SOPHOS
Security made simple.

SafeGuard Enterprise
Guide de conseils pratiques

Version du produit : 8
Date du document : juillet 2016

Table des matières

1 À propos de ce guide

Ce guide est divisé en deux parties :

La section Introduction à Synchronized Encryption à la page 4 vous aide à commencer à utiliser le nouveau module Synchronized Encryption.

Elle fournit un aperçu des fonctions, de leur mode de fonctionnement et de la manière de les intégrer à votre environnement. Retrouvez plus de renseignements sur le module Synchronized Encryption dans l'Aide à l'administration de SafeGuard Enterprise.

La section Conseils pratiques à la page 13 fournit des conseils pour le déploiement, l'administration et l'utilisation harmonieuses de SafeGuard Enterprise.

Cette partie n'est pas un guide d'installation mais est destinée aux personnes qui sont déjà familières avec le produit. Retrouvez plus de renseignements sur l'installation et l'administration dans l'Aide à l'administration de SafeGuard Enterprise.

2 Introduction à Synchronized Encryption

Synchronized Encryption est le nouveau module de chiffrement de fichiers de Sophos SafeGuard Enterprise. Les principales modifications apportées au chiffrement de fichiers par rapport aux versions précédentes de SafeGuard Enterprise sont :

- Chiffrement automatique des fichiers créés ou modifiés par les applications définies (apps intégrées).
- Seules les applications définies peuvent déchiffrer les fichiers.
- Le chiffrement ne dépend pas de l'emplacement du fichier.
- Les clés de chiffrement peuvent être échangées avec les appareils mobiles exécutant iOS ou Android.

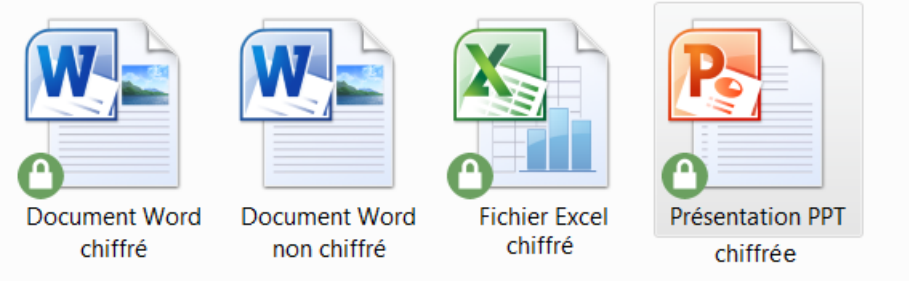
  Remarque : veuillez définir l'environnement Sophos Mobile Control pour communiquer avec SafeGuard Enterprise.
- Les clés de chiffrement peuvent être automatiquement supprimées des appareils des utilisateurs en cas de menace à la sécurité suspectée.

  Remarque : cette fonction est uniquement disponible si vous utilisez Sophos Central Endpoint Protection avec SafeGuard Enterprise. Vous devez créer une stratégie SafeGuard Enterprise pour supprimer les clés de chiffrement. Cette fonction est disponible sur les terminaux Windows et Mac OS X.
- Les utilisateurs peuvent obtenir la clé de récupération de leur chiffrement par volume (Chiffrement de lecteur BitLocker sur les machines Windows ou FileVault2 sur les machines Mac OS X) via leur appareil mobile.

2.1 Utilisation d'applications standard

Synchronized Encryption vous permet de travailler comme d'habitude sans avoir à vous soucier du chiffrement. C'est uniquement lorsque vous partagez des informations en externe que vous devrez penser au destinataire auquel vous envoyez ces informations et au niveau de sécurité le plus adéquat à utiliser.

Par exemple, vous créez du contenu dans Excel ou PowerPoint comme d'habitude. Le document est chiffré dès que vous l'enregistrez. Les documents chiffrés sont identifiables par l'icône d'un cadenas affiché au-dessus de l'icône originale.



2.2 Partage d'informations dans l'entreprise

Une seule clé de chiffrement est utilisée dans cette version de SafeGuard Enterprise (SGN 8). Il est donc plus facile de partager les informations en interne. Chaque utilisateur de SafeGuard Enterprise pourra lire les informations.

Vous pouvez partager les documents chiffrés comme vous le faites d'habitude. Placez-les sur un partage réseau ou copiez-les sur un périphérique de stockage amovible.

Vous devez installer le module Synchronized Encryption sur les ordinateurs de tous les utilisateurs qui nécessitent l'accès aux informations partagées dans l'entreprise.

Remarque : assurez-vous d'installer SafeGuard Enterprise pour les utilisateurs Windows et Mac OS X.

2.3 Partage d'informations avec des parties externes

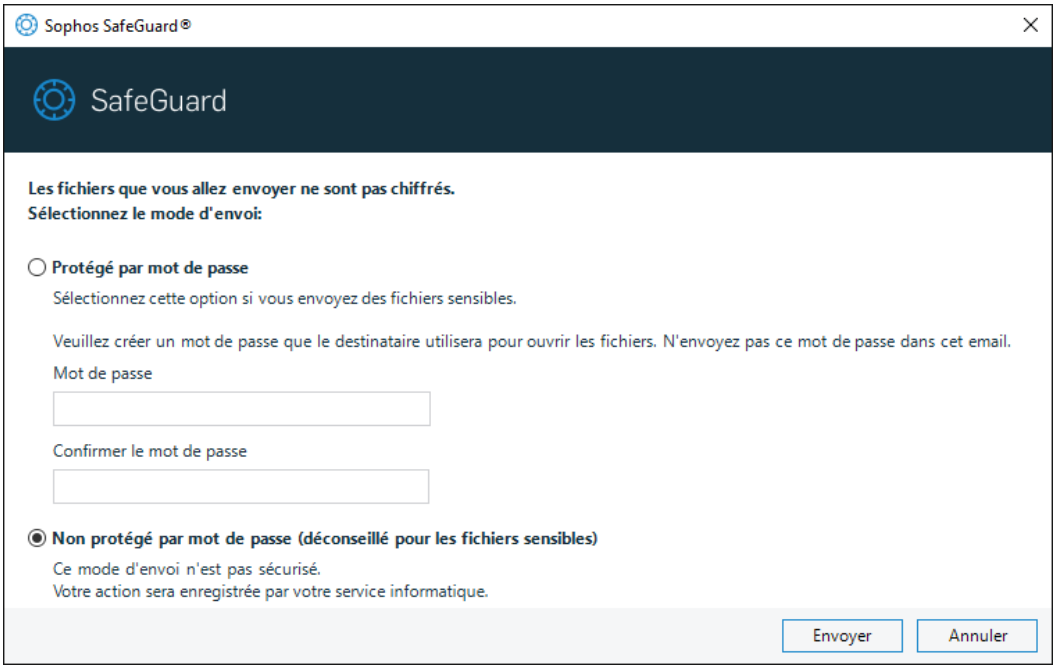
Le chiffrement des informations a pour but de limiter l'accès aux données sensibles. Un document contenant des informations d'ordre financier ou de propriété intellectuelle ne doit pas être mis à la disposition de tous. Toutefois, il peut arriver que vous souhaitiez partager ces informations avec des personnes n'appartenant pas à votre entreprise. Il peut également arriver que vous souhaitiez parfois que ces informations demeurent chiffrées et d'autres fois que vous décidiez que ces informations ne sont plus confidentielles.

Différentes procédures de travail s'appliquent aux utilisateurs d'Outlook et aux autres utilisateurs.

Info : assurez-vous que l'Aide à l'utilisation de SafeGuard Enterprise est disponible pour tous vos utilisateurs.

Utilisateurs d'Outlook

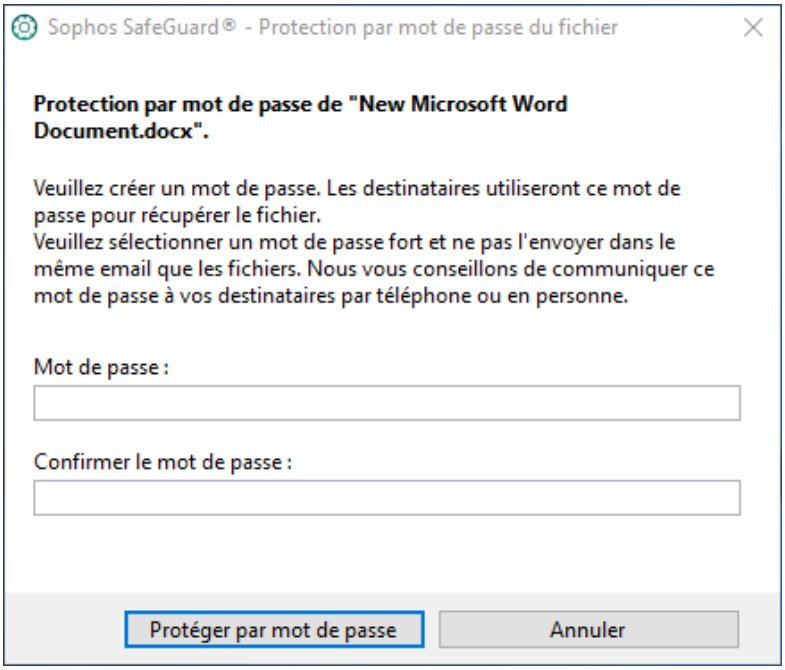
Sur les machines Windows avec Microsoft Outlook (version 32 bits d'Office uniquement), les utilisateurs n'ont pas à se soucier du chiffrement. Vous pouvez configurer Synchronized Encryption afin qu'un message apparaisse pour demander comment traiter le fichier lorsque les utilisateurs envoient un email avec une pièce jointe à au moins un destinataire externe.



Autres utilisateurs

Les utilisateurs Windows et Mac peuvent déchiffrer les fichiers pour les envoyer non chiffrés ou pour créer un fichier protégé par mot de passe avant de le partager.

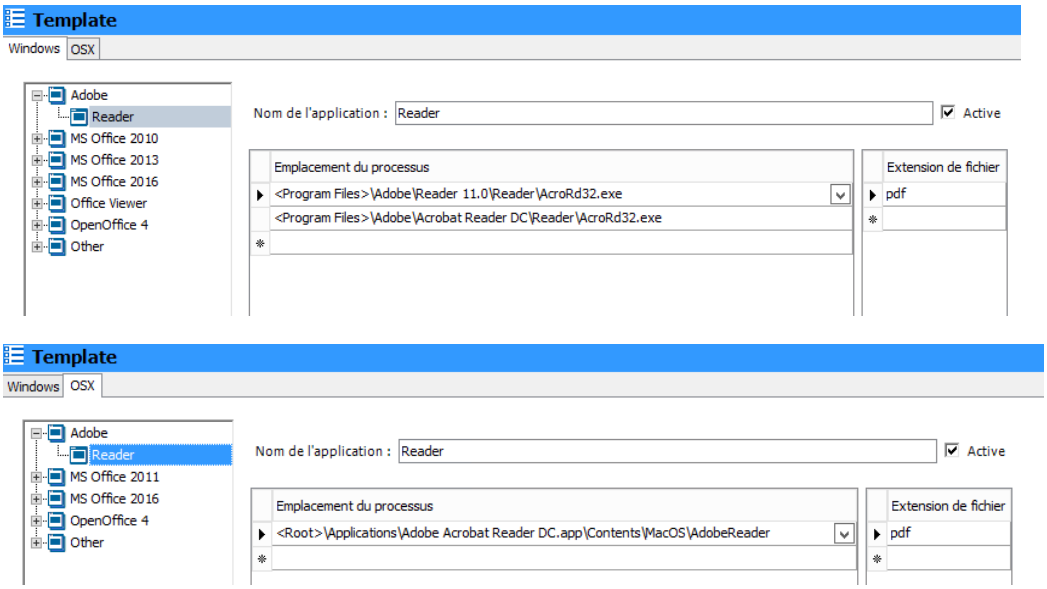
Ils peuvent cliquer avec le bouton droit de la souris sur un fichier puis sélectionner **Chiffrement de fichiers SafeGuard** et **Déchiffrer le fichier sélectionné**. Ils peuvent également cliquer avec le bouton droit de la souris sur un fichier puis sélectionner **Chiffrement de fichiers SafeGuard** et choisir **Créer un fichier protégé par mot de passe**. Dans ce cas, un nouveau fichier est créé avec une extension HTML et le destinataire peut y accéder en saisissant le mot de passe que l'utilisateur a créé.



Retrouvez plus de renseignements dans l'Aide à l'utilisation de SafeGuard Enterprise à la section Envoi sécurisé des pièces jointes par email.

2.4 Définition des apps intégrées

Les apps intégrées sont des applications capables de créer et d'accéder au contenu chiffré. Ces applications sont définies par le responsable de la sécurité de SafeGuard Enterprise à l'aide de chemins complets à la fois sur Windows et sur Mac OS X.



Info : assurez-vous que les applications sont installées au même emplacement sur toutes les machines ou incluez tous les chemins d'installation possibles dans la définition des apps intégrées.

2.4.1 Quelles apps intégrées dois-je définir ?

Les apps intégrées sont les seules applications capables de créer et de lire le contenu chiffré. Veuillez inclure toutes les applications que vous prévoyez d'utiliser pour créer ou lire du contenu chiffré.

Pour les applications de création de contenu, ceci inclut généralement :

- Suites Office (Microsoft Office, OpenOffice, FreeOffice, ...)
- Suites Design (Adobe Creative Suite, ...)

Les applications de lecture sont :

- Visionneuses Office
- Visionneuses PDF
- Visionneuses d'images

  Remarque : vous ne pouvez pas ajouter les apps de la boutique Windows à la liste des apps intégrées.

Info : prenez en compte tous les types de fichiers pouvant être utilisés par le logiciel de création de contenu. Par exemple, pour Microsoft Word, veuillez inclure .docx et .rtf, .odt, etc.

Dans certains cas, vous ajouterez des applications qui sont uniquement utilisées par certains utilisateurs. Ceci ne signifie pas que vous devez uniquement appliquer la stratégie à ces

personnes. Si les utilisateurs reçoivent une stratégie pour une application qu'ils n'ont pas installée, cette partie de la stratégie sera ignorée.

2.4.2 Quelles applications ne doivent jamais être définies comme app intégrée ?

Le but du chiffrement étant d'éviter toute fuite d'informations à l'extérieur de votre entreprise, les applications utilisées pour envoyer des informations ne doivent en aucun cas être définies comme apps intégrées. Si elles le sont, tout le contenu sera déchiffré avant d'être envoyé et les données ne seront pas protégées.

Veuillez ne jamais définir les applications telles que les clients de messagerie, les navigateurs Internet, les logiciels de sauvegarde, etc. en tant qu'apps intégrées.

Remarque : pour Mac OS X, il pourrait être utile d'inclure des programmes de messagerie car le module complémentaire Outlook n'est pas disponible. Retrouvez plus de renseignements à la section Stratégies pour les terminaux Mac OS X à la page 16.

2.5 Problèmes à prendre en compte avant le déploiement

Veuillez envisager de déployer Synchronized Encryption à un nombre limité de personnes (groupe de test) uniquement. Assignez à tous les autres une stratégie sans chiffrement mais fournissez leur la clé de chiffrement afin qu'ils puissent lire les fichiers chiffrés créés par leurs collègues. Retrouvez plus de renseignements à la section Création de stratégies en lecture seule à la page 10.

Veuillez envisager les problèmes suivants avant de déployer Synchronized Encryption.

2.5.1 Ouverture des fichiers créés avec une app particulière dans une app différente

Plusieurs applications peuvent créer des fichiers sous différents formats. Ceci signifie que vous devez penser à l'application utilisée pour ouvrir et lire le fichier. Par exemple, Microsoft Word permet de créer des fichiers PDF facilement. Lorsque Microsoft Word est défini en tant qu'application de chiffrement (app intégrée), les fichiers PDF seront chiffrés. Il s'agit d'un comportement prévu car le contenu est peut être sensible.

Toutefois, ceci signifie que vous devez penser à l'application utilisée pour ouvrir et lire le fichier. Dans notre exemple, nous utilisons un lecteur de PDF et même si les lecteurs de PDF ne sont pas généralement utilisés pour créer des fichiers, ils doivent cependant être définis comme des apps intégrées. Dans le cas contraire, vous ne serez pas en mesure de lire les fichiers dans les lecteurs de PDF. Pour cette raison, nous avons déjà inclus les lecteurs de PDF les plus usuels dans le modèle de la liste d'applications de la version 8 de SafeGuard Management Center.

D'autres exemples :

Les apps intégrées qui exportent des images graphiques

Les apps intégrées qui exportent des fichiers sous différents formats de texte tels que .txt, .rtf, .csv et bien d'autres encore.

Info : envisagez l'utilisation de lecteurs par défaut pour tous les types de fichiers que vous pouvez créer avec les apps intégrées définies. Assurez-vous que ces lecteurs sont installés

sur toutes les machines et faites en également des apps intégrées afin qu'ils puissent lire le contenu chiffré.

2.5.1.1 Fichiers PDF sur Windows 10

Le lecteur de PDF par défaut sur Windows 10 est le nouveau navigateur Internet Edge. Vous pourriez ajouter Edge à la liste des apps intégrées. Dans ce cas, tous les fichier téléchargés sur Internet avec Edge seront déchiffrés.

Important : déployez les machines Windows 10 avec un autre lecteur PDF que le lecteur Edge intégré par défaut. Utilisez par exemple Adobe Acrobat Reader ou Foxit Reader.

2.5.2 Applications Java

Les applications Java partagent souvent le même fichier exécutable `java.exe`. Il n'est pas possible de faire la distinction entre les différentes applications Java par leur chemin d'exécution `java.exe`.

Si vous définissez java.exe en tant qu'app intégrée, veuillez noter que toutes les applications qui utilisent cet exécutable créeront et pourront accéder au contenu chiffré.

2.5.3 Applications Web

Des groupes de personnes travaillent souvent sur des documents qu'ils téléchargent ensuite sur une application Web. Les fichiers chiffrés demeurent chiffrés afin que le système sous-jacent ne soit pas en mesure de les lire. Ceci signifie que :

- Il est impossible d'indexer ces fichiers selon leur contenu.
- Ces fichiers sont illisibles lorsqu'ils sont accédés par une personne externe.

Vous pourriez avoir besoin d'un accès externe à ces fichiers. Les utilisateurs peuvent déchiffrer les fichiers avant de les télécharger. Autrement, vous pouvez créer un dossier dans lequel les fichiers seront enregistrés sans être chiffrés.

Ce dossier d'exception doit exclusivement être utilisé dans ce but. Veillez à communiquer ceci clairement aux utilisateurs.

Info : créez une exception pour les fichiers chiffrés, soit à l'aide d'un chemin complet (par exemple ; **`c:\unencrypted`**) soit à l'aide d'un chemin relatif (uniquement disponible sur les clients Windows). Si vous utilisez un chemin relatif, les utilisateurs ont uniquement besoin de créer un dossier avec un nom convenu entre les deux parties. Par exemple, si le nom du dossier est **`\unencrypted`**, les fichiers et sous-dossiers de chaque dossier **`\unencrypted`** sur l'ordinateur ne seront pas chiffrés quel que soit l'emplacement.

2.5.4 Échange d'informations avec les plates-formes sans chiffrement SafeGuard

Certains utilisateurs créent des fichiers destinés à être utilisés sur un autre environnement. Par exemple, les fichiers créés sur un poste de travail Windows ou Mac OS X sont utilisés sur un environnement Terminal Server. Comme SafeGuard Enterprise n'est pas compatible avec les environnements Terminal Server, ces fichiers demeureront chiffrés et aucune application ne pourra les lire à cet endroit.

La solution est de créer un chemin d'exclusion dans la stratégie de chiffrement pour ces emplacements.

2.5.5 Quel est l'impact sur mes aperçus ?

Les explorateurs de fichiers (Explorateur Windows ou Finder) peuvent afficher des aperçus de différents types de fichiers tels que les images, les documents texte, les feuilles de calcul, les fichiers pdf, etc. Ces aperçus sont généralement compilés lorsque le fichier est stocké ou modifié. L'application qui crée ces aperçus doit avoir accès au contenu déchiffré du fichier. Vous allez donc devoir l'ajouter à la liste des apps intégrées. Sur Mac OS X, ceci est possible (et effectué par défaut) car cette application est séparée.

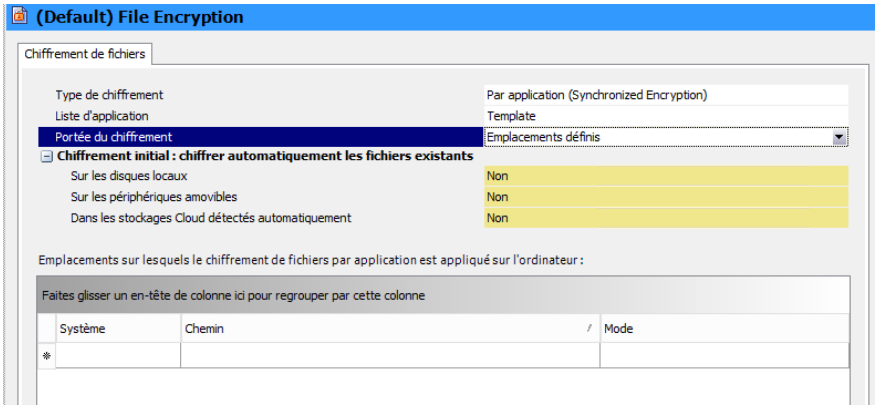
2.6 Création de stratégies en lecture seule

Lorsque vous commencez le déploiement de Synchronized Encryption, les utilisateurs doivent être en mesure de lire les documents chiffrés mais pas de les chiffrer. Vous pouvez alors commencer à activer le chiffrement pour des groupes dédiés et enfin pour tout le monde.

La première stratégie est une stratégie en lecture seule.

Windows

Pour les utilisateurs Windows, vous devez créer une stratégie Synchronized Encryption incluant toutes vos applications et indiquez les **Emplacements définis** en tant que **Portée du chiffrement** mais ne pas définir les emplacements !



Retrouvez plus de renseignements dans l'Aide à l'administration de SafeGuard Enterprise à la section Création d'une stratégie de lecture seule pour les terminaux Windows.

Mac OS X

Mac OS X fonctionne différemment de Windows. Sur les ordinateurs Mac OS X, la lecture de fichiers chiffrés fonctionne uniquement dans les emplacements définis.

Ceci signifie que la stratégie en lecture seule appliquée aux utilisateurs Windows ne peut pas être appliquée aux utilisateurs Mac OS X.

Pour Mac OS X, veuillez créer une stratégie de type **Chiffrement de fichiers** et sélectionnez **Par emplacement** comme type de chiffrement. Vous devez ajouter au moins un emplacement, l'**exclure** du chiffrement et communiquez le nom de cet emplacement à vos utilisateurs Mac OS X. Il peut s'agir par exemple de **`<Documents>/Chiffrés`**. Les utilisateurs qui veulent lire un document chiffré devront alors déplacer ou copier le fichier dans cet emplacement.

Retrouvez plus de renseignements dans l'Aide à l'administration de SafeGuard Enterprise à la section Création d'une stratégie de lecture seule pour les terminaux Mac.

2.7 Information des utilisateurs

Dans la majorité des cas, le chiffrement sera une chose totalement nouvelle pour les utilisateurs. Nous vous conseillons de communiquer les procédures et règles de chiffrement à vos utilisateurs. Il est tout particulièrement important que les utilisateurs sachent à quoi s'attendre avec le chiffrement synchronisé. Par exemple : quelles applications sont considérées comme apps intégrées ? Lorsqu'un utilisateur est au courant de ceci, il peut immédiatement remarquer qu'une clé d'application est manquante et avertir le responsable de la sécurité de SafeGuard Enterprise. Il pourra ensuite ajouter cette application à la liste des apps intégrées.

Procédure conseillée :

Envoyez un email à tous les utilisateurs leur expliquant brièvement les règles de chiffrement appliquées et leurs conséquences. Utilisez idéalement un site Web interne en tant que référence. Ceci vous permettra de le modifier facilement lors, par exemple, de l'ajout de nouvelles apps intégrées.

Incluez une adresse email à laquelle adresser des commentaires dans le message.

Si vous avez déjà déployez SafeGuard Enterprise sur tous les terminaux (par exemple en mode lecture seule), vous pouvez inclure un document qui a été chiffré avec la clé Synchronized Encryption et demandez aux utilisateurs de vérifier s'ils sont en mesure de la lire. Dans le cas contraire, vous saurez qu'un problème a eu lieu lors de l'installation ou lors de la communication entre le terminal et le serveur backend de SafeGuard Enterprise avant que vous ayez activé le chiffrement pour tout le monde.

2.7.1 Exemple de communication

Retrouvez ci-dessous un exemple d'email à utiliser pour informer vos utilisateurs. Il contient les informations les plus importantes mais vous pouvez également ajouter d'autres renseignements que vous jugez utiles comme par exemple lorsque vous avez créé une règle d'exception pour tous les dossiers nommés « unencrypted » ou lorsque vous utilisez d'autres applications. Cet exemple d'email suppose qu'il a été envoyé avec un document en pièce jointe chiffré avec la clé Synchronized Encryption.

= =

Bonjour à tous,

Le service informatique a terminé le déploiement de SafeGuard Enterprise sur toutes vos machines. Il s'agit d'une solution de chiffrement de la société Sophos que tous les employés utiliserons pour protéger les documents de l'entreprise. En principe, ce produit ne devrait pas perturber vos tâches quotidiennes. Toutefois, il existe certaines exceptions.

Nous allons activer le module Synchronized Encryption pour tous les employés à partir de la semaine prochaine. Une fois activé, vous créerez automatiquement des fichiers chiffrés sur votre ordinateur. Nous avons compilé un certain nombre de documents disponible sur intranet pour vous aider à démarrer. Rendez-vous sur la page d'accueil de l'intranet et cliquez sur Chiffrement ou rendez-vous à l'adresse https://entreprise.interne/chiffrement.

Pour vérifier que votre système est prêt, veuillez ouvrir le fichier joint.

Windows et Mac OS X : si vous pouvez ouvrir le document et lire le message, vous êtes prêts ! Si vous ne pouvez pas lire le message dans le fichier correctement, veuillez contacter votre service informatique pour obtenir plus d'assistance.

iOS et Android : ouvrez la pièce jointe dans l'app Sophos Secure Workspace sur votre appareil. La visionneuse de fichiers de l'appareil ne pourra pas ouvrir le fichier car il est

chiffré. Si vous n'avez pas installé Sophos Secure Workspace sur votre appareil mobile, veuillez contacter le service informatique pour obtenir plus d'assistance.

Applications à utiliser

Les applications suivantes vont automatiquement créer du contenu chiffré sur votre ordinateur. Si vous utilisez des applications différentes pour accéder aux fichiers chiffrés, vous ne verrez que le contenu chiffré.

Windows :

- Adobe Reader
- MS Office 2010 (Excel, PowerPoint, Word)
- MS Office 2013 (Excel, PowerPoint, Word)
- MS Office 2016 (Excel, PowerPoint, Word)
- Visionneuses Office
- Foxit Reader pour PDF

Mac OS X :

- Adobe Reader
- Productivité Apple (Keynote, Numbers, Pages, Preview)
- MS Office 2011 (Excel, PowerPoint, Word)
- MS Office 2016 (Excel, PowerPoint, Word)

Envoi de fichiers

Lors de l'envoi d'un email à un destinataire externe, veuillez noter que le fichier sera envoyé chiffré. Ceci signifie que votre destinataire ne sera pas en mesure de lire le contenu. Vous pouvez déchiffrer le fichier avant de l'envoyer si son contenu n'est pas confidentiel. Si le contenu est confidentiel, ou en cas de doute, veuillez créer un fichier chiffré protégé par mot de passe. Cliquez avec le bouton droit de la souris sur le fichier et sélectionnez « Chiffrement de fichiers SafeGuard ». Puis, sélectionnez soit « Déchiffrer le fichier sélectionné », soit « Créer un fichier protégé par mot de passe ».

Si vous utilisez **Windows** et envoyez le fichier avec **Microsoft Outlook**, vous n'avez pas besoin d'effectuer cette opération manuellement. Lorsque le système détecte que vous envoyez un fichier chiffré à un destinataire externe, il vous demande comment vous voulez traiter le fichier.

Téléchargement de fichiers sur nos applications Web

Lorsque vous téléchargez des fichiers chiffrés, ceux-ci ne sont pas déchiffrés. Ils demeurent chiffrés dans SharePoint ou dans toute autre application Web que vous utilisez. Vous pouvez déchiffrer ces fichiers manuellement. Veuillez noter que vous ne serez pas en mesure de voir un aperçu et que l'indexation des fichiers ne fonctionnera pas non plus.

Problèmes ? Suggestions ?

En cas de problèmes avec SafeGuard Enterprise ou avec votre ordinateur suite à l'activation du chiffrement, veuillez créer un ticket informatique auprès du service informatique.

Cordialement,

3 Conseils pratiques

3.1 Déploiement

Remarque : l'utilisation de SafeGuard Enterprise Server et de SafeGuard Management Center nécessite l'installation de .NET 4.5.

Suggestions générales

- Essayez d'éviter un déploiement simultané du nouveau module Synchronized Encryption et de l'ancien module File Encryption de SafeGuard Enterprise.
- Un déploiement par phase nécessite la vérification de chaque étape, tout particulièrement pour les membres de groupes Active Directory imbriqués d'une grande complexité.
- La formation des utilisateurs est essentielle à un déploiement et à un fonctionnement sans problème.
- Une communication claire sur les participants et sur les conséquences d'une telle opération est également primordiale.
- Les équipes des services informatique et du support doivent être en mesure de répondre de manière adéquate.

Conditions préalables

- SafeGuard Enterprise 8 doit être installé sur tous les terminaux. Autrement, le partage des fichiers chiffrés ne sera pas transparent et les procédures de travail habituelles seront affectées.
- Si vous voulez lire les fichiers chiffrés sur les appareils mobiles (une nouvelle fonction de SafeGuard Enterprise 8), veuillez également déployer l'app Sophos Secure Workspace.

  Remarque : pour lire les fichiers chiffrés sur les appareils mobiles, veuillez utiliser Sophos Secure Workspace administrée par Sophos Mobile Control.
- Assurez-vous que les utilisateurs en déplacement se connectent régulièrement au serveur backend de SafeGuard Enterprise via VPN ou par « Accès direct » (Windows) afin que les stratégies de chiffrement les plus récentes soient appliquées.

3.1.1 Préparation des terminaux pour Synchronized Encryption

Pour un fonctionnement correct du module Synchronized Encryption, veuillez installer le programme **`vstor-redist.exe`** de Microsoft. Ce fichier va installer Microsoft Visual Studio 2010 Tools for Office Runtime et il est inclus dans le package d'installation.

Nous vous conseillons d'installer les composants dans l'ordre suivant :

1. **`vstor-redist.exe`**
2. **`SGNClient.msi`**
3. package de configuration

Remarque : vous pouvez déployer le package de configuration pendant l'installation de **`vstor-redist.exe`**.

3.1.2 Déploiement partiel

Dans la majorité des situations, le nouveau module **Synchronized Encryption** ne peut pas être déployé et activé en une seule fois et rapidement pour tous les employés. Dans ce genre de situations, il est important de donner aux utilisateurs l'accès en lecture seule aux fichiers chiffrés même s'ils se trouvent sur des terminaux SafeGuard Enterprise sans que le module **Synchronized Encryption** ne soit activé. Par conséquent, une stratégie en lecture seule est requise.

Pour donner les droits en lecture seule aux utilisateurs, veuillez procéder de la manière suivante :

La clé **Synchronized Encryption**.

Elle est assignée au nœud racine de SafeGuard Management Center par défaut et tous les employés d'une entreprise doivent obtenir automatiquement cette clé.

Une **Liste d'applications** et une stratégie en lecture seule spécifique.

Retrouvez plus de renseignements sur le déploiement partiel de Synchronized Encryption dans l'Aide à l'administration de SafeGuard Enterprise à la section Déploiement partiel de Synchronized Encryption.

3.1.3 Utilisation de Synchronized Encryption et de SafeGuard Enterprise File Encryption dans le même environnement

Remarque : si votre environnement nécessite l'utilisation de SafeGuard Synchronized Encryption et de SafeGuard File Encryption, envisagez la procédure suivante afin de bénéficier d'une intégration harmonieuse.

Synchronized Encryption prend en charge une clé de chiffrement pour toute l'entreprise. L'administration et le déploiement sont donc plus faciles à effectuer. Certains services comme les Ressources Humaines ou les Finances pourraient avoir besoin d'une protection cryptographique différente des autres services afin que leurs documents soient uniquement accessibles au sein de leur service.

Dans ce cas de figure, les modules SafeGuard Enterprise File Encryption (File Share, Cloud Storage, Data Exchange) doivent être utilisés. Ces modules permettent d'utiliser différentes clés pour le chiffrement de fichiers. Vous ne pouvez pas installer le module Synchronized Encryption et les modules SafeGuard Enterprise File Encryption sur la même machine.

Pour utiliser les modules Synchronized Encryption et SafeGuard Enterprise File Encryption, vous allez devoir effectuer des tâches administratives supplémentaires :

1. Le déploiement de SafeGuard Enterprise doit prendre en compte les différents modules à installer pour certains services.
2. Les services avec des besoins spéciaux, doivent récupérer d'autres stratégies que celles assignées sur les terminaux **Synchronized Encryption**. Pour que ceci soit possible, la structure AD importée doit autoriser une assignation de ces stratégies aux utilisateurs et machines concernés.
3. La procédure de déploiement/d'installation des modules SafeGuard Enterprise doit être effectuée conformément aux stratégies assignées : les bonnes machines doivent récupérer les bonnes stratégies.

Remarque : le module complémentaire Outlook n'est pas disponible sur les modules SafeGuard Enterprise File Encryption. Par conséquent, les terminaux Synchronized Encryption et File Encryption ne peuvent pas partager les pièces jointes chiffrées de manière transparente.

Conseils d'utilisation

- Les utilisateurs des modules SafeGuard Enterprise File Encryption doivent récupérer la clé **Synchronized Encryption**. Les utilisateurs peuvent ensuite lire les fichiers chiffrés à l'aide de la clé **Synchronized Encryption** de manière transparente.
- Partage des fichiers chiffrés :

  Pour les utilisateurs des modules SafeGuard Enterprise File Encryption, nous conseillons de créer une stratégie qui définit la clé **Synchronized Encryption** à utiliser pour un partage de « transfert ». Tous les fichiers créés ou déplacés dans ce partage devront être chiffrés avec la clé **Synchronized Encryption**. Les utilisateurs **Synchronized Encryption** sont en mesure de lire ces fichiers.

- Partage des fichiers clairs :

  Pour les utilisateurs des modules SafeGuard Enterprise File Encryption, une stratégie qui exclut un dossier du chiffrement peut être utilisée (**Type de chiffrement** : **Par emplacement**, **Mode** : **Exclure**).

- Lorsque les utilisateurs des modules SafeGuard Enterprise File Encryption veulent partager des fichiers avec les utilisateurs **Synchronized Encryption**, ils doivent d'abord les déchiffrer. Ils peuvent ensuite décider d'envoyer les fichiers déchiffrés ou de les chiffrer à l'aide de la clé Synchronized Encryption.

3.1.4 Vérification de la validité des certificats d'utilisateur

La vérification de la validité des certificats d'utilisateur est particulièrement importante pour les entreprises qui utilisent uniquement l'administration SafeGuard Enterprise BitLocker et qui souhaitent ajouter la fonction de chiffrement synchronisé **Synchronized Encryption**.

Vous pouvez vérifier les certificats dans SafeGuard Management Center sous **Clés et certificats** > **Certificats** > **Certificats assignés**.

Le certificats ayant expiré ou arrivant bientôt à échéance sont marqués en rouge dans la colonne **Expire le**. Pour renouveler un certificat arrivant bientôt à échéance, veuillez cocher la case dans la colonne **Renouveler**. Les utilisateurs dont les certificats ont déjà expiré doivent en obtenir de nouveaux. Veuillez supprimer les certificats expirés. Les utilisateurs affectés en obtiendront des nouveaux automatiquement la prochaine fois qu'ils se connecteront à SafeGuard Enterprise.

SafeGuard Enterprise met à disposition un script de base de données **`UserCertficateRenewal.vbs`** pour automatiser ces tâches. Le script peut être utilisé dans le **Planificateur de tâches** SafeGuard Enterprise ou Windows afin de procéder à des vérifications régulières et de renouveler les certificats si nécessaire. Retrouvez plus de renseignements dans l'article 118878 de la base de connaissances Sophos.

3.1.5 Confirmation de tous les utilisateurs

Dans SafeGuard Enterprise, les nouveaux utilisateurs doivent être confirmés dans SafeGuard Management Center ou authentifiés dans Active Directory. La majorité des utilisateurs seront

des utilisateurs Active Directory qui seront confirmés automatiquement. Toutefois, certains utilisateurs, comme par exemple, les utilisateurs locaux, doivent être confirmés manuellement. Les utilisateurs non confirmés ne deviendront pas des **Utilisateurs SGN** et n'obtiendront donc pas les clés de chiffrement pour Synchronized Encryption. Ceci s'applique aux terminaux Windows et Mac OS X.

Nous vous conseillons de paramétrer la première stratégie pour qu'elle soit déployée en **lecture seule**. Dès que tous les terminaux/utilisateurs ont reçu leurs clés, veuillez activer les stratégies de chiffrement. De cette manière, vous êtes sûr que tous les utilisateurs sont confirmés avant qu'ils ne reçoivent leurs stratégies de chiffrement. Vous évitez également de rencontrer des problèmes d'utilisateurs non confirmés.

3.1.6 Stratégies pour les terminaux Mac OS X

Pour le chiffrement de fichiers, nous conseillons l'utilisation du type de stratégie **Par application (Synchronized Encryption)** avec la **Portée du chiffrement** définie sur **Emplacements définis** et commencez uniquement avec quelques emplacements sur lesquels les fichiers sont chiffrés automatiquement. De cette manière, vous réduisez l'impact sur les utilisateurs et sur leurs procédures de travail habituelles.

Pour faire la distinction entre les terminaux Windows et Mac OS X en matière de gestion des stratégies, veuillez utiliser un groupe Active Directory ou SafeGuard Enterprise séparé pour les utilisateurs et machines Mac OS X. Activez la stratégie Mac OS X uniquement pour les utilisateurs et machines Mac OS X.

3.1.6.1 Suggestions de stratégie de chiffrement synchronisé sur Mac OS X

Apps intégrées

Les applications qui chiffrent leurs données à ajouter à la **Liste des applications** :

- Email

  Remarque : pour Mac OS X, aucun module complémentaire Outlook n'est disponible. Toutefois, vous pouvez ajouter Outlook et Apple Mail à la liste des applications pour vous assurer qu'aucune donnée chiffrée ne soit malencontreusement envoyée à des utilisateurs ne pouvant pas y accéder. Veuillez noter que les apps de messagerie que vous incluez dans la liste enverront toutes les pièces jointes déchiffrées et enregistreront toutes les pièces jointes sous forme chiffrée et tous les fichiers clairs en texte clair.

  - /Applications/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - /Applications/Microsoft Office 2011/Microsoft Outlook.app/Contents/MacOS/Microsoft Outlook
  - Applications/Mail.app/Contents/MacOS/Mail

- Pour activer l'aperçu dans Mac OS X et la fonctionnalité d'aperçu dans le Finder et dans Apple Mail, les processus suivants doivent être ajoutés :
  - /Applications/Preview.app/Contents/MacOS/Preview
  - /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/XPCServices/QuickLookSatellite.xpc/Contents/MacOS/QuickLookSatellite
  - /System/Library/Frameworks/Quartz.framework/Versions/A/Frameworks/QuickLookUI.framework/Versions/A/Resources/QuickLookUIHelper.app/Contents/MacOS/

QuickLookUIHelper

- /System/Library/Frameworks/QuickLook.framework/Versions/A/Resources/quicklookd.app/Contents/MacOS/quicklookd

Chemins de Portée du chiffrement : emplacements définis

- Chiffrer :
  - <Documents>\Encrypted
- Si vous voulez que vos utilisateurs puissent cliquer deux fois sur les documents chiffrés dans leurs clients de messagerie pour les ouvrir, veuillez ajouter ces applications (par exemple Messagerie) à la liste des apps intégrées et leurs dossiers temporaires à la liste des emplacements définis.

  Les emplacements que vous devez définir pour les clients de messagerie sur Mac sont :
  - <%TMPDIR%>\com.apple.mail\com.apple.mail
  - <Profil Utilisateur>\Library\Containers\com.apple.mail\Data\Library\Mail Downloads\

  Ajoutez les emplacements suivants pour Outlook pour Mac OS X :
  - <Profil Utilisateur>\Library\Caches\TemporaryItems\Outlook Temp\
  - <%TMPDIR%>com.microsoft.Outlook\Outlook Temp\

3.2 Serveur backend

3.2.1 Utilisateur avec accès en lecture seule pour la synchronisation Active Directory

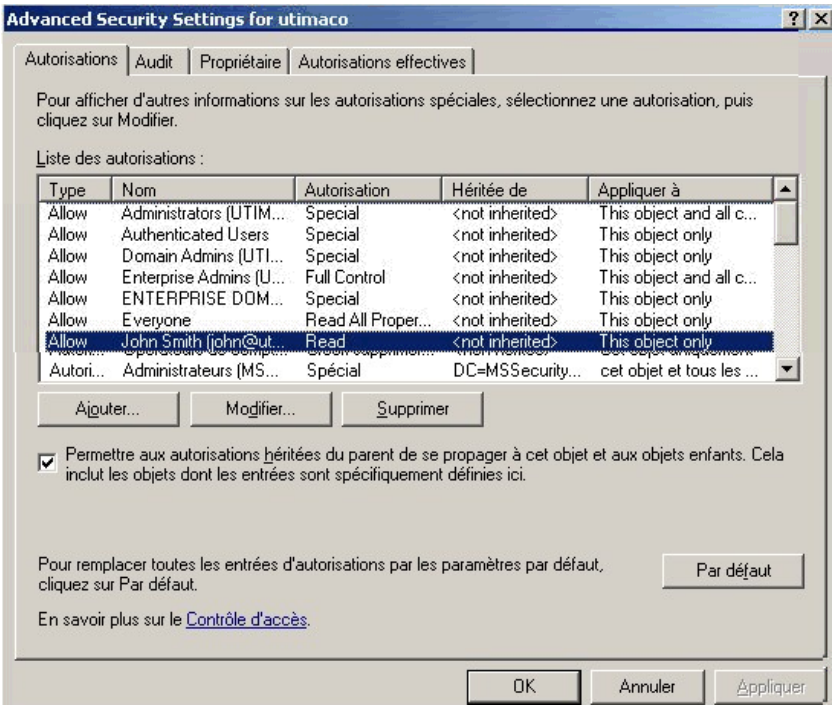
Remarque : renforcez la sécurité de la connexion en utilisant le chiffrement SSL pour la synchronisation Active Directory.

Le compte utilisé pour l'importation et la synchronisation Active Directory doit être un compte d'utilisateur en **lecture seule**. L'utilisateur doit avoir l'accès en lecture au domaine et à tous les objets enfant.

Pour attribuer les droits :

1. Ouvrez la fenêtre d'administration **Utilisateurs et ordinateurs Active Directory** et allez sur **Fonctionnalités avancées**.
2. Cliquez avec le bouton droit de la souris sur le domaine, puis cliquez sur **Propriétés**.
3. Ajoutez un utilisateur (ou un groupe) et sélectionnez la case **Autoriser** pour accorder l'autorisation **Lire**.
4. Cliquez sur **Paramètres avancés** et sélectionnez l'utilisateur (ou le groupe) et cliquez sur **Modifier**.
5. Dans le volet **Liste des autorisations pour <domaine>**, sélectionnez **Cet objet et tous les objets enfants** dans la liste déroulante **Appliquer à :**.

   Vous devriez obtenir le résultat suivant :



3.2.2 Affichage des utilisateurs avec « # » dans SafeGuard Management Center

Les utilisateurs enregistrés dans SafeGuard Enterprise lorsqu'aucun contrôleur de domaine n'était disponible sont identifiés par « # » dans SafeGuard Management Center.

3.3 Stratégies

3.3.1 Dossiers à exclure du chiffrement

Assurez-vous d'exclure les chemins suivants du chiffrement lorsque vous utilisez **Synchronized Encryption** :

Windows

- **`<Données des applications locales\Temp>`**

  Raison : certaines applications créent de nombreux fichiers temporaires de petite taille. S'ils ne sont pas exclus, tous ces fichiers temporaires seront chiffrés conformément à la stratégie. Veuillez exclure le dossier pour éviter tout problème de performances.

- **`<Données des applications locales>\Microsoft et sous-répertoires`**

  Raison : certaines applications appellent d'autres applications (par exemple, une vidéo imbriquée dans Microsoft PowerPoint). Si l'application d'appel est une application qui chiffre les fichiers, le fichier temporaire (par exemple, la vidéo) sera chiffré. Si l'application appelée (par exemple, le navigateur) est une application qui ne chiffre pas les fichiers (elle ne figure pas sur la liste d'applications), elle ne pourra pas exécuter le fichier chiffré.

- **<Program Files>**

  Raison : l'accès à ce dossier nécessite les droits administrateur. Le chiffrement initial de SafeGuard ne peut pas chiffrer ces fichiers en raison des droits d'accès. L'exclusion de ce dossier évite de saturer la base de données SafeGuard de messages d'événements d'échec de chiffrement de fichiers.

Tous les systèmes

- **<!Fournisseurs de stockage Cloud!>**

  En général, nous conseillons de chiffrer l'emplacement de stockage Cloud. Toutefois, vous pouvez exclure certains fournisseurs de stockage Cloud utilisés pour partager des données avec des tierces parties. De cette manière, vous évitez de chiffrer les fichiers dans les dossiers de synchronisation de stockage Cloud local connus. De plus, vous évitez tout problème d'échange de fichiers avec des tierces parties par le biais de la synchronisation Cloud. Il n'est pas nécessaire d'exclure ces dossiers si vous n'utilisez pas les dossiers Cloud pour échanger les fichiers avec des tierces parties.

- **<Musique>**, **<Images>**

  Raison : généralement, ces fichiers n'ont pas besoin d'être chiffrés. Si vous ne voulez pas exclure ces dossier du chiffrement, les applications utilisées pour ouvrir ces fichiers doivent faire partie de la **Liste d'applications**.

  Remarque : sur Mac OS X, vous ne pouvez pas utiliser l'application Photos et la bibliothèque d'images lorsque vous chiffrer les fichiers dans **<Images>**.

- **<Profil Utilisateur>\AppData\Roaming\AppleComputer**

  Raison : il s'agit du dossier de synchronisation local pour Apple iCloud sur les terminaux Windows. Il doit être exclus pour les mêmes raisons s'appliquant aux **<!fournisseurs de stockage cloud!>**.

3.3.2 Conseils pour le paramétrage de stratégie

Créez un dossier « Unencrypted »

Ce dossier peut être utilisé pour partager des fichiers en clair, par exemple avec les terminaux Linux de l'entreprise ou en cas de procédure de déploiement partiel. Retrouvez plus de renseignements à la section Création de stratégies pour le chiffrement de fichiers par application.

- **Windows**

  Pour exclure le dossier « Unencrypted » du chiffrement sur tous les terminaux, veuillez ajouter le dossier **Unencrypted** (chemin relatif) en tant qu'exemption dans une stratégie dont la **Portée du chiffrement** est définie sur **Partout**. En procédant ainsi, tous les fichiers dans les dossiers de ce nom, peu importe l'emplacement du dossier, ne seront pas chiffrés.

- **Mac OS X**

  Les chemins relatifs ne sont pas pris en charge sur Mac OS X. Nous vous conseillons de définir **<Documents>\Unencrypted** en tant qu'exemption dans une stratégie dont la **Portée du chiffrement** est définie sur **Partout**.

Complément Outlook

Nous vous conseillons de paramétrer l'option **Méthode de chiffrement pour les domaines autorisés** dans une stratégie de type **Paramètres généraux** sur **Inchangé**.

Suppression de clés des machines compromises

Les terminaux SafeGuard Enterprise **Synchronized Encryption** sont informés par Sophos Central Endpoint Protection de l'état compromis de la machine.

Nous conseillons de paramétrer l'option **Supprimer les clés des machines compromises** sur **Non**. Veuillez consulter les commentaires sur les terminaux affectés sous **Rapports** dans SafeGuard Management Center sous les détections d'état de fonctionnement rouge. Vérifiez puis procédez au nettoyage des terminaux si nécessaire. Enfin, nous conseillons de paramétrer l'option **Supprimer les clés des machines compromises** sur **Oui**.

3.3.3 Utilisateur invité

Sur les terminaux sur lesquels l'administration SafeGuard Enterprise BitLocker est uniquement installée, les entreprises continueront peut-être à avoir l'option **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** définie sur **Propriétaire**.

Pour les terminaux sans l'authentification au démarrage SafeGuard Enterprise et équipés de l'administration BitLocker ou des modules de chiffrement de fichiers, l'option **Autoriser l'enregistrement de nouveaux utilisateurs SGN pour** doit être définie sur **Tout le monde**. Si vous ne paramétrez pas cette option sur **Tout le monde**, d'autres utilisateurs ne bénéficieront que de l'état **Invité SGN**. Ils ne recevront pas de certificats et ne pourront pas chiffrer les fichiers suite à l'installation d'un module de chiffrement comme **Synchronized Encryption**.

3.3.4 Stratégies pour Mac OS X et l'ensemble de stratégies (RSOP)

Sur Mac OS X, seules les stratégies assignées aux utilisateurs sont évaluées. Si vous les assignez aux machines, les terminaux Mac OS X ne récupéreront pas les stratégies.

Toutefois, l'onglet RSOP dans SafeGuard Management Center affiche la stratégie actuellement assignée au Mac même si elle n'est pas activée.

3.3.5 Suivi de fichiers

Veuillez noter que la fonctionnalité de suivi de fichiers de SafeGuard Enterprise est soumise aux lois en vigueur dans chaque pays d'utilisation. Veuillez vérifier que vous êtes légalement autorisés à procéder au suivi.

3.3.6 Rappel de changement de mot de passe

Si vous utilisez le fournisseur de codes d'accès de SafeGuard Enterprise, la fenêtre Windows informant les utilisateurs que leur mot de passe va bientôt expirer ne s'affiche plus.

Pour rappeler aux utilisateurs qu'ils doivent changer leurs mots de passe, veuillez créer et assigner une stratégie SafeGuard Enterprise de type **Mot de passe** avec les paramètres requis. Retrouvez plus de renseignements à la section Règles de syntaxe des mots de passe.

3.4 Terminaux : toutes les plates-formes

3.4.1 Le terminal ne revient pas à un bon état de fonctionnement : échec de l'opération d'élimination des menaces

La protection des données de nouvelle génération garantit la communication entre Sophos SafeGuard et Sophos Endpoint Protection, si elle est disponible. Il s'agit d'une extension du message de Synchronized Security. Sophos SafeGuard et Sophos Endpoint partagent l'état de bon fonctionnement d'un système en s'envoyant une pulsation sur son état de fonctionnement via Security Hearbeat.

Si un système est gravement infecté par un malware, il sera verrouillé pour protéger tous les fichiers sensibles.

Dans l'éventualité d'une telle situation, les utilisateurs sont informés par Sophos Endpoint Protection que leur système ne fonctionne pas normalement via l'affichage en rouge de l'état de fonctionnement. De plus, Sophos SafeGuard les informe qu'ils ne seront plus en mesure d'accéder aux fichiers chiffrés. Cet état demeurera ainsi (impossibilité d'accéder aux fichiers chiffrés) tant que l'état de fonctionnement du système ne sera pas revenu à la normale (vert). Lorsque le système revient à son état normal de fonctionnement, Sophos SafeGuard se synchronise avec le serveur backend et permet aux utilisateurs d'accéder de nouveau aux fichiers chiffrés.

Si les utilisateurs reçoivent ces notifications et que leur système ne revient pas à un état normal dans les plus brefs délais, ils doivent immédiatement contacter leur service informatique.

Si un terminal n'est pas en mesure de revenir à un état de fonctionnement normal, ceci signifie que l'opération d'élimination des menaces de Sophos Anti-Virus a échoué (cette opération d'élimination s'effectue automatiquement dans Sophos Central). Si l'opération d'élimination échoue, l'intervention du service informatique est nécessaire afin d'éliminer le malware. Retrouvez plus de renseignements sur https://www.sophos.com/fr-fr/support/knowledgebase/112129.aspx.

3.5 Terminaux Windows

3.5.1 Chiffrement/Déchiffrement manuel des fichiers

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

Afficher l'état du chiffrement : indique si le fichier est chiffré ou non ainsi que la clé utilisée.

Chiffrer en fonction de la stratégie : chiffre votre fichier avec la clé Synchronized Encryption à condition que le type de fichier soit inclus dans la liste des applications et que l'emplacement du fichier n'ait pas été exclu du chiffrement.

Déchiffrer le fichier sélectionné (uniquement pour les fichiers chiffrés) : vous permet de déchiffrer votre fichier et de l'archiver en texte clair. Nous vous conseillons de déchiffrer votre fichier uniquement s'il ne contient aucune donnée sensible.

Chiffrer le fichier sélectionné (uniquement pour les fichiers déchiffrés) : vous permet de chiffrer manuellement votre fichier avec la clé Synchronized Encryption.

Créer un fichier protégé par mot de passe : vous permet de définir un mot de passe pour chiffrer manuellement votre fichier. Ceci est particulièrement utile si vous voulez partager votre fichier en toute sécurité avec une personne de votre entreprise n'ayant pas la clé Synchronized Encryption. Votre fichier est chiffré et enregistré en tant que fichier HTML. Vos destinataires peuvent ouvrir le fichier avec leur navigateur Web dès que vous leur avez communiqué le mot de passe.

Remarque : cette option est uniquement disponible pour les fichiers qui sont soit en texte clair, soit chiffré avec une clé disponible dans votre jeu de clés. Si les fichiers sont chiffrés, ils vont être déchiffrés automatiquement avant d'être protégés par mot de passe.

Remarque : la protection par mot de passe utilise l'encodage « base64 ». Les fichiers sont par conséquent de plus grande taille que le fichier original. La taille de fichier maximale prise en charge est de 50 Mo.

Remarque : il est uniquement possible de protéger les fichiers individuels par mot de passe et non les dossiers ou les répertoires. Toutefois, vous pouvez sélectionner plus d'un fichier pour afficher leur état de chiffrement et pour les chiffrer/déchiffrer.

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

Afficher l'état du chiffrement : affiche une liste de fichiers inclus avec des icônes indiquant l'état du chiffrement et la clé utilisée.

Chiffrer en fonction de la stratégie : le système détecte automatiquement tous les fichiers déchiffrés et les chiffre avec la clé Synchronized Encryption par défaut à condition que le type de fichier soit inclus dans la liste des applications et que l'emplacement du fichier n'ait pas été exclu du chiffrement. Selon votre stratégie, les fichiers chiffrés avec d'autres clés peuvent être chiffrés de nouveau avec la clé Synchronized Encryption.

3.5.2 Emails envoyés par la règle de transfert automatique

Lorsque vous créez une règle de transfert automatique ou de redirection sur le **client**, l'envoi automatique de ces emails n'est pas journalisé.

3.6 Terminaux Mac OS X

3.6.1 Position des icônes sur le bureau

Lorsque vous utilisez SafeGuard Enterprise pour Mac, les positions des icônes sur votre bureau peuvent ne pas avoir été enregistrées correctement. Lorsque vous modifiez la position d'un icône, celui-ci revient à sa position originale après chaque redémarrage ou connexion.

Pour enregistrer les positions de vos icônes, procédez de la manière suivante :

1. Démarrez l'application Terminal sur votre Mac.
2. Saisissez la commande suivante :

   ```
   defaults write com.sophos.encryption MountDesktopAsNetworkVolume 1
   ```

3. Déconnectez-vous et rouvrez une session sur votre Mac.

Le système est maintenant en mesure d'enregistrer les positions de vos icônes de bureau.

Important : lorsque vous exécutez cette commande, la fonctionnalité de la Corbeille change. La suppression de fichiers les supprime de façon permanente plutôt que de les déplacer dans

la Corbeille. Pour supprimer ce paramètre, saisissez la commande suivante dans l'application Terminal :

`defaults remove com.sophos.encryption MountDesktopAsNetworkVolume`.

4 Support technique

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

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

5 Mentions légales