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

u.trust LAN Crypt 2Go Reader permet l'échange sécurisé de données confidentielles en déchiffrant des données protégées par mot de passe.

u.trust LAN Crypt 2Go Reader est un complément aux clients *u.trust LAN Crypt*. L'application permet de déchiffrer facilement tous les fichiers chiffrés par mot de passe avec LAN Crypt, de sorte que les fichiers puissent être déchiffrés aisément par des personnes et organisations qui n'utilisent pas encore l'un des produits LAN Crypt.

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

Remarque

- *u.trust LAN Crypt 2Go Reader* est étroitement lié au client LAN Crypt 2Go, mais il ne prend en charge que le déchiffrement des fichiers !
- Les deux produits (*u.trust LAN Crypt 2Go* et *u.trust LAN Crypt 2Go Reader*) peuvent être installés et désinstallés indépendamment l'un de l'autre.

Exemple d’utilisation

Imaginez que vous souhaitiez fournir à une agence de marketing externe plusieurs fichiers Excel contenant des données financières confidentielles, chiffrés avec l'un des produits LAN Crypt. Vous recevez également un mot de passe pour déchiffrer les fichiers.

Vous pouvez alors utiliser *u.trust LAN Crypt 2Go Reader* pour déchiffrer les fichiers fournis à l'aide du mot de passe reçu.

Installation et mise à niveau

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

- **Windows 10** ou supérieur (x64)

Les packages d'installation suivants sont disponibles pour chaque plateforme :

- **lc2go.msi** - Windows (Intel-x64)

Installation

u.trust LAN Crypt 2Go Reader prend en charge deux modes d'installation différents : utilisateur actuel et tous les utilisateurs.

Option d'installation : tous les utilisateurs

L'installation de *u.trust LAN Crypt 2Go Reader* ne nécessite pas de droits d'administrateur par défaut et peut être effectuée par n'importe quel utilisateur. Si l'installation est effectuée par un utilisateur, l'application est installée de manière à être accessible uniquement à cet utilisateur. Les autres comptes utilisateurs du même système n'ont pas accès au produit installé.

L'installation administrative de *u.trust LAN Crypt 2Go Reader* rend le produit accessible à tous les utilisateurs. Pour cela, vous devez exécuter le programme d'installation en mode avancé et remplacer le paramètre MSIINSTALLPERUSER.

Exécutez la commande suivante à partir d'un terminal Windows avec des droits élevés :

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

Cela installe le produit pour tous les utilisateurs du système.

Désinstaller u.trust LAN Crypt 2Go Reader

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

Remarque

- Après la désinstallation de *u.trust LAN Crypt 2Go Reader*, les fichiers cryptés sur l'ordinateur ne peuvent plus être décryptés. La désinstallation de *u.trust LAN Crypt 2Go Reader* n'entraîne la désinstallation d'aucun autre produit de *u.trust LAN Crypt*.

Assistance u.trust LAN Crypt Cloud

L'utilisation de u.trust LAN Crypt Cloud permet aux utilisateurs de stocker leurs clés en toute sécurité 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 Reader*.

Les modifications apportées au trousseau de clés, qu'il s'agisse d'ajouter, de supprimer ou de renommer 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 du compte** dans le coin supérieur droit de l'application *u.trust LAN Crypt 2Go Reader* et sélectionnez **Connexion** :

Si vous disposez de clés basées sur un mot de passe dans votre trousseau, l'utilisateur sera invité à autoriser le téléchargement des clés dans 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, celles-ci doivent être supprimées du u.trust LAN Crypt Cloud avant la connexion. Notez que les mots de passe des clés basées sur un mot de passe ne sont pas téléchargés vers u.trust LAN Crypt Cloud. Par conséquent, l'option **Afficher le mot de passe** n'est pas disponible pour les clés stockées dans u.trust LAN Crypt Cloud.

Après avoir cliqué sur **Se connecter**, le navigateur par défaut de l'utilisateur s'ouvre et lui demande ses identifiants de connexion pour le u.trust LAN Crypt Cloud. Une fois les identifiants de connexion saisis, un message de confirmation s'affiche dans le navigateur. Cela confirme que la procédure de connexion s'est déroulée avec succès et que l'utilisateur a désormais accès à ses clés enregistrées dans le u.trust LAN Crypt Cloud.

Pour vous déconnecter, suivez la même procédure, mais sélectionnez **Déconnexion** au lieu de **Connexion**. Une fois déconnecté, vous n'aurez plus accès aux clés stockées dans u.trust LAN Crypt Cloud jusqu'à ce que vous vous reconnectiez. Cela constitue une couche de sécurité supplémentaire pour empêcher toute personne non autorisée d'accéder à vos clés.

Décryptage de fichiers protégés par mot de passe

Utilisation de l'interface utilisateur graphique

Lorsque vous ouvrez l'application en sélectionnant l'icône du programme *u.trust LAN Crypt 2Go Reader*, la boîte de dialogue de décryptage s'affiche. Utilisez le bouton **Sélectionner...** pour sélectionner le fichier à décrypter ou faites glisser le fichier souhaité dans la fenêtre.

Lors du décryptage d'un fichier qui a été crypté à l'aide d'un mot de passe par l'un des produits *LAN Crypt*, le programme vérifie d'abord si la clé requise est déjà enregistrée. Si c'est le cas, celle-ci est automatiquement utilisée pour le décryptage. Si la clé requise n'est pas encore disponible, le mot de passe de la clé doit être saisi pour décrypter le fichier. Le mot de passe saisi est enregistré comme clé et peut être utilisé pour d'autres cryptages et décryptages.

Remarque

- Lors du décryptage d'un fichier, *u.trust LAN Crypt 2Go Reader* crée une copie non cryptée du fichier. De plus, l'extension d'origine du fichier est restaurée en supprimant l'extension .pcrypt.

Utilisation du menu contextuel

u.trust LAN Crypt 2Go Reader ajoute ses propres commandes au menu contextuel des fichiers. Celles-ci s'affichent lorsque vous cliquez avec le bouton droit de la souris sur un fichier. Les fichiers peuvent être décryptés directement à partir du menu contextuel.

Utilisation du glisser-déposer

Il suffit de faire glisser le fichier à crypter ou à décrypter sur l'icône du programme *u.trust LAN Crypt 2Go Reader*.

Consultation et modification de fichiers cryptés

Les fichiers peuvent également être modifiés directement sans décryptage manuel. Le fichier crypté est alors automatiquement décrypté à l'ouverture et recrypté avec le mot de passe correspondant après modification. Pour cela, la clé requise doit déjà avoir été enregistrée ou être saisie correctement sur demande.

Le programme standard correspondant est utilisé pour modifier le fichier (les fichiers .docx d'origine sont par exemple ouverts par défaut avec Microsoft Office).

Remarque

- Si un fichier crypté est protégé en écriture, le fichier temporairement décrypté est également protégé en écriture. Cela signifie généralement que le programme standard correspondant empêche toute modification du fichier.
- Pour créer une version décryptée d'un fichier .pcrypt, vous pouvez soit utiliser **Enregistrer sous** dans le programme d'édition correspondant, soit ouvrir *u.trust LAN Crypt 2Go*, sélectionner un fichier crypté et cliquer sur le bouton **Décrypter**.

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