Configuration of the FL WLAN 112x/ 102x product family

User manual

User manual

Configuration of the FL WLAN 112x/102x

UM EN SW FL WLAN 112x/102x, revision 01 2024-09-03

This manual is valid for:

Designation	Item No.
FL WLAN 1120	1386091
FL WLAN 1121	1386092
FL WLAN 1020	2702992
FL WLAN 1021	2702993

110820_en_01

Phoenix Contact GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

Table of contents

1 For your safety 7

1.1 Identification of warning notes 7

1.2 Qualification of users 7

1.3 Field of application of the product 8

1.3.1 Intended use 8

1.3.2 Product changes 8

1.4 Scope of the manual 8

1.5 Licensing information on open source software 9

1.6 Requesting the source code 9

1.7 Safety and installation instructions 9

1.7.1 UL warning notes 10

1.8 Security in the network 12

2 Startup and function 13

2.1 Delivery state/default settings 13

2.1.1 Initial IP configuration in the delivery state 13

2.1.2 Configuration in the delivery state 14

2.1.3 Meaning of the diagnostic and status indicators 15

2.1.4 General sequence for commissioning 16

2.1.5 Resetting to the default settings 17

2.1.6 Switching the firmware 19

2.2 Assigning the IP address via BootP 20

2.3 Assigning the IP address via BootP using FL Network Manager 21

3 Configuration and diagnostics in web-based management 25

3.1 General information 25

3.1.1 Accessing web-based management 25

3.1.2 Areas in web-based management 26

3.1.3 Icons and buttons in web-based management 27

3.2 WBM Information area 29

3.2.1 Help & Documentation 29

3.2.2 Device status 30

3.2.3 Local Diagnostics 30

3.2.4 Alarm and events 31

3.2.5 Connections 32

3.2.6 Interface status 33
3.2.7 Licenses 33
3.3 WBM Configuration area 35
3.3.1 My Profile 35
3.3.2 User management 37
3.3.3 Quick setup 42
3.3.4 System 42
3.3.5 Network 45
3.3.6 WLAN setting 47
3.3.7 WLAN interface 49
3.3.8 Service 50
3.3.9 Multicast filtering 55
3.3.10 Security 56
3.4 WBM Diagnostics area 65
3.4.1 Channel allocation (only Access Point operating mode): Diagnostics of WLAN channel assignment 65
3.4.2 RSSI graph 65
3.4.3 Trap Manager 67
3.4.4 Snapshot 69
3.4.5 Syslog for diagnostic purposes 69
3.4.6 Channel assignment/CST 71
3.5 REST API 73
3.6 Firmware update 74
3.6.1 Update via HTTP(S) 75
3.6.2 Update via TFTP 76
3.7 File transfer 76
3.7.1 Transfer via HTTP(S) 77
3.7.2 Transfer via TFTP 80
3.8 Creating user roles 85
4 Device operating modes 89
4.1 Operating mode:Access point 89
4.1.1 General information 89
4.1.2 Configuring an access point 90
4.2 Operating mode: Client 91
4.2.1 Roaming 91
4.2.2 Compatibility between different WLAN device manufacturers 92

4.2.3 Operation as a single client (SCB) 93
4.2.4 Operation as multi-client (MCB) 101
4.2.5 Operation as a fully transparent bridge (FTB) 104
4.3 Operating mode: Client (NAT) 108
4.3.1 1:1 NAT 111
4.3.2 IP masquerading 113
4.3.3 1-to-1 NAT configuration 116
4.3.4 IP masquerading configuration 117
4.4 Operating mode: Client (VXLAN) and access point (VXLAN) 119
4.4.1 Configuring the client (VXLAN) 119
4.4.2 Configuring the access point (VXLAN) 120
4.5 Operating mode: Repeater 122
4.5.1 Example configuration 123
4.5.2 Properties of two virtual wireless interfaces 124
5 DHCP service 125
5.1 Activating the DHCP service 125
5.2 Activating the global DHCP server at all interfaces 126
5.3 Activating the DHCP server on WLAN interfaces only 127
5.4 Diagnostics 130
6 RADIUS certificates 133
6.1 General information 133
6.2 Sequence of the 802.1X authentication process 133
6.3 Example configuration 134
6.4 Configuring RADIUS 134
6.4.1 Configuring the authenticator 134
6.4.2 Configuring the supplicant 136
6.4.3 Deactivating server identity verification 137
7 SNMP – Simple Network Management Protocol 139
7.1 General information 139
7.2 SNMP interface 139
7.2.1 Management Information Base (MIB) 140
7.2.2 Agent 140
8 VLAN – Virtual Local Area Network 143
8.1 Example configuration 143
8.2 Configuration via CLI 143
9 Revision history 145

1 For your safety

Read this documentation thoroughly and save it for future reference.

1.1 Identification of warning notes

This symbol indicates hazards that could lead to personal injury.
There are three signal words indicating the severity of a potential injury:

DANGER
Indicates a hazard with a high risk level. If this hazardous situation is not avoided, it will result in death or serious injury.

WARNING
Indicates a hazard with a medium risk level. If this hazardous situation is not avoided, it will result in death or serious injury.

CAUTION
Indicates a hazard with a low risk level. If this hazardous situation is not avoided, it could result in minor or moderate injury.

NOTE
This symbol together with the NOTE signal word warns the reader of actions that might cause property damage or a malfunction.

Notice
Here you will find additional information or detailed sources of information.

Industrial security
This symbol warns you of settings and actions that could impair the security of your network.

1.2 Qualification of users

The use of the products described in this documentation is intended exclusively for

- Electrically skilled persons or persons instructed by them. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.
- Qualified application programmers and software engineers. The users must be familiar with the relevant safety concepts of automation technology as well as applicable standards and other regulations.

1.3 Field of application of the product

1.3.1 Intended use

This product is recommended for use in industrial environments.

The functional ground must always be connected in industrial environments to comply with immunity requirements.

The device must always be operated within the specified operating temperature range. Direct sunlight may lead to overheating and permanent damage to the device.

1.3.2 Product changes

Modifications to hardware and firmware of the device are not permitted.

Incorrect operation or modifications to the device can endanger your safety or damage the device. Do not repair the device yourself. If the device is defective, please contact Phoenix Contact.

1.4 Scope of the manual

This manual contains information on configuring the FL WLAN 112x/102x product family.

For information about commissioning, refer to the separate manual UM EN HW FL WLAN 112x/102x with item no. 110821 at phoenixcontact.net/qr/<item_number>.

For information about configuration and diagnostics via the Command Line Interface (CLI), refer to the separate UM EN CLI manual with the number 110152: UM EN FL SWITCH CLI

1.5 Licensing information on open source software

The controllers use a Linux operating system. License information on the individual Linux packages can be found in web-based management of the device, see Licenses section.

Notes on LGPL software libraries

Any open source software used in the product is subject to the respective license terms, which are not affected by the Phoenix Contact Software License Terms (SLT) for the product. In particular, the licensee may modify the respective open source software in accordance with the applicable license terms. If the licensee wishes to modify an LGPL software library contained in this product, reverse engineering is permitted for debugging such modifications.

Notes on OpenSSL

This product includes software developed by the OpenSSL project for use in the OpenSSL toolkit. (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

1.6 Requesting the source code

The controllers contain software components that are licensed by the rights holder as free software or open source software under the GNU General Public License.

You can request the source code of these software components in the form of a CD or DVD-ROM for a processing fee of 50 euros within three years of delivery of the controller. To do this, please contact the After Sales Service of Phoenix Contact in writing at the address

PHOENIX CONTACT GmbH & Co. KG
After Sales Service Flachsmarktstrasse 8
32825 Blomberg
GERMANY

Subject: "Source Code Produktfamilie FL WLAN 112x/102x"

1.7 Safety and installation instructions

CAUTION: Risk of burns on hot surfaces
The surfaces of the device can get hot.

- Make sure to allow the device to cool down before working on it.

CAUTION: Noise susceptibility of medical equipment
This device emits radio frequency energy in the ISM frequency range (Industrial, Scientific, Medical) when using the 2.4 GHz and 5 GHz bands.

- Make sure that all medical devices used in the proximity of this device meet the noise susceptibility specifications for this type of radio frequency energy.
- Operate the device with a minimum clearance of 20 cm between the transmitter or antenna and your body.

NOTE: Installation only by qualified personnel
Installation, startup, and maintenance of the product may only be performed by qualified specialist personnel who have been authorized for this by the system operator. An electrically skilled person is someone who, because of their professional training, skills, experience, and their knowledge of relevant standards, can assess any required operations and recognize any possible dangers. Specialist personnel must have read and understand this documentation and comply with instructions. Observe the applicable national regulations with respect to the operation, function testing, repair, and maintenance of electronic devices.

NOTE: Electrostatic discharge
Electrostatic discharge can damage or destroy components.

- When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and IEC 61340-5-1.

NOTE: Statement regarding RF emission
Install and operate the device with a minimum clearance of 20 cm between the transmitter/antenna and your body.

NOTE: Requirement for the power supply
The device is designed exclusively for operation with safety extra-low voltage (SELV/PELV) from a class ES1 “electrical energy source” in accordance with EN/IEC 62368-1 and VDE 0868-1.

- Make sure that the correct power supply is used.

NOTE: Requirement for the current sources
This device may only be operated with power supplies that meet the requirements of EN/IEC 62368-1 for current sources with limited power.

- Operate this device with a power supply that meets the requirements of EN/IEC 62368-1.
- Alternatively, operate this device in a housing that meets the requirements of a fire protection enclosure in accordance with EN/IEC 62368-1.

1.7.1 UL warning notes

NOTE:
The external circuits to be connected to this device must be electrically isolated from the power supply or hazardous voltage by reinforced or double insulation and meet the SELV/PELV requirements of UL/CSA 61010-1, 61010-2-201.

NOTE:
The modules (FL WLAN 1021 only) must be installed the final safety enclosure, which has sufficient strength according to UL 61010-1, 61010-2-201 and meets the requirements with respect to spread of fire.

NOTE:
If the equipment is used in a manner not specified, the protection provided by the equipment may be impaired.

NOTE: Installation instructions for the UL variants FL WLAN 1121 und FL WLAN 1021
This devices are only suitable for indoor use. They only have a UL Type 1 rating. Care must be taken to ensure that the wired connections to the device's interfaces remain within the building or are only routed a maximum of 140 ft (42.67 m) outside the building.
Only use copper cables for the power supply with a permissible temperature range of -30 °C ... 85 °C (for T_{amb} 60 °C).

1.8 Security in the network

NOTE: Network security at risk due to unauthorized access
Connecting devices to a network entails the danger of unauthorized access to the network.

Observe the following safety notes:

- If possible, deactivate unused communication channels.
- Use secure passwords reflecting the complexity and service life recommended in the latest guidelines.
- Only allow authorized persons to access the device. Limit the number of authorized persons to the necessary minimum.
- Always install the latest firmware version. The firmware can be downloaded via the item (phoenixcontact.net/products).
- Observe the IT security requirements and the standards applicable to your application. Take the necessary protective measures. These may include, for example, virtual networks for remote maintenance access or a firewall.
- In security-critical applications, always use the device with an additional security appliance. Phoenix Contact offers security appliances in the mGuard product range. The mGuard routers connect various networks for the remote maintenance and protection of the local network and protect these networks against cyberattacks.
- You must take defense-in-depth strategies into consideration when planning networks.

Further measures for protection against unauthorized network access can be found in the “INDUSTRIAL SECURITY”. The application note can be downloaded via the item (phoenixcontact.net/products).
German: AH DE INDUSTRIAL security, 107913
English: AH EN INDUSTRIAL security, 107913

If there is a security vulnerability for products, solutions, or services from Phoenix Contact, it will be published on the PSIRT (Product Security Incident Response Team) website: phoenixcontact.com/psirt

2 Startup and function

2.1 Delivery state/default settings

2.1.1 Initial IP configuration in the delivery state

In the delivery state, the device has an initial IP configuration and an individual DNS host name. This way, you can access web-based management and configure the device.

The connected PC must be set to “Obtain an IP address automatically”. A static IP address cannot be used here.

Automatic private IP addressing (APIPA)

- You can access your device via link-local IPv4 via the IP address 169.254.2.1.
- If you want to start up several devices in your network, one device has the IP address 169.254.2.1. All other devices are assigned a random IP address from the range 169.254.2.1 to 169.254.255.255. You can determine these IP addresses using external software such as Wireshark or access the device via its host name.

With this dynamic method, it is difficult to find out which device has which IP address when dealing with multiple devices. You can therefore also access the device via a DNS host name.

DNS host name

The host name consists of two parts:

1. Device family: WLAN
2. The individual part of the MAC address of the device, e.g., a8:74:1d:**b2:30:ae**

The complete host name in this example is therefore: WLAN-B230AE

- Enter the host name in your browser as follows:
  http://WLAN-b230ae.local

For name resolution, mDNS (standard for Linux and Mac systems) and LLMNR (usually used for Windows systems) are supported.

This initial IP configuration is deactivated as soon as the device is assigned an IP configuration via a different IP address assignment mechanism, e.g., via BootP, DHCP, web-based management.

If you want to reactivate the initial IP configuration at a later date, you can reset the device. See Resetting to the default settings oder Quick Setup.

2.1.2 Configuration in the delivery state

Observe the safety and installation instructions.

In the delivery state or after the system is reset to the default settings, the following functions and properties are available:

- The user name is “admin”.
- The password is “private”.
- Only with the default settings can the device also be accessed via the link-local IPv4 address 169.254.2.1.
- BootP is activated.
- WLAN is activated.
- Operating mode: MCB (client)
- SSID: PhoenixContact, encryption WPA2: 2bchanged
- Transmission power: 5 dBm
- Confidential web view is activated.

You will find your firmware version in web-based management (WBM) on the “Device status” page.

2.1.3 Meaning of the diagnostic and status indicators

The device indicates the following information via the LEDs. Additional diagnostic options can be accessed via the CLI or web-based management.

While the device is starting up, the US LED lights up green and the WLAN LED lights up white. Once the device has started up and is ready for operation, the LEDs indicate the operating state (see Meaning of the diagnostic and status indicators).

2.1.3.1 FL WLAN 112x

Tabelle 2-1 Meaning of the diagnostic and status indicators (FL WLAN 112x)

Des.	Color	Function:Access point	Function:Client
US	Green (on)	Supply voltage is applied	
WLAN	off	WLAN interface deactivated	
	White (on)	During the start process	
	Red (on)	During the start process for 3 seconds (firmware switching possible)	
	Blue (on)	WLAN interface activated	WLAN interface connected*
	Violet (on)	Automatic channel selection (only with DFS)	Scan for access point

2.1.3.2 FL WLAN 102x

Tabelle 2-2 Meaning of the diagnostic and status indicators (FL WLAN 102x)

Des.	Color	Function:Access point	Function:Client
US	Green (on)	Supply voltage is applied	
WLAN	off	WLAN interface deactivated	
	White (on)	During the start process	
	Red (on)	During the start process for 3 seconds (firmware switching possible)	
	Blue (on)	WLAN interface activated	WLAN interface connected*
	Violet (on)	Automatic channel selection (only with DFS)	Scan for access point
	Green (on)	WLAN interface in Idle mode if radar	WLAN interface in Idle mode

Des.	Color	Function:Access point	Function:Client
		check (DFS) is active at 5 GHz	
RSSI	off	No display	RSSI< -80 dBm
	Orange (on)	No display	RSSI -70 dBm ... -80 dBm
	Green (on)	During the boot process	
	Green (on)	No display	RSSI >-70 dBm
LAN	off	No Ethernet connection at XF1	
	Green (on)	100 Mbps link connected	
	Green (flashing)	100 Mbps link active	
	Orange (on)	1000 Mbps link connected	
	Orange (flashing)	1000 Mbps link active	

* WLAN connection established (blue): The LED lights up blue after a successful key/ certificate exchange.

2.1.4 General sequence for commissioning

To start up the device, proceed as follows:

- Supply the device with operating voltage (nominal value: 24 V DC).
- Connect the device via the Ethernet interface using an RJ45 connector to the PC that will be used for configuration.
- Access the device via the link-local IPv4 address 169.254.2.1 or the DNS host name.

Alternatively, assign an IP address to the device via BootP. The IP address is assigned by a corresponding server in the network or a PC tool (see Assigning the IP address).

The device can now be configured via web-based management (WBM) or the Command Line Interface (CLI).

Make sure that the PC that will be used for configuration via WBM or CLI has an IP address in the same IP range.

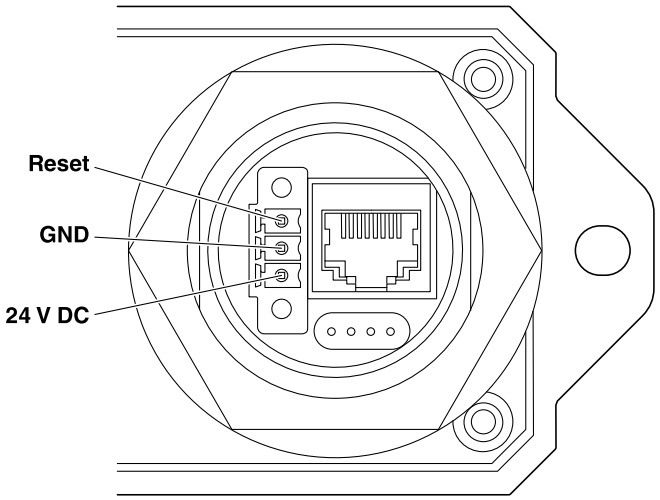
Further information on the Command Line Interface (CLI) can be found in the separate CLI manual.

2.1.5 Resetting to the default settings

2.1.5.1 FL WLAN 112x

The device has a digital input (reset). The digital input is only used to reset the device to the default settings or to switch the firmware to the previous version. It cannot be used to restart the device.

Figure 2-1 Connection of the supply voltage and the digital input on the bottom of the device



- Connect the device to the supply voltage.
- Wait approx. 30 seconds for the device to boot up and be ready for operation.

While the device is starting up, the US LED lights up green and the WLAN LED lights up white. Once the device has started up and is ready for operation, the LEDs indicate the operating state (see Meaning of the diagnostic and status indicators).

You now have approx. 1 minute to reset the device to the default settings.

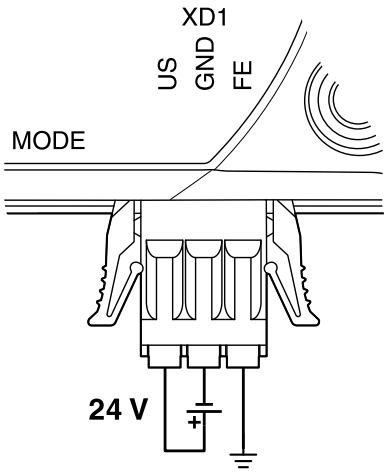
- Apply a voltage equivalent to the operating voltage to the digital input (reset) for at least 5 seconds.
- Disconnect the digital input (reset) from the power supply again.

The device is reset to the default settings and restarted.

2.1.5.2 FL WLAN 102x

The device has a MODE button. You can use the MODE button to reset the device to the default settings or switch the firmware to the previous version.

Figure 2-2 Supply voltage connection and reset via MODE button



- Connect the device to the supply voltage.
- Wait approx. 30 seconds for the device to boot up and be ready for operation.

While the device is starting up, the US LED lights up green and the WLAN LED lights up white. Once the device has started up and is ready for operation, the LEDs indicate the operating state (see Meaning of the diagnostic and status indicators).

You now have approx. 1 minute to reset the device to the default settings.

- Use a suitable item to press the recessed MODE button for at least 5 seconds.
- Release the MODE button again.

The device is reset to the default settings and restarted.

2.1.6 Switching the firmware

2.1.6.1 FL WLAN 112x

The device has a digital input (reset). The digital input is only used to reset the device to the default settings or to switch the firmware to the previous version. It cannot be used to restart the device.

See Connection of the supply voltage and the digital input on the bottom of the device.

- Connect the device to the supply voltage.
- Wait about 4 seconds until the WLAN LED lights up red.

You now have approx. 3 seconds to switch over the firmware.

- Apply a voltage equivalent to the operating voltage to the digital input (reset) for at least 3 seconds.

The WLAN LED of the device flashes green after switching has been completed.

- Disconnect the digital input (reset) from the power supply again.

The device will now start with the previous firmware version.

2.1.6.2 FL WLAN 102x

The device has a MODE button. You can use the MODE button to reset the device to the default settings or switch the firmware to the previous version.

See Supply voltage connection and reset via MODE button

- Connect the device to the supply voltage.
- Wait about 4 seconds until the WLAN LED lights up red.

You now have approx. 3 seconds to switch over the firmware.

- Use a suitable item to press the recessed MODE button for at least 3 seconds.

The WLAN LED of the device flashes green after switching has been completed.

- Release the MODE button again.

The device will now start with the previous firmware version.

2.2 Assigning the IP address via BootP

Notes on BootP

During initial startup and after resetting to the default settings, the device sends BootP requests without interruption until it receives a valid IP address. As soon as the device receives a valid IP address, it stops sending further BootP requests.

If the device has already been configured, it sends three BootP requests when a restart is performed. If these three BootP requests do not receive a response, the device starts with the IP address that was last assigned via BootP.

An activated firewall on the PC can prevent the allocation of IP addresses via BootP.

Numerous BootP servers are available on the Internet. You can use any of these programs for address assignment. The following section explains IP address assignment using the Phoenix Contact software tool “FL Network Manager” (item no. 2702889).

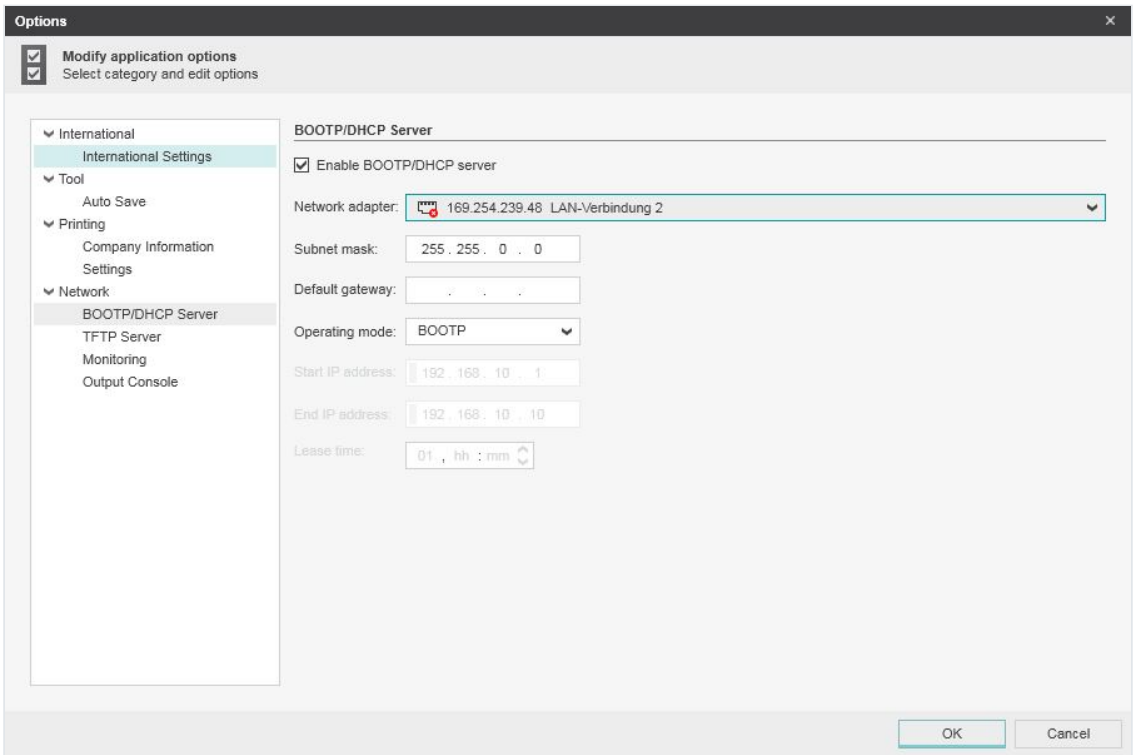
2.3 Assigning the IP address via BootP using FL Network Manager

Requirements

The device is connected to a “Microsoft Windows” operating system and the FL Network Manager is installed.

Step 1: Parameterizing the BootP server

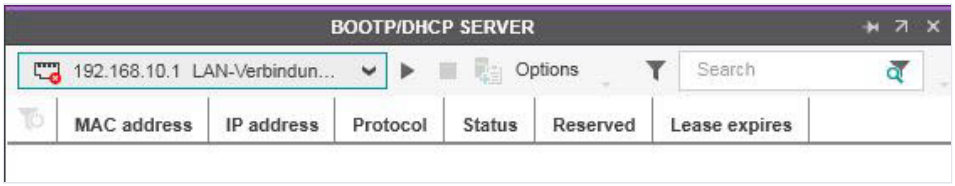
Figure 2-3 Parameterizing the BootP server



- Open FL Network Manager software.
- Open a new project in the software.
- Under the “Extras, Options” menu item, select “BOOTP/DHCP Server”.
- Activate the “Enable BOOTP/DHCP server” check box.
- Configure the network interface of the PC to which the device is connected and select “BootP” operating mode. You can also adjust the subnet mask and configure a default gateway.
- Confirm the parameterization with “OK”.

Step 2: Starting the BootP server

Figure 2-4 Starting the BootP server



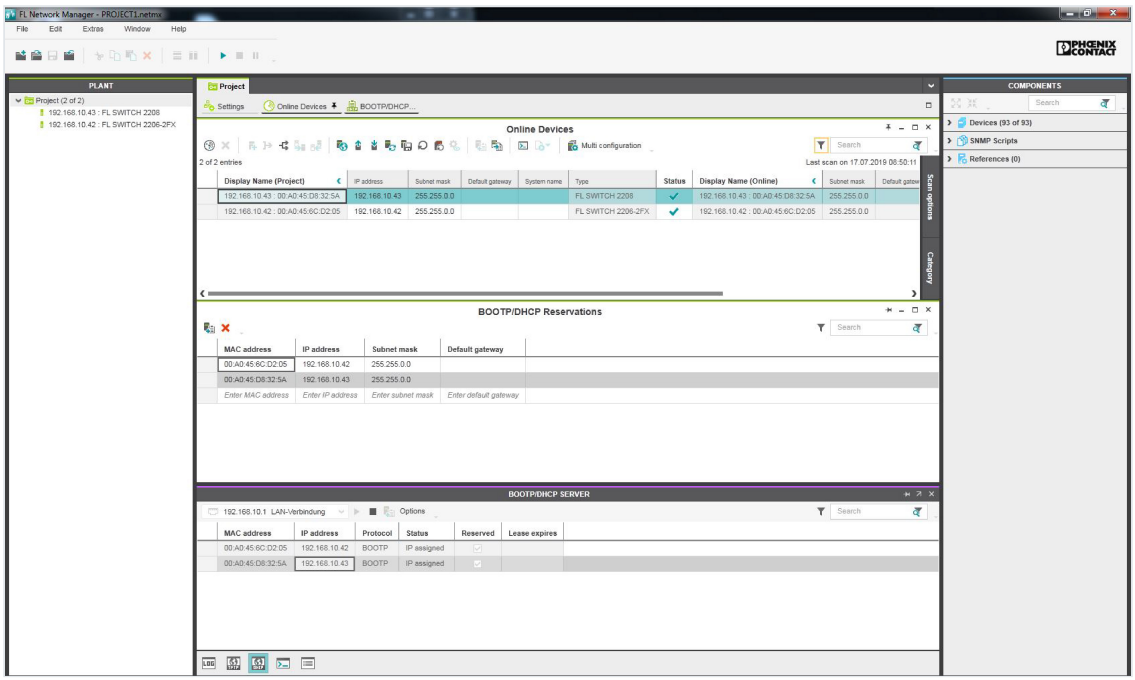
- Open the “BOOTP/DHCP SERVER” window.
- Click on the play icon next to the selected network interface.

↪ The BootP server is activated.

↪ BootP requests received are listed in the “BOOTP/DHCP SERVER” window in table format.

Step 3: Inserting BootP requests in the reservation list and assigning IP parameters

Figure 2-5 Inserting BootP requests in the reservation list



- If you want to assign IP parameters to a device, such as IP address, subnet mask, or default gateway, right-click on an incoming BootP request in the “BOOTP/DHCP SERVER” window. Then, select “Add to BOOTP/DHCP reservations”.
- Enter the IP address to be assigned in the “BOOTP/DHCP Reservations” window. The IP parameters are immediately transferred to the device.
- You can check whether the IP address assignment was successful in the “IP address” column in the “BOOTP/DHCP SERVER” window.

You can change the IP parameters set here in web-based management (see Accessing web-based management).

3 Configuration and diagnostics in web-based management

On the following pages you will find information on the web-based management of your device. The information shown here corresponds to the firmware 3.37.

3.1 General information

You can use web-based management (WBM) to manage your device from anywhere in the network using a standard browser (e.g., Microsoft Edge). The configuration and diagnostic functions are clearly displayed on a graphical user interface. Depending on the permission, each user has read and/or write access to the device. A wide range of information about the device itself, the set parameters, and the operating state can be viewed.

Modifications to the device can only be made with a user account with corresponding rights. In the default settings, the user name is “admin” and the password is “private”.

NOTE: Change initial password
With the initial password, unauthorized access is possible.
- Change the administrator password immediately after the first login.
- Do not share the password.

3.1.1 Accessing web-based management

- Perform the initial startup.

Make sure that the PC that will be used for configuration via WBM or CLI has an IP address in the same IP range.

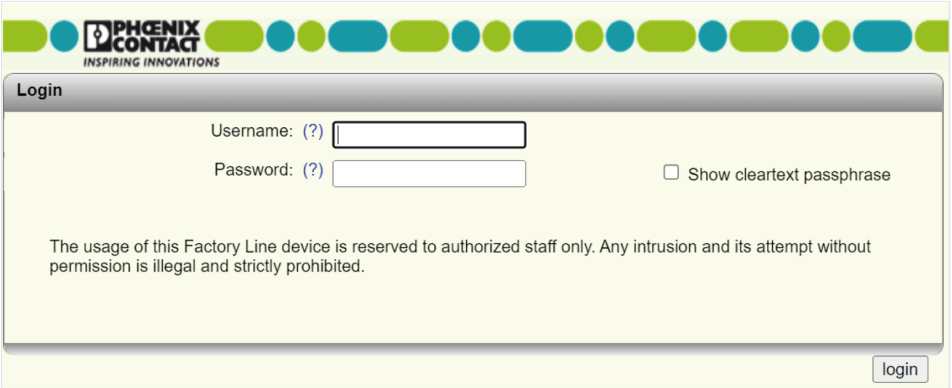
- Open a browser and enter the IP address of the device in the address line.

Web-based management opens.

- Click “Login” and log in using your access data.

In the default settings, the user name is “admin” and the password is “private”.

Figure 3-1 Login area



Depending on the configuration of the device, a user account may be locked for a period of time after a certain number of failed login attempts. During this time, it is not possible to access WBM, even if the correct user data is entered (see User management).

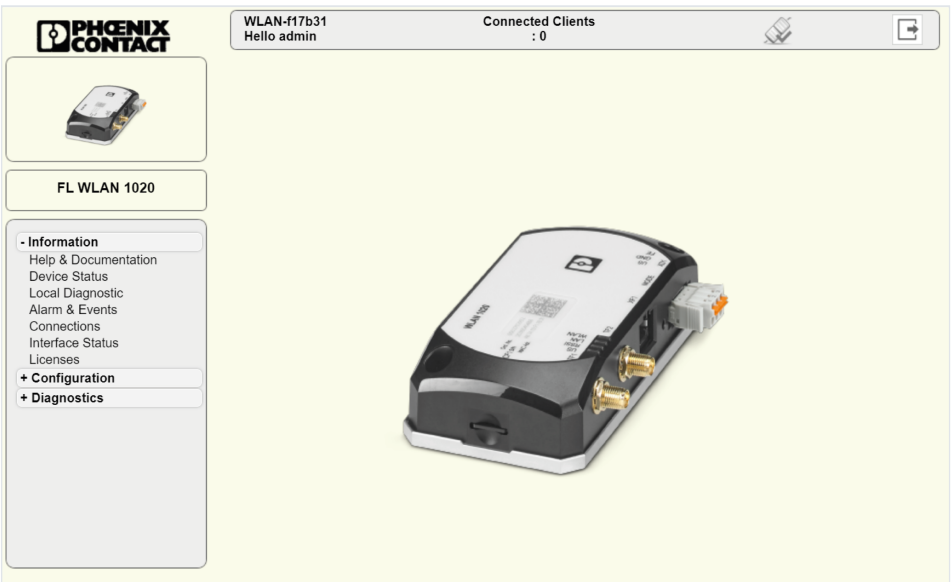
3.1.2 Areas in web-based management

The visibility and configurability of the individual areas and parameters depend on the scope of permissions of the respective user account.

Web-based management is split into the following areas:

- Information:General device information
- Configuration: Device configuration
- Diagnostics: Device-specific diagnostics

Figure 3-2 Start page for web-based management (example)

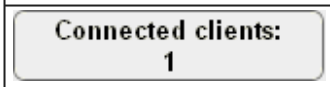


3.1.3 Icons and buttons in web-based management

At the top and bottom of WBM, there are icons and buttons that provide an overview of important device functions.

Figure 3-3 WBM with icons (selection)

Tabelle 3-1 Explanation of icons

Icon	Explanation
	The WLAN interface is deactivated.
	The device operating mode is “Client”. There is no WLAN connection to an access point.
	The device operating mode is “Client”. There is a WLAN connection to an access point. The number of bars indicates the signal strength of the connection: The more bars are displayed, the higher the signal strength.
	The device operating mode is “Access Point”. The number specifies the number of connected clients. If “0” is displayed, there is no connection to a client.
	Connection status: Connected This icon indicates that there is currently a connection between the device and the PC used.
	Connection status: Disconnected This icon indicates that there is currently no connection between the device and the PC used. This is the case if a configuration change is currently being carried out. Alternatively, this is the case after a configuration change has been performed via WLAN and resulted in changes that require a new login.
	To log out the current user, click the icon.
	The active configuration differs from the saved configuration for the device. To save the active configuration, click on the icon.
	The administrator password has not yet been changed and is the initial password. For security reasons, we recommend changing the existing password to a new one known only to you.

NOTE: Change initial password
With the initial password, unauthorized access is possible.

- Change the administrator password immediately after the first login.
- Do not share the password.

Tabelle 3-2 Explanation of the buttons

Icon	Explanation
Revert	This button deletes all the changes that have been made since the last save.
Apply	This button applies the current settings, but does not save the configuration. The changes confirmed with “Apply” are lost during the next voltage reset.
Apply&Save	This button applies the current settings and saves the configuration. The settings made are also retained after a voltage reset. If an SD card is inserted, clicking “Apply&Save” additionally saves the configuration to the SD card. If there is an existing configuration on the SD card, it will be overwritten.

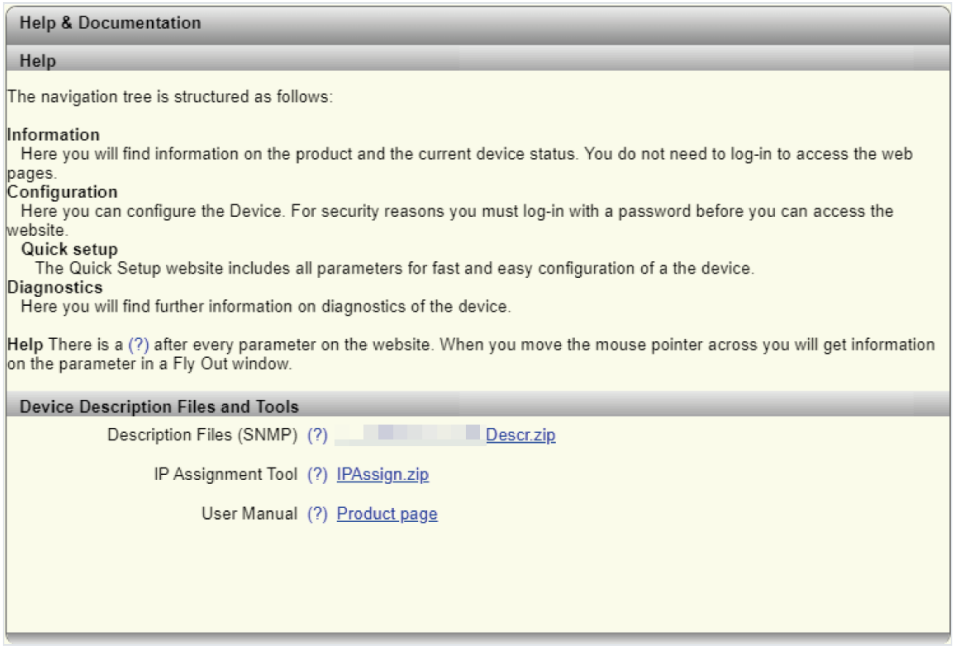
3.2 WBM Information area

3.2.1 Help & Documentation

On this page, you will find useful information on how to use web-based management (WBM).

- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Help & Documentation”.

Figure 3-4 Help & Documentation



On this page, you can also download the following files and software directly from the device:

– User Manual: Click “Product page” to access the product page. Here, you can download the current documentation.

3.2.2 Device status

On this page, you will find general information about your device, such as the serial number, firmware version, or hardware revision.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Device Status”.

Figure 3-5 Device status

Device Status		
Device Identification		
Vendor	:	Phoenix Contact GmbH & Co. KG
Address	:	D-32823 Blomberg
Phone	:	+49 -(0)5235 -3-00
Internet	:	www.PhoenixContact.com
Type	:	FL WLAN 2100
Order No	:	2702535
Serial No	:	2033574356
Firmware Version	:	2.63
Hardware Version	:	RN
Logic Version	:	0x0
Bootloader Version	:	1.26
Hostname	:	WLAN-dd5ebc
Device Name	:	WLAN-dd5ebc
Description	:	
Physical Location	:	
Contact	:	
IP Address	:	172.16.153.32
Subnet Mask	:	255.255.255.0
Gateway	:	172.16.153.2
IP Address Assignment	:	Static
MAC Address	:	00:A0:45:DD:5E:BC
System Status		
Uptime	:	8m:0s
Configuration Status		
Configuration Status	:	Configuration saved

3.2.3 Local Diagnostics

On this page, you will find a brief explanation of the individual LEDs on the device.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Local Diagnostics”.

The FL WLAN 110x/210x devices only have the “US” and “WLAN” LEDs.

Figure 3-6 Local Diagnostics

3.2.4 Alarm and events

On this page, you will find a list of alarms and events in a table. For Event Table entries to be retained after the device is restarted, you can save them. You can download the Event Table from the device in CSV format.

A maximum of 3,000 entries can be stored in the event table. The oldest entries are overwritten. If there is a large number of entries, it may take a few seconds to load the Event Table.

The persistent storage of events is deactivated in the factory default state. This means that the events are deleted when the device is restarted. You can activate the function via “Persistent Event Logging” on the “Service” page (see Service).

- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Alarm and Events”.

Figure 3-7 Alarm and events

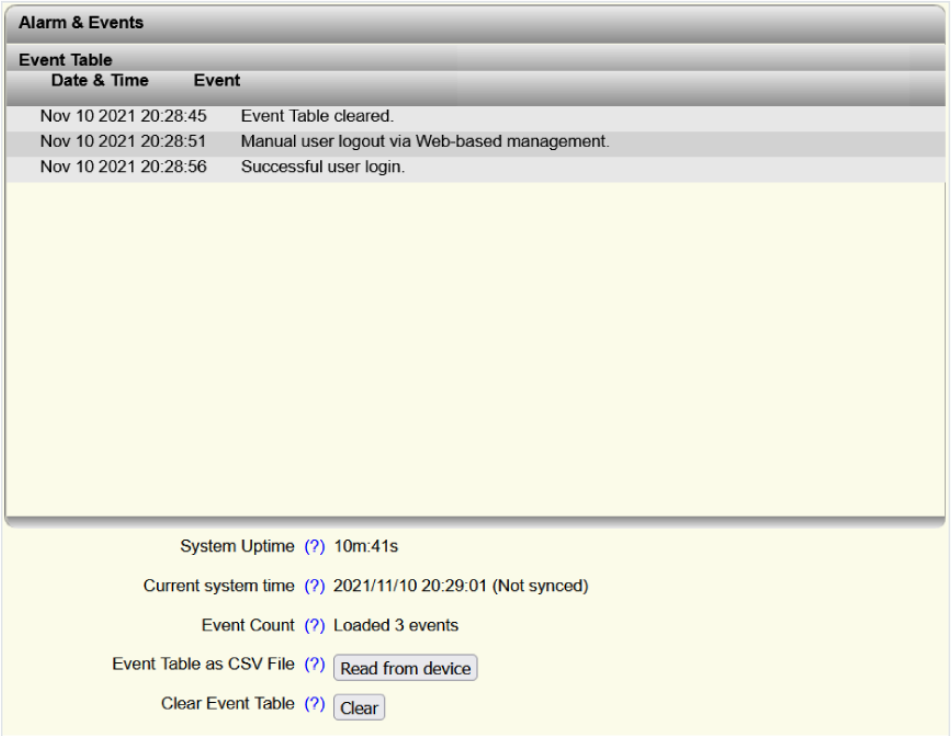


Tabelle 3-3 Alarm and events: Parameters

Parameters	Description
System Uptime	How long the device has been in operation since the last restart is displayed here.
Current system time	The current system time is displayed here. If the time is not synchronized, there may be deviations between the system time and the actual time (see Service).
Event Count	The number of currently loaded events in the event table is displayed here.
Event Table as CSV File	Click “Read from device” to download and save the currently displayed event table as a CSV file.
Clear Event Table	Click “Clear” to delete all the currently displayed events in the event table.

3.2.5 Connections

On this page you will find an overview of all currently active connections with other devices.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Connections”.

Figure 3-8 Connections

Connections

Connected to	SSID	MAC address	Rate [Mbps]	RSSI [dBm]
AP	Phoenix_WLAN2100	0e:72:74:39:7b:a6	8	-69
Client	Phoenix_WLAN1020	a8:74:1d:74:76:ae	5	-85

3.2.6 Interface status

On this page, you will find information about the interface status regarding LAN and WLAN, such as the current IP address or device operating mode.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Interface Status”.

Figure 3-9 Interface status:LAN

Interface Status

LAN | WLAN

Network Information

IP Address	:	172.16.153.30
Subnet Mask	:	255.255.255.0
Gateway	:	0.0.0.0
IP Address Assignment	:	
MAC Address	:	00:A0:45:DD:5D:5C

Physical Ports

Interface/Port	Type	Status	Mode
1	TX 10/100	enable	100 MBit/s FD

Figure 3-10 Interface status:WLAN

Interface Status

LAN | WLAN

WLAN 1

Operating Mode	:	Access Point
Connect state	:	0 clients connected
Network SSID	:	PhoenixContact
Security mode	:	WPA2-PSK AES
WLAN 802.11 mode	:	5GHz (802.11 a/n)
Current TX power	:	5 dBm
Current WLAN Channel	:	165
Channel bandwidth (802.11n)	:	20 MHz
Current medium utilization	:	0 %

3.2.7 Licenses

On this page, you can view which third-party software is used and the corresponding licenses.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Licenses”.

Figure 3-11 Licenses

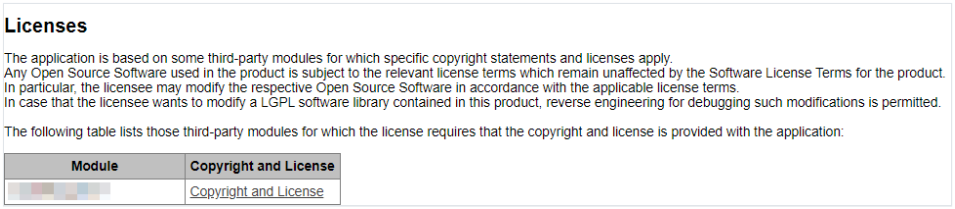


Tabelle 3-4 Licenses: Parameters

Parameters	Description
Copyright and License	Click on the link beside the respective module to jump directly to the corresponding paragraph on copyright and licenses.

3.3 WBM Configuration area

3.3.1 My Profile

On the “My Profile” page, you will find an overview of the rights assigned to your user profile. As a logged-in user you can also change your password.

If you are an “admin” user, you can also configure an individual SNMPv3 password.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, My Profile”.

Figure 3-12 My Profile

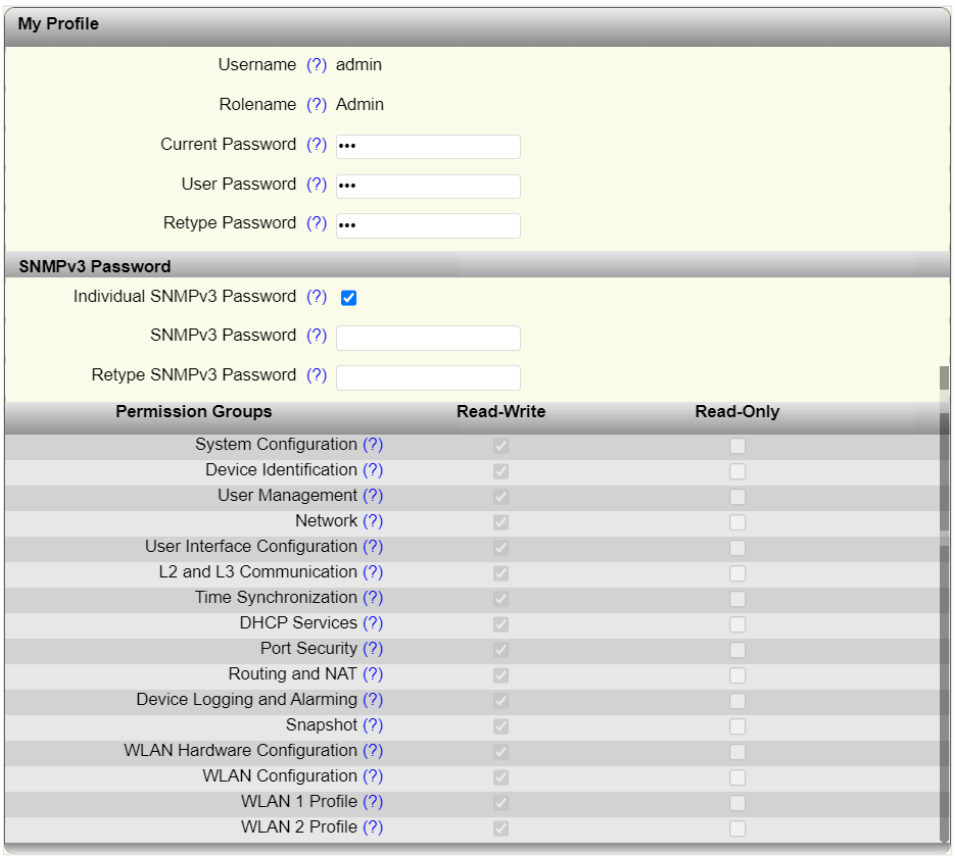


Tabelle 3-5 My Profile: Parameters

Parameters	Description
Username	Your user name as the logged-in user is displayed here. You cannot change the name yourself.
Rolename	The role name your user is assigned to is displayed here.

Parameters	Description
Current Password	Enter the current password in the input field. For security reasons, your password is not displayed as plain text.
User Password	Enter the desired password in the input field. The new password must be between eight and 64 characters long. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space. For security reasons, your password is not displayed as plain text.
Retype Password	Re-enter the new password. The new password will be activated after saving and logging out.

My Profile:SNMPv3 Password

Tabelle 3-6 SNMPv3 Password: Parameters

Parameters	Description
Individual SNMPv3 Password	The “SNMPv3 Password” area is only available to the “admin” user account that was created in the factory default state. Activate the check box to assign an individual SNMPv3 password.
SNMPv3 Password	This option is only available if the check box next to “Individual SNMPv3 Password” has been activated. Enter the desired SNMPv3 password in the input field. The password must be between eight and 64 characters long. For security reasons, your password is not displayed as plain text. If you do not assign an SNMPv3 password, the password of the “admin” user account will be used. If you use this password, a user account with the name “snmpv3_user” will be created. The user is assigned read-only rights and **cannot** access the device via SNMPv3. If you delete the user account “snmpv3_user”, the “Individual SNMPv3 Password” option is deactivated.
Retype SNMPv3 Password	This option is only available if the check box next to “Individual SNMPv3 Password” has been activated. Re-enter the new password.

3.3.2 User management

The “User Management” page allows you to create and manage user accounts. You can assign permissions to users via various user roles.

The device also provides the option of server-based user authentication via LDAP or RADIUS. Configure these settings on the “Security” webpage (see Security).

When a user logs in, the device always searches the local user accounts first. Server-based user authentication is only used if the user name is not available locally.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, User Management”.

Figure 3-13 User management

Tabelle 3-7 User management: Parameters

Parameters	Description
Create/Edit User	Select the user account that you wish to edit or delete. Select “Create” to create a new user account.
Delete	This option is only available if you selected an existing user account for “Create/Edit User”. Click “Delete” to delete the currently selected user account. This action cannot be undone. The “admin” user account cannot be deleted.

Parameters	Description
User Status	Select whether the account is activated or deactivated. When the account is deactivated, access to the device is blocked, even if the correct login parameters are entered.
Username	Enter the desired user name in the text field. The user name can be up to 32 characters long. Letters, numbers, and the following special characters are permitted: -_.@. Once the user name has been created, it cannot be changed.
User Role	From the drop-down list, select the desired role. The role determines the rights the account has in WBM. You can select the following roles in the factory default state: – Read-only: The user has read access to the device and therefore access to the webpages in the Information and Diagnostics areas. Furthermore, the user has permission to change their own access password. – Expert: The user has extensive read and write access to the device and can therefore modify a good portion of the configuration parameters. However, this excludes User Management. – Admin: The user has all administration rights. This includes unrestricted read and write access to the device. You can create further user roles, see Pop-up window: Custom User Roles.
User Password	Enter the desired initial password in the text field. The password must be between eight and 64 characters long. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space. The user can change the password later on.
Retype Password	Enter the initial password again.
User account locking	Select whether the account should be locked after failed login attempts. If a user repeatedly attempts to log in using the wrong password, access to the device can be blocked for a certain period of time.
Login Attempts Limit	This option is only available if you selected “Enable” for “User account locking”. Enter the desired number of login attempts until the account will be locked. The number must be between one and 100.

Parameters	Description
Access Lock Time	This option is only available if you selected “Enable” for “User account locking”. Enter the desired time in minutes that an account will remain locked for after failed login attempts. The time must be between one and 1440 minutes.

User management:Custom user roles

Tabelle 3-8 Custom User Roles: Parameters

Parameters	Description
Custom User Roles webpage	Click “Custom User Roles” to open the “Custom User Roles” pop-up window. Here, you can define the desired permissions for each role (see Pop-up window: Custom User Roles).

User management:User security settings

Tabelle 3-9 User Security Settings: Parameters

Parameters	Description
User Security Settings Webpage	Click “User Security Settings” to open the “User Security Settings” pop-up window. There, you can define minimum requirements for user passwords, e.g., each password must contain a special character (see Pop-up window: User security settings).

3.3.2.1 Custom user roles

Figure 3-14 Pop-up window: Custom User Roles

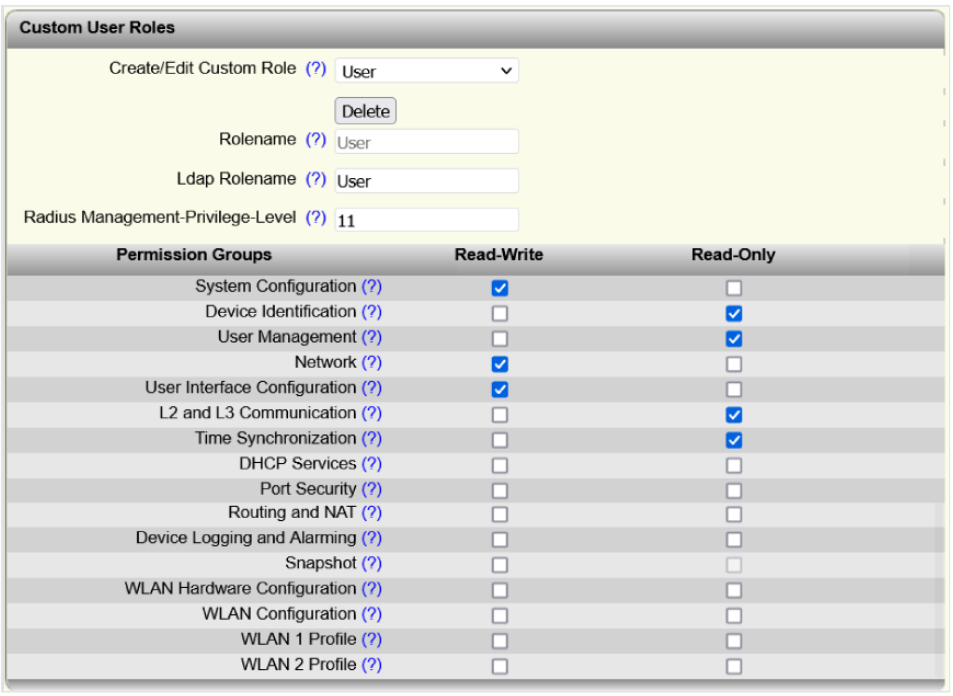


Tabelle 3-10 Pop-up window: Custom user roles: Parameters

Parameters	Description
Create/Edit Custom Role	Select the user account that you wish to edit or delete. Select “Create” to create a new user account.
Delete	Click “Delete” to delete the currently selected role. This action cannot be undone. The preconfigured “Admin”, “Expert”, and “Read-only” roles cannot be deleted.
Rolename	Enter the desired name for the user role in the text field. The name for the user role can have up to 32 characters. Letters, numbers, and the following special characters are permitted: -_.@. Once the role name has been created, it can no longer be changed.
Ldap Rolename	The LDAP role name is made available to a user via the LDAP server. The role name is used to assign a user to a user role and therefore to assign rights on the device. The LDAP role name is mapped to a local user role here. For further information on LDAP, see .
Radius Management-Privilege-Level	You can enter a numerical value here that is made available to a user via the RADIUS server during server-based authentication. This value is used to assign a user to a user role and therefore to assign rights on the device. The management privilege level is mapped to a local user role here. For further information on RADIUS, see .
Permission Groups	In the table, you can assign and edit the read and write permissions for user-defined user roles. The predefined permissions for the “Admin”, “Expert”, and “Read-only” roles available by default cannot be changed. – Read-Write: Select the respective check box to assign read and write permissions for the function group to the selected user role. – Read-Only: Select the respective check box to assign read permissions for the respective function group to the selected user role. – No selection: If you do not select either of the two check boxes for a function group, the user role does not receive any right for this function group.

For further information on user roles and permissions, see *Creating user roles*.

3.3.2.2 User security settings

Figure 3-15 Pop-up window: User security settings

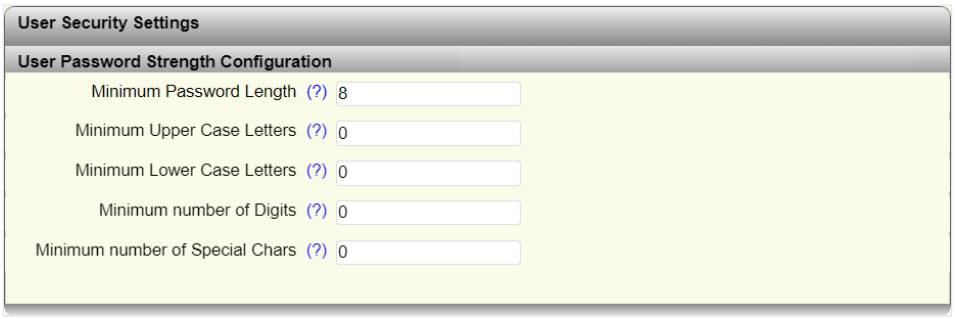


Tabelle 3-11 Pop-up window: User security settings: Parameters

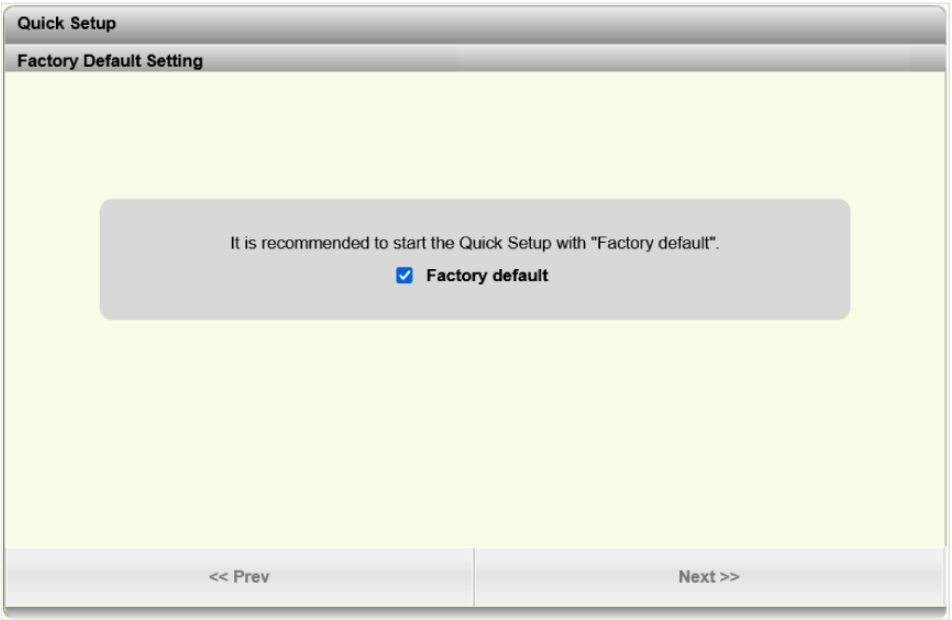
Parameters	Description
Minimum Password Length	Enter the desired minimum length for passwords here. The value can be between eight and 64 characters (default: 8).
Minimum Upper Case Letters	Enter the desired minimum number of uppercase letters (A-Z) here. The value can be between zero and eight characters (default: 0).
Minimum Lower Case Letters	Enter the desired minimum number of lowercase letters (a-z) here. The value can be between zero and eight characters (default: 0).
Minimum number of Digits	Enter the desired minimum number of digits (0-9) here. The value can be between zero and eight characters (default: 0).
Minimum number of Special Chars	Enter the desired minimum number of special characters (e.g., .#:!?). here. The value can be between zero and eight characters (default: 0).

3.3.3 Quick setup

The “Quick Setup” page allows you to quickly configure the minimum requirements of a WLAN network. A wizard will guide you through the individual steps.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, Quick Setup”.

Figure 3-16 Quick setup



It is recommended to perform the quick setup with the default settings. For this, activate the “Factory default” check box. By doing so, all previous configurations are deleted.

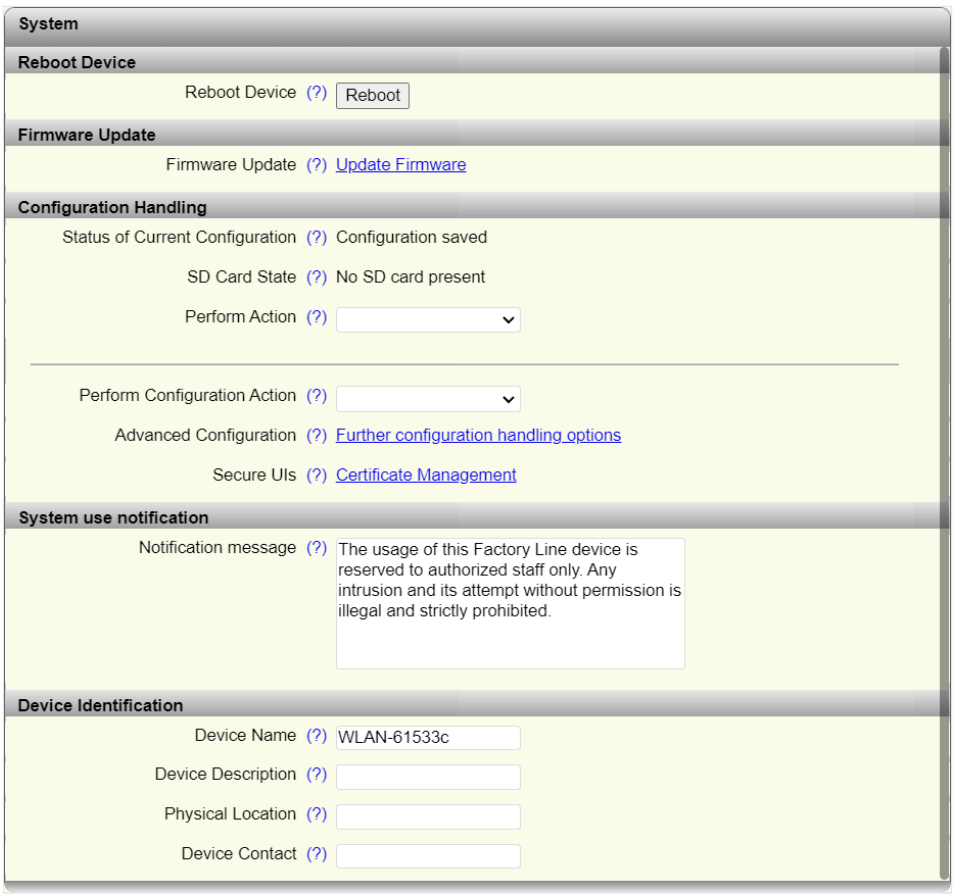
- Click “Next” and follow the setup instructions.

3.3.4 System

On this page, you can make basic system settings such as firmware updates or renaming the device.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, System”.

Figure 3-17 System



System:Reboot Device

Tabelle 3-12 Reboot Device: Parameters

Parameters	Description
Reboot Device	Click on “Reboot” to restart the device. All unsaved parameters will be lost. The connection to the device is interrupted for the boot phase.

System:Firmware update

Tabelle 3-13 Firmware Update: Parameters

Parameters	Description
Firmware Update	Click “Update Firmware” to perform a firmware update. For further information, please refer to .

System:Configuration Handling

Tabelle 3-14 Configuration Handling: Parameters

Parameters	Description
Status of Current Configuration	The status of the current configuration is displayed here. – Configuration saved: The current configuration is saved to the device.

Parameters	Description
	– Configuration modified but not saved: The current configuration was changed but not saved to the device. Click “Apply&Save” to save the configuration to the device.
SD Card State	Whether an SD card is inserted is displayed here. You need to reload the page to see the current status. You can only use FAT-formatted SD cards.
Perform Action	Select the action to be performed. – Compare: The action compares the configuration file on the SD card with the one on the device. Whether the configuration on the SD card is identical, different, or does not exist is shown to you. – Clear: The action deletes the configuration file on the SD card.
Perform Configuration Action	Select an option from the drop-down list. – Factory Default: The action resets the device configuration to the factory setting. – Save Configuration: The action saves the current configuration to the device. After a voltage reset, the settings made are retained. – Reload Configuration: The action loads the configuration last saved and applies it. The configuration can be saved via “Save Configuration” or using the “Apply&Save” button.
Advanced Configuration	Click “Further configuration handling options” to open the “File Transfer” pop-up window (see).
Secure UIs	Click “Certificate Management” to open the “Security Context” pop-up window (see Certificate Management).

System: System Use Notification

Tabelle 3-15 System Use Notification: Parameters

Parameters	Description
Notification message	Enter a text of up to 256 characters that will be displayed on the WBM login page.

System:Device Identification

Tabelle 3-16 Device Identification: Parameters

Parameters	Description
Device Name	Enter the desired device name. In the factory default state, the device name corresponds to the device host name.
Device Description	Optionally, enter a device description.

Parameters	Description
Physical Location	Optionally, enter the location of the device, such as the building in which it is installed.
Device Contact	Optionally, enter a contact address for the device.

3.3.5 Network

On this page, you can make the basic network settings.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, Network”.

Figure 3-18 Network

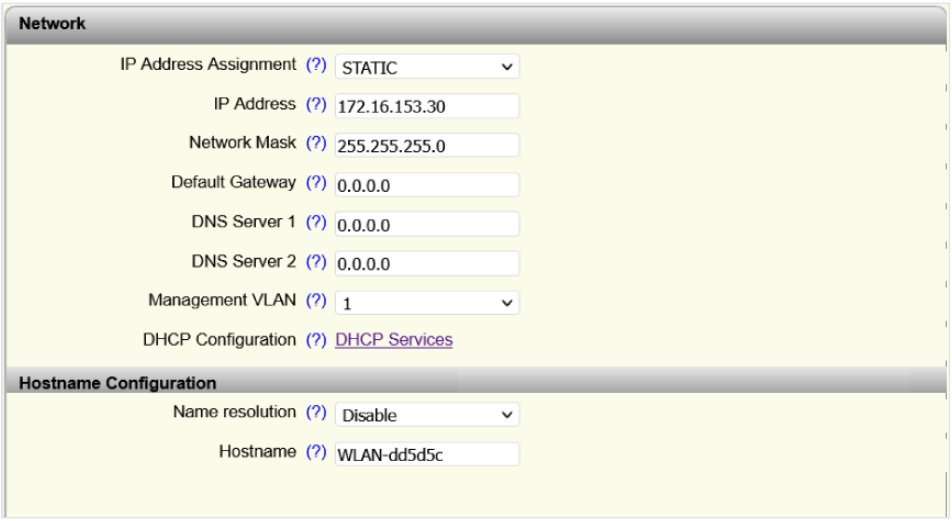


Tabelle 3-17 Network: Parameters

Parameters	Description
IP Address Assignment	Select the type of IP address assignment. – STATIC: Static IP address – BOOTP: Assignment via the bootstrap protocol – DHCP: Assignment via a DHCP server – DCP: Assignment via PROFINET engineering tool or control For further information on IP address assignment, refer to Assigning the IP address.
IP Address	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the desired IP address.
Network Mask	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the desired subnet mask.
Default Gateway	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the default gateway.

Parameters	Description
DNS Server 1	Enter the IP address of the primary DNS server here.
DNS Server 2	Enter the IP address of the secondary DNS server here.
Management VLAN	Select the VLAN in which web-based management is to be accessible. Value “1” is set by default. You can set up further management VLANs via CLI. However, it is recommended that you keep management VLAN 1.
DHCP Configuration	This option is only available if you selected “STATIC” for “IP Address Assignment”. Click “DHCP Services” to open the .

Network:Hostname Configuration

Tabelle 3-18 Hostname Configuration: Parameters

Parameters	Description
Name resolution	Select whether you want to activate DNS name resolution via mDNS and LLMNR. If you activate the function, you can also access the device via the host name (e.g., http://WLAN-dd5d5c.local/).
Hostname	Enter the host name of your device here. The host name must have between two and 63 characters. Alphanumeric characters and dashes are permitted. A host name must not start with a dash. In the default configuration, this host name is made up of the product family name and part of the device MAC address. See DNS-Host-Name).

When you deactivate DNS name resolution, it may take some time until the device can be accessed via the host name. This is due to the DNS cache.

3.3.6 WLAN setting

The “WLAN Setting” page allows you to configure the WLAN network with basic WLAN settings such as the WLAN frequency band used or the channel bandwidth.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Setting”.

Figure 3-19 WLAN setting

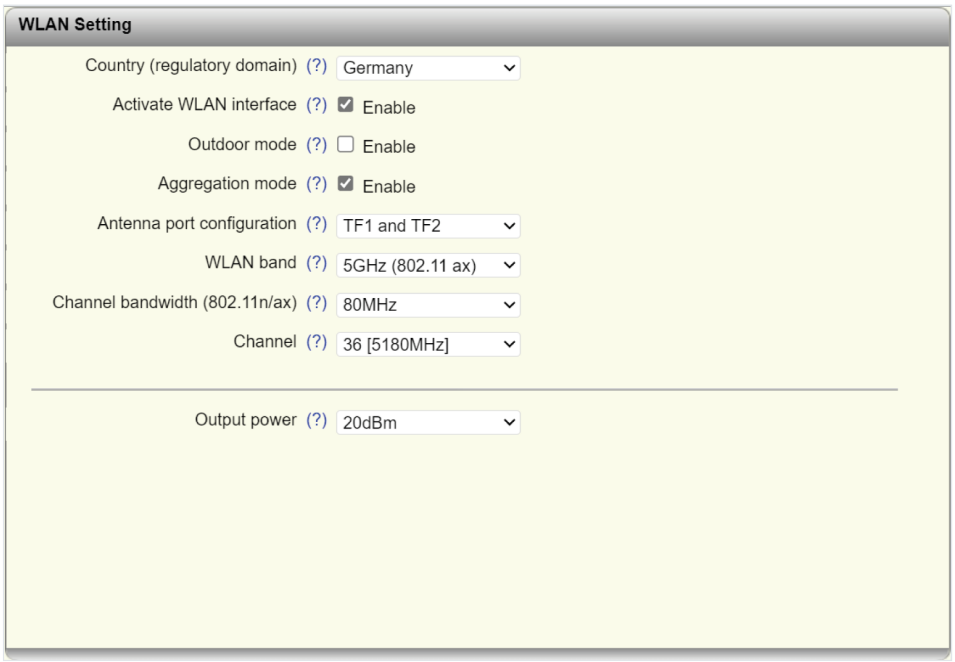


Tabelle 3-19 WLAN setting: Parameters

Parameters	Description
Country (regulatory domain)	Select the country where the device will be used. This selection is mandatory in order to operate the device in compliance with approvals in different countries. If you select a different country, this may constitute a breach of the law. Please note the different country-specific approvals for the device versions. Further information on this can be found in the corresponding installation manual.
Activate WLAN interface	Activate the check box to activate the WLAN interface. If the WLAN interface is deactivated, no communication can take place over the interface.
Outdoor mode	If you operate the device outdoors in the European Union or the European Economic Area (EEA) and use the 5 GHz band, you must activate the check box. The

Parameters	Description
	device will then be operated on the prescribed DFS (Dynamic Frequency Selection) channels.
Aggregation mode	Activate the check box to aggregate multiple data packets. This increases the user data part of a WLAN packet and the utilization of the transmission capacity.
Antenna port configuration	This option is only available on the FL WLAN 102x devices. Select whether one or two antenna connections should be activated. **NOTE: Damage** Only activate the connections to which antennas are connected. Activating antenna connections without connected antenna can cause damage to the connections.
WLAN band	Here, select the desired WLAN frequency band. – 2.4 GHz (802.11 b) – 2.4 GHz (802.11 b/g) – 2.4 GHz (802.11 g/n) – 2.4 GHz (802.11 ax) – 5 GHz (802.11 a) – 5 GHz (802.11 a/n) – 5 GHz (802.11 ax) Note that this setting only takes effect in the “Access Point” and “Mesh” operating modes. Settings for the “Client” operating mode can be made via “Configuration, WLAN Interfaces, Roaming List”, see Operating mode: Client.
Channel bandwidth	Activate the desired radio button for the channel bandwidth. – 20 MHz: The device is operated on one channel. – 40 MHz: The device is operated on two channels (channel bonding). This increases the data rate, but requires two channels. – 80 MHz: The device is operated on four channels (channel bonding). Only available for frequency band 5 GHz (802.11 ax). – 160 MHz: The device is operated on eight channels (channel bonding). Only available for frequency band 5 GHz (802.11 ax).
Channel	Select the desired channel here.

Parameters	Description
	Note that this setting only takes effect in the “Access Point” and “Mesh” operating mode. Settings for the “Client” operating mode can be made via “Configuration, WLAN Interfaces, Roaming List”, see *Operating mode: Client*. Please note that you should configure the “Channel” option last. Different channels are available for selection depending on which option you have selected in the previous parameters. Then confirm your selection with “Apply”. When operating as an “access point” on two or more channels (“channel bonding”), the device automatically changes the primary channel if necessary and does not use the set channel for this. Therefore, activate all channels used in the “Roaming List” on the client.
Output power	Here, select the desired transmission power. – FL WLAN 112x: The transmission power is the effectively radiated power including the antenna gain. – FL WLAN 102x: The transmission power is the power at the antenna connection. The power that is set here can be automatically reduced by the device. This is done as a function of frequency and modulation type depending on the power of the WLAN module.

3.3.7 WLAN interface

The “WLAN Interface” page allows you to configure the WLAN interface. You can make settings such as the network SSID or the encryption method here.

Bei der Konfiguration von zwei virtuellen Funkschnittstellen sollten Sie immer "WLAN 2" als normalen Access Point konfigurieren. "WLAN 1" können Sie wahlweise als Access Point oder Client konfigurieren.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.

Figure 3-20 WLAN interface

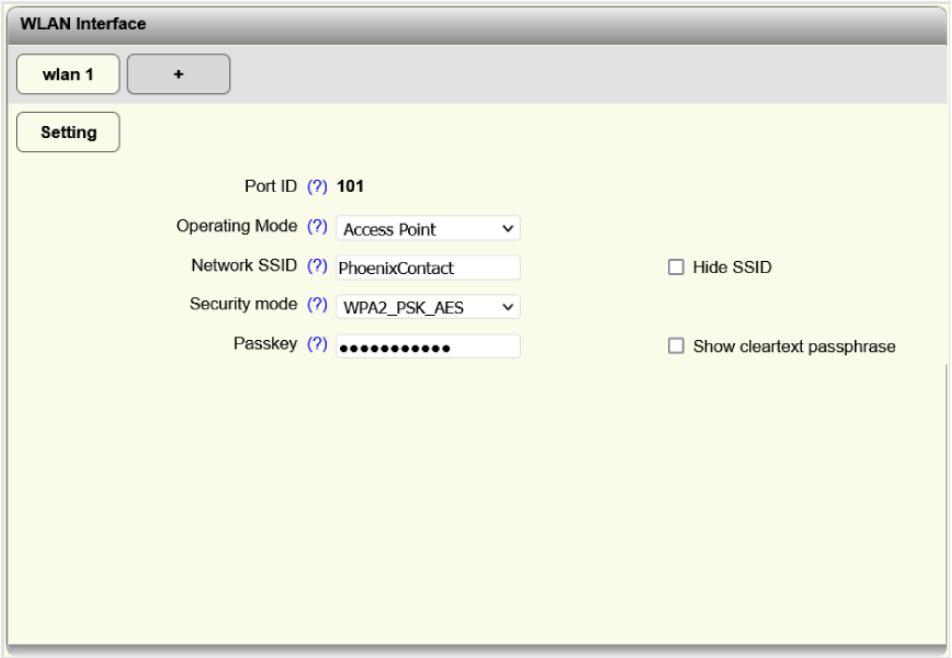


Tabelle 3-20 WLAN interface: Parameters

Parameters	Description
Operating Mode	Here, select the desired operating mode. – Access point – Access Point (VXLAN) – Client (Fully transparent bridge) – Client (Single client bridge) – Client (Multi client bridge) – Client (NAT) – Client (VXLAN) For further information about the various operating modes and the associated setting options, see *Device operating modes*.

The other parameters on this page depend on the selected operating mode and are dealt with in the corresponding section (see *Device operating modes*).

3.3.8 Service

On the “Service” page, you can activate and deactivate various interfaces and displays, for example, the CLI service, the LEDs, or the SNMP agent.

NOTE: Network security at risk
Deactivate unused interfaces to prevent unauthorized access.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, Service”.

Figure 3-21 Service

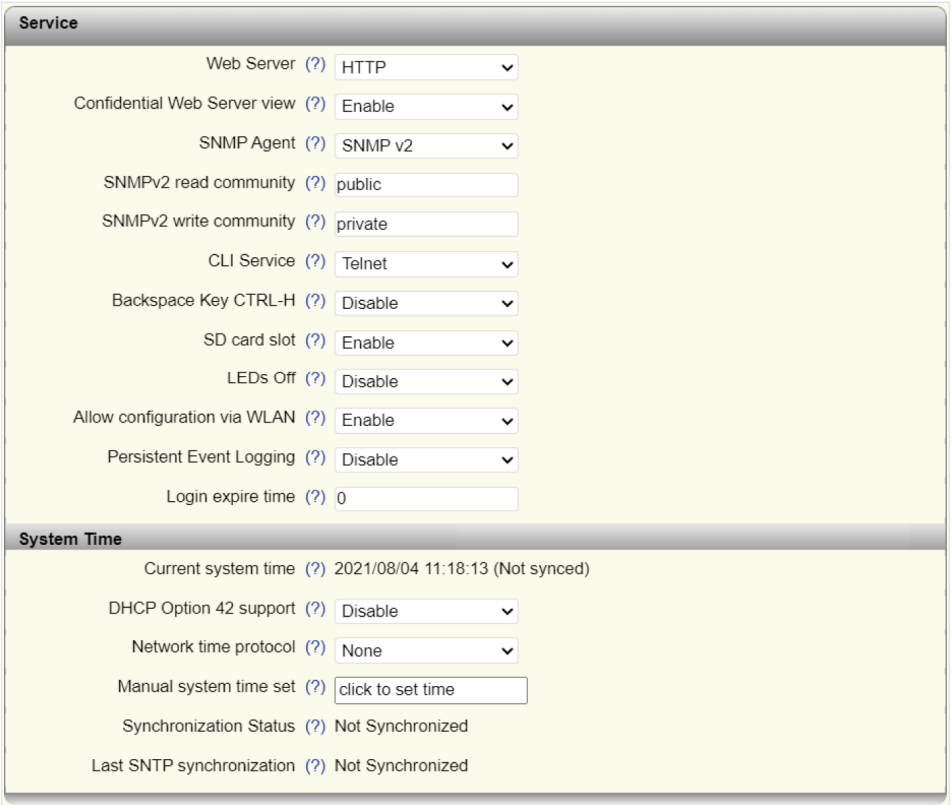


Tabelle 3-21 Service: Parameters

Parameters	Description
Web Server	Select here whether the web server functionality should be activated. – Disable: The web server is disabled. Access to web-based management is disabled. – HTTP: The web server is enabled in “HTTP” mode. The connection is not secured. – HTTPS: The web server is enabled in “HTTPS” mode. Use “https://” to access web-based management. The connection is secured. If you disable the web server, web-based management can no longer be accessed.
Confidential Web Server view	Select here whether the “Information” area in web-based management should be visible without login. – Disable: The “Information” area of web-based management is visible without login data. Access to

Parameters	Description
	other areas is controlled using user roles (see User Management). – Enable: Web-based management is only visible with previous login.
SNMP Agent	Select the SNMP server functionality here (see SNMP). – Disabled: The SNMP server is disabled. – SNMP v2: The SNMP server is enabled in “SNMP v2” mode. SNMP 1 is also supported in this mode. – SNMP v3: The SNMP server is enabled in “SNMP v3”. **NOTE: Network security at risk** SNMPv2 is not a secure encryption method.
SNMPv2 read community	This option is only available if you selected “SNMP v2” for “SNMP Agent”. Enter the string for the SNMPv2 read community here. This password (default value: “public”) must be entered for read access to objects.
SNMPv2 write community	This option is only available if you selected “SNMP v2” for “SNMP Agent”. Enter the string for the SNMPv2 write community here. This password (default value: “private”) must be entered for read and write access to objects. **NOTE: Change the default password** Unauthorized access is possible with the default password. • Change the password immediately after the first login. • Do not share the password.
SNMPv3 Authentication	This option is only available if you selected “SNMP v3” for “SNMP Agent”. Select the desired authentication mode for SNMPv3 here. The first part of the selection (MD5 or SHA) is the authentication protocol based on hash values. The second part (DES or AES) represents the encryption protocol. – MD5/DES:Default – SHA/AES – SHA/DES – MD5/AES For AES protocol, only AES-128 is supported.
CLI Service	Select here whether the input of CLI commands via Telnet or Secure Shell should be enabled. – Disable:Entry of CLI commands is disabled.

Parameters	Description
	– Telnet: The input of CLI commands via Telnet is enabled. – SSH: The input of CLI commands via Secure Shell (SSH) is enabled. For information about configuration and diagnostics via the Command Line Interface (CLI), refer to the separate manual at phoenixcontact.net/qr/<item number>.
Backspace Key CTRL-H	Select here whether the key combination Ctrl+H should additionally be used as a backspace function. Some terminal programs use the backspace key as Delete. If you enable this option, you can instead use the Ctrl+H key combination in your terminal program to delete the last character.
SD card slot	Select whether the SD card slot should be disabled, enabled, or encrypted. – Disable: The SD card slot is disabled. – Enable: The SD card slot is enabled. – Secure: Data is saved encrypted to the SD card. To use an SD card with encrypted data on other devices, you need a common root CA certificate.
LEDs Off	Select here whether the LEDs on the device should be active. – Select “Enable” to disable the LEDs. – Select “Disable” to enable the LEDs.
Allow configuration via WLAN	Select here whether configuration via the WLAN interface should be possible. If you disable configuration via the WLAN interface, configuration via the interface is not possible. The interface is required, for example, for configuring Profisafe applications. The other configuration interfaces are still available.
Persistent Event Logging	Select here whether the persistent storage of events should be enabled. This means that events are not deleted when the device is restarted.
Login expire time	Enter the time until automatic logout here. You can set a number between 30 and 3,600 seconds. The default value is 1,200 seconds. If you set a value of “0”, automatic logout is disabled.

Service:System time

Tabelle 3-22 System Time: Parameters

Parameters	Description
Current system time	The current system time is displayed here. “Not synced” means that the system time has either been configured manually or it has not been synchronized with an (S)NTP server. The device does not have a battery-backed real-time clock. If the time is not synchronized, there may be discrepancies between the system time and the actual time.
DHCP Option 42 support	Select whether the IP address of one or more SNTP servers is to be received via DHCP. If the device receives the IP addresses for the “Primary SNTP server” and “Secondary SNTP server” via DHCP, they are stored in the corresponding parameters and displayed. The “Primary server description” and “Secondary server description” is automatically changed to “Set by DHCP Option 42”.
Network time protocol	Select a protocol here for synchronizing the time via a web server. – None: No synchronization via web server. You can set the time manually. – Unicast: You must configure at least one SNTP server for this option. – Broadcast: With this option, the device listens to all broadcasts from broadcast SNTP servers.
Manual system time set	This option is only available if you selected “None” for “Network time protocol”. Select “click to set time” to set the device system time manually. You can set the current date and the current time.
Primary SNTP server	This option is only available if you selected “Unicast” for “Network time protocol”. Enter the IP address of your SNTP server here. SNTP stands for Simple Network Time Procotol and is a time synchronization protocol used to synchronize the system time in networks.
Primary server description	This option is only available if you selected “Unicast” for “Network time protocol”. Enter a description of your SNTP server here.

Parameters	Description
Secondary SNTP server	This option is only available if you selected “Unicast” for “Network time protocol”. Enter the IP address of your secondary SNTP server here. SNTP stands for Simple Network Time Protocol and is a time synchronization protocol used to synchronize the system time in networks. If the primary server is not accessible, the secondary SNTP server will be used.
Secondary server description	This option is only available if you selected “Unicast” for “Network time protocol”. Enter a description of your secondary SNTP server here.
UTC offset	This option is only available if you selected “Unicast” or “Broadcast” for “Network time protocol”. Enter the difference from the coordinated world time (UTC) for your time zone here.
Synchronization Status	The current status of synchronization with the SNTP server is displayed here.
Last SNTP synchronization	The time of the last synchronization with the SNTP server is displayed here.

3.3.9 Multicast filtering

On the “Multicast Filtering” page, you can make settings for the Internet Group Management Protocol (IGMP). The network protocol is used to organize and manage multicast groups. A device with activated IGMP snooping, which is called a querier, eavesdrops on the multicast data traffic in the network and forwards the multicasts only to the devices the information is intended for. This increases the information security in the network and reduces the data traffic.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, Multicast Filtering”.

Figure 3-22 Multicast filtering

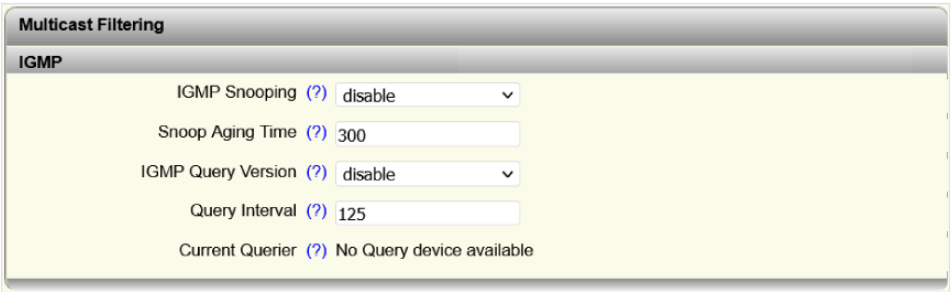


Tabelle 3-23 Multicast filtering: Parameters

Parameters	Description
IGMP Snooping	Here, select whether the “IGMP Snooping” function should be activated.
Snoop Aging Time	Here, enter the snoop aging time. The snoop aging time is the period of time during which the querier waits for membership reports. If no membership reports are received during this time, the associated ports are removed from the multicast groups. The value must be between 30 and 86,400 (default: 300).
IGMP Query Version	Here, select the IGMP query version that the device should use to send the queries. The devices support IGMP query versions v1 and v2. For EtherNet/IP applications, it is recommended that you activate version v2.
Query Interval	Here, enter the interval at which the device should send the queries. The value must be between ten and 3600 seconds.
Current Querier	The IP address of the current querier in the network is displayed here.

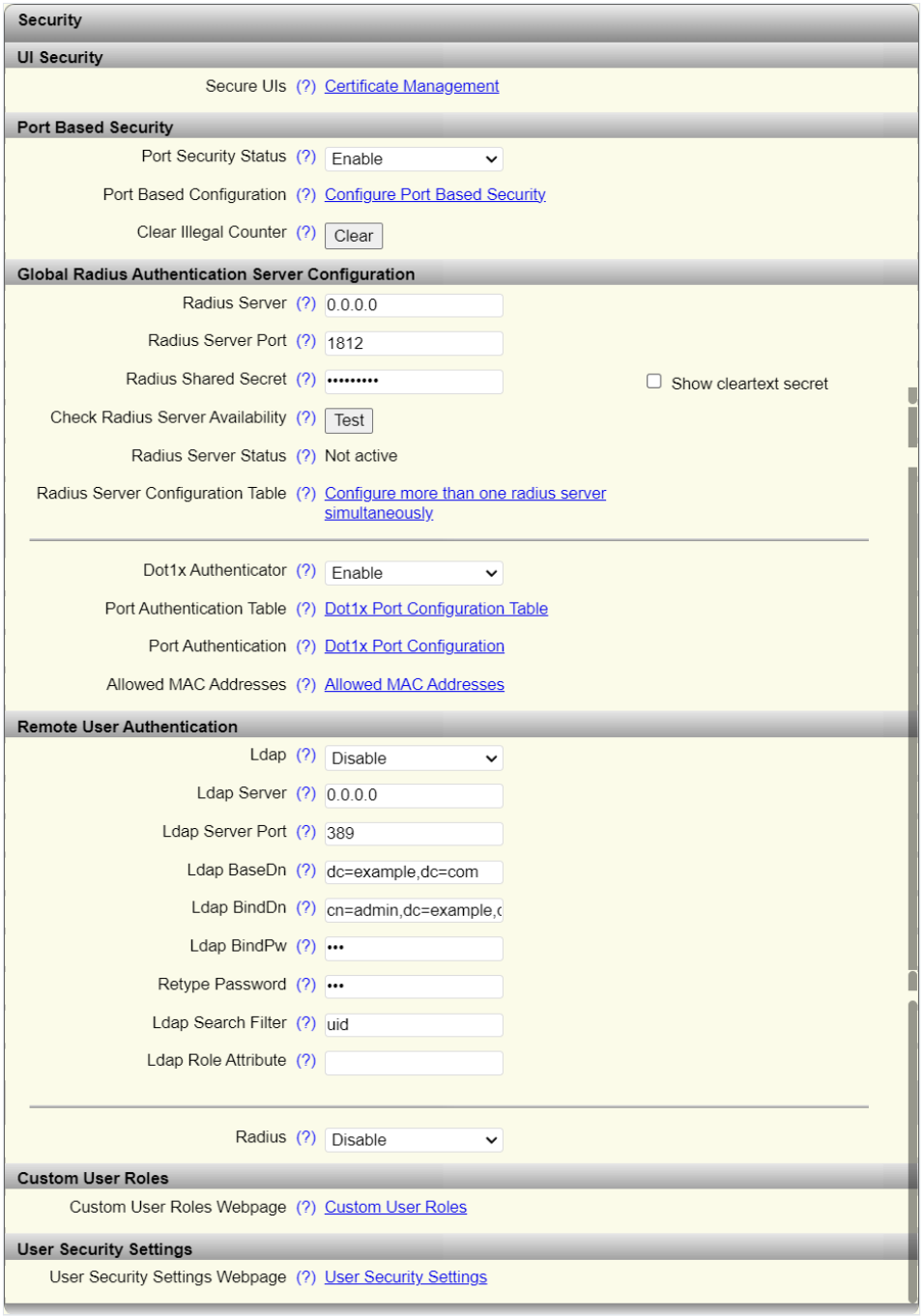
3.3.10 Security

On the “Security” page, you can make numerous settings related to security and network access.

NOTE: Network security at risk
Make sure that the configuration is secure to prevent unauthorized access to your network. More information is available in the AH EN INDUSTRIAL SECURITY application note. The application note can be downloaded at phoenixcontact.net/qr/<item_number>.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, Security”.

Figure 3-23 Security



Security: UI Security

Tabelle 3-24 UI Security: Parameters

Parameters	Description
Secure UIs	Click “Certificate Management” to open the “Certificate Management” pop-up window (see Pop-up window: Certificate Management). You can create the necessary keys and certificates here for operation with HTTPS and SSH.

Security: Port Based Security

Tabelle 3-25 Port Based Security: Parameters

Parameters	Description
Port Security Status	Select whether port-based security should be activated globally.
Port Based Configuration	Click “Configure Port Based Security” to open the “Port Based Configuration” pop-up window (see Pop-up window: Port Based Security).

Security: Global Radius Authentication Server Configuration

Tabelle 3-26 Global Radius Authentication Server Configuration: Parameters

Parameters	Description
Radius Server	Enter the IP address of the RADIUS server here.
Radius Server Port	Enter the port of the RADIUS server here.
Radius Shared Secret	Enter the shared secret that is required for encrypted communication with the RADIUS server here. The shared secret must have between eight and 64 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?[]{}+*-_<>#^.,:~|
Check Radius Server Availability	Click “Test” to check whether the configured RADIUS server is available.
Radius Server Status	The status of the RADIUS server that can be checked via “Check Radius Server Availability” is displayed here.
Radius Server Configuration Table	Click “Configure more than one radius server simultaneously“ to open the “Radius Server Configuration Table” window (see Pop-up window: Radius Server Configuration Table). Here you can configure up to five RADIUS servers.

For further information on RADIUS certificates, see *RADIUS certificates*.

Security: Remote User Authentication

When a user logs in, databases are searched for a valid user name and password combination, where the user rights are also correctly assigned. The local database is searched first. Then, the LDAP is searched, followed by the RADIUS database (if activated and configured in each case). If a valid combination is found, the search is terminated and the user is logged in.

Security:Custom user roles

Tabelle 3-27 Custom User Roles: Parameters

Parameters	Description
Custom User Roles webpage	Click “Custom User Roles” to open the “Custom User Roles” pop-up window. Here, you can define the

Parameters	Description
	desired permissions for each role (see Pop-up window: Custom User Roles).

Security:User security settings

Tabelle 3-28 User Security Settings: Parameters

Parameters	Description
User Security Settings Webpage	Click “User Security Settings” to open the “User Security Settings” pop-up window. There, you can define minimum requirements for user passwords, e.g., each password must contain a special character (see Pop-up window: User security settings).

3.3.10.1 Certificate management

Figure 3-24 Pop-up window: Certificate Management

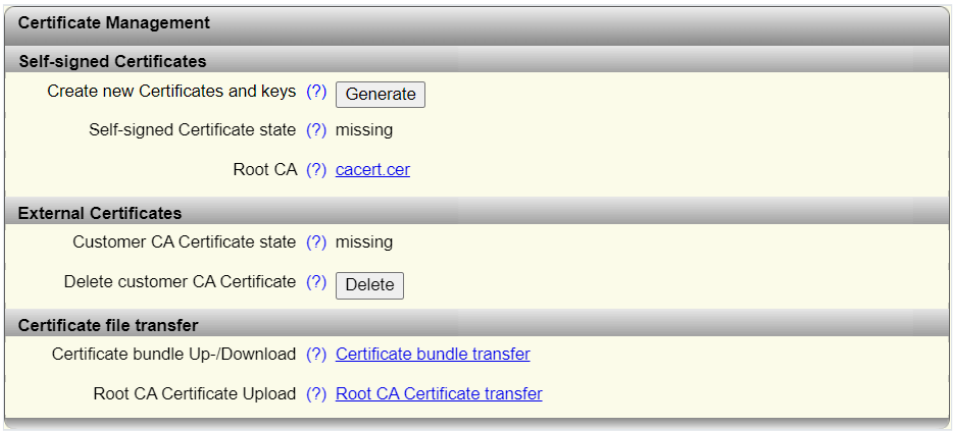


Tabelle 3-29 Pop-up window: Certificate management: Parameters

Parameters	Description
Create new Certificates and keys	Click “Generate” to create all the necessary keys and certificates for operation with HTTPS and SSH.
Self-signed Certificate state	The current availability of the security context is displayed here.
Root CA	Click “cecert.cer” to download the root CA certificate created for the installation from the device.
Customer CA Certificate state	The current status of the customer CA certificate is displayed here. You can store your own signed certificate. Your browser’s security warnings will then no longer be triggered.
Delete Customer CA Certificate	Click “Delete” to delete your own signed certificate.
Certificat bundle Up-/ Download	Click “Certificate bundle transfer” to open the “File Transfer” pop-up window (see).

Parameters	Description
Root CA Certificate Upload	Click “Root CA Certificate transfer” to open the “File Transfer” pop-up window (see).

3.3.10.2 Port-based security

All configurations in the “Port Based Security” pop-up window only become effective if the “Port Security Status” function is activated on the “Security” page (see Security: Port Based SecuritySecurity: Port Based Security).

Settings in this pop-up window are only possible if you selected “Access Point” as the device operating mode, see *Device operating modes*.

Figure 3-25 Pop-up window: Port-based security

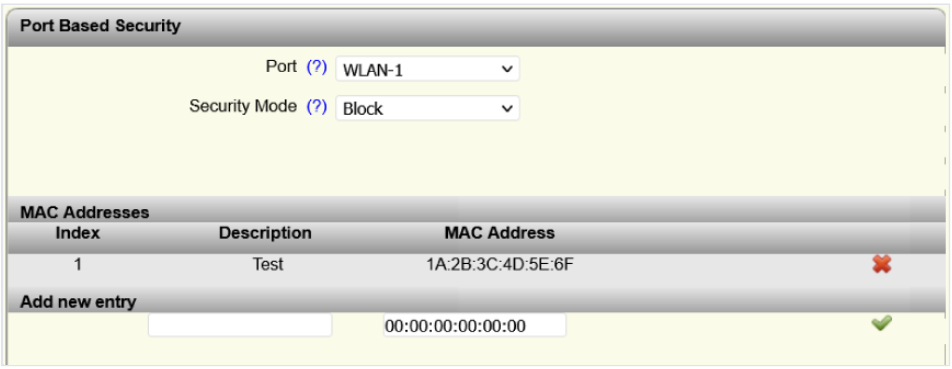


Tabelle 3-30 Pop-up window: Port-based security: Parameters

Parameters	Description
Port	Select the port or interface for which you want to make security settings.
Security Mode	Select what is to happen if a MAC address that is not permitted is detected by the device. – None: There are no security settings for this port. Unknown MAC addresses are not blocked. – Block: All WLAN devices with an unknown MAC address are blocked. WLAN devices whose MAC address is on the allowlist are allowed. – Pass: All WLAN devices with an unknown MAC address are allowed. WLAN devices whose MAC address is on the denylist are blocked. – IP allowlist: The data traffic is blocked with the exception of the IP addresses on the list. The destination IP and TCP/UDP port are taken into account (all or 1 to 65535).
Add new entry	Enter the description and MAC address of the WLAN device that you want to add to the allowlist or denylist in accordance with your setting for “Security Mode”.

3.3.10.3 Radius Server Configuration Table

Figure 3-26 Pop-up window: Radius Server Configuration Table

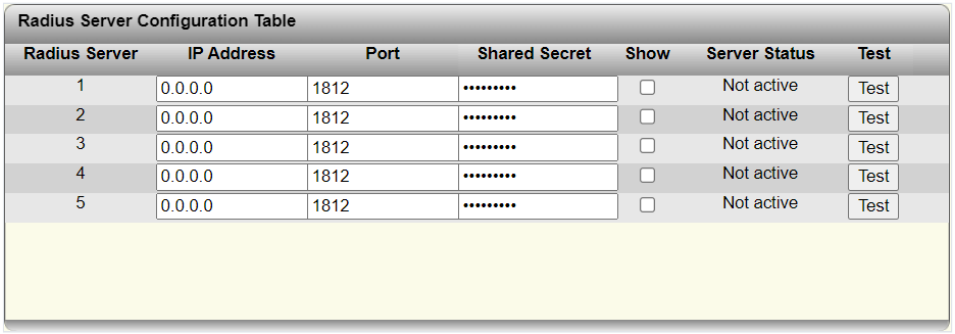


Tabelle 3-31 Pop-up window: Radius Server Configuration Table: Parameters

Parameters	Description
Radius Server	The ID of the RADIUS server is displayed here.
IP Address	Enter the IP address of the RADIUS server here.
Port	Enter the port of the RADIUS server here.
Shared Secret	Enter the shared secret that is required for encrypted communication with the RADIUS server here. The shared secret must have between eight and 64 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?[]{}+*-_<>#^.,:~|
Show	Select the check box to display the shared secret.
Server Status	The status of the RADIUS server that can be tested via “Test” is displayed here.
Test	Click “Test” to check whether the configured RADIUS server is available.

3.3.10.4 Custom user roles

Figure 3-27 Pop-up window: Custom User Roles

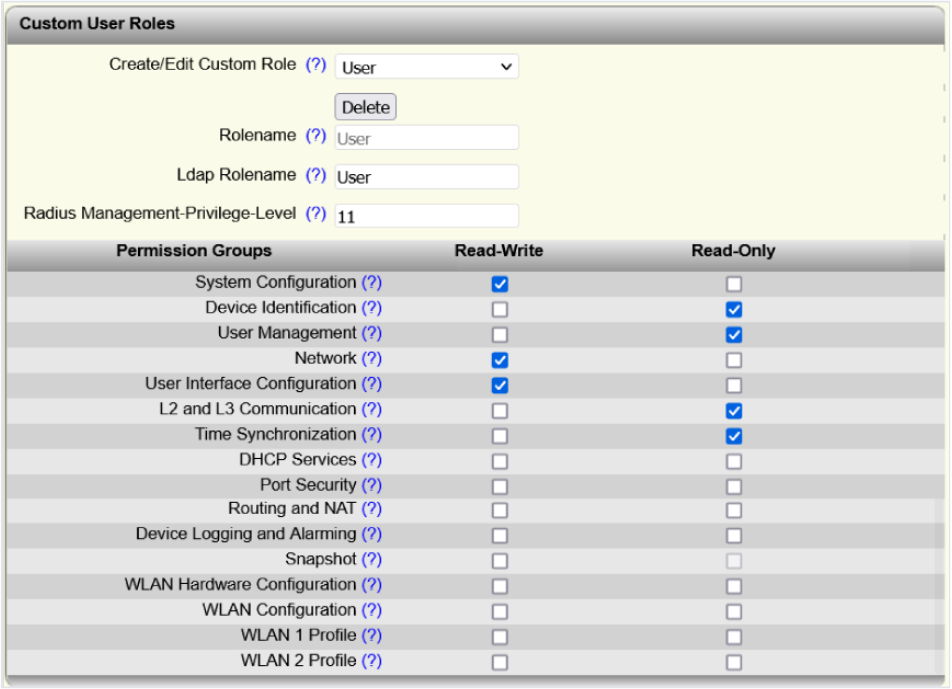


Tabelle 3-32 Pop-up window: Custom user roles: Parameters

Parameters	Description
Create/Edit Custom Role	Select the user account that you wish to edit or delete. Select “Create” to create a new user account.
Delete	Click “Delete” to delete the currently selected role. This action cannot be undone. The preconfigured “Admin”, “Expert”, and “Read-only” roles cannot be deleted.
Rolename	Enter the desired name for the user role in the text field. The name for the user role can have up to 32 characters. Letters, numbers, and the following special characters are permitted: -_.@. Once the role name has been created, it can no longer be changed.
Ldap Rolename	The LDAP role name is made available to a user via the LDAP server. The role name is used to assign a user to a user role and therefore to assign rights on the device. The LDAP role name is mapped to a local user role here. For further information on LDAP, see .
Radius Management-Privilege-Level	You can enter a numerical value here that is made available to a user via the RADIUS server during

Parameters	Description
	server-based authentication. This value is used to assign a user to a user role and therefore to assign rights on the device. The management privilege level is mapped to a local user role here. For further information on RADIUS, see .
Permission Groups	In the table, you can assign and edit the read and write permissions for user-defined user roles. The predefined permissions for the “Admin”, “Expert”, and “Read-only” roles available by default cannot be changed. – Read-Write: Select the respective check box to assign read and write permissions for the function group to the selected user role. – Read-Only: Select the respective check box to assign read permissions for the respective function group to the selected user role. – No selection: If you do not select either of the two check boxes for a function group, the user role does not receive any right for this function group.

For further information on user roles and permissions, see *Creating user roles*.

3.3.10.5 User security settings

Figure 3-28 Pop-up window: User security settings

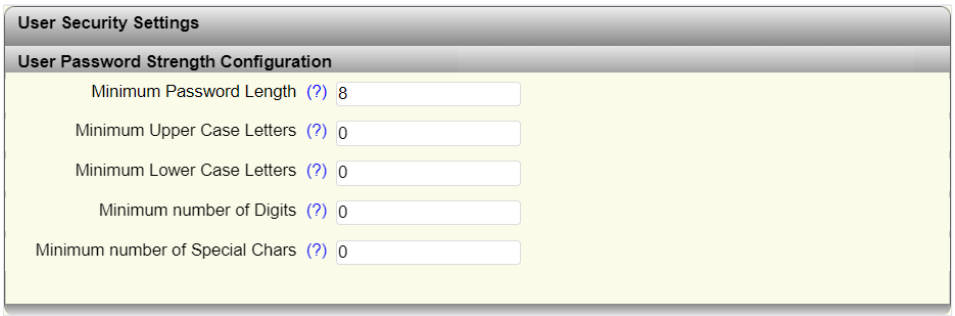


Tabelle 3-33 Pop-up window: User security settings: Parameters

Parameters	Description
Minimum Password Length	Enter the desired minimum length for passwords here. The value can be between eight and 64 characters (default: 8).
Minimum Upper Case Letters	Enter the desired minimum number of uppercase letters (A-Z) here. The value can be between zero and eight characters (default: 0).
Minimum Lower Case Letters	Enter the desired minimum number of lowercase letters (a-z) here. The value can be between zero and eight characters (default: 0).

Parameters	Description
Minimum number of Digits	Enter the desired minimum number of digits (0-9) here. The value can be between zero and eight characters (default: 0).
Minimum number of Special Chars	Enter the desired minimum number of special characters (e.g., .#:!?). here. The value can be between zero and eight characters (default: 0).

3.4 WBM Diagnostics area

3.4.1 Channel allocation (only Access Point operating mode): Diagnostics of WLAN channel assignment

If the device is in access point operating mode, it is possible to detect other WLAN networks that are within range. The WLAN channels used and the number of networks per channel are represented as a graphic. In this way, you can, for example, find a free channel for your own WLAN network.

Requirement:

The device is in access point operating mode.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Diagnostics, Channel Allocation”.
- Click the “Scan” button.

↪ WLAN networks in range are displayed as graphs.

Figure 3-29 Channel allocation:Display of WLAN channel assignment at the access point

3.4.2 RSSI graph

If the device is in access point, client, or repeater operating mode, the current WLAN signal strength of the connected devices can be displayed. This function can be used to determine the signal strength when setting up wireless paths.

Thanks to the dynamic display, it is possible to determine the signal strength of the connected devices at various locations (e.g., mobile clients).

3.4.2.1 Displaying the WLAN signal strength as an RSSI graph

Requirement:

The device is in access point, client, or repeater operating mode.

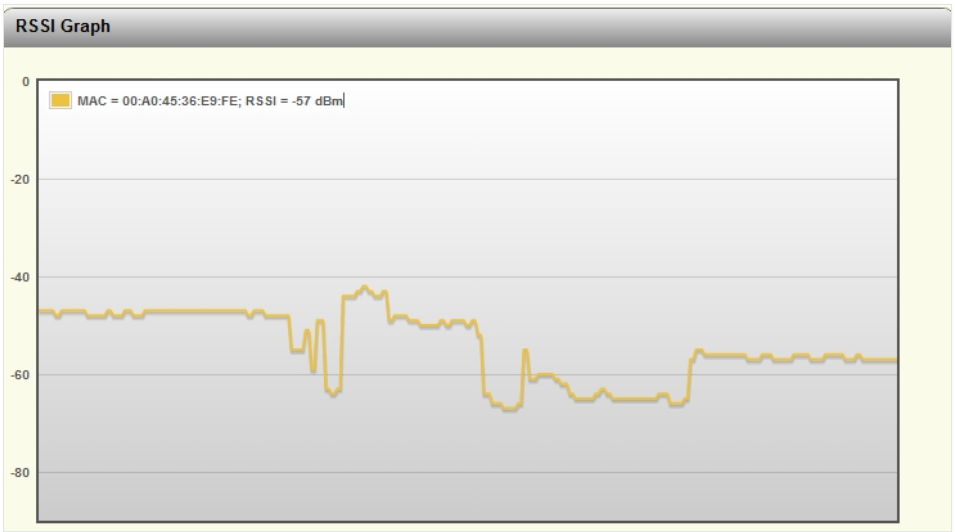
- Open web-based management (see Accessing web-based management) and log in.
- Click “Diagnostics, RSSI Graph”.

↪ The current signal strength value of the connected device is displayed as a graph.

In Client operating mode: The RSSI (Radio Signal Strength Indication) value indicates the signal strength of the connected access point at the client location in dB.

In Access Point operating mode: The MAC address of the connected devices and the current WLAN signal strength (RSSI) are displayed at the top of the window.

Figure 3-30 RSSI graph: Display of the current WLAN strength on the client



The RSSI value is only displayed and updated while the web page is open. When you leave the web page, the display is cleared.

3.4.2.2 Displaying the WLAN signal strength as a bar graph

Requirement:

There must be an active connection between the device and other devices (access point or client depending on the operating mode).

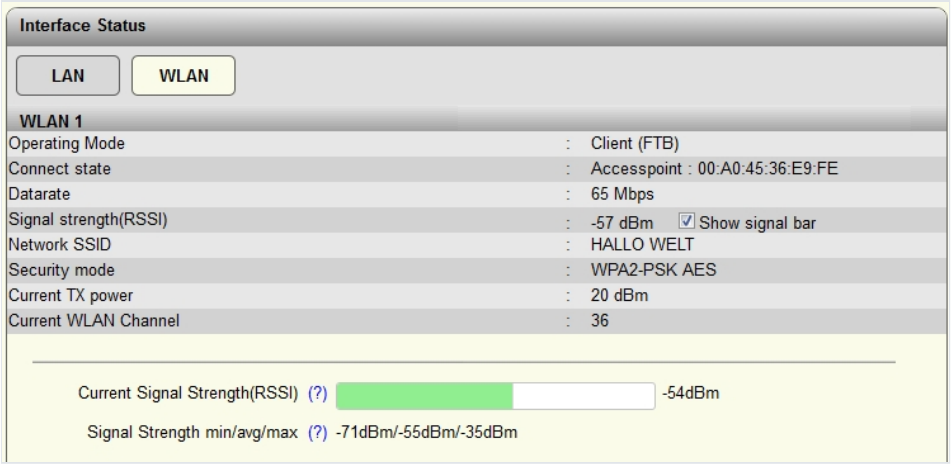
- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Interface Status, WLAN”.
- Activate the “Show signal bar” check box (see Figure).

↪ The current signal strength value of the connected device is displayed as a bar graph.

The current signal strength in dBm is displayed to the right of the bar graph. The average signal strength as well as maximum and minimum values during the current measuring period are displayed below the bar graph.

The RSSI value is only displayed and updated while the web page is open. When you leave the web page, the display is cleared.

Figure 3-31 Display of the current signal strength as a bar graph



3.4.3 Trap Manager

On the “Trap Manager” page you can configure the Trap Manager, which provides notifications when specific events occur. For example, you can be informed about a password change or a firmware change and in this way detect unauthorized access more easily.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Diagnostics, Trap Manager”.

Figure 3-32 Trap Manager

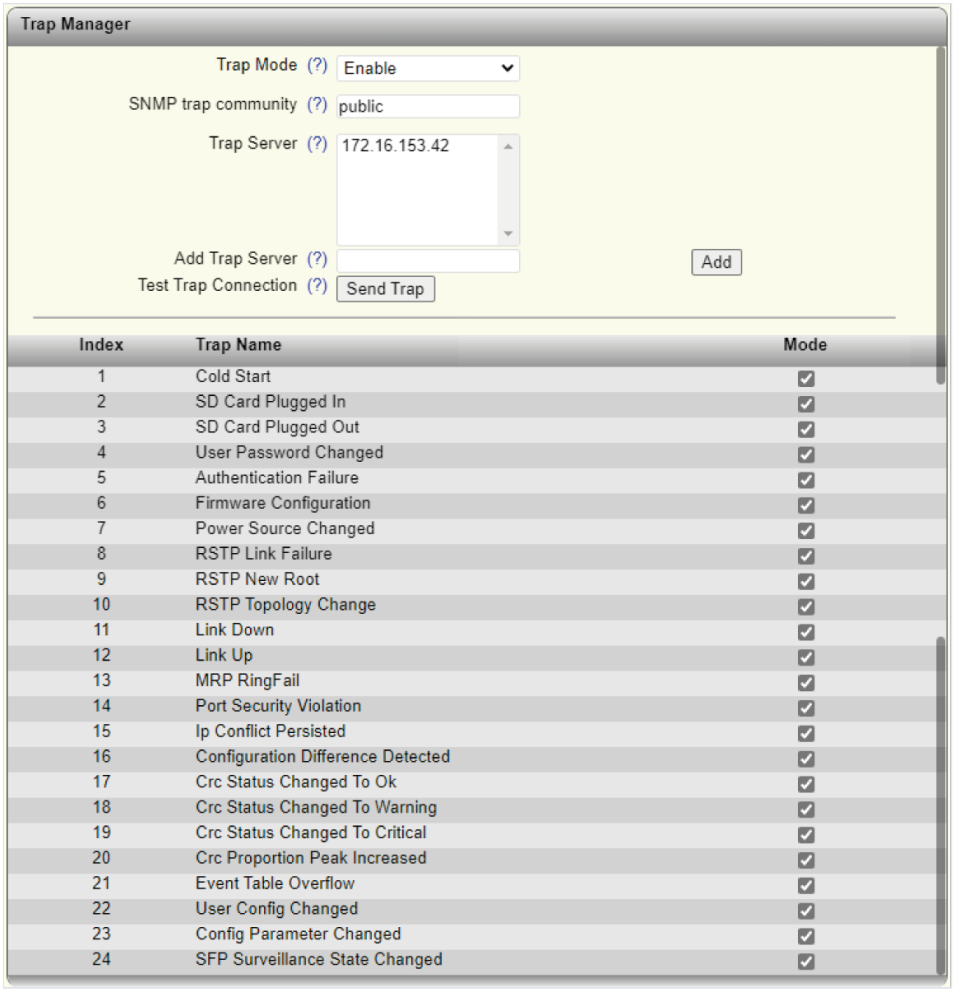


Tabelle 3-34 Trap Manager: Parameters

Parameters	Description
Trap Mode	– Enable: Sending of SNMP traps is activated. – Disable: Sending of SNMP traps is deactivated.
SNMP trap community	Here, enter the name or string of the SNMP trap community.
Trap Server	All trap servers that are to receive SNMP traps from this device are displayed here.
Add Trap Server	Here, enter the IP address or DNS name of a trap server. Click “Apply&Save” to add this trap server.
Test Trap Connection	Click on “Send Trap” to test the connection to the trap server.

The table lists the SNMP traps that the device can send. Select the actions for which SNMP traps are to be sent.

3.4.4 Snapshot

On the “Snapshot” page, you can save device configurations and logs with a click for diagnostic purposes and then download them to send to a service technician for analysis.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Diagnostics, Snapshot”.
- Click the “Snapshot” button.

↪ The snapshot of the device is created.

- Click “File transfer” to download the snapshot (see *File transfer*).

Figure 3-33 Snapshot

Tabelle 3-35 Snapshot: Parameters

Parameters	Description
Take snapshot	Click “Snapshot” to create a snapshot of the current device configuration.
Current snapshot state	The snapshot status is displayed here, e.g., whether the status is currently being generated, is available, or does not exist.
Timestamp of last snapshot	The time at which the last snapshot was generated is displayed here.
Download of snapshot file	Click “File transfer” to download the snapshot (see).

3.4.5 Syslog for diagnostic purposes

On the “Syslog” page, you can transmit messages or events to one or more servers via UDP. This allows you to analyze the environment and the quality of the connection.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Diagnostics, Syslog”.

Figure 3-34 Syslog

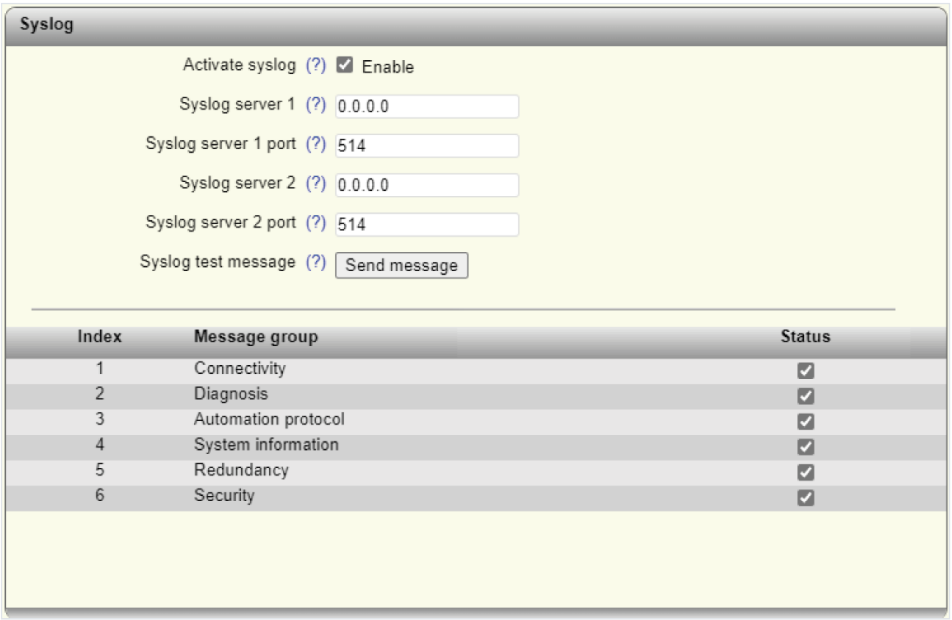
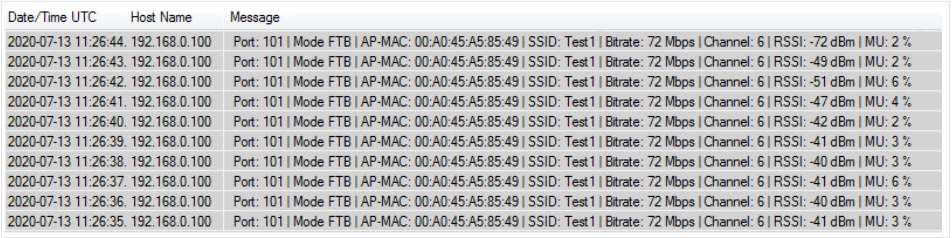


Tabelle 3-36 Syslog: Parameters

Parameters	Description
Activate syslog	Select the check box to activate the Syslog functionality.
Syslog server 1	Enter the IP address or the DNS name of the first Syslog server here.
Syslog server 1 port	Enter the UDP port of the first Syslog server here. Default: 514.
Syslog server 2	Enter the IP address or the DNS name of the second Syslog server here. If you configure two Syslog servers, all device messages and events are sent to both servers.
Syslog server 2 port	Enter the UDP port of the second Syslog server here. Default: 514.
Syslog test message	Click “Send message” to test the connection to the Syslog server. With Syslog, the server does not confirm the receipt of messages. Therefore the connection status can only be checked on the server, and not in web-based management of the device.
Status	Select the check boxes in the “Status” column to select those categories whose events are to be sent to the Syslog server.

Figure 3-35 Received data on a Syslog recipient (example)



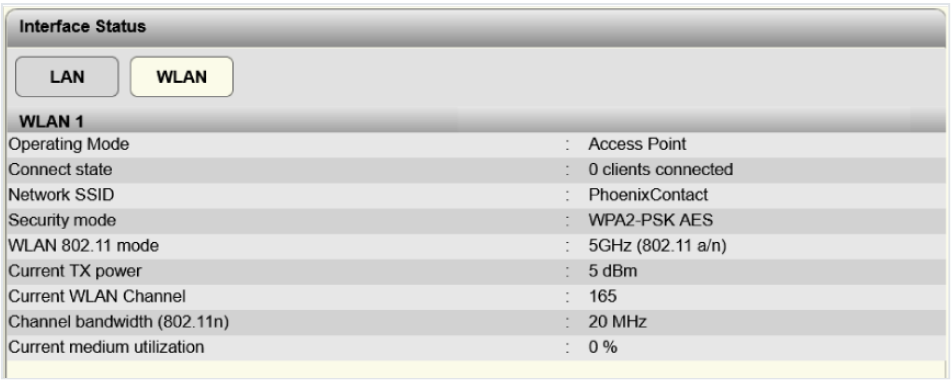
Date/Time UTC	Host Name	Message
2020-07-13 11:26:44.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -72 dBm | MU: 2 %
2020-07-13 11:26:43.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -49 dBm | MU: 2 %
2020-07-13 11:26:42.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -51 dBm | MU: 6 %
2020-07-13 11:26:41.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -47 dBm | MU: 4 %
2020-07-13 11:26:40.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -42 dBm | MU: 2 %
2020-07-13 11:26:39.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -41 dBm | MU: 3 %
2020-07-13 11:26:38.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -40 dBm | MU: 3 %
2020-07-13 11:26:37.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -41 dBm | MU: 6 %
2020-07-13 11:26:36.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -40 dBm | MU: 3 %
2020-07-13 11:26:35.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -41 dBm | MU: 3 %

3.4.6 Channel assignment/CST

In web-based management you can view the current channel assignment.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Information, Interface Status, WLAN”.

Figure 3-36 Interface status: Channel assignment



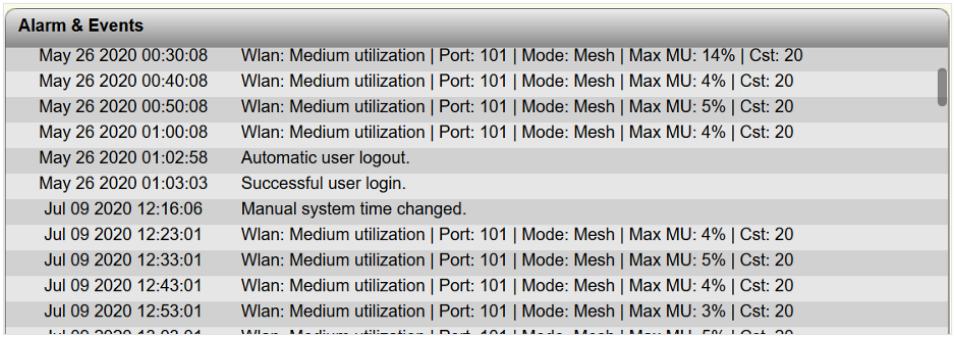
↪ The “Current medium utilization” option shows the current channel assignment.

The display shows the current value at the time when the page was accessed. The display is not automatically refreshed.

You can repeatedly view the maximum channel assignment (Max MU) of the last ten minutes in percent in the event log.

- Click “Information, Alarm & Events”.

Figure 3-37 Alarm and events: Channel assignment



– Max MU: Channel assignment is determined in the device every five seconds. The highest of these values within ten minutes is logged.
– Cst: Carrier sense timeout (Cst) describes the number of media access operations that did not take place. In these moments, the data packet could not be transmitted. The value is incremented until the next device start. It can therefore reach very high values after the device has been running for a long time. The moment when the counter increases can indicate an access problem to a diagnostics expert.

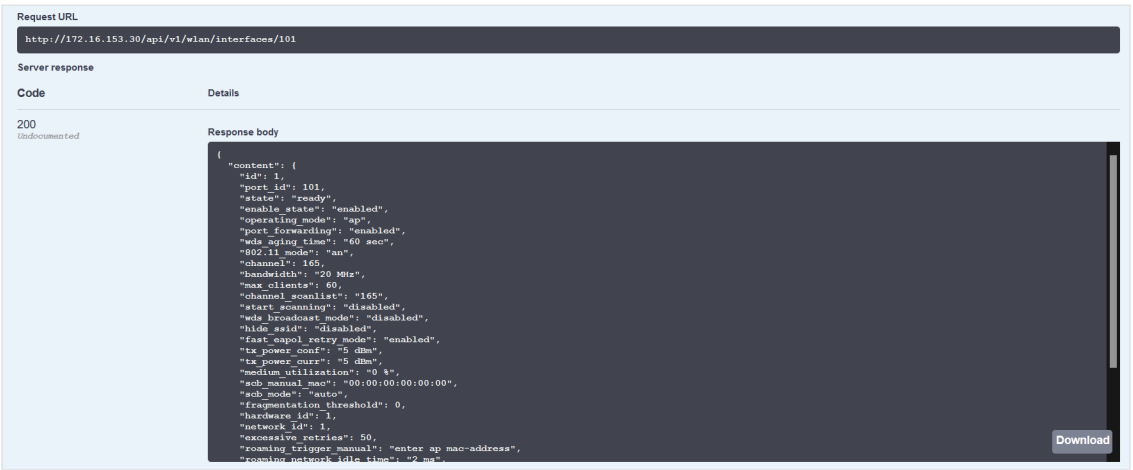
3.5 REST API

The FL WLAN 112x/102x product family offers a REST API. You can access an overview page on the device to get an overview of the possibilities provided by the REST API. You can retrieve data from various device areas (e.g., Configuration or Diagnostics) via the REST API.

The data can be read out and evaluated by a PLC (programmable logic controller) and other end devices that can communicate via HTTP or HTTPS. For example, you can evaluate the quality of a WLAN connection by sending a request to a PLC.

- In your browser, open the “<Device_IP_address>/api/v1” page, e.g., “172.16.153.30/api/v1”.

Figure 3-38 Visualization of the connection data read out for a WLAN connection (example)



In the example shown here (see Figure), the connection data read for a WLAN connection is displayed via virtual interface 101.

3.6 Firmware update

You can perform a firmware update directly via web-based management.

NOTE: We recommend that you always install the latest firmware revision

All devices can be updated to a more current firmware version regardless of their delivery state. Firmware updates are available on the Phoenix Contact website.

We explicitly advise against installing firmware revisions that are older than the one supplied on delivery. Continuous improvements, for example, for the bootloader, may prevent compatibility with older firmware revisions.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, System”.
- Click “Update Firmware”.

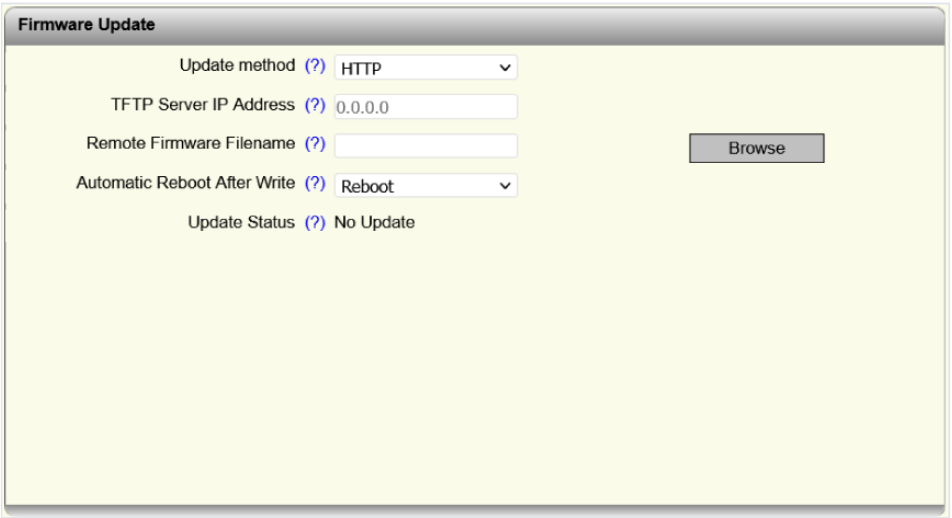
↪ The “Firmware Update” dialog opens.

Configuration settings of the device may be lost when you downgrade the firmware.

3.6.1 Update via HTTP(S)

- Select “HTTP(S)” for “Update method”.

Figure 3-39 Firmware Update: Update via HTTP(S)



- Click “Browse” and select the directory containing the new firmware.

The firmware file type is “.bin”.

- For “Automatic Reboot After Write”, select whether the device should be automatically restarted after the update.
- Click “Apply”.

↪ The firmware is downloaded. The update status is displayed under “Update Status”.

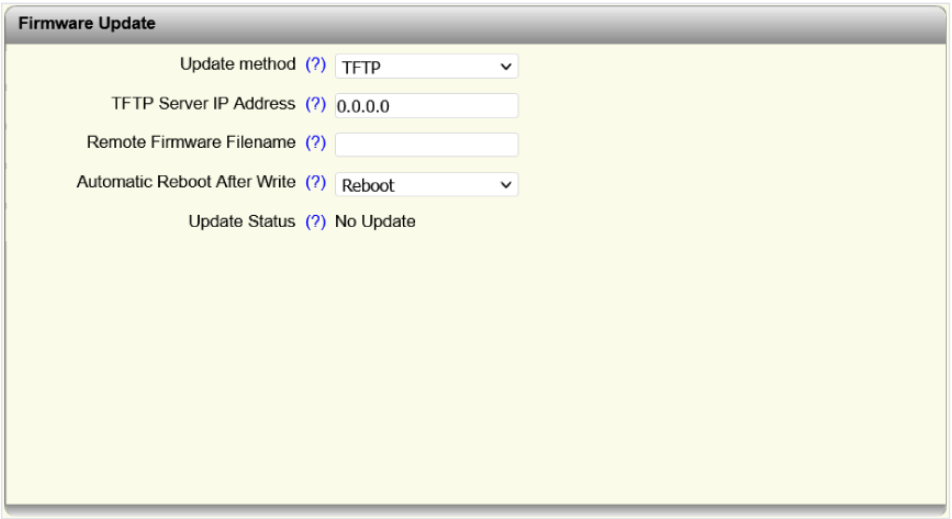
- Wait until the “Firmware Update successful” message is displayed at “Update Status”.
- Close the “Firmware Update” window.

To activate the new firmware, you must restart the device.

3.6.2 Update via TFTP

- Select “TFTP” for “Update method”.

Figure 3-40 Firmware Update: Update via TFTP



- For “TFTP Server IP Address”, enter the IP address of the TFTP server.
- For “Remote Firmware Filename”, enter the file path and name of the firmware file.
- Click “Apply”.

↪ The firmware is downloaded. The update status is displayed under “Update Status”.

- Wait until the “Firmware Update successful” message is displayed at “Update Status”.
- Close the “Firmware Update” window.

To activate the new firmware, you must restart the device.

3.7 File transfer

You can perform data transmission directly via web-based management.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, System”.
- Click “Further configuration handling options”.

↪ The “File Transfer” pop-up window opens.

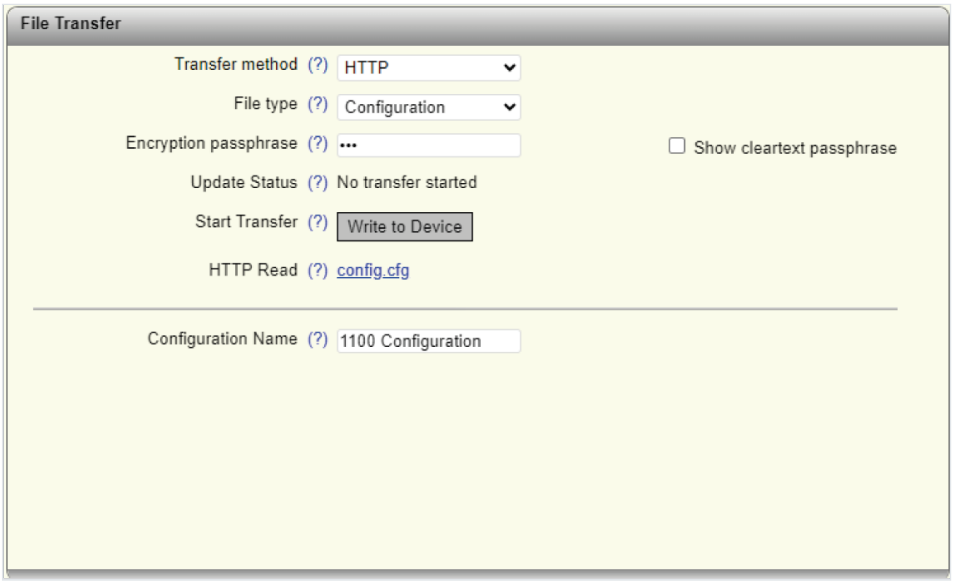
If you enter a password in the “Encryption passphrase” field, the corresponding file is encrypted. Open or edit the encrypted file using encryption and decryption software (e.g., Kleopatra).
Use the same CA certificate for decryption in the chosen software as for the device. Use the same CA certificate for decryption in the software used as for the device. To do this, generate a self-signed certificate on the device before encryption and data transmission, or upload an external certificate to the device (see Pop-up window: Certificate Management).

3.7.1 Transfer via HTTP(S)

- Select “HTTP(S)” for “Transfer method”.

Transferring configuration files or root CA certificate

Figure 3-41 File Transfer HTTP(S): Configuration files or root CA certificate



- Select “Configuration” or “Root CA Certificate” for “File Type”.

If you enter a password in the “Encryption passphrase” field, the corresponding file is encrypted. Open or edit the encrypted file using encryption and decryption software (e.g., Kleopatra).
Use the same CA certificate for decryption in the chosen software as for the device. Use the same CA certificate for decryption in the software used as for the device. To do this, generate a self-signed certificate on the device before encryption and data transmission, or upload an external certificate to the device (see Pop-up window: Certificate Management).

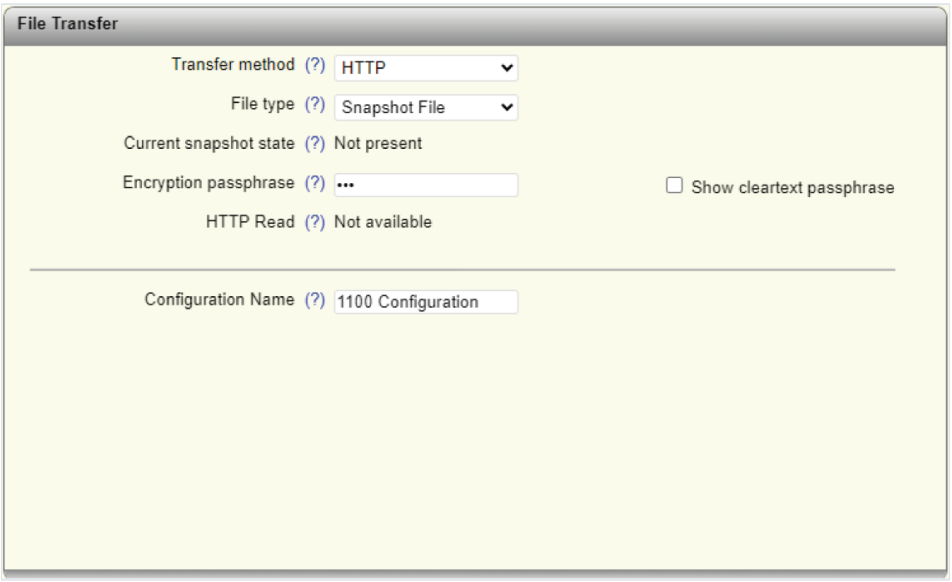
- Optionally, enter a password in the “Encryption passphrase” field to encrypt the file.
- Optionally, enter a name for your configuration or your root CA certificate in the “Configuration Name” field.

- Click “Write to Device” to select a file on your PC that is to be transferred to the device.
- Click the link at “HTTP(S) Read” to download the current configuration or the root CA certificate to your PC.

↪ The selected file is uploaded or downloaded. The current status is displayed under “Update Status”.

Transferring snapshot files

Figure 3-42 File Transfer HTTP(S): Snapshot



First you need to create a snapshot, see Snapshot.

- Select “Snapshot” for “File type”.

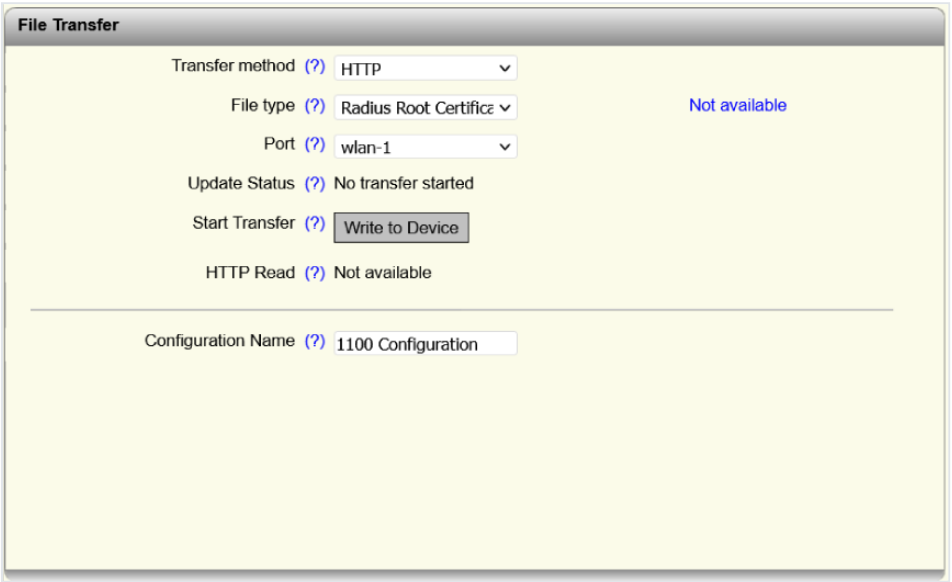
If you enter a password in the “Encryption passphrase” field, the corresponding file is encrypted. Open or edit the encrypted file using encryption and decryption software (e.g., Kleopatra).
Use the same CA certificate for decryption in the chosen software as for the device. Use the same CA certificate for decryption in the software used as for the device. To do this, generate a self-signed certificate on the device before encryption and data transmission, or upload an external certificate to the device (see Pop-up window: Certificate Management).

- Optionally, enter a password in the “Encryption passphrase” field to encrypt the file.
- Optionally, enter a name for your snapshot file in “Configuration Name”.
- Click “snapshot.tar.gz” to download the snapshot to your PC.

↪ The snapshot file is downloaded to your PC.

Transferring RADIUS root certificates

Figure 3-43 File Transfer HTTP(S): RADIUS root certificates

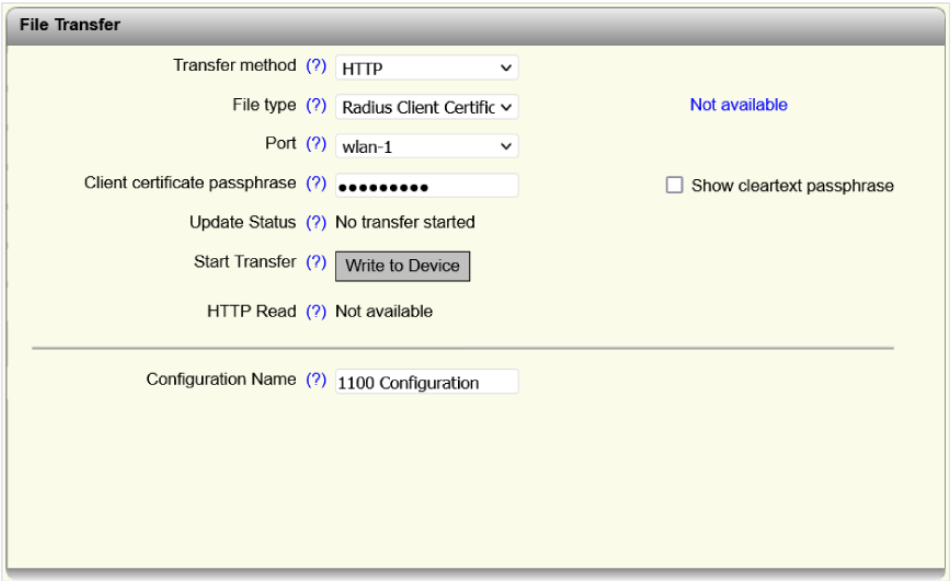


- Select the “Radius Root Certificate” option for “File type”.
- For “Port”, select the port for which the RADIUS root certificate is to be installed.
- Optionally, enter a name for your RADIUS root certificate in “Configuration Name”.
- Click “Write to Device” to select a file on your PC that is to be transferred to the device.

↪ The selected file is uploaded and installed at the selected port. The current status is displayed under “Update Status”.

Transferring RADIUS client certificates

Figure 3-44 File Transfer HTTP(S): RADIUS client certificates



- Select the “Radius Client Certificate” option for “File type”.
- For “Client certificate passphrase”, enter the password that can be used to decrypt the client certificate.
- For “Port”, select the port for which the RADIUS client certificate is to be installed.
- Optionally, enter a name for your RADIUS client certificate at “Configuration Name”.
- Click “Write to Device” to select a file on your PC that is to be transferred to the device.

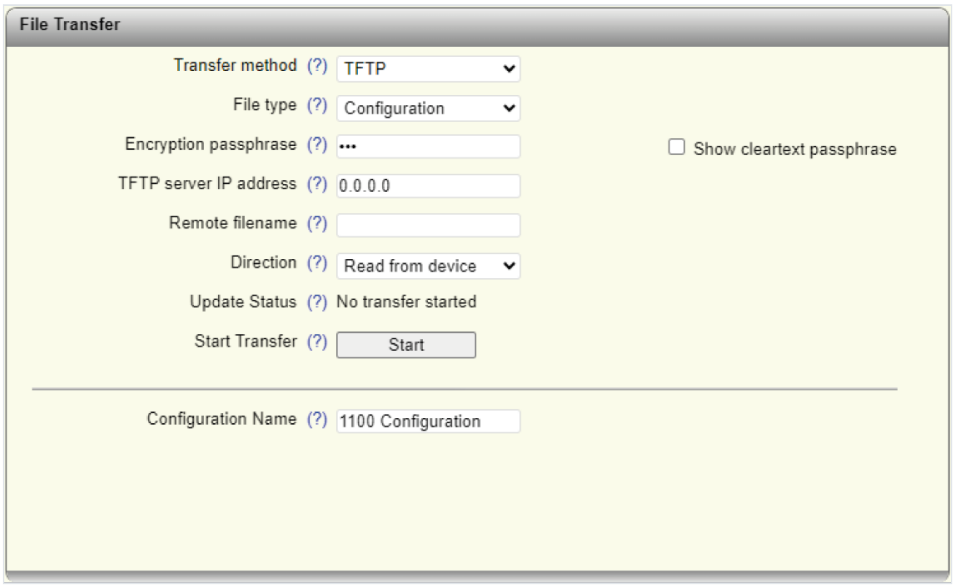
↪ The selected file is uploaded and installed at the selected port. The current status is displayed under “Update Status”.

3.7.2 Transfer via TFTP

- Select “TFTP” for “Transfer method”.

Transferring configuration files or root CA certificate

Figure 3-45 File Transfer TFTP: Configuration files or root CA certificate



- Select “Configuration” or “Root CA Certificate” for “File Type”.

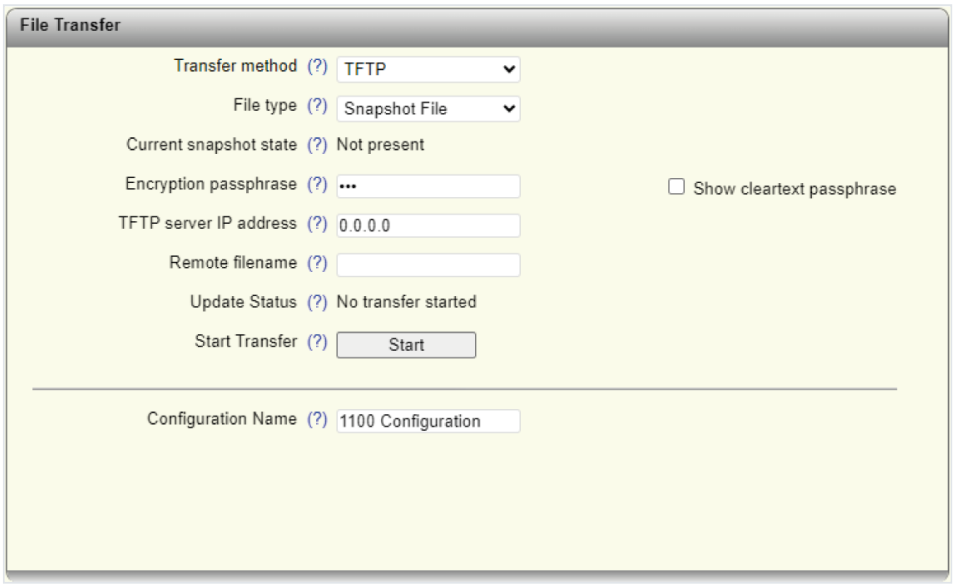
If you enter a password in the “Encryption passphrase” field, the corresponding file is encrypted. Open or edit the encrypted file using encryption and decryption software (e.g., Kleopatra).
Use the same CA certificate for decryption in the chosen software as for the device. Use the same CA certificate for decryption in the software used as for the device. To do this, generate a self-signed certificate on the device before encryption and data transmission, or upload an external certificate to the device (see Pop-up window: Certificate Management).

- Optionally, enter the password in the “Encryption passphrase” field to encrypt the file.
- For “TFTP server IP address”, enter the IP address of the TFTP server.
- For “Remote filename”, specify the file name including file extension. The file extension is *.cfg for a configuration file, *.ctx for a root CA certificate.
- For “Direction”, select whether the file should be uploaded to or downloaded from the device.
  - Select “Read from device” to download the file from the device to the PC.
  - Select “Write to device” to upload the file to the device.
- Optionally, enter a name for your configuration or your root CA certificate in the “Configuration Name” field.
- Click “Start” to start the transfer.

↪ The selected file is uploaded or downloaded. The current status is displayed under “Update Status”.

Transferring snapshot files

Figure 3-46 File Transfer TFTP: Snapshot



First you need to create a snapshot, see Snapshot.

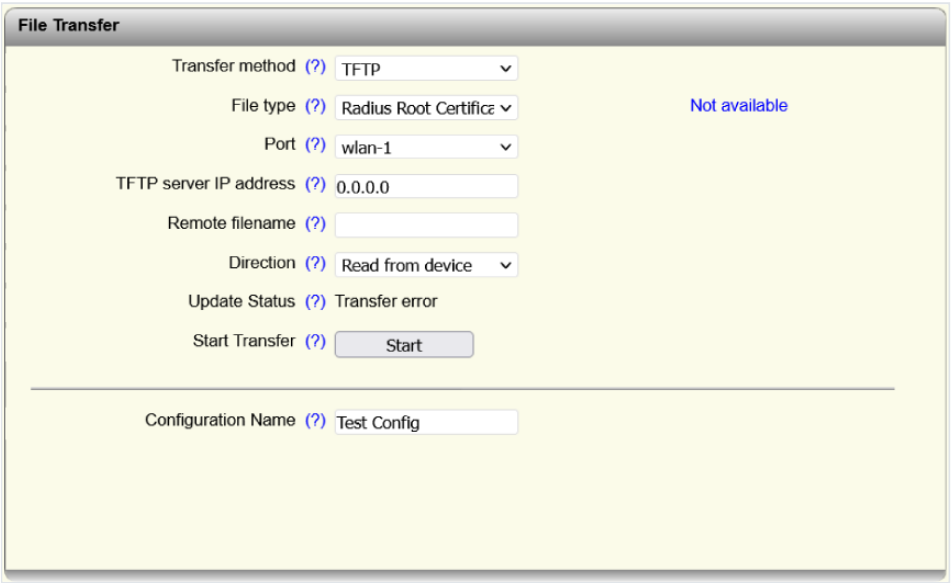
- Select “Snapshot” for “File type”.

If you enter a password in the “Encryption passphrase” field, the corresponding file is encrypted. Open or edit the encrypted file using encryption and decryption software (e.g., Kleopatra).
Use the same CA certificate for decryption in the chosen software as for the device. Use the same CA certificate for decryption in the software used as for the device. To do this, generate a self-signed certificate on the device before encryption and data transmission, or upload an external certificate to the device (see Pop-up window: Certificate Management).

- Optionally, enter the password in the “Encryption passphrase” field to encrypt the file.
- For “TFTP server IP address”, enter the IP address of the TFTP server.
- For “Remote filename”, specify the file name including file extension. The file extension for a snapshot file is *.tar.gz.
- Optionally, enter a name for your snapshot file in “Configuration Name”.
- Click “Start” to download the snapshot to your PC.
- The snapshot file is downloaded to your PC.

Transferring RADIUS root certificates

Figure 3-47 File Transfer TFTP: RADIUS root certificates

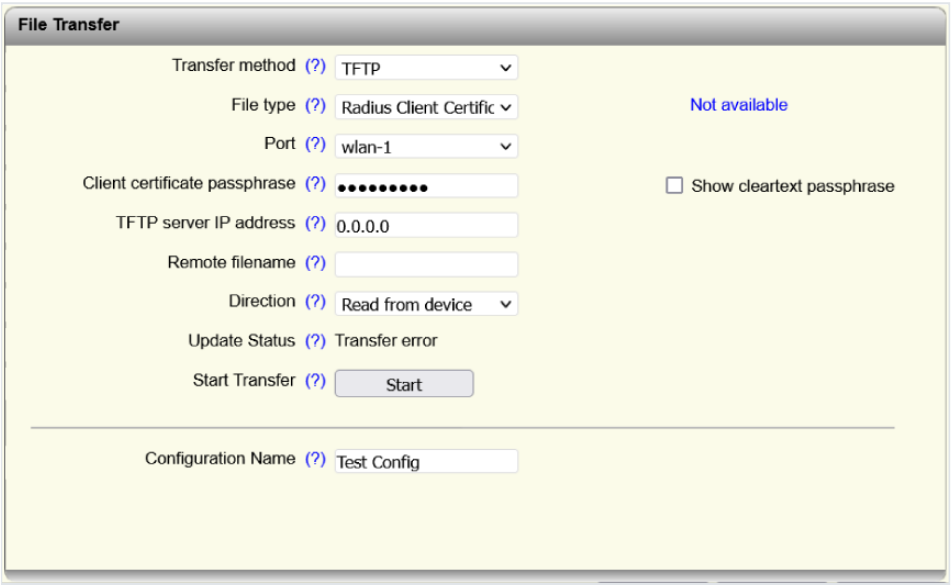


- Select the “Radius Root Certificate” option for “File type”.
- For “Port”, select the port for which the RADIUS root certificate is to be installed.
- For “TFTP server IP address”, enter the IP address of the TFTP server.
- For “Remote filename”, specify the file name including file extension. The file extension is *.pem for a RADIUS root certificate.
- Optionally, enter a name for your RADIUS root certificate in “Configuration Name”.
- Click “Start” to upload the file to the device.

↪ The selected file is uploaded and installed at the selected port. The current status is displayed under “Update Status”.

Transferring RADIUS client certificates

Figure 3-48 File Transfer TFTP: RADIUS client certificates



- Select the “Radius Client Certificate” option for “File type”.
- For “Port”, select the port for which the RADIUS client certificate is to be installed.
- For “Client certificate passphrase”, enter the password that can be used to decrypt the client certificate.
- For “TFTP server IP address”, enter the IP address of the TFTP server.
- For “Remote filename”, specify the file name including file extension. The file extension is *.p12 for a RADIUS client certificate.
- Optionally, enter a name for your RADIUS client certificate at “Configuration Name”.
- Click “Start” to upload the file to the device.

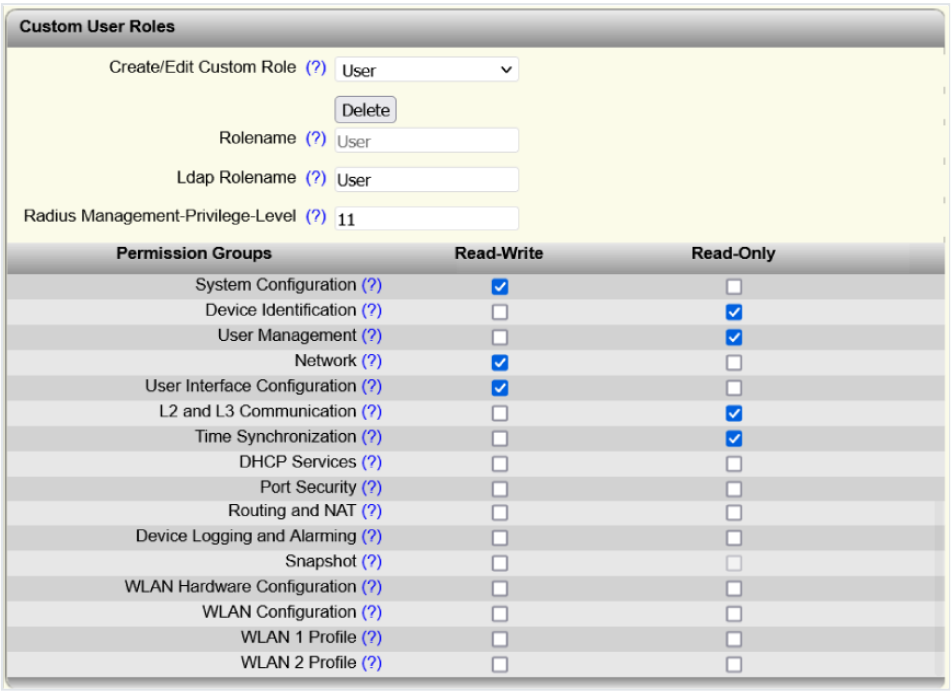
↪ The selected file is uploaded and installed at the selected port. The current status is displayed under “Update Status”.

3.8 Creating user roles

You can create custom user roles and assign detailed rights via the “Custom User Roles” pop-up window. You can choose between read permission (“Read-Only”), read and write permission (“Read-Write”), or no permission.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, User Management”.
- Click “Custom User Roles”.

Figure 3-49 Custom user roles



- Select “Create” for “Create/Edit Custom Role” to create a new user role.
- Enter a name for the user role in “Rolename”.
- Optionally, makes entries in “Ldap Rolename” and “Radius Management-Privilege-Level” to connect the new user role to the LDAP and RADIUS server.
- Activate the desired check boxes under “Permission Groups”. If you omit to activate a check box in a row, the user role will not have access to these settings.

Tabelle 3-37 Custom user roles: Explanation of permission groups

Permission group	Description
System Configuration	The following pages/functions can be edited and/or viewed with this user role: – Firmware updates – Creating and importing a configuration file – Resetting the device to default settings

Permission group	Description
Device Identification	The following pages/functions can be edited and/or viewed with this user role: – Device names – Device location, contact, device description
User Management	The following pages/functions can be edited and/or viewed with this user role: – Creating, editing, and deleting user roles
Network	The following pages/functions can be edited and/or viewed with this user role: – Network parameters such as IP address and host name DHCP services cannot be edited with this permission.
User Interface Configuration	The following pages/functions can be edited and/or viewed with this user role: – Configuring and deactivating interfaces such as WBM, CLI, and SNMP – Editing, exporting, and importing security context
L2 and L3 Communication	The following pages/functions can be edited and/or viewed with this user role: – VLAN – Multicast – QoS – MAC table
Time Synchronization	The following pages/functions can be edited and/or viewed with this user role: – Time synchronization – Setting up an SNTP server
DHCP Services	The following pages/functions can be edited and/or viewed with this user role: – DHCP Services: Setting up a DHCP server
Port Security	The following pages/functions can be edited and/or viewed with this user role: – Port-based security: 802.1X, RADIUS, MAC-based security
Routing and NAT	The following pages/functions can be edited and/or viewed with this user role: – Routing parameters – NAT parameters To be able to fully configure the routing and NAT parameters, the user role additionally requires read/write permission for “L2 and L3 Communication”

Permission group	Description
Device Logging and Alarming	The following pages/functions can be edited and/or viewed with this user role: – Syslog – Event table – SNMP Trap Manager
Snapshot	The following pages/functions can be edited and/or viewed with this user role: – Snapshot “Read-only” permission is not available for this permission group. “Read/write” permission is required to create a snapshot.
WLAN Hardware Configuration	The following pages/functions can be edited and/or viewed with this user role: – Activating the WLAN interface – Outdoor mode – Aggregation mode – Antenna port configuration
WLAN Configuration	The following pages/functions can be edited and/or viewed with this user role: – WLAN band – Channel – Transmission power – Channel bandwidth – Operating mode
WLAN 1 Profile	The following pages/functions can be edited and/or viewed with this user role: – For WLAN interface 1: – Country – Roaming list – scan – Network SSID – Security mode – Authentication method – Client user ID and password – Phase 2 authentication type
WLAN 2 Profile	The following pages/functions can be edited and/or viewed with this user role: – For WLAN interface 2: – Country – Roaming list – scan – Network SSID – Security mode – Authentication method – Client user ID and password – Phase 2 authentication type

- Confirm your settings with “Apply&Save”.
- Click on “Configuration, User Management”.
- For “Create/Edit User”, select the user to whom you want to assign the user role. Alternatively, create a new user.
- For “User Role”, select the desired role.
- Confirm your settings with “Apply&Save”.

4 Device operating modes

The device supports “Access Point”, “Client”, “Client (NAT)”,“Client (VXLAN)”, “Access Point (VXLAN)” and “Repeater” operating modes (with two virtual wireless interfaces). “Client” operating mode has three options: “FTB” (Fully Transparent Bridge), “SCB” (Single Client Bridge), and “MCB” (Multi Client Bridge). Each operating mode supports different applications.

You can define the operating mode of the device on the “WLAN Interface” page.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.

For more information and configuration options for the individual operating modes, refer to the subsequent sections.

4.1 Operating mode:Access point

4.1.1 General information

In “Access Point” operating mode, the device represents the wireless interface of an Ethernet network. Several WLAN devices can be connected wirelessly to a network via this access point.

Important parameters

The WLAN network, which consists of one or more access points, is assigned a network name known as the SSID (Service Set Identifier), which is its main feature. In order to ensure network security against unauthorized access via the WLAN interface (according to IEEE 802.11i), you should also use secure encryption.

The network name and encryption are defined in the access point. You can enter them via web-based management (WBM).

Any WLAN client that would like to access the network via this access point must know the SSID and encryption.

If you want WLAN access to take place at several points in an Ethernet network or you want to cover a wide area, use multiple WLAN access points. These access points are all connected to the network. If all the access points use the same SSID and encryption, a connected WLAN client can switch between the access points, see *Roaming*.

Network planning

The frequencies of the wireless channels, ideally specified as early as the WLAN network planning stage, are also defined via the access point. In addition, it may be possible to select the transmission standard according to 802.11.

Multiple WLAN clients can be connected simultaneously to every access point. Due to the higher number of clients per access point, the amount of data that can be transmitted via each individual client is reduced. This can vary depending on how much data the application requests via the individual clients. If the application has time requirements, you must also take the number of clients into consideration. For example, for PROFINET applications it is recommended to reduce the number of clients

per access point to a few devices. You can achieve this by using multiple access points and assigning different frequencies and SSIDs.

PROFINET and Ethernet/IP can be transmitted via WLAN. You have to adjust the timing for this. On the client side, the SCB or FTB operating mode is also required for layer 2-transparent communication (see Operation as a single client (SCB) and Operation as a fully transparent bridge (FTB)).

4.1.2 Configuring an access point

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.

Figure 4-1 Configuring an access point

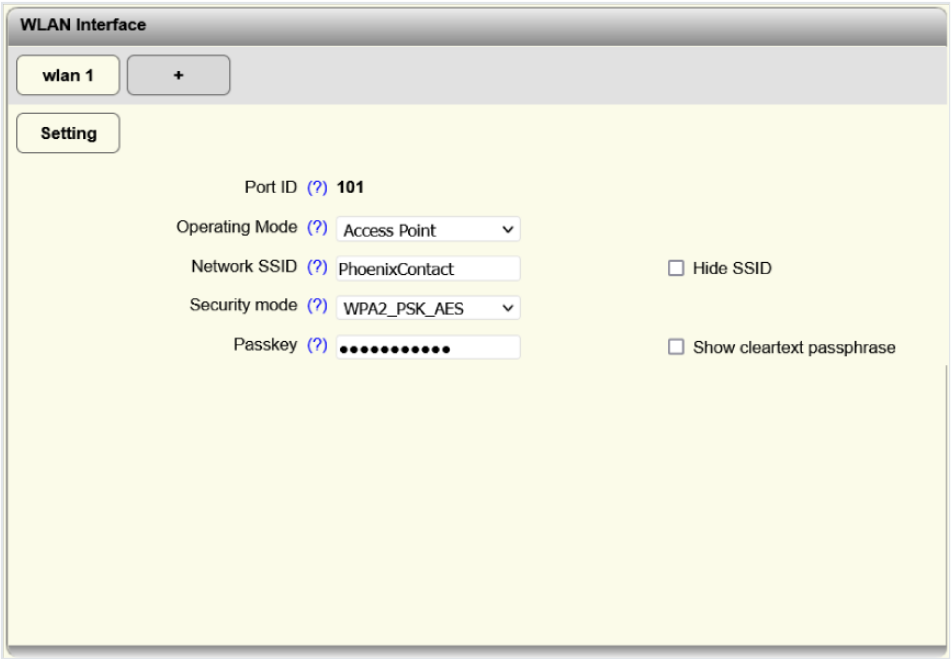


Tabelle 4-1 Configuring an access point: Parameters

Parameters	Description
Operating Mode	Here, select the “Access Point” option.
Network SSID	Here, enter the desired network SSID. The SSID is the network ID by means of which clients can connect to the access point. The network SSID can have a maximum length of 32 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space.
Security mode	Here, set the desired encryption method for the WLAN interface. – None: No encryption. This option puts network security at risk.

Parameters	Description
	– WPA_PSK_TKIP: This encryption method is used by older devices that do not support WPA/AES. – WPA2_PSK_AES: This encryption method is secure and fast. It is suitable for client roaming. – WPA2-EAP: This encryption method is used for RADIUS authentication (see RADIUS certificates). – WPA3-SAE: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. SAE is an established method from mesh networks that is used for the initial handshake. – ENHANCED OPEN: This encryption corresponds to WPA2-PSK encryption. You do not need to enter a passkey, but WPA2-PSK data protection and ease of use are still guaranteed.
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between eight and 64 characters long. For a high level of security, we recommend a random string. Letters, numbers, and the following special characters are permitted: $%@&/\ ()=?![]{}+*-_<>#^.,:~|. Exception for WEP: WEP64: five alphanumeric characters or ten hex digits WEP128: 13 alphanumeric characters or 26 hex digits
Radius authentication server	This option is only available if you selected the “WPA2-EAP” option for “Security mode”. Click “Link to radius server configuration” to open the “Security” page. Here you can configure the RADIUS server for authentication (see *Security* and RADIUS certificates).

- On the “WLAN Interface” page, set the “Access Point” option for “Operating Mode”.
- Define the parameters as desired and click “Apply&Save”.
- Click “Configuration, WLAN Setting”.
- Set the parameters for the WLAN band, bandwidth, channel and transmission power as desired and click “Apply&Save”.

↪ Other WLAN devices can now use the defined access data to connect to the wireless interface.

4.2 Operating mode: Client

WLAN clients are devices that connect to an access point to send and receive data via WLAN. You can choose between different operating modes of the device as a client.

4.2.1 Roaming

The process where a WLAN client switches from one access point to another is known as roaming. The roaming speed varies depending on the type of client used. A

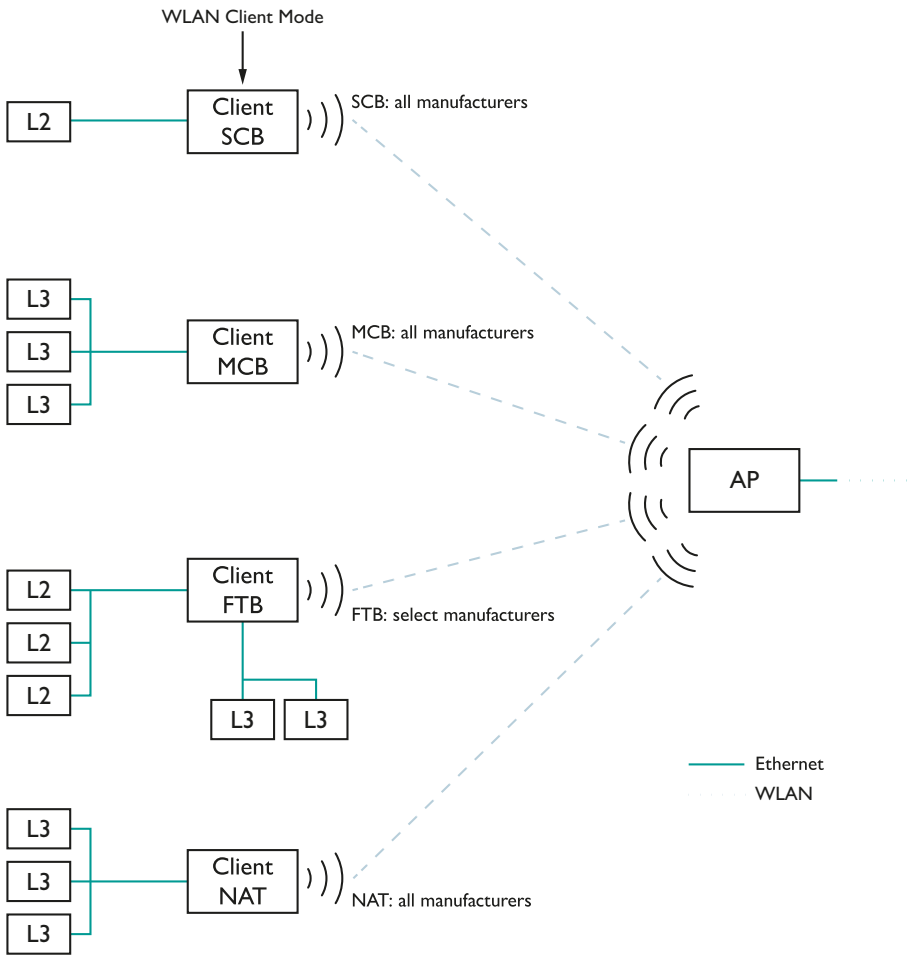
notebook, for example, will need quite a long time. For applications where roaming needs to be carried out in a fraction of a second, you must use industrial WLAN clients. Roaming is primarily defined via the client. Access points in default WLAN networks are effective only due to their physical arrangement, transmission power set, and antenna. They ensure that there is sufficient network coverage available at every location. The FL WLAN 112x/102x product family is already optimized for fast roaming in “Client” operating mode.

The user can improve the roaming speed by restricting channels via the “Roaming list” under “WLAN Interface” (see *Configuring the client (SCB): Roaming List*).

4.2.2 Compatibility between different WLAN device manufacturers

The following describes what should be noted relating to the client configuration when using WLAN access points from different manufacturers. The Ethernet protocols that can be transmitted and the number of Ethernet devices are described.

Figure 4-2 Overview of “Client” operating modes



The two “Client (SCB)” and “Client (MCB)” operating modes support access points from all manufacturers. You can connect one device to a device with the “Client (SCB)” operating mode, while “Client (MCB)” supports several devices.

The “Client (NAT)” operating mode supports devices that are NAT-compatible, regardless of the manufacturer. The “1:1 NAT” and “IP Masquerading” NAT functions are available. “1:1 NAT” lets you connect one device per IP address, “IP Masquerading” lets you connect several devices (see Operating mode: Client (NAT)).

“Client (FTB)” operating mode, on the other hand, only supports communication between Phoenix Contact devices. You can connect several devices to a device with “Client (FTB)” operating mode in a layer 2 transparent manner.

You must use VxLAN for transparent Layer 2 communication via multiple devices in the FL WLAN 112x/102x (see Operating mode: Client (VXLAN) and Access point (VXLAN)).

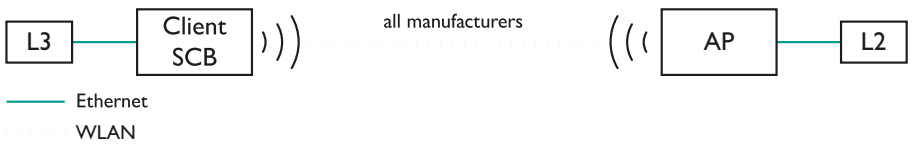
Tabelle 4-2 Layer 2 interoperability of the Phoenix Contact WLAN devices

Module	Operating mode	FTB	MCB	SCB	NAT	VxLAN
FL WLAN 110x/210x FL WLAN 101x/201x 802.11n	Client	X	X	X	X	-
FL WLAN 110x/210x FL WLAN 101x/201x 802.11n	Access point	X	X	X	X	-
FL WLAN 112x/102x 802.11n/ax	Client	X	X	X	X	X
FL WLAN 112x/102x 802.11n/ax	Access point	-	X	X	X	X

4.2.3 Operation as a single client (SCB)

4.2.3.1 General information

Figure 4-3 Single client bridge



Properties:

– The WLAN device transparently connects an Ethernet device to the layer 2 access point via WLAN.

Automatic SCB

The MAC or IP address of the connected device is automatically queried. You do not have to enter it manually in the WLAN device.

You may only connect **one** wired device in SCB operating mode.

The WLAN device can be accessed via its own IP address. However, connected devices still receive the MAC address of the connected end device for the WLAN device. This can lead to problems with some third-party manufacturers.

Static IP example

An Ethernet device (L2) with static IP address is connected to the copper port of the WLAN device (in “Client (SCB)” operating mode).

The PC that is connected to the access point on the other end sends a ping. This may take a few seconds. Alternatively, the IP address of the Ethernet device (L2) behind the client is addressed via a browser.

You can delete old ARP tables (on the PC) via the command prompt with the “arp –d” command to ensure that the ARP request is resent. If necessary, delete the browser cache.

DHCP/BOOTP/DCP example

If the Ethernet device (L2) is in DHCP mode, the MAC address is transmitted to the client and beyond.

Manual SCB

If you connect several Ethernet devices to the Ethernet port of the WLAN device on the cable side, it is recommended that the MAC address of the device that is to be connected via the WLAN interface is entered manually in web-based management.

In contrast to automatic mode, this will ensure that this specific device is addressed. The other devices in the network cannot be accessed via WLAN.

In Single Client Bridge (SCB) mode, data is transmitted transparently on Layer 2. Only the device whose MAC address is entered for the client can be accessed via WLAN.

4.2.3.2 Configuring the client (SCB)

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.

Figure 4-4 Configuring the client (SCB): Setting

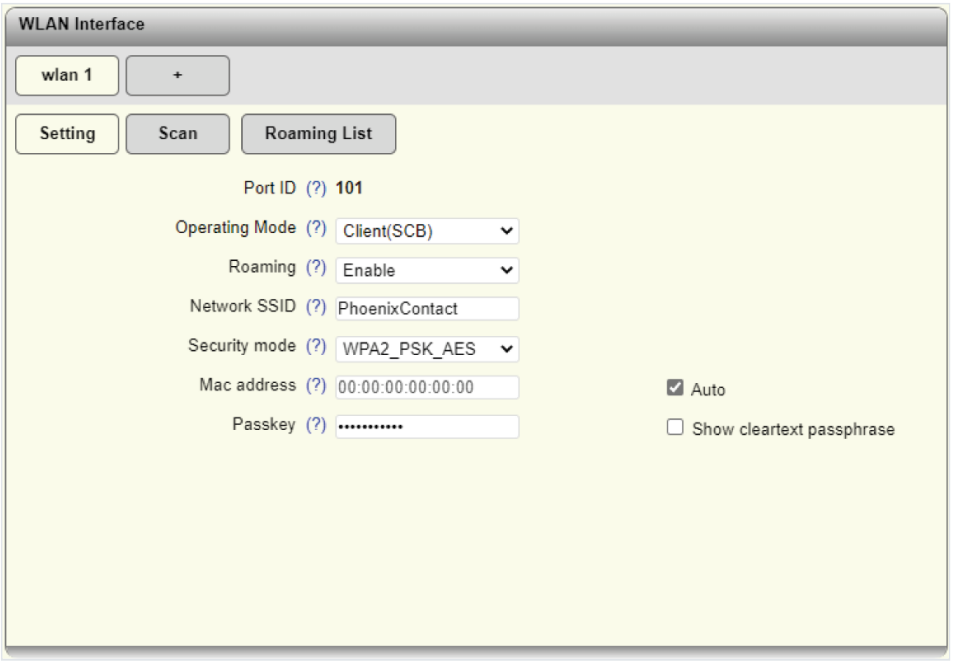


Tabelle 4-3 Configuring the client (SCB): Setting: Parameters

Parameters	Description
Port ID	The internal port ID of the wireless interface is displayed here.
Operating Mode	Here, select the “Client(SCB)” option.
Roaming	Select whether roaming should be activated. – Disable: Roaming is deactivated. The threshold for background scans is set to -94 dBm. This option is used in static configurations without roaming. – Enable: Roaming is activated. The threshold for background scans is set to -60 dBm (default setting). – Advanced config: Select this option if you already configured roaming on another interface (e.g., via CLI).
Network SSID	Here, enter the desired network SSID. The SSID is the network ID by means of which the WLAN device can connect to the client. The network SSID can have a maximum length of 32 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space.

Parameters	Description
Security mode	Here, set the desired encryption method for the WLAN interface. – None: No encryption. This option puts network security at risk. – WPA-PSK (TKIP): This encryption method is used by older devices that do not support WPA/AES. – WPA2-PSK (AES): This encryption method is secure and fast. It is suitable for client roaming. – FT-PSK (AES): This encryption method supports Fast Transition (802.11 r fast roaming). It is a symmetric encryption system with a pre-shared key (PSK) and AES. – WPA2-EAP: This encryption method is used for RADIUS authentication (see RADIUS certificates). For further information about the parameters available for this encryption method, see Encryption:WPA2-EAP and FT-EAP. – FT-EAP: This option supports Fast Transition (802.11 r fast roaming) with authentication via EAP and RADIUS. For further information about the parameters available for this encryption method, see Encryption:WPA2-EAP and FT-EAP. – WPA3-SAE: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. SAE is an established method from mesh networks that is used for the initial handshake. – WPA3-EAP: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. EAP is an established protocol used for this purpose. – ENHANCED OPEN: This encryption corresponds to WPA2-PSK encryption. You do not need to enter a passkey, but WPA2-PSK data protection and ease of use are still guaranteed. – WEP: Only available in “Client” (FTB, MCB, SCB) operating mode. This option is not recommended because of its security features.  **NOTE: Network security at risk** If you select “None”, the data is sent without encryption. This option puts network security at risk.
Mac address	Here, enter the desired MAC address for a manual assignment. To automatically adopt the MAC address of the connected Ethernet device, activate the “Auto” check box.

Parameters	Description
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between eight and 64 characters long. For a high level of security, we recommend a random string. Letters, numbers, and the following special characters are permitted: $%@&/\ ()=?![]{}+*-_<>#^.,:~|. Exception for WEP: WEP64: five alphanumeric characters or ten hex digits WEP128: 13 alphanumeric characters or 26 hex digits

Encryption:WPA2-EAP and FT-EAP

Figure 4-5 Encryption:WPA2-EAP and FT-EAP

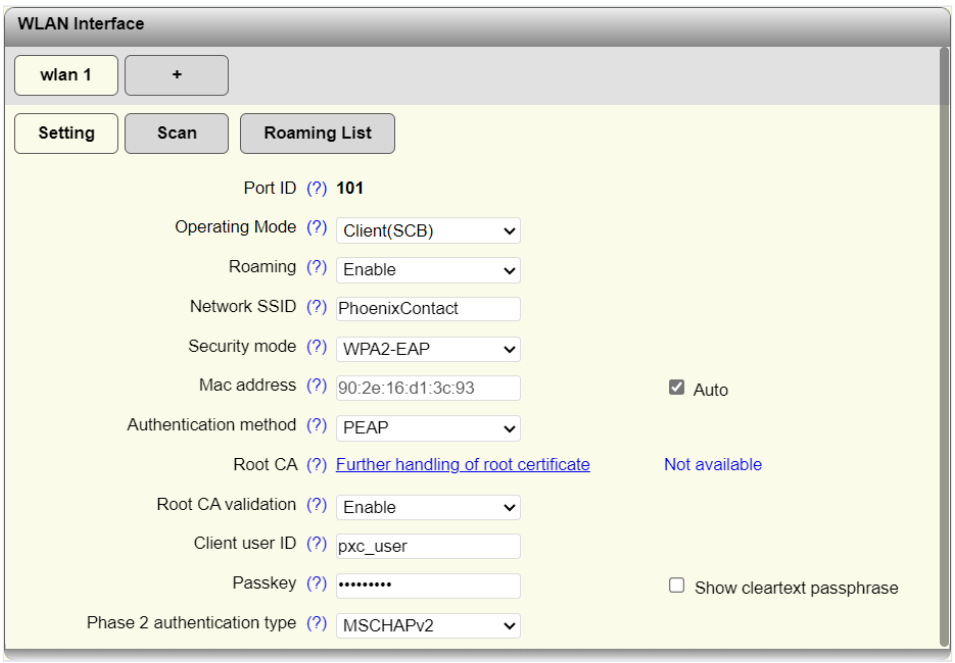


Tabelle 4-4 Encryption: WPA2-EAP and FT-EAP: Parameters

Parameters	Description
Authentication method	Select the desired authentication method. – PEAP: This authentication method uses server authentication and requires phase 2 authentication using the client's login credentials. – TTLS: This authentication method uses server authentication and requires phase 2 authentication using the client's login credentials. – TLS: This authentication method uses client and server authentication. A client key (*.pfx or *.p12) must be provided together with the password.

Parameters	Description
Root CA	Click “Further handling of root certificate” to open the “File Transfer” pop-up window. Here, you can upload a root certificate (see File transfer).
Root CA validation	This option is only available if you selected “PEAP” for “Authentication method”. Select whether validation of the root certificate is required. **NOTE: Network security at risk** If you select “Disable”, the server identity is not validated. This option is not secure.
Client certificate	This option is only available if you selected “TLS” for “Authentication method”. Click “Further handling of client certificate” to open the “File Transfer” pop-up window. Here, you can upload a client certificate (see File transfer).
Client user ID	This option is only available if you selected “PEAP” or “TTLS” for “Authentication method”. Enter a user name for Phase 2 authentication with PEAP. The user name must be alphanumeric and between eight and 64 characters long.
Passkey	This option is only available if you selected “PEAP” or “TTLS” for “Authentication method”. Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between eight and 64 characters long. For a high level of security, we recommend a random string. Letters, numbers, and the following special characters are permitted: $%@&/\ ()=?![]{}+*-_<>#^.,:~|. Exception for WEP: WEP64: five alphanumeric characters or ten hex digits WEP128: 13 alphanumeric characters or 26 hex digits
Phase 2 authentication type	This option is only available if you selected “PEAP” or “TTLS” for “Authentication method”. Select which Phase 2 authentication should be used. – MSCHAPv2: This option is normally used in combination with PEAP. – MD5: This option is normally used in combination with TTLS.

- On the “WLAN Interface” page, set the “Client(SCB)” option for “Operating Mode”.
- Define the parameters as desired and click “Apply&Save”.
- A WLAN device can now use the defined access data to connect to the wireless interface.
- Click “Scan”.

Figure 4-6 Configuring the client (SCB): Scan

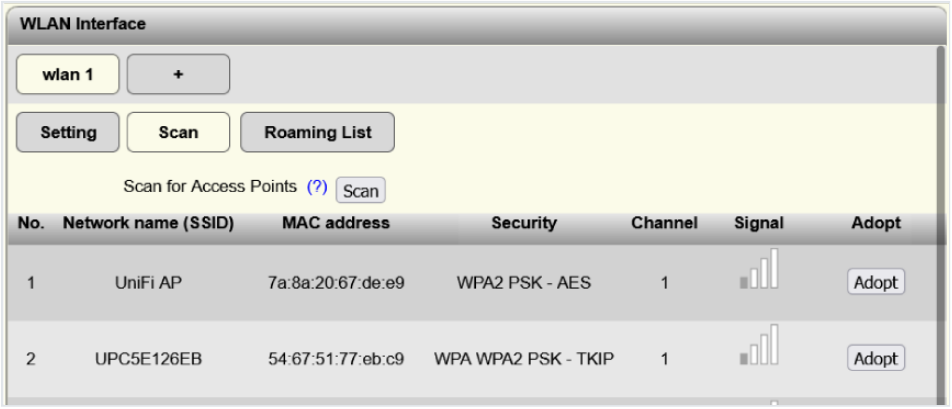


Tabelle 4-5 Configuring the client (SCB): Scan: Parameters

Parameters	Description
Scan for Access Points	Click “Scan” to search for available access points.
Adopt	Click “Adopt” to apply the access point settings.

- Click “Scan” to search for available access points. Available access points are displayed in the table with information such as the SSID or the signal strength.

The scan delivers a maximum of 29 results.

- Click “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.

The “Passkey” is not accepted. Enter the “Passkey” manually under “Settings”.

- Click “Roaming List”.

Figure 4-7 Configuring the client (SCB): Roaming List

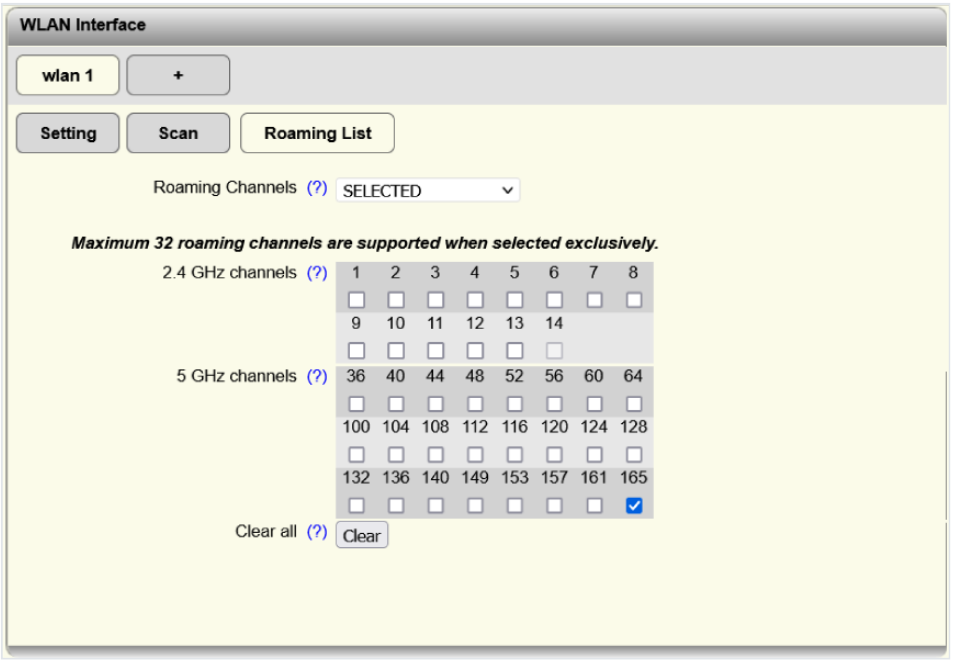


Tabelle 4-6 Configuring the client (SCB):Roaming List: Parameters

Parameters	Description
Roaming Channels	Select whether the device should search for networks on all available channels or just on selected channels. The more channels you select, the longer will roaming take. Only select the channels you want to search for networks.
2.4 GHz channels	This option is only available if you selected “SELECTED” for “Roaming Channels”. Activate the check boxes of all channels in the 2.4 GHz range you want the device to search for networks in.
5 GHz channels	This option is only available if you selected “SELECTED” for “Roaming Channels”. Activate the check boxes of all channels in the 5 GHz range you want the device to search for networks in.
Clear all	This option is only available if you selected “SELECTED” for “Roaming Channels”. Click “Clear all” to disable all check boxes in the 2.4 and 5 GHz ranges.

- Select whether the device should search all available channels for networks or only selected channels.

The more channels you select, the longer will roaming take. Only select the channels you want to search for networks.

- If you select “SELECTED”, you can now select the channels manually for the 2.4 GHz and 5 GHz ranges.
- Confirm your settings with “Apply&Save”.

4.2.4 Operation as multi-client (MCB)

4.2.4.1 General information

Multi Client Bridge is preset as the operating mode in the default settings.

Properties:

– The WLAN device connects several Ethernet devices (connected via Ethernet switches) to the layer 3 access point.
– The Ethernet device is detected automatically.
– Operates between all WLAN devices, even devices (access points) from third-party manufacturers. You can connect several network devices on the cable side. In this operating mode, restrictions apply and not all protocols are transmitted, only layer 3 transparent protocols. This includes, for example, TCP/IP but not PROFINET or EtherNet/IP.

MCB mode only supports IPv4 data traffic. Problems may occur during transmission with mixed data traffic.

4.2.4.2 Configuring the client (MCB)

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.

Figure 4-8 Configuring the client (MCB): Setting

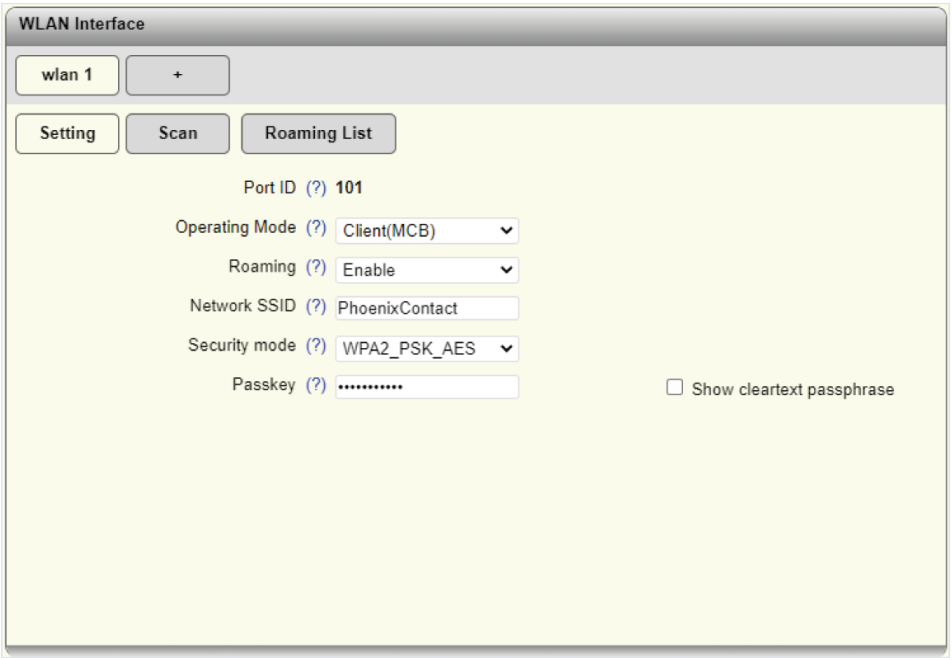


Tabelle 4-7 Configuring the client (MCB): Setting: Parameters

Parameters	Description
Port ID	The internal port ID of the wireless interface is displayed here.
Operating Mode	Here, select the “Client(MCB)” option.
Roaming	Select whether roaming should be activated. – Disable: Roaming is deactivated. The threshold for background scans is set to -94 dBm. This option is used in static configurations without roaming. – Enable: Roaming is activated. The threshold for background scans is set to -60 dBm (default setting). – Advanced config: Select this option if you already configured roaming on another interface (e.g., via CLI).
Network SSID	Here, enter the desired network SSID. The SSID is the network ID by means of which the WLAN device can connect to the client. The network SSID can have a maximum length of 32 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space.

Parameters	Description
Security mode	Here, set the desired encryption method for the WLAN interface. – None: No encryption. This option puts network security at risk.internal-link – WPA-PSK (TKIP): This encryption method is used by older devices that do not support WPA/AES. – WPA2-PSK (AES): This encryption method is secure and fast. It is suitable for client roaming. – FT-PSK (AES): This encryption method supports Fast Transition (802.11 r fast roaming). It is a symmetric encryption system with a pre-shared key (PSK) and AES. – WPA2-EAP: This encryption method is used for RADIUS authentication (see RADIUS certificates). For further information about the parameters available for this encryption method, see Encryption:WPA2-EAP and FT-EAP. – FT-EAP: This option supports Fast Transition (802.11 r fast roaming) with authentication via EAP and RADIUS. For further information about the parameters available for this encryption method, see Encryption:WPA2-EAP and FT-EAP. – WPA3-SAE: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. SAE is an established method from mesh networks that is used for the initial handshake. – WPA3-EAP: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. EAP is an established protocol used for this purpose. – ENHANCED OPEN: This encryption corresponds to WPA2-PSK encryption. You do not need to enter a passkey, but WPA2-PSK data protection and ease of use are still guaranteed. – WEP: Only available in “Client” (FTB, MCB, SCB) operating mode. This option is not recommended because of its security features.  **NOTE: Network security at risk** If you select “None”, the data is sent without encryption. This option puts network security at risk.

Parameters	Description
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between eight and 64 characters long. For a high level of security, we recommend a random string. Letters, numbers, and the following special characters are permitted: $%@&/\ ()=?![]{}+*-_<>#^.,:~|. Exception for WEP: WEP64: five alphanumeric characters or ten hex digits WEP128: 13 alphanumeric characters or 26 hex digits

- On the “WLAN Interface” page, set the “Client(MCB)” option for “Operating Mode”.
- Define the parameters as desired and click “Apply&Save”.

↪ The WLAN devices can now use the defined access data to connect to the wireless interface.

- Click “Scan”.
- Click “Scan” to search for available access points. Available access points are displayed in the table with information such as the SSID or the signal strength (see *Configuring the client (SCB): ScanConfiguring the client (SCB): Scan*).

The scan delivers a maximum of 29 results.

- Click “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.

The “Passkey” is not accepted. Enter the “Passkey” manually under “Settings”.

- Click “Roaming List”.
- Select whether the device should search all available channels for networks or only selected channels (see *Configuring the client (SCB): Roaming ListConfiguring the client (SCB): Roaming List*).

The more channels you select, the longer will roaming take. Only select the channels you want to search for networks.

- If you select “SELECTED”, you can now select the channels manually for the 2.4 GHz and 5 GHz ranges.
- Confirm your settings by clicking “Apply&Save”.

4.2.5 Operation as a fully transparent bridge (FTB)

4.2.5.1 General information

Properties:

– The WLAN device connects several Ethernet devices (connected via Ethernet switches) to the layer 2 access point.

The connection is only possible with devices (access points) that support the same fully transparent bridge mode.

You must use VxLAN for transparent Layer 2 communication via multiple devices in the FL WLAN 112x/102x (see Operating mode: Client (VXLAN) and Access point (VXLAN)).

4.2.5.2 Configuring the client (FTB)

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.

Figure 4-9 Configuring the client (FTB): Setting

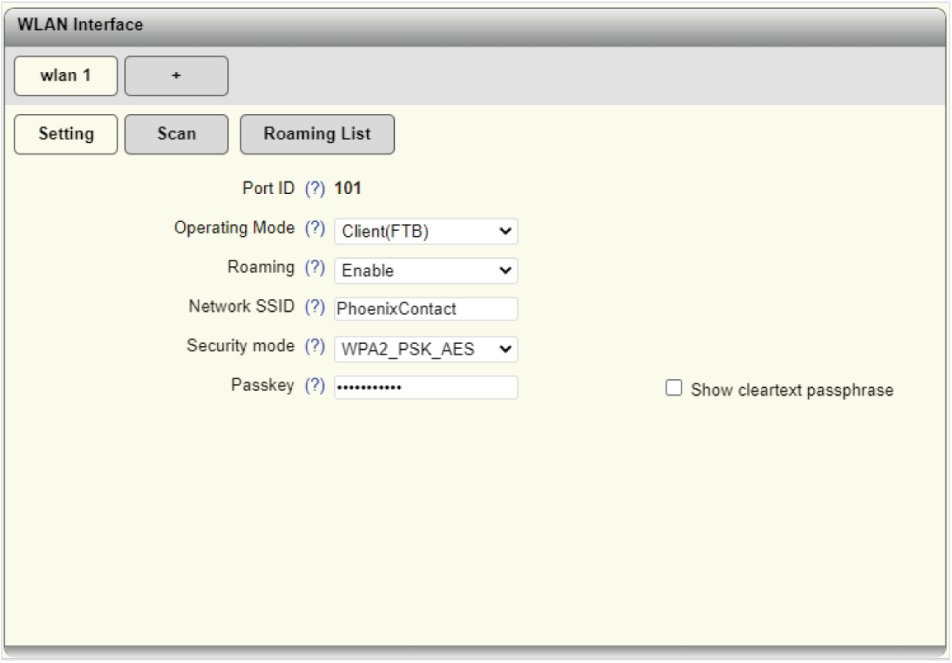


Tabelle 4-8 Configuring the client (FTB): Setting: Parameters

Parameters	Description
Port ID	The internal port ID of the wireless interface is displayed here.
Operating Mode	Here, select the “Client(FTB)” option.
Roaming	Select whether roaming should be activated. – Disable: Roaming is deactivated. The threshold for background scans is set to -94 dBm. This option is used in static configurations without roaming. – Enable: Roaming is activated. The threshold for background scans is set to -60 dBm (default setting).

Parameters	Description
	– Advanced config: Select this option if you already configured roaming on another interface (e.g., via CLI).
Network SSID	Here, enter the desired network SSID. The SSID is the network ID by means of which the WLAN device can connect to the client. The network SSID can have a maximum length of 32 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space.
Security mode	Here, set the desired encryption method for the WLAN interface. – None: No encryption. This option puts network security at risk. – WPA-PSK (TKIP): This encryption method is used by older devices that do not support WPA/AES. – WPA2-PSK (AES): This encryption method is secure and fast. It is suitable for client roaming. – FT-PSK (AES): This encryption method supports Fast Transition (802.11 r fast roaming). It is a symmetric encryption system with a pre-shared key (PSK) and AES. – WPA2-EAP: This encryption method is used for RADIUS authentication (see RADIUS certificates). For further information about the parameters available for this encryption method, see Encryption:WPA2-EAP and FT-EAP.> – FT-EAP: This option supports Fast Transition (802.11 r fast roaming) with authentication via EAP and RADIUS. For further information about the parameters available for this encryption method, see Encryption:WPA2-EAP and FT-EAP. – WPA3-SAE: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. SAE is an established method from mesh networks that is used for the initial handshake. – WPA3-EAP: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. EAP is an established protocol used for this purpose. – ENHANCED OPEN: This encryption corresponds to WPA2-PSK encryption.You do not need to enter a passkey, but WPA2-PSK data protection and ease of use are still guaranteed. – WEP: Only available in “Client” (FTB, MCB, SCB) operating mode. This option is not recommended because of its security features.

Parameters	Description
	NOTE: Network security at risk If you select “None”, the data is sent without encryption. This option puts network security at risk.
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between eight and 64 characters long. For a high level of security, we recommend a random string. Letters, numbers, and the following special characters are permitted: $%@&/\ ()=?![]{}+*-_<>#^.,:~|. Exception for WEP: WEP64: five alphanumeric characters or ten hex digits WEP128: 13 alphanumeric characters or 26 hex digits

- On the “WLAN Interface” page, set the “Client(FTB)” option for “Operating Mode”.
- Define the parameters as desired and click “Apply&Save”.

↪ The WLAN devices can now use the defined access data to connect to the wireless interface.

- Click “Scan”.
- Click “Scan” to search for available access points. Available access points are displayed in the table with information such as the SSID or the signal strength (see *Configuring the client (SCB): ScanConfiguring the client (SCB): Scan*).

The scan delivers a maximum of 29 results.

- Click “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.

The “Passkey” is not accepted. Enter the “Passkey” manually under “Settings”.

- Click “Roaming List”.
- Select whether the device should search all available channels for networks or only selected channels (see *Configuring the client (SCB): Roaming ListConfiguring the client (SCB): Roaming List*).

The more channels you select, the longer will roaming take. Only select the channels you want to search for networks.

- If you select “SELECTED”, you can now select the channels manually for the 2.4 GHz and 5 GHz ranges.
- Confirm your settings by clicking “Apply&Save”.

4.3 Operating mode: Client (NAT)

NAT stands for Network Address Translation and refers to the translation of network addresses within computer networks in IP packets (layer 3).

You can configure a maximum of one virtual interface in “Client (NAT)” operating mode.

- Open web-based management (see “Accessing web-based management”) and log in.
- Click “Configuration, WLAN Interface”.
- On the “WLAN Interface” page, set the “Client (NAT)” option for “Operating Mode”.

Figure 4-10 Configuring the client (NAT): Setting

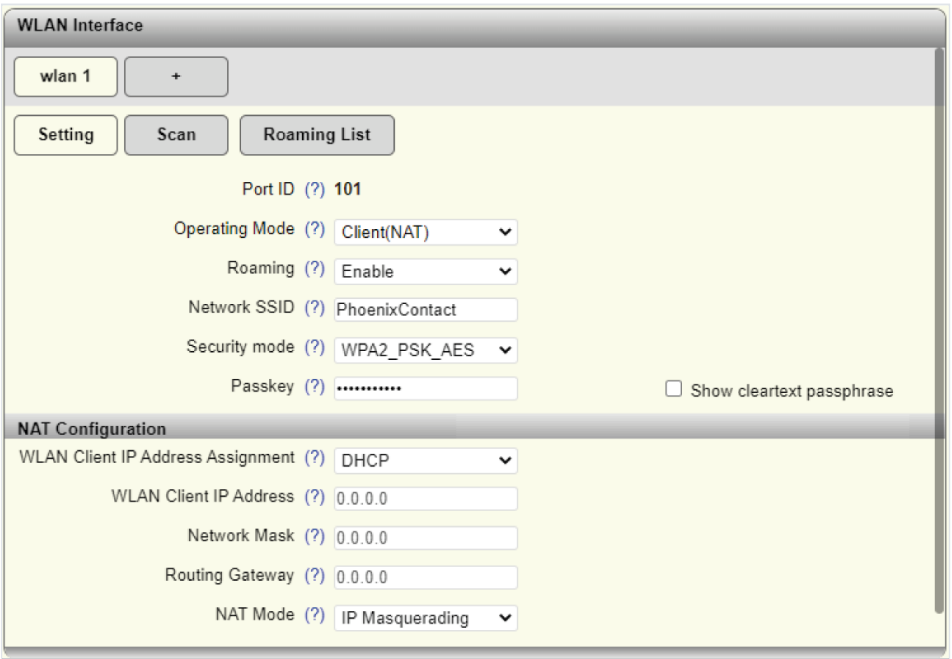


Tabelle 4-9 Configuring the client (NAT): Setting: Parameters

Parameters	Description
Port ID	The internal port ID of the wireless interface is displayed here.
Operating Mode	Select the “Client(NAT)” option for the “NAT” operating mode.
Roaming	Select whether roaming should be activated. – Disable: Roaming is deactivated. The threshold for background scans is set to -94 dBm. This option is used in static configurations without roaming.

Parameters	Description
	– Enable: Roaming is activated. The threshold for background scans is set to -60 dBm (default setting). – Advanced config: Select this option if you already configured roaming on another interface (e.g., via CLI).
Network SSID	Here, enter the desired network SSID. The SSID is the network ID by means of which the WLAN device can connect to the client. The network SSID can have a maximum length of 32 characters. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space.
Security mode	Here, set the desired encryption method for the WLAN interface. – None: No encryption. This option puts network security at risk. – WPA-PSK (TKIP): This encryption method is used by older devices that do not support WPA/AES. – WPA2-PSK (AES): This encryption method is secure and fast. It is suitable for client roaming. – FT-PSK (AES): This encryption method supports Fast Transition (802.11 r fast roaming). It is a symmetric encryption system with a pre-shared key (PSK) and AES. – WPA2-EAP: This encryption method is used for RADIUS authentication (see RADIUS certificates). For further information about the parameters available for this encryption method, see Encryption:WPA2-EAP and FT-EAPEncryption:WPA2-EAP and FT-EAP. – FT-EAP: This option supports Fast Transition (802.11 r fast roaming) with authentication via EAP and RADIUS. For further information about the parameters available for this encryption method, see Encryption:WPA2-EAP and FT-EAP. – WPA3-SAE: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. SAE is an established method from mesh networks that is used for the initial handshake. – WPA3-EAP: WPA3 is the latest generation of WLAN encryption, which fixes some of the known security vulnerabilities of WPA2. EAP is an established protocol used for this purpose. – ENHANCED OPEN: This encryption corresponds to WPA2-PSK encryption. You do not need to enter a passkey, but WPA2-PSK data protection and ease of use are still guaranteed.

Parameters	Description
	NOTE: Network security at risk If you select “None”, the data is sent without encryption. This option puts network security at risk.
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between eight and 64 characters long. For a high level of security, we recommend a random string. Letters, numbers, and the following special characters are permitted: $%@&/\ ()=?![]{}+*-_<>#^.,:~|. Exception for WEP: WEP64: five alphanumeric characters or ten hex digits WEP128: 13 alphanumeric characters or 26 hex digits

WLAN interface: Setting: NAT Configuration

Tabelle 4-10 Setting: NAT Configuration: Parameters

Parameters	Description
WLAN Client IP Address Assignment	Select the type of IP address assignment. – STATIC: Static IP address – DHCP: Assignment via a DHCP server (see DHCP Service).
WLAN Client IP Address	This option is only available if you selected “STATIC” for “WLAN Client IP Address Assignment”. Enter the IP address of the WLAN client here.
Network Mask	This option is only available if you selected “STATIC” for “WLAN Client IP Address Assignment”. Enter the subnet mask of the target network to which the static route refers here.
Routing Gateway	This option is only available if you selected “STATIC” for “WLAN Client IP Address Assignment”. Enter the IP address of the routing gateway here.
NAT Mode	Set the desired NAT mode. Confirm your selection by clicking “Apply”. – 1-to-1 NAT: For further information, see *Configuring 1-to-1 NAT*. – IP Masquerading: For further information, see Configuring IP Masquerading.

The other parameters on this page depend on the selected NAT mode and are dealt with in the corresponding sections (see 1-to-1 NAT Configuration and IP Masquerading Configuration).

4.3.1 1:1 NAT

With 1:1 NAT, each device in the WLAN is assigned an IP address from the higher-level network (WAN). The device can then be addressed from the WAN via this assigned address.

Advantages:

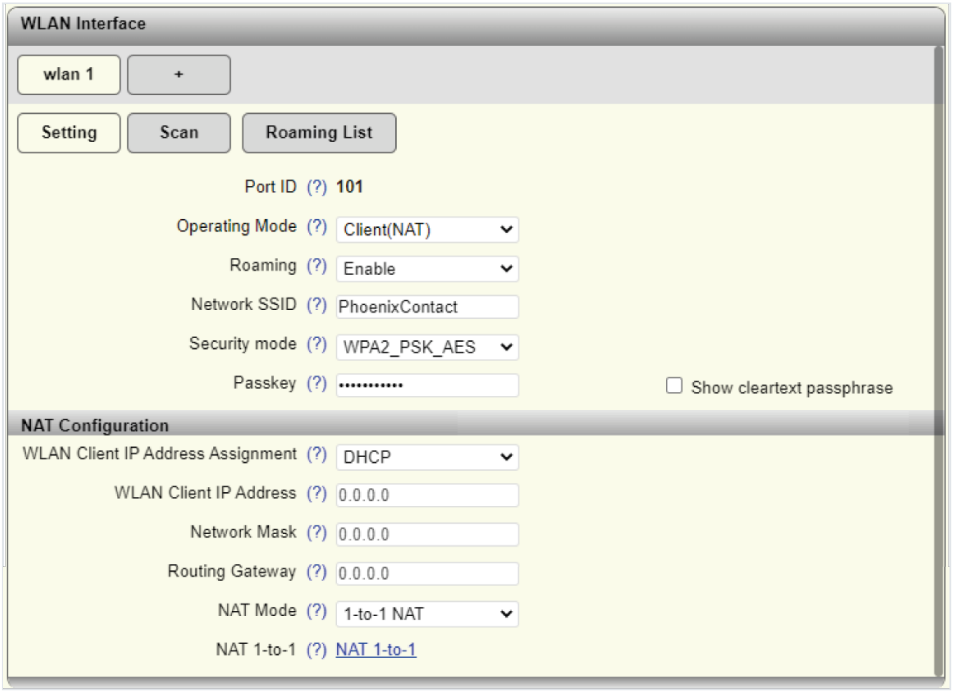
– No route or gateway configuration necessary in the WAN
– Communication can be established from both the LAN and WAN
– Not restricted to dedicated protocols

Disadvantage:

– An IP address must be reserved in the WAN for each device that should be accessible in the LAN.

4.3.1.1 Configuring 1:1 NAT

Figure 4-11 Configuring 1:1 NAT



- On the “WLAN Interface” page, set the “Client (NAT)” option for “Operating Mode”.
- For “NAT Mode”, select the “1-to-1 NAT” option.
- Click “Apply”.

Once you have clicked “Apply”, the additional “NAT 1-to-1” option appears.

- Click “NAT 1-to-1” to open the 1-to-1 NAT Configuration pop-up window. There, you can make further settings for 1:1 NAT.

4.3.1.2 Example configuration

Figure 4-12 1:1 NAT: Example configuration

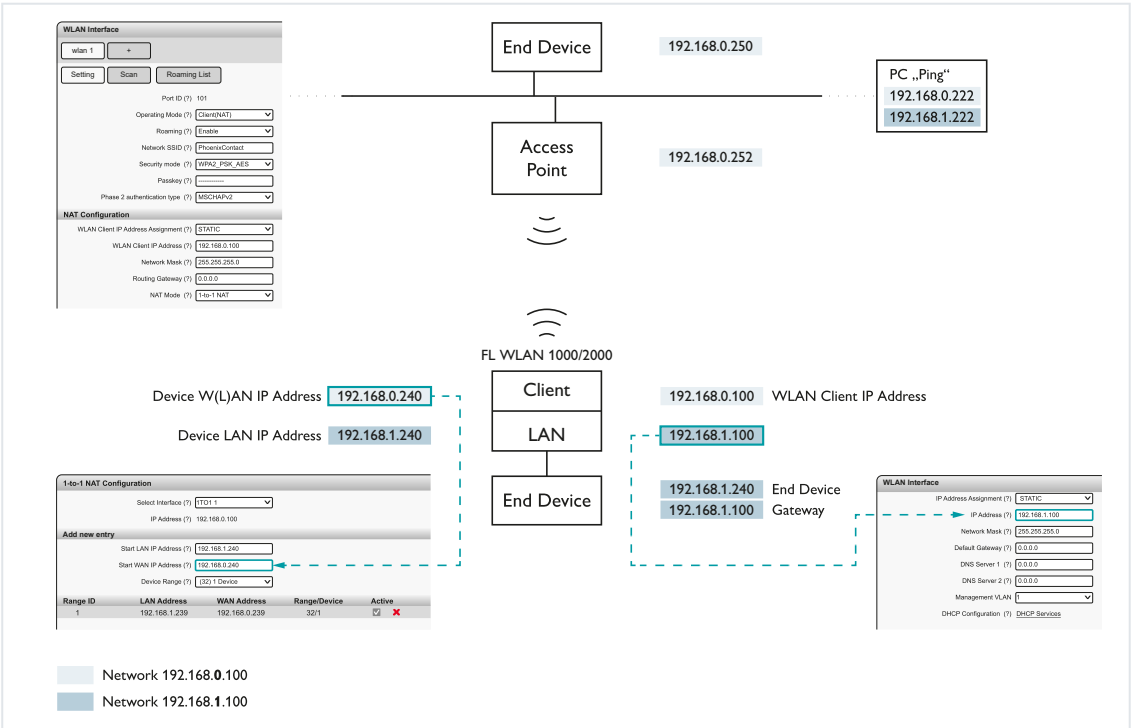
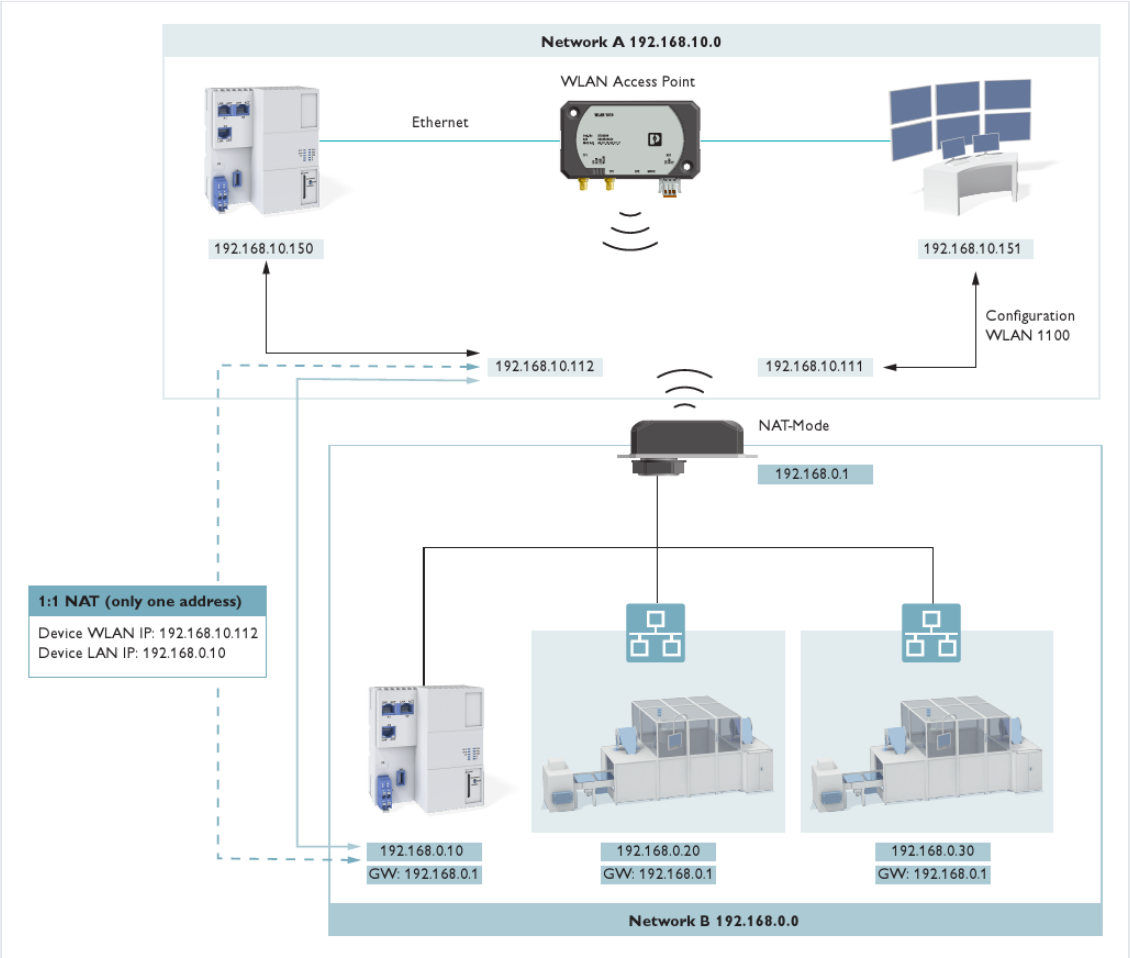


Figure 4-13 1:1 NAT: Example configuration 2



4.3.2 IP masquerading

The NAT device acts as a proxy, so that all the WLAN devices communicate externally using the IP address of the NAT/WAN port. Various TCP/UDP ports are used to differentiate between the different WLAN devices.

Advantages:

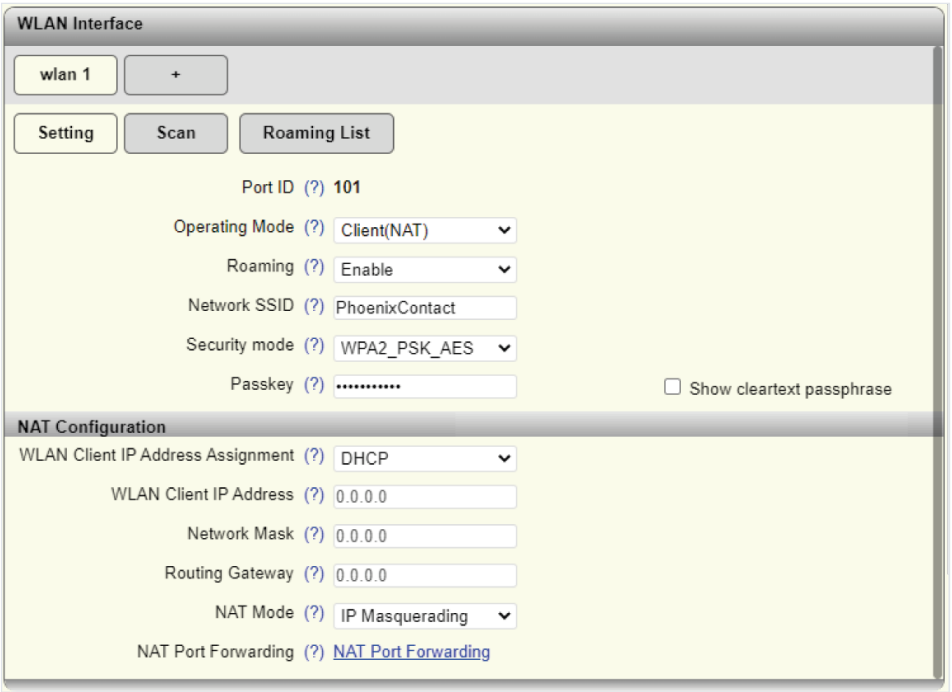
- No additional WAN addresses are required apart from the address for the NAT device itself.
- No route or gateway configuration necessary in the WAN.

Disadvantage:

- WAN devices can only communicate with WLAN devices via port forwarding.

4.3.2.1 Configuring IP masquerading

Figure 4-14 Configuring IP masquerading



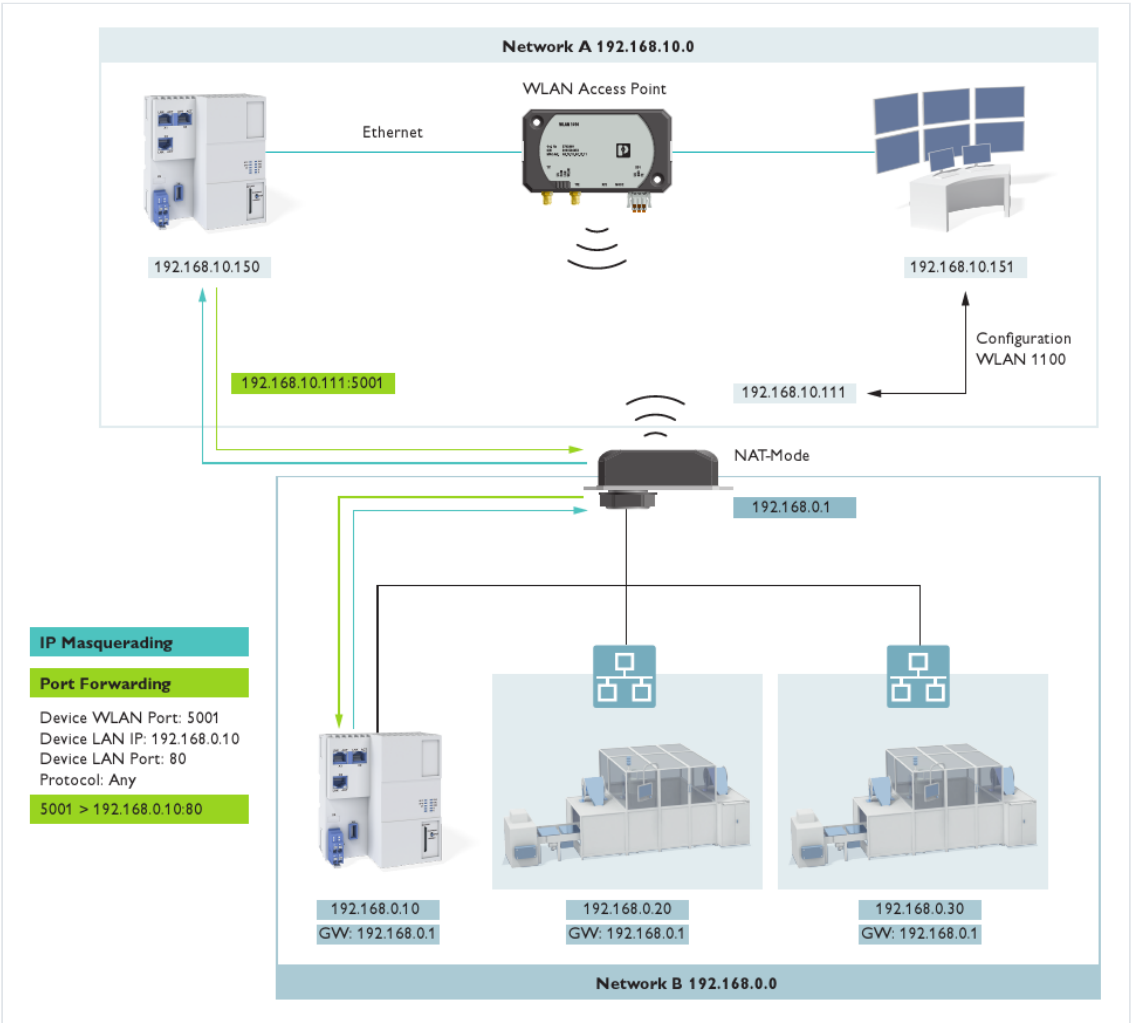
- On the “WLAN Interface” page, set the “Client (NAT)” option for “Operating Mode”.
- For “NAT Mode”, select “IP Masquerading”.
- Click “Apply”.

Once you have clicked “Apply”, the additional “NAT Port Forwarding” option appears.

- Click “NAT Port Forwarding” to open the IP Masquerading Configuration pop-up window. There, you can make further settings for IP masquerading.

4.3.2.2 Example configuration

Figure 4-15 IP masquerading: Example configuration



4.3.3 1-to-1 NAT configuration

Figure 4-16 Pop-up window: 1-to-1 NAT configuration

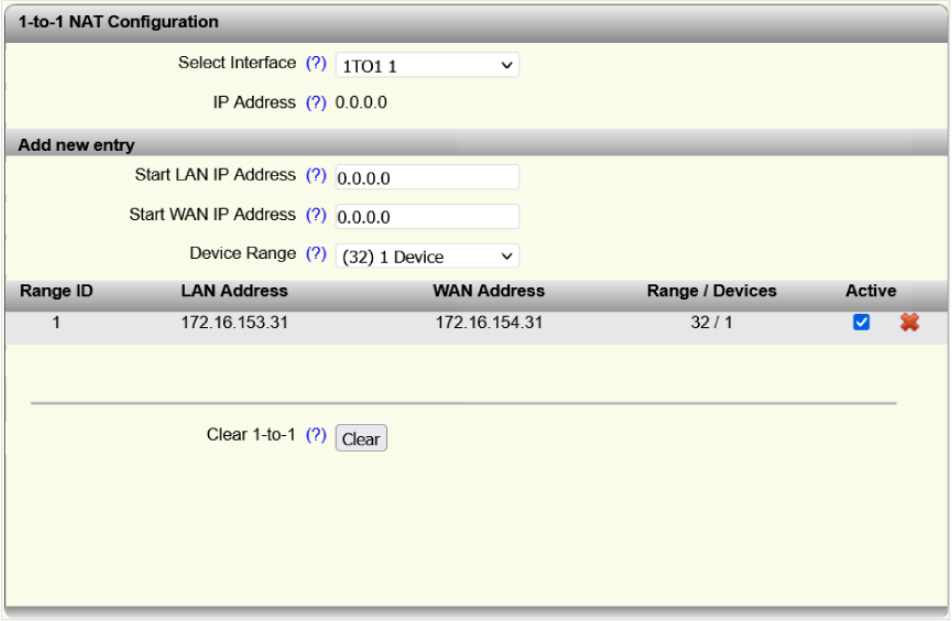


Tabelle 4-11 Pop-up window: 1-to-1 NAT configuration: Parameters

Parameters	Description
Select Interface	The interface is displayed here. There is only ever one interface available.
IP Address	The IP address of the client is displayed here.
Start LAN IP Address	Enter the start IP address of the area that is to be translated here.
Start WAN IP Address	Enter the start IP address of the area that is to be translated to here. The IP addresses must be reserved in the higher-level network. Using 1:1 NAT, the device translates them to the LAN IP address specified above.
Device Range	Select the number of IP addresses that are to be translated here.
Clear 1-to-1	Click “Clear” to delete the complete table for the selected interface.

- Set the parameters as desired.
- Click “Apply” to populate the table with the entered data.
- To populate the table with more data, enter the desired parameters again and click “Apply”.
- Close the “1-to-1 NAT Configuration” pop-up window.
- Click “Scan”.

- Click “Scan” to search for available access points. Available access points are displayed in the table with information such as the SSID or the signal strength (see Configuring the client (SCB): ScanConfiguring the client (SCB): Scan).
- Click “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.
- Click “Roaming List”.
- Select whether the device should search all available channels for networks or only selected channels (see Configuring the client (SCB): Roaming ListConfiguring the client (SCB): Roaming List).

The more channels you select, the longer will roaming take. Only select the channels you want to search for networks.

- If you select “SELECTED”, you can now select the channels manually for the 2.4 GHz and 5 GHz ranges.
- Confirm your settings by clicking “Apply&Save”.

4.3.4 IP masquerading configuration

Figure 4-17 Pop-up window: IP masquerading configuration

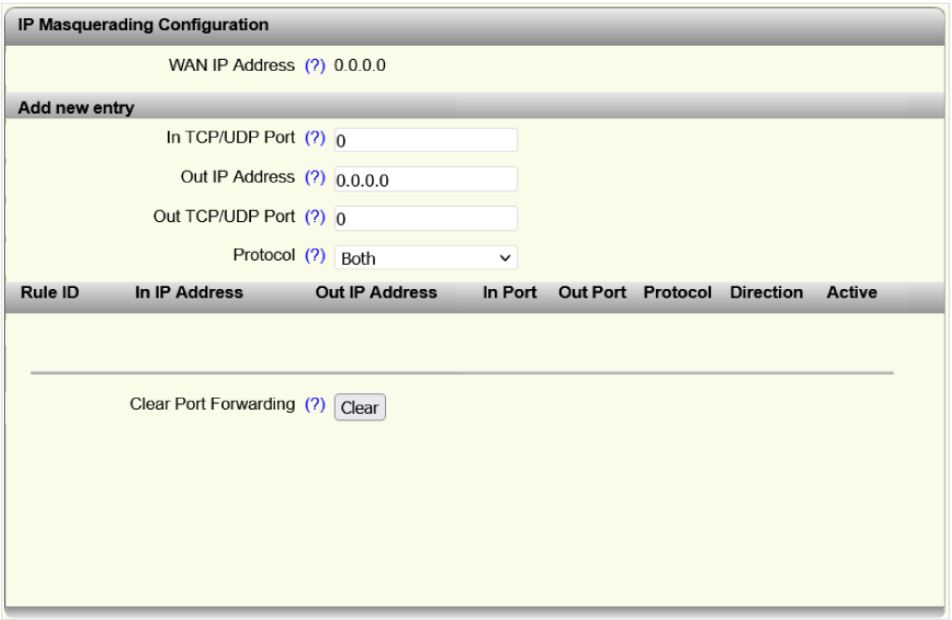


Tabelle 4-12 Pop-up window: IP masquerading configuration: Parameters

Parameters	Description
WAN IP Address	The IP address of the WLAN client is displayed here.
In TCP/UDP Port	Here, enter the TCP/UDP port for incoming data packets.
Out IP Address	Here, enter the IP address for outgoing data packets. This IP address is visible externally.
Out TCP/UDP Port	Here, enter the TCP/UDP port for outgoing data packets.

Parameters	Description
Protocol	Here, select the protocol to be used. – TCP: The Transmission Control Protocol (TCP) uses a three-way handshake to establish communication. This ensures that all data packets are correct and complete on arrival at their destination. The data packets are transmitted more slowly. TCP adds a bigger header to the data packets. – UDP: The User Datagram Protocol (UDP) does not establish an initial connection and does not check whether data packets arrive at their destination. UDP transmits data packets more quickly and adds a header with a smaller size to the data packets. – Both: TCP and UDP are used.
Clear Port Forwarding	Click on “Clear” to delete the complete table for the selected interface.

- Set the parameters as desired.
- Click “Apply” to populate the table with the entered data.
- To populate the table with more data, enter the desired parameters again and click “Apply”.
- Close the “IP Masquerading Configuration“ pop-up window.
- Click “Scan”.
- Click “Scan” to search for available access points. Available access points are displayed in the table with information such as the SSID or the signal strength (see Configuring the client (SCB): ScanConfiguring the client (SCB): Scan).
- Click “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.
- Click “Roaming List”.
- Select whether the device should search all available channels for networks or only selected channels (see Configuring the client (SCB): Roaming ListConfiguring the client (SCB): Roaming List).

The more channels you select, the longer will roaming take. Only select the channels you want to search for networks.

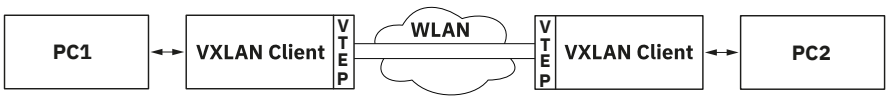
- If you select “SELECTED”, you can now select the channels manually for the 2.4 GHz and 5 GHz ranges.
- Confirm your settings by clicking “Apply&Save”.

4.4 Operating mode: Client (VXLAN) and access point (VXLAN)

The devices provide VXLAN (Virtual Extensible LAN) for communication protocols that are not IP-based but require layer 2 transparent communication.

VXLAN encapsulates each data packet in an IP frame. Virtual tunnel end points (VTEP) are required at the start and end of the communication connection. Any infrastructure that can transmit IP frames can be used in between.

Figure 4-18 VXLAN process



A VXLAN structure does not have to be limited to two tunnel end points. For example, several WLAN clients can communicate with each other in VXLAN mode in a network.

VXLAN is available as a client (VXLAN) and as an access point (VXLAN).

4.4.1 Configuring the client (VXLAN)

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.
- Select the “Client(VXLAN)” option as the “Operating Mode”.

Figure 4-19 Configuring the client (VXLAN)

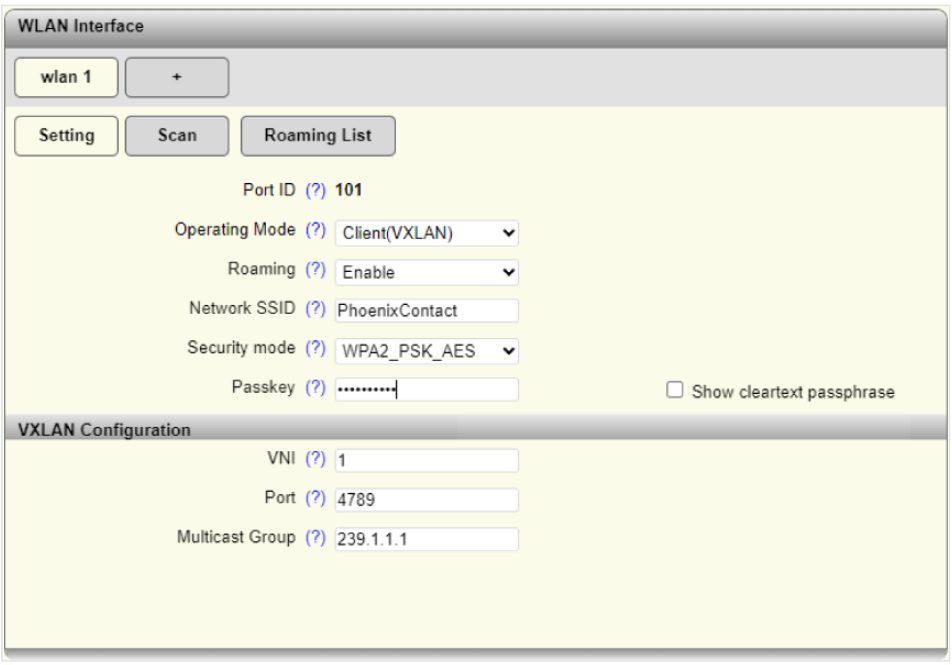


Tabelle 4-13 Configuring the client (VXLAN): Parameters

Parameters	Description
VNI	Enter the VXLAN Network Identifier (VNI). All devices that use this VNI form a shared virtual network.
Port	Enter the IP port number. All devices that form a shared virtual network must use the same IP port number.
Multicast Group	Enter the multicast group. All devices that form a shared virtual network must use the same multicast group. If there are other infrastructure components (e.g., switches, routers) between the two VTEPs, make sure that data traffic to this multicast group is forwarded to the peer.

- Define the parameters in the “VXLAN Configuration” area as desired and click “Apply&Save”.

4.4.2 Configuring the access point (VXLAN)

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.
- Select the “Access Point(VXLAN)” option as the “Operating Mode”.

Figure 4-20 Configuring the access point (VXLAN)

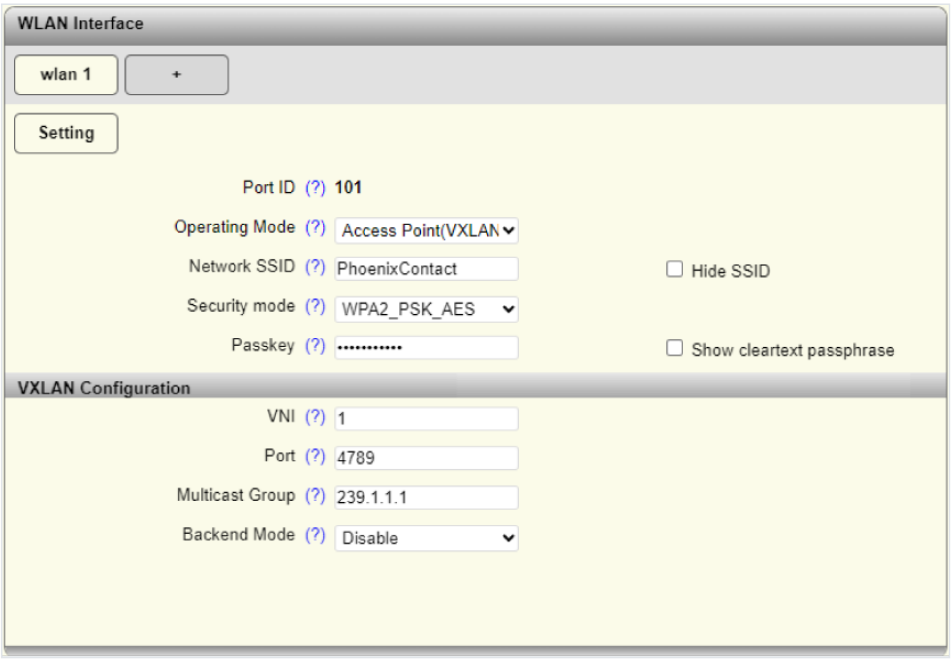


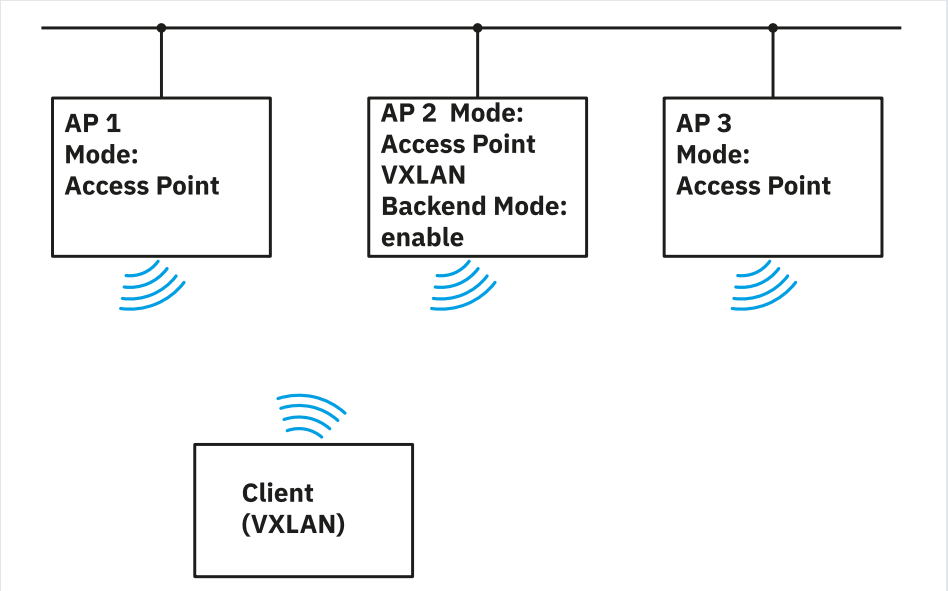
Tabelle 4-14 Configuring the access point (VXLAN): Parameters

Parameters	Description
VNI	Enter the VXLAN Network Identifier (VNI). All devices that use this VNI form a shared virtual network.
Port	Enter the IP port number. All devices that form a shared virtual network must use the same IP port number.
Multicast Group	Enter the multicast group. All devices that form a shared virtual network must use the same multicast group. If there are other infrastructure components (e.g., switches, routers) between the two VTEPs, make sure that data traffic to this multicast group is forwarded to the peer.
Backend Mode	Select whether backend mode should be activated. Activate the mode on the VXLAN access point to enable Layer 2-transparent communication via VxLAN. Roaming to other access points in normal access point mode is possible. Make sure that there are no other access points with activated backend mode and the same multicast group in the network.

- Define the parameters in the “VXLAN Configuration” area as desired and click “Apply&Save”.

To set up a VXLAN-capable access point infrastructure, only one device may work in “Access Point(VXLAN)” mode with a specific port. Additional access points are configured in normal “Access Point” mode.

Figure 4-21 Access point functionality (VXLAN)



In this case, all other access points send their VXLAN packets to the VXLAN access point. The backend mode is switched to “Enable” at this point.

In this configuration, VXLAN clients can roam between the access points. The operating mode also allows layer 2 transparent communication via third-party access points.

Make sure that there is no other VXLAN access point with the same settings for VNI, port, and multicast group. Otherwise a loop is formed.

VXLAN adds additional information to each data packet. This makes the package approx. 50 bytes longer. This can reduce the data throughput. Note this effect when considering the required MTU size.

VXLAN transmits the user data unencrypted. Depending on the application, suitable additional security mechanisms must be used (e.g., WPA2-AES on the WLAN side).

Only one VXLAN end point (VTEP) can be configured in a device. A VXLAN repeater is not possible. If the device is configured as a repeater in MCB mode on the client side, it can establish IP-based communication at the Ethernet port, but not layer 2-based communication.

4.5 Operating mode: Repeater

The devices have two virtual wireless interfaces, which can be individually configured. Two access points or, alternatively, one access point and one client, can be configured at the same time. You can regard the combination of access point and client as a repeater. In the “Quick Setup” menu, you can configure both virtual wireless interfaces under “Repeater” (see Quick setup). The “WLAN Interface” menu shows both virtual

wireless interfaces separately, without using the term “Repeater” (see WLAN interface). The functionality is the same.

Note that both virtual interfaces always run via a physical wireless band. This ensures that both interfaces always operate on the same radio channel. Different SSIDs and passwords can be used on both virtual interfaces. This allows for the setup of two virtual access points with different network names (SSIDs). Alternatively, you can connect a virtual interface to the network with the SSID “A” as a client. Simultaneously, the other virtual interface can be used as an access point to set up another network, SSID “B”.

You cannot set up a chain of repeaters with the devices.

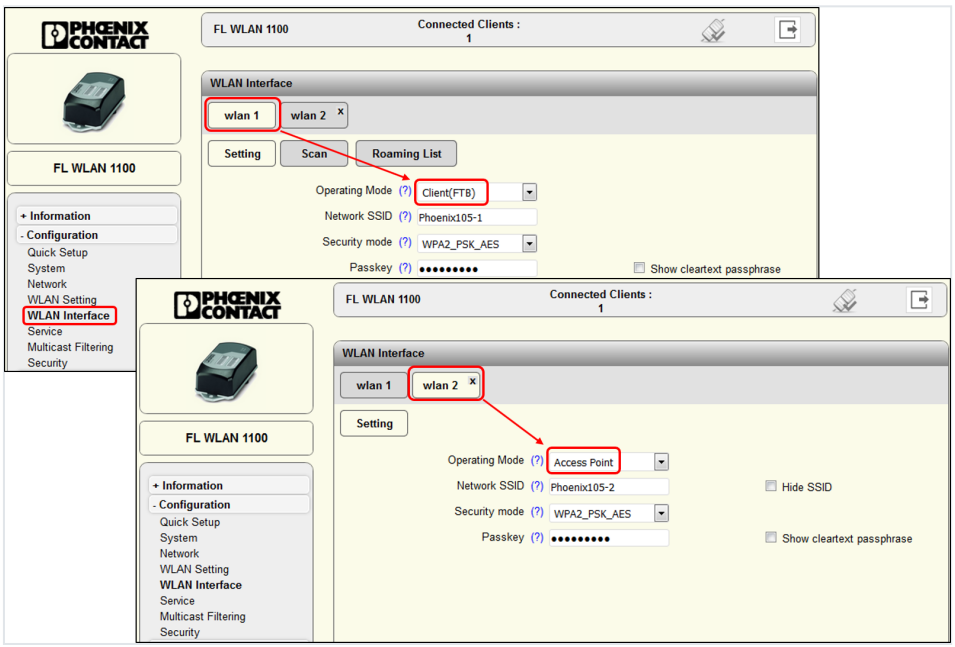
4.5.1 Example configuration

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.

Configure the first interface as a client and the second interface as an access point:

- Set “Client(FTB)” once and “Access Point” once for “Operating Mode”.

Figure 4-22 Configuration of two virtual interfaces



Do not connect any devices in FTB mode to the access point.
Only connect access points to the client (FTB) that support FTB mode (e.g., FL WLAN 510X, FL WLAN 110X/210X).

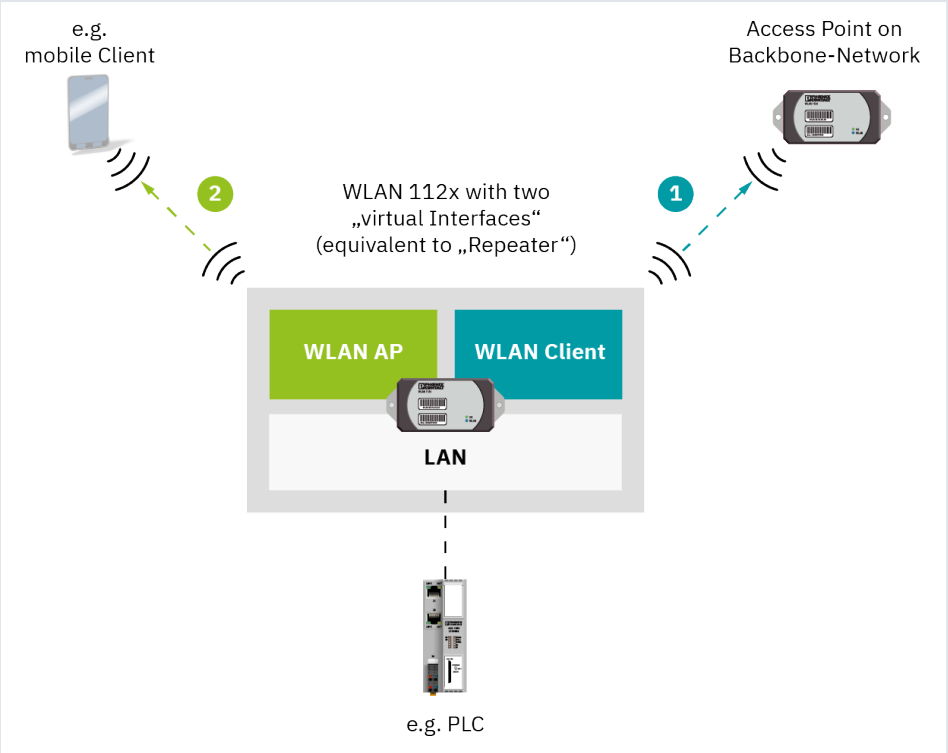
Bei der Konfiguration von zwei virtuellen Funkschnittstellen sollten Sie immer "WLAN 2" als normalen Access Point konfigurieren. "WLAN 1" können Sie wahlweise als Access Point oder Client konfigurieren.

The operating mode as a repeater reduces the bandwidth.

4.5.2 Properties of two virtual wireless interfaces

The properties of the two virtual wireless interfaces and their mutual dependence are described in the following.

Figure 4-23 Structural representation of the two wireless interfaces and one cable interface using the FL WLAN 112x as an example



The connection (1) between the WLAN client and the higher-level access point must be established initially after voltage has been applied. Only then will the connection via the WLAN access point be available. From then on, connection (2) is maintained even if connection (1) is interrupted. The latter applies until the next power reset of the device (see Structural representation of the two wireless interfaces and one cable interface).

When configuring the virtual wireless interface as a client, it is recommended that only those channels that will be utilized by the application be activated in the “Roaming List”. This increases the performance of the device and the connection time is reduced.

5 DHCP service

5.1 Activating the DHCP service

The FL WLAN 112x/102x devices have an interface-based DHCP server. It is deactivated in the default settings. You can activate and configure it as described below.

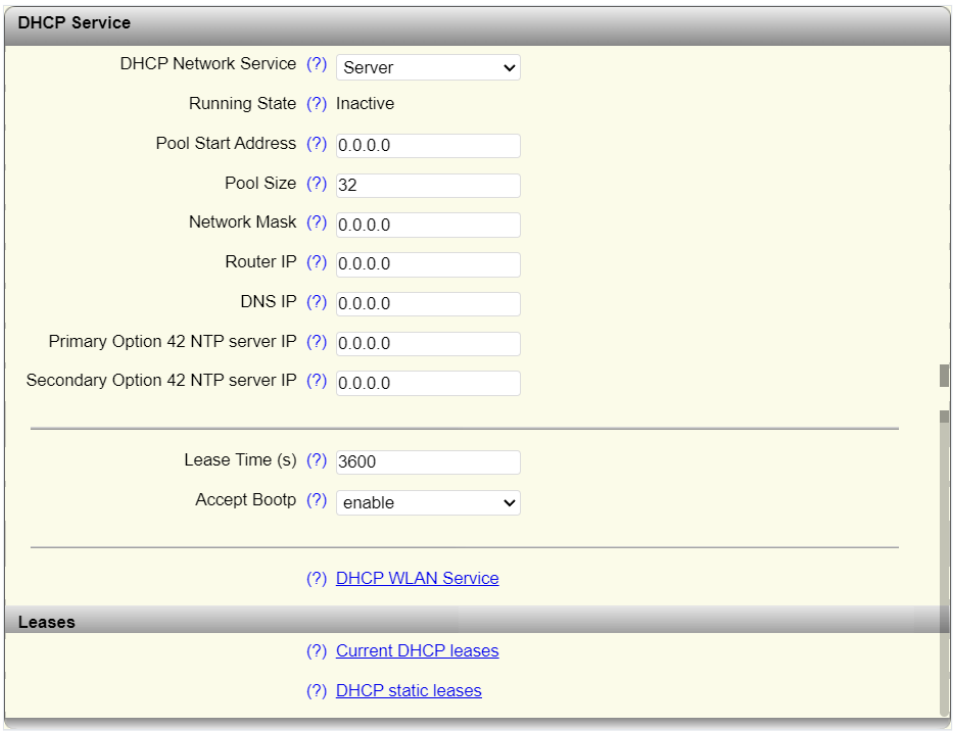
You can configure the various interfaces globally. Alternatively, users can choose to either allow DHCP addresses to be assigned via selected interfaces only or to assign different address blocks for various interfaces. Interfaces include one LAN interface and one or two WLAN wireless interfaces that are configured as access points. Each of the three can be configured separately.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, Network”.
- In the “IP Address Assignment” drop-down list, select the “STATIC” option.

↪ The “DHCP Configuration” menu item appears.

- Click “DHCP Services”.

Figure 5-1 DHCP Service



- In the “DHCP Network Service” drop-down list, select the “Server” option to activate the global DHCP server.

If you select “None”, the assignment of IP addresses via DHCP will be deactivated again if applicable.

- Click “Apply”.

5.2 Activating the global DHCP server at all interfaces

You can assign IP addresses via DHCP via all interfaces, on the cable side via LAN and via the WLAN 1 and WLAN 2 wireless interfaces. The “global IP address pool” is managed on the “DHCP Service” page. The address pool configured here applies to all interfaces.

- Activate the DHCP server (see Activating DHCP Service).
- You can now set the following parameters:

The following fields are only visible if you have selected the “Server” option in the previous step.

Tabelle 5-1 DHCP Service: Parameters

Parameters	Description
DHCP Network Service	Select the DHCP service you want to use. – None: The device does not use any DHCP service. – Server: The device is used as DHCP server.
Running State	The current DHCP server status is displayed here. If “Inactive” is displayed, check your settings. The current status is also “Active” if only the pool of a single interface has been configured. This means you do not necessarily need to configure the global pool.
Pool Start Address	Enter the first IP address of the DHCP server address pool here. The “Pool Start Address”, “Pool Size”, and “Network Mask” parameters must match one other. The IP range 169.254.x.x cannot be configured.
Pool Size	Enter the number of IP addresses in the DHCP server address pool here. Please note that the number of IP addresses must match the configured subnet.
Network Mask	Enter the subnet mask here that is assigned to the DHCP clients.
Router IP	Enter the router/default gateway IP address here that is assigned to the DHCP clients.
DNS IP	Enter the DNS IP address here that is assigned to the DHCP clients.
Primary Option 42 NTP server IP	Enter the primary IP address of the NTP server (option 42) that is assigned to the DHCP clients.
Secondary Option 42 NTP server IP	Enter the secondary IP address of the NTP server (option 42) that is assigned to the DHCP clients.

Parameters	Description
Lease Time (s)	Enter the time here in seconds for which the DHCP server leases an IP address to a client before it has to report to the server again. The value must be between 300 and 2,592,000 seconds (default: 3,600). If no time limit is required, enter a value of “0”.
Accept Bootp	Select here whether the WLAN device acting as the DHCP server accepts BootP requests. If this function is activated, an IP address with an infinite lease time is assigned to the requesting DHCP clients.
DHCP WLAN Service	Click “DHCP WLAN Service” to open the “DHCP WLAN Service” pop-up window (see Pop-up window: DHCP WLAN Service).
Current DHCP leases	Click “Current DHCP leases” to open the “Current DHCP leases” pop-up window containing an overview of all IP addresses that are currently assigned (see Pop-up window: Current DHCP Leases).
DHCP static leases	Click “DHCP static leases” to open the “DHCP Static Leases” pop-up window for configuring static IP address assignments (see Pop-up window: DHCP Static Leases).

You will receive no address via the LAN interface if you do not configure the pool start address (0.0.0.0).

Once all addresses of the global address pool have been assigned, no more addresses will be assigned on request.

5.3 Activating the DHCP server on WLAN interfaces only

By means of the configuration described below, IP addresses can be assigned via DHCP via the WLAN interface(s) only, but not via the cable-side LAN interface.

Use case (example): The device is to be installed as an access point in a machine with static IP addresses, where IP addresses are only to be assigned to temporarily connected smart devices via WLAN.

- Activate the DHCP server (see Activating DHCP Service).
- Do not enter an IP address for “Pool Start Address”. No IP addresses will then be assigned via the LAN interface.
- Click “DHCP WLAN Services”.

Pop-up window: DHCP WLAN Service

Figure 5-2 Pop-up window: DHCP WLAN Service

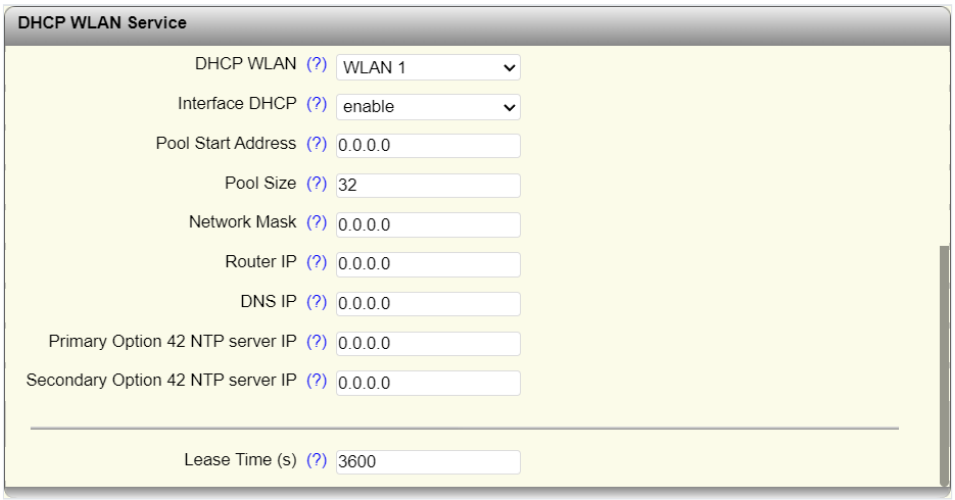


Tabelle 5-2 DHCP WLAN Service: Parameters

Parameters	Description
DHCP WLAN	Here, select the desired WLAN interface. You may need to configure the WLAN interfaces first (see WLAN Interface).
Interface DHCP	Select whether DHCP should be activated on the selected WLAN interface.
Pool Start Address	Here, enter the first IP address of the DHCP server address pool. The parameters “Pool Start Address”, “Pool Size”, and “Network Mask” must match one other. The IP range 169.254.x.x cannot be configured.
Pool Size	Here, enter the number of IP addresses in the DHCP server address pool. Please note that the number of IP addresses must match the configured subnet.
Network Mask	Here, enter the subnet mask that is assigned to the DHCP clients.
Router IP	Here, enter the router/default gateway IP address that is assigned to the DHCP clients.
DNS IP	Here, enter the DNS IP address that is assigned to the DHCP clients.
Primary Option 42 NTP server IP	Enter the primary IP address of the NTP server (option 42) that is assigned to the DHCP clients.
Secondary Option 42 NTP server IP	Enter the secondary IP address of the NTP server (option 42) that is assigned to the DHCP clients.

Parameters	Description
Lease Times (s)	Here, enter the time in seconds for which the DHCP server leases an IP address to a client before it has to report to the server again. The value must be between 300 and 2592000 seconds (default: 3600). If no time limit is required, enter a value of “0”.

This configuration enables addresses from the individually defined pool of each interface to be assigned after a DHCP request.

Overlapping address ranges: The IP address ranges of the address pools should not overlap. However, if that is the case, the address is only output at one interface.

Observe the following notes:

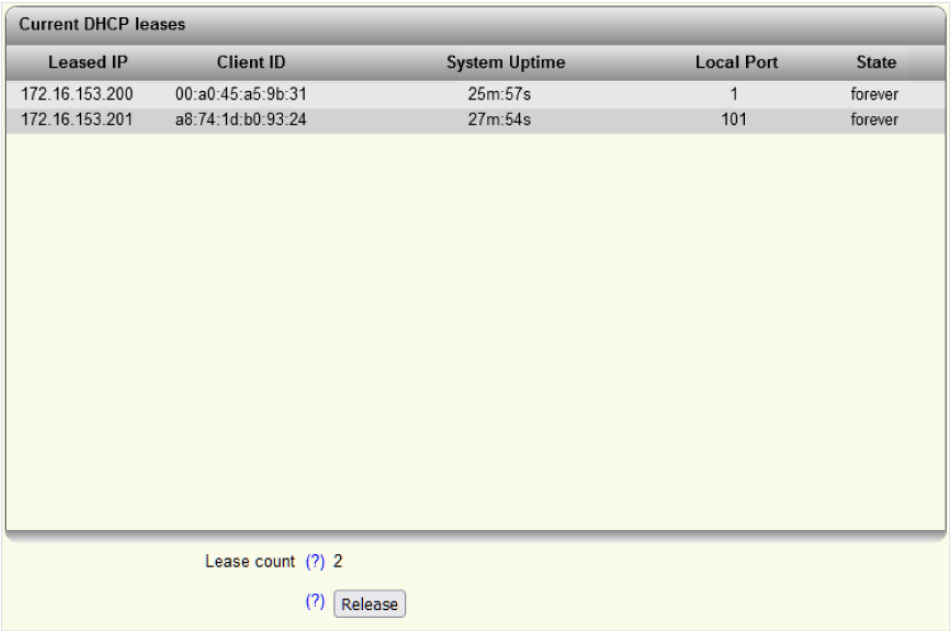
- DHCP requests on inactive interfaces (WLAN 1, WLAN 2) are not answered.
- Once all addresses of an WLAN address pool have been assigned, an address of the global pool is assigned via the WLAN interface.
- Once all addresses of the global address pool have been assigned, no address is assigned on request.
- Once all addresses of a WLAN interface have been assigned with the leases not having expired, no more addresses are assigned.

5.4 Diagnostics

- Activate the DHCP server (see Activating DHCP Service).
- Click “Current DHCP Leases”.

Pop-up window: Current DHCP Leases

Figure 5-3 Pop-up window: Current DHCP Leases



The table shows the IP addresses that are currently assigned via DHCP.

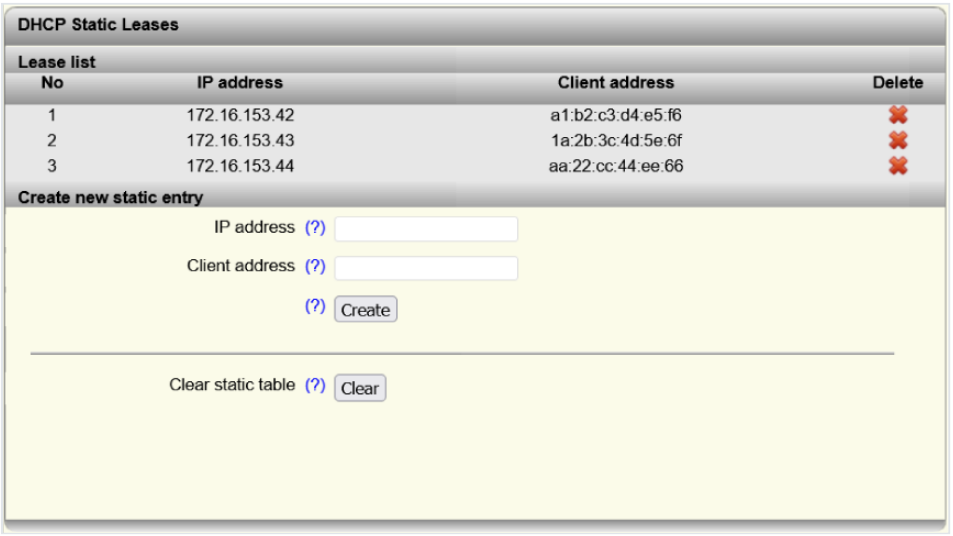
Tabelle 5-3 Current DHCP Leases: Parameters

Parameters	Description
Leased IP	This column shows the assigned IP addresses.
Client ID	This column shows the MAC address of the client to which the IP address is assigned.
System Uptime	This column shows the time that has elapsed since the IP address was assigned to the client.
Local Port	This column shows the interface to which the client is connected.
State	This column shows the status of the client.
Lease count	This field shows the number of assigned IP addresses.
Release	Click “Release” to release unused entries again.

Pop-up window: DHCP Static Leases

- Click “DHCP Static Leases”.

Figure 5-4 Pop-up window: DHCP Static Leases



The pop-up window shows the configured static IP address assignments. In addition, you can create new static IP address assignments here. To do so, assign a fixed IP address to MAC addresses.

Tabelle 5-4 DHCP Static Leases: Parameters

Parameters	Description
Lease list:	
No	This column numbers the entries consecutively.
IP address	This column shows the statically assigned IP address.
Client address	This column shows the MAC address of the client.
Delete	Click on the red “X” to delete the entry.
Create new static entry:	
IP address	Here, enter the static IP address that you wish to assign.
Client address	Here, enter the MAC address of the device for which you wish to assign a static IP address.
Create	Click on “Create” to carry out static assignment.
Clear static table	Click on “Clear” to delete all the static DHCP leases.

6 RADIUS certificates

6.1 General information

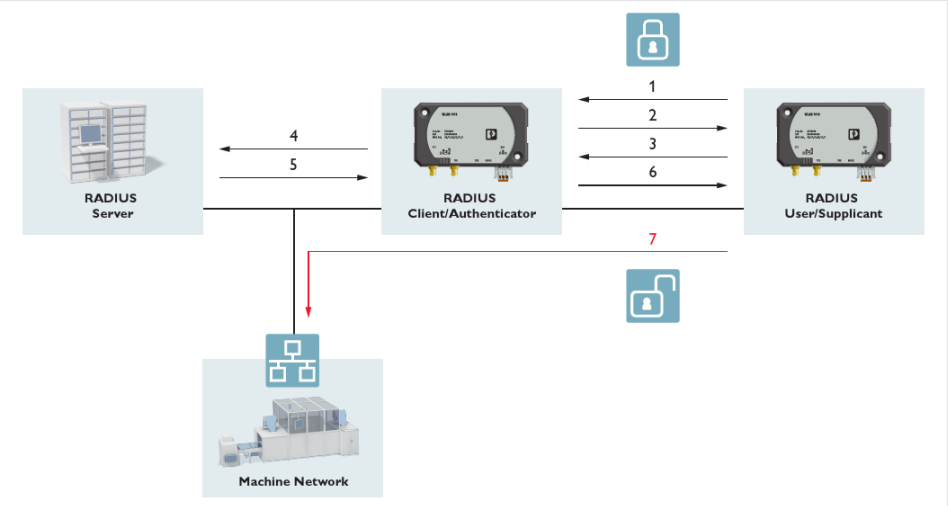
RADIUS stands for “Remote Authentication Dial-in User Service”. It is a client/server protocol that is also referred to as a “triple-A” protocol. The three A’s stand for authentication, authorization, and accounting.

RADIUS authentication implements the authentication method in accordance with standard IEEE 802.1X. This standard provides a general method for authentication and authorization in IEEE 920 networks. When a person (the “supplicant”) attempting access to the network connects to the device (the “authenticator”), a physical port on the device sends the PC’s certificates to a RADIUS authentication server using the Extensible Authentication Protocol (EAP). This verifies and, if applicable, sends a command back to the device that then permits access to the service offered by the device. By using an authentication server, you can also grant local, unrecognized devices access to the network. For example, members of an external service team can log into a network.

This authorization is usually performed once when the device initially connects. Once the device is disconnected, the device closes the port until the next connection. To be protected against sophisticated attempts at unauthorized access, you can configure the device to re-authenticate on a periodic time basis.

6.2 Sequence of the 802.1X authentication process

Figure 6-1 802.1X RADIUS process (simplified)

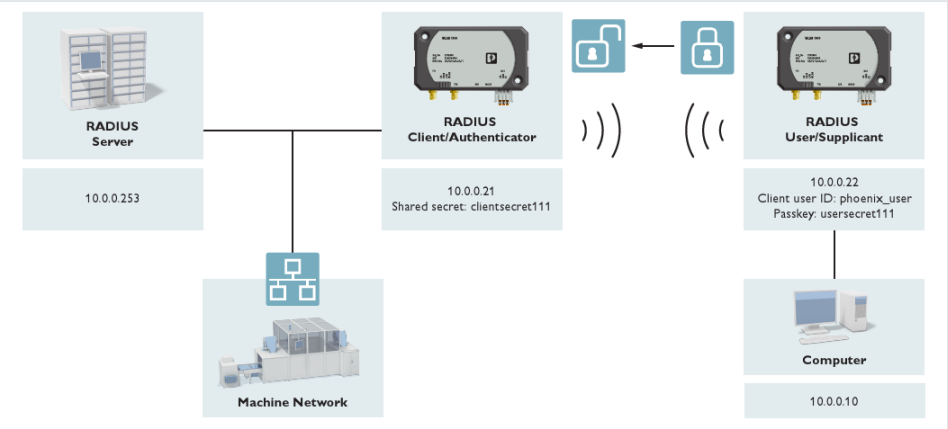


1. The supplicant sends a start packet to the authenticator.
2. The authenticator asks the supplicant for the access data.
3. The supplicant sends the access data to the authenticator.
4. The authenticator sends the supplicant’s access data as well as its own access data to the RADIUS server.
5. The RADIUS server sends its response (accept or refuse) to the authenticator.

6. If the response is positive, the authenticator opens the port for the supplicant and notifies the supplicant.
7. The supplicant can now access the network.

6.3 Example configuration

Figure 6-2 RADIUS: Example configuration



The RADIUS server requires the access data of the authenticator and the supplicant:

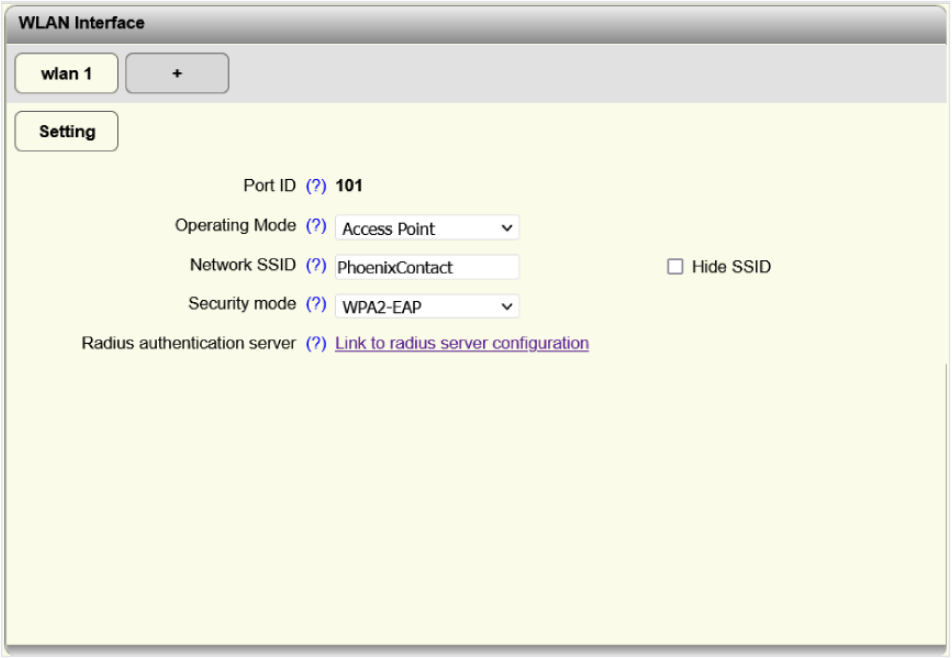
- Authenticator's access data:
  - IP address of authenticator: 10.0.0.21
  - Shared secret of authenticator: clientsecret111
- Supplicant's access data:
  - User name: phoenix_user
  - Passkey: usersecret111

6.4 Configuring RADIUS

6.4.1 Configuring the authenticator

- Open web-based management (see Accessing web-based management) and log in.
- Click "Configuration, WLAN Interface".

Figure 6-3 Configuring the authenticator: WLAN interface



- For “Operating Mode”, select the “Access Point” operating mode and assign a network SSID.
- For “Security mode”, select the “WPA2-EAP” encryption method and save your settings with “Apply&Save”.
- Click “Configuration, Security”.

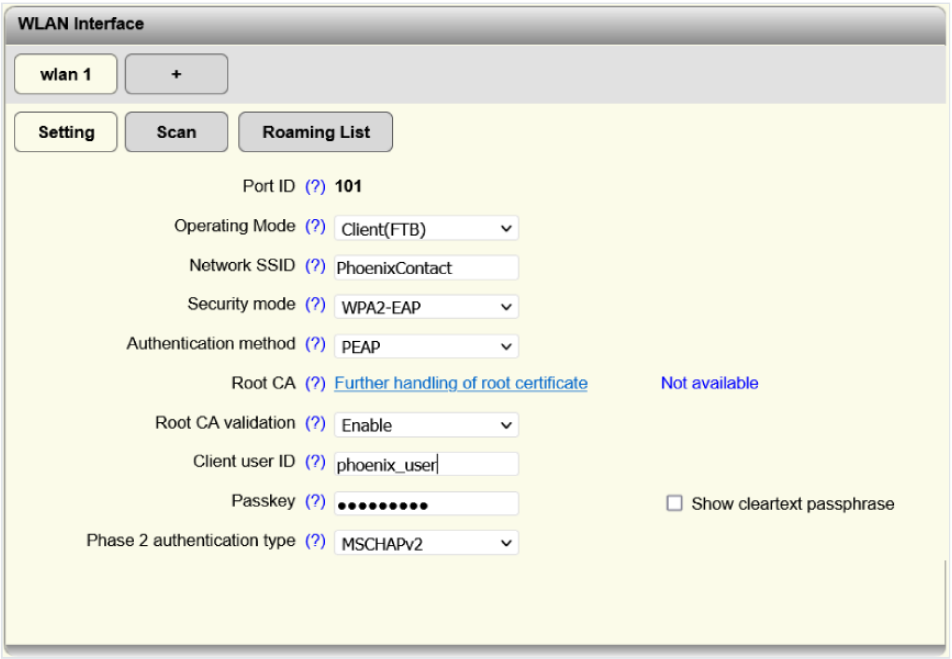
Figure 6-4 Configuring the authenticator: Security

- For “Radius Server”, enter the IP address of your RADIUS server.
- For “Radius Server Port”, enter the RADIUS server port in use.
- For “Radius Shared Secret”, enter the authenticator’s shared secret.
- Click “Apply&Save” to save your settings.

6.4.2 Configuring the supplicant

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.

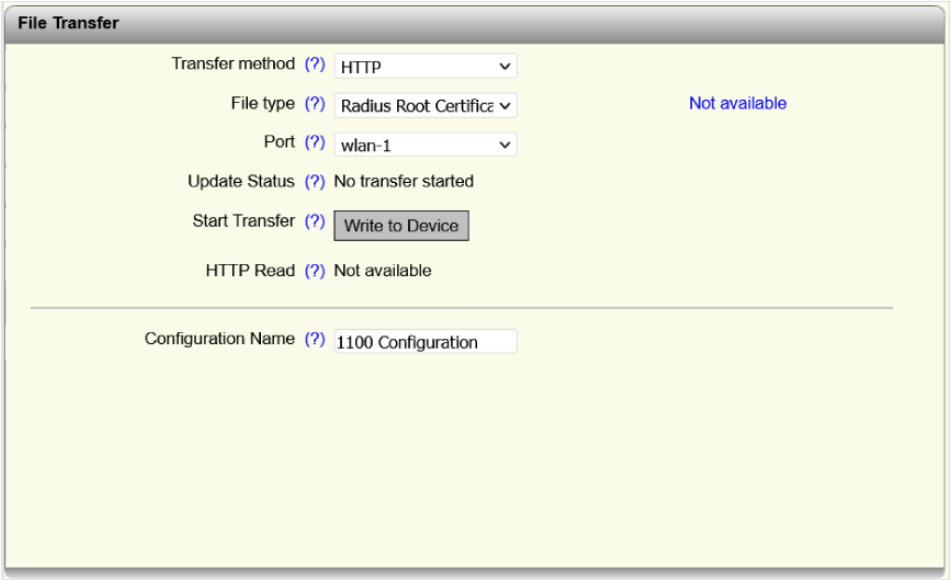
Figure 6-5 Configuring the supplicant: WLAN interface



- For “Operating Mode”, select the “Client(FTB)” operating mode and assign a network SSID.
- For “Security mode”, select the “WPA2-EAP” encryption method.
- For “Authentication method”, select “PEAP”.
- For “Client user ID”, enter a user name.
- For “Passkey”, enter a password.
- For “Phase 2 authentication type”, select “MSCHAPv2”.
- Save your settings with “Apply&Save”.
- Click “Further handling of root certificate” to open the “File Transfer” pop-up window.

For further information about the “HTTP” and “TFTP” transfer methods as well as the other parameters, see File transfer.

Figure 6-6 Configuring the supplicant: RADIUS root certificate with file transfer



- For “File type”, select the “Radius Root Certificate” option.
- For “Port”, select the port for which you made the above settings.
- Click “Write to Device” to select the RADIUS root certificate on your PC that is to be transferred to the device. The certificate is frequently called “ca.pem”.

If you select “TLS” as the authentication method, you must additionally upload a RADIUS client certificate, see File transfer.

The access data of the authenticator and the supplicant must be stored on the RADIUS server.

↪ The RADIUS functionality is set up and ready for operation.

6.4.3 Deactivating server identity verification

You can deactivate the server identity check. The server identity is then not validated.

NOTE: Network security at risk
If you deactivate the server identity check, the server identity is not validated. This option is not secure.

- Open web-based management (see Accessing web-based management) and log in.
- Click “Configuration, WLAN Interface”.
- For “Authentication method”, select “PEAP”.
- For “Root CA validation”, select “Disable”.

7 SNMP – Simple Network Management Protocol

7.1 General information

The Simple Network Management Protocol (SNMP) is a manufacturer-neutral standard for Ethernet management. It defines commands for reading and writing information and defines formats for error and status messages. SNMP also provides a structured model consisting of agents with their respective Management Information Base (MIB) and a manager. The manager is a software product that runs on a network management station. The agents are located within switches, bus terminals, routers, and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager requests this information on a regular basis and displays it. The configuration of the devices is possible with data written to the MIB by the manager. In urgent cases, the agents can also send messages (traps) directly to the manager. On the “Snapshot” page, you can save configurations and logs from the device with a click for diagnostic purposes and then make them available to a service technician for analysis.

All configuration changes that are to take effect after a device restart must be saved permanently.

For the SNMP commands supported by this device, refer to the download area for your device at phoenixcontact.net/qr/<item_number>.

- Download the current firmware for this.
- Unzip the firmware.
- Navigate to the folder “FL_WLAN_XXXX_MIBs_[version and date].zip”.
- Open the file “FL-MGD-INFRASTRUCT-MIB.mi2” with an editor of your choice.

↪ In this file you will find all the SNMP commands supported by this device.

7.2 SNMP interface

The components in the Factoryline product series each have an SNMP agent. This agent of the device manages the Management Information Base II (MIB 2) in accordance with RFC 1213.
Network management stations, such as a PC with the network manager, can read and change configuration and diagnostic data of the network devices via the Simple Network Management Protocol. You can use any SNMP tools or network management tools to access Factoryline products via SNMP. To do this, you must make the MIBs that are supported by the respective device available to the SNMP management tools.

On the one hand, these are globally valid MIBs that are defined and described in requests for comments (RFCs). These include, e.g., MIB 2 according to RFC 1213, which is supported by every SNMP-capable network device. On the other hand, each manufacturer can define its own private SNMP objects, which are then classified in the large SNMP object tree in a private manufacturer area. Each manufacturer is responsible for this private (enterprise) area. For example, they may only assign an object (object name and parameters) to an object ID once and publish it. If this object is then no longer required, it is marked as expiring, but not reused, e.g., with other parameters.

Phoenix Contact provides notification of the ASN1 SNMP objects by publishing their descriptions on the Internet pages.

For SNMP, the password “public” is used for read access and the password “private” is used for read/write access.

For SNMP, the password “public” is used for read access and the password “private” is used for read/write access.

Reading SNMP objects is not password protected. In SNMP, a password is required for read access. As is usual for network devices, however, this is set to “public” and cannot be changed. On delivery, the password for write access is “private” and can be changed by the user.

Another benefit for the user is the option of sending traps using the Simple Network Management Protocol.

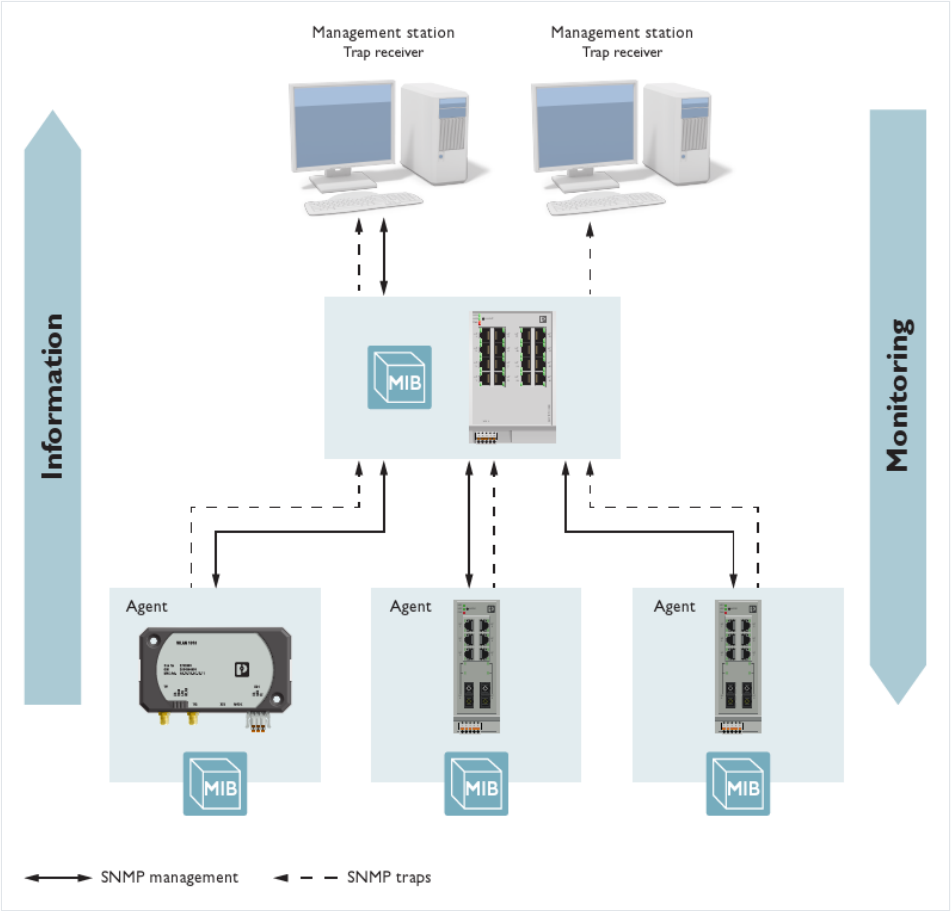
7.2.1 Management Information Base (MIB)

The Management Information Base (MIB) is a database that contains all the data (objects and variables) required for network management.

7.2.2 Agent

An agent is a software tool that collects data from the network device on which it is installed, and transmits this data on request. Agents reside in all managed network components and transmit the values of specific settings and parameters to the management station. On request by a manager or in response to a specific event, the agent transmits the collected information to the management station.

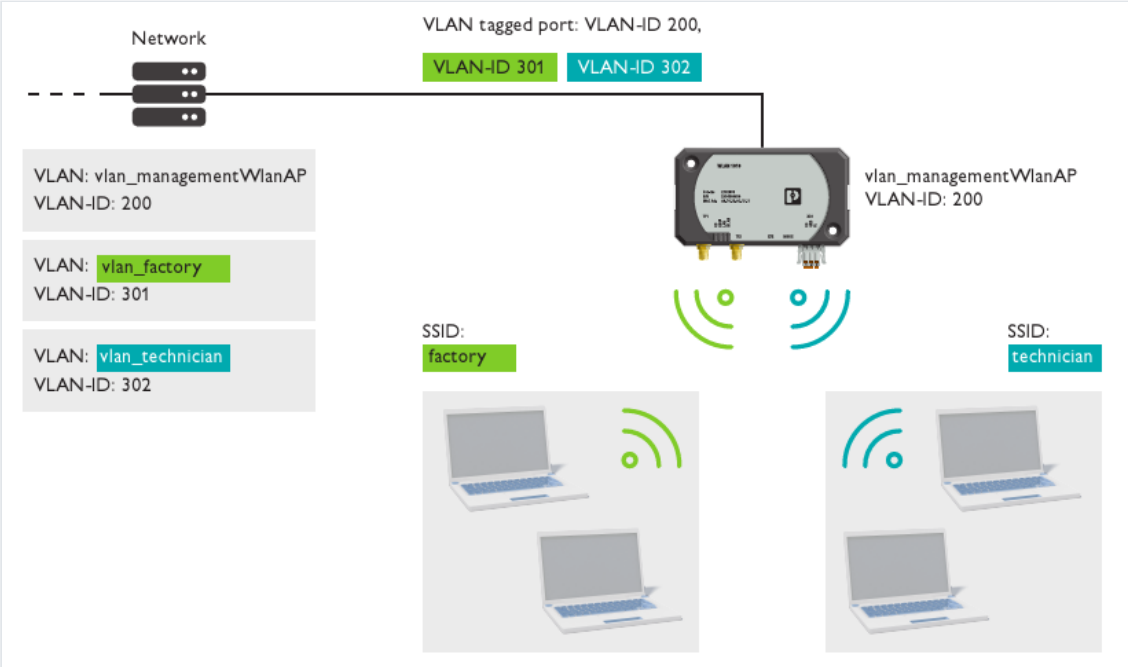
Figure 7-1 Schematic representation of SNMP management



8 VLAN – Virtual Local Area Network

8.1 Example configuration

Figure 8-1 Example of network separation via WLAN using VLAN



In the use case described, the two WLAN networks “factory” and “technician” are separated by different VLAN IDs (301 and 302). In the example, access to the configuration management of the access point was also assigned to another VLAN (VLAN ID 200).

8.2 Configuration via CLI

Network separation via WLAN with VLAN can be configured via the CLI. The following commands are required to implement the example described in the Figure above:

After issuing the “vlan status tagged” command, VLAN tagging is active. For further configuration of the access point, a connection via the management VLAN of the access point is required (here: VLAN ID 200).

Requirement

The WLAN device has an IP address.

```
wlan wifi config 101 operation-mode ap
wlan wifi config 101 profile config 1 ssid factory
ip interface create
wlan wifi config 101 network-ID 2
wlan wifi create 102
wlan wifi config 102 operation-mode ap
```

```
wlan wifi config 102 profile config 1 ssid technician
ip interface create
wlan wifi config 102 network-ID 3
vlan create 200
vlan static 200 name vlan_managementWlanAP
vlan create 301
vlan static 301 name vlan_factory
vlan create 302
vlan static 302 name vlan_technician
network mgmt-vlan 200
vlan routing add 301 2
vlan routing add 302 3
vlan status tagged
write
wlan apply-settings
```

9 Revision history

As the firmware platform continuously evolves and the devices on offer are constantly expanded, this help also changes.

You can find the changes to date in the table.

Revision	Date	Changes
00	2024-04-18	– Creation of this help (PDF)
01	03.09.2024	– Update to firmware 3.37

The changes to the firmware can be found in the respective release notes available for download with the firmware on the item page.

A Appendix

A 1 List of figures

Figure 2-1 Connection of the supply voltage and the digital input on the bottom of the device 17
Figure 2-2 Supply voltage connection and reset via MODE button 18
Figure 2-3 Parameterizing the BootP server 21
Figure 2-4 Starting the BootP server 22
Figure 2-5 Inserting BootP requests in the reservation list 22
Figure 3-1 Login area 26
Figure 3-2 Start page for web-based management (example) 26
Figure 3-3 WBM with icons (selection) 27
Figure 3-4 Help & Documentation 29
Figure 3-5 Device status 30
Figure 3-6 Local Diagnostics 31
Figure 3-7 Alarm and events 32
Figure 3-8 Connections 33
Figure 3-9 Interface status:LAN 33
Figure 3-10 Interface status:WLAN 33
Figure 3-11 Licenses 34
Figure 3-12 My Profile 35
Figure 3-13 User management 37
Figure 3-14 Pop-up window: Custom User Roles 39
Figure 3-15 Pop-up window: User security settings 41
Figure 3-16 Quick setup 42
Figure 3-17 System 43
Figure 3-18 Network 45
Figure 3-19 WLAN setting 47
Figure 3-20 WLAN interface 50
Figure 3-21 Service 51
Figure 3-22 Multicast filtering 55
Figure 3-23 Security 57
Figure 3-24 Pop-up window: Certificate Management 59
Figure 3-25 Pop-up window: Port-based security 60
Figure 3-26 Pop-up window: Radius Server Configuration Table 61

Figure 3-27 Pop-up window: Custom User Roles 39
Figure 3-28 Pop-up window: User security settings 41
Figure 3-29 Channel allocation:Display of WLAN channel assignment at the access point 65
Figure 3-30 RSSI graph: Display of the current WLAN strength on the client 66
Figure 3-31 Display of the current signal strength as a bar graph 67
Figure 3-32 Trap Manager 68
Figure 3-33 Snapshot 69
Figure 3-34 Syslog 70
Figure 3-35 Received data on a Syslog recipient (example) 71
Figure 3-36 Interface status: Channel assignment 71
Figure 3-37 Alarm and events: Channel assignment 72
Figure 3-38 Visualization of the connection data read out for a WLAN connection (example) 73
Figure 3-39 Firmware Update: Update via HTTP(S) 75
Figure 3-40 Firmware Update: Update via TFTP 76
Figure 3-41 File Transfer HTTP(S): Configuration files or root CA certificate 77
Figure 3-42 File Transfer HTTP(S): Snapshot 78
Figure 3-43 File Transfer HTTP(S): RADIUS root certificates 79
Figure 3-44 File Transfer HTTP(S): RADIUS client certificates 80
Figure 3-45 File Transfer TFTP: Configuration files or root CA certificate 81
Figure 3-46 File Transfer TFTP: Snapshot 82
Figure 3-47 File Transfer TFTP: RADIUS root certificates 83
Figure 3-48 File Transfer TFTP: RADIUS client certificates 84
Figure 3-49 Custom user roles 85
Figure 4-1 Configuring an access point 90
Figure 4-2 Overview of “Client” operating modes 92
Figure 4-3 Single client bridge 93
Figure 4-4 Configuring the client (SCB): Setting 95
Figure 4-5 Encryption:WPA2-EAP and FT-EAP 97
Figure 4-6 Configuring the client (SCB): Scan 99
Figure 4-7 Configuring the client (SCB): Roaming List 100
Figure 4-8 Configuring the client (MCB): Setting 102
Figure 4-9 Configuring the client (FTB): Setting 105

Figure 4-10 Configuring the client (NAT): Setting 108
Figure 4-11 Configuring 1:1 NAT 111
Figure 4-12 1:1 NAT: Example configuration 112
Figure 4-13 1:1 NAT: Example configuration 2 113
Figure 4-14 Configuring IP masquerading 114
Figure 4-15 IP masquerading: Example configuration 115
Figure 4-16 Pop-up window: 1-to-1 NAT configuration 116
Figure 4-17 Pop-up window: IP masquerading configuration 117
Figure 4-18 VXLAN process 119
Figure 4-19 Configuring the client (VXLAN) 119
Figure 4-20 Configuring the access point (VXLAN) 120
Figure 4-21 Access point functionality (VXLAN) 122
Figure 4-22 Configuration of two virtual interfaces 123
Figure 4-23 Structural representation of the two wireless interfaces and one cable interface using the FL WLAN 112x as an example 124
Figure 5-1 DHCP Service 125
Figure 5-2 Pop-up window: DHCP WLAN Service 128
Figure 5-3 Pop-up window: Current DHCP Leases 130
Figure 5-4 Pop-up window: DHCP Static Leases 131
Figure 6-1 802.1X RADIUS process (simplified) 133
Figure 6-2 RADIUS: Example configuration 134
Figure 6-3 Configuring the authenticator: WLAN interface 135
Figure 6-4 Configuring the authenticator: Security 135
Figure 6-5 Configuring the supplicant: WLAN interface 136
Figure 6-6 Configuring the supplicant: RADIUS root certificate with file transfer 137
Figure 7-1 Schematic representation of SNMP management 141
Figure 8-1 Example of network separation via WLAN using VLAN 143

Legal information and legal notice

General Terms and Conditions of Use for technical documentation

Phoenix Contact reserves the right to alter, correct, and/or improve the technical documentation and the products described in the technical documentation at its own discretion and without giving prior notice, insofar as this is reasonable for the user. The same applies to any changes that serve the purpose of technical progress.

The receipt of technical documentation (in particular user documentation) does not constitute any further duty on the part of Phoenix Contact to furnish information on alterations to products and/or technical documentation. You are responsible to verify the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. All information made available in the technical documentation is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

In general, the provisions of the current General Terms and Conditions of Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

How to contact us

Internet

You can find the latest information on Phoenix Contact products and on our General Terms and Conditions on the Internet at: phoenixcontact.com.

Make sure you always use the latest documentation. It is available at the following address as a PDF for download: phoenixcontact.net/products.

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary. Subsidiary contact information is available at phoenixcontact.com.

Published by

Phoenix Contact GmbH & Co.KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

If you have any suggestions or ideas for improving the content and layout of our help pages, please send them to: tecdoc@phoenixcontact.com

Phoenix Contact Security Advisories (PSIRT)

The Phoenix Contact Product Security Incident Response Team (PSIRT) collects and analyzes potential security vulnerabilities in Phoenix Contact products, solutions, and services. If a security vulnerability is found, it is published on the PSIRT website under “Recent security advisories”. The website is updated on a regular basis.

Phoenix Contact recommends subscribing to the PSIRT newsletter to keep up-to-date (“Subscribe to PSIRT news”).

Anyone can report information on possible security vulnerabilities to the PSIRT team by email.

Phoenix Contact GmbH & Co. KG
Flachsmarktstr. 8
32825 Blomberg, Germany
Phone: +49 5235 3-00
Email: info@phoenixcontact.com
phoenixcontact.com

110820_en_01