

SOPHOS

Cybersecurity
made
simple.

SafeGuard Enterprise

Guide de démarrage et de conseils pratiques

Version du produit : 8.3

Table des matières

À propos de ce guide.....	1
Bon usage : support multi-clés pour Synchronized Encryption.....	2
Création d'une stratégie de chiffrement de fichiers à plusieurs clés.....	2
Chiffrement par application avec plusieurs clés sur les terminaux.....	3
Complément Outlook pour le chiffrement par emplacement.....	6
Fichiers protégés par mot de passe.....	7
Utiliser un mot de passe pour protéger un fichier.....	7
Protection d'un nouveau fichier par mot de passe.....	8
Synchronized Encryption.....	10
Utilisation d'applications standard.....	10
Partage d'informations dans l'entreprise.....	10
Partage d'informations avec des parties externes.....	11
Définition des apps intégrées.....	13
Problèmes à prendre en compte avant le déploiement.....	14
Création de stratégies en lecture seule.....	16
Information des utilisateurs.....	17
Support.....	20
Mentions légales.....	21

1 À propos de ce guide

Ce guide vous aide à commencer à utiliser les nouvelles fonctions de SafeGuard Enterprise :

- Support multi-clés pour Synchronized Encryption
- Meilleure protection des fichiers par mot de passe
- Complément Outlook pour le chiffrement par emplacement

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 le [Manuel d'administration de SafeGuard Enterprise](#).

Ce guide n'est pas un guide d'installation mais est destinée aux utilisateurs qui sont déjà familiers avec le produit. Retrouvez plus de renseignements sur l'installation et l'administration dans le [Manuel d'administration de SafeGuard Enterprise](#).

2 Bon usage : support multi-clés pour Synchronized Encryption

SafeGuard Enterprise vous permet de configurer des clés de chiffrement supplémentaires pour des emplacements spécifiques lors de l'utilisation de Synchronized Encryption.

Retrouvez ci-dessous des instructions en contexte :

- Votre entreprise a sélectionné **Par application (Synchronized Encryption)** pour chiffrer tous les fichiers créés par des applications usuelles avec la **clé Synchronized Encryption**.
- Les fichiers sont chiffrés dans le dossier `Documents` des utilisateurs avec leur **Clé personnelle**.
 - Le dossier `Documents` des utilisateurs doit contenir le dossier `/unencrypted` dans lequel les utilisateurs peuvent conserver leurs fichiers non chiffrés.
- Pour garantir que tous les fichiers sur les terminaux sont chiffrés conformément à la stratégie de sécurité de votre entreprise, veuillez activer le chiffrement initial.

2.1 Création d'une stratégie de chiffrement de fichiers à plusieurs clés

1. Dans SafeGuard Management Center, sélectionnez la stratégie **Chiffrement de fichiers (par défaut)** et sélectionnez **Par application (Synchronized Encryption)** sous **Type de chiffrement**.
2. Sous **Liste d'application**, sélectionnez **Modèle**.

La liste d'application par défaut est appelée **Modèle**. Elle contient les applications les plus communément utilisées.

3. Sous **Portée du chiffrement**, sélectionnez **Partout**. Il s'agit de l'option la plus sûre généralement utilisée sur les terminaux Windows.

Une règle de chiffrement des fichiers sur tous les emplacements va être créée à l'aide de la **Clé Synchronized Encryption**. Cette règle est ajoutée à la liste des emplacements sur lesquels le chiffrement par application est appliqué.

Vous pouvez à présent ajouter des règles spécifiques pour les emplacements que vous voulez chiffrer avec d'autres clés de chiffrement. Ces emplacements peuvent être locaux ou sur le réseau. Vous pouvez utiliser des valeurs prédéfinies pour les indiquer.

Dans notre exemple, nous voulons chiffrer le dossier `Documents` des utilisateurs.

4. Pour ajouter une règle, cliquez sur le champ de modification du **Chemin** et sélectionnez **<Documents>** dans le menu déroulant.

Remarque

Vous ne pouvez pas modifier la portée du chiffrement.

La **Clé Synchronized Encryption** est utilisée par défaut mais vous pouvez choisir une autre clé de chiffrement. Par exemple, la clé de domaine ou la clé d'une unité organisationnelle. Vous pouvez également sélectionner la **Clé personnelle** qui est unique à chaque utilisateur.

5. Cliquez sur le symbole de la **Clé personnelle** dans le champ **Clé** pour sélectionner les clés personnelles des utilisateurs et chiffrer le dossier `Documents`. Vous pouvez placer le curseur de la souris sur les symboles de clé pour afficher leur fonction.

Pour utiliser un dossier non chiffré, vous devez définir une règle d'exception pour ce dossier spécifique.
6. Cliquez sur le champ **Chemin** et sélectionnez **<Documents>** dans le menu déroulant. Saisissez `\unencrypted` après l'espace réservé **<Documents>**.
7. Dans la colonne **Mode**, sélectionnez **Exclure** dans le menu déroulant.
8. Pour activer le chiffrement initial sur les terminaux, paramétrez l'option **Sur les disques locaux** sous **Chiffrement initial : chiffrer automatiquement les fichiers existants** sur **Oui**.
9. Enregistrez la stratégie et déployez-la.

Remarque

Lorsque vous assignez une stratégie, avec des règles spécifiques pour les emplacements et des clés différentes, aux terminaux sur lesquels SafeGuard Enterprise 8.0 est installé, ces règles s'appliquent correctement. Tous les emplacements indiqués sont chiffrés avec les clés sélectionnées. Toutefois, si une règle dont la **Portée du chiffrement** est définie sur **Partout** fait partie de la stratégie, seule la **Clé Synchronized Encryption** est utilisée. Les fichiers dans les emplacements spécifiques sont également chiffrés avec la **Clé Synchronized Encryption**.

2.2 Chiffrement par application avec plusieurs clés sur les terminaux

Le logiciel SafeGuard Enterprise Encryption est installé sur le terminal mais aucune stratégie n'est appliquée.

Lorsque vous cliquez sur **Synchroniser** dans la zone de notification de SafeGuard Enterprise, le terminal reçoit les stratégies mises à jour. Les modifications de la stratégie inclut la liste des applications indiquant tous les nouveaux fichiers devant être chiffrés. Cette liste inclut Microsoft Office, ce qui signifie que tous les fichiers Microsoft Office sont chiffrés.

Lorsque vous activez le chiffrement initial de tous les lecteurs locaux, tous les fichiers déjà présents sur l'ordinateur sont également chiffrés.

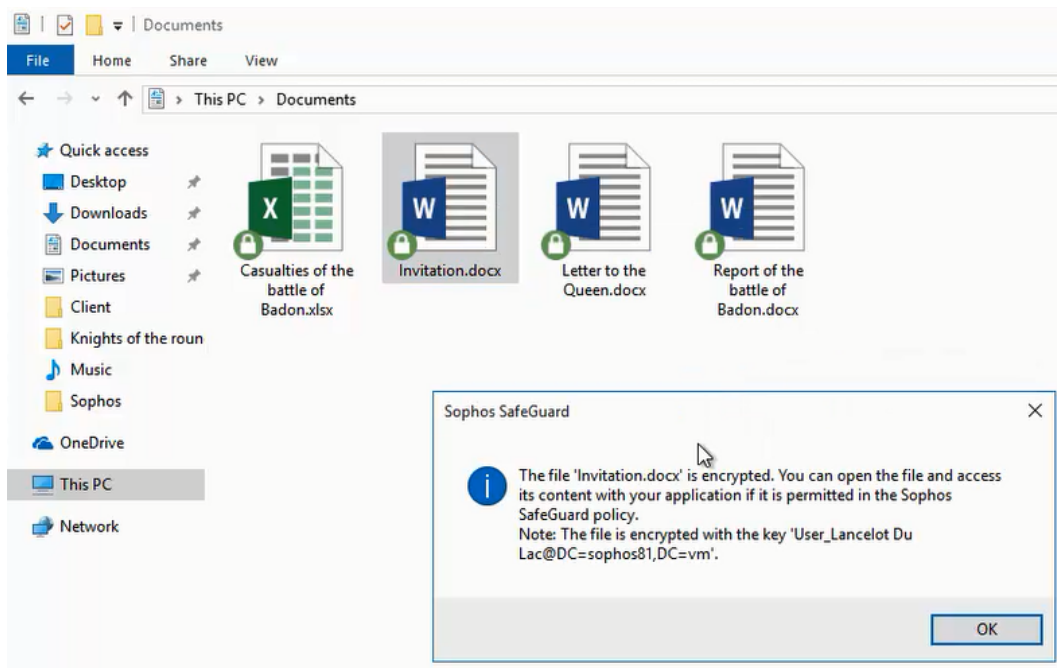
Remarque

Vous devez indiquer les extensions de fichiers devant être traités par le chiffrement initial lorsque vous créez une liste d'applications. La liste d'applications **Modèle** inclut les extensions les plus usuelles pour chaque application.

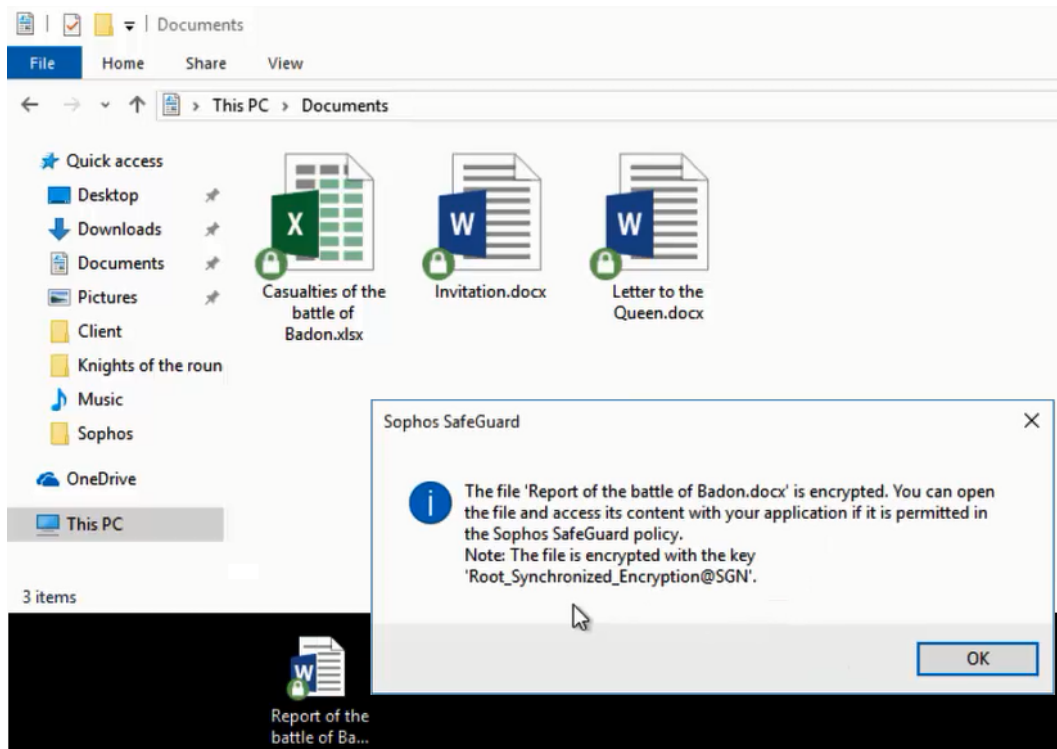
- Les fichiers sont chiffrés dans le dossier `Documents` avec la **Clé personnelle** des utilisateurs.
- Tous les autres fichiers devant être chiffrés selon la liste d'applications sont chiffrés avec la **clé Synchronized Encryption**.

Comparaison entre de la portée du chiffrement Partout et Emplacements définis

Vous avez choisi d'utiliser la **Clé Synchronized Encryption** partout sauf sur le dossier **<Documents>** sur lequel la **Clé personnelle** des utilisateurs doit être appliquée.



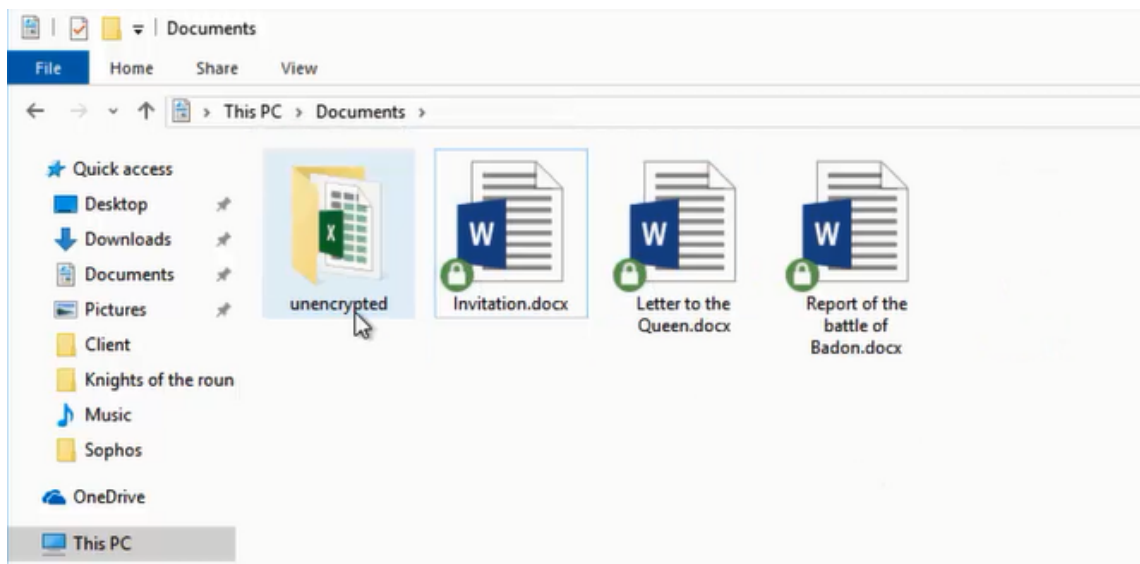
Le déplacement ou la copie d'un fichier modifie la clé de chiffrement. Le nouvel emplacement fait partie de la règle **Partout** et la **Clé Synchronized Encryption** est utilisée.



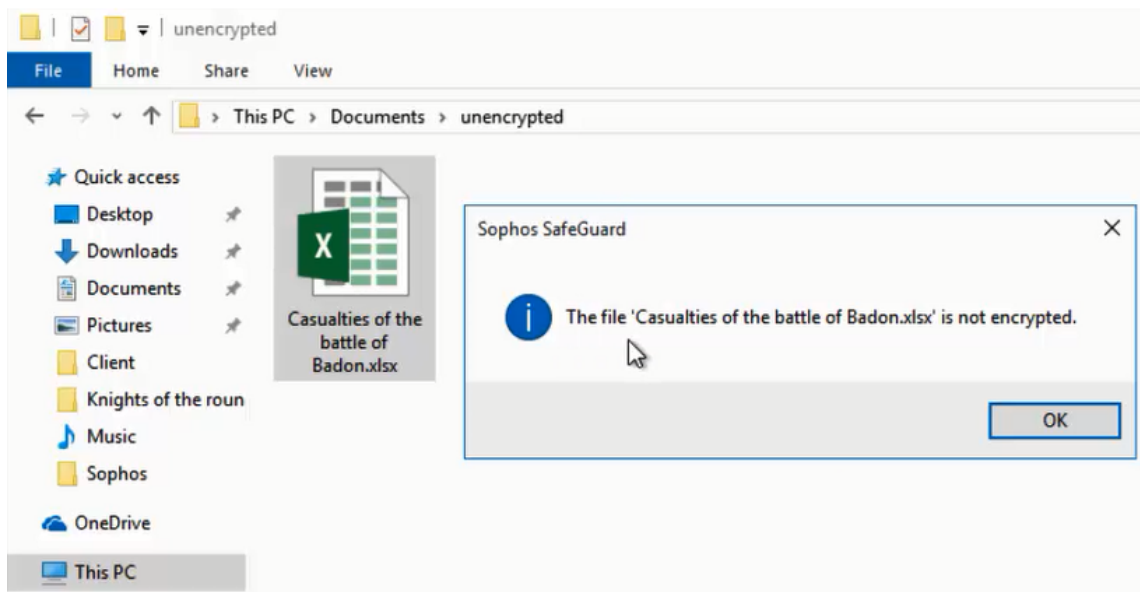
Le déplacement d'un fichier en clair ou déjà chiffré dans le dossier **<Documents>** chiffre le fichier avec la **Clé personnelle** de l'utilisateur.

Dossier sans chiffrement

Dans la stratégie, vous définissez le dossier **<Documents>\unencrypted** comme emplacement dans lequel les fichiers ne doivent pas être chiffrés.



Lorsque vous déplacez un fichier dans le dossier « unencrypted » (non chiffré), celui-ci est déchiffré.



SafeGuard Enterprise déchiffre automatiquement les fichiers si vous mettez un ou plusieurs fichiers dans un emplacement sans chiffrement. Si vous déplacez un dossier vers un dossier exclus du chiffrement ou si vous renommez un dossier du même nom qu'un dossier exclus du chiffrement, les fichiers ne sont pas déchiffrés automatiquement pour éviter tout déchiffrement accidentel. Vous pouvez ensuite déchiffrer les fichiers manuellement ou utiliser l'option Chiffrer en fonction de la stratégie à partir du menu contextuel de SafeGuard Enterprise.

3 Complément Outlook pour le chiffrement par emplacement

À partir de la version 8.1, le complément Outlook pour Windows de SafeGuard Enterprise est disponible pour le chiffrement par emplacement. Il est disponible sur les terminaux lorsque vous installez un module de Chiffrement de fichiers par emplacement.

En général, la fonctionnalité d'envoi d'emails externes est la même que pour le chiffrement par application. Toutefois, l'envoi d'email avec pièces jointes à des domaines autorisés doit être effectués avec une grande prudence en raison de la nature du chiffrement par emplacement et des fonctions à plusieurs clés de Synchronized Encryption.

Dans la stratégie **Paramètres généraux par défaut**, vous pouvez configurer ce qui va se passer lorsque des pièces jointes d'emails sont envoyés à des domaines (généralement internes) autorisés. Les options disponibles pour le **Comportement des domaines autorisés** sont :

- **Chiffré**
- **Aucun chiffrement**
- **Toujours demander**
- **Inchangé (Synchronized Encryption)**

Aucun chiffrement et **Toujours demander** se comportent de la même façon pour tous les modules de Chiffrement de fichiers.

Les options **Chiffré** et **Inchangé (Synchronized Encryption)** se comportent différemment lorsqu'elles sont utilisés avec Synchronized Encryption ou avec le chiffrement par emplacement.

Chiffré

- Synchronized Encryption
Les fichiers chiffrés restent chiffrés et la clé de chiffrement est inchangée. Les fichiers non chiffrés sont chiffrés par la **Clé Synchronized Encryption** uniquement si l'extension de fichier est définie dans la liste des apps intégrées.
- Chiffrement basé sur l'emplacement
Tous les fichiers joints sont chiffrés avec la **Clé Synchronized Encryption** quelles que soient leurs extensions de fichier et quel que soit leur état de chiffrement.

Inchangé (Synchronized Encryption)

- Synchronized Encryption
les fichiers chiffrés seront envoyés chiffrés tandis que les fichiers en clair seront envoyés en clair.
- Chiffrement basé sur l'emplacement
Tous les fichiers sont chiffrés avec la **Clé Synchronized Encryption**.

4 Fichiers protégés par mot de passe

Synchronized Encryption introduit le concept de fichiers protégés par mot de passe grâce auquel les utilisateurs peuvent créer des fichiers HTML chiffrés pouvant uniquement être déchiffrés avec un mot de passe.

À partir de SafeGuard Enterprise 8.1, cette fonction est également disponible dans le module de chiffrement par emplacement sur Windows.

Remarque

Sur macOS, cette fonction est disponible depuis la version 8.

4.1 Utiliser un mot de passe pour protéger un fichier

Lors de l'envoi d'emails à des destinataires n'appartenant pas au réseau de votre entreprise, nous vous conseillons de chiffrer votre fichier avec un mot de passe. Les destinataires ont accès aux fichiers chiffrés sans avoir besoin d'installer SafeGuard Enterprise.

Procédez comme suit :

1. Cliquez avec le bouton droit de la souris sur le fichier que vous voulez envoyer et sélectionnez **Créer un fichier protégé par mot de passe**.
2. Cliquez avec le bouton droit de la souris sur le fichier que vous voulez envoyer et sélectionnez **Créer un fichier protégé par mot de passe**.
Si vous recevez un message d'erreur, sélectionnez **Affichage > Masquer l'aperçu** dans le Finder et réessayez.
3. Suivez les instructions à l'écran pour créer un mot de passe. Nous vous conseillons d'utiliser un mot de passe fort et ne pas l'envoyer dans le même email que les fichiers.
Votre fichier est chiffré et enregistré en tant que fichier HTML. Vous pouvez à présent joindre en toute sécurité le fichier HTML à vos emails.

Remarque

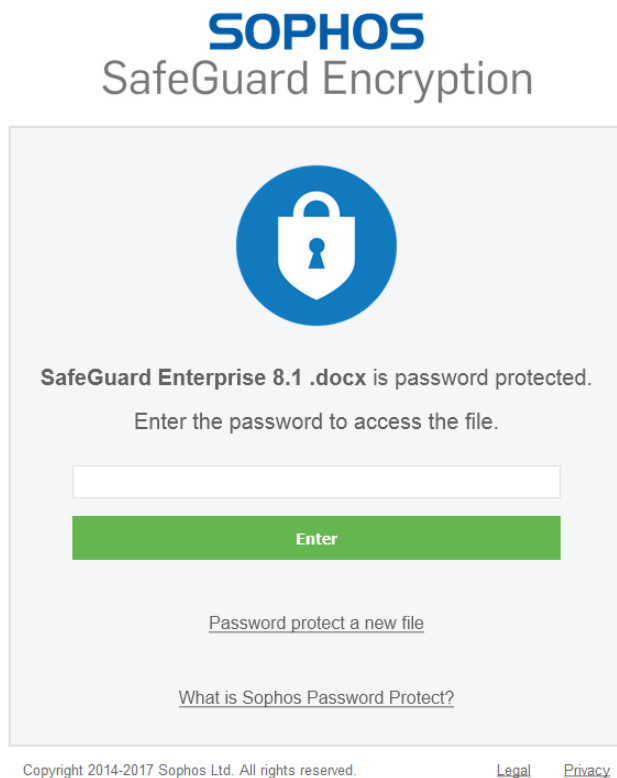
- Le chiffrement nécessite de l'espace disque.
 - Le fichier HTML chiffré est de plus grande taille que le fichier original.
 - La taille de fichier maximale prise en charge est de 50 Mo.
 - Pour envoyer plusieurs fichiers en même temps, vous pouvez les compresser dans un fichier .zip et chiffrer ce fichier .zip.
4. Communiquez le mot de passe aux destinataires par téléphone ou par tout autre moyen de communication.
Les destinataires peuvent utiliser l'un des navigateurs suivants pour ouvrir la pièce jointe protégée par mot de passe :
 - Mozilla Firefox
 - Google Chrome
 - Microsoft Internet Explorer 11

- Microsoft Edge
5. Demandez aux destinataires de cliquer deux fois sur le fichier et de suivre les instructions affichées à l'écran pour procéder de l'une des manières suivantes :
- Saisissez le mot de passe et cliquez sur **Entrée** pour accéder au fichier.
 - Cliquez sur **Protéger un nouveau fichier par mot de passe** pour protéger un autre fichier par mot de passe.

Les destinataires ont accès au fichier que vous avez protégé par mot de passe. Ils peuvent protéger le fichier par mot de passe lorsqu'ils vous le renvoie. Ils ont la possibilité d'utiliser le même mot de passe ou d'en utiliser un nouveau. Ils peuvent même protéger un nouveau fichier par mot de passe.

4.2 Protection d'un nouveau fichier par mot de passe

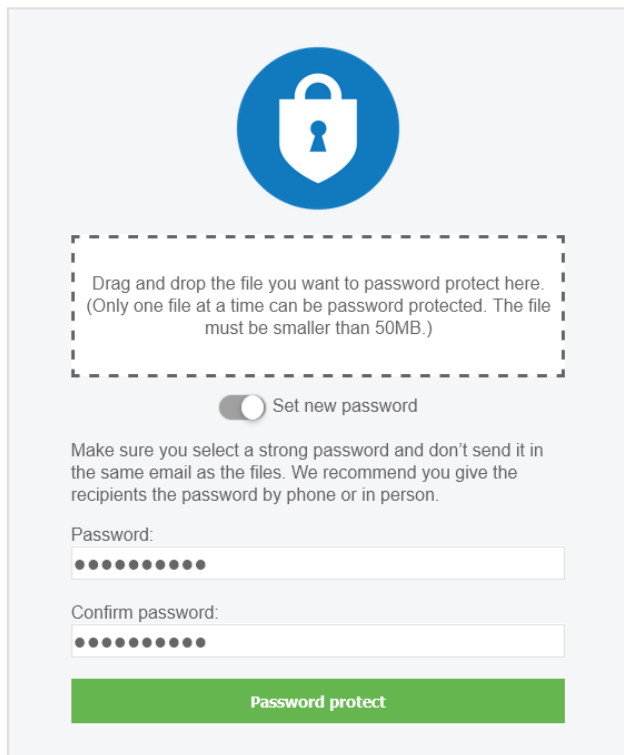
SafeGuard Enterprise 8.1 permet aux destinataires d'un fichier protégé par mot de passe de chiffrer un nouveau fichier avec un mot de passe. Ils n'ont pas besoin de déchiffrer le fichier original. Ceci leur permet de gagner du temps car ils n'ont pas besoin de saisir le mot de passe original.



Il suffit aux utilisateurs de cliquer deux fois sur un fichier HTML chiffré et de cliquer ensuite sur **Protéger un nouveau fichier par mot de passe**.

SOPHOS

SafeGuard Encryption



The image shows the Sophos SafeGuard Encryption web interface. At the top, there is a blue circular icon with a white padlock. Below it is a dashed rectangular box containing the text: "Drag and drop the file you want to password protect here. (Only one file at a time can be password protected. The file must be smaller than 50MB.)". Underneath this box is a toggle switch labeled "Set new password". Below the toggle is a paragraph of instructions: "Make sure you select a strong password and don't send it in the same email as the files. We recommend you give the recipients the password by phone or in person." There are two password input fields, one labeled "Password:" and one labeled "Confirm password:", both with masked characters. At the bottom of the form is a green button labeled "Password protect".

Copyright 2014-2017 Sophos Ltd. All rights reserved.

[Legal](#) [Privacy](#)

Les utilisateurs doivent faire glisser et déposer un fichier dans la zone indiquée, saisir un mot de passe complexe et cliquer sur **Protéger par mot de passe**.

5 Synchronized Encryption

Synchronized Encryption est le module de chiffrement de fichiers par application de Sophos SafeGuard Enterprise. Les différences par rapport au chiffrement de fichiers par emplacement sont :

- Chiffrement automatique des fichiers créés ou modifiés par les applications définies (apps intégrées).
- Seules les applications définies peuvent lire les fichiers.
- Le chiffrement ne dépend pas de l'emplacement du fichier.
- Les clés de chiffrement peuvent être automatiquement supprimées des appareils des utilisateurs en cas de menace à la sécurité suspectée.

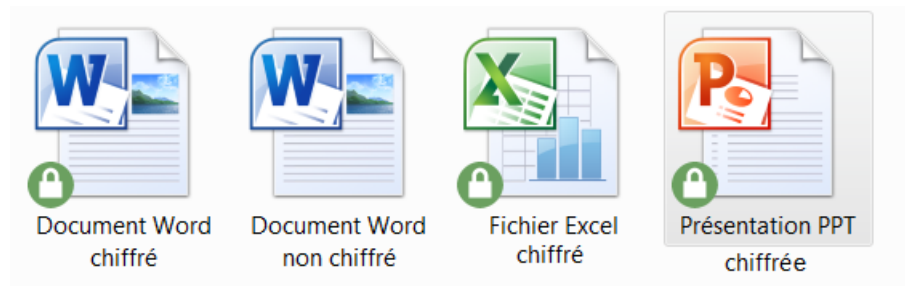
Remarque

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.

5.1 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.



5.2 Partage d'informations dans l'entreprise

L'utilisation de la **Clé Synchronized Encryption** de SafeGuard Enterprise facilite le partage d'informations en interne. Chaque utilisateur de SafeGuard Enterprise de votre entreprise pourra lire ces informations.

Cette version de SafeGuard Enterprise (SGN 8.1) permet de configurer des clés de chiffrement supplémentaires pour des emplacements spécifiques. Pour lire les fichiers chiffrés avec une autre

clé que la clé Synchronized Encryption, les utilisateurs doivent avoir cette clé dans leur jeu de clés comme indiqué à la section [Bon usage : support multi-clés pour Synchronized Encryption](#) (page 2).

Remarque

Les utilisateurs peuvent afficher leur jeu de clés en cliquant avec le bouton droit de la souris sur l'icône de la barre d'état système de SafeGuard Enterprise dans la barre des tâches puis sur **Afficher > Jeu de clés**.

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.

5.3 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.

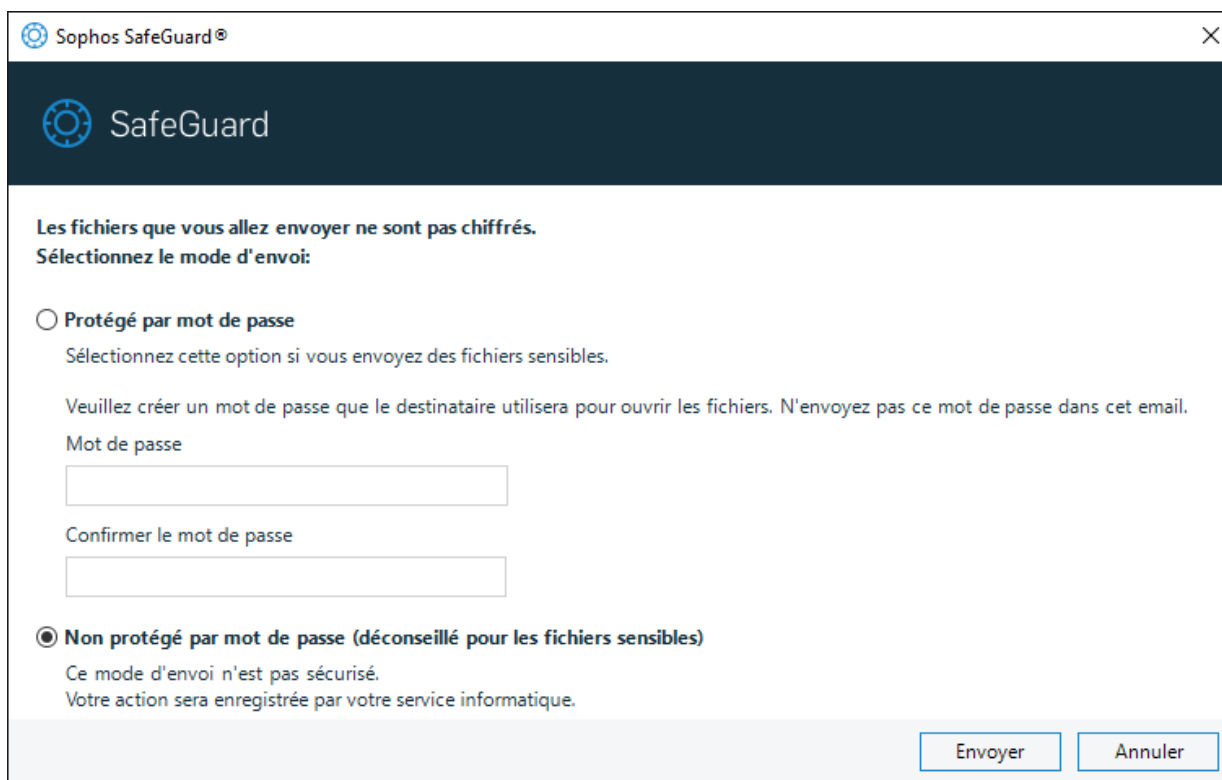
Différentes procédures de travail s'appliquent aux utilisateurs d'Outlook et aux autres utilisateurs.

Conseil

Assurez-vous que le [Manuel d'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.



The screenshot shows a window titled "Sophos SafeGuard®" with a close button in the top right corner. Below the title bar is a dark blue header with the SafeGuard logo and text. The main content area has a white background and contains the following text and controls:

Les fichiers que vous allez envoyer ne sont pas chiffrés.
Sélectionnez le mode d'envoi:

Protégé par mot de passe
Sélectionnez cette option si vous envoyez des fichiers sensibles.

Veuillez créer un mot de passe que le destinataire utilisera pour ouvrir les fichiers. N'envoyez pas ce mot de passe dans cet email.

Mot de passe

Confirmer le mot de passe

Non protégé par mot de passe (déconseillé pour les fichiers sensibles)
Ce mode d'envoi n'est pas sécurisé.
Votre action sera enregistrée par votre service informatique.

At the bottom right, there are two buttons: "Envoyer" and "Annuler".

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.

The screenshot shows a dialog box titled "Sophos SafeGuard® - Protection par mot de passe du fichier". The main heading is "Protection par mot de passe de 'New Microsoft Word Document.docx'". Below this, there is instructional text: "Veillez créer un mot de passe. Les destinataires utiliseront ce mot de passe pour récupérer le fichier. Veuillez sélectionner un mot de passe fort et ne pas l'envoyer dans le même email que les fichiers. Nous vous conseillons de communiquer ce mot de passe à vos destinataires par téléphone ou en personne." There are two input fields: "Mot de passe :" and "Confirmer le mot de passe :". At the bottom, there are two buttons: "Protéger par mot de passe" (highlighted with a blue border) and "Annuler".

Retrouvez plus de renseignements dans le Manuel d'utilisation de SafeGuard Enterprise à la section [Envoi sécurisé des pièces jointes par email](#).

5.4 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.

Conseil

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.

5.4.1 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.

Conseil

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.

5.4.2 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.

5.5 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](#) (page 16).

Veuillez envisager les problèmes suivants avant de déployer Synchronized Encryption.

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

Plusieurs applications peuvent créer des fichiers sous différents formats. 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 sont 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 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.

Conseil

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 de pouvoir lire le contenu chiffré.

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. Toutefois, ceci signifie que lorsque vous téléchargerez des fichiers sur Internet avec Edge, ils seront déchiffrés et téléchargés en clair.

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.

5.5.2 Applications Java

Les applications Java partagent souvent le même fichier exécutable `java.exe`. Il n'est donc 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.

5.5.3 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. Veuillez à communiquer ceci clairement aux utilisateurs.

Conseil

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.

5.5.4 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.

5.5.5 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.

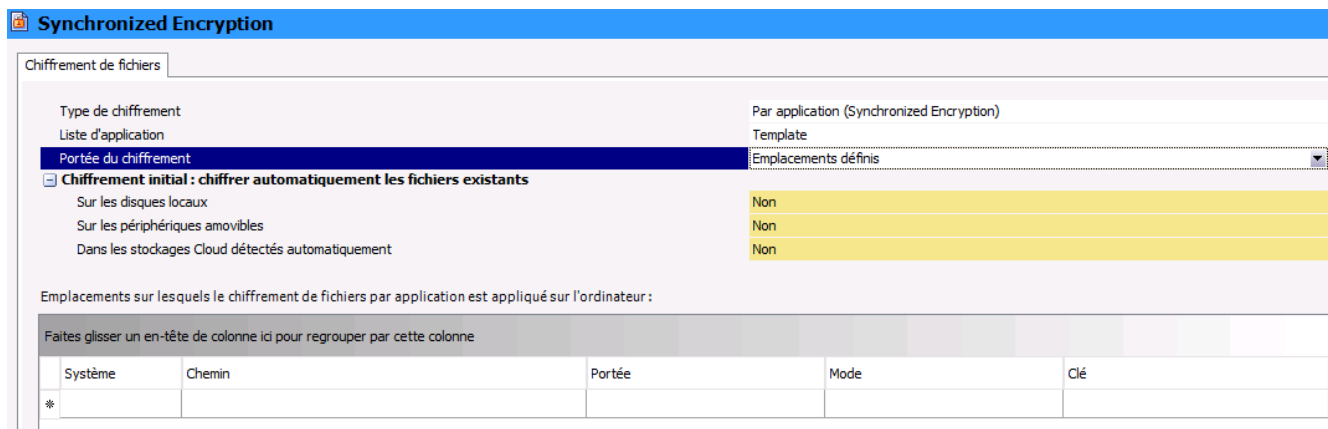
5.6 Création de stratégies en lecture seule

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** sans définir les emplacements.



Retrouvez plus de renseignements dans le Manuel d'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>/Encrypted. Les utilisateurs qui veulent lire un document chiffré devront alors déplacer ou copier le fichier dans cet emplacement.

Retrouvez plus de renseignements dans le Manuel d'administration de SafeGuard Enterprise à la section [Création d'une stratégie de lecture seule pour les terminaux Mac](#).

5.7 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 déployé 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.

5.7.1 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 créez 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,

6 Support

Sortie officielle

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

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

7 Mentions légales

Copyright © 2019 Sophos Limited. Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre sauf si vous possédez une licence valide, auquel cas vous pouvez reproduire la documentation conformément aux termes de cette licence ou si vous avez le consentement préalable écrit du propriétaire du copyright.

Sophos, Sophos Anti-Virus et SafeGuard sont des marques déposées de Sophos Limited, Sophos Group et de Utimaco Safeware AG, partout où ceci est applicable. Tous les autres noms de produits et d'entreprises mentionnés dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

Les informations de copyright des fournisseurs tiers sont disponibles dans le document [Disclaimer and Copyright for 3rd Party Software](#) dans le répertoire de votre produit.