

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy Aide administrateur

Version du produit : 5.60

Date du document : avril 2011



Table des matières

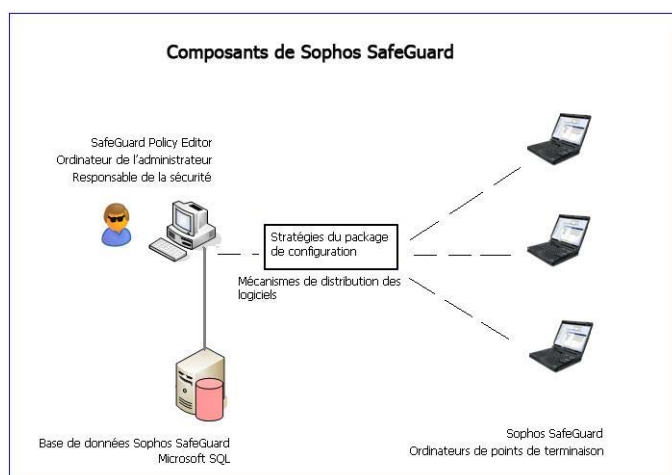
1	À propos de Sophos SafeGuard.....	4
2	Licences.....	6
3	SafeGuard Policy Editor.....	7
4	Sophos SafeGuard sur les ordinateurs d'extrémité.....	9
5	Chiffrement de données.....	10
6	Démarrage.....	14
7	Installation.....	19
8	Installation de Sophos SafeGuard sur les ordinateurs disposant de plusieurs systèmes d'exploitation.....	40
9	Connexion au SafeGuard Policy Editor.....	42
10	Importation de licences.....	43
11	Utilisation de stratégies.....	44
12	Utilisation de packages de configuration.....	49
13	Exportation du certificat d'entreprise et de celui du responsable de la sécurité.....	51
14	Restauration d'une base de données Sophos SafeGuard.....	52
15	Restauration d'une installation corrompue du SafeGuard Policy Editor.....	54
16	Vérification de l'intégrité de la base de données.....	55
17	Accès administratif aux ordinateurs d'extrémité.....	56
18	Stratégies par défaut.....	66
19	Paramètres de stratégie.....	74
20	Authentification au démarrage (POA).....	109
21	Éveil par appel réseau sécurisé (WOL).....	118
22	Clés cryptographiques et cartes à puce.....	120
23	SafeGuard Data Exchange.....	125
24	Options de récupération.....	128
25	Récupération avec Local Self Help.....	129
26	Récupération avec Challenge/Réponse.....	135
27	Récupération du système.....	148

28	Sophos SafeGuard et disques durs compatibles Opal à chiffrement automatique.....	151
29	Blocage de la désinstallation sur les ordinateurs d'extrémité.....	154
30	Mise à jour de Sophos SafeGuard.....	155
31	Mise à niveau de Sophos SafeGuard vers SafeGuard Enterprise.....	159
32	Mise à niveau de SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x vers Sophos SafeGuard 5.6x.....	161
33	À propos de la désinstallation.....	169
34	Support technique.....	170
35	Mentions légales.....	171

1 À propos de Sophos SafeGuard

Pour protéger les informations sur les ordinateurs d'extrémité, Sophos SafeGuard utilise une stratégie de chiffrement basée sur les stratégies.

L'administration s'effectue via le SafeGuard Policy Editor utilisé pour créer et gérer les stratégies de sécurité et pour proposer des fonctions de récupération. Les stratégies sont déployées sur les ordinateurs d'extrémité via des packages de configuration. Côté utilisateur, les fonctions de sécurité principales sont le chiffrement des données et la protection contre l'accès non autorisé. Sophos SafeGuard peut être intégré de façon transparente à l'environnement normal de l'utilisateur, et son utilisation est facile et intuitive. Le système d'authentification de Sophos SafeGuard, l'authentification au démarrage (POA, Power-On Authentication), fournit une protection efficace des accès et offre une prise en charge conviviale lors de la récupération des informations d'identification.



Ensembles de produits

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

Composants Sophos SafeGuard

Sophos SafeGuard est constitué des composants suivants :

Composant	Description
SafeGuard Policy Editor	L'outil de gestion Sophos SafeGuard permet de créer des stratégies de chiffrement et d'authentification. Le SafeGuard Policy Editor crée une stratégie par défaut lors de la toute première configuration.

Composant	Description
	Le SafeGuard Policy Editor contient par ailleurs des fonctions de récupération pour permettre à l'utilisateur de retrouver l'accès à son ordinateur, lorsqu'il a oublié son mot de passe, par exemple.
Base de données Sophos SafeGuard	La base de données Sophos SafeGuard contient tous les paramètres de stratégie des ordinateurs d'extrémité.
Logiciel Sophos SafeGuard sur les ordinateurs d'extrémité	Logiciel de chiffrement sur les ordinateurs d'extrémité

2 Licences

Pour utiliser les composants Sophos SafeGuard, des licences valides sont nécessaires. Concernant l'utilisation des clés cryptographiques, les licences de clés appropriées sont nécessaires. Après l'achat du logiciel, le client reçoit un fichier de licence contenant les licences obtenues auprès de son partenaire commercial.

Le fichier de licence est un fichier .XML comportant une signature et contenant les informations suivantes :

- Nom de la société
- Date de génération
- Nombre de licences achetées par composant ou par fonction (par exemple, SafeGuard Policy Editor, Sophos SafeGuard Client, Device Encryption)
- Informations sur la licence de la clé cryptographique
- Versions de Sophos SafeGuard pour lesquelles la licence est valide
- Date d'expiration de la licence
- Type de licence (standard pour les licences complètes)

Le fichier de licence doit être importé dans la base de données Sophos SafeGuard après l'installation. Pour plus d'informations, voir [Importation de licences](#) à la page 43.

Une licence est valide si les conditions suivantes sont remplies :

- Le type de licence est standard.
- La licence n'a pas expiré. La licence n'est plus valide un mois après la date d'expiration.
- Le numéro de version accordé le plus élevé de Sophos SafeGuard est égal à ou supérieur au numéro de version du SafeGuard Policy Editor.

- **Pour les clients Sophos SafeGuard Disk Encryption (SDE) :**

Le fichier de licence contient au moins une licence SafeGuard Policy Editor et une licence Device Encryption.

- **Pour les clients SafeGuard Easy (SGE) :**

Le fichier de licence contient au moins une licence SafeGuard Policy Editor et une licence Device Encryption ou Data Exchange.

Remarque : si vous n'avez pas importé de licence valide si votre licence a expiré, vous ne pouvez pas créer de packages de configuration pour le déploiement sur l'ordinateur d'extrémité. Lorsque l'utilisateur se connecte à l'ordinateur d'extrémité, un message apparaît indiquant qu'une version de démonstration est utilisée.

2.1 Licences de clé cryptographique

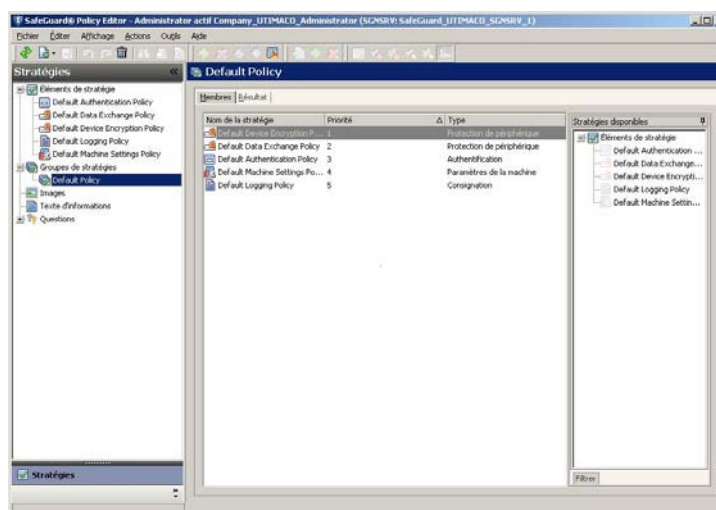
Concernant l'utilisation des clés cryptographiques ou des cartes à puce, les licences de clés appropriées sont nécessaires. Si les licences appropriées ne sont pas disponibles, vous ne pouvez pas créer de stratégies de clés cryptographiques dans le SafeGuard Policy Editor.

3 SafeGuard Policy Editor

Le SafeGuard Policy Editor est l'outil de gestion des ordinateurs protégés par Sophos SafeGuard.

Le SafeGuard Policy Editor est installé sur l'ordinateur que vous utilisez pour réaliser des tâches administratives. En tant que responsable de la sécurité, vous utilisez le SafeGuard Policy Editor pour gérer les stratégies Sophos SafeGuard et pour créer des paramètres de configuration destinés aux ordinateurs d'extrémité. Publiez les stratégies et les paramètres dans un package de configuration pour les déployer sur les ordinateurs d'extrémité. Vous pouvez créer plusieurs packages de configuration et les distribuer à l'aide de mécanismes tiers. Distribuez les packages lorsque vous installez le logiciel de chiffrement Sophos SafeGuard. Vous pourrez déployer ultérieurement des packages supplémentaires pour changer les paramètres sur les ordinateurs d'extrémité.

Le SafeGuard Policy Editor propose également des fonctions de récupération pour accéder de nouveau à l'ordinateur d'extrémité, lorsqu'un utilisateur oublie son mot de passe, par exemple.



Fonctions

Le SafeGuard Policy Editor contient les éléments suivants :

- **Configuration par défaut** : lors de la première configuration, le SafeGuard Policy Editor crée automatiquement une stratégie par défaut avec les stratégies préconfigurées conseillées pour les ordinateurs d'extrémité. Si la stratégie par défaut ne correspond pas à vos attentes, vous pouvez la personnaliser selon vos besoins.
- **Options d'accès administratif** : les options d'accès administratif, comptes de service et comptes d'accès POA permettent un accès spécial aux tâches d'après-installation et administratives sur les ordinateurs d'extrémité.
- **Clés de chiffrement** : une clé machine générée automatiquement est utilisée pour SafeGuard Device Encryption (chiffrement basé sur volume). Les clés générées localement sur l'ordinateur d'extrémité sont utilisées pour SafeGuard Data Exchange (chiffrement basé sur fichier). SafeGuard Data Exchange n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

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

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

Une procédure Challenge/Réponse avec l'assistance du support technique peut être demandée par un utilisateur qui a oublié son mot de passe ou qui l'a trop souvent saisi de façon incorrecte. Elle peut également être utilisée pour récupérer des données en cas de corruption de l'authentification au démarrage. La procédure Challenge/Réponse est basée sur des fichiers de récupération de clé générés automatiquement lors de l'installation de Sophos SafeGuard sur l'ordinateur d'extrémité.

Base de données

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

Mise à niveau

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

Journalisation

Les événements des ordinateurs protégés par Sophos SafeGuard sont journalisés dans l'Observateur d'événements Windows.

En quoi le SafeGuard Policy Editor est-il différent du SafeGuard Management Center ?

Le SafeGuard Management Center dispose d'un serveur de gestion centralisée et propose des fonctionnalités de gestion étendues, notamment :

- Importation d'Active Directory avec gestion utilisateur et domaine.
- Journalisation centrale.
- Possibilité de définir des rôles administratifs.

Le SafeGuard Management Center est disponible avec SafeGuard Enterprise.

Remarque :

Dans le SafeGuard Management Center, vous pouvez aussi définir des paramètres et créer des packages de configuration pour les ordinateurs Sophos SafeGuard qui n'ont pas de connexion à un serveur SafeGuard Enterprise.

4 Sophos SafeGuard sur les ordinateurs d'extrémité

Le chiffrement des données et leur protection contre tout accès non autorisé constituent les principales fonctions de sécurité de Sophos SafeGuard. Sophos SafeGuard peut être intégré de façon transparente à l'environnement normal de l'utilisateur, et son utilisation est facile et intuitive. Le système d'authentification de Sophos SafeGuard, l'authentification au démarrage (POA, Power-On Authentication), assure une protection nécessaire des accès et une prise en charge conviviale lors de la récupération des informations d'identification.

Composants pris en charge

Les modules suivants sont fournis pour les ordinateurs d'extrémité :

■ SafeGuard Device Encryption

Chiffrement basé sur volume : assure que toutes les données présentes sur les volumes spécifiés (volume d'initialisation, disque dur, partitions) sont chiffrées de manière transparente (fichiers d'initialisation, fichiers d'échange, fichiers inactifs/d'hibernation, fichiers temporaires et informations sur les répertoires, etc.) sans que l'utilisateur n'ait besoin de modifier ses habitudes de travail ou de tenir compte de problèmes de sécurité.

Authentification au démarrage : la connexion de l'utilisateur se fait immédiatement après la mise sous tension de l'ordinateur. Une fois l'authentification au démarrage réussie, l'utilisateur est automatiquement connecté au système d'exploitation.

■ SafeGuard Data Exchange

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

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

Remarque :

Ce composant n'est pas pris en charge par ESDP (Endpoint Security and Data Protection).

5 Chiffrement de données

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

Remarque :

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

Les fichiers sont chiffrés de manière transparente. Lorsque les utilisateurs ouvrent, modifient et enregistrent des fichiers, ils ne sont pas invités à chiffrer ou à déchiffrer.

Vous pouvez spécifier des paramètres de chiffrement dans une stratégie de sécurité du type **Protection du périphérique**. Pour plus d'informations, reportez-vous aux sections [Utilisation de stratégies](#) à la page 44 et [Protection des périphériques](#) à la page 96.

5.1 Chiffrement basé sur volume

Avec le chiffrement basé sur volume, toutes les données présentes sur un volume (y compris les fichiers d'initialisation, les fichiers de pages, les fichiers d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sont chiffrées. Les utilisateurs n'ont pas à changer les procédures de fonctionnement normales ou à penser à la sécurité.

Remarque :

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

Remarque :

Si après le chiffrement d'un volume, une nouvelle stratégie est appliquée à un ordinateur d'extrémité qui autorise le déchiffrement, les conditions suivantes s'appliquent : une fois terminé le chiffrement basé sur volume, l'ordinateur d'extrémité doit être redémarré au moins une fois avant que le déchiffrement puisse être lancé.

5.1.1 Chiffrement initial rapide

Sophos SafeGuard propose un chiffrement initial en guise de mode spécial pour le chiffrement basé sur volume. Cela réduit le temps nécessaire pour le chiffrement initial (ou le déchiffrement final) des volumes sur les ordinateurs d'extrémité par l'accès seulement à l'espace disque réellement en cours d'utilisation.

Pour un chiffrement initial rapide, les conditions préalables suivantes s'appliquent :

- Le chiffrement initial rapide fonctionne seulement sur les volumes formatés NTFS.
- Les volumes formatés NTFS avec une taille de clusters de 64 Ko ne peuvent pas être chiffrés avec le mode de chiffrement initial rapide.

Remarque :

Ce mode conduit à un état moins sécurisé si un disque a été utilisé avant son utilisation courante avec Sophos SafeGuard. Les secteurs non utilisés peuvent tout de même contenir des données. Le chiffrement initial rapide est par conséquent désactivé par défaut.

Pour activer le chiffrement initial rapide, sélectionnez le paramètre basé sur volume **Chiffrement initial rapide** dans une stratégie du type **Protection du périphérique**, voir [Protection des périphériques](#) à la page 96.

Remarque :

Pour le déchiffrement des volumes, le mode de chiffrement initial rapide sera toujours utilisé, quel que soit le paramètre de stratégie spécifié. Pour le déchiffrement, les conditions préalables énumérées s'appliquent aussi.

5.1.2 Chiffrement basé sur volume et partition du système Windows 7

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

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

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

Remarque :

Si une stratégie de chiffrement, dont le paramètre **Clé à utiliser pour le chiffrement** est défini de sorte à permettre la sélection de clé (par exemple, **Toute clé du jeu de clés utilisateur**), existe pour un volume d'objets du système de fichiers non identifiés, un intervalle de temps s'écoule entre l'affichage de la boîte de dialogue de sélection de la clé et le refus de l'accès. Pendant cet intervalle, le volume reste accessible. Le volume est accessible tant que la boîte de dialogue de sélection de clé n'est pas confirmée. Pour éviter cela, spécifiez une clé présélectionnée pour le chiffrement. Pour plus d'informations sur les paramètres de stratégie correspondants, voir [Protection des périphériques](#) à la page 96. Cet intervalle de temps existe également pour les volumes d'objets du système de fichiers non identifiés qui sont connectés à un ordinateur d'extrémité, notamment lorsque l'utilisateur a déjà ouvert des fichiers sur le volume lorsque la stratégie de chiffrement prend effet. Dans ce cas, il n'est pas garanti que l'accès au volume sera refusé car cela risque de provoquer une perte de données.

5.1.4 Chiffrement des volumes avec la fonctionnalité Autorun activée

Si vous appliquez une stratégie de chiffrement aux volumes pour lesquels Autorun est activé, voici ce qui peut se produire :

- Le volume n'est pas chiffré.

- Si le volume est un objet du système de fichiers non identifié ([voir Chiffrement basé sur volume et objets du système de fichiers non identifiés](#) à la page 11), l'accès n'est pas refusé.

5.2 Chiffrement basé sur fichier

Remarque :

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

Le chiffrement basé sur fichier garantit que toutes les données sont chiffrées, à part le support d'initialisation et les informations de répertoire. Avec le chiffrement basé sur fichier, même les supports optiques tels que les CD/DVD peuvent être chiffrés. Par ailleurs, les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard Enterprise n'est pas installé, si les stratégies le permettent.

Remarque :

Les données chiffrées utilisant le "chiffrement basé sur fichier" ne peuvent pas être compressées. De même, les données compressées ne peuvent pas être chiffrées en utilisant le chiffrement basé sur fichier.

Remarque :

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

Pour appliquer le chiffrement basé sur fichier aux ordinateurs d'extrémité, créez une stratégie du type **Protection du périphérique** et définissez le **Mode de chiffrement du support** sur **Basé sur fichier**. Pour plus d'informations, [voir Protection des périphériques](#) à la page 96.

5.2.1 Comportement par défaut lors de l'enregistrement des fichiers

Etant donné que les applications se comportent différemment lors de l'enregistrement des fichiers, Sophos SafeGuard propose deux façons de gérer des fichiers chiffrés qui ont été modifiés.

Si un fichier est chiffré avec une clé différente de celle par défaut du volume et si vous modifiez le fichier et l'enregistrez, vous pouvez vous attendre à ce que la clé de chiffrement d'origine soit préservée puisque vous modifiez un fichier et n'en créez pas de nouveau. Mais de nombreuses applications enregistrent des fichiers en effectuant une combinaison d'opérations d'enregistrement, de suppression et de changement de nom (par exemple, Microsoft Office). Si elles font ça, le paramètre Sophos SafeGuard par défaut est d'utiliser la clé par défaut pour cette tâche de chiffrement et donc de changer la clé utilisée pour le chiffrement.

Si vous voulez changer ce comportement et préserver la clé utilisée pour le chiffrement dans tous les cas, vous pouvez modifier une clé de registre sur l'ordinateur d'extrémité.

Pour toujours utiliser la même clé lors de l'enregistrement des fichiers modifiés :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UTIMACO\SGLCENC]  
"ActivateEncryptionTunneling"=dword:00000001
```

Pour permettre l'utilisation d'une clé différente (clé par défaut) lors de l'enregistrement des fichiers modifiés. Il s'agit du paramètre par défaut après l'installation :

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\UTIMACO\SGLCENC]  
"ActivateEncryptionTunneling"=dword:00000000
```

Remarque :

Pour devenir actifs, les changements dans ce paramètre exigent un redémarrage de l'ordinateur d'extrémité.

5.2.2 Exclusion d'applications du chiffrement

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

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

Un cas d'utilisation type est par exemple la définition de programmes de sauvegarde comme exemptés afin qu'ils puissent toujours lire et enregistrer les données chiffrées.

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

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

Pour plus d'informations, voir [Protection des périphériques](#) à la page 96.

6 Démarrage

Cette section explique comment préparer avec succès votre installation de Sophos SafeGuard.

6.1 Stratégie de déploiement

Avant de déployer Sophos SafeGuard sur les ordinateurs d'extrémité, nous vous recommandons de définir une stratégie de déploiement.

Les options suivantes doivent être considérées.

Stratégies

Sophos SafeGuard propose les options suivantes :

■ Stratégie par défaut

Sophos SafeGuard propose une stratégie par défaut avec des paramètres prédéfinis de chiffrement et d'authentification pour un déploiement simple et rapide des stratégies. Lors de la première configuration dans le SafeGuard Policy Editor, la stratégie par défaut est automatiquement créée.

Pour plus de détails sur la stratégie par défaut et sur les paramètres définis, [voir Stratégies par défaut](#) à la page 66.

■ Définition de vos propres stratégies

Si la stratégie par défaut ne couvre pas tous vos besoins spécifiques, vous pouvez la modifier ou définir votre propres stratégies dans le SafeGuard Policy Editor.

Pour plus de détails sur la création de stratégies, [voir Utilisation de stratégies](#) à la page 44. Pour plus de détails sur le déploiement des stratégies sur les ordinateurs d'extrémité, [voir Utilisation de packages de configuration](#) à la page 49.

Pour une description détaillée de toutes les stratégies et de tous les paramètres, [voir Paramètres de stratégie](#) à la page 74.

Options d'accès administratif

Sophos SafeGuard utilise deux types de comptes pour permettre aux utilisateurs de se connecter aux ordinateurs d'extrémité et d'exécuter des tâches administratives après l'installation de Sophos SafeGuard.

■ Comptes de service pour la connexion Windows

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

Les listes de comptes de service sont affectées aux ordinateurs d'extrémité dans les stratégies. Elles doivent être affectées dans le premier package de configuration Sophos SafeGuard, créé pour la configuration des ordinateurs d'extrémité. Vous pouvez mettre à jour les listes

de comptes de service en créant un nouveau package de configuration et en le déployant sur les ordinateurs d'extrémité avant l'activation de la POA.

Pour plus d'informations, voir [Listes de comptes de service pour la connexion Windows](#) à la page 56.

■ Comptes d'accès POA pour connexion POA

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

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

Pour plus d'informations, voir [Comptes d'accès POA pour connexion POA](#) à la page 61.

Options de récupération

Pour les situations nécessitant une procédure de récupération (en cas d'oubli du mot de passe, par exemple), Sophos SafeGuard propose deux options de récupération :

■ Récupération de connexion avec Local Self Help

Local Self Help permet aux utilisateurs ayant oublié leur mot de passe de se connecter à leur ordinateur sans l'aide du support. Pour accéder de nouveau à leur ordinateur, il leur suffit de répondre à un certain nombre de questions prédéfinies dans l'authentification au démarrage.

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

Pour plus d'informations, voir [Récupération avec Local Self Help](#) à la page 129.

■ Récupération par Challenge/Réponse

Le mécanisme Challenge/Réponse est un système de récupération de connexion sécurisé et fiable qui vient en aide aux utilisateurs qui ne peuvent pas se connecter à leur ordinateur ou accéder aux données chiffrées. Pour lancer une procédure Challenge/Réponse, vous aurez besoin de l'aide du support.

Dans la stratégie par défaut, la procédure Challenge/Réponse est activée par défaut. Si vous n'utilisez pas la configuration par défaut, vous devez activer la procédure Challenge/Réponse dans une stratégie. Pour la récupération des données à l'aide de la procédure Challenge/Response, vous devez auparavant créer des fichiers spécifiques appelés clients virtuels dans le SafeGuard Policy Editor.

Pour plus d'informations, voir [Récupération avec Challenge/Response](#) à la page 135 et voir [Création d'un client virtuel](#) à la page 141.

6.2 Préparation à l'installation

Avant de déployer Sophos SafeGuard, nous vous recommandons de vous préparer comme suit.

- Assurez-vous de disposer des droits d'administrateur Windows.
- Fermez toutes les applications ouvertes.
- Vérifiez la configuration système requise du matériel et du logiciel, des Service Packs ainsi que l'espace disque requis pour l'installation et pour un fonctionnement efficace : <http://www.sophos.fr/support/knowledgebase/article/112891.html>.
- Lisez attentivement les notes de publication.

6.3 Téléchargement des programmes d'installation

1. À l'aide de l'adresse Web et des codes d'accès de téléchargement fournis par votre administrateur système, allez sur le site Web et téléchargez le programme d'installation et la documentation de Sophos SafeGuard Disk Encryption/SafeGuard Easy.
2. Placez-les à un emplacement auquel vous pouvez accéder pour effectuer l'installation.

6.4 Paramètres de langue

Les paramètres de langue pour les assistants de configuration, le SafeGuard Policy Editor et Sophos SafeGuard sur les ordinateurs d'extrémité sont les suivants :

Langue de l'assistant de configuration

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

Langue du SafeGuard Policy Editor

Vous pouvez définir la langue du SafeGuard Policy Editor dans le SafeGuard Policy Editor :

- Ouvrez le menu **Outils > Options > Général**. Sélectionnez **Utiliser la langue définie par l'utilisateur** et sélectionnez une langue disponible. L'anglais, l'allemand, le français et le japonais sont les langues prises en charge.
- Redémarrez le SafeGuard Policy Editor. Il apparaît dans la langue sélectionnée.

Langue Sophos SafeGuard sur les ordinateurs d'extrémité

Pour définir la langue de Sophos SafeGuard sur l'ordinateur d'extrémité dans une stratégie de type **Général** dans le SafeGuard Policy Editor, paramètre **Personnalisation > Langue du client** :

- Si la langue du système d'exploitation est sélectionnée, Sophos SafeGuard utilise le paramètre de langue du système d'exploitation. Si la langue du système d'exploitation n'est pas disponible dans Sophos SafeGuard, la langue par défaut choisie est l'anglais.

- Si l'une des langues sélectionnées est sélectionnée, les fonctions de Sophos SafeGuard apparaissent dans la langue sélectionnée sur l'ordinateur d'extrémité.

6.5 Compatibilité avec les autres produits SafeGuard

Notez les interactions suivantes :

Compatibilité avec SafeGuard LAN Crypt

Notez les éléments suivants :

- SafeGuard LAN Crypt 3.7x et Sophos SafeGuard 5.6x peuvent coexister sur le même ordinateur et sont entièrement compatibles.

Remarque :

Si SafeGuard Enterprise 5.6x est installé en plus de SafeGuard LAN Crypt, le programme d'installation se plaint que le composant SGLC Profile Loader est déjà utilisé. Ce message, causé par le fait que SafeGuard LAN Crypt et SafeGuard Enterprise ont des composants communs, peut être ignoré. Les composants affectés seront mis à jour au redémarrage.

- SafeGuard LAN Crypt avec les versions antérieures à 3.7x et Sophos SafeGuard 5.6x ne peuvent pas coexister sur le même ordinateur.

Si vous essayez d'installer Sophos SafeGuard 5.6x sur un ordinateur sur lequel SafeGuard LAN Crypt version 3.6x ou une version antérieure est déjà installée, l'installation est annulée et un message d'erreur apparaît.

Compatibilité avec SafeGuard PrivateCrypto et SafeGuard PrivateDisk

Sophos SafeGuard 5.6x et les produits autonomes SafeGuard PrivateCrypto (à partir de la version 2.30) et SafeGuard PrivateDisk (à partir de la version 2.30) peuvent coexister sur le même ordinateur.

Compatibilité avec SafeGuard Removable Media

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

Les clés locales créées avec SafeGuard Removable Media postérieures à la version 1.20 avant de changer pour SafeGuard Data Exchange peuvent être utilisées sur l'ordinateur d'extrémité protégé par Sophos SafeGuard. Elles ne sont en revanche pas transférées automatiquement dans la base de données Sophos SafeGuard.

Remarque :

SafeGuard DataExchange n'est pas disponible avec ESDP.

Compatibilité avec SafeGuard Easy 4.x

Lorsque SafeGuard Easy 4.x et le module SafeGuard Data Exchange sont installés sur un ordinateur, les mécanismes GINA de SafeGuard Easy GINA (en particulier, Windows Secure Autologon - SAL) ne fonctionnent plus. En guise de solution, SafeGuard Easy 4.x doit être

installé en premier et les deux produits doivent seulement être désinstallés ensemble (sans redémarrage) pour éviter les conflits GINA.

7 Installation

La configuration de Sophos SafeGuard implique ce qui suit :

	Tâche	Package/outil d'installation	
		ESDP	SGE
1	Installer le SafeGuard Policy Editor sur l'ordinateur de l'administrateur.	SDEPolicyEditor.msi	SGNPolicyEditor.msi
2	Exécuter la première configuration dans le SafeGuard Policy Editor pour la création automatique d'une stratégie par défaut.	Assistant de configuration du SafeGuard Policy Editor	
3	Personnaliser une copie de la stratégie par défaut ou créer d'autres stratégies.	Zone de navigation des stratégies du SafeGuard Policy Editor	
4	Publier les stratégies dans le ou les packages de configuration.	Outil de package de configuration du SafeGuard Policy Editor	
5	Sur les ordinateurs d'extrémité, installer le package de préinstallation qui contient les configurations requises nécessaires pour une installation réussie du logiciel de chiffrement.	SGxClientPreinstall.msi	SGxClientPreinstall.msi
6	Pour utiliser SafeGuard Device Encryption (chiffrement basé sur volume) sur les systèmes d'extrémité, installer :	SDEClient.msi, SDEClient_x64.msi	SGNClient.msi SGNClient_x64.msi Remarque : En outre, Sophos SafeGuard Data Exchange (chiffrement basé sur fichier) peut être manuellement activé dans ce package.
	Pour utiliser seulement SafeGuard Data Exchange (chiffrement basé sur fichier, sans POA) sur les systèmes d'extrémité, installer :	non pris en charge par ESDP	SGNClient_withoutDE.msi SGNClient_withoutDE_x64.msi
7	Installer le ou les packages de configuration sur les ordinateurs d'extrémité.	<Packageconfig>.msi généré	

Remarque :

Si le système d'exploitation de l'ordinateur d'extrémité est Windows 7 64 bits ou Windows Vista 64 bits, vous pouvez installer la variante 64 bits du package "Client" (<nom du package>_x64.msi).

7.1 Installation du SafeGuard Policy Editor

Avant de commencer :

- Assurez-vous de disposer des droits d'administrateur Windows.
- Vérifiez si .NET Framework 3.0 Service Pack 1 est installé sur l'ordinateur sur lequel vous voulez installer le SafeGuard Policy Editor. Vous pouvez le télécharger gratuitement sur le site : <http://www.microsoft.com/downloads/fr-fr/default.aspx>.
- Vérifiez la configuration système requise.
<http://www.sophos.fr/support/knowledgebase/article/112891.html>.
- Pour utiliser un serveur de base de données Microsoft SQL existant, vous devez disposer des droits d'accès et des données de compte SQL nécessaires.

Avant de déployer le logiciel de chiffrement sur les ordinateurs d'extrémité, vous devez d'abord installer le SafeGuard Policy Editor sur l'ordinateur d'un administrateur. Vous pouvez également effectuer la première installation du SafeGuard Policy Editor sur un serveur Windows. Ensuite, vous pourrez l'installer sur plusieurs ordinateurs d'administrateurs connectés à la base de données Sophos SafeGuard centrale du serveur. Le même compte est utilisé pour accéder à chaque instance du SafeGuard Policy Editor.

1. Ouvrez une session sur l'ordinateur en tant qu'administrateur.
2. À partir du dossier d'installation du produit, installez l'un des éléments suivants, en fonction de votre produit. Un assistant vous guide tout au long des étapes nécessaires.

Sophos SafeGuard Disk Encryption	SafeGuard Easy
Cliquez deux fois sur SDEPolicyEditor.msi.	Cliquez deux fois sur SGNPolicyEditor.msi.

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

Une instance de base de données SQL est utilisée pour stocker les paramètres de stratégie de Sophos SafeGuard. Si une instance de base de données SQL existante est indisponible, vous pouvez être invité à installer Microsoft SQL Server 2005 Express lors de l'installation du SafeGuard Policy Editor. Dans ce cas, vos codes d'accès Windows sont utilisés pour le compte utilisateur SQL.

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

Le SafeGuard Policy Editor est installé. Vous pouvez à présent effectuer la première configuration dans le SafeGuard Policy Editor.

7.2 Affichage du système d'aide du SafeGuard Policy Editor

Le système d'aide du SafeGuard Policy Editor s'affiche dans votre navigateur. Il fournit des fonctions complètes telle que l'aide spécifique au contexte ainsi que la recherche sur le texte intégral. Il est configuré pour offrir les fonctionnalités complètes des pages de contenu du système d'aide suite à l'activation de JavaScript dans votre navigateur.

Avec Microsoft Internet Explorer, le comportement est le suivant :

- Windows XP/Windows Vista/Windows 7 - Internet Explorer 6/7/8 - sécurité par défaut :

Vous ne voyez pas de barre de sécurité pour vous informer qu'Internet Explorer a bloqué l'exécution des scripts.
JavaScript est en cours d'exécution.

- Windows 2003 Server Enterprise Edition - Internet Explorer 6 - Configuration de sécurité renforcée (configuration de l'installation par défaut) :

Une boîte de dialogue s'affiche vous informant que la Configuration de sécurité renforcée est activée et que la page exécute les scripts. Vous pouvez désactiver ce message.
JavaScript est en cours d'exécution.

Remarque :

La désactivation de JavaScript ne vous empêche pas de pouvoir toujours afficher et naviguer dans le système d'aide du SafeGuard Policy Editor. Toutefois, certaines fonctionnalités ne pourront pas être utilisées comme par exemple la fonctionnalité de Recherche.

7.3 Exécution de la première configuration dans le SafeGuard Policy Editor

Assurez-vous de disposer des droits d'administrateur Windows.

La première configuration du SafeGuard Policy Editor bénéficie d'une assistance confortable pour une introduction rapide et facile de Sophos SafeGuard :

- Une stratégie par défaut avec des paramètres de chiffrement et d'authentification prédéfinis est automatiquement créée pour introduire une stratégie de sécurité à l'échelle de l'entreprise sur les ordinateurs d'extrémité.
- Toutes les spécifications nécessaires sont fournies pour que le support informatique puisse exécuter les tâches de récupération.
- Les certificats nécessaires et la connexion à la base de données sont créés pour stocker les données Sophos SafeGuard.

Pour démarrer la première configuration :

1. Après l'installation, démarrez le SafeGuard Policy Editor depuis le menu **Démarrer**.
L'assistant de configuration démarre et vous guide tout au long des étapes nécessaires.
2. Dans la page **Bienvenue**, cliquez sur **Suivant**.

7.3.1 Création de la connexion à la base de données

Une base de données sert à stocker tous les paramètres et stratégies de chiffrement Sophos SafeGuard.

1. Sur la page **Base de données**, exécutez l'une des actions suivantes :
 - Pour une première installation, sous **Base de données**, sélectionnez **Créer une base de données**.
 - Pour une installation supplémentaire ou pour réutiliser une base de données créée précédemment, sélectionnez la base de données respective dans la liste **Base de données**. Toutes les bases de données disponibles sur le serveur de base de données actuellement connecté apparaissent. Les paramètres correspondants apparaissent sous **Paramètres de base de données**. Pour les changer, cliquez sur **Changer**, voir [Configuration des paramètres de connexion à la base de données](#) à la page 22.

Remarque :

Une base de données existante peut être utilisée lorsque vous souhaitez installer des instances supplémentaires du SafeGuard Policy Editor, par exemple pour permettre à l'équipe du support d'exécuter Challenge/Réponse.

2. Cliquez sur **Suivant**.

La connexion au serveur de base de données est établie.

7.3.1.1 Configuration des paramètres de connexion à la base de données

1. Dans **Connexion à la base de données**, sous **Serveur de base de données**, sélectionnez dans la liste le serveur de base de données SQL souhaité. Tous les serveurs de base de données disponibles sur votre ordinateur ou sur votre réseau s'affichent (la liste est actualisée toutes les 12 minutes).
2. Sous **Base de données sur serveur**, sélectionnez la base de données respective à utiliser.
3. Sélectionnez **Utiliser SSL** pour protéger la connexion à ce serveur de base de données avec SSL. Le chiffrement SSL requiert cependant un environnement SSL sur l'ordinateur sur lequel se trouve la base de données SQL que vous avez préalablement configurée. Pour plus d'informations, rendez-vous sur :
<http://www.sophos.fr/support/knowledgebase/article/108339.html>
4. Sous **Authentification**, sélectionnez le type d'authentification à utiliser pour accéder à la base de données :
 - Sélectionnez **Utiliser l'authentification Windows NT** pour utiliser vos informations d'identification Windows.

Remarque :

Utilisez ce type d'authentification si votre ordinateur appartient à un domaine. Une configuration obligatoire supplémentaire est nécessaire car l'utilisateur doit être autorisé à se connecter à la base de données. Pour plus d'informations, voir http://www.sophos.com/Products/Manuals/Umbraco/KBA/110259_SafGuard%20Enterprise%20Installation%20best%20practice.pdf (anglais).

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

Remarque :

Utilisez ce type d'authentification si votre ordinateur n'appartient à aucun domaine. Grâce à l'authentification SQL, vous pouvez facilement effectuer ultérieurement la mise à niveau vers le SafeGuard Management Center. Assurez-vous de sélectionner **Utiliser SSL** pour sécuriser la connexion au/du serveur de base de données lorsque vous choisissez ce type d'authentification.

5. Cliquez sur **Vérifier la connexion**. Si l'authentification à la base de données SQL a été établie, un message indiquant qu'elle a réussi s'affiche.
6. Cliquez sur **OK**.

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

Exécutez cette étape lorsque vous avez créé une nouvelle base de données. Au cours d'une première installation et lorsque vous utilisez une nouvelle base de données, un certificat du responsable de la sécurité est créé pour des besoins d'authentification. Un seul compte est créé pour chaque installation. En tant que responsable de la sécurité, vous accédez au SafeGuard Policy Editor pour créer des stratégies SafeGuard Enterprise et configurer le logiciel de chiffrement pour les utilisateurs d'extrémité.

Pour créer le certificat du responsable de la sécurité :

1. Sur la page **Responsable de la sécurité**, le nom de ce dernier est déjà affiché.
Pour les installations avec ESDP, le responsable de la sécurité s'appelle systématiquement **Administrateur**. Pour les autres installations, le nom de l'utilisateur actuel est affiché.
2. Saisissez et confirmez un mot de passe nécessaire pour accéder au SafeGuard Policy Editor.
Conservez le mot de passe en lieu sûr. Si vous le perdez, vous ne pourrez plus accéder au SafeGuard Policy Editor. L'accès au compte est nécessaire pour permettre au support informatique d'exécuter les tâches de récupération.
3. Cliquez sur **Suivant**.

Le certificat du responsable de la sécurité est créé et stocké dans le magasin de certificats. Créez ensuite le certificat d'entreprise.

7.3.3 Importation du certificat du responsable de la sécurité (base de données existante)

Exécutez cette étape lorsque vous utilisez une base de données existante. Lorsque vous utilisez une base de données existante, vous devez importer le certificat du responsable de la sécurité. Seuls les certificats générés par le SafeGuard Policy Editor peuvent être importés. Les certificats créés par une infrastructure de clés publiques (par exemple, Verisign) ne sont pas autorisés.

Pour importer le certificat du responsable de la sécurité :

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

La première configuration lors de l'utilisation d'une base de données existante est terminée. Les étapes de configuration restantes sont uniquement nécessaires lorsque vous créez et utilisez une nouvelle base de données.

7.3.4 Création du certificat d'entreprise

Le certificat d'entreprise est utilisé pour sécuriser les paramètres de stratégie dans la base de données et sur les ordinateurs protégés par Sophos SafeGuard. Il est nécessaire pour récupérer une configuration de base de données endommagée, [voir Restauration d'une configuration de base de données en réinstallant le SafeGuard Policy Editor](#) à la page 53.

1. Sur la page **Entreprise**, saisissez le **Nom de l'entreprise**. Le nom ne doit pas dépasser 64 caractères. Vérifiez que l'option **Créer automatiquement un certificat** est sélectionnée.
Si vous effectuez l'installation pour la première fois et avez créé une nouvelle base de données, l'option **Créer automatiquement un certificat** est déjà sélectionnée.
2. Cliquez sur **Suivant**.

Le nouveau certificat d'entreprise est stocké dans la base de données. Ensuite, sauvegardez les certificats.

7.3.5 Sauvegarde de certificats

Pour restaurer une base de données corrompue ou une installation du SafeGuard Policy Editor, les certificats du responsable de la sécurité et d'entreprise sont nécessaires.

Pour sauvegarder les certificats :

1. Sur la page **Sauvegarde des certificats d'entreprise et du responsable de la sécurité**, spécifiez un emplacement de stockage sûr pour la sauvegarde des certificats. Si vous les enregistrez maintenant dans l'emplacement de stockage par défaut, veillez à les exporter tout de suite après la première configuration dans un emplacement sûr accessible en cas de récupération nécessaire, par exemple un lecteur flash USB. Pour plus d'informations, [voir Exportation du certificat d'entreprise et de celui du responsable de la sécurité](#) à la page 51.
2. Cliquez sur **Suivant**.

Les certificats sont sauvegardés à l'emplacement indiqué. Créez ensuite le magasin de clés de récupération.

7.3.6 Création d'un magasin de clés de récupération

Pour activer la récupération pour les ordinateurs d'extrémité, les fichiers de récupération de clé spécifiques qui sont utilisés doivent pouvoir être accessibles par les membres du support informatique en cas de besoin de récupération. Un partage réseau est créé à cette étape pour rassembler ces fichiers avec des droits d'accès suffisants. Les fichiers de récupération de clé sont chiffrés par le certificat d'entreprise, il est donc prudent de les stocker sur un réseau voire sur un support externe.

Remarque :

Le partage réseau doit se trouver sur un lecteur formaté avec NTFS. NTFS permet de paramétrer les autorisations d'accès.

1. Sur la page **Clés de récupération**, cliquez sur **Suivant** pour confirmer les valeurs par défaut.

Les éléments suivants sont créés :

- Un partage réseau où les clés de récupération sont enregistrées automatiquement.
- Un répertoire par défaut sur l'ordinateur local où les clés de récupération sont enregistrées automatiquement.
- Les droits par défaut pour les membres de l'équipe informatique sur le partage réseau : tous les membres du groupe d'administrateurs locaux sont ajoutés au nouveau groupe Windows **SafeGuardRecoveryKeyAccess**.

Dans un environnement de domaine, ceci inclut aussi le groupe des administrateurs du domaine. Dans le SafeGuard Policy Editor, il est possible de créer plusieurs packages de configuration : par exemple un package pour les ordinateurs dans un environnement de domaine et un autre pour les ordinateurs autonomes.

2. Pour changer les valeurs par défaut :

- Cliquez sur [...] près de **Chemin local** pour changer le répertoire de stockage local comme nécessaire.
- Si vous désélectionnez **Créer un partage réseau**, l'utilisateur final est invité à indiquer un emplacement d'enregistrement des fichiers de clés de récupération à la fin du chiffrement.
- Pour afficher ou changer les membres du groupe ayant accès au partage réseau, cliquez sur **Autorisations**. Pour plus d'informations, voir [Changement des autorisations du partage réseau](#) à la page 26.

Le magasin de clés de récupération avec les autorisations correspondantes est créé.

Remarque :

Le logiciel Sophos SafeGuard tente de se connecter au partage réseau pendant environ 4 minutes et, si cela ne fonctionne pas, essaie de nouveau de s'y connecter après chaque connexion Windows jusqu'à ce que la connexion soit établie ou que les fichiers de récupération de clé soient sauvegardés manuellement.

7.3.6.1 Changement des autorisations du partage réseau

1. Dans **Autorisations du partage réseau**, exécutez l'une des actions suivantes :
 - Cliquez sur **Ajouter des membres locaux** pour ajouter des membres locaux disposant des droits d'administration pour exécuter des actions de récupération.
 - Cliquez sur **Ajouter des membres globaux** pour ajouter des membres globaux disposant des droits d'administration pour exécuter des actions de récupération.
2. Cliquez sur **OK**.

Un groupe **SafeGuardRecoveryKeyAccess** est créé sur l'ordinateur contenant tous les membres affichés dans **Autorisations du partage réseau**.

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

- **Tout le monde** : Créer des fichiers - L'ordinateur Sophos SafeGuard fonctionnant dans le contexte des utilisateurs connectés est autorisé à ajouter des fichiers, mais ne peut pas parcourir le répertoire, supprimer ou lire des fichiers.

Remarque :

L'autorisation "Créer des fichiers" est disponible dans les **Paramètres de sécurité avancés** d'un répertoire.

- **SafeGuardRecoveryKeyAccess** : Modifier - Tous les utilisateurs qui figurent dans la boîte de dialogue **Autorisations** sont autorisés à lire, supprimer ou ajouter des fichiers.
- **Administrateurs** : contrôle total

Sophos SafeGuard supprime aussi l'héritage des autorisations sur le répertoire pour s'assurer que les autorisations ci-dessous ne sont pas remplacées accidentellement.

Le partage réseau **SafeGuardRecoveryKeys\$** est créé avec cette permission :

- **Tout le monde** : contrôle total

Remarque :

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

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

7.3.7 Importation de licences (nouvelle base de données)

Un fichier de licence valide est nécessaire pour exécuter Sophos SafeGuard dans un environnement de production. Si aucune licence valide n'est disponible, vous ne pouvez pas créer de packages de configuration pour le déploiement sur les ordinateurs d'extrémité. Les licences sont disponibles auprès de votre partenaire commercial. Elles doivent être importées dans la base de données Sophos SafeGuard.

Vous pouvez exécuter cette étape si vous avez créé une nouvelle base de données. Lorsque vous utilisez une base de données existante, importez les licences une fois la première configuration terminée.

1. Sur la page **Licence**, exécutez l'une des actions suivantes :

- Pour importer les licences immédiatement, cliquez sur [...] pour rechercher le fichier de licence valide. Sélectionnez le fichier et cliquez sur **Ouvrir**. Cliquez sur **Suivant**. Le fichier de licence est importé dans la base de données Sophos SafeGuard une fois la première configuration terminée. Vous pouvez utiliser la version complète et créer des packages de configuration.
- Pour importer les licences ultérieurement, cliquez sur **Suivant**. Vous pouvez utiliser le SafeGuard Policy Editor, mais vous ne pouvez pas créer de packages de configuration. Pour utiliser la version complète, importez le fichier de licence une fois la première configuration terminée, voir [Importation de licences](#) à la page 43.

7.3.8 Fin de la première configuration

1. Cliquez sur **Terminer**.

La configuration initiale est terminée. Vous avez créé :

- Une stratégie par défaut servant à introduire une stratégie de sécurité sur tous les ordinateurs d'extrémité de l'entreprise :

L'authentification au démarrage est activée.

Le chiffrement basé sur volume de tous les disques durs internes est activé.

L'utilisateur peut récupérer un mot de passe oublié avec Local Self Help en répondant à des questions prédéfinies.

Le support peut récupérer les mots de passe ou l'accès aux données à l'aide de Challenge/Réponse.

Pour les installations SafeGuard Easy seulement, le chiffrement basé sur fichier est activé.

- Toutes les configurations requises nécessaires pour que le support informatique puisse exécuter les tâches de récupération.

Remarque :

Un fichier contenant les paramètres de configuration (Networkshare.xml) et les événements (ConfigurationOutput.xml) est stocké dans le répertoire Temp.

Le SafeGuard Policy Editor démarre dès que l'assistant de configuration se ferme. Si vous n'avez pas importé de fichier de licence valide lors de la première configuration, importez-le maintenant pour avoir les fonctionnalités de tous les composants Sophos SafeGuard, voir [Importation de licences](#) à la page 43.

7.4 Configuration des instances supplémentaires du SafeGuard Policy Editor

1. Lancez le SafeGuard Policy Editor sur l'ordinateur sur lequel vous voulez l'utiliser. L'assistant de configuration démarre et vous guide tout au long des étapes nécessaires.
2. Dans la page **Bienvenue**, cliquez sur **Suivant**.
3. Dans la page **Base de données**, sous **Base de données**, toutes les bases de données disponibles sur le serveur de base de données actuellement connecté apparaissent. Dans la liste, sélectionnez la base de données respective. Les paramètres correspondants apparaissent sous **Paramètres de base de données**. Pour les changer, cliquez sur **Changer**, voir [Configuration des paramètres de connexion à la base de données](#) à la page 22.
4. Cliquez sur **Suivant**.
5. Sur la page **Responsable de la sécurité**, sélectionnez **Importer** pour importer le certificat du responsable de la sécurité associé à la base de données sélectionnée. Recherchez le certificat en question et cliquez sur **Ouvrir**.

Seuls les certificats générés par le SafeGuard Policy Editor peuvent être importés. Les certificats créés par une infrastructure de clés publiques (par exemple, VeriSign) ne sont pas autorisés.
6. Saisissez le mot de passe du magasin de certificats.
7. Cliquez sur **Suivant**, puis sur **Terminer** pour terminer l'assistant de configuration du SafeGuard Policy Editor.

7.5 Installation de Sophos SafeGuard sur les ordinateurs d'extrémité

Les ordinateurs d'extrémité peuvent être équipés de différents composants Sophos SafeGuard en fonction de votre installation, voir [Sophos SafeGuard sur les ordinateurs d'extrémité](#) à la page 9.

Sophos SafeGuard peut être déployé de différentes manières sur les ordinateurs d'extrémité :

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

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

7.5.1 Restrictions

- Sophos SafeGuard pour Windows ne prend pas en charge le matériel d'Apple et ne peut pas être installé dans un environnement Boot Camp.
- Si vous utilisez le mécanisme Intel Advanced Host Controller Interface (AHCI) sur l'ordinateur, le disque dur d'initialisation doit être installé dans le connecteur 0 ou le

connecteur 1. Vous pouvez insérer jusqu'à 32 disques durs. Sophos SafeGuard ne s'exécute que sur les deux premiers numéros de connecteur.

- Les disques dynamiques et les disques de table de partition GUID (GPT) ne sont pas pris en charge. Dans ces cas-là, l'installation est interrompue. Si de tels disques sont trouvés sur l'ordinateur ultérieurement, ils ne sont pas pris en charge.
- Le composant Sophos SafeGuard Device Encryption ne prend pas en charge les systèmes équipés de disques durs reliés par un bus SCSI.

7.5.2 Préparation au chiffrement

Avant d'installer le logiciel de chiffrement, nous vous recommandons de vous préparer comme suit.

- Un compte utilisateur doit être configuré et actif sur les ordinateurs d'extrémité.
- Créez une sauvegarde complète des données sur l'ordinateur d'extrémité.
- Assurez-vous de disposer des droits d'administrateur Windows.
- Sophos fournit une liste des configurations matérielles afin de réduire le risque de conflits entre l'authentification au démarrage et le matériel de votre ordinateur. La liste est fournie avec le package d'installation du logiciel de chiffrement.

Nous vous recommandons d'installer une version mise à jour du fichier de configuration matérielle avant de procéder au déploiement de Sophos SafeGuard. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant : <ftp://ftp.ou.utimaco.de/>

Pour plus d'informations, voir [Raccourcis clavier pris en charge dans l'authentification au démarrage](#) à la page 115. Consultez aussi : <http://www.sophos.fr/support/knowledgebase/article/65700.html>.

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

```
chkdsk %lecteur% /F /V /X
```

Dans certains cas, vous pouvez être invité à redémarrer votre ordinateur et à réexécuter la commande **chkdsk**. Pour plus d'informations, consultez : <http://www.sophos.fr/support/knowledgebase/article/107081.html>.

Vous pouvez vérifier les résultats (fichier journal) dans l'Observateur d'événements Windows :

Windows XP : sélectionnez **Application, Winlogon**.

Windows 7, Windows Vista : sélectionnez **Journaux Windows , Application, Wininit**.

- Utilisez l'outil de défragmentation de Windows appelé **defrag** pour localiser et consolider les éléments fragmentés, notamment les fichiers d'initialisation, les fichiers de données et les dossiers sur les volumes locaux. Pour plus d'informations, rendez-vous sur : <http://www.sophos.fr/support/knowledgebase/article/109226.html>.
- Désinstallez les gestionnaires d'initialisation tiers, tels que PROnetworks Boot Pro et Boot-US.

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

Vous pouvez nettoyer le MBR (Master Boot Record) en démarrant à partir d'un DVD Windows et en exécutant la commande **FIXMBR** dans la Console de récupération Windows. Pour plus d'informations, rendez-vous sur :

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

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

7.5.3 Préparation d'une installation "Modifier"

Si une installation Sophos SafeGuard existante est modifiée ou si des fonctions sont installées ultérieurement, le programme d'installation peut se plaindre que certains composants (par exemple, SafeGuard Removable Media Manager) sont actuellement en cours d'utilisation. Ce message est généré lorsque les fonctions sélectionnées, partageant des composants en cours d'utilisation, ne peuvent pas être mises à jour immédiatement. Ce message peut être ignoré car les composants affectés seront automatiquement mis à jour au redémarrage.

Ce comportement s'applique à une installation en mode surveillé et sans surveillance.

7.5.4 Configuration locale des ordinateurs d'extrémité

Si vous souhaitez exécuter une installation d'évaluation sur un ordinateur d'extrémité, il peut être utile d'installer d'abord Sophos SafeGuard en local.

1. Préparez l'installation sur les ordinateurs d'extrémité, voir [Préparation au chiffrement](#) à la page 29.
2. Ouvrez une session sur l'ordinateur en tant qu'administrateur.
3. Installez le package de préinstallation **SGxClientPreinstall.msi**, qui fournit à l'ordinateur d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement.

Remarque : vous pouvez également installer **vcredist_x86.exe**, téléchargeable sur le site suivant :

<http://www.microsoft.com/downloads/details.aspx?FamilyID=766a6af7-ec73-40ff-b072-9112bab119c2>
ou vérifiez que le fichier **MSVCR80.dll**, version 8.0.50727.4053 se trouve sur l'ordinateur, dans le dossier Windows\WinSxS.

4. Cliquez deux fois sur le package d'installation (MSI) <client> correspondant pour démarrer l'assistant d'installation du logiciel de chiffrement. Il vous guidera tout au long des étapes nécessaires. Installez l'un des éléments suivants :

Sophos SafeGuard Disk Encryption	Sophos SafeGuard Easy
<p>SDEClient.msi pour la variante 32 bits. SDEClient_x64.msi pour la variante 64 bits.</p>	<p>SGNClient.msi pour la variante 32 bits. SGNClient_x64.msi pour la variante 64 bits. SGNClient_withoutDE.msi pour SafeGuard Data Exchange uniquement, variante 32 bits. SGNClient_withoutDE_x64.msi pour SafeGuard Data Exchange uniquement, variante 64 bits.</p>

Remarque :

Même s'il est possible d'installer seulement un sous-ensemble de fonctions lors d'une première installation, nous vous conseillons d'installer la fonction Device Encryption (chiffrement basé sur volume) dès le départ.

5. Validez les valeurs par défaut dans les boîtes de dialogue qui suivent.
6. Si vous y êtes invité, sélectionnez le type d'installation. Les clients installant SGNClient.msi ou SGNClient_x64.msi doivent exécuter l'une des actions suivantes :
- Sélectionnez **Complète** pour installer les composants Device Protection et Data Exchange.
 - Sélectionnez **Standard** pour installer Device Protection uniquement.
 - Sélectionnez **Personnalisée** pour activer les fonctions selon vos besoins.
- La fonction **Data Exchange** n'est pas disponible avec ESDP.
7. Validez les valeurs par défaut dans toutes les boîtes de dialogue qui suivent.
Sophos SafeGuard est installé sur l'ordinateur d'extrémité.
8. Dans le SafeGuard Policy Editor, configurez le logiciel de chiffrement selon vos besoins :
- Utilisez la stratégie par défaut prédéfinie pour un déploiement rapide et facile des stratégies automatiquement créées lors de la première configuration dans le SafeGuard Policy Editor.
 - Si la stratégie par défaut ne couvre pas tous vos besoins spécifiques, vous pouvez la modifier ou définir votre propre stratégie dans le SafeGuard Policy Editor ([voir Utilisation de stratégies](#) à la page 44).
- Par exemple, votre stratégie de déploiement peut nécessiter la configuration d'un accès administrateur à l'ordinateur pour le personnel de maintenance. Dans ce cas, vous devez définir une stratégie spécifique et créer un package de configuration contenant ces stratégies.
9. Publiez les stratégies dans un package de configuration, [voir Utilisation de packages de configuration](#) à la page 49.
10. Installez le package de configuration (MSI) correspondant sur l'ordinateur. Veillez à supprimer tous les packages de configuration obsolètes sur l'ordinateur d'extrémité.

Sophos SafeGuard est installé et configuré en fonction des stratégies précédemment créées sur l'ordinateur d'extrémité. Pour en savoir plus sur le comportement de l'ordinateur après l'installation de Sophos SafeGuard, voir l'aide utilisateur (chapitre *Première connexion après l'installation de Sophos SafeGuard*).

Une configuration supplémentaire peut être requise pour garantir que l'authentification au démarrage fonctionne correctement sur chaque plate-forme matérielle. La plupart des conflits matériels peuvent être résolus à l'aide de la fonction **Raccourcis clavier** intégrée à l'authentification au démarrage. Les raccourcis clavier peuvent être configurés après l'installation, depuis l'authentification au démarrage, ou à l'aide d'un paramètre de configuration supplémentaire transmis à l'outil de déploiement msixec. Pour plus d'informations, voir [Raccourcis clavier dans l'authentification au démarrage](#) à la page 115. Consultez aussi :

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

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

7.5.5 Installation du logiciel de chiffrement et des packages de configuration à l'aide d'un script

1. Préparez l'installation sur les ordinateurs d'extrémité, voir [Préparation au chiffrement](#) à la page 29.
2. Sur l'ordinateur de l'administrateur, créez un dossier appelé **Logiciels** à utiliser comme magasin central pour toutes les applications.

3. Utilisez un outil de déploiement de logiciels comme Microsoft System Center Configuration Manager, IBM Tivoli ou Enteo Netinstall pour exécuter l'installation centrale sur les ordinateurs d'extrémité. Les éléments suivants doivent être inclus dans l'ordre mentionné :

Option	Description
Package de préinstallation SGxClientPreinstall.msi	<p>Pour une installation réussie du logiciel de chiffrement, le package fournit les configurations requises aux ordinateurs d'extrémité.</p> <p>Remarque :</p> <p>Si ce package n'est pas installé, l'installation du logiciel de chiffrement échoue.</p>
Package d'installation <Client>*.msi du logiciel de chiffrement	<p>En fonction de votre produit et de votre système d'exploitation, différents packages d'installation sont disponibles. Pour Windows 7 et Windows Vista par exemple, vous pouvez installer la variante du package *_x64.msi. Tous les packages d'installation <Client> disponibles le sont dans votre produit livré.</p> <p>Remarque :</p> <p>Pour plus d'informations sur tous les packages d'installation <Client> disponibles, voir Configuration locale des ordinateurs d'extrémité à la page 30.</p>
Package de configuration pour ordinateurs d'extrémité	<p>Utilisez le package de configuration créé auparavant dans le SafeGuard Policy Editor. Veillez à supprimer tous les packages de configuration obsolètes.</p>
Script avec les commandes de l'installation préconfigurée	<p>Nous recommandons d'utiliser l'outil de ligne de commande de Windows Installer msiexec pour créer le script. Pour plus d'informations, voir Commande pour l'installation centralisée à la page 34 ou consultez : http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx</p>

4. Pour créer le script, ouvrez une invite de commande et saisissez les commandes de script.
5. Distribuez le package de préinstallation, <Client> et de configuration ainsi que le script sur les ordinateurs d'extrémité à l'aide des mécanismes de distribution de logiciels de l'entreprise.

Les packages sont exécutés sur les ordinateurs d'extrémité.

Sophos SafeGuard est installé et configuré en fonction de la configuration des stratégies précédemment créées sur les ordinateurs d'extrémité. Un fichier de récupération de clé est créé pour chaque ordinateur d'extrémité à l'emplacement défini lors de la première configuration du SafeGuard Policy Editor.

Une configuration supplémentaire peut être requise pour garantir que l'authentification au démarrage fonctionne correctement sur chaque plate-forme matérielle. La plupart des conflits matériels peuvent être résolus à l'aide de la fonctionnalité **Raccourcis clavier** intégrée à

l'authentification au démarrage. Les raccourcis clavier peuvent être configurés après l'installation, depuis l'authentification au démarrage, ou via un paramètre de configuration supplémentaire passé à la commande `msiexec` de Windows Installer. Pour plus d'informations, voir [Raccourcis clavier pris en charge dans l'authentification au démarrage](#) à la page 115. Consultez aussi :

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

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

7.5.5.1 Commande pour l'installation centralisée

Lorsque vous installez Sophos SafeGuard de manière centralisée sur les ordinateurs d'extrémité, utilisez le composant Windows Installer **msiexec**. Inclus dans Windows XP, Vista et Windows 7, **Msiexec** exécute automatiquement une installation préconfigurée de Sophos SafeGuard. Comme la source et la destination du programme d'installation peuvent également être spécifiées, l'installation standard sur plusieurs ordinateurs d'extrémité existe.

Pour plus d'informations, rendez-vous sur :

[http://msdn.microsoft.com/en-us/library/aa367988\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa367988(VS.85).aspx).

Syntaxe de la ligne de commande

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

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

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

Options de commande

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

Option	Description
<code>/i</code>	Spécifie qu'il s'agit d'une installation.
<code>/qn</code>	Exécute une installation sans interaction de l'utilisateur et n'affiche pas d'interface utilisateur.
<code>ADDLOCAL=</code>	Répertorie les fonctions à installer. Si l'option n'est pas spécifiée, toutes les fonctions d'une installation standard sont installées. Pour dresser la liste des fonctions sous <code>ADDLOCAL</code> , gardez à l'esprit les éléments suivants :

Option	Description
	Séparez simplement les fonctions à l'aide d'une virgule et non d'un espace. Respectez la casse. Si vous sélectionnez une fonction, vous devez également ajouter toutes les fonctions parentes à la ligne de commande !
ADDLOCAL=ALL	Installe toutes les fonctions disponibles.
REBOOT=Force ReallySuppress	Force ou supprime un redémarrage après l'installation. Si rien n'est spécifié, le redémarrage est forcé après l'installation.
/L* <chemin + nom de fichier>	Journalise tous les avertissements et messages d'erreur dans le fichier journal spécifié. Le paramètre /Le <chemin + nom de fichier> ne journalise que les messages d'erreur.
InstallDir= <répertoire>	Spécifie le répertoire dans lequel installer le client Sophos SafeGuard. Si aucune valeur n'est spécifiée, le répertoire d'installation par défaut est <SYSTEM>:\PROGRAM FILES\SOPHOS.

7.5.5.2 Fonctions de Sophos SafeGuard (ADDLOCAL)

Pour une installation centralisée, vous devez définir en amont quelles fonctions de Sophos SafeGuard sont à installer sur les ordinateurs d'extrémité. Une liste des fonctions s'affiche après avoir saisi l'option **ADDLOCAL** dans la commande.

Remarque :

Même s'il est possible d'installer seulement un sous-ensemble de fonctions lors d'une première installation, nous vous conseillons d'installer la fonction Device Encryption (chiffrement basé sur volume) dès le départ.

Les tableaux ci-dessous dressent la liste des fonctions Sophos SafeGuard qui peuvent être installées sur les ordinateurs d'extrémité. Pour plus d'informations, consultez l'article <http://www.sophos.fr/support/knowledgebase/article/108426.html>.

Fonctions de SafeGuard Device Encryption

SGNClient.msi, SDEClient.msi ou variantes 64 bits respectives.

Remarque :

Enumérez les fonctions **Client** et **Authentification** par défaut. Si vous sélectionnez une fonction, vous devez également ajouter les fonctions parentes à la ligne de commande.

Fonctions parentes	Fonction
Client	Authentification

Fonctions parentes	Fonction
	Indiquez la fonction Authentification et sa fonction parente Client par défaut.
Client, Authentification	<p>CredentialProvider</p> <p>Vous devez sélectionner cette fonction pour les ordinateurs dotés de Windows Vista et Windows 7. Elle permet d'activer la connexion à l'aide du fournisseur d'informations d'identification.</p>
Client, BaseEncryption	<p>SectorBasedEncryption</p> <p>Installe le chiffrement basé sur volume de Sophos SafeGuard avec les fonctions suivantes :</p> <p>Tous les volumes, supports amovibles inclus, peuvent être chiffrés avec le chiffrement basé sur volume de Sophos SafeGuard.</p> <p>Authentification au démarrage (POA) de Sophos SafeGuard.</p> <p>Récupération de Sophos SafeGuard avec Challenge/Réponse.</p>
Client	<p>SecureDataExchange</p> <p>Remarque :</p> <p>Cette fonction n'est pas prise en charge par ESDP.</p> <p>SafeGuard Data Exchange avec chiffrement basé sur fichier est toujours installé localement et pour les supports amovibles. SafeGuard Data Exchange fournit le chiffrement sécurisé pour les supports amovibles. Les données peuvent être partagées avec d'autres utilisateurs en toute sécurité et facilement. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une interaction utilisateur minimale. Si vous avez installé SafeGuard Data Exchange sur votre ordinateur, SafeGuard Portable l'est également. SafeGuard Portable permet aux données d'être partagées en toute sécurité avec les ordinateurs sur lesquels SafeGuard Data Exchange n'est pas installé.</p>

Fonctions pour SafeGuard Data Exchange

SGNClient_withoutDE.msi ou SGNClient_withoutDE_x64.msi.

Remarque :

Ce package d'installation n'est pas pris en charge par ESDP.

Remarque :

Enumérez les fonctions **Client** et **Authentification** par défaut. Si vous sélectionnez une fonction, vous devez également ajouter les fonctions parentes à la ligne de commande.

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

Exemple de commande pour le chiffrement basé sur volume

La commande indiquée ci-dessous a l'effet suivant :

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

Exemple :

```
msiexec /i F:\Software\SGxClientPreinstall.msi /qn /log
I:\Temp\SGxClientPreinstall.log
```

```
msiexec /i F:\Software\SGNClient.msi /qn /log
I:\Temp\SGNClient.log
```

```
ADDLOCAL=Client,Authentication,BaseEncryption,SectorBasedEncryption
```

```
Installdir=C:\Program Files\Sophos\Sophos SafeGuard
```

```
msiexec /i F:\Software\SDEConfig.msi /qn /log  
I:\Temp\SDEConfig.log
```

7.5.6 Installation conforme à FIPS

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

Sophos SafeGuard utilise des algorithmes AES certifiés FIPS. Par défaut, une nouvelle implémentation plus rapide des algorithmes AES pas encore certifiée FIPS est installée.

Pour utiliser la variante certifiée FIPS de l'algorithme AES, définissez la propriété FIPS_AES sur 1 lors de l'installation du logiciel de chiffrement Sophos SafeGuard.

Cela peut être effectuée de deux manières :

- Ajoutez la propriété au script de ligne de commande suivant :
`msiexec /i F:\Software\SGNClient.msi FIPS_AES=1`
- Utilisez une transformée.

7.5.7 Installation sur des ordinateurs d'extrémité avec disques durs à chiffrement automatique et conformes à Opal

Sophos SafeGuard prend en charge la norme Opal indépendamment des fournisseurs pour les disques durs à chiffrement automatique.

Pour vous assurer que la prise en charge des disques durs à chiffrement automatique conformes à la norme Opal respectent strictement la norme, vous pouvez effectuer deux types de vérification lors de l'installation de Sophos SafeGuard sur l'ordinateur d'extrémité :

■ Vérifications fonctionnelles

Elles incluent, entre autres, de vérifier si le lecteur s'identifie en tant que lecteur de disque dur "OPAL", si les propriétés de communications sont correctes et si les fonctions Opal requises pour Sophos SafeGuard sont prises en charge par le lecteur.

■ Vérifications de sécurité

Les vérifications de sécurité garantissent que seuls les utilisateurs Sophos SafeGuard qui sont enregistrés sur le lecteur sont les propriétaires des clés utilisées pour le chiffrement logiciel de lecteurs ne se chiffrant pas automatiquement. Si d'autres utilisateurs se sont enregistrés lors de l'installation, Sophos SafeGuard tente automatiquement de les désactiver.

Cette fonctionnalité est requise par la norme Opal à l'exception de quelques autres "responsabilités" par défaut qui sont requises pour exécuter un système Opal.

Remarque :

Les vérifications de sécurité sont répétées lorsqu'une stratégie de chiffrement pour le lecteur est appliquée suite à l'installation réussie du mode Opal. En cas d'échec, ceci signifie que la gestion des lecteurs a été modifiée en dehors de Sophos SafeGuard. Dans ce cas, Sophos SafeGuard refuse l'accès au lecteur et un message d'information apparaît.

En cas d'échec irrémédiable de l'une de ces vérifications, l'installation ne revient pas au chiffrement basé sur logiciel. A la place, tous les volumes présents sur le disque Opal restent non chiffrés.

Certains disques durs Opal peuvent avoir des problèmes de sécurité. Il n'est pas possible de savoir automatiquement quels privilèges ont été affectés à un utilisateur/responsable qui a déjà été enregistré sur le lecteur lors de l'installation ou du chiffrement de Sophos SafeGuard. Si le lecteur refuse la commande de désactivation de ces utilisateurs, Sophos SafeGuard restaure le chiffrement logiciel afin de garantir une sécurité maximale de l'utilisateur Sophos SafeGuard. Nous ne sommes pas en position de garantir la sécurité de disques durs, aussi nous avons mis en place un commutateur d'installation qui vous permet d'utiliser à votre propre discrétion les lecteurs affichant des problèmes potentiels de sécurité. Pour voir une liste des lecteurs de disque dur nécessitant l'utilisation d'un commutateur d'installation et pour obtenir plus d'informations sur les lecteurs de disque dur pris en charge, reportez-vous aux Notes de publication de Sophos SafeGuard.

Pour appliquer le commutateur d'installation, utilisez la syntaxe de ligne de commande suivante :

```
MSIEXEC /i <nom_du_client_sélectionné_msi.msi>  
IGNORE_OPAL_AUTHORITYCHECK_RESULTS=1
```

Si vous choisissez de procéder à l'installation avec les fichiers .mst ou d'utiliser, par exemple, ORCA pour modifier votre fichier .msi, sachez que la propriété interne de MSI porte le même nom.

Pour plus d'informations sur Sophos SafeGuard en combinaison avec des disques durs compatibles Opal, [voir Sophos SafeGuard et disques durs compatibles Opal à chiffrement automatique](#) à la page 151.

8 Installation de Sophos SafeGuard sur les ordinateurs disposant de plusieurs systèmes d'exploitation

Remarque :

Cette fonction n'est pas prise en charge par ESDP (Endpoint Security and Data Protection).

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

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

8.1 Conditions requises et restrictions

Notez les éléments suivants :

- Sophos SafeGuard Runtime ne fournit aucune fonction ou fonctionnalité Sophos SafeGuard.
- Sophos SafeGuard Runtime prend seulement en charge les systèmes d'exploitation qui sont aussi pris en charge par le logiciel de chiffrement du client Sophos SafeGuard.
- Le fonctionnement des claviers USB peut être limité.
- Seuls les gestionnaires d'initialisation activés à la suite d'une authentification au démarrage sont pris en charge.
- La prise en charge des gestionnaires d'initialisation tiers n'est pas garantie. Nous recommandons d'utiliser les gestionnaires d'initialisation Windows.
- Sophos SafeGuard Runtime ne peut pas être mis à jour à une installation complète de Sophos SafeGuard.
- Le package d'installation runtime doit être installé avant la version complète du package d'installation du client Sophos SafeGuard.
- Seuls les volumes chiffrés avec la clé machine définie de Sophos SafeGuard sont accessibles.

8.2 Préparations

Pour configurer Sophos SafeGuard Runtime, effectuez les préparatifs suivants dans l'ordre indiqué :

1. Assurez-vous que les volumes sur lesquels Sophos SafeGuard Runtime est exécuté sont visibles au moment de l'installation et peuvent porter leur nom Windows (par exemple C:).

2. Choisissez le ou les volumes du disque dur sur lesquels installer Sophos SafeGuard Runtime. Dans Sophos SafeGuard, ces volumes sont définis comme installations "secondaires" de Windows. Il peut y avoir plusieurs installations secondaires de Windows. Utilisez le package suivant : SGNClientRuntime.msi (ou la variante 64 bits correspondante lorsque le système d'exploitation de l'ordinateur est Windows 7 64 bits ou Windows Vista 64 bits).
3. Choisissez le volume du disque dur sur lequel installer la version complète du client Sophos SafeGuard. Dans Sophos SafeGuard, ce volume est défini comme l'installation "principale" de Windows. Il ne peut y avoir qu'une installation principale de Windows. Utilisez le package suivant : SGNClient.msi (ou la variante 64 bits correspondante lorsque le système d'exploitation de l'ordinateur est Windows 7 64 bits ou Windows Vista 64 bits).

8.3 Configuration de Sophos SafeGuard Runtime

1. Sélectionnez le ou les volumes secondaires requis du disque dur sur lesquels installer Sophos SafeGuard Runtime.
2. Démarrez l'installation secondaire de Windows sur le volume sélectionné.
3. Installez le package d'installation runtime sur le volume sélectionné.
4. Dans la boîte de dialogue qui suit du programme d'installation, confirmez les valeurs par défaut. Il n'est pas nécessaire de sélectionner de fonctions spéciales.
5. Sélectionnez un dossier d'installation pour l'installation runtime.
6. Cliquez sur **Terminer** pour finir l'installation runtime.
7. Sélectionnez le volume principal du disque dur sur lequel installer le client Sophos SafeGuard.
8. Démarrez l'installation principale de Windows sur le volume sélectionné.
9. Démarrez le package d'installation SGxClientPreinstall.msi qui fournit aux ordinateurs d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement.
10. Installez le package d'installation du client Sophos SafeGuard sur le volume sélectionné.
11. Créez le package de configuration et déployez-le sur l'ordinateur d'extrémité.
12. Chiffrez les deux volumes à l'aide de la clé machine définie.

8.4 Démarrage à partir d'un volume secondaire via un gestionnaire d'initialisation

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

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

9 Connexion au SafeGuard Policy Editor

1. Démarrez le SafeGuard Policy Editor dans le menu **Démarrer**. Une boîte de dialogue de connexion apparaît.
2. Saisissez les informations d'identification du responsable de la sécurité définies lors de la première configuration et cliquez sur **OK**.

Le SafeGuard Policy Editor est ouvert.

Remarque :

Deux responsables de la sécurité ne doivent pas utiliser le même compte Windows sur le même ordinateur. Dans le cas contraire, il est impossible de distinguer correctement leurs droits d'accès.

10 Importation de licences

Pour utiliser Sophos SafeGuard dans un environnement de production, des licences valides sont nécessaires. Si aucune licence valide n'est disponible, vous ne pouvez pas créer de packages de configuration pour le déploiement sur les ordinateurs d'extrémité. Le fichier de licence vous est envoyé par votre partenaire commercial. Il doit être importé dans la base de données Sophos SafeGuard. Pour les nouvelles bases de données, vous pouvez importer les fichiers de licence lors de la première configuration, [voir Importation de licences \(nouvelle base de données\)](#) à la page 26.

Pour importer les licences de bases de données existantes :

1. Connectez-vous au SafeGuard Policy Editor à l'aide du mot de passe défini lors de la première configuration.
2. Dans la zone de navigation, cliquez sur **Utilisateurs**.
3. Dans la fenêtre de navigation de gauche, cliquez sur le nœud racine.
4. Dans l'onglet **Licences**, cliquez sur **Importer un fichier de licence...**
5. Sélectionnez le fichier de licence que vous souhaitez importer et cliquez sur **Ouvrir**.

La boîte de dialogue **Application de la licence ?** apparaît avec le contenu du fichier de licence.

6. Cliquez sur le bouton **Appliquer la licence**.

Le fichier de licence contenant les licences nécessaires est importé dans la base de données Sophos SafeGuard.

Dans l'onglet **Licences**, les licences importées sont affichées. L'onglet affiche les informations de licence suivantes :

Colonne	Description
Fonction	Indique le composant ou la fonction sous licence (par exemple, le SafeGuard Policy Editor, Sophos SafeGuard Client, Device Encryption)
Licences achetées	Indique le nombre de licences achetées pour le composant ou la fonction installé.
Version attribuée la plus récente	Indique la version de Sophos SafeGuard la plus récente pour laquelle la licence est valide.
Expire	Indique la date d'expiration de la licence.
Type	Indique le type de licence. Pour les licences complètes, ceci est standard .

Après avoir importé un fichier de licence valide, vous pouvez créer des packages de configuration en vue d'un déploiement sur les ordinateurs d'extrémité, [voir Utilisation de packages de configuration](#) à la page 49.

11 Utilisation de stratégies

Les sections suivantes décrivent comment gérer les stratégies, par exemple, comment les créer, les regrouper et les sauvegarder.

Une stratégie par défaut est automatiquement créée lors de la première configuration dans le SafeGuard Policy Editor, [voir Exécution d'une première configuration dans le SafeGuard Policy Editor](#) à la page 21.

Pour une description de tous les paramètres de stratégie disponibles dans Sophos SafeGuard, [voir Stratégies par défaut](#) à la page 66 et [voir Paramètres de stratégie](#) à la page 74.

11.1 Création de stratégies

1. Connectez-vous au SafeGuard Policy Editor à l'aide du mot de passe défini lors de la première configuration.
2. Dans la zone de navigation, cliquez sur **Stratégies**.
3. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Éléments de stratégie**, puis sélectionnez **Nouveau**.
4. Sélectionnez le type de stratégie. Une boîte de dialogue permettant de nommer la nouvelle stratégie s'affiche.
5. Saisissez un nom et éventuellement une description de la nouvelle stratégie.

Stratégies de protection des périphériques :

Lors de la création d'une stratégie de protection des périphériques, spécifiez d'abord la cible de la protection des périphériques. Les cibles possibles sont les suivantes :

Le stockage de masse (volumes d'initialisation/autres volumes)

Les supports amovibles (non pris en charge par les installations avec ESDP).

Les lecteurs optiques (non pris en charge par les installations avec ESDP).

Les modèles de périphériques de stockage (non pris en charge par les installations avec ESDP).

Les périphériques de stockage distincts (non pris en charge par les installations avec ESDP).

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

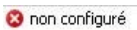
6. Cliquez sur **OK**.

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

11.2 Édition des paramètres de stratégie






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

Remarque :

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

Restauration des valeurs par défaut de paramètres de stratégie

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

	<p>Affiche les valeurs par défaut des paramètres de stratégie qui n'ont pas été configurés (paramètre non configuré).</p>
	<p>Définit le paramètre de stratégie marqué sur non configuré.</p>
	<p>Définit tous les paramètres de stratégie d'une zone sur non configuré.</p>
	<p>Définit la valeur par défaut de la stratégie marquée.</p>
	<p>Définit tous les paramètres de stratégie d'une zone sur la valeur par défaut.</p>

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

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

11.3 Groupes de stratégies

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

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

Remarque :

Les stratégies se chevauchant attribuées à un groupe peuvent aboutir à un calcul incorrect des priorités. Assurez-vous d'utiliser des paramètres de stratégie disjonctifs.

Exception concernant la protection des périphériques :

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

11.3.1 Combinaison de stratégies dans des groupes

Conditions préalables :

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

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

1. Dans la zone de navigation du SafeGuard Policy Editor, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Groupes de stratégies** et sélectionnez **Nouveau**.
3. Cliquez sur **Nouveau groupe de stratégies**. Une boîte de dialogue pour nommer le groupe de stratégies s'affiche.
4. Entrez un nom unique et, éventuellement, la description du groupe de stratégies. Cliquez sur **OK**. Le nouveau groupe de stratégies s'affiche dans la fenêtre de navigation sous **Groupes de stratégies**.
5. Sélectionnez le groupe de stratégies. La zone d'action indique tous les éléments requis pour regrouper les stratégies.
6. Pour ajouter les stratégies au groupe, glissez-les de la liste de stratégies disponibles dans la zone de stratégies.

7. Vous pouvez définir une **priorité** pour chaque stratégie en les organisant grâce au menu contextuel.

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

Exception concernant la protection des périphériques :

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

8. Dans le menu **Fichier**, cliquez sur **Enregistrer**.

Le groupe de stratégies contient maintenant les paramètres des stratégies individuelles. Publiez-le ensuite dans un package de configuration.

11.3.2 Résultats du regroupement de stratégies

Le résultat du regroupement de stratégies s'affiche séparément.

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

- Un onglet distinct s'affiche pour chaque type de stratégie.

Les paramètres obtenus de la combinaison des stratégies individuelles dans un groupe s'affichent.

- Pour les stratégies de protection des périphériques, un onglet s'affiche pour chaque cible de stratégie (volumes d'initialisation, lecteur X, etc.).

11.4 Sauvegarde de stratégies et de groupes de stratégies

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

1. Dans la fenêtre de navigation **Stratégies**, sélectionnez la stratégie/le groupe de stratégies sous **Éléments de stratégie** ou **Groupes de stratégies**.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Sauvegarder la stratégie**.

Remarque :

La commande **Sauvegarder la stratégie** est également accessible dans le menu **Actions**.

3. Dans la boîte de dialogue **Enregistrer sous**, saisissez un nom de fichier et l'emplacement de stockage pour la sauvegarde (fichier XML). Cliquez sur **Enregistrer**.

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

11.5 Restauration de stratégies et de groupes de stratégies

1. Dans la fenêtre de navigation, sélectionnez **Eléments de stratégie/Groupes de stratégies**.
2. Cliquez avec le bouton droit de la souris pour afficher le menu contextuel et sélectionnez **Restaurer une stratégie**.

Remarque :

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

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

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

12 Utilisation de packages de configuration

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

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

Les sections suivantes expliquent comment publier des stratégies dans des packages de configuration et les distribuer sur les ordinateurs d'extrémité.

Remarque :

Vérifiez régulièrement votre réseau et vos ordinateurs pour détecter les packages de configuration obsolètes ou non utilisés, lesquels, pour des raisons de sécurité, devront être supprimés.

12.1 Publication des stratégies dans un package de configuration

Remarque :

Les stratégies sont transférées vers les ordinateurs d'extrémité via un package de configuration. Après avoir créé une nouvelle stratégie ou modifié une stratégie existante, assurez-vous de bien exécuter les étapes suivantes.

Pour créer un package de configuration :

1. Dans le SafeGuard Policy Editor, sélectionnez **Outil de package de configuration** dans le menu **Outils**.
2. Cliquez sur **Ajouter un package de configuration**.
3. Donnez un nom au package de configuration.
4. Spécifiez le **Groupe de stratégies** préalablement créé dans le SafeGuard Policy Editor et que vous souhaitez appliquer aux ordinateurs.

5. Sous **Emplacement de la sauvegarde de la clé**, spécifiez un chemin réseau partagé pour le stockage du fichier de récupération de clé. Saisissez le chemin de partage sous la forme suivante : `\\ordinateurréseau\`, par exemple `\\monentreprise.edu\`. Si vous ne spécifiez pas de chemin ici, l'utilisateur final sera invité à indiquer l'emplacement de stockage de ce fichier lors de sa première connexion à l'ordinateur d'extrémité, suite à l'installation.

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

Remarque :

Veillez à enregistrer le fichier de récupération de clé dans un emplacement accessible au support, un chemin réseau partagé par exemple. Les fichiers peuvent également être fournis au support à l'aide de différents mécanismes. Ce fichier est chiffré par le certificat d'entreprise. Il peut donc être enregistré sur un support externe ou sur le réseau et ainsi être mis à disposition du support à des fins de récupération. Il peut également être envoyé par courriel.

6. Sous **Groupe d'authentification au démarrage**, vous pouvez sélectionner le groupe de comptes d'accès d'authentification au démarrage que vous souhaitez affecter à l'ordinateur d'extrémité. Une fois l'authentification au démarrage activée, les comptes d'accès d'authentification au démarrage fournissent un accès à l'ordinateur d'extrémité pour effectuer des tâches administratives. Pour attribuer des comptes d'accès d'authentification au démarrage, le groupe d'authentification au démarrage doit avoir été préalablement créé dans la zone **Utilisateurs** du SafeGuard Policy Editor.
7. Spécifiez un chemin de sortie pour le package de configuration (MSI).
8. Cliquez sur **Créer un package de configuration**.

Le package de configuration (MSI) a été créé dans le répertoire spécifié. Vous devez maintenant distribuer ce package aux ordinateurs d'extrémité Sophos SafeGuard.

12.2 Distribution de packages de configuration

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

Distribuez le package de configuration sur les ordinateurs d'extrémité en vous aidant des mécanismes de distribution de logiciels de votre entreprise ou installez-le manuellement.

Remarque :

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

Remarque :

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

13 Exportation du certificat d'entreprise et de celui du responsable de la sécurité

Dans une installation Sophos SafeGuard, les deux éléments suivants sont essentiels et doivent être sauvegardés dans un emplacement sûr :

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

Remarque :

Dans l'offre groupée avec ESDP, le responsable de la sécurité est toujours appelé "Administrateur".

Ces deux certificats peuvent être exportés sous la forme de fichiers .p12 à des fins de sauvegarde. Une installation corrompue du SafeGuard Policy Editor ou une configuration de base de données corrompue peut être restaurée en important le certificat approprié (fichier .p12).

Remarque :

Nous vous conseillons de réaliser cette tâche immédiatement après la première configuration dans le SafeGuard Policy Editor.

13.1 Exportation du certificat d'entreprise

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

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

13.2 Exportations du certificat de responsable de la sécurité

Pour sauvegarder le certificat du responsable de la sécurité connecté :

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

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

14 Restauration d'une base de données Sophos SafeGuard

Une base de données Sophos SafeGuard peut être restaurée de la manière suivante :

- Restaurez la base de données Sophos SafeGuard à partir d'un fichier de base de données sauvegardé.

Cette option est seulement disponible avec Sophos SafeGuard Disk Encryption 5.6x (ESDP). La base de données Sophos SafeGuard doit être gérée par Microsoft SQL Server Express et doit résider sur l'ordinateur local.

- Créez une nouvelle instance de la base de données d'après les certificats du responsable de la sécurité et d'entreprise sauvegardés en réinstallant le SafeGuard Policy Editor.

Cette option est disponible avec toutes les installations. Ceci garantit que tous les ordinateurs d'extrémité Sophos SafeGuard acceptent encore les stratégies provenant de la nouvelle instance et permet d'éviter d'avoir à paramétrer et à restaurer l'intégralité de la base de données. En outre, les stratégies sauvegardées peuvent être réimportées.

14.1 Sauvegarde et restauration d'une base de données Sophos SafeGuard

Cette tâche est seulement disponible pour Sophos SafeGuard Disk Encryption (ESDP) et lorsque les conditions préalables requises sont remplies :

- La base de données Sophos SafeGuard est gérée par Microsoft SQL Server Express.
- La base de données Sophos SafeGuard réside sur l'ordinateur local.

Pour sauvegarder et restaurer la base de données :

1. Dans le menu **Outils** du SafeGuard Policy Editor, cliquez sur **Options**, puis cliquez sur **Sauvegarder/Restaurer**.
2. Cliquez sur **Sauvegarder la base de données**, puis cliquez sur **OK**.

Sur votre ordinateur local, la base de données SafeGuard est sauvegardée à l'emplacement spécifié. En tant que responsable de la sécurité, vous pouvez la copier à un emplacement différent. À l'étape suivante, restaurez la base de données.

3. Dans le menu **Outils** du SafeGuard Policy Editor, cliquez sur **Options**, puis cliquez sur **Sauvegarder/Restaurer**.
4. Cliquez sur **Restaurer la base de données**, recherchez le fichier de base de données correspondant et confirmez lorsque vous y êtes invité. Cliquez sur **OK**.

Le SafeGuard Policy Editor est redémarré avec la base de données restaurée.

14.2 Restauration d'une configuration de base de données en réinstallant le SafeGuard Policy Editor

Les conditions préalables suivantes doivent être remplies :

- Les certificats d'entreprise et du responsable de la sécurité de la configuration de base de données correspondante doivent avoir été exportés sous la forme de fichiers .p12, ainsi qu'être disponibles et valides.
- Vous devez également connaître les mots de passe de ces deux fichiers .p12, ainsi que du magasin de certificats.
- Assurez-vous d'exporter les stratégies dans des fichiers de sauvegarde de façon à ce que vous puissiez les restaurer par la suite. Cela vous évitera d'avoir à paramétrer votre configuration de stratégies depuis le début.

Pour restaurer une configuration de base de données corrompue :

1. Effectuez une fraîche installation du package d'installation du SafeGuard Policy Editor.
2. Démarrez le SafeGuard Policy Editor. L'assistant de configuration démarre automatiquement.
3. Sur la page **Base de données**, sélectionnez **Créer une base de données**. Sous **Paramètres de base de données**, configurez la connexion à la base de données. Cliquez sur **Suivant**.
4. Sur la page **Responsable de la sécurité**, sélectionnez le responsable de la sécurité approprié. Deselectionnez **Créer automatiquement un certificat**. Cliquez sur **Importer** pour rechercher le fichier de certificat sauvegardé. Saisissez le mot de passe correspondant au magasin de certificats du responsable de la sécurité. Cliquez sur **Oui** dans le message affiché. Le certificat est alors importé. Saisissez et confirmez le mot de passe du responsable de la sécurité à utiliser pour s'authentifier au SafeGuard Policy Editor. Cliquez sur **Suivant**.
5. Sur la page **Entreprise**, deselectionnez **Créer automatiquement un certificat**. Cliquez sur **Importer** pour rechercher le fichier de certificat sauvegardé qui contient le certificat d'entreprise valide. Vous êtes invité à saisir le mot de passe défini pour le magasin de certificats. Entrez un mot de passe et cliquez sur **OK** pour le confirmer. Cliquez sur **Oui** dans le message affiché. Le certificat d'entreprise est alors importé.
6. Sur la page **Sauvegarde des certificats d'entreprise et du responsable de la sécurité**, spécifiez un emplacement de stockage pour les sauvegardes de certificats. Cliquez sur **Suivant**.
7. Sur la page **Clés de récupération**, deselectionnez **Créer un partage réseau**, cliquez sur **Suivant**, puis sur **Terminer**.

La configuration de la base de données est restaurée. Si vous avez sauvegardé dans un fichier les stratégies précédemment créées, vous pouvez maintenant les importer dans le SafeGuard Policy Editor.

15 Restauration d'une installation corrompue du SafeGuard Policy Editor

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

Pour restaurer l'installation du SafeGuard Policy Editor :

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

L'installation corrompue du SafeGuard Policy Editor est restaurée.

16 Vérification de l'intégrité de la base de données

Lorsque vous vous connectez à la base de données, l'intégrité de cette dernière est vérifiée automatiquement. La boîte de dialogue **Vérifier l'intégrité de la base de données** s'affiche si cette vérification renvoie des erreurs.

Vous pouvez également lancer la vérification de l'intégrité de la base de données et afficher la boîte de dialogue **Vérifier l'intégrité de la base de données** :

1. Dans le menu **Outils** du SafeGuard Policy Editor, sélectionnez **Intégrité base de données**.
2. Pour vérifier les tables, cliquez sur **Tout vérifier** ou **Vérifier sélection**.

Les tables erronées sont indiquées dans la boîte de dialogue.

3. Pour les réparer, cliquez sur **Réparer**.

Les tables de base de données erronées sont réparées.

17 Accès administratif aux ordinateurs d'extrémité

Sophos SafeGuard utilise deux types de comptes pour permettre aux utilisateurs de se connecter aux ordinateurs d'extrémité et d'exécuter des tâches administratives après l'installation de Sophos SafeGuard.

■ Comptes de service pour la connexion Windows

Grâce aux comptes de service, les utilisateurs (opérateurs chargés du déploiement ou membres de l'équipe informatique) peuvent se connecter (connexion Windows) aux ordinateurs d'extrémité après l'installation de Sophos SafeGuard, et ce, sans avoir à activer l'authentification au démarrage et sans être ajoutés en tant qu'utilisateurs sur les ordinateurs. Les utilisateurs figurant sur une liste de comptes de service sont considérés comme des utilisateurs invités lorsqu'ils se connectent à l'ordinateur d'extrémité.

Pour plus d'informations, voir [Listes de comptes de service pour la connexion Windows](#) à la page 56.

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

■ Comptes d'accès POA pour connexion POA

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

Pour plus d'informations, voir [Comptes d'accès POA pour connexion POA](#) à la page 61.

17.1 Listes de comptes de service pour la connexion Windows

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

Le scénario peut ainsi être le suivant :

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

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

Pour garantir que les opérations administratives sur un ordinateur protégé par Sophos SafeGuard ne conduisent pas à une activation de l'authentification au démarrage et à l'ajout d'opérateurs en charge du déploiement comme utilisateurs dudit ordinateur, Sophos SafeGuard vous permet de créer des listes de comptes de service pour les ordinateurs d'extrémité. Les utilisateurs inclus dans ces listes sont traités comme des utilisateurs invités Sophos SafeGuard.

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

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

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

Remarque :

Vous devez affecter des listes de comptes de service dans le premier package de configuration Sophos SafeGuard créé pour configurer les ordinateurs d'extrémité. Vous pouvez mettre à jour les listes de comptes de service en créant un nouveau package de configuration avec des paramètres modifiés et en les déployant sur les ordinateurs d'extrémité avant l'activation de la POA.

17.1.1 Création de listes de comptes de service et ajout d'utilisateurs

1. Dans la zone de navigation, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation de la stratégie, sélectionnez **Listes de comptes de service**.
3. Dans le menu contextuel de l'option **Listes de comptes de service**, cliquez sur **Nouveau > Liste de comptes de service**.
4. Saisissez un nom pour la liste de comptes de service, puis cliquez sur **OK**.
5. Sélectionnez la nouvelle liste sous **Listes de comptes de service** dans la fenêtre de navigation de la stratégie.
6. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel de la liste de comptes de service. Dans le menu contextuel, sélectionnez **Ajouter**.
Une nouvelle ligne utilisateur est ajoutée.
7. Entrez le **Nom d'utilisateur** et le **Nom du domaine** dans les colonnes correspondantes, puis appuyez sur **Entrée**. Répétez cette étape pour ajouter d'autres utilisateurs.
8. Enregistrez vos modifications en cliquant sur l'icône **Enregistrer** de la barre d'outils.

La liste de comptes de service est à présent enregistrée et peut être sélectionnée dès lors que vous créez une stratégie.

17.1.1.1 Informations supplémentaires pour la saisie de noms d'utilisateur et de domaine

Il existe plusieurs méthodes servant à spécifier des utilisateurs dans les listes de comptes de service. Deux champs sont alors utilisés : **Nom d'utilisateur** et **Nom du domaine**. Les restrictions s'appliquent aussi pour les entrées valides dans ces champs.

Présentation des différentes combinaisons de connexion

Les deux champs distincts **Nom d'utilisateur** et **Nom du domaine** par entrée de liste vous permettent de couvrir toutes les combinaisons disponibles de connexion, par exemple "utilisateur@domaine" ou "domaine\utilisateur".

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

Par exemple :

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

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

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

Par exemple :

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

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

Les utilisateurs peuvent se connecter de différentes manières, par exemple :

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

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

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

Remarque :

Afin d'éviter les problèmes liés au fait que Windows peut utiliser des noms tronqués et non la même séquence de caractères, nous vous recommandons de saisir le NomComplet et le nom NetBIOS, voire d'utiliser des caractères génériques.

Restrictions

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

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

Les restrictions suivantes s'appliquent aussi :

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

17.1.2 Modification et suppression des listes de comptes de service

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

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

17.1.3 Attribution d'une liste de comptes de service avec une stratégie

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

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

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

Vous pouvez à présent déployer la stratégie sur les ordinateurs concernés et rendre les comptes de service disponibles sur l'ordinateur.

Remarque :

Si vous sélectionnez des listes de comptes de service différentes dans des stratégies qui le sont tout autant et qui correspondent toutes au RSOP (Resulting Set of Policies, paramètre valide pour un ordinateur/groupe spécifique), la liste de comptes de service affectée à la dernière

stratégie appliquée prend le dessus sur toutes les listes de comptes de service précédemment attribuées. Les listes de comptes de service ne sont pas fusionnées.

17.1.4 Transfert de la stratégie à l'ordinateur d'extrémité

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

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

Remarque :

La fonctionnalité de liste de comptes de service se révèle tout particulièrement utile et importante durant l'installation initiale, au cours de la phase de déploiement d'une mise en œuvre. Nous vous conseillons par conséquent d'inclure une stratégie **Authentification** avec les paramètres requis de la liste de comptes de service du groupe de stratégies transféré avec le premier package de configuration Sophos SafeGuard.

Remarque :

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

17.1.5 Connexion à un ordinateur d'extrémité à l'aide d'un compte de service

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

Affichage de l'état du compte de service sur l'ordinateur d'extrémité

L'état de connexion de l'utilisateur invité peut également être affiché via l'icône de la barre d'état système. Pour plus d'informations, consultez l'aide utilisateur de Sophos SafeGuard au chapitre *Icône de la barre d'état système et infobulle* (description du champ sur l'état de l'utilisateur).

17.1.6 Journalisation des événements

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

Sophos SafeGuard Policy Editor

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

- Liste de comptes de service <nom> supprimée

Ordinateur d'extrémité Sophos SafeGuard

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

17.2 Comptes d'accès POA pour connexion POA

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

Vous pouvez créer des comptes d'accès POA dans le SafeGuard Policy Editor, les regrouper dans des groupes de comptes d'accès POA et affecter ces groupes à des ordinateurs d'extrémité à l'aide des packages de configuration Sophos SafeGuard. Les utilisateurs, c'est-à-dire les comptes d'accès POA, inclus dans le groupe de comptes d'accès POA attribué, sont ajoutés à la POA et peuvent se connecter à l'aide de leur nom d'utilisateur et de leur mot de passe prédéfinis.

17.2.1 Création de comptes d'accès POA

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

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

4. Dans le champ **Nom complet**, saisissez un nom, par exemple le nom de connexion du nouvel utilisateur POA.
5. Vous pouvez également entrer une description pour le nouvel utilisateur POA.
6. Saisissez un mot de passe pour le nouveau compte d'accès POA et confirmez-le.

Remarque :

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

7. Cliquez sur **OK**.

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

17.2.2 Modification du mot de passe d'un compte d'accès POA

1. Dans la zone de navigation du SafeGuard Policy Editor, cliquez sur **Utilisateurs**.
2. Dans la fenêtre de navigation **Utilisateurs**, sous **POA**, **Utilisateurs POA**, sélectionnez un utilisateur POA.
3. Dans le menu contextuel de cet utilisateur POA, sélectionnez **Propriétés**.
La boîte de dialogue Propriétés de l'utilisateur POA s'affiche.
4. Dans l'onglet **Général**, sous **Mot de passe utilisateur**, saisissez le nouveau mot de passe et confirmez-le.
5. Cliquez sur **OK**.

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

17.2.3 Suppression de comptes d'accès POA

1. Dans la zone de navigation du SafeGuard Policy Editor, cliquez sur **Utilisateurs**.
2. Dans la fenêtre de navigation **Utilisateurs**, sous **POA**, **Utilisateurs POA**, sélectionnez un compte d'accès POA.
3. Cliquez avec le bouton droit de la souris sur le compte d'accès POA et sélectionnez **Supprimer** dans le menu contextuel.

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

Remarque :

Si l'utilisateur appartient à un ou plusieurs groupes POA, le compte d'accès POA est également supprimé de ces groupes. Le compte d'accès POA reste cependant disponible sur l'ordinateur d'extrémité jusqu'à ce qu'un nouveau package de configuration soit créé et attribué. Pour en savoir plus sur les groupes POA, [voir Création de groupes de comptes d'accès POA](#) à la page 62. Pour plus de détails sur le changement de l'attribution des comptes d'accès POA, [voir Changement de l'attribution des comptes d'accès POA sur les ordinateurs d'extrémité](#) à la page 64

17.2.4 Création de groupes de comptes d'accès POA

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

1. Dans la zone de navigation du SafeGuard Policy Editor, cliquez sur **Utilisateurs**.
2. Dans la fenêtre de navigation **Utilisateurs**, sous **POA**, sélectionnez **Groupes POA**.
3. Dans le menu contextuel des **Groupes POA**, cliquez sur **Nouveau > Créer un groupe**.
La boîte de dialogue **Créer un groupe** s'affiche.
4. Dans le champ **Nom complet**, saisissez le nom du nouveau groupe POA.

5. Vous pouvez également entrer une description pour le nouveau groupe POA.
6. Cliquez sur **OK**.

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

17.2.5 Ajout de comptes aux groupes de comptes d'accès POA

1. Dans la zone de navigation du SafeGuard Policy Editor, cliquez sur **Utilisateurs**.
2. Dans la fenêtre de navigation **Utilisateurs**, sous **POA, Groupe POA**, sélectionnez un groupe POA.

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

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

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

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

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

Remarque :

Vous pouvez également ajouter des comptes aux groupes en sélectionnant l'utilisateur POA (compte d'accès POA) dans la fenêtre de navigation et en exécutant les étapes décrites ci-dessus. La seule différence est que la zone d'action affiche l'onglet **Membre de** après la sélection de l'utilisateur. Cet onglet affiche les groupes auxquels l'utilisateur a été attribué. Le flux de travail de base reste le même.

17.2.5.1 Suppression de membres des groupes de comptes d'accès POA

1. Dans la zone de navigation du SafeGuard Policy Editor, cliquez sur **Utilisateurs**.
2. Dans la fenêtre de navigation **Utilisateurs**, sous **POA, Groupe POA**, sélectionnez un groupe POA.

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

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

L'utilisateur est supprimé du groupe.

Remarque :

Vous pouvez également supprimer des membres des groupes en sélectionnant l'utilisateur POA (comptes d'accès POA) dans la fenêtre de navigation et en exécutant les étapes décrites ci-dessus. La seule différence est que la zone d'action affiche l'onglet **Membre de** après la

sélection de l'utilisateur. Cet onglet affiche les groupes auxquels l'utilisateur a été attribué. Le flux de travail de base reste le même.

17.2.6 Attribution de comptes d'accès POA aux ordinateurs d'extrémité

1. Dans le SafeGuard Policy Editor, sélectionnez **Outil de package de configuration** dans le menu **Outils**.
2. Sélectionnez un package de configuration existant ou créez-en un nouveau.

Pour plus de détails sur la création d'un package de configuration, voir [Publication des stratégies dans un package de configuration](#) à la page 49.

3. Spécifiez un **Groupe POA** préalablement créé dans la zone **Utilisateurs** du SafeGuard Policy Editor, à appliquer aux ordinateurs.

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

Vous pouvez sélectionner un groupe vide par défaut. Ce groupe peut être utilisé pour supprimer les attributions de groupes de comptes d'accès POA sur les ordinateurs d'extrémité. Pour plus d'informations, voir [Suppression de comptes d'accès POA des ordinateurs d'extrémité](#) à la page 64.

4. Spécifiez un chemin de sortie pour le package de configuration (MSI).
5. Cliquez sur **Créer un package de configuration**.
6. Déployez le package de configuration (MSI) sur les ordinateurs d'extrémité.

L'installation du package de configuration entraîne l'ajout des utilisateurs (comptes d'accès POA) inclus dans le groupe à la POA sur les ordinateurs d'extrémité. Les comptes d'accès POA sont disponibles pour la connexion POA.

17.2.7 Changement de l'attribution de comptes d'accès POA sur les ordinateurs d'extrémité

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

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

17.2.8 Suppression de comptes d'accès POA des ordinateurs d'extrémité

Les comptes d'accès POA peuvent être supprimés des ordinateurs d'extrémité en leur attribuant un groupe de comptes d'accès POA vide.

1. Dans le SafeGuard Policy Editor, sélectionnez **Outil de package de configuration** dans le menu **Outils**.

2. Sélectionnez un package de configuration existant ou créez-en un nouveau.
Pour plus de détails sur la création d'un package de configuration, voir [Publication des stratégies dans un package de configuration](#) à la page 49.
3. Spécifiez un **Groupe POA** vide créé préalablement dans la zone **Utilisateurs** du SafeGuard Policy Editor ou sélectionnez le groupe POA vide disponible par défaut dans l'**Outil de package de configuration**.
4. Spécifiez un chemin de sortie pour le package de configuration (MSI).
5. Cliquez sur **Créer un package de configuration**.
6. Déployez le package de configuration sur les ordinateurs d'extrémité.

L'installation du package de configuration entraîne la suppression de tous les comptes d'accès POA des ordinateurs d'extrémité. Ceci supprime tous les utilisateurs correspondants de la POA.

17.2.9 Connexion à un ordinateur d'extrémité à l'aide d'un compte d'accès POA

1. Mettez l'ordinateur sous tension.
La boîte de dialogue de connexion de l'authentification au démarrage s'affiche.
2. Saisissez le **Nom d'utilisateur** et le **Mot de passe** du compte d'accès POA prédéfini.
Vous n'êtes pas connecté à Windows automatiquement. La boîte de dialogue de connexion de Windows s'affiche.
3. Dans le champ **Domaine**, sélectionnez le domaine <POA>.
4. Connectez-vous à Windows à l'aide de votre compte utilisateur Windows existant.

18 Stratégies par défaut

Lors de la première configuration dans le SafeGuard Policy Editor, une stratégie par défaut avec des paramètres prédéfinis de chiffrement et d'authentification est automatiquement créée.

Après installation, la stratégie par défaut comportant tous les éléments individuels de stratégie apparaît dans la zone de navigation **Stratégies** du SafeGuard Policy Editor.

Remarque :

La stratégie par défaut ne peut être créée que lors de la première configuration dans l'assistant de configuration du SafeGuard Policy Editor.

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

Pour une description détaillée des paramètres de stratégie, [voir Paramètres de stratégie](#) à la page 74.

18.1 Stratégies par défaut disponibles avec SGE

Remarque :

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

Pour une description détaillée des paramètres de stratégie, [voir Paramètres de stratégie](#) à la page 74.

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

Stratégie	Paramètres
	<ul style="list-style-type: none"> ■ Autoriser la connexion Windows automatique : Oui
<p>Stratégie d'authentification par défaut Type de stratégie : Authentification</p>	<p>Accès :</p> <ul style="list-style-type: none"> ■ L'utilisateur peut uniquement initialiser à partir du disque dur : Oui <p>Options de connexion :</p> <ul style="list-style-type: none"> ■ Mode de connexion : ID utilisateur/Mot de passe ■ Afficher les échecs de connexion pour cet utilisateur : Non ■ Afficher la dernière connexion utilisateur : Non ■ Désactiver la 'déconnexion forcée' dans le verrouillage du poste de travail : Non ■ Activer la présélection utilisateur/domaine : Oui ■ Authentification automatique à Windows : Laisser l'utilisateur choisir <p>Échecs de connexion :</p> <ul style="list-style-type: none"> ■ Nbre maximum d'échecs de connexion: 16 ■ Messages d'échec de connexion dans l'authentification au démarrage (POA) : Standard <p>Réaction aux échecs de connexion :</p> <ul style="list-style-type: none"> ■ Verrouiller la machine : Oui
<p>Stratégie de mot de passe par défaut Type de stratégie : Mot de passe</p>	<p>Mot de passe :</p> <ul style="list-style-type: none"> ■ Longueur min. du mot de passe : 4 ■ Longueur max. du mot de passe : 128 ■ Nombre min. de lettres : 0 ■ Nombre min. de chiffres : 0 ■ Nombre min. de caractères spéciaux : 0 ■ Respecter la casse : Non ■ Interdire la succession de touches horizontales : Non ■ Interdire la succession de touches verticales : Non

Stratégie	Paramètres
	<ul style="list-style-type: none"> ■ Au moins 3 caractères consécutifs non autorisés : Non ■ Utilisation interdite du nom d'utilisateur comme mot de passe : Non ■ Utiliser la liste des mots de passe interdits : Non <p>Modifications :</p> <ul style="list-style-type: none"> ■ Modification du mot de passe autorisée après un min. de (jours) : non configuré (la valeur par défaut 0 s'applique) ■ Expiration du mot de passe après (jours) : non configuré (la valeur par défaut 999 s'applique) ■ Avertir d'un changement obligatoire avant (jours) : non configuré (la valeur par défaut 10 s'applique) <p>Général :</p> <ul style="list-style-type: none"> ■ Longueur de l'historique de mot de passe : 0
<p>Stratégie de chiffrement de périphérique par défaut</p> <p>Type de stratégie : Protection des périphériques</p>	<p>Chiffre tous les disques internes.</p> <ul style="list-style-type: none"> ■ Mode de chiffrement du support : Basé sur volume <p>Paramètres généraux :</p> <ul style="list-style-type: none"> ■ Algorithme à utiliser pour le chiffrement : AES256 ■ Clé à utiliser pour le chiffrement : Clé machine définie ■ L'utilisateur est autorisé à créer une clé locale : non configuré (la valeur par défaut Oui s'applique) <p>Paramètres basés sur volume :</p> <ul style="list-style-type: none"> ■ L'utilisateur peut ajouter ou supprimer des clés d'un volume chiffré : non configuré (la valeur par défaut Non s'applique) ■ Réaction aux volumes non chiffrés : Accepter tous les supports et chiffrer ■ L'utilisateur peut déchiffrer le volume : Non ■ Poursuivre sur les secteurs incorrects : Oui

Stratégie	Paramètres
<p>Stratégie d'échange de données par défaut</p> <p>Type de stratégie : Protection des périphériques</p>	<p>Chiffre les supports amovibles</p> <ul style="list-style-type: none"> ■ Mode de chiffrement du support : Basé sur fichier <p>Paramètres généraux :</p> <ul style="list-style-type: none"> ■ Algorithme à utiliser pour le chiffrement : AES256 ■ Clé à utiliser pour le chiffrement : Toute clé du jeu de clés utilisateur <p>Paramètres sur fichier :</p> <ul style="list-style-type: none"> ■ L'utilisateur peut définir une phrase de passe de support pour les périphériques : Oui ■ Copier portable SG vers support amovible : Oui
<p>Stratégie de réglages machine par défaut</p> <p>Type de stratégie : Paramètres machine spécifiques</p>	<p>Authentification au démarrage (POA) :</p> <ul style="list-style-type: none"> ■ Activer l'authentification au démarrage : Oui <p>Éveil par appel réseau (WOL) sécurisé :</p> <ul style="list-style-type: none"> ■ Nombre de connexions automatiques : 0 ■ Connexion à Windows autorisée pendant le WOL : Non <p>Options d'affichage :</p> <ul style="list-style-type: none"> ■ Afficher l'identification de la machine : Nom du poste de travail ■ Afficher la mention légale : Non ■ Afficher des infos supplémentaires : Jamais ■ Activer et afficher l'icône de la barre d'état système : Oui ■ Afficher les icônes en chevauchement dans l'Explorateur : Oui ■ Clavier virtuel dans la POA : Oui <p>Options d'installation :</p> <ul style="list-style-type: none"> ■ Désinstallation autorisée : Oui ■ Activer la protection antialtération Sophos : Oui <p>Remarque :</p> <p>Ce paramètre ne s'applique qu'aux ordinateurs d'extrémité sur lesquels Sophos Endpoint</p>

Stratégie	Paramètres
	Security and Control version 9.5 ou ultérieure est installé.
Stratégie de journalisation par défaut Type de stratégie : Journalisation	Journalise uniquement les erreurs dans le journal d'événements, ignore les autres.

18.2 Stratégies par défaut disponibles avec ESDP

Remarque :

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

Pour une description détaillée des paramètres de stratégie, voir [Paramètres de stratégie](#) à la page 74.

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

Stratégie	Paramètres
	<p>Options de connexion :</p> <ul style="list-style-type: none"> ■ Mode de connexion : ID utilisateur/Mot de passe ■ Afficher les échecs de connexion pour cet utilisateur : Non ■ Afficher la dernière connexion utilisateur : Non ■ Désactiver la 'déconnexion forcée' dans le verrouillage du poste de travail : Non ■ Activer la présélection utilisateur/domaine : Oui ■ Authentification automatique à Windows : Laisser l'utilisateur choisir <p>Échecs de connexion :</p> <ul style="list-style-type: none"> ■ Nbre maximum d'échecs de connexion : 16 ■ Messages d'échec de connexion dans l'authentification au démarrage (POA) : Standard <p>Réaction aux échecs de connexion :</p> <ul style="list-style-type: none"> ■ Verrouiller la machine : Oui
<p>Stratégie de mot de passe par défaut Type de stratégie : Mot de passe</p>	<p>Mot de passe :</p> <ul style="list-style-type: none"> ■ Longueur min. du mot de passe : 4 ■ Longueur max. du mot de passe : 128 ■ Nombre min. de lettres : 0 ■ Nombre min. de chiffres : 0 ■ Nombre min. de caractères spéciaux : 0 ■ Respecter la casse : Non ■ Interdire la succession de touches horizontales : Non ■ Interdire la succession de touches verticales : Non ■ Au moins 3 caractères consécutifs non autorisés : Non ■ Utilisation interdite du nom d'utilisateur comme mot de passe : Non ■ Utiliser la liste des mots de passe interdits : Non

Stratégie	Paramètres
	<p>Modifications :</p> <ul style="list-style-type: none"> ■ Modification du mot de passe autorisée après un min. de (jours) : non configuré (la valeur par défaut 0 s'applique) ■ Expiration du mot de passe après (jours) : non configuré (la valeur par défaut 999 s'applique) ■ Avertir d'un changement obligatoire avant (jours) : non configuré (la valeur par défaut 10 s'applique) <p>Général :</p> <ul style="list-style-type: none"> ■ Longueur de l'historique de mot de passe : 0
<p>Stratégie de chiffrement de périphérique par défaut</p> <p>Type de stratégie : Protection des périphériques</p>	<p>Chiffre tous les disques internes.</p> <ul style="list-style-type: none"> ■ Mode de chiffrement du support : Basé sur volume <p>Paramètres généraux :</p> <ul style="list-style-type: none"> ■ Algorithme à utiliser pour le chiffrement : AES256 ■ Clé à utiliser pour le chiffrement : Clé machine définie <p>Paramètres basés sur volume :</p> <ul style="list-style-type: none"> ■ Réaction aux volumes non chiffrés : Accepter tous les supports et chiffrer ■ L'utilisateur peut déchiffrer le volume : Non ■ Poursuivre sur les secteurs incorrects : Oui
<p>Stratégie de réglages machine par défaut</p> <p>Type de stratégie : Paramètres machine spécifiques</p>	<p>Authentification au démarrage (POA) :</p> <ul style="list-style-type: none"> ■ Activer l'authentification au démarrage : Oui <p>Éveil par appel réseau (WOL) sécurisé :</p> <ul style="list-style-type: none"> ■ Nombre de connexions automatiques : 0 ■ Connexion à Windows autorisée pendant le WOL : Non <p>Options d'affichage :</p> <ul style="list-style-type: none"> ■ Afficher l'identification de la machine : Nom du poste de travail ■ Afficher la mention légale : Non ■ Afficher des infos supplémentaires : Jamais

Stratégie	Paramètres
	<ul style="list-style-type: none"> ■ Activer et afficher l'icône de la barre d'état système : Oui ■ Afficher les icônes en chevauchement dans l'Explorateur : Oui ■ Clavier virtuel dans la POA : Oui <p>Options d'installation :</p> <ul style="list-style-type: none"> ■ Désinstallation autorisée : Oui ■ Activer la protection antialtération Sophos : Oui <p>Remarque :</p> <p>Ce paramètre ne s'applique qu'aux ordinateurs d'extrémité sur lesquels Sophos Endpoint Security and Control version 9.5 ou ultérieure est installé.</p>
<p>Stratégie de journalisation par défaut</p> <p>Type de stratégie : Journalisation</p>	<p>Journalise uniquement les erreurs dans le journal d'événements, ignore les autres.</p>

19 Paramètres de stratégie

Les stratégies de Sophos SafeGuard comportent tous les paramètres nécessaires pour mettre en œuvre une stratégie de sécurité à l'échelle de l'entreprise sur les ordinateurs d'extrémité.

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

■ Paramètres généraux

Paramètres de taux de transfert, d'images d'arrière-plan, etc.

■ Authentification

Paramètres de mode de connexion, verrouillage de périphérique, etc.

■ PIN

Définit la configuration minimale des codes PIN utilisés.

■ Mots de passe

Définit la configuration minimale des mots de passe des utilisateurs.

■ Phrases de passe pour SafeGuard Data Exchange

Remarque :

Ces paramètres ne sont pas pris en charge par ESDP (Endpoint Security and Data Protection).

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

■ Protection du périphérique

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

■ Paramètres machine spécifiques

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

■ Journalisation

Définit les événements à journaliser.

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

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

19.1 Paramètres généraux

Paramètre de stratégie	SGE	ESDP	Explication
PERSONNALISATION			
Langue utilisée sur le client	✔	✔	Langue dans laquelle les paramètres de Sophos SafeGuard sont affichés sur un ordinateur d'extrémité. Les utilisateurs peuvent sélectionner une langue prise en charge ou le paramètre de langue du système d'exploitation de l'ordinateur d'extrémité.
RÉCUPÉRATION DE LA CONNEXION			
Activer la récupération de connexion après la corruption du cache local Windows	✔	✔	Le cache local Windows stocke toutes les clés, stratégies, certificats d'utilisateur et fichiers d'audit. Les données stockées dans le cache local sont signées et ne peuvent pas être modifiées manuellement. Lorsque le cache local Windows est corrompu, la récupération de connexion est désactivée par défaut, c'est-à-dire que sa restauration s'effectue automatiquement à partir de la sauvegarde. Aucune procédure Challenge/Réponse n'est donc requise pour réparer le cache local Windows. Si le cache local Windows doit être réparé explicitement via une procédure Challenge/Réponse, choisissez "OUI" dans ce champ.
Local Self Help			
Activer Local Self Help	✔	✔	Détermine si les utilisateurs sont autorisés à se connecter à leurs ordinateurs avec Local Self Help en cas d'oubli de leur mot de passe. Avec Local Self Help, l'utilisateur peut se connecter en répondant à un nombre spécifique de questions prédéfinies dans l'authentification au démarrage. Il peut de nouveau accéder à son ordinateur même si aucune connexion téléphonique ou Internet n'est disponible. Pour plus d'informations, voir Récupération avec Local Self Help à la page 129.

Paramètre de stratégie	SGE	ESDP	Explication
			<p>Remarque :</p> <p>La connexion automatique à Windows doit être activée pour que l'utilisateur puisse utiliser Local Self Help. Dans le cas contraire, Local Self Help ne fonctionne pas.</p>
Longueur minimale des réponses	✓	✓	Définit une longueur minimale de caractères pour les réponses Local Self Help.
Texte de bienvenue sous Windows	✓	✓	Dans ce champ, vous pouvez spécifier le texte d'informations à afficher dans la première boîte de dialogue au démarrage de l'assistant de Local Self Help sur l'ordinateur d'extrémité. Avant de spécifier le texte ici, il doit être créé et enregistré.
L'utilisateur peut définir des questions personnalisées	✓	✓	En tant que responsable de la sécurité, vous pouvez définir de manière centralisée les questions auxquelles répondre et les distribuer sur l'ordinateur d'extrémité dans la stratégie. Toutefois, vous pouvez également accorder aux utilisateurs le droit de définir des questions personnalisées. Pour autoriser les utilisateurs à définir leurs propres questions, sélectionnez Oui .
Challenge / Réponse (C/R)			
Activer la récupération de la connexion (via C/R)	✓	✓	<p>Détermine si, dans le cadre d'une récupération de connexion, un utilisateur est autorisé à générer un challenge dans l'authentification au démarrage (POA) afin de pouvoir accéder de nouveau à son ordinateur avec une procédure Challenge/Réponse.</p> <ul style="list-style-type: none"> ■ OUI : l'utilisateur peut générer un challenge et le bouton Challenge de la POA est actif. Dans ce cas, l'utilisateur peut de nouveau accéder à son ordinateur via une procédure C/R. ■ NON : l'utilisateur n'est pas autorisé à générer un challenge et le bouton Challenge du POA est



Paramètre de stratégie	SGE	ESDP	Explication
			<p>inactif. Dans ce cas, l'utilisateur ne peut pas lancer de procédure C/R pour accéder de nouveau à son ordinateur.</p> <p>Sophos SafeGuard propose également la méthode de récupération de connexion Local Self Help. Elle peut être activée dans le paramètre de stratégie Activer Local Self Help.</p>
Autoriser la connexion Windows automatique	✔	✔	<p>Permet à l'utilisateur de se connecter automatiquement à Windows après authentification avec la procédure Challenge/Réponse.</p> <ul style="list-style-type: none"> ■ OUI : l'utilisateur est automatiquement connecté à Windows. ■ NON : l'écran de connexion Windows apparaît. <p>Exemple : un utilisateur a oublié son mot de passe. Après la procédure de Challenge/Réponse, Sophos SafeGuard connecte l'utilisateur à l'ordinateur sans mot de passe Sophos SafeGuard. Dans ce cas, la connexion automatique à Windows est désactivée et l'écran de connexion Windows s'affiche. L'utilisateur ne peut pas se connecter car il ne connaît pas le mot de passe Sophos SafeGuard (= mot de passe Windows). OUI autorise la connexion automatique ; l'utilisateur n'est pas bloqué au niveau de l'écran de connexion Windows.</p>
Texte d'informations	✔	✔	<p>Affiche un texte d'informations lorsqu'une procédure Challenge/Réponse est lancée dans l'authentification au démarrage. Par exemple : "Contactez le bureau de support en appelant au 01234-56789." Avant d'insérer un texte ici, vous devez le créer sous forme de fichier texte dans la zone de navigation Stratégies sous Texte d'informations.</p>
IMAGES			
			Condition préalable : les nouvelles images doivent être enregistrées dans

Paramètre de stratégie	SGE	ESDP	Explication
			la zone de navigation de stratégie du SafeGuard Policy Editor sous Images . Les images ne sont disponibles qu'une fois enregistrées. Formats pris en charge : .BMP, .PNG, .JPEG.
Image d'arrière-plan dans la POA Image d'arrière-plan dans la POA (faible résolution)	✔	✔	Remplace l'image bitmap bleue d'arrière-plan par l'écran SafeGuard pour l'arrière-plan que vous avez sélectionné. Par exemple, les clients peuvent utiliser le logo de l'entreprise dans la POA et lors de la connexion Windows. Taille de fichier maximale pour toutes les images bitmap d'arrière-plan : 500 Ko Normal : <ul style="list-style-type: none"> ■ Résolution : 1024 x 768 (mode VESA) ■ Couleurs : illimité Basse : <ul style="list-style-type: none"> ■ Résolution : 640 x 480 (mode VGA) ■ Couleurs : 16 couleurs
Image de connexion dans la POA Image de connexion dans la POA (basse résolution)	✔	✔	Change l'image bitmap de Sophos SafeGuard affichée dans la boîte de dialogue de connexion POA. Par exemple, le logo de l'entreprise peut être affiché dans cette boîte de dialogue. Normal : <ul style="list-style-type: none"> ■ Résolution : 413 x 140 pixels ■ Couleurs : illimité Basse : <ul style="list-style-type: none"> ■ Résolution : 413 x 140 pixels ■ Couleurs : 16 couleurs

19.2 Authentification

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

Paramètre de stratégie	SGE	ESDP	Explication
ACCÈS			
Les utilisateurs peuvent initialiser à partir du disque dur uniquement	✔	✔	Détermine si les utilisateurs peuvent démarrer l'ordinateur à partir du disque dur et/ou d'un autre support. OUI : les utilisateurs peuvent initialiser à partir du disque dur uniquement. L'authentification au démarrage (POA) n'offre pas la possibilité de démarrer l'ordinateur avec une disquette ou un autre support externe. NON : les utilisateurs peuvent démarrer l'ordinateur à partir du disque dur, d'une disquette ou d'un support externe (USB, CD, etc.).
OPTIONS DE CONNEXION			
Le mode de connexion	✔	✔ Options disponibles pour ce paramètre : ID utilisateur/Mot de passe Remarque : La connexion par empreinte digitale et par clé cryptographique n'est pas disponible avec ESDP.	Détermine comment un utilisateur doit s'authentifier dans la POA. ■ ID utilisateur/Mot de passe : les utilisateurs doivent se connecter avec leurs noms d'utilisateur et leurs mots de passe. ■ Carte à puce L'utilisateur ne peut se connecter à la POA qu'avec une clé cryptographique ou une carte à puce. Ce processus offre un niveau de sécurité plus élevé. L'utilisateur doit insérer sa clé lors de la connexion. L'identité de l'utilisateur est vérifiée par la possession de la clé et la présentation du code PIN. Après la saisie d'un code PIN correct, SafeGuard Enterprise lit automatiquement les données pour la connexion de l'utilisateur. Remarque : Lorsque ce processus de connexion a été sélectionné, les utilisateurs ne peuvent se connecter qu'en utilisant une clé préalablement générée. Vous pouvez combiner les paramètres ID utilisateur/Mot de passe et Carte à puce . Pour vérifier si la connexion fonctionne en utilisant une clé cryptographique, sélectionnez tout d'abord les deux paramètres. Ne désélectionnez le mode de connexion ID utilisateur/Mot de passe que si

Paramètre de stratégie	SGE	ESDP	Explication
			<p>l'authentification avec la clé cryptographique a réussi. D'autre part, si vous voulez autoriser Local Self Help pour la connexion par carte à puce, vous devez combiner les deux paramètres. Pour plus d'informations, voir Récupération avec Local Self Help à la page 129.</p> <p>■ Empreinte digitale : sélectionnez ce paramètre pour permettre la connexion à l'aide du lecteur d'empreintes digitales Lenovo. Les utilisateurs auxquels cette stratégie s'applique peuvent alors se connecter à l'aide d'une empreinte digitale ou d'un nom d'utilisateur et d'un mot de passe. Cette procédure offre le niveau de sécurité maximum. Lors de la connexion, l'utilisateur fait glisser son doigt sur le lecteur d'empreintes digitales. Lorsque l'empreinte digitale est correctement reconnue, le processus d'authentification au démarrage lit les informations d'identification de l'utilisateur et connecte l'utilisateur à l'authentification au démarrage. Le système transfère alors les codes d'accès vers Windows et connecte l'utilisateur à l'ordinateur.</p> <p>Remarque :</p> <p>Après avoir sélectionné cette procédure de connexion, l'utilisateur peut se connecter uniquement à l'aide d'une empreinte digitale préenregistrée ou d'un nom d'utilisateur et d'un mot de passe.</p>
Options de connexion à l'aide d'une carte à puce			<p>Détermine le type de clé cryptographique ou de carte à puce à utiliser sur l'ordinateur d'extrémité.</p> <p>Non cryptographique :</p> <p>Authentification à la POA et Windows basée sur les informations d'identification utilisateur.</p>
Code PIN utilisé pour la connexion automatique avec une carte à puce			<p>Spécifiez un code PIN par défaut pour autoriser la connexion automatique de l'utilisateur à l'authentification au démarrage à l'aide d'une clé cryptographique ou d'une carte à puce.</p>

Paramètre de stratégie	SGE	ESDP	Explication
			<p>L'utilisateur doit insérer sa clé lors de la connexion et est orienté vers l'authentification au démarrage. Windows démarre.</p> <p>Il n'est pas nécessaire de suivre les règles relatives au code PIN.</p> <p>Remarque :</p> <ul style="list-style-type: none"> ■ Cette option n'est disponible que si vous sélectionnez Carte à puce comme mode de connexion. ■ Si cette option est sélectionnée, Connexion automatique vers Windows doit être défini sur Désactiver la connexion automatique vers Windows.
Afficher les échecs de connexion pour cet utilisateur	✔	✔	<p>Affiche (paramètre : OUI) après la connexion à la POA et Windows une boîte de dialogue indiquant des informations relatives au dernier échec de connexion (nom d'utilisateur/date/heure).</p>
Afficher la dernière connexion utilisateur	✔	✔	<p>Affiche (paramètre : OUI) après la connexion à partir de l'authentification au démarrage ou la connexion à Windows, une boîte de dialogue s'affiche contenant des informations concernant</p> <ul style="list-style-type: none"> ■ la dernière connexion (nom d'utilisateur/date/heure) ; ■ les derniers codes d'accès de l'utilisateur connecté.
Désactiver la "déconnexion forcée" dans le verrouillage du poste de travail	✔	✔	<p>Si l'utilisateur souhaite quitter l'ordinateur d'extrémité pendant une courte durée, il peut cliquer sur Verrouiller le poste de travail pour empêcher d'autres utilisateurs de l'utiliser et le déverrouiller avec le mot de passe utilisateur.</p> <p>Non : l'utilisateur qui a verrouillé l'ordinateur, ainsi qu'un administrateur, peuvent le déverrouiller. Si un administrateur déverrouille l'ordinateur, l'utilisateur connecté est automatiquement déconnecté. Oui : change ce comportement. Dans ce cas, seul l'utilisateur peut déverrouiller l'ordinateur. L'administrateur ne pourra pas le déverrouiller et l'utilisateur ne sera pas déconnecté automatiquement.</p>

Paramètre de stratégie	SGE	ESDP	Explication
			Remarque : ce paramètre ne prend effet que sous Windows XP.
Activer la présélection utilisateur/domaine	✓	✓	<p>Oui : la POA enregistre les nom et domaine du dernier utilisateur connecté. Il n'est donc pas nécessaire que les utilisateurs saisissent leur nom d'utilisateur chaque fois qu'ils se connectent.</p> <p>Non : la POA n'enregistre pas les nom et domaine du dernier utilisateur connecté.</p>
Liste de comptes de service	✓	✓	<p>Pour éviter que les opérations d'administration sur un ordinateur protégé par Sophos SafeGuard n'activent l'authentification au démarrage et n'entraînent l'ajout des opérateurs en charge du déploiement comme autant d'utilisateurs possibles de l'ordinateur, Sophos SafeGuard offre des listes de comptes de service pour les ordinateurs d'extrémité Sophos SafeGuard. Les utilisateurs inclus dans ces listes sont traités comme des utilisateurs invités Sophos SafeGuard.</p> <p>Avant de sélectionner une liste, vous devez créer les listes dans la zone de navigation Stratégies sous Listes de comptes de service.</p>
Authentification automatique à Windows	✓	✓	<p>Remarque :</p> <p>Pour que l'utilisateur puisse autoriser d'autres utilisateurs à accéder à son ordinateur, il doit pouvoir désactiver la connexion automatique vers Windows.</p> <ul style="list-style-type: none"> ■ Laisser l'utilisateur choisir L'utilisateur peut choisir en activant/désactivant cette option dans la boîte de dialogue de connexion POA d'exécuter ou non la connexion automatique à Windows. ■ Appliquer l'authentification automatique à Windows L'utilisateur se connecte toujours automatiquement à Windows. ■ Désactiver l'authentification automatique à Windows

Paramètre de stratégie	SGE	ESDP	Explication
			Après la connexion POA, la boîte de dialogue de connexion Windows s'affiche. L'utilisateur doit se connecter manuellement à Windows.
ÉCHECS DE CONNEXION			
Nbre maximum d'échecs de connexion	✓	✓	Détermine le nombre de tentatives de connexion d'un utilisateur avec un nom d'utilisateur ou un mot de passe non valide. Par exemple, après trois tentatives successives de saisie d'un nom d'utilisateur ou d'un mot de passe incorrect, une quatrième tentative déclenche le paramètre "Réaction aux échecs de connexion".
Messages d'échec de connexion dans la POA	✓	✓	Définit le niveau de détail des messages d'échec de connexion: <ul style="list-style-type: none"> ■ Standard : affiche une brève description. ■ Détaillé : affiche des informations plus détaillées.
Réaction aux échecs de connexion			
Verrouiller la machine	✓	✓	Détermine si l'ordinateur est verrouillé après l'échec de plusieurs tentatives de connexion. Le verrouillage de l'ordinateur peut être levé par un administrateur qui doit réinitialiser l'ordinateur et se connecter. Tenez également compte du verrouillage utilisateur Windows dans ce contexte.
OPTIONS DE CARTE À PUCE			
Action si l'état de connexion à la carte à puce est perdu	✓		Définit le comportement après suppression de la clé cryptographique de l'ordinateur : Les actions possibles sont les suivantes : <ul style="list-style-type: none"> ■ Verrouiller l'ordinateur ■ Présenter la boîte de dialogue PIN ■ Aucune action
Autoriser le déblocage de la carte à puce	✓		Détermine si la clé cryptographique peut être déblocuée lors de la connexion.
OPTIONS DE VERROUILLAGE			

Paramètre de stratégie	SGE	ESDP	Explication
Verrouiller l'écran après X minutes d'inactivité	✔	✔	Détermine le délai à l'issue duquel un bureau inutilisé est automatiquement verrouillé. La valeur par défaut est de 0 minute, auquel cas le bureau n'est pas verrouillé.
Verrouiller l'écran au retrait de la carte à puce	✔		Détermine si l'écran est verrouillé lorsqu'une clé cryptographique est retirée au cours d'une session.
Verrouiller l'écran après mise en veille	✔	✔	Détermine si l'écran est verrouillé lorsque l'ordinateur est réactivé du mode veille.

19.3 Création de listes de codes PIN interdits à utiliser dans les stratégies

Pour les stratégies de type **PIN**, une liste de codes PIN interdits peut être créée afin de définir quelles sont les séquences de caractères à ne pas utiliser dans les codes PIN. Les codes PIN sont utilisés pour la connexion avec la clé cryptographique. Pour plus d'informations, voir [Clés cryptographiques et cartes à puce](#) à la page 120.

Remarque :

Dans les listes, les codes PIN interdits sont séparés par un saut de ligne.

Des fichiers texte contenant les informations requises doivent être créés avant de pouvoir être enregistrés dans le SafeGuard Policy Editor. La taille maximale de ces fichiers texte est de **50 Ko**. Sophos SafeGuard utilise les textes codés en Unicode UTF-16 uniquement. Si vous créez les fichiers texte dans un autre format, ils seront automatiquement convertis lorsqu'ils seront enregistrés.

Pour enregistrer des fichiers texte :

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

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

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

Remarque :

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

19.4 Règles de syntaxe des codes PIN

Dans les stratégies du type **PIN**, vous définissez les paramètres des codes PIN de la carte à puce.

Remarque :





La connexion à l'aide de clés cryptographiques et de cartes à puce n'est pas prise en charge par ESDP (Endpoint Security and Data Protection).

Les codes PIN peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau code PIN, n'utilisez aucun caractère avec la combinaison ALT + < caractère > car ce mode de saisie n'est pas disponible dans l'authentification au démarrage (POA).

Remarque :

Définissez des règles PIN dans le SafeGuard Policy Editor ou dans l'Active Directory, mais pas dans les deux.

Paramètre de stratégie	SGE	ESDP	Explication
RÈGLES			
Longueur min. du code PIN	✔		Spécifie le nombre de caractères que doit contenir un code PIN lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Longueur max. du code PIN	✔		Spécifie le nombre maximum de caractères que doit contenir un code PIN lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Nombre min. de lettres Nombre min. de chiffres Nombre min. de caractères spéciaux	✔		Ces paramètres spécifient qu'un code PIN ne peut pas contenir seulement des lettres, des nombres ou des caractères spéciaux mais doit comporter une combinaison de ces 2 au moins (par exemple, 15fleur, etc.). Ces paramètres ne sont pratiques que si vous avez défini une longueur minimum de code PIN supérieure à 2.

Paramètre de stratégie	SGE	ESDP	Explication
Respecter la casse			<p>Ce paramètre ne s'applique qu'avec Utiliser la liste des codes PIN interdits et Utilisation interdite du nom d'utilisateur comme code PIN.</p> <p>Exemple 1 : vous avez saisi "tableau" dans la liste des codes PIN interdits. Si l'option Respecter la casse est définie sur OUI, les variantes supplémentaires du mot de passe telles que TABLEAU, TableAU ne seront pas acceptées et la connexion sera refusée.</p> <p>Exemple 2 : "EMaier" est saisi comme nom d'utilisateur. Si l'option Respecter la casse est définie sur OUI et si l'option Utilisation interdite du nom d'utilisateur comme PIN est définie sur NON, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple, "emaier" ou "eMaiER") comme mot de passe.</p>
Interdire la succession de touches horizontales			"123" et "aze" sont des exemples de séquences de touches consécutives. Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire la succession de touches verticales			Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple "wqal", "xsZ2" ou "3edc" (mais pas "wse4", "xdr5" ou "cft6"). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme codes PIN. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Au moins 3 caractères consécutifs non autorisés			<p>L'activation de cette option interdit les séquences de touches</p> <ul style="list-style-type: none"> ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant ("abc"; "cba"; ";", etc.). ■ constituées de trois symboles identiques ou plus ("aaa" ou "111").

Paramètre de stratégie	SGE	ESDP	Explication
Utilisation interdite du nom d'utilisateur comme code PIN	✔		<p>Détermine si le nom d'utilisateur et le code PIN peuvent être identiques.</p> <p>OUI : le nom d'utilisateur Windows et le code PIN doivent être différents.</p> <p>NON : l'utilisateur peut utiliser son nom d'utilisateur Windows comme code PIN.</p>
Utiliser la liste des codes PIN interdits	✔		<p>Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les codes PIN. Les séquences de caractères sont stockées dans la liste des codes PIN interdits (par exemple, un fichier .txt).</p>
Liste de PIN non autorisés	✔		<p>Définit les séquences de caractères à ne pas utiliser pour les codes PIN. Si un utilisateur utilise un code PIN non autorisé, un message d'erreur s'affiche.</p> <p>Condition préalable :</p> <p>Une liste (fichier) de codes PIN non autorisés doit être enregistrée dans le Management Center, dans la zone de navigation de stratégie sous Texte d'informations. La liste n'est disponible qu'après l'enregistrement.</p> <p>Taille de fichier maximale : 50 Ko</p> <p>Format pris en charge : Unicode</p> <p>Définition des codes PIN interdits</p> <p>Dans la liste, les codes PIN non autorisés sont séparés par un espace ou un saut de ligne.</p> <p><i>Caractère générique</i> : le caractère générique "*" peut représenter tout caractère et tout nombre de caractères dans un code PIN. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme code PIN.</p> <p>Remarque :</p> <ul style="list-style-type: none"> ■ Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe. ■ Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier.

Paramètre de stratégie	SGE	ESDP	Explication
			<ul style="list-style-type: none"> ■ L'option Utiliser la liste des codes PIN interdits doit être activée.
MODIFICATIONS			
Modification du code PIN après un min. de (jours)	✔		<p>Détermine la période pendant laquelle un mot de passe ne peut être modifié. Ce paramètre empêche l'utilisateur de changer trop souvent de code PIN au cours d'une période donnée.</p> <p>Exemple :</p> <p>L'utilisateur Miller définit un nouveau code PIN (par exemple, "13jk56"). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de changer le code PIN par "13jk56". Le changement de code PIN est refusé car Monsieur Miller ne peut définir un nouveau code PIN qu'après un délai de cinq jours.</p>
Changement de code PIN après un max. de (jours)	✔		<p>Si la période de validité maximum est activée, l'utilisateur doit définir un nouveau code PIN une fois la période définie expirée.</p>
Avertir d'un changement obligatoire avant (jours)	✔		<p>Un message d'avertissement s'affiche "n" jours avant l'expiration du code PIN pour rappeler à l'utilisateur de changer son code PIN dans "n" jours. L'utilisateur peut également le changer immédiatement.</p>
GÉNÉRAL			
Longueur de l'historique du code PIN	✔		<p>Détermine à quel moment des codes PIN déjà utilisés peuvent l'être à nouveau.</p> <p>Il convient de définir la longueur d'historique avec le paramètre Modification du PIN après (jours) max..</p> <p>Exemple :</p> <p>La longueur d'historique du code PIN pour l'utilisateur Miller est définie à 4 et le nombre de jours à l'issue desquels l'utilisateur doit changer son code PIN est de 30. M. Miller se connecte actuellement en utilisant le code PIN</p>

Paramètre de stratégie	SGE	ESDP	Explication
			"Informatik". Lorsque la période de 30 jours expire, il est invité à changer son code PIN. Miller saisit "Informatik" comme nouveau code PIN et reçoit un message d'erreur indiquant que ce code PIN a déjà été utilisé et qu'il doit en sélectionner un nouveau. Miller ne peut pas utiliser le code PIN "Informatik" avant la quatrième invitation de changement du code PIN (en d'autres termes, longueur d'historique du code PIN = 4).

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

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

Remarque :

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

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans le SafeGuard Policy Editor. La taille maximale des fichiers de textes d'informations est de **50 Ko**. Sophos SafeGuard utilise les textes codés en Unicode UTF-16 uniquement. Si vous créez les fichiers texte dans un autre format, ils seront automatiquement convertis lorsqu'ils seront enregistrés.

Pour enregistrer les fichiers texte :

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

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

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

Remarque :

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

19.6 Règles de syntaxe des mots de passe

Dans les stratégies du type **Mot de passe**, vous définissez les règles des mots de passe utilisés pour vous connecter au système.

Les mots de passe peuvent comporter des nombres, des lettres et des caractères spéciaux (par exemple + - ; etc.). Toutefois, lorsque vous générez un nouveau mot de passe, n'utilisez pas de caractère avec la combinaison ALT + < caractère > car ce mode de saisie n'est pas disponible dans l'authentification au démarrage (POA).

Remarque :

Définissez des règles de mot de passe dans le SafeGuard Policy Editor ou dans l'Active Directory, mais pas dans les deux.

Paramètre de stratégie	SGE	ESDP	Explication
RÈGLES			
Longueur min. du mot de passe	✓	✓	Spécifie le nombre de caractères que doit contenir un mot de passe lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Longueur max. du mot de passe	✓	✓	Spécifie le nombre maximum de caractères que doit contenir un mot de passe lorsque l'utilisateur en change. La valeur requise peut être saisie directement ou augmentée/réduite à l'aide des touches fléchées.
Nombre min. de lettres Nombre min. de chiffres Nombre min. de caractères spéciaux	✓	✓	Ces paramètres spécifient qu'un mot de passe ne peut pas contenir seulement des lettres, des nombres ou des caractères spéciaux mais doit comporter une combinaison de ces 2 au moins (par ex. 15fleur, etc.). Ces paramètres ne sont pratiques que si vous avez défini une longueur minimum de mot de passe supérieure à 2.
Respecter la casse	✓	✓	Ce paramètre ne s'applique qu'avec Utiliser la liste des mots de passe interdits et Utilisation interdite du nom d'utilisateur comme mot de passe . Exemple 1 : Vous avez saisi « tableau » dans la liste des mots de passe interdits.

Paramètre de stratégie	SGE	ESDP	Explication
			<p>Si l'option Respecter la casse est définie sur OUI, les variantes supplémentaires du mot de passe telles que TABLEAU ou TableAU ne seront pas acceptées et la connexion sera refusée.</p> <p>Exemple 2 : "EMaier" est saisi comme nom d'utilisateur. Si l'option Respecter la casse est définie sur OUI et si l'option Utilisation interdite du nom d'utilisateur comme mot de passe est définie sur NON, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple, «emaier» ou «eMaiER») comme mot de passe.</p>
Interdire la succession de touches horizontales	✔	✔	Les séquences de touches consécutives sont, par exemple "123" ou "aze". Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Interdire la succession de touches verticales	✔	✔	Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple "wqal", "xs22" ou "3edc" (mais pas "wse4", "xdr5" ou "cft6"). Un maximum de deux symboles adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mot de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.
Au moins 3 caractères consécutifs non autorisés	✔	✔	<p>L'activation de cette option interdit les séquences de touches.</p> <ul style="list-style-type: none"> ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant ("abc"; "cba"; "<" etc.). ■ constituées de trois symboles identiques ou plus ("aaa" ou "111").
Utilisation interdite du nom d'utilisateur comme mot de passe	✔	✔	<p>Détermine si le nom d'utilisateur et le mot de passe peuvent être identiques.</p> <p>Oui : le nom d'utilisateur Windows et le mot de passe doivent être différents.</p>

Paramètre de stratégie	SGE	ESDP	Explication
			Non : l'utilisateur peut utiliser son nom d'utilisateur Windows comme mot de passe.
Utiliser la liste de mots de passe interdits	✔	✔	Détermine si certaines séquences de caractères ne doivent pas être utilisées pour les mots de passe. Les séquences de caractères sont stockées dans la liste des mots de passe interdits (par exemple, un fichier .txt).
Liste de mots de passe interdits	✔	✔	<p>Définit les séquences de caractères à ne pas utiliser pour les mots de passe. Si un utilisateur utilise un mot de passe non autorisé, un message d'erreur s'affiche.</p> <p>Conditions préalables importantes :</p> <p>Une liste (fichier) de mots de passe non autorisés doit être enregistrée dans le SafeGuard Policy Editor, dans la zone de navigation de stratégie sous Texte d'informations. La liste n'est disponible qu'après l'enregistrement.</p> <p>Taille de fichier maximale : 50 Ko</p> <p>Format pris en charge : Unicode</p> <p>Définition de mots de passe interdits</p> <p>Dans la liste, les mots de passe non autorisés sont séparés par un saut de ligne. Caractère générique : Le caractère générique "*" peut représenter tout caractère et tout nombre de caractères dans un mot de passe. Par exemple, *123* signifie que toute séquence de caractères contenant 123 sera interdite comme mot de passe.</p> <ul style="list-style-type: none"> ■ Si la liste ne contient qu'un seul caractère générique, l'utilisateur ne sera plus en mesure de se connecter au système après un changement obligatoire de mot de passe. ■ Les utilisateurs ne doivent pas être autorisés à accéder à ce fichier. ■ L'option Utiliser la liste des mots de passe interdits doit être activée.
MODIFICATIONS			

Paramètre de stratégie	SGE	ESDP	Explication
Modification du mot de passe autorisée après un min. de (jours)	✔	✔	<p>Détermine la période pendant laquelle un mot de passe ne peut être modifié. Ce paramètre empêche l'utilisateur de changer trop souvent de mot de passe au cours d'une période donnée.</p> <p>Exemple :</p> <p>L'utilisateur Miller définit un nouveau mot de passe (par exemple, "13jk56"). L'intervalle minimum de changement pour cet utilisateur (ou pour le groupe auquel il appartient) est défini à cinq jours. Après deux jours seulement, l'utilisateur décide de remplacer le code PIN par "74jk56". Le changement de mot de passe est refusé car l'utilisateur Miller ne peut définir un nouveau mot de passe qu'après un délai de cinq jours.</p>
Expiration du mot de passe après (jours)	✔	✔	<p>Si la période de validité maximum est activée, l'utilisateur doit définir un nouveau mot de passe une fois la période définie expirée.</p>
Avertir d'un changement obligatoire avant (jours)	✔	✔	<p>Un message d'avertissement s'affiche "n" jours avant l'expiration du mot de passe pour rappeler à l'utilisateur de changer son mot de passe dans "n" jours. L'utilisateur peut également le changer immédiatement.</p>
GÉNÉRAL			
Longueur de l'historique de mot de passe	✔	✔	<p>Détermine à quel moment des mots de passe déjà utilisés peuvent l'être à nouveau. Il est judicieux de définir la longueur d'historique conjointement au paramètre Expiration du mot de passe après (jours).</p> <p>Exemple :</p> <p>La longueur d'historique du mot de passe pour l'utilisateur Miller est définie à 4 et le nombre de jours à l'issue desquels l'utilisateur doit changer son mot de passe est de 30. M.Miller se connecte actuellement en utilisant le mot de passe "Informatik". Lorsque la période de 30 jours expire, il est invité à modifier son mot de passe. M. Miller saisit "Informatik" comme nouveau mot de passe et reçoit un message d'erreur indiquant que ce mot de passe a déjà été</p>

Paramètre de stratégie	SGE	ESDP	Explication
			utilisé et qu'il doit en sélectionner un nouveau. M. Miller ne peut pas utiliser le mot de passe "Informatik" avant la quatrième invitation de changement du mot de passe (en d'autres termes, longueur d'historique du mot de passe = 4).

19.7 Règles de phrase de passe pour SafeGuard Data Exchange

Remarque : ces paramètres ne sont pas pris en charge par ESDP (Endpoint Security and Data Protection). Pour une description de SafeGuard Data Exchange, [voir SafeGuard Data Exchange](#) à la page 125.

L'utilisateur doit entrer une phrase de passe qui est utilisée pour générer des clés locales pour un échange sécurisé des données dans SafeGuard Data Exchange. Dans les stratégies du type **Phrase de passe**, vous définissez les conditions requises correspondantes.

Pour plus d'informations sur SafeGuard Data Exchange, [voir SafeGuard Data Exchange](#) à la page 125.

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

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

Paramètre de stratégie	SGE	ESDP	Explication
Respecter la casse	✔		<p>Ce paramètre est effectif lorsque l'option Utilisation interdite du nom d'utilisateur comme phrase de passe est active.</p> <p>Exemple : "EMaier" est saisi comme nom d'utilisateur. Si l'option Respecter la casse est définie sur OUI et si Utilisation interdite du nom d'utilisateur comme phrase de passe est définie sur NON, l'utilisateur EMaier ne peut utiliser aucune variante de ce nom d'utilisateur (par exemple, emaiier ou eMaiER) comme phrase de passe.</p>
Interdire la succession de touches horizontales	✔		<p>Les séquences de touches consécutives sont, par exemple "123" ou "aze". Un maximum de deux caractères adjacents du clavier est autorisé. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.</p>
Interdire la succession de touches verticales	✔		<p>Concerne les touches disposées consécutivement en colonne sur le clavier, par exemple "wqal", "xs22" ou "3edc" (mais pas "wse4", "xdr5" ou "cft6"). Un maximum de deux caractères adjacents d'une même colonne clavier est autorisé. Si vous n'autorisez pas les colonnes du clavier, ces combinaisons sont rejetées comme mots de passe. Les séquences de touches consécutives ne concernent que la zone du clavier alphanumérique.</p>
Au moins 3 caractères consécutifs non autorisés	✔		<p>L'activation de cette option interdit les séquences de touches</p> <ul style="list-style-type: none"> ■ qui sont des séries consécutives de symboles de code ASCII, que ce soit par ordre croissant ou décroissant ("abc"; "cba"; "<" etc.). ■ constituées de trois symboles identiques ou plus ("aaa" ou "111").
Utilisation interdite du nom d'utilisateur comme phrase de passe	✔		<p>Détermine si le nom d'utilisateur et la phrase de passe peuvent être identiques.</p> <p>OUI : le nom d'utilisateur Windows et la phrase de passe doivent être différents.</p>

Paramètre de stratégie	SGE	ESDP	Explication
			NON : l'utilisateur peut utiliser son nom d'utilisateur Windows comme phrase de passe.

19.8 Protection des périphériques

La fonction principale de Sophos SafeGuard est le chiffrement des données sur différents périphériques de stockage de données. Le chiffrement peut être basé sur volume ou sur fichier avec des clés et des algorithmes différents. Dans des stratégies du type **Protection du périphérique**, vous définissez les paramètres pour le chiffrement des données sur différents périphériques de stockage des données. Ces stratégies incluent également des paramètres pour SafeGuard Data Exchange et SafeGuard Portable. Pour plus d'informations, voir [SafeGuard Data Exchange](#) à la page 125. Pour plus d'informations sur SafeGuard Data Exchange et sur SafeGuard Portable sur l'ordinateur d'extrémité, consultez l'aide utilisateur de Sophos SafeGuard, chapitre *SafeGuard Data Exchange*.

Remarque :

SafeGuard Data Exchange, SafeGuard Portable et le chiffrement basé sur fichier ne sont pas pris en charge par ESDP.

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

- Le stockage de masse (volumes d'initialisation/autres volumes)
- Les supports amovibles (non pris en charge par les installations avec ESDP).
- Les lecteurs optiques (non pris en charge par les installations avec ESDP).


Pour chaque cible, créez une stratégie distincte.

Paramètre de stratégie	SGE	ESDP	Description
Mode de chiffrement du support	✔	✔	<p>Permet de protéger les périphériques (PC, ordinateurs portables) ainsi que tous types de supports amovibles.</p> <p>L'objectif essentiel consiste à chiffrer toutes les données stockées sur des périphériques de stockage locaux ou externes. La méthode de fonctionnement transparente permet aux utilisateurs de continuer à utiliser leurs applications courantes, par exemple Microsoft Office.</p> <p>Le chiffrement transparent signifie que toutes les données chiffrées (dans</p>
		<p>Options disponibles pour ce paramètre :</p> <ul style="list-style-type: none"> ■ Aucun chiffrement ■ Basé sur volume <p>Remarque :</p>	

Paramètre de stratégie	SGE	ESDP	Description
		Les paramètres basés sur fichier ne sont pas disponibles avec ESDP.	des répertoires ou dans des volumes chiffrés) sont automatiquement déchiffrés dans la mémoire principale dès qu'elles sont ouvertes dans un programme. Un fichier est automatiquement chiffré de nouveau lorsqu'il est enregistré.
			<p>Les options suivantes sont disponibles :</p> <ul style="list-style-type: none"> ■ Aucun chiffrement ■ Basé sur volume (= chiffrement transparent basé sur secteur) <p>Garantit que toutes les données sont chiffrées (y compris les fichiers d'initialisation, les fichiers d'échange, les fichiers inactifs/d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sans que l'utilisateur doive modifier ses habitudes de travail ou tenir compte de problèmes de sécurité.</p> <p>Pour plus d'informations, voir Chiffrement basé sur volume à la page 10.</p> ■ Basé sur fichier (= chiffrement transparent basé sur fichier (Chiffrement Smart Media)) <p>Garantit que toutes les données sont chiffrées (à l'exception du support d'initialisation et des informations de répertoire) avec l'avantage que même les supports optiques tels que les CD/DVD peuvent être chiffrés et que les données peuvent être échangées avec des ordinateurs externes sur lesquels SafeGuard n'est pas installé (si les stratégies l'autorisent).</p> <p>Pour plus d'informations, voir Chiffrement basé sur fichier à la page 12.</p>
PARAMÈTRES GÉNÉRAUX			

Paramètre de stratégie	SGE	ESDP	Description
Algorithme à utiliser pour le chiffrement	✔	✔	Définit l'algorithme de chiffrement. Liste des algorithmes utilisables avec les normes respectives : AES256 : 32 octets (256 bits) AES128 : 16 octets (128 bits)
Clé à utiliser pour le chiffrement	✔	✔	Définit la clé utilisée pour le chiffrement. Pour le chiffrement Sophos SafeGuard, seule une clé machine générée automatiquement est utilisée pour le chiffrement basé sur volume. Pour le chiffrement basé sur fichier, seules les clés locales créées par l'utilisateur peuvent être utilisées. L'option suivante est disponible : Clé machine définie : la clé de la machine est utilisée ; l'utilisateur ne peut PAS sélectionner de clé.
L'utilisateur est autorisé à créer une clé locale	✔		Ce paramètre détermine si l'utilisateur peut générer ou non une clé locale sur son ordinateur. Les clés locales sont générées sur l'ordinateur d'extrémité selon une phrase de passe saisie par l'utilisateur. La configuration minimale de la phrase de passe est définie dans des stratégies du type phrase de passe . Remarque : Dans la mesure où seules les clés locales sont utilisées pour le chiffrement basé sur fichier, l'utilisateur doit pouvoir créer des clés locales si des stratégies de chiffrement basé sur fichier s'appliquent. Les clés locales ne sont pas sauvegardées et ne peuvent pas être utilisées pour la récupération. Seule la clé machine définie peut être utilisée dans ce cas. Le paramètre par défaut de ce champ (non configuré) permet à l'utilisateur de créer des clés locales.
PARAMÈTRES BASÉS SUR VOLUME			

Paramètre de stratégie	SGE	ESDP	Description
L'utilisateur peut ajouter des clés au volume chiffré ou en supprimer	✔		<p>OUI : les utilisateurs de Sophos SafeGuard peuvent ajouter ou supprimer des clés d'un jeu de clés. La boîte de dialogue s'affiche dans l'onglet Chiffrement/Chiffrement de la commande du menu contextuel.</p> <p>NON : les utilisateurs de Sophos SafeGuard ne peuvent pas ajouter de clés.</p>
Réaction aux volumes non chiffrés	✔	✔	<p>Définit de quelle manière Sophos SafeGuard gère les supports non chiffrés.</p> <p>Les options suivantes sont disponibles :</p> <ul style="list-style-type: none"> ■ Rejeter (= le support en texte n'est pas chiffré) ■ N'accepter que les supports vierges et chiffrer ■ Accepter tous les supports et chiffrer
L'utilisateur peut déchiffrer un volume	✔	✔	Permet à l'utilisateur Sophos SafeGuard de déchiffrer le volume avec une commande du menu contextuel dans l'Explorateur Windows.
Chiffrement initial rapide	✔	✔	<p>Sélectionnez ce paramètre pour activer le mode de chiffrement initial rapide pour le chiffrement basé sur volume. Ce mode réduit le temps nécessaire pour le chiffrement initial sur les ordinateurs d'extrémité.</p> <p>Remarque :</p> <p>Ce mode peut conduire à un état moins sécurisé.</p> <p>Pour plus d'informations, voir Chiffrement initial rapide à la page 10.</p>
Poursuivre sur les secteurs incorrects	✔	✔	Indique si le chiffrement doit se poursuivre ou être arrêté si des secteurs incorrects sont détectés. Le paramètre par défaut est OUI .
PARAMETRES SUR FICHER			

Paramètre de stratégie	SGE	ESDP	Description
Chiffrement initial de tous les fichiers			Démarre automatiquement le chiffrement initial d'un volume après la connexion de l'utilisateur. Il se peut que l'utilisateur doive sélectionner une clé du jeu de clés au préalable.
L'utilisateur peut annuler le chiffrement initial			Permet à l'utilisateur d'annuler le chiffrement initial.
L'utilisateur n'est pas autorisé à accéder aux fichiers non chiffrés			Définit si un utilisateur peut accéder aux données non chiffrées d'un volume.
L'utilisateur peut déchiffrer des fichiers			Permet à un utilisateur de déchiffrer des fichiers individuels ou des répertoires entiers (avec l'extension de l'Explorateur Windows < clic droit>).
L'utilisateur peut définir une phrase de passe de support pour les périphériques			Permet à l'utilisateur de définir une phrase de passe de support sur son ordinateur. La phrase de passe de support permet d'accéder facilement à l'aide de SafeGuard Portable à toutes les clés locales utilisées sur des ordinateurs sur lesquels SafeGuard Data Exchange n'est pas installé.
Applications non gérées			<p>Permet de définir d'autres applications devant être ignorées par le pilote du filtre SafeGuard Enterprise et devant être exclues du chiffrement/déchiffrement transparent. Pour plus d'informations, voir Exclusion d'applications du chiffrement à la page 13.</p> <p>Utilisez le nom complet du fichier exécutable (en incluant facultativement les informations du chemin) pour spécifier une application exemptée. Le séparateur à utiliser pour ces applications est ';'.</p> <p>Remarque : comme il s'agit de paramètres spécifiques à la machine, ils ne sont appliqués que lorsque l'ordinateur d'extrémité est redémarré.</p>

Paramètre de stratégie	SGE	ESDP	Description
			<p>Remarque :</p> <p>Des applications non gérées ne peuvent être définies que pour des périphériques de stockage locaux. Pour une stratégie globale du type Protection du périphérique, la cible Périphériques de stockage locaux doit être sélectionnée. Pour toutes les autres cibles, l'option Applications non gérées n'est pas disponible.</p>
<p>Supports amovibles uniquement</p> <p>Copier SG Portable vers support amovible</p>	✔		<p>Si cette option est activée, SafeGuard Portable est copié sur tous les supports amovibles connectés à l'ordinateur d'extrémité.</p> <p>SafeGuard Portable permet l'échange des données chiffrées avec le support amovible sans que Sophos SafeGuard ne soit installé sur le destinataire.</p> <p>Le destinataire peut déchiffrer et rechiffrer les fichiers chiffrés en utilisant SafeGuard Portable et le mot de passe correspondant. Le destinataire peut rechiffrer les fichiers avec SafeGuard Portable ou utiliser la clé d'origine pour le chiffrement.</p> <p>Il n'est pas nécessaire que SafeGuard Portable soit installé ou copié sur l'ordinateur du destinataire, il peut être utilisé directement à partir du support amovible.</p>
Dossier en texte brut	✔		<p>Le dossier spécifié ici sera créé sur tous les supports amovibles et périphériques de stockage de masse. Les fichiers copiés dans ce dossier restent au format brut.</p>
L'utilisateur est autorisé à décider de l'opération de chiffrement	✔		<p>Avec ce paramètre de stratégie, vous pouvez autoriser l'utilisateur à décider du chiffrement des fichiers sur les supports amovibles et sur les périphériques de stockage de masse. Si vous définissez cette option sur Oui, les utilisateurs sont invités à décider si les données doivent être chiffrées lorsqu'ils branchent des supports amovibles. Si l'utilisateur</p>

Paramètre de stratégie	SGE	ESDP	Description
			sélectionne Non , ni le chiffrement initial ni le transparent n'a lieu.

19.9 Paramètres spécifiques à la machine - Paramètres de base


Paramètre de stratégie	SGE	ESDP	Explication
AUTHENTIFICATION AU DÉMARRAGE (POA)			
Activer l'authentification au démarrage	✔	✔	Définit si la POA est activée ou désactivée en permanence. Remarque : Pour des raisons de sécurité, nous vous recommandons fortement de laisser active l'authentification au démarrage. La désactivation de l'authentification au démarrage réduit la sécurité du système lors des connexions Windows et accroît le risque d'accès non autorisés aux données chiffrées.
Interdire l'utilisateur invité	✔	✔	Définit si les utilisateurs invités peuvent se connecter à Windows sur l'ordinateur d'extrémité.
Éveil par appel réseau sécurisé (WOL)	✔	✔	Les paramètres Éveil par appel réseau sécurisé (WOL) permettent aux ordinateurs d'extrémité de se préparer aux déploiements de logiciels dans lesquels les paramètres nécessaires tels que la désactivation temporaire de la POA et un intervalle d'éveil par appel réseau peuvent être importés directement dans l'ordinateur d'extrémité et analysés par celui-ci. Remarque : La désactivation de la POA (même pour un nombre limité de processus d'initialisation) réduit le niveau de sécurité de votre système ! Pour plus d'informations sur l'éveil par appel réseau, voir Éveil par appel réseau sécurisé (WOL) à la page 118.


Paramètre de stratégie	SGE	ESDP	Explication
Nombre de connexions automatiques	✔	✔	<p>Définit le nombre de redémarrages lorsque l'authentification au démarrage est inactive pour l'éveil par appel réseau.</p> <p>Ce paramètre remplace temporairement le paramètre Activer l'authentification au démarrage jusqu'à ce que le nombre prédéfini de connexions automatiques soit atteint. L'authentification au démarrage est ensuite réactivée. Exemple : le nombre de connexions automatiques est défini sur deux, "Activer l'authentification au démarrage" est activé. L'ordinateur démarre deux fois sans authentification via la POA.</p> <p>Pour le mode Éveil par appel réseau, nous recommandons de toujours autoriser trois redémarrages de plus que nécessaire pour faire face aux problèmes imprévus.</p>
Connexion à Windows autorisée pendant le WOL	✔	✔	<p>Détermine si la connexion Windows est autorisée pendant l'éveil par appel réseau, par exemple pour une mise à jour de logiciel. Ce paramètre est analysé par la POA.</p>
Début de la plage horaire pour le lancement du WOL externe Fin de la plage horaire pour le lancement du WOL externe	✔	✔	<p>La date et l'heure peuvent être sélectionnées ou saisies pour le début et la fin de l'éveil par appel réseau (WOL).</p> <p>Format de date : <i>MM/JJ/AAAA</i> Format d'heure : <i>HH:MM</i></p> <p>Les combinaisons suivantes de saisie sont possibles :</p> <ul style="list-style-type: none"> ■ début et fin de l'éveil par appel réseau définis ; ■ fin de l'éveil par appel réseau définie, début ouvert ; ■ Aucune entrée : aucun intervalle n'a été défini pour l'ordinateur d'extrémité. <p>Pour un déploiement planifié de logiciels, le responsable de la sécurité doit définir la plage de l'éveil par appel réseau de sorte que le script de programmation puisse démarrer</p>

Paramètre de stratégie	SGE	ESDP	Explication
			<p>suffisamment tôt pour que les ordinateurs d'extrémité aient le temps de s'initialiser.</p> <p>WOLstart (Début WOL) : le point de départ de l'éveil par appel réseau dans le script de programmation doit se trouver dans l'intervalle défini dans la stratégie. Si aucun intervalle n'est défini, l'éveil par appel réseau n'est pas activé localement sur l'ordinateur d'extrémité Sophos SafeGuard.</p> <p>WOLstop (Fin WOL) : cette commande s'effectue quel que soit le point d'extrémité défini pour l'éveil par appel réseau.</p>
OPTIONS D'AFFICHAGE			
Afficher l'identification de la machine	✔	✔	<p>Affiche le nom de l'ordinateur ou un texte défini dans la barre de titre de la POA.</p> <p>Si les paramètres réseau de Windows incluent le nom de l'ordinateur, ce dernier est automatiquement intégré aux paramètres de base.</p>
Texte d'identification de la machine	✔	✔	<p>Le texte à afficher dans la barre de titre de la POA.</p> <p>Si vous avez sélectionné Nom défini dans le champ Afficher l'identification de la machine, vous pouvez entrer le texte dans ce champ de saisie.</p>
Afficher la mention légale	✔	✔	<p>Affiche une zone de texte avec du contenu configurable qui apparaît avant l'authentification dans la POA. Dans certains pays, la loi exige l'affichage d'une zone de texte ayant un certain contenu.</p> <p>L'utilisateur doit confirmer la zone de texte avant que le système ne continue.</p> <p>Avant de spécifier un texte, ce dernier doit être enregistré en tant qu'élément de texte sous Texte d'informations dans la zone de navigation de stratégie.</p>

Paramètre de stratégie	SGE	ESDP	Explication
Texte de la mention légale	✓	✓	Le texte à afficher en tant que mention légale. Dans ce champ, vous pouvez sélectionner un élément de texte enregistré dans Texte d'informations dans la zone de navigation de stratégie.
Afficher des infos supplémentaires	✓	✓	Affiche une zone de texte avec un contenu pouvant être configuré qui apparaît après la mention légale (si elle est activée). Vous pouvez définir si les informations supplémentaires doivent être affichées: <ul style="list-style-type: none"> ■ Jamais ■ À chaque démarrage système ■ À chaque connexion
Texte des informations supplémentaires	✓	✓	Le texte à afficher en tant qu'informations supplémentaires. Dans ce champ, vous pouvez sélectionner un élément de texte enregistré dans Texte d'informations dans la zone de navigation de stratégie .
Afficher pendant (s)	✓	✓	Dans ce champ, vous pouvez définir la durée (en secondes) pendant laquelle les informations supplémentaires doivent être affichées. Vous pouvez spécifier le nombre de secondes après lesquelles la zone de texte d'informations supplémentaires est fermée automatiquement. L'utilisateur peut fermer la zone de texte à tout moment en cliquant sur OK .
Activer et afficher l'icône de la barre d'état système	✓	✓	Grâce à l'icône de la barre d'état système de Sophos SafeGuard, l'utilisateur peut accéder rapidement et facilement à l'ensemble des fonctions de son ordinateur. En outre, des informations concernant l'état de Sophos SafeGuard (nouvelles stratégies reçues, ...) peuvent être affichées dans des infobulles. Oui :

Paramètre de stratégie	SGE	ESDP	Explication
			<p>L'icône de la barre d'état système est affichée dans la zone d'information de la barre des tâches et l'utilisateur est continuellement informé sur l'état du client dans les infobulles.</p> <p>Non : l'icône de la barre d'état système n'apparaît pas. Aucune information d'état n'est affichée via l'infobulle.</p> <p>Muet :</p> <p>l'icône de la barre d'état système est affichée dans la zone d'information de la barre des tâches mais aucune information d'état n'est affichée dans les infobulles.</p>
Afficher les icônes en chevauchement dans l'Explorateur	✓	✓	Définit si des symboles de clé Windows s'affichent pour indiquer l'état de chiffrement des volumes, périphériques, dossiers et fichiers.
Clavier virtuel en POA	✓	✓	Définit si un clavier virtuel peut être affiché sur demande dans la boîte de dialogue POA pour la saisie du mot de passe.
OPTIONS D'INSTALLATION			
Désinstallation autorisée	✓	✓	Détermine si la désinstallation de Sophos SafeGuard est autorisée sur les ordinateurs d'extrémité. Lorsque l'option Désinstallation autorisée est définie sur Non , Sophos SafeGuard ne peut pas être désinstallé, même par un utilisateur avec les droits d'administrateur, lorsque ce paramètre est actif au sein d'une stratégie.
Activer la protection antialtération Sophos	✓	✓	<p>Active/désactive la protection antialtération Sophos. Si vous avez autorisé la désinstallation de Sophos SafeGuard dans le paramètre de stratégie Désinstallation autorisée, vous pouvez définir ce paramètre de stratégie sur Oui, pour garantir que les tentatives de désinstallation sont vérifiées par la protection antialtération Sophos et empêcher la suppression accidentelle du logiciel.</p> <p>Si la protection antialtération Sophos n'autorise pas la désinstallation, les</p>

Paramètre de stratégie	SGE	ESDP	Explication
			<p>tentatives de désinstallation seront annulées.</p> <p>Si l'option Activer la protection antialtération Sophos est définie sur Non, la désinstallation de Sophos SafeGuard ne sera pas vérifiée ou empêchée par la protection antialtération Sophos.</p> <p>Remarque : ce paramètre ne s'applique qu'aux ordinateurs d'extrémité utilisant Sophos Endpoint Security and Control version 9.5 ou ultérieure.</p>
PARAMÈTRES DE SUPPORT DE CLÉ CRYPTOGRAPHIQUE POUR LE MODULE1 PKCS#11			
Nom du module			<p>Enregistre le module PKCS#11 d'une clé cryptographique.</p> <p>Les options suivantes sont disponibles :</p> <ul style="list-style-type: none"> ■ ActiveIdentity ActivClient ■ ActiveIdentity ActivClient (PIV) ■ AET SafeSign Identity Client ■ Aladdin eToken PKI Client ■ a.sign Client ■ Charismathics Smart Security Interface ■ Estonian ID-Card ■ Gemalto Access Client ■ Gemalto Classic Client ■ Gemalto .NET Card ■ IT Solution trustWare CSP+ ■ RSA Authentication Client 2.x ■ RSA Smart Card Middleware 3.x ■ Siemens CardOS API ■ T-Systems NetKey 3.0 ■ Unizeto proCertum <p>Informations de licence pour Siemens et Charismathics :</p> <p>Sachez que l'utilisation des middlewares respectifs pour le système</p>

Paramètre de stratégie	SGE	ESDP	Explication
			<p>d'exploitation standard requiert un accord de licence avec Siemens IT Solutions and Services GmbH/Charismatics. Pour obtenir les licences, veuillez vous renseigner auprès de :</p> <ul style="list-style-type: none"> ■ Siemens IT Solutions und Services GmbH Otto-Hahn-Ring 6 D-81739 München Allemagne ■ http://www.charismatics.com/typo3/stop_content.php ou sales@charismatics.com
Services en attente de			Ce paramètre permet de résoudre les problèmes de certaines cartes à puce. Notre support fournira les paramètres correspondants requis.

19.10 Journalisation

Les événements Sophos SafeGuard sont journalisés dans l'Observateur d'événements Windows. Pour indiquer les événements à journaliser dans l'Observateur d'événements Windows, créez une stratégie du type **Journalisation**, puis sélectionnez les événements souhaités d'un simple clic.

Vous pouvez sélectionner plusieurs types d'événements, de catégories différentes (par exemple authentification, chiffrement, etc.). Nous vous recommandons de définir une stratégie pour la journalisation et de déterminer quels sont les événements nécessaires, en fonction de vos exigences en matière de rapports et d'audits.

20 Authentification au démarrage (POA)

Sophos SafeGuard identifie l'utilisateur avant même le démarrage du système d'exploitation. Pour ce faire, le noyau du système de Sophos SafeGuard démarre en amont. Il est protégé contre toute modification puis il est enregistré et masqué sur le disque dur. Lorsque l'utilisateur est correctement authentifié dans l'authentification au démarrage, seul le système d'exploitation effectif (Windows) est lancé depuis la partition chiffrée. L'utilisateur est connecté automatiquement à Windows. La procédure est identique lorsque l'ordinateur d'extrémité revient du mode hibernation.



L'authentification au démarrage de Sophos SafeGuard offre :

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

20.1 Retard de connexion

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

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

20.2 Verrouillage de la machine

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

20.3 Configuration de l'authentification au démarrage

La boîte de dialogue POA comporte les composants suivants :

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



Vous pouvez modifier l'apparence de la boîte de dialogue POA selon vos préférences à l'aide des paramètres de stratégie du SafeGuard Policy Editor.

20.3.1 Image d'arrière-plan et de connexion

Par défaut, les images d'arrière-plan et de connexion qui s'affichent dans l'authentification au démarrage sont conçues selon SafeGuard. Toutefois, il est possible d'afficher des images différentes telles que le logo de l'entreprise.

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

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

Image d'arrière-plan

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

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

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

Couleurs : aucune restriction

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

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

Couleurs : 16

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

Image de connexion

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

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

- **413 x 140**

Couleurs : aucune restriction

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

- **413 x 140**

Couleurs : 16

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

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

20.3.1.1 Enregistrement d'images

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

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

Répétez la procédure pour enregistrer d'autres images. Toutes les images enregistrées s'affichent sous la forme de nœuds secondaires.

Remarque :

Vous pouvez utiliser le bouton **Modifier l'image** pour changer l'image attribuée.

20.3.2 Texte d'informations défini par l'utilisateur dans l'authentification au démarrage (POA)

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

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

Vous pouvez définir un texte de mention légale en utilisant l'option **Texte d'informations** dans la stratégie du type **Paramètres généraux**

- Mentions légales affichées après la connexion à la POA

Vous pouvez définir un texte d'informations en utilisant l'option **Texte de la mention légale** dans la stratégie du type **Paramètres de machine spécifiques**

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

Vous pouvez définir un texte d'informations supplémentaires en utilisant l'option **Texte d'informations supplémentaires** dans la stratégie du type **Paramètres de machine spécifiques**

20.3.2.1 Enregistrement des textes d'informations

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans le SafeGuard Policy Editor. La taille maximale des fichiers de textes d'informations est de **50 Ko**. Sophos SafeGuard utilise les textes codés en Unicode UTF-16 uniquement. Si vous ne créez pas les fichiers texte dans un ce format, ils seront automatiquement convertis lorsqu'ils seront enregistrés. Les caractères spéciaux doivent par conséquent être utilisés avec prudence dans le texte de mention légale pour la POA. Il est possible que certains de ces caractères n'apparaissent pas correctement.

Pour enregistrer des textes d'informations :

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

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

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

Remarque :

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

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

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

Vous pouvez changer la langue du texte de la boîte de dialogue d'authentification au démarrage après l'installation de Sophos SafeGuard à l'aide de l'une des deux méthodes suivantes :

- Changez la langue par défaut dans les Options régionales et linguistiques Windows sur l'ordinateur d'extrémité. Après deux redémarrages de l'ordinateur par l'utilisateur, le nouveau paramètre de langue est actif dans la POA.
- Créez une stratégie du type **Paramètres généraux**, choisissez la langue dans le champ **Langue utilisée sur le client** et déployez la stratégie sur l'ordinateur d'extrémité.

Remarque : si vous définissez une stratégie et la déployez sur l'ordinateur d'extrémité, la langue choisie dans la stratégie s'applique au lieu de celle spécifiée dans les Options régionales et linguistiques de Windows.

20.3.4 Disposition du clavier

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

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

La langue de la disposition de clavier utilisée est affichée dans l'authentification au démarrage, par exemple "FR" pour français. Outre la disposition du clavier par défaut, la disposition du clavier américain (anglais) peut également être utilisée.

Il existe un certain nombre d'exceptions :

- La disposition du clavier est effectivement prise en charge, mais l'absence d'une police de caractères (par exemple, Bulgare) signifie que seuls les caractères spéciaux sont affichés dans le champ **Nom d'utilisateur**.
- Aucune disposition du clavier n'est disponible (par exemple, pour la République Dominicaine). Dans ces situations, la POA revient à la disposition de clavier d'origine. Pour la République Dominicaine, il s'agit de l'"espagnol".
- Lorsque le nom utilisateur et le mot de passe comportent des caractères non reconnus par la disposition de clavier choisie ou par celle de secours, l'utilisateur ne peut pas se connecter à la POA.

Remarque :

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

Clavier virtuel

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

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

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

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

20.3.4.1 Modification de la disposition du clavier

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

1. Sélectionnez **Démarrer > Panneau de configuration > Options régionales et linguistiques > Options avancées**.
2. Dans l'onglet **Options régionales**, sélectionnez la langue souhaitée.
3. Dans l'onglet **Options avancées**, sélectionnez **Appliquer tous les paramètres au compte d'utilisateur actuel et au profil utilisateur par défaut** sous **Paramètres par défaut du compte d'utilisateur**.
4. Cliquez sur **OK**.

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

Remarque :

Vous devez modifier la langue de la disposition du clavier pour les programmes autres que Unicode.

Si la langue souhaitée n'est pas disponible sur l'ordinateur, Windows peut vous inviter à l'installer. Après avoir effectué cette opération, vous devez redémarrer l'ordinateur deux fois pour que, en premier lieu, la nouvelle disposition du clavier puisse être lue par l'authentification au démarrage et, en second lieu, l'authentification au démarrage puisse définir la nouvelle disposition.

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

Pour voir les langues installées et disponibles sur le système, sélectionnez **Démarrer > Exécuter > regedit > HKEY_USERS\DEFAULT\Keyboard Layout\Preload**.

20.4 Raccourcis clavier pris en charge dans l'authentification au démarrage

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

Nous vous recommandons d'installer une version mise à jour du fichier de configuration de l'authentification au démarrage avant de procéder au déploiement de Sophos SafeGuard. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant : <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

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

Remarque :

Lorsqu'un fichier personnalisé est utilisé, celui-ci remplace le fichier intégré au fichier .msi. Le fichier par défaut s'applique seulement lorsqu'aucun fichier de configuration de la POA est défini ou trouvé.

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

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

Vous pouvez nous aider à améliorer la compatibilité en exécutant un outil que nous fournissons pour recueillir seulement les informations matérielles correspondantes. L'outil est très simple à utiliser. Les informations recueillies sont ajoutées au fichier de configuration matérielle.

Pour plus d'informations, voir

<http://www.sophos.fr/support/knowledgebase/article/110285.html> et

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

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

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

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

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

Matrice de dépendance des raccourcis clavier USB

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

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

Remarque :

Si vous appuyez sur Maj-F5 pendant le démarrage, vous réduirez considérablement la durée du lancement de l'authentification au démarrage. Gardez cependant en mémoire que si l'ordinateur est équipé d'un clavier USB ou d'une souris USB, ces derniers peuvent être désactivés si vous appuyez sur **Maj F5**.

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

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

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

20.5 Authentification au démarrage (POA) désactivée et Lenovo Rescue and Recovery

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

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

21 Éveil par appel réseau sécurisé (WOL)

Dans le SafeGuard Policy Editor, vous pouvez définir des paramètres de stratégie pour l'**Éveil par appel réseau sécurisé (WOL)** afin de préparer les ordinateurs d'extrémité à des déploiements logiciels. Si une stratégie correspondante s'applique aux ordinateurs d'extrémité, les paramètres nécessaires (par exemple, la désactivation de la POA et un intervalle d'éveil par appel réseau) sont transférés directement sur les ordinateurs d'extrémité lorsque les paramètres sont analysés.

L'équipe de déploiement peut concevoir un script de programmation en utilisant les commandes fournies pour garantir la protection maximale de l'ordinateur d'extrémité malgré la désactivation de la POA.

Remarque :

La désactivation de la POA (même pour un nombre limité de processus d'initialisation) réduit le niveau de sécurité de votre système.

Définissez les paramètres de l'**Éveil par appel réseau (WOL)** dans une stratégie du type **Paramètres de machine spécifique**. Pour plus d'informations sur les paramètres individuels, voir [Paramètres de machine spécifique - paramètres de base](#) à la page 102. En guise d'exemple de définition des paramètres d'éveil par appel réseau pour un déploiement logiciel, voir [Exemple d'éveil par appel réseau](#) à la page 118.

21.1 Exemple d'éveil par appel réseau sécurisé

L'équipe de déploiement des logiciels informe le responsable de la sécurité Sophos SafeGuard d'un déploiement de logiciels prévu pour le 25 septembre 2011 entre 03:00 et 06:00 heures du matin. Deux réinitialisations sont requises. L'agent local en charge du déploiement des logiciels doit être en mesure de se connecter à Windows.

Dans le SafeGuard Policy Editor, le responsable de la sécurité crée une stratégie du type **Paramètres de machine spécifiques** avec les paramètres suivants et la déploie aux ordinateurs d'extrémité souhaités.

Paramètre de stratégie	Valeur
Nombre de connexions automatiques (0 = pas de WOL) :	5
Écran de connexion Windows autorisé pendant l'éveil par appel réseau	Oui
Début de la plage horaire pour le lancement du WOL externe	24 sept. 2010, 12:00
Fin de la plage horaire pour le lancement du WOL externe	25 sept. 2010, 06:00

Pour plus d'informations sur les paramètres individuels, voir [Paramètres de machine spécifique - paramètres de base](#) à la page 102.

Etant donné que le nombre de connexions automatiques est défini sur 5, l'ordinateur d'extrémité démarre 5 fois sans authentification à la POA.

Remarque :

Pour le mode Éveil par appel réseau, nous recommandons d'autoriser **trois redémarrages de plus que nécessaire** pour faire face aux problèmes imprévus.

Le responsable de la sécurité définit l'intervalle sur 12 heures ou midi le jour précédant le déploiement de logiciels. Ainsi, le script de planification SGMCMDDIntn.exe démarre à l'heure et l'éveil par appel réseau ne se lance qu'à partir du 25 septembre à 3 heures du matin.

L'équipe de déploiement des logiciels produit deux commandes pour le script de programmation :

- Démarrage 24 sept.2011, 12:15, SGMCMDDIntn.exe /WOLstart
- Démarrage 26 sept.2011, 09:00 SGMCMDDIntn.exe /WOLstop

Le script de déploiement des logiciels est daté du 25.09.2011, 03:00. L'éveil par appel réseau peut être à nouveau explicitement désactivé à la fin du script en utilisant SGMCMDDIntn.exe -WOLstop.

Tous les ordinateurs d'extrémité qui se connectent avant le 24 septembre 2011 et qui se connectent aux serveurs de déploiement recevront la nouvelle stratégie et les commandes de programmation.

Tout ordinateur d'extrémité sur lequel la programmation déclenche la commande SGMCMDDIntn -WOLstart entre le 24 sept. 2011 à midi et le 25 sept. 2011, à 6 heures du matin se trouve dans l'intervalle de l'éveil par appel réseau et ce dernier sera par conséquent activé.

22 Clés cryptographiques et cartes à puce

Remarque :

La connexion à l'aide de clés cryptographiques et de cartes à puce n'est pas prise en charge par ESDP (Endpoint Security and Data Protection).

Les clés cryptographiques et les cartes à puce sont des composants matériels qui aident un utilisateur autorisé dans la procédure d'authentification sur un système informatique. Elles permettent de stocker des certificats, des signatures numériques et des informations biométriques. Ces données ne peuvent pas être manipulées.

De nos jours, il est fréquent que l'authentification avec un nom d'utilisateur et un mot de passe ne réponde plus aux besoins des clients qui souhaitent bénéficier de la meilleure protection possible contre les accès externes. C'est pourquoi, en guise d'alternative et afin d'améliorer la sécurité, Sophos SafeGuard permet de se connecter en utilisant des clés non cryptographiques et des cartes à puce.

La connexion par clé cryptographique est basée sur le principe d'une authentification en deux étapes : l'utilisateur possède une clé cryptographique (propriété), mais il ne peut l'utiliser que s'il en connaît le mot de passe (connaissance). Lorsqu'une clé cryptographique ou une carte à puce sont utilisées, leur présence et un code PIN suffisent à l'utilisateur pour s'authentifier.

Remarque : les cartes à puce et les clés cryptographiques sont traitées de la même manière dans Sophos SafeGuard. Les termes "clé cryptographique" et "carte à puce" recouvrent la même notion dans le produit et le manuel.

Dans le SafeGuard Policy Editor, vous pouvez spécifier des paramètres de stratégie pour la connexion par clé cryptographique.

22.1 Cartes à puce

Pour pouvoir utiliser une carte à puce avec Sophos SafeGuard, un lecteur de cartes et un pilote de carte pour l'ordinateur sont nécessaires en plus de la carte à puce elle-même. En outre, pour que les cartes à puce et les lecteurs de carte puissent communiquer avec Sophos SafeGuard, certains composants middleware, sous la forme d'un module PKCS#11, sont nécessaires.

22.1.1 Cartes à puce et lecteurs/pilotes de cartes à puce

Sophos SafeGuard prend en charge la connexion non cryptographique à l'authentification au démarrage. Avec les cartes à puce non cryptographiques, l'ID utilisateur et le mot de passe sont stockés sur la carte.

■ Windows

Dans le système d'exploitation Windows, les lecteurs de cartes compatibles PC/SC sont pris en charge. L'interface PC/SC régit la communication entre le PC et la carte à puce. Nombre de ces lecteurs de cartes sont déjà intégrés dans l'installation de Windows.

Pour être prises en charge par Sophos SafeGuard, les cartes à puce requièrent des pilotes compatibles PKCS#11.

■ Authentification au démarrage

Reportez-vous aux notes de publication pour obtenir une liste détaillée de toutes les cartes à puce, lecteurs de cartes à puce et pilotes de cartes à puce pris en charge.

Avec l'authentification au démarrage, c'est l'interface PC/SC qui régit la communication entre le PC et la carte à puce. Les pilotes de cartes à puce pris en charge sont fixés, de sorte que les utilisateurs ne peuvent pas en ajouter. Les pilotes de cartes à puce appropriés doivent être activés au moyen d'une stratégie dans Sophos SafeGuard.

L'interface des lecteurs de cartes à puce est standardisée et un grand nombre de ces lecteurs possèdent une interface USB ou une interface ExpressCard/54 et mettent en œuvre la norme CCID. Dans Sophos SafeGuard, il s'agit d'une condition préalable à la prise en charge avec l'authentification au démarrage. De plus, du côté du pilote, le module PKCS#11 doit être pris en charge.

22.1.2 Cartes à puce prises en charge avec l'authentification au démarrage

Sophos SafeGuard prend en charge un grand nombre de cartes à puce et de lecteurs de cartes à puce, ainsi que les pilotes de cartes à puce courants avec l'authentification au démarrage. Avec Sophos SafeGuard, les clés cryptographiques/cartes à puce compatibles avec les opérations 2048 bits RSA sont prises en charge. La prise en charge des cartes à puce faisant l'objet d'améliorations d'une version à la suivante, les clés cryptographiques et cartes à puce pour la version actuelle de Sophos SafeGuard sont répertoriés dans les notes de publication.

22.1.3 Middleware pris en charge

Le middleware de la liste ci-dessous est pris en charge par le module PKCS#11 correspondant. PKCS#11 est une interface standardisée pour connecter des clés cryptographiques/cartes à puce à différents logiciels. Elle est utilisée ici pour la communication entre la clé cryptographique/carte à puce, le lecteur de carte à puce et Sophos SafeGuard.

Fabricant	Middleware
A-Trust	a.sign Client
ActivIdentity	ActivClient, ActivClient (PIV)
AET	SafeSign Identity Client
Aladdin	eToken PKI Client
Charismatics	Smart Security Interface
Gemalto	Gemalto Access Client, Gemalto Classic Client, Gemalto .NET Card
Solution informatique GmbH	IT Solution trustWare CSP+
RSA	RSA Authentication Client 2.x, RSA Smart Card Middleware 3.x

Fabricant	Middleware
Sertifitseerimiskeskus AS	Estonian ID Card
Siemens	CardOS API
T-Systems	NetKey 3.0
Unizeto	proCertum

Informations de licence pour Siemens et Charismatics :

Sachez que l'utilisation des middlewares respectifs pour le système d'exploitation standard requiert un accord de licence avec Siemens IT Solutions and Services GmbH/Charismatics. Pour obtenir les licences, veuillez vous renseigner auprès de :

- Siemens IT Solutions und Services GmbH
Otto-Hahn-Ring 6
D-81739 München
Allemagne
- http://www.charismathics.com/cryptoshop/shop_content.php
ou
sales@charismathics.com

Le middleware est défini dans une stratégie Sophos SafeGuard du type **Paramètres de machine spécifiques** sous **Module de paramètres PKCS#11 de support de carte à puce 1** dans le champ **Nom du module**. Le package de configuration correspondant doit également être installé sur l'ordinateur sur lequel fonctionne le SafeGuard Policy Editor.

22.2 Clés cryptographiques USB

De même que les cartes à puce, les clés cryptographiques USB comportent un lecteur de cartes à puce et une carte à puce, ces deux unités se trouvant dans un même boîtier.

22.2.1 Clés cryptographiques prises en charge avec l'authentification au démarrage

Sophos SafeGuard prend en charge une vaste gamme de clés cryptographiques USB. Comme condition préalable, la carte à puce utilisée doit être prise en charge par l'authentification au démarrage de Sophos SafeGuard et les lecteurs correspondants doivent également être pris en charge. Les clés cryptographiques USB doivent également être prises en charge par le middleware correspondant.

La prise en charge des clés cryptographiques faisant l'objet d'améliorations d'une version à la suivante, les clés cryptographiques et cartes à puce pour chaque version de Sophos SafeGuard sont répertoriées dans les notes de publication.

22.3 Attribution de stratégies pour les clés cryptographiques

Lorsque vous attribuez des stratégies, vous pouvez spécifier d'autres options de clé cryptographique. Elles concernent :

- Les codes PIN
- Le mode de connexion
- La définition de codes PIN de clés cryptographiques pour la connexion automatique à l'authentification au démarrage
- Ce qui se produit lorsque l'état de la clé cryptographique n'est plus reconnu
- Le déblocage de la clé cryptographique
- Le middleware à utiliser (module PKCS#11).

22.4 Utilisation de clés cryptographiques pour se connecter à l'authentification au démarrage

Condition préalable : notez que le support USB est activé dans le BIOS. Le support de clé cryptographique doit être initialisé et la clé cryptographique doit être générée.

1. Connectez la clé cryptographique à l'interface USB.
2. Mettez l'ordinateur sous tension et attendez l'arrêt de l'authentification au démarrage.
3. Entrez le code PIN de la clé cryptographique.

Vous êtes connecté à Sophos SafeGuard.

22.4.1 Mode de connexion à l'authentification au démarrage

Il existe deux méthodes de connexion à l'aide d'une clé cryptographique. Il est possible de combiner les deux méthodes de connexion.

- Connexion avec ID utilisateur/mot de passe
- Connexion avec clé cryptographique

Le responsable de la sécurité spécifie la méthode à utiliser pour les utilisateurs et les ordinateurs dans une stratégie du type **Authentification**.

22.5 Activation de la connexion automatique à l'authentification au démarrage avec des codes PIN de clés cryptographiques par défaut

Un code PIN de clé cryptographique par défaut distribué par la stratégie permet la connexion automatique de l'utilisateur à l'authentification au démarrage. Ceci permet d'éviter la génération de chaque clé cryptographique séparément et permet aux utilisateurs de se connecter automatiquement lors de l'authentification au démarrage sans action de l'utilisateur.

Lorsqu'une clé cryptographique est utilisée lors de la connexion et qu'un code PIN par défaut est attribué à l'ordinateur, l'utilisateur est connecté automatiquement à l'authentification au démarrage sans qu'il ait besoin de saisir un code PIN.

En tant que responsable de la sécurité, vous pouvez définir le code PIN spécifique dans une stratégie du type **Authentification** et l'attribuer à différents ordinateurs ou groupes d'ordinateurs, par exemple à tous les ordinateurs d'un même lieu.

Pour activer la connexion automatique avec un code PIN de clé cryptographique par défaut, procédez comme suit :

1. Dans le SafeGuard Policy Editor, cliquez sur **Stratégies**.
2. Sélectionnez une stratégie du type **Authentification**.
3. Sous **Options de connexion**, dans **Mode de connexion**, sélectionnez **Carte à puce**.
4. Dans **Code PIN utilisé pour la connexion automatique avec une carte à puce**, spécifiez le code PIN par défaut à utiliser pour la connexion automatique. Dans ce cas, il n'est pas nécessaire de suivre les règles relatives au code PIN.

Remarque :

Ce paramètre n'est disponible que si vous sélectionnez **Carte à puce** comme **Mode de connexion** possible.

5. Dans **Authentification automatique à Windows**, définissez **Désactiver l'authentification automatique à Windows**. Si vous ne sélectionnez pas cette option lorsqu'un code PIN par défaut est spécifié, vous ne pourrez pas enregistrer la stratégie.

Si vous souhaitez activer l'option **Authentification automatique à Windows**, vous pouvez créer ultérieurement une autre stratégie du type **Authentification** dans laquelle cette option est activée, puis la déployer sur les ordinateurs d'extrémité correspondants afin que les deux stratégies soient actives dans le RSOP.

6. Vous pouvez également spécifier d'autres paramètres de clé cryptographique.
7. Enregistrez vos paramètres et déployez la stratégie sur les ordinateurs d'extrémité correspondants.

Windows démarre si la connexion automatique sur l'ordinateur d'extrémité réussit.

En cas d'échec de la connexion automatique sur l'ordinateur d'extrémité, l'utilisateur est invité à entrer le code PIN de clé cryptographique lors de l'authentification au démarrage.

23 SafeGuard Data Exchange

Remarque :

SafeGuard Data Exchange et SafeGuard Portable ne sont pas pris en charge par ESDP (Endpoint Security and Data Protection).

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

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

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

23.1 Clés locales

Remarque : SafeGuard Data Exchange et SafeGuard Portable ne sont pas disponibles avec ESDP (Endpoint Security and Data Protection).

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

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

Grâce à SafeGuard Portable, chaque utilisateur connaissant la phrase de passe peut accéder à un fichier chiffré sur un support amovible. Il est ainsi également possible de partager des données chiffrées avec des partenaires ne disposant pas de Sophos SafeGuard. SafeGuard Portable et la phrase de passe des fichiers auxquels ils doivent accéder doivent leur être fournis.

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

Remarque :

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

Les clés locales ne sont pas sauvegardées et ne peuvent pas être utilisées pour la récupération.

23.2 Phrase de passe du support

Remarque : safeguard Data Exchange et SafeGuard Portable ne sont pas disponibles avec ESDP (Endpoint Security and Data Protection).

SafeGuard Data Exchange vous permet de spécifier qu'une seule phrase de passe de support pour tous les supports amovibles (sauf les supports optiques) doit être créée sur les ordinateurs d'extrémité.

La phrase de passe du support permet d'accéder à toutes les clés locales utilisées dans SafeGuard Portable. L'utilisateur ne saisit qu'une seule phrase de passe et peut accéder à tous les fichiers chiffrés dans SafeGuard Portable, quelle que soit la clé locale utilisée pour le chiffrement.

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

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

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

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

Remarque :

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

Ceci n'est disponible que si vous avez sélectionné **Support amovible** comme **Cible de protection de périphérique**.

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

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

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

24 Options de récupération

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

■ Récupération de connexion avec Local Self Help

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

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

Pour plus d'informations, [voir Récupération avec Local Self Help](#) à la page 129.

■ Récupération par Challenge/Réponse

Le mécanisme Challenge/Réponse est un système de récupération de connexion sécurisé et fiable qui vient en aide aux utilisateurs qui ne peuvent pas se connecter à leur ordinateur ou accéder aux données chiffrées. Lors de la procédure Challenge/Réponse, l'utilisateur communique le code de challenge généré sur l'ordinateur d'extrémité au responsable du support qui générera à son tour un code de réponse. Ce code autorisera l'utilisateur à exécuter une action spécifique sur l'ordinateur.

Grâce à la récupération via Challenge/Réponse, Sophos SafeGuard propose plusieurs flux de travail pour les scénarios de récupération types nécessitant l'aide du support.

Pour en savoir plus, [voir Récupération avec Challenge/Réponse](#) à la page 135.

■ Récupération du système

Sophos SafeGuard offre différentes méthodes et outils de récupération de composants système essentiels et de composants Sophos SafeGuard, par exemple :

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

Pour plus d'informations, [voir Récupération du système](#) à la page 148.

25 Récupération avec Local Self Help

Sophos SafeGuard propose Local Self Help afin de permettre à l'utilisateur ayant oublié son mot de passe de se connecter à son ordinateur sans recourir au support technique. Local Self Help réduit le nombre d'appels de récupération de connexion, et ainsi les tâches de routine des membres du support en leur permettant de se concentrer sur des demandes plus complexes.

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

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

Lorsque Local Self Help a été activé par la stratégie, un assistant Local Self Help est disponible pour guider les utilisateurs finaux en fournissant les réponses initiales et en modifiant les questions.

La récupération avec Local Self Help est disponible pour les méthodes de connexion suivantes dans l'authentification au démarrage :

- Connexion avec ID utilisateur et mot de passe
- Connexion avec empreinte digitale

Remarque :

La connexion avec empreinte digitale n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

- Connexion avec une clé non cryptographique dans la mesure où la connexion avec ID utilisateur et mot de passe a aussi été activée dans une stratégie du type **Authentification**. Pour plus d'informations, voir [Authentification](#) à la page 78.

Remarque :

La connexion avec clé cryptographique n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

Pour une description détaillée de Local Self Help sur l'ordinateur d'extrémité, consultez l'aide utilisateur Sophos SafeGuard, chapitre *Récupération avec Local Self Help*.

25.1 Définition des paramètres de Local Self Help dans une stratégie

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

Activation de Local Self Help

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

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

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

Configuration de Local Self Help

Vous pouvez définir les options suivantes pour Local Self Help dans une stratégie du type **Paramètres généraux**.

■ **Longueur minimale des réponses**

Définissez la longueur minimale (en caractères) des réponses. Le nombre par défaut est **1**.

■ **Texte de bienvenue sous Windows**

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

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

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

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

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

25.2 Définition de questions

Pour pouvoir utiliser Local Self Help sur un ordinateur d'extrémité, l'utilisateur doit répondre à un nombre prédéfini de questions et les enregistrer. En tant que responsable de la sécurité avec les droits nécessaires, vous pouvez spécifier le nombre de questions auxquelles l'utilisateur

doit répondre pour activer Local Self Help sur l'ordinateur d'extrémité. Vous pouvez également préciser le nombre de questions qui seront aléatoirement sélectionnées dans la POA. Pour se connecter à la POA avec Local Self Help, l'utilisateur doit répondre correctement à toutes les questions affichées dans la POA. Pour plus d'informations, voir [Définition du nombre de questions qui attendent une réponse](#) à la page 131.

En tant que responsable de la sécurité avec les droits nécessaires, vous pouvez enregistrer et modifier les questions Local Self Help dans le SafeGuard Policy Editor. Pour plus d'informations, voir [Création d'un sujet de question et ajout de questions](#) à la page 132 et voir [Modification des sujets de question](#) à la page 133.

25.3 Définition du nombre de questions qui attendent une réponse

Vous pouvez définir le nombre de questions auxquelles il faut répondre lors de la configuration de Local Self Help et dans la POA.

1. Dans la zone de navigation **Stratégies**, sélectionnez **Questions Local Self Help**.
2. Dans la zone d'action sous **Paramètres Local Self Help**, vous pouvez spécifier deux valeurs différentes pour le nombre de questions Local Self Help :

- a) Dans le champ **Nombre minimum de questions/réponses disponibles**, spécifiez le nombre de questions auxquelles l'utilisateur doit répondre dans l'assistant Local Self Help pour activer Local Self Help sur l'ordinateur d'extrémité.

Pour que Local Self Help soit actif, le nombre de questions spécifiées dans ce champ doit être disponible avec les réponses sur l'ordinateur d'extrémité.

- b) Dans le champ **Nombre de questions présentées dans la POA**, spécifiez le nombre de questions auxquelles l'utilisateur doit répondre dans la POA lors de la connexion avec Local Self Help.

Les questions affichées dans la POA sont sélectionnées de manière aléatoire à partir des questions auxquelles l'utilisateur a répondu dans l'assistant Local Self Help.

Le nombre spécifié dans le champ **Nombre minimum de questions/réponses disponibles** doit être supérieur au nombre spécifié dans le champ **Nombre de questions présentées dans la POA**. Si ce n'est pas le cas, un message d'erreur apparaît lorsque vous enregistrez vos changements.

Les valeurs par défaut sont :

- **Nombre minimum de questions/réponses disponibles : 10**
- **Nombre de questions présentées dans la POA : 5**

3. Enregistrez vos changements dans la base de données.

Le nombre de questions s'applique à la configuration de Local Self Help déployée sur les ordinateurs d'extrémité.

25.4 Utilisation du modèle

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

Le sujet de question est également disponible en option dans d'autres langues comme le français et l'espagnol. Vous pouvez importer ces versions de langue dans la zone de navigation de stratégie.

Remarque : lorsque les utilisateurs finaux entrent les réponses en japonais pour activer Local Self Help sur les ordinateurs d'extrémité, ils doivent utiliser les caractères Romaji (Roman). Sinon, les réponses ne correspondent pas lorsque l'utilisateur les saisit dans l'authentification au démarrage.

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

25.5 Importation de sujets de question

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

1. Créez un nouveau sujet de question ([voir Création d'un sujet de question et ajout de questions](#) à la page 132).
2. Dans la zone de navigation **Stratégies**, sélectionnez le nouveau sujet de question sous **Questions Local Self Help**.
3. Cliquez avec le bouton droit de la souris dans la zone d'action pour ouvrir le menu contextuel du sujet de question. Dans le menu contextuel, sélectionnez **Importer**.
4. Sélectionnez le répertoire et le sujet de question, puis cliquez sur **Ouvrir**.

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

25.6 Création d'un sujet de question et ajout de questions

Vous pouvez créer de nouveaux sujets de question à propos de thèmes différents. Vous pouvez ainsi proposer aux utilisateurs un choix de sujets de question qui pourraient leur convenir.

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

Une nouvelle ligne de question est ajoutée.

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

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

25.7 Modification de sujets de question

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

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

25.8 Suppression de sujets de question

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

Remarque :

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

25.9 Enregistrement de textes de bienvenue

Vous pouvez enregistrer un texte de bienvenue à afficher dans la première boîte de dialogue de l'assistant de Local Self Help.

Les fichiers texte contenant les informations requises doivent être créés avant d'être enregistrés dans le SafeGuard Policy Editor. La taille maximale des fichiers de textes d'informations est de 50 Ko. Sophos SafeGuard utilise les textes codés en Unicode UTF-16 uniquement. Si vous

ne créez pas les fichiers texte dans un ce format, ils seront automatiquement convertis lorsqu'ils seront enregistrés.

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

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

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

26 Récupération avec Challenge/Réponse

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

Cette fonctionnalité est intégrée au SafeGuard Policy Editor en tant qu'assistant de récupération.

Avantages de la procédure Challenge/Réponse

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

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

Situations classiques nécessitant l'aide du support

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

Remarque :

Dans Local Self Help, le mot de passe actuel peut être affiché et l'utilisateur peut continuer à l'utiliser. Ceci pour éviter de réinitialiser le mot de passe ou de recourir à l'assistance technique. Pour plus d'informations, voir [Récupération avec Local Self Help](#) à la page 129.

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

Sophos SafeGuard propose différents flux de travail de récupération pour ces scénarios types, ce qui permet aux utilisateurs d'accéder de nouveau à leurs ordinateurs.

26.1 Flux de travail Challenge/Réponse

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

- L'ordinateur d'extrémité sur lequel le code de challenge est généré.
 - Le SafeGuard Policy Editor où, en tant que responsable du support possédant les droits correspondants, vous créez un code de réponse qui autorisera l'utilisateur à effectuer l'action requise sur l'ordinateur.
1. Sur l'ordinateur d'extrémité, l'utilisateur demande le code de challenge. En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage, soit dans l'outil de récupération de clé KeyRecovery.

Un code de challenge sous la forme d'une chaîne de caractères ASCII est généré puis affiché.

2. L'utilisateur contacte le support. Il lui fournit les données d'identification nécessaires, ainsi que le code de challenge.
3. Le support démarre l'assistant de récupération dans le SafeGuard Policy Editor.
4. Le support sélectionne le type de récupération approprié, confirme les données d'identification et le code de challenge, puis sélectionne l'action de récupération souhaitée.
Un code de réponse sous la forme d'une chaîne de caractères ASCII est généré et s'affiche.
5. Le support transmet le code de réponse à l'utilisateur, par exemple par téléphone ou message texte.
6. L'utilisateur saisit le code de réponse, En fonction du type de récupération, cette opération s'effectue soit dans l'authentification au démarrage, soit dans l'outil de récupération de clé KeyRecovery.

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

26.2 Lancement de l'assistant de récupération

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

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

L'assistant de récupération SafeGuard démarre. Vous pouvez sélectionner le type de récupération que vous souhaitez utiliser.

26.3 Types de récupération

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

■ Procédure Challenge/Réponse pour client Sophos SafeGuard

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

Remarque :

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

■ Challenge/Réponse à l'aide de clients virtuels

Les volumes chiffrés peuvent être récupérés facilement grâce à des fichiers spécifiques appelés clients virtuels, dans les cas où la procédure Challenge/Réponse n'est pas prise en charge, par exemple lorsque l'authentification au démarrage est corrompue.

26.4 Procédure Challenge/Réponse pour clients Sophos SafeGuard

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

Si ce fichier de récupération de clé est accessible au support Sophos SafeGuard, par exemple sur un chemin réseau partagé, une procédure Challenge/Réponse pour un ordinateur protégé par Sophos SafeGuard peut être fournie.

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

Remarque :

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

Actions de récupération de l'authentification au démarrage

La procédure Challenge/Réponse pour un ordinateur d'extrémité intervient dans les situations suivantes :

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

Pour un ordinateur protégé par Sophos SafeGuard, seule la clé machine définie est disponible dans la base de données (pas la clé utilisateur). Par conséquent, la seule action de récupération possible dans une session de Challenge/Réponse est **Initialisation du client SGN sans connexion utilisateur**.

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

Études de cas de récupération potentiels :

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

L'ordinateur est verrouillé et l'utilisateur est invité à lancer une procédure Challenge/Réponse pour le déverrouiller. Si on suppose que l'utilisateur connaît le mot de passe correct, il n'est pas nécessaire de réinitialiser le mot de passe. La procédure Challenge/Réponse permet à

l'ordinateur de démarrer via l'authentification au démarrage. L'utilisateur peut ensuite saisir le mot de passe correctement à l'invite de connexion Windows et s'y connecter.

L'utilisateur a oublié le mot de passe.

Remarque :

Nous vous recommandons d'utiliser Local Self Help pour récupérer un mot de passe oublié. Dans Local Self Help, le mot de passe actuel peut être affiché et l'utilisateur peut continuer à l'utiliser. Ceci pour éviter de réinitialiser le mot de passe ou de recourir à l'assistance technique. Pour plus d'informations, voir [Récupération avec Local Self Help](#) à la page 129.

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

1. La procédure Challenge/Réponse permet à l'ordinateur de démarrer à partir de l'authentification au démarrage.
2. A l'invite de connexion Windows, l'utilisateur ne connaît pas le mot de passe correct et doit par conséquent le modifier au niveau Windows. Cela nécessite d'autres actions de récupération sortant du périmètre de Sophos SafeGuard, via des moyens Windows standard.

Nous recommandons l'utilisation des méthodes de réinitialisation de mot de passe Windows suivantes.

- À l'aide d'un compte de service ou administrateur disponible sur l'ordinateur d'extrémité avec les droits Windows requis.
 - À l'aide d'un disque de réinitialisation de mot de passe Windows sur l'ordinateur d'extrémité.
3. L'utilisateur saisit le nouveau mot de passe Windows fourni par le support. L'utilisateur modifie ensuite ce mot de passe immédiatement en choisissant une valeur connue de lui seul.
 4. Sophos SafeGuard détecte que le nouveau choix de mot de passe ne correspond pas au mot de passe Sophos SafeGuard utilisé actuellement au niveau de l'authentification au démarrage. L'utilisateur est alors invité à saisir son ancien mot de passe Sophos SafeGuard et, puisqu'il a oublié son mot de passe, il doit cliquer sur **Annuler**.
 5. Un nouveau certificat est nécessaire afin de pouvoir définir un nouveau mot de passe sans avoir à fournir l'ancien. L'utilisateur doit confirmer cette procédure.
 6. Un nouveau certificat utilisateur sera créé en fonction du nouveau choix de mot de passe Windows. Cela permet à l'utilisateur de se reconnecter à l'ordinateur ainsi qu'à l'authentification au démarrage à l'aide du nouveau mot de passe.

Remarque :

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

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

Le cache local doit être réparé.

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

26.4.1 Génération d'une réponse à l'aide du fichier de récupération de clé

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

1. Pour ouvrir l'assistant de récupération dans le SafeGuard Policy Editor, sélectionnez **Outils** > **Récupération** dans la barre de menus.
2. Dans **Type de récupération**, sélectionnez **Client Sophos SafeGuard**.
3. Cliquez sur **Parcourir** pour localiser le fichier de récupération de clé requis. Pour faciliter l'identification des fichiers de récupération, leur nom est identique à celui de l'ordinateur : nomordinateur.GUID.xml.
4. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié.

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

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

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

26.5 Challenge/Réponse à l'aide de clients virtuels

Lors de l'utilisation des clients virtuels, Sophos SafeGuard permet de récupérer des volumes chiffrés même dans des situations d'urgence complexes, par exemple lorsque la POA est corrompue. La procédure Challenge/Réponse utilisant les clients virtuels dépend des éléments suivants :

■ Fichier de récupération de clé

Le fichier de récupération de clé est créé lors de l'installation du logiciel de chiffrement Sophos SafeGuard sur les ordinateurs d'extrémité et contient la clé de chiffrement pour l'ordinateur d'extrémité. Ce fichier est généré pour chaque ordinateur protégé par Sophos SafeGuard et contient la clé machine définie qui est chiffrée avec le certificat de l'entreprise. Il doit être accessible pour le support technique, par exemple sur une carte mémoire ou sur un chemin réseau partagé.

■ **Fichier du client virtuel**

Des fichiers spécifiques appelés clients virtuels sont créés dans le SafeGuard Policy Editor et utilisés comme informations de référence dans la base de données.

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

Le disque de récupération sert à démarrer l'ordinateur d'extrémité à partir du BIOS.

■ **Outil de récupération de clé KeyRecovery**

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

26.5.1 Clients virtuels

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

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

26.5.2 Flux de travail de récupération à l'aide de clients virtuels

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

1. Demandez au support technique de vous fournir le disque de récupération Sophos SafeGuard.

Le support peut télécharger le disque de récupération Windows PE avec les derniers pilotes du filtre Sophos SafeGuard sur le site du support Sophos. Pour plus d'informations, consultez : <http://www.sophos.fr/support/knowledgebase/article/108805.html>.

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

L'ordinateur est accessible à nouveau.

26.5.3 Création d'un client virtuel

Les clients virtuels sont des fichiers de clés chiffrés pouvant être utilisés pour une récupération dans une procédure Challenge/Réponse comme informations de référence sur l'ordinateur.

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

1. Dans le SafeGuard Policy Editor, sélectionnez la zone **Clients virtuels**.
2. Dans la fenêtre de navigation de gauche, cliquez sur **Clients virtuels**.
3. Dans la barre d'outils, cliquez sur **Ajouter un client virtuel**.
4. Saisissez un nom unique de client virtuel et cliquez sur **OK**. Les clients virtuels sont identifiés dans la base de données par ces noms.
5. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

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

26.5.4 Exportation d'un client virtuel

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

1. Dans le SafeGuard Policy Editor, sélectionnez la zone **Clients virtuels**.
2. Dans la fenêtre de navigation située à gauche, cliquez sur **Clients virtuels**.
3. Dans la zone d'action, recherchez le client virtuel concerné en cliquant sur la loupe. Les clients virtuels disponibles s'affichent.
4. Sélectionnez l'entrée requise dans la zone d'action et cliquez sur **Exporter le client virtuel** dans la barre d'outils.
5. Sélectionnez un emplacement de stockage pour le fichier du client virtuel **recoverytoken.tok**, puis cliquez sur **OK**.

Enregistrez le fichier dans un emplacement sécurisé.

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

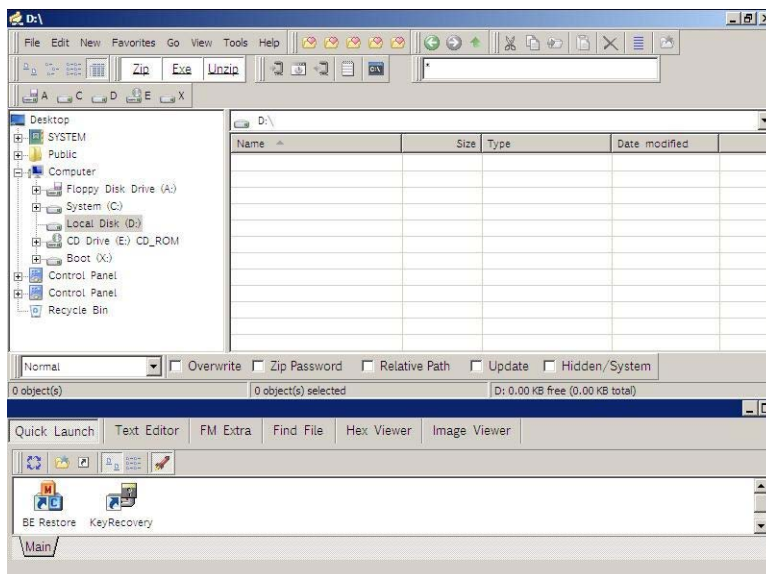
6. Copiez le fichier du client virtuel **recoverytoken.tok** sur un support amovible. Nous recommandons d'utiliser une carte mémoire.

Veillez à conserver ce support de stockage en lieu sûr. Mettez les fichiers à disposition du support et sur les ordinateurs d'extrémité car ils sont requis pour une procédure Challenge/Réponse avec des clients virtuels.

26.5.5 Démarrage de l'ordinateur depuis le disque de récupération

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

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



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

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



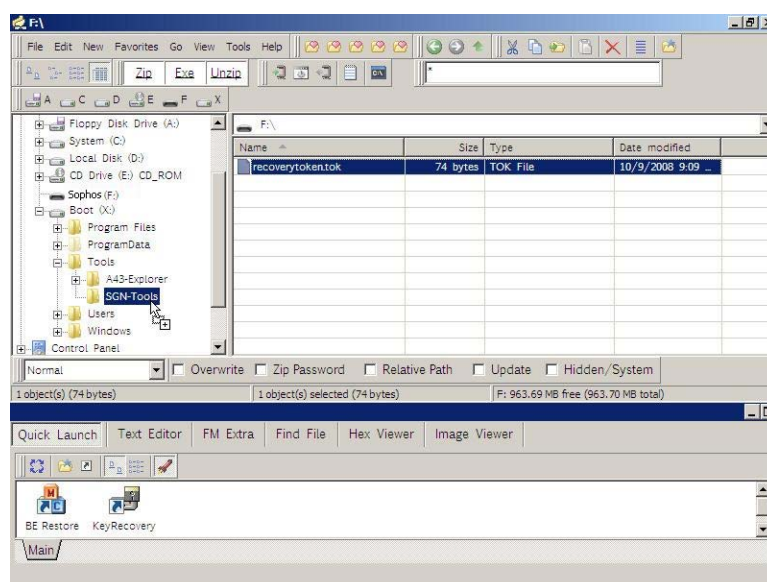
3. Recherchez les ID de clé des lecteurs auxquels vous souhaitez accéder. Vous devrez fournir cet ID de clé ultérieurement.

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

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

Conditions préalables :

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



26.5.7 Initialisation du challenge dans l'outil de récupération de clé KeyRecovery

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

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



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

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

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

26.5.8 Génération d'une réponse à l'aide de clients virtuels

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

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

26.5.8.1 Confirmation du client virtuel

Condition préalable :

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

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

Ensuite, sélectionnez l'action de récupération requise.

26.5.8.2 Sélection du fichier de récupération de clé

Condition préalable :

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

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

1. Dans l'assistant de récupération, dans **Client virtuel**, sélectionnez l'action de récupération **Clé requise** et cliquez sur **Suivant**.
2. Activez l'option **Sélectionner un fichier de récupération de clé contenant une clé de récupération**.
3. Cliquez sur [...] près de cette option pour rechercher le fichier. Pour faciliter l'identification des fichiers de récupération, leur nom est identique à celui de l'ordinateur : nomordinateur.GUID.xml.
4. Cliquez sur **Suivant** pour confirmer. La fenêtre dans laquelle vous devez saisir le code de challenge s'affiche.
5. Saisissez le code de challenge que l'utilisateur vous a indiqué, puis cliquez sur **Suivant**. Ce code est vérifié.

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

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

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

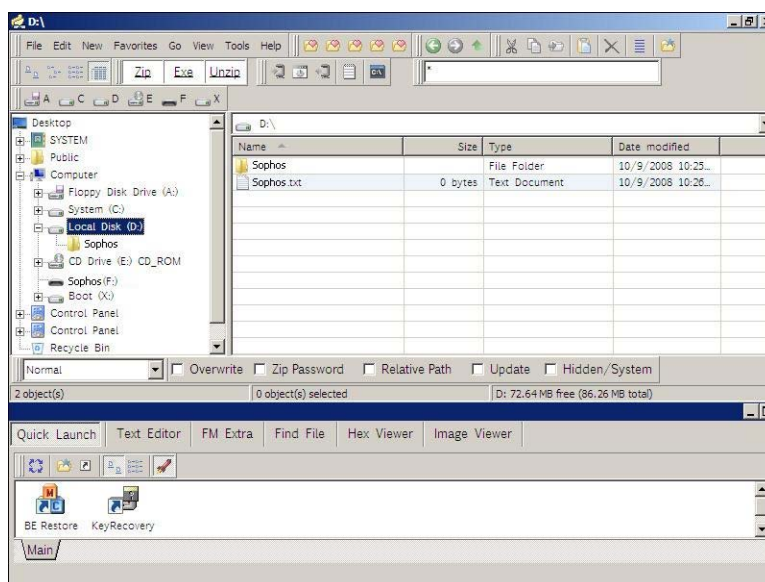
1. Sur l'ordinateur d'extrémité, dans l'outil de récupération de clé KeyRecovery, entrez le code de réponse fourni par le support.

La clé de récupération requise est transférée dans le code de réponse.

2. Cliquez sur **OK**. Le disque sélectionné pour la procédure Challenge/Réponse a été déchiffré.



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



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

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

26.5.10 Suppression de clients virtuels

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

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

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

27 Récupération du système

Sophos SafeGuard chiffre les fichiers et les lecteurs de façon transparente. Les lecteurs d'initialisation peuvent également être chiffrés et les fonctions de déchiffrement telles que le code, les algorithmes de chiffrement et la clé de chiffrement doivent être disponibles très tôt au cours de la phase de démarrage. C'est la raison pour laquelle les informations chiffrées ne sont pas accessibles si les modules essentiels de Sophos SafeGuard ne sont pas disponibles ou ne fonctionnent pas.

Les sections suivantes couvrent les problèmes et les méthodes de récupération envisageables.

27.1 Récupération des données en démarrant depuis un support externe

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

Conditions préalables :

- L'utilisateur qui démarre l'ordinateur à partir d'un support externe doit disposer du droit approprié. Ce droit peut être soit configuré dans le SafeGuard Policy Editor dans une stratégie de type **Authentification (L'utilisateur peut uniquement démarrer à partir du disque dur sur Oui)**, soit obtenu pour une utilisation unique avec une procédure Challenge/Réponse.
- L'ordinateur doit prendre en charge le démarrage à partir de supports autres qu'un disque dur fixe.

Pour récupérer l'accès aux données chiffrées sur l'ordinateur :

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

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

Remarque :

En fonction du BIOS en cours d'utilisation, il est possible que l'initialisation depuis le disque ne fonctionne pas.

27.2 MBR corrompu

Pour résoudre les problèmes d'enregistrement d'amorçage maître (MBR, Master Boot Record) corrompu, Sophos SafeGuard propose l'utilitaire **BE_Restore.exe**.

Pour plus d'informations, consultez le guide des outils.

27.3 Volumes

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

Dès que l'une des unités ci-dessous est endommagée, le volume n'est plus accessible :

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

27.3.1 Secteur d'initialisation

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

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

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

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

L'utilitaire **BE_Restore** peut restaurer le secteur d'initialisation endommagé. Pour plus d'informations, consultez le guide des outils.

27.3.2 Secteur d'initialisation original

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

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

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

27.4 Configuration de WinPE pour Sophos SafeGuard

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

SetupWinPE -pe2 <fichier d'image WinPE>

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

SetupWinPE effectue toutes les modifications nécessaires.

Remarque :

Notez que, dans ce type d'environnement WinPE, seuls les lecteurs chiffrés avec le BOOTKEY sont accessibles.

28 Sophos SafeGuard et disques durs compatibles Opal à chiffrement automatique

Les disques durs à chiffrement automatique offrent un chiffrement de type matériel des données lorsqu'ils sont écrits sur le disque dur. Le Trusted Computing Group (TCG) a publié la norme Opal indépendante des fournisseurs pour les disques durs à chiffrement automatique. Différents fournisseurs de matériels proposent des disques durs compatibles Opal. Sophos SafeGuard prend en charge la norme Opal.

28.1 Comment Sophos SafeGuard intègre-t-il les disques durs compatibles Opal ?

Dans le SafeGuard Policy Editor, vous pouvez créer des stratégies de sécurité et les déployer sur les ordinateurs d'extrémité équipés de disques durs compatibles Opal à chiffrement automatique comme sur tout autre poste protégé par Sophos SafeGuard.

En prenant en charge la norme Opal, nous offrons la série complète des fonctions Sophos SafeGuard aux utilisateurs professionnels des disques durs compatibles Opal à chiffrement automatique. En combinaison avec Sophos SafeGuard, les disques durs compatibles Opal offrent les fonctions de sécurité étendues, [voir Amélioration des disques durs compatibles Opal avec Sophos SafeGuard](#) à la page 151.

28.2 Amélioration des disques durs compatibles Opal avec Sophos SafeGuard

En combinaison avec les disques durs compatibles Opal à chiffrement automatique, Sophos SafeGuard offre les avantages suivants :

- Authentification au démarrage avec interface graphique utilisateur
- Prise en charge des clés non cryptographiques et des cartes à puce

Remarque :

La connexion à l'aide de clés non cryptographiques et de cartes à puce n'est pas prise en charge par ESDP (Endpoint Security and Data Protection).

- Prise en charge de la connexion par empreintes digitales
- Récupération (Local Self Help, Challenge/Réponse)
- Chiffrement des supports amovibles (par exemple, les clés USB) avec SafeGuard Data Exchange

Remarque :

SafeGuard Data Exchange n'est pas pris en charge par ESDP (Endpoint Security and Data Protection).

28.3 Chiffrement de disques durs compatibles Opal

Les disques durs compatibles Opal sont à chiffrement automatique. Les données sont chiffrées automatiquement lorsqu'elles sont écrites sur le disque dur.

Les disques durs sont verrouillés par une clé AES 256 utilisée comme mot de passe Opal. Ce mot de passe est géré par Sophos SafeGuard via une stratégie de chiffrement, voir [Verrouillage des disques durs compatibles Opal](#) à la page 152.

28.4 Verrouillage des disques durs compatibles Opal

Pour verrouiller les disques durs compatibles Opal, la clé de la machine doit être définie pour au moins un volume sur le disque dur dans une stratégie de chiffrement. Au cas où la stratégie de chiffrement inclut un volume d'initialisation, la clé de la machine est définie automatiquement.

1. Dans le SafeGuard Policy Editor, créez une stratégie du type **Protection du périphérique**, voir [Création de stratégies](#) à la page 44.
2. Dans le champ **Mode de chiffrement du support**, sélectionnez **Basé sur volume**.
3. Dans le champ **Clé à utiliser pour le chiffrement**, sélectionnez **Clé machine définie**.
4. Enregistrez vos changements dans la base de données.
5. Déployez la stratégie sur l'ordinateur d'extrémité correspondant.

Le disque dur compatible Opal est verrouillé et est seulement accessible en se connectant sur l'ordinateur à l'authentification au démarrage.

28.5 Permettre aux utilisateurs de déverrouiller les disques durs compatibles Opal

En tant que responsable de la sécurité, vous pouvez permettre aux utilisateurs de déverrouiller les disques durs compatibles Opal sur les ordinateurs d'extrémité à l'aide de la commande **Déchiffrer** du menu contextuel Windows Explorer.

1. Dans le SafeGuard Policy Editor, créez une stratégie du type **Protection du périphérique** et incluez tous les volumes présents sur le disque dur compatible Opal.
2. Dans le champ **Mode de chiffrement du support**, sélectionnez **Aucune chiffrement**.
3. Dans le champ **L'utilisateur peut déchiffrer le volume**, sélectionnez **Oui**.
4. Enregistrez vos changements dans la base de données.
5. Déployez la stratégie sur l'ordinateur d'extrémité correspondant.

L'utilisateur peut déverrouiller le disque dur compatible Opal sur l'ordinateur d'extrémité. Les données sont toujours chiffrées lorsqu'elles sont écrites sur le disque dur.

28.6 Journalisation des événements pour les ordinateurs d'extrémité équipés de disques durs compatibles Opal

Les événements signalés par les ordinateurs d'extrémité équipés de disques durs compatibles Opal à chiffrement automatique sont journalisés, comme pour tout autre ordinateur d'extrémité protégé par Sophos SafeGuard. Les événements ne mentionnent pas particulièrement le type d'ordinateur. Les événements signalés sont identiques à tout autre ordinateur d'extrémité protégé par Sophos SafeGuard.

Pour plus d'informations, [voir Journalisation](#) à la page 108.

29 Blocage de la désinstallation sur les ordinateurs d'extrémité

Pour assurer une protection supplémentaire des ordinateurs d'extrémité, vous pouvez empêcher la désinstallation locale de Sophos SafeGuard. Définissez l'option **Désinstallation autorisée** de la stratégie **Paramètres spécifiques à la machine** sur **Non** et déployez cette stratégie sur les ordinateurs d'extrémité. Si cette sorte de stratégie s'applique à l'ordinateur d'extrémité, les tentatives de désinstallation sont annulées et les tentatives non autorisées sont journalisées.

Remarque :

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

29.1 Protection antialtération Sophos

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

Remarque :

La protection antialtération Sophos ne s'applique qu'aux ordinateurs d'extrémité dotés de Sophos Endpoint Security and Control version 9.5 ou version ultérieure.

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

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

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

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

30 Mise à jour de Sophos SafeGuard

Une mise à jour de Sophos SafeGuard comprend les composants suivants. Exécutez la mise à jour pour chaque composant dans l'ordre ci-dessous :

1. Base de données Sophos SafeGuard

Remarque :

Pour Sophos SafeGuard Disk Encryption 5.5x (ESDP) : lorsque la base de données Sophos SafeGuard est gérée par Microsoft SQL Server Express et réside sur l'ordinateur local, elle est automatiquement mise à jour par le SafeGuard Policy Editor lorsqu'elle est démarrée pour la première fois. Pour plus d'informations, voir [Mise à jour du SafeGuard Policy Editor](#) à la page 156.

2. SafeGuard Policy Editor
3. Ordinateur d'extrémité protégé par Sophos SafeGuard

Sophos SafeGuard 5.6x peut être mis à jour directement depuis SafeGuard Enterprise autonome 5.4x ou Sophos SafeGuard 5.5x sans changer les paramètres précédemment définis. Si vous voulez mettre à jour à partir d'anciennes versions, vous devez tout d'abord mettre à jour à la version 5.40.

30.1 Mise à jour de la base de données Sophos SafeGuard

Remarque :

Pour Sophos SafeGuard Disk Encryption 5.5x (ESDP) : lorsque la base de données Sophos SafeGuard est gérée par Microsoft SQL Server Express et réside sur l'ordinateur local, elle est automatiquement mise à jour avec le SafeGuard Policy Editor. Dans ce cas, vous pouvez ignorer cette tâche. Pour plus d'informations, voir [Mise à jour du SafeGuard Policy Editor](#) à la page 156.

Pour mettre à jour manuellement la base de données, les conditions préalables suivantes doivent être remplies :

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

Dans le répertoire Outils du produit livré, vous trouverez plusieurs scripts SQL pour la mise à jour de la base de données.

1. Fermez le SafeGuard Policy Editor.

2. Définissez la base de données correspondante en mode SINGLE_USER pour exécuter les scripts SQL.
3. La base de données doit être convertie version par version dans la version actuelle. En fonction de la version installée, démarrez les scripts SQL suivants dans cet ordre :
 - a) 5.4x > 5.50 : exécutez **MigrateSGN540_SGN550.sql**.
 - b) 5.5x > 5.60 : exécutez **MigrateSGN550_SGN560.sql**
4. Redéfinissez la base de données correspondante en mode MULTI_USER.

Il se peut que les sommes de contrôle cryptographiques de certains tableaux ne soient plus correctes après la mise à jour de la base de données. Lorsque vous démarrez le SafeGuard Policy Editor, des messages d'avertissement apparaissent. Vous pouvez réparer les tableaux dans la boîte de dialogue correspondante.

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

30.2 Mise à jour du SafeGuard Policy Editor

Conditions préalables

- La version 5.40 ou ultérieure du SafeGuard Policy Editor doit être installée. Les versions antérieures doivent d'abord être mises à jour vers la version 5.40.
- Vous n'avez pas besoin de désinstaller le SafeGuard Policy Editor.

Remarque :

Si le SafeGuard Policy Editor est installé sur un ordinateur sur lequel le logiciel de chiffrement Sophos SafeGuard est installé, ce dernier doit tout d'abord être mis à jour vers la version 5.6x. Ensuite, le SafeGuard Policy Editor doit être mis à jour vers la 5.6x. La mise à jour seule du SafeGuard Policy Editor peut conduire à des échecs de connexion au niveau Windows.

- La base de données Sophos SafeGuard a déjà été mise à jour vers la dernière version. Pour un fonctionnement réussi, les numéros des versions de la base de données Sophos SafeGuard et du SafeGuard Policy Editor doivent être identiques.

Remarque :

Pour Sophos SafeGuard Disk Encryption 5.5x (ESDP) : lorsque la base de données Sophos SafeGuard est gérée par Microsoft SQL Server Express et réside sur l'ordinateur local, elle est automatiquement mise à jour par le SafeGuard Policy Editor lorsqu'elle est démarrée pour la première fois.

- NET Framework 3.0 Service Pack 1 doit être installé pour la mise à jour vers la dernière version. Vous pouvez le télécharger gratuitement sur le site : <http://www.microsoft.com/downloads/fr-fr/default.aspx>.
- Vous devez avoir mis à niveau ASP.NET vers la version 2.0.
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour mettre à jour le SafeGuard Policy Editor :

1. Installez la dernière version du package d'installation du SafeGuard Policy Editor. Vous n'avez pas besoin de réexécuter l'assistant de configuration.
2. Pour Sophos SafeGuard Disk Encryption 5.5x : lorsque la base de données Sophos SafeGuard est gérée par Microsoft SQL Server Express et réside sur l'ordinateur local. Cliquez sur **Oui** pour confirmer la mise à jour de la base de données.

La base de données Sophos SafeGuard 5.5x est sauvegardée et automatiquement mise à jour vers la dernière version.

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

30.3 Configuration minimale des ordinateurs protégés par Sophos SafeGuard

SafeGuard Policy Editor version 5.6x peut gérer des ordinateurs protégés par Sophos SafeGuard version 5.40 ou ultérieure.

Conditions préalables

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

Pour mettre à jour les ordinateurs protégés par Sophos SafeGuard :

1. Installez le package de préinstallation **SGxClientPreinstall.msi**, qui fournit à l'ordinateur d'extrémité la configuration requise pour une installation réussie du logiciel de chiffrement courant.
2. Installez la dernière version du package d'installation du client correspondant.

Windows Installer reconnaît les modules déjà installés et ne réinstalle que ces modules. Si l'authentification au démarrage est installée, un noyau POA à jour est également disponible après une mise à jour réussie (stratégies, clés, etc.). Sophos SafeGuard est automatiquement redémarré sur l'ordinateur.

Remarque :

- Si la configuration de Sophos SafeGuard n'a pas changé, vous n'avez pas besoin de créer ni d'installer un nouveau package de configuration Sophos SafeGuard.
- Si la configuration de Sophos SafeGuard a changé, par exemple différents paramètres de configuration, créez et réinstallez un nouveau package de configuration Sophos SafeGuard.

Pour des raisons de sécurité, supprimez tous les packages de configuration obsolètes ou non utilisés. Si vous tentez de remplacer un package de configuration Sophos SafeGuard récent par un plus ancien, l'installation échoue et un message d'erreur s'affiche.

30.4 Amélioration de Sophos SafeGuard avec le chiffrement basé sur volume

Remarque :

Cette section ne s'applique pas à Sophos SafeGuard avec ESDP (Endpoint Security and Data Protection).

Si vous voulez ajouter le chiffrement basé sur volume à un ordinateur protégé par Sophos SafeGuard sur lequel seul le module SafeGuard Data Exchange avec chiffrement basé sur fichier est installé, vous devez exécuter les étapes suivantes. Ces étapes sont nécessaires pour garantir une authentification au démarrage sécurisée et correcte.

1. Désinstallez le package d'installation de SafeGuard Data Exchange (SGNClient_withoutDE.msi/SGNClient_withoutDE_x64.msi).
2. Désinstallez le package de configuration Sophos SafeGuard.
3. Installez le package Sophos SafeGuard Device Encryption avec chiffrement basé sur volume et sur fichier (SGNClient.msi/SGNClient_x64.msi). Sélectionnez les fonctions **Chiffrement de périphérique** et **Echange de données** lorsque vous y êtes invité et terminez l'assistant d'installation.
4. Créez un nouveau package de configuration et déployez-le sur l'ordinateur.

Le chiffrement basé sur volume a été ajouté sur le client Sophos SafeGuard (autonome).

Remarque :

Le fichier de récupération de clé ainsi que les clés locales créées lors de l'installation du package d'installation Data Exchange restent disponibles.

31 Mise à niveau de Sophos SafeGuard vers SafeGuard Enterprise

Vous pouvez facilement mettre à niveau Sophos SafeGuard vers la suite SafeGuard Enterprise avec gestion centralisée, afin d'utiliser l'ensemble des fonctions de SafeGuard Enterprise.

Pour mettre à niveau vers SafeGuard Enterprise :

- Vous devez mettre à niveau le SafeGuard Policy Editor en SafeGuard Management Center.
- La configuration de l'ordinateur d'extrémité chiffré par Sophos SafeGuard doit être mise à niveau sur les ordinateurs protégés par SafeGuard Enterprise.

31.1 Migration du SafeGuard Policy Editor vers le SafeGuard Management Center

Vous pouvez migrer le SafeGuard Policy Editor vers le SafeGuard Management Center afin d'utiliser les fonctions de gestion complètes, par exemple, la gestion des utilisateurs et des ordinateurs, ainsi que la journalisation.

Conditions préalables

- Vous n'avez pas besoin de désinstaller le SafeGuard Policy Editor.
- Configurez le serveur SafeGuard Enterprise avant la mise à niveau.

Mise à niveau du SafeGuard Policy Editor

Pour la mise à niveau, installez simplement le package SGNManagementCenter.msi sur l'ordinateur sur lequel le SafeGuard Policy Editor a été configuré.

1. Démarrez SGNManagementCenter.msi à partir du dossier d'installation du produit livré.
2. Dans la page **Bienvenue**, cliquez sur **Suivant**.
3. Acceptez le contrat de licence.
4. Sélectionnez un chemin d'installation.
5. Cliquez sur **Terminer** pour terminer l'installation.
6. Si nécessaire, redémarrez votre ordinateur.
7. Configurez le SafeGuard Management Center.

Le SafeGuard Policy Editor a été mis à niveau vers le SafeGuard Management Center.

31.2 Mise à niveau des ordinateurs d'extrémité Sophos SafeGuard vers les ordinateurs d'extrémité SafeGuard Enterprise

Vous pouvez mettre à niveau les ordinateurs d'extrémité avec une configuration Sophos SafeGuard vers une configuration (gérée) de client SafeGuard Enterprise. Les ordinateurs sont ainsi définis dans le SafeGuard Management Center sous la forme d'objets pouvant être gérés et disposant d'une connexion au serveur SafeGuard Enterprise.

Remarque :

La procédure inverse, la mise à niveau inférieure d'une configuration SafeGuard Enterprise vers une configuration Sophos SafeGuard, n'est pas conseillée. Pour ce faire, vous devez complètement réinstaller le logiciel de chiffrement Sophos SafeGuard sur l'ordinateur d'extrémité.

Conditions préalables

- Le SafeGuard Policy Editor a été mis à niveau en SafeGuard Management Center.
- Il n'est pas nécessaire de désinstaller le logiciel de chiffrement Sophos SafeGuard.
- Sauvegardez l'ordinateur d'extrémité avant de démarrer la mise à niveau.
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour mettre à niveau un ordinateur protégé par Sophos SafeGuard vers un client SafeGuard Enterprise (géré) :

1. Dans le menu **Outils** du SafeGuard Management Center, cliquez sur **Outil de package de configuration**. Cliquez sur **Créer un package de configuration (géré)**. Créez le package de configuration pour le client SafeGuard Enterprise (géré)
2. Attribuez ce package aux ordinateurs Sophos SafeGuard à l'aide d'une stratégie de groupe.
L'authentification est désactivée car l'attribution utilisateur-ordinateur n'est pas mise à niveau. Après la mise à niveau, les ordinateurs d'extrémité ne sont donc plus protégés !
3. Redémarrez l'ordinateur d'extrémité. La première connexion est toujours effectuée avec l'ouverture de session automatique. De nouvelles clés et de nouveaux certificats sont attribués à l'utilisateur.
4. Redémarrez l'ordinateur d'extrémité une deuxième fois. Connectez-vous à l'authentification au démarrage. Les ordinateurs sont de nouveau protégés seulement après le second redémarrage.
5. Supprimez tous les packages de configuration obsolètes ou non utilisés.

La configuration de Sophos SafeGuard sur l'ordinateur d'extrémité est désormais une configuration (gérée) du client SafeGuard Enterprise.

32 Mise à niveau de SafeGuard Easy 4.x/ Sophos SafeGuard Disk Encryption 4.x vers Sophos SafeGuard 5.6x

SafeGuard Easy (SGE) 4.5x et Sophos SafeGuard Disk Encryption 4.60 peuvent être directement mis à niveau vers Sophos SafeGuard 5.6x par l'installation sur l'ordinateur du package d'installation du client SafeGuard Device Encryption.

La mise à niveau directe a été testée. Elle est prise en charge pour SafeGuard Easy 4.5x. La mise à niveau directe doit également fonctionner pour les versions qui se trouvent entre la version 4.3x et la version 4.4x. La mise à niveau directe n'est pas prise en charge pour les versions antérieures à la version 4.3x. Ces versions doivent d'abord être mises à niveau vers SafeGuard Easy 4.50.

Le chiffrement des disques durs est conservé ; vous n'avez donc pas besoin de les déchiffrer et de les chiffrer à nouveau. Il n'est pas non plus nécessaire de désinstaller SafeGuard Easy ou Sophos SafeGuard Disk Encryption.

Ce chapitre décrit la mise à niveau vers Sophos SafeGuard, explique les fonctions qui peuvent être migrées et détaille les restrictions.

32.1 Conditions préalables

Les conditions préalables suivantes doivent être remplies :

- La mise à niveau directe a été testée. Elle est prise en charge pour SafeGuard Easy 4.5x. La mise à niveau directe doit également fonctionner pour les versions qui se trouvent entre la version 4.3x et la version 4.4x. La mise à niveau directe n'est pas prise en charge pour les versions antérieures à la version 4.3x. Ces versions doivent d'abord être mises à niveau vers SafeGuard Easy 4.50.
- Vous pouvez effectuer une mise à niveau directe vers Sophos SafeGuard Disk Encryption version 4.6x.
- SafeGuard Easy/Sophos SafeGuard Disk Encryption doivent être exécutés sur le système d'exploitation suivant :
 - Windows XP Professionnel Service Pack 2 et 3
- La version 3.01 ou ultérieure de Windows Installer doit être installée.
- Le matériel doit respecter la configuration requise pour Sophos SafeGuard 5.5x.
- Si vous utilisez un logiciel spécifique, par exemple un middleware Lenovo, il doit respecter la configuration système requise pour Sophos SafeGuard 5.5x.
- La mise à niveau peut être effectuée uniquement si les disques durs sont chiffrés à l'aide des algorithmes suivants : AES128, AES256, 3DES et IDEA.

Restrictions

La mise à niveau est soumise aux restrictions suivantes :

- Seul le package d'installation de SafeGuard Device Encryption, avec les fonctions standard, peut être installé (SGNClient.msi/SDEClient.msi). Si le module SafeGuard Data Exchange doit également être installé, cette installation doit s'effectuer dans une étape séparée (notez que SafeGuard Data Exchange n'est pas pris en charge par ESDP).
- Le package d'installation sans chiffrement basé sur volume (SGNClient_withoutDE.msi) n'est pas pris en charge pour la mise à niveau vers Sophos SafeGuard.
- Les installations suivantes ne peuvent pas être mises à niveau vers Sophos SafeGuard et l'installation de ce dernier ne doit pas être tentée.

Remarque :

Si vous démarrez une mise à niveau dans les cas énoncés ci-dessous, un message d'erreur s'affiche (numéro d'erreur 5006).

Installations à double initialisation

Installations avec commutateur Compaq actif

Installations Lenovo Computrace

Disques durs partiellement chiffrés, par exemple avec le chiffrement des secteurs de démarrage seulement.

Disques durs avec des partitions masquées

Disques durs chiffrés avec l'un des algorithmes suivants : XOR, STEALTH, DES, RIJNDAEL, Blowfish-8, Blowfish-16

Scénarios à plusieurs initialisations avec une seconde partition Windows ou Linux

- Les supports amovibles qui ont été chiffrés avec les algorithmes XOR, STEALTH, DES, RIJNDAEL, Blowfish-8 ou Blowfish-16 ne peuvent pas être mis à niveau.

Remarque :

Des données risquent d'être perdues si un périphérique amovible a été chiffré avec les algorithmes XOR, STEALTH, DES, RIJNDAEL, Blowfish-8 ou Blowfish-16. Il est impossible d'accéder aux données du support amovible avec Sophos SafeGuard après la migration !

- Les supports amovibles avec des volumes Super Floppy ne peuvent pas être transformés après la migration.
- Les supports amovibles peuvent être convertis dans un format compatible avec Sophos SafeGuard. Après la conversion, un support de données chiffrées ne peut être lu que par Sophos SafeGuard et uniquement sur l'ordinateur d'extrémité sur lequel il a été converti.

Remarque :

Le chiffrement et la migration des supports amovibles ne sont pas pris en charge par ESDP.

32.2 Fonctionnalités mises à niveau

Le tableau ci-dessous indique quelles fonctionnalités sont mises à niveau et leur correspondance dans Sophos SafeGuard.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Mise à niveau	Sophos SafeGuard
Disques durs chiffrés	Oui	Les clés des disques durs sont protégées par l'authentification au démarrage Sophos SafeGuard. Elles ne sont donc jamais exposées. Si le mode de protection à l'initialisation est sélectionné dans SafeGuard Easy, vous devez désinstaller la version actuelle. L'algorithme de chiffrement du disque dur n'est pas modifié par la mise à niveau. En conséquence, l'algorithme réel de ce type de disque dur mis à niveau peut différer de la stratégie générale de Sophos SafeGuard.
Supports amovibles chiffrés (seulement applicable lors de la migration depuis SafeGuard Easy)	Oui	Les supports de données chiffrées, par exemple les cartes mémoire USB, peuvent être convertis au format Sophos SafeGuard. Remarque : après la conversion, un support de données chiffrées ne peut être lu que par SafeGuard Enterprise et uniquement sur l'ordinateur d'extrémité sur lequel il a été converti. La conversion doit être confirmée cas par cas.
Algorithmes de chiffrement	Dans une certaine mesure	Les algorithmes AES128, AES256, 3DES et IDEA peuvent être migrés. AES-128 et 3-DES ne peuvent néanmoins pas être sélectionnés dans le SafeGuard Policy Editor pour les supports à chiffrer.
Challenge/Réponse	Dans une certaine mesure	La procédure challenge/réponse est conservée.
Noms d'utilisateur	Non	Étant donné que les noms d'utilisateur Windows sont utilisés dans Sophos SafeGuard, vous n'avez pas besoin de réutiliser les noms d'utilisateur SafeGuard Easy/Sophos SafeGuard Disk Encryption spécifiques. L'enregistrement des ordinateurs mis à niveau s'effectue donc de la même manière que pour une nouvelle installation de Sophos SafeGuard, c'est-à-dire en attribuant de manière centralisée les utilisateurs de l'ordinateur ou en les enregistrant localement. Remarque : Après la mise à niveau, le premier utilisateur qui se connecte à Windows est défini comme utilisateur principal au sein de l'authentification

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Mise à niveau	Sophos SafeGuard
		au démarrage (sauf s'il est indiqué sur la liste de comptes de service).
Mots de passe utilisateur	Non	Étant donné que les mots de passe utilisateur Windows sont utilisés dans Sophos SafeGuard, vous n'avez pas besoin de réutiliser les mots de passe SafeGuard Easy/Sophos SafeGuard Disk Encryption spécifiques. Les mots de passe SafeGuard Easy/Sophos SafeGuard Disk Encryption ne seront donc pas mis à niveau.
Stratégies, paramètres (par exemple, longueur minimum de mot de passe)	Non	Pour garantir la cohérence de tous les paramètres, aucune mise à niveau automatique n'est exécutée. Les paramètres doivent être réinitialisés dans le SafeGuard Policy Editor.
Authentification de préinitialisation	Non	L'authentification de préinitialisation (PBA) est remplacée par l'authentification au démarrage (POA) de Sophos SafeGuard.
Installations sans GINA	Oui	Les installations sans GINA sont mises à niveau vers SafeGuard Enterprise avec installation de SGNINA.
Clés cryptographiques/cartes à puces (s'applique uniquement lors de la migration à partir de SafeGuard Easy)	Dans une certaine mesure	Vous pouvez continuer à utiliser les clés cryptographiques/cartes à puce dans SafeGuard Enterprise. Néanmoins, les informations d'identification ne sont pas mises à niveau. Les clés cryptographiques utilisées dans SafeGuard Easy doivent donc être de nouveau générées dans SafeGuard Enterprise, et comme pour tout autre ordinateur d'extrémité SafeGuard Enterprise, configurées à l'aide de stratégies. Les informations d'identification SafeGuard Easy, regroupées sous forme de fichier sur les clés cryptographiques/cartes à puce, restent telles quelles, mais ne peuvent être utilisées pour que la connexion aux ordinateurs prenant en charge SafeGuard Easy. Si besoin est, le middleware de la clé cryptographique/carte à puce doit être mis à jour vers une version prise en charge par SafeGuard Enterprise.
Connexion avec le lecteur d'empreintes digitales Lenovo	Dans une certaine mesure Remarque : La connexion par empreinte digitale n'est	Vous pouvez continuer à utiliser la connexion par empreinte digitale dans Sophos SafeGuard. Le matériel et le logiciel du lecteur d'empreintes digitales doivent être pris en charge par Sophos SafeGuard et les données d'empreintes digitales de l'utilisateur doivent être réenregistrées. Pour plus d'informations sur la connexion par empreinte digitale, reportez-vous à l'aide de l'utilisateur.

SafeGuard Easy/Sophos SafeGuard Disk Encryption	Mise à niveau	Sophos SafeGuard
	pas disponible avec ESDP.	

32.3 Préparation à la mise à niveau

Avant de démarrer l'installation de Sophos SafeGuard, vous devez prendre les mesures suivantes :

- Avant de mettre à niveau les systèmes d'extrémité, préparez un package de configuration Sophos SafeGuard à l'aide du SafeGuard Policy Editor. Une fois que le logiciel de chiffrement est installé sur les ordinateurs d'extrémité, vous pouvez y déployer le package de configuration. Les stratégies transférées avec le premier package de configuration doivent correspondre à la configuration précédente de l'ordinateur doté de SafeGuard Easy/Sophos SafeGuard Disk Encryption.

Si aucun package de configuration n'est installé avec la mise à niveau, tous les lecteurs qui ont été chiffrés par SafeGuard Easy/Sophos SafeGuard Disk Encryption restent chiffrés.

- Pour réduire le risque de perte de données, nous vous recommandons de créer une sauvegarde complète des ordinateurs que vous souhaitez mettre à niveau.

Avant une installation Sophos SafeGuard, exécutez les étapes conseillées, par exemple l'utilisation de **chkdsk** et **defrag**. Pour plus d'informations, voir [Préparation à l'installation](#) à la page 16. Consultez aussi :

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

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

- Nous vous recommandons de créer une sauvegarde valide du noyau et de l'enregistrer dans un emplacement toujours accessible (par exemple, un chemin d'accès au réseau). Pour plus d'informations, reportez-vous aux manuels ou aux aides de SafeGuard Easy 4.5x/Sophos SafeGuard Disk Encryption 4.60, chapitre *Enregistrement du noyau système et création d'un support d'urgence*.
- Pour réduire le risque de perte de données, nous vous recommandons de créer un environnement de test pour la première mise à niveau.
- Si vous effectuez une mise à niveau de versions antérieures de SafeGuard Easy, vous devez d'abord mettre à niveau vers la version 4.50.
- Laissez les ordinateurs allumés tout au long du processus de mise à niveau.
- Le responsable de la sécurité doit conserver les informations d'identification Windows des utilisateurs au cas où les utilisateurs perdraient leur mot de passe Windows après la migration. Cela peut se produire si les utilisateurs se sont connectés auparavant via l'authentification de préinitialisation et se connectent ensuite via la connexion sécurisée

Windows (SAL, Secure Autologon). Ainsi, ils n'ont jamais utilisé leurs informations d'identification Windows.

Remarque :

Les utilisateurs doivent connaître leur mot de passe de connexion à Windows avant de procéder à la mise à niveau. Cette étape est essentielle car il est impossible de définir un mot de passe Windows après la mise à niveau et l'installation de Sophos SafeGuard. Si les utilisateurs ne le connaissent pas car ils ont utilisé la connexion automatique sécurisée de SafeGuard Easy/Sophos Encryption, ils ne pourront pas se connecter à Sophos SafeGuard. Dans ce cas, la connexion automatique vers Windows est refusée et les utilisateurs ne peuvent pas se connecter à Sophos SafeGuard. Il existe donc un risque de perte de données car les utilisateurs ne peuvent plus accéder à leurs ordinateurs.

32.4 Démarrage de la mise à niveau

Remarque :

L'installation peut être effectuée sur un système exécutant SafeGuard Easy/Sophos SafeGuard Disk Encryption. Aucun déchiffrement de disques durs ou de volumes chiffrés n'est nécessaire.

Utilisez le package du client SafeGuard Device Encryption (SGNClient.msi/SDEClient.msi) depuis le dossier d'installation, avec la fonction standard définie. Vous ne pouvez pas utiliser le package client SGNClient_withoutDE.msi pour effectuer la mise à niveau. Il est préférable d'effectuer l'installation de manière centralisée en mode sans surveillance. L'installation via le dossier de configuration n'est pas recommandée !

1. Cliquez deux fois sur le fichier WIZLDR.exe dans le dossier de programme de SafeGuard Easy/Sophos SafeGuard Disk Encryption de l'ordinateur d'extrémité que vous souhaitez mettre à niveau. Cette opération démarre l'assistant de migration.
2. Dans l'assistant de migration, entrez le mot de passe SYSTEM et confirmez en cliquant sur **Suivant**. Dans **Dossier de destination**, cliquez sur **Suivant**, puis sur **Terminer**. Un fichier de configuration de migration **SGEMIG.cfg** est créé.
3. Dans l'Explorateur Windows, renommez le fichier **SGEMIG.cfg** en **SGE2SGN.cfg**.

Remarque : les droits du propriétaire/de l'auteur doivent être définis pour ce fichier et pour le chemin d'accès au dossier dans lequel il est stocké pendant la mise à niveau. Autrement, la mise à niveau risque d'échouer et un message indiquant que le fichier **SGE2SGN.cfg** est introuvable s'affiche.

4. Saisissez la commande "msiexec" à l'invite de commande pour installer le package de préinstallation Sophos SafeGuard ainsi que le package d'installation du "client" sur l'ordinateur équipé de SafeGuard Easy/Sophos SafeGuard Disk Encryption. Ajoutez le paramètre MIGFILE qui indique le chemin d'accès au fichier de configuration de migration SGE2SGN.cfg :

Exemple :

```
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
msiexec /i \\Distributionserver\Software\Sophos\SafeGuard\SDEClient.msi
/L*VX“\\Distributionserver\Software\Sophos\SafeGuard\%Computername%.log“
MIGFILE=\\Distributionserver\Software\Sophos\SafeGuard\SGE2SGN.cfg
```

- Si la mise à niveau est réussie, Sophos SafeGuard peut être utilisé sur l'ordinateur.
- Même si la mise à niveau échoue, SafeGuard Easy/Sophos SafeGuard Disk Encryption peut quand même être utilisé sur l'ordinateur. Dans de tels cas, Sophos SafeGuard est automatiquement supprimé.

32.5 Configuration des ordinateurs d'extrémité mis à niveau

Les ordinateurs d'extrémité sont initialement configurés par des packages de configuration qui permettent, entre autres, d'activer l'authentification au démarrage.

Par conséquent, lors de la mise à niveau, le package de préinstallation et le package d'installation de Sophos SafeGuard, contenant le logiciel de chiffrement, doivent être installés. La configuration des systèmes d'extrémité doit avoir lieu seulement après l'activation de la POA et la connexion de l'utilisateur à Windows.

1. Créez le package de configuration initiale dans le SafeGuard Policy Editor avec les paramètres de stratégie requis. Cliquez sur **Outils > Créer un package de configuration**.
2. Installez le package de configuration sur les ordinateurs d'extrémité.

Remarque : les stratégies transférées avec le premier package de configuration Sophos SafeGuard doivent correspondre à la configuration précédente de l'ordinateur SafeGuard Easy/Sophos SafeGuard Disk Encryption.

32.6 Après la mise à niveau

Après la mise à niveau, les éléments suivants sont disponibles dans Sophos SafeGuard après la connexion à l'authentification au démarrage :

- les clés et algorithmes des volumes chiffrés ;
- les clés et algorithmes des supports amovibles chiffrés (uniquement applicable lors d'une mise à niveau vers SafeGuard Easy).

Les volumes chiffrés restent inchangés et les clés de chiffrement sont automatiquement converties dans un format compatible avec Sophos SafeGuard.

Remarque :

Pour déchiffrer le disque dur ou ajouter et supprimer des clés de chiffrement du disque dur, l'utilisateur doit d'abord redémarrer l'ordinateur.

Les stratégies doivent être réinitialisées dans le SafeGuard Policy Editor afin de correspondre à la configuration précédente de l'ordinateur SafeGuard Easy/Sophos SafeGuard Disk Encryption.

Migration du support amovible

Remarque :

Applicable seulement lors de la mise à niveau depuis SafeGuard Easy.

Les supports amovibles chiffrés restent également chiffrés, mais les clés doivent être converties dans un format compatible avec Sophos SafeGuard.

Remarque :

Après la conversion, un support de données chiffrées ne peut être lu que par SafeGuard Enterprise et uniquement sur l'ordinateur d'extrémité sur lequel il a été converti.

Pour déchiffrer le support amovible ou ajouter et supprimer des clés de chiffrement des supports amovibles, l'utilisateur doit d'abord déconnecter le support de l'ordinateur et le réinsérer.

Lorsque vous accédez à un support amovible après migration, l'utilisateur doit confirmer explicitement la conversion des clés de chiffrement dans un format compatible avec Sophos SafeGuard. La stratégie appropriée de chiffrement basé sur volume doit être présente sur l'ordinateur avant la conversion. faute de quoi les clés ne sont pas converties.

L'utilisateur est invité à confirmer la conversion pour chaque support amovible. Un message approprié s'affiche.

- Si l'utilisateur confirme la conversion, il bénéficie d'un accès complet aux données migrées.
- Si l'utilisateur refuse la conversion, les données migrées peuvent tout de même être lues et modifiées.

Les supports amovibles nouvellement ajoutés sont chiffrés, comme avec tout ordinateur Sophos SafeGuard, si la configuration de stratégie appropriée est présente sur l'ordinateur d'extrémité.

33 À propos de la désinstallation

- Lorsque le logiciel de chiffrement Sophos SafeGuard est installé sur le même ordinateur que le SafeGuard Policy Editor, assurez-vous de bien suivre cette procédure de désinstallation afin de pouvoir continuer à les utiliser :
 1. Désinstallez le SafeGuard Policy Editor.
 2. Désinstallez le package de configuration Sophos SafeGuard.
 3. Désinstallez le logiciel de chiffrement Sophos SafeGuard.
 4. Installez à nouveau le package que vous souhaitez continuer à utiliser. Pour utiliser le SafeGuard Policy Editor, assurez-vous d'importer l'ancien certificat de la machine suite à l'installation. Pour utiliser le logiciel de chiffrement Sophos SafeGuard, assurez-vous d'installer le package de configuration de Sophos SafeGuard suite à l'installation du logiciel de chiffrement.
- Avant de désinstaller le logiciel de chiffrement, désinstallez d'abord le package de configuration.
- Si le logiciel de chiffrement est installé sur un ordinateur où le SafeGuard Policy Editor est installé, ce dernier ne peut plus être utilisé après la désinstallation du logiciel de chiffrement. Si vous voulez continuer à utiliser le SafeGuard Policy Editor dans ce cas, vous devez le réinstaller.
- Il est possible qu'après une désinstallation, certains fichiers et certaines entrées de registre ne puissent pas être supprimés. Veuillez consulter la base de connaissances Sophos (mots-clés "SGN & désinstaller") pour savoir comment nettoyer l'installation manuellement. Un nettoyage manuel est nécessaire pour réinstaller avec succès le logiciel de chiffrement sur le même ordinateur.
- Si la désinstallation est déclenchée via Active Directory, assurez-vous que tous les volumes chiffrés sur volume ont été déchiffrés correctement auparavant.
- Si vous avez installé SafeGuard Device Encryption et SafeGuard Data Exchange sur un ordinateur, vous ne pouvez pas désinstaller SafeGuard Device Encryption seul. Vous devez désinstaller le package complet.
- Déchiffrez tous les supports amovibles chiffrés avant de désinstaller le dernier client Sophos SafeGuard accessible. Sinon, il se peut que vous ne puissiez plus accéder à vos données. Tant que vous conservez votre base de données Sophos SafeGuard, les données sur les supports amovibles peuvent être récupérées.

34 Support technique

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

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

35 Mentions légales

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

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

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

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