

SOPHOS

Sophos SafeGuard Disk Encryption 5.50 Sophos SafeGuard Easy 5.50 Aide utilisateur

Date du document : Août 2010



Table des matières

1	À propos de Sophos SafeGuard.....	2
2	Sauvegarde des clés pour récupération	5
3	Authentification au démarrage	6
4	Authentification au démarrage sous Windows Vista	19
5	Connexion sous Windows Vista.....	23
6	Connexion avec le lecteur d'empreintes digitales de Lenovo.....	25
7	Options de récupération	35
8	Récupération via Local Self Help	36
9	Récupération par Challenge/Réponse.....	48
10	Icône de la barre d'état système et info-bulle	53
11	Extensions de SafeGuard Explorer	56
12	Chiffrement de données.....	58
13	SafeGuard Data Exchange.....	62
14	Sophos SafeGuard et Lenovo Rescue and Recovery.....	79
15	Support technique.....	87
16	Copyright	88

1 À propos de Sophos SafeGuard

Sophos SafeGuard est une solution de sécurité des données fiable, qui utilise une stratégie de chiffrement basée sur une règle pour protéger efficacement les informations sur les ordinateurs finaux. Le chiffrement des données et leur protection contre tout accès non autorisé constituent les principales fonctions de sécurité de Sophos SafeGuard. Pour l'utilisateur final, Sophos SafeGuard est très simple d'utilisation et très intuitif. 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.

L'administration s'effectue via Sophos SafeGuard Policy Editor utilisé pour créer et gérer les stratégies de sécurité et qui propose des fonctions de récupération. Un ordinateur protégé par Sophos SafeGuard reçoit des stratégies via un package de configuration créé par le biais de Sophos SafeGuard Policy Editor. Il est possible de distribuer ce package de configuration en s'appuyant sur les mécanismes de distribution des logiciels de la société ou en installant manuellement un package de configuration sur l'ordinateur.

Remarque: 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 ce manuel.

Les modules suivants sont disponibles pour les ordinateurs protégés par Sophos SafeGuard :

■ SafeGuard Device Encryption

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 connecté automatiquement au système d'exploitation. Vous pouvez également désactiver l'authentification au démarrage. Dans ce cas, l'authentification de l'utilisateur se fait via le système d'exploitation.

Chiffrement basé sur volume

Toutes les données des volumes (y compris les fichiers d'initialisation, les fichiers d'échange, les fichiers inactifs/d'hibernation, les fichiers temporaires, les informations de répertoire, etc.) sont chiffrées de manière transparente sans que l'utilisateur doive modifier ses habitudes de travail ou tenir compte de problèmes de sécurité.

■ SafeGuard Data Exchange

Remarque: SafeGuard Data Exchange et SafeGuard Portable ne sont pas disponibles avec ESDP.

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: Notez que les fonctions disponibles sur votre ordinateur dépendent des paramètres définis dans Sophos SafeGuard Policy Editor. Le responsable de la sécurité définit ces paramètres via des stratégies dans Sophos SafeGuard Policy Editor et les distribue aux ordinateurs finaux. Par conséquent, il se peut que certaines des fonctions décrites dans ce manuel ne soient pas disponibles sur votre ordinateur.

1.1 Fonctions de Sophos SafeGuard

Sophos SafeGuard propose les fonctions suivantes, pour plus de simplicité :

■ Options de récupération de l'authentification au démarrage

Pour la récupération (en cas d'oubli de mot de passe par exemple), Sophos SafeGuard propose les options suivantes :

- En cas d'oubli de mot de passe, vous pouvez utiliser **Local Self Help** pour récupérer l'accès à votre ordinateur sans l'assistance du support. Pour vous connecter à votre ordinateur, il vous suffit de répondre à un certain nombre de questions prédéfinies dans l'authentification au démarrage. L'utilisation de Local Self Help permet d'accéder de nouveau à votre portable, par exemple dans les situations où aucune connexion par téléphone ou réseau n'est disponible (par exemple à bord d'un avion). Pour obtenir plus d'informations sur Local Self Help, voir [Récupération via Local Self Help](#), à la page 36.
- Avec **Challenge/Réponse**, Sophos SafeGuard propose également un mécanisme de récupération avec support, pour les scénarios de récupération classiques. Challenge/Réponse est un système de récupération sécurisé et fiable qui vous aide lorsque vous ne pouvez pas vous connecter à votre ordinateur ou accéder aux données chiffrées. Pour obtenir plus d'informations sur Challenge/Réponse, voir [Récupération par Challenge/Réponse](#), à la page 48.

■ **Sophos SafeGuard Icône de la barre d'état système**

Vous pouvez accéder à toutes les fonctions principales de Sophos SafeGuard via l'icône de la barre d'état système de Sophos SafeGuard. L'icône de la barre d'état système se trouve dans la barre des tâches Windows. Pour obtenir plus d'informations sur l'icône de la barre d'état système, voir [Icône de la barre d'état système et info-bulle](#), à la page 53.

■ **Sophos SafeGuard Extensions de l'Explorateur**

Vous pouvez accéder aux fonctions liées au chiffrement via les entrées correspondantes dans les menus contextuels de l'Explorateur Windows (voir [Extensions de SafeGuard Explorer](#), à la page 56).

Remarque: Notez que les fonctions disponibles sur votre ordinateur dépendent des paramètres définis dans Sophos SafeGuard Policy Editor. Le responsable de la sécurité définit ces paramètres via des stratégies dans Sophos SafeGuard Policy Editor et les distribue aux ordinateurs finaux. Par conséquent, il se peut que certaines des fonctions décrites dans ce manuel ne soient pas disponibles sur votre ordinateur.

2 Sauvegarde des clés pour récupération

Pour la récupération de connexion, Sophos SafeGuard propose une procédure Challenge/Réponse (voir [Récupération par Challenge/Réponse](#), à la page 48) pour l'échange confidentiel d'informations. La procédure Challenge/Réponse est hautement sécurisée et fiable.

Pour rendre possible la récupération par Challenge/Réponse, les données nécessaires doivent être fournies au support. Ces données sont enregistrées dans des fichiers de récupération de clés spécifiques (fichiers .XML).

Lors de la configuration de votre ordinateur via l'installation du package de configuration de Sophos SafeGuard, le fichier de récupération de clé est créé automatiquement à un emplacement spécifié par le responsable de la sécurité. Si le responsable de la sécurité n'a spécifié aucun emplacement, vous êtes invité à enregistrer le fichier manuellement.

Le responsable de la sécurité peut définir un emplacement pour ces fichiers au moment où il crée le package de configuration. Habituellement, les fichiers sont enregistrés dans un répertoire partagé. Le fichier de récupération de clé est alors automatiquement créé à cet emplacement.

Si l'emplacement de fichier défini n'est pas accessible au moment où Sophos SafeGuard tente de créer le fichier, une info-bulle apparaît, un message est enregistré dans le journal des événements système et Sophos SafeGuard tentera d'enregistrer à nouveau le fichier ultérieurement. Si le responsable de la sécurité n'a spécifié aucun emplacement, une boîte de dialogue s'affiche vous invitant à enregistrer le fichier manuellement.

Si le responsable de la sécurité a défini un partage réseau pour le fichier de récupération de clés et que vous êtes connecté à Windows via un compte d'utilisateur local (par exemple, si l'ordinateur n'est pas un membre de domaine), vous êtes invité à vous connecter au partage réseau. Le responsable de la sécurité doit vous fournir le nom d'utilisateur et le mot de passe requis.

Remarque: Enregistrez le fichier lorsque vous y êtes invité et veillez à ce que le support puisse y accéder. Le fichier est chiffré et peut être enregistré sur tout support externe en vue d'être envoyé au support. Vous pouvez également l'envoyer par e-mail. Tant que vous n'enregistrez pas ce fichier, vous serez invité à le faire à chaque redémarrage de votre ordinateur.

Vous pouvez créer une nouvelle sauvegarde de clé à tout moment, au moyen de l'icône de la barre d'état de Sophos SafeGuard. Il s'avère par exemple nécessaire de créer un nouveau fichier de récupération de clé lorsque les fichiers de clés existants sont corrompus ou que le support n'y a plus accès.

3 Authentification au démarrage

Avec l'authentification au démarrage (POA), les utilisateurs doivent s'authentifier pendant la phase de préinitialisation de l'ordinateur, à savoir avant le démarrage du système d'exploitation du PC. Lorsque l'utilisateur est correctement authentifié dans l'authentification au démarrage, le système d'exploitation effectif (Windows) est démarré et l'utilisateur est connecté automatiquement à Windows. La procédure est identique lorsque l'ordinateur revient du mode hibernation.



3.1 Aspect de l'authentification au démarrage

L'aspect de l'authentification au démarrage peut être personnalisé en fonction des besoins de votre entreprise. Le responsable de la sécurité pour Sophos SafeGuard procède aux réglages appropriés via les paramètres de stratégie dans Sophos SafeGuard Policy Editor.

Les réglages suivants sont possibles :

- **Image de connexion**

L'image de connexion par défaut qui s'affiche dans l'authentification au démarrage est conçue par SafeGuard. Cet écran peut être personnalisé via une stratégie vous permettant d'afficher une image (le logo de votre entreprise, par exemple).

- **Texte des boîtes de dialogue**

Le texte de l'authentification au démarrage s'affiche dans la langue par défaut définie dans les Options régionales et linguistiques Windows lors de l'installation de Sophos SafeGuard sur l'ordinateur final.

Pour définir la langue par défaut, sélectionnez **Démarrer > Paramètres > Panneau de configuration > Options régionales et linguistiques > Options avancées**. Par exemple, si le paramètre par défaut est « Allemand », l'ensemble du texte des boîtes de dialogue dans l'authentification au démarrage s'affiche en allemand.

3.2 Première connexion après l'installation de Sophos SafeGuard

Si Sophos SafeGuard a été installé avec l'authentification au démarrage (POA), la procédure d'initialisation est différente lors du premier démarrage du système, après l'installation de Sophos SafeGuard sur un ordinateur. Plusieurs nouveaux messages de démarrage (écran de connexion automatique par exemple) s'affichent car Sophos SafeGuard a été intégré à la procédure d'initialisation. Ensuite, le système d'exploitation Windows démarre.

Lors de la première connexion après l'installation, connectez-vous à Windows comme vous le faites habituellement. Vous êtes alors enregistré en tant qu'utilisateur Sophos SafeGuard. Ce processus d'enregistrement est nécessaire pour vérifier que vos informations d'identification seront reconnues dans l'authentification au démarrage au prochain démarrage du système.

Remarque: Une info-bulle confirmant la réussite de l'enregistrement s'affiche sur votre ordinateur à la fin du processus.

Lorsque vous redémarrez l'ordinateur, l'authentification au démarrage est activée. Entrez alors vos informations d'identification Windows à partir de l'authentification au démarrage. Vous êtes ainsi connecté automatiquement à Windows sans devoir entrer de mot de passe (si la connexion automatique à Windows est activée).

Vous pouvez vous connecter à partir de l'authentification au démarrage via votre nom d'utilisateur et mot de passe Windows.

Remarque: Les paramètres des ordinateurs finaux sur lesquels Sophos SafeGuard est installé sont définis par le responsable de la sécurité dans Sophos SafeGuard Policy Editor, et distribués aux utilisateurs via des fichiers de stratégie.

3.3 Connexion à partir de l'authentification au démarrage

Après activation de l'authentification au démarrage, vous vous connectez en entrant vos informations d'identification utilisateur Windows dans la boîte de dialogue de connexion de l'authentification au démarrage. Vous êtes connecté automatiquement à Windows.

Remarque: Vous pouvez désactiver la connexion automatique à Windows en appuyant sur le bouton **Options>>** de la boîte de dialogue de connexion et en désactivant l'option **Connexion automatique vers Windows**.

Remarque: La désactivation de la connexion automatique est nécessaire, par exemple, pour permettre à d'autres utilisateurs d'utiliser l'authentification au démarrage sur l'ordinateur concerné (voir Importations d'autres utilisateurs, page 4).

3.3.1 Délai de connexion après un échec de tentative de connexion

En cas d'échec de connexion à partir de l'authentification au démarrage, en raison d'un mot de passe incorrect par exemple, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai est augmenté à chaque échec de tentative de connexion. Les échecs sont consignés.

3.3.2 Verrouillage de la machine

Selon les paramètres de stratégie, votre ordinateur peut se verrouiller après un certain nombre d'échecs de tentatives de connexions. Pour déverrouiller votre ordinateur, lancez une procédure Challenge/Réponse, voir [Récupération par Challenge/Réponse](#), à la page 48.

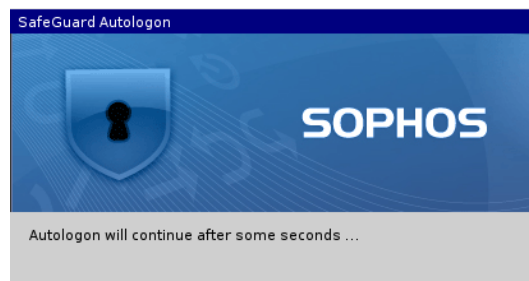
3.3.3 Exemple de première connexion utilisateur à partir de l'authentification au démarrage

La procédure de première connexion correspond strictement à celle décrite ici, si l'authentification au démarrage a été installée et activée sur votre ordinateur.

Selon la configuration de votre système, vous pouvez être invité à appuyer sur la combinaison de touches **Ctrl+Alt+Suppr**. La procédure de connexion se poursuit.

1. L'utilisateur 1 (Alice) met l'ordinateur final XP sous tension.

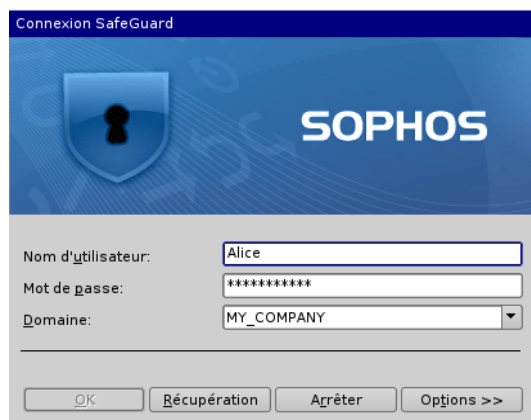
La boîte de dialogue Connexion automatique POA s'affiche.



2. La boîte de dialogue de connexion de Windows s'affiche ensuite. Alice se connecte à Windows.

À présent, Alice est le « propriétaire ». Il n'y a qu'un propriétaire par PC. Par défaut, le premier utilisateur qui se connecte est le propriétaire.

3. Si les stratégies, certificats et clés utilisateur se trouvent sur l'ordinateur final, une entrée est créée pour Alice dans le noyau du système Sophos SafeGuard.
4. Après le redémarrage de l'ordinateur, Alice peut se connecter à partir de l'authentification au démarrage.



Remarque: Si les paramètres par défaut s'appliquent, le premier utilisateur qui se connecte à Windows est automatiquement enregistré comme « propriétaire » de cet ordinateur. En fonction de la stratégie, seul le propriétaire d'un ordinateur peut permettre à d'autres utilisateurs de se connecter à partir de l'authentification au démarrage. Dans cet exemple, seule Alice peut se connecter à partir de l'authentification au démarrage.

Remarque: Si d'autres utilisateurs ont l'intention de se connecter à partir de l'authentification au démarrage, le propriétaire de l'ordinateur doit les y autoriser (voir [Importation d'autres utilisateurs](#), à la page 9).

Remarque: Le responsable de la sécurité définit dans les stratégies correspondantes si la connexion automatique vers Windows est activée ou désactivée et si vous êtes autorisé à changer ce paramètre dans la boîte de dialogue de connexion.

3.4 Importation d'autres utilisateurs

Un autre utilisateur Windows (Bob) souhaite se connecter à l'ordinateur terminal en plus d'Alice.

1. Bob met l'ordinateur sous tension et la boîte de dialogue de l'authentification au démarrage s'affiche.

Bob ne peut pas se connecter à partir de l'authentification au démarrage car il ne dispose pas des clés et des certificats nécessaires.

2. Pour que Bob puisse se connecter à partir de l'authentification au démarrage, le propriétaire de l'ordinateur (Alice) doit l'y autoriser.

Avec le paramètre par défaut, seul le premier utilisateur à se connecter après l'installation est enregistré comme le propriétaire de l'ordinateur.

Remarque: Le responsable de la sécurité peut également définir le propriétaire d'un ordinateur via un paramètre de stratégie.

3. Avant qu'Alice ne se connecte à partir de l'authentification au démarrage, elle doit désactiver l'option **Connexion automatique vers Windows**.



La boîte de dialogue de connexion de Windows s'affiche et invite Bob à se connecter.

4. Bob saisit ses informations d'identification Windows.
5. Une entrée est créée pour Bob dans le noyau du système Sophos SafeGuard.

Au prochain démarrage de l'ordinateur, Bob pourra se connecter à partir de l'authentification au démarrage.

3.5 Mot de passe temporaire dans l'authentification au démarrage

Sophos SafeGuard vous permet de changer temporairement le mot de passe dans l'authentification au démarrage. Le changement temporaire du mot de passe dans l'authentification au démarrage est recommandé si vous pensez que quelqu'un a pu vous voir saisir votre mot de passe.

Exemple : Vous initialisez votre ordinateur portable dans un lieu public, par exemple un aéroport. Vous pensez que quelqu'un vous a vu entrer votre mot de passe à partir de l'authentification au démarrage. Dans la mesure où vous n'êtes pas connecté à Active Directory (AD), vous ne pouvez pas changer votre mot de passe Windows.

Solution : Vous pouvez changer temporairement votre mot de passe dans l'authentification au démarrage et garantir qu'aucune personne non autorisée ne connaît votre mot de passe. Dès que vous serez de nouveau connecté à Active Directory, le système vous invitera automatiquement à changer le mot de passe temporaire.

Pour changer temporairement votre mot de passe dans l'authentification au démarrage :

1. Dans la boîte de dialogue de connexion de l'authentification au démarrage, saisissez le mot de passe existant.
2. Appuyez sur **F8**.

Si vous appuyez sur **F8** avant d'avoir entré le mot de passe existant, le système considère que la connexion a échoué et affiche le message correspondant.

3. Dans la boîte de dialogue, entrez le nouveau mot de passe et confirmez-le.

Le système vous rappelle que le changement du mot de passe est temporaire.

4. Cliquez sur **OK**.

Si vous annulez cette boîte de dialogue, le système vous connecte en utilisant votre ancien mot de passe.

La boîte de dialogue de connexion de Windows s'affiche.

Remarque: La connexion ne passe pas par Windows même si le système est configuré ainsi. Entrez l'ancien mot de passe dans cette boîte de dialogue. Le mot de passe temporaire est valide uniquement pour la connexion à partir de l'authentification au démarrage.

5. Cliquez sur **OK**.

Vous êtes connecté à Windows.

Pour vous connecter à partir de l'authentification au démarrage, vous pouvez désormais utiliser uniquement le mot de passe défini temporairement. Le mot de passe temporaire est valide jusqu'à ce qu'il soit changé à partir de la boîte de dialogue de connexion Windows. Seule cette opération permet de réactiver la connexion automatique vers Windows.

Changement du mot de passe temporaire

Il est indispensable de modifier ultérieurement le mot de passe changé temporairement dans l'authentification au démarrage pour resynchroniser les mots de passe.

Lors de la connexion à Windows, Sophos SafeGuard vous invite automatiquement à changer votre mot de passe dès que vous êtes reconnecté à Active Directory.

Vous pouvez annuler la boîte de dialogue vous invitant à changer le mot de passe sans changer effectivement le mot de passe. Dans ce cas, la boîte de dialogue apparaît à chaque connexion, tant que vous n'avez pas changé le mot de passe.

Remarque: Vous pouvez également changer temporairement le mot de passe de l'authentification au démarrage lorsque vous êtes connecté à Active Directory. Dans ce cas, la boîte de dialogue permettant de changer le mot de passe apparaît immédiatement après le changement temporaire du mot de passe dans l'authentification au démarrage. Toutefois, il est possible de l'annuler et d'utiliser l'ancien mot de passe pour se connecter. Vous pouvez changer le mot de passe ultérieurement.

3.6 Clavier virtuel

Lors de l'authentification au démarrage, vous pouvez afficher/masquer un clavier virtuel et cliquer sur les touches à l'écran pour entrer les informations d'identification, etc.

Condition préalable : Le responsable de la sécurité a activé l'affichage du clavier virtuel dans la stratégie du type **Paramètres machine spécifiques**.

Pour afficher le clavier virtuel dans l'authentification au démarrage, cliquez sur **Options >>** dans la boîte de dialogue de connexion de l'authentification au démarrage et cochez la case **Clavier virtuel**.



Le clavier virtuel prend en charge différentes dispositions et il est possible de modifier la disposition à l'aide des mêmes options que pour la disposition du clavier de l'authentification au démarrage (voir [Modification de la disposition du clavier](#), à la page 14).

3.7 Disposition du clavier

Chaque pays ou presque a une disposition de clavier qui lui est propre, c'est-à-dire une répartition différente des touches. La disposition du clavier dans est importante pour l'authentification au démarrage lorsque vous saisissez des noms d'utilisateur, des mots de passe et des codes de réponse.

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

La langue de la disposition du 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.

3.7.1 Modification de la disposition du clavier

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

Pour modifier la langue de la disposition de votre clavier :

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**, sous **Paramètres par défaut du compte d'utilisateur**, activez l'option **Appliquer tous les paramètres au compte d'utilisateur actuel et au profil utilisateur par défaut**.
4. Cliquez sur **OK**.

L'authentification au démarrage reconnaît 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 final deux fois. Si la disposition du clavier précédente est désactivée via les **Options régionales et linguistiques**, elle est maintenue jusqu'à ce que vous en sélectionniez une nouvelle.

Remarque: Par ailleurs, vous devez modifier la langue de la disposition du clavier pour les programmes non-unicode.

Si la langue souhaitée n'est pas disponible sur votre système, Windows peut vous inviter à l'installer. Ensuite, vous devez redémarrer votre ordinateur deux fois de sorte 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**).

Vous pouvez voir quelles sont les langues installées et disponibles sur votre système via **Démarrer > Exécuter > regedit** : HKEY_USERS\ .DEFAULT\Keyboard Layout\Preload.

3.8 Touches de fonction/raccourcis clavier pris en charge dans l'authentification au démarrage (POA)

Certains paramètres et fonctionnalités matérielles peuvent générer des problèmes lors du démarrage des ordinateurs finaux et provoquer le blocage du système. L'authentification au démarrage prend en charge plusieurs raccourcis clavier pour modifier les paramètres matériels et désactiver les fonctionnalités. De plus, une liste contenant les paramètres et fonctionnalités matérielles connus pour provoquer des problèmes est intégrée au fichier .msi installé sur l'ordinateur.

Nous vous recommandons d'installer une version mise à jour du fichier de configuration POA avant tout déploiement important de Sophos SafeGuard. Le fichier est mis à jour tous les mois et est téléchargeable à l'adresse suivante : <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 est utilisé uniquement lorsqu'aucun fichier de configuration POA n'a été 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>
```

Pour en savoir plus, consultez la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/65700.html>.

Par ailleurs, l'authentification au démarrage prend en charge un certain nombre de touches de fonction.

3.8.1 Raccourcis clavier

Maj-F3 = support du "legacy mode" 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 uniquement (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

Maj-F3	Maj-F5	Maj-F7	Legacy mode	USB 1.x	USB 2.0	Commentaire
désactivé	désactivé	désactivé	actif	actif	actif	3.
actif	désactivé	désactivé	désactivé	actif	actif	Par défaut
désactivé	actif	désactivé	actif	désactivé	désactivé	1., 2.
actif	actif	désactivé	actif	désactivé	désactivé	1., 2.
désactivé	désactivé	actif	actif	actif	désactivé	3.
actif	désactivé	actif	désactivé	actif	désactivé	
désactivé	actif	actif	actif	désactivé	désactivé	
actif	actif	actif	actif	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. Toutefois, n'oubliez pas que si votre ordinateur utilise un clavier USB ou une souris USB, ils peuvent être désactivés en appuyant sur **Maj-F5**.

Remarque: L'authentification au démarrage peut utiliser le clavier USB via BIOS SMM. Pas de support USB par clé cryptographique.

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 "legacy mode" peut fonctionner dans ce scénario.

3. Le "legacy mode" 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.

Remarque: Les modifications possibles à l'aide des raccourcis clavier peuvent déjà avoir été spécifiées au cours de l'installation du client Sophos SafeGuard en utilisant un fichier .mst.

Après avoir modifié les paramètres matériels en utilisant les raccourcis clavier dans l'authentification au démarrage, une boîte de dialogue s'affiche pour vous inviter à enregistrer les paramètres modifiés. Cette boîte de dialogue affiche une présentation de la configuration qui sera enregistrée. Pour enregistrer vos modifications, cliquez sur **Oui**. Après le redémarrage de votre ordinateur, les nouveaux paramètres deviennent actifs. Si vous cliquez sur **Non**, vos modifications ne sont pas enregistrées et l'ancienne configuration reste active après le redémarrage de votre ordinateur.

En appuyant sur **F5** dans n'importe quelle boîte de dialogue POA, vous pouvez afficher une boîte de dialogue montrant la configuration par raccourcis clavier utilisée pour initialiser l'authentification au démarrage. Si des raccourcis clavier ont été modifiés au cours du processus d'initialisation, l'état des touches correspondantes s'affiche en bleu. Bleu signifie que la touche a été utilisée dans cet état pour initialiser l'authentification au démarrage, sinon, c'est qu'il n'a pas encore été enregistré. Les valeurs inchangées sont affichées en noir. Pour fermer la boîte de dialogue, appuyez de nouveau sur **F5** ou appuyez sur **Entrée**.

3.8.2 Touches de fonction de la boîte de dialogue de connexion

Remarque: Les touches de fonction ne sont pas des raccourcis clavier.

F2 = annule la connexion automatique

F5 = affiche une boîte de dialogue montrant la configuration des raccourcis clavier utilisée pour initialiser l'authentification au démarrage.

F8 = change le mot de passe de l'authentification au démarrage. Utilisée à la place de la touche **Entrée** pour déclencher un changement de mot de passe dans l'authentification au démarrage après la connexion.

Alt+Maj (touche **Alt** gauche et touche **Maj** gauche) = change le clavier d'allemand en anglais (ou l'inverse)

Annulation et préparation de l'arrêt de l'authentification au démarrage

Ctrl+Alt+Suppr = après l'échec d'une authentification et si le PC doit être éteint correctement. Cette combinaison de touches a la même fonction que le bouton **Arrêter**.

Remarque: Si une connexion par empreinte digitale est activée, appuyez sur la combinaison de touches **Ctrl+Alt+Suppr** dans la boîte de dialogue POA de connexion avec une empreinte digitale pour ouvrir la boîte de dialogue POA de connexion avec un nom d'utilisateur et un mot de passe. Pour en savoir plus sur la connexion par empreinte digitale, voir [Connexion avec le lecteur d'empreintes digitales de Lenovo](#), à la page 25.

3.9 Synchronisation du mot de passe

Sophos SafeGuard détecte automatiquement si le mot de passe Windows a été modifié et ne correspond plus à celui stocké dans la base de données Sophos SafeGuard. Ceci peut se produire si le mot de passe Windows est a été changé via un VPN, sur un autre ordinateur, ou dans Active Directory.

Si Sophos SafeGuard détecte cette situation, vous êtes invité à saisir l'ancien mot de passe. Par la suite, le mot de passe stocké par Sophos SafeGuard est mis à jour avec le nouveau mot de passe Windows.

La synchronisation du mot de passe se produit dans deux situations :

- pendant la connexion ;
- pendant une procédure de verrouillage/déverrouillage de Windows.

4 Authentification au démarrage sous Windows Vista

L'authentification au démarrage pour Windows Vista est identique à celle de Windows XP en termes d'aspect et de comportement (voir [Authentification au démarrage](#), à la page 6). Les seules différences résident dans la procédure de connexion au système d'exploitation. Windows Vista propose plusieurs méthodes d'authentification parallèles de connexion utilisateur.

Remarque: Cette section décrit uniquement les différences relatives à Windows Vista. Si ces différences ne sont pas expressément définies, les procédures/processus décrits dans la section précédente relative à l'authentification au démarrage s'appliquent également à Vista.

4.1 Première connexion après l'installation de Sophos SafeGuard sous Windows Vista

Si Sophos SafeGuard a été installé avec l'authentification au démarrage, la procédure d'initialisation est différente pour le premier démarrage du système après l'installation de Sophos SafeGuard sur votre ordinateur. Plusieurs nouveaux messages de démarrage (écran de connexion automatique, par exemple) s'affichent car Sophos SafeGuard a été intégré à la procédure d'initialisation. Le système d'exploitation Windows démarre ensuite.

Remarque: Sous Windows Vista, vous devez d'abord appuyer sur la combinaison de touches **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 (Enregistrement interactif : **Ctrl+Alt+Suppr** non requis).

Lors de la première connexion après l'installation, vous devez vous connecter à Windows selon la méthode classique à l'aide de vos informations d'identification. Vous êtes alors enregistré en tant qu'utilisateur Sophos SafeGuard. Ce processus d'enregistrement est nécessaire pour vérifier que vos informations d'identification seront reconnues dans l'authentification au démarrage au prochain démarrage du système.

Une info-bulle vous informant de la réussite de l'enregistrement s'affiche sur votre ordinateur à la fin du processus.

Lorsque vous redémarrez l'ordinateur, l'authentification au démarrage est activée. Entrez alors vos informations d'identification Windows à partir de l'authentification au démarrage. Vous êtes ainsi connecté automatiquement à Windows sans devoir entrer de mot de passe (si la connexion automatique à Windows est activée).

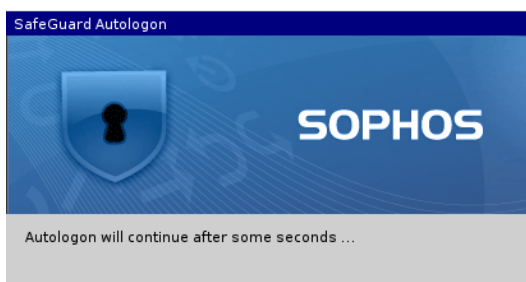
Vous pouvez vous connecter à partir de l'authentification au démarrage via un nom d'utilisateur et un mot de passe.

Remarque: Les paramètres des ordinateurs finaux sur lesquels Sophos SafeGuard est installé sont définis de manière centralisée par le responsable de la sécurité dans Sophos SafeGuard Policy Editor et distribués aux ordinateurs terminaux via des fichiers de stratégie.

4.1.1 Procédure de première connexion

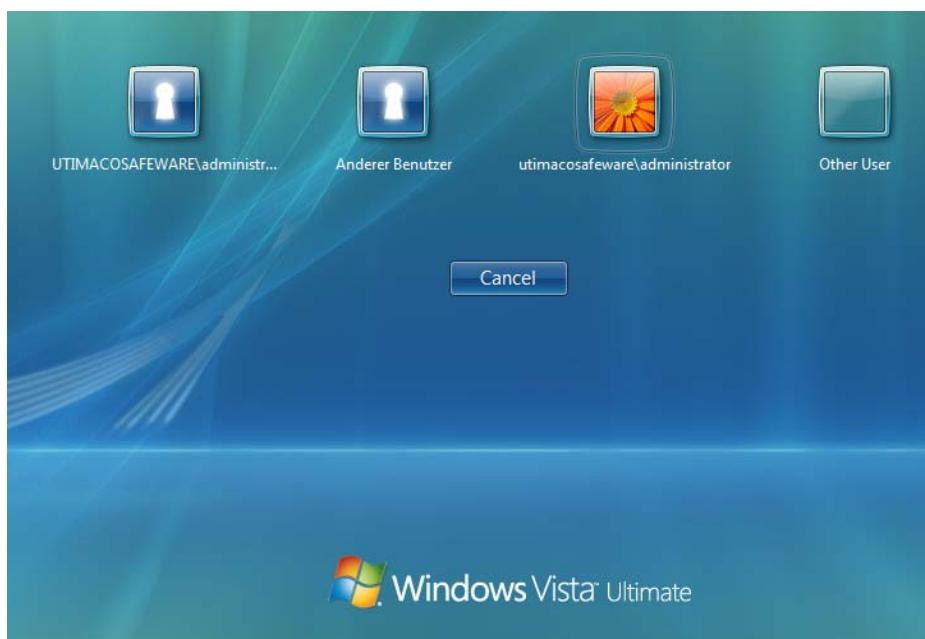
Cette section décrit la procédure de première connexion à votre ordinateur après que Sophos SafeGuard a été installé. La procédure de première connexion correspond strictement à celle décrite ici, si l'authentification au démarrage a été installée et activée sur votre ordinateur.

1. L'ordinateur final démarre et la boîte de dialogue de connexion automatique Sophos SafeGuard s'affiche.



Un utilisateur automatique est connecté.

2. La boîte de dialogue de connexion de Windows Vista s'affiche.

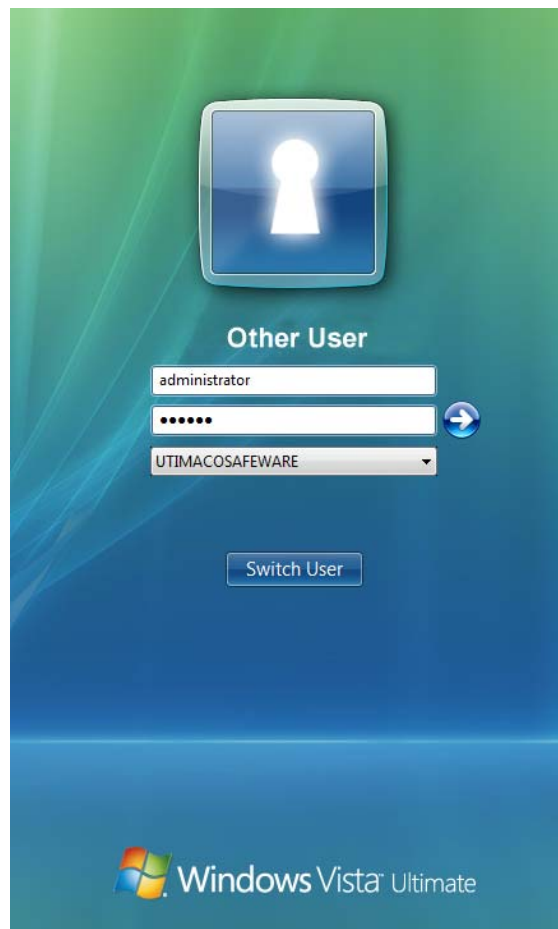


Sous Windows Vista, Sophos SafeGuard propose une méthode d'authentification supplémentaire. L'exemple illustre la méthode d'authentification Sophos SafeGuard et les icônes de la méthode d'authentification Vista.

3. Windows Vista propose deux icônes pour chaque méthode d'authentification:

- Cliquez sur **Autre utilisateur** pour ouvrir une boîte de dialogue de saisie des informations d'identification.
- Cliquez sur la deuxième icône (un nom d'utilisateur apparaît sous l'icône) pour ouvrir une boîte de dialogue contenant les informations sur le dernier utilisateur connecté au système. Entrez uniquement votre mot de passe.

Si votre nom d'utilisateur s'affiche sous une icône Sophos SafeGuard, sélectionnez l'icône correspondante. Dans le cas contraire, sélectionnez l'icône Sophos SafeGuard **Autre utilisateur**.



4. Entrez vos informations d'identification utilisateur Windows, comme à l'accoutumée.

Au prochain démarrage du système, vous n'entrez que vos informations d'identification utilisateur Windows (nom d'utilisateur et mot de passe) dans l'authentification au démarrage et vous serez connecté automatiquement.

Un redémarrage du système est nécessaire pour activer toute la fonctionnalité de l'authentification au démarrage. Après redémarrage, l'authentification au démarrage protège votre ordinateur contre tout accès non autorisé.

4.2 Connexion à partir de l'authentification au démarrage sous Windows Vista

Après activation de l'authentification au démarrage (synchronisation initiale et redémarrage), vous vous connectez en entrant vos informations d'identification utilisateur Windows dans la boîte de dialogue de connexion de l'authentification au démarrage. Vous êtes connecté automatiquement à Windows.

Remarque: Vous pouvez désactiver la connexion automatique à Windows en appuyant sur le bouton **Options>>** de la boîte de dialogue de connexion et en désactivant l'option **Connexion automatique vers Windows**. La désactivation de la connexion automatique est nécessaire, par exemple, pour permettre à d'autres utilisateurs d'utiliser l'authentification au démarrage sur l'ordinateur concerné. Le responsable de la sécurité définit dans les stratégies correspondantes si la connexion automatique vers Windows est activée ou désactivée et si vous êtes autorisé à changer ce paramètre dans la boîte de dialogue de connexion.

4.2.1 Délai de connexion après un échec de tentative de connexion

En cas d'échec de connexion à partir de l'authentification au démarrage, en raison d'un mot de passe incorrect par exemple, un message d'erreur s'affiche et un délai est imposé avant la tentative de connexion suivante. Le délai est augmenté à chaque échec de tentative de connexion. Les échecs sont consignés.

4.2.2 Verrouillage de la machine

Selon les paramètres de stratégie, votre ordinateur peut se verrouiller après un certain nombre d'échecs de tentatives de connexions. Pour déverrouiller votre ordinateur, lancez une procédure Challenge/Réponse, voir [Récupération par Challenge/Réponse](#), à la page 48.

5 Connexion sous Windows Vista

Sous Windows Vista, Sophos SafeGuard propose une méthode d'authentification supplémentaire.

Si vous désactivez l'option **Connexion automatique vers Windows** dans la boîte de dialogue de connexion de l'authentification au démarrage, la boîte de dialogue de connexion Windows Vista s'affiche. Dans cette boîte de dialogue, vous pouvez également choisir une autre méthode d'authentification.

Remarque: L'utilisation d'une autre méthode d'authentification ne signifie pas que Sophos SafeGuard n'est pas actif sur votre ordinateur. Dans ce cas, la connexion à Sophos SafeGuard n'est pas effectuée pendant la connexion Windows mais après la connexion Windows Vista.

5.1 Connexion via Sophos SafeGuard

Vous êtes généralement connecté automatiquement à Windows après avoir entré votre mot de passe à partir de l'authentification au démarrage (POA). Si vous désactivez l'option **Connexion automatique vers Windows** dans la boîte de dialogue de connexion de l'authentification au démarrage et que vous utilisez la méthode Sophos SafeGuard pour vous connecter à Windows, toutes les fonctionnalités de Sophos SafeGuard sont disponibles après la connexion à Windows Vista.

Les clés nécessaires sont disponibles et toutes les données sont chiffrées et déchiffrées en fonction des stratégies définies.

5.2 Connexion via une autre méthode d'authentification

Dans la boîte de dialogue de connexion Windows, vous pouvez également choisir une autre méthode d'authentification pour vous connecter à Windows à la place de la méthode d'authentification Sophos SafeGuard.

Si vous utilisez une autre méthode pour vous connecter au système d'exploitation, la connexion à Sophos SafeGuard est effectuée après la connexion au système d'exploitation.

Après la connexion à Windows Vista, l'application d'authentification Sophos SafeGuard démarre automatiquement.

Selon les paramètres de connexion de l'administration centralisée, une boîte de dialogue permettant de saisir les informations d'identification ou le code PIN s'affiche.

1. Entrez vos informations d'identification ou le code PIN et cliquez sur **OK**.

La fonctionnalité de Sophos SafeGuard est alors disponible et vous pouvez, par exemple, accéder aux données chiffrées si vous disposez de la clé requise.

5.3 Synchronisation du mot de passe sous Windows Vista

Sophos SafeGuard détecte automatiquement si le mot de passe Windows a été modifié et ne correspond plus à celui qui est stocké. Ceci peut se produire si le mot de passe Windows est a été changé via un VPN, sur un autre ordinateur, ou dans Active Directory.

Si Sophos SafeGuard détecte cette situation, vous êtes informé, puis invité à saisir l'ancien mot de passe. Par la suite, le mot de passe stocké par Sophos SafeGuard est mis à jour avec le nouveau mot de passe Windows.

La synchronisation du mot de passe se produit dans deux situations :

- pendant la connexion ;
- pendant une procédure de verrouillage/déverrouillage de Windows.

6 Connexion avec le lecteur d'empreintes digitales de Lenovo

Cette fonction n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

Les utilisateurs doivent mémoriser de nombreux mots de passe et codes PIN différents pour accéder à leur ordinateur, leurs applications et leurs réseaux. Grâce au lecteur d'empreintes digitales, il vous suffit de faire glisser votre doigt sur le lecteur au lieu d'utiliser un mot de passe.

Par ailleurs, vous ne pouvez pas perdre ni oublier vos informations d'identification et les personnes non autorisées ne peuvent pas les deviner. L'utilisation de lecteurs d'empreintes digitales simplifie donc la procédure de connexion et renforce la sécurité.

Sophos SafeGuard prend en charge la connexion par empreinte digitale à partir de l'authentification au démarrage et lors de la phase de connexion Windows. Par exemple, vous pouvez vous connecter à un ordinateur portable Lenovo en faisant simplement glisser votre doigt sur le lecteur d'empreintes digitales intégré. Les autres étapes de la procédure de connexion s'exécutent alors automatiquement. Vous pouvez également verrouiller et déverrouiller votre bureau dans Windows en glissant votre doigt sur le lecteur d'empreintes digitales.

Des lecteurs d'empreintes digitales sont directement intégrés à certains ordinateurs portables Lenovo. Cependant, vous pouvez également utiliser un clavier USB externe pour la connexion par empreinte digitale.

- Vous ne pouvez connecter qu'un seul lecteur d'empreintes digitales à la fois à un ordinateur.
- La connexion à distance par empreinte digitale n'est pas prise en charge.

6.1 Configuration minimale

Afin d'utiliser la connexion par empreinte digitale, la configuration minimale suivante doit être respectée :

6.1.1 Configuration minimale générale

- Matériel Lenovo
- Lecteur d'empreintes digitales Lenovo intégré à l'ordinateur portable ou clavier USB équipé d'un lecteur d'empreintes digitales
- Le dernier BIOS est recommandé
- Sophos SafeGuard, version 5.35 ou ultérieure
- La version logicielle recommandée par le fournisseur doit être installée avant Sophos SafeGuard :
 - ThinkVantage Fingerprint pour AuthenTec
 - ou
 - ThinkVantage Fingerprint pour UPEK
- Le responsable de la sécurité doit avoir configuré l'option avec empreinte digitale dans la stratégie d'**Authentification** concernée.

6.1.2 Configuration minimale du système

- WindowsXP 32bits
- Windows Vista, 32 bits, 64 bits
- Windows 7, 32 bits, 64 bits

6.1.3 Matériel pris en charge

- AuthenTec AES2810
- UPEK TCS3C/TCD42A

6.1.4 Logiciels pris en charge

- Lenovo Fingerprint pour AuthenTec version 3.2.0.166
- ThinkVantage Fingerprint pour UPEK version 5.8.5.6014

6.2 Enregistrement des empreintes digitales

Pour vous connecter à votre ordinateur portable/de bureau à l'aide d'une empreinte digitale, vous devez d'abord enregistrer cette empreinte à l'aide de la version recommandée du logiciel spécifique au fournisseur. La procédure d'enregistrement associe l'empreinte digitale enregistrée aux informations d'identification (nom d'utilisateur et mot de passe).

Conditions préalables : La description ci-dessous suppose que la version recommandée du logiciel spécifique au fournisseur et Sophos SafeGuard sont installés.

Pour enregistrer vos empreintes digitales :

1. Connectez-vous à partir de l'authentification au démarrage (POA) en saisissant votre nom d'utilisateur et votre mot de passe.
2. Enregistrez une ou plusieurs empreintes digitales à l'aide du logiciel spécifique au fournisseur installé. Cette procédure associe votre empreinte digitale à vos informations d'identification Windows.
 - a) Pour en savoir plus sur la procédure d'enregistrement des empreintes digitales, reportez-vous à la documentation du logiciel ThinkVantage Fingerprint.
 - b) Activez l'option **Mot de passe POA dans le BIOS** (UPEK uniquement. Cette étape n'est pas nécessaire pour AuthenTec).
 - c) Pour utiliser la connexion par empreinte digitale à partir de l'authentification au démarrage, vous devez d'abord vous connecter, une première fois, à Windows à l'aide de votre empreinte digitale afin de transférer vos informations d'identification vers le lecteur d'empreintes digitales. Pour UPEK, il vous suffit de faire glisser l'empreinte enregistrée sur le lecteur d'empreintes digitales. Pour AuthenTec, vous devez également fournir votre mot de passe Windows lors de la première connexion.
3. Réinitialisez votre PC/ordinateur portable.
4. Pour tester l'empreinte digitale que vous avez enregistrée, passez votre doigt sur le lecteur d'empreintes digitales après avoir réinitialisé l'ordinateur.

Si votre empreinte digitale correspond à celle que vous avez enregistrée, la session Windows s'ouvre automatiquement.

6.3 Connexion à partir de l'authentification au démarrage avec une empreinte digitale

Conditions préalables :

- Le responsable de la sécurité doit avoir configuré l'option avec empreinte digitale dans la stratégie d'**Authentification** concernée.
- Vous devez avoir enregistré une ou plusieurs empreintes digitales.

1. Réinitialisez votre PC/ordinateur portable.

La boîte de dialogue de connexion par empreinte digitale de l'authentification au démarrage s'affiche.



2. Faites glisser l'un des doigts enregistrés sur le lecteur.

Si le logiciel reconnaît votre empreinte digitale, l'authentification au démarrage lit les informations d'identification et les envoie à Windows.

Remarque: La procédure de connexion utilise des icônes avec des messages texte courts sous forme d'invites, de notifications et d'avertissements (voir [Icônes utilisées dans le processus de connexion](#), à la page 29).

Vous êtes automatiquement connecté à Windows sans demande de données supplémentaires.

- Si la procédure d'enregistrement dans Windows ne s'est pas exécutée avec succès (par exemple, si après l'enregistrement des empreintes digitales, vous ne vous êtes pas déconnecté, puis reconnecté à Windows), le logiciel trouve dans l'authentification au démarrage une correspondance avec les empreintes digitales enregistrées.

Cependant, aucune information d'identification n'est disponible. Dans ce cas, le logiciel affiche un message d'erreur vous invitant à vous connecter à l'aide de votre nom d'utilisateur et de votre mot de passe, sans connexion automatique vers Windows. Vos informations d'identification sont transférées vers le lecteur d'empreintes digitales.

- Dans les stratégies qui vous sont applicables, le responsable de la sécurité spécifie si la connexion automatique vers Windows a été activée ou désactivée et si vous pouvez changer ces paramètres dans la boîte de dialogue POA de connexion avec un nom d'utilisateur et un mot de passe (voir [Connexion avec un nom d'utilisateur et un mot de passe](#), à la page 31).

6.3.1 Icônes utilisées dans le processus de connexion

Lorsque vous vous connectez à l'authentification au démarrage à l'aide d'une empreinte digitale, le système utilise des icônes comme invites, notifications et avertissements. Ces icônes s'affichent pendant la procédure de connexion, accompagnées d'un message texte court.



Vous invite à faire glisser votre doigt sur le lecteur d'empreintes digitales.



Indique que la connexion par empreinte digitale n'est actuellement pas activée. Ce peut être le cas, par exemple, si le module de connexion par empreinte digitale n'a pas encore été initialisé.



Indique que le lecteur d'empreintes digitales fonctionne et qu'il est occupé.



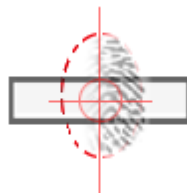
Indique que le lecteur d'empreintes digitales a lu l'empreinte avec succès et trouvé une correspondance.



Indique que le lecteur d'empreintes digitales a lu l'empreinte avec succès mais sans trouver de correspondance.



Indique que le lecteur d'empreintes digitales n'est pas parvenu à lire l'empreinte. Faites glisser une nouvelle fois votre doigt sur le lecteur d'empreintes digitales.



Indique que vous avez placé le doigt trop excentré sur la gauche (ou trop excentré sur la droite). Placez le doigt au centre du lecteur d'empreintes digitales.



Indique que votre glissement de doigt était trop oblique. Faites glisser une nouvelle fois votre doigt sur le lecteur d'empreintes digitales.



Indique que vous avez bougé le doigt trop rapidement. Faites glisser une nouvelle fois votre doigt sur le lecteur d'empreintes digitales.



Indique que votre glissement de doigt était trop court. Faites glisser une nouvelle fois votre doigt sur le lecteur d'empreintes digitales.

6.3.2 Échecs de tentatives de connexion

Si le système ne parvient pas à lire une empreinte digitale après cinq tentatives, il considère que la tentative de connexion a échoué et consigne le problème comme un événement. Dans ce cas, un délai de connexion apparaît.

Si le système est parvenu à lire une empreinte digitale sans erreur, mais ne trouve aucune correspondance avec l'empreinte digitale enregistrée au bout de cinq tentatives, il considère également que la tentative de connexion a échoué et consigne le problème comme un événement. Dans ce cas, un délai de connexion se produit.

Le délai de connexion est augmenté à chaque échec de tentative de connexion.

6.3.3 Connexion avec un nom d'utilisateur et un mot de passe

Même si la connexion par empreinte digitale est activée, vous pouvez continuer à vous connecter à partir de l'authentification au démarrage avec votre nom d'utilisateur et votre mot de passe, par exemple, si vous ne pouvez pas vous connecter avec l'empreinte digitale car votre lecteur d'empreintes digitales est défectueux.

Pour vous authentifier en saisissant vos données de connexion utilisateur :

1. Appuyez sur la touche **Echap** ou sur la combinaison de touches **Ctrl+Alt+Suppr** dans la boîte de dialogue de l'authentification au démarrage pour vous connecter par empreinte digitale.

La boîte de dialogue POA de connexion par nom d'utilisateur et mot de passe s'affiche.



Remarque: Si vous appuyez sur **Ctrl+Alt+Suppr** dans la boîte de dialogue POA de connexion par nom d'utilisateur et mot de passe, l'ordinateur s'éteint. Dans cette boîte de dialogue, la combinaison de touches **Ctrl+Alt+Suppr** équivaut au bouton **Arrêter**.

La boîte de dialogue POA de connexion avec un nom d'utilisateur et un mot de passe apparaît également automatiquement si le lecteur d'empreintes digitales est indisponible ou si le système ne trouve pas de données utilisateur sur le lecteur d'empreintes digitales.

Remarque: La connexion par nom d'utilisateur et mot de passe est également activée automatiquement si le cache local est corrompu. Dans ce cas, votre ordinateur se verrouille et vous devez vous connecter à l'aide d'une procédure Challenge/Réponse (voir [Lancement d'une procédure Challenge/Réponse lors de la connexion par empreinte digitale](#), à la page 33).

2. Vous pouvez également appuyer sur la touche **Echap** pour retourner à la boîte de dialogue POA de connexion par empreinte digitale.

Si vous avez appuyé sur Echap pour ouvrir la boîte de dialogue POA de connexion avec un nom d'utilisateur et un mot de passe, vous pouvez toujours vous connecter en glissant votre doigt sur le lecteur d'empreintes digitales sans avoir à retourner d'abord à la boîte de dialogue POA de connexion avec une empreinte digitale.

6.4 Modification du mot de passe

1. Si une connexion par empreinte digitale est activée dans l'authentification au démarrage, vous pouvez changer votre mot de passe dans Windows via la combinaison de touches **Ctrl+Alt+Suppr**.

Lorsque vous modifiez le mot de passe, le système vous invite à faire glisser votre doigt sur le lecteur d'empreintes digitales pour y transférer le nouveau mot de passe.

Remarque: Chaque fois que vous modifiez le mot de passe, la modification s'applique à toutes les empreintes enregistrées.

6.4.1 Synchronisation du mot de passe

Si le mot de passe Windows ne correspond plus au mot de passe stocké dans le lecteur d'empreintes digitales, par exemple après une modification du mot de passe, et si le nouveau mot de passe n'a pas été transféré vers le lecteur d'empreintes digitales, vous pouvez synchroniser le mot de passe en procédant comme suit:

1. Réinitialisez votre ordinateur.
2. Appuyez sur la touche **Echap** ou sur la combinaison de touches **Ctrl+Alt+Suppr** dans la boîte de dialogue POA de connexion par empreinte digitale afin de basculer vers la boîte de dialogue POA de connexion avec un nom d'utilisateur et un mot de passe.

3. Cliquez sur le bouton **Options** et désactivez l'option **Connexion automatique vers Windows**.

Dans les stratégies qui vous sont associées, le responsable de sécurité indique si la connexion automatique vers Windows a été activée ou désactivée et si vous pouvez modifier les paramètres de la boîte de dialogue de connexion par nom d'utilisateur et mot de passe de l'authentification au démarrage.

4. Connectez-vous à l'aide de votre mot de passe.
5. La boîte de dialogue de connexion de Windows s'affiche. Faites glisser l'un des doigts enregistrés sur le lecteur d'empreintes digitales.
6. Le système reconnaît l'empreinte, mais Windows rejette néanmoins le mot de passe qui lui est associé. Ce problème n'est toutefois pas considéré comme un échec de tentative de connexion et n'entraîne donc aucun délai de connexion.
7. À la place, le système affiche un message confirmant la modification du mot de passe et vous invite à saisir le mot de passe Windows actuel. Saisissez correctement le mot de passe Windows.

Si vous saisissez un mot de passe Windows incorrect, le système consigne un échec de tentative de connexion et applique un délai de connexion. Si vous fermez l'invite d'entrée sans saisir de mot de passe, le système consigne également un échec de tentative de connexion et applique un délai de connexion.

Le transfert effectif du mot de passe met fin à la procédure de synchronisation du mot de passe et vous pouvez alors utiliser le mot de passe pour vous connecter.

6.5 Lancement d'une procédure Challenge/Réponse lors de la connexion par empreinte digitale

Pour récupérer la connexion, vous pouvez lancer une procédure Challenge/Réponse. Cette procédure peut s'avérer nécessaire, par exemple lorsque la connexion par empreinte digitale ne fonctionne pas et que vous avez oublié le mot de passe de connexion. La procédure Challenge/Réponse de Sophos SafeGuard propose une méthode d'échange d'informations confidentielles hautement sécurisée et fiable.

Pour lancer une procédure Challenge/Réponse avec la connexion par empreinte digitale activée :

1. Appuyez sur la touche **Echap** dans la boîte de dialogue pour vous connecter par empreinte digitale.

La boîte de dialogue de connexion avec un nom d'utilisateur et un mot de passe s'affiche.

2. Cliquez sur **Récupération** pour lancer la procédure Challenge/Réponse.

En raison de la procédure Challenge/Réponse, le système risque de vous proposer de modifier le mot de passe lors de l'initialisation de l'ordinateur, par exemple pour permettre la récupération en cas d'oubli du mot de passe. Dans ce cas, le système vous propose également de mettre à jour les informations d'identification associées à l'empreinte digitale.

Pour obtenir une description détaillée de la procédure Challenge/Réponse, voir [Récupération par Challenge/Réponse](#), à la page 48.

7 Options de récupération

Pour la récupération (par exemple, si vous avez oublié votre mot de passe), Sophos SafeGuard propose différentes options adaptées aux différents scénarios :

■ Récupération de connexion via Local Self Help

Si vous avez oublié votre mot de passe, Local Self Help vous permet de vous connecter à votre ordinateur sans l'aide du support. Vous pouvez accéder à votre ordinateur même si aucune connexion téléphonique ou réseau n'est disponible (à bord d'un avion, par exemple). Pour vous connecter, il vous suffit de répondre à un certain nombre de questions prédéfinies dans l'authentification au démarrage.

Pour en savoir plus, voir [Récupération via Local Self Help](#), à la page 36.

■ Récupération par Challenge/Réponse

Le mécanisme de Challenge/Réponse est un système de récupération sécurisé et fiable qui vous aide lorsque vous ne pouvez pas vous connecter à votre ordinateur ou accéder aux données chiffrées. Lors de la procédure de Challenge/Réponse, vous communiquez le code de challenge généré sur votre ordinateur au responsable du support qui générera à son tour un code de réponse. Ce code vous autorisera à exécuter une action spécifique sur l'ordinateur.

Pour en savoir plus, voir [Récupération par Challenge/Réponse](#), à la page 48.

Les deux options de récupération sont activées sur votre ordinateur par le responsable de la sécurité via des stratégies.

8 Récupération via Local Self Help

Si vous avez oublié votre mot de passe et que vous ne pouvez pas contacter le support d'aide, Sophos SafeGuard propose Local Self Help.

L'utilisation de Local Self Help permet d'accéder de nouveau à votre portable dans les situations où aucune connexion par téléphone ou réseau n'est disponible et où vous ne pouvez donc pas utiliser une procédure Challenge/Réponse (par exemple, à bord d'un avion). Vous pouvez vous connecter à votre ordinateur en répondant au nombre indiqué de questions prédéfinies dans l'authentification au démarrage.

Le responsable de la sécurité peut définir les questions devant trouver une réponse et les distribuer aux ordinateurs finaux. Vous pouvez également définir vos propres questions, si la stratégie appropriée vous y autorise. Pour fournir les réponses initiales et modifier les questions, Sophos SafeGuard propose l'assistant Local Self Help. Vous pouvez ouvrir l'assistant Local Self Help en cliquant sur l'icône de la barre d'état de Sophos SafeGuard dans la barre des tâches Windows.

8.1 Conditions préalables

Pour utiliser Local Self Help dans le cadre d'une récupération de connexion, les conditions préalables suivantes doivent être remplies :

- Le responsable de la sécurité a activé Local Self Help, dans la stratégie effective et qui s'applique du type **Paramètres généraux**, et défini le paramètre pour cette fonction (par exemple, le droit de définir vos propres questions).
- Vous avez activé Local Self Help sur votre ordinateur (voir [Activation de Local Self Help](#), à la page 36).

8.2 Activation de Local Self Help

Lorsque la stratégie vous autorisant à utiliser Local Self Help devient effective, vous devez activer la fonction en répondant aux questions prédéfinies que vous avez reçues ou en définissant vos propres questions et en y répondant.

Local Self Help ne devient actif sur votre ordinateur que lorsque vous avez répondu à dix questions au moins et que vous les avez enregistrées.

Selon les paramètres de stratégie, plusieurs scénarios sont possibles :

■ **Vous avez reçu des questions prédéfinies et vous n'êtes pas autorisé à définir vos propres questions.**

Répondez à dix des questions prédéfinies reçues au moins et enregistrez-les.

■ **Vous avez reçu des questions prédéfinies et vous êtes autorisé à définir vos propres questions.**

Répondez à dix questions au moins et enregistrez-les (questions prédéfinies, questions définies par vous ou les deux).

■ **Vous n'avez pas reçu de questions prédéfinies et vous êtes autorisé à définir vos propres questions.**

Définissez dix questions au moins, répondez-y et enregistrez-les.

Remarque: Pour vous connecter à partir de l'authentification au démarrage via Local Self Help, vous devez répondre à cinq questions sélectionnées de façon aléatoire parmi les dix questions ayant une réponse.

Condition préalable : Après avoir reçu la stratégie, l'info-bulle indique qu'il existe des questions Local Self Help sans réponse. Redémarrez l'ordinateur pour ajouter la commande **Local Self Help** au menu contextuel de l'icône de la barre d'état système dans la barre des tâches Windows.

Pour activer Local Self Help :

1. Cliquez avec le bouton droit de la souris sur l'icône de la barre d'état de Sophos SafeGuard dans la barre des tâches Windows.
2. Sélectionnez **Local Self Help**.

La boîte de dialogue de bienvenue dans l'assistant Local Self Help s'affiche.

Pour des raisons de sécurité, vous êtes invité à saisir votre mot de passe.

3. Saisissez votre mot de passe et cliquez sur **Suivant**.

La boîte de dialogue Présentation de l'état s'affiche.

Cette boîte de dialogue offre des instructions brèves permettant l'activation de Local Self Help. Elle affiche en outre des informations relatives à l'état (par exemple le nombre de questions définies par l'utilisateur ayant une réponse, le nombre de questions prédéfinies ayant une réponse, etc.).

4. Cliquez sur **Suivant**.

Si vous avez reçu des questions prédéfinies avec la stratégie effective, la boîte de dialogue Questions prédéfinies s'affiche.

Questions	Réponses	Sujet
Quel est votre artiste préféré ?	<cliquez ici pour répond...	Français
Quel est votre livre préféré ?	<cliquez ici pour répond...	Français
Quelle est l'année de naissance de votre ...	<cliquez ici pour répond...	Français
Quel est votre sportif préféré ?	<cliquez ici pour répond...	Français
Quelle est votre couleur préférée ?	<cliquez ici pour répond...	Français
Quel est votre auteur préféré ?	<cliquez ici pour répond...	Français
Quel est le nom de votre dernier établisse...	<cliquez ici pour répond...	Français
Qui était votre idole lorsque vous étiez en...	<cliquez ici pour répond...	Français
Quel professeur détestiez-vous ou aimez...	<cliquez ici pour répond...	Français
Quel est votre plat favori ?	<cliquez ici pour répond...	Français
Quel(le) est votre acteur/actrice préféré(...	<cliquez ici pour répond...	Français
Quel est votre film préféré ?	<cliquez ici pour répond...	Français

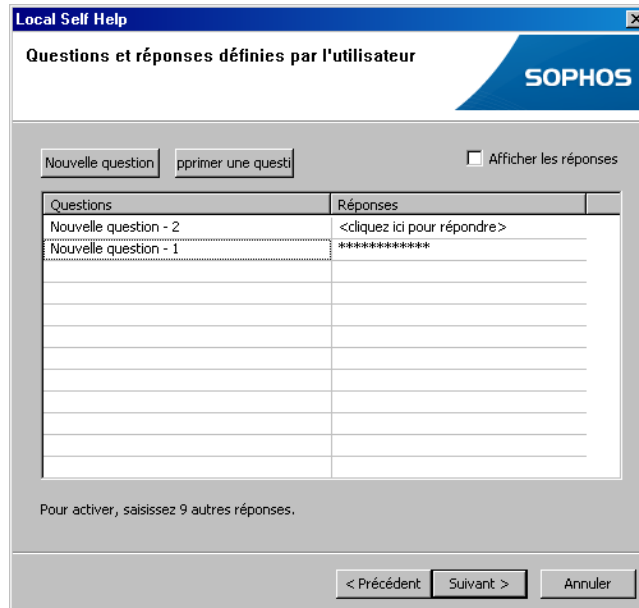
- Si vous avez reçu plusieurs sujets de questions différents, vous pouvez choisir parmi ceux qui s'affichent dans la liste déroulante du champ **Sujet**.
- Pour afficher tous les sujets sous forme de liste continue, sélectionnez l'option **Tous les sujets** (par défaut) dans la liste déroulante.
- Pour répondre aux questions, cliquez sur la question concernée et saisissez votre réponse dans la colonne **Réponses**.
- Après avoir saisi la réponse, le texte est masqué. Pour afficher le texte, sélectionnez **Afficher les réponses**.

Remarque: Lorsque vous répondez aux questions au cours d'un processus de récupération dans l'authentification au démarrage, vous devez saisir les réponses exactement telles que vous les avez saisies dans l'assistant Local Self Help. Par exemple, les réponses sont sensibles à la casse dans Local Self Help.

Remarque: Lorsque vous saisissez des réponses en japonais, vous devez utiliser des caractères Romaji (romains), sinon les réponses ne correspondent pas lorsque vous répondez aux questions dans l'authentification au démarrage.

5. Après avoir terminé de répondre aux questions prédéfinies, cliquez sur **Suivant**.

6. Si vous êtes autorisé à définir vos propres questions, la boîte de dialogue Questions et réponses définies par l'utilisateur s'affiche.



- a) Pour ajouter une nouvelle question, cliquez sur **Nouvelle question**.

Une nouvelle ligne s'ajoute à la liste des questions.

- b) Saisissez votre question dans la colonne **Questions** et la réponse dans la colonne **Réponses**.

Après avoir saisi la réponse, le texte est masqué.

- c) Pour afficher le texte, sélectionnez **Afficher les réponses**.

Remarque: Lorsque vous répondez aux questions au cours d'un processus de récupération dans l'authentification au démarrage, vous devez saisir les réponses exactement telles que vous les avez saisies dans l'assistant Local Self Help. Par exemple, les réponses sont sensibles à la casse dans Local Self Help.

Remarque: Lorsque vous saisissez des réponses en japonais, vous devez utiliser des caractères Romaji (romains), sinon les réponses ne correspondent pas lorsque vous répondez aux questions dans l'authentification au démarrage.

7. Après avoir terminé de définir et de répondre à vos propres questions, cliquez sur **Suivant**.

La dernière boîte de dialogue de l'assistant Local Self Help affiche les nouvelles informations d'état après que vous avez répondu aux questions. Un message indique si les conditions préalables d'activation de Local Self Help sont respectées.

8. Cliquez sur **Terminer**.

Les questions et les réponses sont enregistrées. Un message s'affiche pour indiquer que Local Self Help a été activé.

9. Cliquez sur **OK**.

Local Self Help est actif sur votre ordinateur. Vous pouvez utiliser Local Self Help pour la récupération de la connexion dans l'authentification au démarrage.

Remarque: Si Local Self Help est actif sur votre ordinateur et que vous avez réinitialisé votre mot de passe via une procédure Challenge/Réponse, les réponses stockées pour Local Self Help ne sont plus valides. Local Self Help n'est plus actif sur votre ordinateur. Pour réactiver Local Self Help, répondez de nouveau aux questions.

8.3 Modification des questions

Après avoir activé Local Self Help sur votre ordinateur, vous pouvez, à tout moment, modifier les questions :

- Pour les questions prédéfinies, vous pouvez modifier les réponses fournies en répondant initialement aux questions. Cependant, les questions prédéfinies ne peuvent pas être supprimées.
- Pour les questions définies par l'utilisateur, vous pouvez changer les réponses fournies en répondant initialement aux questions, ajouter des questions ou en supprimer.

Pour modifier les questions dans l'assistant Local Self Help :

1. Cliquez avec le bouton droit de la souris sur l'icône de la barre d'état de Sophos SafeGuard dans la barre des tâches Windows.
2. Sélectionnez **Local Self Help**.

La boîte de dialogue Bienvenue dans l'assistant Local Self Help s'affiche.

Pour des raisons de sécurité, vous êtes invité à saisir votre mot de passe.

3. Saisissez votre mot de passe et cliquez sur **Suivant**.

La boîte de dialogue Présentation de l'état s'affiche.

Cette boîte de dialogue offre des instructions brèves permettant l'activation de Local Self Help. Elle affiche en outre des informations relatives à l'état (par exemple le nombre de questions définies par l'utilisateur ayant une réponse, le nombre de questions prédéfinies ayant une réponse, etc.).

4. Cliquez sur **Suivant**.

- a) Si vous avez reçu des questions prédéfinies et si vous y avez répondu, la boîte de dialogue Questions prédéfinies s'affiche avec les questions ayant une réponse.
- b) Si vous avez reçu plusieurs sujets de questions différents, vous pouvez choisir parmi ceux qui doivent s'afficher dans la liste déroulante du champ **Sujet**.
- c) Pour afficher tous les sujets sous forme de liste continue, sélectionnez l'option **Tous les sujets** (par défaut) dans la liste déroulante.

Par défaut, les réponses saisies ne sont pas affichées sous forme de texte.

- d) Pour afficher le texte saisi, activez la case à cocher **Afficher les réponses**.
- e) Pour modifier les réponses, cliquez sur les questions concernées et saisissez votre nouvelle réponse dans la colonne **Réponses**.

5. Après avoir terminé vos modifications, cliquez sur **Suivant**.

Si vous êtes autorisé à définir vos propres questions, la boîte de dialogue Questions et réponses définies par l'utilisateur s'affiche. Par défaut, les réponses saisies ne sont pas affichées sous forme de texte.

6. Pour afficher le texte saisi, activez la case à cocher **Afficher les réponses**.

- a) Pour modifier les réponses existantes, cliquez sur les questions concernées et saisissez votre nouvelle réponse dans la colonne **Réponses**.
- b) Pour ajouter une nouvelle question, cliquez sur **Nouvelle question**.

Une nouvelle ligne s'ajoute à la liste des questions. Saisissez votre question dans la colonne **Questions** et la réponse dans la colonne **Réponses**.

- c) Pour supprimer des questions, cliquez sur la question concernée, puis sur **Supprimer la question**.

Un message s'affiche pour vous inviter à confirmer la suppression de la question. Cliquez sur **Oui**.

7. Après avoir terminé vos modifications, cliquez sur **Suivant**.

La dernière boîte de dialogue de l'assistant Local Self Help affiche les nouvelles informations d'état après la modification des questions. Un message indique si les conditions préalables permettant à Local Self Help de rester actif sont respectées.

8. Cliquez sur **Terminer**.

Les questions et les réponses sont enregistrées. Un message s'affiche pour indiquer que la procédure de modification s'est déroulée correctement et que Local Self Help reste actif.

9. Cliquez sur **OK**.

Les modifications sont appliquées.

La prochaine fois que vous lancerez Local Self Help dans l'authentification au démarrage, les nouvelles questions et les questions modifiées seront sélectionnées de façon aléatoire, puis affichées. Les nouvelles réponses et les réponses modifiées s'appliquent.

Remarque: Si le nombre de questions ayant une réponse est inférieur au minimum requis du fait des modifications effectuées, un message d'avertissement s'affiche dans la dernière boîte de dialogue de l'assistant Local Self Help indiquant que Local Self Help sera désactivé après la fermeture de l'assistant.

Remarque: Si vous ne souhaitez pas désactiver Local Self Help, vous pouvez retourner aux boîtes de dialogue **Questions définies par l'utilisateur** et **Questions prédéfinies** en cliquant sur le bouton **Précédent**. Vous pouvez ensuite ajouter de nouvelles questions ou y répondre. Si vous cliquez sur **Terminer** et si le nombre de questions ayant une réponse est inférieur au minimum requis, un autre message d'avertissement s'affiche pour indiquer que Local Self Help n'est plus actif sur votre ordinateur. Vous pouvez toutefois réactiver Local Self Help (voir [Activation de Local Self Help](#), à la page 36).

8.4 Changements de paramètres pour Local Self Help lors des processus d'édition

Durant le processus de définition ou de modification des questions dans l'assistant Local Self Help, les paramètres de Local Self Help peuvent être modifiés. Par exemple, une nouvelle stratégie contenant de nouveaux paramètres Local Self Help et/ou un nouvel ensemble de questions Local Self Help peuvent être transférés à votre ordinateur via le mécanisme de distribution spécifique à votre entreprise.

Si de tels changements surviennent durant le processus d'édition, l'ensemble de questions et réponses définies pourrait ne plus être valide et le nombre de questions serait insuffisant pour permettre à Local Self Help de s'activer ou de rester actif sur votre ordinateur.

Par conséquent, chaque fois que vous terminez la définition ou la modification de questions dans l'assistant Local Self Help, l'assistant vérifie si l'une des conditions suivantes s'applique et déclenche l'action appropriée :

Condition	Action de l'assistant LSH	Résultat
Local Self Help a été désactivé entièrement par une nouvelle stratégie.	L'assistant Local Self Help affiche un message indiquant que Local Self Help a été désactivé entièrement et se ferme.	Local Self Help ne peut plus être utilisé.
Les paramètres de Local Self Help ont été modifiés (par exemple, la longueur minimale des réponses, le droit de définir vos propres questions) par une nouvelle stratégie. Cependant, Local Self Help n'a pas été désactivé. Les questions et réponses définies sont toujours valides et en quantité suffisante pour que Local Self Help reste actif sur votre ordinateur.	L'assistant Local Self Help affiche un message indiquant que les paramètres Local Self Help ont été modifiés, enregistre vos modifications et se ferme.	Local Self Help est actif sur votre ordinateur et peut être utilisé pour une récupération de connexion. Toutefois, les proportions de questions disponibles et de réponses valides sont susceptibles d'avoir été modifiées. Pour retrouver la proportion initiale, vous devrez peut-être ajouter ou supprimer des questions et/ou des réponses.
Les paramètres de Local Self Help ont été modifiés (par exemple, la longueur minimale des réponses, le droit de définir vos propres questions) par une nouvelle stratégie. Local Self Help n'a pas été désactivé. Cependant, les questions et réponses définies ne sont plus valides et leur nombre est insuffisant pour que Local Self Help soit actif sur votre ordinateur.	L'assistant Local Self Help affiche un message indiquant que les paramètres Local Self Help ont été modifiés. Local Self Help n'est pas actif sur votre ordinateur. Il est recommandé de réexécuter l'assistant. L'assistant se ferme.	Pour activer Local Self Help, réexécutez l'assistant Local Self Help et redéfinissez les questions et réponses. Ensuite, vous pouvez utiliser Local Self Help pour la récupération de connexion.

8.5 Connexion à partir de l'authentification au démarrage à l'aide de Local Self Help

Pour vous connecter à partir de l'authentification au démarrage via Local Self Help, vous devez répondre à cinq questions sélectionnées de façon aléatoire parmi les dix questions définies correctement.

Comment se connecter à votre ordinateur à l'aide de Local Self Help à partir de l'authentification au démarrage:

1. Entrez votre nom d'utilisateur dans la boîte de dialogue de connexion de l'authentification au démarrage.

Le bouton **Récupération** devient actif.

2. Cliquez sur **Récupération**.

- Si seule la méthode Local Self Help est activée pour la récupération de la connexion, Local Self Help démarre.
- Si les méthodes Local Self Help et Challenge/Réponse sont activées pour la récupération de la connexion, une boîte de dialogue permettant de sélectionner ces deux méthodes s'affiche. Cliquez sur **Local Self Help**.

La boîte de dialogue Bienvenue dans Local Self Help s'affiche.

Cette boîte de dialogue affiche une brève description des étapes suivantes.

3. Cliquez sur **Suivant** pour commencer à répondre aux questions.

La première question s'affiche dans la boîte de dialogue Local Self Help - Question 1 sur 5.

4. Saisissez votre réponse.

Par défaut, et pour des raisons de sécurité, le texte saisi n'est pas affiché dans le champ de saisie. Pour afficher la réponse, désactivez la case à cocher **Masquer la réponse**.



5. Après avoir répondu à la question, cliquez sur **Suivant**.

Vous ne pouvez cliquer sur **Suivant** et passer à la question suivante que si vous avez saisi une réponse.

6. Continuez de répondre aux quatre questions restantes. Après avoir répondu à la dernière, cliquez sur **OK**.

Dans la boîte de dialogue suivante, vous pouvez afficher votre mot de passe actuel.

7. Pour afficher le mot de passe, appuyez sur **Entrée**, sur la **barre d'espace** ou cliquez sur la case bleue.

Ne cliquez PAS sur **OK**. **Si vous cliquez sur OK**, le processus d'initialisation continue SANS afficher le mot de passe.



Le mot de passe ne s'affiche que pendant 5 secondes maximum. Ensuite, le processus d'initialisation continue automatiquement.

Remarque: Vérifiez, par tous les moyens, qu'aucune personne non autorisée ne peut consulter le contenu de votre écran (volontairement ou non). Vous pouvez immédiatement masquer votre mot de passe en appuyant sur la barre d'espace, sur la touche Entrée ou en cliquant sur la case bleue.

8. Vous pouvez lire le mot de passe et l'utiliser pour vous reconnecter à partir de l'authentification au démarrage et à Windows.
9. Après avoir lu le mot de passe, cliquez sur **OK**. Autrement, le processus d'initialisation se poursuit automatiquement après le délai de 5 secondes qui suit l'affichage du mot de passe.

Vous êtes maintenant connecté à l'authentification au démarrage et à Windows.

8.6 Échecs de tentatives de connexion

Si vous saisissez une réponse erronée à une ou plusieurs questions, la connexion échoue. Dans ce cas, un message indiquant l'échec de la connexion s'affiche. Pour des raisons de sécurité, Local Self Help n'indique pas les réponses erronées.

Une procédure de récupération Local Self Help ayant échoué est considérée comme une tentative de connexion ayant échoué et elle est consignée en tant qu'événement. Dans ce cas, un délai de connexion apparaît. Le délai de connexion est augmenté à chaque échec de tentative de connexion.

Si vous redémarrez votre ordinateur à la suite d'un échec de tentative de connexion, et si vous sélectionnez de nouveau la récupération de la connexion via Local Self Help, cinq questions sont sélectionnées une nouvelle fois de façon aléatoire.

9 Récupération par Challenge/Réponse

Pour la récupération, Sophos SafeGuard propose une **Procédure Challenge/Réponse** pour l'échange d'informations confidentielles. La procédure Challenge/Réponse est hautement sécurisée et fiable.

Pendant la procédure Challenge/Réponse, vous générez un code de challenge (chaîne de caractères ASCII) et fournissez ce code au personnel du support. En fonction du code de challenge fourni, le responsable support génère alors un code de réponse qui vous autorise à effectuer une action spécifique sur votre ordinateur.

9.1 Conditions préalables

Pour récupérer la connexion via Challenge/Réponse, il est indispensable que le support puisse accéder au fichier de récupération de clé. Ces fichiers doivent être fournis au support via un dossier partagé, e-mail ou supports séparés.

En cas d'oubli de mot de passe, il est nécessaire de disposer d'un autre compte sur l'ordinateur pour pouvoir le réinitialiser. Vous pouvez également utiliser un disque de réinitialisation de mot de passe.

La procédure Challenge/Réponse vous permet de vous connecter à partir de l'authentification au démarrage. Vous êtes également autorisé à vous connecter à Windows, même si le mot de passe Windows doit être réinitialisé.

9.2 Vous avez entré un mot de passe incorrect un trop grand nombre de fois

Si vous avez entré votre mot de passe de manière incorrecte un trop grand nombre de fois et que votre ordinateur est bloqué au niveau de l'authentification au démarrage, la procédure Challenge/Réponse permet le démarrage de l'ordinateur à partir de l'authentification au démarrage. Ensuite, la boîte de dialogue de connexion Windows s'affiche. Vous pouvez saisir votre mot de passe Windows dans cette boîte de dialogue et vous connectez au système.

Le compteur du nombre maximum de tentatives de saisie du mot de passe peut être réinitialisé.

9.3 Vous avez oublié votre mot de passe

Lors de la récupération du mot de passe via la procédure Challenge/Réponse, une réinitialisation de mot de passe est requise.

Remarque: Nous vous recommandons par conséquent d'utiliser Local Self Help principalement pour récupérer un mot de passe oublié. Avec la récupération via Local Self Help, le mot de passe actuel peut être affiché et vous pouvez continuer à l'utiliser. Cela évitera la réinitialisation du mot de passe et le recours à l'assistance du support. Pour plus d'informations, voir [Récupération via Local Self Help](#), à la page 36.

1. Lancez une procédure Challenge/Réponse et suivez les instructions fournies par le support. Votre ordinateur pourra démarrer à partir de l'authentification au démarrage.
2. Vous ne connaissez pas davantage le mot de passe de la boîte de dialogue de connexion Windows et vous devez donc le modifier au niveau Windows. Cela nécessite d'autres actions de récupération sortant du périmètre de Sophos SafeGuard, via des moyens Windows standard.

Deux méthodes permettent de réinitialiser le mot de passe Windows :

- via un compte de service ou administrateur disponible sur votre ordinateur avec les droits Windows requis ;
- via un disque de réinitialisation de mot de passe Windows.

Le responsable support vous indique la procédure à appliquer et vous fournit les informations d'identification Windows supplémentaires ou le disque requis.

3. Entrez le nouveau mot de passe Windows que le support vous a fourni et modifiez-le immédiatement en choisissant une valeur connue de vous seul.

Sophos SafeGuard détecte que le nouveau choix de mot de passe ne correspond pas au mot de passe Sophos SafeGuard actuel. Vous êtes invité à saisir l'ancien mot de passe.

4. Si vous avez changé vous-même le mot de passe Windows et si vous connaissez toujours l'ancien, vous pouvez également changer le mot de passe pour Sophos SafeGuard en saisissant l'ancien ici. Si ce n'est pas le cas, cliquez sur **Annuler**.

Dans Sophos SafeGuard, la définition d'un nouveau mot de passe sans donner l'ancien requiert un nouveau certificat. Vous devez confirmer cette procédure. Un nouveau certificat utilisateur sera créé en fonction du nouveau choix de mot de passe Windows. Cela vous permet de vous connecter de nouveau à l'ordinateur ainsi qu'à l'authentification au démarrage à l'aide du nouveau mot de passe.

5. Connectez-vous à partir de l'authentification au démarrage avec le nouveau mot de passe.

Remarque: Clés pour SafeGuard Data Exchange

Remarque: Si vous avez oublié le mot de passe Windows et s'il a été réinitialisé, vous ne serez pas en mesure d'utiliser les clés déjà créées pour SafeGuard Data Exchange sans les passphrases correspondantes. Pour continuer d'utiliser les clés utilisateur déjà générées pour SafeGuard Data Exchange, vous devez mémoriser les passphrases SafeGuard Data Exchange requises pour réactiver ces clés.

Remarque: Notez que SafeGuard Data Exchange n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

9.4 Vous ne pouvez plus accéder à votre ordinateur

Si vous ne pouvez plus accéder à votre ordinateur, il se peut que l'authentification au démarrage soit corrompue. Même dans une situation critique de ce type, Sophos SafeGuard Policy Editor propose une procédure Challenge/Réponse avec une assistance du support, vous permettant d'accéder à vos lecteurs chiffrés. Dans ce cas, la procédure Challenge/Réponse est exécutée dans un environnement WinPE. Si vous rencontrez une situation de ce type, nous vous recommandons de contacter le support Sophos SafeGuard Policy Editor. Le responsable du support vous fournira les fichiers nécessaires et vous guidera tout au long des étapes nécessaires pour que vous puissiez accéder à votre ordinateur.

9.5 Procédure Challenge/Réponse

La procédure Challenge/Réponse doit être initiée :

- si vous avez entré un mot de passe incorrect un trop grand nombre de fois ;
- si vous avez oublié votre mot de passe ;
- pour réparer un cache corrompu.

Remarque: 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 via une procédure Challenge/Réponse. Dans ce cas, il vous est demandé automatiquement de lancer une procédure Challenge/Réponse, si le cache local est corrompu.

Remarque: À partir de la génération du challenge, vous disposez de 30 minutes pour entrer correctement la réponse générée par le support dans le cadre d'une procédure Challenge/Réponse. Le code de réponse n'est plus valide et ne peut plus être utilisé une fois les 30 minutes écoulées.

1. Dans la boîte de dialogue de connexion de l'authentification au démarrage, cliquez sur **Récupération**.

- Si seule la méthode Challenge/Réponse est activée pour la récupération de la connexion, cette procédure démarre.
- Si les méthodes Challenge/Réponse et Local Self Help sont disponibles pour la récupération de la connexion, une boîte de dialogue permettant de sélectionner ces deux méthodes s'affiche. Cliquez sur le bouton **Challenge/Réponse** pour lancer la procédure Challenge/Réponse.

Une boîte de dialogue apparaît indiquant le nom du fichier nécessaire à la procédure Challenge/Réponse.



2. Appelez alors le support. Donnez au responsable le nom du fichier.

3. Cliquez sur **Suivant**.

Vos données utilisateur et un code Challenge généré de manière aléatoire s'affichent. Pour une meilleure lisibilité, le code est sous-divisé en bloc de cinq caractères chacun. (Si vous avez besoin d'aide pour l'indication du code de challenge, vous pouvez cliquer sur le bouton **Aide à l'épellation**).

4. Cliquez sur **Suivant**.

La boîte de dialogue Challenge/Réponse - Étape 3 sur 3 s'affiche alors.

Le responsable support vous transmet le code de réponse par téléphone ou SMS.

5. Saisissez le code de réponse dans les champs réservés à cet effet de la boîte de dialogue Challenge/Réponse - Étape 3 sur 3.

Si vous faites une erreur dans la saisie du code de réponse, le bloc de caractères contenant l'erreur s'affiche en rouge.

6. Cliquez sur **OK**.

Vous êtes connecté à partir de l'authentification au démarrage.

10 Icône de la barre d'état système et info-bulle

La fonctionnalité suivante est proposée via l'icône de la barre d'état système :

- **Afficher**

- **Jeu de clés**

- Affiche toutes les clés disponibles.

Remarque: Le client Sophos SafeGuard utilise une clé machine définie pour le chiffrement basé sur volume et le chiffrement basé sur fichier des lecteurs. Cette clé n'apparaît *pas* dans la boîte de dialogue. Seules les clés créées en local sur l'ordinateur sont affichées. Si vous n'avez créé aucune clé, aucune n'apparaît dans cette boîte de dialogue. Notez que le chiffrement basé sur fichier n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

- **Certificat**

- Affiche des informations relatives à votre certificat.

- **Créer une nouvelle clé**

- Ouvre une boîte de dialogue permettant de créer une clé utilisée pour l'échange de données par l'intermédiaire de supports amovibles.

Remarque: Cette fonction n'est pas disponible avec ESDP.

- **Sauvegarde de clé**

- Cette fonction permet de créer une sauvegarde du fichier de clés. Ce dernier est indispensable pour récupérer la connexion via Challenge/Réponse.

- **Local Self Help**

- Si Local Self Help est activé pour votre ordinateur par l'intermédiaire de la stratégie correspondante, la commande Local Self Help s'affiche dans le menu contextuel de l'icône de la barre d'état système. Cette commande permet de lancer l'assistant Local Self Help. Local Self Help est une méthode de récupération de connexion qui ne requiert aucune assistance du support. Pour en savoir plus sur Local Self Help, voir [Récupération via Local Self Help](#), à la page 36.

- **Statut** : Ouvre une boîte de dialogue proposant des informations sur le statut actuel de l'ordinateur protégé par Sophos SafeGuard :

Champ	Informations
Dernière stratégie reçue	Indique quand (date et heure) l'ordinateur a reçu une nouvelle stratégie pour la dernière fois.
Dernière clé reçue	Indique quand (date et heure) l'ordinateur a reçu une nouvelle clé pour la dernière fois.
Dernier certificat reçu	Indique quand (date et heure) l'ordinateur a reçu un nouveau certificat pour la dernière fois.
État de l'utilisateur SGN	<p>Indique le statut de l'utilisateur qui est connecté à l'ordinateur (connexion Windows) :</p> <ul style="list-style-type: none"> ■ En attente L'affectation de l'utilisateur à l'installation Sophos SafeGuard en tant qu'utilisateur Sophos SafeGuard est en cours. Veuillez patienter jusqu'au traitement des données utilisateur. Le statut de l'utilisateur passe ensuite automatiquement à Utilisateur SGN, c'est-à-dire utilisateur Sophos SafeGuard. ■ Utilisateur SGN L'affectation de l'utilisateur à l'installation Sophos SafeGuard en tant qu'utilisateur Sophos SafeGuarda été effectuée. ■ Invité SGN L'utilisateur connecté à Windows est un utilisateur invité Sophos SafeGuard. Ce dernier est autorisé à se connecter à Windows sans être affecté à cet ordinateur protégé par Sophos SafeGuard en tant qu'utilisateur Sophos SafeGuard. ■ Invité SGN (compte de service) L'utilisateur connecté à Windows est un utilisateur Sophos SafeGuard invité connecté via un compte de service pour des tâches d'administration. ■ Inconnu Indique que le statut de l'utilisateur n'a pas pu être déterminé.
État de Local Self Help (LSH) Activé Actif	Indique si Local Self Help a été activé sur l'ordinateur par une stratégie ou par un utilisateur.

- **Aide**

Ouvre l'aide en ligne de Sophos SafeGuard.

- **À propos de Sophos SafeGuard**

Fournit des informations sur votre version de Sophos SafeGuard.

L'info-bulle de l'icône de la barre d'état système indique que l'ordinateur de l'utilisateur est un client Sophos SafeGuard (autonome).

Remarque: Une info-bulle indique la réussite de la synchronisation initiale.

Remarque: Redémarrez votre ordinateur une fois la synchronisation utilisateur initiale réussie. Ce n'est qu'après avoir redémarré votre ordinateur que toutes les fonctions Sophos SafeGuard seront disponibles.

11 Extensions de SafeGuard Explorer

Vous pouvez accéder aux fonctions liées au chiffrement via les entrées correspondantes des menus contextuels de l'Explorateur Windows.

11.1 Extensions de l'Explorateur pour le chiffrement basé sur fichier

Remarque: Le chiffrement basé sur fichier n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

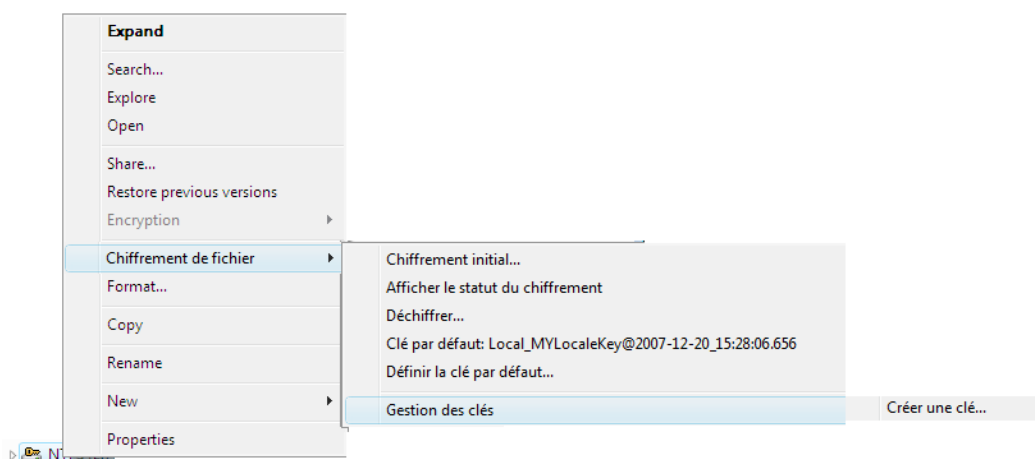
Vous pouvez accéder aux fonctions de chiffrement basé sur fichier (voir [Chiffrement basé sur fichier](#), à la page 59) via les entrées correspondantes des menus contextuels de l'Explorateur Windows. Les fonctions sont disponibles dans les menus contextuels des :

- volumes ;
- supports amovibles ;
- répertoires ;
- fichiers.

L'entrée **Chiffrement de fichier** est ajoutée au menu contextuel. Vous pouvez accéder aux fonctions individuelles via ce menu.

Si aucune stratégie de chiffrement basé sur fichier ne s'applique au volume sélectionné, vous pouvez uniquement déterminer l'état du chiffrement et afficher la boîte de dialogue de génération de clés via le menu contextuel.

Si une stratégie de chiffrement basé sur fichier s'applique au volume, support amovible, répertoire ou fichier sélectionné, les entrées suivantes sont ajoutées au menu contextuel :



Remarque: Les fonctions affichées dépendent des paramètres définis dans les stratégies. Elles dépendent également de la disponibilité ou non de la fonction correspondante pour le volume sélectionné. La portée de la fonction varie en fonction du chiffrement basé sur fichier ou sur volume utilisé pour le volume correspondant.

Les fonctions suivantes sont disponibles :

- **Démarrer le chiffrement** : Si vous sélectionnez cette option dans le menu contextuel d'un volume, tous les fichiers peuvent être chiffrés ou rechiffrés.
- **Afficher le statut du chiffrement** : Indique si un volume, support amovible ou fichier a été chiffré, indique la clé utilisée, si la clé fait partie de votre jeu de clés et si vous pouvez accéder à ce fichier.
- **Déchiffrer** : Déchiffre le volume ou fichier sélectionné.
- **Clé par défaut** : Indique la clé actuellement utilisée pour les nouveaux fichiers ajoutés au volume (enregistrement, copie ou déplacement). Vous pouvez définir la clé standard pour chaque volume ou support amovible séparément.
- **Définir la clé par défaut** : Ouvre une boîte de dialogue permettant de sélectionner une autre clé par défaut.
- **Gestion des clés : Créer une nouvelle clé** : Ouvre une boîte de dialogue permettant de créer des clés locales définies par l'utilisateur.

11.2 Extensions de l'Explorateur pour le chiffrement basé sur volume

L'entrée **Chiffrement** est ajoutée au menu contextuel de l'Explorateur Windows.

Si le volume est chiffré, un symbole de clé s'affiche en regard de l'entrée du menu.

Remarque: **Chiffrement de fichier > Afficher le statut du chiffrement** indique le statut de chiffrement des fichiers sur le volume par rapport à un chiffrement basé sur fichier. Les fichiers d'un volume chiffré peuvent également être chiffrés sur fichier. Dans ce cas, une boîte de dialogue correspondante s'affiche.

Pour obtenir plus d'informations sur le chiffrement basé sur volume, voir [Chiffrement basé sur volume](#), à la page 58.

12 Chiffrement de données

Sophos SafeGuard chiffre les données d'un ordinateur selon une méthode basée sur volume ou sur fichier. Le responsable de la sécurité définit les volumes (lecteurs) à chiffrer dans les stratégies de sécurité.

12.1 Chiffrement transparent

Les fichiers d'un lecteur chiffré sont chiffrés de manière transparente. Vous ne serez pas invité à chiffrer ou à déchiffrer les fichiers lors de leur ouverture, modification ou enregistrement.

Lorsque vous ouvrez les fichiers, ils sont déchiffrés et vous pouvez les modifier. Ils sont rechiffrés à la fermeture ou à l'enregistrement.

Les fichiers sont déchiffrés si vous les copiez ou les déplacez (via Enregistrer sous également) d'un lecteur chiffré vers un emplacement de votre ordinateur non chiffré. Les fichiers sont stockés dans le nouvel emplacement, en texte brut.

12.2 Chiffrement basé sur volume

Sur un ordinateur protégé par Sophos SafeGuard, une clé machine générée automatiquement est utilisée pour le chiffrement des données basé sur volume.

Si une stratégie définissant un chiffrement de ce type s'applique à votre ordinateur, les données seront automatiquement chiffrées. Il est impossible d'ajouter d'autres clés au volume.

Un afficheur de chiffrement indique l'avancement du processus de chiffrement. Il est réduit dans la barre des tâches Windows. Vous pouvez afficher l'afficheur de chiffrement en cliquant simplement sur l'icône. Si l'afficheur de chiffrement de base est réduit, vous pouvez demander une notification une fois le chiffrement terminé en activant l'option **Affiche l'information avant de fermer**. L'afficheur se ferme automatiquement une fois le chiffrement terminé. Vous pouvez utiliser le volume chiffré comme tout autre volume déchiffré de votre ordinateur.

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

12.3 Chiffrement basé sur fichier

Remarque: Le chiffrement basé sur fichier n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

Si une stratégie déterminant le chiffrement de fichiers s'applique à un emplacement de votre ordinateur, un symbole de clé jaune s'affiche en regard des fichiers concernés dans l'Explorateur Windows.

Le symbole de clé jaune seul n'indique pas nécessairement que tous les fichiers du lecteur sont déjà chiffrés. Un chiffrement initial doit tout d'abord être effectué.

Les clés de chiffrement basé sur fichier que vous créez localement sont utilisées. Soit le chiffrement d'un volume démarre automatiquement, soit vous devez lancer le processus.

1. Si le chiffrement ne démarre pas automatiquement, sélectionnez Chiffrement de fichier > Démarrer le chiffrement via les extensions de l'Explorateur.
2. Une boîte de dialogue permettant de sélectionner une clé locale s'affiche au démarrage du chiffrement.
3. Si la boîte de dialogue utilisée pour la sélection des clés n'en contient aucune, fermez-la, puis créez à nouveau une ou plusieurs clés (**Icône de la barre d'état système > Créer une nouvelle clé**).
4. Connectez-vous de nouveau à votre ordinateur.

Le chiffrement redémarre et les clés s'affichent à présent dans la boîte de dialogue pour le chiffrement initial.

5. Sélectionnez une clé, puis cliquez sur **OK**.

Toutes les données du volume concerné sont chiffrées.

12.3.1 Définition d'une clé par défaut

En définissant une clé par défaut, vous définissez la clé à utiliser pour le chiffrement pendant le fonctionnement.

1. Vous pouvez définir la clé par défaut via le menu contextuel du fichier d'un volume ou via le menu contextuel du support amovible.
2. Sélectionnez **Chiffrement de fichier > Définir la clé par défaut** pour afficher une boîte de dialogue permettant de sélectionner la clé.

La clé que vous avez sélectionnée est utilisée pour tous les processus de chiffrement à venir sur le volume.

3. Pour utiliser une autre clé, définissez une nouvelle clé par défaut.

12.3.2 État du chiffrement

Sur les volumes chiffrés selon la méthode basée sur fichier, chaque fichier est indiqué par des symboles de clé de différentes couleurs. Les couleurs indiquent le statut du chiffrement.

- **Clé verte** : Le fichier est chiffré et vous pouvez y accéder.
- **Clé grise** : Une stratégie de chiffrement s'applique au fichier. Il n'est cependant pas encore chiffré.
- **Clé rouge** : Le fichier est chiffré avec une clé ne faisant pas partie de votre jeu de clés. Vous ne pouvez pas y accéder.

Vous pouvez également afficher l'état du chiffrement d'un fichier via son menu contextuel. Sélectionnez **Chiffrement de fichier > Afficher le statut du chiffrement** pour ouvrir une fenêtre indiquant l'état du chiffrement.

Si vous sélectionnez **Chiffrement de fichier > Statut du chiffrement** dans le menu contextuel du volume, une boîte de dialogue s'affiche indiquant tous les fichiers et leur statut de chiffrement.

12.4 Restrictions d'accès aux volumes

Sophos SafeGuard refuse l'accès aux volumes dans les cas suivants :

12.4.1 Le chiffrement des volumes a échoué.

L'accès au volume est refusé s'il existe une stratégie qui définit qu'un volume ou type de volume doit être chiffré et que le processus de chiffrement échoue.

Un message s'affiche lorsque vous tentez d'accéder au volume.

12.4.2 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 comme texte brut ou chiffrés par Sophos SafeGuard.

L'accès au volume est refusé s'il existe une stratégie qui définit qu'un volume de ce type doit être chiffré. Un message s'affiche lorsque vous tentez d'accéder au volume.

Vous pouvez accéder au volume si aucune stratégie de chiffrement n'est définie pour l'objet du système de fichiers non identifié.

13 SafeGuard Data Exchange

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

SafeGuard Data Exchange vous permet de chiffrer des données stockées sur des supports amovibles connectés à votre ordinateur et de les échanger 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 dont les clés appropriées sont disponibles peuvent lire le contenu des données chiffrées. Tout processus de chiffrement ultérieur est exécuté de manière transparente. Le chiffrement transparent signifie que des données, chiffrées et enregistrées, sont déchiffrées automatiquement par une application lors de l'accès suivant.

Le fichier est rechiffré automatiquement lorsque vous l'enregistrez. Au quotidien, vous ne remarquez pas que les données sont chiffrées. Cependant, lorsque vous déconnectez le support amovible, les données restent chiffrées et protégées contre tout accès non autorisé. Les utilisateurs non autorisés peuvent accéder physiquement aux fichiers mais ne peuvent pas les lire sans SafeGuard Data Exchange et la clé correspondante.

Remarque: Le comportement de SafeGuard Data Exchange sur votre ordinateur est défini via des stratégies par le responsable de la sécurité.

Le responsable de la sécurité définit la gestion des données de supports amovibles. Il peut, par exemple, définir un chiffrement obligatoire des fichiers stockés sur un quelconque support amovible. Dans ce cas, tous les fichiers non chiffrés existant sur le périphérique sont initialement chiffrés. De surcroît, tous les nouveaux fichiers enregistrés sur support amovible sont chiffrés. Si des fichiers existants ne doivent pas être chiffrés, le responsable de la sécurité peut choisir d'autoriser l'accès à des fichiers non chiffrés existants. Dans ce cas, SafeGuard Data Exchange ne chiffre pas les fichiers non chiffrés existants. Les nouveaux fichiers sont toutefois chiffrés. Vous pouvez ainsi lire et modifier les fichiers non chiffrés existants mais ils sont chiffrés dès que vous les renommez. Vous n'êtes pas autorisé non plus à accéder aux fichiers non chiffrés, qui resteront non chiffrés.

Deux méthodes permettent d'échanger des fichiers chiffrés et stockés sur un support amovible :

- **Sophos SafeGuard est installé sur l'ordinateur du destinataire** : Vous pouvez utiliser des clés disponibles pour vous deux ou créer une clé. Si vous générez une nouvelle clé, vous devez fournir la passphrase de la clé au destinataire des données.
- **Sophos SafeGuard n'est *pas* installé sur l'ordinateur du destinataire** : Sophos SafeGuard propose SafeGuard Portable. Cet utilitaire peut être copié automatiquement sur le support amovible en plus des fichiers chiffrés. Grâce à SafeGuard Portable et à la passphrase correspondante, le destinataire peut déchiffrer les fichiers chiffrés et les rechiffrer sans que SafeGuard Data Exchange ne soit installé sur son ordinateur.

13.1 Passphrase du support unique pour chaque périphérique amovible connecté à l'ordinateur

SafeGuard Data Exchange permet de définir une passphrase du support unique qui vous donne accès à tous les périphériques amovibles connectés à l'ordinateur, indépendamment de la clé utilisée pour chiffrer les fichiers individuels.

Le cas échéant, l'accès aux fichiers chiffrés peut être accordé par la seule présentation d'une passphrase du support. La passphrase du support est associée aux ordinateurs.

Une passphrase du support est utile dans les situations suivantes :

- Vous souhaitez utiliser des données chiffrées sur un support amovible sur des ordinateurs sur lesquels Sophos SafeGuard n'est pas installé (SafeGuard Data Exchange en combinaison avec SafeGuard Portable).
- Vous souhaitez échanger des données avec des utilisateurs externes : en leur communiquant la passphrase du support, vous pouvez leur permettre d'accéder à tous les fichiers du support amovible, avec une passphrase unique, indépendamment de la clé utilisée pour chiffrer les fichiers individuels.

Vous pouvez également limiter l'accès à tous les fichiers en ne communiquant à l'utilisateur externe que la passphrase d'une clé spécifique. Dans ce cas, l'utilisateur externe a accès uniquement aux fichiers chiffrés au moyen de cette clé. Les autres fichiers ne pourront pas être lus.

Si SafeGuard Data Exchange est installé sur votre ordinateur, les supports amovibles seront gérés selon la configuration du responsable de la sécurité.

Un responsable de la sécurité peut définir les paramètres de comportement suivants de SafeGuard Data Exchange (combinaison de plusieurs paramètres possible) :

- **Chiffrement initial de tous les fichiers** : Dans ce cas, le chiffrement de toutes les données contenues sur un support amovible démarre dès que le périphérique est connecté à l'ordinateur. Le paramètre garantit que les supports amovibles ne contiennent que des données chiffrées. Au démarrage du chiffrement, vous êtes invité à sélectionner une clé.
- **Vous pouvez annuler le chiffrement initial** : Au démarrage du chiffrement initial, une boîte de dialogue s'affiche vous permettant d'annuler le chiffrement initial.
- **Vous n'êtes pas autorisé à accéder à des données non chiffrées** : Dans ce cas, SafeGuard Data Exchange n'accepte que des données chiffrées sur les supports amovibles. S'il existe des données non chiffrées sur les supports amovibles, le système ne vous autorise pas à y accéder. Vous ne pouvez accéder aux données qu'une fois les fichiers chiffrés.
- **Vous êtes autorisé à déchiffrer des fichiers** : Dans ce cas, vous pouvez effectivement déchiffrer les fichiers sur des supports amovibles. Un fichier effectivement déchiffré reste en texte brut sur le support amovible, s'il a été transféré à un tiers par exemple.
- **Vous êtes autorisé à définir une passphrase du support pour le support amovible** : Vous êtes invité à saisir une passphrase du support la première fois que vous vous connectez à un support amovible.
- **Dossier en texte brut sur support amovible** : Le responsable de la sécurité peut définir un dossier en texte brut qui sera créé sur tous vos supports amovibles. Les fichiers de ce dossier ne seront pas chiffrés par SafeGuard Data Exchange.

13.1.1 Supports pris en charge

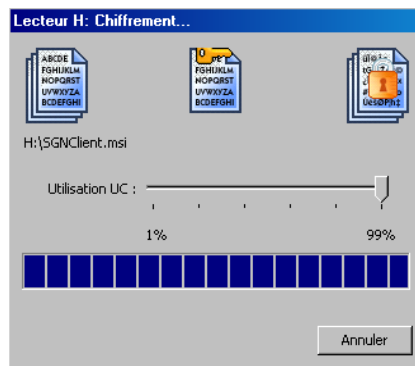
SafeGuard Data Exchange prend en charge les supports amovibles suivants :

- Cartes mémoire USB
- Disques durs externes connectés via USB ou FireWire
- Lecteurs de CD-RW (UDF)
- Lecteurs de DVD-RW (UDF)
- FireWire
- Cartes mémoire dans des lecteurs de cartes USB (ZIP, JAZ inclus)

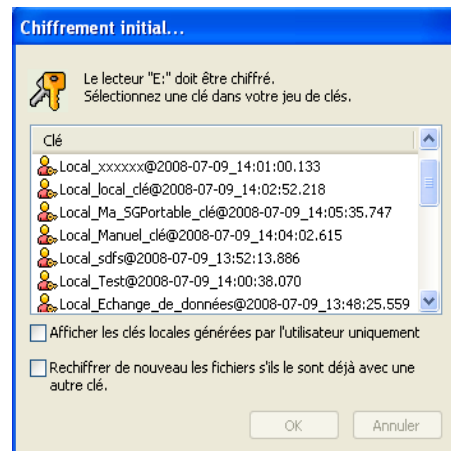
13.2 Chiffrement de supports amovibles

13.2.1 Chiffrement initial

Le chiffrement des données non chiffrées contenues sur des supports amovibles démarre automatiquement dès que vous connectez les supports au système ou nécessite que vous lanciez le processus manuellement.



1. Pour démarrer le processus de chiffrement, sélectionnez **Chiffrement de fichier > Démarrer le chiffrement** via le menu contextuel de l'Explorateur Windows. Si aucune clé spécifique n'a été définie, une boîte de dialogue de sélection de clé s'affiche.



2. Sélectionnez une clé.
3. Si la boîte de dialogue utilisée pour la sélection des clés n'en contient aucune, fermez-la, puis créez à nouveau une ou plusieurs clés (**Icône de la barre d'état système > Créer une nouvelle clé**).

4. Cliquez sur **OK**.
5. Toutes les données contenues sur le support amovible sont chiffrées.
6. La clé par défaut est utilisée tant qu'aucune autre clé n'est définie par défaut. Si vous changez la clé par défaut, la nouvelle est utilisée pour le chiffrement initial des périphériques amovibles qui sont connectés à l'ordinateur par la suite.

Si l'option **Rechiffrer de nouveau les fichiers s'ils le sont déjà avec une autre clé** est activée, les fichiers chiffrés avec une clé existante sont déchiffrés et rechiffrés avec la nouvelle clé.

Dépassement de délai du chiffrement initial

Si le chiffrement initial est configuré pour démarrer automatiquement, il se peut que vous ayez le droit d'annuler le chiffrement initial. Dans ce cas, le bouton **Annuler** est activé, un bouton **Démarrer** s'affiche et le démarrage du processus de chiffrement est retardé de 30 secondes. Si vous ne cliquez pas sur le bouton **Annuler** pendant cette période, le chiffrement initial démarre automatiquement après 30 secondes. Si vous cliquez sur **Démarrer**, le chiffrement initial démarre immédiatement.

13.2.1.1 Chiffrement initial en cas d'utilisation de la passphrase du support

Si l'utilisation d'une passphrase de support a été spécifiée via une stratégie, vous êtes invité à saisir la passphrase du support avant le chiffrement initial. La passphrase du support est valide pour tous vos supports amovibles et est liée à votre ordinateur ou à tous les ordinateurs auxquels vous êtes autorisé à vous connecter.

Le chiffrement initial ne démarre pas tant que vous n'avez pas saisi la passphrase du support. Après l'avoir fait, le chiffrement initial démarre automatiquement.

Après avoir saisi une fois la passphrase du support, le chiffrement initial démarre automatiquement lorsque vous connectez un périphérique différent à votre ordinateur.

Remarque: Sur les ordinateurs sur lesquels votre passphrase de support n'est pas définie, le chiffrement initial ne démarre pas.

13.2.2 Chiffrement transparent

Si les paramètres définis pour votre ordinateur spécifient que les fichiers doivent être chiffrés sur les supports amovibles, tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente.

Les fichiers sont chiffrés lorsqu'ils sont inscrits sur les supports amovibles et déchiffrés lorsqu'ils sont copiés ou déplacés des supports amovibles vers un autre emplacement.

Remarque: Les données sont déchiffrées uniquement si elles sont copiées ou déplacées vers un emplacement auquel aucune autre stratégie de chiffrement ne s'applique. Les données sont alors disponibles en texte brut, à cet emplacement. Si une autre stratégie de chiffrement s'applique au nouvel emplacement, les données seront chiffrées.

13.2.2.1 Passphrase du support

Si l'utilisation d'une passphrase du support a été spécifiée par une stratégie, vous êtes invité à la saisir lorsque vous connectez un périphérique amovible pour la première fois après l'installation de SafeGuard Data Exchange.

Si la boîte de dialogue est affichée, lisez soigneusement les informations et indiquez une passphrase de support. Vous pouvez utiliser cette passphrase du support unique pour accéder à tous les fichiers chiffrés sur votre support amovible, indépendamment de la clé effectivement utilisée pour les chiffrer.

La passphrase du support est valide pour tous les périphériques que vous connectez à l'ordinateur. La passphrase du support peut également être utilisée avec SafeGuard Portable et permet d'accéder à tous les fichiers, indépendamment de la clé utilisée pour les chiffrer.

13.2.2.2 Changer/réinitialiser la passphrase du support

Vous pouvez changer votre passphrase du support à tout moment en utilisant la commande **Changer la passphrase du support** à partir du menu d'icônes de la barre d'état. Une boîte de dialogue s'affiche, dans laquelle vous devez saisir l'ancienne et la nouvelle passphrase du support, puis confirmer la nouvelle.

Si vous avez oublié votre passphrase du support, cette boîte de dialogue offre également une option permettant de la réinitialiser. Si vous activez l'option **Réinitialiser la passphrase du support** et cliquez sur **OK**, vous êtes informé que votre passphrase de support sera réinitialisée à la prochaine connexion.

Déconnectez-vous immédiatement, puis reconnectez-vous. Sélectionnez ensuite **Changer la passphrase du support** dans le menu d'icônes de la barre d'état. Vous êtes informé qu'il n'existe pas de passphrase du support sur votre ordinateur et vous êtes invité à en saisir une nouvelle.

13.2.2.3 Synchronisation de la passphrase du support

La passphrase du support de vos périphériques et de votre ordinateur sera synchronisée automatiquement. Si vous changez la passphrase du support de votre ordinateur et connectez un périphérique qui utilise encore une ancienne version de la passphrase du support, vous êtes informé que les passphrases de support ont été synchronisées. Ceci est vrai pour tous les ordinateurs auxquels vous êtes autorisé à vous connecter.

Remarque: Après avoir changé votre passphrase du support, vous devez connecter tous vos supports amovibles à votre ordinateur. Ceci garantit que la nouvelle passphrase du support est utilisée immédiatement sur tous vos périphériques (synchronisation).

13.2.2.4 Définition d'une clé par défaut

En définissant une clé par défaut, vous définissez la clé à utiliser pour un chiffrement pendant une opération classique.

Vous pouvez définir la clé par défaut via le menu contextuel d'un fichier du support amovible ou via le menu contextuel du support amovible. Par ailleurs, vous pouvez définir une clé par défaut immédiatement lorsque vous créez une nouvelle clé locale dans la boîte de dialogue « Créer une clé ».

Sélectionnez **Chiffrement de fichier > Définir la clé par défaut** pour afficher une boîte de dialogue permettant de sélectionner la clé.

La clé sélectionnée dans cette boîte de dialogue est utilisée pour tous les processus de chiffrement ultérieurs sur le support amovible. Si vous voulez utiliser une autre clé, vous pouvez en définir une nouvelle par défaut à tout moment.

Vous pouvez définir, à l'aide d'une stratégie, une clé par défaut qui sera utilisée pour le chiffrement. Si elle n'est pas définie par une stratégie, vous êtes invité à spécifier une clé initiale par défaut.

13.3 Échange de données à l'aide de SafeGuard Data Exchange

Vous trouverez ci-après des exemples d'application type pour l'échange de données sécurisé à l'aide de SafeGuard Data Exchange :

- Échange de données avec des utilisateurs Sophos SafeGuard ne disposant pas des mêmes clés que vous.

Dans ce cas, créez une clé locale et chiffrez les données avec cette clé. Les clés créées localement sont protégées par une passphrase et peuvent être importées par Sophos SafeGuard. Vous fournissez la passphrase au destinataire des données. Grâce à la passphrase, le destinataire peut importer la clé et accéder aux données.

- Échange de données avec des utilisateurs sans Sophos SafeGuard

Pour les utilisateurs ne disposant pas de Sophos SafeGuard sur leurs ordinateurs, il existe SafeGuard Portable. Pour échanger des données avec SafeGuard Portable, des clés locales doivent être utilisées avec une passphrase.

SafeGuard Portable doit également être copié sur le support amovible. Vous devez également fournir au destinataire les données chiffrées avec la passphrase correspondante. Grâce à la passphrase et à SafeGuard Portable, l'utilisateur peut déchiffrer les fichiers chiffrés, les modifier par exemple, et les réenregistrer chiffrés sur le support amovible. SafeGuard Portable étant une application indépendante, aucun autre logiciel ne doit être installé sur le système hôte pour pouvoir accéder aux données chiffrées.

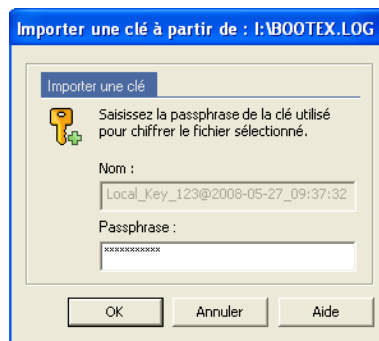
Remarque: Le responsable de la sécurité détermine si SafeGuard Portable est copié sur le support amovible via la stratégie de sécurité qui s'applique à vous.

13.3.1 Importation de clés à partir d'un fichier

Si vous recevez des supports amovibles contenant des données chiffrées avec des clés locales définies par un utilisateur, vous pouvez importer la clé nécessaire au déchiffrement dans votre jeu de clés.

Pour importer la clé, vous avez besoin de la passphrase correspondante. La personne qui a chiffré les données doit vous fournir la passphrase.

Sélectionnez le fichier correspondant sur le support amovible et cliquez sur Chiffrement de fichier > Gestion des clés > Importer une clé.

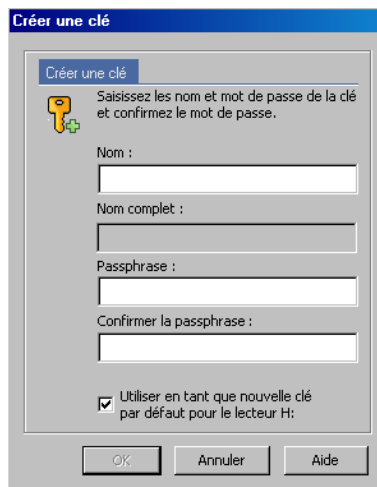


Saisissez la passphrase dans la boîte de dialogue qui s'affiche. La clé est importée et vous pouvez accéder au fichier.

13.3.2 Création de clés locales

Pour créer une clé locale définie par l'utilisateur, veuillez procéder comme suit :

1. Cliquez avec le bouton droit de la souris sur l'icône de la barre d'état de Sophos SafeGuard dans la barre des tâches Windows.
2. Cliquez sur **Créer une nouvelle clé**.



3. Dans la boîte de dialogue Créer une nouvelle clé, entrez un **Nom** et une **Passphrase** pour la clé.

Le nom interne de la clé est affiché dans le champ situé au-dessous.

4. Confirmez la passphrase.

Si vous entrez une passphrase simple, un message d'avertissement s'affiche. Pour renforcer le niveau de sécurité, nous vous recommandons d'utiliser des passphrases complexes. Vous pouvez également décider d'utiliser la passphrase malgré le message d'avertissement. La passphrase doit également être conforme aux stratégies de l'entreprise qui sont définies. Dans le cas contraire, un message d'avertissement s'affichera.

5. L'option **Utiliser en tant que nouvelle clé par défaut pour le lecteur** vous permet de définir immédiatement la nouvelle clé comme clé par défaut pour le lecteur affiché.

La clé par défaut que vous définissez ici est utilisée pour le chiffrement pendant une opération classique. Elle sera utilisée jusqu'à ce qu'une autre clé soit définie.

6. Cliquez sur **OK**.

Si vous définissez cette clé comme clé par défaut, toute donnée ultérieure copiée sur le support amovible sera chiffrée avec cette clé.

Pour que le destinataire puisse déchiffrer toutes les données contenues sur le support amovible, vous devrez peut-être rechiffrer les données sur le support amovible à l'aide de la clé créée localement. Pour cela, sélectionnez **Chiffrement de fichier > Démarrer le chiffrement** dans le menu contextuel du périphérique dans l'Explorateur Windows. Sélectionnez la clé locale requise et chiffrer les données. Cette opération n'est pas nécessaire si vous utilisez une passphrase du support.

13.4 Gravure de fichiers sur CD/DVD en utilisant l'assistant Graver un CD de Windows

Remarque: Avec Windows XP, vous pouvez uniquement graver des fichiers sur CD via l'Assistant Graver un CD de Windows. Windows XP ne prend pas en charge la gravure de fichiers sur DVD avec l'Assistant Graver un CD.

SafeGuard Data Exchange vous permet de graver des fichiers chiffrés sur CD en utilisant l'Assistant Graver un CD de Windows.

Pour ce faire, une règle de chiffrement doit être spécifiée pour le lecteur d'enregistrement sur CD. SafeGuard Data Exchange ajoute une boîte de dialogue à l'Assistant Graver un CD. Vous pouvez y indiquer la méthode de gravure des fichiers sur CD (chiffrés ou bruts).

Remarque: S'il n'existe pas de règle de chiffrement pour le lecteur d'enregistrement sur CD, les fichiers sont toujours gravés sur CD en texte brut. La boîte de dialogue SafeGuard Data Exchange, dans laquelle il est possible d'indiquer l'état de chiffrement des fichiers à graver sur CD, ne s'affiche pas.

Après avoir saisi un nom pour le CD, l'extension de gravure de disque amovible SafeGuard s'affiche.

Sous **Statistique**, les informations suivantes s'affichent :

- nombre de fichiers sélectionnés pour la gravure sur CD ;
- nombre de fichiers chiffrés parmi les fichiers sélectionnés ;
- nombre de fichiers chiffrés parmi les fichiers bruts.

Sous **Statut**, les clés utilisées pour chiffrer les fichiers déjà chiffrés sont affichées.

Pour chiffrer les fichiers à graver sur CD, c'est toujours la clé indiquée dans la règle de chiffrement pour le lecteur d'enregistrement sur CD qui est utilisée.

Les fichiers à graver sur le CD peuvent être chiffrés avec des clés différentes si la règle de chiffrement du lecteur d'enregistrement sur CD a été modifiée. Si la règle de chiffrement a été désactivée lorsque des fichiers ont été ajoutés, les fichiers bruts concernés peuvent se trouver dans le dossier des fichiers à copier sur CD.

13.4.1 Chiffrement de fichiers sur CD

Si vous voulez graver les fichiers chiffrés sur CD, cliquez sur le bouton **(Re)chiffrer tous les fichiers**.

Si nécessaire, les fichiers déjà chiffrés sont chiffrés à nouveau et les fichiers bruts sont chiffrés. Sur le CD, les fichiers sont chiffrés avec la clé indiquée dans la règle de chiffrement pour le lecteur d'enregistrement sur CD.

13.4.2 Gravure de fichiers bruts sur CD

Si vous sélectionnez **Déchiffrer tous les fichiers**, les fichiers sont d'abord déchiffrés, puis gravés sur le CD.

13.4.3 Copier SafeGuard Portable sur le support optique

Si vous sélectionnez cette option, SafeGuard Portable sera également copié sur le CD. La lecture et la modification des fichiers chiffrés avec SafeGuard Data Exchange sans que SafeGuard Data Exchange soit installé sont ainsi possibles.

13.4.4 Gravure de CD/DVD avec Windows Vista

Windows Vista propose également un Assistant Graver un CD pour les CD/DVD.

L'extension de gravure de disque SafeGuard pour l'Assistant Graver un CD n'est disponible que pour la gravure de CD/DVD au format **mastérisé**. L'Assistant ne s'affiche que si des fichiers doivent être copiés sur CD/DVD au format **mastérisé**.

Pour le système de fichiers dynamique, aucun assistant d'enregistrement n'est requis. Dans ce cas, le lecteur d'enregistrement est utilisé comme n'importe quel autre support amovible. S'il existe une règle de chiffrement pour le lecteur d'enregistrement, les fichiers sont chiffrés automatiquement lors de leur copie sur CD/DVD.

13.5 SafeGuard Portable

Remarque: SafeGuard Portable n'est pas disponible avec ESDP (Endpoint Security and Data Protection).

Grâce à SafeGuard Portable, vous pouvez échanger des données chiffrées via des supports amovibles avec des destinataires ne disposant pas de SafeGuard Data Exchange sur leurs ordinateurs. Des données chiffrées via SafeGuard Data Exchange peuvent être chiffrées et déchiffrées avec SafeGuard Portable. Ceci est possible en copiant automatiquement un programme (SGPortable.exe) sur le support amovible.

Remarque: SafeGuard Portable chiffre ou déchiffre uniquement les fichiers chiffrés avec AES256.

Si vous utilisez SafeGuard Portable en combinaison avec la passphrase de support appropriée, vous pouvez accéder à tous les fichiers chiffrés, indépendamment de la clé utilisée pour les chiffrer. La passphrase d'une clé locale ne vous donne accès qu'aux fichiers qui ont été chiffrés à l'aide de cette clé. Le destinataire peut déchiffrer des données chiffrées et les chiffrer à nouveau.

Remarque: La passphrase du support ou la passphrase d'une clé locale doit être communiquée au préalable au destinataire.

Il peut également utiliser des clés existantes créées via SafeGuard Data Exchange pour le chiffrement ou créer une clé via SafeGuard Portable (pour les nouveaux fichiers, par exemple).

Il n'est pas nécessaire que SafeGuard Portable soit installé ou copié sur l'ordinateur du destinataire. Il reste sur le support amovible.

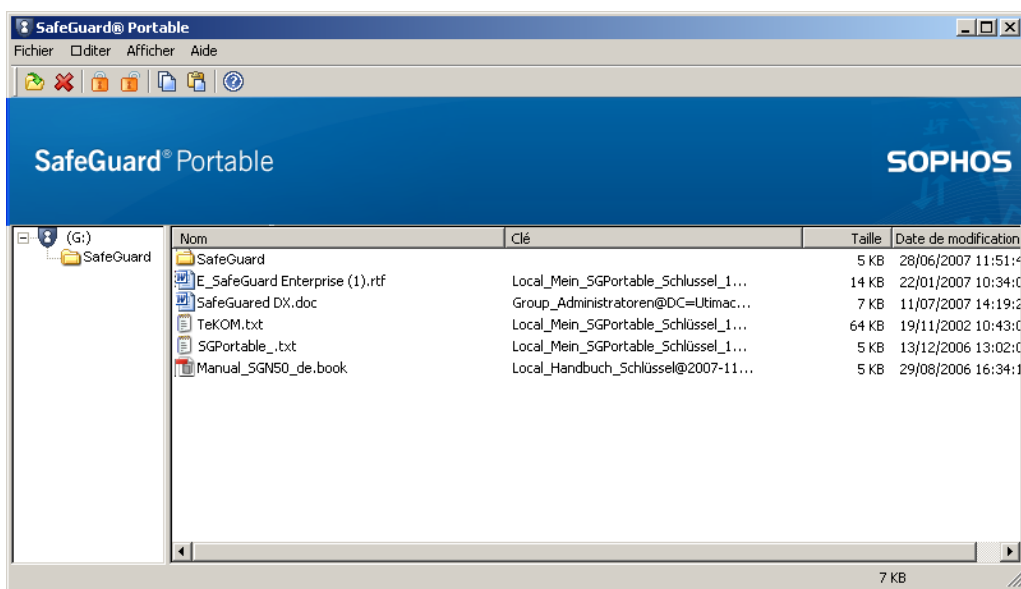
Remarque: En tant qu'utilisateur de Sophos SafeGuard, vous n'avez généralement pas besoin de SafeGuard Portable. La description suivante part du principe que les utilisateurs n'ont pas installé Sophos SafeGuard sur leur ordinateur et doivent donc utiliser SafeGuard Portable pour modifier les données chiffrées.

13.5.1 Édition de fichiers à l'aide de SafeGuard Portable

Vous avez reçu un support amovible contenant des fichiers chiffrés avec SafeGuard Data Exchange ainsi qu'un dossier nommé SGPortable. Ce dossier contient le fichier SGPortable.exe.

1. Démarrez SafeGuard Portable en double-cliquant sur SGPortable.exe.

Grâce à SafeGuard Portable, vous pouvez déchiffrer les données chiffrées contenues sur le support amovible et les rechiffrer. SafeGuard Portable propose une fonctionnalité similaire à l'Explorateur Windows.



En plus d'afficher les détails d'un fichier, comme dans l'Explorateur Windows (nom, taille, etc), SafeGuard Portable affiche la colonne **Clé**. Cette colonne indique si les données correspondantes sont chiffrées. Si un fichier est chiffré, le nom de la clé utilisée s'affiche.

Remarque: Vous ne pouvez déchiffrer des fichiers que si vous connaissez la passphrase correspondant à la clé utilisée.

2. Pour modifier les fichiers d'un support amovible, cliquez sur le fichier pour le sélectionner et choisissez la commande appropriée dans le menu contextuel (en cliquant avec le bouton droit de la souris) ou dans le menu **Fichier**.

Les commandes de menu suivantes sont disponibles dans le menu contextuel :

Définir la clé de chiffrement	Ouvre la boîte de dialogue Saisir une clé. Dans cette boîte de dialogue, vous pouvez générer une clé de chiffrement via SafeGuard Portable.
Chiffrer	Chiffre le fichier actif sur le support amovible. La dernière clé utilisée est utilisée pour le chiffrement.
Déchiffrer	Ouvre la boîte de dialogue Saisir passphrase. Entrez la passphrase pour déchiffrer le fichier sélectionné dans cette boîte de dialogue.
État du chiffrement	Affiche une boîte de dialogue et indique l'état du chiffrement du fichier.
Copier dans	Copie le fichier dans un dossier de votre choix et le déchiffre.
Supprimer	Supprime le fichier activé du support amovible.

Vous pouvez également sélectionner les commandes **Ouvrir**, **Supprimer**, **Chiffrer**, **Déchiffrer** et **Copier** via les icônes affichées dans la barre d'outils.

13.5.1.1 Définition des clés de chiffrement

Pour chiffrer un fichier sur un support amovible et créer une clé de chiffrement :

1. Dans le menu contextuel ou dans le menu **Fichier**, sélectionnez **Définir la clé de chiffrement**.
La boîte de dialogue Saisir une clé s'affiche.
2. Entrez un **Nom** et une **Passphrase** pour la clé. **Confirmez** la passphrase et cliquez sur **OK**.
La passphrase doit être conforme aux stratégies de l'entreprise qui sont définies. Dans le cas contraire, un message d'avertissement s'affichera.

La clé est créée et sera désormais utilisée pour le chiffrement.

13.5.1.2 Chiffrement

Pour chiffrer un fichier sur un support amovible :

1. Sélectionnez le fichier dans l'explorateur SafeGuard Portable, puis sélectionnez **Chiffrer** dans le menu contextuel.

Le fichier est chiffré avec la dernière clé utilisée par SafeGuard Portable.

Lors de l'enregistrement de nouveaux fichiers sur le support amovible, via un glisser-déposer dans l'explorateur SafeGuard Portable, il vous sera demandé si vous souhaitez les chiffrer.

Si oui et s'il s'agit du premier chiffrement avec SafeGuard Portable, une boîte de dialogue de définition des clés s'affiche. Dans cette boîte de dialogue, entrez le nom de la clé et la passphrase (et confirmez la passphrase). Cliquez sur **OK**.

2. Sélectionnez le fichier à chiffrer avec la clé que vous venez de définir, puis sélectionnez **Chiffrer** dans le menu contextuel ou dans le menu **Fichier**.

Le fichier est chiffré. Un message s'affiche une fois le chiffrement terminé.

Remarque: La dernière clé utilisée et définie par SafeGuard Portable sera utilisée pour tout processus de chiffrement ultérieur exécuté avec SafeGuard Portable à moins que vous n'en définissiez une nouvelle.

13.5.1.3 Déchiffrement

Pour déchiffrer un fichier sur un support amovible :

1. Dans l'explorateur SafeGuard Portable, sélectionnez le fichier puis, dans le menu contextuel, sélectionnez **Déchiffrer**.

La boîte de dialogue de saisie de la passphrase du support ou la passphrase d'une clé locale est affichée.

2. Entrez la passphrase correspondante (l'expéditeur doit vous la fournir) et cliquez sur **OK**.

Le fichier est déchiffré.

La passphrase du support permet d'accéder à tous les fichiers chiffrés du support amovible, indépendamment de la clé utilisée pour les chiffrer. Si vous disposez uniquement de la passphrase d'une clé locale, vous n'avez accès qu'aux fichiers chiffrés avec cette clé.

Si vous déchiffrez un fichier chiffré avec une clé que vous avez générée dans SafeGuard Portable, il est déchiffré automatiquement.

Après avoir déchiffré des fichiers sur des supports amovibles et entré la passphrase de la clé, vous n'avez pas besoin de l'entrer à nouveau lors du prochain chiffrement ou déchiffrement de fichiers chiffrés avec la même clé.

SafeGuard Portable stocke la passphrase tant que l'application est exécutée. La dernière clé utilisée par SafeGuard Portable est utilisée pour le chiffrement.

Une fois les fichiers déchiffrés, ils sont disponibles en texte brut sur le support amovible. Les fichiers ayant été déchiffrés seront chiffrés de nouveau lors de la fermeture de SafeGuard Portable.

13.5.1.4 Chiffrement de nouveaux fichiers avec SafeGuard Portable

Vous pouvez également copier vos propres fichiers sous forme chiffrée sur le support amovible avec SafeGuard Portable.

Pour cela :

1. Déplacez simplement les fichiers souhaités dans l'explorateur SafeGuard Portable à l'aide d'un glisser-déposer.
Le système vous demande si vous souhaitez chiffrer le fichier concerné.
2. Confirmez que le fichier a été chiffré avec la dernière clé utilisée et qu'il a été copié dans le support amovible.

13.5.1.5 État du chiffrement

Pour déterminer l'état du chiffrement d'un fichier :

1. Sélectionnez le fichier, puis **État du chiffrement** dans le menu contextuel ou dans le menu **Fichier**.
L'état du chiffrement est également indiqué dans la colonne **Clé** en regard du nom du fichier dans l'explorateur SafeGuard Portable.

13.5.2 Autres opérations à l'aide de SafeGuard Portable

Les opérations suivantes sont également disponibles :

- **Ouvrir** : Cette commande de menu n'est disponible que via le menu Fichier de SafeGuard Portable.

À l'ouverture d'un fichier chiffré via cette commande de menu, vous êtes invité à entrer la passphrase. Entrez la passphrase et cliquez sur **OK**. Le fichier est chiffré et ouvert.

- **Supprimer** : Supprime le fichier sélectionné.

- **Copier dans** : Cette commande de menu n'est disponible que dans le menu contextuel (que vous pouvez afficher à l'aide du bouton droit de la souris) dans l'explorateur SafeGuard Portable.

Grâce à cette commande, vous pouvez copier les fichiers des supports amovibles vers un autre lecteur de votre ordinateur.

- **Quitter** : Cette commande de menu n'est disponible que dans le menu Fichier de SafeGuard Portable.

Quitter ferme SafeGuard Portable.

14 Sophos SafeGuard et Lenovo Rescue and Recovery

Pour obtenir des informations sur les versions de Lenovo Rescue and Recovery (RnR) prises en charge par Sophos SafeGuard, consultez la base de connaissances : <http://www.sophos.com/support/knowledgebase/article/108383.html>

Il est possible de restaurer des sauvegardes de système d'exploitation complètes sur une partition chiffrée sans déchiffrer nécessairement et préalablement le disque dur. Ceci représente un gain de temps considérable lors d'une récupération après sinistre. Sophos SafeGuard a été officiellement certifié par Lenovo pour cette fonctionnalité.

La principale fonction de Lenovo Rescue and Recovery vise à restaurer des données en un seul clic. Même si le système d'exploitation principal est endommagé et ne démarre plus, Rescue and Recovery permet d'enregistrer des données via un environnement d'urgence (WinPE). Vous pouvez accéder aux outils de sauvetage via le bureau de Microsoft Windows ou en appuyant sur la touche bleue ThinkVantage intégrée aux systèmes Lenovo.

Lenovo Rescue and Recovery est particulièrement utile pour les utilisateurs mobiles qui ne disposent pas d'un support administratif. Ils peuvent par exemple l'utiliser lors d'un déplacement professionnel, pour restaurer leur ordinateur.

14.1 Présentation

Sophos SafeGuard est intégré à la fonctionnalité Rescue and Recovery et prend en charge des fonctions Lenovo comme le bouton bleu ThinkVantage sur le clavier de portables Lenovo ou le bouton bleu Enter sur les claviers de PC.

Cette fonctionnalité intégrée vous permet de combiner cette méthode de sauvegarde et de récupération fiable avec des partitions de système d'exploitation chiffrées via Sophos SafeGuard. Les sauvegardes de systèmes chiffrés Sophos SafeGuard peuvent être stockées sur tout disque dur utilisé par RnR. En cas d'urgence, un système peut donc être restauré en chargeant la sauvegarde depuis une partition virtuelle ou de service ou depuis un support amovible comme un CD/DVD ou un disque dur USB.

Sophos SafeGuard n'est pas affecté par la restauration d'un système et tous les paramètres de chiffrement sont conservés. Inutile donc de réinstaller un quelconque logiciel. Vous ne devez pas recommencer le chiffrement.

Dans un environnement Sophos SafeGuard, Rescue and Recovery est basé sur la récupération WinPE. WinPE peut être démarré à partir de différents environnements :

- d'une partition virtuelle ou de service ;
- d'un support amovible comme un CD/DVD ou un disque dur USB.

14.2 Configuration minimale

- Dernier BIOS pour PC/portable.
- Pour en savoir plus sur la compatibilité des versions Rescue and Recovery avec des versions Sophos SafeGuard, consultez : <http://www.sophos.com/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery peut être utilisé pour récupérer des volumes chiffrés via Sophos SafeGuard. Le package d'installation `SGNClient.msi` doit être installé.
- Pour Rescue and Recovery, les volumes doivent être chiffrés avec la clé machine définie. Rescue and Recovery n'est pas pris en charge pour les volumes chiffrés avec d'autres clés.

14.3 Installation

Lorsque le logiciel Rescue and Recovery est installé sur un disque dur sans partition de service, voici ce qui s'applique :

L'environnement Rescue and Recovery est installé sur une partition virtuelle sur la partition de disque dur « C: » de l'ordinateur (partition principale du disque dur principal).

Dans les sections suivantes, repérez la séquence d'installation de Rescue and Recovery et de Sophos SafeGuard. Nous vous recommandons d'installer Lenovo Rescue and Recovery avant d'installer Sophos SafeGuard.

14.3.1 Installation de Rescue and Recovery et de Sophos SafeGuard

Il est recommandé de respecter l'ordre d'installation suivant :

1. Installez la dernière version de Rescue and Recovery.
2. Installez la dernière version du module Sophos SafeGuard Device Encryption (`SGNClient.msi`).

Sophos SafeGuard vérifie si Rescue and Recovery est installé et ajoute ses fichiers et configurations propres à l'environnement de récupération Lenovo.

3. Vérifiez que l'authentification au démarrage est activée afin qu'aucune sauvegarde non autorisée ne puisse être restaurée.

Vous activez l'authentification au démarrage lors de l'installation de Sophos SafeGuard.

14.3.2 Le chiffrement de périphérique Sophos SafeGuard est déjà installé.

Les étapes d'installation nécessaires de Rescue and Recovery dépendent de l'emplacement de RnR WinPE.

- RnR WinPE se trouve sur le premier disque dur d'une partition de service ou d'une partition virtuelle

Dans ce cas, aucun paramètre Sophos SafeGuard automatique n'est défini pour l'environnement RnR WinPE. Vous devez lancer un outil Sophos SafeGuard nommé `SetupWinPE.exe` pour exécuter RnR WinPE et l'utiliser avec Sophos SafeGuard. Cet outil apportera toutes les modifications nécessaires à l'environnement WinPE.

Remarque: `SetupWinPE.exe` peut également être utilisé si la version RnR installée est mise à niveau. Dans le cas d'une mise à niveau de RnR, il est recommandé de relancer `SetupWinPE.exe` pour vérifier que toutes les modifications requises de WinPE ont été appliquées.

Remarque: Notez que cet outil ne peut être utilisé que pour un RnR WinPE situé sur un disque dur local.

- a) Installez Rescue and Recovery sur le disque dur local.
- b) Démarrez l'outil suivant:
`SetupWinPE.exe -r`
- c) Redémarrez le système d'exploitation Windows.

- RnR WinPE se trouve sur un CD-ROM ou un disque dur externe

Lorsque WinPE est créé via la fonction RnR Create Rescue and Recovery Media (Créer un support Rescue and Recovery), toutes les modifications nécessaires sont déjà apportées à l'environnement RnR WinPE.

- a) Installez Rescue and Recovery.
- b) Redémarrez le système d'exploitation Windows.

14.3.3 Rescue and Recovery est déjà installé

RnR WinPE se trouve sur le premier disque dur d'une partition de service ou virtuelle.

Dans ce cas, tous les pilotes et fichiers nécessaires sont copiés aux emplacements correspondants de RnR WinPE, et les entrées de registre nécessaires sont ajoutées aux fichiers de registre de WinPE.

Installez la dernière version du module Sophos SafeGuard Device Encryption (SGNClient.msi).

Sophos SafeGuard vérifie si Rescue and Recovery est installé et ajoute ses fichiers et configurations propres à l'environnement de récupération Lenovo (WinPE).

14.4 Mise à niveau

La mise à niveau suppose que Sophos SafeGuard et Rescue and Recovery sont installés et que vous souhaitez en mettre au moins un des deux à niveau.

14.4.1 Mise à niveau de Sophos SafeGuard

Si vous mettez à niveau Sophos SafeGuard, le système entier est mis à jour. Aucune autre configuration n'est donc nécessaire.

14.4.2 Mise à niveau de Rescue and Recovery

Si vous mettez à niveau Rescue and Recovery, exécutez SetupWinPE.exe avant de redémarrer après la mise à jour.

14.5 Désinstallation

Lors de la désinstallation des produits du logiciel :

- Nous vous recommandons de désinstaller Sophos SafeGuard avant de désinstaller Rescue and Recovery. Si Sophos SafeGuard est désinstallé alors que Rescue and Recovery est toujours installé, toutes les modifications spécifiques à Sophos SafeGuard (lecteurs ajoutés par exemple), les fichiers et entrées de registre sont supprimés de RnR WinPE.
- Ne désinstallez pas Sophos SafeGuard immédiatement après une restauration du système. Après une restauration système, redémarrez l'ordinateur une fois, puis désinstallez Sophos SafeGuard.
- Si Rescue and Recovery est supprimé alors que Sophos SafeGuard est toujours installé, les modifications RnR du secteur d'initialisation du MBR sont supprimées et le secteur d'initialisation du MBR d'origine est restauré.

14.6 Environnement d'initialisation et options de récupération

Sophos SafeGuard vous permet de démarrer dans l'environnement Rescue and Recovery après une connexion à l'authentification au démarrage (POA).

À partir du disque dur local

- La partition virtuelle sur le disque dur local ou la partition de service locale.
- Les volumes doivent être chiffrés dans Sophos SafeGuard avec la clé machine définie. Tous les pilotes nécessaires doivent être ajoutés à RnR WinPE. La clé machine définie est alors disponible dans l'environnement RnR WinPE et les volumes sont de nouveau accessibles.

Remarque: Sophos SafeGuard ne vous permet pas de démarrer dans l'environnement Rescue and Recovery lors d'une initialisation directement depuis le BIOS.

À partir d'un CD/DVD amorçable ou de tout support amovible amorçable

- Dans ce cas, aucune authentification n'est effectuée dans l'authentification au démarrage et aucune clé n'est disponible. Les volumes chiffrés sont donc inaccessibles. Si Rescue and Recovery est démarré directement à partir du BIOS, le système d'exploitation sera récupéré. Sophos SafeGuard sera supprimé lors du processus de restauration. Pour protéger de nouveau le système, Sophos SafeGuard doit être réinstallé.

14.7 Création d'une sauvegarde

Sous Windows, vous créez des sauvegardes à l'aide de Rescue and Recovery. Sur des ordinateurs sur lesquels Rescue and Recovery est déjà installé et Sophos SafeGuard est installé ultérieurement, un message s'affiche et invite l'utilisateur à créer une nouvelle sauvegarde du système.

Avant de créer une sauvegarde de votre système à l'aide de Rescue and Recovery, lisez la documentation fournie par Lenovo.

Sophos SafeGuard n'accepte que l'enregistrement des sauvegardes :

- sur le disque dur local ;
- sur un disque dur secondaire ;
- sur un disque dur USB ;
- sur le réseau ;
- sur une carte mémoire USB ;
- sur CD/DVD.

Les sauvegardes sont enregistrées par défaut dans le dossier `C:\RRUbackups`. Ce dossier est protégé par Rescue and Recovery s'il est stocké sur une partition locale du disque dur principal. Dans ce cas, il ne peut pas être supprimé ou effacé.

14.8 Restauration de sauvegardes de fichiers

Rescue and Recovery permet de restaurer des fichiers ou dossiers à partir de sauvegardes dans lesquelles Sophos SafeGuard est installé. Démarrez simplement Windows, puis Rescue and Recovery, et restaurez les fichiers sélectionnés. Vous ne devez pas redémarrer votre machine une fois la restauration terminée : vous pouvez utiliser vos fichiers immédiatement.

14.9 Restauration du système Sophos SafeGuard

Pour restaurer une sauvegarde système qui inclut Sophos SafeGuard, démarrez dans l'environnement Rescue and Recovery. L'environnement RnR apparaît dès que vous appuyez sur l'une des touches suivantes pendant le processus d'initialisation:

- « Thinkvantage » (portables Lenovo)
- Touche « bleue Enter » (PC de bureau Lenovo)
- **F11** avec d'autres claviers

1. Si vous utilisez un ordinateur Lenovo :

- a) Démarrez l'environnement Rescue and Recovery à partir d'un disque dur local en appuyant sur le bouton bleu « ThinkVantage » du clavier du portable Lenovo ou sur le bouton bleu « Enter » du clavier du PC Lenovo.

L'authentification au démarrage s'affiche.

- b) Entrez les informations d'identification Sophos SafeGuard.

2. Si vous n'utilisez pas un ordinateur Lenovo:

- a) Connectez-vous à partir de l'authentification au démarrage à l'aide de vos informations d'identification Sophos SafeGuard.
- b) Pendant l'initialisation de l'ordinateur, appuyez sur **F11** pour démarrer l'environnement Rescue and Recovery.

L'interface utilisateur de Rescue and Recovery s'affiche. L'écran d'accueil s'affiche.

3. Cliquez sur **Suivant**.

4. Dans le menu de gauche, sélectionnez **Sauvegarde de la restauration**.

Une boîte de dialogue s'affiche dans laquelle vous pouvez sélectionner la sauvegarde.

5. Sélectionnez la sauvegarde et restaurez-la.

14.10 Partitions de récupération de service et d'usine

Lenovo dote ses nouveaux ordinateurs de partitions préinstallées spécifiques :

- **Partition de service Lenovo** : contient l'environnement d'initialisation Rescue and Recovery.
- **Partition de récupération usine** : contient toutes les informations relatives aux paramètres d'usine de l'ordinateur et aux fonctions de récupération usine.

Sous Windows, ces partitions sont visibles sous des lettres de lecteurs distinctes.

Remarque: Lorsque ces partitions sont disponibles sur l'ordinateur, elles ne sont jamais chiffrées même si une stratégie de chiffrement est définie pour chiffrer tous les volumes, par exemple.

Si aucune partition n'existe sur l'ordinateur et que vous souhaitez en créer une, faites-le avant d'installer Sophos SafeGuard. Pour plus d'informations, reportez-vous à la documentation Lenovo.

14.11 POA désactivé et Lenovo Rescue and Recovery

Si l'authentification au démarrage est désactivée sur votre 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.

15 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 qui connaissent le même problème.
- Visitez la base de connaissances du support technique 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.com, y compris le(s) numéro(s) de version du ou des logiciels Sophos, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif ainsi que le texte de tout message d'erreur.

16 Copyright

Copyright © 1996 - 2010 Sophos Group et Utimaco Safeware AG. 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. Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Tous les produits SafeGuard sont sous le copyright d'Utimaco Safeware AG - a member of the Sophos Group, ou, le cas échéant, des concédants de la licence. Tous les autres produits Sophos sont sous copyright de Sophos Plc, ou, le cas échéant, des concédants de la licence.

Vous trouverez des informations de copyright des fournisseurs tiers dans le fichier Disclaimer and Copyright for 3rd Party Software.rtf de votre répertoire d'installation.