SECURE. **NETWORKS.**

LCOS LX 4.00

Reference Manual

05/2019

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 Introduction

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

This 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 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 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 Validity

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

2 Operation

2.1 Configuration software

There is no end of different situations in which configurations have to be carried out, or ways in which operators prefer to work. This is why the device offers a wide range of ways to set up the configuration:

- **LANconfig** – the menu-driven, clearly structured and easy way to set almost all parameters for a device. LANconfig requires a configuration PC with a current Windows operating system. Refer to the chapters *LANconfig – configuring devices* on page 7 and *Configuring features with LANconfig* on page 12 for further information.
- **WEBconfig** – further information can be found in the chapters *WEBconfig – monitoring and configuring devices* on page 8 and *Configuring features with WEBconfig* on page 27.
- **CLI** – as an alternative to LANconfig, you can also use SSH to open a terminal session on the device and access the command-line interface. TCP port 22 provides access to the device via SSH programs such as PuTTY.
- **LANCOM Management Cloud** – the hyper-integrated solution for automated control of your network.

The default credentials for all configuration paths are:

- User: root
- Password: <Empty> (no password is set)

In the interests of security, you will be prompted to change the password when you access the configuration for the first time.

Please note that all methods access the same configuration data.

2.1.1 LANconfig – configuring devices

From the easy commissioning of a single workplace device with convenient Installation Wizards to the overall management of large scale installations—the spectrum of applications for LANconfig is wide:

Basic functions

- Automatic detection of new, unconfigured devices
- (Remote) configuration of devices via IP address, URL, or via the serial interface
- Integration of Telnet, SSH, HTTPS and TFTP configuration
- Context-based help on the configuration parameters
- The Wizards provide customized input masks at every stage of installation
- Backup connection setup

Management of large installations

- Grouping
- Central firmware distribution
- Simultaneous configuration of multiple devices

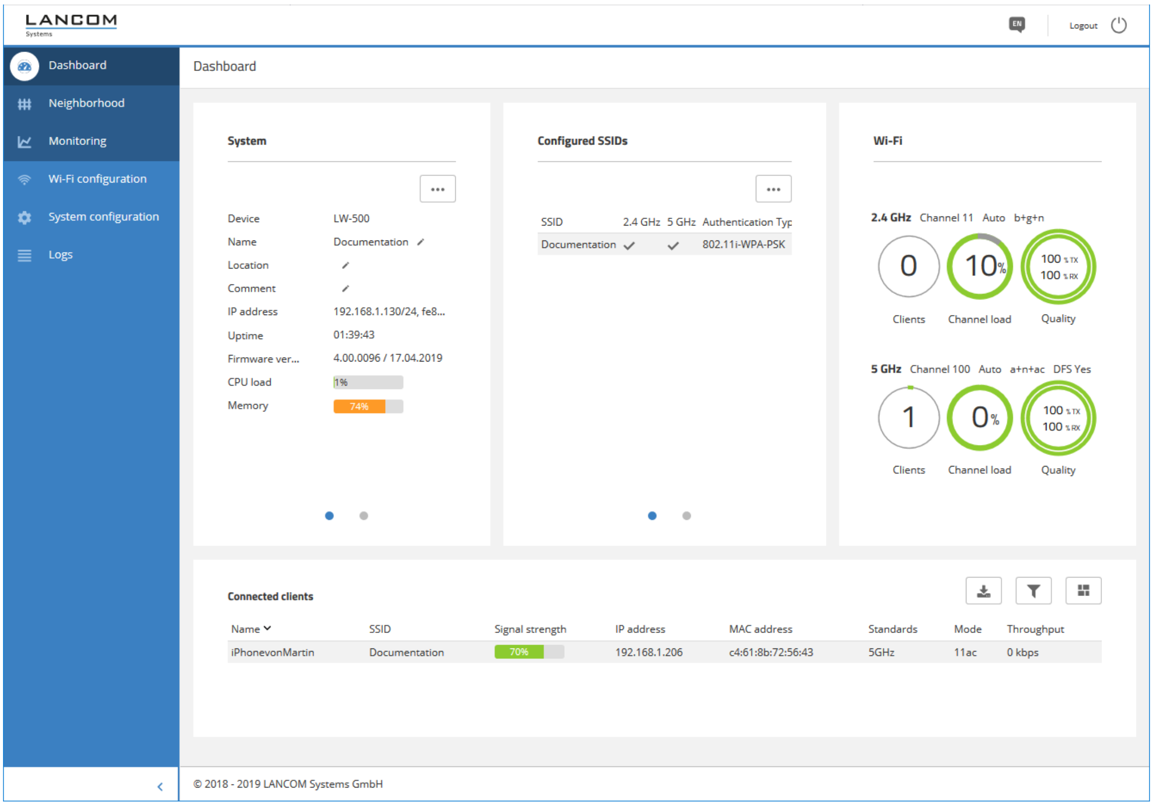
- Configuration script distribution
- WLAN group configuration
- Logging of all actions
- Creation of new "offline" configurations for all devices, for LCOS, and for versions of LCOS LX

2.1.2 WEBconfig – monitoring and configuring devices

Using WEBconfig, you can configure individual devices or monitor them during operation. WEBconfig is reached via HTTP and HTTPS. If you use HTTP, the device automatically redirects you to an encrypted HTTPS connection.

> WEBconfig uses a self-signed SSL certificate, so this must be added as an exception in the browser for each device.

The following provides an overview of the main components of WEBconfig, which are located in the left-hand section in the **sidebar**.



System

Device	LW-500
Name	Documentation
Location	
Comment	
IP address	192.168.1.130/24, fe8...
Uptime	01:39:43
Firmware ver...	4.00.0096 / 17.04.2019
CPU load	1%
Memory	74%

Configured SSIDs

SSID	2.4 GHz	5 GHz	Authentication Typ
Documentation	✓	✓	802.11i-WPA-PSK

Wi-Fi

2.4 GHz Channel 11 Auto b+g+n

Clients	Channel load	Quality
0	10%	100 % TX 100 % RX

5 GHz Channel 100 Auto a+n+ac DFS Yes

Clients	Channel load	Quality
1	0%	100 % TX 100 % RX

Connected clients

Name	SSID	Signal strength	IP address	MAC address	Standards	Mode	Throughput
iPhonevonMartin	Documentation	70%	192.168.1.206	c4:61:8b:72:56:43	5GHz	11ac	0 kbps

© 2018 - 2019 LANCOM Systems GmbH

Dashboard

The Dashboard displays status information of the device during operation.

- System – basic information about the device, e.g. the device name and the firmware version.
- WLAN – information about the load on the WLAN channels operated by the device.
- Connected stations – shows all WLAN stations currently connected to the device.
- Neighborhood – overview of the WLAN environment, especially the WLAN access points and WLAN routers that are locally active.
- Monitoring – graphical representation of the WLAN throughput, LAN throughput, number of WLAN stations and channel load over time.

Configuration

- System configuration – configuration of basic parameters of your device, such as the device name or the IP settings for managing the device.
- WLAN – the WLAN configuration is designed to assist the user with the most common settings and to eliminate the hassle of configuring minor details. It remains possible to configure different scenarios.

Logs

This area outputs the device SYSLOG.

2.1.3 Command-line interface – command summary

The command-line interface is operated with the following commands. An overview of the available configuration parameters and actions is available in the LCOS LX Menu Reference Guide.

ⓘ 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.
`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.
`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.
`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. For further information on this command refer to the section *Diagnosis* on page 42.

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.

3 Configuring features with LANconfig

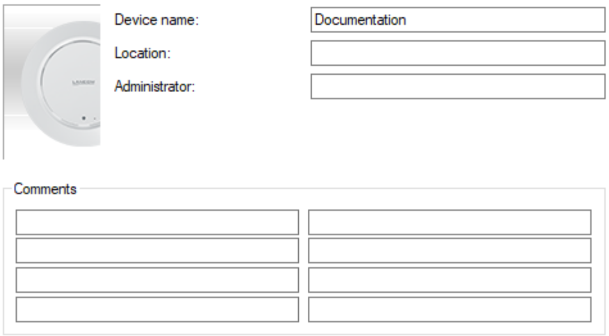
The following explains all of the options for adjusting settings with LANconfig. These depend on the device, so not all of the listed options are available with every device.

3.1 Management

The **Management** section contains general settings for the device.

3.1.1 General

The device settings described here are to be found under **Management** > **General**.



Device name: Documentation

Location:

Administrator:

Comments

Name

Configure the device name here.

Location

Configure the device location here.

Administrator

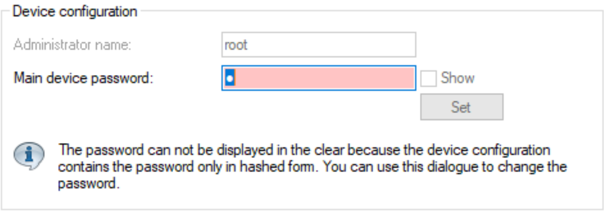
Here you configure the name of the device administrator.

Comments

Use the comment fields to enter any comments about the device configuration.

3.1.2 Admin

The settings for changing the main device password can be found under **Management** > **Admin**.



Device configuration

Administrator name: root

Main device password:

□ Show

Set

The password can not be displayed in the clear because the device configuration contains the password only in hashed form. You can use this dialogue to change the password.

Administrator name

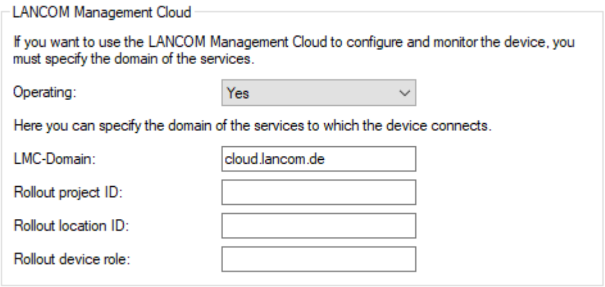
Here you configure the login name of the device administrator. Depending on the device, this name may be fixed and will only be displayed here.

Main device password

Configure the main device password here. Depending on the device, this may be stored as a hash value and consequently cannot be displayed as plain text.

3.1.3 LMC

Settings that relate to the configuration and monitoring of your device via the LANCOM Management Cloud (LMC) are located under **Management** > **LMC**.



LANCOM Management Cloud

If you want to use the LANCOM Management Cloud to configure and monitor the device, you must specify the domain of the services.

Operating: Yes

Here you can specify the domain of the services to which the device connects.

LMC-Domain: cloud.lancom.de

Rollout project ID:

Rollout location ID:

Rollout device role:

Operation

Specify whether the device should be managed via the LMC.

No

The device does not connect to the LMC.

Yes

The LMC manages the device.

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.

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.

Rollout location ID

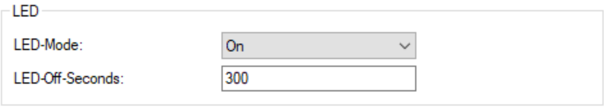
Enter the location of this device in the LMC. The first time the device connects to the LMC, it will be assigned accordingly.

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.

3.1.4 Extended

The settings for the LED functions are located here. These are located under **Management** > **Extended**.



LED

LED-Mode: On

LED-Off-Seconds: 300

LED-Mode

Choose between the different LED modes.

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 are switched off after the configured time.

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

LED off seconds

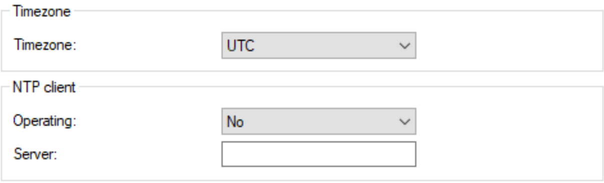
Set a time in seconds after the device starts, after which the LED(s) of the device are switched off if the **LED mode** is set to Timed-Off.

3.2 Date/Time

The section **Date/Time** contains the corresponding device settings.

3.2.1 Configuration

The device settings date and time are to be found under **Date/Time** > **Configuration**.



Timezone

Timezone: UTC

NTP client

Operating: No

Server:

Time zone

Set the correct time zone.

NTP client

Using the Network Time Protocol (NTP), the device can read the current time from a public time server on the Internet (NTP server with an “open access” policy such as the Physikalisch-Technische Bundesanstalt in Germany). LANCOM routers also work as NTP servers, so not every network device needs to access an external NTP server.

Operation

Yes

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

No

Do not use an NTP server.

Server

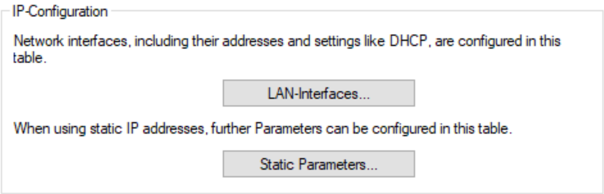
Enter the address of the NTP server.

3.3 IP configuration

The section **IP Configuration** contains the corresponding device configuration.

3.3.1 Configuration

The settings for the IP configuration of your device are located under **IP Configuration** > **Configuration**.



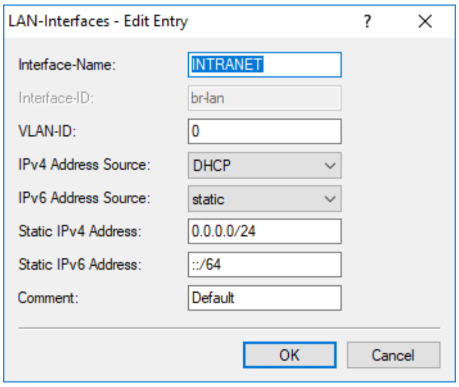
IP-Configuration

Network interfaces, including their addresses and settings like DHCP, are configured in this table.

When using static IP addresses, further Parameters can be configured in this table.

LAN interfaces

Under **IP Configuration** > **Configuration** > **LAN interfaces** you can modify the basic configuration relating to the device's own IP settings and network access.



LAN-Interfaces - Edit Entry

Interface-Name:	INTRANET
Interface-ID:	br-lan
VLAN-ID:	0
IPv4 Address Source:	DHCP
IPv6 Address Source:	static
Static IPv4 Address:	0.0.0.0/24
Static IPv6 Address:	::/64
Comment:	Default

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.

Interface-ID

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

VLAN-ID

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

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:

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.

Static IPv6 address

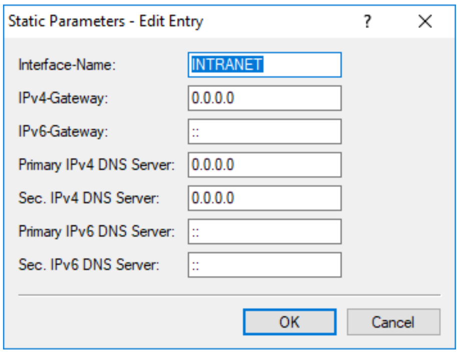
Here you configure the IP address to be used when the IPv6-Address-Source is set to **Static**. Add the subnet mask in CIDR notation (e.g. "/64") as a suffix.

Comment

Here you can enter a comment about the interface configuration.

Static parameters

Other settings related to the IP and network configuration that are required when using static IP addresses are located under **IP Configuration** > **Configuration** > **Static parameters**.


Static Parameters - Edit Entry

Interface-Name: INTRANET

IPv4-Gateway: 0.0.0.0

IPv6-Gateway: ::

Primary IPv4 DNS Server: 0.0.0.0

Sec. IPv4 DNS Server: 0.0.0.0

Primary IPv6 DNS Server: ::

Sec. IPv6 DNS Server: ::

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.

Interface-Name

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

IPv4-Gateway

Here you configure the IPv4 gateway for the referenced interface.

IPv6-Gateway

Here you configure the IPv6 gateway for the referenced interface.

Primary IPv4 DNS server

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

Secondary IPv4 DNS server

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

Primary IPv6 DNS server

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

Secondary IPv6 DNS server

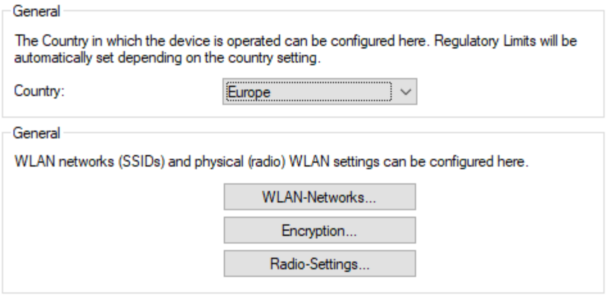
Here you configure the secondary IPv6 DNS gateway for the referenced interface.

3.4 Wireless LAN

In the section **Wireless LAN** you will find all the settings related to the broadcasting of WLAN networks.

3.4.1 WLAN networks

The wireless network settings for your device are located under **Wireless LAN** > **WLAN networks**.



General

The Country in which the device is operated can be configured here. Regulatory Limits will be automatically set depending on the country setting.

Country: Europe

General

WLAN networks (SSIDs) and physical (radio) WLAN settings can be configured here.

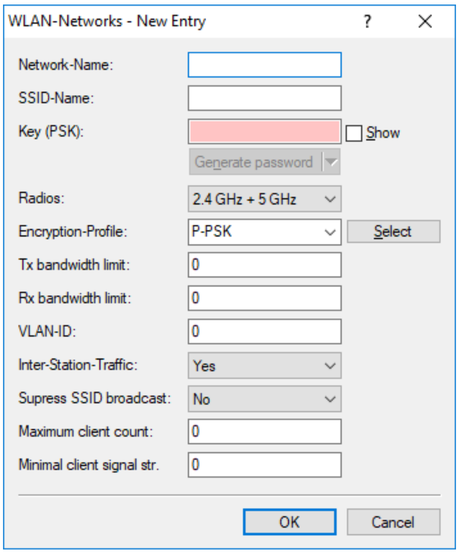
General

Country

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

WLAN networks

General settings relating to the broadcast WLAN networks are configured under **Wireless LAN** > **WLAN networks** > **WLAN networks**. Add a line to the table for each WLAN network. By default, the table is empty.



WLAN-Networks - New Entry

Network-Name:	
SSID-Name:	
Key (PSK):	□ Show
	Generate password
Radios:	2.4 GHz + 5 GHz
Encryption-Profile:	P-PSK
Tx bandwidth limit:	0
Rx bandwidth limit:	0
VLAN-ID:	0
Inter-Station-Traffic:	Yes
Supress SSID broadcast:	No
Maximum client count:	0
Minimal client signal str.	0

Network name

Choose 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. This is configured in the next step.

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.

Key (PSK)

Configure the pre-shared key (PSK) used for the WLAN network here. If you select **Show**, you can use **Generate password** to create a random password. Use the arrow next to it to set the strength, length and various other settings for the characters used for the generated pre-shared key.

ⓘ 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.

Radios

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

2.4 GHz + 5 GHz

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

2.4 GHz

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

5 GHz

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 select an encryption profile that defines the authentication and encryption method used for the SSID.

By default, the following encryption profiles are available for selection:

P-NONE

No encryption, the SSID is open.

P-PSK

The used authentication method is WPA2 with PSK (also known as WPA2-Personal). A key must be configured for the WLAN network.

TX bandwidth limit

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

RX bandwidth limit

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

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.

Direct traffic between stations

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.

Suppress SSID broadcast

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.

Maximum count of clients

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

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).

Minimal client signal 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.

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

Encryption

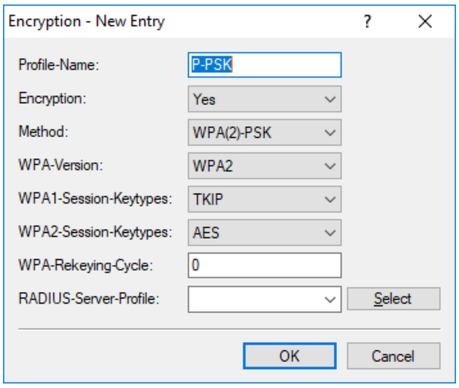
The settings for encryption and authentication on the WLAN networks are configured under **Wireless LAN** > **WLAN networks** > **Encryption**. The following encryption profiles are stored by default and these can be used for the configuration of the WLAN networks.

P-NONE

No encryption, the SSID is open.

P-PSK

The used authentication method is WPA2 with PSK (also known as WPA2-Personal). A key must be configured for the WLAN network.



Encryption - New Entry

Profile-Name:	P-PSK
Encryption:	Yes
Method:	WPA(2)-PSK
WPA-Version:	WPA2
WPA1-Session-Keytypes:	TKIP
WPA2-Session-Keytypes:	AES
WPA-Rekeying-Cycle:	0
RADIUS-Server-Profile:	

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.

Encryption

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

Method

Here you configure the encryption method. The following methods are available:

WPA

- WPA(2)-PSK: WPA(2) with Pre-Shared-Key
- WPA(2)-802.1X: WPA(2) with 802.1X

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

WEP

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.

- WEP-40-Bits: WEP with 40-bits key length
- WEP-104-Bits: WEP with 104-bits key length
- WEP-128-Bits: WEP with 128-bits key length
- WEP-40-Bits-802.1X: WEP 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: WEP 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: WEP with 128-bits key length and 802.1X

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

WPA-Version

Here you configure the WPA version used for the encryption methods WPA(2)-PSK and WPA(2)-802.1X. The following versions are available:

- WPA1: WPA version 1 is used exclusively.
- WPA2: WPA version 2 is used exclusively.
- WPA1/2: Whether the encryption method WPA 1 or 2 is used depends on the capabilities of the client.

We exclusively recommend the use of WPA2.

WPA1-Session-Keytypes

Here you configure the session key type to be used for WPA version 1. This also influences the encryption method used. The following types are available:

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.

ⓘ Employing TKIP is only recommended for operating 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.

WPA2-Session-Keytypes

Here you configure the session key type to be used for WPA version 2. This also influences the encryption method used. The following types are available:

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.

ⓘ Employing TKIP is only recommended for operating 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.

WPA-Rekeying-Cycle

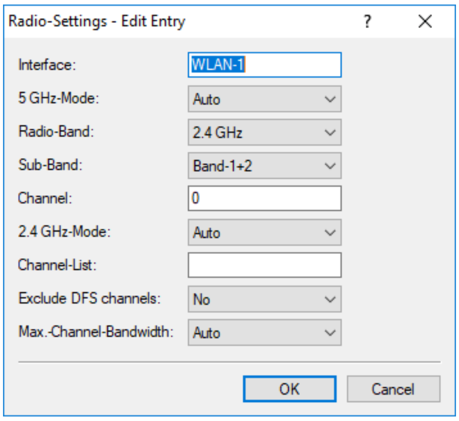
Here you configure the time in seconds after which the access point performs rekeying when operating WPA(2). The value "0" means that no rekeying is performed.

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. The profiles are created under *RADIUS* on page 25.

Radio settings

Settings relating to the physical radio parameters are configured under **Wireless LAN** > **WLAN networks** > **Radio settings**. By default, there is an entry in the table for every physical WLAN radio for modification as required.



Radio-Settings - Edit Entry

Interface:	WLAN-1
5 GHz-Mode:	Auto
Radio-Band:	2.4 GHz
Sub-Band:	Band-1+2
Channel:	0
2.4 GHz-Mode:	Auto
Channel-List:	
Exclude DFS channels:	No
Max.-Channel-Bandwidth:	Auto

Interface

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

5-GHz 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:

Auto

All modes supported by the device are used.

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.

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

Radio band

Here you configure whether this interface operates in the 2.4-GHz or 5-GHz frequency range.

Sub-Band

Here you configure which sub-bands are used in the 5-GHz mode. The following sub-bands are available:

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

Both sub-band 1 and sub-band 2 are used.

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

Channel

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

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

ⓘ 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.

2.4-GHz 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. The following modes are available:

Auto

All modes supported by the device are used.

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.

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

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.

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**.

Max. channel bandwidth

Here you configure the maximum allowed channel bandwidth. The following settings are available:

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 80 MHz) is always used, depending on the environment.

20 MHz

The channel bandwidth is always 20 MHz.

40 MHz

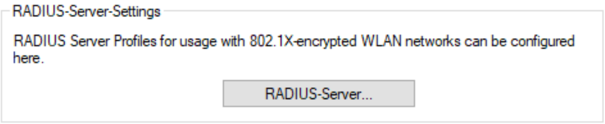
Depending on the environment, channel bandwidth is up to 40 MHz, but this can also fall back to 20 MHz.

80 MHz

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

3.4.2 RADIUS

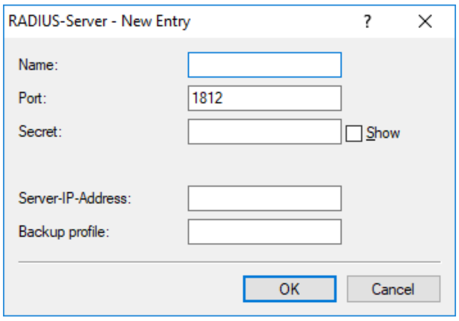
The settings for RADIUS server profiles when operating WLAN networks that use 802.1X as the authentication method can be found under **Wireless LAN** > **RADIUS**.



RADIUS-Server-Settings

RADIUS Server Profiles for usage with 802.1X-encrypted WLAN networks can be configured here.

Configure the RADIUS server profiles in the **RADIUS server** table.



RADIUS-Server - New Entry

Name:

Port: 1812

Secret: □ Show

Server-IP-Address:

Backup profile:

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.

Port

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

> ⓘ This is usually the port 1812 (RADIUS authentication).

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.

Server IP address

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

Backup profile

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

4 Configuring features with WEBconfig

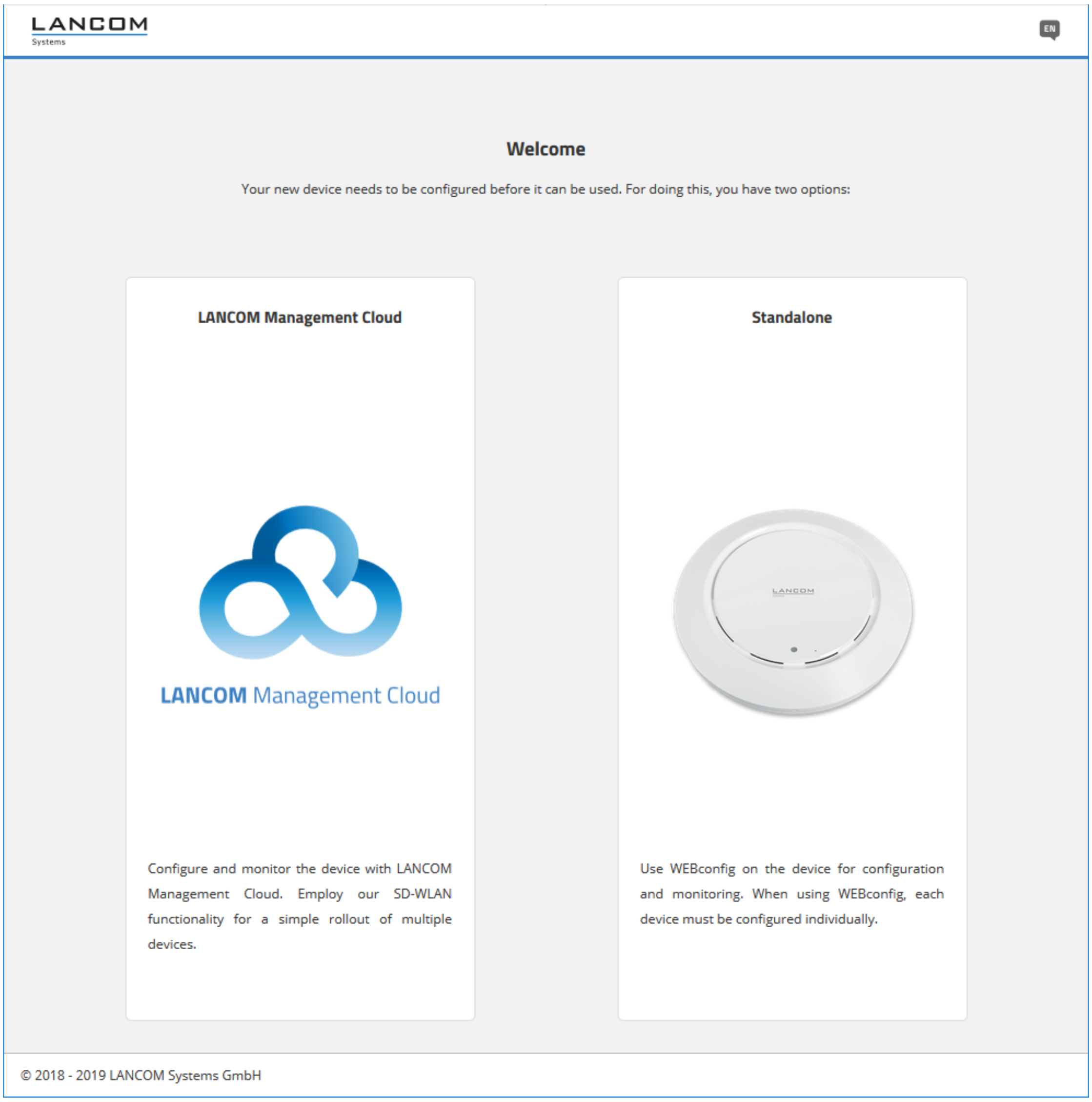
The following section explains how devices are installed with WEBconfig and the various settings that WEBconfig has to offer. These depend on the device, so not all of the listed options are available with every device.

4.1 Commissioning of a device via WEBconfig

WEBconfig is reached via HTTP and HTTPS. If you use HTTP, the device automatically redirects you to an encrypted HTTPS connection.

! WEBconfig uses a self-signed SSL certificate, so this must be added as an exception in the browser for each device.

After invoking the WEBconfig interface of an unconfigured device, you can select whether the device should be managed by the LANCOM Management Cloud or as a stand-alone device.



Welcome

Your new device needs to be configured before it can be used. For doing this, you have two options:

LANCOM Management Cloud

Configure and monitor the device with LANCOM Management Cloud. Employ our SD-WLAN functionality for a simple rollout of multiple devices.

Standalone

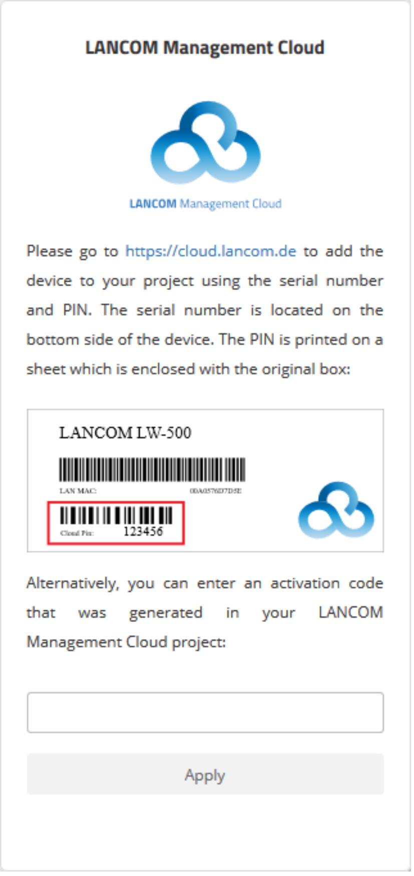
Use WEBconfig on the device for configuration and monitoring. When using WEBconfig, each device must be configured individually.

© 2018 - 2019 LANCOM Systems GmbH

Click the corresponding button here to decide whether the device should be managed by the LANCOM Management Cloud or as a stand-alone device.

4.1.1 Management by LANCOM Management Cloud

You either connect the device to the LANCOM Management Cloud by means of the serial number and PIN (zero touch), or you use the corresponding input field to enter an activation code that you generated previously in your LANCOM Management Cloud project:



LANCOM Management Cloud

Please go to https://cloud.lancom.de to add the device to your project using the serial number and PIN. The serial number is located on the bottom side of the device. The PIN is printed on a sheet which is enclosed with the original box:

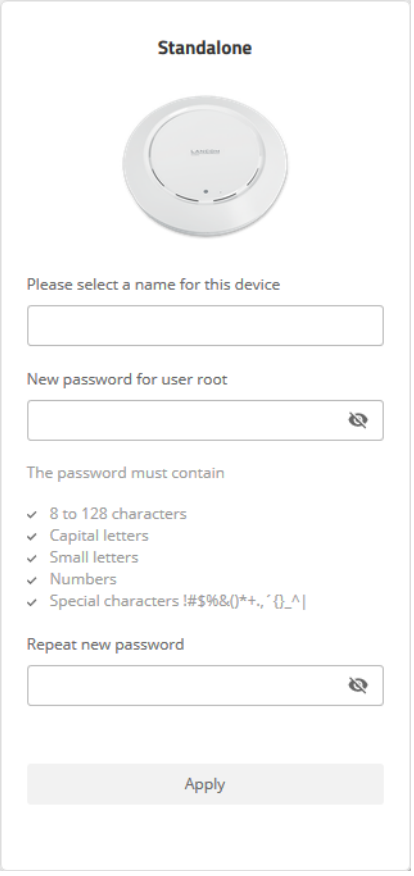
Alternatively, you can enter an activation code that was generated in your LANCOM Management Cloud project:

After confirming the activation code and completing the pairing process, a success message will be displayed and you will be redirected to the WEBconfig login page. The device can now be managed via the LMC.

4.1.2 Stand-alone management

Use the corresponding input fields to set a meaningful name for your device and set a password to be used by the user “root”.

The password set here is valid for the user “root”. This user is also used subsequently to login to WEBconfig.



Standalone

Please select a name for this device

New password for user root

The password must contain

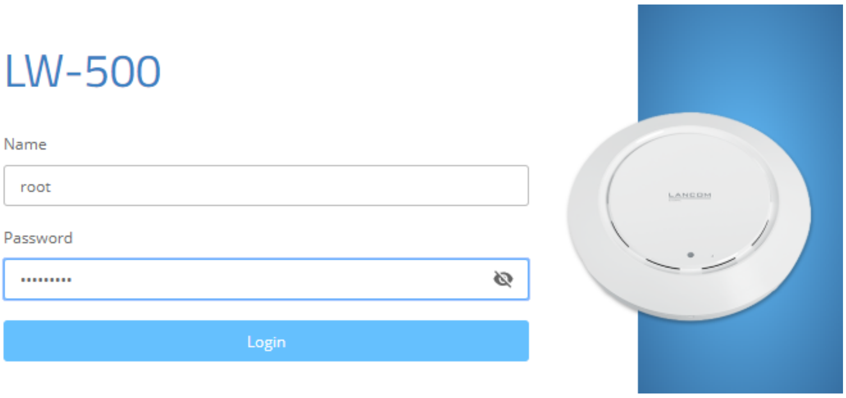
- ✓ 8 to 128 characters
- ✓ Capital letters
- ✓ Small letters
- ✓ Numbers
- ✓ Special characters !#$%&()*+.,´{}_^|

Repeat new password

Clicking on **Apply** will direct you to the login page. Use the username “root” and the previously defined password to login to WEBconfig.

4.2 Login

Login by entering the user name “root” and the password you set earlier:



LW-500

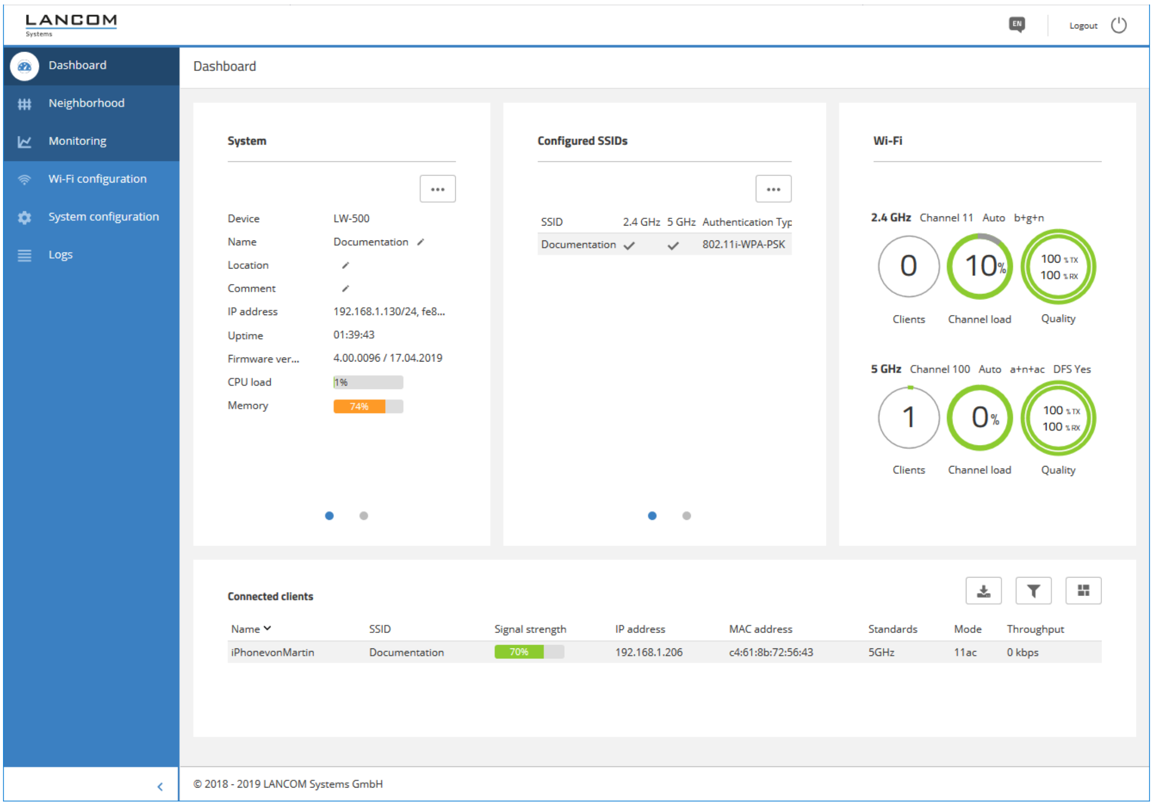
Name: root

Password: •••••••••

After logging in to WEBconfig you will be taken to the dashboard. Refer to section *WEBconfig – Dashboard* on page 31 for information on the dashboard.

4.3 WEBconfig – Dashboard

The dashboard provides an overview of the essential operating data for your device.



System

Device	LW-500
Name	Documentation
Location	
Comment	
IP address	192.168.1.130/24, fe8...
Uptime	01:39:43
Firmware ver...	4.00.0096 / 17.04.2019
CPU load	1%
Memory	74%

Configured SSIDs

SSID	2.4 GHz	5 GHz	Authentication Typ
Documentation	✓	✓	802.11i-WPA-PSK

Wi-Fi

2.4 GHz Channel 11 Auto b+g+n

Clients	Channel load	Quality
0	10%	100 % TX 100 % RX

5 GHz Channel 100 Auto a+n+ac DFS Yes

Clients	Channel load	Quality
1	0%	100 % TX 100 % RX

Connected clients

Name	SSID	Signal strength	IP address	MAC address	Standards	Mode	Throughput
iPhonevonMartin	Documentation	70%	192.168.1.206	c4:61:8b:72:56:43	5GHz	11ac	0 kbps

© 2018 - 2019 LANCOM Systems GmbH

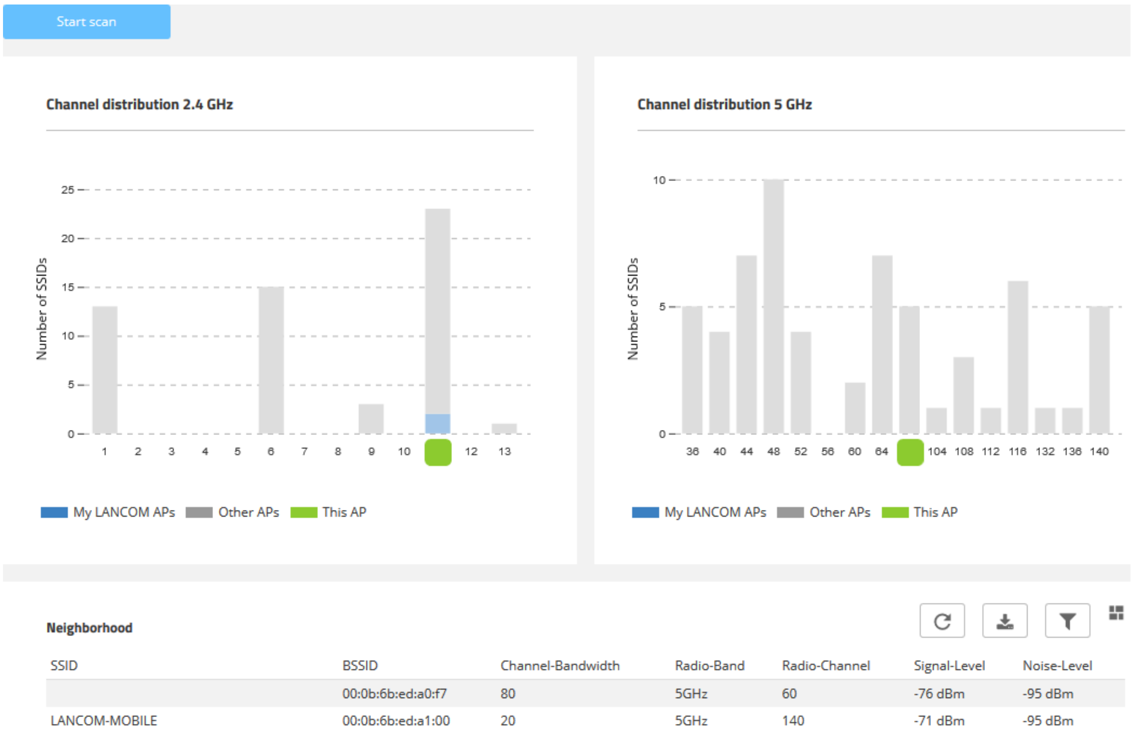
Below the dashboard are the areas **Neighborhood** and **Monitoring**.

4.3.1 Neighborhood

You reach the Neighborhood area by means of the **Neighborhood** item in the sidebar.

The Neighborhood view provides an overview of the WLAN environment, especially the WLAN access points and WLAN routers that are locally active.

Click the button **Start scan** to discover the WLAN environment. After the scan is completed (duration: approx. 10 seconds), the results are shown in various diagrams and tables:



Neighborhood

SSID	BSSID	Channel-Bandwidth	Radio-Band	Radio-Channel	Signal-Level	Noise-Level
	00:0b:6b:ed:a0:f7	80	5GHz	60	-76 dBm	-95 dBm
LANCOM-MOBILE	00:0b:6b:ed:a1:00	20	5GHz	140	-71 dBm	-95 dBm

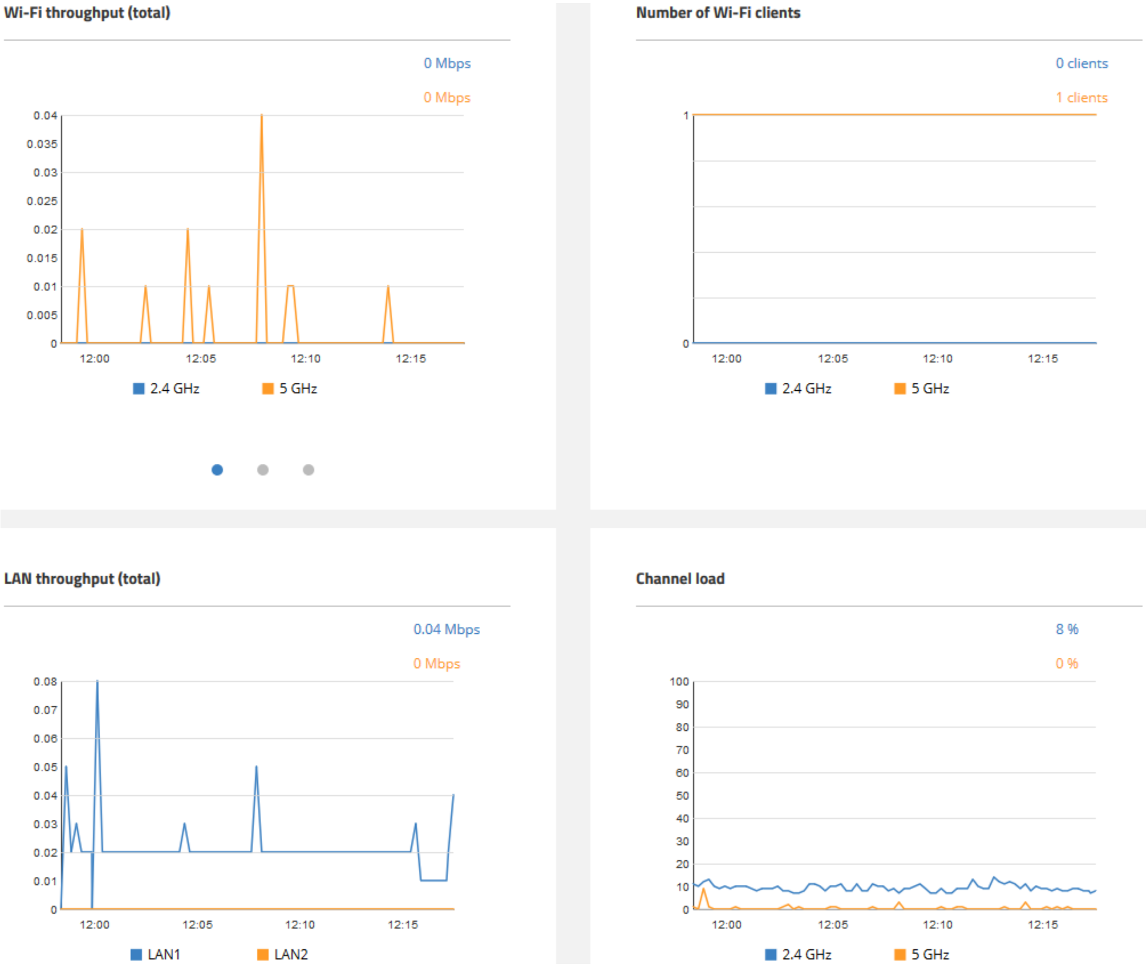
The top two bar charts visualize the number of SSIDs detected by the device on the various 2.4-GHz and 5-GHz channels, which can indicate the potential load on the channels. LANCOM access points detected by the scan and reachable on the same LAN as the current device are highlighted as “My LANCOM APs”. The WLAN channel that the current device itself is working on is also indicated. The **Neighborhood** table also provides details about the SSIDs detected by the scan, such as the name, the BSSID (MAC address), and the signal strength.

4.3.2 Monitoring

You reach the Monitoring area by means of the **Monitoring** item in the sidebar.

The Monitoring view is offers a graphical representation of the WLAN throughput, LAN throughput, number of WLAN stations and channel load over time.

The maximum amount of historical data available corresponds to the duration of the current WEBconfig session.



4.4 Wi-Fi configuration

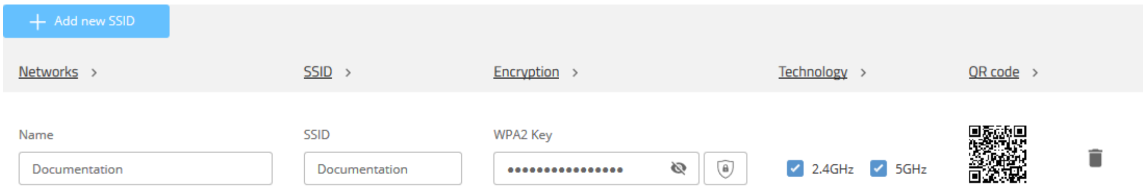
You reach this area by means of the **Wi-Fi configuration** item in the sidebar.

4.4.1 Concept

The Wi-Fi configuration is designed to assist the user with the most common settings and to eliminate the hassle of configuring minor details. It remains possible to configure different scenarios.

4.4.2 Operation

The available SSIDs are displayed in tabular form. Click on the **Add new SSID** button to configure a new SSID. A new line is added. To configure an SSID with WPA2-PSK, all you have to do is fill out the fields **Name**, **SSID** and **WPA2 key**.



+ Add new SSID

Networks ›	SSID ›	Encryption ›	Technology ›	QR code ›
Name Documentation	SSID Documentation	WPA2 Key ••••••••••••••••	☑ 2.4GHz ☑ 5GHz	

Depending on your needs, you can generate a secure WPA2 key automatically (🛡) and limit the frequency bands available for selection. By default, the SSID is broadcast on 2.4 GHz and 5 GHz.

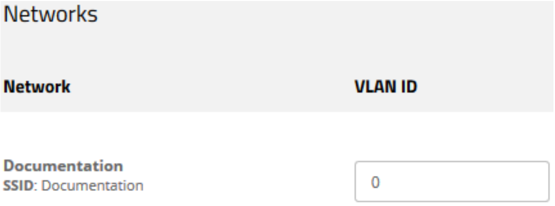
Then click on **Save** to accept your SSID. This will then be broadcast immediately by the device.

> On the 5-GHz band, it may take up to a minute after the initial configuration to broadcast the SSID. This is due to a regulatory requirement to monitor the band for primary users ("radar detection" for one minute, i.e. DFS).

> Further individual configuration is possible by clicking on the respective heading.

Networks

Here you can set the parameters for each SSID as follows:



Networks

Network	VLAN ID
Documentation **SSID**: Documentation	0

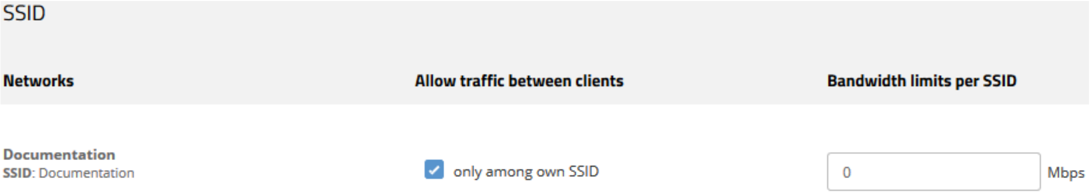
VLAN-ID

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.

SSID

Here you can set the parameters for each SSID as follows:



SSID

Networks	Allow traffic between clients	Bandwidth limits per SSID
Documentation **SSID**: Documentation	☑ only among own SSID	0 Mbps

Allow traffic between clients

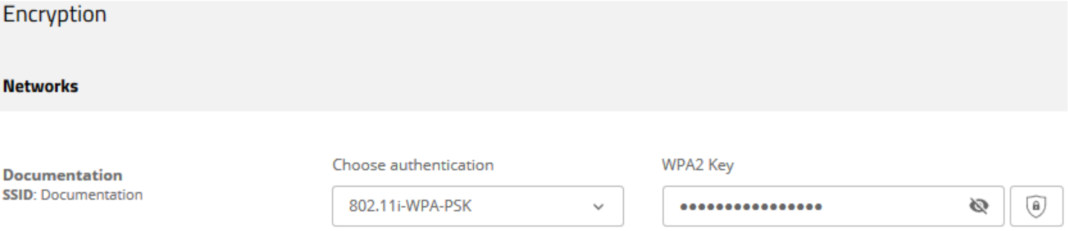
Depending on the application, it may be desirable—or even undesirable—for clients on a WLAN network to communicate with other clients. Here you configure whether communication between the WLAN clients on the WLAN network should be allowed.

Bandwidth limits per SSID

Here you set a WLAN bandwidth limit that applies to the entire WLAN network. All of the logged in clients can only send and receive data with the transmission rate configured here. The value "0" means that no limitation is active.

Encryption

Here you can set the parameters for each SSID as follows:



Encryption

Networks

Documentation
SSID: Documentation

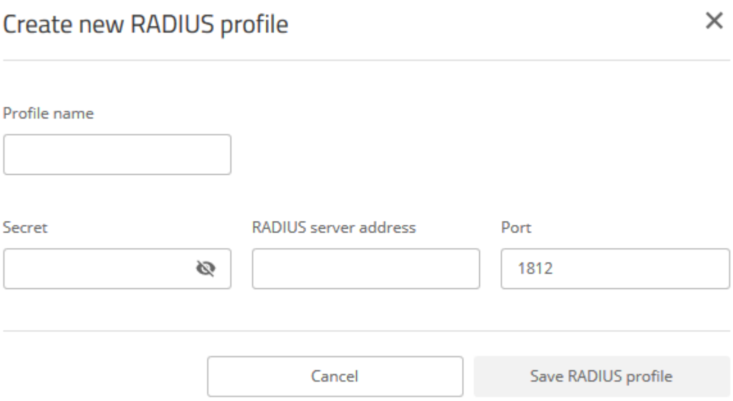
Choose authentication: 802.11i-WPA-PSK

WPA2 Key: ●●●●●●●●●●●●●●●●

Select authentication

Change the encryption and authentication method here. The default setting is WPA2-PSK (**802.11i WPA-PSK**). You can optionally choose **No encryption** or 802.1X (**802.11i WPA-802.1X**).

- In the case of WPA2-PSK you have to enter a **WPA2 key**. You can read the key by clicking on the crossed-out eye symbol. Depending on your needs, you can generate a secure WPA2 key automatically (🛡).
- In the case of 802.1X you have to use **Create new RADIUS profile**:



Create new RADIUS profile

Profile name:

Secret:

RADIUS server address:

Port: 1812

Profile 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.

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.

RADIUS server address

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

Port

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

This is usually the port 1812 (RADIUS authentication).

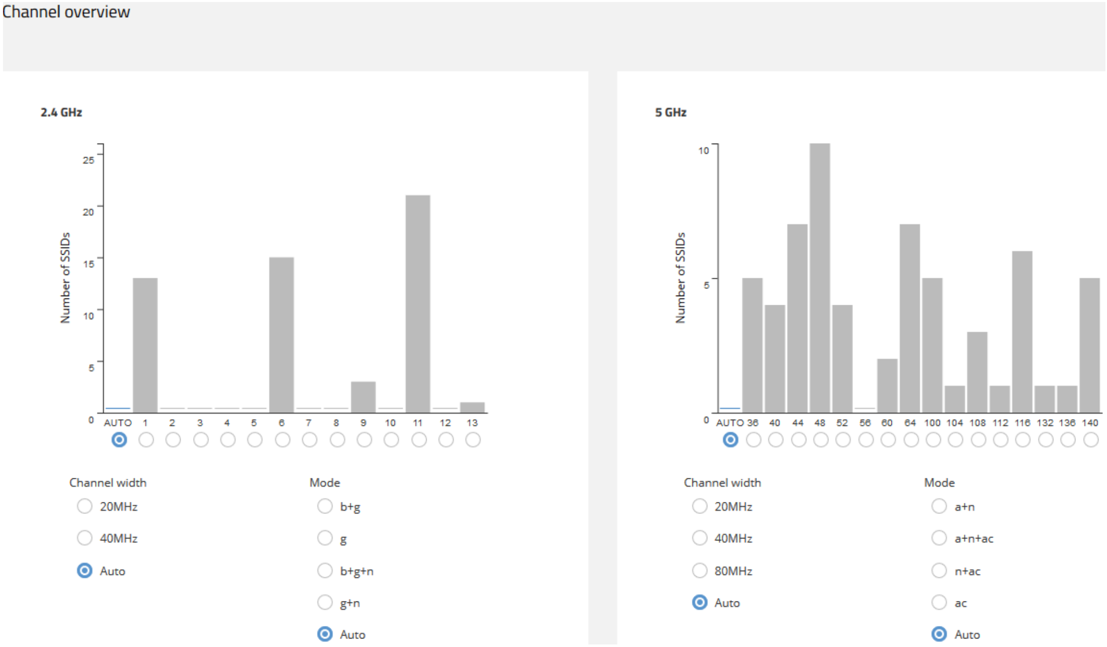
Please note that the RADIUS server generally has to be notified about the RADIUS client by means of an entry in its configuration.

Store your changes by clicking on **Save.**

Technology

The **Technology** page offers the option to set fixed channels for the 2.4- and 5-GHz bands, to specify the available channel width and to determine which radio mode is used. The default setting for all options is automatic selection.

The physical settings that can be configured here apply to the entire frequency band and are not SSID-specific.



Channel overview

2.4 GHz

● AUTO ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○ 11 ○ 12 ○ 13

Channel width
○ 20MHz
○ 40MHz
● Auto

Mode
○ b+g
○ g
○ b+g+n
○ g+n
● Auto

5 GHz

● AUTO ○ 36 ○ 40 ○ 44 ○ 48 ○ 52 ○ 56 ○ 60 ○ 64 ○ 100 ○ 104 ○ 108 ○ 112 ○ 116 ○ 132 ○ 136 ○ 140

Channel width
○ 20MHz
○ 40MHz
○ 80MHz
● Auto

Mode
○ a+n
○ a+n+ac
○ n+ac
○ ac
● Auto

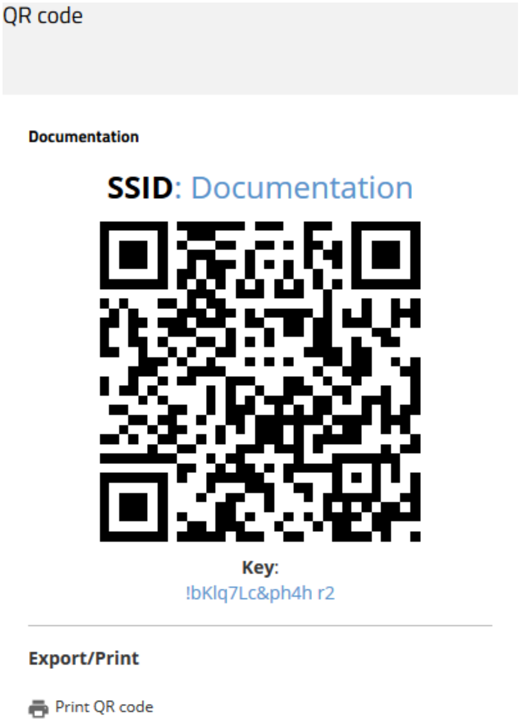
The two bar charts visualize how many SSIDs the device detected on the various 2.4- and 5-GHz channels, which can represent the potential load on the channels.

The bar charts only contain information if a neighborhood scan has been performed under **Neighborhood**.

QR code

This page provides access to a QR code for any open or WPA2-PSK secured SSID. The QR code can be scanned by current smartphones (an additional app may be required) and sets up the respective WLAN automatically on the smartphone. This spares users the laborious entry of a wireless key.

It is also possible to print out individual QR codes separately.



QR code

Documentation

SSID: Documentation

Key:
!bKlq7Lc&ph4h r2

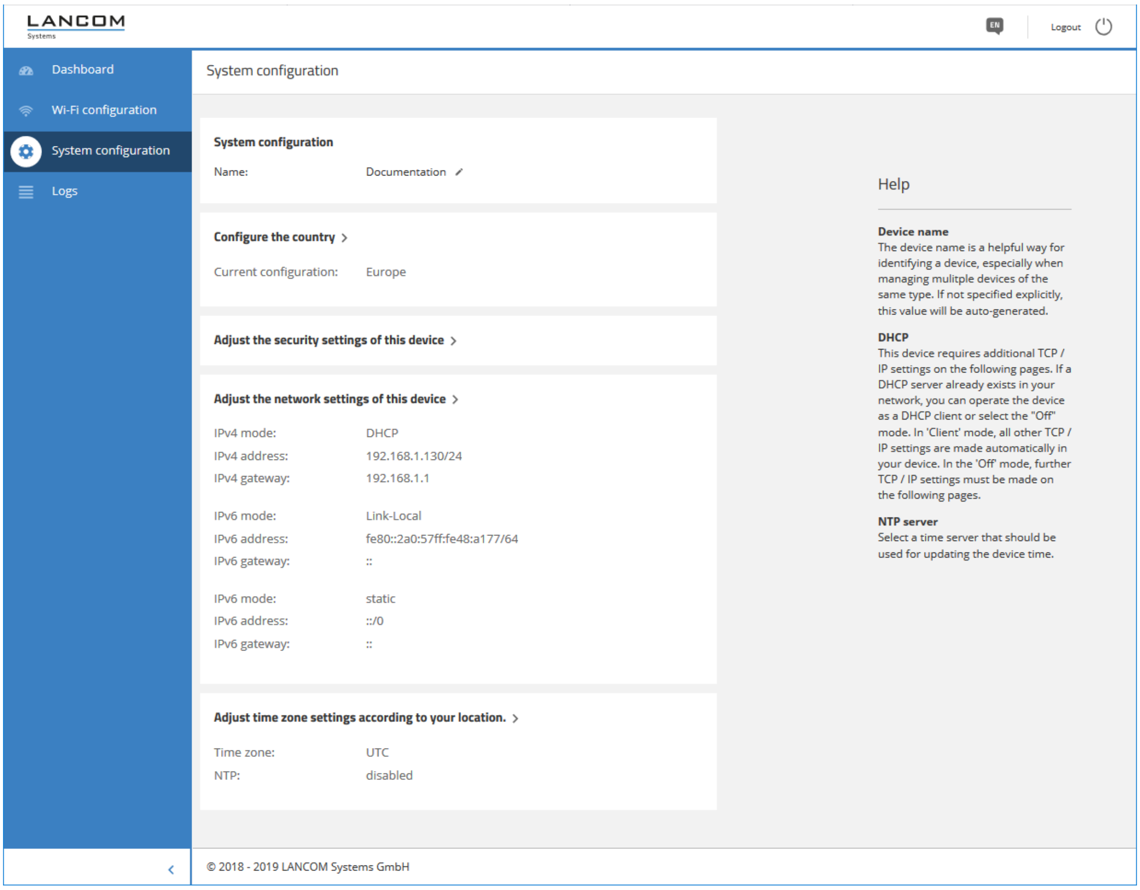
Export/Print

Print QR code

QR codes cannot be used for networks secured by 802.1X as they do not use a static WLAN key (PSK).

4.5 System configuration

This allows you to configure the basic parameters of your device, such as the device name or the IP settings for managing the device.



System configuration

System configuration

Name:	Documentation

Configure the country

Current configuration:	Europe

Adjust the security settings of this device

Adjust the network settings of this device

IPv4 mode:	DHCP
IPv4 address:	192.168.1.130/24
IPv4 gateway:	192.168.1.1
IPv6 mode:	Link-Local
IPv6 address:	fe80::2a0:57ff:fe48:a177/64
IPv6 gateway:	::
IPv6 mode:	static
IPv6 address:	::/0
IPv6 gateway:	::

Adjust time zone settings according to your location.

Time zone:	UTC
NTP:	disabled

Help

Device name
The device name is a helpful way for identifying a device, especially when managing mulitple devices of the same type. If not specified explicitly, this value will be auto-generated.

DHCP
This device requires additional TCP / IP settings on the following pages. If a DHCP server already exists in your network, you can operate the device as a DHCP client or select the "Off" mode. In 'Client' mode, all other TCP / IP settings are made automatically in your device. In the 'Off' mode, further TCP / IP settings must be made on the following pages.

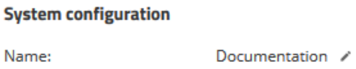
NTP server
Select a time server that should be used for updating the device time.

© 2018 - 2019 LANCOM Systems GmbH

You can edit individual fields such as the system name by clicking on the check mark next to it. An edit mask for the various sections opens after clicking on the headline.

4.5.1 Name

Configure the device name here.

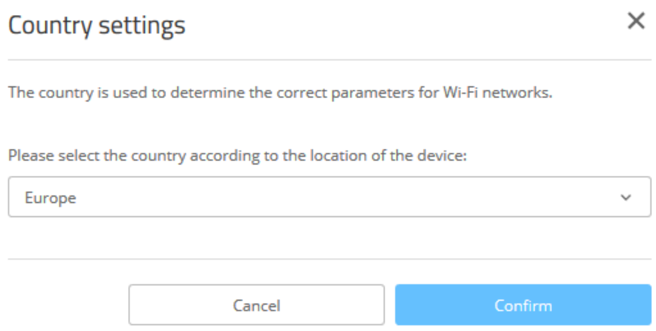


System configuration

Name:	Documentation

4.5.2 Country settings

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



Country settings

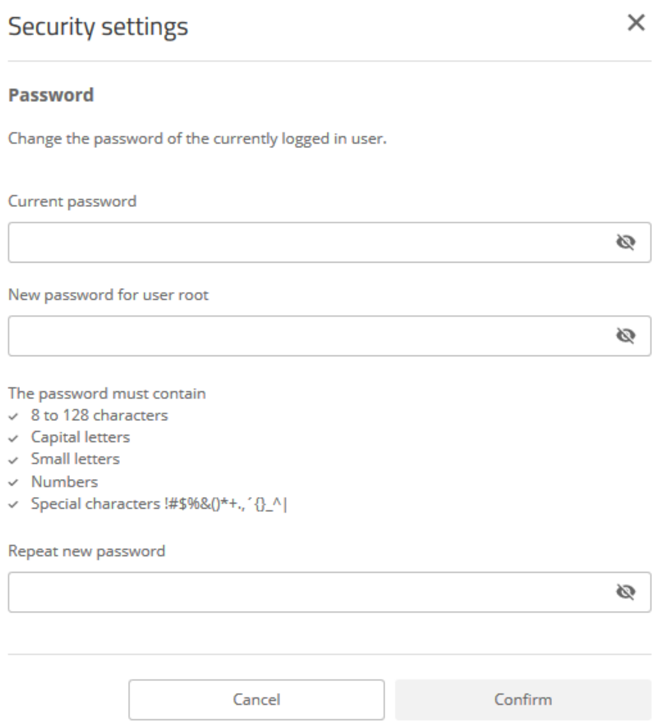
The country is used to determine the correct parameters for Wi-Fi networks.

Please select the country according to the location of the device:

Europe

4.5.3 Security settings

Here you can change the password for the current user (usually “root”).



Security settings

Password

Change the password of the currently logged in user.

Current password

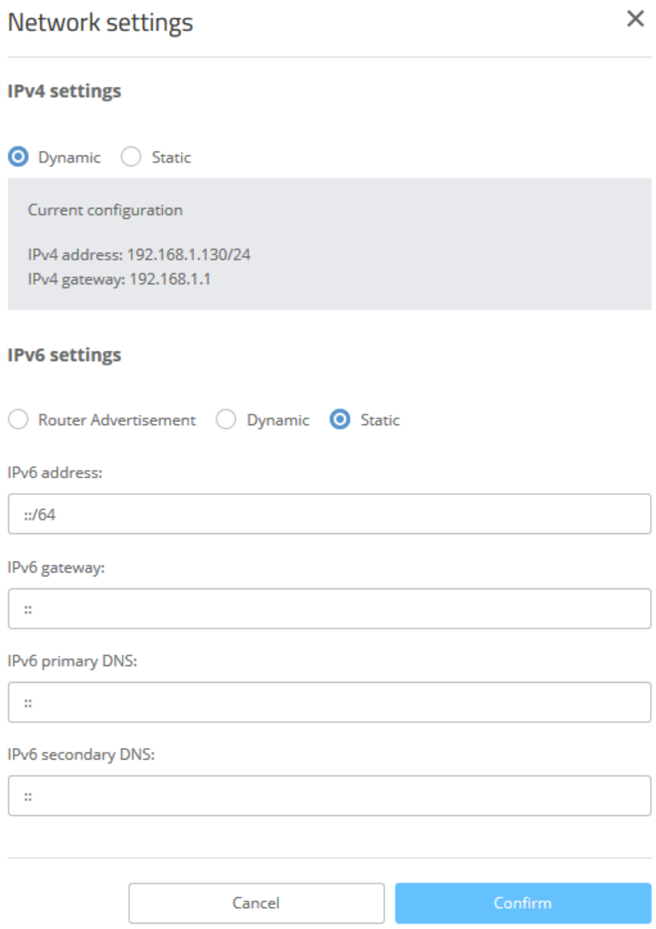
New password for user root

The password must contain
- ✓ 8 to 128 characters
- ✓ Capital letters
- ✓ Small letters
- ✓ Numbers
- ✓ Special characters !#$%&()*+.,´{}_^|

Repeat new password

4.5.4 Network settings

Here you have the option to change network settings of your device, such as its IP address.



Network settings

IPv4 settings

● Dynamic ○ Static

Current configuration

IPv4 address: 192.168.1.130/24
IPv4 gateway: 192.168.1.1

IPv6 settings

○ Router Advertisement ○ Dynamic ● Static

IPv6 address: ::/64

IPv6 gateway: ::

IPv6 primary DNS: ::

IPv6 secondary DNS: ::

IPv4 settings

Dynamic

Uses DHCPv4 to configure the IPv4 parameters. This is the default value.

Static

Uses the IP parameters that you can configure in the fields **IPv4 address**, **IPv4 gateway**, **IPv4 primary DNS** and **IPv4 secondary DNS**.

Note that the IPv4 address must be specified in CIDR notation (for example, 192.168.1.1/24).

IPv6 settings

Router Advertisement

Uses router advertisements/SLAAC to configure the IPv6 parameters. If the received router advertisement contains the M (managed) flag, further parameters are obtained via DHCPv6.

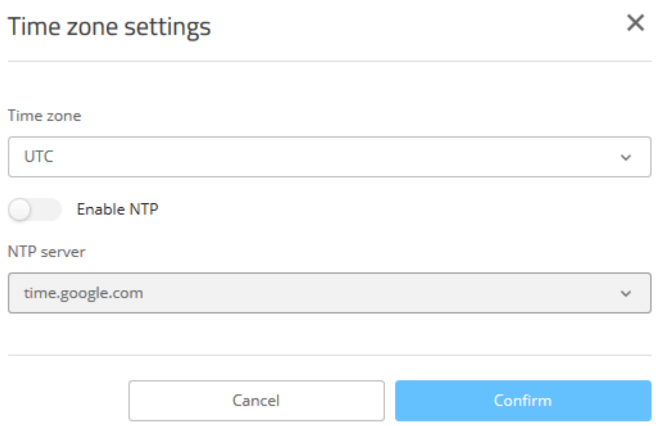
Dynamic

Uses DHCPv6 to configure the IPv6 parameters.

Static

Uses the IP parameters that you can configure in the fields **IPv6 address**, **IPv6 gateway**, **IPv6 primary DNS** and **IPv6 secondary DNS**. This is the default value.

4.5.5 Time zone settings



Time zone settings

Time zone: UTC

Enable NTP

NTP server: time.google.com

Time zone

Select a time zone. The default value is "UTC".

Enable NTP

Here you select whether the time should be obtained from a time server by means of the network time protocol (NTP).

NTP server

From this list you select a time server from which the time is to be obtained via NTP.

5 Diagnosis

5.1 Trace output

Trace output can be used to check the internal processes in the device during or after configuration. Experienced users can read this output and discover any errors in connection establishment. One particular advantage is: The error may be located in the configuration of your own device or in the peer device.

> Trace output has a slight time delay from the actual event, but the order of events is always recorded correctly. This generally does not influence the interpretation of the display, but this should be considered when making precise analyses.

5.1.1 Trace – an overview

Trace output is started in a CLI session. Set up an SSH session to the device. Call the trace with the following syntax:

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

The command trace, the key and the parameters are each separated by a space. The keys control the trace while the parameter determines the actual output.

Table 2: Overview of keys

Key	Meaning
`--log`	Output of "historical" Information from the log
?	displays help
+	switches trace output on
-	switches trace output off
#	Toggles ""between the different trace outputs
no key	displays the current status of trace

Table 3: Overview of parameters

Parameter	Meaning	`--log`
WLAN	WLAN-related outputs, such as client log ins and log offs, key negotiation, ... If the trace is not enabled, the log file will contain only a small amount of information and the "historical" output will not be particularly informative.	Yes
IAPP	Output on IAPP (inter access point protocol)	Yes
Kernel	Output on the basic system and kernel.	Yes
SSH	Output on the SSH service.	Yes
*	Wildcard, which stands for all services.	Depends on the service

5.1.2 Trace – operation

The following examples illustrate the functions of trace:

- Start one or more traces:

  ```
  trace + ssh kernel
  ```

- Stop traces:

  ```
  trace - ssh kernel
  ```

- Stop all traces:

  ```
  trace - *
  ```

- Toggle between “”switching the traces on and off:

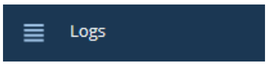
  ```
  trace # ssh kernel
  ```

- Output “historical” information, if supported and available in the log:

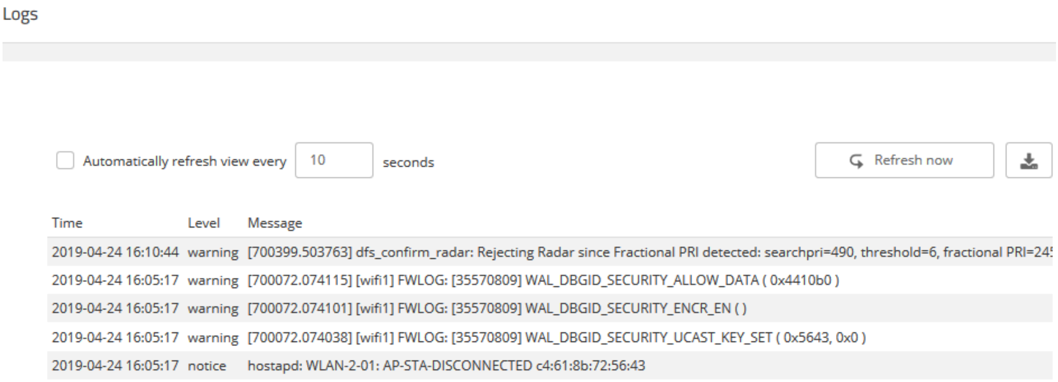
  ```
  trace --log + kernel
  ```

5.2 Logs in WEBconfig

You reach the “Logs” area by means of the **Logs** item in the sidebar.



This area outputs the device SYSLOG.



□ Automatically refresh view every 10 seconds

Time	Level	Message
2019-04-24 16:10:44	warning	[700399.503763] dfs_confirm_radar: Rejecting Radar since Fractional PRI detected: searchpri=490, threshold=6, fractional PRI=24
2019-04-24 16:05:17	warning	[700072.074115] [wifi1] FWLOG: [35570809] WAL_DBGID_SECURITY_ALLOW_DATA (0x4410b0)
2019-04-24 16:05:17	warning	[700072.074101] [wifi1] FWLOG: [35570809] WAL_DBGID_SECURITY_ENCR_EN ( )
2019-04-24 16:05:17	warning	[700072.074038] [wifi1] FWLOG: [35570809] WAL_DBGID_SECURITY_UCAST_KEY_SET (0x5643, 0x0)
2019-04-24 16:05:17	notice	hostapd: WLAN-2-01: AP-STA-DISCONNECTED c4:61:8b:72:56:43