

Sophos SafeGuard Disk Encryption, Sophos SafeGuard Easy Guide de démarrage

Version du produit : 5.60

Date du document : avril 2011



Table des matières

| | |
|---|----|
| 1 À propos de ce guide..... | 3 |
| 2 À propos de Sophos SafeGuard..... | 3 |
| 3 Mise à niveau à partir d'anciennes versions | 5 |
| 4 Que dois-je installer ?..... | 5 |
| 5 Quelles sont les étapes clés ?..... | 6 |
| 6 Installation du SafeGuard Policy Editor..... | 6 |
| 7 Exécution de la configuration initiale..... | 7 |
| 8 Copie de la stratégie par défaut pour modification..... | 8 |
| 9 Configuration des ordinateurs d'extrémité pour les tâches de service suite à l'installation | 9 |
| 10 Publication de la stratégie dans un package de configuration..... | 10 |
| 11 Installation du logiciel de chiffrement et du package de configuration sur les ordinateurs d'extrémité..... | 10 |
| 12 Récupération d'un mot de passe oublié..... | 16 |
| 13 Aide sur les tâches générales..... | 19 |
| 14 Support technique..... | 19 |
| 15 Mentions légales..... | 20 |

1 À propos de ce guide

Ce guide vous indique comment paramétrer Sophos SafeGuard pour protéger les ordinateurs de votre entreprise contre tout accès non autorisé.

Il s'applique aux produits suivants :

- Sophos SafeGuard Disk Encryption (SDE) 5.6x disponible avec la suite Endpoint Security and Data Protection (ESDP).
- Sophos SafeGuard Easy (SGE) 5.6x. À partir de la version 5.50, SGE est le nouveau nom de produit de la solution autonome SafeGuard Enterprise.

Ce guide mentionne toute fonction ou tout paramètre différent entre les deux produits.

Des informations supplémentaires sont disponibles dans l'aide administrateur SDE/SGE et dans l'aide utilisateur SDE/SGE.

2 À propos de Sophos SafeGuard

Sophos SafeGuard permet de chiffrer les données de manière transparente : les utilisateurs n'ont pas besoin de spécifier les données à chiffrer. Le chiffrement et le déchiffrement sont effectués en tâche de fond. Le chiffrement permet d'éviter la consultation ou la modification des données des personnes non autorisées. Le chiffrement Sophos SafeGuard ne peut pas être contourné, même si vous connectez les supports de stockage à un autre système.

Grâce à Sophos SafeGuard, vous pouvez :

- Effectuer une mise en œuvre rapide.
- Protéger la confidentialité des données.
- Chiffrer les données à l'aide d'une technologie certifiée conforme à FIPS 140.

Les ordinateurs protégés par Sophos SafeGuard exécutent l'authentification au démarrage SafeGuard pendant la phase de préinitialisation de l'ordinateur, c'est-à-dire avant le démarrage du système d'exploitation. Une fois que l'utilisateur s'est correctement authentifié dans l'authentification au démarrage, le système d'exploitation démarre et l'utilisateur est connecté à Windows.



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

- Protection antialtération pour Sophos SafeGuard Disk Encryption.

- Délais de connexion en cas de saisies erronées.
- Interface utilisateur graphique personnalisable de type Windows.
- Connexion automatique à Windows.
- Prise en charge de plusieurs langues et du format unicode.

Accès pratique pour les opérations informatiques

Sophos SafeGuard propose plusieurs fonctions facilitant les opérations informatiques sur les ordinateurs d'extrémité :

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

Scénarios de récupération dans Sophos SafeGuard

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

■ Récupération de connexion à l'aide de 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.

■ Récupération par challenge/réponse

Le mécanisme de récupération par challenge/réponse implique l'assistance du support. Il 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 par challenge/réponse, Sophos SafeGuard propose plusieurs flux de travail pour les scénarios de récupération classiques nécessitant l'aide du support.

■ Récupération du système

Sophos SafeGuard propose divers outils et méthodes destinés à la récupération du système, notamment Windows PE personnalisé par Sophos SafeGuard ou Lenovo Rescue and

Recovery. Grâce à ces outils, les problèmes liés au système Windows et aux composants Sophos SafeGuard peuvent être résolus.

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

3 Mise à niveau à partir d'anciennes versions

De nombreuses améliorations ont été apportées à Sophos SafeGuard 5.6x.

■ Mise à niveau à partir de la version 5.5x :

Les ordinateurs déjà chiffrés à l'aide de la version 5.5x de SDE ou de la versions 5.5x de SGE peuvent être mis à niveau à la version 5.6x.

■ Mise à niveau à partir de la version 4.x :

Les ordinateurs déjà chiffrés à l'aide de la version 4.6x de SDE ou des versions 4.3x à 4.5x de SGE peuvent être mis à niveau à Sophos SafeGuard 5.6x.

À partir de la version 5.5x, Sophos SafeGuard utilise un outil d'administration différent appelé SafeGuard Policy Editor qui n'est pas compatible avec SDE 4.x ou SGE 4.x. Les volumes chiffrés restent inchangés et les clés de chiffrement sont automatiquement converties dans un format compatible avec la version 5.5x.

Sophos SafeGuard 5.6x nécessite l'importation d'un fichier de licence valide dans le SafeGuard Policy Editor. Votre partenaire commercial devrait vous avoir envoyé ce fichier.

Avant de procéder à la mise à niveau à Sophos SafeGuard 5.6x, créez un nouveau package de configuration à l'aide du SafeGuard Policy Editor et déployez-le en même temps que le logiciel Sophos SafeGuard 5.6x.

Pour plus d'informations, reportez-vous à l'aide de l'administrateur et au chapitre *Mise à niveau de SafeGuard Easy 4.x/Sophos SafeGuard Disk Encryption 4.x vers Sophos SafeGuard 5.6x* et consultez <http://www.sophos.fr/support/knowledgebase/article/108561.html>.

4 Que dois-je installer ?

Installez les composants suivants :

- SafeGuard Policy Editor. L'outil de gestion de Sophos SafeGuard. Il vous permet de gérer le logiciel de chiffrement sur les ordinateurs d'extrémité et d'effectuer les tâches de récupération.

Microsoft SQL Server 2005 Express utilisé pour stocker les paramètres des stratégies Sophos SafeGuard est installé automatiquement au cours de l'installation du SafeGuard Policy Editor si une instance du serveur SQL est indisponible.

Remarque :

Installez d'abord le 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.

- Logiciel de chiffrement Sophos SafeGuard. Il procède au chiffrement des données sur les ordinateurs d'extrémité et assure leur protection contre tout accès non autorisé.

Remarque :

Nous vous conseillons de ne pas installer le logiciel de chiffrement sur l'ordinateur administrateur utilisé pour la gestion de Sophos SafeGuard.

5 Quelles sont les étapes clés ?

Effectuez les étapes suivantes :

- Installez le SafeGuard Policy Editor.
- Procédez à la première configuration en créant une stratégie par défaut et en définissant les conditions requises les plus importantes pour effectuer les tâches du support.
- Copiez la stratégie par défaut pour pouvoir la modifier.
- Configurez l'ordinateur d'extrémité pour qu'il effectue les tâches de service suite à l'installation.
- Publiez la stratégie modifiée dans un package de configuration.
- Installez le logiciel de chiffrement et le package de configuration sur les ordinateurs d'extrémité.

6 Installation du SafeGuard Policy Editor

Avant de commencer :

- 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, (voir insert link once available here).
- Assurez-vous de disposer des droits d'administrateur Windows.

Pour installer le SafeGuard Policy Editor :

1. Ouvrez une session sur votre ordinateur en tant qu'administrateur.
2. À l'aide de l'adresse Web et des codes d'accès de téléchargement fournis par votre administrateur système, allez sur le site Web Sophos et téléchargez les programmes d'installation.
3. À partir du dossier d'installation du produit, cliquez deux fois sur l'un des fichiers d'installation suivants, selon le produit que vous utilisez. Un assistant vous guide tout au long des étapes nécessaires.

| Sophos SafeGuard Disk Encryption | SafeGuard Easy |
|----------------------------------|----------------------|
| SDEPolicyEditor.msi. | SGNPolicyEditor.msi. |

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

Si vous êtes invité à installer Microsoft SQL Server 2005 Express, cliquez sur **Oui**. Dans ce cas, vos codes d'accès Windows sont utilisés pour le compte utilisateur SQL.

5. 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 Exécution de la configuration initiale

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

1. Démarrez le SafeGuard Policy Editor dans 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**.
3. Sur la page **Base de données**, cliquez sur **Suivant**. La base de données SQL pour l'archivage des paramètres et des stratégies SafeGuard est créée.
4. Sur la page **Responsable de la sécurité**, saisissez et confirmez un mot de passe pour accéder au SafeGuard Policy Editor. Cliquez sur **Suivant**. Le certificat du responsable de la sécurité est créé.

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

Le nom du responsable de la sécurité s'affiche.

| Sophos SafeGuard Disk Encryption | SafeGuard Easy |
|---|---|
| Le nom du responsable de la sécurité est toujours administrateur. | Le nom de l'utilisateur actuel s'affiche. |

5. Sur la page **Entreprise**, cliquez sur **Suivant**. Le certificat d'entreprise est utilisé pour sécuriser les paramètres de stratégie de la base de données et des ordinateurs d'extrémité.
6. Sur la page **Sauvegarde des certificats d'entreprise et du responsable de la sécurité**, définissez un emplacement de stockage sûr pour les sauvegardes de certificats. Puis cliquez sur **Suivant**.

Si vous sauvegardez les certificats dans l'emplacement de stockage par défaut dès maintenant, assurez-vous de les exporter dans un emplacement sûr et accessible en cas de besoin de récupération. Vous pouvez par exemple utiliser une clé USB à mémoire flash immédiatement après la configuration initiale. Vous aurez besoin de ces certificats pour restaurer une installation défectueuse ou une base de données corrompue du SafeGuard Policy Editor.

7. Sur la page **Clés de récupération**, cliquez sur **Suivant**. Un partage réseau avec les droits suffisants pour le personnel du support informatique est créé. Ce partage sert à récupérer les fichiers de clé de récupération à partir des ordinateurs d'extrémité requis pour effectuer la récupération.

Remarque :

Le logiciel Sophos SafeGuard tente de se connecter au partage réseau pendant 4 minutes et en cas de tentative infructueuse, il réessaye de se connecter après chaque ouverture de session Windows jusqu'à ce que la connexion soit établie ou jusqu'à ce que les fichiers de clés de récupération soient sauvegardés manuellement.

8. Sur la page **Licence**, cliquez sur [...] pour naviguer jusqu'au fichier de licence valide et exécuter le SafeGuard Policy Editor en environnement de production. Votre partenaire commercial devrait vous avoir envoyé le fichier de licence. Sélectionnez le fichier et cliquez sur **Ouvrir**. Cliquez sur **Suivant**.
9. Cliquez sur **Terminer**.

La configuration initiale est terminée.

- Une stratégie par défaut a été créée afin de pouvoir appliquer la stratégie de sécurité globale de l'entreprise sur tous les ordinateurs d'extrémité.

L'authentification au démarrage est activée.

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

L'utilisateur peut récupérer un mot de passe oublié à l'aide de Local Self Help en répondant aux questions prédéfinies.

Le support peut récupérer les mots de passe via la procédure challenge/réponse.

Le chiffrement basé sur fichier est activé uniquement pour les clients de SafeGuard Easy.

- Toutes les conditions requises au support pour pouvoir effectuer les tâches de récupération ont été définies.
- Un fichier de licence valide est importé pour pouvoir exécuter Sophos SafeGuard en environnement de production.

Le SafeGuard Policy Editor démarre dès que l'assistant de configuration se ferme.

8 Copie de la stratégie par défaut pour modification

1. Dans la zone de navigation du SafeGuard Policy Editor, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation **Stratégies**, sous **Groupes de stratégies**, cliquez avec le bouton droit de la souris sur **Stratégie par défaut** et cliquez sur **Sauvegarder la stratégie**.
3. Saisissez un nom de fichier et un emplacement de stockage pour la copie (XML) et cliquez sur **Enregistrer**.
4. Dans la fenêtre de navigation, cliquez avec le bouton droit de la souris sur **Groupes de stratégie**, puis cliquez sur **Restaurer une stratégie**.
5. Sélectionnez la nouvelle copie de la stratégie (XML) et cliquez sur **Ouvrir**.

Une copie de la stratégie par défaut incluant tous les éléments de la stratégie individuelle est importée dans le SafeGuard Policy Editor.

Personnalisez ensuite la copie de la stratégie par défaut pour configurer une liste de comptes de service pour les tâches postérieures à l'installation sur les ordinateurs d'extrémité. Ainsi, le personnel de maintenance peut accéder et préconfigurer les ordinateurs suite à l'installation du logiciel de chiffrement sans avoir à être "propriétaire" de l'ordinateur.

9 Configuration des ordinateurs d'extrémité pour les tâches de service suite à l'installation

Le personnel de maintenance pourrait avoir besoin d'accéder et de préconfigurer l'ordinateur d'extrémité une fois que le logiciel de chiffrement a été installé, par exemple, via un déploiement central. Toutefois, le premier utilisateur qui se connecte à l'ordinateur suite à l'installation du logiciel de chiffrement active la POA et est ajouté comme utilisateur Sophos SafeGuard de l'ordinateur. Pour éviter cela, vous pouvez les inclure dans une liste de comptes de service. Les membres du personnel de maintenance inclus dans cette liste peuvent alors se connecter au système d'exploitation de l'ordinateur suite à l'installation et effectuer les tâches nécessaires sans activer la POA et sans être ajouté comme utilisateur Sophos SafeGuard.

Pour configurer une liste de comptes de service :

1. Dans la zone de navigation du SafeGuard Policy Editor, cliquez sur **Stratégies**.
2. Dans la fenêtre de navigation **Stratégies**, cliquez avec le bouton droit de la souris sur **Listes de comptes de service**, cliquez sur **Nouveau** et sur **Listes de comptes de service**.
3. Saisissez un nom pour la liste et cliquez sur **OK**.
4. Dans la fenêtre de navigation **Listes de comptes de service**, sélectionnez la nouvelle liste.
5. Cliquez avec le bouton droit de la souris dans la zone d'action, à droite, et sélectionnez **Ajouter** dans le menu contextuel. Une nouvelle ligne utilisateur est ajoutée.
6. Saisissez le **Nom d'utilisateur** et le **Nom du domaine** dans les colonnes respectives, puis appuyez sur Entrée. Répétez cette étape pour ajouter d'autres utilisateurs. Pour plus d'informations, consultez le chapitre *Informations supplémentaires pour la saisie de nom d'utilisateur et de domaine* de l'aide administrateur.
7. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications dans la base de données.

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

8. Dans la fenêtre de navigation, sous **Éléments de stratégie**, sélectionnez l'élément de stratégie **Authentification** qui a été copié.
9. Sous **Options de connexion**, sélectionnez la nouvelle liste créée dans **Liste de comptes de service**.
10. Cliquez sur l'icône **Enregistrer** de la barre d'outils pour enregistrer vos modifications.

La liste de comptes de service est configurée. L'élément de stratégie **Authentification** et le groupe de stratégies dont il fait partie sont respectivement mis à jour. Publiez ensuite la stratégie modifiée dans un package de configuration.

Remarque :

Vous pouvez modifier d'autres paramètres de stratégie selon vos besoins. Par exemple, pour personnaliser la POA, configurer le chiffrement ou activer l'éveil par appel réseau. Pour plus d'informations, consultez le chapitre *Paramètres de stratégie* de l'aide administrateur.

10 Publication de la stratégie dans un package de configuration

Pour mettre les stratégies à disposition sur l'ordinateur d'extrémité, publiez-les d'abord dans un package de configuration.

1. Démarrez le SafeGuard Policy Editor, sélectionnez **Outils** et cliquez sur **Outil de package de configuration**.
2. Cliquez sur **Ajouter un package de configuration**.
3. Donnez un nom au package de configuration.
4. Sélectionnez un **Groupe de stratégies** modifié à l'étape précédente et qui sera appliqué aux ordinateurs d'extrémité.
5. Spécifiez un emplacement de stockage pour le package de configuration.
6. Cliquez sur **Créer un package de configuration**.
7. Cliquez sur **Fermer**.

La stratégie est publiée dans un package de configuration (MSI) à l'emplacement spécifié. Installez ensuite le logiciel de chiffrement Sophos SafeGuard et le package de configuration sur les ordinateurs d'extrémité.

11 Installation du logiciel de chiffrement et du package de configuration sur les ordinateurs d'extrémité

1. Préparez l'ordinateur d'extrémité au chiffrement
2. Pour vous familiariser avec Sophos SafeGuard, commencez par installer le logiciel de chiffrement sur un ordinateur réservé à l'évaluation. Utilisez un ordinateur différent de celui sur lequel le SafeGuard Policy Editor est installé.
3. Connectez-vous une première fois.
4. Utilisez vos propres outils pour créer et distribuer les packages d'installation et de configuration afin de configurer de manière centralisée le logiciel de chiffrement sur les ordinateurs d'extrémité.

11.1 Préparation des ordinateurs d'extrémité au chiffrement

- Assurez-vous qu'un compte utilisateur est configuré et activé. L'utilisateur doit avoir un mot de passe.
- Créez une sauvegarde complète des données.
- Fermez toutes les applications ouvertes.
- Assurez-vous de disposer des droits d'administrateur Windows.
- Vérifiez que l'espace disque disponible est suffisant.

- 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 conseillons d'installer une version mise à jour de la liste de configuration matérielle avant de procéder au déploiement de Sophos SafeGuard sur l'ordinateur d'extrémité. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant : <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

Pour plus d'informations, consultez le chapitre *Raccourcis clavier pris en charge* de l'aide administrateur. Consultez aussi :

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

- Recherchez les erreurs sur le 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 exécuter de nouveau 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.

defrag %drive%

Pour plus d'informations, consultez :

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

- Désinstallez les gestionnaires d'initialisation tiers, tels que PRONetworks Boot Pro et Boot-US.

- Nous vous conseillons de nettoyer le MBR (master boot record). Pour installer Sophos SafeGuard, votre MBR doit être unique et sain. Suite à l'utilisation d'outils d'image/de clone sur l'ordinateur d'extrémité, il se peut que le MBR ne soit plus sain.

Démarrez l'ordinateur à partir d'un DVD Windows et utilisez la commande **FIXMBR** dans la Console de récupération Windows. Pour plus d'informations, consultez :

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

- Si la partition d'initialisation de l'ordinateur d'extrémité a été convertie du format FAT au format NTFS, mais que l'ordinateur n'a pas encore été redémarré, n'installez pas Sophos SafeGuard avant d'avoir redémarré l'ordinateur. Autrement, 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.

11.2 Installation d'une version d'évaluation

Procédez à l'installation d'une version d'évaluation du logiciel de chiffrement sur un ordinateur différent de celui sur lequel le SafeGuard Policy Editor est installé.

1. Préparez l'installation sur les ordinateurs d'extrémité, (voir [Préparation des ordinateurs d'extrémité au chiffrement](#) à la page 10).
2. Ouvrez une session sur l'ordinateur d'extrémité en tant qu'administrateur.
3. Installez le package de préinstallation **SGxClientPreinstall.msi**, qui fournit à l'ordinateur d'extrémité la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.
4. Installez le logiciel de chiffrement sur l'ordinateur d'extrémité. Cliquez deux fois sur les packages (MSI) suivants pour démarrer l'assistant d'installation du logiciel de chiffrement. Il vous guidera tout au long des étapes nécessaires.

| Sophos SafeGuard Disk Encryption | Sophos SafeGuard Easy |
|--|--|
| SDEClient.msi pour la variante 32 bits ou SDEClient_x64.msi pour la variante 64 bits. | SGNClient.msi pour la variante 32 bits. SGNClient_x64.msi pour la variante 64 bits. |

5. Acceptez les valeurs par défaut dans les boîtes de dialogue suivantes.
6. Si vous y êtes invité, sélectionnez le type d'installation **Complète**.

Sophos SafeGuard Easy : SafeGuard Device Encryption et SafeGuard Data Exchange sont installés. Pour plus d'informations sur les packages d'installation "Client" disponibles, consultez le chapitre *Installation* de l'aide administrateur.

Sophos SafeGuard Disk Encryption : SafeGuard Device Encryption est installé. SafeGuard Data Exchange n'est pas disponible.

7. Acceptez les valeurs par défaut dans toutes les boîtes de dialogue suivantes pour terminer l'assistant d'installation.
8. Accédez à l'emplacement d'enregistrement du package de configuration (MSI).
9. Installez ce package de configuration sur l'ordinateur d'extrémité. Assurez-vous que tous les packages d'installation obsolètes ont été supprimés de l'ordinateur d'extrémité.

Sophos SafeGuard est installé et configuré conformément aux stratégies déjà créées sur l'ordinateur d'extrémité. Connectez-vous ensuite à l'ordinateur après l'installation, soit pour effectuer les tâches postérieures à l'installation (à l'aide d'un compte de service) soit pour prendre possession de l'ordinateur en tant qu'utilisateur normal.

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 msiexec. Pour plus d'informations, reportez-vous au chapitre *Raccourcis clavier pris en charge dans l'authentification au démarrage* de l'aide administrateur. Consultez aussi :

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

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

11.3 Première connexion à l'aide d'un compte de service

Connectez-vous à l'aide d'un compte de service si vous souhaitez effectuer les tâches postérieures à l'installation sur l'ordinateur.

1. Redémarrez l'ordinateur d'extrémité suite à l'installation. La boîte de dialogue de connexion Windows apparaît.

Sous Windows Vista et Windows 7, appuyez d'abord sur CTRL+ALT+SUPPR pour démarrer la session. L'administrateur peut désactiver ce paramètre dans la console MMC de l'éditeur d'objet de stratégie de groupe sous **Paramètres Windows > Paramètres de sécurité > Stratégies locales > Désactiver les options de sécurité** (pour la connexion interactive, il n'est pas nécessaire d'appuyer sur CTRL+ ALT+ SUPPR).

2. Connectez-vous à Windows à l'aide de votre compte de service : saisissez le domaine et les codes d'accès définis auparavant dans la liste des comptes de service dans le SafeGuard Policy Editor.

Vous êtes connecté à Windows en tant qu'utilisateur invité. L'authentification au démarrage n'est pas activée et vous n'êtes pas propriétaire de cet ordinateur. Vous pouvez procéder aux tâches postérieures à l'installation nécessaires.

11.4 Première connexion sans compte de service

1. Redémarrez l'ordinateur. La connexion automatique à Sophos SafeGuard apparaît suivi de la connexion à Windows.

Sous Windows Vista et Windows 7, appuyez d'abord sur CTRL+ALT+SUPPR pour démarrer la connexion automatique et vous connecter. L'administrateur peut désactiver ce paramètre dans la console MMC de l'éditeur d'objet de stratégie de groupe sous **Paramètres Windows > Paramètres de sécurité > Stratégies locales > Désactiver les options de sécurité** (pour la connexion interactive, il n'est pas nécessaire d'appuyer sur CTRL+ ALT+ SUPPR).

2. Saisissez votre nom d'utilisateur et votre mot de passe Windows.
3. Redémarrez de nouveau l'ordinateur. L'authentification au démarrage de Sophos SafeGuard est activée.
4. Saisissez votre nom d'utilisateur et votre mot de passe Windows. Vous êtes automatiquement connecté à Windows.

L'authentification au démarrage est maintenant activée. Vous êtes enregistré en tant qu'utilisateur Sophos SafeGuard. Une infobulle de confirmation apparaît. À votre prochaine ouverture de session, vous devrez uniquement saisir vos codes d'accès Windows à l'authentification au démarrage.

Le chiffrement initial démarre automatiquement. Vous pouvez continuer à travailler et il n'est pas nécessaire de redémarrer l'ordinateur à la fin du chiffrement. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente sans nécessiter aucune

intervention de l'utilisateur. Retrouvez plus d'informations dans l'aide utilisateur (chapitres *Première connexion après l'installation de Sophos SafeGuard* et *Chiffrement de données*).

11.5 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 des ordinateurs d'extrémité au chiffrement](#) à la page 10.
2. Ouvrez une session sur l'ordinateur administrateur en tant qu'administrateur.
3. Créez un dossier appelé **Logiciels** à utiliser pour centraliser toutes les applications.
4. 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 | 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, vous pouvez par exemple installer la variante du package *_x64.msi. Tous les packages d'installation <Client> requis sont inclus à la livraison du produit.</p> <p>Remarque :</p> <p>Pour plus d'informations sur tous les packages d'installation <Client> disponibles, consultez le chapitre <i>Installation</i> de l'aide administrateur.</p> |
| Package de configuration pour ordinateurs d'extrémité | Utilisez le package de configuration créé auparavant dans le SafeGuard Policy Editor. Veillez à supprimer tous les packages de configuration obsolètes. |
| 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, consultez le chapitre <i>Commande pour l'installation centralisée</i> de l'aide administrateur ou consultez :</p> <p>http://msdn.microsoft.com/fr-fr/library/aa367988(VS.85).aspx</p> |

5. Pour créer le script, ouvrez une invite de commande et saisissez les commandes de script. Pour plus d'informations, voir [Exemple de commande de script](#) à la page 15.
6. Distribuez la préinstallation, le package "Client", le package de configuration et 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, reportez-vous au chapitre *Raccourcis clavier pris en charge dans l'authentification au démarrage* de l'aide administrateur. Consultez aussi :

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

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

11.6 Exemple de commande de script

```
msiexec /i F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi  
/qn
```

```
msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi /qn
```

```
/L*VX  
G:\Temp\Sophos\SafeGuard\%nomordinateur%\SDEClient_inst.log
```

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

```
msiexec /i F:\Software\Sophos\SafeGuard\SDEClientConfig.msi  
/qn
```

Cette commande a l'effet suivant :

```
■ msiexec /i  
F:\Software\Sophos\SafeGuard\SGxClientPreinstall.msi
```

Installe le package de préinstallation de Sophos SafeGuard à partir de l'emplacement de stockage défini dans le répertoire d'installation par défaut : **C:\Program Files\Sophos\Sophos SafeGuard**. Les ordinateurs d'extrémité sont fournis avec la configuration requise pour garantir la réussite de l'installation du logiciel de chiffrement.

```
■ msiexec /i F:\Software\Sophos\SafeGuard\SDEClient.msi
```

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

Installe le logiciel de chiffrement, ici SafeGuard Device Encryption avec l'authentification au démarrage à partir de l'emplacement de stockage défini dans le répertoire d'installation par défaut : **C:\Program Files\Sophos\Sophos SafeGuard**.

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

Installe le package de configuration à partir de l'emplacement de stockage spécifié dans le répertoire d'installation par défaut.

```
■ /L*VX  
G:\Temp\Sophos\SafeGuard\%nomordinateur%__SDEClient_inst.log
```

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

```
■ /qn
```

Procède à l'installation sans intervention de l'utilisateur et n'affiche pas d'interface utilisateur.

12 Récupération d'un mot de passe oublié

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

- L'utilisateur peut le récupérer via Local Self Help. Nous vous conseillons d'utiliser cette méthode.
- Le support peut le récupérer via une procédure challenge/réponse.

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

1. L'utilisateur saisit son nom d'utilisateur dans l'authentification au démarrage, sur l'ordinateur d'extrémité.
Le bouton **Récupération** devient actif.
2. L'utilisateur clique sur **Récupération**.
 - Si seule la méthode Local Self Help est activée sur l'ordinateur d'extrémité pour la récupération de la connexion, elle démarre automatiquement.
 - Si les méthodes Local Self Help et challenge/réponse sont disponibles pour la récupération de la connexion, l'utilisateur clique sur **Local Self Help**.
3. Dans les cinq boîtes de dialogue suivantes, l'utilisateur répond à un nombre défini de questions sélectionnées aléatoirement parmi les questions stockées sur l'ordinateur d'extrémité. Après avoir répondu à la dernière, l'utilisateur confirme ses réponses en cliquant sur **OK**.
4. Dans la boîte de dialogue suivante, l'utilisateur peut voir le mot de passe en appuyant sur la touche Entrée, sur la barre d'espace ou en cliquant sur la case bleue.
Le mot de passe s'affiche pendant 5 secondes maximum. Ensuite, le processus de démarrage continue automatiquement. L'utilisateur peut immédiatement masquer le mot de passe en appuyant de nouveau sur la touche Entrée, sur la barre d'espace ou en cliquant de nouveau sur la case bleue.
5. Après avoir lu le mot de passe, l'utilisateur clique sur **OK**.

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

12.2 Récupération d'un mot de passe oublié via challenge/réponse

Conditions préalables :

Le fichier de récupération de clé créé pour chaque ordinateur d'extrémité lors de l'installation du logiciel de chiffrement Sophos SafeGuard doit être accessible au support et son nom doit être connu. La méthode challenge/réponse doit être activée via une stratégie sur l'ordinateur d'extrémité.

Remarque :

Nous vous recommandons d'utiliser en priorité Local Self Help pour récupérer un mot de passe oublié. Local Self Help permet à l'utilisateur d'afficher le mot de passe actuel et de continuer à l'utiliser. Ainsi, il n'a pas besoin de réinitialiser le mot de passe ou de recourir à l'assistance technique.

1. L'utilisateur saisit son nom d'utilisateur dans l'authentification au démarrage, sur l'ordinateur d'extrémité. Le bouton **Récupération** devient actif.

2. L'utilisateur clique sur **Récupération**.
 - Si seule la méthode challenge/réponse est activée pour la récupération de la connexion, elle démarre automatiquement.
 - Si les méthodes challenge/réponse et Local Self Help sont disponibles pour la récupération de la connexion, l'utilisateur clique sur **Challenge/réponse**.

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

3. L'utilisateur clique sur **Suivant**. Un code de challenge généré de manière aléatoire s'affiche.
4. L'utilisateur contacte le support. Il lui fournit le nom du fichier de récupération de clé requis ainsi que le code de challenge.
5. Dans le SafeGuard Policy Editor, le support lance l'**Assistant de récupération**.
6. Le support sélectionne le type de récupération **Client Sophos SafeGuard**, confirme la clé et le code de challenge, puis sélectionne l'action de récupération souhaitée **Initialisation sans connexion utilisateur**.

Un code de réponse sous la forme d'une chaîne de caractères ASCII est généré puis affiché.

7. Le support transmet le code de réponse à l'utilisateur, par exemple par téléphone ou message texte.
8. Sur l'ordinateur d'extrémité, dans l'assistant challenge/réponse, l'utilisateur clique sur **Suivant** pour saisir le code de réponse fourni. L'ordinateur peut démarrer à partir de l'authentification au démarrage.
9. Dans la boîte de dialogue d'ouverture de session Windows, l'utilisateur ne connaît pas le mot de passe 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 vous conseillons d'utiliser les méthodes de réinitialisation de mot de passe Windows.
 - 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.

10. L'utilisateur saisit le nouveau mot de passe Windows fourni par le support. L'utilisateur modifie ensuite ce mot de passe immédiatement en choisissant une valeur connue de lui seul.
11. Sophos SafeGuard détecte que le nouveau choix de mot de passe ne correspond pas au mot de passe Sophos SafeGuard utilisé actuellement au niveau de l'authentification au démarrage. L'utilisateur est alors invité à saisir son ancien mot de passe Sophos SafeGuard et, puisqu'il a oublié son mot de passe, il doit cliquer sur **Annuler**.
12. Dans Sophos SafeGuard, 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.
13. Un nouveau certificat utilisateur est créé en fonction du nouveau choix de mot de passe Windows.

L'utilisateur peut ouvrir une session sur l'ordinateur, se connecter de nouveau à l'authentification au démarrage avec son nouveau mot de passe et pourra utiliser celui-ci pour ses prochaines ouvertures de session.

13 Aide sur les tâches générales

Cette section vous indique où trouver les informations relatives à la réalisation des tâches générales. Retrouvez plus d'informations dans l'aide administrateur, dans l'aide utilisateur ou dans le guide des outils de Sophos SafeGuard.

| Tâche | Manuel/Aide |
|--|--|
| Configuration des instances supplémentaires du SafeGuard Policy Editor | Aide administrateur, Configuration des instances supplémentaires du SafeGuard Policy Editor |
| Garantie du bon fonctionnement de l'authentification au démarrage | Aide administrateur/aide utilisateur : raccourcis clavier pris en charge dans l'authentification au démarrage |
| Affichage des informations spécifiques à Sophos SafeGuard sur l'ordinateur d'extrémité | Aide utilisateur : icône de la barre d'état système et infobulle |
| Création et regroupement des stratégies | Aide administrateur : utilisation de stratégies |
| Exportation des certificats | Aide administrateur : exportation des certificats d'entreprise et du responsable de la sécurité. |
| Création de l'accès administratif aux ordinateurs d'extrémité (comptes d'accès à l'authentification au démarrage). | Aide administrateur : accès administratif aux ordinateurs d'extrémité |
| Récupération de l'accès aux données chiffrées | Aide administrateur : challenge/réponse à l'aide de clients virtuels |
| Récupération d'un Master Boot Record corrompu | Guides des outils : restauration d'un MBR corrompu |
| Mise à niveau de SDE 4.6x ou de SGE 4.3x - 4.5x à Sophos SafeGuard | Aide administrateur : mise à niveau de SafeGuard Easy 4.x/SophosDisk Encryption 4.x vers Sophos SafeGuard 5.6x |

14 Support technique

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

- Rendez-vous sur le forum SophosTalk (anglais) à l'adresse <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur 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 du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte du ou des messages d'erreur.

15 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.