

u.trust LAN Crypt Cloud

**DE**

**utimaco**<sup>®</sup>

## Imprint

Copyright 2023	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany AMERICAS +1-844-UTIMACO (+1 844-884-6226)
Phone	EMEA +49 800-627-3081 APAC +81 800-919-1301 <a href="https://support.hsm.utimaco.com/">https://support.hsm.utimaco.com/</a>
Internet e-mail	<a href="mailto:support@utimaco.com">support@utimaco.com</a>

All rights reserved

No part of this documentation may be reproduced in any form (printing, photocopy or according to any other process) without the written approval of Utimaco IS GmbH or be processed, reproduced or distributed using electronic systems.

Utimaco IS GmbH reserves the right to modify or amend the documentation at any time without prior notice. Utimaco IS GmbH assumes no liability for typographical errors and damages incurred due to them. Any mention of the company name Utimaco in this documents refers to the Utimaco IS GmbH.

All trademarks and registered trademarks are the property of their respective owners.

## Was ist u.trust LAN Crypt Cloud?

u.trust LAN Crypt Cloud ist eine leistungsstarke cloudbasierte Anwendung, die speziell zur Administration von u.trust LAN Crypt Instanzen innerhalb einer Organisation entwickelt wurde. Sie ist eine flexible und effiziente Lösung, die Administratoren eine Vielzahl von Funktionen zur Verwaltung von u.trust LAN Crypt Instanzen bietet.

Diese Anwendung kann entweder als Ergänzung zur bereits vorhandenen On-Premises-Administration von u.trust LAN Crypt Instanzen verwendet werden oder als vollwertige Alternative dazu. Das bedeutet, dass Unternehmen die Möglichkeit haben, die Administration von u.trust LAN Crypt entweder vollständig in die Cloud zu verlagern oder eine hybride Lösung zu nutzen, die sowohl die On-Premises- als auch die Cloud-Administration miteinander kombiniert.

### Funktionalität von u.trust LAN Crypt

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 Officer 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 berechnigte 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.

---

## u.trust LAN Crypt Cloud: Schnelleinstieg

Nach erfolgreicher [Registrierung](#) gliedert sich der Einstieg in den Arbeitsablauf des u.trust LAN Crypt Cloud in **drei einfache Schritte**:

### Schritt 1: Definieren von Assets

Assets sind Speicheradressen, die wichtige Daten für eine Organisation enthalten. Mit u.trust LAN Crypt Cloud können Zugriffsrechte für Assets gesteuert und auf Einzelpersonen oder Gruppen innerhalb der Organisation beschränkt werden. Bevor dies jedoch möglich ist, müssen die Speicheradressen innerhalb von u.trust LAN Crypt Cloud als solche definiert werden.

Siehe [Verwalten von Assets](#) für detaillierte Anweisungen zum definieren von Assets.

### Schritt 2: Definieren von Identitäten

Identitäten in u.trust LAN Crypt Cloud repräsentieren einzelne Nutzer, Gruppen und Untergruppen Ihrer Organisation und ermöglichen somit eine übersichtliche Modellierung Ihrer Unternehmensstruktur und eine einfache Zuordnung von Nutzern zu Gruppen und Untergruppen. Um dies zu erreichen, müssen zunächst Nutzer erstellt und anschließend die entsprechenden Personen Ihrer Organisation dazu eingeladen werden, ein u.trust LAN Crypt Cloud Konto zu erstellen, um sich zu identifizieren. Alternativ zur manuellen Abbildung Ihrer Unternehmensstruktur können Sie bestehende Strukturen von einer Microsoft Entra ID importieren.

Siehe [Verwalten von Identitäten](#) für detaillierte Anweisungen zum definieren von Identitäten und [Microsoft Entra ID Synchronisation](#) für den Import von bestehenden Strukturen aus einer Microsoft Entra ID.

### Schritt 3: Verteilung von Zugriffsberechtigungen

Sobald Assets und Identitäten erstellt wurden, können Zugriffsberechtigungen an Nutzer, Gruppen und Untergruppen vergeben werden. Diese Berechtigungen in den Reitern **Assets** und **Identitäten** verwaltet werden.

Siehe [Verwaltung der Zugriffsberechtigungen von Gruppen, Nutzern und Assets](#) für detaillierte Anweisungen zum Verteilen von Zugriffsberechtigungen.

---

# u.trust LAN Crypt Cloud Kontoverwaltung

## Registrierung und Login als Administrator

Die Nutzung von u.trust LAN Crypt Cloud setzt die [Registrierung eines u.trust LAN Crypt Cloud Kontos](#) voraus. Sobald Sie den Registrierungsvorgang erfolgreich abgeschlossen haben, wird eine E-Mail zur Aktivierung Ihres Kontos an die angegebene Adresse gesendet. Um das registrierte Konto zu aktivieren, muss der Aktivierungslink in der E-Mail innerhalb der nächsten 24 Stunden aufgerufen werden. Falls das registrierte Konto innerhalb dieses Zeitraums nicht aktiviert wird, erfolgt automatisch die Löschung des Kontos. Nach der Aktivierung des Kontos dienen die angegebene E-Mail-Adresse und das gewählte Passwort als Login-Daten.

Alternativ besteht die Möglichkeit, sich über die Verwendung eines Microsoft-Kontos zu registrieren und anzumelden.

### Hinweis

- Bitte beachten Sie, dass zu viele aufeinander folgende Fehlversuche des Logins zu einer Wartezeit zwischen weiteren Versuchen führt. Diese Wartezeit beträgt höchstens 15 Minuten und dient als Schutz gegen Brute-Force-Angriffe auf Ihren Konto.
- Es gibt keine permanente Sperre, die vom System erzwungen wird. Ein gesperrtes Konto kann jedoch nicht verwendet werden, bis die Dauer der Sperre abläuft oder das Kontopasswort zurückgesetzt wurde.
- Besteht bei der Nutzung von u.trust LAN Crypt Cloud eine längere Inaktivität des Nutzers, so ist aus Sicherheitsgründen ein erneuter Login erforderlich.

## Registrierung und Login der Nutzer einer Organisation

Die Registrierung eines Nutzers einer Organisation kann nur von dem Administrator initiiert werden, jedoch werden beide Parteien zum Abschluss des Registrierungsvorgangs benötigt. Beim Hinzufügen eines Mitglieds der Organisation unter dem Reiter **Identitäten**, wird dem Nutzer eine eindeutige E-Mail-Adresse und eine Anmeldemethode zugeordnet.

Der Nutzer erhält im Anschluss eine E-Mail zur Bestätigung seines Nutzer-Kontos. Nach der erfolgreichen Bestätigung durch das Setzen eines Konto-Passworts ist die Registrierung des Nutzers abgeschlossen. Bei der Anmeldemethode mittels Microsoft Entra ID ist es nicht erforderlich, ein zusätzliches Passwort zu erstellen. Nach Bestätigung des Nutzerkontos über den Link in der Bestätigungsmail kann der Nutzer sein Microsoft-Konto für künftige Anmeldevorgänge nutzen.

Der Nutzer kann sich nun auf dem [LAN Crypt Userportal](#) anmelden. Dort hat er Zugriff auf die verschiedenen LAN Crypt Clients sowie die Möglichkeit, sein Passwort zu verwalten.

### Hinweis

- Wenn die Anmeldemethode Microsoft Entra ID ausgewählt wird, ist es wichtig sicherzustellen, dass die angegebene E-Mail-Adresse mit der E-Mail-Adresse des Microsoft-Kontos des zu registrierenden Nutzers übereinstimmt.

## Voraussetzungen für die Erstellung eines sicheren Passworts

**Ein vom Benutzer gewähltes Passwort muss mehrere Anforderungen erfüllen, um die Sicherheit des Kontos zu gewährleisten:**

**Länge:** Das Passwort muss mindestens 8 Zeichen lang sein.

**Großbuchstaben:** Das Passwort muss mindestens einen Großbuchstaben enthalten.

**Kleinbuchstaben:** Das Passwort muss mindestens einen Kleinbuchstaben enthalten.

**Ziffern:** Das Passwort muss mindestens eine Ziffer (0-9) enthalten.

**Sonderzeichen:** Das Passwort muss mindestens ein Sonderzeichen enthalten, wie zum Beispiel !, @, #, \$, %.

**History:** Die Passwort-Historie erfordert, dass das neue Passwort sich von den letzten drei verwendeten Passwörtern unterscheidet. Dies soll verhindern, dass Benutzer zu ähnliche oder bereits verwendete Passwörter erneut verwenden.

**Vermeidung von Nutzer-Namen und E-Mail-Adresse:** Das Passwort darf weder den Nutzer-Namen noch die E-Mail-Adresse enthalten.

Es ist notwendig, diese Anforderungen bei der Erstellung eines Passworts zu beachten, um die Sicherheit des Kontos zu erhöhen und potenzielle Angriffspunkte zu minimieren.

## Verwaltung der Kontodaten

Zur Verwaltung Ihrer Kontodaten klicken Sie oben rechts auf Ihr **Kontosymbol** und wählen Sie **Konto verwalten** aus. Ihnen stehen die folgenden Optionen zur Verfügung:

**Persönliche Informationen:** Überprüfen und Bearbeiten persönlicher Informationen. Hier können Sie auch Ihre bevorzugte Sprache und das regionale Format einstellen.

**Kontakt:** Kontaktieren Sie uns direkt mithilfe unseres Formulars.

**Abonnements:** Erhalten Sie detaillierte Informationen zu Ihren Abonnement.

**Anwendungen:** Hier finden Sie eine Übersicht mit Verlinkungen zu den verschiedenen LAN Crypt Clients.

**Datenexport:** Starten Sie den Exportprozess für Verschlüsselungsschlüssel. Diese Schlüssel sind erforderlich, um auch nach der Deaktivierung des Cloud-Kontos weiterhin auf verschlüsselte Vermögenswerte zugreifen zu können.

**Dashboard:** Hier gelangen Sie zurück zur Übersicht des Dashboards.

---

# Administrieren mit u.trust LAN Crypt Cloud

## Nutzung des Dashboards

Das Dashboard bietet eine schnelle Übersicht über die wichtigsten Informationen, die Sie benötigen, um die Leistung Ihrer Cloud-Plattform zu überwachen. Hier können Sie schnell und einfach auf einen Blick sehen, welche Produkte installiert worden sind und auf welchen Betriebssystemen sie laufen.

Darüber hinaus bietet unser Dashboard auch Informationen über die zuletzt aufgerufenen Nutzerprofile. Sie können sehen, wer zuletzt aktiv war und wer nicht, um besser zu verstehen, wie Ihre Nutzer die Anwendungen nutzen. Außerdem wird auch gezeigt, auf welchen Geräten die Profile der Nutzer abgerufen wurden, damit Sie genau wissen, wo und wie Ihre Benutzer auf die jeweiligen u.trust LAN Crypt Produkte zugreifen.

## Verwalten von Administratoren

Innerhalb der LAN Crypt Cloud Administration haben Sie die Möglichkeit, beliebig viele Administratoren hinzuzufügen. Um die Administration zu verwalten, klicken Sie zunächst auf das **Profil-Icon** oben rechts und wählen anschließend **Konto verwalten**. Im folgenden Schritt öffnen Sie den Reiter **Administratoren**. Hier können Sie Administratoren hinzufügen, bearbeiten und entfernen. Zusätzlich besteht die Option, einen Administrator als primären Ansprechpartner für die Kommunikation mit Utimaco festzulegen.

### Hinweis

- Alle Administratoren verfügen über dieselben administrativen Funktionen und können dementsprechend auch andere Administratoren (außer sich selbst) entfernen.

## Verwalten von Assets

### Was sind Assets?

Assets sind Speicheradressen, welche für eine Organisation wichtige Daten beinhalten. Mit u.trust LAN Crypt Cloud haben Sie die Möglichkeit, den Zugriff auf diese Speicheradressen zu kontrollieren und zu verwalten. Dabei können Sie mehrere Assets besitzen und den Zugriff auf diese auf einzelne Personen oder Gruppen innerhalb Ihrer Organisation beschränken. Die Zugriffsberechtigungen werden durch eine sichere Verschlüsselung der Daten in den Speicheradressen realisiert und passende Schlüssel werden nur an berechtigte Gruppen und Personen verteilt. Zu beachten ist, dass die Zugriffsrechte auf Assets vererbt werden. Das bedeutet, dass Asset-Berechtigungen automatisch nach unten vererbt werden und somit andere Assets, die sich in Unterverzeichnissen befinden, bei der Definition eines neuen Assets immer einbezogen werden.

### Erstellen und Bearbeiten von Assets

Um ein Asset im Reiter **Assets** zu erstellen, wählen Sie **Alle Assets** und klicken auf das Symbol zum Hinzufügen. Nun müssen Sie dem Asset einen Namen, eine **Speicheradresse** und einen **Asset type** zuordnen. Optional können Sie auch direkt Gruppen zuweisen, die auf dieses Asset Zugriff haben sollen. Dies kann aber auch noch im Nachhinein getan werden. Klicken Sie abschließend auf **Save** und die Erstellung des Assets ist abgeschlossen.

Eigenschaften und Zugriffsberechtigungen eines Assets können jederzeit bearbeitet werden. Ausnahme ist hier jedoch der **Asset Typ**, der nach der initialen Erstellung des Assets unveränderbar bleibt. Um die Eigenschaften eines Assets zu bearbeiten, wählen Sie einfach das jeweilige Asset innerhalb der Auflistung unter dem Reiter **Assets** aus. Mit dem **Müll-Icon** neben einem Asset-Eintrag können Sie erstellte Assets auch direkt löschen.

### Löschen und Wiederherstellen von Assets

Soll ein Asset gelöscht werden, navigieren Sie zum Reiter **Assets** und wählen **Alle Assets**. Über das Löschesymbol können Sie das gewünschte Asset entfernen. Gelöschte Assets werden in den Reiter **Gelöschte Assets** verschoben. Zuweisungen von Zugriffsberechtigungen an Benutzer oder Gruppen werden dabei entfernt. Das Asset kann bei Bedarf wiederhergestellt werden.

Um ein Asset wiederherzustellen, wählen Sie im Reiter Assets den Bereich Gelöschte Assets aus. Mit dem Wiederherstellungssymbol kann ein Asset reaktiviert werden.

Beim Wiederherstellen stellen sie bitte sicher, dass die gewählten Einstellungen und Zugriffsberechtigungen für das Asset den aktuellen Anforderungen entsprechen und keine Konflikte mit anderen aktiven Assets bestehen. Im Falle eines Konflikts werden Sie aufgefordert, diesen zu beheben bevor das Asset wiederhergestellt werden kann.

## Asset Typen

### Geteilt

Die Nutzung von **geteilten** Assets empfiehlt sich bei Speicheradressen, dessen Zugriffsberechtigungen an eine oder mehrere Gruppen verteilt werden soll. Hier werden im Hintergrund alle Daten innerhalb der angegebenen Speicheradresse mit einem Asset-spezifischen Schlüssel verschlüsselt, welcher an die zugeordneten Gruppen und Personen verteilt wird.

### Öffentlich

Die Nutzung von **öffentlichen** Assets empfiehlt sich bei Speicheradressen, dessen Inhalte von allen Verschlüsselungen ausgeschlossen werden soll. Dies bewirkt, dass alle Nutzer der Organisation frei auf diese Inhalte zugreifen können.

#### Hinweis

- Damit die Funktionalität eines **öffentlichen** Assets im vollen Umfang nutzen zu können, müssen alle Nutzer, welche im Rahmen eines **geteilten** Assets oder **privaten** Assets auf diese Speicheradresse Zugriff haben, dem jeweiligen **öffentlichen** Assets zugeordnet werden. Findet diese Zuordnung nicht statt, werden alle Daten von nicht zugeordneten Nutzern **verschlüsselt** in die Speicheradresse des **öffentlichen** Assets abgelegt.

### Privat

Es wird empfohlen, **private** Assets zu verwenden, wenn der Zugriff auf einzelne Personen beschränkt werden soll. Innerhalb dieses Assets werden alle Daten mit individuellen Schlüsseln der zugeordneten Personen verschlüsselt, selbst wenn sie sich in derselben Gruppe befinden.

## Angabe von Speicheradressen

Speicheradressen bei u.trust LAN Crypt Cloud definieren, welche Daten verschlüsselt werden sollen. Sie stellen Verschlüsselungspfade dar und definieren Verschlüsselungsregeln für diesen.

### Beispiel:

Speicheradresse: C:\meine\_daten\marketing\

Durch die Angabe dieser Speicheradresse werden sämtliche Dateien innerhalb des Ordners `marketing` verschlüsselt.

Um eine fehlerhafte Funktionsweise zu vermeiden, stellen Sie sicher, dass die Speicheradresse stets mit einem Schrägstrich / (für UNIX-Systeme wie macOS und Linux) oder einem umgekehrten Schrägstrich \ (für Windows) abgeschlossen wird.

#### Hinweis

- Pfade zu komprimierten Ordnern können nicht als Verschlüsselungspfade verwendet werden.

## Angabe von Speicheradressen bei SMB-Freigaben

Um eine korrekte Verschlüsselung Ihrer SMB-Freigaben sicherzustellen, ist es entscheidend, dass die in den Verschlüsselungsregeln angegebenen Pfade genau mit den Pfaden Ihrer Mountpoints übereinstimmen. Wenn die Pfade nicht exakt übereinstimmen, wird die Verschlüsselung nicht aktiviert.

### Beispiel für ein korrektes Match:

Regel: `smb://newhost.newdomain.local/newpath/anotherpath/*.*`

Mount: `smb://newuser@newhost.newdomain.local/newpath`

## Umgebungsvariablen

u.trust LAN Crypt Cloud unterstützt die Verwendung der lokalen Umgebungsvariable `%USERNAME%` in Pfadangaben. Die Umgebungsvariable `%USERNAME%` in Pfadangaben wird von u.trust LAN Crypt Cloud standardmäßig aufgelöst.



## Verwalten von Identitäten

### Was sind Identitäten?

Identitäten stellen innerhalb u.trust LAN Crypt Cloud einzelne Nutzer, Gruppen und Untergruppen in Ihrer Organisation dar. Dies ermöglicht die übersichtliche Modellierung Ihrer internen Unternehmensstruktur und folgend die einfache Zuordnung einzelner Nutzer zu den jeweiligen Gruppen und Untergruppen.

### Erstellen und Einladen von Nutzern

Zum Erstellen und Einladen eines Nutzers innerhalb des Reiters **Identitäten**, klicken Sie in der Liste auf **Nutzer** und anschließend auf den blauen Aktionsknopf neben **Neuer Nutzer**. Nun können Sie dem neuen Nutzer einen Namen, Nachnamen und eine Beschreibung geben. Außerdem ist es notwendig eine E-Mail-Adresse des Nutzers zu hinterlegen und eine Anmeldemethode zu wählen. Optional kann schon beim Anlegen des Nutzers die Zuordnung zu verschiedenen Gruppen getätigt werden. Dies ist jedoch auch zu jedem späteren Zeitpunkt möglich.

Nach dem Anlegen und Einladen des Nutzers wird dieser über die angegebene E-Mail-Adresse aufgefordert, seinen Konto zu aktivieren und ein Passwort für seinen Nutzer-Konto zu setzen. Sind beide dieser Schritte erfolgreich abgeschlossen, so ist die Registrierung des Nutzers abgeschlossen.

Bei der Anmeldemethode mittels Microsoft Entra ID ist es nicht erforderlich, ein zusätzliches Passwort zu erstellen. Nach Bestätigung des Nutzerkontos über den Link in der Bestätigungsmail kann der Nutzer sein Microsoft-Konto für künftige Anmeldevorgänge nutzen.

Wurde ein Nutzer angelegt und eingeladen, erscheint dieser in der Liste aller bestehender Nutzer. Das **Stift-Symbol** im Eintrag erlaubt das nachträgliche Bearbeiten der Nutzerinformationen und Gruppenzuordnungen. Das **Kreissymbol mit drei Punkten** signalisiert das Ausstehen des abgeschlossenen Registrierungsvorgangs. Ist die Registrierung des jeweiligen Nutzers erfolgreich abgeschlossen, verschwindet das Symbol.

Durch Klicken auf das **Pfeil-Symbol** in den jeweiligen Nutzereinträgen können nähere Details zu einem Benutzer abgerufen werden.

### Erstellen und Bearbeiten von Gruppen

Zum Erstellen einer Gruppe innerhalb des Reiters **Identitäten**, klicken Sie erst auf die übergeordnete Gruppensammlung **Users and Groups** und anschließend auf den blauen Aktionsknopf neben **New group**. Nun können Sie der Gruppe einen Namen und eine Beschreibung geben. Auch können Sie die **Übergeordnete Gruppen** noch anpassen, um z.B die Gruppe doch einer anderen Gruppe unterzuordnen. Auch lassen sich noch weitere Zugehörigkeiten hinzufügen.

Um eine Untergruppe zu erstellen, klicken Sie erst auf die gewünschte übergeordnete Gruppe und abschließend auf den blauen Aktionsknopf neben **Neue Gruppe**. Auch hier lassen sich Name, Beschreibung und **Übergeordnete Gruppen** der Untergruppe noch anpassen.

Sie können den Namen, die Beschreibung und die **Übergeordnete Gruppe** im Nachhinein jederzeit bearbeiten indem Sie erst die zu bearbeitende Gruppe innerhalb der Liste wählen und dann auf das **Stift-Symbol** klicken.

#### Hinweis

- Ist eine Untergruppe mehreren Gruppen untergeordnet, so werden Änderungen an der Untergruppe oder deren Untergruppen an allen entsprechenden Stellen automatisch aktualisiert.

## Verwaltung der Zugriffsberechtigungen von Gruppen, Nutzern und Assets

Die Zugriffsberechtigungen für Assets lassen sich auf verschiedene Arten verteilen:

Eine Möglichkeit zur Vergabe von Zugriffsrechten besteht darin, diese direkt im Definitionsdialog für ein Asset zu verteilen. Dort können einzelne Nutzer und Gruppen dem jeweiligen Asset zugeordnet werden. Nach der Erstellung von Assets können Zugriffsberechtigungen auch in der Asset-Übersicht im Reiter **Assets** verwaltet werden.

Eine alternative Möglichkeit zur Verwaltung von Zugriffsberechtigungen besteht darin, diese im Reiter **Identitäten** den jeweiligen Gruppen hinzuzufügen. Jede Gruppe oder Untergruppe enthält **Mitglieder** (Nutzer) und **Assets**. Diese können durch das Aufklappen der Gruppe und das Klicken des jeweiligen blauen Aktionsknopfs neben **Mitglied hinzufügen** oder **Asset zuweisen** zugewiesen werden. Durch diese Zuordnung erhalten alle Nutzer einer Gruppe die spezifischen Zugriffsberechtigungen über die zugeordneten Assets.

## Hinweis

- Die Zugriffsrechte auf Assets werden vererbt. Das bedeutet, dass Asset-Berechtigungen automatisch nach unten vererbt werden und somit andere Assets, die sich in Unterverzeichnissen befinden, bei der Definition eines neuen Assets immer einbezogen werden.

## Einstellungen

### Synchronisation

Im Abschnitt **Synchronisation** in den Einstellungen stehen Ihnen die folgenden Konfigurationsoptionen zur Verfügung:

**Aktualisierungsintervall:** Hier legen Sie fest, in welchem Intervall sich die Clients automatisch mit dem Server verbinden, um Aktualisierungen der Richtlinien abzurufen.

**Richtlinien-Gültigkeitsdauer:** Diese Einstellung definiert, wie lange empfangene Richtlinien ihre Gültigkeit behalten, sofern während dieser Zeitspanne keine Verbindung zum Server hergestellt werden kann. Jedes erfolgreiche Aktualisieren der Richtlinie setzt den gewählten Gültigkeitszeitraum auf die volle Zeitspanne zurück.

### Dateiverschlüsselung

Im Abschnitt **Dateiverschlüsselung** in den Einstellungen stehen Ihnen die folgenden Konfigurationsoptionen zur Verfügung:

**Benutzer darf entschlüsseln:** Diese Einstellung bestimmt, ob der Benutzer berechtigt ist, Dateien, die keiner Verschlüsselungsregel unterliegen, manuell zu ver- und entschlüsseln.

**Persistente Verschlüsselung (Windows):** Diese Einstellung bestimmt, ob Dateien auch nach dem Verschieben oder Kopieren weiterhin verschlüsselt bleiben sollen.

Wenn die persistente Verschlüsselung deaktiviert ist und ein Benutzer eine verschlüsselte Datei in einen Ordner kopiert, der keiner Verschlüsselungsregel unterliegt, wird die Datei im Zielordner automatisch entschlüsselt. Ist die persistente Verschlüsselung hingegen aktiviert, bleibt die Datei auch bei einem Kopieren oder Verschieben in einen Ordner ohne Verschlüsselungsregel weiterhin verschlüsselt. Wird die Datei jedoch in einen Speicherort kopiert oder verschoben, für den eine andere Verschlüsselungsregel gilt, hat diese Vorrang vor der persistenten Verschlüsselung. In diesem Fall wird die Datei gemäß der im Zielspeicherort festgelegten Regel verschlüsselt.

Weitere Informationen zur persistenten Verschlüsselung des Windows-Clients finden Sie [hier](#).

### Key Server

Die Key-Server-Funktion in LAN Crypt Cloud speichert Verschlüsselungsschlüssel sicher außerhalb der Cloud mithilfe eines ESKM (Enterprise Secure Key Manager). Dies gewährleistet eine sichere Schlüsselverwaltung sowie eine nahtlose Verschlüsselung und Entschlüsselung. Weitere Informationen finden Sie im Kapitel [Key-Server \(ESKM\)](#).

### Auditlog

Über den Reiter **Auditprotokolle** haben Sie Zugriff auf eine umfassende Protokollierung Ihrer Admin-Aktivitäten, welche Sie gezielt filtern und durchsuchen können. Sie können dabei beispielsweise nach einem bestimmten Zeitraum, einem spezifischen Aktivitätstyp oder einem betroffenen Nutzer filtern, indem Sie die entsprechenden Felder nutzen. Anschließend können Sie die gesetzten Filter durch Betätigung des blauen Aktionsknopfes mit dem **Lupen-Symbol** bestätigen.

---

# Key Server (ESKM)

## Key Server Funktionalität

Mit LAN Crypt Cloud werden alle Schlüssel standardmäßig sicher in der Cloud gespeichert. Alternativ ermöglicht die cloudbasierte Administration, Schlüssel direkt verschlüsselt auf einem Key-Server zu erzeugen, wodurch eine unabhängige und selbst gehostete Speicherung realisiert werden kann. Alle administrativen Funktionen stehen dabei weiterhin uneingeschränkt zur Verfügung, einschließlich der sicheren Exportfunktion für generierte Schlüssel.

Als Schlüsseltechnologie nutzt LAN Crypt Cloud den Enterprise Secure Key Manager (ESKM) zur sicheren Verschlüsselung und Speicherung von Schlüsseln außerhalb der Cloud. ESKMs sind in verschiedenen Ausführungen erhältlich – von einfachen virtuellen Instanzen bis hin zu hochsicheren, manipulationssicheren physischen Geräten. Alle Modelle lassen sich flexibel mit LAN Crypt Cloud kombinieren und ermöglichen eine sichere Speicherung der Schlüssel.

Wenn eine ESKM-Instanz mit der LAN Crypt Cloud verbunden ist, werden alle administrativen Funktionen automatisch so angepasst, dass alle neu erzeugten Schlüssel direkt von der ESKM-Instanz abgerufen werden. Dies erfolgt nahtlos während der Ver- und Entschlüsselungsprozesse eines verwalteten Clients. Dabei werden alle Schlüsselabrufe von einer ESKM-Instanz zum Client stets durch vorherige Authentisierung und kryptografischen Schutz der Schlüssel selbst geprüft und validiert. Auch bei der Überprüfung und Validierung der Zugangsrechte verbleiben Schlüssel in der gesicherten Umgebung und werden unter keinen Umständen in die Cloud übertragen.

## Konfiguration: LAN Crypt Cloud und ESKM

### LAN Crypt Cloud als lokaler Nutzer einer ESKM-Instanz

Um die Key-Server-Funktionalität zu nutzen und Schlüssel sicher auf einer ESKM-Instanz zu erzeugen, muss LAN Crypt Cloud als lokaler Nutzer zur entsprechenden ESKM-Instanz hinzugefügt werden. Dies kann im ESKM-GUI unter **Security > Users & Groups > Local Users & Groups** erfolgen. Die Kommunikation zwischen der LAN Crypt Cloud und der ESKM-Instanz erfolgt über die RESTful API.

Folgende Einstellungen sind für die Erstellung des Nutzers empfohlen:

**KMIP-enabled:** Deaktiviert

**User Administration Permission:** Deaktiviert

**Change Password Permission:** Deaktiviert

**License Type:** RESTful API

### ESKM als Key Server in LAN Crypt Cloud

Besteht für LAN Crypt Cloud ein lokaler Nutzer in der ESKM-Instanz, kann dieser nun mit LAN Crypt Cloud verknüpft und die ESKM-Instanz als Key Server genutzt werden. Melden Sie sich dazu in Ihrer LAN Crypt Cloud Administration an und navigieren Sie zu **Settings > Key Server**.

Geben Sie nun die Zugangsdaten ein. Der **Benutzername**, das **Passwort** sowie das **Zertifikat** können im angelegten lokalen Nutzer im ESKM-GUI gefunden werden. Die **Standard-Portnummer** des REST-Servers für die Kommunikation über die RESTful API ist **8443**. Diese Portnummer kann jedoch je nach Konfiguration variieren und in der ESKM-GUI unter **Device > Rest Server** angepasst werden.

**Die Aktivierung der Key-Server-Integration ist eine irreversible Aktion. Nach der Aktivierung werden alle neu generierten Schlüssel ausschließlich im Key Server erstellt und sicher gespeichert. Bereits vorhandene Schlüssel verbleiben jedoch in der Cloud und bleiben weiterhin zugänglich. Nach der Aktivierung der Key-Server-Integration liegt die Verantwortung für die Sicherstellung eines unterbrechungsfreien Zugriffs auf verschlüsselte Daten, einschließlich Backup, Wiederherstellung und Verfügbarkeit des Dienstes, beim Betreiber des externen Key Servers. Benutzer müssen sicherstellen, dass der Betreiber diese Anforderungen erfüllt, um einen möglichen Datenzugriffsverlust zu vermeiden.**

## Export von Schlüsseln aus der ESKM-Instanz

### Vorbereitung

Um Schlüssel aus der ESKM-Instanz zu exportieren, benötigen Sie zunächst das Import-Export-Tool (**Profil-Icon > Konto verwalten > Anwendungen > Key Import Export Tool für Key Server**) sowie eine zuvor aus der Cloud Administration erstellte Exportdatei (**Profil-Icon > Konto verwalten > Datenexport > Schlüssel-Export starten**).

Das Import-Export-Tool nutzt die Informationen aus dieser Exportdatei, um die Schlüssel aus der ESKM-Instanz zu extrahieren. Sollten zusätzlich weitere Schlüssel in der Cloud gespeichert sein, werden auch diese in der finalen Schlüsseldatei enthalten sein.

Die erzeugte Schlüsseldatei ist kompatibel mit LAN Crypt 2Go und kann für die manuelle Entschlüsselung von Dateien verwendet werden.

## Ausführen des Import Export Tools

### Windows

Ausführen des Tools: `bash LCKeyImportExport.exe export --keyfile <PATH> --output <OUTPUT>`

### macOS

Quarantäne-Flags entfernen (einmalig): `bash xattr -c LCKeyImportExport`

Tool ausführbar machen (einmalig): `bash chmod +x LCKeyImportExport`

Ausführen des Tools: `bash ./LCKeyImportExport export --keyfile <PATH> --output <OUTPUT>`

### Linux

Tool ausführbar machen (einmalig):

```
bash chmod +x LCKeyImportExport
```

Ausführen des Tools:

```
bash ./LCKeyImportExport export --keyfile <PATH> --output <OUTPUT>
```

### Befehlsoptionen:

Option	Beschreibung
<code>--keyfile &lt;PATH&gt;</code>	Pfad zur Schlüssel-Export-Zip-Datei.
<code>--keyfile-password &lt;keyfile-password&gt;</code>	Passwort zum Öffnen der verschlüsselten Schlüssel-Export-Zip-Datei. Nur erforderlich, wenn die Datei passwortgeschützt ist.
<code>--keyserver-accept-invalid-certs</code>	Akzeptiert ungültige SSL-Zertifikate - <b>MIT VORSICHT VERWENDEN.</b>
<code>--output &lt;OUTPUT&gt;</code>	Name der Ausgabedatei. Sie sollte mit <code>.zip</code> enden.
<code>-h, --help</code>	Hilfe anzeigen.

---

## Microsoft Entra ID Synchronisation

Neben dem manuellen Hinzufügen von Benutzern und Gruppen kann u.trust LAN Crypt Cloud auch Benutzer- und Gruppeninformationen aus einer Microsoft Entra ID synchronisieren. Dies ist ein schneller und einfacher Weg, um Assets basierend auf der Ihnen schon bekannten Organisationsstruktur zuzuweisen. Hierbei handelt es sich um eine Outbound-Only-Synchronisierung, bei welcher Änderungen nur von der Microsoft Entra ID zur Anwendung übertragen werden und nicht umgekehrt. Das bedeutet, dass Änderungen, die in u.trust LAN Crypt Cloud vorgenommen werden, nicht zurück zur Microsoft Entra ID synchronisiert werden, sondern nur Änderungen innerhalb der Microsoft Entra ID zur u.trust LAN Crypt Cloud importiert werden.

Die Synchronisation erfordert einige Einrichtungsschritte, die notwendig sind, um eine Verbindung zwischen u.trust LAN Crypt Cloud und Ihrer Microsoft Entra ID herzustellen. Sobald die Verbindung hergestellt ist, kann der Import und die Synchronisierung der neuesten Benutzerinformationen mit einem Klick innerhalb der u.trust LAN Crypt Cloud getätigt werden.

### Beschreibung des Einrichtungsvorgangs

#### Schritt 1: Registrierung von u.trust LAN Crypt Cloud als Anwendung bei der Microsoft Identity Platform

Der erste Schritt der Einrichtung ist die Registrierung von u.trust LAN Crypt Cloud als Anwendung bei der Microsoft Identity Platform, denn diese führt die Identitäts- und Zugriffsverwaltung (IAM) nur für registrierte Anwendungen durch. Die Registrierung von u.trust LAN Crypt Cloud stellt eine Vertrauensbeziehung zwischen der Anwendung und der Microsoft-Identitätsplattform her. Das Vertrauen ist unidirektional: u.trust LAN Crypt Cloud vertraut der Microsoft-Identitätsplattform und nicht umgekehrt.

Es wird empfohlen für die Registrierung der Anwendung einen eindeutigen Namen zu nutzen, um die Anwendung klar zu identifizieren. Wichtig ist, dass Sie bei der Auswahl der **Unterstützte Kontotypen** für die Registrierung der Anwendung die Option **Konten in einem beliebigen Organisationsverzeichnis (beliebiger Microsoft Entra ID-Mandant – mandantenfähig)** auswählen.

Für Informationen zur Registrierung einer Anwendung bei der Microsoft Identity Platform siehe [Schnellstart: Registrieren einer Anwendung bei Microsoft Identity Platform](#).

#### Schritt 2: Erteilung von API-Berechtigungen

Im nächsten Schritt müssen der registrierten Anwendung API-Berechtigungen zugeteilt werden. Diese sind nötig, um u.trust LAN Crypt Cloud zu erlauben, sich ohne Benutzerinteraktion oder Zustimmung selbst zu authentifizieren.

Um die volle Funktionalität von u.trust LAN Crypt Cloud sicherzustellen werden sechs verschiedene Berechtigungen benötigt:

- **Directory.Read.All**
- **Group.Read.All**
- **GroupMember.Read.All**
- **Organization.Read.All**
- **User.Read**
- **User.Read.All**

#### Hinweis

- Beim Erteilen von Berechtigungen für **Microsoft Graph** haben Sie zwei Möglichkeiten. Es ist wichtig, dass Sie hier **Anwendungsberechtigungen** auswählen, da die Synchronisation im Hintergrund als Dienst arbeitet.

Nach der Konfiguration der API-Berechtigungen muss abschließend die administrative Zustimmung erteilt werden, um die Konfiguration abzuschließen.

img/Permissions\_DE.png

Für Informationen zur Erteilung von API-Berechtigungen für eine Anwendung siehe [Schnellstart: Konfigurieren einer Clientanwendung für den Zugriff auf eine Web-API](#).

### Schritt 3: Konfiguration der Anmeldeinformation

u.trust LAN Crypt Cloud benötigt für den Zugriff auf die Microsoft Graph API die Konfiguration von Anmeldeinformation innerhalb der Registrierten Anwendung bei der Microsoft Identity Platform. Ein geheimer Clientschlüssel ermöglicht es der Anwendung, sich zu authentifizieren, ohne das manuelle Eingreifen eines Nutzers zu erfordern.

Erstellen Sie einen neuen geheimen Clientschlüssel und wählen Sie einen gewünschten Gültigkeitszeitraum aus. Es wird ein Gültigkeitszeitraum von nicht mehr als 12 Monate empfohlen.

**Wichtig:** Die generierte **geheime ID** wird nach einem Wechseln oder Schließen des Dialogs nicht mehr angezeigt. Da diese für den Verbindungsaufbau mit u.trust LAN Crypt Cloud benötigt wird, wird empfohlen, diese an einem anderen sicheren Ort aufzubewahren.

Für Informationen zur Erstellung eines geheimen Clientschlüssels siehe [Schnellstart: Registrieren einer Anwendung bei Microsoft Identity Platform](#).

### Schritt 4: Verbindungsaufbau mit u.trust LAN Crypt Cloud

Nachdem alle Einrichtungsschritte der Microsoft Entra ID Synchronisation abgeschlossen sind, kann die Verbindung mit u.trust LAN Crypt Cloud hergestellt werden.

Loggen Sie sich hierfür bei der u.trust LAN Crypt Cloud ein und wählen Sie den Dialog **Identitätsprovider** und abschließend **Verbindungen**. Erstellen Sie mit dem blauen Aktionsknopf eine neue Verbindung und geben Sie nun einen beliebigen **Verbindungsnamen**, die **Verzeichnis-ID (Mandant)**, die **Anwendungs-ID (Client)** und die vorher generierte **geheime ID** an und klicken Sie auf **Weiter**.

Legen Sie nun die Anmeldemethode für Ihre Benutzer fest und klicken Sie dann erneut auf **Weiter**. Anschließend wird eine Zusammenfassung der zu erstellenden Microsoft Entra ID-Synchronisation angezeigt. Klicken Sie auf **Erstellen**, um den Verbindungsaufbau abzuschließen.

#### Hinweis

- Die **Verzeichnis-ID (Mandant)** und **Anwendungs-ID (Client)** können unter **Übersicht** innerhalb der Anwendung bei der Microsoft Identity Platform eingesehen werden.

### Importieren und Verwalten von Benutzer- und Gruppeninformationen

Die Nutzer- und Gruppeninformationen aus verschiedenen Microsoft Entra IDs können jederzeit innerhalb u.trust LAN Crypt Cloud importiert, aktualisiert oder gelöscht werden. Mit dieser Möglichkeit können Administratoren schnell Änderungen an importierten Benutzer- und Gruppeninformationen vornehmen und sicherstellen, dass das Verzeichnis stets auf dem neuesten Stand ist.

#### Importieren von Benutzer- und Gruppeninformationen

Um neue Benutzer- und Gruppeninformationen erstmals zu importieren, loggen Sie sich bei der u.trust LAN Crypt Cloud ein und wählen Sie im unter dem Punkt **Identitätsprovider** den Dialog **Import**. Nun können Sie unter allen bestehenden Verbindungen die gewünschten Personen und Gruppen auswählen und importieren. Der Importvorgang wird gestartet und kann unter **Import-Jobs** unter dem Punkt **Identitätsprovider** eingesehen werden. Die importierten Benutzer und Gruppen können unter dem Punkt **Identitäten** in die innerhalb der u.trust LAN Crypt Cloud angelegten Gruppen zugeordnet und verwaltet werden.

Weitere Benutzer- und Gruppeninformationen lassen sich ebenfalls jederzeit über den Dialog **Import**

#### Aktualisieren und Löschen von Benutzer- und Gruppeninformationen

Unter dem Punkt **Identitätsprovider** können im Dialog **Verbindungen** bestehende Benutzer- und Gruppeninformationen aktualisiert und Verbindungen zu Microsoft Entra IDs gelöscht werden. Klicken Sie hierfür auf die entsprechenden Icons im Eintrag der jeweiligen Microsoft Entra ID Verbindung.

#### Hinweis

- Beim Aktualisieren sind nur die vorher importierten Benutzer- und Gruppeninformationen betroffen. Es werden keine weiteren Benutzer- oder Gruppeninformationen importiert.
  - Löscht man die Verbindung zu einer Microsoft Entra ID, so werden alle zugehörigen Gruppen und Benutzer aus dem administrierten Pool der Identitäten automatisch entfernt.
-

## Migration passwortbasierter Schlüssel

LAN Crypt 2Go und alle mobilen u.trust LAN Crypt Anwendungen unterstützen die Verschlüsselung mit passwortbasierten Schlüsseln. Diese Schlüssel werden vom Benutzer selbst erstellt und verwaltet. Bei der Erstellung werden passwortbasierte Schlüssel lokal im Schlüsselbund des Benutzers auf dem Gerät selbst gespeichert. Die Schlüssel werden nicht mit anderen Geräten synchronisiert und müssen daher auf jedem Gerät, auf dem sie benötigt werden, manuell hinzugefügt werden.

Bei dem Login eines Nutzers mit seinem **u.trust LAN Crypt Cloud Konto** werden alle neu erstellten Schlüssel mit seinem Konto verknüpft und in das **Cloud-Management-System** hochgeladen. Dies ermöglicht die Synchronisierung mit allen anderen Geräten, bei denen sich der Nutzer mit seinem u.trust LAN Crypt Cloud Konto einloggt.

Loggt ein Nutzer sich das erste Mal innerhalb einer u.trust LAN Crypt Anwendung ein, welche Verschlüsselung mit passwortbasierten Schlüsseln unterstützt, wird geprüft, ob Schlüssel im lokalen Schlüsselbund des Benutzers gespeichert sind. Falls der Benutzer bereits zuvor passwortbasierten Schlüsseln erstellt hat, gibt es zwei Möglichkeiten fortzufahren. Die erste Option ist, sich mit der Cloud zu verbinden - wobei alle lokal erstellten Schlüssel in die Cloud hochgeladen werden. Alternativ kann der Vorgang abgebrochen werden, wenn nicht gewollt wird, dass einige oder alle seiner Schlüssel hochgeladen werden. In letzterem Fall besteht die Möglichkeit, alle Schlüssel aus dem Schlüsselbund zu löschen, die nicht in die Cloud hochgeladen werden sollen. Nach erneutem Login, werden dann alle gewünschten Schlüssel mit dem Konto verknüpft und in die Cloud hochgeladen.

---

## Exportieren von Verschlüsselungsschlüsseln

Administratoren von u.trust LAN Crypt Cloud können eine Schlüsselausgabedatei generieren, die alle erstellten Verschlüsselungsschlüssel enthält. Diese Datei ist für Organisationen praktisch, die die Nutzung von LAN Crypt einstellen möchten, da sie die Entschlüsselung aller verschlüsselten Dateien mit dem {{ site.productName2Goneutral }} Befehlszeilentool ermöglicht.

Um die Schlüssel zu exportieren, klicken Sie auf das Profil-Symbol und wählen Sie **Konto verwalten** im Einstellungsfenster. Klicken Sie dann auf **Export** und starten Sie den Exportprozess. Sobald der Exportvorgang erfolgreich abgeschlossen ist, können Sie die Schlüsseldatei herunterladen. Die Datei ist eine passwortgeschützte ZIP-Datei, welche eine einzelne JSON-Datei enthält, die alle Verschlüsselungsschlüssel Ihrer Organisation enthält.

Das Passwort für die ZIP-Datei wird nach dem erfolgreichen Export per E-Mail gesendet.

Für detaillierte Anweisungen zur Verwendung der exportierten Schlüssel zum Entschlüsseln von Dateien mit dem u.trust LAN Crypt 2Go Befehlszeilentool, siehe [Verwendung des u.trust LAN Crypt 2Go Kommandozeilen-Tools](#) in der u.trust LAN Crypt 2Go Dokumentation.

---



## Technischer Support

**Technischen Support zu Utimaco-Produkten können Sie wie folgt abrufen:**

Unter [support.Utimaco.com](https://support.Utimaco.com) erhalten Wartungsvertragskunden Zugang zu weiteren Informationen, wie beispielsweise Knowledge-Items.

Als Wartungsvertragskunde senden Sie eine E-Mail an den technischen Support:

[support@Utimaco.com](mailto:support@Utimaco.com)

und geben Sie die Versionsnummer(n), Betriebssystem(e) und Patch-Level Ihrer Utimaco Software sowie ggf. den genauen Wortlaut von Fehlermeldungen ergänzend mit an.

---

## Rechtlicher Hinweis

Copyright © 2024 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 25.11.2024**