Qu'est-ce que u.trust LAN Crypt pour Linux?

Grâce au chiffrement 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 d'autorisation 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* correspondante, ils ne verront que leur contenu chiffré.

Protection des données avec u.trust LAN Crypt pour Linux

u.trust LAN Crypt garantit que les fichiers sensibles peuvent être stockés sous forme chiffrée. 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 se font en grande partie 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. Le fichier de stratégie est protégé par un certificat. Pour que les utilisateurs puissent traiter sur leur ordinateur des fichiers chiffrés avec *u.trust LAN Crypt*, ils doivent avoir accès au fichier de stratégie. En possédant la clé privée associée au certificat, l'utilisateur a accès au fichier de stratégie dans lequel le profil de chiffrement est enregistré. Dans le cas de la configuration avec le *u.trust LAN Crypt Cloud* comme administration, les profils sont automatiquement téléchargés et mis en cache lors de la connexion de l'utilisateur.

u.trust LAN Crypt permet de répartir les utilisateurs dans différents groupes d'autorisation. Tous les utilisateurs *u.trust LAN Crypt* dont le fichier de stratégie contient le même profil de chiffrement sont membres d'un même groupe d'autorisation. Ils n'ont pas à se soucier du chiffrement ni de l'échange de clés. Il leur suffit de pouvoir accéder aux stratégies pour que les fichiers puissent être chiffrés ou déchiffrés dès qu'ils sont ouverts ou fermés. Toutes les formes d'organisation peuvent être représentées, d'une administration centralisée des utilisateurs jusqu'à un modèle distribué dans lequel les utilisateurs n'utilisent que des ordinateurs portables.

Différences entre u.trust LAN Crypt pour Windows et u.trust LAN Crypt pour Linux

Les différences suivantes se rapportent à la configuration avec u.trust LAN Crypt Admin pour Windows comme administration et **non** à la configuration avec le *u.trust LAN Crypt Cloud* comme administration.

Le fichier de configuration remplace la stratégie de groupe

Tous les paramètres sont définis via le fichier config.toml, qui doit être créé après l'installation (voir Créer et configurer le fichier de configuration).

La création d'un fichier de configuration est nécessaire, car le client Linux ne peut pas lui-même utiliser les stratégies de groupe de Windows. Le fichier de configuration contient donc tous les paramètres

requis par le client Linux, comme les chemins d'accès où sont enregistrés le fichier de stratégie, le certificat public du responsable de la sécurité et le fichier de clé de l'utilisateur.

Algorithmes de chiffrement pris en charge par u.trust LAN Crypt pour Linux

u.trust LAN Crypt pour Linux prend en charge les algorithmes de chiffrement suivants:

- AES-256 bits
- AES-128 bits

Remarque

- Veuillez noter dans ce contexte que u.trust LAN Crypt pour Windows prend également en charge d'autres algorithmes de chiffrement (tels que « IDEA » ou « 3DES », etc.). u.trust LAN Crypt pour Linux charge toutes les règles d'une stratégie. Cependant, les règles qui imposent un algorithme de chiffrement non pris en charge sont ignorées.

Si le responsable (principal) de la sécurité a activé l'option « Key Wrapping » (paramètre par défaut), les données du responsable de la sécurité et les données du profil utilisateur sont chiffrées avec une clé de session générée de manière aléatoire à l'aide de l'algorithme sélectionné (par défaut : AES). Cette clé est ensuite chiffrée en RSA avec la clé publique issue du certificat.

u.trust LAN Crypt pour Linux prend en charge les algorithmes de chiffrement suivants pour le Key Wrapping:

- AES-256 bits

Chiffrement

Accès aux fichiers chiffrés

Pour pouvoir lire ou écrire des fichiers chiffrés, un utilisateur a toujours besoin de la clé requise à cet effet. Toutes les clés et règles de chiffrement sont attribuées aux utilisateurs par le responsable de la sécurité via leur fichier de stratégie.

Si l'utilisateur dispose de la clé avec laquelle les fichiers ont été chiffrés, il peut toujours les ouvrir. Cela s'applique en particulier même s'il n'existe aucune règle de chiffrement dans la stratégie du profil pour un partage SMB ni pour les répertoires et fichiers qu'il contient.

Si un partage réseau est couvert par une règle de chiffrement, un accès rapide au dossier monté est disponible au sein du client *u.trust LAN Crypt pour Linux*.

Chiffrement des partages SMB

Pour garantir le chiffrement correct de vos partages SMB, les chemins indiqués dans les règles de chiffrement doivent correspondre exactement au chemin distant du point de montage, c'est-à-dire au chemin vers le serveur, et non au chemin local sous lequel le partage est monté. Si les chemins ne correspondent pas exactement, le chiffrement n'est pas activé.

Pour que les règles de chiffrement puissent être appliquées à un partage réseau, celui-ci doit d'abord être monté dans u.trust LAN Crypt pour Linux.

Pour cela, ouvrez l'onglet Volumes dans le client. Les partages réseau disponibles sur votre système ainsi que ceux déjà montés y sont affichés. Cliquez ensuite sur Ajouter pour monter un partage réseau.

Le partage réseau peut également être monté dans u.trust LAN Crypt pour Linux depuis le terminal à l'aide de l'outil lancryptctl.

> **Remarque**
>
> - LAN Crypt ne peut utiliser les lecteurs réseau que s'ils sont montés via un point de montage local et apparaissent dans la sortie de la commande `mount`. Les lecteurs réseau connectés uniquement via un gestionnaire de fichiers tel que Dolphin ne peuvent pas être utilisés par LAN Crypt.

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.

Configuration avec le *u.trust LAN Crypt Cloud* comme administration

Connexion et accès avec un compte u.trust LAN Crypt Cloud

Pour pouvoir accéder à son profil de chiffrement, un utilisateur doit d'abord réussir l'enregistrement d'un compte u.trust LAN Crypt Cloud. Une fois l'enregistrement terminé, toutes les stratégies et tous les paramètres définis par le responsable de la sécurité sont attribués au compte de l'utilisateur. Lors du premier chargement du fichier de stratégie, l'utilisateur est invité à se connecter au *u.trust LAN Crypt Cloud* avec les données de son compte. Si la connexion est réussie, les stratégies attribuées sont automatiquement téléchargées et enregistrées dans le client.

Configuration avec u.trust LAN Crypt Admin pour Windows comme administration

Créer et configurer le fichier de configuration

Tous les paramètres de {{ site.productName*linux*fr }} sont définis via le fichier de configuration config.toml. Créez ce fichier après l'installation dans le chemin suivant:

`/home/<user>/.config/lancrypt/config.toml`

Ajoutez ensuite les paramètres suivants au fichier de configuration:

``` [onprem.general] profile*refresh*interval = 120

[onprem.certificates] storage*path* = *"~/certs" so*cert_path = "~/socerts"

[onprem.profile] storage_path = "~/profiles" ```

| Section | Paramètre | Description | Valeur par défaut |
|---|---|---|---|
| `[onprem.general]` | `profile_refresh_interval` | Intervalle (en secondes) auquel les profils sont actualisés | `120` |
| `[onprem.certificates]` | `storage_path` | Répertoire d'enregistrement des certificats | `~/certs` |
| `[onprem.certificates]` | `so_cert_path` | Répertoire d'enregistrement des certificats publics (.cer) du responsable de la sécurité | `~/socerts` |
| `[onprem.profile]` | `storage_path` | Répertoire d'enregistrement du profil | `~/profiles` |

## Certificats

Avant que les utilisateurs puissent accéder à leur profil de chiffrement, leur **fichier de clé PKCS#12** (leur certificat) et le **certificat public (.cer)** du responsable de la sécurité doivent se trouver sur l'ordinateur dans les répertoires définis dans le fichier de configuration (voir Créer et configurer le fichier de configuration).

Le responsable de la sécurité distribue ces certificats aux utilisateurs, accompagnés du mot de passe ou du code PIN permettant de déverrouiller le certificat. Si les certificats sont en place lors de la première connexion, l'ensemble du processus jusqu'à la saisie du code PIN s'exécute automatiquement.

Le certificat est vérifié à chaque chargement du profil de chiffrement. Si un certificat valide est trouvé, l'utilisateur est connecté et les règles de chiffrement sont appliquées. Dans le cas contraire, l'utilisateur ne peut pas travailler avec des données chiffrées.

**Remarque**

- Ne modifiez pas les noms des fichiers de certificats exportés depuis la console d'administration, sinon ils ne pourront pas être importés automatiquement.
- Si des erreurs surviennent lors de la connexion, consultez le journal à l'aide de la commande suivante : `journalctl --user --grep lancrypt`
```

Connexion 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 politique de sécurité de l'entreprise, puis enregistrés dans des fichiers de stratégie. Un profil de chiffrement ne peut être chargé que si l'utilisateur possède le certificat correspondant.

Les fichiers de stratégie sont enregistrés dans un chemin défini à cet effet (partage réseau). Pour que *u.trust LAN Crypt pour Linux* trouve le fichier de stratégie, son emplacement doit être défini dans le fichier de configuration. Cela s'applique également au chemin où se trouve le certificat public du responsable de la sécurité.

Lorsqu'un utilisateur se connecte à *u.trust LAN Crypt pour Linux*, le système tente de charger le profil de chiffrement enregistré dans le fichier de stratégie. Si l'utilisateur possède la bonne clé, le profil est déchiffré et les règles de chiffrement sont appliquées.

Chargement du fichier de stratégie

Comportement par défaut de u.trust LAN Crypt

Lorsqu'un utilisateur se connecte, son profil utilisateur mis en cache est d'abord chargé. *u.trust LAN Crypt pour Linux* recherche automatiquement de nouveaux fichiers de stratégie pour l'utilisateur si le chemin de stratégie configuré ou, le cas échéant, le *u.trust LAN Crypt Cloud* est accessible. Lorsqu'un nouveau fichier de stratégie est trouvé, la stratégie mise en cache est actualisée.

L'utilisateur peut commencer à travailler avec des fichiers chiffrés pendant que *u.trust LAN Crypt* recherche en continu de nouvelles versions de la stratégie. Si l'emplacement de stratégie indiqué n'est pas accessible, le profil mis en cache est utilisé.

Dans le cas de l'utilisation de la configuration avec le *u.trust LAN Crypt Cloud* comme administration, le profil mis en cache est utilisé jusqu'à l'expiration de l'intervalle d'actualisation. Cela signifie que la limite de temps définie dans le *u.trust LAN Crypt Cloud* détermine la durée de validité d'un profil mis en cache avant que les stratégies doivent être actualisées.

Charger manuellement un fichier de stratégie actualisé

Pour recharger la stratégie manuellement, ouvrez le client et cliquez sur **Recharger le profil** sous l'onglet **Etat**.

Informations sur l'état du client

u.trust LAN Crypt pour Linux fournit des informations détaillées sur son état. Les informations disponibles sont réparties dans des onglets distincts comme suit:

Etat

Affiche l'état actuel du programme, y compris l'utilisateur connecté ainsi que la durée de validité et l'intervalle d'actualisation de la stratégie chargée.

Volumes

Affiche tous les partages réseau disponibles pour le montage ainsi que les partages réseau déjà montés dans LAN Crypt.

Règles

Répertorie toutes les règles de chiffrement attribuées à l'utilisateur.

Clés

Répertorie toutes les clés dont dispose l'utilisateur.

Événements

Affiche un journal chronologique des activités de LAN Crypt.

À propos

Affiche des informations sur le produit, y compris la version installée.

Fonctions de « lancryptctl »

En plus des composants du programme, une application de console « lancryptctl » est installée. Cet outil peut être utile pour résoudre des problèmes techniques. Il met à la disposition de l'utilisateur des fonctions avancées de *u.trust LAN Crypt pour Linux*, décrites ci-dessous.

Appel

Appelez l'outil dans un terminal en utilisant la syntaxe suivante:

```
lancryptctl [COMMANDE]
```

Pour obtenir un aperçu de toutes les commandes disponibles, utilisez `lancryptctl --help` ou `lancryptctl help`. Pour afficher l'aide d'une commande particulière, utilisez `lancryptctl help <COMMANDE>`.

Assistance technique

Pour obtenir une assistance technique sur les produits Utimaco, procédez comme suit:

Sur support.Utimaco.com, les clients sous contrat de maintenance ont accès à des informations complémentaires, telles que des articles de la base de connaissances.

En tant que client sous contrat de maintenance, envoyez un e-mail à l'assistance technique à l'adresse support@Utimaco.com en indiquant le ou les numéros de version, le ou les systèmes d'exploitation et le niveau de correctif de votre logiciel Utimaco ainsi que, le cas échéant, le libellé exact des messages d'erreur.

Mention légale

Dernière mise à jour le 01.09.2026