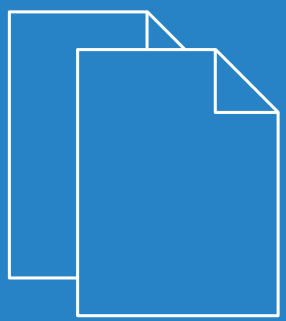
SICHER. **VERNETZT.**

LCOS LX 5.20

Referenzhandbuch



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

Menüreferenz

Die Menüreferenz 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.

2 Bedienung

2.1 Software zur Konfiguration

Die Situationen, in denen konfiguriert wird, unterscheiden sich ebenso wie die persönlichen Ansprüche und Vorlieben der Ausführenden. Das Gerät verfügt daher über ein breites Angebot von Konfigurationsmöglichkeiten:

- **LANconfig** – menügeführt, übersichtlich und einfach lassen sich nahezu alle Parameter eines Gerätes einstellen. LANconfig benötigt einen Konfigurationsrechner mit einem aktuellem Windows-Betriebssystem. Weitere Informationen finden Sie in den Kapiteln *LANconfig – Geräte konfigurieren* auf Seite 7 und *Features über LANconfig konfigurieren* auf Seite 17.
- **WEBconfig** – Weitere Informationen finden Sie in den Kapiteln *WEBconfig – Geräte überwachen und konfigurieren* auf Seite 8 und *Features über WEBconfig konfigurieren* auf Seite 59.
- **Konsole** – alternativ zu LANconfig können Sie auch über SSH eine Konsole auf dem Gerät öffnen und darüber auf das Kommandozeileninterface zugreifen. Über den TCP-Port 22 ist der Zugriff auf das Gerät über ein SSH-Programm wie z. B. PuTTY möglich.
- **LANCOM Management Cloud** – die hyper-integrierte Lösung für die automatisierte Steuerung Ihres Netzwerks.

Die Standard-Zugangsdaten für alle Konfigurationswege lauten:

- Benutzer: root
- Passwort: <Leer> (es ist kein Passwort gesetzt)

Um die Sicherheit zu gewährleisten, werden Sie beim ersten Zugriff über WEBconfig aufgefordert, das Passwort zu ändern.

Bitte beachten Sie, dass alle Verfahren auf dieselben Konfigurationsdaten zugreifen.

2.1.1 LANconfig – Geräte konfigurieren

Von der komfortablen Inbetriebnahme eines Einzelplatzgerätes mit den einfach zu bedienenden Installationsassistenten bis zum ganzheitlichen Management mit Firmware- und Konfigurationsverteilung größerer Installationen reicht das Anwendungsspektrum von LANconfig.

Basisfunktionen

- Automatisches Erkennen von neuen, unkonfigurierten Geräten
- (Fern-)Konfiguration von Geräten über IP-Adresse, URL oder über die serielle Schnittstelle
- Integration von Telnet-, SSH-, HTTPS- und TFTP-Konfiguration
- Kontext-basiertes Hilfesystem zu den Konfigurations-Parametern
- In allen Installationsschritten bieten die Assistenten angepasste Eingabemasken
- Einrichtung von Backup-Verbindungen

Management von größeren Installationen

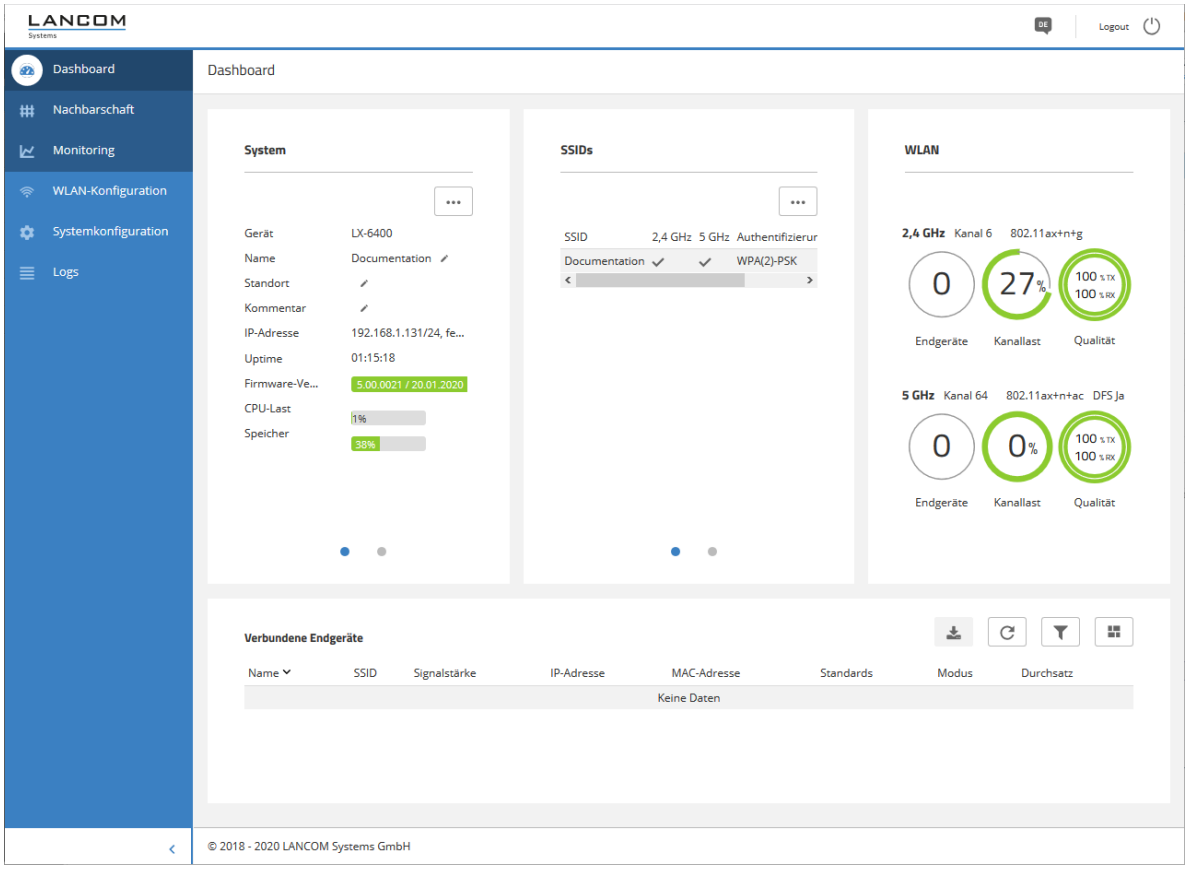
- Gruppenbildung
- Zentrale Firmware-Verteilung
- Simultankonfiguration mehrerer Geräte
- Verteilen von Konfigurations-Scripten
- WLAN-Gruppenkonfiguration
- Logging aller Aktionen
- Erstellung von neuen „Offline"-Konfigurationen für alle Geräte und sowohl LCOS als auch LCOS LX-Versionen

2.1.2 WEBconfig – Geräte überwachen und konfigurieren

Mittels WEBconfig konfigurieren Sie Einzelgeräte oder überwachen diese im laufenden Betrieb. Sie erreichen die WEBconfig über HTTP und HTTPS. Im Falle von HTTP erfolgt automatisch eine Umleitung auf eine verschlüsselte HTTPS-Verbindung.

Da die WEBconfig mit einem selbst-signierten SSL-Zertifikat arbeitet, muss dieses einmalig (pro Gerät) im Browser als Ausnahme hinzugefügt werden.

Im Folgenden eine Übersicht über die wesentlichen Bestandteile der WEBconfig, die Sie jeweils im linken Bereich in der **Sidebar** auswählen können.



Dashboard

Über das Dashboard werden Ihnen Statusinformationen des Gerätes im laufenden Betrieb angezeigt.

- System – grundsätzliche Informationen zum Gerät, z. B. der Gerätename und die Firmware-Version.
- WLAN – Informationen zur Auslastung der vom Gerät betriebenen WLAN-Kanäle.
- Verbundene Stationen – zeigt alle aktuell mit dem Gerät verbundenen WLAN-Stationen.

- Nachbarschaft – Überblick über die WLAN-Umgebung, insbesondere die in der Umgebung aktiven WLAN Access Points und WLAN-Router.
- Monitoring – Graphen zur zeitlichen Visualisierung des WLAN-Durchsatzes, des LAN-Durchsatzes, der Anzahl der WLAN-Stationen sowie der Kanalauslastung.

Konfiguration

- Systemkonfiguration – Konfiguration grundsätzlicher Parameter Ihres Gerätes, z. B. den Gerätenamen oder die IP-Einstellungen zum Management des Gerätes.
- WLAN – Die WLAN-Konfiguration wurde mit dem Ziel entworfen, den Nutzer für die am häufigsten verwendeten Konfigurationsarbeiten zu unterstützen und die mühevolle Konfiguration kleiner Details unnötig zu machen. Gleichzeitig ist aber weiterhin die Konfiguration davon abweichender Szenarien möglich.

Logs

In diesem Bereich wird das Syslog des Gerätes ausgegeben.

2.1.3 Konsole – Befehlsübersicht

Das Kommandozeilen-Interface wird mit den folgenden Befehlen bedient. Eine Übersicht der möglichen Konfigurationsparameter und Aktionen finden Sie in der LCOS LX-Menüreferenz.

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.

Befehl	Beschreibung
`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.).
`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. Weitere Informationen zu dem Befehl erhalten Sie gesondert im Abschnitt *Diagnose* auf Seite 83.

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.

3 Feature-Beschreibungen

Im Folgenden finden Sie Beschreibungen zu einigen ausgewählten WLAN-Features.

3.1 Band Steering

Der Standard IEEE 802.11 enthält kaum Kriterien, nach denen ein WLAN-Client den Access Point für eine Verbindung auswählen sollte. Zwar gibt es allgemeine Richtlinien, wonach z. B. ein Access Point mit höherem RSSI-Wert (d. h. der empfangenen Signalstärke) zu bevorzugen ist. Doch in der Praxis beachten WLAN-Clients weder die oben angesprochenen Definitionen noch die allgemeinen Richtlinien konsequent. Wird eine SSID in sowohl 2,4 GHz als auch 5 GHz ausgestrahlt, besteht im Normalfall keine Möglichkeit auf die Entscheidung des Clients, welches Frequenzband er bevorzugt, Einfluss zu nehmen.

Die gezielte Zuweisung von WLAN-Clients, das sog. „Client Steering", basiert auf dem Prinzip, dass viele Clients die verfügbaren Access Points durch einen aktiven Scan-Vorgang ermitteln. Aktives Scannen bedeutet hier, dass ein Client Test-Anforderungspakete (Probe Requests) versendet, welche die Netzwerkkennung enthalten, zu der ein Client eine Verbindung aufbauen soll. Access Points mit der entsprechenden Kennung versenden daraufhin eine Test-Antwort und ermöglichen es dem Client auf diese Weise, eine Liste mit verfügbaren Access Points zu erstellen. Die Tatsache, dass die weitaus meisten WLAN-Clients sich nur mit solchen Access Points verbinden, von denen sie eine Test-Antwort (Probe Response) erhalten haben, kann zur Steuerung des Auswahlverhaltens (und somit zur gezielten Zuweisung) eingesetzt werden.

Für die gezielte Zuweisung gibt es mehrere, zum Teil sehr fortgeschrittene Kriterien. Eines dieser Kriterien betrifft die verwendeten Funkfrequenzbereiche, in denen Clients kommunizieren. So erwartet man von modernen Dual-Band-WLAN-Clients immer häufiger, dass diese den 5-GHz-Frequenzbereich gegenüber dem inzwischen überfüllten 2,4-GHz-Bereich bevorzugen. Weist man einem WLAN-Client ganz gezielt ein bestimmtes Frequenzband bzw. einen bestimmten Frequenzbereich zu, spricht man von Band Steering.

Die Liste mit den ermittelten (bzw. „gesehenen") Clients enthält alle Clients, von denen der Access Point ein Test-Anforderungspaket empfangen hat. Zusammen mit der Funkfrequenz, auf der der WLAN-Client die Test-Anforderung gesendet hat, bildet diese Liste eine der Entscheidungsgrundlagen für den Access Point, die betreffende Anforderung zu beantworten oder nicht.

Weitere Kriterien für eine solche Entscheidungsfindung hängen mit den gemeldeten Kennungen der Clients und der Konfiguration der Geräte zusammen: So kann es z. B. vorkommen, dass auf dem bevorzugten Frequenzband weniger SSIDs gemeldet werden als auf dem weniger bevorzugten. Ebenso kann eine zu geringe Sendestärke beim Melden der SSIDs dazu führen, dass der Client auf dem bevorzugten Frequenzband keine Test-Antwort erhält. Für den letzteren Fall sollte man sicherstellen, dass der Access Point Test-Antworten auf dem weniger bevorzugten Frequenzband nicht durch den Steuerungsmechanismus unterdrückt.

Sie können das Band-Steering des Access Points im LANconfig unter **Wireless-LAN** > **Client-Management** konfigurieren.

3.2 Fast Roaming

Zusammen mit der Authentifizierung nach dem Standard IEEE 802.1X und dem Schlüsselmanagement nach dem Standard IEEE 802.11i bieten moderne WLAN-Installationen ein hohes Maß an Sicherheit und Vertraulichkeit der übertragenen Daten. Allerdings erfordern diese Standards die Übertragung zusätzlicher Datenpakete während der Verbindungsverhandlung sowie zusätzliche Rechenleistung auf Client- und Serverseite.

IEEE 802.11 benötigte ursprünglich zum Aufbau einer Datenverbindung zwischen WLAN-Client und Accesss Point lediglich bis zu sechs Datenpakete. Die Standard-Erweiterung IEEE 802.11i besserte Schwachstellen bei der WEP-Verschlüsselung aus, verlängerte dabei jedoch den Anmeldeprozess je nach Authentifizierungsmethode um ein Vielfaches.

Diese verlängerte Anmeldezeit des WLAN-Clients am Accesss Point ist für nicht zeitkritische Anwendungen ausreichend. Für ein reibungsloses, verlustfreies Roaming eines WLAN-Clients von einem Accesss Point zum nächsten, ist eine Verzögerung von mehr als 50 ms jedoch nicht akzeptabel. Als Beispiel seien hier Voice-over-IP (VoIP) oder die Anwendung in industriellen Echtzeit-Umgebungen genannt. Roaming bedeutet in diesem Zusammenhang, dass die Netzwerkverbindung ohne Abbruch von einem Access Point auf den anderen übergeht.

Methoden wie Pairwise Master Key Caching (PMK Caching), Pre-Authentication, Opportunistic Key Caching (OKC) sowie der Einsatz von zentralen WLAN-Controllern (WLC) zur Schlüsselverwaltung verbessern die Zeit für die Schlüsselaushandlung zwischen WLAN-Client und Accesss Point bei der Anmeldung. Allerdings reicht das immer noch nicht aus, die vergleichsweise lange Zeit für die Schlüsselverhandlung zwischen WLAN-Client und Accesss Point auf ein brauchbares Maß zu begrenzen.

Neben den verbesserten Verschlüsselungs-Protokollen ermöglicht es IEEE 802.11e dem WLAN-Client, eine zusätzliche Bandbreite beim Accesss Point zu reservieren. Auf diese Weise vermeidet der WLAN-Client Unterbrechungen z. B. bei VoIP-Verbindungen aufgrund von zu hoher Netzlast beim Accesss Point. Beim Roaming von einem Accesss Point zum nächsten muss der WLAN-Client diese zusätzliche Bandbreite erneut beim neuen Accesss Point reservieren. Die dafür notwendigen zusätzlichen Management-Frames erhöhen die Anmeldezeit jedoch wieder deutlich.

IEEE 802.11r sorgt dafür, dass sich bewegende WLAN-Clients beim Roaming ohne aufwändige Neuanmeldung und damit weitgehend störungsfrei von einem Accesss Point zum nächsten wechseln können. Das Ziel ist, die Anzahl der Datenpakete für die Anmeldung am Access Point wieder auf die vom IEEE 802.11 bekannten vier bis sechs Pakete zu verringern.

Wie beim Opportunistic Key Caching (OKC) existiert eine zentrale Schlüssel-Verwaltung, sinnvollerweise in Form eines WLCs, der die angeschlossenen Accesss Points mit den entsprechenden Anmeldedaten der WLAN-Clients versorgt. Im Gegensatz zum OKC kann der WLAN-Client beim Fast Roaming jedoch erkennen, ob der Accesss Point IEEE 802.11r beherrscht.

Die vom WLC verwalteten Accesss Points senden als Kennung das sogenannte „Mobility Domain Information Element (MDIE)“ aus, das den WLAN-Clients im Empfangsbereich u. a. mitteilt, welcher „Mobility Group“ der Accesss Point angehört. Anhand dieser Gruppenkennung erkennt der WLAN-Client, ob er derselben Domain angehört und sich somit ohne Verzögerung anmelden kann. Diese Mobility Domain hat der WLAN-Client während der ersten Anmeldung an einem Accesss Point mitgeteilt bekommen.

Die Domain-Kennung sowie spezielle, bei der Erstanmeldung generierte und an alle verwalteten Accesss Points übertragenen Schlüssel verringern die Verhandlungsschritte bei der Neuanmeldung bei einem Accesss Point auf die angestrebten vier bis sechs Schritte.

Um vergebliche und damit zeitraubende Anmeldeversuche mit abgelaufenen PMKs zu vermeiden, sieht IEEE 802.11r zusätzliche Informationen über die Gültigkeitsdauer von Schlüsseln vor. So kann der Client noch während einer bestehenden Verbindung mit dem aktuellen Accesss Point einen neuen PMK aushandeln. Dieser ist auch auf dem Accesss Point gültig, mit dem sich der WLAN-Client im Anschluss verbinden möchte.

Zusätzlich ermöglicht IEEE 802.11r in Form eines „Resource Requests“ die Reservierung von zusätzlicher Bandbreite auf dem neuen Accesss Point, ohne dass weitere Datenpakete wie bei IEEE 802.11e die Anmeldung unnötig verlängern.

Ältere WLAN-Clients haben möglicherweise Probleme damit, eine Verbindung zu einer SSID mit aktiviertem 802.11r aufzubauen. Daher ist hier der Einsatz zweier SSIDs ratsam: eine SSID für ältere Clients ohne 802.11r-Unterstützung und eine weitere SSID mit aktiviertem 802.11r für Clients mit 802.11r-Unterstützung.

Das Fast-Roaming lässt sich in LANconfig einstellen unter **Wireless-LAN** > **Allgemein** > **Verschlüsselung** > **WPA2-Key-Management**.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

Fast Roaming über Inter Access Point Protocol (IAPP)

Um Fast Roaming über IAPP zu verwenden, ist es erforderlich, jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zuzuweisen. 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. Beim Wechsel eines Clients zu einem anderen Access Point informiert (Handover Request) der übernehmende Access Point den ehemals bedienenden Access Point. Der ehemalige Access Point löscht daraufhin den Client aus seiner Stationstabelle. Im Handover Request ist die MAC-Adresse des Clients enthalten, sodasss im LAN vorhandene Geräte über das neue Routing informiert werden und ihre Zuordnungstabelle aktualisieren können.

Die Eingabe der IAPP-Passphrase erfolgt im LANconfig unter **Wireless-LAN** > **Allgemein** > **Verschlüsselung** > **PMK-IAPP-Secret**.

Beachten Sie bitte, dass es für die Verwendung von Fast Roaming über IAPP erforderlich ist, in den Verschlüsselungs-Einstellungen unter WPA2-Key-Management die Option Fast Roaming auszuwählen.

3.3 LANCOM Enhanced Passphrase Security (LEPS)

Mit LANCOM Enhanced Passphrase Security (LEPS) kann eine Menge von Passphrasen konfiguriert werden, die dann den einzelnen Benutzern, Gruppen oder MAC-Adressen zugeordnet werden können. Somit gibt es nicht eine globale Passphrase für eine SSID, sondern mehrere, die dann individuell verteilt werden können.

Dies kann für das Onboarding von Geräten in das Netzwerk genutzt werden. Wenn ein Netzwerk-Betreiber z. B. mehrere WLAN-Geräte in verschiedene Bereiche seines Netzwerks „onboarden" will, aber die Geräte nicht selber konfigurieren will, da dies die Benutzer der Geräte selber erledigen sollen. In diesem Fall erhalten die Benutzer lediglich einen Preshared Key für das Firmen-WLAN ausgehändigt, welchen die Benutzer selber für ihre Geräte verwenden können. Da LEPS ausschließlich auf der Infrastrukturseite konfiguriert wird, ist jederzeit die volle Kompatibilität zu Fremdprodukten gegeben.

Die Unsicherheit von globalen Passphrasen wird durch LEPS grundsätzlich behoben. Jedem Benutzer wird hierbei seine eigene individuelle Passphrase zugewiesen. Falls eine einem Benutzer zugeordnete Passphrase „verloren geht" oder ein Mitarbeiter mit Kenntnis seiner Passphrase das Unternehmen verlässt, dann muss nur die Passphrase dieses Benutzers geändert bzw. gelöscht werden. Alle anderen Passphrasen behalten ihre Gültigkeit und Vertraulichkeit.

Zusätzlich zu Passphrasen für Benutzer lassen sich auch MAC-Adressen **individuelle** Passphrasen zuordnen – eine beliebige Folge aus 8 bis 63 ASCII-Zeichen. Nur die Verbindung von Passphrase und MAC-Adresse erlaubt dann die Anmeldung am Access Point.

Da Passphrase und MAC-Adresse verknüpft sind, ist auch das Spoofing der MAC-Adressen wirkungslos – LEPS schließt damit auch einen möglichen Angriffspunkt gegen die ACL aus. Wenn als Verschlüsselungsart WPA2 verwendet wird, kann zwar die MAC-Adresse abgehört werden – die Passphrase wird bei diesem Verfahren jedoch nie über die WLAN-Strecke übertragen. Angriffe auf das WLAN werden so deutlich erschwert, da durch die Verknüpfung von MAC-Adresse und Passphrase immer beide Teile bekannt sein müssen, um eine Verschlüsselung zu verhandeln.

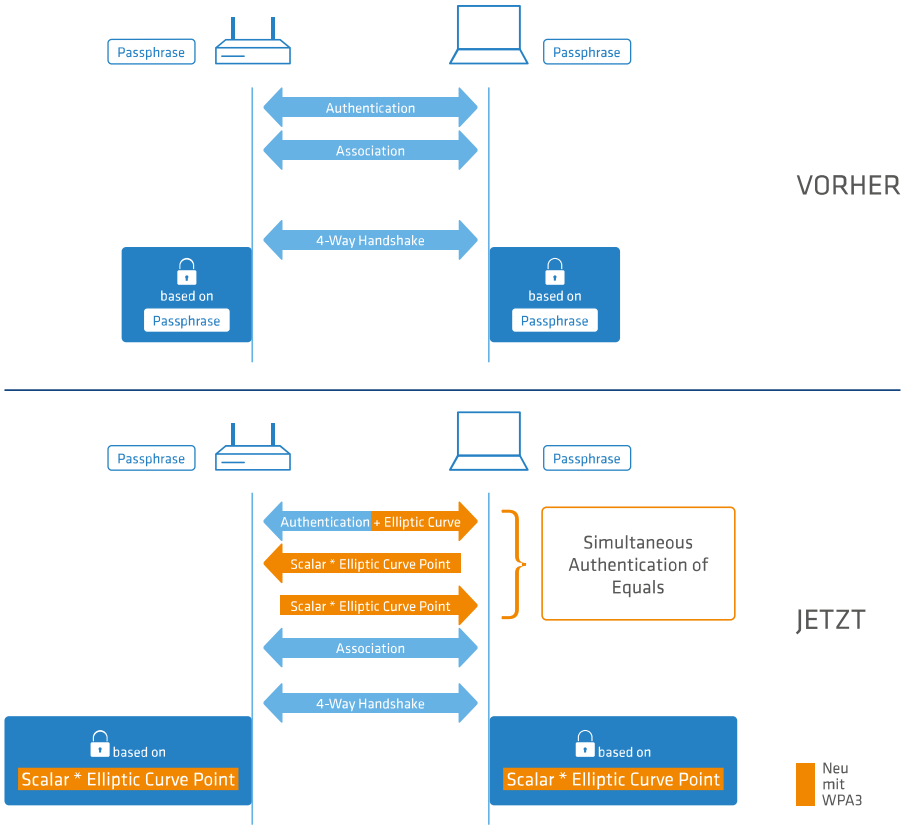
Im Vergleich zu LEPS für Benutzer ist der Verwaltungsaufwand etwas höher, da für jedes Gerät die MAC-Adresse eingetragen werden muss.

Aus technischen Gründen ist LEPS nur mit der WPA-Version WPA2 kompatibel.

3.4 WPA3 (Wi-Fi Protected Access 3)

Der 2018 eingeführte WPA3-Standard der Wi-Fi-Alliance bietet gegenüber dem bereits 2004 eingeführten Vorgängerstandard WPA2 eine verbesserte Sicherheit durch eine Kombination verschiedener aktueller Sicherheitsverfahren. Wie WPA2 existiert auch WPA3 in den Ausprägungen WPA3-Personal und WPA3-Enterprise.

WPA3-Personal bietet durch die Verwendung des Authentisierungsverfahrens Simultaneous Authentication of Equals (SAE) eine Methode, die lediglich ein Passwort für die Authentifizierung voraussetzt und dennoch Brute-Force- und Wörterbuch-Attacken ins Leere laufen lässt. Zudem bietet dieses Verfahren erstmalig Forward Secrecy – dies bedeutet, dass in der Vergangenheit mitgeschnittener, WPA3-gesicherter Datenverkehr auch später nicht mehr entschlüsselt werden kann, wenn der Angreifer Kenntnis des Pre-Shared Keys erlangt.



Zusätzlich wird bei WPA3-Enterprise die Commercial National Security Algorithm (CNSA) Suite B-Kryptographie verwendet. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

In beiden Varianten ist nun die Verwendung von Protected Management Frames (PMF) nach IEEE 802.11w verpflichtend. PMF verhindern, dass Angreifer durch Deassoziieren mittels gefälschter Management Frames und Belauschen der Wiederanmeldung Material bekommen, um das WLAN-Passwort zu errechnen.

3.4.1 WPA3-Personal

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** können die WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Personal unterstützen; die Authentisierung wird mit dieser Konfiguration nur noch über Simultaneous Authentication of Equals (SAE) zugelassen. Ebenfalls wird für diese SSID nun die Verwendung von PMF (Protected Management Frames nach IEEE 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

3.4.2 WPA3-Enterprise

WPA3-Enterprise ändert oder ersetzt die in WPA2-Enterprise definierten Protokolle nicht grundlegend. Stattdessen definiert es Richtlinien, um eine größere Konsistenz bei der Anwendung dieser Protokolle zu gewährleisten und die gewünschte Sicherheit zu gewährleisten.

In den WLAN-Verschlüsselungseinstellungen unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** können die WPA-Versionen **WPA3** und **WPA2/3** ausgewählt werden.

Bei Auswahl von **WPA3** können sich nur noch WLAN-Clients anmelden, die WPA3-Enterprise unterstützen. Für diese SSID wird die Verwendung von PMF (Protected Management Frames nach IEEE 802.11w; verpflichtender Bestandteil von WPA3) erzwungen.

Bei Auswahl von **WPA2/3** werden diese beiden WPA-Versionen parallel angeboten. Diese Auswahl ermöglicht den Mischbetrieb von WLAN-Clients, die nur WPA2 unterstützen mit WLAN-Clients, die bereits WPA3 unterstützen. Für WPA3-kompatible WLAN-Clients wird in dieser Konfiguration die Verwendung von PMF erzwungen; für WPA2-kompatible WLAN-Clients wird PMF aus Gründen der Abwärtskompatibilität optional angeboten.

Suite B-Kryptographie

Zusätzlich wird bei WPA3-Enterprise die Commercial National Security Algorithm (CNSA)-Suite-B-Kryptographie eingeschaltet. Suite B stellt sicher, dass alle Glieder in der Verschlüsselungskette aufeinander abgestimmt sind. Suite B bildet Klassen von Bitlängen für Hash-, symmetrische und asymmetrische Verschlüsselungsverfahren, die passende Schutzniveaus bieten. So passt zum Beispiel zu AES mit 128 Bit ein SHA-2-Hash mit 256 Bit. Wenn Suite B zum Einsatz kommt, ist die Unterstützung aller anderen Kombinationen ausdrücklich ausgeschlossen. In der Verschlüsselungskette gibt es folglich nur noch gleich starke Glieder.

Weitere Informationen zu CNSA Suite B finden Sie unter folgendem Link: *CNSA Algorithm Suite Factsheet*

Es wird die Verwendung der folgenden EAP Cipher-Suiten erzwungen:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Andere Cipher-Suiten können nicht verwendet werden. Ebenfalls wird eine Mindest-Schlüssellänge von 3072 Bit für die RSA- und Diffie-Hellman-Schlüsselaustauschverfahren, sowie 384 Bit für die ECDSA- und ECDHE-Schlüsselaustauschverfahren erzwungen. Zusätzlich wird der Sitzungschlüssel-Typ AES-GCMP-256 erzwungen.

Werden diese Cipher-Suiten von den verwendeten WLAN-Clients oder der restlichen Infrastruktur (z. B. RADIUS-Server) nicht unterstützt, dann ist keine Verbindung möglich!

Der im LCOS integrierte RADIUS-Server unterstützt die hier genannten Cipher-Suiten.

4 Features über LANconfig konfigurieren

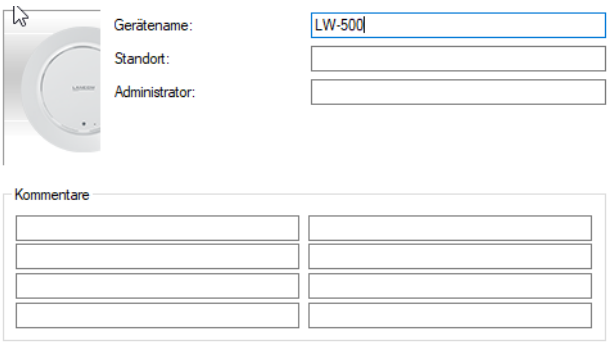
Im Folgenden werden alle Einstellungsmöglichkeiten in LANconfig erläutert. Diese sind abhängig vom Gerät, sodass nicht immer alle aufgeführten Optionen zur Verfügung stehen.

4.1 Management

Im Abschnitt **Management** finden Sie allgemeine Einstellungen zum Gerät.

4.1.1 Allgemein

Die beschreibenden Einstellungen zum Gerät finden Sie unter **Management** > **Allgemein**.



Name

Konfigurieren Sie hier den Gerätenamen.

Standort

Konfigurieren Sie hier den Gerätestandort.

Administrator

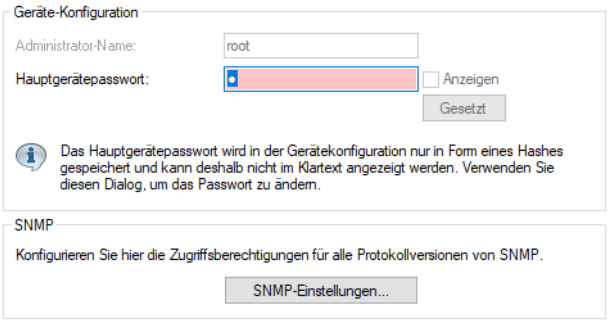
Konfigurieren Sie hier den Namen des Geräte-Administrators.

Kommentare

Verwenden Sie die Kommentarfelder zum Eintragen beliebiger Kommentare zur Gerätekonfiguration.

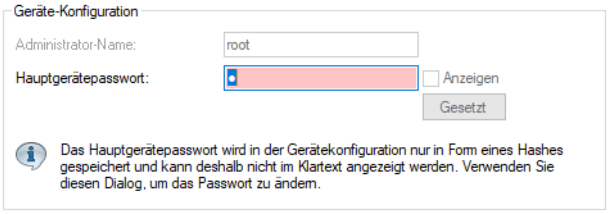
4.1.2 Admin

Die Einstellungen, um das Hauptgerätepasswort des Gerätes und die Einstellungen für SNMP zu ändern, finden Sie unter **Management** > **Admin**.



Hauptgerätepasswort

Die Einstellungen, um das Hauptgerätepasswort des Gerätes zu ändern, finden Sie unter **Management** > **Admin** > **Geräte-Konfiguration**.



Administrator-Name

Konfigurieren Sie hier den Anmeldenamen des Geräte-Administrators. Abhängig vom Gerät kann dieser Name fest vorgegeben sein und wird dann hier nur angezeigt.

Hauptgerätepasswort

Konfigurieren Sie hier das Hauptgerätepasswort. Dieses wird abhängig vom Gerät auf diesem nur als Hashwert gespeichert, sodass die Anzeige im Klartext nicht immer möglich ist.

Wenn Sie ein neues Passwort eingeben, dann erscheint ein Feld, um das geänderte Passwort erneut einzugeben. Da die Eingabe nicht angezeigt wird, dient dies zur Verifikation Ihrer Eingabe. Alternativ aktivieren Sie die Option **Anzeigen**. Danach wird Ihre Eingabe normal angezeigt. Falls ihr Bildschirm während der Eingabe einsehbar ist, dann raten wir von dieser Option ab.

Simple Network Management Protocol (SNMP)

Das Simple Network Management Protocol (SNMP) ermöglicht die Überwachung und Konfiguration von Geräten in einem Netzwerk von einer zentralen Instanz aus. Seit der ersten Veröffentlichung von SNMPv1 im Jahr 1988 entwickelte es sich im Laufe der Zeit über die Version SNMPv2 bis zur Version SNMPv3 weiter, um einer immer komplexeren Netzwerk-Infrastruktur sowie gesteigerten Ansprüchen an Sicherheit, Flexibilität und Komfort gerecht zu werden.

Mit Hilfe des Protokolls SNMP (Simple Network Management Protocol) werden höchste Ansprüche, wie das simple Management und Monitoring eines Netzwerks erfüllt. Es ermöglicht die frühzeitige Erkennung von Problemen und Störungen in einem Netzwerk und unterstützt bei deren Beseitigung. Das Simple Network Management Protocol ermöglicht die Überwachung und Konfiguration von Geräten in einem Netz von einer zentralen Instanz aus und regelt die Kommunikation zwischen den überwachten Geräten und der Überwachungsstation. Dadurch lassen sich Parameter wie der Zustand des Gerätes, CPU-Auslastung, Temperatur eines Geräts, Verbindungsstatus, Störungen, etc. z. B. über LANmonitor überwachen und auswerten. Der Administrator wird aktiv bei der Netzwerkverwaltung unterstützt und kann

Probleme frühzeitig in seinem Monitoringsystem erkennen. Die neueste Version des Protokolls SNMPv3 ermöglicht im Gegensatz zu den Vorgängerversionen SNMPv1 und SNMPv2 eine verschlüsselte Datenkommunikation zwischen Netzwerk und Managementsystem und bietet damit einen entscheidenden Sicherheitsfaktor. Die integrierte Nutzerverwaltung bietet zusätzlich, dank verschiedener Benutzer-Accounts, eine Authentifizierung für die optimale Zugriffskontrolle bei Konfigurationen. So lassen sich Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern und das Netzwerk ist optimal geschützt.

SNMP-Komponenten

Die typische SNMP-Architektur besteht aus drei Komponenten:

SNMP-Manager

Der SNMP-Manager sendet SNMP-Anfragen an den SNMP-Agent und wertet dessen SNMP-Antworten aus. Als solche SNMP-Manager fungieren z. B. LANconfig und LANmonitor. Da LCOS LX-Geräte sich an die Standards von SNMPv1, SNMPv2 und SNMPv3 halten, ist auch der Einsatz einer alternativen SNMP-Verwaltungs- und Management-Software möglich.

SNMP-Agent

Der SNMP-Agent ist ein Modul, das auf dem verwalteten Gerät aktiviert ist. Er nimmt die Anfragen des SNMP-Managers entgegen, sammelt entsprechend der Anfrage die Zustandsdaten des Geräts aus dessen MIB und sendet diese Daten als „SNMP Response" zurück an den SNMP-Manager. Je nach Konfiguration sendet der SNMP-Agent bei bestimmten Zustandsänderungen im verwalteten Gerät auch eigenständig einen sogenannten „SNMP Trap" an den SNMP-Manager. Die Benachrichtigung in Form einer SYSLOG-Meldung oder einer E-Mail an den Administrator des Geräts ist ebenfalls möglich.

Verwaltetes Gerät

Die Zustände dieses Gerätes finden sich in seiner Management Information Base (MIB). Auf Anfrage des SNMP-Agenten liest das Gerät die entsprechenden Daten aus und gibt sie an den SNMP-Agenten zurück.

Die Übertragung von SNMP-Requests und SNMP-Responses zwischen SNMP-Manager und SNMP-Agent erfolgt standardmäßig im User Datagram Procol (UDP) über den Port 161. Die Übertragung von SNMP-Traps erfolgt standardmäßig im UDP über Port 162.

SNMP-Versionen

Die Unterschiede zwischen den verschiedenen SNMP-Versionen lassen sich wie folgt zusammenfassen:

SNMPv1

Die Version 1 startete in 1988 und galt lange Zeit als De-Facto-Standard für Netzwerk-Management. Die Authentifizierung des SNMP-Managers am SNMP-Agent erfolgt bei SNMPv1 über einen Community-String, der in beiden Komponenten identisch sein muss. Diese Sicherheit ist allerdings stark eingeschränkt, da die Übertragung des Community-Strings im Klartext erfolgt. Nicht zuletzt die gesteigerten Anforderungen an eine sichere Netzwerk-Kommunikation machten eine Überarbeitung der Version 1 notwendig.

SNMPv2

In die Version 2 flossen seit 1993 hauptsächlich Verbesserungen im Komfortbereich ein. Mehrere Zwischenschritte und wieder verworfene Konzepte führten letztendlich zur Version SNMPv2c. Diese Version ermöglicht die komfortable Abfrage von großen Datenmengen über einen `GetBulkRequest`-Befehl und die Kommunikation von SNMP-Managern untereinander. Der Austausch des Community-Strings erfolgt allerdings wie bei der Version 1 weiterhin im Klartext.

SNMPv3

Die Version 3 erfüllt schließlich ab 1999 die mittlerweile dringend notwendigen Sicherheitsanforderungen. U. a. erfolgt die Kommunikation verschlüsselt, und auch die Kommunikationspartner müssen sich zuvor authentifizieren und autorisieren. Darüber hinaus ist der SNMP-Aufbau modularer geworden, so dass z. B.

Modernisierungen bei Verschlüsselungstechnologien in SNMPv3 einfließen können, ohne den Standard komplett neu gestalten zu müssen.

LCOS LX unterstützt die folgenden SNMP-Versionen:

- SNMPv1
- SNMPv2c
- SNMPv3

SNMPv3-Grundlagen

Die Protokoll-Struktur von SNMP hat sich in der Version 3 grundlegend geändert. SNMPv3 ist in mehrere Module mit klar definierten Interfaces aufgeteilt, die untereinander kommunizieren. Die drei wichtigsten Elemente in SNMPv3 sind „Message Processing and Dispatch (MPD)", „User-based Security Model (USM)" und „View-based Access Control Mechanism (VACM)".

MPD

Das MPD-Modul ist verantwortlich für die Verarbeitung (processing) und die Weiterbeförderung (dispatch) der ein- und ausgehenden SNMP-Meldungen.

USM

Das USM-Modul verwaltet Sicherheitsfunktionen, die die Authentifizierung der Nutzer sowie die Verschlüsselung und Integrität der Daten sicherstellen. 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.

VACM

Der VACM stellt sicher, dass der Sender einer SNMP-Anfrage berechtigt ist, die angefragte Information zu erhalten. Die entsprechenden Zugriffsberechtigungen finden sich in den folgenden Einstellungen und Parametern:

SNMPv3-Views

„SNMPv3-Views" fassen Inhalte, Statusmeldungen und Aktionen der Management Information Base (MIB) zusammen, die eine SNMP-Anfrage mit entsprechenden Zugriffsrechten erhalten bzw. ausführen darf. Diese Ansichten können einzelne Werte, aber auch komplette Pfade der MIB sein. Die Angabe dieser Inhalte erfolgt anhand der jeweiligen OIDs der MIB-Einträge.

Auf diese Weise erhält der Sender einer SNMP-Anfrage auch nach erfolgreicher Authentifizierung nur Zugriff auf die Daten, für die er gemäß SNMPv3-Views die Zugriffsrechte besitzt.

SNMPv3-Groups

„SNMPv3-Groups" fassen Nutzer mit gleichen Zugriffsrechten in einer jeweiligen Gruppe zusammen.

Security-Levels

„Security Levels" bestimmen die Sicherheitsstufe für den Austausch von SNMP-Nachrichten. Die folgenden Stufen sind auswählbar:

NoAuth-NoPriv

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.

Auth-NoPriv

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

Auth-Priv

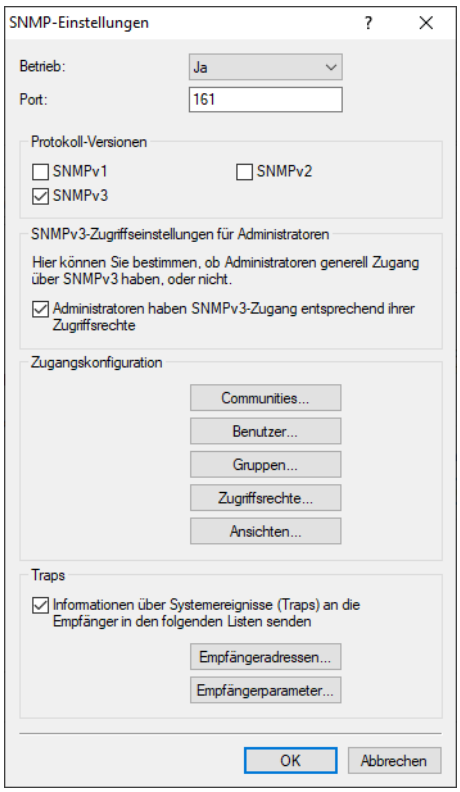
Für die Verarbeitung der SNMP-Anfrage ist eine Authentifizierung mittels HMAC-MD5- oder HMAC-SHA-Algorithmus notwendig, die Datenübertragung erfolgt zusätzlich verschlüsselt über DES- oder AES-Algorithmen.

Kontext

Der „Kontext" ist dafür vorgesehen, die einzelnen SNMP-Entities voneinander zu unterscheiden.

SNMP konfigurieren

Die SNMP-Einstellungen des Gerätes finden Sie unter **Management** > **Admin** > **SNMP** > **SNMP-Einstellungen**.



Betrieb

Aktivieren Sie SNMP für die im Folgenden angegebenen SNMP-Protokollversionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.

Port

Passen Sie ggfs. den Port für SNMP an. Default: 161

Protokoll-Versionen

SNMPv1

Aktiviert SNMPv1.

SNMPv2

Aktiviert SNMPv2c.

SNMPv3

Aktiviert SNMPv3.

SNMPv3-Zugriffseinstellungen für Administratoren

Administratoren haben SNMPv3-Zugang entsprechend ihrer Zugriffsrechte

Sollen registrierte Administratoren, also ebenfalls der Benutzer root, auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

Zugangskonfiguration

SNMP-Communities

Auch bei der Verwaltung von Netzwerken mit SNMP-Management-Systemen lassen sich die Rechte über verschiedene Zugriffsebenen für Administratoren präzise steuern. SNMP kodiert dazu bei den Versionen SNMPv1 und SNMPv2c die Zugangsdaten als Teil einer sogenannten „Community", welche die Bedeutung eines Passworts bzw. Zugangsschlüssels inne hat. Die Authentifizierung kann hierbei wahlweise

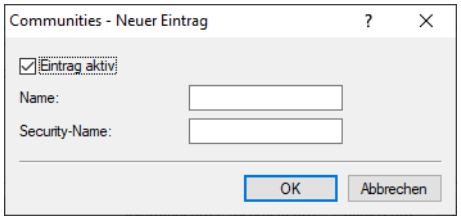
- über die Community `public` (uneingeschränkter SNMP-Lesezugriff),
- ein Master-Passwort (beschränkter SNMP-Lesezugriff),
- oder eine Kombination aus Benutzername und Passwort, getrennt durch einen Doppelpunkt (beschränkter SNMP-Lesezugriff),

erfolgen.

Eine Communitiy fasst somit 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.

Standardmäßig beantwortet Ihr Gerät alle SNMP-Anfragen, die es von LANmonitor oder einem anderen SNMP-Management-System mit der Community `public` erhält. Da dies jedoch (v. a. bei externer Erreichbarkeit) ein potentielles Sicherheitsrisiko darstellt, haben Sie die Möglichkeit, in LANconfig eigene Communities zu definieren.

Diese Konfiguration ist nur für die SNMP-Versionen v1 und v2c relevant.



Eintrag aktiv

Aktiviert oder deaktiviert diese SNMP-Community.

Name

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

Security-Name

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

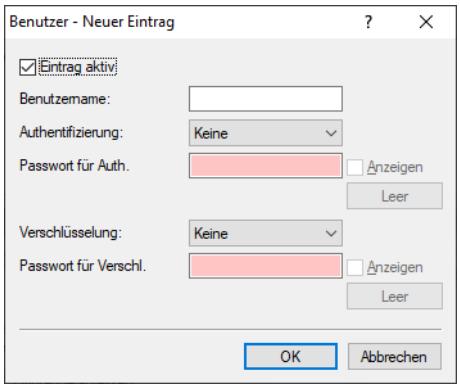
Als Standard ist die SNMP-Community `public` eingerichtet, die den uneingeschränkten SNMP-Lesezugriff ermöglicht.

Um eine autorisierte Abfrage von Zugangsdaten beim SNMP-Lesezugriff über SNMPv1 oder SNMPv2c zu erzwingen, deaktivieren Sie die Community `public` in der Liste der SNMP-Communities. Dadurch lassen sich Informationen über den Zustand des Gerätes, aktuelle Verbindungen, Reports, etc. erst dann via SNMP auslesen, nachdem sich der betreffende Benutzer am Gerät authentifiziert hat. Die Autorisierung erfolgt wahlweise über die Zugangsdaten des Administrator-Accounts oder über den in der individuellen SNMP-Community definierten Zugang.

Das Deaktivieren der Community `public` hat keine Auswirkung auf den Zugriff über eine weitere angelegte Community. Eine individuelle SNMP Read-Only Community bleibt z. B. stets ein alternativer Zugangsweg, der nicht an ein Administrator-Konto gebunden ist.

Benutzer

Neben den am Gerät registrierten Administratoren ist der Zugriff auch für einzelne Nutzer möglich. Hier konfigurieren Sie die Einstellungen für Authentifizierung und Verschlüsselung für diese Anwender bei Nutzung von SNMPv3.



Eintrag aktiv

Aktiviert oder deaktiviert diesen Benutzer.

Benutzername

Vergeben Sie hier einen aussagekräftigen Namen für diesen Benutzer.

Authentifizierung

Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss. Zur Verfügung stehen die folgenden Verfahren:

Keine

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 (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).

Passwort für Authentifizierung

Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

Verschlüsselung

Bestimmen Sie, nach welchem Verschlüsselungsverfahren die Kommunikation mit dem Benutzer verschlüsselt sein soll. Zur Verfügung stehen die folgenden Verfahren:

Keine

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

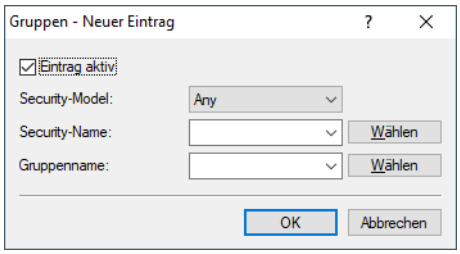
Die Verschlüsselung erfolgt mit AES256 (Schlüssellänge 256 Bits)

Passwort für Verschlüsselung

Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein und wiederholen Sie es im Feld darunter.

Gruppen

Durch die Konfiguration von SNMP-Gruppen lassen sich Authentifizierung und Zugriffsrechte für mehrere Benutzer komfortabel verwalten und zuordnen. Als Standardeintrag ist die Konfiguration für den SNMP-Zugriff über den LANmonitor bereits voreingestellt.



Eintrag aktiv

Aktiviert oder deaktiviert diese Gruppe.

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 einen der folgenden Einträge aus:

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 „Keine Authentifizierung und keine Verschlüsselung".

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 „Keine Authentifizierung und keine Verschlüsselung".

SNMPv3_USM

Die Übertragung der Daten erfolgt über SNMPv3. Für Anmeldung und Kommunikation des Benutzers sind Sicherheitsstufen möglich, die bei den **Zugriffsrechten** aktiviert werden.

Security-Name

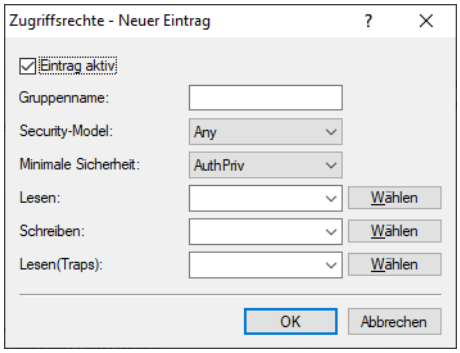
Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben.

Gruppenname

Wählen Sie hier eine Gruppe aus, die Sie unter **Zugriffsrechte** definiert haben.

Zugriffsrechte

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



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Gruppenname

Vergeben Sie hier einen aussagekräftigen Namen für diese Gruppe.

Security-Model

Aktivieren Sie hier das entsprechende Security-Model.

Minimale Sicherheit

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

NoAuthNoPriv (Keine Authentifizierung und keine Verschlüsselung)

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

AuthNoPriv (Authentifizierung, aber keine Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv (Authentifizierung und Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

Lesen

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access“, „LANmonitor-Access“, „Setup-Access“ und „Status-Access“.

Schreiben

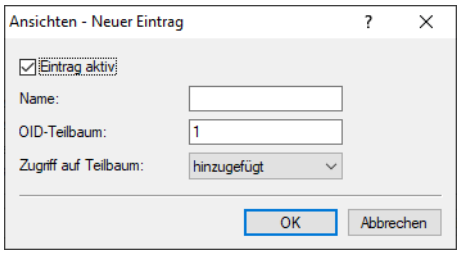
Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Schreibrechte erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access“, „LANmonitor-Access“, „Setup-Access“ und „Status-Access“.

Lesen (Traps)

Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte für Traps erhalten soll. Mögliche Werte sind die in **Ansichten** definierten Einträge. Bereits definiert sind dort „Full-Access“, „LANmonitor-Access“, „Setup-Access“ und „Status-Access“.

Ansichten

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



Eintrag aktiv

Aktiviert oder deaktiviert diese Ansicht.

Name

Vergeben Sie hier einen aussagekräftigen Namen für die Ansicht.

OID-Teilbaum

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

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

Zugriff auf Teilbaum

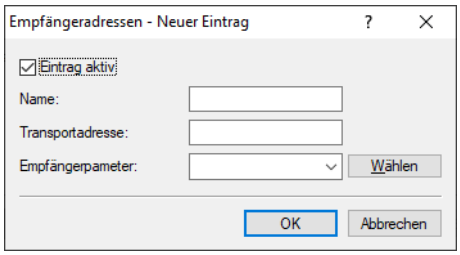
Bestimmen Sie, ob die angegebenen OID-Teilbäume Bestandteil („hinzugefügt“) oder kein Bestandteil („entfernt“) der Ansicht sind.

Traps

Wenn Sie die Option **Informationen über Systemereignisse (Traps) an die Empfänger in den folgenden Listen senden** aktivieren, dann bekommen die unter **Empfängeradressen** und **Empfängerparameter** konfigurierten Empfänger entsprechende Informationen.

Empfängeradressen

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



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Transportadresse

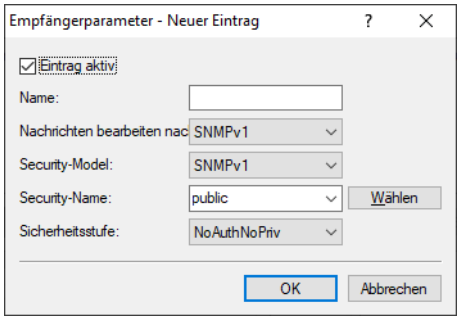
Konfigurieren Sie hier die Adresse des Empfängers. Diese Adresse beschreibt die IP-Adresse und Port-Nummer eines SNMP-Trap-Empfängers und wird in der Syntax „<IP-Adresse>:<Port>" angegeben (z. B. 128.1.2.3:162). Der UDP-Port 162 wird für SNMP-Traps verwendet.

Empfängerparameter

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

Empfängerparameter

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



Eintrag aktiv

Aktiviert oder deaktiviert diesen Eintrag.

Name

Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.

Nachrichten bearbeiten nach

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

Security-Model

SNMPv3 hat das Prinzip des „Security Models" eingeführt, sodass 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 auszuwählen. Entsprechend wählen Sie hier einen der folgenden Einträge aus:

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. Dies kann ausschließlich zusammen mit SNMP-Benutzern gewählt werden. Die effektive mögliche Sicherheitsstufe hängt von den gewählten Authentifizierungs- und Verschlüsselungsmethoden des Benutzers ab.

Security-Name

Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben.

Sicherheitsstufe

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

NoAuthNoPriv (Keine Authentifizierung und keine Verschlüsselung)

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

AuthNoPriv (Authentifizierung, aber keine Verschlüsselung)

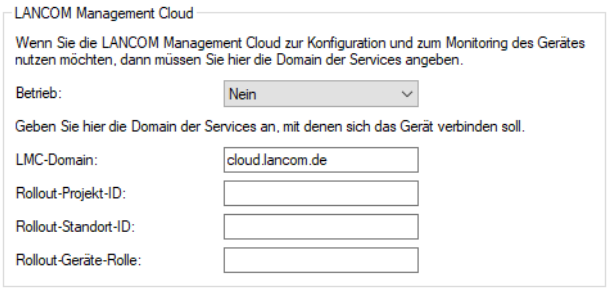
Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Eine Verschlüsselung der Datenübertragung findet nicht statt.

AuthPriv (Authentifizierung und Verschlüsselung)

Die Authentifizierung erfolgt über die für den Benutzer eingestellten Hash-Algorithmen. Die Verschlüsselung der Datenübertragung erfolgt über DES- oder AES-Algorithmen.

4.1.3 LMC

Die Einstellungen für die Konfiguration und das Monitoring Ihres Gerätes durch die LANCOM Management Cloud (LMC) finden Sie unter **Management** > **LMC**.



Betrieb

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

Nein

Das Gerät stellt keine Verbindung zur LMC her.

Ja

Das Gerät wird von der LMC verwaltet.

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.

Rollout-Projekt-ID

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

Rollout-Standort-ID

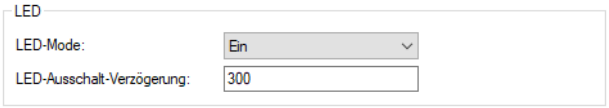
Geben Sie hier den Standort dieses Gerätes in der LMC an. Bei der ersten Verbindung zur LMC wird es dementsprechend zugeordnet.

Rollout-Geräte-Rolle

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

4.1.4 Erweitert

Hier finden Sie die Einstellungen für die LED-Funktionalität. Diese sind unter **Management** > **Erweitert**.



LED-Mode

Wählen Sie zwischen den LED-Betriebsarten:

Ein

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

Aus

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

Verzögert aus

Die LED(s) des Gerätes werden nach einer konfigurierbaren Zeit abgeschaltet.

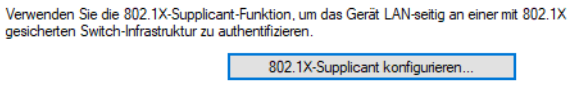
Konsultieren Sie die Hardwareschnellübersicht des jeweiligen Gerätes für gerätespezifische Details zur LED-Signalisierung.

LED-Ausschalt-Verzögerung

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

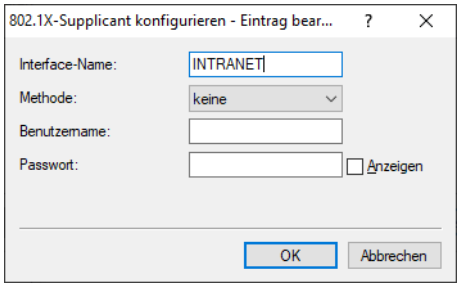
4.1.5 802.1X-Supplicant

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. Diese sind unter **Management** > **802.1X-Supplicant**.



802.1X-Supplicant konfigurieren

Die 802.1X-Supplicant-Funktionalität konfigurieren Sie unter **Management** > **802.1X-Supplicant** > **802.1X-Supplicant konfigurieren**.



Interface-Name

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

Methode

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

Benutzername

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

Passwort

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

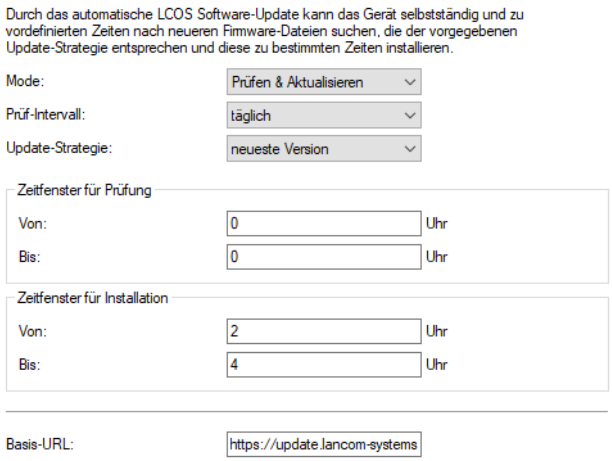
Die Unterstützung für eine Anmeldung mittels Client-Zertifikaten folgt in einer zukünftigen LCOS LX-Version.

4.1.6 Software-Update

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff. 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.

Die Konfiguration des LANCOM Auto Updaters finden Sie in LANconfig unter **Management** > **Software-Update**.



Mode

Stellen Sie hier den Betriebsmodus ein. Die folgenden Modi werden unterstützt:

Prüfen & Aktualisieren

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Der Update-Server ermittelt anhand der **Update-Strategie** 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.

nur Prüfen

- Der Auto Updater prüft regelmäßig beim 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.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manuell

- 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.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Prüf-Intervall

Stellen Sie ein, ob die Überprüfung auf ein verfügbares Update täglich oder wöchentlich stattfinden soll.

Update-Strategie

neueste Version

Releaseübergreifend immer die neueste Version. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber auch auf 10.30 Rel. Es wird also immer auf die neueste Version aktualisiert, aber nicht wieder auf ein vorheriges Release zurückgewechselt.

aktuelle Version

Innerhalb eines Releases die neueste RU/SU/PR. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 RU1 aktualisiert, aber nicht auf 10.30 Rel.

nur Sicherheitsupdates

Innerhalb eines Releases das neueste SU. Beispiel: 10.20 Rel ist installiert; es wird auf 10.20 SU1 aktualisiert, aber nicht auf 10.20 RU2.

neueste Version ohne REL

Releaseübergreifend das neueste RU/SU/PR. Es wird erst bei Verfügbarkeit eines RU aktualisiert. Beispiel: Eine beliebige 10.20 ist installiert; es wird auf 10.30 RU1 aktualisiert, aber nicht auf 10.30 REL.

Zeitfenster für Prüfung

Stellen Sie hier das Zeitfenster für die Prüfung und den Download neuer Aktualisierungen ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung für beide Werte ist 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.

Zeitfenster für Installation

Stellen Sie hier das Zeitfenster für die Update-Installation ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung definiert ein Zeitfenster zwischen 2:00 Uhr und 4:00 Uhr. Wenn ein Update gefunden wurde, dann wird dieses also in diesem Zeitraum installiert und das Gerät neu gestartet, um das Update zu aktivieren. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Installation geplant.

Basis-URL

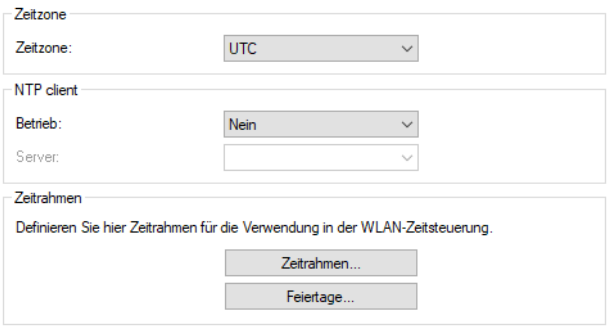
Gibt die URL des Servers an, der die aktuellen Firmware-Versionen zur Verfügung stellt.

4.2 Datum / Zeit

Im Abschnitt **Datum / Zeit** finden Sie die entsprechenden Einstellungen des Gerätes.

4.2.1 Konfiguration

Die Einstellungen des Gerätes zu Datum und Uhrzeit finden Sie unter **Datum / Zeit** > **Konfiguration**.



Zeitzone

Geben Sie die korrekte Zeitzone an.

NTP Client

Über das Network Time Protocol (NTP) kann das Gerät sich die aktuelle Zeit von einem öffentlich zugänglichen Zeit-Server im Internet (NTP-Server mit „Open Access"-Policy, in Deutschland z. B. von der Physikalisch-Technischen Bundesanstalt) beziehen. LANCOM Router können ebenfalls als NTP-Server arbeiten, so dass nicht jedes Gerät auf einen externen NTP-Server zugreifen muss.

Betrieb

Ja

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

Nein

Keinen NTP-Server verwenden.

Server

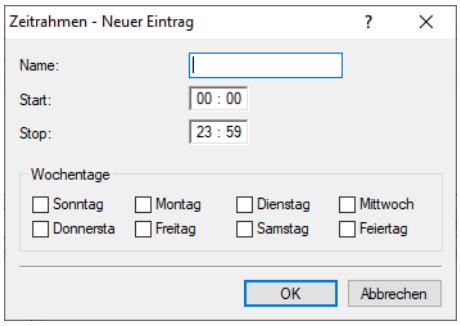
Geben Sie hier die Adresse des zu verwendenden NTP-Servers an.

Zeitrahmen

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.

Beispielhaft sind hier bereits mehrere Zeitrahmen angelegt, die eine Konfiguration für einen Unterrichtstag an einer Schule zeigen sollen. Es existieren zwei Zeitrahmen mit dem identischen Namen „Unterricht" – aber mit unterschiedlicher Start- und Stoppzeit, um zwischen diesen beiden Zeitrahmen eine 45-minütige Pause realisieren zu können. Diese ist wiederum in dem Zeitrahmen „Pause" definiert. Zeitrahmen können auf bestimmte Wochentage eingeschränkt werden. Feiertage, sofern sie in der *Feiertage-Tabelle* hinterlegt wurden, werden ebenfalls beachtet. Sommer / Winterzeit wird ebenfalls anhand der eingestellten Zeitzone beachtet.

Voreingestellt sind die Zeitrahmen ALWAYS und NEVER. Weitere Zeitrahmen können Sie in LANconfig konfigurieren unter **Datum/Zeit** > **Konfiguration** > **Zeitrahmen**. Im gleichen Bereich finden Sie auch die Möglichkeit, für die Zeitrahmen Feiertage vorzugeben.



Name

Hier muss der Name des Zeitrahmens angegeben werden, über den dieser bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil.

Startzeit

Hier kann die Startzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil gelten soll.

Stoppzeit

Hier kann die Stoppzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein 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.

Wochentage

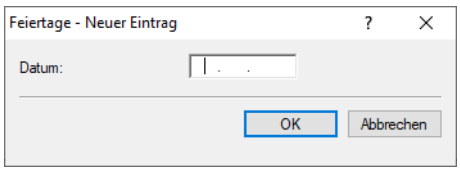
Hier können Sie die Wochentage auswählen, an denen der Zeitrahmen gültig sein soll.

Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren.

Feiertage

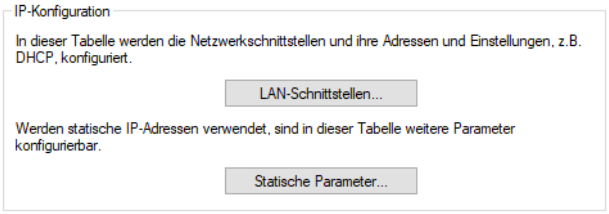


Geben Sie hier die Feiertage an, die in Zeitrahmen berücksichtigt werden sollen.

Das Jahr 0 steht für ein beliebiges Jahr.

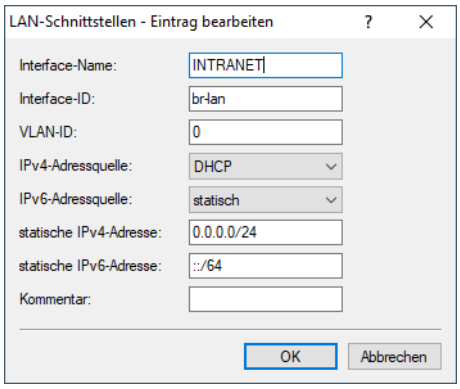
4.3 IP-Konfiguration

Die Einstellungen für die IP-Konfiguration Ihres Gerätes finden Sie unter **IP-Konfiguration** > **Konfiguration**.



4.3.1 LAN-Schnittstellen

Bearbeiten Sie unter **IP-Konfiguration** > **Konfiguration** > **LAN-Schnittstellen** grundsätzliche Konfigurationsoptionen rund um die eigenen IP-Einstellungen und den Netzwerkzugriff des Gerätes.



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.

Interface-ID

Der interne Bezeichner für das Interface.

VLAN-ID

Legen Sie hier eine VLAN-ID fest, für die das Interface aktiv und erreichbar sein soll. Der Standardwert „0" bedeutet, dass kein VLAN verwendet wird.

IPv4-Adressquelle

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

DHCP

Die IP-Adresse wird via DHCP bezogen.

Statisch

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

IPv6-Adressquelle

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

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.

Statisch

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

Statische IPv4-Adresse

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

Statische IPv6-Adresse

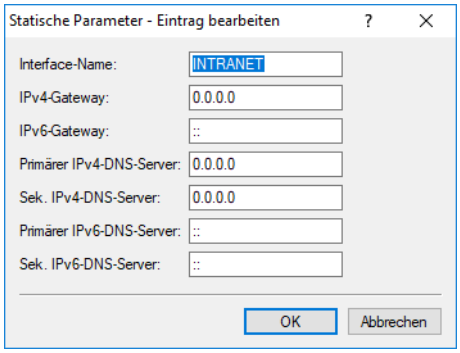
Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als IPv6-Adressquelle **Statisch** eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/64“).

Kommentar

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

4.3.2 Statische Parameter

Bearbeiten Sie unter **IP-Konfiguration** > **Konfiguration** > **Statische Parameter** weitere 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 **Statisch** gewählt haben. Ansonsten werden alle notwendigen Informationen z. B. via DHCP bezogen, sodass in dieser Tabelle keinerlei Konfiguration notwendig ist.

Interface-Name

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

IPv4-Gateway

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

IPv6-Gateway

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

Primärer IPv4-DNS-Server

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

Sekundärer IPv4-DNS-Server

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

Primärer IPv6-DNS-Server

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

Sekundärer IPv6-DNS-Server

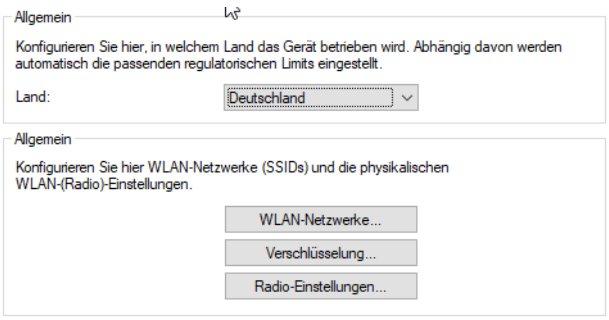
Konfigurieren Sie hier den sekundären IPv6-DNS-Server für das referenzierte Interface.

4.4 Wireless-LAN

Im Abschnitt **Wireless-LAN** finden Sie alle Einstellungen rund um das Ausstrahlen von WLAN-Netzwerken.

4.4.1 WLAN-Netzwerke

Die Einstellungen für WLAN-Netzwerke Ihres Gerätes finden Sie unter **Wireless-LAN** > **WLAN-Netzwerke**.



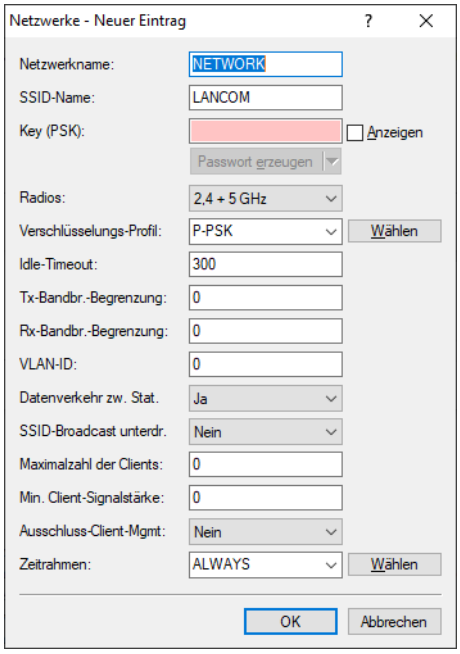
Allgemein

Land

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

Netzwerke

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Netzwerke** 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.



Netzwerkname

Wählen 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. Dieser wird im nächsten Schritt konfiguriert.

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.

Key (PSK)

Konfigurieren Sie hier den Pre-shared Key (PSK), der für das WLAN-Netzwerk verwendet wird. Wenn Sie **Anzeigen** auswählen, dann können Sie über **Passwort erzeugen** ein zufällig erzeugtes Passwort erstellen. Über den Pfeil daneben können Sie die Stärke, Länge und einige Einstellungen zu verwendeten Zeichen des erzeugten Pre-shared Key einstellen.

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.

Radios

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

2,4 GHz + 5 GHz

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

2,4 GHz

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

5 GHz

Die SSID wird nur auf der Frequenz 5 GHz ausgestrahlt.

keiner

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

Verschlüsselungs-Profil

Wählen Sie hier ein Verschlüsselungs-Profil, welches definiert, welches Authentisierungs- und Verschlüsselungsverfahren für die SSID zum Tragen kommen soll.

Standardmäßig sind folgende Verschlüsselungsprofile hinterlegt und können ausgewählt werden:

P-NONE

Keine Verschlüsselung, die SSID ist offen.

P-PSK

Das Authentisierungsverfahren WPA2 mit Pre-Shared-Key (PSK), auch bekannt als WPA2-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA2-3

Das Authentisierungsverfahren WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA3

Das Authentisierungsverfahren WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA3-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

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.

Tx-Bandbreiten-Begrenzung

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

Rx-Bandbreiten-Begrenzung

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

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.

Datenverkehr zwischen Stationen

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.

SSID-Broadcast unterdrücken

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.

Maximalzahl der Clients

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

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

Minimale Client-Signalstärke

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.

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

Ausschluss-Client-Management

Nimmt diese SSID gegebenenfalls vom Band Steering aus.

Zeitrahmen

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

Verschlüsselung

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Verschlüsselung** alle Einstellungen rund um die Verschlüsselung und Authentisierung der WLAN-Netzwerke. Standardmäßig sind folgende Verschlüsselungsprofile hinterlegt und können in der Konfiguration der WLAN-Netzwerke verwendet werden:

P-NONE

Keine Verschlüsselung, die SSID ist offen.

P-PSK

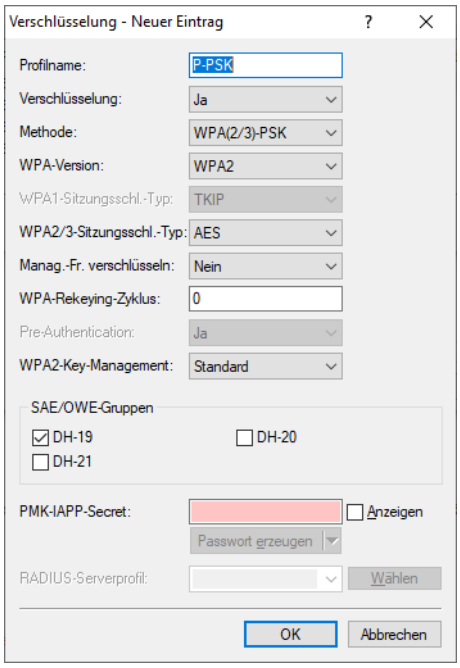
Das Authentisierungsverfahren WPA2 mit Pre-Shared-Key (PSK), auch bekannt als WPA2-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA2-3

Das Authentisierungsverfahren WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.

P-PSK-WPA3

Das Authentisierungsverfahren WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA3-Personal, kommt zum Einsatz. Für das WLAN-Netzwerk muss ein Key konfiguriert sein.



Profilname

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

Verschlüsselung

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

Methode

Konfigurieren Sie hier die Verschlüsselungsmethode. Folgende Methoden stehen zur Auswahl:

WPA

- WPA(2/3)-PSK: WPA2 und / oder WPA3 mit Pre-Shared-Key (PSK), auch bekannt als WPA-Personal
- WPA(2/3)-802.1X: WPA2 und / oder WPA3 mit 802.1X, auch bekannt als WPA-Enterprise

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

WEP

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.

- 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.

WPA-Version

Wi-Fi Protected Access (WPA) ist eine Verschlüsselungsmethode. Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden WPA(2)-PSK und WPA(2)-802.1X verwendet werden. Folgende Versionen stehen zur Auswahl:

- 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.

WPA1-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

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.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg 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.

WPA2/3-Sitzungsschlüssel-Typ

Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Versionen 2 und 3 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren. Folgende Typen stehen zur Auswahl:

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.

Der Einsatz von TKIP wird nur beim Betrieb von älteren WLAN-Clients empfohlen, die keine Unterstützungg 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.

Management-Frames verschlüsseln

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.

WPA-Rekeying-Zyklus

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.

In der Standardeinstellung ist der Wert auf „0“ eingestellt, so dass keine vorzeitige Aushandlung des Schlüssels erfolgt.

Pre-Authentication

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

Normalerweise scannt ein WLAN-Client im Hintergrund die Umgebung nach vorhandenen Access Points, um sich ggf. mit einem von ihnen neu verbinden zu können. Access Points, 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 Access Point über das Infrastruktur-Netzwerk an, das die Access Points 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 Access Point sowie alle anderen Netzwerkpartner die Prä-Authentifizierung als normale Datenübertragung des WLAN-Clients.
- Nach erfolgreicher Prä-Authentifizierung speichern jeweils der neue Access Point 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 Access Point verbinden möchte, kann er sich dank des gespeicherten PMKs schneller anmelden. Der weitere Ablauf entspricht dem PMK-Caching.

WPA2-Key-Management

Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll. 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. Siehe auch *Fast Roaming* auf Seite 12.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

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.

SAE/OWE-Gruppen

Enthält die Auswahl der angebotenen Diffie-Hellman-Gruppen, 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.

DH-19

256-bit random ECP group

DH-20

384-bit random ECP group

DH-21

521-bit random ECP group

PMK-IAPP-Secret

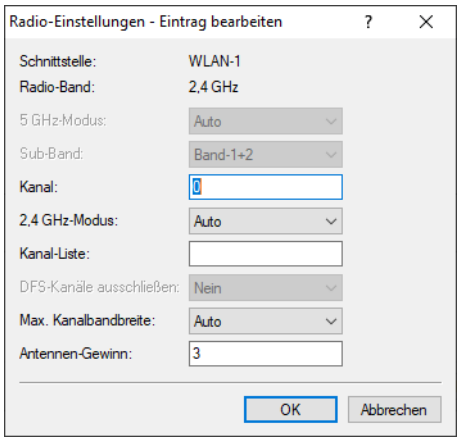
Diese Passphrase wird verwendet, um verschlüsseltes Opportunistic Key Caching zu realisieren. Dies ist erforderlich, um Fast Roaming über IAPP zu verwenden. Dabei muss jeder Schnittstelle in den WLAN-Verbindungseinstellungen eine individuelle IAPP-Passphrase zugewiesen werden. Diese wird verwendet, um 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.

RADIUS-Serverprofil

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. Die Profile erzeugen Sie unter *RADIUS* auf Seite 49.

Radio-Einstellungen

Konfigurieren Sie unter **Wireless-LAN** > **WLAN-Netzwerke** > **Radio-Einstellungen** 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.



Schnittstelle

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

Radio-Band

Zeigt an, ob diese Schnittstelle im 2,4-GHz- oder 5-GHz-Frequenzbereich arbeitet.

5 GHz-Modus

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:

Auto

Es werden alle vom Gerät unterstützten Modi verwendet.

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.

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

Sub-Band

Konfigurieren Sie hier, welche Sub-Bänder im 5-GHz-Modus verwendet werden. Folgende Sub-Bänder stehen zur Auswahl:

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 wird sowohl das Sub-Band 1, als auch das Sub-Band 2 verwendet.

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

Kanal

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

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

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.

2,4 GHz-Modus

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. Folgende Modi stehen zur Auswahl:

Auto

Es werden alle vom Gerät unterstützten Modi verwendet.

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.

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

Kanal-Liste

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.

DFS-Kanäle ausschließen

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 **DFS-Kanäle ausschließen** im Radio-Kanal und in der **Kanal-Liste** fest konfiguriert werden.

Max. Kanalbandbreite

Konfigurieren Sie hier die maximal erlaubte Kanalbandbreite. Folgende Einstellungens stehen zur Auswahl:

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.

20 MHz

Die Kanalbandbreite beträgt immer 20 MHz.

40 MHz

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

80 MHz

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

160 MHz

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

Antennen-Gewinn

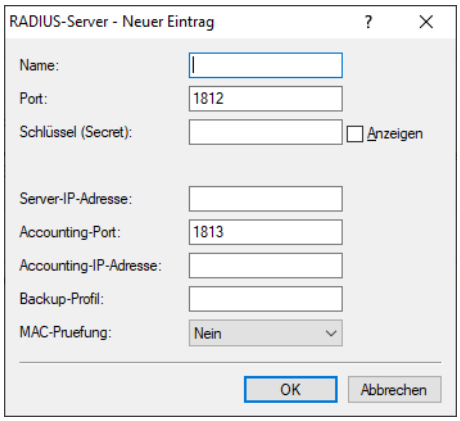
Wenn Antennen mit einer höheren Sendeleistung eingesetzt werden, als in dem jeweiligen Land zulässig, ist eine Dämpfung der Leistung auf den zulässigen Wert erforderlich. Hier wird der Gewinn der Antenne abzüglich der tatsächlichen Kabeldämpfung eingetragen. Bei einer AirLancer Extender O-18a-Antenne mit einem Gewinn von 18 dBi wird bei einer Kabellänge von 4 m Länge mit einer Dämpfung 1 dB/m ein Antennen-Gewinn von 18 - 4 = 14 eingetragen. Aus diesem tatsächlichen Antennengewinn wird dann dynamisch unter Berücksichtigung der anderen eingestellten Parameter wie Land, Datenrate und Frequenzband die maximal mögliche Leistung berechnet und abgestrahlt.

Nur bei Geräten mit externen Antennen verfügbar.

4.4.2 RADIUS

Die Einstellungen für RADIUS-Server-Profile zur Verwendung mit WLAN-Netzwerken, die 802.1X als Authentisierungsverfahren verwenden, finden Sie unter **Wireless-LAN** > **RADIUS**.

Konfigurieren Sie die RADIUS-Server-Profile in der Tabelle **RADIUS-Server**.



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.

Port

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

Normalerweise ist dies der Port 1812 (RADIUS Authentication).

Schlüssel (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.

Server-IP-Adresse

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

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).

Accounting-IP-Adresse

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

Backup-Profil

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

MAC-Prüfung

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

Dynamic VLAN für 802.1X

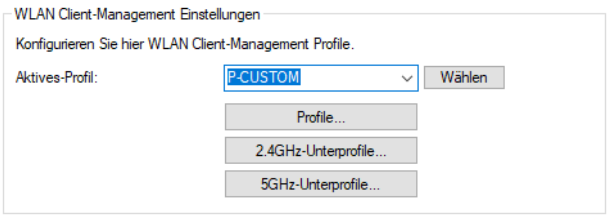
Mit Dynamic VLAN kann der RADIUS-Server im Rahmen einer 802.1X-Anmeldung die VLAN-ID für den WLAN-Client zuweisen. Clients lassen sich somit dem gewünschten VLAN zuweisen, ohne dafür je VLAN eine separate SSID bereitstellen zu müssen.

Der RADIUS-Server muss dazu folgende Attribute in der Accept-Nachricht mitsenden:

ID	Bezeichnung	Bedeutung	Mögliche Werte in LCOS LX
64	Tunnel-Type	Definiert das Tunneling-Protokoll, welches für die Sitzung verwendet wird.	13 (VLAN)
65	Tunnel-Medium-Type	Definiert das Transportmedium, über das eine getunnelte Sitzung hergestellt wird.	6 (IEEE 802)
81	Tunnel-Private-Group-Id	Definiert die gewünschte VLAN-ID.	1-4096

4.4.3 Client Management

Die Einstellungen zum Band Steering für WLAN-Netzwerke finden Sie unter **Wireless-LAN** > **Client-Management**.



Aktives Profil

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

P-DEFAULT

Steering erfolgt anhand der Mediumsauslastung und der erkannten Interferenz 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-DISABLED

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

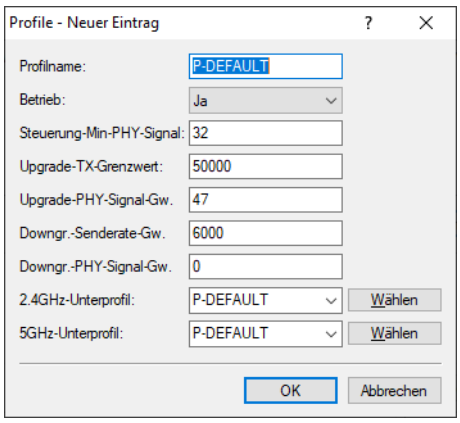
P-LEGACY

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.

Profile

Passen Sie unter **Wireless-LAN** > **Client-Management** > **Profile** die Detaileinstellungen der Steering-Profile an oder erstellen Sie ein neues Profil.

LANCOM empfiehlt die Verwendung der voreingestellten Profile.



Profilname

Geben Sie diesem Profil einen Namen.

Betrieb

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

Steuerung-Min-PHY-Signal

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

Upgrade-TX-Grenzwert

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

Upgrade-PHY-Signal-Grenzwert

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.

Downgrade-Senderate-Grenzwert

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.

Downgrade-PHY-Signal-Grenzwert

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 **Abwertung-Senderate-Grenzwert** erreicht werden.

2,4-GHz-Unterprofil

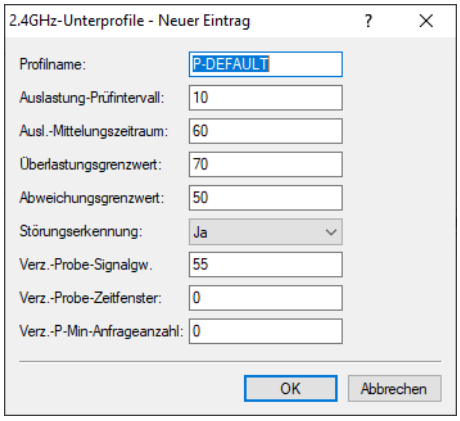
Konfigurieren Sie hier, welches 2,4-GHz-Unterprofil zur Anwendung kommt.

5-GHz-Unterprofil

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

2,4-GHz-Unterprofile

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **2,4 GHz-Unterprofile** die Einstellungen der 2,4-GHz-Unterprofile.



Profilname

Geben Sie diesem 2,4-GHz-Unterprofil einen aussagekräftigen Namen.

Auslastung-Prüfintervall

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

Auslastung-Mitteilungszeitraum

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

Überlastungsgrenzwert

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

Abweichungsgrenzwert

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.

Störungserkennung

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

Verzögerung Probe-Signalgrenzwert

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

Verzögerung Probe-Zeitfenster

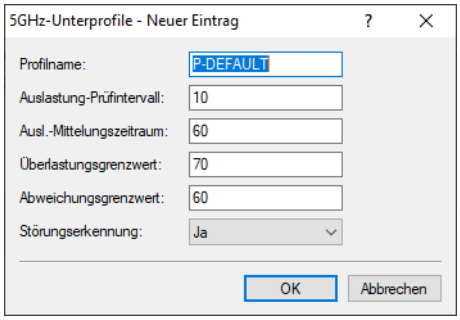
Konfiguriert das Zeitfenster (in Sekunden), in dem von einem Client mindestens so viele Probe Requests empfangen werden müssen, wie es unter **Verzögerung Probe-Min.-Anfrageanzahl** konfiguriert wurde, damit diese beantwortet werden.

Verzögerung Probe-Min.-Anfrageanzahl

Konfiguriert die Anzahl an Probe Requests, die von einem Client im unter **Verzögerung Probe Zeitfenster** konfigurierten Zeitraum empfangen werden müssen, damit diese beantwortet werden.

5-GHz-Unterprofile

Konfigurieren Sie unter **Wireless-LAN** > **Client-Management** > **5 GHz-Unterprofile** die Einstellungen der 5-GHz-Unterprofile.



Profilname

Geben Sie diesem 5-GHz-Unterprofil einen aussagekräftigen Namen.

Auslastung-Prüfintervall

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

Auslastung-Mitteilungszeitraum

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

Überlastungsgrenzwert

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

Abweichungsgrenzwert

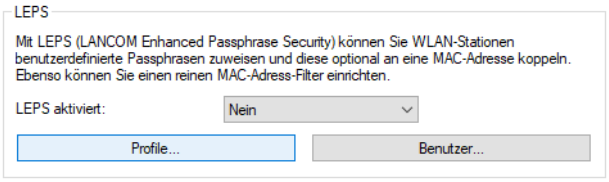
Konfiguriert die Mediumsauslastung (in Prozent), die zusammen mit der erwarteten Mediumsauslastung erreicht werden darf, bevor jedes weitere Downgrade-Steering bis zur nächsten Ermittlung der Mediumslast eingestellt wird.

Störungserkennung

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

4.4.4 Stationen / LEPS

Die Konfiguration der **Profile** und **Benutzer** für LANCOM Enhanced Passphrase Security (LEPS) finden Sie in LANconfig unter **Wireless-LAN** > **Stationen / LEPS** > **LEPS**. Über den Schalter **LEPS aktiviert** wird LEPS eingeschaltet.



Bei der Konfiguration von LEPS wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-Profile angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut vorgenommen werden müssen. Anschließend legen Sie die LEPS-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-Profile.

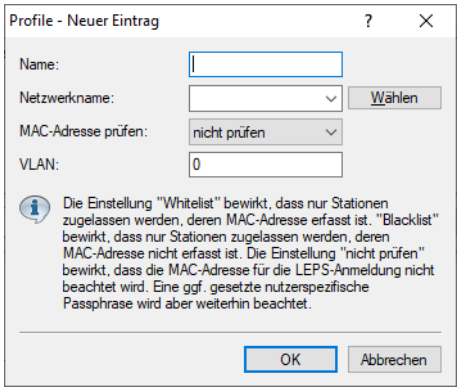
Alternativ können Sie die Passphrase mit einer MAC-Adresse verbinden und auf diese Weise einen MAC-Adress-Filter einrichten.

Aus technischen Gründen ist LEPS nur mit der WPA-Version WPA2 kompatibel.

Beachten Sie, dass bei dem Verschlüsselungsmodus WPA2/3 der Client beide WPA-Versionen verwenden kann, was in Verbindung mit LEPS zu unvorhergesehenem Verhalten führen kann.

Profile

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden.



Name

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

Netzwerkname

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.

MAC-Adresse prüfen

Mögliche Werte:

Nicht prüfen

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.

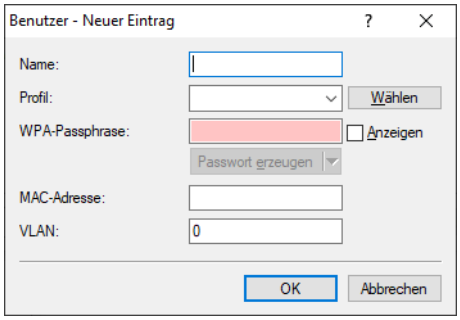
VLAN

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

Benutzer

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger

Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert und dem in dieser Tabelle konfigurierten VLAN zugewiesen. Wird hier kein VLAN zugewiesen, wird er dem am Profil konfigurierten VLAN zugewiesen. Einstellungen am einzelnen Benutzer haben somit Priorität gegenüber Einstellungen am Profil.



Name

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

Profil

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.

WPA-Passphrase

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

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

MAC-Adresse

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.

Im Vergleich zur reinen Zuweisung einer Passphrase an einen Benutzer ist die Verwaltung einer Passphrase pro MAC-Adresse etwas aufwändiger bei gleichzeitig höherer Kontrolle über die Geräte im Netz.

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 beim LEPS-Benutzer ein VLAN konfiguriert, gilt die hier konfigurierte VLAN.

4.4.5 WLC

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.

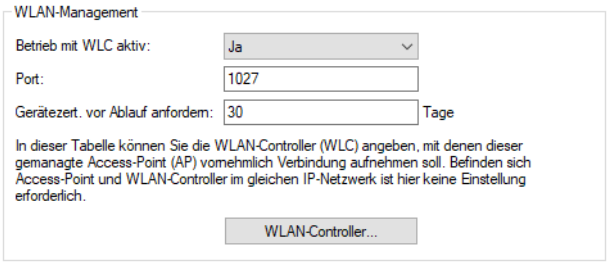
Für Hintergrundinformationen zum WLAN-Management mit LANCOM WLAN-Controllern, konsultieren Sie den Abschnitt „WLAN-Management“ im LCOS-Referenzhandbuch.

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.

Wird der Access Point von der LANCOM Management Cloud verwaltet und in diesem Zusammenhang durch die LMC eine WLAN-Konfiguration auf den Access Point ausgerollt, wird dieser nicht weiter versuchen, einen WLC 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 mit LANconfig unter **Wireless-LAN** > **WLC** möglich.



Betrieb mit WLC aktiv

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.

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.

Gerätezertifikat vor Ablauf anfordern

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

WLAN-Controller

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.

Unterstützte Features

In LCOS LX werden folgende Features im Rahmen des WLC-Betriebs unterstützt:

Bereich	Feature	Unterstützt?
Allgemein	Passwortsynchronisation	Ja
	WLC-Tunnel	Nein
	WLAN-Zeitsteuerung	Ja
Logische WLAN-Konfiguration	VLAN-Tagging	Ja
	WPA2	Ja
	WPA3	Ja
	Enhanced Open	Ja
	Enhanced Open Transitional	Nein

Bereich	Feature	Unterstützt?
	802.1X	Ja
	RADIUS-Profile	Ja
	Autarker Modus	Ja
	802.11u/Hotspot 2.0	Nein
	OKC	Nein
	MAC-Prüfung	Ja
	RADIUS-Accounting	Ja
	Inter-Station-Traffic	Ja
	Fast Roaming	Ja
	Basisrate einstellbar	Nein
	Client-Bridge-Unterstützung	Nein
	Bandbreitenbegrenzung per SSID	Ja
	Bandbreitenbegrenzung per Client	Nein
	Maximalzahl der Clients	Ja
	Min. Client-Signalstärke	Ja
	Client-Trennen-Signalstärke	Nein
	LBS	Nein
	In Unicast konvertieren	Nein
	Nur Unicasts übertragen	Nein
	U-APSD	Dauerhaft eingeschaltet
	Mgmt-Frames verschlüsseln	Ja
Physikalische WLAN-Parameter	Landeseinstellung	Ja
	2,4 GHz-Modus konfigurieren	Ja
	5 GHz-Modus konfigurieren	Ja
	5 GHz-Unterbänder konfigurieren	Ja
	DTIM-Periode einstellen	Nein
	Background-Scan-Intervall einstellen	Nein
	Antennen-Gewinn einstellen	Ja
	Sendeleistungs-Reduktion einstellen	Nein
	VLAN-Modul aktivieren[1]	–
	ARC: Client Steering	Ja[2]
	ARC: Adaptive RF Optimization	Nein

[1] Bei LCOS LX nicht notwendig.

[2] Aktuell wird nur AP-basiertes Band Steering unterstützt. Die Einstellungen **bevorzugtes Frequenzband** und **Ablaufzeit Probe Requests** haben keinen Einfluss.

Bereich	Feature	Unterstützt?
	QoS nach 802.11e einschalten	Dauerhaft eingeschaltet
	Indoor-Only-Modus aktivieren	Ja
	Unbekannte gesehene Clients melden	Nein
Allgemein/Profil	Angabe alternativer WLCs	Nein
	Konfigurations-Verzögerung	Nein
	LED-Profile	Ja
	Wireless ePaper	Nein
	Wireless IDS	Nein
	AutoWDS	Nein
	IP-Parameter-Profile	Ja
	Firmware-Management	Ja
	Skript-Management	Nein
	LEPS-U	Ja
	LEPS-MAC	Ja
	Zuweisung einer VLAN ID via LEPS-MAC (Dynamic VLAN)	Ja
	ARC: Funkfeldoptimierung	Nein

5 Features über WEBconfig konfigurieren

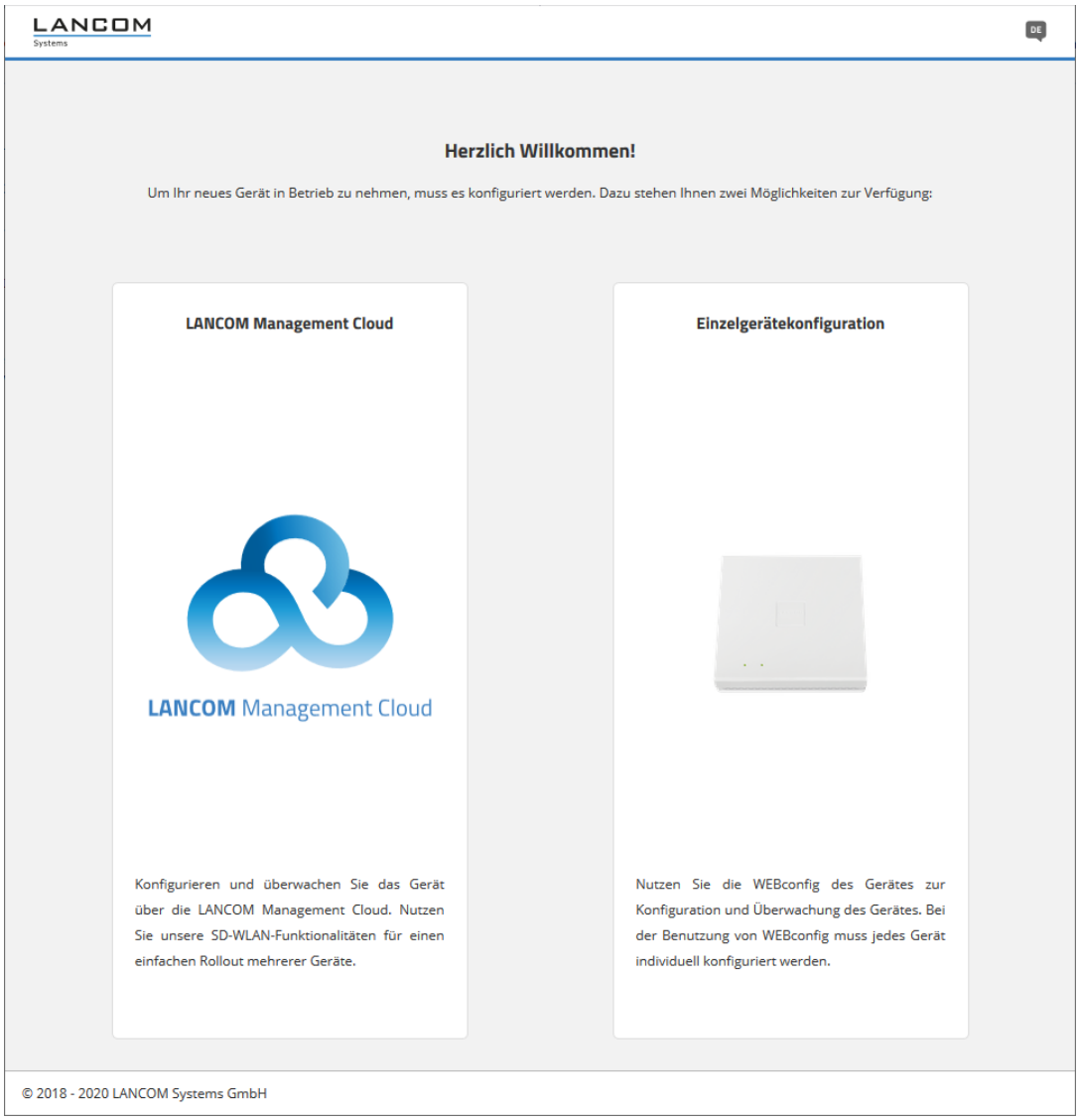
Im Folgenden wird die Inbetriebnahme über WEBconfig sowie alle Einstellungsmöglichkeiten in WEBconfig erläutert. Diese sind abhängig vom Gerät, sodass nicht immer alle aufgeführten Optionen zur Verfügung stehen.

5.1 Inbetriebnahme eines Gerätes über WEBconfig

Sie erreichen die WEBconfig über HTTP und HTTPS. Im Falle von HTTP erfolgt automatisch eine Umleitung auf eine verschlüsselte HTTPS-Verbindung.

Da die WEBconfig mit einem selbst-signierten SSL-Zertifikat arbeitet, muss dieses einmalig (pro Gerät) im Browser als Ausnahme hinzugefügt werden.

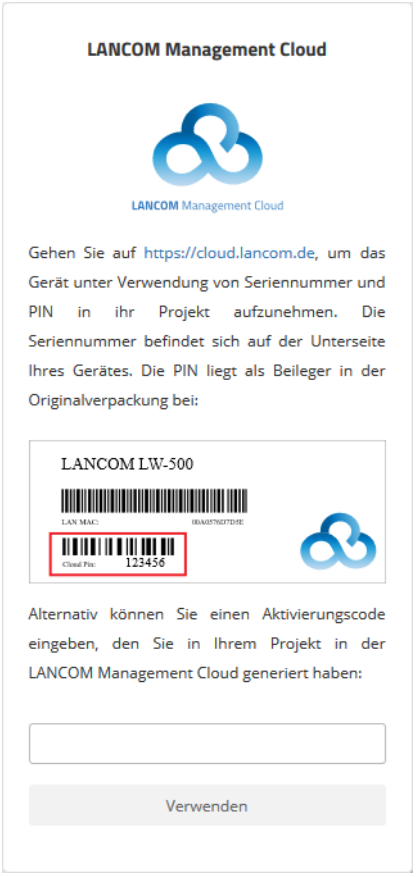
Nach Aufruf der WEBconfig-Oberfläche eines unkonfigurierten Gerätes kann ausgewählt werden, ob das Gerät zukünftig mit der LANCOM Management Cloud verwaltet werden soll oder als Stand-alone-Gerät verwaltet werden soll.



Wählen Sie hier durch einen Klick auf die entsprechende Schaltfläche aus, ob das Gerät zukünftig mit der LANCOM Management Cloud verwaltet werden soll, oder als Stand-alone-Gerät verwaltet werden soll.

5.1.1 Verwaltung über LANCOM Management Cloud

Verbinden Sie das Gerät entweder mittels Seriennummer und PIN mit der LANCOM Management Cloud (Zero-Touch) oder geben Sie in das entsprechende Eingabefeld einen Aktivierungscode ein, den Sie vorab in Ihrem LANCOM Management Cloud-Projekt generiert haben:

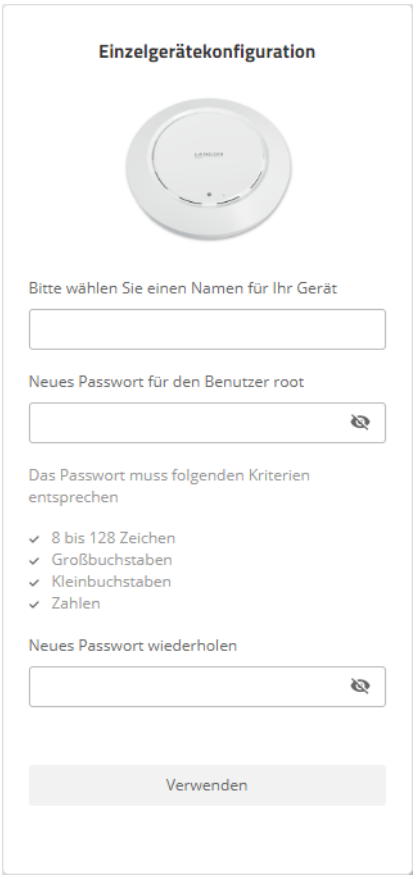


Nach Bestätigung des Aktivierungscodes und Abschluss des Verbindungsvorgangs erhalten Sie eine Erfolgsmeldung und werden auf die Anmeldeseite der WEBconfig weitergeleitet. Das Gerät kann nun über die LMC verwaltet werden.

5.1.2 Verwaltung über Einzelgerätekonfiguration

Legen Sie in den entsprechenden Eingabefeldern einen sprechenden Namen für Ihr Gerät fest und wählen Sie ein Passwort, welches für den Benutzer „root“ verwendet werden soll. Klicken Sie ggfs. auf das durchgestrichene Auge, um sich das von Ihnen eingegebene Passwort anzeigen zu lassen.

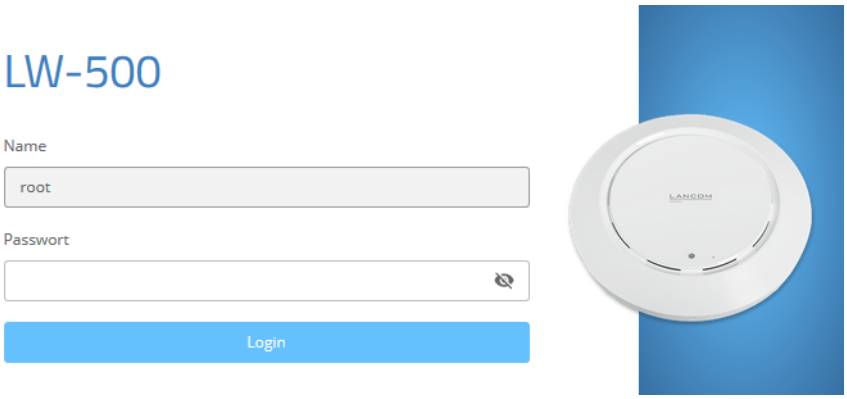
Das hier festgelegte Passwort ist immer für den Benutzer „root“ gültig. Dieser Benutzer wird auch für die spätere Anmeldung an der WEBconfig verwendet.



Nach Klick auf **Verwenden** werden Sie auf die Anmeldeseite geleitet und können sich mit dem Benutzernamen „root“ und dem zuvor festgelegten Passwort an der WEBconfig anmelden.

5.2 Login

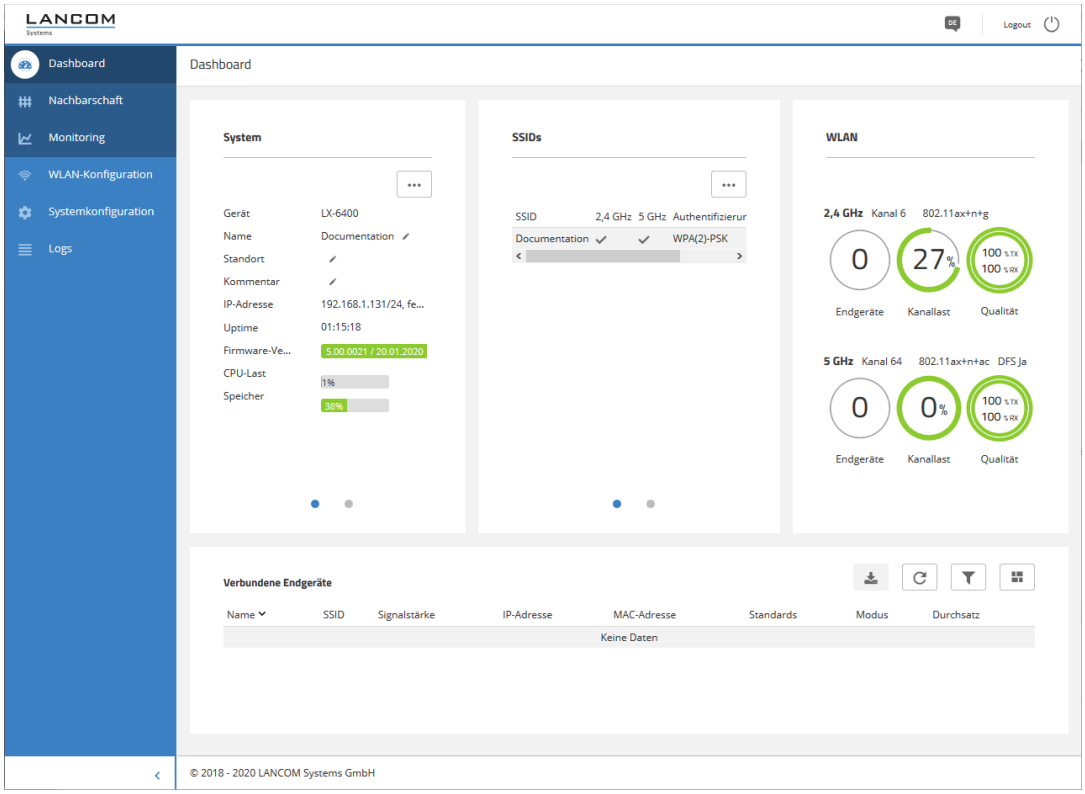
Geben Sie für die Anmeldung den Benutzernamen „root“ und das von Ihnen vergebene Passwort an:



Nach der Anmeldung an der WEBconfig gelangen Sie auf das Dashboard. Informationen zum Dashboard finden Sie im Abschnitt *WEBconfig – Dashboard* auf Seite 63.

5.3 WEBconfig – Dashboard

Das Dashboard bietet eine Übersicht über die wichtigsten Betriebsdaten Ihres Gerätes.



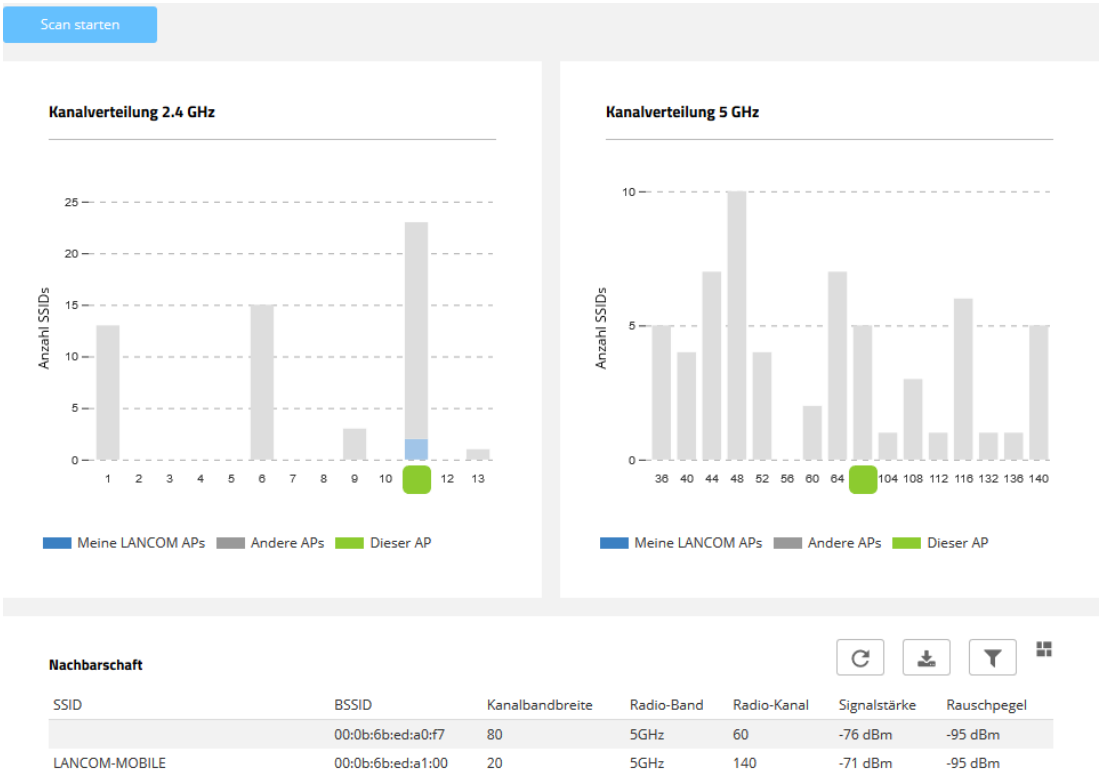
Unterhalb des Dashboards gibt es die Bereiche **Nachbarschaft** und **Monitoring**.

5.3.1 Nachbarschaft

Sie erreichen die Nachbarschaftsübersicht über den Punkt **Nachbarschaft** in der Sidebar.

Die Nachbarschaftsübersicht kann dabei helfen, einen Überblick über die WLAN-Umgebung, insbesondere die in der Umgebung aktiven WLAN Access Points und WLAN-Router zu erhalten.

Klicken Sie den Button **Scan starten**, um die WLAN-Umgebung erfassen zu lassen. Nach Abschluss des Scans (Dauer: ca. 10 Sekunden) werden die verschiedenen Diagramme und Tabellen mit den Ergebnissen befüllt:



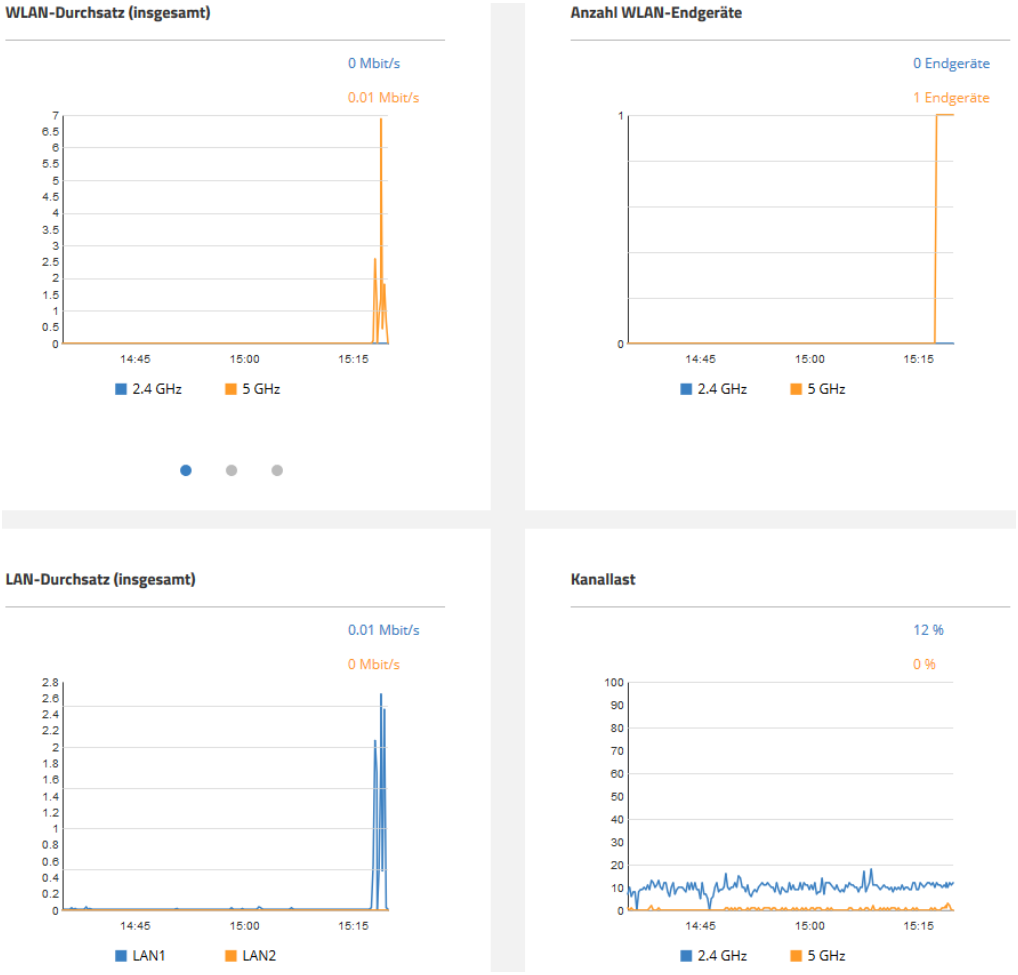
Die oberen beiden Balkendiagramme visualisieren, wie viele SSIDs vom Gerät auf den verschiedenen 2,4-GHz- und 5-GHz-Kanälen erkannt wurden und potentiell eine Belastung des Mediums auf diesem Kanal darstellen. LANCOM Access Points, die vom Scan erkannt wurden und gleicheitig im gleichen LAN-Netzwerk erreichbar sind, wie das aktuelle Gerät, werden in den Diagrammen als „Meine LANCOM APs" besonders hervorgehoben. Zusätzlich wird visualisiert, auf welchem WLAN-Kanal das aktuelle Gerät selber arbeitet. Die Tabelle **Nachbarschaft** liefert zusätzlich detaillierte Ausgaben zu den vom Scan erkannten SSIDs, z. B. den Namen, die BSSID (MAC-Adresse) und die Signalstärke.

5.3.2 Monitoring

Sie erreichen den Bereich Monitoring über den Punkt **Monitoring** in der Sidebar.

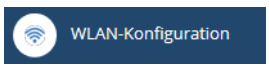
Die Monitoring-Ansicht bietet Graphen zur zeitlichen Visualisierung des WLAN-Durchsatzes, des LAN-Durchsatzes, der Anzahl der WLAN-Stationen sowie der Kanalauslastung.

Historische Daten werden maximal für die Laufzeit der aktuellen WEBconfig-Sitzung angezeigt.



5.4 WLAN-Konfiguration

Sie erreichen diesen Bereich über den Punkt **WLAN-Konfiguration** in der Sidebar.



5.4.1 Konzept

Die WLAN-Konfiguration wurde mit dem Ziel entworfen, den Nutzer bei den am häufigsten verwendeten Konfigurationsarbeiten zu unterstützen und die mühevolle Konfiguration kleiner Details unnötig zu machen. Gleichzeitig ist aber weiterhin die Konfiguration davon abweichender Szenarien möglich.

5.4.2 Bedienung

Die angelegten SSIDs werden tabellarisch dargestellt. Klicken Sie auf **Neue SSID hinzufügen**, um eine neue SSID zu konfigurieren. Danach wird eine neue Zeile hinzugefügt. Zur Konfiguration einer SSID mit WPA2-PSK ist nun nur noch das Ausfüllen der Felder **Name**, **SSID** und **WPA2-Schlüssel** erforderlich.

Je nach Bedarf ist es hier auch möglich, einen sicheren WPA2-Schlüssel automatisch generieren zu lassen ( ) sowie die verwendeten Frequenzbänder einzuschränken. Standardmäßig wird die SSID auf 2,4 GHz und 5 GHz ausgestrahlt.

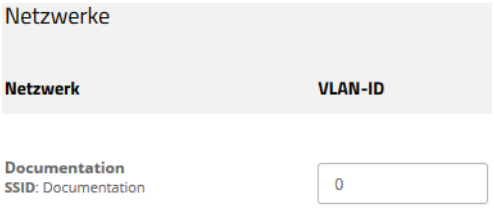
Klicken sie anschließend auf **Speichern**, um die SSID zu übernehmen. Diese wird dann ab sofort vom Gerät ausgestrahlt.

Auf dem 5-GHz-Band kann es bis zu einer Minute nach der erstmaligen Konfiguration dauern, bis die SSID ausgestrahlt wird, da es regulatorisch vorgeschrieben ist, das Band für eine Minute auf Primärnutzer zu überwachen („Radarerkennung", DFS).

Eine weitergehende individuelle Konfiguration ist durch einen Klick auf die jeweilige Überschrift möglich.

Netzwerke

Für jede eingerichtete SSID können Sie hier die folgenden Parameter einstellen:



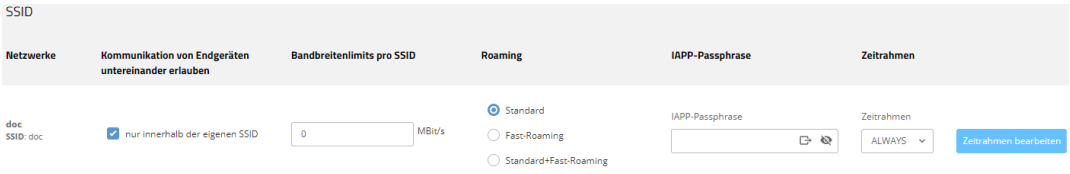
VLAN-ID

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.

SSID

Für jede eingerichtete SSID können Sie hier die folgenden Parameter einstellen:



Kommunikation von Endgeräten untereinander erlauben

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

Bandbreitenlimits pro SSID

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

Roaming

Einstellungen zum Wechsel eines Clients von einem Access Point zu einem anderen Access Point, der die gleiche SSID ausstrahlt.

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 Prä-Authentifizierung verwenden.

Fast-Roaming

Aktiviert Fast Roaming gemäß dem Standard IEEE 802.11r. Siehe auch *Fast Roaming* auf Seite 12.

Fast Roaming zwischen LCOS- und LCOS LX-basierten Geräten ist möglich.

Standard+Fast-Roaming

Eine Kombination aus dem Standardverhalten 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.

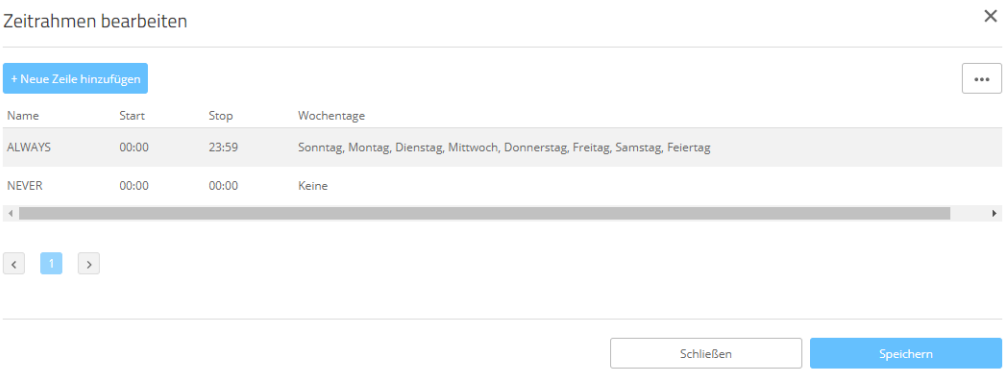
IAPP-Passphrase

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.

Zeitrahmen

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 hier hinzu, damit er für diese SSID beachtet wird.

Zeitrahmen bearbeiten



Name

Hier muss der Name des Zeitrahmens angegeben werden, über den dieser bei einer WLAN-SSID referenziert wird. Mehrere Einträge gleichen Namens ergeben dabei ein gemeinsames Profil. Voreingestellt sind die Zeitrahmen ALWAYS und NEVER.

Start

Hier kann die Startzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil gelten soll.

Stopp

Hier kann die Stoppzeit (Tageszeit) im Format HH:MM (Default: 00:00) angegeben werden, ab der das gewählte Profil nicht mehr gültig sein 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.

Wochentage

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

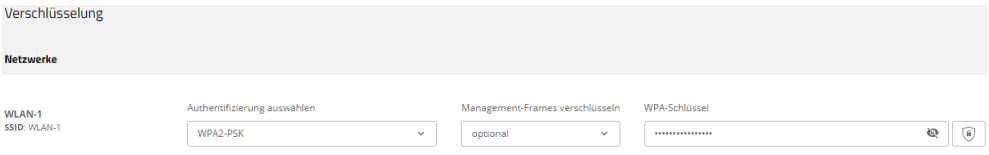
Mögliche Werte:

- Montag, Dienstag, Mittwoch, Donnerstag, Freitag, Samstag, Sonntag, Feiertag

Zeitschemata lassen sich mit gleichem Namen, aber unterschiedlichen Zeiten auch über mehrere Zeilen hinweg definieren.

Verschlüsselung

Für jede eingerichtete SSID können Sie hier die folgenden Parameter einstellen:



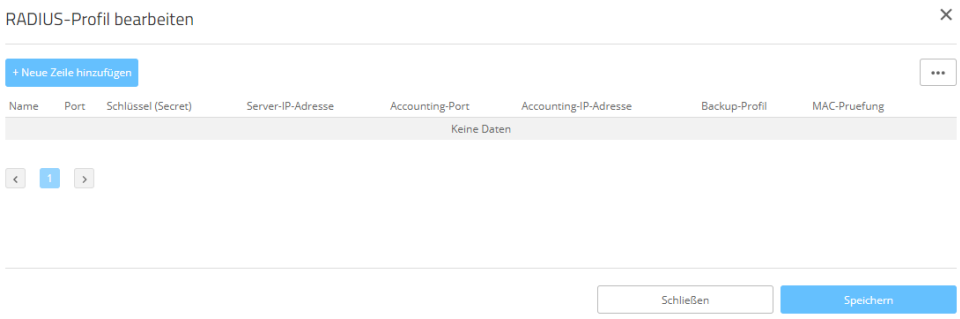
Authentifizierung auswählen

Ändern Sie hier die Verschlüsselungs- und Authentifizierungsmethode. Standardmäßig ist WPA2-PSK (WPA2 mit Pre-shared Key bzw. WPA2-Personal) voreingestellt. Wählen Sie optional **Keine Verschlüsselung** oder aus den folgenden Möglichkeiten:

- WPA3-PSK – WPA3 mit Pre-shared Key bzw. WPA3-Personal
- WPA(2+3)-PSK – WPA2 und / oder WPA3 mit Pre-Shared-Key
- WPA2-801.1X– WPA2 mit 802.1X bzw. WPA2-Enterprise
- WPA3-801.1X– WPA3 mit 802.1X bzw. WPA3-Enterprise
- WPA(2+3)-801.1X– WPA2 und / oder WPA3 mit 802.1X

Im Falle von Verfahren mit Pre-shared Key (PSK) müssen Sie einen **WPA-Schlüssel** eingeben. Schalten Sie die Anzeige über das durchgestrichene Auge um, damit Sie den Schlüssel lesen können. Je nach Bedarf ist es hier auch möglich, einen sicheren WPA-Schlüssel automatisch generieren zu lassen ( )

Im Falle von 802.1X müssen Sie ein RADIUS-Profil anlegen. Klicken Sie dazu auf **RADIUS-Profil bearbeiten** und fügen dort eine neue Zeile hinzu.



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.

Port

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

Normalerweise ist dies der Port 1812 (RADIUS Authentication).

Schlüssel (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.

Server-IP-Adresse

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

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).

Accounting-IP-Adresse

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

Backup-Profil

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

MAC-Prüfung

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

Beachten Sie, dass normalerweise dem RADIUS-Server das hier als RADIUS-Client agierende Gerät ebenfalls in seiner Konfiguration bekannt gemacht werden muss.

Sichern Sie die Änderungen durch Klick auf **Speichern**

Management-Frames verschlüsseln

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.

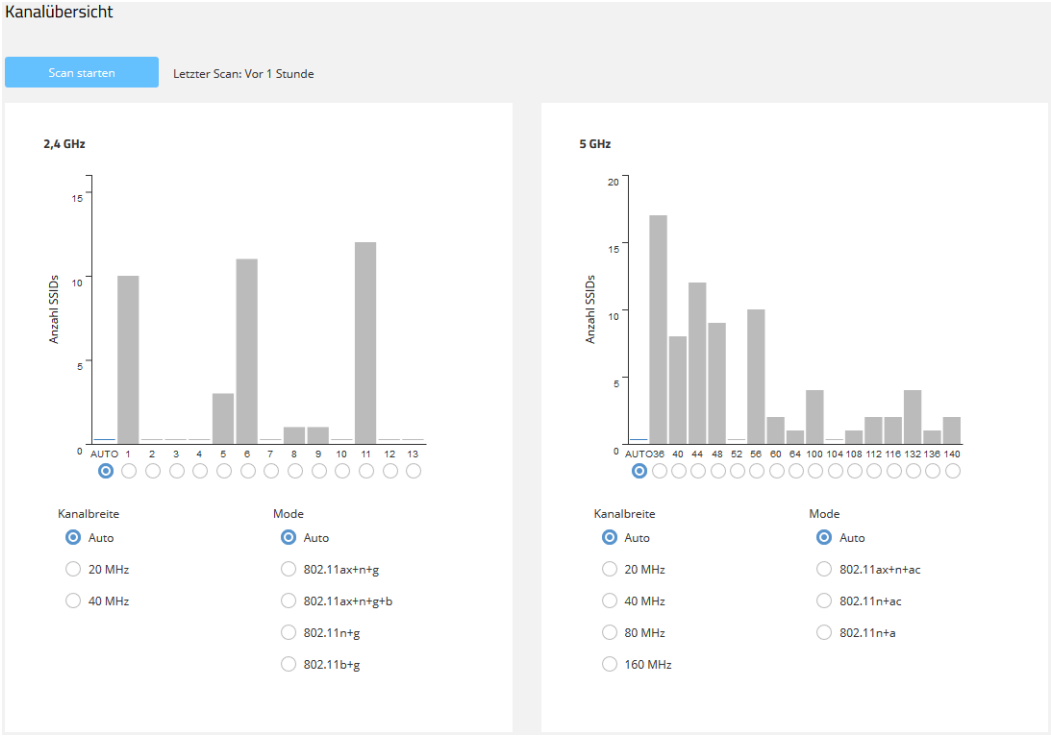
Der Standard IEEE 802.11w verschlüsselt die übertragenen Management-Informationen (Protected Management Frames, PMF), so dass ein Angreifer, der nicht im Besitz des entsprechenden Schlüssels ist, die Kommunikation nicht mehr stören kann.

Ab WPA3 müssen Management Frames verschlüsselt werden, daher wird dort dieser Wert ignoriert und als auf **Notwendig** gesetzt angenommen. Bei WPA2 ist diese Option optional.

Technologie

Die Seite **Technologie** bietet die Möglichkeit, feste Kanäle für das 2,4- und 5-GHz-Band festzulegen, sowohl die verwendete Kanalbreite und den verwendeten Radio-Modus zu bestimmen. Voreingestellt ist für alle Möglichkeiten die automatische Auswahl. Weiter unten auf der Seite finden Sie die Einstellungen zum Client-Management.

Die hier konfigurierbaren physikalischen Einstellungen gelten für das gesamte jeweilige Frequenzband und sind nicht SSID-spezifisch.

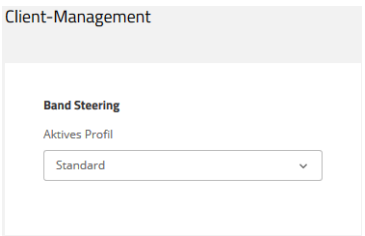


Die beiden Balkendiagramme visualisieren, wie viele SSIDs vom Gerät auf den verschiedenen 2,4- und 5-GHz-Kanälen erkannt wurden und potentiell eine Belastung des Mediums auf diesem Kanal darstellen.

Die Balkendiagramme werden nur mit Informationen befüllt, wenn zuvor entweder hier oder im Bereich **Nachbarschaft** ein Nachbarschaftsscan durchgeführt wurde.

Client Management

Die Einstellungen zum Band Steering für WLAN-Netzwerke finden Sie hier. Mittels Band Steering können Clients vom überlaufenen 2,4-GHz-Frequenzband auf das 5-GHz-Frequenzband gelenkt werden, so dass 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. Siehe auch *Band Steering* auf Seite 12.



Aktives Profil

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

Standard

Steering erfolgt anhand der Mediumsauslastung und der erkannten Interferenz 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.

Ausgeschaltet

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

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.

QR-Code

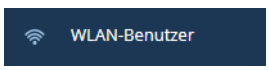
Diese Seite ermöglicht den Zugriff auf einen QR-Code für jede offene oder mit WPA2-PSK gesicherte SSID. Der QR-Code kann von aktuellen Smartphones (ggf. ist eine zusätzliche App erforderlich) gescannt werden und richtet das jeweilige WLAN automatisch auf dem Smartphone ein. So muss keine aufwändige Eingabe eines WLAN-Schlüssels erfolgen.

Zusätzlich besteht die Möglichkeit, einzelne QR-Codes separat auszudrucken.

Es können keine QR-Codes für mit 802.1X gesicherte Netze generiert werden, da diese keinen statischen WLAN-Schlüssel (PSK) verwenden.

5.4.3 WLAN-Benutzer

Sie erreichen diesen Bereich in der WEBconfig über den Punkt **WLAN-Benutzer** in der Sidebar.

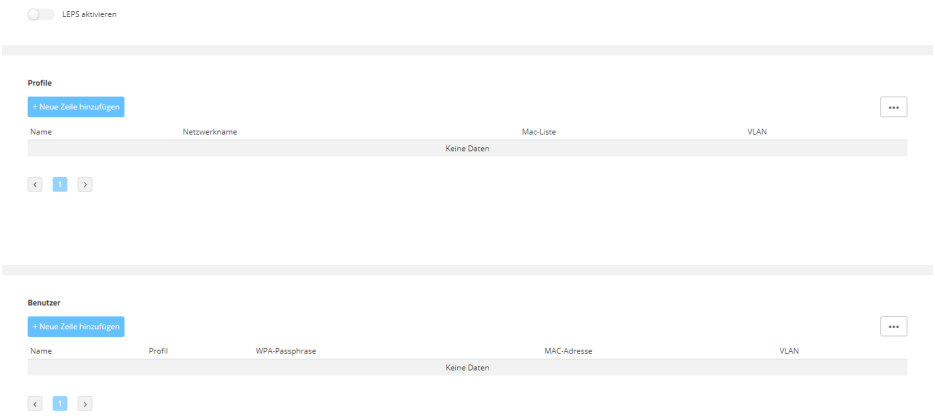


LEPS

Bei der Konfiguration von LEPS wird jedem Benutzer, der sich mit Clients im WLAN anmelden können soll, eine individuelle Passphrase zugeordnet. Dazu werden LEPS-Profile angelegt, damit einige Einstellungen nicht bei jedem Benutzer erneut vorgenommen werden müssen. Anschließend legen Sie die LEPS-Benutzer mit der zugehörigen individuellen Passphrase an und verknüpfen diesen mit einem der vorher angelegten LEPS-Profile.

Alternativ können Sie die Passphrase mit einer MAC-Adresse verbinden und auf diese Weise einen MAC-Adress-Filter einrichten.

Hier konfigurieren Sie die **Profile** und **Benutzer** für LANCOM Enhanced Passphrase Security (LEPS). Über den Schalter **LEPS aktivieren** wird LEPS eingeschaltet.



Profile

Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden.

Name

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

Netzwerkname

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.

MAC-Liste

Mögliche Werte:

Nicht prüfen

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.

VLAN

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

Benutzer

Legen Sie hier einzelne LEPS-Benutzer an. Jeder LEPS-Benutzer muss mit einem zuvor angelegten Profil verbunden werden und eine individuelle WPA-Passphrase zugewiesen bekommen. Mit dieser Passphrase kann sich dann ein beliebiger Client an der SSID anmelden, für die der Benutzereintrag durch die Verknüpfung des Profils gültig ist. Der Benutzer wird anhand der verwendeten Passphrase identifiziert und dem in dieser Tabelle konfigurierten VLAN zugewiesen. Wird hier kein VLAN zugewiesen, wird er dem am Profil konfigurierten VLAN zugewiesen. Einstellungen am einzelnen Benutzer haben somit Priorität gegenüber Einstellungen am Profil.

Name

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

Profil

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.

WPA-Passphrase

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

Als Passphrase können Zeichenketten mit 8 bis 64 Zeichen verwendet werden. Wir empfehlen als Passphrasen zufällige Zeichenketten von mindestens 32 Zeichen Länge.

MAC-Adresse

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.

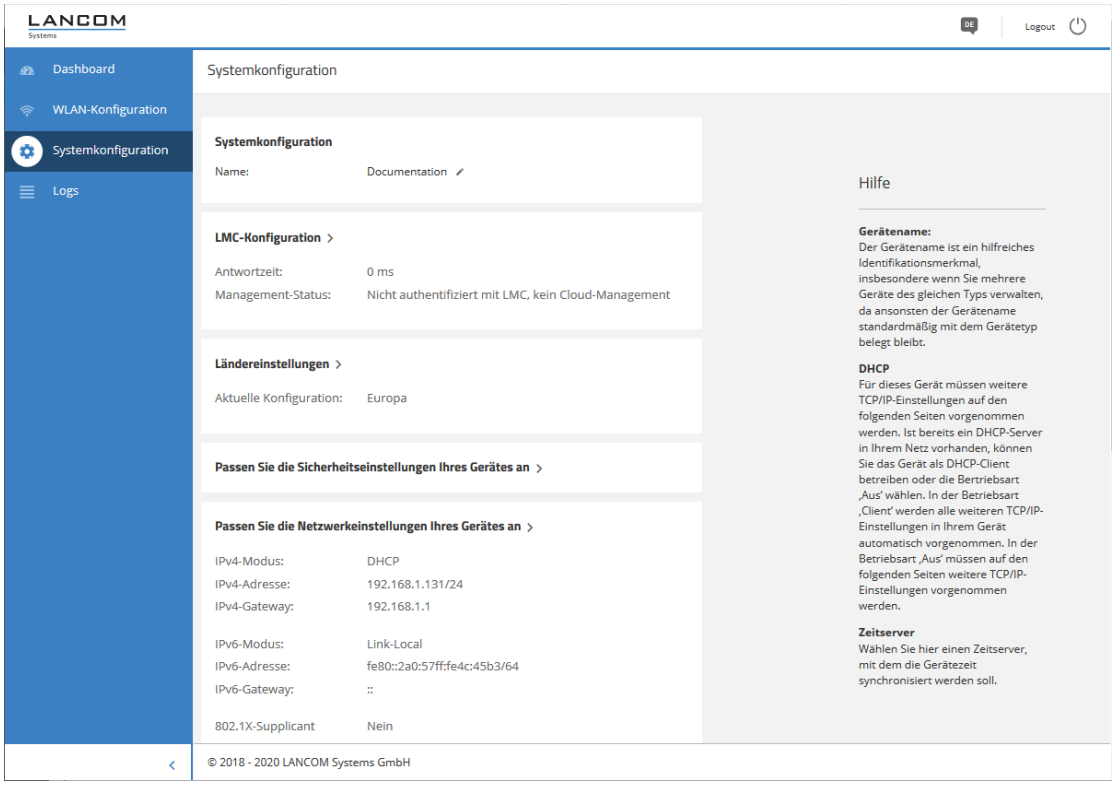
Im Vergleich zur reinen Zuweisung einer Passphrase an einen Benutzer ist die Verwaltung einer Passphrase pro MAC-Adresse etwas aufwändiger bei gleichzeitig höherer Kontrolle über die Geräte im Netz.

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 beim LEPS-Benutzer ein VLAN konfiguriert, gilt die hier konfigurierte VLAN.

5.5 Systemkonfiguration

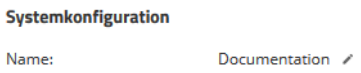
Die Systemkonfiguration bietet die Möglichkeit zur Konfiguration grundsätzlicher Parameter Ihres Gerätes, z. B. den Gerätenamen, die IP-Einstellungen zum Management des Gerätes oder die Aktivierung von SNMP.



Einzelne Felder wie den Systemnamen können Sie nach einem Klick auf den Haken neben diesem direkt bearbeiten. Für Bereiche öffnet sich eine Bearbeitungsmaske nach einem Klick auf die Überschrift.

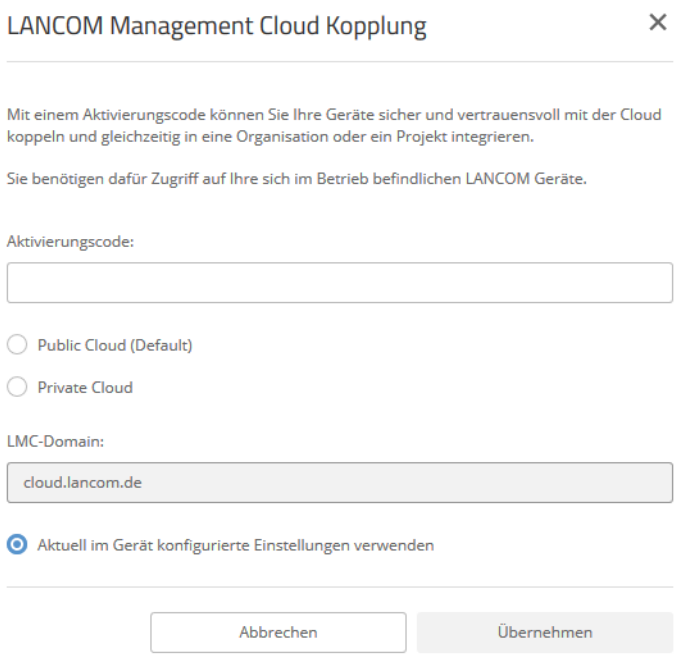
5.5.1 Name

Konfigurieren Sie hier den Gerätenamen.



5.5.2 LMC-Konfiguration

Koppeln Sie hier ihr Gerät nachträglich mit der LANCOM Management Cloud.



Aktivierungscode

Geben Sie den Aktivierungscode ein, den Sie vorab in Ihrem LANCOM Management Cloud-Projekt generiert haben.

Public Cloud

Diese Option gibt die LMC-Domäne der Public Cloud von LANCOM an.

Private Cloud

Bei dieser Option können Sie die LMC-Domäne ihrer privaten Instanz der LANCOM Management Cloud angeben.

LMC-Domain

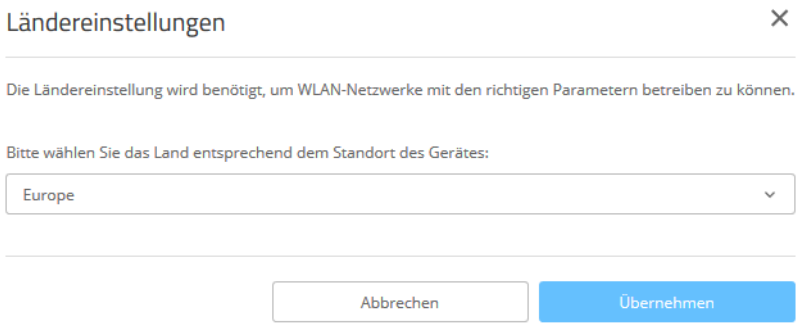
Zeigt entweder die LMC-Domäne der Public Cloud an oder Sie geben hier die LMC-Domäne ihrer privaten Instanz der LANCOM Management Cloud an.

Aktuell im Gerät konfigurierte Einstellungen verwenden

Übernimmt die im Gerät bereits konfigurierten Einstellungen.

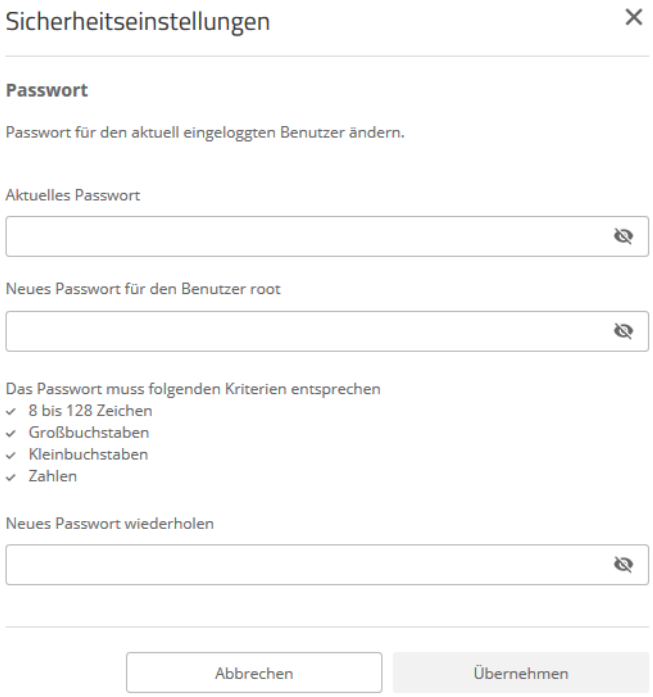
5.5.3 Ländereinstellungen

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



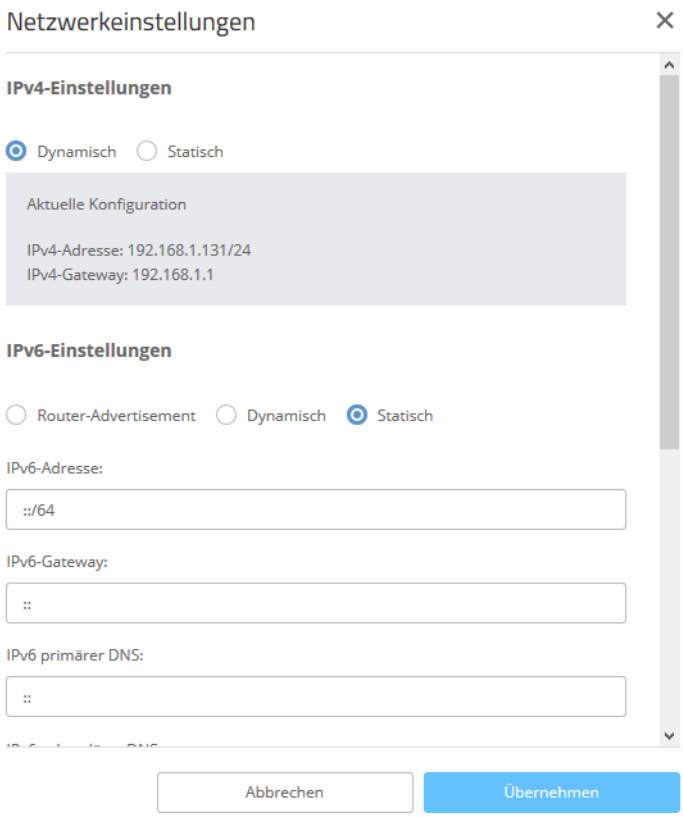
5.5.4 Sicherheitseinstellungen

Ändern Sie hier das Passwort für den aktuellen Benutzer (i. d. R. „root“).



5.5.5 Netzwerkeinstellungen

Hier haben Sie die Möglichkeit, die Netzwerkeinstellungen, wie z. B. die IP-Adresse, Ihres Gerätes anzupasssen.



IPv4-Einstellungen

Dynamisch

Verwendet DHCPv4 zur Konfiguration der IPv4-Parameter. Dies ist der Standardwert.

Statisch

Verwendet die IP-Parameter, die Sie in den folgenden Feldern **IPv4-Adresse**, **IPv4-Gateway**, **IPv4 primärer DNS** und **IPv4 sekundärer DNS** konfigurieren können.

Beachten Sie, dass die IPv4-Adresse in CIDR-Notation angegeben werden muss (z. B. 192.168.1.1/24).

IPv6-Einstellungen

Router-Advertisement

Verwendet Router Advertisements / SLAAC zur Konfiguration der IPv6-Parameter. Ist im empfangenen Router Advertisement das M (managed)-Flag gesetzt, werden weitere Parameter ggf. via DHCPv6 bezogen.

Dynamisch

Verwendet DHCPv6 zur Konfiguration der IPv6-Parameter.

Statisch

Verwendet die IP-Parameter, die Sie in den folgenden Feldern **IPv6-Adresse**, **IPv6-Gateway**, **IPv6 primärer DNS** und **IPv6 sekundärer DNS** konfigurieren können. Dies ist der Standardwert.

802.1X-Supplicant

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.

Benutzername

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

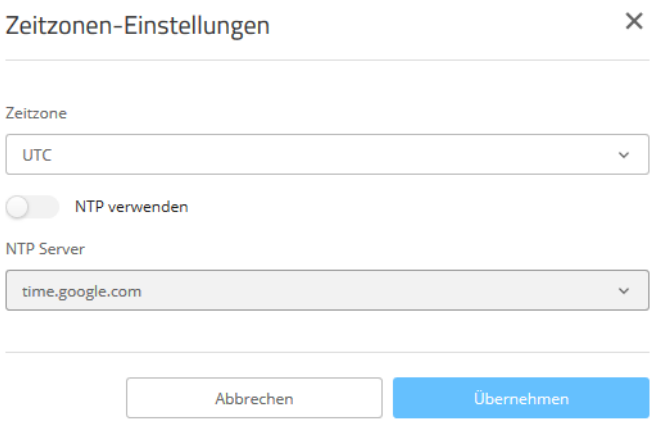
Passwort

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

Methode

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

5.5.6 Zeitzonen-Einstellungen



Zeitzone

Wählen Sie eine Zeitzone. Der Standardwert ist „UTC".

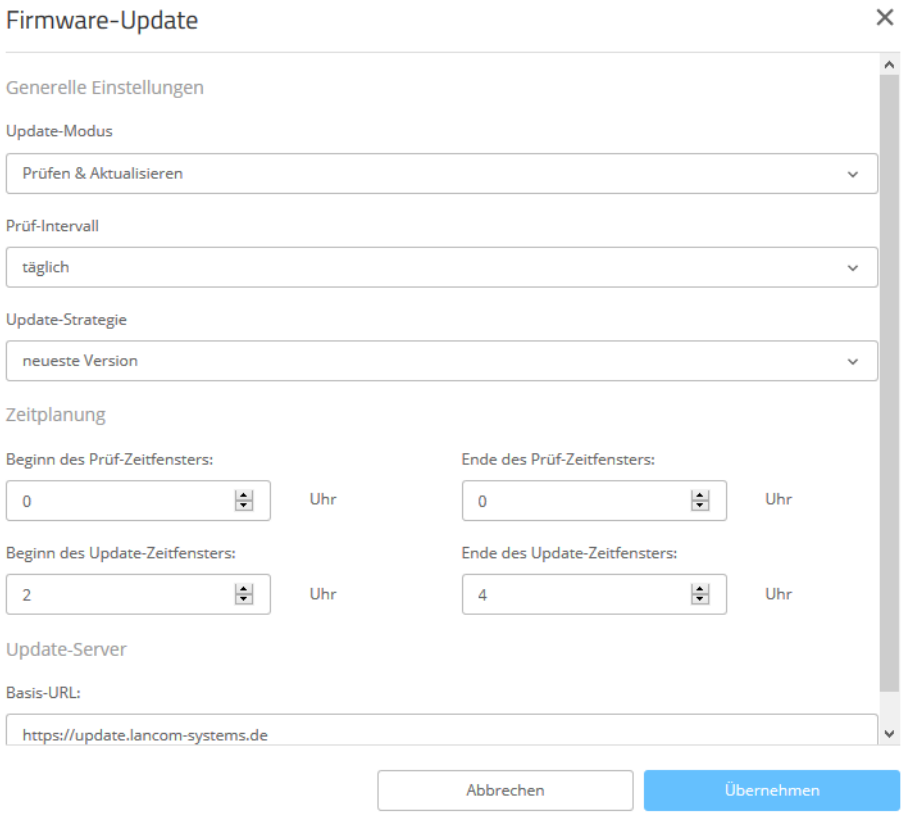
NTP verwenden

Wählen Sie hier, ob die Zeit via Network Time Protocol (NTP) von einem Zeitserver bezogen werden soll.

NTP-Server

Wählen Sie hier einen Zeitserver aus der angebotenen Liste aus, von dem die Zeit via NTP bezogen werden soll.

5.5.7 Automatisches Firmware Update



Update-Modus

Stellen Sie hier den Betriebsmodus ein. Die folgenden Modi werden unterstützt:

Prüfen & Aktualisieren

- Der Auto Updater prüft regelmäßig beim Update-Server auf neue Updates.
- Der Update-Server ermittelt anhand der **Update-Strategie** 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. Dies wird mehrere Minuten lang versucht, um eine eventuelle VDSL-Synchronisation oder einen WWAN-Verbindungsaufbau abzuwarten. 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.

nur Prüfen

- Der Auto Updater prüft regelmäßig beim 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.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Manuell

- 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.

Ein manuelles Update wird über den folgenden Befehl auf der Kommandozeile gestartet:

```
do /setup/Automatic-Firmware-Update/Update-Firmware-Now
```

Prüf-Intervall

Stellen Sie ein, ob die Überprüfung auf ein verfügbares Update täglich oder wöchentlich stattfinden soll.

Update-Strategie

neueste Version

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.

aktuelle Version

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.

nur Sicherheitsupdates

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.

neueste Version ohne 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.

Prüf-Zeitfenster

Stellen Sie hier das Zeitfenster für die Prüfung und den Download neuer Aktualisierungen ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung für beide Werte ist 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.

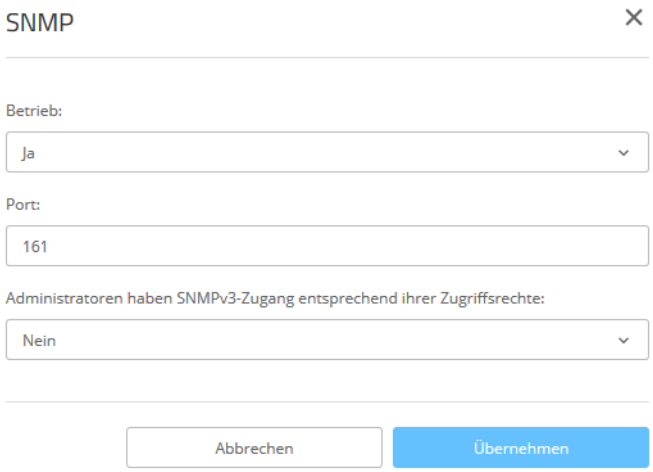
Update-Zeitfenster

Stellen Sie hier das Zeitfenster für die Update-Installation ein. Die tägliche Start- und Endzeit für dieses Zeitfenster kann stundengenau eingestellt werden. Die Standardeinstellung definiert ein Zeitfenster zwischen 2:00 Uhr und 4:00 Uhr. Wenn ein Update gefunden wurde, dann wird dieses also in diesem Zeitraum installiert und das Gerät neu gestartet, um das Update zu aktivieren. Innerhalb des konfigurierten Zeitfensters wird vom Auto Updater ein zufälliger Zeitpunkt für die Installation geplant.

Basis-URL

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

5.5.8 SNMP



Betrieb

Aktivieren Sie SNMP.

Port

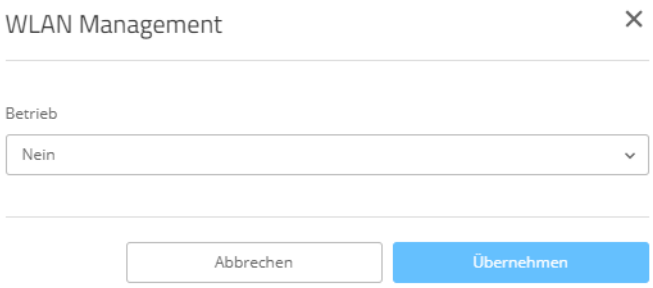
Passen Sie ggfs. den Port für SNMP an. Default: 161

Administratoren haben SNMPv3-Zugang entsprechend ihrer Zugriffsrechte

Sollen registrierte Administratoren, also ebenfalls der Benutzer root, auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.

5.5.9 WLAN-Management

Geben Sie hier an, ob ihr Gerät über einen WLAN-Controller gesteuert wird.



Betrieb

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.

6 Diagnose

6.1 Trace-Ausgaben

Zur Kontrolle der internen Abläufe im Gerät während oder nach der Konfiguration bieten sich die Trace-Ausgaben an. Erfahrene Anwender können durch die Interpretation dieser Ausgaben evtl. Fehler beim Verbindungsaufbau aufspüren. Ein besonderer Vorteil dabei: Die aufzuspürenden Fehler können sowohl in der Konfiguration eigener Geräte als auch bei der Gegenseite zu finden sein.

Die Trace-Ausgaben sind leicht zeitverzögert zum tatsächlichen Ereignis, jedoch immer in der richtigen Reihenfolge. Das stört im Regelfall die Interpretation der Anzeigen nicht, sollte aber bei genaueren Analysen berücksichtigt werden.

6.1.1 Trace – Ein Überblick

Trace-Ausgaben starten Sie in einer Konsolen-Sitzung. Stellen Sie zunächst eine Konsolen-Verbindung zu Ihrem Gerät her. Der Trace-Aufruf erfolgt dann mit dieser Syntax:

```
> trace [--log] [+|-|#|?] <Parameter>
```

Der Befehl trace, der Schlüssel und die Parameter werden jeweils durch Leerzeichen voneinander getrennt. Über die Schlüssel steuern Sie den Trace, während der Parameter die eigentliche Ausgabe bestimmt.

Tabelle 2: Übersicht der Schlüssel

Schlüssel	Bedeutung
`--log`	Ausgabe „historischer" Informationen aus dem Log
`?`	zeigt einen Hilfetext an
`+`	schaltet eine Trace-Ausgabe ein
–	schaltet eine Trace-Ausgabe aus
#	schaltet zwischen den verschiedenen Trace-Ausgaben um („Toggle")
kein Schlüssel	zeigt den aktuellen Zustand des Traces an

Tabelle 3: Übersicht der Parameter

Parameter	Bedeutung	`--log`
WLAN	WLAN-bezogene Ausgaben, z. B. An- und Abmelden von Clients, Schlüsselverhandlungen, …	Ja
	Wenn der Trace nicht aktiv ist, dann werden nur wenige Informationen in das Log eingetragen, sodass die „historischen" Informationen nicht besonders aussagekräftig sind.	
IAPP	Ausgaben zum IAPP (Inter Access Point Protocol).	Ja
Kernel	Ausgaben zum Basissystem und Kernel.	Ja
SSH	Ausgaben zum SSH-Dienst.	Ja
*	Joker-Zeichen, welches für alle Dienste steht.	Dienstabhängig

6.1.2 Trace – Bedienung

Die folgenden Beispiele dienen zur Veranschaulichung der Trace-Funktionalität:

- Starten eines oder mehrerer Traces:

```
trace + ssh kernel
```

- Stoppen von Traces:

```
trace - ssh kernel
```

- Stoppen aller Traces:

```
trace - *
```

- Umschalten zwischen ein- und ausschalten der Traces („Toggle“):

```
trace # ssh kernel
```

- Ausgeben „historischer“ Informationen, sofern unterstützt und im Log vorhanden:

```
trace --log + kernel
```

6.2 Logs in WEBconfig

Sie erreichen den Bereich „Logs“ über den Punkt **Logs** in der Sidebar.

In diesem Bereich wird das Syslog des Gerätes ausgegeben.