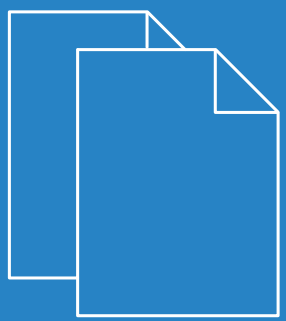
SECURE. NETWORKS.

LCOS LX 5.20

Menu Reference



05/2020

LANCOM Systems

Contents

Copyright

While the information in this manual has been compiled with great care, it may not be deemed an assurance of product characteristics. LANCOM Systems shall be liable only to the degree specified in the terms of sale and delivery.

The reproduction and distribution of the documentation and software supplied with this product and the use of its contents is subject to written authorization from LANCOM Systems. We reserve the right to make any alterations that arise as the result of technical development.

Windows® and Microsoft® are registered trademarks of Microsoft, Corp.

LANCOM, LANCOM Systems, LANcommunity and Hyper Integration are registered trademarks. All other names or descriptions used may be trademarks or registered trademarks of their owners. This document contains statements relating to future products and their attributes. LANCOM Systems reserves the right to change these without notice. No liability for technical errors and/or omissions.

This product contains separate open-source software components. These are subject to their own licenses, in particular the General Public License (GPL). License information relating to the device firmware (LCOS LX) is available on the CLI by using the command `show 3rd-party-licenses`. If the respective license demands, the source files for the corresponding software components will be made available on request. Please contact us via e-mail under *gpl@lancom.de*.

Products from LANCOM Systems include software developed by the "OpenSSL Project" for use in the "OpenSSL Toolkit" (*www.openssl.org*).

Products from include cryptographic software written by Eric Young (*eay@cryptsoft.com*).

Products from LANCOM Systems include software developed by the NetBSD Foundation, Inc. and its contributors.

Products from LANCOM Systems contain the LZMA SDK developed by Igor Pavlov.

LANCOM Systems GmbH

Adenauerstr. 20/B2

52146 Würselen, Germany

Germany

www.lancom-systems.com

1 1 Introduction

1.1 1.1 Components of the documentation

The documentation of your device consists of the following parts:

Installation Guide

The Quickstart user guide answers the following questions:

- Which software has to be installed to carry out a configuration?
- How is the device connected up?
- How can the device be contacted with LANconfig or WEBconfig?
- How is the device assigned to the LANCOM Management Cloud?
- How do I start the Setup Wizard (e.g. to set up Internet access)?
- How do I reset the device?
- Where can I find information and support?

Quick Reference Guide

The Quick Reference Guide contains all the information you need to put your device into operation. It also contains all of the important technical specifications.

Reference manual

The Reference Manual goes into detail on topics that apply to a variety of models. The descriptions in the Reference Manual are based predominantly to the configuration with LANconfig.

Menu Reference Guide

The Menu Reference Guide comprehensively describes all of the parameters in LCOS LX. This guide is an aid to users during the configuration of devices by means of the CLI. Each parameter is described briefly and the possible values for input are listed, as are the default values.

All documents for your product which are not shipped in printed form are available as a PDF file from *www.lancom-systems.com/downloads*.

1.2 1.2 LCOS LX, an operating system from LANCOM

LCOS LX is the operating system for certain LANCOM access points and parts of the LANCOM family of operating systems. The LANCOM operating systems are the trusted basis for the entire LANCOM product portfolio. Each operating system embodies the LANCOM values of security, reliability and future viability.

- **Maximum security for your networks**

  as each LANCOM operating system is carefully maintained and developed in-house and with the accustomed quality. They are all guaranteed backdoor-free.

- **Reliability of the highest order**

  as they receive regular release updates, security updates, and major releases over their entire product lifetime.

- **Future viability for your networks**

according to the LANCOM Lifecycle Policy, i.e. they are free of charge for all LANCOM products and come with major new features.

1.3 1.3 Validity

The functions and settings described in this manual are not all supported by all models or all firmware versions.

1.4 1.4 Command-line interface — access

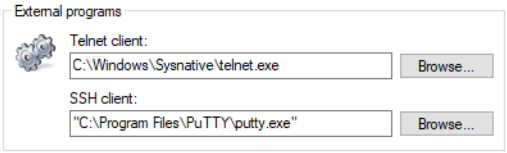
Access to the LCOS LX command-line interface (CLI) is via SSH. Use an SSH client such as PuTTY to connect to the IP address of the device.

Access credentials for a device in its delivery state are:

Username: root

Password: <Empty> (no password is set)

In LANconfig you configure your preferred SSH client under **Tools** > **Options** > **Extras** > **SSH client**:



To open an SSH session, use the context menu of the device and go to **WEBconfig / Console session** > **Open SSH session**.

1.5 1.5 Command-line interface – menu structure

The LCOS LX command-line interface is structured as follows:

Status

Contains the status and statistics of all internal modules in the device. These are not described here as we recommend that you use the GUI available in WEBconfig. Alternatively, you can download the Management Information Base (MIB) for your device, which contains the entries and a short description for use with SNMPv3. You can download the device MIB from *www.lancom-systems.com/downloads/*.

Setup

Contains all adjustable parameters of all internal modules in the device. See *Setup*.

Other

Contains actions such as resetting or rebooting. See *Other*.

1.6 1.6 Command-line interface – command summary

The command-line interface is operated with the following commands.

Which commands are available depends upon the equipment of the device.

Changes to the configuration are not immediately boot-persistent. They have to be saved explicitly by using the command `flash`.

Table 1: Overview of all commands available at the command line

Command	Description
`add [<Path>]`	Adds a row to the table.
`cd <Path>`	Changes the current menu or directory.
`default`	Resets the table or the value to the default setting. This command works recursively. Therefore, all values and tables in the current path and those below it will be reset.
`del <Path>`	Deletes the value or the table row in the branch of the menu tree referenced by `<Path>`.
`do <Path> [<Parameter>]`	Executes the action in the current or referenced directory. If the action has additional parameters, they can be added at the end.
`exit`	Ends the terminal session.
`flash`	Store the configuration Changes to the configuration are not immediately boot-persistent. They have to be saved explicitly by using the command `flash`.
`ls [<Path>]`	Displays the contents of the current directory or path.
`passwd <Password>`	Changes the password of the current user account.
`set <Index> {Column} <Value>`	Sets the value of a table row in a specific column to <Value>.
`set <Path> <Value(s)>`	Sets the value or values of a specific path to the specified value(s).
`show diag [<Parameter>]`	Output diagnostic information on the CLI.
`show 3rd-party-licenses`	Output the device license information on the CLI.
`startlmc <Activation Code> [Domain]`	After you have generated an activation code in the LANCOM Management Cloud, you use this code to pair the device with the LANCOM Management Cloud. You can optionally specify a new LMC domain as well.
`sysinfo`	Shows the system information (e.g., hardware release, software version, MAC address, serial number, etc.).
`trace [--log] [+|-|#|?] <Parameter>`	Starts (+) or stops (–) a trace command to output diagnosis data. # switches between different trace outputs and `?` displays a help text. The parameter `--log` restricts the output to "historical" log information.

Legend

- Characters and brackets:
  - Objects, in this case dynamic or situation-dependent, are in angle brackets.

- Round brackets group command components, for a better overview.
- Vertical lines (pipes) separate alternative inputs.
- Square brackets describe optional switches.

It follows that all command components that are not in square brackets are necessary information.

- `<Path>`:
  - Describes the path name for a menu or parameter, separated by "/".
  - `..` means: one level higher
  - `.` means: the current level
- `<Value>`:
  - Describes a possible input value.
  - `""` is a blank input value
- `<Name>`:
  - Describes a character sequence of [0…9] [A…Z] [a…z] [_].
  - The first character cannot be a digit.
  - There is no difference between small letters and capital letters.
- `<Filter>`:
  - The output of some commands can be restricted by entering a filter expression. Filtering does not occur line by line, but in blocks, depending on the command.
  - A filter expression starts with the "@" symbol by itself and ends either at the end of the line or at a ";" (semicolon) to end the current command.
  - A filter expression also consists of one or more search patterns, which are separated by blank spaces and preceded either by no operator (OR pattern), a "+" operator (AND pattern) or a "-" operator (NOT pattern).
  - For the execution of the command, an information block is output exactly when at least one of the "OR" patterns, all "AND" patterns or none of the "NOT" patterns matches. Capitalization is ignored.
  - For a search pattern to contain characters for structuring in the filter syntax (e.g., blank characters), then the entire search pattern can be enclosed in "". Alternatively, the symbol "\" can be placed before the special characters. If you want to search for a quotation mark (") or "\", another "\" symbol has to be placed in front of it.

    Entering the start of the word, if it is unique, is sufficient.

Explanations for addressing, syntax and command input

- All commands and directory/parameter names can be entered using their short-forms as long as they are unambiguous. For example, the command `cd setup` can be shortened to `cd se`. The input `cd /s` is not valid, however, since it corresponds to both `cd /Setup` and `cd /Status`.
- The values in a table row can alternatively be addressed via the column name or the position number in curly brackets. The command `set ?` in the table shows the name, the possible input values and the position number for each column.
- Multiple values in a table row can be changed with **one** command, for example in the WLAN networks (`/Setup/WLAN/Network`):
  - `add Guest Guest 1234567890` creates a new network named Guest, SSID Guest, and key 1234567890.

    The order of the values must correspond to their order in the table. Values that should not be changed can be specified with a *.
  - `set Guest * 0987654321` changes the value Key in the network Guest. Using the * leaves the SSID unchanged.

- `set Guest {Key} 1234567890` sets the value Key in the network Guest. Individual columns can be referenced by the column name in parentheses.

- Names that contain spaces must be enclosed within quotation marks ("").

Command-specific help

- A command-specific help function is available for actions and commands (call the function with a question mark as the argument). For example, `show ?` displays the options available with the show command.

2 Setup

This menu allows you to adjust the settings for this device.

SNMP ID:

2

Console path:

/

2.1 Name

Configure the device name here. For display purposes only.

SNMP ID:

2.1

Console path:

Setup

Possible values:

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

Default:

empty

2.2 SNMP

This menu contains the configuration of SNMP.

The OIDs can be found in the device MIB, which you can download from *www.lancom-systems.com/downloads/*.

SNMP ID:

2.9

Console path:

Setup

2.2.1 Send-Traps

When serious errors occur, for example when an unauthorized attempt is made to access the device, it can send an error message to one or more SNMP managers automatically. Activate the option and, in the Target addresses table, add the targets where these SNMP managers are installed.

SNMP ID:

2.9.1

Console path:

Setup > SNMP

Possible values:

Yes
No

Default:

No

2.2.2 Port

Using this parameter, you specify the port which external programs such as LANmonitor use to access the SNMP service.

SNMP ID:

2.9.21

Console path:

Setup > SNMP

Possible values:

0 … 65535

Default:

161

2.2.3 Communities

SNMP agents and SNMP managers belong to SNMP communities. These communities collect certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

This table is used to configure the SNMP communities.

The SNMP community `public` is set up by default, and this provides unrestricted SNMP read access.

SNMP ID:

2.9.27

Console path:

Setup > **SNMP**

Name

Enter a descriptive name for this SNMP community.

SNMP ID:

2.9.27.1

Console path:

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

Possible values:

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

Default:

empty

Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

SNMP ID:

2.9.27.3

Console path:

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

Possible values:

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

Default:

empty

Status

This entry is used to enable or disable this SNMP community.

SNMP ID:

2.9.27.8

Console path:

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

Possible values:

Active

The community is enabled.

inactive

The community is disabled.

Default:

Active

2.2.4 Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users.

SNMP ID:

2.9.28

Console path:

Setup > **SNMP**

Security-Model

SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in LCOS LX primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly.

You select a security model here as is appropriate.

SNMP ID:

2.9.28.1

Console path:

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

Possible values:

Any

Any model is accepted.

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

SNMPv2_C

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “NoAuthNoPriv”.

SNMPv3_USM

Data is transmitted by SNMPv3. Users can authenticate and communicate according to the following security levels:

NoAuthNoPriv

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

AuthNoPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is not encrypted.

AuthPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is encrypted by DES or AES algorithms.

Default:

SNMPv3_USM

Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

SNMP ID:

2.9.28.2

Console path:

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

Possible values:

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

Default:

empty

Group-Name

Enter a descriptive name for this group. You will use this name when you go on to configure the access rights.

SNMP ID:

2.9.28.3

Console path:

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

Possible values:

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

Default:

empty

Status

Activates or deactivates this group configuration.

SNMP ID:

2.9.28.5

Console path:

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

Possible values:

Active
inactive

Default:

Active

2.2.5 Accesses

This table brings together the different configurations for access rights, security models, and views.

SNMP ID:

2.9.29

Console path:

Setup > **SNMP**

Group-Name

Here you select the name of a group that is to receive these assess rights.

SNMP ID:

2.9.29.1

Console path:

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

Possible values:

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

Default:

empty

Security-Model

Activate the appropriate security model here.

SNMP ID:

2.9.29.3

Console path:

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

Possible values:

Any
Any model is accepted.

SNMPv1
SNMPv1 is used.

SNMPv2_C
SNMPv2c is used.

SNMPv3_USM
SNMPv3 is used.

Default:

Any

Read-View-Name

Set the view of the MIB entries for which this group is to receive read rights.

SNMP ID:

2.9.29.5

Console path:

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

Possible values:

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

Default:

empty

Write-View-Name

Set the view of the MIB entries for which this group is to receive write rights.

SNMP ID:

2.9.29.6

Console path:

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

Possible values:

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

Default:

empty

Notify-View-Name

Set the view of the MIB entries for which this group is to receive notify rights.

SNMP ID:

2.9.29.7

Console path:

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

Possible values:

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

Default:

empty

Status

Activates or deactivates this entry.

SNMP ID:

2.9.29.8

Console path:

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

Possible values:

Active
inactive

Default:

Active

Min-Security-Level

Specify the minimum security level for access and data transfer.

SNMP ID:

2.9.29.10

Console path:

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

Possible values:

NoAuthNoPriv

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

AuthNoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

AuthPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Default:

AuthPriv

2.2.6 Views

This table is used to collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with their corresponding access rights.

SNMP ID:

2.9.30

Console path:

Setup > **SNMP**

View-Name

Give the view a descriptive name here.

SNMP ID:

2.9.30.1

Console path:

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

Possible values:

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

Default:

empty

OID-Subtree

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in this view.

The OIDs can be found in the device MIB, which you can download from *www.lancom-systems.com/downloads/*.

SNMP ID:

2.9.30.3

Console path:

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

Possible values:

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

Default:

empty

Type

Here you decide whether the OID subtrees specified in the following are “Included” or “Excluded” from the view.

SNMP ID:

2.9.30.4

Console path:

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

Possible values:

Included

This setting outputs MIB values.

Excluded

This setting blocks the output of MIB values.

Default:

Included

Status

Activates or deactivates this view.

SNMP ID:

2.9.30.6

Console path:

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

Possible values:

Active
inactive

Default:

Active

2.2.7 Users

This menu contains the user configuration.

SNMP ID:

2.9.32

Console path:

Setup > **SNMP**

Username

Specify the SNMPv3 user name here.

SNMP ID:

2.9.32.2

Console path:

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

Possible values:

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

Default:

empty

Authentication-Protocol

Specify the method that the user is required to use to authenticate at the SNMP agent.

SNMP ID:

2.9.32.5

Console path:

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

Possible values:

None

Authentication of the user is not necessary.

HMAC-MD5

Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA

Authentication is performed using the hash algorithm HMAC-SHA-96 (hash length 160 bits).

HMAC-SHA224

Authentication is performed using the hash algorithm HMAC-SHA-224 (hash length 224 bits).

HMAC-SHA256

Authentication is performed using the hash algorithm HMAC-SHA-256 (hash length 256 bits).

HMAC-SHA384

Authentication is performed using the hash algorithm HMAC-SHA-384 (hash length 384 bits).

HMAC-SHA512

Authentication is performed using the hash algorithm HMAC-SHA-512 (hash length 512 bits).

Authentication-Password

Enter the user password necessary for authentication here.

Cleartext input is only possible if the parameter in *2.9.32.14 Authentication-Password-Type* on page 24 was changed.

SNMP ID:

2.9.32.6

Console path:

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

Possible values:

Max. 130 characters from `anything printable`

Default:

empty

Privacy-Protocol

Specify which encryption method is used for encrypted communication with the user.

SNMP ID:

2.9.32.8

Console path:

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

Possible values:

None

Communication is not encrypted.

DES

Encryption is performed with DES (key length 56 bits).

AES128

Encryption is performed with AES128 (key length 128 bits).

AES192

Encryption is performed with AES192 (key length 192 bits).

AES256

Encryption is performed with AES256 (key length 256 bits)

Privacy-Password

Enter the user password necessary for encryption here.

Cleartext input is only possible if the parameter in *2.9.32.15 Privacy-Password-Type* on page 25 was changed.

SNMP ID:

2.9.32.9

Console path:

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

Possible values:

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

Default:

empty

Status

Activates or deactivates this user.

SNMP ID:

2.9.32.13

Console path:

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

Possible values:

Active
inactive

Default:

Active

Authentication-Password-Type

The password in *2.9.32.6 Authentication-Password* on page 22 is always stored in encrypted format (type “Masterkey”). If you wish to enter a new password, for example from the command-line interface, you must first change the type to “Plaintext” here. You are then able to enter a password in plain text. LCOS LX will then encrypt the password and reset this value to “Masterkey”.

SNMP ID:

2.9.32.14

Console path:

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

Possible values:

Plaintext
Masterkey

Privacy-Password-Type

The password in *2.9.32.9 Privacy-Password* on page 23 is always stored in encrypted format (type "Masterkey"). If you wish to enter a new password, for example from the command-line interface, you must first change the type to "Plaintext" here. You are then able to enter a password in plain text. LCOS LX will then encrypt the password and reset this value to "Masterkey".

SNMP ID:

2.9.32.15

Console path:

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

Possible values:

Plaintext
Masterkey

2.2.8 Target-Addresses

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.

SNMP ID:

2.9.34

Console path:

Setup > **SNMP**

Name

Specify the target address name here.

SNMP ID:

2.9.34.1

Console path:

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

Possible values:

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

Default:

empty

Transport-Address

The transport address describes the IP address and port number of a recipient of an SNMP trap and is specified in the syntax <IP address> : <Port> (e.g. 128.1.2.3:162). UDP port 162 is used for SNMP traps.

SNMP ID:

2.9.34.3

Console path:

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

Possible values:

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

Default:

empty

Parameters-Name

Here you select the desired entry from the list of recipient parameters.

SNMP ID:

2.9.34.7

Console path:

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

Possible values:

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

Default:

empty

Status

Activates or deactivates this target address.

SNMP ID:

2.9.34.9

Console path:

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

Possible values:

Active
inactive

Default:

Active

2.2.9 Target-Params

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.

SNMP ID:

2.9.35

Console path:

Setup > **SNMP**

Name

Give the entry a descriptive name here.

SNMP ID:

2.9.35.1

Console path:

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

Possible values:

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

Default:

empty

Message-Processing-Model

Here you specify the protocol for which the SNMP agent structures the message.

SNMP ID:

2.9.35.2

Console path:

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

Possible values:

SNMPv1
SNMPv2c
SNMPv3

Default:

SNMPv3

Security-Model

Use this entry to specify the security model.

SNMP ID:

2.9.35.3

Console path:

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

Possible values:

Any
SNMPv1
SNMPv2_C
SNMPv3_USM

Default:

SNMPv3_USM

Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

SNMP ID:

2.9.35.4

Console path:

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

Possible values:

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

Default:

empty

Security-Level

Set the security level that applies for the recipient to receive the SNMP traps

SNMP ID:

2.9.35.5

Console path:

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

Possible values:

NoAuthNoPriv

The SNMP message is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

AuthNoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

AuthPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Default:

NoAuthNoPriv

Status

Activates or deactivates this entry.

SNMP ID:

2.9.35.7

Console path:

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

Possible values:

Active
inactive

Default:

Active

2.2.10 Admitted-Protocols

Here you enable the SNMP versions supported by the device for SNMP requests and SNMP traps.

SNMP ID:

2.9.37

Console path:

Setup > SNMP

Possible values:

SNMPv1
SNMPv2
SNMPv3

Default:

SNMPv3

2.2.11 Allow-Admins

Enable this option if registered administrators (including the root user) should also have access via SNMPv3.

SNMP ID:

2.9.38

Console path:

Setup > SNMP

Possible values:

No
Yes

Default:

No

2.2.12 Operating

This entry enables or disables SNMP traps.

SNMP ID:

2.9.41

Console path:

Setup > SNMP

Possible values:

No
SNMP traps are switched off.

Yes
SNMP traps are enabled.

Default:

No

2.3 Config

Contains the general configuration settings.

SNMP ID:
2.11

Console path:
Setup

2.3.1 Comment-1

Comment on this device. For display purposes only.

SNMP ID:
2.11.1

Console path:
Setup > **Config**

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

Default:
empty

2.3.2 Comment-2

Comment on this device. For display purposes only.

SNMP ID:

2.11.2

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.3 Comment-3

Comment on this device. For display purposes only.

SNMP ID:

2.11.3

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.4 Comment-4

Comment on this device. For display purposes only.

SNMP ID:

2.11.4

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.5 Comment-5

Comment on this device. For display purposes only.

SNMP ID:

2.11.5

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.6 Comment-6

Comment on this device. For display purposes only.

SNMP ID:

2.11.6

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.7 Comment-7

Comment on this device. For display purposes only.

SNMP ID:

2.11.7

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.8 Comment-8

Comment on this device. For display purposes only.

SNMP ID:

2.11.8

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.9 Location

Location of the device. For display purposes only.

SNMP ID:

2.11.9

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.10 Administrator

Name of the device administrator. For display purposes only.

SNMP ID:

2.11.10

Console path:

Setup > **Config**

Possible values:

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

Default:

empty

2.3.11 Config-Aging-Minutes

Specify here the number of minutes after which an inactive TCP configuration connection (e.g. via SSH) is automatically terminated.

SNMP ID:

2.11.11

Console path:

Setup > **Config**

Possible values:

Max. 4 characters from `[0-9]`

Default:

15

2.3.12 LED-Mode

Set the operating mode for the LEDs.

Refer to the Quick Reference Guide for device-specific details about LED signaling.

SNMP ID:

2.11.18

Console path:

Setup > **Config**

Possible values:

On

The LED(s) of the device are permanently in operation and signal the operating state.

Off

The LED(s) of the device are switched off immediately after starting.

Timed-Off

The LED(s) of the device will shut off after a configurable time (**LED-Off-Seconds**).

Default:

On

2.3.13 Admins

Use this table to create administrators with restricted rights.

The root administrator always has all rights.

SNMP ID:

2.11.21

Console path:

Setup > **Config**

Administrator

Login name of the administrator in this row of the table.

SNMP ID:

2.11.21.1

Console path:

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

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-.`

Function-Rights

Here you activate the administrator's function rights in this row of the table.

SNMP ID:

2.11.21.3

Console path:

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

Possible values:

Basic
Admin-Management

Rights

The rights of the administrator in this row of the table.

SNMP ID:

2.11.21.5

Console path:

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

Possible values:

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

Hashed-Password

Hash value of the administrator password in this row of the table.

SNMP ID:

2.11.21.6

Console path:

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

Possible values:

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

2.3.14 LED-Off-Seconds

Set a time in seconds after the device starts, after which the LED(s) of the device are switched off if the **LED-Mode** is set to **Timed-Off**.

SNMP ID:

2.11.90

Console path:

Setup > **Config**

Possible values:

Max. 4 characters from `[0-9]`

Default:

300

2.3.15 LED-Test

This can be used to test the device LED. It will then illuminate in the corresponding color.

SNMP ID:

2.11.91

Console path:

Setup > **Config**

Possible values:

Off
Red
Green
Blue
All
No-Test

Default:

No-Test

2.3.16 Root-Hashed

Hash value of the password of the root administrator.

SNMP ID:

2.11.99

Console path:

Setup > **Config**

Possible values:

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

2.4 Time

Contains the general configuration settings for the time setting.

SNMP ID:

2.14

Console path:

Setup

2.4.1 Holidays

In this table, configure the public holidays for use in timeframes, for example.

SNMP ID:

2.14.15

Console path:

Setup > **Time**

Date

In this table, configure the public holidays for use in timeframes, for example.

SNMP ID:

2.14.15.1

Console path:

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

Possible values:

Max. 10 characters from `mm/dd/yyyy`

Special values:

yyyy = 0

Represents any year.

2.4.2 Timeframes

Timeframes are used to switch individual SSIDs on and off according to a schedule. One profile may contain several rows with different timeframes. Add the time frame to the logical WLAN settings for it to be used with the corresponding SSID.

SNMP ID:

2.14.16

Console path:

Setup > **Time**

Name

Enter the name of the time frame for referencing from the logical WLAN settings.

SNMP ID:

2.14.16.1

Console path:

Setup > **Time** > **Timeframe**

Possible values:

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

Default:

empty

Home

Here you set the start time (time of day) in the format HH:MM when the selected profile becomes valid.

SNMP ID:

2.14.16.2

Console path:

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

Possible values:

Max. 5 characters from `hh:mm`

Default:

00:00

Stop

Here you set the end time (time of day) in the format HH:MM when the selected profile ceases to be valid.

A stop time of HH:MM usually runs until HH:MM:00. The stop time 00:00 is an exception, since this is interpreted as 23:59:59.

SNMP ID:

2.14.16.3

Console path:

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

Possible values:

Max. 5 characters from `hh:mm`

Default:

00:00

Weekdays

Here you select the weekday on which the timeframe is to be valid.

SNMP ID:

2.14.16.4

Console path:

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

Possible values:

None
Sunday
Monday
Tuesday
Wednesday
Thursday
Friday
Saturday
Holiday

All days specified in the table *2.14.15 Holidays* on page 39.

2.4.3 Timezone

Configure the time zone for the location of the device.

SNMP ID:

2.14.20

Console path:

Setup > **Time**

Possible values:

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

Default:

UTC

2.4.4 NTP

Use this menu to configure an NTP server.

SNMP ID:

2.14.21

Console path:

Setup > **Time**

Operating

Enable the configured NTP server.

SNMP ID:

2.14.21.1

Console path:

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

Possible values:

No

Do not use an NTP server.

Yes

The NTP server set under **Server** is used to set the date and time.

Default:

No

Server

Enter the address of the NTP server.

SNMP ID:

2.14.21.1

Console path:

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

Possible values:

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

Default:

empty

2.5 WLAN

Configuration settings for the WLAN parameters

SNMP ID:

2.20

Console path:

Setup

2.5.1 Network

Here you configure the general settings for the WLAN networks (SSIDs) that are broadcast. Add a line to the table for each WLAN network. By default, the table is empty.

SNMP ID:

2.20.1

Console path:

Setup > **WLAN**

Network-Name

Configure a meaningful name for the WLAN network here. This **internal** identifier is used to reference the interface configuration from other parts of the configuration.

This is **not** the name of the SSID and is not displayed by the clients.

SNMP ID:

2.20.1.1

Console path:

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

Possible values:

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

SSID-Name

Here you configure the name of the SSID to be broadcast. This name is displayed on the wireless clients when searching for WLAN networks.

SNMP ID:

2.20.1.2

Console path:

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

Possible values:

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

Closed-Network

Here you configure whether this SSID is displayed to clients searching for a network.

If the SSID broadcast is suppressed, the access point will not respond to probe requests with an empty SSID. In this case, establishing a connection requires the SSID to be explicitly entered into and configured on the client.

SNMP ID:

2.20.1.4

Console path:

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

Possible values:

No

Show SSID.

Yes

Do not show SSID.

Max-Stations

This number determines the number of clients that can log on to the WLAN network simultaneously before further requesting clients are rejected.

SNMP ID:

2.20.1.10

Console path:

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

Possible values:

0 … 512

Special values:

0

The value "0" means that there is no limit, so unlimited number of clients can be logged in at the same time (up to a possible hardware-related limit).

Inter-station traffic

Depending on the application, it may be required that the WLAN clients connected to an access point can—or expressly cannot—communicate with other clients. Here you configure whether communication between the WLAN clients on the WLAN network should be allowed.

SNMP ID:

2.20.1.13

Console path:

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

Possible values:

No

Communication between the WLAN clients on the WLAN network is not permitted.

Yes

Communication between the WLAN clients on the WLAN network is permitted.

Min-Client-Strength

Here you configure the minimum signal strength in percent that a client must "show" at the access point in order for it to be able to connect to the WLAN.

SNMP ID:

2.20.1.16

Console path:

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

Possible values:

0 … 100

Special values:

0

The value "0" means that there is no minimum signal strength requirement and clients are always allowed to connect.

Exclude-From-Client-Management

Excludes this SSID from the band steering if necessary.

SNMP ID:

2.20.1.17

Console path:

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

Possible values:

No

Perform band steering with this SSID.

Yes

Exclude SSID from the band steering.

Timeframe

Enter the name of a *Timeframe* here. This is used to schedule when this SSID is switched on or off.

SNMP ID:

2.20.1.18

Console path:

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

Possible values:

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

Default:

empty

Summaric-Tx-Limit-Kbit/s

Here you set a WLAN bandwidth limit that applies to the entire WLAN network. All of the logged in clients can only receive data with the transmission rate configured here. The transmission direction is considered relative to the access point, so “Tx” means the transmission rate from the access point to the client. This setting affects the download rate at the client.

SNMP ID:

2.20.1.20

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Special values:

0

The value “0” means that no limitation is active.

Summaric-Rx-Limit-Kbit/s

Here you set a WLAN bandwidth limit that applies to the entire WLAN network. All of the logged in clients can only send data with the transmission rate configured here. The transmission direction is considered relative to the access point, so “Rx” means the transmission rate from the client to the access point. This setting affects the upload rate at the client.

SNMP ID:

2.20.1.21

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Special values:

0

The value “0” means that no limitation is active.

Key

Configure the pre-shared key (PSK) used for the WLAN network here.

This entry only applies if an encryption profile using WPA(2)-PSK is selected. If 802.1X is used, the entry has no effect and the field can be left blank.

SNMP ID:

2.20.1.100

Console path:

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

Possible values:

8 to 63 characters `WPA key`

Radios

Configure here the WLAN frequencies that the SSID is to be broadcast on.

SNMP ID:

2.20.1.101

Console path:

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

Possible values:

2.4GHz+5GHz
The SSID is broadcast on the frequencies 2.4 GHz and 5 GHz.

2.4GHz
The SSID is only broadcast on the 2.4-GHz frequency.

5GHz
The SSID is only broadcast on the 5-GHz frequency.

None
The SSID will not be broadcast. This can be used as a general on/off switch for the SSID.

Encryption-Profile

Here you configure an encryption profile from the methods available under **Setup** > **WLAN** > **Encryption**. This profile defines which authentication and encryption method should be used for the SSID.

SNMP ID:

2.20.1.102

Console path:

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

Possible values:

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

Idle-Timeout

This is the time in seconds after which a client is disconnected if the access point has no more packets received from it. Any traffic from the client resets this timeout.

SNMP ID:

2.20.1.103

Console path:

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

Possible values:

Max. 4 characters from `[0-9]`

VLAN-ID

This VLAN ID is used to tag the data packets arriving from the WLAN and heading for the LAN. Similarly, packets with this VLAN ID arriving from the LAN are directed to the WLAN and are de-tagged.

This operating mode corresponds to what is normally known as the “Access” tagging mode, since it is assumed that wireless clients usually transmit data untagged. Tagging mode cannot be adjusted.

SNMP ID:

2.20.1.200

Console path:

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

Possible values:

0 … 4095

Special values:

0

The default value 0 means that no VLAN is used.

2.5.2 Country

Here you configure the country where the device is operated. Depending on this, the appropriate regulatory limits are set automatically.

SNMP ID:

2.20.2

Console path:

Setup > **WLAN**

Possible values:

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

2.5.3 Encryption

Here you configure the settings for the encryption and authentication on the WLAN networks. A variety of encryption profiles are stored by default and these can be used for the configuration of the WLAN networks.

SNMP ID:

2.20.3

Console path:

Setup > **WLAN**

Profile-Name

Choose a meaningful name for the encryption profile here. This internal identifier is used to reference the encryption profile from other parts of the configuration.

SNMP ID:

2.20.3.1

Console path:

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

Possible values:

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

Encryption

Here you configure whether the WLAN network should be encrypted or if no encryption should be used (Open Network).

SNMP ID:

2.20.3.2

Console path:

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

Possible values:

No

Do not use encryption.

Yes

Use encryption.

Method

Here you configure the encryption method.

The WEP process no longer provides adequate security and should only be used to integrate legacy clients that do not support a newer security method. If this is the case, we recommend that you isolate the WEP clients in their own VLAN to keep them separate from the rest of the WLAN infrastructure.

SNMP ID:

2.20.3.4

Console path:

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

Possible values:

WEP-40-Bits
AES with 40 bits key length

WEP-104-Bits
AES with 104 bits key length

WEP-128-Bits
AES with 128 bits key length

WEP-40-Bits-802.1X

AES with 40 bits key length and 802.1X

Note that 802.1X requires a RADIUS server profile to be specified as well.

WEP-104-Bits-802.1X

AES with 104 bits key length and 802.1X

Note that 802.1X requires a RADIUS server profile to be specified as well.

WEP-128-Bits-802.1X

AES with 128 bits key length and 802.1X

Note that 802.1X requires a RADIUS server profile to be specified as well.

802.11i-WPA-PSK
WPA(2) with Pre-Shared-Key

802.11i-WPA-802.1X

WPA(2) with 802.1X

Note that 802.1X requires a RADIUS server profile to be specified as well.

Enhanced-Open

Until now, hotspots were mainly operated without encryption, meaning that the data transmitted over the wireless interface was open to inspection. What also offers only limited security is the widespread practice of securing a hotspot with WPA2-PSK and publicly announcing the shared key, for example, on a poster. Since WPA2-PSK does not offer Perfect Forward Secrecy, an attacker who knows this key can use it to subsequently decrypt recordings of secure data traffic. The Enhanced Open method minimizes these risks. Clients that support this method use encrypted communication to prevent other users in the same radio cell from eavesdropping on their communications. The threat of a man-in-the-middle attack remains, but the risk is much lower than when using an unencrypted open hotspot. Just set the encryption method. That is all you need to do to encrypt communications for clients that support this method.

WPA-Version

Here you configure the WPA version used for the encryption methods **802.11i WPA-PSK** and **802.11i WPA 802.1X**.

SNMP ID:
2.20.3.9

Console path:

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

Possible values:

WPA1

WPA version 1 is used exclusively.

WPA2

WPA version 2 is used exclusively.

WPA3

WPA version 3 is used exclusively.

WPA1/2

Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.

WPA2/3

Whether the encryption method WPA 2 or 3 is used depends on the capabilities of the client.

WPA-Rekeying-Cycle

Here you configure the time in seconds after which the access point performs rekeying when operating WPA(2).

SNMP ID:

2.20.3.11

Console path:

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

Possible values:

Max. 32 characters from `[0-9]`

Special values:

0

The value “0” means that no rekeying is performed.

WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used.

Operating TKIP is only recommended when using older WLAN clients which do not support AES.

If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

SNMP ID:

2.20.3.12

Console path:

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

Possible values:

TKIP
TKIP encryption is used.

AES
AES encryption is used.

TKIP/AES
Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

WPA2-3-Session-Keytypes

Here you configure the session key type to be used for WPA version 2. This also influences the encryption method used.

Operating TKIP is only recommended when using older WLAN clients which do not support AES.

If a WLAN network uses only WEP or WPA with TKIP for encryption, the WLAN clients connected to it achieve a maximum gross data rate of 54 Mbps.

SNMP ID:

2.20.3.13

Console path:

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

Possible values:

TKIP
TKIP encryption is used.

AES
AES encryption is used.

TKIP/AES
Whether the encryption method TKIP or AES is used depends on the capabilities of the client.

Prot.-Mgmt-Frames

By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information (protected management frames, PMF), meaning that potential attackers can no longer interfere with the communications if they don't have the corresponding key.

As of WPA3, management frames have to be encrypted, so this value is ignored there and is assumed to be set as "Mandatory". For WPA2, this is optional.

SNMP ID:

2.20.3.14

Console path:

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

Possible values:

No

Do not use PMF.

optional

Offer PMF. The client decides whether to use them.

mandatory

Use PMF

Pre-Authentication

Fast authentication by means of the Pairwise Master Key (PMK) only works if the WLAN client was logged on to the AP previously. The WLAN client uses pre-authentication to reduce the time to logon to the AP at the first logon attempt.

Usually, a WLAN client carries out a background scan of the environment to find existing APs that it could connect to. APs that support WPA2/802.1X can communicate their pre-authentication capability to any WLAN clients that issue requests. A WPA2 pre-authentication differs from a normal 802.1X authentication as follows:

- The WLAN client logs on to the new AP via the infrastructure network, which interconnects the APs. This can be an Ethernet connection or a WDS link (wireless distribution system), or a combination of both connection types.
- A pre-authentication is distinguished from a normal 802.1X authentication by the differing Ethernet protocol (EtherType). This allows the current AP and all other network partners to treat the pre-authentication as a normal data transmission from the WLAN client.
- After successful pre-authentication, the negotiated PMK is stored to the new AP and the WLAN client.

The use of PMKs is a prerequisite for pre-authentication. Otherwise, pre-authentication is not possible.

- When the client wants to connect to the new AP, the stored PMK significantly accelerates the logon procedure. The further procedure is equivalent to the PMK caching.

SNMP ID:

2.20.3.16

Console path:

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

Possible values:

No

Do not perform pre-authentication.

Yes

Perform pre-authentication.

WPA2-Key-Management

Here you specify which standard the WPA2 key management should follow.

SNMP ID:

2.20.3.19

Console path:

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

Possible values:

Standard

Enables key management according to the IEEE 802.11i standard without Fast Roaming and with keys based on SHA-1. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.

Fast roaming

Enables fast roaming according to the IEEE 802.11r standard.

Standard+Fast-Roaming

Combination of standard and fast roaming

Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients may refuse a connection if an option other than Standard is enabled.

PMK-IAPP-Secret

This passphrase is used to implement encrypted opportunistic key caching. This is required to use Fast Roaming over IAPP. Each interface must be assigned an individual IAPP passphrase in the WLAN connection settings. This is used to encrypt the pairwise master keys (PMKs). Access points that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between one another and ensure uninterrupted connections. You should therefore ensure that this passphrase is identical on all of the access points that should operate fast roaming.

SNMP ID:

2.20.3.20

Console path:

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

Possible values:

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

RADIUS-Server-Profile

Here you configure the RADIUS server profile used when operating 802.1X. No input is required when using PSK-based encryption methods.

SNMP ID:

2.20.3.21

Console path:

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

Possible values:

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

SAE/OWE-Groups

Contains the selection of the available Diffie-Hellman groups as a bit mask used by the protocol partners to create a key for exchanging data. The available groups use elliptical curves

The authentication method SAE (Simultaneous Authentication of Equals) used by WPA3 uses these methods together with AES to generate a cryptographically strong key.

SNMP ID:

2.20.3.26

Console path:

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

Possible values:

DH-19

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

DH-20

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

DH-21

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

Default:

DH-19

2.5.4 Client-Management

Configure the settings for band steering here. Using band steering, clients can be steered from the overloaded 2.4-GHz frequency band to the 5-GHz frequency band, so that more bandwidth is available for the individual client, and the user experience is improved. LCOS LX supports 802.11v standard, which has the option to steer clients to the frequency band that offers them the best signal. Even clients that do not support the 802.11v standard can be steered to the 5-GHz band by deliberately delaying probe responses or by deliberately disconnecting them from the WLAN.

SNMP ID:

2.20.4

Console path:

Setup > **WLAN**

Active-Profile

Here you select the profile with the settings for the band-steering module.

SNMP ID:

2.20.4.1

Console path:

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

Possible values:

P-DEFAULT

Steering is based on the load on the medium and the interference detected on the current channel and is preferably performed with 802.11v. If the client does not support 802.11v, steering is induced by deliberately disassociating the client. Steering can be performed before association and, if necessary, once the client is already associated. This is the recommended profile.

P-LEGACY

Steering is performed before the client associates by deliberately withholding probe responses. Regardless of the load, the 5-GHz band is always preferred.

P-DISABLED

No steering is performed. The client decides independently which frequency band to use.

<Custom>

In addition to the existing profiles, you can also define your own profiles under **Profiles**.

Default:

P-DEFAULT

Profiles

Here you adjust the detailed settings of the steering profiles or you can create a new profile.

SNMP ID:

2.20.4.2

Console path:

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

Profile-Name

The name of the profile.

SNMP ID:

2.20.4.2.1

Console path:

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

Possible values:

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

Operating

Controls whether band steering is active for this profile.

SNMP ID:

2.20.4.2.2

Console path:

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

Possible values:

No

Band steering is not active.

Yes

Band steering is active.

Steering-Min-PHY-Signal

Specifies the client signal strength (in dB) below which client steering is initiated.

SNMP ID:

2.20.4.2.3

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Upgrade-TX-Rate-Threshold

Specifies the limit value of the transmission rate (in kbps), at which the client should potentially be steered to the 5-GHz band.

SNMP ID:

2.20.4.2.4

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Upgrade-PHY-Signal-Threshold

Specifies the client signal strength (in dB) required as a minimum before the client is considered for steering to the 5-GHz band.

SNMP ID:

2.20.4.2.5

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Downgrade-TX-Rate-Threshold

Specifies the limit value of the transmission rate (in kbps), at which the client should potentially be steered to the 2.4-GHz band.

SNMP ID:

2.20.4.2.6

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Downgrade-PHY-Signal-Threshold

Specifies the client signal strength (in dB) that must be exceeded before the client is considered for steering to the 2.4-GHz band.

For steering to 2.4 GHz (downgrade), the signal strength has to fall below the value configured here and also below the **Downgrade TX rate threshold** value.

SNMP ID:

2.20.4.2.7

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

2.4GHz-Sub-Profile

Here you configure which 2.4-GHz sub-profile is used.

SNMP ID:

2.20.4.2.8

Console path:

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

Possible values:

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

5GHz-Sub-Profile

Here you configure which 5-GHz sub-profile is used.

SNMP ID:

2.20.4.2.9

Console path:

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

Possible values:

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

2.4GHz-Sub-Profiles

Configure the settings of the 2.4-GHz sub-profile here.

SNMP ID:

2.20.4.3

Console path:

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

Profile-Name

The profile name of the 2.4-GHz sub-profile.

SNMP ID:

2.20.4.3.1

Console path:

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

Possible values:

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

Utilization-Check-Interval

Configures the interval (in seconds) for checking media utilization.

SNMP ID:

2.20.4.3.2

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Utilization-Average-Period

Configures the period (in seconds) over which the media utilization is averaged. This value must always be higher than the value configured for the Utilization check interval.

SNMP ID:

2.20.4.3.3

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Utilization-Overload-Threshold

Configures the media utilization (in percent) above which the current 2.4-GHz channel is assumed to be overloaded.

SNMP ID:

2.20.4.3.4

Console path:

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

Possible values:

0 … 100

Utilization-Deviation-Threshold

Configures the media utilization (in percent) which, together with the expected media utilization, may be reached before any further downgrade steering is stopped (until the next measurement of medium utilization).

SNMP ID:

2.20.4.3.5

Console path:

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

Possible values:

0 … 100

Interference-Detection

Configures whether interference on the configured 2.4-GHz channel is considered for steering decisions.

SNMP ID:

2.20.4.3.6

Console path:

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

Possible values:

No

Do not take interference into account.

Yes

Take interference into account.

Delay-Probe-PHY-Signal-Threshold

Specifies the client signal strength (in dB) that must be reached before steering-related probe responses are delayed.

SNMP ID:

2.20.4.3.7

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Delay-Probe-Time-Window

Configures the time window (in seconds) in which a client must receive at least the number of probe requests configured under **Delay probe min. request count** before it responds to them.

SNMP ID:

2.20.4.3.8

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Delay-Probe-Min-Request-Count

Configures the number of probe requests that a client must receive within the period configured under **Delay probe time window** before it responds to them.

SNMP ID:

2.20.4.3.9

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

5GHz-Sub-Profiles

Configure the settings of the 5-GHz sub-profile here.

SNMP ID:

2.20.4.4

Console path:

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

Profile-Name

The profile name of the 5-GHz sub-profile.

SNMP ID:

2.20.4.4.1

Console path:

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

Possible values:

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

Utilization-Check-Interval

Configures the interval (in seconds) for checking media utilization.

SNMP ID:

2.20.4.4.2

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Utilization-Average-Period

Configures the period (in seconds) over which the media utilization is averaged. This value must always be higher than the value configured for the Utilization check interval.

SNMP ID:

2.20.4.4.3

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Utilization-Overload-Threshold

Configures the media utilization (in percent) above which the current 5-GHz channel is assumed to be overloaded.

SNMP ID:

2.20.4.4.4

Console path:

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

Possible values:

0 … 100

Utilization-Deviation-Threshold

Configures the media utilization (in percent) which, together with the expected media utilization, may be reached before any further downgrade steering is stopped (until the next measurement of medium utilization).

SNMP ID:

2.20.4.4.5

Console path:

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

Possible values:

0 … 100

Interference-Detection

Configures whether interference on the configured 5-GHz channel is considered for steering decisions.

SNMP ID:

2.20.4.4.6

Console path:

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

Possible values:

No

Do not take interference into account.

Yes

Take interference into account.

2.5.5 Radio-Settings

Here you configure all of the settings relating to the physical radio parameters. By default, there is an entry in the table for every physical WLAN radio for modification as required.

SNMP ID:

2.20.8

Console path:

Setup > **WLAN**

Ifc

The internal name of the WLAN radio. This cannot be changed.

SNMP ID:

2.20.8.1

Console path:

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

5GHz-Mode

Here you configure the mode used for 5-GHz radio operation. This directly affects the available data rates. If a restriction is set here, a client attempting to login triggers a check to see whether the modes used by the client match with those configured here. Depending on this, the login is allowed or denied. The following modes are available:

Maximum compatibility and performance is available by setting the mode to **Auto**.

SNMP ID:

2.20.8.3

Console path:

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

Possible values:

11an-mixed

The modes 802.11a and 802.11n are used.

11anac-mixed

The modes 802.11a, 802.11n and 802.11ac are used.

11nac-mixed

The modes 802.11n and 802.11ac are used.

11ac-only

Only the 802.11ac mode is used.

11anacax-mixed

The modes 802.11a, 802.11n, 802.11ac and 802.11ax (Wi-Fi 6) are used.

Auto

All modes supported by the device are used.

Radio-Band

Here you configure whether this radio module works in the 2.4-GHz or 5-GHz spectrum.

SNMP ID:

2.20.8.6

Console path:

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

Possible values:

2.4GHz
The radio module works in the 2.4-GHz spectrum.

5GHz
The radio module works in the 5-GHz spectrum.

Sub-Band

Here you configure which sub-bands are used in the 5-GHz mode.

WLAN channels 120, 124 and 128 are not used because these channels are reserved for the primary user RADAR.

SNMP ID:

2.20.8.7

Console path:

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

Possible values:

Band-1
Only sub-band 1 is used. This corresponds to the WLAN channels 36, 40, 44, 48, 52, 56, 60 and 64.

Band-2
Only sub-band 2 is used. This corresponds to the WLAN channels 100, 104, 108, 112, 116, 132, 136 and 140.

Band-1+2
Sub-bands 1 and 2 are used.

Channel

Here you configure the channel to be used for WLAN radio operations.

In 5-GHz mode, the channel set here represents a preferred channel. However, since the 5-GHz band requires the use of Dynamic Frequency Selection (DFS), there is no guarantee that the preferred channel will be used.

SNMP ID:

2.20.8.8

Console path:

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

Possible values:

Max. 10 characters from `[0-9]`

Special values:

0

The value “0” allows the automatic selection of a suitable channel.

2.4GHz-Mode

Here you configure the mode used for 2.4-GHz radio operation. This directly affects the available data rates. If a restriction is set here, a client attempting to login triggers a check to see whether the modes used by the client match with those configured here. Depending on this, the login is allowed or denied.

Maximum compatibility and performance is available by setting the mode to **Auto**.

SNMP ID:

2.20.8.9

Console path:

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

Possible values:

11bg-mixed

The modes 802.11b and 802.11g are used.

11g-only

Only the 802.11g mode is used.

11bgn-mixed

The modes 802.11b, 802.11g and 802.11n are used.

11gn-mixed

The modes 802.11g and 802.11n are used.

11bgnax-mixed

The modes 802.11b, 802.11g, 802.11n and 802.11ax (Wi-Fi 6) are used.

11gnax-mixed

The modes 802.11g, 802.11n and 802.11ax (Wi-Fi 6) are used.

Auto

All modes supported by the device are used.

Channel-List

Here you configure a comma-separated list of further WLAN channels. Automatic channel selection selects a channel from this list, rather than from the full range of supported WLAN channels.

SNMP ID:

2.20.8.13

Console path:

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

Possible values:

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

Max.-Channel-Bandwidth

Here you configure the maximum allowed channel bandwidth.

SNMP ID:

2.20.8.24

Console path:

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

Possible values:

20MHz

The channel bandwidth is always 20 MHz.

40MHz

Depending on the environment, channel bandwidth is up to 40 MHz, but this can also fall back to 20 MHz.

80MHz

Depending on the environment, channel bandwidth is up to 80 MHz, but this can also fall back to 40 MHz or 20 MHz.

160MHz

Depending on the environment, channel bandwidth is up to 160 MHz, but this can also fall back to 80 MHz, 40 MHz or 20 MHz.

Auto

For a 2.4-GHz radio the channel bandwidth of 20 MHz is always used. For a 5-GHz radio the maximum possible channel bandwidth (up to 160 MHz) is always used, depending on the environment.

Exclude-DFS-Channels

Here you configure whether to use channels in the 5-GHz band that require Dynamic Frequency Selection (DFS).

If these channels are excluded here, the channels still available in the 5-GHz band are 36, 40, 44 and 48. Since DFS is not required for these channels, they can be set with the option **Exclude-DFS-Channels** in the radio channel and also in the **Channel-List**.

SNMP ID:

2.20.8.29

Console path:

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

Possible values:

No

Use channels reserved for DFS.

Yes

Do not use channels reserved for DFS.

2.5.6 Automatic-Environment-Scan-Enabled

This entry is set by the LANCOM Management Cloud, which requires the environment scan. The results can only be read by the LANCOM Management Cloud.

SNMP ID:

2.20.9

Console path:

Setup > **WLAN**

Possible values:

Yes

Automatic environmental scan is performed.

No

Automatic environmental scan is not performed.

2.5.7 Automatic-Environment-Scan-Time-Begin

Start time for the time window in which the automatic environmental scan is performed.

SNMP ID:

2.20.10

Console path:

Setup > **WLAN**

Possible values:

Time in format `hh:mm`

2.5.8 Automatic-Environment-Scan-Time-End

Stop time for the time window in which the automatic environmental scan is performed.

SNMP ID:

2.20.11

Console path:

Setup > **WLAN**

Possible values:

Time in format `hh:mm`

2.5.9 LEPS

LANCOM Enhanced Passphrase Security (LEPS) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address. An alternative is to implement a MAC address filter.

SNMP ID:

2.20.133

Console path:

Setup > **WLAN**

Operating

Switches LEPS on or off. When switched off, LEPS users are ignored during WLAN client authentication.

SNMP ID:

2.20.133.1

Console path:

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

Possible values:

No
Yes

Default:

No

Profiles

Configure LEPS profiles here and link them to an SSID. You can then assign the LEPS profiles to the LEPS users. You can overwrite the profile values for any particular user with individual values.

SNMP ID:

2.20.133.2

Console path:

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

Name

Enter a unique name for the LEPS profile here.

SNMP ID:

2.20.133.2.1

Console path:

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

Possible values:

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

Network-Name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS profile applies. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS profile.

SNMP ID:

2.20.133.2.2

Console path:

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

Possible values:

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

Mac-List

Here you specify if and how MAC addresses are checked.

SNMP ID:

2.20.133.2.3

Console path:

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

Possible values:

Disabled

The MAC address plays no role during LEPS authentication. If any user-specific passphrase has been set, this will be checked.

Whitelist

Only clients whose MAC address is known are admitted.

Blacklist

Only clients whose MAC address is not known are admitted.

VLAN

Here you specify which VLAN is assigned to a LEPS user who is connected to this profile.

SNMP ID:

2.20.133.2.5

Console path:

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

Possible values:

0 … 4095

Users

Create individual LEPS users here. Every LEPS user must be connected to a profile that was created previously.

SNMP ID:

2.20.133.3

Console path:

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

Name

Enter a unique name for the LEPS user here.

SNMP ID:

2.20.133.3.1

Console path:

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

Possible values:

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

Profiles

Select the profile for which the LEPS user is valid. The only LEPS users who can authenticate at the SSID are those who are connected to it via the LEPS profile.

SNMP ID:

2.20.133.3.2

Console path:

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

Possible values:

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

WPA-Passphrase

Here you can specify the passphrase to be used by LEPS users to authenticate at the WLAN.

SNMP ID:

2.20.133.3.3

Console path:

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

Possible values:

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

VLAN

Here you specify which VLAN is assigned to the LEPS user. If no VLAN is configured here, the VLAN configured in the LEPS profile (if any) applies. If a VLAN is configured in both the LEPS profile and for the LEPS user, the VLAN-ID configured for the LEPS user takes priority.

SNMP ID:

2.20.133.3.4

Console path:

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

Possible values:

0 … 4095

MAC-Address

Optionally specify a MAC address for a MAC filter. The setting in the profile decides whether this entry is ignored or whether the client devices listed in this table only are able to log on (whitelist). Using a blacklist, the MAC filter works the other way round: the specified MAC addresses cannot log on.

SNMP ID:

2.20.133.3.7

Console path:

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

Possible values:

MAC address in the format `xx:xx:xx:xx:xx:xx`

2.6 RADIUS

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

SNMP ID:

2.30

Console path:

Setup

2.6.1 RADIUS server

Here you configure the settings for RADIUS server profiles to be used with WLAN networks that operate 802.1X for authentication.

SNMP ID:

2.30.3

Console path:

Setup > **RADIUS**

Name

Choose a meaningful name for the RADIUS server profile here. This internal identifier is used to reference the RADIUS server profile from other parts of the configuration.

SNMP ID:

2.30.3.1

Console path:

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

Possible values:

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

Port

Select the (UDP) port used to contact the RADIUS server.

This is usually the port 1812 (RADIUS authentication).

SNMP ID:

2.30.3.3

Console path:

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

Possible values:

0 … 65535

Secret

Here you configure the secret used to encrypt the traffic between the device and the RADIUS server. This secret must also be stored on the RADIUS server.

SNMP ID:

2.30.3.4

Console path:

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

Possible values:

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

Backup

Here you configure a backup profile, which will be used if the RADIUS server in the profile configured here cannot be reached.

SNMP ID:

2.30.3.5

Console path:

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

Possible values:

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

Server-IP-Address

Here you configure the host name or IP address where the RADIUS server is to be reached.

SNMP ID:

2.30.3.8

Console path:

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

Possible values:

Max. 64 characters from `IPv4 or IPv6 address`

Accounting port

Select the port (UDP) used to contact the RADIUS accounting server.

This is usually the port 1813 (RADIUS accounting).

SNMP ID:

2.30.3.9

Console path:

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

Possible values:

0 … 65535

Accounting IP address

Here you configure the host name or IP address where the RADIUS accounting server is to be reached.

SNMP ID:

2.30.3.14

Console path:

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

Possible values:

Max. 64 characters from `IPv4 or IPv6 address`

MAC-Check

A user name can be authenticated with a MAC address instead of using the RADIUS server.

SNMP ID:

2.30.3.15

Console path:

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

Possible values:

No

No check based on the MAC address.

Yes

Check the permissions of the clients on the RADIUS server by means of the MAC address.

2.6.2 Supplicant-Ifc-Setup

These are the settings for the 802.1X supplicant functionality, which authenticates the device towards the LAN at a switch infrastructure secured by 802.1X.

SNMP ID:

2.30.11

Console path:

Setup > **RADIUS**

Interface name

The name of the LAN interface. Currently there is only the interface INTRANET, and this cannot be changed.

SNMP ID:

2.30.11.1

Console path:

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

Possible values:

Max. 64 characters from `INTRANET`

Method

The EAP method used to authenticate at the 802.1X infrastructure.

SNMP ID:

2.30.11.2

Console path:

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

Possible values:

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

User name

The user name to use to authenticate at the 802.1X infrastructure.

SNMP ID:

2.30.11.3

Console path:

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

Possible values:

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

Password

The password to use to authenticate at the 802.1X infrastructure.

SNMP ID:

2.30.11.4

Console path:

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

Possible values:

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

2.7 WLAN-Management

LCOS LX-based access points can be managed by a LANCOM WLAN controller (WLC). Like LCOS-based access points, they use the CAPWAP protocol.

The prerequisite for this is a LANCOM WLAN controller with LCOS version 10.40 or higher.

In their factory default settings, LCOS LX-based access points search the local network for a WLAN controller. They also query the DNS name “WLC-Address” to try to reach a WLAN controller.

If an access point is already being managed by a WLC, it will no longer try to contact the LANCOM Management Cloud.

This make it possible to use zero-touch commissioning, which means that no further configuration of the access point is necessary. In certain cases it may still be necessary to carry out a manual configuration. This can be done in the device configuration here.

SNMP ID:

2.59

Console path:

Setup

2.7.1 Static-WLC-Configuration

Configures user-specified WLAN controllers. This may be necessary if a WLC cannot be found via the local network (e.g. with routed connections) and also the DNS name “WLC-Address” cannot be used to inform the access point about the address of the WLC.

SNMP ID:

2.59.1

Console path:

Setup > **WLAN-Management**

IP-Address

Set the IP address or DNS name of a WLAN controller.

SNMP ID:

2.59.1.1

Console path:

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

Possible values:

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

Port

Configures the port used to attempt to reach a WLC.

SNMP ID:

2.59.1.2

Console path:

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

Possible values:

0 … 65535

Default:

1027

2.7.2 Operating

This configures whether an access point actively searches for a WLC and can be managed by one.

This option should be deactivated for operation in stand-alone mode.

SNMP ID:

2.59.2

Console path:

Setup > **WLAN-Management**

Possible values:

No

The search for a WLC is disabled.

Yes

A WLC is actively searched for.

Default:

Yes

2.7.3 Update-Cert-Before

Configures how many days before its expiry that the device certificate used by the access point to authenticate at the WLC is renewed.

SNMP ID:

2.59.3

Console path:

Setup > **WLAN-Management**

Possible values:

Max. 4 characters from `[0-9]`

Default:

30

2.7.4 Capwap-Port

Configures the port used to attempt to reach a WLC. The default value of 1027 is the default port used by the CAPWAP protocol. LANCOM By default, WLCs also use this port.

SNMP ID:

2.59.4

Console path:

Setup > **WLAN-Management**

Possible values:

0 … 65535

Default:

1027

2.8 IP-Configuration

Parameter for the IP configuration of the device.

SNMP ID:

2.70

Console path:

Setup

2.8.1 Static-Parameters

IP and network configuration settings that apply when you use static IP addresses.

The settings made in this table only come into effect if the IPv4 or IPv6 address source for the corresponding LAN interface is set to **static**. Otherwise all of the necessary information is retrieved via DHCP, for example, in which case no configuration is required here.

SNMP ID:

2.70.4

Console path:

Setup > **IP-Configuration**

Interface-Name

Enter the name of the interface, which the other settings made here refer to.

SNMP ID:

2.70.4.1

Console path:

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

Possible values:

Max. 64 characters from `INTRANET`

IPv4-Gateway

Here you configure the IPv4 gateway for the referenced interface.

SNMP ID:

2.70.4.2

Console path:

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

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

IPv6-Gateway

Here you configure the IPv6 gateway for the referenced interface.

SNMP ID:

2.70.4.3

Console path:

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

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

Primary-IPv4-DNS

Here you configure the primary IPv4 DNS gateway for the referenced interface.

SNMP ID:

2.70.4.4

Console path:

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

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

Secondary-IPv4-DNS

Here you configure the secondary IPv4 DNS gateway for the referenced interface.

SNMP ID:

2.70.4.5

Console path:

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

Possible values:

Max. 16 characters from `IPv4 address: a.b.c.d`

Primary-IPv6-DNS

Here you configure the primary IPv6 DNS gateway for the referenced interface.

SNMP ID:

2.70.4.6

Console path:

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

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

Secondary-IPv6-DNS

Here you configure the secondary IPv6 DNS gateway for the referenced interface.

SNMP ID:

2.70.4.7

Console path:

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

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d`

2.8.2 LAN-Interfaces

Here you specify basic configuration options relating to your device's own IP settings and network access.

SNMP ID:

2.70.6

Console path:

Setup > **IP-Configuration**

Interface-Name

Set a meaningful name for the interface here. This name is used to reference the interface configuration from other parts of the configuration.

SNMP ID:

2.70.6.1

Console path:

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

Possible values:

Max. 64 characters from `INTRANET`

Interface-ID

The internal identifier for the interface. This cannot be modified.

SNMP ID:

2.70.6.2

Console path:

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

VLAN-ID

Here you specify a VLAN ID for which the interface should be active and accessible.

SNMP ID:

2.70.6.3

Console path:

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

Possible values:

0 … 4095

Special values:

0

The default value 0 means that no VLAN is used.

IPv4-Address-Source

Here you select how the IPv4 address of the interface is to be obtained.

SNMP ID:

2.70.6.4

Console path:

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

Possible values:

DHCP

The IP address is retrieved via DHCP.

Static

The static IP address configured for the interface is used.

IPv6-Address-Source

Here you select how the IPv6 address of the interface is to be obtained.

SNMP ID:

2.70.6.5

Console path:

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

Possible values:

Router-Advertisement

The IPv6 address is derived from router advertisements that the device receives on the respective interface.

If the flag in the router advertisement is set to Other and/or Managed, additional configuration options are obtained via DHCPv6—even if the address source is set to **Router-Advertisement**.

DHCPv6

The IPv6 address is obtained via DHCPv6.

Static

The static IPv6 address configured for the interface is used.

Static-IPv4-Address

Here you configure the IP address to be used when the **IPv4-Address-Source** is set to **Static**. Add the subnet mask in CIDR notation (e.g. "/24") as a suffix.

SNMP ID:

2.70.6.6

Console path:

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

Possible values:

Max. 19 characters from `IPv4 address: a.b.c.d/xx`

Static-IPv6-Address

Here you configure the IP address to be used when the **IPv6-Address-Source** is set to **Static**. Add the subnet mask in CIDR notation (e.g. "/64") as a suffix.

SNMP ID:

2.70.6.7

Console path:

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

Possible values:

Max. 44 characters from `IPv6 address: a:b:c::d/64`

Comment

Here you can enter a comment about the interface configuration.

SNMP ID:

2.70.6.9

Console path:

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

Possible values:

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

2.9 LMC

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

SNMP ID:

2.102

Console path:

Setup

2.9.1 Operating

Specify whether the device should be managed via the LMC.

SNMP ID:

2.102.1

Console path:

Setup > **LMC**

Possible values:

No

The device does not connect to the LMC.

Yes

The LMC manages the device.

Default:

Yes

2.9.2 Delete-Certificate

Use this action to delete the LMC certificate.

SNMP ID:

2.102.7

Console path:

Setup > **LMC**

Possible arguments:

none

2.9.3 DHCP-Client-Auto-Renew

With this parameter you specify the behavior of the device in the event that there is a change to the DHCP settings in the network and the LMC client is unable to connect to the LMC.

If the LMC client is unable to reach its configured LMC, it is likely that the IP address range of the network has changed. A device that is configured as a DHCP client retains the IP address that was previously allocated to it until the DHCP lease time expires. By enabling this parameter, the device requests a new DHCP address (DHCP-Renew) regardless of the remaining DHCP lease time.

SNMP ID:

2.102.8

Console path:

Setup > **LMC**

Possible values:

No

If the LMC client loses its connection to the LMC, no DHCP-Renew is triggered.

Yes

If the LMC client loses its connection to the LMC, a DHCP-Renew is triggered. If the DHCP-Renew is not successful, the DHCP process is restarted. The device then tries to get an IP address from any DHCP server in order to reconnect to the LMC.

Default:

No

2.9.4 Configuration-Via-DHCP

Specify whether the LMC domain should be obtained from a DHCP server.

SNMP ID:

2.102.13

Console path:

Setup > **LMC**

Possible values:

No

The LMC domain is not obtained from a DHCP server. The value configured in the field **LMC-Domain** is taken.

Yes

The LMC domain is obtained from a DHCP server.

In order for the DHCP server to provide the LMC domain, the DHCP server requires sub-option 18 of the DHCP option 43 to be set to the LMC domain. For further information about configuring the LMC parameters, see the LCOS Reference Manual section “Delivery of the LMC domain by the LCOS DHCP server”.

Default:

No

2.9.5 LMC-Domain

Enter the domain name for the LMC here. By default, the domain is set to the Public LMC for the first connection. If you wish to manage your device with your own Management Cloud (“Private Cloud” or “on-premises installation”), please enter your LMC domain.

SNMP ID:

2.102.15

Console path:

Setup > **LMC**

Possible values:

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

2.9.6 Rollout-Project-ID

Enter the project ID of this device in the LMC. The first time the device connects to the LMC, it will be assigned accordingly.

SNMP ID:

2.102.16

Console path:

Setup > **LMC**

Possible values:

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

2.9.7 Rollout-Location-ID

Enter the location of this device in the LMC. The first time the device connects to the LMC, it will be assigned accordingly.

SNMP ID:

2.102.17

Console path:

Setup > **LMC**

Possible values:

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

2.9.8 Rollout-Device-Role

Enter the role assigned to this device in the LMC. The first time the device connects to the LMC, it will be assigned accordingly.

SNMP ID:

2.102.18

Console path:

Setup > **LMC**

Possible values:

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

2.9.9 Pairing-Token

Here you enter the activation code that you created for pairing with the LMC.

SNMP ID:

2.102.200

Console path:

Setup > **LMC**

Possible values:

Max. 36 characters from `^[1-9A-NP-Z-]{24,47}$|^$`

2.10 Automatic-Firmware-Update

The LANCOM Auto Updater allows on-site LANCOM devices to be updated automatically without further user intervention (unattended). LANCOM Devices can search for new software updates, and download and install them without any user interaction. You can choose whether to install security updates, release updates, or all updates automatically. If you choose not to use automatic updates, the feature can still be used to check for the availability of new updates.

The LANCOM Auto Updater contacts the LANCOM update server to check for updates and firmware downloads. Communication is based on HTTPS. When contacting the server, the LANCOM device uses previously installed TLS certificates for validation. Furthermore, the firmware files for current LANCOM devices are signed. The LANCOM Auto Updater validates this signature before uploading any firmware.

SNMP ID:

2.107

Console path:

Setup

2.10.1 Mode

Set the operating mode of the LANCOM Auto Updater.

SNMP ID:

2.107.1

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

manual

The Auto Updater only checks for new updates when prompted by the user.

Users can manually use the Auto Updater to initiate the latest available update.

check

The Auto Updater regularly checks the LANCOM update server for new updates. The availability of a new update is signaled to the user in the LCOS LX menu tree and via syslog. Users can manually use the Auto Updater to initiate the latest available update.

check-and-update

The Auto Updater regularly checks the LANCOM update server for new updates. The update server uses the version policy to find the most suitable update, it sets the time to download and install the update within a time frame configured by the user, and it sends the update to the Auto Updater. The firmware is installed in test mode. After installation, the Auto Updater performs a connection check. Here, the device checks whether a connection can be established to the update server to ensure that Internet access is still available. If the update server is contacted successfully, the test mode terminates and the firmware goes into regular operation. If the update server cannot be contacted, then Internet access is assumed to be impossible and the second (i.e. the previously active) firmware will be started again.

Default:

check-and-update

2.10.2 Check-Firmware-Now

This command triggers the device to check the LANCOM update server for new firmware.

SNMP ID:

2.107.2

Console path:

Setup > **Automatic-Firmware-Update**

2.10.3 Update-Firmware-Now

This command triggers the device to download and install the latest firmware from the LANCOM update server.

SNMP ID:

2.107.3

Console path:

Setup > **Automatic-Firmware-Update**

2.10.4 Cancel-Current-Action

This command triggers the device to abort any current actions by the Auto Updater. This applies to manually started and scheduled actions.

SNMP ID:

2.107.4

Console path:

Setup > **Automatic-Firmware-Update**

2.10.5 Reset-Updater-Config

This command resets the boot-persistent configuration files that are created by the Auto Updater. This includes the local blacklist of firmware versions that failed an automatic update.

SNMP ID:

2.107.5

Console path:

Setup > **Automatic-Firmware-Update**

2.10.6 Base-URL

Specifies the URL of the server that provides the latest firmware versions.

SNMP ID:

2.107.6

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

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

Default:

https://update.lancom-systems.de

2.10.7 Check-Interval

After booting, the Auto Updater sets a random time period within a day or a week for the check to be performed. The update itself is performed in the next time period between 02:00 - 04:00 (default).

SNMP ID:

2.107.7

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

daily
weekly

Default:

daily

2.10.8 Version-Policy

Set the version policy of the LANCOM Auto Updater. This controls which firmware versions are offered to update a device.

SNMP ID:

2.107.8

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

latest

Always the newest version, irrespective of the release version. Example: 4.00 Rel is installed; an update to 4.00 RU1 is performed, but also to 5.00 Rel. Updates always go to the latest version, but not back to a previous release.

current

The latest RU/SU/PR within a release. Example: 4.00 Rel is installed; an update to 4.00 RU1 is performed, but not to 5.00 Rel.

security-updates-only

The latest SU within a release. Example: 4.00 Rel is installed; an update to 4.00 SU1 is performed, but not to 4.00 RU2.

latest-without-REL

The newest RU/SU/PR, irrespective of the release version. Updates are only performed if a RU is available. Example: Any version of 4.00 is installed; an update to 5.00 RU1 is performed, but not to 5.00 REL.

Default:

security-updates-only

2.10.9 Check-Time-Begin

The hour of the day at the start of the time interval when checks are made to see whether a firmware update is available and, if applicable, downloaded. The start and end are 0 by default, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

SNMP ID:

2.107.10

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

0

2.10.10 Check-Time-End

The hour of the day at the end of the time interval when checks are made to see whether a firmware update is available and, if applicable, downloaded. The start and end are 0 by default, so checks for updates and downloads can be started at any time of day. The Auto Updater schedules a random time for update checks and downloads within the configured time frame.

SNMP ID:

2.107.11

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

0

2.10.11 Install-Time-Begin

The hour of the day at the start of the time interval during which a firmware update is installed. The default is between 2 and 4 o'clock in the morning. After installation, the device reboots.

SNMP ID:

2.107.12

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

2

2.10.12 Install-Time-End

The hour of the day at the end of the time interval during which a firmware update is installed. The default is between 2 and 4 o'clock in the morning. After installation, the device reboots.

SNMP ID:

2.107.13

Console path:

Setup > **Automatic-Firmware-Update**

Possible values:

0 … 23

Default:

4

3 Other

This menu contains additional functions from the LCOS LX menu tree.

SNMP ID:

4

Console path:

/

3.1 Reset-Config

This action allows you to reset the configuration.

Example: `do Reset-Config`

SNMP ID:

4.1

Console path:

Other

3.2 Reboot

This action is used to restart the device.

Example: `do Reboot`

SNMP ID:

4.2

Console path:

Other