conpal LAN Crypt

Persistant
Sécurisé
Adaptable

Manuel Client

Version du produit: 3.97
Date du document: Mai 2019

Contents

1 Qu'est-ce que SafeGuard LAN Crypt ?

SafeGuard LAN Crypt permet d'échanger des fichiers confidentiels grâce au chiffrement transparent de fichiers mis à disposition de groupes d'utilisateurs de confiance dans les grandes entreprises. SafeGuard LAN Crypt fonctionne sans aucune intervention de l'utilisateur. Il prend en charge le rôle de responsable de la sécurité et peut donc limiter les droits d'accès aux fichiers chiffrés par SafeGuard LAN Crypt. Un responsable de la sécurité principal (MSO pour master security officer) peut déléguer le droit d'administrer SafeGuard LAN Crypt. Vous pouvez établir une hiérarchie parmi les responsables de sécurité pour répondre aux exigences de sécurité de toutes les entreprises.

Les fichiers chiffrés ne sont pas assignés à des utilisateurs individuels. Tout utilisateur qui possède la bonne clé peut travailler sur un fichier chiffré. Les administrateurs peuvent ainsi créer des groupes d'utilisateurs logiques bénéficiant d'un accès partagé aux fichiers chiffrés. Ce mode de fonctionnement est comparable à l'utilisation d'un trousseau de clés dans la vie de tous les jours. SafeGuard LAN Crypt offre aux utilisateurs et groupes d'utilisateurs un jeu de clés et chaque clé sert à ouvrir une porte ou un coffre-fort.

Chaque fois qu'un utilisateur déplace un fichier dans un répertoire, qui a été défini comme répertoire chiffré, ce fichier est chiffré sur son ordinateur. Chaque fois qu'un autre utilisateur de confiance du même groupe lit le fichier à partir de ce répertoire, il lui est transféré sous forme chiffrée. Le déchiffrement du fichier intervient uniquement sur l'ordinateur du destinataire. L'utilisateur peut alors le modifier. Le fichier est ensuite de nouveau chiffré avant son retour dans le répertoire chiffré.

Les utilisateurs non autorisés peuvent éventuellement accéder à ces fichiers chiffrés (uniquement à partir de postes de travail non équipés de SafeGuard LAN Crypt), mais s'ils ne disposent pas de l'autorisation SafeGuard LAN Crypt, ils pourront uniquement voir le contenu chiffré. Par conséquent, un fichier est toujours protégé même si aucune protection d'accès n'est définie pour le système lui-même, en cas d'attaque du réseau ou du non-respect de la stratégie de sécurité de l'entreprise par ses employés.

1.1 Protection des données avec SafeGuard LAN Crypt

SafeGuard LAN Crypt garantit que les fichiers sensibles peuvent être stockés en toute sécurité sur des serveurs de fichiers et des postes de travail. Les données sont transférées de manière sécurisée sur des réseaux LAN ou WAN pendant que les opérations de chiffrement ou de déchiffrement sont exécutées dans la mémoire RAM du poste de travail client. Toutes les tâches de chiffrement ou de déchiffrement sont exécutées de manière transparente sur le poste de travail client avec le minimum d'interaction de l'utilisateur. Il n'est pas nécessaire d'installer un logiciel de sécurité spécial sur le serveur de fichiers lui-même.

Un responsable de la sécurité peut définir différents droits d'accès pour les répertoires et fichiers. Ces droits sont regroupés dans des profils de chiffrement destinés aux utilisateurs. Les profils de chiffrement sont distribués par les fichiers de stratégie. Les fichiers de stratégie contiennent l'ensemble des règles, droits d'accès et clés nécessaires à un chiffrement transparent. Ce fichier est sécurisé par l'intermédiaire d'un certificat. Avant que l'utilisateur ne puisse commencer à travailler avec les données chiffrées à l'aide du logiciel SafeGuard LAN Crypt installé sur le poste de travail client, il doit pouvoir accéder au fichier de stratégie. L'utilisateur peut accéder au fichier de stratégie contenant le profil de chiffrement s'il dispose de la clé privée affectée au certificat.

SafeGuard LAN Crypt permet aux utilisateurs de confiance d'être organisés en différents groupes de confiance. Tous les utilisateurs SafeGuard LAN Crypt dont le fichier de stratégie contient le même profil de chiffrement sont membres d'un groupe de confiance. Ils n'ont pas à se préoccuper du chiffrement ni de l'échange de la clé. Ils doivent simplement pouvoir accéder aux fichiers de stratégie pour que leurs données soient chiffrées ou déchiffrées en toute transparence, à l'ouverture ou à la fermeture. Toutes les formes organisationnelles peuvent être mappées à l'aide de groupes de confiance depuis un modèle LAN centralisé dans lequel les utilisateurs sont administrés de manière centrale, vers un modèle distant dans lequel les utilisateurs travaillent sur des ordinateurs portables.

1.2 SafeGuard LAN Crypt et SafeGuard Enterprise

Cette version de SafeGuard LAN Crypt peut être utilisée en parallèle à SafeGuard Enterprise. Par exemple, SafeGuard Data Exchange peut être utilisé pour chiffrer toutes les données sur les supports amovibles tandis que SafeGuard LAN

Crypt peut être utilisé pour chiffrer tous les fichiers sur les partages réseau. Retrouvez plus de renseignements sur les versions prises en charge dans les Notes de publication de SafeGuard LAN Crypt.

La boîte de dialogue **État du client** SafeGuard LAN Crypt affiche toutes les règles de chiffrement valides sur l'ordinateur. Retrouvez plus de renseignements à la section Boîte de dialogue État du client *(page 21)*. En général, les règles SafeGuard Enterprise Data Exchange sont appliquées en premier et les règles SafeGuard LAN Crypt sont appliquées ensuite. L'ordre de priorité peut être modifié.

Note: Le paramètre de SafeGuard Enterprise s'applique toujours pour le **Chiffrement persistant**. Il ne peut pas être modifié.

Nouveau chiffrement de fichiers chiffrés par SafeGuard Enterprise Data Exchange

L'**Assistant de chiffrement initial** vous permet de chiffrer de nouveau les fichiers qui ont été chiffrés à l'aide de SafeGuard Data Exchange. En revanche, la règle de chiffrement de SafeGuard Enterprise ne s'appliquera plus. Retrouvez plus de renseignements à la section Assistant de chiffrement initial *(page 11)*. Ces fichiers existent, par exemple, si la règle de chiffrement a été supprimée et que les fichiers n'ont pas été déchiffrés explicitement. Dans ce cas, l'option **Fichiers chiffrés à nouveau selon le profil** peut être sélectionnée dans l'**Assistant de chiffrement initial**. De cette manière, les fichiers seront de nouveau chiffrés conformément aux règles de chiffrement de SafeGuard LAN Crypt.

2 Chiffrement

2.1 Chiffrement transparent

Pour un utilisateur, le chiffrement transparent signifie que tous les fichiers stockés sous forme chiffrée (dans des répertoires ou lecteurs sécurisés) sont automatiquement déchiffrés dans la mémoire principale lorsqu'ils sont ouverts par une application. Lorsque le fichier est enregistré, il est automatiquement chiffré. Le chiffrement transparent s'applique à toutes les opérations sur fichiers. Comme toutes les tâches sont gérées en arrière-plan, les utilisateurs ignorent ce qui se passe pendant qu'ils travaillent avec des données chiffrées.

Note:

SafeGuard LAN Crypt ne procède pas au chiffrement des fichiers pour lesquels la **Compression NTFS** ou le **Chiffrement EFS** sont utilisés dans le système de fichiers NTFS de Windows. Toutefois, l'Assistant de chiffrement initial peut décompresser puis déchiffrer les fichiers compressés NTFS et/ou les fichiers EFS chiffrés durant le chiffrement initial, à condition qu'une règle adaptée existe pour ces fichiers. Ensuite, SafeGuard LAN Crypt chiffrera les fichiers selon les règles de chiffrement en vigueur. Le responsable de la sécurité définit si un utilisateur est habilité à décompresser les fichiers compressés NTFS ou à déchiffrer les fichiers EFS chiffrés, si nécessaire.

Le chiffrement est régi uniquement par les règles de chiffrement, il ne dépend pas des répertoires. Le chiffrement fonctionne de la manière suivante :

- Tous les fichiers associés à une règle de chiffrement font l'objet d'un chiffrement automatique.
- Si des fichiers sont copiés ou déplacés vers un répertoire sécurisé, ils sont chiffrés conformément à la règle de chiffrement applicable à ce répertoire. Le responsable de la sécurité peut définir des règles de chiffrement différentes pour des extensions ou des noms de fichiers différents dans le même répertoire.
- Lorsque vous renommez un fichier chiffré, celui-ci reste chiffré (tant qu'une autre règle de chiffrement n'existe pas pour le nouveau nom ou la nouvelle extension de fichier).
- Lorsqu'un utilisateur copie ou déplace des fichiers chiffrés vers un emplacement où ne s'applique plus la règle de chiffrement en cours, ces fichiers sont déchiffrés.

  Note: Une exception à cette règle existe lorsqu'un utilisateur déplace les fichiers d'un répertoire à un autre sur le même partage réseau. Dans ce cas, les fichiers restent chiffrés bien qu'aucune règle de chiffrement ne soit valide.

- Lorsque l'administrateur a activé le **Chiffrement persistant**, les fichiers restent chiffrés même s'ils sont déplacés vers un emplacement pour lequel aucune règle de chiffrement ne s'applique.
- Lorsque l'utilisateur copie ou déplace des fichiers chiffrés vers un emplacement où ne s'applique plus la règle de chiffrement en cours car elle a été remplacée par une autre, le système commence par déchiffrer ces fichiers puis les chiffre à nouveau avec la clé définie pour cet emplacement.
- Lorsqu'un utilisateur copie ou déplace des fichiers chiffrés vers un emplacement sur lequel s'applique une règle de chiffrement différente, les fichiers sont déchiffrés, puis chiffrés à nouveau avec la clé définie pour cet emplacement.

2.1.1 Accès aux données chiffrées

Si le profil d'un utilisateur ne contient pas de clé ou de règle de chiffrement pour un répertoire précis dans la stratégie de chiffrement, l'accès aux données chiffrées de ce répertoire sera refusé. L'utilisateur ne pourra pas lire, copier, déplacer, renommer, etc. des fichiers chiffrés dans ce répertoire.

L'utilisateur pourra accéder à ces fichiers s'il possède la clé ayant servi à les chiffrer même si son profil de chiffrement ne contient pas de règle de chiffrement pour ces fichiers.

Note: Lorsque vous stockez des fichiers ouverts uniquement avec la clé disponible (fichiers sans règles de chiffrement associées), vous pouvez les configurer en format non chiffré. Cela est possible car les applications créent des fichiers temporaires, suppriment le fichier source puis renomment le fichier temporaire. Comme le nouveau fichier ne possède pas de règle de chiffrement, il est créé dans un format non chiffré. Pour éviter cela, un programme doit être enregistré

en tant que « programme possédant un comportement particulier à l'enregistrement des fichiers ». Retrouvez plus de renseignements à la section Boîte de dialogue État du client *(page 21)*.

2.1.2 Changement de nom ou déplacement des répertoires

Pour des raisons de performance, SafeGuard LAN Crypt ne modifie pas l'état de chiffrement lorsque des répertoires tout entier sont déplacés sur le même lecteur de disque avec l'Explorateur Windows. Par conséquent, aucun chiffrement ou déchiffrement n'est réalisé lorsqu'un répertoire est renommé ou déplacé.

Si les fichiers dans ces dossiers ont déjà été chiffrés, ils le demeurent même s'ils sont dans un dossier portant un nouveau nom ou s'ils sont archivés à un nouvel emplacement. Si l'utilisateur détient la clé adéquate, il peut continuer à travailler avec ces fichiers comme d'habitude.

La seule exception concerne les fichiers ou les dossiers déplacés vers une autre partition ou sur un support de mémoire USB pour lequel aucune règle de chiffrement n'est mise en œuvre. Si le **Chiffrement persistant** n'est pas activé, les fichiers sont déchiffrés lorsqu'ils sont déplacés vers ces types de support. Toutefois, si le responsable de la sécurité a activé la fonction de **Chiffrement persistant**, ces fichiers restent chiffrés.

Déplacement sécurisé

SafeGuard LAN Crypt prend en charge le déplacement sécurisé des fichiers et des répertoires. Lorsque l'utilisateur déplace les fichiers à l'aide de SafeGuard LAN Crypt, les fichiers et répertoires sont chiffrés, déchiffrés et chiffrés à nouveau conformément aux règles de chiffrement applicables pour le nouvel emplacement de stockage. Ensuite les fichiers sources sont supprimés de manière sécurisée.

Cette fonction est accessible via la commande **SafeGuard LAN Crypt** > **Déplacement sécurisé** dans le menu contextuel de l'Explorateur Windows. Indiquez un emplacement de destination du fichier lorsque vous y êtes invité.

2.1.3 Déchiffrement explicite des fichiers

Pour déchiffrer un fichier, il suffit de le copier ou le déplacer vers un répertoire ne comportant pas de règle de chiffrement. Le fichier est automatiquement déchiffré.

Cependant :

- le profil de chiffrement correct doit être chargé ;
- l'utilisateur doit posséder la bonne clé ;
- le profil de chiffrement actif n'inclut pas une règle de chiffrement pour le nouvel emplacement ; et
- le **Chiffrement persistant** ne doit pas être activé.

Note: SafeGuard LAN Crypt permet également de chiffrer les dossiers hors connexion sous Windows. Dans ce cas, des problèmes risquent de se produire lorsque ce programme est utilisé en conjonction avec des utilitaires antivirus. Les Notes de publication fournies avec SafeGuard LAN Crypt Client vous donne des informations plus spécifiques sur les problèmes couramment rencontrés avec les modules de contrôle antivirus.

2.1.4 Suppression des fichiers chiffrés - Corbeille

Si le profil de chiffrement d'un utilisateur est chargé, il peut supprimer tout fichier chiffré dont il possède la clé.

Note: La suppression des fichiers signifie leur envoi dans la Corbeille Windows. Pour assurer le plus haut niveau de sécurité, les fichiers chiffrés par SafeGuard LAN Crypt demeurent chiffrés dans la Corbeille. Aucune clé n'est nécessaire pour vider la Corbeille.

2.1.5 Fichiers/répertoires exclus du chiffrement

Les fichiers et répertoires suivants sont automatiquement exclus du chiffrement (même si une règle de chiffrement a été définie pour ces fichiers :

- Fichiers dans le répertoire d'installation SafeGuard LAN Crypt
- Fichiers dans le répertoire d'installation Windows
- Cache du fichier de stratégie

  emplacement est indiqué dans SafeGuard LAN Crypt Administration et affiché sur l'onglet **Profil** de la boîte de dialogue **État**.
- Répertoire racine du lecteur système. Les sous-dossiers ne sont pas exclus.
- Emplacements indexés (search-ms).

2.1.6 Chiffrement persistant

Un responsable de la sécurité peut configurer le **Chiffrement persistant** pour SafeGuard LAN Crypt. Les fichiers ne restent chiffrés que tant qu'ils sont soumis à une règle de chiffrement.

Par exemple, si un utilisateur copie un fichier chiffré dans un dossier qui n'est associé à aucune règle de chiffrement, ce fichier sera enregistré en clair dans le dossier cible. En activant le **Chiffrement persistant**, vous êtes sûr que les fichiers restent chiffrés lorsqu'ils sont déplacés ou copiés.

Pour éviter la création non intentionnelle de copies brutes de fichiers chiffrés, les copies des fichiers chiffrés seront créées chiffrées même si elles sont créées dans des emplacements non couverts par une règle de chiffrement.

Les responsables de la sécurité peuvent désactiver ce comportement dans SafeGuard LAN Crypt Configuration. S'il est désactivé, les fichiers sont déchiffrés lorsqu'ils sont copiés/déplacés dans un emplacement qui ne fait pas l'objet d'une règle de chiffrement.

Pour le **Chiffrement persistant**, les règles suivantes s'appliquent :

- Le pilote SafeGuard LAN Crypt conserve uniquement le nom du fichier sans aucune information sur le chemin. Ce nom peut uniquement être utilisé à des fins de comparaison. Par conséquent, ils détecteront uniquement les situations dans lesquelles les noms du fichier source et du fichier cible sont identiques. Si le fichier est renommé pendant la copie, le fichier copié est considéré comme étant un fichier 'différent'. Il n'est donc pas soumis au **Chiffrement persistant**.
- Lorsqu'un utilisateur utilise l'option **Enregistrer sous** pour enregistrer un fichier chiffré sous un nom de fichier différent dans un emplacement non couvert par une règle de chiffrement, le fichier sera déchiffré.
- Les informations sur les fichiers sont conservées pendant une durée de temps limitée uniquement. Si l'opération dure trop longtemps (plus de 15 secondes) le nouveau fichier créé est considéré comme étant un fichier différent et ne sera donc pas soumis au **Chiffrement persistant**.

2.1.6.1 Chiffrement persistant et règle de chiffrement

Comme mentionné précédemment, le **Chiffrement persistant** s'assure qu'un fichier chiffré conserve son état de chiffrement (par exemple, sa clé de chiffrement originale). Ceci est normal si le fichier est déplacé dans un dossier sur lequel aucune stratégie de chiffrement ne s'applique. En revanche, si le fichier est copié ou déplacé à un endroit sur lequel s'applique une stratégie de chiffrement, cette dernière est prioritaire et prévaut sur le **Chiffrement persistant**. Le fichier est chiffré avec la clé définie dans la règle de chiffrement et non pas avec celle utilisée la première fois.

2.1.6.2 Chiffrement persistant et règle Ignorer le chemin

Une règle Ignorer le chemin est prioritaire sur le **Chiffrement persistant**. Ceci signifie que les fichiers chiffrés qui sont copiés dans un dossier sur lequel s'applique une règle Ignorer le chemin seront déchiffrés.

Une règle Ignorer le chemin est généralement activée pour les fichiers utilisés très fréquemment et qui ne nécessitent pas de chiffrement. Elle accroît les performances du système.

2.1.6.3 Chiffrement persistant et règle Exclure le chemin

Une règle Exclure le chemin est prioritaire sur le **Chiffrement persistant**. Ceci signifie que les fichiers chiffrés qui sont copiés dans un dossier sur lequel s'applique une règle Exclure le chemin seront déchiffrés.

2.1.7 Limites du chiffrement persistant

Le **Chiffrement persistant** présente certaines limites. Retrouvez-les ci-dessous :

Les fichiers qui ne sont pas supposés rester clairs sont chiffrés

- **Les fichiers non chiffrés sont copiés à divers endroits en appliquant ou pas les règles de chiffrement.**

  Si un fichier non chiffré est copié à divers endroits en même temps et qu'une règle de chiffrement s'applique sur l'un de ces endroits, il se peut que toutes les autres copies du même fichier soient également chiffrées même si le fichier d'origine ne l'est pas.

  Si un fichier non chiffré est copié à un endroit chiffré en premier lieu, ce fichier est ajouté à la liste interne de l'outil de chiffrement. Lorsque la seconde copie est créée, l'outil de chiffrement retrouve le nom du fichier dans sa liste et chiffre également la seconde copie.

- **Création d'un fichier avec le même nom après accès à un fichier chiffré**

  Si un fichier chiffré est ouvert (accédé) et qu'un nouveau fichier portant le même nom est créé peu de temps après, le nouveau fichier est chiffré avec la même clé que celle du premier fichier.

  Note: ceci s'applique uniquement si la même application ou le même thread est utilisé pour lire le fichier chiffré et pour créer le nouveau fichier.

  Par exemple : dans l'Explorateur Windows, cliquez avec le bouton droit de la souris sur un dossier ayant une règle de chiffrement et cliquez sur **Nouveau** > **Nouveau document texte**. Cliquez avec le bouton droit de la souris sur un dossier n'ayant pas de règle de chiffrement et cliquez sur **Nouveau** > Nouveau document texte. Le second fichier est également chiffré.

Les fichiers sont non chiffrés

- **Plusieurs copies d'un fichier sont créés**

  Si les copies d'un fichier chiffré sont créées dans le même dossier que celui du fichier original, ces copies ne sont pas chiffrées. Les copies créées ayant différents noms de fichier (par exemple doc.txt vs. doc - Copy.txt), la correspondance de nom de fichier échoue et ceux-ci ne sont pas chiffrés par le chiffrement persistant.

2.1.8 API Client et balises de chiffrement pour les produits de protection contre la perte de données

Si un produit de protection contre la perte de données identifie des données devant être chiffrées, il utilise l'API de SafeGuard LAN Crypt Client pour chiffrer ces fichiers. Dans **SafeGuard LAN Crypt Administration**, vous pouvez créer différentes balises de chiffrement qui indiquent la clé SafeGuard LAN Crypt à utiliser. L'API Client utilise les balises de chiffrement prédéfinies afin d'appliquer des clés spéciales en fonction des différences de contenu. Par exemple, la balise de chiffrement **<CONFIDENTIEL>** est utilisée pour chiffrer tous les fichiers considérés comme confidentiels par votre produit de protection contre la perte de données.

2.2 Désactivation/Activation du chiffrement transparent

La désactivation du chiffrement transparent (dans le menu Utilisateur de SafeGuard LAN Crypt) signifie que toutes les données sollicitées après la désactivation du chiffrement transparent ne seront plus chiffrées ou déchiffrées automatiquement. Les nouveaux fichiers ne sont pas chiffrés même s'il existe une règle de chiffrement dans le profil de chiffrement de l'utilisateur.

Note: La désactivation du chiffrement transparent peut avoir des conséquences importantes si les fichiers chiffrés avaient normalement dû rester chiffrés pendant leur copie ou déplacement vers un autre emplacement non régi par des règles de

chiffrement (par exemple, si les fichiers chiffrés doivent être joints à un courrier électronique ou copiés sur un CD). Ces fichiers seront déchiffrés lors de leur copie ou déplacement dans un emplacement sans règles de chiffrement.

Si vous avez activé la fonction de **Chiffrement persistant**, les fichiers restent automatiquement chiffrés même s'ils sont déplacés vers un dossier ne comportant pas de règle de chiffrement. Si le **Chiffrement persistant** est utilisé, vous n'avez pas besoin de désactiver la chiffrement transparent. Le **Chiffrement persistant** permet de s'assurer que les fichiers restent chiffrés, même s'ils sont déplacés vers un autre dossier par accident ou si l'utilisateur a oublié de désactiver le chiffrement avant de les déplacer ou de les copier. Vous devez redémarrer l'ordinateur client pour appliquer le nouveau état du **Chiffrement persistant** (actif ou non actif).

Note: Lorsque le **Chiffrement persistant** est activé et qu'un utilisateur déplace ou copie un fichier dans un dossier régi par une règle d'exclusion, il reçoit un message d'avertissement indiquant que le fichier sera déchiffré.

2.3 Outils de chiffrement transparent et de compression des fichiers

Les outils de compression de fichiers lisent le contenu des fichiers et le compressent. Si une option de chiffrement/ déchiffrement transparent est activée, les outils de compression de fichiers reçoivent les fichiers déchiffrés et les compressent. Les fichiers dans l'archive ainsi créée ne sont plus chiffrés.

Si l'archive est stockée dans un répertoire pour lequel aucune règle de chiffrement n'existe, tous les fichiers stockés sont déchiffrés.

Si le **Chiffrement persistant** est activé, les fichiers ne seront pas compressés sous forme chiffrée.

Pour veiller à ce que les fichiers soient compressés sous une forme chiffrée par les outils de compression de fichiers, l'option de chiffrement transparent doit être désactivée durant l'utilisation de ces outils.

Pour vous assurer que les fichiers sont compressés sous une forme chiffrée, vous pouvez également définir les outils de compression de fichiers en tant qu'applications non gérées. Le responsable de sécurité doit s'en charger.

Le responsable de la sécurité peut définir les outils de compression de fichiers en tant qu'Applications non gérées. Ceci permet d'assurer que les fichiers sont compressés sous forme chiffrée.

2.4 Chiffrement initial et chiffrement explicite

Suite à l'installation de SafeGuard LAN Crypt, veuillez lancer la procédure de chiffrement initial. Au cours de cette procédure, tous les fichiers sont cryptés à l'aide du profil de chiffrement chargé. Pour réaliser ce chiffrement initial, vous devez utiliser :

- l'icône de la barre d'état système de SafeGuard LAN Crypt. Retrouvez plus de renseignements à la section Application de l'utilisateur *(page 20)*.
- les extensions de l'Explorateur de SafeGuard LAN Crypt. Retrouvez plus de renseignements à la section Extensions de l'Explorateur *(page 22)*
- l'outil **sglcinit.exe** qui prend également en charge le mode automatique. Retrouvez plus de renseignements à la section Chiffrement initial en mode automatique *(page 14)*.

Outre le chiffrement initial de dossiers tout entier, l'outil de ligne de commande **sglcinit.exe**, en combinaison avec les extensions de l'Explorateur, permet également de chiffrer, déchiffrer et chiffrer à nouveau des fichiers spécifiques.

Le chiffrement, le déchiffrement ou un nouveau chiffrement explicite peuvent être nécessaires dans les cas suivants :

- Des fichiers en texte clair (non chiffrés) sont placés dans un répertoire associé à une règle de chiffrement.
- Des fichiers chiffrés sont placés dans un répertoire ne disposant d'aucune règle de chiffrement.
- Des fichiers placés dans un répertoire chiffré ont été chiffrés avec la mauvaise clé.
- Si les règles de chiffrement dans le profil de chiffrement ont changé.
- Si les fichiers sont chiffrés à l'aide de plusieurs clés.

2.4.1 Assistant de chiffrement initial

L'outil de chiffrement initial, **sglcinit.exe**, propose un Assistant doté d'une interface utilisateur graphique. Cet Assistant prend en charge :

- le chiffrement, le déchiffrement et le nouveau chiffrement des fichiers ;
- la vérification de l'état de chiffrement des fichiers.

Vous pouvez démarrer cet assistant.

- en cliquant sur son icône dans la barre d'état système ;
- en cliquant sur Démarrer/Tous les programmes/Sophos/SafeGuard LAN Crypt/Chiffrement initial ;
- en le démarrant à partir de l'Écran d'accueil de Windows 8/Windows 2012 ;
- en cliquant deux fois sur sglcinit.exe dans le dossier SafeGuard LAN Crypt Program.

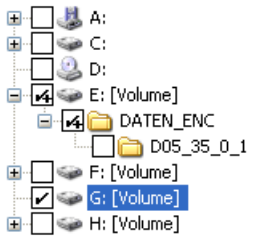
Note: les processus de chiffrement, de déchiffrement et de nouveau chiffrement se font toujours en fonction du profil de chiffrement. Par conséquent, il est essentiel de charger ce dernier.

2.4.1.1 Réalisation d'un chiffrement initial

1. Démarrez l'assistant. Retrouvez plus de renseignements à la section Menu de l'utilisateur *(page 20)*.
2. Sélectionnez l'option Exécuter le chiffrement initial à l'Étape 1 / 5.
3. Cliquez sur **Suivant**.
4. Indiquez à l'Étape 2 / 5 la manière dont les fichiers doivent être traités.
   a. **Fichiers chiffrés selon le profil**
   Si vous sélectionnez cette option, les fichiers seront chiffrés d'après les règles contenues dans le profil de l'utilisateur (paramètres par défaut). Si le système détecte des fichiers déjà chiffrés, il les ignore.
   b. **Fichiers chiffrés à nouveau selon le profil**
   Si vous sélectionnez cette option, les fichiers chiffrés avec une clé différente de celle définie dans le profil seront (également) déchiffrés et chiffrés avec la clé correcte.

   Note: Une condition préalable existe néanmoins. La clé utilisée en premier pour le chiffrement du ou des fichiers doit figurer dans le profil de l'utilisateur.

   Cette option vous permet de chiffrer de nouveau les fichiers qui ont été chiffrés à l'aide de SafeGuard Data Exchange. En revanche, la règle de chiffrement de SafeGuard Enterprise ne s'appliquera plus. Ces fichiers existent, par exemple, si la règle de chiffrement a été supprimée et que les fichiers n'ont pas été déchiffrés explicitement. Dans ce cas, vous pouvez choisir de chiffrer de nouveau ces fichiers à l'aide de l'Assistant de chiffrement initial. Ces fichiers seront de nouveau chiffrés conformément aux règles de chiffrement de SafeGuard LAN Crypt.
5. Cliquez sur **Suivant**.
6. Sélectionnez à présent les dossiers à chiffrer/rechiffrer dans l'arborescence à l'Étape 3 / 5.



Les dossiers sélectionnés sont indiqués d'une coche. Un signe + indique que le dossier contient des sous-dossiers qui ne seront pas traités, c'est-à-dire que ces sous-dossiers ne seront ni chiffrés ni chiffrés de nouveau.

Cliquez sur **Règles de profil** pour sélectionner automatiquement tous les répertoires pour lesquels le profil de l'utilisateur inclut des règles de chiffrement.

Cliquez sur **Avancés** pour accéder aux options supplémentaires :

Note: Ces paramètres, modifiables par l'utilisateur, dépendent de la configuration de la version SafeGuard LAN Crypt Client. Le responsable de sécurité centralise la définition de la configuration.

- **Déchiffrer les fichiers EFS chiffrés si nécessaire**

  Sélectionnez cette option pour déchiffrer et chiffrer de nouveau les fichiers chiffrés par EFS. Veuillez noter qu'une règle de chiffrement doit s'appliquer.

  Si vous ne sélectionnez pas cette option, l'assistant de chiffrement initial ignore les fichiers EFS chiffrés. Ils ne seront pas chiffrés de nouveau par SafeGuard LAN Crypt, même si une règle de chiffrement a été définie les concernant.

- **Décompresser les fichiers NTFS compressés si nécessaire**

  Sélectionnez cette option pour décompresser les fichiers NTFS compressés puis les chiffrer. Veuillez noter qu'une règle de chiffrement doit s'appliquer.

  Si vous ne sélectionnez pas cette option, l'assistant de chiffrement initial ignore les fichiers NTFS chiffrés. Ils ne seront pas chiffrés, même si une règle de chiffrement a été indiquée les concernant.

- **Déchiffrer/chiffrer de nouveau les fichiers chiffrés avec plusieurs clés**

  Sélectionnez cette option pour chiffrer de nouveau les fichiers qui étaient chiffrés avec plusieurs clés. Les fichiers seront chiffrés à l'aide d'une seule clé. Veuillez noter qu'une règle de chiffrement doit s'appliquer.

  Cette option est uniquement disponible si l'option **Fichiers chiffrés selon le profil** ou **Fichiers chiffrés à nouveau selon le profil** a été sélectionnée à l'Étape 2/5. Autrement, cette option est grisée.

- **Inclure les types de fichiers suivants uniquement :**

  Sélectionnez les types de fichier sur lesquels vous souhaitez limiter l'opération de chiffrement initial (par exemple ; .docx, .rtf). Ce paramètre s'applique uniquement aux fichiers pour lesquels une règle de chiffrement existe. Si des fichiers de types différents sont présents dans le répertoire, ils ne seront pas traités pendant le chiffrement initial. Ils ne feront l'objet d'un chiffrement que si l'utilisateur les ouvre et les enregistre. Indiquez les différents types de fichier en les séparant par des points-virgules.

7. Cliquez sur **Suivant**.

8. Indiquez à présent les fichiers à inclure dans le rapport de chiffrement initial à l'Étape 4 / 5. Pour accéder au rapport de chiffrement initial, l'utilisateur doit choisir parmi les options suivantes :

   a. **Signaler les erreurs uniquement**
   Ce rapport d'état signale uniquement les fichiers pour lesquels des erreurs sont apparues au moment du chiffrement.

   b. **Signaler les fichiers modifiés et les erreurs**
   Ce rapport d'état signale tous les fichiers modifiés et pour lesquels des erreurs sont apparues au moment du chiffrement.

   c. **Signaler tous les fichiers.**
   Ce rapport d'état intègre tous les fichiers.

9. Cliquez sur **Suivant**.
   Le **Résultat** du chiffrement, le **nom de la clé** utilisée et l'algorithme de chiffrement seront affichés pour chaque fichier à l'Étape 5 / 5.

   Si le chiffrement a échoué pour les fichiers individuels, vous pouvez immédiatement tenter de les chiffrer à nouveau. Appuyez pour cela sur le bouton **Réessayer**.

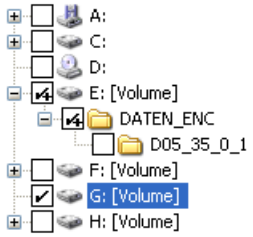
   Il vous suffit de cliquer sur l'en-tête de colonne pour trier les résultats par ordre alphabétique. En outre, vous pouvez enregistrer le rapport d'état sous forme de fichier XML à l'emplacement de votre choix (bouton **Exporter**). Le rapport d'état vous permet d'exécuter à nouveau le chiffrement des fichiers si le chiffrement échoue.

10. Cliquez sur **Terminer**.

L'assistant se ferme.

2.4.1.2 Vérification de l'état de chiffrement

1. Démarrez l'assistant.
2. Sélectionnez l'option **Vérifier l'état du chiffrement** à l'Étape 1/5.
3. Cliquez sur **Suivant**.
4. Sélectionnez les dossier que vous voulez vérifier à l'Étape 2/5.



5. Sélectionnez les dossiers en cochant la case leur correspondant.

   Un signe + indique que le dossier contient des sous-dossiers qui ne seront pas traités. Par conséquent, l'état de chiffrement n'est pas vérifié.

   Cliquez sur **Règles de profil** pour sélectionner automatiquement tous les répertoires pour lesquels le profil de l'utilisateur inclut des règles de chiffrement.

   Cliquez sur **Avancés** pour limiter l'opération de vérification à des types de fichier spécifiques :
   - **Inclure les types de fichiers suivants uniquement** :

     Si vous indiquez des types de fichier spécifiques ici (par exemple .txt, .doc, etc.), seuls les fichiers du type indiqué seront vérifiés.

     Si un répertoire contient également des fichiers d'un type différent (non indiqué ici), ils seront pas pris en compte. Indiquez les différents types de fichier en les séparant par des points-virgules.

6. Cliquez sur **Suivant**.

   Le **Résultat** de la vérification, le **Nom de la clé** utilisée et l'algorithme de chiffrement seront affichés pour chaque fichier à l'Étape 3/5.

   Il vous suffit de cliquer sur l'en-tête de colonne pour trier les résultats par ordre alphabétique.

   Cliquez sur le bouton **Exporter** pour enregistrer le rapport d'état sous dans un fichier XML à l'emplacement de votre choix.

7. Cliquez sur **Terminer**.
   L'assistant se ferme.

2.4.1.3 Déchiffrement des fichiers

Les fichiers chiffrés par SafeGuard LAN Crypt peuvent être déchiffrés si plus aucune règle de chiffrement ne s'applique. Si le chiffrement initial doit être de nouveau exécuté, par exemple en cas de modification des règles de chiffrement dans le profil de l'utilisateur, les fichiers pour lesquels les règles de chiffrement n'existent plus peuvent être déchiffrés au moyen de cet assistant.

Pour déchiffrer les fichiers, sélectionnez l'option **Effectuer le chiffrement initial** à l'Étape 1 / 5 de l'assistant, puis l'option **Déchiffrer les fichiers avec les clés sélectionnées** sous **Déchiffrement** à l'Étape 2 / 5.

Sélectionnez les clés par la suite. Seuls les fichiers chiffrés au moyen des clés sélectionnées peuvent être déchiffrés. Toutefois, ils ne seront que déchiffrés si plus aucune règle de chiffrement ne les concerne.

Note: SafeGuard LAN Crypt ne déchiffre que les fichiers pour lesquels aucune règle de chiffrement ne s'applique.

Exemple :

le lancement de l'Assistant de chiffrement initial intervient car le profil utilisateur a été modifié. Pour veiller à ce que tous les fichiers disposent de l'état de chiffrement souhaité après la fermeture de l'Assistant de chiffrement initial, procédez comme suit :

1. Activez l'option **Chiffrer les fichiers conformément au profil**.

   Tous les fichiers sont chiffrés conformément aux nouvelles règles de chiffrement.
2. Activez l'option **Chiffrer de nouveau les fichiers conformément au profil**.

   Si les fichiers doivent être chiffrés avec une clé différente d'après les nouvelles règles, ils seront alors chiffrés de nouveau.
3. Activez **Déchiffrer les fichiers avec les clés sélectionnées** et sélectionnez toutes les clés.

   Les fichiers chiffrés, pour lesquels aucune règle de chiffrement n'existe, seront déchiffrées. SafeGuard LAN Crypt ne déchiffre que les fichiers pour lesquels aucune règle de chiffrement ne s'applique. Ainsi, la sélection de toutes les clés ne pose aucun problème.

Une fois le processus terminé avec succès et l'Assistant fermé, tous les fichiers possèdent l'état de chiffrement adéquat.

Le déchiffrement explicite des fichiers est important si le **Chiffrement persistant** est activé. Dans ce cas, les fichiers ne seront pas automatiquement déchiffrés au moment où ils seront copiés ou déplacés d'un répertoire sur lequel s'applique une règle de chiffrement vers un répertoire sur lequel aucune règle de chiffrement n'existe.

2.4.2 Chiffrement initial en mode automatique

Si vous souhaitez utiliser l'outil **sglcinit.exe** en mode automatique, exécutez sglcinit.exe à partir de la ligne de commande avec des paramètres spécifiques, à partir de son dossier source (par exemple, C:\Program Files\Sophos\SafeGuard LAN Crypt\).

Syntaxe de la ligne de commande :

```
SGLCInit <startpath | %Profile>[/S]
{-DIgnoreDirectory}[/Tv][/Te][/Tr][/Td]
[/Tdk {GUID}][/Dc][/De][/Dm][+FFiletype][/V1|/V2|/V3|/V4] [/X]
[/LLogfile]
```

Paramètres :

- **Start path**

  Cette option permet de limiter le chiffrement, le déchiffrement ou le nouveau chiffrement à un fichier spécifique (par exemple, C:\Données\ventes.doc) ou de l'étendre à tout un dossier (par exemple, D:\Données). Le paramètre par défaut exclut les sous-dossiers de ce processus !
- **%Profil**

  Traite toutes les règles avec un chemin absolu dans le profil de chiffrement chargé. Chiffre/déchiffre ou chiffre à nouveau les fichiers si nécessaire.

  Note: Avant de déchiffrer un fichier, le profil doit contenir une règle d'EXCLUSION pour ce dernier.
- **/s**

  Inclut tous les sous-dossiers du chemin de départ.
- **/h** ou **/?**

  Ouvre une fenêtre permettant d'obtenir de l'aide sur la syntaxe de sglcinit.exe.
- **-DIgnoreDirectory**

  Ignore ce dossier.

- **/Tv**

  Mode de tâche : v = Affiche l'état de chiffrement des fichiers.

- **/Te**

  Mode de tâche : e = chiffre les fichiers conformément au profil de chiffrement si nécessaire.

- **/Tr**

  Mode de tâche : r = chiffre de nouveau les fichiers conformément au profil de chiffrement si nécessaire.

- **/Td**

  Mode de tâche : d = déchiffre les fichiers conformément au profil de chiffrement si nécessaire.

- /Tdk

  Mode de tâche : dk= Déchiffre les fichiers qui ont été chiffrés à l'aide des clés prédéfinies. Vous devez saisir le GUID des clés.

  Note: tous les paramètres du mode de Tâche peuvent être réunis au sein d'un même appel de commande.

- **/Dc**

  Cette option décompresse les fichiers NTFS compressés puis les chiffre. Si cette option n'est pas définie, les fichiers NTFS compressés sont ignorés.

- **/De**

  Cette option déchiffre les fichiers EFS chiffrés et désactive le chiffrement EFS des dossiers affectés. Si cette option n'est pas définie, les fichiers EFS chiffrés sont ignorés.

- **/Dm**

  Cette option déchiffre les fichiers chiffrés avec plusieurs clés puis les chiffre de nouveau. Les fichiers sont ainsi chiffrés avec une seule clé.

- **+Ffile type**

  Si vous spécifiez les types de fichiers avec cette option (par exemple, +Ftxt+Fdoc), seuls les fichiers dont le type est concerné sont traités. Ce paramètre affecte uniquement les fichiers pour lesquels une règle de chiffrement existe.

  Si un répertoire contient également des fichiers d'un type différent qui n'est pas spécifié par cette option, ils ne sont pas pris en compte lors du chiffrement initial. Ils ne feront l'objet d'un chiffrement que si l'utilisateur les ouvre et les enregistre.

- **/V0**

  Mode commenté 0 : ne rien signaler.

- **/V1**

  Mode commenté 1 : répertorie les messages d'erreur.

- **/V2**

  Mode commenté 2 : répertorie les fichiers modifiés.

- **/V3**

  Mode commenté 3 : répertorie tous les fichiers.

- **/V4**

  Mode commenté 4 : répertorie les fichiers en texte clair.

- **/E**

  Arrêter lors d'une erreur.

- **/X**

  Chiffrement initial sans afficher de fenêtre

- **/LFichierJournal**

  Écrit la sortie dans le fichier indiqué.

Note: les paramètres %PROFILE et /Td doivent uniquement être utilisés ensemble si les fichiers que vous souhaitez déchiffrer sont répertoriés dans le profil avec une règle d'exclusion. Autrement, utilisez /Td avec le chemin de départ (startpath).

```
sglcinit.exe %PROFILE -DC:\ignore /S /Te /Tdk {1234ABCD-1234-1234-1234-1234ABCD}
 {5678EFGH-5678-5678-5678-5678EFGH} /V1 /LC:\logfile.xml
```

sglcinit.exe D:\data /S /V4

Répertorie tous les fichiers en texte clair dans D:\data et dans ses sous-dossiers.

3 Stratégies

3.1 Certificats

Avant qu'un utilisateur puisse accéder à son profil de chiffrement, le certificat correspondant doit être disponible sur l'ordinateur. Le responsable de la sécurité distribue ces certificats aux utilisateurs. Ces derniers importent le certificat dans leurs postes de travail. Si les certificats sont disponibles à la première ouverture de session, la procédure s'effectuera sans aucune interaction de l'utilisateur.

SafeGuard LAN Crypt offre une option d'importation automatique des certificats lors du premier chargement du profil de chiffrement. Dans ce cas, le responsable de sécurité configure le système de sorte que SafeGuard LAN Crypt puisse trouver le fichier du certificat à l'ouverture de la session et lance son importation automatiquement. L'utilisateur est invité une fois à saisir le code confidentiel (PIN) du fichier de clé PKCS#12.

Note: Le responsable de sécurité est chargé de distribuer aux utilisateurs le code PIN exigé pour l'importation automatique du certificat.

Une vérification du certificat est effectuée à chaque chargement du profil de chiffrement. Dès qu'un certificat valide a été trouvé, l'utilisateur est connecté à SafeGuard LAN Crypt. Si aucun certificat valide n'est trouvé, l'utilisateur ne pourra pas travailler avec les données chiffrées.

Note: Lorsqu'un utilisateur ne parvient pas à se connecter à SafeGuard LAN Crypt, il reçoit un message d'erreur lui indiquant les raisons du refus de connexion.

Des règles de chiffrement spéciales intégrées aux profils de chiffrement de SafeGuard LAN Crypt permettent aux utilisateurs d'accéder aux données chiffrées. Ces règles indiquent précisément quels fichiers de quels répertoires doivent être chiffrés par chaque clé. Seul le profil de chiffrement d'un utilisateur doit être chargé. Le chiffrement et le déchiffrement se déroulent en arrière-plan (de manière transparente). L'utilisateur ignore que des tâches de chiffrement ou de déchiffrement sont en cours d'exécution.

Note: Les certificats de l'autorité de certification sont uniquement acceptés s'ils sont détenus par une « autorité de certification racine de confiance ». Cependant, SGLC importe tout certificat CA susceptible d'être enregistré dans des fichiers de clés PKCS#12, ainsi que les certificats utilisateur du dossier « Personal - Certificates ». Pour éviter l'affichage d'un message d'erreur, vous devez déplacer manuellement les certificats CA vers une « autorité de certification racine de confiance ».

3.2 Chargement du fichier de stratégie

Comportement par défaut de SafeGuard LAN Crypt

Lorsqu'un utilisateur se connecte à Windows, le chargement de son profil mis en cache intervient en premier. SafeGuard LAN Crypt vérifie la disponibilité pour l'utilisateur d'un nouveau fichier de stratégie. L'application établit pour cela une connexion vers l'emplacement indiqué du fichier de stratégie (lecteur réseau ou serveur Web via http/https). Si un nouveau fichier de stratégie y figure, le profil en cache de l'utilisateur est mis à jour.

L'utilisateur peut commencer à travailler avec des fichiers chiffrés pendant que SafeGuard LAN Crypt vérifie l'existence d'une nouvelle version du fichier de stratégie. Si l'emplacement spécifié n'est pas accessible, l'utilisateur travaille avec le profil utilisateur mis en cache jusqu'à ce que celui-ci puisse être mis à jour.

Note: SafeGuard LAN Crypt vérifie les certificats de l'utilisateur et du responsable (principal) de la sécurité. Si les certificats contiennent un ”point de distribution CRL” et qu'aucun CRL valide n'est présent dans le système, Windows essaye d'importer le CRL à partir d'une adresse spécifiée. Si un pare-feu est installé, un message apparaît vous indiquant qu'un programme (loadprof.exe) essaye d'établir une connexion à Internet. Dans certains cas, le téléchargement du profil de l'utilisateur peut entraîner l'affichage de ce message.

Comportement défini par les responsables de sécurité

Le responsable de sécurité peut modifier le comportement par défaut à l'aide des paramètres utilisés de manière centrale. Les responsables de la sécurité peuvent définir la durée de validité des stratégies mises en cache sur les ordinateurs clients. Ils peuvent définir les intervalles de mise à jour des fichiers de sécurité. Les paramètres définis par le responsable de la sécurité s'affichent dans l'onglet **Profil** de la boîte de dialogue **État du client**. Retrouvez plus de renseignements à la section Boîte de dialogue État du client *(page 21)*.

Au cours de la période définie ici, le fichier de stratégie est valide sur le client et l'utilisateur peut accéder aux données chiffrées, même si aucune connexion n'existe à l'emplacement du fichier de stratégie.

Une fois ce délai expiré, SafeGuard LAN Crypt tente de charger le fichier de stratégie du lecteur réseau afin de le mettre à nouveau à jour. Si cela se révèle impossible, le fichier de stratégie n'est pas chargé. L'utilisateur n'est alors plus en mesure d'accéder aux données chiffrées.

Le fichier de stratégie ne peut être mis à jour et chargé à nouveau que si un fichier de stratégie valide est disponible (par exemple, lors de la connexion suivante avec une connexion à l'emplacement client des fichiers de stratégie). L'utilisateur accède alors à nouveau aux données chiffrées. Le compteur réservé à la durée de stockage en mémoire cache est réinitialisé.

En indiquant la durée du stockage en mémoire cache, les responsables de la sécurité peuvent s'assurer que les ordinateurs client reçoivent à intervalles réguliers des fichiers de stratégie mis à jour et que les utilisateurs travaillent à tout moment avec des stratégies actualisées. Ils peuvent empêcher les utilisateurs de travailler avec les mêmes fichiers de stratégie pendant une période de temps illimitée. Si cette option est définie sur **non configuré**, un utilisateur peut continuer à travailler avec une version en cache du fichier de stratégie pendant une période de temps illimitée.

Le compteur correspondant à la durée autorisée de stockage en mémoire cache est réinitialisé dans les cas suivants :

- L'emplacement de stockage des fichiers de stratégie est accessible et un fichier de stratégie valide a été transféré sur le client (par ex. au moment de la connexion de l'utilisateur ou par déclenchement après un intervalle de mise à jour défini). Cependant, il ne s'agit pas d'un nouveau fichier de stratégie.
- Un nouveau fichier de stratégie est disponible et a été chargé correctement.

Le compteur correspondant à la durée autorisée de stockage en mémoire cache n'est PAS réinitialisé dans les cas suivants :

- L'ordinateur client tente de recevoir un nouveau fichier de stratégie. Cependant, l'emplacement de stockage des fichiers de stratégie n'est pas accessible.
- Un nouveau fichier de stratégie a été transféré. Cependant, une erreur empêche son chargement.
- Un nouveau fichier de stratégie est disponible. Cependant, il exige un nouveau certificat. L'utilisateur ne dispose pas de ce certificat ou n'est pas en mesure de le charger.

En cas d'échec de la mise à jour du fichier de stratégie, la durée d'expiration du fichier de stratégie mis en cache s'affiche dans une info-bulle, sur l'ordinateur client. L'utilisateur peut alors lancer une mise à jour manuelle via l'icône de la barre d'état de SafeGuard LAN Crypt. Retrouvez plus de renseignements à la section Menu de l'utilisateur *(page 20)*.

Les fichiers de stratégie ne sont pas mis en mémoire cache

Un responsable de la sécurité peut également indiquer que le fichier de stratégie ne sera pas mis en mémoire cache. Cela signifie que les utilisateurs reçoivent leurs profils en se connectant, à condition que l'emplacement du fichier de stratégie soit accessible. S'il ne l'est pas, une erreur survient lors du chargement du profil et l'utilisateur ne peut pas accéder aux fichiers chiffrés.

3.3 Connexion à SafeGuard LAN Crypt

Les profils de chiffrement SafeGuard LAN Crypt sont créés par un responsable de la sécurité, conformément à la stratégie de sécurité de l'entreprise, puis sont stockés dans des fichiers de stratégie. Le profil de chiffrement peut uniquement être chargé si l'utilisateur détient le certificat correspondant.

Le chemin des fichiers de stratégie est écrit par l'administrateur système dans le registre du poste de travail client. Lorsqu'un utilisateur se connecte à SafeGuard LAN Crypt, le profil de chiffrement, stocké dans les fichiers de stratégie, est chargé sur le poste de travail client. SafeGuard LAN Crypt charge les fichiers de stratégie à partir du répertoire indiqué et vérifie si l'utilisateur est autorisé à les charger en vérifiant son certificat.

Connexion avec token

Les utilisateurs peuvent également se connecter à SafeGuard LAN Crypt en vous aidant d'un token. L'une des conditions préalables à cette méthode de connexion est que le certificat SafeGuard LAN Crypt de l'utilisateur soit archivé sur le token. Si le certificat d'utilisateur se trouve sur un token connecté au système, l'utilisateur pourra se connecter.

Lorsque des tokens sont utilisés pour la connexion, SafeGuard LAN Crypt peut tenter de charger un fichier de stratégie avant que le token ne soit identifié par le système d'exploitation. Dans ce cas, un message s'affiche indiquant que le certificat d'utilisateur est introuvable, même si le token est connecté au système.

L'utilisateur doit charger le fichier de stratégie manuellement via l'application d'utilisateur de la barre d'outils **Charger les règles de chiffrement**. Le token est identifié et l'utilisateur est connecté. Pour éviter ceci, un délai de chargement des profils peut être indiqué dans **SafeGuard LAN Crypt Configuration** (paramètre **Délai de chargement des profils**).

4 Application de l'utilisateur

L'état de SafeGuard LAN Crypt est représenté par une icône dans la barre des tâches Windows.

- **Vert** signifie :

  Les règles de chiffrement sont chargées et le chiffrement transparent a été activé.
- **Jaune** signifie :

  Les règles de chiffrement sont chargées et le chiffrement transparent a été désactivé.
- **Rouge** signifie :

  Aucun profil n'a été chargé.

4.1 Menu de l'utilisateur

Cliquez sur l'icône de clé avec le bouton droit de la souris pour ouvrir le menu de l'utilisateur de SafeGuard LAN Crypt et voir les options suivantes :

- **Charger les règles de chiffrement/Mettre à jour les règles de chiffrement**
- **Effacer les règles de chiffrement**
- **Désactiver/Activer le chiffrement**
- **Afficher profil**
- **État du client**
- **Chiffrement initial**
- **Fermer**
- **À propos de**

Note: Les commandes de menu accessibles dépendent de la configuration de la version SafeGuard LAN Crypt Client. Le responsable de sécurité centralise la définition de la configuration.

- **Charger les règles de chiffrement/Mettre à jour les règles de chiffrement**

  Cette option permet de charger les règles de chiffrement en cours de validité. Cela est important en cas de modification du profil pendant l'exécution.
- **Effacer les règles de chiffrement**

  Cette option empêche l'accès aux données chiffrées. Cette option de sécurité protège les données chiffrées de tout accès non autorisé lorsque l'utilisateur n'est pas devant son poste de travail. Veuillez noter que l'utilisation de la clé privée doit être sécurisée par mot de passe. Sinon, il serait possible de recharger le profil à l'aide de la commande **Charger les règles de chiffrement**.
- **Désactiver /Activer le chiffrement**

  Permet de permuter entre l'activation et la désactivation du chiffrement transparent.

  La désactivation du chiffrement sera utilisée si les fichiers doivent rester chiffrés lorsqu'ils sont copiés ou déplacés dans un dossier non associé à une règle de chiffrement valide. Si le chiffrement était activé, les fichiers seraient déchiffrés au moment de leur copie vers ce type de dossier.

  Par exemple, si un fichier chiffré est mis en pièce jointe d'un courrier électronique, il sera déchiffré automatiquement si le chiffrement transparent est activé. En revanche, si le chiffrement transparent est désactivé, le fichier chiffré pourra être envoyé comme pièce jointe.

  Note: si l'administrateur a activé la fonction de **Chiffrement persistant**, les fichiers chiffrés le demeurent même s'ils sont copiés ou déplacés vers un emplacement pour lequel aucune règle de chiffrement n'a été spécifiée.

- **Afficher profil**

  Affiche les règles et les clés de chiffrement présentes dans les informations de chiffrement des deux onglets.

  La page à onglet Règles de chiffrement actives répertorie les règles qui s'appliquent à l'utilisateur connecté. En outre, l'utilisateur peut également sélectionner les options Afficher les règles Ignorer, Afficher les règles d'exclusion et Afficher les balises de chiffrement pour afficher ces règles de chiffrement.

  L'onglet Clés disponibles affiche la liste de toutes les clés qui sont disponibles pour l'utilisateur actuel.

- **État du client**

  L'option **État du client** affiche des informations détaillées réparties sur plusieurs onglets à propos de l'état actuel de la version de SafeGuard LAN Crypt Client. Retrouvez plus de renseignements à la section Boîte de dialogue État du client *(page 21)*.

- **Chiffrement initial**

  Démarre l'assistant qui va chiffrer tous les fichiers avec le profil du chiffrement chargé. Retrouvez plus de renseignements à la section Chiffrement initial et chiffrement explicite *(page 10)*.

- **Fermer**

  Ferme l'application Utilisateur SafeGuard LAN Crypt.

- **À propos de**

  Affiche les informations sur la version SafeGuard LAN Crypt actuellement installée.

Note: L'option **Fermer** ferme uniquement l'application de l'utilisateur de SafeGuard LAN Crypt. Toutefois, SafeGuard LAN Crypt ne change pas d'état. Par conséquent, le chiffrement/déchiffrement transparent continue. La fermeture de l'application utilisateur ne protège pas les fichiers d'un accès non autorisé (par exemple, lorsque vous n'êtes pas devant votre poste de travail).

4.2 Boîte de dialogue État du client

L'option **État du client** affiche plusieurs onglets fournissant des informations sur les paramètres de chiffrement d'un poste de travail d'un utilisateur. Retrouvez-les ci-dessous :

- **État**

  Cet onglet indique si le profil de l'utilisateur a été chargé et si le chiffrement est actif. Il affiche également des informations détaillées sur le fichier de stratégie (date de création, responsable de la sécurité à l'origine de sa création, etc.).

  Si le profil de l'utilisateur a été chargé, le chiffrement est également actif. Toutefois, le chiffrement peut également être (temporairement) désactivé pendant le chargement du profil de l'utilisateur. Retrouvez plus de renseignements à la section (Menu de l'utilisateur *(page 20)* sous **Désactivation/Activation du chiffrement**.

- **Paramètres**

  Cet onglet fournit des informations sur les paramètres actuellement appliqués au client. Ces paramètres sont définis de manière centralisée et se rapportent au chiffrement, à l'icône de la barre d'état système et aux paramètres de l'**Assistant de chiffrement initial**. Cet onglet informe également de la possible activation d'un **Chiffrement persistant**, de même que de la disponibilité de commandes de menu sur les ordinateurs clients.

- **Profil**

  Cet onglet affiche les paramètres du profil de l'utilisateur.

- **Certificats**

  Cet onglet affiche des informations sur le certificat de l'utilisateur (émetteur, numéro de série, validité), ainsi que les règles qui s'appliquent au client pour la vérification du certificat.

- **Clés**

  Cet onglet affiche des informations sur toutes les clés disponibles pour le profil actuellement chargé.

- **Règles**

Cet onglet affiche la liste de toutes les règles de chiffrement qui s'appliquent à l'utilisateur actuel. En sélectionnant les cases, vous pouvez aussi afficher les règles d'exclusion et les règles de chiffrement d'autres produits SafeGuard.

- **Non géré**

  Cet onglet affiche des informations sur les applications, les lecteurs et les périphériques non gérés, ainsi que sur les **règles Ignorer** de tous les produits SafeGuard installés.

  SafeGuard LAN Crypt traite par défaut certaines applications en tant qu'applications non gérées. Ces applications figurent également dans cet onglet.

- **Applications**

  Cet onglet présente les programmes exigeant une approche spéciale par SafeGuard LAN Crypt du fait de leur comportement.

  - **Logiciels antivirus**

    Lorsqu'il analyse des fichiers chiffrés, un antivirus a besoin de la clé qui a été utilisée pour leur chiffrement. L'antivirus indiqué par le responsable de sécurité dans cet onglet accède à toutes les clés et peut ainsi vérifier les fichiers chiffrés.

- **API client**

  Cet onglet affiche les paramètres de l'API client et répertorie toutes les applications autorisées à l'utiliser

- **Fournisseurs de confiance**

  Si l'accès à l'API client est limité aux applications signées par les fournisseurs de confiance, ces fournisseurs doivent être enregistrés dans SafeGuard LAN Crypt Administration. Tous les fournisseurs de confiance enregistrés et toutes les informations de certificats correspondants sont répertoriés sur cet onglet.

- Bouton **Exporter**

  Utilisez le bouton **Exporter** pour exporter les paramètres du client actuel dans un fichier XML.

  De cette manière, il est plus facile de fournir les informations de configuration importantes aux équipes du support.

4.3 Extensions de l'Explorateur

Les extensions de l'explorateur SafeGuard LAN Crypt offrent les fonctionnalités suivantes :

- Chiffrement initial des fichiers et des répertoires
- Chiffrement et déchiffrement explicites des fichiers et des répertoires
- Contrôle simple de l'état du chiffrement de vos données

SafeGuard LAN Crypt ajoute les entrées à l'Explorateur Windows. Elles s'affichent dans les menus contextuels des lecteurs, dossiers et fichiers. Un onglet relatif aux fichiers est ajouté à la boîte de dialogue Propriétés de Windows. Ce nouvel onglet contient des informations sur l'état du chiffrement.

Il suffit de cliquer avec le bouton droit de la souris sur un fichier ou un répertoire pour afficher l'option **SafeGuard LAN Crypt** dans son menu contextuel. Des clés de couleurs différentes indiquent le statut de chiffrement du fichier :

- **Clé verte**

  Le fichier est chiffré et l'utilisateur a accès à la clé.

- **Clé rouge**

  Le fichier est chiffré et l'utilisateur n'a pas accès à la clé.

- **Clé grise**

  Une clé grise indique que le fichier est en texte clair (non chiffré) mais devrait être chiffré conformément à la règle de chiffrement présente dans le profil chargé.

- **Clé jaune**

Le fichier est chiffré mais le chiffrement transparent est désactivé.

- **Clé jaune avec point d'interrogation**

  L'utilisateur n'a pas les droits d'accès suffisants et SafeGuard LAN Crypt n'est donc pas en mesure de déterminer l'état du chiffrement.

Note: Pour les fichiers avec un attribut hors ligne (par ex ; les fichiers qui n'existent pas physiquement), le système n'affiche aucun symbole de clé.

Lorsque vous cliquez sur **SafeGuard LAN Crypt** dans le menu contextuel, le système affiche un sous-menu contenant des options supplémentaires. Ces options varient selon qu'un fichier ou un répertoire a été sélectionné et en fonction du statut de chiffrement du fichier.

Note: Les symboles de clé sont également ajoutés au dossiers dans l'Explorateur Windows. Des clés de couleurs différentes indiquent le statut de chiffrement du fichier :

- **Clé verte**

  Le fichier est chiffré et l'utilisateur a accès à la clé.

- **Clé rouge**

  Le fichier est chiffré et l'utilisateur n'a pas accès à la clé.

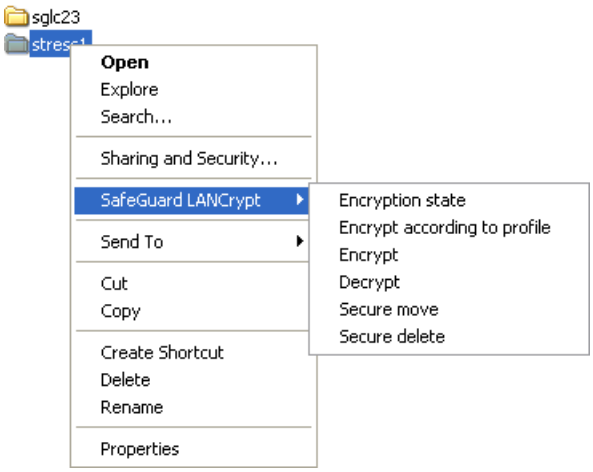
- **Clé grise**

  Une clé grise indique que le fichier est en texte clair (non chiffré) mais devrait être chiffré conformément à la règle de chiffrement présente dans le profil chargé.

- **Clé jaune avec point d'interrogation**

  L'utilisateur n'a pas les droits d'accès suffisants et SafeGuard LAN Crypt n'est donc pas en mesure de déterminer l'état du chiffrement.

Ce menu peut afficher les options suivantes :



4.3.1 Options de menu pour les répertoires

- **État du chiffrement**

  Cette option affiche la liste de tous les fichiers de ce répertoire et leur état de chiffrement (clés de couleur). L'affichage est limité aux fichiers du premier niveau du répertoire. Pour afficher les fichiers d'un sous-répertoire, vous devez ouvrir ce sous-répertoire. Dans l'Explorateur, les dossiers pour lesquels une règle de chiffrement existe sont identifiés par leur icône en forme de clé.

- **Chiffrer selon profil**

Cette option chiffre tous les fichiers dans le répertoire en fonction du profil de chiffrement chargé. Les sous-répertoires avec une règle de chiffrement sont également inclus dans le chiffrement. Une barre de progression vous indique combien de temps le chiffrement initial va durer. Vous pouvez également consulter le nombre de fichiers du dossier et la façon dont ils ont déjà été chiffrés. Vous pouvez également afficher le chemin du fichier qui est en cours de chiffrement.

- **Chiffrer**

  Cette option chiffre tous les fichiers d'un répertoire en utilisant une clé présente dans le profil de chiffrement activé. Une liste des clés disponibles est affichée. Vous y sélectionnez la clé à utiliser pour chiffrer tous les fichiers.

- **Déchiffrer**

  Cette option déchiffre tous les fichiers du premier niveau du répertoire. Par conséquent, toutes les clés concernées doivent être disponibles dans le profil de chiffrement activé. Si une clé manque, les fichiers utilisant cette clé restent chiffrés.

- **Déplacement sécurisé**

  Lors du déplacement d'un dossier avec SafeGuard LAN Crypt, les fichiers dans ce dossier sont chiffrés, déchiffrés ou chiffrés de nouveau dans le nouvel emplacement conformément aux règles de chiffrement appliquées. Les fichiers sources sont effacés après leur déplacement.

- **Suppression sécurisée**

  Cette option remplace les emplacements de stockage à plusieurs reprises. Il est impossible de restaurer ces fichiers via la Corbeille de Windows.

4.3.2 Options du menu pour les fichiers individuels

- **État du chiffrement**

  Cette option affiche l'état du chiffrement du fichier. Pour les fichiers chiffrés, une fenêtre d'information indique la clé utilisée, ainsi que des informations concernant les droits d'utilisation de cette clé.

  Si un autre utilisateur est connecté, mais n'est pas autorisé à utiliser cette clé, le GUID s'affiche dans la zone d'information à la place du nom de clé.

  Les fichiers chiffrés sont identifiés par une petite icône grise dans l'Explorateur. Si l'utilisateur clique sur **Options des dossiers > Afficher**, il peut indiquer si l'état du chiffrement de fichier et l'état du chiffrement de dossier doivent être affichés pour son profil. Les modifications apportées à ces paramètres ne deviennent effectives que lorsque vous connectez de nouveau.

- **Chiffrer selon profil**

  Cette option permet de chiffrer un fichier en fonction du profil de chiffrement actuellement chargé. Cette entrée ne s'affiche dans le menu contextuel que si l'état de chiffrement d'un fichier ne correspond pas au profil de chiffrement.

- **Chiffrer**

  Cette option chiffre le fichier sélectionné. Une liste des clés disponibles est affichée. Vous y sélectionnez la clé à utiliser pour le chiffrement.

- **Déchiffrer**

  Cette option déchiffre le fichier sélectionné. La clé correcte doit être disponible dans le profil de chiffrement activé, sinon le fichier reste chiffré.

- **Déplacement sécurisé**

  Cette option chiffre, déchiffre ou chiffre de nouveau le fichier sélectionné en fonction des règles de chiffrement chargées lorsque les fichiers sont déplacés dans un nouvel emplacement. Le fichier source est effacé après son déplacement.

- **Suppression sécurisée**

  Cette option remplace les emplacements de stockage du fichier sélectionné à plusieurs reprises. Il est impossible de restaurer ce fichier via la Corbeille de Windows.

Note: Les règles de chiffrement actives sont toujours prioritaires. Si l'utilisateur essaye de chiffrer/déchiffrer les fichiers pour lesquels la règle de chiffrement définie est différente, sa commande n'est pas exécutée et un message d'erreur apparaît.

Les situations suivantes entraînent l'apparition d'un message d'erreur lorsqu'un utilisateur essaye de chiffrer les fichiers à l'aide des options de menu :

- Le répertoire contient des fichiers qui sont chiffrés avec une clé inconnue.
- L'utilisateur essaie de chiffrer/déchiffrer un fichier en contradiction avec la règle de chiffrement (par exemple, en utilisant une clé différente de celle sélectionnée dans la règle de chiffrement).

4.3.3 Informations de chiffrement

La page **Propriétés** de Windows comprend un onglet supplémentaire **Statut du chiffrement**. Cet onglet affiche des informations sur le fichier chiffré.

5 Terminal Server

Cette version de SafeGuard LAN Crypt est compatible avec les serveurs Windows Terminal Server et Citrix Terminal Server. Retrouvez plus de renseignement sur les versions compatibles dans les Notes de publication de SafeGuard LAN Crypt.

5.1 Pare-feu

Suite à la connexion de l'utilisateur, SafeGuard LAN Crypt essaye de charger le profil d'utilisateur SafeGuard LAN Crypt. Il vérifie simultanément l'utilisateur et le certificat (M)SO. Si les certificats contiennent un "point de distribution CRL" et qu'aucun CRL valide n'est présent dans le système, Windows essaye d'importer le CRL à partir d'une adresse spécifiée. Si un pare-feu est installé, un message apparaît vous indiquant qu'un programme (loadprof.exe) essaye d'établir une connexion à Internet.

5.2 Installation sur un environnement Terminal Server

En général, la procédure d'installation doit être effectuée de la même manière qu'elle est effectuée sur les environnements sans Terminal Server. Retrouvez plus de renseignements à la section Installation et mise à niveau *(page 27)*.

Pour une installation sur un Terminal Server, utilisez le package d'installation sglcts.msi ou sglcts_x64.msi.

Note:

- Lors de l'installation sur un Terminal Server, veuillez utiliser une session de connexion locale avec les droits administratifs pour installer SafeGuard LAN Crypt.
- Si vous utilisez Citrix Presentation Server ou Citrix XenApp, veuillez les installer avant d'installer SafeGuard LAN Crypt.

5.3 Restrictions

Citrix

- L'utilisation du chiffrement avec la redirection de lecteurs du client Citrix n'est pas prise en charge.

- Les applications en flux de Citrix ne sont pas prises en charge.

6 Installation et mise à niveau

Note: L'installation de SafeGuard LAN Crypt requiert la détention de privilèges d'administrateur Windows. Pour procéder à la mise à niveau à partir d'anciennes versions, il vous suffit simplement d'installer la nouvelle version du client.

1. Cliquez deux fois sur l'un des fichiers .msi dans le répertoire d'installation de votre package d'installation décompressé.
   a. sglc_x64.msi pour une installation sur un système d'exploitation 64 bits ou
   b. sglc.msi pour une installation sur un système d'exploitation 32 bits.

2. Cliquez sur **Suivant**.
   La boîte de dialogue **Contrat de licence** s'affiche.

3. Sélectionnez **J'accepte les termes du contrat de licence** dans le boîte de dialogue **Contrat de licence**. Si vous ne les acceptez pas, vous ne pourrez pas installer SafeGuard LAN Crypt !

4. Cliquez sur **Suivant**.
   La boîte de dialogue **Dossier de destination** apparaît.

5. Sélectionnez l'endroit où vous voulez installer SafeGuard LAN Crypt.

6. Cliquez sur **Suivant**.
   La boîte de dialogue **Sélectionner le type d'installation** s'affiche.

7. Cette boîte de dialogue vous permet de sélectionner les composants de SafeGuard LAN Crypt à installer.
   a. **Standard** : installe les fonctions les plus usuelles de SafeGuard LAN Crypt Client
   b. **Complète** : Installation complète du client
   c. **Personnalisée** : Permet à l'utilisateur de sélectionner les différents composants.

8. Sélectionnez **Personnalisée**, puis cliquez sur **Suivant**.
   Les composants suivants peuvent être installés :
   - **Installation du client**
     - **Extensions du shell**

       Installe les extensions de l'explorateur SafeGuard LAN Crypt.

       SafeGuard LAN Crypt ajoute les entrées à l'Explorateur Windows pour réaliser le chiffrement initial, ainsi que le chiffrement/déchiffrement explicite des fichiers et des répertoires. Il facilite la vérification de l'état de chiffrement de vos données. Ces entrées apparaissent dans les menus contextuels des lecteurs, répertoires et fichiers. La page Propriétés de Windows comprend un onglet supplémentaire nommé Informations de chiffrement.

     - **Applications utilisateur**

       Installe l'application de l'utilisateur de SafeGuard LAN Crypt. Retrouvez plus de renseignements à la section Application de l'utilisateur *(page 20)*.

     - **API client**

       Utilisé pour accéder à la fonctionnalité de chiffrement de fichiers de SafeGuard via une API.

       Note: Vous devez impérativement installer l'API client pour permettre aux produits de protection contre la fuite de données d'accéder aux données à l'aide de l'API de SafeGuard LAN Crypt Client.

9. Sélectionnez les composants à installer et cliquez sur **Suivant**.

10. Vérifiez de nouveau vos entrées, puis cliquez sur **Suivant** pour commencer l'installation.

11. Lorsque l'installation a réussi, une boîte de dialogue s'affiche. Cliquez sur le bouton **Terminer** pour terminer le processus d'installation.

    Note: Redémarrez le système pour charger le pilote et activer tous les paramètres.

6.1 Installation automatique

L'installation automatique signifie que vous pouvez installer SafeGuard LAN Crypt automatiquement sur un grand nombre d'ordinateurs.

Le répertoire Install de votre CD-ROM d'installation inclut le fichier .msi nécessaire à l'installation des composants du client.

6.2 Composants à installer

Les listes suivantes affichent tous les composants à installer et leur configuration pour une installation automatique.

Les mots-clés (en gras, police Courier) représentent la manière de désigner les composants dans ADDLOCAL= lorsque vous procédez à une installation automatique. Respectez les majuscules et minuscules pendant la saisie des noms des composants.

ADDLOCAL=**ALL** installe tous les composants disponibles.

Extensions du shell - **ShellExtensions**

Application utilisateur - **UserApplication**

API Client - **ClientAPI**

6.3 Syntaxe de la ligne de commande

Pour procéder à une installation automatique, vous devez exécuter **msiexec** avec des paramètres spécifiques.

Paramètres obligatoires :

/I

Indique quel module d'installation doit être installé.

/QN

Installation sans interaction de l'utilisateur (installation automatique)

Nom du fichier .msi :

sglc.msi pour systèmes d'exploitation 32 bits

sglc_x64.msi pour systèmes d'exploitation 64 bits

Syntaxe

msiexec /i <chemin>\sglc.msi | sglc_x64.msi /qn ADDLOCAL=<composant1>,<composant2>,...

Paramètres optionnels

/Lvx* <chemin + nom de fichier>

Journalise toute la procédure d'installation à l'emplacement indiqué sous <chemin + nom de fichier>.

NOOVERLAY=1

Désactive les icônes superposées pour les fichiers et dossiers.

Note: Les utilisateurs peuvent activer les icônes superposées après l'installation. Si l'utilisateur clique sur **Options des dossiers > Afficher**, il peut indiquer si l'état du chiffrement de fichier et l'état du chiffrement de dossier doivent être affichés

pour son profil. Les modifications apportées à ces paramètres ne deviennent effectives que lorsque vous connectez de nouveau.

EXEMPLE :

msiexec /i C:\Install\sglc.msi /qn ADDLOCAL=ALL

Une installation complète de SafeGuard LAN Crypt (32 bits) est effectuée. Le programme est installé dans le répertoire d'installation par défaut (<Lecteur système>:\Program Files\Sophos). Le fichier msi se trouve dans le répertoire Install du lecteur C.

6.4 Suppression de SafeGuard LAN Crypt Client

Vous pouvez uniquement supprimer SafeGuard LAN Crypt Client si vous disposez des privilèges d'administrateur Windows.

Dans le **Panneau de configuration** /**Ajouter/supprimer des programmes**, procédez à la suppression du client et redémarrez votre ordinateur pour appliquer ces modifications.

Note: Les fichiers chiffrés ne peuvent plus être déchiffrés une fois que SafeGuard LAN Crypt Client a été supprimé.

Note: Ne réinstallez pas SafeGuard LAN Crypt Client immédiatement après l'avoir supprimé. Veuillez d'abord redémarrer l'ordinateur une fois avant de pouvoir le réinstaller.

7 Support technique

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

- Rendez-vous sur la base de connaissances du support de Sophos sur https://support.conpal.de .
- Téléchargez la documentation des produits sur

  https://docs.lancrypt.com/fr/client/sglc_397_hfra.pdf

  https://docs.lancrypt.com/fr/admin/sglc_397_ahfra.pdf
- Ouvrez un incident support sur support@conpal.de.

8 Mentions légales