# Was ist u.trust LAN Crypt für iOS / iPadOS?

*u.trust LAN Crypt für iOS / iPadOS* ermöglicht unter Windows / macOS mit transparenter Dateiverschlüsselung den Austausch vertraulicher Daten innerhalb von Berechtigungsgruppen in kleinen, mittleren und großen Organisationen. Zahlreiche Unternehmen und Organisationen der Wirtschaft sowie öffentlichen Verwaltung in Deutschland und weltweit setzen bereits auf Utimaco LAN Crypt.

Welche Dateien und Speicherorte durch Utimaco LAN Crypt geschützt werden sollen und welche Benutzer auf welche Daten zugreifen dürfen, legt ein Security Officer (SO) zentral durch eine oder mehrere Verschlüsselungsregeln fest. Jede einzelne Verschlüsselungsregel besteht aus einem Verschlüsselungspfad und einem Schlüssel sowie einem Verschlüsselungsalgorithmus. Die Utimaco LAN Crypt Richtliniendateien beinhalten sämtliche Verschlüsselungsregeln, die der Benutzer benötigt, um mit verschlüsselten Daten arbeiten zu können.

Damit der Benutzer seine Richtliniendatei verwenden kann, benötigt er ein Zertifikat, das ihm durch den Utimaco LAN Crypt Security Officer als Schlüsseldatei (.p12-Datei) zur Verfügung gestellt wird. Die Schlüsseldatei enthält das Zertifikat sowie den persönlichen Schlüssel des Benutzers. Der Zugriff auf diese Datei ist passwortgeschützt. Das dazugehörige Passwort erhält der Benutzer durch den Security Officer. Mit *u.trust LAN Crypt für iOS / iPadOS* können Sie auf verschlüsselte Utimaco LAN Crypt-Dateien zugreifen, die entweder lokal, d. h. auf dem Gerät selbst, auf einem Netzwerk-Laufwerk oder auf einem entfernten Speicher, zum Beispiel einem Cloud-Speicher, abgelegt sind. Ein Benutzer erhält so auf einfache Weise Zugriff auf die gleichen Utimaco LAN Crypt-Dateien, die ihm auch an seinem Arbeitsplatz-Rechner zur Verfügung stehen.

*u.trust LAN Crypt für iOS / iPadOS* ermöglicht es Benutzern, dass sie nunmehr auch mithilfe ihrer mobilen Geräte, wie iPhone oder iPad, mit ihren verschlüsselten Daten arbeiten können.

*u.trust LAN Crypt für iOS / iPadOS* bietet Ihnen zum einen die Möglichkeit, per se auf verschlüsselte Dateien zuzugreifen, diese zu öffnen, zu bearbeiten und verschlüsselt zu speichern und zum anderen die Erweiterung der gewohnten Utimaco LAN Crypt typischen Sicherheitsinfrastruktur, der Nutzung von Zertifikaten (.p12-Dateien) und der Richtliniendateien (.xml.bz2) für mobile Geräte.

## u.trust LAN Crypt 2Go

Mithilfe des neu integrierten u.trust LAN Crypt 2Go können Sie darüber hinaus Dateien auch passwortbasiert ver- und entschlüsseln. So können Sie auf einfache und sichere Weise Informationen mit anderen Personen austauschen, wie beispielsweise mit Ihren Geschäftspartnern oder auch mit externen Mitarbeitern.

## SafeGuard Enterprise: Migration der Dateiverschlüsselung

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

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

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

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

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

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

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

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

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

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

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

**Hinweis**

- Wenn Sie *SafeGuard Enterprise* installiert haben und eine Migration auf *u.trust LAN Crypt* planen, wenden Sie sich bitte an den u.trust LAN Crypt Support. Weitere Informationen finden Sie unter www.conpal.de/en/sgn-migration-en.

## Welche Versionen von iOS / iPadOS werden unterstützt?

*u.trust LAN Crypt für iOS / iPadOS* unterstützt iOS 16 / iPadOS 16 oder neuere Versionen.

*u.trust LAN Crypt für iOS / iPadOS* ist in den Sprachen Deutsch und Englisch verfügbar.

---

# Unterstützte Verschlüsselungs-Algorithmen

## Unterstützte Verschlüsselungsalgorithmen für Dateiverschlüsselung

*u.trust LAN Crypt für iOS / iPadOS* unterstützt folgende Verschlüsselungsalgorithmen:

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

## Unterstützte Verschlüsselungsalgorithmen für das Key-Wrapping

*u.trust LAN Crypt für iOS / iPadOS* unterstützt folgende Verschlüsselungsalgorithmen für das Key-Wrapping.

- AES-256
- AES-192
- AES-128
- Unterstützt, aber nicht empfohlen: 3DES, 3DES TWO KEY, DES, RC4

  **Hinweis**

  - Durch Key-Wrapping (Standardeinstellung) wird der Transportschlüssel der Security Officer-Daten und der Benutzerprofildaten mit einem per Zufallsverfahren erzeugten Session-Key mit dem ausgewählten Algorithmus verschlüsselt. Dieser Schlüssel wird dann wiederum mit dem öffentlichen Schlüssel aus dem Zertifikat RSA-verschlüsselt.
  - Bitte beachten Sie, dass im Vergleich zu u.trust LAN Crypt für Windows der Algorithmus "RC2" von *u.trust LAN Crypt für iOS / iPadOS* nicht unterstützt wird. Wenn das Key-Wrapping für Ihre Richtliniendatei auf den Algorithmus "RC2" eingestellt ist, kann die Richtliniendatei mit *u.trust LAN Crypt für iOS / iPadOS* nicht genutzt werden! In dem Fall müssen Sie die Einstellung für das Key-Wrapping ändern und hierfür einen der anderen Algorithmen (wie z. B. AES-128) wählen, die unterstützt werden.
  - Wenn Sie einen Sicherheitstoken verwenden, überprüfen Sie bitte, ob die verwendete Middleware den für das Key-Wrapping verwendeten Algorithmus unterstützt. In dem Fall muss der Security Officer entweder den Algorithmus für das Key-Wrapping entsprechend ändern und dann die Richtliniendatei neu erstellen bzw., wenn Sie einen aktuellen und sicheren Algorithmus verwenden wollen und Sie einen Sicherheitstoken nutzen, ggf. die von Ihnen verwendete Middleware entsprechend aktualisieren.

# Allgemeine Vorbereitungen und Konfiguration

Bitte aktivieren Sie aus Sicherheitsgründen vor der Verwendung dieser App immer einen Passcode für das Gerät. Sobald die App gestartet wird, prüft diese zunächst, ob auch ein Geräte-Passcode eingestellt ist. Wird dabei feststellt, dass das Gerät nicht geschützt ist, wird die Verwendung von *u.trust LAN Crypt für iOS / iPadOS* so lange blockiert, bis ein Geräte-Passcode festgelegt wurde. Verwenden Sie hierbei niemals ein leicht zu erratendes Passwort, wie z. B. "1234" oder "000000". Nur so stellen Sie sicher, dass unautorisierte Personen nicht an Ihre vertraulichen Daten gelangen können, wenn z. B. Ihr mobiles Gerät einmal verloren gehen oder es Ihnen gestohlen werden sollte. Grundsätzlich empfiehlt Utimaco bei längerer Nichtnutzung des Gerätes oder wenn Sie es gegen ein neues Gerät tauschen wollen, alle vorhandenen App-Daten von Utimaco LAN Crypt auf dem Apple-Gerät zu löschen (siehe Richtliniendatei löschen und Benutzerzertifikat löschen).

**Hinweis**

- Wird der Geräte-Passcode deaktiviert, wird auch das Passwort für das Benutzerzertifikat entfernt. Dieses muss dann nach dem Aktivieren des Sperrbildschirms neu eingegeben werden.

## Bereitstellen der Konfigurationsdaten

Nach dem Verlassen des Begrüßungsbildschirms von *u.trust LAN Crypt für iOS / iPadOS* werden Sie aufgefordert die Konfigurationsdaten anzugeben:

- Importieren Sie Ihre Richtliniendatei
- Importieren Sie Ihr Benutzerzertifikat

**Hinweis**

- Insofern die Verteilung Ihrer Konfigurationsdateien über SMB-Freigaben erfolgen soll, wird in den Einstellungen ein zusätzlicher Abschnitt Netzwerk angezeigt. Beachten Sie: Wenn Sie dort die SMB-Zugangsdaten löschen, werden in der Folge auch die Konfigurationsdateien gelöscht.

## Verwaltung von Schlüsseln

Sowohl verwaltete Schlüssel als auch passwortbasierte Schlüssel sind in den Einstellungen zu finden. Verwaltete Schlüssel stammen ausschließlich aus der jeweiligen Richtliniendatei, während passwortbasierte Schlüssel in den zugehörigen Einstellungen frei erstellt, umbenannt und gelöscht werden können. Das Umbenennen eines Schlüssels ändert nicht den generierten Schlüssel, der für die Verschlüsselung verwendet wird.

**Hinweis**

- Passwortbasierte Schlüssel können auch im Rahmen der Verschlüsselung einer Datei erstellt werden. Diese Schlüssel werden dann automatisch zur gespeicherten Liste der passwortbasierten Schlüssel hinzugefügt.
- Durch die erfolgreiche Entschlüsselung durch einen passwortbasierten Schlüssel wird der verwendete Schlüssel automatisch zur gespeicherten Liste der passwortbasierten Schlüssel hinzugefügt.
- Für die Generierung passwortbasierter Schlüssel genutzte Passwörter sind ebenfalls noch nach der Erstellung einsehbar.

# Richtlinien

## Was sind Utimaco LAN Crypt Richtliniendateien?

Ein Security Officer (SO) legt über die Administration von Utimaco LAN Crypt zentral fest, welche Dateien und Speicherorte durch Utimaco LAN Crypt durch Verschlüsselung geschützt werden sollen und auch, welche Benutzer jeweils auf welche dieser Daten Zugriff erhalten. Hierzu erstellt der Security Officer eine oder mehrere Verschlüsselungsregeln für den Benutzer. Jede einzelne Verschlüsselungsregel besteht aus einem Verschlüsselungspfad und einem Schlüssel sowie einem Verschlüsselungsalgorithmus. Die Utimaco LAN Crypt Richtliniendateien beinhalten sämtliche Verschlüsselungsregeln, die der Benutzer benötigt, um mit verschlüsselten Dateien arbeiten zu können. Damit der Benutzer die Richtliniendatei verwenden kann, benötigt er zudem ein Zertifikat, das ihm durch den Utimaco LAN Crypt Security Officer als Schlüsseldatei (.p12-Datei) zur Verfügung gestellt wird. Die Schlüsseldatei enthält das Zertifikat sowie den persönlichen Schlüssel des Benutzers. Der Zugriff auf diese Datei ist passwortgeschützt. Das dazugehörige Passwort erhält der Benutzer durch den Security Officer.

## Automatisierter Import mit LAN Crypt Cloud

Wenn der Security Officer (SO) die Administration über die LAN Crypt Cloud durchführt, werden Richtliniendateien und Benutzerzertifikate automatisch geladen. Dafür muss der Nutzer lediglich im Client mit dem entsprechenden LAN Crypt-Konto angemeldet sein. Die Anmeldefunktion kann über das Antippen des Profil-Icons oben rechts in der Anwendung erreicht werden.

## Manueller Import von Richtliniendateien

**ÖFFNEN** Sie die App *u.trust LAN Crypt für iOS / iPadOS* auf Ihrem Mobilgerät. Tippen Sie dann auf das **Zahnradsymbol** in der Mitte unten innerhalb der App, um die Einstellungsansicht aufzurufen. Tippen Sie dort auf die Auswahl **Importieren Sie Ihre Richtliniendatei** und wählen Sie hierüber dann den Speicherort, auf dem sich die Richtliniendatei befindet. Tippen Sie anschließend auf die Richtliniendatei, um sie in die Applikation zu importieren.

## Manueller Import von Benutzer-Zertifikaten

**ÖFFNEN** Sie die App *u.trust LAN Crypt für iOS / iPadOS* auf Ihrem Mobilgerät. Tippen Sie dann auf das **Zahnradsymbol** in der Mitte unten innerhalb der App, um die Einstellungsansicht aufzurufen. Tippen Sie dort auf die Auswahl **Importieren Sie Ihr Zertifikat** und wählen Sie dann den Speicherort, auf dem sich die Schlüsseldatei (.p12-Datei) befindet. Geben Sie dann in dem folgenden Dialog das Passwort ein, das Sie vom Security Officer für Ihr Zertifikat / Ihre Schlüsseldatei erhalten haben. Nachdem Sie das korrekte Passwort eingegeben haben, werden das Zertifikat und der zugehörige private Schlüssel im Zertifikatsspeicher der Applikation gespeichert.

**Hinweis**

- *u.trust LAN Crypt für iOS / iPadOS* unterstützt auch die Angabe von mehreren Zertifikaten des Benutzers in der Richtliniendatei. Um die Richtliniendatei verwenden zu können, muss der Benutzer mindestens im Besitz eines dieser Zertifikate sein. Mit dem öffentlichen Schlüssel seines Zertifikats ist die Richtliniendatei verschlüsselt. Um mit der Richtliniendatei arbeiten zu können, muss er daher eines dieser Zertifikate importiert haben.

## Zertifikatsinformationen

Öffnen Sie die App *u.trust LAN Crypt für iOS / iPadOS* auf Ihrem Mobilgerät. Tippen Sie auf das **Benutzer-Icon** im LAN Crypt Verlauf (Datei-Browser), um innerhalb der App die Einstellungen aufzurufen. Tippen Sie dort auf die Auswahl **Benutzerzertifikat**. Im nächsten Dialog werden Ihnen zu diesem Zertifikat auch der Inhaber und die Seriennummer angezeigt. Sollte das Zertifikat nicht vertrauenswürdig sein, wird auch dies an dieser Stelle angezeigt.

# Richtliniendateien und Zertifikate mithilfe von MDM ausrollen

Wenn Sie ein Mobile Device Management (MDM) verwenden, können Sie damit neben der App selbst auch die individuelle Konfiguration (d. h. Richtliniendatei und Zertifikat) für die mobilen Geräte der Benutzer bereitstellen. Insofern Ihnen keine MDM-Lösung zur Verfügung stehen sollte, müssen diese Daten wie zuvor beschrieben manuell durch den Benutzer selbst installiert bzw. von diesem die individuelle Konfiguration (Richtliniendatei und Zertifikat) geladen bzw. importiert werden.

## Einstellungen

Die Konfigurationsdaten bestehen aus einer Liste, die Schlüssel und Zeichenfolgen beinhaltet. Die Dateien müssen als Base64-kodierte Zeichenkette über eine URL bereitgestellt werden. die auf einem HTTPS oder SMB-Server gehostet wird. Die folgenden Konfigurationsschlüssel werden von LAN Crypt angeboten:

**Betriebsmodus**

*operation_mode*: Kann verwendet werden, um die Konfigurationsoptionen der App einzuschränken **(STRING)**.

- Mögliche Werte:
  - `"cloud"`: Nur die LAN-Crypt Cloud Administration kann verwendet werden.
  - `"classic"`: Nur die LAN Crypt On-Premise Administration (Nutzung von Richtliniendateien) kann verwendet werden.
  - Kein Wert: Cloud- oder On-Premise Administration sind möglich.

**Hinweis**

- Wenn *operation_mode* nicht gesetzt ist oder einen ungültigen Wert hat und eine der MDM-Einstellungen gesetzt ist (*policy_url*, *policy_blob*, *usercert_url*, *usercert_blob*, *admcert_url*, *admcert_blob*), wird `"classic"` von der App erzwungen.

**Schlüssel für die Richtliniendatei**

*policy_blob:* Richtliniendatei im Format XML oder XML.bz2 (komprimiert) als Base64-kodierte Zeichenfolge **(STRING)**.

*policy_url:* URL zu einer Richtliniendatei im Format XML oder XML.bz2 **(STRING)**.

**Schlüssel für das Benutzerzertifikat / P12-Datei**

*usercert_blob:* PKCS-12-Zertifikatsdatei als Base64-kodierte Zeichenfolge **(STRING)**.

*usercert_url:* URL zu einer PKCS-12-Zertifikatsdatei **(STRING)**.

**Schlüssel für Security Officer-Zertifikate**

*admcert_blob:* Security Officer-Zertificat ("cer"-Datei / DER-kodiert) als Base64-kodierte Zeichenfolge **(STRING)**.

*admcert_url:* URL zu einem Security Officer-Zertifikat ("cer"-Datei / DER-kodiert) **(STRING)**.

**Standardschlüssel**

*default_key_guid:* GUID des Standardschlüssels, der für die Verschlüsselung neuer Dateien verwendet werden muss **(STRING)**.

**Hinweis**

- Ist ein Standardschlüssel gesetzt, so kann der Benutzer ausschließlich diesen Schlüssel zur Verschlüsslung nutzen. Die Verschlüsselung durch einen passwortbasierten Schlüssel ist jedoch trotzdem jederzeit möglich. Diese führt dann zu einer verschlüsselten Kopie der Originaldatei.

**Schlüssel für Samba-Anmeldedaten**

*smb_username:* Verweist eine der Einstellungen für die Richtliniendatei oder für das Zertifikat auf einen SMB-Speicherort kann hier der Benutzername für die SMB-Verbindung über diesen Schlüssel konfiguriert werden **(STRING)**.

**Hinweis**

- Wird kein Wert für diesen Schlüssel definiert, wird der Benutzer aufgefordert neben seinem Passwort auch seinen Benutzernamen für die SMB-Verbindung einzugeben. Aus Sicherheitsgründen muss die Eingabe des Passwortes für die SMB-Verbindung immer durch den Benutzer erfolgen.

**Schlüssel für Zertifikatsüberprüfung**

*cert_validation:* Aktiviert die Zertifikatsüberprüfung **(BOOLEAN)**.

**Hinweis**

- Eine Zertifikatsüberprüfung erfolgt nicht, wenn diese Einstellung fehlt.

## Regeln

- Vordefinierte Einstellungen können durch den Benutzer nicht geändert oder außer Kraft gesetzt werden.
- URLs müssen auf HTTPS-Servern mit einem gültigen SSL-Zertifikat gehostet werden. Sie können dies überprüfen, indem Sie die URL in einem Browser (z. B. Chrome, Safari) auf dem mobilen Gerät eingeben. Wenn die Datei angezeigt werden kann, wird auch die URL als Konfigurationswert funktionieren.
- Wenn sowohl BLOB als auch URL für eine Einstellung unterstützt werden, hat der BLOB Vorrang.
- Wenn der Daten-BLOB oder die URL einer Einstellung ungültig ist, wird eine Fehlermeldung angezeigt.
- Bei der Verwendung von URLs für SMB-Freigaben werden Benutzernamen und Passwörter ignoriert (verwenden Sie stattdessen smb_username)(`smb://localfileserver/certificates/sepp.p12`)
- Format der Eingabe: `smb://<Host>/<Freigabe>/<Ordner>/<Dateiname>`
- Es bestehen zwar grundsätzlich keine Einschränkungen bezüglich der Länge von Zeichenfolgen, die Konfigurationsdatei sollte aber dennoch nicht größer als ein paar Kilobyte sein.

**WARNHINWEIS zu Intune und Base64-kodierten Zeichenfolgen für iOS-Konfigurationsdateien:**

- Wenn Sie Microsoft Intune verwenden und Base64-kodierte Zeichenfolgen bereitstellen: Verwenden Sie unbedingt das XML-Konfigurationsdateiformat, da Zeichenfolgen andernfalls von Intune ohne Warnung abgeschnitten und dadurch unvollständige Daten an das mobile Gerät übertragen werden.

---

# Richtliniendatei und Benutzerzertifikat löschen

**Richtliniendatei löschen**

Öffnen Sie die App *u.trust LAN Crypt für iOS / iPadOS* auf Ihrem iPhone oder iPad. Tippen Sie dann oben rechts auf das **Benutzer-Icon** im LAN Crypt Verlauf (Datei-Browser) innerhalb der App, um die Einstellungen aufzurufen. Tippen Sie dort rechts neben der Richtliniendatei auf den Papierkorb. Tippen Sie dann auf **Löschen**, wenn Sie Ihre Richtliniendatei wirklich löschen wollen. Tippen Sie auf **Abbrechen**, wenn Sie den Vorgang nicht fortsetzen und Ihre Richtliniendatei behalten wollen.

**Benutzerzertifikat löschen**

Öffnen Sie die App *u.trust LAN Crypt für iOS / iPadOS* auf Ihrem iPhone oder iPad. Tippen Sie dann oben rechts auf das **Benutzer-Icon** im LAN Crypt Verlauf (Datei-Browser) innerhalb der App, um die Einstellungen aufzurufen. Tippen Sie dort rechts neben dem Benutzerzertifikat auf den Papierkorb. Tippen Sie dann auf **Löschen**, wenn Sie Ihr Benutzerzertifikat wirklich löschen wollen. Tippen Sie auf **Abbrechen**, wenn Sie den Vorgang nicht fortsetzen und Ihr Benutzerzertifikat nicht löschen wollen.

---

# Dateien öffnen, bearbeiten, verschlüsseln, entschlüsseln und freigeben

Mit *u.trust LAN Crypt für iOS / iPadOS* wird der Zugriff auf Dateien ermöglicht, die auf dem Gerät selbst gespeichert sind (lokaler Speicher). Der Zugriff auf entfernte Speichersysteme (z. B. auf OneDrive oder Google Drive) über den Datei-Browser ist durch die iOS-Sandbox-Sicherheit auf sehr sichere Weise geschützt. Die iOS-Sandbox-Sicherheit bietet Datei-Browsern, welche von installierten Apps auf dem Apple-Gerät zur Verfügung gestellt werden, einen geschützten Fernzugriff. So kann ein Benutzer beispielsweise über die *u.trust LAN Crypt für iOS / iPadOS*-App auf Dateien zugreifen, die auf OneDrive gespeichert sind, wenn die OneDrive-App auf seinem Gerät installiert ist. Diese ermöglicht den Remote-Zugriff zu nutzen, der von anderen auf demselben Gerät installierten Apps bereitgestellt wird. So kann beispielsweise die Utimaco LAN Crypt-App auf die Daten des Benutzers in OneDrive zugreifen, wenn die OneDrive-App installiert ist. In ähnlicher Weise erfolgt dann auch der Zugriff auf Google Drive, wenn die dazugehörige App auf dem mobilen Gerät installiert ist.

## Wie erfolgt der Zugriff auf verschlüsselte Dateien?

Mit dem iPhone oder iPad kann auf unterschiedliche Weise auf Dateien zugegriffen werden. Dies kann innerhalb der Utimaco LAN Crypt für íOS-App über den Datei-Browser oder von dort aus über eine proprietäre App für Cloud-Speicher (wie z. B. OneDrive) bzw. auch über eine andere App erfolgen. Mit *u.trust LAN Crypt für iOS / iPadOS* können Benutzer unverschlüsselte und verschlüsselte Dateien öffnen, diese bearbeiten und danach speichern. War die Datei zuvor verschlüsselt, bleibt diese auch nach dem Bearbeiten weiterhin verschlüsselt. Sie können zum Bearbeiten von Dateien auch ihre bevorzugte App verwenden. So kann beispielsweise Microsoft Office zum Bearbeiten von Dokumenten, Präsentationen oder Tabellenkalkulationen verwendet werden. Die Dateivorschau verfügt über eine Bearbeiten-Schaltfläche. Hierüber lässt sich eine Datei dann auch mit einer Drittanbieter-App öffnen bzw. bearbeiten.

## Verschlüsselte Datei öffnen

Um eine verschlüsselte Datei zu öffnen, wählen Sie über den integrierten Datei-Browser innerhalb der *u.trust LAN Crypt für iOS / iPadOS*-App einen Speicherort aus und tippen Sie dort auf die verschlüsselte Datei, die Sie öffnen möchten. Danach wird diese Datei direkt über den integrierten Viewer der Utimaco LAN Crypt-App auf Ihrem iPhone oder iPad geöffnet und entschlüsselt angezeigt. Hierzu bedient sich *u.trust LAN Crypt für iOS / iPadOS* des Quick-Look-Frameworks von Apple. Alle Dateien verbleiben beim Anzeigen immer in der Sandbox der Utimaco LAN Crypt-App und sind damit immer optimal geschützt. Auf dem Speicherort selbst bleibt diese Datei jedoch weiterhin verschlüsselt. Alle Ver- und Entschlüsselungsvorgänge ereignen sich nur auf dem mobilen Apple-Gerät selbst.

> **Das QuickLook Framework für iOS / iPadOS bietet für die Bearbeitung bestimmter Dateitypen nur eine eingeschränkte Funktionsunterstützung:**
>
> - ***PDF- und Bilddateien:*** Unterstützung für Markup-Funktion. Tippen Sie beim Anzeigen der Datei auf das Stift-Symbol in der Navigationsleiste.
> - ***Videodateien:*** Unterstützung für die Funktionen Drehen und Zuschneiden. Tippen Sie, während Sie sich die Videodatei anzeigen lassen, auf die Schaltfläche Drehen oder Zuschneiden in der Navigationsleiste. Durch Tippen auf die Schaltfläche Fertig werden die Änderungen in der Datei gespeichert.

## Dateien über Apps von Drittanbietern bearbeiten

1. Tippen Sie in der Dateivorschau auf die Schaltfläche **Bearbeiten**.
2. Die Dateivorschau wird geschlossen und der iOS-Freigabebildschirm wird angezeigt. Wählen Sie dort die von Ihnen gewünschte Anwendung (wie z. B. Microsoft Word) aus.
3. Die gewählte Anwendung wird geöffnet und zeigt die Datei an. Sie können die Datei wie von Ihnen gewohnt bearbeiten.
4. Sobald durch die Anwendung Änderungen an der Datei erfolgen, stellt u.trust LAN Crypt für iOS / iPadOS sicher, dass eine verschlüsselte Datei auf dem entsprechenden Speicherort gespeichert wird und weiterhin verschlüsselt bleibt (z. B., wenn sich diese in einer Cloud befindet).

## Verschlüsselungsinformationen anzeigen lassen

Über ein Symbol in der rechten oberen Ecke der Miniaturansicht wird der jeweilige Status der Datei angezeigt:

- **grüner Schlüssel:** Die Datei ist verschlüsselt und sie kann von Ihnen geöffnet werden.
- **grauer Schlüssel:** Die Datei ist unverschlüsselt und sie kann von Ihnen geöffnet werden.
- **roter Schlüssel:** Die Datei ist verschlüsselt und kann nicht geöffnet werden (der Schlüssel ist entweder nicht verfügbar oder der verwendete Verschlüsselungsalgorithmus wird für mobile Geräte nicht unterstützt).

Um weitere Informationen zu erhalten, drücken Sie etwas länger auf eine Datei. Es öffnet sich ein Kontextmenü, über welches Sie nun die Auswahl **Verschlüsselungsinfos** treffen können. Im Abschnitt **Verschlüsselungsinfos** werden nun detaillierte Informationen angezeigt:

- **Verschlüsselungsstatus:** Zeigt an, ob die Datei verschlüsselt ist oder nicht.
- **Schlüsselname:** Zeigt den Namen des Schlüssels an, mit dem die Datei verschlüsselt ist (wird nur bei verschlüsselten Dateien angezeigt).
- **Schlüssel-ID:** Zeigt die GUID des Schlüssels an, mit dem die Datei verschlüsselt ist (wird nur bei verschlüsselten Dateien angezeigt).
- **Schlüssel verfügbar:** Zeigt an, ob der Schlüssel in der Richtliniendatei vorhanden ist (wird nur bei verschlüsselten Dateien angezeigt).
- **Auf Mobilgeräten unterstützt:** Zeigt an, ob der verwendete Verschlüsselungsalgorithmus vom mobilen Gerät unterstützt wird (wird nur bei verschlüsselten Dateien angezeigt, bei welchem das Verschlüsselungsverfahren nicht unterstützt wird).

## Datei mit einem Schlüssel aus der Richtliniendatei verschlüsseln

Um eine Datei zu verschlüsseln, wählen Sie über den integrierten Datei-Browser innerhalb der *u.trust LAN Crypt für iOS / iPadOS*-App einen Speicherort aus und tippen Sie dort etwas länger auf die Datei, die Sie verschlüsseln möchten. Danach wird Ihnen das Kontextmenü angezeigt. Tippen Sie dort dann auf die Option **Verschlüsseln**. Im nächsten Dialog können Sie entscheiden, mit welcher Methode Sie die Datei verschlüsseln wollen. Im mittleren Teil des Dialogs werden Ihre verfügbaren Schlüssel angezeigt. Wenn ein Standardschlüssel für Sie eingerichtet wurde, ist dieser dort markiert. Wählen Sie den Schlüssel aus, den Sie zum Verschlüsseln der Datei verwenden möchten. Tippen Sie dann auf **Fertig** in der oberen rechten Ecke. Die Datei wird mit dem zuvor ausgewählten Schlüssel verschlüsselt.

**Hinweis**

- Wenn kein Standardverschlüsselungsschlüssel für Sie eingerichtet wurde, können Sie den Verschlüsselungsschlüssel in der Liste ändern, indem Sie auf einen anderen verfügbaren Schlüssel tippen. In diesem Fall wird die Datei mit diesem Schlüssel anstelle des zuvor ausgewählten Schlüssels verschlüsselt.

- Im Gegensatz zur Verschlüsselung mit einem passwortbasierten Schlüssel wird die Datei bei der Verschlüsselung mit einem Schlüssel aus der Richtliniendatei an Ort und Stelle verschlüsselt, sodass die Datei ohne den verwendeten Schlüssel nicht gelesen werden kann.

## Datei mit einem Passwort verschlüsseln und teilen (u.trust LAN Crypt 2Go)

Wenn Sie die Datei stattdessen mit einem Passwort verschlüsseln möchten, tippen Sie auf den Schieberegler Datei passwortgeschützt teilen, sodass dieser grün markiert ist. Nun können Sie entweder ein zuvor verwendetes Passwort auswählen oder ein neues Passwort für die Verschlüsselung erstellen. Wenn Sie auf diese Weise ein neues Kennwort erstellen, wird es automatisch auf dem Gerät gespeichert und kann zum weiteren Ver- und Entschlüsseln von Dateien verwendet werden. Passwortbasierte Schlüssel können auch im Einstellungsmenü gefunden und bearbeitet werden. Wählen Sie im nächsten Dialog die von Ihnen gewünschte App, über die Sie die Datei verschlüsselt teilen möchten oder tippen Sie alternativ auf **In Dateien sichern**, wenn Sie die Datei beispielsweise in einen Ordner in der iCloud verschlüsselt speichern möchten.

**Hinweis**

- Die Verschlüsselung erfordert immer ein sicheres Passwort! Dieses muss aus mindestens 8 Zeichen bestehen sowie Groß- und Kleinschreibung, Ziffern und

Sonderzeichen beinhalten. Das für den Schlüssel genutzte Passwort kann im Nachhinein noch in den Einstellungen eingesehen werden.

- Der Name des Verschlüsselungspassworts hat keinen Einfluss auf den für die Verschlüsselung verwendeten Schlüssel. Der eigentliche Schlüsselwert für die Verschlüsselung wird separat erzeugt.
- Anders als bei der Verschlüsselung an Ort und Stelle mit einem Schlüssel aus der Richtliniendatei wird bei der Verschlüsselung mit einem kennwortbasierten Schlüssel die Originaldatei nicht manipuliert, sondern eine verschlüsselte Kopie der Datei erstellt, die dann geteilt oder abgespeichert werden kann.

## Datei entschlüsseln und teilen

Um eine Datei zu entschlüsseln, navigieren Sie zunächst zu dem Ort, an dem die verschlüsselte Datei gespeichert ist, indem Sie den integrierten Dateibrowser in der *u.trust LAN Crypt für iOS / iPadOS*-App verwenden. Drücken Sie lange auf die Datei, die Sie entschlüsseln möchten. Das Kontextmenü erscheint. Tippen Sie dann dort auf die Option **Entschlüsseln**.

Handelt es sich bei der Datei um eine passwortgeschützte Datei, kann an dieser Stelle ein zusätzlicher Dialog angezeigt werden. Geben Sie in diesem Fall das erforderliche Kennwort in das Feld Kennwort eingeben ein.

Wählen Sie im nächsten Dialog die App aus, mit der Sie die entschlüsselte Datei teilen möchten, oder tippen Sie alternativ auf In Dateien speichern, wenn Sie die entschlüsselte Datei an einem anderen Ort speichern möchten. Tippen Sie anschließend in der oberen rechten Ecke auf **Speichern**. Die Datei wird entschlüsselt geteilt oder entschlüsselt an dem zuvor ausgewählten Ort gespeichert.

**Hinweis**

- Wenn Sie denselben Speicherort wählen, werden Sie in einem weiteren Dialog gefragt, ob Sie die vorhandene Datei ersetzen möchten.
- Bei erfolgreicher Entschlüsselung einer Datei mit einem passwortbasierten Schlüssel wird der verwendete Schlüssel automatisch zur gespeicherten Liste der passwortbasierten Schlüssel hinzugefügt. Die Liste der passwortbasierten Schlüssel kann in den Einstellungen gefunden und bearbeitet werden. Ebenfalls kann dort das für den passwortbasierten Schlüssel genutzte Passwort eingesehen werden.

# Protokollfunktion

*u.trust LAN Crypt für iOS / iPadOS* verfügt über eine ausführliche Protokollierung. Diese dient ausschließlich zur Fehleranalyse und sollte daher von Ihnen nur dann aktiviert werden, wenn mit dieser App Fehler oder Probleme auftreten sollten.

## Erweiterte Protokollierung

Wenn Sie die Erweiterte Protokollierung ausführen wollen, öffnen Sie die App *u.trust LAN Crypt für iOS / iPadOS* auf Ihrem iPhone oder iPad. Tippen Sie dann oben rechts auf das **Benutzer-Icon** im LAN Crypt Verlauf (Datei-Browser) innerhalb der App, um die Einstellungen aufzurufen. Tippen Sie dort dann auf den Schieberegler **Erweiterte Protokollierung**. Die Protokollfunktion wird dann als aktiviert (grün) angezeigt. Führen Sie dann alle Schritte aus, die zu einem Fehler geführt haben.

**Hinweis**

- Die Logdateien speichern keine sensiblen Informationen ab!

## Protokolldateien senden

Mithilfe der Funktion Protokolldateien senden können Sie diese Protokollinformationen zu Analysezwecken dann an den Utimaco-Support als E-Mail versenden. Tippen Sie hierfür auf das Symbol **Teilen**, das rechts neben Protokolldateien senden angezeigt wird. Wählen Sie dann die App, die Sie für Ihre E-Mail-Kommunikation nutzen. Die Protokolldatei wird der E-Mail dann automatisch als komprimierte Datei (.zip) angehängt. Deaktivieren Sie die Funktion **Erweiterte Protokollierung**, indem Sie erneut auf den Schieberegler tippen. Die Erweiterte Protokollierung wird dann wieder als deaktiviert (grau) angezeigt.

**Hinweis**

- Sie können sich den Inhalt der Protokolldatei auch anzeigen lassen, wenn Sie anstelle der App, die Sie für Ihre E-Mail-Kommunikation nutzen, weiter unten auf das Schlüsselsymbol tippen, das rechts neben In Utimaco LAN Crypt anzeigen angezeigt wird. Ebenso können Sie die Protokolldatei in diesem Dialog auch Kopieren oder diese über In Dateien sichern auf einem beliebigen Speicherort sichern.s

# 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**