conpal LAN Crypt

smart
hochsicher
persistent

Admin Hilfe

Produktversion: 3.97
Stand: Mai 2019

Inhalt

1 Überblick

1.1 Was ist conpal LAN Crypt?

conpal LAN Crypt schützt vertrauliche Daten durch Dateiverschlüsselung. Es wurde entwickelt, um den vertraulichen Austausch von Daten zwischen Benutzern innerhalb von Berechtigungsgruppen in großen Organisationen zu ermöglichen. In diesem Fall können verschlüsselte Dateien lokal auf der Festplatte des Anwenders liegen oder auf Wechselmedien beziehungsweise Netzlaufwerken gespeichert sein..

Die Verschlüsselung erfolgt für den Benutzer transparent. Sie erfolgt automatisch bei der Erstellung oder Speicherung von Dateien. Ebenso erfolgt die Entschlüsselung unbemerkt, beim Lesen der Daten. Die Verantwortung dafür übernimmt ein Filtertreiber, der sich in das Dateisystem eines Windows-Rechners integriert. Ähnlich einem Virenscanner erkennt der conpal LAN Crypt Filtertreiber, auf welche Dateien zugegriffen werden soll, und führt dabei die gewünschte Ver- beziehungsweise Entschlüsselung durch.

Jedes Mal, wenn ein Benutzer eine Datei in ein verschlüsseltes Verzeichnis verschiebt, wird die Datei auf dem Computer dieses Benutzers verschlüsselt und jedes Mal, wenn ein anderer Benutzer aus derselben Berechtigungsgruppe die Datei aus dem Verzeichnis liest, wird sie in verschlüsselter Form übertragen. Die Datei wird erst entschlüsselt, wenn sie auf dem Zielrechner ankommt, wo der Benutzer sie dann ändern kann. Bevor sie in das verschlüsselte Verzeichnis zurückgestellt wird, wird sie wieder verschlüsselt.

Verschlüsselte Dateien sind nicht an einen einzelnen Benutzer „gebunden“. Alle Benutzer, die den notwendigen Schlüssel besitzen, können auf die verschlüsselte Datei zugreifen. Dies erlaubt Security Officers das Erzeugen von logischen Benutzergruppen, die gemeinsam auf verschlüsselte Dateien zugreifen 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 Schlüssel für verschiedene Türen oder Safes verwendet werden können.

Nicht berechtigte Benutzer können eventuell auf diese verschlüsselten Dateien zugreifen (jedoch nur von Arbeitsstationen ohne conpal LAN Crypt). Sie sind jedoch ohne entsprechende conpal LAN Crypt-Berechtigung nicht in der Lage, diese zu lesen.

Auf diese Weise bleibt die Datei immer geschützt, auch wenn im Dateisystem selbst kein Zugriffsschutz definiert ist, das Netzwerk angegriffen wird oder die Mitarbeiter sich nicht an die Sicherheitsrichtlinien der Organisation halten.

conpal LAN Crypt ist das Produkt Ihrer Wahl, wenn es darum geht, geistiges Eigentum in Dateiform vor unberechtigtem Zugriff in einem LAN, auf einem File-Server, auf der lokalen Festplatte oder sogar auf mobilen Datenträgern zu schützen.

Welche Dateien und Verzeichnisse durch conpal LAN Crypt geschützt werden sollen, legt ein Security Officer (SO) zentral durch eine oder mehrere Verschlüsselungsregeln fest. Um beispielsweise die Verschlüsselung aller Word-Dokumente sicherzustellen, definiert der SO die Regel *.doc. Sobald die Regel über eine Richtliniendatei (Policy) auf die Client3 conpal LAN Crypt Administration Systeme ausgerollt ist, werden sämtliche Word-Dokumente verschlüsselt und zwar unabhängig davon, wo sie liegen.
Bei Bedarf lassen sich mehrere Verschlüsselungsregeln zu einem Verschlüsselungsprofil kombinieren.

Im folgenden Beispiel sind drei verschiedene Regeln zu einem Verschlüsselungsprofil kombiniert:

Regel	Schlüssel	Beschreibung
*.doc	Schlüssel1	Verschlüsselt alle Word-Dokumente mit Schlüssel1, unabhängig davon, wo sie liegen.
D:\Daten*.*	Schlüssel2	Verschlüsselt alle Dateien im angegebenen Verzeichnis mit Schlüssel2.
\\Server1\Share1\Personal*.xls	Schlüssel3	Verschlüsselt alle Excel-Dateien unter dem angegebenen File-Server-Verzeichnis mit Schlüssel3.

conpal LAN Crypt erlaubt die Definition beliebig komplexer Regeln, so dass der SO sicherstellen kann, dass nur die gewünschten Daten an den tatsächlich gewünschten Speicherorten verschlüsselt werden. Das Ausrollen von Regeln erfolgt über Richtliniendateien, welche auf einem File-Server oder im Netlogon-Verzeichnis eines Windows Domain Controllers abgelegt werden können. Auf Knopfdruck erzeugt ein Security Officer für jeden Benutzer eine eigene Richtlinie. In dieser sind alle Schlüssel und Regeln zusammengefasst, die für den betreffenden Benutzer gelten.

Für die Erzeugung und Verwaltung der Richtliniendateien nutzt der SO die grafische Benutzeroberfläche conpal LAN Crypt Administration. Diese bedient sich wiederum der Microsoft Management Console (MMC) als Schnittstelle. Snap-Ins stellen dem Security Officer Werkzeuge zur Verfügung, um ihm die Arbeit zu erleichtern.

Die Richtliniendateien werden mit Hilfe von Zertifikaten für jeden einzelnen Benutzer individuell verschlüsselt. Hierbei kommt eine bereits in der Organisation vorhandene Public Key Infrastructure (PKI) zum Einsatz. Alternativ kann der SO die Möglichkeit nutzen, die Zertifikate durch conpal LAN Crypt selbst zu erzeugen.

Die Speicherung der Administrationsdaten von conpal LAN Crypt erfolgt in einer SQL-Datenbank. In der SQL Datenbank werden wichtige Datensätze und vor allem die Schlüssel verschlüsselt gespeichert. Durch den Einsatz einer von der Systemadministration unabhängigen Datenbank lässt sich eine strikte Trennung der Sicherheits- gegenüber der Systemadministration

realisieren. Darüber hinaus bietet conpal LAN Crypt die Möglichkeit zur Konfiguration unterschiedlicher SO-Rollen, deren Rechte sich je nach Anforderung beliebig einschränken lassen.

Lediglich ein Master Security Officer (MSO) hat stets sämtliche Rechte inne. Ein SO ist zudem in der Lage, Rechte zur Administration von conpal LAN Crypt zu delegieren und so eine Administrationshierarchie zu schaffen, die der Organisationsform jedes Unternehmens gerecht wird.

1.2 Schutz von Daten durch conpal LAN Crypt

conpal LAN Crypt garantiert, dass sensible Dateien auf File Servern und Arbeitsstationen verschlüsselt gespeichert werden können. Ebenso erfolgt die Übertragung in Netzwerken (LAN oder WAN) geschützt, da Ver- und Entschlüsselung im Hauptspeicher der Arbeitsstation des Benutzers durchgeführt werden. Auf dem File-Server selbst muss keine spezielle Sicherheitssoftware installiert werden.

Die Richtliniendateien enthalten alle Regeln, Zugriffsrechte und Schlüssel, die für die transparente Verschlüsselung benötigt werden.
Damit ein Benutzer auf seiner Arbeitsstation Daten mit conpal LAN Crypt ver- und entschlüsseln kann, muss er in der Lage sein, auf die Richtliniendatei zuzugreifen. Die Richtliniendatei ist durch ein Zertifikat vor unberechtigtem Zugriff gesichert. Um Zugriff zu erhalten, muss ein Benutzer über den privaten Schlüssel des passenden Zertifikats verfügen.
Auf den Arbeitsstationen laufen alle Ver- und Entschlüsselungen transparent und weitgehend ohne die Notwendigkeit von Benutzerinteraktionen ab.

conpal LAN Crypt ermöglicht die Einteilung der Benutzer in verschiedene Berechtigungsgruppen durch die Definition unterschiedlicher Rechte auf Verzeichnis- und Dateiebene. Die Sammlung dieser Rechte ergibt ein Verschlüsselungsprofil für den Benutzer. Durch den Besitz des zum Zertifikat gehörenden privaten Schlüssels hat der Benutzer Zugriff auf seine Richtliniendatei, in der das Verschlüsselungsprofil gespeichert ist.

Alle conpal LAN Crypt Benutzer, die in ihrer Richtliniendatei dasselbe Verschlüsselungsprofil gespeichert haben, sind Mitglieder einer Berechtigungsgruppe. Die Benutzer müssen sich dazu weder um die Verschlüsselung noch um den Schlüsselaustausch kümmern. Sie müssen nur in der Lage sein, auf die Richtliniendateien zuzugreifen. Ist diese Voraussetzung erfüllt, werden die Dateien der Benutzer transparent ver- bzw. entschlüsselt, sobald sie geöffnet bzw. geschlossen werden.

Durch die Verteilung der Verschlüsselungsprofile über Richtliniendateien können alle Organisationsformen abgebildet werden: von einem zentralen LAN-Modell, in dem die Benutzer zentral administriert werden, bis zu einem verteilten Modell, in dem Benutzer Notebooks einsetzen.

conpal LAN Crypt Administration und Windows Administration

Die Verwaltung der Verschlüsselungsprofile und die Konfiguration von conpal LAN Crypt erfolgt auf einem eigenen Administrationsrechner. Um eine klare Unterscheidung zwischen der Windows Administration und der Administration von conpal LAN Crypt zu erreichen, muss die Rolle eines Security Officers eingerichtet werden. Der Security Officer legt durch die Definition der Verschlüsselungsprofile in Richtliniendateien fest, welche verschlüsselten Daten in welchen Verzeichnissen abzulegen sind und wer auf diese Daten Zugriff hat. Nach der Erzeugung der Richtliniendateien auf dem Administrationsrechner müssen diese an die Benutzer verteilt werden.

Zur Administration von conpal LAN Crypt wird ein Windows-Standardmechanismus, die Microsoft Management Konsole (MMC), verwendet. Die Benutzeroberfläche der conpal LAN Crypt Administration besteht aus Snap-Ins für die MMC. Die conpal LAN Crypt Administration speichert die meisten administrierbaren Objekte (Benutzerdaten, Schlüssel, Verschlüsselungspfade, etc.) in einer eigenen Datenbank.

Die Verwendung des Datenbankkonzepts anstelle von ausschließlich Windows-Mechanismen (z. B. Active Directory) hat vor allem zwei Vorteile:

- Systemadministration und Security-Administration können streng getrennt werden. Die Verwendung einer eigenen Datenbank macht conpal LAN Crypt unabhängig von der Systemadministration. Die Schlüssel in der conpal LAN Crypt Administrationsdatenbank sind verschlüsselt und dadurch vor unberechtigtem Zugriff geschützt. Zusätzlich verhindert die Datenbank, dass unbeabsichtigt Änderungen vorgenommen werden (z. B. dass ein Systemadministrator ein benötigtes Sicherheitsobjekt löscht).

- Andererseits ist es oft nicht erwünscht, dass Personen, die keine Systemadministratoren sind, die Systemkonfiguration ändern können. Es liegt auf der Hand, dass es problematisch ist, Schreibrechte bei der Systemadministration zu delegieren. Auch aus dieser Sicht ist es sehr sinnvoll, die conpal LAN Crypt spezifischen Daten in einer separaten Datenbank zu speichern.

Um den bestmöglichen Schutz zu bieten, sind die conpal LAN Crypt Funktionen wiederum in zwei Bereiche gegliedert:

- conpal LAN Crypt Benutzerfunktionen
  Die conpal LAN Crypt Benutzerfunktionen enthalten die Ver- und Entschlüsselungsinformationen von Daten.
  Diese Informationen sind zur täglichen Arbeit mit conpal LAN Crypt notwendig. Sobald ein Benutzer auf die Schlüsselinformationen zugreifen kann, werden die Dateien transparent ver- bzw. entschlüsselt. Es ist ansonsten kein Benutzereingriff mehr notwendig.
  Zusätzlich bietet conpal LAN Crypt einige Anzeigefunktionen, die es dem Benutzer ermöglichen, sich “seine” Verschlüsselungsvorschriften anzeigen zu lassen.

- conpal LAN Crypt Security Officer Funktionen

Die conpal LAN Crypt Administration bietet Funktionen, die einem Security Officer vorbehalten sind.
Verschlüsselungsprofile können nur dann administriert werden, wenn man im Besitz des Security Officer-Zertifikats ist.Nur dann ist es möglich, Verschlüsselungsprofile zu erzeugen und bestehende zu verwalten.
Die conpal LAN Crypt Administration kann getrennt vom Benutzerprogramm installiert werden, da nur ein Security Officer Zugriff darauf haben sollte.
Wenn Sie conpal LAN Crypt installieren, dann können Sie die erforderlichen Komponenten auswählen (nur Administration, nur Benutzerprogramm oder beides).

1.3 Transparente Verschlüsselung

Transparente Verschlüsselung bedeutet für den Benutzer, dass alle verschlüsselt gespeicherten Daten (sei es in verschlüsselten Verzeichnissen oder Laufwerken) automatisch im Hauptspeicher entschlüsselt werden, sobald sie in einem Programm geöffnet werden. Beim Abspeichern der Datei wird diese automatisch wieder verschlüsselt.

- Alle Dateien, für die eine Verschlüsselungsregel existiert, werden automatisch verschlüsselt.
- Werden Dateien in ein verschlüsseltes Verzeichnis verschoben oder kopiert, werden sie gemäß der für dieses Verzeichnis definierten Verschlüsselungsregel verschlüsselt. Natürlich ist es möglich, verschiedene Verschlüsselungsregeln für verschiedene Dateierweiterungen oder -namen in ein und demselben Verzeichnis festzulegen. Verschlüsselung ist nicht von Verzeichnissen abhängig, sondern nur von Verschlüsselungsregeln!
- Beim Umbenennen von verschlüsselten Dateien bleiben diese verschlüsselt (sofern nicht eine andere oder keine Verschlüsselungsregel für den neuen Dateinamen oder die neue Dateierweiterung besteht).
- Kopieren oder verschieben Sie verschlüsselte Dateien an einen Ort, an dem die bisherige Verschlüsselungsregel nicht mehr gilt, bleiben die Dateien dennoch verschlüsselt, da die persistente Verschlüsselung standardmäßig aktiviert ist.
- Kopieren oder verschieben Sie verschlüsselte Dateien an einen Ort, an dem nicht mehr die bisherige Verschlüsselungsregel gilt, sondern eine andere, werden die betreffenden Dateien zuerst entschlüsselt und danach gemäß der neuen Verschlüsselungsregel wieder verschlüsselt.
- Transparente Verschlüsselung betrifft alle Arbeiten mit Dateien. Der Benutzer bemerkt nur wenig von den Ver- bzw. Entschlüsselungsvorgängen, da alle Prozesse im Hintergrund ablaufen.
- Über die persistente Verschlüsselung kann verhindert werden, dass ein Benutzer ungewollt Dateien entschlüsselt, indem er sie per Explorer in ein Verzeichnis kopiert oder verschiebt, für das keine Verschlüsselungsregel existiert. Wird die Datei außerhalb des Explorers kopiert oder verschoben, greift dieser Mechanismus nicht.

1.3.1 Zugriff auf verschlüsselte Daten

Ist der Benutzer nicht im Besitz des passenden Schlüssels, darf er nicht auf die verschlüsselten Dateien in einem Verzeichnis zugreifen. Er darf dort keine verschlüsselte Datei lesen, kopieren, verschieben, umbenennen etc.

Verfügt der Benutzer über den Schlüssel, mit dem die Dateien verschlüsselt sind, kann er, auch wenn in seinen Verschlüsselungsvorschriften keine Verschlüsselungsregel auf diese Dateien verweist, diese Dateien öffnen.

Hinweis: Beim Abspeichern von Dateien, die „nur" mit dem vorhandenen Schlüssel (keine Verschlüsselungsregel für diese Dateien) geöffnet wurden, kann es dazu kommen, dass diese unverschlüsselt angelegt werden. Dies ist bei Programmen der Fall, die beim Speichern eine temporäre Datei anlegen, die Quelldatei dann löschen und anschließend die temporäre Datei umbenennen. Da für die neu angelegte Datei keine Verschlüsselungsregel existiert, wird sie unverschlüsselt angelegt.

1.3.2 Verzeichnisse umbenennen oder verschieben

conpal LAN Crypt führt aus Performance-Gründen beim Verschieben ganzer Verzeichnisse über den Windows Explorer keine Änderung des Verschlüsselungsstatus durch. Das bedeutet, dass es beim Verschieben eines Verzeichnisses zu keiner Ver-, Ent- bzw. Umschlüsselung kommt.

Waren die Dateien verschlüsselt, bleiben sie unter dem neuen Verzeichnisnamen bzw. am neuen Speicherort verschlüsselt. Besitzt der Benutzer den entsprechenden Schlüssel, kann er wie gewohnt mit diesen Dateien arbeiten.

Sicheres Verschieben

conpal LAN Crypt unterstützt jedoch das sichere Verschieben von Dateien und Verzeichnissen. Dabei werden die Dateien auch entsprechend der geltenden Verschlüsselungsregeln bei Bedarf ver-, ent- bzw. umgeschlüsselt. Die Quelldateien werden nach dem Verschieben sicher gelöscht.

Diese Funktion steht über den Eintrag **Sicheres Verschieben** im Windows Explorer Kontextmenü zur Verfügung. Über einen Dialog kann dann ausgewählt werden, wohin die Dateien verschoben werden sollen.

1.3.3 Explizite Entschlüsselung von Dateien

Wenn eine Datei entschlüsselt werden soll, muss sie nur in ein Verzeichnis kopiert oder verschoben werden, für das keine Verschlüsselungsregel existiert. Dabei wird sie automatisch entschlüsselt.

Allerdings nur unter der Bedingung, dass

- ein entsprechendes Verschlüsselungsprofil geladen ist,
- Sie über den richtigen Schlüssel verfügen,
- im aktiven Verschlüsselungsprofil keine Verschlüsselungsregel für den neuen Ablageort existiert,
- persistente Verschlüsselung deaktiviert ist.

1.3.4 Löschen verschlüsselter Dateien - Windows Papierkorb

Wenn Ihr Verschlüsselungsprofil geladen ist, können Sie jede verschlüsselte Datei löschen, für die Sie einen Schlüssel besitzen.

Hinweis: Eigentlich handelt es sich beim Löschen von Dateien um ein Verschieben der Dateien in den Windows Papierkorb. Um den höchsten Sicherheitsstandard zu gewährleisten, bleiben die conpal LAN Crypt verschlüsselten Dateien natürlich auch im Papierkorb verschlüsselt. Um den Papierkorb zu leeren, ist kein Schlüssel notwendig.

1.3.5 Von einer Verschlüsselung ausgenommene Dateien und Verzeichnisse

Folgende Dateien und Verzeichnisse sind von einer Verschlüsselung automatisch ausgenommen (auch wenn für sie eine Verschlüsselungsregel definiert wurde):

- Dateien im Installationsverzeichnis von conpal LAN Crypt,
- Dateien im Installationsverzeichnis von Windows.
- Richtliniendatei-Cache
  Der Ablageort ist in conpal LAN Crypt Administration spezifiziert und wird in der Registerkarte **Profile** im Dialog **Status** angezeigt.
- Stammverzeichnis des Systemlaufwerks. Unterordner werden nicht ausgeschlossen
- Indizierte Speicherorte (search-ms)

1.3.6 Persistente Verschlüsselung

Für conpal LAN Crypt kann ein Security Officer die **Persistente Verschlüsselung** konfigurieren. Dateien bleiben normalerweise nur so lange verschlüsselt, wie sie einer Verschlüsselungsregel unterliegen.

Wenn zum Beispiel ein Benutzer eine verschlüsselte Datei in einen Ordner kopiert, für den keine Verschlüsselungsregel definiert ist, wird die Datei im Zielordner entschlüsselt. Durch Aktivieren

von **Persistente Verschlüsselung** können Sie sicherstellen, dass Dateien auch dannverschlüsselt bleiben, wenn sie verschoben oder kopiert werden.

Um zu verhindern, dass unerwünschte Klartextkopien von verschlüsselten Dateien erstellt werden, werden Kopien verschlüsselter Dateien auch dann verschlüsselt, wenn sie an Speicherorten erstellt werden, für die keine Verschlüsselungsregel gilt.

Security Officer können dieses Verhalten in der conpal LAN Crypt Konfiguration deaktivieren. Ist die persistente Verschlüsselung deaktiviert, so werden von verschlüsselten Dateien Klartextkopien erstellt, wenn sie an einen Speicherort kopiert/verschoben werden, für den keine Verschlüsselungsregel gilt.

Für die **Persistente Verschlüsselung** gelten folgende Regeln:

- Der conpal LAN Crypt Treiber behält nur den Namen der Datei ohne Pfadinformationen. Zum Vergleich kann nur dieser Name benutzt werden. Es werden somit nur Situationen erfasst, in denen Quell- und Zieldatei einen identischen Namen haben.Wenn die Datei während des Kopiervorgangs umbenannt wird, wird die resultierende Datei als "andere" Datei betrachtet. Sie unterliegt daher nicht der persistenten Verschlüsselung.
- Wenn ein Benutzer eine verschlüsselte Datei mit **Speichern unter** unter einem anderen Dateinamen an einem Speicherort, für den keine Verschlüsselungsregel gilt, speichert, so ist das Ergebnis eine Klartextdatei.
- Informationen zu Dateien werden nur für eine begrenzte Zeit beibehalten. Dauert der Vorgang zu lang (länger als 15 Sekunden), wird die resultierende Datei als andere, unabhängige Datei betrachtet. Sie unterliegt daher nicht der persistenten Verschlüsselung.

1.3.6.1 Persistente Verschlüsselung und Verschlüsselungsregeln

Wie bereits beschrieben, versucht die Persistente Verschlüsselung sicherzustellen, dass eine verschlüsselte Datei Ihren Verschlüsselungsstatus aufrecht erhält (zum Beispiel den ursprünglichen Verschlüsselungsschlüssel). Dies funktioniert problemlos, wenn die Datei in einen Ordner kopiert oder verschoben wird, für den keine Verschlüsselungsrichtlinie gilt. Wird die Datei jedoch an einen Speicherort kopiert oder verschoben, für den eine Verschlüsselungsrichtlinie gilt, hat die Verschlüsselungsrichtlinie höhere Priorität und setzt die **Persistente Verschlüsselung** außer Kraft Die Datei wird in diesem Fall mit dem in der Verschlüsselungsrichtlinie definierten Schlüssel verschlüsselt, nicht mit dem ursprünglich verwendeten Schlüssel.

1.3.6.2 Persistente Verschlüsselung und Ignorieren-Regeln

Eine Ignorieren-Regel setzt ebenfalls die eine Ignorieren-Regel gilt, Verschlüsselung außer Kraft.Verschlüsselte Dateien, die in einen Ordner kopiert werden, für den eine Ignorieren-Regel gilt, werden im Klartext gespeichert!

Die Ignorieren-Regel wird hauptsächlich für Dateien benutzt, auf die sehr häufig zugegriffen wird und bei denen kein bestimmter Grund für eine Verschlüsselung vorliegt. Dadurch lässt sich die System-Leistung steigern.

1.3.6.3 Persistente Verschlüsselung und Ausnahmeregeln

Eine Ausnahmeregel setzt ebenfalls die persistente Verschlüsselung außer Kraft.Verschlüsselte Dateien, die in einen Ordner kopiert werden, für den eine Ausnahmeregel gilt, werden im Klartext gespeichert!

1.3.7 Einschränkungen bei der persistenten Verschlüsselung

Aus technischen Gründen gelten für die persistente Verschlüsselung einige Einschränkungen. Das tatsächliche Ergebnis der persistenten Verschlüsselung erfüllt unter Umständen nicht immer die Erwartungen der Benutzer. In den folgenden Szenarien kann dies der Fall sein:

Dateien, die eigentlich unverschlüsselt bleiben sollten, sind verschlüsselt

- **Klartext-Dateien werden an mehrere Speicherorten kopiert, ohne dass Verschlüsselungsregeln angewendet werden.**

  Wenn eine Klartextdatei gleichzeitig an mehrere Speicherorte, von denen für einen Speicherort eine Verschlüsselungsregel gilt, kopiert wird, werden die anderen Kopien der Datei unter Umständen auch verschlüsselt, obwohl die ursprüngliche Datei nicht verschlüsselt ist. Wenn die Datei zum ersten Mal an einen verschlüsselten Speicherort kopiert wird, wird die Datei zur internen Liste des Treibers hinzugefügt. Wenn die zweite Kopie woanders erstellt wird, findet der Treiber den Dateiname in seiner Liste und verschlüsselt daher auch die zweite Kopie.

- **Nach dem Zugriff auf eine verschlüsselte Datei wird eine Datei mit dem gleichen Namen erstellt.**

  Wird kurz nach dem Öffnen einer Datei (d. h. Zugriff auf eine Datei) eine Datei mit dem gleichen Namen erstellt, wird die neu erstellte Datei mit dem gleichen Schlüssel wie die zuerst geöffnete Datei verschlüsselt.

  Hinweis: Dies gilt nur dann, wenn für das Lesen der verschlüsselten Datei und das Erstellen einer neuen Datei die gleiche Anwendung/der gleiche Thread verwendet wird.

  Typischer Anwendungsfall: Rechtsklicken Sie im Windows Explorer auf einen Ordner mit Verschlüsselungsregel und wählen Sie **Neu** > **Neues Textdokument.** Rechtsklicken Sie dann sofort in einem Ordner ohne Verschlüsselungsregel und wählen Sie **Neu** > **Neues Textdokument**. Die zweite Datei wird ebenfalls verschlüsselt.

Dateien werden nicht verschlüsselt

- **Von einer Datei werden mehrere Kopien angelegt**

  Werden Kopien von einer verschlüsselten Datei im gleichen Ordner wie die ursprüngliche Datei erstellt, so werden diese Kopien nicht verschlüsselt. Da die erstellten Kopien unterschiedliche Dateinamen haben (zum Beispiel doc.text im Gegensatz zu doc - Copy.txt), schlägt der Abgleich des Dateinamens fehl. Die Dateien werden daher nicht mit der persistenten Verschlüsselung verschlüsselt.

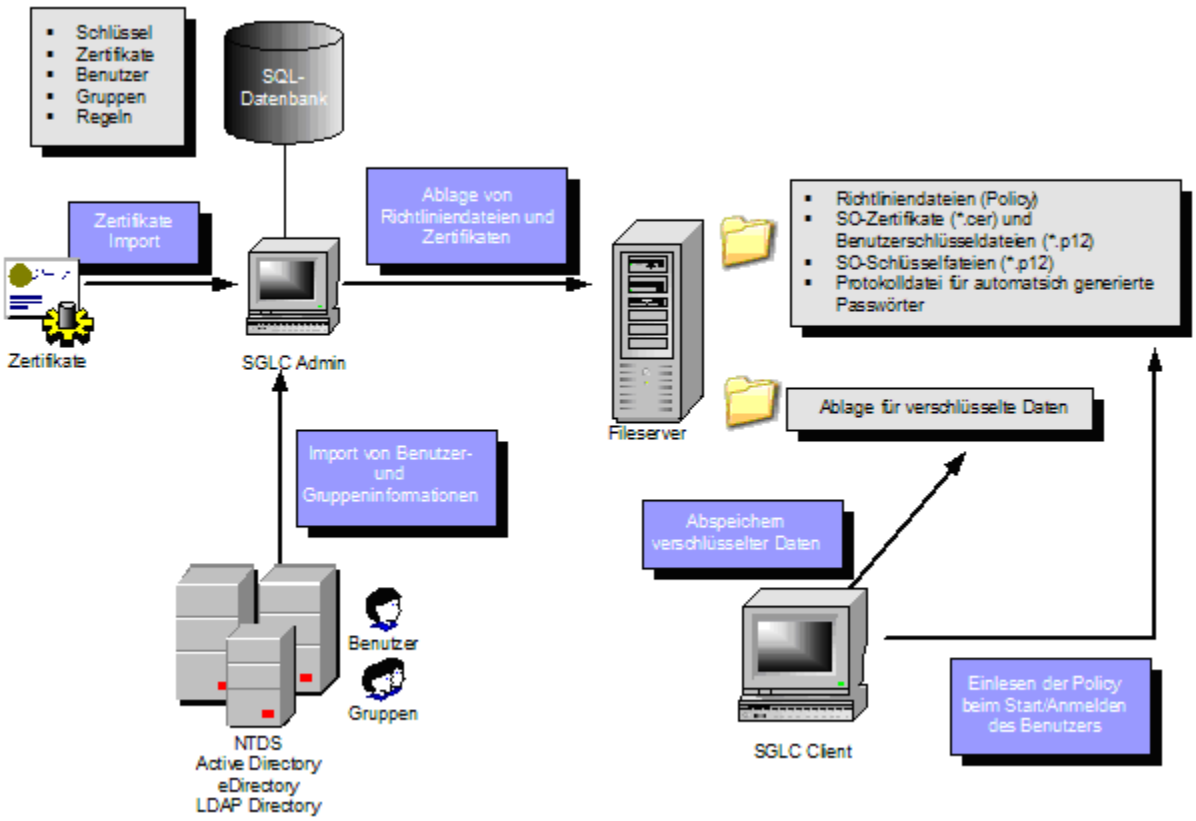
1.3.8 Client-API und Verschlüsselungs-Tags für DLP-Produkte

Identifiziert ein DLP-Produkt Daten, die verschlüsselt werden sollen, so kann es die conpal LAN Crypt Client API verwenden, um die Dateien zu verschlüsseln. In der conpal LAN Crypt Administration können Sie unterschiedliche Verschlüsselungs-Tags definieren, die den zu verwendenden conpal LAN Crypt-Schlüssel angeben.

Die Client-API kann diese vordefinierten Verschlüsselungs-Tags verwenden, um bestimmte Schlüssel auf unterschiedliche Inhalte anzuwenden wie z.B. das Verschlüsselungs-Tag <CONFIDENTIAL>, um alle Dateien zu verschlüsseln, die als vertraulich von Ihrem DLP-Produkt kategorisiert sind.

1.4 Architektur

conpal LAN Crypt besteht aus den beiden Komponenten: Der conpal LAN Crypt Administration und dem conpal LAN Crypt Client. Die Installation beider Komponenten erfolgt typischerweise auf Standard-Arbeitsplatzrechnern mit den Betriebssystemen Windows XP, Windows Vista oder Windows 7. Security Officer nutzen conpal LAN Crypt Administration zur Definition und Verteilung von Verschlüsselungsprofilen. Folgende Abbildung veranschaulicht das Zusammenspiel der einzelnen Komponenten und wie sich conpal LAN Crypt in das Unternehmensnetz integriert.



1.4.1 conpal LAN Crypt Administration

Die Administrationskomponente beinhaltet die erforderlichen Werkzeuge zur zentralen Verwaltung von conpal LAN Crypt und wird von einem oder mehreren Security Officers genutzt. Typischerweise erfolgt die Installation auf einem oder mehreren Arbeitsplatzrechnern mit Windows XP, Windows Vista oder Windows 7 als Betriebssystem. Darüber hinaus ist auch die Installation auf einem Windows 2003 Server System möglich, wenn eine zentrale Administration per Windows Terminal Services oder Citrix Metaframe gewünscht ist. Dies ist vor allem in größeren Umgebungen und insbesondere bei verteilten Standorten empfehlenswert. Der

Zugriff auf die SGLC Administration erfolgt dann per Remote Desktop (RDP) oder Independent Computing Architecture (ICA) Protokoll.

Da die Sicherheit und Vertraulichkeit der zu schützenden Daten nur dann maximal gewährleistet werden kann, wenn die SGLC Administration und Systemadministration voneinander unabhängig sind, verfügt SGLC über eine separate Benutzer- und Gruppenverwaltung. Zur Arbeitserleichterung können von conpal LAN Crypt verwaltete Benutzer und Gruppen aus einem vorhandenen Active Directory oder einem anderen LDAP-basierenden Directory importiert werden.

Die conpal LAN Crypt Administration benötigt zur Speicherung von Konfigurationsdaten und zur Verwaltung von SGLC Benutzern und Gruppen eine SQL-Datenbank. Die Datenbank kann lokal auf dem Administrationssystem installiert sein, sofern die Microsoft Express Edition zum Einsatz kommt. Für größere Installationen mit mehreren Security Officers empfiehlt sich der Einsatz eines zentralen Datenbank-Systems in Form eines Microsoft SQL beziehungsweise Oracle Servers.

Security Officer sind mit der Definition der Security Policy einer Organisation betraut. Sie legen die Policies fest und sorgen für deren Umsetzung, Einhaltung und Anpassung. Ein kleines Unternehmen kommt meist mit einem einzigen Security Officer aus. In größeren Organisationen sind häufig mehrere Security Officer gleichzeitig eingesetzt, die in der Regel auf Abteilungs- oder Standortebene arbeiten und entsprechend hierarchisch organisiert sind. Die hieraus resultierenden Hierarchieebenen lassen sich auch mit conpal LAN Crypt abbilden. An der Spitze einer Organisation stehen dabei ein oder mehrere Master Security Officer, die bei der Erzeugung der conpal LAN Crypt Datenbank anwesend sein müssen. Sie legen die ersten Policies fest und entscheiden, ob für sicherheitskritische Aktionen ein Vier-Augen-Prinzip zur Anwendung kommen muss. Jeder Security Officer erhält bestimmte Berechtigungen (Permissions) in der Administration, die seine grundsätzlichen Rechte festlegen. Zusätzlich lässt sich sein Aufgabenbereich durch Access Control Lists (ACLs) auf wenige Benutzergruppen einschränken.

conpal LAN Crypt verwaltet die Zugriffsrechte der Anwender mit Hilfe von Key Encryption Keys (KEK). Diese liegen in der SQL-Datenbank, sind verschlüsselt und sind wie alle Datenbankinhalte mit MAC- und Hashwerten vor Veränderung geschützt. Die Administration ist so ausgelegt, dass ein Security Officer nur den Namen des Schlüssels, jedoch nicht seinen tatsächlichen Wert kennen muss. So kann er mit Schlüsselobjekten arbeiten und Verschlüsselungsregeln erstellen. Durch die flexible Rechtesteuerung lassen sich verschiedenste Anwendungsszenarien abdecken. Beispielsweise können Abteilungsleiter Schlüssel definieren und Verzeichnissen zuweisen. Ein zentraler Security Officer erzeugt in einem weiteren Arbeitsgang die Verschlüsselungsprofile. So bleiben die Schlüssel unter zentraler Kontrolle.

conpal LAN Crypt kennt zwei automatisch generierte Schlüsseltypen: User- und Groupkeys. Userkeys werden pro Benutzer generiert und können für generische Verschlüsselungsregeln genutzt werden, wie z. B. die Verschlüsselung von Home Directories oder lokaler bzw. temporärer Verzeichnisse. Pro Benutzer gibt es genau einen Userkey. Für den Notfall-Recovery von per

Userkey geschützten Daten muss der Security Officer diesen Schlüssel explizit einem anderen Benutzer zuweisen. Diese Art von Recovery benötigt ein besonderes Recht in der Administration und kann an ein Vier-Augen-Prinzip gekoppelt werden, damit kein Missbrauch entsteht. Auch für Benutzergruppen steht ein ähnliches Konzept in Form von Groupkeys zur Verfügung.

Die Richtliniendateien enthalten alle Regeln, Zugriffsrechte und Schlüssel, die für die transparente Verschlüsselung benötigt werden. Bevor ein Benutzer auf seiner Arbeitsstation Daten mit conpal LAN Crypt ver- und entschlüsseln kann, muss er in der Lage sein, auf die Verschlüsselungsinformationen, die in einer Richtliniendatei gespeichert sind, zuzugreifen. Dazu erfolgt die Ablage der Richtliniendateien entweder auf einem Fileserver oder im Netlogon-Share eines Domain Controllers.

Hinweis: Eine Installation von conpal LAN Crypt Komponenten auf File-Servern oder Domain Controllern ist nicht erforderlich.

Die Richtliniendatei ist durch ein Zertifikat vor unberechtigtem Zugriff gesichert. Nur der Besitzer des Zertifikats hat Zugriff auf den zum Zertifikat gehörenden privaten Schlüssel und kann es zum Zugriff auf die entsprechenden Verschlüsselungsinformationen verwenden. Sofern selbst signierte Zertifikate zum Einsatz kommen, liegen diese ebenfalls auf einem Fileserver, auf den der Benutzer in jedem Fall Lesezugriff benötigt. Alternativ unterstützt conpal LAN Crypt auch die Verwendung von Zertifikaten auf Smartcards, USB Token oder geeigneten Hardware Boards.

Hinweis: Die Verwendung von Smartcards oder Token zur Speicherung von Zertifikaten ist keine Voraussetzung für den Einsatz von conpal LAN Crypt.

Die Pfade zu den Richtlinien (vom Standpunkt des Benutzers aus) und andere conpal LAN Crypt Einstellungen werden durch Mechanismen im Betriebssystem erkannt.

Eine conpal LAN Crypt Berechtigungsgruppe wird durch Benutzer mit demselben Verschlüsselungsprofil gebildet. In der Administration werden Richtliniendateien für jeden einzelnen Benutzer erzeugt. Alle conpal LAN Crypt Benutzer, die in ihrer Richtliniendatei dasselbe Profil gespeichert haben, sind Mitglieder einer Berechtigungsgruppe. Die Benutzer müssen sich dazu weder um die Verschlüsselung noch um den Schlüsselaustausch kümmern. Sie müssen nur in der Lage sein, auf die Richtliniendateien zuzugreifen, und ihre Dateien werden transparent ver- bzw. entschlüsselt, sobald sie geöffnet bzw. geschlossen werden.

1.4.2 conpal LAN Crypt Client

Der conpal LAN Crypt Client wird auf den Windows-Systemen (PC, Workstation, Notebook, Terminal Server) installiert, auf denen eine Verschlüsselung stattfinden soll. Die Client-Komponente bietet neben dem zur Ver- und Entschlüsselung obligatorischen Filtertreiber noch folgende optionale Komponenten:

- Explorererweiterungen zur initialen und expliziten Verschlüsselung

- Benutzerprogramm zum Laden und Löschen von Verschlüsselungsregeln, sowie Aktivieren und Deaktivieren der Verschlüsselung
- Benutzerprogramm zum Anzeigen aller am Client wirksamen Einstellungen und Regeln. Dies ist vor allem für Support-Fälle wichtig.
- Benutzerprogramm zur Initialverschlüsselung
- Token Support zur Verwendung von Token-basierten Zertifikaten für den Zugriff auf die gespeicherten Verschlüsselungsinformationen

Die Clientkomponente lädt zunächst das vom Security Officer hinterlegte Profil. Dann entschlüsselt sie dieses und ermittelt die für den angemeldeten Benutzer gültigen Verschlüsselungsregeln. Diese werden anschließend über den installierten Filtertreiber angewendet. Damit der Benutzer Zugriff auf sein Verschlüsselungsprofil hat, muss das ihm zugeordnete Zertifikat bereits auf seinem Computer vorhanden sein oder von einem Fileserver- bzw. Netlogon-Share ladbar sein. Die Zertifikate müssen von einem Security Officer zur Verfügung gestellt und vom jeweiligen Benutzer importiert werden. conpal LAN Crypt bietet darüber hinaus die Möglichkeit, das Zertifikat beim ersten Laden des Benutzerprofils automatisch zu importieren.

Der Benutzer wird aufgefordert, eine PIN für den Import des Zertifikats einzugeben. Dazu muss die PIN den Benutzern vorab vom Security Administrator mitgeteilt werden. Das Zertifikat wird bei jedem Laden des Verschlüsselungsprofils geprüft. Wird ein gültiges Zertifikat gefunden, ist der Benutzer an conpal LAN Crypt angemeldet. Ist kein gültiges Zertifikat vorhanden, kann der Benutzer nicht mit den verschlüsselten Daten arbeiten. Ist das Zertifikat auf einem von SGLC Client unterstützten hardware-basierten Token abgelegt, so ist nach dem Entsperren des Token keine weitere Benutzerinteraktion zur Ver- und Entschlüsselung erforderlich.

2 Erste Schritte

2.1 Zertifikate

conpal LAN Crypt verwendet Zertifikate und Public/Private Key Schlüsselpaare zur Sicherung der in Richtliniendateien gespeicherten Verschlüsselungsinformationen. Nur der Besitzer des Zertifikats hat Zugriff auf den zum Zertifikat gehörenden privaten Schlüssel und kann ihn daher zum Zugriff auf die Verschlüsselungsinformationen verwenden.

Welche Zertifikate verwendet werden können und woher sie kommen:

- Ein Unternehmen verfügt über eine eigene Public Key Infrastructure (PKI) oder nutzt ein Trust Center, um Zertifikate für die Benutzer zu erzeugen. Existierende Zertifikate können in diesem Fall verwendet werden.
- Die Administration von conpal LAN Crypt kann optional selbst-signierte Zertifikate erzeugen. Diese Zertifikate können ausschließlich von conpal LAN Crypt verwendet werden! Die Zertifikate sind zudem mit einer Critical Extension versehen, um anderen Applikationen anzuzeigen, dass sie nicht verwendet werden dürfen. Es handelt sich um einfache Zertifikate (vergleichbar mit Klasse-1- Zertifikaten), die aber dem X.509 Standard entsprechen.
  In conpal LAN Crypt können Sie festlegen, ob zu einem neu erzeugten Zertifikat eine Critcal Extension hinzugefügt werden soll oder nicht.

Hinweis: Einzelne Applikationen ignorieren unter Umständen diese Critical Extension der conpal LAN Crypt Zertifikate. Dies führt dann zu Problemen mit diesen selbst-signierten Zertifikaten. Deaktivieren Sie in diesem Fall explizit alle Nutzungszwecke für die conpal LAN Crypt Zertifikate über das Zertifikate-Snap-In der Microsoft Management Console, um die Verwendung des Zertifikats in anderen Applikationen zu verhindern.

Die Zertifikate werden den Benutzern in der conpal Administration zugewiesen.

Im Folgenden erhalten Sie einige wichtige Informationen zur Verwendung von Zertifikaten:

- conpal LAN Crypt verwendet das Microsoft Crypto API ausschließlich für die Zertifikatsfunktionalität.
- conpal LAN Crypt unterstützt alle Cryptographic Service Provider (CSPs), die bestimmte Standards erfüllen (z. B. RSA Schlüssellänge mindestens 1024 Bit). Dazu gehört u. a. der Microsoft Enhanced CSP.

Hinweis: Der Microsoft-Standard CSP (Microsoft Base CSP) kann nicht verwendet werden.

Sollten Sie Fragen bezüglich der Kompatibilität anderer CSPs haben, kontaktieren Sie bitte den Support.

2.1.1 Sicherheitsniveau

Da conpal LAN Crypt das höchstmögliche Sicherheitsniveau anstrebt, ist die Verwendung von starken CSPs, wie den Microsoft Strong Cryptographic Service Provider, erforderlich. Diese CSPs erlauben die Verwendung von Schlüssellängen bis zu 16384 Bit und bieten starke Verschlüsselungsalgorithmen (wie 3DES).

Des Weiteren müssen Sie beim Import eines Zertifikats über den *Zertifikatsimport-Assistent* die Option Hohe Sicherheit für den privaten Schlüssel aktivieren.

Immer wenn der private Schlüssel von einer Anwendung verwendet wird, werden Sie zur Eingabe des Kennworts aufgefordert.
Nachdem Sie im *Zertifikatsimport-Assistenten* auf **Fertigstellen** geklickt haben, wird der Dialog *Ein neuer privater Austauschschlüssel wird importiert* angezeigt. Durch Klicken auf die Schaltfläche **Sicherheitsstufe** können Sie noch einmal die Sicherheitsstufe bestimmen:

- Hoch
  Wenn Sie *Hoch* wählen, müssen Sie die Verwendung des privaten Schlüssels durch die Eingabe eines Kennworts bestätigen. Im folgenden Dialog kann dann ein neues Kennwort angegeben werden.

- Mittel
  Wenn Sie *Mittel* wählen, wird eine Meldung angezeigt, in der Sie die Verwendung des privaten Schlüssels durch Klicken auf **OK** bestätigen müssen.

Höchstes Sicherheitsniveau bei automatisch importierten Schlüsselaustauschdateien (.p12, .pfx)

conpal LAN Crypt bietet die Möglichkeit, Zertifikate automatisch zu importieren. Um bei den zu diesen Zertifikaten gehörenden privaten Schlüsseln die mittlere bzw. hoche Sicherheitsstufe anzuwenden, stellen Sie die Option **Hohe Sicherheit für den privaten Schlüssel** in der conpal LAN Crypt Konfiguration auf **Ja** ein.

Wird diese Einstellung nicht vorgenommen, wird für die so importierten Benutzerzertifikate automatisch die niedrige Sicherheitsstufe angewendet.

Auf diese Weise kann im Sinne eines unternehmensweiten Sicherheitskonzepts die verpflichtende Verwendung von Zertifikaten mit einer hohen Sicherheitsstufe durchgesetzt werden.

Hinweis: Für einen conpal LAN Crypt Benutzer bedeutet die Verwendung der höchsten Sicherheitsstufe, dass er das Kennwort für den privaten Schlüssel einmal bei der Anmeldung und immer wenn „manuell“ eine Verschlüsselungsregel geladen wird, eingeben muss.
Smartcard:
Werden auf Smartcard gespeicherte Zertifikate verwendet, so muss das Passwort nur ein Mal eingegeben werden. Solange sich die Smartcard im Kartenleser befindet, braucht das Passwort nicht erneut eingegeben zu werden.

Achtung: Wir empfehlen vor dem ersten Start der conpal LAN Crypt Administration die Aktivierung der Hohen Sicherheit für den privaten Schlüssel. Anderenfalls wird das Zertifikat des initialen Master Security Officers, wenn es von conpal LAN Crypt erzeugt wird und nicht z.B. von Smartcard importiert wird, ohne hohe Sicherheit verwendet.

Achtung: Die Pins werden von Windows standardmäßig 24 zwischengespeichert. Bei der Verwendung von Software-Zertifikaten kann dies bei der Anmeldung an die Administration und beim Ausführen einer zusätzlichen Autorisierung zu Sicherheitsproblemen führen. Es wird daher dringend empfohlen, diese Funktionalität zu deaktivieren.
Setzen Sie dafür die folgenden Werte:

```
"PrivKeyCacheMaxItems"=dword:00000000
"PrivKeyCachePurgeIntervalSeconds"=dword:00000000
```

unter den Schlüssel

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Microsoft\
Cryptography
```

In diesem Fall werden PINs für private Schlüssel nicht mehr zwischengespeichert.

Vorbedingungen zur Verwendung von Zertifikaten mit conpal LAN Crypt

- Das Zertifikat muss einen öffentlichen Schlüssel enthalten.
- Um Zugriff auf die Verschlüsselungsvorschriften zu erhalten, muss der private Schlüssel des zugewiesenen Zertifikats verfügbar sein.
- Nur Zertifikate, die unter *Benutzerkonfiguration* in den Zertifikatsspeichern *Eigene Zertifikate*, *Andere Personen* und *Active Directory-Benutzerobjekt* sowie unter *Richtlinien für Lokaler Computer* im Zertifikatsspeicher *Eigene Zertifikate* gespeichert sind, werden von conpal LAN Crypt aufgelistet. Zertifikate, die an anderen Orten gespeichert sind, werden von conpal LAN Crypt nicht berücksichtigt.
  Zertifikate können mit dem Zertifikats-Snap-In für die Management Konsole importiert und verwaltet werden.
- Zum „Verbinden“ eines Zertifikats mit den LAN Crypt Verschlüsselungsinformationen wird nur der öffentliche Schlüssel verwendet. Der private Schlüssel muss nicht bekannt sein. Der private Schlüssel bleibt immer im Eigentum des Besitzers und nur dieser ist dann imstande auf die Verschlüsselungsinformationen zuzugreifen.

Es ist empfehlenswert, die Zertifikate zur Verfügung zu haben, bevor die Installation von conpal LAN Crypt begonnen wird. Auf diese Weise werden sie sofort nach der Installation in der Microsoft Management Konsole unter *Zertifikate* angezeigt und können verwendet werden.

Hinweis: Die Verwaltung von Zertifikaten ist keine Aufgabe von conpal LAN Crypt. Die Zertifikatsverwaltung kann mittels einer firmeneigenen PKI-Infrastruktur oder mittels eines Trust Centers durchgeführt werden.

2.1.2 Zertifikatsprüfung

conpal LAN Crypt erlaubt es, eine erweiterte Zertifikatsprüfung durchzuführen. Dies bedeutet, dass Zertifikate nur akzeptiert werden, wenn Sie vollständig überprüft werden können (Auswertung einer **C**ertificate **R**evocation **L**ist).

In der conpal LAN Crypt Administration wird diese Zertifikatsprüfung für folgende Zertifikate angewendet:

- Für die Zertifikate, die beim Anlegen des initialen Master Security Officers angeboten werden. Es werden nur Zertifikate angeboten, die vollständig überprüft werden konnten.
- Für die Zertifikate, die nach der Verwendung des Wiederherstellungsschlüssels angeboten werden, um einem Security Officer ein neues Zertifikat zuzuweisen. Es werden nur Zertifikate angeboten, die vollständig überprüft werden konnten.
- Für die Zertifikate der Security Officer, die sich an die conpal LAN Crypt Datenbank anmelden. Kann das Zertifikat nicht vollständig überprüft werden, ist keine Anmeldung möglich.
- Für Zertifikate von Security Officers, die im Rahmen der zusätzlichen Autorisierung verwendet werden.

Die erweiterte Zertifikatsprüfung erfordert folgende Voraussetzungen:

- In dem verwendeten Zertifikat ist eine CRL eingetragen.
  Manche PKIs erlauben es, ein Zertifikat in eine CRL einzutragen. Ist ein solcher Eintrag vorhanden, wird diese Liste ausgewertet. Hierzu muss bei Bedarf eine CRL des Ausstellers über das Netzwerk geladen werden. Kann das Zertifikat nicht überprüft werden, wird es nicht zur Auswahl angeboten bzw. nicht zur Anmeldung akzeptiert.
- Eine CRL wurde in den lokalen Zertifikatsspeicher geladen.

Hinweis: Bitte beachten Sie, dass zur Auswertung einer CRL eine Netzwerkverbindung notwendig sein kann. Kann die Verbindung nicht hergestellt werden, so wird der Zugriff verweigert, auch wenn das Zertifikat eigentlich gültig wäre.

2.1.3 Smartcard Leser

Da die Benutzung von Zertifikaten durch die Verwendung von Cryptographic Service Providern (CSPs) abgewickelt wird, werden Smartcard-Leser automatisch unterstützt, wenn ein Smartcard-

CSP verwendet wird. Der Zugriff auf die gespeicherten Verschlüsselungsinformationen kann daher durch ein auf Smartcard gespeichertes Zertifikat abgewickelt werden.

Wenn Sie Zertifikate auf Smartcards verwenden wollen, stellen Sie bitte sicher, dass der Smartcard Leser und ein entsprechender Cryptographic Service Provider korrekt installiert sowie funktionsbereit sind!

2.2 Installation

Hinweis: Die Installation von conpal LAN Crypt ist nur möglich, wenn Sie mit Administratorrechten an dem Betriebssystem angemeldet sind.

1. Wählen Sie das Installationsverzeichnis Ihres extrahierten Installationspakets und doppelklicken Sie auf die .msi-Datei.
   Ein Installations-Assistent führt Sie durch die sehr einfache Installation von conpal LAN Crypt. Klicken Sie auf **Weiter**.

2. Der Dialog *Lizenzvertrag* wird angezeigt.
   Bitte aktivieren Sie die Option **Ich akzeptiere die Lizenzvereinbarung**. Wenn Sie dies nicht tun, ist eine Installation von conpal LAN Crypt nicht möglich! Klicken Sie auf **Weiter**.

3. Der Dialog *Zielordner* wird angezeigt.
   Wählen Sie aus, wo conpal LAN Crypt installiert werden soll.
   Klicken Sie auf **Weiter**.

4. Der Dialog *Installationsart auswählen* wird angezeigt.
   In diesem Dialog können Sie auswählen, welche Komponenten von conpal LAN Crypt installiert werden sollen. Wählen Sie **Anpassen** und klicken Sie auf **Weiter**.

Folgende Komponenten können installiert werden:

- Administration
  Installiert die conpal LAN Crypt Administration.

- **Scripting API**
  Installiert das conpal LAN Crypt Scripting API für die Script-gesteuerte Administration von conpal LAN Crypt.

5. Wählen Sie aus, welche Komponenten installiert werden sollen und klicken Sie auf **Weiter**.

6. Nachdem Sie Ihre Angaben noch einmal geprüft haben, klicken Sie auf **Weiter** im Installationsvorbereitungsdialog. Die Installation wird gestartet.

7. Bei erfolgreicher Installation erscheint ein Dialogfenster. Klicken Sie darin auf **Beenden**, um die Installation abzuschließen.

Hinweis: Um alle Einstellungen zu übernehmen, müssen Sie das System neu starten! Damit werden auch alle Treiber geladen.

2.3 Installation ohne Benutzerinteraktion

Die Installation ohne Benutzerinteraktion erlaubt die automatische Installation von conpal LAN Crypt auf einer großen Zahl von Rechnern.
Das Verzeichnis `Install` enthält die Datei `sglcadm.msi`, die für die Installation ohne Benutzerinteraktion unbedingt notwendig ist.

2.3.1 Installierbare Komponenten

Die folgende Liste zeigt alle Komponenten, die Sie installieren können und die Art und Weise, wie sie bei der Installation ohne Benutzerinteraktion angegeben werden müssen.

Die Schlüsselwörter (Courier, fett) geben an, wie die einzelnen Komponenten unter ADDLOCAL= angegeben werden müssen, wenn eine Installation ohne Benutzerinteraktion ausgeführt wird. Bei den Bezeichnungen der einzelnen Komponenten wird zwischen Groß- und Kleinschreibung unterschieden!

conpal LAN Crypt Administration - **`Administration`**

Scripting API - **`ScriptingAPI`**

Hinweis: Wenn Sie keine Komponente angeben, wird eine vollständige Installation durchgeführt.

2.3.2 Kommandozeilensyntax

Zum Ausführen einer Installation ohne Benutzerinteraktion muss `msiexec` mit bestimmten Parametern aufgerufen werden.

Unbedingt erforderliche Parameter:
`/I`
Gibt das Installations-Package an, das zu installieren ist.

`/QN`
Installation ohne Benutzerinteraktion.

Name der `.msi`-Datei: `sglcadm.msi`

Syntax:
```
msiexec /i <Pfad>\sglcadm .msi /qn
```

Optionale Parameter:
```
/Lxv <Pfad + Dateiname>
```

Protokolliert den gesamten Installationsvorgang in dem unter `<Pfad + Dateiname>` angegebenen Speicherort.

Beispiel:
`msiexec /i C:\Install\sglcadm.msi /qn`

Die Installation von conpal LAN Crypt wird ausgeführt. Das Programm wird im Standardverzeichnis (`<Systemlaufwerk>:\Programme\Sophos`) installiert. Die `.msi`-Datei befindet sich im Verzeichnis `Install` auf Laufwerk C.

2.4 Upgrade

Für einen Upgrade von älteren Versionen auf diese Version der conpal LAN Crypt Administration sind folgende Schritte notwendig:

- Installieren der neuen Version
- Upgraden der bestehenden Datenbank
- Ausführen des Upgrade-Assistenten
- Eingabe der neuen Server-Anmeldedaten bei einem Upgrade von einer Version vor 3.61.

Hinweis: Die erste Anmeldung nach einem Upgrade muss vom Master Security Officer vorgenommen werden.

2.4.1 Installieren der neuen Version

Installieren Sie die neue Version wie beschrieben.

Hinweis: Stellen Sie sicher, dass alle Instanzen der conpal LAN Crypt Administration geschlossen sind, bevor Sie die neue Version installieren..

2.4.2 Upgraden der bestehenden conpal LAN Crypt Datenbankstruktur

Mit dem Kommandozeilen-Tool `CreateTables.exe` können Sie die Struktur der Tabellen in Ihrer conpal LAN Crypt Datenbank aktualisieren. Sie finden das Tool im \Install Ordner Ihres Installationspakets.

Hinweis: Die Anmeldung an der Datenbank muss mit Berechtigungen erfolgen, die das Erzeugen und Ändern des Datenbankschemas ermöglichen.

Kommandozeilensyntax:

```
CreateTables <ODBCName[.Besitzer-Name]> <SQL-Dialekt > <Aktion>
```

`CreateTables.exe` bietet die folgenden Parameter zur Tabellenerstellung in anderen Konfigurationen:

ODBCName:
Der Name, den Sie für die ODBC- Datenquelle verwendet haben.

DatenbankbesitzerName
Damit die Datenbank korrekt angesprochen werden kann, muss für Oracle-Datenbanken der Datenbankbesitzer angegeben werden. Der Datenbankbesitzer muss unbedingt in GROSSBUCHSTABEN angegeben werden.

SQL Dialekt:
```
m ... Microsoft SQL Server
o ... Oracle 9 oder neuere Version
```

Aktionen:
```
u ... Update der Datenbankstruktur
```

Beispiel 1:
```
CreateTables SGLCSQLServer m u
```

Beispiel 2:
```
CreateTables SGLCSQLServer.SGLC o u
```

2.4.3 Upgrade-Assistent

Nach dem Upgrade der Datenbank führt Sie ein Upgrade-Assistent durch die für das Abschließen des Upgrade erforderlichen Schritte. Der Assistent wird nach der ersten Anmeldung an der aktualisierten Administration gestartet.

Hinweis: Nur ein Master Security Officer ist zur ersten Anmeldung nach dem Upgrade der Administration berechtigt. Wenn Sie nicht über die erforderlichen Rechte verfügen, wird eine entsprechende Meldung angezeigt.
Die für das Abschließen des Upgrade notwendigen Schritte können je nach Version, von der der Upgrade durchgeführt wird, variieren.

Im Assistenten führen Sie die folgenden Schritte durch:

- Eingabe eines Standorts.
- Prüfung der Datenbankintegrität und gegebenenfalls Fehlerbehebung.
  Es werden Informationen zu allen korrigierten Fehlern angezeigt.
- Erstellen eines neuen Wiederherstellungsschlüssels

Nach Beenden des Assistenten kann die Administration benutzt werden.

2.4.4 Server-Anmeldeinformationen für Versionen vor 3.61

Nach einem Upgrade müssen die Anmeldeinformationen erneut unter *Zentrale Einstellungen* auf der *Server*-Seite eingegeben werden. Wenn Sie einen **Microsoft-Verzeichnisdienst** verwenden, gehen Sie folgendermaßen vor:

- Geben Sie den `Domänennamen` unter *Domänen- oder Servernamen* ein.
- Geben Sie den *Benutzernamen* als `Benutzername@Domänenname` ein.

2.5 Deinstallation

Hinweis: Die Deinstallation von conpal LAN Crypt ist nur möglich, wenn Sie mit Administratorrechten am Betriebssystem angemeldet sind.

1. Klicken Sie auf **Start**, **Systemsteuerung**, **Software - Programme ändern oder entfernen**.
2. Wählen Sie aus der Liste der installierten Programme **conpal LAN Crypt Administration** .
3. Klicken Sie auf **Entfernen**, um conpal LAN Crypt Administration zu deinstallieren.
4. Bestätigen Sie den Warnhinweis mit **OK**, wenn Sie conpal LAN Crypt Administration tatsächlich deinstallieren möchten.
5. Führen Sie einen Neustart des Systems aus, um die Deinstallation abzuschließen.

Hinweis: Bei der Deinstallation von conpal LAN Crypt bleibt der Inhalt der conpal LAN Crypt Datenbank erhalten. Diese muss bei Bedarf gesondert mit Mitteln des Betriebssystems bzw. des Datenbankadministrationswerkzeugs gelöscht werden.

3 Administration

Die conpal LAN Crypt Administration fügt sich nahtlos in Microsofts Management Konsole (MMC) ein und bietet einem Security Officer eine vertraute Benutzerschnittstelle mit den typischen MMC Funktionen.
Die Administration wurde entwickelt, um die Vorteile bestehender Windows Replikationsmechanismen nutzen zu können. Dies ermöglicht eine sehr hohe Effizienz und die Reduktion der Gesamtkosten (TCO), da Kunden, die viele Arbeitsstationen zu verwalten haben, in der Regel nur ein System zur Verwaltung ihrer Arbeitsstationen einsetzen wollen.

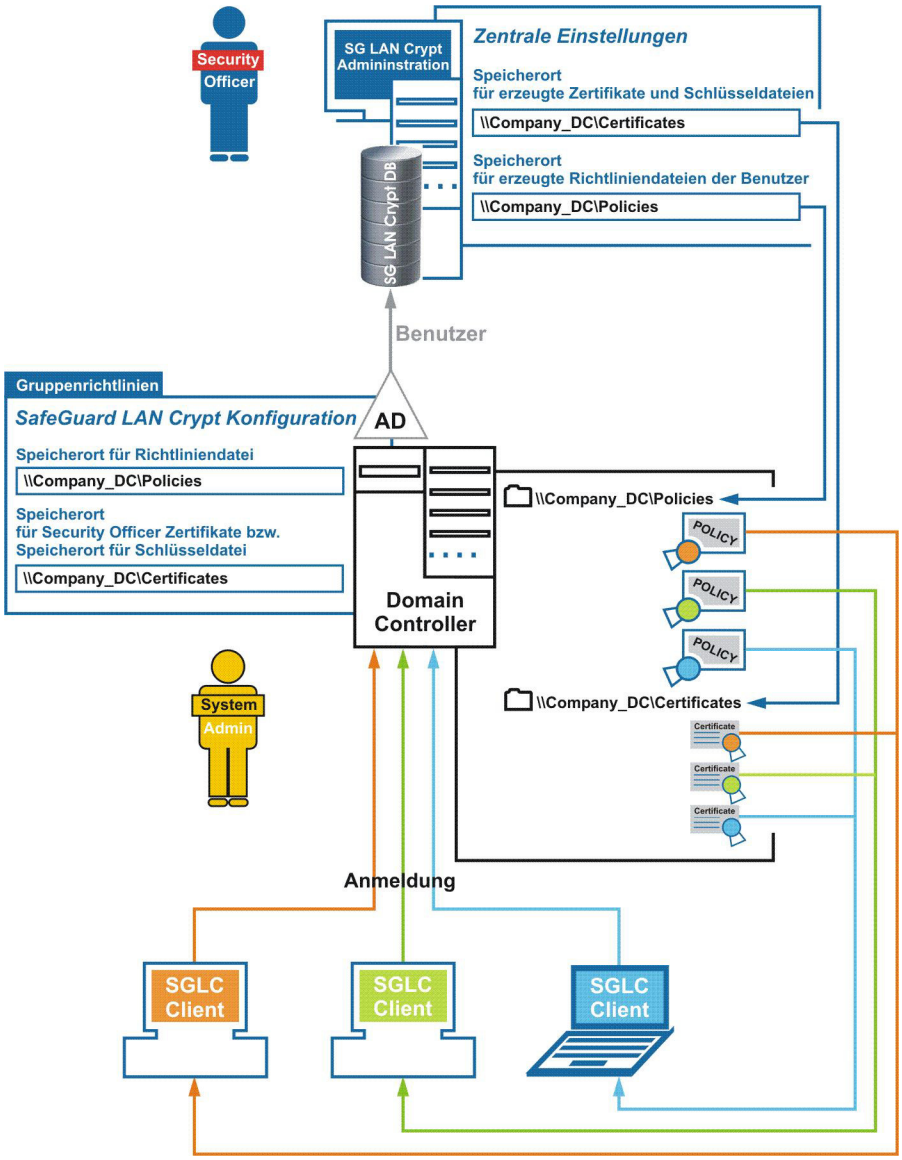
Die Administration von conpal LAN Crypt findet in der Regel auf einem eigenen Administrationsrechner statt, von dem aus auf die benötigten Verzeichnisdienste und auf die conpal LAN Crypt Datenbank zugegriffen wird.

conpal LAN Crypt verwendet das Security Officer-Konzept. Zu Beginn steht ein **Master Security Officer**, der die conpal LAN Crypt Administrationskonsole installiert. Bei der Installation können bereits Speicherorte für von conpal LAN Crypt erzeugte Zertifikate und Schlüsseldateien (der öffentliche Teil des Security Administrator Zertifikats und .p12 Dateien, die die Zertifikate der Benutzer enthalten und auf den Clients importiert werden) angegeben werden. Nach der Installation der Administration wird ein Speicherort für die Richtliniendateien der Benutzer definiert. Die Richtliniendateien werden in der conpal LAN Crypt Administration für jeden einzelnen Benutzer erzeugt und enthalten die Verschlüsselungsinformationen.

Zertifikate, .p12 Dateien und Richtliniendateien werden später von den conpal LAN Crypt Clients automatisch aus den angegebenen Verzeichnissen importiert.

Dazu ist es notwendig, dass die Clients Zugriff auf diese Verzeichnisse haben. Aus diesem Grund definieren **Master Security Officer** und **Systemadministrator** gemeinsam Verzeichnisse, in denen diese Dateien gespeichert werden (in der Regel sind dies freigegebene Netzwerk-Shares).

Die Clients erhalten die Information, wo sich diese Dateien befinden, über Gruppenrichtlinien bei der Anmeldung an einen Domain Controller. Die Speicherorte der Dateien müssen vom Systemadministrator in der conpal LAN Crypt Konfiguration eingetragen werden. Die conpal LAN Crypt Konfiguration wird in der für die Benutzer gültigen Gruppenrichtlinie vorgenommen.



Die conpal LAN Crypt Clients benötigen keine Verbindung zur conpal LAN Crypt Datenbank. Bei der Anmeldung erhalten sie die Information, wo die jeweiligen Zertifikate, .p12 Dateien und Richtliniendateien zu finden sind, über Gruppenrichtlinien. Danach werden diese Dateien automatisch auf die Clients übertragen.

Für den Import des Zertifikats benötigt der Benutzer ein Passwort. Bei durch LAN Crypt erzeugten Zertifikaten wird das Passwort in der Datei p12pwlog.csv gespeichert, und kann z. B. über PIN-Mailer an die Benutzer verteilt werden.

3.1 Notwendige Schritte

- Vorarbeiten:
  - Optional: Installation des mitgelieferten Datenbanksystems
  - Datenquelle (ODCB) hinzufügen
  - Datenbanktabellen erzeugen (CreateTables.exe)
- Systemadministrator: Einstellungen in der conpal LAN Crypt Konfiguration vornehmen.
- Initialen Master Security Officer anlegen

  Angaben des Speicherortes
  - für von conpal LAN Crypt erzeugte Zertifikate und Schlüsseldateien

Achtung: Aus diesem Verzeichnis werden später die Benutzerzertifikate (.p12-Dateien) und der öffentliche Teil des Security Officer- Zertifikats von den Clients importiert. Daher sollte zu diesem Zeitpunkt bereits ein mit dem Systemadministrator definiertes Verzeichnis feststehen (Netzwerk-Share).

  - für von conpal LAN Crypt erzeugte SO Zertifikate
  - für die Protokolldatei für automatisch generierte Passwörter der Schlüsseldateien.
- Zentrale Einstellungen definieren

  Hier geben Sie an, wo die für die Benutzer erzeugten Richtliniendateien gespeichert werden sollen. Sprechen Sie sich mit dem **System Administrator** ab, um diesen Schritt umzusetzen.

Hinweis: Bei der Verwendung von Oracle-Datenbanken sollten, wenn von verschiedenen Administrationsstationen auf die Datenbank zugegriffen wird, jetzt auch die Code Page Einstellungen vorgenommen werden (siehe *Datenbank* auf Seite 60).

- Weitere Security Officer anlegen
- Rechte für die Security Officer definieren
- Objekte (Organisationseinheiten, Gruppen, Benutzer) aus dem Verzeichnis (z. B. Active Directory) importieren
- Den Organisationseinheiten Security Officers zuordnen und deren Rechte festlegen
- Schlüssel anlegen
- Verschlüsselungsregeln anlegen
- Zertifikate erzeugen bzw. zuweisen
- Richtliniendateien erzeugen

3.2 Vorarbeiten für die Administration von conpal LAN Crypt

Nach der Installation sind folgende Schritte notwendig, bevor Sie mit der Administration von conpal LAN Crypt beginnen können:

- Optional: Datenbankverwaltungssystem installieren
  Dies ist nur notwendig, wenn Sie nicht selbst über ein Datenbanksystem verfügen, aus dem Sie eine Datenbank für die Administration von conpal LAN Crypt verwenden wollen.
  Für diesen Fall wird mit conpal LAN Crypt ein frei verwendbares Datenbanksystem ausgeliefert, das Sie für die Administration verwenden können. Es handelt sich dabei um die Microsoft SQL Server 2008 R2 Express Edition.
  Darüber hinaus unterstützt conpal LAN Crypt folgende Datenbanksysteme:
  - Microsoft SQL Server 2005
  - Microsoft SQL Server 2005 Express
  - Microsoft SQL Server 2008 R2
  - Microsoft SQL Server 2008 R2 Express
  - Oracle*9i*
  - Oracle*10g*
  - Oracle11

Hinweis: Kommt eine Oracle-Datenbank zum Einsatz, ist für die conpal LAN Crypt Administration die Installation eines Oracle-Client notwendig. Bei Wahl der Oracle-Clientvariante "Laufzeit" ist die Installation des Oracle ODBC-Treiber erforderlich.
Microsoft ODBC für Oracle wird von conpal LAN Crypt nicht unterstützt.
Achten Sie darauf, dass Sie bei der Erzeugung von Datenbankobjekten keine vom jeweiligen Hersteller reservierten Schlüsselwörter verwenden.

- Datenquelle angeben (ODBC)
  Wenn Sie ein eigenes Datenbanksystem verwenden, müssen Sie die Zugangsdaten für die entsprechende Datenbank für die Angabe der Datenquelle kennen.

- Datenbanktabellen erzeugen
  Nach dem Angeben der Datenquelle müssen Sie mit einem mitgelieferten Tool (CreateTables.exe) die conpal LAN Crypt Tabellen in der Datenbank erzeugen.

3.2.1 Installation des mitgelieferten Datenbanksystems

Die folgende Beschreibung bezieht sich auf die Microsoft SQL Server 2008 R2 Express Edition. Für diese beispielhafte Beschreibung werden soweit wie möglich die Voreinstellungen dieser Version verwendet.

Gehen Sie für die Installation des Datenbanksystems folgendermaßen vor:

1. Doppelklicken Sie im „\INSTALL“-Verzeichnis Ihres Installationspakets auf die Datei SQLEXPR32_x86_ENU.exe.

Hinweis: Wenn Sie ein 64 Bit Betriebssystem verwenden, laden Sie bitte die 64 Bit Version von Microsoft SQL Server 2008 R2 Express Edition von www.microsoft.com herunter.

2. Akzeptieren Sie die Lizenzbestimmungen und klicken Sie auf **Weiter**.

3. Die Installationsdateien werden extrahiert und ein Installationsassistent wird gestartet.

4. Folgen Sie den Anweisungen des Installationsassistenten und übernehmen Sie alle Voreinstellungen.

Voreinstellungen: Die folgenden Beschreibungen der Vorarbeiten beziehen sich auf diese Voreinstellungen. Sollten Sie Änderungen vornehmen (Authentisierungsmethode, Datenbankinstanz) müssen Sie diese bei der Angabe der Datenquelle und dem Erzeugen der Dantenbanktabellen berücksichtigen.

Datenbankauthentisierung: Standardmäßig arbeitet die Express Edition mit Windows-Authentisierung.
Diese wiederum setzt voraus, dass der Benutzer, der sich an der Datenbank anmeldet, über Windows-Administratorrechte verfügt.

Master-Datenbank: Standardmäßig wird bei der Angabe der Datenquelle die vorhandene Master-Datenbank verwendet. Im Allgemeinen empfehlen wir, NICHT die Master-Datenbank zu verwenden, da diese beim Upgrade der Express Edition oder der SQL Server Version unter Umständen Probleme verursacht.

Sie können eine separate Datenbank für conpal LAN Crypt erstellen und diese beim Hinzufügen der Datenquelle angeben. Für die Microsoft SQL Server 2008 R2 Express Edition können Sie mit dem folgenden Kommando auf der Kommandozeile eine Datenbank erstellen:

osql -E -S .\SQLEXPRESS -Q “CREATE DATABASE <Name_der_Datenbank>“
Es wird eine Datenbank mit dem angegebenen Namen und mit Windows-Authentisierung erstellt.
Mit dem Parameter -U können Sie zum Beispiel einen Benutzernamen für die Authentisierung angeben. Um alle Parameter anzeigen zu lassen, geben Sie osql -? ein.

Sie können auch Microsoft SQL Server 2008 R2 Management Studio Express herunterladen.Diese Programm steht kostenlos zur Verfügung und kann zum Erstellen einer separaten Datenbank verwendet werden.

Im nächsten Schritt muss eine Datenquelle angegeben werden, damit conpal LAN Crypt das Datenbanksystem benutzen kann.

3.2.2 Datenquelle (ODBC) hinzufügen

Hinweis: Die Datenquelle muss mit dem 32 Bit ODBC Data Source Administrator hinzugefügt werden.Dieser ist auch bei 64 Bit Systemen verfügbar. Wenn Sie ein 64 Bit System benutzen, starten Sie den ODBC Data Source Administrator über Start\Alle Programme\Sophos\conpal LAN Crypt \ODBC Data Source Administrator (x86). Damit stellen Sie sicher, dass die richtige Version gestartet wird.

Damit conpal LAN Crypt die Datenbank über das Datenverwaltungssystem verwenden kann, muss dem System die Datenquelle mitgeteilt werden. Dies erfolgt über den ODBC-Datenquellen-Administrator.

ODBC (Open Database Connectivity) ermöglicht den Zugriff auf Daten aus den unterschiedlichsten Datenbankverwaltungssystemen. Verfügen Sie beispielsweise über ein Programm für den Zugriff auf Daten in einer SQL-Datenbank, bietet Ihnen ODBC die Möglichkeit, mit demselben Programm auf Daten in einer anderen Datenbank zuzugreifen. Hierzu müssen Sie dem System Softwarekomponenten, die so genannten Treiber, hinzufügen. ODBC unterstützt Sie beim Hinzufügen und Konfigurieren dieser Treiber.

Zum Hinzufügen der Datenquelle

1. Klicken Sie auf Start\Systemsteuerung\Verwaltung\Datenquellen (ODBC).
   Der ODBC-Datenquellen-Administrator wird gestartet.

2. Wählen Sie den Reiter System-DSN aus und klicken Sie auf **Hinzufügen**.
   Mithilfe dieser Registerkarte werden Datenquellen mit System-Datenquellennamen (DSN) hinzugefügt. Diese Datenquellen sind lokal auf einem Computer gespeichert, jedoch nicht einem bestimmten Benutzer zugewiesen; jeder Benutzer mit entsprechenden Berechtigungen kann einen System-DSN verwenden.

3. Wählen Sie als Treiber, für den Sie die Datenquelle erstellen wollen, **SQL Server** aus und klicken Sie auf **Fertig stellen**.

Hinweis: Wenn SQL Server Native Client in der Liste verfügbar ist, wählen Sie diesen Eintrag aus.

4. Geben Sie im nächsten Dialog als Namen, mit dem Sie auf die Datenquelle verweisen wollen, **SGLCSQLServer** ein.
   Der Name für den Verweis auf die Datenquelle ist in der conpal LAN Crypt Konfiguration einstellbar. In der Standardeinstellung wird **SGLCSQLServer** verwendet. Wenn Sie einen anderen Namen verwenden wollen, muss dieser in der Konfiguration angegeben werden.

Hinweis: Der Name der ODBC Quelle unterscheidet nach Groß-/Kleinschreibung! Er muss hier genauso angegeben werden wie er in der conpal LAN Crypt Konfiguration angegeben wird. Sie müssen den Namen in der Konfiguration angeben, bevor die conpal LAN Crypt Administration das erste Mal gestartet wird.

5. Wählen Sie unter *Server* aus, mit welchem Server die Verbindung hergestellt werden soll und klicken Sie auf **Weiter**.

6. Verwenden Sie im nächsten Dialog die Standardeinstellungen. Durch die Wahl der Option **Mit Windows NT-Authentifizierend anhand des Benutzernamens im Netzwerk** werden die Windows Benutzerdaten zur Anmeldung an das Datenbanksystem verwendet. Eine Eingabe des Passwortes ist nicht notwendig.
   Klicken Sie auf **Weiter**.

7. Bestätigen Sie im nächsten Dialog die Standardeinstellungen.
   Dadurch wird die bereits existierende Master-Datenbank verwendet.
   Sollten Sie eine eigene Datenbank erzeugt haben, muss diese hier ausgewählt werden.

8. Belassen Sie im nächsten Dialog die Standardeinstellungen und klicken Sie auf **Fertig stellen**.

3.2.3 Tabellen in der conpal Datenbank erzeugen

Mit dem Kommandozeilen-Tool `CreateTables.exe` können Sie die erforderlichen Tabellen in Ihrer conpal LAN Crypt-Datenbank anlegen. Sie finden das Tool im Install -Verzeichnis Ihres extrahierten Installationspakets..

Hinweis: Die Anmeldung an der Datenbank muss mit Berechtigungen erfolgen, die das Erzeugen und Ändern des Datenbankschemas ermöglichen.

So erzeugen Sie die Tabellen in Ihrer Datenbank:

1.) Geben Sie auf der Kommandozeile folgendes ein: `CreateTables SGLCSQLServer m c.`

Wenn Sie die Installation mit den Voreinstellungen vorgenommen haben, ist das Datenbanksystem nun fertig konfiguriert. Sie können nun die conpal LAN Crypt Administration starten.

3.2.3.1 CreateTables Kommandozeilensyntax

```
CreateTables <ODBCName[.Besitzer-Name]> <SQL-Dialekt > <Aktion>
```

`CreateTables.exe` verfügt für das Erzeugen der Tabellen in unterschiedlichen Konfigurationen über folgende Parameter:

ODBCName:
Der Name, den Sie für die ODBC- Datenquelle verwendet haben.

DatenbankbesitzerName
Damit die Datenbank korrekt angesprochen werden kann, muss für Oracle-Datenbanken der Datenbankbesitzer angegeben werden. Der Besitzer der Datenbank muss unbedingt in GROSSBUCHSTABEN angegeben werden.

SQL Dialekt:
```
m ... Microsoft SQL Server
o ... Oracle 9 oder neuere Version
```

Aktionen:
```
c ... Alle Tabellen erzeugen
```

Beispiel 1:
```
CreateTables SGLCSQLServer m c
```

Beispiel 2:
```
CreateTables SGLCSQLServer.SGLC o c
```

3.3 Master Security Officer

conpal LAN Crypt verwendet das Security Officer-Konzept. Am Beginn steht ein Master Security Officer, der in weiterer Folge Aufgaben delegieren kann, indem er weitere Security Officers (eventuell auch weitere Master Security Officers) anlegt und diese mit bestimmten Rechten für die Administration von conpal LAN Crypt ausstattet. Der zuerst angelegte Master Security Officer kann zusätzliche Security Officer anlegen.

Die Rechte der von einem Master Security Officer angelegten Security Officers, werden über ACLs definiert. Die einzelnen Security Officers können dann verschiedenen Organisationseinheiten in der zentralen Administration zugeordnet werden. Deren Rechte beziehen sich dann ausschließlich auf die Organisationseinheit der sie zugeordnet wurden. Diese Rechte werden in der Organisationshierarchie nach unten weitervererbt, bis an einem Punkt andere Rechte festgelegt werden.

Nachdem das Datenbanksystem und die Datenquelle vorbereitet wurden, wird beim ersten Starten der Administration von conpal LAN Crypt, ein initialer **Master Security Officer** angelegt.
Ein Master Security Officer ist immer mit allen zur Verfügung stehenden Rechten ausgestattet.

Achtung: Beim Anlegen dieses initialen Master Security Officers wird auch der Speicherort für von conpal LAN Crypt erzeugte Zertifikate und Schlüsseldateien angegeben. Dort wird auch der öffentliche Teil des Security Officer Zertifikats gespeichert, der von den Clients benötigt wird. Aus diesem Verzeichnis werden später auch die Benutzerzertifikate (.p12-Dateien) von den Clients importiert. das Verzeichnis, dass Sie mit dem **System Administrator** definiert haben, sollte nun verfügbar sein (Netzwerk-Share).

Alle Einstellungen, die Sie beim Anlegen des initialen Master Security Officers vornehmen, können Sie später in der conpal LAN Crypt Administration unter *Zentrale Einstellungen* ändern.

3.3.1 Initialer Master Security Officer

Nach dem ersten Start der Administration (Programme/Sophos/conpal/LAN Crypt/SGLC Administration) wird nach der Anmeldung an die Datenbank der Assistent zum Anlegen des initialen Master Security Officers angezeigt, mit dessen Hilfe Sie in vier Schritten diesen Master Security Officer anlegen.

Geben Sie im ersten Dialog des Assistenten die Daten für den initialen Master Security Officer ein. Der hier eingetragene Name wird als Common Name im Zertifikat eingetragen, wenn Sie von conpal LAN Crypt erzeugte Zertifikate verwenden.
E-Mail Adresse und Kommentar sind optional. Klicken Sie auf **Weiter**.

Hinweis: Die E-Mail-Adresse wird auch in die Passwortprotokolldatei für von conpal LAN Crypt erzeugte Zertifikate eingetragen. So kann sie z. B. für die Erstellung eines PIN Mailers via E-Mail verwendet werden.

Im zweiten Dialog des Assistenten werden der Speicherort für

- erzeugte Zertifikate und Schlüsseldateien (.p12)
- für erzeugte Security Officer Zertifikate und
- die Protokolldatei für automatisch generierte Passwörter der erzeugten Schlüsseldateien angegeben.

Speicherort für erzeugte Zertifikate und Schlüsseldateien

conpal LAN Crypt kann bei Bedarf selbst-signierte Zertifikate erzeugen. Diese Zertifikate (.p12-Dateien) werden bei der Zuweisung der Zertifikate an die Benutzer erzeugt. Der Ort, wo diese Dateien gespeichert werden sollen, muss im zweiten Dialog des Assistenten angegeben werden.

Auch der öffentliche Teil des Security Officer Zertifikats (.cer), mit dem die Administrationsdatenbank gesichert ist, wird hier gespeichert.

Die Schlüsseldateien (.p12) und der öffentliche Teil des Security Officer Zertifikats müssen den Benutzern zur Verfügung gestellt werden.

Dazu kann in der conpal LAN Crypt Konfiguration eingestellt werden, in welchem Verzeichnis conpal LAN Crypt nach einer .p12 Datei für den Benutzer sucht, falls der private Schlüssel für die Richtliniendatei nicht vorhanden ist. Gleiches gilt für den öffentlichen Teil des Security Officer Zertifikats.

Wird eine entsprechende .cer Datei, die den öffentlichen Teil des Security Officer Zertifikats enthält, gefunden, wird diese automatisch importiert.

Hinweis: Um die beschriebene Funktionalität zu verwenden, müssen die entsprechenden Pfade in der conpal LAN Crypt Konfiguration gesetzt sein.

Als Alternative dazu können die Schlüsseldateien der Benutzer und der öffentliche Teil des Administratorzertifikats auch manuell verteilt werden. Stellen Sie in diesem Fall sicher, dass beide von den Clients importiert werden.

Hinweis: Auf den Clients muss immer der öffentliche Teil des Zertifikats jenes Security Officers importiert werden, von dem die Richtliniendateien erzeugt werden.
Wird der Pfad, wo die .cer-Dateien der Security Officers und die .p12-Dateien der Benutzer gespeichert werden, nach dem Anlegen der Security Officers geändert, müssen diese in das neue Verzeichnis kopiert werden. Die öffentlichen Teile der Zertifikate können ansonsten nicht gefunden werden. Die .p12-Dateien der Benutzer müssen natürlich ebenfalls unter dem „neuen" Pfad erzeugt werden.

Speicherort für erzeugte Security Officer Zertifikate

conpal LAN Crypt speichert, z. B. für Backup-Zwecke, Security Officer Zertifikate in .p12 Dateien. Das Verzeichnis, in dem diese Zertifikate gespeichert werden, kann hier angegeben werden.

Hinweis: Da es sich hierbei um sensible Daten handelt, müssen diese unbedingt vor unberechtigtem Zugriff geschützt werden!

Datei für Passwortprotokoll

Hier kann Speicherort und Name für die Protokolldatei der generierten PKCS#12 Dateien angegeben werden (Standardname:p12pwlog.csv). Diese Datei enthält die Passwörter der erzeugten PKCS#12 Dateien und kann z. B. für die Erstellung eines PIN-Briefs verwendet werden.

Hinweis: Diese Datei sollte geschützt werden und unter keinen Umständen im gleichen Verzeichnis wie die POL-Dateien gespeichert werden.
Mit conpal LAN Crypt können Sie die Datei für das Passwortprotokoll auf einfache Art und Weise schützen. Installieren Sie hierzu Administration und Client auf demselben Computer. Erstellen Sie nach dem Anlegen des initialen Master Security Officer eine Verschlüsselungsregel, durch die die Datei für das Passwortprotokoll verschlüsselt wird, erzeugen Sie ein Profil für den ersten MSO und laden Sie das Profil. Der verwendete Verschlüsselungsschlüssel sollte nur den MSOs und den Security Officern zur Verfügung stehen, die das Recht haben, Zertifikate zu erzeugen.
Durch Ausführen des Assistenten zur Initialverschlüsselung wird die Datei für das Passwortprotokoll verschlüsselt. Um sicherzustellen, dass das Passwort für den initialen MSO nicht manipuliert wurde, als die Datei noch nicht verschlüsselt war, erstellen Sie ein neues Zertifikat und ordnen Sie es dem initialen MSO zu.

Hinweis: Wenn der Benutzer, der die Zertifikatszuordnung durchführt, im Dateisystem kein Recht hat, die Passwortprotokolldatei zu ändern, können keine conpal LAN Crypt Zertifikate erzeugt werden.

Klicken Sie auf **Weiter**.

Zertifikatsgültigkeit

Im dritten Dialog des Assistenten können Sie die Gültigkeitsdauer für die von conpal LAN Crypt erzeugten Zertifikate angeben und dem Security Officer ein bereits existierendes oder ein von conpal LAN Crypt erzeugtes Zertifikat zuweisen.

Wenn Sie zur Sicherung der Daten dieses Security Officers ein von conpal LAN Crypt erzeugtes Zertifikat verwenden, wird es mit dieser Gültigkeitsdauer erzeugt.
Alle weiteren mit conpal LAN Crypt erzeugten Zertifikate besitzen ebenfalls diese Gültigkeitsdauer.

Zertifikat des initialen Security Officers

Sie müssen ein Verschlüsselungszertifikat auswählen, mit dem die Daten des Security Officers gesichert werden. Optional können Sie zusätzlich ein Signaturzertifikat auswählen, mit dem sich der Security Officer gegenüber der conpal LAN Crypt Administration authentifiziert. Geben Sie kein Signaturzeritfikat an, wird das Verschlüsselungszertifikat auch zur Authentisierung herangezogen.

Klicken Sie auf die **Suchen** Schaltfläche, um ein bestehendes Zertifikat auszuwählen, bzw. ein neues von conpal LAN Crypt erzeugen zu lassen.

Hinweis: Wenn Sie ein bereits vorhandenes Zertifikat verwenden wollen, müssen Sie dieses jetzt zur Verfügung haben. Falls Sie mit einem Software-Zertifikat arbeiten, muss sich dieses im Zertifikatsspeicher befinden. Ist das Zertifikat auf einem Token gespeichert, muss dieser mit dem System verbunden sein. Zum Importieren des Zertifikats klicken Sie auf die Schaltfläche **Zertifikat Importieren**.

Klicken Sie im angezeigten Dialog auf **Neues Zertifikat**. Wählen Sie das neue Zertifikat aus der Liste aus und klicken Sie auf **OK**.

Klicken Sie auf **Weiter**.

Im vierten Dialog des Assistenten können Sie optional eine Region mit einem entsprechenden Prefix angeben. Der Prefix wird beim Erzeugen der Schlüssel dem Schlüsselnamen vorangestellt. Es wird immer der Prefix jener Region verwendet, die dem Security Officer zugeteilt ist, der den Schlüssel erzeugt. Aufgrund des Prefix ist dann immer eindeutig ersichtlich, für welche Administrationseinheit der Schlüssel verwendet werden soll. In den zentralen Einstellungen für die Administration können später weitere Regionen erstellt werden und dann den verschiedenen Security Officers zugeteilt werden. Diese Vorgehensweise ist speziell für verteilte Umgebungen gedacht.

Die Angabe eines Standorts ist zwingend. Der Standort wird benötigt, um bei der Protokollierung von conpal LAN Crypt bei der Verwendung von verteilten Datenbanken die Einträge eindeutig zuordnen zu können.

Sie müssen einen Standort eintragen, auch wenn Sie keine verteilte Datenbank verwenden. Nur so stellen Sie sicher, dass Einträge eindeutig zugeordnet werden, falls die Datenbank später auf verschiedene Standorte
verteilt wird.

Nach dem Klicken auf **Fertig stellen** wird der initiale Master Security Officer angelegt und der Dialog zur Anmeldung an die conpal LAN Crypt Administration wird angezeigt.

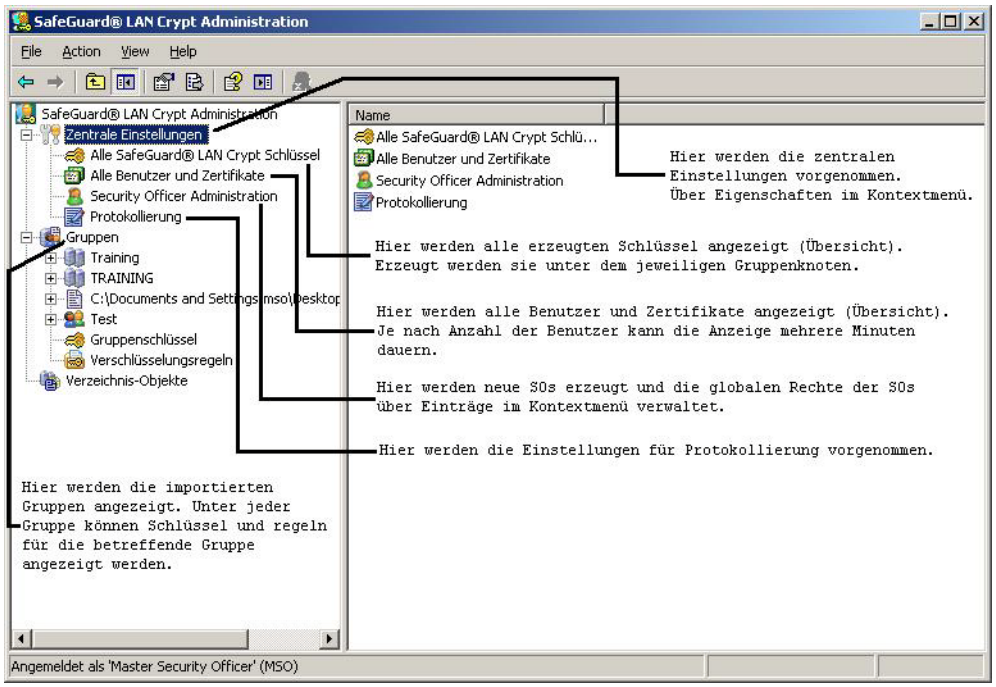
In diesem Dialog werden später alle Security Officers, die das Recht haben, sich an die conpal LAN Crypt Administrationsdatenbank anzumelden, angezeigt.

Markieren Sie in diesem Dialog den neu angelegten Master Security Officer und klicken Sie auf **OK**. Die conpal LAN Crypt Administration wird geöffnet.

Hinweis: Nach der Anmeldung werden Sie in einem Dialog darauf hingewiesen, dass noch kein Wiederherstellungsschlüssel erzeugt wurde. Ohne ein Wiederherstellungszertifikat ist bei einem Notfall (z. B. wenn kein Zertifikat zur Anmeldung zur Verfügung steht) das Risiko eines vollständigen Datenverlusts sehr hoch.
Dieser Dialog wird bei der Anmeldung eines Master Security Officers angezeigt, bis ein Wiederherstellungsschlüssel erzeugt wurde. Durch Aktivieren der Option **Diese Warnung nicht mehr anzeigen** kann die Anzeige des Dialogs unterdrückt werden, auch wenn kein Wiederherstellungsschlüssel erzeugt wurde.

3.4 Administration: Überblick

Bei der Installation von conpal LAN Crypt wird die Datei **SGLCAdmin.msc** im Installationsverzeichnis von conpal LAN Crypt angelegt. Über das Windows-Start-Menü (Start/Programme/ ...) kann durch Klicken auf diesen Eintrag ein Fenster der Management Konsole geöffnet werden, das nur die für die Administration von conpal LAN Crypt notwendigen Snap-Ins enthält.



Das Snap-In für die conpal LAN Crypt Administration kann auch der Standardansicht der Management Konsole hinzugefügt werden (Datei/Snap-In hinzufügen/entfernen - conpal LAN Crypt Administration). Beim Hinzufügen ist bereits das Passwort für die conpal LAN Crypt Administrationsdatenbank notwendig.

Wer ist angemeldet:
In der Statuszeile wird der aktuell angemeldete Security Officer angezeigt. Aiußerdem sehen Sie, ob es sich um einen Master Security Officer oder einen Security Officer handelt.

Symbolleiste in der Administration

conpal LAN Crypt stellt für viele seiner Funktionen Symbole in der Symbolleiste der Management Konsole zur Verfügung. Art und Anzahl der Symbole in der Symbolleiste sind anhängig vom jeweils markierten Knoten.

Alle Funktionen, die über diese Symbole auswählbar sind, können auch über das entsprechende Kontextmenü durchgeführt werden.

Über einen Klick mit der rechten Maustaste auf den Knoten **conpal LAN Crypt Administration** können Sie sich die Eigenschaften des Knotens anzeigen lassen und diese bei Bedarf anpassen. Eine Beschreibung der Eigenschaften können Sie den folgenden Abschnitten entnehmen.

3.4.1 Bestätigungen

Sie haben in der conpal LAN Crypt Administration die Möglichkeit einzustellen, welche Aktionen vor der Ausführung bestätigt werden müssen. Klicken Sie dazu auf **Eigenschaften** im Kontextmenü des *conpal LAN Crypt Administration* Basisknotens. Ein Dialog zeigt diese Optionen an.

Wenn Sie hier eine Aktion markieren, muss Sie vor der Ausführung in einem Dialog bestätigt werden.
Erst nach der Bestätigung wird die Aktion tatsächlich ausgeführt.

- Gruppenreferenz erstellen bestätigen
  Das Hinzufügen einer Gruppenreferenz zu einer anderen Gruppe muss bestätigt werden. Gruppe markieren > rechte Maustaste > Kopieren > andere Gruppe auswählen > rechte Maustaste > Einfügen > Bestätigung

Hinweis: Alle Kopier-; Ausschneide- und Einfügeoperationen sind sowohl über die Kontextmenüs als auch mit der Maus über Drag&Drop oder Drag&Drop + STRG möglich.

- **Gruppenreferenz erstellen bestätigen**
  Das Erstellen einer Gruppenreferenz zu einer anderen Gruppe muss bestätigt werden.
- **Gruppen in andere Gruppen verschieben bestätigen**
  Das Verschieben einer Gruppe in eine andere Gruppe muss bestätigt werden.
- **Gruppe aus Datenbank löschen bestätigen**
  Das Löschen einer Gruppe muss bestätigt werden.
- **Shortcut aus Gruppe entfernen bestätigen**
  Das Entfernen einer Gruppenreferenz muss bestätigt werden.
- **Alle Shortcuts aus Gruppe entfernen bestätigen**
  Wenn es eine Referenz von einer Gruppe zu einer anderen Gruppe gibt, z.B. eine Verknüpfung von Gruppe 1 und Gruppe 2 in Gruppe 3, so muss das Löschen dieser Referenz bestätigt werden. (Gruppe3 auswählen > rechte Maustaste > **Referenz entfernen** auswählen).
- **Shortcut aus Gruppe entfernen bestätigen**
  Das Löschen von Schlüsseln, die bereits in einer Regel verwendet und anschließend deaktiviert wurden, muss bestätigt werden. Bereits verwendete Schlüssel sind in der Administration entsprechend markiert und verbleiben in der Datenbank auch wenn sie aus der Gruppe entfernt werden. Schlüssel, die noch nicht verwendet wurden, werden beim Entfernen aus einer Gruppe auch aus der Datenbank gelöscht.
- **Schlüssel aus Gruppe hinzufügen bestätigen**
  Schlüssel die in einer Regel verwendet und anschließend aus allen Gruppen entfernt wurden, verbleiben in der Datenbank und werden unter *Zentrale Einstellungen > Alle conpal LAN Crypt-Schlüssel* angezeigt. Von dort können sie wieder über Drag&Drop zu einer Gruppe hinzugefügt werden. Diese Aktion muss bestätigt werden.

- **Schlüsselreferenz in Gruppe erzeugen bestätigen**
  Das Hinzufügen einer Schlüsselreferenz zu einer Gruppe (z.B. einen Schlüssel über Drag&Drop in eine andere Gruppe ziehen) muss bestätigt werden. Schlüssel werden immer kopiert oder referenziert. Ausschneiden ist nicht möglich.

- **Schlüsselreferenz aus Gruppe entfernen bestätigen**
  Das Entfernen einer Schlüsselreferenz aus einer Gruppe muss bestätigt werden.

Welcher Security Officer ist angemeldet

Darüber hinaus ist in diesem Dialog sichtbar, welcher SO an die conpal LAN Crypt Administration angemeldet ist. Der aktuelle SO wird unter den Aktionen, für die eine Bestätigung verlangt werden kann, angezeigt.
Welcher SO angemeldet ist, wird auch in der Statuszeile der conpal LAN Crypt Administration angezeigt.

3.4.2 Benutzereinstellungen

Über den Reiter **Benutzereinstellungen** können Sie die Darstellung von Informationen in der conpal LAN Crypt Administration beeinflussen.

Aktivieren Sie

- *Name der Domäne zum Gruppennamen hinzufügen*, um in der conpal LAN Crypt Administration die Zuordnung zwischen conpal LAN Crypt Gruppen und Domänen dargestellt zu bekommen. Diese Option ist insbesondere dann hilfreich, wenn conpal LAN Crypt für mehrere unterschiedliche Domänen zum Einsatz kommt.

- *Ausgewählte Benutzer und Zertifikate' anzeigen*, um sich unter dem Knoten *Zentrale Einstellungen* in conpal LAN Crypt alle importierten Benutzer und deren Zertifikate anzeigen zu lassen. Beachten Sie, dass das Anzeigen aller Benutzer und Zertifikate bei größeren Installationen einen Zeitraum von mehreren Minuten in Anspruch nehmen kann. Damit Änderungen an der Option *Ausgewählte Benutzer und Zertifikate anzeigen* wirksam werden, müssen Sie die conpal LAN Crypt Administration neu starten.

- Den Benutzern übergeordnete Objekte anzeigen, um sich unter dem Knoten *Mitglieder und Zertifikate für Gruppe* die Parent-Gruppe des jeweiligen Benutzers anzeigen zu lassen. Damit können Sie auf einen Blick erkennen, ob die conpal LAN Crypt Datenbank Benutzer enthält, die keiner Gruppe zugeordnet sind. Damit Änderungen an der Option *Parent der Benutzer anzeigen* wirksam werden, müssen Sie die conpal LAN Crypt Administration neu starten.

- *Zwischenspeichern von Benutzerlisten deaktivieren*
  Zur Perfomance-Steigerung baut conpal LAN Crypt standardmäßig Benutzerlisten im Hintergrund auf und setzt den Aufbau auch fort, wenn der Anwender zu anderen Knoten in der Administration wechselt. Die Ergebnisse des Listenaufbaus werden zwischengespeichert,

so dass ein erneuter Abruf dieser Liste keinen Datenbankzugriff erfordert. Dies ist bei umfangreichen Listen sehr zeitsparend.
Dies führt unter Umständen in Umgebungen mit mehreren parallelen conpal LAN Crypt Administratoren (Terminal Server) zu einem erhöhten Speicherverbrauch. Um das zu verhindern, kann diese Option aktiviert werden. Dadurch werden die Listen nicht zwischengespeichert und der Listenaufbau wird beim Verlassen des Knotens abgebrochen. Es wird empfohlen, diese Option nur dann zu aktivieren, wenn tatsächlich Probleme mit Speicherknappheit auftreten.
Innerhalb einer Sitzung werden Änderungen in der Datenbank nicht automatisch in eine aufgebaute Liste übernommen.
Eine Aktualisierung kann jederzeit durch Drücken von F5 vorgenommen werden.

Hinweis: Änderungen an den oben genannten Einstellungen werden nicht in der Datenbank hinterlegt. Dies sind persönliche Einstellungen, deren Speicherung für jeden Benutzer individuell im Snap-In der Microsoft Management Console erfolgt.

3.5 Zentrale Einstellungen

Für den Knoten *Zentrale Einstellungen* können Sie verschiedene Eigenschaften für die conpal LAN Crypt Administration zentral festlegen.

Klicken Sie dazu auf **Eigenschaften** im Kontextmenü des Knotens *Zentrale Einstellungen*. Alternativ können Sie auch das Symbol 'Eigenschaften' in der SGLC-Administrationssymbolleiste anklicken. Sie können die Eigenschaften anschließend über mehrere Reiter einsehen und bei Bedarf anpassen.

Hinweis: Die Reiter **Zusätzliche Autorisierung**, **Wiederherstellungsschlüssel** und **Regionen** sind nur für Master Security Officer sichtbar.
Die Reiter **Server** und **Konfiguration** sind nur sichtbar und der Reiter **Verzeichnisse** bearbeitbar, wenn der Security Officer das globale Recht Konfiguration ändern besitzt. Die Reiter **Algorithmen** und **Zertifikate** sind ausschließlich für den Master Security Officer bearbeitbar. Nur Master Security Officers können Änderungen in den Reitern **Algorithmen**, **Zertifikate** und **Regeln** auflösen vornehmen.

3.5.1 Algorithmen

conpal LAN Crypt bietet folgende Verschlüsselungsalgorithmen an:

- **AES-128**
- **AES-256**
- **3DES**

- **DES** (nicht empfohlen)
- **IDEA**
- **XOR** (nicht empfohlen)

Wählen Sie aus, welche Algorithmen Sie verwenden wollen. Die hier ausgewählten Algorithmen stehen Ihnen später beim Erzeugen der verschiedenen Schlüssel zur Verfügung.

Hinweis: Werden diese Einstellungen später geändert (z. B. DES wird aus der Liste der verfügbaren Algorithmen gestrichen) sind bereits erzeugte Schlüssel und damit verschlüsselte Daten davon nicht betroffen.
Die betroffenen Algorithmen stehen dann nur bei der Erzeugung neuer Schlüssel nicht mehr zur Verfügung.

Standard Algorithmus

Wählen Sie hier aus, welcher Algorithmus für die automatische Erzeugung von Benutzer -und Gruppenschlüsseln verwendet werden soll.

3.5.2 Schlüssel

Schlüssel

Bei der Zusammenführung mehrerer conpal LAN Crypt Installationen z. B. im Rahmen von Firmenverschmelzungen oder Abteilungszusammenlegungen kann es zu Problemen mit doppelten internen Schlüsselnamen kommen.
Aus diesem Grund werden Schlüssel über eindeutige Global Unique IDs (GUID) identifiziert. Die GUID wird standardmäßig von conpal LAN Crypt nach einem Zufallsprinzip generiert und lässt sich nachträglich nicht ändern.

Falls jedoch zwischen zwei Unternehmen ein Austausch von Dateien stattfinden soll, die per conpal LAN Crypt verschlüsselt wurden, wird eine Möglichkeit benötigt, einen gemeinsamen Schlüssel zu erzeugen.
Nur so ist sicherzustellen, dass eine Datei, die von Unternehmen A mit dem Beispielschlüssel CRYPTOKEY verschlüsselt wurde, von Unternehmen B entschlüsselbar ist. Voraussetzung dafür ist, dass Unternehmen B ebenfalls einen Schlüssel namens CRYPTOKEY erzeugt, der über dieselben Einstellungen verfügt, wie der Schlüssel von Unternehmen A.
Dies beinhaltet auch die GUID des Schlüssels.

Für einen solchen Fall bietet conpal LAN Crypt die Möglichkeit, bei der Erzeugung eines neuen Schlüssels die GUID manuell einzugeben. Hierfür muss die Option **Security Officers dürfen die GUID neuer Schlüssel festlegen** aktiviert werden.

Schlüsselwert

Durch Aktivieren der Option **Nur Security Officer mit dem Recht 'Profile erzeugen' dürfen Schlüssel erzeugen** (**Schlüsselohne Wert *are not* nicht zulassen**) können Sie sicherstellen, dass nur Security Officers, die die Rechte *Schlüssel erzeugen* und *Profile erzeugen* besitzen, Schlüssel (Namen und Wert) erzeugen können.

conpal LAN Crypt bietet die Möglichkeit, Schlüssel ohne Wert zu erzeugen. Mit diesen Schlüsseln kann in der Administration uneingeschränkt gearbeitet werden. Die Werte werden erst beim Erzeugen der Richtliniendateien generiert. Bei verteilten Datenbanken kann dies jedoch zu Problemen führen. Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre, Wenn in einem Replikationszeitfenster an verschiedenen Standorten Richtliniendateien erzeugt werden, die Schlüssel ohne Wert enthalten (manuelle angelegte Schlüssel ohne Wert, Gruppenschlüssel <GROUPKEY>). Bei Erzeugen der Richtliniendateien würde an jedem Standort ein eigener Wert für den Schlüssel erzeugt. Ergebnis wäre ein Schlüssel mit zwei unterschiedlichen Werten.

Wird die Option **Nur Security Officer mit dem Recht "Profile erzeugen" dürfen Schlüssel erzeugen** (**Schlüsselohne Wert nicht*are not* zugelassen**) aktiviert (Schlüssel ohne Wert sind nicht zugelassen), können nur Security Officer, die die Rechte *Schlüssel erzeugen* und *Profile erzeugen* besitzen, Schlüssel erzeugen. Es ist nicht mehr möglich, Schlüssel ohne einen Wert zu erzeugen. Wird dem Schlüssel vom Security Officer beim Anlegen kein Wert zugewiesen, wird der Wert beim Speichern des Schlüssels automatisch generiert.

Für Gruppenschlüssel, deren Werte erst beim Erzeugen der Richtliniendateien generiert werden würden, werden die Werte ebenfalls sofort erzeugt, wenn sie beim Anlegen einer Verschlüsselungsregel verwendet werden.

Ist diese Option aktiviert, können Security Officers, die das Recht *Profile erzeugen* nicht besitzen, keine Schlüssel mehr anlegen.

Die Verwendung von Gruppenschlüsseln (<GROUPKEY>) in Verschlüsselungsregeln ist für diese Security Officers ebenfalls nicht mehr möglich.

Hinweis: Die Option **Nur Security Officer mit dem Recht "Profile erzeugen" dürfen Schlüssel erzeugen** (**Schlüsselohne Wert sind nicht erlaubt**) beeinflusst die Verwendung von benutzerspezifischen Schlüsseln (<USERKEY>) in Verschlüsselungsregeln nicht!

3.5.3 Zertifikate

Auf dieser Seite können Sie Schlüssellänge für neu erzeugte Zertifikate (1024, 2048, 4096 Bit) und die Gültigkeitsdauer für die von conpal LAN Crypt erzeugten Zertifikate festlegen.

Unter Anzeigename für neu erzeugte Zertifikate können Sie einen Namen für von conpal LAN Crypt erstellte Zertifikate angeben. Alle Zertifikate erhalten diesen Namen und können daher leicht als conpal LAN Crypt Zertifikate identifiziert werden.

Wenn Sie die Option **Kritische Erweiterung zu neu erzeugten Zertifikaten hinzufügen** wählen, wird zu neu erzeugten Zertifikaten eine Critical Extension hinzugefügt, die anderen Anwendungen zeigt, dass Sie diese Zertifikate nicht verwenden dürfen.

Sie können eine Frist in Tagen bestimmen, innerhalb der eine Warnung (beim Auflösen der Regeln, oder als gelbe Markierung in der Liste der Zertifikate) ausgegeben wird, dass das Zertifikat ablaufen wird.

3.5.4 Regeln auflösen

Benutzer ohne zugeordnetes Zertifikat immer überspringen

("Zurücksetzen" bedeutet in diesem Abschnitt "ignorieren", wenn es sich auf Regeln bezieht). Aktivieren Sie diese Option, wenn Benutzer, denen kein Zertifikat zugewiesen wurde, beim Erzeugen der Richtliniendateien übersprungen werden sollen. Für diese Benutzer wird dann keine Richtliniendatei erzeugt.

Hinweis: Wird ein Benutzer hinzugefügt, wenn diese Option aktiviert ist und dem Benutzer wurde noch kein Zertifikat zugewiesen, erfolgt keine Warnung, wenn für diesen Benutzer beim Auflösen der Verschlüsselungsregeln keine Richtliniendatei angelegt werden konnte.

Wählen Sie aus, wie die Regeln auf dem Client gereiht werden sollen:

Hinweis: Diese Einstellung wird nur auf Clients ab Version 3.90 angewendet.

Hier können Sie aus drei verschiedenen Sortiermethoden wählen. Sortiermethode 3 ist die Standardmethode, die von Client-Versionen vor Version 3.90 verwendet wird.

- **Sortiermethode 1**
  1. Ignorieren-Regeln
  2. Ausschließen-Regeln
  3. Verschlüsselungsregeln

- **Sortiermethode 2**
  1. Ignorieren-Regeln
  2. Ausschließen-Regeln
  3. Als absolute Pfade definierte Verschlüsselungsregeln ohne Platzhalter
  4. Als absolute Pfade definierte Verschlüsselungsregeln mit Platzhaltern, ohne Unterordner
  5. Als absolute Pfade definierte Verschlüsselungsregeln mit Platzhaltern, mit Unterordnern
  6. Alle anderen Verschlüsselungsregeln

  Ein absoluter Pfad wird entweder als UNC Pfad (mit doppeltem Backslash zu Beginn) oder als <Laufwerksbuchstabe>:\ angegeben.
  Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre, \\server\share *.* oder c:\encrypt *.*.

- **Sortiermethode 3 (Standard)**
  Die Sortiermethode 3 unterscheidet nicht zwischen Ignorieren-Regeln, Ausschließen-Regeln und Verschlüsselungsregeln.
  Die Regeln werden in der folgenden Reihenfolge sortiert:
  1. Alle absoluten Pfade ohne Platzhalter
  2. Alle absoluten Pfade mit Platzhaltern, ohne Unterordner
  3. Alle absoluten Pfade mit Platzhaltern, mit Unterordnern
  4. Alle anderen Regeln

  Ein absoluter Pfad wird entweder als UNC Pfad (mit doppeltem Backslash zu Beginn) oder als <Laufwerksbuchstabe>:\ angegeben.
  Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre, \\server\share *.* oder c:\encrypt *.*.

Innerhalb der oben angegebenen Abschnitte (zum Beispiel: Sortiermethode 3 - Alle anderen Regeln), richtet sich die Sortierung danach, wie präzise die Pfaddefinition ist.

Hier gilt folgende Reihenfolge:
1. UNC-Pfade
2. Pfade, die mit <Laufwerkbuchstabe> beginnen: Hier wird der Backslash nach dem Laufwerksbuchstaben nicht berücksichtigt.
2. Alle anderen Pfade
Außerdem gilt:
- Pfade mit mehr Backslashes werden vor Pfaden mit weniger Backslashes aufgelistet
- Pfade ohne Platzhalter werden vor Pfaden mit den Platzhaltern *. und *.* aufgelistet

Hinweis: Änderungen an dieser Option werden auf den Clients wirksam, nachdem neue Profile generiert und verteilt wurden.

Wählen Sie aus, welches Verschlüsselungsformat vom conpal LAN Crypt Client verwendet werden soll

Hier können Sie den Verschlüsselungsmodus konfigurieren, den die Clients verwenden sollen. conpal LAN Crypt unterstützt folgende Verschlüsselungsmodi:

- CBC-Format (Versionen 3.50 oder höher)
  Dieses Format wird von Clients ab Version 3.50 oder höher verwendet. Diese Clients können Dateien lesen, die im OFB-Modus (Format von Vorgängerversionen) verschlüsselt sind. Für neue Dateien wird der Verschlüsselungsmodus CBC verwendet.

- XTS-AES-Format (Versionen 3.90 oder höher)
  Dieses Format kann von Clients ab Version 3.90 oder höher verwendet werden. Diese Clients können Dateien lesen, die im OFB und im CBC-Modus verschlüsselt sind. Für neue Dateien wird der Verschlüsselungsmodus XTS-AES verwendet. Dieser Modus wird nur für AES-Schlüssel verwendet. Wird eine Datei mit einem Schlüssel, der einen anderen Algorithmus verwendet, verschlüsselt, so wird der CBC-Verschlüsselungsmodus stattdessen verwendet.

Für Client-Versionen vor Version 3.90 ist nur die folgende Konfiguration gültig:
CBC-Format zur Verschlüsselung mit optionaler Anwendung des Formats von Vorgängerversionen als "altes Verschlüsselungsformat". Alle anderen Einstellungen werden von diesen Clients ignoriert. Sie verwenden standardmäßig das CBC- oder das Format von Vorgängerversionen.

Dieses Verschlüsselungsformat bis zu folgendem Datum verwenden

Während eines Upgrade-Vorgangs kann ein alter Verschlüsselungsmodus konfiguriert werden. Dieser alte Verschlüsselungsmodus ist bis zu einem angegebenen Datum aktiv. Ab diesem Datum müssen alle Clients migriert werden, damit sie den konfigurierten Verschlüsselungsmodus unterstützen. Andernfalls legen neue Clients zwar verschlüsselte Dateien im konfigurierten Verschlüsselungsmodus an, diese Dateien können jedoch nicht von älteren Clients gelesen werden.

Je nach Einstellung für das zu verwendende Verschlüsselungsformat, können die folgenden Formate hier ausgewählt werden:

- **Format von Vorgängerversionen** (**Versionen 2.x, 3.0x, 3.1x**)
- **CBC-Format** (**Versionen 3.50 oder höher**)
  ist nur verfügbar, wenn XTS-AES als Verschlüsselungsformat konfiguriert ist.

Für CBC ist eine Client-Version ab Version 3.90 oder höher erforderlich. Ältere Clients werten die Einstellung **Dieses Verschlüsselungsformat bis zu folgendem Datum verwenden** nur dann aus, wenn **Format von Vorgängerversionen** ausgewählt ist.

Sie müssen festlegen, bis zu welchem Datum die verschlüsselten Dateien im alten Format geschrieben werden. Wird dieses Datum überschritten, oder die Option deaktiviert, werden die Dateien im neuen Format geschrieben. Änderungen an dieser Option werden auf den Clients erst nach dem Erzeugen und Verteilen neuer Profile wirksam.

Nach der Aktualisierung aller Clients empfehlen wir, eine Initialverschlüsselung mit dem Initialverschlüsselungs-Tool durchzuführen. Damit stellen Sie sicher, dass ausschließlich das neue Verschlüsselungsformat von conpal LAN Crypt verwendet wird

Diese Änderungen werden beim nächsten Auflösen der Verschlüsselungsregeln wirksam.

3.5.5 Server

Zum Importieren der Gruppen und Benutzer von einem Server, benötigt conpal LAN Crypt die Anmeldeinformationen für diesen Server. Diese Informationen müssen im Register Server angegeben werden. Klicken auf **Hinzufügen** öffnet einen weiteren Dialog mit drei Reitern: *Details*, *Einstellungen* und *Zertifikate*

Server-Details: Anmeldung mit Passwort

1. Geben Sie *Domänen- oder Servername*, *Benutzername* und das entsprechende *Passwort* ein. Geben Sie bitte zur Vermeidung doppelter Einträge auch einen alternativen Namen als *Alias* für den Server an, falls der Server durch mehrere Namen angesprochen werden kann.

Hinweis: Wenn Sie einen **Microsoft-Verzeichnisdienst** verwenden, gehen Sie folgendermaßen vor:

- Geben Sie den `Domänennamen` unter *Domänen- oder Servernamen* ein.
- Geben Sie den *Benutzernamen* als `Benutzername@domain`. an.

Hinweis: Der Benutzername muss in LDAP- Syntax (kanonischer Name) angegeben werden, um Objekte aus einem Verzeichnisdienst, der nicht von Microsoft stammt, zu importieren.
Beispiel: `cn=admin,O=techops`

2. Geben Sie die zu benutzende API an.
   Wählen Sie <Microsoft> oder <andere> aus der Drop-down-Liste. Der Platzhalter <andere> steht für alle Nicht-Microsoft-APIs.

3. Geben Sie die LDAP Authentisierungsmethode an, die für den Zugriff auf den Server benutzt werden soll. SafeGuardLAN Crypt bietet folgende Methoden:
   - Passwort (LDAP)
   - Passwort (LDAP mit SSL)

4. Klicken Sie auf **OK**.

▶ Der Server wird in der Tabelle auf dem Reiter *Server* angezeigt.

Fehlermeldung beim Fehlschlagen der Anmeldung
Wenn conpal LAN Crypt die Anmeldung an den Server nicht durchführen kann, wird eine Fehlermeldung in der conpal LAN Crypt Administration angezeigt.

Server Details: Anonyme Anmeldung

1. Geben Sie den *Servernamen* ein. Geben Sie bitte zur Vermeidung doppelter Einträge auch einen alternativen Namen als *Alias* für den Server an, falls der Server durch mehrere Namen angesprochen werden kann.

2. Geben Sie die zu benutzende API an.
   Wählen Sie <Microsoft> oder <andere> aus der Drop-down-Liste. Der Platzhalter <andere> steht für alle Nicht-Microsoft-APIs.

3. Geben Sie die LDAP Authentisierungsmethode an, die für den Zugriff auf den Server benutzt werden soll. SafeGuardLAN Crypt bietet folgende Methoden für die anonyme Anmeldung:

- Anonym (LDAP)
- Anonym (LDAP mit SSL)

4. Klicken Sie auf OK.

▶ Der Server wird in der Tabelle auf dem Reiter *Server* angezeigt.

Fehlermeldung beim Fehlschlagen der Anmeldung
Wenn conpal LAN Crypt die Anmeldung an den Server nicht durchführen kann, wird eine Fehlermeldung in der conpal LAN Crypt Administration angezeigt.

Einstellungen

Identifizierung der Objekte

conpal LAN Crypt identifiziert importierte Objekte im Active Directory anhand einer eindeutigen, immer gleich bleibenden GUID (Global Unique ID). Diese GUID wird auch bei der Synchronisation von Datenbank und Verzeichnisdienst verwendet, da z. B. die Namen der einzelnen Objekte sich ändern können, um sicherzustellen, dass Änderungen im Active Directory auch in die Datenbank übernommen werden und nicht aufgrund des neuen Namens in der Datenbank ein neues Objekt erzeugt wird.

Einige andere Verzeichnisdienste verwenden diesen ID-Typ jedoch nicht. In diesem Fall stellt conpal LAN Crypt eine andere Methode zur eindeutigen Identifizierung von Objekten zur Verfügung. conpal LAN Crypt kann so konfiguriert werden, dass bestimmte LDAP-Attribute zur eindeutigen Identifizierung der Objekte verwendet werden. Die zu verwendeten Attribute können in der conpal LAN Crypt Administration frei konfiguriert werden.

Die Einstellungen `<Standard>` und `<Andere>` stehen immer zur Verfügung. Im Normalfall wird die Einstellung `<Standard>` für den Server, auf den sich die Einstellung bezieht, ausreichen. Unter `<Standard>` werden jeweils die Attribute angezeigt, die bei Einstellung `<Standard>` ausgewertet werden. Einerseits wird dadurch angezeigt, welche Attribute in der Standardeinstellung ausgewertet werden. Andererseits können Sie ein spezifisches Attribut angeben, sofern dieses Attribut im betroffenen Verzeichnisdienst existiert. Über `<Andere>` können andere, als die zur Auswahl stehenden Attribute angegeben werden.

Achtung: Wenn Sie hier ein Attribut angeben, müssen Sie sicherstellen, dass dieses Attribut auch Daten enthält, die eine eindeutige Identifizierung ermöglichen.

- **Objekt GUID**

  Hier können Sie einstellen, welches Attribut zur Identifizierung verwendet wird.
  Belassen Sie die Einstellung auf `<Standard>`, so werden beide Attribute `GUID` und `objectGUID` ausgewertet.
  Wenn Sie ein anderes LDAP-Attribut zur Identifizierung der Objekte verwenden wollen, wählen Sie `<Andere>` unter *Object GUID* und geben Sie im Eingabefeld daneben den Namen

des LDAP-Attributs an. Dieses Attribut muss Daten enthalten, die eine eindeutige Identifizierung des Objekts erlauben.

- **GUID Attribut ist ein binärer Wert**

  Diese Option hat nur Auswirkungen für die Darstellung der GUID in den *Eigenschaften* Dialogen der Objekte. Damit diese korrekt dargestellt werden, sollten Sie diese Option aktivieren, wenn es sich bei der verwendeten GUID um einen binären Wert handelt.
  Im Zweifelsfall aktivieren Sie bitte diese Option.

Attribute für Benutzer

- **Attribut für Benutzernamen**
  Diese Einstellung wirkt sich nur auf die Anzeige der Benutzer in der conpal LAN Crypt Administration aus. Die Benutzer werden im Dialog *Eigenschaften* einer Gruppe und im Snap-In *Benutzer und Zertifikate* angezeigt.
  Sie können eines der vorgegebenen Attribute auswählen oder durch Auswahl von <Andere> ein LDAP-Attribut angeben.
  `<Standard>` wertet (`CN` und `SN`) aus.

- **Attribut für Logonname**
  Dem Attribut für den Logonnamen kommt besondere Bedeutung zu. conpal LAN Crypt benennt die Richtliniendateien nach dem Logonnamen der Benutzer. Nur wenn Logonname und Name der Richtliniendatei identisch sind, kann sich der Benutzer anmelden.
  Hier können Sie bestimmen durch welches LDAP-Attribut der Logonname des Benutzers festgelegt wird.
  `<Standard>` wertet`SAMAccountName`, `userPrincipalName` und `UID` aus. Sollten zwei oder drei dieser Attribute im Verzeichnisdienst existieren, können Sie eines auswählen, das den Logonnamen des Benutzers bestimmt.
  `<Andere>` ermöglicht die Angabe eines weiteren Attributs, das im Verzeichnisdienst den Logonnamen enthält.

Hinweis: Sollte der Name im Attribut das @-Zeichen enthalten, trennt conpal LAN Crypt den Namen an dieser Stelle ab. Dies kann z. B. bei der Verwendung von E-Mail-Adressen zu Problemen führen.

- **Attribut für E-Mail Adresse**

  Dieses Attribut wird in selbsterzeugte Zertifikate eingefügt.

- **Attribut für Kommentar**

  Dieses Attribut kann wie die E-Mail Adresse zur Identifizierung der Benutzerobjekte verwendet werden. Das ist vor allem hilfreich, wenn Benutzername und Logonname nicht zur Objektidentifizierung beim Assistenten zur Zertifikatszuordnung geeignet sind. Der Name des Attributs anhand dessen der zugehörige Benutzer vom Assistenten zur Zertifikatszuordnung

gefunden werden soll, kann hier eingetragen werden.

Hinweis: Werden bei einer Synchronisierung leere Attribute importiert (wenn z. B. ein Attribut im AD gelöscht wurde), sind die conpal LAN Crypt Kommentare davon nicht betroffen. Existierende Einträge bleiben erhalten. Neue Attributinhalte überschreiben existierende Kommentare.
Bei der Auswahl von <Standard> wird kein Kommentar importiert.

Zertifikate

Auf dem Reiter Zertifikate können Sie festlegen, ob Zertifikate, die dem Benutzer im LDAP-Verzeichnis zugewiesen wurden, beim Importieren der Benutzer in die conpal LAN Crypt Datenbank übernommen werden sollen.
Eine Zuordnung der Zertifikate in der conpal LAN Crypt Administration ist für diese Benutzer dann nicht mehr notwendig. Sie haben auch hier die Möglichkeit, ein Attribut anzugeben, welches das Zertifikat für den Benutzer enthält.

Hinweis: Zertifikate, die dem Benutzer so zugewiesen werden, werden nicht geprüft (Gültigkeitsdauer, auf einer CRL usw.)!

Aktivieren Sie die Option

- **Zertifikate beim Importieren automatisch zuordnen**

wenn die Zertifikate aus dem LDAP-Verzeichnis automatisch beim Übernehmen in die conpal LAN Crypt Datenbank importiert und dem Benutzer zugewiesen werden sollen.

`<Standard>` wertet `userCertificate` und `userCertificate; binary` aus.
Klicken Sie auf `<Andere>` um ein weiteres Attribut anzugeben, dass das Zertifikat enthält.

Durch Klicken auf **OK** werden die Anmeldeinformationen in die Liste der Server übertragen. Dort können diese Angaben auch bearbeitet oder gelöscht werden.

3.5.6 Verzeichnisse

Hinweis: Die hier vorgenommenen Einstellungen werden immer im aktuellen Konfigurationssatz des SOs gespeichert. Wurden noch keine Konfigurationssätze erstellt, ist das der Konfigurationssatz <STANDARD KONFIGURATION>.

Speicherort für erzeugte Richtliniendateien

Sie müssen angeben, wo die für die Benutzer erzeugten Richtliniendateien gespeichert werden sollen.

Geben Sie im Eingabefeld den Speicherort (in der Regel ein für die Benutzer freigegebenes Netzwerklaufwerk) an. Das angegebene Verzeichnis muss existieren!

Hinweis: Bitte achten Sie darauf, dass dieses Verzeichnis für die Benutzer erreichbar ist, da die erzeugten Richtliniendateien von dort bei der Anmeldung geladen werden bzw. von dort kopiert werden.

Achtung: Bitte vergessen Sie nicht den Speicherort für die Richtliniendateien auch aus Client-Sicht einzustellen. Sie finden diese Einstellung unter conpal LAN Crypt Konfiguration.

Achtung: Bitte vergessen Sie nicht den Speicherort für die Richtliniendateien auch aus Client-Sicht einzustellen. Sie finden diese Einstellung unter conpal LAN Crypt Konfiguration.

Optionen für die Richtliniendatei - Dateiformat festlegen

Wenn Sie verschiedene conpal Client Versionen verwenden, müssen Sie sicherstellen, dass alle Ihre conpal Clients die generierten Richtliniendateien lesen können. conpal LAN Crypt unterstützt verschiedene Richtliniendateiformate:

- Richtliniendateien einer Vorgängerversion erzeugen (.pol)
  conpal LAN Crypt Client-Versionen älter als 3.12.1
- Richtliniendateien einer Vorgängerversion erzeugen (.pol.bz2) (Standard)
  conpal LAN Crypt Client-Versionen älter als 3.90
- Neue Richtliniendateien erzeugen (.xml.bz2) conpal
  LAN Crypt Client - Version 3.90 oder höher

Wählen Sie das Format, das alle Ihre Clients abdeckt.

Zusätzliche Richtliniendateien basierend auf dem Novell-Namen erzeugen

Wenn Sie diese Option auswählen, generiert conpal LAN Crypt für jeden Benutzer zwei Richtliniendateien: Eine mit dem Novell-Logonnamen und eine mit dem Windows-Benutzernamen. Der Inhalt der beiden Dateien ist identisch.

Die Benutzung des Novell-Anmeldenamens muss auch in LAN Crypt Konfiguration/Client Einstellungen definiert sein, damit er zur Anmeldung benutzt werden kann.

Hinweis: Diese Einstellung hat Auswirkungen auf die Art und Weise, wie Profile in der conpal LAN Crypt Administrationskonsole gelöscht werden. Der Vorgang des Löschens eines Profils ähnelt dem Vorgang des Erzeugens von Profilen. Wenn hier der Novell-Anmeldename verwendet werden soll (zwei Richtliniendateien werden erstellt), dann werden beide Profile gelöscht, sofern diese Einstellung nicht geändert wird. In diesem Zusammenhang bedeutet “Löschen”, dass leere Richtliniendateien generiert werden. Wird die Einstellung zur Laufzeit geändert, kann es vorkommen, dass obwohl zwei Richtliniendateien erstellt wurden, nur die Datei mit dem Windows-Benutzernamen gelöscht wird. Dadurch, dass die Einstellung aktiviert wurde, wird nur die Richtliniendatei mit dem Windows-Benutzernamen gelöscht. Die Novell-Richtliniendatei verbleibt am definierten Speicherort und kann theoretisch für die Anmeldung benutzt werden. Bei Aktivieren der Option **Richtliniendateien komprimieren** verhält sich das System ähnlich. In diesem Fall werden pro Benutzer bis zu vier Richtliniendateien erzeugt.

Bitte bedenken Sie diesen Sachverhalt und stimmen Sie die Vorgehensweise, wenn nötig, mit dem Systemadministrator ab.

Speicherort für erzeugte Zertifikate und Schlüsseldateien (*.p12)

conpal LAN Crypt kann bei Bedarf selbst-signierte Zertifikate erzeugen. Diese Zertifikate (.p12-Dateien) werden bei der Zuweisung der Zertifikate an die Benutzer erzeugt.

Der Ort, wo diese Dateien gespeichert werden sollen, muss auf dem Reiter Verzeichnisse angegeben werden.

Auch der öffentliche Teil des Security Officer Zertifikats (.cer), mit dem die Administrationsdatenbank gesichert ist, wird hier gespeichert.

Die Schlüsseldateien (.p12) und der öffentliche Teil des Security Officer Zertifikats müssen den Benutzern zur Verfügung gestellt werden.

Dazu kann in der conpal LAN Crypt Konfiguration eingestellt werden, in welchem Verzeichnis conpal LAN Crypt nach einer .p12 Datei für den Benutzer sucht, falls der private Schlüssel für die Richtliniendatei nicht vorhanden ist. Gleiches gilt für den öffentlichen Teil des Security Officer Zertifikats.

Damit die Benutzer-Schlüsseldateien automatisch erkannt werden, müssen die Dateinamen dem Anmeldenamen des Benutzers (`"Anmeldename.p12"`) entsprechen.

Wird eine entsprechende Datei gefunden, erscheint ein PIN Dialog. Diese PIN (enthalten in der Passwortprotokolldatei) muss dem Benutzer über einen PIN-Brief mitgeteilt werden. Das Zertifikat und die dazugehörigen Schlüssel werden nach Eingabe der PIN automatisch importiert.

Wird eine entsprechende .cer-Datei, die den öffentlichen Teil des Security Officer Zertifikats enthält, gefunden, wird diese automatisch importiert.

Hinweis: Um die beschriebene Funktionalität zu verwenden, müssen die entsprechenden Pfade in der conpal LAN Crypt Konfiguration gesetzt sein.

Als Alternative dazu können die Schlüsseldateien der Benutzer und der öffentliche Teil des Administratorzertifikats auch manuell verteilt werden. Stellen Sie in diesem Fall sicher, dass beide von den Clients importiert werden.

Hinweis: Auf den Clients muss immer der öffentliche Teil des Zertifikats jenes Security Officers importiert werden, von dem die Richtliniendateien erzeugt werden.
Wird der Pfad, wo die .cer-Dateien der Security Officers und die .p12-Dateien der Benutzer gespeichert werden, nach dem Anlegen der Security Officers geändert, müssen diese in das neue Verzeichnis kopiert werden. Die öffentlichen Teile der Zertifikate können ansonsten nicht gefunden werden.

Standardpasswort für Benutzer-Schlüsseldateien

conpal LAN Crypt bietet die Möglichkeit, alle Benutzer-Schlüsseldateien mit einem einheitlichen Standardpasswort auszustatten.

Dazu muss eine Datei, die das gewünschte Passwort enthält (maximal 32 Zeichen), in dasselbe Verzeichnis kopiert werden, in dem sich die Datei für das Passwortprotokoll befindet (siehe *Passwortprotokolldatei* auf Seite 53).

Die Datei mit dem Standardpasswort muss denselben Namen wie die Passwortprotokolldatei (Standardname: p12pwlog.csv) selbst haben, jedoch mit der Dateiendung .pwd (analog zum Standardnamen der Passwortprotokolldatei: p12pwlog.pwd). Ist eine solche Datei vorhanden, erhalten alle erzeugten Benutzer-Schlüsseldateien dieses Passwort.

Wird in dieser Datei anstelle des Standardpassworts das Schlüsselwort `*logonname*` eingetragen, wird der jeweilige Anmeldename als Passwort verwendet.

Hinweis: .p12 Dateien für Security Officers erhalten wegen der höheren Sicherheit IMMER ein zufälliges Passwort.

Speicherort für erzeugte Security Officer Zertifikate

conpal LAN Crypt speichert, z. B. für Backup-Zwecke, Security Officer Zertifikate in .p12 Dateien. Das Verzeichnis, in dem diese Zertifikate gespeichert werden, kann hier angegeben werden.

Hinweis: Da es sich hierbei um sensible Daten handelt, müssen diese unbedingt vor unberechtigtem Zugriff geschützt werden!

Passwortprotokolldatei

Hier kann Speicherort und Name für die Protokolldatei der generierten PKCS#12 Dateien angegeben werden (Standardname: p12pwlog.csv). Diese Datei enthält die Passwörter der erzeugten PKCS#12 Dateien und kann z. B. für die Erstellung eines PIN-Briefs verwendet werden.

Die .csv-Datei enthält folgende Informationen (die Schlüsselwörter in Klammern repräsentieren die jeweiligen Spaltenüberschriften in der .csv-Datei):

- Datum der Erstellung (`CreateDate`)
- Uhrzeit der Erstellung (`CreateTime`)
- Ablaufdatum (`ExpirationDate`)
- Genaue Uhrzeit, wann die Gültigkeit abläuft (`ExpirationTime`)
- Benutzername (`Name`)
- Anmeldename (`Logonname`)

- E-Mail-Adresse (`EMail`)
- Erstellungsmodus/-kontext (`Mode`). Mögliche Werte sind:
  `<GUI>`-Zertifikat wurde im Dialog *Eigenschaften* des Benutzers erzeugt.
  `<SO>`-Zertifikat eines SO. Wurde beim Anlegen des SO erzeugt.
  `<WIZARD>`-Zertifikat wurde mit dem Assistenten zur Zertifikatszuordnung erzeugt.
- Dateiname (`FileName`)
- Passwort (`Password`)

Hinweis: Diese Datei sollte geschützt werden und unter keinen Umständen im gleichen Verzeichnis wie die POL-Dateien gespeichert werden.

Hinweis: Wenn der Benutzer, der die Zertifikatszuordnung durchführt, im Dateisystem kein Recht hat, die Passwortprotokolldatei zu ändern, können keine conpal LAN Crypt Zertifikate erzeugt werden.

3.5.7 Regionen

conpal LAN Crypt ermöglicht optional die Angabe von Regionen, um die Administration der Schlüssel übersichtlicher zu gestalten. Die Region wird dem zuständigen Security Officer zugeordnet. Bei der Erzeugung der Schlüssel durch diesen Security Officer wird dem Schlüsselnamen automatisch der Prefix für diese Region vorangestellt. Dadurch ist immer ersichtlich, für welche Administrationseinheit der Schlüssel erzeugt wurde. Diese Vorgehensweise empfiehlt sich vor allem in verteilten Umgebungen.

Geben Sie in die Eingabefelder Namen und Prefix für die Regionen ein. Durch Klicken auf **Hinzufügen** wird die neue Region in die Liste der bestehenden Regionen eingetragen. Die hier angezeigten Regionen können beim Anlegen der Security Officers ausgewählt werden.

Bestehende Regionen können bearbeitet bzw. gelöscht werden, indem Sie sie markieren und anschließend auf **Bearbeiten** bzw. **Löschen** klicken.

Hinweis: Eine Region kann nur gelöscht werden, wenn sie keinem Security Officer zugeordnet ist.

3.5.8 Konfiguration

Auf dieser Seite können für die einzelnen Regionen bestimmte Konfigurationssätze erzeugt werden. Diese können anschließend einem Security Officer zugeteilt werden können.

Die Konfigurationssätze enthalten alle Angaben, die auf der Seite Verzeichnisse eingegeben werden können:

- den Speicherort für erzeugte Richtliniendateien

- den Speicherort für erzeugte Zertifikate und Schlüsseldateien
- den Speicherort für erzeugte Security Officer Zertifikate
- Speicherort und Namen der Passwortprotokolldatei
- die Optionen für die Richtliniendateien

Die Konfigurationssätze werden immer einer bestehenden Region zugeteilt. Für einen einer Region zugeteilten SO stehen immer nur die Konfigurationssätze, die für diese Region erzeugt wurden, zur Verfügung. Ausgenommen davon ist der Konfigurationssatz <STANDARD KONFIGURATION>, der in jeder Region zur Verfügung steht.

Die Verwendung einer bestimmten Konfiguration für eine Organisationseinheit (Region) stellt sicher, dass die richtigen Pfade für einen oder mehrere Security Officers einfach gesetzt werden können und dass alle SOs immer die gleichen Pfade zum Speichern der erzeugten Dateien verwenden.

Änderungen auf der Seite *Verzeichnisse* werden immer im derzeit zugewiesenen Konfigurationssatz gespeichert.

Hinweis: Das globale Recht Konfiguration ändern steuert, ob ein SO in der Lage sein soll, seine Konfigurationseinstellungen zu ändern. Wird es einem SO nicht gewährt, kann er ausschließlich die voreingestellten Pfade verwenden.
Ein SO, der einen bestehenden Konfigurationssatz ändert, ändert damit immer auch die Konfiguration aller SOs, denen ebenfalls diese Konfiguration zugewiesen ist.

Konfigurationssatz erzeugen

Zum Erzeugen eines Konfigurationssatzes

1. Wählen Sie eine bestehende Region aus für die der Konfigurationssatz erstellt werden soll, oder wählen Sie <Keine Region> um einen Konfigurationssatz zu erstellen, der SOs zugeteilt werden kann, die sich in keiner Region befinden.
2. Geben Sie unter *Neuer Name* eine Bezeichnung für den neuen Konfigurationssatz ein.
3. Markieren Sie einen bestehenden Konfigurationssatz in der Liste.
   Dieser Konfigurationssatz wird kopiert und unter dem neuen Namen gespeichert. Klicken Sie auf **Kopieren**.
4. Durch Markieren des Konfigurationssatzes und Klicken auf **Bearbeiten** können Sie diesen editieren.
5. Der angezeigte Dialog entspricht dem *Verzeichnisse* Dialog unter *Eigenschaften*. Geben Sie hier die entsprechenden Pfade an und definieren Sie die Richtliniendateioptionen. Klicken Sie auf OK.

6. Der neue Konfigurationssatz wird nun in der Liste unter der entsprechenden Region angezeigt und kann beim Anlegen weiterer SOs verwendet werden. Die Konfiguration (und die Region) eines bereits existierenden kann über die *Eigenschaften* Seite des jeweiligen SO geändert werden.

7. Sie können beliebig weitere Konfigurationssätze anlegen.

3.5.9 Zusätzliche Autorisierung

In conpal LAN Crypt kann festgelegt werden, dass bestimmte Aktionen einer zusätzlichen Autorisierung durch mindestens einen zweiten Security Officers bedürfen. Eine zusätzliche Autorisierung kann für folgende Aktionen verlangt werden:

Aktionen	Notwendige Rechte
Einstellungen für zusätzliche Autorisierung ändern	Darf nur von einem Master Security Officer ausgeführt werden.
Wiederherstellungsschlüssel ändern	Darf nur von einem Master Security Officer ausgeführt werden.
Die folgenden Aktionen dürfen nur von SOs ausgeführt werden, die als globales Recht Operationen autorisieren und das der Aktion entsprechende Recht besitzen. **Achtung:** Bitte beachten Sie, dass nur der Besitz eines globalen Rechts zum Ausführen einer zusätzlichen Autorisierung unter Umständen nicht ausreichend ist. Die zusätzlichen Security Officers benötigen dieses Recht explizit an dem Objekt, an dem die zusätzliche Autorisierung ausgeführt wird.	
Globale Einstellungen ändern	Erfordert das globale Recht **Konfiguration ändern**. Eine Autorisierung wird bei Änderungen an den Registern *Algorithmen*, *Zertifikat*, *Regionen*, *Verzeichnisse*, *Schlüssel*, *Antiviren-Software*, *Regeln auflösen*, *Server*, Konfiguration, und Andere Einstellungen verlangt. Änderungen an den Registern *Algorithmen*, *Zertifikate*, *Schlüssel*, *Regeln Auflösen*, Regionen und Andere Einstellungen dürfen nur von Master Security Officers autorisiert werden!
Security Officer anlegen	Erfordert das globale Recht **SOs erzeugen**
Zugriffslisten ändern	Erfordert das globale Recht **ACL ändern** und die entsprechenden gruppenspezifischen bzw. SO spezifischen Rechte.
Globale Rechte ändern	Erfordert das globale Recht **Globale Rechte ändern** und die entsprechenden SO-spezifischen Rechte.

Aktionen	Notwendige Rechte
Zertifikate zuweisen	Erfordert das globale Recht **Zertifikate zuweisen** und die entsprechenden gruppenspezifischen bzw. SO-spezifischen Rechte.
Benutzer- und gruppenspezifische Schlüssel in Regeln verwenden	Erfordert das globale Recht Spezifische Schlüssel verwenden. Wenn Sie die zusätzliche Autorisierung für die Verwendung von spezifischen Schlüsseln festlegen, so hat dies keine Auswirkungen auf die Anwendung der Platzhalter <userkey> und <groupkey>. Dies schränkt nur die Handhabung (anzeigen/benutzen/bearbeiten) eines tatsächlichen, spezifischen Schlüssels ein.
Gruppen verwalten	Erfordert das globale Recht **Gruppen ändern** und die entsprechenden gruppenspezifischen Rechte.
Benutzer verwalten	Erfordert das globale Recht **Benutzer ändern** und die entsprechenden gruppenspezifischen Rechte.
Protokollierung verwalten	Erfordert die globalen Rechte **Protokoll lesen** und **Protokollierung verwalten**
Regeln erzeugen	Erfordert das globale Recht **Regel erzeugen** und das entsprechende gruppenspezifische Recht.
Schlüssel erzeugen oder verschieben	Erfordert das globalen Recht **Schlüssel erzeugen** und das entsprechende gruppenspezifische Recht.
Profile erzeugen	Erfordert das globale Recht **Profile erzeugen** und das entsprechende gruppenspezifische Recht.
Schlüsselwert anzeigen	Erfordert das globale Recht Schlüssel lesen. Wenn Sie die Option Schlüsselwert anzeigen im Eigenschaftendialog eines Schlüssels auswählen, ist zusätzliche Autorisierung erforderlich.

Soll für eine dieser Aktionen eine zusätzliche Autorisierung notwendig sein, muss für diese Aktion angegeben werden, wie viele Security Officers dafür notwendig sind.

Markieren Sie dazu die entsprechende Aktion. Ein Doppelklick auf die markierte Aktion öffnet einen Dialog, in dem die Anzahl der notwendigen Security Officers angegeben werden kann. Nach dem Klick auf **OK** wird die Liste auf der Seite Zusätzliche Autorisierung entsprechend aktualisiert.

Wird festgestellt, dass die erforderliche Anzahl an Security Officers mit entsprechenden Rechten nicht zur Verfügung steht, wird eine Meldung angezeigt, die Sie darauf hinweist.

Hinweis: Die Anzahl der tatsächlich zur Verfügung stehenden Security Officers kann zu diesem Zeitpunkt vom System nicht genau festgestellt werden. Bitte beachten Sie, dass möglicherweise die geforderte Anzahl nicht zur Verfügung steht, auch wenn diese Meldung nicht angezeigt wird.

Zum Beispiel, wenn die Rechte der Security Officers geändert werden oder Security Officers gelöscht werden.

Achtung: Wenn Sie darauf hingewiesen werden, dass die erforderliche Security Officers nicht zur Verfügung stehen, und Sie bei der Anzahl der notwendigen Security Officers angeben, dass mindestens ein zusätzlicher Security Officer notwendig ist, anschließend den Dialog mit OK bestätigen und schließen, wird die Einstellung aus technischen Gründen dennoch übernommen. Dies führt dazu, dass die Aktionen die eine zusätzliche Autorisierung verlangen nicht mehr ausgeführt werden können, da die dazu notwendigen Security Officers nicht vorhanden sind. Wird eine solche Einstellung z.B. für die Option **Einstellungen für zusätzliche Autorisierung ändern** vorgenommen, kann keine Einstellung in diesem Dialog mehr geändert werden.
Die einzigen Möglichkeit, diese Einstellung wieder zu ändern besteht dann darin, einen Wiederherstellungsschlüssel zu erzeugen (siehe *Zusätzliche Autorisierung aufheben* auf Seite 59).

Eine vergleichbare Situation kann beim Löschen von Security Officers entstehen, da dabei nicht geprüft wird ob nach dem Löschen eines Security Officers noch die für eine zusätzliche Autorisierung notwendige Anzahl vorhanden ist. conpal LAN Crypt stellt nur sicher, dass immer ein Master Security Officer im System vorhanden ist.

Hinweis: Wenn Sie keine Token zur zusätzlichen Autorisierung benutzen, empfehlen wir, die Option **Hohe Sicherheit für den privaten Schlüssel** auf **Ja** einzustellen.

Zusätzliche Autorisierung ausführen

Wurde für eine Aktion eine zusätzliche Autorisierung festgelegt, wird bei deren Aufruf ein Assistent für die zusätzliche Autorisierung gestartet. Dieser Assistent verlangt die Autorisierung durch mindestens einen weiteren Security Officer. Der betreffende Security Officer kann in einem Dialog ausgewählt werden.
War die Authentisierung dieses Security Officers über sein Zertifikat erfolgreich, kann die gewünschte Aktion ausgeführt werden.

Verfügen Security Officers über dasselbe Zertifikat, kann dieses Zertifikat nur einmal in einer Autorisierungsaktion verwendet werden. Ein weiterer SO, dem dieses Zertifikat zugeteilt ist, wird in der Liste der auswählbaren SOs nicht mehr angezeigt.

Hinweis: Der Dialog zur Auswahl eines Security Officers enthält eine Option zur Anzeige der SOs einer bestimmten Region. Security Officers, die keiner Region zugeordnet sind, werden in der Liste immer angezeigt.

Autorisierung zurücksetzen

Eine zusätzliche Autorisierung für eine Aktion hat in der Regel Gültigkeit für die gesamte Dauer einer Sitzung in der conpal LAN Crypt Administration. Über das Symbol **Autorisierung zurücksetzen** in der Symbolleiste der Administration werden die entsprechenden Informationen gelöscht, sodass beim nächsten Ausführen der Aktion in derselben Sitzung wieder eine zusätzliche Autorisierung notwendig wird.

Zusätzliche Autorisierung aufheben

Falls die Konfiguration dazu führt, dass nicht mehr genügend Security Officers vorhanden sind, um die Aktionen zu genehmigen, kann mit dem Wiederherstellungsschlüssel die Anzahl der zusätzlichen Security Officers, die notwendig sind, um die Einstellungen für die zusätzliche Autorisierung zu ändern, auf 0 zurückgesetzt werden.

Klicken Sie dazu im Anmeldedialog zur Datenbank auf die Schaltfläche **Zertifikat wechseln**. So starten Sie den Assistenten für den Wiederherstellungsschlüssel, der Ihnen ermöglicht, die Anzahl der notwendigen zusätzlichen Security Officers auf 0 zu setzen. Details siehe unten.

3.5.10 Wiederherstellungsschlüssel

conpal LAN Crypt sieht die Möglichkeit vor, einen Recovery Key zu generieren. Mit Hilfe dieses Schlüssels kann einem Security Officer bei der Anmeldung an die conpal LAN Crypt Datenbank ein neues Zertifikat zugewiesen werden (über die Schaltfläche "Zertifikat wechseln" im Anmeldedialog), wenn dieses z.B. beschädigt ist und nicht mehr verwendet werden kann. Mit dem Wiederherstellungsschlüssel kann auch die Anzahl der zusätzlichen Security Officers, die notwendig sind, um die Einstellungen für die zusätzliche Autorisierung zu ändern, auf 0 zurückgesetzt werden.

Ein Recovery Key kann in mehrere Teile aufgeteilt werden, und es kann festgelegt werden, wie viele Teile zum Zuweisen eines neuen Zertifikats notwendig sind. Die einzelnen Teile des Recovery Keys können an verschiedene Security Officers verteilt werden. Die Besitzer der einzelnen Teile müssen bei der Verwendung des Recovery Keys anwesend sein und über einen Assistenten die Teile des Schlüssels präsentieren. Der Recovery Key bzw. dessen Teile können manuell eingegeben werden oder aus einer Datei geladen werden.

Zur Erzeugung eines Recovery Keys klicken Sie auf die Schaltfläche **Wiederherstellungsschlüssel erzeugen** auf der Seite *Wiederherstellungsschlüssel*. Der Assistent zur Erzeugung des Wiederherstellungsschlüssels wird gestartet.

Wählen Sie über die Dropdownmenüs aus, aus wie vielen Teilen der Schlüssel bestehen soll und wie viele Teile davon für eine Verwendung des Recovery Keys notwendig sind. In unserem Beispiel soll der Schlüssel aus drei Teilen bestehen, wobei mindestens zwei davon für das Zuweisen eines neuen Security Officer Zertifikats bei der Anmeldung notwendig sind. Klicken Sie auf **Weiter**.

Der Assistent zeigt für jeden Teil des Schlüssels einen Dialog an, in dem Sie auswählen können, ob der Teilschlüssel in einer Datei gespeichert wird, oder ob er angezeigt werden soll. Wenn alle Teile abgearbeitet wurden, wird der Assistent geschlossen.

Auf der Seite Recovery Key wird neben Default Recovery Key angezeigt, aus wie vielen Teilen der Schlüssel besteht (im Beispiel 3) und wie viele Teile davon bei der Verwendung notwendig sind (im Beispiel 2).

Hinweis: Bitte beachten Sie bei der Erzeugung und dem Verteilen der Teile des Recovery Keys, dass es sich dabei um äußerst sensible Daten handelt. Der Recovery Key muss unbedingt vor Unbefugten geschützt werden.

Achtung: Es kann immer nur der letzte erzeugte Recovery Key verwendet werden!
Die zuvor erzeugten Schlüssel sind nicht mehr gültig und können nicht zum Zuweisen eines Zertifikats verwendet werden.

Verwenden des Wiederherstellungsschlüssels

Sollte eine Anmeldung an die conpal LAN Crypt Datenbank nicht mehr möglich sein (z. B. weil das Zertifikat abgelaufen ist), klicken Sie im Dialog zur Auswahl des Security Officers auf die Schaltfläche **Zertifikat wechseln**, um den *Assistenten für den Wiederherstellungsschlüssel* zu starten.

Sollten Sie nach der Auswahl eines Security Officers zur Anmeldung durch einen Dialog darauf hingewiesen werden, dass das Zertifikat nicht mehr gültig ist, können Sie den Assistenten direkt von dort aus starten.

Folgen Sie den Anweisungen des Assistenten.

In diesem Assistenten ist auch ein Dialog enthalten, in dem Sie die Möglichkeit haben, die Anzahl der Security Officers, die nötig ist, um die Einstellungen für zusätzliche Autorisierung zu ändern, zurück auf 0 zu setzen.

Durch diesen Mechanismus ist sichergestellt, dass nie eine Situation entstehen kann, in der keine zusätzliche Autorisierung mehr möglich ist, da die notwendigen Security Officers nicht vorhanden sind.

Wenn Sie diese Option aktivieren, kann anschließend ein einzelner Security Officer die Einstellungen für die zusätzliche Autorisierung ändern.

3.5.11 Datenbank

Hinweis: Diese Einstellung ist nur bei der Verwendung einer Oracle-Datenbank notwendig, auf die von verschiedenen Administrationsstationen zugegriffen wird. Sie kann nur von einem Master Security Officer vorgenommen werden.

Der National Language Support (NLS) von Oracle konvertiert Texte in der Form, dass Texte unabhängig vom eingestellten Character Set für den Anwender immer gleich dargestellt werden, auch wenn sie aufgrund der zugrunde liegenden Character Sets numerisch unterschiedlich codiert werden (Beispiel: WE8MSWIN1252: ü=FC00, AL16UTF16: ü=7C00).

Werden Texte in die Datenbank eingefügt und basierend auf einem anderen Character Set ausgelesen (Zeichen werden konvertiert, binäre Daten wie MAC nicht), führt dies dazu, dass bei der Berechnung der Prüfsumme (MAC) Fehler auftreten.

Um diese Fehler zu vermeiden, sollte sichergestellt werden, dass auf allen Administrationsstationen auf die über den Oracle Client auf die Datenbank zugegriffen wird, dieselbe Code Page/dasselbe Character Set verwendet wird.

Dazu kann auf der Seite *Datenbank* ein Character Set angegeben werden, das von allen Administrationsstationen, die auf die Datenbank zugreifen, verwendet werden muss. Beim Start der Administration prüft conpal LAN Crypt, ob die Einstellung des Oracle Clients der Einstellung in der Administration entspricht. Ist dies nicht der Fall, wird eine Warnung angezeigt und die Administration wird nicht gestartet.

Geben Sie im Eingabefeld das Character Set an, das auf den Oracle Clients angegeben sein muss, damit sich diese an die conpal LAN Crypt Administration anmelden dürfen. Auf den Oracle-Clients finden Sie diese Einstellung in der Registrierung unter dem Wert `NLS_Lang` (`Language.Territory.CharacterSet`. Beispiel: `GERMAN_GERMANY.`**`WE8MSWIN1252`**).

Der Zeichensatz der aktuellen Maschine wird in *INFO*: in der Registerkarte *Datenbank* angezeigt. In der Regel muss dieses auch von allen anderen Clients, die auf die Datenbank zugreifen, verwendet werden.

Hinweis: Wir empfehlen Ihnen, nur einen Zeichensatz zu verwenden! Wenn Sie mehr als einen Zeichensatz verwenden, dann können Fehler beim Errechnen der Prüfsumme (MAC) auftreten. Prinzipiell ist es aber möglich, mehrere Zeichensätze anzugeben. Dies sollte aber ausschließlich dann getan werden, wenn es sich um Zeichensätze handelt, die weitgehend identisch sind und sich nur in wenigen Zeichen unterscheiden. Diese Zeichen sollten bekannt sein und dürfen dann für Einträge in die Datenbank nicht verwendet werden!

Deaktivierung der Prüfung

conpal LAN Crypt ermöglicht es, die Prüfung der verwendeten Character Sets zu deaktivieren. Wird das Eingabefeld leer gelassen, findet keine Prüfung statt und die Anmeldung wird immer erlaubt. Bitte beachten Sie, dass dies zu Fehlern bei der Berechnung der Prüfsumme (MAC) führen kann.

Um zu verhindern, dass bei der Angabe eines Character Sets Fehler passieren (z. B. Tippfehler), die dazu führen würden, dass sich auch der Master Security Officer, der die Einstellung vorgenommen hat, nicht mehr an die Administration anmelden kann, wird die Eingabe beim Klicken auf **Übernehmen** bzw. **OK** geprüft. Entspricht die angegebene Einstellung nicht den derzeit auf dieser Arbeitsstation gültigen, wird eine entsprechende Meldung angezeigt und das derzeitige gültige Character Set wird zusätzlich in das Eingabefeld eingefügt. Die Seite Datenbank bleibt geöffnet, sodass die eingegebenen Daten noch einmal geprüft werden können. Ändern Sie gegebenenfalls die Einstellung und klicken Sie erneut auf **Übernehmen** bzw. **OK**.

3.5.12 Antiviren-Software

Damit Virenscanner in der Lage sind, auch mit conpal LAN Crypt verschlüsselte Dateien zu scannen, müssen sie hier angegeben werden. Die Antiviren-Software erhält dann Zugriff auf alle conpal LAN Crypt Schlüssel und kann so auch Virensignaturen in verschlüsselten Dateien erkennen. Ohne die conpal LAN Crypt Schlüssel ist dies nicht möglich.

Um einen Virusscanner hinzuzufügen, klicken Sie auf **Hinzufügen**. Geben Sie die folgenden Daten in das angezeigte Dialogfeld ein:

- Einen beliebigen Namen für die Antiviren-Software (dieser Name wird in der Tabelle im Reiter *Antiviren-Software* unter *Produkt* angezeigt.)
- Den Namen der ausführbaren Datei die, den Scan ausführt.

Aktivieren Sie die Option **Authenticode-Verifizierung verwenden**.

Hinweis: Wir empfehlen, unbedingt einen Authenticode-signierten Virenscanner zu verwenden, diesen hier einzutragen und die Authenticode-Verifizierung zu aktivieren. Nur durch diese Verifizierung kann sichergestellt werden, dass es sich um die gewünschte ausführbare Datei des Virenscanners handelt und damit ausschließlich vertrauenswürdige Applikationen Zugriff auf die conpal LAN Crypt Schlüssel haben.

Nach dem Klicken auf **OK** wird die Antiviren-Software in der Liste angezeigt. Sie können weitere Virenscanner hinzufügen.

3.5.13 Client-API

conpal LAN Crypt stellt eine Client-API zur Verfügung, die es Anwendungen erlaubt, die Dateiverschlüsselungsfunktionalität über eine einfache Kommandozeile oder eine COM-style-API zu steuern. Details dazu finden Sie in der Client-API-Dokumentation im Verzeichnis \DOC Ihres entpackten Installationspakets.

Hinweis: Die API muss während der Installation des conpal LAN Crypt Clients ausgewählt werden. Wenn Sie die Client -API auf Ihren Clients verwenden wollen. dann stellen Sie sicher, dass sie korrekt installiert ist.

Geben Sie dazu im Register *Client API* die Einstellungen für die Client API an.

- Wählen Sie **Client API aktivieren**, um die API auf dem Client verfügbar zu machen. Nun können Anwendungen die Dateifunktionalität über die COM-style-API steuern.
- Wählen Sie **API-Zugriff für das conpal Dateiverschlüsselungs-Komandozeilen-Tool aktivieren**, um die Steuerung der Dateiverschlüsselungsfunktionalität über ein einfaches Kommandozeilenwerkzeug zu ermöglichen.
- **Nur COM-style API**: Standardmäßig haben Verschlüsselungsregeln, die in der conpal

LAN Crypt Administration definiert sind, Priorität vor Verschlüsselungen, die über die Client-API ausgeführt werden. Wenn Sie die API-Regeln priorisieren wollen. wählen Sie die Option **API-Regeln haben Vorrang gegenüber Verschlüsselungsregeln in Profilen**.
Hinweis: Die conpal LAN Crypt **Ignorieren Regeln** und **Ausschließen-Regeln** haben höchste Priorität und können nicht durch API-Regeln außer Kraft gesetzt werden, die wiederum automatisch von einer Verschlüsselung ausgenommen sind (siehe *Von einer Verschlüsselung ausgenommene Dateien und Verzeichnisse* auf Seite 9).

Da der API-Zugang nur auf erlaubte Anwendungen beschränkt ist, müssen Sie diese Anwendungen angeben.

1. Klicken Sie auf **Hinzufügen** im Register **Client API**.
2. Geben Sie den Anwendungsnamen ein.
3. Geben Sie den Namen der ausführbaren Datei an, die auf die API zugreifen soll.
4. Wenn Sie wollen, dass nur Authenticode-signierte ausführbare Dateien auf die API zugreifen sollen, wählen Sie die Option **Ausführbare Datei muss Authenticode-signiert sein**.
5. Wenn Sie nur ausführbare Dateien verwenden wollen, die von vertrauenswürdigen Anbietern signiert sind, wählen Sie die Option **Ausführbare Datei muss von einem vertrauenswürdigen Anbieter Authenticode-signiert sein**. Damit stellen Sie sicher, dass nur ausführbare Dateien zugelassen werden, die ein Zertifikat verwenden, das in *Signaturzertifikat* eines Anbieters aus dem Register *Vertrauenswürdiger Anbieter* registriert ist.
   Hinweis: Vertrauenswürdiger Anbieter müssen im Register *Vertrauenswürdiger Anbieter* in den *conpal LAN Crypt Einstellungen* eingetragen sein.
6. Geben Sie optional einen Kommentar ein.

Nach dem Klicken auf **OK** erscheint die Anwendung in der Liste. Sie können weitere Anwendungen hinzufügen.

3.5.14 Vertrauenswürdige Anbieter

Im RegisterVertrauenswürdiger Anbieter können Sie Anbieter eintragen, die mit einer Authenticode-signierten ausführbaren Datei auf die Client-API zugreifen dürfen.

Zum Hinzufügen eines vertrauenswürdigen Anbieters

1. klicken Sie auf **Hinzufügen** im Register **Vertrauenswürdiger Anbieter**.
2. Geben Sie den Namen des Anbieters ein.
3. Geben Sie das Signaturzertifikat des Anbieters ein.
   Sofern im Register Client API ausgewählt, werden von der API nur ausführbare Dateien

akzeptiert, die mit diesem Zertifikat Authenticode-signiert sind.

4. Geben Sie optional einen Kommentar ein.

Nach Klicken auf **OK** erscheint der Anbieter in der Liste. Sie können weitere Anbieter hinzufügen.

3.5.15 Andere Einstellungen

Security Officer-Optionen

conpal LAN Crypt kann so konfiguriert werden, dass automatisch eine ACL mit Leserecht für die Stammgruppe für einen neu erstellten Security Officer erzeugt wird. Hierfür ist erforderlich, dass der SO die globale Berechtigung Gruppen verwalten oder Benutzer verwalten hat. Dadurch wird garantiert, dass der SO Zugriff (einsehen und/oder bearbeiten) auf alle Gruppen hat, für die er verantwortlich ist.

Wenn Sie die Option Gruppenrechte für Security Officers setzen, die Gruppen oder Benutzer verwalten dürfen auswählen, werden automatisch ACLs für die Stammgruppe erstellt.

Cryptographic Service Provider Optionen

Wenn **Key Wrapping verwenden** (**Standardeinstellung**) ausgewählt ist, werden Security Officer-Daten und Benutzerprofildaten mit einem per Zufallsprinzip erzeugten Session Key mit dem ausgewählten Algorithmus (Standard: 3DES) verschlüsselt. Dieser Schlüssel wird dann wiederum mit dem öffentlichen Schlüssel aus dem Zertifikat RSA-verschlüsselt.

Wenn Sie Smartcards verwenden, stellen Sie sicher, dass die Smartcards, die Sie verwenden wollen, auch den von Ihnen ausgewählten Algorithmus unterstützen.

Wenn Sie diese Option deaktivieren, werden die Daten ohne einen solchen Session Key RSA-verschlüsselt. Beachten Sie, dass Smartcards diese Option unter Umständen nicht unterstützen.

3.6 Alle conpal LAN Crypt Schlüssel anzeigen

Über den Knoten *Alle conpal LAN Crypt Schlüssel* können Sie sich einen Überblick über sämtliche von conpal LAN Crypt verwalteten Schlüssel verschaffen. Sie bekommen dabei folgende Informationen angezeigt:

- Langer Schlüsselname.
- Für den Schlüssel verwendeter Algorithmus.
- Information, ob der Schlüssel aktiv ist.
- Wer hat den Schlüssel angelegt (Erzeuger).
- Information, ob der Schlüssel vererbt werden soll.

- Für welche Gruppe wurde der Schlüssel erzeugt.
- Information, ob der Schlüssel in Verwendung ist.
- Kommentarfeld.

Durch Klicken auf den Kopf einer Spalte können Sie die Tabelle auf- oder absteigend nach der gewünschten Information sortieren lassen.

3.6.1 Schlüssel finden

Zusätzlich zum Sortieren der Schlüsselinformationen besteht die Möglichkeit, einen bestimmten Schlüssel suchen zu lassen. Klicken Sie dazu mit der rechten Maustaste auf den Knoten **Alle conpal LAN Crypt Schlüssel anzeigen** und wählen Sie dann aus dem Kontextmenü den Eintrag **Schlüssel finden**.

Hinweis: Die Funktion **Schlüssel finden** steht auch für den Knoten Gruppenschlüssel in jeder Gruppe zur Verfügung.
Zum Hinzufügen eines Schlüssels zu einer Gruppe müssen Sie auch das Recht *Schlüssel kopieren* für die Gruppe, in der sich der Schlüssel befindet und das Recht *Schlüssel erzeugen* für die Gruppe, der der Schlüssel hinzugefügt werden soll, besitzen.

Anschließend wird ein Assistent aufgerufen, der Sie beim Suchen des gewünschten Schlüssels unterstützt. In Schritt 1 können Sie angeben, ob Sie nach der GUID oder dem Namen eines Schlüssels suchen möchten.

Beispiel:

`{[56]%` liefert alle Schlüssel, deren GUIDs mit 5 oder 6 beginnen.

Klicken Sie anschließend auf **Weiter**, um in der Datenbank nach dem gewünschten Schlüssel zu suchen. Wurde der Schlüssel gefunden, erhalten Sie in Schritt 2 den Schlüsselnamen, die GUID des Schlüssels und die Gruppe angezeigt, in welcher der Schlüssel erzeugt wurde.

Haben Sie die Funktion **Schlüssel finden** über den Gruppenschlüsselknoten einer Gruppe aufgerufen, können Sie durch Aktivieren der Option **Schlüssel der aktuellen Gruppe zuordnen** einen Verweis auf den gefundenen Schlüssel erzeugen. Sie sind dann in der Lage, den in einer anderen Gruppe erzeugten Schlüssel in der aktuell ausgewählten Gruppe zu verwenden. Wenn Sie die Option aktivieren, auf **Weiter** klicken und anschließend in Schritt 3 auf **Beenden**, erhalten Sie im Knoten Gruppenschlüssel der dazugehörigen aktuellen Gruppe ein spezielles Schlüsselsymbol angezeigt. Sie können diesen Schlüssel nun in Verschlüsselungsregeln einsetzen.

Hinweis: Das Auswählen der Option **Schlüssel der aktuellen Gruppe zuordnen** wirkt sich nur aus, wenn Sie die Funktion **Schlüssel finden** über den Knoten **Gruppenschlüssel** einer Gruppe aufgerufen haben und nicht über den Knoten **Alle conpal LAN Crypt Schlüssel anzeigen**. Sie können auch spezifische Schlüssel auswählen; diese werden der aktuellen Gruppe jedoch nicht

zugeordnet. Wenn Ihre Auswahl einen spezifischen Schlüssel enthält, so erscheint auf der letzten Seite des Assistenten eine entsprechende Meldung.

3.7 Ausgewählte Benutzer und Zertifikate anzeigen

Der Knoten *Ausgewählte Benutzer und Zertifikate* steht nur zur Verfügung, wenn in den Benutzereinstellungen der *conpal LAN Crypt Administration* die Option „*Alle Benutzer und Zertifikate*“ anzeigen aktiviert ist (siehe *Benutzereinstellungen* auf Seite 40).

Wenn Sie auf den Knoten *Ausgewählte Benutzer und Zertifikate anzeigen* klicken, erscheint ein Dialog, in dem Sie auswählen können, welche Benutzer angezeigt werden. Da das Anzeigen aller Benutzer sehr zeitaufwendig werden kann, ermöglicht conpal LAN Crypt das Einschränken der Suche durch die Definition von Suchkriterien.

Hinweis: Ist eingestellt, dass die Benutzerlisten zwischengespeichert werden, müssen Sie die Anzeigen entweder über das Symbol in der Symbolleiste oder durch Drücken von **F5** zuerst aktualisieren, bevor Sie neue Suchkriterien angeben können.

Durch Auswählen der Option *Passende Benutzer anzeigen* werden die Eingabefelder zum Festlegen der Suchkriterien aktiviert:

Folgende Informationen über die Benutzer werden aus der conpal LAN Crypt Datenbank ermittelt:

- Logonname
- Benutzername
- Zuordnung zwischen Benutzer und Zertifikat
- Antragssteller des Zertifikats
- Seriennummer des Zertifikats
- Datum, ab welchem das Zertifikat gültig ist
- Datum, bis zu dem das Zertifikat gültig ist
- Name der Parentgruppe

Basierend auf diesen Attributen können die Suchkriterien angegeben werden. conpal LAN Crypt sucht nach festgelegten Zeichenketten in den ausgelesenen Attributen der Benutzer.

In der ersten Dropdownliste können Sie auswählen, auf welche/welches Attribut/e die Suche angewendet werden soll.

Daneben können Sie festlegen, ob die Zeichenkette enthalten sein soll (*soll sein*) oder ob nur Benutzer angezeigt werden, in denen die Zeichenkette im ausgewählten Attribut nicht enthalten sein darf (*darf nicht sein*).

In der Dropdownliste ganz rechts können Sie die eigentliche Zeichenkette, die conpal LAN Crypt im angegebenen Attribut sucht, eingeben.

Zur Angabe der Zeichenkette können Sie folgende SQL-Platzhalter verwenden:

%	beliebige Zeichenfolge
_	einzelnes Zeichen (z.B. a__ bedeutet suche nach allen Namen mit drei Buchstaben, die mit a beginnen)
[]	einzelnes Zeichen aus einer Liste (z.B. [a-cg]% bedeutet suche nach allen Namen, die mit a,b,c oder g beginnen)
[^]	einzelnes Zeichen, das nicht in einer Liste ist (z.B. [^a]% bedeutet suche nach allen Namen, die mit a beginnen)

Sie können bis zu drei Bedingungen für die Suche angeben.

Geben Sie mehr als eine Bedingung an, können Sie festlegen, wie diese Bedingungen verknüpft werden sollen (UND/ ODER).

Über einen Klick mit der rechten Maustaste auf den Knoten *Ausgewählte Benutzer und Zertifikate anzeigen* können Sie alle Funktionen des Zertifikat-Snap-Ins nutzen, die auch für jede einzelne Gruppe verfügbar sind (siehe *Zuordnung der Zertifikate* auf Seite 119).

Der Assistent zur Zertifikatszuordnung steht an dieser Stelle nur Master Security Officers zur Verfügung. Ein Security Officer kann, sofern er die entsprechenden Rechte besitzt, einem einzelnen Benutzer über das *Eigenschaften* Menü ein Zertifikat zuweisen.

Hat der Security Officer für den dargestellten Benutzer keine Rechte, wird ein entsprechendes Symbol angezeigt.

3.8 Anlegen eines Security Officers

Master Security Officers, und Security Officers die dazu berechtigt sind, können weitere Security Officer anlegen. Diese Security Officers können dann einzelnen Organisationseinheiten zugeordnet werden. Sie werden in einem ersten Schritt mit globalen Rechten ausgestattet, die exakt definieren, welche Aufgaben sie generell übernehmen dürfen. Werden Security Officers einer Organisationseinheit (einem Objekt in der conpal LAN Crypt Administration) zugeordnet, können deren Rechte an diesem speziellen Objekt noch einmal über ACLs eingeschränkt werden.

Hinweis: Besitzt ein Security Officer nach seinen globalen Rechten die Erlaubnis für eine bestimmte Aktion nicht, kann ihm dieses Recht über eine ACL nicht mehr zugestanden werden.

1. Neue Security Officers werden unter dem Knoten *Zentrale Einstellungen/Security Officers*

Administration angelegt. Durch Klicken auf **Neuen SO hinzufügen** im Kontextmenü dieses Knotens oder durch Klicken auf **Neuen SO hinzufügen** im Menü Aktion, wird der erste Dialog zum Hinzufügen eines SO geöffnet.

2. Geben Sie in diesem Dialog einen Namen und optional eine E-Mail Adresse und einen Kommentar ein. Klicken Sie auf **Weiter**.

Hinweis: Die E-Mail-Adresse wird auch in die Passwortprotokolldatei für von conpal LAN Crypt erzeugte Zertifikate eingetragen. So kann sie z. B. für die Erstellung eines PIN Mailers via E-Mail verwendet werden.

3. Geben Sie in diesem Dialog an, ob der neue Security Officer mit den Rechten für einen Master Security Officer ausgestattet sein soll. Ein Master Security Officer besitzt immer alle zur Verfügung stehenden Rechte. Wählen Sie über die **Suchen**-Schaltfläche ein vorhandenes Verschlüsselungszertifikat aus, oder lassen Sie von conpal LAN Crypt ein neues erzeugen.
   Zertifikate über eine LDAP-Quelle zuordnen
   conpal LAN Crypt ermöglicht die Zuordnung von Zertifikaten aus einem Microsoft Active Directory oder LDAP-Quellen.
   Markieren Sie dafür **LDAP** in der Drop-Down-Liste des Dialogs *Wählen Sie ein Zertifikat*.

   Es wird jetzt ein Eingabefeld angezeigt, in das Sie die URL der LDAP Quelle eingeben können. Nach Klicken auf **Aktualisieren** wird der Inhalt der LDAP Quelle angezeigt.
   Begriffe in eckigen Klammern (z. B. [Sub_OU1]) bezeichnen die OUs in der LDAP Quelle. Ein Doppelklick auf eine OU zeigt die darin enthaltenen Zertifikate an.
   Doppelklicken Sie [..] um in der Organisationsstruktur eine Ebene höher zu gelangen.
   Wählen Sie ein Zertifikat aus und klicken Sie auf **OK**. Das Zertifikat wird dem Security Officer zugewiesen.

Hinweis: Wenn auf den LDAP Server nicht über eine Anonymous-Anmeldung zugegriffen werden kann, müssen die Anmeldedaten im Register **Server** in den **Zentralen Einstellungen** eingetragen werden.

Hinweis: Wenn Sie conpal LAN Crypt ein Verschlüsselungszertifikat erzeugen lassen, muss dieser Security Officer den privaten Schlüssel aus der erzeugten .p12 Datei auf seiner Arbeitsstation importieren.
Wenn das Verschlüsselungszertifikat aus einem LDAP Verzeichnis zugewiesen wurde, muss der dazugehörige private Schlüssel auf der Arbeitsstation des Security Officers vorhanden sein. Das Verschlüsselungszertifikat wird für den kryptografischen Zugriff auf die symmetrischen Datenbankschlüssel verwendet.

4. Wählen Sie optional über die zweite Browse Schaltfläche ein vorhandenes Signaturzertifikat aus, oder lassen Sie von conpal LAN Crypt ein Neues erzeugen.

Hinweis: Wenn Sie conpal LAN Crypt ein Signaturzertifikat erzeugen lassen, muss dieser Security Officer den privaten Schlüssel aus der erzeugten .p12 Datei auf seiner Arbeitsstation importieren.
Wenn das Signaturzertifikat aus einem LDAP Verzeichnis certificate zugewiesen wurde, muss der dazugehörige private Schlüssel auf der Arbeitsstation des Security Officers vorhanden sein. Das Signaturzertifikat wird für die Signatur in den erzeugten Profilen und für die Authentisierung im Rahmen des erweiterten API-Logon verwendet.

5. Wenn Sie Regionen für Ihre Security Officers definiert haben, können Sie jetzt eine Region auswählen.

6. Wenn Sie einzelne *Konfigurationssätze* für die Regionen erstellt haben, können Sie jetzt einen auswählen.

Hinweis: Es werden immer nur jene Konfigurationen angezeigt, die für die eingestellte Region erzeugt wurden.

7. Klicken Sie auf **Weiter**.

8. Im letzten Dialog des Assistenten können Sie festlegen, welche Aktionen der neue Security Officer durchführen können soll.
   Wenn Sie eine Aktion auswählen, werden automatisch alle dafür notwendigen globalen Rechte gesetzt. Diese Rechte werden unter den Eigenschaften des SOs (werden durch einen Doppelklick auf den SO angezeigt) auf der Seite *Globale Rechte* angezeigt. Die globalen Rechte können an dieser Stelle weiter bearbeitet werden.
   Wenn Sie dem SO das Ausführen einer bestimmten Aktion in diesem Dialog erlauben, ist sichergestellt, dass er alle für diese Aktion notwendigen globalen Rechte erhält.

   Wenn ein neuer SO, die globale Berechtigung Gruppen verwalten oder Benutzer verwalten auf diese Weise erhält, erstellt conpal LAN Crypt automatisch eine ACL mit Leserechten für die Stammgruppe für diesen Security Officer, vorausgesetzt, dass die Option Gruppenrechte für Security Officers setzen, die Gruppen oder Benutzer verwalten dürfen ausgewählt ist .
   Dadurch wird garantiert, dass der SO Zugriff (einsehen und/oder bearbeiten) auf alle Gruppen hat, für die er verantwortlich ist.

Sie können die Option Gruppenrechte für Security Officers setzen, die Gruppen oder Benutzer verwalten dürfen im Reiter *Andere Einstellungen* unter **Zentrale Einstellungen** auswählen.

9. Klicken Sie auf **Fertigstellen**.

Der neue Security Officer wird in der conpal LAN Crypt Administration angezeigt.

3.8.1 Zuweisen/bearbeiten der globalen Rechte

Der Security Officer muss mit globalen Rechten ausgestattet sein. Ist der Knoten Security Officer Administration markiert, werden im rechten Konsolenfenster alle vorhandenen Security Officers angezeigt. Ein Doppelklick auf einen Security Officer öffnet die Reiter mit den ihm zugeordneten Eigenschaften.

Im Register *Globale Rechte* wird der Security Officer mit den „Basisrechten“ für die Administration von conpal LAN Crypt ausgestattet. Wurden dem Security Officer, als er angelegt wurde, bereits die Berechtigung zum Ausführen bestimmter Aktionen erteilt, sind alle dazu notwendigen Rechte bereits aktiviert.

Hinweis: Ein Master Security Officer ist immer mit allen globalen Rechten ausgestattet.

Ein Security Officer kann global mit folgenden Rechten ausgestattet werden:

Hinweis: Durch einen Klick auf die Spaltenüberschrift **Zulassen** können alle Rechte ausgewählt werden. Ein weiterer Klick hebt die Auswahl aller Rechte wieder auf.

Rechte	Beschreibung
Security Officer anlegen	Der SO hat das Recht, weitere SOs zu erzeugen.
Profile erzeugen	Der SO hat die globale Berechtigung, den Profile Resolver zu starten und Richtliniendateien für einzelne Benutzer zu erzeugen. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung Profile erzeugen für eine spezifische Gruppe für einen SO gesetzt werden kann. Profile erzeugen berechtigt den SO zum Erstellen von Benutzerprofilen, wenn der SO die Berechtigung Profile erzeugen für die übergeordnete Gruppe des Benutzers hat *(siehe Übergeordnete Gruppe eines Benutzers* auf Seite 91*).* Diese Berechtigung ist eine Voraussetzung für das Zuweisen von Werten zu Schlüsseln. Ein Benutzer, der nur die Berechtigung Schlüssel erzeugen hat, kann nur Schlüssel ohne Werte erzeugen!

Rechte	Beschreibung
Profile für alle Mitglieder erzeugen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung Profile erzeugen gesetzt ist. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung Profile für alle Mitglieder erzeugen für eine spezifische Gruppe gesetzt werden kann. Profile für alle Mitglieder erzeugen berechtigt einen SO zum Erzeugen von Profilen für alle Benutzer, wenn der SO die Berechtigung Profile erzeugen für die übergeordnete Gruppe des Benutzers oder die Berechtigung Profile für alle Mitglieder erzeugen für eine der Gruppen, zu denen der Benutzer gehört, hat. **Hinweis:** Da die globale Berechtigung Profile erzeugen eine Voraussetzung für Profile für alle Mitglieder erzeugen ist, gilt: Wenn Sie die Berechtigung Profile erzeugen deaktivieren, wird auch die Berechtigung Profile für alle Mitglieder erzeugen deaktiviert. Wenn Sie die Berechtigung Profile für alle Mitglieder erzeugen aktivieren, wird automatisch auch die Berechtigung Profile erzeugen aktiviert.
Schlüssel erzeugen	Der SO darf Schlüssel in den einzelnen Gruppen erzeugen. Das Recht *Schlüssel erzeugen* alleine erlaubt dem SO nur das Erzeugen von Schlüsseln ohne Wert! In der Administration können Schlüssel ohne Wert Verschlüsselungsregeln zugeordnet werden. Der Wert selbst wird erst generiert, wenn der Profile Resolver gestartet wird. Um direkt beim manuellen Anlegen auch den zum Schlüssel gehörenden Wert erzeugen zu können, benötigt der SO das Recht *Profile erzeugen*.
Schlüssel kopieren	Der SO darf Schlüssel kopieren.
Schlüssel entfernen	Der SO darf Schlüssel aus den Gruppen entfernen.
Schlüssel lesen	Der SO darf die Daten zu den einzelnen Schlüsseln der Gruppe sehen.
Zertifikate erzeugen	Der SO darf Zertifikate für die Benutzer erzeugen.
Zertifikate zuweisen	Der SO darf den Benutzern Zertifikate zuweisen. Der SO darf den Assistenten zur Zertifikatszuweisung starten. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung Zertifikate zuweisen für eine spezifische Gruppe für einen SO gesetzt werden kann. Zertifikate zuweisen berechtigt den SO zum Zuweisen von Zertifikaten zu Benutzern, wenn der SO die Berechtigung Zertifikate zuweisen für die übergeordnete Gruppe des Benutzers hat (siehe *Übergeordnete Gruppe eines Benutzers* auf Seite 91).

Rechte	Beschreibung
Zertifikate allen Mitgliedern zuweisen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung Zertifikate zuweisen gesetzt ist. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung Zertifikate allen Mitgliedern zuweisen für eine spezifische Gruppe gesetzt werden kann. Zertifikate allen Mitgliedern zuweisen berechtigt einen SO zum Zuweisen von Zertifikaten zu Benutzern, wenn der SO die Berechtigung Zertifikate zuweisen für die übergeordnete Gruppe des Benutzers oder die Berechtigung Zertifikate allen Mitgliedern zuweisen für eine Gruppe, zu der der Benutzer gehört, hat. **Hinweis:** Da die globale Berechtigung Zertifikate zuweisen eine Voraussetzung für Zertifikate allen Mitgliedern zuweisen ist, gilt: Wenn Sie die Berechtigung Zertifikate zuweisen deaktivieren, wird auch die Berechtigung Zertifikate allen Mitgliedern zuweisen deaktiviert. Wenn Sie die Berechtigung Zertifikate allen Mitgliedern zuweisen aktivieren, wird automatisch die Berechtigung Zertifikate zuweisen aktiviert.
Gruppen verwalten	Der SO darf Änderungen in den Gruppen vornehmen. Untergruppen aufnehmen, Gruppen verschieben, Gruppen synchronisieren, Gruppen löschen.
Anmeldung an DB	Der SO darf sich an der conpal LAN Crypt Datenbank anmelden. Dieses Recht ist standardmäßig immer aktiviert. Dieses Recht stellt eine Möglichkeit dar, einem SO ohne großen Aufwand die Möglichkeit zu nehmen, an der Datenbank Veränderungen vorzunehmen (z. B. wenn er das Unternehmen verlässt). Personen, die ausschließlich Vier-Augen-Aktionen autorisieren dürfen, kann dieses Recht verweigert werden. Damit ist sichergestellt, dass sie neben der Autorisierung von Vier-Augen-Aktionen, keine Möglichkeit haben, Änderungen in conpal LAN Crypt vorzunehmen.
Operationen autorisieren	Der SO darf an Vier-Augen-Aktionen teilnehmen.
Benutzer verwalten	Der SO darf Benutzer in eine Gruppe aufnehmen/entfernen und Gruppen synchronisieren.
Benutzer kopieren	Der SO darf Benutzer zu Gruppen hinzufügen (kopieren). Diese globale Berechtigung ist eine Voraussetzung für das Setzen der Berechtigung Benutzer kopieren für eine spezifische Gruppe für einen SO. Um einen Benutzer zu einer Gruppe hinzuzufügen, muss der Benutzer die Berechtigung Benutzer kopieren für die übergeordnete Gruppe des Benutzers haben.

Rechte	Beschreibung
Regeln erzeugen	Der SO darf Verschlüsselungsregeln erzeugen.
Globale Rechte ändern	Der SO darf die globalen Rechte eines anderen SOs ändern.
ACL ändern	Der SO darf die ACL einer Gruppe ändern.
Spezifische Schlüssel verwenden	Der SO darf bestimmte konkrete Schlüssel in Verschlüsselungsregeln verwenden und bestimmte Schlüssel in *Alle conpal LAN Crypt Schlüssel* anzeigen lassen.
Konfiguration ändern	Der SO darf die Konfiguration (die Pfade) ändern. Dieses Recht ist die Voraussetzung dafür, dass die Seite Konfiguration in den zentralen Einstellungen angezeigt wird, und die Seite Verzeichnisse bearbeitbar ist, wenn dieser SO an die Datenbank angemeldet ist.
Protokoll lesen	Für den SO sind die Einstellungen für die Protokollierung und die Einträge in das Protokoll sichtbar.
Protokollierung verwalten	Der SO darf die Einstellungen für die Protokollierung ändern. Er ist berechtigt, die Einträge zu archivieren, zu löschen und zu prüfen.
Verzeichnisobjekte importieren	Der SO darf OUs, Gruppen und Benutzer aus einem Verzeichnisdienst importieren und in die conpal LAN Crypt Datenbank übertragen. Dieses Recht bedingt, dass der SO die Rechte *Gruppen verwalten* und *Benutzer verwalten* besitzt. Sie werden automatisch gesetzt, wenn das Recht *Verzeichnisobjekte importieren* ausgewählt wird. Besitzt ein SO dieses Recht nicht, ist der Knoten *Verzeichnis-Objekte*, der das Importieren von OUs, Gruppen und Benutzern ermöglicht, in der Administration nicht sichtbar.

Bitte beachten Sie bei der Vergabe der globalen Rechte folgende Punkte:

- Wird einem Security Officer ein globales Recht nicht ausdrücklich gegeben, ist er nicht mit diesem ausgestattet.
- Ein Security Officer darf in weiterer Folge nur jene Rechte ändern, die er selbst besitzt.
- Ein Security Officer darf eine ACL, die seine eigenen Rechte beschreibt, nicht ändern.
- Manche Rechte bedingen das Setzen eines zweiten Rechts. Dies wird bei der Auswahl eines solchen Rechts automatisch gesetzt.
- SafeGuard LAN Crypt kann so konfiguriert werden, dass automatisch eine ACL mit Leserechten für die Stammgruppe für einen neu erstellten Security Officer angelegt wird. Hier ist erforderlich, dass der SO die globale Berechtigung Gruppen verwalten oder Benutzer verwalten hat. Dadurch wird garantiert, dass der SO Zugriff (einsehen und/oder bearbeiten)

auf die Gruppen hat, für die er verantwortlich ist.
Dieses Verhalten muss im Reiter *Andere Einstellungen* unter **Zentrale Einstellungen** aktiviert werden.

- Wenn ein Security Officer durch Änderung die globale Berechtigung Gruppe verwalten oder Benutzer verwalten erhält und er keine ACL für die Stammgruppe hat, so wird diese angelegt. Die ACL hat Leserechte für die Gruppe. Vorhandene ACLs bleiben unverändert.

Markieren Sie die globalen Rechte, mit denen der Security Officer ausgestattet werden soll, und klicken Sie auf **Übernehmen**.

3.8.2 Rechte zum Bearbeiten der Einstellungen für einen Security Officer

Anderen Security Officers können Rechte zum Bearbeiten der Einstellungen für einen Security Officer übertragen werden.
Ein Master Security Officer ist immer imstande, diese Einstellungen zu ändern. Einem Security Officer muss dieses Recht explizit erteilt werden.

Welche Einstellungen ein Security Officer für einen SO ändern darf, richten sich nach den globalen Rechten, die dieser selbst besitzt.

Im Register Sicherheit können Sie festlegen, welche Rechte andere SOs bezogen auf dieses Objekt (= Security Officer) besitzen. Im oberen Teil des Dialogs werden die SOs angezeigt, die das Recht besitzen, die Einstellungen für diesen SO zu bearbeiten.

1. Durch Klicken auf **Hinzufügen** wird ein Assistent zum Hinzufügen eines Security Officers gestartet. Auf der ersten Seite des Assistenten wird aus der Liste der vorhandenen SOs der gewünschte ausgewählt.

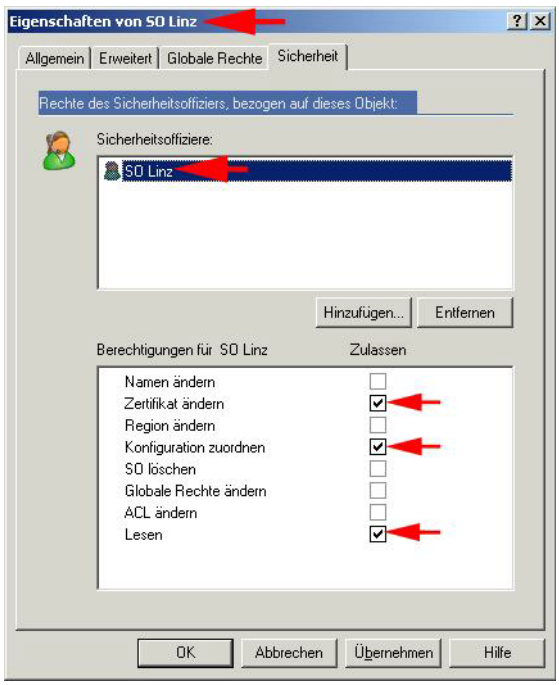
2. Klicken auf **Weiter** öffnet die Seite, auf der die Rechte für diesen SO, betreffend die Bearbeitungsrechte für dieses Objekt (den SO, dessen Eigenschaften derzeit bearbeitet werden), eingestellt werden können.

Hinweis: Durch einen Klick auf die Spaltenüberschrift **Zulassen** können alle Rechte ausgewählt werden. Ein weiterer Klick hebt die Auswahl aller Rechte wieder auf. Ausgegraute Rechte können dem Security Officer aufgrund der Einstellungen in den globalen Rechten nicht zugestanden werden.

Rechte	Beschreibung
Namen ändern	Ermöglicht die Änderung des Namens des SOs, dem der Inhaber des Rechts zugeteilt wird.
Zertifikat ändern	Ermöglicht die Änderung des Zertifikats des SOs, dem der Inhaber des Rechts zugeteilt wird.

Rechte	Beschreibung
Region ändern	Ermöglicht die Änderung des Regions-Prefix des SOs, dem der Inhaber des Rechts zugeteilt wird.
Konfiguration zuordnen	Ermöglicht die Änderung der Konfiguration (bearbeiten der Pfade und zuordnen) des SOs, dem der Inhaber dieses Rechts zugeordnet ist.
SO löschen	Ermöglicht das Löschen des SOs, dem der Inhaber des Rechts zugeteilt wird.
Globale Rechte ändern	Ermöglicht die Änderung der globalen Rechte des SOs, dem der Inhaber des Rechts zugeteilt wird.
ACL ändern	Ermöglicht die Änderung der ACL des SOs, dem der Inhaber des Rechts zugeteilt wird.
Lesen	Zeigt den SO, dem der Inhaber des Rechts zugeteilt wird unter *Zentrale Einstellungen/Security Officer Administration* an. Dies ist die Voraussetzung für alle Rechte, die eine Bearbeitung dieses SOs erlauben. Wird automatisch gesetzt, wenn ein derartiges Recht ausgewählt wird.

Die Rechte **Zertifikat ändern**, **Konfiguration zuordnen** und **Lesen** können auch dem SO gegeben werden, dessen Eigenschaften hier definiert werden. Dazu muss er selbst in die Liste der SOs, die Rechte auf dieses Objekt haben (in diesem Fall er selbst), aufgenommen werden.



Lesen
Zeigt den in *Zentrale Einstellungen\Security Officer Administration* angelegten SO an. Für den SO sind die für ihn gesetzten Rechte sichtbar.

Zertifikat ändern
Voraussetzung dafür ist das Recht "Lesen". Es erlaubt dem SO, sein eigenes Zertifikat zu ändern.

Konfiguration zuordnen
Ermöglicht dem SO, sich selbst eine andere Konfiguration zuzuordnen.

Hinweis: Rechte, für die das Kontrollkästchen ausgegraut ist, können nicht vergeben werden, da der ausgewählte SO nicht über die globalen Rechte verfügt, die dafür notwendig sind.

3. Statten Sie den Security Officer durch Anklicken der Kontrollkästchen mit den entsprechenden Rechten aus und klicken Sie auf **Übernehmen.**
   Der Security Officer wird jetzt im oberen Teil der Seite Sicherheit angezeigt. Im unteren Teil der Seite zeigt eine ACL die Rechte des markierten SOs an.

3.8.3 Alle Rechte für Gruppen/OUs eines spezifischen Security Officer

Um die Rechte eines spezifischen SO für alle Gruppen/OUs einzusehen, für die der SO Berechtigungen hat, doppelklicken Sie in Security Officer Administration auf dem relevanten SO.

Wählen Sie im Eigenschaftendialog des SO den Reiter Gruppen. Dieser Reiter hat zwei Listenansichten:

- Die obere Listenansicht zeigt alle Gruppen/OUs, für die dieser SO Berechtigungen hat.
- Die zweite Listenansicht zeigt die entsprechenden Rechte des SO für die ausgewählte Gruppe/OU.

So erhalten Sie auf einfache Art und Weise einen Überblick zu allen Rechten, die ein spezifischer SO für die verschiedenen Gruppen in Ihrer Organisationsstruktur hat.

Sie können die Rechte eines SO in dieser Ansicht nicht ändern. Dies ist nur im Eigenschaftendialog einer Gruppe möglich.

Hinweis: Es werden nur Gruppen, für die ein SO eine Berechtigung (durch Zulassen oder Verweigern) hat, angezeigt. Gruppen, für die ein SO Rechte geerbt hat, werden nicht angezeigt.

3.8.4 Wechsel oder Erneuern eines MSO- oder SO-Zertifikats

Für den Wechsel bzw. die Erneuerung eines (M)SO-Zertifikats gibt es Möglichkeiten, die nachfolgend beschrieben sind:

Variante 1: Über Security Officer Administration

1. Starten Sie die conpal LAN Crypt Administration und melden Sie sich als MSO an. Alternativ können Sie sich auch als SO anmelden, der das Recht hat, das Zertifikat des betroffenen SOs zu ändern. Dies kann auch der betroffene SO selbst sein, sofern er über das benötigte Recht verfügt und sein Zertifikat noch gültig ist.
2. Wechseln Sie zum Knoten *Zentrale Einstellungen* und von dort in den Knoten *Security Officer Administration*.
3. Klicken Sie mit der rechten Maustaste auf den betroffenen SO und wählen Sie aus dem Kontextmenü den Eintrag *Eigenschaften*.
4. Wechseln Sie zum Reiter *Erweitert*.
5. Klicken Sie unter *Verschlüsselungszertifikat* auf die Schaltfläche *Suchen*, um ein neues Verschlüsselungszertifikat für den SO auszuwählen.
6. Klicken Sie gegebenenfalls unter *Signaturzertifikat (optional)* auf die Schaltfläche *Suchen*, um ein neues Signaturzertifikat für den SO auszuwählen.

Hinweis: SO-Signaturzertifikate lassen sich nur per Variante 1 ändern und nicht per Variante 2

Variante 2: Über Wiederherstellungsschlüssel

1. Starten Sie die conpal LAN Crypt Administration.
2. Markieren Sie im Dialogfenster zur Auswahl des SO den betroffenen (M)SO.
3. Klicken Sie auf die Schaltfläche *Zertifikat wechseln* und folgen Sie den Anweisungen des *Assistenten für Wiederherstellungsschlüssel.*

Im Normalfall sollten Sie mit Variante 1 arbeiten. Variante 2 ist primär dazu vorgesehen, einen alternativen Weg zu haben, falls sich kein SO mit ausreichenden Rechten mehr an die conpal LAN Crypt Administration anmelden kann.

Hinweis: Voraussetzung für Variante 2 ist das Vorhandensein eines Wiederherstellungsschlüssels. Unabhängig von der verwendeten Methode stellen Sie sicher, dass das Profil, das der betroffene SO erzeugt hat, neu erzeugt werden muss, bevor das alte Zertifikat abgelaufen ist. Ist dies nicht der Fall, können die Profile von den Clients nicht mehr geladen werden.
Es ist möglich, die Zuweisung von Zertifikaten nur mit zusätzlicher Autorisierung zu erlauben. Eine derartige Einstellung wirkt sich natürlich auch beim Wechsel des SO Zertifikats aus.

3.9 Anmeldung an der Administration

Um sich an der Administration von conpal LAN Crypt anmelden zu können, muss ein Security Officer mit dem Recht zur Anmeldung ausgestattet sein. Master Security Officers haben dieses Recht immer, da sie automatisch mit allen zur Verfügung stehenden Rechten ausgestattet sind.

Nach dem Aufruf der Administration über Programme/Sophos/conpal LAN Crypt/SGLC Administration wird der Anmeldedialog angezeigt.

Alle berechtigten Security Officers werden in der Liste angezeigt. Durch Aktivieren der Option **Nur Security Officers einer bestimmten Region anzeigen** und der Auswahl der entsprechenden Region, kann die Anzeige auf die Security Officers dieser Region eingeschränkt werden.

Damit eine Anmeldung möglich ist, muss auf den zum Zertifikat gehörenden privaten Schlüssel (Software-Schlüssel oder auf einem Token) zugegriffen werden können.
Nach der Auswahl des gewünschten Security Officers und dem Klicken auf **OK** wird die Administration von conpal LAN Crypt geöffnet.

Wiederherstellungsschlüssel

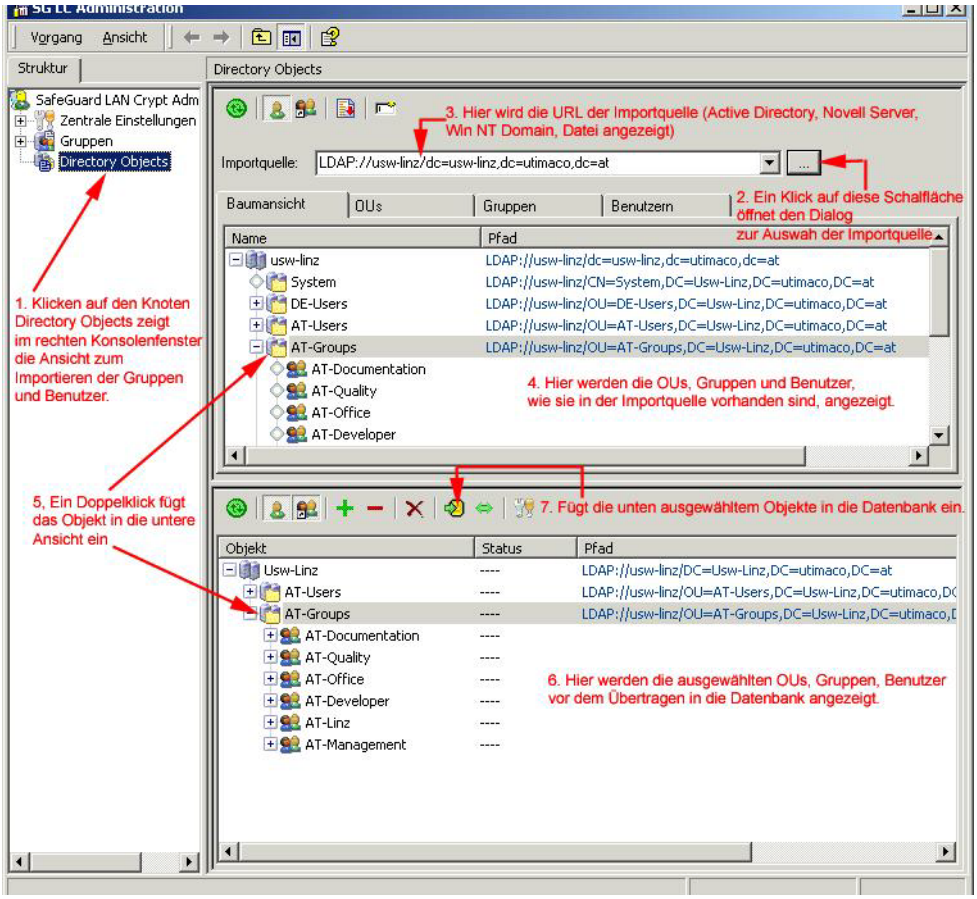
Ist der zum Zertifikat gehörende Schlüssel eines Security Officers abgelaufen, beschädigt oder verloren gegangen, besteht die Möglichkeit, das Zertifikat durch die Eingabe eines Wiederherstellungsschlüssels zu erneuern.

Achtung: Wird während des Wiederherstellens ein neues Zertifikat erzeugt, so wird dieses Zertifikat mit zugehörigem Passwort unter dem Standardpfad (C:\Dokumente und Einstellungen\All Users\Dokumente\Sophos\Admin\) und nicht unter dem konfigurierten Pfad gespeichert, da zu diesem Zeitpunkt keine SO-spezifische Konfiguration wirksam ist.

3.10 Gruppen und Benutzer importieren

conpal LAN Crypt ermöglicht den Import von Gruppen und Benutzern aus Verzeichnisdiensten, auf die über LDAP oder aus der Domäne oder auch über den Import aus einer manuell erstellten Datei, die die Gruppen und Benutzer mit den jeweiligen Zugehörigkeiten enthält, zugegriffen werden kann.

Wenn Sie auf den Knoten *Verzeichnis-Objekte* klicken, werden im rechten Konsolenfenster die Dialoge zum Import und zur Zusammenstellung der Gruppen für den Import in die Datenbank angezeigt.



Hinweis: Ist der Knoten Verzeichnis-Objekte nicht sichtbar, verfügt der angemeldete SO nicht über das globale Recht Verzeichnisobjekte importieren. Erst wenn ihm dieses Recht gegeben wird, wird der Knoten Verzeichnis-Objekte angezeigt.

3.10.1 Benutzer und Benutzergruppen aus einer Datei importieren

Benutzer und Benutzergruppen können auch aus einer Datei importiert werden. Die importierten Benutzer und Gruppen werden in der conpal LAN Crypt Administration angelegt und unter dem Knoten *Gruppen* angezeigt.

Zum Importieren von Benutzern und Gruppen aus einer Datei wählen Sie im Dialog *Importquelle* **Datei suchen** aus. Durch Klicken auf die **Durchsuchen** Schaltfläche können Sie anschließend die Datei auswählen, aus der die Benutzer und Gruppen importiert werden sollen (siehe *Importquelle auswählen* auf Seite 83).

Bei der Importdatei handelt es sich um eine Textdatei mit einer beliebigen Endung (als Standardendung wird .lcg vorgeschlagen). Der Inhalt der Datei muss ein bestimmtes Format aufweisen.

Format der Importdatei

Eine Importdatei enthält mehrere Abschnitte. Die einzelnen Abschnitte können durch eine beliebige Anzahl von Leerzeilen getrennt sein.

Jeder Abschnitt steht für je einen Benutzer bzw. je eine Gruppe.

Jeder Abschnitt besteht aus einer Kopfzeile und einer bestimmten Anzahl von Zeilen mit je einem Schlüsselwort. Zeilen müssen durch ein Zeilenumbruch-Zeichen abgeschlossen werden. Zwischen den Zeilen eines Abschnitts dürfen keine Leerzeilen vorkommen.

Die Kopfzeile wird in eckige Klammern gesetzt und enthält den Abschnittnamen. Der Abschnittname wird verwendet, um die Mitgliedschaften von Benutzern und Gruppen zu definieren.

Die Schlüsselwörter geben die Daten der Benutzer und Gruppen an.Diese Daten werden auch in den *Eigenschaften* Dialogen der Gruppen und Benutzer angezeigt.

Schlüselwörter	Beschreibung

type=	`USER`
	`GROUP`
	Gibt an, ob es sich bei dem importierten Objekt um einen Benutzer (USER) oder um eine Gruppe (GROUP) handelt.

name=	Gibt den Anmeldenamen des Benutzers an. Wird in der conpal LAN Crypt Administration als *Logonname* angezeigt.
display= optional	Ermöglicht die Angabe eines Benutzernamens, der nicht identisch mit dem Anmeldenamen ist. Wird in der conpal LAN Crypt Administration als *Benutzername* angezeigt. Ist hier kein Name eingetragen, so wird der unter `name=` eingegebene Anmeldename als *Benutzername* in der conpal LAN Crypt Administrationskonsole angezeigt.
mail= optional	Ermöglicht die Angabe der E-Mail-Adresse des Benutzers. Diese wird unter Details in den Benutzereigenschaften angezeigt. **Hinweis:** Die E-Mail-Adresse wird auch in die Passwortprotokolldatei für von conpal LAN Crypt erzeugte Zertifikate eingetragen. So kann sie z. B. für die Erstellung eines PIN Mailers via E-Mail verwendet werden.

Schlüselwörter	Beschreibung
members=	Gibt für Gruppen an, welche Benutzer und andere Gruppen, Mitglied sind. Um ein Mitglied hinzuzufügen, geben Sie den Name der Kopfzeile des Abschnitts, der den Benutzer bzw. die Gruppe beschreibt, ein (z.B. `U_BKA,G_Sophos`). Die einzelnen Mitglieder der Gruppe müssen durch Kommas getrennt werden.

Hinweis: Durch die Verwendung von // am Zeilenbeginn kann an jeder beliebigen Stelle der Datei ein Kommentar eingefügt werden.

Hinweis: Groß- und Kleinschreibung werden in der Importdatei NICHT unterschieden.

Beispiel:

```
[U_JB1]
type=USER
name=JB1
Display=Jesse Black
Mail=jb1@company.com
// Mein Kommentar .....

[U_PW1]
type=USER
name=PW1
Mail=jb1@company.com

[U_JG1]
type=USER
name=JG1

[U_JFU]
type=USER
name=JFU

[G_COMPANY]
type=GROUP
name=Company
members=G_QA,G_Linz, G_PDM,G_Empty,U_JFU
// Mein Kommentar ..... .....

[G_QA]
type=GROUP
name=QA
members=U_JB1,U_PW1

[G_PDM]
type=GROUP
```

```
name=JG1
members=U_NGR
```

3.10.2 Symbole

Aktualisiert die Ansicht im jeweiligen Fenster.

Zeigt die Benutzer in den jeweiligen Gruppen an.

Zeigt auch die Mitgliedschaften von Gruppen und Benutzern in den jeweiligen Gruppen an.
Mitgliedschaften, bei denen das Objekt nicht direkt in der Gruppe enthalten ist, werden grau dargestellt.

Fügt das ausgewählte Objekt in die untere Ansicht ein. Entspricht einem Doppelklick auf das ausgewählte Objekt.

Als neuer Pfad übernehmen.
Erlaubt es, die Anzeige der Struktur einzuschränken. Wird ein Knoten markiert und anschließend auf diese Schaltfläche geklickt, wird nur noch die Struktur unter dem markierten Knoten angezeigt. Der Pfad wird zusätzlich der Drop-Down-Liste hinzugefügt, sodass wieder schnell zu dieser Anzeige gewechselt werden kann.

Zeigt die Baumstruktur an.

Schließt die Baumstruktur.

Löscht ein markiertes Objekt aus der Ansicht.

Fügt die im rechten unteren Fenster angezeigten Objekte in die conpal LAN Crypt Datenbank ein.

Synchronisiert die im rechten unteren Fenster angezeigten Objekte mit den bereits in der Datenbank vorhandenen.

Öffnet den Dialog zum Festlegen der Übernahmeoptionen.
Die Übernahmeoptionen müssen vor der Übernahme aus der Importquelle festgelegt werden.

3.10.3 Importquelle auswählen

Die URL des Servers, von dem die Daten importiert werden sollen, kann direkt in das Eingabefeld *Importquelle* eingegeben werden (z. B. LDAP://usw-linz/dc=usw-linz,dc=sophos,dc=at für den Active Directory Verzeichnisdienst auf dem Domain Controller usw-linz).

Wenn Sie auf die **Durchsuchen** Schaltfläche klicken, stellt conpal LAN Crypt einen Dialog zur Auswahl der Importquelle zur Verfügung:

LDAP://

- **Domäne**

  Ist der Rechner Mitglied in einer Active Directory Domäne, wird die gesamte Struktur der Domäne, wie sie am Domänen Controller vorhanden ist, angezeigt.

Hinweis: Der Import von Built-in Gruppen aus dem Active Directory ist nicht möglich. Es wird daher empfohlen, die Benutzer in OUs bzw. Gruppen zu organisieren und diese zu importieren.

- **Container suchen**

  Ist der Rechner Mitglied in einer Active Directory Domäne, wird nach dem Klicken auf die **Durchsuchen** Schaltfläche (wird angezeigt, nachdem Container suchen markiert wurde) ein weiterer Dialog angezeigt. In diesem Dialog kann dann ein bestimmter Knoten in der Active Directory Struktur ausgewählt werden.

WinNT://

- **Computer**

  Zeigt die lokalen Gruppen und Benutzer des Rechners an, an dem Sie angemeldet sind. Diese Gruppen und Benutzer werden in der Regel nur für Testzwecke verwendet.

- **Domäne**

  Ist der Rechner Mitglied in einer Windows NT Domäne, wird die gesamte Struktur der Domäne, wie sie am Domänen Controller vorhanden ist, angezeigt.

  Hinweis: Bei Verwendung des WinNT-Protokolls können bei einer Synchronisation umbenannte Benutzer nicht von neu angelegten unterschieden werden, da das WinNT-Protokoll Benutzerobjekten keine eindeutige GUID zuweist.

FILE://

- **Datei suchen**

  Zum Importieren von Benutzern und Gruppen aus einer Datei wählen Sie im Dialog *Importquelle* **Datei suchen** aus. Durch Klicken auf die **Durchsuchen** Schaltfläche können Sie anschließend die Datei auswählen, aus der die Benutzer und Gruppen importiert werden sollen.
  Die Datei muss vor dem Import in einem bestimmten Format erstellt werden. Für Informationen zum Erstellen der Importdatei, siehe *Benutzer und Benutzergruppen aus einer Datei importieren* auf Seite 79.

Wenn Sie eine Importquelle ausgewählt haben, zeigt ein Klick auf die **Übernehmen** Schaltfläche die URL der Quelle unter *Pfad* an.

Durch Klicken auf **OK** werden die ausgewählten Daten im rechten oberen Teil der Konsole angezeigt. Diese Ansicht erlaubt die Anzeige der ausgewählten Daten in einer Baumansicht, nach OUs, Gruppen und Benutzer.

Nur für LDAP Server

Ist der Administrationsrechner nicht Mitglied einer Domäne, können Sie die Gruppen und Benutzer folgendermaßen von einem Server importieren:

1. Geben Sie auf der Seite *Server* in den zentralen Einstellungen den Namen des Servers, Benutzername und Passwort ein.
2. Wählen Sie, ob es sich für LDAP bzw. SSL um die <Microsoft> bzw. <andere> Implementierung handelt.
3. Geben Sie im Eingabefeld *Importquelle* die Adresse des Servers ein, von dem die Daten importiert werden sollen.

3.10.4Vorbereitung zur Übernahme in die conpal LAN Crypt-Datenbank

Im oberen rechten Konsolenfenster werden die OUs, Gruppen und Benutzer, wie sie in der Importquelle vorhanden sind, angezeigt.

Hier können Sie auswählen, welche der angezeigten OUs, Gruppen oder Benutzer in die conpal LAN Crypt-Datenbank aufgenommen werden sollen. Die ausgewählten Objekte werden in einem ersten Schritt in die darunterliegende Ansicht übernommen, wo sie noch einmal bearbeitet werden können.

Hinweis: Das Hinzufügen eines Knotens in die untere Ansicht fügt das Objekt noch nicht in die Datenbank ein. Hier werden die Objekte nur zusammengestellt. Um sie in die Datenbank zu übertragen, klicken Sie **In die Datenbank einfügen** oder **Synchronisieren**.

3.10.4.1 Übernahmeeinstellungen

Zur Performance-Optimierung können Übernahmeeinstellungen festgelegt werden. Diese Übernahmeeinstellungen betreffen nur die Übernahme in die untere Ansicht, zur Vorbereitung auf das Übertragen der Daten in die Datenbank. Klicken auf das Symbol für die Übernahmeeinstellungen öffnet einen Dialog mit drei Optionen:

- **Status der Objekte in der Datenbank anzeigen**

  Wirkt sich nur aus, wenn in der Datenbank bereits Einträge vorhanden sind, also beim Synchronisieren der Datenbank. Ist diese Option ausgewählt, wird in der unteren Ansicht für jedes Objekt angezeigt:

  - Ob es bereits in der Datenbank vorhanden ist (in der Spalte Status).
  - Ob der angemeldete SO das Recht besitzt, die Gruppen zu modifizieren (in der Spalte Gruppe hinzufügen). Ein rotes Kreuz besagt, dass der SO kein Recht, hat die Gruppe hinzuzufügen. Ein grünes Häkchen bedeutet, dass er dieses Recht besitzt.
  - Ob der angemeldete SO das Recht besitzt, Benutzer hinzuzufügen (in der Spalte Benutzer hinzufügen). Ein rotes Kreuz besagt, dass der SO kein Recht hat, Benutzer hinzuzufügen. Ein grünes Häkchen bedeutet, dass er dieses Recht besitzt.

- **Mitgliedschaften neu berechnen und anzeigen**

  Ist diese Option aktiviert, werden auch die Gruppenmitgliedschaften (Gruppen und Benutzer, die nicht direkte Mitglieder der einzelnen Gruppen sind) angezeigt. Zur Unterscheidung zu den direkten Mitgliedern werden diese in grauen Symbolen dargestellt.

Hinweis: Die Berechnung der Mitgliedschaften kann auch erst beim Übernehmen in die Datenbank vorgenommen werden.

- **Sortieren**

  Da die alphabetische Sortierung der Einträge bei umfangreichen Gruppen sehr zeitintensiv werden kann, werden die Einträge standardmäßig nicht sortiert. Wenn Sie die Objekte alphabetisch sortieren möchten, wählen Sie diese Option.

Aktualisieren der Ansicht

Wurden beim Übernehmen keine Optionen gesetzt, können diese Aktionen nach der Übernahme über die Schaltfläche **Aktualisieren** ausgeführt werden. Klicken auf "Aktualisieren" öffnet einen Dialog mit denselben Optionen. Die Aktualisierung betrifft nur die Daten in der unteren Ansicht.

3.10.4.2 Übernehmen in die untere Ansicht

Durch einen Doppelklick auf einen Knoten bzw. durch Markieren des Knotens und Klicken auf die Schaltfläche **Übernehmen** werden die Objekte aus der Struktur der Importquelle in die untere

Ansicht übertragen. Bevor die Objekte übertragen werden, wird ein Dialog angezeigt, in dem ausgewählt werden kann, wie die einzelnen Container und Objekte übernommen werden sollen.

- **Nur dieses Objekt übernehmen**
  Fügt das ausgewählte Objekt ohne seinen Inhalt ein.
- **Direkte Mitglieder auch übernehmen**
  Fügt alle Objekte, die in dem ausgewählten Container existieren, ein.
- **Alle Mitglieder auch rekursiv übernehmen**
  Fügt alle Objekte, die in diesem Container direkt existieren, ein sowie alle Objekte, die Mitglieder sind, und in einem anderen Container existieren. Die Mitglieder werden in ihrer vollständigen Hierarchie übernommen.

Nach der Auswahl der gewünschten Option und dem Klicken auf **OK** werden die Objekte in die untere Ansicht übernommen und sind damit bereit zum Einfügen in die conpal LAN Crypt Datenbank.

Vor der Übernahme in die Datenbank können dieser Ansicht weitere Gruppen (z. B. auch aus anderen Quellen) hinzugefügt werden und dann in einem Schritt in die Datenbank eingefügt werden.

3.10.4.3 Daten in die Datenbank einfügen bzw. synchronisieren

Die Objekte werden erst in die conpal LAN Crypt Datenbank eingefügt, nachdem sie in der unteren Ansicht zusammengestellt wurden und dort dann die Schaltflächen **In die Datenbank einfügen** bzw. **Synchronisieren** gedrückt werden.

Hinweis: Werden Objekte zu einer bestehenden Struktur hinzugefügt, so müssen Sie sie immer zuerst zur Datenbank hinzufügen. Klicken Sie dazu auf **In die Datenbank einfügen**. Synchronisieren wird verwendet, wenn sich ausschließlich die Relationen zwischen den Objekten verändert haben.

Nach dem Klicken auf **In die Datenbank einfügen**, werden die Objekte zuerst eingefügt und anschließend wird der Synchronisationsprozess gestartet. Dieser Prozess beginnt mit einem Dialog mit drei Optionen.

- **Komplette Datenbank synchronisieren**
  Wird diese Option gewählt, werden alle in der conpal LAN Crypt Datenbank enthaltenen Einträge mit jenen in der Importquelle synchronisiert. Änderungen werden auf einer folgenden Zusammenstellung angezeigt.

  Diese Option muss gewählt werden, wenn Objekte im AD gelöscht wurden und diese auch aus der Datenbank gelöscht werden sollen.

Hinweis: Die komplette Synchronisierung kann bei einer komplexen Struktur viel Zeit in Anspruch nehmen.

- **Nur sichtbare Einträge synchronisieren**

  Bezieht sich auf die Auswahl im rechten unteren Fenster der Administrationskonsole.

  - **Alle Mitgliedschaften neu berechnen**

    Wird diese Option gewählt, werden alle Mitgliedschaften auf Basis der Importquelle neu berechnet und in die Datenbank eingefügt. Mitgliedschaften werden eingefügt, auch wenn sie bei der Anzeige im rechten unteren Konsolenfenster ausgeschaltet waren (die Option **Mitgliedschaften berechnen** in den Übernahmeeinstellungen war ausgeschaltet).

  - **Sichtbare Mitgliedschaften verwenden**

    Wird diese Option gewählt, werden nur die im rechten unteren Konsolenfenster sichtbaren Relationen in die Datenbank eingefügt. „Ausgeblendete Mitgliedschaften" (**Mitgliedschaften berechnen** in den Übernahmeeinstellungen deaktiviert) werden nicht in die Datenbank eingefügt.

Hinweis: Wird diese Option beim Synchronisieren verwendet und die Mitgliedschaften wurden für in der Datenbank existierende Objekte in der rechten unteren Konsolenansicht ausgeblendet, werden zuvor vorhandene Mitgliedschaften in der Datenbank gelöscht.

Nach der Auswahl einer Option und dem Klicken auf **OK** wird ein Dialog angezeigt, der die Synchronisation dokumentiert. Die Änderungen müssen in diesem Dialog bestätigt werden.

- **Alle Einträge**

  Zeigt alle Änderungen in einer Liste an. Entspricht der Summe der Einträge auf den weiteren Seiten.

- **Gelöschte Objekte**

  Zeigt die Objekte an, die seit der letzten Synchronisation in der Importquelle (Server) gelöscht wurden, die aber in der conpal LAN Crypt Datenbank noch vorhanden sind.

- **Neue Relationen im Verzeichnis**

  Zeigt die Objekte und Mitgliedschaften an, die zur conpal LAN Crypt Datenbank hinzugefügt wurden bzw. die seit der letzten Synchronisation in der Importquelle (Server) neu angelegt und noch nicht in die Datenbank übernommen wurden.

- **Alte Relationen in der Datenbank**

  Zeigt Objekte und Mitgliedschaften an, die in der Datenbank zwar noch vorhanden sind, in der Importquelle aber nicht mehr. Zum Beispiel können auf dem Server Gruppen gelöscht oder Mitgliedschaften geändert worden sein.

Hinweis: Bei der Synchronisation, werden nur Objekte ausgewertet, die mindestens einmal aus einer Importquelle in die Datenbank importiert wurden.
Werden in einer Importquelle Objekte gelöscht, werden diese Änderungen nur in die Datenbank übernommen, wenn die Option Komplette Datenbank synchronisieren verwendet wird.
In der Administration manuell hinzugefügte Gruppen und Benutzer werden bei der Synchronisation nicht ausgewertet und somit auf diesen Seiten nicht angezeigt.

Die Aktion für jedes aufgelistete Objekt kann in dieser Ansicht aufgehoben werden, in dem durch einen Klick das Häkchen bei der entsprechenden Aktion entfernt wird. Es werden nur die mit einem Häkchen versehenen Aktionen ausgeführt. Durch Klicken auf **OK** wird die Synchronisation der Daten abgeschlossen.

Nachdem OUs, Gruppen und Benutzer importiert wurden, können den einzelnen Organisationseinheiten die verantwortlichen Security Officers zugeordnet werden.

3.10.4.4 Gruppen manuell einfügen

Zum manuellen Erzeugen von Gruppen markieren Sie den Knoten/die Gruppe, unter dem/der Sie eine neue Gruppe anlegen wollen und klicken Sie auf **Neue Gruppe** im Kontextmenü.

Geben Sie einen Namen für die Gruppe ein und klicken Sie auf **OK**. Die Gruppe wird nun in der conpal LAN Crypt Administration angezeigt.

Über den *Eigenschaften* Dialog der Gruppe können Sie der Gruppe existierende Benutzer hinzufügen bzw. neue Benutzer erzeugen.

Im Gegensatz zu importierten Gruppen können manuell erzeugte Gruppen via Drag and Drop auch in der Hierarchie verschoben werden.

3.10.4.5 Verknüpfungen zwischen Gruppen

Um Verknüpfungen zu Gruppen herzustellen, können einzelne Gruppen kopiert werden und in eine andere Gruppe eingefügt werden. Die so eingefügte Gruppe wird als Verknüpfung in der übergeordneten Gruppe angezeigt. Die Mitglieder der kopierten Gruppe erben so alle Schlüssel und Verschlüsselungsregeln der übergeordneten Gruppe. Die Voraussetzung für die Vererbung der Schlüssel ist, dass diese in der übergeordneten Gruppe als vererbbar definiert wurden. Die Rechte zum Bearbeiten der Gruppe werden NICHT vererbt.

Da die Gruppe als Verknüpfung eingefügt wurde, sind ihre Verschlüsselungsregeln, Mitglieder und Zertifikate sowie Schlüssel an dieser Stelle nicht sichtbar. Sichtbar sind diese Daten nur an der tatsächlichen Position der Gruppe in der Hierarchie. Dort können auch die so vererbten Schlüssel in Verschlüsselungsregeln verwendet werden.

Zum Hinzufügen einer Gruppe zu einer anderen über eine Referenz:

1. Markieren Sie die Gruppe und klicken Sie auf **Kopieren** im Kontextmenü.

2. Markieren Sie die Gruppe, in die Sie die Gruppe einfügen wollen und klicken Sie auf **Einfügen** im Kontextmenü. Sie können eine Referenz auch durch Drag and Drop bei gedrückter STRG-Taste einfügen.

3. Sie werden gefragt, ob Sie diese Gruppe einer anderen Gruppe hinzufügen wollen. Klicken Sie auf **OK**.

4. Die Gruppe wird jetzt als Verknüpfung unterhalb der Gruppe dargestellt.

Auf diese Weise können Sie ohne großen Aufwand allen Mitgliedern einer Gruppe dieselben Rechte wie den Mitgliedern einer anderen Gruppe erteilen.

Sollen z. B. die Mitglieder von Team 1 zur Unterstützung von Team 2 zeitlich begrenzt auch auf die Daten von Team 2 zugreifen können, ist es nur notwendig, in der Gruppe Team 2 eine Verknüpfung zur Gruppe Team 1 zu erstellen. Erzeugen Sie dann neue Richtliniendateien. Bei der nächsten Anmeldung haben die Mitglieder von Team 1 auch Zugriff auf die Daten von Team 2. Sind die Arbeiten abgeschlossen, entfernen Sie die Verknüpfung aus der Gruppe Team 2 und erzeugen Sie erneut neue Richtliniendateien.
Bei der nächsten Anmeldung haben die Mitglieder von Team 1 keinen Zugriff mehr auf die Daten von Team 2.

3.10.5 Gruppen löschen

Einzelne Gruppen/OUs und Referenzen auf Gruppen/OUs können in der conpal LAN Crypt Administration gelöscht werden.

Zum **Löschen einer Gruppe** klicken Sie auf **Löschen** im Kontextmenü der entsprechenden Gruppe/OU. Es werden alle Untergruppen und die Benutzermitgliedschaften gelöscht. Die Benutzer selbst werden nur gelöscht, wenn eine OU in der conpal LAN Crypt Administration gelöscht wird. In diesem Fall werden auch die Mitgliedschaften der Benutzer, die eventuell in anderen OUs bestehen, gelöscht. Schlüssel werden NICHT gelöscht. Sie verbleiben in der conpal LAN Crypt Datenbank.
Vor dem Löschen der Gruppe wird ein Dialog angezeigt, in dem Sie das Löschen der Gruppe bestätigen müssen.

Zum **Löschen einer Referenz auf eine Gruppe** klicken Sie auf **Löschen** im Kontextmenü der entsprechenden Gruppenreferenz. Dadurch wird die Referenz gelöscht. Die Gruppe selbst wird davon nicht beeinflusst.
Vor dem Löschen der Referenz wird ein Dialog angezeigt, in dem Sie das Löschen nur dieser Referenz bestätigen müssen.

Zum Löschen aller Referenzen auf eine Gruppe steht der Befehl **Referenzen entfernen** im Kontextmenü der tatsächlichen Gruppe zur Verfügung. Klicken auf **Referenzen entfernen** löscht alle Referenzen auf die betreffende Gruppe. Die Gruppe selbst wird davon nicht beeinflusst.

3.10.6 Gruppensymbole

Abhängig davon, von wo die OUs und Gruppen importiert worden sind, werden sie in der conpal LAN Crypt Administration mit verschiedenen Symbolen angezeigt:


Symbol für den Server, von dem die OUs und Gruppen importiert worden sind.


Symbol für die Verknüpfung mit einem Server (durch Kopieren erzeugte Referenz).


Symbol für von einem Server importierte OUs.


Referenz auf eine importierte OU.


Symbol für eine von einem Server importierte Gruppe.


Referenz auf die importierte Gruppe.


Symbol für die Datei, aus der Gruppen und Benutzer importiert wurden.


Referenz auf die importierte Datei.


Symbol für eine aus einer Datei importierte Gruppe.


Referenz auf die importierte Gruppe.


Manuell in der conpal LAN Crypt Administration angelegte Gruppe.

Referenz auf eine manuell angelegte Gruppe.

3.11 SOs den Organisationseinheiten zuordnen

Nachdem OUs, Gruppen und Benutzer in die conpal LAN Crypt Administration importiert wurden, können den verschiedenen Organisationseinheiten vom Master Security Officer einzelne SOs zugeordnet werden.

Entsprechend der ihm erteilten Rechte, kann der SO dann die Organisationseinheiten, denen er zugeordnet wurde, bearbeiten.

Damit ausschließlich die Organisationseinheit, für die der Security Officer zuständig ist, für ihn bearbeitbar ist, können vom Master Security Officer die anderen Knoten für diesen Security Officer „ausgeblendet“ werden. Das bedeutet, dass die Struktur über dem Knoten, für den der Security Officer zuständig ist, zwar als Knoten sichtbar, aber nicht bearbeitbar ist.

Wenn sich der Security Officer an die conpal LAN Crypt Administration anmeldet, ist dann ausschließlich der Teil der Organisationsstruktur sichtbar, für den der SO zuständig ist.

3.11.1 Übergeordnete Gruppe eines Benutzers

Ein Benutzer kann in conpal LAN Crypt Mitglied mehrerer Gruppen sein.Er hat jedoch eine bestimmte Gruppe als übergeordnete Gruppe:

- Bei Import des Benutzers über LDAP ist die übergeordnete Gruppe die OU, zu der der Benutzer gehört.
- Bei Import des Benutzers über eine Datei, ist die übergeordnete Gruppe die Gruppe, zu der der Benutzer gemäß der Definition in der Datei gehört.
- Wird ein neuer Benutzer über den Gruppeneigenschaftendialog erstellt, so ist die übergeordnete Gruppe die Gruppe, von der aus der Gruppeneigenschaftendialog geöffnet wurde.

In der conpal LAN Crypt Administrationskonsole wird die übergeordnete Gruppe als Spalte im Ausgewählte Benutzer und Zertifikate Knoten oder im Mitglieder und Zertifikate für Gruppe Knoten angezeigt (falls im Reiter Benutzereinstellungen konfiguriert, *siehe Benutzereinstellungen auf Seite 40*).

Die übergeordnete Gruppe eines Benutzers wirkt sich in folgenden Situationen auf die Rechteauswertung aus:

- Einsehen der Eigenschaften eines Benutzers: SOs können die Eigenschaften eines Benutzers

einsehen, wenn Sie die Rechte Lesen und Sichtbar für die übergeordnete Gruppe des Benutzers haben.

- Ändern der Eigenschaften eines Benutzers: SOs können die Eigenschaften eines Benutzers ändern, wenn Sie die globale Berechtigung Benutzer verwalten und die Rechte Benutzer hinzufügen und Benutzer löschen für die übergeordnete Gruppe des Benutzers haben.
- Erzeugen von Profilen: Wenn die Berechtigung Profile erzeugen für eine Gruppe für einen SO gesetzt ist, darf der SO Profile für alle Mitglieder der Gruppe erstellen, für die die Gruppe auch das übergeordnete Objekt der Gruppe ist. Der SO darf keine Profile für Benutzer erstellen, die nur Mitglieder der Gruppe sind und eine andere übergeordnete Gruppe haben. Hierfür ist die Berechtigung Profile für alle Mitglieder erzeugen erforderlich.
- Zuweisen von Zertifikaten: Wenn Zertifikate zuweisen für eine Gruppe gesetzt ist, darf der SO allen Mitgliedern der Gruppe Zertifikate zuweisen, für die die Gruppe auch das übergeordnete Objekt der Gruppe ist. Der SO darf keine Zertifikate zu Benutzern zuweisen, die nur Mitglieder der Gruppe sind und eine andere übergeordnete Gruppe haben. Hierfür ist die Berechtigung Zertifikate allen Mitgliedern zuweisen erforderlich.
- Kopieren von Benutzern: Wenn ein SO einen Benutzer zu einer Gruppe über den Eigenschaftendialog einer Gruppe (im Reiter Mitglieder mit der Schaltfläche Hinzufügen) hinzufügen will, muss der SO das Recht Benutzer kopieren für die übergeordnete Gruppe des Benutzers haben.

3.11.2 Gruppen für einen SO sichtbar und bearbeitbar machen

1. Damit ein Knoten in der Administration für einen Security Officer sichtbar wird, muss zuerst beim Basisknoten der Organisationsstruktur das Recht **Sichtbar** gesetzt werden.
2. Markieren Sie dazu den Basisknoten der Struktur und öffnen Sie durch Klicken auf **Eigenschaften** im Kontextmenü den *Eigenschaften* Dialog für diesen Knoten.
3. Wechseln Sie zum Register *Sicherheit* und klicken Sie auf **Hinzufügen**.
   Sie können hier den Security Officer auswählen, den Sie zur Bearbeitung der Gruppen vorgesehen haben.

Hinweis: Einer Gruppe können mehrere Security Officers zugeteilt werden.

4. Durch Klicken auf **Weiter** wird der *Rechte* Dialog für diesen SO geöffnet. Wählen Sie an dieser Stelle nur das Recht *Sichtbar* aus und klicken Sie auf **Fertig stellen**. Dieses Recht wird in der Gruppenhierarchie nach unten vererbt und Sie haben damit für den SO alle Gruppen sichtbar gemacht.
   Würde sich der SO mit diesen Einstellungen an die Datenbank anmelden, würde er die gesamte Struktur in der Administration sehen, diese aber nicht bearbeiten können.
5. Im nächsten Schritt können Sie nun die Gruppen, an denen der SO keine Rechte haben soll,

und diese auch in seiner Administration nicht sehen soll, ausblenden.

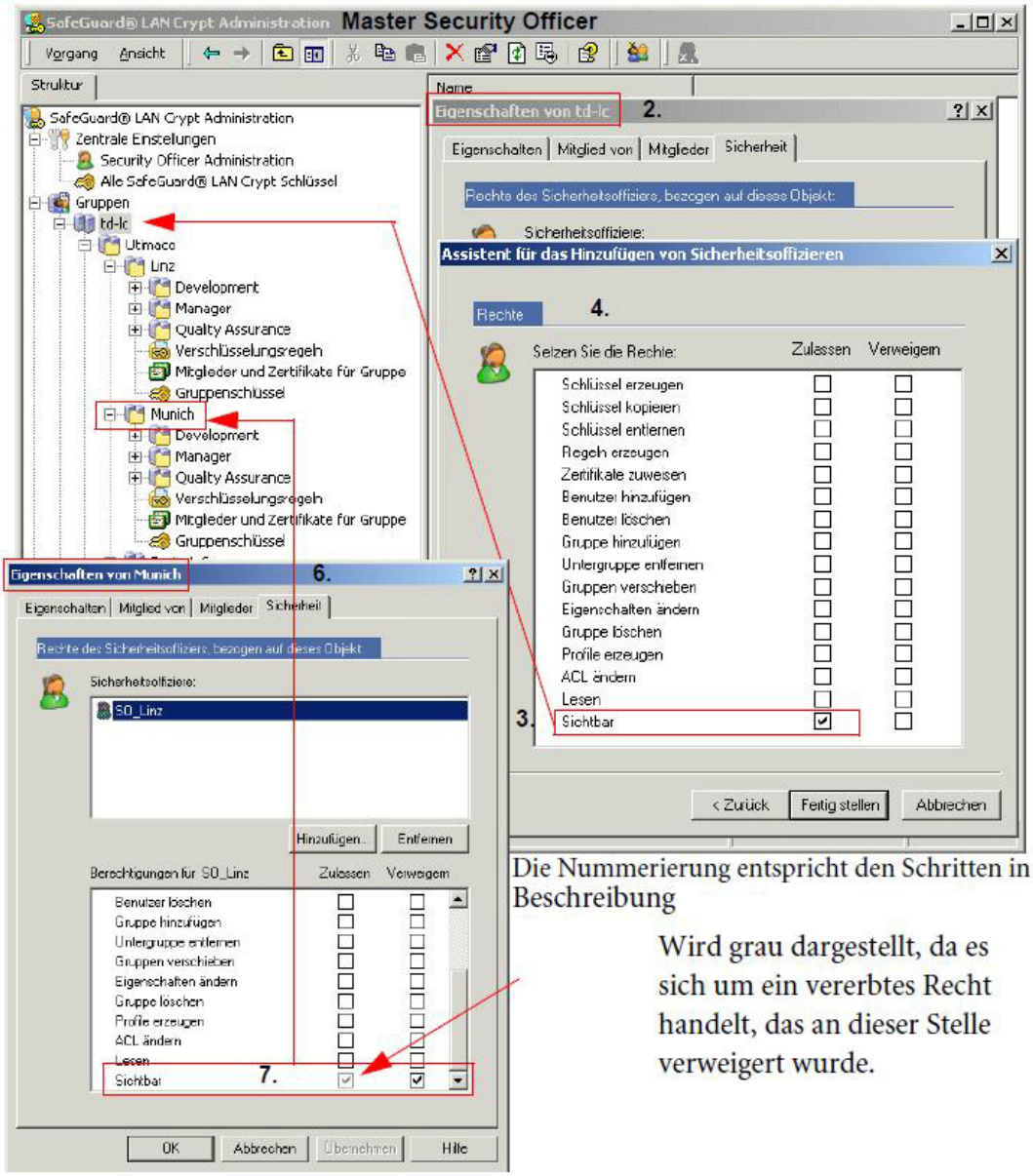
6. Markieren Sie dazu die entsprechenden Gruppen, öffnen Sie deren *Eigenschaften* Dialoge und wechseln Sie zur Seite *Sicherheit*.

7. Setzen Sie bei den Gruppen, die für den SO nicht sichtbar sein sollen, das Recht **Sichtbar** auf **Verweigern**.

Hinweis: Wurde einem SO explizit ein Recht auf einer übergeordneten Gruppe verweigert, ist eine Zulassung dieses Rechts in einer untergeordneten Gruppe nicht möglich. Es wird daher empfohlen, einem SO auf einer übergeordneten Gruppe lediglich die Rechte **Lesen** und **Sichtbar** zu erteilen, damit in untergeordneten Gruppen die Rechtevergabe problemlos möglich ist.

Hinweis: conpal LAN Crypt kann so konfiguriert werden, dass automatisch eine ACL mit Leserechten für die Stammgruppe für einen neu erstellten Security Officer angelegt wird. Hier ist erforderlich, dass der SO die globale Berechtigung Gruppen verwalten oder Benutzer verwalten hat. Dadurch wird garantiert, dass der SO Zugriff (einsehen und/oder bearbeiten) auf die Gruppen hat, für die er verantwortlich ist.
Dieses Verhalten muss im Reiter *Andere Einstellungen* unter **Zentrale Einstellungen** aktiviert werden.

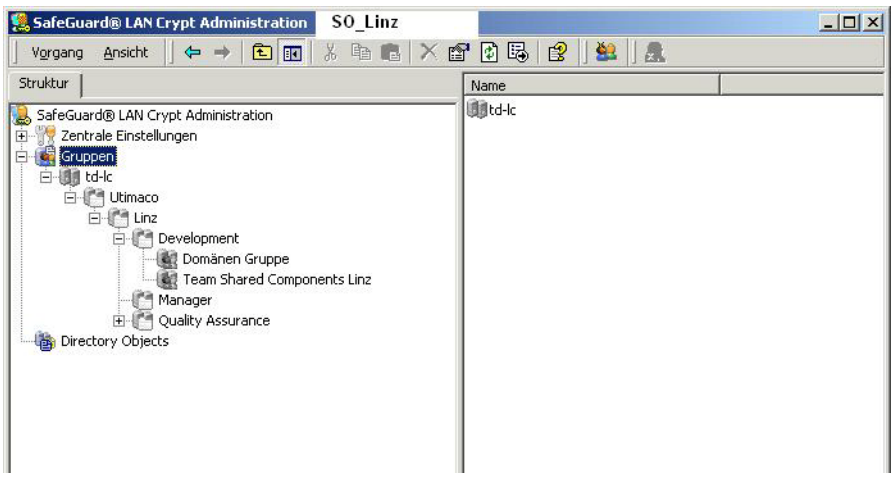
Beispiel (Master Security Officer):



Die Nummerierung entspricht den Schritten in der Beschreibung

Wird grau dargestellt, da es sich um ein vererbtes Recht handelt, das an dieser Stelle verweigert wurde.

Für den SO ergäbe sich mit diesen Einstellungen bei der Anmeldung folgendes Bild:



Es werden nur die Gruppen angezeigt, für die der SO das Recht **Sichtbar** besitzt. Diese Gruppen werden grau dargestellt, da dem SO noch keine Rechte zur Bearbeitung der Gruppen zugeteilt wurden.

Wird dem SO gleichzeitig mit dem Recht **Sichtbar** auch das Recht **Lesen** erteilt, würden unter den Gruppen auch die Snap-Ins für *Verschlüsselungsregeln*, *Mitglieder und Zertifikate für Gruppe* und *Gruppenschlüssel* angezeigt werden. Der SO könnte den Inhalt der Snap-Ins sehen, wäre aber noch nicht in der Lage, ihn zu bearbeiten.

Das Recht **Lesen** ermöglicht es, einem SO Informationen über andere Gruppen zu geben, ohne dass er diese bearbeiten darf, indem sie in seiner Ansicht einfach eingeblendet werden.

Hinweis: Wurde dem SO auch das Recht **Lesen** erteilt, so muss es explizit verweigert werden, um die Gruppen wieder auszublenden. Es genügt nicht, nur das Recht **Sichtbar** zu verweigern.

3.11.3 Dem SO Rechte zur Bearbeitung der Gruppen zuweisen

Nachdem für den SO die Gruppen sichtbar sind, die er bearbeiten soll, können ihm die entsprechenden Rechte zugeteilt werden.

Diese Rechte werden von oben nach unten in der Hierarchie vererbt und können an einer weiter unten gelegenen Stelle wieder verweigert werden.

1. Markieren Sie die Gruppe, für die Sie dem SO Rechte zuteilen wollen, öffnen Sie den Dialog *Eigenschaften* und wechseln Sie zum Register *Sicherheit.*

2. Unter Security Officers werden alle SOs angezeigt, die dieser Gruppe zugeteilt sind. Wenn Sie einen SO auswählen, werden dessen geltende Berechtigungen im unteren Teil des Dialogs angezeigt.

Aus einer anderen Gruppe **vererbte Rechte** sind durch ein graues Häkchen gekennzeichnet. Bei Rechten, die aufgrund der Einstellungen in den globalen Rechten nicht vergeben werden können, ist das Kontrollkästchen ganz ausgegraut.

Hinweis: Die für den SO zur Verfügung stehenden Rechte sind abhängig von den Einstellungen bei den globalen Rechten. Die globalen Rechte wurden bei der Erzeugung des SOs festgelegt.

Hinweis: Klicken Sie auf **Zulassen/Verweigern**, um alle Rechte in einem Schritt zuzulassen bzw. zu verweigern. Ein weiterer Klick hebt die Auswahl aller Rechte wieder auf. Sind alle Rechte markiert, können sie anschließend selektiv wieder ein bzw. ausgeschaltet werden. Ausgegraute Rechte können dem Security Officer aufgrund anderer Einstellungen nicht zugestanden werden.

Folgende Rechte können vergeben werden:

Rechte	Beschreibung
Schlüssel erzeugen	Der SO darf Schlüssel in der Gruppe erzeugen.
Schlüssel kopieren	Der SO darf Schlüssel kopieren.
Schlüssel entfernen	Der SO darf Schlüssel entfernen.
Regeln erzeugen	Der SO darf Verschlüsselungsregeln erzeugen.
Zertifikate zuweisen	Der SO darf den Benutzern Zertifikate zuweisen. Der SO darf den Assistenten zur Zertifikatszuweisung starten. Diese Berechtigung erlaubt es dem SO, den Benutzern in der Gruppe Zertifikate zuzuweisen, wenn die Gruppe auch die übergeordnete Gruppe ist.
Zertifikate allen Mitgliedern zuweisen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung Zertifikate zuweisen gesetzt ist. Zertifikate allen Mitgliedern zuweisen berechtigt einen SO zum Zuweisen von Zertifikaten zu Benutzern, wenn der SO die Berechtigung Zertifikate zuweisen für die übergeordnete Gruppe des Benutzers oder die Berechtigung Zertifikate allen Mitgliedern zuweisen für eine Gruppe, zu der der Benutzer gehört, hat. **Hinweis:** Wenn Sie Zertifikate allen Mitgliedern zuweisen auf Zulassen setzen, wird die Berechtigung Zertifikate zuweisen automatisch auf Zulassen gesetzt. Wenn Sie die Berechtigung Zertifikate zuweisen auf Verweigern setzen, wird auch die Berechtigung Zertifikate allen Mitgliedern zuweisen auf Verweigern gesetzt.

Rechte	Beschreibung
Benutzer hinzufügen	Der SO darf manuell Benutzer zur Gruppe hinzufügen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Benutzer kopieren	Der SO darf Benutzer zu Gruppen hinzufügen (kopieren). Dies ist nur denjenigen Mitgliedern erlaubt, für die diese Gruppe auch das übergeordnete Objekt ist.
Benutzer löschen	Der SO darf Benutzer über das Snap-In *Mitglieder und Zertifikate für Gruppe* löschen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Gruppe hinzufügen	Der SO darf über das Kontextmenü einer Gruppe neue Gruppen hinzufügen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Untergruppe entfernen	Der SO darf Untergruppen dieser Gruppe entfernen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Gruppen verschieben	Der SO darf manuell angelegte Gruppen in der Administration (mit Drag and Drop) verschieben. Importierte Gruppen können nicht verschoben werden. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Eigenschaften ändern	Der SO darf die Eigenschaften der Gruppe ändern
Gruppe löschen	Der SO darf Gruppen löschen. Dies setzt voraus, dass er in der übergeordneten Gruppe das Recht Untergruppe entfernen hat. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.

Rechte	Beschreibung
Profile erzeugen	Der SO darf den Profile Resolver starten und Richtliniendateien für ausgewählte Benutzer erstellen. Profile erzeugen berechtigt den SO, Profile für Benutzer zu erstellen, für die die Gruppe auch die übergeordnete Gruppe ist.
Profile für alle Mitglieder erzeugen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung Profile erzeugen gesetzt ist. Profile für alle Mitglieder erzeugen berechtigt den SO dazu, Profile für alle Benutzer in der Gruppe zu erzeugen: Benutzer, für die die Gruppe auch die übergeordnete Gruppe ist, und Benutzer, die Mitglieder der Gruppe sind, jedoch eine andere übergeordnete Gruppe haben. **Hinweis:** Wenn Sie Profile für alle Mitglieder erzeugen auf Zulassen setzen, wird die Berechtigung Profile erzeugen automatisch auf Zulassen gesetzt. Wenn Sie Profile erzeugen auf Verweigern setzen, wird die Berechtigung Profile für alle Mitglieder erzeugen automatisch auf Verweigern gesetzt.
ACL ändern	Der SO darf die ACL dieser Gruppe ändern (z. B. einen anderen SO hinzufügen).
Lesen	Der SO hat Leserechte an dieser Gruppe, er kann den Inhalt der Snap-Ins sehen. Wird automatisch gesetzt, wenn Bearbeitungsrechte vergeben werden.
Sichtbar	Die Gruppe ist für den SO sichtbar. Wird am Basisknoten gesetzt und nach unten vererbt. Wird es dem SO verweigert, wird die Gruppe ausgeblendet (auch Lesen muss verweigert sein).

3. Wählen Sie die Rechte aus, die Sie dem SO zuteilen wollen. **Übernehmen** speichert die Einstellungen in der Datenbank.

4. Haben Sie dieser Gruppe weitere SOs zugeordnet, können Sie jetzt auch deren Rechte einstellen. Markieren des SOs unter *Security Officers* zeigt dessen eingestellte Rechte an.

Hinweis: Änderungen an den Berechtigungen eines SO für eine Gruppe werden erst wirksam, wenn der SO sich wieder an der conpal LAN Crypt angemeldet hat.

3.12 Eigenschaften von Gruppen

Der Dialog *Eigenschaften* einer Gruppe (<Gruppe>/Kontextmenü/Eigenschaften) besteht aus vier Seiten, auf denen die Eigenschaften der Gruppe bearbeitet werden können.

3.12.1 Der Reiter Eigenschaften

Der Reiter Eigenschaften zeigt

- Name
- DNS Name
- GUID
- Kommentar

zur Gruppe an.

3.12.2 Der Reiter Mitglied von

Auf dem Reiter *Mitglied von* werden jene Gruppen angezeigt, in denen die aktuelle Gruppe Mitglied ist

3.12.3 Mitglieder hinzufügen/entfernen

Auf der Seite *Mitglieder* können der aktuellen Gruppe Mitglieder hinzugefügt werden. In der Liste werden alle vorhandenen Benutzer und Gruppen, die Mitglieder dieser Gruppe sind, angezeigt. Es können nur die aufgelisteten Benutzer bearbeitet werden, keine Gruppen!

Hinzufügen:

Öffnet einen Dialog, in dem Benutzer ausgewählt werden können, die dann der Gruppe hinzugefügt werden können.

Es werden entweder alle Benutzer angezeigt oder es können Benutzergruppen bzw. einzelne Benutzer mit Hilfe von SQL Platzhaltern ausgewählt werden.

Da das Anzeigen aller Benutzer sehr zeitaufwendig werden kann, ermöglicht conpal LAN Crypt das Einschränken der Suche durch die Definition von Suchkriterien.

Durch Auswählen der Option *Passende Benutzer anzeigen* werden die Eingabefelder zum Festlegen der Suchkriterien aktiviert:

Folgende Informationen über die Benutzer werden aus der conpal LAN Crypt Datenbank ermittelt:

- Logonname
- Benutzername
- Zuordnung zwischen Benutzer und Zertifikat
- Antragssteller des Zertifikats
- Seriennummer des Zertifikats
- Datum, ab welchem das Zertifikat gültig ist
- Datum, bis zu dem das Zertifikat gültig ist
- Name der Parentgruppe

Basierend auf diesen Attributen können die Suchkriterien angegeben werden. conpal LAN Crypt sucht nach festgelegten Zeichenketten in den ausgelesenen Attributen der Benutzer.

In der ersten Dropdownliste können Sie auswählen, auf welche/welches Attribut/e die Suche angewendet werden soll.

Daneben können Sie festlegen, ob die Zeichenkette enthalten sein soll (*soll sein*) oder ob nur Benutzer angezeigt werden, in denen die Zeichenkette im ausgewählten Attribut nicht enthalten sein darf (*darf nicht sein*).

In der Dropdownliste ganz rechts können Sie die eigentliche Zeichenkette, die conpal LAN Crypt im angegebenen Attribut sucht, eingeben.

Zur Angabe der Zeichenkette können Sie folgende SQL-Platzhalter verwenden:

%	beliebige Zeichenfolge
_	einzelnes Zeichen (z.B. a__ bedeutet suche nach allen Namen mit drei Buchstaben, die mit a beginnen)
[]	einzelnes Zeichen aus einer Liste (z.B. [a-cg]% bedeutet suche nach allen Namen, die mit a,b,c oder g beginnen)
[^]	einzelnes Zeichen, das nicht in einer Liste ist (z.B. [^a]% bedeutet suche nach allen Namen, die mit a beginnen)

Sie können bis zu drei Bedingungen für die Suche angeben.

Geben Sie mehr als eine Bedingung an, können Sie festlegen, wie diese Bedingungen verknüpft werden sollen (UND/ ODER).

Durch Klicken auf OK werden alle in der Liste markierten Benutzer der aktuellen Gruppe hinzugefügt.

Neu:
Öffnet einen Dialog, in dem ein neuer Benutzer angelegt werden kann.

Löschen:
Löscht die ausgewählte Benutzermitgliedschaft aus der aktuellen Gruppe.
Wenn der Benutzer keiner weiteren Gruppe angehört, wird er aus der conpal LAN Crypt Datenbank gelöscht.
Wenn der Benutzer mehreren Gruppen angehört, und es sich bei der aktuellen Gruppe um die übergeordnete Gruppe des Benutzers handelt, hängt die resultierende Aktion vom Typ der Gruppe ab:

- Wenn es sich bei der Gruppe um eine Organizational Unit oder eine Stammgruppe handelt und der Benutzer Mitglied einer anderen OU oder Stammgruppe ist, wird diese OU oder Stammgruppe zur übergeordneten Gruppe des Benutzers. Wenn keine andere OU oder Stammgruppe vorhanden ist, der der Benutzer angehört, wird der Benutzer gelöscht (ähnlich wie bei Active Directory oder Novell. Hier wird der Benutzer gelöscht, wenn die OU, der er angehört, gelöscht wird.)
- Wenn es sich bei der Gruppe um eine einfache Gruppe (keine OU oder Stammgruppe) handelt, wird eine der anderen Gruppen, denen der Benutzer angehört, zur übergeordneten Gruppe des Benutzers.

Eigenschaften:
Zeigt die Eigenschaften des markierten Benutzers an.

Hinweis: Ein Benutzer darf in einem Container genau einmal vorhanden sein. Wird versucht, einen Benutzer in einem Container anzulegen/hinzuzufügen, der bereits darin enthalten ist, wird eine Meldung angezeigt, dass dies nicht möglich ist.
Es kann im System jedoch mehrere Benutzer geben, die den gleichen Namen haben, solange sie sich nicht im selben Container befinden.

3.12.4SOs hinzufügen

Auf der Seite *Sicherheit* kann auch ein SO der aktuellen Gruppe weitere SOs hinzufügen und ihnen Rechte an der Gruppe zuweisen. Voraussetzung dafür ist, dass der SO, der einen weiteren SO hinzufügen will, das Recht **ACL ändern** besitzt.

Hinweis: Der SO kann jenen SO, den er der Gruppe hinzufügt, nur mit Rechten ausstatten über die er selbst verfügt.
Ein SO kann sich selbst nicht in ACLs aufnehmen oder seine eigenen Rechte in einer ACL bearbeiten.

3.13 Eigenschaften von Benutzern

Der Dialog *Eigenschaften* eines Benutzers (<Benutzer>/Kontextmenü/Eigenschaften) besteht aus vier Seiten, auf denen die Eigenschaften des Benutzers bearbeitet werden können.

Zertifikate

Auf der Seite *Zertifikate* werden alle Zertifikate, die dem Benutzer zugeordnet sind, angezeigt. Hier kann auch ein neues conpal LAN Crypt Zertifikat für den Benutzer erzeugt werden, ein bestehendes Zertifikat aus dem Zertifikatsspeicher hinzugefügt werden und ein Zertifikat aus einer Datei importiert werden (siehe *Zertifikat einem Benutzer zuordnen* auf Seite 120).

Gruppen

Auf der Seite *Gruppe* werden jene Gruppen angezeigt, in denen der Benutzer Mitglied ist.

Regeln

Auf der Seite *Regeln* werden alle Verschlüsselungsregeln, die für den Benutzer gültig sind, angezeigt. Sie gibt einen schnellen Überblick über alle Regeln, die für den Benutzer gelten, auch wenn sie aus verschiedenen Gruppen stammen.

Die Spalten S, X, I geben Auskunft, um welche Art von Regeln es sich handelt:

- **S** (Subdirectories): Unterverzeichnisse werden in die Verschlüsselung eingeschlossen.
- **X** (Exclude path): Pfad wird von der Verschlüsselung ausgeschlossen.
- **I** (Ignore path): Der Ordner wird von conpal LAN Crypt ignoriert. Weitere Informationen, siehe *Erzeugen von Verschlüsselungsregeln* auf Seite 114.

Unter **Geerbt von** ist ersichtlich, aus welchen Gruppen die einzelnen Regeln geerbt wurden.

Details

Auf der Seite *Details* werden die Daten des Benutzers angezeigt und können dort bearbeitet werden.

Die E-Mail-Adresse wird auch in die Passwortprotokolldatei für von conpal LAN Crypt erzeugte Zertifikate eingetragen. So kann sie z. B. für die Erstellung eines PIN Mailers via E-Mail verwendet werden.

Hinweis: Bitte gehen Sie bei einer eventuellen Änderung der Benutzerdaten vorsichtig vor. Es können dabei leicht unerwünschte Nebeneffekte auftreten.
Zum Beispiel kann eine Änderung des Logonnamens an dieser Stelle bewirken, dass der Benutzer keinen Zugriff auf seine Richtliniendatei mehr hat, da der Client nach einer Richtliniendatei mit einem anderem -dem alten - Logonnamen sucht.

3.14 Design der Sicherheitsumgebung

Durch seine große Flexibilität ist es möglich, conpal LAN Crypt an die Sicherheitserfordernisse jedes Unternehmens anzupassen.

Doch ist es von großer Bedeutung, eine unternehmensweite Sicherheitsstrategie zu entwerfen, bevor die conpal LAN Crypt Umgebung aufgebaut wird.

Generell ist zu empfehlen, mit einer eher restriktiven Sicherheitspolitik zu beginnen, da es leichter ist, diese zu lockern, als hinterher eine strengere Sicherheitspolitik im conpal LAN Crypt System einzuführen. Im letzteren Fall können Sicherheitsprobleme auftreten, die nicht leicht zu lösen sind. Um dies zu vermeiden, ist es äußerst wichtig, eine unternehmensweite Sicherheitspolitik zu definieren, bevor die Verschlüsselungsprofile erzeugt und verteilt werden.

3.15 Schlüssel erzeugen

Neue Schlüssel werden unter dem Gruppenknoten der Gruppe erzeugt, für die sie verwendet werden sollen. Für jeden Schlüssel kann festgelegt werden, ob er in der Hierarchie der Gruppen nach unten vererbt werden soll.

Hinweis: Alle in der conpal LAN Crypt-Datenbank vorhandenen Schlüssel werden unter **Zentrale Einstellungen \Alle conpal LAN Crypt Schlüssel** angezeigt. Sie können dort aber nicht bearbeitet werden. Diese Ansicht stellt einen Überblick über die in conpal LAN Crypt verwendeten Schlüssel dar.

Hinweis: Ein SO, der das Recht **Profile erzeugen** nicht hat, sondern nur das Recht **Schlüssel erzeugen**, darf beim Anlegen des Schlüssels keinen Wert vergeben! Der Wert wird bei der ersten Übertragung des Schlüssels in ein Profil automatisch erzeugt.

Ein conpal LAN Crypt Schlüssel besteht aus folgenden Komponenten:

- **Name**
  Im Sinne einer Übersichtlichkeit ist es empfehlenswert, dass der Namen der Benutzergruppe Teil des Schlüsselnamens ist.
  Da conpal LAN Crypt auch über die Fähigkeit verfügt, Schlüssel zu sortieren, kommt der Namengebung besondere Bedeutung zu.
  conpal LAN Crypt erzeugt aus dem angegebenen Schlüsselnamen einen 16 Zeichen langen Schlüsselnamen zur internen Verwendung. Diesem Schlüsselnamen wird der Prefix für die entsprechende Region vorangestellt.

- **Schlüsselwert**
  Die Länge des Schlüssels ist abhängig vom gewählten Algorithmus. Der Schlüsselwert kann entweder in ANSI-Zeichen oder in Hexadezimal-Notation (erlaubte Zahlen bzw. Zeichen: 0123456789abcdef) eingegeben werden. Der jeweils andere Wert wird automatisch ergänzt.

Es muss kein Schlüsselwert angegeben werden. In diesem Fall wird der Wert zufällig erzeugt, sobald der Schlüssel das erste Mal in einem Benutzerprofil verwendet wird.

- **Verschlüsselungsalgorithmus**
  AES-128, AES-256, DES, 3DES, IDEA, XOR
- **Kommentar** (optional)
- **Schlüssel-GUID** (optional)
  Ermöglicht die manuelle Eingabe einer Schlüssel-GUID, um verschlüsselte Dateien zwischen zwei unterschiedlichen conpal LAN Crypt Installationen austauschen zu können (siehe *Schlüssel* auf Seite 42).
  Bleibt das Feld leer, wird automatisch eine GUID gebildet.

Um einen neuen Schlüssel zu erzeugen

1. Markieren Sie **Gruppenschlüssel** unter der Gruppe, für die Sie einen Schlüssel erzeugen wollen.
2. Klicken Sie auf das gelbe Schlüsselsymbol in der Symbolleiste oder klicken Sie nach einem Rechtsklick im rechten Fenster der Konsole auf **Neuer Schlüssel** im Kontextmenü.
3. Geben Sie einen Namen für den neuen Schlüssel in das oberste Eingabefeld ein. Backslash (\), Slash (/), Hochkomma und das & Zeichen sind keine gültigen Zeichen für Schlüsselnamen. conpal LAN Crypt erzeugt aus diesem Namen einen 16 Zeichen langen eindeutigen Schlüsselnamen zur internen Verwendung. Dabei wird diesem eindeutigen Namen der Prefix für die Region (falls dieser in den Eigenschaften des Security Officers angegeben wurde) vorangestellt. Der interne Name wird rechts, neben der Dropdownliste zur Auswahl des Algorithmus, angezeigt.
   Der Schlüsselname kann später geändert werden (im **Eigenschaften** Dialog des betreffenden Schlüssels), der daraus erzeugte, interne Name, nicht.
4. Wählen Sie einen Verschlüsselungsalgorithmus aus der Dropdownliste aus (AES, AES256, DES, 3DES, IDEA, XOR).
   Es werden hier nur die Algorithmen, die Sie in den *Zentralen Einstellungen* als verfügbar angegeben haben, angezeigt.
5. Geben Sie an, ob der Schlüssel an die Untergruppen vererbt werden soll:
   - **Nein**
     Der Schlüssel wird nicht vererbt und steht damit nur in der aktuellen Gruppe zur Verfügung.
   - **Einmal**
     Der Schlüssel wird in die Gruppe(n), die sich eine Hierarchieebene unter der aktuellen

Gruppe befinden, vererbt.

- **Ja**
  Der Schlüssel wird an alle Gruppen, die sich unter der aktuellen befinden, vererbt und steht dort zum Erzeugen der Verschlüsselungsregeln zur Verfügung.

6. Im nächsten Eingabefeld können Sie einen Kommentar zu diesem Schlüssel eingeben.

7. Aktivieren Sie bei Bedarf das Kontrollkästchen **Schlüssel-GUID manuell im Format 88888888-4444-4444-4444-CCCCCCCCCCCC eingeben** und geben Sie die gewünschte GUID ein (setzt aktivierte Option "Security Officers dürfen die GUID neuer Schlüssel festlegen" in Einstellungen von "Zentrale Einstellungen" voraus). Die voreingestellte GUID 88888888-4444-4444-4444-CCCCCCCCCCCC kann hier nicht einfach übernommen werden.
   Sie muss in jedem Fall angepasst werden.

8. Geben Sie einen Hexadezimalwert (Buchstaben A-F, Ziffern 0-9) in das Eingabefeld oder eine Zeichenkette in das Eingabefeld für den Schlüsselwert ein. Der jeweils andere Wert wird automatisch ergänzt. Oder klicken Sie auf **Zufällig** (empfohlen), um conpal LAN Crypt einen Wert berechnen zu lassen.

9. Klicken Sie auf **OK**.

▶ Der neue Schlüssel wird in der Schlüsselansicht der Konsole angezeigt.

3.15.1 Spezifische Schlüssel

Neben den so erzeugten Schlüsseln bietet conpal LAN Crypt auch die Möglichkeit, benutzer- bzw. gruppenspezifische Schlüssel zu verwenden.

Beim Erzeugen der Verschlüsselungsregeln wird in der Liste der Schlüssel auch immer ein Schlüssel <**USERKEY**> angezeigt. Dabei handelt es sich um einen Platzhalter für einen benutzerspezifischen Schlüssel, der bei der Auflösung der Verschlüsselungsregeln automatisch für jeden einzelnen Benutzer erzeugt wird.
<**GROUPKEY**>
Analog zu zur Verwendung von <USERKEY> kann durch die Verwendung von <GROUPKEY> ein gruppenspezifischer Schlüssel für alle Mitglieder der Gruppe erzeugt werden. Bei der Auflösung der Verschlüsselungsregeln wird der Gruppenschlüssel automatisch erzeugt.

Beispiel: Netzwerklaufwerk U:verbunden haben, das je ein Verzeichnis für einen Benutzer enthält, auf das ausschließlich der betreffende Benutzer Zugriff haben soll.
Eine solche Verschlüsselungsregel könnte folgendermaßen aussehen:

```
U:\*.* <USERKEY>
```

Ein weiteres Beispiel für die Anwendung von <USERKEY> wäre die Verschlüsselung von lokalen temporären Verzeichnissen.

Benutzer- und gruppenspezifische Schlüssel werden in der Standardansicht unter Zentrale Einstellungen/Alle conpal LAN Crypt Schlüssel nicht angezeigt, da sie in der Regel nicht benötigt werden. Ein Master Security Officer oder ein Security Officer mit dem globalen Recht Spezifische Schlüssel verwenden kann diese Schlüssel jedoch bei Bedarf einblenden, sodass die Daten der einzelnen Schlüssel sichtbar werden.

Im *Eigenschaften* Dialog des Schlüssels (Kontextmenü/**Eigenschaften**) kann bei Bedarf auch der Schlüsselwert eines spezifischen Schlüssels eingeblendet werden.

Zum Einblenden der spezifischen Schlüssel klicken Sie in der Liste der verfügbaren Schlüssel mit der rechten Maustaste und wählen Sie **Spezifische Schlüssel anzeigen** aus dem Kontextmenü. Es werden dann ausschließlich die spezifischen Schlüssel angezeigt. Zum Wechseln in die Standardansicht klicken Sie erneut auf **Spezifische Schlüssel anzeigen**.

Hinweis: Spezifische Schlüssel werden nicht aus der Datenbank entfernt, wenn die dazugehörigen Benutzer/Gruppen gelöscht werden. Sie verbleiben in der Datenbank und können unter Zentrale Einstellungen/Alle conpal LAN Crypt Schlüssel/Spezifische Schlüssel anzeigen angezeigt werden.

Spezifische Schlüssel wieder zuweisen

Es können Situationen auftreten, in denen es notwendig wird, einen benutzer- bzw. gruppenspezifischen Schlüssel wieder einem Benutzer einer Gruppe zuzuweisen.

Beispiel: Ein Benutzer wird aus dem Active Directory in conpal LAN Crypt importiert. Für diesen Benutzer wird dann ein Benutzerschlüssel angelegt. Wird dann die Gruppe, in der sich der Benutzer befindet, in conpal LAN Crypt komplett gelöscht und die Gruppe dann wieder importiert, wird für den Benutzer beim Erzeugen der Richtliniendateien automatisch ein neuer Benutzerschlüssel erzeugt.
Auf Daten, die zuvor mit dem „alten“ Benutzerschlüssel verschlüsselt waren, kann der Benutzer dann nicht mehr zugreifen.

Um solche Situationen zu vermeiden, kann conpal LAN Crypt so konfiguriert werden, dass es möglich ist, die spezifischen Schlüssel von einmal gelöschten Benutzern/Gruppen wieder zuzuweisen.

Fügen Sie dazu den DWORD-Wert mit dem Namen `"ShowUserKeyPage"` und dem Wert `"1"` in der Windows-Registierung unter dem Schlüssel

```
HKEY_LOCAL_MACHINE\
SOFTWARE\
Policies\
Sophos\
SGLANCrypt
```

hinzu. Dieser Eintrag in der Registrierung kann auch benutzerspezifisch unter `HKEY_CURRENT_USER\....` eingefügt werden.

Ist dieser Wert in der Windows-Registrierung vorhanden, so wird der Reiter *Spezifischer Schlüssel* dem Dialog *Eigenschaften*
von Gruppen und Benutzern hinzugefügt (<Benutzer/Gruppe>/Kontextmenü/Eigenschaften).

In diesem Reiter können Benutzern/Gruppen in der Datenbank vorhandene nicht zugeordnete spezifische Schlüssel zugeordnet werden.

Ist dem Benutzer/der Gruppe ein spezifischer Schlüssel zugeordnet, wird er auf der Seite *Spezifischer Schlüssel* angezeigt. Sie können den aktuellen spezifischen Schlüssel durch einen anderen ersetzen bzw. einen existierenden zuweisen, wenn kein spezifischer Schlüssel angezeigt wird. Zur Verfügung stehen alle spezifischen Schlüssel, die in der Datenbank vorhanden sind und keinem Benutzer/keiner Gruppe zugeordnet sind.

Hinweis: Ein SO benötigt das Recht **Spezielle Schlüssel verwenden**, um eine Änderung vornehmen zu können. Besitzt er dieses Recht nicht, hat der SO nur Leserechte.

Durch Klicken auf die **Durchsuchen...**Schaltfläche wird eine Liste aller verfügbaren spezifischen Schlüssel angezeigt. Wählen Sie einen aus und klicken Sie auf **OK**.

Klicken Sie im Register Spezifischer Schlüssel auf **OK**.

Wurde der aktuelle spezifische Schlüssel durch einen anderen ersetzt, verbleibt er als nicht zugeordneter spezifischer Schlüssel in der Datenbank.

3.15.2 Schlüssel importieren

Diese Version von conpal LAN Crypt erlaubt es, Schlüssel der Versionen 2.x zu verwenden. Die Schlüssel der Versionen 2.x können zu diesem Zweck aus Schlüsseldateien der Versionen 2.x importiert werden.

Voraussetzung dafür ist, dass die Schlüssel in den Schlüsseldateien als **exportierbar** markiert sind, Sie über die Master-ID und das Masterpasswort für die Schlüsseldatei verfügen und Sie als Security Officer die entsprechenden Rechte besitzen. Die Datei darf nicht schreibgeschützt sein.

Zum Importieren der Schlüssel markieren Sie den Knoten *Gruppenschlüssel* unter der betreffenden Gruppe und klicken Sie auf **Schlüssel aus Schlüsseldatei** importieren im Kontextmenü.

Wählen Sie die Schlüsseldatei aus und geben Sie unter *Benutzername* die Master-ID und unter *Passwort* das Masterpasswort der Schlüsseldatei an.

Klicken Sie auf **OK**. Die Schlüssel werden im rechten Konsolenfenster angezeigt.

3.15.3 Aktiver/nicht aktiver Schlüssel

conpal LAN Crypt bietet die Möglichkeit, bestehende Schlüssel passiv zu schalten. Dies hat die Auswirkung, dass dieser Schlüssel bei der Definition von Verschlüsselungsregeln nicht mehr zur Verfügung steht.

In bereits verwendeten Verschlüsselungsregeln kann dieser Schlüssel weiter verwendet werden. Er bleibt in der Administrationsdatenbank gespeichert und kann bei Bedarf auch wieder aktiviert werden.

Zum Passiv/Aktiv schalten markieren Sie den Schlüssel und klicken Sie auf **Passiv/Aktiv** im Kontextmenü.

Ein rotes Schlüsselsymbol am Beginn einer Zeile markiert einen passiv geschalteten Schlüssel.

3.15.4 Schlüssel referenzieren

Neben dem Anlegen eines Schlüssels in einer Gruppe können den Benutzern einer Gruppe auch Schlüssel aus einer anderen Gruppe über eine Referenz zur Verfügung gestellt werden.

Beispiel: Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre, wenn den Mitgliedern einer Gruppe zeitlich begrenzt Zugriff auf verschlüsselte Daten einer anderen Gruppe gegeben werden soll. Dazu kann der Schlüssel aus einer Gruppe über eine Referenz in die andere Gruppe eingefügt werden und dort zum Erzeugen von Verschlüsselungsregeln für die Daten der anderen Gruppe verwendet werden.
Ohne die Möglichkeit der Referenzierung müsste zur Realisierung dieses einfachen Datenaustausches eine neue Gruppe angelegt werden, dort die Benutzer beider Gruppen hinzugefügt werden, dann neue Schlüssel und Verschlüsselungsregeln definiert werden. Die Referenzierung stellt eine Möglichkeit dar, den Datenaustausch einfach und schnell zu gestalten.

Um einen Schlüssel einer anderen Gruppe über Referenz hinzuzufügen ziehen Sie den Knoten *Gruppenschlüssel* einer Gruppe in den Knoten der betreffenden Gruppe. Sie können den Schlüssel der Quellgruppe auch kopieren und in die Zielgruppe einfügen.

Ein Schlüssel, der über eine Referenz eingefügt wurde, wird durch dieses Symbol gekennzeichnet  .

Damit ein Security Officer Schlüssel über eine Referenz einfügen darf, muss er über folgende globale Rechte verfügen:

- **Schlüssel erzeugen**
- **Schlüssel kopieren**

Zusätzlich benötigt er in der Quellgruppe das **gruppenspezifische Recht**

- **Schlüssel kopieren**

und

- **Schlüssel erzeugen**

in der Zielgruppe.

Für das Löschen einer Referenz benötigt er das globale und gruppenspezifische Recht **Schlüssel entfernen**.

Referenzierte Schlüssel haben folgende Eigenschaften:

- Sie werden NICHT vererbt und stehen daher ausschließlich in der Gruppe zur Verfügung, in der sie erzeugt wurden. Sie stehen NICHT in Untergruppen zur Verfügung.
- Wird das „Original" aus seiner Gruppe entfernt, werden damit auch alle Referenzen entfernt.

Hinweis: Analog zu „normalen" Gruppenschlüsseln bedeutet das Entfernen einer Referenz nicht, dass die Regel, in der sie verwendet wurde, nicht mehr gültig ist. Damit kein Zugriff auf die Daten (siehe Beispiel) mehr möglich ist, muss die entsprechende Regel gelöscht werden und eine neue Richtliniendatei erzeugt werden. Erst nachdem der Client die neue Richtliniendatei geladen hat, kann er nicht mehr auf die Daten zugreifen.

3.15.5 Schlüssel aus Gruppen entfernen

Das Löschen eines Schlüssels ist nur in der Gruppe, in der der Schlüssel erzeugt wurde, möglich. Der Schlüssel muss vor dem Löschen deaktiviert werden.

Schlüssel, die in Verwendung sind, werden beim Löschen zwar aus der Gruppe entfernt, verbleiben aber als nicht zugeordnete Schlüssel in der Datenbank und werden unter *Zentrale Einstellungen*/*Alle conpal LAN Crypt Schlüssel* weiter angezeigt.

Schlüssel wieder hinzufügen

Sollte ein aus einer Gruppe entfernter Schlüssel später wieder benötigt werden (z. B. zum Zugriff auf ein verschlüsseltes Backup alter Daten), kann er mittels Drag and Drop einfach aus der Liste aller conpal LAN Crypt Schlüssel auf die betreffende Gruppe gezogen werden und steht dort wieder zur Verfügung. Der Schlüssel kann jeder beliebigen Gruppe, für die der ausführende Security Officer das Recht **Schlüssel erzeugen** hat, hinzugefügt werden. Dabei wird der Schlüssel tatsächlich der Gruppe hinzugefügt, es handelt sich nicht um eine Referenz.

Hinweis: Wird ein Schlüssel entfernt, der nie in einer Regel verwendet wurde, wird er aus der Datenbank gelöscht. Dieser Schlüssel wird auch nicht mehr unter Alle conpal LAN Crypt Schlüssel angezeigt.

3.15.6 Schlüssel aus der Datenbank löschen

Unter folgenden Voraussetzungen können Schlüssel unter *Alle conpal LAN Crypt Schlüssel* tatsächlich aus der Datenbank gelöscht werden:

- Der Ausführende muss als Master Security Officer angemeldet sein.
- Der Schlüssel darf in keiner Regel verwendet werden.
- Der Schlüssel darf in keiner Gruppe vorhanden sein.
- Der Schlüssel darf kein spezifischer Schlüssel, der einem Benutzer oder einer Gruppe zugeordnet ist, sein.
- Der Schlüssel muss deaktiviert sein.

3.15.7 Schlüssel bearbeiten

Der Schlüsselname, die Art der Vererbung und der Kommentar zu einem Schlüssel können geändert werden, nachdem der Schlüssel erzeugt wurde.

Ob ein Schlüssel bereits in Verwendung ist, wird in der Spalte *verwendet* im Schlüsselfenster der Konsole angezeigt.

Zum Ändern eines Schlüssels, wechseln Sie in die Gruppe, in der der Schlüssel erzeugt wurde und klicken Sie doppelt auf den entsprechenden Schlüsselnamen. In diesem Dialog kann der Schlüssel geändert werden.

3.15.7.1 Der Dialog Eigenschaften

Der Dialog *Eigenschaften* zeigt Informationen zum ausgewählten Schlüssel an. Er ermöglicht die Änderung des langen Schlüsselnamens und der Einstellungen, die die Vererbung des Schlüssels betreffen. Der von conpal LAN Crypt erzeugte 16 Zeichen lange interne Schlüsselname kann nicht geändert werden.

Hinweis: Zum Bearbeiten des Schlüssels muss der Security Officer das gruppenspezifische Recht **Schlüssel erzeugen** in der Gruppe, in der der Schlüssel erzeugt wurde, besitzen.
Schlüssel, die in keiner Gruppe vorhanden sind, können nicht bearbeitet werden.

Zur Anzeige der Eigenschaftenseiten eines Schlüssels klicken Sie doppelt auf den Schlüssel.

Der *Eigenschaften* Dialog besteht aus drei Registern:

- Im Register *Schlüssel* werden die Daten des Schlüssels angezeigt. Hier können Sie den langen Schlüsselnamen sowie die Einstellungen, die die Vererbung des Schlüssels betreffen, ändern. Durch Aktivieren der Option Schlüsselwert anzeigen kann auch der Schlüsselwert eingeblendet werden.

- Auf der Seite *Gruppen* wird angezeigt, in welchen Gruppen der Schlüssel für Regeln zur Verfügung steht.
- Auf der Seite *Regeln* werden alle Regeln, in denen der Schlüssel verwendet wird, angezeigt.

Die Seite *Gruppen* und *Regeln* dienen nur Informationszwecken. Es können hier keine Veränderungen vorgenommen werden.

3.16 Verschlüsselungsregeln

Die conpal LAN Crypt Verschlüsselungsregeln definieren genau, welche Daten mit welchem Schlüssel verschlüsselt werden sollen. Eine Verschlüsselungsregel besteht aus einem Verschlüsselungspfad und einem Schlüssel.

Die Verschlüsselungsregeln, die für eine Gruppe definiert werden, bilden ein conpal LAN Crypt Verschlüsselungsprofil.

Das Verschlüsselungsprofil für eine Gruppe kann verschiedene Verschlüsselungsregeln enthalten, wobei jede einzelne einen ganz bestimmten Typ von Daten verschlüsselt.

Es besteht die Möglichkeit, ganze Verzeichnisse (einschließlich Unterverzeichnisse), bestimmte Dateitypen (identifiziert durch die Dateiendungen) und einzelne Dateien (identifiziert durch den Dateinamen oder Teilen davon) zu verschlüsseln.

Beim Erzeugen der einzelnen Verschlüsselungsregeln werden alle für die Gruppe vorhandenen Schlüssel angezeigt. Der conpal LAN Crypt Security Officer kann nun durch die Zuweisung der entsprechenden Schlüssel festlegen, auf welche Daten die Benutzer Zugriff haben sollen.

Verschlüsselungsregeln werden immer auf Gruppenbasis erzeugt. Sie bestehen aus einem Pfad und einem Schlüssel und werden unter dem Knoten **Verschlüsselungsregeln** angelegt. Pfadangabe, Schlüsselauswahl und verschiedene Optionen sind in einem Dialog zusammengefasst, sodass eine Verschlüsselungsregel einfach erzeugt werden kann.

Verschlüsselungsregeln werden immer an untergeordnete Gruppen vererbt.

Hinweis: Für den Ordner „Temporäre Internetdateien“ sollte keine Verschlüsselungsregel definiert werden.

3.16.1 Verschlüsselungspfade

Die Verschlüsselungspfade definieren, welche Daten verschlüsselt werden sollen. Sie definieren diese im Knoten **Verschlüsselungsregeln** *unter dem jeweiligen Gruppenknoten*. Sie gelten dann für alle in dieser Gruppe enthaltenen Benutzer.

Hinweis: Pfade zu .zip-Dateien oder komprimierten Ordnern können nicht als Verschlüsselungspfade verwendet werden.

Relative Pfade:

conpal LAN Crypt unterstützt relative Pfadangaben. Eine relative Pfadangabe gibt den Pfad zu einem Verzeichnis bzw. einer Datei unabhängig vom Laufwerk bzw. vom übergeordneten Verzeichnis an. Wird eine relative Pfadangabe gewählt, wird jedes Verzeichnis verschlüsselt, auf das die Pfadangabe passt.

Relative Pfade können auf zwei Arten verwendet werden:

- **Eintrag:** `\my_data\*.*`
  verschlüsselt jedes Verzeichnis `my_data` in den ROOT-Verzeichnissen.

  Beispiel:

  ```
  C:\my_data\*.*
  D:\my_data\*.*
  Z:\my_data\*.*
  ```

- **Eintrag:** `\my_data\*.*`
  verschlüsselt **JEDES** Verzeichnis `my_data`.

  Beispiel:

  ```
  C:\company\my_data\*.*
  Z:\Departments\development\Team1\my_data\*.*
  ```

In beiden Fällen werden alle Dateien des Verzeichnisses `my_data` verschlüsselt.

Sobald eine Verzeichnisangabe mit einem Backslash beginnt, bezieht sich die relative Pfadangabe nur noch auf die Root-Verzeichnisse.

%USERNAME%

conpal LAN Crypt unterstützt die Verwendung der lokalen Umgebungsvariable %USERNAME% in Pfadangaben.
Die Umgebungsvariable %USERNAME% in Pfadangaben wird von conpal LAN Crypt standardmäßig aufgelöst. Sollen auch andere Umgebungsvariablen aufgelöst werden, muss dies in der conpal LAN Crypt Konfiguration eingestellt werden (siehe *Alle Umgebungsvariablen verwenden* auf Seite 138).

Standardverzeichnis

Durch die Unterstützung der von Windows vordefinierten Standardverzeichnisse (zum Beispiel Eigene Dateien, Gemeinsame Dateien, etc.) vereinfacht conpal LAN Crypt die Verschlüsselung dieser benutzerspezifischen Ordner. Die Verwendung der Standardverzeichnisse befreit den Security Officer somit von der Notwendigkeit, systemspezifische Unterschiede in der Client-Konfiguration zu berücksichtigen. conpal LAN Crypt ermittelt aus dem jeweiligen Standardverzeichnis den korrekten benutzerspezifischen Pfad in der richtigen Sprache und verschlüsselt die dort abgelegten Daten.

Weitere Verzeichnisse können in LAN Crypt durch die Eingabe der ID angegeben werden:
Beispiel:
<0x002f>*.*
Das Verzeichnis, das die Verwaltungs-Tools für alle Benutzer des Computers enthält (CSIDL_COMMON_ADMINTOOLS).

Eine Liste aller möglichen IDs finden Sie unter:
http://msdn2.microsoft.com/en-us/library/ms649274.aspx

3.16.2 Schlüssel

Die Schlüssel zur Verschlüsselung der Daten werden vor dem Erzeugen der Verschlüsselungsregel angelegt. Alle für die betreffende Gruppe verfügbaren Schlüssel werden im Dialog zum Erstellen einer Verschlüsselungsregel angezeigt und können aus einer Liste ausgewählt werden.

3.16.3 Reihenfolge der Verschlüsselungsregeln

conpal LAN Crypt sortiert die Verschlüsselungsregeln beim Laden der Richtliniendateien auf dem Client nach der Methode, die Sie im Reiter Regeln auflösen in Zentrale Einstellungen ausgewählt haben:

- Sortiermethode 1
  1. Ignorieren-Regeln
  2. Ausschließen-Regeln
  3. Verschlüsselungsregeln

- Sortiermethode 2
  1. Ignorieren-Regeln
  2. Ausschließen-Regeln
  3. Als absolute Pfade definierte Verschlüsselungsregeln ohne Platzhalter
  4. Als absolute Pfade definierte Verschlüsselungsregeln mit Platzhaltern, ohne Unterordner
  5. Als absolute Pfade definierte Verschlüsselungsregeln mit Platzhaltern, mit Unterordnern
  6. Alle anderen Verschlüsselungsregeln

  Ein absoluter Pfad wird entweder als UNC Pfad (mit doppeltem Backslash zu Beginn) oder als <Laufwerksbuchstabe>:\ angegeben.
  Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre, \\server\share *.* oder c:\encrypt *.*.

- Sortiermethode 3 (Standard)
  Die Sortiermethode 3 unterscheidet nicht zwischen Ignorieren-Regeln, Ausschließen-Regeln und Verschlüsselungsregeln.
  Die Regeln werden in der folgenden Reihenfolge sortiert:
  1. Alle absoluten Pfade ohne Platzhalter
  2. Alle absoluten Pfade mit Platzhaltern, ohne Unterordner

3. Alle absoluten Pfade mit Platzhaltern, mit Unterordnern
4. Alle anderen Regeln

Ein absoluter Pfad wird entweder als UNC Pfad (mit doppeltem Backslash zu Beginn) oder als <Laufwerksbuchstabe>:\ angegeben.
Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre, \\server\share *.* oder c:\encrypt *.*.

Innerhalb der oben angegebenen Abschnitte (zum Beispiel: Sortiermethode 3 - Alle anderen Regeln), richtet sich die Sortierung danach, wie präzise die Pfaddefinition ist.

Hier gilt folgende Reihenfolge:
1. UNC-Pfade
2. Pfade, die mit <Laufwerkbuchstabe> beginnen: Hier wird der Backslash nach dem Laufwerksbuchstaben nicht berücksichtigt.
2. Alle anderen Pfade
Außerdem gilt:
- Pfade mit mehr Backslashes werden vor Pfaden mit weniger Backslashes aufgelistet
- Pfade ohne Platzhalter werden vor Pfaden mit den Platzhaltern *. und *.* aufgelistet

3.16.4 Erzeugen von Verschlüsselungsregeln

1. Klicken Sie mit der rechten Maustaste auf **Verschlüsselungsregeln** unter dem entsprechenden Gruppenknoten und klicken Sie auf **Neue Regel** im Kontextmenü.
   Der Befehl **Neue Regel** steht auch über ein Kontextmenü zur Verfügung, wenn Sie im rechten Konsolenfenster mit der rechten Maustaste klicken. Im rechten Konsolenfenster werden alle erzeugten Verschlüsselungsregeln angezeigt.

2. Geben Sie im Eingabefeld unter *Verschlüsselungspfad* einen relativen oder absoluten Pfad ein. Die Verwendung von Jokern (*) und Wildcards (?) in Dateinamen (nicht im restlichen Pfad) ist erlaubt (z. B. *.doc). Klicken Sie auf **Durchsuchen** ("..."), um einen Pfad auszuwählen.

Relative Pfade und Programme, die ausschließlich Datei- bzw. Pfadangaben in 8.3 Notation beherrschen
Bei der Verwendung von Programmen, die ausschließlich Datei- bzw. Pfadangaben in 8.3 Notation beherrschen und die auf verschlüsselte Dateien mit Dateinamen länger als 8 Zeichen oder auf Dateien in Verzeichnissen mit Namen länger als 8 Zeichen zugreifen, müssen relative Verschlüsselungspfade in 8.3 Notation angegeben werden.
Diese Verschlüsselungsregeln müssen zusätzlich definiert werden. Ansonsten werden 32-Bit-Programme nicht mehr funktionieren.
Das Kommando `dir /x` kann zur Anzeige des korrekten 8.3 Namens von langen Dateinamen verwendet werden.

3. Unter *Verschlüsselungspfad* werden drei Optionen angezeigt:

- Unterverzeichnisse einschließen
- Von Verschlüsselung ausschließen
- Verschlüsselungsregel nicht berücksichtigen

Unterverzeichnisse einschließen

Wenn nicht ausdrücklich angegeben, werden Unterverzeichnisse nicht in die Verschlüsselung einbezogen. Um auch alle Unterverzeichnisse zu verschlüsseln, muss die Option **Unterverzeichnisse einschließen** aktiviert werden.

Beispiel:

Eintrag: `\my_data\*.* Unterverzeichnisse einschließen`

Diese Verschlüsselungsregel verschlüsselt alle Dateien in:

```
C:\company\my_data
C:\company\my_data\project NT
C:\company\my_data\project 2000\demo
```

Von Verschlüsselung ausschließen

Dazu müssen Sie eine Verschlüsselungsregel definieren, die diese Daten von der Verschlüsselung ausnimmt. Dies wird erreicht, indem Sie die Option **Von Verschlüsselung ausschließen** im Dialog *Dateiverschlüsselung* aktivieren. Damit werden die in der Verschlüsselungsregel angegebenen Dateien nicht verschlüsselt. Standardmäßig ist diese Option deaktiviert.

Beispiel:

Alle Dateien mit der Dateierweiterung `.TXT` sollen von der Verschlüsselung ausgenommen werden.

Erste Zeile:

Eintrag `C:\MYDIR\*.TXT`, **Von Verschlüsselung ausschließen**, kein Schlüssel: schließt alle Dateien mit der Erweiterung `.TXT` im Verzeichnis `MYDIR` von der Verschlüsselung aus.

Zweite Zeile:

Eintrag `C:\MYDIR\*.*`, **Von Verschlüsselung ausschließen** deaktiviert, verschlüsselt alle Dateien im Verzeichnis `MYDIR` (außer `.TXT`) mit dem angegebenen Schlüssel.

Verschlüsselungsregel nicht berücksichtigen

conpal LAN Crypt stellt die Option **Verschlüsselungsregel nicht berücksichtigen** zur Verfügung. Dateien, die von solchen Verschlüsselungsregeln betroffen sind, werden von conpal LAN Crypt einfach ignoriert.

Verglichen mit der Option **Von Verschlüsselung ausschließen** heißt das, dass es für diese Dateien auch keine Zugriffskontrolle gibt. Sie können geöffnet (der verschlüsselte Inhalt wird angezeigt), verschoben, gelöscht, usw. werden. Dateien in Verzeichnissen, die von der Verschlüsselung ausgenommen sind, werden trotzdem geprüft, ob sie verschlüsselt sind oder nicht. Auf diese Weise stellt conpal LAN Crypt fest, ob Dateien in solchen Verzeichnissen verschlüsselt sind oder nicht. Der Zugriff auf verschlüsselte Daten wird verwehrt. Dateien in Verzeichnissen, für die die Option **Verschlüsselungsregel nicht berücksichtigen** gewählt wurde, werden einfach ignoriert! Sie werden von conpal LAN Crypt nicht geprüft, der Zugriff auf verschlüsselte Dateien wird nicht verwehrt.

Diese Option wird hauptsächlich für Dateien verwendet, auf die sehr häufig zugegriffen wird und für die keine Veranlassung besteht, sie zu verschlüsseln. Dadurch lässt sich die System-Leistung steigern.

4. Wählen Sie einen Schlüssel aus der Liste aus.

Hinweis: In der Standardansicht werden nur die Platzhalter für <USERKEY> und <GROUPKEY> sowie die von einem SO erzeugten Schlüssel angezeigt. Mit der Schaltfläche Spezifischer Schlüssel können Sie nach spezifischen Schlüsseln suchen und diese anzeigen.

Verschlüsselungspfad und Schlüssel bilden eine conpal LAN Crypt Verschlüsselungsregel. Die Gesamtheit der Verschlüsselungsregeln, die Sie für den Benutzer/die Gruppe definieren, bildet das Verschlüsselungsprofil des Benutzers/der Gruppe.

<USERKEY>

In der Liste der Schlüssel wird auch immer ein Schlüssel <USERKEY> angezeigt. Dabei handelt es sich um einen Platzhalter für einen benutzerspezifischen Schlüssel, der bei der Auflösung der Verschlüsselungsregeln automatisch für jeden einzelnen Benutzer erzeugt wird.

<GROUPKEY>

Analog zu zur Verwendung von <USERKEY> kann durch die Verwendung von <GROUPKEY> ein gruppenspezifischer Schlüssel für alle Mitglieder der Gruppe erzeugt werden.

Hinweis: Stellen Sie bei der Verwendung von <USERKEY> sicher, dass ausschließlich der Benutzer, dem dieser Schlüssel zugewiesen wurde, auf die Daten zugreift. Andere Benutzer können diese Daten nicht entschlüsseln!

Beispiel: Ein Beispiel für die Anwendung von <USERKEY> wäre, wenn alle Benutzer z.B. über ein Netzwerklaufwerk U: verbunden sind, das je ein Verzeichnis für einen Benutzer enthält. Ausschließlich der betreffende Benutzer soll darauf Zugriff haben.
Eine solche Verschlüsselungsregel könnte folgendermaßen aussehen:

```
U:\*.* <USERKEY>
```

Ein weiteres Beispiel für die Anwendung von <USERKEY> wäre die Verschlüsselung von lokalen temporären Verzeichnissen.

Schlüssel ohne Pfad

In der Liste der definierten Verschlüsselungspfade befindet sich auch ein Platzhalter *Schlüssel ohne Pfad*.
Er dient dazu, dem Benutzer einen Schlüssel zur Verfügung zu stellen, mit dem er auf verschlüsselte Daten zugreifen kann, für die kein Verschlüsselungspfad existiert. Dies kann der Fall sein, wenn verschlüsselte Dateien an einen Ort kopiert werden (bei deaktivierter Verschlüsselung), für den keine Verschlüsselungsregel definiert wurde. Der Zugriff auf diese Dateien ist mit dem entsprechenden Schlüssel weiter möglich.
Wird ein Schlüssel ohne Pfad angelegt, wird automatisch ein neuer Platzhalter angelegt, um die Erzeugung weiterer Schlüssel ohne Pfad zu ermöglichen.

5. Markieren Sie die entsprechenden Optionen.
6. Unter *Kommentar* können Sie eine Beschreibung oder Informationen über die angelegte Verschlüsselungsregel eingeben.
7. Klicken Sie auf **OK**.

Die neue Verschlüsselungsregel wird in der conpal Administration angezeigt.

Zum Bearbeiten bestehender Verschlüsselungsregeln markieren Sie diese und klicken Sie auf **Eigenschaften** im *Kontextmenü*. Oder doppelklicken Sie den entsprechenden Eintrag.

3.16.5 Suchen eines spezifischen Schlüssels

Klicken Sie auf die Schaltfläche Spezifischer Schlüssel, um einen Assistenten für die Suche nach spezifischen Schlüsseln zu starten. Schlüssel, die im Assistenten ausgewählt werden, werden zur Schlüsselliste hinzugefügt und können für Verschlüsselungsregeln benutzt werden. Der Schlüssel wird nur vorübergehend hinzugefügt. Wird der Assistent erneut ausgeführt und ein anderer Schlüssel ausgewählt, so wird der zuvor hinzugefügte Schlüssel aus der Liste entfernt.

Auf der ersten Seite können Sie Suchkriterien festlegen. Folgende Kriterien stehen in der Dropdown-Liste zur Auswahl:

- **Einem Benutzer zugewiesener Schlüssel**
  Sucht nach allen spezifischen Schlüsseln, die einem Benutzer zugewiesen sind. Geben Sie den Benutzernamen oder den Anmeldenamen im Eingabefeld (Suchbedingung) ein. Für Platzhaltersuchvorgänge können Sie SQL-Platzhalter verwenden. Wenn Sie zum Beispiel, "Vorstand Benutzer 1%" eingeben, werden alle Schlüssel gefunden, die Benutzern zugewiesen sind, deren Benutzer- oder Anmeldenamen mit "Vorstand Benutzer 1" beginnen.
- **Einer Gruppe zugewiesener Schlüssel**
  Sucht nach allen spezifischen Schlüsseln, die einer Gruppe zugewiesen sind. Geben Sie den Namen der Gruppe ein.
- **Schlüsselname**

Sucht nach allen spezifischen Schlüsseln mit einem bestimmten Namen. Geben Sie den langen oder den kurzen Namen des Schlüssels ein.

- **Schlüssel-GUID**
  Sucht nach allen spezifischen Schlüsseln mit einer bestimmten GUID. Geben Sie die GUID des Schlüssels ein.
- **Zur Zeit nicht zugewiesene Schlüssel**
  Zeigt alle Schlüssel, die derzeit keinem Benutzer und keiner Gruppe zugewiesen sind.

Das Suchergebnis wird auf der zweiten Seite angezeigt.

Wenn ein Schlüssel derzeit zugewiesen ist, wird der Benutzer- oder der Gruppenname unter Zugewiesen an angezeigt. Die Liste enthält nur spezifische Schlüssel, auch wenn nicht-spezifische Schlüssel die Suchkriterien erfüllen würden.

Wählen Sie einen Schlüssel aus und klicken Sie auf **Beenden**, um den Schlüssel zur Liste im Dialog für das Erstellen von Verschlüsselungsregeln hinzuzufügen.

3.17 Verschlüsselungs-Attribute

Identifiziert ein DLP-Produkt Daten, die verschlüsselt werden sollen, so kann es die conpal LAN Crypt Client API verwenden, um die Dateien zu verschlüsseln. In der conpal LAN Crypt Administration können Sie unterschiedliche Verschlüsselungs-Tags definieren, die den zu verwendenden conpal LAN Crypt-Schlüssel angeben.

Die Client-API kann diese vordefinierten Verschlüsselungs-Tags verwenden, um bestimmte Schlüssel auf unterschiedliche Inhalte anzuwenden wie z.B. das Verschlüsselungs-Tag <CONFIDENTIAL>, um alle Dateien zu verschlüsseln, die als vertraulich von Ihrem DLP-Produkt kategorisiert sind.

Ein Beispiel für die Anwendung einer Referenz auf einen Schlüssel wäre:

```
SGFEAPI encrypt /Tag:CONFIDENTIAL c:\documents\encrypt.doc
```

Damit würde die Datei encrypt.doc im Verzeichnis \Documents mit dem Schlüssel aus dem Verschlüsselungs-Attribut <CONFIDENTIAL> verschlüsselt.

Details dazu finden Sie in der Client-API-Dokumentation im Verzeichnis \DOC Ihres entpackten Installationspakets.

Um ein Verschlüsselungs-Attribut zu erzeugen

1. klicken Sie mit der rechten Maustaste auf **Verschlüsselungsregeln** unter dem entsprechenden Gruppenknoten und klicken Sie auf **Neue Regel** im Kontextmenü.
   Der Befehl **Neue Regel** steht auch über ein Kontextmenü zur Verfügung, wenn Sie im rechten Konsolenfenster mit der rechten Maustaste klicken. Im rechten Konsolenfenster werden alle erzeugten Verschlüsselungsregeln angezeigt.

2. Geben Sie im Eingabefeld unter *Verschlüsselungspfad* einen relativen oder absoluten Pfad ein.

3. Wählen Sie einen Schlüssel aus.

Hinweis: In der Standardansicht werden nur die Platzhalter für <USERKEY> und <GROUPKEY> sowie die von einem SO erzeugten Schlüssel angezeigt. Mit der Schaltfläche Spezifischer Schlüssel können Sie nach spezifischen Schlüsseln suchen und diese anzeigen.

<USERKEY>

In der Liste der Schlüssel wird auch immer ein Schlüssel <USERKEY> angezeigt. Dabei handelt es sich um einen Platzhalter für einen benutzerspezifischen Schlüssel, der bei der Auflösung der Verschlüsselungsregeln automatisch für jeden einzelnen Benutzer erzeugt wird.

<GROUPKEY>

Analog zu zur Verwendung von <USERKEY> kann durch die Verwendung von <GROUPKEY> ein gruppenspezifischer Schlüssel für alle Mitglieder der Gruppe erzeugt werden.

Hinweis: Stellen Sie bei der Verwendung von <USERKEY> sicher, dass ausschließlich der Benutzer, dem dieser Schlüssel zugewiesen wurde, auf die Daten zugreift. Andere Benutzer können diese Daten nicht entschlüsseln!

4. Unter Kommentar können Sie eine Beschreibung oder Informationen über die angelegte Verschlüsselungsregel eingeben.

5. Klicken Sie auf **OK**.

Das neue Verschlüsselungsattribut wird in der conpal Administration angezeigt.

Zum Bearbeiten bestehender Verschlüsselungsattribute markieren Sie diese und klicken Sie auf **Eigenschaften** im Kontextmenü. Oder doppelklicken Sie den entsprechenden Eintrag.

3.18 Zuordnung der Zertifikate

Jedes Profil ist mit dem öffentlichen Schlüssel seines Besitzers geschützt. Dieser öffentliche Schlüssel muss dem Benutzer in der conpal LAN Crypt Administration über sein Zertifikat zugewiesen werden.

Hinweis: Dieser Schritt muss nicht notwendigerweise in der beschriebenen Reihenfolge ausgeführt werden. Er kann auch bereits zu einem früheren Zeitpunkt erfolgen.

Es ist empfehlenswert, dass die Zertifikate bereits im Zertifikatsspeicher bzw. in einem Verzeichnis zur Verfügung stehen (z. B. LDAP), wenn Sie mit der Zuweisung beginnen. Zum Importieren der Zertifikate in den entsprechenden Zertifikatsspeicher können die Windows Standardmechanismen verwendet werden.

Zur automatischen Zuordnung der Zertifikate stellt conpal LAN Crypt einen Zertifikatszuordnungsassistenten zur Verfügung.

Hinweis: Wenn der Benutzer, der die Zertifikatszuordnung durchführt, im Dateisystem kein Recht hat, die Passwortprotokolldatei zu ändern, können keine conpal LAN Crypt-Zertifikate erzeugt werden.

3.18.1 Zertifikat einem Benutzer zuordnen

Zum Zuweisen eines Zertifikats

1. Markieren Sie **Mitglieder und Zertifikate für Gruppe** unter dem jeweiligen Gruppenknoten. Im rechten Konsolenfeld werden alle Benutzer aufgelistet.

2. Klicken Sie doppelt auf einen Benutzer oder klicken Sie mit der rechten Maustaste auf den Benutzer und anschließend auf **Eigenschaften** im Kontextmenü.
   Der Dialog *Eigenschaften von ...* wird angezeigt.

3. Der Dialog bietet folgende Möglichkeiten, dem Benutzer ein oder mehrere Zertifikate zuzuweisen.

- **Neu**
  Klicken auf **Neu** lässt conpal LAN Crypt ein neues Zertifikat für den Benutzer erzeugen. Sollten keine Zertifikate zur Verfügung stehen, kann die Administration von conpal LAN Crypt optional selbst Zertifikate erzeugen. Diese Zertifikate sollten ausschließlich von conpal LAN Crypt verwendet werden!
  Das erzeugte Zertifikat wird als PKCS#12 Datei im vordefinierten Verzeichnis gespeichert.

Hinweis: Die so erzeugten Zertifikate müssen anschließend an die entsprechenden Benutzer verteilt werden. Ansonsten haben die Benutzer keinen Zugriff auf ihre Verschlüsselungsprofile.

- **Importieren**
  Sollte das gewünschte Zertifikat noch nicht im Zertifikatsspeicher vorhanden sein, wird es in der Liste der verfügbaren Zertifikate nicht angezeigt.
  Klicken Sie in diesem Fall auf **Importieren.**Es wird ein Dialog geöffnet, in dem Sie das gewünschte Zertifikat auswählen können. Klicken Sie anschließend auf **OK** und das Zertifikat wird dem Benutzer zugeordnet.
  Das importierte Zertifikat wird automatisch in den Zertifikatsspeicher *Andere Personen* importiert.

Hinweis: Es können nur Zertifikatsdateien im Format .cer, .crt und .der importiert werden. Nicht jedoch .p12 bzw. .pfx Dateien.

- **Hinzufügen**

Öffnet einen Dialog, in dem ein bestehendes Zertifikat dem Benutzer zugeordnet werden kann. In diesem Dialog werden alle im Zertifikatsspeicher vorhandenen Zertifikate aufgelistet.
Zertifikate über eine LDAP-Quelle zuordnen
conpal LAN Crypt bietet zusätzlich die Möglichkeit, Zertifikate aus einer LDAP Quelle zuzuweisen.
Markieren Sie dafür **LDAP** in der Drop-Down-Liste des Dialogs Wählen Sie ein Zertifikat.

Es wird jetzt ein Eingabefeld angezeigt, in das Sie die URL der LDAP Quelle eingeben können. Nach Klicken auf **Aktualisieren** wird der Inhalt der LDAP Quelle angezeigt.
Begriffe in eckigen Klammern (z. B. [Sub_OU1] bezeichnen die OUs in der LDAP Quelle. Ein Doppelklick auf eine OU zeigt die darin enthaltenen Zertifikate an.
Ein Doppelklick auf [..] bringt Sie in der Organisationsstruktur eine Ebene höher.
Wählen Sie ein Zertifikat aus und klicken Sie auf **OK**. Das Zertifikat wird dem Security Officer zugewiesen.

Hinweis: Wenn auf den LDAP-Server nicht über eine Anonymous-Anmeldung zugegriffen werden kann, müssen die Anmeldedaten als Distinguished Name (Beispiel: CN= John Doe,O=Marketing) im Register **Server** in den **Zentralen Einstellungen**.

Hinweis: Wenn das Zertifikat aus einem LDAP Verzeichnis zugewiesen wurde, muss der dazugehörige private Schlüssel auf der Arbeitsstation des Benutzers vorhanden sein.

4. Wählen Sie durch eine der Möglichkeiten ein Zertifikat aus und klicken Sie auf **OK**.
   Das Zertifikat wird im Konsolenfenster rechts neben dem Benutzer angezeigt. Im Konsolenfenster werden Informationen über das verwendete Zertifikat (Gültigkeitsdauer, Seriennummer, Antragsteller, Aussteller) angezeigt.

Hinweis: Das Zertifikats-Snap-In steht unter jedem Benutzer-/Gruppen-Knoten zur Verfügung. Hier werden nur die Benutzer angezeigt, die Mitglied der entsprechenden Gruppe sind.

3.18.2 SafeGuard LAN Crypt Zertifikate erzeugen und zuordnen

Dieser Assistent erzeugt Zertifikate für **alle** Benutzer, denen noch kein Zertifikat zugeordnet wurde und ordnet diese den Benutzern automatisch zu.

Zum Öffnen dieses Assistenten klicken Sie auf **Zertifikate erzeugen** im Kontextmenü jedes Knotens *Mitglieder und Zertifikate für Gruppe* oder klicken Sie auf das entsprechende Symbol in der Symbolleiste.

Im angezeigten Dialog können Sie auswählen, ob Sie die Zertifikate nur **in dieser Gruppe** oder **in dieser Gruppe und allen Untergruppen** bzw. **nur für ausgewählte Benutzer** erzeugen und zuweisen wollen.

Nur für ausgewählte Benutzer

Diese Option wird nur angezeigt, wenn zuvor ein oder mehrere Benutzer ausgewählt wurden. Die einzelnen Benutzer einer Gruppe werden im rechten Konsolenfenster angezeigt, wenn mit der linken Maustaste auf *Mitglieder und Zertifikate für Gruppe* unter dem entsprechenden Gruppenknoten geklickt wird. Das Markieren der Benutzer funktioniert analog zum Markieren von Dateien im Windows Explorer (Auswahl der Benutzer mit der linken Maustaste bei gedrückter Umschalt-, oder STRG-Taste bzw. durch Ziehen mit der Maus bei gedrückter linker Maustaste und gedrückter Umschalt-Taste).

Die Erzeugung und Zuordnung der Zertifikate erfolgt vollautomatisch. Klicken Sie auf **Fertig stellen,** um den Assistenten zu schließen.

Hinweis: Die hier erzeugten Schlüsseldateien (.p12) und der öffentliche Teil des Security Officer Zertifikats werden in dem in den Zentralen Einstellungen angegebenen Verzeichnis gespeichert und müssen den Benutzern zur Verfügung gestellt werden.
Dazu kann in der conpal LAN Crypt Konfiguration eingestellt werden, in welchem Verzeichnis conpal LAN Crypt nach einer .p12-Datei für den Benutzer sucht, falls der Private Schlüssel für die Richtliniendatei nicht vorhanden ist.
Gleiches gilt für den öffentlichen Teil des Security Officer Zertifikats.
Damit die Benutzer-Schlüsseldateien automatisch erkannt werden, müssen die Dateinamen dem Anmeldenamen des Benutzers entsprechen („Anmeldename*.p12“).
Wird eine entsprechende Datei gefunden, erscheint ein PIN Dialog. Diese PIN (enthalten in der Passwortprotokolldatei) muss dem Benutzer über einen PIN-Brief mitgeteilt werden. Das Zertifikat und die dazugehörigen Schlüssel werden nach Eingabe der PIN automatisch importiert.

Wird eine entsprechende .cer-Datei, die den öffentlichen Teil des Security Officer Zertifikats enthält, gefunden, wird diese automatisch importiert.
Als Alternative dazu können die Schlüsseldateien der Benutzer und der öffentliche Teil des Administratorzertifikats auch manuell verteilt werden. Stellen Sie in diesem Fall sicher, dass beide von den Clients importiert werden.

3.18.3 Assistent zur Zertifikatszuordnung

conpal LAN Crypt stellt einen Assistenten zur Zertifikatszuordnung zur Verfügung, der die Zuordnung der Zertifikate zu den Benutzern weitgehend automatisiert. Der Assistent wird über **Assistent zur Zertifikatszuordnung** im Kontextmenü von *Mitglieder und Zertifikate für Gruppe* gestartet.

Im ersten Dialog des Assistenten können Sie auswählen, ob Sie die Zertifikate nur **in diese Gruppe** oder **in dieser Gruppe und allen Untergruppen** bzw. **nur für ausgewählte Benutzer** zuordnen wollen.

Nur für ausgewählte Benutzer

Diese Option wird nur angezeigt, wenn zuvor ein oder mehrere Benutzer ausgewählt wurden. Die einzelnen Benutzer einer Gruppe werden im rechten Konsolenfenster angezeigt, wenn mit der linken Maustaste auf *Mitglieder und Zertifikate für Gruppe* unter dem entsprechenden Gruppenknoten geklickt wird. Das Markieren der Benutzer funktioniert analog zum Markieren von Dateien im Windows Explorer (Auswahl der Benutzer mit der linken Maustaste bei gedrückter Umschalt-, oder STRG-Taste bzw. durch Ziehen mit der Maus bei gedrückter linker Maustaste und gedrückter Umschalt-Taste).

Der Assistent unterstützt die Zuordnung der Zertifikate aus folgenden Quellen:

- Zertifikate aus dem **Active Directory**
- Zertifikate aus dem **LDAP-Verzeichnis**
- Zertifikate aus einem **Dateisystemverzeichnis**
- Zertifikate aus dem **Zertifikatspeicher**

3.18.3.1 Zertifikate aus dem Active Directory zuordnen

Wenn Sie die Option Zertifikate aus dem **Active Directory** zuordnen gewählt haben, müssen Sie in Schritt 2 die DNS-Adresse des Active Directory Servers angeben. In der Regel ist dies der Domain Controller.

Durch Klicken auf **Standardwert** wird die Adresse des Domain Controllers, an den Sie zurzeit angemeldet sind, eingetragen.

Starten Sie den Assistenten durch Klicken auf **Weiter**. Der Import und die Zuordnung der Zertifikate erfolgt vollautomatisch. Eine Meldung bestätigt die erfolgreiche Zuordnung der Zertifikate. Klicken Sie auf **Fertig stellen,** um den Assistenten zu schließen.

3.18.3.2 Zertifikate aus einem LDAP Verzeichnis zuordnen

Wenn Sie die Option Zertifikate aus einem **LDAP Verzeichnis** zuordnen gewählt haben, müssen Sie in Schritt 2 Angaben zum LDAP Verzeichnis, aus dem die Zertifikate importiert werden sollen, machen.

Tragen Sie unter *Adresse*, den vollständigen Computernamen des LDAP Servers ein (zum Beispiel: Server.MeineDomäne.com) und geben Sie den entsprechenden Port an. Der übliche Port für LDAP Server ist standardmäßig eingestellt.

Geben Sie unter DN ein, ab welchem Knoten in der LDAP Struktur das Verzeichnis durchsucht werden soll. Geben Sie den Knoten im LDAP Verzeichnis mit seinem Distinguished Name an. Der Rechnername (dc=rechnername ...) .. darf hier nicht noch einmal eingetragen werden.

Hinweis:
Microsoft AD:
Das Eingabefeld darf nicht leer bleiben. Hier ist zumindest die Angabe der Domäne und des Landes erforderlich.
Beispiel 1: DC=mydomain,DC=De
Beispiel 2: OU=marketing,DC=mydomain,DC=DE

Durch Klicken auf **Standardwert** wird die Adresse des Domain Controllers, an den Sie zurzeit angemeldet sind, eingetragen.

Zur Zuordnung der Zertifikate werden Übereinstimmungen zwischen Eigenschaften der LDAP Benutzer und der conpal LAN Crypt Benutzer verwendet.

Folgende Eigenschaften der LDAP Benutzer können verwendet werden:

- E-Mail-Adresse
- Common Name
- Vollständiger Name
- NT 4.0 Kontoname
- User Principal Name
- Benutzerdefiniertes Attribut

Diese Eigenschaften können als übereinstimmend mit folgenden conpal LAN Crypt Benutzereigenschaften definiert werden:

- E-Mail-Adresse
- Benutzername
- Logonname
- Kommentar

Wählen Sie aus, welche LDAP Benutzereigenschaft der des conpal LAN Crypt Benutzers entsprechen soll.
Wird die Übereinstimmung festgestellt, wird das Zertifikat des LDAP Benutzers importiert und automatisch dem entsprechenden conpal LAN Crypt Benutzer zugeordnet.

Hinweis: Zur Vermeidung von Inkonsistenzen wird die Verwendung der E-Mail-Adresse als Zuordnungskriterium empfohlen, da diese immer eindeutig sein sollte.

Starten Sie den Assistenten durch Klicken auf **Weiter**. Der Import und die Zuordnung der Zertifikate erfolgt vollautomatisch. Eine Meldung bestätigt die erfolgreiche Zuordnung der Zertifikate. Klicken Sie auf **Fertig stellen,** um den Assistenten zu schließen.

3.18.3.3 Zertifikate aus einem Verzeichnis zuordnen

Wenn Sie die Option **Zertifikate aus einem Verzeichnis zuordnen** gewählt haben, müssen Sie in Schritt 2 des Assistenten angeben, in welchem Verzeichnis sich die Zertifikate befinden.

Nach der Angabe des Verzeichnisses können Sie im folgenden Dialog festlegen, nach welcher Methode conpal LAN Crypt die Zertifikate den Benutzern zuordnen soll.

- **Benutzername entspricht Dateiname**
  Wählen Sie diese Option, wenn die Dateinamen der Zertifikatsdateien identisch mit den Benutzernamen sind.
  Allen Benutzern, denen ein Dateiname entspricht, wird das entsprechende Zertifikat zugeordnet.

- **Benutzername ist im DN enthalten**
  Ist der Benutzername im Distinguished Name des Zertifikats enthalten, so ist conpal LAN Crypt in der Lage, diesen zu finden und das Zertifikat dem entsprechenden Benutzer zuzuordnen. Dazu ist ein Suchmuster erforderlich, durch das conpal LAN Crypt den Benutzernamen im DN identifizieren kann.
  Das Suchmuster kann in den Eingabefeldern unter der Option **Benutzername ist im DN enthalten** festgelegt werden. Es wird nach dem Benutzernamen, der sich im DN zwischen den beiden angegebenen Zeichenfolgen befindet, gesucht.
  Beispiel:
  Der Benutzername steht im DN des Zertifikats immer unter CN=.
  (z.B. CN=HansMeier,OU=conpal LAN Crypt)
  Durch Eingabe von `CN=` im ersten und `,OU=conpal` im zweiten Eingabefeld kann conpal LAN Crypt den Benutzernamen, der sich zwischen den beiden Zeichenfolgen befindet, eindeutig identifizieren (im Beispiel HansMeier). Das Zertifikat wird dem Benutzer automatisch zugeordnet.

- **Zuordnung aus Datei entnehmen**
  Die gewünschte Zuordnung kann auch einer Datei entnommen werden.
  Zum Beispiel wird der öffentliche Teil der mit der conpal Smartcard Administration erzeugten Zertifikate in einer Datei in einem angegebenen Verzeichnis gespeichert. Zusammen mit diesen Dateien wird von der conpal Smartcard Administration eine Datei erzeugt, die die Information enthält, welchem Benutzer welches Zertifikat zugeordnet ist. Auch andere PKIs sind im Stande, derartige Listen zu erzeugen. Natürlich kann diese Liste auch selbst generiert werden.

  Sie muss folgendem Format entsprechen:

  ```
  Benutzername;Dateiname
  ```

  Beispiel:

  ```
  Gast;Gastcer.cer
  ```

```
HansMeier;Meier.cer
....
```

Die Zertifikate werden entsprechend der Zuordnung in dieser Datei zugeordnet.

- Nach dem Klicken auf **Weiter** müssen Sie noch festlegen, wie conpal LAN Crypt bestehende Zuordnungen behandeln soll.

3.18.3.4 Zertifikate aus Zertifikatsspeicher zuordnen

Wenn Sie die Option **Zertifikate aus Zertifikatsspeicher zuordnen** gewählt haben, werden Sie im zweiten Schritt des Assistenten gefragt, ob eine Liste aller verfügbaren Zertifikate erzeugt und importiert werden soll bzw. ob eine vorhandene Liste importiert werden soll. Anhand dieser Liste nimmt conpal LAN Crypt die Zuordnung der Zertifikate vor.

Die Option Importieren einer vorhandenen Liste kann z. B. verwendet werden, wenn die Zuordnung bereits einmal gestartet wurde, der Vorgang aber nach dem Erzeugen der Liste abgebrochen wurde. Die erstellte Datei kann dann wieder verwendet werden.

Wird die Option **Erzeuge und importiere eine Liste aller verfügbaren Zertifikate** gewählt, wird der folgende Dialog angezeigt.

Wählen Sie einen Namen für die Ausgabedatei der Liste aus.

conpal LAN Crypt erzeugt eine Liste aller im Zertifikatsspeicher verfügbaren Zertifikate. Diese Liste enthält Platzhalter für die Benutzernamen, denen das Zertifikat zugeordnet werden soll.

Beispiel:

*****; My; OU=conpal LAN Crypt Certificate, CN=LAN Crypt Admin; 0010-ae671e47...
*****; Root; CN=Microsoft Root Certificate Authority, DC=microsoft, DC=com; 0010-4cad...

Die Platzhalter (*****) können durch den Benutzernamen ersetzt werden.

Ist der Benutzername im Zertifikat enthalten, kann folgende Option verwendet werden:

- **Versuche Benutzer zu erkennen**

  Ist der Benutzername im Distinguished Name des Zertifikats enthalten, so ist conpal LAN Crypt in der Lage, diesen zu finden und das Zertifikat dem entsprechenden Benutzer zuzuordnen. Dazu ist ein Suchmuster erforderlich, durch das conpal LAN Crypt den Benutzernamen im DN identifizieren kann.
  Das Suchmuster kann in den Eingabefeldern unter dieser Option festgelegt werden. Es wird nach dem Benutzernamen, der sich im DN zwischen den beiden angegebenen Zeichenfolgen befindet, gesucht.

  Beispiel:

  Der Benutzername steht im DN des Zertifikats immer unter CN=.

(z.B. CN=HansMeier,OU=conpal LAN Crypt)
Durch Eingabe von `CN=` im ersten und `,OU=conpal` im zweiten Eingabefeld kann conpal LAN Crypt den Benutzernamen, der sich zwischen den beiden Zeichenfolgen befindet, eindeutig identifizieren (im Beispiel HansMeier). Der Platzhalter wird durch den Benutzernamen ersetzt und das Zertifikat wird dem Benutzer automatisch zugeordnet.

- **Ausgabedatei nach Fertigstellung mit Editor öffnen**
  Wird diese Option aktiviert, wird die Liste der Zertifikate nach dem Erzeugen geöffnet. Sie können die Liste nun bearbeiten. Die Platzhalter können bei den entsprechenden Zertifikaten durch die Benutzernamen ersetzt werden. Nach dem Abspeichern der Liste wird die editierte Version für die Zuordnung verwendet.

Nach dem Klicken auf **Weiter** müssen Sie noch festlegen, wie conpal LAN Crypt bestehende Zuordnungen behandeln soll.

3.19 Bereitstellen der Verschlüsselungsregeln - Richtliniendateien erzeugen

Alle Profile, die erzeugt wurden (oder wenn Änderungen in den Profilen vorgenommen wurden), werden in der conpal LAN Crypt internen Administrationsdatenbank gespeichert. Sie haben dann noch keine Auswirkungen auf die einzelnen Benutzer.

Zum Auflösen der einzelnen Profile und zum Erzeugen der Richtliniendateien muss der conpal LAN Crypt Profile Resolver von einem conpal LAN Crypt Security Officer gestartet werden. Er erzeugt Richtliniendateien für jeden Benutzer, entsprechend den Einstellungen, die in der Administration vorgenommen wurden. Wenn sich der Benutzer das nächste Mal anmeldet, wird das neue Verschlüsselungsprofil geladen.

Hinweis: Bitte beachten Sie, dass nach Änderungen in der conpal LAN Crypt Administration (neue Schlüssel, neue Regeln, usw.) immer neue Richtliniendateien erzeugt werden müssen. Die Änderungen für die Benutzer werden erst aktiv, wenn diese die neuen Richtliniendateien geladen haben.

3.19.1 Erzeugen (Bereitstellen) von Richtliniendateien für eine gesamte Gruppe oder ausgewählte Benutzer

Richtliniendateien werden mit dem Assistenten zum Profile erzeugen erzeugt. Der Assistent startet, wenn mehr als ein Benutzer ausgewählt wird und das Erzeugen des Profils von der Symbolleiste oder dem Kontextmenü von Benutzern aus gestartet wird.

Wird für einen einzelnen Benutzer Profil bereitstellen/löschen aus dem Kontextmenü ausgewählt, so wird das Profil unmittelbar erzeugt. Eine Meldung informiert den Security Officer über das Ergebnis.

Die Ausgangspunkte für den Assistenten richten sich danach, aus welcher Ansicht der Assistent gestartet wird:

- **Auswahl des Geltungsbereichs** (Standard)
- **Zusammenstellung der Benutzer und Prüfung der Zertifikate:**
  Wenn keine Auswahl des Geltungsbereichs möglich ist, zum Beispiel, wenn die Profilerzeugung für ausgewählte Benutzer im Knoten Ausgewählte Benutzer und Zertifikate gestartet wird.
- **Erzeugen des Profils:**
  Wenn Profil löschen für mehrere Benutzer gestartet wird. Diese Aktion kann nicht für eine gesamte Gruppe gestartet werden. Zertifikatsprüfungen sind hier nicht notwendig.

Auf der ersten Seite des Assistenten kann der Geltungsbereich für die Profilerzeugung ausgewählt werden. Für folgende Geltungsbereiche können Profile erzeugt werden:

- Nur Benutzer in dieser Gruppe
- Benutzer in dieser Gruppe und alle Untergruppen
- Nur ausgewählte Benutzer

Wählen Sie die Option Nur Richtliniendateien für geänderte Gruppen bereitstellen, um die Erzeugung von Richtliniendateien auf Benutzer zu beschränken, für die aufgrund von vorgenommenen Änderungen neue Richtliniendateien erforderlich sind. Dadurch lässt sich die Erzeugung von Richtliniendateien in großen Organisationen beschleunigen.

Auf der zweiten Seite des Assistenten wird der Fortschritt angezeigt, während alle Benutzerdaten gesammelt und Benutzerzertifikate geprüft werden. Wenn alle Benutzer verarbeitet sind, wird die nächste Seite angezeigt.

Auf der dritten Seite des Assistenten werden Zertifikatswarnungen angezeigt. Auf dieser Seite werden Benutzer angezeigt, denen kein gültiges Zertifikat zugeordnet ist, oder deren Zertifikat bald abläuft. Die folgenden Zertifikatswarnungen und -fehler werden angezeigt:

- Das Zertifikat des Benutzers läuft bald ab (Warnung).
- Alle zugeordneten Zertifikate des Benutzers sind abgelaufen (Fehler).
- Einem Benutzer ist kein Zertifikat zugeordnet (Fehler).
- Dem Benutzer ist kein Zertifikat zugeordnet und er ist als zu überspringen markiert (Warnung).

Wird ein Fehler angezeigt, so muss auf dieser Seite mindestens eine der folgenden Optionen ausgewählt werden, damit die Profilerzeugung fortgesetzt werden kann:

- **Für die Benutzer in der Liste nicht mehr warnen**
  Es werden alle Benutzer übersprungen, deren Zertifikate abgelaufen sind oder denen keine Zertifkate zugeordnet sind. Diese Benutzer werden in der Profilerzeugung so lange

übersprungen, bis sie neue Zertifikate erhalten.

- **Benutzer ohne zugeordnetes Zertifikat immer überspringen**
  Es werden alle Benutzer ohne gültiges Zertifikat ignoriert. Dies ist eine globale Einstellung, die auch in Zentrale Einstellungen konfiguriert werden kann.

Klicken Sie auf **Zurück**, um zur Seite für die Auswahl des Geltungsbereichs zurückzukehren.

Die vierte Seite des Assistenten zeigt eine Fortschrittsanzeige während alle Profile erzeugt werden. Der Assistent kann zwar abgebrochen werden, dadurch wird jedoch nur die Profilerzeugung gestoppt. Bereits erzeugte Richtliniendateien werden nicht gelöscht oder zurückgesetzt.

Auf der fünften und letzten Seite des Assistenten wird die Anzahl an erzeugten Profilen angezeigt. Wenn ein Fehler aufgetreten ist, durch den die Profilerzeugung gestoppt werden musste, wird eine Fehlermeldung angezeigt.

Hinweis: Wenn Sie auf den Reitern Antivirus-Software, Regeln auflösen oder Andere Einstellungen in Zentrale Einstellungen Änderungen vornehmen, ändern sich jeweils auch die Richtliniendateien für alle Benutzer. Nach einer Änderung dieser Art müssen neue Richtliniendateien für alle Benutzer erzeugt werden.

3.19.2 Selektives Bereitstellen über Zertifikats-Snap-In

Das Zertifikats-Snap-In kann ebenfalls zum Bereitstellen der Richtliniendateien verwendet werden. Es steht unter dem Knoten *Mitglieder und* Zertifikate *für Gruppen* und unter jedem Gruppenknoten zur Verfügung.

Das Erzeugen der Richtliniendateien über das Zertifikats-Snap-In bietet folgende Zusatzfunktionen:

- Benutzer, denen ein Zertifikat zugewiesen werden soll, können ausgewählt werden. Es ist nicht notwendig für alle Benutzer neue Richtliniendateien zu erzeugen.
  Mehrere Benutzer können wie im Windows Explorer (Maus + SHIFT bzw. STRG) ausgewählt werden.
- Der Security Officer sieht sofort, welche Benutzer in der Gruppe vorhanden sind.
- Die Zertifikatssymbole neben den Benutzernamen zeigen den Status der Zertifikate an:
  - **rot bedeutet:**
    Das Zertifikat ist abgelaufen.
  - **gelb bedeutet:**
    Das Zertifikat läuft innerhalb der konfigurierten Warnfrist ab.
  - **grün bedeutet:**
    Alles OK.
  - graues Symbol bedeutet:

Entweder wurde dem Benutzer kein Zertifikat zugeordnet oder er wurde bei der Zuordnung der Zertifikate übersprungen.

Zum Bereitstellen der Richtliniendateien markieren Sie die gewünschten Benutzer und klicken anschließend auf das blaue Zahnradsymbol in der Symbolleiste oder auf **Profile bereitstellen** im Kontextmenü des markierten Benutzers.

3.19.3 Profile löschen

Im Zertifikats-Snap-In können die Profile eines oder mehrerer Benutzer gelöscht werden. Beim Löschen von Profilen wird eine leere Richtliniendatei erstellt. Der Benutzer muss sich einmal an diese Datei anmelden, damit die Einstellungen in der auf seinem Rechner zwischengespeicherten Richtliniendatei überschrieben werden. Danach hat er auf verschlüsselte Daten keinen Zugriff mehr.

Zum Löschen eines Profils markieren Sie den Benutzer im Zertifikats-Snap-In und klicken auf das Symbol **Profil für den gewählten Benutzer löschen** oder auf **Profil löschen** im Kontextmenü.

Sie können auch mehrere Benutzer auswählen (Markieren bei gedrückter Umschalt-Taste) und deren Profil durch Klicken auf das Symbol löschen.

Hinweis: In den Einstellungen in conpal LAN Crypt Zentrale Einstellungen legen Sie fest, wie Profile gelöscht werden. Der Vorgang des Löschens eines Profils ähnelt dem Vorgang des Erzeugens von Profilen. Wenn hier der Novell-Name verwendet werden soll (zwei Richtliniendateien werden erstellt), dann werden beide Profile gelöscht, sofern diese Einstellung nicht geändert wird. Wird die Einstellung zur Laufzeit geändert, kann es vorkommen, dass obwohl zwei Richtliniendateien erstellt wurden, nur die Datei mit dem Windows-Benutzernamen gelöscht wird. Dies geschieht, weil die Einstellung "Zusätzliche Richtliniendateien basierend auf dem Novell-Namen erzeugen" deaktiviert wurde, und daher nur die Richtliniendatei mit dem Windows-Benutzernamen gelöscht wird. Die Novell-Richtliniendatei bleibt bestehen und könnte theoretisch zur Anmeldung verwendet werden. Das System verhält sich je nach für Richtliniendateien ausgewähltem Dateiformat (.po/.pol.biz/ .xml.bz2) ähnlich. In diesem Fall werden pro Benutzer bis zu vier Richtliniendateien erzeugt. Bitte bedenken Sie diesen Sachverhalt und stimmen Sie die Vorgehensweise, wenn nötig, mit dem Systemadministrator ab.

3.20 Datenbankprotokollierung

Die Protokollierung von conpal LAN Crypt protokolliert ausgewählte Ereignisse in der conpal LAN Crypt Datenbank. Sie bietet die Möglichkeit, die zu protokollierenden Ereignisse festzulegen, diese zu archivieren und zu prüfen.

Über die globalen Rechte **Protokoll lesen** und **Protokollierung verwalten** kann der Zugriff von Security Officers auf die Protokollierung kontrolliert werden. Diese Rechte kann der Master Security Officer dem Security Officer geben.

Protokoll lesen	Für den SO sind die Einstellungen für die Protokollierung und die Einträge in das Protokoll sichtbar.
Protokollierung verwalten	Der SO darf die Einstellungen für die Protokollierung ändern. Er ist berechtigt, die Einträge zu archivieren, zu löschen und zu prüfen.

Grundeinstellungen zur Protokollierung werden in der conpal LAN Crypt Administration über den Knoten *Protokollierung* unter dem Knoten *Zentrale Einstellungen* vorgenommen. Dieser Knoten ist nur sichtbar, wenn der Security Officer zumindest das Recht **Protokoll lesen** besitzt.

Die Basiseinstellungen können nur von einem Master Security Officer vorgenommen werden. Sie können darüber hinaus durch eine zusätzliche Autorisierung abgesichert werden (Operation **Protokollierung verwalten**; erfordert die globalen Rechte **Protokoll lesen** und **Protokoll verwalten**).

Zu den Grundeinstellungen zählt auch die Auswahl der Ereignisse, die protokolliert werden sollen. Diese Auswahl kann ebenfalls nur von einem Master Security Officer vorgenommen werden.

Hinweis: Ereignisse, die vor der Anmeldung eines SOs eintreten, können nicht direkt in der Datenbank protokolliert werden. Sie werden zwischengespeichert und bei der nächsten erfolgreichen Anmeldung in die Datenbank übertragen.

3.20.1 Einstellungen

Durch Klicken auf *Eigenschaften* im Kontextmenü des Knotens *Protokollierung* wird der Dialog zum Festlegen der Grundeinstellungen geöffnet.

Seite Einstellungen

Auf dieser Seite wird das Mindestalter von Protokolleinträgen, bevor sie gelöscht werden können, angegeben.

Mit dieser Einstellung soll sichergestellt werden, dass beim Einsatz von verteilten Datenbanken die Einträge sicher zur Zentrale repliziert werden, bevor sie in den einzelnen Niederlassungen gelöscht werden können.

Seite Status

Auf der Seite *Status* werden Informationen über den Stand der Protokollierung angezeigt.

3.20.2 Protokollierte Ereignisse

Wird der Knoten *Protokollierung* ausgewählt, werden im rechten Konsolenfenster die Ereignisse angezeigt, die für eine Protokollierung zur Verfügung stehen. Hier können Sie auswählen, welche Aktionen protokolliert werden.

Hinweis: Die Auswahl, welche Aktionen protokolliert werden sollen, kann nur von einem Master Security Officer vorgenommen werden.

Durch Klicken auf die Spaltenüberschrift *Stufe* können Sie die Ereignisse nach Kategorien sortieren (Notfall, Alarm, Fehler, Warnung, Notiz, Information).

Einträge werden durch einen Doppelklick oder durch Klicken auf das entsprechende Symbol in der Symbolleiste zur Protokollierung ausgewählt.

Aktiviert die Protokollierung für ausgewählte Ereignisse.

Deaktiviert die Protokollierung für ausgewählte Ereignisse.

Durch Klicken bei gedrückter Umschalt-Taste können Sie mehrere Aktionen gleichzeitig auswählen.

Nachdem die Einträge ausgewählt wurden, müssen Sie die Einstellungen durch Klicken auf das Disketten-Symbol speichern. Außerdem werden Sie beim Verlassen dieser Ansicht gefragt, ob die geänderten Einträge gespeichert werden sollen.

3.20.3 Einträge ansehen und exportieren

Hinweis: Zum Ansehen und Exportieren der protokollierten Einträge benötigt ein Security Officer das Recht **Protokoll lesen**.

Ein Security Officer, der das globale Recht Protokoll lesen besitzt, kann sich die protokollierten Einträge anzeigen lassen und diese Einträge in eine Datei exportieren.

Die Einträge werden durch Klicken auf **Einträge ansehen und exportieren** im *Kontextmenü* des Knotens Protokollierung bzw. durch Klicken auf das Symbol in der Symbolleiste angezeigt.

Öffnet den Dialog zum Ansehen und Exportieren der protokollierten Ereignisse.

Im angezeigten Dialog werden alle Ereignisse, die für die Protokollierung aktiviert wurden, angezeigt.

Durch Klicken auf die jeweiligen Spaltenüberschriften können die Einträge sortiert werden.

Ein Doppelklick auf einen Eintrag zeigt Details zum protokollierten Ereignis an.

Zusätzlich stellt conpal LAN Crypt einen Filter zur Verfügung, über den Bedingungen für die angezeigten Ereignisse angegeben werden können.

3.20.4 Filtern

Durch Klicken auf **Filtern** im Dialog der protokollierten Ereignisse wird ein Dialog angezeigt, in dem ein Filter für die protokollierten Ereignisse definiert werden kann.

Für das Filtern der Ereignisse können folgende Parameter angegeben werden:

- **Nur Einträge eines bestimmten Ereignisses anzeigen**
  Wird diese Option ausgewählt, werden nur die Einträge für die in der Drop-Down-Liste ausgewählte Aktion angezeigt. Die Liste enthält alle protokollierbaren Ereignisse.

- **Nur Einträge eines bestimmten SO anzeigen**
  Wird diese Option ausgewählt, kann in der Drop-Down-Liste ein Security Officer ausgewählt werden. Es werden dann nur die Ereignisse angezeigt, die protokolliert wurden, als dieser SO an der Administration angemeldet war. Die Drop-Down-Liste enthält nur Security Officer, für die Einträge vorhanden sind.

- **Nur Ereignisse einer bestimmten Stufe anzeigen**
  Wird diese Option ausgewählt, kann mit den beiden Drop-Down-Listen eine einzelne Kategorie bzw. ein Bereich von Kategorien angeben werden, der angezeigt werden soll. *Stufe ist höchstens* und *Stufe ist mindestens* beziehen sich auf die Zahl vor der jeweiligen Kategorie.

- **Nur Ereignisse einer bestimmten Zeitspanne anzeigen**
  Wird diese Option ausgewählt, kann eine Zeitspanne angegeben werden, in der die angezeigten Einträge liegen sollen.

- **Nur Ereignisse mit einem bestimmten Status anzeigen**
  Wird diese Option aktiviert, kann ausgewählt werden, ob nur noch nicht archivierte oder nur archivierte Beiträge (bereits archivierte Einträge verbleiben in der Datenbank, bis sie gelöscht werden) angezeigt werden sollen. Wird die Option nicht aktiviert, werden immer alle Einträge angezeigt.

- **Nur Ereignisse eines bestimmten Standortes anzeigen**
  Wird diese Option aktiviert, werden nur die Ereignisse, die an einem bestimmten Standort protokolliert wurden, angezeigt.

Verschiedene Standorte existieren nur, wenn mit einer verteilten Datenbank gearbeitet wird. Welche Standorte sichtbar sind, hängt davon ab, wie die Datenbank repliziert wird.

3.20.5 Einträge archivieren, löschen, prüfen

Hinweis: Zum Archivieren, Löschen und Prüfen der protokollierten Einträge benötigt ein Security Officer das Recht **Protokollierung verwalten**.

Ein Security Officer, der das globale Recht ***Protokollierung verwalten*** besitzt, kann protokollierte Einträge archivieren, löschen und prüfen.

Durch Klicken auf **Einträge archivieren, löschen, prüfen** im *Kontextmenü* des Knotens Protokollierung bzw. durch Klicken auf das Symbol in der Symbolleiste wird für diese Aktionen ein Assistent gestartet.

Startet einen Assistenten zum Archivieren, Löschen und Prüfen protokollierter Ereignisse.

Einträge archivieren

Zum Archivieren von Einträgen markieren Sie **Einträge archivieren** und klicken Sie auf **Weiter**.

Im nächsten Dialog können Sie festlegen:

- Datum und Zeitpunkt des letzten Eintrags, der archiviert werden soll. Alle Einträge von diesem Zeitpunkt an bis heute werden archiviert.
- Die Einträge welchen Standorts (soweit vorhanden) archiviert werden
- Den Namen der Datei, in der die Einträge archiviert werden sollen.

Klicken Sie auf **Weiter**. Im nächsten Dialog wird angezeigt, wie viele Einträge ausgewählt wurden. Klicken Sie auf **Weiter**. Sind alle Einträge archiviert, wird die letzte Seite des Assistenten angezeigt. Klicken Sie auf **Fertig stellen,** um den Assistenten zu schließen.

Archivierte Einträge verbleiben in der Datenbank und können gelöscht werden. Sie werden auf den Status *Archiviert* gesetzt.

Archivierte Einträge löschen

Um archivierte Einträge zu löschen, klicken Sie auf *Archivierte Einträge löschen* und klicken Sie auf **Weiter**.

Im nächsten Dialog können Sie festlegen:

- Datum und Zeitpunkt des letzten Eintrags, der gelöscht werden soll. Alle Einträge von diesem Zeitpunkt an bis heute werden gelöscht.

Hinweis: Der letzte mögliche Zeitpunkt ist abhängig vom in den Grundeinstellungen angegebenen Mindestalter von Protokolleinträgen.

- Standort, dessen Einträge (soweit vorhanden) gelöscht werden soll.

Klicken Sie auf **Weiter**. Im nächsten Dialog wird angezeigt, wie viele Einträge ausgewählt wurden. Klicken Sie auf **Weiter**. Sind die Einträge gelöscht, wird die letzte Seite des Assistenten angezeigt. Klicken Sie auf **Fertig stellen,** um den Assistenten zu schließen.

Archiveinträge prüfen

Zum Prüfen der Integrität der Protokollereignisse klicken Sie auf *Archiveinträge prüfen* und klicken Sie auf **Weiter**.

Im nächsten Dialog können Sie festlegen, welche Daten geprüft werden sollen. Es können die Daten einer Datenbank oder eines Archivs geprüft werden.

Soll eine Datenbank geprüft werden, können Sie bei verteilten Datenbanken den Standort der zu prüfenden Datenbank auswählen.

Soll ein Archiv geprüft werden, können Sie die Datei über die **Durchsuchen** Schaltfläche auswählen.

Klicken Sie auf **Weiter**. Im nächsten Dialog wird angezeigt, wie viele Einträge ausgewählt wurden. Klicken Sie auf **Weiter**. Sind alle Einträge geprüft, wird die letzte Seite des Assistenten angezeigt. In diesem Dialog wird das Ergebnis der Prüfung angezeigt. Wurden die geprüften Daten manipuliert, wird eine entsprechende Meldung angezeigt.

Klicken Sie auf **Fertig stellen,** um den Assistenten zu schließen.

4 conpal LAN Crypt Konfiguration

Hinweis: Konfigurationseinstellungen müssen mit dem 32 Bit Group Policy Management Editor oder dem 32 Bit Local Group Policy Editor definiert werden. Wenn Sie ein 64 Bit System benutzen, starten Sie diese Editoren, indem Sie auf den entsprechenden Eintrag unter Start\Alle Programme\Sophos\conpal LAN Crypt klicken. Damit stellen Sie sicher, dass die richtige Version gestartet wird.

Die folgenden Einstellungen sind maschinen- oder benutzerspezifische Einstellungen. Um diese Einstellungen zu bearbeiten, benötigen Sie Administratorrechte in der Domäne oder im Active Directory. Sie sollten nur vom Systemadministrator vorgenommen werden.

Die Konfigurationseinstellungen werden über den Knoten *LAN Crypt Konfiguration* vorgenommen. Dieser Knoten wird bei der Arbeit mit Systemrichtlinien in der Management Konsole unter jedem Computerknoten und unter jedem Benutzerknoten angezeigt.

In der Active Directory Umgebung wird der Knoten *LAN Crypt Konfiguration* unter dem GPO *Computerkonfiguration* bzw. Benutzerkonfiguration/Windows Einstellungen/conpal angezeigt.

Hinweis: Alternativ können Sie die Administratorvorlagen aus dem Verzeichnis \config Ihres extrahierten Installationspakets verwenden. Eventuell wollen Sie diese auf Rechnern verwenden, auf denen conpal LAN Crypt Administration nicht installiert ist.

In der Regel werden die Konfigurationseinstellungen maschinenspezifisch vorgenommen werden. Die Möglichkeit, diese auch benutzerspezifisch vorzunehmen erlaubt es, bestimmten Benutzern spezielle Einstellungen zukommen zu lassen. Wenn Sie **benutzerspezifische** Einstellungen vorgenommen haben, so **überschreiben** diese die maschinenspezifischen Einstellungen.

Sollen einmal getroffene benutzerspezifische Einstellungen wieder aufgehoben werden, damit wieder die Computereinstellungen ausgewertet werden, muss die entsprechende Einstellung auf *nicht konfiguriert* gesetzt werden. Markieren Sie dazu die betreffende Einstellung und drücken Sie die **Entfernen**-Taste. In der Management Konsole wird in der Spalte *Konfiguriert* dann **Nein** angezeigt.

4.1 Client-Einstellungen

Bei markiertem Knoten *Client Einstellungen* werden im rechten Konsolenfenster die konfigurierbaren Einstellungen angezeigt. Ein Doppelklick auf einen Eintrag öffnet jeweils einen Dialog, in dem die Einstellungen vorgenommen werden können.

4.1.1 Ver-/Entschlüsselung erlauben

Die Benutzeranwendung von conpal LAN Crypt erlaubt die Ver- und Entschlüsselung von Dateien durch einen Eintrag im Kontextmenü der Dateien. Auf diese Weise können auch Dateien verschlüsselt werden, für die keine Regel definiert wurde.
Soll das verhindert werden, kann hier festgelegt werden, dass diese Möglichkeit im Kontextmenü von Dateien nicht angeboten wird.

Ver-/Entschlüsselung erlauben: nein
Verhindert, dass Dateien, für die keine Verschlüsselungsregel definiert wurde, über das Kontextmenü ver-/entschlüsselt werden.

4.1.2 Fehler bei der Zertifikatsüberprüfung ignorieren

conpal LAN Crypt erlaubt festzulegen, ob mögliche Fehler bei der Überprüfung der Zertifikate der Benutzer ignoriert werden.

Ein Anlass für eine solche Vorgehensweise kann sein, dass die Gültigkeitsdauer der Zertifikate abläuft und noch keine neuen Zertifikate zur Verfügung stehen. Um sicherzustellen, dass die Benutzer weiter Zugriff auf ihre Verschlüsselungsprofile haben, kann bis zur Verteilung der neuen Zertifikate die Prüfung der Gültigkeitsdauer ignoriert werden. Damit können diese eigentlich abgelaufenen Zertifikate noch weiter verwendet werden. Sind die neuen Zertifikate verfügbar, kann **Gültigkeitsdauer ignonieren** wieder aufgehoben werden.

Hinweis: Fehler bei der Zertifikatsprüfung zu ignorieren, bedeutet immer auch eine Senkung des Sicherheitsniveaus.

- **Widerruf des Zertifikats ignorieren**

  Wenn sich das Zertifikat auf einer **C**ertificate **R**evocation **L**ist befindet, die bei der Anmeldung ausgewertet wird, darf es eigentlich nicht zur Anmeldung verwendet werden. Wird diese Option aktiviert, kann der Benutzer das Zertifikat trotzdem verwenden, um Zugriff auf sein Verschlüsselungsprofil zu haben.

- **Gültigkeitsdauer ignorieren**

  Obwohl die Gültigkeitsdauer abgelaufen ist, kann das Zertifikat zum Zugriff auf das Verschlüsselungsprofil verwendet werden.

- **Ungültigen Zertifizierungspfad ignorieren**

  Obwohl der öffentliche Teil des Zertifikats des Ausstellers auf dem Client nicht vorhanden ist oder sich nicht im richtigen Zertifikatsspeicher befindet, kann das Zertifikat zum Zugriff auf das Verschlüsselungsprofil verwendet werden, wenn diese Option aktiviert ist.

- **Unbekannten Widerruf ignorieren**

  PKI von manchen Herstellern tragen nicht standardisierte Gründe für den Widerruf eines Zertifikats in eine CRL ein. In der Regel ist ein Zertifikat nicht erlaubt, auch wenn der Grund des Widerrufs nicht bekannt ist. Wird diese Option aktiviert, kann das Zertifikat zum Zugriff auf das Verschlüsselungsprofil verwendet werden.

Hinweis: Bitte beachten Sie, dass das Ignorieren von Fehlern bei der Zertifikatsprüfung in den meisten Fällen auch ein Umgehen der Sicherheitsrichtlinien eines Unternehmens bedeutet.

Diese Einstellungen können auch unter Server Einstellungen definiert werden. Zertifikate werden sowohl bei der Anmeldung eines Security Officer an der conpal LAN Crypt Administrationskonsole als auch bei der Durchführung einer zusätzlichen Autorisierung geprüft.

4.1.3 Novell-Namen verwenden

Geben Sie hier an, ob beim Suchen der Richtliniendateien nach der Datei mit dem Novell-Logonnamen gesucht werden soll. Wenn Sie in der Administration unter Zentrale Einstellungen/ Verzeichnisse angeben, dass Richtliniendateien mit Novell-Namen erzeugt werden sollen, erzeugt conpal LAN Crypt für jeden Benutzer zwei Richtliniendateien. Eine mit dem Novell-Logonnamen und eine mit dem Windows-Benutzernamen. Der Inhalt der beiden Dateien ist identisch.

Bei der Anmeldung an einen Novell-Server muss immer der Novell-Logonname verwendet werden.

Ist in den Systemeinstellungen festgelegt, dass der Windows-Benutzername als Logonname verwendet werden muss, so setzen Sie **Use Novell Logon Name verwenden** auf **nein.**

Hinweis: Sollte eine Novell-Anmeldung für den Client einmal nicht möglich sein (z. B. keine Verbindung zum Server) und der Benutzer sich lokal mit dem Windows Benutzernamen anmeldet, wird das Verschlüsselungsprofil trotzdem korrekt aus der Richtliniendatei geladen, da conpal LAN Crypt die entsprechende Richtliniendatei auch anhand des Windows Benutzernamens identifizieren kann. Die Datei wird bei einer lokalen Anmeldung aus dem Cache gelesen. Deren Aktualität entspricht der der letzten Novell Netzwerkanmeldung.

4.1.4 Alle Umgebungsvariablen verwenden

Die Umgebungsvariable %USERNAME% in Pfadangaben wird von conpal LAN Crypt standardmäßig aufgelöst.

Hier können Sie festlegen, ob auch andere Umgebungsvariablen in Pfadangaben aufgelöst werden sollen.

Der Einsatz anderer Umgebungsvariablen in Pfadangaben kann problematisch werden, wenn die Benutzer in der Lage sind, diese zu ändern. Dies kann dazu führen, dass Pfadangaben im Verschlüsselungsprofil ihre Wirkung verlieren.

4.1.5 Menüeinträge aktivieren

Hier können Sie festlegen, welche Menüeinträge im conpal LAN Crypt Benutzermenü auf einem Client-Rechnern sichtbar sind. In der Standardeinstellung werden alle Menüeinträge angezeigt. Deaktivieren Sie hier einen Menüeintrag, wird er auf dem Client-Rechner nicht angezeigt. Damit steht diese Funktionalität auf diesem Client nicht zur Verfügung. So können Sie zum Beispiel verhindern, dass die Verschlüsselung auf einem Client-Rechner deaktiviert wird.

4.1.6 Standard 'Ignorieren Regel'

Da beim Booten einer Arbeitsstation der conpal LAN Crypt Treiber geladen wird, werden bereits alle Dateien auf eine mögliche Verschlüsselung und damit auf die entsprechenden Zugriffsrechte geprüft, auch wenn noch kein benutzerspezifisches Verschlüsselungsprofil geladen ist. Dies kann zu Performance-Einbußen in dieser Phase führen.

Mit Hilfe einer maschinenspezifischen Einstellung in der conpal LAN Crypt Konfiguration kann der conpal LAN Crypt Treiber angewiesen werden, bestimmte Verzeichnisse zu ignorieren, bis das Verschlüsselungsprofil des Benutzers geladen ist.

Doppelklicken Sie **Standard "Ignorieren Regel"** in den Client-Einstellungen, um einen Dialog zu öffnen, in dem Verzeichnisse (z.B. **"**`c:\*.*;d:\*.*`**"**) angegeben werden können, die vom conpal LAN Crypt-Treiber ignoriert werden.

Werden mehrere Pfade angegeben, müssen diese durch einen Strichpunkt getrennt werden.

Bei der Verwendung von solchen Regeln muss aber berücksichtigt werden, dass dadurch die conpal LAN Crypt spezifische Zugriffskontrolle entfällt, bis das Verschlüsselungsprofil des Benutzers geladen ist.

Beispiel:

Wenn Sie **"**`c:\*.*;d:\*.*`**"** als Standard „Ignorieren Regel“ angeben, so wird der Treiber angewiesen, alle Verzeichnisse auf den Laufwerken C und D, zu ignorieren, bis das Verschlüsselungsprofil des Benutzers geladen wird.

Auch beim Einsatz von conpal LAN Crypt auf einem Terminal Server kann der Einsatz von Standard „Ignorieren Regel“ zu einem Performance-Gewinn führen. Arbeiten auf dem Terminal Server z. B. mehrere Benutzer, von denen nur einer conpal LAN Crypt verwendet, kann der Treiber so angewiesen werden, die Sessions der anderen Benutzer zu ignorieren. Da diese kein Verschlüsselungsprofil geladen haben, gilt für sie nur die Standard „Ignorieren Regel“.

4.1.7 Speicherort für Security Officer Zertifikate

Zur Angabe des Speicherorts markieren Sie *Client Einstellungen* und klicken Sie im rechten Konsolenfenster auf **Speicherort für Security Officer Zertifikate** doppelt.

Nach Angabe eines Pfads versucht conpal LAN Crypt, automatisch das Security Officer Zertifikat aus diesem Verzeichnis zu importieren, falls das Zertifikat für die betreffende Benutzerrichtliniendatei nicht vorhanden ist. Als Ergebnis werden alle (!) .cer-Dateien aus dem angegebenen Verzeichnis importiert.

4.1.8 Speicherort für Schlüsseldatei

Zur Angabe des Speicherorts markieren Sie *Client Einstellungen* und klicken Sie im rechten Konsolenfenster doppelt auf **Speicherort für Schlüsseldatei**.

Nach Angabe eines Pfads versucht conpal LAN Crypt, automatisch eine .p12-Schlüsseldatei für den Benutzer zu importieren, falls der private Schlüssel der Richtliniendatei nicht vorhanden ist. Die Datei muss "l`Anmeldename*.p12`" heißen, damit sie für den betreffenden Benutzer erkannt wird.

Beide oben beschriebenen Pfade sind standardmäßig nicht gesetzt, d. h. es erfolgt kein automatisches Laden des öffentlichen Teils des Security- Administrator-Zertifikats bzw. der Zertifikate des Benutzers. Ein automatisches Laden erfolgt erst, nachdem der Security Officer die Pfade explizit gesetzt hat.

Die conpal LAN Crypt Administration speichert sowohl die .p12-Dateien für die Benutzer als auch den öffentlichen Teil des Security Officer Zertifikates in dasselbe Verzeichnis. Aus Client-Sicht sind die Pfade trotzdem getrennt konfigurierbar, um eventuell eine der beiden Funktionen abschalten zu können. In der Regel werden diese beiden Pfade daher aber gleich sein. Sollen Security Officer Zertifikat und Benutzerzertifikate automatisch aus verschiedenen Verzeichnissen geladen werden, müssen sie manuell in die entsprechenden Verzeichnisse kopiert werden.

4.1.9 Speicherort für Richtliniendatei

Zur Angabe des Speicherorts markieren Sie *Client Einstellungen* und klicken Sie im rechten Konsolenfenster doppelt auf **Speicherort für Richtliniendatei**.

Geben Sie den Pfad für den Speicherort der benutzerspzefischen Richtliniendatei ein. Um sicherzustellen, dass Clients auf ihre Richtliniendateien zugreifen können (zum Beispiel auf einer Netzwerkfreigabe), muss der Pfad aus der Sicht des Client angegeben werden.

Üblicherweise ist dies das Verzeichnis, in dem sie von conpal LAN Crypt erzeugt wurden. Es muss unbedingt die UNC-Schreibweise (Universal Naming Convention) verwendet werden, da zu diesem Zeitpunkt noch keine Laufwerke verbunden sind!

Die %LOGONSERVER% Umgebungsvariable kann bei dieser Einstellung verwendet werden (für Load Balancing oder ähnliches).

4.1.10 Zwischenspeicherort für Richtliniendatei

Zur Angabe des Zwischenspeicherorts markieren Sie *Client Einstellungen* und klicken Sie im rechten Konsolenfenster doppelt auf **Zwischenspeicherort für Richtliniendatei**.

In diesem Verzeichnis wird eine lokale Kopie der Richtliniendatei gespeichert. Diese Kopie wird normalerweise von einem Netzwerkverzeichnis gelesen. Der Benutzer muss über Schreibrechte in dem lokalen Verzeichnis verfügen. Damit kann sichergestellt werden, dass ein Verschlüsselungsprofil eines Benutzers verfügbar ist, auch wenn keine Netzwerkverbindung besteht.

Es kann entweder einer der vorgeschlagenen Speicherorte aus der Liste verwendet werden, oder es wird nach der Auswahl von <Andere> ein beliebiger Pfad im Eingabefeld eingetragen.

Hinweis: Bei den angebotenen Speicherorten handelt es sich um Windows Standard-Verzeichnisse, die vom verwendeten Betriebssystem abhängig sind. <Lokale Anwendungsdaten> bezieht sich immer auf ein Verzeichnis auf der lokalen Maschine, während sich alle anderen unter Umständen (z. B. Roaming Users) auch auf Netzwerklaufwerken befinden können.
Wird ein Speicherort manuell angegeben, muss sichergestellt werden, dass das Verzeichnis auf den Client-Rechnern existiert.

Hinweis: Wenn Sie einen Benutzer aus Ihrer conpal LAN Crypt Umgebung entfernen wollen, müssen Sie bedenken, dass die lokale Kopie auf dem Rechner gespeichert bleibt. Solange dies der Fall ist, kann der Benutzer mit den darin enthaltenen Rechten auf Daten zugreifen.
Um dies zu vermeiden, sollten Sie für diesen Benutzer eine leere Richtliniendatei erzeugen. Löschen Sie hierzu die Richtliniendatei und entfernen Sie den Benutzer aus allen Gruppen.

4.1.11 Verzögerung beim Laden des Profils

Hier können Sie eine Zeitspanne in Sekunden angeben, die gewartet wird bis das Profil des Benutzers geladen wird. Diese Verzögerung ist z.B. dann von Bedeutung, wenn ein Zertifikat auf einem Token verwendet wird. Die Verzögerung beim Laden des Profils stellt sicher, dass auf den Token zugegriffen werden kann, wenn das Zertifikat benötigt wird. Typischer Wert: 20 Sekunden.

4.1.12 Dateitypen für den Assistenten zur Initialverschlüsselung

Wenn Sie hier bestimmte Dateitypen angeben, werden ausschließlich Dateien vom angegebenen Typ vom Assistenten zur Initialverschlüsselung bearbeitet. Der Benutzer kann diese Einstellung im Assistenten zur Initialverschlüsselung nicht verändern!

Diese Einstellung wirkt sich nur auf Dateien aus, für die eine Verschlüsselungsregel existiert.

Befinden sich auch noch andere Dateien eines Typs, der nicht hier angegeben wird, in einem Verzeichnis, werden sie bei der Initialverschlüsselung nicht berücksichtigt. Sie werden erst verschlüsselt, wenn sie vom Benutzer geöffnet und wieder abgespeichert werden.

Möchten Sie den Benutzer die Möglichkeit geben, diese Einstellung im Assistenten zur Initialverschlüsselung selbst vorzunehmen, belassen Sie diese Einstellung auf nicht konfiguriert.

Haben Sie hier Dateitypen angegeben und wollen zu einem späteren Zeitpunkt dem Benutzer die Auswahl vornehmen lassen, müssen Sie diese Einstellung wieder auf nicht konfiguriert setzen.

Hinweis: Diese Einstellung gilt nur für den Assistenten zur Initialverschlüsselung. Wird die Initialverschlüsselung über die Explorer-Erweiterung gestartet, hat sie keine Auswirkung.

Verwenden Sie zur Angabe der Dateitypen eine durch Strichpunkte getrennte Liste.

Beispiel: `doc;xls;txt`

4.1.13 Lebensdauer der Zwischenspeicherung der Richtliniendatei

Standardverhalten von conpal LAN Crypt

Wenn sich ein Benutzer an Windows anmeldet, wird zuerst sein (zwischen)gespeichertes Benutzerprofil geladen. Danach überprüft conpal LAN Crypt, ob es eine neue Richtliniendatei für den Benutzer gibt, indem es eine Verbindung zum festgelegten Speicherort für Richtliniendateien (Netzwerklaufwerk) aufbaut. Wird dort einen neuere Richtliniendatei gefunden, wird das zwischengespeicherte Benutzerprofil aktualisiert.

Diese Vorgehensweise hat den Vorteil, dass der Benutzer bereits mit verschlüsselten Daten arbeiten kann, während conpal LAN Crypt überprüft, ob es eine neuere Version der Richtliniendatei gibt.

Ist das Netzwerklaufwerk nicht erreichbar, arbeitet der Benutzer solange mit dem zwischengespeicherten Benutzerprofil, bis dieses aktualisiert werden kann.

Ist diese Option auf *nicht konfiguriert* gesetzt, verhält sich conpal LAN Crypt wie hier beschrieben.

Mit dieser Einstellung können Sie das Standardverhalten verändern.

Hinweis: Sie können eine Einstellung auf nicht konfiguriert setzen, indem Sie diese markieren, und in ihrem Kontextmenü (Klick mit der rechten Maustaste) auf Löschen klicken. In der Spalte ***Konfiguriert*** wird neben der relevanten Option jetzt **nein** angezeigt.

Sie können hier angeben, wie lange die zwischengespeicherte Richtlinie auf den Client-Computern gültig ist.

Innerhalb des angegebenen Zeitraums ist die Richtliniendatei auf dem Client gültig und der Benutzer hat Zugriff auf verschlüsselte Daten, auch wenn keine Verbindung zum Speicherort der Richtliniendatei besteht.

Der Zeitraum, wie lange die Richtliniendateien zwischengespeichert werden und damit gültig bleiben, kann in Tagen oder Wochen angegeben werden.

Läuft die angegebene Dauer ab, versucht conpal LAN Crypt noch einmal, die Richtliniendatei vom Netzwerklaufwerk zu laden, um sie zu aktualisieren. Ist dies nicht möglich, wird die Richtliniendatei entladen. Der Benutzer hat keinen Zugriff mehr auf verschlüsselte Daten. Erst wenn wieder eine gültige Richtliniendatei zur Verfügung steht (z. B. bei der nächsten Anmeldung mit einer Verbindung zum Speicherort der Richtliniendateien für die Clients), wird die Richtliniendatei aktualisiert und geladen. Der Benutzer hat wieder Zugriff auf verschlüsselte Daten. Der Zähler für die Dauer der Zwischenspeicherung wird zurückgesetzt.

Die Angabe der Dauer der Zwischenspeicherung kann einerseits sicherstellen, dass die Client-Computer in regelmäßigen Intervallen mit aktuellen Richtliniendateien versorgt werden und die Benutzer immer aktuelle Richtlinien verwenden. Denn solange die Richtliniendateien durch eine Verbindung zum Speicherort für Richtliniendateien nicht aktualisiert werden, kann ein Benutzer mit einer zwischengespeicherten Version der Richtliniendatei unbeschränkt lange arbeiten, wenn diese Einstellung auf *nicht konfiguriert* gesetzt ist.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung zurückgesetzt:

- Der Speicherort der Richtliniendateien ist erreichbar, es wurde eine gültige Richtliniendatei auf den Client übertragen (z. B. bei der Anmeldung des Benutzers, oder ausgelöst durch ein eingestelltes Aktualisierungsintervall), diese ist aber nicht neuer als die bestehende.
- Eine neue Richtliniendatei ist verfügbar und wurde erfolgreich geladen.

In folgenden Fällen wird der Zähler für die erlaubte Dauer der Zwischenspeicherung NICHT zurückgesetzt:

- Der Client-Computer versucht, eine neue Richtliniendatei zu erhalten. Der Speicherort der Richtliniendateien ist jedoch nicht erreichbar.
- Eine neue Richtliniendatei wurde übertragen. Sie konnte aber aufgrund eines Fehlers nicht geladen werden.
- Es ist eine neue Richtliniendatei verfügbar. Diese Richtliniendatei verlangt aber ein neues Zertifikat. Der Benutzer besitzt dieses Zertifikat nicht oder kann es nicht laden.

Schlägt die Aktualisierung der Richtliniendatei fehl, wird auf dem Client-Computer der Ablaufzeitpunkt der zwischengespeicherten Richtliniendatei in Form einer Sprechblasen-Hilfe angezeigt. Der Benutzer kann dann eine manuelle Aktualisierung über das conpal LAN Crypt Tray-Icon anstoßen. Eine automatische Aktualisierung wird auch entsprechend den Einstellungen unter *Aktualisierungsintervall für das Benutzerprofil* durchgeführt.

Keine Zwischenspeicherung der Richtliniendatei

Wird diese Einstellung auf 0 gesetzt, wird die Richtliniendatei nicht zwischengespeichert. Das bedeutet, dass der Benutzer sein Benutzerprofil bei der Anmeldung erhält, wenn der Speicherort der Richtliniendatei erreichbar ist. Ist dieser nicht erreichbar oder tritt ein Fehler beim Laden des Profils auf, kann der Benutzer nicht auf verschlüsselte Daten zugreifen.

Clients ab Version 3.12

Diese Funktionalität steht für ältere Client-Versionen nicht zur Verfügung. Clients ab der Version 3.12 können aber mit dieser Version der Adminstration betrieben werden. Diese Clients verhalten sich beim Laden der Richtliniendateien wie folgt:
Es wird immer versucht, die Richtliniendatei aus dem angegebenen Speicherort zu laden. Ist dieser nicht erreichbar, wird eine zwischengespeicherte Version der Richtliniendatei geladen. Diese zwischengespeicherte Richtliniendatei hat kein Ablaufdatum und wird erst aktualisiert, wenn eine neuere Version erfolgreich geladen wurde. Es kann auch kein Aktualisierungsintervall für die Richtlinien festgelegt werden (siehe *Aktualisierungsintervall für das Benutzerprofil* auf Seite 145). Zwischengespeicherte Richtliniendateien behalten ihre Gültigkeit, bis der Speicherort erreichbar ist und sie durch eine von dort neu geladene Datei ersetzt werden können.

4.1.14 NTFS-Dateidekomprimierung

Diese Einstellung ermöglicht die Bearbeitung von NTFS komprimierten Dateien durch den Assistenten zur Initialverschlüsselung. Wird die Option **NTFS-Dateidekomprimierung** auf **ja** gesetzt, dekomprimiert der Assistent NTFS-komprimierte Dateien und verschlüsselt sie anschließend, wenn für sie eine Verschlüsselungsregel gilt.

Ist die Option **NTFS-Dateidekomprimierung** auf **nein** gesetzt, werden NTFS-komprimierte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht verschlüsselt, auch wenn für sie eine Verschlüsselungsregel festgelegt wurde.

Wird diese Option konfiguriert, kann der Benutzer diese Option im Assistenten zur Initialverschlüsselung nicht ändern! Nur wenn diese Option auf *nicht konfiguriert* gesetzt wird, kann der Benutzer diese Option im Assistenten zur Initialverschlüsselung selbst vornehmen.

4.1.15 EFS-Dateientschlüsselung

Diese Einstellung ermöglicht die Bearbeitung von EFS verschlüsselten Dateien durch den Assistenten zur Initialverschlüsselung. Wird die Option **EFS Dateientschlüsselung** auf **ja** gesetzt, entschlüsselt der Assistent EFS verschlüsselte Dateien und verschlüsselt sie anschließend, wenn für sie eine conpal LAN Crypt Verschlüsselungsregel gilt.

Ist die Option **EFS Dateientschlüsselung** auf nein gesetzt, werden EFS verschlüsselte Dateien vom Assistenten zur Initialverschlüsselung ignoriert. Sie werden nicht von conpal LAN Crypt umgeschlüsselt, auch wenn für sie eine Verschlüsselungsregel besteht.

Wird diese Option konfiguriert, kann der Benutzer diese Option im Assistenten zur Initialverschlüsselung nicht ändern! Nur wenn diese Option auf *nicht konfiguriert* gesetzt wird, kann der Benutzer diese Option im Assistenten zur Initialverschlüsselung selbst vornehmen.

Hinweis: Sie können eine Einstellung auf *nicht konfiguriert* setzen, indem sie diese markieren, und in ihrem Kontextmenü (Klick mit der rechten Maustaste) auf **Löschen** klicken. In der Spalte ***Konfiguriert*** wird neben der relevanten Option jetzt **nein** angezeigt.

4.1.16 Aktualisierungsintervall für das Benutzerprofil

Diese Einstellung legt fest, wie oft conpal LAN Crypt überprüft, ob eine neue Richtliniendatei zur Verfügung steht und diese bei Bedarf aktualisiert.

Um eine Aktualisierung durchführen zu können, muss conpal LAN Crypt Zugriff auf das Netzwerklaufwerk, auf dem sich die Richtliniendateien befinden, haben. Es wird dann geprüft, ob dort eine neuere Version der Richtliniendatei existiert und diese wird bei Bedarf auf dem Client-Computer aktualisiert.

conpal LAN Crypt führt alle für das erfolgreiche Laden des Benutzerprofils notwendigen Schritte (wenn notwendig neue Zertifikate suchen und verifizieren, ...) automatisch durch. Nur wenn kein Fehler dabei aufgetreten ist, wird das alte durch das neue Benutzerprofil ersetzt und geladen. Danach wird der Zähler für die Dauer der Zwischenspeicherung zurückgesetzt. Sind beide Richtliniendateien identisch, wird der Zähler ebenfalls zurückgesetzt.

Ist diese Option auf nicht konfiguriert gesetzt, werden Richtliniendateien nicht aktualisiert.

Das Aktualisierungsintervall kann in Minuten, Stunden, Tagen und Wochen angegeben werden.

Hinweis: conpal LAN Crypt lässt keine Aktualisierungsintervalle zu, die kürzer als 15 Minuten sind. Wenn Sie die Option auf 0 setzen, wird die Richtlinienaktualisierung deaktiviert.

4.1.17 Fehlermeldung nicht anzeigen wenn kein Benutzerprofil gefunden

conpal LAN Crypt zeigt in der Standardeinstellung eine Fehlermeldung an, wenn kein Benutzerprofil gefunden wird.

Hier können Sie festlegen, dass diese Fehlermeldung unterdrückt wird, wenn kein Benutzerprofil gefunden wird.

Wird die **Option Fehlermeldung nicht anzeigen** auf **ja** gesetzt, wird die Anzeige der Fehlermeldung unterdrückt.

4.1.18 Persistente Verschlüsselung

Dateien bleiben normalerweise nur so lange verschlüsselt, wie sie einer Verschlüsselungsregel unterliegen. Wenn zum Beispiel ein Benutzer eine verschlüsselte Datei in einen Ordner kopiert, für den keine Verschlüsselungsregel definiert ist, wird die Datei im Zielordner entschlüsselt. Durch Aktivierung der persistenten Verschlüsselung kann der Security Officer dafür sorgen, dass Dateien auch dann verschlüsselt bleiben, wenn sie verschoben oder kopiert werden.

Die Funktion deaktivieren Sie durch einen Doppelklick auf **Persistente Verschlüsselung** und Auswahl von **Nein** aus dem Listenfeld hinter **Persist. Verschlüsselung aktivieren**.

4.1.19 Hohe Sicherheit für den privaten Schlüssel

Hier können Sie festlegen, dass der Benutzer jedesmal, wenn der private Schlüssel von conpal LAN Crypt verwendet wird, zur Authentisierung aufgefordert wird.

4.1.20 CSPs und Algorithmen

Hier können Sie den CSP und den Hash-Algorithmus angeben.

Für die neueste Client-Version muss nur der CSP für das Importieren eines privaten Schlüssels ausgewählt werden.

Für Clients vor Version 3.90 müssen zusätzliche Einstellungen konfiguriert werden. Sie müssen einen CSP für das Verifizieren der Signature der Richtliniendateien und einen Hash-Algorithmus für das Signieren/Verifizieren der Richtliniendateien auswählen.

4.2 Server-Einstellungen

Hinweis: Diese Einstellungen müssen unbedingt für den Server gesetzt sein. Sie haben für die Client-Rechner keine Auswirkung.
Sie müssen unbedingt gesetzt werden, bevor die Administration zum ersten Mal gestartet wird.

4.2.1 Hohe Sicherheit für den privaten Schlüssel

Hier können Sie festlegen, dass der Benutzer jedesmal, wenn der private Schlüssel von conpal LAN Crypt verwendet wird, zur Authentisierung aufgefordert wird.

4.2.2 SQL-Dialekt

Hier muss der SQL Dialekt, der für die Kommunikation mit der ODBC Datenquelle verwendet wird, angegeben werden.

Wählen Sie aus:

- MS SQL Server
- Oracle
- Standard SQL

Die Einstellung wird dann in Ihrer Systemkonfiguration verwendet.

4.2.3 Datenbankbesitzer

Damit die verwendete Datenbank korrekt angesprochen werden kann, muss hier der Datenbankbesitzer angegeben werden.

Für den MS SQL Server darf der Standardwert „dbo“ für den Erzeuger nicht verändert werden. Eine Änderung ist nur bei der Verwendung einer Oracle-Datenbank notwendig.

Achtung: Bei Verwendung einer Oracle Datenbank müssen Sie den Datenbankbesitzer unbedingt in GROSSBUCHSTABEN angeben. Es muss sich hier um denselben Namen handeln, der während der Erzeugung der Datenbanktabellen verwendet wurde.

4.2.4 OBDC-Datenquelle

Hier kann der Name, mit dem auf die ODBC Datenquelle verwiesen werden soll, konfiguriert werden.

Standardmäßig verwendet conpal LAN Crypt SGLCSQLServer als Name für die ODBC Datenquelle. Wollen Sie einen anderen Namen verwenden, müssen Sie ihn hier angeben, bevor die conpal LAN Crypt Administration das erste Mal gestartet wird.

Hinweis: Der Name der hier angegebenen ODBC Quelle unterscheidet nach Groß-/ Kleinschreibung! Er muss hier genauso angegeben werden wie bei der Erstellung der ODBC Quelle. Es können nur 32 Bit ODBC Datenquellen verwendet werden.

4.2.5 Fehler bei Zertifikatsüberprüfung ignorieren

Hier können Sie angeben, welcher Zertifikatsstatus ignoriert werden soll, wenn sich ein Security Officer anmeldet oder wenn in der Administrationskonsole Zertifikate zugewiesen werden.

4.2.6 Hash-Algorithmus

Der Hash-Algorithmus muss in Client Einstellungen konfiguriert werden.

4.2.7 Zertifikatserweiterung prüfen

Standardmäßig werden von conpal LAN Crypt bei der Zuweisung aus dem Zertifikatsspeicher nur Zertifikate angeboten, die als Eigenschaft unter Schlüsselverwendung *Schlüsselverschlüsselung* und/oder *Datenverschlüsselung* eingetragen haben.

Unter **Zertifikatserweiterung prüfen** kann jedoch eingestellt werden, dass diese Prüfung entfällt und so auch Zertifikate mit anderen Eigenschaften zur Verwendung mit conpal LAN Crypt zugelassen werden.

Erweiterungen prüfen: **nein**
ermöglicht die Verwendung von Zertifikaten mit anderen Eigenschaften.

Hinweis: Werden solche Zertifikate verwendet, ist es jedoch vom verwendeten CSP abhängig, ob diese Zertifikate für conpal LAN Crypt verwendet werden können.
Sollten Sie diese Prüfung ausschalten, stellen Sie bitte sicher, dass die verwendeten Zertifikate mit conpal LAN Crypt verwendet werden können.

4.3 Unberücksichtigte Laufwerke Unberücksichtigte Anwendungen Unberücksichtigte Geräte

conpal LAN Crypt erlaubt die Definition von Laufwerken, Anwendungen und Geräten (Netzwerk-Dateisysteme), die vom conpal LAN Crypt Filter-Treiber ignoriert werden sollen und damit von der transparenten Ver-/Entschlüsselung ausgenommen sind.

Ein Beispiel für eine unberücksichtigte Anwendung kann ein Backup-Programm sein. Damit die Daten beim Erstellen eines Backups nicht entschlüsselt werden, kann diese Anwendung von der Verschlüsselung/Entschlüsselung ausgenommen werden. Die Daten werden verschlüsselt gesichert.

Das Ausschließen ganzer Laufwerke führt zu einem Performance-Gewinn. Soll z. B. auf Laufwerk E keine Verschlüsselung stattfinden, wird es einfach als „Unberücksichtigtes Laufwerk“ definiert. Alternativ könnte man eine Regel für dieses Laufwerk mit der Option „Verschlüsselungsregel nicht berücksichtigen“ definieren.

Durch die Definition als „Unberücksichtigtes Laufwerk“ entfällt aber die Abarbeitung des Profils durch den Filter-Treiber, so dass Dateioperationen schneller durchgeführt werden können.

Sie finden diese Einstellungen unter dem Knoten **LAN Crypt Konfiguration**.

Hinweis: Da es sich dabei um maschinenspezifische Einstellungen handelt, werden diese erst nach einem Neustart der Client-Rechner wirksam.

4.3.1 Unberücksichtigte Laufwerke hinzufügen

Markieren Sie *Unberücksichtigte Laufwerke* und klicken Sie im Kontextmenü auf **Unberücksichtigte(s) Laufwerk(e)** hinzufügen.

Markieren Sie die Laufwerke, die conpal LAN Crypt nicht berücksichtigen soll, und klicken Sie auf **OK**.

4.3.2 Unberücksichtigte Anwendungen hinzufügen

Markieren Sie *Unberücksichtigte Anwendungen* und klicken Sie im Kontextmenü auf **Unberücksichtigte Anwendungen hinzufügen**.

Typische Verwendung:

- Backup-Programme können als unberücksichtigt definiert werden, damit sie immer die verschlüsselten Daten lesen und sichern.
- Anwendungen, die bei gleichzeitiger Verwendung mit conpal LAN Crypt Funktionsstörungen auslösen können, aber keine Verschlüsselung benötigen, können generell von der Verschlüsselung ausgenommen werden.

Um eine unberücksichtigte Anwendung anzugeben, geben Sie den gesamten Namen der ausführbaren Datei ein.

Geben Sie den Namen und den Pfad (falls erforderlich) der Anwendung ein und klicken Sie auf OK.

4.3.3 Unberücksichtigte Geräte hinzufügen

Markieren Sie *Unberücksichtigte Geräte* und klicken Sie im Kontextmenü auf **Unberücksichtigte Geräte hinzufügen**.

Im Dialog *Unberücksichtigte Geräte* werden Netzwerk-Dateisysteme angeboten, die nicht von conpal LAN Crypt verschlüsselt werden sollen. Aus technischen Gründen ist es nicht möglich, hier einzelne Netzwerklaufwerke auszuschließen. Es können nur ganze Netzwerk-Dateisysteme ausgeschlossen werden. Als vordefinierte Geräte stehen hier zur Verfügung:

- Citrix Client Drive Mapping
- Client für Microsoft-Netzwerke

- Microsoft Client für Netware
- Multiple UNC Provider
- Novell Client für Netware

Hinweis: Einzelne (Netz-)Laufwerke können vom Security Officer durch das Anlegen einer entsprechenden Verschlüsselungsregel von der Verschlüsselung ausgenommen werden.

Neben den bekannten Netzwerk-Dateisystemen können auch Geräte durch die Angabe ihres Gerätenamens ausgeschlossen werden. Dies kann nützlich sein, wenn Dateisysteme von Drittanbietern verwendet werden, die von einer Verschlüsselung ausgenommen werden sollen.

Administratoren können Werkzeuge wie OSRs DeviceTree verwenden, um sich die Namen der auf dem System verwendeten Dateisysteme anzeigen zu lassen.

Windows Vista und Windows 7

Für Windows Vista und Windows 7 wird nur die **Multiple UNC Provider** (**nur Vista**) berücksichtigt.

Unter Windows Vista und Windows 7 wurden die einzelnen Redirektoren durch den Multiple UNC Provider ersetzt. Das hat zur Folge, dass es nicht mehr möglich ist, einzelne Netzwerk-Dateisysteme von der Verschlüsselung auszunehmen. Windows Vista und Windows 7 erlaubt nur das Ausschließen aller Netzwerk-Dateisysteme von der Verschlüsselung oder die Aktivierung der Verschlüsselung für alle Netzwerk-Dateisysteme.

Wird die Option **Multiple UNC Provider** verwendet, findet auf keinem Netzwerklaufwerk eine Verschlüsselung statt.

Alle anderen Einstellungen werden unter Windows Vista und Windows 7 ignoriert.

4.4 Programme mit speziellem Speicherverhalten

Manche Programme (z. B. Microsoft Office 2007) verwenden beim Abspeichern von Dateien eine spezielle Vorgehensweise. Dabei können beim Öffnen einer noch unverschlüsselten Datei, für die eigentlich eine Verschlüsselungsregel gelten würde (weil z. B. noch keine Initialverschlüsselung durchgeführt wurde), und anschließendem Speichern dieser Datei Probleme auftreten. Die Datei müsste wegen der geltenden Verschlüsselungsregel eigentlich verschlüsselt gespeichert werden. Wegen des besonderen Verhaltens dieser Programme beim Speichern (temporäre Datei anlegen - umbenennen --> Änderung des Verschlüsselungsstatus) ist conpal LAN Crypt nicht in der Lage, diese Datei zu verschlüsseln.

Zur Lösung dieses Problems können diese Programme hier angegeben werden. Mit den hier angegebenen Informationen ist conpal LAN Crypt in der Lage, auch solche Dateien korrekt zu verschlüsseln.

Zum Hinzufügen eines solchen Programms:

1. Markieren Sie *Programme mit speziellem Speicherverhalten* und klicken Sie im Kontextmenü auf **Programm mit speziellem Speicherverhalten hinzufügen**.
2. Geben Sie den Namen der ausführbaren Datei des Programms an.
   Beispiel: `WINWORD.EXE`
3. Klicken Sie auf **OK**.
4. Wiederholen Sie diese Schritte für jedes weitere Programm, das Sie hinzufügen wollen.

Die Programme, deren spezielles Verhalten beim Abspeichern von Dateien eine besondere Behandlung durch conpal LAN Crypt erfordert, werden in der rechten Ansicht angezeigt.

Hinweis: Dieses Problem tritt nur beim Speichern einer beim Öffnen noch unverschlüsselten Datei auf, die beim Speichern aufgrund einer geltenden Verschlüsselungsregel, verschlüsselt werden muss (Änderung des Verschlüsselungsstatus).

Bei der Verwendung von Microsoft Office 2007, wird dringend empfohlen, die ausführbaren Dateien dieser Software hier einzutragen.

5 Anhang

5.1 Rechteprotokollierung

```
.... Rechte für 'SO_Sophos-Linz' wurden hinzugefügt. Zulassen: 0x86000000
- Verweigern: 0x0)...
```

Aus den Werten hinter **Zulassen:** und **Verweigern:** ist ersichtlich, welche Rechte konkret bearbeitet wurden.
Die folgenden Tabellen dienen zur Interpretation der Werte:

Zulassen: 0x86000000

ACL für SO: Lesen	0x80000000
ACL für SO: Zertifikat ändern	0x02000000
ACL für SO: Region ändern	0x04000000
Zulassen:	0x86000000

Globale Rechte des Security Officers

Rechte	Werte
SOs erzeugen	0x000001
Profile erzeugen	0x000002
Schlüssel erzeugen	0x000004
Schlüssel kopieren	0x000008
Schlüssel entfernen	0x000010
Schlüssel lesen	0x000020
Zertifikate erzeugen	0x000040
Zertifikate zuweisen	0x000080
Gruppen ändern	0x000200
Anmeldung an DB	0x000400
Operationen autorisieren	0x000800
Benutzer ändern	0x001000
Regeln erzeugen	0x002000
Globale Rechte ändern	0x004000
ACL ändern	0x008000

Rechte	Werte
Spezifische Schlüssel verwenden	0x010000
Konfiguration ändern	0x020000
Protokoll lesen	0x040000
Protokollierung verwalten	0x080000
Verzeichnisobjekte importieren	0x100000

ACL für eine Gruppe

Rechte	Werte
Schlüssel erzeugen	0x00000001
Schlüssel kopieren	0x00000002
Schlüssel entfernen	0x00000004
Regeln erzeugen	0x00000008
Zertifikate zuweisen	0x00000010
Benutzer hinzufügen	0x00000020
Benutzer löschen	0x00000040
Gruppe hinzufügen	0x00000080
Untergruppe entfernen	0x00000100
Gruppen verschieben	0x00000200
Eigenschaften ändern	0x00000400
Gruppe löschen	0x00000800
Profile erzeugen	0x00001000
ACL ändern	0x00002000
Lesen	0x00004000
Sichtbar	0x00008000

ACL für SOs

Rechte	Werte
Namen ändern	0x01000000
Zertifikat ändern	0x02000000

Rechte	Werte
Region ändern	0x04000000
Konfiguration zuordnen	0x08000000
SO löschen	0x10000000
Globale Rechte ändern	0x20000000
ACL ändern	0x40000000
Lesen	0x80000000

5.2 Rechte

5.2.1 Globale Rechte

Rechte	Beschreibung
Security Officer anlegen	Der SO hat das Recht, weitere SOs zu erzeugen.
Profile erzeugen	Der SO hat die globale Berechtigung, den Profile Resolver zu starten und Richtliniendateien für einzelne Benutzer zu erzeugen. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung Profile erzeugen für eine spezifische Gruppe für einen SO gesetzt werden kann. *Profile erzeugen* berechtigt den SO zum Erstellen von Profilen für Benutzer, wenn der SO die Berechtigung *Profile erzeugen* für die übergeordnete Gruppe des Benutzers hat Diese Berechtigung ist eine Voraussetzung für das Zuweisen von Werten zu Schlüsseln. Ein Benutzer, der nur die Berechtigung *Schlüssel erzeugen* hat, kann nur Schlüssel ohne Werte erzeugen.
Profile für alle Mitglieder erzeugen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung *Profile erzeugen* gesetzt ist. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung *Profile für alle Mitglieder erzeugen* für eine spezifische Gruppe gesetzt werden kann. *Profile für alle Mitglieder erzeugen* berechtigt einen SO zum Erzeugen von Profilen für alle Benutzer, wenn der SO die Berechtigung *Profile erzeugen* für die übergeordnete Gruppe des Benutzers oder die Berechtigung *Profile für alle Mitglieder erzeugen* für eine der Gruppen, zu denen der Benutzer gehört, hat. **Hinweis:** Da die globale Berechtigung *Profile erzeugen* eine Voraussetzung für *Profile für alle Mitglieder erzeugen* ist, gilt: Wenn Sie die Berechtigung *Profile erzeugen* deaktivieren, wird auch die Berechtigung *Profile für alle Mitglieder erzeugen* deaktiviert. Wenn Sie die Berechtigung *Profile für alle Mitglieder erzeugen* aktivieren, wird automatisch auch die Berechtigung *Profile erzeugen* aktiviert.
Schlüssel erzeugen	Der SO darf Schlüssel in den einzelnen Gruppen erzeugen. Das Recht *Schlüssel erzeugen* alleine erlaubt dem SO nur das Erzeugen von Schlüsseln ohne Wert! In der Administration können Schlüssel ohne Wert Benutzern/Gruppen zugeordnet werden. Der Wert selbst wird erst generiert, wenn der Profile Resolver gestartet wird. Um direkt beim manuellen Anlegen auch den zum Schlüssel gehörenden Wert erzeugen zu können, benötigt der SO das Recht *Profile erzeugen*.

Rechte	Beschreibung
Schlüssel kopieren	Der SO darf Schlüssel kopieren.
Schlüssel entfernen	Der SO darf Schlüssel aus den Gruppen entfernen.
Schlüssel lesen	Der SO darf die Daten zu den einzelnen Schlüsseln der Gruppe sehen.
Zertifikate erzeugen	Der SO darf Zertifikate für die Benutzer erzeugen.
Zertifikate zuweisen	Der SO darf den Benutzern Zertifikate zuweisen. Der SO darf den Assistenten zur Zertifikatszuweisung starten. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung *Zertifikate zuweisen* für eine spezifische Gruppe für einen SO gesetzt werden kann. *Zertifikate zuweisen* berechtigt den SO zum Zuweisen von Zertifikaten zu Benutzern, wenn der SO die Berechtigung *Zertifikate zuweisen* für die übergeordnete Gruppe des Benutzers hat.
Zertifikate allen Mitgliedern zuweisen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung Zertifikate zuweisen gesetzt ist. Diese globale Berechtigung ist die Voraussetzung dafür, dass die Berechtigung *Zertifikate allen Mitgliedern zuweisen* für eine spezifische Gruppe gesetzt werden kann. *Zertifikate allen Mitgliedern zuweisen* berechtigt einen SO zum Zuweisen von Zertifikaten zu Benutzern, wenn der SO die Berechtigung *Zertifikate zuweisen* für die übergeordnete Gruppe des Benutzers oder die Berechtigung *Zertifikate allen Mitgliedern zuweisen* für eine Gruppe, zu der der Benutzer gehört, hat. **Hinweis:** Da die globale Berechtigung *Zertifikate zuweisen* eine Voraussetzung für *Zertifikate allen Mitgliedern zuweisen* ist, gilt: Wenn Sie die Berechtigung *Zertifikate zuweisen* deaktivieren, wird auch die Berechtigung *Zertifikate allen Mitgliedern zuweisen* deaktiviert. Wenn Sie die Berechtigung *Zertifikate allen Mitgliedern zuweisen* aktivieren, wird automatisch die Berechtigung *Zertifikate zuweisen* aktiviert.
Gruppen verwalten	Der SO darf Änderungen in den Gruppen vornehmen: Untergruppen aufnehmen, Gruppen verschieben, Gruppen synchronisieren, Gruppen löschen.

Rechte	Beschreibung
Anmeldung an DB	Der SO darf sich an der conpal LAN Crypt Datenbank anmelden. Dieses Recht ist standardmäßig immer aktiviert. Dieses Recht stellt eine Möglichkeit dar, einem SO ohne großen Aufwand die Möglichkeit zu nehmen, an der Datenbank Veränderungen vorzunehmen (z. B. wenn er das Unternehmen verlässt). Personen, die ausschließlich Vier-Augen-Aktionen autorisieren dürfen, kann dieses Recht verweigert werden. Damit ist sichergestellt, dass sie neben der Autorisierung von Vier-Augen-Aktionen, keine Möglichkeit haben, Änderungen in conpal LAN Crypt vorzunehmen.
Operationen autorisieren	Der SO darf an Vier-Augen-Aktionen teilnehmen.
Benutzer verwalten	Der SO darf Benutzer in eine Gruppe aufnehmen/entfernen und Gruppen synchronisieren.
Benutzer kopieren	Der SO darf Benutzer zu Gruppen hinzufügen (kopieren). Diese globale Berechtigung ist eine Voraussetzung für das Setzen der Berechtigung Benutzer kopieren für eine spezifische Gruppe für einen SO. Um einen Benutzer zu einer Gruppe hinzuzufügen, muss der Benutzer die Berechtigung Benutzer kopieren für die übergeordnete Gruppe des Benutzers haben.
Regeln erzeugen	Der SO darf Verschlüsselungsregeln erzeugen.
Globale Rechte ändern	Der SO darf die globalen Rechte eines anderen SOs ändern.
ACL ändern	Der SO darf die ACL einer Gruppe ändern.
Spezifische Schlüssel verwenden	Der SO darf bestimmte konkrete Schlüssel in Verschlüsselungsregeln verwenden und bestimmte Schlüssel in *Alle conpal LAN Crypt Schlüssel* anzeigen lassen.
Konfiguration ändern	Der SO darf die Konfiguration (die Pfade) ändern. Dieses Recht ist die Voraussetzung dafür, dass die Seite Konfiguration in den zentralen Einstellungen angezeigt wird, und die Seite Verzeichnisse bearbeitbar ist, wenn dieser SO an die Datenbank angemeldet ist.
Protokoll lesen	Für den SO sind die Einstellungen für die Protokollierung und die Einträge in das Protokoll sichtbar.
Protokollierung verwalten	Der SO darf die Einstellungen für die Protokollierung ändern. Er ist berechtigt, die Einträge zu archivieren, zu löschen und zu prüfen.

Rechte	Beschreibung
Verzeichnisobjekte importieren	Der SO darf OUs, Gruppen und Benutzer aus einem Verzeichnisdienst importieren und in die conpal LAN Crypt Datenbank übertragen. Dieses Recht bedingt, dass der SO die Rechte *Gruppen verwalten* und *Benutzer verwalten* besitzt. Sie werden automatisch gesetzt, wenn das Recht *Verzeichnisobjekte importieren* ausgewählt wird. Besitzt ein SO dieses Recht nicht, ist der Knoten *Verzeichnis-Objekte*, der das Importieren von OUs, Gruppen und Benutzern ermöglicht, in der Administration nicht sichtbar.

5.2.2 Rechte zum Bearbeiten der Einstellungen für einen Security Officer

Rechte	Beschreibung
Namen ändern	Ermöglicht die Änderung des Namens des SOs, dem der Inhaber des Rechts zugeteilt wird.
Zertifikat ändern	Ermöglicht die Änderung des Zertifikats des SOs, dem der Inhaber des Rechts zugeteilt wird.
Region ändern	Ermöglicht die Änderung des Regions-Prefix des SOs, dem der Inhaber des Rechts zugeteilt wird.
Konfiguration zuordnen	Ermöglicht die Änderung der Konfiguration (bearbeiten der Pfade und zuordnen) des SOs, dem der Inhaber dieses Rechts zugeordnet ist.
SO löschen	Ermöglicht das Löschen des SOs, dem der Inhaber des Rechts zugeteilt wird.
Globale Rechte ändern	Ermöglicht die Änderung der globalen Rechte des SOs, dem der Inhaber des Rechts zugeteilt wird.
ACL ändern	Ermöglicht die Änderung der ACL des SOs, dem der Inhaber des Rechts zugeteilt wird.
Lesen	Zeigt den SO, dem der Inhaber des Rechts zugeteilt wird unter *Zentrale Einstellungen/Security Officer Administration* an. Dies ist die Voraussetzung für alle Rechte, die eine Bearbeitung dieses SO erlauben. Wird automatisch gesetzt, wenn ein derartiges Recht ausgewählt wird.

5.2.3 Rechte zur Bearbeitung von Gruppen

Rechte	Beschreibung
Schlüssel erzeugen	Der SO darf Schlüssel in der Gruppe erzeugen.
Schlüssel kopieren	Der SO darf Schlüssel kopieren.
Schlüssel entfernen	Der SO darf Schlüssel entfernen.
Regeln erzeugen	Der SO darf Verschlüsselungsregeln erzeugen.
Zertifikate zuweisen	Der SO darf den Benutzern Zertifikate zuweisen. Der SO ist dazu berechtigt, den Assistenten für das Zuweisen von Zertifikaten auszuführen. Diese Berechtigung erlaubt es dem SO, den Benutzern in der Gruppe Zertifikate zuzuweisen, wenn die Gruppe auch die übergeordnete Gruppe ist.
Zertifikate allen Mitgliedern zuweisen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung *Zertifikate zuweisen* gesetzt ist. *Zertifikate allen Mitgliedern zuweisen* berechtigt einen SO zum Zuweisen von Zertifikaten zu Benutzern, wenn der SO die Berechtigung *Zertifikate zuweisen* für die übergeordnete Gruppe des Benutzers oder die Berechtigung *Zertifikate allen Mitgliedern zuweisen* für eine Gruppe, zu der der Benutzer gehört, hat. **Hinweis:** Da die globale Berechtigung *Zertifikate zuweisen* eine Voraussetzung für *Zertifikate allen Mitgliedern zuweisen* ist, gilt: Wenn Sie die Berechtigung *Zertifikate zuweisen* deaktivieren, wird auch die Berechtigung *Zertifikate allen Mitgliedern zuweisen* deaktiviert.
Benutzer hinzufügen	Der SO darf manuell Benutzer zur Gruppe hinzufügen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Benutzer kopieren	Der SO darf Benutzer zu Gruppen hinzufügen (kopieren). Dies ist nur denjenigen Mitgliedern erlaubt, für die diese Gruppe auch das übergeordnete Objekt ist.

Rechte	Beschreibung
Benutzer löschen	Der SO darf Benutzer über das Snap-In *Mitglieder und Zertifikate für Gruppe* löschen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Gruppe hinzufügen	Der SO darf über das Kontextmenü einer Gruppe neue Gruppen hinzufügen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Untergruppe entfernen	Der SO darf Untergruppen dieser Gruppe entfernen. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Gruppen verschieben	Der SO darf manuell angelegte Gruppen in der Administration (mit Drag and Drop) verschieben. Importierte Gruppen können nicht verschoben werden. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Eigenschaften ändern	Der SO darf die Eigenschaften der Gruppe ändern
Gruppe löschen	Der SO darf Gruppen löschen. Dies setzt voraus, dass er in der übergeordneten Gruppe das Recht Untergruppe entfernen hat. Dieses Recht ist eine Voraussetzung für das Importieren/Synchronisieren von Gruppen und Benutzern.
Profile erzeugen	Der SO darf den Profile Resolver starten und Richtliniendateien für ausgewählte Benutzer erstellen. *Profile erzeugen* berechtigt den SO, Profile für Benutzer zu erstellen, für die die Gruppe auch die übergeordnete Gruppe ist.

Rechte	Beschreibung
Profile für alle Mitglieder erzeugen	Für diese Berechtigung ist es erforderlich, dass die Berechtigung *Profile erzeugen* gesetzt ist. *Profile für alle Mitglieder erzeugen* berechtigt den SO dazu, Profile für alle Benutzer in der Gruppe zu erzeugen: Benutzer, für die die Gruppe auch die übergeordnete Gruppe ist, und Benutzer, die Mitglieder der Gruppe sind, jedoch eine andere übergeordnete Gruppe haben. **Hinweis:** Wenn Sie *Profile für alle Mitglieder erzeugen* auf **Zulassen** setzen, wird die Berechtigung *Profile erzeugen* automatisch auf **Zulassen** gesetzt. Wenn Sie *Profile erzeugen* auf **Verweigern** setzen, wird die Berechtigung *Profile für alle Mitglieder erzeugen* automatisch auf **Verweigern** gesetzt.
ACL ändern	Der SO darf die ACL dieser Gruppe ändern (z. B. einen anderen SO hinzufügen).
Lesen	Der SO hat Leserechte an dieser Gruppe, er kann den Inhalt der Snap-Ins sehen. Wird automatisch gesetzt, wenn Bearbeitungsrechte vergeben werden.
Sichtbar	Die Gruppe ist für den SO sichtbar. Wird am Basisknoten gesetzt und nach unten vererbt. Wird es dem SO verweigert, wird die Gruppe ausgeblendet (auch Lesen muss verweigert sein).

6 Rechtlicher Hinweis

7 Technischer Support

Technischen Support zu conpal Produkten können Sie wie folgt abrufen:

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

• Die Dokumentation zu LAN Crypt Client erhalten Sie zum Herunterladen
in deutscher Sprache: https://docs.lancrypt.com/de/client/sglc_397_hdeu.pdf
in englischer Sprache: https://docs.lancrypt.com/en/client/sglc_397_heng.pdf
in französisch: https://docs.lancrypt.com/fr/client/sglc_397_hfra.pdf

• Die Dokumentation zu LAN Crypt Admin erhalten Sie zum Herunterladen
in deutscher Sprache: https://docs.lancrypt.com/de/admin/sglc_397_ahdeu.pdf
in englischer Sprache: https://docs.lancrypt.com/en/admin/sglc_397_aheng.pdf
in französisch: https://docs.lancrypt.com/fr/admin/sglc_397_ahfra.pdf

• 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 Wortlautvon Fehlermeldungen an.