un utilisateur existant qui va être supprimé à l'exécution du fichier de configuration sur ce système cible (dans notre exemple, l'utilisatrice *Mary*).

**Remarque :** Dans les fichiers Delta sans configuration de base, la propriété « Supprimer » doit être attribuée aux utilisateurs via le champ « Commande de configuration ».



Lorsque vous avez entré toutes les données, cliquez sur **Suivant**. L'Assistant ouvre la boîte de dialogue d'authentification.

L'utilisateur Sophos SafeGuard Disk Encryption spécifié ici doit exister sur le poste de travail sur lequel le fichier de configuration est exécuté et disposer des droits correspondants.



Lorsque vous avez entré toutes les données, cliquez sur **Suivant**. L'Assistant ouvre la boîte de dialogue **Enregistrer les fichiers de configuration**. Entrez un nom et un emplacement pour le fichier de configuration.

### 10.4.1 Exécuter le fichier Delta

Mode d'exécution du fichier delta :

1. Démarrez le mode MS DOS.
2. Accédez au répertoire où est installé Sophos SafeGuard Disk Encryption.
3. Tapez la commande suivante sur la ligne de commande:

```
EXECCFG.EXE /f :<chemin et nom du fichier de configuration >
```

**Ne laissez pas d'espaces entre « /f » et le nom de dossier du fichier delta !**

Tous les paramètres sont affichés avec la commande `EXECCFG.EXE /?`

EXECCFG prend en charge le paramètre `/Reboot`, qui entraîne l'arrêt après l'exécution avec succès du fichier de configuration défini.

**Exemple :**

```
C : \Programs\Sophos\Sophos SafeGuard Disk Encryption\EXECCFG /  
f :D : \Delta.cfg /Reboot
```

Cette commande vous permet alors d'appeler le fichier de configuration créé.

## 10.4.2 Éditer un fichier de configuration

Les paramètres des fichiers de configuration avec la propriété **Installer** peuvent être ultérieurement modifiés, même une fois enregistrés.

Pour modifier un fichier de configuration, veuillez procéder comme suit :

1. Démarrez l'assistant de configuration pour le déploiement.
2. Choisissez le type de fichier **Installer** et chargez le fichier à éditer dans la boîte de dialogue **Configuration de base**.
3. Vous chargez la configuration en cliquant sur **Suivant**.
4. Les paramètres qui y sont enregistrés sont affichés et peuvent être modifiés.
5. Si vous essayez d'appeler un fichier avec la propriété « Modifier » ou « Désinstaller », un message d'erreur est affiché.

## 10.5 Exemple d'application

Dans l'assistant de configuration pour le déploiement, créez un fichier permettant d'installer Sophos SafeGuard Disk Encryption sans intervention de l'utilisateur sur plusieurs postes de travail d'une entreprise. Le fichier de configuration doit prendre en outre en charge un concept d'administration hiérarchisé et comporter les profils d'utilisateur suivants :

- **SYSTEM** : administrateur Sophos SafeGuard Disk Encryption possédant tous les droits
- **SUBADMIN** : sous-administrateur auquel les tâches administratives ont été déléguées. Permet de modifier les paramètres utilisateur.
- **USER** : utilisateur final ne disposant d'aucun droit.

**Comment procéder :**

1. Démarrez l'assistant de configuration pour le déploiement.
2. Sélectionner le type de fichier de configuration **Installer**.

3. Ne pas choisir de configuration de base.
4. Entrez le mot de passe SYSTEM et choisissez **Afficher les paramètres avancés**.
5. Sous la rubrique **Général**, choisissez l'option **Activation du mot de passe au démarrage**.
6. Choisissez **Chiffrement > Disk dur chiffré**. Choisissez les partitions C: et D: pour le chiffrement.
7. Dans les paramètres d'utilisateur, choisir les paramètres suivants :
  - SYSTEM (mot de passe : System)  
Droits : tous
  - SUBADMIN (Subadmin)  
Génération d'un code C/R abrégé : Activee  
Droits : modifier les paramètres d'utilisateur
  - USER (User)  
Droits : aucun
8. Acceptez l'emplacement par défaut pour enregistrer le fichier de configuration de base `Install.cfg`.
9. Distribuer le fichier `Install.cfg`.

## 10.6 Génération d'un fichier de configuration à partir de la ligne de commande

Si vous souhaitez générer un fichier de configuration à partir de la ligne de commande, utilisez le programme `CfgWiz`. `CfgWiz` est situé dans le dossier Sophos SafeGuard Disk Encryption.

`CfgWiz` peut être appelé avec les paramètres suivants :

```
/cmd :install | change | uninstall
```

Cette option remplace la boîte de dialogue du type de fichier de configuration.

```
/base :<nom_fichier>
```

Cette option définit le nom de la configuration de base à utiliser. Lors de l'installation, cette option remplace la boîte de dialogue de configuration de base `CFGWIZ`. Dans le cas d'un fichier de modification, cette option remplace la boîte de dialogue pour sélectionner la configuration d'installation.

```
/instfile :<nom_fichier>
```

Cette option définit le nom du fichier d'installation à générer. Lorsque ce paramètre est actif, l'administrateur n'est pas invité à enregistrer. Si le fichier existe déjà, il sera remplacé par la nouvelle configuration.

```
/changefile :<nom_fichier>
```

Cette option définit le nom du fichier delta à générer. Lorsque ce paramètre est actif, l'administrateur n'est pas invité à enregistrer. Si le fichier existe déjà, il sera remplacé par la nouvelle configuration.

```
/uninstfile :<nom_fichier>
```

Cette option définit le nom de la configuration de désinstallation à générer en tant que sortie. Lorsque ce paramètre est actif, l'administrateur n'est pas invité à enregistrer. Si le fichier existe déjà, il sera remplacé par la nouvelle configuration.

**Exemple :**

```
CfgWiz /cmd :change /base :C :\install.cfg /changefile :C :\Change.cfg
```

## 11 Modification des paramètres de registre fréquemment utilisés via le modèle d'administration

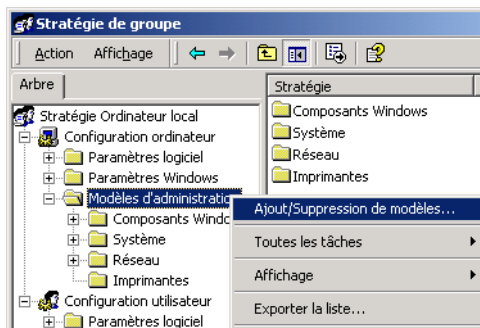
Pour améliorer le confort lors de la configuration, Sophos a généré un modèle d'administration spécifique pour l'éditeur de stratégies de groupes (Gpedit.msc). Ce modèle (nom de fichier : Sguard.adm) permet de définir confortablement certains paramètres Sophos SafeGuard Disk Encryption sans avoir à éditer le registre.

Un administrateur peut modifier les paramètres du modèle administratif pour le PC de l'utilisateur, soit localement, par l'intermédiaire de l'éditeur de stratégie de groupe (Gpedit.msc), soit centralement par l'intermédiaire des objets de stratégie de groupe (GPOs) dans un environnement Active Directory. Les utilisateurs dans un environnement informatique n'ont normalement pas de droits d'administrateur et ne peuvent par conséquent pas modifier eux-mêmes les stratégies Sophos SafeGuard Disk Encryption.

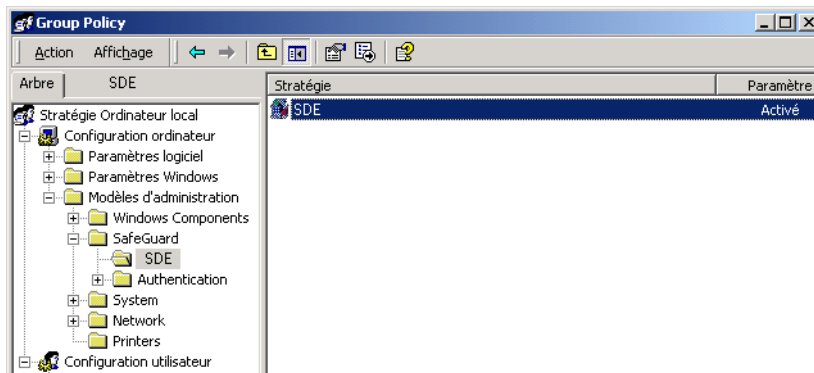
Vous trouverez ci-dessous des instructions brèves sur la manière d'intégrer le modèle Sophos dans un système local. Pour la manipulation de modèles d'administration dans un environnement avec OSG, veuillez consulter la documentation Microsoft usuelle.

1. Ouvrir une session comme utilisateur avec droits d'administrateur Windows
2. Cliquez sur Démarrer \ Exécuter, tapez la commande `gpedit.msc` et ouvrez l'éditeur de stratégies de groupes local.
3. Ajouter modèle SafeGuard `Sguard.adm` via **Modèles d'administration** > **Ajout/Suppression de modèles**.

`Sguard.adm` se trouve dans le répertoire d'installation Sophos SafeGuard Disk Encryption, dans le dossier `\ADM`.



4. Outre les dossiers précédents, le dossier « SafeGuard » apparaît dans la rubrique Configuration ordinateur de la MMC.



5. Avec les modèles non Windows, la vue préalablement configurée pose un problème. Par conséquent, le paramètre suivant doit être désactivé pour les stratégies individuelles :

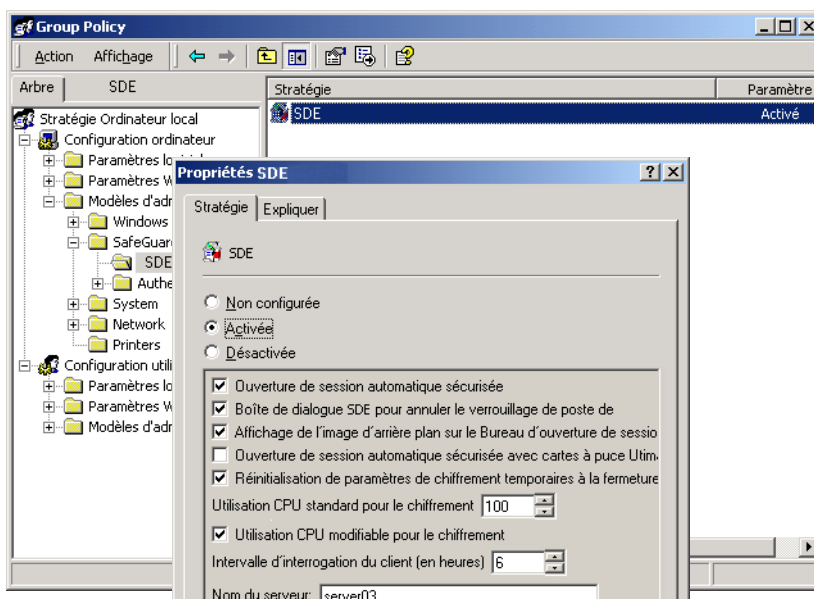
*Windows 2000 :*

Sélectionnez **Modèles administratifs**, sélectionnez le menu **Affichage** et désactivez **Afficher uniquement les stratégies**.

*Windows XP :*

Sélectionnez **Modèles administratifs**, sélectionnez le menu **Affichage**, puis **Filtrage** et désactivez **N'afficher que les paramètres de stratégie pouvant être entièrement gérés**.

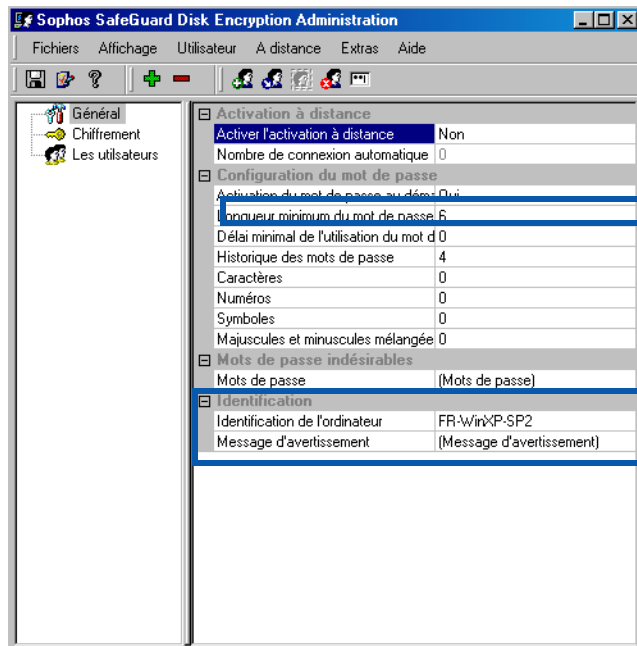
6. Double-cliquer sur la stratégie pour l'ouvrir et procéder aux réglages à la page des **Propriétés de SDE**.



Les stratégies peuvent avoir trois états différents :

- **Non configurée**  
Les paramètres actuels chez l'utilisateur ne sont pas modifiés, c'est-à-dire que le réglage effectué précédemment demeure.
- **Activé**  
Les paramètres sont transférés.
- **Désactivé**  
Les paramètres sont supprimés.

## 12 Authentification avant l'amorçage (PBA)



La fonction Pre-Boot Authentication (PBA) est la fonction Sophos SafeGuard Disk Encryption qui requiert une authentification avant l'amorçage. Pour plus amples informations sur l'authentification avant amorçage, voir [Démarage du système et ouverture de session](#) sur page 34.

Vous pouvez spécifier les paramètres PBA sur la page de configuration Général.

### 12.1 Vous pourrez modifier la langue choisie ultérieurement

L'écran de connexion applique la langue sélectionnée pendant l'installation (Français, Anglais ou Allemand). Les utilisateurs n'ont pas à désinstaller Sophos SafeGuard Disk Encryption pour afficher le texte d'authentification avant le démarrage dans une autre langue.

**Avis :** Vous pouvez seulement modifier ultérieurement l'affichage des textes sur l'écran PBA, pas la composition du clavier.

#### Paramètres de changement de langue

Vous pouvez lancer SetPBALang avec les paramètres suivants :

```
SetPBALang [en | de | fr] | [n]
```

[en | de | fr]      Définit la nouvelle langue

[n] Utilise un numéro (1-255) pour le réglage de la langue  
Les langues suivantes sont proposées :  
9=Anglais  
7=Allemand  
12=Français

Le réglage de la langue prend effet après le redémarrage.

Vous trouverez SetPBALang dans le répertoire programme de Sophos SafeGuard Disk Encryption.

## 12.2 Activation du mot de passe au démarrage du système

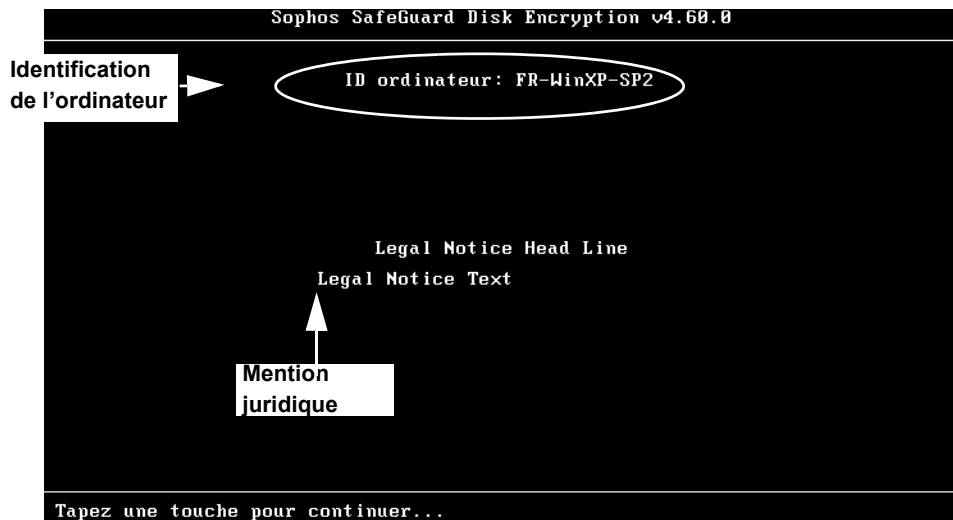
L'option « Activation du mot de passe au démarrage » active/désactive l'authentification avant amorçage (PBA). Si la PBA est activée, un écran d'ouverture de session apparaît avant le chargement du système d'exploitation. Windows ne démarre qu'une fois l'authentification effectuée avec les données d'accès Sophos SafeGuard Disk Encryption correctes.

Si vous désactivez la fonction PBA, une ouverture de session avant le démarrage du système n'est pas nécessaire. L'authentification s'effectue alors comme d'habitude via la boîte de dialogue d'ouverture de session du système d'exploitation. Mais sans PBA le niveau de sécurité de l'ordinateur est plus faible.

**Avis :** Pour des raisons de sécurité, il est conseillé de ne pas désactiver l'authentification avant amorçage (PBA), parce que le système autrement redémarre sans entrée du mot de passe.

## 12.3 Identification de l'ordinateur

Les options sous **Identification** permettent d'afficher dans la PBA des textes définissables.



### 12.3.1 Spécifier l'identification de l'ordinateur

Le texte entré dans ce champ apparaît dans la boîte de dialogue d'ouverture de session de la PBA. Vous pouvez, par exemple, spécifier un nom exact pour votre station de travail dans ce champ, ce qui vous permet d'identifier l'ordinateur avec précision. Si un nom d'ordinateur est déjà défini par les paramètres réseau de Windows, il est transféré de façon automatique.

Vous pouvez taper un maximum de 63 caractères.

L'identification de machine peut également contenir des liens avec des variables d'environnement. Ces liens sont convertis à l'installation. Ceci est utile en particulier lors de la création de fichiers de configuration, installés sur plusieurs postes de travail.

#### Exemple :

L'entrée dans le champ « *Identification de la machine* » *Ceci est %USERDOMAIN%.*

L'amorçage est effectué de *%WINDIR%*

devient « *Le PC1234 démarre à partir de C:\WINNT* »

pendant l'installation.

Pour tous les systèmes d'exploitation, il existe la variable spéciale *%COMPUTERNAME%*.

Le nom de l'ordinateur est intégré avec cette variable, indépendamment de la plate-forme.

La variable *%COMPUTERNAME%* est toujours convertie dans le nom NETBIOS de l'ordinateur.

Les règles suivantes sont en outre valables :

- Les variables d'environnement non définies génèrent des liens vides.
- Quand la variable dans le champ d'identification de la machine est trop longue, elle est convertie en « [...] ».
- Pour les noms de variables, il n'est pas nécessaire de respecter la casse (majuscules/minuscules).
- Quand un signe de pourcentage est nécessaire dans le lien, utilisez « %% ».
- La conversion de variables n'est exécutée qu'une seule fois au moment de l'installation, pas à chaque démarrage de l'ordinateur.

### 12.3.2 Zone de texte pour le message d'avertissement

Vous pouvez librement configurer le contenu d'une zone de texte pour PBA. Dans certains pays, l'affichage d'un champ de texte d'un contenu donné est prescrit par le législateur. Le titre peut contenir jusqu'à 68 caractères et le bloc des textes peut contenir jusqu'à 10 lignes avec 70 caractères chacune.

La zone de texte de contenu librement configurable est affichée avant l'ouverture de session avec les données Sophos SafeGuard Disk Encryption. Les données doivent être confirmées par l'utilisateur avant que le système poursuive.

## 13 Chiffrement

La fonction principale de Sophos SafeGuard Disk Encryption est le chiffrement des données sur les disques durs.

Pour le chiffrement, l'algorithme AES-256 est disponible. Selon sa définition de la loi du hasard, la clé est chiffrée et non stockée dans le système pour des raisons de sécurité. A chaque amorçage du système, elle est générée de nouveau à partir d'un code enregistré sur le disque dur et du mot de passe Sophos SafeGuard Disk Encryption de l'utilisateur.

Seules les zones du système ou des partitions isolées, ou encore un maximum de quatre disques durs, peuvent être chiffrés. Le nombre de partitions d'un disque dur est limité à huit. Les systèmes de fichiers suivants sont pris en charge : FAT-32 et NTFS.

Pour disposer d'une solution de sécurité des données encore plus professionnelle, nous recommandons la solution de sécurité des données SafeGuard Enterprise, structurée de façon modulaire. SafeGuard Enterprise prend notamment en charge le chiffrement de supports amovibles.

### 13.1 Lecteurs pris en charge

Les disques durs suivantes sont pris en charge pour le chiffrement :

- Disques durs IDE/SCSI
- Disques durs ATA série (« connectables à chaud »)
- Disques durs Firewire (« connectables à chaud »)
- Disques durs USB (« connectables à chaud »)

### 13.2 Chiffrement de disques durs

Veillez noter l'informations suivantes relative au chiffrement de disques durs:

#### **Disques durs connectables à chaud**

- Tous les disques durs qui doivent être chiffrés doivent être déjà connectés à l'ordinateur à l'installation de Sophos SafeGuard Disk Encryption.
- Le premier chiffrement de disques durs connectables à chaud ne doit pas être interrompu !
- Les disques durs connectables à chaud doivent rester connectés même au premier redémarrage après le premier chiffrement. Après le premier chiffrement, le lecteur peut être connecté et déconnecté selon les besoins. Il est nécessaire que l'utilisateur se serve toujours du même disque dur, par ex. pour les sauvegardes régulières des données. Cela se déroule généralement sans problème.

- Si plusieurs disques durs sont utilisés (par ex. déconnexion d'un disque dur chiffré et connexion d'un disque dur non chiffré), des problèmes peuvent survenir à la suite par ex. d'incohérences dans le tableau de chiffrement Sophos SafeGuard Disk Encryption.
- Règle générale : La numérotation du disque (DiskManagement) utilisé doit correspondre à la numérotation pendant la procédure d'installation ou le premier chiffrement.

Les restrictions citées ne valent pour les disques durs ATA série uniquement lorsqu'ils sont utilisés comme disques durs connectables à chaud.

### **Divers types de disque dur**

Évitez si possible de mélanger plusieurs types de disque dur (IDE/SCSI) sur un système.

### **Disques durs supplémentaires**

Sophos SafeGuard Disk Encryption reconnaît automatiquement le nombre de disques durs de votre ordinateur. Après l'installation de Sophos SafeGuard Disk Encryption, aucun disque dur supplémentaire ne doit être intégré dans le système. Si vous souhaitez intégrer un disque dur supplémentaire dans votre système, vous devez d'abord désinstaller entièrement Sophos SafeGuard Disk Encryption. Après la désinstallation, vous intégrez le nouveau disque dur et vous réinstallez le programme.

### **Repartitionnement**

- Si un disque dur a été repartitionné, un redémarrage doit être effectué AVANT l'installation de Sophos SafeGuard Disk Encryption.
- Veuillez ne plus modifier le partitionnement du disque dur après le chiffrement. Ceci peut entraîner la perte de données.

### **Clé**

Une seule clé de disque dur est définie, indépendamment du nombre de disques durs.

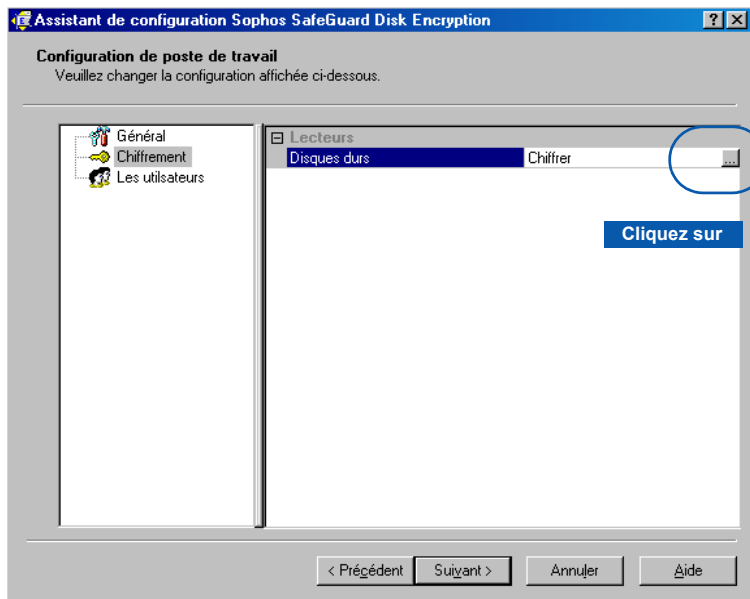
## **13.3 Configuration du chiffrement**

Les paramètres de chiffrement sont définis dans l'Administration Sophos SafeGuard Disk Encryption ou dans l'Assistant Fichier de configuration.

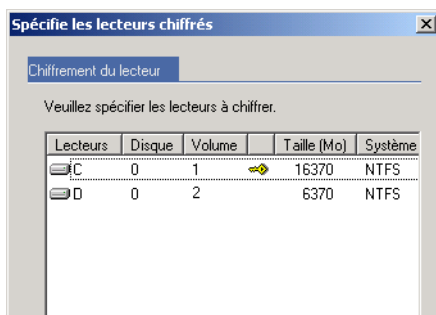
La partition C: est toujours chiffrée par défaut. Ce paramètre est spécifié automatiquement.

Procédez comme suit pour chiffrer autres disques durs.

1. Cliquez sur **Disques durs** dans la rubrique **Lecteurs**. Après cliquez sur [...].



2. La boîte de dialogue Spécifie les lecteurs chiffrer s'ouvre.



3. La clé symbolique indique que le chiffrement est activé pour le lecteur/la partition.

Pour activer le chiffrement pour autres partitions, double-cliquez sur la lettre de lecteur correspondante.

Si vous voulez désactiver le chiffrement, double-cliquez de nouveau sur les lettres des lecteurs. La clé symbolique disparaît et le chiffrement est désactivé.

## 13.4 Clés

Seul un utilisateur avec une authentification correcte peut accéder aux lecteurs chiffrés. Une clé se compose d'une série de caractères (nombres, lettres, caractères spéciaux) et, tout comme un mot de passe, elle est soumise à certaines règles.

### 13.4.1 Clés et type de algorithme

Sophos SafeGuard Disk Encryption prend en charges des clés aléatoires. Une clé aléatoire a toujours une longueur de 32 octets (256 bits).

Sophos SafeGuard Disk Encryption prend en charge l'algorithme AES-256. L'algorithme de chiffrement Advanced Encryption Standard (AES) remplace l'algorithme DES. Le National Institute for Standards and Technology américain (NIST) a opté pour l'algorithme Rijndael, un algorithme de chiffrement sécurisé et très rapide, pour l'AES-256. L'AES-256 fonctionne avec une clé 256 bits et une longueur de bloc de 128 bits.

Ci-après, vous trouverez une liste de tous les algorithmes utilisables avec leurs normes correspondantes :

| Algorithme | Longueurs de clés    |
|------------|----------------------|
| AES-256    | 32 octets (256 bits) |

### 13.4.2 Gestion de clés

La gestion des clés Sophos SafeGuard Disk Encryption enregistre les clés de façon sûre. Toutes les clés sont conservées dans un domaine chiffré du noyau système Sophos SafeGuard Disk Encryption, chiffrées avec une clé de chiffrement, à savoir la clé « KEK » (pour **K**ey **E**ncryption **K**ey). La KEK proprement dite n'est pas mémorisée sur le disque dur, mais créée à partir du mot de passe Sophos SafeGuard Disk Encryption.

**Si la PBA est active**, les clés ne sont créées pour le déchiffrement des lecteurs que lorsque les données Sophos SafeGuard Disk Encryption correctes ont été saisies dans la PBA.

**Si la PBA est désactivée**, les clés sont chiffrées et mémorisées sur le disque dur. Le chiffrement et la gestion des clés sont malgré cela absolument identiques à la sélection « PBA activée ». L'utilisation du mot de passe (ou du Scan Code) ne l'est pas. Sans attendre au niveau de la PBA que l'utilisateur tape manuellement son nom d'utilisateur et son mot de passe, Sophos SafeGuard Disk Encryption dispose de ces données. A cet effet, Sophos SafeGuard Disk Encryption crée – toujours quand la PBA est désactivée – un utilisateur ('\*AUTOUSER') et lui attribue un mot de passe aléatoire.

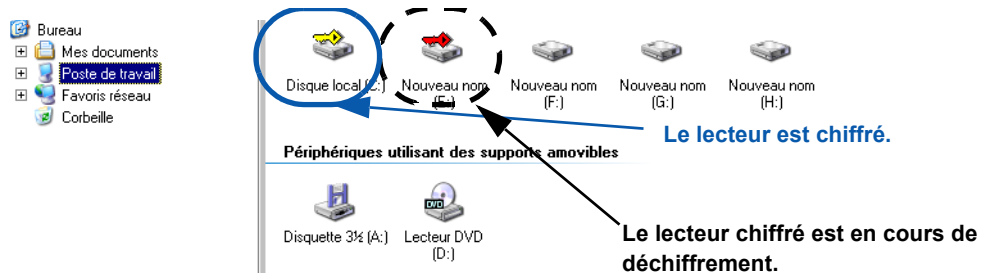
Partagé en différents éléments,, ce mot de passe est stocké dans le noyau Sophos SafeGuard Disk Encryption. A l'amorçage, Sophos SafeGuard Disk Encryption est en mesure d'en restaurer le mot de passe complet (ou à proprement parler la séquence du Scan Code complète).

## 13.5 Affichage de l'état de chiffrement dans l'Explorateur Windows

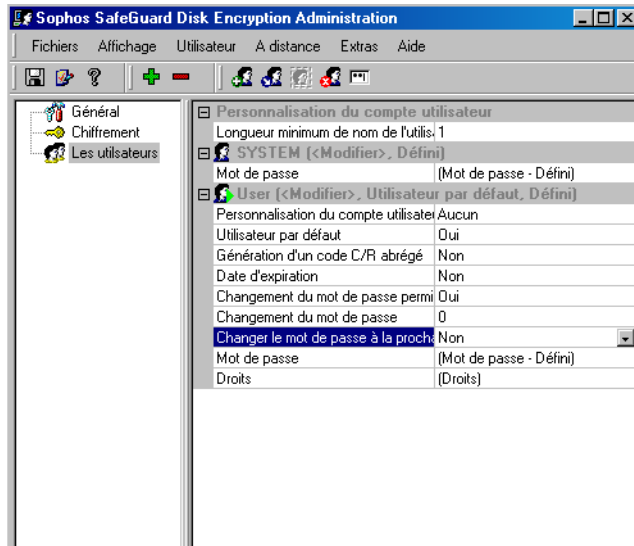
L'état de chiffrement des lecteurs est indiqué dans l'Explorateur Windows par une clé en couleur.

Une clé jaune indique qu'un lecteur est chiffré.

Une clé rouge signifie qu'un lecteur chiffré est en cours de déchiffrement (ou inversement).



## 14 Création de profils utilisateur



Vous déterminez ici les utilisateurs autorisés à travailler sur un poste de travail protégé par Sophos SafeGuard Disk Encryption. Vous pouvez créer ici de nouveaux utilisateurs Sophos SafeGuard Disk Encryption, modifier des utilisateurs existants ou supprimer des utilisateurs inutiles. Vous déterminez en outre de quels droits et pouvoirs complémentaires les utilisateurs Sophos SafeGuard Disk Encryption définis disposent.

Sophos SafeGuard Disk Encryption autorise l'accès au système pour 16 utilisateurs (\*AUTOUSER inclus) au maximum. SYSTEM et USER sont définis par défaut, l'utilisateur SYSTEM ne devant jamais être supprimé.

**Remarque :** L'assistant de configuration pour le déploiement ne montre que SYSTEM et USER si un fichier avec la propriété « Installer » est créé ou quand une configuration de base est utilisée.

Pour plus d'informations à la création d'un utilisateur HELPDESK voir [Configuration de mots de passe et de chiffrement](#) sur page 47 ou l'article suivant de la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/56457.html>.

### 14.1 Détermination de tâches d'administration

Une distinction est faite entre les utilisateurs avec tâches d'administration et les utilisateurs sans tâches d'administration.

Les utilisateurs avec tâches d'administration sont

- l'administrateur du système et

- les utilisateurs disposant de fonctions d'administrateur

La personne sans tâches d'administration est

- l'utilisateur.

La fonction d'administrateur peut être séparée de la fonction d'utilisateur, mais également y être associée. Les tâches d'administration peuvent être exécutées par une ou plusieurs personnes. Sophos SafeGuard Disk Encryption peut par conséquent configurer un ou au maximum 16 utilisateurs (\*AUTOUSER inclus).

Selon l'organisation, il peut être toutefois utile de créer un système de rôles à plusieurs niveaux, l'administrateur ou le sous-administrateur du système pouvant disposer de droits différents. La structure hiérarchique ci-dessous est imaginable :

### **Administrateur du système (l'utilisateur du système)**

Seul l'administrateur du système est en droit d'exécuter toutes les fonctions du programme. Il peut définir un assistant et lui octroyer certains droits d'administration. L'administrateur du système ne doit jamais oublier son mot de passe. Il doit le noter et le conserver dans un endroit sûr.

### **Sous-administrateur du système**

Les sous-administrateurs du système, par exemple personnel du service d'assistance, peuvent aider l'utilisateur, quand celui-ci a par ex. oublié son mot de passe. Dans quelle mesure un sous-administrateur peut assister l'administrateur du système dépend des droits qui lui sont octroyés au préalable.

Pour plus d'informations à la création d'un utilisateur « Helpdesk » voir [Configuration de mots de passe et de chiffrement](#) sur page 47 ou l'article suivant de la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/56457.html>.

### **Utilisateurs**

L'utilisateur ne peut que visionner ses paramètres. Il ne peut exécuter de façon autonome que la modification du mot de passe d'utilisateur. L'administrateur du système peut en outre lui octroyer certains droits.

## **14.2 Utilisateurs prédéfinis**

Sophos SafeGuard Disk Encryption fournit les profils d'utilisateurs prédéfinis suivants :

- SYSTEM
- USER
- \*AUTOUSER

### 14.2.1 L'utilisateur SYSTEM

Cet utilisateur du système (administrateur) est le seul à posséder les droits du niveau hiérarchique le plus élevé. Il ne peut pas modifier ses propres paramètres. Personne ne peut le supprimer ni l'administrer. L'utilisateur SYSTEM est le seul à pouvoir modifier les paramètres de tous les autres profils d'utilisateurs. Seul le responsable au niveau supérieur de la sécurité du système doit par conséquent pouvoir ouvrir une session avec le nom d'utilisateur SYSTEM. Le mot de passe de l'utilisateur SYSTEM ne doit être connu que du responsable au niveau supérieur de la sécurité. Il doit noter ce mot de passe et le conserver p.ex. dans un coffre-fort.

### 14.2.2 Utilisateur USER

Comme l'utilisateur SYSTEM, l'utilisateur USER est automatiquement présent après une installation de Sophos SafeGuard Disk Encryption. Ce profil d'utilisateur dispose seulement du droit à changer le mot de passe et peut être supprimé à tout moment.

### 14.2.3 Utilisateur \*AUTOUSER


L'utilisateur \*AUTOUSER est particulier. Sophos SafeGuard Disk Encryption crée – toujours quand la PBA est désactivée – un utilisateur (\*AUTOUSER) et lui attribue un mot de passe aléatoire. Partagé en différents éléments, ce mot de passe est stocké dans le noyau Sophos SafeGuard Disk Encryption. A l'amorçage, Sophos SafeGuard Disk Encryption est en mesure de restaurer le mot de passe complet et d'exécuter l'ouverture de session.

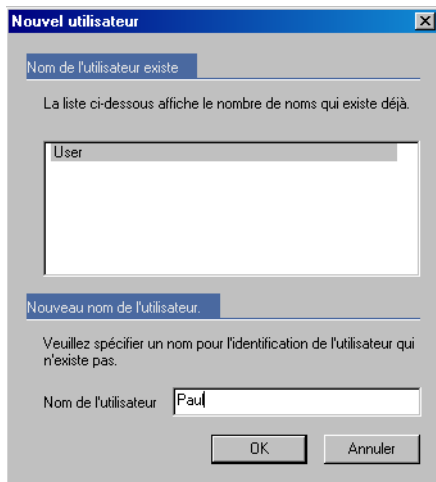
Par défaut, \*AUTOUSER n'a aucun droit.

Quand la PBA est désactivée, tous les utilisateurs ouvrent la session avec les droits octroyés sur le système à l'utilisateur \*AUTOUSER. Quand la PBA est de nouveau activée, \*AUTOUSER disparaît de la liste des utilisateurs.

## 14.3 Création d'utilisateurs

Un nouveau profil d'utilisateur est créé dans la boîte de dialogue **Configuration du poste du travail** dans les programmes d'administration via la page de configuration « Utilisateur.


Après un clic sur l'icône pour la création d'un nouvel utilisateur , la boîte de dialogue **Nouvel utilisateur** s'ouvre.

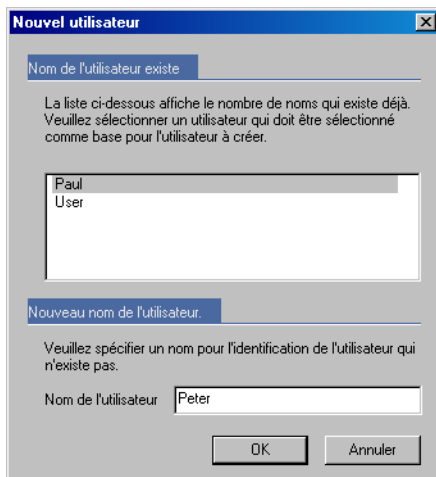


Donnez un nom au nouvel utilisateur en tapant une désignation dans le champ de saisie. Le nom du nouvel utilisateur ne doit pas dépasser **16 caractères** au maximum. Si le nom est déjà attribué, un message d'erreur s'affiche. Par défaut, le nouveau profil ne dispose d'aucun droit. Pour l'attribution de droits, voir [Droits utilisateur](#) sur page 77.

## 14.4 Copie d'un utilisateur

Les profils d'utilisateurs similaires peuvent être copiés, puis modifiés si besoin est. Ceci permet de gagner du temps.

Après un clic sur l'icône pour la copie d'un nouvel utilisateur , la boîte de dialogue Copier utilisateur s'ouvre.



Dans la liste d'utilisateurs, sélectionnez le profil que vous souhaitez copier. Tous les profils faisant partie de votre domaine d'administration s'affichent. Vous pouvez cependant ne copier que les profils possédant un niveau hiérarchique inférieur à votre propre profil.


L'utilisateur SYSTEM ne peut pas être copié.

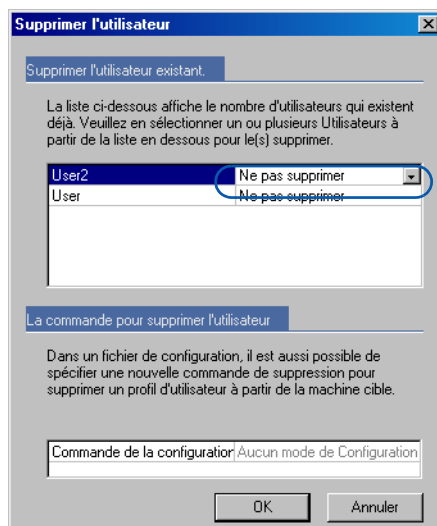
Attribuez un nouveau nom à l'utilisateur et cliquez sur OK pour confirmer le nom. Si le nom est déjà attribué, un message d'erreur s'affiche.

Vous pouvez ensuite modifier le nouveau profil à votre convenance.

## 14.5 Suppression d'un utilisateur

Les profils d'utilisateurs devenus inutiles peuvent être supprimés.

Après un clic sur l'icône pour la suppression d'un utilisateur , la boîte de dialogue **Supprimer l'utilisateur** s'ouvre.



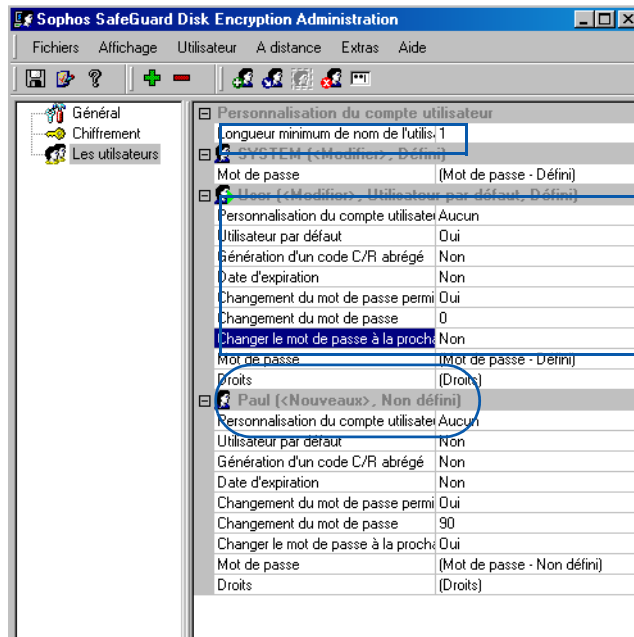
Dans la liste d'utilisateurs, sélectionnez le profil d'utilisateur que vous souhaitez supprimer. Tous les profils faisant partie de votre domaine d'administration s'affichent. Ouvrez le menu déroulant derrière le nom d'utilisateur et choisissez la propriété **Supprimer** correspondant au nom d'utilisateur à supprimer.

Vous pouvez cependant ne supprimer que les profils possédant un niveau hiérarchique inférieur à votre propre profil.

La suppression d'un utilisateur est irréversible.

## 14.6 Caractéristiques d'utilisateur

Les droits attribués à un utilisateur sont affichés près de son nom.



### 14.6.1 Longueur minimum du nom de l'utilisateur

Dans ce champ, vous indiquez le nombre minimum de caractères que doit comporter un nom d'utilisateur. Vous pouvez saisir le nombre souhaité des caractères soit directement, soit en augmentant ou diminuant la valeur à l'aide des touches de direction. La valeur pour la longueur du mot de passe peut se situer entre un et 16 caractères.

### 14.6.2 Utilisateur par défaut (mot de passe uniquement)

Un utilisateur de Sophos SafeGuard Disk Encryption peut être défini comme utilisateur par défaut, à l'exception de l'utilisateur SYSTEM. Pour se connecter, l'utilisateur par défaut doit seulement entrer le mot de passe Sophos SafeGuard Disk Encryption. Si d'autres utilisateurs que l'utilisateur par défaut souhaitent se connecter au poste de travail, ils doivent activer la fonction de « connexion étendue » (pendant la phase PBA, en appuyant sur F2).

### 14.6.3 Personnalisation du compte utilisateur

Les modèles ont une fonction bien particulière. Ils sont en règle générale utilisés quand Sophos SafeGuard Disk Encryption doit être installé sur plusieurs ordinateurs avec un fichier de configuration. S'il n'existait pas de modèles, les utilisateurs posséderaient le même ID d'utilisateur sur tous les ordinateurs. Ceci va cependant à l'encontre, dans de nombreux cas, des directives en matière d'organisation dans de nombreuses entreprises, exigeant la présence de nom/mots de passe d'utilisateur individuels, p.ex. nom, code personnel, etc. Dans de tels environnements, un profil d'utilisateur Sophos SafeGuard Disk Encryption peut être alors défini comme modèle. Il en résulte que cet utilisateur de Sophos SafeGuard Disk Encryption reçoit un nouveau nom d'utilisateur, par conséquent personnalisé, à la première ouverture de session avec PBA.

Un modèle peut servir soit à renommer, soit à copier un utilisateur.

Un modèle est utilisée comme suit :

L'administrateur crée un utilisateur Sophos SafeGuard Disk Encryption et le définit comme modèle. Sophos SafeGuard Disk Encryption est installé avec ces paramètres sur l'ordinateur de destination. Le nom d'utilisateur et le mot de passe de l'utilisateur défini comme modèle sont indiqués par l'administrateur à l'utilisateur de l'ordinateur de destination à la première ouverture de session. Quand un utilisateur ouvre alors une session pour la première fois, il est tenu d'entrer ces données d'accès sur l'écran d'ouverture de session. Il est ensuite invité à entrer son nouveau nom d'utilisateur et son nouveau mot de passe avec lesquels il devra également se connecter à la prochaine ouverture de session.

#### **Renommer un modèle**

Si vous souhaitez absolument vous assurer qu'un seul utilisateur par modèle ouvre une session sur (p.ex. ordinateurs portables pour collaborateurs des services extérieurs), attribuez au modèle la propriété « Renommer ». Le modèle est « écrasé » avec les nouvelles données d'utilisateur. Une ouverture de session avec les données d'accès connus n'est plus possible, celles-ci ayant été remplacées par celle de l'utilisateur connecté.

#### **Copier un modèle**

Si l'attribut « Copier » est sélectionné, le nouveau nom d'utilisateur est ajouté à la liste des utilisateurs de Sophos SafeGuard Disk Encryption, mais le modèle reste conservé. Les autres utilisateurs peuvent ouvrir une session avec les données d'accès du modèle. Si SYSTEM et UTILISATEUR sont définis par défaut, 13 autres utilisateurs peuvent être également créés. **Pour des raisons de sécurité, il est conseillé de n'utiliser les modèles qu'avec la fonction « Renommer ».**

### 14.6.4 Date d'expiration

La date d'expiration indique la durée de validité maximum d'un profil d'utilisateur Sophos SafeGuard Disk Encryption. Vous pouvez spécifier un jour de référence (ou une période) auquel l'utilisateur pourra ouvrir une dernière session dans le système. Vous pouvez taper directement la date ou la période.

Ce paramètre est notamment utile dans les cas où l'utilisation d'un poste de travail n'est prévue que pour un certain temps, p.ex. employés temporaires ou étudiants, etc. Une fois le délai écoulé, le poste de travail est verrouillé pour l'utilisateur.

Ce paramètre n'a aucun effet sur l'utilisateur SYSTEM.

## 14.7 Droits utilisateur

Réfléchissez aux droits d'accès susceptibles d'être octroyés aux différents utilisateurs de Sophos SafeGuard Disk Encryption, par exemple pour personnel du service d'assistance. Pour des raisons de sécurité, l'attribution des droits pour les différents utilisateurs doit être mûrement réfléchie.

Vous pouvez autoriser à des utilisateurs l'accès à des paramètres temporaires et permanents. Les paramètres temporaires ne sont valables que pour la durée d'une ouverture de session. Après un redémarrage de l'ordinateur, ils ne sont plus valides et les paramètres du système sont rétablis. Les paramètres permanents sont ceux qui restent conservés même après redémarrage du système.

Les droits suivants peuvent être octroyés :

|  |  |
|--|--|
| <b>Modifier les paramètres de chiffrement</b>          | Permet de modifier l'état de chiffrement et les clés.  |
| <b>Modifier les règles de mot de passe</b>             | Permet de modifier les règles générales des mots de passe.   |
| <b>Modifier les paramètres de l'utilisateur</b>        | Permet de modifier les paramètres des utilisateurs.<br>Doit être défini pour octroyer des droits à d'autres utilisateurs ! |
| <b>Pour une désinstallation</b>                        | Permet de désinstaller Sophos SafeGuard Disk Encryption  |
| <b>Amorçage autorisé à partir de supports externes</b> | Permet de démarrer un système protégé par Sophos SafeGuard Disk Encryption à partir de la disquette/CD/clé USB.            |

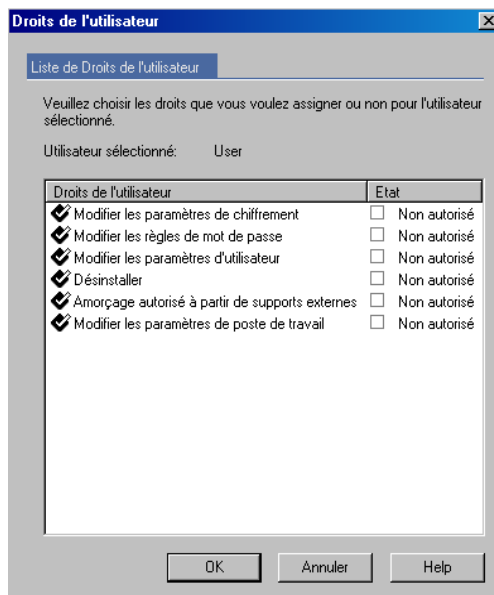
**Modification générale**

Permet de modifier les paramètres généraux suivants :

- Wake On LAN
- Modifier mot de passe au démarrage du système
- Saisie de mot de passe masquée
- Identification

### 14.7.1 Octroi de droits d'utilisateurs

Après un double-clic sur « Droits de l'utilisateur », tous les droits attribuables sont affichés dans l'onglet „Utilisateurs“ de la boîte de dialogue **Configuration du poste de travail**. Le double-clic sur un droit commute l'état préalable « Autorisé » en état « Non autorisé » et inversement



Les nouveaux utilisateurs n'ont aucun droit lors de leur création sauf le droit à changer leur mot de passe. Seul l'utilisateur SYSTÈME dispose de tous les droits. Les droits auxquels l'utilisateur n'a pas accès ne sont pas affichés dans l'aperçu et ne peuvent pas être modifiés.

### 14.7.2 Transfert de droits d'utilisateurs

Un utilisateur peut également transférer des droits à d'autres utilisateurs, si tant est qu'il en dispose lui-même. Si un administrateur (par ex. un sous-administrateur système) souhaite modifier des propres droits, il ne peut pas le faire lui-même. Il doit s'adresser à un administrateur plus haut que lui dans la hiérarchie (p.ex. l'utilisateur du système) et lui demander de procéder aux modifications souhaitées.

Pour transférer ses propres droits à d'autres utilisateurs, un profil d'utilisateur doit avoir la propriété « Modifier les paramètres d'utilisateur ».

## 15 Paramètres du mot de passe

Le mot de passe joue un rôle central dans Sophos SafeGuard Disk Encryption : A partir du mot de passe Sophos SafeGuard Disk Encryption saisi à l'authentification avant amorçage, la clé de déchiffrement d'un disque dur chiffré, requise pour l'amorçage, est calculée.

Le mot de passe Sophos SafeGuard Disk Encryption doit être choisi avec circonspection. Les utilisateurs préfèrent généralement utiliser les mêmes mots de passe, ou mots de passe faibles, tels que leur prénom ou nom, leur nom de société, les séquences de lettres ou de numéros, etc. Lorsqu'un mot de passe Sophos SafeGuard Disk Encryption est trop évident, il risque d'être découvert facilement par une personne malveillante. Pour définir des restrictions à l'attribution de mots de passe, il convient donc de bien réfléchir et d'essayer.

### 15.1 Règles générales de mot de passe internes

Pour des raisons de sécurité, certaines règles pour tous les mots de passe des utilisateurs sont prescrites après l'installation.

**Un mot de passe Sophos SafeGuard Disk Encryption doit ...**

- comporter au maximum 16 caractères.

**Un mot de passe Sophos SafeGuard Disk Encryption ne doit en aucun cas ...**

- comporter 50 % (ou plus) de caractères identiques (par ex. « aaabba », « 222122 »).
- comporter de caractères et/ou chiffres consécutifs (par ex. « abcdef », « 1234567 »).
- comporter de séquences de clavier (par ex. « asdfghj »).
- être identique avec les noms d'utilisateurs Sophos SafeGuard Disk Encryption (exception : mot de passe pour l'utilisateur « SYSTEM »).
- être similaire aux noms d'utilisateurs Sophos SafeGuard Disk Encryption (exception : mot de passe pour l'utilisateur « SYSTEM »).
- être similaire à l'ancien mot de passe.

La séquence de caractères du nouveau mot de passe doit se différencier d'au moins 20 % de l'ancien mot de passe / nom d'utilisateur. Sinon, le mot de passe nouveau est similaire à l'ancien mot de passe. Par exemple, l'utilisateur « UTILISATEUR » Sophos SafeGuard Disk Encryption peut utiliser le mot de passe « U2UTILISATEUR13 », « U345UTILISATEUR », etc., mais Sophos SafeGuard Disk Encryption refuse les mots de passe tels que « UTILISATEUR1 », « UTILISATEUR2 », « UTILISATEURab », « 12UTILISATEUR », « 1UTILISATEURF », etc.

## 15.2 Les clés autorisées pour le mot de passe Sophos SafeGuard Disk Encryption

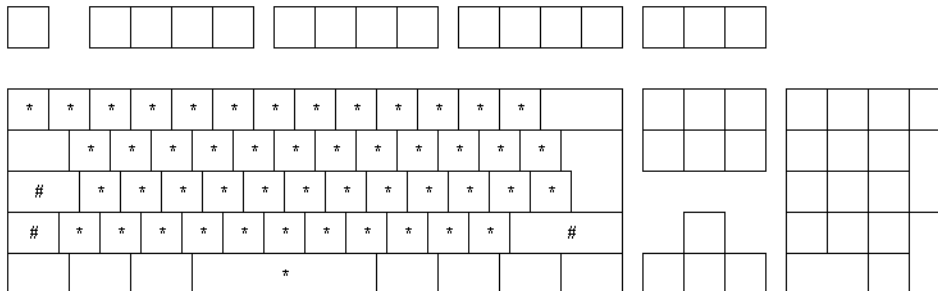
Le mot de passe Sophos SafeGuard Disk Encryption peut se composer de caractères alphanumériques et de signes de ponctuation.

Sophos SafeGuard Disk Encryption accepte

- toutes les touches signalées par « \* » dans l'illustration.
- les touches Maj et Verr Maj (signalées par « # » dans l'illustration).

Sophos SafeGuard Disk Encryption n'accepte pas

- la touche Maj lorsque la touche Verr Maj est déjà enfoncée
- la touche Alt
- la touche Ctrl
- les touches du pavé numérique
- les touches de fonction (par ex. F1, F2)
- les touches de direction

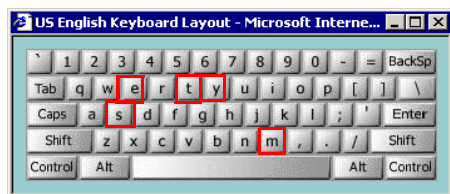


## 15.3 Configuration de Sophos SafeGuard Disk Encryption pour l'utilisation dans un contexte international

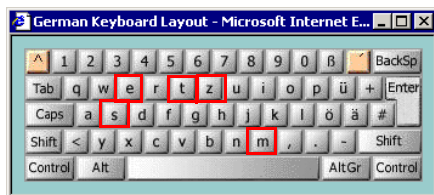
Sophos SafeGuard Disk Encryption enregistre toutes les séquences de caractères en format « Scan Code », étant donné qu'aucun pilote de clavier n'est normalement chargé dans la phase avant l'amorçage. Le « Scancode » est un numéro de code (Scancode hexadécimal) que le clavier transmet à l'ordinateur à l'appui sur une touche. Ce code est indépendant des lettres, chiffres ou symbole illustrés sur la touche. Il représente un caractère spécial pour la touche proprement dite et il est toujours le même pour une touche donnée.

### 15.3.1 Diverses configurations de clavier

Sophos SafeGuard Disk Encryption enregistre toutes les séquences de caractères en format « Scan Code ». Cela signifie que par exemple « system » sur un clavier anglais donne encore un autre Scan Code : 1f-15-1f-14-12-32.



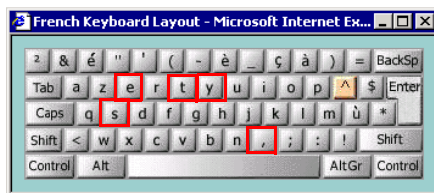
La séquence Scan Code pour « system » avec un clavier allemand est : 1 f-2d-1f-14-12-32.



**Remarque :** Y et le Z sont permutés ! L'utilisateur doit taper « szstem » pour s'authentifier avec succès.

« System » sur un clavier anglais donne le Scan Code suivant 1 f-15-1f-14-12-27.

Sur un clavier français, l'utilisateur doit donc taper « syste, » pour s'authentifier avec succès.



Vous trouverez d'autres configurations de clavier à l'adresse suivant:

<http://www.microsoft.com/globaldev/reference/keyboards.mspx>

### 15.3.2 Créations de données internationales unitaires pour Sophos SafeGuard Disk Encryption

Dès que Sophos SafeGuard Disk Encryption est utilisé dans un contexte international, il convient de s'assurer que mot de passe et code peuvent être saisis de façon correcte sur tous les claviers disponibles. Pour une utilisation internationale, il faut en particulier veiller à ce que les profils d'utilisateur Sophos SafeGuard Disk Encryption remplissent les tâches d'administration.

Il faudrait mentionner par exemple la procédure Requête/Réponse, si l'utilisateur appelant et l'utilisateur helpdesk qui fait office d'assistant de codes de réponse, utilisent différents claviers.

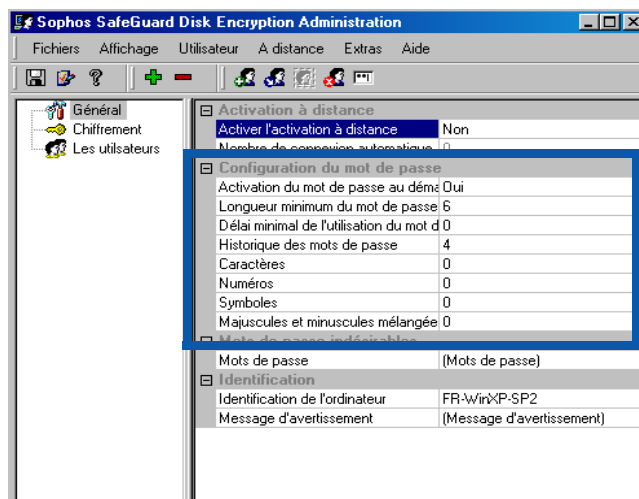
Si les données Sophos SafeGuard Disk Encryption (ou bien : séquences de touches) sont créées à partir d'une combinaison des 21 touches suivantes, il y a de fortes chances pour qu'elles puissent être utilisées sans problème dans un contexte international.

| Valeurs inscrites sur les touches | Scan Code hexadécimal |
|-----------------------------------|-----------------------|
| b                                 | 30                    |
| c                                 | 2E                    |
| d                                 | 20                    |
| e                                 | 12                    |
| f                                 | 21                    |
| g                                 | 22                    |
| h                                 | 23                    |
| i                                 | 17                    |
| j                                 | 24                    |
| k                                 | 25                    |
| l                                 | 26                    |
| n                                 | 31                    |
| o                                 | 18                    |
| p                                 | 19                    |
| r                                 | 13                    |
| s                                 | 1F                    |
| t                                 | 14                    |
| u                                 | 16                    |
| x                                 | 2D                    |

|          |    |
|----------|----|
| v        | 2F |
| [Espace] | 39 |

## 15.4 Règles générales de mots de passe

Les règles de mot de passe générales permettent dans la boîte de dialogue Configuration du poste du travail des programmes d'administration de définir des modèles pour la composition de mots de passe, comme par exemple le pourcentage de lettres et de chiffres ou leur longueur maximum. Ces modèles sont valables pour chaque utilisateur Sophos SafeGuard Disk Encryption et aucun mot de passe ne correspondant pas à ces standards n'est accepté.



### 15.4.1 Activation du mot de passe au démarrage du système

Pour détails voir [Authentification avant l'amorçage \(PBA\)](#) sur page 61.

La valeur par défaut est PBA activé.

### 15.4.2 Longueur minimum du mot de passe

Vous devez spécifier la longueur du mot de passe dans ce champ. Dans ce champ, vous déterminez le nombre de caractères minimum que le mot de passe doit comporter en cas de modification par l'utilisateur.

Vous pouvez saisir le nombre souhaité des caractères soit directement, soit en augmentant ou diminuant la valeur à l'aide des touches de direction. Le mot de passe peut compter entre 1 et 16 caractères. La valeur par défaut est 6.

### 15.4.3 Délai minimal de l'utilisation du mot de passe

Le délai d'utilisation du mot de passe a une durée minimale en jours. Au cours de cette période, l'utilisateur ne doit pas modifier le mot de passe. Cette option vise à empêcher une réinitialisation du mot de passe par l'utilisateur. La valeur par défaut est 0.

### 15.4.4 Historique des mots de passe

Pour éviter que l'utilisateur passe en permanence d'un mot de passe à l'autre, vous pouvez définir un nombre de générations de mot de passe plus élevé. Chaque mot de passe est comparé au mot de passe utilisé dans le passé et refusé quand il est identique à un mot de passe existant. Le nombre de mots de passe utilisés dans le passé et enregistrés pour comparaison est régulé par ce paramètre.

Vous pouvez enregistrer jusqu'à 16 mots de passe utilisateurs. Cliquez sur le champ de saisie, puis définissez la valeur, soit en tapant le mot de passe, soit en cliquant sur les touches de direction. La définition du nombre de générations de mot de passe est particulièrement important si vous activez le paramètre « *Changer le mot de passe après 'n' jours* » (voir [Règles de mot de passe spécifiques à l'utilisateur](#) sur page 87).

**Exemple :**

Vous avez défini à 4 le nombre de générations de mot de passe pour l'utilisateur Dupond, et à 30 celui des jours au bout desquels l'utilisateur doit modifier son mot de passe. Jusqu'ici, Monsieur Dupond ouvrait sa session avec le mot de passe Sophos SafeGuard Disk Encryption « *Informatique* ». Ce délai étant écoulé, il est invité, dans l'écran d'ouverture de session Sophos SafeGuard Disk Encryption (PBA), à modifier son mot de passe. Par exemple, l'utilisateur Miller tape « *Ordinateur* » une deuxième fois et reçoit un message d'erreur indiquant que ce mot de passe a déjà été utilisé et qu'il doit en choisir un autre. L'utilisateur Miller doit attendre la quatrième invite pour utiliser de nouveau « *Ordinateur* » (dans la mesure où l'option de génération de mots de passe est définie sur 4).

### 15.4.5 Règles de syntaxe (caractères, chiffres, symboles, inversion de casse)

Pour augmenter l'efficacité des mots de passe, vous pouvez faire appel à un mélange de lettres et de chiffres (et/ou de symboles). Le nombre indiqué définit toujours une **valeur minimum**.

Les **symboles** sont des caractères spéciaux comme par ex.

\* # !"§\$%&/() etc.

**Majuscules/minuscules** signifie qu'un nombre égal de majuscules et de minuscules doit être utilisé.

**Exemple :**

L'exemple suivant montre l'utilisation correcte des règles de syntaxe :

Spécification

lettres : 1

chiffres : 2

symboles : 1

Majuscules/minuscules : 2

Résultat :

- AAaa12# peut être utilisé
- aaAA123## peut être utilisé
- 3456## est refusé
- AAB1# est refusé

Les mots de passe déjà utilisés par des utilisateurs restent valables, même s'ils ne correspondent pas aux spécifications.

Les règles n'interviennent que lorsque l'utilisateur modifie son mot de passe.

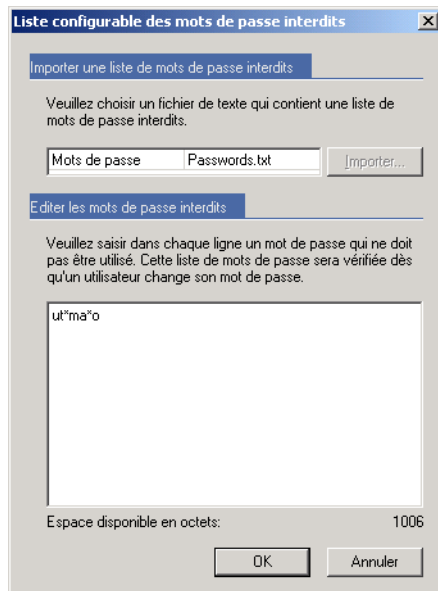
## 15.5 Mots de passe indésirables

Les mots de passe indésirables concernent certaines chaînes de caractères dont l'emploi dans le mot de passe Sophos SafeGuard Disk Encryption est exclu. Chaque nouveau mot de passe est comparé à une liste et n'est accepté que lorsqu'il n'y est pas contenu.

Vous pouvez importer une liste existante ou entrer vous-même des mots de passe interdits.

### 15.5.1 Définition de mots de passe interdits

Double-cliquez sur « Mots de passe » sous « Mots de passe interdits », entrez des combinaisons de chiffres indésirables sous « Éditer les mots de passe interdits » et séparez-les avec **Ctrl + Entrée**.



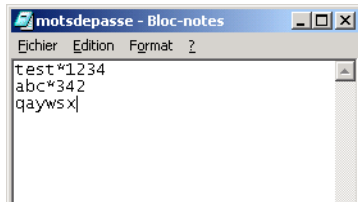
Dans la liste, entrez des mots de passe triviaux, comme par ex. Test, Système, Utilisateur, etc. Tous les mots de passe similaires à un mot de passe interdit sont refusés. La séquence de caractères du nouveau mot de passe doit se différencier d'au moins 20 % de l'ancien mot de passe / nom d'utilisateur. Sinon, le mot de passe nouveau est similaire à l'ancien mot de passe. Par exemple, l'utilisateur Si « Tester » par exemple se trouve dans la liste, l'utilisateur peut saisir le mot de passe « Tester1234 », tandis que « Tester12 » est refusé par Sophos SafeGuard Disk Encryption.

Vous pouvez également utiliser des caractères de remplacement pour la définition. Seul l'astérisque (\*) est accepté comme caractère de remplacement). Remplace **un** caractère au choix dans le mot de passe. « Saf\*Gu\*rd » par ex. interdit les mots de passe comme « SafeGuard », « Saf1Gu2rd », etc.

**Avis :** Si vous ajoutez un ou plusieurs caractères génériques dans la liste des mots de passe interdits, des utilisateurs ne peuvent plus ouvrir de session dans le système après une modification forcée du mot de passe.

## 15.5.2 Importation d'une liste de mots de passe

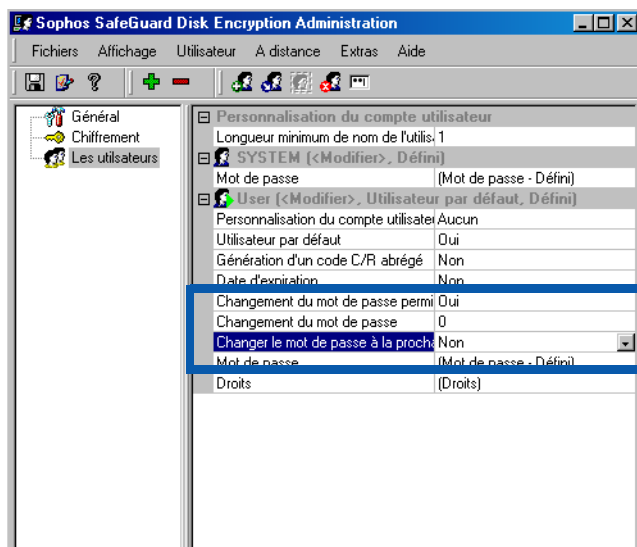
Si une liste de mots de passe indésirables existe déjà, elle peut être importée. Ceci vous permet d'utiliser la même liste sur plusieurs postes de travail. La liste peut être éditée avec n'importe quel éditeur et pourrait avoir l'aspect suivant :



Les différents mots de passe sont séparés par un espace ou par un saut de ligne.

Remarque : Les utilisateurs ne doivent en aucun cas avoir accès à ce fichier

## 15.6 Règles de mot de passe spécifiques à l'utilisateur



Les règles de mot de passe spécifiques à l'utilisateur s'appliquent aux options de changement de mot de passe.

### 15.6.1 Autorisation de la modification de mot de passe

Cette option indique si un utilisateur peut modifier ou non son mot de passe Sophos SafeGuard Disk Encryption dans la PBA ou l'administration.

### 15.6.2 Changement du mot de passe après 'n' jours

Un mot de passe Sophos SafeGuard Disk Encryption est valide sans limite de durée. Le risque d'être découvert un jour ou l'autre est toutefois très élevé. Pour minimiser ce risque, vous pouvez

spécifier qu'un de ces utilisateurs doit changer son mot de passe au bout d'un certain nombre de jours.

Avec les touches fléchées ou par entrée directe via le clavier, définissez une période à la fin de laquelle le mot de passe doit être changé.

La période de validité des mots de passe peut aller de 1 à 365 jours. La période par défaut est de 90 jours. Une fois le délai écoulé, l'utilisateur est tenu de modifier son mot de passe à la prochaine ouverture de session.

### 15.6.3 Changement du mot de passe à la prochaine ouverture de session

L'utilisateur doit modifier son mot de passe Sophos SafeGuard Disk Encryption à la prochaine ouverture de session. Pour utiliser cette fonction, l'authentification avant amorçage doit être activée.

### 15.6.4 Génération d'un code C/R abrégé

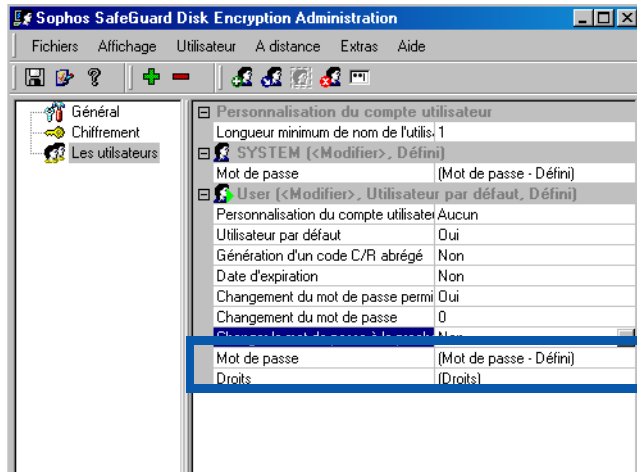
Cette fonction est particulièrement adaptée aux administrateurs de sous-systèmes qui sont chargés de l'administration à distance.

Cette propriété influe sur la longueur du code de réponse échangé pendant une procédure Requête/Réponse.

Les utilisateurs disposant de la propriété « Génération d'un code C/R abrégé » et l'utilisateur SYSTÈME génèrent des codes de réponse courts qui ne comptent que 30 caractères, tandis que les utilisateurs « ordinaires » de Sophos SafeGuard Disk Encryption génèrent des codes de réponse qui comptent 56 caractères. Quand vous le tapez ou le transmettez à l'utilisateur, ceci peut entraîner un pourcentage d'erreur élevé.

Pour une procédure de Requête/Réponse avec succès cette option doit être définie sur OUI pour un utilisateur du service d'assistance. Pour plus de détails sur la procédure Requête/Réponse, voir [Maintenance à distance \(Requête/Réponse\)](#) sur page 122.

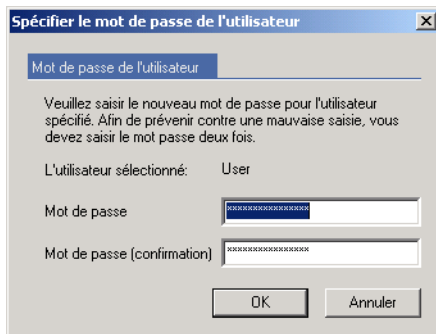
## 15.7 Définition de mot de passe



Les mots de passe d'utilisateur doivent être choisis avec circonspection pour ne pas être aisément devinés. Les mots de passe peuvent contenir des lettres majuscules ou minuscules non accentuées, des chiffres et des caractères spéciaux (!,,\$%&/()\*+;,;:\_-), à condition que cette combinaison n'ait pas été interdite par les règles générales de mot de passe.

Les chiffres du pavé numérique ne doivent pas être utilisés.

Un double-clic sur « Mot de passe » ouvre la boîte de dialogue dans laquelle le mot de passe est défini.



Tapez le mot de passe souhaité dans la ligne supérieure et tapez-le de nouveau dans le champ **Confirmation**. La répétition est nécessaire pour éviter les fautes de frappe. La correspondance des caractères tapés est vérifiée et un message d'erreur apparaît quand les mots de passe ne correspondent pas ou lorsqu'ils sont banals (par ex. « 12345 » ou « AAABBB »). Pour des raisons de sécurité, le mot de passe n'est affiché qu'avec des astérisques (\*). Pour corriger les entrées, veuillez utiliser la touche Reset.

Il n'est pas possible de contourner la seconde saisie du mot de passe en utilisant la fonction « Copier-Coller ».

## 16 Configuration du mot de passe Windows

Avec l'authentification avant amorçage (PBA) comme premier composant du système, Sophos SafeGuard Disk Encryption requiert une authentification. Ce n'est qu'après que le système a été déverrouillé avec des données Sophos SafeGuard Disk Encryption valides que la boîte de dialogue d'ouverture de session de Windows apparaît.

Sophos SafeGuard Disk Encryption offre la fonctionnalité de SAL (Secure Automatic Logon) pour éviter aux utilisateurs d'avoir à s'identifier de plusieurs façons.

Désormais, il leur suffit d'entrer leurs données utilisateur une fois, pendant la préparation du démarrage. Pour que l'ouverture de session Windows soit encore plus conviviale, le modèle d'administration comprend des options supplémentaires.

### 16.1 Ouverture de session automatique sécurisée (SAL)

L'ouverture de session automatique est une fonction confortable pour la procédure d'ouverture de session. Un utilisateur entre une fois ses données Windows. Pour les autres ouvertures de session, la connexion à Windows s'effectue automatiquement et l'utilisateur n'a plus à s'authentifier qu'avec les données d'utilisateur Sophos SafeGuard Disk Encryption dans la PBA. Sophos SafeGuard Disk Encryption appelle cette procédure d'ouverture de session une **ouverture de session automatique** sécurisée, en bref SAL.

L'ouverture de session automatique dans le système d'exploitation peut être désactivée ultérieurement avec la commande Sophos SafeGuard Disk Encryption `Chgsal.exe`.

**Avis :** SAL est installé par défaut. A la première ouverture de session les utilisateurs sont invités à activer SAL.

Toutes les autres ouvertures de session dans d'autres applications doivent se faire manuellement. Si l'option Windows « Connecter toujours cet utilisateur » est activée, aucune SAL ne peut être effectuée.

Techniquement, la SAL fonctionne comme suit : un utilisateur ouvre une session dans la PBA avec des données d'accès Sophos SafeGuard Disk Encryption et entre ensuite ses données Windows dans la boîte de dialogue d'ouverture de session de Windows. La SAL établit une relation entre l'utilisateur Sophos SafeGuard Disk Encryption ayant ouvert la session et l'utilisateur Windows et l'enregistre dans le fichier chiffré `Sgsal.dat`. `Sgsal.dat` se trouve dans `<disque système>\SYSTEM`. A une nouvelle ouverture de session dans la PBA, la SAL transmet les données Windows dans la boîte de dialogue d'ouverture de session Windows, sans intervention de l'utilisateur.

Après l'installation, procédez de la façon suivante :

1. Authentifiez-vous dans la PBA avec les données d'utilisateur Sophos SafeGuard Disk Encryption.

2. Après l'ouverture de session, la boîte de dialogue d'ouverture de session Windows usuelle apparaît à la première ouverture de session.
3. Remplissez les champs de saisie avec les informations d'ouverture de session correctes et cliquez sur **OK**.
4. La boîte de dialogue SAL est alors affichée.



**Oui** : Active la relation entre l'utilisateur Sophos SafeGuard Disk Encryption et l'utilisateur Windows

**Non** : N'utilise pas la fonctionnalité SAL

L'état de la case à cocher « Ne plus reposer la question pour l'utilisateur Sophos SafeGuard Disk Encryption actuel » indique si la boîte de dialogue doit être affichée après chaque connexion ou non.

5. Cliquez sur **OK** et cochez la case. L'utilisateur Sophos SafeGuard Disk Encryption est associé à l'utilisateur Windows. automatiquement.

Au prochain redémarrage de l'ordinateur, l'ouverture de session dans Windows sera automatiquement effectuée après saisie des données d'utilisateur Sophos SafeGuard Disk Encryption dans la PBA.

## Modification du mot de passe Windows

Pour des raisons de sécurité, les mots de passe Windows doivent toujours être changés de temps à autre. La manière d'intégrer un mot de passe nouvellement défini dans l'ouverture de session automatique sécurisée dépend cependant de la méthode utilisée pour le modifier.

### ■ Modification forcée du mot de passe

Une modification de mot de passe est imposée dans le profil d'utilisateur via l'option « L'utilisateur doit modifier le mot de passe à la prochaine ouverture de session. Quand cette option est activée, l'utilisateur reçoit un message d'invite du système. A ce moment, la SAL est désactivée.

Vous devez confirmer le message système en cliquant sur **OK**. La boîte de dialogue suivante demande à l'utilisateur d'entrer un nouveau mot de passe. Dès que l'utilisateur a confirmé le nouveau mot de passe, le fichier SAL est synchronisé avec les nouvelles données. A l'ouverture de session suivante, les données d'utilisateur Windows sont à nouveau transmises automatiquement.

■ **L'utilisateur modifie lui-même son mot de passe**

- Quand l'utilisateur appuie sur son Bureau sur les boutons CTRL+ALT+SUPPR, il peut modifier son mot de passe dans la **boîte de dialogue de connexion Windows** via « Modifier le mot de passe ». Quand la modification est effectuée de cette manière, **une synchronisation de mot de passe automatique** a lieu et les nouvelles données sont enregistrées dans le fichier `sgsal.dat`. En cas d'ouverture de session après modification du mot de passe, l'utilisateur n'a pas à entrer de nouveau les données d'accès à Windows.
- Lorsque le mot de passe est modifié par le service d'**administration des utilisateurs de Windows**, le système **n'accepte pas de façon automatique le nouveau mot de passe Windows** et ce dernier n'est pas enregistré dans le fichier `sgsal.dat`.

Par contre, un message d'avertissement s'affiche pour indiquer que le mot de passe Windows n'est pas valide et que l'utilisateur doit entrer le nouveau mot de passe dans l'écran de connexion. Une fois le mot de passe modifié, l'utilisateur peut se connecter sans avoir à spécifier de nouveau ses données d'accès à Windows et SAL s'exécute sans notification.

### 16.1.1 Désactivation temporaire du module SAL

Avec `CHGSAL.EXE` dans le répertoire Sophos SafeGuard Disk Encryption, le fonction SAL peut être désactivé ultérieurement par un utilisateur possédant des droits d'administrateur Windows et de nouveau activé.

Procédez de la façon suivante :

1. Démarrez l'ordinateur en mode MS DOS ou sélectionnez la commande Exécuter dans le menu Démarrer de Windows, puis exécutez « `cmd` » pour afficher l'invite DOS.
2. Accédez au répertoire où est installé Sophos SafeGuard Disk Encryption. Tapez la commande suivante, avec les paramètres correspondants :

```
CHGSAL.EXE /SAL :ON | /SAL :OFF | [ /? ]
```

|                       |                    |
|-----------------------|--------------------|
| <code>/SAL:ON</code>  | Activer SAL        |
| <code>/SAL:OFF</code> | Désactiver SAL     |
| <code>/?</code>       | Sommaire de l'Aide |

Cet outil ne fonctionne que lorsque Sophos SafeGuard Disk Encryption a été installé avec SAL.

### 16.1.2 Suppression de données pour la connexion SAL

Si vous supprimez le fichier `sgsal.dat` (<disque système>\SYSTEM32), toutes les données d'utilisateur enregistrées sont supprimées. Après un redémarrage de l'ordinateur, vous pouvez attribuer de nouvelles données à un utilisateur Sophos SafeGuard Disk Encryption.

Quand un utilisateur Sophos SafeGuard Disk Encryption ayant déjà établi une connexion est supprimé d'un système, cette relation reste conservée à la création du même utilisateur.

### 16.1.3 Restriction

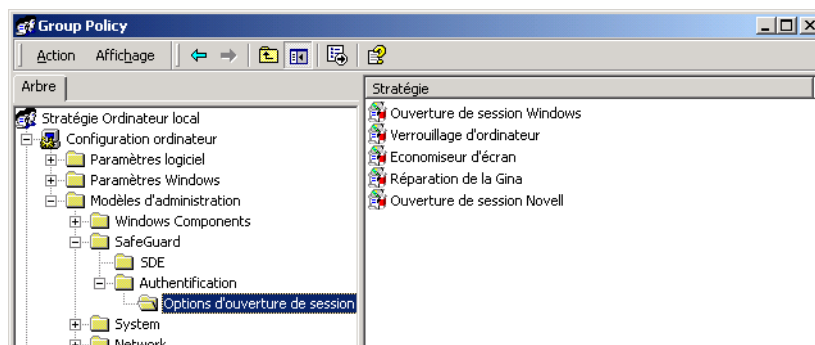
La SAL est provisoirement désactivée quand un utilisateur ouvre une session par Requête/Réponse via l'option « Ouverture de session unique. Cette « ouverture de session unique » permet à un utilisateur d'ouvrir une session dans l'authentification avant amorçage (PBA) de Sophos SafeGuard Disk Encryption sans connaître le mot de passe Sophos SafeGuard Disk Encryption (voir [Maintenance à distance \(Requête/Réponse\)](#) sur page 122).

Si l'ouverture de session unique dans la PBA a été alors permise à un utilisateur, il n'ouvrira pas automatiquement de session dans Windows, même quand la SAL est activée. Dans ce cas, le système d'exploitation stoppe à la boîte de dialogue d'ouverture de session spécifique de Windows et requiert des données Windows valides. Toutes les actions sont dès lors enregistrées sous le nom de l'utilisateur ayant ouvert la session Windows.

Après chaque nouvelle ouverture de session régulière avec données Sophos SafeGuard Disk Encryption dans la PBA, la SAL et l'ouverture de session Windows automatique sont exécutées comme c'est normalement le cas.

## 16.2 Options supplémentaires de connexion sous Windows

Vous pouvez utiliser le modèle d'administration `Sguard.adm` pour définir des paramètres connexion Windows par l'intermédiaire de stratégies de groupe. On peut ici en outre définir par ex. des paramètres d'économiseur d'écran normalement intouchables dans Windows.



## 16.3 Personnalisation de l'écran de connexion de Windows

Ces paramètres conditionnent l'affichage du bureau pendant les procédures de connexion et déconnexion, et lorsque la station de travail est verrouillée.

Cette stratégie se trouve dans le modèle d'administration de Sophos SafeGuard Disk Encryption sous

### Configuration ordinateur

\Modèles d'administration

\SafeGuard

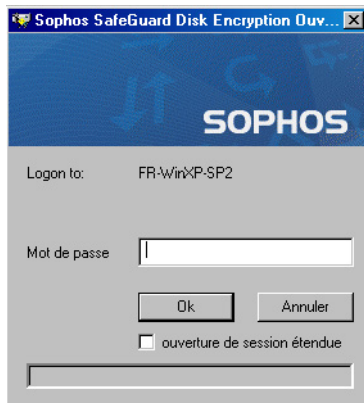
\Authentification

\Options d'ouverture de session

\Ouverture/fermeture de session Windows

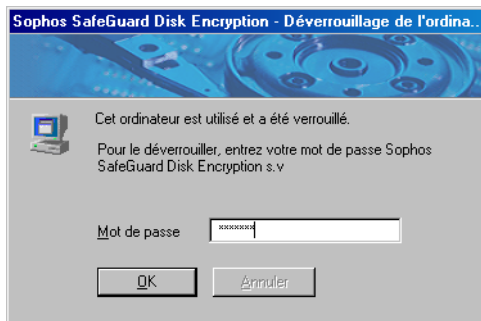
#### ■ Utiliser l'écran d'ouverture de session Sophos

Quand la case est cochée, la boîte de dialogue d'ouverture de session est affichée à l'ouverture de session. Quand la case n'est plus cochée, vous pouvez ouvrir une session dans le système avec la boîte de dialogue d'ouverture de session de Windows.



#### ■ Utiliser l'écran de démarrage Sophos

Quand la case est cochée, la boîte de dialogue Sophos Commencer ouverture de session est affichée. Vous êtes invité à taper **Ctrl + Alt + Suppr** pour ouvrir la boîte de dialogue d'ouverture de session. Quand la case n'est plus cochée, la boîte de dialogue Windows correspondante est affichée.



- **Utiliser l'écran de verrouillage Sophos**  
Quand la case est cochée, la boîte de dialogue SafeGuard Lock est affichée au lieu de la boîte de dialogue Windows au verrouillage du poste de travail avec **Ctrl+Alt+Suppr.** Si une connexion utilisateur non valide a été enregistrée, cette dernière s'affiche dans la boîte de dialogue de verrouillage de Sophos.
- **Désactiver la vérification des données utilisateur avec le RAS**  
Quand la case est cochée, aucune vérification préliminaire n'est effectuée à l'établissement de la connexion RAS.
- **Désactiver l'option RAS de l'écran d'ouverture de session Sophos**  
Quand la case est cochée, l'option « Ouverture de session via réseau RAS » est désactivée dans la boîte de dialogue d'ouverture de session Sophos.
- **Remplacer le bitmap par**  
Ce champ d'édition, qui s'affiche dans la boîte de dialogue de connexion, permet de spécifier un fichier bitmap, tel qu'un logo de société avec un arrière-plan standard. Le bitmap doit être au format .bmp et doit résider dans le dossier System32 du dossier d'installation de Windows. La taille de l'image est fixée à 413x140 pixels.

### 16.3.1 Remplacement de l'image d'arrière plan de l'ouverture de session Windows

Vous avez la possibilité de personnaliser l'image d'arrière plan apparaissant après saisie des données d'utilisateur Sophos SafeGuard Disk Encryption.

Ceci permet au client de personnaliser l'arrière plan de Sophos SafeGuard Disk Encryption selon les besoins de son entreprise.

L'image affichée par défaut a le nom **SgeLogo.bmp** et se trouve dans le répertoire **Sophos SafeGuard Disk Encryption** sélectionné.

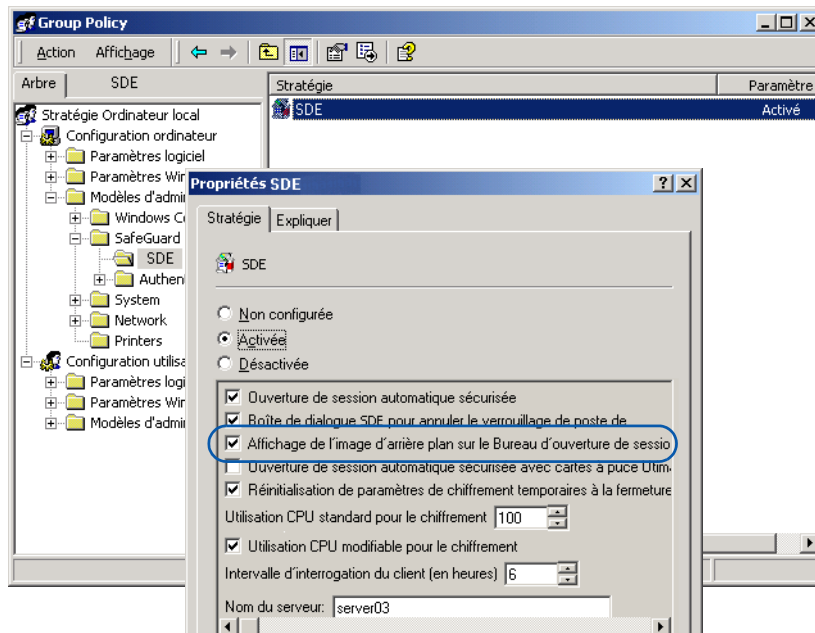
Pour remplacer l'image de titre, il suffit de remplacer l'image par défaut par une image de même nom et de même taille personnalisée.

L'image d'arrière-plan peut être désactivée via une stratégie dans le modèle d'administration Sophos. La stratégie se trouve sous

#### **Configuration ordinateur**

\Modèles d'administration  
\SafeGuard  
\SDE

A la page des propriétés de « SDE », il suffit d'ôter la coche devant « Affichage de l'image d'arrière-plan sur le Bureau d'ouverture de session de Windows ». L'image Sophos SafeGuard Disk Encryption n'apparaît alors plus.



### 16.3.2 Verrouillage du poste

Au verrouillage de poste, on détermine après combien de tentatives infructueuses d'ouverture de session l'ordinateur va être verrouillé et comment le temps d'attente entre des tentatives d'ouverture de session augmente. Le mécanisme ne fonctionne qu'avec les utilisateurs qui ne sont pas membres du groupe local des administrateurs.

Cette stratégie se trouve dans le modèle d'administration de Sophos SafeGuard Disk Encryption sous

#### Configuration ordinateur

\Modèles d'administration  
\SafeGuard  
\Authentification  
\Options d'ouverture de session  
\Verrouillage du poste

Le mécanisme ne fonctionne qu'avec les utilisateurs qui ne sont pas membres du groupe local des administrateurs.

#### ■ Essais d'ouverture de session

Dans ce champ, vous déterminez le nombre des essais infructueux d'ouverture de session par un utilisateur se connectant avec un nom et/ou un mot de passe incorrect. Si vous spécifiez par ex. « 3 », l'ordinateur sera verrouillé si l'utilisateur entre trois fois de suite un nom ou un mot de passe incorrect à l'ouverture de session.

Valeur minimum/maximum : 0-999

■ **Délai en secondes**

Entrez ici la valeur de base qui, multipliée avec le « Multiplicateur », donne le temps d'attente après la première tentative infructueuse d'ouverture de session. Quand une nouvelle tentative infructueuse est effectuée, le temps d'attente de la tentative précédente est pris comme valeur de base. La valeur par défaut est 10.

Valeur minimum/maximum : 0-999

■ **Multiplicateur**

Le multiplicateur est multiplié avec le délai de base en secondes. La valeur par défaut est 3.

Valeur minimum/maximum : 0-99

■ **Désactiver le Ctrl+Alt+Suppr lorsque la station est verrouillée**

Le verrouillage du poste ne peut pas être annulé avec Ctrl+Alt+Suppr.

**Exemple :**

Délai de 10 secondes et multiplicateur de :

1<sup>ère</sup> tentative infructueuse : 50 secondes d'attente (10 \* 5)

2<sup>ème</sup> tentative infructueuse : 250 secondes d'attente (10 \* 5 \* 5)

3<sup>ème</sup> tentative infructueuse : 1250 secondes d'attente (10 \* 5 \* 5 \* 5)

**Remarque :** Le verrouillage du poste peut être annulé

- en redémarrant l'ordinateur
- via l'ouverture de session par l'administrateur.
- en répliquant des données à partir du contrôleur de domaine.

A ce sujet, veuillez noter également le verrouillage d'utilisateur de Windows.

### 16.3.3 Économiseur d'écran

Si, sur un poste de travail, on a spécifié la mise en route de l'économiseur d'écran au bout d'une durée donnée, vous pouvez décider comment le système doit réagir à son activation après une période déterminée. Les paramètres ne sont effectifs que lorsque l'économiseur d'écran de Windows est lui aussi activé !

Cette stratégie se trouve dans le modèle d'administration de Sophos SafeGuard Disk Encryption sous

**Configuration ordinateur**

\Modèles d'administration

\SafeGuard

\Authentification

\Options d'ouverture de session

\Économiseur d'écran

■ **Action**

La section *Action* permet de définir les réactions suivantes lors de l'exécution d'un économiseur d'écran.

A) *Déconnecter l'utilisateur :*

L'utilisateur actif sera déconnecté de l'ordinateur. D'autres utilisateurs enregistrés sur le poste de travail ou dans le réseau peuvent (aussi) ouvrir une session.

B) *Arrêt du système*

Le PC est automatiquement arrêté et doit être redémarré pour une autre session de travail.

C) *Redémarrer la station de travail*

La station de travail sera redémarrée de façon automatique..

D) *Mise en veille prolongée de la station de travail*

Place l'ordinateur en mode Veille prolongée.

E) *Déconnecter la session*

N'a aucun effet sur la station de travail locale.

Lors des sessions Terminal Server, la session sera déconnectée.

F) *Standby*

(Veille) L'ordinateur est mis en veille.

Aperçu des actions possibles et leurs effets sur l'ordinateur local :

| <b>Paramètre</b>                       | <b>Action local</b>        |
|--|----------------------------|
| <Aucun>                                | aucune                     |
| Fermeture de la session                | fermer                     |
| Arrêter la station de travail          | arrêter                    |
| Redémarrage du système                 | redémarrer                 |
| Mettre en veille la station de travail | mettre en veille prolongée |
| Déconnexion de la session              | aucune                     |
| En veille                              | En veille                  |

■ **Délai**

Sous "Délai", vous réglez la durée (en minutes) après laquelle le système doit exécuter une action décrite. La valeur par défaut est 15. Vous pouvez taper le nombre directement au clavier

ou le modifier avec les touches fléchées.  
Valeurs minimales et maximales : 0-900

■ **Désactiver l'écran de veille**

De manière générale l'écran de veille est désactivé lorsqu'un utilisateur déplace la souris ou utilise le clavier. Il peut ensuite poursuivre normalement son travail. Si la case « Désactiver l'économiseur d'écran » est cochée, le poste de travail est verrouillé. L'accès au poste de travail n'est plus possible qu'après saisie des données d'accès correctes.

**Exemple :**

Sur les postes de travail, on a spécifié que l'économiseur d'écran devait démarrer dix minutes après la dernière action de l'utilisateur. Si vous avez choisi l'action 'Arrêt du système' et entré un délai de 13, le PC sera automatiquement arrêté 23 minutes après la dernière action effectuée sur le poste de travail.

### 16.3.4 Réparation de la GINA

Sophos utilise son propre composant de connexion (SafeGuard GINA (SGGINA.dll)). Suite à l'installation, il s'agit toujours du premier composant de connexion Windows appelé par le système d'exploitation.

L'installation d'autres produits peut modifier l'ordre des composants d'ouverture de session appelés.

Cette stratégie se trouve dans le modèle d'administration de Sophos SafeGuard Disk Encryption sous

**Configuration ordinateur**

\Modèles d'administration

\SafeGuard

\Authentification

\Options d'ouverture de session

\Réparation de la Gina

■ **Réparer le registre GINADLL si modifié**

Assure le que le composant SafeGuard GINA apparaît en première position lors du démarrage du système d'exploitation.

■ **En cas de GINA inconnue**

*Demander à l'utilisateur*

A la première initialisation, le système demande dans une boîte de dialogue si la GINA inconnue ou la GINA Microsoft d'origine doit être utilisée. Si, dans cette boîte de dialogue, la case « Ne plus afficher ce message » est cochée, l'action de l'utilisateur est enregistrée dans le registre et cette valeur est utilisée au prochain redémarrage.

*Utiliser la GINA Microsoft d'origine*

La GINA Microsoft d'origine est placée en première position de la chaîne GINA.

*Utiliser la GINA inconnue*

La GINA inconnue est placée en première position de la chaîne GINA.

## 17 Sophos SafeGuard Disk Encryption Verrouillage du poste

Sophos SafeGuard Disk Encryption peut remplacer le verrouillage de poste de travail Windows normal par sa propre boîte de dialogue.



Quand l'ordinateur est en mode veille, seul l'utilisateur l'ayant verrouillé peut réactiver l'interface utilisateur en entrant son mot de passe Sophos SafeGuard Disk Encryption.

Écran et interface utilisateur sont verrouillés

- après appui sur CTRL+ALT+SUPPR et Verrouiller ordinateur
- après écoulement d'une durée réglée sans intervention de l'utilisateur (temps d'attente)

Pour le verrouillage du poste de travail, le même écran d'arrière-plan que pendant l'ouverture de session apparaît (voir [Personnalisation de l'écran de connexion de Windows](#) sur page 94).

### 17.1 Conditions

Le verrouillage du poste de travail ne fonctionne que si

- l'authentification avant amorçage est active
- l'utilisateur a été automatiquement connecté via SAL au système d'exploitation
- l'économiseur d'écran de Windows est activé avec protection par mot de passe

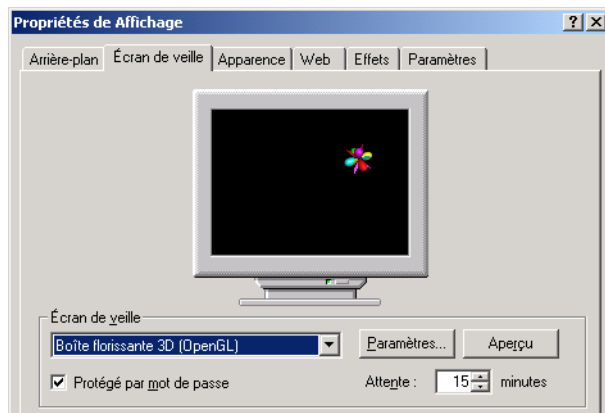
Après configuration de l'économiseur d'écran de Windows, l'ordinateur doit être redémarré.

Le verrouillage de poste de travail de Sophos SafeGuard Disk Encryption est ultérieurement désactivé quand un utilisateur ferme et rouvre une session après une ouverture de session avec succès dans Windows.

## 17.2 Activation de l'économiseur d'écran de Windows avec protection par mot de passe

Le verrouillage du poste de travail Sophos SafeGuard Disk Encryption est commandé dans les paramètres Windows via Programmes \ Panneau de configuration \ Affichage \ Écran de veille.

Redémarrez la station de travail après avoir activé l'économiseur d'écran.



Il convient de choisir également un économiseur d'écran et d'adapter ensuite les options « Protégé par mot de passe » et « Attente ».

- **Protégé par mot de passe**  
Impose la demande du mode de passe Sophos SafeGuard Disk Encryption, la case doit être cochée.
- **Attente**  
Indique la durée (en minutes) devant s'écouler sans intervention de l'utilisateur sur le poste de travail avant que le verrouillage du poste de travail ne s'active.  
Si vous entrez ici 15, l'écran sera éteint au bout de 15 minutes si aucune intervention de l'utilisateur n'a lieu pendant ce temps. Pour continuer son travail, l'utilisateur doit ouvrir à nouveau une session avec le mot de passe Sophos SafeGuard Disk Encryption.

Pour protéger le poste de travail contre l'intervention non autorisée de tierces personnes, veuillez activer le verrouillage de poste de travail.

## 17.3 Désactivation du verrouillage de poste de travail Sophos SafeGuard Disk Encryption

Vous avez la possibilité de désactiver le verrouillage de poste de travail Sophos SafeGuard Disk Encryption et d'afficher à la place la boîte de dialogue Windows normale.

**Conseil :** La boîte de dialogue Windows normale n'est pas déverrouillée avec le mot de passe Sophos SafeGuard Disk Encryption, mais avec le mot de passe de Windows. La protection par mot

de passe de Sophos SafeGuard Disk Encryption pour le verrouillage de poste de travail n'est alors plus disponible.

Si AUCUN verrouillage de poste de travail Sophos SafeGuard Disk Encryption ne doit être indiqué, ceci peut être configuré via la stratégie « Utiliser boîte de dialogue SDE pour annuler le verrouillage de poste de travail » (retirez la coche devant la stratégie).

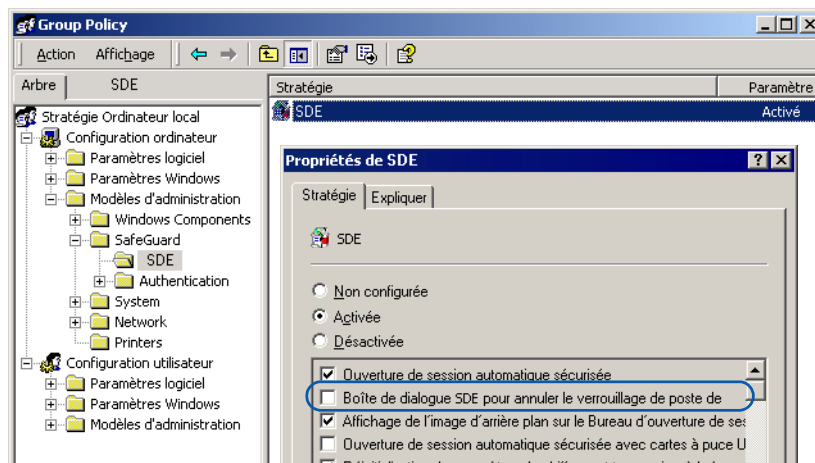
Cette stratégie se trouve dans le modèle d'administration de Sophos SafeGuard Disk Encryption sous

### Configuration ordinateur

\Modèles d'administration

\SafeGuard

\SDE



## 18 Activation à distance (Wake-On-LAN) sécurisée

Le mode d'activation à distance sécurisée de Sophos SafeGuard Disk Encryption constitue le moyen le plus sûr d'allier les avantages de l'activation à distance et le chiffrement des disques durs pour protéger le PC. Pour ce faire, l'activation à distance de Sophos SafeGuard Disk Encryption autorise la désactivation de l'authentification avant amorçage pendant un nombre prédéfini de redémarrages. Ensuite, cette fonction peut être réactivée pour permettre, par exemple, la distribution de nouveaux logiciels. Cependant, avec l'activation à distance, il est impossible de désactiver l'authentification avant amorçage et de s'introduire dans le système avec un identifiant Windows.

WOL représente un compromis optimal entre la protection avant amorçage et l'exécution de tâches exécutées de manière centralisée.

### 18.1 Aperçu

En général, l'activation à distance sécurisée permet à tout ordinateur d'un réseau local d'être démarré par un autre ordinateur du réseau. Ceci peut se produire de façon à charger les nouvelles mises à jour ou procéder à des tâches de maintenance de routine.

La technique WOL dans Sophos SafeGuard Disk Encryption permet à l'administrateur d'autoriser aux clients Sophos SafeGuard Disk Encryption un certain nombre de redémarrages avant d'activer à nouveau l'authentification avant amorçage. Par exemple, lorsque le nombre de connexions automatiques est défini sur « 3 », le PC peut être redémarré trois fois de suite avec l'authentification avant amorçage (PBA) désactivée. Lors du quatrième démarrage, l'écran d'authentification avant amorçage (PBA) s'affiche de nouveau de façon automatique (si cette fonction est active).

Lors de ces phases de connexion automatique, la boîte de dialogue de connexion de Windows ne s'affiche pas. L'ordinateur démarre de façon autonome et la mise à jour automatique du logiciel peut être exécutée via le réseau.

### 18.2 Verrouillage de l'ouverture de session Windows

En mode Wake On LAN, l'ordinateur est protégé contre les ouvertures de session Windows locales par l'utilisateur. Par contre, le système affiche une boîte de dialogue d'activation à distance (« L'authentification Windows n'est pas permise, car cet ordinateur a été démarré à distance (Wake-On-LAN) sans aucune authentification »).



### Connexion à Windows avec Wake-On-LAN

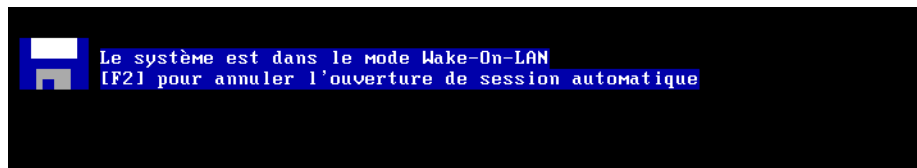
**Remarque:** Cependant, le verrouillage de connexion Windows en mode d'activation à distance fonctionne uniquement lorsque Sophos SafeGuard GINA est installé !



## 18.3 Annulation temporaire du verrouillage d'activation à distance

Si un utilisateur doit utiliser son ordinateur malgré le verrouillage WOL, il est possible d'annuler provisoirement ce verrouillage.

Pendant la phase de pré-amorçage, une icône de disquette s'affiche pendant environ 5 secondes dans la partie supérieure gauche de l'écran.



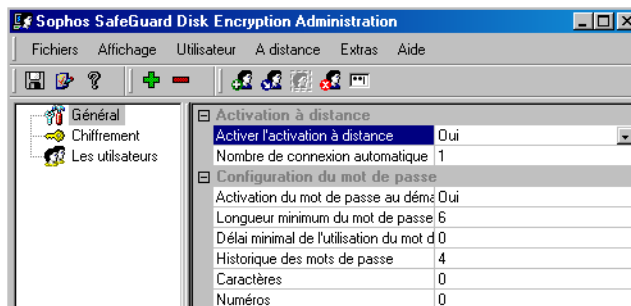
Si, pendant cette durée, F2 est actionnée, la PBA apparaît et l'utilisateur peut ouvrir normalement sa session avec les données Sophos SafeGuard Disk Encryption valides et plus tard dans Windows. L'utilisateur remarque que l'ordinateur se trouve en mode Wake On LAN à un petit avertissement clignotant au-dessus de F2.

Si l'ordinateur est démarré en mode sécurisé (appuyer sur F8 pendant le processus d'amorçage), le verrouillage incorporé permet seulement aux utilisateurs possédant des droits d'administrateur d'ouvrir leur session en mode sécurisé.

## 18.4 Configuration de l'activation à distance

WOL est utilisé en règle générale dans les environnements informatiques plus étendus et non pas pour les ordinateurs autonomes. L'administrateur crée un fichier de configuration avec les paramètres WOL correspondants et le distribue aux clients dans l'entreprise.

Le mode d'activation à distance Sophos SafeGuard Disk Encryption Wake-On LAN sécurisée est configuré dans les outils d'administration par le biais de la page « Général ».



Les réglages suivants sont possibles :

- **Activer l'activation à distance :**  
Active/désactive le mode Wake On LAN.
- **Nombre de connexions automatiques (par défaut : 1) :**  
Définit le nombre des redémarrages avec PBA désactivée quand l'activation à distance est en service.

Nous recommandons de toujours **autoriser un redémarrage de plus que nécessaire** pour contourner les problèmes inattendus.

Dès que le fichier de configuration a été distribué aux ordinateurs des utilisateurs, le PC redémarre n fois sans PBA. Une fois que le nombre de redémarrages sans PBA défini est atteint, l'authentification avant l'amorçage est réactivée et demande les données d'utilisateur Sophos SafeGuard Disk Encryption correctes.

## 19 Mise en veille prolongée

La fonctionnalité de Windows « Mise en veille prolongée » est très appréciée des utilisateurs d'appareils mobiles pour interrompre provisoirement leur travail. Lorsqu'un ordinateur portable disposant d'une fonction de mise en veille prolongée active est arrêté pendant une opération, il s'arrête automatiquement. Lors du redémarrage suivant, il rétablit l'écran tel qu'il était lors de la demande d'arrêt.

Pour la sauvegarde des données en veille prolongée, Sophos SafeGuard Disk Encryption propose ici une solution particulière qui n'est pas propre à tout produit de chiffrement.

### 19.1 Aperçu

En mode Veille prolongée, le contenu de la mémoire vive est écrit dans un fichier système, Hiberfile.sys, situé dans le répertoire racine de la partition du système d'exploitation (généralement C:) et est stocké sur le disque dur. La taille du fichier Hiberfile.sys correspond à peu près à la taille de la mémoire de travail disponible. L'ordinateur est ensuite éteint. Si vous rallumez l'ordinateur, le Bureau réapparaît exactement tel que vous l'avez quitté à l'extinction de l'ordinateur, c'est-à-dire que le contenu du fichier Hiberfile.sys est réécrit dans la mémoire de travail. Après désactivation du mode de veille prolongée, le fichier Hiberfile.sys est invalidé.

### 19.2 Mise en veille prolongée et Sophos SafeGuard Disk Encryption

Lorsque la partition système du système d'exploitation n'est pas chiffrée, l'activation du mode Veille prolongée représente un risque de sécurité dans la mesure où cette procédure transfère tout le contenu de la mémoire vive, qui est alors accessible librement par des personnes non autorisées.

Dans une partition de système d'exploitation chiffrée, Sophos SafeGuard Disk Encryption permet d'utiliser le mode de veille prolongée et de chiffrer le fichier Hiberfile.sys créé, puis de le stocker de façon sûre sur le disque dur. Toutes les données sont ainsi chiffrées à tout moment sur le disque dur. L'accès au système est réservé exclusivement aux utilisateurs ayant pu s'authentifier avec des données Sophos SafeGuard Disk Encryption correctes après un redémarrage de l'ordinateur en mode PBA (pour autant qu'elle soit activée).

**Remarque :** Quand plusieurs utilisateurs Sophos SafeGuard Disk Encryption se partagent un poste de travail, chacun d'entre eux parvient, après authentification via diverses données Sophos SafeGuard Disk Encryption dans la PBA, dans le profil de l'utilisateur qui a initié la mise en veille prolongée.

Il est possible dans ce cas d'exiger l'entrée du mot de passe Windows au redémarrage (Options d'alimentation \ Avancé \ Demander un mot de passe lorsque l'ordinateur sort de mise en veille). Ce paramètre oblige l'utilisateur à ouvrir une session supplémentaire avec ses données Windows (inconvenient : double authentification).

## 19.3 Conditions et restrictions

La combinaison de Sophos SafeGuard Disk Encryption et de la mise en veille prolongée fonctionne dans les conditions suivantes :

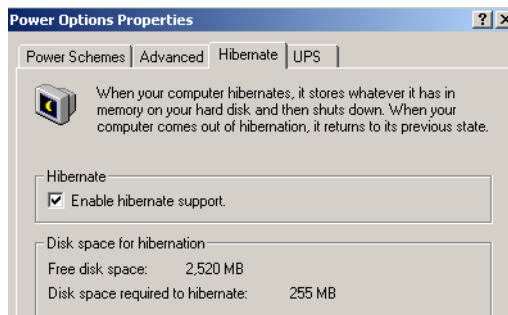
| La mise en veille prolongée avec Sophos SafeGuard Disk Encryption prend en charge...   | La mise en veille prolongée avec Sophos SafeGuard Disk Encryption ne prend pas en charge... |
|--|---|
| Windows 2000 et Windows XP les disques durs (Microsoft IDE, Serial-ATA, SCSI) qui utilisent les interfaces par défaut de Microsoft. Si aucune interface par défaut n'est utilisée, Serial-ATA risque de provoquer des problèmes pour certains périphériques. | Pilotes de disque dur d'autres fabricants   |

**Remarque :** Lorsque vous utilisez des périphériques externes ou des cartes d'extension (cartes son, etc.) assurez-vous qu'elles prennent en charge les fonctionnalités de gestion d'énergie Microsoft et que l'ordinateur peut être placé en mode Veille prolongée et réactivé, même si Sophos SafeGuard Disk Encryption n'est pas installé.

## 19.4 Configuration de la mise en veille prolongée

Pour garantir la plus haute sécurité possible à l'activation de la mise en veille prolongée, nous recommandons la configuration ci-dessous :

1. Dans le menu de démarrage de Windows, appelez successivement Paramètres \ Panneau de configuration \ Options d'alimentation. Sous l'onglet *Mise en veille prolongée*, cochez la case « Activer la prise en charge de la mise en veille prolongée ».



2. Si deux utilisateurs partagent un ordinateur géré par Sophos SafeGuard Disk Encryption, ouvrez l'onglet *Avancé*. Dans cet onglet, sélectionnez le champ « Mot de passe pour sortir d'une mise en veille (prolongée) ».
3. Démarrez l'utilitaire d'administration de Sophos SafeGuard Disk Encryption.
4. Activez l'authentification avant amorçage (PBA), si ce n'est pas déjà fait, dans Général\Choix des mots de passe\Mot de passe lors du démarrage du système.
5. Chiffrez la partition du système d'exploitation avec Chiffrement\Lecteurs\Disque dur.  
Pour protéger votre système, nous recommandons de chiffrer en outre les partitions de données complètes, en plus de la partition de système d'exploitation.

## 20 Certification FIPS 140-2 (Level 1)

La certification FIPS décrit les exigences en matière de sécurité pour les modules de chiffrement. Les administrations gouvernementales des États-unis et du Canada requièrent par exemple un logiciel certifié FIPS 140-2 pour les informations particulièrement critiques en matière de sécurité.

La caractéristique d'une installation Sophos SafeGuard Disk Encryption conforme à la certification FIPS est que seuls certains algorithmes doivent être utilisés pour le chiffrement. Pour Sophos SafeGuard Disk Encryption c'est :

- AES-256

Quand Sophos SafeGuard Disk Encryption est installé en mode FIPS, une icône apparaît dans la barre des tâches.

Sophos SafeGuard Disk Encryption prend en charge les fonctionnalités suivantes pour satisfaire aux exigences de la certification FIPS 140-2.

### Test à réponse connue (« Known Answer Test » – KAT)

Le test KAT est exécuté pour vérifier si les algorithmes de chiffrement utilisés fonctionnent correctement et s'ils fournissent des résultats appropriés. Le KAT est exécuté pour tous les algorithmes de chiffrement autorisés par le FIPS, et également pour la fonctionnalité hash HMAC-256 utilisée pour le contrôle d'intégrité.

Pour le test KAT, un module de chiffrement chiffre un bloc de données défini et vérifie, au vu du résultat, si les données générées chiffrées sont celles que l'on attend. Si le résultat est erroné, le module de chiffrement doit verrouiller tout autre processus de chiffrement. Les pilotes de chiffrement de Sophos SafeGuard Disk Encryption exécutent automatiquement le test KAT après initialisation du pilote. Le texte KAT est exécuté pour le chiffrement et le déchiffrement. Les modules de chiffrement installés dans le noyau système Sophos SafeGuard Disk Encryption exécutent les mêmes tests.

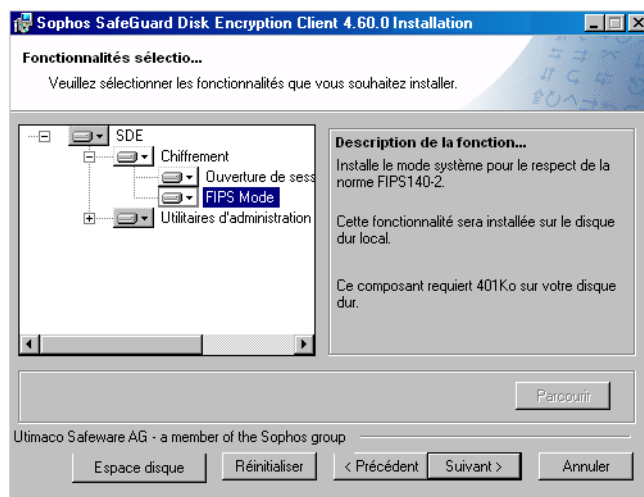
### Contrôle d'intégrité

Un contrôle d'intégrité est exécuté pour les modules de chiffrement afin de s'assurer qu'ils n'ont pas été modifiés. En cas d'échec d'un contrôle d'intégrité, le système stoppe tous les autres processus. Ce test est exécuté pour les fichiers pilotes de chiffrement de Sophos SafeGuard Disk Encryption et les modules de chiffrement dans le noyau système Sophos SafeGuard Disk Encryption. Un contrôle d'intégrité est également exécuté au sein du noyau système pour les données du système afin de détecter les manipulations illégales.

Dès que Sophos SafeGuard Disk Encryption est installé de façon conforme à la certification FIPS, les deux procédures de test pour le noyau système et le mode Win32 sont exécutées. Le test KAT est exécuté même si le mode FIPS est désactivé.

## 20.1 Installation de Sophos SafeGuard Disk Encryption de façon conforme à la certification FIPS

Avec une installation du type „Personnalisée“ vous pouvez déterminer si un système Sophos SafeGuard Disk Encryption doit être installé de façon conforme à la certification FIPS.



Une fois l'installation terminée, une icône dans la barre des tâches indique que Sophos SafeGuard Disk Encryption fonctionne en mode FIPS.



## 20.2 Utilisation sécurisée de Sophos SafeGuard Disk Encryption dans la configuration certifiée

Pour utiliser Sophos SafeGuard Disk Encryption dans une configuration certifiée et donc pour garantir la plus grande sécurité de produit possible, le système doit être configuré de la manière suivante :

- Installation avec PBA
- Longueur de mot de passe minimum : 6 caractères
- Activer le chiffrement intégral du disque dur
- Activer le verrouillage d'écran Sophos SafeGuard Disk Encryption

## 21 Sophos SafeGuard Disk Encryption et Lenovo Thinkvantage - Rescue and Recovery

Ceci permet aux utilisateurs de faire appel à la méthode efficace de sauvegarde et de restauration de Lenovo, même quand la partition du système d'exploitation est chiffrée avec Sophos SafeGuard Disk Encryption. Sophos SafeGuard Disk Encryption offre ici une fonctionnalité unique en son genre !

### 21.1 Aperçu

Rescue and Recovery™ offre une fonction centrale pour la restauration de données par appui sur une touche. Même quand le système d'exploitation primaire est endommagé et n'amorce plus, Rescue and Recovery™ sauvegarde les données via un environnement de secours. Les outils de sauvetage peuvent être appelé depuis le Bureau de Microsoft Windows ou la touche bleue « Thinkvantage » intégrée dans les systèmes Lenovo. Rescue and Recovery™ prend cependant également en charge les système non-Lenovo.

Rescue and Recovery sert surtout de « planche de salut » aux utilisateurs d'ordinateurs quand le système d'exploitation est défaillant et quand des données importantes ne sont plus accessibles. Cette solution protège l'ensemble des données du système et assure la sécurité des données.

Pour de plus amples informations sur Rescue and Recovery™, veuillez consulter votre documentation Lenovo.

### 21.2 Rescue and Recovery et Sophos SafeGuard Disk Encryption

Sophos SafeGuard Disk Encryption s'intègre sans problèmes dans les schémas Rescue and Recovery et prend également en charge les fonctions spécifiques à Lenovo telles que la touche bleue « Thinkvantage » sur le clavier des ordinateurs portables ou la touche « Entrée » bleue des ordinateurs.

Une fois le chiffrement terminé, l'utilisateur a la possibilité de créer une copie de sauvegarde des modifications. Pour ce faire, le système contient, par exemple, le pilote Sophos SafeGuard Disk Encryption, qui permet de restaurer ce type de sauvegarde. (La sauvegarde sécurisée avec Sophos SafeGuard Disk Encryption et ses pilotes est appelée « sauvegarde SDE »).

Sophos SafeGuard Disk Encryption n'est pas affecté par une restauration système, tous ses paramètres restent valides et il n'est nécessaire de procéder à sa réinstallation. L'utilisateur peut continuer à travailler sans interruption après la restauration et n'est pas importuné par un relancement du chiffrement.

### 21.2.1 Avantages de la combinaison de Rescue and Recovery™ et de Sophos SafeGuard Disk Encryption

- Sophos SafeGuard Disk Encryption chiffre tout le disque dur, fichiers temporaires, fichier d'échange, mise en veille prolongée et fichier de vidage de mémoire inclus, et le protège en interrogeant les données d'utilisateur Sophos SafeGuard Disk Encryption contre un accès non autorisé.
- Toutes les copies de sauvegarde sont stockées de façon chiffrées dès qu'elles sont enregistrées sur un disque dur local chiffré.
- Le module Rescue and Recovery permet de restaurer un système endommagé sans avoir à réinstaller Sophos SafeGuard Disk Encryption et chiffrer de nouveau le disque dur.
- La restauration d'une sauvegarde Sophos SafeGuard Disk Encryption de l'environnement Rescue and Recovery n'est possible que si les données d'utilisateur Sophos SafeGuard Disk Encryption ont été entrées au préalable dans l'authentification avant amorçage.

### 21.2.2 Préparation

- Ordinateurs de bureau ou portables de Lenovo
- BIOS actuel pour votre système
- Version de Rescue and Recovery™ :
  - Rescue and Recovery™ 1.0 (Build 033)
  - Rescue and Recovery™ 2.0 (Build 2.00.0170)
  - Rescue and Recovery™ 3.0 (Build 3.00.0029.00)
  - Rescue and Recovery™ 4.0 (Build 4.0.0114)
  - Rescue and Recovery™ 4.2 (Build 4.20.0510)

## 21.3 Pour une installation

Pour les exemples d'installation ci-dessous, nous supposons que l'environnement Rescue and Recovery n'est pas installé sur la partition IBM\_SERVICE. Toutes les particularités dont il convient de tenir compte quand on utilise la partition IBM\_SERVICE sont listées au chapitre Particularités.

Si vous installez Rescue and Recovery sur un disque dur sans partition IBM\_SERVICE, Rescue and Recovery™ sera installé avec les paramètres par défaut suivants :

- L'environnement Rescue and Recovery se trouve par défaut sur une partition virtuelle, installée sur le disque C (partition primaire du disque dur principal) de l'ordinateur.

- Une partition virtuelle comporte deux répertoires : \minint et \preboot. Ces deux répertoires sont protégés par Rescue and Recovery lui-même.
- Les sauvegardes ou copies de sauvegarde sont enregistrées par défaut dans le répertoire C:\RRUbackups. Quand il se trouve sur la partition locale du disque dur primaire, ce répertoire est protégé par Rescue and Recovery pour qu'il ne soit ni effacé, ni déplacé. Dans ce cas, la suppression est impossible.

A l'installation de Rescue and Recovery et de Sophos SafeGuard Disk Encryption, l'ordre d'installation est important. Lisez impérativement les instructions des chapitres suivants.

### **21.3.1 Ni Sophos SafeGuard Disk Encryption, ni Rescue and Recovery ne sont installés**

1. Installez Rescue and Recovery™.
2. Installez Sophos SafeGuard Disk Encryption version 4.60.

Sophos SafeGuard Disk Encryption vérifie si la version Rescue and Recovery correcte est installée et ajoute ses fichiers et ses paramètres dans l'environnement de secours Lenovo.

Veillez vous assurer que l'authentification avant amorçage est bien activée de façon à ce qu'aucune personne non autorisée ne puisse restaurer des sauvegardes.

**L'authentification avant amorçage est activée pendant l'installation ou vous pouvez l'activer plus tard dans l'administration via le dossier Général \ Configuration de mot de passe \ Activation du mot de passe au démarrage du système.**

### **21.3.2 Seul Sophos SafeGuard Disk Encryption est déjà installé.**

Sophos SafeGuard Disk Encryption version 4.60 est installé.

1. Installez Rescue and Recovery.
2. Avant le redémarrage, appelez successivement les outils suivants du répertoire Sophos SafeGuard Disk Encryption- MBRsync.exe
  - MBRsync.exe
  - WinPERepair.exe

### 21.3.3 Mise à niveau de Rescue and Recovery

A chaque fois que Rescue and Recovery est mis à jour, les outils MBRsync.exe et WinPErepair.exe doivent être exécutés avant le redémarrage. Les deux outils se trouvent dans le répertoire Sophos SafeGuard Disk Encryption et sont exécutés simplement en double-cliquant dessus.

## 21.4 Désinstallation

A la désinstallation des deux produits, veuillez observer ce qui suit :

- Désinstallez d'abord Sophos SafeGuard Disk Encryption, puis Rescue and Recovery.
- Si vous désinstallez Rescue and Recovery avant Sophos SafeGuard Disk Encryption, vous devez exécuter l'outil MBRsync.exe avant le redémarrage.
- La désinstallation de Sophos SafeGuard Disk Encryption ne doit pas s'effectuer aussitôt après une restauration du système. Redémarrez l'ordinateur et désinstallez ensuite Sophos SafeGuard Disk Encryption !

## 21.5 Création d'une copie de sauvegarde

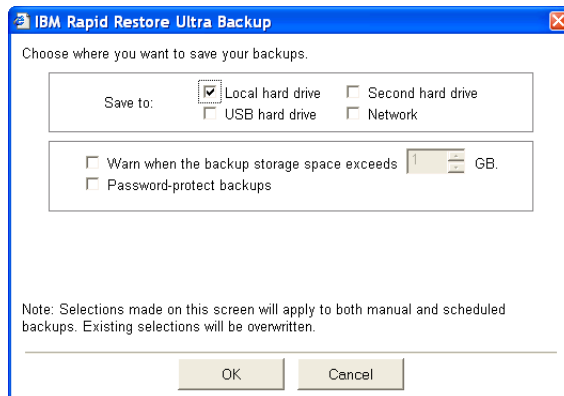
**Remarque :** Les captures d'écran des chapitres suivants présentent des extraits de la version Rescue and Recovery™ avec Rapid Restore™ 4.0 (version 033). L'interface utilisateur des versions suivantes pourra partiellement différer, les fonctionnalités restant toutefois identiques.

Les copies de sauvegarde sont créées via le logiciel Rescue and Recovery™ dans l'environnement Windows actif. Sur les ordinateurs avec Rescue and Recovery, Sophos SafeGuard Disk Encryption conseille à l'utilisateur de créer impérativement une nouvelle copie de sauvegarde du système une fois l'installation effectuée avec succès.

La manière de créer une sauvegarde du système à partir de l'environnement Windows est décrite dans les documents Lenovo correspondants.

Pour les sauvegardes, Sophos SafeGuard Disk Encryption prend en charge les supports suivants :

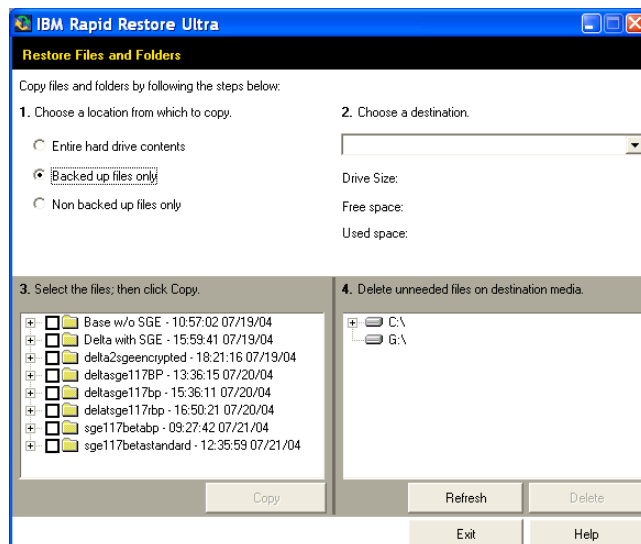
- disque dur local
- 2ème disque dur
- disque dur USB
- réseau
- Support mémoire USB
- CD/DVD



Les sauvegardes sont enregistrées par défaut dans le répertoire C:\RRUbackups. Quand il se trouve sur la partition locale du disque dur primaire, ce répertoire est protégé par Rescue and Recovery pour qu'il ne soit ni effacé, ni déplacé. Dans ce cas, la suppression est impossible.

## 21.6 Restauration de fichiers

Rescue and Recovery™ restaure sans problème des fichiers individuels ou des répertoires d'une sauvegarde Sophos SafeGuard Disk Encryption en un environnement Windows fonctionnel. Il suffit aux utilisateurs de démarrer Windows, puis le logiciel Rapid Restore et de restaurer les fichiers recherchés. Un redémarrage n'est pas nécessaire, c'est-à-dire que les données restaurées sont immédiatement disponibles pour la poursuite du traitement par l'utilisateur.



## 21.7 Restauration du système

Pour restaurer une sauvegarde Sophos SafeGuard Disk Encryption, l'utilisateur démarre l'environnement Rescue and Recovery. Ceci s'affiche lorsque vous appuyez sur cette touche pendant le démarrage du PC ou de l'ordinateur portable :

- "Thinkvantage"/"Access IBM" (ordinateurs portables Lenovo).
- Touche « Entrée bleue » (ordinateurs de bureau Lenovo).
- [F11] sur tout autre clavier.

### Remarque relative à Rescue and Recovery™ 2.0 :

Nous recommandons en général de restaurer le disque dur complet.

Si vous avez cependant sélectionné par inadvertance l'option « Ne restaurer que le système d'exploitation Windows et les applications depuis la sauvegarde », nous ne garantissons pas que les fichiers Sophos SafeGuard Disk Encryption seront complètement restaurés. Si, dans ce cas, des problèmes surviennent à l'amorçage, vous ne devez pas craindre de conséquences négatives pour votre système. Après un redémarrage, appelez simplement l'environnement Rescue and Recovery™ avec la touche Lenovo de votre PC ou Notebook et restaurez l'ensemble du disque dur.

### 21.7.1 Environnement de démarrage

Pour amorcer l'environnement Rescue and Recovery, les conditions suivantes doivent être remplies :

Sophos SafeGuard Disk Encryption **autorise** l'amorçage de l'environnement Rescue and Recovery à partir du...

- *disque dur local*  
Partition virtuelle sur le disque dur local ou partition IBM\_SERVICE locale

Sophos SafeGuard Disk Encryption **n'autorise PAS** l'amorçage de l'environnement Rescue and Recovery à partir d'un...

- CD exécutable
- Disque dur USB exécutable

Si l'environnement Rescue and Recovery est amorcé quand même à partir d'un support externe, Sophos SafeGuard Disk Encryption est supprimé pendant le processus de restauration.

Pour sauvegarder à nouveau le système, Sophos SafeGuard Disk Encryption doit être réinstallé.

## 21.7.2 Restauration d'un système Sophos SafeGuard Disk Encryption

1. Ouvrir l'environnement Rescue and Recovery en appuyant sur la touche « Thinkvantage » (ordinateur portable) ou la touche « Entrée » bleue.
2. L'invite d'authentification avant amorçage apparaît. L'utilisateur doit entrer les données Sophos SafeGuard Disk Encryption.
3. L'interface utilisateur de l'environnement Rescue and Recovery apparaît.
4. L'écran de bienvenue s'affiche. Cliquez sur le bouton **Suivant** pour continuer.
5. Dans le menu de gauche, sélectionnez **Restaurer via sauvegarde**.
6. La boîte de dialogue **Restaurer d'une sauvegarde** apparaît.
7. Sélectionnez la sauvegarde SafeGuard Sophos Disk Encryption et restaurez.

## 21.8 Partitions de récupération de service et d'usine

Lenovo fournit de nouveaux PC dotés de partitions préinstallées, appelées "partition de service (service partition)" et "partition de récupération usine (factory recovery partition)" :

- Partition de service : contient l'environnement d'initialisation Rescue and Recovery.
- Partition de récupération usine : contient toutes les informations pour la récupération des paramètres d'usine de l'ordinateur.

Si votre ordinateur ne comporte pas encore de partition de service, et si vous voulez quand même travailler avec, créez-la avant d'installer Sophos SafeGuard Disk Encryption.

Pour créer la partition de service, consultez la documentation Lenovo correspondante.

## 21.8.1 Particularités

Les particularités suivantes doivent être notées quand vous utilisez la partition de service et de récupération usine :

| Système d'exploitation | Mode de chiffrement Sophos SafeGuard Disk Encryption | État des deux partitions spéciales  |
|------------------------|--|---|
| Windows 2000           | Par partition  | Les partitions ne sont pas chiffrées.   |
| Windows XP             | Par partition  | Avantage : les paramètres d'usine Lenovo peuvent être restaurés du disque dur local.<br>Inconvénient : les pirates informatiques peuvent manipuler un environnement d'amorçage Rescue and Recovery non chiffré. |

Nous recommandons, soit de chiffrer la partition de service, soit d'installer l'environnement Rescue and Recovery sur la partition virtuelle. La partition virtuelle est toujours protégée dès que le disque système de Windows est chiffré.

## 21.9 Que faire, si ...

... un avertissement de virus est affiché à l'écran par Sophos SafeGuard Disk Encryption après redémarrage de l'ordinateur ?



Causes possibles :

1. *Le système contient un virus.*

Contactez sans retard votre administrateur système.

2. Vous avez oublié, après l'installation, la modification ou la désinstallation de Rescue and Recovery, de synchroniser le MBR avec la commande `MBRsync.exe`.

Sophos SafeGuard Disk Encryption détecte des modifications du MBR et affiche un avertissement de virus, si nécessaire. Par précaution utilisez la sauvegarde de noyau système du support de secours créé avant, voir [Sauvegarde du noyau du système et création de supports de secours](#) sur page 130.

#### ... le système de fichiers est endommagé ?

Il suffit ici, en règle générale, de charger simplement une copie de sauvegarde (avec Sophos SafeGuard Disk Encryption) avec Rescue and Recovery.

En alternative, le disque dur peut être déchiffré via la disquette de secours et l'utilitaire DOS `Sgeasy.exe` (désinstallation de Sophos SafeGuard Disk Encryption). Le disque dur est alors de nouveau disponible en texte clair et peut être traité avec les outils de sauvegarde de fichiers normaux. Si l'utilisateur n'est pas autorisé à désinstaller Sophos SafeGuard Disk Encryption en raison de droits insuffisants, la procédure Requête/Réponse de Sophos SafeGuard Disk Encryption peut être activée pour accorder un droit provisoire à cet effet à l'utilisateur.

#### ... le disque dur est physiquement endommagé ?

Si le disque dur est physiquement endommagé et ne peut pas être déchiffré, même avec `Sgeasy.exe`, nous contactons à la demande des partenaires spécialisés dans le sauvetage de disques durs physiquement endommagés.

#### ... le noyau système Sophos SafeGuard Disk Encryption est endommagé ?

Avec les défauts minimales, comme un MBR écrasé, `Sgeasy.exe` répare le MBR ou charge une sauvegarde du noyau système préalablement enregistrée.

**...if the initial encryption has been interrupted and the computer cannot be booted up to Windows any more?**

In this case contact the Sophos technical support.

**...if the final decryption has been interrupted and the computer cannot be booted up to Windows any more?**

In this case contact the Sophos technical support.

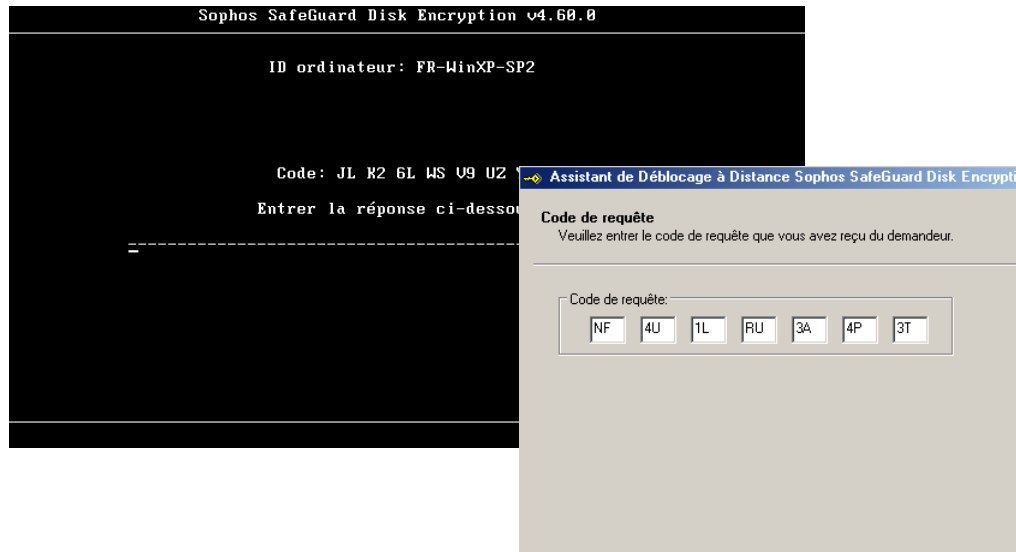
## **22 Compatibilité avec le logiciel Absolute Computrace**

Lenovo protège ses nouveaux ordinateurs portables Thinkpad avec de nombreuses fonctions de sécurité (entre autres Sophos SafeGuard Disk Encryption et SafeGuard PrivateDisk) et garantit ainsi à leurs utilisateurs une sécurité « mobile » élevée. En complément de ces produits de la famille SafeGuard, Computrace, d'Absolute Software Corp. est également installé en usine sur les ordinateurs portables Lenovo.

Computrace aide à retrouver un ordinateur portable en cas de vol, dès que l'appareil volé est connecté à Internet. À la demande du propriétaire légal, il permet également d'effacer des données confidentielles de l'ordinateur volé. Lenovo est le seul constructeur à intégrer Computrace dans le matériel de l'ordinateur (BIOS persistent agent).

Grâce à sa compatibilité avec Sophos SafeGuard Disk Encryption, le logiciel Computrace fonctionne avec des disques durs chiffrés.

## 23 Maintenance à distance (Requête/Réponse)

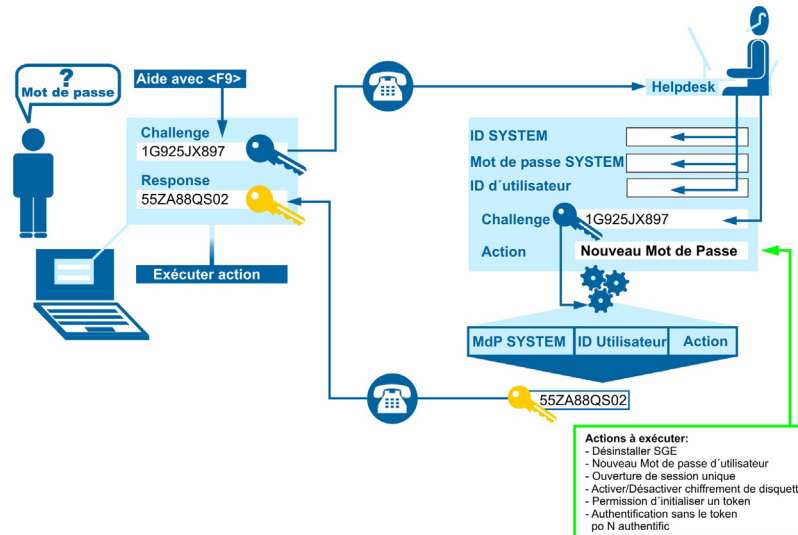


Sophos SafeGuard Disk Encryption propose la procédure de Requête/Réponse pour réinitialiser des mots de passe Sophos SafeGuard Disk Encryption « oubliés ».

La procédure Requête/Réponse est très sûre et très efficace :

- pas d'échange de données confidentielles ;
- écoute ou interception de données est sans effets ;
- utilisation également avec des appareils sans connexion réseau ;
- utilisateur peut reprendre son travail en très peu de temps.

## 23.1 Mode de fonctionnement



Si un utilisateur (utilisateur supprimé) a besoin d'aide, il doit générer un code de requête. Ce code de requête est affiché sur l'ordinateur de l'utilisateur sous forme de chaîne de caractères ASCII. L'utilisateur appelle ensuite son administrateur (helpdesk) et lui fournit ses informations personnelles et le code de requête. Le personnel d'assistance ouvre l'assistant de déblocage à distance Sophos SafeGuard Disk Encryption et génère le code de réponse. Ce personnel fournit le code de réponse à l'utilisateur via téléphone ou SMS. Après saisie de ce code de réponse, l'utilisateur peut redéfinir son mot de passe.

En règle générale, les droits spéciaux suivants peuvent être octroyés via Requête/Réponse :

- définition d'un nouveau mot de passe d'utilisateur Sophos SafeGuard Disk Encryption (quand l'ancien a été oublié)
- désinstallation de Sophos SafeGuard Disk Encryption
- ouverture de session unique (par ex. pour travaux de maintenance)

## 23.2 Création d'un code de requête

Le code de requête est généré par l'utilisateur qui a par ex. oublié son mot de passe Sophos SafeGuard Disk Encryption. Indépendamment du type de démarrage du système, il en résulte des méthodes différentes à la création du code de requête.

### Démarrage du système avec PBA

Lors du démarrage du système avec PBA, l'utilisateur doit entrer son nom Sophos SafeGuard Disk Encryption dans la PBA, puis modifier son mot de passe. Le code de requête est affiché après appui sur F9.



### Démarrage du système sans PBA

Au démarrage du système sans PBA, un symbole de disquette apparaît pendant quelques secondes dans le coin de gauche dans le haut de l'écran lors de l'amorçage de l'ordinateur. L'utilisateur doit appuyer sur la touche F2 pendant ce laps de temps. La boîte de dialogue d'ouverture de session de la PBA s'ouvre et l'utilisateur y entre son nom Sophos SafeGuard Disk Encryption dans la PBA. Le champ de mot de passe est ensuite activé. Le code de requête est affiché après appui sur F9.

### Cas particulier : désinstallation

Pour désinstaller Sophos SafeGuard Disk Encryption via Requête/Réponse, le code de requête doit être généré dans la boîte de dialogue de désinstallation (Programmes \ Panneau de configuration \ Ajout \ Suppression de Programmes, puis « Sophos SafeGuard Disk Encryption »). Une désinstallation de Sophos SafeGuard Disk Encryption avec la fonctionnalité Requête/Réponse ne peut pas être lancée dans la PBA.

## 23.3 Code de réponse

Le code de réponse est généré par l'administrateur ou le collaborateur du service d'assistance avec l'assistant de déblocage à distance.

Quiconque génère le code de réponse doit d'abord connaître les données d'un profil d'utilisateur Sophos SafeGuard Disk Encryption sur un ordinateur éloigné, par ex. les données du profil utilisateur « Helpdesk ». Sur l'ordinateur de l'utilisateur, « Helpdesk » doit avoir au moins les mêmes droits que le demandeur Sophos SafeGuard Disk Encryption.

Pour que le profil d'utilisateur « Helpdesk » puisse octroyer des droits spéciaux, il doit disposer pour l'action concernée des droits d'utilisateur suivants :

| Action Sophos SafeGuard Disk Encryption | Droit d'utilisateur requis de Sophos SafeGuard Disk Encryption |
|---|--|
| Pour une désinstallation                | Désinstallation de Sophos SafeGuard Disk Encryption            |
| Définir un nouveau mot de passe         | Modifier les paramètres de l'utilisateur                       |
| Ouverture de session unique             | Modifier les paramètres de l'utilisateur                       |

### 23.3.1 Créer un code de réponse

#### Remarque :

Critères de génération d'un code de réponse sur un ordinateur : Assistant de code de réponse.

Démarrez l'assistant via **Programmes \ Sophos \ SafeGuard Disk Encryption \ Assistant de déblocage à distance**.

La première boîte de dialogue affiche des informations sur l'assistant. Confirmez successivement la saisie en cliquant sur **Suivant**.

#### Compte d'autorisation

Dans la boîte de dialogue suivante, sélectionnez l'utilisateur Sophos SafeGuard Disk Encryption avec lequel vous souhaitez ouvrir une session dans le système de l'utilisateur à distance.

- **SYSTEM :**  
Nom de l'administrateur du système pour Sophos SafeGuard Disk Encryption.

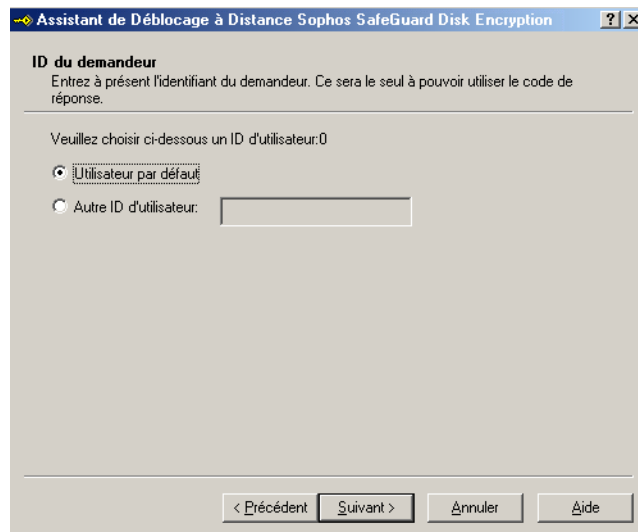
- **Utilisateur avec droit « Génération d'un code C/R abrégé » :**  
L'utilisateur auquel ce pouvoir a été affecté sur le système cible.  
Il doit posséder au moins les droits de l'utilisateur à distance.
- **Autre ID d'utilisateur :**  
Nom d'un utilisateur Sophos SafeGuard Disk Encryption pouvant octroyer le droit spécial.

Les noms de l'utilisateur choisis ici influent sur la longueur du code réponse généré ultérieurement. Plus il est long, plus grand est le risque d'erreurs au moment de sa saisie et/ou de sa transmission à l'utilisateur.

| ID d'utilisateur                | Longueur de la réponse (caractères) |
|---------------------------------|-------------------------------------|
| SYSTEM                          | 30                                  |
| Autre ID d'utilisateur          | 56                                  |
| Génération d'un code C/R abrégé | 30                                  |

### ID du demandeur distant

Dans la boîte de dialogue suivante, sélectionnez le nom de l'utilisateur distant. Demandez à cet utilisateur de fournir les données d'ouverture de session.

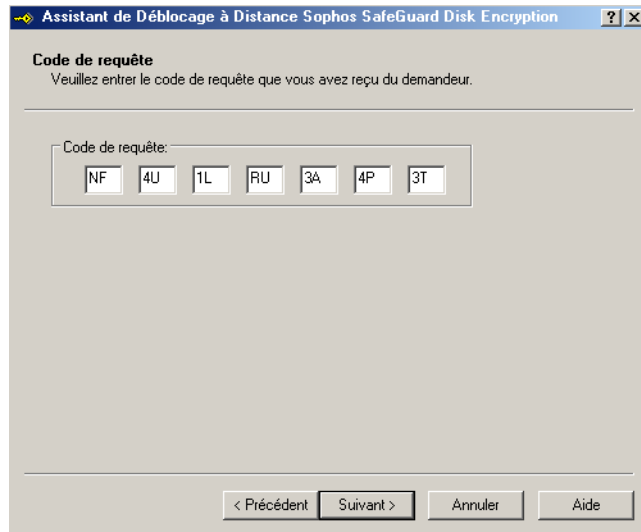


- **Utilisateur par défaut :**  
l'utilisateur ouvre sa session avec son mot de passe Sophos SafeGuard Disk Encryption. Ceci signifie qu'il est enregistré comme utilisateur par défaut sur le système cible et qu'il ne connaît pas son nom d'utilisateur par défaut.
- **Autre ID d'utilisateur :**  
l'utilisateur ouvre sa session avec le nom d'utilisateur Sophos SafeGuard Disk Encryption et le

mot de passe. Le nom de l'utilisateur Sophos SafeGuard Disk Encryption est par conséquent connu. Entrez-le dans le champ.

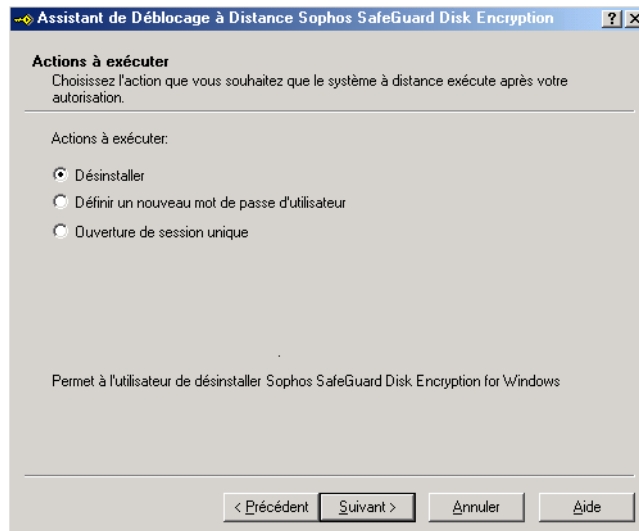
## Code de requête

Dans les champs répartis par paires de la boîte de dialogue suivante, tapez le code que l'utilisateur distant vous a transmis (p.ex. Par téléphone). Le **code de requête** s'affiche sur l'ordinateur de l'utilisateur comme chaîne de caractères ASCII (14 caractères).



## Commande distante

Dans la boîte de dialogue suivante, sélectionnez l'action qui doit être exécutée par l'utilisateur.



Une des actions suivantes peut être exécutée :

■ **Désinstaller**

L'utilisateur est autorisé à désinstaller Sophos SafeGuard Disk Encryption. Ce mode de désinstallation n'est utile que lorsque l'administrateur du système est absent.

■ **Définir un nouveau mot de passe d'utilisateur**

L'utilisateur peut modifier son mot de passe, par ex. quand il a oublié l'ancien ou quand le temps d'attente à la PBA est dépassé à la suite d'une saisie incorrecte répétée du mot de passe.

Le mot de passe de l'utilisateur SYSTEM ne peut pas être de nouveau attribué via Requête/Réponse.

■ **Ouverture de session unique**

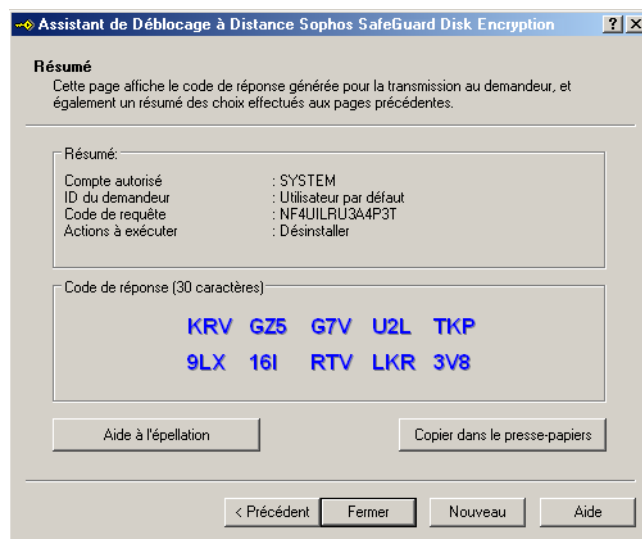
L'utilisateur obtient l'accès à l'ordinateur concerné pour la durée d'une session de travail).

Ceci peut être utile, par ex. quand un technicien exécute des travaux de maintenance.

Le code de réponse est généré quand la saisie est confirmée.

## Résumé

Dans la dernière boîte de dialogue, vous obtenez un aperçu complet des paramètres que vous avez définis dans les boîtes de dialogue précédentes de l'assistant de déblocage à distance. Ce qui suit est en outre affiché :



### Code de réponse

Affiche le code de réponse en lettres bleues. Ce code doit être transmis au demandeur. Le demandeur entre le code de réponse dans les champs prévus à cet effet. Le code de réponse n'est valable qu'une seule fois !

Un nouveau code doit être généré pour chaque requête.

### Copie dans le Presse-papiers

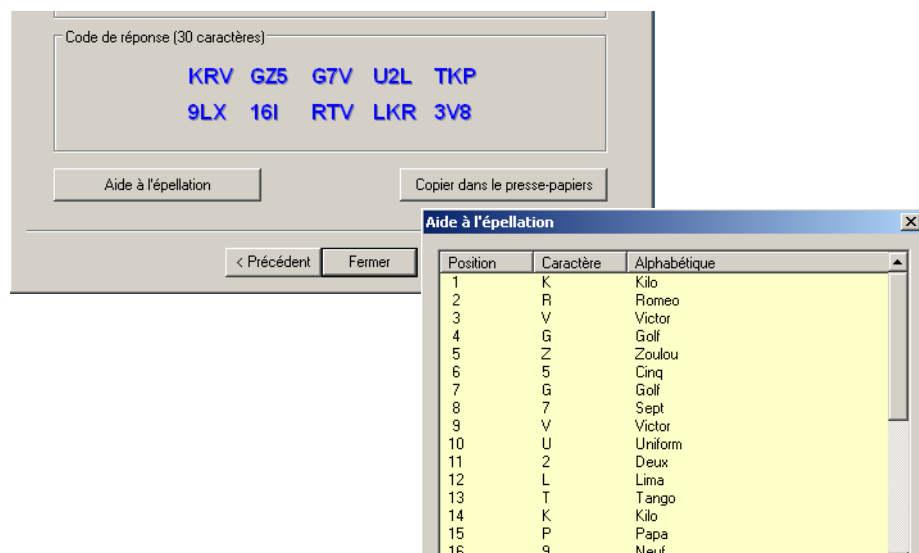
Le code de réponse est copié dans le Presse-papiers et peut être entré dans n'importe quel éditeur de texte. Cette fonctionnalité permet, par exemple, d'envoyer le code de réponse de façon simple par SMS ou courrier électronique à l'utilisateur.

Si toutes les valeurs sont correctes et si le demandeur a pu exécuter les actions requises, l'assistant de déblocage à distance est fermé en cliquant sur **Quitter**. Un clic sur **Nouveau** efface toutes les valeurs et permet de générer un nouveau code de réponse ou un code supplémentaire.

### Aide à l'épellation

Pour faciliter la transmission du code et pour éviter les erreurs, l'assistant de déblocage à distance inclut un correcteur orthographique.

Quand vous cliquez sur le bouton **Aide à l'épellation**, une fenêtre divisée en trois colonnes apparaît avec les titres de colonne correspondants. « Position » indique l'emplacement du caractère dans le code. Il est ainsi possible de répondre sans perte de temps (par exemple, décompte des positions) aux questions. Vous pouvez voir le caractère qui doit être entré. « Alphabétique » indique avec quel mot le caractère peut être « lié » pour éviter les confusions, comme les mots de code radio (dans cet exemple). En règle générale, on utilise des prénoms dont la première lettre est alors entrée dans les champs de code. La fenêtre affiche le code de réponse réel. Il vous suffit de le lire de haut en bas.



## 24 Sauvegarde du noyau du système et création de supports de secours

Le noyau du système contient toutes les fonctions nécessaires à l'authentification sur l'ordinateur, ainsi que les pilotes requis au démarrage d'un système d'exploitation et tous les paramètres système d'un client Sophos SafeGuard Disk Encryption. Si, en situation d'urgence, le noyau du système d'un client Sophos SafeGuard Disk Encryption est endommagé et que l'utilisateur ne peut plus se connecter au système, une copie de sauvegarde à jour du noyau du système intact est requise pour le restaurer à son état initial et permettre au système de fonctionner à nouveau.

Si votre ordinateur possède un disque dur chiffré et que des messages d'erreur de Sophos SafeGuard Disk Encryption s'affichent, cela signifie probablement que le noyau du système Sophos SafeGuard Disk Encryption est introuvable.

Sophos SafeGuard Disk Encryption propose les fonctions de récupération de système suivantes :

- Sauvegarde automatique du noyau du système
- Assistant de création d'une disquette de secours
- Outil de récupération d'urgence `Sgeasy.exe`

Sophos SafeGuard Disk Encryption sauvegarde automatiquement le noyau du système dans l'ordinateur, sans intervention de l'utilisateur, afin que la version la plus récente du noyau soit toujours disponible sur le disque dur.

Cependant, si une erreur système intervient, le disque dur peut ne plus être accessible. Il est donc recommandé de créer une disquette de secours en plus de la sauvegarde (disquette, CD-ROM ou clé USB). Cette disquette de secours contient la sauvegarde du noyau du système, ainsi que plusieurs fichiers de secours qui vont permettre de résoudre les erreurs Sophos SafeGuard Disk Encryption et d'accéder de nouveau à votre ordinateur.

### 24.1 Sauvegarde de automatique de noyau du système

Lorsqu'il est installé ou soumis à une modification, le noyau du système est sauvegardé automatiquement. Aucune intervention de l'utilisateur n'est requise pour la sauvegarde automatique du noyau du système. Cette tâche est effectuée par une fonction de sauvegarde automatique. Même si des modifications sont apportées à la configuration de Sophos SafeGuard Disk Encryption (par exemple via l'exécution de fichiers de configuration), le client Sophos SafeGuard Disk Encryption génère la sauvegarde automatiquement. Pour plus de sécurité, la dernière et l'avant-dernière version du noyau du système sont sauvegardées.

Le noyau du système est toujours sauvegardé sur le disque dur, par défaut. Vous pouvez toutefois stocker la sauvegarde sur un support externe. Pour cela, vous devez définir une clé dans le registre Windows.

## 24.2 Sauvegarde manuelle du noyau du système

En complément de la sauvegarde automatique, vous pouvez à tout moment effectuer une sauvegarde manuelle du noyau du système et l'enregistrer à un emplacement spécifié. Cette option est utile pour les sauvegardes planifiées, par exemple.

Cette tâche s'effectue à l'aide des outils suivants :

Assistant de création d'une disquette de secours (voir [Comment créer une disquette de secours/sauvegarde du noyau du système](#) sur page 131).

Ligne de commande (voir [Sauvegarde du noyau système via la ligne de commande](#) sur page 134).

## 24.3 Comment créer une disquette de secours/sauvegarde du noyau du système

L'Assistant de création d'une disquette de secours ", présent après chaque installation par défaut sur un client, vous permet de lancer une sauvegarde du noyau du système ou de créer une disquette de secours.

Cette disquette de secours est un disque de démarrage et contient la sauvegarde du noyau du système, ainsi que plusieurs fichiers de secours qui vont permettre de résoudre les erreurs Sophos SafeGuard Disk Encryption et d'accéder de nouveau à votre ordinateur.

Pour s'assurer que la disquette de secours contient systématiquement la dernière version du noyau, il est fortement recommandé de sauvegarder sur cette dernière toute modification importante, telle qu'une modification de l'état du chiffrement. Vous pouvez configurer une fonction de rappel qui vous invite à sauvegarder le noyau du système à intervalles réguliers. Vous devez ensuite copier cette sauvegarde sur les supports amovibles de secours.

**Remarque :** Pour créer un CD de démarrage et pour exécuter un démarrage d'urgence consultez les articles suivants dans la base de connaissances :

<http://www.sophos.com/support/knowledgebase/article/56544.html>

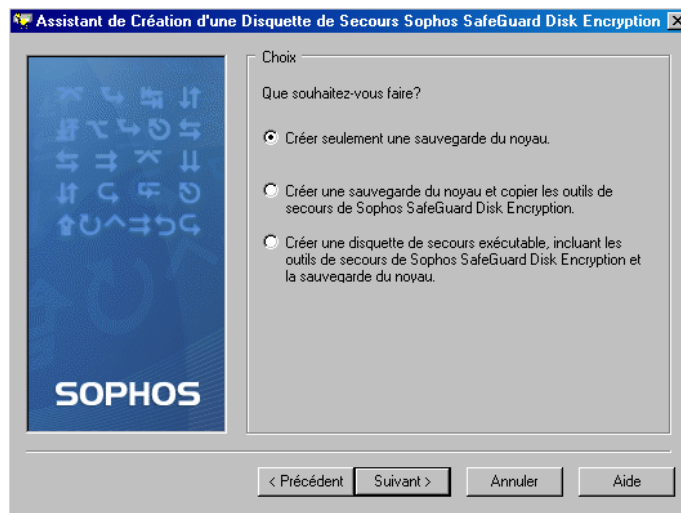
<http://www.sophos.com/support/knowledgebase/article/56456.html>

### 24.3.1 Exécution de l'Assistant de création d'une disquette de secours

Exécutez L'Assistant de création de disquette de secours en sélectionnant Programmes\Sophos\SafeGuard Disk Encryption\Assistant de création de disquette de secours.

Pour valider les données entrées dans l'assistant, cliquez sur Suivant.

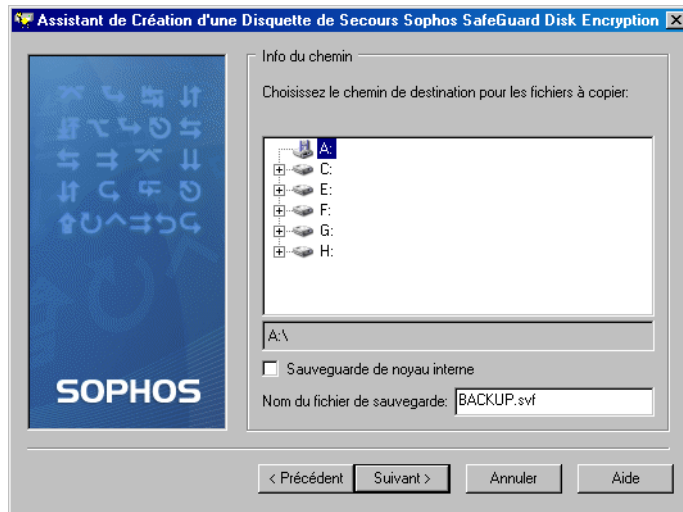
1. Une fois l'Assistant démarré, une seconde boîte de dialogue s'affiche. Cette boîte de dialogue permet de spécifier les fichiers à enregistrer sur la disquette de démarrage d'urgence.



Les options ci-dessous sont disponibles :

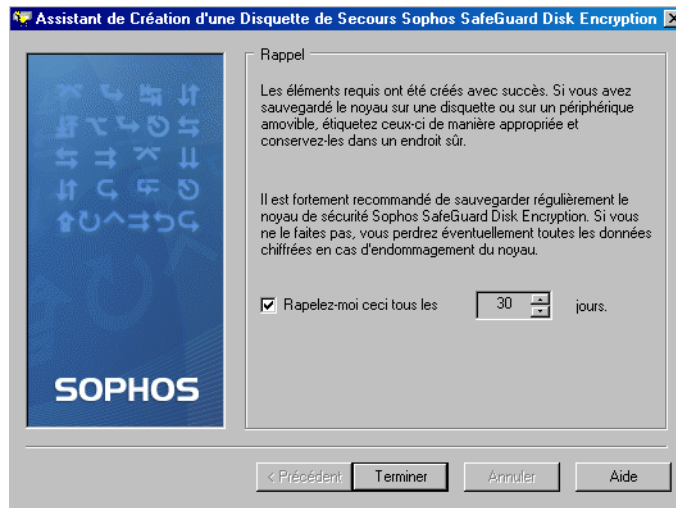
- **Créer seulement une sauvegarde du noyau**  
Cette fonction sauvegarde le noyau système complet (pilotes pour Sophos SafeGuard Disk Encryption et le MBR) dans un fichier.
  - **Créer une sauvegarde du noyau et copier les outils de secours de Sophos SafeGuard Disk Encryption**  
Copie le noyau système et les fichiers de démarrage suivants :
  - **Créer une disquette de secours exécutable, incluant les outils de secours de Sophos SafeGuard Disk Encryption et la sauvegarde du noyau**  
Crée une disquette exécutable avec une version FreeDOS, le noyau système et les fichiers de démarrage.
2. Dans **Info du chemin**, vous choisissez ensuite l'endroit où les données (noyau système et fichiers de secours) doivent être enregistrées.  
Vous pouvez enregistrer le noyau système internement, sur un lecteur local ou sur un réseau.  
En cas d'erreur système, cependant, il est probable que vous ne pourrez pas accéder au disque dur. Vous devez pas conséquent toujours stocker le noyau système et les fichiers de

démarrage d'urgence sur un support amovible comme un CD, un clé de USB ou sur un lecteur réseau.



- Si vous avez choisi **Créer seulement une sauvegarde du noyau**, le champs **Sauvegarde de noyau interne** est activé par défaut et la sauvegarde de noyau est enregistrée internement sur le disque dur local.
- Pour enregistrer le sauvegard de noyau dans un autre emplacement, désactivez le champs **auvegarde de noyau interne** et indiquez un emplacement différent.
- Si vous avez choisi **Créer une sauvegarde du noyau et copier les outils de secours de Sophos SafeGuard Disk Encryption** ou **Créer une disquette de secours exécutable**, indiquez l'emplacement d'enregistrement du noyau système et des fichiers d'urgence (si sélectionnés). Entrez le nom du noyau système dans le champ *Nom du fichier de sauvegarde*. La valeur par défaut est `BACKUP.svf`, mais vous pouvez modifier le nom et l'extension `.svf` si nécessaire. Vous pouvez enregistrer le noyau système internement, sur un lecteur local ou sur un réseau.

3. Dans la boîte de dialogue *Rappel*, vous pouvez indiquer ici les intervalles de rappels de sauvegarder du noyau système.



Dans la mesure où il est essentiel que vous disposiez de la version la plus récente du noyau système en cas d'erreur système, nous recommandons fortement de procéder toujours à des sauvegardes régulières.

### 24.3.2 Sauvegarde du noyau système via la ligne de commande

Le noyau système peut être également sauvegardé à partir de la ligne de commande de la manière suivante :

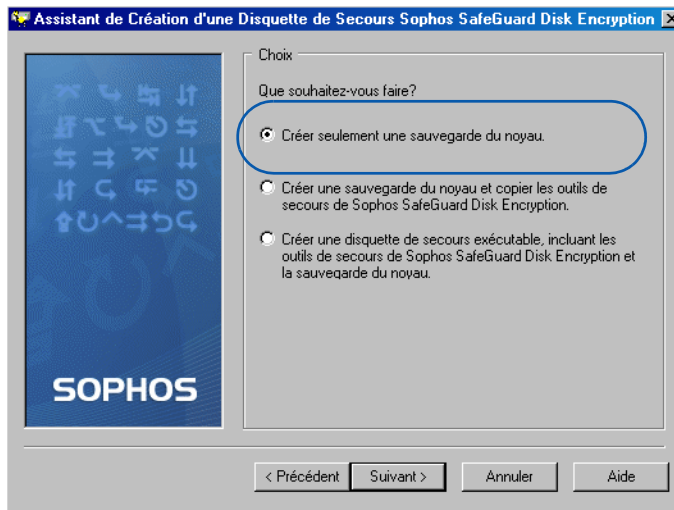
```
SGEBACK.EXE /f :<chemin/nom de fichier> | /?
```

/f :           Affiche le chemin et le nom de fichier utilisé pour enregistrer le noyau.  
              Vous pouvez donner le nom et l'extension de votre choix au fichier cible.

//?           Affiche cette aide

## 24.4 Création d'un CD de démarrage

En cas d'urgence vous pouvez utiliser un CD de secours pour récupérer l'accès à l'ordinateur.



**Prérequis :** le BIOS de l'ordinateur doit prendre en charge le démarrage à partir d'un CD.

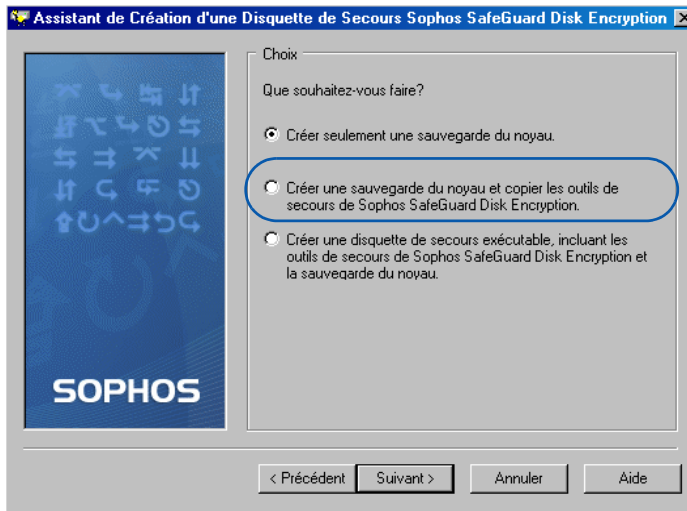
Pour créer un CD de démarrage, exécutez les actions suivantes sur l'ordinateur de l'utilisateur final :

1. Créer une sauvegarde du noyau de système:
  - a) Sur l'ordinateur de l'utilisateur final, ouvrez l'**assistant de création d'une disquette de secours** dans le dossier Sophos SafeGuard Disk Encryption du menu **Démarrer**.
  - b) Dans **Choix**, sélectionnez **Créer seulement une sauvegarde du noyau**.
  - c) Dans **Chemin**, sélectionnez l'emplacement de la sauvegarde du noyau du système.
  - d) Cliquez sur **Terminer**.
2. Créer un CD de démarrage. Suivez les instructions dans l'article suivant de la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/56544.html>.
3. Copiez la sauvegarde du noyau précédemment créée de l'emplacement de stockage sur le CD de démarrage.

Nous recommandons de créer un CD de démarrage après l'installation et de mettre à jour celle-ci dès que le noyau système est modifié.

## 24.5 Création d'une clé USB de démarrage

En cas d'urgence vous pouvez utiliser une clé USB de secours pour récupérer l'accès à l'ordinateur.



**Prérequis :** le BIOS de l'ordinateur doit prendre en charge le démarrage à partir d'une clé USB.

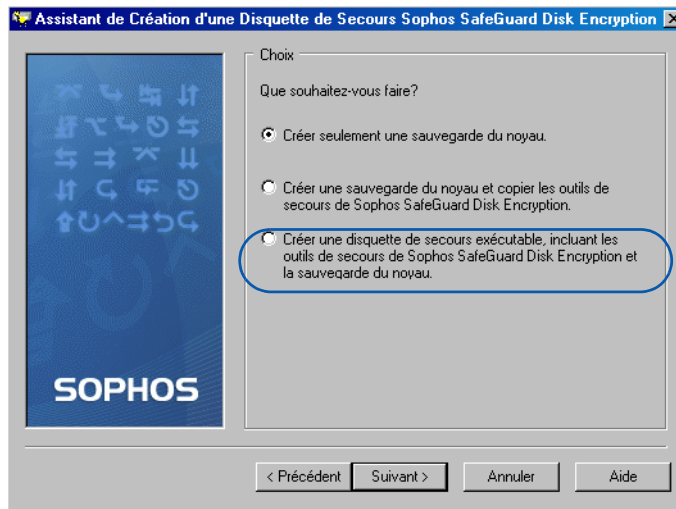
Pour créer une clé USB de démarrage, exécutez les actions suivantes sur l'ordinateur de l'utilisateur final :

1. Formatez la clé USB de façon à créer une clé de démarrage.
2. Sur l'ordinateur de l'utilisateur final, ouvrez l'**assistant de création d'une disquette de secours** dans le dossier Sophos SafeGuard Disk Encryption du menu Démarrer.
3. Dans **Choix**, sélectionnez **Créer une sauvegarde du noyau et copier les outils de secours Sophos SafeGuard Disk Encryption**.
4. Dans **Chemin**, sélectionnez l'emplacement de la sauvegarde du noyau du système et des outils de secours.
5. Cliquez sur **Terminer**.
6. Copiez la sauvegarde du noyau et les outils de secours Sophos Disk Encryption sur la clé USB de secours.

Nous recommandons de créer une clé USB de démarrage e après l'installation et de mettre à jour celle-ci dès que le noyau système est modifié.

## 24.6 Création d'une disquette de démarrage

L'Assistant propose en outre l'option de création d'une disquette de démarrage avec noyau système, outils de secours et fichiers de pilotes pour la configuration du clavier. Cette option simple permet de combiner disquette de démarrage et disquette de secours Sophos SafeGuard Disk Encryption.



**Prérequis :** le BIOS de l'ordinateur doit prendre en charge le démarrage à partir d'une disquette.

Pour créer une disquette de démarrage, exécutez les actions suivantes sur l'ordinateur de l'utilisateur final :

1. Insérez une disquette et lancez l'Assistant de création de disquette de secours.
2. Sélectionnez l'option **Créer une disquette de secours exécutable, incluant les outils de secours de Sophos SafeGuard Disk Encryption et la sauvegarde du noyau.**

La sauvegarde du noyau et les outils de secours sont copiées sur la disquette.

3. Cliquez sur **Terminer**.

Nous recommandons de créer un support amovible amorçable après l'installation et de mettre à jour celle-ci dès que le noyau système est modifié.

### 24.6.1 Sauvegarde des fichiers de secours Sophos SafeGuard Disk Encryption sur disquette

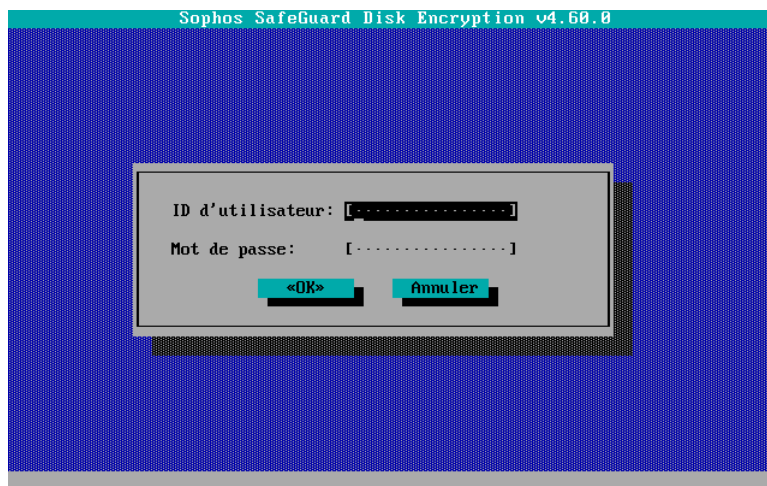
Vous pouvez également enregistrer les fichiers d'urgence sur une disquette de façon manuelle. Copiez les fichiers suivants du répertoire d'installation de Sophos SafeGuard Disk Encryption :

- SGEASY.exe
- Sgeasy.hmf  
Sgecrypt.mod
- Sgenls.mod
- Sgekrnl.mod

## 24.7 Exécution d'un démarrage d'urgence

En cas de problème sur un disque dur chiffré, procéder comme suit :

1. Insérez une disquette ou un support amovible de secours et démarrez l'ordinateur .
2. Le programme des secours `Sgeasy.exe` est lancé automatiquement.
3. Entrez le mot de passe Sophos SafeGuard Disk Encryption. Confirmez la saisie en cliquant sur OK.



4. Un menu avec les rubriques *Désinstaller*, *Sauvegarder*, *Restaurer* et *Réparer* apparaît.



Remarque : Vous trouverez plus d'informations dans l'article suivant de la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/56456.html>.

### 24.7.1 Restauration du noyau système

Le noyau système est automatiquement sauvegardé internement sur le disque dur. C'est pourquoi une sauvegarde valide et récente du noyau système est toujours disponible sur le poste de travail utilisé pour restaurer le noyau système. Après sélection de la fonction **Restaurer**, le système demande que vous voulez utiliser la sauvegarde interne.

- Si vous choisissez **Oui**, le MBR (Master Boot Record) et le noyau système Sophos SafeGuard Disk Encryption sont restaurés par utiliser la sauvegarde interne sur l'ordinateur.
- Si vous choisissez **Non**, vous pouvez chercher la sauvegarde de noyau nécessaire.

Cette fonction *ne doit pas* être exécutée si

- Sophos SafeGuard Disk Encryption a été précédemment désinstallé
- la sauvegarde du noyau système ne correspond plus à sa version actuelle. C'est le cas quand, par exemple, l'état de chiffrement du ou des disques durs a été modifié entre la sauvegarde et la restauration du noyau système.

Tous les utilisateurs de Sophos SafeGuard Disk Encryption (et pas seulement l'utilisateur « SYSTEM ») peuvent restaurer le noyau système.

### 24.7.2 Réparation du noyau système

Contrairement à la fonction « Restaurer », une réparation s'effectue également sans copie de sauvegarde du noyau système. La fonction de réparation parcourt la totalité du disque dur à la

recherche du noyau système Sophos SafeGuard Disk Encryption et essaie de le restaurer (succès non garanti !).

Cette fonction est requise uniquement quand la sauvegarde du noyau système ne correspond plus à sa version actuelle.

Après sélection de la fonction « Réparer », une routine de diagnostic essaie de localiser le noyau système et de le réactiver. Ceci peut durer plusieurs minutes. Le déroulement est indiqué par une barre de progression. Le système vous indique ensuite si la réparation s'est effectuée avec succès.

**Remarque :** Les tentatives de résolution de panne système avec la fonction **Réparer** n'ont pas toujours le succès escompté. Il est donc recommandé de toujours disposer d'une sauvegarde récente du noyau système.

### 24.7.3 Désinstallation d'urgence de Sophos SafeGuard Disk Encryption

Quand l'erreur système ne peut être éliminée ni avec « Restaurer », ni avec « Réparer », il ne reste plus que la variante trois, le déchiffrement du disque dur et la désactivation de la PBA. Après la désinstallation, le poste de travail est redémarré automatiquement deux fois.

Cependant, avant de procéder, le profil utilisateur de Sophos SafeGuard Disk Encryption doit disposer de droits suffisants. Si un utilisateur ne dispose pas de droits de désinstallation, ces derniers ne peuvent être affectés à l'utilisateur par l'intermédiaire de la procédure Requête/Réponse ([voir Maintenance à distance \(Requête/Réponse\)](#) sur page 122).

Il est judicieux de procéder également à une vérification des supports de données dans Windows. Vous trouverez des informations à ce sujet dans votre documentation Windows.

#### Échec du déchiffrement

Veillez contacter notre équipe de support en cas d'échec de la procédure de chiffrement ou déchiffrement.

#### Support étendu des expertises (paramètre /NoReboot)

La fonction de déchiffrement d'urgence de Sophos SafeGuard Disk Encryption inclut le paramètre de commande `/NoReboot` pour le programme d'urgence `SGEASY.exe`. Ce paramètre de ligne de commande permet d'éviter le redémarrage automatique après le déchiffrement d'urgence. Ceci est particulièrement utile en cas d'expertise du disque dur.

Comment procéder :

1. Démarrez le support d'urgence.
2. Démarrer `Sgeasy.exe /NoReboot`.

3. Le déchiffrement ou la désinstallation d'urgence est terminée
4. L'ordinateur est arrêté et le système affiche un texte d'information. Il est possible d'exécuter d'autres programmes ou d'effectuer toute autre opération avec l'ordinateur.

**Hint:** Vous trouverez plus d'informations au déchiffrement et désinstallation d'urgence dans la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/58682.html>.

### **Le disque dur est endommagé**

Veillez noter ce qui suit : Si vous suspectez que le disque dur chiffré présente des dommages physiques, il est recommandé de ne pas le déchiffrer avec un support de secours.

Un défaut physique peut se remarquer par exemple de la manière suivante : le disque dur émet de bruits de frottement ou des cliquets, ou n'est plus reconnu par le BIOS. Dans ce cas, n'intervenez pas vous-même, mais adressez-vous à un spécialiste. Ils tenteront de transférer le contenu du disque dur corrompu sur un disque intact, de façon à pouvoir procéder à un déchiffrement d'urgence des données. Cette intervention externe entraîne naturellement des frais, qui seront à opposer à la valeur des données présentes sur le disque dur.

**Remarque :** Vous trouverez plus d'informations à ce sujet dans la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/57259.html>.

## **24.7.4 Remarques**

### ■ **Emplacement du noyau système**

Si la partition d'amorçage de Windows ne se trouve pas sur le premier disque dur, le noyau système Sophos SafeGuard Disk Encryption est automatiquement stocké pendant l'installation sur la partition C:. Cette partition ne doit par conséquent plus être formatée après l'installation, car elle contient les informations Windows les plus importantes (noyau système, pilotes, etc.). Si toutefois un formatage est effectué après l'installation de Sophos SafeGuard Disk Encryption, le système doit être réinstallé.

Cette sauvegarde est toutefois spécifique au système, c'est-à-dire qu'elle ne peut être restaurée que sur l'ordinateur où elle a été effectuée.

Cependant, si une erreur système se produit, le disque dur risque de ne plus être accessible. Comme vous ne pourrez probablement pas, en cas de défaillance du système, accéder au disque dur, le noyau système et tous les fichiers de secours doivent être toujours sauvegardés sur une disquette ou sur un périphérique amovible.

### ■ **Langue de Sgeasy.exe**

La langue de l'interface utilisateur du programme de secours est déterminée par le fichier Sgeasy.hmf (qui se trouve sur la disquette de secours). Les différentes éditions du fichier de langue pour l'Allemand (Sgeasy07.hmf), l'Anglais (Sgeasy09.hmf) et le Français (Sgeasy0C.hmf) se trouvent dans le répertoire d'installation de Sophos SafeGuard Disk

Encryption. L'utilisateur doit renommer le fichier SGEASY, <09,07,0C>.hmf pour la disquette de secours, en SGEASY.HMF pour obtenir la langue souhaitée dans SGEASY.EXE.

## **24.8 Accès aux données chiffrées lors du redémarrage à partir d'un support externe**

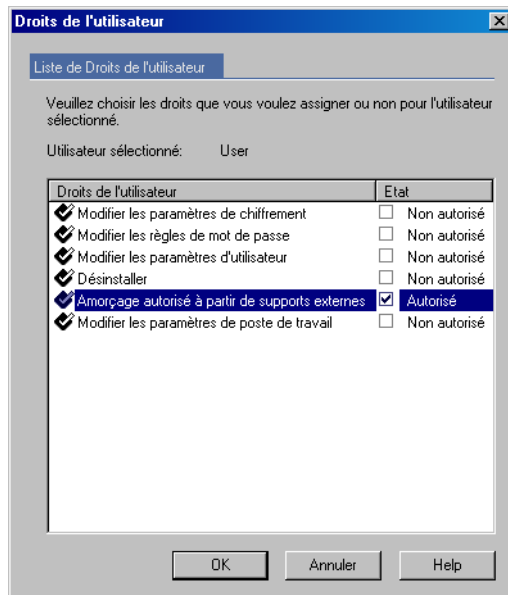
Dans certaines situations (d'urgence), les utilisateurs doivent démarrer un système chiffré avec Sophos SafeGuard Disk Encryption à partir d'un support de données externe, par exemple pour sauvegarder des données quand le système d'exploitation ne démarre plus. Les utilisateurs ne peuvent toutefois démarrer le système à partir d'un support externe (et accéder aux données sur l'ordinateur) qu'une fois que des données Sophos SafeGuard Disk Encryption valides ont été entrées dans l'authentification avant amorçage.

Cette méthode d'amorçage est recommandée pour sauvegarder des données en cas d'urgence avant la réparation du système d'exploitation ou la désinstallation d'urgence de Sophos SafeGuard Disk Encryption.

Les supports d'amorçage pris en charge par Sophos SafeGuard Disk Encryption sont les CD/clés USB (pour DOS et Windows EP) et les disquettes. Il est essentiel que les supports d'amorçage contiennent le pilote Sophos SafeGuard Disk Encryption.

### **24.8.1 Conditions**

L'amorçage à partir d'un support externe est un droit d'administrateur Sophos SafeGuard Disk Encryption qui n'est accordé, dans la configuration de base, qu'à l'utilisateur « SYSTEM ». Si le système doit être démarré à partir d'un support externe, le profil Sophos SafeGuard Disk Encryption s'étant identifié dans la PBA doit disposer du droit « Amorçage autorisé à partir de supports externes ».



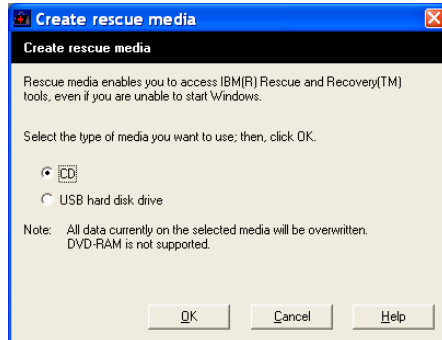
## 24.8.2 Comment procéder

1. Démarrez le système à partir du disque dur.
2. L'authentification avant amorçage de Sophos SafeGuard Disk Encryption apparaît.
3. Entrez les données dans la PBA.
4. a) Insérez la **disquette de démarrage**. Confirmez les données PBA en appuyant sur **Entrée**.  
b) Insérez le **CD de démarrage**. Confirmez les données PBA en appuyant sur **F7**.
5. L'ordinateur redémarre à partir du support de démarrage externe.
6. Une fois le redémarrage effectué avec succès, il est possible d'accéder aux données ou de les sauvegarder.

## 24.8.3 Remarques

- La version du BIOS conditionne le bon démarrage via CD/clé USB !
- Vous trouverez dans la base de connaissances une description du mode de création de CD Windows PE de démarrage.  
Vous trouverez plus d'informations à ce sujet dans la base de connaissances :  
<http://www.sophos.com/support/knowledgebase/article/57525.html>.
- La fonction Rescue and Recovery de Lenovo, « Create Rescue Media », crée automatiquement

un CD, avec pilotes Sophos SafeGuard Disk Encryption lorsque Sophos SafeGuard Disk Encryption est installé. Cette option est disponible via Programmes \ Thinkvantage.



#### 24.8.4 Que faire, si ...

... le démarrage à partir d'un support externe échoue ?

Les raisons suivantes sont possibles :

- L'utilisateur Sophos SafeGuard Disk Encryption ayant ouvert la session ne dispose pas du droit « Amorçage autorisé à partir de supports externes ».
- Le chiffrement du disque dur a été lancé, mais n'est pas encore terminé.

La raison suivante est également possible en cas d'échec de démarrage à l'aide d'une disquette :

- Le lecteur de disquettes n'est pas appelé par le contrôleur de disquettes standard, mais via l'interface USB.

### 24.9 Support de BartPE

BartPE (Bart's Preinstalled Environment) est une variante légère des systèmes d'exploitation 32 bits Microsoft Windows et peut être utilisé pour réparer des installations corrompues de Windows en cas d'urgence.

Dans le dossier de produit Sophos SafeGuard Disk Encryption vous trouverez un module d'extension spécifique avec lequel vous pouvez créer une CD de secours BartPE.

**Remarque:** Le module d'extension est valable pour Sophos SafeGuard Disk Encryption (SDE) même si il quelquefois réfère à "SGEasy" ou "SGE".

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

<http://www.sophos.com/support/knowledgebase/article/57525.html>.

## 25 Affichage de l'état système de Sophos SafeGuard Disk Encryption

Sophos SafeGuard Disk Encryption dispose d'un outil de ligne de commande, Sophos Disk Encryption State Tool (`SGEState.exe`), qui indique l'état de l'installation Sophos SafeGuard Disk Encryption sur l'ordinateur de l'utilisateur (version, chiffré/non chiffré, etc.). Cet outil convient particulièrement aux installations dans un environnement étendu en permettant à un administrateur d'interroger simplement l'état d'une installation Sophos SafeGuard Disk Encryption.

On peut également utiliser Sophos Disk Encryption State Tool pour exécuter certaines opérations ou procédures lorsque l'installation (ou le chiffrement) de Sophos SafeGuard Disk Encryption est terminée.

Vous trouverez `SGEState.exe` dans le dossier de produit Sophos SafeGuard Disk Encryption téléchargé.

### 25.1 Génération de rapports

`SGEState.exe` peut également servir à la génération de rapports :

La commande `SGEState /LD` renvoie une sortie formatée pour LANDesk (et autres produits).

Cette sortie est dirigée vers un fichier.

## 25.2 Paramètres

La commande `SGESTate` peut être appelée avec les paramètres suivants

```
SGESTATE [/?] [/Q | /L | /LD] [/E [/Mvalue]] [/Dvalue] [/R]
```

La commande `SGESTate /?` donne une vue d'ensemble de tous les paramètres de ligne de commande disponibles :

```

c:\ Invite de commandes
C:\Documents and Settings\Administrateur>sgestate.exe /?

Sophos Disk Encryption State Tool U3.16
Copyright (c) 1992 - 2009 by Utimaco Safeware AG - a member of the Sophos group.
All rights reserved

Usage: SGESTATE [/Q | /L | /LD] [/E [/Mvalue]] [/Dvalue] [/R]
/Q...Quiet mode: No output, program ends with return code:
 0...Sophos Disk Encryption not installed.
 2...Sophos Disk Encryption installed.
 3...Sophos Disk Encryption installed. Encryption or decryption process active.
255...An error occurred during the check. In this case, a message
to the console will state the nature of the problem.
/L...Loud mode. Will display details to the console including:

Operating System: [WINDOWS 2000 | WINDOWS XP | WINDOWS SERVER 2003]

Installation Status      : [INSTALLED | NOT INSTALLED | UNKNOWN |
                          INSTALLED (NOT READY FOR BACKUP)]
Version number           : [N/A | number1]
Installation Mode        : [N/A | STANDARD | PARTITIONED | BOOT PROTECTION |
                          UNKNOWN]
Disk Encryption          : [N/A | OFF | ON]
Initial Encryption       : [N/A | ACTIVE | INACTIVE]
Pre Boot Authentication  : [N/A | OFF | ON]
Current Authentication   : [N/A | USER | WAKE ON LAN]
Secure Auto Logon        : [N/A | OFF | ON]

Disk Encryption Status   : [N/A | %s | <drive letter>=<state>]
Drive letter states:

SDE volume is recognized but not encrypted           : 0
SDE volume en-/decryption in process                 : 1
SDE volume is fully encrypted                       : 2
SDE volume is unrecognized (new partition after SGE installation) : 3

Return code      : [ReturnCode]

/LD...The details are displayed in LANDesk mode

/E...Extended return code:

En-/Decryption in process      : 1
SafeGuard Lite installed      : 2
Disk Encryption "ON"          : 3
Installation Mode "Boot Protection" : 16 (hex 10)
Installation Mode "Partitioned"   : 32 (hex 20)
Installation Mode "Standard"      : 64 (hex 40)
                                only one mode is possible, (16, 32 or 64)
/Mvalue...value mask for extended return code 1..127

For example: SGESTATE /E produces return code 43 (hex 2b). This indicates:
Partitioned mode, Disk Encryption "ON", SafeGuard Lite installed, Encryption in
process

```

## 26 Audit

L'enregistrement d'événements intéressant la sécurité est la condition pour une analyse approfondie du système. Sur la base des événements audités, des opérations effectuées sur une station de travail ou dans un réseau peuvent être suivies de manière plus exacte. L'audit permet de prouver par exemple des violations de droits par des tiers non autorisés. L'audit offre également à l'administrateur une aide pour retrouver ou corriger des droits d'utilisateur refusés par erreur.

Les événements déclenchés par des produits SafeGuard installés, tels qu'une connexion par carte à puce, modification d'un code confidentiel, certificat expiré, etc, sont enregistrés dans l'observateur d'événements de Windows.

L'utilisateur possédant les droits appropriés peut visualiser les événements audités directement via l'observateur d'événements de Windows.

L'audit enregistre les événements Sophos SafeGuard Disk Encryption suivants :

- déroulement du processus d'ouverture de session à la PBA (succès/échec)
- actions d'administration (création d'un utilisateur, etc.)
- succès/échec de l'exécution de fichiers de configuration
- processus d'installation/désinstallation
- processus de chiffrement/déchiffrement

### 26.1 Visualisation des événements enregistrés

Les événements enregistrés peuvent être visualisés dans l'observateur d'événements.

L'observateur d'événements de Windows est un outil permettant de recueillir des informations de surveillance. L'observateur d'événements peut afficher et administrer des journaux pour les événements intéressant le système, la sécurité ou l'application, et également sauvegarder ces journaux d'événements. Il permet également d'enregistrer ces journaux d'événements.

Les événements enregistrés affichent les paramètres suivants :

- Ordinateur : nom de l'ordinateur sur lequel l'événement audité s'est produit.
- Date : date système à laquelle l'événement a été créé.
- Heure : heure système à laquelle l'événement a été créé.
- Utilisateur : utilisateur connecté au moment de l'événement.
- Type : classification de l'événement par Windows, par ex. avertissement, erreur.

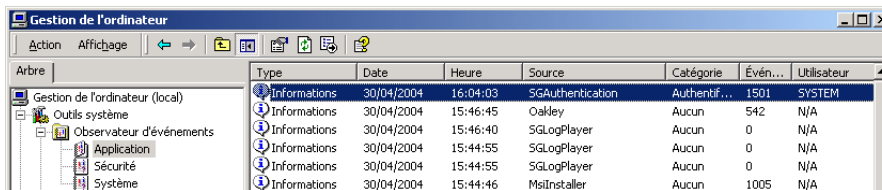
- ID événement : numéro d'identification de l'événement. Il peut s'agir de tout numéro compris entre 0 et 0xffffffff (par ex. 4 294 967 295.)
- Source : Application enregistrant l'événement, par ex. SGPWC = restrictions du mot de passe.
- Catégorie : classification de l'événement par la source.

Les événements sont toujours affichés dans la langue système définie.

### 26.1.1 Observateur d'événements

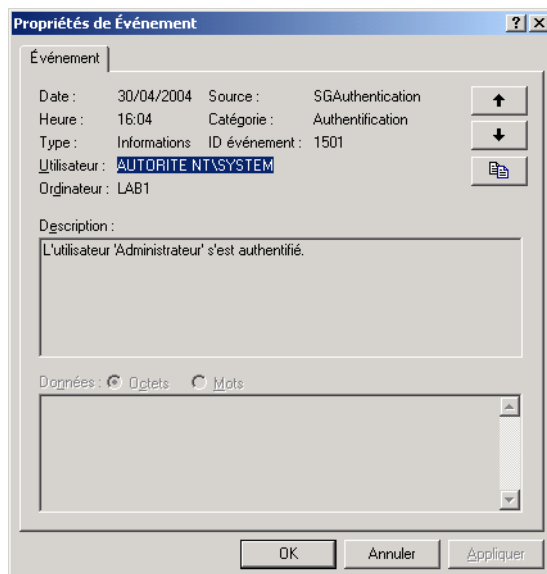
Les événements sont enregistrés dans le journal applications de l'Observateur d'événements de Windows.

Pour ouvrir l'observateur d'événements, cliquez sous Windows sur Démarrer, pointez sur Programmes, pointez sur Outils d'administration, puis cliquez sur Observateur d'événements. Dans l'arborescence de la console, cliquez sur le journal Application. Les événements s'affichent dans la fenêtre des détails. Un clic sur le journal des applications affiche ensuite les événements dans la liste détaillée.



| Type         | Date       | Heure    | Source           | Catégorie    | Évén... | Utilisateur |
|--------------|------------|----------|------------------|--------------|---------|-------------|
| Informations | 30/04/2004 | 16:04:03 | SGAuthentication | Authentif... | 1501    | SYSTEM      |
| Informations | 30/04/2004 | 15:46:45 | Oakley           | Aucun        | 542     | N/A         |
| Informations | 30/04/2004 | 15:46:40 | SGLogPlayer      | Aucun        | 0       | N/A         |
| Informations | 30/04/2004 | 15:44:55 | SGLogPlayer      | Aucun        | 0       | N/A         |
| Informations | 30/04/2004 | 15:44:55 | SGLogPlayer      | Aucun        | 0       | N/A         |
| Informations | 30/04/2004 | 15:44:46 | MsiInstaller     | Aucun        | 1005    | N/A         |

Double-cliquez sur un événement de la liste pour en afficher le détail.



## 27 Erreurs

Dans ce chapitre, vous trouverez une liste de tous les messages d'erreur. Comme à chaque message d'erreur de Sophos SafeGuard Disk Encryption le numéro d'erreur est affiché, il vous est facile de trouver le commentaire recherché.

Le format est le suivant : SDEnnnn : <texte>

« SDE » correspond à l'ID de produit Sophos SafeGuard Disk Encryption et « nnnn » est un code d'erreur à quatre chiffres.

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

<http://www.sophos.com/support/knowledgebase/article/58683.html>.

Vous y trouverez des informations détaillées sur les messages d'erreur Sophos SafeGuard Disk Encryption suivants :

0104, 0113, 1048, 1089, 1104, 1109, 1121, 1123, 1244, 1254, 1264, 1274, 1306, 1315, 1602.

### Erreur du produit

|      |   |
|------|---|
| 0001 | Erreur fatale.  |
| 0002 | Répéter   |
| 0100 | Version différente de [PN] ou Crypton déjà installée. |
| 0101 | Lecture impossible du fichier de configuration.       |
| 0102 | Fichier de configuration invalide.                    |
| 0103 | Écriture impossible du fichier de configuration.      |
| 0104 | Le pilote installé n'est pas compatible.              |
| 0105 | Pilote déjà installé.                                 |
| 0106 | Ce programme ne peut pas être exécuté sous &0.        |
| 0107 | Écriture impossible du fichier de sauvegarde.         |
| 0108 | Lecture impossible du fichier de sauvegarde.          |
| 0109 | Fichier de sauvegarde invalide.                       |

|      |   |
|------|---|
| 0110 | Installation impossible d'une seconde partition d'amorçage sur le disque.     |
| 0111 | Installation impossible sur le Gestionnaire d'amorçage OS/2.                  |
| 0112 | Version antérieure de [PN] ou C :CRYPT déjà installée.                        |
| 0113 | Dernière opération d'installation, désinstallation ou mise à jour incomplète. |
| 0114 | Espace mémoire contigu insuffisant sur la partition d'amorçage.               |
| 0115 | Accès impossible à la partition d'amorçage du pilote.                         |
| 0116 | Fichier de ressources introuvable.  |
| 0117 | Ouverture impossible du fichier de ressources.                                |
| 0118 | Fichier de ressources erroné ou illisible.                                    |
| 0119 | Le module algorithme manque.  |
| 0120 | Le module noyau manque.   |
| 0121 | Le module PBA manque.   |
| 0122 | Création impossible de *AUTOUSER.   |
| 0200 | Analyse impossible de la structure du disque dur.                             |
| 0201 | Erreur de lecture du disque dur.  |
| 0202 | Erreur d'écriture sur le disque dur.  |
| 0203 | Table de partition invalide sur le disque 0.                                  |
| 0204 | Incompatibilité ROM BIOS.   |
| 0205 | Secteur d'amorçage invalide.  |
| 0206 | Verrouillage impossible du volume.  |
| 0300 | Disque protégé en écriture.   |
| 0301 | Unité inconnue.   |
| 0302 | Le lecteur &0 n'est pas prêt.   |

|      |   |
|------|---|
| 0303 | Commande inconnue.                              |
| 0304 | Erreur contrôle CRC.                            |
| 0305 | Longueur de structure de requête erronée.       |
| 0306 | Erreur de recherche.                            |
| 0307 | Type de périphérique inconnu.                   |
| 0308 | Secteur introuvable.                            |
| 0309 | Plus de papier dans l'imprimante.               |
| 0310 | Erreur d'écriture.                              |
| 0311 | Erreur de lecture.                              |
| 0312 | Erreur générale.                                |
| 0320 | Mémoire insuffisante.                           |
| 0321 | Erreur de division à l'adresse du programme &0. |
| 0322 | Dépassement de pile à l'exécution.              |
| 0500 | Pilote de chiffrement non installé.             |
| 0501 | Version incorrecte du pilote de chiffrement.    |
| 0502 | Argument(s) de ligne de commande invalide(s).   |
| 0503 | Aucune clé définie pour le déchiffrement.       |
| 0999 | Erreur inconnue.                                |

#### **Erreurs du System API**

|      |   |
|------|---|
| 1001 | Aucun sous-système n'est actif.                 |
| 1002 | Changement invalide d'un paramètre système.     |
| 1003 | Algorithme de chiffrement invalide ou manquant. |

|      |  |
|------|--|
| 1004 | Erreur interne décelée dans le sous-système.   |
| 1005 | Le sous-système a signalé une erreur E/S.  |
| 1006 | La tentative d'accès au noyau a échoué.  |
| 1007 | Un utilisateur a déjà ouvert une session dans<br>[[FILELINK]=SGE_INFO.DLL][[MSGLINK]=102]. |
| 1008 | Un utilisateur incorrect a été défini.   |
| 1009 | L'assignation de droits définis à l'utilisateur n'est pas autorisée.                       |
| 1010 | L'utilisateur défini existe déjà.  |
| 1011 | Le mot de passe attribué a déjà été utilisé par cet utilisateur.                           |
| 1012 | Le mot de passe attribué fait partie de la liste des mots de passe interdits.              |

#### Erreurs de fichier

|      |   |
|------|---|
| 1031 | Ouverture impossible du fichier %1.                       |
| 1032 | Fermeture impossible du fichier %1.                       |
| 1033 | Création impossible du fichier %1.                        |
| 1034 | Erreur d'écriture dans le fichier %1.                     |
| 1035 | Erreur de lecture du fichier %1.                          |
| 1036 | La tentative d'accès au fichier %1 a échoué.              |
| 1037 | Fichier %1 introuvable.                                   |
| 1038 | Chemin ou nom de fichier invalide.                        |
| 1039 | Espace mémoire insuffisant sur le disque.                 |
| 1040 | La partition du disque dur est trop fortement fragmentée. |
| 1041 | Détection d'un système de fichiers invalide.              |

|      |  |
|------|--|
| 1042 | Détection d'un système de fichiers inconnu.                  |
| 1043 | Le fichier %1 existe déjà.                                   |
| 1044 | Détection d'une structure erronée du système de fichiers.    |
| 1045 | Détection d'une entrée invalide dans le système de fichiers. |
| 1046 | La demande d'informations de partition a échoué.             |
| 1047 | Détection d'un système de fichiers inconnu ou invalide.      |
| 1048 | Impossible de copier le fichier %1.                          |
| 1049 | Impossible de supprimer le fichier %1.                       |
| 1052 | Le contrôle CRC pour le fichier %1 a échoué.                 |
| 1053 | Impossible de renommer le fichier %1.                        |

#### **Erreurs d'installation**

|      |   |
|------|---|
| 1061 | Lecteur d'installation invalide.  |
| 1063 | Sophos SafeGuard Disk Encryption est déjà installé.   |
| 1065 | Le fichier Config.sys est protégé en écriture.  |
| 1066 | Entrée introuvable dans le fichier INI ou dans le fichier de configuration.   |
| 1067 | Un système [PN] complet ou exécutable ne peut pas être installé avec des disques dynamiques.\n\nSeuls les utilitaires d'administration peuvent être sélectionnés pour l'installation. |
| 1068 | Impossible de créer le fichier de noyau.  |
| 1069 | Impossible de modifier le fichier Config.sys.   |
| 1070 | Impossible de copier le fichier %1.   |
| 1071 | Aucun répertoire de destination n'a été défini.   |

- 1072 Un mot de passe d'administrateur système incorrect a été spécifié.\n\nVoulez-vous essayer à nouveau ?
- 1073 Aucun mot de passe d'administrateur système n'a été défini.
- 1076 L'opération de désinstallation a échoué.\n\nVous trouverez des informations additionnelles dans le fichier Sgeasy.log.
- 1077 La désinstallation du système GINA a échoué.
- 1078 De nouveaux pilotes et services ont été installés. Nous vous recommandons fermement de créer maintenant une nouvelle sauvegarde parce que vous ne pouvez pas utiliser les anciennes sauvegardes pour la restauration lorsque Sophos SafeGuard Disk Encryption est installé !
- 1079 La désinstallation du client GINA SGEgina a échoué.
- 1080 La suppression d'une entrée de menu système a échoué.
- 1081 La suppression d'une entrée de menu système a échoué.
- 1082 Entrée introuvable dans le fichier INI.
- 1083 L'installation de Cardman API a échoué.
- 1084 Pour le mode à double amorçage (Twin-Boot), le lecteur contenant le noyau doit être chiffré.
- 1086 Un système [PN] complet est déjà installé\nsur votre ordinateur, dans un autre système d'exploitation. Vous devez désinstaller ce système\navant de pouvoir désinstaller la composante exécutable du système d'exploitation actuel.
- 1087 L'installation d'un système [PN] n'est pas autorisée.
- 1088 Un fichier de ressources PBA requis (.MOD) n'a pas pu être trouvé !
- 1089 L'[i] de [PN] n'a pas été effectuée avec succès.\n\nL'échec de l'[i] est dû à l'erreur suivante :\n\n%1\n\nVeuillez cliquer sur le bouton OK pour supprimer tous les composants installés de [PN].\n\nEnsuite, un redémarrage automatique du système
- 1090 Détection d'une version incorrecte du système d'exploitation.\n\nLe système d'exploitation Windows NT v4.00 est requis.

- 1091 Détection d'une version incorrecte du système d'exploitation. \n\nLe système d'exploitation Windows 95/98/ME est requis.
- 1092 La procédure de désinstallation ne peut pas être démarrée car un ou plusieurs composants[[FILELINK]=SGE\_INFO.DLL][[MSGLINK]=102] sont actuellement inactifs.
- 1093 Ce processus ne peut pas être exécuté car une opération de chiffrement est actuellement en cours. Veuillez attendre que toutes les opérations de chiffrement soient terminées et redémarrer ce programme.
- 1094 Le processus de désinstallation est en cours. L'administration n'est plus possible.
- 1095 Nombre maximum de disques durs dépassé. \nInstallation de [PN] non prise en charge sur ce système.
- 1096 Quelques partitions non-DOS susceptibles d'être chiffrées avec le type d'installation sélectionné ont été trouvées.\nIl est donc recommandé de choisir le type d'installation 'Par partition'.
- 1097 Détection d'une version incorrecte du système d'exploitation. \n\nLe système d'exploitation Windows 2000 est requis.
- 1098 L'installation de Sophos SafeGuard Disk Encryption a échoué.
- 1099 La désinstallation de Sophos SafeGuard Disk Encryption a échoué.

### Erreurs générales

- 1101 Échec du test automatique.
- 1102 Initialisation impossible du système d'aide.
- 1103 Une classe n'a pas pu être enregistrée.
- 1104 Les informations sur la configuration de partition sont incohérentes.
- 1105 Paramètre invalide ou incorrect.
- 1106 Pas ou trop peu de paramètres ont été définis.

|      |   |
|------|---|
| 1107 | Définition d'un paramètre inconnu.  |
| 1108 | Capacité mémoire insuffisante.  |
| 1109 | Impossible de charger le module '%1'.   |
| 1110 | Impossible de créer une boîte de dialogue.  |
| 1111 | Impossible d'initialiser une boîte de dialogue.   |
| 1112 | Impossible de créer un thread.  |
| 1113 | Impossible de créer une fenêtre.  |
| 1114 | Vous devez posséder des droits d'administrateur pour l'installation ou la désinstallation.  |
| 1115 | Une violation d'accès à la mémoire s'est produite !   |
| 1117 | Impossible d'ouvrir le fichier journal '%1'.  |
| 1118 | Vous ne pouvez pas exécuter simultanément les programmes Désinstallation et Administration de [PN].\n\nVeuillez quitter le programme en cours avant d'en démarrer un autre. |
| 1119 | Fichier noyau introuvable.  |
| 1120 | L'installation du gestionnaire de contrôle a échoué.  |
| 1121 | Définition d'une variable d'environnement inconnue.   |
| 1122 | Impossible de définir une variable d'environnement.   |
| 1123 | Taille de mémoire tampon insuffisante.  |
| 1124 | Impossible de charger la bibliothèque de liaisons dynamiques '%5'.  |
| 1125 | La fonction '%5' spécifiée est introuvable.   |
| 1126 | Impossible d'ouvrir le sémaphore '%5'.  |
| 1127 | Impossible de libérer le module '%5'.   |

- 1128 Une exception s'est produite pendant l'exécution d'une fonction sous-système de [PN].\nCode dernière erreur :%1\nCode de retour fonction :%2\nModule :%3\nNuméro de ligne :%4\nAdresse :%5\nVeuillez contacter Utimaco Safeware AG - a member of the Sophos group !
- 1129 Une erreur critique s'est produite pendant l'exécution\nd'une ou de plusieurs fonctions sous-système de [PN].\n\nCode d'erreur fatale : %1\nCode d'erreur OS : %2\nModule : %3\nFonction : %4\nDescription : [[MSGLINK]=%1
- 1130 Impossible de libérer une mémoire allouée.
- 1131 Une fonction n'est actuellement pas prise en charge.
- 1132 Accès refusé.
- 1133 Le démarrage du programme '%1' a échoué.
- 1134 Fonction ou ressource non disponible.
- 1135 Processus interrompu par l'utilisateur.
- 1136 Entrée invalide ou incorrecte.
- 1137 Le système est actuellement en train de procéder à des changements de paramètres systèmes. Les nouveaux changements ne sont pas permis actuellement.
- 1139 Type de données non valide pour le champ de boîte de dialogue
- 1141 La sauvegarde du noyau a échoué.
- 1143 La station de travail définie n'existe pas
- 1144 Client d'ouverture de session « SgeGina.dll » introuvable. Ce composant est vital pour le fonctionnement de[PN]. Sa suppression ou sa désactivation peuvent causer de sérieux problèmes requérant une nouvelle installation de [PN] ou du système d'exploitation.
- 1145 Service « SgeCtl.exe » introuvable. Ce composant est vital pour le fonctionnement de base de[PN]. Sa suppression ou sa désactivation peuvent causer de sérieux problèmes requérant une nouvelle installation de [PN] ou du système d'exploitation.
- 1146 Le noyau système est altéré !

- 1147 Une opération de chiffrement ou de déchiffrement du disque dur est en cours d'exécution ou une opération de ce type a été initialisée.\nVous ne pourrez effectuer une sauvegarde du noyau que lorsque toutes ces opérations auront été achevées.
- 1148 Impossible de trouver l'interface sur le système.\n\nIdentifiant de classe :%1 (%3)\nInterface :%2\nRésultat :%4 ([[OSERLINK]=%5])\n\nIl est possible que [[FILELINK]=SGE\_INFO.DLL][[MSGLINK]=102] ne soit pas installé sur '%6' !

#### **Erreurs de fichier de configuration.**

- 1151 Fichier de configuration %1 introuvable.
- 1152 Aucun fichier de configuration défini.
- 1153 Fichier de configuration invalide.
- 1154 Entrée invalide détectée dans le fichier de configuration.
- 1155 Impossible de créer le fichier de configuration %1.
- 1156 Erreur décelée à la ligne %1 du fichier de configuration.
- 1158 Le fichier de configuration spécifié est introuvable !
- 1159 Une commande inconnue a été trouvée dans le fichier de configuration.
- 1160 Un type de fichier de configuration inconnu a été détecté.
- 1161 Le type de fichier de configuration est invalide.
- 1162 Impossible de créer l'identificateur pour le fichier de configuration.
- 1163 Impossible de créer le fichier de configuration pour la désinstallation.
- 1164 Impossible de créer le fichier de configuration pour l'installation.
- 1165 Fichier de configuration %1 introuvable.
- 1166 Le type de fichier de configuration est invalide.

1167 L'exécution du fichier de configuration '%1' a échoué.

#### Erreurs de contrôle MESSAGE.

1171 ID message %1 introuvable.

1172 Texte de contrôle pour introuvable pour l'ID de contrôle.

1173 Impossible d'écrire le journal des événements de Windows NT.

1174 Un lien fichier ou message invalide a été détecté :\n\nIdentificateur de message : %1\nCommande de lien : %2.

1175 Le format du fichier de message '%1' est invalide.

1176 Erreur de mot de passe.

#### Erreurs liées au mot de passe

1181 Aucun mot de passe d'administrateur système n'est défini.

1182 Mot de passe inconnu. Veuillez retaper votre mot de passe.

1183 Aucun mot de passe n'est défini.

1184 Le mot de passe défini est trop court.

1185 Le mot de passe défini est trop long.

1186 Les mots de passe définis ne correspondent pas.

1187 Le mot de passe est faible.\nVoulez-vous entrer un autre mot de passe ?

1188 Un autre utilisateur possède déjà ce mot de passe. \nVoulez-vous l'utiliser quand même ?

1189 Le mot de passe ne contient pas le nombre requis de caractères, des caractères de casse différente, des caractères avec des chiffres et des symboles.

1190 Le mot de passe n'a pas encore atteint sa durée minimale définie.

#### Erreurs de clé

1201 Une clé de disque dur n'est pas encore définie.\n\nL'activation du déchiffrement pour des partitions de disque dur n'est pas autorisée\ntant qu'aucune clé n'est définie pour ces disques durs.

1205 La clé définie est trop courte.

1206 Les clés définies ne correspondent pas.

1207 Aucune clé n'a été définie.

1209 Le mode Disques complets requiert une\ncle de chiffrement pour le disque dur.

#### Erreurs IPC

1221 Impossible de démarrer le serveur IPC.

1222 Impossible de démarrer le client IPC.

1223 Impossible d'établir la communication IPC.

1224 Impossible d'appeler le message IPC.

1225 Impossible d'attribuer le message IPC.

1226 La fonction IPC IPC\_SGE\_PROCESS\_DEF\_MSG\nn'a pas pu être traitée.

1227 Impossible de fermer le serveur IPC.

1228 Impossible de fermer le client IPC.

- 1229 Impossible de démarrer le thread IPC.
- 1230 L'attente d'un message IPC a échoué.
- 1231 Objet de communication IPC introuvable.

**Erreurs de lecteur.**

- 1241 Lecteur inconnu ou invalide.
- 1242 Autres lecteurs introuvables.
- 1243 L'opération E/S lecteur a échoué.
- 1244 La tentative de lecture d'un lecteur a échoué.
- 1245 La tentative d'écriture sur un lecteur a échoué.
- 1246 La tentative d'accès à un lecteur a échoué.
- 1247 Lecteur non prêt.
- 1248 La tentative de verrouillage d'un lecteur a échoué.
- 1249 La tentative de déverrouillage d'un lecteur a échoué.
- 1250 La partition système doit être une partition primaire.\n\nCeci est par exemple nécessaire si l'option « Accès à la partition de configuration Compaq » est active.
- 1251 Le démontage d'un volume a échoué.\n\nDes fichiers ou fenêtres du volume sont peut-être encore ouverts.
- 1252 Le premier disque physique n'est pas un disque dur.
- 1253 Toutes les entrées de la table de partition du secteur MBR sur le premier disque dur sont déjà utilisées.\n\nL'option « Accès à la partition de configuration Compaq » requiert une entrée de table de partition libre !
- 1254 Le système a démarré en mode compatible.

- 1255 Pour installer Sophos SafeGuard Disk Encryption, veuillez retirer le disque dur connectable.
- 1256 Aucun lecteur de ce type n'est disponible.
- 1257 Erreur interne lors de l'accès à la partition système

#### Erreurs SERVICE

- 1261 Des informations sur un objet de mémoire pour un service système\nn'ont pas pu être débloquées.
- 1262 Erreur décelée dans le répartiteur du service système.
- 1263 Impossible de démarrer le service système.
- 1264 Impossible de modifier l'état du service système.
- 1265 Impossible d'enregistrer la routine pour le service système.
- 1266 La fonction d'initialisation du service a signalé une erreur.
- 1267 Bloc d'information de service introuvable.\nLa mémoire est vraisemblablement insuffisante.\n\nCode d'erreur : %1.

#### Erreurs BASE DE REGISTRES

- 1271 Impossible d'ouvrir l'entrée dans la base de registres.
- 1272 Impossible de lire l'entrée dans la base de registres.
- 1273 Impossible d'écrire l'entrée dans la base de registres.
- 1274 Impossible de créer l'entrée dans la base de registres.
- 1275 Impossible de supprimer l'entrée de la base de registres.
- 1276 L'entrée pour le service système dans la base de registres\nn'a pas pu être ouverte.

- 1277 L'entrée pour le service système dans la base de registres\nn'a pas pu être créée.
- 1278 L'entrée pour le service système dans la base de registres\nn'a pas pu être supprimée.
- 1279 L'entrée pour le service système dans la base de registres\nn'existe déjà.
- 1280 Impossible d'ouvrir le 'Session Control Manager'.
- 1281 L'entrée pour une session dans la base de registres\nn'a pas pu être trouvée.
- 1282 Entrée invalide détectée dans la base de registres.

#### **Erreur de base de données de pilotes.**

- 1291 Autres pilotes de chiffrement introuvables.
- 1292 Base de données de pilotes introuvable.
- 1293 Erreur survenue à la lecture de la base de données de pilotes.
- 1294 La base de données de pilotes est vide.
- 1295 Entrée illégale ou invalide dans la base de données de pilotes.

#### **Erreurs CRAREA**

- 1301 Accès impossible au lecteur d'installation.
- 1302 La demande d'informations de partition a échoué.
- 1303 La tentative d'accès à la partition d'amorçage a échoué.
- 1304 Option de processus invalide.
- 1305 Définition d'un système de fichiers inconnu ou invalide.

|      |  |
|------|--|
| 1306 | Différence notée entre le type de système de fichiers actuel et le type de système de fichiers défini. |
| 1307 | Différence notée entre la taille de cluster actuelle et la taille de cluster définie.                  |
| 1308 | Cluster de démarrage invalide pour la zone de noyau.   |
| 1309 | Secteur de démarrage invalide pour la zone de noyau.   |
| 1310 | Type de partition invalide.  |
| 1311 | Clusters libres introuvables pour le noyau.  |
| 1312 | Impossible de marquer les clusters comme « utilisés ».   |
| 1313 | Impossible de marquer les clusters comme « corrects ».   |
| 1314 | Impossible de marquer les clusters comme « non utilisés ».   |
| 1315 | Impossible de marquer les clusters comme « incorrects ».   |
| 1316 | Les informations sur les clusters sont altérées.   |
| 1317 | Zones marquées comme « incorrectes » introuvables.   |
| 1318 | Taille de zone de noyau invalide.  |
| 1319 | Impossible de remplacer le secteur MBR sur le 1er disque dur.  |

#### **Erreurs SGOCA**

|      |  |
|------|--|
| 1401 | Les informations requises pour la zone de communication d'objet existent déjà. |
| 1402 | La zone de communication d'objet existe déjà.                                  |
| 1403 | Les informations requises pour la zone de communication d'objet existent déjà. |
| 1404 | Zone de communication d'objet introuvable.                                     |

1405 Les informations requises pour la zone de communication d'objet n'existent pas.

1406 Informations d'objet supplémentaires trouvées.

#### Erreurs SGUICL

1511 La configuration des composants n'a pas pu être chargée !

#### Erreurs ADMLOGON

1601 La tentative d'ouverture de session a échoué. Essayez à nouveau.

1602 Le sous-système [PN] n'autorise pas plus de 5 tentatives d'ouverture de session. Vous devez redémarrer votre ordinateur pour relancer cette application.

1603 La tentative de démarrage de la composante d'ouverture de session de [PN] a échoué.

1604

1605 L'ouverture de la session [PN] s'est effectuée avec succès, mais vous n'avez pas les droits suffisants pour désinstaller le produit.

#### Erreurs Administration - USER

1801 L'utilisateur '%1' ne peut pas être créé car le nombre d'utilisateurs maximum est atteint.

1802 Il n'est pas possible de créer ou de supprimer le '\*AUTOUSER'.

1803 L'utilisateur '%1' existe déjà. Veuillez spécifier un autre nom d'utilisateur.

- 1804 Le nombre d'utilisateurs maximum a été dépassé.
- 1805 Il n'est pas possible de créer ou de supprimer le profil d'utilisateur\n'SYSTEM'. Il est seulement permis de le modifier.
- 1807 L'application a été bloquée pendant plus de 30 secondes, car elle attend un appel pour se terminer. Dans la plupart des cas, ceci se produit lorsque l'ordinateur est occupé. Voulez-vous attendre jusqu'à ce que l'application soit prête, ou terminer l'appel ?

#### Erreurs SGEGINA

- 2100 La tentative d'ouverture automatique de session a échoué.\n\nVoulez-vous modifier la relation actuelle entre l'utilisateur de [PN]\net l'utilisateur du système d'exploitation ?
- 2101 Vous devez modifier votre mot de passe. \nLa connexion automatique (SAL) sera désactivée au cours de cette session de connexion !

#### Erreurs de désinstallation

- 2201 La procédure de désinstallation ne peut pas être démarrée car une\nopération de chiffrement ou de déchiffrement est actuellement en cours !
- 2202 Le désenregistrement d'un composant a échoué !
- 2203 La procédure de désinstallation ne peut pas continuer, car au moins une partition étrangère de disque dur a été détectée. La désinstallation de [[MSGFILE]=SGE\_INFO.dll][[MSGLINK=102] ne peut pas se poursuivre.

### Erreurs d'installation étendue

- |      |  |
|------|--|
| 2301 | Le programme d'installation possède le mauvais numéro de version et n'a pas pu être utilisé !  |
| 2302 | Pour l'installation en mode « Disques complets » ou « Protection des zones d'amorçage », le nombre maximum de partitions par disque dur est de 8 !   |
| 2303 | L'enregistrement du composant a échoué !   |
| 2304 | L'installation de [PN] requiert Microsoft's Windows Installer<br>!\nVeuillez lire le fichier LISEZMOI pour la manière d'installer Windows Installer. |
| 2305 | Détection d'une version incorrecte du système d'exploitation.\n\nLe système d'exploitation Windows NT/2000 est requis.                               |

### Erreurs de l'Assistant de création de disquette de démarrage

- |      |   |
|------|---|
| 2401 | La création du fichier de sauvegarde de noyau a été annulée !     |
| 2402 | Tous les outils de secours n'ont pas pu être copiés avec succès ! |

### Erreurs SAL

- |      |   |
|------|---|
| 2501 | Impossible d'ouvrir le fichier SAL.                                   |
| 2502 | Le fichier SAL est dans un état indéfini.                             |
| 2503 | Une erreur indéfinie s'est produite lors d'opérations sur le fichier. |
| 2504 | Impossible de positionner correctement le fichier SAL.                |
| 2505 | Erreur à la lecture du fichier SAL.                                   |
| 2506 | Erreur à l'écriture du fichier SAL                                    |

|      |   |
|------|---|
| 2507 | L'utilisateur spécifié est introuvable.   |
| 2508 | Aucune utilisateur actuellement connecté n'a été trouvé.                                      |
| 2509 | L'écriture dans le fichier SAL a échoué. L'enregistrement existant doit avoir la même taille. |
| 2510 | Le tampon de destination est trop petit pour toute l'entrée.                                  |
| 2511 | Pas de mémoire disponible.  |

#### Erreurs Interface

|      |  |
|------|--|
| 3001 | Impossible de chiffrer l'interface COM spécifiée.\nNom de l'interface :%1\nNuméro d'erreur : %2\nDétails :%3   |
| 3002 | L'exécution d'une méthode d'interface a échoué. Les détails suivants sont disponibles :\nNuméro d'erreur : %1\nRésultat : %2\nDescription : %3\nInterface :%4\nVeuillez contacter votre administrateur système ! |

## 28 Support technique

Pour obtenir du support technique, consultez <http://www.sophos.fr/support>.

Si vous contactez le support technique, fournissez autant d'informations que possible, notamment :

- Le ou les numéro(s) de version(s) des logiciels Sophos
- Le ou les système(s) d'exploitation et niveau(x) de correctif(s)
- Le texte exact de tous les messages d'erreur

## **29 Copyright**

Copyright © 1992 - 2009 Utimaco Safeware AG - a member of the Sophos group

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.

Droits de brevet d'Ascom Tech Ltd. pour l'Union Européenne, le Japon et les États-Unis. IDEA est une marque commerciale d'Ascom Tech Ltd.

Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.