Was ist u.trust LAN Crypt 2Go?

u.trust LAN Crypt 2Go ermöglicht den sicheren Austausch vertraulicher Daten durch passwortgeschützte Verschlüsselung. Dateien können einfach und sicher mit AES-256 XTS verschlüsselt werden, entweder on demand über die *u.trust LAN Crypt 2Go* App oder transparent über das Outlook für Windows Add-In für per E-Mail geteilte Anhänge. Eine Version für Webhosting ist ebenfalls verfügbar. Sie ermöglicht die Verschlüsselung und Entschlüsselung auf Systemen, auf denen *u.trust LAN Crypt 2Go* nicht installiert ist oder nicht installiert werden kann. Das für die Verschlüsselung zu verwendende Passwort kann der Benutzer individuell auswählen. Passwörter müssen einen vordefinierten Satz von Anforderungen und Komplexität erfüllen, um ein Mindestmaß an Sicherheit zu gewährleisten. Erzwungene Anforderungen für ein Passwort sind die Mindestlänge, Groß- und Kleinschreibung sowie eine Mischung aus alphanumerischen Zeichen und Sonderzeichen.

Personen, die das zur Verschlüsselung verwendete geheime Passwort nicht kennen, haben keinen Zugriff auf die in der Datei enthaltenen Informationen. Sie sehen beim Öffnen einer mit *u.trust LAN Crypt 2Go* geschützten Datei nur deren verschlüsselten Inhalt.

u.trust LAN Crypt 2Go ist eine Ergänzung zu den *LAN Crypt* Clients für Windows und macOS. Es ermöglicht den scicheren Austausch vertraulicher Daten mit anderen Personen oder externen Partnern, die *LAN Crypt* noch nicht nutzen. Neben Windows und macOS ist es auch unter Linux (Ubuntu, Debian) verfügbar. Auf mobilen Endgeräten wie Android und iOS/iPadOS ist die Funktionalität Bestandteil der *LAN Crypt* für Mobile App.

u.trust LAN Crypt 2Go ist in deutscher und englischer Sprache verfügbar.

Anwendungsbeispiel

Stellen Sie sich vor, Sie möchten einer externen Marketingagentur eine Excel-Datei mit vertraulichen Finanzdaten zur Verfügung stellen, mit denen die Agentur einen trendigen Finanzbericht mit attraktiven Grafiken erstellen soll. *LAN Crypt* nutzt die Marketingagentur allerdings noch nicht.

So können Sie die Datei sicher mit Ihrer Marketingagentur teilen:

1. Verschlüsseln Sie die Datei (z. B. „Finanzbericht.xlsx“) mit *u.trust LAN Crypt 2Go*. Hierfür können Sie einen neuen Schlüssel erstellen oder einen bereits bestehenden Schlüssel verwenden.
2. Senden Sie die verschlüsselte Datei („Finanzbericht.xlsx.pcrypt“) an Ihre Marketingagentur, z.B. über E-Mail.
3. Teilen Sie Ihrem Ansprechpartner bei der Marketingagentur das Passwort mit, mit dem die Datei entschlüsselt werden kann, z.B. während eines Telefongesprächs.
4. Die Marketingagentur kann die verschlüsselte Datei auf der Webseite von *u.trust LAN Crypt 2Go* entschlüsseln, ohne zuvor eine Software installieren zu müssen. Alternativ kann die Marketingagentur *u.trust LAN Crypt 2Go Reader* nutzen um die Datei lokal zu entschlüsseln (nur Windows).

   Hinweis

   - *u.trust LAN Crypt 2Go* ist kompatibel mit *LAN Crypt*. Daher können Sie Dateien auch in Ordnern ver- und entschlüsseln, für die eine Verschlüsselungsrichtlinie von *LAN Crypt* gilt. **Dateien bleiben jederzeit verschlüsselt!**

Installation und Upgrade

u.trust LAN Crypt 2Go ist auf folgenden Plattformen verfügbar:

- **Windows** 10 oder höher (x64)
- **macOS** 12 oder höher (Intel, Apple Silicon)
- **Debian** 11 oder höher
- **Ubuntu** 20.04 oder höher

Folgende Installationspakete sind für die einzelnen Plattformen verfügbar:

- **lc2go.msi** - Windows (x64)
- **lc2go.dmg** - macOS (Intel, Apple Silicon)
- **lc2go.deb** - Debian, Ubuntu (AMD64)

  Hinweis

  - Eine webbasierte Version von *u.trust LAN Crypt 2Go* wird auf der Utimaco Homepage gehostet. Diese Version erfordert keine Installation von Software und kann von jedem verwendet werden, der Dateien verschlüsseln oder entschlüsseln möchte.

Windows-spezifische Installation

Die Windows-Version des Produkts weist einige Besonderheiten auf, die sich von anderen Plattformen unterscheiden. Erstens unterstützt sie zwei verschiedene Installationsmodi: Aktueller Benutzer und alle Benutzer. Zweitens enthält sie ein Add-In für Microsoft Outlook (32-Bit und 64-Bit), das nur auf der Windows-Plattform verfügbar ist.

Installations-Option: Alle Benutzer

Die Installation von *u.trust LAN Crypt 2Go* erfordert standardmäßig keine Administratorrechte und kann von jedem Benutzer ausgeführt werden. Wenn die Installation von einem Benutzer durchgeführt wird, wird die Anwendung so installiert, dass sie ausschließlich diesem Benutzer zur Verfügung steht. Andere Benutzerkonten auf demselben System haben keinen Zugriff auf das installierte Produkt.

Die administrative Installation von *u.trust LAN Crypt 2Go* macht das Produkt für alle Benutzer verfügbar. Dazu müssen Sie das Setup im erweiterten Modus ausführen und den Parameter MSIINSTALLPERUSER überschreiben.

Führen Sie den folgenden Befehl von einem Windows-Terminal mit erhöhten Rechten aus:

```
msiexec /i lc2go.msi MSIINSTALLPERUSER=""
```

Dadurch wird das Produkt für alle Benutzer auf dem System installiert.

Installations-Option: Microsoft Outlook Add-In

u.trust LAN Crypt 2Go bietet modulare Installationsoptionen, die es Kunden ermöglichen, Installationen an ihre spezifischen Bedürfnisse anzupassen. Über den Parameter **ADDLOCAL** können die zu installierenden Features ausgewählt werden.

Führen Sie den folgenden Befehl von einem Windows-Terminal mit erhöhten Rechten aus:

```
msiexec /i lc2go.msi ADDLOCAL=ALL REMOVE=outlook_addin_feature
```

Dadurch wird das Produkt selbst installiert, aber die Installation des Add-Ins für Microsoft Outlook wird ausgelassen.

u.trust LAN Crypt 2Go deinstallieren

u.trust LAN Crypt 2Go kann jederzeit von einem System entfernt werden. Die Deinstallation folgt den standardmäßigen Verfahren zum Entfernen von Software für jede Plattform.

Hinweis

- Nach der Deinstallation von *u.trust LAN Crypt 2Go* können passwortgeschützt verschlüsselte Dateien auf dem Rechner nicht mehr entschlüsselt werden. Durch die Deinstallation von *u.trust LAN Crypt 2Go* wird *LAN Crypt* nicht deinstalliert.

u.trust LAN Crypt Cloud Support

Die Nutzung der u.trust LAN Crypt Cloud ermöglicht es Benutzern, ihre Schlüssel sicher in der Cloud zu speichern. Dies geschieht automatisch und stellt den Zugriff auf den Schlüsselbund von allen Geräten des Benutzers bereit, auf allen Plattformen, die von *u.trust LAN Crypt 2Go* unterstützt werden.

Änderungen am Schlüsselbund, sei es das Hinzufügen, Löschen oder Umbenennen eines Schlüssels, werden automatisch mit den anderen Geräten synchronisiert. Dies stellt sicher, dass der Benutzer stets Zugriff auf die aktuellsten Schlüssel hat, unabhängig davon, auf welchem Gerät er arbeitet.

An- und Abmeldung

Um sich anzumelden, tippen Sie auf das **Kontosymbol** in der oberen rechten Ecke der *u.trust LAN Crypt 2Go* Anwendung und wählen Sie **Anmelden**:

Sollten Sie passwortbasierte Schlüssel im Schlüsselbund haben, wird der Benutzer um die Erlaubnis zum Hochladen der Schlüssel in die u.trust LAN Crypt Cloud gebeten. Die Erlaubnis, bestehende Schlüssel hochzuladen, ist zwingend notwendig. Wenn ein Benutzer nicht möchte, dass bestehende Schlüssel hochgeladen werden, müssen die Schlüssel vor der Anmeldung an die u.trust LAN Crypt Cloud gelöscht werden. Beachten Sie, dass Passwörter für passwortbasierte Schlüssel nicht zur u.trust LAN Crypt Cloud hochgeladen werden, daher ist die Option **Passwort anzeigen** für Schlüssel, die in der u.trust LAN Crypt Cloud gespeichert sind, nicht verfügbar.

Nach dem Klicken auf **Anmelden** öffnet sich der Standardbrowser des Benutzers, der nach den Anmeldedaten für die u.trust LAN Crypt Cloud fragt. Nach der Eingabe der Anmeldedaten wird eine Erfolgsmeldung im Browser angezeigt. Dies bestätigt, dass der Anmeldevorgang erfolgreich abgeschlossen wurde und der Benutzer nun Zugang zu seinen in der u.trust LAN Crypt Cloud gespeicherten Schlüsseln hat.

Um sich abzumelden, folgen Sie dem gleichen Verfahren, wählen Sie jedoch **Abmelden** anstatt **Anmelden**. Nach der Abmeldung haben Sie keinen Zugriff mehr auf die in der u.trust LAN Crypt Cloud gespeicherten Schlüssel, bis Sie sich erneut anmelden. Dies dient als zusätzliche Sicherheitsebene, um zu verhindern, dass Unbefugte auf Ihre Schlüssel zugreifen können.

Verwaltete Schlüssel

Über das **Zahnradsymbol** in der unteren linken Ecke der Anwendung öffnen Sie das Einstellungsmenü. Unter **Verwaltete Schlüssel** können Sie die verwalteten Schlüssel Ihres Cloud-Kontos einsehen. Diese werden von *u.trust LAN Crypt* für Windows, macOS und Linux verwendet, um Dateien regelkonform und transparent zu ver- und entschlüsseln.

Verwaltete Schlüssel stehen Ihnen auch im Schlüsselbund von *u.trust LAN Crypt 2Go* zur Verfügung. Die Spalte für den **Schlüsseltyp** zeigt an, ob es sich um einen passwortbasierten oder einen verwalteten Schlüssel handelt.

Wenn eine Datei bereits durch einen LAN Crypt Client mit einem verwalteten Schlüssel verschlüsselt wurde, können Sie diese in *u.trust LAN Crypt 2Go* öffnen, bearbeiten und wieder verschlüsselt speichern. Voraussetzung ist, dass sich der zugehörige verwaltete Schlüssel in Ihrem Schlüsselbund befindet.

Verwaltete Schlüssel können nicht zum Erstellen passwortgeschützter Dateien verwendet werden. Für diese Funktion bietet *u.trust LAN Crypt 2Go* ausschließlich passwortbasierte Schlüssel zur Auswahl an. Der Unterschied: Passwortbasierte Schlüssel werden aus einem Passwort abgeleitet, verwaltete Schlüssel dagegen nicht.

Hinweis zum Outlook Add-In

- Das Outlook Add-In schützt Anhänge ebenfalls durch das Erstellen verschlüsselter Dateien mit passwortbasierten Schlüsseln. Empfänger können diese mit dem zugehörigen Passwort öffnen, ohne über den verwalteten Schlüssel Ihrer Organisation zu verfügen. Deshalb verwendet auch das Outlook Add-In ausschließlich passwortbasierte Schlüssel.
- „Verwaltet" bezeichnet hier den Schlüsseltyp, nicht den Speicherort. Passwortbasierte Schlüssel bleiben auch dann passwortbasiert, wenn sie in der Cloud verwaltet werden.

Passwortgeschützte Ver- und Entschlüsselung von Dateien

u.trust LAN Crypt 2Go ermöglicht den sicheren Austausch vertraulicher Daten durch passwortgeschützte Verschlüsselung. Mit *u.trust LAN Crypt 2Go* (AES 256-Bit) können Sie Dateien ganz einfach und sicher ver- und entschlüsseln. *u.trust LAN Crypt 2Go* nutzt für die Ver- und Entschlüsselung durch Passwörter generierte Schlüssel, die in einem Schlüsselbund innerhalb der Anwendung gespeichert werden. Benutzer können jederzeit neue Schlüssel hinzufügen, alte löschen oder die genutzten Passwörter für bereits vorhandene Schlüssel einsehen.

Hinweis

- Die Verschlüsselung erfordert immer ein sicheres Passwort! Dieses muss aus mindestens 8 Zeichen bestehen sowie Groß- und Kleinschreibung, Ziffern und Sonderzeichen beinhalten.
- Der Name des Verschlüsselungspassworts hat keinen Einfluss auf den für die Verschlüsselung verwendeten Schlüssel. Der eigentliche Schlüsselwert für die Verschlüsselung wird separat erzeugt.

Verwendung der grafischen Benutzeroberfläche

Beim Öffnen der App durch Auswahl des *u.trust LAN Crypt 2Go* Programmsymbols erscheint der Verschlüsselungsdialog. Verwenden Sie die Schaltfläche **Auswählen...**, um die zu verschlüsselnde oder zu entschlüsselnde Datei auszuwählen.

Um die Datei zu verschlüsseln, wählen Sie nun den gewünschten Schlüssel aus und klicken Sie auf abschließend auf **Verschlüsseln**. Neue Schlüssel können durch die Schaltfläche **Neuer Schlüssel** hinzugefügt und in den **Programm-Einstellungen** verwaltet werden.

u.trust LAN Crypt 2Go erstellt eine verschlüsselte Kopie der Datei. Verschlüsselte Dateien erhalten die zusätzliche Dateiendung .pcrypt und sind eindeutig durch das grafische Dokumentsymbol erkennbar.

Hinweis

- Die Originaldatei wird von *u.trust LAN Crypt 2Go* niemals gelöscht oder überschrieben.

Beim Entschlüsseln einer Datei, welche durch eines der *LAN Crypt* Produkte passwortbasiert verschlüsselt worden ist, wird vorerst geprüft ob der benötigte Schlüssel schon gespeichert ist. Ist das der Fall, so wird dieser automatisch zum Entschlüsseln verwendet. Ist der benötigte Schlüssel noch nicht vorhanden, so muss das Schlüsselpasswort eingegeben werden, um die Datei erfolgreich zu entschlüsseln. Das eingegebene Passwort wird als Schlüssel gespeichert und kann für weitere Ver- und Entschlüsselungen genutzt werden.

Hinweis

- Beim Entschlüsseln einer Datei erstellt *u.trust LAN Crypt 2Go* eine unverschlüsselte Kopie der Datei. Außerdem wird die ursprüngliche Dateierweiterung der Datei wiederhergestellt, indem die Dateierweiterung .pcrypt entfernt wird.

Um die erstellten Schlüssel einzusehen und zu verwalten, öffnen Sie die Programm-Einstellungen. Nun sehen Sie eine Auflistung der gespeicherten Schlüssel inklusive Informationen wie z.B deren GUIDs. Mit einem **Rechtsklick** auf einen Schlüssel können Sie diesen nun umbenennen, löschen oder sich das ursprüngliche Passwort anzeigen lassen (nur Windows).

Verwenden des Kontextmenüs

Wird eine unverschlüsselte Datei mit **Öffnen mit** -> **u.trust LAN Crypt 2Go** geöffnet, wird die Möglichkeit angeboten, das Dokument zu verschlüsseln.

Eine verschlüsselte Datei wird auf diese Weise temporär entschlüsselt und nach dem Einsehen oder Bearbeiten der Datei abschließend automatisch wieder verschlüsselt.

Verwenden von Drag-and-drop (nur Windows)

Um eine Datei mit *u.trust LAN Crypt 2Go* zu verschlüsseln oder zu entschlüsseln, können Sie ganz einfach die betreffende Datei auf das Programm-Icon ziehen.

Einsehen und Bearbeiten von verschlüsselten Dateien

Dateien können ohne manuelles Entschlüsseln auch direkt bearbeitet werden. Hierbei wird die verschlüsselte Datei beim Öffnen automatisch entschlüsselt und nach der Bearbeitung wieder mit dem entsprechenden Passwort verschlüsselt. Voraussetzung hierfür ist, dass der benötigte Schlüssel schon gespeichert worden ist oder auf Anfrage richtig eingegeben wird.

Zum Bearbeiten der Datei wird das jeweilige Standardprogramm genutzt (ursprüngliche .docx Dateien werden z.B. standardgemäß mit Microsoft Office geöffnet).

Hinweis

- Wenn eine verschlüsselte Datei schreibgeschützt ist, ist auch die temporär entschlüsselte Datei schreibgeschützt. Dies führt in der Regel dazu, dass das jeweilige Standardprogramm Änderungen an der Datei verhindert.
- Um eine entschlüsselte Version einer .pcrypt-Datei zu erstellen, können Sie entweder **Speichern unter** innerhalb des jeweiligen Bearbeitungsprogramms nutzen oder *u.trust LAN Crypt 2Go* öffnen, eine verschlüsselte Datei auswählen und auf die Schaltfläche **Entschlüsseln** tippen.

Verwenden des Microsoft Outlook-Add-Ins

u.trust LAN Crypt 2Go erweitert Microsoft Outlook um die Möglichkeit, Anhänge vor dem Versenden zu verschlüsseln.

Das Add-In wird in zwei Versionen zur Verfügung gestellt:

Classic Add-In: Wird mit dem LAN Crypt 2Go Windows-Client installiert. Die LAN Crypt Cloud Anbindung ist optional und dient lediglich dem Abruf und der Speicherung verwendeter Schlüssel. Die zentrale **Administration mit LAN Crypt Cloud ist nicht erforderlich**.

Modern Add-In: Wird über **Microsoft AppSource** bereitgestellt und ist kompatibel mit den neusten Versionen von Outlook auf Windows, macOS und der webbasierten Anwendung. Die zentrale **Administration mit LAN Crypt Cloud ist zwingend erforderlich**. Neben dem Abruf und der Speicherung verwendeter Schlüssel, ermöglicht das **Modern Add-In** auch weitere administrative Funktionen. Weitere Informationen zu den Add-In-Anforderungen in Exchange- und Outlook-Versionen finden Sie unter Systemanforderungen für Office-Add-Ins.

Hinweis

- Zu Testzwecken können Outlook-Web-Add-Ins auch per Sideloading installiert werden. Die **Manifest-XML-Datei** für das Sideloading kann unter folgendem Link heruntergeladen werden.

Beide Versionen unterstützen zwei Verschlüsselungsmodi:

Sofort verschlüsseln (Encrypt On-Demand):

Mit dieser Funktion können Anhänge bereits **vor dem Hochladen auf den Exchange-Server verschlüsselt** werden.

Um diese Funktion zu nutzen, muss der Benutzer das LAN Crypt 2Go-Add-in beim Bearbeiten der E-Mail auswählen. Daraufhin wird eine Ansicht geöffnet, in der ein Verschlüsselungsschlüssel für die anzuhängenden Dateien ausgewählt werden kann. Die ausgewählten Dateien werden anschließend automatisch **in verschlüsselter Form** an die E-Mail angehängt.

Hinweis

- Aufgrund einer technischen Einschränkung seitens Microsoft steht die Funktion **„Beim Senden verschlüsseln"** des Modern Add-Ins nur dann zur Verfügung, wenn das Add-In **von der Administration der Organisation bereitgestellt** oder **manuell per Sideloading installiert** wurde. Wird das Add-In direkt über den **Microsoft Marketplace** installiert, ist die Funktion **„Beim Senden verschlüsseln"** in Outlook deaktiviert. Damit Benutzerinnen und Benutzer Zugriff auf die ereignisbasierte Aktivierung erhalten, muss das Modern Add-In zentral durch die Organisation bereitgestellt oder zu Testzwecken per Sideloading eingebunden werden.

Beim Senden verschlüsseln (Encrypt On-Send):

Beim Versenden einer E-Mail mit dem **Modern Add-In** prüft LAN Crypt 2Go automatisch, ob und wie unverschlüsselte Anhänge behandelt werden sollen. Die Verschlüsselung erfolgt nur unter bestimmten Bedingungen:

1. Inhalte werden **nicht verschlüsselt**, wenn …
    - keine Anhänge in der E-Mail enthalten sind oder alle Anhänge bereits verschlüsselt sind,
    - die E-Mail ausschließlich an interne Empfänger gesendet wird (keine externen Adressen),
    - der Benutzer in der LAN Crypt 2Go-Seitenleiste die Option **Unverschlüsselt (Plain)** ausgewählt hat.
2. Inhalte werden **automatisch verschlüsselt**, wenn …
    - der Benutzer die Option **Verschlüsselt (Encrypted)** in der LAN Crypt 2Go-Seitenleiste auswählt. In diesem Fall verschlüsselt das System alle unverschlüsselten Anhänge automatisch mit dem ausgewählten Schlüssel.

3. Der Benutzer wird **zur Entscheidung aufgefordert**, wenn …
    - keine der beiden Optionen (**Unverschlüsselt (Plain)** oder **Verschlüsselt (Encrypted)**) ausgewählt wurde. Beim Senden der E-Mail erscheint ein Hinweisfenster, in dem der Benutzer festlegen muss, wie mit den Anhängen verfahren werden soll.

Wenn dem eine Benutzerentscheidung fehlt oder nicht klar ist, wie mit den E-Mail-Anhängen umgegangen werden soll, wird der Nutzer darauf hingewiesen und die Seitenleiste mit den verfügbaren Optionen automatisch geöffnet.

Anders als beim Modern Add-In erscheint beim Senden einer E-Mail mit dem **Classic Add-In** jedes Mal ein Dialog zur Auswahl der Verschlüsselungsoptionen für die Anhänge.

Hinweis

- Inline-Bilder, die direkt im Nachrichtentext eingebettet sind, werden nicht mitverschlüsselt. Um die Vertraulichkeit solcher Inhalte zu gewährleisten, müssen sie als reguläre Dateianhänge eingefügt werden.
- Bei der Verwendung des **Modern Add-In** kann der Admistrator innerhalb der LAN Crypt Cloud Administration den Verschlüsselungsmodus **Beim Senden verschlüsseln** (Encrypt On-Send) deaktivieren. Außerdem kann er interne E-Mail Domänen definieren und auch bestimmte Dateitypen von der automatischen Verschlüsselung ausschließen.

Verwendung von Registry Keys (nur Windows)

Die Windows-Version von LAN Crypt 2Go kann mit den folgenden Registry-Schlüsseln konfiguriert werden:

HKCU\Software\conpal\LAN Crypt\2Go

Dieser Schlüssel kann auch von Benutzern mit eingeschränkten Rechten bearbeitet werden:

Name	Typ	Standardwert	Wert
VerboseLogging	DWORD	0	Dieser Wert kann verwendet werden, um ausführliche Protokolle zu aktivieren, was bei der Fehlersuche hilfreich sein kann: 0 = Keine ausführliche Protokollierung (nur Info, Warn- und Fehlermeldungen werden protokolliert) 1 (und alle anderen Werte) = Ausführliche Protokollierung (auch Debug- und Verbose-Einträge werden in die Protokolldatei geschrieben)

HKCU\Software\Policies\conpal\LAN Crypt\2Go

HKLM\Software\Policies\conpal\LAN Crypt\2Go

Diese Registrierungsschlüssel können von eingeschränkten Benutzern nicht geändert werden.

Für die Versionen von *u.trust LAN Crypt 2Go* 1.0 bis 4.0 wird nur die HKEY*CURRENT*USER (**HKCU**)-Registrierungsstruktur unterstützt.

Bei den *u.trust LAN Crypt 2Go* Versionen 10.0 und neuer wird auch die HKEY*LOCAL*MACHINE (**HKLM**)-Registrierungsstruktur überprüft, wenn einer der unten aufgeführten Registrierungsschlüssel **NICHT** in der HKEY*CURRENT*USER-Ressource (**HKCU**) gesetzt ist. Dies ermöglicht es Administratoren, Einstellungen für alle Benutzer (über **HKLM**) zu verteilen und gleichzeitig Ausnahmen für bestimmte Benutzer (**HKCU**) zu ermöglichen.

Name	Typ	Standardwert	Wert
CheckOnSend	DWORD	1	Dieser Wert kann verwendet werden, um die Verschlüsselung beim Versenden zu deaktivieren: 0 = Senden ohne Prüfung 1 (und alle anderen Werte) = Prüfung der Anhänge beim Versenden und bei Bedarf Verschlüsselung anbieten

Name	Typ	Standardwert	Wert
`InternalMailDomains`	String	(Leer)	Eine durch Semikolon getrennte Zeichenfolge von Mail-Domänen, die als **intern** betrachtet werden sollen (= keine Verschlüsselung erforderlich). **Beispiel:** `{{ site.company_name_small }}.de;` `{{ site.company_name_small }}.at`, wobei alle Mails an nnn@{{ site.company*name*small }}.de und nnn@{{ site.company*name*small }}.at werden nicht auf auf ungeschützte Anhänge geprüft werden. Wenn `InternalMailDomains` nicht festgelegt ist, werden die E-Mail-Domains der Empfänger mit der E-Mail-Domain des Absenders verglichen. Nur die E-Mail-Domain des Absenders wird als **intern** betrachtet.
`ExcludedAttachments`	String	(Leer)	Eine durch Semikolon getrennte Zeichenfolge von Dateierweiterungen für Dateien, die nicht verschlüsselt werden sollten. **Beispiel:** `.txt;.png;.pdf`
`AllowSendUnencrypted`	DWORD	1	Mit diesem Wert kann die Verschlüsselung von Anhängen an externe E-Mail-Domänen erzwungen werden, wodurch die Sicherheit Ihrer Korrespondenz gewährleistet wird. Bitte beachten Sie, dass Anhänge an interne E-Mail-Domänen weiterhin im Klartext versendet werden. 1 (oder nicht gesetzt) = Dem Benutzer wird erlaubt, Anhänge im Klartext an externe Empfänger zu senden. 0 (und alle anderen Werte außer 1) = Verschlüsselung beim Versenden von E-Mails an externe Empfänger erzwingen.

Hinweis

- Für zusätzliche Informationen zur Verwendung von Registry-Schlüsseln in Windows-Umgebungen können Sie weitere Details und Anleitungen hier{:target="_blank"} nachlesen.

Verwendung des u.trust LAN Crypt 2Go Kommandozeilen-Tools

Mit dem Kommandozeilen-Tool von u.trust LAN Crypt 2Go können Sie Dateien über die Kommandozeile oder das Terminal ver- und entschlüsseln. Hierfür öffnen Sie über die Konsole den jeweiligen Pfad:

Windows:

```
C:\Users\<Benutzername>\AppData\Local\Programs\conpal\LAN Crypt\2Go\lancrypt.exe
```

macOS:

```
/Applications/u.trust LAN Crypt 2Go.app/Contents/Resources/lancrypt.app/Contents/MacOS/lancrypt
```

Linux:

Da das Installationsprogramm das Kommandozeilentool automatisch zum Suchpfad hinzufügt, muss kein bestimmter Pfad über die Konsole geöffnet werden.

Nun können Sie mit dem Befehl `lancrypt` und einer folgenden Anweisung die Anwendung innerhalb der Konsole nutzen.

Verwaltung von Schlüsseln

u.trust LAN Crypt 2Go ermöglicht das Verwalten von Schlüsseln über die Konsole. Schlüssel können dort hinzugefügt, gelöscht, umbenannt und aufgelistet werden.

Schlüssel hinzufügen:

```
lancrypt /A schlüsselname passwort
```

oder

```
lancrypt /A /F datei passwort
```

Fügt einen Schlüssel für weitere Ver- und Entschlüsselungen hinzu. Bei der Zusatzoption `/F datei` werden der Name des Schlüssels, seine GUID und weitere Schlüsselinformationen aus einer gegeben Datei entnommen.

Schlüssel löschen:

```
lancrypt /P /N name
```

oder

```
lancrypt /P /G guid
```

Löscht den angegebenen Schlüssel. Bei der Zusatzoption `/N name` wird der zu löschende Schlüssel anhand seines Namens identifiziert. Bei der Zusatzoption `/G guid` wird der zu löschende Schlüssel anhand seiner GUID identifiziert.

Schlüssel umbenennen:

```
lancrypt /R /N name neuer-name
```

oder

```
lancrypt /R /G guid neuer-name
```

Benennt den Schlüssel um. Bei der Zusatzoption `/N name` wird der gewählte Schlüssel anhand seines Namens identifiziert und umbenannt. Bei der Zusatzoption `/G guid` wird der gewählte Schlüssel anhand seiner GUID identifiziert und umbenannt.

Schlüssel auflisten:

```
lancrypt /L
```

Listet alle gespeicherten Schlüssel auf.

Hinweis

- Während Sie in der u.trust LAN Crypt Cloud angemeldet sind, stehen Befehlszeilenoptionen zum Hinzufügen, Löschen oder Umbenennen von Schlüsseln nicht zur Verfügung. Diese Funktionen können jedoch durch die Verwendung der Anwendung ausgeführt werden.

Verschlüsseln

```
lancrypt /E datei /N schlüsselname
```

oder

```
lancrypt /E datei /G schlüsselguid
```

oder

```
lancrypt /E datei passwort
```

Verschlüsselt die gewählte Datei entweder mit einem bereits bestehenden Schlüssel (identifiziert durch entweder `/N name` oder `/G guid`) oder mit einem neu gewählten Passwort.

Hinweis

- Die Verschlüsselung erfordert immer ein sicheres Passwort! Dieses muss aus mindestens 8 Zeichen bestehen sowie Groß- und Kleinschreibung, Ziffern und Sonderzeichen beinhalten.
- Der Name des Verschlüsselungspassworts hat keinen Einfluss auf den für die Verschlüsselung verwendeten Schlüssel. Der eigentliche Schlüsselwert für die Verschlüsselung wird separat erzeugt.

Entschlüsseln

```
lancrypt /D datei
```

oder

```
lancrypt /D datei password
```

Entschlüsselt die gewählte Datei entweder automatisch mit dem passenden bereits gespeicherten Schlüssel oder mit dem gegebenen Passwort.

Hinweis

- Bei der Entschlüsselung mit einem Passwort, wird dieses nicht automatisch in den gespeicherten Schlüsseln hinterlegt.

Mit exportierten Schlüsseln entschlüsseln

Das Befehlszeilentool enthält jetzt einen optionalen Parameter `/K` für die Entschlüsselungsoption (`/D`). Dieser Parameter gibt den Pfad zu einer exportierten Schlüsseldatei (im JSON-Format) an.

Einzelne Datei entschlüsseln

Um eine einzelne Datei zu entschlüsseln, verwenden Sie die Option `/D` mit dem Dateinamen und die Option `/K` mit dem Pfad zur Schlüsseldatei:

```
lancrypt /D exportedKeysTest.txt.pcrypt /K exportedKeys.json
```

Alle Dateien in einem Ordner entschlüsseln

Um alle Dateien in einem Ordner zu entschlüsseln, verwenden Sie die Option `/D` mit dem Ordnerpfad und die Option `/K` mit dem Pfad zur Schlüsseldatei:

```
lancrypt /D directory /K exportedKeys.json
```

Hinweis

- Das Entschlüsseln eines Ordners schließt alle Dateien in dessen Unterverzeichnissen ein.

Standalone-Version

LAN Crypt 2Go unterstützt jetzt die Erstellung von **Standalone-Versionen** der Anwendung. Eine Standalone-Version kann auf Wechseldatenträgern (z. B. USB-Sticks) oder in cloud-synchronisierten Ordnern abgelegt werden.

Diese Versionen laufen **ohne Installation** auf dem Host-System und können auf **jedem Rechner ausgeführt werden, der dasselbe Betriebssystem verwendet wie beim Erstellen der Standalone-Version**. Alle Softwarekomponenten und Konfigurationsdaten werden zusammen mit der Standalone-Kopie gespeichert.

> **Hinweis**
>
> - Es werden keine Anwendungsdaten außerhalb einer generierten `readme`-Datei und eines `LAN Crypt 2Go Data`-Ordners neben der Standalone-Datei auf dem System gespeichert.
> - Unter **Windows** werden keine Informationen in der **Windows-Registry** gespeichert.

Erstellen einer Standalone-Version

So erstellen Sie eine Standalone-Version von LAN Crypt 2Go:

1. Öffnen Sie das Menü **Programm-Einstellungen**.
2. Wählen Sie **Stand-alone Version erzeugen**.
3. Wählen Sie den Zielordner, in dem die Anwendung erzeugt werden soll.

Nach Abschluss des Vorgangs enthält der gewählte Ordner die vollständige **LAN Crypt 2Go Standalone-Anwendung**.

Verwenden einer Standalone-Version

Standalone-Versionen von LAN Crypt 2Go speichern ihre Konfiguration und Schlüssel in verschlüsselter Form, geschützt durch ein **Master-Passwort**.

Beim ersten Start der Standalone-Anwendung wird der Benutzer aufgefordert, ein Master-Passwort festzulegen. Beim nächsten Start bleiben alle gespeicherten Schlüssel und Konfigurationsdaten verschlüsselt, bis das definierte Master-Passwort korrekt eingegeben wird.

Ändern oder Zurücksetzen des Master-Passworts

Um das Master-Passwort zu ändern, öffnen Sie die **Anwendungseinstellungen**, während die Standalone-Version von LAN Crypt 2Go ausgeführt wird. Unter **Anwendungspasswort ändern** kann das Master-Passwort geändert oder zurückgesetzt werden.

Das Zurücksetzen des Master-Passworts löscht alle gespeicherten Schlüssel und Passwörter und fordert den Benutzer beim nächsten Start der Anwendung auf, ein neues Master-Passwort zu definieren.

Einschränkungen

Da die Standalone-Version nicht auf einer systemweiten Installation basiert, werden bestimmte Funktionen **nicht unterstützt**:

- Das **Outlook-Add-In** steht nicht zur Verfügung.
- **LAN Crypt Cloud-Support** ist nicht verfügbar.
- Unter Windows werden `.pcrypt`-Dateien **nicht automatisch** mit der Standalone-Anwendung verknüpft.

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 21.09.2026