SOPHOS

Security made simple.

SafeGuard Native Device Encryption pour Mac

Manuel d'administration

Version du produit : 7

Date du document : décembre 2014

Table des matières

1 À propos de SafeGuard Native Device Encryption pour Mac

Sophos SafeGuard Native Device Encryption pour Mac fait bénéficier aux utilisateurs Mac OS X du même niveau de protection des données que la fonction de chiffrement de disque de SafeGuard Enterprise offre déjà aux utilisateurs Windows.

SafeGuard Native Device Encryption pour Mac est compatible avec la technologie de chiffrement FileVault 2 intégrée de Mac OS X. Le logiciel a recours à FileVault 2 pour chiffrer l'intégralité du disque dur afin que vos données soient en sécurité même en cas de perte ou de vol de votre ordinateur. Vous avez également la possibilité d'appliquer et de gérer le chiffrement du disque sur des réseaux tout entier.

Le chiffrement fonctionne de manière transparente. L'utilisateur n' pas besoin de chiffrer ou de déchiffrer les fichiers lors de leur ouverture, modification ou enregistrement.

SafeGuard Management Center vous permet de sélectionner les ordinateurs (Windows et Macs) à chiffrer, de suivre l'état de leur chiffrement et de fournir des outils de récupération aux utilisateurs ayant oublié leur mot de passe.

1.1 À propos de ce document

Le présent document vous explique comment installer, configurer et administrer Sophos SafeGuard Native Device 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 Native Device 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
GUID	Globally Unique Identifier (identifiant unique universel) : un numéro de référence unique utilisé en tant qu'identifiant dans les logiciels informatiques.
POA	Authentification au démarrage (synonyme : « authentification préalable au démarrage »)
SGN	SafeGuard Enterprise

Terme ou acronyme	Signification ou explication
SSL	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 Native Device 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)

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.

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.

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.

1. Demandez à l'administrateur de votre serveur SafeGuard de vous fournir le certificat du serveur SafeGuard Enterprise pour la connexion SSL (fichier *<nom certificat>.cer*).
2. Importez le fichier *<nom certificat>.cer* dans votre trousseau de clés. 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 **`sgdeadmin --disable-server-verify`** avec les droits sudo conformément aux instructions de la section Options de ligne de commande à la page 15. 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 le serveur est configuré correctement conformément aux instructions de la section Conditions préalables à l'installation à la page 5.

1. Ouvrez le fichier *Sophos SafeGuard DE.dmg*.
2. Après avoir lu le fichier « readme », cliquez deux fois sur *Sophos SafeGuard DE.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 DE/*.
3. Cliquez sur **Fermer** pour terminer l'installation.
4. Suite au redémarrage de l'ordinateur, connectez-vous à l'aide de votre mot de passe Mac.
5. Ouvrez les **Préférences Système** et cliquez sur l'icône Sophos Encryption pour afficher les paramètres du produit.

   

6. Cliquez sur l'onglet **Serveur**.
7. 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.
8. Sélectionnez le fichier ZIP de configuration (retrouvez plus d'informations sur la création d'un package de configuration pour les Macs dans la version 7.0 du *Manuel d'administration de SafeGuard Enterprise* à la section *Utilisation de packages de configuration* > *Création d'un package de configuration pour les Macs*).
9. Faites glisser le fichier ZIP dans la boîte de dialogue **Serveur** et déposez-le dans la zone de dépôt.
10. Vous allez être invité à saisir un mot de passe d'administrateur Mac. Saisissez le mot de passe et cliquez sur **OK** pour confirmer.

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 13.

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 Native Device Encryption pour Mac. Veuillez utiliser le logiciel d'administration installé sur votre système. Les étapes peuvent varier selon la solution d'administration que vous utilisez.

Remarque :

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

1. Téléchargez le programme d'installation *Sophos SafeGuard DE.dmg*.
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 plus d'informations sur la création d'un package de configuration pour les Macs dans la version 7.0 du *Manuel d'administration de SafeGuard Enterprise* à la section *Utilisation de packages de configuration* > *Création d'un package de configuration pour les Macs*) et copiez-le sur les machines cibles.
5. Exécutez la commande suivante sur les machines cibles :

    ```
    /usr/bin/sgdeadmin --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.

3 Configuration

Sophos SafeGuard Native Device 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*.

Remarque :

SafeGuard Native Device Encryption pour Mac utilise uniquement les règles de type **Protection des périphériques** et **Paramètres généraux** et ignore tous les paramètres de règle à l'exception de **Cible**, **Mode de chiffrement des supports** et **Intervalle de connexion au serveur (minutes)**.

3.1 Options de configuration administrées de manière centralisée

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

Règles

Les règles sont configurées de manière centralisée dans SafeGuard Management Center. Pour commencer à utiliser le chiffrement intégral du disque, les paramètres doivent être choisi comme suit :

1. Créez une nouvelle règle de type **Protection des périphériques**. Pour **Cible de protection des périphériques**, sélectionnez **Périphériques de stockage locaux**, **Stockage interne** ou **Volumes de démarrage**. Saisissez un nom pour la règle et cliquez sur **OK**.
2. Pour le **Mode de chiffrement des supports**, sélectionnez **Basé sur le volume**.

Une nouvelle règle de protection des périphériques est créée et configurée pour le chiffrement intégral du disque des Macs.

Remarque : assurez-vous que la règle est attribuée aux clients qui seront chiffrés. Si tous les ordinateurs d'extrémité doivent être chiffrés, vous pouvez attribuer la règle sur le dossier de premier niveau de votre domaine ou de votre groupe de travail. Si votre équipe du service informatique effectue l'installation, n'affectez pas la règle avant que les ordinateurs clients aient été distribués aux utilisateurs. En effet, il y a un risque que l'ordinateur d'extrémité soit chiffré trop tôt et que le technicien du service informatique soit enregistré dans FileVault 2 à la place des utilisateurs.

Intervalle de connexion au serveur

Retrouvez plus d'informations sur les règles et l'intervalle de connexion au serveur dans le *Manuel d'administration de SafeGuard Enterprise*.

3.2 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 **`sgdeadmin --synchronize`** pour commencer à synchroniser les informations de la base de données (stratégies, clés, etc.) à partir du serveur backend SafeGuard Enterprise.

- **Activer ou désactiver le menu système**

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

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

  Remarque : le paramètre par défaut suite à l'installation de SafeGuard Native Device Encryption est « désactivé ».

  Retrouvez plus d'informations sur le menu système à la section Menu système de Sophos SafeGuard Native Device Encryption à la page 14.

Retrouvez une vue générale complète de toutes les options de la ligne de commande à la section Options de la ligne de commandes à la page 15.

4 Utilisation de SafeGuard Native Device Encryption pour Mac

Un Guide de démarrage rapide de SafeGuard Native Device 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 SafeGuard Native Device Encryption pour Mac.

4.1 Fonctionnement du chiffrement

FileVault 2 maintient toutes les données sécurisées sur le disque dur grâce au chiffrement de données XTS-AES-128 opérant au niveau du disque. L'algorithme a été optimisé pour les blocs de 512 octets. La conversion du texte brut en texte crypté et vice versa est effectuée instantanément et a peu d'impact sur l'activité de l'utilisateur étant donné sa priorité peu élevée.

L'un des obstacles classiques à l'utilisation du chiffrement intégral du disque était que l'utilisateur devait s'authentifier par deux fois : une fois pour déverrouiller le volume de démarrage chiffré (authentification au démarrage) et une seconde fois pour se connecter à son ordinateur.

Ces opérations ne sont, à présent, plus nécessaires. L'utilisateur saisit son mot de passe à la connexion avant le démarrage et le système déclenche le transfert du mot de passe lorsque le système d'exploitation est en route et demande les codes d'accès de connexion. Le transfert de mot de passe évite à l'utilisateur d'avoir à se connecter deux fois après un démarrage à froid.

L'utilisateur peut réinitialiser son mot de passe à tout moment sans avoir à chiffrer de nouveau le volume. Ceci est rendu possible par le système de clé multi-niveaux qui est utilisé. Les clés affichées à l'utilisateur (clés de connexion et clés de récupération) sont des clés de chiffrement dérivées pouvant être remplacées. L'authentique clé de chiffrement de volume n'est jamais transmise à l'utilisateur.

Retrouvez plus d'informations sur FileVault 2 dans le *Livre blanc technique d'Apple - Bon usage pour le déploiement de FileVault 2 (Août 2012)*, disponible au téléchargement sur le site Web d'Apple.

4.2 Chiffrement initial

Si un chiffrement de volume du disque système est indiqué dans la règle, le chiffrement du disque sera activé pour l'utilisateur connecté. Sur le client, procédez aux étapes suivantes :

1. Avant que l'opération de chiffrement ne démarre, une boîte de dialogue apparaît invitant à saisir le mot de passe de connexion. Veuillez saisir le mot de passe Mac OS X.

   Si la boîte de dialogue vibre, le mot de passe est incorrect. Veuillez réessayer.

   Remarque : si le mot de passe est vide, veuillez-le changer. Il n'est pas possible d'activer le chiffrement du disque sans mot de passe.

2. Patientez pendant le redémarrage du Mac.

   Remarque : en cas d'échec de l'activation du chiffrement, un message d'erreur apparaît. Retrouvez plus d'informations dans les fichiers d'historique. L'emplacement par défaut est `/var/log/system.log`

3. Le chiffrement du disque commence et s'effectue en tâche de fond. L'utilisateur peut continuer à travailler.

L'utilisateur est ajouté en tant que premier utilisateur FileVault 2 de l'ordinateur d'extrémité.

4.3 Déchiffrement

Il n'est généralement pas nécessaire de déchiffrer. Si vous définissez une règle stipulant qu'**aucun chiffrement** n'est nécessaire pour vos clients Mac déjà chiffrés, ceux-ci resteront chiffrés. Par contre, les utilisateurs auront la possibilité de les déchiffrer. Ils trouveront le bouton correspondant dans le volet de préférences. Retrouvez plus d'informations à la section Onglet Chiffrement du disque à la page 14.

Les utilisateurs disposant des droits d'administrateur local pourront déchiffrer manuellement leur disque dur à l'aide de la fonctionnalité FileVault 2 intégrée. Toutefois, ils seront invités à redémarrer pour terminer l'opération de déchiffrement. Dès que le Mac aura redémarré, SafeGuard Native Device Encryption pour Mac appliquera le chiffrement si une règle a été définie dans ce sens.

4.4 Ajout d'un utilisateur FileVault 2

Seuls les utilisateurs qui sont déjà enregistrés dans FileVault 2 sur l'ordinateur d'extrémité pourront se connecter au système après son redémarrage. Pour ajouter un utilisateur à FileVault 2, procédez de la manière suivante :

1. Lorsque le Mac est en cours de fonctionnement, connectez-vous sous le nom de l'utilisateur que vous souhaitez enregistrer dans FileVault 2.
2. Saisissez les codes d'accès de cet utilisateur dans la boîte de dialogue **Activation de votre compte**. Si vous utilisez la version 10.8 de Mac OS X, vous allez devoir saisir les codes d'accès de l'utilisateur ainsi que ceux d'un utilisateur déjà activé dans FileVault 2. La version 10.9 de Mac OS X ne vous demande pas d'effectuer ces opérations.

Par conséquent, à l'exception de la version 10.8 de Mac OS X, les utilisateurs pourront se connecter aussi facilement que s'il n'y avait aucun logiciel de chiffrement du disque installé sur leur ordinateur.

4.5 Suppression d'un utilisateur FileVault 2

Il est possible de supprimer un utilisateur de la liste des utilisateurs affectés à un Mac dans SafeGuard Management Center. À la prochaine synchronisation, l'utilisateur sera également retiré de la liste des utilisateurs FileVault 2 sur l'ordinateur d'extrémité. En revanche, ceci ne signifie pas que l'utilisateur ne sera plus en mesure de se connecter au Mac. Comme pour tout autre nouvel utilisateur, il lui suffira de se connecter à un Mac afin d'être à nouveau autorisé d'accès.

Si vous voulez vraiment empêcher un utilisateur de démarrer un Mac, indiquez que cet utilisateur est bloqué dans Management Center. L'utilisateur sera supprimé de la liste des utilisateurs FileVault 2 du client et aucune nouvelle autorisation ne sera possible.

Il est possible de supprimer les utilisateurs FileVault 2 à l'exception du dernier d'entre eux. Si le propriétaire est supprimé, l'utilisateur suivant dans la liste est indiqué comme étant le propriétaire. SafeGuard Native Device Encryption pour Mac ne fait aucune différence entre un utilisateur et un propriétaire.

4.6 Synchronisation avec le serveur backend

Pendant le processus de synchronisation, l'état des clients est signalé au serveur backend de SafeGuard Enterprise. Les règles sont mises à jour et l'attribution utilisateur/machine est vérifiée.

Les informations suivantes sont donc envoyées à partir des clients et apparaissent dans SafeGuard Management Center :

- Dès que l'ordinateur d'extrémité est chiffré, l'authentification au démarrage est vérifiée. Les autres informations affichées incluent le nom du lecteur, l'intitulé, le type, l'état, l'algorithme et le système d'exploitation.
- Les nouveaux utilisateurs FileVault 2 sont également ajoutés dans Management Center.

Remarque : si le logiciel client SafeGuard Enterprise est supprimé d'un ordinateur d'extrémité, cet ordinateur ainsi que ses utilisateurs demeurent visibles dans SafeGuard Management Center. En revanche, la date et l'heure auxquelles le serveur a été contacté pour la dernière fois ne changent plus.

Les modifications ci-dessous ont lieu sur le client :

- Les règles modifiées dans Management Center sont modifiées sur le client.
- Les utilisateurs supprimés ou bloqués dans Management Center sont également supprimés de la liste des utilisateurs FileVault 2 sur le client.

4.7 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 SafeGuard Native Device Encryption (ou Sophos SafeGuard File 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 :

4.7.1 Onglet À propos

L'onglet **À propos** vous donne des renseignements sur la version du produit installée sur le client, sur les droits d'auteur et sur les marques déposées. Si Sophos SafeGuard File Encryption est installé, il sera également répertorié dans la liste.

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

4.7.2 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 15 (commande **`sgdeadmin --enable-server-verify`** ou **`sgdeadmin --disable-server-verify`**).

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. 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 :

Ouvrez le fichier d'historique pour trouver plus de renseignements sur les causes possibles du problème.

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.

4.7.3 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 Native Device Encryption** : lorsque cette option est activée, l'icône Sophos SafeGuard Native Device Encryption apparaît dans la barre de menus. Retrouvez plus d'informations à la section Menu système de Sophos SafeGuard Native Device Encryption à la page 14.

Le troisième volet sur la fenêtre affiche les informations du **Certificat de l'utilisateur** (si un certificat d'utilisateur a été affecté dans SafeGuard Management Center) :

- **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.

4.7.4 Onglet Chiffrement du disque

Cliquez sur **Chiffrement du disque** pour afficher des informations sur les règles en cours d'application et sur l'état du client Mac.

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

Le second volet affiche l'état du client 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, un bouton **Déchiffrer le disque système** apparaît. Il sera activé si FileVault 2 est activé, si l'utilisateur est activé dans FileVault 2 et si le responsable de la sécurité a défini une règle stipulant que le chiffrement n'est pas nécessaire pour le client.

Remarque : si aucune clé de récupération centrale n'est disponible, le support technique ne pourra pas vous aider à récupérer votre mot de passe. Dans ce cas, la clé de récupération doit être importée à l'aide de l'outil de ligne de commande : **`sgdeadmin --import-recoverykey`**. Si l'utilisateur et le responsable de la sécurité ne savent pas quelle clé de récupération utiliser, le déchiffrement et le chiffrement du disque seront nécessaires afin de créer une nouvelle clé de récupération.

4.8 Menu système de Sophos SafeGuard Native Device Encryption

Le menu système fournit les informations suivantes :

- L'icône (sur la gauche) indique l'état du chiffrement :

Figure 1 : menu système

	Icône verte : le disque système est chiffré.
	Icône rouge : le disque système n'est pas chiffré.

- L'élément suivant du menu est disponible lorsque vous cliquez sur l'icône :
  - **Ouvrir les préférences Sophos Encryption...**

    Ouvre la fenêtre de préférences Sophos Encryption.

Remarque : retrouvez plus d'informations sur l'activation ou la désactivation du menu système à la section Onglet Utilisateur à la page 13.

4.9 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)
`sgdeadmin`	Répertorie toutes les commandes disponibles y compris les conseils d'utilisation.	**`--help`**
`sgdeadmin --version`	Affiche la version et le copyright du produit installé.	
`sgdeadmin --status`	Renvoie des informations sur l'état du système telle que la version, le serveur et le certificat.	
`sgdeadmin --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.
`sgdeadmin --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.

Nom de la commande	Définition	Paramètres additionnels (facultatif)
`sgdeadmin --synchronize`	Force l'établissement d'un contact immédiat avec le serveur (une connexion au serveur est nécessaire).	
`sgdeadmin --import-recoverykey` ["recoverykey"]	Importe la clé de récupération FileVault 2 et remplace la clé de récupération déjà existante.	**`--force`** remplace la clé de récupération déjà existante sans demander de confirmation supplémentaire **`"recoverykey"`** demande à l'utilisateur de saisir la clé de récupération s'il ne l'a pas fait.
`sgdeadmin --import-config "/path/to/target/file"`	Importe le fichier ZIP de configuration indiqué. Retrouvez plus d'informations à la section Installation manuelle (sous surveillance) à la page 6. 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.	
`sgdeadmin --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).	
`sgdeadmin --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.	

Nom de la commande	Définition	Paramètres additionnels (facultatif)
`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 8 :

- **`sgdeadmin --enable-systemmenu`**
- **`sgdeadmin --disable-systemmenu`**
- **`sgdeadmin --synchronize`**

5 Récupération

La récupération est un moyen d'accéder à un volume chiffré à l'aide d'une clé de récupération archivée de manière centralisée. Cette opération est particulièrement utile lorsqu'un utilisateur a oublié son mot de passe de connexion Mac OS X et qu'aucun autre code d'accès n'est disponible.

5.1 Gestion de la clé de récupération

Si tous les utilisateurs FileVault d'un système particulier oublient leur mot de passe, si les autres codes d'accès ne sont pas disponibles et si aucune clé de récupération n'est disponible, le volume chiffré ne peut pas être déverrouillé et les données sont inaccessibles. Il se peut que les données soient définitivement perdues. Par conséquent, il est essentiel de préparer un programme de récupération correct.

Une nouvelle clé de récupération est générée à chaque activation du chiffrement du disque. Si Sophos SafeGuard Native Device Encryption n'est pas installé au moment de l'opération de chiffrement, elle est visible par l'utilisateur qui en est, par conséquent, responsable et doit veiller à ne pas la perdre. Si Sophos SafeGuard Native Device Encryption est installé, elle est envoyée par un canal sécurisé au serveur backend de SafeGuard Enterprise et archivée de manière centralisée. Le responsable de la sécurité peut la récupérer à chaque fois qu'il en a besoin. Retrouvez plus d'informations sur le processus de récupération à la section Oubli du mot de passe de connexion à Mac OS X à la page 18.

Même si SafeGuard Native Device Encryption n'a pas été installé lorsque le disque a été chiffré, la clé de récupération peut être gérée de manière centralisée. Il est donc nécessaire de l'importer. L'option de ligne de commande adéquate est **`sgdeadmin --import-recoverykey`**. Retrouvez plus d'informations à la section Options de ligne de commande à la page 15. La clé de récupération sera envoyée en lettre majuscule.

Remarque :

- Mac OS X 10.8 : la clé de récupération ne sera pas vérifiée. Il relève de la responsabilité de l'utilisateur de la saisir correctement. Un message d'erreur apparaîtra uniquement en cas de format incorrect.
- Mac OS X 10.9 : la clé de récupération sera vérifiée.

Retrouvez plus d'informations sur la vérification qu'une clé de récupération est bien présente pour un client à la section Onglet Chiffrement du disque à la page 14.

En cas de présence d'une clé de récupération institutionnelle, elle peut également être utilisée à des fins de récupération. Retrouvez plus d'informations dans l'article *OS X : création et déploiement d'une clé de secours pour FileVault 2* sur support.apple.com/kb/HT5077

5.2 Oubli du mot de passe de connexion Mac OS X

Si un utilisateur oublie son mot de passe de connexion Mac OS X et que vous n'avez pas d'autres codes d'accès à disposition, procédez de la manière suivante :

1. L'utilisateur allume le Mac.

2. L'utilisateur clique sur le symbole **?** dans la boîte de dialogue de connexion. L'utilisateur peut également saisir un mot de passe de connexion incorrect trois fois successivement.

   Le mémo de mot de passe apparaît et l'utilisateur est invité à réinitialiser son mot de passe à l'aide de la clé de récupération.

3. L'utilisateur clique sur le triangle se trouvant à côté du message afin de passer à l'étape suivante (saisie de la clé de récupération) :

   

4. Dans SafeGuard Management Center, ouvrez l'assistant de récupération en sélectionnant **Outils** > **Récupération** pour afficher la clé de récupération de la machine spécifique.
5. Communiquez à l'utilisateur la clé de récupération à saisir sur le Mac.

   Le Mac démarre et l'utilisateur est invité à saisir le nouveau mot de passe et un mémo de mot de passe.

Mac OS X 10.9 uniquement : la clé de récupération est remplacée dès sa première utilisation pour démarrer le système. La nouvelle clé de récupération est générée automatiquement et envoyée au serveur backend SafeGuard Enterprise sur lequel elle va être archivée et mise à disposition pour la prochaine opération de récupération.

Remarque : veuillez uniquement communiquer la clé de récupération d'un ordinateur d'extrémité à une personne de confiance. Une clé de récupération est toujours spécifique à une machine et pas à un utilisateur. Il est donc nécessaire de vérifier qu'elle n'est pas utilisée pour obtenir un accès non autorisé aux données sensibles d'un autre utilisateur sur la même machine.

6 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 */Library*.
2. Sélectionnez le dossier */Sophos SafeGuard DE*.
3. Sélectionnez et cliquez deux fois sur le fichier *Sophos SafeGuard DE Uninstaller.pkg*
4. Un assistant vous guide tout au long de la désinstallation.

Remarque : il n'est pas nécessaire de déchiffrer le disque avant de désinstaller le logiciel.

Remarque : tout utilisateur avec les droits administratifs sera en mesure de désinstaller le logiciel. (Une règle empêchant d'effectuer cette opération sur les clients Windows n'a aucun effet sur les clients 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.

7 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.

8 Mentions légales