SOPHOS
Security made simple.

SafeGuard Enterprise
Manuel d'utilisation

Version du produit : 7
Date du document : décembre 2014

Table des matières

1 À propos de SafeGuard Enterprise 7.0

Cette version de SafeGuard Enterprise prend en charge Windows 7 et Windows 8 fonctionnant sur des ordinateurs d'extrémité dotés de BIOS ou d'UEFI.

- Pour les plates-formes BIOS, les administrateurs peuvent choisir entre le chiffrement intégral du disque SafeGuard Enterprise et le chiffrement BitLocker géré par SafeGuard. La version BIOS est livrée avec le mécanisme de récupération BitLocker.

  Remarque : si l'authentification au démarrage SafeGuard ou le chiffrement intégral du disque SafeGuard sont mentionnés dans le présent manuel, il font uniquement référence aux ordinateurs d'extrémité Windows 7 avec BIOS.

- Pour les plates-formes UEFI, SafeGuard Enterprise gère le composant BitLocker de chiffrement du disque. Pour ces ordinateurs d'extrémité, SafeGuard Enterprise offre des fonctionnalités améliorées de Challenge/Réponse. Retrouvez plus de renseignements sur les versions UEFI prises en charge et sur les limites de la prise en charge du Challenge/Réponse SafeGuard BitLocker dans les Notes de publication disponibles sur http://downloads.sophos.com/readmes/readsgn_7_fra.html.

Remarque : la mention UEFI apparaît de manière explicite à chaque fois qu'elle doit être utilisée.

Le tableau ci-dessous indique quels composants sont disponibles.

	Chiffrement intégral du disque SafeGuard avec authentification au démarrage SafeGuard	BitLocker avec authentification préalable au démarrage par SafeGuard	Récupération C/R SafeGuard pour l'authentification préalable au démarrage BitLocker
Windows 7 BIOS	**OUI**	**OUI**	
Windows 7 UEFI		**OUI**	**OUI**
Windows 8 BIOS		**OUI**	
Windows 8 UEFI		**OUI**	**OUI**
Windows 8.1 BIOS		**OUI**	
Windows 8.1 UEFI		**OUI**	**OUI**

Remarque : la **Récupération C/R SafeGuard pour l'authentification préalable au démarrage BitLocker** est uniquement disponible sur les systèmes 64 bits.

Le **Chiffrement intégral du disque SafeGuard avec authentification au démarrage SafeGuard** est le module Sophos permettant de chiffrer les volumes sur les ordinateurs d'extrémité. Il est livré avec l'authentification préalable au démarrage Sophos nommée authentification au démarrage SafeGuard qui prend en charge les options de connexion par

cartes à puce, par empreinte digitale et qui offre un mécanisme Challenge/Réponse pour la récupération.

L'**authentification préalable au démarrage BitLocker gérée par SafeGuard** est le composant qui active et gère le moteur de chiffrement BitLocker et l'authentification préalable au démarrage BitLocker.

Elle est disponible sur les plates-formes BIOS et UEFI :

- La version UEFI propose également un mécanisme Challenge/Réponse SafeGuard pour la récupération de BitLocker lorsque l'utilisateur oublie son code confidentiel. La version UEFI peut être utilisée si la plate-forme répond à certaines conditions préalables requises. Par exemple, la version UEFI doit être 2.3.1. Retrouvez plus de renseignements dans les Notes de publication.
- La version BIOS ne propose pas toutes les fonctions de récupération offertes par le mécanisme Challenge / Réponse SafeGuard. Elle sert d'option de secours lorsque les conditions requises à l'utilisation de la version UEFI ne sont pas remplies. Le programme d'installation Sophos vérifie si les conditions requises sont remplies et en cas contraire, il installe automatiquement la version BitLocker sans Challenge/Réponse.

Ordinateurs d'extrémité Mac

Les produits mentionnés ci-dessous sont disponibles pour les ordinateurs d'extrémité Mac. Ils sont également gérés par SafeGuard Enterprise ou communiquent leur rapport d'état à la console d'administration Management Center.

	Sophos SafeGuard File Encryption 7.0	Sophos SafeGuard Native Device Encryption (gestion FileVault 2) 7.0
OS X 10.8	**OUI**	**OUI**
OS X 10.9	**OUI**	**OUI**
OS X 10.10	**OUI**	**OUI**

Ce manuel fait uniquement référence à la plate-forme Windows. Retrouvez plus d'informations sur les versions Mac dans la documentation produit respective.

Sophos Mobile Encryption

Sophos Mobile Encryption vous permet de lire les fichiers chiffrés par les modules **SafeGuard Cloud Storage** ou **SafeGuard Data Exchange** de SafeGuard Enterprise. Vous avez la possibilité de chiffrer les fichiers à l'aide d'une clé locale. Ces clés locales sont générées par une phrase secrète saisie par l'utilisateur. Vous pouvez uniquement déchiffrer un fichier lorsque vous connaissez la phrase secrète utilisée pour chiffrer le fichier. Retrouvez plus de renseignement à propos de Sophos Mobile Encryption sur www.sophos.com.

2 SafeGuard Enterprise sur les ordinateurs d'extrémité Windows

SafeGuard Enterprise est une solution de sécurité modulaire qui renforce la sécurité des ordinateurs d'extrémité 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 SafeGuard Management Center.

Les fonctions de protection principales 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

- **Chiffrement intégral du disque SafeGuard**
  - **Authentification au démarrage SafeGuard**

    La connexion se fait immédiatement après la mise sous tension de l'ordinateur. Une fois l'authentification au démarrage SafeGuard réussie, vous êtes connecté automatiquement au système d'exploitation. Vous pouvez également désactiver l'authentification au démarrage SafeGuard. Dans ce cas, l'authentification est effectuée par le système d'exploitation.

  - **Chiffrement de volumes**

    Toutes les données des volumes (y compris les fichiers de démarrage, les fichiers d'échange, les fichiers inactifs/de mise en veille prolongée, les fichiers temporaires, les informations de répertoire, etc.) sont chiffrées de manière transparente sans que l'utilisateur ait à modifier ses habitudes de travail ou tenir compte de problèmes de sécurité.

- **BitLocker avec authentification préalable au démarrage gérée par SafeGuard Enterprise**

  SafeGuard Enterprise gère le moteur de chiffrement Microsoft BitLocker. Sur les plates-formes UEFI, l'authentification préalable au démarrage BitLocker s'effectue à l'aide d'un mécanisme de Challenge / Réponse SafeGuard tandis que la version BIOS permet de récupérer la clé de récupération à partir de Management Center.

- **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 de stockage inscriptibles amovibles, notamment les disques durs externes et les cartes mémoire USB, sont chiffrés de manière transparente.

- **SafeGuard File Encryption**
  - SafeGuard File Encryption permet un chiffrement basé sur fichier, surtout pour les groupes de travail afin de stocker en lieu sûr les données sur les partages réseau.

- Les fichiers dans les emplacements couverts par les stratégies File Encryption seront chiffrés instantanément et sans aucune intervention de l'utilisateur.

- **SafeGuard Cloud Storage**

  SafeGuard Cloud Storage offre un chiffrement basé sur fichier des données stockées dans le Cloud. Il s'assure que les copies locales des données du Cloud sont chiffrées de manière transparente et restent chiffrées une fois stockées dans le Cloud.

Remarque : il se peut que certaines des fonctions décrites dans ce manuel ne soient pas disponibles sur votre ordinateur. En effet, la disponibilité des fonctions dépend des stratégies définies par le responsable de la sécurité.

3 Bon usage en matière de sécurité

Les étapes simples mentionnées ci-dessous vous aident à maintenir la sécurité et la protection des données présentes sur votre ordinateur.

Éteignez complètement votre ordinateur ou mettez-le en mode Veille prolongée lorsqu'il n'est pas utilisé

Sur les ordinateurs protégés par SafeGuard Enterprise, il est possible que certains individus malintentionnés accèdent aux clés de chiffrement dans certains modes de veille. Tout particulièrement lorsque le système d'exploitation de l'ordinateur n'est pas correctement éteint et que les processus en tâche de fond ne sont pas terminés correctement. La protection est renforcée lorsque le système d'exploitation est complètement arrêté ou mis en veille prolongée.

Lorsque vous n'utilisez pas votre ordinateur ou que vous le laissez sans surveillance :

- Évitez le mode de mise en veille. Évitez la Veille mode hybride. La Veille mode hybride allie la mise en veille prolongée à la mise en veille.
- Ne vous contentez pas de verrouiller l'ordinateur et d'éteindre votre écran (ou de fermer l'écran de votre ordinateur portable) sans avoir complètement arrêté l'ordinateur ou l'avoir mis en veille prolongée. La demande d'un mot de passe supplémentaire après la reprise d'une session ne fournit pas une protection suffisante.
- Arrêtez plutôt l'ordinateur complètement ou mettez-le en veille prolongée.

  Remarque : il est important que le fichier de mise en veille prolongée soit sur le volume chiffré. Généralement, il se trouve sur C:\.

Suivez ces étapes tout particulièrement si vous utilisez un portable dans des lieux publics tel qu'un aéroport.

Lorsque l'ordinateur est en veille prolongée ou arrêté complètement, l'authentification au démarrage SafeGuard est toujours activée jusqu'à sa prochaine utilisation. Ainsi il est totalement protégé.

Assurez-vous qu'une lettre a été attribuée à tous les volumes.

Seuls les volumes auxquels une lettre a été attribuée sont chiffrés. Les volumes sans lettre sont susceptibles d'entraîner des fuites de données confidentielles en texte brut.

Pour écarter ce type de menace :

- Si vous découvrez un volumes auquel n'a pas été attribué une lettre sur votre ordinateur, contactez votre administrateur système.
- Ne changez pas les attributions de lettres au lecteur.

Choisissez des mots de passe forts.

Les mots de passe forts sont une partie fondamentale de la protection de vos données. Utilisez des mots de passe forts, surtout pour sécuriser la connexion à votre ordinateur.

Un mot de passe fort suit les règles suivantes :

- Il est assez long pour être sûr : il est conseillé d'utiliser au moins 10 caractères.
- Il contient une combinaison de lettres (majuscules et minuscules) ainsi que des caractères spéciaux ou des symboles.
- Il ne contient pas de mot ou de nom fréquemment utilisé.
- Il est difficile à deviner mais vous devez être en mesure de vous en rappeler facilement et de le saisir correctement.

Changez vos mots de passe à intervalles réguliers. Ne les confiez à personne et ne laissez aucune trace écrite de ces codes d'accès.

4 Authentification au démarrage SafeGuard

L'authentification au démarrage (POA, Power-on Authentication) SafeGuard 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 est sorti du mode veille prolongée.

Apparence de l'authentification au démarrage SafeGuard

L'apparence de l'authentification au démarrage SafeGuard peut être personnalisée en fonction des besoins de votre entreprise. Le responsable de la sécurité procède aux réglages appropriés via les paramètres de stratégie dans 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 SafeGuard est exclusive à SafeGuard. Cet écran peut être personnalisé via une stratégie afin d'afficher le logo de votre entreprise par exemple.

- **Texte des boîtes de dialogue**

  Le texte de l'authentification au démarrage SafeGuard s'affiche dans la langue par défaut définie dans les Options régionales et linguistiques Windows. Vous pouvez changer la langue utilisée dans l'authentification au démarrage en modifiant la langue définie par défaut. La langue du texte de la boîte de dialogue peut être spécifiée par le responsable de la sécurité dans une stratégie.

4.1 Première connexion après l'installation de SafeGuard Enterprise

Si SafeGuard Enterprise a été installé avec l'authentification au démarrage SafeGuard , 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 :

SafeGuard Enterprise utilise une connexion basée sur certificat. 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 codes d'accès. Vous êtes ensuite enregistré en tant qu'utilisateur SafeGuard Enterprise. Ce processus d'enregistrement est nécessaire pour vérifier que vos codes d'accès seront reconnues dans l'authentification au démarrage SafeGuard au prochain démarrage du système.

Une infobulle apparaît pour vous informer du succès de l'enregistrement et de la réception de toutes les données requises.

Lorsque vous redémarrez l'ordinateur, l'authentification au démarrage SafeGuard est activée. Saisissez alors vos codes d'accès Windows à partir de l'authentification au démarrage SafeGuard. 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 SafeGuard 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 SafeGuard a été installée et activée sur votre ordinateur.

4.1.1 Connexion automatique de SafeGuard

1. L'ordinateur d'extrémité démarre et la boîte de dialogue de Connexion automatique SafeGuard apparaît.
   - Un utilisateur automatique SafeGuard est connecté.
   - 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.

4.1.2 Connexion Windows

1. La boîte de dialogue de connexion de Windows s'affiche.
2. SafeGuard Enterprise offre la possibilité d'utiliser la méthode d'authentification SafeGuard Enterprise et Windows. Windows 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 SafeGuard Enterprise **Autre utilisateur** qui se trouve en-dessous.

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 sont disponibles dans l'authentification au démarrage SafeGuard dès que toutes les données ont été synchronisées entre le serveur SafeGuard Enterprise et votre ordinateur.

   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 SafeGuard pour être connecté automatiquement.

Redémarrez l'ordinateur pour activer toutes les fonctionnalités de l'authentification au démarrage SafeGuard. Suite au redémarrage, l'authentification au démarrage SafeGuard assurera la protection de votre ordinateur contre tout accès non autorisé.

4.1.3 Connexion à l'authentification au démarrage SafeGuard après redémarrage

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

   Les certificats et les clés sont disponibles et vous pouvez vous connecter à l'authentification au démarrage SafeGuard 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 codes d'accès.

   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.

4.2 Connexion à l'authentification au démarrage SafeGuard

Après activation de l'authentification au démarrage SafeGuard (synchronisation initiale et redémarrage), vous pouvez vous connecter en saisissant vos codes d'accès utilisateur Windows dans la boîte de dialogue de connexion de l'authentification au démarrage SafeGuard. 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 **Authentification 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 SafeGuard sur l'ordinateur. Retrouvez plus d'informations à la section Enregistrement d'utilisateurs SafeGuard Enterprise supplémentaires à la page 14. 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 une tentative ratée de connexion

En cas d'échec de connexion lors de l'authentification au démarrage SafeGuard, 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 augmente à chaque échec de tentative de connexion. Les tentatives ratées de connexion sont consignées dans le journal.

Verrouillage de la machine

Après un nombre défini de tentatives échouées de connexion, votre ordinateur sera verrouillé. Pour déverrouiller votre ordinateur, lancez une procédure Challenge/Réponse. Retrouvez plus d'informations à la section Récupération avec le Challenge/Réponse ou la clé de récupération à la page 76.

4.2.1 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. Retrouvez plus d'informations à la section Options de récupération à la page 65.

4.3 Enregistrement d'utilisateurs SafeGuard Enterprise supplémentaires

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 SafeGuard s'affiche. Le second utilisateur Windows ne peut pas se connecter à partir de l'authentification au démarrage SafeGuard car il ne dispose pas des clés et certificats nécessaires.

2. Pour que le second utilisateur puisse se connecter à l'authentification au démarrage SafeGuard, le propriétaire de l'ordinateur doit lui donner l'autorisation.

   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 SafeGuard, cliquez sur **Options** et dessélectionnez la case à cocher **Connexion automatique vers Windows**. Connectez-vous à l'aide de vos codes d'accès en tant que propriétaire de l'ordinateur.

   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 SafeGuard Enterprise.

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

Remarque : les responsables de la sécurité peuvent attribuer des utilisateurs à l'authentification au démarrage SafeGuard sur une nouvelle machine dans SafeGuard Management Center. Les utilisateurs attribués de cette manière peuvent également se connecter à ces ordinateurs à l'authentification au démarrage SafeGuard.

4.4 Mot de passe temporaire de l'authentification au démarrage SafeGuard

SafeGuard Enterprise vous permet de changer temporairement le mot de passe dans l'authentification au démarrage SafeGuard. Le changement temporaire du mot de passe 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 l'authentification au démarrage SafeGuard. 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 de l'authentification au démarrage SafeGuard 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 à l'authentification au démarrage SafeGuard, 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 l'authentification au démarrage SafeGuard.

5. Cliquez sur **OK**.

Vous êtes connecté à Windows.

Pour vous connecter à l'authentification au démarrage SafeGuard, vous pouvez désormais utiliser uniquement le mot de passe temporaire. 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 à l'authentification au démarrage SafeGuard 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 SafeGuard 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 fermer la boîte de dialogue vous invitant à changer de mot de passe sans avoir à changer 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 SafeGuard 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 SafeGuard. Vous pouvez fermer cette boîte de dialogue sans la modifier et utiliser votre « ancien mot de passe » pour vous connecter. Vous pouvez changer le mot de passe ultérieurement.

4.5 Connexion à l'authentification au démarrage SafeGuard à l'aide de cartes à puce ou de tokens

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

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

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

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

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

4.5.1 Première connexion par token après installation

La première connexion par token est identique à la procédure de connexion sans token.

Si vous disposez d'un token, vous pouvez l'utiliser pour vous connecter à Windows en saisissant son code confidentiel.

Remarque : nous vous conseillons de configurer votre token avec vos codes d'accès d'utilisateur Windows avant de redémarrer l'ordinateur. Retrouvez plus d'informations à la section Stockage des codes d'accès de l'utilisateur Windows sur le token à la page 17. Les stratégies de sécurité qui s'appliquent peuvent nécessiter l'utilisation d'un token à l'authentification au démarrage SafeGuard. Si votre token ne contient pas vos codes d'accès, vous ne pouvez pas vous connecter à l'authentification au démarrage SafeGuard.

4.5.2 Connexion à l'authentification au démarrage SafeGuard avec un token

Conditions préalables : assurez-vous que le support USB est activé dans le BIOS. La prise en charge des tokens doit être initialisé et le token doit être généré.

1. Connectez le token.

2. Mettez l'ordinateur sous tension.

   La boîte de dialogue de connexion par token s'affiche.

   Remarque : si votre stratégie autorise la connexion avec vos codes d'accès et que vous déconnectez le token, vous serez invité à saisir vos codes d'accès de l'utilisateur pour la connexion. Si la boîte de dialogue de connexion avec un identifiant utilisateur et un mot de passe ne s'affiche pas, vous pouvez uniquement vous connecter avec un token à l'authentification au démarrage SafeGuard.

3. Saisissez le code confidentiel de votre token.

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

4.5.3 Changement de code confidentiel

Vous pouvez changer le code confidentiel de votre token dans la boîte de dialogue du journal Windows.

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

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

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

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

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

   Le code confidentiel du token est changé et la connexion Windows se poursuit.

4.5.4 Stockage des codes d'accès utilisateur Windows sur le token

Si votre token ne contient pas vos codes d'accès utilisateur Windows, vous pouvez les stocker dessus vous-même.

Remarque : nous vous conseillons de configurer votre token à la première connexion. Les stratégies de sécurité qui s'appliquent peuvent nécessiter l'utilisation d'un token à l'authentification au démarrage SafeGuard. Si votre token ne contient aucune information utilisateur, vous ne pouvez pas vous connecter à l'authentification au démarrage.

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

   Si le système détecte un token vide, il affiche automatiquement la boîte de dialogue **Génération d'un token**.

2. Saisissez votre nom d'utilisateur et votre mot de passe Windows.
3. Confirmez le mot de passe.

4. Sélectionnez ou saisissez le domaine et cliquez sur **OK**.

   Le système tente de vous connecter à Windows avec les données saisies. Si la connexion est réussie, les données sont inscrites sur le token.

   Vous êtes connecté à Windows.

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

Dans la boîte de dialogue d'authentification au démarrage SafeGuard, cliquez sur **Options** et dessélectionnez la case à cocher **Connexion automatique vers Windows**. La boîte de dialogue de connexion Windows s'affiche et vous pouvez stocker vos codes d'accès sur le token conformément aux instructions.

4.5.5 Récupération de la connexion par token

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 avec Local Self Help à la page 66.
- Récupération avec le Challenge/Réponse ou la clé de récupération à la page 76.

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 token.

Remarque : ces méthodes de récupération ne sont pas disponibles pour les tokens cryptographiques. Si des problèmes de connexion surviennent, veuillez contacter votre responsable de la sécurité.

4.5.6 Déblocage des tokens

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

Le responsable de la sécurité doit vous fournir le code confidentiel de l'administrateur défini pour votre token.

1. Dans la boîte de dialogue **Débloquer le token**, saisissez le mot de passe existant.
2. Saisissez un nouveau code confidentiel et confirmez-le.

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

3. Cliquez sur **OK**.

Le token est débloqué 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. Toutefois, vous ne pouvez pas changer le code confidentiel ou vos codes d'accès via Challenge/Réponse.

4.5.7 Tokens cryptographiques - Kerberos

Si vous utilisez un token, vous êtes identifié à l'authentification au démarrage SafeGuard par le certificat stocké sur le token.

Pour ce type de connexion, un token généré dans son intégralité est requise. Le responsable de la sécurité ou toute autre personne autorisée doit vous fournir ce token. Pour vous connecter au système, il vous suffit de saisir le code confidentiel du token. Si ce type de connexion est le seul type valide pour votre ordinateur, vous ne pouvez pas vous connecter sans token.

Remarque : lors de l'utilisation d'un token 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, veuillez contacter votre responsable de la sécurité.

4.5.8 Changement du certificat pour la connexion par token

Pour changer ou renouveler le certificat utilisé pour les connexions par token, votre responsable de la sécurité doit attribuer un nouveau certificat à votre ordinateur. Après synchronisation entre votre ordinateur et le serveur SafeGuard Enterprise, la boîte de dialogue d'état avec l'icône SafeGuard Enterprise de la barre d'état système indique que votre ordinateur est **Prêt pour la modification du certificat**.

Le responsable de la sécurité vous fournit un nouveau token.

Pour modifier le certificat de votre ordinateur :

1. Connectez-vous à l'authentification au démarrage SafeGuard avec votre ancienne méthode d'authentification (token ou nom d'utilisateur/mot de passe) sans la connexion automatique à Windows.

   Cliquez sur **Options** et dessélectionnez la case à cocher **Connexion automatique vers Windows** ou déconnectez-vous de nouveau après exécution de la connexion automatique à Windows.

2. Connectez-vous à Windows avec votre nouveau token.

Le nouveau token est valide pour la connexion à l'authentification au démarrage SafeGuard. L'ancien token n'est plus valide pour la connexion.

4.6 Connexion automatique à l'authentification au démarrage SafeGuard à l'aide d'un token

Conditions préalables :

- la prise en charge USB est activée dans le BIOS.
- La prise en charge des tokens est initialisée et le token est généré.
- Le responsable de la sécurité a affecté la stratégie appropriée à votre ordinateur.

Si une stratégie avec un code confidentiel défini a été attribuée à votre ordinateur, vous pouvez vous connecter automatiquement à l’authentification au démarrage SafeGuard à l’aide d’un token. Vous n'avez pas besoin de saisir vos codes d'accès ou votre code confidentiel. En effet, vous êtes authentifié automatiquement à l'authentification au démarrage SafeGuard. Selon les paramètres de votre stratégie, vous êtes également authentifié automatiquement à la connexion à Windows.

Pour vous connecter automatiquement à l'authentification au démarrage avec un token :

1. Connectez le token.
2. Mettez l'ordinateur sous tension.

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

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

4.7 Clavier virtuel

Lors de l'authentification au démarrage SafeGuard, vous pouvez afficher/masquer un clavier virtuel et cliquer sur les touches à l'écran pour entrer les codes d'accès, 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 SafeGuard, 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 du clavier. Il est également possible de changer la disposition du clavier à l'aide des mêmes options que celles utilisées pour changer la disposition du clavier de l'authentification au démarrage SafeGuard. Retrouvez plus d'informations à la section Modification de la disposition du clavier à la page 20.

4.8 Disposition du clavier

Chaque pays ou presque a une disposition de clavier qui lui est propre. La disposition du clavier est très importante pour l'authentification au démarrage SafeGuard 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 SafeGuard (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).

4.8.1 Modification de la disposition du clavier

La disposition du clavier pour l'authentification au démarrage SafeGuard (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 SafeGuard reconnaît la disposition du clavier utilisée au cours de la dernière connexion et l'active automatiquement à la connexion suivante. Deux redémarrages sont requis. Si la disposition du clavier précédente est dessélectionnée 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, redémarrez votre ordinateur deux fois de sorte que la nouvelle disposition du clavier puisse être lue par l'authentification au démarrage SafeGuard et que l'authentification au démarrage puisse définir la nouvelle disposition.

Vous pouvez changer la disposition du clavier requise pour l'authentification au démarrage SafeGuard 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`**.

4.9 Raccourcis clavier/touches de fonction pris en charge dans l'authentification au démarrage SafeGuard

Certains paramètres et fonctionnalités du matériel peuvent générer des problèmes lors du démarrage des ordinateurs et provoquer le blocage du système. L'authentification au démarrage SafeGuard 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 causer ces 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 SafeGuard 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 : http://www.sophos.com/fr-fr/support/knowledgebase/65700.aspx.

Vous pouvez personnaliser ce fichier pour qu'il reflète le 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 SafeGuard n'a été défini ou trouvé.

Pour installer le fichier de configuration de l'authentification au démarrage SafeGuard, saisissez la commande suivante :

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

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

4.9.1 Raccourcis clavier

Maj-F3 = support hérité USB (activé/désactivé)

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)

Tableau de dépendance des raccourcis clavier

Maj - F3	Maj - F5	Maj - F7	Hérité	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 SafeGuard. 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 prise en charge du token USB.

2. Si aucun support USB n'est actif, l'authentification au démarrage SafeGuard tente d'utiliser BIOS SMM au lieu de sauvegarder et de restaurer le contrôleur USB. Le mode hérité peut fonctionner dans ce scénario.
3. Le support hérité est actif, USB est actif. L'authentification au démarrage SafeGuard 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 SafeGuard, 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 une boîte de dialogue d'authentification au démarrage SafeGuard, vous pouvez afficher une boîte de dialogue montrant la configuration par raccourcis clavier utilisée pour démarrer l'authentification au démarrage. 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 SafeGuard 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**.

Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/107785.aspx.

4.9.2 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 SafeGuard.

F8 = change le mot de passe de l'authentification au démarrage SafeGuard. Utilisez-la à la place de la touche **Entrée** pour déclencher un changement de mot de passe dans l'authentification au démarrage SafeGuard 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'authentification au démarrage SafeGuard pour l'arrêt

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 d'authentification au démarrage SafeGuard et vous connecter à l'aide d'un nom d'utilisateur et d'un mot de passe. Retrouvez plus d'informations à la section Connexion avec le lecteur d'empreintes digitales Lenovo à la page 25.

4.10 Synchronisation du mot de passe

SafeGuard Enterprise détecte automatiquement le moment auquel 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 les deux situations suivantes :

- Pendant la procédure de connexion.
- Pendant une procédure de verrouillage/déverrouillage de Windows.

5 Connexion à Windows

SafeGuard Enterprise propose une méthode d'authentification supplémentaire.

Si vous dessélectionnez la case à cocher **Connexion automatique vers Windows** dans la boîte de dialogue de connexion de l'authentification au démarrage SafeGuard, la boîte de dialogue de connexion Windows 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.

5.1 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 SafeGuard. Si vous dessélectionnez la case **Connexion automatique vers Windows** dans la boîte de dialogue de connexion de l'authentification au démarrage SafeGuard et que vous utilisez la méthode SafeGuard Enterprise pour vous connecter à Windows, toutes les fonctionnalités de SafeGuard Enterprise seront disponibles suite à votre connexion à Windows.

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

5.2 Connexion avec la méthode d'authentification de Windows

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

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

Suite à la connexion à Windows, l'application d'authentification SafeGuard Enterprise démarre automatiquement, si nécessaire, pour vous faire bénéficier de toutes les fonctionnalités de SafeGuard Enterprise.

Selon les paramètres de connexion de l'administration centralisée, une boîte de dialogue permettant de saisir les codes d'accès ou le code confidentiel s'affiche.

1. Saisissez vos codes d'accès ou le code confidentiel 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.

6 Connexion avec le lecteur d'empreintes digitales Lenovo

Remarque : la connexion au lecteur d'empreintes digitales Lenovo est uniquement prise en charge sur les ordinateurs d'extrémité Windows 7 (BIOS).

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 un token.

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 lors de l'authentification au démarrage SafeGuard et 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 token et par empreinte digitale sur le même ordinateur.
- La connexion à distance par empreinte digitale n'est pas prise en charge.

6.1 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
- La dernière version de BIOS (conseillé)
- 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 système requise

- Windows 7, 32 bits, 64 bits
- Windows 8, 32 bits, 64 bits

Matériel pris en charge

Retrouvez plus d'informations sur les matériels de connexion par empreinte digitale pris en charge dans l'article http://www.sophos.com/fr-fr/support/knowledgebase/108789.aspx.

Logiciels pris en charge

Retrouvez plus d'informations sur les logiciels d'empreinte digitale pris en charge dans l'article http://www.sophos.com/fr-fr/support/knowledgebase/111626.aspx.

6.2 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 l'authentification au démarrage SafeGuard 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 codes d'accès 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 **POA password in BIOS**. (UPEK uniquement. Cette étape n'est pas nécessaire pour AuthenTec).
   c) Pour utiliser la connexion par empreinte digitale à partir de l'authentification au démarrage SafeGuard, veuillez d'abord vous connecter, une première fois, à Windows à l'aide de votre empreinte digitale afin de transférer vos codes d'accès 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.

6.3 Connexion par empreinte digitale à l'authentification au démarrage SafeGuard

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 SafeGuard s'affiche.

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

   Si le logiciel reconnaît votre empreinte digitale, l'authentification au démarrage SafeGuard 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. Retrouvez plus d'informations à la section Icônes utilisées lors du processus de connexion à la page 27.

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 recherche dans l'authentification au démarrage SafeGuard une correspondance avec les empreintes digitales enregistrées.

  Cependant, aucun code d'accès ne sera 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 codes d'accès sont transférés 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 d'authentification au démarrage SafeGuard de connexion par nom d'utilisateur et mot de passe. Retrouvez plus d'informations à la section Connexion avec un nom d'utilisateur et un mot de passe à la page 30.

6.3.1 Icônes utilisées dans le processus de connexion

Lors de votre connexion à l'authentification au démarrage SafeGuard par empreinte digitale, le système communique les demandes, notifications et avertissements sous forme d'icônes. Ces icônes s'affichent pendant la procédure de connexion, accompagnées d'un court message.

	Vous demande de glisser votre doigt sur le lecteur d'empreintes digitales.
	Indique que la connexion par empreinte digitale n'est actuellement pas activée. Ce peut être le cas, par exemple, si le module de connexion par empreinte digitale n'a pas encore été initialisé.
	Indique que le lecteur d'empreintes digitales fonctionne et qu'il est occupé.
	Indique que le lecteur d'empreintes digitales a lu l'empreinte avec succès et trouvé une correspondance.
	Indique que le lecteur d'empreintes digitales a lu l'empreinte avec succès mais sans trouver de correspondance.
	Indique que le lecteur d'empreintes digitales n'est pas parvenu à lire l'empreinte. Faites glisser une nouvelle fois votre doigt sur le lecteur d'empreintes digitales.
	Indique que votre doigt est trop excentré sur la gauche (ou trop excentré sur la droite). Placez le doigt au centre du lecteur d'empreintes digitales.

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

6.3.2 Échecs de tentatives de connexion

Si le système ne parvient pas à lire votre empreinte digitale après cinq tentatives, il considère que la tentative de connexion a échoué et consigne le problème dans le journal des événements. Dans ce cas, un délai de connexion se produit.

Si le système est parvenu à lire votre 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 dans le journal des événements. Dans ce cas, un délai de connexion se produit également.

Le délai de connexion augmente à chaque échec de tentative de connexion.

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

Même si la connexion par empreinte digitales est activée, vous pouvez toujours vous connecter à l'authentification au démarrage SafeGuard à l'aide de votre nom d'utilisateur et de votre mot de passe si, par exemple, voter lecteur d'empreinte digitale ne fonctionne pas.

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 SafeGuard de connexion par empreinte digitale.

   La boîte de dialogue de l'authentification au démarrage SafeGuard 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 de l'authentification au démarrage SafeGuard 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 de l'authentification au démarrage SafeGuard de connexion par 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 dans la boîte de dialogue d'authentification au démarrage SafeGuard de connexion par empreinte digitale.

   Si vous avez appuyé sur **Echap** pour ouvrir la boîte de dialogue d'authentification au démarrage SafeGuard pour la connexion par nom d'utilisateur et 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 d'authentification au démarrage SafeGuard de connexion par empreinte digitale.

6.4 Modification du mot de passe

1. Si une connexion par empreinte digitale est activée dans l'authentification au démarrage SafeGuard, 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.

6.4.1 Synchronisation de votre 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 SafeGuard de connexion par empreinte digitale.

   La boîte de dialogue de l'authentification au démarrage SafeGuard de connexion par nom d'utilisateur et mot de passe s'affiche.

3. Cliquez sur **Options** et dessélectionnez la case à cocher **Connexion automatique vers 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 SafeGuard.

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 dans le journal 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 dans le journal 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.

6.5 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 avec Local Self Help à la page 66.
- Récupération avec le Challenge/Réponse ou la clé de récupération à la page 76.

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 demander de changer votre mot de passe au démarrage de l'ordinateur si, par exemple, vous avez oublié votre mot de passe. Dans ce cas, le système vous propose également de mettre à jour les codes d'accès associés à l'empreinte digitale.

7 Chiffrement du disque

Pour le chiffrement du disque, SafeGuard Enterprise offre les options suivantes selon le système d'exploitation utilisé sur les ordinateurs d'extrémité :

- **Ordinateurs Windows 7 :**
  - Le chiffrement intégral du disque SafeGuard avec l'authentification au démarrage SafeGuard. Retrouvez plus d'informations à la section Chiffrement intégral du disque SafeGuard à la page 32
  - Chiffrement de lecteur BitLocker avec connexion Windows. Retrouvez plus d'informations à la section Chiffrement de lecteur BitLocker à la page 35.
- **Ordinateurs Windows 8 :** Chiffrement de lecteur BitLocker avec connexion Windows. Retrouvez plus d'informations à la section Chiffrement de lecteur BitLocker à la page 35.

7.1 Chiffrement intégral du disque SafeGuard

SafeGuard Enterprise assure le chiffrement intégral et transparent du disque basé sur les volumes. Le responsable de la sécurité définit les volumes à chiffrer dans les stratégies de sécurité.

7.1.1 Chiffrement transparent

Les fichiers d'un volume 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 volume 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.

7.1.2 Chiffrement initial

Au cours de la configuration initiale des ordinateurs protégés par SafeGuard Enterprise, les stratégies de chiffrement peuvent être créées et distribuées aux ordinateurs à l'aide d'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.

7.1.2.1 Chiffrement initial pour le chiffrement de volumes

Dès que votre ordinateur reçoit une stratégie de chiffrement de volumes suite à l'installation de SafeGuard Enterprise, le chiffrement initial de volumes démarre automatiquement.

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

Remarque : lors du chiffrement initial de la partition système (c'est-à-dire la partition sur laquelle se trouve le fichier hiberfil.sys), ne mettez pas l'ordinateur en veille. Après le

chiffrement initial de la partition système, redémarrez l'ordinateur pour vous assurer que le mode veille fonctionne de nouveau correctement.

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

Au cours de la configuration initiale des ordinateurs protégés par SafeGuard Enterprise, les stratégies de chiffrement peuvent être créées et distribuées aux ordinateurs à l'aide d'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.

7.1.3 Chiffrement intégral du disque basé sur volume

Le chiffrement d'un volume 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 Afficheur 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'Afficheur de chiffrement en cliquant sur l'icône. Si l'Afficheur de chiffrement est réduit, vous pouvez demander une notification une fois le chiffrement terminé en activant l'option **Affiche l'information avant de fermer**. L'afficheur se ferme automatiquement une fois le chiffrement terminé. Vous pouvez utiliser le volume chiffré comme tout autre volume déchiffré de votre ordinateur.

   Remarque :

   - Le chiffrement/déchiffrement de volume n'est pas pris en charge pour les volumes sans lettre de lecteur attribuée.
   - Pour Windows 7 Professionnel, Entreprise et Édition Intégrale, une partition système est créée sur les ordinateurs d'extrémité sans attribution de lettre de lecteur. Cette partition système ne peut pas être chiffrée par SafeGuard Enterprise.
   - Si une stratégie de chiffrement existe pour un volume ou un type de volume et si le chiffrement du volume échoue, l'utilisateur n'est pas autorisé à y accéder.
   - Les ordinateurs d'extrémité peuvent être éteints et redémarrés lors du chiffrement/déchiffrement.
   - Si le déchiffrement est suivi d'une désinstallation, nous conseillons de ne pas suspendre, ni de mettre en veille l'ordinateur d'extrémité lors du déchiffrement.
   - Si après le chiffrement d'un volume, une nouvelle stratégie est appliquée à un ordinateur d'extrémité qui autorise le déchiffrement, les conditions suivantes s'appliquent : une fois le chiffrement basé sur volume terminé, l'ordinateur d'extrémité doit être redémarré au moins une fois avant que le déchiffrement puisse être lancé.

   Remarque :

   À la différence du Chiffrement de lecteur BitLocker SafeGuard, le chiffrement de volume SafeGuard ne prend pas en charge les disques de tables de partitions (GPT). L'installation sera abandonnée si ce disque est détecté. Si un disque GPT est ajouté au système ultérieurement, les volumes présents sur ce disque seront chiffrés. Veuillez noter que les outils de récupération SafeGuard, comme par exemple BE_Restore.exe et recoverkeys.exe, ne peuvent pas gérer ces volumes. Sophos déconseille vivement de chiffrer les disques GPT. Pour déchiffrer les volumes accidentellement chiffrés, veuillez changer les stratégies SGN en conséquence et demander à l'utilisateur de les déchiffrer.

7.1.3.1 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.

7.2 Chiffrement de lecteur BitLocker

Le Chiffrement de lecteur BitLocker est une fonction de chiffrement intégral du disque avec authentification préalable au démarrage incluse dans les systèmes d'exploitation Microsoft Windows. Elle est conçue pour protéger les données en permettant le chiffrement des volumes de démarrage et de données. SafeGuard Enterprise gère le Chiffrement de lecteur BitLocker et offre d'autres fonctions.

7.2.1 Stratégies de chiffrement de BitLocker

Le responsable de la sécurité peut créer une stratégie de chiffrement dans SafeGuard Management Center et la distribuer aux ordinateurs d'extrémité BitLocker sur lesquels elle sera appliquée.

Les clients BitLocker sont gérés de manière transparente dans SafeGuard Management Center. La même stratégie de chiffrement peut être utilisée sur Mac avec le chiffrement intégral du disque SafeGuard et les clients BitLocker. SafeGuard Enterprise détecte l'état des clients et sélectionne le chiffrement BitLocker adéquat.

7.2.2 Authentification avec BitLocker

BitLocker propose toute une gamme d'options d'authentification. Le responsable de la sécurité peut définir les différents modes de connexion dans une stratégie dans SafeGuard Management Center et la distribuer aux ordinateurs d'extrémité BitLocker.

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

- TPM
- TPM + PIN
- TPM + Clé de démarrage
- Clé de démarrage uniquement (sans TPM)
- Mot de passe (sans TPM)

Vous devez fournir ces codes d'accès au démarrage de votre ordinateur d'extrémité BitLocker.

Module de plate-forme sécurisée (Trusted Platform Module ou TPM)

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 de démarrage sur la carte mémoire USB

Les clés externes peuvent être stockées sur une carte mémoire USB non protégée. La carte mémoire USB doit être insérée pour que l'authentification ait lieu au démarrage.

7.2.3 Chiffrement sur un ordinateur protégé par BitLocker

Lorsque la stratégie de chiffrement est envoyée à un ordinateur protégé par BitLocker, et avant que ce dernier ne redémarre et effectue le chiffrement initial, les clés de chiffrement sont générées par BitLocker. Le comportement est légèrement différent selon le système utilisé.

Ordinateurs d'extrémité avec TPM

Votre responsable de la sécurité peut définir différents mode de connexion (TPM, TPM + PIN, TPM + Clé de démarrage, Clé de démarrage ou Mot de passe) pour BitLocker. Si un mode de connexion avec TPM est défini, BitLocker stocke ses propres clés de chiffrement dans un périphérique matériel sécurisé nommé « Trusted Platform Module » (TPM) ou module de plate-forme sécurisée. Les clés ne sont pas stockées sur le disque dur de l'ordinateur. Le module TPM doit être accessible par le BIOS au cours du démarrage. Lorsque vous démarrez votre ordinateur, BitLocker récupère ces clés automatiquement à partir du TPM.

Ordinateurs d'extrémité sans TPM

Si votre ordinateur n'est pas équipé d'un TPM, vous allez être invité à saisir un mot de passe ou à créer une clé de démarrage BitLocker à l'aide d'une carte mémoire USB pour stocker les clés de chiffrement. Une boîte de dialogue affiche les bons lecteurs de destination dans lesquels vous pouvez stocker la clé de démarrage. Vous devrez insérer la carte mémoire à chaque démarrage de l'ordinateur.

Remarque : pour les **volumes de démarrage**, il est essentiel que vous disposiez de la clé de démarrage lorsque vous allumez votre ordinateur. La clé de démarrage peut donc uniquement être stockée sur des supports amovibles.

Pour les volumes de données, la clé de démarrage BitLocker peut être stockée sur un volume de démarrage déjà chiffré. Cette opération est effectuée automatiquement si le responsable de la sécurité a paramétré le mode de connexion des volumes non démarrables sur **Auto-déverrouiller**. Autrement, sélectionnez un appareil amovible affiché sous **Lecteurs de destination corrects** en tant qu'emplacement de stockage.

Clés de récupération BitLocker

Pour la récupération BitLocker, SafeGuard Enterprise propose une procédure Challenge/Réponse qui permet l'échange confidentiel d'informations ainsi que la possibilité de récupérer la clé de récupération BitLocker à partir du support. Retrouvez plus d'informations aux sections Challenge/Réponse pour les utilisateurs BitLocker à la page 82 et Clé de récupération BitLocker à la page 83.

Pour rendre possible la récupération par Challenge/Réponse, les données nécessaires doivent être fournies au support. Ces données nécessaires à la récupération sont téléchargées et enregistrées dans la base de données SafeGuard Enterprise.

Remarque : si le volume chiffré avec BitLocker d'un ordinateur est remplacé par un nouveau volume chiffré avec BitLocker et que ce dernier se voit affecter la même lettre de lecteur que l'ancien volume, SafeGuard Enterprise n'enregistre que la clé de récupération du nouveau volume. Veuillez conserver une copie de sauvegarde de la clé de l'ancien volume en utilisant les mécanismes de sauvegarde mis à disposition par Microsoft.

Gestion des volumes déjà chiffrés avec BitLocker

Si des volumes déjà chiffrés avec BitLocker sont présents sur votre ordinateur, ils seront gérés par SafeGuard Enterprise dès que le logiciel sera installé.

Volumes de démarrage chiffrés

- Selon la prise en charge SafeGuard Enterprise BitLocker utilisée, il se peut que vous deviez redémarrer l'ordinateur. Veuillez redémarrer l'ordinateur aussitôt que possible.
- Si une stratégie de chiffrement SafeGuard Enterprise s'applique au volume chiffré :
  - **Le Challenge/Réponse BitLocker** est installé : la gestion est prise en charge et il est possible d'utiliser le Challenge/Réponse SafeGuard.
  - **SafeGuard BitLocker** est installé : la gestion est prise en charge et il est possible d'utiliser la récupération SafeGuard.
- Si aucune stratégie de chiffrement SafeGuard Enterprise ne s'applique au volume chiffré :
  - **Le Challenge/Réponse BitLocker** est installé : la gestion n'est pas prise en charge et il n'est pas possible d'utiliser le Challenge/Réponse SafeGuard.
  - **SafeGuard BitLocker** est installé : il est possible d'utiliser la récupération SafeGuard.

Volume de données chiffrés

- Si une stratégie de chiffrement SafeGuard Enterprise s'applique au volume chiffré :

  la gestion est prise en charge et il est possible d'utiliser la récupération SafeGuard.
- Si aucune stratégie de chiffrement SafeGuard Enterprise ne s'applique au volume chiffré :

  il est possible d'utiliser la récupération SafeGuard.

Important : si le volume chiffré avec BitLocker d'un ordinateur est remplacé par un nouveau volume chiffré avec BitLocker et que ce dernier se voit affecter la même lettre de lecteur que l'ancien volume, SafeGuard Enterprise n'enregistre que la clé de récupération du nouveau volume. Veuillez conserver une copie de sauvegarde de la clé de l'ancien volume en utilisant les mécanismes de sauvegarde mis à disposition par Microsoft.

Remarque : il se peut que SafeGuard Enterprise ne soit pas en mesure de prendre en charge la gestion d'un volume déjà chiffré. Dans ce cas, vous ne pouvez pas utiliser SafeGuard Enterprise à des fins de récupération. Veuillez contacter votre responsable de la sécurité.

7.2.4 Chiffrement initial sur un ordinateur d'extrémité protégé par BitLocker

Selon le mode de connexion indiqué par le responsable de la sécurité pour votre ordinateur d'extrémité, la prise en charge SafeGuard Enterprise BitLocker peut se comporter de façon légèrement différente.

Dans tous les cas, une boîte de dialogue s'ouvre et vous offre la possibilité de continuer avec le chiffrement ou de le remettre à plus tard.

Si vous confirmez que vous souhaitez enregistrer, redémarrer et/ou chiffrer, l'opération de chiffrement ne commence pas immédiatement. Un test matériel est effectué pour garantir que votre ordinateur d'extrémité est conforme aux conditions requises pour le chiffrement SafeGuard Enterprise BitLocker. Le système redémarre et vérifie si toutes les conditions matérielles requises sont remplies. Si par exemple, le TPM ou la carte mémoire USB n'est pas disponible ou accessible, vous allez être invité à stocker la clé externe sur un autre appareil. Le système vérifie également si vous avez fourni des codes d'accès corrects. Si

vous ne pouvez pas fournir vos codes d'accès, l'ordinateur redémarre tout de même mais le chiffrement ne se lance pas. Vous allez être invité à saisir de nouveau votre code confidentiel ou votre mot de passe. Suite au succès du test matériel, le chiffrement BitLocker commence.

Si vous sélectionnez **Retarder**, le chiffrement ne commence pas et vous ne serez plus invité à chiffrer ce volume jusqu'à ce que :

- une nouvelle stratégie arrive,
- l'état du chiffrement BitLocker d'un volume change, ou
- vous vous reconnectiez au système.

Remarque : si le Chiffrement de lecteur BitLocker est géré par SafeGuard Enterprise pour votre lecteur de système d'exploitation ou pour vos volumes de données fixes, n'activez pas BitLocker manuellement pour ces volumes.

7.2.4.1 Enregistrement d'une clé de démarrage

Si votre responsable de la sécurité a indiqué un mode de connexion **TPM + Clé de démarrage** ou **Clé de démarrage**, vous allez devoir indiquer l'emplacement dans lequel la clé de démarrage est enregistrée. Insérez une carte mémoire USB pour stocker la clé. N'utilisez pas une carte mémoire USB chiffrée. Les lecteurs de destination valides pour la clé de démarrage sont répertoriés dans la boîte de dialogue. Vous devrez insérer la clé à chaque démarrage de l'ordinateur.

Sélectionnez le lecteur de destination et cliquez sur **Enregistrer et redémarrer**.

7.2.4.2 Création du mot de passe

Si votre responsable de la sécurité a indiqué un mode de connexion **Mot de passe**, vous êtes invité à saisir et confirmer votre nouveau mot de passe. Vous aurez besoin de ce mot de passe à chaque démarrage de l'ordinateur. La longueur et la complexité requises pour le mot de passe dépendent des objets de stratégie de groupe spécifiés par votre responsable de la sécurité. Vous êtes informé des conditions requises pour créer un mot de passe dans cette boîte de dialogue.

Remarque : si vous utilisez des caractères spéciaux lors de la création de votre mot de passe, veuillez prendre en compte que la disposition du clavier que vous utilisez peut être différente de la disposition de clavier EN-US prise en charge par BitLocker. Veuillez envisager de régler temporairement la disposition de votre clavier sur EN-US afin de pouvoir créer votre mot de passe.

7.2.4.3 Création du code confidentiel

Si votre responsable de la sécurité a indiqué un mode de connexion **TPM + PIN**, vous êtes invité à saisir et confirmer votre nouveau code confidentiel. Vous aurez besoin de ce code confidentiel à chaque démarrage de l'ordinateur. La longueur et la complexité requises dépendent des objets de stratégie de groupe spécifiés par votre responsable de la sécurité. Vous êtes informé des conditions requises pour créer un code confidentiel dans cette boîte de dialogue.

Remarque : si votre responsable de la sécurité a activé les codes confidentiels améliorés, vous avez la possibilité d'utiliser des caractères spéciaux dans votre code confidentiel. Veuillez prendre en compte que la disposition du clavier que vous utilisez peut être différente de la disposition de clavier EN-US prise en charge par BitLocker. Veuillez envisager de régler temporairement la disposition de votre clavier sur EN-US afin de pouvoir créer votre code confidentiel.

7.2.4.4 Boîte de dialogue pour TPM uniquement

Si votre responsable de la sécurité a indiqué un mode de connexion **TPM**, il vous suffit de confirmer le redémarrage et le chiffrement de votre ordinateur.

7.2.5 Déchiffrement avec BitLocker

Les ordinateurs chiffrés avec BitLocker ne peuvent pas être déchiffrés automatiquement. Le déchiffrement doit être effectué soit à l'aide du **Chiffrement de lecteur BitLocker** depuis le **Panneau de configuration** soit en utilisant l'outil de ligne de commande « Manage-bde » de Microsoft.

8 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 sur le périphérique sont initialement chiffrés. De surcroît, tous les nouveaux fichiers enregistrés sur le 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 indiquer 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 créez une nouvelle clé, veuillez fournir la phrase secrète 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 secrète correspondante, le destinataire peut déchiffrer les fichiers chiffrés et les chiffrer de nouveau sans que SafeGuard Data Exchange ne soit installé sur son ordinateur.

Important : lors de l'extraction d'un fichier archive ZIP à l'aide du programme d'archivage de Microsoft Windows, le processus s'arrête dès qu'il rencontre un fichier chiffré pour lequel aucune clé n'est disponible. L'utilisateur reçoit un message l'informant que l'accès a été interdit mais il n'est pas informé que des fichiers n'ont pas été traités et sont donc manquants. D'autres programmes d'archivage, par exemple 7-Zip, fonctionne correctement avec les archives ZIP contenant des fichiers chiffrés.

8.1 Paramètres de gestion des supports amovibles

Si SafeGuard Data Exchange est installé sur votre ordinateur, les supports amovibles seront gérés selon les règles prédéfinies par votre 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.
- **L'utilisateur peut annuler le chiffrement initial :** au démarrage du chiffrement initial, une boîte de dialogue s'affiche vous permettant d'annuler le chiffrement initial.
- **L'utilisateur est autorisé à accéder aux fichiers non chiffrés : Non** : 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.
- **L'utilisateur peut 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.
- **L'utilisateur peut définir une phrase secrète de support pour les périphériques :** vous êtes invité à saisir une phrase secrète des supports à votre première connexion au support amovible.
- **Dossier en texte brut** : 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.
- **L'utilisateur est autorisé à décider de l'opération de chiffrement :** lorsque vous connectez un support amovible à votre ordinateur, un message vous demande si vous désirez chiffrer les fichiers présents sur le support connecté. En outre et si activé par la stratégie, vous pouvez sélectionner si ce paramètre doit être conservé et toujours appliqué aux supports appropriés. Si vous sélectionnez **Mémoriser le paramètre et ne plus afficher cette boîte de dialogue**, la boîte de message ne réapparaîtra pas pour le support correspondant. Dans ce cas, la nouvelle commande **Réactiver le chiffrement** devient disponible dans le menu contextuel du périphérique correspondant dans l'Explorateur Windows. Sélectionnez cette commande pour annuler votre décision concernant le chiffrement du périphérique correspondant. Si ce n'est pas possible, par exemple parce que vous n'avez pas les droits appropriés sur le périphérique, un message d'erreur apparaît. Après avoir annulé votre décision, vous êtes invité à décider de nouveau si le périphérique doit être chiffré.

8.2 Phrase secrète unique des supports pour tous les supports amovibles connectés à l'ordinateur

SafeGuard Data Exchange permet de définir une phrase secrète unique du support qui vous donne accès à tous les périphériques amovibles connectés à l'ordinateur. Ceci se fait 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 secrète des supports. La phrase secrète des supports est liée aux ordinateurs auxquels vous êtes autorisé à vous connecter. Vous utilisez donc la même phrase secrète de support sur chaque ordinateur.

La phrase secrète des supports peut être changée et elle est synchronisée automatiquement sur chaque ordinateur avec lequel vous travaillez, dès que vous connectez un support amovible à cet ordinateur.

Une phrase secrète des supports est utile dans les situations suivantes :

- Vous souhaitez utiliser des données chiffrées sur des supports amovibles 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 secrète du support, vous pouvez leur permettre d'accéder à tous les fichiers du support amovible, avec une phrase secrète 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 secrète 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 secrète des supports 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 secrète ou un mot de passe. En effet, les clés de groupe et les phrase secrète 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 secrète des supports ou la phrase secrète d'une clé locale.

Supports pris en charge

SafeGuard Data Exchange prend en charge les supports amovibles suivants:

- Clés de démarrage
- Disques durs externes connectés par USB ou FireWire
- Lecteurs de CD-RW (UDF)
- Lecteurs de DVD-RW (UDF)
- Cartes mémoire dans des lecteurs de cartes USB

8.3 Chiffrement de supports amovibles

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. Tous les processus de chiffrement et de déchiffrement qui suivent sont exécutés de manière transparente et nécessitent une intervention minimale de l'utilisateur.

8.3.1 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** en cliquant avec le bouton droit de la souris dans l'Explorateur Windows pour ouvrir le menu. 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 clé est utilisée pour le chiffrement initial des supports 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 secrète des supports. 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 sélectionnée, les fichiers chiffrés avec une clé existante sont déchiffrés et chiffrés de nouveau avec la nouvelle clé.

Annulation 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 secrète des supports

Si l'utilisation d'une phrase secrète des supports a été spécifiée dans l'administration centralisée, vous êtes invité à saisir la phrase secrète des supports avant le chiffrement initial. La phrase secrète des supports 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 secrète des supports.

Une fois que vous avez saisi une fois la phrase secrète des supports, 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 secrète des supports n'est pas paramétrée.

8.3.2 Chiffrement manuel

Si vous êtes autorisé à décider si les fichiers sur les supports amovibles doivent être chiffrés, vous pouvez démarrer le processus de chiffrement manuellement. Ainsi, vous pouvez aussi chiffrer des fichiers déjà chiffrés à l'aide d'une clé différente.

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 présentes 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 secrète des supports. 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.

8.3.3 Chiffrement transparent

Si les paramètres définis pour votre ordinateur indiquent 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 écrits 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 sur lequel 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.

8.3.3.1 Phrase secrète des supports

Si l'utilisation d'une phrase secrète des supports 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 secrète des supports. Vous pouvez utiliser cette phrase secrète unique des supports pour accéder à tous les fichiers chiffrés sur votre support amovible, indépendamment de la clé effectivement utilisée pour les chiffrer.

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

8.3.3.2 Changement/réinitialisation de la phrase secrète des supports

Vous pouvez changer votre phrase secrète des supports à tout moment en utilisant la commande **Changer la phrase secrète des supports** 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 secrète des supports, puis confirmer la nouvelle.

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

Déconnectez-vous immédiatement, puis reconnectez-vous. Vous êtes informé qu'il n'existe pas de phrase secrète des supports sur votre ordinateur et vous êtes invité à en saisir une nouvelle.

8.3.3.3 Synchronisation de la phrase secrète des supports

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

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

8.4 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 secrète et peuvent être importées par SafeGuard Enterprise. Vous fournissez la phrase secrète au destinataire des données. Grâce à la phrase secrète, 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 secrète.

  SafeGuard Portable doit également être copié sur le support de stockage amovible. Vous devez également fournir au destinataire les données chiffrées avec la phrase secrète

correspondante. Grâce à la phrase secrète 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.

8.4.1 Importation de clés à partir d'un fichier

Si vous avez reçu des supports amovibles contenant des données chiffrées ou voulez accéder aux données Cloud Storage dans un dossier partagé avec des clés locales définies par un utilisateur, vous pouvez importer la clé nécessaire au déchiffrement dans votre jeu de clés privé.

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

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

La clé est importée et vous pouvez accéder au fichier.

8.4.2 Création de clés locales

1. Cliquez avec le bouton droit de la souris sur l'icône SafeGuard Enterprise de la barre d'état système dans la barre des tâches Windows ou cliquez avec le bouton droit de la souris sur volume/dossier/fichier.
2. Cliquez sur **Créer une nouvelle clé**.
3. Dans la boîte de dialogue **Création d'une clé**, saisissez un **Nom** et une **Phrase secrète** pour la clé.

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

4. Confirmez la phrase secrète.

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

5. Si vous avez ouvert la boîte de dialogue à l'aide d'un menu contextuel, il contient l'option **Utiliser en tant que nouvelle clé par défaut pour le chemin**. L'option **Utiliser en tant que nouvelle clé par défaut pour le chemin** vous permet de définir immédiatement la nouvelle clé comme clé par défaut pour un volume ou un dossier de synchronisation Cloud Storage.

   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, toutes les données copiées sur un support de stockage amovible ou dans un dossier de synchronisation Cloud Storage sont désormais chiffrées avec cette clé.

Pour qu'un destinataire puisse déchiffrer toutes les données contenues sur un support de stockage amovible, vous allez peut-être devoir chiffrer de nouveau les données sur le périphérique 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 secrète de supports.

8.5 Gravure de fichiers sur CD en utilisant l'Assistant Graver un CD de Windows

SafeGuard Data Exchange vous permet de graver des fichiers chiffrés sur CD à l'aide de 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 texte brut).

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 **Statistiques**, 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 en texte brut 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 en texte brut concernés se trouvent 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 en texte brut 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 en texte brut 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.

8.5.1 Copie sur CD/DVD

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

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

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

8.6 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 secrète de support appropriée, vous pouvez accéder à tous les fichiers chiffrés, indépendamment de la clé locale utilisée pour les chiffrer. La phrase secrète 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 secrète des supports ou la phrase secrète 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 du partenaire de travail avec lequel 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.

8.6.1 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 secrète 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 la phrase secrète**. Saisissez la phrase secrète pour déchiffrer le fichier sélectionné dans cette boîte de dialogue.
État de 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.

8.6.1.1 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 secrète** pour la clé. Veuillez **Confirmer** la phrase secrète et cliquez sur **OK**.

   La phrase secrète 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.

8.6.1.2 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 secrète (et confirmez-la). 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 et 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.

8.6.1.3 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 secrète des supports ou la phrase secrète d'une clé locale est affichée.

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

   Le fichier est déchiffré.

La phrase secrète des supports 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 secrète 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 secrète 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 secrète 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.

8.6.1.4 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. Faites glisser et déposer les fichiers souhaités dans l'explorateur SafeGuard Portable.

   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 copié sur le support amovible.

8.6.1.5 État de 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.

8.6.2 Autres opérations à l'aide de SafeGuard Portable

Les opérations suivantes sont également disponibles :

- **Ouvrir** : cette commande de menu est uniquement disponible dans le menu **Fichier** de SafeGuard Portable.

  À l'ouverture d'un fichier chiffré avec cette commande de menu, vous êtes invité à saisir la phrase secrète. Saisissez votre phrase secrète 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 volume de votre ordinateur.

- **Quitter** : cette commande de menu est uniquement disponible dans le menu **Fichier** de SafeGuard Portable.

  Quitter : ferme SafeGuard Portable.

9 SafeGuard File Encryption

Le module File Encryption de SafeGuard Enterprise offre le chiffrement de fichiers sur les lecteurs locaux et les emplacements réseau. Il a surtout été créé pour les groupes de travail, pour stocker en toute sécurité les données sur les partages réseau.

Après attribution d'une stratégie **File Encryption** sur votre ordinateur, les fichiers présents dans les emplacements couverts par la stratégie sont chiffrés de manière transparente sans intervention de l'utilisateur :

- Les nouveaux fichiers dans les emplacements correspondants sont chiffrés automatiquement.
- Si vous avez la clé d'un fichier chiffré, vous pouvez lire et modifier le contenu.
- Si vous n'avez pas la clé d'un fichier chiffré, l'accès est refusé.
- Si vous accédez à un fichier chiffré sur un ordinateur sur lequel File Encryption n'est pas installé, le contenu chiffré apparaît.
- Retrouvez plus d'informations sur la manière de vérifier l'état du chiffrement de vos fichiers avec les extensions de l'Explorateur SafeGuard Enterprise pour le chiffrement de fichiers à la section Extensions de Explorer pour le chiffrement de fichiers. à la page 62.

9.1 Chiffrement en fonction de la stratégie

Après attribution d'une stratégie **File Encryption** sur votre ordinateur, les fichiers déjà existants dans les emplacements couverts par la stratégie de chiffrement ne sont pas chiffrés automatiquement. Un chiffrement initial doit être effectué.

Nous vous conseillons d'effectuer ce chiffrement initial dès que votre ordinateur d'extrémité reçoit une stratégie File Encryption même si le responsable de la sécurité peut automatiquement lancer cette tâche de chiffrement. Ceci garantit que vos données sont chiffrées en fonction de la stratégie aussitôt possible après réception d'une stratégie File Encryption.

Certaines applications créent un nouveau fichier suite à la modification du contenu d'un fichier et suppriment l'ancien fichier. Le fichier est uniquement chiffré suite à sa modification avec ces applications. Toutes les autres applications laissent le fichier déchiffré s'il l'était déjà avant sa modification.

Pour commencer le chiffrement, procédez comme suit :

1. Sélectionnez **Chiffrement de fichier > Chiffrer en fonction de la stratégie** dans le menu contextuel du nœud *Poste de travail* dans l'Explorateur Windows.
2. L'**Assistant de chiffrement des fichiers SafeGuard** apparaît.

   Tous les fichiers présents dans les dossiers et sous-dossiers couverts par les règles de chiffrement sont chiffrés avec la clé définie dans la règle correspondante.

9.2 Assistant SafeGuard File Encryption

L'assistant SafeGuard File Encryption apparaît lorsque vous sélectionnez la commande **Chiffrer en fonction de la stratégie** dans le menu contextuel du nœud *Poste de travail* ou

la commande **Démarrer le chiffrement** dans le menu contextuel des dossiers et des fichiers dans l'Explorateur Windows.

Il vérifie tous les dossiers qui sont définis dans une règle de chiffrement pour l'utilisateur :

- Les fichiers bruts qui doivent être chiffrés le seront avec la clé définie dans la règle.
- Les fichiers chiffrés qui doivent être chiffrés avec une clé différente seront de nouveau chiffrés avec la clé définie dans la règle.
- Une erreur apparaît lorsque l'utilisateur ne possède pas la clé courante.
- Les fichiers chiffrés qui doivent être bruts conformément à la stratégie de chiffrement demeurent chiffrés.

Une image indique l'état général de l'opération :

- **Vert :** l'opération s'est terminée avec succès.
- **Rouge :** l'opération s'est terminée avec des erreurs.
- **Jaune :** l'opération est en cours.

Quatre pages à onglets fournissent des informations sur les fichiers traités :

- La page à onglets **Récapitulatif** affiche les compteurs relatifs aux fichiers trouvés/chiffrés/rechiffrés/ ... Le bouton **Exporter...** peut être utilisé pour créer des rapports XML contenant les fichiers traités et les résultats.
- La page à onglets **Erreurs** affiche les fichiers qui n'ont pas pu être gérés comme prévu.
- La page à onglets **Modifié** affiche les fichiers qui ont été modifiés avec succès.
- La page à onglets **Tous** affiche tous les fichiers traités et leurs résultats.

Si vous cliquez sur le bouton **Arrêter** en haut à droit, l'opération est annulée. Le bouton **Arrêter** se transforme en bouton **Redémarrer** pour redémarrer l'opération.

Lorsque l'opération se termine avec des erreurs, le bouton **Arrêter** se transforme en bouton **Réessayer**. Si vous cliquez sur le bouton **Réessayer**, l'opération est relancée mais seulement pour les fichiers qui ont échoué.

9.3 Chiffrement permanent

Le contenu des fichiers chiffrés par File Encryption est déchiffré instantanément si vous possédez la clé nécessaire. Lorsque le contenu est enregistré sous la forme d'un nouveau fichier dans un emplacement qui ne fait pas l'objet d'une règle de chiffrement, le fichier obtenu ne sera pas chiffré.

Avec le chiffrement permanent, les copies des fichiers chiffrés seront chiffrées, même lorsqu'elles sont enregistrées dans un emplacement qui ne fait pas l'objet d'une règle de chiffrement.

Remarque : les responsables de la sécurité peuvent désactiver ce comportement. S'il est désactivé, les fichiers sont créés en texte brut lorsqu'ils sont copiés/déplacés dans un emplacement qui ne fait pas l'objet d'une règle de chiffrement.

10 SafeGuard Cloud Storage

Le module Cloud Storage de SafeGuard Enterprise offre le chiffrement de fichiers des données stockées dans le Cloud.

Il ne change en rien votre utilisation des données stockées dans le Cloud. En revanche, Cloud Storage s'assure que les copies locales de vos données dans le Cloud sont chiffrées de manière transparente et restent chiffrées une fois stockées dans le Cloud.

Remarque : n'ajoutez pas de fichiers dans votre dossier Dropbox en les déposant sur l'icône Dropbox de votre Bureau Windows. Ces fichiers seront copiés dans votre dossier Dropbox sous format brut. Pour chiffrer les fichiers, copiez-les directement dans votre dossier Dropbox.

Important : lors de l'extraction d'un fichier archive ZIP à l'aide du programme d'archivage de Microsoft Windows, le processus s'arrête dès qu'il rencontre un fichier chiffré pour lequel aucune clé n'est disponible. L'utilisateur reçoit un message l'informant que l'accès a été interdit mais il n'est pas informé que des fichiers n'ont pas été traités et sont donc manquants. D'autres programmes d'archivage, par exemple 7-Zip, fonctionne correctement avec les archives ZIP contenant des fichiers chiffrés.

10.1 Détection automatique Cloud Storage

SafeGuard Cloud Storage détecte automatiquement votre fournisseur de stockage dans le Cloud. Il paramètre automatiquement la stratégie de chiffrement sur le dossier à synchroniser.

10.2 Chiffrement initial Cloud Storage

SafeGuard Cloud Storage n'exécute pas de chiffrement initial de vos données. Les fichiers qui ont été stockés avant que SafeGuard Cloud Storage ne soit installé ou activé par une stratégie restent en texte brut.

Si vous voulez chiffrer ces fichiers, vous devez d'abord les supprimer du Cloud et les ajouter de nouveau.

10.3 Définition des clés par défaut

SafeGuard Cloud Storage vous permet de définir des clés par défaut pour le chiffrement des données dans votre stockage dans le Cloud. L'utilisation des clés par défaut vous permet de chiffrer différents sous-dossiers de votre stockage dans le Cloud à l'aide de clé différentes en définissant une clé par défaut distincte pour chaque dossier. Pour définir des clés par défaut, sélectionnez la commande **Chiffrement de fichier > Définir la clé par défaut...** dans les extensions de l'Explorateur SafeGuard. Retrouvez plus d'informations à la section Définition d'une clé par défaut à la page 63.

Remarque : pour ce faire, votre responsable de la sécurité doit explicitement autoriser l'utilisation des clés par défaut pour Cloud Storage. Si vous y êtes autorisé, vous pouvez sélectionner une clé par défaut dans un jeu de clés prédéfini et l'utiliser pour chiffrer les dossiers de votre stockage dans le Cloud.

Remarque : si vous envisagez de lire les fichiers chiffrés sur les appareils Android et iOS à l'aide de Sophos Mobile Encryption, veuillez utiliser les clés locales pour procéder au

chiffrement. Retrouvez plus d'informations sur Sophos Mobile Encryption dans l'*Aide de Sophos Mobile Encryption*.

Si vous voulez utiliser Dropbox pour fournir des données sécurisées à différents partenaires. Chaque partenaire doit avoir accès à un sous-dossier de votre Dropbox. Pour cela, il vous suffit simplement de définir une clé par défaut distincte pour chacun des sous-dossiers. SafeGuard Enterprise ajoutera alors automatiquement une copie de SafeGuard Portable, ce qui donnera aux partenaires un accès SafeGuard Cloud Storage aux données chiffrées, dans chaque sous-dossier. Donnez à vos partenaires les phrases secrètes correspondant aux clés. Grâce à SafeGuard Portable et à la phrase secrète, ils pourront déchiffrer les données présentes dans le dossier que vous avez créé pour eux. En revanche, ils n'auront pas accès aux données stockées dans d'autres sous-dossiers, car elle seront chiffrées avec une clé différente.

10.4 SafeGuard Portable pour Cloud Storage

Vous pouvez envisager d'accéder au stockage dans le Cloud depuis votre domicile ou échanger des données chiffrées dans le Cloud en utilisant un dossier partagé dans votre stockage dans le Cloud. SafeGuard Portable permet d'accéder aux données chiffrées stockées dans le Cloud sans que SafeGuard Cloud Storage soit installé.

Les données chiffrées avec SafeGuard Cloud Storage peuvent être chiffrées et déchiffrées avec SafeGuard Portable. Cette opération est possible en copiant automatiquement un programme (SGPortable.exe) sur votre dossier de synchronisation.

La phrase secrète d'une clé locale vous permet d'accéder seulement aux fichiers qui ont été chiffrés à l'aide de cette clé. Vous, ou un destinataire quelconque, pouvez déchiffrer des données chiffrées et les chiffrer à nouveau.

Remarque : la phrase secrète d'une clé locale doit être communiquée au préalable au destinataire.

Le destinataire peut utiliser des clés existantes 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 du partenaire de travail avec lequel vous communiquez. Il reste dans le stockage du Cloud.

Retrouvez une description détaillée de l'utilisation de SafeGuard Portable à la section Modification de fichiers à l'aide de SafeGuard Portable à la page 49.

Remarque : si vous cliquez deux fois sur un fichier ou sélectionnez la commande ouverte, le fichier ne sera pas immédiatement déchiffré. En effet, les fichiers déchiffrés dans les dossiers de synchronisation du stockage dans le Cloud seraient automatiquement synchronisés avec le Cloud. Lorsque vous exécutez cette opération, une boîte de dialogue apparaît vous demandant de choisir un emplacement sûr pour le fichier. Les fichiers déchiffrés ne sont pas automatiquement effacés lorsque SafeGuard Portable est fermé. Les modifications dans les fichiers déchiffrés avec SafeGuard Portable pour Cloud Storage ne seront pas effectuées dans les fichiers d'origine chiffrés.

Remarque : ne stockez pas les dossiers de synchronisation du stockage dans le Cloud sur un support amovible ou sur le réseau. Si vous le faites, SafeGuard Portable crée des fichiers déchiffrés dans ces dossiers. SafeGuard Portable ne doit dans ce cas pas être utilisé. Envisagez plutôt de déplacer les dossiers de synchronisation sur des disques fixes.

11 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. 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 prend en charge la norme Opal et permet la gestion des ordinateurs d'extrémité avec disques durs compatibles Opal à chiffrement automatique. Retrouvez plus d'informations sur http://www.sophos.com/fr-fr/support/knowledgebase/113366.aspx.

11.1 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 128/256 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 SafeGuard Management Center et la distribue à votre ordinateur.

11.2 Extensions des icônes de la barre d'état système 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 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.

12 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 barre d'état système 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 barre d'état 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.

    Remarque : si votre ordinateur d'extrémité a été migré d'un environnement non administré à un environnement administré, une deuxième connexion à SafeGuard Enterprise sera peut être nécessaire pour afficher les clés locales définies par l'utilisateur sur voter jeu de clés.

  - **Certificat d'utilisateur** : affiche des informations relatives à votre certificat.
  - **Certificat d'entreprise** : affiche des informations relatives au certificat d'entreprise utilisé.
- **Créer une nouvelle clé** : ouvre une boîte de dialogue pour la création d'un nouvelle clé utilisée pour l'échange des données avec le support amovible ou SafeGuard Cloud Storage. Reportez-vous aux sections SafeGuard Data Exchange à la page 40 et SafeGuard Cloud Storage à la page 54.
- **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 barre d'état système. Cette commande permet de lancer l'assistant Local Self Help. Local Self Help est une méthode de récupération de connexion qui ne requiert aucune assistance du support. Retrouvez plus d'informations à la section Récupération avec Local Self Help à la page 66.

- **Changer la phrase secrète des supports** : ouvre une boîte de dialogue pour changer la phrase secrète des supports. Reportez-vous à la section SafeGuard Data Exchange à la page 40.
- **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 la date et l'heure auxquelles l'ordinateur a reçu une nouvelle stratégie.
Dernière clé reçue	Indique la date et l'heure auxquelles l'ordinateur a reçu une nouvelle clé.
Dernier certificat reçu	Indique la date et l'heure auxquelles l'ordinateur a reçu un nouveau certificat.
Dernier contact du serveur	Indique la date et l'heure du dernier contact avec le serveur.
État de l'utilisateur SGN	Indique l'état de l'utilisateur connecté à l'ordinateur (connexion Windows) : ▪ **En attente** : la réplication de l'utilisateur dans l'authentification au démarrage SafeGuard 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. En effet, vous pouvez uniquement vous connecter à partir de l'authentification au démarrage SafeGuard après la synchronisation utilisateur initiale. ▪ **Utilisateur SGN** : L'utilisateur connecté à Windows est un utilisateur SafeGuard Enterprise. Un utilisateur SGN est autorisé à se connecter à l'authentification au démarrage SafeGuard, est ajouté à l'attribution utilisateur/machine et se voit fournir un certificat d'utilisateur et un jeu de clés lui permettant d'accéder aux données chiffrées. ▪ **Utilisateur SGN (propriétaire)** : Si les paramètres par défaut n'ont pas été modifiés, un propriétaire a le droit d'autoriser d'autres utilisateurs à se connecter à l'ordinateur d'extrémité et à devenir des utilisateurs SGN. ▪ **Invité SGN** : Les utilisateurs invités SGN ne sont pas ajoutés à l'attribution utilisateur/machine, ne disposent pas des droits de connexion à l'authentification au démarrage SafeGuard, n'ont pas de certificat ou de jeu de clés et ne sont pas enregistrés dans la base de données.

Champ	Informations
	▪ **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. ▪ **Utilisateur Windows de SGN** Un utilisateur Windows de SafeGuard Enterprise n'est pas ajouté à l'authentification au démarrage SafeGuard. En revanche, il dispose d'un jeu de clés pour accéder aux fichiers chiffrés comme le ferait un utilisateur SafeGuard Enterprise. Les utilisateurs sont ajoutés à l'attribution utilisateur/machine. Ils sont donc autorisés à se connecter à Windows depuis cet ordinateur d'extrémité. ▪ **Inconnu** : Indique que l'état de l'utilisateur n'a pas pu être déterminé.
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.
Prêt pour la modification du certificat	Ce texte est affiché si le responsable de la sécurité a attribué un nouveau certificat pour la connexion par token sur votre ordinateur. Vous pouvez désormais changer le certificat de connexion par token. Retrouvez plus d'informations à la section Changement du certificat pour la connexion par token à la page 19.

- **Aide** : ouvre l'aide en ligne de SafeGuard Enterprise.
- **À propos de SafeGuard Enterprise** : affiche des informations relatives à la version de SafeGuard Enterprise que vous utilisez.

12.1 Création de clés locales

1. Cliquez avec le bouton droit de la souris sur l'icône SafeGuard Enterprise de la barre d'état système dans la barre des tâches Windows ou cliquez avec le bouton droit de la souris sur volume/dossier/fichier.

2. Cliquez sur **Créer une nouvelle clé**.
3. Dans la boîte de dialogue **Création d'une clé**, saisissez un **Nom** et une **Phrase secrète** pour la clé.

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

4. Confirmez la phrase secrète.

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

5. Si vous avez ouvert la boîte de dialogue à l'aide d'un menu contextuel, il contient l'option **Utiliser en tant que nouvelle clé par défaut pour le chemin**. L'option **Utiliser en tant que nouvelle clé par défaut pour le chemin** vous permet de définir immédiatement la nouvelle clé comme clé par défaut pour un volume ou un dossier de synchronisation Cloud Storage.

   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, toutes les données copiées sur un support de stockage amovible ou dans un dossier de synchronisation Cloud Storage sont désormais chiffrées avec cette clé.

Pour qu'un destinataire puisse déchiffrer toutes les données contenues sur un support de stockage amovible, vous allez peut-être devoir chiffrer de nouveau les données sur le périphérique 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 secrète de supports.

12.2 Icônes superposées

Les icônes superposées sont des icônes de petite taille affichées sur les éléments dans l'Explorateur Windows. Les icônes superposées de Data Exchange apparaissent uniquement sur les fichiers et volumes. Elles vous renseignent rapidement sur l'état du chiffrement d'un fichier ou vous indiquent si une règle de chiffrement est appliquée à un volume.

- Une clé rouge indique que vous n'avez pas de la clé de déchiffrement d'un fichier. Cette icône apparaît uniquement sur les fichiers.
- Une clé verte indique que la clé du fichier chiffré est sur votre jeu de clés. Cette icône apparaît uniquement sur les fichiers.
- Une clé clé grise indique qu'un fichier n'est pas chiffré mais qu'une règle de chiffrement pour ledit fichier est disponible. Cette icône apparaît uniquement sur les fichiers.
- Une clé jaune indique qu'une stratégie de chiffrement est définie pour un lecteur. Cette icône apparaît uniquement sur les lecteurs.

Les icônes superposées apparaissent uniquement sur les volumes non démarrables, les supports amovibles et les CD/DVD. Dans le cas des lecteurs de démarrage, les icônes

superposées apparaissent dans le dossier intermédiaire de gravure (le dossier dans lequel Windows conserve les fichiers qui vont être gravés sur un CD/DVD). Si vous choisissez un dossier non chiffré, la clé grise ne s'affichera pas sur les fichiers non chiffrés dans ce dossier et dans ses sous-dossiers. Généralement, s'il n'y a aucune règle de chiffrement appliquée à un fichier, la clé grise n'apparaît pas.

13 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.

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 nœud de l'Explorateur sélectionné. La portée de la fonction varie en fonction du chiffrement de fichiers ou de volumes utilisé pour le volume/dossier/fichier correspondant.

13.1 Extensions de l'Explorateur pour le chiffrement de fichiers

Vous pouvez accéder aux fonctions de chiffrement de fichiers (Data Exchange, File Encryption, Cloud Storage) à partir des entrées correspondantes des menus contextuels de l'Explorateur Windows. Les fonctions sont disponibles dans les menus contextuels suivants :

- Nœud « Poste de travail »
- Supports amovibles
- Dossiers
- Fichiers

Les fonctions affichées dans le menus dépendent des composants installés.

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

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

Les fonctions suivantes sont disponibles :

- **Chiffrer en fonction de la stratégie** : n'apparaît que lorsque File Encryption est installé et que le nœud « Poste de travail » est sélectionné. Si vous sélectionnez cette option, tous les fichiers présents dans les dossiers et sous-dossiers couverts par des règles de chiffrement sont chiffrés en fonction de la stratégie valide pour votre ordinateur.
- **Démarrer le chiffrement** : si vous sélectionnez cette option dans un menu contextuel, tous les fichiers peuvent être chiffrés ou chiffrés de nouveau. Lorsqu'une stratégie File Encryption est applicable, un assistant de chiffrement de fichiers est lancé.
- **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 les fichiers sélectionnés.

  Remarque : il n'est pas possible de déchiffrer des fichiers auxquels s'appliquent une règle File Encryption.

- **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.
- **Réactiver le chiffrement :** votre responsable de la sécurité peut vous permettre de décider si les fichiers présents sur les supports amovibles connectés à votre ordinateur doivent être chiffrés. Lorsque vous connectez un support amovible à votre ordinateur, un message vous demande si vous désirez chiffrer les fichiers présents sur le support connecté. En outre, votre responsable de la sécurité peut vous permettre de sélectionner si votre choix doit être conservé pour les supports équivalents. Si vous sélectionnez **Mettre le paramètre en mémoire et ne plus afficher cette boîte de dialogue**, la boîte de message ne réapparaîtra pas pour le support correspondant. Dans ce cas, la nouvelle commande **Réactiver le chiffrement** devient disponible dans le menu contextuel du périphérique correspondant dans l'Explorateur Windows. Sélectionnez cette commande pour annuler votre décision concernant le chiffrement du périphérique correspondant. Si ce n'est pas possible, par exemple parce que vous n'avez pas les droits appropriés sur le périphérique, un message d'erreur apparaît. Après avoir annulé votre décision, vous êtes invité à décider de nouveau si le périphérique doit être chiffré.

13.1.1 Définition d'une clé par défaut

En définissant une clé par défaut, vous indiquez la clé à utiliser pour le chiffrement lors du fonctionnement normal de SafeGuard Data Exchange et de SafeGuard Cloud Storage.

Vous pouvez définir la clé par défaut à partir du menu contextuel

- d'un fichier sur support amovible
- du support amovible
- d'un dossier ou sous-dossier de synchronisation Cloud Storage
- d'un fichier présent dans un dossier ou sous-dossier de synchronisation Cloud Storage
- de surcroît, vous pouvez définir une clé par défaut immédiatement lorsque vous créez une nouvelle clé locale dans la boîte de dialogue **Créer une clé**.

Pour définir une clé par défaut :

Sélectionnez **Chiffrement de fichier > Définir la clé par défaut** pour ouvrir 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 de stockage amovible ou dans votre dossier de synchronisation Cloud Storage. Si vous voulez utiliser une autre clé, vous pouvez en définir une nouvelle par défaut à tout moment.

Remarque : si une clé locale est sélectionnée pour le chiffrement de Cloud Storage, SafeGuard Portable sera copié dans le dossier de synchronisation Cloud Storage.

En règle générale, vous pouvez définir la clé à utiliser pour le chiffrement dans la stratégie. Si elle n'est pas définie dans la stratégie et si vous êtes autorisé à définir des clés par défaut, vous êtes invité à indiquer une clé initiale par défaut.

13.1.2 Importation de clés à partir d'un fichier

Si vous avez reçu des supports amovibles contenant des données chiffrées ou voulez accéder aux données Cloud Storage dans un dossier partagé avec des clés locales définies par un utilisateur, vous pouvez importer la clé nécessaire au déchiffrement dans votre jeu de clés privé.

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

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

La clé est importée et vous pouvez accéder au fichier.

13.2 Extensions de l'Explorateur pour le chiffrement de volumes

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.

14 Options de récupération

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

- **Récupération de connexion avec Local Self Help** (uniquement disponible avec l'authentification au démarrage SafeGuard)

  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 SafeGuard.

  Retrouvez plus d'informations à la section Récupération avec Local Self Help à la page 66.

- **Récupération avec le Challenge/Réponse ou la clé de récupération BitLocker**

  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 va générer à son tour un code de réponse. Ce code vous permettra ensuite d'exécuter une action spécifique sur l'ordinateur.

  Sur les ordinateurs d'extrémité ne prenant pas en charge le Challenge/Réponse, les clés de récupération sont fournies. Il s'agit de la procédure standard de Microsoft. Pendant l'opération de récupération, vous devez fournir le nom de l'ordinateur au responsable du support qui en retour vous enverra la clé de récupération nécessaire au démarrage de l'ordinateur.

  Retrouvez plus d'informations à la section Récupération avec le Challenge/Réponse ou la clé de récupération à la page 76.

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

15 Récupération avec Local Self Help

Remarque : l'assistant Local Self Help est uniquement disponible sur les ordinateurs d'extrémité sous Windows 7 et avec l'authentification au démarrage SafeGuard.

Si vous avez oublié votre mot de passe, Local Self Help vous permet de vous connecter à votre ordinateur sans l'aide du support.

L'utilisation de Local Self Help permet d'accéder de nouveau à votre ordinateur 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 SafeGuard.

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 système de SafeGuard Enterprise dans la barre des tâches Windows.

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.

15.1 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 auxquelles vous devez répondre. L'assistant Local Self Help vous guide durant le processus et vous indique le nombre de questions auxquelles vous devez 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 auxquelles vous devez 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 SafeGuard 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 auxquelles vous devez répondre dans l'authentification au démarrage SafeGuard.

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 barre d'état système 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 ou le nombre de questions prédéfinies ayant une réponse).

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 SafeGuard, 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 : les caractères saisis dans Windows ne sont pas tous gérés par l'authentification au démarrage SafeGuard. Par exemple, les polices de caractères en hébreu et en arabe ne peuvent pas être utilisées. Lorsque vous saisissez des réponses en japonais, veuillez utiliser des caractères Romaji (romains). Autrement, les réponses ne correspondront pas lorsque vous répondrez aux questions dans l'authentification au démarrage SafeGuard.

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 SafeGuard, 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 :

   Les caractères saisis dans Windows ne sont pas tous gérés par l'authentification au démarrage SafeGuard. Par exemple, les polices de caractères en hébreu et en arabe ne peuvent pas être utilisées. Lorsque vous saisissez des réponses en japonais, veuillez utiliser des caractères Romaji (romains). Autrement, les réponses ne correspondront pas lorsque vous répondrez aux questions dans l'authentification au démarrage SafeGuard.

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

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

8. Cliquez sur **Terminer**.

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

9. Cliquez sur **OK**.

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

15.2 Activation de Local Self Help - Rappel

L'activation de Local Self Help est indispensable. Pour cette raison, SafeGuard Enterprise vous rappelle que vous devez vous enregistrer dans Local Self Help.

SafeGuard Enterprise vous rappelle que vous devez paramétrer vos questions Local Self Help en trois étapes :

- **Étape 1**

  Une infobulle s'ouvre toutes les heures pendant un jour pour vous rappeler que vous devez configurer Local Self Help. Le jour suivant, l'étape 2 est initiée.

- **Étape 2**

  À l'opération décrite à l'étape 1 vient s'ajouter le démarrage de l'Assistant Local Self Help à chaque fois que vous vous connectez ou déverrouillez l'ordinateur. Vous pouvez retarder l'exécution de cet assistant. Au bout de 3 jours, l'étape 3 est initiée.

- **Étape 3**

  À l'opération décrite à l'étape 2 mais cette fois-ci sans infobulle, vient s'ajouter le démarrage de l'Assistant Local Self Help toutes les 60 minutes.

L'utilisateur est immédiatement informé par une infobulle et l'étape 1 est initiée à chaque fois que Local Self Help doit être réactivé suite à la modification de l'un des éléments suivants :

- Paramètres Local Self Help
- Mot de passe Windows
- Certificat

15.3 Modification des questions

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

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

1. Cliquez avec le bouton droit de la souris sur l'icône de la barre d'état système 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 et si vous y avez répondu, la boîte de dialogue **Questions prédéfinies** s'affiche avec les questions ayant une réponse.

   a) 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**.

   b) 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.

   c) Pour afficher le texte saisi, sélectionnez la case **Afficher les réponses**.

   d) Pour modifier les réponses, cliquez sur les questions concernées et saisissez votre nouvelle réponse dans la colonne **Réponses**.

5. 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.

   a) Pour afficher le texte saisi, sélectionnez la case **Afficher les réponses**.

   b) Pour modifier les réponses existantes, cliquez sur la question concernée et saisissez votre nouvelle réponse dans la colonne **Réponses**.

   c) 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**.

   d) 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**.

6. 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.

7. 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.

8. Cliquez sur **OK**.

   Les modifications sont appliquées.

La prochaine fois que vous lancerez Local Self Help dans l'authentification au démarrage SafeGuard, 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. Toutefois, dans ce cas, vous pouvez réactiver Local Self Help.

15.4 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 auxquelles vous devez 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 indiqué doit être disponible.

- Le nombre de questions auxquelles vous devez répondre dans l'authentification au démarrage SafeGuard pour pouvoir vous connecter à Local Self Help. Les questions affichées dans l'authentification au démarrage SafeGuard sont sélectionnées aléatoirement à partir des réponses que vous avez fournies aux questions posées 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 questions change dans l'assistant Local Self Help 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 change dans l'assistant Local Self Help 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.
Le nombre de questions dans l'authentification au démarrage SafeGuard pour se connecter à 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.

15.5 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.

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 de modification, l'ensemble de questions et réponses définies pourrait ne plus être valide et le nombre de questions sera 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 auxquelles vous devez répondre) par une nouvelle stratégie. Local Self Help n'a pas été désactivé. Les questions et réponses définies sont toujours valides et en quantité suffisante pour que Local Self Help reste actif sur votre ordinateur.	L'assistant Local Self Help affiche un message indiquant que les paramètres Local Self Help ont été modifiés, enregistre vos modifications et se ferme.	Local Self Help est actif sur votre ordinateur et peut être utilisé pour une récupération de connexion. Toutefois, les proportions de questions disponibles et de réponses valides sont susceptibles d'avoir été modifiées. Pour retrouver la proportion initiale, vous devrez peut-être ajouter ou supprimer des questions et/ou des réponses.
▪ Le mot de passe utilisateur a été modifié **et/ou** ▪ 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 auxquelles vous devez répondre, etc.) par une nouvelle stratégie. Local Self Help n'a pas été désactivé. Les questions et réponses définies ne sont plus valides et leur nombre est insuffisant pour que Local Self Help soit actif sur votre ordinateur.	L'assistant Local Self Help affiche un message indiquant que 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 conseillons d'exécuter de nouveau l'assistant. L'assistant se ferme.	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.
Le certificat utilisateur a été modifié.	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 conseillons d'exécuter de nouveau l'assistant. L'assistant se ferme.	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

Condition	Action de l'assistant LSH	Résultat
		pour la récupération de connexion.

15.6 Connexion à l'authentification au démarrage SafeGuard à l'aide de Local Self Help

1. Dans la boîte de dialogue de connexion à l'authentification au démarrage SafeGuard, 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 SafeGuard avec un token ou une carte à puce, vous devez tout d'abord retirer le token ou la carte à puce de votre ordinateur. Ensuite, la boîte de dialogue de l'authentification au démarrage SafeGuard de connexion par nom d'utilisateur et mot de passe s'affiche. Saisissez votre identifiant utilisateur et cliquez sur le bouton **Récupération**.

   La boîte de dialogue de **Bienvenue dans 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 connecter à partir de l'authentification au démarrage SafeGuard et pour vous reconnecter 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 SafeGuard et à Windows.

15.7 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 dans le journal des événements. Dans ce cas, un délai de connexion se produit. Le délai de connexion augmente 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.

15.8 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 barre d'état système de SafeGuard Enterprise de 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 SafeGuard avec Local Self Help.

16 Récupération avec le Challenge/Réponse ou la clé de récupération

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 au support central.

Remarque : si vous utilisez Windows 7 et l'authentification au démarrage SafeGuard, nous vous conseillons d'utiliser Local Self Help pour récupérer votre mot de passe en cas d'oubli. Vous pouvez afficher le mot de passe existant dans Local Self Help et continuer à l'utiliser. Il n'est donc pas nécessaire de réinitialiser le mot de passe ou de contacter le support.

16.1 Challenge/Réponse pour les utilisateurs de l'authentification au démarrage SafeGuard

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

Pendant la procédure Challenge/Réponse, vous générez un code de challenge (chaîne de caractères ASCII) et fournissez ce code au responsable 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 SafeGuard :

- Connexion par identifiant utilisateur et mot de passe
- Connexion par empreinte digitale
- Connexion à l'aide d'un token non cryptographique

16.1.1 Cas de figure classiques de demande d'assistance au 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 SafeGuard. L'ordinateur a été verrouillé.
- Vous avez oublié ou perdu votre token/carte à puce.
- Le cache local de l'authentification au démarrage SafeGuard est partiellement endommagé.
- Un autre utilisateur doit démarrer l'ordinateur protégé par SafeGuard Enterprise.

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

- **Démarrage du client SafeGuard Enterprise sans connexion utilisateur :**

  Le démarrage 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 démarrer 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.

- **Démarrage 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 et qui ne sont pas connectés au contrôleur de domaine, certaines conditions doivent être prises en compte. Retrouvez plus d'informations à la section Challenge/Réponse pour les utilisateurs hors ligne à la page 80.

- **Restauration du cache de la stratégie 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. En revanche, la récupération de connexion peut être activée par stratégie, si le cache local doit effectivement être réparé avec une procédure Challenge/Réponse. Dans ce cas, il vous est demandé automatiquement de lancer une procédure Challenge/Réponse si le cache local est corrompu.

16.1.3 Procédure Challenge/Réponse

1. L'authentification au démarrage SafeGuard 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 SafeGuard. Un code de challenge sous la forme d'une chaîne de caractères ASCII est généré puis affiché.

3. Veuillez contacter le support.

   Fournissez au support technique vos données utilisateur (ID de l'utilisateur, ID de l'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 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 SafeGuard.

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

Vous pouvez reprendre vos activités.

16.1.4 Demande de challenge

1. Dans la boîte de dialogue de connexion de l'authentification au démarrage SafeGuard, 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 confidentiel.

   Remarque : si vous saisissez un mot de passe/code confidentiel 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 l'épellation**.

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

3. Cliquez sur **Suivant**.

16.1.5 Saisie de la réponse

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 l'authentification au démarrage SafeGuard.

Si nécessaire, SafeGuard Enterprise vous invite à modifier vos codes d'accès utilisateur Windows.

16.1.6 Bon usage

16.1.6.1 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 SafeGuard 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. Le responsable du support génère une réponse pour le démarrage sans connexion utilisateur.

   Le démarrage 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.

16.1.6.2 Vous avez oublié votre mot de passe

Nous vous conseillons d'utiliser les méthodes suivantes pour récupérer un mot de passe oublié. Ces méthodes vous évitent d'avoir à réinitialiser le mot de passe de manière centralisée :

- Utilisez Local Self Help. Grâce à la récupération avec Local Self Help, le mot de passe actuel peut être affiché et vous pouvez continuer à l'utiliser sans devoir le réinitialiser et sans demander l'assistance du support.

- 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 démarrer 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 SafeGuard.

16.1.6.3 Vous avez oublié ou perdu votre token

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 un token et un code confidentiel 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 token**

     Vous pouvez ignorer le changement de mot de passe en cliquant sur **Annuler** dans la boîte de dialogue si vous avez oublié votre token 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 token, vous pouvez uniquement vous connecter à partir de l'authentification au démarrage SafeGuard via la procédure Challenge/Réponse. Une fois votre token récupéré, vous pouvez l'utiliser pour vous connecter à partir de l'authentification au démarrage SafeGuard.

   - **Vous avez perdu votre token**

     En cas de perte de votre token, saisissez 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 un token à partir de l'authentification au démarrage SafeGuard n'est pas obligatoire), vous pouvez également vous connecter à partir de l'authentification au démarrage SafeGuard en utilisant ce mot de passe.

     L'interdiction d'utilisation du token ayant été trouvé peut être spécifiée. Des utilisateurs non autorisés ne peuvent pas utiliser le token pour se connecter (même s'ils connaissent le code confidentiel) puisque votre mot de passe a été changé.

16.1.6.4 Vous avez oublié votre code confidentiel

1. Si vous avez oublié le code confidentiel de votre token, 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 SafeGuard 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 confidentiel au token et stocker vos nouveaux codes d'accès de connexion sur celui-ci. Vous pouvez alors l'utiliser pour vous connecter.

16.1.6.5 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 SafeGuard 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 conseillons 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 à la récupération de l'accès à votre ordinateur.

16.1.7 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), il n'est pas possible de changer de mot de passe automatiquement pendant la procédure Challenge/Réponse.

16.1.7.1 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. Le responsable du support 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 SafeGuard.
2. Appelez le support technique et indiquez votre code de challenge.
3. Indiquez au responsable support que vous souhaitez démarrer 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 de démarrage continue SANS afficher le mot de passe.

   Le mot de passe s'affiche pendant 5 secondes. Le processus de démarrage 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'espacement**, 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 SafeGuard et pour vous connecter à Windows.

   Vous pouvez reprendre vos activités sur l'ordinateur.

16.1.7.2 Challenge/Réponse pour utilisateurs hors ligne avec le mode de connexion « Token uniquement »

Dans ce cas, si vous avez oublié votre code confidentiel ou oublié/perdu votre token, la procédure à utiliser n'est pas la même selon que vous connaissez vos codes d'accès Windows ou non.

- Vous connaissez vos codes d'accès Windows

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

  Le mode de connexion **Token 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 saisissant votre mot de passe Windows. Toutefois, la connexion à partir de l'authentification au démarrage SafeGuard est uniquement possible à l'aide de la procédure Challenge/Réponse.

- Vous ne connaissez pas vos codes d'accès Windows

  a) Si vous ne connaissez pas vos codes d'accès Windows et que vous avez oublié votre code confidentiel, 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 **Token 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 SafeGuard est uniquement possible à l'aide de la procédure Challenge/Réponse.

16.2 Challenge/Réponse pour les utilisateurs BitLocker

Consignes générales pour l'utilisation de la souris et/ou du clavier

- Vous pouvez sélectionner les commandes à l'aide de la souris et/ou du clavier. Pour passer d'une commande à une autre à l'aide du clavier, appuyez sur la touche de **Tabulation**. Pour revenir à la commande précédente, utilisez **Maj.+Tab**.
- Confirmez vos sélections en appuyant sur **Entrée**.

Procédure Challenge/Réponse

Si vous avez besoin d'une clé de récupération BitLocker, procédez de la manière suivante :

1. Redémarrez l'ordinateur. Suite au redémarrage, un message de couleur jaune apparaît. Appuyez sur n'importe quelle touche dans un délai de trois secondes.
2. L'écran Challenge/Réponse apparaît.
3. À l'étape 2, vous recevez les informations utiles pour appeler le service d'assistance.
4. Fournissez les informations suivantes au service d'assistance :

   Ordinateur. Par exemple, Sophos\<Nom de l'ordinateur>

Code du **challenge**. Par exemple, ABC12-3DEF4-56GHO-892UT-Z654K-LM321. Passez votre souris sur les caractères pour afficher une aide à l'épellation. Ou appuyez plusieurs fois sur **F1** pour afficher cette boîte de dialogue d'aide. Le code expire au bout de 30 minutes et entraîne l'arrêt automatique de l'ordinateur.

5. Saisissez ensuite le **Code de réponse** émis par le service d'assistance (six cases avec deux champs de texte de cinq caractères chacun à remplir par champ).
   - Lorsqu'un champ de texte est rempli, vous passez automatiquement au champ de texte suivant.
   - Si vous saisissez accidentellement un caractère erroné dans un case, celle-ci s'affiche en rouge. Utilisez la touche **Supprimer** ou **Retour arrière** pour corriger les entrées.
6. Après avoir saisi le code de réponse, cliquez sur **Continuer** ou appuyez sur **Entrée** pour terminer l'action de Challenge/Réponse.

Réinitialisation des codes d'accès BitLocker

Dès que vous êtes reconnecté au système, indiquez les nouveaux codes d'accès BitLocker afin de ne pas avoir à passer par une autre procédure Challenge/réponse à votre prochaine connexion. Selon votre système d'exploitation et sa version BIOS/UEFI, le système va afficher une boîte de dialogue de réinitialisation des codes d'accès.

Si cette boîte de dialogue n'apparaît pas automatiquement, cliquez avec le bouton droit de la souris sur l'icône SafeGuard Enterprise dans la barre des tâches. Un menu contextuel s'ouvre. Sélectionnez **Réinitialiser les codes d'accès BitLocker** et suivez les instructions à l'écran.

Remarque :

Si vous voulez arrêter ou redémarrer le système, cliquez sur le bouton d'arrêt ou appuyez sur la touche de **Tabulation** jusqu'à ce que le bouton d'arrêt soit sélectionné :

16.3 Clé de récupération BitLocker

En tant qu'utilisateur BitLocker sur un système ne prenant pas en charge le Challenge/Réponse de SafeGuard, vous avez la possibilité de demander une clé de récupération BitLocker à votre service d'assistance.

Consignes générales pour l'utilisation de la souris et/ou du clavier

- Vous pouvez sélectionner les commandes à l'aide de la souris et/ou du clavier. Pour passer d'une commande à une autre à l'aide du clavier, appuyez sur la touche de **Tabulation**. Pour revenir à la commande précédente, utilisez **Maj.+Tab**.
- Confirmez vos sélections en appuyant sur **Entrée**.

Demande de la clé de récupération

Si vous avez besoin de demander une clé de récupération BitLocker à votre service d'assistance, procédez de la manière suivante :

1. Redémarrez le système. Suite au redémarrage, appuyez sur la touche **Echap** lorsque l'écran de connexion BitLocker apparaît.

2. La boîte de dialogue de saisie d'une clé de récupération BitLocker s'ouvre.
3. À l'étape 2, vous recevez les informations utiles pour appeler le service d'assistance.

   Par exemple : <Nom de l'ordinateur> C: 9/25/2014

4. Communiquez le **Nom de l'ordinateur** au support technique.
5. Saisissez ensuite la **Clé de récupération BitLocker** fournie par le service d'assistance (huit cases de six caractères requis par champ).
6. Après avoir saisi le code de réponse, cliquez sur **Continuer** ou appuyez sur **Entrée** pour terminer l'action de récupération.

Réinitialisation des codes d'accès BitLocker

Dès que vous êtes reconnecté au système, indiquez les nouveaux codes d'accès BitLocker afin de ne pas avoir à passer par une autre procédure Challenge/réponse à votre prochaine connexion. Selon votre système d'exploitation et sa version BIOS/UEFI, le système va afficher une boîte de dialogue de réinitialisation des codes d'accès.

Si cette boîte de dialogue n'apparaît pas automatiquement, cliquez avec le bouton droit de la souris sur l'icône SafeGuard Enterprise dans la barre des tâches. Un menu contextuel s'ouvre. Sélectionnez **Réinitialiser les codes d'accès BitLocker** et suivez les instructions à l'écran.

Remarque :

Si vous voulez arrêter ou redémarrer le système, cliquez sur le bouton d'arrêt ou appuyez sur la touche de **Tabulation** jusqu'à ce que le bouton d'arrêt soit sélectionné :

17 SafeGuard Enterprise et Lenovo Rescue and Recovery

Remarque : Lenovo Rescue and Recovery est uniquement disponible pour les ordinateurs d'extrémité Windows 7.

Vous pouvez restaurer des sauvegardes complètes de système d'exploitation 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. Par exemple, lors d'un déplacement professionnel, les utilisateurs peuvent restaurer leur ordinateur avec Lenovo Rescue and Recovery.

Retrouvez plus d'informations sur les versions de Lenovo Rescue and Recovery (RnR) prises en charge par SafeGuard Enterprise, sur http://www.sophos.com/fr-fr/support/knowledgebase/108383.aspx

17.1 Présentation générale

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 d'ordinateurs 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. Il est donc inutile 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 depuis :

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

17.2 Configuration requise

- La plus récente version de BIOS pour ordinateur de bureau/portable.

- Retrouvez plus d'informations sur la compatibilité des versions Rescue and Recovery avec des versions SafeGuard Enterprise sur : http://www.sophos.com/fr-fr/support/knowledgebase/108383.aspx
- 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.

17.3 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 aborde 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.

17.3.1 Installation de Rescue and Recovery et de SafeGuard Enterprise

Il est conseillé 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 SafeGuard est activée afin qu'aucune sauvegarde non autorisée ne puisse être restaurée.

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

17.3.2 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).

17.4 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.

17.5 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.

17.6 Environnement de démarrage et options de récupération

SafeGuard Enterprise vous permet de démarrer dans l'environnement Rescue and Recovery après avoir réussi à vous connecter à l'authentification au démarrage (POA) SafeGuard.

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 démarrable ou de tout support amovible démarrable

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

17.7 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, veuillez consulter la documentation fournie par Lenovo.

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

- Disque dur local
- Disque dur secondaire
- Disque dur USB
- Réseau
- Clé de démarrage
- 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.

17.8 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 utiliser vos fichiers immédiatement.

17.9 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 » (ordinateurs portables Lenovo)
- Touche bleue « Entrée » (ordinateurs 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 « Entrée » du clavier du PC Lenovo.

      L'authentification au démarrage SafeGuard s'affiche.

   b) Saisissez les codes d'accès SafeGuard Enterprise.

2. Si vous n'utilisez pas un ordinateur Lenovo :
   a) Connectez-vous à l'authentification au démarrage SafeGuard 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 **Restaurer la sauvegarde**.

   Une boîte de dialogue s'affiche dans laquelle vous pouvez sélectionner la sauvegarde.
5. Sélectionnez la sauvegarde et restaurez-la.

17.10 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 des paramètres d'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. Retrouvez plus d'informations dans la documentation Lenovo.

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

Si l'authentification au démarrage SafeGuard 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.

Retrouvez plus d'informations sur l'activation de l'authentification Rescue and Recovery dans la documentation Lenovo Rescue and Recovery.

18 Support technique

Vous bénéficiez du support technique des produits Sophos de l'une des manières suivantes :

- Rendez-vous sur le forum de la communauté SophosTalk en anglais sur community.sophos.com et recherchez d'autres utilisateurs rencontrant le même problème que le vôtre.
- Rendez-vous sur la base de connaissances du support de Sophos sur www.sophos.com/fr-fr/support.aspx.
- Téléchargez la documentation des produits sur www.sophos.com/fr-fr/support/documentation/.
- Ouvrez un incident support sur https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx.

19 Mentions légales