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.

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.

---

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 Anmeldungmethode 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.

Bei Verwendung der Microsoft Entra ID Anmeldemethode wird keine Aktivierungs-E-Mail versendet. Der Benutzer kann sich sofort mit dem Microsoft-Konto anmelden.

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.

Schlüssel: Sie können Ihre Verschlüsselungsschlüssel exportieren, um auch nach einer Deaktivierung des Cloud-Kontos weiterhin Zugriff auf verschlüsselte Assets zu behalten. Zusätzlich steht Ihnen die Schlüsselrotation als empfohlene Sicherheitsmaßnahme zur Verfügung, mit der Sie Ihre Schlüssel regelmäßig erneuern 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 **Aktive 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.

Hinweis

- Die Asset-Verschlüsselung wird über den LAN Crypt Client durchgeführt. Um eine ordnungsgemäße Implementierung zu gewährleisten, stellen Sie bitte sicher, dass die Asset-Definition mit dem Datei-/Pfadmuster übereinstimmt, das auf dem Endpunkt für den Zugriff auf die darin gespeicherten Daten verwendet wird (z. B. müssen die in der Asset-Definition verwendeten UNC-Pfade oder Laufwerksbuchstaben auch auf dem Endpunkt verfügbar sein und von diesem verwendet werden).

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 erstelle Assets auch direkt löschen.

Löschen und Wiederherstellen von Assets

Soll ein Asset gelöscht werden, navigieren Sie zum Reiter **Assets** und wählen **Aktive Assets** oder **Passives Asset**. Über das Löschsymbol 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.

Hinweis

- Wird ein passives Asset gelöscht und später wiederhergestellt, wird es im Zustand **Passives Asset** reaktiviert.

Passive Assets

Ein **passives Asset** bezeichnet ein Asset, bei dem die Verschlüssel ung für neu hinzukommende Dateien vorübergehend deaktiviert wird.

Ein Asset kann über den Menüpunkt **Assets → Aktive Assets** durch Auswahl des Icons **Asset passiv schalten** passiv geschaltet werden. Nach der Passivschaltung eines Assets werden neu erstellte Dateien in diesem Asset nicht mehr verschlüsselt. Bereits vorhandene, verschlüsselte Dateien bleiben jedoch geschützt und zugewiesene Benutzer behalten weiterhin Zugriff darauf.

Das Asset wird nun unter **Assets → Passive Assets** gelistet. Passive Assets behalten alle Konfigurationsparameter bei. Nur der Name des Assets und die zugewiesenen Benutzer und Gruppen können jedoch weiterhin angepasst werden, um Zugriffsrechte auf das Asset weiterhin zu steuern.

Passive Assets können über den Menüpunkt **Assets → Passive Assets** durch Auswahl des Icons für **Asset aktivieren** jederzeit wieder aktiviert werden und sind dann wieder im Fenster **Assets → Aktive Assets** einsehbar. Wird ein passives Asset erneut aktiviert, werden sowohl bereits vorhandene als auch künftig hinzugefügte Dateien in diesem Asset wieder automatisch verschlüsselt.

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 **geteitlen** 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: `\\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

Nutzer können unter **Identitäten** > **Benutzer** angelegt und eingeladen werden. Beim Erstellen eines neuen Nutzers sind **Vorname**, **Nachname**, **E-Mail-Adresse** sowie eine **Anmeldemethode** anzugeben. Eine **Beschreibung** ist optional. Die Zuordnung zu **Gruppen** kann direkt beim Anlegen oder zu einem späteren Zeitpunkt erfolgen.

Nach dem Anlegen erhält der Nutzer eine **Aktivierungs-E-Mail** an die hinterlegte Adresse. Abhängig von der gewählten Anmeldemethode wird der Nutzer aufgefordert, ein **Passwort** zu vergeben und sein Konto zu aktivieren. Bei Verwendung von **Microsoft Entra ID** entfällt die Passwortvergabe - der Nutzer authentifiziert sich nach der Kontobestätigung über sein bestehendes Microsoft-Konto.

Innerhalb der **Details** eines Benutzers lassen sich die zugewiesenen **Assets**, **Gruppenmitgliedschaften**, autorisierten Vertreter, genutzten Clients sowie weitere Sicherheitsinformationen einsehen und bearbeiten.

Erstellen und Bearbeiten von Gruppen

Gruppen können unter **Identitäten** > **Gruppen** angelegt werden. Beim Erstellen einer Gruppe werden ein **Name** und optional eine **Beschreibung** vergeben. Darüber hinaus lassen sich **übergeordnete Gruppen** definieren, um eine hierarchische Gruppenstruktur abzubilden.

Name, **Beschreibung** und **übergeordnete Gruppen** können nachträglich jederzeit über die Bearbeitungsfunktion in der Gruppenübersicht angepasst werden.

Innerhalb der **Details** einer Gruppe lassen sich die zugewiesenen **Assets**, **Gruppenmitgliedschaften**, **Untergruppen** sowie zugeordnete **Benutzer** einsehen und bearbeiten.

> **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

Zugriffsberechtigungen für Assets können auf zwei Wegen vergeben werden.

Über das Asset Direkt im Definitionsdialog eines Assets können einzelne Nutzer und Gruppen zugeordnet werden. Nach der Erstellung ist dies auch nachträglich in der Asset-Übersicht unter **Assets** möglich.

Über Identitäten Alternativ können Zugriffsberechtigungen unter **Identitäten** > **Benutzer** bzw. **Identitäten** > **Gruppen** direkt den jeweiligen Nutzern oder Gruppen zugewiesen werden. Öffnen Sie hierfür die **Details** des gewünschten Nutzers oder der gewünschten Gruppe und fügen Sie dort die entsprechenden Assets hinzu.

> **Hinweis** Zugriffsberechtigungen auf Assets werden vererbt. Berechtigungen, die für ein Asset vergeben werden, gelten automatisch auch für alle Assets in dessen Unterverzeichnissen.

Hinweis zur Gruppenverwaltung bei synchronisierten Identitätsprovidern

Sind Nutzer und Nutzergruppen durch die Synchronisation eines Identitätsproviders in der **LAN Crypt Administration** hinterlegt und wurden diesen Gruppen bereits Assets zugewiesen, kann es vorkommen, dass die zentrale Benutzerverwaltung des Unternehmens (z.B. die IT-Abteilung) ohne Zutun eines LAN Crypt-Administrators neue Nutzer zu diesen Gruppen hinzufügt. Dadurch erhalten diese Nutzer automatisch Zugriff auf entsprechende Assets - ohne dass dies innerhalb der LAN Crypt Administration explizit freigegeben wurde.

Um eine solche unbeabsichtigte Rechtevergabe zu vermeiden, wird empfohlen, statt der direkt synchronisierten Gruppen eigene Gruppen innerhalb der **LAN Crypt Administration** zu verwenden. Nutzer von Identitätsprovider können gezielt diesen internen Gruppen hinzugefügt werden, um die Zugriffskontrolle zentral und nachvollziehbar innerhalb von LAN Crypt zu steuern.

Autorisierter Vertreter

LAN Crypt Cloud ermöglicht es Ihnen, Benutzern (*autorisierten Vertretern*) Zugriff auf die *privaten* Assets eines anderen Benutzers zu gewähren. Dies deckt typische Szenarien im Benutzerlebenszyklus ab, wie Datenwiederherstellung, Aufgabenübertragung und Nachfolgeplanung.

1. **Wiederherstellung**: Wenn ein Benutzer die Organisation dauerhaft verlassen hat, müssen Sie möglicherweise einer bestimmten Person Zugriff auf die privaten Assets des ausscheidenden Benutzers gewähren.

2. **Aufgabenübertragung**: Wenn ein Benutzer jemanden benötigt, der in seinem Namen handelt – z. B. während einer längeren Abwesenheit – kann ein bevollmächtigter Stellvertreter auf die privaten Assets dieses Benutzers zugreifen.

3. **Nachfolger**: Wenn ein Benutzer den Platz oder die Rolle eines anderen einnimmt oder erbt, benötigt der Nachfolger möglicherweise Zugriff auf die privaten Assets seines Vorgängers, um die Geschäftskontinuität zu gewährleisten.

   Hinweis

   - Nur *private* Assets werden automatisch in den Zugriffsumfang des bevollmächtigten Vertreters übertragen. Assets anderer Art müssen weiterhin manuell verwaltet werden.
   - Die Autorisierung ist **nicht rekursiv**. Wenn Benutzer A der bevollmächtigte Vertreter für Benutzer B ist und Benutzer B der Stellvertreter für Benutzer C, erhält Benutzer A **nicht** automatisch Zugriff auf die privaten Assets von Benutzer C.
   - Ein autorisierter Vertreter kann für aktive und gelöschte Benutzer benannt werden. Das gilt für lokale Benutzer und Benutzer, die nicht mehr über die Microsoft Entra ID Synchronisierung erfasst sind.
   - Wenn ein aktiver Benutzer gelöscht wird (lokaler Benutzer) oder aus der Microsoft Entra ID-Synchronisierung entfernt wird, bleibt die autorisierte Vertretung bestehen.

Einrichtung eines bevollmächtigten Vertreters

Unter **Identitäten** > **Benutzer** können in den **Details** eines Benutzers im Abschnitt **Autorisierter Vertreter** bevollmächtigte Vertreter hinzugefügt und entfernt werden. Ein autorisierter Vertreter erhält Zugriff auf die privaten Assets des jeweiligen Benutzers.

Netzwerk-Firewall

Für eine sichere und zuverlässige Konfiguration von LAN Crypt müssen bestimmte Domains über Ihre Netzwerk-Firewall kommunizieren dürfen. Im Folgenden finden Sie eine Liste der wichtigsten LAN Crypt-Domains, die Zugriff benötigen:

```
auth.lancrypt.com

portal.lancrypt.com

user-portal.lancrypt.com

feature-flag.lancrypt.com

api.lancrypt.com

2go.lancrypt.com
```

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.

Fehlermeldungen unterdrücken (Windows): Mit dieser Einstellung wird gesteuert, ob Fehlermeldungen auf dem Windows LAN Crypt Client sichtbar sind. Bei aktivierter Option erfolgt keine Anzeige der Meldungen.

Outlook

u.trust LAN Crypt 2Go erweitert Microsoft Outlook um die Funktion, Dateianhänge vor dem Versand zu verschlüsseln. In der Administration können Sie die folgenden Einstellungen für das Outlook Add-In konfigurieren:

Prüfung beim Senden:

Aktiviert die Überprüfung der Empfänger-Domäne. Beim Versand an externe E-Mail-Domänen wird das Versenden unverschlüsselter Anhänge verhindert.

Interne Mail-Domänen:

Ermöglicht das Hinzufügen weiterer E-Mail-Domänen, die als intern gelten sollen. Standardmäßig wird nur die Domäne des Absenders als intern betrachtet.

Ausgenommene Anhänge:

Ermöglicht die Definition von Dateitypen (z. B. *.dat*, *.txt*, *.xls* usw.), die von der Prüfung ausgenommen sind und unverschlüsselt versendet werden dürfen.

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 **Auditprotokoll** 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 für LAN Crypt Cloud ein bestehender oder neu anzulegender lokaler Benutzer auf der entsprechenden ESKM-Instanz verwendet werden. Ein neuer Benutzer kann im ESKM-GUI unter **Security > Users & Groups > Local Users & Groups** angelegt werden. 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

Zertifikatserstellung

Um eine sichere Kommunikation zwischen LAN Crypt Cloud und einer ESKM-Instanz einzurichten, müssen Sie im ESKM-GUI über **Security > Certificates** ein Zertifikat generieren.

Beim Erstellen eines Zertifikats können Sie in der Einstellung **Subject Alternative Name** eine oder mehrere IP-Adressen und DNS-Namen hinzufügen. Diese sollten in folgendem Format aufgeführt sein:

```
IP: 192.0.2.1, DNS: example.com, IP: 2001:db8::1
```

> **Hinweis**
>
> Es gibt zwei Möglichkeiten, ein Zertifikat zu erstellen: **Certificate Request – to be signed by external CA** und **Certificate Signed by Local CA**.
>
> Wenn Sie ein von einer lokalen CA signiertes Zertifikat verwenden möchten, müssen Sie zuerst unter **Security > Local CAs** im ESKM-GUI eine lokale CA erstellen.

Nachdem Sie das Zertifikat generiert haben, müssen Sie es der REST-Server-Schnittstelle der ESKM-Instanz zuweisen. Wechseln Sie dazu im ESKM-GUI zu **Device > Rest Server** und wählen Sie das Zertifikat in der Einstellung **Server Certificate** aus. Zudem muss die Einstellung **Enable Key and Crypto Operation** aktiviert sein.

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** und das **Passwort** 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.

Das **Zertifikat**, das für LAN Crypt Cloud verwendet wird, wird im ESKM-GUI generiert und mit der REST-Server-Schnittstelle verknüpft. Es ist unter **Security > Certificates** zu finden und erscheint in der Regel in folgendem Format:

```
-----BEGIN CERTIFICATE-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtJDJ5Jd+G7BRM4nV1P8K
Kw2RyOaTYXZBfHlxNE+g9kw+j8HjkEHzEJDrZH4uD8mDKOPrlgP9S/y9YZRJaSHo
yMbHQU3WpCvNDgNm84hfdU9KsXqY5GWiVmVz3XOiF3pyT7ynwwEvF8Fv5RJF7BtT
QKnST1m4H19dkc4pYrX53MStpSpxrZ7FkUXYHRdLdU47jUGRP2/lSyJ4DH9D5vIe
mT2HBgh69y8QoXaNzThpjDEy4oqTcVPAVC9MzP9kX9iNSp9hWeSWkwWKHxZCbfKP -----END
CERTIFICATE-----
```

Kopieren Sie die vollständigen Zertifikatsdaten einschließlich der BEGIN- und END-Zeilen und fügen Sie sie in das **Zertifikat**-Feld in der LAN Crypt Cloud Administration ein.

> **Hinweis**
>
> Um zu überprüfen, welches Zertifikat mit der REST-Server-Schnittstelle der ESKM verknüpft ist, navigieren Sie im ESKM-GUI zu **Device > Rest Server**. Hier wird das aktuell verknüpfte Zertifikat angezeigt.

Bevor Sie die Key-Server-Integration aktivieren, sollten Sie unbedingt einen Verbindungstest durchführen. Beim Speichern der Einstellungen öffnet sich ein Bestätigungsfenster, in dem Ihnen ein passender Befehl (basierend auf Ihren eingegebenen Daten wie Benutzername, Passwort und Host/IP) angezeigt wird. Klicken Sie dort auf das 'Kopier-Symbol', um diesen Befehl in die Zwischenablage zu kopieren, führen Sie ihn in der Kommandozeile aus und prüfen Sie, ob die Ausgabe „Success" lautet. Erst wenn der Verbindungstest erfolgreich ist, sollten Sie die Konfiguration endgültig abschließen.

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 > Schlüssel > 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
`--keyfile <PATH>`	Pfad zur Schlüssel-Export-Zip-Datei.
`--keyfile-password <keyfile-password>`	Passwort zum Öffnen der verschlüsselten Schlüssel-Export-Zip-Datei. Nur erforderlich, wenn die Datei passwortgeschützt ist.
`--keyserver-accept-invalid-certs`	Akzeptiert ungültige SSL-Zertifikate - **MIT VORSICHT VERWENDEN**.
`--output <OUTPUT>`	Name der Ausgabedatei. Sie sollte mit `.zip` enden.
`-h, --help`	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.



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 belieben **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.
- Änderungen an der Anmeldemethode werden **erst nach der nächsten Synchronisierung für alle Benutzer wirksam**. Ab der darauffolgenden Anmeldung müssen sich alle Benutzer mit der neu festgelegten Methode anmelden.

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** einsehen.

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.

Es besteht auch die Möglichkeit, eine automatische, wiederkehrende Synchronisation zu aktivieren. Unter dem Punkt Wiederkehrend kann hierfür ein Zeitintervall festgelegt werden, in dem die aktuellen Benutzer- und Gruppeninformationen automatisch abgeglichen werden. Unabhängig davon kann die Synchronisation jederzeit auch manuell angestoßen werden.

Hinweis

- Das Intervall berechnet sich ab dem Zeitpunkt der letzten Synchronisation – ein angestoßener Abgleich setzt den Timer zurück und dient als neuer Ausgangspunkt für die folgenden Intervalle.
- Wird die Verbindung zu einer Microsoft Entra ID gelöscht, werden alle zugehörigen Gruppen und Benutzer automatisch aus dem verwalteten Identitätenpool entfernt.

Migration passwortbasierter Schlüssel

LAN Crypt 2Go und alle mobilen u.trust LAN Crypt Anwendungen unterstützten 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.

Schlüsselverwaltung

Durchführen einer Schlüsselrotation

Die Schlüsselrotation ist eine Sicherheitsfunktion, mit der bestehende Verschlüsselungsschlüssel durch neue ersetzt werden, um die Datensicherheit dauerhaft zu gewährleisten. Sie kann jederzeit und beliebig oft gestartet werden.

Mit jeder Rotation werden neue Schlüssel generiert, die ab diesem Zeitpunkt für die Verschlüsselung und Entschlüsselung neuer Daten innerhalb von Assets verwendet werden. Bereits vorhandene Dateien bleiben weiterhin mit den zuvor genutzten Schlüsseln verschlüsselt; diese Schlüssel gehen nicht verloren und werden auch beim Export der Verschlüsselungsschlüssel mit ausgegeben.

Um eine Schlüsselrotation zu starten, klicken Sie auf das Profil-Symbol und wählen Sie **Konto verwalten** im Einstellungsfenster. Klicken Sie dann auf **Schlüssel** und starten sie eine Schlüsselrotation. Nach Abschluss einer Schlüsselrotation erhält der Administrator eine Benachrichtigung per E-Mail, zudem lässt sich der aktuelle Status der Schlüsselrotation direkt im entsprechenden Tab einsehen.

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.productName*2Go*neutral }} Befehlszeilentool ermöglicht.

Um die Schlüssel zu exportieren, klicken Sie auf das Profil-Symbol und wählen Sie **Konto verwalten** im Einstellungsfenster. Klicken Sie dann auf **Schlüssel** 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.

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

Technischer Support

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

Unter 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

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 - 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 12.06.2026