SOPHOS

Security made simple.

Sophos SafeGuard File Encryption pour Mac

Guide de démarrage rapide

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 transparent 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 personnes.

- Les nouveaux fichiers dans les emplacements correspondants sont chiffrés automatiquement.
- Si vous avez la clé d'un fichier chiffré, vous pouvez lire et modifier le contenu.
- Si vous n'avez pas la clé d'un fichier chiffré, vous ne pouvez pas lire son contenu en texte brut et pouvez uniquement voir le contenu chiffré.
- Si vous accédez à un fichier chiffré sur un ordinateur sur lequel File Encryption n'est pas installé, le contenu chiffré apparaît.

2 Première utilisation

Ce guide suppose que le logiciel a été installé conformément aux instructions du *Manuel d'administration de Sophos SafeGuard File Encryption pour Mac* et que la communication avec le serveur backend de SafeGuard Enterprise a été établie correctement.

1. Mettez le Mac sous tension.
2. Ouvrez une session sur votre Mac à l'aide de votre mot de passe OS X habituel.
3. Lorsque vous ouvrez une session juste après l'installation du produit, vous êtes invité à saisir de nouveau votre mot de passe dans la boîte de dialogue suivante :

Figure 1 : cette boîte de dialogue de connexion apparaît uniquement après l'installation et à la première ouverture de session par l'utilisateur.

4. Saisissez votre mot de passe et cliquez sur OK pour confirmer.

   Remarque : pour pouvoir utiliser le produit correctement, vous devez avoir un certificat personnel. Ce certificat est généré par utilisateur lorsque vous saisissez votre mot de passe dans la boîte de dialogue. Cette opération est uniquement requise suite à l'installation du produit, à la première connexion ou à la réinitialisation du mot de passe.

5. Selon les paramètres de sécurité qui vous ont été affectés, vous allez voir un ou plusieurs volumes apparaître sur votre bureau.

   Important : assurez-vous que l'option « Serveurs connectés » est activée dans les paramètres du Finder. Sélectionnez **Finder - Préférences - Général** et activez l'option **Serveurs connectés**.

3 Utilisation de SafeGuard File Encryption pour Mac

SafeGuard File Encryption pour Mac permet à votre administrateur de la sécurité d'indiquer si les fichiers présents dans les répertoires et/ou les volumes spécifiés seront chiffrés ou non. Les options de recherche Spotlight et de stockage permanent des versions (« Parcourir toutes les versions... ») ne sont pas disponibles. Toutefois, si vous essayez d'éjecter un volume dirigeant vers un répertoire local, il sera immédiatement et automatiquement reconnecté.

Le chiffrement lui-même est transparent. Suite au chiffrement initial, le système s'assure que les fichiers se trouvant dans un volume ou dans un répertoire de chiffrement (nommé « Dossier sécurisé ») sont chiffrés.

3.1 Chiffrement initial

Avant de commencer à travailler, veuillez procéder au chiffrement initial :

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** et cliquez sur **Appliquer toutes les règles** pour appliquer toutes les règles.

Tous les fichiers bruts seront chiffrés suite à cette opération.

Si vous voulez appliquer une seule règle, sélectionnez-la à l'aide de votre souris et cliquez sur **Appliquer la règle**. Pour dessélectionnez une seule règle, appuyez sur la touche **Cmd** et cliquez avec la souris.

4 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 de la barre des menus affiche automatiquement l'état du chiffrement et 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 doit être 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.

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 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, le chemin complet du dossier s'affiche.

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

     Ouvre la fenêtre de préférences Sophos Encryption.

5 Fenêtre de préférences

Une fenêtre de préférences vous permet de définir vos préférences pour une application spécifique ou pour le système. Suite à l'installation de Sophos 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 la fenêtre 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 :

5.1 Onglet À propos

L'onglet **À propos** vous donne des renseignements sur la version du produit installée sur votre Mac, 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.

5.2 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. Il est défini de manière centralisé par le responsable de la sécurité.
- **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.

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.

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, veuillez contacter votre administrateur de la sécurité.

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.

5.3 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 6.

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.

5.4 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 vous êtes le propriétaire de cette clé.

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 vous êtes le propriétaire de cette clé.

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

  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 autorisés. 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.

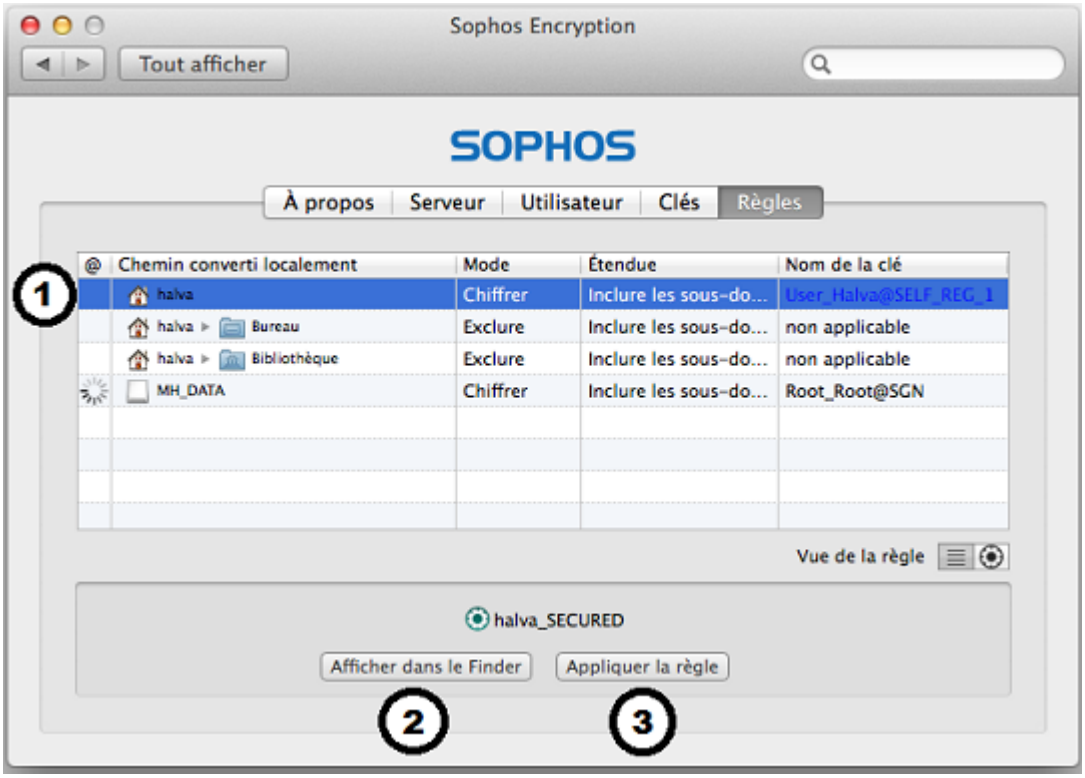

Figure 2 : vue du Chemin converti localement dans l'onglet Règles

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.

6 Utilisation des périphériques amovibles

Important : assurez-vous d'avoir attribué une règle et une clé qui vous permettront de chiffrer et de modifier les fichiers sur les supports amovibles.

Pour chiffrer les fichiers sur un périphérique amovible, procédez de la manière suivante :

1. Insérez le périphérique sur le Mac.
2. Une boîte de dialogue apparaît et vous demande de confirmer si vous voulez chiffrer les fichiers.

3. Pour confirmer, cliquez sur **Oui**.
4. Les fichiers présents sur votre périphérique vont être chiffrés. La roue entourant l'icône se met à tourner.
5. Lorsque tous les fichiers présents sur votre périphérique sont chiffrés, la roue entourant l'icône s'arrête de tourner.
6. Éjectez le périphérique amovible. L'icône du volume correspondant disparaît automatiquement.

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.

Important : 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.

7 Consignes générales

Si vous rencontrez la fonctionnalité de chiffrement du disque FileVault 2 de Mac OS X...

Si vous sélectionnez un volume (sur votre bureau ou dans le Finder) et que vous cliquez avec le bouton droit de la souris, un élément du menu "Chiffrer <nom du volume> ..." apparaît :

Il s'agit de l'application de chiffrement de disque interne d'Apple OS X nommée FileVault 2 qui n'est pas reliée à notre application SafeGuard File Encryption.

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