SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise

Manuel d’utilisation

Version du produit : 8.3

Table des matières

1 À propos de SafeGuard Enterprise

Sophos SafeGuard assure la protection des terminaux Windows. Il est composé de plusieurs modules.

Il se peut que toutes les fonctions ne soient pas décrites dans ce manuel. Ceci dépend de votre licence et des stratégies que vous avez reçues de la part de votre responsable de la sécurité.

Sophos SafeGuard est configuré et administré de manière centralisée à partir de Sophos SafeGuard Management Center.

Pour accéder aux informations générales sur votre installation de Sophos SafeGuard, cliquez sur l’icône Sophos SafeGuard dans la Barre d’état système de Sophos SafeGuard (page 8).

Les options de chiffrement et de déchiffrement les plus importantes sont disponibles dans un menu par clic droit dans l’Explorateur Windows.

Le présent document mentionne uniquement l’utilisation avec des terminaux Windows. Retrouvez plus de renseignements sur les terminaux Mac dans le Manuel d’utilisation de SafeGuard Enterprise pour Mac.

Modules :

Chiffrement intégral du disque

Synchronized Encryption

Chiffrement de fichiers

2 Modules

2.1 Chiffrement intégral du disque avec BitLocker

Le chiffrement intégral du disque avec BitLocker est basé sur la technologie de Chiffrement de lecteur BitLocker disponible sur votre système d’exploitation. Le logiciel chiffre l’intégralité du disque dur afin que vos données soient en sécurité même en cas de perte ou de vol de votre ordinateur.

Lorsque vous vous connectez à votre terminal, vous devez saisir vos codes d’accès pour déverrouiller BitLocker. Retrouvez plus de renseignements à la section Chiffrer un ordinateur avec BitLocker (page 11).

Sophos SafeGuard vous permet de gérer BitLocker sur les terminaux exécutant l’un des systèmes d’exploitation suivants :

- Windows 8.1 Professional / Enterprise
- Windows 10 Professionnel / Entreprise

2.2 Chiffrement de fichiers SafeGuard (par application)

Le chiffrement de fichiers par application chiffre les fichiers créés ou modifiés par des applications spécifiques (par exemple ; Microsoft Word). Une stratégie définit une liste d’applications sur lesquelles le chiffrement de fichiers est exécuté automatiquement. Ce chiffrement étant permanent, vos fichiers sont sécurisés même lorsque vous les déplacez, les téléchargez chez un fournisseur de stockage Cloud ou les envoyez par email.

Si votre responsable de la sécurité a indiqué Microsoft Word en tant qu’application sur laquelle le chiffrement de fichiers est activé, tous les fichiers que vous allez créer et/ou enregistrer avec Microsoft Word sont chiffrés avec la clé définie. Tout utilisateur, dont le jeu de clés comprend cette clé, peut accéder à votre fichier.

- Les nouveaux fichiers créés avec des apps ou des extensions de fichier définies 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, vous ne pouvez pas lire son contenu.
- Si vous accédez à un fichier chiffré sur un ordinateur sur lequel le Chiffrement de fichiers n’est pas installé, vous ne pouvez pas lire ce fichier.
- Les fichiers sont copiés ou déplacés à partir d’un dossier non chiffrés dans un dossier sur lequel une règle de chiffrement s’applique.
- Les fichiers copiés ou déplacé d’un dossier chiffré vers un dossier non chiffré sont déchiffrés.
- Les fichiers qui sont copiés ou déplacés d’un dossier chiffré vers un dossier sur lequel une règle de chiffrement différente s’applique sont chiffrés conformément à la règle appliquée au dossier cible.
- Les fichiers sont créés par des applications pour lesquelles le chiffrement de fichiers n’est pas activé. Toutefois, une règle de chiffrement existe pour cette extension de fichier. Le fichier est

chiffré et ne peut pas être ouvert par l’application qui l’a créé. Par exemple, si vous créez un fichier .doc avec OpenOffice et qu’OpenOffice ne figure pas dans les **Listes d’application**.

Important
Si la copie ou le déplacement de fichiers est interrompue (en cas de redémarrage par exemple), l’opération ne sera pas reprise automatiquement. Par conséquent, il se peut que des fichiers ne soient pas chiffrés involontairement. Retrouvez plus de renseignements sur la manière de garantir que les fichiers sont toujours chiffrés correctement à la section Chiffrer des fichiers en fonction de la stratégie (page 13).

Retrouvez plus de renseignements sur les emplacements chiffrés sur un ordinateur à la section Afficher l’emplacement dans lequel les fichiers sont chiffrés (page 15).

Retrouvez plus de renseignements sur l’état du chiffrement d’un ou de plusieurs fichiers en cliquant avec le bouton droit de la souris sur le(s) fichier(s) et en sélectionnant **Chiffrement de fichiers SafeGuard > Afficher l’état du chiffrement**.

Dans l’Explorateur Windows, les fichiers chiffrés sont identifiés par un verrou de couleur verte. Si aucun symbole de verrou n’est affiché alors que le fichier est chiffré, veuillez consulter l’article 108784 de la base de connaissances de Sophos.

2.3 Chiffrement de fichiers SafeGuard (par emplacement)

Le chiffrement de fichiers par emplacement permet à votre responsable de la sécurité de définir les emplacements dans lesquels les fichiers seront chiffrés comme par exemple les **Documents**.

Après l’assignation d’une stratégie **Chiffrement de fichiers** de type **Basé sur emplacement** 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 se trouvant dans un emplacement destiné au chiffrement 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, vous ne pouvez pas lire son contenu.
- Si vous accédez à un fichier chiffré sur un ordinateur sur lequel le Chiffrement de fichiers n’est pas installé, vous ne pouvez pas lire ce fichier.

Retrouvez plus de renseignements sur les emplacements chiffrés sur votre ordinateur à la section Afficher l’emplacement dans lequel les fichiers sont chiffrés (page 15).

Retrouvez plus de renseignements sur l’état du chiffrement d’un ou de plusieurs fichiers en cliquant avec le bouton droit de la souris sur le(s) fichier(s) et en sélectionnant **Chiffrement de fichiers SafeGuard > Afficher l’état du chiffrement**.

Dans l’Explorateur Windows, les fichiers chiffrés sont identifiés par un verrou de couleur verte. Si aucun symbole de verrou n’est affiché alors que le fichier est chiffré, veuillez consulter l’article 108784 de la base de connaissances de Sophos.

2.4 SafeGuard Cloud Storage

SafeGuard Cloud Storage offre le chiffrement par emplacement des fichiers stockés dans le Cloud. Il ne change en rien la façon dont vous utilisez vos fichiers. En revanche, il 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.

SafeGuard Cloud Storage détecte automatiquement votre fournisseur de stockage Cloud (s’il est compatible) et applique la stratégie de chiffrement au dossier de synchronisation.

SafeGuard Cloud Storage n’exécute pas de chiffrement initial de vos données. Les fichiers stockés avant que SafeGuard Cloud Storage ne soit installé ou activé par une stratégie restent déchiffrés. Si vous voulez chiffrer ces fichiers, vous devez d’abord les supprimer du Cloud et les ajouter de nouveau.

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 en clair. Pour vous assurer que ces fichiers seront chiffrés, 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.

2.5 SafeGuard Data Exchange

SafeGuard Data Exchange offre le chiffrement par emplacement des fichiers stockés sur des supports amovibles afin de pouvoir les échanger avec d’autres utilisateurs. Seuls les utilisateurs disposant des clés appropriées peuvent lire le contenu des données chiffrées. Tous les processus de chiffrement et de déchiffrement sont exécutés de manière transparente et impliquent une intervention minimale de l’utilisateur.

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.

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

2.5.1 Icônes superposées

Les icônes superposées sont des icônes de petite taille affichées sur les éléments dans l’Explorateur Windows. Elles sont destinées à vous donner des informations rapides sur l’état de chiffrement des fichiers. L’apparence des icônes varie en fonction du module que vous avez installé.

Les icônes superposées de Data Exchange apparaissent uniquement sur les fichiers et volumes.

- 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 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.

Remarque
Si aucune icône superposée n’est affichée, veuillez consulter l’article 108784 de la base de connaissances Sophos.

2.5.2 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.

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.

2.5.3 Phrase secrète des supports amovibles

SafeGuard Data Exchange permet de définir une phrase secrète unique des supports 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 des supports sur chaque ordinateur.

Retrouvez plus de renseignements sur la création d’une phrase secrète des supports à la section Utilisation d’une phrase secrète des supports (page 21).

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 des supports, 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.

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 indiqué, 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 est compatible avec les supports multimédia 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

Disques Blu-ray et DVD DL incompatibles.

3 Barre d’état système de Sophos SafeGuard

Vous avez accès à toutes les fonctions du terminal Sophos SafeGuard sur votre ordinateur en cliquant sur l’icône de la barre d’état du système Sophos SafeGuard à partir de votre barre d’état Windows. La disponibilité des fonctions spécifiques dépend des modules que vous avez installés.

Cliquez avec le bouton droit de la souris sur l’icône de la zone de notification de Sophos SafeGuard pour voir :

- **Affichage** :
  - **Jeu de clés** : affiche toutes les clés disponibles.

    Remarque
    Si votre terminal 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 les informations relatives à votre certificat.
  - **Certificat d’entreprise** : affiche les informations relatives à votre certificat d’entreprise.
- **Réinitialiser les codes d’accès BitLocker** : ouvre une boîte de dialogue vous permettant de changer votre code confidentiel BitLocker.
- **Créer une nouvelle clé** : ouvre une boîte de dialogue permettant de créer une clé utilisée pour SafeGuard Data Exchange (page 4) ou pour SafeGuard Cloud Storage (page 3). Uniquement disponible si l’un des deux modules est installé sur votre ordinateur.
- **Changer la phrase secrète des supports** : ouvre une boîte de dialogue pour changer la phrase secrète des supports comme indiqué à la section SafeGuard Data Exchange (page 4).
- **Synchroniser** : lance la synchronisation avec le serveur SafeGuard Enterprise. Des infobulles affichent la progression de la synchronisation. Vous pouvez également cliquez deux fois sur l’icône de la barre d’état système pour lancer la synchronisation.
- **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	Date et heure auxquelles l’ordinateur a reçu une nouvelle stratégie.
Dernière clé reçue	Date et heure auxquelles l’ordinateur a reçu une nouvelle clé.
Dernier certificat reçu	Date et heure auxquelles l’ordinateur a reçu un nouveau certificat.
Dernier contact du serveur	Date et heure du dernier contact avec le serveur.

Champ	Informations
État de l’utilisateur SGN	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. Ceci signifie que la synchronisation initiale de l’utilisateur 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’assignation 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 au terminal et à devenir des utilisateurs SGN. — **Invité SGN** Les utilisateurs invités SGN ne sont pas ajoutés à l’assignation 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. — **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’assignation utilisateur/machine. Ils sont donc autorisés à se connecter à Windows depuis ce terminal. — **Utilisateur non confirmé** Les utilisateurs non confirmés n’ont pas accès au jeu de clés pour l’une des raisons suivantes : – L’utilisateur a fourni des codes d’accès incorrects. – L’utilisateur est un utilisateur local. – Le serveur d’authentification AD est injoignable. – L’authentification a échoué. Retrouvez également plus de renseignements

Champ	Informations
État de la machine SGN	Indique le niveau de sécurité du terminal. — **non applicable** La fonction associée est inactive. — **machine sécurisée** Le diagnostic de la machine indique qu’elle est sécurisée. — **machine compromise** Le diagnostic de la machine indique qu’elle n’est pas sécurisée. Les clés ont donc été révoquées et vous ne pouvez pas accéder aux fichiers chiffrés.
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 assigné un nouveau certificat pour la connexion par token sur votre ordinateur. Vous pouvez maintenant modifier le certificat pour la connexion par token. Retrouvez plus de renseignements dans le Manuel d’utilisation de SafeGuard Enterprise.

- **Aide** : ouvre l’aide en ligne de SafeGuard Enterprise.
- **À propos de SafeGuard Enterprise** : affiche les informations sur la version de SafeGuard Enterprise que vous utilisez.

4 Comment faire pour...

4.1 Chiffrer un ordinateur avec BitLocker

Selon le mode de connexion indiqué par le responsable de la sécurité pour votre terminal, 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 terminal 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 le lecteur flash 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 va pas commencer et vous ne serez plus invité à chiffrer ce volume jusqu’à ce que :

- Une nouvelle stratégie soit appliquée.
- L’état du chiffrement BitLocker d’un volume change.
- Vous vous reconnectiez au système.

4.1.1 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. Nous vous conseillons d’utiliser un lecteur flash USB non chiffré pour stocker la clé. Les lecteurs de destination valides pour la clé de démarrage sont répertoriés dans la boîte de dialogue. Plus tard, vous devrez insérer le périphérique de stockage avec la clé à chaque démarrage de l’ordinateur.

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

4.1.2 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
Faites attention lors de la création d’un code confidentiel ou d’un mot de passe. L’environnement préalable au démarrage prend uniquement en charge la disposition de clavier Anglais (États-Unis) ou EN-US. Si vous créez un code confidentiel ou un mot de passe avec des caractères spéciaux, vous devrez utiliser des touches différentes lors de sa saisie à votre prochaine connexion.

4.1.3 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
Faites attention lors de la création d’un code confidentiel ou d’un mot de passe. L’environnement préalable au démarrage prend uniquement en charge la disposition de clavier Anglais (États-Unis) ou EN-US. Si vous créez un code confidentiel ou un mot de passe avec des caractères spéciaux, vous devrez utiliser des touches différentes lors de sa saisie à votre prochaine connexion.

4.1.4 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.

4.2 Réinitialiser en cas d’oubli du code confidentiel/ mot de passe BitLocker

Si vous ne pouvez pas vous connecter à votre ordinateur en raison de l’oubli de votre code confidentiel, de votre mot de passe ou de votre clé USB, vous allez avoir besoin d’une clé de récupération. Pour demander une clé de récupération :

1. Redémarrez votre ordinateur et appuyez sur la touche **Échap** sur l’écran de connexion **BitLocker**.
2. Sur l’écran **Récupération BitLocker**, recherchez l’**ID de la clé de récupération**.
   L’**ID de la clé de récupération** s’affiche uniquement pendant un court moment. Pour l’afficher de nouveau, veuillez redémarrer l’ordinateur.
3. Contactez votre administrateur et communiquez-lui l’**ID de la clé de récupération**.
   Votre administrateur doit trouver la clé de récupération de votre ordinateur dans Sophos SafeGuard Management Center et vous la communiquer.
4. Sur l’écran **Récupération BitLocker**, saisissez la clé de récupération.
   Vous pouvez à présent démarrer votre ordinateur.

Dés que vous êtes de nouveau connecté au système, indiquez les nouveaux codes d’accès BitLocker. Selon votre système d’exploitation, une boîte de dialogue de réinitialisation des codes d’accès apparaît. Si cette boîte de dialogue n’apparaît pas automatiquement, cliquez avec le bouton droit de la souris sur l’icône Sophos SafeGuard de la barre des tâches et sélectionnez **Réinitialiser les codes d’accès BitLocker** puis suivez les instructions à l’écran.

4.3 Réinitialiser par Challenge/Réponse en cas d’oubli du code confidentiel/mot de passe BitLocker

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. Déplacez le curseur de votre souris sur les caractères pour afficher l’aide à l’épellation ou appuyez plusieurs fois sur la touche **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 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).
   - Dès que le champ de texte est entièrement 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.
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

Dés que vous êtes de nouveau connecté au système, indiquez les nouveaux codes d’accès BitLocker. Selon votre système d’exploitation, une boîte de dialogue de réinitialisation des codes d’accès apparaît. Si cette boîte de dialogue n’apparaît pas automatiquement, cliquez avec le bouton droit de la souris sur l’icône Sophos SafeGuard de la barre des tâches et sélectionnez **Réinitialiser les codes d’accès BitLocker** puis suivez les instructions à l’écran.

4.4 Chiffrer des fichiers en fonction de la stratégie

Après assignation d’une stratégie de **Chiffrement de fichiers** 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 terminal reçoit une stratégie de Chiffrement de fichiers même si le responsable de la sécurité peut automatiquement lancer cette tâche de chiffrement.

Pour commencer l’opération de chiffrement manuel : cliquez avec le bouton droit de la souris sur le nœud **Poste de travail** dans l’Explorateur Windows et sélectionnez **Chiffrement de fichiers SafeGuard > Chiffrer en fonction de la stratégie**. L’Assistant de Chiffrement de fichiers SafeGuard (page 14) chiffre tous les fichiers dans les dossiers et sous-dossiers soumis aux règles de chiffrement définies.

4.4.1 Assistant de Chiffrement de fichiers SafeGuard

Pour ouvrir l’assistant de Chiffrement de fichiers SafeGuard, cliquez avec le bouton droit de la souris sur le nœud **Poste de travail** ou sur un dossier dans l’Explorateur Windows et sélectionnez **Chiffrement de fichiers SafeGuard > Chiffrer en fonction de la stratégie**.

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 en cours d’utilisation.
- Les fichiers chiffrés qui doivent être en clair 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 ou traités. 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.

4.5 Chiffrer/déchiffrer manuellement des fichiers

SafeGuard File Encryption vous permet de chiffrer ou de déchiffrer chaque fichier manuellement. Cliquez avec le bouton droit de la souris sur un fichier et sélectionnez **Chiffrement de fichiers SafeGuard**. Les fonctions suivantes sont disponibles :

- **Afficher l’état du chiffrement** : indique si le fichier est chiffré ou non ainsi que la clé utilisée.
- **Chiffrer en fonction de la stratégie** : Retrouvez plus de renseignements à la section Chiffrer des fichiers en fonction de la stratégie (page 13).

- **Déchiffrer** : (uniquement pour le chiffrement de fichiers par emplacement) : Vous permet de déchiffrer un fichier qui ne fait pas l’objet d’une règle de chiffrement de fichiers.
- **Déchiffrer le fichier sélectionné** (uniquement pour le chiffrement de fichiers par application) : vous permet de déchiffrer votre fichier et de l’archiver en texte clair. Nous vous conseillons de déchiffrer votre fichier uniquement s’il ne contient aucune donnée sensible.
- **Chiffrer le fichier sélectionné** (uniquement pour le chiffrement de fichiers par application) : vous permet de chiffrer manuellement les fichiers avec la clé définie dans votre stratégie.
- **Créer un fichier protégé par mot de passe** : vous permet de définir un mot de passe pour chiffrer manuellement chaque fichier. Ceci s’avère utile si vous voulez partager votre fichier en toute sécurité avec une personne n’appartenant pas au réseau de votre entreprise. Retrouvez plus de renseignements à la section Envoyer des fichiers chiffrés par email (page 17).

Si vous cliquez avec le bouton droit de la souris sur des dossiers ou lecteurs, les fonctions suivantes sont disponibles :

- **Afficher l’état du chiffrement** : affiche une liste de fichiers inclus avec des icônes indiquant l’état du chiffrement et la clé utilisée.
- **Chiffrer en fonction de la stratégie** : Retrouvez plus de renseignements à la section Chiffrer des fichiers en fonction de la stratégie (page 13).

Les options suivantes sont uniquement disponibles pour les modules « Cloud Storage » et « Data Exchange » :

- **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 **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.

4.6 Afficher l’emplacement dans lequel les fichiers sont chiffrés

Si vous voulez vérifier l’emplacement dans lequel les fichiers sont chiffrés sur votre ordinateur et quelles clés sont utilisées pour protéger vos fichiers, vous pouvez utiliser l’outil SafeGuard Enterprise `FETool`.

Pour ouvrir l’outil SafeGuard Enterprise `FETool`, ouvrez une invite de commande, allez dans `C:\Program Files (x86)\Sophos\SafeGuard Enterprise\FileEncryption` et saisissez `fetool rli -a`.

Cette commande répertorie toutes les règles de chiffrement s’appliquant à votre ordinateur. La liste contient le mode de chiffrement, le chemin complet vers les dossiers et les clés utilisées.

4.7 Utiliser un mot de passe pour protéger un fichier

Lors de l’envoi d’emails à des destinataires n’appartenant pas au réseau de votre entreprise, nous vous conseillons de chiffrer votre fichier avec un mot de passe. Les destinataires ont accès aux fichiers chiffrés sans avoir besoin d’installer SafeGuard Enterprise.

Procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur le fichier que vous voulez envoyer et sélectionnez **Créer un fichier protégé par mot de passe**.
2. Suivez les instructions à l’écran pour créer un mot de passe. Nous vous conseillons d’utiliser un mot de passe fort et ne pas l’envoyer dans le même email que les fichiers.
   Votre fichier est chiffré et enregistré en tant que fichier HTML. Vous pouvez à présent joindre en toute sécurité le fichier HTML à vos emails.

   Remarque
   - Le chiffrement nécessite de l’espace disque.
   - Le fichier HTML chiffré est de plus grande taille que le fichier original.
   - La taille de fichier maximale prise en charge est de 50 Mo.
   - Pour envoyer plusieurs fichiers en même temps, vous pouvez les compresser dans un fichier .zip et chiffrer ce fichier .zip.

3. Communiquez le mot de passe aux destinataires par téléphone ou par tout autre moyen de communication.
   Les destinataires peuvent utiliser l’un des navigateurs suivants pour ouvrir la pièce jointe protégée par mot de passe :
   - Mozilla Firefox
   - Google Chrome
   - Microsoft Internet Explorer 11
   - Microsoft Edge
4. Demandez aux destinataires de cliquer deux fois sur le fichier et de suivre les instructions affichées à l’écran pour procéder de l’une des manières suivantes :
   - Saisissez le mot de passe et cliquez sur **Entrée** pour accéder au fichier.
   - Cliquez sur **Protéger un nouveau fichier par mot de passe** pour protéger un autre fichier par mot de passe.

Les destinataires ont accès au fichier que vous avez protégé par mot de passe. Ils peuvent protéger le fichier par mot de passe lorsqu’ils vous le renvoie. Ils ont la possibilité d’utiliser le même mot de passe ou d’en utiliser un nouveau. Ils peuvent même protéger un nouveau fichier par mot de passe.

4.8 Envoyer des fichiers chiffrés par email

Lorsque vous envoyez des fichiers chiffrés aux destinataires du réseau de votre entreprise, vous n’avez pas à vous soucier du chiffrement et du déchiffrement. Si votre destinataire possède la bonne clé, il pourra lire le fichier.

Pour envoyer des emails à des destinataires n’appartenant pas à votre réseau professionnel, SafeGuard Enterprise offre un complément pour Microsoft Outlook qui permet de chiffrer les pièces jointes aux emails en toute simplicité. Lorsque vous envoyez un email avec un ou plusieurs fichiers joints, le système vous invite à choisir la méthode d’envoi des pièces jointes. Les options disponibles varient en fonction de l’état du chiffrement des fichiers que vous avez joint à votre email.

Remarque
Lorsque vous envoyez des éléments incorporés tels que des contacts (.vcf) ou des emails (.msg) en tant que pièces jointes, vous n’êtes pas invité à les chiffrer. Ils sont envoyés déchiffrés.

- **Protégé par mot de passe**

  Sélectionnez cette option si vous envoyez des fichiers sensibles à des destinataires ne faisant pas partie de votre entreprise.

  Après avoir créé un mot de passe et appuyé sur Envoyer, votre fichier est chiffré et enregistré en tant que fichier HTML. Si vous protégez plusieurs fichiers par mot de passe en même temps, chaque fichier sera chiffré séparément avec le même mot de passe. Les fichiers qui sont déjà chiffrés sont déchiffrés automatiquement avant d’être protégés par mot de passe.

  Les destinataires peuvent ouvrir le fichier avec leur navigateur Web dès que vous leur avez communiqué le mot de passe. Nous vous conseillons d’utiliser un mot de passe fort et ne pas l’envoyer dans le même email que les fichiers. Nous vous conseillons de communiquer le mot de passe aux destinataires par téléphone ou par tout autre moyen de communication.

  Les destinataires peuvent utiliser l’un des navigateurs suivants pour ouvrir la pièce jointe protégée par mot de passe :

  — Mozilla Firefox

  — Google Chrome

  — Microsoft Internet Explorer 11

  — Microsoft Edge

  Le déchiffrement avec d’autres navigateurs tel que les navigateurs mobiles peut fonctionner mais n’est pas entièrement pris en charge.

  Les destinataires peuvent modifier le fichier et le renvoyer en utilisant le même mot de passe ou en créant un nouveau. Ils peuvent même protéger un nouveau fichier par mot de passe. Un assistant de leur navigateur les aide à suivre la bonne procédure. Retrouvez plus de renseignements dans l’article 124440 de la base de connaissances de Sophos.

  Vous pouvez également protéger les fichiers par mot de passe manuellement comme indiqué à la section Utiliser un mot de passe pour protéger un fichier (page 16).

- **Non protégé**

  Sélectionnez cette option uniquement si votre pièce jointe ne contient aucune donnée sensible. Toutes les fois où vous enverrez des pièces jointes non protégées dans un email pourront être consignées dans un journal et surveillées par votre responsable de la sécurité.

- **Pièces jointes à envoyer dans l’état**

Si l’email contient des pièces jointes ne pouvant pas être protégées par mot de passe, vous pouvez les envoyer dans l’état ou les supprimer de votre email. La boîte de dialogue contient une liste de fichiers qui ne peuvent pas être protégés pour l’une des raisons suivantes :

— Le fichier est déjà protégé par mot de passe. Vous pouvez soit commencer par déchiffrer le fichier et utiliser un nouveau mot de passe, soit envoyer le fichier dans l’état et communiquer le mot de passe au destinataire.

— Le fichier est chiffré avec une clé qui n’est pas actuellement disponible dans votre jeu de clés. La clé peut avoir été temporairement révoquée en raison d’un problème de sécurité ou vous n’êtes pas en possession de la clé utilisée pour chiffrer le fichier. Dans ce cas, veuillez la demander à votre responsable de la sécurité.

Lorsque vous envoyez un email à des destinataires internes et externes en même temps, le système traite l’email comme s’il était envoyé à des domaines externes.

4.9 Créer une clé locale

Les clés locales servent à chiffrer les fichiers dans des emplacements spécifiques sur un périphérique amovible ou chez un fournisseur de stockage Cloud. Ces emplacements doivent déjà être inclus dans une stratégie de chiffrement.

Pour créer une clé locale :

1. Cliquez avec le bouton droit de la souris sur l’icône Sophos SafeGuard 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 fichiers SafeGuard > Chiffrer**

en fonction de la stratégie 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.

4.9.1 Importer clés à partir d’un fichier

Si vous avez reçu des supports amovibles contenant des données chiffrées ou voulez accéder aux données de stockage Cloud 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 fichiers SafeGuard > 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.

4.10 Échanger des données avec 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 qui n’ont pas SafeGuard Enterprise sur leur ordinateur peuvent utiliser SafeGuard Portable pour accéder aux fichiers chiffrés. SafeGuard Portable n’est pas compatible avec les ordinateurs Macs. Retrouvez plus de renseignements sur :

  — Échange de données sur des supports multimédia amovibles sans SafeGuard Enterprise (page 21)

  — Modifier des fichiers avec SafeGuard Portable (page 25)

4.10.1 Chiffrement des supports amovibles par SafeGuard Data Exchange

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 fichiers SafeGuard > Chiffrer en fonction de la stratégie** dans le menu contextuel du périphérique 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 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.

Annuler le 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 indiquée 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.

Le chiffrement initial ne démarre pas sur les ordinateurs sur lesquels votre phrase secrète des supports n’est pas paramétrée.

4.10.2 Utilisation d’une phrase secrète des supports

Si l’utilisation d’une phrase secrète des supports a été indiquée 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.

Veuillez noter que vous ne pouvez pas utiliser une phrase secrète des supports sur des Macs.

Changement/réinitialisation d’une 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.

Synchronisation d’une 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. Veuillez noter que vous ne pouvez pas utiliser une phrase secrète des supports sur des Macs.

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).

4.10.3 Échange de données sur des supports multimédia amovibles sans SafeGuard Enterprise

SafeGuard Portable vous permet d’échanger des données chiffrées sur des supports multimédia amovibles avec des destinataires qui n’ont pas SafeGuard Enterprise.

Remarque
SafeGuard Portable n’est pas compatible avec les ordinateurs Macs ou avec les ordinateurs sur lesquels Sophos SafeGuard est installé.

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.

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.

Les destinataires peuvent déchiffrer les données et les chiffrer de nouveau dès que vous leur communiquez la phrase secrète des supports ou la phrase secrète d’une clé locale. Ils peuvent 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 d’installer SafeGuard Portable sur l’ordinateur des destinataires. Il reste sur le support amovible.

Retrouvez plus de renseignements à la section Modifier des fichiers avec SafeGuard Portable (page 25).

4.10.4 Écriture des fichiers sur CD-ROM/DVD avec SafeGuard Data Exchange

SafeGuard Data Exchange vous permet de graver des fichiers chiffrés sur des CD/DVD à l’aide de l’Assistant Graver un CD de Windows. Votre responsable de la sécurité doit définir une règle de chiffrement pour le lecteur d’enregistrement sur CD. 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 clair.

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**. 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.

Dans l’Assistant Graver un CD, vous pouvez y indiquer la méthode de gravure des fichiers sur CD (chiffrés ou en clair). 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 clair 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 de nouveau chiffrés et les fichiers en texte clair 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 sur CD en clair

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.

4.11 Échanger des données dans le Cloud sans SafeGuard Enterprise

SafeGuard Portable vous permet d’échanger des données chiffrées dans le Cloud avec des destinataires qui n’ont pas SafeGuard Enterprise.

SafeGuard Portable vous permet d’accéder aux données chiffrées dans votre stockage Cloud à partir d’ordinateurs sur lesquels SafeGuard Enterprise n’est pas 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. 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 d’installer ou de copier SafeGuard Portable sur l’ordinateur du partenaire avec lequel vous communiquez. Il reste dans le stockage Cloud.

Retrouvez une description détaillée de l’utilisation de SafeGuard Portable à la section Modifier des fichiers avec SafeGuard Portable (page 25).

Un fichier ne peut pas être déchiffré en cliquant deux fois dessus ou en sélectionnant la commande d’ouverture. En effet, les fichiers déchiffrés dans les dossiers de synchronisation du stockage Cloud sont automatiquement synchronisés dans 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 sont pas effectuées dans les fichiers d’origine chiffrés.

Remarque
Ne stockez pas les dossiers de synchronisation du stockage Cloud sur un support amovible ou sur le réseau. Si vous le faites, SafeGuard Portable crée des fichiers déchiffrés dans ces dossiers.

4.12 Utiliser des clés 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.

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 Cloud.

Vous pouvez définir la clé par défaut à partir du menu contextuel dans les emplacements suivants :

- Supports amovibles
- Fichiers sur supports amovibles
- Dossiers ou sous-dossiers de synchronisation du stockage Cloud
- Fichiers dans un dossier ou sous-dossier de synchronisation du stockage Cloud
- 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 fichiers SafeGuard > Définir la clé par défaut**.

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 de stockage Cloud. Si vous voulez utiliser une autre clé, vous pouvez en définir une nouvelle par défaut à tout moment.

Si une clé locale est sélectionnée pour le chiffrement de stockage Cloud, SafeGuard Portable sera copié dans le dossier de synchronisation stockage Cloud.

Si vous envisagez de lire les fichiers chiffrés sur les appareils Android et iOS à l’aide de Sophos Secure Workspace, veuillez utiliser les clés locales pour procéder au chiffrement. Retrouvez plus de renseignements dans l’Aide de Sophos Secure Workspace.

Exemple

Vous voulez utiliser Dropbox pour fournir des données sécurisées à vos différents partenaires et pour donner à chacun de vos partenaires accès à un sous-dossier uniquement. Il vous suffit de définir une clé par défaut différente pour chaque sous-dossier. SafeGuard Enterprise ajoutera automatiquement une copie de SafeGuard Portable, ce qui donnera aux partenaires n’utilisant pas SafeGuard Cloud Storage d’accéder 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.

4.13 Récupérer des fichiers chiffrés

Si un fichier est chiffré à l’aide d’une clé qui ne se trouve pas dans votre jeu de clés, vous ne pouvez pas ouvrir le fichier. Il se peut que vous ne soyez pas autorisé à accéder à ce fichier conformément à la stratégie de votre entreprise. Toutefois, dans certains cas, vous êtes autorisé à accéder au fichier mais vous n’êtes tout simplement pas en possession de la clé nécessaire pour le faire. Dans ce cas, vous devez découvrir quelle clé a été utilisée et demander à votre responsable de la sécurité d’ajouter la clé à votre jeu de clés. Veuillez procéder comme suit :

1. Cliquez sur le fichier avec le bouton droit de la souris et cliquez sur **Chiffrement de fichiers SafeGuard > Afficher l’état du chiffrement**.
   La clé utilisée pour le chiffrement du fichier s’affiche.
2. Veuillez contacter votre responsable de la sécurité et lui communiquer le nom de la clé.
3. Veuillez demander à votre responsable de la sécurité d’ajouter la clé à votre jeu de clés.
4. Dès que votre responsable de la sécurité vous a confirmé que votre stratégie d’utilisateur a été mise à jour, cliquez avec le bouton droit de la souris sur l’icône de la barre d’état du système de Sophos SafeGuard dans la barre des tâches de votre ordinateur.
5. Cliquez sur **Synchroniser**.
6. Cliquez de nouveau avec le bouton droit de la souris sur l’icône de la barre d’état du système et cliquez sur **État**.
   Une boîte de dialogue affiche la date de transfert de la dernière clé sur votre ordinateur. La date actuelle est affichée sous **Dernière clé reçue** lorsque la clé que vous avez demandée a été ajoutée à votre jeu de clés.

Vous pouvez à présent accéder au fichier.

4.14 Vérifier la connexion au serveur SafeGuard Enterprise

Si vous rencontrez des problèmes de synchronisation de votre terminal avec le serveur, utilisez l’outil de vérification de la connexion client/serveur (Client/Server Connectivity Check) pour obtenir plus de renseignements sur les raisons de l’échec de la communication entre le terminal et le serveur SafeGuard Enterprise.

Pour ouvrir l’outil SafeGuard Enterprise Client/Server Connectivity Check, allez dans `C:\Program Files (x86)\Sophos\SafeGuard Enterprise\Client` et exécutez l’application `SGNCSCC.exe`.

Retrouvez plus de renseignements dans l’article 109662 de la base de connaissances de Sophos.

4.15 Modifier des fichiers avec SafeGuard Portable

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

Vous avez reçu 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`.

SafeGuard Portable vous permet de déchiffrer les données chiffrées et de les chiffrer de nouveau.

En plus des informations sur le fichier, SafeGuard Portable affiche également 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. Vous ne pouvez déchiffrer des fichiers que si vous connaissez la phrase secrète correspondant à la clé utilisée.

2. Pour modifier un fichier, cliquez dessus avec le bouton droit de la souris et sélectionnez l’une des commandes suivantes :

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 avec la dernière clé utilisée.
Déchiffrer	Ouvre la boîte de dialogue **Saisir la phrase secrète** pour saisir la phrase secrète de déchiffrement du fichier sélectionné.
État du chiffrement	Affiche l’état du chiffrement du fichier.
Copier dans	Copie le fichier dans un dossier de votre choix et le déchiffre.
Supprimer	Supprime le fichier sélectionné.

Vous pouvez également sélectionner les commandes **Ouvrir**, **Supprimer**, **Chiffrer**, **Déchiffrer** et **Copier** à l’aide des icônes de la barre d’outils.

4.15.1 Définir des clés de chiffrement pour SafeGuard Portable

Pour définir une clé de chiffrement pour SafeGuard Portable :

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.
3. 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.

4.15.2 Chiffrer des fichiers avec SafeGuard Portable

1. Dans SafeGuard Portable, cliquez avec le bouton droit de la souris sur le fichier et sélectionnez **Chiffrer**.

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

   Lors de l’enregistrement de nouveaux fichiers en utilisant l’opération glisser-déposer, il vous sera demandé si vous souhaitez les chiffrer.

   Si aucune clé par défaut n’est définie, une boîte de dialogue concernant ce paramètre s’ouvre. Saisissez le nom de la clé et de la phrase secrète, confirmez la phrase secrète et cliquez sur **OK**.
2. Pour chiffrer plus de fichiers avec la clé que vous venez de définir, sélectionnez **Chiffrer** dans le menu contextuel ou dans le menu **Fichier**.

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.

4.15.3 Déchiffrer des fichiers avec SafeGuard Portable

1. Dans SafeGuard Portable, cliquez avec le bouton droit de la souris sur le fichier et 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, indépendamment de la clé locale utilisée pour les chiffrer. Si vous disposez uniquement de la phrase secrète d’une clé locale, vous avez uniquement accès 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 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.

Les fichiers ayant été déchiffrés seront chiffrés automatiquement lors de la fermeture de SafeGuard Portable.

5 Support

Sortie officielle

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

- Rendez-vous sur le forum Sophos Community 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.aspx.
- Ouvrez un incident support sur https://secure2.sophos.com/fr-fr/support/contact-support/support-query.aspx.

6 Mentions légales