

Le chiffrement intelligent des fichiers

Utimaco Safeware

SafeGuard® LAN Crypt

Version 3.70

Client

Windows® XP SP2

Windows® XP SP3

Windows® Vista SP1

Windows Server 2003 R2 SP2 32bit

utimaco[®]
s a f e w a r e

a member of the Sophos Group

CONTENU

CHAPITRE 1	Présentation	1
	1.1 Qu'est-ce que SafeGuard LAN Crypt ?	1
	1.2 Protection des données avec SafeGuard LAN Crypt	2
	1.3 Chiffrement transparent	4
	1.3.1 Accès aux données chiffrées	5
	1.3.2 Renommage ou déplacement des répertoires	5
	1.3.3 Déchiffrement explicite des fichiers	6
	1.3.4 Suppression des fichiers chiffrés - Corbeille	7
	1.3.5 Fichiers/répertoires exclus du chiffrement	7
	1.3.6 SafeGuard LAN Crypt et SafeGuard Enterprise.....	7
	1.3.7 Chargement du fichier de stratégie	8
	1.4 Configuration requise.....	11
	1.4.1 Plates-formes	11
	1.4.2 Pare-feu	11
	1.5 SafeGuard LAN Crypt et SafeGuard Enterprise	11
CHAPITRE 2	Installation	12
	2.1 Installation automatique.....	14
	2.1.1 Composants à installer	14
	2.1.2 Syntaxe de la ligne de commande	14
CHAPITRE 3	Désinstallation	16
CHAPITRE 4	Serveur de terminal	17
	4.1 Configuration requise.....	17
	4.1.1 Plates-formes	17
	4.1.2 Pare-feu	17
	4.2 Installation	18
	4.3 Restrictions	18

CONTENU

CHAPITRE 5	Application utilisateur SafeGuard LAN Crypt	19
	5.1 Connexion à SafeGuard LAN Crypt.....	19
	5.1.1 Connexion avec clé cryptographique	19
	5.2 Certificats.....	20
	5.3 Application utilisateur	21
	5.3.1 Menu Utilisateur	22
	5.3.2 Boîte de dialogue Statut client	24
	5.4 Chiffrement initial et chiffrement explicite	26
	5.4.1 Assistant chiffrement initial.....	26
	5.4.2 Chiffrement initial en mode automatique	31
	5.5 Extensions de l'explorateur	34
	5.5.1 Informations de chiffrement	37
	5.6 Désactivation/Activation Chiffrement transparent	38
	5.6.1 Outils de chiffrement transparent et de compression des fichiers	39
	5.7 Compatibilité avec les versions précédentes	40
	5.8 Désinstallation de la version Client.....	41
	5.9 Annexe : Messages d'erreur affichés lors du chargement du profil ..	42
CHAPITRE 6	Copyright.....	44
CHAPITRE 7	Assistance technique.....	45

1 Présentation

1.1 Qu'est-ce que SafeGuard LAN Crypt ?

SafeGuard LAN Crypt permet un chiffrement transparent des fichiers. Il a été conçu pour faciliter l'échange des fichiers entre des groupes d'utilisateurs de confiance au sein d'une grande entreprise.

À l'inverse des autres produits de chiffrement de fichiers, SafeGuard LAN Crypt fonctionne sans nécessiter d'interaction de l'utilisateur, en jouant le rôle d'un responsable de sécurité qui peut également restreindre les droits d'accès de l'administrateur système par des fichiers chiffrés avec LAN Crypt. Un responsable de sécurité principal peut déléguer le droit d'administrer SafeGuard LAN Crypt. Il est ainsi possible d'établir une hiérarchie parmi les responsables de sécurité pour répondre aux exigences de sécurité de toutes les entreprises.

Chaque fois qu'un utilisateur déplace un fichier dans un répertoire sécurisé, ce fichier est chiffré dans son ordinateur. De même, chaque fois qu'un autre utilisateur sécurisé 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. Ce fichier peut être modifié et rechiffré sur cet ordinateur avant de le transférer à nouveau vers le répertoire chiffré.

Les fichiers chiffrés ne sont pas assignés à des utilisateurs individuels. Tout utilisateur qui possède la bonne clé peut accéder à 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.

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 ils ne pourront pas lire sans autorisation SafeGuard LAN Crypt.

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'organisation par ses employés.

Si vous devez protéger votre propriété intellectuelle, stockée sur fichiers, d'un accès non autorisé via le réseau local, sur des serveurs de fichiers, des disques locaux ou même des supports amovibles, SafeGuard LAN Crypt est le produit idéal.

1.2 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 et les processus de chiffrement et de déchiffrement sont exécutés dans la mémoire RAM du poste de travail client. Il n'est pas nécessaire d'installer un logiciel de sécurité spécial sur le serveur de fichiers lui-même.

SafeGuard LAN Crypt présente à ce niveau un avantage particulier : aucun accès réseau n'est nécessaire pour accéder au serveur de sécurité dans la mesure où tous les utilisateurs se voient attribuer un profil de sécurité via les informations de chiffrement stockées dans le registre Windows. En conséquence, même les fichiers chiffrés stockés en externe (sur des supports tels que des CD-ROM) peuvent être traités en toute transparence.

Les fichiers de stratégie contiennent l'ensemble des règles, droits d'accès et clés nécessaires à un chiffrement transparent. Avant que les utilisateurs ne puissent chiffrer/déchiffrer les données à l'aide du logiciel SafeGuard LAN Crypt installé sur le poste de travail client, ils doivent pouvoir accéder au fichier de stratégie. Ce fichier est sécurisé par l'intermédiaire d'un certificat. Pour accéder au fichier de stratégie, l'utilisateur doit disposer de la clé privée du certificat approprié.

Toutes les tâches de chiffrement/déchiffrement sont exécutées de manière transparente sur le poste de travail client avec le minimum d'interaction de l'utilisateur.

SafeGuard LAN Crypt permet d'organiser les utilisateurs de confiance en plusieurs groupes du même type. Il s'agit de définir des droits d'accès différents aux répertoires et aux fichiers. Ces droits sont regroupés dans des profils de chiffrement destinés aux utilisateurs. L'utilisateur peut accéder au fichier de stratégie contenant le profil de chiffrement s'il dispose de la clé privée affectée au certificat.

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.

Du fait que les profils de chiffrement sont répartis via des fichiers de stratégie, toutes les formes organisationnelles peuvent être cartographiées 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.

SafeGuard LAN Crypt Administration et Administration Windows

Un ordinateur d'administration distinct est utilisé pour configurer SafeGuard LAN Crypt et gérer les profils de chiffrement. Pour établir une distinction nette entre l'administration Windows et l'administration SafeGuard LAN Crypt, il convient de définir le rôle de responsable de sécurité. Le responsable de sécurité définit les profils de chiffrement des fichiers de stratégie afin d'indiquer quelles données chiffrées doivent être stockées dans des répertoires particuliers et qui est autorisé à accéder à ces données. Une fois les fichiers de stratégie créés sur la station d'administration, le responsable de sécurité les déploie.

Un outil Windows standard, la console de gestion MMC de Microsoft, sert à administrer SafeGuard LAN Crypt. L'interface utilisateur de SafeGuard LAN Crypt Administration comprend les composants logiciels enfichables pour la console MMC. SafeGuard LAN Crypt Administration stocke la plupart des objets à administrer (données utilisateur, clés, chemins de chiffrement, etc.) dans leurs propres bases de données.

L'utilisation des bases de données présente deux avantages notables par rapport aux outils Windows du type Active Directory :

- Il est possible de maintenir strictement séparées l'administration du système et l'administration de la sécurité. Cela s'explique par le fait que SafeGuard LAN Crypt utilise une base de données dédiée et se révèle totalement indépendant de l'administration du système. La base de données SafeGuard LAN Crypt est alors chiffrée, puis protégée contre tout accès non autorisé. En outre, cette base de données prévient les changements non intentionnels du système SafeGuard LAN Crypt (par ex. si l'administrateur système supprime un objet de sécurité nécessaire).
- D'autre part, il n'est pas toujours judicieux de laisser des personnes, autres que les administrateurs dédiés, modifier la configuration du système. L'assignation d'autorisations d'écriture de données dans le cadre d'une administration de système pose évidemment un véritable problème. Il existe une autre bonne raison justifiant le stockage des données spécifiques à SafeGuard LAN Crypt dans une base de données séparée.

Le chemin des fichiers de stratégie (du point de vue de l'utilisateur) et les autres paramètres non liés à la sécurité sont distribués par les mécanismes du système d'exploitation (par ex. Active Directory ou `ntconfig.pol`, le fichier de configuration central).

Pour offrir la meilleure protection possible, les fonctions SafeGuard Lan Crypt sont divisées en deux parties :

■ **Fonctions d'utilisateur SafeGuard LAN Crypt**

Concernant les données, les fonctions d'utilisateur SafeGuard LAN Crypt intègrent le chiffrement et le déchiffrement des informations. Celles-ci servent aux tâches qui utilisent SafeGuard LAN Crypt au quotidien. Dès qu'un utilisateur est autorisé à accéder aux informations de chiffrement, les fichiers sont chiffrés et déchiffrés de manière transparente. Aucune autre interaction utilisateur n'est requise. Par ailleurs, SafeGuard LAN Crypt possède un large éventail de fonctions d'affichage permettant aux utilisateurs de visualiser « leur » profil de chiffrement.

■ **Fonctions de responsable de sécurité SafeGuard LAN Crypt**

SafeGuard LAN Crypt Administration possède des fonctions réservées aux responsables de sécurité. Détenir un certificat de responsable de sécurité est une condition préalable à la création de profils de chiffrement et à l'administration des profils de chiffrement existants. Le composant SafeGuard LAN Crypt Administration peut être installé séparément de l'application de l'utilisateur du fait que seul un responsable de sécurité doit pouvoir y accéder. Lorsque vous installez SafeGuard LAN Crypt, vous pouvez sélectionner les composants souhaités (administration et/ou utilisateur).

1.3 Chiffrement transparent

Pour l'utilisateur, le chiffrement transparent signifie que toutes les données stockées sous forme chiffrée (dans des répertoires ou lecteurs sécurisés) sont automatiquement déchiffrées dans la mémoire principale lorsqu'elles sont ouvertes par une application. Lorsque le fichier est enregistré, il est automatiquement chiffré à nouveau.

- 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. Vous pouvez naturellement définir des règles de chiffrement différentes pour des extensions ou des noms de fichiers différents dans le même répertoire. Le chiffrement est régi uniquement par les règles de chiffrement, il ne dépend pas des répertoires !
- 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).
- Lorsque l'utilisateur copie ou déplace des fichiers chiffrés vers un emplacement où ne s'applique plus la règle de chiffrement en cours, le système effectue automatiquement leur déchiffrement.
- Lorsque l'administrateur a activé le *chiffrement persistant*, les fichiers restent chiffrés même s'ils sont , dans l'Explorateur Windows, vers un emplacement qui n'est régi par aucune clé de chiffrement. Cette fonction n'a aucun effet lorsque les fichiers sont copiés en dehors de l'Explorateur Windows (par exemple, à partir de la ligne de commande). Dans ce cas, les fichiers sont copiés en clair.
- 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.
- 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.

REMARQUE :

SafeGuard LAN Crypt ne procède pas au chiffrement des fichiers pour lesquels la **compression** 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 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 sécurité définit si un utilisateur est habilité à décompresser les fichiers compressés ou à déchiffrer les fichiers EFS chiffrés, si nécessaire.

1.3.1 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.

REMARQUE :

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 » ([voir « Programmes possédant un comportement spécifique à l'enregistrement des fichiers », page 25](#)).

1.3.2 Renommage ou déplacement des répertoires

Pour des raisons de performance, SafeGuard Lan Crypt ne modifie pas le statut de chiffrement lorsque des répertoires entiers 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.

Les fichiers chiffrés dans ces dossiers restent chiffrés dans leur nouvel emplacement (avec le nouveau nom du répertoire). 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 sur un support de mémoire USB pour lequel aucune règle de chiffrement n'est mise en œuvre. Si le *chiffrement persistant* n'est pas actif, les fichiers sont déchiffrés lorsqu'ils sont déplacés vers ces types de support, comme avant. Cependant, si l'administrateur a activé la fonction de *chiffrement persistant*, ces fichiers resteront chiffrés.

Le *chiffrement persistant* n'a aucun effet lorsque les fichiers sont copiés ou déplacés en dehors de l'Explorateur Windows (par exemple, à partir de la ligne de commande). Dans ce cas, les fichiers sont copiés en clair.

Déplacement vers SafeGuard LAN Crypt

Cependant, SafeGuard LAN Crypt prend en charge le déplacement sécurisé des fichiers et des répertoires. Lorsque vous déplacez les fichiers vers SafeGuard LAN Crypt, les fichiers et répertoires sont chiffrés, déchiffrés et chiffrés à nouveau en fonction des 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 **Déplacer via SGLC** dans le menu contextuel de l'Explorateur Windows. Une boîte de dialogue s'affiche, dans laquelle vous indiquez les fichiers à déplacer.

1.3.3 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* n'est pas actif (pour plus de détails).

REMARQUE :

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. Le fichier LisezMoi fourni avec la version SGLC Client vous donne des informations plus spécifiques sur les problèmes couramment rencontrés avec les utilitaires antivirus.

1.3.4 Suppression des fichiers chiffrés - Corbeille

Si votre profil de chiffrement est chargé, vous pouvez supprimer tout fichier chiffré dont vous possédez la clé.

REMARQUE :

La suppression des fichiers signifie que vous les envoyez dans la Corbeille Windows. Pour offrir le niveau de sécurité le plus élevé, les fichiers chiffrés par SafeGuard Lan Crypt restent chiffrés dans la Corbeille. La clé servant à chiffrer un fichier doit être disponible dans le profil activé avant de supprimer définitivement le fichier. Si la clé est indisponible, un message d'erreur s'affichera et vous ne pourrez pas effacer ces fichiers du système.

Dans certains cas, les règles de chiffrement ont pu être modifiées après l'envoi du fichier dans la Corbeille. Dans ce cas, l'ancienne clé doit être disponible dans le profil activé avant de supprimer définitivement le fichier.

Si les fichiers chiffrés sont envoyés dans la Corbeille et si l'utilisateur se déconnecte puis accède à l'un de ces fichiers dans la Corbeille, il sera impossible de restaurer les fichiers. Cela s'explique par le fait que SafeGuard LAN Crypt les supprime automatiquement de la Corbeille lorsque l'utilisateur se déconnecte.

1.3.5 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

1.3.6 SafeGuard LAN Crypt et SafeGuard Enterprise

Cette version de SafeGuard LAN Crypt peut être utilisée parallèlement à SafeGuard Enterprise. Par exemple, l'application SafeGuard Data Exchange peut être utilisée pour chiffrer l'ensemble des données contenues sur les supports amovibles, et l'application SafeGuard LAN Crypt peut être utilisée pour chiffrer l'ensemble des fichiers des partages réseau.

La boîte de dialogue *Statut client* de SafeGuard LAN affiche toutes les règles de chiffrement valides sur l'ordinateur. En général, les règles de SafeGuard Enterprise Data Exchange sont appliquées avant celles de SafeGuard LAN Crypt. Le classement des priorités peut être modifié.

Nouveau chiffrement des fichiers chiffrés par SafeGuard Enterprise Data Exchange

L'Assistant de chiffrement initial permet de chiffrer à nouveau les fichiers qui ont été chiffrés à l'aide de SafeGuard Data Exchange, mais la règle de chiffrement de SafeGuard Enterprise ne s'applique plus. De tels fichiers existent par exemple si la règle de chiffrement a été supprimée, mais que les fichiers n'ont pas été déchiffrés de façon explicite. Dans ce cas, l'option **Fichiers chiffrés à nouveau selon le profil** peut être activée dans l'Assistant de chiffrement initial, qui chiffre à nouveau ces fichiers en fonction des règles de chiffrement de SafeGuard LAN Crypt.

1.3.7 Chargement du fichier de stratégie

Comportement standard 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 ensuite 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). Si un nouveau fichier de stratégie y figure, le profil en cache de l'utilisateur sera mis à jour.

Cette approche a pour avantage que 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 le lecteur réseau 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.

REMARQUE :

SafeGuard LAN Crypt vérifie les certificats de l'utilisateur et du responsable de sécurité (principal). S'ils contiennent un « point de distribution de liste de révocation de certificats (CRL) » et qu'aucune CRL valide n'existe sur le système, Windows tente d'importer la CRL à partir de l'adresse spécifiée. Si un pare-feu est installé, un message peut s'afficher et indiquer qu'un programme (loadprof.exe) tente d'établir une connexion à Internet. Ce message peut également s'afficher dans certains cas à la suite du téléchargement du profil utilisateur.

Comportement défini par les responsables de sécurité

Le responsable de sécurité peut modifier le comportement standard à l'aide des paramètres utilisés de manière centrale. Les responsables de sécurité peuvent définir la durée de validité des stratégies mises en cache sur les ordinateurs clients. En outre, ils peuvent également définir les intervalles de mise à jour des fichiers de sécurité. Les paramètres définis par le responsable de sécurité s'affichent dans l'onglet *Profil* de la boîte de dialogue *Statut client* (voir « [Boîte de dialogue Statut client](#) », page 24).

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.

D'un côté, en indiquant la durée du stockage en mémoire cache, vous pouvez vous assurer que les ordinateurs clients reçoivent à intervalles réguliers des fichiers de stratégie mis à jour et que les utilisateurs travaillent à tout moment avec des stratégies actualisées. D'un autre côté, vous évitez aux utilisateurs de travailler indéfiniment avec les mêmes fichiers de stratégie. Un utilisateur peut en effet travailler indéfiniment avec une version mise en cache du fichier de stratégie si cette option est définie sur *non configurée*.

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 SafeGuard LAN Crypt ([voir « Charger les règles de chiffrement/ Mettre à jour les règles de chiffrement », page 22](#)).

Les fichiers de stratégie ne sont pas mis en mémoire cache

Les responsables de sécurité peuvent également indiquer que le fichier de stratégie ne sera pas mis en mémoire cache. Cela signifie que les utilisateurs reçoivent leurs profils utilisateurs 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.

Clients de la version 3.12

Cette fonctionnalité n'est pas disponible dans les versions client précédentes. Toutefois, il est tout à fait possible d'utiliser les clients de la version 3.12 avec SafeGuard LAN Crypt Administration version 3.60. Au moment du chargement des fichiers de stratégie, les clients de ce type adoptent le comportement suivant :

Le client tente toujours de charger le fichier de stratégie depuis l'emplacement de fichier indiqué. Si cet emplacement n'est pas accessible, une version mise en cache du fichier de stratégie est chargée. Ce fichier de stratégie mis en cache ne possède aucune date d'expiration et n'est pas mis à jour tant qu'une version plus récente n'est pas correctement chargée. En outre, il est impossible de définir un intervalle de mise à jour pour ces stratégies. Les fichiers de stratégie mis en cache restent valides tant que l'emplacement indiqué des fichiers de stratégie est accessible et le fichier de stratégie mis en cache est remplacé par un fichier de stratégie provenant de cet emplacement.

1.4 Configuration requise

1.4.1 Plates-formes

SafeGuard LAN Crypt Client est compatible avec les systèmes d'exploitation suivants :

- Windows XP SP2 32 bits
- Windows XP SP3 32 bits
- Windows Vista Édition Intégrale SP1 32 bits
- Windows Vista Entreprise SP1 32 bits
- Windows Vista Professionnel SP1 32 bits

1.4.2 Pare-feu

Une fois qu'un utilisateur s'est connecté, SafeGuard LAN Crypt tente de charger le profil utilisateur SafeGuard LAN Crypt. Parallèlement, il vérifie le certificat utilisateur et le certificat du responsable de sécurité principal. S'ils contiennent un « point de distribution CRL » et qu'aucune CRL valide n'existe sur le système, Windows tente d'importer la CRL à partir de l'adresse spécifiée. Si un pare-feu est installé, un message peut s'afficher et indiquer qu'un programme (loadprof.exe) tente d'établir une connexion à Internet.

1.5 SafeGuard LAN Crypt et SafeGuard Enterprise

- SafeGuard LAN Crypt 3.7x et SafeGuard Enterprise 5.35.4 ou supérieur peuvent coexister sur un même ordinateur et sont complètement compatibles.
- Les versions antérieures à la version 3.7x de SafeGuard LAN Crypt et SafeGuard Enterprise 5.4x ne peuvent pas coexister sur un même ordinateur.
Si vous essayez d'installer SafeGuard Enterprise 5.4x sur un ordinateur sur lequel la version 3.6x ou une version antérieure de SafeGuard LAN Crypt est installée, l'installation est annulée et un message d'erreur correspondant s'affiche.
- SafeGuard LAN Crypt 3.7x et une version antérieure à la version 5.35.4 de SafeGuard Enterprise ne peuvent pas coexister sur un même ordinateur.
Si vous essayez d'installer SafeGuard LAN Crypt 3.7x sur un ordinateur sur lequel une version antérieure à la version 5.35.4 de SafeGuard Enterprise est installée, l'installation est annulée et un message d'erreur correspondant s'affiche.

2 Installation

REMARQUE :

L'installation de SafeGuard LAN Crypt requiert la détention de privilèges d'administrateur Windows.

1. La procédure d'installation est lancée dès que vous insérez le CD dans le lecteur de CD-ROM (sinon, lancez le fichier **.msi** dans le répertoire `Install` du CD-ROM d'installation). L'Assistant d'installation vous guide pendant la procédure simple d'installation de SafeGuard LAN Crypt. Cliquez sur **Suivant**.
2. La boîte de dialogue *Contrat de licence* s'affiche. Sélectionnez **J'accepte les termes du contrat de licence** dans la boîte de dialogue *Contrat de licence*. Si vous ne les acceptez pas, vous ne pourrez pas installer SafeGuard LAN Crypt ! Cliquez sur **Suivant**.
3. La boîte de dialogue *Dossier destination* s'affiche. Choisissez où vous voulez installer SafeGuard LAN Crypt. Cliquez sur **Suivant**.
4. La boîte de dialogue *Sélectionner le type d'installation* s'affiche. Vous pouvez sélectionner quels composants SafeGuard Lan Crypt doivent être installés.
 - **Standard :**
Installe les fonctions les plus courantes de SafeGuard LAN Crypt Client
 - **Complète :**
Installation complète du client
 - **Personnalisée :**
Permet à l'utilisateur de sélectionner les différents composants.
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 du statut 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 *Informations de chiffrement*.

■ **Application utilisateur**

Installe l'application utilisateur de SafeGuard LAN Crypt. Une icône dans la barre des tâches Windows représente l'application utilisateur de SafeGuard LAN Crypt. Une icône en forme de clé présente l'état de SafeGuard LAN Crypt. Cette application fournit aux utilisateurs les fonctions suivantes (accessibles avec le bouton droit de la souris) :

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

■ **API client**

API permettant d'automatiser les tâches sur le client LAN Crypt

5. Sélectionnez les composants à installer et cliquez sur **Suivant**.
6. Vérifiez vos entrées, puis cliquez sur **Suivant** pour procéder à l'installation.
7. Lorsque l'installation réussit, une boîte de dialogue s'affiche. Cliquez sur **Terminer** pour mettre fin au processus d'installation.

REMARQUE :

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

2.1 Installation automatique

Si vous optez pour une installation automatique, vous pouvez installer SafeGuard LAN Crypt automatiquement sur un grand nombre d'ordinateurs. Le répertoire `Install` du CD d'installation propose le fichier `sglc.msi` qui sert à l'installation automatique des composants clients.

2.1.1 Composants à installer

La liste suivante affiche 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.

sglc.msi :

`ADDLOCAL=ALL` permet d'installer tous les composants disponibles.

Extensions du shell - **ShellExtensions**

Application utilisateur - **UserApplication**

API client - **ClientAPI**

2.1.2 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`

Syntaxe :

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

Paramètre en option :

`/L* <chemin + nom de fichier>`

Journalise tous les avertissements et messages et messages dans l'emplacement indiqué

à `<chemin + nom de fichier>`.

EXEMPLE :

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

SafeGuard LAN Crypt est installé complètement. Le programme est installé dans le répertoire d'installation par défaut (`<disque système>:\Program Files\Utimaco`). Le fichier `msi` est placé dans le répertoire `Install` du lecteur `C`.

3 Désinstallation

La désinstallation de SafeGuard LAN Crypt Client requiert la détention de privilèges d'administrateur Windows.

Veillez noter que des fichiers chiffrés ne peuvent plus être déchiffrés une fois que SafeGuard LAN Crypt Client a été désinstallé !

ATTENTION :

Ne réinstallez pas SafeGuard LAN Crypt 3.70 Client immédiatement après l'avoir désinstallé.
Vous devez redémarrer l'ordinateur au moins une fois avant de procéder à une nouvelle installation.

4 Serveur de terminal

Cette version de SafeGuard LAN Crypt prend en charge les serveurs Windows Terminal Server et Citrix Terminal Server.

4.1 Configuration requise

4.1.1 Plates-formes

SafeGuard LAN Crypt Client est compatible avec les systèmes d'exploitation suivants :

- Windows Server 2003 R2 SP2 32 bits avec les services Terminal Server
- Citrix Presentation Server 4.5 32 bits avec Hotfix Rollup Pack 3 sur Windows Server 2003 R2 SP2 32 bits

4.1.2 Pare-feu

Une fois qu'un utilisateur s'est connecté, Safeguard LAN Crypt tente de charger le profil utilisateur SafeGuard LAN Crypt. Parallèlement, il vérifie le certificat utilisateur et le certificat du responsable de sécurité principal. S'ils contiennent un « point de distribution CRL » et qu'aucune CRL valide n'existe sur le système, Windows tente d'importer la CRL à partir de l'adresse spécifiée. Si un pare-feu est installé, un message peut s'afficher et indiquer qu'un programme (loadprof.exe) tente d'établir une connexion à Internet.

4.2 Installation

En général, la procédure d'installation doit être effectuée de la même façon que dans les environnements dépourvus de serveur de terminal (voir le chapitre *Installation*).

Pour exécuter une installation sur un serveur de terminal, veuillez utiliser le module d'installation `sglcts.msi`.

IMPORTANT :

- Si vous effectuez l'installation sur un serveur de terminal, veuillez utiliser une session de connexion locale avec des droits d'administration pour installer LAN Crypt.
- Si vous utilisez Citrix Presentation Server, installez l'application Presentation Server avant SafeGuard LAN Crypt.

4.3 Restrictions

Citrix

- Le chiffrement associé à Citrix Client Drive Redirection n'est pas pris en charge.
- Les applications de transmission en continu de Citrix ne sont pas prises en charge.

5 Application utilisateur SafeGuard LAN Crypt

Lors des tâches routinières, SafeGuard LAN Crypt ne nécessite pratiquement aucune interaction de l'utilisateur. Un certain nombre d'améliorations ont été apportées au nouveau client SafeGuard LAN, afin de permettre aux utilisateurs de manipuler leurs fichiers de façon plus sûre et plus efficace. Le client SafeGuard LAN procède à un chiffrement et déchiffrement dynamique des données.

5.1 Connexion à SafeGuard LAN Crypt

Lorsque vous vous connectez à SafeGuard LAN Crypt, le profil de chiffrement, stocké dans les fichiers de stratégie, est chargé sur le poste de travail client. Le profil de chiffrement ne pourra être chargé que si l'utilisateur détient le certificat correspondant.

Les profils de chiffrement SafeGuard LAN Crypt sont créés par un responsable de sécurité, conformément à la stratégie de sécurité de l'entreprise, puis sont stockés dans des fichiers de stratégie. Lors de l'ouverture d'une session sur le réseau, les postes clients trouvent l'emplacement de ces fichiers de stratégie. L'administrateur système est chargé de cette configuration. Le chemin des fichiers de stratégie est entré dans la base de registre du poste client. SafeGuard LAN Crypt charge les fichiers de stratégie à partir de ce répertoire et vérifie si l'utilisateur est autorisé à les charger en vérifiant son certificat.

5.1.1 Connexion avec clé cryptographique

Vous pouvez également vous connecter à SafeGuard LAN Crypt en vous aidant d'une clé cryptographique. L'une des conditions préalables à cette méthode de connexion est que le certificat SafeGuard LAN Crypt de l'utilisateur soit enregistré sur la clé cryptographique. Si le certificat utilisateur se trouve sur une clé cryptographique connectée au système, l'utilisateur pourra se connecter.

Lorsque des clés cryptographiques sont utilisées pour la connexion, SafeGuard LAN Crypt peut tenter de charger un fichier de stratégie avant que la clé cryptographique ne soit identifiée par le système d'exploitation.

Dans ce cas, un message s'affiche indiquant que le certificat utilisateur est introuvable, bien que la clé cryptographique soit connectée au système.

L'utilisateur doit charger le fichier de stratégie manuellement via l'application utilisateur. Pour cela, il accède à la barre d'outils, puis sélectionne > Charger les règles de chiffrement. De cette façon, la clé cryptographique sera identifiée et l'utilisateur pourra se connecter.

5.2 Certificats

Avant qu'un utilisateur puisse accéder à son profil de chiffrement, le certificat correspondant doit être disponible sur le poste de l'utilisateur. Le responsable de sécurité est chargé de distribuer 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 également 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 PIN du fichier de clés PKCS#12.

REMARQUE :

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.

REMARQUE :

Lorsqu'un utilisateur ne parvient pas à se connecter à SafeGuard LAN Crypt, il reçoit un message d'erreur indiquant les raisons du refus de connexion ([voir « Annexe : Messages d'erreur affichés lors du chargement du profil », page 42](#) pour la liste des différents messages d'erreur).

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. Le chargement du profil de chiffrement d'un utilisateur est exigé uniquement pour le chiffrement puisque le déchiffrement se déroule en arrière-plan (de manière transparente). L'utilisateur ignore que des tâches de chiffrement ou de déchiffrement sont en cours d'exécution.

REMARQUE :

Les certificats CA ne sont acceptés que s'ils proviennent d'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 - Certificats ». Pour éviter l'affichage d'un message d'erreur, vous devez déplacer manuellement les certificats CA vers une « autorité de certification racine de confiance ».

5.3 Application utilisateur

Une icône en forme de clé dans la barre des tâches Windows indique le statut de SafeGuard LAN Crypt :

- **Une icône verte signifie** que les règles de chiffrement sont chargées et que le chiffrement transparent a été activé.
- **Une icône jaune signifie** que les règles de chiffrement sont chargées et que le chiffrement transparent a été désactivé.
- **Une icône rouge signifie** qu'aucun profil n'a été chargé.

Les utilisateurs peuvent accéder aux fonctions suivantes dans l'application (par un clic droit) :

- Charger les règles de chiffrement/Mettre à jour les règles de chiffrement
- Supprimer les règles de chiffrement
- Désactiver/Activer le chiffrement
- Afficher profil
- Statut client
- Chiffrement initial
- Fermer
- À propos

5.3.1 Menu Utilisateur

Le menu de l'utilisateur SafeGuard LAN Crypt est représenté par une icône dans la barre des tâches Windows. Cette icône est différente en fonction du statut de SafeGuard LAN Crypt.

REMARQUE :

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.

Cliquez sur l'icône avec le bouton droit de la souris pour ouvrir le menu de l'utilisateur de SafeGuard LAN Crypt.

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

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

■ **Supprimer les règles de chiffrement**

L'accès aux données chiffrées sera impossible si les règles de chiffrement ont été effacées. Cette fonction de sécurité protège les données chiffrées de tout accès non autorisé lorsque l'utilisateur n'est pas devant son poste de travail. Bien entendu, cette fonction n'a de sens que si l'utilisation de la clé privée est sécurisée par un 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.

REMARQUE :

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, dans l'Explorateur Windows. Le chiffrement persistant n'a aucun effet lorsque les fichiers sont copiés en dehors de l'Explorateur Windows (par exemple, à partir de la ligne de commande). Dans ce cas, les fichiers sont copiés en clair.

- **Afficher profil**

Affiche dans deux onglets les règles de chiffrement et les clés contenues dans les informations de chiffrement. La page d'onglets *Règles de chiffrement* dresse la liste des règles qui s'appliquent à l'utilisateur connecté. En outre, l'utilisateur peut également sélectionner les options *règles d'exclusion* et *règles d'exception* pour afficher ces règles de chiffrement.

La page d'onglets *Clés disponibles* affiche la liste de toutes les clés disponibles pour l'utilisateur actuel.

- **Statut client**

La fonction **Statut client** affiche des informations détaillées réparties sur sept onglets à propos du statut actuel de la version SafeGuard LAN Crypt Client.

- **Chiffrement initial**

Active l'Assistant qui va chiffrer le fichier sélectionné pour la première fois ([voir « Chiffrement initial et chiffrement explicite », page 26](#) pour des informations plus spécifiques sur cette rubrique).

- **Fermer**

Ferme l'application Utilisateur SafeGuard LAN Crypt.

- **À propos**

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

REMARQUE :

La commande **Fermer** opère uniquement la fermeture de l'application Utilisateur SafeGuard LAN Crypt. Toutefois, SafeGuard LAN Crypt ne change pas de statut ! 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).

5.3.2 Boîte de dialogue Statut client

Vous pouvez également accéder à la boîte de dialogue **Statut client** en cliquant sur Démarrer/Tous les programmes/Utimaco/SafeGuard LAN Crypt/Statut client. La fonction *Statut client* affiche des informations utiles réparties sur huit onglets, notamment à propos des règles de chiffrement actuelles :

Les informations suivantes s'affichent :

■ Statut

Indique si le profil utilisateur a été chargé et si le chiffrement est actif. En outre, cet onglet présente des informations détaillées sur le fichier de stratégie (date de création, responsable de sécurité à l'origine de sa création, etc.). Si le profil utilisateur a été chargé, le chiffrement est également actif. Toutefois, le chiffrement peut également être (temporairement) désactivé alors que le profil utilisateur a été chargé ([voir « Désactiver/Activer le chiffrement », page 22](#)).

■ Paramètres

Fournit des informations sur les paramètres actuellement appliqués au client. La définition de ces paramètres est centralisée par le responsable de sécurité. Elle fait référence 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 utilisateur définis de manière centralisée par le responsable de sécurité.

■ Certificats

Affiche des détails 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

Affiche des informations sur toutes les clés disponibles pour le profil actuellement chargé.

- **Règles**

Affiche la liste de toutes les règles de chiffrement qui s'appliquent à l'utilisateur actuel. Vous pouvez également afficher les règles d'exception et les règles de chiffrement des autres produits SafeGuard en cliquant sur les cases à cocher.

- **Non géré**

Désigne les applications, les lecteurs et les périphériques non traités ainsi que les *règles ignorer* de tous les produits SafeGuard installés.

SafeGuard LAN Crypt gère par défaut certaines applications du type « 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.

Programmes possédant un comportement spécifique à l'enregistrement des fichiers

Le responsable de sécurité a mentionné ici ces programmes car ils présentent un comportement particulier au moment de l'enregistrement des fichiers. Pour que ces programmes puissent fonctionner correctement, SafeGuard LAN Crypt doit utiliser à leur égard une approche spéciale.

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.

- **Boutons Importer/Exporter**

Cliquez sur le bouton *Importer* pour importer les paramètres de SafeGuard LAN Crypt à partir d'un fichier XML ou sur le bouton *Exporter* pour exporter les paramètres actuels du client vers un fichier XML.

5.4 Chiffrement initial et chiffrement explicite

L'installation de SafeGuard LAN Crypt doit être suivie du 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 ;
- les extensions de l'explorateur SafeGuard LAN Crypt ([voir « Extensions de l'explorateur », page 34](#)) ; ou
- l'outil graphique `sglcinit.exe` qui prend également en charge le mode automatique (voir ci-dessous).

Outre le chiffrement initial de dossiers entiers, l'outil de ligne de commande `sglcinit.exe`, en combinaison avec les extensions de l'Explorateur Windows, 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 du profil de chiffrement ont changé.

5.4.1 Assistant chiffrement initial

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

- le chiffrement, déchiffrement et rechiffrement des fichiers ;
- la vérification du statut de chiffrement des fichiers.

Vous pouvez activer cet Assistant de différentes façons :

- en cliquant sur son icône dans la barre d'état système ;
- en cliquant sur Démarrer/Tous les programmes/Utimaco/SafeGuard LAN Crypt/Chiffrement initial ;
- en double cliquant sur `sglcinit.exe` dans `C:\Fichiers programme\Utimaco\SafeGuard LAN Crypt\`

REMARQUE :

Les processus de chiffrement, déchiffrement et rechiffrement se font toujours en fonction du profil de chiffrement. Par conséquent, il est essentiel de charger ce dernier.

5.4.1.1 Réalisation d'un chiffrement initial

1. Au lancement de l'Assistant, sélectionnez l'option **Exécuter le chiffrement initial** au cours de l'*Étape 1 / 5*.
2. Cliquez sur **Suivant**, puis définissez la façon dont les fichiers doivent être gérés à l'*Étape 2 / 5*.

- **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.

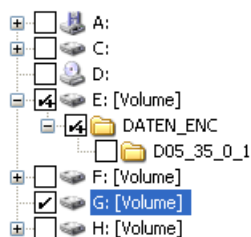
- **Fichiers chiffrés à nouveau selon le profil**

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. 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 permet de chiffrer à nouveau les fichiers qui ont été chiffrés à l'aide de SafeGuard Data Exchange, mais la règle de chiffrement de SafeGuard Enterprise ne s'applique plus. De tels fichiers existent par exemple si la règle de chiffrement a été supprimée, mais que les fichiers n'ont pas été déchiffrés de façon explicite. Dans ce cas, une option peut être activée dans l'*Assistant de chiffrement initial*, qui chiffre à nouveau ces fichiers en fonction des règles de chiffrement de SafeGuard LAN Crypt.

Les fichiers déjà chiffrés peuvent être déchiffrés si aucune (autre) règle de chiffrement ne les concerne ([voir « Déchiffrement des fichiers », page 30](#)).

3. Cliquez sur **Suivant**, puis définissez 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 rechiffrés.

Appuyez sur le bouton **Règles de profil** pour sélectionner automatiquement tous les répertoires pour lesquels des fichiers de chiffrement existent dans le profil de l'utilisateur.

Appuyez sur le bouton **Avancé** pour accéder à d'autres paramètres concernant le chiffrement initial :

REMARQUE :

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**

Si vous sélectionnez cette option, l'Assistant déchiffre les fichiers EFS chiffrés, puis les chiffre à nouveau dans les cas où une règle de chiffrement s'applique. Si vous ne sélectionnez pas cette option, l'Assistant de chiffrement initial ignore les fichiers EFS chiffrés. Ils ne seront pas rechiffrés par SafeGuard LAN Crypt, même si une règle de chiffrement a été indiquée les concernant.
- **Décompresser les fichiers NTFS compressés si nécessaire**

Si vous sélectionnez cette option, l'Assistant décompresse les fichiers NTFS compressés, puis les chiffre dans les cas où une règle de chiffrement s'applique. Si vous ne sélectionnez pas cette option, l'Assistant de chiffrement initial ignore les fichiers NTFS compressés. Ils ne seront pas chiffrés, même si une règle de chiffrement a été indiquée les concernant.
- **Inclure les types de fichier suivants uniquement :**

Si vous indiquez dans cette section des types de fichier spécifiques (par ex. .txt, .doc, etc.), les fichiers de ce type uniquement seront traités par l'Assistant de chiffrement initial. Ce paramètre affecte uniquement les fichiers pour lesquels une règle de chiffrement existe. Si un répertoire contient également des fichiers d'un type différent (non indiqué ici), ils ne seront pas pris en compte pour le chiffrement initial. Ils ne feront l'objet d'un chiffrement que si l'utilisateur les ouvre et les enregistre à nouveau. Si vous indiquez plusieurs types de fichier, séparez-les par des points-virgules.
- 4. Cliquez sur **Suivant**, puis définissez la façon dont les fichiers doivent être intégrés au rapport de chiffrement initial à l'*Étape 4 / 5*. Pour accéder au rapport de chiffrement initial, l'utilisateur doit choisir parmi les options suivantes :
 - **Signaler les erreurs uniquement**

Ce rapport de statut signale uniquement les fichiers pour lesquels des erreurs sont apparues au moment du chiffrement.
 - **Signaler les fichiers modifiés et les erreurs**

Ce rapport de statut signale tous les fichiers modifiés et pour lesquels des erreurs sont apparues au moment du chiffrement.
 - **Signaler tous les fichiers**

Ce rapport de statut intègre tous les fichiers.

5. Cliquez sur **Suivant**. Le **résultat** du chiffrement et le **nom** de la clé utilisée s'affichent alors pour chacun des fichiers à l'*Étape 5 / 5*.

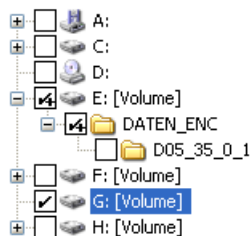
Si le chiffrement a échoué pour certains fichiers, vous pouvez immédiatement tenter de les chiffrer à nouveau. Appuyez pour cela sur le bouton **Réessayer**.

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 de statut sous forme de fichier XML à l'emplacement de votre choix (bouton **Exporter**). Le rapport de statut vous permet de réexécuter le chiffrement des fichiers si le chiffrement échoue.

Cliquez sur **Terminer** pour fermer l'Assistant.

5.4.1.2 Vérification de l'état de chiffrement

1. Au lancement de l'Assistant, sélectionnez l'option **Vérifier l'état du chiffrement** au cours de l'*Étape 1 / 5*.
2. Cliquez sur **Suivant**, puis définissez les dossiers pour lesquels le statut de chiffrement doit être vérifié à l'*Étape 2 / 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 déchiffrés.

Appuyez sur le bouton **Règles de profil** pour sélectionner automatiquement tous les répertoires pour lesquels des fichiers existent dans le profil de l'utilisateur.

Appuyez sur le bouton **Avancé** pour effectuer la vérification sur certains types de fichier uniquement :

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

Si vous indiquez dans cette section des types de fichier spécifiques (par ex. .txt, .doc, etc.), les fichiers de ce type uniquement feront l'objet d'une vérification. Si un répertoire contient également des fichiers d'un type différent (non indiqué ici), ils ne seront pas pris en compte. Si vous indiquez plusieurs types de fichier, séparez-les par des points-virgules.

3. Cliquez sur **Suivant**. Le **résultat** de la vérification et le **nom** de la clé utilisée s'affichent alors pour chacun des fichiers à l'*Étape 3 / 5*.

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 de statut sous forme de fichier XML à l'emplacement de votre choix (bouton **Exporter**).

Cliquez sur **Terminer** pour fermer l'Assistant.

5.4.1.3 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 réexécuté, 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 **Exécuter 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.

REMARQUE :

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 :

- **Activez Fichiers chiffrés selon le profil**
Tous les fichiers sont chiffrés d'après les nouvelles règles de chiffrement.
- **Activez Fichiers chiffrés à nouveau selon le profil**
Si les fichiers doivent être chiffrés au moyen d'une clé différente d'après les nouvelles règles, ils seront alors rechiffrés.
- **Activez Déchiffrer les fichiers avec les clés sélectionnées**, puis sélectionnez **toutes** les clés.
Les fichiers chiffrés pour lesquels aucune règle de chiffrement n'existe plus, seront alors déchiffrés. 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 un chiffrement persistant est activé. Dans ce cas, les fichiers ne seront pas automatiquement chiffrés au moment où ils seront copiés ou déplacés d'un répertoire pour lequel une règle de chiffrement existe vers un répertoire pour lequel aucune règle de chiffrement n'existe.

5.4.2 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\Utimaco\SafeGuard LAN Crypt`).

Syntaxe de la ligne de commande :

```
SGLCInit <Chemin de départ | %Profil>[/S]
{-DRépertoireExclusion}[/Te] [/Tr] [/Td]
[/Tdk {GUID}] [/V1|/V2|/V3] [/X] [/LFichierJournal]
```

Paramètre :

- `Chemin de départ`

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

- `%Profil`

Traite toutes les règles figurant dans le profil de chiffrement chargé avec le chemin absolu. Chiffre/ déchiffre ou rechiffre les fichiers si nécessaire.

REMARQUE :

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`.

- `-DRépertoireExclusion`
Permet d'exclure le dossier spécifié.
- `/Te`
Mode tâche : e = chiffre les fichiers, si nécessaire, conformément au profil de chiffrement.
- `/Tr`
Mode tâche : r = rechiffre les fichiers, si nécessaire, conformément au profil de chiffrement.
- `/Td`
Mode tâche : d = déchiffre les fichiers, si nécessaire, conformément au profil de chiffrement.
- `/Tdk`
Mode tâche : dk= déchiffre les fichiers qui ont été chiffrés à l'aide des clés prédéfinies. Vous devez entrer le GUID des clés.

REMARQUE :

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

- `/V1`
Mode commenté 1 : seuls les messages d'erreur s'affichent.
- `/V2`
Mode commenté 2 : renvoie les fichiers qui doivent être chiffrés, déchiffrés ou chiffrés à nouveau.
- `/V3`
Mode commenté 3 : renvoie tous les fichiers.
- `/X`
Chiffrement initial sans afficher de fenêtre
- `/LFichierJournal`
Les résultats sont consignés dans un fichier journal.

REMARQUE :

Le paramètre `/Td` ne doit être combiné avec `%Profil` que lorsque les fichiers à déchiffrer sont associés à une règle d'exclusion dans le profil. Sinon, utilisez `/Td` avec le chemin de départ.

Exemple :

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

5.5 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
- Un contrôle simple du statut de 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 le statut 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 possède l'accès à la clé.
- **Clé rouge**
Le fichier est chiffré et l'utilisateur ne possède pas l'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.

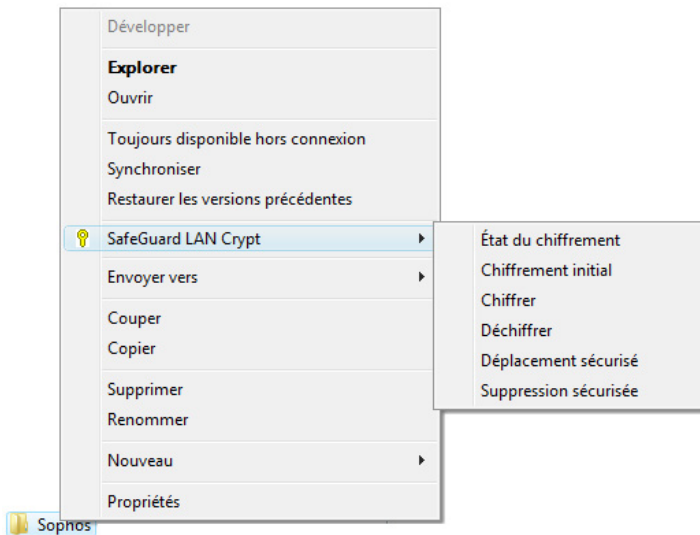
Lorsque vous cliquez sur l'option **SafeGuard LAN Crypt** dans le menu contextuel, le système affiche un sous-menu contenant des options supplémentaires. Ces options varient selon qu'un fichier ou un répertoire a été sélectionné et en fonction du statut de chiffrement du fichier.

REMARQUE :

Des symboles de clé sont aussi ajoutés aux dossiers et fichiers 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 possède l'accès à la clé.
- **Clé rouge**
Le fichier est chiffré et l'utilisateur ne possède pas l'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.

Ce menu peut afficher les options suivantes :

**Pour les répertoires****■ Statut de chiffrement**

En cliquant sur cette option, vous affichez la liste de tous les fichiers de ce répertoire et leur statut 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**

Chiffre tous les fichiers dans le répertoire en fonction du profil de chiffrement chargé. Les sous-répertoires associés à une règle de chiffrement existante sont également inclus dans le chiffrement.

Une barre de progression indique la durée prévue du chiffrement initial. 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**

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**

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**

Cette commande sert, le cas échéant, à chiffrer, déchiffrer ou rechiffrer les fichiers sélectionnés en fonction des règles de chiffrement chargées. Les fichiers sources sont effacés après leur déplacement.

- **Suppression sécurisée**

Cette commande permet d'écraser les emplacements de stockage des fichiers. Il est impossible de restaurer ces fichiers via la Corbeille de Windows.

Pour les fichiers individuels :

- **Statut de chiffrement**

Affiche le statut de 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/Autres options*, il peut indiquer si les statuts de chiffrement de fichier et de règle de 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**

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

- **Chiffrer**

Utilisez cette option pour chiffrer un fichier précis. Une liste des clés disponibles est affichée. Vous y sélectionnez la clé à utiliser pour le chiffrement.

- **Déchiffrer**

Permet de déchiffrer le fichier sélectionné. Il est donc nécessaire que la clé correcte soit disponible dans le profil de chiffrement activé, sinon le fichier reste chiffré.

REMARQUE :

Les règles de chiffrement actives sont toujours prioritaires par rapport à une procédure de chiffrement/déchiffrement explicite lancée avec la commande **Chiffrer/Déchiffrer**. Si vous essayez de chiffrer/déchiffrer des fichiers associés à une règle de chiffrement différente, la commande ne sera pas exécutée et un message d'erreur sera affiché.

Les situations suivantes peuvent être l'origine d'un message d'erreur lorsque l'utilisateur essaie de chiffrer des fichiers via le menu contextuel :

- 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).

5.5.1 Informations de chiffrement

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

5.6 Désactivation/Activation 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 restent en texte clair (non chiffrés) même s'il existe une règle de chiffrement dans le profil de chiffrement de l'utilisateur.

REMARQUE :

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). Conformément à la philosophie de SafeGuard LAN Crypt, ces fichiers devraient être chiffrés au moment de leur copie ou déplacement vers ce dossier.

Par opposition, lorsque l'administrateur désactive la fonction de *chiffrement persistant*, les fichiers restent automatiquement chiffrés même s'ils sont déplacés vers un dossier utilisant l'Explorateur Windows et n'utilisant aucune règle de chiffrement. Lorsque le chiffrement persistant est utilisé dans les cas décrits ci-dessus, il n'est plus nécessaire de désactiver le chiffrement transparent en premier. 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 statut du chiffrement persistant (actif ou non actif).

REMARQUE :

Lorsque le chiffrement persistant est actif et si 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.

5.6.1 Outils de chiffrement transparent et de compression des fichiers

Les outils de compression de fichiers lisent le contenu des fichiers et le compressement. Si une option de chiffrement/déchiffrement transparent est activée, les outils de compression de fichiers reçoivent les fichiers déchiffrés et les compressement. 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 sont à présent enregistrés en texte clair.

Même si une option de chiffrement persistant est activée, les fichiers ne seront pas compressés sous une forme chiffrée tant que le chiffrement persistant se réfère uniquement à la copie et au déplacement des fichiers dans l'Explorateur Windows.

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.

5.7 Compatibilité avec les versions précédentes

Si vous souhaitez exécuter le nouveau logiciel SafeGuard LAN Crypt 3.70 avec les versions précédentes, vous devez tenir compte des points suivants :

- La version SafeGuard LAN Crypt 3.70 Client peut uniquement charger les profils créés avec la version 3.60 de SafeGuard LAN Crypt Administration.
- Les versions SafeGuard LAN Crypt Client antérieures peuvent utiliser des profils et des règles créés avec la version 3.60. (Il existe toutefois quelques exceptions, telles que les règles créées en Unicode pour le japonais, dans la mesure où cette fonction n'est pas prise en charge avant la version 3.50).
- Les versions SafeGuard LAN Crypt Client antérieures à la version 3.50 ne peuvent pas lire les fichiers chiffrés avec les versions Client 3.50 ou supérieures. Il est possible de configurer la nouvelle version Client et de l'utiliser pour chiffrer les fichiers d'un ancien format.
- Cependant, la nouvelle version SafeGuard LAN Crypt 3.70 Client peut lire des fichiers chiffrés avec des versions Client plus anciennes.

Pour procéder à la migration vers SafeGuard LAN Crypt 3.70, nous recommandons d'appliquer les instructions suivantes, dans l'ordre indiqué :

1. Tout d'abord, mettez SafeGuard LAN Crypt Administration à jour vers la version 3.60.
2. **Pour les versions Client antérieures à la version 3.50** : dans le module Administration, sélectionnez l'option **Utilisez anci format d'enchiffrement jusqu'à la date suivante**. Ensuite, utilisez SafeGuard LAN Crypt 3.60 Administration pour créer de nouveaux profils. Cette approche permet de s'assurer que tous les clients peuvent lire des fichiers chiffrés lors de la phase de migration, pendant laquelle il est nécessaire d'exécuter des clients anciens et nouveaux en parallèle.
3. Mettez les versions Client à jour vers SafeGuard LAN Crypt Version 3.70.
4. Une fois toutes les versions Client mises à jour, générez de nouveaux profils sans le paramètre mentionné ci-dessus. Vous pouvez ignorer cette étape si la date spécifiée est déjà écoulée.
5. Exécutez le chiffrement initial afin de convertir tous les fichiers au nouveau format.

5.8 Désinstallation de la version Client

Pour désinstaller la version SGLC Client, ouvrez le Panneau de configuration de Windows : sélectionnez Démarrer/Panneau de configuration/Ajout ou Suppression de programmes, puis sélectionnez l'entrée correspondant à *SafeGuard LAN Crypt Client*. Cliquez ensuite sur *Supprimer*.

Dans les deux cas, vous devez redémarrer l'ordinateur pour appliquer les modifications.

REMARQUE :

Tous les fichiers qui ont été chiffrés avec SafeGuard LAN Crypt ne peuvent plus être déchiffrés une fois la version SGLC Client désinstallée.

5.9 Annexe : Messages d'erreur affichés lors du chargement du profil

Si des problèmes se produisent pendant le chargement du profil, la version SGLC Client affiche l'un des messages d'erreur suivants, pour en identifier la cause :

- Certificat utilisateur introuvable.
- Certificat du responsable de sécurité LAN Crypt introuvable !
- Problème lors du chargement des certificats - processus terminé...
- Erreur pendant la vérification du certificat utilisateur.
- Le certificat utilisateur a expiré ou n'est pas encore valide.
- Le certificat du responsable de sécurité LAN Crypt a expiré ou n'est pas encore valide.
- Certificat utilisateur supprimé.
- Le certificat du responsable de sécurité LAN Crypt a été annulé.
- Erreur pendant la vérification du certificat du responsable de sécurité LAN Crypt.
- Impossible de copier le profil utilisateur « %s » dans le dossier de mémoire cache local « %s » !
- Erreur pendant le chargement de la clé de gestion des clés.
- Cette version du fichier de stratégie n'est pas prise en charge.
- L'émetteur du certificat est introuvable ou n'a pas pu être vérifié.
- Impossible de trouver ou vérifier l'emplacement principal de certification.
- Le statut de révocation du certificat est inconnu. CRL introuvable ou périmé.
- Le certificat utilisateur ne dispose pas de l'extension requise d'utilisation de la clé.
- Le certificat utilisateur comporte une extension non prise en charge.
- Le certificat utilisateur est lié au fournisseur de services de chiffrement de base de Microsoft non pris en charge.
- Le code entré peut être incorrect !
- L'émetteur du certificat du responsable de sécurité LAN Crypt est introuvable ou n'a pas pu être modifié.

- Impossible de trouver ou vérifier l'emplacement principal de certification du responsable de sécurité LAN Crypt.
- Le statut de révocation du certificat de responsable de sécurité LAN Crypt est inconnu. CRL introuvable ou périmé.
- Le certificat de responsable de sécurité LAN Crypt ne dispose pas de l'extension requise d'utilisation de la clé.
- Le certificat du responsable de sécurité LAN Crypt comporte des extensions qui ne sont pas prises en charge.
- Impossible de déchiffrer le fichier de stratégie.
- Impossible de télécharger le fichier de stratégie.

6 Copyright

Copyright © 1996 - 2009 Utimaco Safeware AG- a member of the Sophos Group.

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.

SafeGuard est une marque déposée de Utimaco Safeware AG - a member of the Sophos Group.

Microsoft, Windows et le logo Windows sont des marques commerciales ou des marques déposées de Microsoft Corporation aux Etats-Unis et dans d'autres pays.

Ce produit inclut des programmes logiciels développés par Eric Young (eay@mincom.oz.au). Les droits de propriété industrielle de Ascom Tech Ltd. ont été accordés en Europe, au Japon et aux Etats-Unis. IDEA est une marque commerciale de Ascom, Tech Ltd. Ce produit inclut des programmes logiciels développés par OpenSSL Project aux fins d'utilisation dans OpenSSL Toolkit. (<http://www.openssl.org/>)

Tous les autres noms de produits et d'entreprises cités dans ce document sont des marques ou des marques déposées de leurs propriétaires respectifs.

7 Assistance technique

Documentation en ligne

Notre base de données en ligne fournit des réponses à de nombreuses questions courantes sur la gamme de produits SafeGuard, notamment sur leurs fonctionnalités, leur mise en œuvre, l'administration et la résolution des problèmes.

Lien vers la rubrique d'assistance : <http://www.utimaco.com/myutimaco>

Pour accéder à l'espace public de la base de connaissances, vous pouvez vous connecter en tant qu'utilisateur invité (Guest). Pour accéder à l'espace réservé de la base de connaissances, vous devez être détenteur d'un contrat de maintenance logicielle en cours de validité.

Notre équipe d'assistance enrichit constamment le contenu des deux espaces en les mettant à jour régulièrement.

Services de support et support téléphonique

Notre équipe peut également fournir une assistance par téléphone aux clients possédant un contrat de maintenance logicielle en cours de validité. Pour recevoir une proposition de contrat adaptée à vos besoins, veuillez contacter votre distributeur.

Vous comprendrez certainement que nous avons besoin de plusieurs jours pour traiter certaines demandes de nos clients ne disposant pas d'un contrat de maintenance logicielle en cours de validité. En cas d'urgence, veuillez contacter votre distributeur qui vous a vendu vos licences ou votre abonnement logiciel.