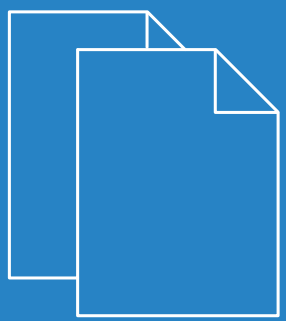
SICHER. **VERNETZT.**

LCOS FX 10.7

Addendum



11/2021

LANCOM Systems

Inhalt

Copyright

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Addendum zur LCOS FX-Version 10.7

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS FX-Version 10.7 gegenüber der vorherigen Version.

2 Netmap

Ab LCOS FX-Version 10.7 können Sie für ganze Netzwerke SNAT- und DNAT-Einstellungen vornehmen. Die bisherige Möglichkeit des NAT für einzelne Dienste ist natürlich weiterhin verfügbar.

Dazu wurde im Verbindungsdialog ein neuer Tab **NAT** hinzugefügt:

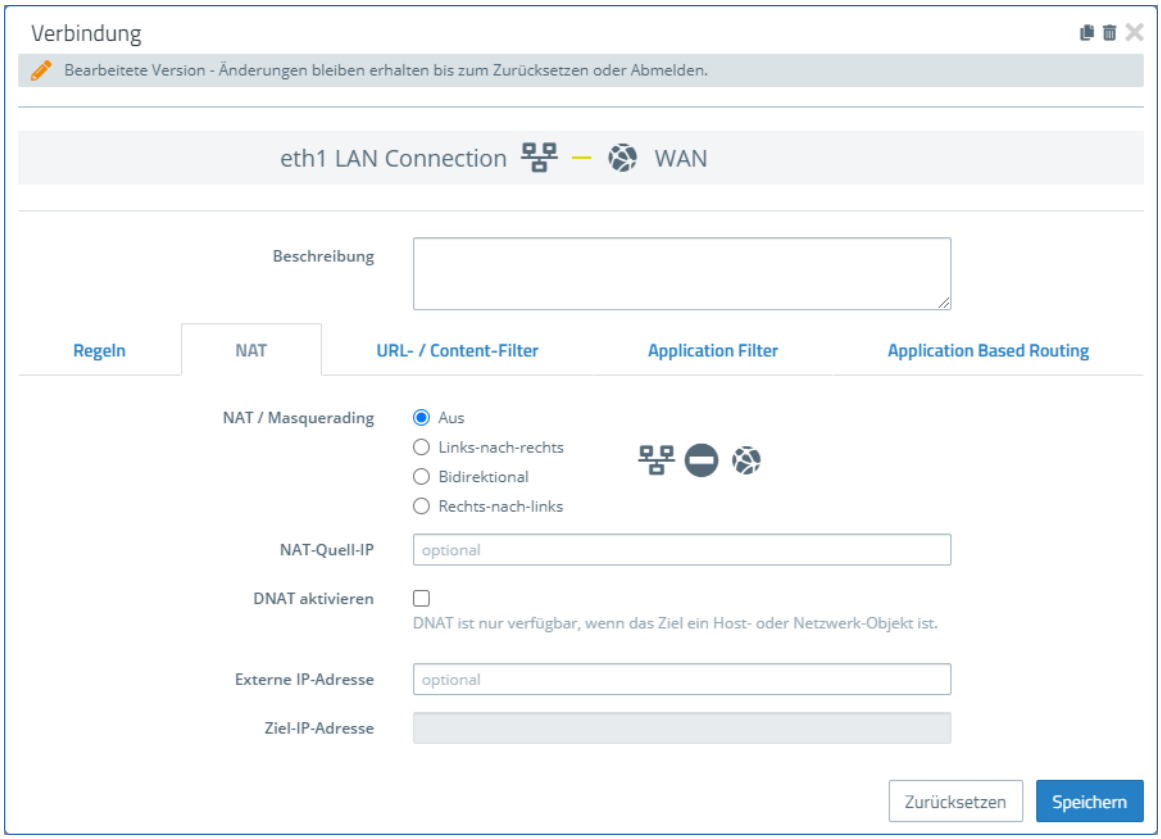


Abbildung 1: Verbindungsdialog > NAT

Im Tab **NAT** können Sie für ganze Netzwerke SNAT- und DNAT-Einstellungen konfigurieren. Die Einstellungen entsprechen dabei den Einstellungen für einzelne Services mit Ausnahme des Ziel-Ports, der bei den NAT-Einstellungen der Verbindung entfällt.

Eingabefeld	Beschreibung
NAT / Masquerading	Geben Sie für NAT / Masquerading die gewünschte Richtung an (**Bidirektional**, **Links-nach-rechts** oder **Rechts-nach-links**) oder deaktivieren Sie (**Aus**) die Funktion für diese Regel, indem Sie die entsprechende Optionsschaltfläche auswählen. Die Standardeinstellung hängt von den für die Verbindung ausgewählten Quell- und Zielobjekten ab.
NAT-Quell-IP	Optional: Wenn Sie mehrere ausgehende IP-Adressen haben, geben Sie die IP-Adresse an, die für Source-NAT verwendet werden soll. Wenn Sie keine IP-Adresse angeben, wählt das System automatisch die Haupt-IP-Adresse des ausgehenden Interface aus. Wenn ein verbundenes Objekt ein Netzwerk ist, können Sie hier auch ein Netzwerk eintragen unter der Voraussetzung, dass das eingetragene Netz dieselbe Größe hat wie das Netzwerk des Objektes.

Eingabefeld	Beschreibung
DNAT aktivieren	Ist ein einzelnes Host- oder Netzwerk-Objekt das Ziel, können Sie den Haken in diesem Kontrollkästchen setzen, um DNAT zu aktivieren.
Externe IP-Adresse	Optional: Geben Sie die Ziel-IP-Adresse des zu bearbeitenden Datenverkehrs an. DNAT wird nur auf diesen Datenverkehr angewandt. Diese IP-Adresse muss eine der IP-Adressen der Firewall sein. Wenn ein verbundenes Objekt ein Netzwerk ist, können Sie hier auch ein Netzwerk eintragen unter der Voraussetzung, dass das eingetragene Netz dieselbe Größe hat wie das Netzwerk des Objektes.
Ziel-IP-Adresse	Optional: Geben Sie die Ziel-IP-Adresse des zu bearbeitenden Datenverkehrs an.

Im Tab **Regeln** wurde eine zusätzliche Spalte **NAT der Verbind.** hinzugefügt, um den Wechsel der NAT-Einstellungen von verbindungsbasiert auf servicebasiert und umgekehrt zu erleichtern. Standardmäßig ist bei neu hinzugefügten Services die Option zur Verwendung der NAT-Einstellungen der Verbindung aktiviert. Wenn Sie die im Folgenden beschriebenen Service-spezifischen Einstellungen verwenden wollen, dann müssen Sie hier den Haken entfernen.

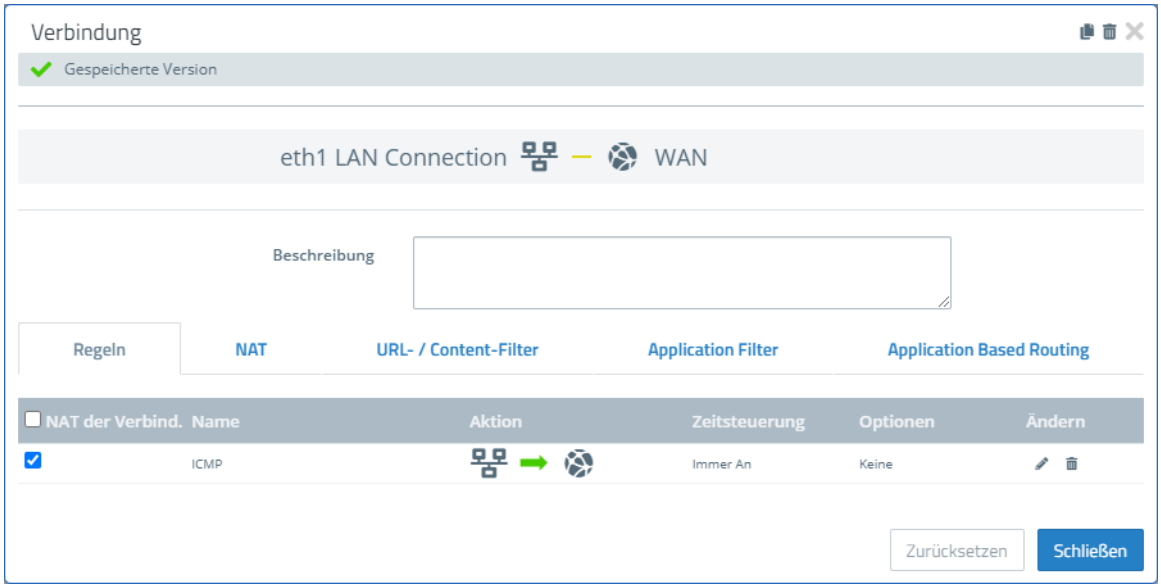


Abbildung 2: Verbindungsdialog > Regeln

Um die von früher bekannten Service-spezifischen Einstellungen zu erhalten, müssen Sie die Regel bearbeiten und dann im Dialog auf dem Tab **Erweitert** von der Option **Verbindungs-Einstellungen verwenden** auf

Servicespezifische-Einstellungen verwenden umstellen. Dadurch werden die bekannten Einstellungen wieder zur Bearbeitung eingeblendet:

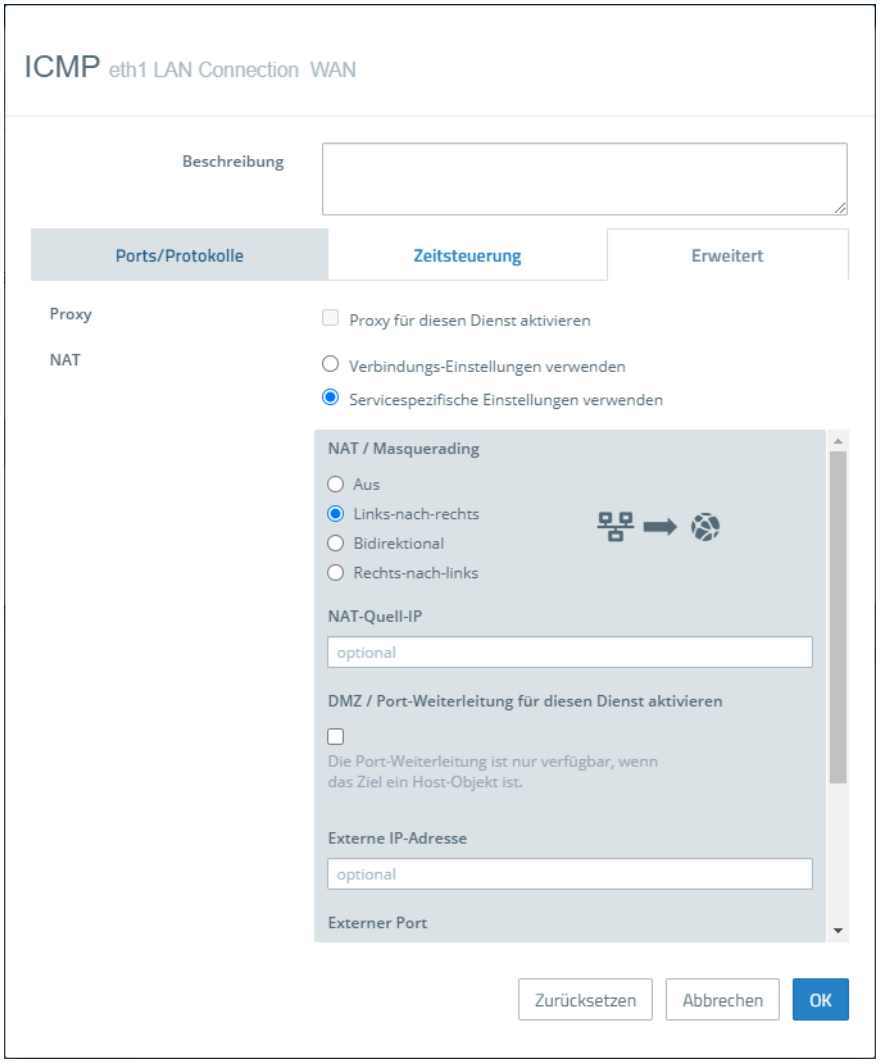


Abbildung 3: Servicedialog > Erweitert

3 Zertifikatsverwaltung

Ab LCOS FX-Version 10.7 wurde die **Zertifikatsverwaltung** überarbeitet, so dass sich u. a. die Menüstruktur unter dem Punkt Zertifikatsverwaltung geändert hat. Die Punkte **Zertifikate** und **Vorlagen** sind mit erweiterter Funktionalität geblieben, die **Vertrauenswürdige CAs** wurden erweitert um **Nicht vertrauenswürdige CAs**. Der Punkt **OCSP/CRL** wurde komplett entfernt. Die Zertifikats-Requests werden nun unter dem Punkt **Zertifikate** erstellt.

Abbildung 4: Menü Zertifikatsverwaltung

Im Folgenden eine komplette Beschreibung des überarbeiteten Bereichs, ggf. mit Hinweisen auf geänderte bzw. weggefallene Funktionalitäten.

3.1 Zertifikate

Mit den Einstellungen unter **Zertifikate** können Sie die Zertifikate verwalten, die der LANCOM R&S®Unified Firewall-Webclient, der integrierte SSL-Proxy und der OpenVPN-Server nutzen.

Um verschlüsselte Verbindungen abzusichern, nutzt Ihre LANCOM R&S®Unified Firewall digitale Zertifikate, wie im X.509-Standard beschrieben.

Die LANCOM R&S®Unified Firewall selbst agiert als Zertifizierungsstelle (Certification Authority). Daher ist ein so genanntes CA-Zertifikat erforderlich. Um die Verwaltung der Zertifikate zu zentralisieren, ist es empfehlenswert, ein CA-Zertifikat in einer zentralen Firewall zu erstellen und es direkt für die Signatur aller für die Anwendung genutzten Zertifikate zu verwenden. Dies wird als einstufige Zertifizierungskette bezeichnet.

Alle Zertifikate für Anwendungen müssen von der zentralen Firewall signiert werden. Wenn ein Zertifikat für eine andere Firewall benötigt wird, müssen Sie darauf eine Anforderung erstellen. Diese Anforderung muss von der zentralen Firewall signiert werden. Die signierte Anforderung, die Sie erstellt haben, muss von den anderen Firewalls importiert werden, um genutzt werden zu können.

Um die anderen Firewalls dazu zu befähigen, Zertifikate zu erstellen, die zwar hauptsächlich lokalen Zwecken dienen, aber dennoch in Ihrer gesamten Organisation als gültig anerkannt werden, können Sie mehrstufige Zertifizierungsketten einsetzen. Dafür benötigen Sie in Ihrer zentralen Firewall ein so genanntes Root-CA-Zertifikat, mit dem Sie die untergeordneten CA-Zertifikate signieren können. Sie müssen für diese untergeordneten CA-Zertifikate Anforderungen auf Ihren anderen Firewalls erstellen. Nachdem Sie die signierten CA-Zertifikate importiert haben, sind die anderen Firewalls selbst in der Lage, Zertifikate für Anwendungen zu signieren. Um diese Hierarchien übersichtlich darzustellen, zeigt die LANCOM R&S®Unified Firewall sie in einer Baumansicht.

3.1.1 Übersicht Zertifikate

Navigieren Sie zu **Zertifikatsverwaltung** > **Zertifikate**, um die Liste der derzeit im System angelegten Zertifikate in einem Baumdiagramm nach Zertifizierungsstellen im rechten Bereich anzuzeigen.

Mit den Schaltflächen oberhalb der Liste können Sie Äste ein bzw. ausklappen, ein Zertifikat aus einer Datei importieren (➔]) bzw. eine Zertifikatsignierungsanforderung signieren oder ein neues Zertifikat erstellen.

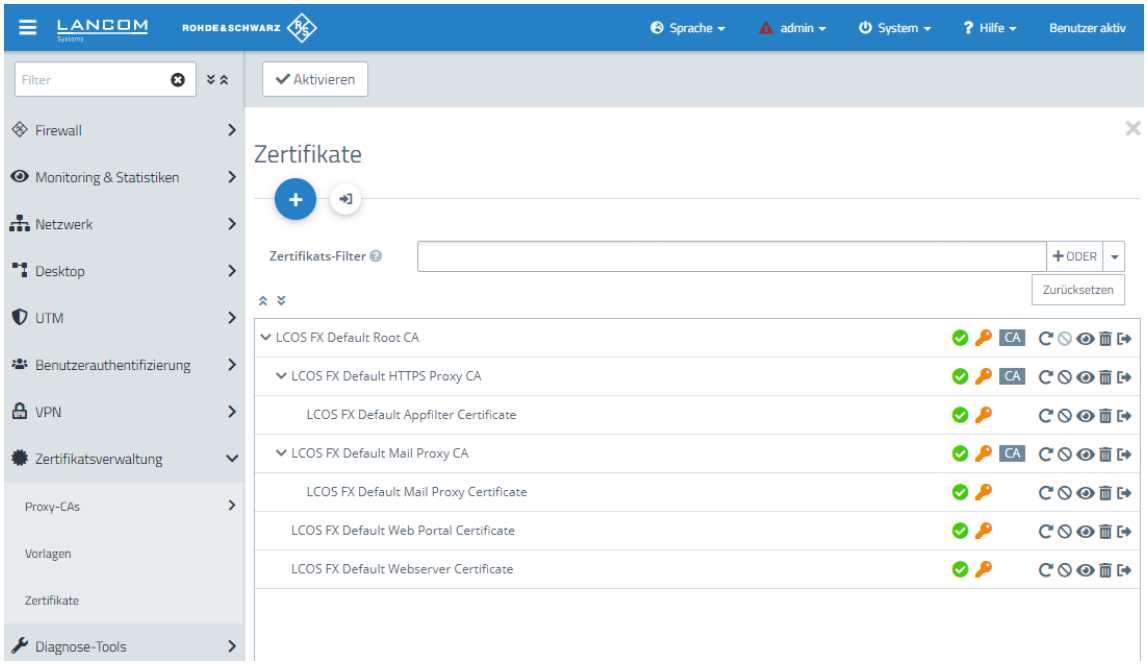


Abbildung 5: Ansicht Zertifikatsverwaltung > Zertifikate

Nach dem ersten Hochfahren und nach einer erneuten Installation werden die folgenden Zertifikate standardmäßig, teilweise allerdings erst nach Auswahl im Setup-Assistent, angelegt:

Tabelle 1: Bereits angelegte Zertifikate

Name des Zertifikats	Beschreibung
LCOS FX Default Root CA	Oberste Zertifizierungsstelle zur Erstellung von untergeordneten Zertifizierungsstellen und Zertifikaten.
LCOS FX Default HTTPS Proxy CA	Zertifizierungsstelle zur Erstellung von untergeordneten Zertifikaten zur Verwendung durch den HTTPS Proxy.
LCOS FX Default Appfilter Certificate	Vorkonfiguriertes Zertifikat für das Application Management.
LCOS FX Default Mail Proxy CA	Zertifizierungsstelle zur Erstellung von untergeordneten Zertifikaten zur Verwendung durch den Mailproxy.
LCOS FX Default Mail Proxy Certificate	Vorkonfiguriertes Zertifikat für den Mailproxy.
LCOS FX Default Web Portal Certificate	Vorkonfiguriertes Zertifikat für das Web Portal.
LCOS FX Default Webserver Certificate	Vorkonfiguriertes Zertifikat für den Webserver.

In der Liste werden der Name des jeweiligen Zertifikats und durch die Baumstruktur auch dessen Abhängigkeiten angezeigt. Die Schaltflächen hinter den jeweiligen Zertifikaten zeigen den Gültigkeitsstatus:

- – Zertifikat ist gültig
- – Zertifikat läuft in 8 bis 30 Tagen ab
- – Zertifikat läuft in einem bis 7 Tagen ab
- – Zertifikat ist abgelaufen
- – Zertifikat wurde revoziert
- – Zertifikat wurde ersetzt

Zudem wird angezeigt, ob ein privater Schlüssel für das Zertifikat vorhanden ist () und über ein „CA“, ob das Zertifikat eine Zertifizierungsstelle ist. Außerdem können Sie mithilfe der Schaltflächen Details zu jedem Zertifikat anzeigen lassen (), ein Zertifikat exportieren (), die Gültigkeit eines Zertifikats temporär aussetzen oder erneuern (), das Zertifikat revozieren () und das Zertifikat oder nur den zugehörigen privaten Schlüssel löschen ().

Zertifikatsansicht filtern

Ab LCOS FX-Version 10.7 wurde der bisherige einfache Textfilter durch einen Filter ersetzt, wie Sie ihn bereits vom Alarmprotokoll kennen.

Sie können die Zertifikatsansicht mithilfe der Filterfunktion im Eingabefeld **Zertifikats-Filter** um verschiedene Suchkriterien und -optionen eingrenzen.

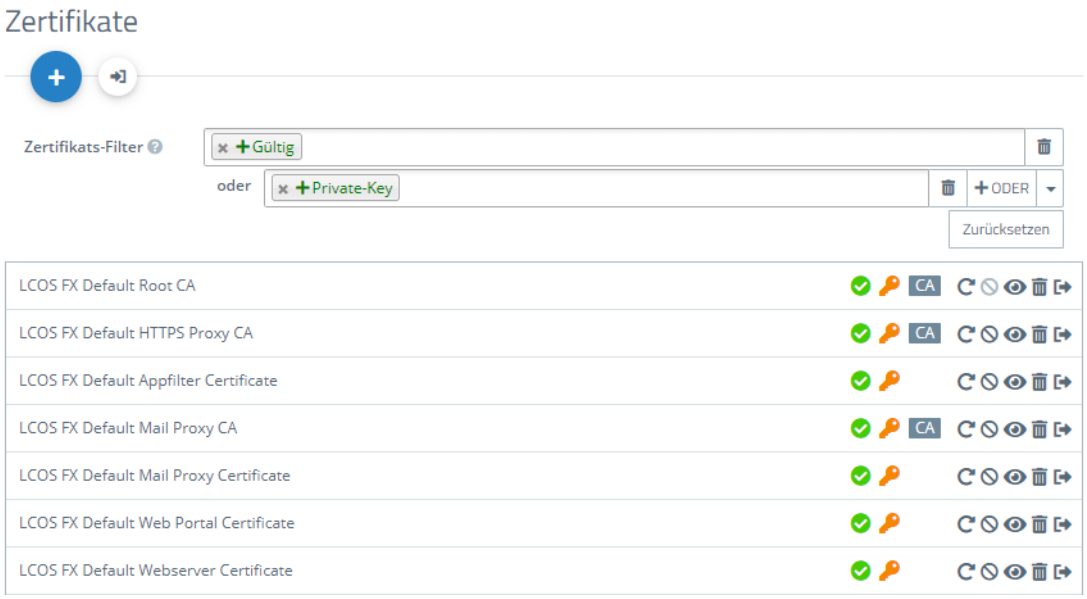


Abbildung 6: Zertifikate mit angewandtem Filter

Um einen Filter zu erstellen, gehen Sie wie folgt vor:

1. Klicken Sie in das Eingabefeld.

   Der Webclient zeigt Filtervorschläge an.

2. Wählen Sie einen der vorgeschlagenen Filter aus der Drop-down-Liste aus oder geben Sie einen beliebigen Suchtext ein, um weitere Vorschläge zu erhalten. Vordefinierte Filter sind:

   - Status
     - Gültige Zertifikate
     - Abgelaufene Zertifikate
     - Revozierte Zertifikate
     - Weniger als eine Woche gültige Zertifikate

- Weniger als einen Monat gültige Zertifikate
- Noch nicht gültige Zertifikate

- Eigenschaft
  - Mit Private-Key
  - Ist eine Certificate Authority
  - Ist ein Request
  - Wurde mit Hilfe eines der folgenden Schlüssel-Algorithem generiert: RSA, NIST Curves, ED448, ED25519
  - NIST-Kurventypen: secp224r1, secp256r1, secp384r1, secp521r1, secp256k1
  - Schlüsselgröße: 1024, 1536, 2048, 3072, 4096, 6144 und 8192
  - Schlüsselverwendung: Inhaltsverpflichtung, CRL-Signierung, Datenverschlüsselung, Nur Entschlüsselung, Digitale Signatur, Nur Verschlüsselung, Schlüsselvereinbarung, Schlüsselzertifikats-Signierung, Schlüsselverschlüsselung
  - Erweiterte Schlüsselverwendung: Beliebige erweiterte Schlüsselverwendung, Client-Authentifizierung, Code-Signierung, E-Mail-Schutz, OCSP-Signierung, Server-Authentifizierung, Zeitstempel
  - Hash-Algorithmen: sha1, sha224, sha256, sha384, sha512
  - Revozierungsgründe: Nicht spezifiziert, Schlüssel gefährdet, CA gefährdet, Zugehörigkeit geändert, Ersetzt, Geschäftsaufgabe, Recht entzogen, Attribut-Authorität gefährdet

Sobald ein Text eingegeben wird, werden weitere Filter-Eigenschaften angeboten:

- Text
  - Common Name enthält eingegebenen Text
  - Subjekt enthält eingegebenen Text
  - Subjekt des Ausstellers enthält eingegeben Text
- Hexadezimal-Notation (Bindestriche und Doppelpunkte werden ignoriert, d. h. Sie können z. B. „dddd“ eingeben und sowohl „dd-dd“ als auch „dd:dd“ werden als gültig angesehen)
  - Fingerabdruck enthält eingegebenen Text
  - Signatur enthält eingegebenen Text

Für jeden Vorschlag können Sie auswählen, ob dieser als Inklusionsfilter (+ / UND-Verknüpfung) oder Exklusionsfilter (⊘ / UND-NICHT-Verknüpfung) verwendet werden soll.

Nach der Auswahl wird der Filtervorschlag als Suchkriterium in das Eingabefeld eingefügt.

Die Liste der Zertifikate passt sich an die Suchabfrage an.

Wiederholen Sie die obigen Schritte, bis Sie die gewünschten Filterkriterien zu Ihrer Suchanfrage hinzugefügt haben.

Es werden nur Einträge angezeigt, die mit allen Filterkriterien übereinstimmen.

Um ein Filterkriterium in einer Suchabfrage zu löschen, klicken Sie auf ✖.

Sie können mehrere Zeilen zu Ihrer Suchanfrage hinzufügen, indem Sie neben dem Eingabefeld auf **+ ODER** klicken. Sie können wählen, ob Sie eine neue leere Zeile einfügen, oder die zuletzt angelegte Zeile kopieren möchten. Jede Zeile ist in sich eine eigene Suchabfrage, die mit den anderen Zeilen ODER-verknüpft wird.

Löschen Sie die Zeile, indem Sie neben der Zeile auf 🗑 klicken.

Zertifikat oder Zertifikats-Request erstellen

Mit der Plus-Schaltfläche ⊕ oberhalb der Liste mit den Elementen können Sie neue Zertifikate und Signierungsanfragen erzeugen. Für die Erstellung können Sie die folgenden Elemente konfigurieren:

Eingabefeld	Beschreibung
Zertifikatstyp	Wählen Sie zwischen den Optionen **Zertifikat** zur Erstellung eines Zertifikats bzw. einer Zertifizierungsstelle (CA) und einem **Zertifikats-Request**. Mit letzterem erstellen Sie eine Zertifizierungsanfrage für ein Zertifikat oder eine untergeordnete CA, welches dann von einer übergeordneten CA signiert werden muss, damit es gültig wird. Bei Auswahl der Option **Zertifikats-Request** können weder **Gültigkeit** noch die **Signierende CA** ausgewählt werden, da diese bei der Signierung des Zertifikats festgelegt werden. Der erstellte Request erscheint in dem Zertifikatsbaum im Anschluss an die Zertifikate in einem gesonderten Zweig **Ausstehende Zertifikatssignierungsanforderungen**.
Common Name (CN)	Legen Sie einen Namen für das Zertifikat fest.
Private-Key-Passwort	Obligatorisch: Geben Sie ein Passwort ein, um den privaten Schlüssel abzusichern.
Passwort anzeigen	Optional: Setzen Sie den Haken im Kontrollkästchen, um das Passwort zur Überprüfung anzuzeigen.
Gültigkeit	Legen Sie den anfänglichen Zeitraum fest, für den das Zertifikat gültig sein soll. Die Eingabefelder sind bereits mit dem aktuellen Datum als Erstellungsdatum und dem gleichen Tag ein Jahr später im Falle eines Zertifikats bzw. 5 Jahre später bei einer Certificate Authority als Ablaufdatum ausgefüllt. Um einen anderen Zeitraum festzulegen, wählen Sie eine der vorgegebenen Optionen aus oder selektieren Sie im angezeigten Kalender das Start- und Enddatum. Das Start- und Enddatum wird in folgendem Format angezeigt: MM/DD/JJJJ - MM/DD/JJJJ (z. B. `04/18/2021 - 04/18/2031`).
Vorlage	Optional: Wählen Sie eine der unter *Vorlagen* auf Seite 16 vorhandenen Vorlagen aus, um die Felder im Bereich „Optionen“ und „Subject und SAN“ aus der Vorlage zu übernehmen. Bei Auswahl einer Vorlage werden bereits vorgenommene Einstellungen überschrieben!
Signierende CA	Wählen Sie die signierende CA aus.
CA-Passwort	Wenn eine CA ausgewählt ist, ist dieses Feld obligatorisch, es sei denn, es handelt sich um eine der in *Tabelle 1: Bereits angelegte Zertifikate* auf Seite 9 aufgeführten LCOS FX CAs. Geben Sie ein Passwort für den privaten Schlüssel der signierenden Zertifizierungsstelle ein. Das Passwort ist notwendig, da die Signatur des öffentlichen Schlüssels für das neue Zertifikat mit dem privaten Schlüssel der signierenden Zertifizierungsstelle erfolgt.
Zeige CA-Passwort	Optional: Setzen Sie den Haken im Kontrollkästchen, um das Passwort zur Überprüfung anzuzeigen.
Certificate Authority	Diese Option bestimmt, ob das zu erstellende Zertifikat als Zertifizierungsstelle auch andere Zertifikate signieren kann oder nicht. **Vorsicht**: Die Standard-Gültigkeitsdauern für Zertifikate (1 Jahr) und Certificate Authorities (5 Jahre) unterscheiden sich. Bei Änderung dieser Eigenschaft wird die Gültigkeitsdauer angepasst.
Pfad-Länge	Nur bei Auswahl von **Certificate Authority** vorhanden. Hier bestimmen Sie, wie viele Sub-CA-Ebenen mit dieser CA erzeugt werden können. Bei einem Wert von 0 können keine Sub-CAs mit dieser CA signiert werden, d. h. nur noch „normale“ Zertifikate können mit dieser CA signiert werden. Wenn das Feld leer bleibt, gibt es keine Begrenzung.
Schlüsselverwendung	Hier können Sie nach einem Klick in das Feld vordefinierte Eigenschaftswerte aus einer Liste hinzufügen wie z. B. Datenverschlüsselung.
Verschlüsselungs-Algorithmus	Der Algorithmus „DSA“ wurde ab LCOS FX-Version 10.7 entfernt. Dafür wurden mit „NIST Curves“, „ed448“ und „ed25519“ Elliptic Curve-Verfahren hinzugefügt.

Eingabefeld	Beschreibung
	Wählen Sie aus der Liste der Algorithmen den von Ihnen gewünschten aus. Bei Auswahl der Option „NIST Curves“ muss in dem Feld **Kurve** die Art der NIST-Kurve gewählt werden.
Kurve	Falls Sie unter **Verschlüsselungs-Algorithmus** die Option „NIST Curves“ ausgewählt haben, dann können Sie hier die Art der NIST-Kurve auswählen.
Schlüssel-Größe	Falls Sie unter **Verschlüsselungs-Algorithmus** die Option „RSA“ ausgewählt haben, dann können Sie hier die Schlüsselgröße auswählen.
Hash-Algorithmus	Wählen Sie einen der vorgegebenen Hash-Algorithmen aus.
Erweiterte Schlüsselverwendung	Hier können Sie nach einem Klick in das Feld weitere vordefinierte Eigenschaftswerte aus einer Liste hinzufügen wie z. B. Zeitstempel.
Subjekt	Optional: Wählen Sie eine beliebige Anzahl an Subjekten wie z. B. **Land (C)**, **Bundesland (ST)**, **Organisation (O)**, oder **Abteilung (OU)** aus der Drop-down-Liste aus und geben Sie den dazu gewünschten Inhalt in das Eingabefeld rechts daneben ein. Klicken Sie rechts auf ⊕, um einen Eintrag zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Wenn Sie ein **Subjekt** bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.
Subject Alternative Name (SAN)	Optional: Geben Sie eine beliebige Anzahl benutzerdefinierter alternativer Namen für bestimmte Nutzungszwecke ein und wählen Sie die entsprechenden Typen aus der Drop-down-Liste aus. Die folgenden Typen stehen zur Verfügung: `E-Mail`, `DNS`, `DirName`, `URI`, `IP` und `RegID`. Klicken Sie rechts auf ⊕, um einen Subject Alternative Name (SAN) zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Wenn Sie einen **Subject Alternative Name (SAN)** bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie ein neues Zertifikat erstellen und zu der Liste der verfügbaren Zertifikate hinzufügen oder die Erstellung eines neuen Zertifikats abbrechen (**Abbrechen**).

Zertifikat importieren oder Certificate Signing Request signieren

Mit der Schaltfläche oberhalb der Liste können Sie ein Zertifikat aus einer Datei importieren bzw. einen Certificate Signing Request signieren.

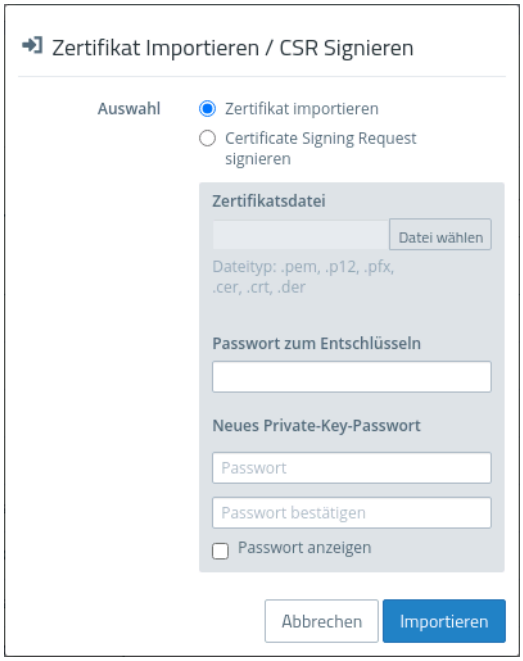


Abbildung 7: Zertifikat importieren / Certificate Signing Request signieren

Über die Auswahl im oberen Bereich entscheiden Sie, ob Sie ein Zertifikat importieren oder einen Certificate Signing Request signieren wollen.

Für den Import können Zertifikatsdateien mit verschiedenen Datei-Endungen ausgewählt werden (*.pem, *.p12, *.pfx, *.cer, *.crt, *.der). Je nachdem, ob in der Datei ein privater Schlüssel vorhanden ist, muss ein Passwort zum Entschlüsseln und ein Passwort zum Wiederverschlüsseln des privaten Schlüssels eingegeben werden. Optional können Sie sich das Passwort anzeigen lassen.

Im Falle einer Zertifikatssignierungsanforderung wählen Sie die zugehörige Datei aus. In Frage kommen die folgenden Dateitypen: *.pem, *.crt, *.cer, *.der. Es muss eine signierende CA ausgewählt und das dazugehörige Passwort eingegeben werden. Zudem muss der Gültigkeitszeitraum gewählt werden. Sobald das Zertifikat erfolgreich signiert wurde, wird das signierte Zertifikat als PEM zum Download angeboten.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie die ausgewählte Zertifikatsdatei importieren und zu der Liste der verfügbaren Zertifikate hinzufügen bzw. den Certificate Signing Request signieren oder den Dialog abbrechen (**Abbrechen**).

Zertifikat erneuern

Mit der Schaltfläche bei einem Zertifikat in der Liste wird ein neues Zertifikat mit einem neuen Gültigkeitszeitraum erstellt.

Im Falle eines einfachen Zertifikats wählen Sie unter **Gültigkeit** den neuen Zeitraum und geben das **CA-Passwort** des zugehörigen CA-Zertifikats ein. Bei nicht selbstsignierten Zertifikaten kann bei der Erneuerung eine komplett andere CA gewählt werden. Es ist nicht beschränkt auf die gegenwärtige CA. Bei nicht selbstsignierten Zertifikaten müssen zwei Passwörter eingegeben werden; das CA-Passwort und das Private-Key-Passwort des zu erneuernden Zertifikats.

Bei einer Certificate Authority (CA) können Sie zusätzlich den Common Name ändern und den von dieser CA signierten Zertifikaten einen neuen Gültigkeitszeitraum zuweisen.

Abgeleitete Sub-CAs und Zertifikate müssen manuell erneuert werden.

Die zu erneuernden Zertifikate werden nicht mehr automatisch revoziert. Optional können Sie das Revozieren im Anschluss an die Erneuerung durchführen.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie den Gültigkeitszeitraum des ausgewählten Zertifikats bzw. der CA und ggf. den von dieser signierten Zertifikaten erneuern oder den Dialog abbrechen (**Abbrechen**).

Zertifikat revozieren

Mit der Schaltfläche ⃠ bei einem Zertifikat in der Liste können Sie dieses revozieren. Dazu müssen Sie einen Grund auswählen und das Passwort des privaten Schlüssels der übergeordneten CA des Zertifikats eingeben.

Zertifikate können nicht revoziert werden, wenn

- das Zertifikat bereits revoziert wurde,
- das Zertifikat eine CA ist und ersetzt wurde,
- das Zertifikat keine CA hat (First-Level-CA) oder
- die CA des Zertifikats keinen privaten Schlüssel hat.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie die Revozierung des ausgewählten Zertifikats durchführen oder den Dialog abbrechen (**Abbrechen**).

Zertifikatsdetails ansehen

Mit der Schaltfläche 👁 bei einem Zertifikat in der Liste können Sie sich die Zertifikatsdetails ansehen.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie den öffentlichen Schlüssel und den Fingerabdruck des Zertifikats in die Zwischenablage kopieren oder den Dialog schließen (**Schließen**).

Zertifikat oder privaten Schlüssel löschen

Mit der Schaltfläche 🗑 bei einem Zertifikat in der Liste können Sie das Zertifikat oder nur den zugehörigen privaten Schlüssel löschen. Das gelöschte Zertifikat wird im Gegensatz zum Revozieren auch aus dem Zertifikatsbaum entfernt. Es wird kein Passwort zum Löschen benötigt.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie das Zertifikat bzw. alternativ nur den privaten Schlüssel löschen oder den Dialog abbrechen (**Abbrechen**).

Zertifikat exportieren

Mit der Schaltfläche ⮆ bei einem Zertifikat in der Liste können Sie dieses in einem der Formate PEM, PKCS oder DER exportieren

PEM

Beim Export im PEM-Format wird in der Regel nur der öffentliche Teil des Zertifikats exportiert. Optional können zusätzlich auch alle zugehörigen CAs der PEM-Datei hinzugefügt werden. Zusätzlich kann, wenn vorhanden, der private Schlüssel mit exportiert werden. Dafür müssen sowohl das aktuell gültige Passwort für den privaten Schlüssel zum Entschlüsseln und ein neues Passwort zum Verschlüsseln des exportierten privaten Schlüssels eingegeben werden. Wenn das Zertifikat keinen privaten Schlüssel hat, wird diese Option nicht angeboten.

PKCS

Das PKCS-Format kann beim Export nur gewählt werden, wenn das Zertifikat einen privaten Schlüssel besitzt. Dazu wird wie beim PEM-Export mit Schlüssel das aktuell gültige Passwort und ein neues Passwort zum Verschlüsseln zwingend benötigt. Im Gegensatz zu PEM wird das Passwort zum Verschlüseln des gesamten Containers verwendet und nicht für den privaten Schlüssel.

DER

Beim Export im DER-Format, wird das Zertifikat im PEM-Format exportiert, wobei die PEM Base64-kodiert wird. Optional kann auch hier der private Schlüssel unter Eingabe der Passwörter exportiert werden. Da das DER-Format nur ein Zertifikat unterstützt, wird in diesem Fall das Zertifikat und der private Schlüssel separat gespeichert und in einer ZIP-Datei zusammengefasst. Der private Schlüssel wird im pkcs8-Format gespeichert.

Mit den Schaltflächen rechts unten im Bearbeitungsfeld können Sie das Zertifikat exportieren oder den Dialog abbrechen (**Abbrechen**).

3.1.2 Private-Key-Passwort

Ab LCOS FX-Version 10.7 müssen Sie immer, wenn ein Zertifikat mit einem privaten Schlüssel benötigt wird, dieses Passwort zur Entschlüsselung des Schlüssels eingeben, wenn

- die jeweiligen Einstellungen aktiviert werden oder
- das verwendete Zertifikat geändert wird.

Dieses Verhalten betrifft folgende Dialoge bzw. Einstellungen:

- Command-Center-Einstellungen
- Webclient-Einstellungen
- Application-Management-Einstellungen
- HTTP-Proxy-Einstellungen
- Mail-Proxy-Einstellungen
- Reverse-Proxy-Frontend-Einstellungen
- Einstellungen des externen Portals
- VPN-Profile
- Einstellungen des internen Portals
- IPsec-Verbindungen mit Zert. oder CA-Authentifizierung
- VPN-SSL-Einstellungen

Abweichend hiervon muss kein Private-Key-Passwort eingegeben werden, wenn es sich um eine der in *Tabelle 1: Bereits angelegte Zertifikate* auf Seite 9 aufgeführten LCOS FX CAs handelt.

3.2 Vorlagen

Zur vereinfachten Erstellung neuer Zertifikate können Sie Vorlagen nutzen, um die Eingabefelder für einige optionale Felder, z. B. den **Distinguished Name** und die **Subject Alternative Names** automatisch auszufüllen.

3.2.1 Übersicht Vorlagen

Navigieren Sie zu **Zertifikatsverwaltung** > **Vorlagen**, um die Liste der derzeit im System angelegten Vorlagen in der Objektleiste anzuzeigen. Zwei Vorlagen für Zertifikate und Certificate Authorities sind nach Installation der LANCOM R&S®Unified Firewall bereits eingerichtet.

In der erweiterten Ansicht zeigen die Tabellenspalten den Namen und die Einstellungen der Vorlage. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für eine vorhandene Vorlage einsehen und anpassen, eine neue Vorlage ausgehend von einer vorhandenen anlegen, oder eine Vorlage aus dem System löschen.

Die beiden Standardvorlagen können nicht gelöscht werden.

3.2.2 Einstellungen für Vorlagen

Im Bearbeitungsfenster **Vorlagen** können Sie zusätzliche Optionen für Zertifikate vorgeben, die bei der Zertifikatserstellung dann automatisch übernommen werden können. Die folgenden Elemente können vorgegeben werden:

Eingabefeld	Beschreibung
Name	Geben Sie einen Namen für die Vorlage an. Über diesen Namen können Sie die Vorlage bei der Zertifikatserstellung auswählen.
Certificate Authority	Diese Option bestimmt, ob das zu erstellende Zertifikat als Zertifizierungsstelle auch andere Zertifikate signieren kann oder nicht. **Vorsicht**: Die Standard-Gültigkeitsdauer für Zertifikate (1 Jahr) und Certificate Authorities (5 Jahre) unterscheiden sich. Bei Änderung dieser Eigenschaft wird die Gültigkeitsdauer angepasst.
Pfad-Länge	Nur bei Auswahl von **Certificate Authority** vorhanden. Hier bestimmen Sie, wie viele Sub-CA-Ebenen mit dieser CA erzeugt werden können. Bei einem Wert von 0 können keine Sub-CAs mit dieser CA signiert werden, d. h. nur noch „normale" Zertifikate können mit dieser CA signiert werden. Wenn das Feld leer bleibt, gibt es keine Begrenzung.
Schlüsselverwendung	Hier können Sie nach einem Klick in das Feld vordefinierte Eigenschaftswerte aus einer Liste hinzufügen wie z. B. Datenverschlüsselung.
Verschlüsselungs-Algorithmus	Wählen Sie aus der Liste der Algrithmen den von Ihnen gewünschten aus. Bei Auswahl der Option „NIST Curves" muss in dem Feld **Kurve** die Art der NIST-Kurve gewählt werden.
Kurve	Falls Sie unter **Verschlüsselungs-Algorithmus** die Option „NIST Curves" ausgewählt haben, dann können Sie hier die Art der NIST-Kurve auswählen.
Schlüssel-Größe	Falls Sie unter **Verschlüsselungs-Algorithmus** die Option „RSA" ausgewählt haben, dann können Sie hier die Schlüsselgröße auswählen.
Hash-Algorithmus	Wählen Sie einen der vorgegebenen Hash-Algorithmen aus.
Erweiterte Schlüsselverwendung	Hier können Sie nach einem Klick in das Feld weitere vordefinierte Eigenschaftswerte aus einer Liste hinzufügen wie z. B. Zeitstempel.
Subjekt	Optional: Wählen Sie eine beliebige Anzahl an Subjekten wie z. B. **Land (C)**, **Bundesland (ST)**, **Organisation (O)**, oder **Abteilung (OU)** aus der Drop-down-Liste aus und geben Sie den dazu gewünschten Inhalt in das Eingabefeld rechts daneben ein. Klicken Sie rechts auf ⊕, um einen Eintrag zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Wenn Sie ein **Subjekt** bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.
Subject Alternative Name (SAN)	Optional: Geben Sie eine beliebige Anzahl benutzerdefinierter alternativer Namen für bestimmte Nutzungszwecke ein und wählen Sie die entsprechenden Typen aus der Drop-down-Liste aus. Die folgenden Typen stehen zur Verfügung: `E-Mail`, `DNS`, `DirName`, `URI`, `IP` und `RegID`. Klicken Sie rechts auf ⊕, um einen Subject Alternative Name (SAN) zur Liste hinzuzufügen. Sie können einzelne Einträge in den Listen bearbeiten oder löschen, indem Sie auf die entsprechende Schaltfläche neben einem Eintrag klicken. Wenn Sie einen **Subject Alternative Name (SAN)** bearbeiten, erscheint auf der rechten Seite des Eintrags ein Haken. Sie müssen Ihre Änderung zunächst mit diesem Haken bestätigen, bevor Sie die Einstellungen für das Zertifikat speichern können.

Die Schaltflächen rechts unten im Bearbeitungsfeld hängen davon ab, ob Sie eine neue Vorlage hinzufügen oder eine bestehende bearbeiten. Klicken Sie für eine neu konfigurierte Vorlage auf **Erstellen**, um sie zur Liste der verfügbaren

Vorlagen hinzuzufügen, oder auf **Abbrechen**, um Ihre Änderungen zu verwerfen. Zum Bearbeiten einer vorhandenen Vorlagen klicken Sie auf **Speichern**, um die neu konfigurierte Vorlage zu speichern, oder auf **Zurücksetzen**, um Ihre Änderungen zu verwerfen.

3.3 Proxy-CAs

Mit den Einstellungen unter **Proxy CA** können Sie Ihre CA-Zertifikate verwalten. Dazu werden diese in vertrauenswürdige und nicht vertrauenswürdige Listen eingeordnet.

3.3.1 Vertrauenswürdige Proxy-CAs

Navigieren Sie zu **Zertifikatsverwaltung** > **Proxy-CAs** > **Vertrauenswürdige CAs**, um die Liste der derzeit im System angelegten benutzerdefinierten und System-Zertifizierungsstellen, denen der SSL-Proxy für externe Verbindungen vertraut, in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Tabellenspalte der **Common Name** des CA-Zertifikats angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes CA-Zertifikat einsehen oder ein CA-Zertifikat als nicht vertrauenswürdig kennzeichnen. Dadurch wird es in die Liste unter **Zertifikatsverwaltung** > **Proxy-CAs** > **Nicht vertrauenswürdige CAs** verschoben. Benutzerdefinierte CA-Zertifikate können Sie auch löschen.

Um eine benutzerdefinierte CA an Ihre LANCOM R&S®Unified Firewall zu senden, klicken Sie auf die ➜] (Import)-Schaltfläche in der Kopfzeile der Objektleiste, wählen Sie die gewünschte PEM-/CRT-Datei aus, öffnen Sie sie und klicken Sie auf **Importieren**. Das importierte benutzerdefinierte Zertifikat wird zur Liste verfügbarer vertrauenswürdiger Proxy-CAs hinzugefügt. Über die Option **Nur benutzerdefinierte CAs anzeigen** können Sie die angezeigte Liste auf die von Ihnen hinzugefügten Certificate Authorities reduzieren.

3.3.2 Nicht vertrauenswürdige Proxy-CAs

Navigieren Sie zu **Zertifikatsverwaltung** > **Proxy-CAs** > **Nicht vertrauenswürdige CAs**, um die Liste der derzeit im System angelegten benutzerdefinierten und System-Zertifizierungsstellen, denen der SSL-Proxy für externe Verbindungen **nicht** vertraut, in der Objektleiste anzuzeigen.

In der erweiterten Ansicht wird in der ersten Tabellenspalte der **Common Name** des CA-Zertifikats angezeigt. Mit den Schaltflächen in der letzten Spalte können Sie die Einstellungen für ein vorhandenes CA-Zertifikat einsehen oder ein CA-Zertifikat als vertrauenswürdig kennzeichnen. Dadurch wird es in die Liste unter **Zertifikatsverwaltung** > **Proxy-CAs** > **Vertrauenswürdige CAs** verschoben. Benutzerdefinierte CA-Zertifikate können Sie auch löschen.

Über die Option **Nur benutzerdefinierte CAs anzeigen** können Sie die angezeigte Liste auf die von Ihnen hinzugefügten Certificate Authorities reduzieren.