# Qu’est-ce que u.trust LAN Crypt pour Windows?

Grâce à un chiffrement transparent des fichiers, *u.trust LAN Crypt* permet l’échange de données confidentielles au sein de groupes d’autorisation dans les petites, moyennes et grandes organisations. *u.trust LAN Crypt* fonctionne sans intervention de l’utilisateur. Il soutient le rôle d’un responsable de la sécurité (SO), qui peut restreindre les droits d’accès aux fichiers chiffrés à l’aide de *u.trust LAN Crypt*. Un responsable principal de la sécurité (MSO) dispose du droit de gérer *u.trust LAN Crypt* ou de déléguer des autorisations. De cette manière, il est possible de mettre en place une hiérarchie de responsables de la sécurité capable de répondre aux exigences de sécurité de toute société.

Les fichiers chiffrés n’ont pas besoin d’être attribués à des utilisateurs individuels. Tout utilisateur disposant de la clé requise peut travailler avec un fichier chiffré. Cela permet aux administrateurs de créer des groupes d’utilisateurs logiques qui peuvent partager l’accès et travailler avec des fichiers chiffrés. Pour prendre un exemple de la vie de tous les jours, ce processus peut être comparé à une sorte de porte-clés. *u.trust LAN Crypt* munit les utilisateurs et les groupes d’utilisateurs d’un trousseau de clés. Chaque clé individuelle peut être utilisée pour différents dossiers ou fichiers.

Chaque fois qu’un utilisateur déplace un fichier vers un dossier chiffré, ledit fichier est chiffré sur son ordinateur. Si un autre utilisateur du même groupe de privilèges lit le fichier à partir du dossier, ledit fichier est transféré sous forme chiffrée. Le fichier n’est déchiffré que sur l’ordinateur du destinataire. C’est là que l’utilisateur peut le modifier. Le fichier est de nouveau chiffré avant d’être retransféré vers le dossier chiffré.

Les utilisateurs non autorisés peuvent avoir accès à ces fichiers chiffrés (uniquement à partir de postes de travail sans *u.trust LAN Crypt*), mais sans l’autorisation *u.trust LAN Crypt* correspon- dante, ils ne verront que leur contenu chiffré. De cette façon, même si aucune protection d’accès n’est définie dans le système de fichiers lui-même, si le réseau est attaqué ou si les employés ne suivent pas les directives de sécurité de l’organisation, le fichier reste protégé.

## Protection des données avec *u.trust LAN Crypt*

*u.trust LAN Crypt* garantit que les fichiers sensibles peuvent être stockés chiffrés sur les serveurs de fichiers et les postes de travail. De même, la transmission en réseau (LAN ou WAN) est protégée, car le chiffrement et le déchiffrement s’effectuent au niveau de la mémoire principale du poste de travail de l’utilisateur. Sur les postes de travail, toutes les opérations de chiffrement et de déchiffrement sont transparentes et se font sans intervention de l’utilisateur. Aucun logiciel de sécurité particulier ne doit être installé sur le serveur de fichiers lui-même.

Un responsable de la sécurité peut définir différents droits d’accès pour les dossiers et les fichiers. Ces droits sont répertoriés dans des profils de chiffrement pour les utilisateurs. Les profils de chiffrement sont distribués aux utilisateurs via des fichiers de stratégie. Les fichiers de stratégie contiennent toutes les règles, les droits d’accès et les clés nécessaires au chiffrement transparent. Le fichier de stratégie est protégé par un certificat. Pour que les utilisateurs puissent traiter les données chiffrées à l’aide de *u.trust LAN Crypt* sur leurs ordinateurs, ils doivent avoir accès au fichier de stratégie. Doté de la clé privée appartenant au certificat, l’utilisateur a accès au fichier de stratégie où le profil de chiffrement est stocké.

*u.trust LAN Crypt* permet de répartir les utilisateurs en différents groupes d’autorisation. Tous les utilisateurs de *u.trust LAN Crypt* ayant enregistré le même profil de chiffrement dans leur fichier de stratégie sont membres d’un groupe d’autorisation. Vous n’avez pas à vous soucier du chiffrement ou de l’échange de clés. Seul l’accès aux fichiers de stratégie est nécessaire pour que les fichiers puissent être chiffrés ou déchiffrés de manière transparente dès leur ouverture ou fermeture. Toutes les formes d’organisation peuvent être mappées. Cela va d’un modèle LAN dans lequel les utilisateurs sont administrés de manière centralisée à un modèle distribué dans lequel les utilisateurs n’utilisent que des blocs-notes.

Depuis la version 4.03, le pilote du mini-filtre *u.trust LAN Crypt* peut également traiter les fichiers chiffrés avec SafeGuard Enterprise (Fileshare). Le déchiffrement de ces fichiers n'est pas nécessaire. Les clés respectives de SafeGuard Enterprise doivent uniquement être migrées vers *u.trust LAN Crypt* à l'aide d'un outil d'exportation et d'importation de clés.

**Remarque**

- Dans ce contexte, veuillez également noter que les fichiers qui sont chiffrés avec SafeGuard Enterprise Fileshare et ensuite édités avec *u.trust LAN Crypt* ne peuvent plus être lus par *SafeGuard Enterprise Fileshare*!

- Même en fonctionnement normal, Windows transfère souvent des parties de la mémoire de travail sur le disque dur. Dans certains cas, par exemple en cas de plantage ou d'"écrans bleus", l'ensemble du contenu de la mémoire peut même être écrit sur le disque dur. Par conséquent, des informations sensibles qui ne sont autrement disponibles que dans la mémoire principale (comme le contenu de documents ouverts) peuvent être stockées dans un fichier sur le disque dur. Le cryptage du disque dur (tel que *BitLocker* ou *Utimaco DiskEncrypt*) garantit que le contenu de ces données souvent sensibles est stocké sur le disque dur sous forme cryptée dans tous les cas et qu'il est ainsi protégé de manière optimale contre l'espionnage. C'est pourquoi l'utilisation du cryptage du disque dur est recommandée comme une protection de base importante et comme un complément utile lors de l'utilisation de *u.trust LAN Crypt*.

## SafeGuard Enterprise : Migration du chiffrement des fichiers

SafeGuard Enterprise est une suite de sécurité de Sophos, composée de plusieurs modules. Data Exchange (DX), Cloud Storage (CS) et File Encryption (FE) fournissent tous un chiffrement au niveau des fichiers. Cependant, l'ensemble de la suite logicielle est en cours d'abandon, ce qui expose les utilisateurs au risque de perdre l'accès à leurs documents chiffrés. La migration d'un produit de sécurité à un autre peut s'avérer fastidieuse et représenter un risque supplémentaire, en particulier si le processus implique le décryptage des données. Ce n'est toutefois pas le cas lors de la migration vers u.trust LAN Crypt.

u.trust LAN Crypt et Sophos SafeGuard Enterprise sont entièrement compatibles. Ils partagent la même base technique et le même sous-système de chiffrement des fichiers. Par conséquent, les fichiers chiffrés dans SafeGuard Enterprise sont entièrement compatibles avec u.trust LAN Crypt et peuvent être lus en mode natif par ce dernier. Les clés de chiffrement sont spécifiques à chaque installation et seules celles-ci doivent être migrées.

**Étape 1 : Exportation des clés de SafeGuard Enterprise**

Les clés utilisées pour chiffrer les fichiers sont uniques pour chaque installation de SafeGuard Enterprise. Sophos fournit un outil simple qui permet d'exporter facilement toutes les clés de chiffrement utilisées dans SafeGuard Enterprise pour chiffrer les fichiers. Toutes les clés sont facilement copiées dans un seul paquet.

**Étape 2 : Importer les clés dans u.trust LAN Crypt**

Les clés, désormais disponibles dans un paquet séparé, peuvent être facilement importées dans tout système u.trust LAN Crypt existant. Une fois importée, l'installation u.trust LAN Crypt dispose de tout ce dont elle a besoin pour accéder aux fichiers chiffrés avec SafeGuard Enterprise.

**Étape 3 : Mise à jour de la stratégie / Attribution des clés**

Attribuez les clés nouvellement importées à tous les utilisateurs qui ont besoin d'accéder aux fichiers chiffrés par SafeGuard Enterprise. Ces clés permettent aux utilisateurs de lire les fichiers qui ont été chiffrés par n'importe quel module de chiffrement de fichiers SafeGuard dans le passé. Cela s'applique également aux fichiers qui ont été chiffrés par SafeGuard Enterprise après l'importation des clés.

**Étape 4 : Accès aux fichiers de SafeGuard Enterprise**

Le client u.trust LAN Crypt partage sa base technique avec SafeGuard Enterprise. Une fois que les clés ont été déployées sur le client, celui-ci peut lire tous les fichiers qui ont été chiffrés avec l'un des modules de chiffrement de fichiers de SafeGuard Enterprise - DX, CS, FS. Il n'est pas nécessaire de décrypter un seul fichier. Quel que soit le temps écoulé depuis le chiffrement d'un fichier, u.trust LAN Crypt peut le lire.

La compatibilité totale au niveau des fichiers permet une migration en douceur. Même si certaines parties de l'entreprise utilisent encore SafeGuard Enterprise, tous les fichiers chiffrés qu'elles créent peuvent être lus par toute personne ayant déjà migré vers u.trust LAN Crypt.

> **Note** Si vous avez installé *SafeGuard Enterprise* et prévoyez de migrer vers *u.trust LAN Crypt*, veuillez contacter l'assistance u.trust LAN Crypt. De plus amples informations sont

disponibles à l'adresse suivante : https://utimaco.com/file-encryption-migration-five-easy-steps-safeguard-enterprise.

# Chiffrement

## Chiffrement transparent

Pour l'utilisateur, le chiffrement transparent signifie que toutes les données stockées sous forme chiffrée (dans des dossiers ou des lecteurs chiffrés) sont automatiquement déchiffrées dans la mémoire principale dès leur ouverture par une application (par exemple, Office). Le fichier est automatiquement chiffré de nouveau lors de son enregistrement. Le chiffrement transparent couvre toutes les opérations de fichiers. Tous les processus s'exécutent en arrière-plan. Par conséquent, les utilisateurs ne remarquent pas quand ils travaillent avec des fichiers chiffrés.

**Remarque**

- *u.trust LAN Crypt* ne peut pas chiffrer de fichiers utilisant la **compression NTFS** ou le **chiffrement EFS** sous le système de fichiers NTFS de Windows. Cependant, si une règle de chiffrement existe, l'assistant de chiffrement initial offre la possibilité de décompresser ou de déchiffrer les fichiers compressés au format NTFS et/ou chiffrés au format EFS pendant le chiffrement initial. Les fichiers sont ensuite chiffrés par *u.trust LAN Crypt* selon les règles de chiffrement. Si nécessaire, le responsable de la sécurité doit déterminer à l'avance si l'utilisateur a la possibilité de décompresser des fichiers compressés au format NTFS ou de déchiffrer des fichiers chiffrés au format EFS.

Le chiffrement ne dépend pas des dossiers, mais uniquement des règles de chiffrement. Le chiffrement fonctionne comme suit:

- Tous les fichiers pour lesquels une règle de chiffrement existe sont automatiquement chiffrés.
- Lorsque des fichiers sont déplacés ou copiés dans un dossier chiffré, leur chiffrement s'effectue conformément à la règle de chiffrement définie pour ce dossier. Le responsable de la sécurité peut définir plusieurs règles de chiffrement pour différents types de fichiers ou noms de fichiers au sein du même dossier via l'administration *u.trust LAN Crypt*. Par exemple, vous pouvez chiffrer des fichiers Word avec une règle différente de celle des fichiers Excel, même si les deux fichiers se trouvent dans le même dossier.
- Lorsque vous renommez des fichiers chiffrés, ceux-ci restent chiffrés (sauf si une autre règle de chiffrement existe, ou s'il n'existe aucune règle de chiffrement pour le nouveau nom de fichier ou l'extension).
- Si un utilisateur copie ou déplace des fichiers chiffrés vers un emplacement où la règle de chiffrement précédente ne s'applique plus, ces fichiers sont automatiquement déchiffrés.

  **Remarque**

  - Cela ne s'applique pas si un utilisateur déplace des fichiers vers un autre dossier au sein du même partage réseau. Dans ce cas, les fichiers restent chiffrés, même s'il n'existe aucune règle de chiffrement.
- Si le responsable de la sécurité ou l'administrateur système a activé la fonctionnalité de **chiffrement persistant** via la stratégie de groupe (GPO) *u.trust LAN Crypt*, les fichiers chiffrés restent chiffrés, et ce, même s'ils sont déplacés ou copiés vers un autre dossier ou emplacement pour lequel aucune règle de chiffrement n'existe (par exemple sur une clé USB).
- Si un utilisateur copie ou déplace des fichiers chiffrés vers un emplacement qui possède une règle de chiffrement, les fichiers sont d'abord déchiffrés, puis chiffrés à l'aide de l'autre clé définie pour cet emplacement.

### Accès aux données chiffrées

Si, pour un dossier spécifique, la stratégie de chiffrement d'un utilisateur ne contient ni clé ni règle de chiffrement, l'utilisateur n'est pas autorisé à accéder aux fichiers chiffrés du dossier. L'utilisateur n'est autorisé à lire, copier, déplacer, renommer, supprimer, etc. aucun fichier chiffré de ce dossier.

Si l'utilisateur dispose de la clé avec laquelle les fichiers ont été chiffrés, il peut les ouvrir, et ce, même si son profil de chiffrement pour cet emplacement ou dossier ne comporte pas de règle de chiffrement.

**Remarque**

- À partir de LAN Crypt Administration Windows version 13.0.0, le chiffrement au format CBC-uIV est disponible. Les versions antérieures du client LAN Crypt Classic (avant la version 13.0.0) ne reconnaissent pas ce format et ne peuvent donc pas déchiffrer les fichiers concernés. Veillez donc à toujours utiliser la version la plus récente du client.

**Intégration de {{ site.productName*2Go*fr }}.**

Les fichiers qui ont été cryptés par *{{ site.productName_2Go_fr }}* sur la base d'un mot de passe peuvent être ouverts et modifiés avec *u.trust LAN Crypt pour Windows* depuis la version 4.2.0. Pour cela, il faut que la clé nécessaire soit disponible dans la politique de chiffrement de l'utilisateur.

Après avoir consulté ou modifié le fichier, celui-ci peut toujours être crypté et décrypté sans problème avec la même clé par *{{ site.productName_2Go_fr }}* et toutes les autres applications *u.trust LAN Crypt* qui prennent en charge le cryptage et le décryptage basés sur un mot de passe.

**Renommer ou déplacer un dossier**

Pour des raisons de performances, *u.trust LAN Crypt* ne modifie pas l'état du chiffrement lors du déplacement de dossiers entiers dans un lecteur via l'Explorateur Windows. Cela signifie qu'aucun chiffrement, déchiffrement ou rechiffrèrent ne se produit lors du déplacement d'un dossier entier.

Si les fichiers de ces dossiers ont été chiffrés, ils resteront chiffrés sous le nouveau nom de dossier ou dans le nouvel emplacement. Si l'utilisateur dispose de la clé correspondante, il peut travailler avec ces fichiers comme à son habitude.

Le comportement est différent lors du déplacement de fichiers ou de dossiers vers une autre partition ou vers des périphériques de stockage USB pour lesquels aucune règle de chiffrement n'a été définie. Si la fonctionnalité de **chiffrement persistant** de *u.trust LAN Crypt* n'est pas activée, les fichiers seront déchiffrés lorsqu'ils seront déplacés vers ce support. Si le responsable de la sécurité ou l'administrateur système a activé le **chiffrement persistant** pour les clients, les fichiers restent chiffrés.

**Remarque**

- Cependant, cela ne s'applique que s'il n'y a pas de règle de chiffrement pour le nouvel emplacement de stockage. Cependant, s'il y a une règle de chiffrement, les fichiers seront chiffrés selon la règle de chiffrement applicable au nouvel emplacement de stockage.

**Déplacement sécurisé**

*u.trust LAN Crypt* prend en charge le déplacement sécurisé des fichiers et des dossiers. Lors du déplacement de fichiers via *u.trust LAN Crypt*, les fichiers sont chiffrés, déchiffrés ou chiffrés à nouveau au niveau du nouvel emplacement conformément aux règles de chiffrement applicables. Après cela, les fichiers sources sont supprimés de manière sécurisée.

Cette fonction est disponible via l'entrée *u.trust LAN Crypt* > Déplacement sécurisé du menu contextuel de l'Explorateur Windows dans *u.trust LAN Crypt*. Une boîte de dialogue vous permet ensuite de sélectionner l'emplacement vers lequel les fichiers doivent être déplacés.

**Déchiffrement explicite des fichiers**

Pour déchiffrer un fichier, il suffit de le copier ou de le déplacer dans un dossier sans règles de chiffrement. Le fichier est ensuite automatiquement déchiffré.

Prérequis:

- un profil de chiffrement correspondant est chargé
- l'utilisateur dispose de la clé requise
- le profil de chiffrement actif ne contient aucune règle de chiffrement pour le nouvel emplacement
- **chiffrement persistant** n'est pas actif

**Remarque**

- *u.trust LAN Crypt* peut également chiffrer les dossiers hors ligne dans Windows. Cependant, des problèmes peuvent survenir en relation avec les scanners antivirus. Retrouvez des informations plus détaillées sur les problèmes connus relatifs aux scanners antivirus dans les informations de version du client *u.trust LAN Crypt*.

**Supprimer des fichiers chiffrés**

Une fois votre règle de chiffrement chargée, vous pouvez supprimer n'importe quel fichier chiffré pour lequel vous disposez d'une clé.

**Remarque**

- En fait, la suppression de fichiers consiste à déplacer les fichiers vers la Corbeille Windows. Pour assurer d'offrir la norme de sécurité la plus élevée, les fichiers chiffrés avec *u.trust LAN Crypt* restent chiffrés, même dans la corbeille. Aucune clé n'est nécessaire pour vider la corbeille.

**Fichiers et dossiers exclus du chiffrement**

Les fichiers et dossiers suivants sont automatiquement exclus du chiffrement, même dans le cas où une règle de chiffrement a été définie pour eux:

- Fichiers du dossier d'installation de *u.trust LAN Crypt*.
- Fichiers des dossiers Programmes et Programmes (x86).
- Fichiers du dossier d'installation de Windows.
- Fichiers du dossier Windows.old.
- Fichiers du dossier $SGNTMP$.
- Cache du fichier de stratégie

L'emplacement est spécifié dans l'administration *u.trust LAN Crypt* et est affiché dans 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).
- Fichiers de dossiers qui sont définis avec une règle d'exclusion ou Ignorer dans *u.trust LAN Crypt*.

**Chiffrement persistant**

Concernant *u.trust LAN Crypt*, un responsable de la sécurité ou administrateur système peut configurer le chiffrement persistant via une stratégie de groupe (GPO) *u.trust LAN Crypt*. Normalement, les fichiers ne sont chiffrés que s'ils sont soumis à une règle de chiffrement.

Par exemple, si un utilisateur copie un fichier chiffré dans un dossier pour lequel aucune règle de chiffrement n'est définie, le fichier est déchiffré dans le dossier de destination. Cependant, si le **chiffrement persistant** est activé, les fichiers restent chiffrés même s'ils sont déplacés ou copiés vers un autre emplacement pour lequel aucune règle de chiffrement n'est définie.

Les responsables de la sécurité ou les administrateurs système peuvent définir ce comportement via une stratégie de groupe (GPO) *u.trust LAN Crypt*. Lorsque le **chiffrement persistant** est désactivé, les fichiers sont déchiffrés s'ils sont copiés ou déplacés vers un emplacement ne comportant pas de règle de chiffrement. Les fichiers peuvent ainsi être déchiffrés, par exemple pour un envoi sous forme de pièce jointe. Cependant, il est préférable de ne pas désactiver le **chiffrement persistant** et, à la place, de copier ces fichiers dans un dossier qui a une règle Ignorer ou une règle d'exception. La fonction de protection du **chiffrement persistant** est ainsi maintenue, et il peut exister dans le même temps un emplacement de stockage permettant aux utilisateurs de déchiffrer explicitement les fichiers, par exemple pour les envoyer sous forme de courriels.

Les règles suivantes s'appliquent au **chiffrement persistant**:

- Le pilote de *u.trust LAN Crypt* conserve uniquement le nom du fichier, sans aucune information relative au chemin d'accès. Seul ce nom peut être utilisé à des fins de comparaison. Cela ne concerne donc que des situations dans lesquelles les fichiers source et cible ont un nom identique. Si le fichier est renommé pendant l'opération de copie, le fichier résultant est considéré comme un fichier « différent » et n'est donc pas soumis au **chiffrement persistant**.
- Lorsqu'un utilisateur enregistre un fichier chiffré à l'aide de la fonction Enregistrer sous dans un emplacement non couvert par une règle de chiffrement, le fichier est stocké sous une forme déchiffrée.
- Les informations relatives aux fichiers ne sont conservées que pendant une durée limitée. Si l'opération prend trop de temps (plus de 15 secondes), le fichier nouvellement créé est considéré comme un fichier différent et indépendant, et n'est donc pas soumis au chiffrement persistant.

**Remarque**

- Le chiffrement persistant utilise le cache de tunneling Windows. Si un thread ouvre un fichier chiffré puis crée, dans l'intervalle de tunneling (par défaut : 15 s), un fichier portant *le même nom*, le nouveau fichier sera automatiquement chiffré - quel que soit le chemin de destination et même si aucune politique de chiffrement n'existe pour cet emplacement. Ce comportement dépend du système et doit être pris en compte lors de l'utilisation de LAN Crypt.

#### Chiffrement persistant par rapport à la règle de chiffrement

Le **chiffrement persistant** garantit qu'un fichier chiffré conserve son état de chiffrement, c'est-à-dire la clé de chiffrement d'origine. Cela fonctionne bien avec le **chiffrement persistant** si le fichier est copié ou déplacé vers un dossier sans règle de chiffrement. Cependant, si le fichier est copié ou déplacé vers un emplacement ayant une règle de chiffrement différente, celle-ci a priorité sur le **chiffrement persistant**. Le fichier est ensuite converti selon la règle de chiffrement de cet emplacement à l'aide de l'algorithme de chiffrement (par exemple, AES) et de la clé définie pour cet emplacement.

#### Chiffrement persistant par rapport à la règle Ignorer ce chemin

Une règle Ignorer ce chemin remplace le **chiffrement persistant**. Cela signifie que les fichiers chiffrés qui sont copiés dans un dossier contenant une règle Ignorer ce chemin applicable sont déchiffrés.

Une règle Ignorer ce chemin s'utilise principalement pour les fichiers auxquels on accède très fréquemment, ainsi que pour les fichiers qui n'ont pas de raison particulière d'être chiffrés. Cela améliore les performances du système.

#### Chiffrement persistant par rapport à la règle Exclure ce chemin

Une règle Exclure ce chemin remplace le chiffrement persistant. Cela signifie que les fichiers chiffrés qui sont copiés dans un dossier contenant une règle Exclure ce chemin applicable sont déchiffrés.

### Limitations du chiffrement persistant

Le **chiffrement persistant** a certaines limites. Ces limites sont les suivantes:

#### Les fichiers qui sont censés rester simples sont chiffrés.

### Les fichiers non chiffrés sont copiés vers plusieurs emplacements avec et sans application de règles de chiffrement.

- Si un fichier non chiffré est copié vers plusieurs emplacements en même temps et qu'une règle de chiffrement est appliquée à l'un de ces emplacements, toutes les copies de ce fichier risquent d'être également chiffrées.

- Si un fichier non chiffré est copié vers un emplacement chiffré, le fichier est ajouté à la liste interne de l'outil de chiffrement. Lorsqu'une deuxième copie du fichier est créée, l'outil de chiffrement trouve le nom du fichier dans sa liste et chiffre également la deuxième copie.

**Créer un fichier portant le même nom après avoir accédé à un fichier chiffré**

- Si un fichier chiffré est ouvert (consulté) et qu'un nouveau fichier portant le même nom est créé peu de temps après, le fichier nouvellement créé est chiffré à l'aide de la même clé que le premier fichier.
- Ceci ne s'applique que si la même application / thread est utilisée pour lire le fichier chiffré et pour créer le nouveau.

**Par exemple:** Dans l'Explorateur Windows, faites un clic droit dans un dossier comportant une règle de chiffrement et cliquez sur *Nouveau -> Document texte*. Cliquez immédiatement avec le bouton droit dans un dossier dépourvu de règle de chiffrement et cliquez sur *Nouveau -> Document texte*. Le second fichier est également chiffré.

#### Les fichiers ne sont pas chiffrés

**Plusieurs copies d'un fichier sont créées**

- Si des copies d'un fichier chiffré sont créées dans le même dossier que le fichier original, celles-ci ne sont pas chiffrées. Comme les copies créées ont des noms de fichiers différents (par exemple doc.txt par rapport à doc - Raccourci.txt), la correspondance du nom de fichier échoue et elles ne sont donc pas chiffrées par le **chiffrement persistant**.

**API client et libellés de chiffrement pour les produits DLP**

Si un produit de protection contre la perte de données (DLP) identifie des données qui doivent être chiffrées, il peut utiliser l'API client *u.trust LAN Crypt* pour chiffrer ces fichiers. Dans l'administration *u.trust LAN Crypt* (voir Aide d'administration), vous pouvez définir différentes balises de chiffrement qui spécifient la clé *u.trust LAN Crypt* à utiliser. L'API client peut utiliser ces balises de chiffrement prédéfinies afin d'appliquer des clés spéciales pour différents contenus. Par exemple, la balise de chiffrement `\<CONFIDENTIAL\>` destinée à chiffrer tous les fichiers classés comme confidentiels par votre produit DLP.

## Désactiver / activer le chiffrement transparentn

La désactivation du chiffrement transparent dans le menu utilisateur de *u.trust LAN Crypt* entraîne l'arrêt du chiffrement et du déchiffrement automatiques des fichiers auxquels on accède par la suite. Les fichiers nouvellement générés restent également non chiffrés, même si le profil de chiffrement de l'utilisateur inclut une règle de chiffrement les concernant.

> **Remarque**
>
> - Les paramètres peuvent être définis par le responsable de la sécurité ou l'administrateur système via la stratégie de groupe (GPO) *u.trust LAN Crypt*. En outre, leurs fonctions ou éléments peuvent être sélectionnés via le menu utilisateur. De cette manière, le client peut être configuré de telle sorte d'empêcher la désactivation du chiffrement transparent par l'utilisateur.

En comparaison, la désactivation du **chiffrement persistant** provoque le déchiffrement des fichiers chiffrés lors de leur copie/déplacement vers un emplacement ou dossier ne comportant aucune règle de chiffrement. La fonction de chiffrement et de déchiffrement automatiques basée sur des règles pour les dossiers et les fichiers (voir Chiffrement transparent) este effective lorsque vous désactivez le **chiffrement persistant**. Le responsable de la sécurité ou l'administrateur effectue également la configuration du **chiffrement persistant** via une stratégie de groupe (GPO) *u.trust LAN Crypt*.

Si la fonction de **chiffrement persistant** est activée, les fichiers chiffrés restent chiffrés, et ce, même s'ils sont copiés ou déplacés vers un emplacement ou dossier sans règle de chiffrement. Si vous utilisez le chiffrement persistant, il n'est pas nécessaire de désactiver le **chiffrement transparent** avant de copier des fichiers chiffrés vers un autre emplacement. Le **chiffrement persistant** garantit que les fichiers restent chiffrés, même s'ils sont déplacés accidentellement vers un autre dossier ou si l'utilisateur oublie de désactiver le chiffrement avant de les déplacer ou de les copier. Vous devez redémarrer votre ordinateur pour que les modifications apportées au **chiffrement persistant** (activé ou désactivé) soient prises en compte.

**Remarque**

- Si le chiffrement persistant est activé et qu'un utilisateur déplace ou copie un fichier vers un dossier dans lequel une règle Ignorer ou Exclure s'applique, le fichier est alors déchiffré. Notez également que la modification du paramètre de chiffrement persistant nécessite un redémarrage de l'ordinateur client. Le paramètre précédemment défini reste valide jusqu'à ce que l'ordinateur soit redémarré.

## Chiffrement transparent et outils de compression de fichiers

Les outils de compression de fichiers ouvrent, lisent et compressent le contenu des fichiers. Si le chiffrement/déchiffrement transparent est activé, les outils de compression de fichiers reçoivent les fichiers déchiffrés. Les fichiers sont alors compressés. Les fichiers de l'archive résultante 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 sont pas compressés sous forme chiffrée. Cependant, le fichier d'archivage lui-même reste chiffré. Il ne peut donc être lu que par un utilisateur disposant de la clé nécessaire. Toutefois, il existe une condition préalable à cela. Les fichiers d'archivage doivent en effet également être soumis à une règle de chiffrement.

Cependant, si vous souhaitez aussi utiliser des programmes de compression pour regrouper des fichiers chiffrés dans un fichier d'archivage, le chiffrement transparent doit être désactivé au préalable. En général, cette procédure est uniquement nécessaire s'il n'existe aucune règle de chiffrement pour le fichier d'archivage à créer.

Cependant, si une telle règle de chiffrement existe, les fichiers contenus dans le fichier d'archivage créé ne sont pas chiffrés. Cependant, le fichier d'archivage lui-même est chiffré selon la règle de chiffrement définie à cet effet, et donc protégé de manière sécurisée contre tout accès non autorisé.

Une autre façon de s'assurer que les fichiers sont compressés sous forme chiffrée dans un fichier d'archivage consiste à définir les programmes de compression comme une *application non gérée*. Si nécessaire, le responsable de la sécurité (RPS/RS) ou l'administrateur système peut configurer cela via la stratégie de groupe (GPO) *u.trust LAN Crypt*.

## Synchronisation Cloud

Lors de l'installation, des applications de synchronisation cloud connues, y compris Microsoft OneDrive, Google Drive, Nextcloud et BoxDrive, sont automatiquement configurées pour être enregistrées dans l'application. Par défaut, l'accès au contenu des fichiers chiffrés est interdit à ces applications ainsi qu'à tous leurs processus subordonnés.

Si vous souhaitez étendre cette restriction à des applications cloud supplémentaires et à leurs processus subordonnés afin d'empêcher l'accès au contenu des fichiers chiffrés, vous pouvez ajouter des applications de synchronisation cloud supplémentaires dans le registre système :

Clé : `HKLM\SYSTEM\CurrentControlSet\Services\cplcdt2\Parameters`

Paramètre : `IgnoredCloudSyncApps`

Type : `REG_MULTI_SZ`

## Chiffrement initial et chiffrement explicite

Une fois l'installation de *u.trust LAN Crypt* terminée, vous devez effectuer le processus de chiffrement initial. Pendant ce processus, tous les fichiers sont chiffrés à l'aide du profil de chiffrement chargé. Ce chiffrement initial peut être effectué à l'aide des éléments suivants:

- l'icône de la barre d'état de *u.trust LAN Crypt*, voir Application utilisateur
- les extensions de l'Explorateur *u.trust LAN Crypt*, voir Extensions de l'Explorateur
- l'outil lcinit.exe, qui prend également en charge le mode sans assistance, voir Initial encryption in Unattended mode

En plus d'effectuer le chiffrement initial de dossiers entiers, l'outil de ligne de commande **lcinit.exe**, associé aux extensions de l'Explorateur, peut également être utilisé pour chiffrer, déchiffrer et chiffrer à nouveau des fichiers individuels.

**Remarque**

- Lors du chiffrement initial, les fichiers s'affichent par ordre lexicographique.

Un chiffrement, déchiffrement ou rechiffrèrent explicite ciblé peut être nécessaire dans les cas suivants:

- Si les fichiers simples (non chiffrés) sont situés dans un répertoire pour lequel une règle de chiffrement existe.
- Si les fichiers chiffrés sont situés dans un répertoire pour lequel il n'existe aucune règle de chiffrement.
- Si les fichiers d'un répertoire chiffré sont chiffrés avec la mauvaise clé.
- Si les règles de chiffrement contenues dans le profil de chiffrement ont changé.
- Si les fichiers sont chiffrés avec plusieurs clés.

**Assistant de chiffrement initial**

L'outil de chiffrement initial **lcinit.exe** propose un assistant avec interface utilisateur graphique. Cet assistant prend en charge

- le chiffrement, déchiffrement et rechiffrèrent des fichiers
- la vérification de l'état de chiffrement des fichiers, et ce, même dans les dossiers et sous-dossiers

Vous pouvez démarrer cet **assistant**

- en cliquant sur l'icône de la barre des tâches ou
- en accédant à `Start/u.trust LAN Crypt Client/Initial encryption`
- en double-cliquant sur **lcinit.exe** dans le dossier du programme

**Remarque**

- Les processus de chiffrement, déchiffrement et rechiffrèrent s'effectuent toujours en fonction du profil de chiffrement. C'est pourquoi vous devez charger un profil de chiffrement.2

**Exécution du chiffrement initial**

**Étape 1:** Démarrez l'assistant, voir Menu utilisateur.

**Étape 2:** Sélectionnez l'option Effectuer le chiffrement initial à l'étape 1/5.

**Étape 3:** Cliquez sur **Suivant**. **Étape 4:** Définissez maintenant le mode de traitement des fichiers à l'étape 2/5.

- **Fichiers chiffrés selon le profil:** Si vous sélectionnez cette option, les fichiers seront chiffrés selon les règles contenues dans le profil de l'utilisateur (paramètre par défaut). Si le système trouve des fichiers déjà chiffrés, ils seront ignorés.
- **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 appropriée.

  **Remarque**

  - Une condition préalable à cette procédure est que la clé qui a été utilisée pour chiffrer le ou les fichier(s) en premier lieu soit contenue dans le profil de l'utilisateur.

**Étape 5:** Cliquez sur **Suivant**. **Étape 6:** Spécifiez maintenant à l'étape 3/5 les lecteurs, dossiers et sous-dossiers que vous souhaitez inclure dans le processus de chiffrement initial ou de déchiffrement. Les dossiers spécifiés dans les règles peuvent être sélectionnés à l'aide du bouton Règles de profil.

Les lecteurs et dossiers sélectionnés sont marqués d'une coche. Une coche avec un signe « + » supplémentaire en regard d'un dossier indique que ce dernier contient d'autres sous-dossiers qui ne sont pas en cours de traitement. Cela signifie qu'aucun chiffrement/déchiffrement de fichiers n'est effectué. Si ces éléments doivent également être traités, ils doivent alors eux aussi être marqués d'une coche par un clic de souris.

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

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

**Remarque**

- Les paramètres qui peuvent être modifiés par l'utilisateur dépendent de la configuration du client *u.trust LAN Crypt*. Le responsable de la sécurité définit la configuration de manière centralisée.

- **Déchiffrer les fichiers EFS chiffrés si nécessaire:** Sélectionnez cette option pour déchiffrer et chiffrer à nouveau les fichiers EFS chiffrés. Notez qu'une règle de chiffrement doit s'appliquer à ces fichiers. Si vous ne sélectionnez pas cette option, l'assistant de chiffrement initial ignorera les fichiers chiffrés EFS. Ils ne seront donc pas chiffrés à nouveau par *u.trust LAN Crypt*, même si une règle de chiffrement a été spécifiée pour eux.

- **Décompresser les fichiers NTFS compressés si nécessaire:** Sélectionnez cette option pour décompresser les fichiers NTFS compressés et les chiffrer. Notez qu'une règle de chiffrement doit s'appliquer à ces fichiers.

Si vous ne sélectionnez pas cette option, l'assistant de chiffrement initial ignorera les fichiers NTFS compressés. Ils ne seront donc pas chiffrés, même si une règle de chiffrement a été spécifiée pour eux.

- **Déchiffrer/chiffrer de nouveau les fichiers chiffrés avec plusieurs clés:** Sélectionnez cette option pour chiffrer à nouveau les fichiers qui ont été chiffrés avec plusieurs clés. Les fichiers sont chiffrés à l'aide d'une seule clé. Notez qu'une règle de chiffrement doit s'appliquer à ces fichiers.

  **Remarque**

  - Cette option n'est disponible que si l'option **Fichiers chiffrés selon le profil** ou **Fichiers chiffrés à nouveau selon le profil** a été sélectionnée à l'étape 2/5. Dans le cas contraire, elle est grisée.

- **Inclure les types de fichiers suivants uniquement:** Sélectionnez les types de fichiers auxquels vous souhaitez restreindre le processus de chiffrement initial (par exemple .docx, .pdf, txt). Ce paramètre ne s'applique qu'aux fichiers pour lesquels une règle de chiffrement existe. Si le dossier contient des fichiers de différents types, ceux-ci ne seront pas traités lors du chiffrement initial. Ils ne seront chiffrés que lors de leur ouverture et enregistrement par l'utilisateur. Pour spécifier plusieurs types de fichiers, utilisez une liste séparée par des points-virgules.

**Étape 7:** Cliquez sur **Suivant**. **Étape 8:** Définissez maintenant quels fichiers doivent être inclus dans le rapport de chiffrement initial à l'étape 4/5. Pour le rapport de chiffrement initial, l'utilisateur peut choisir entre les options suivantes:

- **Signaler uniquement les erreurs:** Le rapport d'état n'inclura que les fichiers pour lesquels des erreurs sont survenues lors du chiffrement.

- **Signaler les fichiers modifiés et les erreurs:** Le rapport d'état inclura tous les fichiers qui ont été modifiés et pour lesquels des erreurs sont survenues lors du chiffrement.

- **Signaler tous les fichiers:** Le rapport d'état inclura tous les fichiers.

**Étape 9:** Cliquez sur **Suivant**. Le **résultat** du chiffrement, le **nom de clé 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 des fichiers individuels, vous pouvez immédiatement réessayer de les chiffrer en appuyant sur le bouton **Réessayer**.

Vous pouvez trier les résultats par ordre alphabétique en cliquant sur l'en-tête de la colonne. En outre, vous pouvez enregistrer le rapport d'état en tant que fichier XML à l'emplacement de fichier de votre choix (bouton **Exporter**). Par la suite, vous pourrez réessayer de chiffrer les fichiers pour lesquels le chiffrement a échoué à l'aide du rapport d'état.

**Étape 10:** Cliquez sur **Terminer**. Cette action ferme l'assistant.

#### Vérification de l'état de chiffrement

**Étape 1:** Démarrez l'assistant.

**Étape 2:** Sélectionnez l'option **Vérifier l'état du chiffrement** à l'étape 1/5.

**Étape 3:** Cliquez sur **Suivant**.

**Étape 4:** Sélectionnez tous les lecteurs et dossiers que vous souhaitez vérifier à l'étape 2/5.

**Étape 5** Marquez les lecteurs et les dossiers d'une coche pour les sélectionner.

Un signe « + » indique que le dossier contient des sous-dossiers qui ne seront pas traités. L'état du chiffrement n'est donc pas vérifié.

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

Cliquez sur **Avancé** pour restreindre la vérification à des types de fichiers spécifiques:

- **Inclure les types de fichiers suivants uniquement:** Si vous indiquez des types de fichiers spécifiques ici (par exemple : .txt, .docx, .pdf), seuls les fichiers des types spécifiés seront vérifiés. Si un dossier contient également des fichiers d'un type différent (non spécifié ici), ceux-ci ne seront pas pris en compte. Pour spécifier plusieurs types de fichiers, utilisez une liste séparée par des points-virgules.

**Étape 6:** Cliquez sur **Suivant**.

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

Vous pouvez trier les résultats par ordre alphabétique en cliquant sur l'en-tête de la colonne.

Cliquez sur **Exporter** pour enregistrer le rapport d'état en tant que fichier XML à l'emplacement de fichier de votre choix.

**Étape 7:** Cliquez sur **Terminer**. Cette action ferme l'assistant.

#### Déchiffrement de fichiers

Les fichiers chiffrés par *u.trust LAN Crypt* peuvent être déchiffrés si plus aucune règle de chiffrement ne s'y applique. Si un chiffrement initial doit à nouveau être effectué, par exemple en raison de règles de chiffrement modifiées dans le profil de l'utilisateur, les fichiers pour lesquels les règles de chiffrement n'existent plus peuvent être déchiffrés via cet assistant.

Pour déchiffrer des fichiers:

1. Sélectionnez **Effectuer le chiffrement initial** à l'étape 1/5 de l'assistant.
2. Sous **Déchiffrement** à l'étape 2/5, sélectionnez **Décrypter les fichiers avec les clés sélectionnées**.
3. Vous pouvez ensuite sélectionner les clés.

Seuls les fichiers chiffrés avec les clés sélectionnées seront déchiffrés. Cependant, ils ne seront déchiffrés que si plus aucune règle de chiffrement ne s'y applique.

**Remarque**

- *u.trust LAN Crypt* ne déchiffre que les fichiers pour lesquels aucune règle de chiffrement ne s'applique.

**Exemple:** La modification du profil utilisateur entraîne le démarrage de l'assistant de chiffrement initial. Pour vous assurer que tous les fichiers disposent de l'état de chiffrement prévu après la fermeture de l'assistant de chiffrement initial, procédez comme suit:

1. Activez l'option **Fichiers chiffrés selon le profil:** Tous les fichiers sont chiffrés conformément au nouveau chiffrement.
2. Activez l'option **Fichiers chiffrés à nouveau selon le profil:** Si, conformément aux nouvelles règles, les fichiers doivent être chiffrés à l'aide d'une clé différente, le chiffrement est à nouveau effectué.
3. Activez l'option **Déchiffrer les fichiers avec les clés sélectionnées puis sélectionnez *toutes les clés:*** *Les fichiers chiffrés pour lesquels il n'existe plus de règle de chiffrement seront déchiffrés. *u.trust LAN Crypt* ne déchiffre que les fichiers pour lesquels il n'existe pas de règle de chiffrement. Par conséquent, sélectionner toutes les clés ne causera aucun problème.

Une fois le processus terminé et l'assistant fermé, tous les fichiers disposent de l'état de chiffrement approprié.

Si le **chiffrement persistant** est activé, le déchiffrement explicite des fichiers peut être important. Dans ce cas, les fichiers ne sont pas automatiquement déchiffrés au moment de leur copie/ déplacement à partir d'un répertoire pour lequel une règle de chiffrement s'applique vers un répertoire ne comportant aucune règle de chiffrement.

**Chiffrement initial en mode sans assistance**

Si vous souhaitez exécuter l'outil **lcinit.exe** en mode sans assistance, vous devez appeler **lcinit.exe** à partir de la ligne de commande avec des paramètres spécifiques, depuis le dossier dans lequel il se trouve (par exemple, `C:\Programmes\Utimaco\u.trust LAN Crypt\Apps\`).

**Syntaxe de ligne de commande:**

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

**Paramètres:**

**Chemin de départ**

Il en résulte soit un fichier unique devant être chiffré, déchiffré ou chiffré à nouveau (par exemple, `C:\Data\sales.docx`), soit un dossier dans lequel le chiffrement, le déchiffrement ou le rechiffrèrent doit être effectué par exemple, `D:\Data`. Le paramètre par défaut indique que les sous-dossiers ne sont pas inclus dans ce processus!

**%Profile**

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

**Remarque**

- Pour qu'un fichier puisse être déchiffré, le profil doit contenir une règle d'EXCLUSION.

**/s**

Inclut tous les sous-dossiers du chemin de départ.

**/h ou /?**

Ouvre une fenêtre qui affiche l'aide sur la syntaxe utilisée dans **lcinit.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 en fonction du profil de chiffrement, si nécessaire.

**/Tr**

Mode de tâche: r = chiffre à nouveau les fichiers en fonction du profil de chiffrement, si nécessaire.

**/Td**

Mode de tâche: d = déchiffre les fichiers en fonction du profil de chiffrement, si nécessaire.

**/Tdk**

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

**Remarque**

- Tous les paramètres de mode de tâche peuvent être utilisés ensemble dans un seul appel de commande.

**/Dc**

Cette option décompresse les fichiers compressés au format NTFS avant de les chiffrer. Si cette option n'est pas définie, les fichiers compressés au format NTFS sont ignorés.

**/De**

Cette option déchiffre les fichiers chiffrés au format EFS avant de les chiffrer à nouveau. Si cette option n'est pas définie, les fichiers chiffrés au format EFS sont ignorés.

**/Dm**

Cette option déchiffre les fichiers chiffrés avec plusieurs clés avant de les chiffrer à nouveau. En conséquence, les fichiers sont chiffrés à l'aide d'une seule clé.

**+Ffiletype**

Si vous spécifiez des types de fichiers à l'aide de cette option (par exemple +Ftxt ou +Fdocx), seuls les fichiers du type pertinent sont traités. Ce paramètre n'affecte que les fichiers pour lesquels une règle de chiffrement existe.

Si un dossier contient également des fichiers d'un type différent n'ayant pas été spécifié avec cette option, lesdits fichiers ne sont pas pris en compte lors du chiffrement initial. Ils ne seront chiffrés que lors de leur ouverture et enregistrement par l'utilisateur.

**Exemple:** Le fichier « *123.pdf* » n'est pas chiffré car les fichiers du type « PDF » de l'exemple ci-dessus ne doivent pas être chiffrés lors du chiffrement initial. Si l'utilisateur ouvre ce fichier, par exemple avec un éditeur PDF, avant de l'enregistrer dans le même dossier, ledit fichier est alors chiffré. Si l'utilisateur copie un tel fichier à partir de ce dossier avant de l'y coller à nouveau, le fichier est également chiffré. Cependant, cela n'est possible que si la règle de chiffrement définie pour le dossier s'applique également aux fichiers de type « PDF ».

**/V0**

Mode détaillé 0 : Pas de rapport.

**/V1**

Mode détaillé 1 : Répertorie les messages d'erreur.

**/V2**

Mode détaillé 2 : Répertorie les fichiers modifiés.

**/V3**

Mode détaillé 3 : Répertorie tous les fichiers.

**/V4**

Mode détaillé 4 : Répertorie les fichiers simples.

**/E**

Arrêter lors d’une erreur.

**/X**

Chiffrement initial sans affichage de fenêtre.

**/LLogfile**

Consigner les résultats dans le fichier indiqué.

**Remarque**

- Le paramètre /Td ne doit être combiné avec %Profile que lorsque les fichiers que vous souhaitez déchiffrer sont répertoriés dans le profil avec une règle d’exclusion. Dans le cas contraire, vous devez utiliser /Td avec le chemin de départ.

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

lcinit.exe D:\data /S /V4
```

Répertorie tous les fichiers simples dans `D:\data` et ses sous-dossiers.

---

# Stratégies

## Certificats

Pour que les utilisateurs puissent accéder à leur profil de chiffrement, le certificat correspondant doit être disponible sur l'ordinateur. Le responsable de la sécurité distribue ces certificats aux utilisateurs. Les utilisateurs importent ensuite le certificat sur leur propre machine. Si les certificats sont disponibles à la première connexion, l'ensemble du processus s'exécute sans aucune interaction utilisateur.

*u.trust LAN Crypt* propose une option d'importation automatique des certificats lors du premier chargement du profil de chiffrement. Dans ce cas, le responsable de la sécurité configure le système de sorte que *u.trust LAN Crypt* puisse trouver un fichier de certificat lors de la connexion et commencer à importer le certificat automatiquement. L'utilisateur est invité une fois à saisir le code PIN pour le fichier clé PKCS#12.

**Remarque**

- Le responsable de la sécurité est en charge de distribuer aux utilisateurs le code PIN requis pour l'importation automatique d'un certificat.

Le certificat est vérifié chaque fois que le profil de chiffrement est chargé. Si un certificat valide est trouvé, l'utilisateur est connecté à *u.trust LAN Crypt*. Si aucun certificat valide n'est trouvé, l'utilisateur n'est pas en mesure de travailler avec des données chiffrées.

**Remarque** Les utilisateurs qui tentent de se connecter à *u.trust LAN Crypt* et font face à l'échec de la connexion reçoivent un message d'erreur leur indiquant la raison de cet échec.

Les règles de chiffrement spéciales incluses dans les profils de chiffrement de *u.trust LAN Crypt* permettent aux utilisateurs d'accéder aux données chiffrées. Ces règles définissent précisément quels fichiers de répertoires particuliers doivent être chiffrés par chaque clé. Le profil de chiffrement d'un utilisateur a uniquement besoin d'être chargé. Le chiffrement et le déchiffrement ont lieu en arrière-plan (de manière transparente).

L'utilisateur ne remarque pas l'exécution des tâches de chiffrement/déchiffrement.

**Remarque**

- Les certificats CA sont uniquement acceptés comme étant corrects s'ils sont stockés dans le magasin de certificats sous « Autorités de certification racines de confiance ». *u.trust LAN Crypt* importe cependant les certificats CA, qui peuvent être contenus dans les fichiers clés PKCS#12, ainsi que les certificats utilisateur dans le dossier « Mes certificats - Certificats ». Pour éviter les messages d'erreur, les certificats CA du magasin de certificats doivent être déplacés manuellement vers « Autorités de certification racines de confiance ». Si vous utilisez des certificats générés par *u.trust LAN Crypt*, une telle étape n'est pas nécessaire.

### Lecteurs de cartes à puce

Comme l'utilisation des certificats est gérée par les Cryptographic Service Providers (CSPs) et les Key Storage Providers (KSPs), les lecteurs de cartes à puce sont automatiquement pris en charge lorsqu'un KSP pour cartes à puce est utilisé. Vous pouvez donc gérer l'accès aux informations de chiffrement en utilisant des certificats sur les cartes à puce.

**Remarque**

- Si vous souhaitez utiliser des certificats sur des cartes à puce, assurez-vous que le lecteur de carte à puce, l'intergiciel associé et un Fournisseur de service ou de stockage (CSP ou KSP) correspondant sont correctement installés et opérationnels !

**Remarque**

- Veuillez également noter que les Cryptographic Service Provider (CSP) pour les opérations clés de u.trust LAN Crypt ne sont désormais pris en charge qu'en association avec des shims qui les rendent accessibles en tant que Key Storage Provider (KSP).

## Chargement du fichier de stratégie

#### Comportement par défaut de *u.trust LAN Crypt*

Lorsqu'un utilisateur se connecte à Windows, son profil en cache est chargé en premier. *u.trust LAN Crypt* vérifie si un nouveau fichier de stratégie est disponible pour l'utilisateur en établissant une connexion vers l'emplacement spécifié dudit fichier (lecteur réseau ou serveur web). Si un nouveau fichier de stratégie est trouvé, le profil utilisateur en cache est mis à jour.

L'utilisateur peut commencer à travailler avec des fichiers chiffrés pendant que *u.trust LAN Crypt* vérifie s'il existe une nouvelle version du fichier de stratégie. Si l'emplacement spécifié n'est pas accessible, l'utilisateur travaille avec le profil utilisateur en cache jusqu'à ce qu'il puisse être mis à jour.

**Remarque**

- *u.trust LAN Crypt* vérifie les certificats de l'utilisateur et du responsable (principal) de la sécurité. Si les certificats contiennent un point de distribution de la liste de révocation des certificats (CRL) et qu'aucune CRL valide n'est présente dans le système, Windows essaie d'importer la CRL à partir de l'adresse spécifiée. Si un pare-feu est installé, vous pouvez voir un message indiquant qu'un programme (loadprof.exe) tente d'établir une connexion à Internet. Dans certains cas, le téléchargement du profil utilisateur peut également provoquer l'affichage de ce message.

#### Comportement défini par les responsables de la sécurité

Le responsable de la sécurité peut modifier le comportement par défaut à l'aide des paramètres centraux. Les responsables de la sécurité peuvent spécifier la durée de validité de la stratégie en cache sur les ordinateurs clients. Ils peuvent définir des intervalles de mise à jour pour les fichiers de stratégie. Les paramètres définis par le responsable de la sécurité apparaissent dans l'onglet Profil de la boîte de dialogue État du client. Voir Boîte de dialogue État du client.

Dans la période définie ici, le fichier de stratégie est valide sur le client et l'utilisateur peut accéder aux données chiffrées, même s'il n'y a pas de connexion à l'emplacement du fichier de stratégie.

Lorsque la période spécifiée expire, *u.trust LAN Crypt* tente de charger le fichier de stratégie à partir du lecteur réseau pour le mettre à jour à nouveau. Si cela est impossible, le fichier de stratégie est déchargé. L'utilisateur ne peut alors plus accéder aux données chiffrées. Ce fichier est mis à jour et chargé à nouveau lorsqu'un fichier de stratégie valide est mis à disposition (par exemple à l'ouverture de session suivante, avec connexion à l'emplacement client des fichiers de stratégie). L'utilisateur peut ainsi à nouveau accéder aux données chiffrées. Le compteur relatif à la durée du stockage en cache est réinitialisé.

Spécifier la durée du stockage en cache permet aux responsables de la sécurité de s'assurer que les ordinateurs clients reçoivent régulièrement des fichiers de stratégie à jour, et que les utilisateurs travaillent à tout moment avec des stratégies à jour. Ils peuvent empêcher les utilisateurs de travailler avec les mêmes fichiers de stratégie pendant une période illimitée. Notez que si cette option n'est **pas configurée**, un utilisateur peut continuer à travailler avec une version en cache du fichier de stratégie pendant une période illimitée.

Le compteur relatif à la durée de stockage en cache autorisée est réinitialisé dans les situations suivantes:

- L'emplacement de stockage des fichiers de stratégie est accessible et un fichier de stratégie valide a été transféré au client (par exemple lors de la connexion de l'utilisateur, ou suite au déclenchement par un intervalle de mise à jour spécifié). Cependant, le fichier de stratégie n'est pas nouveau par rapport au fichier existant.
- Un nouveau fichier de stratégie est disponible et a été chargé avec succès.

Le compteur pour la durée de stockage du cache autorisée ne sera PAS réinitialisé dans les situations suivantes:

- 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, il n'a pas pu être chargé en raison d'une erreur.

- Un nouveau fichier de stratégie est disponible. Cependant, il nécessite un nouveau certificat. L'utilisateur n'a pas ce certificat ou il n'a pas été chargé.

Si la mise à jour du fichier de stratégie échoue, l'heure d'expiration du fichier de stratégie mis en cache sera affichée dans une infobulle sur l'ordinateur client. L'utilisateur peut alors lancer une mise à jour manuelle via l'icône de bac de *u.trust LAN Crypt*, voir Menu utilisateur.

#### Les fichiers de stratégie ne sont pas mis en cache.

Un agent de sécurité peut préciser que le fichier de stratégie ne sera pas mis en cache. Cela signifie que les utilisateurs reçoivent leurs profils lors de la connexion, si l'emplacement du fichier de stratégie est accessible. S'il n'est pas accessible ou si une erreur se produit lors du chargement du profil, l'utilisateur ne peut pas accéder aux fichiers chiffrés.

## Se connecter à *u.trust LAN Crypt*

Les profils de chiffrement de *u.trust LAN Crypt* sont créés par un responsable de la sécurité, conformément à la stratégie de sécurité de l'entreprise, puis stockés dans des fichiers de stratégie. Un profil de chiffrement ne peut être chargé que si l'utilisateur possède le certificat correspondant.

Le chemin du fichier de stratégie est écrit dans le registre d'une machine client par l'administrateur système ou l'agent de sécurité. Cela se fait via une stratégie de groupe *u.trust LAN Crypt*. Lorsqu'un utilisateur se connecte à *u.trust LAN Crypt*, le profil de chiffrement, qui est stocké dans le fichier de stratégie, est chargé sur la machine client. Le client *u.trust LAN Crypt* charge les fichiers de stratégie à partir de l'emplacement défini (par exemple un partage réseau) et vérifie si l'utilisateur est autorisé à le charger, en analysant le certificat de l'utilisateur.

### Se connecter avec un jeton

Les utilisateurs peuvent également se connecter à *u.trust LAN Crypt* à l'aide d'un jeton. Pour utiliser cette méthode d'ouverture de session, le certificat utilisateur *u.trust LAN Crypt* de l'utilisateur doit être stocké sur le jeton. Si le certificat utilisateur se trouve sur un jeton connecté au système, l'utilisateur est connecté.

Lorsque vous utilisez des jetons pour vous connecter, *u.trust LAN Crypt* peut essayer de charger un fichier de stratégie avant que le jeton puisse être identifié par le système d'exploitation. Dans ce cas, un message s'affiche indiquant que le certificat utilisateur n'a pas pu être trouvé, bien que le jeton soit connecté au système.

L'utilisateur doit charger le fichier de stratégie manuellement via l'application utilisateur dans la barre d'outils > **Charger les règles de chiffrement**. Le jeton est identifié et l'utilisateur est connecté. Pour éviter cela, un temps de chargement des profils peut être spécifié dans **la configuration *u.trust LAN Crypt*** (paramètre **Temps de chargement des profils**).

---

# Application utilisateur

L'état de *u.trust LAN Crypt* est représenté par une icône clé dans la barre des tâches Windows.

**Vert signifie:** Les règles de chiffrement sont chargées et le chiffrement transparent est activé.

**Jaune signifie:** Les règles de chiffrement sont chargées, mais le chiffrement transparent est désactivé.

**Rouge signifie:** Aucun profil n'est chargé.

## Menu utilisateur

Faites un clic droit sur l'icône clé pour ouvrir le menu utilisateur *u.trust LAN Crypt* qui offre 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 le profil**
- **Statut du client**
- **Cryptage initial**
- **Fermer**
- **À propos**

  **Remarque**

  - Les commandes du menu disponibles dépendent de la configuration du client *u.trust LAN Crypt*. Le responsable de la sécurité définit la configuration de manière centralisée.

**Charger / mettre à jour les règles de chiffrement**

Cette option charge les règles de chiffrement actuellement valides. Cela est important si le profil a été modifié pendant l'exécution.

**Effacer les règles de chiffrement**

Cette option empêche l'accès aux données chiffrées. Il s'agit d'une option de sécurité qui sécurise les données chiffrées contre tout accès non autorisé lorsque le poste de travail est laissé sans surveillance. Veuillez noter que l'utilisation de la clé privée doit être sécurisée à l'aide d'un mot de passe. Dans le cas contraire, le profil peut être rechargé à l'aide de la commande **Charger les règles de chiffrement**.

**Désactiver/activer le chiffrement**

Active ou désactive le chiffrement transparent. La désactivation du chiffrement est utilisée dans les cas où les fichiers doivent rester chiffrés lors de leur copie ou déplacement vers un dossier qui ne comporte aucune règle de chiffrement valide. Avec le chiffrement actif, les fichiers sont déchiffrés en cas de copie vers ce type de dossier.

Par exemple, en cas de chiffrement transparent actif, un fichier chiffré joint à un e-mail est déchiffré automatiquement. Si le chiffrement transparent est désactivé, le fichier chiffré peut être envoyé en pièce jointe.

**Remarque**

- Si l'administrateur a activé la fonction de chiffrement persistant, les fichiers chiffrés restent chiffrés, et ce, même en cas de copie ou de déplacement vers un emplacement pour lequel aucune règle de chiffrement n'a été spécifiée.

**Afficher le profil** Affiche les règles de chiffrement et les clés contenues dans les informations de chiffrement dans deux onglets.

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

La page de l'onglet *Clés disponibles* répertorie toutes les clés disponibles pour l'utilisateur actuel.

**État du client**

L'option **État du client** utilise plusieurs onglets pour afficher des informations détaillées sur l'état actuel du client *u.trust LAN Crypt*, voir Boîte de dialogue État du client.

**Cryptage initial**

Démarre l'assistant qui va chiffrer tous les fichiers à l'aide du profil de chiffrement chargé, voir Chiffrement initial et chiffrement explicite.

**Fermer**

Ferme l'application utilisateur *u.trust LAN Crypt*.

**À propos**

Affiche des informations relatives à votre version actuelle de *u.trust LAN Crypt*.

**Remarque**

- L'option **Fermer** ferme uniquement l'application utilisateur *u.trust LAN Crypt*. *u.trust LAN Crypt* reste dans son état actuel. Cela signifie que le chiffrement transparent ou le déchiffrement continue. La fermeture de l'application utilisateur ne protège pas vos fichiers contre les accès non autorisés (par exemple, lorsque vous quittez votre poste de travail).

## Boîte de dialogue État du client

L'option **Statut du client** affiche plusieurs onglets qui fournissent des informations sur les paramètres de chiffrement relatifs à la machine d'un utilisateur.

Ces limites sont les suivantes:

**Statut**

Cet onglet indique si le profil 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 ayant créé le fichier, etc.).

Si le profil utilisateur a été chargé, le chiffrement est également actif. Cependant, le chiffrement peut aussi être désactivé (temporairement) lorsque le profil utilisateur a été chargé. Voir « Menu utilisateur, commande **Désactiver/activer le chiffrement** ».

**Paramètres** Cet onglet fournit des informations sur les paramètres qui s'appliquent actuellement au client. Ces paramètres sont définis de manière centralisée et se réfèrent au chiffrement, à l'icône de la barre d'état et aux paramètres de **l'assistant de chiffrement initial**. Entre autres détails, cet onglet indique si le **chiffrement persistant** a été activé ainsi que les options de menu mises à disposition sur les ordinateurs clients.

**Profil** Cet onglet affiche les paramètres du profil utilisateur.

**Certificats** Cet onglet affiche les détails du certificat utilisateur (émetteur, numéro de série, validité) ainsi que les règles qui s'appliquent au client concernant la vérification de ce certificat.

**Clés** Cet onglet affiche des informations sur toutes les clés disponibles du profil actuellement chargé.

**Règles** Cet onglet répertorie toutes les règles de chiffrement qui s'appliquent à l'utilisateur actuel.

**Non géré** Cet onglet fournit des informations sur les applications, les lecteurs de disque et les périphériques non gérés. De plus, les règles d'ignorance et de bypass actives de l'utilisateur actuel sont listées.

Par défaut, *u.trust LAN Crypt* traite certaines applications comme des « applications non gérées ». Ces applications apparaissent également dans cet onglet.

**Applications** Cet onglet affiche les programmes qui, en raison de leur comportement, nécessitent une approche spéciale de la part de *u.trust LAN Crypt*.

**Logiciel antivirus**

Afin d'analyser des fichiers chiffrés, les logiciels antivirus ont besoin de la clé qui a été utilisée pour chiffrer lesdits fichiers. Le logiciel antivirus spécifié par le responsable de la sécurité dans cet onglet a accès à toutes les clés et peut donc également 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 confirmées par des fournisseurs de confiance, ces fournisseurs doivent être enregistrés dans l'administration *u.trust LAN Crypt*. Tous les fournisseurs de confiance enregistrés et les informations de certificat correspondantes sont répertoriés dans cet onglet.

Bouton **Exporter**

Utilisez le bouton **Exporter** pour exporter les paramètres actuels du client vers un fichier XML.

De cette façon, les équipes de support peuvent facilement recevoir des informations de configuration importantes.

## Extensions de l'Explorateur

Les extensions de l'Explorateur de *u.trust LAN Crypt* offrent les fonctionnalités suivantes:

- Chiffrement en fonction du profil (fichiers, dossiers et lecteurs);
- Chiffrement et déchiffrement explicites des fichiers, dossiers et lecteurs ;
- Contrôle facile de l'état de chiffrement de vos données.

*u.trust LAN Crypt* ajoute des options de menu à l'Explorateur Windows. Ces options apparaissent dans les menus contextuels des lecteurs, dossiers et fichiers. De plus, un onglet est ajouté à la fenêtre Propriétés Windows pour les fichiers. Ce nouvel onglet contient des informations sur l'état du chiffrement.

Vous pouvez cliquer avec le bouton droit sur un fichier ou un dossier pour afficher l'entrée *u.trust LAN Crypt* dans son menu contextuel. Les clés de différentes couleurs indiquent l'état 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 simple (non chiffré) mais doit être chiffré conformément à une règle de chiffrement contenue dans le profil chargé.

**Clé jaune:** L'affichage d'une clé jaune indique que le fichier est chiffré, mais que le chiffrement transparent est actuellement désactivé.

**Clé jaune avec point d'interrogation:** Les droits d'accès de l'utilisateur sont insuffisants. *u.trust LAN Crypt* n'est donc pas en mesure de déterminer l'état de chiffrement.

**Remarque**

- Aucun symbole de clé n'est affiché pour les fichiers définis avec l'attribut hors ligne (par exemple, pour les fichiers physiquement inexistants).
- Des symboles de clés sont également ajoutés aux fichiers dans l'Explorateur Windows lui-même. Si une règle de chiffrement existe pour des lecteurs ou des dossiers entiers, ceux-ci sont également marqués d'un symbole de clé. À cet

emplacement, les clés de différentes couleurs affichent également l'état du chiffrement.

L'entrée *u.trust LAN Crypt* du menu contextuel ouvre un sous-menu contenant d'autres entrées. Ces entrées varient selon qu'un dossier ou un fichier a été sélectionné et l'état de chiffrement dans lequel se trouve un fichier.

**Options de menu pour les dossiers**

**État du chiffrement**

Cette option affiche une liste de tous les fichiers de ce dossier et leur état de chiffrement (clés colorées). Seuls les fichiers du premier niveau de dossier sont affichés. Pour afficher les fichiers d'un sous-dossier, il vous faut d'abord accéder à ce sous-dossier. Dans l'Explorateur, une icône de clé permet de reconnaître les dossiers pour lesquels une règle de chiffrement existe.

**Chiffrement selon le profil**

Cette option chiffre tous les fichiers du dossier en fonction du profil de chiffrement chargé. Les sous-dossiers avec une règle de chiffrement existante sont également inclus dans le chiffrement. Une barre de progression indique le temps que le **chiffrement initial** est susceptible de prendre. Vous pouvez également voir le nombre total de fichiers que contient le dossier, ainsi que le nombre de fichiers ayant déjà été chiffrés. Cela vous permet aussi de consulter le chemin du fichier en cours de chiffrement.

**Chiffrer**

Cette option chiffre tous les fichiers du dossier. Cette opération est effectuée à l'aide d'une clé mise à disposition dans le profil de chiffrement actif. Une liste des clés disponibles s'affiche, à partir de laquelle il est possible de sélectionner la clé à utiliser pour chiffrer tous les fichiers.

**Remarque**

- Si une règle de cryptage existe pour les fichiers d'un dossier et que tous ces fichiers ne sont pas (déjà) cryptés selon la règle, un message d'erreur peut apparaître pendant le cryptage après avoir marqué le répertoire ou le dossier et sélectionné l'option *Chiffrer*.

**Exemple:** Marquez un dossier dans lequel au moins un des fichiers qu'il contient a une règle de cryptage avec par exemple "Clé-1", sélectionnez une autre Clé, par exemple "Clé-2", via l'option *Chiffrer* et cliquez sur **Ok**.

**Remarque**

- Pour les dossiers qui ont déjà une règle de cryptage, cryptez-les en utilisant plutôt l'option "*Chiffrement selon le profil*". Vous pouvez également crypter les fichiers en utilisant le menu utilisateur *u.trust LAN Crypt*.

**Déchiffrer**

Cette option déchiffre tous les fichiers du premier niveau de dossier. Par conséquent, toutes les clés pertinentes doivent être disponibles dans le profil de chiffrement actif. Si une clé est manquante, les fichiers qui utilisent cette clé restent chiffrés.

**Déplacement sécurisé**

Lors du déplacement d'un dossier via *u.trust LAN Crypt*, les fichiers contenus dans ce dossier sont chiffrés, déchiffrés ou chiffrés de nouveau au niveau du nouvel emplacement selon les règles de chiffrement qui s'appliquent. Les fichiers sources sont effacés après avoir été déplacés.

**Suppression sécurisée**

Cette option écrit plusieurs fois sur les emplacements de stockage des fichiers. Les fichiers ne peuvent pas être restaurés via la Corbeille Windows.

**Options de menu pour les fichiers individuels**

**État du chiffrement**

Cette option affiche l'état de chiffrement des fichiers. Pour les fichiers chiffrés, une zone d'informations contextuelle affiche la clé utilisée pour le chiffrement ainsi que des informations supplémentaires sur le droit de l'utilisateur d'utiliser cette clé.

Si un autre utilisateur est connecté, mais que ce dernier n'est pas autorisé à utiliser cette clé, le GUID apparaît dans la zone d'informations à la place du nom de la clé.

Vous pouvez identifier les fichiers chiffrés dans l'Explorateur à l'aide de la petite icône de clé verte affichée en regard de ces derniers. En cliquant sur **Options des dossiers** -> **Affichage**, l'utilisateur peut indiquer si l'état de chiffrement du fichier et celui du dossier doivent être affichés pour son profil. Les modifications apportées à ces paramètres ne deviennent effectives qu'une fois que l'utilisateur s'est déconnecté puis reconnecté.

**Chiffrement selon le profil**

Cette option permet de chiffrer un fichier conformément au profil de chiffrement actuellement chargé. Cette entrée n'apparaît dans le menu contextuel que si l'état de chiffrement d'un fichier ne correspond pas au profil de chiffrement.

**Chiffrer**

Cette option permet de chiffrer le fichier sélectionné. Une liste des clés disponibles s'affiche, à partir de laquelle il est possible de sélectionner la clé à utiliser pour le chiffrement.

**Remarque**

- Si une règle de cryptage existe pour les fichiers d'un dossier et que tous ces fichiers ne sont pas (déjà) cryptés selon la règle, un message d'erreur peut apparaître pendant le cryptage après avoir marqué le répertoire ou le dossier et sélectionné l'option *Chiffrer*.

**Exemple:** Marquez un dossier dans lequel au moins un des fichiers qu'il contient a une règle de cryptage avec par exemple "Clé-1", sélectionnez une autre Clé, par exemple "Clé-2", via l'option *Chiffrer* et cliquez sur **Ok**.

**Remarque**

- Pour les dossiers qui ont déjà une règle de cryptage, cryptez-les en utilisant plutôt l'option "*Chiffrement selon le profil*". Vous pouvez également crypter les fichiers en utilisant le menu utilisateur *u.trust LAN Crypt*.

**Déchiffrer**

Cette option permet de déchiffrer le fichier sélectionné. La clé appropriée doit être disponible dans le profil de chiffrement actif. Si ce n'est pas le cas, le fichier reste chiffré.

**Déplacement sécurisé**

Cette option permet, lors du déplacement de fichiers vers un nouvel emplacement, de chiffrer, déchiffrer ou chiffer à nouveau le fichier sélectionné selon les règles de chiffrement chargées. Le fichier source sélectionné est supprimé après avoir été déplacé.

**Suppression sécurisée**

Cette option permet d'écrire plusieurs fois sur les emplacements de stockage du fichier sélectionné. Le fichier ne peut pas être restauré via la Corbeille Windows.

**Remarque**

- Les règles de chiffrement actives sont toujours prioritaires. Si l'utilisateur tente de chiffrer/déchiffrer des fichiers pour lesquels une règle de chiffrement définit quelque chose de différent, sa commande n'est pas exécutée et un message d'erreur s'affiche.

**Les situations suivantes provoquent un message d'erreur lorsqu'un utilisateur tente de chiffrer des fichiers à l'aide des options du menu:**

- Le dossier contient des fichiers chiffrés à l'aide d'une clé inconnue.
- L'utilisateur tente de chiffrer/déchiffrer un fichier en contradiction avec sa règle de chiffrement (par exemple, une clé différente de celle utilisée dans la règle de chiffrement est sélectionnée).

**Informations de chiffrement**

Dans la boîte de dialogue **Propriétés**, l’onglet **État du chiffrement** affiche des informations sur le fichier chiffré.

# Terminal server

Cette version de *u.trust LAN Crypt* prend en charge les serveurs de terminaux Windows et Citrix. Pour obtenir plus de détails sur les versions prises en charge, reportez-vous aux notes de publication de *u.trust LAN Crypt*.

## Pare-feu

Après la connexion d'un utilisateur, *u.trust LAN Crypt* tente de charger le profil utilisateur *u.trust LAN Crypt*. En même temps, il vérifie 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 essaie d'importer le CRL à partir de l'adresse spécifiée. Si un pare-feu est installé, vous pouvez voir un message indiquant qu'un programme (*loadprof.exe*) tente d'établir une connexion à Internet.

## Installation dans un environnement Terminal Server

L'installation du client LAN Crypt sur un serveur terminal s'effectue en principe comme sur un système Windows classique. Cependant, lorsqu'il est utilisé dans un environnement RemoteApp (virtualisation d'applications), des étapes supplémentaires sont nécessaires pour garantir que **LoadProf** ne s'exécute pas globalement pour toute la session, mais uniquement dans le contexte de la RemoteApp.

### Installation dans un environnement RemoteApp (virtualisation d'applications)

#### Préparation avant l'installation

Avant de lancer le package d'installation, l'entrée existante pour *loadprof.exe* doit être supprimée. Ouvrez l'Éditeur du Registre et supprimez l'entrée dans la clé suivante :

```
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Appsetup
```

Si *loadprof.exe* apparaît dans cette valeur, supprimez-le complètement.

#### Installation avec un fichier de transformation (.mst)

Pour exécuter le package d'installation, un fichier de transformation (.mst) doit être créé et intégré.

> **Remarque**
>
> - Veuillez noter que le fichier .mst doit être créé manuellement.

Dans ce fichier .mst, la propriété privée **TerminalServer** doit être définie sur **1** afin que l'installation s'effectue correctement en mode Terminal Server.

#### Exemple de commande d'installation avec fichier .mst :

```
msiexec /i LCClient.msi /qn [autres paramètres] TRANSFORMS="C:\Fichier_Transform.mst"
```

Cette configuration garantit un comportement de démarrage correct dans les scénarios RemoteApp.

> **Remarque**
>
> - Lors de l'installation sur un serveur de terminaux, utilisez une session de connexion locale avec des droits d'administration pour installer *u.trust LAN Crypt*.
> - S'il est prévu d'utiliser Citrix Presentation Server ou Citrix XenApp, installez-les avant *u.trust LAN Crypt*.

## Restrictions

### Citrix

- Le chiffrement en combinaison avec la redirection de lecteurs clients Citrix n'est pas pris en charge.
- Les applications livrées en streaming Citrix ne sont pas prises en charge.

# Installation et mise à niveau

**Remarque**

- Si vous installez les deux composants de *u.trust LAN Crypt*, à savoir la console d'administration et l'application client, sur le même ordinateur, leur version doit être la même.

**Étape 1:** Dans votre package d'installation décompressé, double-cliquez sur l'un des fichiers **DataFileClient.msi** du dossier d'installation de *u.trust LAN Crypt*.

**Étape 2:** Cliquez sur **Suivant**.

La boîte de dialogue Contrat de licence s'affiche.

**Étape 3:** Dans cette boîte de dialogue **Contrat de licence**, sélectionnez **J'accepte le contrat de licence**. Sans cela, l'installation de *u.trust LAN Crypt* est impossible.

**Étape 4:** Cliquez sur **Suivant**.

La boîte de dialogue **Dossier de destination** s'affiche.

**Étape 5:** Sélectionnez où installer *u.trust LAN Crypt*.

**Étape 6:** Cliquez sur **Suivant**.

La boîte de dialogue **Sélectionner le type d'installation** s'affiche.

**Étape 7:** Dans cette boîte de dialogue, vous sélectionnez les composants du client *u.trust LAN Crypt* à installer.

- *Standard*: Installe les fonctions d'application les plus couramment utilisées du client *u.trust LAN Crypt*.
- *Complet*: Installation complète du client, y compris l'API client.
- *Personnalisé*: Permet à l'utilisateur de sélectionner les différents composants.

**Étape 8:** Sélectionnez **Personnalisé** et cliquez sur **Suivant**.

Les composants suivants peuvent être installés:

**Application utilisateur**

Installe l'application utilisateur *u.trust LAN Crypt*, voir Application utilisateur.

**Extensions de shell**

Installe les extensions de l'Explorateur *u.trust LAN Crypt*.

*u.trust LAN Crypt* ajoute des entrées à l'Explorateur Windows, lesquelles permettent le chiffrement initial ainsi que le chiffrement/déchiffrement explicite des fichiers et dossiers, et vous permettent de vérifier facilement l'état du chiffrement de vos données. Ces entrées sont affichées dans les menus contextuels des lecteurs, dossiers et fichiers. De plus, un onglet **Informations de chiffrement** est ajouté à la page des *Propriétés Windows*.

**API client**

Utilisé pour accéder à la fonctionnalité de chiffrement des fichiers *u.trust LAN Crypt* via une API.

**Remarque**

- Pour permettre aux produits de protection contre la perte de données d'accéder aux données à l'aide de l'API client de *u.trust LAN Crypt*, vous devez installer l'API client.

**Filtre réseau**

Utilisé pour accéder à la fonctionnalité de cryptage de fichiers *Utimaco* via une API.

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

**Remarque**

- Veuillez noter que la version 4.1.0 de *u.trust LAN Crypt* ne prend plus en charge les anciens pilotes de filtre. Toutes les opérations de chiffrement et de déchiffrement s'effectuent exclusivement via la nouvelle technologie de pilote de mini-filtre, plus moderne et plus durable.

**Étape 10:** Vérifiez à nouveau vos entrées, puis cliquez sur **Suivant** pour démarrer l'installation.

**Étape 11:** Si l'installation est réussie, une boîte de dialogue apparaît, dans laquelle vous pouvez cliquer sur le bouton Terminer pour **terminer** le processus d'installation.

**Remarque**

- Pour appliquer tous les paramètres, vous devez redémarrer l'ordinateur.

## Installation sans assistance

L'installation sans assistance signifie que vous pouvez installer *u.trust LAN Crypt* automatiquement sur un grand nombre d'ordinateurs.

Le répertoire d'installation de votre CD d'installation inclut le fichier *.msi*, requis pour l'installation sans assistance des composants du client.

## Composants à installer

La liste suivante montre tous les composants qui doivent être installés, ainsi que la façon dont ils doivent être spécifiés dans le cadre d'une installation sans assistance.

Les mots-clés ( **Courier** , **bold** ) représentent la manière dont les composants doivent être spécifiés sous AddLocal= lors de l'exécution d'une installation sans assistance. Les noms de composants sont sensibles à la casse!

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

## Syntaxe de ligne de commande

Pour effectuer une installation sans assistance, vous devez exécuter **msiexec** avec certains paramètres.

**Paramètres obligatoires:**

**/I**

Spécifie le package d'installation à installer.

**/QN**

Installation sans interaction utilisateur (installation sans assistance).

Nom du fichier .msi: **LCClient.msi**

**Syntax:**

```
msiexec /i \<path\>\LCClient.msi /qn AddLocal=\<component1\>,\<component2\>,...
```

**Paramètres facultatifs**

```
/Lvx\* \<chemin + nom du fichier\>
```

Enregistre la procédure d'installation complète à l'emplacement spécifié sous `\<chemin + nom du fichier\>`.

**AddLocal=**

```
AddLocal= ALL
```

Installe tous les composants disponibles.

```
AddLocal= LanCrypt
```

N’installe aucun des composants disponibles.

```
AddLocal= UserApplication
```

Installe l’application utilisateur *u.trust LAN Crypt*.

```
AddLocal= NetworkFilter
```

Installe un pilote qui aide à améliorer les performances des accès réseau.

```
AddLocal= ClientAPI
```

Installe l’API client de *u.trust LAN Crypt*. Il sera utilisé pour accéder à la fonctionnalité de chiffrement des fichiers *u.trust LAN Crypt* via une API.

```
AddLocal= ShellExtensions
```

nstalle les extensions de l’Explorateur *u.trust LAN Crypt*, voir Extensions de l’Explorateur.

*u.trust LAN Crypt* ajoute des entrées à l’Explorateur Windows, lesquelles permettent le chiffrement initial ainsi que le chiffrement/déchiffrement explicite des fichiers et dossiers, et vous permettent de vérifier facilement l’état du chiffrement de vos données. Ces entrées sont affichées dans les menus contextuels des lecteurs, dossiers et fichiers. De plus, un onglet **Informations de chiffrement** est ajouté à la page des *Propriétés Windows*.

**NOOVERLAY=**

**(Fonctionne uniquement lors de nouvelles installations, pas lors de mises à niveau de version)**

```
NOOVERLAY=0
```

Active les icônes superposées pour les fichiers et dossiers.

```
NOOVERLAY=1
```

Désactive les icônes superposées pour les fichiers et dossiers.

> **Remarque**
>
> - Les utilisateurs peuvent activer les icônes superposées après l’installation. En cliquant sur **Options des dossiers** -> **Affichage**, les utilisateurs peuvent spécifier si l’état de chiffrement des fichiers et celui des dossiers doivent être affichés pour leur profil. Les modifications apportées à ces paramètres ne deviennent effectives qu’une fois que l’utilisateur s’est déconnecté puis reconnecté.

**Productlanguage=**

Installe le module linguistique MSI pour le client *u.trust LAN Crypt* dans une langue spécifique, quel que soit le paramètre de langue existant sur l’ordinateur. Cette langue définie est ensuite utilisée pour l’installation elle-même ainsi que pour les modifications ultérieures par l’assistant de configuration de *u.trust LAN Crypt*. Les paramètres de langue suivants sont actuellement pris en charge via le paramètre d’installation « Productlanguage= ».

```
Productlanguage=1031
```

Installe le module linguistique MSI allemand pour le client *u.trust LAN Crypt*.

```
Productlanguage=1033
```

Installe le module linguistique MSI anglais pour le client *u.trust LAN Crypt*.

```
Productlanguage=1036
```

Installe le module linguistique MSI français pour le client *u.trust LAN Crypt*.

**RESET_CONFIGURATION=**

```
RESET_CONFIGURATION=1
```

Réinitialise toutes les configurations existantes du client LAN Crypt dans le registre Windows. Toutes les anciennes configurations seront définitivement supprimées. Toutes les entrées de registre par défaut sont créées lors de l'installation.

**ONEDRIVE=**

```
ONEDRIVE=1
```

Active la prise en charge de Microsoft OneDrive pour l'utilisateur pour lequel le setup est prévu.

**Exemples:**

```
msiexec /i C:\Install\LCClient.msi /qn AddLocal=ALL
```

Une installation complète de *u.trust LAN Crypt* est effectuée. Le programme est installé dans le répertoire d'installation par défaut (`\<System drive\>:\Programmes\Utimaco\u.trust LAN Crypt`).

```
msiexec /i C:\Install LCClient.msi /qn AddLocal=UserApplication,ShellExtensions
Productlanguage=1033
```

L'installation de *u.trust LAN Crypt* est exécutée. Le programme est installé dans le répertoire d'installation par défaut (`\<System drive\>:\Programmes\Utimaco\u.trust LAN Crypt`) avec l'application utilisateur, les extensions de l'Explorateur et le module linguistique MSI anglais, mais sans l'API client.

Le « fichier .msi » se trouve dans le dossier d'installation de *u.trust LAN Crypt*.

**Remarque**

- Veuillez noter que le programme d'installation sera abandonné si la ligne située après le paramètre « AddLocal= » reste vide ou si un paramètre y est saisi de manière incorrecte.

## Suppression du client *u.trust LAN Crypt*

Vous ne pouvez supprimer le client *u.trust LAN Crypt* que si vous disposez des privilèges d'administrateur Windows.

Sélectionnez Démarrer -> Paramètres -> Applications. Double-cliquez sur *u.trust LAN Crypt* Client dans la liste des applications et cliquez sur le bouton **Désinstaller**. Dans la boîte de dialogue suivante, cliquez à nouveau sur le bouton **Désinstaller**. *u.trust LAN Crypt* Client est désinstallé. Redémarrez ensuite votre ordinateur.

**Remarque**

- Parfois, les *bibliothèques d'exécution Visual C++ requises ne sont pas (ou plus) installées sur certains ordinateurs clients. En raison de ce composant manquant, *u.trust LAN Crypt* ne peut pas être désinstallé sur ces ordinateurs. Un message d'erreur lors de la désinstallation indique alors qu'il y aurait un problème avec le package Windows Installer. Dans ce cas, vous devez installer les _bibliothèques d'exécution Visual C++* requises sur l'ordinateur client concerné. Vous pouvez les trouver aux URLs suivants:

https://docs.microsoft.com/en-us/cpp/windows/latest-supported-vc-redist?view=msvc-170

https://aka.ms/vs/17/release/vc_redist.x86.exe

https://aka.ms/vs/17/release/vc_redist.x64.exe

Après avoir installé avec succès les _bibliothèques d'exécution Visual C++ requises sur l'ordinateur client, il devrait être possible de désinstaller à nouveau *u.trust LAN Crypt* sans erreur.

**Remarque**

- Les fichiers chiffrés ne peuvent plus être déchiffrés après la suppression du client *u.trust LAN Crypt*.

**Remarque**

- Ne réinstallez pas le client *u.trust LAN Crypt* immédiatement après l'avoir supprimé. Vous devez redémarrer la machine au moins une fois avant de l'installer à nouveau.

# Désinstallation Sans Interaction Utilisateur

**Prérequis :** Le paquet MSI qui doit être désinstallé doit être présent sur le système.

Exemple :

```
msiexec /X {00000000-0000-0000-0000-000000000000} /qn /norestart
```

Cette commande désinstalle le paquet MSI avec le ProductCode {00000000-0000-0000-0000-000000000000} en mode silencieux et empêche le redémarrage du système.

**Options de ligne de commande :**

**/X {ProductCode}**

Le ProductCode du paquet MSI à désinstaller. Le ProductCode peut être extrait directement du fichier MSI.

**/qn**

Exécute la désinstallation en mode silencieux, sans afficher d'interface utilisateur à l'utilisateur.

**/norestart**

Empêche un redémarrage du système après la désinstallation.

# Messages d'erreur personnalisés dans LAN Crypt Client

LAN Crypt Client offre la possibilité d'enregistrer des messages individuels pour certains messages d'erreur. Vous pouvez ainsi compléter les messages standard par vos propres remarques, par exemple avec une référence au support informatique.

**Remarque**

- Actuellement, l'ajout de vos propres informations n'est pris en charge que pour les messages d'erreur liés au **chargement de profils (LoadProf)**.

## Configuration

Les textes personnalisés sont enregistrés dans le chemin d'accès suivant du registre :
« HKEY*LOCAL*MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt\Customer Messages\Client »

Pour chaque message d'erreur à ajouter, un sous-répertoire distinct doit être créé au format : « Client-MsgId- »

Le <code d'erreur> correspond au code d'erreur du message d'erreur concerné. Pour le code d'erreur **1056**, le chemin d'accès est par exemple :
« HKEY*LOCAL*MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt\Customer Messages\Client\Client-MsgId-1056 ».

**Remarque**

- Le code d’erreur peut être identifié via le document lié (sous réserve de modifications) ou en reproduisant l’erreur.

Les messages peuvent être enregistrés dans différentes langues dans ce registre. Pour cela, le code de langue et de pays est utilisé comme nom de l'entrée (de-DE, de-AT, en-US, ...).

La valeur correspondante contient le message à joindre. Il convient de noter que le message ne doit pas dépasser **1000 caractères**. Si cette longueur est dépassée, le message n'apparaîtra pas dans le message d'erreur.

# Intégration de la documentation dans un environnement sans accès Internet

Si LAN Crypt est utilisé dans un environnement sans accès à Internet, les liens intégrés du client vers l'aide en ligne ne fonctionneront pas. Pour fournir malgré tout un lien direct vers une documentation locale ou interne, la valeur de registre suivante peut être définie:

HKLM\SOFTWARE\Policies\conpal\LAN Crypt\HelpURL

Ce paramètre permet de spécifier un fichier d'aide alternatif, tel qu'une documentation PDF locale. La valeur de registre doit contenir un chemin URL absolu accessible depuis le système client (par ex. « https://intranet.local/docs/lancrypt_help.pdf »).

# Compatibilité avec les services cloud

LAN Crypt prend en charge le chiffrement des fichiers stockés sur des plateformes cloud et offre ainsi une protection supplémentaire contre les accès non autorisés - même de la part des opérateurs des services cloud. Les fournisseurs de services cloud tels que Microsoft, Google ou d'autres plateformes similaires proposent généralement des fonctions supplémentaires, comme l'édition collaborative de documents ou la recherche de fichiers basée sur le contenu. Comme ces services ne peuvent pas accéder au contenu des fichiers chiffrés, ces fonctionnalités ne sont pas disponibles pour les fichiers protégés par LAN Crypt. Les données chiffrées bénéficient d'un niveau de protection particulièrement élevé et ne peuvent donc pas être traitées par ces services.

## Services Microsoft 365 non compatibles

Les fonctionnalités Microsoft 365 suivantes nécessitent une analyse du contenu des fichiers et ne peuvent donc pas être utilisées lorsque les fichiers sont chiffrés avec LAN Crypt:

- Règles de flux de messages, y compris les analyses anti-malware et anti-spam nécessitant l'accès aux pièces jointes
- Microsoft Delve
- eDiscovery
- Recherche et indexation de contenu
- Office Web Apps, y compris l'édition collaborative de documents
- Copilot

---

# Signalement des vulnérabilités de sécurité

Utimaco reconnaît qu'une sécurité robuste repose sur la collaboration. Nous nous engageons à travailler de manière responsable et constructive avec nos clients, les professionnels de la sécurité, les chercheurs en sécurité et la communauté au sens large afin d'identifier et de corriger les vulnérabilités.

Nous accueillons favorablement et encourageons le signalement responsable des vulnérabilités. Chaque signalement reçu est traité avec diligence et urgence, et nous nous efforçons d'en accuser réception rapidement, de communiquer de manière responsable tout au long du processus d'investigation et de partager les mises à jour pertinentes (avis de sécurité et correctifs) dès qu'elles sont disponibles.

Si vous découvrez une vulnérabilité, nous vous encourageons à la signaler sans délai et de manière sécurisée au PSIRT d'Utimaco (Product Security Incident Response Team), qui traitera votre signalement en urgence.

Tout signalement de vulnérabilité doit être transmis sous forme chiffrée à l'aide du chiffrement PGP, afin d'éviter toute divulgation accidentelle d'informations critiques.

## (Étape 1) Préparez votre signalement

Fournissez autant de détails que possible pour nous aider à comprendre et à reproduire le problème :

Bref résumé de la vulnérabilité Description de la vulnérabilité Produits, versions et configuration concernés Description de l'environnement du produit Système d'exploitation utilisé. Instructions de reproduction étape par étape Cause racine possible. Code de preuve de concept, captures d'écran ou journaux (si disponibles) Impact potentiel et mesures correctives suggérées (facultatif) Vos coordonnées pour le suivi et votre clé publique de chiffrement PGP.

Tous les signalements seront traités de manière strictement confidentielle, et aucune donnée personnelle ne sera communiquée à des tiers

## (Étape 2) Chiffrez votre e-mail avec PGP

Pour protéger les informations sensibles, vous devez chiffrer votre signalement à l'aide de notre clé publique PGP du PSIRT avant de l'envoyer.

1. Importez notre clé publique du PSIRT (fournie ci-dessous) dans votre outil PGP/GPG.
2. Chiffrez le signalement de vulnérabilité à l'aide de cette clé
3. Envoyez un e-mail à PSIRT@utimaco.com avec la pièce jointe chiffrée.
4. Vous pouvez également signer votre message avec votre propre clé PGP afin que nous puissions en vérifier l'authenticité.

## Contact PSIRT

**Équipe PSIRT** : PSIRT@Utimaco.com

**Empreinte PGP** : 77F3 05F8 11AF 228B 7623 33E5 DA5F 264E A9C1 64CB

**Clé PGP** : Télécharger

---

# Support technique

**Pour accéder au support technique des produits Utimaco, procédez comme suit:**

Tous les clients sous contrat de maintenance peuvent accéder à des informations supplémentaires et/ou à des articles de la base de connaissances à partir du lien suivant support.Utimaco.com. En tant que client sous contrat de maintenance, envoyez un courriel au support technique en utilisant l'adresse suivante support@Utimaco.de et indiquez-nous le numéro de version exact, le système d'exploitation et le niveau de correction de votre logiciel Utimaco et, le cas échéant, une description détaillée des messages d'erreur que vous recevez ou des articles de la base de connaissances applicables.

---

# Mentions légales

Copyright © 2024 - 2026 Utimaco IS GmbH, 2018 - 2024 conpal GmbH, 1996 - 2018 Sophos Limited et Sophos Group. Tous droits réservés. conpal® est une marque déposée d’conpal GmbH.

Tous les autres noms de produits et de sociétés mentionnés sont des marques commerciales ou des marques déposées de leurs propriétaires respectifs.

Aucune partie de cette publication ne peut être reproduite, stockée dans un système d’extraction ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, par photocopie, enregistrement ou autre, à moins que vous ne disposiez d’une licence valide permettant la reproduction de la documentation conformément aux termes de la licence, ou que vous ayez l’autorisation écrite préalable du propriétaire du droit d’auteur.

Vous trouverez des informations sur les droits d’auteur de fournisseurs tiers dans le document Logiciel tiers de votre répertoire de produits.

---

**Dernière mise à jour le 14.08.2026**