connecting your business

Addendum

LCOS 9.10 RC1

LANCOM
Systems

Inhalt

1 Addendum zur LCOS-Version 9.10

Dieses Dokument beschreibt die Änderungen und Ergänzungen in der LCOS-Version 9.10 gegenüber der vorherigen Version.

2 Übersicht über die Neuerungen der LCOS-Version 9.10

In der LCOS-Version 9.10 haben wir eine Vielzahl neuer Features umgesetzt.

Tabelle 1: Neue Features der LCOS-Version 9.10

Smart Certificate

LANCOM setzt einen Meilenstein im Bereich Sicherheit!

Maximale Sicherheit bei VPN-Zugriffen: Profitieren Sie ab sofort von der in LANCOM Geräte integrierten Funktion zur komfortablen Erstellung digitaler Zertifikate - ganz ohne externe Zertifizierungsstelle! VPN-Verbindungen lassen sich somit mit selbst erstellten Zertifikaten sicher verschlüsselt einrichten. Dieses Maximum an Sicherheit ist enthalten in allen LANCOM Central Site VPN Gateways, WLAN-Controllern sowie in allen LANCOM Routern mit LANCOM VPN 25 Option.

High Availability Clustering

Gruppierung und zentrales Management von mehreren WLAN-Controllern und Central Site VPN Gateways

Gruppieren Sie mehrere WLAN-Controller oder Central Site VPN Gateways zu einer hochverfügbaren Gerätegruppe (High Availability Cluster)! Über die LANCOM High Availability Clustering Optionen lassen sich mehrere Geräte zu einem Cluster zusammenfassen. Somit ergeben sich viele Vorteile, wie das zentrale Management und der komfortable Konfigurationsabgleich (Config Sync) aller Cluster-Geräte. Hiervon profitieren Sie insbesondere beim Aufbau von intelligenten Backup-Szenarien, da nur ein WLAN-Controller oder Central Site VPN Gateway im Cluster konfiguriert werden muss - für den Administrator eine enorme Zeitersparnis. Darüber hinaus ermöglicht High Availability Clustering eine automatische Lastverteilung sowie die Vergabe von Cluster-Zertifikaten.

Über 100 weitere Features

Mehr Sicherheit, mehr Management, mehr Virtualisierung.

Profitieren Sie von vielen neuen Möglichkeiten, Ihr Netzwerk-Management weiter zu professionalisieren. So verschlüsseln Sie ab LCOS 9.10 bei Bedarf Ihre Konfiguration, koppeln entfernte Netzwerke flexibel per GRE-Tunnel über ein "virtuelles Ethernet-Kabel", gewähren allen WLAN-Nutzern pro SSID eine gleichberechtigte Bandbreite oder setzen Sie Hochleistungs-Punkt-zu-Punkt-Strecken über Gigabit Wireless mit bis zu 1,3 GBit/s auf.

Weitere Features

Management der Client-Bandbreite je SSID

Mehr Kontrolle über die verwendete Bandbreite pro WLAN-Client: Das Bandbreiten-Limit pro SSID (Download und Upload) lässt sich für jeden Client konfigurieren.

GRE-Tunnel

Maximale Flexibilität bei der Kopplung von entfernten Netzwerken: Mit Generic Routing Encapsulation (GRE) werden Pakete eingekapselt und in Form eines Tunnels zwischen zwei Endpunkten transportiert.

Ethernet over GRE-Tunnel

Das "virtuelle Ethernet-Kabel" - ideal zur Verbindung zweier Netze via Layer-2-Tunnel z. B. per IPSec-VPN.

16 SSIDs

Pro WLAN-Funkmodul sind ab sofort 16 individuelle SSIDs konfigurierbar. Somit können doppelt so viele WLAN-Dienste parallel angeboten werden - bei Dual Radio Access Points mit zwei WLAN-Funkmodulen sogar bis zu 32!

Anzeige verwendeter Public Spot-Lizenzen

Im LANmonitor wird die aktuelle sowie die maximal mögliche Anzahl verwendeter Public Spot-Benutzer angezeigt und zudem ein Hinweis bei 90% Lizenzauslastung ausgegeben.

Load Balancer Client Binding

Neue Anwendungsmöglichkeiten in Load Balancing-Szenarien - In anspruchsvollen Anwendungen wie Online-Banking werden zusammenhängende Sessions auf einer WAN-Leitung erkannt und aufrechterhalten.

TR-069-Unterstützung

"Zero-touch Management" - Das Protokoll TR-069 ermöglicht die automatische Provisionierung und ein sicher verschlüsseltes Remotemanagement eines Routers in Provider-Umgebungen.

Verschlüsselte Konfigurationsablage in LANconfig

Gewähren Sie Unbefugten keinen Zugriff auf Ihre Konfiguration - In LANconfig lassen sich Konfigurationsdateien per Passwort verschlüsseln und sicher speichern.

E-Mail-Benachrichtigung des LANCOM Content Filters

Benachrichtigungen per E-Mail bei Content Filter-Ereignissen werden auf Wunsch sofort oder täglich ausgelöst.

Erweiterte Zeichenanzahl

Die mögliche Zeichenanzahl zur Vergabe von Gerätenamen wurde auf 64 erweitert.

Neuere SCEP-Algorithmen

Mehr Sicherheit bei Zertifikaten: Es werden die SCEP-Algorithmen AES192 und AES256 zur Verschlüsselung sowie SHA256, SHA384 und SHA512 zur Signaturprüfung unterstützt.

Neue DynDNS-Anbieter im Setup-Assistenten

Die Anbieter "Strato" und "feste-ip.net" und wurden im DynDNS-Assistenten hinzugefügt.

Deaktivierbare Konfigurationsvergabe durch WLC

Mehr Sicherheit vor Rogue-APs: Die automatische Konfigurationsvergabe durch einen WLAN-Controller an neue Access Points über eine WAN-Verbindung ist konfigurierbar.

LEDs per WLC abschaltbar

Die LEDs verwalteter WLAN-Geräte lassen sich zentral über den WLAN-Controller abschalten.

Überwachung von Konfigurationsänderungen

Einfache Überprüfung von Konfigurationsänderungen dank der Darstellung von Hash-Werten, Zeitstempeln und Change-Countern.

Verbesserte Kontrolle über Public Spot-Volumenbudgets

Im Public Spot-Volumenbudget kann nun mehr als 4 GB Datenvolumen als Limit angelegt und zusätzlich das festgelegte Budget pro Nutzer auf dem Voucher gedruckt werden.

Direkteinstieg zur Voucher-Erstellung im Public Spot

Stark vereinfachter Zugang zur Erstellung von Public Spot-Vouchern durch automatische Weiterleitung auf die entsprechende Seite - ideal für ungeschultes Personal!

3 Digitale Zertifikate (Smart Certificate)

Ab LCOS-Version 9.10 haben Sie die Möglichkeit, digitale Zertifikate durch einen LANCOM Router zu erstellen und zu vergeben.

Außerdem zeigt der LANmonitor ab LCOS-Version 9.10 eine Übersicht über aktive und zurückgezogene Zertifikate.

Tabelle 2: Übersicht der Funktionsrechte

Bezeichnung: [1]LANconfig, [2]Setup-Menü	Hexschreibweise an der Konsole	Rechtebeschreibung
1. CA-Web-Schnittstellen-Assistent **2.** CA-Web-Schnittstelle	0x1000000	Erstellen für Profile der CA-Web-Schnittstelle

3.1 Verwendung digitaler Zertifikate (Smart Certificate)

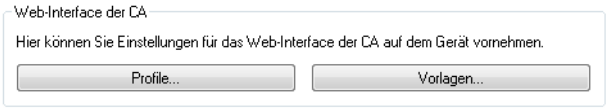
Die Konfiguration des SCEP-Clients für die Erstellung und Verteilung von Zertifikaten wird in einer komplexen und ausgedehnten Netz-Infrastruktur schnell aufwändig. Durch vordefinierte, auswählbare Profile und den Zugriff über eine Web-Schnittstelle lässt sich dieser Aufwand reduzieren.

Mit einem LANCOM Router haben Sie die Möglichkeit, hochsichere Zertifikate zu generieren und zuzuweisen. Sie verwalten die Zertifikate bequem über die WEBconfig-Oberfläche des entsprechenden Gerätes. Eine externe Zertifizierungsstelle ist somit nicht mehr erforderlich, was gerade bei kleineren Infrastrukturen vorteilhaft ist.

Mit dem Zertifikats-Wizard von LANCOM können selbst Anwender ohne Zertifikats-Knowhow in wenigen Schritten Zertifikate erstellen.

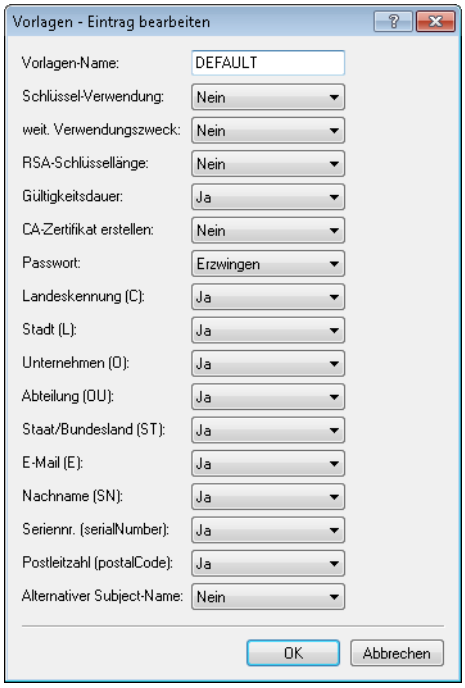
Der Geräte-Administrator erstellt das Profil als Sammlung von Zertifikats-Eigenschaften. Es enthält einerseits die Konfiguration des Zertifikats sowie eine eindeutige Zertifikats-ID. Statt also alle Zertifikats-Parameter einzugeben, genügt es von da an, eines der angezeigten Profile auszuwählen, um ein Zertifikat zu erstellen und zu verteilen.

Die Verwaltung von Profilen erfolgt auch im LANconfig unter **Zertifikate** > **Zertifikatsbehandlung** im Abschnitt **Web-Interface der CA**.



3.1.1 Vorlagen für Zertifikats-Profile erstellen

In LANconfig erfolgt die Profil-Erstellung unter **Zertifikate** > **Zertifikatsbehandlung** > **Vorlagen**.



Standardmäßig ist bereits eine Vorlage „DEFAULT“ angelegt.

Der Adminstrator legt fest, welche der Profileigenschaften erforderlich und welche durch den Anwender zu editieren sind. Die folgenden Optionen stehen zur Auswahl:

- Nein: Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.
- Fest: Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.
- Ja: Das Feld ist sichtbar und durch den Anwender änderbar.
- Erzwingen: Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

Diese Zugriffsrechte gelten für die folgenden Profil- und ID-Felder:

Profilfelder

- Schlüssel-Verwendung
- weit. Verwendungszweck
- RSA-Schlüssellänge
- Gültigkeitsdauer
- CA-Zertifikat erstellen
- Passwort

Identifier

- Landeskennung (C)
- Stadt (L)
- Unternehmen (O)
- Abteilung (OU)
- Staat / Bundesland (ST)
- E-Mail (E)
- Nachname (SN)

- Seriennr. (serialNumber)
- Postleitzahl (postalCode)
- Subject alt. name

Bei leerer Vorlagen-Tabelle sieht der Anwender nur Eingabefelder für die Profilnamen, die allgemeinen Namen (CN) sowie das Passwort. Die restlichen Profilfelder behalten die vom Geräte-Administrator festgelegten Defaultwerte.

3.1.2 Erstellen eines Profils in LANconfig

Der Anwender benötigt für Erstellung, Auswahl, Änderung und Zuweisung der Profile die entsprechenden Zugriffsrechte.

In LANconfig erfolgt die Profil-Erstellung unter **Zertifikate** > **Zertifikatsbehandlung** > **Profile**.

Standardmäßig sind bereits drei Profile für gängige Anwendungsszenarien angelegt.

Profil-Name

Ist der eindeutige Name des Profils.

Profil-Vorlage

Wählen Sie hier ggf. eine passende Profil-Vorlage aus.

In der Profil-Vorlage ist festgelegt, welche Zertifikatsangaben notwendig und welche änderbar sind. Die Vorlagen-Erstellung erfolgt unter **Zertifikate** > **Zertifikats-Behandlung** > **Vorlagen**.

Schlüssel-Verwendung

Gibt an, für welche Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen zur Auswahl:

Tabelle 3: Zur Verfügung stehende Schlüssel-Verwendungen

Wert	Bedeutung
critical	Ist diese Einschränkung gesetzt, ist es immer erforderlich, die Schlüsselverwendungs-Erweiterung zu beachten. Wird die Erweiterung nicht unterstützt, wird das Zertifikat als nicht gültig abgelehnt.
digitalSignature	Ist diese Option gesetzt, wird der öffentliche Schlüssel für digitale Signaturen verwendet.
nonRepudiation	Ist diese Option ist gesetzt, wird der Schlüssel für digitale Signaturen eines Nichtabstreitbarkeitsservice verwendet. d. h. eher langfristigen Charakter besitzt, z. B. Notariatsservice.
keyEncipherment	Ist diese Option gesetzt, wird der Schlüssel für die Verschlüsselung von anderen Schlüsseln oder Sicherheitsinformation verwendet. Es ist möglich, die Verwendung mit **encipher only** und **decipher only** einzuschränken.
dataEncipherment	Ist diese Option gesetzt, wird der Schlüssel zur Verschlüsselung von Benutzerdaten (außer andere Schlüssel) verwendet.
keyAgreement	Ist diese Option gesetzt, wird der "Diffie-Hellman" Algorithmus für die Schlüsselvereinbarung verwendet.
keyCertSign	Ist diese Option gesetzt, wird der Schlüssel für die Verifikation von Signaturen auf Zertifikaten verwendet. Dies ist z. B. für CA-Zertifikate sinnvoll.
cRLSign	Ist diese Option gesetzt, wird der Schlüssel für die Verifikation von Signaturen auf CRLs verwendet. Dies ist z. B. für CA-Zertifikate sinnvoll.
encipherOnly	Ist nur mit der Schlüsselvereinbarung nach Diffie Hellman (keyAgreement) sinnvoll.
decipherOnly	Ist nur mit der Schlüsselvereinbarung nach Diffie Hellman (keyAgreement) sinnvoll.

Eine kommagetrennte Mehrfachauswahl ist möglich.

weit. Verwendungszweck

Gibt an, für welche erweiterte Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen zur Auswahl:

Tabelle 4: Erweiterte Verwendungen

Wert	Bedeutung
critical	
serverAuth	SSL/TLS-Web-Server-Authentifizierung
clientAuth	SSL/TLS-Web-Client-Authentifizierung
codeSigning	Signierung von Programmcode
emailProtection	E-Mail-Schutz (S/MIME)
timeStamping	Daten mit zuverlässigen Zeitstempeln versehen
msCodeInd	Microsoft Individual Code Signing (authenticode)
msCodeCom	Microsoft Commercial Code Signing (authenticode)
msCTLSign	Microsoft Trust List Signing
msSGC	Microsoft Server Gated Crypto
msEFS	Microsoft Encrypted File System
nsSGC	Netscape Server Gated Crypto

Eine kommagetrennte Mehrfachauswahl ist möglich.

RSA-Schlüssellänge

Gibt die Länge des Schlüssels an.

Gültigkeitsdauer

Gibt die Zeitdauer in Tagen an, für die der Schlüssel gültig ist. Nach Ablauf dieser Frist verliert der Schlüssel seine Gültigkeit, falls der Anwender ihn nicht vorher erneuert.

CA-Zertifikat erstellen

Gibt an, ob es sich um ein CA-Zertifikat handelt.

Passwort

Passwort, um die PKCS12-Zertifikatsdatei abzusichern.

Die folgenden Eingaben dienen zur Erstellung einer Zertifikats-ID. Zur Auswahl stehen die folgenden Optionen:

Landeskennung (C)

Geben Sie die Staatenkennung ein (z. B. „DE" für Deutschland).

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **C**= (**C**ountry).

Stadt (L)

Geben Sie den Ort ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **L**= (**L**ocality).

Unternehmen (O)

Geben Sie das Unternehmen an, welches das Zertifikat ausstellt.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **O**= (**O**rganization).

Abteilung (OU)

Geben Sie die Abteilung an, die das Zertifikat ausstellt.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **OU**= (**O**rganization **U**nit).

Staat / Bundesland (ST)

Geben Sie das Bundesland ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **ST**= (**ST**ate).

E-Mail (E)

Geben Sie eine E-Mail-Adresse ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter `emailAddress=`.

Nachname (SN)

Geben Sie einen Nachnamen ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **SN**= (**S**ur**N**ame).

Seriennr. (serialNumber)

Geben Sie eine Seriennummer ein.

Im Zertifikat erscheint dieser Eintrag unter `serialNumber=`.

Postleitzahl (postalCode)

Geben Sie die Postleitzahl des Ortes ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter `postalCode=`.

Subject alt. Name (SAN)

Mit dem „Subject Alternative Name“ (SAN) verknüpfen Sie weitere Daten mit diesem Zertifikat. Die folgenden Daten sind möglich:

- E-Mail-Adressen
- IPv4- oder IPv6-Adressen
- URIs
- DNS-Namen
- Verzeichnis-Namen
- Beliebige Namen

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter `subjectAltName=` (z. B. `subjectAltName=IP:192.168.7.1`).

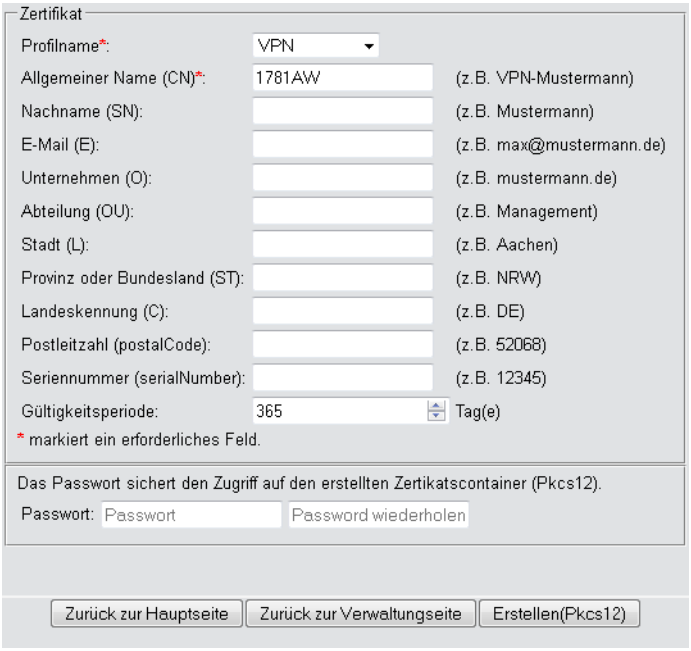
Der Zertifikatersteller vergibt den allgemeinen Namen "CN". Die Angabe des "CN" ist mindestens erforderlich.

3.1.3 Zertifikaterstellung über WEBconfig

Sie benötigen für Auswahl, Änderung und Zuweisung der Profile die entsprechenden Zugriffsrechte.

Zur Zertifikaterstellung wechseln Sie in die WEBconfig des LANCOM-Gerätes.

1. Um über die Webschnittstelle ein Zertifikat zu erstellen, wechseln Sie in die Ansicht **Setup-Wizards** > **Zertifikate verwalten** und wählen Sie **Neues Zertifikat erstellen**.



2. Wählen Sie im Dropdown-Menü **Profilname** das Profil aus, auf dem das Zertifikat beruhen soll.

Leere Vorlagen enthalten nur Felder mit der Auswahl „Nein“. Wählt der Anwender ein Profil aus, das auf einer leeren Vorlage basiert, erscheint in der Eingabemaske nur der allgemeine Name (Common-name). Die restlichen Profilfelder behalten die vom Geräte-Administrator festgelegten Defaultwerte.

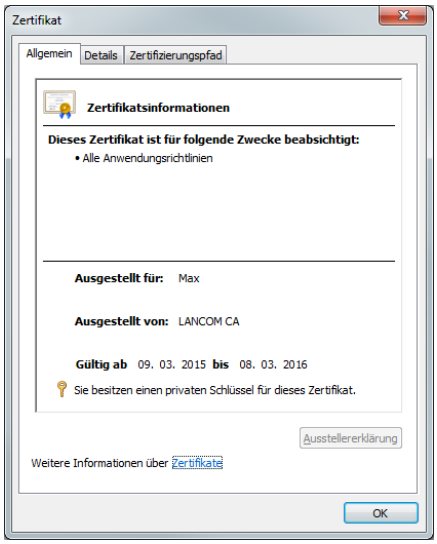
3. Füllen Sie das Feld **Allgemeiner Name (CN)** aus. Definieren Sie eine Gültigkeitsperiode für das Zertifikat und vergeben Sie ein sicheres Passwort (PIN). Die übrigen Felder wie **E-Mail**, **Unternehmen** etc. sind optionale Informationen. Sie erleichtern jedoch ggf. die schnellere Suche des Zertifikat-Empfängers, wenn es zu Problemen mit dem Zertifikat kommen sollte.

   Für das Passwort sind folgende Zeichen zulässig: [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

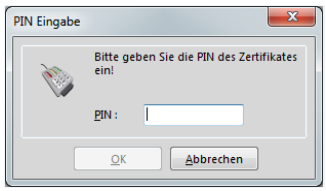
4. Zum Abschluss der Änderungen klicken Sie auf die Schaltfläche **Erstellen (PKCS12)**. Im darauf folgenden Speicherdialog haben Sie die Möglichkeit, den Namen und Speicherort der Datei festzulegen.

   Die so neu erstellten Zertifikate erscheinen in der Zertifikate-Status-Tabelle unter **Status** > **Zertifikate** > **SCEP-CA** > **Zertifikate**.

5. Übergeben Sie dem Empfänger das erstellte Zertifikat zusammen mit dem Zugangspasswort, das Sie in Schritt 3 vergeben haben.



6. Der Empfänger hat jetzt die Möglichkeit einer sicheren VPN-Einwahl. Für eine erfolgreiche Einwahl ist die Eingabe des Zugangspassworts (PIN) erforderlich, das Sie in Schritt 3 vergeben haben.



3.1.4 Zertifikatverwaltung über die WEBconfig

Sie benötigen für die Verwaltung der Zertifikate die entsprechenden Zugriffsrechte.

Um über die Webschnittstelle ein Zertifikat zu verwalten, wechseln Sie in die Ansicht **Setup-Wizards** > **Zertifikate verwalten**. Hier erhalten Sie eine Übersicht der erstellten Zertifikate und können diese auch widerrufen.

Die Tabellenspalten haben die folgenden Bedeutungen:

Seite

In dieser Spalte markieren Sie den Eintrag.

Index

Zeigt den fortlaufenden Index des Eintrags an.

Name

Zeigt den Namen des Zertifikats an.

Seriennummer

Enthält die Seriennummer des Zertifikats.

Status

Zeigt den aktuellen Status des Zertifikats. Mögliche Werte sind:

- V: Gültig (valid)
- R: Widerrufen (revoked)
- P: Angefragt (pending)

Erstellungszeitpunkt

Zeigt den Zeitpunkt der Zertifikaterstellung an (Datum, Uhrzeit).

Ablaufzeit

Gibt den Zeitpunkt mit Datum und Uhrzeit an, zu dem das Zertifikat regulär abläuft.

Rückrufzeit

Gibt den Zeitpunkt mit Datum und Uhrzeit an, zu dem das Zertifikat vorzeitig widerrufen wurde.

Rückrufgrund

Gibt den Grund für einen vorzeitigen Widerruf an. Die Auswahl erfolgt über eine Drop-Down-Auswahlliste.

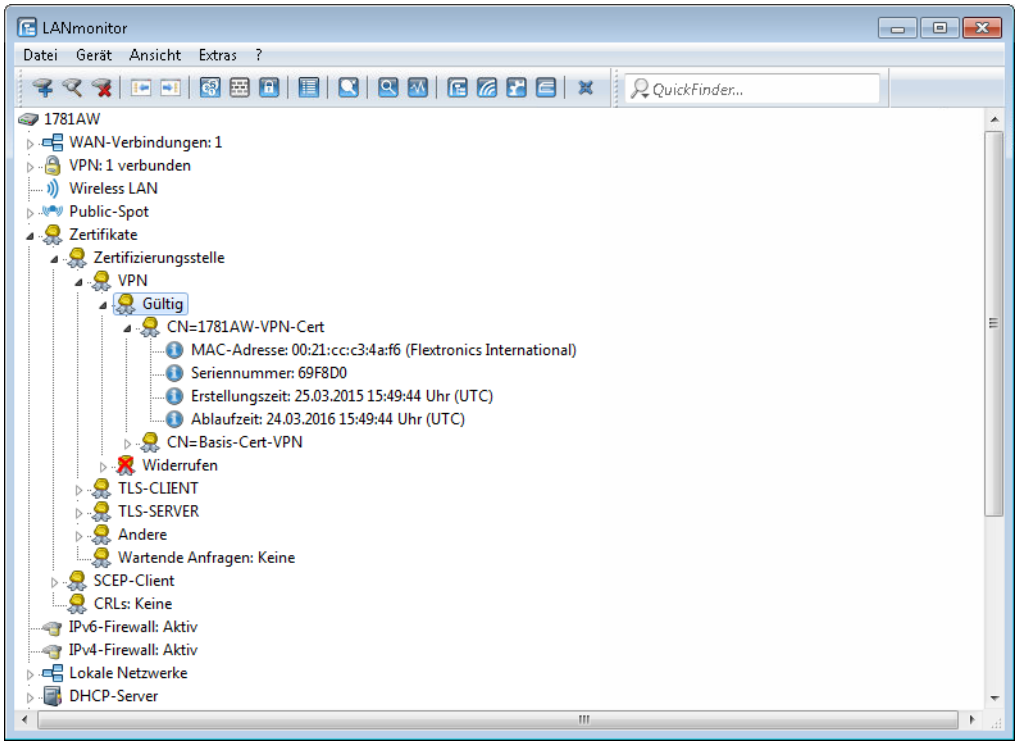
Um ein Zertifikat zu widerrufen, markieren Sie es in der Spalte **Seite**, geben in der Spalte **Rückrufgrund** an, warum Sie das Zertifikat widerrufen und klicken auf **Widerrufen**.

Die Spalteneinträge von **Status**, **Rückrufzeit** und **Rückrufgrund** ändern sich entsprechend.

Um ein zuvor widerrufenes Zertifikat wieder für gültig zu erklären, markieren Sie es wieder in der ersten Spalte und klicken auf **Als gültig erklären**.

3.1.5 Zertifikate verwalten im LANmonitor

Der LANmonitor zeigt die aktiven und widerrufenen Zertifikate sowie die Zertifikatsanfragen der SCEP-Clients an.



Um ein Zertifikat zu widerrufen, klicken Sie mit der rechten Maustaste auf das entsprechende Zertifikat und wählen Sie im Kontextdialog den Punkt **Zertifikat widerrufen** aus.

Eine Übersicht aller widerrufenen Zertifikate sehen Sie im Abschnitt **Widerrufen**.

Zertifikatanfragen von SCEP-Clients sehen Sie im Abschnitt **Wartende Anfragen**. Klicken Sie mit der rechten Maustaste auf die entsprechende Anfrage und wählen Sie im Kontextdialog entweder **Ablehnen** oder **Akzeptieren** aus.

3.1.6 Zertifikate über URL-API erstellen

Die Erstellung von Zertifikaten ist in einer komplexen und ausgedehnten Netz-Infrastruktur komfortabel über eine spezielle API möglich.

Durch den Aufruf einer URL mit angehängten Parametern lässt sich die Erstellung z. B. über ein Skript automatisieren. Die folgenden Parameter sind möglich:

- `a`: Gibt den Profilnamen an.
- `b`: Gibt den allgemeinen Namen (common name) an.
- `c`: Gibt den Familiennamen (surname) an.
- `d`: Gibt die E-Mail (email) an.
- `e`: Gibt die Organisation an.
- `f`: Gibt die Organisations-Einheit (organization unit) an.
- `g`: Gibt den Ort (locality) an.
- `h`: Gibt das Bundesland (state) an.
- `i`: Gibt den Staat (country) an.
- `j`: Gibt die Postleitzahl (postal code) an.
- `k`: Gibt die Seriennummer an.
- `l`: Gibt den Alternative Subject Name an.

- m: Gibt die Verwendung (key usage) an.
- n: Gibt die erweiterte Verwendung (extended key usage) an.
- o: Gibt die Schlüssellänge (key length) an.
- p: Gibt die Gültigkeitsdauer (validity period) in Tagen an.
- q: Gibt das Passwort für die PKCS12-Datei an.
- r: Gibt an, ob es sich um ein CA-Zertifikat handelt.
  - 1: CA-Zertifikat
  - 0: kein CA-Zertifikat

Der Wizard verarbeitet nur die Parameter, für die in der Presets-Tabelle die entsprechenden Zugriffsrechte gesetzt sind.

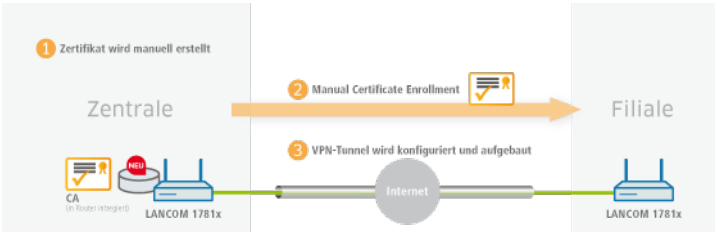
Der Aufruf der URL mit den entsprechenden Parametern sieht wie folgt aus:

```
192.168.10.74/scepwiz/a=VPN&b=iPhone&q=company
```

3.1.7 Tutorials

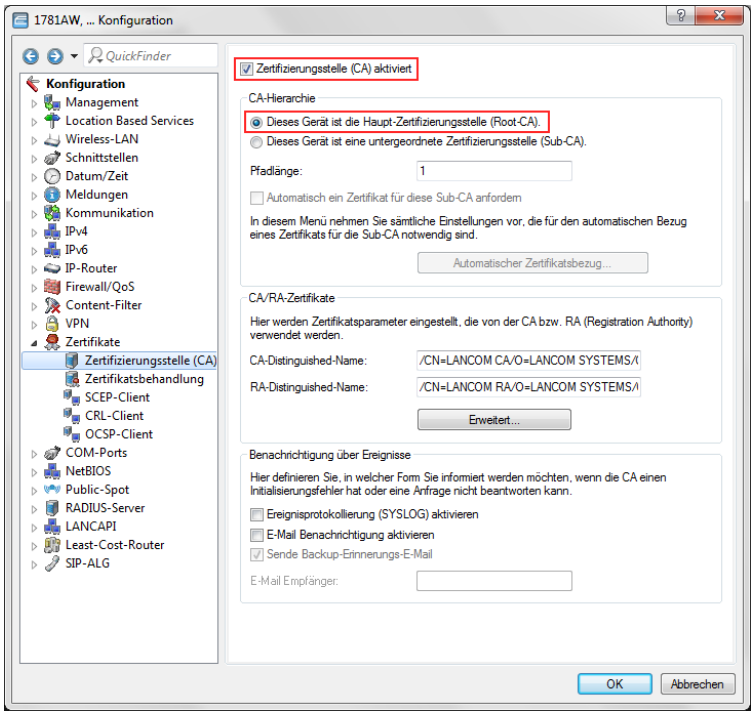
Einrichten einer CA und Erstellen und Nutzen von Zertifikaten für eine VPN-Verbindung

Dieses Tutorial beschreibt, wie Sie eine CA (Certificate-Authority) auf einem LANCOM Router aktivieren und wie die CA Sie dabei unterstützt, neue Zertifikate für eine VPN-Verbindung zwischen zwei LANCOM Routern zu erstellen und zu nutzen (Manuelle Zertifikatsverteilung).



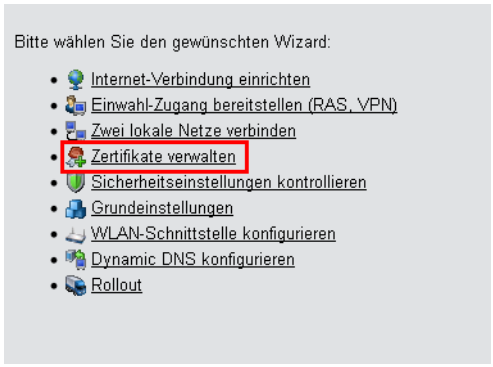
Auf allen Geräten müssen Datum und Uhrzeit gültig sein.

1. Aktivieren Sie Sie die Certificate-Authority in LANconfig und definieren Sie das Gerät als Haupt-Zertifizierungsstelle (Root-CA). Diese Einstellungen finden Sie unter **Zertifikate** > **Zertifizierungsstelle (CA)**.



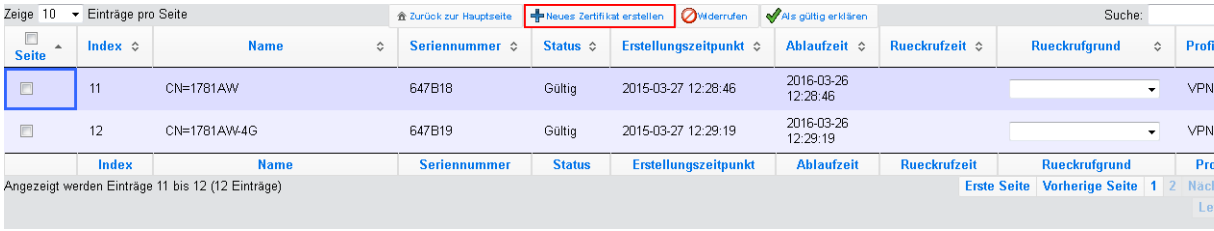
2. Sie haben nun die Möglichkeit, mit der CA Zertifikate für die VPN-Endpunkte zu erstellen, über die die Verbindung später eingerichtet wird.

   a) In dem Setup-Wizard **Zertifikate verwalten** erstellen Sie Zertifikate einfach und komfortabel.



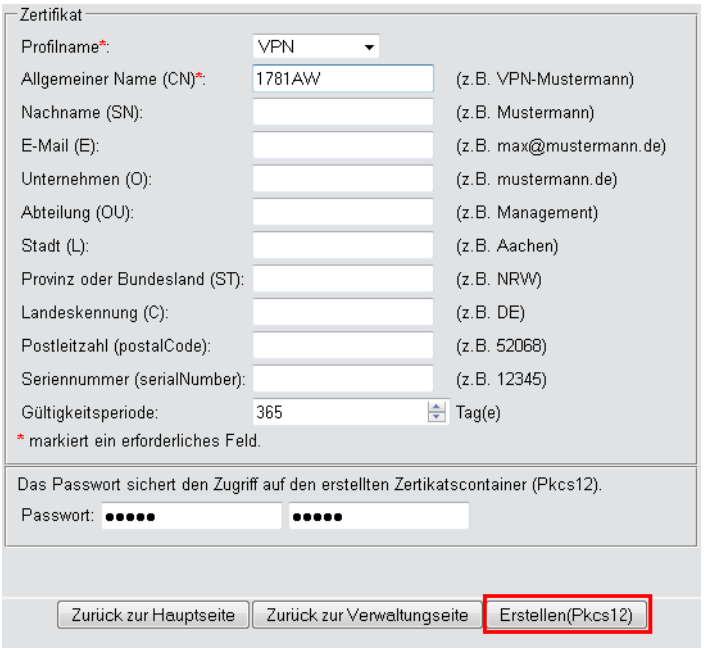
   b) Auf der ersten Seite des Wizards finden Sie eine Übersicht aller bisher ausgestellten Zertifikate der CA.

   Das Zertifikat der CA selbst wird nicht angezeigt.



   Über die Schaltfläche **Neues Zertifikat erstellen** starten Sie den Prozess zur Generierung eines neuen Zertifikates.

c) Unter dem Eintrag **Zertifikate erstellen** haben Sie die Möglichkeit, neben dem Profil und dem offiziellen Namen des Zertifkates (Common-name, kurz CN) noch weitere Zertifikats-Informationen zu konfigurieren, die bei der Identifizierung des Zertifikates hilfreich sind. Legen Sie die Gültigkeit für das Zertifikat sowie das Passwort für die Pkcs12-Datei fest, in der das erstellte Zertifikat, der entsprechende private Schlüssel und das Zertifikat der CA zusätzlich gespeichert werden.



Haben Sie alle notwendigen und gewünschten Informationen eingetragen, erstellen Sie das Zertifikat über die Schaltfäche **Erstellen (Pkcs12)**. Das Fenster zum Speichern der Pkcs12-Datei erscheint automatisch, sobald das Zertifikat im Gerät erstellt wurde. Dieser Vorgang kann einige Sekunden in Anspruch nehmen.

d) Im Fenster **Speichern der Pkcs12-Datei** wählen Sie den Speicherort und den Namen der Pkcs12-Datei. Als Default wird der Dateiname nach folgendem Format vergeben:
`pkcs12<YYYY_MM_DD-hh_mm_ss>.p12`

YYYY: Jahr

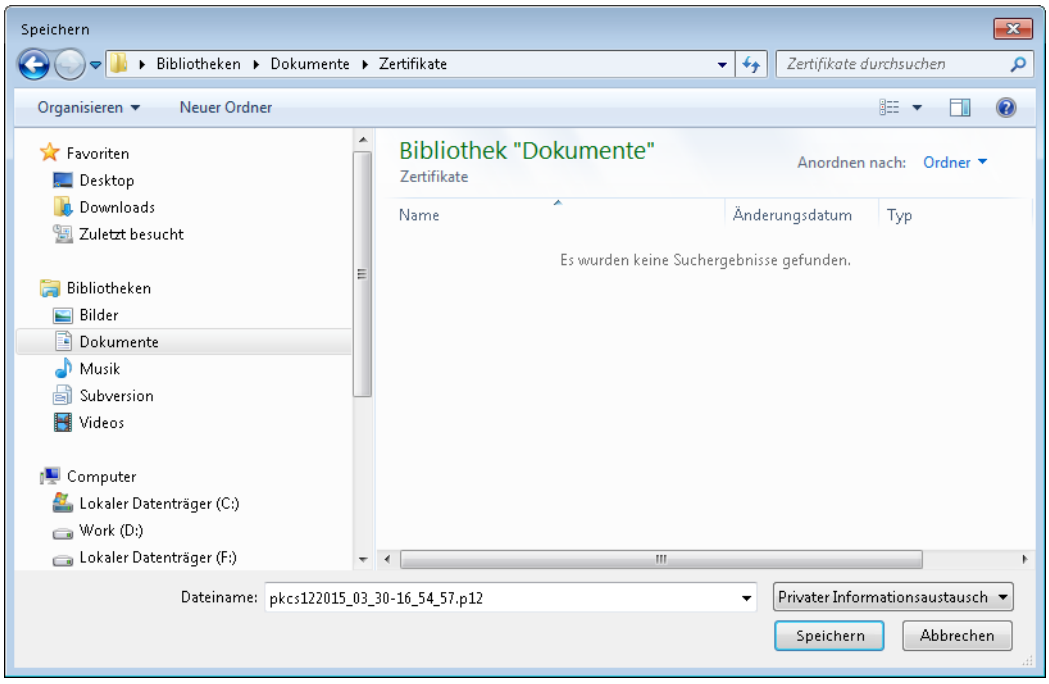
MM: Monat

DD: Tag

hh: Stunde

mm: Minute

ss: Sekunde



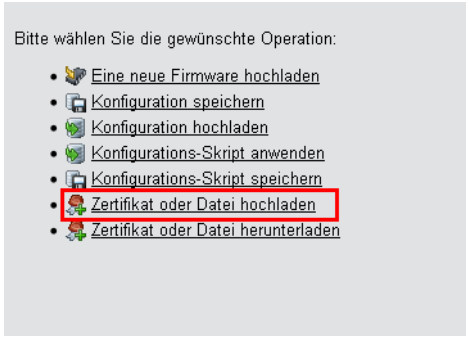
Der Dateiname kann wie im Beispiel beliebig abgewandelt werden.

e) Weitere Zertifikate erstellen Sie nach dem gleichen Schema.

Übersichtsseite mit zwei erstellten Zertifikaten.

3. Damit Sie die Zertifikate für eine VPN-Verbindung nutzen können, ist es erforderlich, diese den Geräten zur Verfügung zu stellen.

a) Den Upload auf die jeweiligen VPN-Endpunkte können Sie komfortabel über WEBconfig unter **Dateimanagement** > **Zertifikat oder Datei hochladen** durchführen.



b) **Zertifikat oder Datei hochladen**

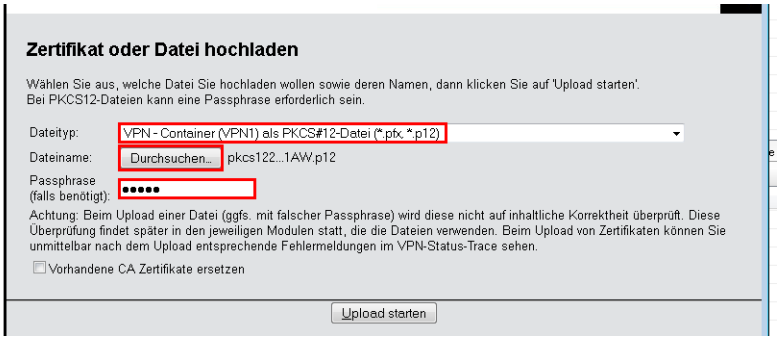
Wählen Sie zunächst den Dateityp und Speicherort. Für VPN-Verbindungen wählen Sie einen ungenutzten VPN-Container.

Solange noch keine Zertifikate für VPN eingerichtet wurden, sind alle VPN-Container ungenutzt.

Im nächsten Schritt wählen Sie die Pkcs12-Datei aus, welche das Zertifikat enthält, das Sie für diesen VPN-Endpunkt nutzen möchten.

Geben Sie das Passwort an, welches Sie in Schritt 2.c beim Erstellen der Datei vergeben haben.

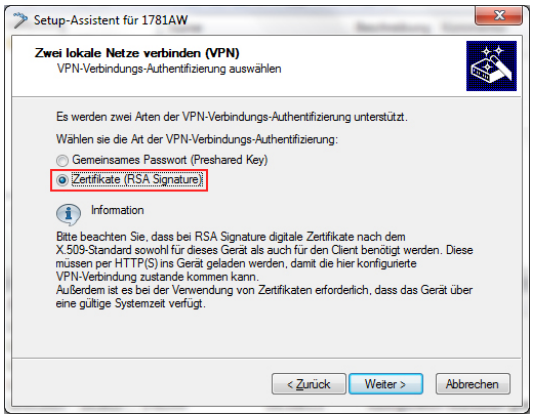
Starten Sie abschließend den Upload.



Dieser Vorgang ist für alle VPN-Endpunkte erforderlich. Beachten Sie, dass jeder VPN-Endpunkt ein eigenes Zertifikat braucht.

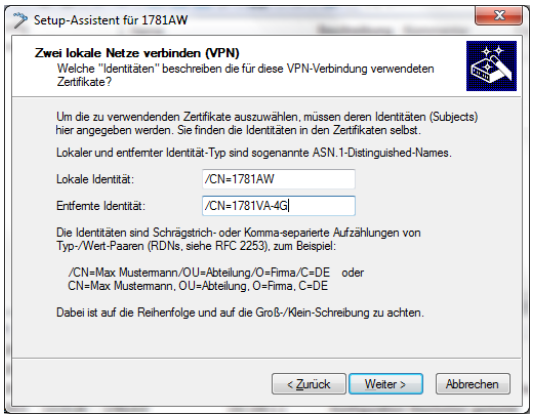
4. Stellen Sie eine VPN-Verbindung zwischen zwei VPN-Endpunkten her. Dies erfolgt über den Setup-Wizard **Zwei lokale Netze verbinden (VPN)**.

   a) Wählen Sie als VPN-Verbindungs-Authentifizierung im Setup-Wizard **Zertifikate (RSA Signature)** aus.



   b) Im Fenster **Lokale und entfernte Identitäten** geben Sie den sogenannten "ASN.1-Distinguished-Name" an. Dies ist der offizielle Name des Zertifikates plus aller zusätzlichen Informationen, die Sie in Schritt 2.c angegeben haben. Diese zusätzlichen Informationen finden Sie in der Übersicht der Zertifikate (Schritt 2.e) in der Spalte "Name". Bei dem Punkt **Lokale Identität** geben Sie die Informationen des Zertifikates an, welches sich auf dem

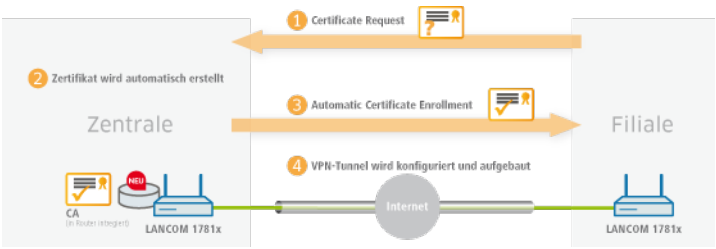
lokalen Gerät befindet. Der Punkt **Entfernte Identität** erhält die Zertifikat-Informationen des anderen VPN-Endpunktes.



c) Führen Sie abschließend den Wizard weiter aus. Bei dem anderen VPN-Endpunkt für diese VPN-Verbindung gehen Sie äquivalent vor.

Einrichten einer CA und Erstellen und Nutzen von Zertifikaten für eine VPN-Verbindung mit Zertifikatsrollout über SCEP

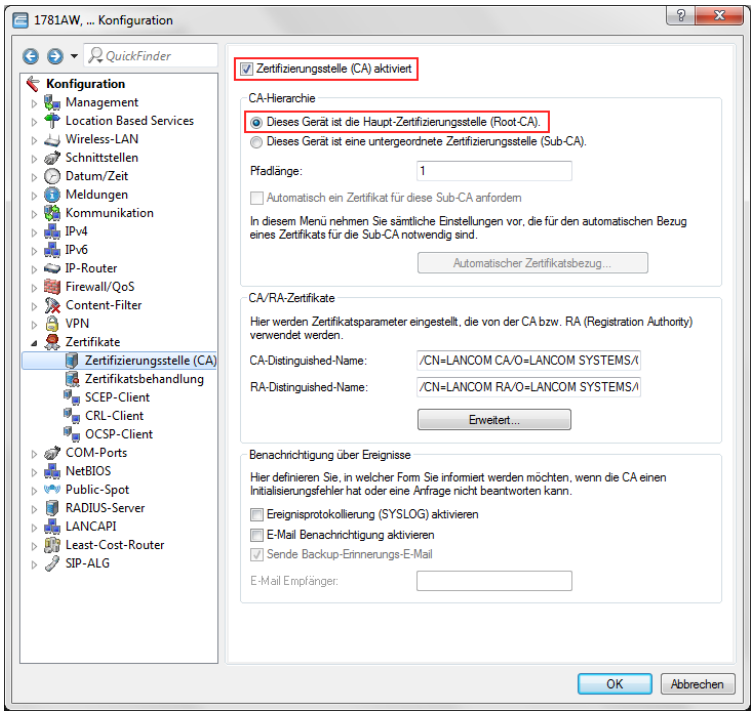
Dieses Tutorial beschreibt, wie Sie eine CA (Certificate-Authority) auf einem LANCOM Router aktivieren und wie die CA Sie dabei unterstützt, neue Zertifikate für eine VPN-Verbindung zwischen zwei LANCOM Routern zu erstellen und zu nutzen (Zertifikatsverteilung über SCEP).



Es werden nur Menüpunkte erläutert, die zur erfolgreichen Durchführung des Tutorials dienen.

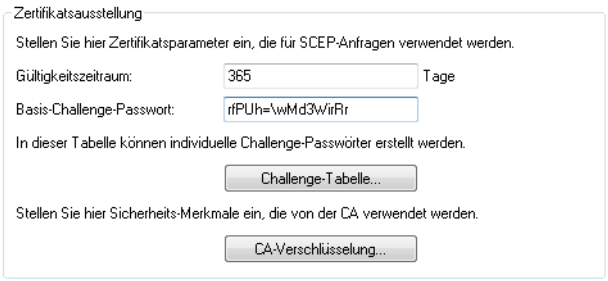
Auf allen Geräten müssen Datum und Uhrzeit gültig und die Certificate-Authority über "HTTPS" erreichbar sein.

1. Aktivieren Sie die Certificate-Authority in WEBconfig oder LANconfig und definieren Sie das Gerät als Hauptzertifizierungsstelle (Root-CA). Diese Einstellungen finden Sie unter **Zertifikate** > **Zertifizierungsstelle (CA)**.



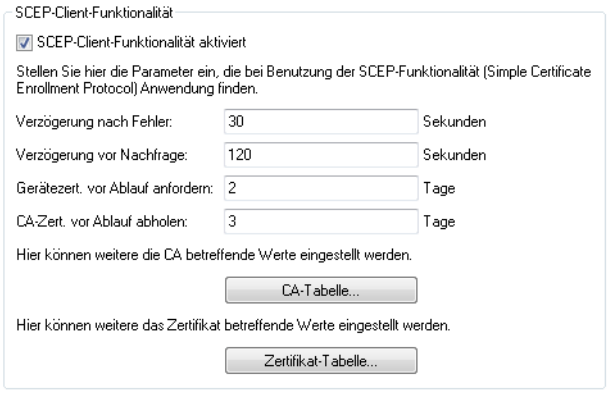
2. SCEP-Clients können Zertifikate durch SCEP (Simple Certificate Enrolement Protocol) automatisch beziehen. Dafür ist es erforderlich, dass Sie in der Haupt-Zertifizierungsstelle (Root-CA) ein Basis-Challenge-Passwort vergeben. Definieren Sie ein Kennwort unter **Zertifikate** > **Zertifikatsbehandlung**.

Schreiben Sie die Konfiguration nach der CA-Aktivierung zurück, generiert die CA automatisch ein Basis-Challenge-Passwort.

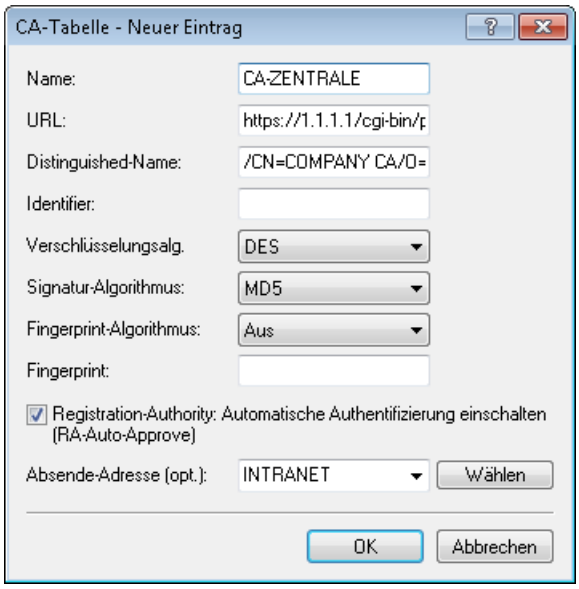


Sie haben nun die Möglichkeit, mit der CA Zertifikate für die VPN-Endpunkte zu erstellen, über die die Verbindung später eingerichtet wird.

3. Damit die VPN-Endpunkte über SCEP ein Zertifikat beziehen können, ist es erforderlich, den SCEP-Client auf jedem Endpunkt zu konfigurieren. Diese Einstellung finden Sie unter **Zertifikate** > **SCEP-Client**.



a) Definieren Sie unter **Zertifikate** > **SCEP-Client** > **CA-Tabelle** weiterführende Informationen zur Certificate-Authority. Diese Tabelle enthält Informationen zur CA, von der ein Zertifikat bezogen werden soll.



Name

Der Name kann frei gewählt werden und dient zur Identifizierung auf diesem Gerät.

URL

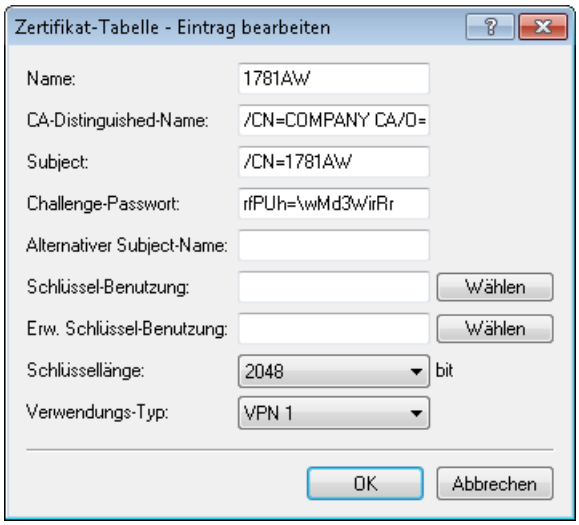
Die URL ist immer nach dem gleichen Schema aufgebaut:
`https://<IP-Adresse>/cgi-bin/pkiclient.exe`. Ersetzen Sie `<IP-Adresse>` mit der IPv4-Adresse, unter der die CA aus dem WAN erreichbar ist.

Ist der VPN-Endpunkt gleichzeitig die CA, ist es erforderlich, an dieser Stelle die Loopback-Adresse einzutragen.

Distinguished-Name

Der Distinguished-Name der CA (siehe Screenshot in Schritt 1).

b) Definieren Sie unter **Zertifikate** > **SCEP-Client** > **Zertifikat-Tabelle** weiterführende Informationen zu dem Zertifikat, das von der CA an dieses Gerät vergeben werden soll.



Name

Der Name kann frei gewählt werden und dient zur Identifizierung auf diesem Gerät.

CA-Distinguished-Name

Der CA-Distinguished-Name (siehe Screenshot in Schritt 1).

Subject

Der gewünschte Distinguished-Name des Zertifikates. In diesem Beispiel wird nur der Common-Name gesetzt.

Challenge-Passwort

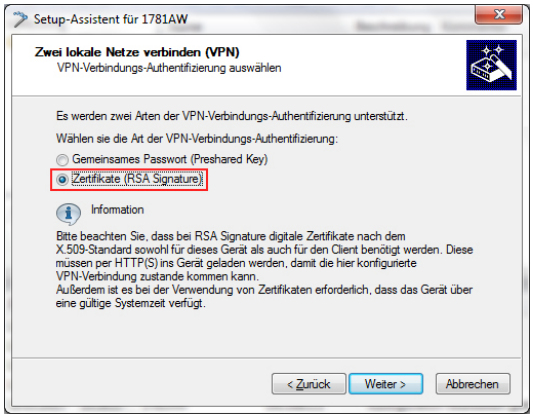
Das Basis-Challenge-Passwort, das auf der Certificate Authority vergeben wurde (siehe Schritt 2).

Verwendungstyp

Der Speicherplatz, in dem dieses Zertifikat abgelegt werden soll. In diesem Beispiel "VPN 1".

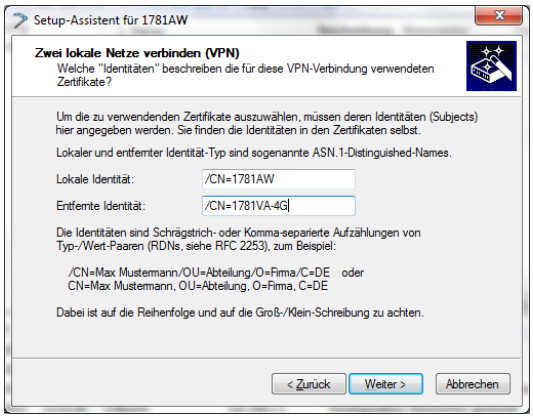
4. Wenn Sie den SCEP-Client auf jedem VPN-Endpunkt eingerichtet haben, stellen Sie eine VPN-Verbindung zwischen zwei VPN-Endpunkten her. Dies erfolgt über den Setup-Wizard **Zwei lokale Netze verbinden (VPN)**.

a) Wählen Sie als VPN-Verbindungs-Authentifizierung im Setup-Wizard **Zertifikate (RSA Signature)** aus.



b) Im Fenster **Lokale und entfernte Identitäten** geben Sie den sogenannten "ASN.1-Distinguished-Name" an. Dies ist der offizielle Name des Zertifikates plus aller zusätzlichen Informationen, die Sie in Schritt 3.b unter "Subject" angegeben haben. Bei dem Punkt **Lokale Identität** geben Sie die Informationen des Zertifikates an,

welches sich auf dem lokalen Gerät befindet. Der Punkt **Entfernte Identität** erhält die Zertifikat-Informationen des anderen VPN-Endpunktes.



c) Führen Sie abschließend den Wizard weiter aus. Bei dem anderen VPN-Endpunkt für diese VPN-Verbindung gehen Sie äquivalent vor.

3.2 Ergänzungen im Status-Menü

3.2.1 SCEP-CA

Zeigt eine Übersicht über SCEP-CA-Zertifikate und -Anfragen an und ermöglicht die Verwaltung dieser Zertifikate.

SNMP-ID:

1.61.2

Pfad Telnet:

Status > **Zertifikate**

Zertifikate

Zeigt aktuelle SCEP-CA-Zertifikate an und ermöglicht deren Verwaltung.

SNMP-ID:

1.61.2.1

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA**

Zertifikatsstatus-Tabelle

Diese Tabelle zeigt den Status der aktuellen SCEP-CA-Zertifikate an.

SNMP-ID:

1.61.2.1.1

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate**

Index

Zeigt den fortlaufenden Index des Eintrags an.

SNMP-ID:

1.61.2.1.1.1

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Seriennummer

Zeigt die Seriennummer des Zertifikats an.

Im Zertifikat erscheint dieser Eintrag unter `serialNumber=`.

SNMP-ID:

1.61.2.1.1.2

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Status

Zeigt den Status des Zertifikats an. Mögliche Werte sind:

- V: Gültig (valid)
- R: Widerrufen (revoked)
- P: Angefragt (pending)

SNMP-ID:

1.61.2.1.1.3

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Erstellungszeitpunkt

Zeigt den Erstellungszeitpunkt des Zertifikats an.

SNMP-ID:

1.61.2.1.1.4

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Ablaufzeit

Zeigt die Ablaufzeit des Zertifikats an.

Im Zertifikat erscheint dieser Eintrag unter `Validity`.

SNMP-ID:

1.61.2.1.1.5

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Rueckrufzeit

Zeigt die Rückrufzeit des Zertifikats an, falls es sich um ein widerrufenes Zertifikat handelt.

SNMP-ID:

1.61.2.1.1.6

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Rueckrufgrund

Zeigt den Rückrufgrund des Zertifikats an, falls es sich um ein widerrufenes Zertifikat handelt.

SNMP-ID:

1.61.2.1.1.7

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Mögliche Werte:

unspecified
Kein Grund angegeben.

keyCompromise
Der private Schlüssel ist kompromittiert.

cACompromise
Der private CA-Schlüssel ist kompromittiert.

affiliationChanged
Informationen über den Inhaber oder Aussteller des Zertifikats haben sich geändert.

superseded
Das Zertifikat ist veraltet und wurde durch ein neues Zertifikat ersetzt.

cessationOfOperation
Das Zertifikat ist für den ursprünglichen Zweck nicht mehr notwendig.

certificateHold
Das Zertifikat ist gesperrt, bis es endgültig widerrufen oder wieder freigegeben wird.

privilegeWithdrawn
Das Zertifikat enthält ein Recht, das nicht mehr gültig ist.

aACompromise
Der private AA-Schlüssel ist kompromittiert.

MAC-Adresse

Zeigt die MAC-Adresse des Gerätes an.

SNMP-ID:
1.61.2.1.1.8

Pfad Telnet:
Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Name

Zeigt den Namen an.

SNMP-ID:
1.61.2.1.1.9

Pfad Telnet:
Status > **Zertifikate** > **SCEP-CA** > **Zertifikate** > **Zertifikatsstatus-Tabelle**

Zertifikat-widerrufen

Mit dieser Aktion widerrufen Sie ein Zertifikat. Das ist dann notwendig, wenn das Zertifikat kompromittiert wurde oder sich Änderungen (Rechte, Informationen über den Aussteller) am Zertifikat ergeben haben.

SNMP-ID:
1.61.2.1.2

Pfad Telnet:
Status > **Zertifikate** > **SCEP-CA** > **Zertifikate**

Zertifikat-auf-Hold-setzen

Mit dieser Aktion setzen Sie ein Zertifikat auf „Hold". Das ist dann notwendig, wenn Sie zunächst den Zustand des Zertifikats klären wollen, es aber noch nicht sofort widerrufen möchten.

SNMP-ID:

1.61.2.1.3

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate**

Zertifikat-wieder-als-gueltig-erklaeren

Mit dieser Aktion erklären Sie ein zuvor auf „Hold" gesetztes Zertifikat wieder für gültig.

SNMP-ID:

1.61.2.1.4

Pfad Telnet:

Status > **Zertifikate** > **SCEP-CA** > **Zertifikate**

3.3 Ergänzungen im Setup-Menü

3.3.1 Web-Schnittstelle

In diesem Verzeichnis konfigurieren Sie die Einstellungen für die SCEP-CA-Web-Schnittstelle.

SNMP-ID:

2.39.2.14

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Profile

In dieser Tabelle legen Sie Profile mit gesammelten Zertifikats-Eigenschaften an.

Standardmäßig sind bereits drei Profile für gängige Anwendungsszenarien angelegt.

SNMP-ID:

2.39.2.14.1

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle**

Profilname

Vergeben Sie hier einen eindeutigen Namen des Profils.

SNMP-ID:

2.39.2.14.1.1

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Schluessel-Verwendung

Gibt an, für welche Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen zur Auswahl:

- critical
- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- cRLSign
- encipherOnly
- decipherOnly

Eine kommagetrennte Mehrfachauswahl ist möglich.

SNMP-ID:

2.39.2.14.1.2

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

critical,digitalSignature,keyEncipherment

Erw.-Schluessel-Verwendung

Gibt an, für welche erweiterte Verwendung das Profil einzusetzen ist. Die folgenden Verwendungen stehen zur Auswahl:

- critical

- serverAuth: SSL/TLS-Web-Server-Authentifizierung
- clientAuth: SSL/TLS-Web-Client-Authentifizierung
- codeSigning: Signierung von Programmcode
- emailProtection: E-Mail-Schutz (S/MIME)
- timeStamping: Daten mit zuverlässigen Zeitstempeln versehen
- msCodeInd: Microsoft Individual Code Signing (authenticode)
- msCodeCom: Microsoft Commercial Code Signing (authenticode)
- msCTLSign: Microsoft Trust List Signing
- msSGC: Microsoft Server Gated Crypto
- msEFS: Microsoft Encrypted File System
- nsSGC: Netscape Server Gated Crypto

Eine kommagetrennte Mehrfachauswahl ist möglich.

SNMP-ID:

2.39.2.14.1.3

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

RSA-Schluessellaenge

Gibt die Länge des Schlüssels an.

SNMP-ID:

2.39.2.14.1.4

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

1024
2048
3072
4096
8192

Default-Wert:

2048

Gueltigkeitsperiode

Gibt die Zeitdauer in Tagen an, für die der Schlüssel gültig ist. Nach Ablauf dieser Frist verliert der Schlüssel seine Gültigkeit, falls der Anwender ihn nicht vorher erneuert.

SNMP-ID:

2.39.2.14.1.5

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

365

CA

Gibt an, ob es sich um ein CA-Zertifikat handelt.

SNMP-ID:

2.39.2.14.1.6

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

ja
nein

Default-Wert:

nein

Passwort

Passwort, um die PKCS12-Zertifikatsdatei abzusichern.

SNMP-ID:

2.39.2.14.1.7

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Land

Geben Sie die Staatenkennung ein (z. B. „DE" für Deutschland).

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **C**= (**C**ountry).

SNMP-ID:

2.39.2.14.1.8

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

2 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Stadt

Geben Sie den Ort ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **L**= (**L**ocality).

SNMP-ID:

2.39.2.14.1.9

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Unternehmen

Geben Sie die das Zertifikat ausstellende Organisation ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **O**= (**O**rganization).

SNMP-ID:

2.39.2.14.1.10

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Abteilung

Geben Sie die das Zertifikat ausstellende Abteilung ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **OU=** (**O**rganization **U**nit).

SNMP-ID:

2.39.2.14.1.11

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Provinz-oder-Bundesland

Geben Sie das Bundesland ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter **ST=** (**ST**ate).

SNMP-ID:

2.39.2.14.1.12

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

E-Mail

Geben Sie eine E-Mail-Adresse ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter `emailAddress=`.

SNMP-ID:

2.39.2.14.1.13

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 36 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Nachname

Geben Sie einen Nachnamen ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter SN= (**S**ur**N**ame).

SNMP-ID:

2.39.2.14.1.14

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Seriennummer

Geben Sie eine Seriennummer ein.

Im Zertifikat erscheint dieser Eintrag unter `serialNumber=`.

SNMP-ID:

2.39.2.14.1.15

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Postleitzahl

Geben Sie die Postleitzahl des Ortes ein.

Im Subject oder Issuer des Zertifikats erscheint dieser Eintrag unter `postalCode=`.

SNMP-ID:

2.39.2.14.1.16

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 25 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Vorlage

Wählen Sie hier ggf. eine passende Profil-Vorlage aus.

In der Profil-Vorlage ist festgelegt, welche Zertifikatsangaben notwendig und welche änderbar sind. Die Vorlagen-Erstellung erfolgt unter **Setup** > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**.

SNMP-ID:

2.39.2.14.1.17

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Alternative-Subject-Name

Geben Sie hier den alternativen Subject-Namen an.

SNMP-ID:

2.39.2.14.1.18

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Profile**

Mögliche Werte:

max. 254 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Vorlage

In dieser Tabelle definieren Sie Vorlagen für Zertifikat-Profile.

Hier legen Sie fest, welche der Profileigenschaften erforderlich und welche durch den Anwender zu editieren sind. Die folgenden Optionen stehen zur Auswahl:

- Nein: Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.
- Fest: Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.
- Ja: Das Feld ist sichtbar und durch den Anwender änderbar.
- Erzwingen: Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

Standardmäßig ist bereits eine Vorlage „Default“ angelegt.

SNMP-ID:

2.39.2.14.2

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle**

Name

Vergeben Sie hier einen eindeutigen Namen für die Vorlage.

SNMP-ID:

2.39.2.14.2.1

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Schluessel-Verwendung

Gibt an, für welche Verwendung das Profil einzusetzen ist.

SNMP-ID:

2.39.2.14.2.2

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Erw.-Schluessel-Verwendung

Gibt an, für welche erweiterte Verwendung das Profil einzusetzen ist.

SNMP-ID:

2.39.2.14.2.3

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

RSA-Schluessellaenge

Gibt die Länge des Schlüssels an.

SNMP-ID:

2.39.2.14.2.4

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Gueltigkeitsperiode

Gibt die Zeitdauer in Tagen an, für die der Schlüssel gültig ist. Nach Ablauf dieser Frist verliert der Schlüssel seine Gültigkeit, falls der Anwender ihn nicht vorher erneuert.

SNMP-ID:

2.39.2.14.2.5

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

CA

Gibt an, ob es sich um ein CA-Zertifikat handelt.

SNMP-ID:

2.39.2.14.2.6

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Passwort

Passwort, um die PKCS12-Zertifikatsdatei abzusichern.

SNMP-ID:

2.39.2.14.2.7

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Land

Gibt die Staatenkennung an (z. B. „DE" für Deutschland).

SNMP-ID:

2.39.2.14.2.8

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Stadt

Gibt den Ort an.

SNMP-ID:

2.39.2.14.2.9

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Unternehmen

Gibt die das Zertifikat ausstellende Organisation an.

SNMP-ID:

2.39.2.14.2.10

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Abteilung

Gibt die das Zertifikat ausstellende Abteilung an.

SNMP-ID:

2.39.2.14.2.11

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Provinz-oder-Bundesland

Gibt das Bundesland an.

SNMP-ID:

2.39.2.14.2.12

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

E-Mail

Gibt die E-Mail-Adresse an.

SNMP-ID:

2.39.2.14.2.13

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Nachname

Gibt den Nachnamen an.

SNMP-ID:

2.39.2.14.2.14

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Seriennummer

Gibt die Seriennummer an.

SNMP-ID:

2.39.2.14.2.15

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Postleitzahl

Gibt die Postleitzahl an.

SNMP-ID:

2.39.2.14.2.16

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

Subject-Alternative-Name

Der „Subject-Alternative-Name" (SAN) verknüpft weitere Daten mit diesem Zertifikat.

SNMP-ID:

2.39.2.14.2.17

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Web-Schnittstelle** > **Vorlage**

Mögliche Werte:

ja

Das Feld ist sichtbar und durch den Anwender änderbar.

nein

Das Feld ist unsichtbar, der eingetragene Wert gilt als Defaultwert.

erforderlich

Das Feld ist sichtbar, der Anwender muss einen Wert eintragen.

fest

Das Feld ist sichtbar, aber nicht durch den Anwender änderbar.

Default-Wert:

ja

4 High Availability Clustering

Ab LCOS-Version 9.10 haben Sie mit der LANCOM WLC High Availability Clustering XL Option beziehungsweise der LANCOM VPN High Availability Clustering XL Option die Möglichkeit, mehrere Geräte zu einem Cluster zusammenfassen. Dies betrifft LANCOM WLAN-Controller (LANCOM WLC-4025+ und LANCOM WLC-4100) sowie LANCOM Central Site VPN Gateways (LANCOM 7100+ VPN und LANCOM 9100+ VPN). Dies ermöglicht Ihnen ein zentrales Management und einen komfortablen Konfigurationsabgleich (Config Sync) aller Cluster-Geräte. In WLAN-Controller-basierten Installationen profitieren Sie darüber hinaus von automatischer Lastverteilung, intelligenten Hochverfügbarkeitsszenarien sowie der Vergabe von Cluster-Zertifikaten.

4.1 Automatischer Konfigurationsabgleich (Config-Sync) mit der LANCOM WLC High Availability Clustering XL Option

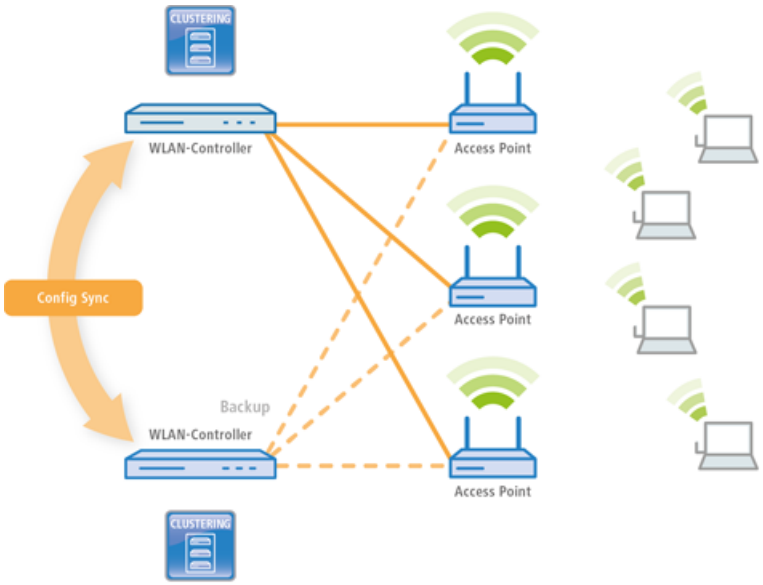
Anwendungsbeispiel WLAN-Controller:

WLAN-Infrastrukturen sind inzwischen integraler Bestandteil moderner Unternehmensnetzwerke. Mit zunehmendem Anspruch an die Verfügbarkeit einer WLAN-Lösung im Kontext des "All Wireless Office" steigt auch der Bedarf an zuverlässigen Backup- und Hochverfügbarkeitslösungen ("High Availability"). In WLAN-Infrastrukturen mit genau einem WLAN-Controller und verbundenen APs kommt es bisher bei Ausfall oder Wartung (z. B. Firmware-Update) des WLCs zu einem automatischen und autarken Weiterbetrieb der am WLC angebundenen APs. Das bedeutet, dass die APs im autarken Betriebsmodus nicht mehr auf die Funktionen zugreifen können, die auf dem WLC zentral verfügbar sind, wie z. B. Public Spot, IEEE 802.1X-Authentifizierung oder Layer-3-Tunnel.

Um dies zu vermeiden und den vollständigen Weiterbetrieb aller WLAN-Funktionen auch bei einer temporären Nichtverfügbarkeit eines WLCs aufrecht zu erhalten, können ein oder mehrere Redundanz- oder Backup-WLCs eingesetzt werden. Im Backup-Fall wechseln die APs automatisch vom temporär nicht verfügbaren WLC zu einem Backup-WLC. Hierfür ist auf dem Backup-WLC die gleiche Konfiguration (z. B. AP-Tabelle oder WLAN-Profile) wie auf dem primären WLC der APs erforderlich. Ersteinrichtung der WLCs sowie jede weitere Konfigurationsänderung muss auf den Geräten dabei jeweils separat und identisch erfolgen – für den Administrator ein enormer Aufwand. Die manuelle Pflege von Konfigurationen über mehrere identische Geräte kann im Backup-Fall mit veralteter bzw. nicht synchroner Konfiguration des Backup-WLCs zu einem fatalen Zustand der gesamten WLAN-Infrastruktur führen. Die dann startende Fehlersuche gestaltet sich in der Regel als Herausforderung. Auf der Anwenderseite von WLAN-Clients führt dies zu einem Ausfall der Produktivität, die unter Umständen unternehmensweit großen Schaden verursachen kann.

Neu mit der LANCOM WLC High Availability Clustering XL Option: Diese Software-Option ermöglicht die Gruppierung von mehreren WLCs zu einer hochverfügbaren Gerätegruppe (High Availability Cluster). Damit können Konfigurationsänderungen, Funktionen und Erweiterungen, die an einem WLC vorgenommen werden, automatisch auf die anderen WLCs des Clusters übertragen werden, ohne dass jedes einzelne Gerät manuell gemanagt werden muss.

Gemeinsame Parameter in einem Cluster (z. B. WLAN-Profile, AP-Tabellen oder Public Spot-Einstellungen) werden hierbei synchronisiert, individuelle Parameter (wie z. B. die IP-Adresse des WLCs) werden nicht untereinander ausgetauscht.



Mit der LANCOM WLC High Availability Clustering XL Option profitieren Sie von einer deutlich vereinfachten Administration sowie einer enormen Zeitersparnis, da Sie nur einen WLC des Clusters konfigurieren müssen. Die vorgenommenen Änderungen überträgt dieser WLC dann automatisch auf die anderen Cluster-Geräte. In Hinblick auf das oben beschriebene Szenario verbinden sich nun bei Ausfall oder Wartung (z. B. Firmware-Update) eines WLCs die APs automatisch mit einem anderen WLC, der dank Config Sync ganz ohne Zutun des Administrators bereits die identische Konfiguration besitzt. Dadurch wird eine komfortable Hochverfügbarkeit realisiert.

Die Voraussetzungen für eine gültige Gruppenmitgliedschaft eines Gerätes sind:

- Es muss eine LANCOM WLC High Availability Clustering XL Option vorhanden sein (ab LCOS-Version 9.10).
- Es muss eine IP-Kommunikation zu allen anderen Geräten möglich sein, z. B. über LAN, WAN oder VPN.
- Es muss in der Gruppenliste aufgeführt sein, die in jedem Gerät gespeichert ist.
- Es muss ein gültiges Zertifikat vorhanden sein.
- Es muss sich als Gruppenmitglied per Zertifikat authentifizieren können.

4.2 Automatischer Konfigurationsabgleich (Config-Sync) mit der LANCOM VPN High Availability Clustering XL Option

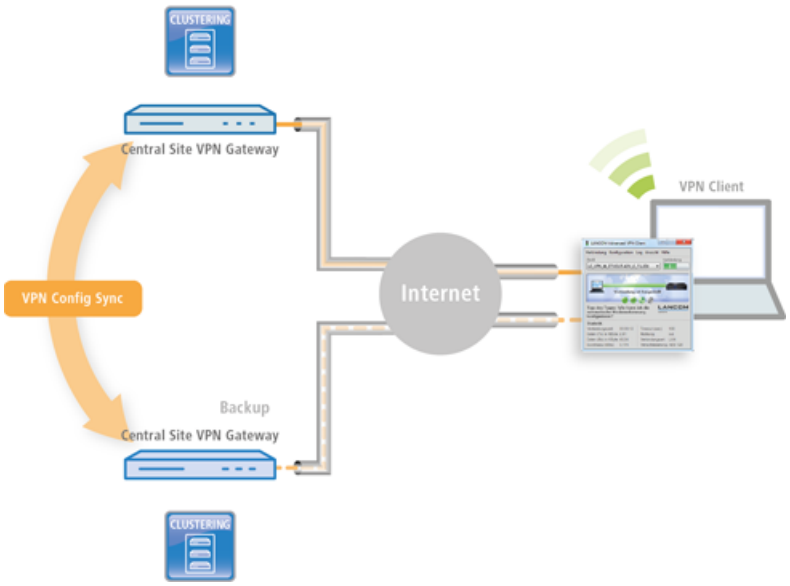
Anwendungsbeispiel VPN:

VPN-Infrastrukturen sind seit langer Zeit Bestandteil von Unternehmensnetzwerken. Die Ansprüche an die Verfügbarkeit von VPN-Gateways sind in den letzten Jahren enorm gestiegen. Wurden VPN-Lösungen im Unternehmensbereich in der Vergangenheit häufig temporär z. B. von Außendienstmitarbeitern mit VPN-Client genutzt, so werden heute Home Offices oder Zweigniederlassungen dauerhaft per VPN-Tunnel an die Zentrale angebunden. Genutzt werden dann beispielsweise Sprachdienste (VoIP), Datenbankanwendungen oder Dateidienste. Mit zunehmender Abhängigkeit von VoIP-Diensten oder kritischen Unternehmensanwendungen steigt auch der Bedarf an zuverlässigen Backup- und Hochverfügbarkeitslösungen ("High Availability") der VPN-Lösung.

Um VPN-Dienste in größeren kritischen Netzwerkinfrastrukturen hochverfügbar zu gestalten, ist der Einsatz eines oder mehrerer Backup-VPN-Gateways neben dem primären VPN-Gateway empfehlenswert. So kann bei Ausfall oder Wartung eines Central-Site-VPN-Gateways ein anderes Gerät als Backup dienen. Die VPN-Verbindung wird automatisch über das erreichbare Backup-Central-Site-VPN-Gateway aufgebaut.

Hierfür ist auf dem Backup-Central-Site-VPN-Gateway die gleiche Konfiguration wie auf dem primären Central-Site-VPN-Gateway erforderlich. Speziell die VPN-Benutzerdaten oder die Firewall-Konfiguration müssen auf beiden Geräten vorhanden sein, damit ein Benutzer authentifiziert werden kann und seine Dienste korrekt bereitgestellt werden können. Dies erfordert eine manuelle Einrichtung jedes einzelnen Gerätes – für den Administrator ein enormer Aufwand.

Neu mit der LANCOM VPN High Availability Clustering XL Option: Diese Option ermöglicht die Gruppierung von mehreren Central Site VPN Gateways zu einem Cluster. Damit können Konfigurationsänderungen, Funktionen und Erweiterungen, die an einem Central-Site-VPN-Gateway vorgenommen werden, automatisch auf die anderen übertragen werden, ohne dass jedes einzelne Gerät manuell gemanagt werden muss. Gemeinsame Parameter in einem Cluster (z. B. VPN-Benutzerdatenbank und Firewall) werden hierbei synchronisiert, individuelle Parameter (wie z. B. die IP-Adresse) werden nicht untereinander ausgetauscht.



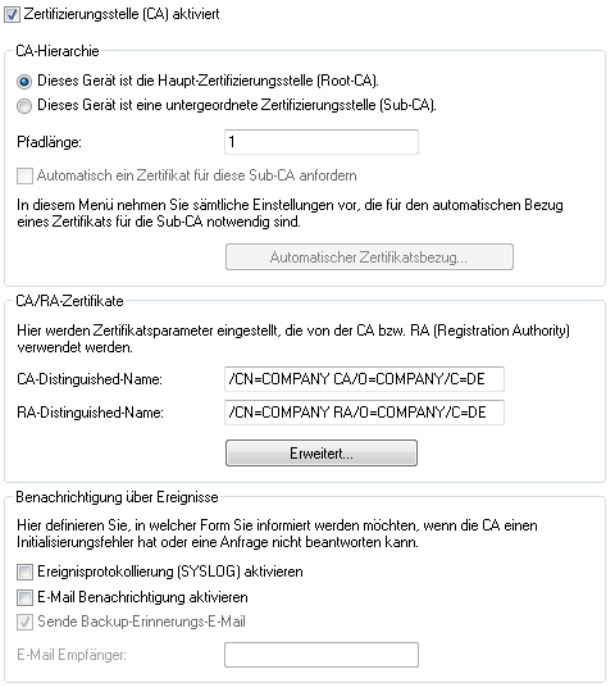
Die Voraussetzungen für eine gültige Gruppenmitgliedschaft eines Gerätes sind:

- Es muss eine LANCOM VPN High Availability Clustering XL Option vorhanden sein (ab LCOS-Version 9.10).
- Es muss eine IP-Kommunikation zu allen anderen Geräten möglich sein, z. B. über LAN, WAN oder VPN.
- Es muss in der Gruppenliste aufgeführt sein, die in jedem Gerät gespeichert ist.
- Es muss ein gültiges Zertifikat vorhanden sein.
- Es muss sich als Gruppenmitglied per Zertifikat authentifizieren können.

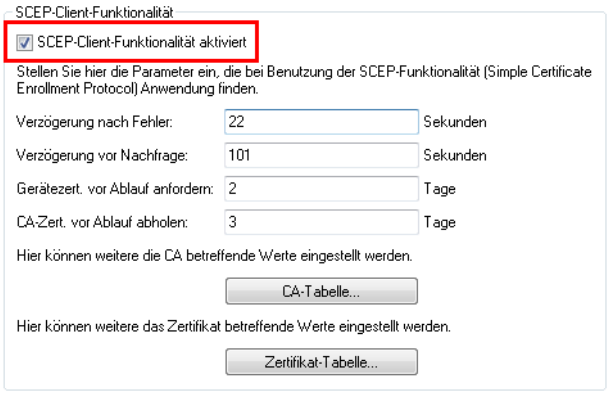
4.3 Konfigurations-Synchronisation einrichten

Damit die Konfigurations-Synchronisation möglich ist, müssen alle zu konfigurierenden Geräte gültige Zertifikate vorweisen können. Für eine einfache Zertifikatsverteilung konfigurieren Sie daher zuerst auf einem Gerät eine SCEP-CA.

1. Dazu ist es notwendig, unter **Zertifikate** > **SCEP-Server** den SCEP-Server zu aktivieren. Wenn Sie die Konfigurations-Synchronisation auf einem WLC einrichten, ist der SCEP-Server höchstwahrscheinlich schon aktiv.



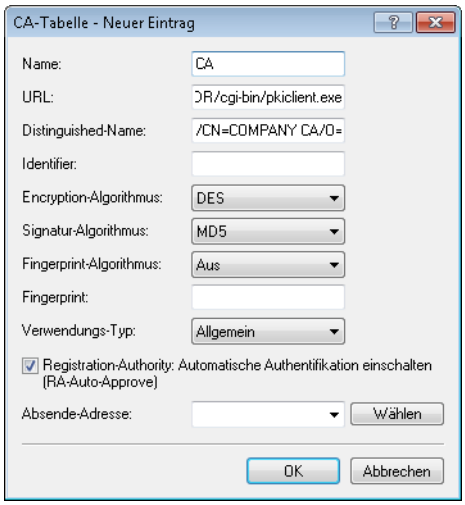
2. Aktivieren Sie anschließend auf jedem Gerät, auf dem Sie die Konfigurations-Synchronisation verwenden möchten (inklusive des SCEP-CA-Gerätes), die SCEP-Client-Funktion unter **Zertifikate** > **SCEP-Client**. Wenn Sie die Konfigurations-Synchronisation auf einem WLC einrichten, ist der SCEP-Client höchstwahrscheinlich schon aktiv.



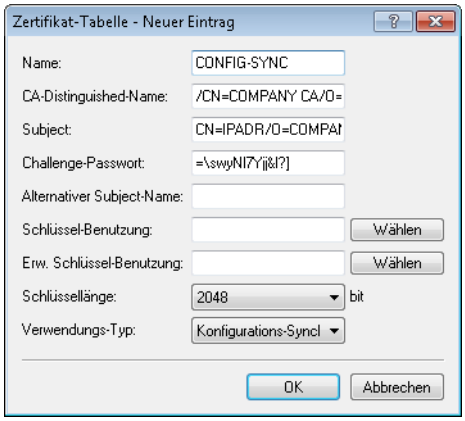
3. Ergänzen Sie die **CA-Tabelle** um einen neuen Eintrag für den SCEP-Server.

   Die Werte für die CA-Tabelle entsprechen den Einstellungen des SCEP-Servers aus Schritt 1 und sind somit für alle Stationen identisch. Für die URL tragen Sie `http://IPADR/cgi-bin/pkiclient.exe` ein, wobei Sie `IPADR` durch die IP-Adresse des als SCEP-CA konfigurierten Geräts ersetzen.

Wenn Sie die Konfigurations-Synchronisation auf einem WLC einrichten, ist ein entsprechender Eintrag schon für den WLC-Betrieb vorhanden; dieser ist auch für den Bezug eines Zertifikates für die Konfigurations-Synchronisation einsetzbar, so dass in diesem Fall in der CA-Tabelle keine Änderung notwendig ist.



4. Ergänzen Sie die **Zertifikat-Tabelle** im SCEP-Client um einen neuen Eintrag für den Bezug eines Konfigurations-Synchronisation-Zertifikates. Als **CA-Distinguished-Name** verwenden Sie den bereits bei Erstellung des CA-Tabellen-Eintrages verwendeten Namen.

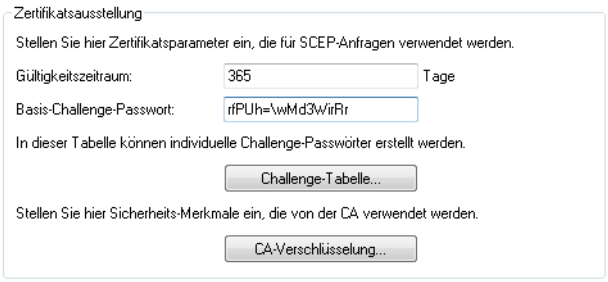


Als Subject tragen Sie die jeweils geräteeigene IP-Adresse ein (z. B. `/CN=IPADR /O=COMPANY/C=DE`, wobei Sie `IPADR` durch die IP-Adresse des als SCEP-CA konfigurierten Geräts ersetzen.

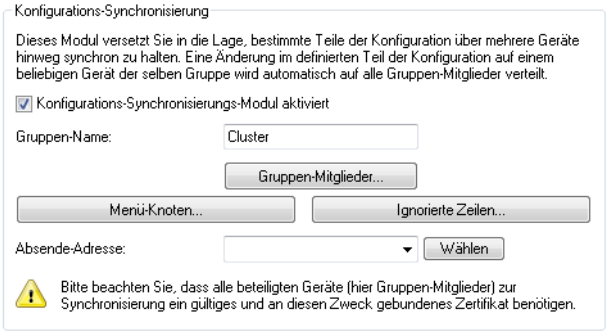
Es ist für die Funktion der Konfigurations-Synchronisation zwingend erforderlich, dass die IP-Adresse des Gerätes im Subject des Zertifikats enthalten ist.

Als **Verwendungs-Typ** geben Sie „Konfigurations-Synchronisation" an. Passen Sie außerdem die **Schlüssellänge** auf „2048 bit" an. Den **Namen** des Tabelleneintrags können Sie frei wählen.

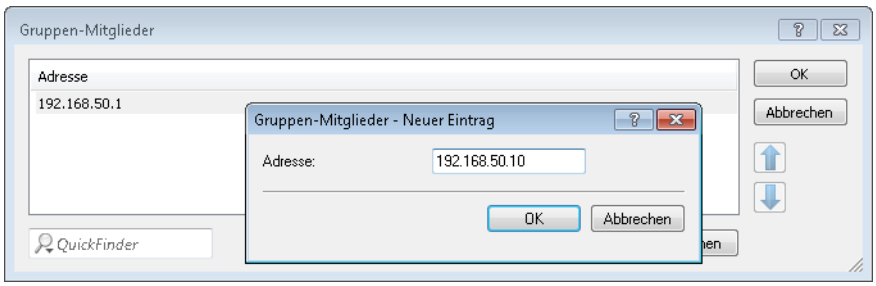
Das Challenge-Passwort des als SCEP-CA konfigurierten Gerätes finden Sie in dessen Konfiguration unter **Zertifikate** > **Zertifikats-Behandlung** > **Basis-Challenge-Passwort**.



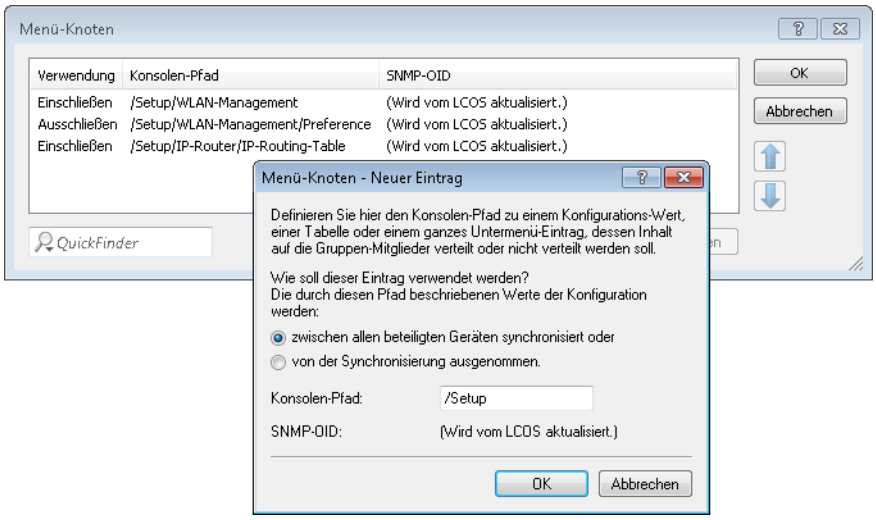
5. Hiermit ist die Einrichtung der SCEP-CA sowie des SCEP-Clients zum Bezug der Konfigurations-Synchronisation-Zertifikate abgeschlossen. Sie können die Konfiguration an diesem Punkt bereits einmal in das Gerät zurückschreiben, um den Bezug der Zertifikate zu bewirken.
6. Aktivieren Sie nun die Konfigurations-Synchronisation unter **Management** > **Synchronisierung** mit der Option **Konfigurations-Synchronisierungs-Modul aktiviert**. Unter **Gruppen-Name** können Sie ebenfalls einen benutzerdefinierten Namen für den Cluster festlegen, der anschließend auch in der LANconfig-Geräteliste erscheint.



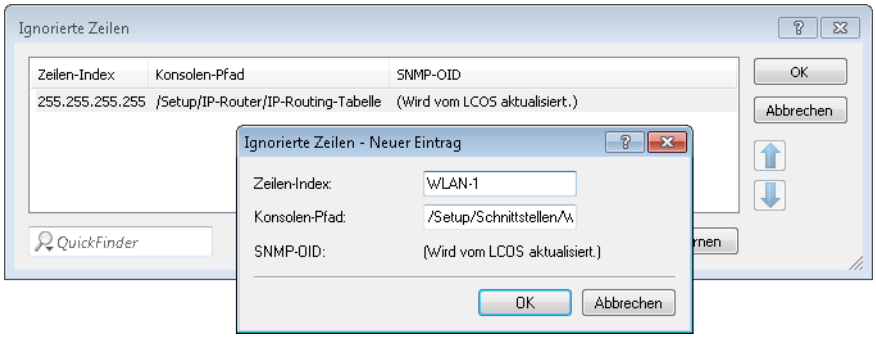
7. Tragen Sie unter **Gruppen-Mitglieder** die IP-Adressen **aller** Geräte ein, die Mitglieder des Clusters werden sollen.



8. Definieren Sie unter **Menü-Knoten** die zu synchronisierenden Menüs. Möchten Sie Menüknoten explizit von der Synchronisation ausnehmen, wählen Sie unter **Verwendung** "von der Synchronisation ausgenommen".



Definieren Sie optional unter "Ignorierte Zeilen", welche Zeilen einer Tabelle von der Synchronisation ausgenommen werden sollen. Beispiel: Default-Route auf VPN-Gateways, die für jedes Gateway unterschiedlich sein soll. Die restliche Routing-Tabelle kann durch einen Eintrag in den **Menü-Knoten** synchronisiert werden.



9. Die Einrichtung der Konfigurations-Synchronisation ist auf diesem Gerät nun abgeschlossen. Sie können die Konfiguration nun in das Gerät zurückschreiben.
10. Führen Sie die Schritte 2 bis 9 auf den weiteren zum Cluster gehörigen Geräten aus. Verweisen Sie dabei bei der Konfiguration des SCEP-Clients, wie oben angegeben, auf die SCEP-CA des ersten Gerätes.
11. Starten Sie nun den Cluster auf dem Gerät, welches initial seine Konfiguration auf alle Mitglieder des Clusters verteilen soll. Wählen Sie dazu in der LANconfig-Geräteliste im Kontextmenü des Gerätes **[Cluster starten…]**.
12. Der Cluster ist nun in Betrieb. Sie können den Zustand des Clusters in der WEBconfig unter **Status** > **Config** > **Sync** > **Zustand** überprüfen. Änderungen an der Konfiguration können nun an jedem Mitglied des Clusters vorgenommen werden und werden auf die anderen Mitglieder synchronisiert.

Beachten Sie folgende Anforderungen:

- Auf den beteiligten Geräten muss die korrekte Uhrzeit gesetzt sein (Zertifikatsprüfung).
- Die eigene IP-Adresse des Gerätes muss im Subject des eigenen Zertifikates auftauchen.
- Die zu synchronisierenden Menübäume müssen auf beiden Geräten gleich sein (bei unterschiedlichen Firmware-Versionen oder Geräte-Optionen nicht immer der Fall).
- Wenn die Konfiguration der Konfigurations-Synchronisation (Menüknoten etc.) geändert wird, nachdem der Cluster bereits gestartet wurde, muss der Cluster erneut gestartet werden.

4.4 Ergänzungen im Status-Menü

4.4.1 Sync

Dieses Menü zeigt Statuswerte des automatischen Konfigurationsabgleiches an.

SNMP-ID:

1.11.51

Pfad Telnet:

Status > **Config**

Zustand

Dieser Eintrag zeigt Ihnen den Geräte-Zustand beim automatischen Konfigurationsabgleich an.

SNMP-ID:

1.11.51.1

Pfad Telnet:

Status > **Config** > **Sync**

Mögliche Werte:

Aus
PKCS#12-Datei-fehlerhaft
TCP-Listen-gescheitert
Noch-nicht-gestartet
Inkompatible-Firmware
Inkompatible-Menueknoten
Eigene-Adresse-falsch
Kein-Schnappschuss
Zeit-unbekannt
OK

Neuer-Cluster

Diese Tabelle zeigt Ihnen die Werte des aktuellen automatischen Konfigurationsabgleiches an.

SNMP-ID:

1.11.51.2

Pfad Telnet:

Status > **Config** > **Sync**

Name

Dieser Eintrag zeigt Ihnen den Namen des aktuellen Konfigurationsabgleiches an.

SNMP-ID:

1.11.51.2.1

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster**

Gruppen-Mitglieder

Dieser Eintrag zeigt Ihnen Informationen über die Gruppenmitglieder des Clusters an.

SNMP-ID:

1.11.51.2.2

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster**

ID

Dieser Eintrag zeigt Ihnen die ID des Eintrages an.

SNMP-ID:

1.11.51.2.2.2

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster** > **Gruppen-Mitglieder**

Adresse

Dieser Eintrag zeigt Ihnen die Adresse des Gruppenmitgliedes an.

SNMP-ID:

1.11.51.2.2.3

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster** > **Gruppen-Mitglieder**

Dieses-Geraet

Dieser Eintrag zeigt Ihnen an, ob es sich dabei um dieses Gerät handelt.

SNMP-ID:

1.11.51.2.2.4

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster** > **Gruppen-Mitglieder**

Mögliche Werte:

Ja
Nein

Menueknoten

Dieser Eintrag zeigt Ihnen die Menüknoten an, die im automatischen Konfigurationsabgleich enthalten sind.

SNMP-ID:

1.11.51.2.3

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster**

ID

Dieser Eintrag zeigt Ihnen die ID des Eintrags an.

SNMP-ID:

1.11.51.2.3.2

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Pfad

Dieser Eintrag zeigt Ihnen den Pfad des Menü-Knotens an.

SNMP-ID:

1.11.51.2.3.3

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

SNMP-OID

Dieser Eintrag zeigt Ihnen die SNMP-ID des Menü-Knotens an.

SNMP-ID:

1.11.51.2.3.4

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Indexspalten

Dieser Eintrag zeigt Ihnen die Index-Spalten des Menü-Knotens an.

SNMP-ID:

1.11.51.2.3.5

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Ignorierte-Zeilen

Dieser Eintrag zeigt Ihnen Informationen zu Tabellen-Zeilen an, die von diesem automatischen Konfigurationsabgleich ausgeschlossen sind.

SNMP-ID:

1.11.51.2.4

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer Cluster**

ID

Dieser Eintrag zeigt Ihnen die ID des Eintrages an.

SNMP-ID:

1.11.51.2.4.2

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer Cluster** > **Ignorierte-Zeilen**

Pfad

Dieser Eintrag zeigt Ihnen den Pfad des Tabellen-Knotens an.

SNMP-ID:

1.11.51.2.4.3

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer Cluster** > **Ignorierte-Zeilen**

SNMP-OID

Dieser Eintrag zeigt Ihnen die SNMP-ID des Tabellen-Knotens an.

SNMP-ID:

1.11.51.2.4.4

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer Cluster** > **Ignorierte-Zeilen**

Indexspalten

Dieser Eintrag zeigt Ihnen die Tabellenzeile an, die vom automatischen Konfigurationsabgleich ausgeschlossen ist.

SNMP-ID:

1.11.51.2.4.5

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer Cluster** > **Ignorierte-Zeilen**

Zustand

Dieser Eintrag zeigt Ihnen den Zustand des automatischen Konfigurationsabgleiches an.

SNMP-ID:

1.11.51.2.5

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster**

Mögliche Werte:

Aus
Ungueltig
Laeuft-nicht
Laeuft
Geaendert

Info

Dieser Eintrag zeigt Ihnen allgemeine Informationen zum automatischen Konfigurationsabgleich an.

SNMP-ID:

1.11.51.2.6

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster**

Start

Mit dieser Aktion verteilen Sie die Konfiguration des Gerätes auf alle anderen Mitglieder der Gruppe. Gleichzeitig ist dieser Startzeitpunkt der Referenzpunkt für die Gruppe. Ab diesem Zeitpunkt gilt der Cluster als aktiviert.

SNMP-ID:

1.11.51.2.7

Pfad Telnet:

Status > **Config** > **Sync** > **Neuer-Cluster**

Clusterzeit

Dieser Eintrag zeigt Ihnen die Clusterzeit an.

SNMP-ID:

1.11.51.3

Pfad Telnet:

Status > **Config** > **Sync**

Lokale-Konfiguration

Dieses Menü enthält Informationen über die lokale Gerätekonfiguration.

SNMP-ID:

1.11.51.4

Pfad Telnet:

Status > **Config** > **Sync**

Beobachtete-Aenderungen

Dieser Eintrag zeigt Ihnen an, welche Änderungen Sie beobachten.

SNMP-ID:

1.11.51.4.1

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration**

Beobachtet-um

Dieser Eintrag zeigt den Zeitpunkt an, zu dem eine Änderung durch ein anderes Gerät erfolgte.

SNMP-ID:

1.11.51.4.1.2

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Beobachtete-Aenderungen**

Pfad

Dieser Eintrag zeigt den geänderten Pfad an.

SNMP-ID:

1.11.51.4.1.4

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Beobachtete-Aenderungen**

Typ

Dieser Eintrag zeigt den Typ der Änderung an.

SNMP-ID:

1.11.51.4.1.5

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Beobachtete-Aenderungen**

Mögliche Werte:

Setze-Skalar
Die Änderung betraf einen Wert.

Setze-Zeile
Die Änderung fügte eine Tabellenzeile hinzu.

Loesche-Zeile
Die Änderung entfernte eine Tabellenzeile.

Wert

Dieser Eintrag zeigt den geänderten Wert an.

SNMP-ID:

1.11.51.4.1.6

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Beobachtete-Aenderungen**

Angewandte-Aenderungen

Dieser Eintrag zeigt an, welche Konfigurationsänderungen dieses Gerät veranlasst hat.

SNMP-ID:

1.11.51.4.2

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration**

Angewandt-um

Dieser Eintrag zeigt den Zeitpunkt an, zu dem eine Änderung durch dieses Gerät erfolgte.

SNMP-ID:

1.11.51.4.2.2

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Angewandte-Aenderungen**

Pfad

Dieser Eintrag zeigt den geänderten Pfad an.

SNMP-ID:

1.11.51.4.2.4

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Angewandte-Aenderungen**

Typ

Dieser Eintrag zeigt den Typ der Änderung an.

SNMP-ID:

1.11.51.4.2.5

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Angewandte-Aenderungen**

Mögliche Werte:

Setze-Skalar
Die Änderung betraf einen Wert.

Setze-Zeile
Die Änderung fügte eine Tabellenzeile hinzu.

Loesche-Zeile
Die Änderung entfernte eine Tabellenzeile.

Wert

Dieser Eintrag zeigt den geänderten Wert an.

SNMP-ID:

1.11.51.4.2.6

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Angewandte-Aenderungen**

Ergebnis

Dieser Eintrag zeigt das Ergebnis der Änderung an.

SNMP-ID:

1.11.51.4.2.7

Pfad Telnet:

Status > **Config** > **Sync** > **Lokale-Konfiguration** > **Angewandte-Aenderungen**

Mögliche Werte:

OK
Konfigurationsabgleich war erfolgreich.

OK(Msg-gesendet)
OK(Zeilenende)
OK(Schliessen)
OK(Abbrechen)
OK(Mehr)
OK(Gestartet)
Konfigurationsabgleich ist gestartet.

Kein-Login

Syntax-Fehler

Kein-Pfad-angegeben

Der Konfigurationsabgleich beinhaltet keine Pfadangabe.

Pfadteil-fehlt

Der Konfigurationsabgleich beinhaltet eine fehlerhafte Pfadangabe.

Pfadteil-mehrdeutig

Eine Pfadangabe im Konfigurationsabgleich ist nicht eindeutig.

Kein-Menuestack

Nicht-setzbar

Der Konfigurationsabgleich versucht, einen Wert zu setzen oder zu ändern, bei dem das nicht möglich ist.

Wert-ungueltig

Der Konfigurationsabgleich versucht, einen Wert außerhalb des gültigen Bereiches zu setzen.

Nur-Lese-Verbindung

Die Verbindung zu einem Gerät besitzt keine Schreibrechte.

Nicht-durchfuehrbar

Die Verbindung zu einem Gerät besitzt keine Ausführungsrechte.

Tabelle-ist-voll

Der Konfigurationsabgleich vesucht, eine weitere Zeile in ein volle Tabelle zu schreiben.

Wurde-ignoriert

Passwort-falsch

Der Anmeldeversuch an einem anderen Gerät scheiterte aufgrund eines falschen Passwortes.

Pfadname-ohne-Inhalt

Der Pfad eines Konfigurationsabgleiches ist ohne den zu ändernden Wert angegeben.

Zeilenende

Laufender-Cluster

Dieses Menü enthält Informationen über einen laufenden Konfigurationsabgleich.

SNMP-ID:

1.11.51.5

Pfad Telnet:

Status > **Config** > **Sync**

ID

Dieser Eintrag zeigt Ihnen die ID des laufenden Konfigurationsabgleiches an.

SNMP-ID:

1.11.51.5.1

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster**

Name

Dieser Eintrag zeigt Ihnen den Namen des laufenden Konfigurationsabgleiches an.

SNMP-ID:

1.11.51.5.2

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster**

Gruppen-Mitglieder

Diese Tabelle enthält die Gruppen-Mitglieder des laufenden Konfigurationsabgleiches.

SNMP-ID:

1.11.51.5.3

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster**

ID

Dieser Eintrag zeigt Ihnen die ID des Eintrages an.

SNMP-ID:

1.11.51.5.3.2

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Gruppen-Mitglieder**

Adresse

Dieser Eintrag zeigt Ihnen die Adresse des Gerätes an.

SNMP-ID:

1.11.51.5.3.3

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Gruppen-Mitglieder**

Dieses-Geraet

Dieser Eintrag zeigt an, ob es sich bei dem Eintrag um dieses Gerät handelt.

SNMP-ID:

1.11.51.5.3.4

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Gruppen-Mitglieder**

Mögliche Werte:

Ja
Nein

Menueknoten

Diese Tabelle enthält die Menü-Knoten des laufenden Konfigurationsabgleiches.

SNMP-ID:

1.11.51.5.4

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster**

ID

Dieser Eintrag zeigt die ID dieses Eintrages an.

SNMP-ID:

1.11.51.5.4.2

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Menueknoten**

Pfad

Dieser Eintrag zeigt den Pfad des Menüknotens an.

SNMP-ID:

1.11.51.5.4.3

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Menueknoten**

SNMP-OID

Dieser Eintrag zeigt die SNMP-ID des Menüknotens an.

SNMP-ID:

1.11.51.5.4.4

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Menueknoten**

Indexspalten

Dieser Eintrag zeigt Ihnen die Index-Spalten des Menü-Knotens an.

SNMP-ID:

1.11.51.5.4.5

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Menueknoten**

Ignorierte-Zeilen

Diese Tabelle enthält die ignorierten Tabellenzeilen des laufenden Konfigurationsabgleiches.

SNMP-ID:

1.11.51.5.5

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster**

ID

Dieser Eintrag zeigt die ID dieses Eintrages an.

SNMP-ID:

1.11.51.5.5.2

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Ignorierte-Zeilen**

Pfad

Dieser Eintrag zeigt den Pfad des Tabellenknotens an.

SNMP-ID:

1.11.51.5.5.3

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Ignorierte-Zeilen**

SNMP-OID

Dieser Eintrag zeigt die SNMP-ID des Tabellenknotens an.

SNMP-ID:

1.11.51.5.5.4

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Ignorierte-Zeilen**

Zeilenindex

Dieser Eintrag zeigt Ihnen die Tabellenzeile an, die vom automatischen Konfigurationsabgleich ausgeschlossen ist.

SNMP-ID:

1.11.51.5.5.5

Pfad Telnet:

Status > **Config** > **Sync** > **Laufender-Cluster** > **Ignorierte-Zeilen**

Konfigurations-Historie

Dieses Menü enthält Informationen über die Konfigurations-Historie des Gerätes.

SNMP-ID:

1.11.51.6

Pfad Telnet:

Status > **Config** > **Sync**

Schnappschuss-empfangen-um

Dieser Eintrag zeigt Ihnen an, zu welchem Zeitpunkt das Gerät einen Schnappschuss empfangen hat.

SNMP-ID:

1.11.51.6.1

Pfad Telnet:

Status > **Config** > **Sync** > **Konfigurations-Historie**

Schnappschuss-Zeitstempel

Dieser Eintrag enthält den Zeitstempel des erhaltenen Schnappschusses.

SNMP-ID:

1.11.51.6.2

Pfad Telnet:

Status > **Config** > **Sync** > **Konfigurations-Historie**

Schnappschuss

Diese Tabelle zeigt Ihnen Informationen zum zuletzt angelegten Schnappschuss an.

SNMP-ID:

1.11.51.6.3

Pfad Telnet:

Status > **Config** > **Sync** > **Konfigurations-Historie**

Pfad

Dieser Eintrag enthält den Pfad zu einem Menüknoten.

SNMP-ID:

1.11.51.6.3.2

Pfad Telnet:

Status > **Config** > **Sync** > **Konfigurations-Historie** > **Schnappschuss**

Wert

Dieser Eintrag enthält den Wert des entsprechenden Pfades.

SNMP-ID:

1.11.51.6.3.3

Pfad Telnet:

Status > **Config** > **Sync** > **Konfigurations-Historie** > **Schnappschuss**

Aenderungen

Diese Tabelle enthält Änderungen an der Konfiguration seit dem letzten Schnappschuss.

SNMP-ID:

1.11.51.6.4

Pfad Telnet:

Status > **Config** > **Sync** > **Konfigurations-Historie**

Schnappschuss-erneuern

Mit Anklicken dieser Schaltfläche erstellen Sie einen neuen Schnappschuss der aktuellen Geräte-Konfiguration.

SNMP-ID:

1.11.51.6.5

Pfad Telnet:

Status > **Config** > **Sync** > **Konfigurations-Historie**

Replikate

Diese Tabelle enthält Informationen zu Geräten, die sich am automatischen Konfigurationsabgleich beteiligen.

SNMP-ID:

1.11.51.7

Pfad Telnet:

Status > **Config** > **Sync**

ID

Dieser Eintrag enthält die ID des Eintrages.

SNMP-ID:

1.11.51.7.2

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

Adresse

Dieser Eintrag enthält die Adresse des Gerätes.

SNMP-ID:

1.11.51.7.3

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

Aufgeloeste-Adresse

Dieser Eintrag enthält die aufgelöste IPv4- oder IPv6-Adresse des Gerätes.

SNMP-ID:

1.11.51.7.4

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

Verbindungszustand

Dieser Eintrag enthält den Verbindungszustand zum entfernten Gerät.

SNMP-ID:

1.11.51.7.5

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

Mögliche Werte:

Nicht-verbunden
DNS-Aufloesung
Verbindungsaufbau
OK
Adresse-nicht-aufloesbar
TCP-Aufbau-gescheitert
TLS-Aufbau-gescheitert
Von-Replikat-geschlossen
Inkompatible-Firmware
Uebertragungsfehler

Zustand

Dieser Eintrag enthält den Zustand des entfernten Gerätes.

SNMP-ID:

1.11.51.7.6

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

Mögliche Werte:

Unbekannt
Fehlende-Nachrichten
Fehlende-Updates
Alter-Cluster
Neuer-Cluster
Kein-Schnappschuss
Zeit-unbekannt
OK

Clusterzeit

Dieser Eintrag enthält die Zeit des Konfigurationsabgleiches.

SNMP-ID:

1.11.51.7.7

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

Letzte-Nachricht-empfangen-um

Dieser Eintrag zeigt an, wann das entfernte Gerät die letzte Nachricht empfangen hat.

SNMP-ID:

1.11.51.7.8

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

Letztes-Update-empfangen-um

Dieser Eintrag zeigt an, wann das entfernte Gerät das letzte Konfigurations-Update empfangen hat.

SNMP-ID:

1.11.51.7.10

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

Letzte-Nachricht-gesendet-um

Dieser Eintrag zeigt an, wann das entfernte Gerät die letzte Nachricht gesendet hat.

SNMP-ID:

1.11.51.7.12

Pfad Telnet:

Status > **Config** > **Sync** > **Replikate**

4.5 Ergänzungen im Setup-Menü

4.5.1 Config-Sync

Gibt an, ob über diese Schnittstelle ein Config-Sync (eingeschränkt) möglich ist.

SNMP-ID:

2.11.15.10

Pfad Telnet:

Setup > **Config** > **Zugriffstabelle**

Mögliche Werte:

VPN
ja

Default-Wert:

ja

Mögliche Werte:

Read
nein

4.5.2 Sync

In diesem Verzeichnis konfigurieren Sie den automatischen Konfigurationsabgleich.

SNMP-ID:

2.11.51

Pfad Telnet:

Setup > **Config**

Aktiv

Aktiviert oder deaktiviert den automatischen Konfigurationsabgleich.

SNMP-ID:

2.11.51.1

Pfad Telnet:

Setup > **Config** > **Sync**

Mögliche Werte:

Nein
ja

Default-Wert:

Nein

Neuer-Cluster

Hier konfigurieren Sie den Umfang eines Konfigurationsabgleiches.

SNMP-ID:

2.11.51.2

Pfad Telnet:

Setup > **Config** > **Sync**

Name

Vergeben Sie eine Bezeichnung für diesen Eintrag.

SNMP-ID:

2.11.51.2.1

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

Mögliche Werte:

max. 254 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

Default

Gruppen-Mitglieder

Diese Tabelle listet Geräte auf, die am automatischen Konfigurationsabgleich teilnehmen.

SNMP-ID:

2.11.51.2.2

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

Idx.

Index zu diesem Eintrag in der Liste.

SNMP-ID:

2.11.51.2.2.1

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Gruppen-Mitglieder**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

leer

Adresse

IP-Adresse des entsprechenden Gerätes.

SNMP-ID:

2.11.51.2.2.2

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Gruppen-Mitglieder**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Mögliche Argumente:

IPv4-Adresse
IPv6-Adresse

Default-Wert:

leer

Menueknoten

Hier konfigurieren Sie, welche Konfigurationselemente der automatische Konfigurationsabgleich enthalten soll. Sie können dabei Werte, Tabellen und ganze Menüs einbeziehen oder ausschließen.

SNMP-ID:

2.11.51.2.3

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

Idx.

Index zu diesem Eintrag in der Liste.

SNMP-ID:

2.11.51.2.3.1

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

leer

Enthalten

Bestimmen Sie hier, ob der angegebene Menüknoten im automatischen Konfigurationsabgleich enthalten oder ausgenommen ist.

SNMP-ID:

2.11.51.2.3.2

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Mögliche Werte:

Enthalten
Ausgenommen

Default-Wert:

Enthalten

Pfad

Geben Sie den Pfad zum Menüknoten an. Es kann sich hierbei um einen Wert, eine Tabelle oder um ein komplettes Menü handeln.

SNMP-ID:

2.11.51.2.3.3

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

/Setup

SNMP-OID

Zeigt die SNMP-ID des angegebenen Menüknotens an.

Die Anzeige aktualisiert sich nach dem Speichern des Eintrages.

SNMP-ID:

2.11.51.2.3.4

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Menueknoten**

Mögliche Werte:

2

Default-Wert:

2

Ignorierte-Zeilen

Wenn Sie eine Tabelle in den automatischen Konfigurationsabgleich übernehmen, bestimmen Sie hier, welche Zeilen dieser Tabelle davon ausgenommen sein sollen.

SNMP-ID:

2.11.51.2.4

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

Idx.

Index zu diesem Eintrag in der Liste.

SNMP-ID:

2.11.51.2.4.1

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Ignorierte-Zeilen**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

Default-Wert:

leer

Zeilenindex

Geben Sie hier die Zeilennummer an, die vom automatischen Konfigurationsabgleich ausgenommen sein soll.

SNMP-ID:

2.11.51.2.4.2

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Ignorierte-Zeilen**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. `

Default-Wert:

leer

Pfad

Geben Sie den Pfad zum Knoten der Tabelle an, die im automatischen Konfigurationsabgleich enthalten ist.

SNMP-ID:

2.11.51.2.4.3

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Ignorierte-Zeilen**

Mögliche Werte:

max. 127 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

/Setup

SNMP-OID

Zeigt die SNMP-ID des angegebenen Tabellenknotens an.

Die Anzeige aktualisiert sich nach dem Speichern des Eintrages.

SNMP-ID:

2.11.51.2.4.4

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster** > **Ignorierte-Zeilen**

Mögliche Werte:

2

Default-Wert:

2

Start

Startet den automatischen Konfigurationsabgleich für diesen Eintrag.

SNMP-ID:

2.11.51.2.5

Pfad Telnet:

Setup > **Config** > **Sync** > **Neuer-Cluster**

TLS-Verbindungen

In diesem Verzeichnis legen Sie fest, über welche Adresse und auf welchem Port das Gerät eingehende Konfigurationsänderungen entgegennehmen soll.

SNMP-ID:

2.11.51.3

Pfad Telnet:

Setup > **Config** > **Sync**

Port

Geben Sie den Port an, auf dem das Gerät eingehende Konfigurationsänderungen entgegennehmen soll.

SNMP-ID:

2.11.51.3.1

Pfad Telnet:

Setup > **Config** > **Sync** > **TLS-Verbindungen**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

0 … 65535

Default-Wert:

1941

Loopback-Adresse

Geben Sie die Loopback-Adresse an, auf der das Gerät eingehende Konfigurationsänderungen entgegennehmen soll.

SNMP-ID:

2.11.51.3.2

Pfad Telnet:

Setup > **Config** > **Sync** > **TLS-Verbindungen**

Mögliche Werte:

max. 39 Zeichen aus `[A-Z][a-z][0-9].-:%`

Mögliche Argumente:

Namen der IP-Netzwerke, deren Adresse eingesetzt werden soll
„INT" für die Adresse des ersten Intranets
„DMZ" für die Adresse der ersten DMZ
LBO ... LBF für die 16 Loopback-Adressen
beliebige gültige IPv4- oder IPv6-Adresse

Default-Wert:

leer

Schnappschuss-erneuern

In diesem Verzeichnis konfigurieren Sie die Schnappschüsse.

SNMP-ID:

2.11.51.4

Pfad Telnet:

Setup > **Config** > **Sync** > **Schnappschuss-erneuern**

Aenderungs-Limit

Geben Sie hier das Änderungs-Limit an.

SNMP-ID:

2.11.51.4.1

Pfad Telnet:

Setup > **Config** > **Sync** > **Schnappschuss-erneuern**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Besondere Werte:

0

Dieser Wert deaktiviert die Funktion.

Default-Wert:

2048

Verbleibende-Aenderungen

Dieser Wert gibt die Anzahl der verbleibenden Änderungen an.

SNMP-ID:

2.11.51.4.2

Pfad Telnet:

Setup > **Config** > **Sync** > **Schnappschuss-erneuern**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

0 … 4294967295 Zweierpotenzen

Besondere Werte:

0

Dieser Wert deaktiviert die Funktion.

Default-Wert:

256

Schnappschuss-erneuern

Mit dieser Aktion erneuern Sie den Schnappschuss.

SNMP-ID:

2.11.51.4.3

Pfad Telnet:

Setup > **Config** > **Sync** > **Renew-Snapshot**

Lokale-Konfiguration

In diesem Verzeichnis bestimmen Sie die Anzahl der angewandten und beobachteten Änderungen.

SNMP-ID:

2.11.51.5

Pfad Telnet:

Setup > **Config** > **Sync** > **Local-Config**

Beobachtete-Aenderungen

Geben Sie die Anzahl der beobachteten Änderungen an.

SNMP-ID:

2.11.51.5.1

Pfad Telnet:

Setup > **Config** > **Sync** > **Local-Config**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Angewandte-Aenderungen

Geben Sie die Anzahl der angewandten Änderungen an.

SNMP-ID:

2.11.51.5.2

Pfad Telnet:

Setup > **Config** > **Sync** > **Local-Config**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

5 Konfiguration

5.1 TR-069-Unterstützung

Ab LCOS-Version 9.10 unterstützen Router bestimmte Features der Spezifikation TR-069 (CWMP) für eine automatische Provisionierung und ein sicher verschlüsseltes Remotemanagement eines Routers beispielsweise in Provider-Umgebungen.

5.1.1 CPE WAN Management Protokoll (CWMP)

Über das CPE WAN Management Protokoll (CWMP) lassen sich Endgeräte mit einem entsprechenden Konfigurationsserver über eine WAN-Verbindung fernkonfigurieren. Die Kommunikation zwischen dem Gerät (Customer Premises Equipment, CPE) und dem Konfigurationsserver (Auto Configuration Server, ACS) erfolgt über SOAP/HTTP(S) in Form von Remote Procedure Calls (RPC). Im CWMP ist eine Vielzahl von RPCs festgelegt, von denen im LCOS die folgenden realisiert sind:

- GetRPCMethods
- SetParameterValues
- GetParameterValues
- GetParameterNames
- FactoryReset
- Reboot
- Download
  - Firmware-Update
  - Script-Download (*.lcs-Dateien)

Zusätzlich unterstützt LCOS das herstellerspezifische RPC:

- X_LANCOM_DE_Command

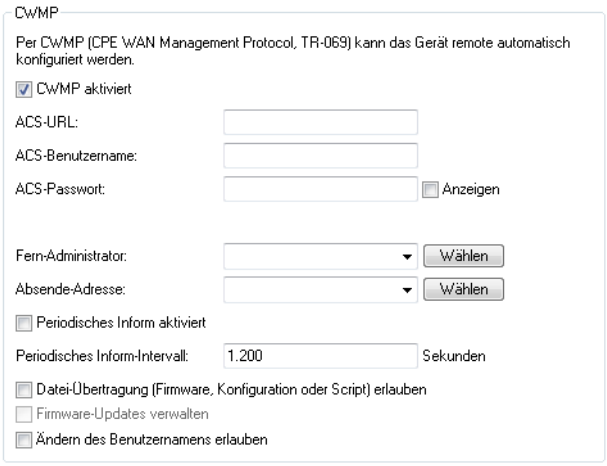
Weitere Informationen zu den Parametern der RPCs finden Sie im *Broadband-Forum*.

Die folgenden Authentifizierungsarten unterstützt das CPE gegenüber einem ACS:

- HTTP Basic
- HTTP Digest
- HTTPS durch Client-Zertifikat

CWMP mit LANconfig einrichten

In LANconfig konfigurieren Sie das CPE WAN Management Protokoll unter **Management** > **CWMP**.



CWMP aktiviert

Aktiviert oder deaktiviert das CWMP.

ACS-URL

Bestimmen Sie hier die Adresse des ACS (Auto Configuration Server), mit dem sich das CPE (Customer Premises Equipment) verbindet. Die Eingabe der Adresse erfolgt im IPv4-, IPv6- oder FQDN-Format.

Erlaubt sind HTTP und HTTPS, wobei der Einsatz von HTTPS zu bevorzugen ist, da die Geräte ansonsten gerätespezifische Parameter wie Passwörter oder Zugangsdaten unverschlüsselt übertragen. Vor dem Einsatz von HTTPS müssen Sie das vertrauenswürdige Stammzertifikat zur Überprüfung der Serveridentität in das Gerät laden.

ACS-Benutzername

Vergeben Sie einen Benutzernamen, den das Gerät zur Verbindung mit dem ACS (Auto Configuration Server) verwendet.

ACS-Passwort

Vergeben Sie ein Passwort, das das Gerät zur Verbindung mit dem ACS (Auto Configuration Server) verwendet.

Fern-Administrator

Wählen Sie einen der konfigurierten Geräte-Administratoren, den der ACS (Auto Configuration Server) beim Verbindungs-Aufbau zu diesem Gerät verwenden soll. Der ausgewählte Name muss ein aktivierter Geräte-Administrator mit entsprechenden Rechten sein, d.h., er muss Root-Zugriff zum Ändern der Firmware besitzen.

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, verwendet das Gerät diese auch auf maskiert arbeitenden Gegenstellen unmaskiert.

Als Adresse akzeptiert das Gerät verschiedene Eingabeformate:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.

- "DMZ" für die Adresse der ersten DMZ (Achtung: Wenn es eine Schnittstelle Namens "DMZ" gibt, dann nimmt das Gerät deren Adresse).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Eine beliebige IP-Adresse in der Form x.x.x.x.

Periodisches Inform aktiviert

Aktiviert oder deaktiviert das Senden von periodischen Inform-Nachrichten vom Gerät zum ACS (Auto Configuration Server).

Periodisches Inform-Intervall

Dies ist das Intervall in Sekunden zwischen zwei durch das Gerät zum ACS (Auto Configuration Server) eingeleiteten periodischen Inform-Nachrichten. Der ACS erfragt daraufhin weitere Informationen vom Gerät.

Der Standard-Wert beträgt 1200 Sekunden, d. h. 20 Minuten. Wählen Sie diesen Wert nicht zu klein, da Inform-Nachrichten einen erhöhten Netzwerk-Verkehr verursachen. Das Intervall startet nicht, bevor Gerät und Server alle Informationen ausgetauscht haben.

Datei-Übertragung erlauben

Dieser Schalter erlaubt die Übertragung einer Firmware oder einer Skript-Datei vom ACS (Auto Configuration Server) zu diesem Gerät.

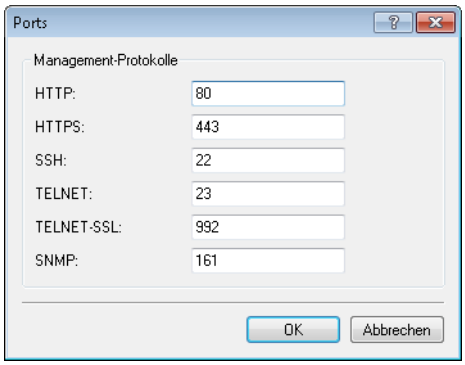
Firmware-Updates verwalten

Dieser Schalter erlaubt dem ACS (Auto Configuration Server), Firmware-Änderungen am Gerät vorzunehmen.

Ändern des Benutzernamens erlauben

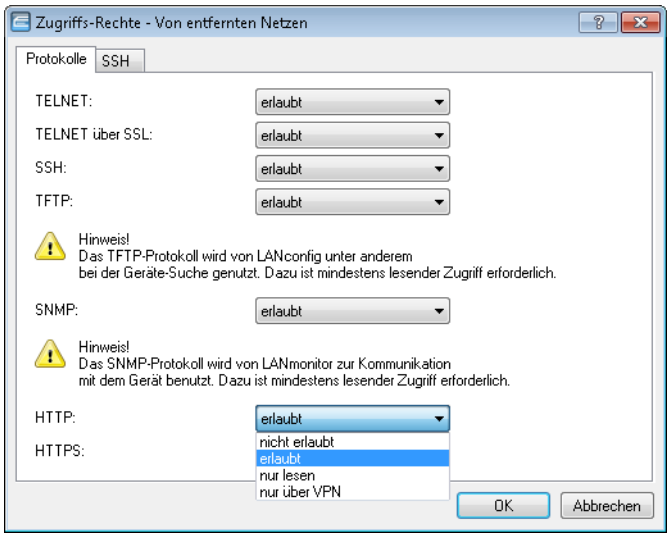
Dieser Schalter erlaubt dem ACS (Auto Configuration Server), den Geräte-Administrator zu wechseln oder den Namen und das Passwort des Geräte-Administrators, den er zur Verbindung mit dem Gerät verwendet, zu ändern..

Standardmäßig wird für die Connection-Request-URL der HTTP-Port 80 verwendet. Diesen konfigurieren Sie im LANconfig unter **Management** > **Admin** im Abschnitt **Management-Protokolle** unter **Ports**.

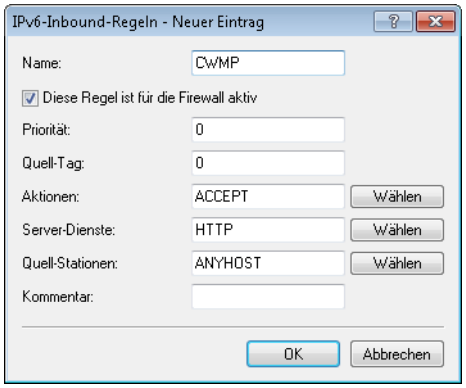


Damit ein ACS das Gerät zum Verbindungsaufbau auffordern kann, muss der Zugriff über WAN oder VPN auf den entsprechenden HTTP-Port möglich sein. Dazu muss der Zugriff im LANconfig unter **Management** > **Admin** im Abschnitt

Konfigurations-Zugriffs-Wege unter **Zugriffs-Rechte** > **Von entfernten Netzen** entweder auf WAN oder VPN freigeschaltet werden.



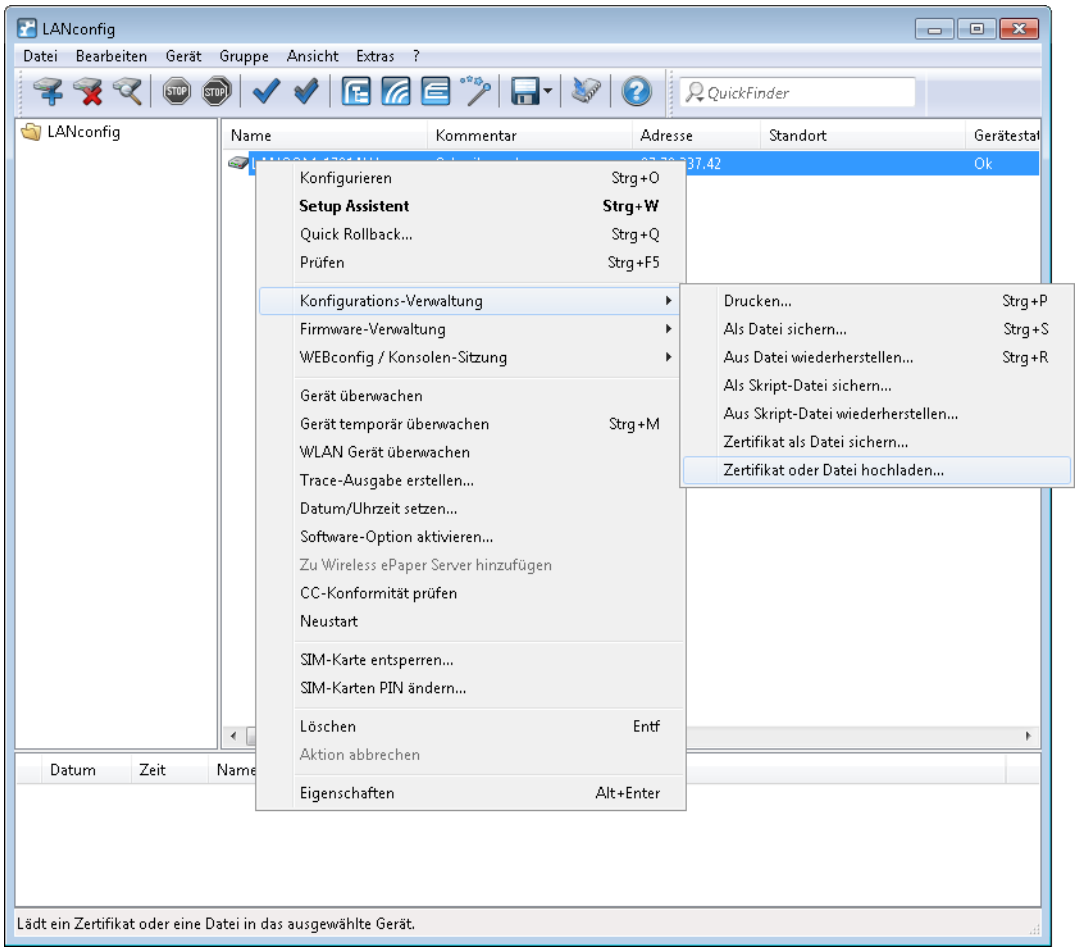
Wenn IPv6 verwendet wird, muss in der IPv6-Firewall unter **Firewall/QoS** > **IPv6-Regeln** > **IPv6-Inbound-Regeln** zusätzlich der Zugriff auf den entsprechenden Port erlaubt werden.



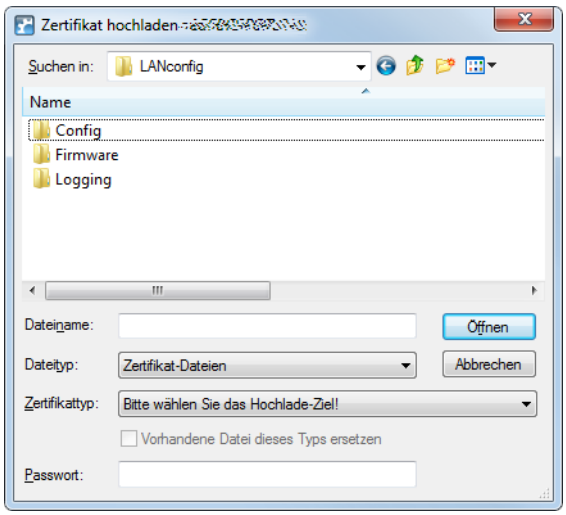
Der Connection-Request ist nur über eine Authentifizierung per Benutzername und Passwort möglich.

Bei der Verwendung von HTTPS in der ACS-URL validiert das CPE das ACS-Zertifikat. Dazu speichern Sie zuvor das CWMP Root-CA-Zertifikat im CPE. Kann das CPE das Serverzertifikat nicht gegen das vorhandene Root-CA-Zertifikat validieren, so lehnt es die Verbindung ab. Der Zertifikatsupload erfolgt entweder durch LANconfig oder WEBconfig. In LANconfig gehen Sie dazu wie folgt vor:

1. Rechtsklicken Sie in der Geräteübersicht das entsprechende Gerät und wählen Sie unter **Konfigurationsverwaltung** den Menüpunkt **Zertifikat oder Datei hochladen**.



2. Wählen Sie im folgenden Dialog als Zertifikattyp „CWMP-Root-CA-Zertifikat“ aus, und klicken Sie auf **Öffnen**.



Bei der Verwendung von SSL/TLS zur CPE-Authentifizierung laden Sie das Client-Zertifikat und den privaten Schlüssel per PKCS#12-Datei (CWMP-Container als PKCS#12-Datei) in das CPE.

Gerätekonfiguration über CWMP

Alle CWMP-Parameter konfigurieren Sie auf der Kommandozeile entweder durch eine Skript-Datei oder durch das herstellerspezifische RPC `X_LANCOM_DE_Command`.

Konfiguration per Skript

Über das CWMP-Download-Kommando `<cwmp:download>` konfigurieren Sie das Gerät per Skipt-Datei (`*.lcs`). Filetype ist hierbei `3 Vendor Configuration File` und als URL geben Sie die Adresse des Servers an, auf dem das Konfigurationsskript gespeichert ist.

LANconfig-Dateien mit Format *.lcf werden nicht unterstützt.

Konfiguration per herstellerspezifischem RPC `X_LANCOM_DE_Command`

Die Funktion `X_LANCOM_DE_Command` ist wie folgt definiert:

Anfrage

```
<cwmp:X_LANCOM_DE_Command>
<Command> CLI-Kommando </Command>
</cwmp:X_LANCOM_DE_Command>
```

Antwort

```
<cwmp:X_LANCOM_DE_CommandResponse>
<Status>1</Status>
<Result>1</Result>
</cwmp:X_LANCOM_DE_CommandResponse>
```

Das folgende Beispiel setzt die IPv4-Adresse des Gerätes auf dem „INTRANET“:

```
<cwmp:X_LANCOM_DE_Command>
<Command>set /Setup/TCP-IP/Network-list/INTRANET {IP-address} 192.168.80.1</Command>
</cwmp:X_LANCOM_DE_Command>
```

Aufgrund der asynchronen Ausführung der Konsolen-Befehle meldet `X_LANCOM_DE_Command` immer eine erfolgreiche Ausführung des Kommandos zurück, unabhängig davon, ob der Befehl korrekt ausgeführt werden konnte oder nicht. Die erfolgreiche Ausführung erfolgt durch Auslesen des Config-Status unter **Status** > **Config**.

Zur Überprüfung des Konfigurationsstatus können Sie die folgenden CWMP-Parameter vor oder nach Anwendung des Skripts oder von `X_LANCOM_DE_Command` auslesen:

- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_ConfigVersion
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptComment
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptErrorLine
- InternetGatewayDevice.DeviceInfo.X_LANCOM_DE_LastScriptSuccessful

Die Werte entsprechen den Status-Werten unter **Status** > **Config**.

5.1.2 Ergänzungen im Setup-Menü

CWMP

Über das CPE WAN Management Protokoll (CWMP) lassen sich Endgeräte mit einem entsprechenden Konfigurationsserver über eine WAN-Verbindung fernkonfigurieren. Die Kommunikation zwischen dem Gerät (Customer Premises Equipment, CPE) und dem Konfigurationsserver (Auto Configuration Server, ACS) erfolgt über SOAP/HTTP(S) in Form von Remote Procedure Calls (RPC).

SNMP-ID:

2.44

Pfad Telnet:

Setup

NTP-Server

Dieses Verzeichnis zeigt die vom CWMP konfigurierten NTP-Server zur Zeitsynchronisation an.

SNMP-ID:

2.44.1

Pfad Telnet:

Setup > **CWMP**

NTP-Server-1

Zeigt den ersten NTP-Server an.

SNMP-ID:

2.44.1.1

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

NTP-Server-2

Zeigt den zweiten NTP-Server an.

SNMP-ID:

2.44.1.2

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

NTP-Server-3

Zeigt den dritten NTP-Server an.

SNMP-ID:

2.44.1.3

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

NTP-Server-4

Zeigt den vierten NTP-Server an.

SNMP-ID:

2.44.1.4

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

NTP-Server-5

Zeigt den fünften NTP-Server an.

SNMP-ID:

2.44.1.5

Pfad Telnet:

Setup > **CWMP** > **NTP-Server**

Aktiv

Aktiviert oder deaktiviert das CWMP.

SNMP-ID:

2.44.2

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Datei-Uebertragung-erlaubt

Dieser Schalter erlaubt die Übertragung einer Firmware oder einer Skript-Datei vom ACS (Auto Configuration Server) zu diesem Gerät.

SNMP-ID:

2.44.3

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Inform-Wiederholung-Limit

Geben Sie hier an, wie oft der CPE nach einem erfolglosen Übertragungsversuch versuchen soll, eine Inform-Meldung an den ACS zu übermitteln.

SNMP-ID:

2.44.4

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

10

Besondere Werte:

0

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, verwendet das Gerät diese auch auf maskiert arbeitenden Gegenstellen unmaskiert.

SNMP-ID:

2.44.5

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Besondere Werte:

Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll.
"INT" für die Adresse des ersten Intranets.
"DMZ" für die Adresse der ersten DMZ (Achtung: Wenn es eine Schnittstelle Namens "DMZ" gibt, dann nimmt das Gerät deren Adresse).
LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
Eine beliebige IP-Adresse in der Form x.x.x.x.

Default-Wert:

leer

ACS-URL

Bestimmen Sie hier die Adresse des ACS (Auto Configuration Server), mit dem sich das Gerät verbindet. Die Eingabe der Adresse erfolgt im IPv4-, IPv6- oder FQDN-Format.

SNMP-ID:

2.44.6

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

ACS-Benutzername

Vergeben Sie einen Benutzernamen, den das Gerät zur Verbindung mit dem ACS (Auto Configuration Server) verwendet.

SNMP-ID:

2.44.7

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

ACS-Passwort

Vergeben Sie ein Passwort, das das Gerät zur Verbindung mit dem ACS (Auto Configuration Server) verwendet.

SNMP-ID:

2.44.8

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Periodisches-Inform-Aktiviert

Aktiviert oder deaktiviert das Senden von periodischen Inform-Nachrichten vom Gerät zum ACS (Auto Configuration Server).

SNMP-ID:

2.44.9

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Periodisches-Inform-Intervall

Dies ist das Intervall in Sekunden zwischen zwei durch das Gerät zum ACS (Auto Configuration Server) eingeleiteten periodischen Inform-Nachrichten. Der ACS erfragt daraufhin weitere Informationen vom Gerät.

Der Standard-Wert beträgt 1200 Sekunden, d. h. 20 Minuten. Wählen Sie diesen Wert nicht zu klein, da Inform-Nachrichten einen erhöhten Netzwerk-Verkehr verursachen. Das Intervall startet nicht, bevor Gerät und Server alle Informationen ausgetauscht haben.

SNMP-ID:

2.44.10

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

1200

Besondere Werte:

0

Periodische-Inform-Zeit

Geben Sie die periodische Inform-Zeit an.

SNMP-ID:

2.44.11

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.``

Default-Wert:

leer

Verbindungs-Anfrage-Benutzername

Wählen Sie einen der konfigurierten Geräte-Administratoren, den der ACS (Auto Configuration Server) beim Verbindungs-Aufbau zu diesem Gerät verwenden soll. Der ausgewählte Name muss ein aktivierter Geräte-Administrator mit entsprechenden Rechten sein, d.h., er muss Root-Zugriff zum Ändern der Firmware besitzen.

SNMP-ID:

2.44.12

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

max. 255 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.``

Default-Wert:

leer

Firmware-Updates-Verwalten

Dieser Schalter erlaubt dem ACS (Auto Configuration Server), Firmware-Änderungen am Gerät vorzunehmen.

SNMP-ID:

2.44.13

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Benutzernamen-Aendern-erlaubt

Dieser Schalter erlaubt dem ACS (Auto Configuration Server), den Geräte-Administrator zu wechseln oder den Namen des Geräte-Administrators zu ändern, den er zur Verbindung mit dem Gerät verwendet.

SNMP-ID:

2.44.14

Pfad Telnet:

Setup > **CWMP**

Mögliche Werte:

Nein
Ja

Default-Wert:

Nein

Provisionierungs-Code

Zeigt den Provisioning-Code an.

SNMP-ID:

2.44.15

Pfad Telnet:

Setup > **CWMP**

Parameter-Schluessel

Zeigt den Parameter-Key an.

SNMP-ID:

2.44.16

Pfad Telnet:

Setup > **CWMP**

Command-Key

Zeigt den Command-Key an.

SNMP-ID:

2.44.17

Pfad Telnet:

Setup > **CWMP**

5.1.3 Ergänzungen im Status-Menü

CWMP

Dieses Menü zeigt Ihnen bestimmte Features der Spezifikation TR-069 (CWMP) an.

SNMP-ID:

1.85

Pfad Telnet:

Status > **CWMP**

Operating

Dieses Menü zeigt Ihnen, ob CWMP aktiviert ist.

SNMP-ID:

1.85.1

Pfad Telnet:

Status > **CWMP**

Mögliche Werte:

Ja
Nein

Allow-File-Download

Dieses Menü zeigt Ihnen, ob das Gerät Firmware- oder Skript-Dateien von einem externen Server herunterladen darf.

SNMP-ID:

1.85.2

Pfad Telnet:

Status > **CWMP**

Mögliche Werte:

Ja
Nein

Provisioning-Code

Dieser Eintrag zeigt Ihnen den vom Provider konfigurierten Provisionierungscode an.

SNMP-ID:

1.85.3

Pfad Telnet:

Status > **CWMP**

Parameter-Key

Zeigt den CWMP-Parameter-Schlüssel.

SNMP-ID:

1.85.4

Pfad Telnet:

Status > **CWMP**

Command-Key

Zeigt den CWMP-Command-Schlüssel.

SNMP-ID:

1.85.5

Pfad Telnet:

Status > **CWMP**

NTP-Server-1

Dieser Eintrag zeigt Ihnen den ersten NTP-Server zur Zeitsynchronisation an.

SNMP-ID:

1.85.6

Pfad Telnet:

Status > **CWMP**

NTP-Server-2

Dieser Eintrag zeigt Ihnen den zweiten NTP-Server zur Zeitsynchronisation an.

SNMP-ID:

1.85.7

Pfad Telnet:

Status > **CWMP**

NTP-Server-3

Dieser Eintrag zeigt Ihnen den dritten NTP-Server zur Zeitsynchronisation an.

SNMP-ID:

1.85.8

Pfad Telnet:

Status > **CWMP**

NTP-Server-4

Dieser Eintrag zeigt Ihnen den vierten NTP-Server zur Zeitsynchronisation an.

SNMP-ID:

1.85.9

Pfad Telnet:

Status > **CWMP**

NTP-Server-5

Dieser Eintrag zeigt Ihnen den fünften NTP-Server zur Zeitsynchronisation an.

SNMP-ID:

1.85.10

Pfad Telnet:

Status > **CWMP**

Allow-User-Change

Dieser Eintrag zeigt Ihnen, ob Benutzerwechsel zugelassen sind.

SNMP-ID:

1.85.11

Pfad Telnet:

Status > **CWMP**

Mögliche Werte:

Ja
Nein

5.2 Verschlüsselte Konfigurationsablage in LANconfig

Ab LCOS-Version 9.10 besteht die Möglichkeit, Konfigurations- und Skriptdateien zu verschlüsseln und um Prüfsummen zu ergänzen. Somit lassen sich in LANconfig Konfigurationsdateien per Passwort verschlüsseln und sicher speichern, um Unbefugten keinen Zugriff auf Konfigurationen zu gewähren.

Tabelle 5: Übersicht aller auf der Kommandozeile eingebbaren Befehle

Befehl	Beschreibung
`readconfig [-h] [-s <password>]`	Gibt die komplette Konfiguration in Form der Geräte-Syntax aus. ■ `-h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme. ■ `-s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes. **Zugriffsrecht**: Supervisor-Read

Befehl	Beschreibung
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>]`	Erzeugt eine Textausgabe aller Befehle und Parameter, die für die Konfiguration des Gerätes im aktuellen Zustand benötigt werden. Dabei können Sie folgende Optionsschalter angeben: ■ `-n`: Die Textausgabe erfolgt nur auf numerischer Basis ohne Bezeichner. Die Ausgabe enthält somit nur die aktuellen Zustandswerte der Konfiguration sowie die zugehörigen SNMP-IDs. ■ `-d`: Nimmt die Default-Werte in die Textausgabe mit auf. ■ `-i`: Nimmt die Bezeichnungen der Tabellen-Felder in die Textausgabe mit auf. ■ `-c`: Nimmt eventuelle Kommentare, die sich in der Skriptdatei befinden, in die Textausgabe mit auf. ■ `-m`: Die Textausgabe erfolgt in einer kompakten, am Bildschirm jedoch schwer lesbaren Darstellung (ohne Einrückungen). ■ `-h`: Ergänzt die Skriptdatei um eine Prüfsumme. ■ `-s <password>`: Verschlüsselt die Skriptdatei auf Basis des angegebenen Passwortes. **Zugriffsrecht**: Supervisor-Read

5.2.1 Speichern und Laden von Gerätekonfiguration und Skriptdateien

Die Konfigurationsdatei eines Gerätes umfasst seine kompletten Einstellungen. Und mit Hilfe von Script-Dateien lassen sich die Einstellungen eines Gerätes automatisiert verwalten. Zum Schutz dieser Dateien vor unberechtigtem Zugriff oder Übertragungsfehlern ist es möglich, sie verschlüsselt und mit einer Prüfsumme versehen aus dem Gerät zu exportieren oder in das Gerät zu laden.

Es existieren somit grundsätzlich drei verschiedene Dateitypen:

- Keine Prüfsumme, keine Verschlüsselung: Eine Textdatei, deren Inhalt mit einem Texteditor lesbar ist.
- Prüfsumme: Die Textdatei enthält Informationen über die Prüfsumme sowie den Hash-Algorithmus zur Berechnung dieser Prüfsumme. Der Inhalt dieser Textdatei ist mit einem einfachen Texteditor lesbar.

  Ein LANconfig vor Version 9.10 erkennt auch Dateien mit Prüfsummen.

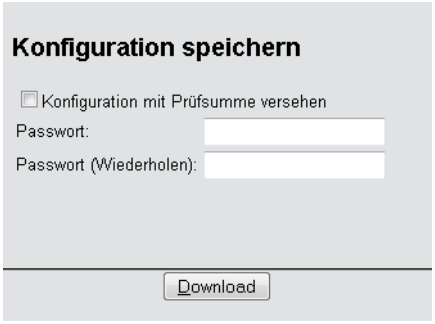
- Verschlüsselung: Vor dem Export verschlüsselt das Gerät die Datei mit einem vom Administrator gewählten Passwort. Die Textdatei enthält Informationen über den verwendeten Verschlüsselungsalgorithmus sowie eine Prüfsumme. Der Inhalt der Textdatei ist bis auf den Dateiheader mit einem Texteditor nicht mehr entzifferbar.

  Ein LANconfig vor Version 9.10 erkennt verschlüsselte Dateien nicht.

Die Dateiendungen dieser Dateien sind jeweils `.lcf` für Konfigurationsdateien bzw. `.lcs` für Skriptdateien. Die Erkennung, ob es sich um verschlüsselte oder mit Prüfsummen versehene Dateien handelt, geschieht ausschließlich über den Dateiheader.

Konfigurationsverwaltung über WEBconfig und Konsole

Um über WEBconfig eine Konfigurationsdatei zu exportieren, wechseln Sie in die Ansicht **Dateimanagement** > **Konfiguration speichern**.



Folgende Optionen stehen zur Auswahl:

Keine Angaben

In der Standardeinstellung sind alle Optionen deaktiviert. Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Konfigurationsdatei ohne Prüfsumme.

Konfiguration mit Prüfsumme versehen

Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Konfigurationsdatei mit Prüfsumme.

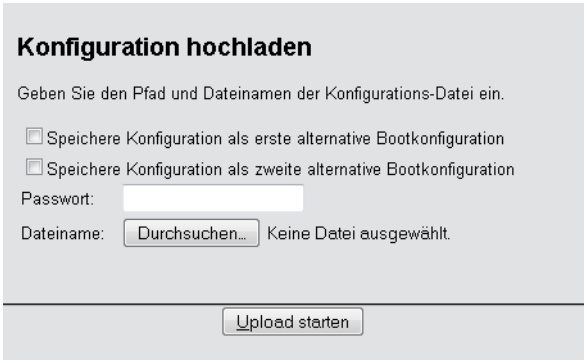
Passwort

Geben Sie ein Passwort an, wenn Sie die Konfigurationsdatei vor dem Download verschlüsseln möchten.

Um die Konfiguration über die Konsole zu sichern, verwenden Sie die folgenden Parameter:

- `readconfig`: Sichert die Konfiguration ohne Prüfsumme und Verschlüsselung.
- `readconfig -h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme.
- `readconfig -s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes.

Um über WEBconfig eine Konfigurationsdatei in das Gerät zu laden, wechseln Sie in die Ansicht **Dateimanagement** > **Konfiguration hochladen**.

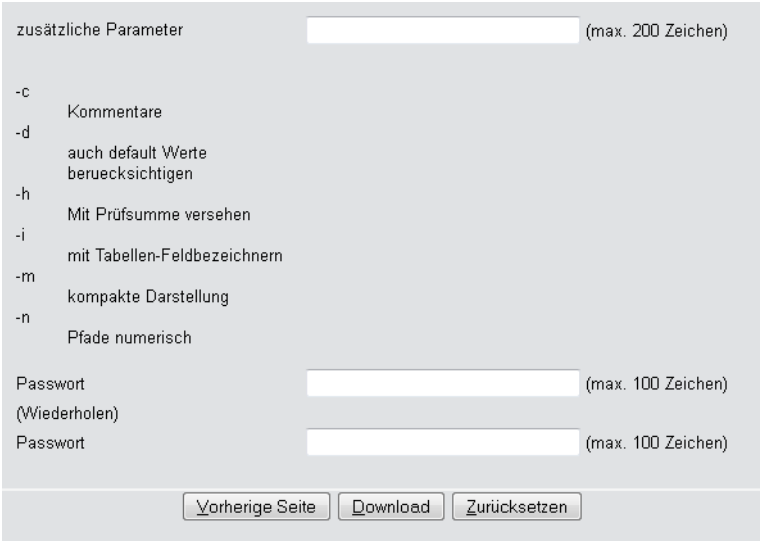


Geben Sie zusätzlich das entsprechende Passwort ein, wenn die Konfigurationsdatei verschlüsselt ist, und klicken Sie auf **Upload starten**.

Weitere Informationen zu alternativen Boot-Konfigurationen finden Sie im Abschnitt *Alternative Boot-Config*.

Skriptverwaltung über WEBconfig und Konsole

Um über WEBconfig eine Skriptdatei zu exportieren, wechseln Sie in die Ansicht **Dateimanagement** > **Konfigurations-Skript speichern**.



Folgende Optionen stehen zur Auswahl:

zusätzliche Parameter

In der Standardeinstellung sind alle Optionen deaktiviert. Nach einem Klick auf **Download** startet der Dialog zum Download einer unverschlüsselten Skriptdatei ohne Prüfsumme.

Passwort

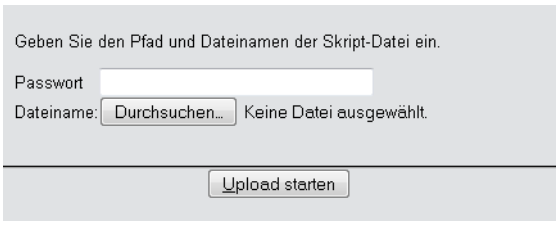
Geben Sie ein Passwort an, wenn Sie die Skriptdatei vor dem Download verschlüsseln möchten.

Um die Skriptdatei über die Konsole zu sichern, verwenden Sie z. B. die folgenden Parameter:

- `readscript`: Sichert die Konfiguration ohne Prüfsumme und Verschlüsselung.
- `readscript -h`: Ergänzt die Konfigurationsdatei um eine Prüfsumme.
- `readscript -s <password>`: Verschlüsselt die Konfigurationsdatei auf Basis des angegebenen Passwortes.

Mehr Informationen zu den Parametern finden Sie im Abschnitt *Befehle für die Konsole* in der Zeile für `readscript`.

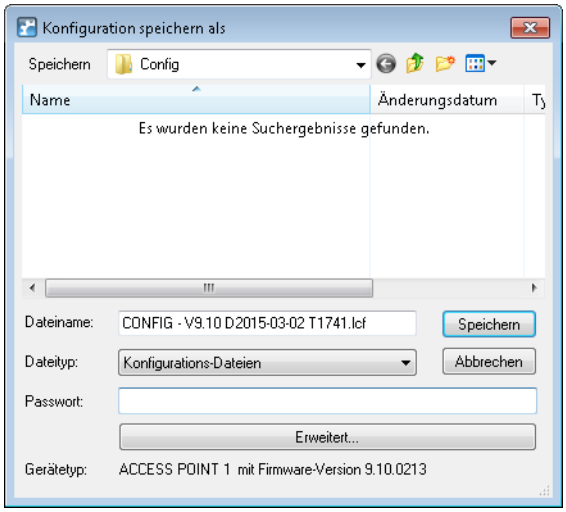
Um über WEBconfig eine Skriptdatei in das Gerät zu laden, wechseln Sie in die Ansicht **Dateimanagement** > **Konfigurations-Skript anwenden**.



Geben Sie zusätzlich das entsprechende Passwort ein, wenn die Skriptdatei verschlüsselt ist, und klicken Sie auf **Upload starten**.

Konfigurationsverwaltung über LANconfig

Um über LANconfig eine Konfigurationsdatei zu speichern, klicken Sie in der Liste der Geräte mit der rechten Maustaste auf das Gerät, dessen Konfiguration Sie speichern möchten. Öffnen Sie im Kontextdialog unter **Konfigurations-Verwaltung** > **Als Datei sichern** den Speicherdialog.



Folgende Angaben stehen zur Auswahl:

Dateiname

LANconfig belegt den Dateinamen mit verschiedenen Angaben vor (u. a. Versionsnummer, Datum und Uhrzeit). Ändern Sie den Namen Ihren Anforderungen entsprechend.

Dateityp

Wählen Sie, ob es sich um eine Konfigurationsdatei oder etwas anderes handelt.

Passwort

Geben Sie ein Passwort an, wenn Sie die Konfigurationsdatei vor dem Download verschlüsseln möchten.

Unter **Erweitert** bestimmen Sie weitere, optionale Parameter, die das Gerät beim automatischen Laden einer Konfigurations-Datei (Auto-Load) auswertet. Hiermit individualisieren Sie die Konfiguration.

Um über LANconfig eine Konfigurationsdatei in das Gerät zu laden, klicken Sie in der Liste der Geräte mit der rechten Maustaste auf das Gerät, in das Sie eine Konfiguration laden möchten. Öffnen Sie im Kontextdialog unter **Konfigurations-Verwaltung** > **Aus Datei wiederherstellen** den Uploaddialog.

Wählen Sie die gewünschte Konfigurationsdatei aus, geben Sie ggf. das benötigte Passwort an und klicken Sie auf **Öffnen**, um die Konfiguration in das Gerät zu laden.

5.2.2 Ergänzungen im Status-Menü

Skript-Log

Diese Tabelle zeigt eine Übersicht der durchgeführten Skripte an.

SNMP-ID:

1.11.23

Pfad Telnet:

Status > **Config**

Index

Zeigt den Index dieses Eintrages.

SNMP-ID:

1.11.23.1

Pfad Telnet:

Status > **Config** > **Skript-Log**

Uhrzeit

Zeigt die Uhrzeit dieses Eintrages.

SNMP-ID:

1.11.23.2

Pfad Telnet:

Status > **Config** > **Skript-Log**

Kommentar

Zeigt den Kommentar dieses Eintrages.

SNMP-ID:

1.11.23.3

Pfad Telnet:

Status > **Config** > **Skript-Log**

Erfolgreich

Zeigt, ob das Skript erfolgreich durchgelaufen ist.

SNMP-ID:

1.11.23.4

Pfad Telnet:

Status > **Config** > **Skript-Log**

Fehlerzeile

Zeigt im Fehlerfall, in welcher Zeile das Skript abgebrochen ist.

SNMP-ID:

1.11.23.5

Pfad Telnet:

Status > **Config** > **Skript-Log**

6 Diagnose

6.1 Erweiterte Config-Versionsinformationen im Status

Das aktuelle LCOS-Release bietet Ihnen die Möglichkeit, die aktuelle Konfigurations-Version abzufragen. Diese Parameter finden Sie unter **Status** > **Config**.

Config-Date

Diesen Parameter erreichen Sie über die SNMP-ID 1.11.20.

Die angezeigten Werte beziehen sich auf das UTC-Format.

Config-Hash

Diesen Parameter erreichen Sie über die SNMP-ID 1.11.21.

Bei dem angezeigten Wert handelt es sich um einen SHA1-Hash.

Config-Version

Diesen Parameter erreichen Sie über die SNMP-ID 1.11.22.

6.1.1 Ausgabe des Konfigurations-Datums

Ab LCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-date` das Datum und die Uhrzeit der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.20

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

Die Werte werden im UTC-Format angezeigt.

6.1.2 Ausgabe des Konfigurations-Hashs

Ab LCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-hash` den Hash-Wert der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.21

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

Bei dem angezeigten Wert handelt es sich um einen SHA1-Hash.

6.1.3 Ausgabe der Konfigurations-Version

Ab LCOS-Version 9.10 haben Sie die Möglichkeit, über `status/config/config-version` die Versionsnummer der Geräte-Konfiguration auszulesen.

SNMP-ID: 1.11.22

```
root@LANCOM_1781AW:/Status/Config
> ls

LAN-Active-Connections      INFO:    1
LAN-Total-Connections       INFO:    7
WAN-Active-Connections      INFO:    0
WAN-Total-Connections       INFO:    0
Outband-Active-Connections  INFO:    0
Outband-total-Connections   INFO:    0
Outband-Bitrate             INFO:    115200
Login-Errors                INFO:    0
Login-Locks                 INFO:    0
Login-Rejects               INFO:    0
Start-Scan                  ACTION:
Scan-Results                TABINFO: 0 x [IP-Address,Rtg-tag,Name,..]
Features                    TABINFO: 7 x [Feature,Expires,State,Index,Count]
Anti-Theft-Protection       MENU:
Delete-Values               ACTION:
Event-Log                   TABINFO: 64 x [Idx.,System-time,Event,Access,..]
Config-Date                 INFO:    03/25/2014 06:47:12
Config-Hash                 INFO:    cbba4fc366a8ae2b71d35e1ce58ee8f496588cf9
Config-Version              INFO:    126
Script-Log                  TABINFO: 8+ x [Index,Time,Comment,Successful,..]
```

6.1.4 Ergänzungen im Status-Menü

Konfigurations-Datum

Dieser Eintrag zeigt Ihnen an, wann Sie die Konfiguration des Gerätes zuletzt geändert haben.

SNMP-ID:

1.11.20

Pfad Telnet:

Status > **Config**

Konfigurations-Hash

Dieser Eintrag zeigt Ihnen den Hash-Wert der aktuellen Konfiguration an.

SNMP-ID:

1.11.21

Pfad Telnet:

Status > **Config**

Konfigurations-Version

Dieser Eintrag zeigt Ihnen die aktuelle Version der Geräte-Konfiguration an.

SNMP-ID:

1.11.22

Pfad Telnet:

Status > **Config**

7 LCMS

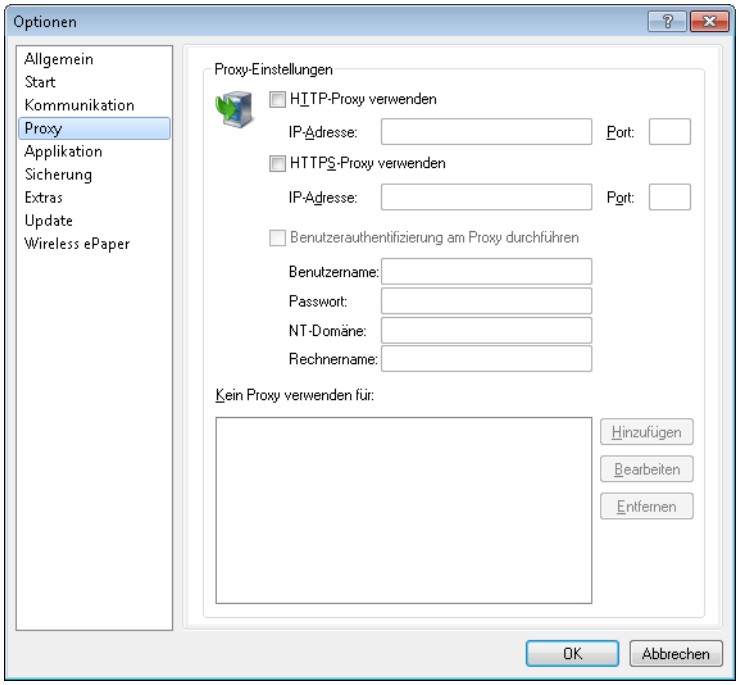
7.1 Proxyauthentifizierung über NTLM

Ab LCOS-Version 9.10 ist die Proxyauthentifizierung von LANconfig auch über NTLM (NT LAN Manager) möglich.

7.1.1 Proxy

Wenn Sie für den Zugriff auf Ihre Geräte einen Proxy-Server verwenden möchten, können Sie diesen hier konfigurieren. Aktivieren Sie dazu das gewünschte Protokoll und tragen Sie die Adresse und den Port ein, über den der Proxy-Server erreichbar ist.

Protokollunabhängig ist die Angabe einer Liste von Netzen oder einzelnen Hosts möglich, für die die Proxy-Einstellungen nicht gelten.



HTTP-Proxy verwenden

Aktiviert die Verwendung eines HTTP-Proxys.

- **Adresse**: Tragen Sie hier die IP-Adresse ein, über die der HTTP-Proxy-Server erreichbar ist.
- **Port**: Tragen Sie hier ein, welchen Port der HTTP-Proxy-Server verwendet.

HTTPS-Proxy verwenden

Aktiviert die Verwendung eines HTTPS-Proxys.

- **Adresse**: Tragen Sie hier die IP-Adresse ein, über die der HTTPS-Proxy-Server erreichbar ist.
- **Port**: Tragen Sie hier ein, welchen Port der HTTPS-Proxy verwendet.

Benutzerauthentifizierung am Proxy durchführen

Falls der Proxy-Server eine Authentifizierung erfordert, geben Sie den Benutzernamen und das Passwort ein. Wenn die Authentifizierung über NTLM (NT LAN Manager) erfolgen soll, geben Sie zusätzlich die NT-Domäne und den Rechnernamen ein.

Diese Option ist nur bei aktivierter Proxy-Einstellung verfügbar.

Kein Proxy verwenden für

Tragen Sie hier die IP-Adressen und die zugehörige Netzmaske ein, für die die Proxy-Einstellungen nicht gelten.

Diese Option ist nur bei aktivierter Proxy-Einstellung verfügbar.

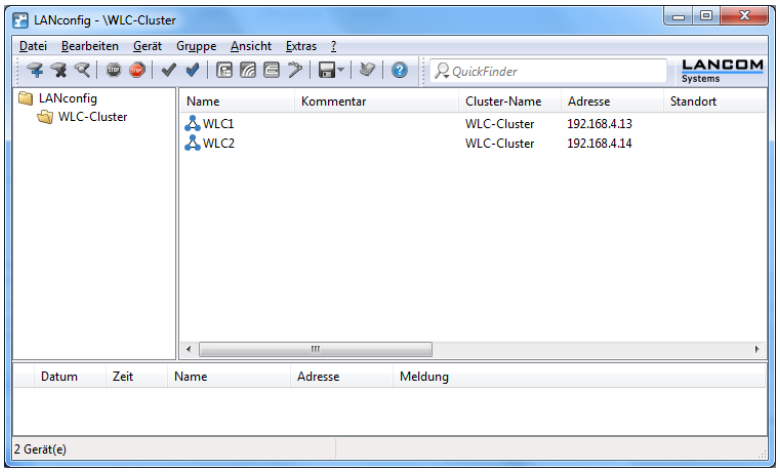
7.2 Spezielles LANconfig-Icon für Cluster-Geräte bzw. mit Config-Sync

LANconfig markiert Geräte, die ihre Konfiguration per Config-Sync teilen, mit einem eigenen Symbol. Zudem ist in der Spalte **Config Cluster** die Konfigurationsgruppe jedes Gerätes ersichtlich. Somit bietet Ihnen LANconfig die Möglichkeit, die Geräteauflistung nach Clusternamen zu sortieren und zu bearbeiten.

Möchten Sie an der Konfiguriation eines Clustermitgliedes Änderungen vornehmen, so erhalten Sie folgende Warnung:

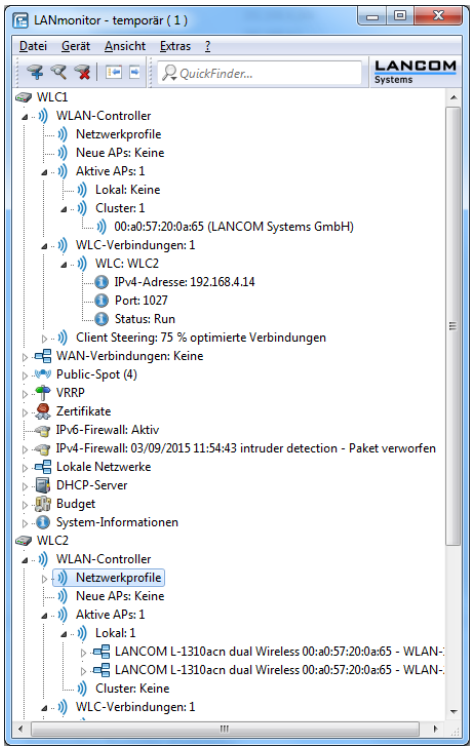
"Dieses Gerät gehört zu dem Config-Cluster: [clustername]. Das Bearbeiten dieser Konfiguration wirkt sich auch auf folgende Geräte aus: [Auflistung aller Geräte des gleichen Clusters]"

Diese Meldung können Sie bei Bedarf umgehen. Aktivieren Sie hierfür die Option **Nicht wieder anzeigen** innerhalb des angezeigten Fensters.



7.3 Spezielles LANmonitor-Icon für Cluster-Geräte bzw. mit Config-Sync

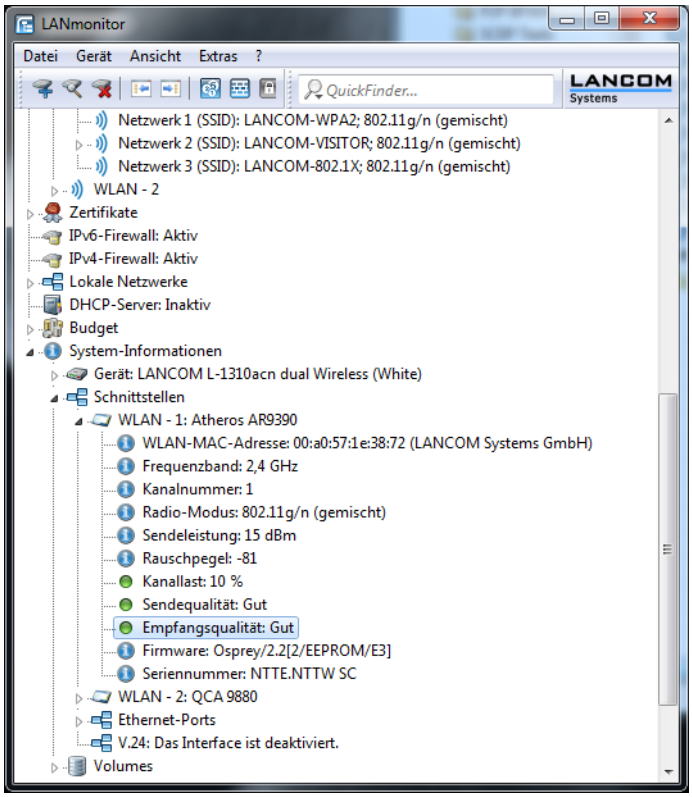
LANmonitor markiert Geräte, die ihre Konfiguration per Config-Sync teilen, mit einem eigenen Symbol. Zudem wird hinter den Gerätenamen der Name der Konfigurationsgruppe (Cluster name) angegeben. Somit können Sie mit LANmonitor die Geräte mit gleicher Konfiguration leichter zuordnen.



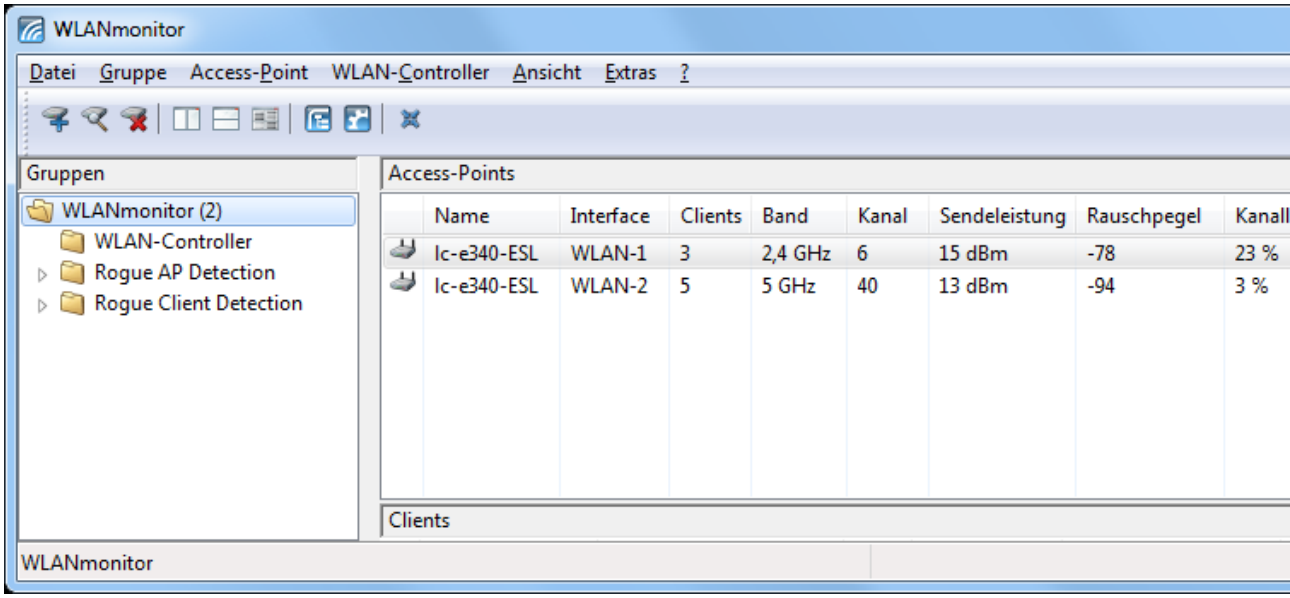
7.4 LANCOM "Wireless Quality Indicators" (WQI)

LANmonitor bietet Ihnen die Möglichkeit, die Signalqualität der einzelnen Schnittstellen anhand von **Wireless Quality Indicators** anzuzeigen. Diese Dartellung von Empfangs- und Sendequalität (RX und TX) dient der schnellen Identifizierung

der Signalqualität. Öffnen Sie zum Anzeigen dieser Informationen im LANmonitor den Bereich **System-Informationen** des Gerätes. Unter **Schnittstellen** werden Ihnen die Indikatoren angezeigt.



Der WLANmonitor zeigt Ihnen die **Wireless Quality Indicators** ebenfalls an. Klicken Sie hierfür auf den Gruppen-Hauptordner.



7.5 Erweiterte Zeichenzahl für Gerätenamen

Das aktuelle LCOS-Release bietet Ihnen die Möglichkeit, in LANconfig und WEBconfig längere Gerätenamen zu vergeben. Die Anzahl der zulässigen Zeichen beträgt nun 64 statt bisher 16 Zeichen.

8 IPv6

8.1 Präfix-Exclude-Option für DHCPv6-Präfix-Delegation

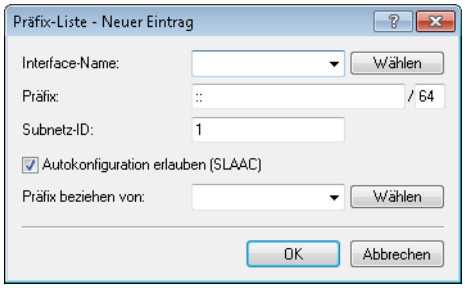
Ab LCOS-Version 9.10 unterstützt der DHCPv6-Client des Gerätes bei der Präfix-Delegation den Ausschluss von delegierten IPv6-Präfixen nach RFC 6603 (Prefix Exclude Option for DHCPv6-based Prefix Delegation).

8.1.1 Präfix-Exclude-Option für DHCPv6-Präfix-Delegation

Der DHCPv6-Client des Gerätes unterstützt bei der Präfix-Delegation den Ausschluss von delegierten IPv6-Präfixen nach RFC 6603 (Prefix Exclude Option for DHCPv6-based Prefix Delegation).

Diesen Mechanismus verwenden Provider bei DHCPv6 Präfix-Delegation, um ein Präfix aus dem delegierten Präfix für die Verwendung auf dem Kunden-LAN auszuschließen. Damit benötigt das Gerät für die WAN-Verbindung kein zusätzliches Präfix, sondern verwendet dafür das ausgeschlossene Präfix aus dem delegierten DHCPv6-Präfix. Dieses Präfix steht nicht mehr für das LAN auf der Kundenseite zur Verfügung.

Sollte im Gerät das ausgeschlossene Präfix für das LAN konfiguriert sein, erfolgt eine Syslog-Meldung und das Präfix wird im LAN nicht angekündigt. In diesem Fall konfigurieren Sie unter **IPv6** > **Router-Advertisement** > **Präfix-Liste** manuell eine andere Subnetz-ID für dieses LAN, um den Konflikt aufzulösen.



9 ISDN

9.1 Ergänzungen im Status-Menü

9.1.1 PCM-SYNC-SOURCE

Dieser Statuswert zeigt, auf welcher Busleitung die Pulscodemodulation (PCM) des ISDN-Signals stattfindet .

SNMP-ID:

1.33.2.2

Pfad Telnet:

Status > **ISDN** > **Framing**

9.1.2 PCM-Switch

Dieses Menü enthält die Statuswerte für PCM-Switch.

SNMP-ID:

1.33.20

Pfad Telnet:

Status > **ISDN**

PCM-Verbindung

Diese Tabelle zeigt eine Übersicht der PCM-Verbindungen.

SNMP-ID:

1.33.20.1

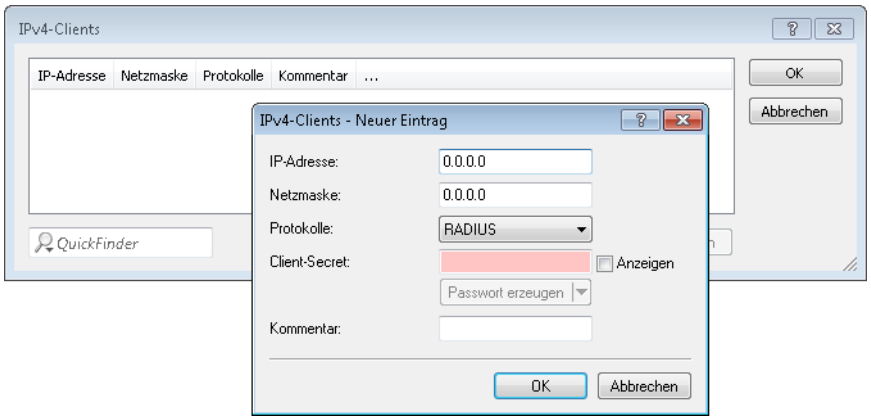
Pfad Telnet:

Status > **ISDN** > **PCM-Switch**

10 RADIUS

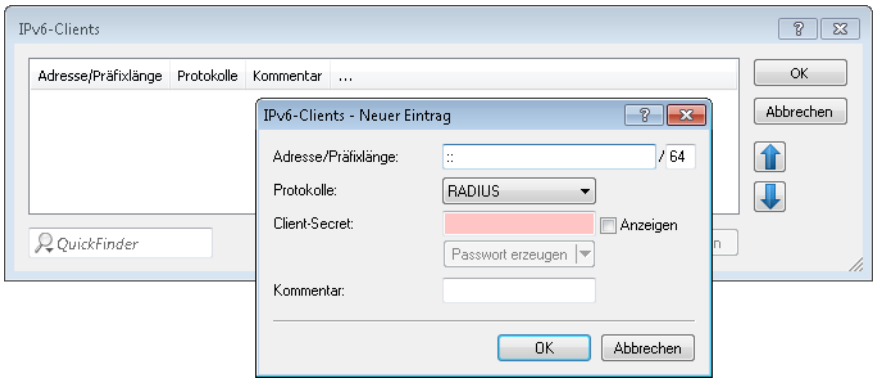
10.1 Kommentarfeld für RADIUS-Clients

Ab LCOS-Version 9.10 ist es möglich, in der RADIUS-Tabelle für jeden RADIUS-Client (IPv4 und IPv6) auch einen Kommentar zu hinterlegen.



Kommentar

Kommentar zu diesem Eintrag.



Kommentar

Kommentar zu diesem Eintrag.

10.1.1 RADIUS-Clients

IP-Adresse

IP-Adressen (oder Adressbereich) der Clients, für die das in diesem Dialog eingetragene Kennwort gilt.

Netzmaske

IP-Netzmasken der Clients.

Protokolle

Protokoll für die Kommunikation zwischen dem internen Server und den Clients.

Client-Secret

Kennwort, das die Clients für den Zugang zum internen Server benötigen.

Kommentar

Kommentar zu diesem Eintrag.

10.1.2 Ergänzungen im Setup-Menü

Clients

Hier tragen Sie die Clients ein, die mit dem RADIUS-Server kommunizieren.

SNMP-ID:

2.25.10.2

Pfad Telnet:

Setup > **RADIUS** > **Server**

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.25.10.2.5

Pfad Telnet:

Setup > **RADIUS** > **Server** > **Clients**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

IPv6-Clients

Hier bestimmen Sie die RADIUS-Zugangsdaten von IPv6-Clients.

SNMP-ID:

2.25.10.16

Pfad Telnet:

Setup > **RADIUS** > **Server**

Kommentar

Kommentar zu diesem Eintrag.

SNMP-ID:

2.25.10.16.5

Pfad Telnet:

Setup > **RADIUS** > **Server** > **IPv6-Clients**

Mögliche Werte:

max. 251 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

10.2 Attribut-Umfang in RADIUS-Requests erweitert

Ab LCOS-Version 9.10 unterstützt das Gerät weitere RADIUS-Attribute im Public Spot, siehe Kapitel *Public Spot*.

Tabelle 6: Die folgenden Attribute werden vom Gerät im Access-Request übertragen:

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
1	User-Name	Der vom Benutzer eingegebene Name.	Verwendet bei 802.1x WLAN, PPPoE-Server, L2TP, PPTP, VPN
2	User-Password	Das vom Benutzer eingegebene Passwort.	Verwendet bei 802.1x WLAN, PPPoE-Server, L2TP, PPTP, VPN
4	NAS-IP-Address	Gibt die IPv4-Adresse des Gerätes an, das den Zugang für einen Anwender anfragt.	<IPv4-Adresse des Gerätes>
6	Service-Type	Gibt den Service-Typ an, den das Gerät anfragt bzw. als Antwort erwartet.	■ Authenticate-Only ■ Framed
7	Framed-Protocol	Gibt an, welches Protokoll zu verwenden ist.	PPP
30	Called-Station-Id	Gibt die ID der gerufenen Station an (z. B. des VPN-Servers).	■ Server-IP-Adresse (bei VPN-Verbindungen über PPTP oder L2TP) ■ Dienst-Name (bei PPPoE) ■ BSSID:SSID (bei WLAN) ■ MAC-Adresse des Gerätes (bei Public Spot)
31	Calling-Station-Id	Gibt die ID der rufenden Station an (z. B. des VPN-Clients).	■ Client-IP-Adresse (bei VPN-Verbindungen über PPTP oder L2TP) ■ Client-MAC-Adresse (bei PPPoE, WLAN und Public Spot)

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
32	NAS-Identifier	Gibt den Namen des Gerätes an, für das der RADIUS-Server den Zugang verwaltet.	<Geräte-Name>
61	NAS-Port-Type	Gibt den physikalischen Port an, über den das Gerät den Benutzer authentifiziert.	■ Virtual (bei VPN-Verbindungen über PPTP oder L2TP) ■ Ethernet (bei PPPoE) ■ Wireless-802.11 (bei WLAN)
95	NAS-IPv6-Address	Gibt die IPv6-Adresse des Gerätes an, das den Zugang für einen Anwender anfragt.	<IPv6-Adresse des Gerätes>
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	■ 13 (VLAN; bei Public Spot)
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	■ 6 (802; bei Public Spot)
81	Tunnel-Private-Group-Id	Definiert die Gruppen-ID, falls die Sitzung getunnelt ist.	■ 1-4096 (bei Public Spot)
177	Mobility-Domain-ID	Kennzeichnet die Mobility-Domain, in der sich der Client befindet.	
181	WLAN-HESSID	Enthält die HESSID der 802.11u SSID.	
182	WLAN-Venue-Info	Enthält Informationen zur Kategorie des Standortes.	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
183	WLAN-Venue-Language	Enthält Informationen zur Sprache des Standortes.	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
184	WLAN-Venue-Name	Enthält die Bezeichnung des Standortes (Standort-Name).	Zu konfigurieren unter **Wireless-LAN** > **802.11u** > **Standortinformationen**.
186	WLAN-Pairwise-Cipher	Enthält Informationen über den paarweisen Schlüssel, den Client und AP verwenden.	
187	WLAN-Group-Cipher	Enthält Informationen über den Gruppenschlüssel, den Client und AP verwenden.	
188	WLAN-AKM-Suite	Enthält Informationen über die Zugriffsverwaltung (Authentication and Key Management) zwischen Client und AP.	
189	WLAN-Group-Mgmt-Cipher	Enthält Informationen über den Gruppenverwaltungsschlüssel, der eine Verbindung über RSNA (Robust Security Network Association) zwischen AP und mobilem Client absichert.	
190	WLAN-RF-Band	Enthält Informationen über das Frequenzband, das der Client verwendet.	

Für die folgenden herstellerspezifischen RADIUS-Attribute wird die IANA Private Enterprise Number „3561" des Broadband-Forums verwendet.

Tabelle 7: Übersicht aller unterstützten Hersteller spezifischen RADIUS-Attribute im Access-Request

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
1	ADSL-Agent-Circuit-Id	Gibt die Schnittstelle des Gerätes an, für das der RADIUS-Server den Zugang verwaltet. Wird nur übertragen,	<Schnittstelle des Gerätes>

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
		wenn Agent-Relay-Infos im PPPoED-Paket enthalten sind (siehe *PPPoE-Snooping*).	
2	ADSL-Agent-Remote-Id	Gibt die Bezeichnung des Gerätes an, für das der RADIUS-Server den Zugang verwaltet. Wird nur übertragen, wenn Agent-Relay-Infos im PPPoED-Paket enthalten sind (siehe *PPPoE-Snooping*).	<Bezeichnung des Gerätes>
16	LCS-Orig-NAS-Identifier	NAS-Identifier des ursprünglichen Access Points im WLC-Betrieb.	
17	LCS-Orig-NAS-IP-Address	NAS-IP-Adresse des ursprünglichen Access Points im WLC-Betrieb.	<IPv4-Adresse des Gerätes>
18	LCS-Orig-NAS-IPv6-Address	NAS-IPv6-Adresse des ursprünglichen Access Points im WLC-Betrieb.	<IPv6-Adresse des Gerätes>

10.3 Accounting-Statustypen "Accounting-On" und "Accounting-Off"

Ab LCOS-Version 9.10 verarbeitet das Gerät bei Verwendung von RADIUS bei WLAN und Public Spots auch die RADIUS-Accounting-Statustypen "Accounting-On" und "Accounting-Off".

10.3.1 Accounting-Statustypen "Accounting-On" und "Accounting-Off"

RADIUS-Server und AP tauschen Status-Informationen wie Start, Ende oder Update von Client-Sessions am AP aus. Diese Datenpakete orientieren sich am Verhalten des angemeldeten Clients.

Mit den Statustypen "Accounting-On" und "Accounting-Off" gibt der AP Informationen über seine generelle Eignung für das RADIUS-Accounting an den RADIUS-Server weiter:

Accounting-On

Wenn das Gerät in einen Betriebszustand wechselt, in dem es Accounting-Informationen mit einem RADIUS-Server austauschen kann, sendet es ein "Accounting-On".

Accounting-Off

Wenn das Gerät in einen Betriebszustand wechselt, in dem es keine Accounting-Informationen mit einem RADIUS-Server austauschen kann, sendet es ein "Accounting-Off".

Die folgenden Bedingungen lösen die Übertragung eines "Accounting-On" oder "Accounting-Off" aus:

- Das Gerät aktiviert oder deaktiviert eine physikalische WLAN-Schnittstelle mit der entsprechenden SSID.

  Die Deaktivierung kann auch die Folge von Überhitzung, Verbindungsverlust oder fehlerhafter Link-Erkennung sein.
- Die WLAN-Schnittstelle wechselt in einen nicht-AP-Modus (also weder 'managed' noch Stand-alone-AP) oder zurück.
- Im P2P-Modus wechselt das Gerät in die Betriebsart "exklusiv", was alle SSIDs deaktiviert.
- Das Gerät aktiviert oder deaktiviert eine SSID.
- Das Gerät aktiviert oder deaktiviert das RADIUS-Accounting für eine SSID.

10.4 Volumen-Budget im RADIUS-Server und Public Spot erweitert

Ab LCOS-Version 9.10 verwaltet der RADIUS-Server Volumen-Budgets von mehr als 4GByte.

Der RADIUS-Server interpretiert das existierende Volumen-Budget nun als Wert in MByte (statt wie vorher in Byte). Beim Update auf die LCOS-Version 9.10 konvertiert das Gerät existierende Werte und rundet sie auf volle MByte. So ändert sich z. B. der Eintrag "1000000" (Byte) zu "1" (MByte).

Diese Erweiterung wirkt sich auf das Public-Spot-Modul aus. Die Angabe des Volumenbudgets über das Public-Spot-Web-API kann zusätzlich eine Einheit enthalten:

`volumebudget`

Volumen-Budget

Die folgenden Angaben sind möglich:

- `k` oder `K`: Angabe in Kilobytes (kB), z. B. `volumebudget=1000k`.
- `m` oder `M`: Angabe in Megabytes (MB), z. B. `volumebudget=100m`.
- `g` oder `G`: Angabe in Gigabytes (GB), z. B. `volumebudget=1g`.

Ohne Einheit entspricht die Angabe einem Wert in Byte (B).

Fehlt dieser Parameter komplett, verwendet der Assistent den Default-Wert.

Diese Erweiterung wirkt sich auf das XML-Interface aus. Die Angabe des Volumenbudgets beim Login-Request und Login-Response kann zusätzlich eine Einheit enthalten:

`TRAFFICEXPIRE`

Maximales Datenvolumen für einen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

Die folgenden Angaben sind möglich:

- `k` oder `K`: Angabe in Kilobytes (kB), z. B. `<TRAFFICEXPIRE>1000k</TRAFFICEXPIRE>`.
- `m` oder `M`: Angabe in Megabytes (MB), z. B. `<TRAFFICEXPIRE>100m</TRAFFICEXPIRE>`.
- `g` oder `G`: Angabe in Gigabytes (GB), z. B. `<TRAFFICEXPIRE>1g</TRAFFICEXPIRE>`.

Ohne Einheit entspricht die Angabe einem Wert in Byte (B).

10.4.1 Ergänzungen im Setup-Menü

Volumen-Budget

Maximales Datenvolumen in MByte für diesen Benutzer-Account. Dieses Datenvolumen kann der Benutzer bis zum Erreichen einer ggf. definierten relativen oder absoluten Ablaufzeit ausschöpfen.

SNMP-ID:

2.25.10.7.12

Pfad Telnet:

Setup > **RADIUS** > **Server**

Mögliche Werte:

Max. 10 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

schaltet die Überwachung des Datenvolumens aus.

Volumen-Budget-MByte

Mit diesem Eintrag haben Sie die Möglichkeit, das Volumenbudget des RADIUS-Benutzers in Megabyte festzulegen.

SNMP-ID:

2.25.10.7.22

Pfad Telnet:

Setup > **RADIUS** > **Server** > **Benutzer**

Mögliche Werte:

max. 10 Zeichen aus `[0-9]`

Default-Wert:

0

Besondere Werte:

0

Das Volumenbudget ist deaktiviert.

Volumen-Budget

Über diesen Eintrag definieren Sie das Volumen-Budget in MByte, welches automatisch angelegte Benutzer erhalten. Der Wert `0` deaktiviert die Funktion.

SNMP-ID:

2.24.41.3.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Authentifizierungs-Module** > **Benutzer-Template**

Mögliche Werte:

max. 4 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

schaltet die Überwachung des Datenvolumens aus.

10.5 RADIUS-Server: Realm-Ermittlung bei Computer-Authentisierung

Ab LCOS-Version 9.10 ermittelt der RADIUS-Server den Realm eines RADIUS-Requests auch aus einer Computerauthentifizierung.

Das Gerät betrachtet die folgenden Bestandteile eines Benutzernamens als Realm:

`user@company.com`

`company.com` bildet den Realm und ist durch ein @-Zeichen vom Benutzernamen getrennt.

`company\user`

`company` bildet den Realm und ist durch einen Backslash („\") vom Benutzernamen getrennt. Diese Authentifizierung ist z. B. bei einem Windows-Login gebräuchlich.

`host/user.company.com`

Beginnt der Benutzername mit dem String `host/` und enthält der restliche Name mindestens einen Punkt, dann betrachtet das Gerät alles hinter dem ersten Punkt als Realm (in diesem Fall also `company.com`).

10.5.1 Ergänzungen im Setup-Menü

Realm-Typen

Bestimmen Sie, wie der RADIUS-Server den Realm eines RADIUS-Requests ermittelt.

SNMP-ID:

2.25.10.17

Pfad Telnet:

Setup > **RADIUS** > **Server**

Mögliche Werte:

Mail-Domaene

`user@company.com`: `company.com` bildet den Realm und ist durch ein @-Zeichen vom Benutzernamen getrennt.

MS-Domaene

`company\user`: `company` bildet den Realm und ist durch einen Backslash („\") vom Benutzernamen getrennt. Diese Authentifizierung ist z. B. bei einem Windows-Login gebräuchlich.

MS-CompAuth

`host/user.company.com`: Beginnt der Benutzername mit dem String `host/` und enthält der restliche Name mindestens einen Punkt, dann betrachtet das Gerät alles hinter dem ersten Punkt als Realm (in diesem Fall also `company.com`).

Default-Wert:

Mail-Domaene

MS-Domaene

11 Public Spot

11.1 Administratoren auf die Voucher-Ausgabe einschränken

Sofern Sie in LCOS einen beschränkten Administrator allein mit dem Funktions-Recht **Public-Spot-Assistent (Benutzer anlegen)** versehen, hat dieser künftig ausschließlich Zugriff auf die Eingabemaske des Benutzer-Erstellungs-Assistenten. Die Navigationsleiste in WEBconfig bleibt ihm verborgen.

11.1.1 Assistent zum Einrichten und Verwalten von Benutzern

Mit Hilfe des Setup-Wizards **Public-Spot-Benutzer einrichten** (Benutzer-Erstellungs-Assistent) erstellen Sie über WEBconfig zeitlich begrenzte Zugänge zu einem Public Spot-Netzwerk mit wenigen Mausklicks. Dabei bestimmen Sie im einfachsten Fall lediglich die Dauer des Zugangs; der Assistent vergibt Benutzername und Kennwort automatisch und speichert den Zugang in der Benutzerdatenbank des geräteinternen RADIUS-Servers. Der Anwender erhält abschließend ein ausdruckbares, personalisiertes Ticket (Voucher), mit dem er sich im Public Spot-Netzwerk ab sofort bis zur definierten Ablaufzeit anmelden kann.

Alternativ lassen sich Voucher auch auf Vorrat anlegen und ausdrucken, um z. B. in Stoßzeiten die Voucher-Ausgabe zu beschleunigen oder Mitarbeitern ohne Gerätezugriff die Voucher-Ausgabe zu ermöglichen. Hierzu geben Sie im Benutzer-Erstellungs-Assistenten an, dass die Nutzungsdauer erst ab dem ersten Login des Anwenders beginnt. Außerdem definieren Sie eine maximale Gültigkeitsdauer für den Zugang – nach dieser Zeit löscht der Public Spot den Zugang automatisch, auch wenn die Nutzungsdauer noch nicht abgelaufen ist.

Der Setup-Wizard **Public-Spot-Benutzer verwalten** (Benutzer-Verwaltungs-Assistent) stellt alle eingetragenenen Public Spot-Zugänge auf einer eigenen Webseite in einer tabellarischen Übersicht dar. So haben Sie mit einem Klick die wichtigsten Daten Ihrer Nutzer im Blick und können auf komfortable Weise die Gültigkeit des Zugangs verlängern / verkürzen oder das betreffende Benutzerkonto komplett löschen. Zusätzlich lassen sich über den Assistenten Informationen zum Benutzerkonto abrufen, wie z. B. das vergebene Passwort im Klartext, der Authentifizierungsstatus, die IP-Adresse, die gesendeten / empfangenen Datenmengen oder etwaige Beschränkungen, die für das Benutzerkonto gelten.

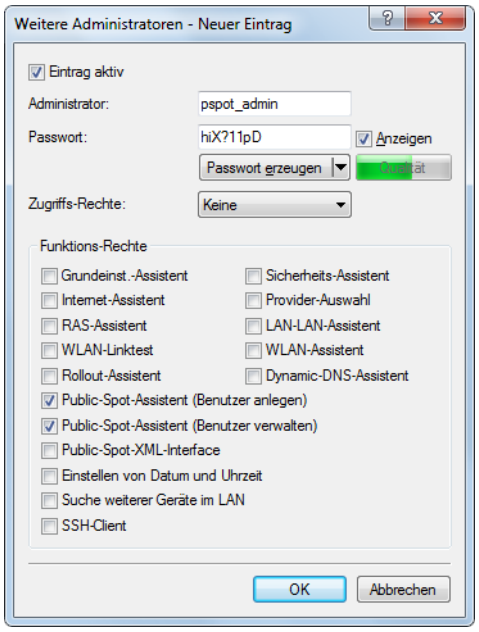
11.1.2 Beschränkten Administrator zur Public Spot-Verwaltung einrichten

Um Mitarbeitern auch ohne Zugriff auf die Gerätekonfiguration die Einrichtung und Verwaltung von Benutzern zu erlauben, haben Sie die Möglichkeit, einen beschränkten Administrator einzurichten, welcher ausschließlich über die Rechte zur Verwendung der *Public Spot-Assistenten* verfügt. Dieses Tutorial beschreibt die dafür erforderlichen Schritte sowie die notwendigen Zugriffs- und Funktionsrechte in LANconfig.

Da die Rechte zur Verwendung der Public Spot-Assistenten getrennt von einander konfigurierbar sind, lässt sich ein beschränkter Administrator auch auf einen einzelnen Assistenten einschränken. Im Falle des Benutzer-Erstellungs-Assistenten leitet das Gerät den beschränkten Administrator nach dem WEBconfig-Login dann automatisch an die entsprechende Eingabemaske weiter.

1. Öffnen Sie in LANconfig den Konfigurationsdialog des Gerätes, für das Sie einen Public Spot-Administrator hinzufügen wollen.
   In diesem Gerät muss das Public Spot-Modul aktiviert sein.
2. Wechseln Sie in die Ansicht **Management** > **Admin**. Klicken Sie im Abschnitt **Geräte-Konfiguration** auf **Weitere Administratoren** und klicken Sie anschließend **Hinzufügen**.

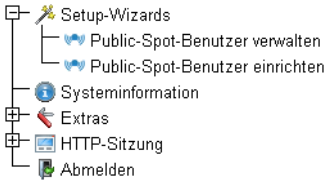
Wenn Sie einem vorhandenen Administrator die Public Spot-Verwaltung zuweisen möchten, markieren Sie dessen Tabelleneintrag und klicken stattdessen **Bearbeiten**.



3. Aktivieren Sie das Profil, indem Sie die Option **Eintrag aktiv** markieren.
4. Vergeben Sie einen aussagekräftigen Namen im Feld **Administrator**.
5. Bestimmen Sie ein **Passwort** und wiederholen Sie es zur Kontrolle.
6. Setzen Sie die **Zugriffs-Rechte** auf **Keine**.
7. Aktivieren Sie im Abschnitt **Funktions-Rechte** die Optionen **Public-Spot-Assistent (Benutzer anlegen)** für den Benutzer-Erstellungs-Assistenten und **Public-Spot-Assistent (Benutzer verwalten)** für den Benutzer-Verwaltungs-Assistenten.

   Das Funktionsrecht **Public-Spot-XML-Interface** wird von einem Public Spot-Administrator nicht benötigt. Das Recht ist nur relevant, wenn Sie das XML-Interface verwenden und sollte auch dann aus Sicherheitsgründen nicht mit den oben beschriebenen Funktionsrechten kombiniert werden.
8. Speichern Sie das erstellte oder geänderte Administratorprofil mit einem Klick auf **OK**.

Sofern Sie die Funktions-Rechte für mehrere Assistenten gesetzt haben, kann der beschränkte Administrator in WEBconfig über die Navigationsleiste zwischen den Assistenten navigieren.



Sofern Sie ausschließlich das Funktionsrecht **Public-Spot-Assistent (Benutzer anlegen)** gesetzt haben, kann ein beschränkter Administrator lediglich innerhalb des Benutzer-Erstellungs-Assistenten navigieren; die Navigationsleiste bleibt verborgen. Ein manuelles Abmelden über WEBconfig ist in diesem Fall nicht mehr möglich. Aus Sicherheitsgründen ist die Lebensdauer der WEBconfig-Sitzung daher sehr kurz gehalten. Bei entsprechender Inaktivität loggt das Gerät den beschräkten Administrator automatisch aus.

Aus technischen Gründen kann sich der Benutzer-Erstellungs-Assistent nach Verwenden der Schaltfläche **User anlegen und CSV-Export** nicht automatisch aktualisieren. Möchte ein beschränkter Administrator weitere Benutzer einrichten und Voucher ausdrucken, muss er den Assistenten neu aufrufen (z. B. via URL oder Aktualisieren der Webseite, wenn die Navigationsleiste verbogen ist).

11.2 Volumen-Budget auf Vouchern angeben

Mit LCOS 9.10 haben Sie die Möglichkeit, den Platzhalter-Tag `<pbelem vollimit>` auch innerhalb des Voucher-Templates zu verwenden, um einem Public Spot-Benutzer das ihm zugewiesene Datenvolumen mitzuteilen.

VOLLIMIT

Gültig für: `<pbelem> <pbcond>`

Dieser Bezeichner gibt die verbleibende Datenmenge an, die dem Benutzer noch zur Verfügung steht, bevor das Gerät die aktuelle Sitzung automatisch beendet. Für eine Sitzung ohne Datenlimit ist dieser Bezeichner gleich Null.

Abbildung 1: Beispiel für einen Public Spot-Voucher

11.3 XML-Interface: Erweitertes VLAN-Handling

Ab LCOS-Version 9.10 haben Sie die Möglichkeit, über ein externes Gateway die Quell-VLAN eines Benutzers an den Public Spot zu übermitteln und zur VLAN-ID-abhängigen Authentisierung an einen externen RADIUS-Server weiterzuleiten.

SOURCE_VLAN (optional, nur in Verbindung mit der Authentifizierung über einen RADIUS-Server)

Die VLAN-ID des Netzes, aus dem sich ein Public Spot-Benutzer anzumelden versucht (Quell-VLAN). Der Public Spot leitet die Quell-VLAN in seinem Access-Request an den internen oder einen externen RADIUS-Server weiter. Dazu verwendet der Public Spot das RADIUS-Attribut 81 (**Tunnel-Private-Group-Id**) im Zusammenspiel mit den RADIUS-Attributen 64 (**Tunnel-Type**) und 65 (**Tunnel-Medium-Type**). Der RADIUS-Server kann auf Basis der Quell-VLAN dann z. B. entscheiden, ob er den Access-Request des Public Spots akzeptiert oder ablehnt.

Hat der RADIUS-Server die Anfrage akzeptiert, überträgt er in seinem Access-Accept die o. g. RADIUS-Attribute zurück an den Public Spot. Anschließend hinterlegt der Public Spot das Quell-VLAN für den jeweiligen Client und dessen Stationsliste und gibt dem Benutzer den Zugriff auf das Public Spot-Netz frei.

Nutzen Sie Quell-VLAN in Verbindung mit dem Setup-Parameter *2.24.47*. Dadurch verhindern Sie, dass sich ein Public Spot-Benutzer in VLAN-getrennten Public Spot-Netzen/SSIDs nach einmaliger

Authentisierung durch den RADIUS-Server an sämtlichen verwalteten Public Spot-Netzen/SSIDs anmelden kann.

Die SOURCE_VLAN ist nicht mit der VLAN_ID zu verwechseln. Die VLAN_ID wird nicht an den RADIUS-Server übermittelt, sondern vom Public Spot dazu genutzt, einem Benutzer nach erfolgreicher Authentifizierung eine vom Gateway vorgegebene VLAN-ID zuzuweisen.

Zur internen Prüfung hinterlegt der Public Spot innerhalb seiner Stationstabelle die Quell-VLAN, sobald der externe RADIUS-Server den Authentication Request akzeptiert hat. Wechselt ein Benutzer anschließend in ein anderers Public Spot-Netzwerk/SSIDs, dessen VLAN-ID von der eingetragenen abweicht, setzt der Public Spot den Benutzer auf "nicht authentisiert" und zeigt ihm beim nächsten Aufruf wieder die Anmeldeseite.

11.3.1 Ergänzungen im Setup-Menü

Herkunft-VLAN-verifizieren

Über diesen Parameter legen Sie fest, ob das XML-Interface die VLAN-ID des Netzes, aus dem sich ein Benutzer authentisiert hat, bei der Verifikation von Benutzer-Requests berücksichtigt. Dies ist z. B. in Szenarien relevant, in denen Sie mehrere Public Spot-SSIDs via VLAN trennen und eine einmalige Authentifizierung an einer dieser SSIDs den Benutzer nicht automatisch für den Zugriff auf die übrigen SSIDs berechtigen soll.

Der Parameter setzt voraus, dass Sie die Setup-Parameter 2.24.40.1 (das XML-Interface selbst) und 2.24.40.2 (die Authentifizierung für das XML-Interface über einen internen oder einen externen RADIUS-Server) ebenfalls aktiviert haben.

SNMP-ID:

2.24.47

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein

Der Public Spot berücksichtigt die VLAN-ID nicht bei der Verifikation von Benutzern. Eine einmalige Authentifizierung eines Benutzers berechtigt zum Zugriff auf sämtliche vom Public Spot verwaltete SSIDs. Solange das Benutzerkonto gültig ist, erfolgt die Anmeldung automatisch.

ja

Der Public Spot berücksichtigt die VLAN-ID bei der Verifikation von Benutzern. Hierzu hinterlegt der Public Spot die VLAN-ID in der gleichnamigen Spalte der Stationstabelle, sofern die Authentifizierung durch den RADIUS-Server erfolgreich war. Diese VLAN-ID entspricht dem Wert für SOURCE_VLAN im Login-Request des externen Gateways. Wechselt der Public Spot-Benutzer in ein Netz mit abweichender VLAN-ID, ändert der Public Spot dessen Stationstabelleneintrag zu „nicht authentifiziert“ und fordert den Benutzer zur erneuten Authentifizierung am RADIUS-Server auf. Der Benutzer erhält in diesem Fall bei erneuter Anmeldung die Anmeldeseite.

Weitere Informationen zu den Request- und Response-Typen sowie dem SOURCE_VLAN-Element finden Sie im Referenzhandbuch.

Default-Wert:

nein

VLans

Über diesen Parameter definieren Sie für den angegebenen Host-Namen optional eine Liste von VLAN-IDs, an welche die Erreichbarkeit der freien Seite(n) gekoppelt ist. Auschließlich Benutzer, welche über die in der Stationstabelle hinterlegte VLAN-ID verfügen, sind in der Lage, diesen Host ohne Anmeldung aufzurufen. Nutzen Sie diesen Parameter, um z. B. in Anwendungsszenarien mit VLAN-getrennten Public Spot-Netzen/SSIDs den Zugriffsbereich für einzelne Nutzergruppen unterschiedlich stark einzuschränken.

SNMP-ID:

2.24.31.3

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Freie-Netze** > **VLans**

Mögliche Werte:

Default-Wert:

leer

Kommaseparierte Liste, max. 16 Zeichen aus `[0-9],`

Besondere Werte:

leer, **0**

Der Zugriff auf den eingetragenen Host ist aus allen VLANs heraus möglich.

11.3.2 Meldungen an den und vom Authentifizierungs-Server

Übertragene Attribute

Wie bereits erwähnt, übermittelt Ihr Gerät in einer RADIUS-Anfrage weit mehr als ausschließlich Benutzername und -kennwort. RADIUS-Server können diese zusätzlichen Informationen komplett ignorieren oder lediglich eine Teilmenge davon verarbeiten. Viele dieser Attribute werden auch für den Serverzugang über Dial-in verwendet und sind in den RADIUS RFCs als Standard-Attribute definiert. Einige für den Hotspot-Betrieb wichtige Informationen lassen sich jedoch nicht mit den Standard-Attributen abbilden. LANCOM hat daher beschlossen, diese zusätzlichen Attribute als herstellerspezifisch zu markieren und mit der Herstellerkennung 2356 zu versehen.

Tabelle 8: Übersicht der vom Gerät an den Authentifizierungs-Server übertragenen RADIUS-Attribute

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
1	User-Name	Der vom Benutzer eingegebene Name.	
2	User-Password	Das vom Benutzer eingegebene Passwort.	
4	NAS-IP-Address	IP-Adresse Ihres Gerätes.	<IPv4-Adresse des Gerätes>
6	Service-Type	Art des Dienstes, den der Benutzer angefragt hat. Der Wert „1“ steht dabei für Login.	
8	Framed-IP-Address	Gibt die dem Client zugewiesene IP-Adresse an.	<IP-Adresse des Clients>
30	Called-Station-Id	MAC-Adresse Ihres Gerätes.	<nn:nn:nn:nn:nn:nn>
31	Calling-Station-Id	MAC-Adresse des Clients. Die Ausgabe erfolgt byte-weise in hexadezimaler Schreibweise mit Trennzeichen.	<nn:nn:nn:nn:nn:nn>
32	NAS-Identifier	Name Ihres Gerätes, sofern konfiguriert.	<Geräte-Name>
61	NAS-Port-Type	Art des physikalischen Ports, über den ein Benutzer eine Authentifizierung angefragt hat.	■ **Id 19** kennzeichnet Clients aus dem WLAN.

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
			■ **Id 15** kennzeichnet Clients aus dem Ethernet.
87	NAS-Port-Id	Bezeichnung des Interfaces, über welches ein Client mit Ihrem Gerät verbunden ist. Dies kann sowohl eine physische als auch logische Schnittstelle sein. Bedenken Sie, dass mehr als nur ein Client über ein Interface verbunden sein kann; die Port-Nummer verweist also im Gegensatz zu Dial-in-Servern nicht eindeutig auf einen Client.	z. B. ■ LAN-1 ■ WLAN-1-5 ■ WLC-TUNNEL-27

Ausgewertete Attribute

Ihr Gerät untersucht die Authentifizierungs-Antwort eines RADIUS-Servers auf Attribute, die es eventuell weiterverarbeiten kann. Die meisten Attribute haben allerdings nur dann eine Bedeutung, wenn die Antwort positiv war, sodass sie die anschließende Sitzung beeinflussen.

Tabelle 9: Übersicht aller unterstützten RADIUS-Attribute

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
18	Reply-Message	Eine beliebige Zeichenfolge des RADIUS-Servers, die entweder ein gescheitertes Anmelden oder eine Willkommensnachricht beinhaltet. Diese Nachricht lässt sich über das SERVERMSG-Element in eine benutzerdefinierte Start- oder Fehlerseite integrieren.	
25	Class	Ein beliebiges Oktett oder Achtbitzeichen, das die Daten vom Authentifizerungs- / Accounting-Backend enthält. Jedes Mal, wenn das Gerät eine RADIUS-Accounting-Anfrage stellt, wird dieses Attribut unverändert gesendet. Innerhalb einer Authentifizierungs-Antwort kann dieses Attribut mehrmals vorkommen, um z. B. eine Zeichenfolge zu übertragen, die länger als 255 Bytes ist. Das Gerät behandelt alle Vorkommen dieses Attributes in Accounting-Anfragen in der Reihenfolge, in der sie in der Authentifizierungs-Antwort aufgetreten sind.	
26	Vendor 2356, Id 1 Trafficlimit	Definiert eine Datenmenge in Bytes, nach der das Gerät die Sitzung automatisch beendet. Dieser Wert ist nützlich, um Volumen-limitierte Benutzerkonten zu erstellen. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Volumen-Limit angenommen. Ein Datenlimit von 0 wird als ein Benutzerkonto interpretiert, das zwar grundsätzlich gültig ist, aber sein Datenvolumen aufgebraucht hat. In diesem Fall startet das Gerät keine Sitzung.	
26	Vendor 2356, Id 3 LCS-Redirection-URL	Kann eine beliebige URL enthalten, die als zusätzlicher Link auf der Startseite angeboten wird. Dies kann die Startseite des Benutzers sein oder eine Seite mit zusätzlichen Informationen zum Benutzerkonto.	
26	Vendor 2356, Id 5 LCS-Account-End	Definiert einen absoluten Zeitpunkt (gemessen in Sekunden seit dem 1. Januar 1970 0:00:00), nach dem der Account ungültig wird. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Datumslimit angenommen. Das Gerät startet keine Sitzung, wenn die interne Systemuhr nicht eingestellt ist oder der angegebene Zeitpunkt in der Vergangenheit liegt.	

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS
26	Vendor 2356, Id 7 LCS-Public-Spot-Username	Enthält den Namen eines Public Spot-Benutzers für den Auto-Login. Der Auto-Login bezieht sich dabei auf die Tabelle der MAC-authentifizierten Benutzer, denen der Server automatisch einen Benutzernamen zuweist.	
26	Vendor 2356, Id 8 LCS-TxRateLimit	Definiert eine maximale Downstream-Rate in kbps. Diese Beschränkung lässt sich mit der dazugehörigen Public Spot-Funktion kombinieren.	
26	Vendor 2356, Id 9 LCS-RxRateLimit	Definiert eine maximale Upstream-Rate in kbps. Diese Beschränkung lässt sich mit der dazugehörigen Public Spot-Funktion kombinieren.	
26	Vendor 2356, Id 13 LCS-Advertisement-URL	Definiert eine kommaseparierte Liste von Werbe-URLs.	
26	Vendor 2356, Id 14 LCS-Advertisement-Interval	Definiert das Intervall in Minuten, nach dem der Public Spot einen Benutzer an eine Werbe-URL umleitet. Bei einem Intervall von 0 erfolgt die Umleitung direkt nach der Anmeldung.	
27	Session-Timeout	Definiert eine optionale Maximal-Dauer für die Sitzung in Sekunden. Wenn dieses Attribut in der Authentifizierungs-Antwort fehlt, wird kein Zeitlimit angenommen. Ein Zeitlimit von 0 wird als ein Benutzerkonto interpretiert, das zwar grundsätzlich gültig ist, aber seine verfügbare Zeit aufgebraucht hat. In diesem Fall startet das Gerät keine Sitzung.	
28	Idle-Timeout	Definiert einen Zeitraum in Sekunden, nach dem das Gerät die Sitzung beendet, wenn es keine Pakete vom Client mehr empfängt. Dieser Wert überschreibt möglichweise eine unter **Public-Spot** > **Server** > **Leerlaufzeitüberschreitung** lokal definierte Leerlauf-Zeitüberschreitung.	
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	
81	Tunnel-Private-Group-ID	Definiert die Gruppen-ID, falls die Sitzung getunnelt ist.	
85	Acct-Interim-Interval	Definiert die Zeit zwischen aufeinander folgenden RADIUS-Accounting-Aktualisierungen. Dieser Wert wird nur dann ausgewertet, wenn auf dem RADIUS-Client lokal kein eigenes Accounting-Intervall festgelegt ist, Sie für das Public-Spot-Modul also keinen **Update-Zyklus** festgelegt haben.	

Beachten Sie, dass sich die Attribute für LCS-Account-Ende und Session-Zeitüberschreitung gegenseitig ausschließen und daher beide Attribute nicht in einer Antwort auftreten sollten. Sollten dennoch beide Attribute auftreten, wertet das Gerät das zuletzt auftretende Attribut aus.

11.4 "Small Header Image": Optimierte Darstellung für 19"-Geräte

Ab LCOS-Version 9.10 verfügen 19-Zoll-Geräte ebenfalls über eine Anmeldeseite mit individualisierbarem Kopfbild für schmale Bildschirme, um eine bessere Darstellung des Public Spots auf Mobilgeräten zu erzielen.

11.5 Ergänzungen im Status-Menü

11.5.1 Benutzerlimit

Dieser Eintrag zeigt Ihnen die maximale Benutzerzahl an, die auf dem Public Spot zeitgleich authentifiziert sein darf.

SNMP-ID:

1.44.11

Pfad Telnet:

Status > **Public-Spot**

11.5.2 PbSpot-authentifizierte-Benutzer

Dieser Eintrag zeigt Ihnen die Anzahl der Public Spot-Benutzer an, die gegenwärtig über den Public Spot selbst authentifiziert sind.

SNMP-ID:

1.44.12

Pfad Telnet:

Status > **Public-Spot**

11.5.3 PMS-authentifizierte-Benutzer

Dieser Eintrag zeigt Ihnen die Anzahl der Public Spot-Benutzer an, die gegenwärtig über die PSM-Schnittstelle authentifiziert sind.

SNMP-ID:

1.44.13

Pfad Telnet:

Status > **Public-Spot**

11.5.4 Lokal-konfigurierte-Benutzer

Dieser Eintrag zeigt Ihnen an, wie viele Public Spot-Benutzer auf dem Gerät gegenwärtig lokal eingerichtet sind.

SNMP-ID:

1.44.14

Pfad Telnet:

Status > **Public-Spot**

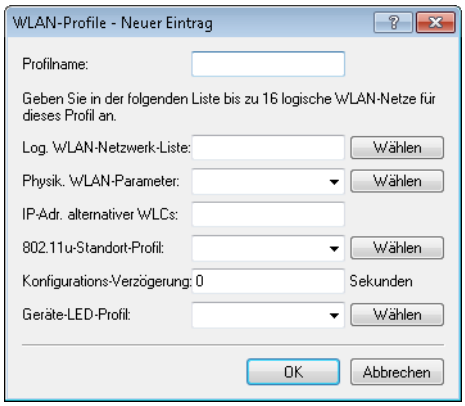
12 WLAN

12.1 Erweiterung auf 16 SSIDs pro WLAN-Modul

Ab LCOS-Version 9.10 bilden IEEE 802.11n WLAN-Module bis zu 16 SSIDs und IEEE 802.11ac WLAN-Module 15 SSIDs ab.

Auch WLCs mit der LCOS-Version 9.10 verwalten je AP-Profil bis zu 16 SSIDs.

Für jedes WLAN-Profil können Sie unter **WLAN-Controller** > **Profile** > **WLAN-Profile** die folgenden Parameter definieren:



12.2 WLAN in der Standardeinstellung deaktiviert

Ab LCOS-Version 9.10 sind alle WLAN-Schnittstellen von WLAN-Routern standardmäßig deaktiviert.

12.3 Wildcards für MAC-Adressen und SSID-Filter

Ab LCOS-Version 9.10 ist die Angabe von Wildcards (* und ?) innerhalb von MAC-Adressen möglich. Außerdem lässt sich der Zugriff von WLAN-Clients auf vorgegebene SSIDs beschränken.

Im WEBconfig ersetzt die neue Stationsliste die bisherige Stationsliste unter **Setup** > **WLAN** > **Zugangs-Liste** (bei APs) oder **Setup** > **WLAN-Management** > **Zugangs-Liste** (bei WLCs).

Beim Update auf die neue Version übernimmt LCOS die vorhandenen Werte aus der bestehenden Stationsliste.

Tabelle 10: Übersicht aller durchführbaren Traces

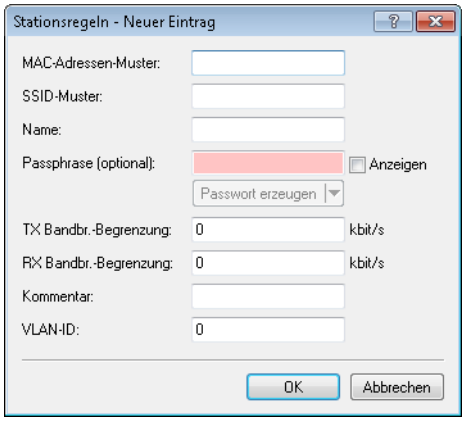
Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
`WLAN-ACL`	Status-Meldungen über MAC-Filterregeln. Die Anzeige ist abhängig von der Konfiguration des WLAN-Data-Trace. Ist dort eine MAC-Adresse vorgegeben, zeigt der Trace nur die Filterergebnisse an, die diese spezielle MAC-Adresse betreffen.

12.3.1 Access Control List

Mit der **A**ccess **C**ontrol **L**ist (ACL) gewähren oder untersagen Sie einzelnen WLAN-Clients den Zugriff auf Ihr WLAN. Die Festlegung erfolgt anhand der fest programmierten MAC-Adressen der WLAN-Adapter.

Bei der zentralen Verwaltung der LANCOM WLAN-Router und LANCOM APs über einen WLC finden Sie die Stationstabelle unter **WLAN-Controller** > **Stationen** unter der Schaltfläche **Stationen**.

Kontrollieren Sie unter **Wireless-LAN** > **Stationen**, ob die Einstellung **Daten von den aufgeführten Stationen übertragen, alle anderen Stationen ausfiltern** aktiviert ist. Fügen Sie neue Stationen, die an Ihrem Funk-Netzwerk teilnehmen sollen, ggf. über die Schaltfläche **Stationen** hinzu.



MAC-Adressen-Muster

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Die Verwendung von Wildcards ist möglich.

SSID-Muster

Dieser Eintrag begrenzt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen auf diese SSID.

Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

Name

Sie können zu jedem WLAN-Client einen beliebigen Namen und einen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

Passphrase

Hier können Sie optional für jede physikalische Adresse (MAC) eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i/WEP** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

TX Bandbreitenbegrenzung

Sende-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein WLAN-Gerät im Client-Modus übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

RX Bandbreitenbegrenzung

Empfangs-Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein WLAN-Gerät im Client-Modus übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die RX-Bandbreiten-Begrenzung ist nur aktiv für WLAN-Geräte im Client-Modus. Für normale WLAN-Clients wird dieser Wert nicht verwendet.

VLAN-ID

Diese VLAN-ID wird Paketen zugewiesen, die von dem Client mit der eingetragenen MAC-Adresse empfangen wurden. Bei der VLAN-ID '0' wird der Station keine spezielle VLAN-ID zugewiesen, es gilt die VLAN-ID der Funkzelle (SSID).

Falls sich Filterregeln widersprechen, hat die individuellere Regel eine höhere Priorität: Eine Regel ohne Wildcards in der MAC-Adresse oder SSID hat Vorrang vor einer Regel mit Wildcards. Ansonsten hat der Anwender beim Anlegen von Einträgen darauf zu achten, dass sich die Filterregeln nicht widersprechen. Mit dem Trace-Aufruf `trace WLAN-ACL` in einer Telnet-Sitzung lassen sich die Filterangaben kontrollieren.

Die Filterkriterien in der Stationsliste erlauben oder verweigern den Zugriff von WLAN-Clients auf das WLAN-Netzwerk. Die Einträge **Name**, **Bandbreiten-Begrenzung**, **VLAN-ID** und **Passphrase** sind bedeutungslos, wenn das Gerät bei gültigen Filterkriterien den WLAN-Zugriff verweigert.

12.3.2 Ergänzungen im Setup-Menü

Zugriffsregeln

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie bestimmte Stationen von der Übertragung ausschließen oder nur bestimmte Stationen gezielt freischalten.

SNMP-ID:

2.12.89

Pfad Telnet:

Setup > **WLAN**

MAC-Adress-Muster

Geben Sie hier die MAC-Adresse einer Station ein.

Die Verwendung von Wildcards ist möglich.

SNMP-ID:

2.12.89.1

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 20 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Mögliche Argumente:

MAC-Adresse

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressenbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Die Verwendung von Wildcards ist möglich.

Name

Sie können zu jeder Station einen beliebigen Namen eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

SNMP-ID:

2.12.89.2

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Kommentar

Sie können zu jeder Station einen beliebigen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

SNMP-ID:

2.12.89.3

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 30 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

WPA-Passphrase

Hier können Sie optional für jeden Eintrag eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i/WEP** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

Bei WEP gesicherten Netzwerken hat dieses Feld keine Bedeutung.

SNMP-ID:

2.12.89.4

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Tx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für "Daten senden" und Tx für "Daten empfangen".

SNMP-ID:

2.12.89.5

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 9 Zeichen aus `0123456789`

0 … 999999999

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

Rx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für "Daten senden" und Tx für "Daten empfangen".

SNMP-ID:

2.12.89.6

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 9 Zeichen aus `0123456789`

0 … 999999999

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

VLAN-Id

Das Gerät weist diese VLAN-ID den Paketen zu, die der WLAN-Client mit der eingetragenen MAC-Adresse empfängt.

SNMP-ID:

2.12.89.7

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 4 Zeichen aus `0123456789`

0 … 4096

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

SSID-Muster

Dieser Eintrag reduziert oder erlaubt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen für diese SSID.

Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

SNMP-ID:

2.12.89.9

Pfad Telnet:

Setup > **WLAN** > **Zugriffsregeln**

Mögliche Werte:

max. 40 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Besondere Werte:

*****

Platzhalter für beliebig viele Zeichen

?

Platzhalter für genau ein Zeichen

Default-Wert:

leer

Zugriffsregeln

Um den Datenverkehr zwischen dem Wireless-LAN und Ihrem lokalen Netz einzuschränken, können Sie bestimmte Stationen von der Übertragung ausschließen oder gezielt bestimmte Stationen freischalten.

SNMP-ID:

2.37.21

Pfad Telnet:

Setup > **WLAN-Management**

MAC-Adress-Muster

Geben Sie hier die MAC-Adresse einer Station ein.

Die Verwendung von Wildcards ist möglich.

SNMP-ID:

2.37.21.1

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 20 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Mögliche Argumente:

MAC-Adresse

MAC-Adresse des WLAN-Clients, für den dieser Eintrag gilt. Die folgenden Eingaben sind möglich:

einzelne MAC-Adresse

Eine MAC-Adresse im Format `00a057112233`, `00-a0-57-11-22-33` oder `00:a0:57:11:22:33`.

Wildcards

Wildcards '*' und '?' für die Angabe von MAC-Adressbereichen, z. B. `00a057*`, `00-a0-57-11-??-??` oder `00:a0:??:11:*`.

Vendor-ID

Das Gerät hat eine Liste der gängigen Hersteller-OUIs (Organizationally Unique Identifier) gespeichert. Der MAC-Adressbereich ist gültig, wenn dieser Eintrag den ersten drei Bytes der MAC-Adresse des WLAN-Clients entspricht.

Die Verwendung von Wildcards ist möglich.

Name

Sie können zu jeder Station einen beliebigen Namen eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

SNMP-ID:

2.37.21.2

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Kommentar

Sie können zu jeder Station einen beliebigen Kommentar eingeben. Dies ermöglicht Ihnen eine einfachere Zuordnung der MAC-Adressen zu bestimmten Stationen oder Benutzern.

SNMP-ID:

2.37.21.3

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 30 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

WPA-Passphrase

Hier können Sie optional für jeden Eintrag eine separate Passphrase eintragen, die in den 802.11i/WPA/AES-PSK gesicherten Netzwerken benutzt wird. Ohne die Angabe einer gesonderten Passphrase für diese MAC-Adresse werden die im Bereich **802.11i/WEP** für jedes logische Wireless-LAN-Netzwerk hinterlegten Passphrasen verwendet.

Verwenden Sie als Passphrase zufällige Zeichenketten von mindestens 22 Zeichen Länge, was einer kryptographischen Stärke von 128 Bit entspricht.

Bei WEP-gesicherten Netzwerken hat dieses Feld keine Bedeutung.

SNMP-ID:

2.37.21.4

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 63 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Tx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für "Daten senden" und Tx für "Daten empfangen".

SNMP-ID:

2.37.21.5

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 9 Zeichen aus `0123456789`

0 … 999999999

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

Rx-Limit

Bandbreiten-Begrenzung für die sich einbuchenden WLAN-Clients. Ein Client übermittelt seine eigene Einstellung bei der Anmeldung an den AP. Dieser bildet daraus zusammen mit dem hier eingestellten Wert das Bandbreiten-Minimum.

Die Bedeutung der Werte Rx und Tx ist abhängig von der Betriebsart des Gerätes. In diesem Fall als AP steht Rx für "Daten senden" und Tx für "Daten empfangen".

SNMP-ID:

2.37.21.6

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 9 Zeichen aus `0123456789`

0 … 999999999

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

VLAN-Id

Das Gerät weist diese VLAN-ID den Paketen zu, die der WLAN-Client mit der eingetragenen MAC-Adresse empfängt.

SNMP-ID:

2.37.21.7

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 4 Zeichen aus `0123456789`

0 … 4096

Default-Wert:

0

Besondere Werte:

0

keine Begrenzung

SSID-Muster

Dieser Eintrag reduziert oder erlaubt den Zugriff der WLAN-Clients mit den entsprechenden MAC-Adressen für diese SSID.

Die Verwendung von Wildcards ist möglich, um den Zugriff auf mehrere SSIDs zu erlauben.

SNMP-ID:

2.37.21.9

Pfad Telnet:

Setup > **WLAN-Management** > **Zugriffsregeln**

Mögliche Werte:

max. 40 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.` `

Besondere Werte:

*****

Platzhalter für beliebig viele Zeichen

?

Platzhalter für genau ein Zeichen

Default-Wert:

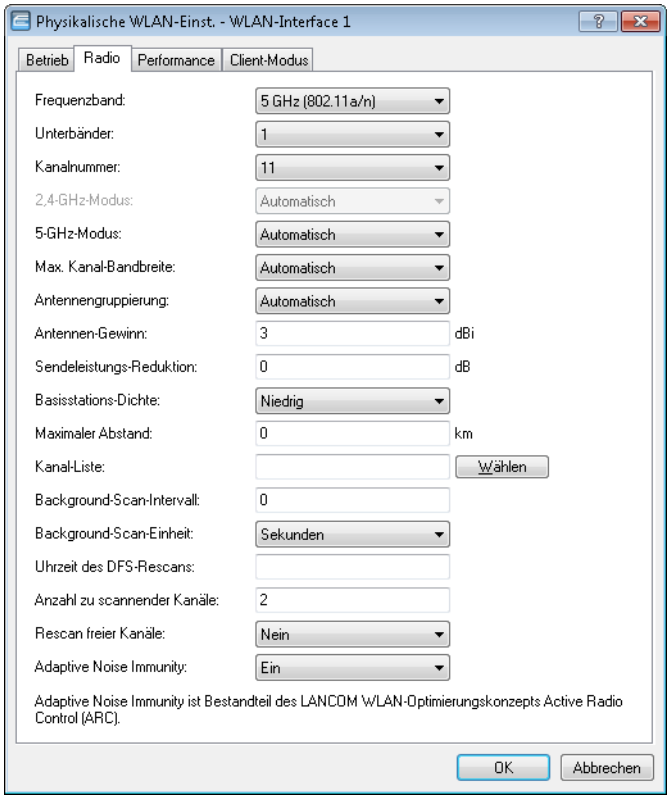
leer

12.4 Konformität mit aktuellen ETSI-Funkstandards im 2,4GHz/5GHz-Band

Ab LCOS-Version 9.10 unterstützt der AP auch die Funkstandards ETSI EN 300328-V1.7.1, ETSI EN 300328-V1.8.1 und ETSI EN 301893-V1.7.1.

12.4.1 DFS-Konfiguration

In LANconfig konfigurieren Sie die DFS-Einstellungen unter **Wireless-LAN** > **Allgemein** durch einen Klick auf **Physikalische WLAN-Einst.** und Auswahl des Reiters **Radio**.



Uhrzeit des DFS-Rescans

Dieser Eintrag bestimmt, um welche Uhrzeit (0-24 Uhr) das Gerät die DFS-Datenbank löscht und einen DFS-Rescan durchführt. Ohne Eintrag führt das Gerät erst dann einen DFS-Rescan durch, wenn kein freier Kanal mehr verfügbar ist. Das ist dann der Fall, wenn die beim initialen DFS-Scan ermittelte Kanalzahl die minimale Anzahl der freien Kanäle unterschreitet.

Für die Definition der Uhrzeit lassen sich Möglichkeiten der cron-Befehle nutzen: Der Eintrag '1,6,13' startet den Rescan immer um 1 Uhr, 6 Uhr und 13 Uhr. Der Eintrag '0-23/4' startet alle vier Stunden einen Rescan in der Zeit zwischen 0 und 23 Uhr.

Anzahl zu scannender Kanäle

Dieser Eintrag bestimmt die minimale Anzahl an freien Kanälen, die ein DFS-Scan erreichen muss. Der Standardwert '2' bedeutet, dass das Gerät solange einen DFS-Scan durchführt, bis es 2 freie Kanäle erkennt. Im Falle eines nötigen Kanalwechsels, z. B. auf Grund eines aktivierten Radarmusters, steht der zweite Kanal sofort für einen Wechsel zur Verfügung.

Der Wert '0' deaktiviert die Beschränkung. Die physikalische WLAN-Schnittstelle führt einen DFS-Scan auf sämtlichen zur Verfügung stehenden Kanälen aus.

Rescan freier Kanäle

Diese Auswahl bestimmt, ob die physikalische WLAN-Schnittstelle nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle löscht oder für weitere DFS-Rescans zwischenspeichert.

- **Ja**: Die physikalische WLAN-Schnittstelle löscht nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle, damit diese bei einem erneuten DFS-Rescan wieder zur Verfügung stehen.
- **Nein**: Das Gerät speichert nach einem abgeschlossenen DFS-Rescan die als besetzt erkannten Kanäle, so dass das Gerät diese Kanäle bei einem erneuten DFS-Rescan sofort überspringt (Default).

12.4.2 Ergänzungen im Setup-Menü

Bevorzugtes-DFS-Schema

Um das WLAN-Gerät gemäß aktueller ETSI-Funkstandards zu betreiben, wählen Sie hier den entsprechenden Standard aus.

Beim Upgrade einer LCOS-Version auf einen aktuellen Funk-Standard wird die vorherige Einstellung beibehalten.

SNMP-ID:

2.23.20.8.20

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen** > **Bevorzugtes-DFS-Schema**

Mögliche Werte:

EN 301 893-V1.3
EN 301 893-V1.5
EN 301 893-V1.6
EN 301 893-V1.7

Default-Wert:

EN 301 893-V1.7

Bevorzugtes-2.4-Schema

Über diesen Parameter legen Sie fest, nach welcher Version der EN 300 328 das Gerät im 2,4-GHz-Band operiert.

Bei einem Firmware-Update wird die aktuelle Version beibehalten. Neue Geräte und Geräte, bei denen ein Konfigurations-Reset durchgeführt wurde, verwenden standardmäßig Version 1.8.

SNMP-ID:

2.23.20.8.28

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Radio-Einstellungen**

Mögliche Werte:

EN300328-V1.7
EN300328-V1.8

Default-Wert:

EN300328-V1.8

12.5 Uhrzeit des DFS-Rescans über LANconfig konfigurierbar

Ab LCOS-Version 9.10 ist die Konfiguration der Uhrzeit für einen DFS-Rescan auch über LANconfig möglich.

12.6 P2P-Unterstützung für 802.11ac

Ab LCOS-Version 9.10 ist der Aufbau von P2P-Verbindungen auch für 802.11ac-Module möglich. Dabei kann die Distanz zwischen zwei Access Points bis zu einem Kilometer (1km) betragen.

Die maximale Entfernung hängt von dem verwendeten Antennensystem ab.

12.7 Client-Modus für 802.11ac

Ab LCOS-Version 9.10 ist der Client-Modus auch für 802.11ac-Module möglich. Dabei kann die Distanz zwischen zwei Access Points bis zu einem Kilometer (1km) betragen.

Die maximale Entfernung hängt von dem verwendeten Antennensystem ab.

12.8 Bandbreitenlimit pro WLAN-Client je SSID

Ab LCOS-Version 9.10 ist eine Begrenzung der Bandbreite für WLAN-Clients pauschal je SSID möglich.

Client TX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

Client RX Bandbr.-Begrenzung

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert `0` deaktiviert die Begrenzung.

12.8.1 Ergänzungen im Setup-Menü

Pro-Client-Tx-Limit

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Senderichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert 0 deaktiviert die Begrenzung.

SNMP-ID:

2.23.20.1.23

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

Deaktiviert die Begrenzung.

Pro-Client-Rx-Limit

Hier begrenzen Sie die Bandbreite (Limit in kBit/s) in Empfangsrichtung, die jedem WLAN-Client auf dieser SSID zur Verfügung steht. Der Wert 0 deaktiviert die Begrenzung.

SNMP-ID:

2.23.20.1.24

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

Deaktiviert die Begrenzung.

12.9 Opportunistic Key Caching (OKC) auf Client-Seite einstellbar

Ab LCOS-Version 9.10 ist das OKC auch für Geräte im Client-Modus einstellbar.

12.9.1 Ergänzungen im Setup-Menü

OKC

Diese Option aktiviert oder deaktiviert das Opportunistic Key Caching (OKC).

Diesen Wert übernimmt das Gerät ausschließlich, wenn die Schnittstelle im Client-Modus arbeitet. Befindet sich die Schnittstelle im AP-Modus, ist die Aktivierung oder Deaktivierung von OKC nur über die Profilverwaltung eines WLCs möglich.

Im PMK-Caching-Status unter **Status** > **WLAN** > **PMK-Caching** > **Inhalt** sind OKC-PMKs an der Authenticator-Adresse `ff:ff:ff:ff:ff:`n zu erkennen, wobei n die zugeordnete Profilnummer ist (z. B. `0` für „WLAN-1“, `1` für „WLAN1-2“ etc.).

SNMP-ID:

2.23.20.3.17

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Verschlüsselung**

Mögliche Werte:

ja
nein

Default-Wert:

ja

13 WLAN-Management

13.1 AutoWDS-Betrieb

13.1.1 Ergänzungen im Status-Menü

CAPWAP-Aktiv

Zeigt an, ob CAPWAP aktiv ist.

SNMP-ID:

1.59.109.2

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Betrieb**

Mögliche Werte:

Nein
Ja

CAPWAP-Erneut-Aktiv-Nach-Konfig

Zeigt an, ob CAPWAP nach erfolgter Konfiguration wieder aktiv ist.

SNMP-ID:

1.59.109.3

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Betrieb**

Mögliche Werte:

Nein
Ja

AutoWDS-Fallback-Timer

Zeigt den Wert des AutoWDS-Fallback-Timers an.

SNMP-ID:

1.59.109.4

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Betrieb**

AutoWDS-Fallback-Force-Deassoc-Timer

Zeigt den Wert des AutoWDS-Fallback-Force-Deassoc-Timers an.

SNMP-ID:

1.59.109.5

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Betrieb**

CAPWAP-Continuation-Timer

Zeigt den Wert des CAPWAP-Continuation-Timers an.

SNMP-ID:

1.59.109.6

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Betrieb**

CAPWAP-Silent-Timer

Zeigt den Wert des CAPWAP-Silent-Timers an.

SNMP-ID:

1.59.109.7

Pfad Telnet:

Status > **WLAN-Management** > **AutoWDS-Betrieb**

13.2 Beantwortung von CAPWAP-Anfragen einer WAN-Gegenstelle deaktivieren

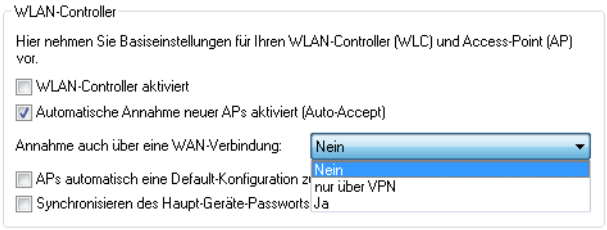
Ab LCOS-Version 9.10 ist es möglich, die Beantwortung von CAPWAP-Anfragen einer WAN-Gegenstelle zu deaktivieren.

13.2.1 Schutz vor unberechtigtem CAPWAP-Zugriff aus dem WAN

Der WLC oder LANCOM-Router mit aktiver WLC-Option behandelt CAPWAP-Anfragen aus dem LAN und dem WAN identisch. Bei Anfragen von unbekannten WAN-Gegenstellen übernimmt er die APs in seine AP-Verwaltung und übergibt

ggf. eine Default-Konfiguration. Entsprechend konfiguriert ignoriert der WLC trotz automatischer AP-Annahme und automatischer Zuweisung einer Default-Konfiguration die CAPWAP-Anfragen einer WAN-Gegenstelle.

Die Konfiguration erfolgt unter **WLAN-Controller** > **Allgemein** im Bereich **WLAN-Controller**. Ist die automatische Annahme neuer APs aktiviert, können Sie unter **Annahme auch über eine WAN-Verbindung** diese Funktion einschränken.



Nein

Das Gerät nimmt keine neuen APs über die WAN-Verbindung an.

Nur über VPN

Das Gerät nimmt nur neue APs an, wenn die WAN-Verbindung über VPN erfolgt.

Ja

Das Gerät nimmt alle neuen APs über die WAN-Verbindung an.

13.2.2 Ergänzungen im Setup-Menü

Erlaube-WAN-Verbindungen

Um bei CAPWAP-Anfragen von unbekannten WAN-Gegenstellen diesen APs nicht versehentlich eine Default-Konfiguration mit internen Netzwerkeinstellungen zuzuweisen, konfigurieren Sie hier, wie der WLC mit solchen Anfragen aus dem WAN umgehen soll.

SNMP-ID:

2.37.29

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Werte:

Ja

Der WLC übernimmt einen über WAN anfragenden AP in die AP-Verwaltung und übergibt bei entsprechender Einstellung eine Default-Konfiguration.

VPN

Der WLC übernimmt einen über WAN anfragenden AP in die AP-Verwaltung und übergibt bei entsprechender Einstellung eine Default-Konfiguration, wenn die WAN-Verbindung über einen VPN-Tunnel besteht.

Nein

Der WLC übernimmt einen über WAN anfragenden AP nicht in die AP-Verwaltung.

Default-Wert:

Nein

13.3 Zusätzliche Datumsangabe beim zentralen Firmware-Management

Ab LCOS-Version 9.10 ist im WLC die Tabelle für das zentrale Firmware-Management um eine Datumsangabe erweitert.

13.3.1 Firmware-Management-Tabelle

In dieser Tabelle wird hinterlegt, welche Geräte (MAC-Adresse) und Gerätetypen mit welcher Firmware betrieben werden sollen.

Gerätetypen

Wählen Sie hier aus, für welchen Gerätetyp die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

- Mögliche Werte: Alle oder Auswahl aus der Liste der verfügbaren Gerätetypen.
- Default: Alle

MAC-Adresse

Wählen Sie hier aus, für welches Gerät (identifiziert anhand der MAC-Adresse) die in diesem Eintrag spezifizierte Firmware-Version verwendet werden soll.

- Mögliche Werte: Gültige MAC-Adresse.
- Default: Leer

Version

Firmware-Version, welche für die in diesem Eintrag spezifizierten Geräte oder Gerätetypen verwendet werden soll.

- Mögliche Werte: Firmware-Version in der Form `X.XX`
- Default: Leer

Datum

Das Datum ermöglicht ein Downgrade auf eine spezifische Firmware-Version innerhalb einer Release, z. B. von einem Release-Upgrade (RU) auf ein früheres Upgrade.

- Mögliche Werte: 8 Zeichen aus 0123456789. Der Eintrag muss dem Format des UPX-Headers entsprechen, also z. B. "01092014" für den 01.09.2014.
- Default: Leer

13.3.2 Ergänzungen im Setup-Menü

Datum

Datum der entsprechenden Firmware-Version.

SNMP-ID:

2.37.27.15.5

Pfad Telnet:

Setup > **WLAN-Management** > **Zentrales-Firmware-Management** > **Firmware-Versionsverwaltung**

Mögliche Werte:

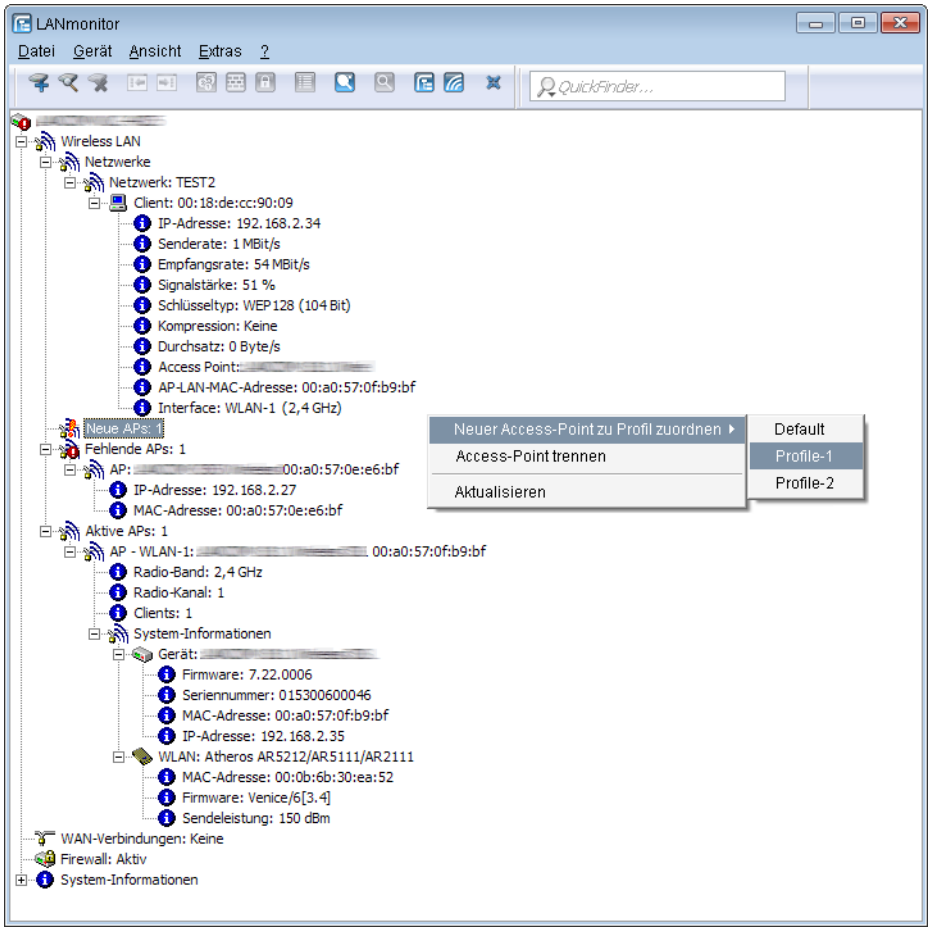
max. 8 Zeichen aus `[0-9]`

Default-Wert:

Entspricht dem UPX-Header der Firmware (z. B. "01072014" für den 01.07.2014)

13.4 Anzeige von Kanal und Frequenz der am AP angemeldeten Clients

Ab LCOS-Version 9.10 zeigt die Stations-Tabelle im WLC auch den Kanal und die Frequenz der an aktiven WLAN-Netzwerken angemeldeten Clients an.



Falls der AP wegen einer älteren Firmware diese Daten nicht überträgt, entnimmt der WLC den Kanal und die Frequenz aus der Status-Tabelle **Aktive-Radios** unter **Status** > **Aktive-Radios** > **WLAN-Management** > **AP-Status**.

13.4.1 Ergänzungen im Status-Menü

Radio-Band

Dieser Wert zeigt das Radio-Band an, das der am AP angemeldete Client verwendet.

SNMP-ID:

1.73.100.27

Pfad Telnet:

Status > **WLAN-Management** > **Stationstabelle**

Mögliche Werte:

0

unbekannt

2.4GHz

Der Client verwendet das 2,4GHz-Band.

5GHz

Der Client verwendet das 5GHz-Band.

Radio-Kanal

Dieser Wert zeigt den Kanal an, den der am AP angemeldete Client verwendet.

SNMP-ID:

1.73.100.28

Pfad Telnet:

Status > **WLAN-Management** > **Stationstabelle**

Mögliche Werte:

1 … 140

13.5 Backup der Zertifikate über LANconfig anlegen

Ab LCOS-Version 9.10 ist das Backup und Einspielen von Zertifikaten auch vollständig über LANconfig möglich.

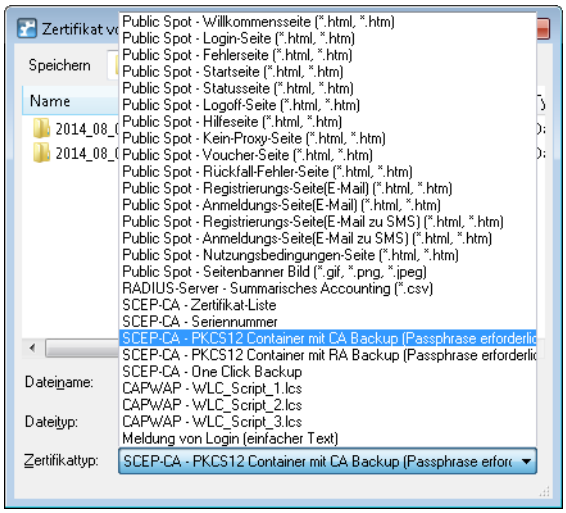
13.5.1 Backup und Einspielen der Zertifikate über LANconfig

Um die Zertifikate über LANconfig zu speichern und hochzuladen, gehen Sie wie folgt vor:

Speichern

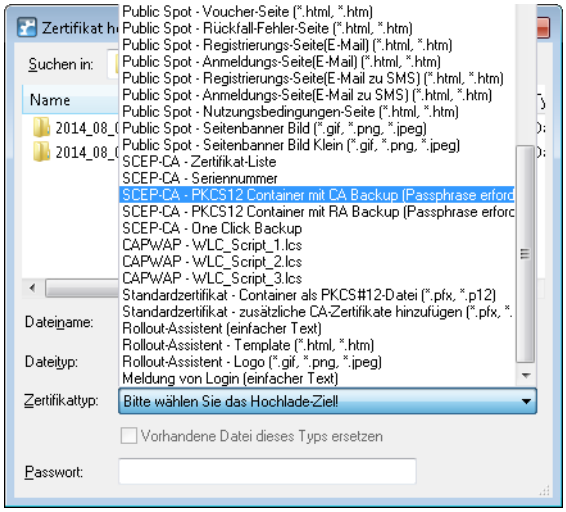
1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat als Datei sichern**.

2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container-Typ aus und klicken Sie auf **Speichern**.



Hochladen

1. Markieren Sie den entsprechenden WLC in der Geräteübersicht und wählen Sie im Menü **Gerät** > **Konfigurations-Verwaltung** den Punkt **Zertifikat oder Datei hochladen**.
2. Wählen Sie in der Liste **Zertifikattyp** den gewünschten PKCS12-Container-Typ aus.
3. Navigieren Sie anschließend zur gewünschten Datei, geben Sie ggf. ein Passwort an und klicken Sie auf **Öffnen**.



One Click Backup

Für das One Click Backup wählen Sie aus der Dialogliste jeweils den Eintrag "SCEP-CA - One Click Backup" aus.

13.6 Anzeige des Zertifikatsstatus eines APs

Ab LCOS-Version 9.10 überträgt ein AP seinen Zertifikatsstatus an den WLC.

13.6.1 Ergänzungen im Status-Menü

Zertifikat-Status

Zeigt den Status des APs an.

SNMP-ID:

1.73.9.3.9

Pfad Telnet:

Status > **WLAN-Management** > **AP-Status** > **Neue-AP**

Mögliche Werte:

0

unbekannt (Standard für APs mit älterer Firmware)

1

fehlt

2

abgelaufen

3

inkompatibel (Zertifikat passt nicht zur CA-Chain des WLC)

4

noch nicht gültig (z. B., wenn Uhren in WLC und AP nicht synchron laufen)

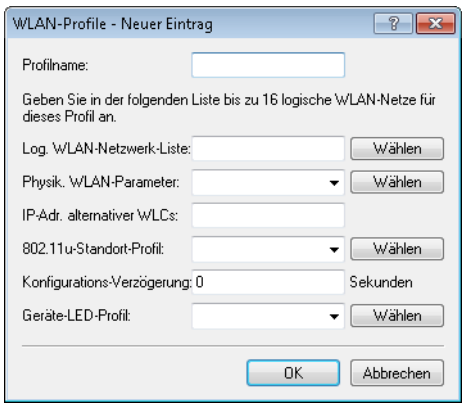
5

gültig

13.7 AP-LEDs per WLC schalten

Ab LCOS-Version 9.10 lassen sich in Multi-AP-Umgebungen die Geräte-LEDs jedes APs über einen WLC separat konfigurieren.

Für jedes WLAN-Profil können Sie unter **WLAN-Controller** > **Profile** > **WLAN-Profile** die folgenden Parameter definieren:

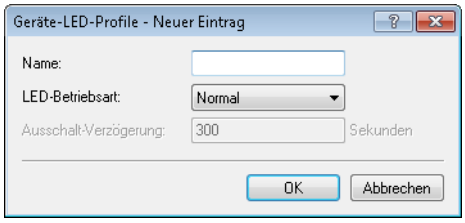


Geräte-LED-Profil

Wählen Sie aus der Liste der Geräte-LED-Profile das Profil aus, das im WLAN-Profil gelten soll. Die Geräte-LED-Profile verwalten Sie unter **WLAN-Controller** > **Profile** > **Geräte-LED-Profile**.

13.7.1 Geräte-LED-Profile

Die Geräte-LEDs lassen sich am Gerät konfigurieren, um den AP unauffällig betreiben zu können. Um diese Konfiguration auch über einen WLC durchzuführen, erstellen Sie unter **WLAN-Controller** > **Profile** > **Geräte-LED-Profile** entsprechende Profile, die Sie anschließend einem WLAN-Profil zuordnen.



Name

Vergeben Sie hier einen Namen für das Geräte-LED-Profil.

LED-Betriebsart

Die folgenden Optionen stehen zur Auswahl:

- **Normal**: Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.
- **Verzögert aus**: Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.
- **Alle aus**: Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Ausschalt-Verzögerung

In der Betriebsart **Verzögert aus** können Sie im Feld **LED-Ausschalt-Verzögerung** die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll.

13.7.2 Ergänzungen im Setup-Menü

LED-Profile

Die Geräte-LEDs lassen sich am Gerät konfigurieren, um den AP unauffällig betreiben zu können. Um diese Konfiguration auch über einen WLC durchzuführen, erstellen Sie hier entsprechende Profile, die Sie anschließend einem WLAN-Profil zuordnen.

SNMP-ID:

2.37.1.21

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

Name

Vergeben Sie hier einen Namen für das Geräte-LED-Profil.

SNMP-ID:

2.37.1.21.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]`

Default-Wert:

leer

LED-Modus

Bestimmen Sie hier die LED-Betriebsart.

SNMP-ID:

2.37.1.21.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

An

Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.

Aus

Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Zeitgesteuert-Aus

Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.

Default-Wert:

An

LED-Ausschalten-Sekunden

In der Betriebsart **Verzögert aus** können Sie hier die Dauer in Sekunden festlegen, nach der das Gerät die LEDs bei einem Neustart deaktivieren soll. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.

SNMP-ID:

2.37.1.21.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

300

LED-Profil

Wählen Sie aus der Liste der Geräte-LED-Profile das Profil aus, das im WLAN-Profil gelten soll.

SNMP-ID:

2.37.1.3.8

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Gesamtprofile**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]`

Default-Wert:

leer

13.7.3 Ergänzungen im Status-Menü

LED-Profile

Dieser Eintrag zeigt die angelegten LED-Profile an.

SNMP-ID:

1.59.110

Pfad Telnet:

Status > **WLAN-Management**

LED-Profil

Zeigt Informationen zu den eingerichteten LED-Profilen an.

SNMP-ID:

1.73.2.23

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Name

Zeigt den Namen des LED-Profils an.

SNMP-ID:

1.73.2.23.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]`

Default-Wert:

leer

LED-Modus

Zeigt die LED-Betriebsart an.

SNMP-ID:

1.73.2.23.4

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

An

Die LEDs sind immer aktiviert, auch nach einem Neustart des Gerätes.

Aus

Die LEDs sind alle deaktiviert. Auch nach einem Neustart des Gerätes bleiben die LEDs deaktiviert.

Zeitgesteuert-Aus

Nach einem Neustart sind die LEDs für einen bestimmten Zeitraum aktiviert, danach schalten sie sich aus. Das ist dann hilfreich, wenn die LEDs während des Neustarts auf kritische Fehler hinweisen.

LED-Ausschalten-Sekunden

In der Betriebsart **Verzögert aus** zeigt diese Spalte an, nach wievielen Sekunden das Gerät die LEDs bei einem Neustart deaktiviert.

SNMP-ID:

1.73.2.23.5

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **LED-Profile**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

300

LED-Profil

Diese Spalte zeigt das zugewiesene LED-Profil an.

SNMP-ID:

1.73.2.3.8

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **Gesamtprofile**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][a-z][0-9]`

Default-Wert:

leer

LED-Prof.-Fehler

Enthält Fehlercodes, die die Geräte-LEDs anzeigen.

SNMP-ID:

1.73.2.22

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration**

Index

Enthält den aufsteigenden Index der Fehlermeldungen.

SNMP-ID:

1.73.2.22.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **LED-Prof.-Fehler**

Index

Enthält den Namen des LED-Profils.

SNMP-ID:

1.73.2.22.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **LED-Prof.-Fehler**

Fehler

Enthält den aufgetretenen Fehler.

SNMP-ID:

1.73.2.22.3

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **LED-Prof.-Fehler**

Mögliche Werte:

keine

Kein Fehler aufgetreten

Vererbungsfehler
Kein-Profil
Profil-nicht-gefunden
Kein-Speicher
SSID-fehlt
Netzwerk-nicht-gefunden
AP-Parameter-nicht-gefunden
AP-Intranet-nicht-gefunden
RADIUS-Profil-nicht-gefunden
AutoWDS-Profil-nicht-gefunden
Master-ist-gleich-Slave
kein-Profile-weder-Gruppe-gefunden
Info-Profile-gewinnt-Gruppe
Gruppe-falsche-definiert
SSID-WLC-tunnel-fehlt
SSID-Datenverkehr-zw-Stationen-erlaubt
zu-viele-Netzwerke-fuer-AutoWDS
Gemeldet-von-AP

13.8 Verwaltung von Wireless ePaper- und iBeacon-Profilen mit WLCs

Ab LCOS-Version 9.10 ist die Erstellung und Verteilung von Wireless ePaper- und iBeacon-Profilen für Access Points der E-Serie möglich.

13.9 Ergänzungen im Status-Menü

13.9.1 Statistikdaten-erfassen

Dieser Eintrag zeigt Ihnen, ob das Gerät Statistikdaten erfasst.

SNMP-ID:

1.73.123.9

Pfad Telnet:

Status > **WLAN-Management** > **Client-Steering**

Mögliche Werte:

Ja

Das Gerät erfasst Statistikdaten.

Nein

Das Gerät erfasst keine Statistikdaten.

14 LANCOM Location Based Services (LBS)

14.1 Grundlagen

LANCOM Location Based Services (LBS) nutzen die gemeldete oder erkannte Position eines WLAN-Clients, um ihm positionsabhängige Informationen zukommen zu lassen, wenn der Client für diesen Empfang registriert ist. Die folgenden Szenarien sind denkbar:

Aktive Informationsanzeige

Auf dem Client (z. B. ein Smartphone) ist eine anbieterspezifische Anwendung installiert, die den Kontakt zu den APs in einem definierten Bereich hält. Die APs senden diese Anfragen an einen Server, der die Verwaltung von Kunden und positionsabhängigen Informationen übernimmt. Wechselt der Client die WLAN-Funkzelle, gibt der aktuelle AP diese Information an den LBS-Server weiter, der daraufhin die für diese WLAN-Funkzelle gültigen und für diesen Client freigegebenen Informationen zurücksendet.

Beispiel: Ein Freizeitpark installiert APs jeweils in der Nähe seiner Attraktionen für ein flächendeckendes WLAN. Beim Eintritt in den Park installiert und startet der Besucher eine spezielle Anwendung auf seinem Smartphone (WLAN-Client) und meldet sich für diverse Info-Dienste an. Wechselt der Besucher nun von einer Funkzelle in die benachbarte, sendet der Server ihm Informationen über Wartezeiten vor Fahrgeschäften oder Angebote in Restaurants in seiner Nähe auf sein Smartphone.

Passive Informationsauswertung

Ebenso ist es möglich, dass der LBS-Anbieter die Bewegungsdaten der Clients nutzt, um damit Verkehrsströme zu erfassen und z. B. Verbindungswege zu optimieren. Sobald der Client die WLAN-Funkzelle wechselt, gibt der aktuelle AP diese Information an den LBS-Server weiter. Der sammelt die Daten und erstellt daraus z. B. eine Heatmap aller Clients im gesamten WLAN-Bereich.

Beispiel:

14.2 LBS mit LANconfig konfigurieren

LANCOM Location Based Services konfigurieren Sie unter **Location Based Services** > **Allgemein**.

Location Based Services aktiviert

Aktiviert bzw. deaktiviert die ortsbasierenden Dienste.

LBS Server-Adresse

Geben Sie hier die IPv4-Adresse des LBS-Servers ein.

LBS Server-Port

Geben Sie hier den Port des LBS-Servers ein (Default: 9091).

Beschreibung

Geben Sie hier eine Beschreibung des Gerätes ein.

Stockwerk

Geben Sie hier die Etage ein, auf der sich das Gerät befindet. So differenzieren Sie z B. zwischen Ober- und Untergeschoss.

Höhe

Geben Sie hier die Höhe ein, auf der sich das Gerät befindet. Die Angabe eines negativen Wertes ist möglich, so dass Sie zwischen einer Position über und unter dem Meeresspiegel differenzieren können.

Mit **Koordinaten** bestimmen Sie die Standortkoordinaten des Gerätes. Die Angabe erfolgt im geographischen Koordinatensystem (Grad, Minute, Sekunde, Orientierung).

Das Auswahlfeld **Hemisphäre** gibt die Orientierung des geographischen Koordinatensystems an.

Für die geographische Breite (Latitude) sind folgende Werte möglich:

- Nord: nördliche Breite (Default)
- Süd: südliche Breite

Für die geographische Länge (Longitude) sind folgende Werte möglich:

- Ost: östliche Länge (Default)
- West: westliche Länge

14.3 Ergänzungen im Status-Menü

14.3.1 LBS

Dieses Menü zeigt Ihnen die Einstellungen für die LANCOM Location Based Services (LBS) an.

SNMP-ID:

1.59.111

Pfad Telnet:

Status > **WLAN-Management**

Allgemein

Dieser Eintrag zeigt Ihnen die allgemeinen Einstellungen für die LANCOM Location Based Services (LBS).

SNMP-ID:

1.59.111.1

Pfad Telnet:

Status > **WLAN-Management** > **LBS**

Mögliche Werte:

Name

Dieser Eintrag zeigt Ihnen den Namen des LANCOM Location Based Services (LBS) an.

Aktiv

Dieser Eintrag zeigt Ihnen an, ob LANCOM Location Based Services (LBS) aktiv sind. Mögliche Werte sind:

- ja
- nein

TLS-Verbindung verwenden

Dieser Eintrag zeigt Ihnen an, ob TLS-Verbindungen verwendet werden. Mögliche Werte sind:

- ja
- nein

LBS-Server-Adresse

Dieser Wert zeigt Ihnen die IPv4-Adresse des LBS-Servers an.

Mögliche Werte:

LBS-Server-Port

Dieser Wert zeigt Ihnen den verwendeten Port des LBS-Servers an.

Device-Location

Dieser Eintrag zeigt Ihnen den Standort Ihres Gerätes an.

SNMP-ID:

1.59.111.2

Pfad Telnet:

Status > **WLAN-Management** > **LBS**

Mögliche Werte:

Name
Dieser Eintrag zeigt Ihnen den Namen des Gerätes an.

Etage
Dieser Eintrag zeigt Ihnen an, auf welcher Etage sich Ihr Gerät befindet.

Höhe
Dieser Eintrag zeigt Ihnen an, in welcher Höhe sich Ihr Gerät befindet.

Breitengrad
Dieser Wert zeigt Ihnen an, auf welchem Breitengrad sich Ihr Gerät befindet.

Mögliche Werte:

Breitengrad-Minuten
Breitengrad-Sekunden
Breitengrad-Hemisphäre
Dieser Wert zeigt Ihnen an, auf welchem Teil der Erdhalbkugel sich Ihr Gerät befindet. Mögliche Werte sind:

- N
- S

Längengrad
Dieser Wert zeigt Ihnen an, auf welchem Längengrad sich Ihr Gerät befindet.

Längengrad-Minuten
Längengrad-Sekunden
Längengrad-Hemisphäre
Dieser Wert zeigt Ihnen die Hemisphäre bezüglich des Nullmeridians an. Mögliche Werte sind:

- O
- W

Beschreibung
Dieser Eintrag zeigt Ihnen eine Beschreibung des Gerätestandorts an.

14.3.2 LBS

Dieses Menü zeigt Ihnen die Einstellungen für die LANCOM Location Based Services (LBS) an.

SNMP-ID:
1.73.2.24

Pfad Telnet:
Status > **WLAN-Management** > **AP-Configuration**

Allgemein

Dieser Eintrag zeigt Ihnen die allgemeinen Einstellungen für die LANCOM Location Based Services (LBS).

SNMP-ID:

1.73.2.24.1

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **LBS**

Mögliche Werte:

Name

Dieser Eintrag zeigt Ihnen den Namen des LANCOM Location Based Services (LBS) an.

Aktiv

Dieser Eintrag zeigt Ihnen an, ob LANCOM Location Based Services (LBS) aktiv sind. Mögliche Werte sind:

- ja
- nein

TLS-Verbindung verwenden

Dieser Eintrag zeigt Ihnen an, ob TLS-Verbindungen verwendet werden. Mögliche Werte sind:

- ja
- nein

LBS-Server-Adresse

Dieser Wert zeigt Ihnen die IPv4-Adresse des LBS-Servers an.

Mögliche Werte:

LBS-Server-Port

Dieser Wert zeigt Ihnen den verwendeten Port des LBS-Servers an.

Device-Location

Dieser Eintrag zeigt Ihnen den Standort Ihres Gerätes an.

SNMP-ID:

1.73.2.24.2

Pfad Telnet:

Status > **WLAN-Management** > **AP-Konfiguration** > **LBS**

Mögliche Werte:

Name

Dieser Eintrag zeigt Ihnen den Namen des Gerätes an.

Etage

Dieser Eintrag zeigt Ihnen an, auf welcher Etage sich Ihr Gerät befindet.

Höhe

Dieser Eintrag zeigt Ihnen an, in welcher Höhe sich Ihr Gerät befindet.

Breitengrad

Dieser Wert zeigt Ihnen an, auf welchem Breitengrad sich Ihr Gerät befindet.

Mögliche Werte:

Breitengrad-Minuten
Breitengrad-Sekunden
Breitengrad-Hemisphäre

Dieser Wert zeigt Ihnen an, auf welchem Teil der Erdhalbkugel sich Ihr Gerät befindet. Mögliche Werte sind:

- N
- S

Längengrad

Dieser Wert zeigt Ihnen an, auf welchem Längengrad sich Ihr Gerät befindet.

Längengrad-Minuten
Längengrad-Sekunden
Längengrad-Hemisphäre

Dieser Wert zeigt Ihnen die Hemisphäre bezüglich des Nullmeridians an. Mögliche Werte sind:

- O
- W

Beschreibung

Dieser Eintrag zeigt Ihnen eine Beschreibung des Gerätestandorts an.

14.3.3 LBS

Dieses Menü zeigt Ihnen die Einstellungen für die LANCOM Location Based Services (LBS) an.

SNMP-ID:

1.101

Pfad Telnet:

Status

Log-Tabelle

Dieser Eintrag zeigt Ihnen die Log-Tabelle der LANCOM Location Based Services (LBS) an.

SNMP-ID:

1.101.1

Pfad Telnet:

Status > **LBS**

Mögliche Werte:

Index

Ordnet jedem Eintrag eine eindeutige Nummer zu.

Zeit

Gibt an, wann ein Log-Eintrag angelegt wurde.

Ereignis

Enthält genauere Informationen zum Grund des Log-Eintrages.

Cache-Max-Groesse

Dieser Eintrag zeigt Ihnen die maximale Cache-Größe für die LANCOM Location Based Services (LBS) an.

SNMP-ID:

1.101.2

Pfad Telnet:

Status > **LBS**

Cache-Belegt

Dieser Eintrag zeigt Ihnen an, wie viel Cache die LANCOM Location Based Services (LBS) belegen.

SNMP-ID:

1.101.3

Pfad Telnet:

Status > **LBS**

Cache-Zaehler

Zeigt die Anzahl der Einträge im Cache.

SNMP-ID:

1.101.4

Pfad Telnet:

Status > **LBS**

14.4 Ergänzungen im Setup-Menü

14.4.1 LBS-Tracking

Bestimmen Sie hier, ob der LBS-Server die am Public-Spot angemeldeten Benutzer nachverfolgen darf.

SNMP-ID:

2.24.38

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

nein
ja

Default-Wert:

nein

14.4.2 LBS-Tracking-Liste

Name der LBS-Tracking-Liste

SNMP-ID:

2.24.39

Pfad Telnet:

Setup > **Public-Spot-Modul**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default-Wert:

leer

14.4.3 LBS-Tracking

Diese Option gibt an, ob der LBS-Server die Client-Informationen nachverfolgen darf.

Diese Option konfiguriert das Tracking aller Clients einer SSID. Im Public-Spot-Modul bestimmen Sie, ob der LBS-Server die am Public-Spot angemeldeten Benutzer tracken darf.

SNMP-ID:

2.37.1.1.46

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Netzwerkprofile**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

14.4.4 LBS

Konfigurieren Sie hier die Einstellungen für die LANCOM Location Based Services (LBS).

SNMP-ID:

2.37.1.22

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

Allgemein

In diesem Verzeichnis konfigurieren Sie die allgemeinen Einstellungen für die LANCOM Location Based Services (LBS).

SNMP-ID:

2.37.1.22.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS**

Name

Geben Sie hier eine Beschreibung des Gerätes ein.

SNMP-ID:

2.37.1.22.1.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

max. 251 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Aktiv

Aktiviert oder deaktiviert die ortsbasierten Dienste.

SNMP-ID:

2.37.1.22.1.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

ja
nein

Default-Wert:

nein

TLS-Verbindung-Verwenden

Diese Einstellung legt fest, ob die Verbindung zur LBSEngine SSL/TLS-gesichert ist.

Das Gerät übernimmt eine Änderung nicht im laufenden Betrieb, sondern erst nach einer erneuten Aktivierung der LBS.

SNMP-ID:

2.37.1.22.1.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

ja
nein

LBS-Server-Adresse

Geben Sie hier die Adresse des LBS-Servers ein.

SNMP-ID:

2.37.1.22.1.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

LBS-Server-Port

Geben Sie hier den Port des LBS-Servers ein.

SNMP-ID:

2.37.1.22.1.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Allgemein**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

9090

Device-Location

In dieser Tabelle bestimmen Sie die Standortkoordinaten des Gerätes. Die Angabe erfolgt im geographischen Koordinatensystem (Grad, Minute, Sekunde, Orientierung).

SNMP-ID:

2.37.1.22.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS**

Name

Geben Sie hier eine Beschreibung des Gerätes ein.

SNMP-ID:

2.37.1.22.2.1

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 251 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Etage

Geben Sie hier die Etage ein, auf der sich das Gerät befindet. So differenzieren Sie z. B. zwischen Ober- und Untergeschoss.

SNMP-ID:

2.37.1.22.2.2

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]-`

Default-Wert:

0

Hoehe

Geben Sie hier die Höhe ein, auf der sich das Gerät befindet. Die Angabe eines negativen Wertes ist möglich, so dass Sie zwischen einer Position über und unter dem Meeresspiegel differenzieren können.

SNMP-ID:

2.37.1.22.2.3

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]-`

Default-Wert:

0

Breitengrad

Dieser Wert gibt den Winkel des Breitengrades in Grad an.

SNMP-ID:

2.37.1.22.2.4

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

0 … 90

Default-Wert:

0

Breitengrad-Minuten

Dieser Wert gibt die Minute des Breitengrades an.

SNMP-ID:

2.37.1.22.2.5

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

0 … 60

Default-Wert:

0

Breitengrad-Sekunden

Dieser Wert gibt die Sekunde des Breitengrades an.

SNMP-ID:

2.37.1.22.2.6

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

0 … 60

Default-Wert:

0

Breitengrad-Hemisphaere

Dieser Wert gibt die Orientierung des Breitengrades (Latitude) an. Mögliche Werte sind:

- N: nördliche Breite
- S: südliche Breite

SNMP-ID:

2.37.1.22.2.7

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

N
S

Default-Wert:

N

Laengengrad

Dieser Wert gibt den Winkel des Längengrades in Grad an.

SNMP-ID:

2.37.1.22.2.8

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

0 … 90

Default-Wert:

0

Laengengrad-Minuten

Dieser Wert gibt die Minute des Längengrades an.

SNMP-ID:

2.37.1.22.2.9

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

0 … 60

Default-Wert:

0

Laengengrad-Sekunden

Dieser Wert gibt die Sekunde des Längengrades an.

SNMP-ID:

2.37.1.22.2.10

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 2 Zeichen aus `[0-9]`

0 … 60

Default-Wert:

0

Laengengrad-Hemisphaere

Dieser Wert gibt die Orientierung des Längengrades (Longititude) an. Mögliche Werte sind:

- W: Westliche Länge
- O: Östliche Länge

SNMP-ID:

2.37.1.22.2.8

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

O
W

Default-Wert:

W

Beschreibung

Geben Sie hier eine Beschreibung des Gerätes ein.

SNMP-ID:

2.37.1.22.2.12

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **LBS** > **Device-Location**

Mögliche Werte:

max. 251 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

14.4.5 LBS

Konfigurieren Sie hier die Einstellungen für die LANCOM Location Based Services (LBS).

SNMP-ID:

2.100

Pfad Telnet:

Setup

Operating

Aktiviert bzw. deaktiviert die ortsbasierenden Dienste.

SNMP-ID:

2.100.1

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Beschreibung

Geben Sie hier eine Beschreibung des Gerätes ein.

SNMP-ID:

2.100.2

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

max. 251 Zeichen aus `#[A-Z][a-z][0-9]@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Etage

Geben Sie hier die Etage ein, auf der sich das Gerät befindet. So differenzieren Sie z. B. zwischen Ober- und Untergeschoss.

SNMP-ID:

2.100.3

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]-`

Default-Wert:

0

Höhe

Geben Sie hier die Höhe ein, auf der sich das Gerät befindet. Die Angabe eines negativen Wertes ist möglich, so dass Sie zwischen einer Position über und unter dem Meeresspiegel differenzieren können.

SNMP-ID:

2.100.4

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

max. 6 Zeichen aus `[0-9]-`

Default-Wert:

0

Koordinaten

In dieser Tabelle bestimmen Sie die Standortkoordinaten des Gerätes. Die Angabe erfolgt im geographischen Koordinatensystem (Grad, Minute, Sekunde, Orientierung).

SNMP-ID:

2.100.5

Pfad Telnet:

Setup > **LBS**

Index

Diese Spalte gibt an, ob es sich beim Eintrag um die Latitude (geographische Breite) oder die Longitude (geographische Länge) handelt.

Sie können diesen Eintrag nicht ändern.

SNMP-ID:

2.100.5.1

Pfad Telnet:

Setup > **LBS** > **Koordinaten**

Mögliche Werte:

Latitude
Longitude

Grad

Diese Spalte gibt den Winkel in Grad des geographischen Koordinatensystems an.

SNMP-ID:

2.100.5.2

Pfad Telnet:

Setup > **LBS** > **Koordinaten**

Mögliche Werte:

max 2 Zeichen aus `[0-9]`

0 … 90

Default-Wert:

0

Minute

Diese Spalte gibt die Minute des geographischen Koordinatensystems an.

SNMP-ID:

2.100.5.3

Pfad Telnet:

Setup > **LBS** > **Koordinaten**

Mögliche Werte:

max 2 Zeichen aus `[0-9]`

0 … 60

Default-Wert:

0

Sekunde

Diese Spalte gibt die Sekunde des geographischen Koordinatensystems an.

SNMP-ID:

2.100.5.4

Pfad Telnet:

Setup > **LBS** > **Koordinaten**

Mögliche Werte:

max 2 Zeichen aus `[0-9]`

0 … 60

Default-Wert:

0

Orientierung

Diese Spalte gibt die Orientierung des geographischen Koordinatensystems an.

Für die geographische Breite (Latitude) sind folgende Werte möglich:

- N: nördliche Breite
- S: südliche Breite

Für die geographische Länge (Longitude) sind folgende Werte möglich:

- O: östliche Länge
- W: westliche Länge

SNMP-ID:

2.100.5.5

Pfad Telnet:

Setup > **LBS** > **Koordinaten**

Mögliche Werte:

N
S
O
W

Default-Wert:

N

0

LBS-Server-Adresse

Geben Sie hier die Adresse des LBS-Servers ein.

SNMP-ID:

2.100.6

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

LBSEngine-Port

Geben Sie hier den Port des LBS-Servers ein.

SNMP-ID:

2.100.7

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

9090

TLS-Verbindung-benutzen

Diese Einstellung legt fest, ob die Verbindung zur LBSEngine SSL/TLS-gesichert ist.

Das Gerät übernimmt eine Änderung nicht im laufenden Betrieb, sondern erst nach einer erneuten Aktivierung der LBS.

SNMP-ID:

2.100.8

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

Ja
Nein

Default-Wert:

Ja

TLS_Client-Einstellungen

In diesem Menü konfigurieren Sie die Einstellungen für eine SSL/TLS-gesicherte Verbindung zur LBSEngine.

SNMP-ID:

2.100.9

Pfad Telnet:

Setup > **LBS**

Versionen

Wählen Sie hier die Verschlüsselungsprotokolle für die SSL/TLS-Verbindung aus.

SNMP-ID:

2.100.9.1

Pfad Telnet:

Setup > **LBS** > **TLS_Client-Einstellungen**

Mögliche Werte:

SSLv3
TLSv1
TLSv1.1
TLSv1.2

Default-Wert:

SSLv3

TLSv1

Keyex-Algorithmen

Wählen Sie hier die Verschlüsselungsverfahren für die SSL/TLS-Verbindung aus.

SNMP-ID:

2.100.9.2

Pfad Telnet:

Setup > **LBS** > **TLS_Client-Einstellungen**

Mögliche Werte:

RSA
DHE
ECDHE

Default-Wert:

RSA

DHE

ECDHE

Krypro-Algorithmen

Wählen Sie hier die Krypto-Algorithmen für die SSL/TLS-Verbindung aus.

SNMP-ID:

2.100.9.3

Pfad Telnet:

Setup > **LBS** > **TLS_Client-Einstellungen**

Mögliche Werte:

RC4-40
RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default-Wert:

RC4-128

3DES

AES-128

AES-256

AESGCM-128

AESGCM-256

Hash-Algorithmen

Wählen Sie hier die Hash-Algorithmen für die SSL/TLS-Verbindung aus.

SNMP-ID:

2.100.9.4

Pfad Telnet:

Setup > **LBS** > **TLS_Client-Einstellungen**

Mögliche Werte:

MD5
SHA1
SHA-2-256
SHA2-384

Default-Wert:

MD5

SHA1

SHA-2-256

SHA2-384

PFS-bevorzugen

Bestimmen Sie, ob für die SSL/TLS-gesicherte Verbindung PFS (Perfect Forward Secrecy) aktiviert ist.

SNMP-ID:

2.100.9.5

Pfad Telnet:

Setup > **LBS** > **TLS_Client-Einstellungen**

Mögliche Werte:

Ja
Nein

Default-Wert:

Ja

Loopback-Adresse

Geben Sie hier die LBS-Loopback-Adresse an.

SNMP-ID:

2.100.10

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Cache-Aktiv

Aktivieren oder deaktivieren Sie hier den LBS-Cache.

SNMP-ID:

2.100.11

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

nein
ja

Cache-Groesse

Geben Sie hier die Größe des LBS-Caches an.

SNMP-ID:

2.100.12

Pfad Telnet:

Setup > **LBS**

Mögliche Werte:

max. 10 Zeichen aus `0123456789`

15 VPN

15.1 SCEP-CA-Funktion im VPN-Umfeld

Ab LCOS-Version 9.10 ist die Nutzung der vorhandenen CA mit SCEP-Funktion im VPN-Umfeld möglich.

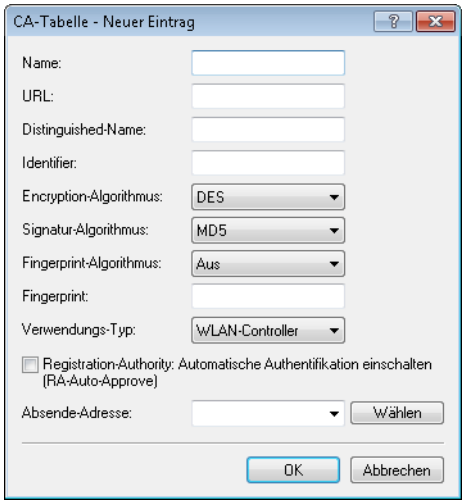
15.2 SCEP-Algorithmen aktualisiert

Ab LCOS-Version 9.10 unterstützen der SCEP-Client und -Server auch AES192 und AES256 sowie SHA256, SHA384 und SHA512.

Die Default-Einträge ändern sich nicht, um bei einem Firmware-Update die Kompatibilität zu den Gegenstellen zu wahren. Verwenden Sie die aktuellen Algorithmen nur, wenn Sie auch die Gegenstellen entsprechend angepasst haben.

15.2.1 Konfiguration der CAs

Die Konfiguration erfolgt in LANconfig unter **Zertifikate** > **SCEP-Client** mit der Schaltfläche **CA-Tabelle**.



Name

Konfigurationsname der CA.

URL

URL der CA.

Distinguished-Name

Distinguished Name der CA. Über diesen Parameter erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung, ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen.

Durch die Verwendung eines vorangestellten Backslash ("\") können Sie auch reservierte Zeichen benutzen. Diese unterstützten reservierten Zeichen sind:

- Komma (",")
- Slash ("/")
- Plus ("+")
- Semikolon (";")
- Gleich ("=")

Außerdem lassen sich die folgenden internen Firmware-Variablen nutzen:

- %% fügt ein Prozentzeichen ein.
- %f fügt die Version und das Datum der aktuellen im Gerät aktiven Firmware ein.
- %r fügt die Hardware-Release des Gerätes ein.
- %v fügt die Version des aktuellen im Gerät aktiven Loaders ein.
- %m fügt die MAC-Adresse des Gerätes ein.
- %s fügt die Seriennummer des Gerätes ein.
- %n fügt den Namen des Gerätes ein.
- %l fügt den Standort des Gerätes ein.
- %d fügt den Typ des Gerätes ein.

Identifier

CA-Identifier (wird von manchen Webservern benötigt, um die CA zuordnen zu können).

Encryption-Algorithmus

Mit diesem Algorithmus wird die Nutzlast des Zertifikatsantrags verschlüsselt. Mögliche Werte sind:

- DES (Default)
- 3-DES
- Blowfish
- AES128
- AES192
- AES256

Signatur-Algorithmus

Mit diesem Algorithmus wird der Zertifikatsantrag signiert. Mögliche Werte sind:

- MD5 (Default)
- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint-Algorithmus

Algorithmus zum Signieren der Fingerprints. Legt fest, ob eine Überprüfung der CA-Zertifikate anhand des Fingerprints vorgenommen wird und mit welchem Algorithmus. Der CA-Fingerprint muss mit der Prüfsumme übereinstimmen, der sich bei Verwendung des Algorithmus ergibt. Mögliche Werte sind:

- Aus (Default)
- MD5
- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint

Anhand der hier eingetragenen Prüfsumme (Fingerprint) kann die Authentizität des erhaltenen CA-Zertifikats überprüft werden (entsprechend des eingestellten CA-Fingerprintalgorithmus).

Verwendungs-Typ

Gibt den Verwendungszweck der eingetragenen CA an. Die hier eingetragene CA wird dann nur für den entsprechenden Verwendungszweck abgefragt. Mögliche Werte sind:

- VPN
- EAP/TLS
- WLAN-Controller
- Allgemein

Wenn eine allgemeine CA vorhanden ist, lässt sich keine weitere konfigurieren, da sonst die Wahl der CA nicht eindeutig ist.

RA-Autoapprove

Manche CAs bieten die Möglichkeit, ein bereits von dieser CA ausgestelltes Zertifikat als Nachweis der Authentizität für nachfolgende Anträge zu benutzen. Mit dieser Option wird festgelegt, ob bei bereits vorliegendem Systemzertifikat Neuanträge mit dem vorhandenen Systemzertifikat unterschrieben werden. Mögliche Werte sind:

- Ja
- Nein (Default)

Absende-Adresse

Hier konfigurieren Sie optional eine Absendeadresse, die statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet wird. Falls Sie z. B. Loopback-Adressen konfiguriert haben, können Sie diese hier als Absendeadresse angeben.

Als Adresse werden verschiedene Eingabeformen akzeptiert:

- Name des IP-Netzwerks (ARF-Netz), dessen Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets.
- "DMZ" für die Adresse der ersten DMZ (Achtung: wenn es eine Schnittstelle Namens "DMZ" gibt, dann wird deren Adresse genommen).
- LB0 ... LBF für eine der 16 Loopback-Adressen oder deren Name.
- Desweiteren kann eine beliebige IP-Adresse in der Form x.x.x.x angegeben werden.

Sofern die hier eingestellte Absendeadresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

15.2.2 Ergänzungen im Setup-Menü

Enc-Alg

Wählen Sie hier den Verschlüsselungs-Algorithmus (Encryption-Algorithmus) zur Verschlüsselung innerhalb des SCEP-Protokolls (Simple Certificate Enrollment Protocol) aus. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen. Es stehen mehrere Verfahren zur Auswahl.

Verwenden Sie nach Möglichkeit eines der letzteren Verfahren (3DES, BLOWFISH, AES), wenn die Zertifizierungsstelle (CA) und alle Clients es unterstützen. Als Standard ist hier DES-Verschlüsselung voreingestellt, um die Interoperabilität zu wahren.

SNMP-ID:

2.39.1.14.4

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-Client** > **CAs**

Mögliche Werte:

DES

Data Encryption Standard: Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel. Dies ist die SCEP-Standard-Verschlüsselung. DES ist ein vom amerikanischen National Bureau of Standards (NBS) entwickelter Algorithmus. Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel, der Kombinationen von Substitutions-Chiffre, Transpositions-Chiffre und Exklusiv-Oder-Funktionen (XOR) ermöglicht. Der 64-Bit-Datensatz besteht aus einer effektiven Schlüssellänge von 56 Bits und 8 Parity-Bits, das zugrunde liegende Verschlüsselungsverfahren heißt Lucifer.

3DES

Dreifach-DES: Dies ist eine verbesserte DES-Verschlüsselung, die zwei 64-Bit-Schlüssel verwendet.

BLOWFISH

Der BLOWFISH-Algorithmus benutzt eine variable Schlüssellänge von 32 bis 448 Bit und zeichnet sich durch einen schnellen und sehr sicheren Algorithmus aus. Er hat wesentliche Vorteile gegenüber anderen symmetrischen Verfahren wie DES und 3DES.

AES

Advanced Encryption Standard: Der AES-Algorithmuss besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit und bietet ein sehr hohes Maß an Sicherheit.

Default-Wert:

DES

CA-Signaturalgorithmus

Wählen Sie hier den Signaturalgorithmus aus, den die Zertifizierungsstelle (CA) zur Signatur (Unterschrift) der Zertifikate verwenden soll. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen, da der Client die Integrität des Zertifikates anhand der Signatur prüft. Es stehen zwei weit verbreitete kryptographische Hash-Funktionen zur Auswahl.

SNMP-ID:

2.39.1.14.6

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-Client** > **CAs**

Mögliche Werte:

MD5

Message Digest Algorithm 5: Der MD5-Algorithmus erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der

Message Digest gebildet, der an die unverschlüsselte Nachricht angehängt wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

SHA1

Secure Hash Algorithm 1: Der SHA1-Algorithmus erzeugt einen 160-Bit-Hashwert. Dieser dient zur Berechnung eines eindeutigen Prüfwerts für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden.

SHA256

Wie SHA1, nur mit einem 256 Bit langen Hashwert.

SHA384

Wie SHA1, nur mit einem 384 Bit langen Hashwert.

SHA512

Wie SHA1, nur mit einem 512 Bit langen Hashwert.

Default-Wert:

MD5

CA-Fingerprintalgorithmus

Wählen Sie hier einen Fingerprint-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Berechnung des Fingerprints (Fingerabdruck) der Signatur (Unterschrift) verwenden soll. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen.

Der Fingerprint ist eine Hash-Wert von Daten (Schlüssel, Zertifikat, etc.), d. h. eine kurze Zahlenfolge, die zur Überprüfung der Integrität der Daten benutzt werden kann.

SNMP-ID:

2.39.1.14.8

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-Client** > **CAs**

Mögliche Werte:

aus
MD5

Message Digest Algorithm 5: Der MD5-Algorithmus erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest gebildet, der an die unverschlüsselte Nachricht angehängt wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

SHA1

Secure Hash Algorithm 1: Der SHA1-Algorithmus erzeugt einen 160-Bit-Hashwert. Dieser dient zur Berechnung eines eindeutigen Prüfwerts für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden.

SHA256

Wie SHA1, nur mit einem 256 Bit langen Hashwert.

SHA384

Wie SHA1, nur mit einem 384 Bit langen Hashwert.

SHA512

Wie SHA1, nur mit einem 512 Bit langen Hashwert.

Default-Wert:

MD5

Verschluesselungsalgorithmus

Wählen Sie hier den Verschlüsselungs-Algorithmus (Encryption-Algorithmus) zur Verschlüsselung innerhalb des SCEP-Protokolls (Simple Certificate Enrollment Protocol) aus. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen. Es stehen mehrere Verfahren zur Auswahl.

Verwenden Sie nach Möglichkeit eines der letzteren Verfahren (3DES, BLOWFISH, AES), wenn die Zertifizierungsstelle (CA) und alle Clients es unterstützen. Als Standard ist hier DES-Verschlüsselung voreingestellt, um die Interoperabilität zu wahren.

SNMP-ID:

2.39.2.3

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

DES

Data Encryption Standard: Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel. Dies ist die SCEP-Standard-Verschlüsselung. DES ist ein vom amerikanischen National Bureau of Standards (NBS) entwickelter Algorithmus. Der DES-Algorithmus benutzt einen 64-Bit-Schlüssel, der Kombinationen von Substitutions-Chiffre, Transpositions-Chiffre und Exklusiv-Oder-Funktionen (XOR) ermöglicht. Der 64-Bit-Datensatz besteht aus einer effektiven Schlüssellänge von 56 Bits und 8 Parity-Bits, das zugrunde liegende Verschlüsselungsverfahren heißt Lucifer.

3DES

Dreifach-DES: Dies ist eine verbesserte DES-Verschlüsselung, die zwei 64-Bit-Schlüssel verwendet.

BLOWFISH

Der BLOWFISH-Algorithmus benutzt eine variable Schlüssellänge von 32 bis 448 Bit und zeichnet sich durch einen schnellen und sehr sicheren Algorithmus aus. Er hat wesentliche Vorteile gegenüber anderen symmetrischen Verfahren wie DES und 3DES.

AES

Advanced Encryption Standard: Der AES-Algorithmuss besitzt eine variable Blockgröße von 128, 192 oder 256 Bit und eine variable Schlüssellänge von 128, 192 oder 256 Bit und bietet ein sehr hohes Maß an Sicherheit.

Default-Wert:

DES

Signatur-Algorithmus

Wählen Sie hier den Signaturalgorithmus aus, den die Zertifizierungsstelle (CA) zur Signatur (Unterschrift) der Zertifikate verwenden soll. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen, da der Client die Integrität des Zertifikates anhand der Signatur prüft. Es stehen zwei weit verbreitete kryptographische Hash-Funktionen zur Auswahl.

SNMP-ID:

2.39.2.6

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

MD5

Message Digest Algorithm 5: Der MD5-Algorithmus erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest gebildet, der an die unverschlüsselte Nachricht angehängt wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

SHA1

Secure Hash Algorithm 1: Der SHA1-Algorithmus erzeugt einen 160-Bit-Hashwert. Dieser dient zur Berechnung eines eindeutigen Prüfwerts für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden.

SHA256

Wie SHA1, nur mit einem 256 Bit langen Hashwert.

SHA384

Wie SHA1, nur mit einem 384 Bit langen Hashwert.

SHA512

Wie SHA1, nur mit einem 512 Bit langen Hashwert.

Default-Wert:

MD5

Fingerabdruck-Algorithmus

Wählen Sie hier einen Fingerprint-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Berechnung des Fingerprints (Fingerabdruck) der Signatur (Unterschrift) verwenden soll. Sowohl die Zertifizierungsstelle (CA), als auch der Zertifikat-Nehmer (Client) müssen den Algorithmus unterstützen.

Der Fingerprint ist eine Hash-Wert von Daten (Schlüssel, Zertifikat, etc.), d. h. eine kurze Zahlenfolge, die zur Überprüfung der Integrität der Daten benutzt werden kann.

SNMP-ID:

2.39.2.7

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA**

Mögliche Werte:

MD5

Message Digest Algorithm 5: Der MD5-Algorithmus erzeugt einen 128-Bit-Hashwert. MD5 wurde 1991 von Ronald L. Rivest entwickelt. Aus dem Ergebnis können keine Rückschlüsse auf den Schlüssel erfolgen. Dem Verfahren nach wird aus einer beliebig langen Nachricht eine 128 Bit lange Information, der Message Digest gebildet, der an die unverschlüsselte Nachricht angehängt wird. Der Empfänger vergleicht den Message Digest mit dem von ihm aus der Information ermittelten Wert.

SHA1

Secure Hash Algorithm 1: Der SHA1-Algorithmus erzeugt einen 160-Bit-Hashwert. Dieser dient zur Berechnung eines eindeutigen Prüfwerts für beliebige Daten. Meist handelt es sich dabei um Nachrichten. Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten mit dem gleichen SHA-Wert zu finden.

SHA256

Wie SHA1, nur mit einem 256 Bit langen Hashwert.

SHA384

Wie SHA1, nur mit einem 384 Bit langen Hashwert.

SHA512

Wie SHA1, nur mit einem 512 Bit langen Hashwert.

Default-Wert:

MD5

15.3 Absende-Adresse bei L2TP-Verbindungen

Ab LCOS-Version 9.10 ist bei L2TP-Verbindungen die Angabe einer Absende-Adresse möglich.

Wenn für die Absende-Adresse eine Loopback-Adresse eingetragen ist und das Routing-Tag den Wert "0" besitzt, verwendet das Gerät das Routing-Tag der Loopback-Adresse.

15.3.1 Ergänzungen im Setup-Menü

Absende-Adresse

Hier können Sie optional eine Absende-Adresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet.

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, verwendet das Gerät die zugehörige IP-Adresse.

Sofern die hier eingestellte Absende-Adresse eine Loopback-Adresse ist, wird diese auch auf maskiert arbeitenden Gegenstellen unmaskiert verwendet.

SNMP-ID:

2.2.35.10

Pfad Telnet:

Setup > **WAN** > **L2TP-Endpunkte**

Mögliche Werte:

Gültiger Eintrag aus der Liste möglicher Adressen.

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.

"INT" für die Adresse des ersten Intranets

"DMZ" für die Adresse der ersten DMZ

LB0 bis LBF für die 16 Loopback-Adressen

Beliebige gültige IP-Adresse

leer

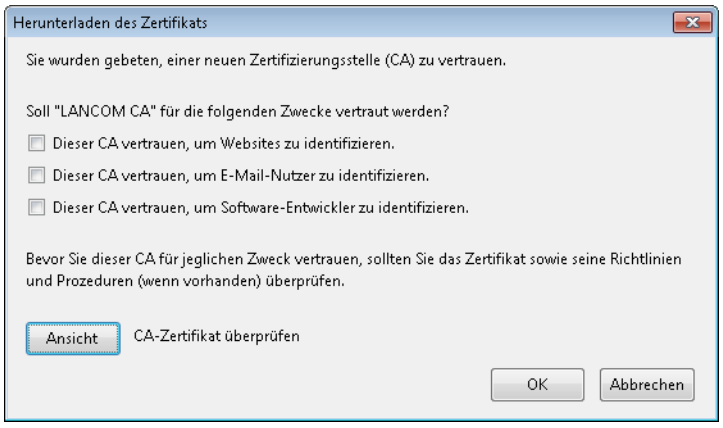
Default-Wert:

15.4 Downloadlink für den öffentlichen Teil des CA-Zertifikats

Ab LCOS-Version 9.10 steht der öffentliche Teil des CA-Zertifikats über einen Download-Link zur Verfügung.

15.4.1 Downloadlink für den öffentlichen Teil des CA-Zertifikats

Sie können den öffentlichen Teil des CA-Zertifikats ohne Anmeldung über den Link `http://<URL>/getcacert/cacert.crt` herunterladen. Die Übertragung erfolgt mit dem Mime-Typ `application/x/x509-ca-cert`, so dass die verwendete Software je nach Fähigkeit die sofortige Installation des Zertifikats anbietet.



Der Download ist nur möglich bei aktivierter CA. Bei deaktivierter CA erscheint eine Fehlermeldung.

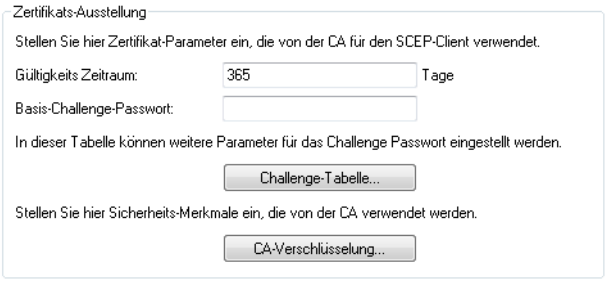
Bei aktivierter CA ist im WEBconfig der Zertifikats-Download auch über **Extras** > **Aktuelles CA Zertifikat herunterladen** möglich.

15.5 Konfigurierbare Einmalpasswörter (OTP) für SCEP-CA

Ab LCOS-Version 9.10 ist die Erstellung von One-Time-Passworten (OTP) auch für SCEP-CA möglich.

15.5.1 Challenge-Passwörter konfigurieren

Im LANconfig konfigurieren Sie unter **Zertifikate** > **Zertifikats-Behandlung** im Abschnitt **Zertifikats-Ausstellung** die Zertifikats-Parameter.



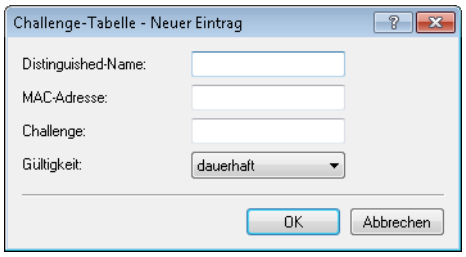
Gültigkeitszeitraum

Bestimmen Sie hier die Gültigkeitsdauer des Zertifikats in Tagen.

Basis-Challenge-Passwort

Hier kann ein weiteres „Passwort" eingetragen werden, das an die CA übertragen wird. Dieses kann standardmäßig zur Authentifizierung von Rücknahme-Anträgen benutzt werden. Auf CAs mit Microsoft-SCEP (mscep) können (falls dort aktiviert) die von der CA vergebenen Einmalpasswörter zur Antragsauthentifizierung eingetragen werden.

Die **Challenge-Tabelle** verwaltet die eigenen Passwörter der Zertifikat-Nehmer (Client).



Distinguished-Name

Hier muss der „Distinguished Name" eingegeben werden. Hierüber erfolgt einerseits die Zuordnung von CAs zu Systemzertifikaten (und umgekehrt). Andererseits spielt dieser Parameter auch eine Rolle bei der Bewertung ob erhaltene bzw. vorhandene Zertifikate der Konfiguration entsprechen. Es handelt sich um eine durch Komma oder Schrägstrich separierte Auflistung, in der Name, Abteilung, Bundesland und Land des Gateways angegeben werden können. Die folgenden Beispiele zeigen, wie der Eintrag aussehen kann: `CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=LANCOM CA/O=LANCOM SYSTEMS/C=DE`

MAC-Adresse

Tragen Sie hier die MAC-Adresse des Clients ein, dessen Passwort in der Challange-Passwort-Tabelle verwaltet wird.

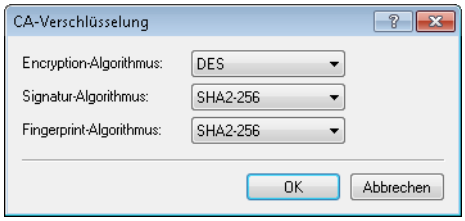
Challenge

Geben Sie hier die Challenge (Passwort) für den Client an.

Gültigkeit

Geben Sie hier die Gültigkeit des Passwortes an. Wenn Sie „einmalig" auswählen, handelt es sich bei diesem Passwort um ein One-Time-Passwort (OTP), das nur für die einmalige Verwendung z. B. bei einer Authentifizierung gültig ist.

Unter **CA-Verschlüsselung** konfigurieren Sie die Sicherheitsmerkmale der CA-Verschlüsselung.



Encryption-Algorithmus

Wählen Sie hier den Verschlüsselungs-Algorithmus zur Verschlüsselung innerhalb des SCEP-Protokolls aus. Sowohl die Zertifizierungsstelle (CA), als der Zertifikatnehmer (Client) müssen den Algorithmus unterstützen. Die folgenden Verfahren stehen zur Auswahl:

- DES
- 3DES
- BLOWFISH
- AES128
- DES192
- DES256

Signatur-Algorithmus

Wählen Sie hier den Signatur-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Signatur (Unterschrift) der Zertifikate verwenden soll. Sowohl die CA als auch der Zertifikatnehmer (Client) müssen das Verfahren unterstützen, da der Client die Integrität des Zertifikates anhand der Signatur prüft. Es stehen die folgenden kryptographischen Hash-Funktionen zur Auswahl:

- MD5
- SHA1
- SHA2-256
- SHA2-384
- SHA2-512

Fingerprint-Algorithmus

Wählen Sie hier einen Fingerprint-Algorithmus aus, den die Zertifizierungsstelle (CA) zur Berechnung des Fingerprints (Fingerabdruck) der Signatur (Unterschrift) verwenden soll. Sowohl die CA als auch der Zertifikatnehmer (Client) müssen das Verfahren unterstützen.

Der Fingerprint ist ein Hash-Wert von Daten (Schlüssel, Zertifikat, etc.), d. h. eine kurze Zahlenfolge, die zur Überprüfung der Integrität der Daten benutzt werden kann. Es stehen die folgenden kryptographischen Hash-Funktionen zur Auswahl:

- MD5
- SHA1
- SHA2-256

- SHA2-384
- SHA2-512

15.5.2 Ergänzungen im Setup-Menü

Challenge

Die Gültigkeit des Passwortes ist mit „permanent" fest vorgegeben.

Geben Sie hier die Gültigkeit des Passwortes an. Wenn Sie „einmalig" auswählen, handelt es sich bei diesem Passwort um ein One-Time-Passwort (OTP), das nur für die einmalige Verwendung bei einer Authentifizierung gültig ist.

SNMP-ID:

2.39.2.5.3.5

Pfad Telnet:

Setup > **Zertifikate** > **SCEP-CA** > **Client-Zertifikate** > **Challenge-Passwoerter**

Mögliche Werte:

permanent

Default-Wert:

permanent

Mögliche Werte:

einmalig
permanent

Default-Wert:

permanent

16 Routing und WAN-Verbindungen

16.1 Client-Binding

Ab LCOS-Version 9.10 ist das Load-Balancing um das Feature Client-Binding erweitert.

16.1.1 Client-Binding

Der Einsatz von Load-Balancing führt bei Servern zu Problemen, die zur Identifizierung eines angemeldeten Benutzers dessen IP-Adresse verwenden. Wählt der Load-Balancer z. B. beim Aufruf einer neuen Webseite eine andere Internetverbindung als die, über die sich der Benutzer am Server angemeldet hat, wertet der Server das als Verbindungsversuch eines nicht angemeldeten Benutzers. Der Benutzer bekommt bestenfalls erneut einen Anmeldedialog zu sehen, nicht aber die gewünschte Webseite.

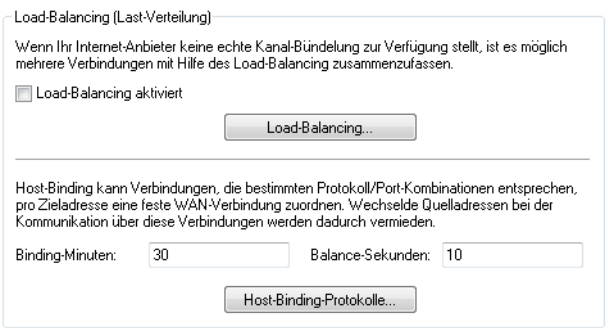
Eine Möglichkeit zur Abhilfe ist, in den Firewall-Regeln den Datenverkehr mit diesem Server auf eine bestimmte Internetverbindung festzulegen (Policy Based Routing). Damit ist jedoch der gesamte Datenverkehr zu diesem Server auf die Bandbreite dieser einen Verbindung beschränkt. Außerdem lassen sich so keine Backup-Verbindung aufbauen, falls die erste Verbindung gestört ist.

Das Client-Binding überwacht im Gegensatz dazu nicht die jeweiligen einzelnen TCP/IP-Sessions, sondern orientiert sich am Client, mit dem bei der ersten Session eine Internetverbindung zustande kommt. Es leitet alle nachfolgenden Sessions ebenfalls über diese Internetverbindung, was im Prinzip dem zuvor angesprochenen Policy Based Routing entspricht. Das erfolgt protokollabhängig, d. h., es überträgt nur Daten des selben Protokolltyps (z. B. HTTPS) über diese Internetverbindung. Lädt der Client sich zusätzlich Daten über eine HTTP-Verbindung, erfolgt das wahrscheinlich über eine andere Verbindung.

Um zu vermeiden, dass nun auch Daten über diese Internetverbindung fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

16.1.2 Load-Balancing mit Client-Binding

In LANconfig konfigurieren Sie das Client-Binding unter **IP-Router** > **Routing** im Abschnitt **Load-Balancing (Lastverteilung)**.



Binding-Minuten

Definieren Sie hier die Zeit in Minuten, für die die Binding-Einträge für einen Client gültig sein sollen.

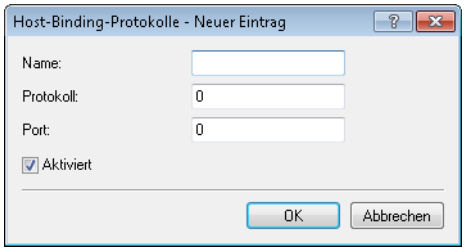
Balance-Sekunden

Um zu vermeiden, dass Daten über die Internetverbindung der Haupt-Session fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

Definieren Sie hier die Zeit in Sekunden, innerhalb der der Load-Balancer neue Sessions nach dem Start der Haupt-Session frei auf andere Internetverbindungen verteilt.

Das Client-Binding erfolgt protokollorientiert. Die entsprechenden Protokolle bestimmen Sie unter **Client-Binding-Protokolle**. Die Tabelle enthält bereits die Standard-Einträge

- HTTPS
- HTTP
- ANY



Name

Enthält eine aussagekräftige Bezeichnung dieses Eintrags.

Protokoll

Enthält die IP-Protokollnummer.

Mehr Informationen über IP-Protokollnummern finden Sie in der *Online-Datenbank* der IANA

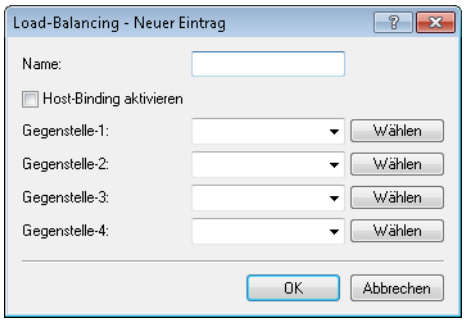
Port

Enthält den Port des IP-Protokolls.

Aktiviert

Aktiviert bzw. deaktiviert diesen Eintrag.

Das Client-Binding lässt sich unter **Load-Balancing** für den jeweiligen Eintrag aktivieren bzw. deaktivieren.



16.1.3 Ergänzungen im Menüsystem

Ergänzungen im Setup-Menü

Client-Binding

In diesem Menü konfigurieren Sie das Client-Binding.

Der Einsatz von Load-Balancing führt bei Servern zu Problemen, die zur Identifizierung eines angemeldeten Benutzers dessen IP-Adresse verwenden. Wählt der Load-Balancer z. B. beim Aufruf einer neuen Webseite eine andere Internetverbindung als die, über die sich der Benutzer am Server angemeldet hat, wertet der Server das als Verbindungsversuch eines nicht angemeldeten Benutzers. Der Benutzer bekommt bestenfalls erneut einen Anmeldedialog zu sehen, nicht aber die gewünschte Webseite.

Eine Möglichkeit zur Abhilfe ist, in den Firewall-Regeln den Datenverkehr mit diesem Server auf eine bestimmte Internetverbindung festzulegen (Policy Based Routing). Damit ist jedoch der gesamte Datenverkehr zu diesem Server auf die Bandbreite dieser einen Verbindung beschränkt. Außerdem lassen sich so keine Backup-Verbindung aufbauen, falls die erste Verbindung gestört ist.

Das Client-Binding überwacht im Gegensatz dazu nicht die jeweiligen einzelnen TCP/IP-Sessions, sondern orientiert sich am Client, mit dem bei der ersten Session eine Internetverbindung zustande kommt. Es leitet alle nachfolgenden Sessions ebenfalls über diese Internetverbindung, was im Prinzip dem zuvor angesprochenen Policy Based Routing entspricht. Das erfolgt protokollabhängig, d. h., es überträgt nur Daten des selben Protokolltyps (z. B. HTTPS) über diese Internetverbindung. Lädt der Client sich zusätzlich Daten über eine HTTP-Verbindung, erfolgt das wahrscheinlich über eine andere Verbindung.

Um zu vermeiden, dass nun auch Daten über diese Internetverbindung fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

SNMP-ID:

2.8.20.3

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer**

Protokolle

In dieser Tabelle definieren Sie die vom Client-Binding überwachten Protokolle sowie deren Ports.

Die Tabelle enthält bereits die Standard-Einträge

- HTTPS
- HTTP
- ANY

SNMP-ID:

2.8.20.3.1

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding**

Name

Vergeben Sie einen aussagekräftigen Namen für diesen Eintrag.

SNMP-ID:

2.8.20.3.1.1

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protokolle**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]`

Default-Wert:

leer

Protokoll

Wählen Sie die IP-Protokollnummer aus.

Mehr Informationen über IP-Protokollnummern finden Sie in der *Online-Datenbank* der IANA

SNMP-ID:

2.8.20.3.1.2

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protokolle**

Mögliche Werte:

max. 3 Zeichen von `[0-255]`

Besondere Werte:

0

alle Protokolle

Default-Wert:

0

Port

Wählen Sie den Port aus.

SNMP-ID:

2.8.20.3.1.3

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protokolle**

Mögliche Werte:

max. 5 Zeichen von `[0-65535]`

Besondere Werte:

0

alle Ports

Default-Wert:

0

Aktiv

Aktivieren bzw. deaktivieren Sie das Client-Binding für diesen Eintrag.

SNMP-ID:

2.8.20.3.1.4

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protokolle**

Mögliche Werte:

Ja

Aktiviert den Eintrag

Nein

Deaktiviert den Eintrag

Default-Wert:

Ja

Bindung-Minuten

Definieren Sie die Zeit in Minuten, für die die Binding-Einträge für einen Client gültig sein sollen.

SNMP-ID:

2.8.20.3.2

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding**

Mögliche Werte:

max. 3 Zeichen von `[0-999]`

Besondere Werte:

0

Default-Wert:

30

Balance-Sekunden

Um zu vermeiden, dass Daten über diese Internetverbindung der Haupt-Session fließen, die problemlos über parallele Verbindung zu übertragen wären, sorgt ein entsprechender Timer dafür, dass der Load-Balancer für eine definierte Dauer zusätzliche Sessions auf die zur Verfügung stehenden Internetverbindungen verteilt. Erst nach Ablauf des Timers zwingt das Client-Binding eine neue Session wieder auf die ursprüngliche Internetverbindung und startet den Timer neu. Der Server erkennt somit weiterhin den Anmeldestatus des Benutzers anhand seiner aktuellen IP-Adresse.

Definieren Sie hier die Zeit in Sekunden, innerhalb der der Load-Balancer neue Sessions nach dem Start der Haupt-Session frei auf andere Internetverbindungen verteilt.

SNMP-ID:

2.8.20.3.3

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding**

Mögliche Werte:

max. 3 Zeichen von `[0-999]`

Besondere Werte:

0

Der Timer ist deaktiviert. Alle Sessions sind fest an die bestehende Internetverbindung gebunden.

Default-Wert:

10

Client-Binding

Aktivieren bzw. deaktivieren Sie hier das Client-Binding je Load-Balancer.

SNMP-ID:

2.8.20.2.10

Pfad Telnet:

Setup > **IP-Router** > **Load-Balancer** > **Buendel-Gegenstellen**

Mögliche Werte:

Ja

Das Client-Binding ist aktiv.

Nein

Das Client-Binding ist nicht aktiv.

Default-Wert:

Nein

Ergänzungen im Status-Menü

Client-Binding

Diese Tabelle zeigt die Informationen über aktuelle Client-Bindings.

SNMP-ID:

1.10.32.3

Pfad Telnet:

Status > **IP-Router** > **Load-Balancer**

Source-IP

Dieser Eintrag zeigt die Quell-IP-Adresse des Clients.

SNMP-ID:

1.10.32.3.1

Pfad Telnet:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Buendel-GgSt

Dieser Eintrag zeigt den Namen der gewählten Internetverbindung an.

SNMP-ID:

1.10.32.3.2

Pfad Telnet:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Timeout

Dieser Eintrag zeigt die verbleibende Zeit an, bis der Load-Balancer diesen Eintrag löscht.

SNMP-ID:

1.10.32.3.3

Pfad Telnet:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Balance

Dieser Eintrag zeigt an, ob der Timer für die Freigabe von weiteren Internetverbindungen aktiviert ist.

SNMP-ID:

1.10.32.3.4

Pfad Telnet:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

16.2 Schnittstellenbindung "Beliebig" bei IPv4 entfernt

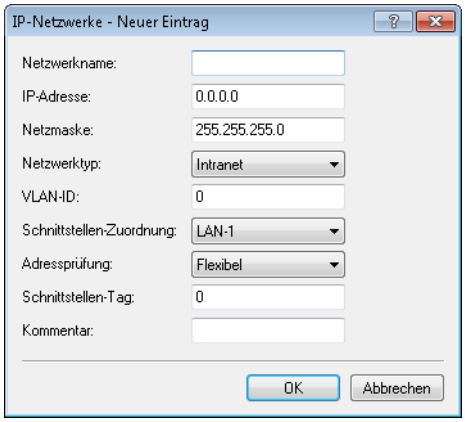
Ab LCOS-Version 9.10 ist bei der Zuordnung von Schnittstellen zu IPv4-Netzwerken die Auswahl "Beliebig" nicht mehr möglich.

Die neue Standardeinstellung ist "LAN-1" bzw. "BRG-1".

16.2.1 Definition von Netzwerken und Zuordnung von Interfaces

Bei der Definition eines Netzwerks wird zunächst festgelegt, welcher IP-Adress-Kreis auf einem bestimmten lokalen Interface des Routers gültig sein soll. „Lokale Interfaces" sind dabei logische Interfaces, die einem physikalischen Ethernet- (LAN) oder Wireless-Port (WLAN) zugeordnet sind. Um die oben aufgeführten Szenarien zu realisieren, können durchaus mehrere Netzwerke auf einem Interface aktiv sein – umgekehrt kann ein Netzwerk auch auf mehreren Interfaces aktiv sein (über Bridge-Gruppen oder mit der Schnittstellenzuordnung 'beliebig').

Die Netzwerke werden in einer Tabelle unter **IPv4** > **Allgemein** > **IP-Netzwerke** definiert. Neben der Definition des Adresskreises und der Interfacezuordnung wird darin auch ein eindeutiger Name für die Netzwerke festgelegt. Dieser Netzwerkname erlaubt es, die Netze in anderen Modulen (DHCP-Server, RIP, NetBIOS etc.) zu identifizieren und diese Dienste nur in bestimmten Netzen anbieten zu können.



16.2.2 Ergänzungen im Setup-Menü

Interface

Wählen Sie hier die Schnittstelle aus, die dem Netzwerk zugeordnet sein soll.

Die in der Liste angegebenen Werte für 'x' variieren je Modell.

SNMP-ID:

2.7.30.5

Pfad Telnet:

Setup > **TCP-IP** > **Netzliste**

Mögliche Werte:

LAN-1
LAN-x
WLAN-x-x
P2P-x-x
BRG-x

Default-Wert:

LAN-1

16.3 Generic Routing Encapsulation (GRE)

Ab LCOS-Version 9.10 ist die Übertragung von Datenpaketen beliebiger Übertragungsprotokolle per GRE-Tunnel innerhalb von IP-Paketen möglich.

Um Probleme bei GRE-Tunneln aufzuspüren, besitzt der Trace-Befehl einen weiteren Parameter:

Tabelle 11: Übersicht aller durchführbaren Traces

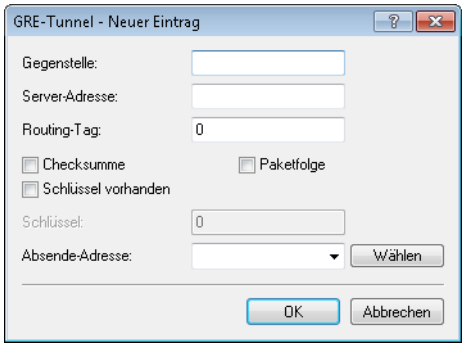
Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
GRE	Meldungen zu GRE-Tunneln

16.3.1 Grundlagen zum Generic Routing Encapsulation Protokoll (GRE)

Das GRE-Protokoll tunnelt beliebige Layer-3-Datenpakete (u. a. IP, IPsec, ICMP etc.) über eine Point-to-Point-Netzwerkverbindung, indem es diese Daten mit einem IP-Daten-Gerüst umgibt. Das ist unter anderem dann hilfreich, wenn beide Kommunikationspartner ein bestimmtes Übertragungsprotokoll verwenden (z. B. IPsec), das auf dem Übertragungsweg nicht zur Verfügung steht. Da GRE selbst keine Verschlüsselung der getunnelten Daten durchführt, müssen beide Kommunikationspartner für die Absicherung dieser Daten sorgen.

Konfiguration eines GRE-Tunnels

Mit LANconfig erfolgt die Konfiguration eines GRE-Tunnels unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** nach einem Klick auf **GRE-Tunnel**.



Gegenstelle

Name der Gegenstelle dieses GRE-Tunnels. Verwenden Sie diesen Namen z. B. in der Routing-Tabelle, um Daten durch diesen GRE-Tunnel zu versenden.

Server-Adresse

Adresse des GRE-Tunnel-Endpunktes (gültige IPv4- bzw. IPv6-Adresse oder FQDN).

Routing-Tag

Routing-Tag für die Verbindung zum GRE-Tunnel-Endpunkt. Anhand des Routing-Tags ordnet das Gerät Datenpakete diesem GRE-Tunnel zu.

Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

Schlüssel vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses GRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

Schlüssel

Der Schlüssel, der die Datenflusskontrolle in diesem GRE-Tunnel sicherstellt. Anhand dieses Schlüssels ordnen zwei über mehrere GRE-Tunnel verbundene Geräte die Datenpakete dem entsprechenden GRE-Tunnel zu.

Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem GRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

Absende-Adresse

Hier können Sie optional eine Absendeadresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absendeadresse verwendet. Mögliche Werte sind:

- Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.
- "INT" für die Adresse des ersten Intranets
- "DMZ" für die Adresse der ersten DMZ
- LB0 bis LBF für die 16 Loopback-Adressen
- Beliebige gültige IP-Adresse

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, verwendet das Gerät die zugehörige IP-Adresse.

Um IPv6 als GRE-Tunnel Transport Protokoll zu verwenden, erstellen Sie unter **IPv6** > **WAN-Schnittstellen** einen neuen Eintrag, z. B. "IPV6GRE". Diese Schnittstelle vergeben Sie anschließend bei der Konfiguration des entsprechenden GRE-Tunnels als **Gegenstelle**.

Falls die Angabe einer IP-Adresse für die Tunnel-Schnittstelle notwendig ist, gehen Sie wie folgt vor:

IPv4-Adresse

Erstellen Sie unter **Kommunikation** > **Protokolle** > **IP-Parameter** einen neuen Eintrag und geben Sie für den Gegenstellennamen den Namen der GRE-Tunnel-Gegenstelle an. Vergeben Sie anschließend unter **IP-Adresse** und **Netzmaske** die notwendigen Werte.

IPv6

Erstellen Sie unter **IPv6** > **Allgemein** > **IPv6-Adressen** einen neuen Eintrag und geben Sie für den Netzwerknamen den Namen der GRE-Tunnel-Gegenstelle an. Vergeben Sie anschließend unter **Adresse/Präfixlänge** die notwendigen Werte.

16.3.2 Ergänzungen im Setup-Menü

GRE-Tunnel

Das GRE-Protokoll tunnelt beliebige Layer-3-Datenpakete (u. a. IP, IPsec, ICMP etc.) über eine Point-to-Point-Netzwerkverbindung, indem es diese Daten mit einem IP-Daten-Gerüst umgibt. Konfigurieren Sie hier die jeweiligen GRE-Tunnel.

SNMP-ID:

2.2.51

Pfad Telnet:

Setup > **WAN**

Gegenstelle

Name der Gegenstelle dieses GRE-Tunnels. Verwenden Sie diesen Namen z. B. in der Routing-Tabelle, um Daten durch diesen GRE-Tunnel zu versenden.

SNMP-ID:

2.2.51.1

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

IP-Adresse

Adresse des GRE-Tunnel-Endpunktes (gültige IPv4- bzw. IPv6-Adresse oder FQDN).

SNMP-ID:

2.2.51.3

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Routing-Tag

Routing-Tag für die Verbindung zum GRE-Tunnel-Endpunkt.

SNMP-ID:

2.2.51.4

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Schluessel-vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses GRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem GRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

SNMP-ID:

2.2.51.5

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Schluessel

Der Schlüssel, der die Datenflusskontrolle in diesem GRE-Tunnel sicherstellt.

SNMP-ID:

2.2.51.6

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

0 … 4294967295

Default-Wert:

0

Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

SNMP-ID:

2.2.51.7

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem GRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

SNMP-ID:

2.2.51.8

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Absende-Adresse

Hier können Sie optional eine Absende-Adresse konfigurieren, die das Gerät statt der ansonsten automatisch für die Zieladresse gewählten Absende-Adresse verwendet.

Wenn in der Liste der IP-Netzwerke oder in der Liste der Loopback-Adressen ein Eintrag mit dem Namen 'DMZ' vorhanden ist, verwendet das gerät die zugehörige IP-Adresse.

SNMP-ID:

2.2.51.9

Pfad Telnet:

Setup > **WAN** > **GRE-Tunnel**

Mögliche Werte:

Gültiger Eintrag aus der Liste möglicher Adressen.

Name der IP-Netzwerke, deren Adresse eingesetzt werden soll.

"INT" für die Adresse des ersten Intranets
"DMZ" für die Adresse der ersten DMZ
LB0 bis LBF für die 16 Loopback-Adressen
Beliebige gültige IP-Adresse

leer

Default-Wert:

16.3.3 Ergänzungen im Status-Menü

GRE-Tunnel

Diese Tabelle zeigt Statuswerte der eingerichteten GRE-Tunnel.

SNMP-ID:

1.86

Pfad Telnet:

Status

Gegenstelle

Diese Spalte enthält die Namen der jeweiligen GRE-Tunnel-Gegenstellen.

SNMP-ID:

1.86.1

Pfad Telnet:

Status > **GRE-Tunnel**

Server-Adresse

Diese Spalte enthält die Adressen der GRE-Tunnel-Endpunkte (gültige IP-Adresse oder FQDN).

SNMP-ID:

1.86.3

Pfad Telnet:

Status > **GRE-Tunnel**

Routing-Tag

Diese Spalte enthält die Routing-Tags für die Verbindungen zu den jeweiligen GRE-Tunnel-Endpunkten.

SNMP-ID:

1.86.4

Pfad Telnet:

Status > **GRE-Tunnel**

Schlüssel-vorhanden

Diese Spalte zeigt an, ob der GRE-Header des jeweiligen Tunnels einen Schlüssel enthält.

SNMP-ID:

1.86.5

Pfad Telnet:

Status > **GRE-Tunnel**

Schlüssel

Diese Spalte enthält den Schlüssel, wenn einer im GRE-Header des entsprechenden Tunnels vorhanden ist.

SNMP-ID:

1.86.6

Pfad Telnet:

Status > **GRE-Tunnel**

Checksumme

Diese Spalte zeigt an, ob der GRE-Header des entsprechenden Tunnels eine Checksumme enthält.

SNMP-ID:

1.86.7

Pfad Telnet:

Status > **GRE-Tunnel**

Paketfolge

Diese Spalte zeigt an, ob der GRE-Header des entsprechenden Tunnels eine Paketfolgesequenz enthält.

SNMP-ID:

1.86.8

Pfad Telnet:

Status > **GRE-Tunnel**

Absende-Adresse

Diese Spalte enthält die für den entsprechenden GRE-Tunnel angegebene Absende-Adresse.

SNMP-ID:

1.86.9

Pfad Telnet:

Status > **GRE-Tunnel**

16.4 Ethernet-over-GRE-Tunnel (EoGRE)

Ab LCOS-Version 9.10 ist die Übertragung von Ethernet-Paketen per EoGRE-Tunnel innerhalb von IP-Paketen möglich.

Um Probleme bei GRE-Tunneln aufzuspüren, besitzt der Trace-Befehl einen weiteren Parameter:

Tabelle 12: Übersicht aller durchführbaren Traces

Dieser Parameter ...	... ruft beim Trace die folgende Anzeige hervor:
GRE	Meldungen zu GRE-Tunneln

16.4.1 Ethernet-over-GRE (EoGRE)

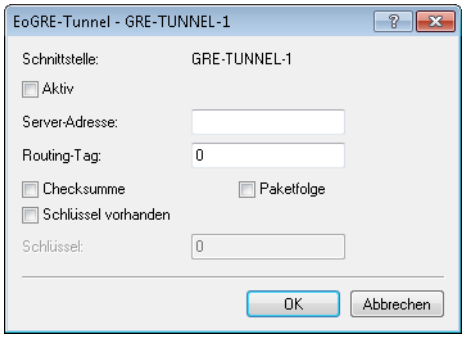
Weitere Informationen zum GRE-Potokoll finden Sie unter *Grundlagen zum Generic Routing Encapsulation Protokoll (GRE)*.

Die aktuelle LCOS-Version stellt mehrere „Ethernet over GRE"-Tunnel (EoGRE) zur Verfügung, um Ethernet-Pakete per GRE zu übertragen. Da sich diese Ethernet-Pakete auf OSI-Layer-2 bewegen, bieten diese EoGRE-Tunnel lediglich eine Bridge-Funktionalität an.

Auf diese Weise lassen sich beispielsweise L2VPN (VPN als einfache Level-2-Brigde) oder eine transparente Ethernet-Bridge über WAN realisieren.

Konfiguration eines EoGRE-Tunnels

Mit LANconfig erfolgt die Konfiguration eines EoGRE-Tunnels unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** nach einem Klick auf **EoGRE-Tunnel** und der Auswahl des entsprechenden Tunnels.



Schnittstelle

Name des gewählten EoGRE-Tunnels.

Aktiv

Aktiviert bzw. deaktiviert den EoGRE-Tunnel. Deaktivierte EoGRE-Tunnel senden bzw. empfangen keinen Daten.

Server-Adresse

Adresse des EoGRE-Tunnel-Endpunktes (gültige IPv4- bzw. IPv6-Adresse oder FQDN).

Routing-Tag

Routing-Tag für die Verbindung zum EoGRE-Tunnel-Endpunkt. Anhand des Routing-Tags ordnet das Gerät Datenpakete diesem EoGRE-Tunnel zu.

Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

Schlüssel vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses EoGRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

Schlüssel

Der Schlüssel, der die Datenflusskontrolle in diesem EoGRE-Tunnel sicherstellt. Anhand dieses Schlüssels ordnen zwei über mehrere EoGRE-Tunnel verbundene Geräte die Datenpakete dem entsprechenden EoGRE-Tunnel zu.

Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem EoGRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

Lokale Schnittstelle mit einem EoGRE-Tunnel verbinden

Um eine lokale Schnittstelle mit einem EoGRE-Tunnel zu verbinden, gehen Sie wie folgt vor:

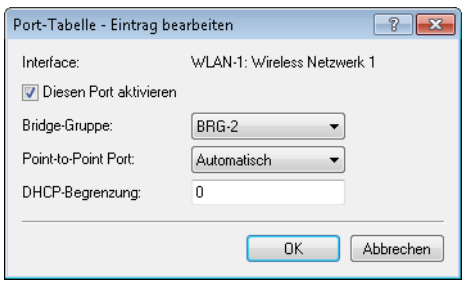
1. Erstellen Sie unter **Kommunikation** > **Gegenstellen** > **GRE-Tunnel** > **EoGRE-Tunnel** einen neuen Eintrag.

Aktivieren Sie den Tunnel und geben Sie unter **Server-Adresse** die Adresse des entfernten Gerätes an, zu dem der EoGRE-Tunnel bestehen soll (IPv4- bzw. IPv6-Adresse oder FQDN).

2. Ergänzen Sie unter **Schnittstellen** > **LAN** > **Port-Tabelle** eine Bridge-Gruppe um den aktivierten EoGRE-Tunnel.

Aktivieren Sie den Port und wählen Sie die gewünschte Bridge-Gruppe aus.

3. Ergänzen Sie ebenfalls unter **Schnittstellen** > **LAN** > **Port-Tabelle** dieselbe Bridge-Gruppe um das lokale Interface, das Sie über den EoGRE-Tunnel verbinden möchten (z. B. WLAN-1).



Aktivieren Sie den Port und wählen Sie aus der Liste dieselbe Bridge-Gruppe aus, in der sich auch der EoGRE-Tunnel befindet.

16.4.2 Ergänzungen im Status-Menü

EoGRE-Tunnel

Diese Tabelle zeigt Ihnen Informationen zu den EoGRE-Tunneln an.

SNMP-ID:

1.87

Pfad Telnet:

Status

16.4.3 Ergänzungen im Setup-Menü

EoGRE-Tunnel

Die aktuelle LCOS-Version stellt mehrere "Ethernet over GRE"-Tunnel (EoGRE) zur Verfügung, um Ethernet-Pakete per GRE zu übertragen. Konfigurieren Sie hier die jeweiligen EoGRE-Tunnel.

SNMP-ID:

2.2.50

Pfad Telnet:

Setup > **WAN**

Schnittstelle

Name des gewählten EoGRE-Tunnels.

SNMP-ID:

2.2.50.1

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Aktiv

Aktiviert bzw. deaktiviert den EoGRE-Tunnel. Deaktivierte EoGRE-Tunnel senden bzw. empfangen keinen Daten.

SNMP-ID:

2.2.50.2

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

IP-Adresse

Adresse des EoGRE-Tunnel-Endpunktes (gültige IPv4- bzw. IPv6-Adresse oder FQDN).

SNMP-ID:

2.2.50.3

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Routing-Tag

Routing-Tag für die Verbindung zum EoGRE-Tunnel-Endpunkt.

SNMP-ID:

2.2.50.4

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

0 … 65535

Default-Wert:

0

Schluessel-vorhanden

Bestimmen Sie hier, ob der GRE-Header einen Schlüssel zur Datenflusskontrolle enthalten soll.

Wenn Sie diese Funktion aktivieren, integriert das Gerät den im Feld **Schlüssel** angegebenen Wert in den GRE-Header dieses EoGRE-Tunnels. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header einen identischen Schlüsselwert enthält.

Bei deaktivierter Funktion enthält der GRE-Header abgehender Datenpakete keinen Schlüssel-Wert. Das Gerät ordnet ankommende Datenpakete nur diesem EoGRE-Tunnel zu, wenn ihr GRE-Header ebenfalls keinen Schlüsselwert enthält.

SNMP-ID:

2.2.50.5

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Schluessel

Der Schlüssel, der die Datenflusskontrolle in diesem EoGRE-Tunnel sicherstellt.

SNMP-ID:

2.2.50.6

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

0 … 4294967295

Default-Wert:

0

Checksumme

Bestimmen Sie hier, ob der GRE-Header eine Checksumme enthalten soll.

Wenn Sie die Checksummenfunktion aktivieren, berechnet das Gerät für die zu übertragenen Daten eine Checksumme und fügt diese dem GRE-Tunnel-Header an. Enthält der GRE-Header der ankommenden Daten eine Checksumme, kontrolliert das Gerät diese mit den übertragenen Daten. Bei einer fehlerhaften oder fehlenden Checksumme verwirft das Gerät die empfangenen Daten.

Bei deaktivierter Checksummenfunktion versendet das Gerät alle Tunnel-Daten ohne Checksumme, und es erwartet Datenpakete ohne Checksumme. Ankommende Datenpakete mit einer Checksumme im GRE-Header verwirft das Gerät.

SNMP-ID:

2.2.50.7

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

Paketfolge

Bestimmen Sie hier, ob der GRE-Header der Datenpakete Informationen zur Reihenfolge der Pakete enthält.

Wenn Sie diese Funktion aktivieren, integriert das Gerät in den GRE-Header der abgehenden Datenpakete einen Zähler, um dem EoGRE-Tunnel-Endpunkt die Reihenfolge der Datenpakete vorzugeben. Das Gerät wertet die Paketfolge der ankommenden Datenpakete aus und verwirft Pakete mit falscher oder fehlender Paketfolge.

SNMP-ID:

2.2.50.8

Pfad Telnet:

Setup > **WAN** > **EoGRE-Tunnel**

Mögliche Werte:

Ja
Nein

Default-Wert:

Nein

16.5 Loopback-Adressen für RIP

Ab LCOS-Version 9.10 ist die Angabe einer Loopback-Adresse bei WAN-RIP möglich.

16.5.1 Ergänzungen im Setup-Menü

Loopback-Adresse

Geben Sie hier eine Loopback-Adresse an. Mögliche Werte sind:

- Name eines ARF-Netzwerks
- konfigurierte Loopback-Adresse
- IPv4-Adresse

SNMP-ID:

2.8.8.4.13

Pfad Telnet:

Setup > **IP-Router** > **RIP** > **WAN-Tabelle**

Mögliche Werte:

Geben Sie eine gültige IPv4-Adresse ein.

Default-Wert:

leer

16.6 PPPoE-Snooping ergänzt

Ab LCOS-Version 9.10 ist PPPoE-Snooping implementiert.

16.6.1 PPPoE-Snooping

Das PPPoE-Snooping ermöglicht Geräten, die PPPoE-Discovery-Pakete (PPPoED) empfangen und weiterleiten, diese Datenpakete zu analysieren und mit zusätzlichen Informationen zu versehen. Diese Informationen ermöglichen es einem PPPoE Access Concentrator (AC), die PPPoED-Datenpakete entsprechend zu verarbeiten. Diese Rolle wird als „PPPoE-Intermediate-Agent" bezeichnet.

PPPoE-Snooping im LCOS verarbeitet die folgenden PPPoED-Pakete:

- PADI (PPPoE Active Discovery Indication)
- PADR (PPPoE Active Discovery Request)
- PADT (PPPoE Active Discovery Terminate)

Der für das PPPoE-Snooping zuständige PPPoE Intermediate Agent erweitert das PPPoED-Paket um Hersteller spezifische Attribute (Circuit-ID und Remote-ID) bzw. ersetzt diese IDs durch eigene Werte, falls sie bereits im empfangenen Datenpaket enthalten sind.

- Remote-ID: kennzeichnet eindeutig den Client, der einen PPPoE-Request stellt.
- Circuit-ID: kennzeichnet eindeutig die Schnittstelle, über die ein Client einen PPPoE-Request stellt.

Die Konfiguration von PPPoE-Snooping erfolgt pro LAN/WLAN-Schnittstelle.

16.6.2 Ergänzungen im Setup-Menü

PPPoE-Snooping

Hier konfigurieren Sie das PPPoE-Snooping je Schnittstelle.

SNMP-ID:

2.20.43

Pfad Telnet:

Setup > **LAN-Bridge**

Port

Zeigt das physikalische oder logische Interface an, für das die PPPoE-Snooping-Konfiguration gültig ist.

SNMP-ID:

2.20.43.1

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

LAN-x
Alle physikalischen LAN-Schnittstellen

WLAN-x
Alle physikalischen WLAN-Schnittstellen

WLAN-x-x
Alle logischen WLAN-Schnittstellen

P2P-x-x
Alle logischen P2P-Schnittstellen

WLC-TUNNEL-x
Alle virtuellen WLC-Tunnel

GRE-TUNNEL-x
Alle virtuellen GRE-Tunnel

Agent-Info-hinzufuegen

Bestimmen Sie hier, ob der PPPoE-Intermediate-Agent den ankommenden PPPoE-Paketen einen Hersteller spezifischen PPPoE-Tag mit Vendor-ID „3561" hinzufügen soll, bevor er die Anfrage an einen PPPoE-Server weiterleitet.

Mit dieser Option übermittelt der PPPoE-Intermediate-Agent dem PPPoE-Server zusätzliche Informationen über die Schnittstelle, über die der Client die Anfrage gestellt hat.

Der PPPoE-Tag setzt sich aus den Werten für **Remote-Id** und **Circuit-Id** zusammen.

Sollten diese beiden Felder leer sein, fügt der PPPoE-Intermediate-Agent auch keinen PPPoE-Tag in die Datenpakete ein.

SNMP-ID:

2.20.43.2

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

Ja
Fügt den PPPoE-Paketen die „Relay Agent Info" an.

Nein
Diese Einstellung deaktiviert das PPPoE-Snooping für diese Schnittstelle.

Default-Wert:

Nein

Remote-Id

Die Remote-ID ist eine Unteroption der PPPoE-Intermediate-Agent-Option und kennzeichnet eindeutig den Client, der einen PPPoE-Request stellt.

Sie können die folgenden Variablen verwenden:

- %%: fügt ein Prozent-Zeichen ein.
- %c: fügt die MAC-Adresse der Schnittstelle ein, auf der der PPPoE-Intermediate-Agent den PPPoE-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- %i: fügt den Namen der Schnittstelle ein, auf der der PPPoE-Intermediate-Agent den PPPoE-Request erhalten hat.
- %n: fügt den Namen des PPPoE-Intermediate-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.
- %v: fügt die VLAN-ID des PPPoE-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des PPPoE-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- %p: fügt den Namen der Ethernet-Schnittstelle ein, die das PPPoE-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind %p und %i identisch.
- %s: fügt die WLAN-SSID ein, wenn das PPPoE-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- %e: fügt die Seriennummer des PPPoE-Intermediate-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

SNMP-ID:

2.20.43.3

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

max. 30 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Circuit-Id

Die Circuit-ID ist eine Unteroption der PPPoE-Intermediate-Agent-Option und kennzeichnet eindeutig die Schnittstelle, über die ein Client einen PPPoE-Request stellt.

Sie können die folgenden Variablen verwenden:

- %%: fügt ein Prozent-Zeichen ein.
- %c: fügt die MAC-Adresse der Schnittstelle ein, auf der der PPPoE-Intermediate-Agent den PPPoE-Request erhalten hat. Handelt es sich um eine WLAN-SSID, ist das die entsprechende BSSID.
- %i: fügt den Namen der Schnittstelle ein, auf der der PPPoE-Intermediate-Agent den PPPoE-Request erhalten hat.
- %n: fügt den Namen des PPPoE-Intermediate-Agents ein, wie er z. B. unter **Setup** > **Name** festgelegt ist.

- %v: fügt die VLAN-ID des PPPoE-Request-Pakets ein. Diese VLAN-ID stammt entweder direkt aus dem VLAN-Header des PPPoE-Datenpakets oder aus der VLAN-ID-Zuordnung für diese Schnittstelle.
- %p: fügt den Namen der Ethernet-Schnittstelle ein, die das PPPoE-Datenpaket empfangen hat. Diese Variable ist hilfreich bei Geräten mit eingebautem Ethernet-Switch oder Ethernet-Mapper, da diese mehr als eine physikalische Schnittstelle auf eine logische Schnittstelle mappen können. Bei anderen Geräten sind %p und %i identisch.
- %s: fügt die WLAN-SSID ein, wenn das PPPoE-Paket von einem WLAN-Client stammt. Bei anderen Clients enthält diese Variable einen leeren String.
- %e: fügt die Seriennummer des PPPoE-Intermediate-Agents ein, wie sie z. B. unter **Status** > **Hardware-Info** > **Seriennummer** zu finden ist.

SNMP-ID:

2.20.43.4

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

max. 30 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default-Wert:

leer

verwerfe-Server-Pakete

Hier bestimmen Sie, ob der PPPoE-Intermediate-Agent bereits vorhandene PPPoE-Tags behalten oder verwerfen soll.

SNMP-ID:

2.20.43.5

Pfad Telnet:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Mögliche Werte:

Ja

Der PPPoE-Intermediate-Agent entfernt vorhandene PPPoE-Tags und lässt sowohl „Circuit-ID" als auch „Remote-ID" leer.

Nein

Der PPPoE-Intermediate-Agent übernimmt vorhandene PPPoE-Tags.

Default-Wert:

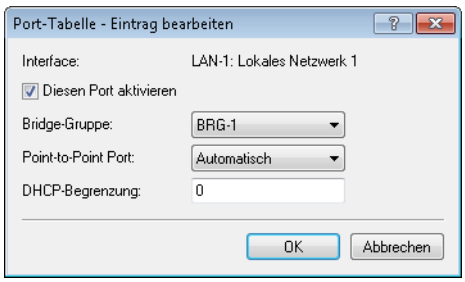
Nein

16.7 WAN-Bridge entfällt

Ab LCOS-Version 9.10 entfällt die Funktion „WAN-Bridge" für alle Geräte, die diese Version unterstützen.

16.7.1 Zuweisung von logischen Interfaces zu Bridge-Gruppen

Unter **Schnittstellen** > **LAN** definieren Sie in der **Port-Tabelle** spezielle Eigenschaften der logischen Interfaces.



Diesen Port aktivieren

Mit dieser Option wird das logische Interface aktiviert bzw. deaktiviert.

Bridge-Gruppe

Ordnet das logische Interface einer Bridge-Gruppe zu und ermöglicht so das Bridging von/zu diesem logischen Interface über die LAN-Bridge. Durch die Zuordnung zu einer gemeinsamen Bridge-Gruppe können mehrere logische Interfaces gemeinsam angesprochen werden und wirken so für den Router wie ein einzelnes Interface – z. B. für die Nutzung im Zusammenhang mit Advanced Routing and Forwarding.

Wird das Interface über die Einstellung **keine** aus allen Bridge-Gruppen entfernt, so findet keine Übertragung über die LAN-Bridge zwischen LAN und WLAN statt (isolierter Modus). In dieser Einstellung ist eine Datenübertragung zwischen LAN und WLAN für dieses Interface nur über den Router möglich.

Voraussetzung für die Datenübertragung von/zu einem logischen interface über die LAN-Bridge ist die Deaktivierung des globalen „Isolierten Modus", der für die gesamte LAN-Bridge gilt. Außerdem muss das logische Interface einer Bridge-Gruppe zugeordnet sein – in der Einstellung **keine** ist keine Übertragung über die LAN-Bridge möglich.

Point-to-Point Port

Dieser Wert beschreibt die in der IEEE 802.1D definierte „adminPointToPointMAC"-Einstellmöglichkeit. Standardmäßig wird die Point-to-Point-Einstellung der LAN-Schnittstelle automatisch aufgrund der Technologie und des momentanen Status hergeleitet. Es ist jedoch möglich, diese automatisch getroffene Festlegung zu revidieren, falls diese z. B. nicht brauchbar für die vorliegende Konfiguration erscheint.

Schnittstellen im Point-to-Point-Modus haben besondere Fähigkeiten, die benutzt werden können, um z. B. im Rapid-Spanning-Tree Verfahren die Port-Status-Wechsel zu beschleunigen.

DHCP-Begrenzung

Anzahl der Clients, die über DHCP zugewiesen werden können. Bei Überschreiten des Limits wird der jeweils älteste Eintrag verworfen. Dies kann in Kombination mit der Protokoll-Filter-Tabelle genutzt werden, um den Zugang auf ein logisches Interface zu begrenzen.

17 Backup-Lösungen

17.1 Backup-Verbindungen für Dual-SIM-Geräte

Ab LCOS-Version 9.10 sind bei Dual-SIM-Geräten auch Backup-Verbindungen möglich, wenn als primäre Verbindung eine Mobilfunkverbindung besteht. Darüber hinaus lässt sich die Zeit bis zum Rückschalten zur Primärverbindung explizit angeben.

17.1.1 Konfiguration der Backup-Verbindung

Zur Definition einer Backup-Verbindung sind im Prinzip die folgenden Konfigurationsschritte notwendig:

1. Für die Backup-Verbindung wird auf der entsprechenden WAN-Schnittstelle die Gegenstelle so eingerichtet, dass sie über diesen alternativen Weg erreichbar ist. Soll z. B. die ISDN-Leitung als Backup-Verbindung dienen, wird die Gegenstelle als ISDN-Gegenstelle angelegt (mit den zugehörigen Einträgen bei den Kommunikations-Layern und in der PPP-Liste).
2. Ggf. müssen Sie zur Überwachung der Verbindung noch einen Eintrag in der Polling-Tabelle anlegen, wenn die Gegenstelle nicht über LCP-Anfragen geprüft werden kann.
3. Zuordnung der neuen Backup-Verbindung zu der Gegenstelle, die über das Backup abgesichert werden soll. Diesen Eintrag nehmen Sie in der Backup-Tabelle vor. Für die Backup-Verbindung werden keine eigenen Einträge in der Routing-Tabelle benötigt. Die Backup-Verbindung übernimmt die Quell- und Ziel-Netze automatisch von der Gegenstelle, die im störungsfreien Betrieb die Daten routet.

   In der Backup-Tabelle können einer Gegenstelle auch mehrere Backup-Leitungen zugeordnet werden. Dabei wird dann festgelegt, welche der Backup-Leitungen im Bedarfsfalle zuerst aufgebaut werden soll:

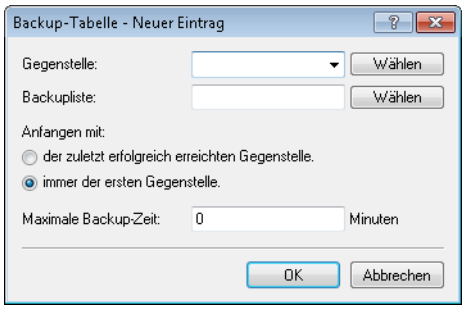
   - Die zuletzt erfolgreich erreichte Gegenstelle
   - Immer die erste Gegenstelle in der Liste

Die **maximale Backup-Zeit** gibt die maximale Zeitspanne in Minuten an, die der Backup-Zustand aufrecht erhalten wird. Wenn hier eine Zeit angegeben ist, so wird die Backup-Verbindung nach Ablauf dieser Zeit getrennt und der Backup-Zustand beendet.

Bei Backup-Szenarien mit Mobilfunk-Verbindungen (Multi-SIM), bei denen das Mobilfunk-Modul aus technischen Gründen zu jeder Zeit nur genau eine Verbindung haben kann, löst erst das Ende des Backup-Zustands einen erneuten Verbindungs-Versuch der Haupt-Verbindung aus.

Unabhängig vom Szenario tritt der Backup-Fall erneut ein, wenn die Haupt-Verbindung nach der außerhalb dieses Dialogs eingestellten Backup-Verzögerung nicht wieder aufgebaut werden kann.

Die Backup-Tabelle finden Sie in LANconfig unter **Kommunikation** > **Ruf-Verwaltung** in der **Backup-Tabelle**.



17.1.2 Backup-Verbindungen für Dual-SIM-Geräte

Bei Dual-SIM-Geräten ist es möglich, den zweiten Mobilfunk-Slot als Backup-Verbindung zu nutzen, wenn bereits die Primärverbindung eine Mobilfunkverbindung (über den ersten Mobilfunk-Slot) besteht.

1. .
2. .

17.1.3 Ergänzungen im Setup-Menü

Rueckfall-Minuten

Gibt die maximale Zeitspanne in Minuten an, die der Backup-Zustand aufrecht erhalten wird. Wenn hier eine Zeit angegeben ist, so wird die Backup-Verbindung nach Ablauf dieser Zeit getrennt und der Backup-Zustand beendet.

Bei Backup-Szenarien mit Mobilfunk-Verbindungen (Multi-SIM), bei denen das Mobilfunk-Modul aus technischen Gründen zu jeder Zeit nur genau eine Verbindung haben kann, löst erst das Ende des Backup-Zustands einen erneuten Verbindungs-Versuch der Haupt-Verbindung aus.

Unabhängig vom Szenario tritt der Backup-Fall erneut ein, wenn die Haupt-Verbindung nach der außerhalb dieses Dialogs eingestellten Backup-Verzögerung nicht wieder aufgebaut werden kann.

SNMP-ID:

2.2.24.4

Pfad Telnet:

Setup > **WAN** > **Backup-Gegenstellen**

Mögliche Werte:

max. 4 Zeichen aus `0123456789`

Default-Wert:

0

Besondere Werte:

0

18 Weitere Dienste

Ein Gerät bietet eine Reihe von Dienstleistungen für die PCs im LAN an. Es handelt sich dabei um zentrale Funktionen, die von den Arbeitsplatzrechnern genutzt werden können. Im Einzelnen handelt es sich um:

- Automatische Adressverwaltung mit DHCP
- Namenverwaltung von Rechnern und Netzen mit DNS
- Protokollierung von Netzverkehr mit SYSLOG
- Gebührenerfassung
- Bürokommunikations-Funktionen mit LANCAPI
- Zeit-Server

18.1 Perfect Forward Secrecy (PFS) bei Verbindungen bevorzugen

Ab LCOS-Version 9.10 ist es möglich, eine PFS-Chiffriermethode (Cipher-Suite) unabhängig von der abweichenden Einstellung des Clients vorzugeben.

18.1.1 Ergänzungen im Setup-Menü

PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

SNMP-ID:

2.11.29.6

Pfad Telnet:

Setup > **Config** > **Telnet-SSL**

Mögliche Werte:

Ein
Aus

Default-Wert:

Ein

PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

SNMP-ID:

2.21.40.7

Pfad Telnet:

Setup > **HTTP** > **SSL**

Mögliche Werte:

Ein
Aus

Default-Wert:

Ein

PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

SNMP-ID:

2.25.10.10.19.6

Pfad Telnet:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Mögliche Werte:

Ein
Aus

Default-Wert:

Ein

PFS-bevorzugen

Bei der Auswahl der Chiffrier-Methode (Cipher-Suite) richtet sich das Gerät normalerweise nach der Einstellung des anfragenden Clients. Bestimmte Anwendungen auf dem Client verlangen standardmäßig eine Verbindung ohne Perfect Forward Secrecy (PFS), obwohl Gerät und Client durchaus PFS beherrschen.

Mit dieser Option legen Sie fest, dass das Gerät immer eine Verbindung über PFS bevorzugt, unabhängig von der Standard-Einstellung des Clients.

SNMP-ID:

2.25.20.5

Pfad Telnet:

Setup > **RADIUS** > **RADSEC**

Mögliche Werte:

Ein
Aus

Default-Wert:

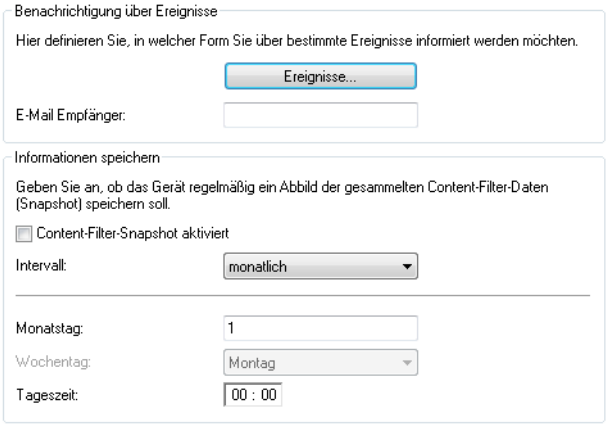
Ein

18.2 E-Mail-Benachrichtigung des Content-Filters

Ab LCOS-Version 9.10 ist es möglich, sich je nach Filterursache des Content-Filters eine E-Mail sofort oder täglich als Zusammenfassung zusenden zu lassen.

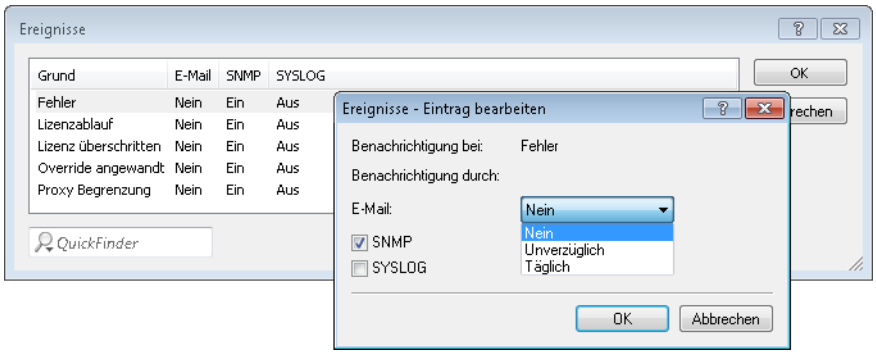
18.2.1 Optionen des LANCOM Content-Filters

Unter **Content-Filter** > **Optionen** können Sie einstellen, ob Sie über Ereignisse benachrichtigt werden und an wo die Informationen des LANCOM Content Filters gespeichert werden sollen.



Ereignisse

Hier definieren Sie, in welcher Form Sie über bestimmte Ereignisse informiert werden. Die Benachrichtigung kann erfolgen durch E-Mail, SNMP oder SYSLOG. Für verschiedene Ereignisse kann separat definiert werden, ob und in welcher Menge Meldungen ausgegeben werden sollen.



E-Mail

Definieren Sie hier, ob und wie eine E-Mail-Benachrichtigung erfolgt:

Nein

Für dieses Ereignis erfolgt keine E-Mail-Benachrichtigung.

Unverzüglich

Die Benachrichtigung erfolgt, sobald das Ereignis eintritt.

Täglich

Die Benachrichtigung erfolgt einmal am Tag.

Die folgenden Ereignisse stehen für Benachrichtigungen zur Verfügung:

Fehler

Bei SYSLOG: Quelle „System", Priorität „Alarm".

Default: Benachrichtigung SNMP

Lizenzablauf

Bei SYSLOG: Quelle „Verwaltung", Priorität „Alarm".

Default: Benachrichtigung SNMP

Lizenz überschritten

Bei SYSLOG: Quelle „Verwaltung", Priorität „Alarm".

Default: Benachrichtigung SNMP

Override angewandt

Bei SYSLOG: Quelle „Router", Priorität „Alarm".

Default: Benachrichtigung SNMP

Proxy-Begrenzung

Bei SYSLOG: Quelle „Router", Priorität „Info".

Default: Benachrichtigung SNMP

E-Mail Empfänger

Um die E-Mail-Benachrichtigungsfunktion zu nutzen, muss ein SMTP-Client entsprechend konfiguriert sein. Sie können den Client in diesem Gerät dazu verwenden oder einen anderen Ihrer Wahl.

Wenn kein E-Mail-Empfänger angegeben wird, dann wird keine E-Mail verschickt.

Content-Filter-Snapshot

Hier können Sie den Content-Filter-Snapshot aktivieren und bestimmen, wann und wie häufig er stattfindet. Der Schnappschuss kopiert die Tabelle der Kategoriestatistik in die Letzter-Schnappschuss-Tabelle, dabei wird der alte Inhalt der Schnappschuss-Tabelle überschrieben. Die Werte der Kategoriestatistik werden dann auf 0 gesetzt.

Intervall

Wählen Sie hier, ob der SnapShot monatlich, wöchentlich oder täglich angefertigt werden soll.

Mögliche Werte:

- monatlich, wöchentlich, täglich
- Default: monatlich

Monatstag

Ist eine monatliche Ausführung des SnapShot gewünscht, wählen Sie hier den Tag, an dem der SnapShot angefertigt werden soll. Mögliche Werte:

- max. 2 Zeichen
- Default:1

Wählen Sie als Monatstag sinnvollerweise eine Zahl zwischen 1 und 28, damit der Tag in jedem Monat vorkommt.

Wochentag

Ist eine wöchentliche Ausführung des SnapShot gewünscht, selektieren Sie hier den Wochentag, an dem der SnapShot angefertigt werden soll. Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag
- Default: Montag

Tageszeit

Ist eine tägliche Ausführung des SnapShot gewünscht, tragen Sie hier die Tageszeit in Stunden und Minuten ein. Mögliche Werte:

- max. 5 Zeichen, Format HH:MM
- Default: 00:00

18.2.2 Ergänzungen im Setup-Menü

Email

Geben Sie hier an, ob Sie eine Benachrichtigung per Email bekommen möchten.

Je nach Grund ist diese Option unterschiedlich vorbelegt.

SNMP-ID:

2.41.2.2.9.2

Pfad Telnet:

Setup > **UTM** > **Content-Filter** > **Globale-Einstellungen** > **Benachrichtigungen**

Mögliche Werte:

Aus
Sofort
Täglich

18.3 TACACS+-Erweiterung des passwd-Befehles

Ab LCOS-Version 9.10 ist die Passwort-Änderung eines Benutzers bei aktivierter TACAS+-Authentifizierung auch über den Konsolenbefehl `passwd` möglich.

Tabelle 13: Übersicht aller auf der Kommandozeile eingebbaren Befehle

Befehl	Beschreibung
`setpass|passwd [-u <User>][-n <new> <old>]`	Ändert das Passwort des aktuellen Benutzerkontos. Um das Passwort ohne die darauf folgende Eingabeaufforderung zu ändern, verwenden Sie den Optionsschalter `-n` mit Angabe des neuen und alten Passworts. Um bei aktivierter TACACS+-Authentifizierung das Passwort des lokalen Benutzerkontos zu ändern, verwenden Sie den Optionsschalter `-u` mit dem Namen des entsprechenden Benutzers. Existiert der lokale Benutzer nicht oder fehlt die Angabe des Benutzernamens, bricht der Befehl ab. Der Benutzer benötigt außerdem Supervisorrechte bzw. die TACAS-Authorisierung muss aktiv sein.

19 Sonstige Parameter

19.1 Profil

Zeigt das Profil des Mobilfunk-Modems an.

SNMP-ID:

1.49.45

Pfad Telnet:

Status > **Modem-Mobilfunk**

19.2 Neuverhandlungen

SNMP-ID:

2.11.29.7

Pfad Telnet:

Setup > **Config** > **Telnet-SSL**

Mögliche Werte:

verboten

Mögliche Werte:

erlaubt

Default-Wert:

erlaubt

Mögliche Werte:

ignoriert

19.3 TLS-Verbindungen

In diesem Verzeichnis legen Sie fest, über welche Adresse und auf welchem Port das Gerät eingehende Konfigurationsänderungen entgegennehmen soll.

SNMP-ID:

2.11.51.3

Pfad Telnet:

Setup > **Config** > **Sync**

19.3.1 Port

Geben Sie den Port an, auf dem das Gerät eingehende Konfigurationsänderungen entgegennehmen soll.

SNMP-ID:

2.11.51.3.1

Pfad Telnet:

Setup > **Config** > **Sync** > **TLS-Verbindungen**

Mögliche Werte:

max. 5 Zeichen aus `0123456789`

0 … 65535

Default-Wert:

1941

19.4 Error-Aging-Minutes

SNMP-ID:

2.11.65

Pfad Telnet:

Setup > **Config**

19.5 MTU

SNMP-ID:

2.19.34

Pfad Telnet:

Setup > **VPN**

19.6 Neuverhandlungen

SNMP-ID:

2.21.40.8

Pfad Telnet:

Setup > **HTTP** > **SSL**

Mögliche Werte:

verboten
erlaubt
ignoriert

19.7 Permanente-L1-Aktivierung

SNMP-ID:

2.23.18

Pfad Telnet:

Setup > **Schnittstellen**

Mögliche Werte:

deaktiviert
nur Sync-Quelle
Alle TE-Schnittstellen

19.8 PCM-SYNC-SOURCE

SNMP-ID:

2.23.19

Pfad Telnet:

Setup > **Schnittstellen**

Mögliche Werte:

Auto
S0-1

19.9 LBS-Tracking

SNMP-ID:

2.23.20.1.25

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

nein
ja

19.10 LBS-Tracking-Liste

SNMP-ID:

2.23.20.1.26

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Netzwerk**

Mögliche Werte:

Name aus **Setup** > **WLAN** > **Netzwerk** > **LBS-Tracking**

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

19.11 OKC

Diese Option aktiviert oder deaktiviert das Opportunistic Key Caching (OKC).

Diesen Wert übernimmt das Gerät ausschließlich, wenn die Schnittstelle im Client-Modus arbeitet. Befindet sich die Schnittstelle im AP-Modus, ist die Aktivierung oder Deaktivierung von OKC nur über die Profilverwaltung eines WLCs möglich.

Im PMK-Caching-Status unter **Status** > **WLAN** > **PMK-Caching** > **Inhalt** sind OKC-PMKs an der Authenticator-Adresse `ff:ff:ff:ff:ff:`n zu erkennen, wobei n die zugeordnete Profilnummer ist (z. B. `0` für „WLAN-1", `1` für „WLAN1-2" etc.).

SNMP-ID:

2.23.20.3.17

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Verschlüsselung**

Mögliche Werte:

ja
nein

Default-Wert:

ja

19.12 Netzwerk-Name

Geben Sie hier einen eindeutigen Namen für das Netzwerk ein, in dem sich diese WLAN-Schnittstelle befindet.

SNMP-ID:

2.23.20.5.15

Pfad Telnet:

Setup > **Schnittstellen** > **WLAN** > **Interpoint-Einstellungen**

Mögliche Werte:

max. 32 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

19.13 Passworteingabe-Einstellung

SNMP-ID:

2.24.19.18

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

Buchstaben+Zahlen
Buchstaben
Zahlen

19.14 CSV-Export-verstecken

Dieser Parameter gibt Ihnen die Möglichkeit, den Export der Konfiguration in eine CSV-Datei zu verhindern.

SNMP-ID:

2.24.19.19

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Neuer-Benutzer-Assistent**

Mögliche Werte:

nein
ja

Default-Wert:

nein

19.15 Verwalte-Benutzer-Assistent

SNMP-ID:

2.24.44

Pfad Telnet:

Setup > **Public-Spot-Modul**

19.15.1 Zeige-Statusinformationen

Dieser Eintrag bietet Ihnen die Möglichkeit, Statusinformationen im Setup-Wizard zu verbergen.

SNMP-ID:

2.24.44.10

Pfad Telnet:

Setup > **Public-Spot-Modul** > **Verwalte-Benutzer-Assistent**

Mögliche Werte:

nein

Der Setup-Wizard blendet folgende Spalten aus: **Online-Zeit**, **Traffic**, **Status**, **MAC-Adresse**, **IP-Adresse**.

ja

Der Setup-Wizard zeigt alle Statusinformationen an.

19.16 Neuverhandlungen

SNMP-ID:

2.25.20.6

Pfad Telnet:

Setup > **RADIUS** > **RADSEC**

Mögliche Werte:

verboten
erlaubt
ignoriert

19.17 LBS-Tracking-Liste

SNMP-ID:

2.37.1.1.47

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

Mögliche Werte:

Name aus **Setup** > **WLAN-Management** > **AP-Konfiguration** > **LBS-Tracking**

max. 16 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

19.18 LBS-General-Profil

SNMP-ID:

2.37.1.3.9

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration**

19.19 LBS-Device-Location-Profil

SNMP-ID:

2.37.1.4.28

Pfad Telnet:

Setup > **WLAN-Management** > **AP-Konfiguration** > **Basisstationen**

19.20 Max.-Anzahl-gleichzeitiger-Updates

SNMP-ID:

2.37.27.38

Pfad Telnet:

Setup > **WLAN-Management** > **Zentrales-Firmware-Management**

Mögliche Werte:

max. 31 Zeichen aus `[0-9]`

Default-Wert:

leer

19.21 CAPWAP-Port

SNMP-ID:

2.59.5

Pfad Telnet:

Setup > **WLAN-Management**

Mögliche Werte:

max. 31 Zeichen aus `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

19.22 RS-Anzahl

Konfiguriert die Anzahl der IPv6-Router-Solicitations, die das Gerät nach dem Start des IPv6-LAN-Interfaces versenden soll.

SNMP-ID:

2.70.6.13

Pfad Telnet:

Setup > **IPv6** > **LAN-Interfaces**

Mögliche Werte:

max. 1 Zeichen aus `[0-9]`

Default-Wert:

3

19.23 RS-Anzahl

Konfiguriert die Anzahl der IPv6 Router Solicitations, die das Gerät nach dem Start des IPv6 WAN-Interfaces versenden soll.

SNMP-ID:

2.70.7.11

Pfad Telnet:

Setup > **IPv6** > **WAN-Interfaces**

Mögliche Werte:

max. 1 Zeichen aus `[0-9]`

Default-Wert:

3

19.24 Secure Upload

In diesem Menü haben Sie die Möglichkeit, sichere Uploads zu definieren.

SNMP-ID:

3.5

Pfad Telnet:

Firmware

19.25 Flash-Restore

Befindet sich das Gerät im Testmodus, können Sie die Konfiguration aus dem Flash wieder herstellen. Nutzen Sie dazu auf der Kommandozeilenebene den Befehl `do/Other/Flash-Restore`. Dieser Befehl stellt die ursprüngliche Konfiguration aus dem Flash vor der Ausführung des Kommandos "Flash No" wieder her.

SNMP-ID:

4.7

Pfad Telnet:

Sonstiges > **Flash-Restore**

19.26 Ergänzungen im Status-Menü

19.26.1 DSLAM-Chipsatzhersteller-Dump

Zeigt einen Dump des DSLAM-Chipsatzherstellers an.

SNMP-ID:

1.41.25.47

Pfad Telnet:

Status > **ADSL** > **Erweitert**

19.26.2 DSLAM-Hersteller-Dump

Zeigt einen Dump des DSLAM-Herstellers an.

SNMP-ID:

1.41.25.48

Pfad Telnet:

Status > **ADSL** > **Erweitert**

19.26.3 DSLAM-Chipsatzhersteller-Dump

Zeigt den DSLAM-Chipsatzhersteller-Dump an.

SNMP-ID:

1.75.25.47

Pfad Telnet:

Status > **VDSL** > **Erweitert**

19.26.4 DSLAM-Hersteller-Dump

Zeigt den DSLAM-Hersteller-Dump an.

SNMP-ID:

1.75.25.48

Pfad Telnet:

Status > **VDSL** > **Erweitert**