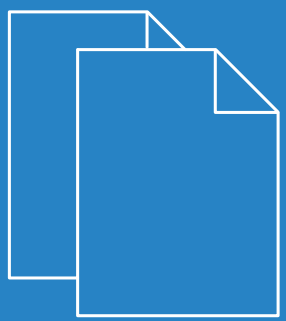
SICHER. **VERNETZT.**

LCOS LX 5.20

Menüreferenz



05/2020

LANCOM Systems

Inhalt

Copyright

Alle Angaben in dieser Dokumentation sind nach sorgfältiger Prüfung zusammengestellt worden, gelten jedoch nicht als Zusicherung von Produkteigenschaften. LANCOM Systems haftet ausschließlich in dem Umfang, der in den Verkaufs- und Lieferbedingungen festgelegt ist.

Das Produkt enthält separate Komponenten, die als sogenannte Open Source Software eigenen Lizenzen, insbesondere der General Public License (GPL), unterliegen. Die Lizenzinformationen zur Geräte-Firmware (LCOS LX) finden Sie über die Kommandozeile mit dem Befehl `show 3rd-party-licenses`. Sofern die jeweilige Lizenz dies verlangt, werden Quelldateien zu den betroffenen Software-Komponenten auf Anfrage bereitgestellt. Wenden Sie sich hierzu via E-Mail an *gpl@lancom.de*.

Produkte von LANCOM Systems enthalten Software, die vom „OpenSSL Project" für die Verwendung im „OpenSSL Toolkit" entwickelt wurde (*www.openssl.org*).

Produkte von LANCOM Systems enthalten kryptographische Software, die von Eric Young (*eay@cryptsoft.com*) geschrieben wurde.

Produkte von LANCOM Systems enthalten Software, die von der NetBSD Foundation, Inc. und ihren Mitarbeitern entwickelt wurde.

Produkte von LANCOM Systems enthalten das LZMA SDK, das von Igor Pavlov entwickelt wurde.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen

Deutschland

www.lancom-systems.de

1 Einleitung

1.1 Bestandteile der Dokumentation

Die Dokumentation Ihres Gerätes besteht aus folgenden Teilen:

Installation Guide

In dieser Kurzanleitung finden Sie Antworten auf die folgende Fragen:

- Welche Software muss zur Konfiguration installiert werden?
- Wie wird das Gerät angeschlossen?
- Wie kann das Gerät über LANconfig bzw. WEBconfig erreicht werden?
- Wie wird das Gerät der LANCOM Management Cloud zugeordnet?
- Wie startet man die Setup-Assistenten (z. B. zur Einrichtung des Internetzugangs)?
- Wie wird ein Gerätereset durchgeführt?
- Wo gibt es weitere Informationen und Hilfe?

Hardware-Schnellübersicht

Die Hardware-Schnellübersicht enthält alle Informationen, die zur raschen Inbetriebnahme Ihres Gerätes notwendig sind. Außerdem finden Sie hier alle wichtigen technischen Spezifikationen.

Referenzhandbuch

Das Referenzhandbuch geht ausführlich auf Themen ein, die übergreifend für mehrere Modelle gelten. Die Beschreibungen im Referenzhandbuch orientieren sich überwiegend an der Konfiguration mit LANconfig.

Menü-Referenz

Die vorliegende Menü-Referenz beschreibt alle Parameter von LCOS LX. Diese Beschreibung unterstützt den Anwender bei der Konfiguration der Geräte über die Konsole. Zu jedem Parameter werden neben der Beschreibung auch die möglichen Eingabewerte und die Standardbelegung wiedergegeben.

Alle Dokumente, die Ihrem Produkt nicht in gedruckter Form beiliegen, finden Sie als PDF-Datei unter *www.lancom-systems.de/downloads*.

1.2 LCOS LX, ein Betriebssystem von LANCOM

LCOS LX ist das Betriebssystem für bestimmte LANCOM Access Points und Teil der LANCOM Betriebssystem-Familie. Die LANCOM Betriebssysteme sind die vertrauenswürdige Grundlage für das gesamte LANCOM Produktportfolio. Jedes Betriebssystem verkörpert die LANCOM Werte Sicherheit, Zuverlässigkeit und Zukunftsfähigkeit.

- **Für höchste Sicherheit Ihrer Netzwerke**

  wird jedes LANCOM Betriebssystem in gewohnter Qualität von unseren Entwicklern sorgfältig gepflegt und weiterentwickelt und ist garantiert Backdoor-frei.

- **Sie stehen für größtmögliche Zuverlässigkeit,**

  denn über die gesamte Lebenszeit eines Produktes werden regelmäßig Release Updates, Security Updates und Major Releases zur Verfügung gestellt.

> **Als Grundlage maximaler Zukunftsfähigkeit Ihrer Netzwerke**
>
> stehen sie im Zuge der LANCOM Lifecycle-Richtlinien für alle LANCOM Produkte kostenlos zur Verfügung, inklusive neuer Major Features.

1.3 Gültigkeit

Die in diesem Handbuch beschriebenen Funktionen und Einstellungen werden nicht von allen Modellen bzw. allen Firmware-Versionen unterstützt.

1.4 Konsole – Zugang

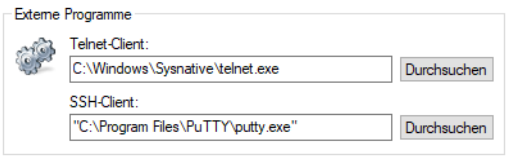
Der Zugang zur LCOS LX-Konsole erfolgt über SSH. Nutzen Sie einen SSH-Client wie z. B. PuTTY, um sich unter Angabe der IP-Adresse des Gerätes mit diesem zu verbinden.

Die Zugangsdaten eines Gerätes im Auslieferungszustand sind:

Benutzername: root

Passwort: <Leer> (es ist kein Passwort gesetzt)

Konfigurieren Sie den von Ihnen präferierten SSH-Client in LANconfig unter **Extras** > **Optionen** > **Extras** > **SSH-Client**:



Anschließend können Sie im Kontextmenü des Gerätes unter **WEBconfig / Konsolen-Sitzung** > **SSH-Sitzung öffnen** eine Konsole öffnen.

1.5 Konsole – Menüstruktur

Das LCOS LX-Kommandozeilen-Interface (die Konsole) ist wie folgt strukturiert:

Status

Enthält die Zustände und Statistiken aller internen Module des Gerätes. Diese sind hier nicht beschrieben, da sich die aufbereitete Visualisierung in WEBconfig empfiehlt. Alternativ können Sie für ihr Gerät die Management Information Base (MIB) herunterladen, welche für die Verwendung mit SNMPv3 die Einträge jeweils mit einer kurzen Beschreibung enthält. Die Geräte-MIB können Sie von *www.lancom-systems.de/downloads/* herunterladen.

Setup

Beinhaltet alle einstellbaren Parameter aller internen Module des Gerätes. Siehe *Setup*.

Sonstiges

Enthält Aktionen wie z. B. für den Reset oder den Reboot. Siehe *Other*.

1.6 Konsole – Befehlsübersicht

Das Kommandozeilen-Interface wird mit den folgenden Befehlen bedient.

Die verfügbaren Befehle sind abhängig vom Funktionsumfang des jeweiligen Gerätes.

Änderungen an der Konfiguration sind nicht sofort boot-persistent. Sie müssen mit dem Befehl `flash` explizit gespeichert werden.

Tabelle 1: Übersicht aller auf der Kommandozeile eingebbaren Befehle

Befehl	Beschreibung
`add [<Path>]`	Fügt eine Tabellenzeile hinzu.
`cd <Path>`	Wechselt das aktuelle Menü bzw. Verzeichnis.
`default`	Setzt die Tabelle oder den Wert auf die Defaulteinstellung zurück. Dieses Kommando arbeitet rekursiv. Daher werden alle Werte und Tabellen sowohl im aktuellen als auch in allen darunter liegenden Pfaden zurückgesetzt.
`del <Path>`	Löscht den Wert oder die Tabellenzeile im mittels `<Path>` referenzierten Zweig des Menübaums.
`do <Path> [<Parameter>]`	Führt die angegebene Aktion im aktuellen bzw. referenzierten Verzeichnis aus. Sofern die Aktion über zusätzliche Parameter verfügt, lassen sich diese nachfolgend angeben.
`exit`	Beendet die Terminalsitzung.
`flash`	Konfiguration speichern. Änderungen an der Konfiguration sind nicht sofort boot-persistent. Sie müssen mit dem Befehl `flash` explizit gespeichert werden.
`ls [<Path>]`	Zeigt den Inhalt des aktuellen Verzeichnisses oder des angegebenen Pfades an.
`passwd <Password>`	Ändert das Passwort des aktuellen Benutzerkontos.
`set <Index> {Column} <Value>`	Setzt den Wert einer bestimmten Spalte (Column) einer Tabellenzeile auf <Value>.
`set <Path> <Value(s)>`	Setzt den oder die Werte eines bestimmten Pfades auf den oder die angegebenen Werte.
`show diag [<Parameter>]`	Diagnoseinformationen auf der Konsole ausgeben.
`show 3rd-party-licenses`	Die Lizenzinformationen des Gerätes auf der Konsole ausgeben.
`startlmc <Activation Code> [Domain]`	Nachdem Sie in der LANCOM Management Cloud einen Aktivierungscode erzeugt haben, können Sie dieses Gerät über diesen Code mit der LANCOM Management Cloud koppeln. Optional können Sie dabei auch eine neue LMC-Domain angeben.
`sysinfo`	Zeigt Systeminformationen an (z. B. Hardware-Release, Softwareversion, MAC-Adresse, Seriennummer etc.).

Befehl	Beschreibung
`trace [--log] [+|-|#|?] <Parameter>`	Startet (+) oder stoppt (–) einen Trace-Befehl zur Ausgaben von Diagnose-Daten. # schaltet zwischen verschiedenen Trace-Ausgaben um und ? zeigt einen Hilfetext an Über den Parameter `--log` kann die Ausgabe auf „historische" Informationen aus dem Log eingeschränkt werden.

Legende

- Zeichen- und Klammernregelung:
  - Objekte – hier: dynamische oder situationsabhängige Eingaben – stehen in spitzen Klammern.
  - Runde Klammern gruppieren Befehlsbestandteile zur besseren Übersicht.
  - Vertikale Striche (Pipes) trennen alternative Eingaben.
  - Eckige Klammern beschreiben optionale Schalter.

  Somit sind alle Befehlsbestandteile, die nicht in eckigen Klammern stehen, notwendigen Angaben zuzurechnen.
- `<Path>`:
  - Beschreibt den Pfadnamen für ein Menü, eine Tabelle oder einen Parameter, getrennt durch "/".
  - `..` bedeutet: eine Ebene höher.
  - `.` bedeutet: aktuelle Ebene.
- `<Value>`:
  - Beschreibt einen möglichen Eingabewert.
  - `""` ist ein leerer Eingabewert.
- `<Name>`:
  - Beschreibt eine Zeichensequenz von [0…9] [A…Z] [a…z] [_].
  - Das erste Zeichen darf keine Ziffer sein.
  - Es gibt keine Unterscheidung zwischen Groß- und Kleinschreibung.
- `<Filter>`:
  - Die Ausgaben einiger Kommandos können durch die Angabe eines Filterausdrucks eingeschränkt werden. Die Filterung erfolgt dabei nicht zeilenweise, sondern blockweise abhängig vom jeweiligen Kommando.
  - Ein Filterausdruck beginnt mit einem alleinstehenden '@' und endet entweder am Zeilenende oder an einem alleinstehenden ';', welches das aktuelle Kommando abschließt.
  - Ein Filterausdruck besteht des Weiteren aus einem oder mehreren Suchmustern, die durch Leerzeichen voneinander getrennt sind und denen entweder kein Operator ('Oder'-Muster) oder einer der Operatoren '+' ('Und'- Muster) oder '-' ('Nicht'-Muster) vorangestellt ist.
  - Bei der Ausführung des Kommandos wird ein Informationsblock genau dann ausgegeben, wenn mindestens eines der 'Oder'-Muster, alle 'Und'-Muster und keines der 'Nicht'-Muster passen. Dabei wird die Groß- und Kleinschreibung nicht beachtet.
  - Soll ein Suchmuster Zeichen enthalten, die zur Strukturierung in der Filtersyntax verwendet werden (z. B. Leerzeichen), dann kann das Suchmuster als Ganzes mit '"' umschlossen werden. Alternativ kann den speziellen Zeichen ein '\' vorangestellt werden. Wenn ein '"' oder ein '\' gesucht werden soll, muss diesem ein '\' vorangestellt werden.

    Es reicht die Eingabe des eindeutigen Wortanfangs.

Erläuterungen zur Adressierung, Schreibweise und Befehlseingabe

- Alle Befehle, Verzeichnis- und Parameternamen können verkürzt eingegeben werden, solange sie eindeutig sind. Zum Beispiel kann der Befehl `cd setup` zu `cd se` verkürzt werden. Die Eingabe `cd /s` dagegen ist ungültig, da dieser Eingabe sowohl `cd /Setup` als auch `cd /Status` entspräche.
- Die Werte in einer Tabellenzeile können alternativ über den Spaltennamen oder die Positionsnummer in geschweiften Klammern angesprochen werden. Der Befehlt `set ?` in der Tabelle zeigt neben dem Namen und den möglichen Eingabewerten auch die Positionsnummer für jede Spalte an.
- Mehrere Werte in einer Tabellenzeile können mit **einem** Befehl verändert werden, z. B. in der Tabelle der WLAN-Netzwerke (`/Setup/WLAN/Network`):
  - `add Guest Guest 1234567890` erstellt ein neues Netzwerk mit dem Namen Guest, der SSID Guest und dem Key 1234567890.

    Die Reihenfolge der Werte muss der Reihenfolge in der Tabelle entsprechen. Werte, die nicht verändert werden sollen, können mit einem * angegeben werden.
  - `set Guest * 0987654321` ändert den Wert Key im Netzwerk Guest. Die SSID wird durch den * unverändert gelassen.
  - `set Guest {Key} 1234567890` setzt den Wert Key im Netzwerk Guest. Einzelne Spalten lassen sich durch den Spaltennamen in runden Klammern referenzieren.
- Namen, die Leerzeichen enthalten, müssen in Anführungszeichen ("") eingeschlossen werden.

Kommandospezifische Hilfe

- Für Aktionen und Befehle steht eine kommandospezifische Hilfefunktion zur Verfügung, indem die Funktion mit einem Fragezeichen als Optionsschalter aufgerufen wird. Zum Beispiel zeigt der Aufruf `show ?` die Optionen des show-Kommandos an.

2 Setup

In diesem Menü finden Sie die Einstellungen des Gerätes.

Pfad Konsole:

/

2.1 Name

Konfigurieren Sie hier den Gerätenamen. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9 SNMP

Dieses Menü enthält die Konfiguration von SNMP.

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie von *www.lancom-systems.de/downloads/* herunterladen können.

Pfad Konsole:

Setup

2.9.1 Send-Traps

Bei schwerwiegenden Fehlern, zum Beispiel bei einem unberechtigten Zugriff, kann das Gerät automatisch eine Fehlermeldung an einen oder mehrere SNMP-Manager senden. Schalten Sie dazu diese Option ein und geben Sie in der Tabelle Target-Addresses die Ziele ein, auf denen diese SNMP-Manager installiert sind.

Pfad Konsole:

Setup > SNMP

Mögliche Werte:

Yes
No

Default-Wert:

No

2.9.21 Port

Über diesen Parameter legen Sie den Port fest, über den der SNMP-Dienst für externe Programme wie z. B. LANmonitor erreichbar ist.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

0 … 65535

Default-Wert:

161

2.9.27 Communities

SNMP-Agents und SNMP-Manager gehören SNMP-Communities an. Diese Communities fassen bestimmte SNMP-Hosts zu Gruppen zusammen, um diese einerseits einfacher verwalten zu können. Andererseits bieten SNMP-Communities eine eingeschränkte Sicherheit beim Zugriff über SNMP, da ein SNMP-Agent nur SNMP-Anfragen von Teilnehmern akzeptiert, deren Community ihm bekannt ist.

In dieser Tabelle konfigurieren Sie die SNMP-Communities.

Als Standard ist die SNMP-Community `public` eingerichtet, die den uneingeschränkten SNMP-Lesezugriff ermöglicht.

Pfad Konsole:

Setup > **SNMP**

2.9.27.1 Name

Vergeben Sie hier einen aussagekräftigen Namen für diese SNMP-Community.

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

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

Default-Wert:

leer

2.9.27.3 Security-Name

Geben Sie hier die Bezeichnung für die Zugriffsrichtlinie ein, die die Zugriffsrechte für alle Community-Mitglieder festlegt.

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

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

Default-Wert:

leer

2.9.27.8 Status

Mit diesem Eintrag aktivieren oder deaktivieren Sie diese SNMP-Community.

Pfad Konsole:

Setup > **SNMP** > **Communities**

Mögliche Werte:

Active
Die Community ist aktiviert.

Inactive
Die Community ist deaktiviert.

Default-Wert:

Active

2.9.28 Groups

Durch die Konfiguration von SNMP-Gruppen lassen sich Authentifizierung und Zugriffsrechte für mehrere Benutzer komfortabel verwalten und zuordnen.

Pfad Konsole:

Setup > **SNMP**

2.9.28.1 Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, so dass in der SNMP-Konfiguration von LCOS LX hauptsächlich das Security-Model „SNMPv3" zum Einsatz kommt. Aus Kompatibilitätsgründen kann es jedoch notwendig sein, auch die Versionen SNMPv2c oder sogar SNMPv1 zu berücksichtigen und entsprechend als „Security-Model" auszuwählen.

Entsprechend wählen Sie hier ein Security-Modell aus.

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

Any

Jedes Modell wird akzeptiert.

SNMPv1

Die Übertragung der Daten erfolgt über SNMPv1. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv".

SNMPv2_C

Die Übertragung der Daten erfolgt über SNMPv2c. Die Authentifizierung des Benutzers erfolgt ausschließlich über den Community-String in der SNMP-Nachricht. Eine Verschlüsselung der Kommunikation findet nicht statt. Das entspricht der Sicherheitsstufe „NoAuthNoPriv".

SNMPv3_USM

Die Übertragung der Daten erfolgt über SNMPv3. Für Anmeldung und Kommunikation des Benutzers sind die folgenden Sicherheitsstufen möglich:

NoAuthNoPriv

Die Authentifizierung erfolgt nur über die Angabe und Auswertung des Benutzernamens. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthNoPriv

Die Authentifizierung erfolgt über die Hash-Algorithmen HMAC-MD5 oder HMAC-SHA. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv

Die Authentifizierung erfolgt über die Hash-Algorithmen HMAC-MD5 oder HMAC-SHA. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

Default-Wert:

SNMPv3_USM

2.9.28.2 Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

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

Default-Wert:

leer

2.9.28.3 Group-Name

Vergeben Sie hier einen aussagekräftigen Namen für diese Gruppe. Diesen Namen verwenden Sie anschließend bei der Konfiguration der Zugriffsrechte.

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

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

Default-Wert:

leer

2.9.28.5 Status

Aktiviert oder deaktiviert diese Gruppenkonfiguration.

Pfad Konsole:

Setup > **SNMP** > **Groups**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.29 Accesses

Diese Tabelle führt die verschiedenen Konfigurationen für Zugriffsrechte, Security-Models und Ansichten zusammen.

Pfad Konsole:

Setup > **SNMP**

2.9.29.1 Group-Name

Wählen Sie hier den Namen einer Gruppe aus, für die diese Zugriffsrechte gelten sollen.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

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

Default-Wert:

leer

2.9.29.3 Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

Any
Jedes Modell wird akzeptiert.

SNMPv1
SNMPv1 wird verwendet.

SNMPv2_C
SNMPv2c wird verwendet.

SNMPv3_USM
SNMPv3 wird verwendet.

Default-Wert:

Any

2.9.29.5 Read-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

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

Default-Wert:

leer

2.9.29.6 Write-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Schreibrechte erhalten soll.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

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

Default-Wert:

leer

2.9.29.7 Notify-View-Name

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Notify-Rechte erhalten soll.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

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

Default-Wert:

leer

2.9.29.8 Status

Aktiviert oder deaktiviert diesen Eintrag.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.29.10 Min-Security-Level

Geben Sie die minimale Sicherheit an, die für Zugriff und Datenübertragung gelten soll.

Pfad Konsole:

Setup > **SNMP** > **Accesses**

Mögliche Werte:

NoAuthNoPriv

Die SNMP-Anfrage ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

AuthNoPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt jedoch unverschlüsselt.

AuthPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Default-Wert:

AuthPriv

2.9.30 Views

In dieser Tabelle fassen Sie verschiedene Werte oder ganze Zweige der MIB des Gerätes zusammen, die ein Benutzer gemäß seiner Zugriffsrechte einsehen oder verändern kann.

Pfad Konsole:

Setup > **SNMP**

2.9.30.1 View-Name

Vergeben Sie hier der Ansicht einen aussagekräftigen Namen.

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

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

Default-Wert:

leer

2.9.30.3 OID-Subtree

Bestimmen Sie durch komma-separierte Angabe der jeweiligen OIDs, welche Werte und Aktionen der MIB diese Ansicht einschließen soll.

Die OIDs entnehmen Sie bitte der Geräte-MIB, die Sie von *www.lancom-systems.de/downloads/* herunterladen können.

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.30.4 Type

Bestimmen Sie, ob die nachfolgend angegebenen OID-Teilbäume Bestandteil („Included") oder kein Bestandteil („Excluded") der Ansicht sind.

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

Included

Diese Einstellung gibt MIB-Werten mit aus.

Excluded

Diese Einstellung blockt die Ausgabe von MIB-Werten.

Default-Wert:

Included

2.9.30.6 Status

Aktiviert oder deaktiviert diese Ansicht.

Pfad Konsole:

Setup > **SNMP** > **Views**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.32 Users

Dieses Menü enthält die Benutzerkonfiguration.

Pfad Konsole:

Setup > **SNMP**

2.9.32.2 Username

Geben Sie hier den SNMPv3 Benutzernamen an.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

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

Default-Wert:

leer

2.9.32.5 Authentication-Protocol

Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

None
Eine Authentifizierung des Benutzers ist nicht notwendig.

HMAC-MD5
Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-MD5-96 (Hash-Länge 128 Bits).

HMAC-SHA
Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-96 (Hash-Länge 160 Bits).

HMAC-SHA224
Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-224 (Hash-Länge 224 Bits).

HMAC-SHA256
Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-256 (Hash-Länge 256 Bits).

HMAC-SHA384
Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-384 (Hash-Länge 384 Bits).

HMAC-SHA512
Die Authentifizierung erfolgt mit dem Hash-Algorithmus HMAC-SHA-512 (Hash-Länge 512 Bits).

2.9.32.6 Authentication-Password

Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein.

Eine Klartexteingabe ist nur möglich wenn vorher der Parameter in *2.9.32.14 Authentication-Password-Type* auf Seite 22 geändert wird.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

max. 130 Zeichen aus `anything printable`

Default-Wert:

leer

2.9.32.8 Privacy-Protocol

Bestimmen Sie, nach welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt sein soll.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

None

Die Kommunikation erfolgt unverschlüsselt.

DES

Die Verschlüsselung erfolgt mit DES (Schlüssellänge 56 Bits).

AES128

Die Verschlüsselung erfolgt mit AES128 (Schlüssellänge 128 Bits).

AES192

Die Verschlüsselung erfolgt mit AES192 (Schlüssellänge 192 Bits).

AES256

Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

2.9.32.9 Privacy-Password

Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein.

Eine Klartexteingabe ist nur möglich wenn vorher der Parameter in *2.9.32.15 Privacy-Password-Type* auf Seite 22 geändert wird.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

max. 130 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.``

Default-Wert:

leer

2.9.32.13 Status

Aktiviert oder deaktiviert diesen Benutzer.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.32.14 Authentication-Password-Type

Das Passwort in *2.9.32.6 Authentication-Password* auf Seite 20 wird immer verschlüsselt abgelegt (Typ „Masterkey“). Falls Sie z. B. über die Konsole dort ein neues Passwort eintragen wollen, dann müssen Sie vorher hier den Typ auf „Plaintext“ ändern. Danach kann ein Passwort im Klartext eingegeben werden. LCOS LX wird anschließend das Passwort verschlüsseln und diesen Wert wieder auf „Masterkey“ zurücksetzen.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

Plaintext
Masterkey

2.9.32.15 Privacy-Password-Type

Das Passwort in *2.9.32.9 Privacy-Password* auf Seite 21 wird immer verschlüsselt abgelegt (Typ „Masterkey“). Falls Sie z. B. über die Konsole dort ein neues Passwort eintragen wollen, dann müssen Sie vorher hier den Typ auf „Plaintext“ ändern. Danach kann ein Passwort im Klartext eingegeben werden. LCOS LX wird anschließend das Passwort verschlüsseln und diesen Wert wieder auf „Masterkey“ zurücksetzen.

Pfad Konsole:

Setup > **SNMP** > **Users**

Mögliche Werte:

Plaintext
Masterkey

2.9.34 Target-Addresses

In der Liste der Empfängeradressen konfigurieren Sie die Empfänger, an die der SNMP-Agent die SNMP-Traps versendet.

Pfad Konsole:

Setup > **SNMP**

2.9.34.1 Name

Geben Sie hier den Ziel-Adress-Namen an.

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

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

Default-Wert:

leer

2.9.34.3 Transport-Address

Die Transportadresse beschreibt die IP-Adresse und Port-Nummer eines SNMP-Trap-Empfängers und wird in der Syntax <IP-Adresse>:<Port> angegeben (z. B. 128.1.2.3:162). Der UDP-Port 162 wird für SNMP-Traps verwendet.

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.9.34.7 Parameters-Name

Wählen Sie hier den gewünschten Eintrag aus der Liste der Empfängerparameter aus.

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

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

Default-Wert:

leer

2.9.34.9 Status

Aktiviert oder deaktiviert diese Zieladresse.

Pfad Konsole:

Setup > **SNMP** > **Target-Addresses**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.35 Target-Params

In dieser Tabelle konfigurieren Sie, wie der SNMP-Agent die SNMP-Traps behandelt, die er an die Empfänger versendet.

Pfad Konsole:

Setup > **SNMP**

2.9.35.1 Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

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

Default-Wert:

leer

2.9.35.2 Message-Processing-Model

Bestimmen Sie hier, nach welchem Protokoll der SNMP-Agent die Nachricht strukturiert.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

SNMPv1
SNMPv2c
SNMPv3

Default-Wert:

SNMPv3

2.9.35.3 Security-Model

Legen Sie mit diesem Eintrag das Sicherheitsmodell fest.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

Any
SNMPv1
SNMPv2_C
SNMPv3_USM

Default-Wert:

SNMPv3_USM

2.9.35.4 Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

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

Default-Wert:

leer

2.9.35.5 Security-Level

Legen Sie die Sicherheitsstufe fest, die für den Erhalt der SNMP-Traps beim Empfänger gelten soll.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

NoAuthNoPriv

Die SNMP-Meldung ist ohne die Verwendung von speziellen Authentifizierungs-Verfahren gültig. Als Authentifizierung genügt die Zugehörigkeit zu einer SNMP-Community (bei SNMPv1 und SNMPv2c) bzw. die Angabe des Benutzernamens (bei SNMPv3). Die Übertragung der Daten erfolgt unverschlüsselt.

AuthNoPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt jedoch unverschlüsselt.

AuthPriv

Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Default-Wert:

NoAuthNoPriv

2.9.35.7 Status

Aktiviert oder deaktiviert diesen Eintrag.

Pfad Konsole:

Setup > **SNMP** > **Target-Params**

Mögliche Werte:

Active
Inactive

Default-Wert:

Active

2.9.37 Admitted-Protocols

Aktivieren Sie hier die SNMP-Versionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

SNMPv1
SNMPv2
SNMPv3

Default-Wert:

SNMPv3

2.9.38 Allow-Admins

Sollen registrierte Administratoren (darunter fällt auch der Benutzer root) auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

No
Yes

Default-Wert:

No

2.9.41 Operating

Dieser Eintrag aktiviert oder deaktiviert SNMP-Traps.

Pfad Konsole:

Setup > **SNMP**

Mögliche Werte:

No
SNMP-Traps sind ausgeschaltet.

Yes
SNMP-Traps sind eingeschaltet.

Default-Wert:

No

2.11 Config

Enthält die allgemeinen Konfigurationseinstellungen.

Pfad Konsole:

Setup

2.11.1 Comment-1

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.2 Comment-2

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.3 Comment-3

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.4 Comment-4

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.5 Comment-5

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.6 Comment-6

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.7 Comment-7

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.8 Comment-8

Kommentar zu diesem Gerät. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.9 Location

Standort des Gerätes. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.10 Administrator

Name des Geräte-Administrators. Wird nur zu Anzeigezwecken verwendet.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

Default-Wert:

leer

2.11.11 Config-Aging-Minutes

Hier können Sie angeben, nach wieviel Minuten der Inaktivität eine Konfigurations-Verbindung über TCP (z. B. SSH-Verbindung) automatisch beendet wird.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

15

2.11.18 LED-Mode

Bestimmen Sie die LED-Betriebsart.

Konsultieren Sie die Hardwareschnellübersicht des jeweiligen Gerätes für gerätespezifische Details zur LED-Signalisierung.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

On

Die LED(s) des Gerätes sind permanent in Betrieb und signalisieren den Betriebszustand.

Off

Die LED(s) des Gerätes werden nach dem Startvorgang sofort abgeschaltet.

Timed-Off

Die LED(s) des Gerätes werden nach einer konfigurierbaren Zeit (**LED-Off-Seconds**) abgeschaltet.

Default-Wert:

On

2.11.21 Admins

Legen Sie für Administratoren in dieser Tabelle an, die gegebenenfalls über eingeschränkte Rechte verfügen.

Der Administrator root hat immer alle Rechte.

Pfad Konsole:

Setup > **Config**

2.11.21.1 Administrator

Anmeldename des Administrators in dieser Zeile der Tabelle.

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

max. 16 Zeichen aus `[A-Z][a-z][0-9]-.`

2.11.21.3 Function-Rights

Aktivieren Sie hier die Funktionsrechte des Administrators in dieser Zeile der Tabelle.

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

Basic
Admin-Management

2.11.21.5 Rights

Die Rechte des Administrators in dieser Zeile der Tabelle.

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

None
Admin-RO-Limit
Admin-RW-Limit
Admin-RO
Admin-RW
Supervisor

2.11.21.6 Hashed-Password

Hashwert des Passworts des Administrators in dieser Zeile der Tabelle.

Pfad Konsole:

Setup > **Config** > **Admins**

Mögliche Werte:

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

2.11.90 LED-Off-Seconds

Legen Sie eine Zeit in Sekunden nach dem Gerätestart fest, nach der die LED(s) des Gerätes ausgeschaltet werden, wenn der **LED-Mode Timed-Off** eingestellt ist.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

300

2.11.91 LED-Test

Hiermit kann die LED des Gerätes getestet werden, die dann in der entsprechenden Farbe eingeschaltet wird.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

Off
Red
Green
Blue
All
No-Test

Default-Wert:

No-Test

2.11.99 Root-Hashed

Hashwert des Passworts des Administrators root.

Pfad Konsole:

Setup > **Config**

Mögliche Werte:

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

2.14 Time

Enthält die allgemeinen Konfigurationseinstellungen zur Zeiteinstellung.

Pfad Konsole:

Setup

2.14.15 Holidays

Konfigurieren Sie in dieser Tabelle die Feiertage, die z. B. in Zeitrahmen verwendet werden können.

Pfad Konsole:

Setup > **Time**

2.14.15.1 Date

Konfigurieren Sie in dieser Tabelle die Feiertage, die z. B. in Zeitrahmen verwendet werden können.

Pfad Konsole:

Setup > **Time** > **Holidays**

Mögliche Werte:

max. 10 Zeichen aus `mm/dd/yyyy`

Besondere Werte:

yyyy = 0

Steht für ein beliebiges Jahr.

2.14.16 Timeframes

Zeitrahmen werden verwendet, um einzelne SSIDs anhand eines Zeitplans ein- und auszuschalten. Zu einem Profil kann es auch mehrere Zeilen mit unterschiedlichen Zeitrahmen geben. Fügen Sie den Zeitrahmen bei den logischen WLAN-Einstellungen hinzu, damit er für die entsprechende SSID beachtet wird.

Pfad Konsole:

Setup > **Time**

2.14.16.1 Name

Hier muss der Name des Zeitrahmens angegeben werden, über den er in den logischen WLAN-Einstellungen referenziert wird.

Pfad Konsole:

Setup > **Zeit** > **Zeitrahmen**

Mögliche Werte:

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

Default-Wert:

leer

2.14.16.2 Start

Hier kann die Startzeit (Tageszeit) im Format HH:MM angegeben werden, ab der das gewählte Profil gelten soll.

Pfad Konsole:

Setup > **Time** > **Timeframes**

Mögliche Werte:

max. 5 Zeichen aus `hh:mm`

Default-Wert:

00:00

2.14.16.3 Stop

Hier kann die Endzeit (Tageszeit) im Format HH:MM angegeben werden, bis zu der das gewählte Profil gelten soll.

Eine Stoppzeit von HH:MM geht normalerweise bis HH:MM:00. Eine Ausnahme ist die Stoppzeit 00:00, die als 23:59:59 interpretiert wird.

Pfad Konsole:

Setup > **Time** > **Timeframes**

Mögliche Werte:

max. 5 Zeichen aus `hh:mm`

Default-Wert:

00:00

2.14.16.4 Weekdays

Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Pfad Konsole:

Setup > **Time** > **Timeframes**

Mögliche Werte:

None
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Holiday

Alle in der Tabelle *2.14.15 Holidays* auf Seite 33 definierten Tage.

2.14.20 Timezone

Konfigurieren Sie die korrekte Zeitzone, in der sich das Gerät befindet.

Pfad Konsole:

Setup > **Time**

Mögliche Werte:

UTC
Europe/Berlin
Europe/Vienna
Europe/Zurich
Europe/London
Europe/Prague
Europe/Warsaw
Europe/Zagreb
Europe/Copenhagen
Europe/Paris
Europe/Helsinki
Europe/Tallinn
Europe/Athens
Europe/Budapest
Europe/Dublin
Europe/Rome
Europe/Riga
Europe/Vilnius
Europe/Luxembourg
Europe/Malta
Europe/Amsterdam
Europe/Nicosia
Europe/Lisbon
Europe/Bucharest
Europe/Bratislava
Europe/Ljubljana
Europe/Madrid
Europe/Stockholm
Europe/Brussels
Europe/Sofia
US/Alaska
US/Pacific
US/Mountain
US/Central
US/Eastern
Pacific/Auckland
Pacific/Honolulu
Australia/Brisbane
Australia/Sydney
Australia/Perth
Australia/Darwin
Australia/Adelaide

Default-Wert:

UTC

2.14.21 NTP

Konfigurieren Sie in diesem Menü einen NTP-Server.

Pfad Konsole:

Setup > **Time**

2.14.21.1 Operating

Aktivieren Sie den konfigurierten NTP-Server.

Pfad Konsole:

Setup > **Time** > **NTP**

Mögliche Werte:

No

Keinen NTP-Server verwenden.

Yes

Der unter **Server** eingestellte NTP-Server wird verwendet, um das Datum und die Zeit zu stellen.

Default-Wert:

No

2.14.21.2 Server

Geben Sie hier die Adresse des zu verwendenden NTP-Servers an.

Pfad Konsole:

Setup > **Time** > **NTP**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

2.20 WLAN

Konfigurationseinstellungen der WLAN-Parameter.

Pfad Konsole:

Setup

2.20.1 Network

Konfigurieren Sie hier alle generellen Einstellungen rund um die auszustrahlenden WLAN-Netzwerke (SSIDs). Fügen Sie je WLAN-Netzwerk eine Zeile zur Tabelle hinzu. Standardmäßig ist die Tabelle leer.

Pfad Konsole:

Setup > **WLAN**

2.20.1.1 Network-Name

Konfigurieren Sie hier einen sprechenden Namen für das WLAN-Netzwerk. Dieser **interne** Name wird verwendet, um die Interface-Konfiguration in weiteren Teilen der Konfiguration zu referenzieren.

Es handelt sich hierbei **nicht** um den SSID-Namen, der z. B. auf den Clients angezeigt wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.20.1.2 SSID-Name

Konfigurieren Sie hier den nach außen sichtbaren SSID-Namen. Dieser Name wird auf den WLAN-Clients angezeigt, wenn nach WLAN-Netzwerken gesucht wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

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

2.20.1.4 Closed-Network

Konfigurieren Sie hier, ob die konfigurierte SSID während der Netzwerksuche durch Clients angezeigt werden soll.

Wenn der SSID-Broadcast unterdrückt wird, dann antwortet der Access Point nicht mehr auf Probe Requests mit leerer SSID. In diesem Fall muss für einen Verbindungsaufbau die SSID explizit am Client eingetragen und konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

SSID anzeigen.

Yes

SSID nicht anzeigen.

2.20.1.10 Max-Stations

Die Zahl gibt an, wieviele Clients gleichzeitig im WLAN-Netzwerk eingebucht sein können, bevor die Anfrage eines weiteren Clients abgewiesen wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

0 … 512

Besondere Werte:

0

Der Wert „0" bedeutet, dass es keine Begrenzung gibt, also unbegrenzt viele Clients gleichzeitig eingebucht sein können (bis zu einer eventuellen Hardware-spezifischen Grenze).

2.20.1.13 Inter-Station-Traffic

Je nach Anwendungsfall ist es gewünscht oder eben auch nicht erwünscht, dass die an einem Access Point angeschlossenen WLAN-Clients mit anderen Clients kommunizieren. Konfigurieren Sie hier, ob die Kommunikation der WLAN-Clients innerhalb des WLAN-Netzwerks erlaubt sein soll.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

Kommunikation der WLAN-Clients untereinander innerhalb des WLAN-Netzwerks ist nicht erlaubt.

Yes

Kommunikation der WLAN-Clients untereinander innerhalb des WLAN-Netzwerks erlaubt.

2.20.1.16 Min-Client-Strength

Konfigurieren Sie hier die minimale Signalstärke in Prozent, mit der ein Client vom Access Point „gesehen" werden muss, damit diesem die Anmeldung am WLAN-Netzwerk erlaubt wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

0 … 100

Besondere Werte:

0

Der Wert „0" bedeutet, dass keine minimale Signalstärke vorausgesetzt wird und Clients die Anmeldung immer erlaubt wird.

2.20.1.17 Exclude-From-Client-Management

Nimmt diese SSID gegebenenfalls vom Band Steering aus.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

No

Band Steering mit dieser SSID durchführen.

Yes

SSID vom Band Steering ausnehmen.

2.20.1.18 Timeframe

Geben Sie hier den Namen eines *Zeitrahmens* an, über den diese SSID zeitgesteuert an- bzw. abgeschaltet wird.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

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

Default-Wert:

leer

2.20.1.20 Summaric-Tx-Limit-Kbit/s

Hier können Sie eine WLAN Bandbreiten-Begrenzung einstellen, die für das gesamte WLAN-Netzwerk dient. Alle darin angemeldeten Clients können Daten insgesamt nur mit der hier konfigurierten Übertragungsrate empfangen. Die Angabe der Übertragungsrichtung versteht sich aus Sicht des Access Points, „Tx" bedeutet hier also die Übertragungsrate, mit der der Access Point Daten an den Client sendet. Diese Einstellung beeinflusst also die Download-Rate am Client.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

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

Besondere Werte:

0

Der Wert „0" bedeutet, dass keine Begrenzung aktiv ist.

2.20.1.21 Summaric-Rx-Limit-Kbit/s

Hier können Sie eine WLAN Bandbreiten-Begrenzung einstellen, die für das gesamte WLAN-Netzwerk dient. Alle darin angemeldeten Clients können Daten insgesamt nur mit der hier konfigurierten Übertragungsrate senden. Die Angabe

der Übertragungsrichtung versteht sich aus Sicht des Access Points, „Rx" bedeutet hier also die Übertragungsrate, mit der die Clients Daten an den Access Point senden. Diese Einstellung beeinflusst also die Upload-Rate am Client.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

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

Besondere Werte:

0

Der Wert „0" bedeutet, dass keine Begrenzung aktiv ist.

2.20.1.100 Key

Konfigurieren Sie hier den Pre-shared Key (PSK), der für das WLAN-Netzwerk verwendet wird.

Dieser Eintrag kommt nur dann zum Tragen, wenn ein Verschlüsselungsprofil ausgewählt wird, welches WPA(2)-PSK verwendet. Wird 802.1X verwendet, hat der Eintrag keine Auswirkung, das Feld kann dann leer gelassen werden.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

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

2.20.1.101 Radios

Konfigurieren Sie hier, auf welchen WLAN-Radios bzw. -Frequenzen die SSID ausgestrahlt werden soll.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

2.4GHz+5GHz

Die SSID wird auf den Frequenzen 2,4 GHz und 5 GHz ausgestrahlt.

2.4GHz

Die SSID wird nur auf der Frequenz 2,4 GHz ausgestrahlt.

5GHz

Die SSID wird nur auf der Frequenz 5 GHz ausgestrahlt.

none

Die SSID wird nicht ausgestrahlt. Dies kann als genereller Ein- / Aus-Schalter für die SSID verwendet werden.

2.20.1.102 Encryption-Profile

Konfigurieren Sie hier ein Verschlüsselungs-Profil aus den in **Setup** > **WLAN** > **Encryption** vorhandenen, welches definiert, welches Authentisierungs- und Verschlüsselungsverfahren für die SSID zum Tragen kommen soll.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.20.1.103 Idle-Timeout

Dies ist die Zeit in Sekunden, nach der ein Client getrennt wird, wenn der Access Point keine Pakete mehr von ihm empfangen hat. Jeglicher Datenverkehr des Clients setzt diesen Timeout wieder zurück.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

2.20.1.200 VLAN-ID

Mit dieser VLAN-ID werden Datenpakete, die aus dem WLAN an das LAN gerichtet sind, getaggt. Ebenso werden Pakete, die mit dieser VLAN-ID vom LAN kommen und an das WLAN gerichtet sind, wieder ent-taggt.

Diese Betriebsart entspricht dem normalerweise als „Access" bekannten Tagging-Modus, da davon ausgegangen wird, dass WLAN-Clients Daten normalerweise untagged übertragen. Der Tagging-Modus ist nicht anpassbar.

Pfad Konsole:

Setup > **WLAN** > **Network**

Mögliche Werte:

0 … 4095

Besondere Werte:

0

Der Standardwert 0 bedeutet, dass kein VLAN verwendet wird.

2.20.2 Country

Konfigurieren Sie hier, in welchem Land das Gerät betrieben wird. Abhängig davon werden automatisch die passenden regulatorischen Begrenzungen eingestellt.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Australia
Austria
Belgium
Bulgaria
Croatia
Cyprus
Czech-Republic
Denmark
Estonia
Finland
France
Germany
Greece
Hungary
Ireland
Italy
Latvia
Lithuania
Luxembourg
Malta
Netherlands
New-Zealand
Poland
Portugal
Romania
Slovakia
Slovenia
Spain
Sweden
Switzerland
United-Kingdom
United-States
Europe

2.20.3 Encryption

Konfigurieren Sie hier alle Einstellungen rund um die Verschlüsselung und Authentisierung der WLAN-Netzwerke. Standardmäßig sind bereits einige Verschlüsselungsprofile hinterlegt und können in der Konfiguration der WLAN-Netzwerke verwendet werden.

Pfad Konsole:

Setup > **WLAN**

2.20.3.1 Profile-Name

Wählen Sie hier einen sprechenden Namen für das Verschlüsselungsprofil. Dieser interne Name wird verwendet, um das Verschlüsselungsprofil in weiteren Teilen der Konfiguration zu referenzieren.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.3.2 Encryption

Konfigurieren Sie hier, ob das WLAN-Netzwerk verschlüsselt sein soll oder keine Verschlüsselung verwendet werden soll (Open Network).

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No

Keine Verschlüsselung verwenden.

Yes

Verschlüsselung verwenden.

2.20.3.4 Method

Konfigurieren Sie hier die Verschlüsselungsmethode.

Das Verfahren WEP bietet heutzutage keinerlei Vertraulichkeit mehr und sollte nur eingesetzt werden, um Legacy-Clients einzubinden, die kein neueres Sicherheitsverfahren unterstützen. In diesem Fall empfiehlt es sich, die WEP-Clients in einem eigenen VLAN vom Rest der WLAN-Infrastruktur zu isolieren.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

WEP-40-Bits

WEP mit Schlüssellänge 40 Bit

WEP-104-Bits

WEP mit Schlüssellänge 104 Bit

WEP-128-Bits

WEP mit Schlüssellänge 128 Bit

WEP-40-Bits-802.1X

WEP mit Schlüssellänge 40 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

WEP-104-Bits-802.1X

WEP mit Schlüssellänge 104 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

WEP-128-Bits-802.1X

WEP mit Schlüssellänge 128 Bit und 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

802.11i-WPA-PSK

WPA(2) mit Pre-Shared-Key

802.11i-WPA-802.1X

WPA(2) mit 802.1X

Beachten Sie, dass für das Funktionieren von 802.1X zusätzlich ein RADIUS-Serverprofil angegeben werden muss.

Enhanced-Open

Hotspots werden bisher hauptsächlich unverschlüsselt betrieben, wodurch auf der Funkschnittstelle keinerlei Vertraulichkeit der übertragenen Daten gegeben ist. Auch die verbreitete Praxis, einen Hotspot mit WPA2-PSK abzusichern und den gemeinsamen Schlüssel etwa durch einen Aushang bekannt zu machen, bietet nur eingeschränkte Sicherheit. Da WPA2-PSK keine Perfect Forward Secrecy bietet, kann ein Angreifer, dem dieser Schlüssel bekannt ist, nachträglich damit abgesicherten Datenverkehr entschlüsseln. Das Enhanced Open-Verfahren kann verwendet werden, um diese Risiken zu minimieren. Es bietet verschlüsselte Kommunikation für alle Clients, die dieses Verfahren unterstützen, so dass nicht jeder in der gleichen Funkzelle alles einfach mitlesen kann. Es bleibt das Risiko einer Man-in-the-Middle-Attacke, aber im Vergleich zu einem unverschlüsselten offenen Hotspot ist es ein deutlich geringeres Risiko. Es muss nur die Verschlüsselungsmethode eingestellt werden. Mehr ist nicht notwendig, um die Kommunikation mit Clients, welche dieses Verfahren unterstützen, zu verschlüsseln.

2.20.3.9 WPA-Version

Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden **802.11i-WPA-PSK** und **802.11i-WPA-802.1X** verwendet werden.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

WPA1

Die WPA-Version 1 wird exklusiv verwendet.

WPA2

Die WPA-Version 2 wird exklusiv verwendet.

WPA3

Die WPA-Version 3 wird exklusiv verwendet.

WPA1/2

Abhängig von den Fähigkeiten des Clients wird die WPA-Version 1 oder 2 verwendet.

WPA2/3

Abhängig von den Fähigkeiten des Clients wird die WPA-Version 2 oder 3 verwendet.

2.20.3.11 WPA-Rekeying-Cycle

Ein 48 Bit langer Initialization Vector (IV) erschwerte bei WEP die Berechnung des Schlüssels für Angreifer. WPA führte darüber hinaus die Verwendung eines neuen Schlüssels für jedes Datenpaket ein (Per-Packet Key Mixing und Re-Keying). Die Wiederholung des aus IV und WPA-Schlüssel bestehenden echten Schlüssels würde erst nach 16 Millionen Paketen erfolgen. In stark genutzten WLANs also erst nach einigen Stunden. Um die Wiederholung des echten Schlüssels zu verhindern, sieht WPA eine automatische Neuaushandlung des Schlüssels in regelmäßigen Abständen vor. Damit wird der Wiederholung des echten Schlüssels vorgegriffen.

Konfigurieren Sie hier die Zeit in Sekunden, nach der der Access Point bei Verwendung einer WPA-Version einen Austausch der verwendeten Schlüssel durchführt.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

max. 32 Zeichen aus `[0-9]`

Besondere Werte:

0

Der Wert „0" bedeutet, dass kein Wechsel der Schlüssel durchgeführt wird.

2.20.3.12 WPA1-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützung für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

TKIP

Die TKIP-Verschlüsselung wird verwendet.

AES

Die AES-Verschlüsselung wird verwendet.

TKIP/AES

Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

2.20.3.13 WPA2-3-Session-Keytypes

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 2 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützung für AES bieten.

Wenn ein WLAN-Netzwerk ausschließlich WEP oder WPA mit TKIP als Verschlüsselungsverfahren verwendet, erreichen die angebundenen WLAN-Clients eine maximale Brutto-Datenrate von 54 MBit/s.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

TKIP

Die TKIP-Verschlüsselung wird verwendet.

AES

Die AES-Verschlüsselung wird verwendet.

TKIP/AES

Abhängig von den Fähigkeiten des Clients wird das Verschlüsselungsverfahren TKIP oder AES verwendet.

2.20.3.14 Prot.-Mgmt-Frames

Die in einem WLAN übertragenen Management-Informationen zum Aufbau und Betrieb von Datenverbindungen sind standardmäßig unverschlüsselt. Jeder innerhalb einer WLAN-Zelle kann diese Informationen empfangen und auswerten, selbst wenn er nicht an einem Access Point angemeldet ist. Das birgt zwar keine Gefahren für eine verschlüsselte Datenverbindung, kann aber die Kommunikation innerhalb einer WLAN-Zelle durch gefälschte Management-Informationen empfindlich stören.

Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen (Protected Management Frames, PMF), so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Ab WPA3 müssen Management Frames verschlüsselt werden, daher wird dort dieser Wert ignoriert und als auf „Mandatory (Obligatorisch)“ gesetzt angenommen. Bei WPA2 ist diese Option optional.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No

PMF nicht verwenden.

optional

PMF anbieten. Der Client entscheidet, ob diese verwendet werden.

mandatory

PMF verwenden.

2.20.3.16 Pre-Authentication

Die schnelle Authentifizierung über den Pairwise Master Key (PMK) funktioniert nur, wenn der WLAN-Client sich bereits zuvor am AP angemeldet hat. Um die Dauer für die Anmeldung am AP schon beim ersten Anmeldeversuch zu verkürzen, nutzt der WLAN-Client die Prä-Authentifizierung.

Normalerweise scannt ein WLAN-Client im Hintergrund die Umgebung nach vorhandenen APs, um sich ggf. mit einem von ihnen neu verbinden zu können. APs, die WPA2/802.1X unterstützen, können ihre Fähigkeit zur Prä-Authentifizierung den anfragenden WLAN-Clients mitteilen. Eine WPA2-Prä-Authentifizierung unterschiedet sich dabei von einer normalen 802.1X-Authentifizierung in den folgenden Abläufen:

- Der WLAN-Client meldet sich am neuen AP über das Infrastruktur-Netzwerk an, das die APs miteinander verbindet. Das kann eine Ethernet-Verbindung, ein WDS-Link (Wireless Distribution System) oder eine Kombination beider Verbindungen sein.
- Ein abweichendes Ethernet-Protokoll (EtherType) unterscheidet eine Prä-Authentifizierung von einer normalen 802.1X-Authentifizierung. Damit behandeln der aktuelle AP sowie alle anderen Netzwerkpartner die Prä-Authentifizierung als normale Datenübertragung des WLAN-Clients.
- Nach erfolgreicher Prä-Authentifizierung speichern jeweils der neue AP und der WLAN-Client den ausgehandelten PMK.

  Die Verwendung von PMKs ist eine Voraussetzung für Prä-Authentifizierung. Andernfalls ist eine Prä-Authentifizierung nicht möglich.
- Sobald der Client sich später mit dem neuen AP verbinden möchte, kann er sich dank des gespeicherten PMKs schneller anmelden. Der weitere Ablauf entspricht dem PMK-Caching.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

No

Prä-Authentifizierung nicht durchführen.

Yes

Prä-Authentifizierung durchführen.

2.20.3.19 WPA2-Key-Management

Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

Standard

Aktiviert das Schlüsselmanagement gemäß dem Standard IEEE 802.11i ohne Fast Roaming und mit SHA-1-basierten Schlüsseln. Die WLAN-Clients müssen in diesem Fall je nach Konfiguration Opportunistic Key Caching, PMK Caching oder Pre-Authentifizierung verwenden.

Fast-Roaming

Aktiviert Fast Roaming gemäß dem Standard IEEE 802.11r.

Standard+Fast-Roaming

Kombination aus Standard und Fast Roaming

Obwohl eine Mehrfachauswahl möglich ist, sollten Sie diese nur vornehmen, wenn sichergestellt ist, dass sich nur entsprechend geeignete Clients am Access Point anmelden wollen. Ungeeignete Clients verweigern ggf. eine Verbindung, wenn eine andere Option als Standard aktiviert ist.

2.20.3.20 PMK-IAPP-Secret

Diese Passphrase wird verwendet, um verschlüsseltes Opportunistic Key Caching zu realisieren. Dies ist erforderlich, um Fast Roaming über IAPP zu verwenden. Dabei muss jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zugewiesen werden. Diese wird verwendet, um die Pairwise Master Keys (PMKs) zu verschlüsseln. Somit können Access Points mit übereinstimmender IAPP-Passphrase (PMK-IAPP-Secret) PMKs untereinander austauschen und unterbrechungsfreie Verbindungen sicherstellen. Stellen Sie daher sicher, dass diese Passphrase auf allen Access Points, zwischen denen mittels Fast Roaming geroamt werden soll, identisch ist.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.3.21 RADIUS-Server-Profile

Konfigurieren Sie hier das RADIUS-Serverprofil, welches bei der Verwendung von 802.1X zum Einsatz kommt. Bei der Verwendung von PSK-basierten Verschlüsselungsmethoden ist hier keine Eingabe erforderlich.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.3.26 SAE/OWE-Groups

Enthält die Auswahl der angebotenen Diffie-Hellman-Gruppen als Bitmaske, auf deren Basis die Protokollpartner einen Schlüssel für den Datenaustausch erstellen. Die vorhandenen Gruppen nutzen elliptische Kurven.

Das bei WPA3 verwendete Authentisierungsverfahrens SAE (Simultaneous Authentication of Equals) nutzt diese Verfahren zusammen mit AES zur Erzeugung eines kryptographisch starken Schlüssels.

Pfad Konsole:

Setup > **WLAN** > **Encryption**

Mögliche Werte:

DH-19

Bit 0x80000 (524288) – 256-bit random ECP group

DH-20

Bit 0x100000 (1048576) – 384-bit random ECP group

DH-21

Bit 0x200000 (2097152) – 521-bit random ECP group

Default-Wert:

DH-19

2.20.4 Client-Management

Konfigurieren Sie hier die Einstellungen zum Band Steering. Mittels Band Steering können Clients vom überlaufenen 2,4-GHz-Frequenzband auf das 5-GHz-Frequenzband gelenkt werden, sodass für den einzelnen Client mehr Bandbreite zur Verfügung steht und die Benutzererfahrung verbessert wird. LCOS LX bietet die Möglichkeit, Clients mittels des 802.11v-Standards auf das jeweils für sie optimale Frequenzband zu leiten. Auch Clients, die den 802.11v-Standard nicht unterstützen, können durch eine gezielte Verzögerung von Probe Responses oder gezielte Trennung vom WLAN auf das 5-GHz-Band geleitet werden.

Pfad Konsole:

Setup > **WLAN**

2.20.4.1 Active-Profile

Wählen Sie hier das Profil, welches die Einstellungen für das Band-Steering-Modul festlegt.

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

Mögliche Werte:

P-DEFAULT

Steering erfolgt anhand der Mediumsauslastung und der erkannten Intereferenz auf dem aktuellen Kanal und erfolgt bevorzugt mittels 802.11v. Unterstützt der Client kein 802.11v, wird das Steering mittels einer gezielten Disassoziierung des Clients durchgeführt. Das Steering erfolgt sowohl vor der Assoziierung, als auch, bei Bedarf, während der Client bereits assoziiert ist. Dies ist das empfohlene Profil.

P-LEGACY

Steering erfolgt vor der Assoziierung des Clients durch gezielte Zurückhaltung von Probe Responses. Es wird unabhängig von der Auslastung immer das 5-GHz-Band bevorzugt.

P-DISABLED

Es wird keinerlei Steering durchgeführt. Der Client entscheidet autark, welches Frequenzband er wählt.

<Custom>

Neben den vorgegebenen Profilen können Sie auch in **Profiles** selbst erstellte Profile einstellen.

Default-Wert:

P-DEFAULT

2.20.4.2 Profiles

Passen Sie hier die Detaileinstellungen der Steering-Profile an oder erstellen Sie ein neues Profil.

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

2.20.4.2.1 Profile-Name

Der Name des Profils.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.2.2 Operating

Steuert, ob das Band Steering für dieses Profil aktiv ist.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

No
Band Steering ist nicht aktiv.

Yes
Band Steering ist aktiv.

2.20.4.2.3 Steering-Min-PHY-Signal

Legt die Client-Signalstärke (in dB) fest, ab der ein Steering des Clients durchgeführt wird.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

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

2.20.4.2.4 Upgrade-TX-Rate-Threshold

Legt den Grenzwert der Übertragungsrate (in kBit/s) fest, bei dessen erreichen potentiell ein Steering des Clients auf das 5-GHz-Band erfolgen soll.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

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

2.20.4.2.5 Upgrade-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die mindestens erreicht sein muss, damit der Client für ein Steering auf das 5-GHz-Band in Betracht gezogen wird.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

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

2.20.4.2.6 Downgrade-TX-Rate-Threshold

Legt den Grenzwert der Übertragungsrate (in kBit/s) fest, bei dessen Erreichen potentiell ein Steering des Clients auf das 2,4-GHz-Band erfolgen soll.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

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

2.20.4.2.7 Downgrade-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die unterschritten sein muss, damit der Client für ein Steering auf das 2,4-GHz-Band in Betracht gezogen wird.

Für ein Steering auf 2,4 GHz (Downgrade) muss sowohl die hier konfigurierte Signalstärke unterschritten sein, als auch der Grenzwert aus **Downgrade-TX-Rate-Threshold** erreicht werden.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

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

2.20.4.2.8 2.4GHz-Sub-Profile

Konfigurieren Sie hier, welches 2,4-GHz-Unterprofil zur Anwendung kommt.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.2.9 5GHz-Sub-Profile

Konfigurieren Sie hier, welches 5-GHz-Unterprofil zur Anwendung kommt.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.3 2.4GHz-Sub-Profiles

Konfigurieren Sie hier die Einstellungen der 2,4-GHz-Unterprofile.

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

2.20.4.3.1 Profile-Name

Der Profilname des 2,4-GHz-Unterprofils.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.20.4.3.2 Utilization-Check-Interval

Konfiguriert das Intervall (in Sekunden), in dem die Mediumsauslastung geprüft wird.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

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

2.20.4.3.3 Utilization-Average-Period

Konfiguriert den Zeitraum (in Sekunden), über den die Mediumsauslastung gemittelt wird. Dieser Wert muss immer über dem für das Auslastung-Prüfintervall konfiguriertem Wert liegen.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

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

2.20.4.3.4 Utilization-Overload-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), ab welcher der aktuelle 2,4-GHz-Kanal als ausgelastet angenommen wird.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

2.20.4.3.5 Utilization-Deviation-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

2.20.4.3.6 Interference-Detection

Konfiguriert, ob Interferenzen auf dem konfigurierten 2,4-GHz-Kanal für die Entscheidung zum Steering herangezogen werden.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

No

Interferenzen nicht berücksichtigen.

Yes

Interferenzen berücksichtigen.

2.20.4.3.7 Delay-Probe-PHY-Signal-Threshold

Legt die Client-Signalstärke (in dB) fest, die erreicht sein muss, damit Probe Responses an den Client zum Zwecke des Steerings zurückgehalten werden.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

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

2.20.4.3.8 Delay-Probe-Time-Window

Konfiguriert das Zeitfenster (in Sekunden), in dem von einem Client mindestens so viele Probe Requests empfangen werden müssen, wie es unter **Delay-Probe-Min-Request-Count** konfiguriert wurde, damit diese beantwortet werden.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

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

2.20.4.3.9 Delay-Probe-Min-Request-Count

Konfiguriert die Anzahl an Probe Requests, die von einem Client im unter **Delay-Probe-Time-Window** konfigurierten Zeitraum empfangen werden müssen, damit diese beantwortet werden.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **2.4GHz-Sub-Profiles**

Mögliche Werte:

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

2.20.4.4 5GHz-Sub-Profiles

Konfigurieren Sie hier die Einstellungen der 5-GHz-Unterprofile.

Pfad Konsole:

Setup > **WLAN** > **Client-Management**

2.20.4.4.1 Profile-Name

Der Profilname des 5-GHz-Unterprofils.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

max. 128 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.``

2.20.4.4.2 Utilization-Check-Interval

Konfiguriert das Intervall (in Sekunden), in dem die Mediumsauslastung geprüft wird.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

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

2.20.4.4.3 Utilization-Average-Period

Konfiguriert den Zeitraum (in Sekunden), über den die Mediumsauslastung gemittelt wird. Dieser Wert muss immer über dem für das Auslastung-Prüfintervall konfiguriertem Wert liegen.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

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

2.20.4.4.4 Utilization-Overload-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), ab welcher der aktuelle 5-GHz-Kanal als ausgelastet angenommen wird.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

2.20.4.4.5 Utilization-Deviation-Threshold

Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

0 … 100

2.20.4.4.6 Interference-Detection

Konfiguriert, ob Interferenzen auf dem konfigurierten 5-GHz-Kanal für die Entscheidung zum Steering herangezogen werden.

Pfad Konsole:

Setup > **WLAN** > **Client-Management** > **5GHz-Sub-Profiles**

Mögliche Werte:

No

Interferenzen nicht berücksichtigen.

Yes

Interferenzen berücksichtigen.

2.20.8 Radio-Settings

Konfigurieren Sie hier alle Einstellungen rund um die physikalischen Radio-Parameter. Standardmäßig ist für jedes physikalisch vorhandene WLAN-Radio ein Eintrag in der Tabelle enthalten, der bei Bedarf modifiziert werden kann.

Pfad Konsole:

Setup > **WLAN**

2.20.8.1 Ifc

Der interne Name des WLAN-Radios. Dieser kann nicht verändert werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

2.20.8.3 5GHz-Mode

Konfigurieren Sie hier, in welchem Modus das 5-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt. Folgende Modi stehen zur Auswahl:

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

11an-mixed

Es werden die Modi 802.11a und 802.11n verwendet.

11anac-mixed

Es werden die Modi 802.11a, 802.11n und 802.11ac verwendet.

11nac-mixed

Es werden die Modi 802.11n und 802.11ac verwendet.

11ac-only

Es wird nur der Modus 802.11ac verwendet.

11anacax-mixed

Es werden die Modi 802.11a, 802.11n, 802.11ac und 802.11ax (Wi-Fi 6) verwendet.

Auto

Es werden alle vom Gerät unterstützten Modi verwendet.

2.20.8.6 Radio-Band

Konfigurieren Sie hier, ob dieses Radio-Modul im 2,4-GHz- oder 5-GHz-Spektrum arbeitet.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

2.4GHz

Das Radio-Modul arbeitet im 2,4-GHz-Spektrum.

5GHz

Das Radio-Modul arbeitet im 5-GHz-Spektrum.

2.20.8.7 Sub-Band

Konfigurieren Sie hier, welche Sub-Bänder im 5-GHz-Modus verwendet werden.

Die WLAN-Kanäle 120, 124 und 128 werden nicht verwendet, da diese Kanäle durch den Primärnutzer RADAR verwendet werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

Band-1

Es wird nur das Sub-Band 1 verwendet. Dies entspricht den WLAN-Kanälen 36, 40, 44, 48, 52, 56, 60 und 64.

Band-2

Es wird nur das Sub-Band 2 verwendet. Dies entspricht den WLAN-Kanälen 100, 104, 108, 112, 116, 132, 136 und 140.

Band-1+2

Es werden die Sub-Bänder 1 und 2 verwendet.

2.20.8.8 Channel

Konfigurieren Sie hier den Kanal, auf dem das WLAN-Radio arbeiten soll.

Im 5-GHz-Betrieb stellt der hier eingestellte Kanal einen bevorzugten Kanal dar. Da im 5-GHz-Band Dynamic Frequency Selection (DFS) vorgeschrieben ist, kann die Verwendung des bevorzugten Kanals allerdings nicht garantiert werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

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

Besondere Werte:

0

Der Wert „0" bewirkt die automatische Auswahl eines geeigneten Kanals.

2.20.8.9 2.4GHz-Mode

Konfigurieren Sie hier, in welchem Modus das 2,4-GHz-Radio betrieben werden soll. Dies wirkt sich direkt auf die möglichen Datenraten aus. Bei einer hier vorgenommenen Einschränkung wird beim Einbuchungsvorgang eines Clients geprüft, ob die vom Client verwendeten Modi mit den hier konfigurierten übereinstimmen und abhängig davon die Einbuchung erlaubt oder abgelehnt.

Für eine größtmögliche Kompatibilität und Leistungsfähigkeit sollte der Modus **Auto** gewählt werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

11bg-mixed

Es werden die Modi 802.11b und 802.11g verwendet.

11g-only

Es wird nur der Modus 802.11g verwendet.

11bgn-mixed

Es werden die Modi 802.11b, 802.11g und 802.11n verwendet.

11gn-mixed

Es werden die Modi 802.11g und 802.11n verwendet.

11bgnax-mixed

Es werden die Modi 802.11b, 802.11g, 802.11n und 802.11ax (Wi-Fi 6) verwendet.

11gnax-mixed

Es werden die Modi 802.11g, 802.11n und 802.11ax (Wi-Fi 6) verwendet.

Auto

Es werden alle vom Gerät unterstützten Modi verwendet.

2.20.8.13 Channel-List

Konfigurieren Sie hier eine kommaseparierte Liste von weiteren WLAN-Kanälen. Im Rahmen der automatischen Kanalwahl wird ein Kanal aus dieser Liste ausgewählt, anstatt aus allen unterstützten WLAN-Kanälen.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.20.8.24 Max.-Channel-Bandwidth

Konfigurieren Sie hier die maximal erlaubte Kanalbandbreite.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

20MHz

Die Kanalbandbreite beträgt immer 20 MHz.

40MHz

Abhängig von der Umgebung beträgt die Kanalbandbreite bis zu 40 MHz, kann aber auch auf 20 MHz zurückfallen.

80MHz

Abhängig von der Umgebung beträgt die Kanalbandbreite bis zu 80 MHz, kann aber auch auf 40 MHz oder 20 MHz zurückfallen.

160MHz

Abhängig von der Umgebung beträgt die Kanalbandbreite bis zu 160 MHz, kann aber auch auf 80 MHz, 40 MHz oder 20 MHz zurückfallen.

Auto

Für ein 2,4-GHz-Radio wird immer die Kanalbandbreite 20 MHz verwendet. Für ein 5-GHz-Radio wird immer die anhand der Umgebung maximal mögliche Kanalbandbreite (bis zu 160 MHz) verwendet.

2.20.8.29 Exclude-DFS-Channels

Konfigurieren Sie hier, ob im 5-GHz-Band Kanäle verwendet werden sollen, für die Dynamic Frequency Selection (DFS) vorgeschrieben ist.

Werden diese Kanäle hierüber ausgeschlossen, stehen im 5-GHz-Band noch die Kanäle 36, 40, 44 und 48 zur Verfügung. Da für diese kein DFS vorgeschrieben ist, können diese Kanäle bei aktivierter Option **Exclude-DFS-Channels** im Radio-Channel und in der **Channel-List** fest konfiguriert werden.

Pfad Konsole:

Setup > **WLAN** > **Radio-Settings**

Mögliche Werte:

No

Für DFS reservierte Kanäle verwenden.

Yes

Für DFS reservierte Kanäle nicht verwenden.

2.20.9 Automatic-Environment-Scan-Enabled

Dieser Eintrag wird durch die LANCOM Management Cloud gesetzt, welche diesen Umgebungsscan benötigt. Die Ergebnisse sind nur durch die LANCOM Management Cloud lesbar.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Yes

Automatischer Umgebungsscan wird durchgeführt.

No

Automatischer Umgebungsscan wird nicht durchgeführt.

2.20.10 Automatic-Environment-Scan-Time-Begin

Startzeit für das Zeitfenster, in dem der automaische Umgebungsscan durchgeführt wird.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Uhrzeit im Format `hh:mm`

2.20.11 Automatic-Environment-Scan-Time-End

Stoppzeit für das Zeitfenster, in dem der automaische Umgebungsscan durchgeführt wird.

Pfad Konsole:

Setup > **WLAN**

Mögliche Werte:

Uhrzeit im Format `hh:mm`

2.20.133 LEPS

Mit LANCOM Enhanced Passphrase Security (LEPS) können Sie WLAN-Stationen benutzerdefinierte Passphrasen zuweisen, ohne die Stationen vorher anhand ihrer MAC-Adresse erfassen zu müssen. Alternativ lässt sich auch ein MAC-Adress-Filter realisieren.

Pfad Konsole:

Setup > **WLAN**

2.20.133.1 Operating

Schaltet LEPS ein oder aus. Im ausgeschalteten Zustand werden die angelegten LEPS-Benutzer bei der Anmeldung von WLAN-Clients nicht beachtet.

Pfad Konsole:

Setup > **WLAN** > **LEPS**

Mögliche Werte:

No
yes

Default-Wert:

No

2.20.133.2 Profiles

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden. Dabei können Sie für einen Benutzer die Profilwerte durch individuelle Werte überschreiben.

Pfad Konsole:

Setup > **WLAN** > **LEPS**

2.20.133.2.1 Name

Vergeben Sie hier einen eindeutigen Namen für das LEPS-Profil.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Profiles**

Mögliche Werte:

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

2.20.133.2.2 Network-Name

Wählen Sie hier die SSID bzw. beim WLC das logische WLAN-Netzwerk aus, für die das LEPS-Profil gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID bzw. beim WLC an dem logischen WLAN-Netzwerk anmelden, mit der sie über das LEPS-Profil verbunden sind.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Profiles**

Mögliche Werte:

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

2.20.133.2.3 Mac-List

Hier können Sie angeben, ob und wie die MAC-Adressen überprüft werden sollen.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Profiles**

Mögliche Werte:

Disabled

Die MAC-Adresse wird für die LEPS-Anmeldung nicht beachtet. Eine ggf. gesetzte benutzerspezifische Passphrase wird hingegen geprüft.

Whitelist

Nur die Clients werden zugelassen, deren MAC-Adresse bekannt ist.

Blacklist

Nur die Clients werden zugelassen, deren MAC-Adresse nicht bekannt ist.

2.20.133.2.5 VLAN

Hier können Sie festlegen, welchem VLAN ein LEPS-Benutzer, der mit diesem Profil verbunden ist, zugewiesen wird.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Profiles**

Mögliche Werte:

0 … 4095

2.20.133.3 Users

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden.

Pfad Konsole:

Setup > **WLAN** > **LEPS**

2.20.133.3.1 Name

Vergeben Sie hier einen eindeutigen Namen für den LEPS-Benutzer.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Users**

Mögliche Werte:

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

2.20.133.3.2 Profile

Wählen Sie hier das Profil aus, für das der LEPS-Benutzer gültig sein soll. Es können sich nur LEPS-Benutzer an der SSID anmelden, mit der sie über das LEPS-Profil verbunden sind.

Pfad Konsole:

Setup > **WLAN** > **LEPS-U** > **Users**

Mögliche Werte:

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

2.20.133.3.3 WPA-Passphrase

Vergeben Sie hier die Passphrase, mit der der LEPS-Benutzer sich am WLAN anmelden soll.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Users**

Mögliche Werte:

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

2.20.133.3.4 VLAN

Hier können Sie festlegen, welchem VLAN der LEPS-Benutzer zugewiesen wird. Wird hier kein VLAN konfiguriert, gilt eine eventuelle, im LEPS-Profil konfigurierte VLAN. Wird sowohl im LEPS-Profil als auch am LEPS-Benutzer ein VLAN konfiguriert, gilt die am LEPS-Benutzer konfigurierte VLAN-ID.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Users**

Mögliche Werte:

0 … 4095

2.20.133.3.7 MAC-Address

Optionale Angabe einer MAC-Adresse für einen MAC-Filter. Abhängig von der Einstellung im Profil wird dieser Eintrag nicht beachtet oder es können sich dann nur die in dieser Tabelle aufgeführten Clientgeräte anmelden (Whitelist). Mittels Blacklist funktioniert der MAC-Filter genau anders herum – die angegebenen MAC-Adressen können sich nicht anmelden.

Pfad Konsole:

Setup > **WLAN** > **LEPS** > **Users**

Mögliche Werte:

MAC-Adresse im Format `xx:xx:xx:xx:xx:xx`

2.30 RADIUS

Konfigurationseinstellungen der Parameter für RADIUS und IEEE 802.1X.

Pfad Konsole:

Setup

2.30.3 RADIUS-Server

Konfigurieren Sie hier die Einstellungen für RADIUS-Server-Profile zur Verwendung mit WLAN-Netzwerken, die 802.1X als Authentisierungsverfahren verwenden.

Pfad Konsole:

Setup > **RADIUS**

2.30.3.1 Name

Wählen Sie hier einen sprechenden Namen für das RADIUS-Server-Profil. Dieser interne Name wird verwendet, um das RADIUS-Server-Profil in weiteren Teilen der Konfiguration zu referenzieren.

Pfad Konsole:

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

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.30.3.3 Port

Wählen Sie hier den (UDP)-Port, der verwendet wird, um den RADIUS-Server zu kontaktieren.

Normalerweise ist dies der Port 1812 (RADIUS Authentication).

Pfad Konsole:

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

Mögliche Werte:

0 … 65535

2.30.3.4 Secret

Konfigurieren Sie hier das Secret, mit welchem der Datenverkehr zwischen dem Gerät und dem RADIUS-Server verschlüsselt wird. Dieses Secret muss ebenfalls auf dem RADIUS-Server hinterlegt sein.

Pfad Konsole:

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

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.30.3.5 Backup

Konfigurieren Sie hier ein Backup-Profil, welches verwendet wird, wenn der RADIUS-Server im hier konfigurierten Profil nicht erreichbar ist.

Pfad Konsole:

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

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

2.30.3.8 Server-IP-Address

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Server erreichbar ist.

Pfad Konsole:

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

Mögliche Werte:

max. 64 Zeichen aus `IPv4- oder IPv6-Adresse`

2.30.3.9 Accounting-Port

Wählen Sie hier den Port (UDP), der verwendet wird, um den RADIUS-Accounting-Server zu kontaktieren.

Normalerweise ist dies der Port 1813 (RADIUS Accounting).

Pfad Konsole:

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

Mögliche Werte:

0 … 65535

2.30.3.14 Accounting-IP-Address

Konfigurieren Sie hier den Hostnamen oder die IP-Adresse, unter der der RADIUS-Accounting-Server erreichbar ist.

Pfad Konsole:

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

Mögliche Werte:

max. 64 Zeichen aus `IPv4- oder IPv6-Adresse`

2.30.3.15 MAC-Check

Statt einen Benutzernamen über den RADIUS-Server zu authentifizieren, kann dies auch mit einer MAC-Adresse geschehen.

Pfad Konsole:

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

Mögliche Werte:

No

Keine Überprüfung anhand der MAC-Adresse.

Yes

Die Berechtigungen der Clients am RADIUS-Server über die MAC-Adresse überprüfen.

2.30.11 Supplicant-Ifc-Setup

Hier finden Sie die Einstellungen für die 802.1X-Supplicant-Funktionalität, um das Gerät LAN-seitig an einer mit 802.1X gesicherten Switch-Infrastruktur zu authentifizieren.

Pfad Konsole:

Setup > **RADIUS**

2.30.11.1 Interface-Name

Der Name der LAN-Schnittstelle. Aktuell gibt es nur die Schnittstelle INTRANET, daher kann diese nicht geändert werden.

Pfad Konsole:

Setup > **RADIUS** > **Supplicant-Ifc-Setup**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET`

2.30.11.2 Method

Die zur Anmeldung an der 802.1X-Infrastruktur zu verwendende EAP-Methode.

Pfad Konsole:

Setup > **RADIUS** > **Supplicant-Ifc-Setup**

Mögliche Werte:

none
MD5
TTLS/MD5
TTLS/PAP
TTLS/CHAP
TTLS/MSCHAPv2
TTLS/MSCHAP
PEAP/GTC
PEAP/MSCHAPv2

2.30.11.3 Username

Der zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Benutzername.

Pfad Konsole:

Setup > **RADIUS** > **Supplicant-Ifc-Setup**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.30.11.4 Password

Das zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Passwort.

Pfad Konsole:

Setup > **RADIUS** > **Supplicant-Ifc-Setup**

Mögliche Werte:

max. 64 Zeichen aus `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.59 WLAN-Management

LCOS LX-basierte Access Points können von einem LANCOM WLAN-Controller (WLC) verwaltet werden. Wie bei LCOS-basierten Access Points kommt hierzu das Protokoll CAPWAP zum Einsatz.

Voraussetzung ist ein LANCOM WLAN-Controller mit LCOS-Version 10.40 oder höher.

Im Auslieferungszustand suchen LCOS LX-basierte Access Points im lokalen Netzwerk nach einem WLAN-Controller. Ebenso wird unter dem DNS-Namen „WLC-Address“ versucht, einen WLAN-Controller zu erreichen.

Wurde der Access Point in die Verwaltung durch einen WLC aufgenommen, wird dieser Access Point nicht weiter versuchen, die LANCOM Management Cloud zu kontaktieren.

Auf diese Weise ist eine Zero-Touch-Inbetriebnahme möglich, bei der keine weitere Konfiguration des Access Points notwendig ist. In besonderen Fällen kann es dennoch erforderlich sein, eine manuelle Konfiguration vorzunehmen. Dies ist in der Gerätekonfiguration hier möglich.

Pfad Konsole:

Setup

2.59.1 Static-WLC-Configuration

Konfiguriert benutzerdefinierte WLAN-Controller. Dies kann notwendig sein, wenn ein WLC nicht über das lokale Netzwerk (z. B. bei gerouteten Verbindungen) gefunden wird und auch der DNS-Name „WLC-Address“ nicht verwendet werden kann, um dem Access Point die Adresse des WLCs mitzuteilen.

Pfad Konsole:

Setup > **WLAN-Management**

2.59.1.1 IP-Address

Geben Sie die IP-Adresse oder den DNS-Namen eines WLAN-Controllers an.

Pfad Konsole:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Mögliche Werte:

max. 44 Zeichen aus `[A-Za-z0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]"^_.`

2.59.1.2 Port

Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen.

Pfad Konsole:

Setup > **WLAN-Management** > **Static-WLC-Configuration**

Mögliche Werte:

0 … 65535

Default-Wert:

1027

2.59.2 Operating

Konfiguriert, ob ein Access Point aktiv nach einem WLC sucht und von diesem verwaltet werden kann.

Für den Stand-Alone-Betrieb empfiehlt es sich, diese Option abzuschalten.

Pfad Konsole:

Setup > **WLAN-Management**

Mögliche Werte:

No

Die Suche nach einem WLC ist ausgeschaltet.

Yes

Es wird aktiv nach einem WLC gesucht.

Default-Wert:

Yes

2.59.3 Update-Cert-Before

Konfiguriert, wie viele Tage vor dem Ablaufdatum das Gerätezertifikat erneuert wird, mit dem sich der Access Point am WLC authentifiziert.

Pfad Konsole:

Setup > **WLAN-Management**

Mögliche Werte:

max. 4 Zeichen aus `[0-9]`

Default-Wert:

30

2.59.4 Capwap-Port

Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen. Der Standardwert von 1027 ist der Standardport des CAPWAP-Protokolls. LANCOM WLCs verwenden standardmäßig ebenfalls diesen Port.

Pfad Konsole:

Setup > **WLAN-Management**

Mögliche Werte:

0 … 65535

Default-Wert:

1027

2.70 IP-Configuration

Parameter für die IP-Konfiguration des Gerätes.

Pfad Konsole:

Setup

2.70.4 Static-Parameters

Einstellungen rund um die IP- und Netzwerkkonfiguration, die zum Tragen kommen, wenn Sie statische IP-Adressen verwenden möchten.

Sämtliche in dieser Tabelle vorgenommenen Einstellungen kommen nur zum Tragen, wenn Sie für das entsprechende LAN-Interface die IPv4- oder IPv6-Adressquelle **static** gewählt haben. Ansonsten werden alle notwendigen Informationen z. B. via DHCP bezogen, sodass in dieser Tabelle keinerlei Konfiguration notwendig ist.

Pfad Konsole:

Setup > **IP-Configuration**

2.70.4.1 Interface-Name

Tragen Sie hier den Namen des Interface ein, auf das sich die weiteren hier vorgenommenen Einstellungen beziehen sollen.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET`

2.70.4.2 IPv4-Gateway

Konfigurieren Sie hier das IPv4-Gateway für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.70.4.3 IPv6-Gateway

Konfigurieren Sie hier das IPv6-Gateway für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

2.70.4.4 Primary-IPv4-DNS

Konfigurieren Sie hier den primären IPv4-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.70.4.5 Secondary-IPv4-DNS

Konfigurieren Sie hier den sekundären IPv4-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 16 Zeichen aus `IPv4-Adresse: a.b.c.d`

2.70.4.6 Primary-IPv6-DNS

Konfigurieren Sie hier den primären IPv6-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

2.70.4.7 Secondary-IPv6-DNS

Konfigurieren Sie hier den sekundären IPv6-DNS-Server für das referenzierte Interface.

Pfad Konsole:

Setup > **IP-Configuration** > **Static-Parameters**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d`

2.70.6 LAN-Interfaces

Legen Sie hier grundsätzliche Konfigurationsoptionen rund um die eigenen IP-Einstellungen und den Netzwerkzugriff des Gerätes fest.

Pfad Konsole:

Setup > **IP-Configuration**

2.70.6.1 Interface-Name

Vergeben Sie hier einen sprechenden Namen für das Interface. Dieser Name wird verwendet, um die Interface-Konfiguration in weiteren Teilen der Konfiguration zu referenzieren.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

max. 64 Zeichen aus `INTRANET`

2.70.6.2 Interface-ID

Der interne Bezeichner für das Interface. Dieser kann nicht geändert werden.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

2.70.6.3 VLAN-ID

Legen Sie hier eine VLAN-ID fest, für die das Interface aktiv und erreichbar sein soll.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

0 … 4095

Besondere Werte:

0

Der Standardwert 0 bedeutet, dass kein VLAN verwendet wird.

2.70.6.4 IPv4-Address-Source

Wählen Sie hier, woher die IPv4-Adresse des Interface bezogen werden soll.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

DHCP

Die IP-Adresse wird via DHCP bezogen.

static

Es wird die statisch konfigurierte IP-Adresse für das Interface verwendet.

2.70.6.5 IPv6-Address-Source

Wählen Sie hier, woher die IPv6-Adresse des Interface bezogen werden soll.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

Router-Advertisement

Die IPv6-Adresse wird aus Router-Advertisements abgeleitet, die vom Gerät auf dem jeweiligen Interface empfangen werden.

Ist im Router-Advertisement das Other- und / oder Managed-Flag gesetzt, werden zusätzliche Konfigurationsoptionen via DHCPv6 bezogen – auch, wenn als Adressquelle **Router-Advertisement** eingestellt ist.

DHCPv6

Die IPv6-Adresse wird per DHCPv6 bezogen.

static

Es wird die statisch konfigurierte IPv6-Adresse für das Interface verwendet.

2.70.6.6 Static-IPv4-Address

Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als **IPv4-Address-Source static** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/24“).

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

max. 19 Zeichen aus `IPv4-Adresse: a.b.c.d/xx`

2.70.6.7 Static-IPv6-Address

Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als **IPv6-Address-Source static** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/64“).

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

max. 44 Zeichen aus `IPv6-Adresse: a:b:c::d/64`

2.70.6.9 Comment

Legen Sie hier einen beliebigen Kommentar zur Interface-Konfiguration ab.

Pfad Konsole:

Setup > **IP-Configuration** > **LAN-Interfaces**

Mögliche Werte:

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

2.102 LMC

Einstellungen für die Konfiguration und das Monitoring Ihres Gerätes durch die LANCOM Management Cloud (LMC).

Pfad Konsole:

Setup

2.102.1 Operating

Legen Sie fest, ob das Gerät über die LMC verwaltet werden soll.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

No

Das Gerät stellt keine Verbindung zur LMC her.

Yes

Das Gerät wird von der LMC verwaltet.

Default-Wert:

Yes

2.102.7 Delete-Certificate

Mit dieser Aktion löschen Sie das LMC-Zertifikat.

Pfad Konsole:

Setup > **LMC**

Mögliche Argumente:

keine

2.102.8 DHCP-Client-Auto-Renew

Mit diesem Parameter legen Sie das Verhalten des Gerätes fest, wenn sich die DHCP-Einstellungen des Netzes ändern und der LMC-Client keine Verbindung zur LMC aufbauen kann.

Kann der LMC-Client die konfigurierte LMC nicht erreichen, hat sich wahrscheinlich der IP-Adressbereich des Netzes geändert. Geräte, die als DHCP-Client konfiguriert sind, behalten jedoch die zuvor zugewiesene IP-Adresse, bis deren DHCP-Lease-Time abgelaufen ist. Durch Aktivieren dieses Parameters fordert das Gerät unabhängig von der verbleibenden DHCP-Lease-Time die DHCP-Adresse erneut an (DHCP-Renew).

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

No

Wenn der LMC-Client die Verbindung zur LMC verliert, löst dies keinen DHCP-Renew aus.

Yes

Wenn der LMC-Client die Verbindung zur LMC verliert, löst dies einen DHCP-Renew aus. Ist das DHCP-Renew nicht erfolgreich, wird der DHCP-Prozess komplett neu angestoßen. Das Gerät versucht dann, eine IP-Adresse von einem beliebigen DHCP-Server zu erhalten, um die Verbindung zur LMC wiederherzustellen.

Default-Wert:

No

2.102.13 Configuration-Via-DHCP

Legen Sie fest, ob die LMC-Domain von einem DHCP-Server bezogen werden soll.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

No

Die LMC-Domain wird nicht von einem DHCP-Server bezogen. Es wird der im Feld **LMC-Domain** konfigurierte Wert genommen.

Yes

Die LMC-Domain wird von einem DHCP-Server bezogen.

Um die LMC-Domain von einem DHCP-Server bereitzustellen, konfigurieren Sie am DHCP-Server innerhalb der DHCP-Option 43 die Sub-Option 18 mit der LMC-Domain. Weitere Informationen zur Konfiguration der LMC Parameter finden Sie im LCOS-Referenzhandbuch im Abschnitt „Auslieferung der LMC-Domain durch den LCOS-DHCP-Server“.

Default-Wert:

No

2.102.15 LMC-Domain

Geben Sie hier den Domain-Namen der LMC an. Standardmäßig ist die Domain für den ersten Verbindungsaufbau mit der Public LMC eingetragen. Möchten Sie Ihr Gerät von einer eigenen Management Cloud verwalten lassen („Private Cloud" oder „on premise installation"), tragen Sie bitte die entsprechende LMC-Domain ein.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

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

2.102.16 Rollout-Project-ID

Geben Sie hier die Projekt-ID dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

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

2.102.17 Rollout-Location-ID

Geben Sie hier den Standort dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

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

2.102.18 Rollout-Device-Role

Geben Sie hier die Rolle dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

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

2.102.200 Pairing-Token

Geben Sie hier den Aktivierungscode an, den Sie zum Koppeln mit der LMC erzeugt haben.

Pfad Konsole:

Setup > **LMC**

Mögliche Werte:

max. 36 Zeichen aus `^[1-9A-NP-Z-]{24,47}$|^$|^\*$|^-$`

2.107 Automatic-Firmware-Update

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff (unattended). LANCOM Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Sie wählen, ob Sie Security Updates, Release Updates oder alle Updates automatisch installieren möchten. Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden.

Der LANCOM Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den LANCOM Update-Server. Die Kontaktaufnahme erfolgt via HTTPS. Bei der Kontaktaufnahme wird der Server mittels der im LANCOM Gerät bereits hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle LANCOM Geräte signiert. Der LANCOM Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

Pfad Konsole:

Setup

2.107.1 Mode

Stellen Sie hier den Betriebsmodus des LANCOM Auto Updaters ein.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

manual

Der Auto Updater prüft nur nach Aufforderung durch den Benutzer auf neue Updates.

Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

check

Der Auto Updater prüft regelmäßig beim LANCOM Update-Server auf neue Updates. Die Verfügbarkeit eines neuen Updates wird dem Benutzer im LCOS LX-Menübaum und via Syslog signalisiert. Der Benutzer hat die Gelegenheit, manuell – aber über den Auto Updater gesteuert – auf das neueste verfügbare Update zu aktualisieren.

check-and-update

Der Auto Updater prüft regelmäßig beim LANCOM Update-Server auf neue Updates. Der Update-Server ermittelt anhand der Versions-Policy das passende Update, bestimmt den Zeitpunkt für Download und Installation des Update innerhalb des vom Benutzer konfigurierten Zeitfensters und übermittelt dies an den Auto Updater. Die Installation der Firmware erfolgt im Testmodus. Nach der Installation führt der Auto Updater eine Verbindungsprüfung durch. Hierbei wird geprüft, ob weiterhin eine Verbindung zum Update-Server aufgebaut werden kann, der Internetzugang also weiterhin gewährleistet ist. Konnte der Update-Server erfolgreich kontaktiert werden, wird der Testmodus beendet, die Firmware ist nun regulär aktiv. Konnte der Updateserver nicht kontaktiert werden, muss davon ausgegangen werden, dass der Internetzugang nicht mehr möglich ist und es wird wieder die zweite (und damit die vorher aktive) Firmware gestartet.

Default-Wert:

check-and-update

2.107.2 Check-Firmware-Now

Dieser Befehl veranlasst das Gerät, zu prüfen, ob auf dem LANCOM Update-Server eine neuere Firmware vorhanden ist.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

2.107.3 Update-Firmware-Now

Dieser Befehl veranlasst das Gerät, die neueste Firmware vom LANCOM Update-Server herunterzuladen und zu installieren.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

2.107.4 Cancel-Current-Action

Dieser Befehl veranlasst das Gerät, die aktuelle laufende Aktion des Auto Updaters abzubrechen. Dies bezieht sich sowohl auf manuell gestartete als auch auf geplant ausgeführte Aktionen.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

2.107.5 Reset-Updater-Config

Dieser Befehl setzt die auf den Auto Updater bezogenen bootpersistenten Konfigurationsdateien zurück. Dies schließt die lokale Blacklist ein, die Firmware-Versionen enthält, mit denen ein automatisches Update fehlgeschlagen ist.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

2.107.6 Base-URL

Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

max. 252 Zeichen aus `[A-Z][a-z][0-9]/?.-;:@&=$_+!*'(),%`

Default-Wert:

https://update.lancom-systems.de

2.107.7 Check-Interval

Der Auto Updater bestimmmt beim ersten Start einen zufälligen Zeitraum innerhalb eines Tages oder einer Woche, an dem die Prüfung durchgeführt wird. Das eigentliche Update soll dann im nächsten Zeitraum zwischen 2-4 Uhr (Voreinstellung) durchgeführt werden.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

daily
weekly

Default-Wert:

daily

2.107.8 Version-Policy

Stellen Sie hier die Versionsrichtlinie des LANCOM Auto Updaters ein. Diese steuert, welche Firmware-Versionen einem Gerät zum Update angeboten werden.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

latest

Releaseübergreifend immer die neueste Version. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 RU1 aktualisiert, aber auch auf 5.00 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

current

Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 RU1 aktualisiert, aber nicht auf 5.00 Rel.

security-updates-only

Innerhalb eines Releases das neueste SU. Beispiel: 4.00 Rel ist installiert; es wird auf 4.00 SU1 aktualisiert, aber nicht auf 4.00 RU2.

latest-without-REL

Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 4.00 ist installiert; es wird auf 5.00 RU1 aktualisiert, aber nicht auf 5.00 REL.

Default-Wert:

security-updates-only

2.107.10 Check-Time-Begin

Anfang des Zeitintervalls als Stundenangabe, in dem die Überprüfung stattfindet, ob ein Firmware-Update vorhanden ist und dieses ggfs. heruntergeladen wird. Die Voreinstellung für Anfang und Ende ist jeweils 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

0

2.107.11 Check-Time-End

Ende des Zeitintervalls als Stundenangabe, in dem die Überprüfung stattfindet, ob ein Firmware-Update vorhanden ist und dieses ggfs. heruntergeladen wird. Die Voreinstellung für Anfang und Ende ist jeweils 0, es kann also rund um die Uhr auf Updates geprüft und ein Download gestartet werden. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Update-Prüfung und den Download geplant.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

0

2.107.12 Install-Time-Begin

Anfang des Zeitintervalls als Stundenangabe, in dem die Installation eines Firmware-Updates durchgeführt wird. Die Voreinstellung ist zwischen 2 und 4 Uhr morgens. Nach der Installation findet ein Neustart des Gerätes statt.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

2

2.107.13 Install-Time-End

Ende des Zeitintervalls als Stundenangabe, in dem die Installation eines Firmware-Updates durchgeführt wird. Die Voreinstellung ist zwischen 2 und 4 Uhr morgens. Nach der Installation findet ein Neustart des Gerätes statt.

Pfad Konsole:

Setup > **Automatic-Firmware-Update**

Mögliche Werte:

0 … 23

Default-Wert:

4

4 Other

In diesem Menü finden Sie zusätzliche Funktionen aus dem LCOS LX-Menübaum.

Pfad Konsole:

/

4.1 Reset-Config

Mit dieser Aktion können Sie die Konfiguration zurücksetzen.

Beispiel: `do Reset-Config`

Pfad Konsole:

Other

4.2 Reboot

Mit dieser Aktion starten Sie das Gerät neu.

Beispiel: `do Reboot`

Pfad Konsole:

Other