

SOPHOS

Sophos SafeGuard Disk Encryption 4.60 Guide de démarrage

Date du document: Juin 2009



Sommaire

1	À propos de ce guide.....	3
2	À propos du chiffrement de disque et de l'authentification avant amorçage.....	3
3	Quel est l'impact du chiffrement sur la gestion de l'ordinateur ou du réseau ?	4
4	Quelles sont les étapes clés ?	5
5	Vérification de la configuration requise	5
6	Installation d'évaluation	6
7	Attribution de droits d'administration.....	8
8	Installation des outils d'administration	9
9	Configuration du logiciel de chiffrement	10
10	Déploiement du logiciel de chiffrement sur les ordinateurs des utilisateurs finaux.....	11
11	Récupération d'un mot de passe oublié.....	13
12	Récupération de l'accès au système.....	14
13	Assistance relative aux tâches courantes.....	14
14	Support technique.....	15
15	Copyright.....	15

1 À propos de ce guide

Ce guide vous explique comment installer et configurer Sophos SafeGuard Disk Encryption (SDE) afin de protéger les ordinateurs de votre entreprise contre les accès non autorisés.

2 À propos du chiffrement de disque et de l'authentification avant amorçage

Le logiciel SDE chiffre l'ensemble du contenu du disque dur et ce, de manière parfaitement transparente. L'utilisateur n'a pas besoin de sélectionner le type de données à chiffrer. De plus, le déchiffrement de données s'exécute en arrière-plan.

Grâce à l'authentification avant amorçage, seul un utilisateur Sophos SafeGuard Disk Encryption enregistré sur un ordinateur peut s'y connecter. Les clés de chiffrement et de déchiffrement requises sont calculées de manière dynamique. Elles sont ensuite chiffrées et stockées sur le disque dur. Ces clés ne peuvent être utilisées que pour le démarrage du système d'exploitation, une fois l'utilisateur connecté à l'ordinateur au moyen des données d'identification SDE adéquates.

Les avantages de Sophos SafeGuard Disk Encryption sont les suivants :

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

3 Quel est l'impact du chiffrement sur la gestion de l'ordinateur ou du réseau ?

Informations importantes :

- En général, vous pouvez utiliser des outils de gestion système comme Microsoft SMS, Tivola ou NetInstall avec Sophos SafeGuard Disk Encryption.
- Sophos SafeGuard Disk Encryption prend également en charge le logiciel Lenovo Rescue and Recovery™. Par contre, les outils permettant de faire une image du disque ne sont pris en charge et n'ont pas été testés avec notre produit.
- Sophos SafeGuard Disk Encryption faut être spécialement configurer pour Wake-On-LAN. Pour utiliser Wake-On-LAN vous devrez activer la fonction Wake-On-LAN lors de la configuration, au moyen des **paramètres avancés**, voir [Configuration du logiciel de chiffrement](#) sur page 10.

- Créez un service de support technique, afin de garantir la récupération des données en cas d'urgence. Le logiciel Sophos SafeGuard Disk Encryption propose des fonctions de récupération conviviales, en cas d'oubli d'un mot de passe, voir [Récupération d'un mot de passe oublié](#) sur page 13 .

Ainsi, vous devez créer un compte d'utilisateur « Helpdesk » et lui accorder le droit de modifier les paramètres d'utilisateur. Pour ce faire, utilisez les **paramètres avancés** lors de la préconfiguration du logiciel de chiffrement, voir [Configuration du logiciel de chiffrement](#) sur page 10.

Consultez l'aide de Sophos SafeGuard Disk Encryption pour en savoir plus et aussi le sujet suivant dans la base de connaissances :

<http://www.sophos.com/support/knowledgebase/article/56457.html>.

- Au cours de l'installation, vous devez définir un mot de passe initial pour l'utilisateur par défaut (USER). Les utilisateur finaux ont besoin de ce mot de passe pour ouvrir une session de Sophos SafeGuard Disk Encryption pour la première fois. Ils sont invités à modifier ce mot de passe à la première ouverture de session.
- Pour pouvoir administrer Sophos SafeGuard Disk Encryption, vous devez disposer d'un mot de passe spécifique SYSTEM, à définir lors de l'installation. N'oubliez pas ce mot de passe et stockez-le à un emplacement sûr, voir [Installation des outils d'administration](#) sur page 9.
- Pour être toujours en mesure d'accéder au fichier journal d'installation lorsque vous déployez le logiciel de chiffrement sur les ordinateurs des utilisateurs finaux, assurez vous de l'enregistrer sur un chemin UNC sur le réseau.

4 Quelles sont les étapes clés ?

Pour sécuriser votre réseau, configurez SDE sur l'ordinateur de l'administrateur et déployez-le ensuite sur les ordinateurs des utilisateurs finaux. Les étapes clés sont les suivantes :

- Vérification de la configuration requise
- Installation d'évaluation
- Attribution de droits d'administration
- Installation des outils d'administration
- Configuration du logiciel de chiffrement
- Déploiement du logiciel de chiffrement sur les ordinateurs des utilisateurs finaux

5 Vérification de la configuration requise

Configuration matérielle requise

- L'installation nécessite un minimum de 25 Mo d'espace disque. La configuration minimale requise est la même que celle du système d'exploitation utilisé.
- Le produit prend en charge un maximum de quatre disques durs par machine et de huit partitions par disque dur.

Configuration logicielle requise

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

- "Windows 2000 Professionnel Service Pack 4 (SP 4)
- "Windows XP Édition familiale Service Pack 2 (SP 2)
- "Windows XP Professionnel Service Pack 2 (SP 3)

L'utilisation de Service Packs à jour est recommandée.

6 Installation d'évaluation

Pour vous familiariser avec Sophos SafeGuard Disk Encryption, installez le logiciel de chiffrement sur l'ordinateur d'évaluation.

6.1 Préparation de l'installation

Vous devez d'abord :

- fermer toutes les applications ouvertes ;
- vous assurer que vous disposez de suffisamment d'espace disque ;
- réaliser une sauvegarde complète de vos supports de données ;
- vous assurer que les partitions du ou des disques durs sont entièrement formatées et qu'une lettre de lecteur leur est attribuée ;

- vérifier les défauts éventuels de votre ou de vos disques durs avec la commande suivante :
`chkdsk %systemdrive% /F /V /L /X`

Dans certains cas, vous pourriez être invité à redémarrer l'ordinateur et d'exécuter `chkdsk` de nouveau.

Vous trouverez plus d'informations à ce sujet dans la base de connaissances <http://www.utimaco.com/myutimaco>, article 107081.

6.2 Installation du logiciel de chiffrement

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

6. Dans **Mots de passe**, saisissez et confirmez un mot de passe pour les deux utilisateurs SDE standard sur les ordinateurs des utilisateurs finaux : utilisateur du système (administrateur du niveau le plus élevé SYSTEM) et utilisateur par défaut (USER).

Remarque: Le mot de passe de l'utilisateur par défaut (USER) est le mot de passe initiale. Vous êtes invités à modifier ce mot de passe à la première ouverture de session de Sophos SafeGuard Disk Encryption.

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

Le chiffrement par défaut et les paramètres de sécurité (chiffrement de la partition C: et authentification avant amorçage activée) sont définis automatiquement. Pour modifier les paramètres par défaut, cochez la case **Afficher les paramètres avancés** dans **Mots de passe** et effectuez les modifications souhaitées dans les boîtes de dialogue **Configuration du poste de travail**.

7. Acceptez les propositions par défaut dans toutes les boîtes de dialogue suivantes.

L'installation est terminée. Vous devez ensuite exécuter des tâches de post-installation.

6.3 Exécution des tâches de post-installation

Suivez les étapes ci-dessous :

1. Redémarrez votre ordinateur. La boîte de dialogue d'ouverture de session Windows s'affiche.
2. Saisissez vos données d'identification Windows.
Le chiffrement initial démarre automatiquement. Cette étape peut prendre un certain temps. Vous pouvez continuer à travailler sur l'ordinateur. Le noyau du système est sauvegardé automatiquement.
3. Redémarrez votre ordinateur de nouveau. La boîte de dialogue d'authentification avant amorçage de Sophos SafeGuard Disk Encryption s'affiche.
4. Saisissez le mot de passe utilisateur Sophos SafeGuard Disk Encryption défini au cours de l'installation.
5. Vous êtes invité à modifier ce mot de passe.
6. Vous êtes de nouveau invité à saisir vos données d'identification Windows.
7. Confirmez de nouveau et vous serez automatiquement dirigé vers Windows. Vous êtes connecté à votre ordinateur.

Lorsque vous redémarrez la prochaine fois, vous devez seulement saisir le mot de passe utilisateur Sophos SafeGuard Disk Encryption au moment de l'authentification avant amorçage et vous serez automatiquement connecté à Windows.

7 Attribution de droits d'administration

Avant de procéder à l'installation sur le réseau, décidez quels utilisateurs disposeront de droits d'administration.

Par défaut, l'installation crée deux types d'utilisateurs :

- **L'utilisateur du système** (administrateur du niveau le plus élevé SYSTEM) dispose de tous les droits d'accès et de configuration des ordinateurs des utilisateurs finaux et d'exécution des tâches d'urgence. Seul l'administrateur SYSTEM peut accorder des droits à d'autres utilisateurs.

Remarque : seul l'utilisateur du système (administrateur du niveau le plus élevé SYSTEM) doit connaître le mot de passe SYSTEM, qu'il doit conserver en lieu sûr. S'il perd ce mot de passe, il ne sera plus possible d'accéder aux ordinateurs des utilisateurs finaux en cas d'urgence !

- **L'utilisateur** a uniquement le droit d'ouvrir une session sur son ordinateur et de modifier son mot de passe utilisateur SDE. Les utilisateurs ne disposent d'aucun droit d'administration. Cependant, il est possible de créer d'autres types d'utilisateurs dotés de droits permettant d'exécuter des tâches spécifiques. Ainsi, vous souhaitez peut-être accorder à un technicien d'assistance le droit de modifier les paramètres d'utilisateur. Pour ce faire, utilisez les **paramètres avancés** lors de la préconfiguration du logiciel de chiffrement voir [Configuration du logiciel de chiffrement](#) sur page 10.

Consultez l'aide de Sophos SafeGuard Disk Encryption pour en savoir plus et aussi le sujet suivant dans la base de connaissances :

<http://www.sophos.com/support/knowledgebase/article/56457.html>.

8 Installation des outils d'administration

Pour le déploiement du logiciel de chiffrement sur les ordinateurs des utilisateurs finaux les outils d'administration doivent être installés sur l'ordinateur de l'administrateur. Cependant, vous devez d'abord :

- fermer toutes les applications ouvertes ;
- vous assurer que vous disposez de suffisamment d'espace disque.

Pour installer les outils d'administration, suivez les étapes ci-dessous :

1. Ouvrez une session en tant qu'administrateur.
2. Cliquez deux fois sur le programme d'installation téléchargé précédemment. Dans la fenêtre du programme d'installation, cliquez sur **Installer** pour extraire le contenu du programme d'installation sur votre ordinateur et lancer l'assistant d'installation. Les instructions du **Programme d'installation Sophos SafeGuard Disk Encryption** vous guident à travers les étapes nécessaires.

Les instructions du **Programme d'installation Sophos SafeGuard Disk Encryption** vous guident à travers les étapes nécessaires.

3. Acceptez les propositions par défaut dans les boîtes de dialogue suivantes.
4. Dans **Sélection du type d'installation**, choisissez **Installation distribuée sur les ordinateurs du réseau** et cliquez sur **Suivant**.
5. Acceptez les propositions par défaut dans toutes les boîtes de dialogue suivantes.

L'installation des outils d'administration de SDE est terminée. Utilisez ensuite les outils d'administration pour configurer SDE avant son installation sur les ordinateurs des utilisateurs finaux.

9 Configuration du logiciel de chiffrement

Suivez les étapes ci-dessous :

1. Ouvrez l'**Assistant de configuration pour le déploiement** via le dossier Sophos SafeGuard du menu **Démarrer**.
2. Dans **Types de fichier de configuration**, sélectionnez **Installation** et cliquez sur **Suivant**.
3. Dans **Fichier de configuration de base (facultatif)**, acceptez le fichier par défaut et cliquez sur **Suivant** pour créer un nouveau fichier.

Un fichier de configuration de base constitue une base permettant d'automatiser l'installation et d'harmoniser la configuration de Sophos SafeGuard Disk Encryption sur plusieurs ordinateurs d'utilisateurs finaux.


4. Dans **Mots de passe**, saisissez et confirmez un mot de passe pour les deux utilisateurs SDE standard sur les ordinateurs des utilisateurs finaux : utilisateur du système (administrateur du niveau le plus élevé SYSTEM) et utilisateur par défaut (USER).

Remarque : Le mot de passe de l'utilisateur par défaut (USER) est le mot de passe initiale. Les utilisateurs finaux sont invités à modifier ce mot de passe à la première ouverture de session de Sophos SafeGuard Disk Encryption.

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

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

Remarque : Les paramètres avancés vous permettent également de modifier les paramètres par défaut de chiffrement et de sécurité (chiffrement de la partition C: et authentification avant amorçage activée).

5. Sous **Configuration du poste de travail**, sélectionnez **Utilisateurs**. Cliquez ensuite sur l'icône de création d'un utilisateur .
6. Dans le champ **Nouveau nom de l'utilisateur** de la boîte de dialogue **Nouvel utilisateur**, entrez le nom `Helpdesk`. Les fonctionnalités attribuées à l'utilisateur « Helpdesk » sont affichées. Définissez les options comme suit :
 - **Changement du mot de passe permis :** défini sur **Non**.
 - **Mot de passe :** Cliquez sur **Mot de passe** et ensuite sur [...] pour configurer un mot de passe. Une boîte de dialogue s'affiche. Entrez un nouveau mot de passe pour l'utilisateur « Helpdesk », puis confirmez-le.
 - **Droits :** Cliquez sur **Droits** et ensuite sur [...]. Dans la boîte de dialogue **Droits de**

l'utilisateur, double-cliquez sur la case **Modifier les paramètres d'utilisateurs** de manière à ce que l'utilisateur «Helpdesk» puisse définir un nouveau mot de passe utilisateur et autoriser une ouverture de session unique. Cochez **Désinstaller** pour permettre à l'utilisateur « Helpdesk » de désinstaller SDE.

Cliquez sur **Suivant**.

7. Enregistrez le fichier en tant que fichier de configuration de base et acceptez l'emplacement d'enregistrement par défaut.
8. Cliquez sur **Terminer**.

La configuration de base `Install.cfg` est créée. Vous devez alors déployer le logiciel de chiffrement sur les ordinateurs des utilisateurs finaux.

10 Déploiement du logiciel de chiffrement sur les ordinateurs des utilisateurs finaux

Avant de déployer le logiciel de chiffrement sur les ordinateurs des utilisateurs finaux, voir [Préparation de l'installation](#) sur page 6.

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

Exemple de script :

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

```
/i C:\Software\Sophos\SDE.msi
```

Installe (à partir de l'emplacement de stockage spécifié) le package d'installation Sophos SafeGuard Disk Encryption dans le répertoire d'installation par défaut

C:\Programmes\Sophos\SafeGuard Disk Encryption. L'élément suivant est installé par défaut : chiffrement de la partition C: y compris l'activation de l'authentification avant amorçage et la connexion automatique sécurisée à Windows.

```
/L*VX \\%distributionserver%\Sophos\%computername%_SDE_inst.log
```

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

```
CFGFILE=C:\Software\Sophos\Install.cfg
```

Indique le fichier de configuration de base devant être appliqué sur les ordinateurs des utilisateurs finaux.

```
/QN
```

Procède à l'installation sans intervention de l'utilisateur et sans afficher une interface utilisateur.

4. Distribuez le package d'installation sur les ordinateurs des utilisateurs finaux.
5. Communiquez le mot de passe SDE par défaut aux utilisateurs finaux et informez-les des tâches de post-installation à exécuter, voir [Exécution des tâches de post-installation](#) sur page 7.

Remarque :

Si vous souhaitez également soumettre l'ordinateur de l'administrateur à une opération de chiffrement avec Sophos SafeGuard Disk Encryption, procédez de l'une des façons suivantes :

- Exécutez le fichier `setup.exe` en mode **Modification**, en choisissant le type **Installation chiffrée sur cet ordinateur**. Acceptez les propositions par défaut dans toutes les boîtes de dialogue.
- Déployez l'installation préconfigurée créée précédemment sur l'ordinateur de l'administrateur.

11 Récupération d'un mot de passe oublié

Si l'utilisateur oublie son mot de passe SDE, le technicien d'assistance peut le réinitialiser en suivant la procédure Requête/Réponse décrite ci-dessous :

Prérequis : l'Assistant de déblocage à distance doit être installé sur l'ordinateur du technicien d'assistance. Le technicien d'assistance doit avoir le droit de modifier les paramètres d'utilisateur.

Consultez l'aide de Sophos SafeGuard Disk Encryption pour en savoir plus.

1. L'utilisateur final démarre l'ordinateur. L'authentification avant amorçage s'affiche.
2. Dans le champ **Mot de passe**, l'utilisateur final appuie sur la touche F9 du clavier.
3. Un code de requête s'affiche sur l'écran de l'ordinateur de l'utilisateur final.
4. L'utilisateur appelle le service d'assistance et communique au technicien d'assistance son identifiant utilisateur et le code de requête.
5. Le technicien d'assistance ouvre l'assistant de déblocage à distance via le dossier Sophos Disk Encryption du menu **Démarrer**.
6. Le technicien d'assistance autorise l'accès à l'ordinateur de l'utilisateur final.
7. Le technicien d'assistance confirme l'identifiant utilisateur et saisit le code de la requête.
8. Le technicien d'assistance donne le droit à l'utilisateur de réinitialiser son mot de passe SDE. Un code de réponse est généré.
9. Le technicien d'assistance communique le code de réponse à l'utilisateur final.
10. L'utilisateur final saisit le code de réponse sous le code de requête.
11. L'utilisateur final réinitialise son mot de passe SDE et peut ensuite continuer à travailler sur son ordinateur.

12 Récupération de l'accès au système

Remarque : Procédez toujours à des sauvegardes régulières et stocker la sauvegarde sur un support amovible ou sur le réseau pour avoir la version la plus récente du noyau système à tout moment .

Pour ce faire, utilisez l'assistant de création d'une disquette de secours dans le dossier Sophos SafeGuard Disk Encryption du menu **Démarrer**. Consultez l'aide de Sophos SafeGuard Disk Encryption pour en savoir plus.

Si l'utilisateur final ne peut plus se connecter au système car le noyau du système a été endommagé, consultez l'article suivant dans la base de connaissances :

<http://www.sophos.com/support/knowledgebase/article/56456.html>.

13 Assistance relative aux tâches courantes

Cette section vous explique où trouver des informations sur l'exécution de tâches courantes.

Consultez l'aide de Sophos SafeGuard Disk Encryption pour en savoir plus.

Tâche	Chapitre de l'aide de Sophos SafeGuard Disk Encryption
Ouverture d'une session Sophos SafeGuard Disk Encryption	Démarrage du système et ouverture de session, Ouverture de session comme utilisateur par défaut
Modification du mot de passe utilisateur Sophos SafeGuard Disk Encryption	Démarrage du système et ouverture de session, Modifier le mot de passe SDE avec la touche [F10]
Verrouillage de l'ordinateur	Sophos SafeGuard Disk Encryption Verrouillage du poste
Attribution de droits d'administration	Création de profils utilisateur
Modification de la configuration de Sophos SafeGuard Disk Encryption	Aperçu de l'administration
Chiffrement d'autres partitions de disque dur	Chiffrement, Configuration du chiffrement
Obtention d'aide sur la réinitialisation d'un mot de passe oublié	Démarrage du système et ouverture de session, Fonction d'aide pour réinitialiser les mots de passe oubliés avec la touche [F9]
Assistance sur la réinitialisation d'un mot de passe oublié	Requête/Réponse
Récupération de l'accès au système	Sauvegarde du noyau du système et création de supports de secours

14 Support technique

Pour obtenir du support technique, consultez <http://www.sophos.com/support>.

Si vous contactez le support technique, fournissez autant d'informations que possible, notamment :

- Le ou les numéro(s) de version(s) des logiciels Sophos
- Le ou les système(s) d'exploitation et niveau(x) de correctif(s)
- Le texte exact de tous les messages d'erreur

15 Copyright

Copyright © 1992 - 2009 Utimaco Safeware AG - a member of the Sophos group

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

Sophos est une marque déposée de Sophos Plc et de Sophos Group.

SafeGuard est une marque déposée de Utimaco Safeware AG - a member of the Sophos group.

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

Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.