LANCOM Access Points

Sicherheitsrelevante Einstellungen

01/2026

LANCOM SYSTEMS

Inhalt

1 LCOS LX-Version und -Syntaxbeschreibung

Dieses Dokument beschreibt die sicherheitsrelevanten Einstellungen LCOS LX-basierter Access Points. Es dient als Nachschlagewerk für die Geräte-Administration und den sicheren Betrieb von LANCOM Access Points.

Die beschriebenen Einstellungen gelten für Geräte mit mindestens LCOS LX-Version 7.10. Um insbesondere im Bereich der zentralen Administratorenverwaltung eine umfassende Absicherung zu gewährleisten, sind die Funktionen dieser LCOS LX-Version erforderlich.

Für alle aufgeführten Konfigurationsparameter werden der zugehörige Kommandozeilenpfad, die erforderlichen Befehle zur Parametereinstellung sowie Empfehlungen zu Einstellungen sicherheitsrelevanter Werte dargestellt.

Bei allen Verschlüsselungs- und Hash-Verfahren empfehlen wir, stets die stärksten Krypto-Algorithmen zu verwenden!

Bitte beachten Sie die Mindestanforderungen für sichere Passwörter:

Um die Mindestanforderung an Passwörter zu erfüllen, sollten die nachfolgenden Anforderungen umgesetzt werden. Alle Passwörter dürfen nicht im Wörterbuch vorkommen, sollten keine persönlichen Daten enthalten (z. B. Geburtsdatum, Name des Haustiers) und dürfen kein Tastaturmuster (z. B. „qwertz“) sein.

Es kann aus einem Merksatz abgeleitet werden und muss alle vier Zeichensätze (Großbuchstaben, Kleinbuchstaben, Ziffern und Sonderzeichen) nutzen (z. B. „Unser Zweckverband besteht aus 13 Gemeinden und wir arbeiten alle wirklich sehr gerne dort!“ ergibt das dadurch merkbare „UZba13Guwaawsgd!“).

Hinweis: Unbedingt einen eigenen Merksatz ausdenken!

Das Passwort sollte mindestens 10 Zeichen lang sein oder mindestens die technisch maximal möglichen Stellen umfassen. Dies gilt auch für Passwörter für den Zugang zu sensiblen Bereichen z. B. die Passwörter für Systemadministratoren.

Um die Komplexitätsanforderungen zu erfüllen müssen alle der folgenden Zeichensätze genutzt werden:

- Großbuchstaben (A bis Z)
- Kleinbuchstaben (a bis z)
- Ziffern (0 bis 9)
- Sonderzeichen (z. B. !, $, -, %)

Sollte dies nicht möglich sein, so sind zumindest die technisch möglichen Zeichensätze zu verwenden.

Beachten Sie auch die *Richtline des Bundesamt für Sicherheit in der Informationstechnik zur Erstellung sicherer Passwörter*.

2 SNMP

In diesem Menü konfigurieren Sie SNMP.

Pfad Konsole

Setup

Parameter	Pfad	Beschreibung
Send-Traps	**Setup** > **SNMP**	Bei schwerwiegenden Fehlern, zum Beispiel bei einem unberechtigten Zugriff, kann das Gerät automatisch eine Fehlermeldung an einen oder mehrere SNMP-Manager senden. Schalten Sie dazu diese Option ein und geben Sie in der Tabelle **Target-Addresses** die Ziele ein, auf denen diese SNMP-Manager installiert sind.
Port	**Setup** > **SNMP**	Über diesen Parameter legen Sie den Port fest, über den der SNMP-Dienst für externe Programme wie z. B. LANmonitor erreichbar ist.
Admitted-Protocols	**Setup** > **SNMP**	Aktivieren Sie hier die SNMP-Versionen, die das Gerät bei SNMP-Anfragen und SNMP-Traps unterstützen soll.
Allow-Admins	**Setup** > **SNMP**	Sollen registrierte Administratoren (darunter fällt auch der Benutzer `root`) auch den Zugriff über SNMPv3 erhalten, aktivieren Sie diese Option.
Operating	**Setup** > **SNMP**	Dieser Eintrag aktiviert oder deaktiviert SNMP-Traps.

Empfehlungen

- **Setup** > **SNMP** > **Admitted-Protocols**: **SNMPv3** verwenden.
- **Setup** > **SNMP** > **Allow-Admins**: **No** (nur in Ausnahmefällen **Yes**).
- **Setup** > **SNMP** > **Operating**: **Yes** (nur wenn Trap-Empfänger definiert sind, sonst **No**).

2.1 Communities

In diesem Menü konfigurieren Sie die SNMP-Communities.

Beschreibung

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

SNMP-Communities werden nur bei der Verwendung von SNMPv1 & SNMPv2 benötigt. LANCOM Systems empfiehlt aus Sicherheitsgründen, immer SNMPv3 zu verwenden!

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Name	**Setup** > **SNMP** > **Communities**	Vergeben Sie hier einen aussagekräftigen Namen für diese SNMP-Community.
Security-Name	**Setup** > **SNMP** > **Communities**	Geben Sie hier die Bezeichnung für die Zugriffsrichtlinie ein, die die Zugriffsrechte für alle Community-Mitglieder festlegt.
Status	**Setup** > **SNMP** > **Communities**	Mit diesem Eintrag aktivieren oder deaktivieren Sie diese SNMP-Community.

Empfehlungen

- Default-Community `public` deaktivieren oder löschen.
- Niemals die vordefinierte Community `public` aktiv lassen, da sie allgemein bekannt ist und unautorisierten Lesezugriff ermöglicht.
- Eigene Communities mit komplexen Namen verwenden: mindestens 16 Zeichen, zufällige Kombination aus Groß- / Kleinbuchstaben, Zahlen und Sonderzeichen.
- Nicht benötigte Communities **deaktivieren** oder löschen.
- Communities, die nicht im Einsatz sind, auf **Inactive** setzen oder ganz **löschen**.

2.2 Gruppen

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

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Security-Model	**Setup** > **SNMP** > **Groups**	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.
Security-Name	**Setup** > **SNMP** > **Groups**	Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.
Group-Name	**Setup** > **SNMP** > **Groups**	Vergeben Sie hier einen aussagekräftigen Namen für diese Gruppe. Diesen Namen verwenden Sie anschließend bei der Konfiguration der Zugriffsrechte.
Status	**Setup** > **SNMP** > **Groups**	Aktiviert oder deaktiviert diese Gruppenkonfiguration.

Empfehlungen

- **Setup** > **SNMP** > **Groups** > **Security-Model**: **SNMPv3_USM** (AuthPriv mit SHA + AES) verwenden.
- **Setup** > **SNMP** > **Groups** > **Status**: Nur notwendige Gruppen aktivieren, den Rest deaktivieren.

2.3 Accesses

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

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Security-Model	**Setup** > **SNMP** > **Accesses**	Aktivieren Sie hier das entsprechende Security-Model.
Read-View-Name	**Setup** > **SNMP** > **Accesses**	Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Leserechte erhalten soll.
Write-View-Name	**Setup** > **SNMP** > **Accesses**	Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Schreibrechte erhalten soll.
Notify-View-Name	**Setup** > **SNMP** > **Accesses**	Bestimmen Sie die Ansicht der MIB-Einträge, für die diese Gruppe die Notify-Rechte erhalten soll.
Status	**Setup** > **SNMP** > **Accesses**	Aktiviert oder deaktiviert diesen Eintrag.
Min-Security-Level	**Setup** > **SNMP** > **Accesses**	Geben Sie die minimale Sicherheit an, die für Zugriff und Datenübertragung gelten soll.

Empfehlungen

- **Setup** > **SNMP** > **Accesses** > **Security-Model**: **SNMPv3_USM** verwenden.
- **Setup** > **SNMP** > **Accesses** > **Write-View-Name**: Leer lassen und nur bei zwingendem Bedarf definieren.
- **Setup** > **SNMP** > **Accesses** > **Status**: Nur notwendige Einträge aktivieren.
- **Setup** > **SNMP** > **Accesses** > **Min-Security-Level**: **AuthPriv** (SHA+AES) verwenden.

2.4 Views

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

Pfad Konsole

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

Parameter	Pfad	Beschreibung
View-Name	**Setup** > **SNMP** > **Views**	Vergeben Sie hier der Ansicht einen aussagekräftigen Namen.
OID-Subtree	**Setup** > **SNMP** > **Views**	Bestimmen Sie durch komma-separierte Angabe der jeweiligen OIDs, welche Werte und Aktionen der MIB diese Ansicht einschließen soll.
Type	**Setup** > **SNMP** > **Views**	Bestimmen Sie, ob die angegebenen OID-Teilbäume Bestandteil (**Included**) oder kein Bestandteil (**Excluded**) der Ansicht sind.
Status	**Setup** > **SNMP** > **Views**	Aktiviert oder deaktiviert diese Ansicht.

Empfehlungen

- **Setup** > **SNMP** > **Views** > **OID-Subtree**: Nur relevante Monitoring-OIDs verwenden (z. B. `ifTable`, `Systemstatus`).
- **Setup** > **SNMP** > **Views** > **Type**: **Included** für notwendige, **Excluded** für sensible OIDs verwenden.
- **Setup** > **SNMP** > **Views** > **Status**: Nur notwendige Views aktivieren, den Rest deaktivieren.

2.5 Users

Dieses Menü enthält die Benutzerkonfiguration für SNMPv3.

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Username	**Setup** > **SNMP** > **Users**	Geben Sie hier den SNMPv3-Benutzernamen an.
Authentication-Protocol	**Setup** > **SNMP** > **Users**	Bestimmen Sie, mit welchem Verfahren sich der Benutzer am SNMP-Agent authentifizieren muss.
Authentication-Password	**Setup** > **SNMP** > **Users**	Geben Sie hier das für die Authentifizierung notwendige Passwort des Benutzers ein.
Privacy-Password	**Setup** > **SNMP** > **Users**	Geben Sie hier das für die Verschlüsselung notwendige Passwort des Benutzers ein.
Status	**Setup** > **SNMP** > **Users**	Aktiviert oder deaktiviert diesen Benutzer.
Authentication-Password-Type	**Setup** > **SNMP** > **Users**	Passworttyp für die Authentifizierung. Für die Eingabe eines neuen Passworts muss der Typ vorübergehend auf **Plaintext** gesetzt werden. Nach der Eingabe verschlüsselt LCOS LX das Passwort automatisch und setzt den Wert zurück auf **Masterkey**.
Privacy-Password-Type	**Setup** > **SNMP** > **Users**	Passworttyp für die Verschlüsselung. Für die Eingabe eines neuen Passworts muss der Typ vorübergehend auf **Plaintext** gesetzt werden. Nach der Eingabe verschlüsselt LCOS LX das Passwort automatisch und setzt den Wert zurück auf **Masterkey**.

Empfehlungen

- **Setup** > **SNMP** > **Users** > **Authentication-Protocol**: **HMAC-SHA256** oder höher verwenden.
- **Setup** > **SNMP** > **Users** > **Authentication-Password**: Langes, komplexes Passwort verwenden und regelmäßig rotieren.
- **Setup** > **SNMP** > **Users** > **Privacy-Protocol**: **AES256** verwenden.
- **Setup** > **SNMP** > **Users** > **Privacy-Password**: Separates, komplexes Passwort verwenden — nicht identisch mit dem Authentication-Password.
- **Setup** > **SNMP** > **Users** > **Authentication-Password-Type** / **Privacy-Password-Type**: **Masterkey** (Standard) verwenden. Nur für Eingabe kurzzeitig **Plaintext**.
- **Setup** > **SNMP** > **Users** > **Status**: Nur aktive und benötigte User verwenden.

2.6 Target-Addresses

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

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Name	**Setup** > **SNMP** > **Target-Addresses**	Geben Sie hier den Ziel-Adress-Namen an.
Transport-Address	**Setup** > **SNMP** > **Target-Addresses**	Die Transportadresse beschreibt die IP-Adresse und Port-Nummer eines SNMP-Trap-Empfängers und wird im Format `<IP-Adresse>:<Port>` angegeben (z. B. `128.1.2.3:162`). Der UDP-Port 162 wird für SNMP-Traps verwendet.
Parameters-Name	**Setup** > **SNMP** > **Target-Addresses**	Wählen Sie hier den gewünschten Eintrag aus der Liste der Empfängerparameter aus.
Status	**Setup** > **SNMP** > **Target-Addresses**	Aktiviert oder deaktiviert diese Zieladresse.

Empfehlungen

- **Setup** > **SNMP** > **Target-Addresses** > **Status**: Nur produktive Ziele aktivieren, den Rest deaktivieren.

2.7 Target-Params

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

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Name	**Setup** > **SNMP** > **Target-Params**	Vergeben Sie hier dem Eintrag einen aussagekräftigen Namen.
Message-Processing-Model	**Setup** > **SNMP** > **Target-Params**	Bestimmen Sie hier, nach welchem Protokoll der SNMP-Agent die Nachricht strukturiert.
Security-Model	**Setup** > **SNMP** > **Target-Params**	Legen Sie mit diesem Eintrag das Sicherheitsmodell fest.
Security-Name	**Setup** > **SNMP** > **Target-Params**	Wählen Sie hier einen Security-Namen aus, den Sie einer SNMP-Community zugeordnet haben. Auch die Angabe des Namens eines bereits konfigurierten Benutzers ist möglich.
Security-Level	**Setup** > **SNMP** > **Target-Params**	Legen Sie die Sicherheitsstufe fest, die für den Erhalt der SNMP-Traps beim Empfänger gelten soll.
Status	**Setup** > **SNMP** > **Target-Params**	Aktiviert oder deaktiviert diesen Eintrag.

Empfehlungen

- **Setup** > **SNMP** > **Target-Params** > **Message-Processing-Model**: **SNMPv3** verwenden.
- **Setup** > **SNMP** > **Target-Params** > **Security-Model**: **SNMPv3_USM** verwenden.
- **Setup** > **SNMP** > **Target-Params** > **Security-Level**: **AuthPriv** verwenden.
- **Setup** > **SNMP** > **Target-Params** > **Status**: **Active** (nur für produktive Einträge).

3 Config

Enthält die allgemeinen Konfigurationseinstellungen.

Pfad Konsole

Setup > **Config**

Parameter	Pfad	Beschreibung
Administrator	**Setup** > **Config**	Name des Geräte-Administrators. Wird nur zu Anzeigezwecken verwendet.
Config-Aging-Minutes	**Setup** > **Config**	Hier können Sie angeben, nach wieviel Minuten der Inaktivität eine Konfigurations-Verbindung über TCP (z. B. SSH-Verbindung) automatisch beendet wird.
Admins	**Setup** > **Config**	Legen Sie für Administratoren in dieser Tabelle an, die gegebenenfalls über eingeschränkte Rechte verfügen.
Administrator	**Setup** > **Config** > **Admins**	Anmeldename des Administrators in dieser Zeile der Tabelle.
Function-Rights	**Setup** > **Config** > **Admins**	Aktivieren Sie hier die Funktionsrechte des Administrators in dieser Zeile der Tabelle.
Rights	**Setup** > **Config** > **Admins**	Die Rechte des Administrators in dieser Zeile der Tabelle.
Hashed-Password	**Setup** > **Config** > **Admins**	Hashwert des Passworts des Administrators in dieser Zeile der Tabelle.

Empfehlungen

- **Setup** > **Config** > **Admins** > **Administrator**: Individuellen Benutzername pro Administrator verwenden.
- **Setup** > **Config** > **Admins** > **Function-Rights** / **Setup** > **Config** > **Admins** > **Rights**: Nur benötigte Rechte vergeben (Least Privilege).

3.1 TACACS+

Konfigurieren Sie hier Authentifizierung, Autorisierung und Accounting (AAA) mittels des TACACS+-Protokolls.

Pfad Konsole

Setup > **Config** > **Tacacs-Plus**

Parameter	Pfad	Beschreibung
Operating	**Setup** > **Config** > **Tacacs-Plus**	Schaltet die Verwendung von TACACS+ ein oder aus.
Internal-fallback-allowed	**Setup** > **Config** > **Tacacs-Plus**	Ist diese Option aktiviert, kann bei nicht erreichbaren TACACS+-Servern ein Login mit lokalen Benutzerdaten durchgeführt werden.
Server-Address	**Setup** > **Config** > **Tacacs-Plus**	Die IP-Adresse des primären TACACS+-Servers.
Server-Port	**Setup** > **Config** > **Tacacs-Plus**	Der Port des primären TACACS+-Servers.

Parameter	Pfad	Beschreibung
Server-Secret	**Setup** > **Config** > **Tacacs-Plus**	Der für die Kommunikation mit dem primären TACACS+-Server verwendete Schlüssel.
Spare-Server-Address	**Setup** > **Config** > **Tacacs-Plus**	Die IP-Adresse des Backup-TACACS+-Servers.
Spare-Server-Port	**Setup** > **Config** > **Tacacs-Plus**	Der Port des Backup-TACACS+-Servers.
Spare-Server-Secret	**Setup** > **Config** > **Tacacs-Plus**	Der für die Kommunikation mit dem Backup-TACACS+-Server verwendete Schlüssel.

Empfehlungen

- **Setup** > **Config** > **Tacacs-Plus** > **Operating**: **Yes**
- **Setup** > **Config** > **Tacacs-Plus** > **Internal-fallback-allowed**: **No**
- **Setup** > **Config** > **Tacacs-Plus** > **Server-Address**: Interne Management-IP verwenden (z. B. 10.0.0.10).
- **Setup** > **Config** > **Tacacs-Plus** > **Server-Port**: **49**
- **Setup** > **Config** > **Tacacs-Plus** > **Server-Secret**: Starkes Secret mit mindestens 32 Zeichen einsetzen.
- **Setup** > **Config** > **Tacacs-Plus** > **Spare-Server-Address**: Interne Backup-IP verwenden (z. B. 10.0.0.11).
- **Setup** > **Config** > **Tacacs-Plus** > **Spare-Server-Port**: **49**
- **Setup** > **Config** > **Tacacs-Plus** > **Spare-Server-Secret**: Eigenes starkes Secret verwenden.

3.2 SSH

Konfigurieren Sie hier Einstellungen zu SSH.

Pfad Konsole

Setup > **Config** > **SSH**

Parameter	Pfad	Beschreibung
RSA-Hostkey-Length	**Setup** > **Config** > **SSH**	Die Länge des SSH-Hostkeys kann zwischen 2048 Bits und 4096 Bits gewählt werden. Nach der Änderung der Einstellung wird der Hostkey sofort neu generiert.
Root-Hashed	**Setup** > **Config** > **SSH**	Hashwert des Passworts des Administrators root.

Empfehlungen

- **Setup** > **Config** > **SSH** > **RSA-Hostkey-Length**: **4096 Bits** Schlüssellänge verwenden.

4 WLAN

Konfigurationseinstellungen der WLAN-Parameter.

Pfad Konsole

Setup > **WLAN**

4.1 Network

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

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

Parameter	Pfad	Beschreibung
Network-Name	**Setup** > **WLAN** > **Network**	Konfigurieren Sie hier einen sprechenden Namen für das WLAN-Netzwerk. Dieser interne Name wird verwendet, um die Interface-Konfiguration in weiteren Teilen der Konfiguration zu referenzieren.
SSID-Name	**Setup** > **WLAN** > **Network**	Konfigurieren Sie hier den nach außen sichtbaren Namen der SSID.
Closed-Network	**Setup** > **WLAN** > **Network**	Konfigurieren Sie hier, ob die konfigurierte SSID während der Netzwerksuche durch Clients angezeigt werden soll. Wenn der SSID-Broadcast unterdrückt wird, dann antwortet der Access Point nicht mehr auf Probe Requests mit leerer SSID. In diesem Fall muss für einen Verbindungsaufbau die SSID explizit am Client eingetragen und konfiguriert werden.
Max-Stations	**Setup** > **WLAN** > **Network**	Maximale Anzahl gleichzeitig verbundener WLAN-Clients.
Inter-Station-Traffic	**Setup** > **WLAN** > **Network**	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.
Client-Isolation	**Setup** > **WLAN** > **Network**	Soll die Kommunikation von WLAN-Clients untereinander, bzw. generell zu nicht zulässigen Zielen im Netzwerk unterbunden werden, kann die Client-Isolierung konfiguriert werden. Hierbei wird jeglicher Datenverkehr ausgehend von WLAN-Clients zu nicht explizit in einer Whitelist erfassten Zielen verboten. Die Client-Isolierung kann hier je SSID eingeschaltet werden.
Min-Client-Strength	**Setup** > **WLAN** > **Network**	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.
Exclude-From-Client-Management	**Setup** > **WLAN** > **Network**	Schließt diese SSID ggf. vom Band Steering aus.
Timeframe	**Setup** > **WLAN** > **Network**	Name eines Zeitrahmens, über den die SSID zeitgesteuert aktiviert oder deaktiviert wird.

Parameter	Pfad	Beschreibung
Block-Multicast	**Setup** > **WLAN** > **Network**	Blockiert Multicast-Datenverkehr nach IPv4 und / oder IPv6.
Bridge	**Setup** > **WLAN** > **Network**	Wird bei WLC-Betrieb intern verwendet bzw. bei Verwendung von L2TP muss hier das L2TP-Interface eingetragen werden.
Key	**Setup** > **WLAN** > **Network**	Konfigurieren Sie hier den Pre-Shared Key (PSK) der SSID.
Encryption-Profile	**Setup** > **WLAN** > **Network**	Konfigurieren Sie hier ein Verschlüsselungs-Profil aus den in **Setup** > **WLAN** > **Encryption** vorhandenen, welches definiert, welches Authentisierungs- und Verschlüsselungsverfahren für die SSID zum Tragen kommen soll.
Idle-Timeout	**Setup** > **WLAN** > **Network**	Zeit in Sekunden, nach der inaktive Clients getrennt werden. Jeglicher Verkehr des Clients setzt den Timer zurück.

Empfehlungen

- **Setup** > **WLAN** > **Network** > **Inter-Station-Traffic**: **Yes** (Wenn Clients untereinander kommunizieren sollen)
- **Setup** > **WLAN** > **Network** > **Client-Isolation**: **No** (Keine Isolation, interne Kommunikation erlaubt)
- **Setup** > **WLAN** > **Network** > **Min-Client-Strength**: **20** (Sehr schwache Verbindungen werden verhindert)
- **Setup** > **WLAN** > **Network** > **Block-Multicast**: **No** (Multicast für z. B. Drucker/Streaming erlaubt)
- **Setup** > **WLAN** > **Network** > **Key**: Starkes WPA3-PSK-Passwort verwenden (Hohe Sicherheit für WLAN-Zugriff)
- **Setup** > **WLAN** > **Network** > **Idle-Timeout**: **600** Sekunden (Trennt inaktive Clients nach 10 Minuten und schont somit Ressourcen)

4.2 Encryption

Konfigurieren Sie hier alle Einstellungen rund um die Verschlüsselung und Authentisierung der WLAN-Netzwerke.

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Profile-Name	**Setup** > **WLAN** > **Encryption**	Wählen Sie hier einen sprechenden Namen für das Verschlüsselungsprofil. Dieser interne Name wird verwendet, um das Verschlüsselungsprofil in weiteren Teilen der Konfiguration zu referenzieren.
Encryption	**Setup** > **WLAN** > **Encryption**	Konfigurieren Sie hier, ob das WLAN-Netzwerk verschlüsselt sein soll oder keine Verschlüsselung verwendet werden soll (Open Network).
Method	**Setup** > **WLAN** > **Encryption**	Konfigurieren Sie hier die Verschlüsselungsmethode.
WPA-Version	**Setup** > **WLAN** > **Encryption**	Konfigurieren Sie hier die WPA-Version, welche für die Verschlüsselungsmethoden 802.11i-WPA-PSK und 802.11i-WPA-802.1X verwendet werden.
WPA-Rekeying-Cycle	**Setup** > **WLAN** > **Encryption**	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

Parameter	Pfad	Beschreibung
		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.
WPA1-Session-Keytypes	**Setup** > **WLAN** > **Encryption**	Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 1 verwendet wird. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.
WPA2-3-Session-Keytypes	**Setup** > **WLAN** > **Encryption**	Konfigurieren Sie hier, welcher Sitzungsschlüssel-Typ für die WPA-Version 2 bzw.3 angeboten werden sollen. Dies beeinflusst auch das verwendete Verschlüsselungsverfahren.
Prot.-Mgmt-Frames	**Setup** > **WLAN** > **Encryption**	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.
Prot.-Beacons	**Setup** > **WLAN** > **Encryption**	Der Standard IEEE 802.11be (WiFi 7) schreibt die Verwendung von Beacon Protection vor. Dies kann hier konfiguriert werden.
Pre-Authentication	**Setup** > **WLAN** > **Encryption**	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 unterscheidet 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

Parameter	Pfad	Beschreibung
		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.
OKC	**Setup** > **WLAN** > **Encryption**	Diese Option aktiviert oder deaktiviert das Opportunistic Key Caching (OKC).
WPA2-Key-Management	**Setup** > **WLAN** > **Encryption**	Bestimmen Sie hier, nach welchem Standard das WPA2-Schlüsselmanagement funktionieren soll.
PMK-IAPP-Secret	**Setup** > **WLAN** > **Encryption**	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-Server-Profile	**Setup** > **WLAN** > **Encryption**	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.
SAE/OWE-Groups	**Setup** > **WLAN** > **Encryption**	Enthält die Auswahl der angebotenen Diffie-Hellman-Gruppen als Bitmaske, auf deren Basis die Protokollpartner einen Schlüssel für den Datenaustausch erstellen. Die vorhandenen Gruppen nutzen elliptische Kurven. Das bei WPA3 verwendete Authentisierungsverfahrens SAE (Simultaneous Authentication of Equals) nutzt diese Verfahren zusammen mit AES zur Erzeugung eines kryptographisch starken Schlüssels.

Empfehlungen

- **Setup** > **WLAN** > **Encryptionn** > **Encryption**: **Yes** (Verschlüsselung immer aktivieren für sichere Datenübertragung).
- **Setup** > **WLAN** > **Encryption** > **Method**: **802.11i-WPA-PSK** oder **802.11i-WPA-802.1X** (Sichere Verfahren für PSK oder RADIUS).
- **Setup** > **WLAN** > **Encryption** > **WPA-Version**: **WPA3** (Maximale Sicherheit, moderne WLAN-Clients unterstützen diese).
- **Setup** > **WLAN** > **Encryption** > **WPA-Rekeying-Cycle**: **3600** Sekunden (Schlüssel regelmäßig erneuern, denn es schützt vor Schlüsselwiederholung).
- **Setup** > **WLAN** > **Encryption** > **WPA2-3-Session-Keytypes**: **AES-CCMP-256** oder **AES-GCMP-256** (Funktioniert nur mit kompatiblen Clients. Vermeiden Sie die Verwendung von TKIP, da es nicht mehr als sicher gilt).
- **Setup** > **WLAN** > **Encryption** > **Prot.-Mgmt-Frames**: **Mandatory** (Management Frames verschlüsseln, schützt gegen Manipulation).
- **Setup** > **WLAN** > **Encryption** > **Prot.-Beacons**: **Yes** (Beacon Protection aktiviert für Wi-Fi 7,).
- **Setup** > **WLAN** > **Encryption** > **Pre-Authentication**: **Yes** (Schnellere Anmeldung beim Roaming zwischen Access Points).

- **Setup** > **WLAN** > **Encryption** > **WPA2-Key-Management**: **Standard+Fast-Roaming** (Roaming für moderne WLAN-Clients, Standard für Legacy-Clients).
- **Setup** > **WLAN** > **Encryption** > **PMK-IAPP-Secret**: Identisch auf allen Access Points (Sicheres Fast Roaming über IAPP).
- **Setup** > **WLAN** > **Encryption** > **RADIUS-Server-Profile**: Nur bei 802.1X nötig, ansonsten leer lassen (PSK benötigt keinen RADIUS).
- **Setup** > **WLAN** > **Encryption**: Wählen Sie die höchsten verfügbaren Gruppen wenn Sie WPA3 verwenden. Andernfalls ist dies nicht relevant.

4.3 Client-Isolation-Allowed

Konfigurieren Sie hier die erlaubten Ziele für die Client-Isolierung.

Pfad Konsole

Setup > **WLAN** > **Client-Isolation-Allowed**

Parameter	Pfad	Beschreibung
Network-Name	**Setup** > **WLAN** > **Client-Isolation-Allowed**	Wählen Sie hier das Netzwerk bzw. die SSID, für die der Eintrag gelten soll. Erfassen Sie dann wahlweise eine Ziel-IP-Adresse.
IP-Network	**Setup** > **WLAN** > **Client-Isolation-Allowed**	Erlaubte Ziel-IP-Adresse für dieses Netzwerk.
MAC-Address	**Setup** > **WLAN** > **Client-Isolation-Allowed**	Erlaubte Ziel-MAC-Adresse für dieses Netzwerk.

Empfehlungen

- **Setup** > **WLAN** > **Client-Isolation-Allowed** > **Network-Name**: SSID wählen (Isolation nur für das gewünschte WLAN aktivieren)
- **Setup** > **WLAN** > **Client-Isolation-Allowed** > **IP-Network**: IP-Adressen erlaubter Ziele eintragen (z. B. Drucker oder Server)
- **Setup** > **WLAN** > **Client-Isolation-Allowed** > **MAC-Address**: MAC-Adressen erlaubter Geräte eintragen (zusätzliche Sicherheit)

4.4 LEPS

Mit LANCOM Enhanced Passphrase Security (LEPS) können Sie WLAN-Stationen benutzerdefinierte Passphrasen zuweisen, ohne die Stationen vorher anhand ihrer MAC-Adresse erfassen zu müssen.

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Operating	**Setup** > **WLAN** > **LEPS**	Schaltet LEPS ein oder aus. Im ausgeschalteten Zustand werden die angelegten LEPS-Benutzer bei der Anmeldung von WLAN-Clients nicht beachtet.

Parameter	Pfad	Beschreibung
Profiles	**Setup** > **WLAN** > **LEPS**	Konfigurieren Sie hier LEPS-Profile und verbinden Sie sie mit einer SSID. Anschließend können die LEPS-Profile den LEPS-Benutzern zugeordnet werden. Profilwerte können überschrieben werden.
Name	**Setup** > **WLAN** > **LEPS** > **Profiles**	Vergeben Sie hier einen eindeutigen Namen für das LEPS-Profil.
Network-Name	**Setup** > **WLAN** > **LEPS** > **Profiles**	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-List	**Setup** > **WLAN** > **LEPS** > **Profiles**	Hier können Sie angeben, ob und wie MAC-Adressen geprüft werden sollen.
VLAN	**Setup** > **WLAN** > **LEPS** > **Profiles**	Definiert das VLAN, dem ein LEPS-Benutzer mit diesem Profil zugewiesen wird.
Users	**Setup** > **WLAN** > **LEPS**	Legen Sie LEPS-Benutzer an. Jeder Benutzer muss mit einem Profil verbunden werden.
Name	**Setup** > **WLAN** > **LEPS** > **Users**	Vergeben Sie einen eindeutigen Namen für den LEPS-Benutzer.
Profile	**Setup** > **WLAN** > **LEPS** > **Users**	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	**Setup** > **WLAN** > **LEPS** > **Users**	Vergeben Sie hier die Passphrase für die WLAN-Anmeldung dieses LEPS-Benutzers.
VLAN	**Setup** > **WLAN** > **LEPS** > **Users**	Hier können Sie festlegen, welchem VLAN der LEPS-Benutzer zugewiesen wird. Wird hier kein VLAN konfiguriert, gilt eine eventuelle, im LEPS-Profil konfigurierte VLAN. Wird sowohl im LEPS-Profil als auch am LEPS-Benutzer ein VLAN konfiguriert, gilt die am LEPS-Benutzer konfigurierte VLAN-ID.
MAC-Address	**Setup** > **WLAN** > **LEPS** > **Users**	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.

Empfehlungen

- **Setup** > **WLAN** > **LEPS** > **Operating**: **Yes** (LEPS aktivieren, damit Benutzer individuelle Passphrasen nutzen können)
- **Setup** > **WLAN** > **LEPS** > **Users** > **Profile**: „OfficeLEPS“ (Verbindung zum zuvor erstellten Profil)
- **Setup** > **WLAN** > **LEPS** > **Users** > **WPA-Passphrase**: Starke individuelle Passphrase verwenden
- **Setup** > **WLAN** > **LEPS** > **Users** > **MAC-Address**: Optional (nur bei Whitelist/Blacklist nötig)

5 RADIUS

Konfigurationseinstellungen der Parameter für RADIUS und IEEE 802.1X.

Pfad Konsole

Setup > **RADIUS**

5.1 RADIUS-Server

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

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Name	**Setup** > **RADIUS** > **RADIUS-Server**	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	**Setup** > **RADIUS** > **RADIUS-Server**	Wählen Sie hier den UDP-Port, der verwendet wird, um den RADIUS-Server zu kontaktieren.
Secret	**Setup** > **RADIUS** > **RADIUS-Server**	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.
Backup	**Setup** > **RADIUS** > **RADIUS-Server**	Konfigurieren Sie hier ein Backup-Profil, das genutzt wird, wenn der primäre RADIUS-Server nicht erreichbar ist.
Server-IP-Address	**Setup** > **RADIUS** > **RADIUS-Server**	Konfigurieren Sie hier den Hostnamen oder die IP-Adresse des RADIUS-Servers.
Accounting-Port	**Setup** > **RADIUS** > **RADIUS-Server**	Wählen Sie hier den UDP-Port, über den der RADIUS-Accounting-Server erreicht wird.
Accounting-IP-Address	**Setup** > **RADIUS** > **RADIUS-Server**	Konfigurieren Sie hier den Hostnamen oder die IP-Adresse des RADIUS-Accounting-Servers.

Empfehlungen

- **Setup** > **RADIUS** > **RADIUS-Server** > **Server-IP-Address**: IP-Adresse des RADIUS-Servers
- **Setup** > **RADIUS** > **RADIUS-Server** > **Port**: **1812** (Standardport für RADIUS-Authentifizierung)
- **Setup** > **RADIUS** > **RADIUS-Server** > **Secret**: Starkes gemeinsames Secret verwenden
- **Setup** > **RADIUS** > **RADIUS-Server** > **Backup**: Optional für Ausfallsicherheit
- **Setup** > **RADIUS** > **RADIUS-Server** > **Accounting-IP-Address**: IP-Adresse des RADIUS-Accounting-Servers für Nutzungsprotokollierung.
- **Setup** > **RADIUS** > **RADIUS-Server** > **Accounting-Port**: **1813** (Standardport für Accounting)

5.2 MAC-Check

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

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Fallback-Dynamic-VLAN-ID	**Setup** > **RADIUS** > **RADIUS-Server**	Wenn von einem RADIUS-Server keine VLAN-ID für einen WLAN-Client übermittelt wird, so wird die hier vergebene verwendet.
Require-Message-Authenticator	**Setup** > **RADIUS** > **RADIUS-Server**	Legt fest, ob ein Message-Authenticator in RADIUS-Nachrichten zwingend erforderlich ist. Nachrichten ohne Message-Authenticator werden verworfen.

Empfehlungen

- **Setup** > **RADIUS** > **RADIUS-Server** > **Require-Message-Authenticator**: **Yes** (Höhere Sicherheit, weil nur gültige RADIUS-Nachrichten akzeptiert werden.)

5.3 LAN-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.

Pfad Konsole

Setup > **RADIUS** > **LAN-Supplicant**

Parameter	Pfad	Beschreibung
Interface-Name	**Setup** > **RADIUS** > **LAN-Supplicant**	Der Name der LAN-Schnittstelle. Aktuell existiert nur die Schnittstelle INTRANET.
Method	**Setup** > **RADIUS** > **LAN-Supplicant**	Die zur Anmeldung an der 802.1X-Infrastruktur zu verwendende EAP-Methode.
Username	**Setup** > **RADIUS** > **LAN-Supplicant**	Der zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Benutzername.
Password	**Setup** > **RADIUS** > **LAN-Supplicant**	Das zur Anmeldung an der 802.1X-Infrastruktur zu verwendende Passwort.

Empfehlungen

- **Setup** > **RADIUS** > **LAN-Supplicant** > **Method**: **PEAP/MSCHAPv2** (sicherste Authentifizierungsmethode für Ihren LAN-Supplicant)
- **Setup** > **RADIUS** > **LAN-Supplicant** > **Username**: Eindeutiger 802.1X-Benutzername zur Authentifizierung am Switch.
- **Setup** > **RADIUS** > **LAN-Supplicant** > **Password**: Starkes Passwort oder Zertifikat zur Authentifizierung am Switch.verwenden.

5.4 WLAN-Supplicant

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

Pfad Konsole

Setup > **RADIUS** > **WLAN-Supplicant**

Parameter	Pfad	Beschreibung
Profile-Name	**Setup** > **RADIUS** > **WLAN-Supplicant**	Verwenden Sie einen eindeutigen Profilnamen, welchen Sie später im Verschlüsselungsprofil angeben.
Method	**Setup** > **RADIUS** > **WLAN-Supplicant**	Wählen Sie eine passende Authentifizierungsmethode. Bei TLS muss ein Zertifikat hochgeladen werden.
Username	**Setup** > **RADIUS** > **WLAN-Supplicant**	RADIUS-Benutzername. Bei TLS ist kein Eintrag erforderlich.
Password	**Setup** > **RADIUS** > **WLAN-Supplicant**	RADIUS-Passwort. Bei TLS ist kein Eintrag erforderlich.
Certificate	**Setup** > **RADIUS** > **WLAN-Supplicant**	Automatisch annehmen oder hochgeladenes Zertifikat prüfen. Empfehlung: Zertifikat hochladen, um Integrität des RADIUS-Servers sicherzustellen.
Delete-WLAN-Supplicant-Certificates	**Setup** > **RADIUS** > **WLAN-Supplicant**	Löscht alle vorhandenen Zertifikate der WLAN-Supplicants.

Empfehlungen

- **Setup** > **RADIUS** > **WLAN-Supplicant** > **Method**: **PEAP/MSCHAPv2** (sicherste Authentifizierungsmethode für den WLAN-Supplicant)
- **Setup** > **RADIUS** > **WLAN-Supplicant** > **Certificate**: **Container** (Zertifikat prüfen für Server-Integrität)

6 WLAN-Management

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

Pfad Konsole

Setup > **WLAN-Management**

6.1 Static-WLC-Configuration

Konfiguriert benutzerdefinierte WLAN-Controller. Dies ist notwendig, wenn ein WLC nicht automatisch gefunden wird und der DNS-Name „WLC-Address“ nicht verwendet werden kann.

Pfad Konsole

Setup > **WLAN-Management**

Parameter	Pfad	Beschreibung
IP-Address	**Setup** > **WLAN-Management** > **Static-WLC-Configuration**	Geben Sie die IP-Adresse oder den DNS-Namen eines WLAN-Controllers an.
Port	**Setup** > **WLAN-Management** > **Static-WLC-Configuration**	Konfiguriert den Port, unter dem versucht wird, einen WLC zu erreichen.
Operating	**Setup** > **WLAN-Management**	Konfiguriert, ob ein Access Point aktiv nach einem WLC sucht und von diesem verwaltet werden kann.
Update-Cert-Before	**Setup** > **WLAN-Management**	Gibt an, wie viele Tage vor Ablauf das Gerätezertifikat erneuert wird, das für die Authentifizierung am WLC genutzt wird.
Capwap-Port	**Setup** > **WLAN-Management**	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.

Empfehlung

- **Setup** > **WLAN-Management** > **Static-WLC-Configuration** > **IP-Address**: <IP-Adresse oder DNS-Name des WLC> (damit der Access Point den Controller auch bei gerouteten Netzwerken zuverlässig findet)
- **Setup** > **WLAN-Management** > **Static-WLC-Configuration** > **Port**: **1027**(Standard CAPWAP-Port, passend zum LANCOM WLC).
- **Setup** > **WLAN-Management** > **Operating**: **Yes** (ermöglicht dem Access Point, aktiv nach dem WLC zu suchen und verwaltet zu werden).
- **Setup** > **WLAN-Management** > **Update-Cert-Before**: **30** (Tage vor Ablauf. Stellt sicher, dass Zertifikate rechtzeitig erneuert werden)
- **Setup** > **WLAN-Management** > **Capwap-Port**: **5246** (Standardport für CAPWAP-Kommunikation, sorgt für stabile Verbindung zum WLC)

7 L2TP

LCOS LX unterstützt das Layer 2 Tunneling Protocol (L2TP) in Version 3. Bei L2TPv3 wird Ethernet-Traffic (Layer 2) getunnelt über UDP übertragen. Hiermit können also LANs über Netzwerk- und Standortgrenzen hinweg verbunden werden. Insbesondere bietet es sich an, WLAN-Traffic auf Seiten der Access Points in einen L2TPv3 Ethernet-Tunnel einzukoppeln und an einem zentralen Konzentrator wieder auszukoppeln. Dies erforderte ohne L2TPv3 immer einen WLAN-Controller, der dieses mittels CAPWAP Layer-3-Tunnel realisiert hat. Nun ist dies mit L2TPv3 losgelöst von WLAN-Controllern möglich, so dass der WLAN-Traffic getunnelt übertragen und zentral ausgekoppelt werden kann.

Pfad Konsole

Setup > **L2TP**

7.1 Endpoints

In dieser Tabelle werden die grundsätzlichen Einstellungen zur Konfiguration eines L2TP-Tunnels vorgenommen.

Pfad Konsole

Setup > **L2TP** > **Endpoints**

Parameter	Pfad	Beschreibung
Tunnel-Id	**Setup** > **L2TP** > **Endpoints**	Bezeichnung des Tunnel-Endpunkts. Bei authentifiziertem Tunnel müssen Tunnel-Id und Hostname überkreuz übereinstimmen.
IP-Address	**Setup** > **L2TP** > **Endpoints**	IP-Adresse oder FQDN des Tunnel-Endpunkts.
Port	**Setup** > **L2TP** > **Endpoints**	Zu nutzender UDP-Port für L2TP.
Hostname	**Setup** > **L2TP** > **Endpoints**	Benutzername für die Authentifizierung. Muss bei authentifiziertem Tunnel mit Tunnel-Id überkreuz übereinstimmen.
Password	**Setup** > **L2TP** > **Endpoints**	Passwort zur Authentifizierung; optional zur Verschleierung der Tunnelaushandlung.
Auth-Peer	**Setup** > **L2TP** > **Endpoints**	Gibt an, ob die Gegenstelle authentifiziert werden soll.
Hide	**Setup** > **L2TP** > **Endpoints**	Legt fest, ob die Tunnelaushandlung mithilfe des Passworts verschleiert werden soll.
Operating	**Setup** > **L2TP** > **Endpoints**	Aktiviert oder deaktiviert den L2TP-Endpunkt.

Empfehlung

- **Setup** > **L2TP** > **Endpoints** > **IP-Address**: IP-Adresse oder FQDN des Tunnel-Endpunkts
- **Setup** > **L2TP** > **Endpoints** > **Port**: **1701** (Standard-UDP-Port für L2TP)
- **Setup** > **L2TP** > **Endpoints** > **Hostname**: Benutzername zur Authentifizierung. Muss mit Tunnel-Id gekreuzt übereinstimmen.
- **Setup** > **L2TP** > **Endpoints** > **Password**: Passwort für Authentifizierung / optional für Verschleierung
- **Setup** > **L2TP** > **Endpoints** > **Auth-Peer**: **Yes** (Gegenstelle muss authentifiziert werden)
- **Setup** > **L2TP** > **Endpoints** > **Hide**: **Yes**(Tunnelaushandlung verschleiern)
- **Setup** > **L2TP** > **Endpoints** > **Operating**: **Yes** (Endpunkt aktivieren)

7.2 Ethernet

In dieser Tabelle verknüpfen Sie L2TPv3-Endpunkte mit einem WLAN-Netzwerk.

Pfad Konsole

Setup > **L2TP** > **Ethernet**

Parameter	Pfad	Beschreibung
L2TP-Endpoint	**Setup** > **L2TP** > **Ethernet**	Konfigurieren Sie hier den Namen des in der L2TP-Endpunkte-Tabelle konfigurierten L2TP-Endpunkts (2.61.1.1 Tunnel-Id). Somit wird eine Ethernet-Tunnel-Session über diesen Endpunkt aufgebaut. Wenn nur Verbindungen angenommen, aber nicht selber aufgebaut werden sollen, kann durch leer lassen des Feldes erwirkt werden, dass beliebige Sessions angenommen werden. Natürlich müssen diese trotzdem über einen akzeptierten / aufgebauten Endpunkt aus der L2TP-Endpunkte-Tabelle „laufen“. Dies kann in Szenarien, in denen nicht jeder Endpunkt auf der annehmenden Seite separat konfiguriert werden soll, sinnvoll sein.
Remote-End	**Setup** > **L2TP** > **Ethernet**	Name, anhand dessen der Ethernet-Tunnel auf der Gegenseite zugeordnet wird. Dieser Name muss auf beiden Seiten identisch sein.
Interface-Name	**Setup** > **L2TP** > **Ethernet**	Die für die L2TPv3-Session zu verwendende virtuelle Ethernet-Schnittstelle.
MTU	**Setup** > **L2TP** > **Ethernet**	Passt die MTU des Ethernet-Tunnels an, z. B. für Netzwerke mit kleineren MTU-Werten.

Empfehlung

- **Setup** > **L2TP** > **Ethernet** > **L2TP-Endpoint**: <Tunnel-Id aus Endpoints-Tabelle>
- **Setup** > **L2TP** > **Ethernet** > **Remote-End**: <Name des gegenüberliegenden Endpunkts> (Muss auf beiden Seiten identisch sein.)
- **Setup** > **L2TP** > **Ethernet** > **MTU**: **1500** (oder angepasst bei reduzierter Netzwerk-MTU)

8 IP-Configuration

In diesem Menü werden Parameter für die IP-Konfiguration des Gerätes konfiguriert.

Pfad Konsole

Setup > **IP-Configuration**

Parameter	Pfad	Beschreibung
Static-Parameters	**Setup** > **IP-Configuration**	Einstellungen rund um die IP- und Netzwerkkonfiguration bei Verwendung statischer IP-Adressen.
Interface-Name	**Setup** > **IP-Configuration** > **Static-Parameters**	Name des Interface, auf das sich die weiteren Einstellungen beziehen.
IPv4-Gateway	**Setup** > **IP-Configuration** > **Static-Parameters**	Konfiguration des IPv4-Gateways für das referenzierte Interface.
IPv6-Gateway	**Setup** > **IP-Configuration** > **Static-Parameters**	Konfiguration des IPv6-Gateways für das referenzierte Interface.
Primary-IPv4-DNS	**Setup** > **IP-Configuration** > **Static-Parameters**	Primärer IPv4-DNS-Server für das referenzierte Interface.
Secondary-IPv4-DNS	**Setup** > **IP-Configuration** > **Static-Parameters**	Sekundärer IPv4-DNS-Server für Redundanz.
Primary-IPv6-DNS	**Setup** > **IP-Configuration** > **Static-Parameters**	Primärer IPv6-DNS-Server für das referenzierte Interface.
Secondary-IPv6-DNS	**Setup** > **IP-Configuration** > **Static-Parameters**	Sekundärer IPv6-DNS-Server für Redundanz.

Empfehlungen

- **Setup** > **IP-Configuration** > **Static-Parameters** > **IPv4-Gateway**: <interne, vertrauenswürdige IPv4-Adresse des Gateway>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **IPv6-Gateway**: <interne, vertrauenswürdige IPv6-Adresse des Gateway>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **Primary-IPv4-DNS**: <interne IPv4-Adresse des DNS-Servers>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **Secondary-IPv4-DNS**: <interne IPv4-Adresse des sekundären DNS-Servers>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **Primary-IPv6-DNS**: <interne IPv6-Adresse des DNS-Servers>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **Secondary-IPv6-DNS**: <interne IPv6-Adresse des sekundären DNS-Servers>

8.1 LAN-Interfaces

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

Pfad Konsole

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

Parameter	Pfad	Beschreibung
Interface-Name	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Vergeben Sie hier einen sprechenden Namen für das Interface. Dieser Name wird in weiteren Teilen der Konfiguration referenziert.
VLAN-ID	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Definieren Sie hier die VLAN-ID, für die das Interface aktiv sein soll.
IPv4-Address-Source	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Wählen Sie die Quelle der IPv4-Adresse für das Interface.
IPv6-Address-Source	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Wählen Sie die Quelle der IPv6-Adresse für das Interface.
Static-IPv4-Address	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als IPv4-Address-Source static eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/24“).
Static-IPv6-Address	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Konfigurieren Sie hier die IP-Adresse, welche genutzt wird, wenn als IPv6-Address-Source static eingestellt ist. Ergänzen Sie die Subnetz-Maske in CIDR-Notation (z. B. „/64“).

Empfehlungen

- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **VLAN-ID**: Getrenntes Management- oder Client-VLAN (z. B. 10 für Management, 20 für WLAN)
- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **IPv4-Address-Source**: **static** (falls feste IP benötigt, sonst DHCP)
- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **IPv6-Address-Source**: **static** (oder Router-Advertisement, falls Netzwerk dynamisch IPv6 verteilt)
- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **Static-IPv4-Address**: <z. B. 192.168.10.5/24>
- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **Static-IPv6-Address**: <z. B. fd00:10::5/64>

8.2 LMC

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

Pfad Konsole

Setup > **LMC**

Parameter	Pfad	Beschreibung
Operating	**Setup** > **LMC**	Legen Sie fest, ob das Gerät über die LMC verwaltet werden soll.
Proxy	**Setup** > **LMC**	Soll die Verbindung vom Gerät zur LMC über einen HTTP-Proxy-Server aufgenommen werden, kann dieser hier konfiguriert werden. Sobald eine Proxy-URL eingetragen ist, wird die LMC-Verbindung immer über den Proxy-Server aufgenommen. Ist zusätzlich der Schalter (2.102.2.4 Tunnel) aktiviert, wird eine transparenter Tunnel über den Proxy-Server mittels der HTTP CONNECT-Methode verwendet. Der Proxy-Server muss dies unterstützen. Ist der Schalter nicht aktiviert, werden einzelne HTTP-Requests über den Proxy weitergeleitet.

Parameter	Pfad	Beschreibung
URL	**Setup** > **LMC** > **Proxy**	Soll die Verbindung vom Gerät zur LMC über einen HTTP-Proxy-Server aufgenommen werden, kann dieser hier konfiguriert werden. Sobald eine Proxy-URL eingetragen ist, wird die LMC-Verbindung immer über den Proxy-Server aufgenommen.
Username	**Setup** > **LMC** > **Proxy**	Benutzername für die Authentifizierung am Proxy-Server.
Password	**Setup** > **LMC** > **Proxy**	Passwort für die Authentifizierung am Proxy-Server.
Tunnel	**Setup** > **LMC** > **Proxy**	Falls eine Proxy-URL angegeben wurde und dieser Schalter aktiviert wird, dann wird ein transparenter Tunnel über den Proxy-Server mittels der HTTP CONNECT-Methode verwendet. Der Proxy-Server muss dies unterstützen. Ist der Schalter nicht aktiviert, werden einzelne HTTP-Requests über den Proxy weitergeleitet.
Delete-Certificate	**Setup** > **LMC**	Löscht das bestehende LMC-Zertifikat.

Empfehlungen

- **Setup** > **LMC** > **Operating**: **No** (nur aktivieren, wenn Verwaltung über LMC gewünscht ist)
- **Setup** > **LMC** > **Proxy** > **URL**: <Proxy-URL nur bei Bedarf eintragen>
- **Setup** > **LMC** > **Proxy** > **Username**: Benutzername für Proxy, falls notwendig
- **Setup** > **LMC** > **Proxy** > **Password**: Sicheres Passwort, falls Proxy genutzt wird
- **Setup** > **LMC** > **Proxy** > **Tunnel**: **Yes** (HTTP CONNECT Tunnel verwenden, sofern Proxy unterstützt)
- **Setup** > **LMC** > **Delete-Certificate**: Nur bei Zertifikatswechsel oder Bereinigung verwenden.

9 Automatic-Firmware-Update

Der LANCOM Auto Updater ermöglicht die automatische Aktualisierung von im Feld befindlichen LANCOM Geräten ohne weiteren Benutzereingriff (unattended). LANCOM Geräte können auf Wunsch ohne Nutzerinteraktion nach neuen Software-Updates suchen, diese herunterladen und einspielen. Sie wählen, ob Sie Security Updates, Release Updates oder alle Updates automatisch installieren möchten.

Sollen keine automatischen Updates durchgeführt werden, so kann das Feature auch zur Prüfung auf neue Updates verwendet werden. Der LANCOM Auto Updater kontaktiert zur Update-Prüfung und zum Firmware-Download den LANCOM Update-Server. Die Kontaktaufnahme erfolgt via HTTPS.

Bei der Kontaktaufnahme wird der Server mittels der im LANCOM Gerät bereits hinterlegten TLS-Zertifikate validiert. Zusätzlich sind Firmware-Dateien für aktuelle LANCOM Geräte signiert. Der LANCOM Auto Updater validiert vor dem Einspielen einer Firmware diese Signatur.

Pfad Konsole

Setup > **Automatic-Firmware-Update**

Parameter	Pfad	Beschreibung
Mode	**Setup** > **Automatic-Firmware-Update**	Legt den Betriebsmodus des Auto Updaters fest.
Check-Firmware-Now	**Setup** > **Automatic-Firmware-Update**	Startet sofort eine Prüfung auf neue Firmware-Versionen.
Update-Firmware-Now	**Setup** > **Automatic-Firmware-Update**	Lädt die neueste Firmware herunter und installiert sie.
Cancel-Current-Action	**Setup** > **Automatic-Firmware-Update**	Bricht die aktuell laufende Auto-Updater-Aktion ab. Dies bezieht sich sowohl auf manuell gestartete als auch auf geplant ausgeführte Aktionen.
Reset-Updater-Config	**Setup** > **Automatic-Firmware-Update**	Dieser Befehl setzt die auf den Auto Updater bezogenen bootpersistenten Konfigurationsdateien zurück. Dies schließt die lokale Blacklist ein, die Firmware-Versionen enthält, mit denen ein automatisches Update fehlgeschlagen ist.
Base-URL	**Setup** > **Automatic-Firmware-Update**	URL des Firmware-Update-Servers.
Check-Interval	**Setup** > **Automatic-Firmware-Update**	Gibt an, in welchem Intervall nach Updates gesucht wird. Der Updater wählt automatisch einen zufälligen Zeitpunkt im Intervall.
Version-Policy	**Setup** > **Automatic-Firmware-Update**	Steuert, welche Firmware-Versionen dem Gerät angeboten werden.

Empfehlungen

- **Setup** > **Automatic-Firmware-Update** > **Mode**: **Check** (immer aktuellen Firmwarestand prüfen)
- **Setup** > **Automatic-Firmware-Update** > **Cancel-Current-Action**: Bei Bedarf laufende Aktionen abbrechen
- **Setup** > **Automatic-Firmware-Update** > **Check-Interval**: **Daily** (kürzestes Intervall)
- **Setup** > **Automatic-Firmware-Update** > **Version-Policy**: **security-updates-only** (nur sicherheitsrelevante Updates)
- **Setup** > **Automatic-Firmware-Update** > **Reset-Updater-Config**: Nur bei Fehlern oder fehlerhafter Konfiguration verwenden.