SOPHOS

Cybersecurity made simple.

SafeGuard Enterprise pour Mac

Manuel d’utilisation

Version du produit : 8.3

Table des matières

1 À propos de SafeGuard Enterprise pour Mac

Sophos SafeGuard assure la protection des Macs. Il est composé de :

- SafeGuard Native Device Encryption (page 1) qui protège votre ordinateur avec la technologie de chiffrement FileVault.
- SafeGuard File Encryption (page 2) qui vous permet de chiffrer les fichiers avec une clé ou un mot de passe.

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. Retrouvez plus de renseignements sur l’administration de Sophos Safeguard Enterprise sur la page de documentation.

Pour accéder aux informations générales sur votre installation de Sophos SafeGuard, cliquez sur l’icône Sophos SafeGuard dans le menu système et ouvrez la Fenêtre de préférences de Sophos SafeGuard (page 5).

Les options de chiffrement et de déchiffrement les plus importantes sont disponibles dans un menu par clic droit dans le Finder.

Important
Avant de mettre à jour votre système d’exploitation, assurez-vous que votre version de Sophos SafeGuard est compatible avec la version la plus récente du système d’exploitation. Retrouvez plus de renseignements dans les Notes de publication de SafeGuard Enterprise. Si vous procédez d’abord à la mise à jour de votre système d’exploitation; vous risquez de perdre l’accès à vos données.

1.1 SafeGuard Native Device Encryption

Sophos SafeGuard Native Device Encryption est basé sur la technologie de chiffrement des disques FileVault intégrée à 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.

SafeGuard Native Device Encryption fonctionne en tâche de fond. Vous n’avez pas besoin de chiffrer ou de déchiffrer les fichiers lors de leur ouverture, modification ou enregistrement.

Retrouvez plus de renseignements sur votre installation en ouvrant l’Onglet Chiffrement du disque (page 7) dans la fenêtre de préférences de Sophos SafeGuard.

SafeGuard Native Device Encryption vous permet de :

- Chiffrer un ordinateur (page 9)
- Déchiffrer un ordinateur (page 9)
- SafeGuard Native Device Encryption et SafeGuard File Encryption (page 10)
- Vérifier la connexion au serveur SafeGuard Enterprise (page 16)

1.2 SafeGuard File Encryption

SafeGuard File Encryption permet à votre responsable de la sécurité de définir les fichiers à chiffrer sur votre ordinateur et les autorisations de lecture de ces fichiers. Il y a deux moyens de définir les fichiers à chiffrer :

- Chiffrement de fichiers par emplacement (page 3)
- Chiffrement de fichiers par application (page 3)

Les stratégies de Chiffrement de fichiers sont assignées aux utilisateurs et pas aux ordinateurs. Généralement, les stratégies de Chiffrement indiquent que les fichiers dans vos dossiers comme par exemple le dossier **Documents** sont chiffrés. Toutefois, votre responsable de la sécurité peut définir des dossiers dans lesquels les fichiers demeurent non chiffrés. Retrouvez plus de renseignements sur les emplacements chiffrés sur votre ordinateur dans l’Onglet Stratégie (page 6) de la fenêtre de préférences.

Dans le Finder, les fichiers chiffrés sont identifiés par un verrou de couleur verte. Les fichiers n’affichant aucun symbole sont généralement déchiffrés.

Remarque
Les fichiers qui ont été enregistrés en tant que groupes ou packages n’afficheront peut être pas d’icône superposée même s’ils sont chiffrés. Par exemple, lorsque vous insérez un fichier image chiffré dans un fichier texte chiffré dans TextEdit et que vous l’enregistrez en tant que RTF (Rich Text Document) avec des pièces jointes, le fichier créé apparaît déchiffré. Toutefois, il est bien chiffré.

Suite à l’installation du logiciel de chiffrement et à l’établissement de la communication avec le serveur SafeGuard Enterprise, vous êtes invité à saisir votre mot de passe macOS. Vous devez également avoir un certificat personnel. Ce certificat est généré sur le serveur SafeGuard Enterprise lorsque vous saisissez le mot de passe. Cette opération est uniquement requise suite à l’installation du produit, à la première connexion ou à la réinitialisation du mot de passe.

Dès que SafeGuard File Encryption est installé, assurez-vous d’appliquer toutes les stratégies que votre responsable de la sécurité vous a assignées comme indiqué à la section Chiffrer les fichiers en fonction de la stratégie (page 11).

SafeGuard File Device Encryption vous permet de :

- Chiffrer les fichiers en fonction de la stratégie (page 11)
- Chiffrer/déchiffrer des fichiers manuellement (page 12)
- Envoyer des fichiers chiffrés par email (page 12)
- Utiliser un mot de passe pour protéger un fichier (page 13)
- Chiffrer des fichiers sur les périphériques amovibles (page 14)
- Récupérer des fichiers chiffrés (page 16)

Accord de l’utilisateur sur macOS 10.14

À partir de macOS 10.14, les applications doivent obtenir l’accord de l’utilisateur pour contrôler d’autres applications. Suite à l’installation, macOS affiche un message **« Sophos SafeGuard » demande l’accès pour contrôler le « Finder »** vous invitant à l’autoriser ou à le refuser. Cliquez sur **OK** car vous avez besoin du Finder pour le bon fonctionnement de SafeGuard File Encryption.

Une entrée va être ajoutée à la section **Automatisation** de vos paramètres **Confidentialité** permettant à SafeGuard File Encryption d'automatiser le Finder.

Si vous cliquez sur **Ne pas autoriser**, cette boîte de dialogue n'apparaîtra plus et SafeGuard File Encryption ne pourra plus utiliser le Finder.

Pour modifier les paramètres ultérieurement, allez dans la section **Automatisation** de vos paramètres **Confidentialité** et sélectionnez le **Finder** sous **Sophos SafeGuard** pour autoriser SafeGuard File Encryption à contrôler le Finder.

1.2.1 Chiffrement de fichiers 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. Ces emplacements sont appelés Dossiers sécurisés (page 4). Retrouvez plus de renseignements sur les emplacements chiffrés sur votre ordinateur dans l'Onglet Stratégie (page 6) de la fenêtre de préférences.

- Les nouveaux fichiers se trouvant dans un emplacement destiné au chiffrement sont chiffrés automatiquement.
- Si vous déplacez un fichier non chiffré dans un emplacement destiné au chiffrement, ce fichier est chiffré.
- Si vous déplacez un fichier chiffré dans un emplacement exclus du chiffrement, ce fichier est déchiffré.
- 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 ce fichier ni le déplacer dans un autre emplacement.
- 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.

1.2.2 Chiffrement de fichiers 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. Le chiffrement de fichiers par application s'applique à tous les Dossiers sécurisés (page 4). Par ailleurs, votre responsable de la sécurité peut exclure des emplacements spécifiques du chiffrement. Retrouvez plus de renseignements sur les emplacements chiffrés sur votre ordinateur dans l'Onglet Stratégie (page 6) de la fenêtre de préférences.

- Les nouveaux fichiers créés par des apps spécifiques sont chiffrés automatiquement.
- Les fichiers modifiés par des apps spécifiques 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.
- Si vous accédez à un fichier chiffrés par une application qui n'est pas définie dans votre stratégie, vous ne pouvez pas lire son contenu.

1.2.3 Dossiers sécurisés

Les Dossiers sécurisés sont des emplacements sur votre Mac, sur les partages réseau ou sur les périphériques amovibles dans lesquels les fichiers sont chiffrés. Votre responsable de la sécurité définit vos Dossiers sécurisés dans une stratégie. Généralement, il s’agit des dossiers Documents et de dossiers temporaires dans lesquels sont archivés les pièces jointes de messages Microsoft Outlook et Apple Mail.

Avec macOS Catalina, SafeGuard Enterprise a besoin de votre autorisation pour accéder aux dossier Documents, Bureau, Photos et Apple Mail.

Suivez ces étapes pour permettre à SafeGuard Enterprise d’accéder à ces dossiers :

1. Ouvrir **Sécurité et confidentialité**.
2. Déverrouillez pour faire vos changements.
3. Sélectionnez **Accès intégral au disque**.
4. Cliquez sur le bouton + pour ajouter ces deux applis SafeGuard au volet **Accès intégral au disque** :
   - sgd dans le dossier `/usr/local/bin/`
   - Sophos SafeGuard dans le dossier `/Library/Sophos SafeGuard FS`

Restrictions

- **Fichiers chiffrés uniquement accessibles dans les Dossiers sécurisés**

  Vous ne pouvez pas accéder à un fichier chiffré se trouvant hors d’un Dossier sécurisé. Vous devez soit le déplacer dans un Dossier sécurisé soit le déchiffrer manuellement.

- **Stockage permanent des versions indisponibles dans les Dossiers sécurisés**

  Pour les fichiers dans les Dossiers sécurisés, la fonctionnalité de base **Parcourir toutes les versions...** n’est pas disponible.

- **Recherche de fichiers**

  — Par défaut, la recherche de fichiers dans les Dossiers sécurisés avec Spotlight n’est pas possible. Retrouvez plus de renseignements sur la prise en charge de Spotlight à la section Recherche de fichiers chiffrés (page 15).

  — La recherche des fichiers identifiés ne fonctionne pas dans les Dossiers sécurisés.

- **Partage des Dossiers sécurisés**

  Un dossier sécurisé ne peut pas être partagé sur le réseau.

2 Fenêtre de préférences de Sophos SafeGuard

Suite à l’installation de Sophos SafeGuard Enterprise pour Mac, l’icône Sophos SafeGuard apparaît dans les **Préférences Système** :

Cliquez sur l’icône pour ouvrir la fenêtre des préférences Sophos SafeGuard.

L’onglet **À propos de** apparaît. Il contient toutes les informations sur la version du produit installée sur votre Mac.

2.1 Onglet Serveur

L’onglet **Serveur** contient les informations et fonctionnalités suivantes associées au serveur SafeGuard Enterprise :

Informations sur le serveur

- **Intervalle de contact :** temps entre les synchronisations avec le serveur.
- **Dernier contact :** date de la dernière synchronisation avec le serveur.
- **URL du serveur principal :** URL de connexion au serveur principal.
- **URL du serveur secondaire :** URL de connexion au serveur secondaire.
- **Vérification du serveur :** indique si la vérification du serveur SSL pour établir la communication avec le serveur est activée.

Faire glisser le fichier ZIP de configuration ici

Faites glisser le fichier ZIP de configuration dans cette zone pour appliquer les informations de configuration du serveur SafeGuard Enterprise au Mac.

Synchroniser

Cliquez sur ce bouton pour synchroniser manuellement avec le serveur SafeGuard Enterprise.

Vérifier la connexion

Cliquez sur ce bouton pour vérifier votre connexion au serveur SafeGuard Enterprise.

Certificat d’entreprise

- **Valide à compter du :** date de début de validité du certificat.
- **Valide jusqu’au :** date de fin de validité du certificat.
- **Émetteur :** instance ayant émis le certificat.
- **N° de série :** numéro de série du certificat de l'entreprise.

2.2 Onglet Utilisateur

L’onglet **Utilisateur** affiche les informations suivantes :

- Votre **Nom d’utilisateur**.

- L’annuaire du **Domaine** auquel appartient votre Mac. Le nom de l’ordinateur local est affiché pour les utilisateurs locaux.
- Le **GUID de l’utilisateur SafeGuard** qui a été généré lors de votre première connexion.
- L’**État d’utilisateur SGN** indique si vous êtes un **Utilisateur SGN** ou un **Utilisateur non confirmé**. Un utilisateur non confirmé n’a pas accès ou ne peut pas créer de fichiers chiffrés. Dans ce cas, veuillez demander à votre responsable de la sécurité de confirmer votre compte.

Le second volet de la fenêtre affiche les informations sur le **Certificat de l’utilisateur** : Ceci s’applique uniquement au chiffrement de fichiers.

- **Valide à compter du :** date de début de validité du certificat.
- **Valide jusqu’au :** date de fin de validité du certificat.
- **Émetteur :** instance ayant émis le certificat.
- **N° de série :** numéro de série du certificat.

Dans la troisième section de la fenêtre, vous pouvez choisir d’afficher l’icône de chaque composant dans le menu système. Ces options sont uniquement disponibles lorsque le composant correspondant est installé.

- **Afficher le menu système de Native Device Encryption**
- **Afficher le menu système de File Encryption**

2.3 Onglet Clés

Cet onglet apparaît uniquement si SafeGuard File Encryption est installé.

L’onglet **Clés** affiche tous les noms de clé existants dans une liste.

Cliquez sur l’icône de la liste dans le coin inférieur droit située à côté de **Nombre de clés** pour masquer ou afficher les informations GUID des clés.

Vous pouvez répertorier et trier les clés à l’aide de l’un des éléments d’en-tête **Nom de la clé** ou **GUID de la clé**.

Une clé de couleur bleue signifie que vous êtes le propriétaire de cette clé. Les clés locales apparaissent en couleur verte (voir la section Utiliser des clés locales (page 15)). Toutes les autres clés (standard) apparaissent en couleur noire.

2.4 Onglet Stratégie

Cet onglet apparaît uniquement si SafeGuard File Encryption est installé.

Sous l’onglet **Stratégies**, cliquez sur l’une des icônes dans le coin inférieur droit pour permuter entre la vue **Chemin converti localement** et la vue **Stratégies reçues**.

- La vue **Chemin converti localement** affiche uniquement les stratégies s’appliquant actuellement à l’utilisateur connecté sur un ordinateur Mac spécifique. Les colonnes du tableau incluent les informations suivantes :
  - @ : lors de la première opération de chiffrement ou du chiffrement de fichiers de grande taille, vous allez voir une roue tourner dans la première colonne.
  - **Chemin converti localement** : affiche l’emplacement de votre Mac.
  - **Mode** : indique si un emplacement est défini pour être chiffré ou être exclus du chiffrement.
  - **Portée** : indique si les sous-dossiers d’un emplacement doivent être chiffrés.

- **Nom de la clé** : affiche le nom de la clé assignée à l'emplacement indiqué.

  Votre clé personnelle apparaît en couleur bleue.

  Une clé de couleur orange signifie qu'elle a été configurée dans une stratégie qui vous a été assignée. En revanche, vous n'êtes pas propriétaire de cette clé car elle n'a pas été assignée à votre jeu de clés. Ceci peut entraîner des problèmes d'accès aux données. Dans ce cas, veuillez contacter votre responsable de la sécurité.

- La vue **Stratégies reçues** affiche toutes les stratégies reçues du serveur. Le tableau répertorie les informations suivantes :
  - **Stratégies reçues** : indique les fichiers ou dossiers à chiffrer.
  - Toutes les autres colonnes affichent les informations mentionnées ci-dessus à propos de la vue du **Chemin converti localement**.

Appliquer les stratégies dans la vue Chemin converti localement

- Lorsqu'aucune stratégie n'est sélectionnée, cliquez sur le bouton **Appliquer toutes les stratégies** pour lancer la première opération de chiffrement. Retrouvez plus de renseignements à la section Chiffrer les fichiers en fonction de la stratégie (page 11).
- Lorsque vous sélectionnez une stratégie, vous pouvez cliquer sur le bouton **Appliquer la stratégie** pour appliquer uniquement la stratégie sélectionnée.
- Lorsque vous sélectionnez une stratégie, vous pouvez cliquer sur le bouton **Afficher dans le Finder** pour ouvrir le Dossier sécurisé sélectionné dans le Finder.

Résultats éventuels suite à l'application des stratégies

- Les fichiers en clair sont chiffrés avec la clé assignée par une stratégie.
- Les fichiers déjà chiffrés avec la clé de indiquée dans la stratégie demeurent chiffrés.
- Les fichiers déjà chiffrés avec une autre clé
  - Ne sont pas modifiés si la clé requise ne se trouve pas dans le jeu de clés de l'utilisateur ou
  - Sont chiffrés à nouveau avec la clé de chiffrement assignée par une stratégie si celle-ci se trouve dans le jeu de clés de l'utilisateur.
- Les fichiers dans les dossiers qui sont exclus de la stratégie de chiffrement sont déchiffrés.
- Les fichiers qui ne sont pas accessibles en raison de l'absence d'autorisations (lecture seule) ne sont pas modifiés.

2.5 Onglet Chiffrement du disque

Cet onglet apparaît uniquement si SafeGuard Native Device Encryption est installé.

L'onglet **Chiffrement du disque** contient des informations sur les stratégies en cours d'utilisation et sur l'état de chiffrement de votre Mac.

Le premier volet vous indique si le disque système doit être chiffré conformément à la stratégie définie par le responsable de la sécurité.

Le second volet affiche l'état du Mac. Il peut s'agir de l'un des suivants :

- Le disque système est chiffré et une clé de récupération stockée de manière centralisée est disponible.
- Le disque système est chiffré mais aucune clé de récupération stockée de manière centralisée n’est disponible.
- Le disque système n’est pas chiffré.

En bas de la fenêtre, le bouton **Déchiffrer le disque système** apparaît. Il est disponible si le responsable de la sécurité a défini une stratégie stipulant que le chiffrement n’est pas nécessaire pour le terminal.

3 Comment faire pour...

3.1 Chiffrer un ordinateur

Lorsque votre responsable de la sécurité vous assigne une stratégie de Chiffrement de périphériques, une boîte de dialogue vous invite à saisir votre mot de passe macOS. Le chiffrement de votre ordinateur commence.

1. Saisissez votre mot de passe macOS.
2. Cliquez sur **Activer** ou sur **Activer et redémarrer**.

   Les Macs utilisant le format Apple File System (APFS) n’ont pas besoin d’être redémarrés. Par conséquent, seule l’option **Activer** est disponible.

Le chiffrement de disque s’effectue en fond de tâche afin de vous permettre de continuer à travailler. Retrouvez plus de renseignements à la section SafeGuard Native Device Encryption (page 1).

S’il est impossible d’activer le chiffrement, veuillez contacter l’administrateur système.

3.2 Déchiffrer un ordinateur

Il n’est généralement pas nécessaire de déchiffrer. Si le responsable de la sécurité définit une stratégie stipulant qu’aucun chiffrement n’est nécessaire pour votre Mac déjà chiffré, celui-ci restera chiffré. Par contre, vous aurez la possibilité de le déchiffrer. Utilisez le bouton correspondant dans le volet des préférences. Retrouvez plus de renseignements à la section Onglet Chiffrement du disque (page 7).

3.3 Réinitialisation du mot de passe en cas d’oubli

La procédure de réinitialisation du mot de passe en cas d’oubli dépend du type de chiffrement installé sur votre Mac :

- SafeGuard Native Device Encryption (page 9)
- SafeGuard Native Device Encryption et SafeGuard File Encryption (page 10)

3.3.1 SafeGuard Native Device Encryption

Si vous avez oublié votre mot de passe macOS, procédez de la manière suivante :

1. Allumez votre Mac.
2. Cliquez sur le point d’interrogation dans le champ **Mot de passe**.
   Votre mémo de mot de passe apparaît et vous invite à réinitialiser votre mot de passe à l’aide de votre clé de récupération.
3. Cliquez sur la flèche à côté du message pour passer dans le champ de la clé de récupération.
4. Contactez votre responsable de la sécurité pour lui demander votre clé de récupération.
5. Saisissez votre clé de récupération dans le champ correspondant et cliquez sur l’icône en forme de flèche sur le côté droit.

Le Mac démarre et la boîte de dialogue **Réinitialisation du mot de passe** apparaît.

6. Si vous êtes un utilisateur Active Directory, demandez à votre administrateur de réinitialiser votre mot de passe puis demander un nouveau mot de passe.
   a) Assurez-vous que votre ordinateur est connecté aux services de domaine Active Directory.
   b) Dans la boîte de dialogue **Réinitialisation du mot de passe**, cliquez sur **Annuler** et saisissez votre nouveau mot de passe.
   c) Modifiez votre mot de passe si nécessaire.
7. Si vous êtes un utilisateur local de macOS, saisissez un nouveau mot de passe et un mémo de mot de passe, puis cliquez sur **Réinitialiser le mot de passe**.
8. Si le système ne peut pas déverrouiller votre jeu de clés de connexion, cliquez sur **Créer un nouveau jeu de clés**.
9. Un Mac sous macOS 10.13 et avec un disque système APFS pourrait nécessiter l’utilisation d’un nouveau mot de passe afin de créer un nouveau mot de passe de récupération. Lorsque vous y êtes invité, saisissez le mot de passe.

   La boîte de dialogue apparaît uniquement si vous êtes connecté au serveur SafeGuard Enterprise. En l’absence de connexion, elle apparaîtra la prochaine fois qu’une connexion sera établie.

3.3.2 SafeGuard Native Device Encryption et SafeGuard File Encryption

Ces instructions supposent que vous avez installé SafeGuard Native Device Encryption et SafeGuard File Encryption sur votre Mac. Si vous utilisez uniquement l’un des logiciels ci-dessus, les étapes à suivre peuvent être différentes.

Si vous avez oublié votre mot de passe macOS, procédez de la manière suivante :

1. Allumez votre Mac.
2. Cliquez sur le point d’interrogation dans le champ **Mot de passe**.
   Votre mémo de mot de passe apparaît et vous invite à réinitialiser votre mot de passe à l’aide de votre clé de récupération.
3. Cliquez sur la flèche à côté du message pour passer dans le champ de la clé de récupération.
4. Contactez votre responsable de la sécurité pour lui demander votre clé de récupération. Votre responsable de la sécurité doit également supprimer votre certificat d’utilisateur dans SafeGuard Management Center.
5. Saisissez votre clé de récupération dans le champ correspondant et cliquez sur l’icône en forme de flèche sur le côté droit.
   Le Mac démarre et la boîte de dialogue **Réinitialisation du mot de passe** apparaît.
6. Si vous êtes un utilisateur Active Directory, demandez à votre administrateur de réinitialiser votre mot de passe puis demander un nouveau mot de passe.
   a) Assurez-vous que votre ordinateur est connecté aux services de domaine Active Directory.
   b) Dans la boîte de dialogue **Réinitialisation du mot de passe**, cliquez sur **Annuler** et saisissez votre nouveau mot de passe.
   c) Modifiez votre mot de passe si nécessaire.
7. Si vous êtes un utilisateur local de macOS, saisissez un nouveau mot de passe et un mémo de mot de passe, puis cliquez sur **Réinitialiser le mot de passe**.
8. Cliquez sur **Créer un nouveau jeu de clés**.
   Un nouveau jeu de clés de connexion est créé. Veuillez noter que toutes les entrées existantes de votre jeu de clés demeurent valides.

9. Un Mac sous macOS 10.13 et avec un disque système APFS pourrait nécessiter l'utilisation d'un nouveau mot de passe afin de créer un nouveau mot de passe de récupération. Lorsque vous y êtes invité, saisissez le mot de passe.

   La boîte de dialogue apparaît uniquement si vous êtes connecté au serveur SafeGuard Enterprise. En l'absence de connexion, elle apparaîtra la prochaine fois qu'une connexion sera établie.
10. Saisissez votre nouveau mot de passe pour créer le certificat d'utilisateur SafeGuard.
    Si vous êtes un utilisateur Active Directory, vos clés vont être chargées automatiquement dans le jeu de clés SafeGuard Enterprise. Vous avez accès à vos documents comme auparavant.
11. Si vous êtes un utilisateur local, veuillez demander à votre responsable de la sécurité de confirmer l'enregistrement de l'utilisateur.
12. Ouvrez l'onglet **Serveur** dans la Fenêtre de préférences et cliquez sur **Synchroniser**.

Vos clés sont restaurées et vous avez de nouveau accès à vos documents chiffrés.

3.4 Enregistrer la clé de récupération de Device Encryption centralement

Si aucune clé de récupération centrale n'est disponible, le support technique ne pourra pas vous aider à récupérer votre mot de passe. Pour mettre la clé de récupération à disposition, veuillez l'importer à l'aide de l'outil de ligne de commande : `sgdeadmin --import-recoverykey`. Le responsable de la sécurité peut vous fournir la clé de récupération sur demande.

Si vous ne connaissez pas la clé de récupération, veuillez contacter votre responsable de la sécurité. En effet, si vous avez oublié votre mot de passe de connexion et qu'aucune clé de récupération n'est disponible, toutes les données archivées sur le disque chiffré seront perdues.

3.5 Chiffrer les fichiers en fonction de la stratégie

Votre responsable de la sécurité utilise les stratégies pour définir les fichiers à chiffrer et les clés à utiliser. Pour garantir que les fichiers sensibles sur votre ordinateur sont chiffrés, nous vous conseillons de procéder au chiffrement initial. Ceci signifie que toutes les stratégies auxquelles votre responsable de la sécurité vous a assigné seront appliquées. Pour lancer un chiffrement initial :

1. Ouvrez les **Préférences Système**.
2. Cliquez sur l'icône Sophos SafeGuard.
3. Sélectionnez l'onglet **Stratégies**.
4. Passez dans la vue **Chemin converti localement** et cliquez sur **Appliquer toutes les stratégies**.

Tous les fichiers se trouvant dans les Dossiers sécurisés (page 4) sont chiffrés ou chiffrés de nouveau avec la clé indiquée dans la stratégie.

Si vous voulez appliquer une seule stratégie, sélectionnez-la et cliquez sur **Appliquer la stratégie**.

Si vous voulez chiffrer des fichiers ou des dossiers individuellement conformément à la stratégie, cliquez avec le bouton droit de la souris sur un fichier ou un dossier et sélectionnez **Chiffrer en fonction de la stratégie**.

3.6 Chiffrer/déchiffrer des fichiers manuellement

SafeGuard File Encryption vous permet de chiffrer ou de déchiffrer chaque fichier manuellement. Cliquez sur un fichier avec le bouton droit de la souris et effectuez l’une des opérations suivantes :

- **Afficher l’état du chiffrement** : indique si le fichier est chiffré ou non ainsi que la clé utilisée.
- **Chiffrer en fonction de la stratégie** : les fichiers sélectionnés sont chiffrés ou chiffrés de nouveau avec la clé indiquée dans une stratégie.
- **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 Utiliser un mot de passe pour protéger un fichier (page 13). Cette option est uniquement disponible pour les fichiers qui ne sont pas chiffrés ou qui sont chiffrés avec une clé disponible dans votre jeu de clés.

3.7 Voir l’emplacement dans lequel les fichiers sont chiffrés

Votre responsable de la sécurité utiliser les stratégies pour définir les emplacements sur votre ordinateur dans lesquels les fichiers sont chiffrés et ceux dans lesquels ils ne le sont pas. Pour obtenir plus d’informations sur vos stratégies :

1. Ouvrez les **Préférences Système**.
2. Cliquez sur l’icône Sophos SafeGuard.
3. Sélectionnez l’onglet **Stratégies** comme indiqué à la section Onglet Stratégie (page 6).

3.8 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.

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 comme indiqué à la section Utiliser un mot de passe pour protéger un fichier (page 13).

Si vous envoyez des fichiers à des destinataires n’appartenant pas au réseau de votre entreprise et que vous ne voulez pas utiliser la protection par mot de passe, veuillez d’abord déchiffrer le fichier. Autrement, les destinataires ne pourront pas accéder aux fichiers chiffrés.

3.9 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**.
   Si vous recevez un message d’erreur, sélectionnez **Affichage > Masquer l’aperçu** dans le Finder et réessayez.
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.

3.10 Chiffrer des fichiers dans le Cloud

Sophos SafeGuard chiffre automatiquement vos fichiers dans le Cloud si les conditions sont satisfaites :

- Votre administrateur a indiqué que les fichiers dans les dossiers de stockage Cloud sont chiffrés.
- Le dossier de stockage Cloud n’est pas dans un Dossier sécurisé (voir la section Dossiers sécurisés (page 4)).
- Vous utilisez l’un des fournisseurs de stockage Cloud compatibles :
  - Boîte
  - Dropbox
  - Google Drive
  - Microsoft OneDrive
  - Microsoft OneDrive Entreprise

Pour savoir si votre dossier de stockage Cloud est chiffré, vérifiez l’onglet **Stratégies** dans la fenêtre de préférences comme indiqué à la section Onglet Stratégie (page 6).

Remarque

- Vous allez voir les icônes superposées de Sophos SafeGuard sur les fichiers chiffrés à la place des icônes du fournisseur de stockage Cloud.
- Vous ne pouvez pas voir ou modifier les fichiers chiffrés dans le Cloud en même temps que d’autres utilisateurs.

3.11 Chiffrer des fichiers sur les périphériques amovibles

Lorsque vous connectez un périphérique amovible à votre ordinateur, une boîte de dialogue vous demande de sélectionner la manière dont vous voulez traiter les fichiers sur le périphérique. Vous avez le choix entre les options suivantes :

1. Sélectionnez **Mémoriser le paramètre et ne plus afficher cette boîte de dialogue** et cliquez sur **Non**.
   Les fichiers ne seront jamais chiffrés sur le périphérique.
2. Sélectionnez **Mémoriser le paramètre et ne plus afficher cette boîte de dialogue** et cliquez sur **Oui**.
   Tous les nouveaux fichiers que vous enregistrerez sur le périphérique seront chiffrés automatiquement.
3. Sélectionnez **Chiffrer les fichiers existants** et cliquez sur **Oui**.
   Les fichiers déjà présents sur le périphérique seront chiffrés tant que le périphérique sera connecté à votre ordinateur.
4. Sélectionnez **Mémoriser le paramètre et ne plus afficher cette boîte de dialogue** et **Chiffrer les fichiers existants** et cliquez sur **Oui**.
   Les fichiers déjà présents sur votre périphérique ainsi que tous les nouveaux fichiers seront toujours chiffrés automatiquement.

3.12 Échanger des fichiers chiffrés sur des périphériques amovibles

Vous pouvez utiliser des périphériques amovibles tels que les lecteurs flash USB ou les disques durs externes pour échanger des fichiers chiffrés.

Pour échanger et modifier des données présentes sur les périphériques amovibles entre deux personnes, la stratégie et la clé adéquates doivent leur avoir été assignées.

Pour tout échange de données entre les terminaux macOS et Windows, le périphérique doit impérativement être formaté à l’aide de FAT32. Tout autre format de fichier fonctionnera avec des fonctionnalités limitées. Le format de fichier ne pouvant pas être affiché dans le Finder, veuillez utiliser l’Utilitaire de disque pour vérifier le système de fichiers.

Si vous échangez des fichiers plus volumineux sur les périphériques amovibles, assurez-vous d’avoir assez un espace libre disponible correspondant à deux fois la taille du plus gros fichier à échanger.

Sur les appareils amovibles qui sont également utilisés pour les sauvegardes Time Machine, le répertoire `Backups.backupdb` est exclus automatiquement du chiffrement.

3.13 Utiliser des clés locales

Les clés locales sont uniquement disponibles pour le Chiffrement de fichiers par emplacement (page 3).

Les clés locales servent à chiffrer les fichiers dans les dossiers 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. Assurez-vous que votre terminal est connecté au serveur SafeGuard Enterprise comme indiqué à la section Onglet Serveur (page 5).
2. Cliquez avec le bouton droit de la souris sur un fichier ou sur une série de fichiers et sélectionnez **Créer une nouvelle clé**.
3. Choisissez un nom et une phrase secrète pour votre clé et cliquez sur **OK**.

   Le nom de la clé est préfixé par « Local_ » et suivi de la date et de l’heure.

La clé locale est créée et ajoutée à votre jeu de clés. Vous pouvez à présent appliquer la clé locale à un périphérique amovible ou à un dossier de stockage Cloud.

3.14 Recherche de fichiers chiffrés

Si vous voulez rechercher les fichiers chiffrés, vous devez activer Spotlight manuellement.

1. Pour activer la recherche Spotlight, veuillez exécuter la commande du Terminal suivante :

   ```
   sgfsadmin --enable-spotlight
   ```
2. Pour désactiver la recherche Spotlight, veuillez exécuter la commande du Terminal suivante :

   ```
   sgfsadmin --disable-spotlight
   ```


Remarque
L’utilisation de Spotlight avec Sophos SafeGuard risque de ralentir la vitesse de recherche.

3.15 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 avec le bouton droit de la souris et sélectionnez **Afficher l’état du chiffrement** dans le menu contextuel.
   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 le responsable de la sécurité vous confirme que la stratégie d’utilisateur a été mise à jour, allez dans **Préférences système > Sophos SafeGuard > Serveur**.
5. Cliquez sur le bouton **Synchroniser**.
6. Ouvrez l’onglet **Clés** et assurez-vous que la clé requise figure dans la liste.

Si la clé utilisée pour chiffrer le fichier en question figure dans la liste sur l’onglet **Clés**, vous pouvez accéder au fichier.

3.16 Vérifier la connexion au serveur SafeGuard Enterprise

Si vous rencontrez des problèmes de synchronisation de votre terminal avec le serveur SafeGuard Enterprise, procédez comme suit :

1. Ouvrez le Fenêtre de préférences de Sophos SafeGuard (page 5) et cliquez sur le Onglet Serveur (page 5).
2. Cliquez sur le bouton **Vérifier la connexion**.
   La fenêtre **Vérifier la connectivité Client-Serveur de SafeGuard Enterprise** s’ouvre.
3. Cliquez sur **Exécuter**.
   Le système vérifie la connexion au serveur SafeGuard Enterprise.
4. Cliquez sur le bouton **Exporter** en bas de la fenêtre pour enregistrer les résultats dans un fichier texte.
5. Si la connexion au serveur SafeGuard Enterprise échoue, veuillez contacter votre administrateur.

4 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.

5 Mentions légales