LANCOM Access Points

Security-relevant settings

01/2026

LANCOM SYSTEMS

Contents

1 LCOS LX version and syntax description

This document describes the security-relevant settings of LCOS LX-based access points. It serves as a reference for device administration and the secure operation of LANCOM access points.

The settings described apply to devices running at least LCOS LX version 7.10. In order to ensure comprehensive protection, especially in the area of centralized administrator management, the features of this LCOS LX version are required.

For all configuration parameters listed, the corresponding command-line path, the required commands for setting parameters, and recommendations for security-relevant values are provided.

For all encryption and hash mechanisms, we recommend always using the strongest cryptographic algorithms available.

Please observe the minimum requirements for secure passwords:

To meet the minimum password requirements, the guidelines below should be followed. Passwords must not appear in dictionaries, should not contain personal data (e. g. date of birth, pet name), and must not be based on keyboard patterns (e. g. “qwerty”).

A password can be derived from a mnemonic sentence and must use all four character sets (uppercase letters, lowercase letters, digits, and special characters) (e. g. “Our regional association consists of 13 municipalities and we all really enjoy working there!” results in the memorable password “ORAco13Mawearewd!”).

Note: Be sure to create your own individual mnemonic sentence.

The password should be at least 10 characters long or use the maximum number of characters technically possible. This also applies to passwords for access to sensitive areas, e. g. passwords for system administrators.

To meet the complexity requirements, all of the following character sets must be used:

- Uppercase letters (A to Z)
- Lowercase letters (a to z)
- Digits (0 to 9)
- Special characters (e. g. !, $, -, %)

If this is not possible, at least the technically available character sets must be used.

Please also observe the *guideline of the German Federal Office for Information Security on creating secure passwords*.

2 SNMP

In this menu, you configure SNMP.

Console path

Setup

Parameter	Path	Description
Send-Traps	**Setup** > **SNMP**	In the event of serious errors, for example unauthorized access, the device can automatically send an error message to one or more SNMP managers. To do so, enable this option and specify the targets on which these SNMP managers are installed in the **Target-Addresses** table.
Port	**Setup** > **SNMP**	This parameter defines the port through which the SNMP service can be reached by external applications such as, e. g. LANmonitor.
Admitted-Protocols	**Setup** > **SNMP**	Enable the SNMP versions that the device is to support for SNMP requests and SNMP traps.
Allow-Admins	**Setup** > **SNMP**	If registered administrators (including the `root` user) are also to be granted access via SNMPv3, enable this option.
Operating	**Setup** > **SNMP**	This entry enables or disables SNMP traps.

Recommendations

- **Setup** > **SNMP** > **Admitted-Protocols**: Use **SNMPv3**.
- **Setup** > **SNMP** > **Allow-Admins**: **No** (use **Yes** only in exceptional cases).
- **Setup** > **SNMP** > **Operating**: **Yes** (only if trap recipients are defined; otherwise **No**).

2.1 Communities

In this menu, you configure the SNMP communities.

Description

SNMP agents and SNMP managers belong to SNMP communities. These communities group specific SNMP hosts together, making them easier to manage. At the same time, SNMP communities provide a limited level of security for SNMP access, as an SNMP agent only accepts SNMP requests from members whose community is known to it. In this table, you configure the SNMP communities.

SNMP communities are required only when using SNMPv1 and SNMPv2. For security reasons, LANCOM Systems recommends always using SNMPv3.

Console path

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

Parameter	Path	Description
Name	**Setup** > **SNMP** > **Communities**	Assign a meaningful name to this SNMP community.
Security-Name	**Setup** > **SNMP** > **Communities**	Enter the name of the access policy that defines the access rights for all community members.
Status	**Setup** > **SNMP** > **Communities**	Use this entry to enable or disable this SNMP community.

Recommendations

- Disable or delete the default community `public`.
- Never leave the predefined community `public` enabled, as it is widely known and allows unauthorized read access.
- Use custom communities with complex names: at least 16 characters, a random combination of uppercase/lowercase letters, numbers, and special characters.
- **Disable** or delete communities that are not required.
- Set communities that are not in use to **Inactive** or **delete** them entirely.

2.2 Groups

By configuring SNMP groups, authentication and access rights for multiple users can be conveniently managed and assigned.

Console path

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

Parameter	Path	Description
Security-Model	**Setup** > **SNMP** > **Groups**	SNMPv3 introduced the concept of a “security model”, which is why the “SNMPv3” security model is primarily used in the SNMP configuration of LCOS LX. For compatibility reasons, however, it may be necessary to also consider SNMPv2c or even SNMPv1 and select them accordingly as the security model.
Security-Name	**Setup** > **SNMP** > **Groups**	Select a security name here that you have assigned to an SNMP community. It is also possible to specify the name of an already configured user.
Group-Name	**Setup** > **SNMP** > **Groups**	Assign a descriptive name to this group. You will subsequently use this name when configuring access rights.
Status	**Setup** > **SNMP** > **Groups**	Enables or disables this group configuration.

Recommendations

- **Setup** > **SNMP** > **Groups** > **Security-Model**: Use **SNMPv3_USM** (AuthPriv with SHA + AES).
- **Setup** > **SNMP** > **Groups** > **Status**: Enable only the required groups and disable all others.

2.3 Accesses

This table consolidates the various configurations for access rights, security models, and views.

Console path

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

Parameter	Path	Description
Security-Model	**Setup** > **SNMP** > **Accesses**	Enable the appropriate security model here.
Read-View-Name	**Setup** > **SNMP** > **Accesses**	Define the view of MIB entries for which this group is granted read access.
Write-View-Name	**Setup** > **SNMP** > **Accesses**	Define the view of MIB entries for which this group is granted write access.
Notify-View-Name	**Setup** > **SNMP** > **Accesses**	Define the view of MIB entries for which this group is granted notify rights.
Status	**Setup** > **SNMP** > **Accesses**	Enables or disables this entry.
Min-Security-Level	**Setup** > **SNMP** > **Accesses**	Specify the minimum security level required for access and data transmission.

Recommendations

- **Setup** > **SNMP** > **Accesses** > **Security-Model**: Use **SNMPv3_USM**.
- **Setup** > **SNMP** > **Accesses** > **Write-View-Name**: Leave empty and define only if strictly required.
- **Setup** > **SNMP** > **Accesses** > **Status**: Enable only the required entries.
- **Setup** > **SNMP** > **Accesses** > **Min-Security-Level**: Use **AuthPriv** (SHA + AES).

2.4 Views

In this table, you group individual values or entire branches of the device MIB that a user is allowed to view or modify according to their access rights.

Console path

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

Parameter	Path	Description
View-Name	**Setup** > **SNMP** > **Views**	Assign a descriptive name to the view.
OID-Subtree	**Setup** > **SNMP** > **Views**	Specify, as a comma-separated list of OIDs, which MIB values and actions are to be included in this view.
Type	**Setup** > **SNMP** > **Views**	Define whether the specified OID subtrees are part of the view (**Included**) or not part of the view (**Excluded**).
Status	**Setup** > **SNMP** > **Views**	Enables or disables this view.

Recommendations

- **Setup** > **SNMP** > **Views** > **OID-Subtree**: Use only relevant monitoring OIDs (e. g. `ifTable`, `System status`).
- **Setup** > **SNMP** > **Views** > **Type**: Use **Included** for required OIDs and **Excluded** for sensitive OIDs.
- **Setup** > **SNMP** > **Views** > **Status**: Enable only the required views and disable the rest.

2.5 Users

This menu contains the user configuration for SNMPv3.

Console path

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

Parameter	Path	Description
Username	**Setup** > **SNMP** > **Users**	Specify the SNMPv3 user name here.
Authentication-Protocol	**Setup** > **SNMP** > **Users**	Define the method the user must use to authenticate to the SNMP agent.
Authentication-Password	**Setup** > **SNMP** > **Users**	Enter the password required for user authentication.
Privacy-Password	**Setup** > **SNMP** > **Users**	Enter the password required for encryption.
Status	**Setup** > **SNMP** > **Users**	Enables or disables this user.
Authentication-Password-Type	**Setup** > **SNMP** > **Users**	Password type used for authentication. To enter a new password, the type must be temporarily set to **Plaintext**. After entry, LCOS LX automatically encrypts the password and resets the value to **Masterkey**.
Privacy-Password-Type	**Setup** > **SNMP** > **Users**	Password type used for encryption. To enter a new password, the type must be temporarily set to **Plaintext**. After entry, LCOS LX automatically encrypts the password and resets the value to **Masterkey**.

Recommendations

- **Setup** > **SNMP** > **Users** > **Authentication-Protocol**: Use **HMAC-SHA256** or higher.
- **Setup** > **SNMP** > **Users** > **Authentication-Password**: Use a long, complex password and rotate it regularly.
- **Setup** > **SNMP** > **Users** > **Privacy-Protocol**: Use **AES256**.
- **Setup** > **SNMP** > **Users** > **Privacy-Password**: Use a separate, complex password—not identical to the Authentication-Password.
- **Setup** > **SNMP** > **Users** > **Authentication-Password-Type** / **Privacy-Password-Type**: Use **Masterkey** (default). Use **Plaintext** only temporarily for password entry.
- **Setup** > **SNMP** > **Users** > **Status**: Use only active and required users.

2.6 Target-Addresses

In this table, you configure the recipients to which the SNMP agent sends SNMP traps.

Console path

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

Parameter	Path	Description
Name	**Setup** > **SNMP** > **Target-Addresses**	Specify the target address name here.
Transport-Address	**Setup** > **SNMP** > **Target-Addresses**	The transport address describes the IP address and port number of an SNMP trap receiver and is specified in the format `<IP address>:<Port>` (e. g. `128.1.2.3:162`). UDP port 162 is used for SNMP traps.
Parameters-Name	**Setup** > **SNMP** > **Target-Addresses**	Select the desired entry from the list of recipient parameters here.
Status	**Setup** > **SNMP** > **Target-Addresses**	Enables or disables this target address.

Recommendations

- **Setup** > **SNMP** > **Target-Addresses** > **Status**: Enable only productive targets and disable all others.

2.7 Target-Params

In this table, you configure how the SNMP agent processes the SNMP traps that it sends to the recipients.

Console path

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

Parameter	Path	Description
Name	**Setup** > **SNMP** > **Target-Params**	Assign a descriptive name to this entry.
Message-Processing-Model	**Setup** > **SNMP** > **Target-Params**	Specify the protocol according to which the SNMP agent structures the message.
Security-Model	**Setup** > **SNMP** > **Target-Params**	Use this entry to define the security model.
Security-Name	**Setup** > **SNMP** > **Target-Params**	Select a security name that you have assigned to an SNMP community. Alternatively, you can specify the name of an already configured user.
Security-Level	**Setup** > **SNMP** > **Target-Params**	Define the security level that applies when the recipient receives SNMP traps.
Status	**Setup** > **SNMP** > **Target-Params**	Enables or disables this entry.

Recommendations

- **Setup** > **SNMP** > **Target-Params** > **Message-Processing-Model**: Use **SNMPv3**.
- **Setup** > **SNMP** > **Target-Params** > **Security-Model**: Use **SNMPv3_USM**.

- **Setup** > **SNMP** > **Target-Params** > **Security-Level**: Use **AuthPriv**.
- **Setup** > **SNMP** > **Target-Params** > **Status**: **Active** (for productive entries only).

3 Config

Contains the general configuration settings.

Console path

Setup > **Config**

Parameter	Path	Description
Administrator	**Setup** > **Config**	Name of the device administrator. Used for display purposes only.
Config-Aging-Minutes	**Setup** > **Config**	Specifies after how many minutes of inactivity a configuration connection via TCP (e.g. an SSH connection) is automatically terminated.
Admins	**Setup** > **Config**	In this table, you define administrators who may have restricted privileges.
Administrator	**Setup** > **Config** > **Admins**	Login name of the administrator in this row of the table.
Function-Rights	**Setup** > **Config** > **Admins**	Enable the functional rights of the administrator in this row of the table.
Rights	**Setup** > **Config** > **Admins**	The permissions assigned to the administrator in this row of the table.
Hashed-Password	**Setup** > **Config** > **Admins**	Hash value of the administrator's password in this row of the table.

Recommendations

- **Setup** > **Config** > **Admins** > **Administrator**: Use an individual username for each administrator.
- **Setup** > **Config** > **Admins** > **Function-Rights** / **Setup** > **Config** > **Admins** > **Rights**: Assign only the permissions that are required (principle of least privilege).

3.1 TACACS+

Configure authentication, authorization, and accounting (AAA) using the TACACS+ protocol here.

Console path

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

Parameter	Path	Description
Operating	**Setup** > **Config** > **Tacacs-Plus**	Enables or disables the use of TACACS+.
Internal-fallback-allowed	**Setup** > **Config** > **Tacacs-Plus**	If this option is enabled, login using local user credentials is possible if the TACACS+ servers are unreachable.
Server-Address	**Setup** > **Config** > **Tacacs-Plus**	The IP address of the primary TACACS+ server.
Server-Port	**Setup** > **Config** > **Tacacs-Plus**	The port of the primary TACACS+ server.
Server-Secret	**Setup** > **Config** > **Tacacs-Plus**	The shared secret used for communication with the primary TACACS+ server.

Parameter	Path	Description
Spare-Server-Address	**Setup** > **Config** > **Tacacs-Plus**	The IP address of the backup TACACS+ server.
Spare-Server-Port	**Setup** > **Config** > **Tacacs-Plus**	The port of the backup TACACS+ server.
Spare-Server-Secret	**Setup** > **Config** > **Tacacs-Plus**	The shared secret used for communication with the backup TACACS+ server.

Recommendations

- **Setup** > **Config** > **Tacacs-Plus** > **Operating**: **Yes**
- **Setup** > **Config** > **Tacacs-Plus** > **Internal-fallback-allowed**: **No**
- **Setup** > **Config** > **Tacacs-Plus** > **Server-Address**: Use an internal management IP (e.g. 10.0.0.10).
- **Setup** > **Config** > **Tacacs-Plus** > **Server-Port**: **49**
- **Setup** > **Config** > **Tacacs-Plus** > **Server-Secret**: Use a strong secret with at least 32 characters.
- **Setup** > **Config** > **Tacacs-Plus** > **Spare-Server-Address**: Use an internal backup IP (e.g. 10.0.0.11).
- **Setup** > **Config** > **Tacacs-Plus** > **Spare-Server-Port**: **49**
- **Setup** > **Config** > **Tacacs-Plus** > **Spare-Server-Secret**: Use a separate strong secret.

3.2 SSH

Configure SSH settings here.

Console path

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

Parameter	Path	Description
RSA-Hostkey-Length	**Setup** > **Config** > **SSH**	The length of the SSH host key can be set between 2048 bits and 4096 bits. After changing this setting, the host key is regenerated immediately.
Root-Hashed	**Setup** > **Config** > **SSH**	Hash value of the root administrator's password.

Recommendations

- **Setup** > **Config** > **SSH** > **RSA-Hostkey-Length**: Use a key length of **4096 bits**.

4 WLAN

Configuration settings for WLAN parameters.

Console path

Setup > **WLAN**

4.1 Network

Configure all general settings related to the WLAN networks (SSIDs) that are broadcast. Add one row to the table for each WLAN network. By default, the table is empty.

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

Parameter	Path	Description
Network-Name	**Setup** > **WLAN** > **Network**	Configure a descriptive name for the WLAN network. This internal name is used to reference the interface configuration in other parts of the configuration.
SSID-Name	**Setup** > **WLAN** > **Network**	Configure the externally visible name of the SSID.
Closed-Network	**Setup** > **WLAN** > **Network**	Configure whether the SSID should be displayed to clients during network scans. If SSID broadcasting is suppressed, the access point no longer responds to probe requests with an empty SSID. In this case, the SSID must be explicitly configured on the client in order to establish a connection.
Max-Stations	**Setup** > **WLAN** > **Network**	Maximum number of WLAN clients that can be connected simultaneously.
Inter-Station-Traffic	**Setup** > **WLAN** > **Network**	Depending on the use case, it may or may not be desirable for WLAN clients connected to an access point to communicate with other clients. Configure here whether communication between WLAN clients within the WLAN network is permitted.
Client-Isolation	**Setup** > **WLAN** > **Network**	If communication between WLAN clients or communication to unauthorized destinations in the network should be prevented, client isolation can be configured. This blocks all traffic originating from WLAN clients to destinations that are not explicitly listed in a whitelist. Client isolation can be enabled per SSID.
Min-Client-Strength	**Setup** > **WLAN** > **Network**	Configure the minimum signal strength in percent at which a client must be “seen” by the access point in order to be allowed to associate with the WLAN network.
Exclude-From-Client-Management	**Setup** > **WLAN** > **Network**	Optionally excludes this SSID from band steering.
Timeframe	**Setup** > **WLAN** > **Network**	Name of a timeframe used to enable or disable the SSID based on a schedule.
Block-Multicast	**Setup** > **WLAN** > **Network**	Blocks multicast traffic for IPv4 and/or IPv6.

Parameter	Path	Description
Bridge	**Setup** > **WLAN** > **Network**	Used internally during WLC operation, or when using L2TP the L2TP interface must be specified here.
Key	**Setup** > **WLAN** > **Network**	Configure the pre-shared key (PSK) of the SSID.
Encryption-Profile	**Setup** > **WLAN** > **Network**	Select an encryption profile from **Setup** > **WLAN** > **Encryption** that defines which authentication and encryption methods are used for the SSID.
Idle-Timeout	**Setup** > **WLAN** > **Network**	Time in seconds after which inactive clients are disconnected. Any traffic from the client resets the timer.

Recommendations

- **Setup** > **WLAN** > **Network** > **Inter-Station-Traffic**: **Yes** (If clients should be able to communicate with each other)
- **Setup** > **WLAN** > **Network** > **Client-Isolation**: **No** (No isolation, internal communication allowed)
- **Setup** > **WLAN** > **Network** > **Min-Client-Strength**: **20** (Prevents very weak connections)
- **Setup** > **WLAN** > **Network** > **Block-Multicast**: **No** (Allows multicast, e.g. for printers/streaming)
- **Setup** > **WLAN** > **Network** > **Key**: Use a strong WPA3-PSK password (high security for WLAN access)
- **Setup** > **WLAN** > **Network** > **Idle-Timeout**: **600** seconds (Disconnects inactive clients after 10 minutes, conserving resources)

4.2 Encryption

Configure all settings related to encryption and authentication for the WLAN networks.

Console path

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

Parameter	Pfad	Description
Profile-Name	**Setup** > **WLAN** > **Encryption**	Select a descriptive name for the encryption profile. This internal name is used to reference the encryption profile in other parts of the configuration.
Encryption	**Setup** > **WLAN** > **Encryption**	Configure whether the WLAN network should be encrypted or whether no encryption should be used (open network).
Method	**Setup** > **WLAN** > **Encryption**	Configure the encryption method.
WPA-Version	**Setup** > **WLAN** > **Encryption**	Configure the WPA version used for the encryption methods 802.11i-WPA-PSK and 802.11i-WPA-802.1X.
WPA-Rekeying-Cycle	**Setup** > **WLAN** > **Encryption**	A 48-bit initialization vector (IV) made it more difficult for attackers to calculate the key with WEP. WPA also introduced the use of a new key for each data packet (per-packet key mixing and re-keying). The repetition of the actual key consisting of IV and the WPA key would only occur after 16 million packets—after several hours in heavily used WLANs. To prevent the actual key from being repeated, WPA provides automatic key renegotiation at regular intervals. This prevents the actual key from being reused. Configure here the time in seconds after which the access point performs a key exchange when a WPA version is used.

Parameter	Pfad	Description
WPA1-Session-Keytypes	**Setup** > **WLAN** > **Encryption**	Configure which session key type is used for WPA version 1. This also affects the encryption method used.
WPA2-3-Session-Keytypes	**Setup** > **WLAN** > **Encryption**	Configure which session key types should be offered for WPA version 2 or 3. This also affects the encryption method used.
Prot.-Mgmt-Frames	**Setup** > **WLAN** > **Encryption**	The management information transmitted in a WLAN for establishing and operating data connections is unencrypted by default. Anyone within a WLAN cell can receive and evaluate this information even if they are not associated to an access point. While this does not pose a risk to an encrypted data connection, it can significantly disrupt communication within a WLAN cell through forged management information. The IEEE 802.11w standard encrypts transmitted management information (Protected Management Frames, PMF), preventing an attacker who does not possess the corresponding key from disrupting the communication.
Prot.-Beacons	**Setup** > **WLAN** > **Encryption**	The IEEE 802.11be (WiFi 7) standard requires the use of Beacon Protection. Configure it here.
Pre-Authentication	**Setup** > **WLAN** > **Encryption**	Fast authentication using the Pairwise Master Key (PMK) only works if the WLAN client has previously associated to the access point. To shorten the time required to associate to an access point even on the first attempt, the WLAN client uses pre-authentication. Typically, a WLAN client scans the surroundings in the background for available access points so it can reconnect to one of them if necessary. Access points that support WPA2/802.1X can advertise their pre-authentication capability to requesting WLAN clients. WPA2 pre-authentication differs from normal 802.1X authentication in the following ways: › The WLAN client pre-authenticates to the new access point via the infrastructure network that connects the access points to each other. This can be an Ethernet connection, a WDS link (Wireless Distribution System), or a combination of both. › A different Ethernet protocol (EtherType) distinguishes pre-authentication from normal 802.1X authentication. As a result, the current access point and all other network participants treat the pre-authentication as normal data traffic from the WLAN client. › After successful pre-authentication, both the new access point and the WLAN client store the negotiated PMK.
OKC	**Setup** > **WLAN** > **Encryption**	This option enables or disables Opportunistic Key Caching (OKC).
WPA2-Key-Management	**Setup** > **WLAN** > **Encryption**	Specify which standard WPA2 key management should follow.
PMK-IAPP-Secret	**Setup** > **WLAN** > **Encryption**	This passphrase is used to implement encrypted Opportunistic Key Caching. This is required for fast roaming via IAPP. A unique IAPP passphrase must be assigned to each interface in the WLAN connection settings. It is used to encrypt the Pairwise Master Keys (PMKs). This allows access points with matching IAPP passphrases (PMK-IAPP-Secret) to exchange PMKs with each other and ensure uninterrupted connections. Therefore, ensure that this passphrase

Parameter	Pfad	Description
		is identical on all access points between which fast roaming is intended.
RADIUS-Server-Profile	**Setup** > **WLAN** > **Encryption**	Configure the RADIUS server profile that is used when 802.1X is enabled. When using PSK-based encryption methods, no entry is required here.
SAE/OWE-Groups	**Setup** > **WLAN** > **Encryption**	Contains the selection of the offered Diffie-Hellman groups as a bitmask, on the basis of which the protocol peers generate a key for data exchange. The available groups use elliptic curves. The SAE (Simultaneous Authentication of Equals) authentication method used with WPA3 uses these methods together with AES to generate a cryptographically strong key.

Recommendations

- **Setup** > **WLAN** > **Encryptionn** > **Encryption**: **Yes** (Always enable encryption for secure data transmission).
- **Setup** > **WLAN** > **Encryption** > **Method**: **802.11i-WPA-PSK** or **802.11i-WPA-802.1X** (Secure methods for PSK or RADIUS).
- **Setup** > **WLAN** > **Encryption** > **WPA-Version**: **WPA3** (Maximum security; modern WLAN clients support this).
- **Setup** > **WLAN** > **Encryption** > **WPA-Rekeying-Cycle**: **3600** seconds (Renew keys regularly; helps prevent key reuse).
- **Setup** > **WLAN** > **Encryption** > **WPA2-3-Session-Keytypes**: **AES-CCMP-256** or **AES-GCMP-256** (Only works with compatible clients. Avoid using TKIP because it is no longer considered secure).
- **Setup** > **WLAN** > **Encryption** > **Prot.-Mgmt-Frames**: **Mandatory** (Encrypt management frames; protects against manipulation).
- **Setup** > **WLAN** > **Encryption** > **Prot.-Beacons**: **Yes** (Enable Beacon Protection for Wi-Fi 7).
- **Setup** > **WLAN** > **Encryption** > **Pre-Authentication**: **Yes** (Faster association during roaming between access points).
- **Setup** > **WLAN** > **Encryption** > **WPA2-Key-Management**: **Standard+Fast-Roaming** (Roaming for modern WLAN clients; standard for legacy clients).
- **Setup** > **WLAN** > **Encryption** > **PMK-IAPP-Secret**: Identical on all access points (Secure fast roaming via IAPP).
- **Setup** > **WLAN** > **Encryption** > **RADIUS-Server-Profile**: Only required for 802.1X; otherwise leave blank (PSK does not require RADIUS).
- **Setup** > **WLAN** > **Encryption**: Select the highest available groups when using WPA3. Otherwise, this is not relevant.

4.3 Client-Isolation-Allowed

Configure the allowed destinations for client isolation here.

Console path

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

Parameter	Pfad	Description
Network-Name	**Setup** > **WLAN** > **Client-Isolation-Allowed**	Select the network or SSID to which this entry applies. Then optionally specify a destination IP address.
IP-Network	**Setup** > **WLAN** > **Client-Isolation-Allowed**	Allowed destination IP address for this network.

Parameter	Pfad	Description
MAC-Address	**Setup** > **WLAN** > **Client-Isolation-Allowed**	Allowed destination MAC address for this network.

Recommendations

- **Setup** > **WLAN** > **Client-Isolation-Allowed** > **Network-Name**: Select the SSID (enable isolation only for the desired WLAN)
- **Setup** > **WLAN** > **Client-Isolation-Allowed** > **IP-Network**: Enter IP addresses of allowed destinations (e.g. printers or servers)
- **Setup** > **WLAN** > **Client-Isolation-Allowed** > **MAC-Address**: Enter MAC addresses of allowed devices (additional security)

4.4 LEPS

With LANCOM Enhanced Passphrase Security (LEPS), you can assign custom passphrases to WLAN stations without having to register the stations in advance by their MAC address.

Console path

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

Parameter	Pfad	Description
Operating	**Setup** > **WLAN** > **LEPS**	Enables or disables LEPS. When disabled, the configured LEPS users are ignored when WLAN clients attempt to log in.
Profiles	**Setup** > **WLAN** > **LEPS**	Configure LEPS profiles here and link them to an SSID. You can then assign LEPS profiles to LEPS users. Profile values can be overridden.
Name	**Setup** > **WLAN** > **LEPS** > **Profiles**	Assign a unique name to the LEPS profile.
Network-Name	**Setup** > **WLAN** > **LEPS** > **Profiles**	Select the SSID—or, when using a WLC, the logical WLAN network—for which the LEPS profile is to apply. Only LEPS users who are linked via the LEPS profile can log on to the SSID or, with a WLC, to the logical WLAN network.
Mac-List	**Setup** > **WLAN** > **LEPS** > **Profiles**	Specify whether and how MAC addresses are to be checked.
VLAN	**Setup** > **WLAN** > **LEPS** > **Profiles**	Defines the VLAN to which a LEPS user is assigned with this profile.
Users	**Setup** > **WLAN** > **LEPS**	Create LEPS users. Each user must be linked to a profile.
Name	**Setup** > **WLAN** > **LEPS** > **Users**	Assign a unique name to the LEPS user.
Profile	**Setup** > **WLAN** > **LEPS** > **Users**	Select the profile for which the LEPS user is to be valid. Only LEPS users who are linked via the LEPS profile can log on to the SSID.
WPA-Passphrase	**Setup** > **WLAN** > **LEPS** > **Users**	Set the passphrase for this LEPS user's WLAN login.
VLAN	**Setup** > **WLAN** > **LEPS** > **Users**	Specify the VLAN to which the LEPS user is assigned. If no VLAN is configured here, any VLAN configured in the LEPS profile applies. If a VLAN is configured both in the LEPS profile and for the LEPS user, the VLAN ID configured for the LEPS user applies.
MAC-Address	**Setup** > **WLAN** > **LEPS** > **Users**	Optional MAC address for a MAC filter. Depending on the setting in the profile, this entry is ignored, or only the client devices listed in

Parameter	Pfad	Description
		this table can log in (whitelist). With a blacklist, the MAC filter works the other way around—specified MAC addresses cannot log in.

Recommendations

- **Setup** > **WLAN** > **LEPS** > **Operating**: **Yes** (enable LEPS so users can use individual passphrases)
- **Setup** > **WLAN** > **LEPS** > **Users** > **Profile**: "OfficeLEPS" (link to the previously created profile)
- **Setup** > **WLAN** > **LEPS** > **Users** > **WPA-Passphrase**: Use a strong, individual passphrase
- **Setup** > **WLAN** > **LEPS** > **Users** > **MAC-Address**: Optional (only required for whitelist/blacklist)

5 RADIUS

Configuration settings for the parameters of RADIUS and IEEE 802.1X.

Console path

Setup > **RADIUS**

5.1 RADIUS-Server

Configure the settings for RADIUS server profiles to be used with WLAN networks that use 802.1X as the authentication method.

Console path

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

Parameter	Path	Description
Name	**Setup** > **RADIUS** > **RADIUS-Server**	Select a descriptive name for the RADIUS server profile. This internal name is used to reference the RADIUS server profile in other parts of the configuration.
Port	**Setup** > **RADIUS** > **RADIUS-Server**	Select the UDP port used to contact the RADIUS server.
Secret	**Setup** > **RADIUS** > **RADIUS-Server**	Configure the shared secret used to encrypt communication between the device and the RADIUS server. This secret must also be configured on the RADIUS server.
Backup	**Setup** > **RADIUS** > **RADIUS-Server**	Configure a backup profile that is used if the primary RADIUS server is not reachable.
Server-IP-Address	**Setup** > **RADIUS** > **RADIUS-Server**	Configure the hostname or IP address of the RADIUS server.
Accounting-Port	**Setup** > **RADIUS** > **RADIUS-Server**	Select the UDP port used to reach the RADIUS accounting server.
Accounting-IP-Address	**Setup** > **RADIUS** > **RADIUS-Server**	Configure the hostname or IP address of the RADIUS accounting server.

Recommendations

- **Setup** > **RADIUS** > **RADIUS-Server** > **Server-IP-Address**: IP address of the RADIUS server
- **Setup** > **RADIUS** > **RADIUS-Server** > **Port**: **1812** (standard port for RADIUS authentication)
- **Setup** > **RADIUS** > **RADIUS-Server** > **Secret**: Use a strong shared secret
- **Setup** > **RADIUS** > **RADIUS-Server** > **Backup**: Optional for redundancy
- **Setup** > **RADIUS** > **RADIUS-Server** > **Accounting-IP-Address**: IP address of the RADIUS accounting server for usage logging.
- **Setup** > **RADIUS** > **RADIUS-Server** > **Accounting-Port**: **1813** (standard port for accounting)

5.2 MAC check

Instead of authenticating a username via the RADIUS server, authentication can also be performed using a MAC address.

Console path

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

Parameter	Path	Description
Fallback-Dynamic-VLAN-ID	**Setup** > **RADIUS** > **RADIUS-Server**	If a RADIUS server does not transmit a VLAN ID for a WLAN client, the value configured here is used.
Require-Message-Authenticator	**Setup** > **RADIUS** > **RADIUS-Server**	Specifies whether a Message-Authenticator is mandatory in RADIUS messages. Messages without a Message-Authenticator are discarded.

Recommendations

- **Setup** > **RADIUS** > **RADIUS-Server** > **Require-Message-Authenticator**: **Yes** (Higher security, as only valid RADIUS messages are accepted.)

5.3 LAN-Supplicant

Here you can find the settings for the 802.1X supplicant functionality to authenticate the device on the LAN side against a switch infrastructure secured with 802.1X.

Console path

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

Parameter	Path	Description
Interface-Name	**Setup** > **RADIUS** > **LAN-Supplicant**	The name of the LAN interface. Currently, only the INTRANET interface exists.
Method	**Setup** > **RADIUS** > **LAN-Supplicant**	The EAP method to be used for authentication against the 802.1X infrastructure.
Username	**Setup** > **RADIUS** > **LAN-Supplicant**	The username to be used for authentication against the 802.1X infrastructure.
Password	**Setup** > **RADIUS** > **LAN-Supplicant**	The password to be used for authentication against the 802.1X infrastructure.

Recommendations

- **Setup** > **RADIUS** > **LAN-Supplicant** > **Method**: **PEAP/MSCHAPv2** (most secure authentication method for your LAN supplicant)
- **Setup** > **RADIUS** > **LAN-Supplicant** > **Username**: Unique 802.1X username for authentication at the switch.
- **Setup** > **RADIUS** > **LAN-Supplicant** > **Password**: Use a strong password or certificate for authentication at the switch.

5.4 WLAN-Supplicant

Here you can find the settings for the 802.1X supplicant functionality to authenticate the device on the WLAN side against an infrastructure secured with 802.1X.

Console path

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

Parameter	Path	Description
Profile-Name	**Setup** > **RADIUS** > **WLAN-Supplicant**	Use a unique profile name that you will later specify in the encryption profile.
Method	**Setup** > **RADIUS** > **WLAN-Supplicant**	Select a suitable authentication method. When using TLS, a certificate must be uploaded.
Username	**Setup** > **RADIUS** > **WLAN-Supplicant**	RADIUS username. No entry is required when using TLS.
Password	**Setup** > **RADIUS** > **WLAN-Supplicant**	RADIUS password. No entry is required when using TLS.
Certificate	**Setup** > **RADIUS** > **WLAN-Supplicant**	Automatically accept or verify the uploaded certificate. Recommendation: Upload a certificate to ensure the integrity of the RADIUS server.
Delete-WLAN-Supplicant-Certificates	**Setup** > **RADIUS** > **WLAN-Supplicant**	Deletes all existing WLAN supplicant certificates.

Recommendations

- **Setup** > **RADIUS** > **WLAN-Supplicant** > **Method**: **PEAP/MSCHAPv2** (most secure authentication method for the WLAN supplicant)
- **Setup** > **RADIUS** > **WLAN-Supplicant** > **Certificate**: **Container** (verify the certificate to ensure server integrity)

6 WLAN-Management

LCOS LX-based access points can be managed by a LANCOM WLAN Controller (WLC). As with LCOS-based access points, the CAPWAP protocol is used for this purpose.

Console path

Setup > **WLAN-Management**

6.1 Static-WLC-Configuration

Configures user-defined WLAN controllers. This is required if a WLC is not discovered automatically and the DNS name "WLC-Address" cannot be used.

Console path

Setup > **WLAN-Management**

Parameter	Path	Description
IP-Address	**Setup** > **WLAN-Management** > **Static-WLC-Configuration**	Specify the IP address or DNS name of a WLAN controller.
Port	**Setup** > **WLAN-Management** > **Static-WLC-Configuration**	Configures the port on which attempts are made to reach a WLC.
Operating	**Setup** > **WLAN-Management**	Configures whether an access point actively searches for a WLC and can be managed by it.
Update-Cert-Before	**Setup** > **WLAN-Management**	Specifies how many days before expiration the device certificate used for authentication with the WLC is renewed.
Capwap-Port	**Setup** > **WLAN-Management**	Configures the port on which attempts are made to reach a WLC. The default value of 1027 is the standard port of the CAPWAP protocol. LANCOM WLCs also use this port by default.

Recommendation

- **Setup** > **WLAN-Management** > **Static-WLC-Configuration** > **IP-Address**: <IP address or DNS name of the WLC> (so that the access point can reliably find the controller even in routed networks)
- **Setup** > **WLAN-Management** > **Static-WLC-Configuration** > **Port**: **1027** (standard CAPWAP port, matching the LANCOM WLC).
- **Setup** > **WLAN-Management** > **Operating**: **Yes** (allows the access point to actively search for and be managed by the WLC).
- **Setup** > **WLAN-Management** > **Update-Cert-Before**: **30** (days before expiration. Ensures that certificates are renewed in time)
- **Setup** > **WLAN-Management** > **Capwap-Port**: **5246** (standard port for CAPWAP communication, ensures a stable connection to the WLC)

7 L2TP

LCOS LX supports Layer 2 Tunneling Protocol (L2TP) version 3. With L2TPv3, Ethernet traffic (Layer 2) is tunneled and transmitted over UDP. This allows LANs to be interconnected across network and site boundaries. In particular, WLAN traffic on the access point side can be encapsulated into an L2TPv3 Ethernet tunnel and decapsulated again at a central concentrator. Without L2TPv3, this always required a WLAN controller that implemented this using CAPWAP Layer 3 tunnels. With L2TPv3, this is now possible independently of WLAN controllers, allowing WLAN traffic to be transmitted in tunnels and centrally terminated.

Console path

Setup > **L2TP**

7.1 Endpoints

This table is used to configure the basic settings for an L2TP tunnel.

Console path

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

Parameter	Path	Description
Tunnel-Id	**Setup** > **L2TP** > **Endpoints**	Identifier of the tunnel endpoint. For authenticated tunnels, the Tunnel-Id and hostname must match crosswise.
IP-Address	**Setup** > **L2TP** > **Endpoints**	IP address or FQDN of the tunnel endpoint.
Port	**Setup** > **L2TP** > **Endpoints**	UDP port to be used for L2TP.
Hostname	**Setup** > **L2TP** > **Endpoints**	Username for authentication. For authenticated tunnels, it must match the Tunnel-Id crosswise.
Password	**Setup** > **L2TP** > **Endpoints**	Password for authentication; optional for obfuscating the tunnel negotiation.
Auth-Peer	**Setup** > **L2TP** > **Endpoints**	Specifies whether the peer is to be authenticated.
Hide	**Setup** > **L2TP** > **Endpoints**	Specifies whether the tunnel negotiation is to be obfuscated using the password.
Operating	**Setup** > **L2TP** > **Endpoints**	Enables or disables the L2TP endpoint.

Recommendation

- **Setup** > **L2TP** > **Endpoints** > **IP-Address**: IP address or FQDN of the tunnel endpoint
- **Setup** > **L2TP** > **Endpoints** > **Port**: **1701** (standard UDP port for L2TP)
- **Setup** > **L2TP** > **Endpoints** > **Hostname**: Username for authentication. Must match the Tunnel-Id crosswise.
- **Setup** > **L2TP** > **Endpoints** > **Password**: Password for authentication / optional for obfuscation
- **Setup** > **L2TP** > **Endpoints** > **Auth-Peer**: **Yes** (the peer must be authenticated)
- **Setup** > **L2TP** > **Endpoints** > **Hide**: **Yes** (obfuscate tunnel negotiation)
- **Setup** > **L2TP** > **Endpoints** > **Operating**: **Yes** (enable the endpoint)

7.2 Ethernet

This table is used to link L2TPv3 endpoints with a WLAN network.

Console path

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

Parameter	Path	Description
L2TP-Endpoint	**Setup** > **L2TP** > **Ethernet**	Configure here the name of the L2TP endpoint configured in the L2TP endpoints table (2.61.1.1 Tunnel-Id). An Ethernet tunnel session is then established via this endpoint. If connections are only to be accepted but not initiated locally, leaving this field empty allows arbitrary sessions to be accepted. These sessions must still “pass” through an accepted / established endpoint from the L2TP endpoints table. This can be useful in scenarios where not every endpoint on the receiving side is to be configured individually.
Remote-End	**Setup** > **L2TP** > **Ethernet**	Name used to associate the Ethernet tunnel on the remote side. This name must be identical on both sides.
Interface-Name	**Setup** > **L2TP** > **Ethernet**	The virtual Ethernet interface to be used for the L2TPv3 session.
MTU	**Setup** > **L2TP** > **Ethernet**	Adjusts the MTU of the Ethernet tunnel, e. g. for networks with smaller MTU values.

Recommendation

- **Setup** > **L2TP** > **Ethernet** > **L2TP-Endpoint**: <Tunnel-Id from the Endpoints table>
- **Setup** > **L2TP** > **Ethernet** > **Remote-End**: <Name of the remote endpoint> (must be identical on both sides)
- **Setup** > **L2TP** > **Ethernet** > **MTU**: **1500** (or adjusted for reduced network MTU)

8 IP-Configuration

This menu is used to configure parameters for the IP configuration of the device.

Console path

Setup > **IP-Configuration**

Parameter	Path	Description
Static-Parameters	**Setup** > **IP-Configuration**	Settings related to IP and network configuration when using static IP addresses.
Interface-Name	**Setup** > **IP-Configuration** > **Static-Parameters**	Name of the interface to which the subsequent settings apply.
IPv4-Gateway	**Setup** > **IP-Configuration** > **Static-Parameters**	Configuration of the IPv4 gateway for the referenced interface.
IPv6-Gateway	**Setup** > **IP-Configuration** > **Static-Parameters**	Configuration of the IPv6 gateway for the referenced interface.
Primary-IPv4-DNS	**Setup** > **IP-Configuration** > **Static-Parameters**	Primary IPv4 DNS server for the referenced interface.
Secondary-IPv4-DNS	**Setup** > **IP-Configuration** > **Static-Parameters**	Secondary IPv4 DNS server for redundancy.
Primary-IPv6-DNS	**Setup** > **IP-Configuration** > **Static-Parameters**	Primary IPv6 DNS server for the referenced interface.
Secondary-IPv6-DNS	**Setup** > **IP-Configuration** > **Static-Parameters**	Secondary IPv6 DNS server for redundancy.

Recommendations

- **Setup** > **IP-Configuration** > **Static-Parameters** > **IPv4-Gateway**: <internal, trusted IPv4 address of the gateway>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **IPv6-Gateway**: <internal, trusted IPv6 address of the gateway>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **Primary-IPv4-DNS**: <internal IPv4 address of the DNS server>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **Secondary-IPv4-DNS**: <internal IPv4 address of the secondary DNS server>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **Primary-IPv6-DNS**: <internal IPv6 address of the DNS server>
- **Setup** > **IP-Configuration** > **Static-Parameters** > **Secondary-IPv6-DNS**: <internal IPv6 address of the secondary DNS server>

8.1 LAN-Interfaces

Define basic configuration options related to the device's own IP settings and network access here.

Console path

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

Parameter	Path	Description
Interface-Name	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Assign a descriptive name to the interface here. This name is referenced in other parts of the configuration.
VLAN-ID	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Define the VLAN ID for which the interface is to be active.
IPv4-Address-Source	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Select the source of the IPv4 address for the interface.
IPv6-Address-Source	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Select the source of the IPv6 address for the interface.
Static-IPv4-Address	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Configure the IP address to be used when “static” is selected as the IPv4 address source. Append the subnet mask in CIDR notation (e.g. “/24”).
Static-IPv6-Address	**Setup** > **IP-Configuration** > **LAN-Interfaces**	Configure the IP address to be used when “static” is selected as the IPv6 address source. Append the subnet mask in CIDR notation (e.g. “/64”).

Recommendations

- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **VLAN-ID**: Separate management or client VLAN (e.g. 10 for management, 20 for WLAN)
- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **IPv4-Address-Source**: **static** (if a fixed IP address is required, otherwise DHCP)
- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **IPv6-Address-Source**: **static** (or Router Advertisement if the network distributes IPv6 dynamically)
- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **Static-IPv4-Address**: <e.g. 192.168.10.5/24>
- **Setup** > **IP-Configuration** > **LAN-Interfaces** > **Static-IPv6-Address**: <e.g. fd00:10::5/64>

8.2 LMC

Settings for configuring and monitoring your device via the LANCOM Management Cloud (LMC).

Console path

Setup > **LMC**

Parameter	Path	Description
Operating	**Setup** > **LMC**	Specify whether the device is to be managed via the LMC.
Proxy	**Setup** > **LMC**	If the device is to connect to the LMC via an HTTP proxy server, it can be configured here. As soon as a proxy URL is entered, the LMC connection is always established via the proxy server. If the switch (2.102.2.4 Tunnel) is also enabled, a transparent tunnel via the proxy server using the HTTP CONNECT method is used. The proxy server must support this. If the switch is not enabled, individual HTTP requests are forwarded via the proxy.
URL	**Setup** > **LMC** > **Proxy**	If the device is to connect to the LMC via an HTTP proxy server, it can be configured here. As soon as a proxy URL is entered, the LMC connection is always established via the proxy server.

Parameter	Path	Description
Username	**Setup** > **LMC** > **Proxy**	Username for authentication with the proxy server.
Password	**Setup** > **LMC** > **Proxy**	Password for authentication with the proxy server.
Tunnel	**Setup** > **LMC** > **Proxy**	If a proxy URL is specified and this switch is enabled, a transparent tunnel via the proxy server using the HTTP CONNECT method is used. The proxy server must support this. If the switch is not enabled, individual HTTP requests are forwarded via the proxy.
Delete-Certificate	**Setup** > **LMC**	Deletes the existing LMC certificate.

Recommendations

- **Setup** > **LMC** > **Operating**: **No** (enable only if management via LMC is required)
- **Setup** > **LMC** > **Proxy** > **URL**: <Enter proxy URL only if required>
- **Setup** > **LMC** > **Proxy** > **Username**: Username for the proxy, if required
- **Setup** > **LMC** > **Proxy** > **Password**: Strong password if a proxy is used
- **Setup** > **LMC** > **Proxy** > **Tunnel**: **Yes** (use HTTP CONNECT tunnel if supported by the proxy)
- **Setup** > **LMC** > **Delete-Certificate**: Use only when changing or cleaning up certificates.

9 Automatic-Firmware-Update

The LANCOM Auto Updater enables the automatic update of deployed LANCOM devices without any further user interaction (unattended). If desired, LANCOM devices can check for new software updates without user interaction, download them, and install them. You can choose whether security updates, release updates, or all updates are installed automatically.

If no automatic updates are to be performed, the feature can also be used solely to check for new updates. For update checks and firmware downloads, the LANCOM Auto Updater contacts the LANCOM update server. The connection is established via HTTPS.

When establishing the connection, the server is validated using the TLS certificates already stored on the LANCOM device. In addition, firmware files for current LANCOM devices are signed. Before installing firmware, the LANCOM Auto Updater validates this signature.

Console path

Setup > **Automatic-Firmware-Update**

Parameter	Path	Description
Mode	**Setup** > **Automatic-Firmware-Update**	Defines the operating mode of the Auto Updater.
Check-Firmware-Now	**Setup** > **Automatic-Firmware-Update**	Immediately starts a check for new firmware versions.
Update-Firmware-Now	**Setup** > **Automatic-Firmware-Update**	Downloads and installs the latest firmware.
Cancel-Current-Action	**Setup** > **Automatic-Firmware-Update**	Cancels the currently running Auto Updater action. This applies to both manually started and scheduled actions.
Reset-Updater-Config	**Setup** > **Automatic-Firmware-Update**	This command resets the boot-persistent configuration files related to the Auto Updater. This includes the local blacklist containing firmware versions for which an automatic update failed.
Base-URL	**Setup** > **Automatic-Firmware-Update**	URL of the firmware update server.
Check-Interval	**Setup** > **Automatic-Firmware-Update**	Specifies the interval at which updates are checked. The updater automatically selects a random time within the interval.
Version-Policy	**Setup** > **Automatic-Firmware-Update**	Controls which firmware versions are offered to the device.

Recommendations

- **Setup** > **Automatic-Firmware-Update** > **Mode**: **Check** (always check the current firmware version)
- **Setup** > **Automatic-Firmware-Update** > **Cancel-Current-Action**: Cancel running actions if required
- **Setup** > **Automatic-Firmware-Update** > **Check-Interval**: **Daily** (shortest interval)
- **Setup** > **Automatic-Firmware-Update** > **Version-Policy**: **security-updates-only** (security-relevant updates only)
- **Setup** > **Automatic-Firmware-Update** > **Reset-Updater-Config**: Use only in case of errors or incorrect configuration.