

SOPHOS

simple + secure

SafeGuard Enterprise

Aide utilisateur

Version du produit : 5.60
Date du document : avril 2011



Table des matières

1 SafeGuard Enterprise sur les ordinateurs d'extrémité.....	3
2 Authentification au démarrage.....	3
3 Authentification au démarrage sous Windows Vista et Windows 7.....	18
4 Connexion sous Windows Vista et Windows Vista 7.....	21
5 Connexion avec le lecteur d'empreintes digitales de Lenovo.....	22
6 Options de récupération.....	29
7 Récupération avec Local Self Help.....	30
8 Récupération avec Challenge/Réponse.....	40
9 Icône de la barre d'état système et infobulles.....	48
10 Accès aux fonctions via les extensions de l'Explorateur.....	50
11 Chiffrement de données.....	52
12 SafeGuard Data Exchange.....	56
13 SafeGuard Configuration Protection.....	68
14 SafeGuard Enterprise et BitLocker Drive Encryption.....	69
15 SafeGuard Enterprise et disques durs compatibles Opal à chiffrement automatique.....	71
16 SafeGuard Enterprise et Lenovo Rescue and Recovery.....	72
17 Support technique.....	77
18 Mentions légales.....	77

1 SafeGuard Enterprise sur les ordinateurs d'extrémité

SafeGuard Enterprise est une solution de sécurité modulaire qui renforce la sécurité des PC et des périphériques mobiles sur l'ensemble d'une plate-forme, en utilisant des stratégies de sécurité définies par l'administrateur. SafeGuard Enterprise est simple d'utilisation. L'administration du système s'effectue de manière centralisée depuis le SafeGuard Management Center.

Les fonctions de protection centralisées de SafeGuard Enterprise sur un ordinateur d'extrémité sont le chiffrement et la protection des données contre tout accès non autorisé à un ordinateur par l'intermédiaire de supports externes.

Modules de SafeGuard Enterprise

■ SafeGuard Enterprise Device Encryption

- Authentification au démarrage
- La connexion se fait immédiatement après la mise sous tension de l'ordinateur. Une fois l'authentification au démarrage réussie, vous êtes connecté automatiquement au système d'exploitation. Vous pouvez également désactiver l'authentification au démarrage. Dans ce cas, l'authentification est effectuée par le système d'exploitation.
- Chiffrement basé sur volume
- Prise en charge de BitLocker

■ SafeGuard Data Exchange

- SafeGuard Data Exchange facilite l'échange de données avec les supports amovibles sur toutes les plates-formes sans nécessiter un nouveau chiffrement.
- Chiffrement basé sur fichier
- Tous les supports inscriptibles mobiles, disques durs externes et clés USB inclus, sont chiffrés de manière transparente.

■ SafeGuard Configuration Protection

Grâce à SafeGuard Configuration Protection, le responsable de la sécurité peut autoriser uniquement certaines interfaces ou certains périphériques sur des ordinateurs sélectionnés. Ce module empêche l'introduction de programmes malveillants, ainsi que les exportations de données via des canaux non désirés tels que les réseaux locaux sans fil (WLAN). Il peut également détecter et bloquer les matériels nuisibles tels que les enregistreurs de frappe.

Remarque : il se peut que certaines des fonctions décrites dans ce manuel ne soient pas disponibles sur votre ordinateur. Ceci est dû au fait que la disponibilité des fonctions dépend des stratégies définies par le responsable de la sécurité.

2 Authentification au démarrage

L'authentification au démarrage (POA, Power-on Authentication) vous demande de vous identifier avant le démarrage du système d'exploitation de l'ordinateur. Une fois identifié, Windows démarre et vous êtes connecté automatiquement. La procédure est identique lorsque l'ordinateur revient du mode hibernation.



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 procède aux réglages appropriés via les paramètres de stratégie dans le SafeGuard Management Center.

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 par 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 SafeGuard Enterprise sur l'ordinateur d'extrémité. Après l'installation, vous pouvez changer le texte de la boîte de dialogue de la POA en modifiant la langue par défaut dans les Options régionales et linguistiques Windows. La langue du texte de la boîte de dialogue peut être spécifiée par le responsable de la sécurité dans une stratégie.

2.1 Première connexion après l'installation de SafeGuard Enterprise

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

Lors de votre première connexion suite à l'installation, vous devez d'abord vous connecter à Windows avec succès. Vous êtes alors enregistré en tant qu'utilisateur SafeGuard Enterprise. 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 fois l'enregistrement effectué et toutes les données requises reçues, une info-bulle de confirmation s'affiche sur votre ordinateur.

Lorsque vous redémarrez l'ordinateur, l'authentification au démarrage est activée. Saisissez alors vos informations d'identification Windows à partir de l'authentification au démarrage.

Vous êtes ainsi connecté automatiquement à Windows sans avoir à saisir de mot de passe (si la connexion automatique à Windows est activée).

Vous pouvez vous connecter à l'authentification au démarrage en utilisant :

- un nom d'utilisateur et un mot de passe ;
- une clé cryptographique/carte à puce et un code PIN.

Lisez les notes de publication pour consulter la liste à jour des périphériques pris en charge.

Remarque : les paramètres des ordinateurs d'extrémité sur lesquels SafeGuard Enterprise est installé sont définis par le responsable de la sécurité dans le SafeGuard Management Center, et distribués aux utilisateurs dans des fichiers de stratégie.

Procédure de première connexion

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.** Ensuite, le processus de connexion continue automatiquement.

2.1.1 Connexion automatique de SafeGuard

L'ordinateur d'extrémité démarre et la boîte de dialogue de **Connexion automatique SafeGuard** apparaît.

Que se passe-t-il ?

1. Un utilisateur est connecté automatiquement.
2. Si une connexion à un serveur SafeGuard Enterprise existe, l'ordinateur est automatiquement enregistré sur le serveur SafeGuard Enterprise.
3. La clé machine est envoyée au serveur SafeGuard Enterprise et stockée dans la base de données SafeGuard Enterprise.
4. Les stratégies de la machine sont envoyées à l'ordinateur.

2.1.2 Connexion Windows

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

Saisissez vos codes d'accès utilisateur Windows, comme à l'accoutumée.

Remarque : si vous utilisez une **carte à puce** ou une **clé cryptographique**, saisissez le code PIN.

Que se passe-t-il ?

1. L'ID utilisateur et un hachage de vos codes d'accès sont envoyés au serveur.

2. Les stratégies, certificats et clés utilisateur sont créés et envoyés à l'ordinateur d'extrémité.

Les données utilisateur ne sont disponibles à partir de l'authentification au démarrage qu'après que les données utilisateur indiquées ci-dessus ont été synchronisées entre le serveur SafeGuard Enterprise et l'ordinateur final.

Remarque : une fois l'enregistrement effectué et toutes les données requises reçues, une infobulle confirmant ce processus s'affiche sur votre ordinateur.

Au prochain démarrage de votre ordinateur, vous n'aurez qu'à saisir vos codes d'accès Windows (nom utilisateur et mot de passe) à l'authentification au démarrage. Vous êtes connecté automatiquement à Windows.

Redémarrez l'ordinateur pour activer toutes les fonctionnalités de l'authentification au démarrage. Après redémarrage, l'authentification au démarrage protège votre ordinateur contre tout accès non autorisé.

2.1.3 Connexion d'authentification au démarrage après redémarrage

Lorsque vous redémarrez l'ordinateur, la boîte de dialogue de connexion d'authentification au démarrage s'affiche.

Saisissez votre nom d'utilisateur et votre mot de passe.

Que se passe-t-il ?

1. Vos informations d'identification font l'objet d'une évaluation. Les certificats et clés sont alors disponibles et vous êtes connecté automatiquement à Windows.

Remarque : l'authentification automatique à la connexion à Windows peut être désactivée par une stratégie. Dans ce cas, la boîte de dialogue de connexion Windows s'affiche et vous devez saisir vos informations d'identification.

2.2 Connexion à partir de l'authentification au démarrage

Après activation de l'authentification au démarrage, vous vous connectez en saisissant vos codes d'accès 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 cliquant sur le bouton **Options>>** de la boîte de dialogue de connexion et en désactivant l'option **Connexion automatique à Windows**. La désactivation de la connexion automatique est nécessaire, par exemple, pour permettre à d'autres utilisateurs d'utiliser l'authentification au démarrage sur cet ordinateur ([voir Importation d'autres utilisateurs](#) à la page 7).

Assurez-vous de saisir des caractères sensibles aux majuscules lors de la connexion à la POA.

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 journalisés.

Verrouillage de la machine

Selon les paramètres de stratégie, votre ordinateur peut se verrouiller après un certain nombre d'échecs de tentatives de connexion. Pour déverrouiller votre ordinateur, lancez une procédure Challenge/Réponse, voir [Récupération avec Challenge/Réponse](#) à la page 40.

2.2.1 Récupération de connexion

Pour la récupération (par exemple, si vous avez oublié votre mot de passe), SafeGuard Enterprise propose différentes options adaptées aux différents scénarios : les méthodes de récupération disponibles sur votre ordinateur dépendent des paramètres définis par le responsable de la sécurité. Pour plus d'informations, voir [Options de récupération](#) à la page 29.

2.3 Importation d'autres utilisateurs

Pour autoriser un autre utilisateur Windows à se connecter à votre ordinateur :

1. Mettez l'ordinateur sous tension.

La boîte de dialogue d'authentification au démarrage s'affiche. Le second utilisateur Windows 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 le second utilisateur puisse se connecter à l'authentification au démarrage, le propriétaire du client doit l'autoriser.

Remarque : avec le paramètre par défaut, seul le premier utilisateur à se connecter après l'installation est enregistré comme le propriétaire de l'ordinateur. Le responsable de la sécurité peut également utiliser un paramètre de stratégie pour définir le propriétaire d'un ordinateur.

3. Dans la boîte de dialogue d'authentification au démarrage, cliquez sur **Options** et désélectionnez la case à cocher **Connexion automatique vers Windows**.

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

4. Le second utilisateur saisit ses codes d'accès Windows.
5. Si le certificat et la clé du second utilisateur se trouvent sur le client (dans l'infobulle correspondante), une entrée est créée pour le second utilisateur dans le noyau du système SafeGuard Enterprise.

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

Remarque : si des utilisateurs sont déjà connectés à partir de l'authentification au démarrage sur une autre machine de l'environnement, le responsable de la sécurité peut les affecter à l'authentification au démarrage sur une nouvelle machine depuis le Safeguard Management

Center. Les utilisateurs affectés de cette manière peuvent également se connecter à ces ordinateurs à partir de l'authentification au démarrage.

2.4 Mot de passe temporaire dans l'authentification au démarrage

SafeGuard Enterprise 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 soupçonnez quelqu'un de vous avoir vu saisir votre mot de passe.

Exemple : vous démarrez votre ordinateur portable dans un lieu public, par exemple un aéroport. Vous pensez que quelqu'un vous a vu saisir 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 êtes de nouveau connecté à Active Directory, le système vous invite automatiquement à changer le mot de passe temporaire.

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

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

3. Dans la boîte de dialogue, saisissez 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**.

Remarque : 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. Saisissez 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 vous permettra par la suite de vous authentifier automatiquement lors de l'authentification au démarrage et de vous connecter à 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 synchroniser de nouveau les mots de passe.

Lors de la connexion à Windows, SafeGuard Enterprise 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.

2.5 Connexion à partir de l'authentification au démarrage à l'aide de cartes à puce ou de clés cryptographiques

Il existe deux types de connexion avec des cartes à puce ou des clés cryptographiques :

- Connexion *autorisée uniquement avec des cartes à puce ou des clés cryptographiques.*
- Connexion *autorisée via un nom d'utilisateur et un mot de passe ou via une carte à puce ou une clé cryptographique.*

Le responsable de la sécurité définit le type de connexion autorisé dans une stratégie.

Le responsable de la sécurité crée votre carte à puce/clé cryptographique et vous la fournit. Vous pouvez également mettre vous-même vos propres codes d'accès Windows sur votre carte à puce/clé cryptographique.

Remarque : les cartes à puce et les clés cryptographiques sont traitées de la même manière dans SafeGuard Enterprise. Les termes « clé cryptographique » et « carte à puce » recouvrent la même notion dans le produit et le manuel. Le terme « clé cryptographique » est privilégié dans les sections suivantes.

2.5.1 Première connexion de clé cryptographique après l'installation

La première connexion avec une clé cryptographique est identique à la procédure de connexion sans clé cryptographique.

Si vous disposez d'une clé cryptographique, vous pouvez l'utiliser pour vous connecter à Windows en entrant son code PIN.

Remarque : nous vous recommandons de configurer votre clé cryptographique avec les codes d'accès Windows ([voir Stockage d'informations utilisateur Windows sur la clé cryptographique](#) à la page 11) avant de redémarrer l'ordinateur. Les stratégies de sécurité qui s'appliquent peuvent nécessiter l'utilisation d'une clé cryptographique à l'authentification au démarrage. Si votre clé cryptographique ne contient pas vos codes d'accès, vous ne pouvez pas vous connecter à partir de l'authentification au démarrage.

2.5.2 Connexion à l'authentification au démarrage avec une clé cryptographique

Conditions préalables : assurez-vous que le support USB est activé dans le BIOS. Le support de clé cryptographique doit être initialisé et la clé cryptographique doit être générée.

1. Connectez la clé cryptographique.
2. Mettez l'ordinateur sous tension.

La boîte de dialogue de connexion avec une clé cryptographique s'affiche.

Remarque : si votre stratégie autorise la connexion avec vos informations d'identification et que vous déconnectez la clé cryptographique, vous serez invité à saisir vos informations d'identification pour la connexion. Si la boîte de dialogue de connexion avec un ID utilisateur et un mot de passe ne s'affiche pas, vous ne pouvez vous connecter qu'avec une clé cryptographique à partir de l'authentification au démarrage.

3. Saisissez le code PIN de votre clé cryptographique.

Vous êtes connecté à partir de l'authentification au démarrage et à Windows (si l'option **Authentification automatique à Windows** est activée dans la boîte de dialogue de connexion).

2.5.3 Changement du code PIN

Vous pouvez changer le code PIN de votre clé cryptographique dans la boîte de dialogue du journal Windows.

En général, si l'option **Authentification automatique à Windows** est activée à l'authentification au démarrage, la boîte de dialogue de connexion Windows ne s'affiche pas. Pour afficher la boîte de dialogue de connexion Windows, vous devez désactiver cette option lors de la connexion à partir de l'authentification au démarrage.

Remarque : vous êtes automatiquement invité à changer le code PIN si le responsable de la sécurité a défini des règles nécessitant un changement de code PIN (à intervalles donnés par exemple).

1. Dans la boîte de dialogue **Code PIN** utilisée pour la connexion à Windows, sélectionnez **Changer le code PIN**.
2. Saisissez le code PIN de votre clé cryptographique et cliquez sur **OK**.

La boîte de dialogue **Changement de code PIN** s'affiche.

3. Saisissez le nouveau code PIN et confirmez-le.
4. Cliquez sur **OK**.

Le code PIN de la clé cryptographique est changé et la connexion Windows se poursuit.

2.5.4 Stockage des codes d'accès utilisateur Windows sur la clé cryptographique

Si votre clé cryptographique ne contient pas vos codes d'accès utilisateur Windows, vous pouvez les stocker sur la clé cryptographique.

Remarque : nous vous recommandons de configurer votre clé cryptographique lors de la première connexion. Les stratégies de sécurité qui s'appliquent peuvent nécessiter l'utilisation d'une clé cryptographique à l'authentification au démarrage. Si votre clé cryptographique ne contient aucune information utilisateur, vous ne pouvez pas vous connecter à partir de l'authentification au démarrage.

1. Lors de la première connexion après l'installation, connectez votre clé cryptographique au système lorsque la boîte de dialogue de connexion Windows s'affiche.

Si le système détecte une clé cryptographique vide, il affiche automatiquement la boîte de dialogue **Générer des clés cryptographiques**.

2. Saisissez votre nom d'utilisateur et votre mot de passe Windows.
3. Confirmez le mot de passe.
4. Sélectionnez ou entrez le domaine et cliquez sur **OK**.

Le système tente de vous connecter à Windows avec les données entrées. Si la connexion est réussie, les données sont inscrites sur la clé cryptographique.

Vous êtes connecté à Windows.

Si la connexion à l'aide d'une clé cryptographique est définie en option pour votre utilisateur (c'est-à-dire que vous vous êtes déjà connecté à partir de l'authentification au démarrage avec votre nom d'utilisateur et votre mot de passe), vous pouvez également générer la clé cryptographique ultérieurement.

Dans la boîte de dialogue d'authentification au démarrage, cliquez sur **Options** et désélectionnez la case à cocher **Authentification automatique à Windows**. La boîte de dialogue de connexion Windows s'affiche et vous pouvez stocker vos codes d'accès sur la clé cryptographique comme décrit ci-dessus.

2.5.5 Récupération de la connexion de clé cryptographique

Si vous utilisez une clé non cryptographique et que vous avez oublié votre mot de passe, vous pouvez accéder à votre ordinateur grâce à l'une des méthodes suivantes :

- Récupération via Local Self Help, [voir Récupération via Local Self Help](#) à la page 30.
- Récupération par Challenge/Réponse, [voir Récupération par Challenge/Réponse](#) à la page 40.

Les méthodes de récupération disponibles sur votre ordinateur dépendent des paramètres définis par le responsable de la sécurité.

Pour commencer la récupération, cliquez sur le bouton **Récupération** dans la boîte de dialogue de connexion de clé cryptographique.

Remarque :

Pour les clés cryptographiques, ces méthodes de récupération ne sont pas disponibles. Si des problèmes de connexion surviennent, contactez votre responsable de la sécurité.

2.5.6 Déblocage des clés cryptographiques

Si vous saisissez un code PIN incorrect plusieurs fois, votre clé cryptographique se verrouille. Dans ce cas, le responsable de la sécurité peut configurer SafeGuard Enterprise pour afficher la boîte de dialogue **Déblocage de la clé cryptographique**

Le responsable de la sécurité doit vous fournir le code PIN d'administrateur défini pour votre clé cryptographique.

1. Dans la boîte de dialogue **Déblocage de la clé cryptographique**, saisissez le mot de passe existant.
2. Saisissez un nouveau code PIN et confirmez-le.

Le code PIN entré est soumis aux règles définies pour les codes PIN (par exemple, des combinaisons spécifiques de caractères peuvent être requises, des codes PIN déjà utilisés ne peuvent pas être réutilisés, etc.).

3. Cliquez sur **OK**.

La clé cryptographique est débloquée et la connexion se poursuit.

Remarque :

Si cette fonction n'est pas disponible sur votre ordinateur, vous pouvez de nouveau accéder à votre ordinateur avec la procédure Challenge/Réponse. Grâce au Challenge/Réponse, vous pouvez récupérer l'accès à votre ordinateur, en revanche, vous ne pouvez pas changer le code PIN ou les codes d'accès utilisateur.

2.5.7 Connexion Bureau à distance

Sous Windows XP il n'est pas possible d'établir une connexion Bureau à distance à un ordinateur, si l'utilisateur s'est connecté localement en utilisant une clé cryptographique.

La capture à distance n'est pas possible dans ce cas.

2.5.8 Clés cryptographiques - Kerberos

Si vous utilisez une clé cryptographique, vous êtes identifié à l'authentification au démarrage par le certificat stocké sur la clé cryptographique.

Pour ce type de connexion, une clé cryptographique générée dans son intégralité est requise. Le responsable de la sécurité ou toute autre personne autorisée doit vous fournir cette clé cryptographique. Pour vous connecter au système, il vous suffit de saisir le code PIN de la clé cryptographique. Si ce type de connexion est le seul type valide pour votre ordinateur, vous ne pouvez pas vous connecter sans clé cryptographique.

Remarque : lors de l'utilisation d'une clé cryptographique de ce type, ni la procédure Challenge/Réponse ni Local Self Help ne seront disponibles en cas de problèmes de connexion. Si des problèmes de connexion surviennent, contactez votre responsable de la sécurité.

2.5.8.1 Changement du certificat pour les connexions avec clé cryptographique

Pour changer ou renouveler le certificat utilisé pour les connexions avec clé cryptographique, votre responsable de la sécurité doit attribuer un nouveau certificat à votre ordinateur. Après synchronisation entre l'ordinateur et le serveur SafeGuard Enterprise, la boîte de dialogue de statut (qui peut être affichée avec l'icône SafeGuard Enterprise de la barre d'état système) indique que l'ordinateur d'extrémité est **Prêt pour la modification du certificat**.

Le responsable de la sécurité vous fournit une nouvelle clé cryptographique.

Pour modifier le certificat de votre ordinateur :

1. Connectez-vous à partir de l'authentification au démarrage avec votre ancienne clé cryptographique sans la connexion automatique à Windows.
Cliquez sur **Options** et désélectionnez la case à cocher **Connexion automatique à Windows** ou déconnectez-vous après la connexion automatique à Windows.
2. Connectez-vous à Windows avec votre nouvelle clé cryptographique.

La nouvelle clé cryptographique est valide pour la connexion POA. L'ancienne clé cryptographique n'est plus valide pour la connexion.

2.6 Connexion automatique POA avec une carte à puce ou une clé cryptographique

Conditions préalables :

- Assurez-vous que le support USB est activé dans le BIOS.
- Le support de clé cryptographique doit être initialisé et la clé cryptographique doit être générée.
- Le responsable de la sécurité a affecté la stratégie appropriée à votre ordinateur.

Si une stratégie avec un code PIN défini a été attribuée à votre ordinateur, vous pouvez vous connecter automatiquement à l'authentification au démarrage à l'aide d'une clé cryptographique. Vous n'avez pas besoin de saisir vos codes d'accès ou votre code PIN car vous êtes identifié automatiquement au moment de l'authentification au démarrage. Selon les paramètres de votre stratégie, vous êtes également identifié automatiquement au moment de la connexion à Windows.

Pour vous connecter automatiquement à partir de l'authentification au démarrage avec une clé cryptographique :

1. Connectez la clé cryptographique.
2. Mettez l'ordinateur sous tension.

Vous êtes connecté automatiquement à partir de l'authentification au démarrage. Selon les paramètres de votre stratégie, vous êtes également identifié automatiquement au moment de la connexion à Windows.

- Si la connexion automatique réussie, Windows démarre.
- Si la connexion automatique échoue, vous êtes invité à saisir le code PIN de votre clé cryptographique. Vous êtes ensuite connecté à partir de l'authentification au démarrage.

2.7 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 via une stratégie.

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 celles utilisées pour la disposition du clavier de l'authentification au démarrage ([voir Modification de la disposition du clavier](#) à la page 14).

2.8 Disposition du clavier

Chaque pays ou presque a une disposition de clavier qui lui est propre. La disposition du clavier 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, SafeGuard Enterprise adopte la disposition de clavier qui est définie dans les Options régionales et linguistiques de Windows pour l'utilisateur par défaut au moment de l'installation de SafeGuard Enterprise.

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, vous avez également la possibilité d'utiliser la disposition du clavier américain (anglais).

2.8.1 Modification de la disposition du clavier

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

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**, sélectionnez **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 d'extrémité deux fois. Si la disposition du clavier précédente est désélectionnée dans les **Options régionales et linguistiques**, elle est maintenue jusqu'à ce que vous en sélectionniez une nouvelle.

Remarque :

Modifiez 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 la nouvelle disposition du clavier puisse être lue par l'authentification au démarrage et que l'authentification au démarrage puisse définir la nouvelle disposition.

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

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

2.9 Raccourcis clavier/touches de fonction pris en charge dans l'authentification au démarrage (POA)

Certains paramètres et fonctionnalités matérielles peuvent générer des problèmes lors du démarrage des ordinateurs 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 de l'authentification au démarrage avant de procéder au déploiement de SafeGuard Enterprise. Ce fichier bénéficie d'une mise à jour mensuelle et peut être téléchargé depuis l'emplacement suivant : <ftp://POACFG:POACFG@ftp.ou.utimaco.de>

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

Remarque :

Lorsqu'un fichier personnalisé est défini, il remplace le fichier intégré au fichier .msi. Le fichier par défaut est utilisé uniquement lorsqu'aucun fichier de configuration de l'authentification au démarrage 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 plus d'informations, consultez :

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

L'authentification au démarrage prend en charge un certain nombre de touches de fonction.

2.9.1 Raccourcis clavier

Maj - F3 = support patrimonial 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	Patrimonial	USB 1.x	USB 2.0	Commentaire
désactivé	désactivé	désactivé	activé	activé	activé	3.
activé	désactivé	désactivé	désactivé	activé	activé	Par défaut
désactivé	activé	désactivé	activé	désactivé	désactivé	1., 2.
activé	activé	désactivé	activé	désactivé	désactivé	1., 2.
désactivé	désactivé	activé	activé	activé	désactivé	3.
activé	désactivé	activé	désactivé	activé	désactivé	
désactivé	activé	activé	activé	désactivé	désactivé	
activé	activé	activé	activé	désactivé	désactivé	2.

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

Remarque : si vous appuyez sur **Maj - F5** pendant le démarrage, vous réduirez considérablement la durée du lancement de l'authentification au démarrage. 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**.

L'authentification au démarrage peut utiliser le clavier USB via BIOS SMM. Il n'y a pas de support de clé cryptographique USB.

- Si aucun support USB n'est actif, l'authentification au démarrage tente d'utiliser BIOS SMM au lieu de sauvegarder et de restaurer le contrôleur USB. Le mode patrimonial peut fonctionner dans ce scénario.
- Le support patrimonial 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 SafeGuard Enterprise 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 sont 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 démarrer la POA. Si des raccourcis clavier ont été modifiés au cours du démarrage, l'état des touches correspondantes s'affiche en bleu. La couleur bleue signifie que la touche a été utilisée dans cet état pour démarrer l'authentification au démarrage mais qu'elle n'a pas encore été enregistrée. Les valeurs inchangées sont affichées en noir. Pour fermer la boîte de dialogue, appuyez de nouveau sur **F5** ou appuyez sur **Entrée**.

2.9.2 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 démarrer 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 l'ordinateur 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** pour ouvrir la boîte de dialogue POA de connexion avec un nom d'utilisateur et un mot de passe. Pour plus d'informations, reportez-vous à la section [Connexion avec le lecteur d'empreintes digitales Lenovo](#) à la page 22.

2.10 Synchronisation du mot de passe

SafeGuard Enterprise détecte automatiquement à quel moment le mot de passe Windows a été modifié et ne correspond plus à celui qui est stocké dans la base de données SafeGuard Enterprise. Ceci peut se produire si le mot de passe Windows a été changé à l'aide d'un VPN, sur un autre ordinateur, ou dans Active Directory.

Si SafeGuard Enterprise détecte cette situation, vous êtes invité à saisir l'ancien mot de passe. Par la suite, le mot de passe stocké par SafeGuard Enterprise 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.

3 Authentification au démarrage sous Windows Vista et Windows 7

L'authentification au démarrage pour Windows Vista et pour Windows 7 est identique à celle de Windows XP en termes d'aspect et de comportement. Les seules différences résident dans la procédure de connexion au système d'exploitation.

Remarque : cette section décrit uniquement les différences relatives à Windows Vista et à Windows 7. Si ces différences ne sont pas expressément définies, ce sont les procédures/processus décrits dans la section relative à l'authentification au démarrage qui s'appliquent ([voir Authentification au démarrage](#) à la page 3).

3.1 Première connexion après l'installation de SafeGuard Enterprise sous Windows Vista et Windows 7

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

Remarque : sous Windows Vista et Windows 7, appuyez sur les 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** (pour la connexion interactive, **Ctrl + Alt + Suppr** n'est pas nécessaire).

SafeGuard Enterprise utilise une connexion basée sur certificat. Vous avez donc besoin de clés et de certificats pour vous connecter à partir de l'authentification au démarrage. Les clés et certificats spécifiques à un utilisateur ne sont cependant créés qu'après une connexion Windows.

Lors de la première connexion après l'installation, connectez-vous d'abord à Windows selon la méthode classique à l'aide de vos informations d'identification. Vous êtes ensuite enregistré en tant qu'utilisateur SafeGuard Enterprise. 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 fois l'enregistrement effectué et toutes les données requises reçues, une info-bulle de confirmation s'affiche sur votre ordinateur.

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

Vous pouvez vous connecter à partir de l'authentification au démarrage en utilisant vos nom d'utilisateur et mot de passe.

Remarque : les paramètres des ordinateurs sur lesquels SafeGuard Enterprise est installé sont définis de manière centralisée par le responsable de la sécurité dans SafeGuard Management Center et distribués aux ordinateurs d'extrémité dans les fichiers de stratégie.

Procédure de première connexion

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

3.1.1 Connexion automatique de SafeGuard

1. L'ordinateur d'extrémité démarre et la boîte de dialogue de Connexion automatique SafeGuard apparaît.
 - Un utilisateur est connecté automatiquement.
 - Si une connexion à un serveur SafeGuard Enterprise existe, l'ordinateur est automatiquement enregistré sur le serveur SafeGuard Enterprise.
 - La clé machine est envoyée au serveur SafeGuard Enterprise et stockée dans la base de données SafeGuard Enterprise.
 - Les stratégies de la machine sont envoyées à l'ordinateur.

3.1.2 Connexion à Windows Vista/Windows 7

1. La boîte de dialogue de connexion de Windows Vista/Windows 7 s'affiche.
2. Sous Windows Vista et Windows 7, SafeGuard Enterprise offre la méthode d'authentification de SafeGuard Enterprise et de Windows Vista/Windows 7. Windows Vista/Windows 7 propose deux icônes pour les deux méthodes :
 - Cliquez sur **Autre utilisateur** pour ouvrir une boîte de dialogue de saisie des codes d'accès.
 - 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 ayant ouvert une session sur le système. Saisissez uniquement votre mot de passe.

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

3. Saisissez vos codes d'accès utilisateur Windows, comme à l'accoutumée.
 - Un ID utilisateur et un hachage de vos codes d'accès sont envoyés au serveur.
 - Les stratégies, certificats et clés utilisateur sont créés et envoyés à l'ordinateur d'extrémité.

Les données utilisateur ne sont disponibles dans l'authentification au démarrage qu'une fois toutes les données synchronisées entre le serveur SafeGuard Enterprise et votre ordinateur.

Cela signifie qu'au **prochain démarrage du système**, il vous suffira de saisir vos codes d'accès utilisateur Windows (nom d'utilisateur et mot de passe) dans l'authentification au démarrage pour être connecté automatiquement.

Redémarrez l'ordinateur pour activer toutes les fonctionnalités de l'authentification au démarrage. Après redémarrage, l'authentification au démarrage protège votre ordinateur contre tout accès non autorisé.

3.1.3 Connexion d'authentification au démarrage après redémarrage

1. Lorsque vous redémarrez l'ordinateur, la boîte de dialogue de connexion d'authentification au démarrage s'affiche.

Des certificats et des clés sont disponibles et vous pouvez vous connecter à partir de l'authentification au démarrage avec vos codes d'accès utilisateur Windows.

2. Saisissez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **OK**.

Vos codes d'accès utilisateur font l'objet d'une évaluation. Vous êtes automatiquement connecté à Windows une fois que le système a vérifié vos informations d'identification.

Remarque : la connexion automatique vers Windows peut être désactivée par un paramètre de stratégie. Dans ce cas, la boîte de dialogue de connexion Windows s'affiche et vous devez saisir vos codes d'accès utilisateur.

3.2 Connexion à partir de l'authentification au démarrage sous Windows Vista et Windows 7

Après activation de l'authentification au démarrage (synchronisation initiale et redémarrage), vous vous connectez en saisissant vos codes d'accès 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 ([voir Importation d'autres utilisateurs](#) à la page 7). 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.

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.

Verrouillage de la machine

Selon les paramètres de stratégie, votre ordinateur peut se verrouiller après un certain nombre d'échecs de tentatives de connexion. Pour déverrouiller votre ordinateur, lancez une procédure Challenge/Réponse, [voir Récupération avec Challenge/Réponse](#) à la page 40.

4 Connexion sous Windows Vista et Windows 7

Sous Windows Vista et Windows 7, SafeGuard Enterprise propose une méthode d'authentification supplémentaire.

Si vous désactivez l'option **Authentification automatique à Windows** dans la boîte de dialogue de connexion de l'authentification au démarrage, la boîte de dialogue de connexion Windows Vista/Windows 7 s'affiche. Dans cette boîte de dialogue, vous pouvez également choisir une autre méthode d'authentification.

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

4.1 Connexion avec SafeGuard Enterprise

Vous êtes généralement connecté automatiquement à Windows après avoir saisi votre mot de passe à partir de l'authentification au démarrage (POA). Si vous désactivez l'option **Authentification automatique à Windows** dans la boîte de dialogue de connexion de l'authentification au démarrage et que vous utilisez la méthode SafeGuard Enterprise pour vous connecter à Windows, toutes les fonctionnalités de SafeGuard Enterprise sont disponibles après la connexion à Windows Vista ou à Windows 7.

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

4.2 Connexion avec la méthode d'authentification de Windows Vista/Windows 7

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

Si vous utilisez la méthode d'authentification de Windows Vista/Windows 7, la connexion à SafeGuard Enterprise est effectuée après la connexion au système d'exploitation.

Après la connexion à Windows Vista/Windows 7, l'application d'authentification de SafeGuard Enterprise démarre automatiquement, si nécessaire, pour obtenir toutes les fonctionnalités de SafeGuard Enterprise.

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. Saisissez vos codes d'accès ou le code PIN et cliquez sur **OK**.

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

4.3 Synchronisation des mots de passe sous Windows Vista et Windows 7

SafeGuard Enterprise 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 a été changé à l'aide d'un VPN, sur un autre ordinateur, ou dans Active Directory.

Si SafeGuard Enterprise détecte cette situation, vous êtes informé et invité à saisir l'ancien mot de passe. Par la suite, le mot de passe stocké par SafeGuard Enterprise 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.

5 Connexion avec le lecteur d'empreintes digitales de Lenovo

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 ou une clé cryptographique.

Vous ne perdez, ni n'oubliez vos codes d'accès, et aucune personne non autorisée ne peut deviner cette information. L'utilisation de lecteurs d'empreintes digitales simplifie donc la procédure de connexion et renforce la sécurité.

SafeGuard Enterprise 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. Vous pouvez également utiliser un clavier USB externe pour la connexion par empreinte digitale.

Remarque :

- Vous ne pouvez connecter qu'un seul lecteur d'empreintes digitales à la fois à un ordinateur.
- Vous ne pouvez pas utiliser conjointement les procédures de connexion par clé cryptographique et par empreinte digitale sur le même ordinateur.
- La connexion à distance par empreinte digitale n'est pas prise en charge.

5.1 Configuration requise

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

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 BIOS le plus récent est recommandé
- SafeGuard Enterprise
- La version logicielle recommandée par le fournisseur doit être installée avant SafeGuard Enterprise :
 - ThinkVantage Fingerprint pour AuthenTec
 - ou
 - ThinkVantage Fingerprint pour UPEK.
- Le responsable de la sécurité doit avoir activé la connexion par empreinte digitale par la stratégie.

Configuration requise

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

Matériel pris en charge

Pour plus d'informations sur les matériels de connexion par empreinte digitale pris en charge, consultez l'article <http://www.sophos.fr/support/knowledgebase/article/108789.html>.

Logiciels pris en charge

Pour plus d'informations sur les logiciels de lecture par empreinte digitale pris en charge, consultez l'article <http://www.sophos.fr/support/knowledgebase/article/111626.html>.

5.2 Enregistrement des empreintes digitales

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

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

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**. (TPM 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. Redémarrez votre ordinateur.
4. Pour tester l'empreinte digitale que vous avez enregistrée, passez votre doigt sur le lecteur d'empreintes digitales après avoir redémarré l'ordinateur.

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

5.3 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. Redémarrez votre ordinateur.

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 vos codes d'accès 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 25).

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

Remarque :





- 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 authentification automatique à 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 l'authentification automatique à 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 27).

5.3.1 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.

	<p>Vous invite à faire glisser votre doigt sur le lecteur d'empreintes digitales.</p>
	<p>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.</p>
	<p>Indique que le lecteur d'empreintes digitales fonctionne et qu'il est occupé.</p>
	<p>Indique que le lecteur d'empreintes digitales a lu l'empreinte avec succès et trouvé une correspondance.</p>

	<p>Indique que le lecteur d'empreintes digitales a lu l'empreinte avec succès mais sans trouver de correspondance.</p>
	<p>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.</p>
	<p>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.</p>
	<p>Indique que votre glissement de doigt était trop oblique. Faites glisser une nouvelle fois votre doigt sur le lecteur d'empreintes digitales.</p>
	<p>Indique que vous avez bougé le doigt trop rapidement. Faites glisser une nouvelle fois votre doigt sur le lecteur d'empreintes digitales.</p>
	<p>Indique que votre glissement de doigt était trop court. Faites glisser une nouvelle fois votre doigt sur le lecteur d'empreintes digitales.</p>

5.3.2 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.

5.3.3 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.

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, **Ctrl+Alt+Suppr** correspond 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. Lorsque ceci se produit, votre ordinateur est verrouillé et vous devez vous connecter en utilisant une procédure Challenge/Réponse.

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.

5.4 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 en appuyant sur les 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.

5.4.1 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. Redémarrez votre ordinateur.
2. 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. Le système vous fait passer vers la boîte de dialogue de connexion par nom d'utilisateur et mot de passe.
3. Cliquez sur le bouton **Options** et désactivez l'option **Authentification automatique à Windows**.

Remarque : 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 digitale, mais Windows rejette 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.

Un message indiquant la modification du mot de passe s'affiche et le système vous invite à saisir votre mot de passe Windows actuel.

7. Saisissez correctement le mot de passe Windows.

Remarque :

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 réussi 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.

5.5 Récupération de la connexion par empreinte digitale

Si la connexion par empreinte digitale ne fonctionne pas et que vous avez oublié votre mot de passe, SafeGuard Enterprise vous offre les méthodes de récupération suivantes :

- Récupération via Local Self Help, voir [Récupération via Local Self Help](#) à la page 30.
- Récupération par Challenge/Réponse, voir [Récupération par Challenge/Réponse](#) à la page 40.

Les méthodes de récupération disponibles sur votre ordinateur dépendent des paramètres définis par le responsable de la sécurité.

Pour commencer la récupération, cliquez sur le bouton **Récupération** dans la boîte de dialogue de connexion par empreinte digitale.

Remarque :

En raison de la procédure de récupération, le système risque de vous proposer de modifier le mot de passe lors du démarrage 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 codes d'accès associés à l'empreinte digitale.

6 Options de récupération

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

■ Récupération de connexion avec 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 plus d'informations, reportez-vous à la section [Récupération avec Local Self Help](#) à la page 30.

■ Récupération avec 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 plus d'informations, reportez-vous à la section [Récupération par Challenge/Réponse](#) à la page 40.

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

7 Récupération avec Local Self Help

Si vous avez oublié votre mot de passe et que vous ne pouvez pas contacter le support technique, SafeGuard Enterprise met à votre disposition 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 auxquelles vous devez répondre et les distribuer sur les ordinateurs d'extrémité. Vous pouvez également définir vos propres questions, si la stratégie appropriée vous y autorise. L'assistant Local Self Help vous aide à fournir les premières réponses et à modifier les questions. Vous pouvez ouvrir l'assistant Local Self Help en cliquant sur l'icône de la barre d'état de SafeGuard Enterprise dans la barre des tâches Windows.

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

- Connexion avec ID utilisateur et mot de passe
- Connexion avec empreinte digitale
- Connexion avec clé non cryptographique si la connexion avec ID utilisateur et mot de passe a été activé comme moyen de connexion dans la stratégie.

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 appropriée de type Paramètres généraux, et a 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 31).

7.1 Activation de Local Self Help

Lorsque la stratégie vous autorisant à utiliser Local Self Help est en vigueur, activez la fonction en répondant aux questions prédéfinies que vous avez reçues ou en définissant vos propres questions et en y répondant.

Local Self Help est activé sur votre ordinateur lorsque vous avez répondu à un nombre prédéfini de questions et que vous les avez enregistrées. Le responsable de la sécurité définit le nombre de questions à répondre. L'assistant Local Self Help vous guide durant le processus et vous indique le nombre de questions à répondre. 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 aux questions prédéfinies reçues et enregistrez-les. L'assistant Local Self Help vous indique le nombre de questions à répondre.

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

Répondez au nombre prédéfini de questions 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 le nombre de questions requis, répondez-y et enregistrez-les.

Remarque : pour vous connecter à partir de l'authentification au démarrage avec Local Self Help, répondez à des questions sélectionnées de façon aléatoire parmi les questions définies dans l'assistant Local Self Help. Le responsable de la sécurité définit le nombre de questions à répondre dans la POA.

Condition préalable : après avoir reçu la stratégie, l'infobulle 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 zone de notification de SafeGuard Enterprise 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 vous indique comment activer 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.

- 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, saisissez 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, utilisez 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, saisissez 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, utilisez des caractères Romaji (romains), sinon les réponses ne correspondent pas lorsque vous répondez aux questions dans l'authentification au démarrage.

- 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.

- Cliquez sur **Terminer**.

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

- 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.

7.2 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.
- Cliquez avec le bouton droit de la souris sur l'icône de la zone de notification de SafeGuard Entreprise dans la barre des tâches Windows.
 - 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.

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

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

Cette boîte de dialogue vous indique comment activer 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, sélectionnez la case **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 la question concernée 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. 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 31).

7.3 Changement des paramètres des questions

Le responsable de la sécurité peut définir les paramètres suivants à appliquer aux questions Local Self Help :

- le nombre de questions à répondre dans l'assistant Local Self Help pour activer Local Self Help sur votre ordinateur. Pour que Local Self Help soit actif, le nombre de questions/réponses spécifié doit être disponible.
- le nombre de questions à répondre dans la POA pour se connecter avec Local Self Help. Les questions affichées dans la POA sont sélectionnées aléatoirement à partir des questions répondues dans l'assistant Local Self Help.

Si ces deux paramètres changent suite au déploiement sur votre ordinateur d'une nouvelle stratégie, les scénarios suivants peuvent se produire :

Condition	Action de LSH	Action utilisateur requise
Le nombre de question à répondre dans l'assistant Local Self Help change mais il existe suffisamment de questions disponibles pour garder Local Self Help actif sur votre ordinateur.	Local Self Help reste actif sur votre ordinateur.	Aucune.
Le nombre de question à répondre dans l'assistant Local Self Help change mais il n'existe pas suffisamment de questions disponibles pour garder Local Self Help actif sur votre ordinateur.	Un message s'affiche pour indiquer que les paramètres Local Self Help ont été changés. Les questions disponibles sur votre ordinateur ne sont plus valides. Local Self Help n'est plus actif sur votre ordinateur.	Pour activer Local Self Help, exécutez de nouveau l'assistant Local Self Help et suivez les instructions de l'assistant.

Condition	Action de LSH	Action utilisateur requise
Le nombre de questions à répondre dans la POA pour se connecter avec Local Self Help a changé.	Un message s'affiche pour indiquer que les paramètres Local Self Help ont été changés. Les questions disponibles sur votre ordinateur sont toujours valides. Les proportions de questions disponibles et de réponses valides ont été modifiées.	Exécutez de nouveau l'assistant Local Self Help et suivez les instructions de l'assistant.

7.4 Changements de conditions ou paramètres pour Local Self Help lors des processus d'édition

Les paramètres de Local Self Help et toutes autres conditions cruciales à l'utilisation de Local Self Help peuvent changer pendant que vous définissez ou modifiez les questions dans l'assistant Local Self Help Wizard.

Par exemple :

- Un nouveau mot de passe utilisateur peut être défini.
- Une nouvelle stratégie contenant de nouveaux paramètres Local Self Help et/ou un nouvel ensemble de questions Local Self Help peut être transféré à votre ordinateur par le biais du mécanisme de mises à jour régulières.

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 totalement désactivé par une nouvelle stratégie.	L'assistant Local Self Help affiche un message indiquant que Local Self Help a été totalement désactivé 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, le nombre de questions à répondre) par une nouvelle stratégie. Cependant, Local Self Help n'a pas été désactivé.	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

Condition	Action de l'assistant LSH	Résultat
<p>Les questions et réponses définies sont toujours valides et en quantité suffisante pour que Local Self Help reste actif sur votre ordinateur.</p>		<p>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.</p>
<ul style="list-style-type: none"> ■ Le mot de passe utilisateur a été modifié <p>et/ou</p> <ul style="list-style-type: none"> ■ Les paramètres de Local Self Help ont été modifiés (par exemple, la longueur minimale des réponses, le droit de définir vos propres questions, le nombre de questions à répondre, etc.) par une nouvelle stratégie. Local Self Help n'a pas été désactivé. <p>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.</p>	<p>L'assistant Local Self Help affiche un message indiquant que le mot de passe utilisateur ou les paramètres Local Self Help ont été modifiés. Local Self Help n'est pas actif sur votre ordinateur. Nous vous recommandons d'exécuter de nouveau l'assistant. L'assistant se ferme.</p>	<p>Pour activer Local Self Help, exécutez de nouveau l'assistant Local Self Help et redéfinissez les questions et réponses. Ensuite, vous pouvez utiliser Local Self Help pour la récupération de connexion.</p>
<p>Le certificat utilisateur a été modifié.</p>	<p>L'assistant Local Self Help affiche un message indiquant que le certificat utilisateur a été modifié. Local Self Help n'est pas actif sur votre ordinateur. Nous vous recommandons d'exécuter de nouveau l'assistant. L'assistant se ferme.</p>	<p>Pour activer Local Self Help, exécutez de nouveau l'assistant Local Self Help et redéfinissez les questions et réponses. Ensuite, vous pouvez utiliser Local Self Help pour la récupération de connexion.</p>

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

1. Dans la boîte de dialogue de connexion de l'authentification au démarrage, 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 l'une de ces deux méthodes s'affiche. Cliquez sur **Local Self Help**.

Remarque :

Si vous vous connectez habituellement à l'authentification au démarrage avec un code PIN ou une carte à puce, vous devez tout d'abord retirer le code PIN ou la carte à puce de votre ordinateur. Après cela, la boîte de dialogue de connexion POA pour se connecter par nom d'utilisateur et mot de passe s'affiche. Saisissez votre ID utilisateur et cliquez sur le bouton **Récupération**.

La boîte de dialogue de **Bienvenue Local Self Help** apparaît.

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

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

La première question s'affiche.
3. 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**.
4. 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.
5. Répondez aux 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.

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

Remarque :

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

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

Remarque :

Assurez-vous qu'aucune personne non autorisée ne peut voir 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.

7. Vous pouvez lire le mot de passe et l'utiliser pour vous reconnecter à partir de l'authentification au démarrage et à Windows.
8. Après avoir lu le mot de passe, cliquez sur **OK**. Autrement, le processus de démarrage 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.

7.6 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 avec Local Self Help, des questions sont sélectionnées une nouvelle fois de façon aléatoire.

7.7 Réactivation des questions et réponses après des changements de mots de passe sur plusieurs machines

Si vous utilisez plusieurs ordinateurs sur lesquels Local Self Help est activé et que vous modifiez votre mot de passe Windows sur l'une des machines, les questions et réponses de Local Self Help ne sont plus actives sur la seconde machine (ni sur aucune autre) après la modification du mot de passe. Les questions et réponses restent toutefois disponibles dans l'assistant Local Self Help. Pour réutiliser le même ensemble de questions sur le second ordinateur, confirmez-le dans l'assistant Local Self Help.

1. Après avoir modifié votre mot de passe sur une machine, connectez-vous à la seconde.

Une infobulle indique qu'il reste des questions Local Self Help sans réponse.

2. Cliquez avec le bouton droit de la souris sur l'icône de la zone de notification de SafeGuard Enterprise sur la barre des tâches Windows et sélectionnez **Local Self Help**.

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

3. Saisissez votre mot de passe et cliquez sur **Suivant**.
4. Dans toutes les boîtes de dialogue de l'assistant Local Self Help qui s'affichent ensuite, cliquez sur **Suivant**, puis sur **Terminer** dans la dernière.

Les questions et réponses stockées précédemment sur l'ordinateur redeviennent actives et sont utilisées lors de la connexion à partir de l'authentification au démarrage avec Local Self Help.

8 Récupération avec Challenge/Réponse

Pour la récupération, SafeGuard Enterprise propose une **procédure Challenge/Réponse** pour l'échange d'informations confidentielles.

Si vous utilisez SafeGuard Enterprise et que vous avez, par exemple, oublié votre mot de passe, vous pouvez accéder à votre ordinateur très rapidement grâce à un support centralisé.

Remarque :

Nous vous recommandons d'utiliser Local Self Help pour récupérer un mot de passe oublié. Dans Local Self Help, le mot de passe actuel peut être affiché et l'utilisateur peut continuer à l'utiliser. Ceci pour éviter de réinitialiser le mot de passe ou de recourir à l'assistance technique.

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 un code de réponse qui vous autorise à effectuer une action spécifique sur votre ordinateur.

La récupération avec Challenge/Réponse est disponible pour les méthodes de connexion suivantes dans l'authentification au démarrage :

- Connexion avec ID utilisateur et mot de passe
- Connexion avec empreinte digitale
- Connexion avec une clé non cryptographique.

8.1 Scénarios type pour lesquels vous demandez l'assistance du support

- Vous avez oublié votre mot de passe.
- Vous avez saisi un mot de passe incorrect un trop grand nombre de fois à l'authentification au démarrage. L'ordinateur a été verrouillé.
- Vous avez oublié ou perdu votre clé cryptographique/carte à puce.
- Le cache local de l'authentification au démarrage est partiellement endommagé.
- Un autre utilisateur doit démarrer l'ordinateur protégé par SafeGuard Enterprise.
- Un utilisateur doit démarrer l'ordinateur protégé par SafeGuard Enterprise depuis un support externe.

8.2 Procédures pour lesquelles une réponse peut être demandée et scénarios correspondants

■ Initialisation du client SafeGuard Enterprise sans connexion utilisateur :

L'initialisation de l'ordinateur sans connexion utilisateur est utile si vous avez saisi un mot de passe incorrect (par exemple à cause de fautes de frappe, de l'activation de la touche Verr. maj, etc.) mais que vous connaissez le mot de passe correct. La procédure Challenge/Réponse permet de vous connecter à votre ordinateur sans réinitialiser le mot de passe.

Si vous avez saisi un mot de passe incorrect un trop grand nombre de fois, le support génère automatiquement un code de réponse pour initialiser le client sans connexion utilisateur. Les exigences de ce cas particulier sont incluses dans le challenge. Vous pouvez ultérieurement vous reconnecter avec vos nom d'utilisateur et mot de passe.

■ Initialisation du client SafeGuard Enterprise avec une connexion utilisateur :

Si vous avez oublié votre mot de passe, demandez immédiatement un challenge sans essayer de saisir de nouveau le mot de passe. Le support peut alors générer une réponse pour la connexion avec ou sans nom d'utilisateur. Lors d'une connexion avec votre nom d'utilisateur, demandez au support l'affichage de votre ancien mot de passe lors de la procédure Challenge/Réponse. Ceci évite d'avoir à réinitialiser le mot de passe. Sinon, lors d'une connexion avec votre nom d'utilisateur, vous devez réinitialiser votre mot de passe de connexion Windows pendant la procédure Challenge/Réponse.

Remarque : pour les utilisateurs travaillant hors ligne (qui ne sont pas connectés au contrôleur de domaine), certaines conditions doivent être pris en compte ([voir Challenge/Réponse pour les utilisateurs hors ligne](#) à la page 46).

■ Restauration du cache de stratégies SafeGuard Enterprise :

Cette procédure est nécessaire si le cache de stratégies SafeGuard est endommagé. Le cache local stocke toutes les clés et stratégies ainsi que les certificats utilisateur et les fichiers d'audit. Lorsque le cache local est corrompu, la récupération de connexion est désactivée par défaut, c'est-à-dire que sa restauration s'effectue automatiquement à partir de la sauvegarde. Aucune procédure Challenge/Réponse n'est donc requise pour réparer le cache local. Cependant, la récupération de connexion peut être activée par stratégie, si le cache local doit effectivement être réparé 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.

■ Initialisation à partir d'un support externe ou d'une disquette :

Il est également possible d'utiliser la procédure Challenge/Réponse pour autoriser la réinitialisation d'un ordinateur à partir d'un support externe. Dans la boîte de dialogue de connexion de l'authentification au démarrage, sélectionnez **Disquette/Support externe** dans le champs **Poursuivre l'initialisation à partir de :** et lancez la procédure Challenge/Réponse. Le support peut alors générer une réponse pour les actions suivantes :

- Initialisation du client SGN avec une connexion utilisateur
- Initialisation du client SGN sans connexion utilisateur

- Autorisation de la procédure d'initialisation à partir d'un support externe

8.3 Procédure Challenge/Réponse

1. L'authentification au démarrage démarre.

Remarque : lorsque vous générez le challenge, vous avez 30 minutes pour saisir la réponse générée par le support dans une procédure Challenge/Réponse. Le code de réponse n'est plus valide et ne peut plus être utilisé une fois les 30 minutes écoulées.

2. Demande de challenge :

Ouvre la boîte de dialogue **Challenge** dans l'authentification au démarrage. Un code de challenge sous la forme d'une chaîne de caractères ASCII est généré puis affiché.

3. Contactez le support.

Fournissez au support technique vos données utilisateur (ID utilisateur, ID ordinateur) comme indiqué dans la boîte de dialogue **Challenge**, ainsi que le code de challenge.

4. Le support technique génère un code de réponse dans le SafeGuard Management Center.
5. Le support technique fournit la réponse par téléphone ou par SMS.
6. Saisissez le code de réponse dans l'authentification au démarrage.

Vous pouvez maintenant exécuter l'action autorisée, Par exemple, la réinitialisation du mot de passe.

Vous pouvez reprendre vos activités.

8.4 Demande de challenge

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

Le bouton **Récupération** n'est activé que si vous entrez un nom d'utilisateur ou au moins un caractère dans la boîte de dialogue du code PIN.

Remarque : si vous saisissez un mot de passe/code PIN incorrect un trop grand nombre de fois ou si le cache de stratégies est endommagé, SafeGuard Enterprise vous informe automatiquement et propose de résoudre le problème via la procédure Challenge/Réponse.

Vos données utilisateur et un code de challenge généré de manière aléatoire s'affichent. Pour une meilleure lisibilité, le code de challenge est divisé en blocs de cinq caractères.

2. Contactez le support technique de SafeGuard Enterprise et fournissez vos données utilisateur ainsi que le code de challenge au responsable du support.

Si vous avez besoin d'aide pour l'indication du code de challenge, vous pouvez cliquer sur le bouton **Aide à la correction orthographique**.

Le responsable du support technique se sert du code de challenge pour identifier le scénario approprié.

3. Cliquez sur **Suivant**.

8.5 Saisie des informations d'identification .

1. Saisissez le code de réponse fourni par le responsable du support technique dans la boîte de dialogue **Réponse** et cliquez sur **OK**.

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

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

Si nécessaire, SafeGuard Enterprise vous invite à modifier vos informations d'identification utilisateur Windows.

8.6 Pratique recommandée

8.6.1 Vous avez saisi un mot de passe incorrect un trop grand nombre de fois

Vous avez saisi un mot de passe incorrect dans l'authentification au démarrage un trop grand nombre de fois (erreurs de saisie, touche Verr. maj activée, etc.) mais vous connaissez le mot de passe correct. Vous êtes connecté au domaine.

1. Votre ordinateur est verrouillé. Vous êtes invité à lancer une procédure Challenge/Réponse pour le déverrouiller.
2. Votre responsable du support génère une réponse pour l'initialisation sans connexion utilisateur.

L'initialisation sans connexion utilisateur signifie que vous ne devez pas modifier le mot de passe avant de vous connecter à Windows.

3. La boîte de dialogue de connexion de Windows s'affiche. Saisissez votre mot de passe Windows dans la boîte de dialogue.

Vous êtes connecté au système.

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

Remarque: vous pouvez également demander une réponse avec une connexion utilisateur. Dans ce cas, vous êtes invité à modifier vos codes d'accès Windows avant de vous connecter à Windows.

8.6.2 Vous avez oublié votre mot de passe

Nous vous recommandons d'utiliser les méthodes suivantes pour récupérer un mot de passe oublié. En utilisant ces méthodes, vous évitez d'avoir à réinitialiser le mot de passe de manière centralisée :

- Utilisez Local Self Help. Grâce à la récupération via Local Self Help, le mot de passe actuel peut être affiché et vous pouvez continuer à l'utiliser sans devoir le réinitialiser et sans requérir l'assistance du support. Pour plus d'informations, voir [Récupération via Local Self Help](#) à la page 30.
- Lors de l'utilisation de la procédure Challenge/Réponse : demandez au support de générer une réponse avec la connexion de l'utilisateur et d'afficher votre ancien mot de passe lors de la procédure Challenge/Réponse. Cela évitera d'avoir à le réinitialiser. Vous pouvez continuer à travailler avec l'ancien mot de passe et le modifier localement par la suite, si vous le souhaitez.

Si vous n'utilisez pas l'une de ces méthodes, procédez comme suit :

1. En cas d'oubli du mot de passe, vous recevez une réponse pour initialiser votre ordinateur avec une connexion utilisateur. Dans ce cas, modifiez votre mot de passe lors de la connexion à Windows (à condition que le domaine soit accessible).
2. Une fois le mot de passe changé, utilisez le nouveau mot de passe pour vous connecter à partir de l'authentification au démarrage.

8.6.3 Vous avez oublié ou perdu votre clé cryptographique

Dans ce cas, la procédure Challenge/Réponse avec une connexion utilisateur doit être effectuée.

1. Vous êtes invité à changer votre mot de passe pendant la procédure Challenge/Réponse.

Remarque : la boîte de dialogue permettant de changer le mot de passe ne s'affiche que si une connexion au contrôleur de domaine est établie.

2. Si la connexion avec une clé cryptographique et un code PIN est obligatoire, vous pouvez changer le mot de passe ou ignorer le changement du mot de passe en cliquant sur **Annuler**.

■ **Vous avez oublié votre clé cryptographique**

Vous pouvez ignorer le changement de mot de passe en cliquant sur **Annuler** dans la boîte de dialogue si vous avez oublié votre clé cryptographique mais que vous en disposerez pour les connexions futures. Lorsque vous cliquez sur **Annuler**, vous êtes connecté au système et vous pouvez de nouveau utiliser votre ordinateur.

Sans clé cryptographique, vous ne pouvez vous connecter à partir de l'authentification au démarrage que via la procédure Challenge/Réponse. Une fois votre clé cryptographique récupérée, vous pouvez l'utiliser pour vous connecter à partir de l'authentification au démarrage.

■ **Vous avez perdu votre clé cryptographique**

En cas de perte de votre clé cryptographique, entrez un nouveau mot de passe dans la boîte de dialogue de changement du mot de passe. Vous êtes connecté à Windows avec ce mot de passe. Si les stratégies définies sur votre ordinateur vous y autorisent (la connexion avec une clé cryptographique à partir de l'authentification au démarrage n'est pas obligatoire), vous pouvez également vous connecter à partir de l'authentification au démarrage en utilisant ce mot de passe.

L'utilisation non autorisée de la clé cryptographique par quiconque la trouve peut être spécifiée. Des utilisateurs non autorisés ne peuvent pas utiliser la clé cryptographique pour se connecter (même s'ils connaissent le code PIN) puisque votre mot de passe a été changé.

8.6.4 Vous avez oublié votre code PIN

1. Si vous avez oublié votre code PIN de votre clé cryptographique, demandez une réponse et saisissez un nouveau mot de passe. Vous êtes connecté à Windows avec ce mot de passe. Vous pouvez aussi l'utiliser pour vous connecter à partir de l'authentification au démarrage à condition d'être autorisé à vous connecter en utilisant un mot de passe.
2. Un responsable de la sécurité doit attribuer un nouveau code PIN à la clé cryptographique et stocker vos nouveaux codes d'accès de connexion sur celle-ci. Vous pouvez alors l'utiliser pour vous connecter.

8.6.5 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, SafeGuard Enterprise 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 par le biais d'un environnement WinPE. Lorsque vous êtes dans une situation critique de ce type, nous vous recommandons de contacter le support technique de SafeGuard Enterprise. 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.

8.7 Challenge/Réponse pour les utilisateurs hors ligne

Les utilisateurs hors ligne doivent prendre en compte certaines conditions pour la procédure Challenge/Réponse. Pour les utilisateurs hors ligne (qui ne sont pas connectés au contrôleur de domaine, par exemple, les représentants de commerce travaillant sur un ordinateur portable), aucun changement de mot de passe automatique ne peut être effectué pendant la procédure Challenge/Réponse.

8.7.1 Challenge/Réponse pour utilisateurs hors ligne avec le mode de connexion nom d'utilisateur/mot de passe

Exemple :

Vous travaillez hors ligne (vous n'êtes pas connecté au contrôleur de domaine) et vous avez oublié votre mot de passe. Grâce à la procédure Challenge/Réponse, vous pouvez rapidement et facilement accéder de nouveau à votre ordinateur.

SafeGuard Enterprise peut également vous connecter à Windows automatiquement pendant la procédure Challenge/Réponse. Néanmoins, comme vous ne connaissez pas le mot de passe après cette procédure, vous devez la répéter à chaque démarrage de l'ordinateur. Par ailleurs, vous ne pouvez pas déverrouiller l'ordinateur lorsqu'il est verrouillé (activation du verrouillage via l'économiseur d'écran par exemple). Dans ce cas, redémarrez l'ordinateur, au risque d'entraîner une perte de données (puis relancer une procédure Challenge/Réponse).

Remarque: c'est pour cela que SafeGuard Enterprise permet d'afficher le mot de passe pendant une procédure Challenge/Réponse. En tant qu'utilisateur hors ligne, vous devez afficher votre mot de passe pendant une procédure Challenge/Réponse. Indiquez au responsable du support que vous souhaitez afficher votre mot de passe. Il doit activer explicitement l'affichage du mot de passe avant de générer votre code de réponse.

Veuillez procéder comme suit :

1. Pour lancer la procédure Challenge/Réponse, cliquez sur **Récupération** dans la boîte de dialogue de connexion de l'authentification au démarrage.
2. Appelez le support technique et indiquez-lui votre code de challenge.
3. Indiquez au responsable support que vous souhaitez initialiser votre ordinateur avec une connexion utilisateur et que votre mot de passe doit être affiché.
4. Cliquez sur **Suivant** dans la boîte de dialogue **Challenge/Réponse** et saisissez la réponse.
5. Cliquez sur **OK**.

Il vous est demandé si vous souhaitez que l'ancien mot de passe s'affiche à l'écran.

6. Répondez **Oui** et cliquez sur **OK**.

7. La boîte de dialogue suivante vous informe que le mot de passe s'affichera si vous appuyez sur la touche **Entrée** ou sur la **Barre d'espace** de votre clavier, ou si vous cliquez dans le texte.

Remarque : 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 s'affiche pendant 5 secondes. Le processus d'initialisation continue ensuite automatiquement.

8. Appuyez sur la touche **Entrée** ou sur la **Barre d'espace** de votre clavier, ou cliquez dans le texte.

Le mot de passe s'affiche.

Remarque : assurez-vous qu'aucune personne non autorisée ne peut voir 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. Le mot de passe ne s'affiche que pendant 5 secondes maximum.

9. Vous pouvez lire le mot de passe et l'utiliser pour vous connecter à partir de l'authentification au démarrage et pour vous connecter à Windows.

Vous pouvez reprendre vos activités sur l'ordinateur.

8.7.2 Challenge/Réponse pour utilisateurs hors ligne avec le mode de connexion «**clé cryptographique uniquement**»

Dans ce cas, si vous avez oublié votre code PIN ou oublié/perdu votre clé cryptographique, la procédure à utiliser n'est pas la même selon que vous connaissez vos informations d'identification Windows ou non.

❖ Vous connaissez vos informations d'identification Windows

- a) Si vous connaissez vos informations d'identification Windows, lancez la procédure Challenge/Réponse comme décrit. Vous êtes automatiquement connecté à Windows.

Le mode de connexion **Clé cryptographique uniquement** est réinitialisé pour la durée de la session de travail après la procédure Challenge/Réponse. Par conséquent, une connexion à Windows avec votre nom d'utilisateur et votre mot de passe devient également possible.

En cas de verrouillage de l'ordinateur, vous pouvez le déverrouiller en entrant votre mot de passe Windows. Toutefois, la connexion à partir de l'authentification au démarrage est également possible en utilisant la procédure Challenge/Réponse.

❖ Vous ne connaissez pas vos informations d'identification Windows

- a) Si vous ne connaissez pas vos informations d'identification Windows et que vous avez oublié votre code PIN, vous pouvez également lancer une procédure Challenge/Réponse pendant laquelle votre mot de passe s'affiche.

- b) Indiquez à votre responsable support que votre mot de passe doit être affiché.

Dans la mesure où le mode de connexion **Clé cryptographique** uniquement est désactivé, vous pouvez, le cas échéant, également déverrouiller votre ordinateur en utilisant ce mot de passe.

Toutefois, la connexion à partir de l'authentification au démarrage est également possible en utilisant la procédure Challenge/Réponse.

9 Icône de la barre d'état système et infobulles

Vous pouvez accéder facilement à toutes les fonctions importantes du client SafeGuard Enterprise de votre ordinateur. L'icône de la zone de notification de SafeGuard Enterprise est placée sur la barre des tâches Windows pour permettre l'accès à ces fonctions.

Remarque : le comportement de l'icône de la barre d'état sur votre ordinateur est déterminé par le responsable de la sécurité. Il définit, dans une stratégie, l'affichage de l'icône sur votre ordinateur. Elle peut également être définie sur «Muet». Dans ce cas, les infobulles ne s'affichent pas sur votre ordinateur.

Grâce à l'icône de la zone de notification du système, vous pouvez afficher des informations ou effectuer des actions spécifiques. Cliquez avec le bouton droit de la souris sur l'icône pour afficher un menu proposant les entrées suivantes :

■ Affichage :

- **Jeu de clés :** affiche toutes les clés disponibles.
- **Certificat :** affiche des informations relatives à votre certificat.

■ **Créer une nouvelle clé :** ouvre une boîte de dialogue permettant de créer une nouvelle clé à utiliser pour l'échange de données par l'intermédiaire de supports amovibles ([voir Échange de données SafeGuard](#) à la page 56).

■ Local Self Help

Si Local Self Help est activé pour votre ordinateur dans la stratégie correspondante, la commande Local Self Help s'affiche dans le menu contextuel de l'icône de la zone de notification du 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 plus d'informations, reportez-vous à la section [Récupération avec Local Self Help](#) à la page 30.

■ **Changer la phrase de passe du support :** ouvre une boîte de dialogue permettant de créer une nouvelle clé à utiliser pour l'échange de données par l'intermédiaire de supports amovibles ([voir Échange de données SafeGuard](#) à la page 56).

■ **Synchroniser :** lance une synchronisation des données avec le serveur SafeGuard Enterprise. Les infobulles indiquent la progression et le résultat de la synchronisation des données.

Remarque : vous pouvez également lancer la synchronisation en cliquant deux fois sur l'icône de la zone de notification système.

■ **État :** ouvre une boîte de dialogue proposant des informations sur l'état actuel de l'ordinateur protégé par SafeGuard Enterprise :

Champ	Informations
Dernière stratégie reçue	Indique quand (date et heure) l'ordinateur a reçu la dernière stratégie.
Dernière clé reçue	Indique quand (date et heure) l'ordinateur a reçu la dernière clé.
Dernier certificat reçu	Indique quand (date et heure) l'ordinateur a reçu le dernier certificat.
Dernier contact du serveur	Indique la date et l'heure du dernier contact avec le serveur.
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 La réplication de l'utilisateur dans l'authentification au démarrage est en attente, c'est-à-dire que la synchronisation utilisateur initiale n'est pas encore terminée. Ces informations sont tout particulièrement importantes après la première connexion à SafeGuard Enterprise car vous ne pouvez vous connecter à partir de l'authentification au démarrage qu'une fois la synchronisation utilisateur initiale terminée. ■ Utilisateur SGN Lors de l'installation de SafeGuard Enterprise, l'utilisateur a été affecté en tant qu'utilisateur SafeGuard Enterprise. ■ Invité SGN L'utilisateur connecté à Windows est un utilisateur SafeGuard Enterprise invité. L'utilisateur est autorisé à se connecter à Windows mais il n'est pas affecté à l'ordinateur protégé par SafeGuard Enterprise en tant qu'utilisateur SafeGuard Enterprise. ■ Invité SGN (compte de service) L'utilisateur connecté à Windows est un utilisateur SafeGuard Enterprise invité qui s'est connecté via un compte de service pour effectuer des tâches administratives. ■ Inconnu Indique que le statut de l'utilisateur n'a pas pu être déterminé.

Champ	Informations
État du cache de stratégies Paquets de données préparés pour la transmission	Indique si des packages doivent être envoyés au serveur SafeGuard Enterprise.
État de Local Self Help (LSH) Activé Actif	Indique si Local Self Help a été activé dans une stratégie et s'il est actif sur l'ordinateur de l'utilisateur. Pour plus d'informations, voir Récupération avec Local Self Help à la page 30.
Prêt pour le renouvellement du certificat	Ce texte est affiché si le responsable de la sécurité a affecté un nouveau certificat pour la connexion avec une clé non cryptographique sur votre ordinateur. Vous pouvez changer le certificat de connexion de clé cryptographique, reportez-vous à la section Changement du certificat pour les connexions avec clé cryptographique à la page 13.

- **Aide** : ouvre l'aide en ligne de SafeGuard Enterprise.
- **À propos de SafeGuard Enterprise** : fournit des informations sur votre version de SafeGuard Enterprise.

10 Accès aux fonctions via les extensions de l'Explorateur

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

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

Vous pouvez accéder aux fonctions de chiffrement basé sur fichier à partir des 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 à partir de 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 à partir du menu contextuel.

Si une stratégie de chiffrement basé sur fichier s'applique au volume sélectionné, support amovible, répertoire ou fichier sélectionné, les entrées de chiffrement 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 chiffrés de nouveau.
- **Afficher l'état 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.
- **Créer une nouvelle clé** : ouvre une boîte de dialogue permettant de créer des clés locales définies par l'utilisateur.

10.2 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. Un symbole de clé verte indique que vous disposez des clés requises et que vous pouvez accéder au volume.

Remarque : **Chiffrement de fichier > Afficher l'état du chiffrement** indique l'état du 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.

Ajout/Suppression de clés

Vous pouvez ajouter des clés au volume chiffré et en supprimer si les paramètres définis dans les stratégies applicables l'autorisent. Vous autorisez ainsi tous les propriétaires de la clé concernée à accéder aux données chiffrées de ce volume.

Vous pouvez attribuer des clés au volume dans la boîte de dialogue **Propriétés** du volume. Cette boîte de dialogue comprend l'onglet **Chiffrement** (clic droit sur **Volume > Propriétés > Chiffrement**).

Sélectionnez une clé dans la liste du bas et cliquez sur **Ajouter une clé**. Le fichier est déplacé vers le haut dans la liste de sélection des clés. Il est inclus dans la liste des clés pouvant être utilisées pour accéder au volume chiffré.

Grâce à l'option **Supprimer une clé**, vous pouvez supprimer la clé de la liste de clés qui sont utilisées pour accéder au support.

11 Chiffrement de données

SafeGuard Enterprise 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.

11.1 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. Les fichiers sont chiffrés de nouveau dès que vous les fermez ou que vous les enregistrez.

Si vous copiez ou déplacez les fichiers (en utilisant également **Enregistrer sous**) à partir d'un lecteur chiffré vers un emplacement de fichiers non chiffrés sur votre ordinateur, ils sont alors déchiffrés. Les fichiers sont stockés au nouvel emplacement en texte brut.

11.2 Chiffrement initial

La configuration initiale des ordinateurs protégés par SafeGuard Enterprise peut impliquer la création de stratégies de chiffrement qui seront distribuées sur les ordinateurs via un package de configuration.

Après le premier déploiement de la stratégie de chiffrement sur votre ordinateur, le chiffrement initial s'effectue selon les paramètres reçus.

11.2.1 Chiffrement initial pour le chiffrement basé sur volume

Dès que votre ordinateur reçoit une stratégie de chiffrement basé sur volume suite à l'installation de SafeGuard Enterprise, le chiffrement initial basé sur volume démarrera automatiquement.

Le chiffrement initial basé sur volume s'exécute en fond de tâche, vous permettant ainsi de continuer à utiliser votre ordinateur.

11.2.2 Chiffrement initial pour le chiffrement basé sur fichier

Si une stratégie spécifiant le chiffrement de fichiers s'applique à un emplacement de votre ordinateur, un symbole de clé jaune s'affiche à côté 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.

Si un chiffrement est défini pour des fichiers, soit le chiffrement initial démarre automatiquement, soit vous devez le démarrer manuellement.

11.2.3 Restrictions pour le chiffrement initial des ordinateurs protégés par SafeGuard Enterprise

La configuration initiale des ordinateurs protégés par SafeGuard Enterprise peut impliquer la création de stratégies de chiffrement qui seront distribuées sur les ordinateurs via un package de configuration. Lorsque le client SafeGuard Enterprise ne se connecte pas à un serveur SafeGuard Enterprise juste après l'installation du package de configuration, mais est temporairement hors ligne, seules les stratégies de chiffrement présentant les paramètres spécifiques suivants sont immédiatement activées sur l'ordinateur protégé par SafeGuard Enterprise :

- Protection des périphériques basés sur le volume avec la **Clé machine définie** comme clé de chiffrement

Pour que toutes les autres stratégies impliquant le chiffrement à l'aide de clés définies par l'utilisateur soient activées sur l'ordinateur protégé par SafeGuard Enterprise, le package de configuration correspondant doit également être réaffecté à l'ordinateur. Les clés définies par l'utilisateur sont créées uniquement lorsque la connexion entre le client SafeGuard Enterprise et le serveur SafeGuard Enterprise est rétablie.

La **clé machine définie** est en effet créée sur l'ordinateur protégé par SafeGuard Enterprise au premier redémarrage suivant l'installation, tandis que les clés définies par les utilisateurs ne peuvent être créées sur l'ordinateur qu'après avoir été enregistrées sur le serveur SafeGuard Enterprise.

11.3 Chiffrement basé sur volume

Le chiffrement basé sur volume d'un disque sur l'ordinateur protégé par SafeGuard Enterprise démarre automatiquement si le responsable de la sécurité a défini la stratégie correspondante.

1. Une boîte de dialogue s'affiche ; vous êtes invité à sélectionner une clé vous permettant d'accéder au volume.

Remarque : chaque utilisateur, dont le jeu de clés comprend cette clé, peut accéder à ce volume. Le responsable de la sécurité définit la portée des clés proposées. Si le responsable de la sécurité a défini une clé spécifique, vous ne pouvez pas en sélectionner une autre.

2. Cliquez sur **OK** pour démarrer le chiffrement.

Un observateur de chiffrement indique l'avancement du processus de chiffrement du volume à chiffrer. Il montre aussi les volumes chiffrés disponibles. Il est en vue réduite dans la barre des tâches Windows. Vous pouvez ouvrir l'observateur de chiffrement en cliquant sur l'icône. Si l'observateur 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'observateur 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 d'extrémité sans assignation de lettre de lecteur. Cette partition système ne peut pas être chiffrée par SafeGuard Enterprise.

11.4 Chiffrement basé sur fichier

Le chiffrement d'un volume démarre automatiquement ou vous devez lancer le processus.

1. Si le chiffrement ne démarre pas automatiquement, sélectionnez **Chiffrement de fichier > Démarrer le chiffrement**.
2. Si le responsable de la sécurité n'a pas défini de clé spécifique, une boîte de dialogue s'affiche et vous invite à sélectionner une clé vous permettant d'accéder à ce volume.

Remarque :

Chaque utilisateur, dont le jeu de clés comprend cette clé, peut accéder à ce volume. Le responsable de la sécurité définit la portée des clés proposées. Si le responsable de la sécurité a défini une clé spécifique, vous ne pouvez pas en sélectionner une autre.

Pour échanger des données avec des utilisateurs disposant de SafeGuard Enterprise sur leur ordinateur mais n'utilisant pas la même clé que vous, vous avez généralement besoin des **clés locales définies par l'utilisateur**. Ces clés sont également nécessaires à l'échange de données sécurisé avec des utilisateurs ne disposant pas de SafeGuard Enterprise. Les clés locales sont reconnaissables au préfixe (Local_).

Si l'option **Chiffrer de nouveau les fichiers s'ils le sont déjà avec une autre clé** est activée, les fichiers chiffrés et pour lesquels une clé existe sont déchiffrés et chiffrés de nouveau avec la nouvelle clé.

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

Toutes les données du volume concerné sont chiffrées.

11.4.1 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 en utilisant le menu contextuel du fichier sur un volume ou en utilisant le menu contextuel du support de stockage 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.

11.4.2 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 l'état 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 > État du chiffrement** dans le menu contextuel du volume, une boîte de dialogue s'affiche indiquant tous les fichiers et leur état de chiffrement.

11.5 Restrictions d'accès aux volumes

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

Le chiffrement des volumes a échoué

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

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

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 SafeGuard Enterprise.

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

12 SafeGuard Data Exchange

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 intervention minimale de l'utilisateur.

Seuls les utilisateurs disposant des clés appropriées 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 de nouveau chiffré 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 de manière centralisée par le responsable de la sécurité.

Dans le cadre de son administration centralisée, 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 existants 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. Le responsable de la sécurité peut également spécifier que vous n'êtes pas autorisé à accéder aux fichiers non chiffrés et laisser ces fichiers non chiffrés.

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

- **SafeGuard Enterprise 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 phrase de passe de la clé au destinataire des données.
- **SafeGuard Enterprise n'est pas installé sur l'ordinateur du destinataire :** SafeGuard Enterprise met à votre disposition SafeGuard Portable. Cet utilitaire peut être copié automatiquement sur le support amovible en plus des fichiers chiffrés. Grâce à SafeGuard Portable et à la phrase de passe correspondante, le destinataire peut déchiffrer les fichiers chiffrés et les rechiffrer sans que SafeGuard Data Exchange ne soit installé sur son ordinateur.

12.1 Paramètres de gestion des supports amovibles

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 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, sélectionnez une clé ou utilisez une clé prédéfinie.
- **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 de stockage amovible, s'il a été transféré à un tiers par exemple.
- **Vous êtes autorisé à définir une phrase de passe du support pour le support amovible** : vous êtes invité à saisir une phrase de passe 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 sont pas chiffrés par SafeGuard Data Exchange.
- **Vous pouvez décider du chiffrement** : lorsque vous connectez un support amovible à votre ordinateur, un message vous demande si vous désirez chiffrer les fichiers du support.

12.2 Phrase de passe du support unique pour chaque périphérique amovible connecté à l'ordinateur

SafeGuard Data Exchange permet de définir une phrase de passe 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 saisie d'une phrase de passe du support. La phrase de passe du support est liée aux ordinateurs auxquels vous êtes autorisé à vous connecter. Vous utilisez donc la même phrase de passe de support sur chaque ordinateur.

La phrase de passe du support peut être changée et est synchronisée automatiquement sur chaque ordinateur avec lequel vous travaillez, dès que vous connectez un support amovible à cet ordinateur.

Une phrase de passe du support est utile dans les situations suivantes :

- Vous souhaitez utiliser des données chiffrées sur un support amovible qui se trouvent également sur des ordinateurs sur lesquels SafeGuard Enterprise 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 phrase de passe du support, vous pouvez leur permettre d'accéder à tous les fichiers du support amovible, avec une phrase de passe 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 phrase de passe d'une clé spécifique (une « clé locale », qui peut être créée par un utilisateur de SafeGuard Data Exchange). 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.

Remarque : une phrase de passe du support n'est pas nécessaire si vous utilisez des clés de groupe SafeGuard Enterprise pour échanger des données sur un support amovible, au sein d'un groupe de travail dans lequel les membres partagent cette clé. Dans ce cas, si votre responsable de la sécurité l'a spécifié, l'accès aux fichiers chiffrés du support amovible est entièrement transparent. Il n'est pas nécessaire de saisir une phrase de passe ou un mot de passe. En effet, les clés de groupe et les phrases de passe de support pour les supports amovibles peuvent être utilisées simultanément. Dans la mesure où le système détecte automatiquement une clé de groupe disponible, l'accès pour les utilisateurs partageant cette clé est entièrement transparent. Si aucune clé de groupe n'est détectée, SafeGuard Data Exchange affiche une boîte de dialogue qui invite l'utilisateur à saisir une phrase de passe du support ou la phrase de passe d'une clé locale.

Supports pris en charge

SafeGuard Data Exchange prend en charge les supports amovibles suivants :

- Clés USB
- Disques durs externes connectés par 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)

12.3 Chiffrement de supports amovibles

12.3.1 Chiffrement initial

Le chiffrement des données non chiffrées présentes sur des supports amovibles démarre automatiquement dès que vous connectez les supports au système ou nécessite que vous lanciez le processus manuellement. Si vous êtes autorisé à décider si les fichiers sur support amovible doivent être chiffrés, vous êtes invité à effectuer le chiffrement lorsque le support amovible est connecté à l'ordinateur.

Pour commencer le chiffrement, procédez comme suit :

1. Sélectionnez **Chiffrement de fichier > Démarrer le chiffrement** dans le menu contextuel du support dans 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, puis cliquez sur **OK**. Toutes les données contenues sur le support amovible sont chiffrées.

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.

Remarque: pour échanger des données avec des utilisateurs disposant de SafeGuard Enterprise sur leur ordinateur mais n'utilisant pas la même clé que vous, vous avez besoin des clés locales définies par l'utilisateur ou de la phrase de passe du support. Ces clés sont également nécessaires à l'échange de données sécurisé avec des utilisateurs ne disposant pas de SafeGuard Enterprise. Les clés locales sont reconnaissables au préfixe (Local_).

Si l'option **Chiffrer les fichiers bruts et mettre à jour les fichiers chiffrés** est activée, les fichiers chiffrés avec une clé existante sont déchiffrés et chiffrés de nouveau 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.

Chiffrement initial pour les utilisateurs avec une phrase de passe de supports amovibles

Si l'utilisation d'une phrase de passe du support amovible a été spécifiée dans l'administration centralisée, vous êtes invité à saisir la phrase de passe du support avant le chiffrement initial. La phrase de passe 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 phrase de passe du support amovible.

Une fois que vous avez saisi une fois la phrase de passe du support amovible, le chiffrement initial démarre automatiquement lorsque vous connectez un périphérique différent à votre ordinateur.

Remarque: le chiffrement initial ne démarre pas sur les ordinateurs sur lesquels votre phrase de passe du support amovible n'est pas paramétrée.

12.3.2 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.

Phrase de passe du support

Si l'utilisation d'une phrase de passe du support a été spécifiée dans l'administration centralisée, 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, veuillez indiquer une phrase de passe de support. Vous pouvez utiliser cette phrase de passe du support unique pour accéder à tous les fichiers chiffrés sur votre support amovible, indépendamment de la clé effectivement utilisée pour les chiffrer.

La phrase de passe du support est valide pour tous les périphériques que vous connectez à l'ordinateur. La phrase de passe 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.

Changement/réinitialisation de la phrase de passe du support

Vous pouvez changer votre phrase de passe du support à tout moment en utilisant la commande **Changer la phrase de passe 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 phrase de passe du support, puis confirmer la nouvelle.

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

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

Synchronisation de la phrase de passe du support

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

Remarque : après avoir changé votre phrase de passe du support, connectez tous vos supports amovibles à votre ordinateur. Ceci garantit que la nouvelle phrase de passe du support est utilisée immédiatement sur tous vos périphériques (synchronisation).

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 à partir du menu contextuel d'un fichier du support amovible ou à partir du 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.

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

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

- Échange de données avec des utilisateurs SafeGuard Enterprise disposant d'au moins une clé faisant également partie de votre jeu de clés.

Dans ce cas, chiffrez les données du support amovible avec une clé faisant également partie du jeu de clés du destinataire (sur son ordinateur portable par exemple). Le destinataire peut utiliser la clé pour accéder aux données chiffrées de manière transparente.

- Échange de données avec des utilisateurs SafeGuard Enterprise 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 phrase de passe et peuvent être importées par SafeGuard Enterprise. Vous fournissez la phrase de passe au destinataire des données. Grâce à la phrase de passe, le destinataire peut importer la clé et accéder aux données.

- Échange de données avec des utilisateurs ne disposant pas de SafeGuard Enterprise

Les utilisateurs ne disposant pas de SafeGuard Enterprise sur leurs ordinateurs peuvent utiliser SafeGuard Portable. Pour échanger des données avec SafeGuard Portable, des clés locales doivent également être utilisées avec une phrase de passe.

SafeGuard Portable doit également être copié sur le support de stockage amovible. Vous devez également fournir au destinataire les données chiffrées avec la phrase de passe correspondante. Grâce à la phrase de passe et à SafeGuard Portable, l'utilisateur peut déchiffrer les fichiers chiffrés, pour les modifier par exemple, et les réenregistrer chiffrés sur le support de stockage amovible. SafeGuard Portable étant une application indépendante, aucun autre logiciel n'a besoin d'être installé sur l'ordinateur 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.

12.4.1 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 phrase de passe correspondante. La personne qui a chiffré les données doit vous fournir la phrase de passe.

1. Sélectionnez le fichier correspondant sur le support amovible et cliquez sur **Chiffrement de fichier > Gestion des clés > Importer une clé**.
2. Saisissez la phrase de passe dans la boîte de dialogue qui s'affiche.

La clé est importée et vous pouvez accéder au fichier.

12.4.2 Création de clés locales

1. Cliquez avec le bouton droit de la souris sur l'icône de la zone de notification de SafeGuard Enterprise dans la barre des tâches Windows.
2. Cliquez sur **Créer une nouvelle clé**.
3. Dans la boîte de dialogue **Création d'une clé**, saisissez un **Nom** et une **Phrase de passe** pour la clé.

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

4. Confirmez la phrase de passe.

Si vous saisissez une phrase de passe simple, un message d'avertissement s'affiche. Pour renforcer le niveau de sécurité, nous vous recommandons d'utiliser des phrases de passe complexes. Vous pouvez également décider d'utiliser la phrase de passe malgré le message d'avertissement. La phrase de passe doit 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**.

La clé est créée et sera disponible dès que les données auront été synchronisées avec le serveur SafeGuard Enterprise.

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

Pour que le destinataire puisse déchiffrer toutes les données contenues sur le support de stockage amovible, vous allez peut-être devoir chiffrer de nouveau les données sur le support de stockage 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 chiffrez les données. Cette opération n'est pas nécessaire si vous utilisez une phrase de passe du support.

12.5 Gravure de fichiers sur CD 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 bruts parmi les fichiers sélectionnés ;

Sous **État**, 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.

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 simples 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.

Gravure de fichiers bruts sur CD

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

Copie de 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.

12.5.1 Gravure de CD-ROM/DVD avec Windows Vista et Windows 7

Windows Vista et Windows 7 dispose d'un Assistant Graver un CD pour les CD-ROM/DVD.

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

12.6 SafeGuard Portable

Grâce à SafeGuard Portable, vous pouvez échanger des données chiffrées sur des supports amovibles avec des destinataires ne disposant pas de SafeGuard Data Exchange sur leurs ordinateurs. Les données chiffrées avec 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 AES 256.

Si vous utilisez SafeGuard Portable en combinaison avec la phrase de passe de support appropriée, vous pouvez accéder à tous les fichiers chiffrés, indépendamment de la clé locale utilisée pour les chiffrer. La phrase de passe 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 phrase de passe du support ou la phrase de passe d'une clé locale doit être communiquée au préalable au destinataire.

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

Il n'est pas nécessaire que SafeGuard Portable soit installé ou copié sur l'ordinateur de la personne avec laquelle vous communiquez. Il reste sur le support amovible.

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

12.6.1 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 cliquant deux fois sur **SGPortable.exe**.

Grâce à SafeGuard Portable, vous pouvez déchiffrer les données chiffrées contenues sur le support amovible et les chiffrer de nouveau. 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 phrase de passe correspondant à la clé utilisée.

2. Pour modifier les fichiers d'un support amovible, cliquez sur le fichier 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 Saisie d'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 . Saisissez la phrase de passe 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** à l'aide des icônes affichées dans la barre d'outils.

12.6.1.1 Définition de la clé 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 **Saisie d'une clé** s'affiche.

2. Saisissez un **Nom** et une **Phrase de passe** pour la clé. **Confirmez** la phrase de passe et cliquez sur **OK**.

La phrase de passe 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.

12.6.1.2 Chiffrement de fichiers sur 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, saisissez le nom de la clé et la phrase de passe (et confirmez la phrase de passe). 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.

12.6.1.3 Déchiffrement de fichiers sur 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 phrase de passe du support ou la phrase de passe d'une clé locale est affichée.

2. Saisissez la phrase de passe correspondante (l'expéditeur doit vous la fournir) et cliquez sur **OK**.

Le fichier est déchiffré.

La phrase de passe du support permet d'accéder à tous les fichiers chiffrés du support amovible, indépendamment de la clé locale utilisée pour les chiffrer. Si vous disposez uniquement de la phrase de passe 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 saisi la phrase de passe de la clé, vous n'aurez pas besoin de la saisir à nouveau au prochain chiffrement ou déchiffrement de fichiers chiffrés avec la même clé.

SafeGuard Portable stocke la phrase de passe 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 automatiquement lors de la fermeture de SafeGuard Portable.

12.6.1.4 Chiffrement de nouveaux fichiers avec SafeGuard Portable

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

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 votre souhait de chiffrer le fichier. Le fichier est chiffré avec la dernière clé utilisée et a été copié sur le support amovible.

12.6.1.5 Détermination de 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.

12.6.2 Autres opérations à l'aide de SafeGuard Portable

Les opérations suivantes sont également disponibles :

- ❖ **Ouvrir** : cette commande de menu n'est disponible que dans le menu **Fichier** de SafeGuard Portable.

À l'ouverture d'un fichier chiffré avec cette commande de menu, vous êtes invité à entrer la phrase de passe. Saisissez la phrase de passe et cliquez sur **OK**. Le fichier est déchiffré 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.

13 SafeGuard Configuration Protection

Grâce à SafeGuard Configuration Protection, vous pouvez définir les interfaces et les périphériques autorisés sur les ordinateurs d'extrémité. Ce module empêche l'introduction de programmes malveillants, ainsi que les exportations de données via des canaux non désirés tels que les réseaux locaux sans fil (WLAN). Il détecte et bloque également les matériels nuisibles tels que les enregistreurs de frappe.

En général, l'autorisation et le blocage des ports et des périphériques sur votre ordinateur s'effectuent à l'aide des stratégies. L'utilisation peut en outre être limitée à certains périphériques.

La restriction à certains périphériques est possible pour les types de ports suivants :

- USB
- PCMCIA
- Firewire

Les périphériques autorisés et interdits peuvent être définis pour ces ports.

Le responsable de la sécurité concerné définit de manière centralisée les ports et les périphériques susceptibles d'être utilisés.

Si un port spécifique n'est pas autorisé de manière générale, un message s'affiche une fois à la réception de la stratégie appropriée. Le port ne peut pas être utilisé.

Le message se présente sous la forme d'une infobulle associée à l'icône Configuration Protection dans la barre des tâches Windows.

Si des restrictions d'utilisation des ports et des supports de stockage ont été définies pour votre ordinateur, l'info-bulle vous avertit dès que vous essayez d'utiliser les ports et les supports de stockage non autorisés.

13.1 Procédure Challenge/Réponse pour la suspension de la stratégie de protection de la configuration

La SafeGuard Configuration Protection peut être suspendue sur l'ordinateur d'extrémité en utilisant la procédure Challenge/Réponse.

Cela implique les éléments suivants :

- Sur l'ordinateur d'extrémité, vous devez demander le code de challenge.
- Le responsable du support technique crée une réponse qui vous permet de suspendre sur l'ordinateur la stratégie pendant une période donnée.

13.2 Suspension de la stratégie de protection de la configuration

Vous devez avoir les droits suffisants pour pouvoir suspendre la stratégie de protection de la configuration.

1. Sur l'ordinateur d'extrémité, cliquez avec le bouton droit de la souris sur l'icône de la barre d'état système et sélectionnez **Suspendre la protection de la configuration**.

2. Dans **Suspendre la protection de la configuration**, sélectionnez la période de suspension désirée. Le code de challenge est généré automatiquement. Il est valide pendant 30 minutes.
3. Contactez l'assistance du support et fournissez les informations utilisateur, le code de challenge et la période de suspension désirée par courriel, texto ou téléphone.
4. L'assistance du support confirmera les informations données et vous fournira le code de réponse nécessaire par courriel, texto ou téléphone.
5. Sur l'ordinateur d'extrémité, dans **Suspendre la protection de la configuration**, entrez ou copiez le code de réponse fourni par l'assistance du support. Veuillez vous assurer que la période correspond à celle fournie par l'assistance du support. Cliquez sur **OK**.

La stratégie de protection de la configuration est suspendue pour la période spécifiée. Elle peut être relancée de deux manières :

- Lors de la période de suspension spécifiée, sur l'ordinateur d'extrémité, l'utilisateur clique avec le bouton droit de la souris sur l'icône de la barre d'état système et sélectionne **Reprendre la protection de la configuration**.
- Une fois que la période de suspension spécifiée s'est écoulée, la stratégie de protection de la configuration est reprise automatiquement.

13.3 Reprise de la stratégie de protection de la configuration

Lorsque la période de suspension spécifiée s'est écoulée, la stratégie de protection de la configuration est reprise automatiquement. Pour reprendre manuellement la stratégie de protection de la configuration avant l'écoulement de la période spécifiée :

1. Sur l'ordinateur d'extrémité, cliquez avec le bouton droit de la souris sur l'icône de la barre d'état système et sélectionnez **Reprendre la protection de la configuration**.
2. Pour confirmer, cliquez sur **Oui**.

La protection de la configuration est reprise.

14 SafeGuard Enterprise et BitLocker Drive Encryption

BitLocker Drive Encryption est une fonction de chiffrement de disque complet avec authentification de préinitialisation incluse dans les systèmes d'exploitation Windows Vista et Windows 7 de Microsoft. Elle est conçue pour protéger les données en permettant un chiffrement du volume d'initialisation.

14.1 Stratégies de chiffrement de BitLocker

Le responsable de la sécurité peut créer une stratégie de chiffrement (initial) dans le SafeGuard Management Center et la distribuer aux ordinateurs d'extrémité BitLocker lors de l'exécution.

Les clients BitLocker étant gérés de manière transparente dans le SafeGuard Management Center, le responsable de la sécurité n'a pas besoin de spécifier des paramètres BitLocker spécifiques pour le chiffrement. SafeGuard Enterprise détecte l'état des clients et sélectionne le chiffrement BitLocker approprié. Lorsqu'un client BitLocker est installé avec SafeGuard Enterprise et que le chiffrement basé sur volume est activé, les volumes sont chiffrés par BitLocker.

14.2 Chiffrement initial sur l'ordinateur protégé par BitLocker

Lorsque la stratégie de chiffrement est envoyée à l'ordinateur protégé par BitLocker, et avant que ce dernier ne démarre le chiffrement initial, les clés de chiffrement sont générées par BitLocker. Vous devez préciser l'emplacement de stockage de la clé de chiffrement BitLocker. Une sauvegarde de cette clé est également stockée dans la base de données de SafeGuard Enterprise à des fins de récupération.

Lorsque SafeGuard Enterprise est installé sur votre ordinateur, l'icône du produit SafeGuard Enterprise s'affiche dans la barre d'état système de la barre des tâches de l'ordinateur. Vous pouvez accéder de manière centralisée aux fonctions importantes de SafeGuard Enterprise sur votre ordinateur. Notez que les fonctions disponibles dépendent des paramètres définis dans le SafeGuard Management Center. Le responsable de la sécurité définit ces paramètres de manière centralisée dans le SafeGuard Management Center et les distribue aux ordinateurs d'extrémité.



Remarque :

Si un disque dur chiffré BitLocker sur un ordinateur est remplacé par un nouveau disque dur chiffré BitLocker et que celui-ci prend la même lettre de lecteur que le précédent, SafeGuard Enterprise n'enregistre que la clé de récupération du nouveau disque.

Si un volume est déjà chiffré avec BitLocker avant l'installation de la prise en charge par BitLocker de SafeGuard Enterprise, sauvegardez les clés du volume précédemment chiffré à l'aide des mécanismes de sauvegarde proposés par Microsoft.

14.3 Déchiffrement avec BitLocker

Les ordinateurs chiffrés avec BitLocker ne peuvent pas être déchiffrés automatiquement. Le déchiffrement doit être exécuté à l'aide de l'outil Microsoft «Manage-bde».

14.4 Authentification avec BitLocker

BitLocker propose toute une gamme d'options d'authentification. Les utilisateurs BitLocker peuvent s'authentifier via un TPM (Trusted Platform Module) ou une clé USB ou une combinaison des deux.

Le responsable de la sécurité peut définir les différents modes de connexion dans une stratégie depuis le SafeGuard Management Center et la distribuer aux ordinateurs d'extrémité BitLocker.

Les modes de connexion suivants sont proposés aux utilisateurs SafeGuard Enterprise BitLocker:

- TPM uniquement
- TPM + PIN
- TPM + clé USB

- Carte mémoire USB uniquement (sans TPM)

TPM (Trusted Platform module)

TPM est un module semblable à une carte à puce sur la carte mère qui exécute des fonctions cryptographiques et des opérations de signature numérique. Il permet de créer, stocker et gérer des clés utilisateur. Il est protégé contre les attaques.

Clé USB

Les clés externes peuvent être stockées sur une clé USB non protégée.

Authentification au niveau de l'ordinateur BitLocker

Pendant la préinitialisation de l'ordinateur BitLocker, saisissez le code PIN TPM ou insérez une clé USB pour l'authentification.

15 SafeGuard Enterprise et disques durs compatibles Opal à chiffrement automatique

Les disques durs à chiffrement automatique offrent un chiffrement de type matériel des données lorsqu'ils sont écrits sur le disque dur. Le Trusted Computing Group (TCG) a publié la norme Opal indépendante des fournisseurs pour les disques durs à chiffrement automatique. Différents fournisseurs de matériels proposent des disques durs compatibles Opal. SafeGuard Enterprise supporte le standard Opal et permet la gestion des ordinateurs d'extrémité avec disques durs compatibles Opal à chiffrement automatique.

15.1 Chiffrement de disques durs compatibles Opal

Les disques durs compatibles Opal sont à chiffrement automatique. Les données sont chiffrées automatiquement lorsqu'elles sont écrites sur le disque dur.

Les disques durs compatibles Opal sont verrouillés par une clé AES 256 utilisée comme mot de passe Opal. Ce mot de passe est géré par SafeGuard Enterprise via une stratégie de chiffrement. Votre responsable de la sécurité définit cette stratégie de chiffrement dans le SafeGuard Management Center et la distribue à votre ordinateur.

15.2 Extensions des icônes de la barre d'état et de l'Explorateur sur les ordinateurs d'extrémité avec disques durs compatibles Opal

Lorsque SafeGuard Enterprise est installé sur votre ordinateur, l'icône du produit SafeGuard Enterprise s'affiche dans la barre d'état système de la barre des tâches de l'ordinateur. Vous pouvez accéder de manière centralisée aux fonctions importantes de SafeGuard Enterprise sur votre ordinateur. Notez que les fonctions disponibles dépendent des paramètres définis dans SafeGuard Management Center. Le responsable de la sécurité définit ces paramètres de manière centralisée dans le SafeGuard Management Center et les distribue aux ordinateurs d'extrémité.

Si le responsable de la sécurité vous a autorisé via une stratégie à déchiffrer les disques durs compatibles Opal, la commande **Déchiffrer** de SafeGuard Enterprise est disponible dans le menu contextuel de l'Explorateur Windows.

16 SafeGuard Enterprise et Lenovo Rescue and Recovery

Pour plus d'informations sur les versions de Lenovo Rescue and Recovery (RnR) prises en charge par SafeGuard Enterprise, consultez

<http://www.sophos.fr/support/knowledgebase/article/108383.html>

Vous pouvez restaurer des sauvegardes de système d'exploitation complètes sur une partition chiffrée sans déchiffrer préalablement le disque dur. Ceci permet de gagner du temps lors d'une récupération après sinistre. SafeGuard Enterprise a été certifié officiellement par Lenovo pour cette fonctionnalité.

La principale fonction de Lenovo Rescue and Recovery vise à restaurer des données sur simple pression d'une touche. Même si le système d'exploitation principal est endommagé et ne démarre plus, Rescue and Recovery permet d'enregistrer des données par le biais d'un environnement d'urgence (WinPE). Vous pouvez accéder aux outils de sauvetage à partir du 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.

16.1 Présentation

SafeGuard Enterprise 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 la touche bleue "Entrée" sur les claviers de PC Lenovo.

Cette fonctionnalité intégrée vous permet de combiner cette méthode de sauvegarde et de récupération fiable avec des partitions de système d'exploitation chiffrées avec SafeGuard Enterprise. Les sauvegardes de systèmes SafeGuard Enterprise chiffrés 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.

SafeGuard Enterprise 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 n'avez pas besoin de recommencer le chiffrement.

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

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

16.2 Configuration minimale

- BIOS le plus récent pour PC/portable.

- Pour plus d'informations sur la compatibilité des versions Rescue and Recovery avec des versions SafeGuard Enterprise, consultez :
<http://www.sophos.fr/support/knowledgebase/article/108383.html>
- Lenovo Rescue and Recovery peut être utilisé pour récupérer des volumes chiffrés SafeGuard Enterprise. 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.

16.3 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: » (partition principale du disque dur principal) de l'ordinateur.

Les sections suivantes abordent en détails la procédure d'installation de Rescue and Recovery et de SafeGuard Enterprise. Nous vous recommandons d'installer Lenovo Rescue and Recovery avant d'installer SafeGuard Enterprise.

16.3.1 Installation de Rescue and Recovery et de SafeGuard Enterprise

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 SafeGuard Enterprise Device Encryption (SGNClient.msi).

SafeGuard Enterprise vérifie si Rescue and Recovery est installé et ajoute ses propres fichiers et configurations 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.

Activez l'authentification au démarrage lors de l'installation de SafeGuard Enterprise.

16.3.2 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 SafeGuard Enterprise Device Encryption (SGNClient.msi).

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

16.4 Mise à niveau

La mise à niveau suppose que SafeGuard Enterprise et Rescue and Recovery sont installés et que vous souhaitez en mettre au moins un des deux à niveau vers une nouvelle version.

Mise à niveau de SafeGuard Enterprise

Si vous mettez à niveau SafeGuard Enterprise, le système tout entier est mis à jour et aucune autre configuration n'est donc nécessaire.

16.5 Désinstallation

Lors de la désinstallation des produits du logiciel :

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

16.6 Environnement de démarrage et options de récupération

SafeGuard Enterprise 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 SafeGuard Enterprise 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 : safeguard Enterprise ne vous permet pas de démarrer dans l'environnement Rescue and Recovery lors d'un démarrage effectué 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 lancé directement à partir du BIOS, le système d'exploitation sera récupéré. SafeGuard Enterprise sera supprimé pendant le processus de restauration. Pour sécuriser de nouveau le système, SafeGuard Enterprise doit être réinstallé.

16.7 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 sur lesquels SafeGuard Enterprise sera 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.

SafeGuard Enterprise prend uniquement en charge l'enregistrement des sauvegardes sur :

- le disque dur local ;
- un disque dur secondaire ;
- un disque dur USB ;
- le réseau ;
- une clé USB ;
- un 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.

16.8 Restauration de sauvegardes de fichiers

Rescue and Recovery permet de restaurer des fichiers ou dossiers à partir de sauvegardes dans lesquelles SafeGuard Enterprise est installé. Démarrez simplement Windows, puis Rescue and Recovery, et restaurez les fichiers sélectionnés. Vous n'avez pas besoin de redémarrer votre machine une fois la restauration terminée : vous pouvez travailler sur vos fichiers immédiatement.

16.9 Restauration du système SafeGuard Enterprise

Pour restaurer une sauvegarde système qui inclut SafeGuard Enterprise, 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) Saisissez les codes d'accès SafeGuard Enterprise.
2. Si vous n'utilisez pas un ordinateur Lenovo :
 - a) Connectez-vous à la POA à l'aide de vos codes d'accès SafeGuard Enterprise.
 - b) Au démarrage 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 **Restauration à partir d'une sauvegarde**.
Une boîte de dialogue s'affiche dans laquelle vous pouvez sélectionner la sauvegarde.
5. Sélectionnez la sauvegarde et restaurez-la.

16.10 Partitions de récupération de service et d'usine

Lenovo dote ses nouveaux ordinateurs de partitions préinstallées spécifiques :

- **Partition de service Lenovo** : contient l'environnement de démarrage de 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 SafeGuard Enterprise. Pour plus d'informations, reportez-vous à la documentation Lenovo.

16.11 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 empêcher 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.

17 Support technique

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

- Visitez le forum SophosTalk à l'adresse <http://community.sophos.com/> et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Visitez la base de connaissances du support de Sophos à l'adresse <http://www.sophos.fr/support/>
- Téléchargez la documentation des produits à l'adresse <http://www.sophos.fr/support/docs/>
- Envoyez un courriel à support@sophos.fr, y compris le ou les numéros de version(s) du logiciel Sophos, le ou les systèmes d'exploitation et le ou les niveaux de correctif ainsi que le texte de tout message d'erreur.

18 Mentions légales

Copyright © 1996 - 2011 Sophos Group. Tous droits réservés. SafeGuard est une marque déposée de Sophos Group.

Sophos est une marque déposée de Sophos Limited, Sophos Group et Utimaco Safeware AG, selon le cas. Tous les autres noms de produits et de sociétés mentionnés sont des marques ou des marques déposées de leurs propriétaires respectifs.

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

Les informations de copyright des fournisseurs tiers sont disponibles dans le fichier appelé Disclaimer and Copyright for 3rd Party Software.rtf dans votre répertoire des produits.