# Was ist u.trust LAN Crypt für Windows?

*u.trust LAN Crypt* ermöglicht mit transparenter 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 Officers 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. Auf diese Weise bleibt die Datei immer geschützt, auch wenn im Dateisystem selbst kein Zugriffsschutz definiert ist, das Netzwerk angegriffen wird oder die Mitarbeiter sich nicht an die Sicherheitsrichtlinien der Organisation halten.

## Schutz von Daten durch u.trust LAN Crypt

*u.trust LAN Crypt* garantiert, dass sensible Dateien auf Dateiservern und Arbeitsstationen 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 transparent und weitgehend ohne Benutzerinteraktionen ab. Auf dem Dateiserver 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 transparente Verschlüsselung benötigt werden. Die Richtliniendatei ist durch ein Zertifikat geschützt. Damit Benutzer auf ihren Computern mit *u.trust LAN Crypt* verschlüsselte Daten verarbeiten können, 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.

*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 kümmern. Sie müssen nur in der Lage sein, auf die Richtliniendateien zuzugreifen, damit die Dateien transparent ver- bzw. entschlüsselt werden können, sobald sie geöffnet bzw. geschlossen werden. Es können alle Organisationsformen abgebildet werden - von einem LAN-Modell, in dem die Benutzer zentral administriert werden, bis zu einem verteilten Modell, in dem Benutzer nur Notebooks einsetzen.

Der Minifiltertreiber von *u.trust LAN Crypt* kann seit Version 4.03 auch Dateien, die mit *SafeGuard Enterprise (Fileshare)* verschlüsselt sind, verarbeiten. Eine Entschlüsselung von solchen Dateien ist hierbei nicht erforderlich. Die jeweiligen Schlüssel von *SafeGuard Enterprise* müssen hierzu lediglich mithilfe eines Schlüsselexport- und Schlüsselimport-Tools nach *u.trust LAN Crypt* migriert werden.

**Hinweis**

- Auch im normalen Betrieb lagert Windows meist Teile des Arbeitsspeichers auf die Festplatte aus. In manchen Fällen, etwa bei einem Absturz bzw. bei sog. "Blue

Screens", kann sogar der gesamte Speicherinhalt auf die Festplatte geschrieben werden. Dadurch könnten sensitive Informationen, die sonst nur im Hauptspeicher verfügbar sind (wie z. B. die Inhalte geöffneter Dokumente), auf der Festplatte in einer Datei gespeichert sein. Eine Festplattenverschlüsselung (wie beispielsweise mit *BitLocker* oder *Utimaco DiskEncrypt*) gewährleistet, dass der Inhalt dieser oftmals sensitiven Daten in jedem Fall verschlüsselt auf der Festplatte gespeichert und somit gegen Ausspähung optimal abgesichert ist. Aus diesem Grund wird der Einsatz einer Festplattenverschlüsselung als wichtiger Basis-Schutz und als sinnvolle Ergänzung beim Einsatz von *u.trust LAN Crypt* empfohlen.

## SafeGuard Enterprise: Migration der Dateiverschlüsselung

SafeGuard Enterprise ist eine Sicherheitssuite von Sophos, die aus mehreren Modulen besteht. Data Exchange (DX), Cloud Storage (CS) und File Encryption (FE) bieten alle Verschlüsselung auf Dateiebene. Die gesamte Software-Suite wird jedoch eingestellt, so dass Benutzer Gefahr laufen, den Zugriff auf ihre verschlüsselten Dokumente zu verlieren. Die Umstellung von einem Sicherheitsprodukt auf ein anderes kann mühsam und risikoreich sein, vor allem, wenn die Daten dabei entschlüsselt werden müssen. Bei der Migration zu u.trust LAN Crypt ist dies jedoch nicht der Fall.

u.trust LAN Crypt und Sophos SafeGuard Enterprise sind vollständig kompatibel. Sie verfügen über dieselbe technische Grundlage und dasselbe Subsystem zur Dateiverschlüsselung. Folglich sind die in SafeGuard Enterprise verschlüsselten Dateien vollständig kompatibel mit u.trust LAN Crypt und können von diesem gelesen werden. Die Verschlüsselungsschlüssel sind spezifisch für jede Installation, und nur diese müssen migriert werden.

**Schritt 1: Schlüssel aus SafeGuard Enterprise exportieren**

Die zum Verschlüsseln von Dateien verwendeten Schlüssel sind für jede SafeGuard Enterprise-Installation eindeutig. Sophos stellt ein einfaches Tool zur Verfügung, mit dem Sie alle in SafeGuard Enterprise zur Verschlüsselung von Dateien verwendeten Verschlüsselungsschlüssel einfach exportieren können. Alle Schlüssel werden bequem in ein einziges Paket kopiert.

**Schritt 2: Importieren von Schlüsseln in u.trust LAN Crypt**

Die Schlüssel, die jetzt in einem separaten Paket verfügbar sind, können einfach in ein bestehendes u.trust LAN Crypt-System importiert werden. Nach dem Import verfügt die u.trust LAN Crypt-Installation über alles, was sie für den Zugriff auf Dateien benötigt, die mit SafeGuard Enterprise verschlüsselt wurden.

**Schritt 3: Richtlinie aktualisieren / Schlüssel zuweisen**

Weisen Sie die neu importierten Schlüssel allen Benutzern zu, die Zugriff auf von SafeGuard Enterprise verschlüsselte Dateien benötigen. Diese Schlüssel ermöglichen es den Benutzern, Dateien zu lesen, die in der Vergangenheit mit einem beliebigen SafeGuard Dateiverschlüsselungsmodul verschlüsselt wurden. Dies gilt auch für Dateien, die nach dem Schlüsselimport durch SafeGuard Enterprise verschlüsselt wurden.

**Schritt 4: Zugriff auf SafeGuard Enterprise-Dateien**

Der u.trust LAN Crypt Client teilt seine technische Grundlage mit SafeGuard Enterprise. Sobald die Schlüssel auf den Client übertragen wurden, kann er alle Dateien lesen, die mit einem der SafeGuard Enterprise-Dateiverschlüsselungsmodule - DX, CS, FS - verschlüsselt wurden. Es besteht keine Notwendigkeit, eine einzelne Datei zu entschlüsseln. Unabhängig davon, wie lange eine Datei verschlüsselt wurde, kann u.trust LAN Crypt sie lesen.

Die vollständige Kompatibilität auf Dateiebene ermöglicht eine reibungslose Migration. Selbst wenn Teile des Unternehmens noch SafeGuard Enterprise verwenden, können alle verschlüsselten Dateien, die sie erstellen, von jedem gelesen werden, der bereits zu u.trust LAN Crypt migriert ist.

**Hinweis**

- Wenn Sie *SafeGuard Enterprise* installiert haben und eine Migration auf *u.trust LAN Crypt* planen, wenden Sie sich bitte an den u.trust LAN Crypt Support. Weitere Informationen finden Sie unter https://utimaco.com/file-encryption-migration-five-easy-steps-safeguard-enterprise.

# Verschlüsselung

## Transparente Verschlüsselung

Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (in verschlüsselten Ordnern oder Laufwerken) automatisch im Hauptspeicher entschlüsselt werden, sobald sie von einer Anwendung (wie z. B. von Office) geöffnet werden. Beim Speichern der Datei wird sie automatisch wieder verschlüsselt. Von der transparenten Verschlüsselung werden alle Dateivorgänge erfasst. Da alle Prozesse im Hintergrund laufen, bemerken Benutzer nichts davon, wenn sie mit verschlüsselten Dateien arbeiten.

**Hinweis**

- *u.trust LAN Crypt* kann keine Dateien verschlüsseln, für die unter dem NTFS-Dateisystem von Windows die **NTFS-Komprimierung** oder **EFS-Verschlüsselung** verwendet wird. Der Assistent zur Initialverschlüsselung bietet allerdings die Möglichkeit, wenn für NTFS-komprimierte und/oder EFS-verschlüsselte Dateien eine Verschlüsselungsregel besteht, diese im Rahmen der Initialverschlüsselung zu dekomprimieren bzw. zu entschlüsseln. Die Dateien werden anschließend von *u.trust LAN Crypt* entsprechend den Verschlüsselungsregeln verschlüsselt. Ob der Benutzer die Möglichkeit hat, NTFS-komprimierte Dateien zu dekomprimieren oder EFS-verschlüsselte Dateien, wenn erforderlich, zu entschlüsseln, muss der Security Officer vorher festlegen.

Die Verschlüsselung ist nicht von Ordnern abhängig, sondern nur von Verschlüsselungsregeln. Die Verschlüsselung funktioniert wie folgt:

- Alle Dateien, für die eine Verschlüsselungsregel existiert, werden beim Speichern automatisch verschlüsselt.
- Werden Dateien in einen verschlüsselten Ordner verschoben oder kopiert, werden sie gemäß der für diesen Ordner definierten Verschlüsselungsregel verschlüsselt. Der Security Officer kann über die *u.trust LAN Crypt* Administration mehrere Verschlüsselungsregeln für unterschiedliche Dateitypen oder Dateinamen definieren, die sich im selben Ordner befinden. Sie können so beispielsweise Worddateien mit einer anderen Regel verschlüsseln als Exceldateien, obwohl sich beide Dateien im selben Ordner befinden.
- Beim Umbenennen von verschlüsselten Dateien bleiben diese verschlüsselt (sofern nicht eine andere oder keine Verschlüsselungsregel für den neuen Dateinamen oder die neue Dateierweiterung besteht).
- Wenn ein Benutzer verschlüsselte Dateien an einen Ort kopiert oder verschiebt, an dem die bisherige Verschlüsselungsregel nicht mehr gilt, werden sie automatisch entschlüsselt.

  **Hinweis**

  - Dies gilt nicht, wenn ein Benutzer Dateien innerhalb derselben Netzwerkfreigabe in einen anderen Ordner verschiebt. In diesem Fall bleiben die Dateien verschlüsselt, und zwar auch dann, wenn keine Verschlüsselungsregel besteht.
- Wenn der Security Officer oder Systemadministrator über die *u.trust LAN Crypt* Gruppenrichtlinie (GPO) die Funktion **Persistente Verschlüsselung** aktiviert hat, bleiben verschlüsselte Dateien auch dann weiterhin verschlüsselt, wenn sie in einen anderen Ordner oder an einen anderen Ort verschoben oder kopiert werden, für den keine Verschlüsselungsregel besteht (z. B. auf einem USB-Stick).
- Wenn ein Benutzer verschlüsselte Dateien an einen Ort kopiert oder verschiebt, für den eine andere Verschlüsselungsregel gilt, werden diese Dateien zuerst entschlüsselt und danach mit dem für diesen Speicherort definierten anderen Schlüssel verschlüsselt.

**Zugriff auf verschlüsselte Daten**

Gibt es in den Verschlüsselungsrichtlinien eines Benutzers keinen Schlüssel und keine Verschlüsselungsregel für einen bestimmten Ordner, darf er nicht auf die verschlüsselten Dateien in diesem Ordner zugreifen. Er darf dort keine verschlüsselte Datei lesen, kopieren, verschieben, umbenennen, löschen, usw.

Verfügt der Benutzer über den Schlüssel, mit dem die Dateien verschlüsselt sind, kann er sie öffnen, auch wenn sein Verschlüsselungsprofil für diesen Ort oder Ordner keine Verschlüsselungsregel beinhaltet.

**Hinweis**

- Ab LAN Crypt Administration Windows Version 13.0.0 ist die Verschlüsselung im CBC-uIV-Format verfügbar. Ältere Classic LAN Crypt Clients (vor Version 13.0.0) erkennen dieses Format nicht und können die betroffenen Dateien daher nicht entschlüsseln. Stellen Sie daher sicher, dass stets eine aktuelle Client-Version im Einsatz ist

**Integration von u.trust LAN Crypt 2Go**

Dateien, die durch *u.trust LAN Crypt 2Go* passwortbasiert verschlüsselt worden sind, können seit der Version 4.2.0 mit *u.trust LAN Crypt für Windows* geöffnet und bearbeitet werden. Voraussetzung hierfür ist, dass der benötigte Schlüssel innerhalb der Verschlüsselungsrichtlinien des Benutzers vorhanden ist.

Nach dem Einsehen oder Bearbeiten der Datei kann die Datei weiterhin von *u.trust LAN Crypt 2Go* und allen weiteren *u.trust LAN Crypt* Anwendungen, die *u.trust LAN Crypt 2Go* bzw. passwortbasierte Ver- und Entschlüsselung unterstützen, problemlos mit demselben Schlüssel ver- und entschlüsselt werden.

**Ordner umbenennen oder verschieben**

*u.trust LAN Crypt* führt aus Performance-Gründen beim Verschieben ganzer Ordner innerhalb eines Laufwerks über den Windows Explorer keine Änderung des Verschlüsselungsstatus durch. Das bedeutet, dass es beim Verschieben eines ganzen Ordners zu keiner Ver-, Ent- bzw. Umschlüsselung kommt.

Waren die Dateien in solchen Ordnern verschlüsselt, bleiben sie unter dem neuen Ordnernamen bzw. am neuen Speicherort auch weiterhin verschlüsselt. Besitzt der Benutzer den dazugehörigen Schlüssel, kann er wie gewohnt mit diesen Dateien arbeiten.

Anders ist das Verhalten beim Verschieben von Dateien oder Ordnern auf eine andere Partition oder auf USB-Speichermedien, für die keine Verschlüsselungsregel eingerichtet wurde. Ist die *u.trust LAN Crypt* Funktion **Persistente Verschlüsselung** nicht aktiviert, werden die Dateien entschlüsselt, wenn sie auf derartige Medien verschoben werden. Hat der Security Officer oder der Systemadministrator dagegen die **Persistente Verschlüsselung** für die Client-Rechner aktiviert, bleiben die Dateien weiterhin verschlüsselt.

**Hinweis**

- Das gilt jedoch nur, wenn für den neuen Speicherort keine Verschlüsselungsregel besteht. Besteht eine solche jedoch, werden die Dateien nach der geltenden Verschlüsselungsregel des neuen Speicherortes verschlüsselt.

**Sicheres Verschieben**

*u.trust LAN Crypt* unterstützt das sichere Verschieben von Dateien und Ordnern. Beim Verschieben durch *u.trust LAN Crypt* werden die Dateien auch am neuen Speicherort entsprechend den geltenden Verschlüsselungsregeln ver-, ent- bzw. umgeschlüsselt. Danach werden die Quelldateien sicher gelöscht.

Diese Funktion steht über den Eintrag **u.trust LAN Crypt Sicheres Verschieben** im Windows Explorer Kontextmenü von *u.trust LAN Crypt* zur Verfügung. Über einen Dialog kann dann ausgewählt werden, wohin die Dateien verschoben werden sollen.

**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,
- und die **Persistente Verschlüsselung** ist nicht aktiv.

  **Hinweis**

  - *u.trust LAN Crypt* kann auch Offlineordner in Windows verschlüsseln. Allerdings können hierbei in Verbindung mit Virenscannern Probleme auftreten. Genauere Informationen zu bekannten Problemen mit Virenscannern finden Sie in den Versionsinfos zum *u.trust LAN Crypt* Client.

**Löschen verschlüsselter Dateien**

Wenn Ihr Verschlüsselungsprofil geladen ist, können Sie jede verschlüsselte Datei löschen, für die Sie einen Schlüssel besitzen.

**Hinweis**

- Eigentlich handelt es sich beim Löschen von Dateien um ein Verschieben der Dateien in den Windows Papierkorb. Um den höchsten Sicherheitsstandard zu gewährleisten, bleiben die mit *u.trust LAN Crypt* verschlüsselten Dateien auch im Papierkorb verschlüsselt. Um den Papierkorb zu leeren ist kein Schlüssel notwendig.

**Von der Verschlüsselung ausgenommene Dateien und Ordner**

Folgende Dateien und Ordner sind automatisch von der Verschlüsselung ausgenommen, auch wenn für sie eine Verschlüsselungsregel definiert wurde:

- Dateien im Installationsordner von *u.trust LAN Crypt*
- Dateien in den Ordnern *Programme* und *Programme (x86)*
- Dateien im Installationsordner von *Windows*
- Dateien im Ordner *Windows.old*
- Richtliniendatei-Cache

Der Speicherort des lokalen Richtlinien-Caches wird in der *u.trust LAN Crypt* Client Richtlinie (Gruppenrichtlinie) bestimmt. Der *u.trust LAN Crypt* Client zeigt den eingestellten Speicherort in der Registerkarte **Profil** im Menü *Client-Status* an.

- Stammverzeichnis des Systemlaufwerkes. Unterordner werden nicht ausgeschlossen.
- Indizierte Speicherorte (search-ms)
- Dateien in Ordnern, die in *u.trust LAN Crypt* mit einer Ausnahme- oder Ignorieren-Regel definiert sind.

**Persistente Verschlüsselung**

Für *u.trust LAN Crypt* kann ein Security Officer oder Systemadministrator über eine **u.trust LAN Crypt Gruppenrichtlinie (GPO)** die **Persistente Verschlüsselung** konfigurieren. Dateien werden normalerweise nur dann verschlüsselt, wenn sie einer Verschlüsselungsregel unterliegen.

Wenn zum Beispiel ein Benutzer eine verschlüsselte Datei in einen Ordner kopiert, für den keine Verschlüsselungsregel definiert ist, wird die Datei im Zielordner entschlüsselt. Ist die **Persistente Verschlüsselung** dagegen aktiviert, bleiben Dateien auch dann verschlüsselt, wenn sie an einen anderen Speicherort verschoben oder kopiert werden, für den keine Verschlüsselungsregel besteht.

Security Officer oder Systemadministratoren können dieses Verhalten über eine *u.trust LAN Crypt* Gruppenrichtlinie (GPO) einstellen. Wird die **Persistente Verschlüsselung** deaktiviert, so werden Dateien entschlüsselt, wenn sie an einen Speicherort kopiert oder verschoben werden, für den keine Verschlüsselungsregel besteht. Auf diese Weise können beispielsweise Dateien entschlüsselt werden, um sie z. B. als E-Mail-Anhang zu verschicken. Besser wäre es allerdings, die **Persistente Verschlüsselung** aktiviert zu lassen und solche Dateien stattdessen in einen Ordner zu kopieren, für

den eine Ignorieren- oder Ausnahmeregel besteht. So könnte die Schutzfunktion der **Persistenten Verschlüsselung** weiterhin erhalten bleiben und gleichzeitig ein Speicherort vorhanden sein, in den Benutzer Dateien explizit entschlüsseln könnten, um sie beispielsweise als E-Mail zu versenden.

Für die **Persistente Verschlüsselung** gelten folgende Regeln:

- Der *u.trust LAN Crypt* Treiber behält nur den Namen der Datei ohne Pfadinformationen. Es werden somit nur Situationen erfasst, in denen Quell- und Zieldatei einen identischen Namen haben. Sollte die Datei jedoch während des Kopiervorgangs umbenannt werden, wird die resultierende Datei als eine neue Datei betrachtet und unterliegt daher nicht der **Persistenten Verschlüsselung**.
- Wenn ein Benutzer eine verschlüsselte Datei durch **Speichern unter** an einem Ort speichert, für den keine Verschlüsselungsregel besteht, unterliegt dies auch nicht der **Persistenten Verschlüsselung**. Das Ergebnis ist dann ebenfalls eine Klartextdatei.
- Informationen zu Dateien werden nur für eine begrenzte Zeit beibehalten. Dauert der Vorgang zu lange (z. B. das Kopieren oder Bewegen länger als 15 Sekunden), wird die resultierende Datei als eine neue Datei betrachtet und unterliegt daher nicht der **Persistenten Verschlüsselung**. Die Datei ist dann ebenfalls unverschlüsselt.

  **Hinweis**

  - Persistente Verschlüsselung verwendet den Windows-Tunneling-Cache. Wenn ein Thread eine verschlüsselte Datei öffnet und anschließend innerhalb des Tunneling-Intervalls (Standard: 15 s) eine Datei mit *dem gleichen Namen* erstellt, wird die neue Datei automatisch verschlüsselt - unabhängig vom Zielpfad und selbst dann, wenn für diesen Ort keine Verschlüsselungsrichtlinie existiert. Dieses Verhalten ist systemabhängig und sollte bei der Verwendung von LAN Crypt berücksichtigt werden.

#### Persistente Verschlüsselung und Verschlüsselungsregeln

Die **Persistente Verschlüsselung** stellt sicher, dass eine verschlüsselte Datei ihren Verschlüsselungsstatus beibehält, d. h. den ursprünglichen Verschlüsselungsschlüssel. Dies funktioniert mithilfe der **Persistenten Verschlüsselung** problemlos, wenn die Datei in einen Ordner ohne Verschlüsselungsregel kopiert oder verschoben wird. Wird die Datei jedoch an einen Speicherort kopiert oder verschoben, für den eine andere Verschlüsselungsregel besteht, hat diese Verschlüsselungsregel allerdings Vorrang vor der **Persistente Verschlüsselung**. Die Datei wird dann gemäß der für diesen Speicherort geltenden Verschlüsselungsregel und mit dem hierfür definierten Verschlüsselungsalgorithmus (z. B. AES) und Schlüssel umgeschlüsselt.

#### Persistente Verschlüsselung und Ignorieren-Regeln

Eine Ignorieren-Regel setzt die **Persistente Verschlüsselung** für alle Ordner außer Kraft, für die solch eine Regel besteht. Das bedeutet, dass Dateien, die in einen Ordner kopiert werden, für den eine Ignorieren-Regel besteht, entschlüsselt werden.

Die Ignorieren-Regel wird hauptsächlich für Dateien benutzt, auf die sehr häufig zugegriffen wird oder bei denen kein bestimmter Grund für eine Verschlüsselung vorliegt. Dadurch lässt sich die System-Leistung steigern.

#### Persistente Verschlüsselung und Ausnahmeregeln

Eine Ausnahmeregel setzt die **Persistente Verschlüsselung** für einen mit einer solchen Regel definierten Ordner außer Kraft. Das bedeutet, dass Dateien, die in einen Ordner kopiert werden, für den eine Ausnahmeregel gilt, entschlüsselt werden.

### Einschränkungen bei der persistenten Verschlüsselung

Bei der **persistenten Verschlüsselung** gelten einige Einschränkungen.

#### Dateien, die eigentlich unverschlüsselt bleiben sollten, sind verschlüsselt

**Klartext-Dateien werden an mehrere Speicherorten kopiert, ohne dass Verschlüsselungsregeln angewendet werden.**

- Wenn eine unverschlüsselte Datei gleichzeitig an mehrere Speicherorte, von denen für einen Speicherort eine Verschlüsselungsregel gilt, kopiert wird, werden die anderen Kopien der Datei möglicherweise auch verschlüsselt.

**Nach dem Zugriff auf eine verschlüsselte Datei eine Datei mit dem gleichen Namen erstellen**

- Wird kurz nach dem Öffnen einer mit *u.trust LAN Crypt* verschlüsselten Datei eine Datei mit dem gleichen Namen erstellt, wird die neu erstellte Datei mit dem gleichen Schlüssel wie die zuerst geöffnete Datei verschlüsselt.
- Dies gilt nur dann, wenn für das Lesen der verschlüsselten Datei und das Erstellen einer neuen Datei die gleiche Anwendung / der gleiche Thread verwendet wird.

#### Dateien werden nicht verschlüsselt

**Von einer Datei werden mehrere Kopien angelegt**

Werden Kopien von einer verschlüsselten Datei im gleichen Ordner wie die ursprüngliche Datei erstellt, so werden diese Kopien nicht verschlüsselt. Da die erstellten Kopien unterschiedliche Dateinamen haben (zum Beispiel *datei.txt* im Gegensatz zu *datei-kopie.txt*), schlägt der Abgleich des Dateinamens fehl und sie werden daher nicht im Rahmen der **Persistenten Verschlüsselung** verschlüsselt.

**Client-API und Verschlüsselungs-Tags für DLP-Produkte**

Identifiziert eine **Data Loss Prevention** (DLP) Anwendung Dateien, die verschlüsselt werden sollen, so kann es die *u.trust LAN Crypt* Client-API verwenden, um diese Dateien zu verschlüsseln. Sie können unter der *u.trust LAN Crypt* **Administration** (siehe Administrator-Handbuch) unterschiedliche Verschlüsselungs-Tags definieren, die den zu verwendenden *u.trust LAN Crypt*-Schlüssel angeben. Die Client-API kann diese vordefinierten Verschlüsselungs-Tags verwenden, um bestimmte Schlüssel auf unterschiedliche Inhalte anzuwenden. Zum Beispiel kann der Verschlüsselungs-Tag `<CONFIDENTIAL>`verwendet werden, um somit alle Dateien zu verschlüsseln, die von Ihrer DLP-Anwendung als vertraulich eingestuft sind.

## Aktivieren und Deaktivieren der transparenten Verschlüsselung

Wird die transparente Verschlüsselung im *u.trust LAN Crypt* Benutzermenü deaktiviert, werden Dateien, auf die nach der Deaktivierung zugegriffen wird, nicht mehr automatisch ver- bzw. entschlüsselt. Neu erzeugte Dateien bleiben unverschlüsselt, auch wenn für diese eine Verschlüsselungsregel im Verschlüsselungsprofil des Benutzers vorhanden ist. Bereits verschlüsselte Dateien bleiben verschlüsselt. Dies kann dazu genutzt werden, um beispielsweise eine durch *u.trust LAN Crypt* verschlüsselte Datei als Dateianhang per E-Mail vertraulich verschicken zu können.

**Hinweis**

- Die Einstellungen, welche Funktionen bzw. Elemente über das Benutzermenü ausgewählt werden können, kann der Security Officer bzw. System Administrator über eine *u.trust LAN Crypt* Gruppenrichtlinie (GPO) einstellen. Der Client lässt sich auf diese Weise beispielsweise auch so konfigurieren, dass der Benutzer die transparente Verschlüsselung nicht selbst deaktivieren kann.

Im Vergleich hierzu führt eine Deaktivierung der **Persistenten Verschlüsselung** dazu, dass beim Kopieren / Verschieben von verschlüsselten Dateien an einen Ort bzw. Ordner, für den keine Verschlüsselungsregel besteht, dass diese dort entschlüsselt werden. Die regelbasierte automatische Ver- und Entschlüsselungsfunktion für Ordner und Dateien (vgl. Transparente Verschlüsselung bleibt bei einer Deaktivierung der persistenten Verschlüsselung weiterhin bestehen. Die Konfiguration der persistenten Verschlüsselung erfolgt durch den Security Officer oder Administrator ebenfalls über eine *u.trust LAN Crypt* Gruppenrichtlinie (GPO).

Wenn Sie die Funktion **Persistente Verschlüsselung** aktiviert haben, bleiben verschlüsselte Dateien auch dann verschlüsselt, wenn sie in an einen Ort bzw. in einen Ordner ohne Verschlüsselungsregel kopiert oder verschoben werden. Wenn Sie die **Persistente Verschlüsselung** verwenden, ist es nicht notwendig, vorher die transparente Verschlüsselung zu deaktivieren, um verschlüsselte Dateien an einen anderen Ort zu kopieren. Die **Persistente Verschlüsselung** sorgt dafür, dass Dateien auch

dann verschlüsselt bleiben, wenn sie versehentlich in einen anderen Ordner verschoben wurden oder wenn der Benutzer vergessen hat, die Verschlüsselung vor dem Verschieben bzw. Kopieren zu deaktivieren. Sie müssen den Computer neu starten, damit vorgenommene Änderungen der **Persistenten Verschlüsselung** (aktiv oder nicht aktiv) Wirkung zeigen.

**Hinweis**

- Ist die **Persistente Verschlüsselung** aktiv und ein Benutzer verschiebt oder kopiert eine Datei in einen Ordner, für den eine Ignorieren-Regel oder Ausnahmeregel gilt, so wird diese Datei an diesem Ort entschlüsselt abgelegt. Beachten Sie auch, dass eine Änderung der Einstellung für die **Persistente Verschlüsselung** einen Neustart des Client-Rechners erfordert. Bis zum Neustart des Rechners behält die zuvor definierte Einstellung weiterhin ihre Gültigkeit.

## Transparente Verschlüsselung und Komprimierungsprogramme

Komprimierungsprogramme öffnen Dateien, lesen deren Inhalte und erzeugen hieraus eine komprimierte Archivdatei. Die gepackten Archivdateien können mithilfe des Komprimierungsprogramms jederzeit wieder entpackt werden. Auf diese Weise lassen sich die ursprünglichen Dateien an jedem beliebigen Ort wiederherstellen. Wenn die transparente Ent-/Verschlüsselung aktiviert ist, erhalten diese Programme die entschlüsselten Dateien und diese werden dann komprimiert. Die Dateien im Archiv selbst sind dann nicht mehr mit *u.trust LAN Crypt* verschlüsselt. Wird das Archiv an einem Ort bzw. in einem Ordner gespeichert, für den keine Verschlüsselungsregel existiert, dann sind alle Dateien im Klartext und damit unverschlüsselt.

Auch wenn die **Persistente Verschlüsselung** aktiviert ist, werden die Dateien unverschlüsselt komprimiert. Die Archivdatei selbst bleibt jedoch verschlüsselt und kann nur von einem Benutzer gelesen werden, der den hierfür erforderlichen Schlüsselt besitzt. Voraussetzung hierfür ist jedoch, dass auch Archivdateien einer Verschlüsselungsregel unterliegen.

Wenn Sie allerdings auch verschlüsselte Dateien mithilfe von Komprimierungsprogrammen in eine Archivdatei packen wollen, muss die transparente Verschlüsselung vor der Verwendung solcher Programme deaktiviert werden. Diese Vorgehensweise ist meist nur dann erforderlich, wenn für die zu erstellende Archivdatei keine Verschlüsselungsregel besteht. Ist aber eine solche vorhanden, wären die Dateien innerhalb der erstellten Archivdatei zwar unverschlüsselt, die Archivdatei selbst aber wiederum analog der hierfür definierten Verschlüsselungsregel verschlüsselt und somit vor unautorisiertem Zugriff sicher geschützt. Eine weitere Möglichkeit um sicherzustellen, dass Dateien verschlüsselt in eine Archivdatei gepackt werden, besteht darin, Komprimierungsprogramme als Unberücksichtigte Anwendung zu definieren. Dies kann im Bedarfsfall durch den (Master) Security Officer (MSO / SO) oder Systemadministrator über die *u.trust LAN Crypt* Gruppenrichtlinie (GPO) konfiguriert werden.

## Cloud-Synchronisation

Bei der Installation werden bekannte Cloud-Synchronisationsanwendungen, darunter Microsoft OneDrive, Google Drive, Nextcloud und BoxDrive, automatisch so eingerichtet, dass sie in der Applikation registriert sind. Standardmäßig ist diesen Anwendungen und allen dazugehörigen untergeordneten Prozessen der Zugriff auf die Inhalte verschlüsselter Dateien untersagt.

Wenn Sie diese Beschränkung auf zusätzliche Cloud-Anwendungen und deren untergeordnete Prozesse ausweiten möchten, um zu verhindern, dass sie auf die Inhalte verschlüsselter Dateien zugreifen, können Sie zusätzliche Cloud-Synchronisationsanwendungen in der Systemregistrierung ergänzen:

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

Einstellung: `IgnoredCloudSyncApps`

Typ: `REG_MULTI_SZ`

## Initialverschlüsselung und explizite Verschlüsselung

Nach der Installation und Konfiguration von *u.trust LAN Crypt* können Sie eine Initialverschlüsselung durchführen. Dabei werden alle Dateien analog zu den Regeln des geladenen Verschlüsselungsprofils verschlüsselt. Die Initialverschlüsselung kann über eine der folgenden Methoden gestartet werden:

- *u.trust LAN Crypt* Taskleistensymbol (siehe Benutzerprogramm)
- *u.trust LAN Crypt* Explorer-Erweiterungen (siehe Explorer-Erweiterungen)

- **lcinit.exe**-Tool, das auch den Unattended-Modus unterstützt (siehe Initialverschlüsselung im Unattended-Modus ohne Benutzerinteraktion)

Neben der Initialverschlüsselung von ganzen Ordnern ist mit dem Kommandozeilen-Tool **lcinit.exe** und über die Explorer-Erweiterung auch die Ver-, Ent- und Umschlüsselung einzelner Dateien möglich.

**Hinweis**

- Bei der Initialverschlüsselung werden die Dateien lexikografisch sortiert angezeigt.

Die explizite Ver-, Ent- oder Umschlüsselung kann in folgenden Fällen erforderlich sein:

- Wenn sich unverschlüsselte Dateien in Ordnern befinden, für die eine (neue) Verschlüsselungsregel besteht.
- Wenn sich verschlüsselte Dateien in Ordnern befinden, für die keine Verschlüsselungsregel besteht.
- Wenn Dateien in verschlüsselten Ordnern mit einem falschen Schlüssel verschlüsselt sind.
- Wenn sich die Verschlüsselungsregeln im Verschlüsselungsprofil geändert haben.
- Wenn Dateien versehentlich mit mehreren Schlüsseln verschlüsselt wurden.

**Assistent zur Initialverschlüsselung**

Das Tool für die Initialverschlüsselung, **lcinit.exe**, verfügt über einen Assistenten mit einer grafischen Benutzeroberfläche. Dieser Assistent unterstützt

- das Ver-, Ent- und Umschlüsseln von Dateien und
- das Prüfen des Verschlüsselungsstatus von Dateien – auch in Ordnern und Unterordnern.

Sie können den **Assistenten starten**, indem Sie

- auf das Taskleistensymbol klicken oder
- `Start/Programme/u.trust LAN Crypt Client/Initialverschlüsselung` wählen oder
- diesen aus dem Windows-Startbildschirm starten oder
- auf die Datei **lcinit.exe** im *u.trust LAN Crypt*-Installationsordner, Unterordner *Apps* doppelklicken.

**Hinweis**

- Die Ver-, Ent- und Umschlüsselung erfolgt immer analog zu den Regeln eines geladenen Verschlüsselungsprofils. Daher muss hierzu grundsätzlich ein Verschlüsselungsprofil geladen sein.

**Initialverschlüsselung durchführen**

**Schritt 1:** Starten Sie den Assistenten (siehe Benutzermenü).

**Schritt 2:** Wählen Sie die Option Initialverschlüsselung durchführen in Schritt 1/5.

**Schritt 3:** Klicken Sie auf **Weiter**. **Schritt 4:** Legen Sie nun in Schritt 2/5 fest, wie mit den Dateien verfahren werden soll.

- **Dateien den Regeln entsprechend verschlüsseln** Wenn Sie diese Option auswählen, werden die Dateien nach den im Profil des Benutzers stehenden Regeln verschlüsselt (Standardeinstellung). Bereits korrekt verschlüsselte Dateien werden bei diesem Vorgang übersprungen.
- **Dateien den Regeln entsprechend umschlüsseln** Wenn Sie diese Option auswählen, werden Dateien, die mit einem anderen Schlüssel als im Profil festgelegt verschlüsselt sind, entschlüsselt und mit dem korrekten Schlüssel verschlüsselt.

**Hinweis**

- Voraussetzung hierfür ist, dass der Schlüssel, mit dem die Datei(en) verschlüsselt wurden, dem Benutzer über sein Profil zur Verfügung steht.

**Schritt 5:** Klicken Sie danach auf **Weiter**. **Schritt 6:** Legen Sie nun über die Ordnerstruktur in Schritt 3/5 fest, welche Laufwerke/Ordner verschlüsselt oder umgeschlüsselt werden sollen.

Ausgewählte Laufwerke und Ordner werden mit einem Häkchen markiert. Ein Häkchen mit einem zusätzlichen „+" Zeichen bei einem Ordner zeigt an, dass sich darin noch weitere Unterordner befinden, die nicht bearbeitet werden, in denen also keine Verschlüsselung oder Umschlüsselung der Dateien durchgeführt wird. Wenn diese auch bearbeitet werden sollen, sind diese per Mausklick ebenfalls mit einem Häkchen zu markieren.

Klicken Sie auf **Profilregeln**, um automatisch alle Ordner zu markieren, für die Verschlüsselungsregeln im Profil des Benutzers bestehen.

Klicken Sie auf **Erweitert**, um weitere Einstellungen für die Initialverschlüsselung anzuzeigen.

**Hinweis**

- Welche Einstellung vom Benutzer geändert werden können, ist von der Konfiguration des *u.trust LAN Crypt* Clients abhängig. Der Security Officer oder Systemadministrator nimmt die Konfiguration zentral über die Gruppenrichtlinie (GPO) von *u.trust LAN Crypt* vor (siehe Kapitel 4 „Menüeinträge aktivieren" im Admin-Handbuch).

- **EFS verschlüsselte Dateien, wenn notwendig, entschlüsseln** Wählen Sie diese Option, um EFS verschlüsselte Dateien zu entschlüsseln und umzuschlüsseln. Beachten Sie, dass eine entsprechende Verschlüsselungsregel gelten muss. Wenn Sie diese Option nicht auswählen, werden EFS verschlüsselte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht von *u.trust LAN Crypt* umgeschlüsselt, auch wenn für sie eine Verschlüsselungsregel besteht.

- **NTFS-komprimierte Dateien, wenn notwendig, dekomprimieren** Wählen Sie diese Option, um NTFS-komprimierte Dateien zu dekomprimieren und zu verschlüsseln. Beachten Sie, dass eine entsprechende Verschlüsselungsregel gelten muss. Wenn Sie diese Option nicht auswählen, werden NTFS-komprimierte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht verschlüsselt, auch wenn für sie eine Verschlüsselungsregel besteht.

- **Dateien, die wiederholt mit mehreren Schlüsseln verschlüsselt wurden, entschlüsseln/ umschlüsseln** Wählen Sie diese Option, um Dateien umzuschlüsseln, die mit mehreren Schlüsseln verschlüsselt wurden. Die Dateien sind dann mit nur einem Schlüssel verschlüsselt. Beachten Sie, dass hierzu eine entsprechende Verschlüsselungsregel gelten muss.

  **Hinweis**

  - Diese Option ist nur verfügbar, wenn in Schritt 2/5 **Dateien entsprechend den Regeln verschlüsseln** oder **Dateien entsprechend den Regeln umschlüsseln** ausgewählt wurde. Andernfalls ist diese Option ausgegraut.

- **Nur folgende Dateien einschließen:** Wählen Sie hier bestimmte Dateitypen (.txt, .docx, usw.), die bei der Initialverschlüsselung berücksichtigt werden sollen. Bei der Angabe mehrerer Dateitypen in Form einer Liste, sind diese durch Strichpunkte (Semikola) voneinander zu trennen. Diese Einstellung wirkt sich nur auf Dateien aus, für die eine Verschlüsselungsregel gilt. Befinden sich noch weitere von dieser Regel abweichende Dateien in einem Ordner, bleiben diese im Rahmen der Initialverschlüsselung unberührt. Öffnet der Benutzer diese später und speichert sie wieder, werden sie gemäß den geltenden Verschlüsselungsregeln verschlüsselt.

**Schritt 7:** Klicken Sie auf **Weiter**. **Schritt 8:** Legen Sie nun in Schritt 4/5 fest, für welche Dateien Informationen im Bericht der Initialverschlüsselung enthalten sein sollen. Für den Bericht kann der Benutzer zwischen folgenden Optionen wählen:

- **Nur Fehler berichten** Der Statusbericht enthält nur Informationen über Dateien, bei denen während der Verschlüsselung Fehler aufgetreten sind.

- **Geänderte Dateien und Fehler berichten** Der Statusbericht enthält Informationen über alle Dateien, die geändert wurden oder bei denen während der Verschlüsselung Fehler aufgetreten sind.

- **Alle Dateien berichten** Der Statusbericht enthält Informationen über alle Dateien.

**Schritt 9:** Klicken Sie auf **Weiter**. In Schritt 5/5 wird das **Ergebnis** der Verschlüsselung, der **Schlüsselname** des verwendeten Schlüssels und der Verschlüsselungsalgorithmus angezeigt.

Ist bei einer bestimmten Datei die Verschlüsselung fehlgeschlagen, können Sie die Verschlüsselung über die Schaltfläche **Wiederholen** erneut starten.

Die Ergebnisse lassen sich per Mausklick auf die Spaltenüberschrift alphabetisch sortieren. Darüber hinaus können Sie den Statusbericht als XML-Datei an einem gewünschten Ort speichern (Schaltfläche **Exportieren**). Anhand des Statusberichtes können Sie später jene Dateien, bei denen die Verschlüsselung fehlgeschlagen ist, erneut versuchen zu verschlüsseln.

**Schritt 10:** Klicken Sie auf **Beenden**. Der Assistent wird geschlossen.

#### Verschlüsselungsstatus prüfen

**Schritt 1:** Starten Sie den Assistenten.

**Schritt 2:** Wählen Sie in Schritt 1 / 5 die Option **Verschlüsselungsstatus prüfen**.

**Schritt 3:** Klicken Sie auf **Weiter**.

**Schritt 4:** Legen Sie in Schritt 2 / 5 fest, welche Laufwerke und Ordner geprüft werden sollen.

**Schritt 5:** Wählen Sie die gewünschten Laufwerke und Ordner aus, indem Sie diese markieren.

Ein + Zeichen neben einem Häkchen bei einem Ordner zeigt an, dass sich darin Unterordner befinden, die nicht bearbeitet werden, in denen also keine Überprüfung des Verschlüsselungsstatus der Dateien durchgeführt wird. Soll die Überprüfung auch Unterordner einschließen, müssen diese ebenfalls per Mausklick gewählt werden, d. h. mit einem Häkchen markiert sein.

Klicken Sie auf **Profilregeln**, um automatisch alle Ordner zu markieren, für die Verschlüsselungsregeln im Profil des Benutzers existieren.

Klicken Sie auf **Erweitert**, um die Prüfung auf bestimmte Dateitypen einzuschränken:

- **Nur folgende Dateien einschließen**: Wenn Sie hier bestimmte Dateitypen angeben (z.B. .txt, .docx, .xlsx), so werden nur diese Dateitypen überprüft. Befinden sich auch noch weitere Dateien eines anderen Typs, der hier nicht angegeben ist, in dem Ordner, werden diese nicht berücksichtigt. Zur Angabe mehrerer Dateitypen ist eine durch Semikola getrennte Liste zu verwenden.

**Schritt 6:** Klicken Sie auf **Weiter**.

In Schritt 3 / 5 wird das **Ergebnis** der Prüfung, der **Schlüsselname** des verwendeten Schlüssels und der Verschlüsselungsalgorithmus angezeigt.

Die Ergebnisse lassen sich per Mausklick auf die Spaltenüberschrift alphabetisch sortieren.

Darüber hinaus können Sie den Statusbericht als XML-Datei an einem gewünschten Ort speichern (Schaltfläche **Exportieren**).

**Schritt 7:** Klicken Sie auf **Beenden**. Der Assistent wird geschlossen.

#### Dateien entschlüsseln

Dateien, die mit *u.trust LAN Crypt* verschlüsselt wurden, können entschlüsselt werden, wenn keine Verschlüsselungsregel (mehr) für sie besteht. Wurde eine erneute Initialverschlüsselung notwendig, zum Beispiel, weil sich Verschlüsselungsregeln im Profil des Benutzers geändert haben, können Dateien, für die es nun keine Verschlüsselungsregeln mehr gibt, über diesen Assistenten ganz einfach entschlüsselt werden.

Um Dateien zu entschlüsseln, wählen Sie im Assistenten zuerst **Initialverschlüsselung durchführen** (Schritt 1/5), dann **Entschlüsselung** > **Dateien mit den ausgewählten Schlüsseln entschlüsseln** (Schritt 2/5).

Anschließend können Sie die Schlüssel auswählen. Nur die Dateien, die mit einem der ausgewählten Schlüssel verschlüsselt wurden, werden entschlüsselt. Die Dateien werden jedoch nur dann

entschlüsselt, wenn für sie in der Richtliniendatei des Benutzers keine Verschlüsselungsregel mehr besteht.

**Hinweis**

- *u.trust LAN Crypt* entschlüsselt nur Dateien, für die keine Verschlüsselungsregel besteht. Sie können für diesen Vorgang bedenkenlos alle Schlüssel auswählen, die sie besitzen.

**Beispiel:** Der Assistent zur Initialverschlüsselung wird gestartet, weil Änderungen im Benutzerprofil vorgenommen wurden. Um sicherzustellen, dass nach dem Beenden des Assistenten zur Initialverschlüsselung alle Dateien den gewünschten Verschlüsselungsstatus haben, gehen Sie wie folgt vor:

1. Aktivieren Sie **Dateien entsprechend den Regeln verschlüsseln**. Alle Dateien werden gemäß den im Verschlüsselungsprofil definierten Verschlüsselungsregeln verschlüsselt.
2. Aktivieren Sie **Dateien entsprechend den Regeln umschlüsseln**. Müssen Dateien wegen einer Änderung von Verschlüsselungsregeln mit einem anderen Schlüssel verschlüsselt werden, werden sie umgeschlüsselt.
3. Aktivieren Sie **Dateien mit den ausgewählten Schlüsseln entschlüsseln** und wählen Sie dann alle Schlüssel aus. Verschlüsselte Dateien, für die keine Verschlüsselungsregel mehr bestehen, werden entschlüsselt. *u.trust LAN Crypt* entschlüsselt dabei ausschließlich Dateien, für die keine Verschlüsselungsregel besteht. Auch die Auswahl aller Schlüssel ist daher vollkommen unkritisch.

Alle Dateien besitzen nach dem erfolgreichen Beenden des Assistenten den korrekten Verschlüsselungsstatus.

Das explizite Entschlüsseln von Dateien kann dann wichtig sein, wenn die **Persistente Verschlüsselung** aktiviert ist. In diesem Fall werden Dateien nicht automatisch entschlüsselt, wenn sie aus einem Ordner, für den eine Verschlüsselungsregel gilt, in einen Ordner ohne Verschlüsselungsregel kopiert/verschoben werden. Mithilfe des Assistenten lassen sich solche Dateien auf einfache Weise wieder entschlüsseln.

### Initialverschlüsselung im Unattended-Modus (ohne Benutzerinteraktion)

Wenn **lcinit.exe** im Unattended-Modus ausgeführt werden soll, müssen Sie das Tool mit bestimmten Parametern über die Kommandozeile aus dem Ordner heraus aufrufen, in dem es sich befindet (zum Beispiel: `C:\Programme\Utimaco\u.trust LAN Crypt\Apps\`).

**Kommandozeilen-Syntax:**

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

**Parameter:**

**Startpath**

Gibt entweder eine einzelne Datei an, die ver-, ent- oder umgeschlüsselt werden soll (z. B. `C:\Daten\Vertrieb.docx`), oder einen Ordner, in dem die Ver-, Ent- oder Umschlüsselung durchgeführt werden soll (z. B. `D:\Daten`). Unterordner werden hierbei standardmäßig nicht miteinbezogen!

**%Profile**

Verarbeitet alle Regeln mit einem absoluten Pfad im geladenen Verschlüsselungsprofil. Ver- / entschlüsselt bzw. schlüsselt die Dateien, wenn notwendig, um.

**Hinweis**

- Zum Entschlüsseln muss für die entsprechenden Dateien im Profil eine EXCLUDE-Regel existieren.

**/s**

Inklusive aller Unterordner ab dem Startpfad.

**/h**

Oder alternativ **/?** - öffnet ein Hilfefenster zur Syntax von lcinit.exe.

**-DIgnoreDirectory**

Schließt diesen Ordner aus.

**/Tv**

Task-Modus: v = Zeigt den Verschlüsselungsstatus der Dateien an.

**/Te**

Task-Modus: e = Verschlüsselt, falls notwendig, Dateien gemäß dem Verschlüsselungsprofil.

**/Tr**

Task-Modus: r = Schlüsselt, falls notwendig, Dateien gemäß dem Verschlüsselungsprofil um.

**/Td**

Task-Modus: d = Entschlüsselt, falls notwendig, Dateien gemäß dem Verschlüsselungsprofil.

**/Tdk**

Task-Modus: dk = Entschlüsselt Dateien, die mit den angegebenen Schlüsseln verschlüsselt sind. Sie müssen die GUID für die Schlüssel angeben.

**Hinweis**

- Alle Task-Modus-Parameter können in einem Befehlsaufruf zusammen genutzt werden.

- **/Dc**

Diese Option dekomprimiert NTFS komprimierte Dateien und verschlüsselt diese anschließend. Ist diese Option nicht gesetzt, werden NTFS komprimierte Dateien von *u.trust LAN Crypt* ignoriert.

- **/De**

Diese Option entschlüsselt EFS-verschlüsselte Dateien und verschlüsselt diese anschließend mit *u.trust LAN Crypt*. Ist diese Option nicht gesetzt, werden EFS-verschlüsselte Dateien ignoriert.

- **/Dm**

Diese Option entschlüsselt mehrfach verschlüsselte Dateien und verschlüsselt sie anschließend neu. Die Dateien sind dann mit nur einem Schlüssel verschlüsselt.

- **+Ffiletype**

Wenn Sie mit dieser Option Dateitypen angeben (z. B. +Ftxt+Fdocx+Fxlsx), so werden ausschließlich Dateien der dort explizit angegebenen Dateitypen bearbeitet. Diese Einstellung wirkt sich nur auf Dateien aus, für die eine Verschlüsselungsregel existiert.

Enthält ein Ordner auch noch weitere Dateien, die nicht den Angaben dieser Option entsprechen, d. h. nicht den dort definierten Dateitypen angehören, bleiben diese bei der Initialverschlüsselung unberücksichtigt. Sie werden erst dann verschlüsselt, wenn sie durch den Benutzer bearbeitet oder durch diesen kopiert oder verschoben werden.

**Beispiel:** Die Datei „123.pdf" ist nicht verschlüsselt, weil Dateien des Typs „PDF" im o. g. Beispiel im Rahmen der Initialverschlüsselung nicht verschlüsselt werden sollen. Öffnet der Benutzer diese Datei, z. B. mit einem PDF-Editor, und speichert diese Datei im gleichen Ordner ab, wird die Datei verschlüsselt. Die Datei wird auch dann verschlüsselt, wenn der Benutzer eine solche Datei aus diesem Ordner heraus und dann wieder hineinkopiert. Bedingung hierfür ist jedoch, dass die für den Ordner definierte Verschlüsselungsregel auch für Dateien des Typs „PDF" gilt.

- **/V0**

Verbose Modus 0: Kein Reporting (Bericht).

- **/V1**

Verbose Modus 1: Listet Fehlermeldungen auf.

- **/V2**

Verbose Modus 2: Listet geänderte Dateien auf.

- **/V3**

Verbose Modus 3: Listet alle Dateien auf.

- **/V4**

Verbose Modus 4: Listet unverschlüsselte Dateien auf.

- **/E**

Bei Fehler abbrechen.

- **/X**

Initialverschlüsselung ohne Fenster ausführen.

- **/LLogfile**

Schreibt die Ausgabe in die dort angegebene Datei.

**Hinweis**

- Der Parameter /Td kann nur dann mit %Profile sinnvoll kombiniert werden, wenn die zu entschlüsselnden Dateien im Profil über eine Ausnahmeregel aufgeführt sind. Andernfalls muss /Td mit dem Startpfad kombiniert werden.

```
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
```

Listet alle Klartextdateien in `D:\Daten` und dessen Unterordnern auf.

---

# Richtlinien

## Zertifikate

Bevor ein Benutzer Zugriff auf sein Verschlüsselungsprofil hat, muss das entsprechende Zertifikat auf seinem Computer vorhanden sein. Der Security Officer muss diese Zertifikate an die Benutzer verteilen und ihnen auch das Passwort bzw. die PIN für den Zugriff auf ihr Zertifikat mitteilen. Dann importieren die Benutzer ihr Zertifikat auf ihren Computer. Sind die Zertifikate bereits bei der ersten Anmeldung verfügbar, läuft der gesamte Vorgang bis zur PIN-Eingabe ohne weitere Interaktion des Benutzers automatisch ab.

*u.trust LAN Crypt* bietet die Möglichkeit, die Zertifikate beim ersten Laden des Verschlüsselungsprofils automatisch zu importieren. In diesem Fall wird das System vom Security Officer so konfiguriert, dass *u.trust LAN Crypt* bei der ersten Anmeldung auch eine Zertifikatsdatei findet und dann den Importvorgang automatisch durchführt. Der Benutzer wird einmal aufgefordert, die PIN für den Import der PKCS#12 Schlüsseldatei einzugeben.

**Hinweis**

- Der (Master) Security Officer muss den Benutzern deren PIN auch beim automatischen Import ihrer Zertifikate mitteilen.

Das Zertifikat wird bei jedem Laden des Verschlüsselungsprofils geprüft. Wird ein gültiges Zertifikat gefunden, wird der Benutzer an *u.trust LAN Crypt* angemeldet. Ist kein gültiges Zertifikat vorhanden, kann der Benutzer nicht mit den verschlüsselten Daten arbeiten.

**Hinweis**

- Wenn die Anmeldung an *u.trust LAN Crypt* fehlschlägt, erhalten Benutzer eine Fehlermeldung mit einem entsprechenden Hinweis, weshalb die Anmeldung nicht möglich war.

Die spezifischen Verschlüsselungsregeln, die in den *u.trust LAN Crypt* Verschlüsselungsprofilen enthalten sind, ermöglichen dem Benutzer den Zugriff auf verschlüsselte Daten. Die Regeln definieren, welche Dateien in welchen Ordnern oder Laufwerken und mit welchem Schlüssel zu verschlüsseln sind. Es muss nur ein Verschlüsselungsprofil eines Benutzers geladen werden, dann finden Verschlüsselung und Entschlüsselung transparent im Hintergrund statt.

Der Benutzer selbst bemerkt die durchgeführten Verschlüsselungs-/Entschlüsselungsvorgänge nicht. Die Regeln lassen sich jederzeit und beliebig durch den *u.trust LAN Crypt* (Master) Security Officer (MSO/SO) ändern. So können beispielsweise auch Dateien mit einem anderen Schlüssel umgeschlüsselt werden.

**Hinweis**

- *u.trust LAN Crypt* importiert CA-Zertifikate, die in PKCS#12 Schlüsseldateien enthalten sein können, gemeinsam mit den Benutzerzertifikaten in den Ordner „Eigene Zertifikate -Zertifikate". Um Fehlermeldungen zu vermeiden, müssen CA-Zertifikate im Zertifikatsspeicher manuell nach „Vertrauenswürdige Stammzertifizierungsstellen" verschoben werden. Wenn Sie Zertifikate verwenden, die von *u.trust LAN Crypt* erzeugt wurden, ist ein solcher Schritt nicht erforderlich.

### Smartcard Leser

Da die Benutzung von Zertifikaten durch die Verwendung von Cryptographic Service Providern (CSPs) und Key Storage Providern (KSPs) abgewickelt wird, werden Smartcard-Leser automatisch unterstützt, wenn ein Smartcard-KSP verwendet wird. Der Zugriff auf die gespeicherten Verschlüsselungsinformationen kann so über ein auf Smartcard gespeichertes Zertifikat erfolgen.

**Hinweis**

- Wenn Sie Zertifikate auf Smartcards verwenden wollen, stellen Sie bitte sicher, dass der Smartcard Leser, die dazugehörige Middleware und ein entsprechender Service- oder Storage-Provider (CSP oder KSP) korrekt installiert sowie funktionsbereit sind!

**Hinweis**

- Bitte beachten Sie außerdem, dass Cryptographic Service Provider (CSP) für Schlüsseloperationen von u.trust LAN Crypt nur noch in Verbindung mit Shims unterstützt werden, die diesen als Key Storage Provider (KSP) ansprechbar machen.

## Laden der Richtliniendatei

#### Standardverhalten von u.trust LAN Crypt

Wenn sich ein Benutzer an Windows anmeldet, wird zuerst sein (zwischen)gespeichertes Benutzerprofil geladen. Danach prüft *u.trust LAN Crypt*, ob für den Benutzer eine neue Richtliniendatei verfügbar ist, indem es eine Verbindung zum festgelegten Speicherort für Richtliniendateien (Netzwerklaufwerk oder Webserver) aufbaut. Wird eine neuere Richtliniendatei gefunden, führt dies zu einer Aktualisierung des zwischengespeicherten Benutzerprofils.

Der Benutzer kann weiterhin mit verschlüsselten Daten arbeiten, während *u.trust LAN Crypt* noch überprüft, ob es eine neuere Version der Richtliniendatei gibt. Ist der für die Richtliniendatei angegebene Speicherort nicht erreichbar, arbeitet der Benutzer dann solange mit dem zwischengespeicherten Benutzerprofil, bis dieses aktualisiert werden kann.

**Hinweis**

- *u.trust LAN Crypt* verifiziert die Zertifikate der Benutzer und das öffentliche Zertifikat vom (Master) Security Officer (.cer), der die Richtliniendatei erstellt hat. Enthält ein Zertifikat einen „CRL Distribution Point" und es ist keine gültige CRL auf dem System verfügbar, versucht Windows, eine CRL von der angegebenen Adresse zu importieren. Ist eine Firewall aktiv, wird unter Umständen eine Meldung angezeigt, dass ein Programm (*loadprof.exe*) versucht, eine Verbindung zum Internet herzustellen. In seltenen Fällen kann auch das Laden des Benutzerprofils diese Meldung auslösen.

#### Durch Security Officer festgelegtes Verhalten

Ein Security Officer kann das Standardverhalten durch zentrale Einstellungen beeinflussen. Security Officer können festlegen, wie lange die zwischengespeicherte Richtlinie auf den Client-Computern gültig sein soll. Darüber hinaus können sie die Aktualisierungs-Intervalle der Richtliniendateien festlegen. Die jeweiligen Einstellungen, die der Security Officer vorgenommen hat, werden in der Registerkarte **Profil** des Dialogs **Client-Status** angezeigt (siehe Der Dialog Client-Status).

Innerhalb des dort angegebenen Zeitraumes ist die Richtliniendatei auf dem Client gültig und der Benutzer hat Zugriff auf verschlüsselte Dateien, auch dann, wenn keine Verbindung zum Speicherort der Richtliniendatei besteht.

Läuft die angegebene Dauer ab, versucht *u.trust LAN Crypt* erneut die Richtliniendatei vom Netzwerklaufwerk zu laden, um sie zu aktualisieren. Ist dies nicht möglich, wird die Richtliniendatei entladen. Der Benutzer hat keinen Zugriff mehr auf verschlüsselte Dateien.

Erst wenn wieder eine gültige Richtliniendatei zur Verfügung steht (z. B. bei der nächsten Anmeldung mit einer Verbindung zum Speicherort der Richtliniendateien für die Clients), wird die Richtliniendatei beim Benutzer aktualisiert und geladen. Der Benutzer hat dann wieder Zugriff auf verschlüsselte Dateien. Der Zähler für die Dauer der Zwischenspeicherung wird zurückgesetzt.

Die Angabe der Dauer der Zwischenspeicherung kann einerseits sicherstellen, dass die Client-Computer in regelmäßigen Intervallen mit aktuellen Richtliniendateien versorgt werden und die Benutzer immer aktuelle Richtlinien verwenden. Andererseits kann durch die Beschränkung der Gültigkeitsdauer verhindert werden, dass Benutzer mit Richtliniendateien unbeschränkt lange weiterarbeiten können. Ist diese Option auf **nicht konfiguriert gesetzt**, können Benutzer mit einer zwischengespeicherten Version der Richtliniendatei unbeschränkt lange arbeiten.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung zurückgesetzt:

- Der Speicherort der Richtliniendateien ist erreichbar und es wurde eine gültige Richtliniendatei auf den Client übertragen (z. B. bei der Anmeldung des Benutzers, oder ausgelöst durch ein definiertes Aktualisierungsintervall).
- Eine neue Richtliniendatei ist verfügbar und wurde erfolgreich geladen.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung **NICHT** zurückgesetzt:

- Der Client-Computer versucht, eine neue Richtliniendatei zu erhalten. Der Speicherort der Richtliniendateien ist jedoch nicht erreichbar.
- Eine neue Richtliniendatei wurde übertragen. Sie konnte aber aufgrund eines Fehlers nicht geladen werden.
- Eine neue Richtliniendatei ist verfügbar. Diese Richtliniendatei erfordert aber ein neues Zertifikat. Der Benutzer besitzt dieses Zertifikat nicht oder kann es nicht laden.

Schlägt die Aktualisierung der Richtliniendatei fehl, wird auf dem Client-Computer der Ablaufzeitpunkt der zwischengespeicherten Richtliniendatei in Form einer Sprechblasen-Hilfe angezeigt. Der Benutzer kann dann eine manuelle Aktualisierung über das *u.trust LAN Crypt* Taskleistensymbol anstoßen (Benutzermenü).

#### Keine Zwischenspeicherung der Richtliniendatei

Ein Security Officer kann festlegen, dass die Richtliniendatei nicht zwischengespeichert werden soll. Das bedeutet, dass der Benutzer sein Benutzerprofil bei der Anmeldung nur dann erhält, wenn der Speicherort der Richtliniendatei auch erreichbar ist. Ist dieser nicht erreichbar oder tritt ein Fehler beim Laden des Profils auf, kann der Benutzer nicht auf verschlüsselte Dateien zugreifen.

## Anmeldung an u.trust LAN Crypt

*u.trust LAN Crypt* Verschlüsselungsprofile werden von einem Security Officer entsprechend der firmenweiten Sicherheitspolitik für die Benutzer erstellt und in Richtliniendateien gespeichert. Ein Verschlüsselungsprofil kann nur geladen werden, wenn der Benutzer auch über das hierfür erforderliche Zertifikat verfügt.

Der Pfad der Richtliniendatei wird vom Systemadministrator oder Security Officer durch eine *u.trust LAN Crypt* Gruppenrichtlinie (GPO) in die Registrierung der Client-Rechner eingetragen. Wenn sich ein Benutzer an *u.trust LAN Crypt* anmeldet, wird das Verschlüsselungsprofil, das in der Richtliniendatei gespeichert ist, vom Client-Rechner geladen. *u.trust LAN Crypt* lädt die Richtliniendateien aus dem angegebenen Ort (z. B. eine Netzwerkfreigabe) und prüft anhand des Benutzerzertifikats, ob der Benutzer berechtigt ist, es zu laden.

### Anmeldung mit Sicherheitstoken

Benutzer können für die Anmeldung an *u.trust LAN Crypt* auch einen Sicherheitstoken verwenden. Voraussetzung dafür ist, dass das *u.trust LAN Crypt* Benutzerzertifikat auf dem Token gespeichert ist. Wird das Benutzerzertifikat auf einem mit dem System verbundenen Token gefunden, erfolgt die Anmeldung.

Werden Token zur Anmeldung verwendet, kann es vorkommen, dass *u.trust LAN Crypt* eine Richtliniendatei zu laden versucht, bevor der Token vom Betriebssystem korrekt identifiziert wurde. In diesem Fall wird eine Meldung angezeigt, dass das Benutzerzertifikat nicht gefunden wurde, obwohl der Token bereits mit dem System verbunden ist.

Dann muss der Benutzer die Richtliniendatei manuell laden. Dies erfolgt über die Benutzeranwendung in der Task-Leiste > **Verschlüsselungsregeln laden**. Dadurch wird der Token identifiziert und die Anmeldung wird durchgeführt. Sie können jedoch in der *u.trust LAN Crypt* Konfiguration (Einstellung **Verzögerung beim Laden des Profils**) auch eine Verzögerung angeben, sodass der Token mit hoher Wahrscheinlichkeit immer identifiziert wird und somit die Anmeldung hiermit durchgeführt werden kann.

# Benutzerprogramm

Ein Schlüssel-Symbol in der Taskleiste zeigt den Status von *u.trust LAN Crypt* an.

**Grün:** Verschlüsselungsregeln wurden geladen, die transparente Verschlüsselung ist aktiviert.

**Gelb:** Verschlüsselungsregeln wurden geladen, die transparente Verschlüsselung ist aktiviert.

**Rot:** Es ist kein Profil geladen.

## Benutzermenü

Ein Rechtsklick auf das Schlüssel-Symbol öffnet das *u.trust LAN Crypt* Benutzermenü mit folgenden Einträgen:

- **Verschlüsselungsregeln laden/Verschlüsselungsregeln aktualisieren**
- **Lösche Verschlüsselungsregeln**
- **Verschlüsselung deaktivieren/aktivieren**
- **Profil anzeigen**
- **Client-Status**
- **Initialverschlüsselung**
- **Schließen**
- **Info**

  **Hinweis**

  - Welche der o. a. Menüeinträge tatsächlich verfügbar sind, ist von der Konfiguration des *u.trust LAN Crypt* Clients abhängig. Der Security Officer bzw. Systemadministrator von Windows kann die Konfiguration hierfür zentral über die Gruppenrichtlinie von *u.trust LAN Crypt* vornehmen.

**Verschlüsselungsregeln laden/Verschlüsselungsregeln aktualisieren**

Mit diesem Befehl werden die aktuell gültigen Verschlüsselungsrichtlinien geladen. Dies ist dann wichtig, wenn im laufenden Betrieb das Verschlüsselungsprofil geändert wurde.

**Lösche Verschlüsselungsregeln**

Diese Option verhindert den Zugriff auf verschlüsselte Daten. Dies stellt eine Sicherheitsfunktion dar, die die verschlüsselten Daten auf dem Rechner vor unbefugtem Zugriff schützt, wenn der Arbeitsplatz kurzfristig verlassen werden muss. Die Verwendung des privaten Schlüssels muss entweder durch ein Passwort geschützt sein bzw. bei Verwendung eines Sicherheitstokens oder einer Smartcard mit einem Leser die PIN abfragen. Ansonsten könnte das Profil durch den Befehl **Verschlüsselungsregeln laden** einfach wieder geladen werden.

**Verschlüsselung deaktivieren/aktivieren**

Schaltet die transparente Verschlüsselung ein bzw. aus.

Das Ausschalten der transparenten Verschlüsselung kann von Bedeutung sein, wenn Dateien weiterhin verschlüsselt bleiben sollen, die von einem verschlüsselten Ordner an einen Ort kopiert oder verschoben werden, für den keine Verschlüsselungsregel besteht. Bei aktivierter Verschlüsselung würden diese Dateien dann entschlüsselt werden.

Wenn zum Beispiel eine verschlüsselte Datei an eine E-Mail angehängt wird, würde sie bei aktivierter Verschlüsselung automatisch entschlüsselt werden. Ist die transparente Verschlüsselung jedoch deaktiviert, können verschlüsselte Dateien als Anhang von E-Mails versendet werden.

**Hinweis**

- Wenn durch den Administrator die Funktion **Persistente Verschlüsselung** aktiviert wurde, bleiben verschlüsselte Dateien auch dann verschlüsselt, wenn sie an einen Ort kopiert oder verschoben werden, für den keine Verschlüsselungsregel existiert. Die transparente Verschlüsselung müsste somit nicht, wie im Beispiel oben angegeben, deaktiviert werden, um eine Datei verschlüsselt als Anhang von E-Mails zu versenden.

**Profil anzeigen** Zeigt auf zwei Registerkarten die Verschlüsselungsregeln und die in den Verschlüsselungsinformationen enthaltenen Schlüssel an.

Die Registerkarte *Aktive Verschlüsselungsregeln* enthält eine Übersicht der gültigen Regeln für den angemeldeten Benutzer. Zusätzlich stehen dem Benutzer folgende Optionen zur Verfügung: *Ignorieren-Regeln anzeigen*, *Ausnahmeregeln anzeigen*, *Verschlüsselungstags anzeigen* und *Bypass-Regeln anzeigen*.

Die Registerkarte *Verfügbare Schlüssel* zeigt alle für den Benutzer verfügbaren Schlüssel an.

**Client-Status**

Die Funktion **Client-Status** zeigt auf mehreren Registerkarten detaillierte Informationen zum aktuellen Status des *u.trust LAN Crypt* Clients (siehe Der Dialog Client-Status).

**Initialverschlüsselung**

Startet den Assistenten für die Initialverschlüsselung der gewünschten Dateien (siehe Initialverschlüsselung und explizite Verschlüsselung).

**Schließen**

Schließt das *u.trust LAN Crypt* Benutzerprogramm

**Info**

Zeigt Informationen zur Version von *u.trust LAN Crypt* an.

**Hinweis**

- Die Option „**Schließen**“ schließt nur das *u.trust LAN Crypt* Benutzerprogramm. *u.trust LAN Crypt* behält aber weiterhin seinen aktuellen Status. Dies bedeutet, dass die transparente Ver- und Entschlüsselung weiterhin ausgeführt wird.

## Der Dialog Client-Status

Die Option **Client-Status** zeigt mehrere Registerkarten mit Informationen zu den Verschlüsselungseinstellungen auf dem Computer des Benutzers an.

Diese sind:

**Status**

Diese Registerkarte zeigt an, ob das Benutzerprofil geladen ist und ob die Verschlüsselung aktiv ist. Zudem werden detaillierte Informationen zur Richtliniendatei angezeigt (Erstellungsdatum, Security Officer, der die Datei erstellt hat, etc.). Solange das Benutzerprofil geladen ist, ist auch die Verschlüsselung aktiviert.

Die Verschlüsselung kann bei geladenem Benutzerprofil aber auch (temporär) deaktiviert werden.

**Einstellungen** Diese Registerkarte enthält Informationen zu den aktuell für den Client gültigen Einstellungen. Diese Einstellungen werden zentral festgelegt und betreffen die Verschlüsselung, das Taskleistensymbol und den **Assistenten zur Initialverschlüsselung**. Es wird unter anderem angezeigt, ob die **Persistente Verschlüsselung** aktiviert ist und welche Menüeinträge auf dem Client-Computer angezeigt werden.

**Profile** Diese Registerkarte zeigt die Einstellungen des Benutzerprofils.

**Zertifikate** Diese Registerkarte zeigt Details zum Benutzerzertifikat (Aussteller, Seriennummer, Gültigkeit) sowie die für den Client geltenden Regeln für die Zertifikatsüberprüfung.

**Schlüssel** Diese Registerkarte zeigt Informationen zu allen für das geladene Profil verfügbaren Schlüsseln.

**Regeln** Diese Registerkarte zeigt die für den aktuellen Benutzer gültigen Verschlüsselungsregeln.

**Ausnahmen** Diese Registerkarte gibt Auskunft über unberücksichtigte Anwendungen, Laufwerke und Geräte. Außerdem werden die aktiven Ignorieren- und Bypass-Regeln des aktuellen Benutzers aufgelistet.

*u.trust LAN Crypt* behandelt standardmäßig bestimmte Anwendungen als „*Unberücksichtigte Anwendungen*". Auch diese Anwendungen werden in dieser Registerkarte angezeigt.

**Anwendungen** Diese Registerkarte zeigt Programme an, die von *u.trust LAN Crypt* aufgrund ihres Verhaltens eine besondere Behandlung verlangen.

**Antiviren-Software**

Antiviren-Software benötigt zum Scannen von verschlüsselten Dateien den Schlüssel, mit dem diese Dateien verschlüsselt sind. Hier vom Security Officer eingetragene Antiviren-Software hat Zugriff auf alle Schlüssel und kann dadurch auch verschlüsselte Dateien auf schadhaften Code untersuchen.

**Client API** Diese Registerkarte zeigt die Einstellungen der Client-API und listet alle Applikationen auf, welche die API verwenden dürfen.

**Trusted Vendors** Wenn der Client-API-Zugriff auf Applikationen vertrauenswürdiger Anbieter beschränkt ist, dann müssen diese in der *u.trust LAN Crypt*-Administration eingetragen sein. Alle eingetragenen vertrauenswürdigen Anbieter und ihre zugehörigen Zertifikate sind in dieser Registerkarte aufgeführt.

Schaltfläche **Exportieren**

Verwenden Sie die Schaltfläche **Exportieren**, um die aktuellen Client-Einstellungen in eine XML-Datei zu exportieren.

So können dem Support auf einfache Weise wichtige Konfigurationsinformationen zur Verfügung gestellt werden.

## Explorer-Erweiterungen

Die *u.trust LAN Crypt* Explorer-Erweiterungen bieten folgende Funktionen:

- Verschlüsseln von Dateien und Ordnern gemäß den definierten Regeln des geladenen Profils.
- Explizite Ver- und Entschlüsselung von Dateien und Ordnern.
- Einfache Kontrolle über den Verschlüsselungsstatus Ihrer Daten.

*u.trust LAN Crypt* fügt dem Windows Explorer Einträge hinzu. Diese werden in den Kontextmenüs bei Laufwerken, Ordnern und Dateien angezeigt. Zudem steht im Fenster Eigenschaften eine zusätzliche Registerkarte zur Verfügung. Diese enthält Informationen zum aktuellen Verschlüsselungsstatus.

Bei einem Rechtsklick auf einen Ordner oder eine Datei wird im Kontextmenü der Eintrag **u.trust LAN Crypt** angezeigt. Schlüssel in verschiedenen Farben zeigen den Verschlüsselungsstatus der ausgewählten Datei an:

**Grüner Schlüssel:** Die Datei ist verschlüsselt und der Benutzer hat Zugriff auf den Schlüssel.

**Roter Schlüssel:** Die Datei ist verschlüsselt, aber der Benutzer hat keinen Zugriff auf den Schlüssel.

**Grauer Schlüssel:** Die Datei ist unverschlüsselt, sollte aber entsprechend einer Verschlüsselungsregel im geladenen Profil verschlüsselt sein.

**Gelber Schlüssel:** Die Datei ist verschlüsselt, die transparente Verschlüsselung ist aber derzeit deaktiviert.

**Gelber Schlüssel mit Fragezeichen:** Der Benutzer verfügt nicht über die notwendigen Leserechte, sodass die Client-Anwendung von *u.trust LAN Crypt* den Verschlüsselungsstatus nicht feststellen kann.

**Hinweis**

- Für Dateien, die das Offline-Attribut gesetzt haben (z. B. für physikalisch nicht vorhandene Dateien), werden keine Schlüsselsymbole angezeigt.
- Auch den Dateien im Windows Explorer selbst werden Schlüsselsymbole hinzugefügt. Wenn eine Verschlüsselungsregel für ganze Laufwerke oder Ordner besteht, erhalten diese ebenfalls ein Schlüsselsymbol. Dieses zeigt dann, je nach Farbe, den jeweiligen Verschlüsselungsstatus an.

**Menüoptionen für Ordner**

**Verschlüsselungsstatus**

Diese Option zeigt eine Liste aller Dateien in diesem Ordner mit deren jeweiligen Verschlüsselungsstatus (farbige Schlüssel) an. Es werden immer nur die Dateien der ersten Ordnerebene angezeigt. Um Dateien in Unterordnern anzuzeigen, müssen Sie zuerst zu einem Unterordner wechseln. Im Explorer sind Ordner, für die eine Verschlüsselungsregel existiert, an einem Schlüsselsymbol zu erkennen.

**Gemäß Profil verschlüsseln**

Diese Option verschlüsselt alle Dateien im Ordner entsprechend dem geladenen Verschlüsselungsprofil. Auch Unterordner, für die eine Verschlüsselungsregel gilt, werden miteinbezogen. Eine Statusanzeige gibt an, wie lange etwa die Initialverschlüsselung dauern wird. Zudem wird angezeigt, wie viele Dateien der Ordner insgesamt enthält und wie viele davon bereits verschlüsselt wurden. Dabei wird auch der Pfad der Datei mit angezeigt, die gerade verschlüsselt wird.

**Verschlüsseln**

Diese Option verschlüsselt alle Dateien im Ordner mit einem Schlüssel aus dem geladenen Verschlüsselungsprofil. Es wird eine Liste der verfügbaren Schlüssel angezeigt, aus welcher der gewünschte Schlüssel ausgewählt werden kann.

**Hinweis**

- Besteht für Dateien in einem Ordner eine Verschlüsselungsregel und sind dort (noch) nicht alle Dateien regelkonform verschlüsselt, kann es nach Markieren des Ordners und nach Auswahl der Option *Verschlüsseln* zu einer Fehlermeldung bei der Verschlüsselung kommen.
- Führen Sie die Verschlüsselung von Ordnern, für die bereits eine Verschlüsselungsregel besteht, stattdessen über die Option *„Gemäß Profil verschlüsseln*" aus.

Alternativ können Sie die Verschlüsselung von Ordnern auch mithilfe des *u.trust LAN Crypt* Benutzermenüs eine Initialverschlüsselung durchführen.

**Entschlüsseln**

Diese Option entschlüsselt alle Dateien auf der ersten Ordnerebene. Dazu müssen die dazugehörigen Schlüssel im Verschlüsselungsprofil vorhanden sein. Fehlt ein Schlüssel, bleiben die hiervon betroffenen Dateien weiterhin verschlüsselt. Befinden sich Dateien jedoch auf einem Speicherort, für den eine aktive Verschlüsselungsregel besteht, können diese Dateien nicht durch den Benutzer entschlüsselt werden.

**Sicheres Verschieben**

Beim sicheren Verschieben eines Ordners über *u.trust LAN Crypt* werden die Dateien analog zu den geltenden Verschlüsselungsregeln am neuen Speicherort ver-, ent- oder umgeschlüsselt. Die ausgewählten Quelldateien werden nach dem erfolgreichen Verschieben gelöscht.

**Sicheres Löschen**

Beim sicheren Löschen wird der Speicherort der ausgewählten Dateien mehrmals überschrieben. Die Dateien können über den Papierkorb nicht wiederhergestellt werden.

### Menüoptionen für einzelne Dateien

#### Verschlüsselungsstatus

Diese Option zeigt den Verschlüsselungsstatus der Datei an. Bei verschlüsselten Dateien zeigt eine Popup-Infobox den zugehörigen Schlüssel an und gibt Auskunft, ob der Benutzer berechtigt ist, diesen Schlüssel zu verwenden.

Ist ein anderer Benutzer angemeldet, der hierzu nicht berechtigt ist, erscheint in der Infobox anstelle des Schlüsselnamens die GUID.

Verschlüsselte Dateien sind im Explorer an einem kleinen grünen Schlüsselsymbol zu erkennen. Über **Ordneroptionen > Ansicht/Erweiterte Einstellungen** können Benutzer für ihr Profil festlegen, ob der Verschlüsselungsstatus von Dateien und der Status von Verschlüsselungsregeln auf Ordnern angezeigt wird oder nicht. Änderungen an diesen Einstellungen werden erst wirksam, nachdem sich der Benutzer ab- und wieder angemeldet hat.

#### Gemäß Profil verschlüsseln

Diese Option verschlüsselt eine Datei entsprechend dem geladenen Verschlüsselungsprofil. Dieser Eintrag wird im Kontextmenü nur dann angezeigt, wenn der Verschlüsselungsstatus einer Datei nicht mit dem Verschlüsselungsprofil übereinstimmt.

#### Verschlüsseln

Diese Option verschlüsselt die ausgewählte Datei. Es wird eine Liste der verfügbaren Schlüssel angezeigt, aus welcher der entsprechende Schlüssel ausgewählt werden kann.

**Hinweis**

- Besteht für Dateien in einem Laufwerk oder Ordner eine Verschlüsselungsregel und sind dort (noch) nicht alle Dateien verschlüsselt, kann es nach dem Markieren von mehreren Dateien und Auswahl der Option *Verschlüsseln* zu einer Fehlermeldung bei der Verschlüsselung kommen. Beispiel: Sie markieren mehrere Dateien, von denen für mindestens eine dieser Dateien bereits eine Verschlüsselungsregel mit „Schlüssel-1" besteht, wählen dann aber über die Option *Verschlüsseln* den „Schlüssel-2" aus und klicken danach auf **Ok**.

**Beispiel:** Führen Sie die Verschlüsselung von Dateien, für die bereits eine Verschlüsselungsregel besteht, stattdessen über die Option *„Gemäß Profil verschlüsseln*" aus.

**Hinweis**

- Führen Sie die Verschlüsselung von Dateien, für die bereits eine Verschlüsselungsregel besteht, stattdessen über die Option *„Gemäß Profil verschlüsseln*" aus.

Alternativ können Sie die Verschlüsselung dieser Dateien auch mithilfe des *u.trust LAN Crypt* Benutzermenüs eine Initialverschlüsselung durchführen.

#### Entschlüsseln

Diese Option entschlüsselt die ausgewählte Datei. Der erforderliche Schlüssel muss im aktiven Verschlüsselungsprofil vorhanden sein, andernfalls bleibt die Datei verschlüsselt.

#### Sicheres Verschieben

Mit dieser Option werden Dateien beim Verschieben an einen anderen Speicherort entsprechend der geltenden Verschlüsselungsregeln ver-, ent- oder umgeschlüsselt. Die ausgewählten Quelldateien werden nach dem Verschieben gelöscht.

#### Sicheres Löschen

Beim sicheren Löschen wird der Speicherort der ausgewählten Dateien mehrmals überschrieben. Die Dateien können über den Papierkorb nicht wiederhergestellt werden.

**Hinweis**

- Aktive Verschlüsselungsregeln haben stets die höchste Priorität. Versucht ein Benutzer, Dateien zu ent-/verschlüsseln, für die eine Verschlüsselungsregel etwas

anderes definiert, wird der Befehl nicht ausgeführt und es wird eine Fehlermeldung angezeigt.

**In folgenden Situationen kommt es beim Versuch, Dateien über das Kontextmenü zu verschlüsseln, zu einer Fehlermeldung:**

- Der Ordner enthält Dateien, die mit einem unbekannten Schlüssel verschlüsselt sind.
- Der Benutzer versucht, eine Datei im Widerspruch zu ihrer Verschlüsselungsregel zu ver- / entschlüsseln (z. B. wenn ein anderer Schlüssel gewählt wird als in der Regel definiert).

**Verschlüsselungsinformation**

Die Registerkarte **Verschlüsselungsstatus** im Fenster **Eigenschaften** zeigt Informationen zur verschlüsselten Datei an.

---

# Terminal Server

Diese Version von *u.trust LAN Crypt* unterstützt Windows Terminal Server und Citrix Terminal Server. Nähere Informationen zu den unterstützten Versionen finden Sie in den *u.trust LAN Crypt* Versionsinfos.

## Firewall

Nachdem sich ein Benutzer angemeldet hat, versucht *u.trust LAN Crypt* das Benutzerprofil zu laden. Dabei werden die Zertifikate von Benutzer und (Master) Security Officer überprüft. Enthält ein Zertifikat einen „CRL Distribution Point" und es ist keine gültige CRL auf dem System verfügbar, versucht Windows, eine CRL von der angegebenen Adresse zu importieren. Ist eine Firewall aktiv, wird unter Umständen eine Meldung angezeigt, dass ein Programm (*loadprof.exe*) versucht, eine Verbindung zum Internet herzustellen.

## Installation in einer Terminal-Server-Umgebung

Die Installation des LAN Crypt Clients auf einem Terminalserver erfolgt grundsätzlich wie auf regulären Windows-Systemen. Wird LAN Crypt jedoch in einer RemoteApp-Umgebung (Applikationsvirtualisierung) betrieben, sind zusätzliche Schritte erforderlich, um sicherzustellen, dass **LoadProf** nicht global für die gesamte Sitzung, sondern ausschließlich im Kontext der RemoteApp ausgeführt wird.

### Installation in einer RemoteApp-Umgebung (Applikationsvirtualisierung)

#### Vorbereitung vor dem Setup

Vor dem Start des Installationspakets muss der vorhandene Eintrag zu *loadprof.exe* entfernt werden. Öffnen Sie dazu den Registrierungs-Editor und löschen Sie den Eintrag im folgenden Schlüssel:

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

Wenn in diesem Wert *loadprof.exe* aufgeführt ist, entfernen Sie den Eintrag vollständig aus der Liste.

#### Installation mit Transform-Datei (.mst)

Für das Ausführen des Installationspakets muss eine Transform-Datei (.mst) erstellt und eingebunden werden.

**Hinweis**

- Bitte beachten Sie, dass die .mst-Datei selbst erstellt werden muss.

In dieser Transform-Datei ist die private Property **TerminalServer** auf den Wert **1** zu setzen, damit das Setup korrekt im Terminalserver-Modus installiert wird.

#### Beispiel für den Installationsaufruf mit Transform-Datei:

```
msiexec /i LCClient.msi /qn [weitere Parameter] TRANSFORMS="C:\Transform_Datei.mst"
```

Durch diese Konfiguration wird das korrekte Startverhalten in RemoteApp-Szenarien gewährleistet.

**Hinweis**

- Verwenden Sie eine lokale Anmelde-Session mit Administrationsrechten, wenn Sie *u.trust LAN Crypt* auf einem Terminal-Server installieren.
- Wenn Sie den „*Citrix Presentation Server*" oder „*Citrix XenApp*" verwenden möchten, installieren Sie diese(n), bevor Sie *u.trust LAN Crypt* installieren.

## Einschränkungen

#### Citrix

- Verschlüsselung in Verbindung mit Citrix Client Drive Redirection-Laufwerken wird nicht unterstützt.
- Citrix Streamed Applications werden nicht unterstützt.

# Installation und Upgrade

**Hinweis**

- Wenn Sie beide *u.trust LAN Crypt* Komponenten, *Admin-Konsole* und *Clientanwendung* auf demselben Computer installieren, müssen diese unbedingt von der gleichen Version sein.

**Schritt 1:** Doppelklicken Sie auf die Datei „**LCClient.msi**" im *u.trust LAN Crypt* Installations-Verzeichnis für die Client-Software Ihres extrahierten Installationspakets.

**Schritt 2:** Klicken Sie auf **Weiter**.

Der Dialog **Lizenzvertrag** wird angezeigt.

**Schritt 3:** Wählen Sie die Option **Ich akzeptiere den Lizenzvertrag** im Dialog **Lizenzvertrag**. Andernfalls ist eine Installation von *u.trust LAN Crypt* nicht möglich.

**Schritt 4:** Klicken Sie auf **Weiter**.

Der Dialog **Zielordner** wird angezeigt.

**Schritt 5:** Wählen Sie aus, an welchem Ort *u.trust LAN Crypt* installiert werden soll.

**Schritt 6:** Klicken Sie auf **Weiter**.

Der Dialog **Installationsart auswählen** wird angezeigt.

**Schritt 7:** In diesem Dialog können Sie auswählen, welche Komponenten von *u.trust LAN Crypt* installiert werden sollen.

- *Standard*: Installiert die gebräuchlichsten Funktionen des *u.trust LAN Crypt* Clients.
- *Vollständig*: Komplette Client-Installation, inkl. der Client-API.
- *Benutzerdefiniert*: Die Komponenten sind jeweils auswählbar.

**Schritt 8:** Wählen Sie **Benutzerdefiniert** und klicken Sie auf **Weiter**.

Folgende Komponenten können installiert werden:

**u.trust LAN Crypt Client Installation**

Installiert das *u.trust LAN Crypt* Benutzerprogramm.

**Explorer-Erweiterungen**

Installiert die *u.trust LAN Crypt* Explorer-Erweiterungen.

*u.trust LAN Crypt* fügt dem Windows Explorer Einträge hinzu, die die Initialverschlüsselung von Dateien und Ordnern, die explizite Ver- und Entschlüsselung von Dateien und Ordnern und die einfache Kontrolle über den Verschlüsselungsstatus Ihrer Dateien erlauben. Die Einträge erscheinen in den Kontextmenüs von Laufwerken, Ordnern und Dateien. Darüber hinaus wird auch dem Windows-Eigenschaften-Fenster für Dateien eine zusätzliche Seite mit den Verschlüsselungsinformationen hinzugefügt.

**Client-API**

Wird verwendet, wenn Applikationen über diese API auf die *u.trust LAN Crypt* Dateiverschlüsselungsfunktion zugreifen sollen.

**Hinweis**

- Sie müssen die Client-API installieren, wenn Sie z. B. DLP-Produkten den Datenzugriff über die *u.trust LAN Crypt* Client-API ermöglichen wollen.

**Netzwerk-Filter**

Installiert einen Treiber, der die Performance bei Netzwerkzugriffen verbessern hilft.

**Schritt 9:** Wählen Sie aus, welche Komponenten installiert werden sollen, und klicken Sie auf **Weiter**.

**Hinweis**

- Bitte beachten Sie, dass *u.trust LAN Crypt* seit Version 4.1.0 keinen Legacy-Filtertreiber mehr unterstützt. Sämtliche Ver- und Entschlüsselungsvorgänge erfolgen ausschließlich über die neue aktuellere und zukunftssichere Minifiltertreiber-Technologie.

**Schritt 10:** Überprüfen Sie Ihre Eingaben noch einmal und klicken Sie auf **Weiter**, um den Installationsprozess auszuführen.

**Schritt 11:** Ist die Installation erfolgreich, so erscheint ein Dialog, in dem Sie auf **Beenden** klicken können, um den Installationsprozess abzuschließen.

**Hinweis**

- Um alle Einstellungen zu übernehmen, müssen Sie den Computer neu starten.

## Installation ohne Benutzerinteraktion

Die Installation ohne Benutzerinteraktion erlaubt die automatische Installation von *u.trust LAN Crypt* auf einer großen Anzahl von Rechnern.

Das Installationsverzeichnis auf Ihrer Installations-CD enthält die „.msi-Datei" zur Installation der Client-Komponenten.

## Installierbare Komponenten

In den folgenden Abschnitten werden alle weiteren Komponenten beschrieben, die Sie installieren können, und die Art und Weise, wie sie bei der Installation ohne Benutzerinteraktion angegeben werden müssen.

Die Schlüsselwörter (**Courier, fett**) geben an, wie die einzelnen Komponenten unter "AddLocal=" angegeben werden müssen, wenn eine Installation ohne Benutzerinteraktion ausgeführt wird (siehe Optionale Parameter). Bei den Bezeichnungen der einzelnen Komponenten wird zwischen Groß- / Kleinschreibung unterschieden!

## Kommandozeilen-Syntax

Zum Ausführen einer Installation ohne Benutzerinteraktion müssen Sie **msiexec** mit bestimmten Parametern aufrufen.

**Erforderliche Parameter:**

**/I**

Gibt das Installationspaket an, das zu installieren ist.

**/QN**

Installation erfolgt ohne Benutzerinteraktion.

Name der .msi-Datei: **LCClient.msi** Syntax:

**Syntax:**

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

**Optionale Parameter**

```
/Lvx\* \<path + filename\>
```

Protokolliert den gesamten Installationsvorgang in dem unter `<Pfad + Dateiname>` angegebenen Speicherort.

**AddLocal=**

```
AddLocal= ALL
```

Installiert alle verfügbaren Komponenten.

```
AddLocal= LanCrypt
```

Installiert keine der verfügbaren Komponenten.

```
AddLocal= UserApplication
```

Installiert das *u.trust LAN Crypt* Benutzerprogramm.

```
AddLocal= NetworkFilter
```

Installiert einen Treiber, der die Performance bei Netzwerkzugriffen verbessern hilft.

```
AddLocal= ClientAPI
```

Installiert die *u.trust LAN Crypt* Client-API.

```
AddLocal= ShellExtensions
```

Installiert die *u.trust LAN Crypt* Explorer-Erweiterungen (vgl. Explorer-Erweiterungen).

*u.trust LAN Crypt* fügt dem Windows Explorer Einträge hinzu, die die Erstverschlüsselung von Dateien und Ordnern, die explizite Ver-/Entschlüsselung von Dateien und Ordnern und die einfache Überprüfung des Verschlüsselungsstatus Ihrer Daten ermöglichen. Diese Einträge werden in den Kontextmenüs von Laufwerken, Ordnern und Dateien angezeigt. Darüber hinaus wird der Seite *Windows Eigenschaften* eine Registerkarte **Verschlüsselungsinformationen** hinzugefügt.

**NOOVERLAY=**

**(Greift nur bei Neuinstallationen und nicht bei Versionsupgrades)**

```
NOOVERLAY=0
```

Aktiviert Overlay-Symbole für Dateien und Ordner.

```
NOOVERLAY=1
```

Deaktiviert Overlay-Symbole für Dateien und Ordner.

Über **Erweiterte Einstellungen** können Benutzer für ihr Profil festlegen, ob der Verschlüsselungsstatus von Dateien und der Status von Verschlüsselungsregeln auf Ordnern angezeigt werden soll oder nicht. Änderungen an diesen Einstellungen werden erst wirksam, nachdem sich der Benutzer ab- und wieder angemeldet hat.

**Hinweis**

- Nach der Installation können Benutzer Overlay-Symbole über **Ordneroptionen > Ansicht** aktivieren. Änderungen werden erst nach Ab- und erneuter Anmeldung wirksam.

**Productlanguage=**

Installiert das MSI-Sprachpaket für den *u.trust LAN Crypt* Client in einer bestimmten Sprache, unabhängig von der vorhandenen Spracheinstellung des Computers. Diese eingestellte Sprache wird dann für die Installation selbst und auch bei späteren Änderungen durch den Setup-Assistenten von *u.trust LAN Crypt* verwendet. Folgende Spracheinstellungen werden derzeit über den Installationsparameter „Productlanguage=“ unterstützt:

```
Productlanguage=1031
```

Installiert für den *u.trust LAN Crypt* Client das deutsche MSI-Sprachpaket.

```
Productlanguage=1033
```

Installiert für den *u.trust LAN Crypt* Client das englische MSI-Sprachpaket.

```
Productlanguage=1036
```

Installiert für den *u.trust LAN Crypt* Client das französische MSI-Sprachpaket.

**RESET_CONFIGURATION=**

`RESET_CONFIGURATION=1`

Setzt alle bestehenden LAN Crypt Client-Konfigurationen in der Windows-Registry zurück. Alle vorherigen Einstellungen gehen unwiderruflich verloren. Alle Standard-Registry-Einträge werden während der Installation erstellt.

**ONEDRIVE=**

`ONEDRIVE=1`

Aktiviert für den jeweiligen User, für welchen das Setup vorgesehen ist, die Unterstützung von Microsoft OneDrive.

**Beispiel:**

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

Die Installation von *u.trust LAN Crypt* wird ausgeführt. Die Clientanwendung wird im Standardverzeichnis (`<Systemlaufwerk>:\Programme\Utimaco\u.trust LAN Crypt`) installiert.

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

Die Installation von *u.trust LAN Crypt* wird ausgeführt. Das Programm wird im Standardverzeichnis (`<Systemlaufwerk>:\Programme\Utimaco\u.trust LAN Crypt`) mit dem Benutzerprogramm, den Explorer-Erweiterungen und englischsprachigem MSI-Sprachpaket, aber ohne die Client-API installiert.

Die Installationsdatei (*LCClient.msi*) befindet sich im Installationsordner von *u.trust LAN Crypt*.

**Hinweis**

- Bitte beachten Sie, dass das Installationsprogramm abgebrochen wird, wenn die Zeile nach dem Parameter „AddLocal=" leer bleibt oder dort ein Parameter fehlerhaft eingetragen ist.

## u.trust LAN Crypt Client entfernen

Sie können den *u.trust LAN Crypt* Client nur entfernen, wenn Sie mit Administratorrechten am Betriebssystem angemeldet sind.

Wählen Sie **Start** > **Einstellungen** > **Apps**. Doppelklicken Sie in der Liste der Apps auf **u.trust LAN Crypt Client** und klicken Sie dort auf die Schaltfläche **Deinstallieren**. Klicken Sie im dann folgenden Dialog abermals auf die Schaltfläche **Deinstallieren**. Der *u.trust LAN Crypt* Client wird deinstalliert. Starten Sie danach Ihren Computer neu.

**Hinweis**

- Auf manchen Client-Rechnern kann es ggf. vorkommen, dass die erforderlichen *Visual C++ Runtime-Bibliotheken* nicht (mehr) installiert sind. Wegen dieser fehlenden Komponente lässt sich *u.trust LAN Crypt* auf diesen Rechnern dann nicht deinstallieren. Eine Fehlermeldung während der Deinstallation zeigt dann an, dass ein Problem mit dem Windows-Installer-Paket vorliegen würde. In dem Fall müssen Sie die erforderlichen *Visual C++ Runtime-Bibliotheken* auf dem betroffenen Client-Rechner nachinstallieren. Sie finden diese jeweils unter den folgenden URLs:

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

Nachdem Sie die erforderlichen *Visual C++ Runtime-Bibliotheken* erfolgreich auf dem Client-Rechner installiert haben, sollte eine Deinstallation von *u.trust LAN Crypt* wieder fehlerfrei möglich sein.

**Hinweis**

- Nach der Deinstallation von *u.trust LAN Crypt* können auf dem Computer keine verschlüsselten Dateien mehr entschlüsselt werden. Die Deinstallation von *u.trust LAN Crypt* führt nicht zu einer Entschlüsselung von Dateien.

**Hinweis**

- Installieren Sie den *u.trust LAN Crypt* Client nach einer Deinstallation nicht unmittelbar neu. Sie müssen den Computer mindestens einmal neu starten, bevor Sie *u.trust LAN Crypt* erneut installieren.

# Deinstallation ohne Benutzerinteraktion

**Voraussetzung:** Das MSI-Paket, das deinstalliert werden soll, muss im System vorhanden sein.

Beispiel:

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

Dieser Befehl deinstalliert das MSI-Paket mit dem ProductCode {00000000-0000-0000-0000-000000000000} im unbeaufsichtigten Modus und unterdrückt einen Neustart des Systems.

**Befehlszeilenoptionen:**

**/X {ProductCode}**

Der ProductCode des MSI-Pakets, das deinstalliert werden soll. Der ProductCode kann aus der MSI-Datei selbst extrahiert werden.

**/qn**

Führt die Deinstallation im unbeaufsichtigten Modus aus, ohne dass dem Benutzer eine Benutzeroberfläche angezeigt wird.

**/norestart**

Unterdrückt einen Neustart des Systems nach der Deinstallation.

# Benutzerdefinierte Fehlermeldungen im LAN Crypt Client

Der LAN Crypt Client bietet die Möglichkeit, individuelle Nachrichten für bestimmte Fehlermeldungen zu hinterlegen. Auf diese Weise können Sie die Standardmeldungen durch eigene Hinweise ergänzen, beispielsweise mit einem Verweis auf den IT-Support.

**Hinweis**

- Aktuell wird das Hinzufügen eigener Informationen ausschließlich für Fehlermeldungen im Zusammenhang mit dem **Laden von Profilen (LoadProf)** unterstützt.

## Einrichtung

Die benutzerdefinierten Texte werden im folgenden Registrypfad hinterlegt: 'HKEY*LOCAL*MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt\Customer Messages\Client'

Für jede Fehlermeldung, die ergänzt werden soll, muss ein eigenes Unterverzeichnis im Format erstellt werden: 'Client-MsgId-'

Der `<Fehlercode>` entspricht dabei dem Fehlercode der betreffenden Fehlermeldung. Für den Fehlercode **1056** lautet der Pfad beispielsweise: 'HKEY*LOCAL*MACHINE\SOFTWARE\Policies\Utimaco\SGLANCrypt\Customer Messages\Client\Client-MsgId-1056'

**Hinweis**

- Der Fehlercode kann über das verlinkte Dokument (Änderungen vorbehalten) oder durch gezielte Reproduktion des Fehlers ermittelt werden.

Innerhalb dieser Registry können die Nachrichten in verschiedenen Sprachen hinterlegt werden. Dazu wird der Sprach- und Ländercode als Name des Eintrags verwendet (`de-DE`, `de-AT`, `en-US`, ...).

Der jeweilige Wert enthält die anzuhängende Nachricht. Dabei ist zu beachten, dass die Nachricht nicht mehr als **maximal 1000 Zeichen** umfassen darf. Wird diese Länge überschritten, erscheint die Nachricht nicht in der Fehlermeldung.

# Integrieren von Dokumentation in einer Umgebung ohne Internetzugang

Wenn LAN Crypt in einer Umgebung ohne Zugang zum öffentlichen Internet verwendet wird, funktionieren die im Client integrierten Links zur Online-Hilfe nicht. Um dennoch einen direkten Link zu lokaler oder interner Dokumentation bereitzustellen, kann der folgende Registryschlüssel gesetzt werden:

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

Diese Einstellung ermöglicht es, eine alternative Hilfedatei anzugeben, wie z. B. die lokale PDF-Dokumentation. Der Registry-Wert muss einen absoluten URL-Pfad enthalten, der vom Client-System erreichbar ist (z. B. „https://intranet.local/docs/lancrypt_help.pdf").

# Kompatibilität mit Cloud-Diensten

LAN Crypt unterstützt die Verschlüsselung von Dateien auch auf cloudbasierten Speichermedien und bietet damit einen zusätzlichen Schutz vor unbefugtem Zugriff - selbst durch die Betreiber der jeweiligen Cloud-Dienste. Cloud-Anbieter wie Microsoft, Google oder ähnliche Plattformen stellen üblicherweise zusätzliche Funktionen bereit, beispielsweise die kollaborative Bearbeitung von Dokumenten oder die inhaltsbasierte Suche von Dateien. Da Cloud-Dienste keinen Zugriff auf den Inhalt verschlüsselter Dateien erhalten, stehen diese Funktionen für von LAN Crypt geschützte Dateien nicht zur Verfügung. Die verschlüsselten Daten unterliegen einem besonders hohen Schutz und können daher von den Diensten nicht verarbeitet werden.

## Nicht kompatible Microsoft-365-Dienste

Folgende Microsof-365-Funktionen setzen eine inhaltliche Analyse der Dateien voraus und sind daher nicht nutzbar, wenn die Dateien durch LAN Crypt verschlüsselt sind:

- Nachrichtenflussregeln, einschließlich Anti-Schadsoftware- und Spam-Prüfungen, die Zugriff auf Anlagen benötigen
- Microsoft Delve
- eDiscovery
- Inhaltssuche und -indizierung
- Office Web Apps, einschließlich Funktionen zur gemeinsamen Dokumentbearbeitung

### * Copilot

# Sicherheitslücken melden

Utimaco ist sich bewusst, dass hohe Sicherheit durch Zusammenarbeit entsteht. Wir verpflichten uns, verantwortungsbewusst und konstruktiv mit Kunden, Sicherheitsexperten, Sicherheitsforschern und der breiteren Gemeinschaft zusammenzuarbeiten, um Sicherheitslücken zu identifizieren und zu beheben.

Wir begrüßen und fördern die verantwortungsvolle Meldung von Sicherheitslücken. Jede eingehende Meldung wird mit Sorgfalt und Dringlichkeit behandelt. Wir streben an, den Eingang von Meldungen zeitnah zu bestätigen, während des gesamten Untersuchungsprozesses verantwortungsbewusst zu kommunizieren und relevante Aktualisierungen (Sicherheitshinweise und Patches) bereitzustellen, sobald diese verfügbar sind.

Wenn Sie eine Sicherheitslücke entdecken, bitten wir Sie, diese unverzüglich und auf sicherem Weg dem Utimaco PSIRT (Product Security Incident Response Team) zu melden, das Ihre Meldung mit Dringlichkeit bearbeiten wird.

Jede Meldung einer Sicherheitslücke muss mittels PGP-Verschlüsselung verschlüsselt übermittelt werden, um eine versehentliche Offenlegung kritischer Informationen zu verhindern.

## (Schritt 1) Bereiten Sie Ihre Meldung vor

Geben Sie möglichst viele Details an, damit wir das Problem verstehen und reproduzieren können:

```
Kurze Zusammenfassung der Sicherheitslücke Beschreibung der Sicherheitslücke Betroffene Produkte, Versionen und Konfiguration Beschreibung der Produktumgebung Verwendetes Betriebssystem. Schrittweise Anleitung zur Reproduktion Mögliche Grundursache. Proof-of-Concept-Code, Screenshots oder Protokolle (falls verfügbar) Mögliche Auswirkungen und vorgeschlagene Abhilfemaßnahmen (optional) Ihre Kontaktinformationen für Rückfragen und Ihr öffentlicher PGP-Verschlüsselungsschlüssel.
```

Alle Meldungen werden streng vertraulich behandelt, und es werden keine personenbezogenen Daten an Dritte weitergegeben

## (Schritt 2) Verschlüsseln Sie Ihre E-Mail mit PGP

Zum Schutz sensibler Informationen müssen Sie Ihre Meldung vor dem Versand mit unserem öffentlichen PGP-Schlüssel des PSIRT verschlüsseln.

1. Importieren Sie unseren öffentlichen PSIRT-Schlüssel (unten bereitgestellt) in Ihr PGP/GPG-Tool.
2. Verschlüsseln Sie die Meldung der Sicherheitslücke mit diesem Schlüssel
3. Senden Sie eine E-Mail mit verschlüsseltem Anhang an PSIRT@utimaco.com.
4. Optional können Sie Ihre Nachricht mit Ihrem eigenen PGP-Schlüssel signieren, damit wir die Authentizität überprüfen können.

## PSIRT-Kontakt

**PSIRT-Team:** PSIRT@Utimaco.com

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

**PGP-Schlüssel:** Herunterladen

---

# Technischen Support

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

Copyright © 2024 - 2026 Utimaco IS GmbH, 2018 - 2024 conpal GmbH, 1996 - 2018 Sophos Limited und Sophos Group. Alle Rechte vorbehalten. conpal®, AccessOn® und AuthomaticOn® sind eingetragene Warenzeichen von conpal GmbH.

Alle anderen erwähnten Produkt- und Unternehmensnamen sind Marken oder eingetragene Marken der jeweiligen Inhaber.

Diese Publikation darf weder elektronisch oder mechanisch reproduziert, elektronisch gespeichert oder übertragen, noch fotokopiert oder aufgenommen werden, es sei denn, Sie verfügen entweder über eine gültige Lizenz, gemäß der die Dokumentation in Übereinstimmung mit dem Lizenzvertrag reproduziert werden darf, oder Sie verfügen über eine schriftliche Genehmigung des Urheberrechtsinhabers.

Copyright-Informationen von Drittanbietern finden Sie in dem 3rd Party Software Dokument in Ihrem Produktverzeichnis.

---

**Zuletzt aktualisiert am 21.09.2026**