Was ist u.trust LAN Crypt für Linux?

u.trust LAN Crypt ermöglicht mit Dateiverschlüsselung den Austausch vertraulicher Daten innerhalb von Berechtigungsgruppen in kleinen, mittleren und großen Organisationen. u.trust LAN Crypt funktioniert ohne Benutzerinteraktion. Es unterstützt die Rolle eines Security Officers (SO), der die Zugriffsrechte auf Dateien, die mit u.trust LAN Crypt verschlüsselt sind, einschränken kann. Ein Master Security Officer (MSO) hat das Recht, u.trust LAN Crypt zu verwalten oder auch Berechtigungen zu delegieren. Auf diese Weise lässt sich auch eine Hierarchie von Security Officern einrichten, die die Sicherheitsanforderungen in jedem Unternehmen erfüllen kann.

Verschlüsselte Dateien müssen nicht einzelnen Benutzern zugewiesen sein. Jeder Benutzer, der über den erforderlichen Schlüssel verfügt, kann mit einer verschlüsselten Datei arbeiten. Dies erlaubt Administratoren das Erzeugen von logischen Benutzergruppen, die gemeinsam auf verschlüsselte Dateien zugreifen und mit diesen arbeiten können. Dieser Vorgang kann mit einer Art Schlüsselbund, wie er im täglichen Leben verwendet wird, verglichen werden. u.trust LAN Crypt stattet Benutzer und Benutzergruppen mit einem Schlüsselbund aus, dessen einzelne Schlüssel für verschiedene Ordner oder Dateien verwendet werden können.

Jedes Mal, wenn ein Benutzer eine Datei in einen verschlüsselten Ordner verschiebt, wird die Datei auf dem Computer dieses Benutzers verschlüsselt. Wenn ein anderer Benutzer aus derselben Berechtigungsgruppe die Datei aus dem Ordner liest, wird sie in verschlüsselter Form übertragen. Die Datei wird nur auf dem Computer des Empfängers entschlüsselt. Der Benutzer kann sie dort bearbeiten. Bevor die Datei wieder in den verschlüsselten Ordner übertragen wird, wird sie wieder verschlüsselt.

Nicht berechtigte Benutzer können unter Umständen auf diese verschlüsselten Dateien zugreifen (nur von Arbeitsstationen ohne u.trust LAN Crypt), sehen aber ohne die entsprechende u.trust LAN Crypt Berechtigung nur deren verschlüsselten Inhalt.

Schutz von Daten durch u.trust LAN Crypt für Linux

u.trust LAN Crypt garantiert, dass sensible Dateien verschlüsselt gespeichert werden können. Ebenso erfolgt die Übertragung in Netzwerken (LAN oder WAN) geschützt, da die Ver- und Entschlüsselung im Hauptspeicher der Arbeitsstation des Benutzers durchgeführt werden. Auf den Arbeitsstationen laufen alle Ver- und Entschlüsselungen weitgehend ohne Benutzerinteraktionen ab. Auf dem Datei-Server selbst muss keine spezielle Sicherheitssoftware installiert werden.

Ein Security Officer kann unterschiedliche Zugriffsrechte für Ordner und Dateien definieren. Diese Rechte werden in Verschlüsselungsprofilen für die Benutzer zusammengefasst. Verschlüsselungsprofile werden über Richtliniendateien an die Benutzer verteilt. Richtliniendateien enthalten alle Regeln, Zugriffsrechte und Schlüssel, die für die Verschlüsselung benötigt werden. Die Richtliniendatei ist durch ein Zertifikat geschützt. Damit Benutzer auf ihren Computern Dateien verarbeiten können, die mit u.trust LAN Crypt verschlüsselt sind, müssen sie Zugriff auf die Richtliniendatei haben. Durch den Besitz des zum Zertifikat gehörenden privaten Schlüssels hat der Benutzer Zugriff auf die Richtliniendatei, in der das Verschlüsselungsprofil gespeichert ist. Im Fall der Konfiguration mit der u.trust LAN Crypt Cloud als Administration, werden die Profile mit dem Login des Users automatisch heruntergeladen und zwischengespeichert.

u.trust LAN Crypt ermöglicht die Einteilung der Benutzer in verschiedene Berechtigungsgruppen. Alle u.trust LAN Crypt Benutzer, die in ihrer Richtliniendatei dasselbe Verschlüsselungsprofil gespeichert haben, sind Mitglieder einer Berechtigungsgruppe. Sie brauchen sich nicht um die Verschlüsselung oder um den Schlüsselaustausch zu kümmern. Sie müssen nur in der Lage sein, auf die Richtlinien zuzugreifen, damit die Dateien ver- bzw. entschlüsselt werden können, sobald sie geöffnet bzw. geschlossen werden. Es können alle Organisationsformen abgebildet werden, indem die Benutzer zentral administriert werden, bis zu einem verteilten Modell, in dem Benutzer nur Notebooks einsetzen.

Unterschiede von u.trust LAN Crypt für Windows und u.trust LAN Crypt für Linux

Folgende Unterschiede beziehen sich auf die Konfiguration mit u.trust LAN Crypt Admin für Windows als Administration und **nicht** auf die Konfiguration mit der u.trust LAN Crypt Cloud als Administration.

Konfigurationsdatei ersetzt Gruppenrichtliniendatei

Sämtliche Einstellungen erfolgen über die Datei config.toml, die nach der Installation zu erstellen ist (siehe Konfiguration).

Die Erstellung einer Konfigurationsdatei ist notwendig, da der Linux-Client selbst keine Gruppenrichtlinien von Windows verwenden kann. Die Konfigurationsdatei enthält daher alle für den Linux-Client erforderlichen Einstellungen, wie z. B. die Pfadangaben, in denen die Richtliniendatei, das öffentliche Zertifikat des Security Officers und auch die Schlüsseldatei des Benutzers gespeichert sind.

Von u.trust LAN Crypt für Linux unterstützte Verschlüsselungsalgorithmen

u.trust LAN Crypt für Linux unterstützt folgende Verschlüsselungsalgorithmen:

- AES-256 Bit
- AES-128 Bit

Hinweis

- Bitte beachten Sie in diesem Zusammenhang, dass u.trust LAN Crypt für Windows auch noch weitere Verschlüsselungsalgorithmen (wie z. B. „IDEA" oder „3DES", etc.) unterstützt. u.trust LAN Crypt für Linux lädt alle Regeln aus einer Policy. Regeln, die einen Verschlüsselungsalgorithmus vorschreiben, der nicht unterstützt wird, werden allerdings verworfen.

Wurde durch den (Master) Security Officer die Option „Key-Wrapping" aktiviert (Standardeinstellung), werden Security Officer-Daten und Benutzerprofildaten mit einem per Zufallsverfahren erzeugten Session-Key mit dem ausgewählten Algorithmus (Standard: AES) verschlüsselt. Dieser Schlüssel wird dann wiederum mit dem öffentlichen Schlüssel aus dem Zertifikat RSA-verschlüsselt.

u.trust LAN Crypt für Linux unterstützt folgende Verschlüsselungsalgorithmen für das Key-Wrapping:

- AES-256 Bit

Verschlüsselung

Zugriff auf verschlüsselte Dateien

Um verschlüsselte Dateien lesen oder schreiben zu können, benötigt ein Benutzer immer den dafür erforderlichen Schlüssel. Alle Schlüssel und Verschlüsselungsregeln werden den Benutzern vom Security Officer über ihre Richtliniendatei zugewiesen.

Wenn der Benutzer den erforderlichen Schlüssel hat, mit dem Dateien verschlüsselt sind, kann er sie immer öffnen. Dies gilt insbesondere auch dann, wenn es in der Profilrichtlinie für eine SMB-Freigabe und die dortigen Verzeichnisse und Dateien keine Verschlüsselungsregel gibt.

Wenn eine Netzwerkfreigabe durch eine Verschlüsselungsregel abgedeckt ist, steht innerhalb des *u.trust LAN Crypt für Linux* Clients ein Schnellzugriff auf den eingehängten Ordner zur Verfügung.

Verschlüsselung von SMB-Freigaben

Um eine korrekte Verschlüsselung Ihrer SMB-Freigaben sicherzustellen, müssen die in den Verschlüsselungsregeln angegebenen Pfade genau mit dem Remote-Pfad des Mountpoints übereinstimmen, also mit dem Pfad zum Server, nicht mit dem lokalen Pfad, unter dem die Freigabe eingebunden ist. Stimmen die Pfade nicht exakt überein, wird die Verschlüsselung nicht aktiviert.

Damit Verschlüsselungsregeln auf einer Netzwerkfreigabe angewendet werden können, muss die Netzwerkfreigabe zunächst in u.trust LAN Crypt für Linux eingebunden werden.

Öffnen Sie dazu im Client den Reiter Datenträger. Dort werden die auf Ihrem System verfügbaren und bereits eingebundenen Netzwerkfreigaben angezeigt. Klicken Sie anschließend auf Hinzufügen, um eine Netzwerkfreigabe einzubinden.

Alternativ kann die Netzwerkfreigabe auch über das Terminal mithilfe des Tools lancryptctl in u.trust LAN Crypt für Linux eingebunden werden.

> **Hinweis**
>
> - LAN Crypt kann Netzlaufwerke nur verwenden, wenn sie über einen lokalen Mountpunkt eingebunden sind und in der Ausgabe des Befehls `mount` erscheinen. Netzlaufwerke, die lediglich über einen Dateimanager wie Dolphin verbunden wurden, können von LAN Crypt nicht verwendet werden.

Explizite Entschlüsselung von Dateien

Um eine Datei zu entschlüsseln, müssen Sie diese nur in einen Ordner ohne Verschlüsselungsregeln kopieren oder verschieben. Die Datei wird dann automatisch entschlüsselt.

Voraussetzungen:

- Ein entsprechendes Verschlüsselungsprofil ist geladen
- Der Benutzer verfügt über den erforderlichen Schlüssel
- Das aktive Verschlüsselungsprofil enthält keine Verschlüsselungsregel für den neuen Speicherort.

Konfiguration mit u.trust LAN Crypt Cloud als Administration

Anmeldung und Zugriff mit einem u.trust LAN Crypt Cloud Konto

Um auf sein Verschlüsselungsprofil zugreifen zu können, muss ein Benutzer zuerst die Registrierung eines u.trust LAN Crypt Cloud Konto erfolgreich abschließen. Sobald die Registrierung abgeschlossen ist, werden alle vom Sicherheitsbeauftragten festgelegten Richtlinien und Einstellungen dem Benutzerkonto zugewiesen. Beim erstmaligen Laden der Richtliniendatei wird der Benutzer dazu aufgefordert, sich mit seinen Kontodaten bei der u.trust LAN Crypt Cloud anzumelden. Bei erfolgreicher Anmeldung werden die zugewiesenen Richtlinien automatisch heruntergeladen und im Client gespeichert.

Konfiguration mit u.trust LAN Crypt Admin für Windows als Administration

Konfigurationsdatei erstellen und konfigurieren

Alle Einstellungen für {{ site.productName*linux*de }} werden über die Konfigurationsdatei config.toml vorgenommen. Erstellen Sie diese Datei nach der Installation unter folgendem Pfad:

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

Fügen Sie anschließend die folgenden Parameter in die Konfigurationsdatei ein:

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

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

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

| Abschnitt | Parameter | Beschreibung | Standardwert |
|---|---|---|---|
| `[onprem.general]` | `profile_refresh_interval` | Intervall (in Sekunden), in dem Profile aktualisiert werden | `120` |
| `[onprem.certificates]` | `storage_path` | Verzeichnis zur Speicherung der Zertifikate | `~/certs` |
| `[onprem.certificates]` | `so_cert_path` | Verzeichnis zur Speicherung der öffentlichen Zertifikate (.cer) des Sicherheitsbeauftragten | `~/socerts` |
| `[onprem.profile]` | `storage_path` | Verzeichnis zur Speicherung des Profils | `~/profiles` |

## Zertifikate

Bevor Benutzer auf ihr Verschlüsselungsprofil zugreifen können, müssen ihre **PKCS#12-Schlüsseldatei** (ihr Zertifikat) und das **öffentliche Zertifikat (.cer)** des Sicherheitsbeauftragten auf dem Rechner in den Verzeichnissen liegen, die in der Konfigurationsdatei definiert sind (siehe Konfigurationsdatei erstellen und konfigurieren).

Der Security Officer verteilt diese Zertifikate an die Benutzer, zusammen mit dem Passwort oder der PIN, mit der das Zertifikat entsperrt wird. Liegen die Zertifikate bei der ersten Anmeldung vor, läuft der gesamte Vorgang bis zur PIN-Eingabe automatisch ab.

Das Zertifikat wird bei jedem Laden des Verschlüsselungsprofils überprüft. Wird ein gültiges Zertifikat gefunden, wird der Benutzer angemeldet und die Verschlüsselungsregeln werden angewendet. Andernfalls kann der Benutzer nicht mit verschlüsselten Daten arbeiten.

**Hinweis**

- Ändern Sie die Dateinamen der aus der Admin-Konsole exportierten Zertifikate nicht, da sie sonst nicht automatisch importiert werden können.
- Treten bei der Anmeldung Fehler auf, lesen Sie das Protokoll mit folgendem Befehl aus: `journalctl --user --grep lancrypt`

## Anmeldung an u.trust LAN Crypt

Verschlüsselungsprofile von *u.trust LAN Crypt* werden von einem Security Officer gemäß der Sicherheitsrichtlinie des Unternehmens erstellt und dann in Richtliniendateien gespeichert. Ein Verschlüsselungsprofil kann nur geladen werden, wenn der Benutzer das entsprechende Zertifikat besitzt.
```

Die Richtliniendateien werden in einem dafür definierten Pfad (Netzwerkfreigabe) abgelegt. Damit *u.trust LAN Crypt für Linux* die Richtliniendatei findet, muss der Speicherort in der Konfigurationsdatei definiert werden. Dies gilt auch für den Pfad, in dem das öffentliche Zertifikat des Security Officers zu finden ist.

Wenn sich ein Benutzer bei *u.trust LAN Crypt für Linux* anmeldet, wird versucht das in der Richtliniendatei hinterlegte Verschlüsselungsprofil zu laden. Wenn der Benutzer den richtigen Schlüssel besitzt, wird das Profil entschlüsselt und die Verschlüsselungsregeln werden angewendet.

Laden der Richtliniendatei

Standardverhalten von u.trust LAN Crypt

Wenn sich ein Benutzer anmeldet, wird zuerst sein zwischengespeichertes Benutzerprofil geladen. *u.trust LAN Crypt für Linux* sucht automatisch nach neuen Richtliniendateien für den Benutzer, wenn der konfigurierte Richtlinienpfad oder gegebenenfalls die u.trust LAN Crypt Cloud erreichbar ist. Wenn eine neue Richtliniendatei gefunden wird, wird die zwischengespeicherte Richtlinie aktualisiert.

Der Benutzer kann beginnen, mit verschlüsselten Dateien zu arbeiten, während *u.trust LAN Crypt* kontinuierlich nach neuen Versionen der Richtlinie sucht. Wenn auf den angegebenen Richtlinienspeicherort nicht zugegriffen werden kann, wird das zwischengespeicherte Profil verwendet.

Im Fall der Verwendung der Konfiguration mit u.trust LAN Crypt Cloud als Administration wird das zwischengespeicherte Profil genutzt, bis das Aktualisierungs-Intervall abgelaufen ist. Das bedeutet, dass das in der u.trust LAN Crypt Cloud eingestellte Zeitlimit dafür verwendet wird, wie lange ein zwischengespeichertes Profil gültig ist, bevor die Richtlinien aktualisiert werden müssen.

Aktualisierte Richtliniendatei manuell laden

Um die Richtlinie manuell neu zu laden, öffnen Sie den Client und klicken Sie unter der Registerkarte **Status** auf **Profil neu laden**.

Client Status-Information

u.trust LAN Crypt für Linux gibt detaillierte Auskunft über seinen Zustand. Die verfügbaren Informationen sind wie folgt in einzelne Registerkarten unterteilt:

Status

Zeigt den aktuellen Programmstatus an, einschließlich des angemeldeten Benutzers sowie der Gültigkeitsdauer und des Aktualisierungsintervalls der geladenen Richtlinie.

Datenträger

Zeigt alle zur Einbindung verfügbaren Netzwerkfreigaben sowie die bereits in LAN Crypt eingebundenen Netzwerkfreigaben an.

Regeln

Listet alle dem Benutzer zugewiesenen Verschlüsselungsregeln auf.

Schlüssel

Listet alle Schlüssel auf, die dem Benutzer zur Verfügung stehen.

Ereignisse

Zeigt ein chronologisches Protokoll der LAN Crypt Aktivitäten an.

Über

Zeigt Produktinformationen an, einschließlich der installierten Version.

Funktionen von "lancryptctl"

Zusätzlich zu den Programmkomponenten wird eine Konsolenanwendung „lancryptctl" installiert. Dieses Tool kann bei der Lösung technischer Probleme hilfreich sein. Damit stehen dem Benutzer erweiterte Funktionen von *u.trust LAN Crypt für Linux* zur Verfügung, die im Folgenden beschrieben werden.

Aufruf

Rufen Sie das Tool in einem Terminal mit folgender Syntax auf:

```
lancryptctl [BEFEHL]
```

Eine Übersicht aller verfügbaren Befehle erhalten Sie mit `lancryptctl --help` oder `lancryptctl help`. Die Hilfe zu einem einzelnen Befehl rufen Sie mit `lancryptctl help <BEFEHL>` auf.

Technische Unterstützung

Technischen Support zu Utimaco Produkten können Sie wie folgt abrufen:

Unter support.Utimaco.com erhalten Wartungsvertragskunden Zugang zu weiteren Informationen, wie Knowledge-Items.

Als Wartungsvertragskunde senden Sie eine E-Mail an den technischen Support support@Utimaco.com und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch Level Ihrer Utimaco Software sowie ggf. den genauen Wortlaut von Fehlermeldungen an.

Rechtlicher Hinweis

Zuletzt aktualisiert am 01.09.2026