SOPHOS

Security made simple.

Sophos SafeGuard File Encryption pour Mac

Manuel d'administration

Version du produit : 7

Date du document : décembre 2014

Table des matières

1 À propos de Sophos SafeGuard File Encryption pour Mac

Sophos SafeGuard File Encryption pour Mac étend la protection des données offerte par Sophos SafeGuard Enterprise sur Windows aux utilisateurs de Macs. Il offre le chiffrement des fichiers sur les lecteurs locaux, les partages réseaux, les lecteurs amovibles et dans le Cloud.

SafeGuard File Encryption pour Mac vous permet de chiffrer et de déchiffrer les fichiers puis d'échanger ces fichiers avec d'autres utilisateurs sur les ordinateurs Macs ou Windows.

Pour lire les fichiers chiffrés par SafeGuard Enterprise sur des appareils mobiles, veuillez utiliser Sophos Mobile Encryption pour iOS ou Android.

Dans SafeGuard Management Center, vous définissez les règles du chiffrement basé sur fichier dans les règles File Encryption. Dans les règles File Encryption, vous indiquez les dossiers qui doivent être gérés par File Encryption, le mode de chiffrement et la clé à utiliser pour le chiffrement. Grâce à cette administration centralisée, vous pouvez être sûr que les mêmes dossiers et clés de chiffrement sont traités sur des plates-formes différentes.

1.1 À propos de ce document

Le présent document vous explique comment installer, configurer et gérer Sophos SafeGuard File Encryption pour Mac.

Retrouvez plus d'informations sur le fonctionnement de SafeGuard Management Center et sur le paramétrage des règles dans le *Manuel d'administration de SafeGuard Enterprise*.

Retrouvez plus d'informations sur l'utilisation du logiciel dans le *Guide de démarrage rapide de Sophos SafeGuard File Encryption pour Mac*.

1.2 Terminologie et acronymes

La terminologie et les acronymes ci-dessous sont utilisés dans le présent document :

Terme ou acronyme	Signification ou explication
FUSE	Système de fichiers sur l'espace de l'utilisateur ou « Filesystem in Userspace » (http://osxfuse.github.io/)
GUID	Globally Unique Identifier (identifiant unique universel) : un numéro de référence unique utilisé en tant qu'identifiant dans les logiciels informatiques.
Dossier sécurisé	Un Dossier sécurisé est un dossier sur lequel est appliqué une règle qui a été créée dans SafeGuard

Terme ou acronyme	Signification ou explication
	Management Center. Cette règle indique que le contenu du dosser sera chiffré.
Sophos	Secure Sockets Layer : un protocole cryptographique permettant d'établir des communications sécurisées sur Internet.

2 Installation

Le chapitre suivant décrit l'installation de Sophos SafeGuard File Encryption sur les clients Mac OS X. Retrouvez plus d'informations sur la procédure d'installation de l'environnement d'administration (serveur backend) dans le *Guide d'installation de SafeGuard Enterprise*.

Deux types d'installation du client Mac OS X sont disponibles :

- Installation manuelle (sous surveillance).
- Installation automatisée (sans surveillance).

Remarque : si vous avez installé SafeGuard Disk Encryption 6.01 ou une version antérieure, veuillez la désinstaller avant d'installer la version 7 de SafeGuard File Encryption pour Mac.

Si vous voulez utiliser SafeGuard File Encryption et SafeGuard Native Device Encryption (appelé SafeGuard Disk Encryption jusqu'à la version 6.10), vous devez utiliser la version 7 de ces deux logiciels. L'utilisation de versions différentes de ces produits sur un Mac n'est pas prise en charge.

Le package du programme d'installation est signé et OS X va essayer de valider cette signature. Si la connexion à Internet est lente ou mal configurée, la procédure d'installation peut être retardée d'au moins 20 minutes.

2.1 Conditions préalables à l'installation

Avant de procéder à l'installation, assurez-vous que le certificat du serveur SafeGuard Enterprise-SSL a été importé dans le trousseau d'accès système et qu'il est défini sur **Toujours approuver** pour SSL.

Remarque : il ne doit pas être stocké sur le trousseau de session.

1. Demandez à l'administrateur de votre serveur SafeGuard de vous fournir le certificat pour la connexion SSL (fichier *<nom certificat>.cer*).
2. Importez le fichier *<nom certificat>.cer* dans votre trousseau. Allez dans **Applications** - **Utilitaires** et cliquez deux fois sur **Trousseaux d'accès.app**.
3. Dans le volet de gauche, sélectionnez **Système**.
4. Ouvrez une fenêtre Finder et sélectionnez le fichier *<nom certificat >.cer* .
5. Faites glisser le fichier certificat et déposez-le dans la fenêtre Trousseaux d'accès système.
6. Vous allez être invité à saisir votre mot de passe Mac OS X.
7. Après avoir saisi le mot de passe, cliquez sur **Modifier le trousseau** pour confirmer votre action.
8. Cliquez deux fois sur le fichier *<nom certificat>.cer*. Cliquez sur la flèche de gauche située à côté de **Se fier** pour ouvrir les paramètres de confiance.
9. Pour **Secure Sockets Layer (SSL)**, sélectionnez l'option **Toujours approuver**.
10. Fermez la boîte de dialogue. Vous allez être invité à saisir de nouveau votre mot de passe Mac OS X.
11. Saisissez votre mot de passe et cliquez sur **Réglages de mise à jour** pour confirmer. Un symbole + bleu apparaît dans le coin inférieur droit de l'icône de certificat. Il indique que ce certificat est marqué comme fiable pour tous les utilisateurs.

12. Ouvrez un navigateur Web et vérifiez que votre serveur SafeGuard Enterprise est disponible en saisissant **`https://<nom serveur>/SGNSRV`**.

Vous pouvez à présent commencer l'installation.

Remarque :

L'importation de certificats peut également être effectuée à l'aide de la commande **`sudo /usr/bin/security add-trusted-cert -d -k /Library/Keychains/System.keychain -r trustAsRoot -p ssl « /<dossier>/<nom du certificat>.cer »`**. Celle-ci peut également être utilisée pour le déploiement automatisé à l'aide d'un script. Changez les noms de dossier et de certificat en fonction de vos paramètres.

Remarque :

Si vous voulez éviter la procédure décrite ci-dessus, vous pouvez exécuter la commande **`sudo sgfsadmin --disable-server-verify`**. Retrouvez plus d'informations à la section Options de ligne de commande à la page 19. Nous déconseillons l'utilisation de cette option car elle risque de créer une faille de sécurité.

2.2 Installation manuelle (sous surveillance)

Une installation manuelle (ou sous surveillance) vous permet de contrôler et de tester l'installation étape par étape. Elle est effectuée sur un seul Mac.

Remarque :

Assurez-vous que la version 2.7.0 ou supérieure de FUSE pour OS X (OSXFUSE) est installée. Retrouvez plus d'informations sur FUSE pour OS X et sur les options de téléchargement sur http://osxfuse.github.io/.

Assurez-vous que la connexion au serveur est configurée conformément aux instructions de la section Conditions préalables à l'installation à la page 5.

1. Ouvrez le fichier *Sophos SafeGuard FE.dmg*.
2. Après avoir lu le fichier « readme », cliquez deux fois sur *Sophos SafeGuard FE.pkg* et suivez les instructions de l'assistant d'installation. Vous allez être invité à saisir votre mot de passe pour permettre l'installation du nouveau logiciel. Le produit va être installé dans le dossier */Library/Sophos SafeGuard FS/*.
3. Cliquez sur **Fermer** pour terminer l'installation.
4. Ouvrez les **Préférences Système** et cliquez sur l'icône Sophos Encryption pour afficher les paramètres du produit.

   

5. Cliquez sur l'onglet **Serveur**.
6. Si les détails du serveur et du certificat apparaissent, passez les étapes suivantes et rendez-vous directement à l'étape 11 puis cliquez sur **Synchroniser**. Si aucune information n'apparaît, passez à l'étape suivante.
7. Sélectionnez le fichier ZIP de configuration (retrouvez plus d'informations sur la création d'un package de configuration pour les ordinateurs d'extrémité Macs à la section *Utilisation de packages de configuration > Création d'un package de configuration pour les Macs* du *Manuel d'administration de SafeGuard Enterprise*).
8. Faites glisser le fichier ZIP dans la boîte de dialogue **Serveur** et déposez-le dans la zone de dépôt.
9. Vous allez être invité à saisir un mot de passe d'administrateur Mac. Saisissez le mot de passe et cliquez sur **OK** pour confirmer.

10. Saisissez votre mot de passe Mac pour demander votre certificat d'utilisateur SafeGuard.
11. Vérifiez la connexion au serveur SafeGuard Enterprise : les détails du certificat d'entreprise sont affichés dans la section inférieure de la boîte de dialogue **Serveur**. Cliquez ensuite sur **Synchroniser**. Une connexion réussie entraînera la mise à jour des informations sous « Dernier contact » (Onglet **Serveur**, zone **Informations sur le serveur**, **Dernier contact :**). Un échec de la connexion sera indiqué par l'icône ci-dessous :

    

    Retrouvez plus d'informations dans le fichier d'historique du système.

    Retrouvez plus d'informations sur la synchronisation et la connexion au serveur à la section Onglet Serveur à la page 15.

2.3 Installation automatisée (sans surveillance) via un logiciel de gestion à distance

L'installation automatisée (sans surveillance) ne nécessite aucune intervention de la part de l'utilisateur pendant la procédure d'installation.

Cette section décrit les étapes de base pour l'installation automatisée (sans surveillance) de SafeGuard File Encryption pour Mac. Les étapes peuvent varier selon la solution d'administration que vous utilisez. Utilisez le logiciel d'administration que vous avez installé.

Remarque :

Installez les packages dans le bon ordre.

Pour installer SafeGuard File Encryption pour Mac sur les ordinateurs clients, effectuez les étapes suivantes :

1. Téléchargez le programme d'installation *Sophos SafeGuardFS.pkg*.
2. Copiez le fichier sur les machines cibles.
3. Installez le fichier sur les machines cibles. Si vous utilisez Apple Remote Desktop, les étapes 2 et 3 représentent une seule et même étape.
4. Sélectionnez le fichier ZIP de configuration (retrouvez une description de la création d'un package de configuration pour les Macs à la section *Utilisation de packages de configuration > Création d'un package de configuration pour les Macs* du *Manuel d'administration de SafeGuard Enterprise*) et copiez-le sur les machines cibles.
5. Exécutez la commande suivante sur les machines cibles :

    ```
    /usr/bin/sgfsadmin --import-config /full/path/to/file.zip
    ```

    Changez */full/path/to/file* en fonction de vos paramètres. Cette commande doit être exécutée à l'aide des droits administrateur. Si vous utilisez Apple Remote Desktop, saisissez **`root`** dans le champ **Nom d'utilisateur** pour indiquer quel utilisateur a émis la commande mentionnée ci-dessus.

6. Vous pouvez ajouter des étapes supplémentaires à votre processus en fonction de vos paramètres (par exemple, arrêter les machines cibles).

3 Conseils et restrictions

3.1 Conseils

Réduction de la charge administrative

- Essayez d'avoir le moins de points de montage (ou Dossiers sécurisés) possibles.
- **Désactivez l'option « Exiger une confirmation avant de créer un compte mobile »**

  Si vous créez ou utilisez des comptes mobiles pour les ordinateurs d'extrémité Mac, assurez-vous que l'option **Exiger une confirmation avant de créer un compte mobile** est désactivée. Lorsque cette option est activée, l'utilisateur peut sélectionner « Ne pas créer ». Ceci peut entraîner la création d'un utilisateur OS X incomplet. Par exemple, un utilisateur qui n'as pas de répertoire de départ local.

  Pour désactivez cette option, procédez aux étapes suivantes :

  1. Ouvrez les **Préférences Système** et cliquez sur **Utilisateurs et groupes**.
  2. Cliquez sur le cadenas et saisissez votre mot de passe.
  3. Sélectionnez l'utilisateur.
  4. Cliquez sur **Options d’ouverture de session**.
  5. Dans **Compte serveur réseau**, cliquez sur **Modifier...**
  6. Sélectionnez le domaine Active Directory.
  7. Cliquez sur **Ouvrir Utilitaire d’annuaire...**
  8. Cliquez sur le cadenas et saisissez votre mot de passe, puis cliquez sur **Modifier la configuration**.
  9. Sélectionnez Active Directory et cliquez sur l'icône Modifier.
  10. Cliquez sur la flèche se trouvant à gauche de **Afficher les options avancées**.
  11. Sélectionnez **Créer un compte mobile lors de l’ouverture de session** et dessélectionnez l'option **Exiger une confirmation avant de créer un compte mobile**.
  12. Cliquez sur **OK** pour confirmer.

3.2 Restrictions

- **Nombre maximal de dossiers sécurisés (points de montage) sur un client**

  Chaque client Mac OS X contient un nombre maximal de 24 dossiers sécurisés (points de montage). Si plusieurs utilisateurs sont connectés à la même machine, vous devez ajouter les points de montage de tous les utilisateurs connectés. Si vous utilisez d'autres produits sur votre Mac qui se servent également de FUSE pour OS X, veuillez également compter ces points de montage dans le nombre maximal de 24 points de montage.

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

  Lorsque vous ouvrez un fichier (qui a été modifié auparavant) à partir d'un Dossier sécurisé, la fonction **Parcourir toutes les versions...** n'est pas disponible.

- **Dossiers exclus**

Les dossiers ci-dessous sont exclus du chiffrement :

- **Dossiers exclus et sous-dossiers non exclus :**
  - <Racine>/
  - <Racine>/Volumes/
  - <Profil utilisateur>/
- **Dossiers et sous-dossiers exclus :**
  - <Poste de travail>/
  - <Racine>/bin/
  - <Racine>/sbin/
  - <Racine>/usr/
  - <Racine>/private/
  - <Racine>/dev/
  - <Racine>/Applications/
  - <Racine>/Système/
  - <Racine>/Bibliothèque/
  - <Profil utilisateur>/Bibliothèque/
  - /<Amovibles>/SGPortable/
  - /<Amovibles>/Informations sur le volume système/

Ceci signifie, par exemple, qu'une règle de chiffrement pour la racine d'une partition supplémentaire (<Racine>/Volumes/) n'a aucun effet même si elle signalée comme ayant reçue la règle.

Une règle de chiffrement sur <Racine>/abc aura un effet tandis qu'une règle de chiffrement sur <Racine>/private/abc n'en aura aucun.

- **Recherche de fichiers**
  - **Recherche Spotlight**

    La recherche Spotlight ne fonctionne pas sur les fichiers chiffrés. Elle ne trouvera donc aucun résultat lors de la recherche dans les Dossiers sécurisés.

  - **Fichiers identifiés**

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

- **Gravure de CD**

  Il n'est pas possible de graver un CD chiffré.

- **Partage des Dossiers sécurisés**

  Un dossier sécurisé ne peut pas être partagé sur le réseau. Par exemple, si une règle s'applique sur <Documents>, ce dossier ne peut plus être partagé.

- **Suppression de fichiers**

  Lorsque vous supprimez des fichiers à partir d'un Dossier sécurisé (point de montage), vous voyez apparaître un message vous demandant de confirmer l'opération de

suppression. Les fichiers supprimés ne sont pas déplacés dans le dossier Corbeille et ne peuvent donc pas être restaurés.

- **SafeGuard Portable**

  SafeGuard Portable n’est pas disponible sur Mac OS X.

- **Utilisation de Time Machine**

  Si vous utilisez Time Machine avec un dossier chiffré, les anciennes versions ne sont pas affichées. Toutefois et à condition que vous ayez activé Time Machine, les copies de sauvegarde existent mais sont cachées. Veuillez procéder comme suit :

  - Ouvrez Time Machine (par exemple en saisissant « Time Machine » dans la recherche Spotlight). Le contenu de votre dossier racine s'affiche.
  - Appuyez sur **Maj - Commande - G** (pour « Aller au dossier : ») et saisissez le chemin caché du dossier chiffré que vous souhaitez restaurer. Exemple : si le dossier chiffré que vous utilisez habituellement est nommé /Utilisateurs/admin/Documents, veuillez saisir /Utilisateurs/admin/.sophos_safeguard_Documents/.
  - Naviguez jusqu'au fichier que vous souhaitez restaurer, puis, cliquez sur l'icône en forme de roue de la barre de menu de Time Machine et sélectionnez **Restaurer <nom de fichier> dans...**. Une fois que vous aurez quitté Time Machine pour revenir sur votre poste de travail, votre fichier aura été restauré et vous allez pouvoir le déchiffrer.

    Remarque : vous ne pouvez pas lire le contenu des fichiers dont le chemin de l'emplacement est caché. La copie de sauvegarde contient uniquement les données chiffrées et votre contenu est maintenu en sécurité.

- **Utilisation d'AirDrop**

  Les fichiers chiffrés peuvent être transférés avec AirDrop. Assurez-vous que l'appareil de destination peut gérer les fichiers chiffrés. En cas contraire, les applications pourraient fonctionner de manière inattendue.

- **Handoff**

  Il n'est pas possible d'utiliser Handoff sur les fichiers chiffrés.

- **Montage de partages de fichier réseau avec `autofs`**

  Les partages de fichier réseau sur lesquels une règle est appliquée et qui sont automatiquement montés au démarrage ne seront pas détectés par Sophos SafeGuard File Encryption. La gestion de ces points de montage est impossible car le point de montage d'origine ne peut pas être remplacé.

4 Configuration

Sophos SafeGuard File Encryption pour Mac OS X est administré dans SafeGuard Management Center. Le chapitre suivant aborde exclusivement la configuration Mac. Retrouvez des informations détaillées sur les fonctionnalités standard de Management Center dans le *Manuel d'administration de SafeGuard Enterprise*. Retrouvez plus d'informations sur les stratégies de Chiffrement de fichiers dans le *Manuel d'administration de SafeGuard Enterprise* au chapitre « Paramètres des stratégies » et aux chapitres suivants.

Remarque :

SafeGuard File Encryption pour Mac utilise uniquement les règles **Chiffrement de fichiers** et **Paramètres généraux**. Ainsi, vous avez uniquement besoin d'utiliser la règle **Chiffrement de fichiers** pour administrer le chiffrement des données sur le système de fichiers local, les supports amovibles, les partages réseau et le stockage Cloud. Les règles **Protection des périphériques** (notamment **Stockage Cloud** et **Chiffrement des supports amovibles**) seront ignorées pour SafeGuard File Encryption pour Mac OS X. Veuillez toujours affecter les règles de **Chiffrement de fichiers** aux objets des utilisateurs. Les règles **Chiffrement de fichiers** affectées aux ordinateurs d'extrémité n'auront aucun effet sur les ordinateurs d'extrémité OS X.

Remarque :

Dans SafeGuard Enterprise Management Center, veuillez saisir les chemins en utilisant des barres obliques inverses. Elles sont automatiquement converties en barres obliques sur le client Mac.

4.1 Options de configuration administrées centralement

Les options suivantes sont configurées de manière centralisée dans Management Center :

- **Règles**
- **Clés**
- **Certificats**

  Le serveur SafeGuard Enterprise fournit le certificat X.509 à l'utilisateur. Un certificat est généré à la première connexion. Ce certificat assure la sécurité du trousseau de clés de l'utilisateur. Retrouvez plus de renseignements sur la demande de certificat après la connexion dans le *Guide de démarrage rapide*.

- **Intervalle de connexion au serveur**

Remarque : retrouvez plus d'informations sur les options mentionnées ci-dessus dans le *Manuel d'administration de SafeGuard Enterprise*.

4.2 Options de configuration administrées localement

Les options suivantes sont configurées localement sur le client Mac :

- **Synchroniser les informations de la base de données**

Utilisez la commande **`sgfsadmin --synchronize`** pour commencer à synchroniser les informations de la base de données (règles, clés et certificats) à partir de Management Center.

- **Activer ou désactiver le menu système**

  Utilisez la commande **`sgfsadmin --enable-systemmenu`** pour activer le menu système dans le coin supérieur droit.

  Utilisez la commande **`sgfsadmin --disable-systemmenu`** pour désactiver le menu système.

  Retrouvez plus d'informations sur les deux options à la section Menu système de Sophos SafeGuard File Encryption à la page 18.

Retrouvez une vue générale complète de toutes les options de la ligne de commande à la section Options de ligne de commande à la page 19.

5 Utilisation de File Encryption pour Mac

Un Guide de démarrage rapide de Sophos SafeGuard File Encryption vous explique l'utilisation de l'application. Retrouvez la dernière version de la documentation des produits sur http://www.sophos.com/fr-fr/support/documentation.aspx.

Les sections suivantes contiennent des informations destinées aux administrateurs sur l'utilisation de File Encryption pour Mac.

5.1 Fonctionnement du chiffrement

Chaque fichier est chiffré à l'aide d'une clé de chiffrement de données DEK (Data Encryption Key) générée aléatoirement par l'algorithme AES-256. Cette clé DEK générée aléatoirement est unique. Elle est chiffrée et archivée en tant qu'en-tête de fichier avec le fichier chiffré et augmente la taille du fichier de 4 Ko.

La clé DEK est chiffrée à l'aide d'une clé de chiffrement de clés ou KEK (Key Encryption Key). Cette clé KEK est archivée dans la base de données centrale de SafeGuard Enterprise. Le responsable de la sécurité l'attribue soit à un utilisateur, à un groupe d'utilisateurs ou à des unités organisationnelles.

Pour déchiffrer un fichier chiffré, l'utilisateur doit avoir la clé KEK correspondant à ce fichier dans son trousseau de clés.

5.2 Chiffrement initial

Sur le client, procédez aux étapes suivantes :

1. Ouvrez les **Préférences Système**.
2. Cliquez sur l'icône Sophos Encryption :

   

3. Sélectionnez l'onglet **Règles**.
4. Passez dans la vue **Chemin converti localement** si elle n'est pas déjà ouverte. Vous pouvez à présent

   a) Appliquer toutes les règles. Veuillez cliquer sur le bouton **Appliquer toutes les règles** au bas de la fenêtre.

   ou

   b) veuillez sélectionner une seule règle et cliquez sur le bouton **Appliquer la règle**.

   Remarque : ne déconnectez pas les appareils pendant l'opération de chiffrement.

   Remarque : si vous souhaitez voir les détails et le contenu du chemin converti localement, sélectionnez ce chemin dans le tableau et cliquez sur **Afficher dans le Finder**. La fenêtre du Finder s'ouvre et affiche le chemin sélectionné et son contenu éventuel.

5.3 Gestion des mots de passe

Le jeu de clés Sophos SafeGuard est sécurisé à l'aide d'un certificat d'utilisateur. La clé privée correspondante est protégée par le mot de passe OS X.

Le mot de passe permet de générer un certificat si l'utilisateur n'a pas été créé dans SafeGuard Enterprise.

Changement local de mot passe

Les utilisateurs ont la possibilité de changer localement leur mot de passe dans **Préférences Système > Utilisateurs et groupes**. Aucune autre étape supplémentaire n'est requise.

Le mot de passe a été changé sur un autre ordinateur d'extrémité

Remarque : les mots de passe peuvent être changés sur les ordinateurs d'extrémité Windows et Mac.

Le mot de passe n'étant plus connu sur cet ordinateur d'extrémité, les étapes suivantes doivent être effectuées :

1. Connectez-vous à OS X avec votre nouveau mot de passe.
2. Le message **Le système n'a pas réussi à déverrouiller votre trousseau de session** apparaît.
3. Sélectionnez **Mettre à jour le mot de passe du trousseau**.
4. Saisissez l'ancien mot de passe.

Retrouvez plus de renseignements sur la réinitialisation d'un mot de passe oublié à la section Oubli du mot de passe de connexion à Mac OS X à la page 23.

5.4 Permutation rapide d'utilisateur

SafeGuard File Encryption pour Mac prend également en charge la permutation rapide d'utilisateur. Le logiciel vous permet de permuter entre les comptes d'utilisateur à partir d'un seul ordinateur d'extrémité sans avoir à quitter les applications ou à fermer la session sur l'ordinateur.

Remarque : le module OS X FUSE gère un nombre maximal de 24 points de montage (Dossiers sécurisés). Retrouvez plus d'informations à la section Conseils et restrictions à la page 8.

5.5 Fenêtre de préférences

La fenêtre de préférences vous permet de définir vos préférences pour une application spécifique ou pour le système. Suite à l'installation de Sophos SafeGuard File Encryption (ou Sophos SafeGuard Native Device Encryption) sur un client Mac, vous allez voir apparaître l'icône de la fenêtre de préférences ci-dessous dans les **Préférences Système** :

Cliquez sur l'icône pour ouvrir le volet des préférences Sophos Encryption. La boîte de dialogue **À propos** s'ouvre.

La barre de menus vous permet d'ouvrir les fenêtres d'informations du menu suivantes :

5.5.1 Onglet À propos

L'onglet **À propos** vous donne des renseignements sur la version du produit installée sur votre Mac OS X, sur les droits d'auteur et sur les marques déposées. Si Sophos SafeGuard Disk Encryption ou Native Device Encryption est installé, il apparaîtra également dans la liste.

Cliquez sur le lien Sophos en bas de la fenêtre pour ouvrir le site Web de Sophos.

5.5.2 Onglet Serveur

Cliquez sur **Serveur** pour afficher une fenêtre contenant les informations et fonctionnalités suivantes :

Informations sur le serveur

- **Intervalle de contact :** indique l'intervalle auquel a lieu la synchronisation avec le serveur. Retrouvez plus d'informations sur la manière de définir cet intervalle dans le *Manuel d'administration de SafeGuard Enterprise à la section Paramètres de stratégie > Paramètres généraux*.
- **Dernier contact :** indique la date à laquelle le client a communiqué pour la dernière fois 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 entrer en communication avec le serveur SafeGuard Enterprise est activée ou désactivée. Retrouvez plus d'informations sur la modification de cette option à la section Options de ligne de commande à la page 19.

Faire glisser le fichier ZIP de configuration ici

Faites glisser le fichier ZIP de configuration dans cette zone pour appliquer les informations de configuration de SafeGuard Management Center au client Mac. Retrouvez plus d'informations à la section Installation manuelle (sous surveillance) à la page 6.

Synchroniser

Cliquez sur ce bouton pour démarrer manuellement la synchronisation des informations de la base de données telles que les stratégies et/ou les clés. Cette opération pourrait être nécessaire suite aux modifications effectuées dans SafeGuard Management Center.

En cas d'échec de la synchronisation, l'icône ci-dessous apparaît :

Si le problème persiste, vérifiez la connexion au serveur en utilisant l'URL du serveur principal et du serveur secondaire. Retrouvez plus d'informations sur les conditions préalables requises à la section Installation à la page 5. Si la synchronisation avait réussi auparavant, il se peut que le certificat SSL ait expiré. Consultez également le fichier d'historique du système pour obtenir plus d'informations sur les causes éventuelles.

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.

5.5.3 Onglet Utilisateur

Cliquez sur **Utilisateur** pour afficher les informations sur :

- Le **Nom d'utilisateur** de l'utilisateur connecté.
- Le **Domaine** répertoriant le répertoire du domaine auquel appartient le client. Le nom de l'ordinateur local est affiché pour les utilisateurs locaux.
- La **GUID de l'utilisateur SafeGuard** affiche la GUID qui a été générée pour l'utilisateur suite à sa première connexion.

Dans le second volet, vous pouvez sélectionner/dessélectionner l'option suivante :

- **Afficher le menu système de File Encryption** : lorsque cette option est activée, l'icône Sophos SafeGuard File Encryption apparaît dans la barre de menus. Retrouvez plus d'informations à la section Menu système de Sophos SafeGuard File Encryption à la page 18.

Le troisième volet de la fenêtre affiche les informations sur le **Certificat de l'utilisateur** :

- **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.

5.5.4 Onglet Clés

Cliquez sur **Clés** pour afficher 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 de ou des clés respectives.

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 l'utilisateur est propriétaire de cette clé.

5.5.5 Onglet Règles

Cliquez sur **Règles** pour ouvrir la vue des règles. Cliquez sur l'une des icônes dans le coin inférieur droit pour permuter entre la vue **Chemin converti localement** et la vue **Règles reçues** :

- Le **Chemin converti localement** affiche uniquement les règles s'appliquant à un moment donné à l'utilisateur connecté sur un ordinateur Mac spécifique. Les colonnes du tableau incluent les informations suivantes :
  - **Symbole** @ : lors du chiffrement initial ou du chiffrement de fichiers de plus grande taille, vous allez voir le symbole @ tourner dans la première colonne jusqu'à ce que le chiffrement soit terminé.
  - **Mode** : le mode **chiffrer** ou **exclure** est affiché.

    Remarque :

    Retrouvez plus d'informations sur ces modes dans le *Manuel d'administration de SafeGuard Enterprise*.

- **Étendue** : indique si les sous-dossiers doivent être chiffrés.
- **Nom de la clé** : nom de la clé attribuée à l'emplacement indiqué.

  Une clé de couleur bleue signifie que l'utilisateur est propriétaire de cette clé.

  Une clé de couleur orange signifie qu'elle a été configurée dans une stratégie qui a été affectée à l'utilisateur. En revanche, l'utilisateur n'est pas propriétaire de cette clé car elle n'a pas été affectée à son trousseau de clés. Ceci peut poser des problèmes d'accès aux données. Retrouvez plus d'informations à la section Problèmes d'accès aux données à la page 23.

Pour basculer vers la vue Règles reçues, cliquez dans le coin inférieur droit indiquant **Vue de la règle** sur l'icône de droite :

- La vue **Règles reçues** affiche toutes les règles reçues du serveur. Cette vue est identique à la vue dans SafeGuard Management Center. Le tableau répertorie les informations suivantes :
  - **Règles 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**.

Affichage des dossiers sécurisés et application des règles dans la vue Chemin converti localement

Si une règle est sélectionnée (1) dans le tableau **Chemin converti localement** :

- Cliquez sur le bouton **Afficher dans le Finder** (2) pour ouvrir le dossier sécurisé (point de montage) sélectionné dans une fenêtre Finder et afficher son contenu.
- Cliquez sur **Appliquer la règle** (3) pour appliquer la règle sélectionnée sur tous les fichiers de l'emplacement indiqué. Une barre de progression apparaît. Attendez que le système termine l'opération d'application de la règle ou annulez l'opération en cliquant sur la croix située à côté de la barre.

  Remarque :

  Pour dessélectionnez une seule règle, appuyez sur la touche **Cmd** et cliquez avec la souris.

  Remarque :

  Les fichiers protégés en écriture ou inaccessibles en raison d'autorisations manquantes seule seront exclus du chiffrement.

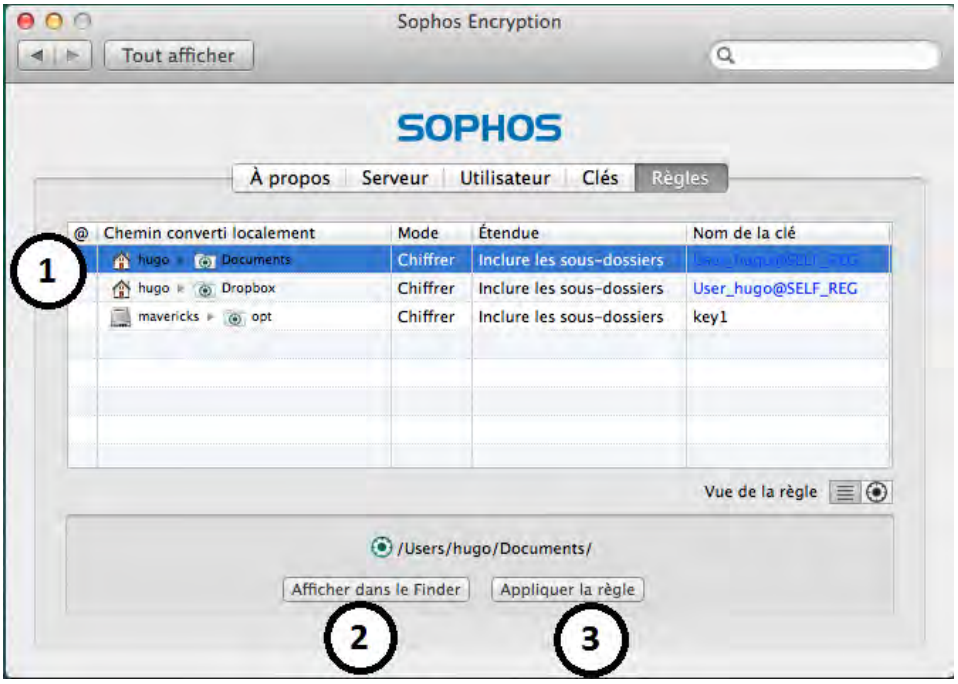

Figure 1 : onglet Règles : vue du Chemin converti localement

Résultats éventuels suite à l'application des règles

Si vous avez des règles déjà appliquées :

- Les fichiers brut seront chiffrés à l'aide de la clé de chiffrement attribuée par une règle.
- Les fichiers déjà chiffrés à l'aide de la clé de chiffrement indiquée dans la règle demeureront chiffrés.
- Les fichiers déjà chiffrés à l'aide d'une autre clé de chiffrement :
  - Ne seront pas modifiés si la clé de chiffrement correspondante ne se trouve pas dans le trousseau de clés de l'utilisateur.
  - Seront chiffrés à nouveau à l'aide de la clé de chiffrement attribuée par la règle si celle-ci se trouve dans le trousseau de clés de l'utilisateur.
- Les fichiers chiffrés à plusieurs reprises seront considérés comme étant chiffrés dès qu'une clé de chiffrement leur aura été attribuée par une règle. Si l'une des clés de chiffrement est indisponible, ces fichiers seront déchiffrés dans la mesure du possible mais continueront à bénéficier d'un niveau de chiffrement.

5.6 Menu système de Sophos SafeGuard File Encryption

Le menu système vous fournit les informations et fonctionnalités suivantes :

1. Lorsqu'un fichier est sélectionné, l'icône affiche automatiquement l'état du chiffrement et le nom de la clé :

	Icône verte : le fichier est chiffré et vous possédez la clé correspondante.

	Icône rouge : le fichier est chiffré et vous ne possédez pas la clé correspondante.
	Icône grise : le fichier devant être chiffré n'a pas encore été chiffré. (*)
	Icône noire : le fichier est ignoré ou exclus du chiffrement.

(*) Cas de figure possible : si vous avez sélectionné un fichier non chiffré se trouvant dans un répertoire sur lequel une règle de chiffrement est appliquée, l'icône devient grise. Ouvrez l'onglet **Règles** et sélectionnez la règle correspondante au répertoire, puis sélectionnez **Appliquer la règle** pour chiffrer le fichier pour la première fois. Retrouvez plus d'informations à la section Onglet Règles à la page 16.

2. Lorsqu'un fichier est en cours de traitement, la roue entourant l'icône tourne. Ce comportement est indépendant de l'état de chiffrement en cours.
3. Selon les fichiers ou volumes sélectionnés, les éléments du menu suivants sont disponibles :
   - État actuel du chiffrement et de la clé

     Si un fichier, un répertoire ou un volume est sélectionné, un message concernant l'état actuel du chiffrement, le nom de la clé nécessaire et des informations indiquant si l'utilisateur est le propriétaire ou non de la clé apparaissent.

     Remarque :

     Pour vous assurer que l'état actuel du chiffrement et que le nom de la clé des fichiers et des répertoires s'affichent, vous allez peut être devoir passer de la vue du fichier/répertoire sélectionné à une autre vue sur le bureau puis revenir au fichier/répertoire sélectionné.

   - Liste des dossiers sécurisés SafeGuard disponibles (points de montage)

     Remarque :

     Si vous passez le curseur de la souris sur l'une des icônes d'un Dossier sécurisé, le chemin complet du dossier s'affiche :

   - **Ouvrir les préférences Sophos Encryption...**

     Ouvre la fenêtre de préférences Sophos Encryption. Retrouvez également plus d'informations à la section Fenêtre de préférences à la page 14

5.7 Options de ligne de commande

L'application Terminal vous permet de saisir les commandes et les options de ligne de commande. Les options de ligne de commande suivantes sont disponibles :

Nom de la commande	Définition	Paramètres additionnels (facultatif)
`sgfsadmin`	Répertorie toutes les commandes disponibles y compris les conseils d'utilisation.	**`--help`**

Nom de la commande	Définition	Paramètres additionnels (facultatif)
sgfsadmin --version	Affiche la version et le copyright du produit installé.	
sgfsadmin --status	Renvoie des informations sur l'état du système telle que la version, le serveur et le certificat.	
sgfsadmin --list-user-details	Renvoie des informations sur l'utilisateur connecté.	**--all** affiche les informations sur tous les utilisateurs (commande sudo requise) **--xml** renvoie un fichier généré au format xml.
sgfsadmin --list-keys	Répertorie les GUID existants et les noms de toutes les clés dans le magasin de clés.	**--all** affiche les informations sur tous les utilisateurs (commande sudo requise) **--xml** renvoie un fichier généré au format xml.
sgfsadmin --list-policies	Affiche des informations relatives à la règle. Les GUID de clé sont résolus en noms de clé si possible. Une clé personnelle sera affichée en caractères gras.	**--all** affiche les informations sur tous les utilisateurs (commande sudo requise). **--xml** renvoie un fichier généré au format xml. **--raw** affiche les règles brutes, c'est-à-dire les règles paramétrées sur le serveur SafeGuard Management Center.
sgfsadmin --enforce-policies	Applique la règle de chiffrement.	**--all** applique la règle à tous les répertoires auxquels les règles s'appliquent. **"directoryname"** applique la règle au répertoire indiqué.
sgfsadmin --file-status "filename1" ["filename2"..."filenameN"]	Renvoie les informations de chiffrement d'un fichier ou d'une liste de fichiers. Les caractères de remplacement sont acceptés.	**--xml** renvoie un fichier généré au format xml.
sgfsadmin --import-config "/path/to/target/file"	Importe le fichier ZIP de configuration indiqué. Reportez-vous également à la section Installation manuelle (sous surveillance) à la page 6.	

Nom de la commande	Définition	Paramètres additionnels (facultatif)
	Cette commande nécessite de disposer des droits administratifs (sudo). **Remarque :** Utilisez l'opération glisser-déplacer pour déplacer, par exemple, un chemin complet du Finder à l'application Terminal.	
`sgfsadmin --enable-server-verify`	Active la vérification du serveur SSL pour la communication avec le serveur SafeGuard Enterprise. Suite à l'installation, la vérification du serveur SSL est activée. Cette commande nécessite de disposer des droits administratifs (sudo).	
`sgfsadmin --disable-server-verify`	Désactive la vérification du serveur SSL pour la communication avec le serveur SafeGuard Enterprise. Cette commande nécessite de disposer des droits administratifs (sudo). **Remarque :** Nous déconseillons l'utilisation de cette option car elle risque de créer une faille de sécurité.	
`sgdeadmin --update-machine-info [--domain "domain"]`	Met à jour les informations de la machine qui sont utilisées pour enregistrer ce client sur le serveur SafeGuard Enterprise. Cette commande nécessite de disposer des droits administratifs (sudo). **Remarque :** Utilisez uniquement cette commande après avoir changé le domaine ou le groupe de travail auquel appartient l'ordinateur. Si l'ordinateur est membre de plusieurs domaines ou groupes de travail et que vous exécutez cette commande, il se peut que l'enregistrement du domaine soit modifié et que les clés personnelles et/ou les utilisateurs FileVault 2 soient supprimés.	**`--domain "domain"`** Le domaine que le client doit utiliser pour s'enregistrer sur le serveur SafeGuard Enterprise. Ce paramètre est uniquement nécessaire si la machine est membre de plusieurs domaines. Si l'ordinateur n'est pas relié à ce domaine, la commande échouera.

Les commandes suivantes sont expliquées en détails à la section Options de configuration administrées localement à la page 11 :

- **`sgfsadmin --enable-systemmenu`**
- **`sgfsadmin --disable-systemmenu`**
- **`sgfsadmin --synchronize`**

5.8 Utilisation des périphériques amovibles

Remarque :

Avant d'utiliser les périphériques amovibles, assurez-vous qu'une règle et une clé vous ont été attribuées afin de vous permettre de chiffrer les fichiers sur les supports amovibles.

1. Connectez le périphérique amovible.
2. Une boîte de dialogue s'ouvre et vous demande si vous voulez chiffrer les fichiers en texte brut sur le périphérique. Cliquez sur **Oui** pour démarrer le chiffrement. Si vous cliquez sur **Non**, ces fichiers ne sont pas chiffrés. En revanche, vous avez accès aux fichiers déjà chiffrés sur le périphérique. Quelle que soit l'option sélectionnée, les nouveaux fichiers présents sur le périphérique seront toujours chiffrés conformément à la règle définie.
3. Les fichiers présents sur votre périphérique vont être chiffrés automatiquement. Une roue tournant sur le menu système vous indique la progression de l'opération.
4. Dès que tous les fichiers présents sur votre périphérique sont chiffrés, la roue s'arrête de tourner.
5. Éjectez le périphérique amovible. L'icône du Dossier sécurisé correspondant disparaît automatiquement.

   Remarque :

   Pour pouvoir échanger et modifier des données présentes sur les périphériques amovibles entre deux personnes, ces deux personnes doivent disposer de la règle correspondante et être affectées à une clé. Pour l'échange entre les clients Windows et Mac OS X, le périphérique doit impérativement être formaté à l'aide de FAT32. Aucune clé personnelle ne peut être utilisée. Pour le client Windows, il est nécessaire de créer une règle d'échange des données. La phrase secrète des supports est uniquement disponible sur Windows. Sur un client Mac OS X, les données sont uniquement accessibles si les règles correspondantes de **Chiffrement des fichiers** sont définies.

6 Résolution des problèmes

6.1 Oubli du mot de passe de connexion à Mac OS X

Si un utilisateur oublie son mot de passe de connexion à Mac OS X, procédez de la manière suivante :

1. L'utilisateur va vous demander de créer un nouveau mot de passe utilisateur.
2. Réinitialisez le mot de passe déjà existant dans votre environnement d'administration des utilisateurs et générez un nouveau mot de passe. Sélectionnez l'option correspondante afin de vous assurer que l'utilisateur soit obligé de modifier son mot de passe après sa première connexion.
3. Dans l'application SafeGuard Management Center, supprimez le certificat de l'utilisateur.
4. Contactez l'utilisateur et communiquez lui son nouveau mot de passe.
5. Informez l'utilisateur qu'il doit se connecter avec son nouveau mot de passe.
6. Une fois connecté, la boîte de dialogue **Réinitialisation de mot de passe** apparaît.
7. Demandez à l'utilisateur de définir un nouveau mot de passe, de le saisir et de le vérifier, puis d'indiquer un mémo pour ce mot de passe. Enfin, l'utilisateur doit cliquer sur **Réinitialiser le mot de passe** pour confirmer les modifications.
8. Après la réinitialisation du mot de passe, l'utilisateur voit apparaître le message suivant :

   Le système n'a pas réussi à déverrouiller votre trousseau de session
9. Demandez à l'utilisateur de sélectionner l'option **Créer un trousseau**.
10. Un nouveau trousseau est créé pour l'utilisateur.
11. L'utilisateur va devoir saisir le nouveau mot de passe OS X à partir de l'étape 7 afin de créer le certificat utilisateur SafeGuard.

Les clés de l'utilisateur vont être chargées automatiquement dans le nouveau trousseau afin que tous les documents soient accessibles comme auparavant.

6.2 Problèmes d'accès aux données

Si un utilisateur rencontre des problèmes d'accès aux données, il se peut que la clé correspondante ne figure pas dans son trousseau de clés :

- Vérifiez l'environnement du Management Center et procédez à toutes les corrections nécessaires. Retrouvez plus d'informations sur la manière de vérifier si l'utilisateur connecté possède déjà la clé correspondante à la section Menu système de Sophos SafeGuard File Encryption à la page 18.

  Les fichiers chiffrés à l'aide d'une clé ne se trouvant pas sur le trousseau de clés de l'utilisateur ne peuvent pas être déchiffrés. Si l'utilisateur copie les fichiers dans un Dossier sécurisé (qui déclenche le chiffrement initial de ces fichiers) et que la clé correspondante n'est pas disponible, Mac OS X affiche alors une boîte de dialogue invitant l'utilisateur à saisir un nom et un mot de passe d'administrateur. Dans ce cas, l'utilisateur doit cliquer sur **Annuler** (le mot de passe ne donne pas accès aux fichiers chiffrés).

6.3 Fichiers récupérés par SafeGuard

Dans certaines circonstances, un dossier nommé **Fichiers récupérés par Sophos SafeGuard** peut être présent dans un dossier. Ceci arrive si SafeGuard File Encryption essaye de créer un nouveau Dossier sécurisé (point de montage) et que le dossier caché qui doit être créé pour le stockage du contenu chiffré (par exemple /Utilisateurs/admin/.sophos_safeguard_Documents/) existe déjà et contient des fichiers. Le contenu du dossier d'origine (par exemple /Utilisateurs/admin/Documents) est donc déplacé dans le dossier **Fichiers récupérés par Sophos SafeGuard** et seul le contenu du dossier caché est affiché comme d'habitude.

7 Désinstallation à partir du client

Si vous devez désinstaller le logiciel à partir d'un ordinateur client, procédez de la manière suivante :

1. Sur le client Mac, allez dans */Bibliothèque*.
2. Ouvrez le dossier *Sophos SafeGuard FS*.
3. Sélectionnez et cliquez deux fois sur le fichier *Sophos SafeGuard FS Uninstaller.pkg*
4. Un assistant vous guide tout au long de la désinstallation.
5. Redémarrez le système avant de continuer à utiliser votre Mac.

   Remarque : le package du programme de désinstallation est signé et OS X va essayer de valider cette signature. Si la connexion à Internet est lente ou mal configurée, la procédure de désinstallation peut être retardée d'au moins 20 minutes.

8 Support technique

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

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

9 Mentions légales