CONPAL LAN CRYPT HILFE

DE

CONPAL LAN CRYPT FÜR macOS

Was ist conpal LAN Crypt für macOS?

conpal LAN Crypt ermöglicht mit transparenter Dateiverschlüsselung den Austausch vertraulicher Daten innerhalb von Berechtigungsgruppen in kleinen, mittleren und großen Organisationen. conpal LAN Crypt funktioniert ohne Benutzerinteraktion. Es unterstützt die Rolle eines Security Officers (SO), der die Zugriffsrechte auf Dateien, die mit conpal LAN Crypt verschlüsselt sind, einschränken kann. Ein Master Security Officer (MSO) hat das Recht, conpal 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. conpal 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 conpal LAN Crypt), sehen aber ohne die entsprechende conpal LAN Crypt Berechtigung nur deren verschlüsselten Inhalt.

Schutz von Daten durch conpal LAN Crypt für macOS

conpal 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 transparent und 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 transparente Verschlüsselung benötigt werden. Die Richtliniendatei ist durch ein Zertifikat geschützt. Damit Benutzer auf ihren Computern Dateien verarbeiten können, die mit conpal 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.

conpal LAN Crypt ermöglicht die Einteilung der Benutzer in verschiedene Berechtigungsgruppen. Alle conpal 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 Richtliniendateien zuzugreifen, damit die Dateien transparent ver- bzw. entschlüsselt werden können, sobald sie geöffnet bzw. geschlossen werden. Es können alle Organisationsformen abgebildet werden, in dem die Benutzer zentral administriert werden, bis zu einem verteilten Modell, in dem Benutzer nur Notebooks einsetzen.

Unterschiede von conpal LAN Crypt für Windows und conpal LAN Crypt für macOS

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 conpal LAN Crypt für macOS unterstützte Verschlüsselungsalgorithmen

conpal 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 conpal LAN Crypt für Windows auch noch weitere Verschlüsselungsalgorithmen (wie z. B. „IDEA“ oder „3DES“, etc.) unterstützt. conpal 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.

conpal 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

Transparente Verschlüsselung

Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (in verschlüsselten Ordnern auf Netzwerkfreigaben) automatisch im Hauptspeicher entschlüsselt, sobald sie von einer Anwendung (wie z. B. von Office) geöffnet werden. Beim Speichern der Datei wird sie automatisch wieder verschlüsselt. Von der transparenten Verschlüsselung werden alle Dateivorgänge erfasst. Da alle Prozesse im Hintergrund laufen, bemerken Benutzer nichts davon, wenn sie mit verschlüsselten Dateien arbeiten.

Die Verschlüsselung ist nicht von Ordnern abhängig, sondern nur von Verschlüsselungsregeln. Die Verschlüsselung funktioniert wie folgt:

- Alle Dateien, für die eine Verschlüsselungsregel existiert, werden automatisch verschlüsselt.
- Wenn Dateien in einen verschlüsselten Ordner verschoben oder kopiert werden, werden sie gemäß der für diesen Ordner definierten Verschlüsselungsregel verschlüsselt. Über die *conpal LAN Crypt* Administration kann der Sicherheitsbeauftragte mehrere Verschlüsselungsregeln für unterschiedliche Dateitypen oder Dateinamen definieren, die sich im selben Ordner befinden. Sie können beispielsweise Word-Dateien mit einer anderen Regel verschlüsseln als Excel-Dateien, obwohl sich beide Dateien im selben Ordner befinden.
- Wenn verschlüsselte Dateien umbenannt werden, bleiben sie verschlüsselt. Wenn für den Zielordner eine andere Verschlüsselungsregel aktiv ist, wird die Datei mit dem in dieser Regel angegebenen Schlüssel verschlüsselt. Eine Umbenennungsoperation führt jedoch niemals zu einer Entschlüsselung der Datei.
- Wenn eine Datei in einen anderen Ordner innerhalb derselben SMB-Freigabe oder auf eine andere SMB-Freigabe ohne Verschlüsselungsregel kopiert wird, wird sie automatisch ent- schlüsselt. Wenn Dateien innerhalb derselben SMB-Freigabe verschoben werden, bleiben sie verschlüsselt. Dies gilt auch für Ordner, für die eine **„Ausschließen“- oder „Ignorieren“-Regel existiert** (siehe Administratorhandbuch, Abschnitt „Erzeugen von Verschlüsselungsregeln“).

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.

Hinweis

- Besteht für eine SMB-Freigabe eine „Ignorieren-Regel“, kann ein Benutzer dort enthaltene verschlüsselte Dateien jedoch nicht öffnen, auch wenn dieser den hierfür erforderlichen Schlüssel besitzen sollte

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

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.

Von der Verschlüsselung ausgenommene Dateien und Ordner

Folgende Dateien und Ordner sind automatisch von der Verschlüsselung ausgenommen, auch wenn für sie eine Verschlüsselungsregel definiert wurde:

- Dateien auf allen lokalen Laufwerken.
- Dateien in Ordnern, die in conpal LAN Crypt mit einer „Ausnahme“- oder „Ignorieren“-Regel definiert sind.

Transparente Verschlüsselung und Komprimierungsprogramme

Dateikomprimierungswerkzeuge öffnen Dateien, lesen ihren Inhalt und komprimieren ihn. Wenn die transparente Verschlüsselung/Entschlüsselung aktiviert ist, erhalten diese Tools Klartext-Inhalte. Daher ist es für den Datenschutz unerlässlich sicherzustellen, dass das resultierende Archiv in einem Ordner gespeichert wird, der einer Verschlüsselungsregel unterliegt.

Konfiguration

Konfigurationsdatei erstellen

Alle Einstellungen für *conpal 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/conpal/LAN Crypt/useragent.app/Contents/Resources/config.plist.template
```

Nachdem Sie die Vorlage angepasst haben, kopieren Sie sie an den folgenden Speicherort:

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

Zwingend erforderliche Einträge in der Konfigurationsdatei

PolicyPath: Mount-Point der Richtliniendatei Tragen Sie im Abschnitt `<string>` die Netzwerkfreigabe ein, auf der die Richtliniendateien (.xml.bz2) der Benutzer gespeichert sind.

Beispiel:

```
<key>PolicyPath<key> <string>/Volumes/lancrypt/Profile</string>
```

SOCertLocation: Mount-Point des öffentlichen Zertifikats des Security Officers Tragen Sie im Abschnitt `<string>` die Netzwerkfreigabe ein, in der die öffentlichen Zertifikate (.cer) des Sicherheitsbeauftragten gespeichert sind.

Beispiel:

```
<key>SOCertLocation</key> <string>/Volumes/lancrypt/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 *conpal 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 *conpal LAN Crypt* Administration generierten Namen übereinstimmt. Nur wenn der Anmeldename und der Name der Richtliniendatei identisch sind, kann der Benutzer mit *conpal LAN Crypt für macOS* arbeiten.

CertificatePath: Mount-Point der Schlüsseldatei (.p12) des Benutzers Nach Angabe des Einhängepunkts für die Schlüsseldatei (.p12) des Benutzers versucht *conpal 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.

AutoMountAllNetworkShares: Alle Netzwerkfreigaben automatisch einhängen Regeln sind normalerweise an den UNC-Pfad eines Servers gebunden, entweder über die IP- Adresse oder den DNS-Namen. Wenn solche absoluten Regeln nicht erwünscht sind, kann der Sicherheitsbeauftragte auch relative Regeln verwenden, die mit Teilen des UNC-Pfads übereinstimmen. Während dieser Ansatz unter Microsoft Windows funktioniert, da er UNC-Pfade wie jeden anderen (lokalen) Ordner im Dateisystem durchsuchen kann, erfordert macOS, dass ein freigegebener Ordner bereitgestellt wird, bevor darauf zugegriffen werden kann. Wenn ein freigegebener Ordner von einem Benutzer mit nur relativen Regeln in seiner Richtlinie eingehängt wird, würde *conpal LAN Crypt für macOS* ihn ignorieren, da er mit keiner Regel in der Richtlinie übereinstimmt. In solchen Szenarien können Sie den Parameter AutoMountAllNetworkShares auf `true` setzen, um eine transparente Verschlüsselung und Entschlüsselung unabhängig von der Richtlinie zu aktivieren. Falls konfiguriert, werden alle UNC-Pfade von *conpal LAN Crypt für macOS* ignoriert. Relative Regeln funktionieren wie erwartet.

Beispiel:

```
<key>AutoMountAllNetworkShares</key> <false/>
```

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>
```

Konfigurationsdatei neu laden

Änderungen an der Konfigurationsdatei erfordern einen Neustart von *conpal LAN Crypt*. Öffnen Sie dazu ein Terminal und führen Sie den folgenden Befehl aus oder führen Sie eine Abmeldung und Anmeldung durch.

```
launchctl unload /Library/LaunchAgents/de.conpal.lancrypt.useragent.plist && launchctl load /Library/LaunchAgents/de.conpal.lancrypt.useragent.plist
```

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 *conpal LAN Crypt* Administration die Benutzerzertifikate sowie das öffentliche Zertifikat (.cer) des Sicherheitsbeauftragten speichert (siehe Handbuch der *conpal 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 *conpal LAN Crypt* fehlschlägt, werden Fehler im Systemprotokoll protokolliert. Um nach *LAN Crypt* zu filtern, stellen Sie das Subsystem auf „de.conpal.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 ansehen folgender Befehl: `log stream --level debug --predicate 'subsystem == "de.conpal.lancrypt"'`

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

Verschlüsselungsregeln mit den ihnen zugeordneten Schlüsseln aus den *conpal 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 (transparent).

Hinweis

- Damit *conpal 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.

Laden der Richtliniendatei

Standardverhalten von conpal LAN Crypt

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

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

Hinweis

- *conpal LAN Crypt* verifiziert die Zertifikate des Benutzers und das öffentliche Zertifikat (.cer) des (Master-)Security Officers, der die Richtliniendatei erstellt hat. Enthält das Zertifikat einen „CRL Distribution Point" und es ist keine gültige CRL auf dem System vorhanden, vertraut *conpal 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.

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**.

Anmeldung an conpal LAN Crypt

Verschlüsselungsprofile von *conpal 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 *conpal 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 *conpal 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 conpal LAN Crypt für macOS auch einen Sicherheitstoken verwenden. Voraussetzung dafür ist, dass das conpal 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.

Client Status-Information

conpal 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 das derzeit aktive Konto angezeigt. Diese Registerkarte ist nur unter macOS 12 und höher verfügbar.

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

Konfiguration für Microsoft OneDrive

conpal LAN Crypt für macOS bietet Unterstützung für die Verschlüsselung in Microsoft OneDrive. Diese Funktion kann nur auf Macs mit Apple Silicon auf Intel-Macs mit einem T2-Sicherheitschip mit macOS 12 oder höher aktiviert

werden. Auf allen anderen Computern muss FileVault aktiviert sein. Dadurch wird sichergestellt, dass Dateien geschützt sind, nachdem sie aus der Cloud auf den Mac heruntergeladen wurden.

Benutzer können ihr OneDrive-Konto auf der Registerkarte **Konten** im Informations-Dialog von *conpal LAN Crypt für macOS* hinzufügen. Nachdem das Konto erfolgreich hinzugefügt wurde, erscheint im Finder unter **Orte** ein neuer Eintrag namens „*conpal LAN Crypt*“, der dem Benutzer Zugriff auf sein persönliches Laufwerk einschließlich aller damit verknüpften Ordner gibt.

Bei der ersten Anmeldung werden Sie möglicherweise von OneDrive aufgefordert, *conpal LAN Crypt für macOS* die Berechtigung zum Zugriff auf Ihr OneDrive zu erteilen. Damit das Produkt ordnungsgemäß funktioniert, ist eine Genehmigung erforderlich.

Konfiguration für Google Drive

conpal LAN Crypt für macOS bietet ebenfalls Unterstützung für die Verschlüsselung in Google Drive. Hierbei werden Google Workspace Konten wie auch persönliche Google Konten unterstützt.

Benutzer können ihr Google-Konto auf der Registerkarte **Konten** im Informationsdialog von *conpal LAN Crypt für macOS* hinzufügen. Nach einem Autorisierungs- und Authentifizierungsdialog (OAuth) ist das Konto erfolgreich verknüpft. Im Finder erscheint unter **Orte** ein neuer Eintrag namens „*conpal LAN Crypt*“, der den Benutzern Zugriff auf ihr persönliches Laufwerk einschließlich aller damit verknüpften Ordner gibt.

Verknüpfung mehrerer Cloud-Speicher-Konten

Wird mehr als ein Cloud-Speicher-Konto mit *conpal LAN Crypt für macOS* verknüpft, so werden die zugehörigen Namensgebungen der Einträge im Finder zur besseren Übersicht mit den jeweiligen Accountinformationen (Cloud-Speicher-Dienst und genutzte E-Mail-Adresse) ergänzt.

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 *conpal 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 *conpal LAN Crypt für macOS* können problemlos parallel arbeiten. *conpal LAN Crypt für macOS* kann als Ersatz für die Clients von OneDrive und Google Drive verwendet werden.
- Verschlüsselungsfunktionen sind nur verfügbar, wenn über den *conpal LAN Crypt*-Ort auf die Ordner zugegriffen wird.

Schnellaktion-Erweiterung aktivieren

conpal 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

conpal LAN Crypt für macOS installieren

conpal LAN Crypt für macOS unterstützt folgende Versionen von macOS:

- **macOS 12 Monterey**
- **macOS 11 Big Sur**
- **macOS 10.15 Catalina**

macOS 10.13 High Sierra führte eine neue Sicherheitsfunktion ein, die erfordert, dass Benutzer das Laden von Kernel-Erweiterungen explizit genehmigen. Da *conpal LAN Crypt für macOS* eine solche Erweiterung enthält, um seine transparente Verschlüsselungs- und Entschlüsselungsfunktionalität bereitzustellen, müssen Administratoren je nach Umgebung möglicherweise zusätzliche Schritte unternehmen.

Nicht verwaltete Macs

Nach der Installation von *conpal LAN Crypt für macOS* erscheint ein Dialog, der den Benutzer auffordert, die Systemeinstellungen zu öffnen und auf der Registerkarte **Allgemein** im Bereich **Sicherheit & Datenschutz** auf die Schaltfläche **Zulassen** zu klicken. Diese Schaltfläche ist nur 30 Minuten nach der Installation sichtbar. Nach dem Neustart des Systems ist *conpal LAN Crypt für macOS* funktionsfähig.

Verwaltete Macs

Für MDM-verwaltete Macs können Administratoren Richtlinien konfigurieren, um die Teamkennung, die zum Signieren der Kernel-Erweiterung *conpal LAN Crypt für macOS* verwendet wird, auf die Whitelist zu setzen. Informationen zum Konfigurieren solcher Richtlinien finden Sie in der Dokumentation zur Verwaltung mobiler Geräte. Für *conpal LAN Crypt für macOS* muss die **Teamkennung NXV97CU3K4** auf die Whitelist gesetzt werden

conpal LAN Crypt für macOS deinstallieren

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

```
/Library/conpal/LAN Crypt/Uninstaller.pkg
```

Hinweis

- Nach der Deinstallation von conpal LAN Crypt für macOS können auf dem Mac keine Dateien mehr ver- oder entschlüsselt werden. Die Deinstallation von conpal 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/conpal/LAN Crypt/useragent.app/Contents/Resources
```

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

Version von conpal LAN Crypt für macOS anzeigen lassen

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

```
/Library/conpal/LAN\ Crypt/useragent.app/Contents/Resources/lcutil version
```

Protokolldatei erstellen

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

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

```
/Library/conpal/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 and
- config.plist
- Informationen über konfigurierte Cloud-Provider-Konten (macOS 12 oder höher)

Technische Unterstützung

Technischen Support zu conpal Produkten können Sie wie folgt abrufen:

Unter support.conpal.de erhalten Wartungsvertragskunden Zugang zu weiteren Informationen, wie Knowledge-Items.

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