Qu'est-ce que u.trust LAN Crypt 2Go ?

u.trust LAN Crypt 2Go permet l'échange sécurisé de données confidentielles via un chiffrement basé sur un mot de passe. Les fichiers peuvent être chiffrés facilement et en toute sécurité avec AES-256 XTS. Soit à la demande, en utilisant l'application *u.trust LAN Crypt 2Go* ou de manière transparente via le module complémentaire Outlook pour Windows pour les pièces jointes partagées par email. Une version hébergée sur le web est également disponible, permettant le chiffrement et le déchiffrement sur des systèmes où le produit n'est pas installé ou ne peut pas être installé. L'utilisateur peut choisir individuellement le mot de passe à utiliser pour le chiffrement. Les mots de passe doivent répondre à un ensemble de critères prédéfinis et de complexité afin de garantir un niveau minimum de sécurité. Les exigences imposées sont la longueur minimale du mot de passe, la sensibilité à la casse et un mélange de caractères alphanumériques et spéciaux.

Les personnes qui ne connaissent pas le mot de passe secret utilisé pour le chiffrement n'auront pas accès aux informations contenues dans le fichier et, lorsqu'elles ouvriront un fichier protégé par *u.trust LAN Crypt 2Go*, elles ne verront que son contenu chiffré.

u.trust LAN Crypt 2Go est un complément aux clients u.trust LAN Crypt pour Windows et macOS afin de permettre un échange sécurisé de données confidentielles également avec d'autres personnes ou partenaires externes qui n'utilisent pas encore u.trust LAN Crypt. Outre Windows et macOS, il est également disponible sur Linux (Ubuntu, Debian). Sur les appareils mobiles comme Android et iOS/iPadOS, la fonctionnalité fait partie de l'application u.trust LAN Crypt pour mobile.

u.trust LAN Crypt 2Go est disponible en anglais et en allemand.

Exemple d'utilisation

Imaginez que vous souhaitiez fournir un fichier Excel avec des données financières confidentielles à une agence de marketing externe, qui doit créer un rapport financier tendance avec des graphiques attractifs. Cependant, l'agence de marketing n'utilise pas encore *LAN Crypt*.

Voici comment vous pouvez partager le fichier de manière sécurisée avec votre agence de marketing :

1. Chiffrez le fichier (par exemple, "Rapport financier.xlsx") avec *u.trust LAN Crypt 2Go*. Pour cela, vous pouvez créer une nouvelle clé ou utiliser une clé existante.
2. Envoyez le fichier chiffré ("Rapport financier.xlsx.pcrypt") à votre agence de marketing, par exemple via un email non sécurisé.
3. Communiquez à votre contact à l'agence de marketing le mot de passe qui peut être utilisé pour déchiffrer le fichier, par exemple lors d'une conversation téléphonique.
4. L'agence de marketing peut se rendre sur la page web de *u.trust LAN Crypt 2Go* pour déchiffrer le fichier chiffré, sans avoir besoin d'installer de logiciel. Alternativement, l'agence de marketing peut utiliser *u.trust LAN Crypt 2Go Reader* pour déchiffrer le fichier localement (Windows uniquement).

   Note

   - *u.trust LAN Crypt 2Go* est compatible avec *LAN Crypt*. Par conséquent, vous pouvez chiffrer et déchiffrer des fichiers même dans des dossiers qui ont une politique de chiffrement appliquée par u.trust LAN Crypt. Les fichiers restent chiffrés en permanence !

Installation et mise à jour

u.trust LAN Crypt 2Go est disponible sur les plateformes suivantes :

- Windows 10 ou version ultérieure (x64)
- macOS 12 ou version ultérieure (Intel, Apple Silicon)
- Debian 11 ou version ultérieure
- Ubuntu 20.04 ou version ultérieure

Des packages d'installation individuels sont disponibles pour les plateformes suivantes :

- **lc2go.msi** - Windows (x64)
- **lc2go.dmg** - macOS (Intel, Apple Silicon)
- **lc2go.deb** - Debian, Ubuntu (AMD64)

  Note

  - Une version web de *u.trust LAN Crypt 2Go* est hébergée sur la page d'accueil de Utimaco. Cette version ne nécessite aucune installation de logiciel et peut être utilisée par toute personne souhaitant chiffrer ou déchiffrer des fichiers.

La version Windows du produit présente quelques spécificités qui diffèrent des autres plateformes. Premièrement, elle prend en charge deux modes d'installation différents : utilisateur actuel et tous les utilisateurs. Deuxièmement, elle contient un module complémentaire pour Microsoft Outlook (32 bits et 64 bits), qui n'est disponible que sur la plateforme Windows.

Option d'installation : Tous les utilisateurs

Par défaut, l'installation de *u.trust LAN Crypt 2Go* ne nécessite pas de privilèges administratifs et peut être installée par n'importe quel utilisateur. Si elle est installée par un utilisateur, l'application sera installée et ne sera disponible que pour cet utilisateur uniquement. Les autres comptes d'utilisateurs sur le même système n'auront pas accès au produit installé.

L'installation administrative de *u.trust LAN Crypt 2Go* rendra le produit disponible pour tous les utilisateurs. Pour cela, vous devez exécuter le programme d'installation en mode avancé et écraser le paramètre MSIINSTALLPERUSER.

Par exemple, exécutez la commande suivante à partir d'un terminal Windows élevé :

```
msiexec /i lc2go.msi MSIINSTALLPERUSER=""
```

Cela installera le produit pour tous les utilisateurs du système.

Option d'installation : Module complémentaire Microsoft Outlook

u.trust LAN Crypt 2Go offre des options d'installation modulaires permettant aux clients de personnaliser les installations en fonction de leurs besoins spécifiques. Le paramètre **ADDLOCAL** peut être utilisé pour sélectionner les fonctionnalités à installer.

Exécutez la commande suivante à partir d'un terminal Windows élevé :

```
msiexec /i lc2go.msi ADDLOCAL=ALL REMOVE=outlook_addin_feature
```

Cela installera le produit lui-même, mais omettra l'installation du module complémentaire pour Microsoft Outlook.

Désinstaller u.trust LAN Crypt 2Go

u.trust LAN Crypt 2Go peut être supprimé d'un système à tout moment. La désinstallation suit les procédures standard de suppression de logiciel pour chaque plateforme.

Note

- Après la désinstallation de *u.trust LAN Crypt 2Go*, les fichiers chiffrés par mot de passe ne peuvent plus être déchiffrés sur l'ordinateur. La désinstallation de *u.trust LAN Crypt 2Go* ne désinstalle pas *LAN Crypt*.

Support de u.trust LAN Crypt Cloud

L'utilisation de u.trust LAN Crypt Cloud permet aux utilisateurs de stocker en toute sécurité leurs clés dans le cloud. Cela se fait automatiquement et permet d'accéder au trousseau de clés depuis tous les appareils de l'utilisateur, sur toutes les plateformes prises en charge par *u.trust LAN Crypt 2Go*.

Les modifications apportées au trousseau de clés, qu'il s'agisse de l'ajout, de la suppression ou du renommage d'une clé, sont automatiquement synchronisées avec les autres appareils. Cela garantit que l'utilisateur a toujours accès aux clés les plus récentes, quel que soit l'appareil sur lequel il travaille.

Connexion et déconnexion

Pour vous connecter, appuyez sur l'**icône de compte** dans le coin supérieur droit de l'application *{{ site.productName_2Go_Englisch }}* et sélectionnez **Se connecter** :

Si vous avez des clés basées sur un mot de passe dans votre trousseau de clés, l'utilisateur sera invité à autoriser le téléchargement des clés vers u.trust LAN Crypt Cloud. L'autorisation de télécharger les clés existantes est obligatoire. Si un utilisateur ne souhaite pas que les clés existantes soient téléchargées, les clés doivent être supprimées avant de se connecter à u.trust LAN Crypt Cloud. Notez que les mots de passe des clés basées sur un mot de passe ne sont pas téléchargés vers u.trust LAN Crypt Cloud, donc l'option **Afficher le mot de passe** pour les clés stockées dans u.trust LAN Crypt Cloud n'est pas disponible.

Après avoir cliqué sur **Se connecter**, le navigateur par défaut de l'utilisateur s'ouvre, demandant les informations de connexion pour u.trust LAN Crypt Cloud. Après avoir entré les informations de connexion, un message de succès s'affiche dans le navigateur. Cela confirme que le processus de connexion a été complété avec succès et que l'utilisateur a maintenant accès à ses clés stockées dans u.trust LAN Crypt Cloud.

Pour vous déconnecter, suivez la même procédure, mais sélectionnez **Se déconnecter** au lieu de **Se connecter**. Après la déconnexion, vous n'aurez plus accès aux clés stockées dans u.trust LAN Crypt Cloud jusqu'à ce que vous vous reconnectiez. Cela sert de niveau de sécurité supplémentaire pour empêcher l'accès non autorisé à vos clés.

Clés gérées

L'icône en forme de **roue dentée** située dans le coin inférieur gauche de l'application ouvre le menu des paramètres. Sous **Clés gérées**, vous pouvez consulter les clés gérées de votre compte cloud. Ces clés sont utilisées par *u.trust LAN Crypt* pour Windows, macOS et Linux afin de chiffrer et de déchiffrer les fichiers de manière transparente, sur la base de règles.

Les clés gérées sont également disponibles dans le porte-clés de *{{ site.productName_2Go_fr }}*. La colonne **type de clé** indique s'il s'agit d'une clé basée sur un mot de passe ou d'une clé gérée.

Si un fichier a déjà été chiffré par un client LAN Crypt à l'aide d'une clé gérée, vous pouvez l'ouvrir dans *{{ site.productName_2Go_fr }}*, le modifier et l'enregistrer de nouveau sous forme chiffrée. La clé gérée correspondante doit pour cela figurer dans votre porte-clés.

Les clés gérées ne peuvent pas servir à créer des fichiers protégés par mot de passe. Pour cette fonction, *{{ site.productName_2Go_fr }}* propose exclusivement des clés basées sur un mot de passe. La différence : les clés basées sur un mot de passe sont dérivées d'un mot de passe, ce qui n'est pas le cas des clés gérées.

Remarque concernant le module Outlook

- Le module Outlook protège lui aussi les pièces jointes en créant des fichiers chiffrés avec des clés basées sur un mot de passe. Les destinataires peuvent les ouvrir avec le mot de passe correspondant, sans disposer de la clé gérée de votre organisation. C'est pourquoi le module Outlook utilise exclusivement des clés basées sur un mot de passe.
- Ici, « gérée » désigne le type de clé et non l'emplacement de stockage. Les clés basées sur un mot de passe restent basées sur un mot de passe, même lorsqu'elles sont gérées dans le cloud.

Chiffrement et déchiffrement de fichiers basés sur un mot de passe

u.trust LAN Crypt 2Go permet l'échange sécurisé de données confidentielles grâce à un chiffrement protégé par mot de passe. Avec *u.trust LAN Crypt 2Go* (AES 256 bits), vous pouvez facilement et en toute sécurité chiffrer et déchiffrer des fichiers. LAN Crypt 2GO utilise des clés générées par mot de passe pour le chiffrement et le déchiffrement, qui sont stockées dans un trousseau de clés au sein de l'application. Les utilisateurs peuvent ajouter de nouvelles clés, supprimer les anciennes ou afficher les mots de passe utilisés pour les clés existantes à tout moment.

Note

- Le chiffrement nécessite toujours un mot de passe sécurisé ! Il doit comporter au moins 8 caractères et contenir des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.
- Le nom du mot de passe de chiffrement n'a aucune influence sur la clé utilisée pour le chiffrement. La valeur de clé réelle pour le chiffrement est générée séparément.

Utilisation de l'interface graphique

Lors de l'ouverture de l'application en sélectionnant l'icône du programme *u.trust LAN Crypt 2Go*, la boîte de dialogue de chiffrement apparaît. Utilisez le bouton **Sélectionner...** pour choisir le fichier à chiffrer ou déchiffrer.

Pour chiffrer le fichier, sélectionnez maintenant la clé souhaitée et cliquez enfin sur **Chiffrer**. De nouvelles clés peuvent être ajoutées via le bouton **Nouvelle clé** et gérées par **Paramètres de l'application**.

u.trust LAN Crypt 2Go crée une copie chiffrée du fichier. Les fichiers chiffrés obtiennent l'extension de fichier supplémentaire .pcrypt et sont clairement reconnaissables grâce à l'icône graphique du document.

Note

- Le fichier original n'est jamais supprimé ou écrasé par *u.trust LAN Crypt 2Go*.

Lors du déchiffrement d'un fichier qui a été chiffré par mot de passe par l'un des produits LAN Crypt, le système vérifie d'abord si la clé requise est déjà stockée. Si c'est le cas, elle est automatiquement utilisée pour le déchiffrement. Si la clé requise n'est pas encore disponible, le mot de passe de la clé doit être entré pour déchiffrer le fichier avec succès. Une clé est dérivée du mot de passe entré et enregistrée, afin qu'elle puisse être utilisée pour d'autres opérations de chiffrement et de déchiffrement.

Note

- Lors du déchiffrement d'un fichier, *u.trust LAN Crypt 2Go* crée une copie non chiffrée du fichier. Il restaure également l'extension de fichier originale du fichier en supprimant l'extension .pcrypt.

Pour voir et gérer les clés créées, cliquez sur **Paramètres de l'application** et sélectionnez **Clés basées sur un mot de passe**. Vous verrez maintenant une liste des clés enregistrées avec des informations telles que leurs GUID. Avec un **clic droit** sur une clé, vous pouvez maintenant la renommer, la supprimer ou afficher le mot de passe original (Windows uniquement).

Utilisation du menu contextuel

Si un fichier non chiffré est ouvert avec **Ouvrir avec** -> **u.trust LAN Crypt 2Go**, l'option de chiffrer le document est proposée.

Un fichier chiffré est temporairement déchiffré de cette manière et automatiquement rechiffré après affichage ou modification du fichier.

Utilisation du glisser-déposer

Pour chiffrer ou déchiffrer un fichier avec *u.trust LAN Crypt 2Go*, vous pouvez simplement glisser le fichier en question sur l'icône du programme.

Affichage et modification des fichiers chiffrés

Les fichiers peuvent également être modifiés directement sans déchiffrement manuel. Dans ce cas, le fichier chiffré est automatiquement déchiffré à l'ouverture, puis rechiffré avec le mot de passe correspondant après modification. La condition préalable est que la clé requise ait déjà été enregistrée ou soit correctement entrée sur demande.

Le programme standard respectif est utilisé pour modifier le fichier (par exemple, les fichiers .docx originaux sont ouverts par défaut avec Microsoft Office).

Note

- Si un fichier chiffré est en lecture seule, le fichier temporairement déchiffré est également en lecture seule. Cela entraîne généralement que le programme par défaut respectif empêche les modifications du fichier.
- Pour créer une version déchiffrée d'un fichier .pcrypt, vous pouvez soit utiliser **Enregistrer sous** dans le programme de modification respectif, soit ouvrir *u.trust LAN Crypt 2Go*, sélectionner un fichier chiffré et appuyer sur le bouton **Déchiffrer**.

Utilisation du module complémentaire Microsoft Outlook

u.trust LAN Crypt 2Go étend Microsoft Outlook en y ajoutant la possibilité de chiffrer les pièces jointes avant l'envoi.

Le module complémentaire est disponible en deux versions :

Module complémentaire classique : Installé avec le client LAN Crypt 2Go pour Windows. La connexion à LAN Crypt Cloud est optionnelle et sert uniquement à récupérer et à stocker les clés utilisées. L'**administration centrale via LAN Crypt Cloud n'est pas requise**.

Module complémentaire moderne : Disponible sur **Microsoft AppSource** et compatible avec les versions les plus récentes d'Outlook pour Windows, macOS et l'application web. L'**administration centrale via LAN Crypt Cloud est obligatoire**. En plus de la récupération et du stockage des clés, le **module complémentaire moderne** offre également d'autres fonctions d'administration. Pour plus d'informations sur les exigences des modules complémentaires dans les versions d'Exchange et d'Outlook, consultez Conditions requises pour l'exécution des compléments Office.

Remarque

- À des fins de test, les modules complémentaires Outlook Web peuvent également être installés par sideloading. Le fichier **manifest XML** nécessaire au sideloading peut être téléchargé via le Link .

Les deux versions prennent en charge deux modes de chiffrement :

Chiffrer à la demande (Encrypt On-Demand) :

Cette fonction permet de **chiffrer les pièces jointes avant leur téléversement sur le serveur Exchange**.

Pour utiliser cette fonction, l'utilisateur sélectionne le module complémentaire LAN Crypt 2Go lors de la rédaction d'un e-mail. Une fenêtre s'ouvre alors, dans laquelle une clé de chiffrement pour les fichiers à joindre peut être choisie. Les fichiers sélectionnés sont ensuite automatiquement **ajoutés à l'e-mail sous forme chiffrée**.

Remarque

- En raison d'une limitation technique imposée par Microsoft, la fonction **« Chiffrer à l'envoi »** du module complémentaire moderne n'est disponible que si le module est **déployé par l'administrateur de l'organisation** ou **installé manuellement via sideloading**. Si le module est installé directement depuis le **Microsoft Marketplace**, la fonction **« Chiffrer à l'envoi »** est désactivée dans Outlook. Pour que les utilisateurs puissent accéder à l'activation basée sur les événements, le module complémentaire moderne doit être déployé de manière centralisée par l'organisation ou chargé manuellement pour les tests.

Chiffrer à l'envoi (Encrypt On-Send) :

Lors de l'envoi d'un e-mail avec le **module complémentaire moderne**, LAN Crypt 2Go vérifie automatiquement si et comment les pièces jointes non chiffrées doivent être traitées. Le chiffrement n'a lieu que dans certaines conditions :

1. Le contenu **n'est pas chiffré** si …
    - aucun fichier joint n'est présent ou toutes les pièces jointes sont déjà chiffrées,
    - l'e-mail est envoyé uniquement à des destinataires internes (aucune adresse externe),
    - l'utilisateur a sélectionné **Non chiffré (Plain)** dans le panneau latéral de LAN Crypt 2Go.
2. Le contenu est **automatiquement chiffré** si …
    - l'utilisateur sélectionne **Chiffré (Encrypted)** dans le panneau latéral de LAN Crypt 2Go. Dans ce cas, toutes les pièces jointes non chiffrées sont automatiquement chiffrées avec la clé choisie.

3. L’utilisateur est **invité à choisir** si …
    - aucune des deux options (**Non chiffré (Plain)** ou **Chiffré (Encrypted)**) n’a été sélectionnée. Lors de l’envoi de l’e-mail, une fenêtre contextuelle s’affiche, demandant à l’utilisateur de décider comment traiter les pièces jointes.

Si aucune décision n’est prise ou si le traitement des pièces jointes reste indéfini, l’utilisateur en est informé et le panneau latéral avec les options disponibles s’ouvre automatiquement.

Contrairement au module complémentaire moderne, lors de l’envoi d’un e-mail avec le **module complémentaire classique**, une boîte de dialogue s’affiche à chaque fois pour sélectionner les options de chiffrement des pièces jointes.

Remarque

- Les images intégrées directement dans le corps du message ne sont pas chiffrées. Pour garantir la confidentialité de ces contenus, elles doivent être ajoutées en tant que pièces jointes classiques.
- Lors de l’utilisation du **module complémentaire moderne**, l’administrateur peut désactiver le mode de chiffrement **Chiffrer à l’envoi** (Encrypt On-Send) dans l’administration LAN Crypt Cloud. Il peut également définir des domaines de messagerie internes et exclure certains types de fichiers du chiffrement automatique.

Utilisation des clés de registre (Windows uniquement)

La version Windows de LAN Crypt 2Go peut être configurée à l'aide des clés de registre suivantes :

HKCU\Software\conpal\LAN Crypt\2Go

Cette clé peut être modifiée par des utilisateurs avec des privilèges restreints :

Nom	Type	Valeur par défaut	Valeur
VerboseLogging	DWORD	0	Cette valeur peut être utilisée pour activer la journalisation détaillée, ce qui peut être utile pour le dépannage : 0 = Pas de journalisation détaillée (seuls les messages d'information, d'avertissement et d'erreur sont enregistrés) 1 (et toutes les autres valeurs) = Journalisation détaillée (comprend des entrées de débogage et détaillées dans le fichier journal)

HKCU\Software\Policies\conpal\LAN Crypt\2Go

HKLM\Software\Policies\conpal\LAN Crypt\2Go

Ces clés de registre ne peuvent pas être modifiées par des utilisateurs restreints.

Pour les versions 1.0 à 4.0 de *u.trust LAN Crypt 2Go*, seule la ruche de registre HKEY*CURRENT*USER (**HKCU**) est prise en charge.

Pour les versions 10.0 et plus récentes de *u.trust LAN Crypt 2Go*, si l'une des clés de registre ci-dessous n'est PAS définie dans la ruche HKEY*CURRENT*USER (**HKCU**), la ruche HKEY*LOCAL*MACHINE (**HKLM**) est également vérifiée. Cela permet aux administrateurs de distribuer des paramètres pour tous les utilisateurs (via HKLM) et prend toujours en charge les exceptions pour des utilisateurs spécifiques (**HKCU**).

Nom	Type	Valeur par défaut	Valeur
CheckOnSend	DWORD	1	Cette valeur peut être utilisée pour désactiver la fonction de chiffrement à l'envoi : 0 = Envoyer sans vérifier 1 (et toutes les autres valeurs) = Vérifier les pièces jointes lors de l'envoi et proposer le chiffrement si nécessaire
InternalMailDomains	String	(Vide)	Une chaîne de domaines de messagerie séparés par des points-

Nom	Type	Valeur par défaut	Valeur
			virgules à considérer comme **internes** (= pas de chiffrement requis). **Exemple :** `{{ site.company_name_small }}.de;` `{{ site.company_name_small }}.at`, où tous les emails à nnn@{{ site.company*name*small }}.de et nnn@{{ site.company*name*small }}.at ne seront pas vérifiés pour les pièces jointes non protégées. Si `InternalMailDomains` n'est pas défini, les domaines de messagerie des destinataires sont comparés avec le domaine de messagerie de l'expéditeur. Seul le domaine de messagerie de l'expéditeur est considéré comme **interne**.
`ExcludedAttachments`	String	(Vide)	Une chaîne de types de fichiers séparés par des points-virgules pour les fichiers qui ne doivent pas être chiffrés. **Exemple :** `.txt;.png;.pdf`
`AllowSendUnencrypted`	DWORD	1	Cette valeur permet d'imposer le chiffrement des pièces jointes envoyées vers des domaines de messagerie externes, garantissant ainsi la sécurité de votre correspondance. Veuillez noter que les pièces jointes envoyées vers des domaines de messagerie internes restent en texte clair. 1 (ou non défini) = autorise l'utilisateur à envoyer des pièces jointes en texte clair à des destinataires externes. 0 (et toutes les autres valeurs sauf 1) = forcer le chiffrement lors de l'envoi d'e-mails à des destinataires externes.

Note

- Pour plus d'informations sur l'utilisation des clés de registre dans les environnements Windows, vous pouvez trouver plus de détails et des conseils ici{:target="_blank"}.

Utilisation de u.trust LAN Crypt 2Go depuis la console.

Avec l'outil en ligne de commande de u.trust LAN Crypt 2Go, vous pouvez chiffrer et déchiffrer des fichiers via la ligne de commande ou le terminal. Pour ce faire, ouvrez le chemin respectif via la console :

Windows :

```
C:\Users\<Username>\AppData\Local\Programs\conpal\LAN Crypt\2Go\lancrypt.exe
```

macOS :

```
/Applications/LAN Crypt 2Go.app/Contents/Resources/lancrypt.app/Contents/MacOS/lancrypt
```

Linux :

Comme l'installateur ajoute automatiquement l'outil en ligne de commande au chemin de recherche, il n'est pas nécessaire d'ouvrir un chemin spécifique via la console.

Vous pouvez maintenant utiliser l'application dans la console avec la commande `lancrypt` suivie d'une instruction.

Gestion des clés

u.trust LAN Crypt 2Go permet de gérer les clés via la console. Les clés peuvent y être ajoutées, supprimées, renommées et listées.

Ajouter une clé :

```
lancrypt /A nom de clé mot de passe
```

ou

```
lancrypt /A /F fichier mot de passe
```

Ajoute une clé pour un chiffrement et un déchiffrement ultérieurs. Avec l'option supplémentaire `/F fichier`, le nom de la clé, son GUID et d'autres informations de clé sont pris d'un fichier donné.

Supprimer une clé :

```
lancrypt /P /N nom
```

ou

```
lancrypt /P /G guid
```

Supprime la clé spécifiée. Avec l'option supplémentaire `/N nom`, la clé à supprimer est identifiée par son nom. Avec l'option supplémentaire `/G guid`, la clé à supprimer est identifiée par son GUID.

Renommer une clé :

```
lancrypt /R /N nom nouveau-nom
```

ou

```
lancrypt /R /G guid nouveau-nom
```

Renomme la clé. Avec l'option supplémentaire `/N nom`, la clé sélectionnée est identifiée par son nom et renommée. Avec l'option supplémentaire `/G guid`, la clé sélectionnée est identifiée et renommée par son GUID.

Lister les clés :

```
LANCRYPT /L
```

Liste toutes les clés enregistrées.

Remarque

- Tant que vous êtes connecté à u.trust LAN Crypt Cloud, les options de ligne de commande pour ajouter, supprimer ou renommer des clés ne sont pas disponibles. Cependant, ces fonctions peuvent être effectuées via l'utilisation de l'application.

Chiffrer

```
lancrypt /E fichier /N nom de clé
```

ou

```
lancrypt /E fichier /G keyguid
```

ou

```
lancrypt /E fichier mot de passe
```

Chiffre le fichier sélectionné soit avec une clé existante (identifiée par `/N nom` ou `/G guid`) soit avec un nouveau mot de passe choisi.

Remarque

- Le chiffrement nécessite toujours un mot de passe sécurisé ! Celui-ci doit comporter au moins 8 caractères et contenir des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.
- Le nom du mot de passe de chiffrement n'a aucune influence sur la clé utilisée pour le chiffrement. La valeur réelle de la clé de chiffrement est générée séparément.

Déchiffrer

```
lancrypt /D fichier
```

ou

```
lancrypt /D fichier mot de passe
```

Déchiffre le fichier sélectionné soit automatiquement avec la clé déjà enregistrée correspondante, soit avec le mot de passe donné.

Remarque

- Lors du déchiffrement avec un mot de passe, celui-ci n'est pas automatiquement enregistré dans les clés sauvegardées.

Déchiffrer avec des clés exportées

L'outil en ligne de commande inclut désormais un paramètre optionnel `/K` pour l'option de déchiffrement (`/D`). Ce paramètre spécifie le chemin vers un fichier d'exportation de clé déchiffrée (en format JSON).

Déchiffrer un seul fichier

Pour déchiffrer un seul fichier, utilisez l'option `/D` avec le nom du fichier et l'option `/K` avec le chemin vers le fichier d'exportation de clé:

```
lancrypt /D exportedKeysTest.txt.pcrypt /K exportedKeys.json
```

Déchiffrer tous les fichiers dans un dossier

Pour déchiffrer tous les fichiers dans un dossier, utilisez l'option `/D` avec le chemin du dossier et l'option `/K` avec le chemin vers le fichier d'exportation de clé:

```
lancrypt /D directory /K exportedKeys.json
```

Remarque

- Le déchiffrement d'un dossier inclut tous les fichiers dans ses sous-dossiers.

Version autonome

LAN Crypt 2Go prend désormais en charge la création de **versions autonomes** de l'application. Une version autonome peut être placée sur un support amovible (par ex. clé USB) ou dans des dossiers synchronisés via le cloud.

Ces versions fonctionnent **sans installation** sur la machine hôte et peuvent être exécutées sur **tout ordinateur utilisant le même système d'exploitation que celui sur lequel la version autonome a été créée**. Tous les composants logiciels et les données de configuration restent stockés avec la copie autonome.

Remarque

- Aucune donnée de l'application n'est écrite sur le système en dehors d'un fichier `readme` généré et d'un dossier `LAN Crypt 2Go Data` situé à côté de l'exécutable autonome.
- Sous **Windows**, aucune information n'est écrite dans le **Registre Windows**.

Création d'une version autonome

Pour créer une version autonome de LAN Crypt 2Go :

1. Ouvrez le menu **Paramètres de l'application**.
2. Sélectionnez **Créer une version autonome**.
3. Choisissez le dossier dans lequel l'application doit être générée.

Une fois le processus terminé, le dossier sélectionné contient la **version autonome complète de LAN Crypt 2Go**.

Utilisation d'une version autonome

Les versions autonomes de LAN Crypt 2Go stockent leur configuration et leurs clés sous forme chiffrée, protégées par un **mot de passe maître**.

Lors du premier lancement de l'application autonome, l'utilisateur doit définir un mot de passe maître. Lors des lancements suivants, toutes les clés enregistrées et les données de configuration resteront chiffrées jusqu'à ce que le mot de passe maître défini soit correctement saisi.

Modifier ou réinitialiser le mot de passe maître

Pour modifier le mot de passe maître, ouvrez les **Paramètres de l'application** pendant l'exécution de la version autonome de LAN Crypt 2Go. Sous **Modifier le mot de passe de l'application**, vous pouvez changer ou réinitialiser le mot de passe maître.

La réinitialisation du mot de passe maître supprime toutes les clés et mots de passe enregistrés et demandera à l'utilisateur de définir un nouveau mot de passe maître lors du prochain démarrage de l'application.

Limitations

Étant donné que la version autonome ne repose pas sur une installation système, certaines fonctionnalités ne sont **pas prises en charge** :

- Le **complément Outlook** n'est pas disponible.
- La **prise en charge LAN Crypt Cloud** n'est pas disponible.

* Sous Windows, les fichiers `.pcrypt` ne sont pas automatiquement associés à l'exécutable autonome.

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

Vous pouvez trouver le support technique pour les produits Utimaco de l'une des façons suivantes :

Sur support.Utimaco.com, les clients enregistrés avec des contrats de maintenance actifs ont accès aux téléchargements, à la documentation et aux éléments de connaissance.

En tant que client de maintenance enregistré, envoyez un email à :

support@Utimaco.de

en incluant votre numéro de version du logiciel Utimaco, le(s) système(s) d'exploitation et le(s) niveau(x) de correctif(s), ainsi que le texte de tout message d'erreur.

Mention légale

Copyright © 2024 - 2026 Utimaco IS GmbH, 2018 - 2024 conpal GmbH, 1996 - 2018 Sophos Limited et Sophos Group. Tous droits réservés. conpal®, AccessOn® et AuthomaticOn® sont des marques déposées de 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 de récupération ou transmise, sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre, à moins que vous ne disposiez d'une licence valide où la documentation peut être reproduite conformément aux termes de la licence ou que vous ayez obtenu l'autorisation préalable écrite du propriétaire des droits d'auteur.

Vous trouverez les informations de copyright sur les fournisseurs tiers dans le document 3rd Party Software dans votre répertoire de produit.

Dernière mise à jour 21.09.2026