Was ist u.trust LAN Crypt für macOS?

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

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

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

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

Schutz von Daten durch u.trust LAN Crypt für macOS

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

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

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

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

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

Konfigurationsdatei ersetzt Gruppenrichtliniendatei

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

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

Von u.trust LAN Crypt für macOS unterstützte Verschlüsselungsalgorithmen

u.trust LAN Crypt für macOS unterstützt folgende Verschlüsselungsalgorithmen:

- AES-256 Bit (XTS-Modus)
- AES-256 Bit (CBC-Modus)
- AES-128 Bit (XTS-Modus)
- AES-128 Bit (CBC-Modus)

Hinweis

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

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

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

- AES-256 Bit
- 3DES

Hinweis

- Wenn Sie Sicherheitstoken oder Smartcards verwenden, stellen Sie bitte sicher, dass diese bzw. die in diesem Zusammenhang verwendete Middleware auch den von Ihnen ausgewählten Algorithmus unterstützt.

Verschlüsselung

Zugriff auf verschlüsselte Dateien

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

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

Wenn eine Netzwerkfreigabe durch eine Verschlüsselungsregel abgedeckt ist, steht im Menü-Eintrag von *u.trust LAN Crypt für macOS* ein Schnellzugriff auf den eingehängten Ordner zur Verfügung.

Verschlüsselung von 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`

Explizite Entschlüsselung von Dateien

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

Voraussetzungen:

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

Konfiguration mit u.trust LAN Crypt Cloud als Administration

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

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

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

Konfigurationsdatei erstellen

Alle Einstellungen für *u.trust LAN Crypt für macOS* erfolgen über die Konfigurationsdatei config.plist, die nach der Installation erstellt werden muss. Eine Vorlage wird mitgeliefert und im Verzeichnis installiert:

```
/Library/Utimaco/u.trust LAN Crypt/useragent.app/Contents/Resources/
config.plist.template
```

Kopieren Sie zuerst die Vorlage an einen anderen Ort, bearbeiten Sie sie, und kopieren Sie sie anschließend an den unten angegebenen Ort:

```
~/Library/Application Support/de.utimaco.lancrypt/config.plist
```

Das Kopieren und Bearbeiten der Vorlage außerhalb des Anwendungsbundles bewahrt die Code-Signatur und stellt sicher, dass die Anwendung korrekt gestartet wird.

Zwingend erforderliche Einträge in der Konfigurationsdatei

PolicyPath: Mount-Point der Richtliniendatei

Tragen Sie im Abschnitt `<string>` den Pfad zu einer gemounteten Netzwerkfreigabe oder einem lokalen Speicherort ein, auf der die Richtliniendateien (.xml.bz2) der Benutzer gespeichert sind. Wenn die Dateien auf einer entfernten Freigabe gespeichert sind, muss der entsprechende Mount-Point zugänglich und aktiv sein, damit LAN Crypt die Policy-Datei abrufen kann.

Beispiel:

```
<key>PolicyPath<key> <string>/Volumes/polices</string>
```

oder

```
<key>PolicyPath<key> <string>\\server\share\policies</string>
```

oder

```
<key>PolicyPath<key> <string>smb://server/share/policies</string>
```

SOCertLocation: Mount-Point des öffentlichen Zertifikats des Security Officers

Tragen Sie im Abschnitt `<string>` den Pfad zu einer gemounteten Netzwerkfreigabe oder einem lokalen Speicherort ein, in der die öffentlichen Zertifikate (.cer) des Sicherheitsbeauftragten gespeichert sind. Wenn die Dateien auf einer entfernten Freigabe gespeichert sind, muss der entsprechende Mount-Point zugänglich und aktiv sein, damit LAN Crypt die Policy-Datei abrufen kann.

Beispiel:

```
<key>SOCertLocation</key> <string>/Volumes/certificates</string>
```

oder

```
<key>SOCertLocation</key> <string>\\server\share\certificates</string>
```

oder

```
<key>SOCertLocation</key> <string>smb://server/share/policies/certificates</string>
```

Optionale Einstellungen der Konfigurationsdatei

Darüber hinaus können Sie optional weitere Einstellungen in der Konfigurationsdatei vornehmen. Diese Einstellungen sind wichtig, wenn z. B. der Benutzer-Anmeldename auf macOS von dem Benutzernamen in der *u.trust LAN Crypt* Administration abweicht.

UserName: Login-Name des Benutzers

Wenn der Benutzername aus der Nutzerverwaltung und der lokale Benutzername nicht übereinstimmen, müssen Sie diese Option so konfigurieren, dass sie mit dem von der *u.trust LAN Crypt* Administration generierten Namen übereinstimmt. Nur wenn der Anmeldename und der Name der Richtliniendatei identisch sind, kann der Benutzer mit *u.trust LAN Crypt für macOS* arbeiten.

CertificatePath: Mount-Point der Schlüsseldatei (.p12) des Benutzers

Nach Angabe des Einhängepunkts für die Schlüsseldatei (.p12) des Benutzers versucht *u.trust LAN Crypt für macOS* automatisch, eine .p12-Schlüsseldatei in den Schlüsselbund des Benutzers zu importieren, wenn der private Schlüssel der Richtliniendatei nicht verfügbar ist.

Diese Datei muss entsprechend dem jeweiligen Benutzer-Login benannt werden:

[LOGIN_NAME].p12

Hinweis

- Wenn Benutzer mit einem Sicherheitstoken oder einer Smartcard angemeldet werden sollen, muss der gesamte Eintrag (`<key>CertificatePath</key>`) weggelassen werden.

DisableCertificateValidation: Zertifikatvalidierung deaktivieren

Festlegen, ob bei der Prüfung von Benutzerzertifikaten gefundene Fehler ignoriert werden sollen.

Beispiel:

```
<key>DisableCertificateValidation</key> <true/>
```

Diese Einstellung ist sinnvoll, wenn z.B.: die Gültigkeitsdauer eines Zertifikats abgelaufen ist und noch kein neues Zertifikat verfügbar ist. Um sicherzustellen, dass ein Benutzer weiterhin auf sein Verschlüsselungsprofil zugreifen kann, bietet die Option die Möglichkeit, die Überprüfung der Gültigkeitsdauer des Zertifikats zu deaktivieren. Sobald die neuen Zertifikate verfügbar sind, kann diese Einstellung wieder deaktiviert werden, indem der Parameter für diese Einstellung auf **false** geändert wird.

Hinweis

- Alternativ können Vertrauenseinstellungen auch in der Schlüsselbundverwaltung konfiguriert werden. Das Ignorieren von Fehlern, die bei der Zertifikatsprüfung auftreten, bedeutet jedoch immer eine Verringerung der Sicherheit.

AgentEnvironment: Liste von verwendeten Umgebungsvariablen

Wenn eine Richtlinie mit Schlüsselwörtern verwendet wird, die erst am Client aufgelöst werden sollen, kann ein Administrator dies tun, indem er sie in **AgentEnvironment** angibt

Beispiel:

```
<key>AgentEnvironment</key> <dict> <key>%Username2%</key> <string>steve</string>
<key>%directory1%</key> <string>finances</string> <key>%directory2%</key>
<string>management</string> </dict>
```

PolicyUpdateInterval: Policy Update-Intervall

Zeitintervall zwischen Prüfungen auf neue Richtlinien (Minuten). Wenn eine neue Richtlinie verfügbar ist, wird sie automatisch geladen und angewendet.

Beispiel:

```
<key>PolicyUpdateInterval<key> <integer>240</integer>
```

Zertifikate

Bevor Benutzer auf ihr Verschlüsselungsprofil zugreifen können, muss das entsprechende Zertifikat auf dem Mac verfügbar sein. Der Security Office verteilt diese Zertifikate an die Benutzer, zusammen mit dem entsprechenden Passwort oder PIN mit dem der Benutzer das Zertifikat entsperren kann. Es muss ein Pfad konfiguriert werden, in dem die *u.trust LAN Crypt* Administration die Benutzerzertifikate sowie das öffentliche Zertifikat (.cer) des Sicherheitsbeauftragten speichert (siehe Handbuch der *u.trust LAN Crypt* Administration, „Zentrale Einstellungen", „Verzeichnisse"). Aus diesem Pfad importieren die

Benutzer dann ihre **PKCS#12-Schlüsseldatei** (ihr Zertifikat) auf ihren Computer. Liegen die Zertifikate bei der ersten Anmeldung vor, läuft der gesamte Prozess bis zur PIN-Eingabe automatisch ohne jegliche Benutzerinteraktion ab.

Hinweis

- Wenn die Anmeldung bei *u.trust LAN Crypt* fehlschlägt, werden Fehler im Systemprotokoll protokolliert. Um nach *LAN Crypt* zu filtern, stellen Sie das Subsystem auf `de.utimaco.lancrypt`. Aktivieren Sie außerdem die Optionen „Include Info Messages" und „Include Debug Messages" in der Konsole. Alternativ können Sie diese Informationen auch live im Terminal mit folgendem Befehl ansehen: `log stream --level debug --predicate 'subsystem == "de.utimaco.lancrypt"`
- *u.trust LAN Crypt* verifiziert die Zertifikate des Benutzers und das öffentliche Zertifikat (.cer) des (Master-)Security Officers, der die Richtliniendatei erstellt hat.Bei diesem Verfahren wird die Authentizität und Vertrauenswürdigkeit eines Zertifikats überprüft, indem es zu einer vertrauenswürdigen Stammzertifizierungsstelle zurückverfolgt wird. Um Vertrauen in die Zertifikatskette aufzubauen, müssen die erforderlichen Zertifikate installiert und vom Betriebssystem als vertrauenswürdig erkannt werden.
- Enthält das Zertifikat einen „CRL Distribution Point" und es ist keine gültige CRL auf dem System vorhanden, vertraut *u.trust LAN Crypt für macOS* diesem Zertifikat zunächst nicht. Im Schlüsselbund des Benutzers kann der Benutzer die Vertrauenseinstellung ändern und diesem Zertifikat dann die Einstellung „Immer vertrauen" zuweisen.

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

Verschlüsselungsregeln mit den ihnen zugeordneten Schlüsseln aus den *u.trust LAN Crypt* Verschlüsselungsprofilen geben Benutzern Zugriff auf verschlüsselte Daten. Diese Regeln definieren genau, welche Dateien in welchen Verzeichnissen mit welchem Schlüssel verschlüsselt werden müssen. Es muss lediglich das Verschlüsselungsprofil eines Benutzers geladen werden und die Ver- und Entschlüsselung erfolgt im Hintergrund.

Hinweis

- Damit *u.trust LAN Crypt für macOS* die Zertifikate automatisch importieren kann, ist es wichtig, dass die Dateinamen der Zertifikate, die von der Admin-Konsole exportiert wurden, nicht verändert werden.

Anmeldung an u.trust LAN Crypt

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

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

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

Anmeldung mit Sicherheitstoken

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

Hinweis

- Wenn Benutzer mit einem Sicherheitstoken oder einer Chipkarte angemeldet werden sollen, dürfen Sie in der Konfigurationsdatei keinen Mount-Point zur Schlüsseldatei (.p12) des Benutzers eingeben.

Laden der Richtliniendatei

Standardverhalten von u.trust LAN Crypt

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

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

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

Aktualisierte Richtliniendatei manuell laden

Um die Richtlinie manuell neu zu laden, öffnen Sie die Client-Informations-Benutzeroberfläche und klicken Sie im Tools-Menü der Registerkarte **Über** auf **Tools** und dann **Regeln aktualisieren**.

Client Status-Information

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

Status

Zeigt allgemeine Informationen zum Programmstatus an. Neben Informationen zum aktiven Benutzer werden auch die Lebensdauer und das Aktualisierungsintervall der geladenen Richtlinie angezeigt.

Konten

Auf dieser Registerkarte werden Konten von Cloud-Speicheranbietern konfiguriert und die derzeit aktiven Konten angezeigt.

Regeln

Diese Registerkarte listet alle zugewiesenen Verschlüsselungsregeln auf.

Schlüssel

Diese Registerkarte listet alle Schlüssel auf, die dem Benutzer zur Verfügung stehen.

Über

Diese Registerkarte zeigt Informationen über das Produkt und ermöglicht dem Benutzer, die Aktualisierung der Richtlinie zu erzwingen oder Client-Protokolle für Support-Fälle zu sammeln.

Verschlüsselung für Cloud-Speicher-Dienste und Netzwerkfreigaben

Um einen Cloud-Speicher oder einen Netzwerkfreigabe zur Verschlüsselung hinzuzufügen, klicken Sie auf das u.trust LAN Crypt-Icon in der Statusleiste.

Wählen Sie die Art des Speichers aus, den Sie hinzufügen möchten (Cloud oder Netzwerk). OneDrive und Google Drive werden für die Cloud-Anbindung unterstützt. Nachdem Sie Ihren gewünschten Speicher hinzugefügt haben, wird ein entsprechender Eintrag/Ort in der Finder-Sidebar erstellt, in dem alle hinzugefügten Dateifreigaben gesammelt werden.

Hinweis

- Seit macOS 26 erfordert LAN Crypt eine explizite Zugriffserlaubnis für den Zugriff auf Netzwerkfreigaben. Beim ersten Hinzufügen einer Netzwerkfreigabe kann dieser Zugriff direkt über den angezeigten Systemdialog gewährt werden. Wird die Erlaubnis in diesem einmalig erscheinenden Dialog nicht erteilt, kann sie nachträglich über **Systemeinstellungen** → **Datenschutz & Sicherheit** → **Dateien & Ordner** vergeben werden.

Um einen Netzwerkspeicher wieder zu entfernen, klicken Sie erneut auf das Statusleistensymbol von u.trust LAN Crypt und wählen Sie das Auswerfen-Symbol neben der jeweiligen Netzwerk-Freigabe aus.

Die Option, eine Cloud-Speicher-Anbindung zu entfernen, befindet sich in den Einstellungen von *u.trust LAN Crypt für macOS* im Abschnitt **Accounts**.

Verwendung

Beim Durchsuchen der jeweiligen Ordnerstruktur im Finder erstellt das System datenlose Dateien für jedes Element, das auf dem Laufwerk des Benutzers gefunden wird. Diese datenlosen Dateien belegen keinen Speicherplatz auf dem Gerät und werden nur heruntergeladen, wenn der Benutzer aktiv eine Datei öffnet oder **Jetzt laden** im Kontextmenü verwendet. Heruntergeladene Dateien und geänderte Dateien, die erfolgreich zurück auf OneDrive/Google Drive synchronisiert wurden, können ebenfalls vom Gerät entfernt werden, um Speicherplatz freizugeben. Diese Aktion ist ebenfalls im Kontextmenü verfügbar.

Um eine Datei oder einen Ordner mit anderen zu teilen, bringt der die Option **Online anzeigen** im Kontextmenü den Benutzer mit dem Standardbrowser zu der Datei oder dem Ordner in die Online-Einsicht des jeweiligen Cloud-Speicher-Dienst. Der Nutzer kann hier nun z.B. die bekannte **Teilen**-Funktionalität nutzen.

Hinweis

- In der *u.trust LAN Crypt* Administration ist kein Schlüsselwort für OneDrive oder Google Drive vorhanden. Es werden nur relative Regeln unterstützt.
- Dateien, die einer Verschlüsselungsregel unterliegen, werden verschlüsselt, wenn ihr Inhalt in die Cloud hochgeladen wird.
- Wenn der Inhalt verschlüsselter Dateien heruntergeladen wird, wird er entschlüsselt, wenn der entsprechende Verschlüsselungsschlüssel verfügbar ist.
- Jede Datei in OneDrive/Google Drive hat einen Versionsverlauf. Das Hochladen einer verschlüsselten Version einer Datei entfernt nicht ihren Verlauf. Es ist daher möglich, eine unverschlüsselte Version wiederherzustellen.
- Die unterstützten Cloud-Speicher-Dienste und *u.trust LAN Crypt für macOS* können problemlos parallel arbeiten. *u.trust LAN Crypt für macOS* kann als Ersatz für die Clients von OneDrive und Google Drive verwendet werden.
- Verschlüsselungsfunktionen sind nur verfügbar, wenn über den *u.trust LAN Crypt*-Ort auf die Ordner zugegriffen wird.

Schnellaktion-Erweiterung aktivieren

u.trust LAN Crypt für macOS kommt mit einer Schnellaktion-Erweiterung für das schnelle Einsehen von dateispezifischen Verschlüsselungsinformationen. Vorerst muss diese Erweiterung jedoch innerhalb der Systemeinstellungen aktiviert werden.

Hierfür befolgen Sie einfach folgende Schritte:

1. Öffnen Sie die **Systemeinstellungen**.
2. Klicken Sie nun auf **Erweiterungen**.
3. Wählen Sie nun links den Reiter **Finder** und aktivieren Sie die Schnellaktion-Erweiterung **Verschlüsselungsinformationen**.

Um die Verschlüsselungsinformationen einer Datei einzusehen, können Sie diese nun mit einem Rechtsklick unter **Schnellaktionen** aufrufen. Wenn Dateien keiner Regel unterliegen und der Schlüssel verfügbar ist, lassen sie sich über den Dialog der Verschlüsselungsinformationen auch direkt entschlüsseln.

Installation

u.trust LAN Crypt für macOS installieren

u.trust LAN Crypt für macOS unterstützt folgende Versionen von macOS:

- **macOS 26 Tahoe**
- **macOS 15 Sequoia**

Öffnen Sie die Installationsdatei und folgen Sie den angegebenen Installationsschritten. Darüber hinaus sind keine weiteren Änderungen/Anpassungen in den Betriebssystemeinstellungen zu tätigen.

u.trust LAN Crypt für macOS deinstallieren

Klicken Sie im unten angegebenen Pfad auf **Uninstaller.pkg**.

```
/Library/Utimaco/u.trust LAN Crypt/Uninstaller.pkg
```

Hinweis

- FileVault muss für die Verwendung von u.trust LAN Crypt für macOS aktiviert sein.
- Nach der Deinstallation von u.trust LAN Crypt für macOS können auf dem Mac keine Dateien mehr ver- oder entschlüsselt werden. Die Deinstallation von u.trust LAN Crypt für macOS führt nicht zu einer Entschlüsselung von Dateien.

Funktionen von "lcutil"

Zusätzlich zu den Programmkomponenten wird eine Konsolenanwendung „lcutil" installiert. Dieses Tool kann bei der Lösung technischer Probleme hilfreich sein. Es wird im folgenden Verzeichnis installiert:

```
/Library/Utimaco/u.trust LAN Crypt/useragent.app/Contents/Resources
```

Damit stehen dem Benutzer erweiterte Funktionen von *u.trust LAN Crypt für macOS* zur Verfügung, die im Folgenden beschrieben werden.

Version von u.trust LAN Crypt für macOS anzeigen lassen

Um sich die Version von u.trust LAN Crypt für macOS anzeigen zu lassen, muss der Benutzer das Terminal öffnen und dort den folgenden Befehl ausführen:

```
/Library/Utimaco/u.trust LAN Crypt/useragent.app/Contents/Resources/lcutil version
```

Protokolldatei erstellen

Sie können alle Logs von *u.trust LAN Crypt für macOS* in eine Datei (.xz) exportieren. Bestimmte Ereignisse können so aufgezeichnet, ausgewertet, archiviert und jederzeit überprüft werden.

Um alle Logs von *u.trust LAN Crypt für macOS* in eine Datei zu exportieren, muss der Benutzer das Terminal öffnen und folgenden Befehl ausführen:

```
/Library/Utimaco/u.trust LAN Crypt/useragent.app/Contents/Resources/lcutil collect-logs
```

Folgende Logs und Systeminformationen werden in die Protokolldatei aufgenommen:

- System log
- Mount table
- Process table
- Version information
- System profiler
- Cached policies
- Config.plist
- Crashdumps
- Informationen über konfigurierte Cloud-Provider-Konten

Kompatibilität mit Cloud-Diensten

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

Nicht kompatible Microsoft-365-Dienste

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

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

* Copilot

Sicherheitslücken melden

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

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

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

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

(Schritt 1) Bereiten Sie Ihre Meldung vor

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

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

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

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

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

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

PSIRT-Kontakt

PSIRT-Team: PSIRT@Utimaco.com

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

PGP-Schlüssel: Herunterladen

Technische Unterstützung

Technischen Support zu Utimaco Produkten können Sie wie folgt abrufen:

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

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

Rechtlicher Hinweis

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

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

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

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

Zuletzt aktualisiert am 21.09.2026