Configuration of the FL WLAN 1000/2000 product family

User manual

User manual

Configuration of the FL WLAN 1000/2000 product family

UM EN SW FL WLAN 1000/2000, Revision 03 2025-07-21

This manual is valid for:

Designation	Item No.
FL WLAN 1100	2702534
FL WLAN 1101	2702538
FL WLAN 2100	2702535
FL WLAN 2101	2702540
FL WLAN 1010	2702899
FL WLAN 1011	2702900
FL WLAN 2010	1119246
FL WLAN 2011	1119248

109065_en_03

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

Table of contents

1 For your safety

Read this manual carefully and keep 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 could 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.

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

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 products described in this configuration manual is oriented exclusively to 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 both industrial and domestic environments.

To comply with immunity requirements, functional ground needs to be connected in industrial environments. If you use a shielded Ethernet cable in domestic environments, functional ground must be omitted to meet the emission requirements.

Observe the permitted operating temperatures of the wireless module when using it outdoors. The device is suitable for mounting in protected outdoor areas (e.g., under a porch roof). Direct sunlight may lead to overheating and permanent damage to the device.

Observe the applicable regulations for using wireless devices outdoors.

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 application of this manual

This configuration manual contains information about how to configure the FL WLAN 1000/2000 product family.

For information about startup, refer to the separate manual at phoenixcontact.com/qr/<item_number>.

For information about configuration and diagnostics via the Command Line Interface (CLI), refer to the separate manual at phoenixcontact.com/qr/<item_number>.

1.5 Safety and installation instructions

CAUTION: Noise susceptibility of medical equipment
This device emits radio frequency energy in the Industrial Scientific Medical (ISM) band.
– 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.

NOTE: Radio interference in residential areas
This device is a Class A item of equipment. When using the equipment in residential areas, it may cause radio interference.
– In this case, the operator can be obligated to carry out appropriate measures.

NOTE: Electrostatic discharge
This device contains parts that can be damaged by electrostatic discharge (ESD).
– Take appropriate protective measures against electrostatic discharge.

NOTE: Requirements for the power supply

The module is designed exclusively for operation with safety extra-low voltage (SELV) in accordance with EN/IEC 60950-1 and VDE 0805.

– Make sure that the correct power supply is used.

NOTE: Requirements for the current source

This device should only be operated with power supplies that meet the requirements of EN/IEC 60951-1 for limited power sources.

– Operate this device with a power supply that meets the requirements of EN/IEC 60951-1.
– Alternatively, operate this device in a housing that meets the requirements of a fire protection enclosure in accordance with EN/IEC 60951-1.

NOTE: RF emission

This device emits radio frequency energy in the Industrial Scientific Medical (ISM) band.

– Operate the device with a minimum clearance of 20 cm between the transmitter or antenna and your body.

1.6 Security in the network

NOTE: Network security jeopardized by 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.com/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.
- For reasons of compatibility, it is possible to use TFTP for the transfer (e.g., via CLI) of files. The use of TFTP is not recommended because the file is transferred without encryption. To encrypt the transfer, use HTTPS.
- To protect IT security, operate the device only in areas that are exclusively accessible to authorized persons.

Additional measures for protection against unauthorized network access can be found in the “INDUSTRIAL SECURITY” application note. The application note can be downloaded via the item (phoenixcontact.com/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) web page: phoenixcontact.com/psirt

This symbol indicates potential security risks in devices, solutions, or services from Phoenix Contact. These may be IT and security risks in industry automation, for example.

2 Startup

2.1 Delivery state/default settings

Observe the safety and installation instructions in “Safety and installation instructions” on page 8.

The following default settings are valid up to and including firmware version 2.21:

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”.
- All IP parameters are deleted. The device has no valid IP address.
- BootP is activated.
- WLAN is deactivated.

The following changes in the default settings are valid from firmware version 2.40:

- WLAN is activated.
- Operating mode: MCB (client)
- SSID: PhoenixContact, WPA2 encryption: 2bchanged
- Transmission power: 5 dBm

The following default settings are valid from firmware version 2.50:

- 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, WPA2 encryption: 2bchanged
- Transmission power: 5 dBm

The following default settings are valid from firmware version 3.47:

NOTE: Change initial password

- Before using the device for the first time, you must change the password of the user “admin”.

The new password must meet the following criteria:

- at least 10 characters
- at least one special character
- at least one digit
- at least one uppercase and lowercase letter

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 deactivated.
- Confidential web view is activated.
- CLI Service: SSH

When the firmware is updated, the device configuration settings are applied. To apply the specified settings, you must first reset the device to the default settings after the update.

You will find your firmware version in web-based management on the “Device Status” page (see “Device Status” on page 28).

2.1.1 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, all LEDs light up green.

2.1.1.1 FL WLAN 110x/210x

Table 2-1 Meaning of the diagnostic and status indicators (FL WLAN 110x/210x)

Des.	Color	Function	
		Access Point	Client
US	Green (on)	Supply voltage is applied	
WLAN	Off	WLAN interface deactivated	
	Blue (on)	WLAN interface activated	WLAN interface connected*
	Violet (on)	Automatic channel selection (only with DFS)	Scanning for access point
	Green (on)	WLAN interface in Idle mode if radar check (DFS) is active at 5 GHz	WLAN interface in Idle mode

* WLAN connection established (blue): Whether data transmission occurs depends on whether the passwords and certificates are valid. A WLAN connection can therefore exist although data cannot be transmitted. If WLAN authentication fails, this is indicated in the log file.

2.1.1.2 FL WLAN 101x/201x

Table 2-2 Meaning of the diagnostic and status indicators (FL WLAN 101x/201x)

Des.	Color	Function	
		Access point/mesh	Client
US	Green (on)	Supply voltage is applied	
WLAN	Off	WLAN interface deactivated	
	Blue (on)	WLAN interface activated	WLAN interface connected*
	Violet (on)	Automatic channel selection (only with DFS)	Scanning for access point
	Green (on)	WLAN interface in Idle mode if radar check (DFS) is active at 5 GHz	WLAN interface in Idle mode
RSSI	Green (on)	During the boot process	
	Green (on)	No display	RSSI > –70 dBm
	Orange (on)	No display	RSSI –70 dBm ... –80 dBm
	Off	No display	RSSI < –80 dBm
LAN	Off	No Ethernet connection at XF1	
	Green (on)	Ethernet connection available	
	Green (flashing)	Ethernet connection active	

* WLAN connection established (blue): Whether data transmission occurs depends on whether the passwords and certificates are valid. A WLAN connection can therefore exist although data cannot be transmitted. If WLAN authentication fails, this is indicated in the log file.

2.1.2 General sequence for startup

To start up the device, proceed as follows:

- Supply the device with operating voltage (nominal value: 24 V DC). The assignment of the connector is shown in Figure 2-1.
- Connect the device via the Ethernet interface using an RJ45 connector to the PC that will be used for configuration.
- Assign an IP address to the device via BootP. The IP address is allocated by a corresponding server in the network or a PC tool (see “Assigning the IP address” on page 15).
- Alternatively, you can access the device via the link-local IPv4 address from firmware version 2.50 (see “Assigning the IP address via BootP using Network Manager” on page 16).

↪ 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.

Up to and including firmware version 2.21, the WLAN interface is deactivated in delivery state (default settings) for security reasons. Configuration via the WLAN interface is therefore not possible in this state.

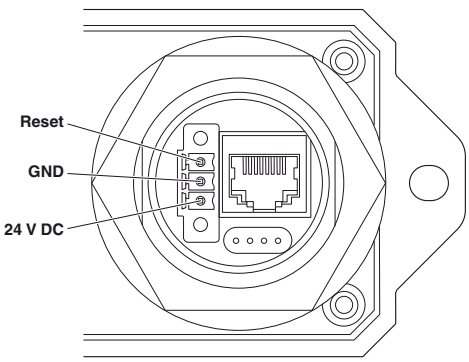
For further information on the Command Line Interface, refer to the separate manual at phoenixcontact.com/qr/<item_number>.

2.1.3 Resetting to the default settings

2.1.3.1 FL WLAN 110x/210x

The device has a digital input (reset). This digital input is used exclusively to reset the device to the default settings. 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 approximately 30 seconds for the device to boot up and be ready for operation.

While the device is starting, all LEDs light up green. Once the device is booted and ready for operation, the LEDs change (see “Meaning of the diagnostic and status indicators” on page 12).

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

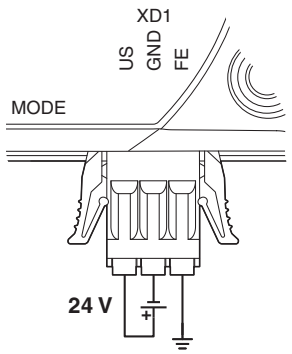
- Apply a voltage equivalent to the operating voltage to the digital input (reset) for at least 5 seconds.

↪ The device is reset to the default settings and restarted.

2.1.3.2 FL WLAN 101x/201x

The device has a MODE button. The device can be reset to the default settings using the MODE button.

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



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

While the device is starting, all LEDs light up green. Once the device is booted and ready for operation, the LEDs change (see “Meaning of the diagnostic and status indicators” on page 12).

You now have approximately 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.

↪ The device is reset to the default settings and restarted.

2.2 Assigning the IP address

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 hinder 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 two sections explain IP address assignment using the “FL Network Manager Basic” (item number 2702889) and the “IP Assignment Tool” software tool from Phoenix Contact.

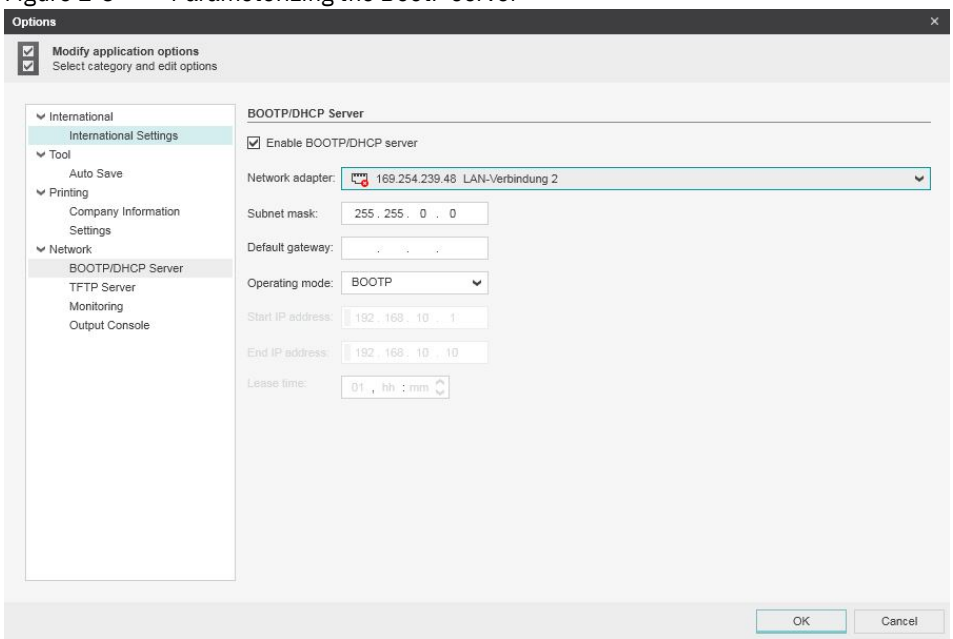
2.2.1 Assigning the IP address via BootP using Network Manager

Requirements

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

Step 1: Parameterizing the BootP server

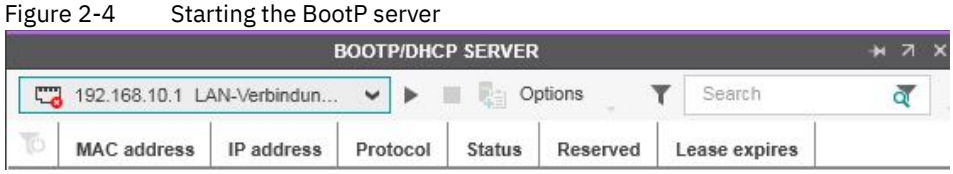
Figure 2-3 Parameterizing the BootP server



- Open the FL Network Manager software.
- Open a new project in the software.
- Under “Extras, Options”, select the “BOOTP/DHCP Server” menu item.
- Activate the “Enable BOOTP/DHCP server” check box.
- Configure the network interface on your PC to which the device is connected and select the “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



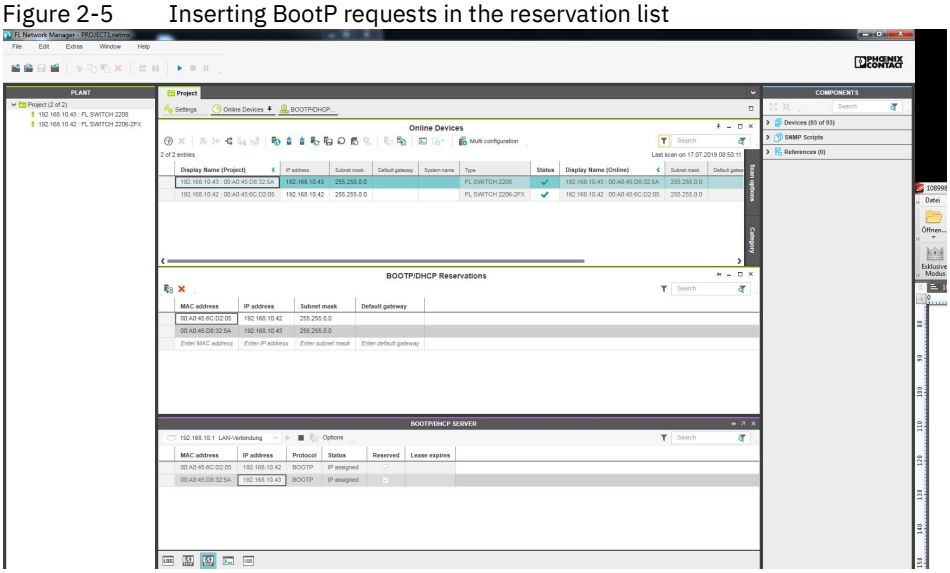
- Open the “BOOTP/DHCP SERVER” window.
- Click on the play icon next to the selected network interface.

↪ The BootP server is activated.

↪ BootP requests that are 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 IP address assignment was successful in the “IP address” column in the “BOOTP/DHCP SERVER” window.

The IP parameters set here can be changed in web-based management (see “Network” on page 42).

2.2.2 Assigning the IP address via BootP using IPAssign.exe

This section deals with IP address assignment using the “IP Assignment Tool” Windows software (IPAssign.exe).

The software can be downloaded free of charge at phoenixcontact.com/qr/<item_number>.

Requirement:

The device is connected to a computer with a Windows operating system.

Step 1: Downloading and running the software

You can download the software from the Internet or copy it from the device (see “Help & Documentation” on page 28).

Downloading from the Internet:

- Go to phoenixcontact.com/qr/<item_number>.
- Under “Software”, download the BootP IP addressing tool.
- Double-click on the “IPAssign.exe” file and, if necessary, click on “Execute”.

↪ The software is opened.

Step 2: IP Assignment Wizard

For the device to send BootP requests, you have to switch the device to BootP on the “Quick setup/IP Address assignment” web page.

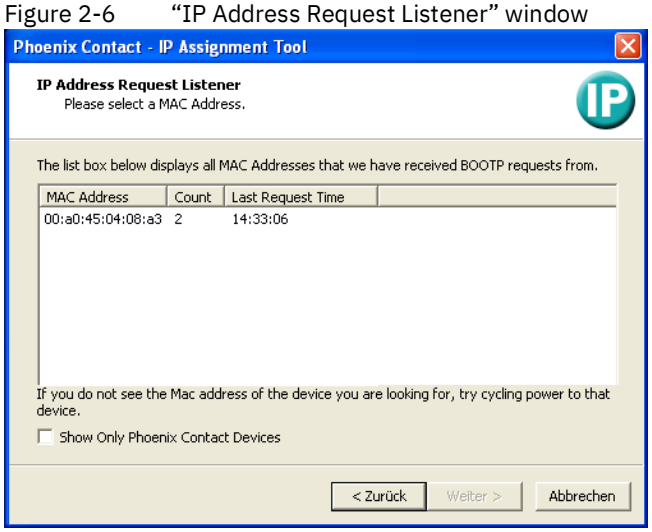
The software is in English for international purposes. However, the software buttons change according to your country-specific settings.

- Click on “Next”.

↪ You now see a list of all devices that send BootP requests and are waiting for an IP address.

Step 3: IP Address Request Listener

Figure 2-6 “IP Address Request Listener” window



In this example, the device has MAC address 00:a00:45:04:08:a3.

- Select the device you want to assign an IP address for.
- Click on “Next”.

Step 4: Set IP Address

In the “Set IP Address” window, you can view and define various parameters:

Figure 2-7 “Set IP Address” window

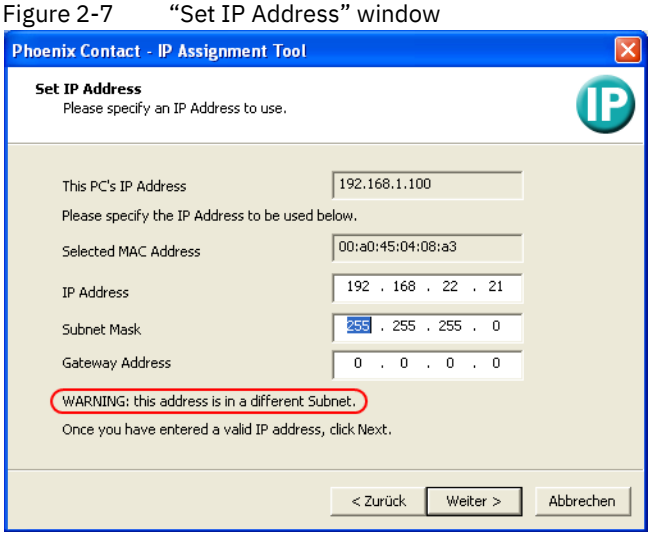


Table 2-3 “Set IP Address” window: Parameters

Parameter	Description
This PC‘s IP Address	The IP address of the currently used PC is displayed here.
Selected MAC Address	The MAC address selected in the previous step is displayed here.
IP Address	In this input field, enter the desired IPv4 address for the connected device. Make sure to enter a valid IP address.
Subnet Mask	In this input field, enter the desired subnet mask for the connected device.
Gateway Address	In this input field, enter the desired gateway address for the connected device.

- Adjust the IP parameters according to your requirements.

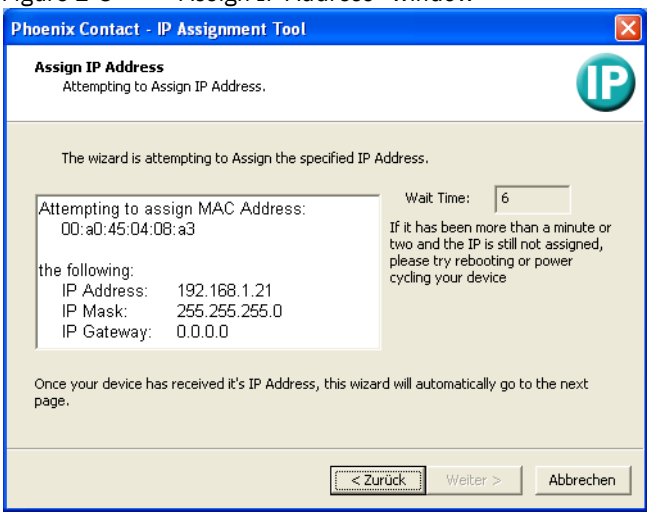
↳ If no inconsistencies are detected, a message appears indicating that a valid IP address has been set.

- Click on “Next”.

Step 5: Assign IP Address

The software now attempts to transfer the set IP parameters to the device. Following successful transfer, the next window automatically opens.

Figure 2-8 “Assign IP Address” window



Step 6: Completing IP address assignment

The window informs you that IP address assignment has been completed successfully. It provides an overview of the IP parameters that have been transferred to the selected device.

- To assign IP parameters for additional devices, click on “Back”.
- To exit the IP address assignment, click on “Finish”.

2.2.3 IP address via link-local IPv4

Requirement:

– The device is set to the default settings and has firmware version 2.50 or higher.
– Configure the connected PC to “Obtain an IP address automatically”. Alternatively, assign an IP address from the range 169.254.2.1–169.254.255.255.

Automatic private IP addressing (APIPA)

- You can access your device via link-local IPv4 via the IP address https://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 169.254.2.1–169.254.255.255. You can determine these IP addresses using external software such as Wireshark or access the device via its host name.

Accessing devices via the host name

You can access your connected device via a browser without having to make any further settings.

The host name consists of two parts:

1. Device type: WLAN
2. The individual part of the MAC address of the device, for example, a8:74:1d:**b0:93:24**

The complete host name in this example is therefore: WLAN-B09324

- Enter the host name in your browser as follows: https://WLAN-b09324.local

2.2.4 Assigning the IP address via DHCP services

You can also assign IP addresses via DHCP services (see “DHCP services” on page 119).

2.3 MAC addresses

For technical reasons, a WLAN device works internally with several MAC addresses. This information can be found in the table below so that you can assign the MAC address for your data analysis (e.g., snapshot data) to the respective device.

Table 2-4 Handling of MAC addresses

MAC address (example)	Description	Position
A8:74:1D:74:B0:84	MAC address is printed on the housing	
A8:74:1D:74:B0:85	MAC address of LAN	1 byte higher than MAC address on the housing
A8:74:1D:74:B0:88*	MAC address of internal MESH VLAN (cannot be accessed externally)	4 bytes higher than MAC address on housing
A8:74:1D:74:B0:89	MAC address of WLAN card	5 bytes higher than MAC address on housing

* Only for FL WLAN 210x and FL WLAN 201x versions

3 Configuration and diagnostics in web-based management

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: Changing the 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 (see “General sequence for startup” on page 14).

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

Device login is only possible if cookies are enabled in the browser settings.

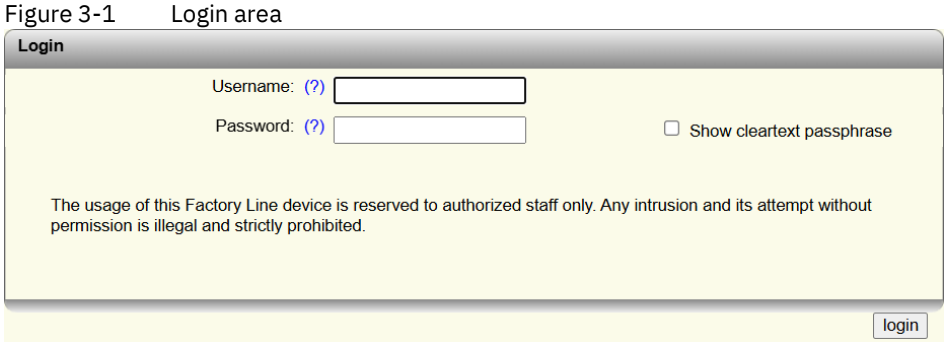
Some functions are opened in pop-up windows. Use of all the functions is therefore only possible if pop-ups are permitted in the browser settings.

The web server operates using the Hypertext Transfer Protocol (HTTP). A standard browser can therefore be used. For full operation of the web pages, the browser must support JavaScript 1.2 and Cascading Style Sheets Level 1.

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

↪ Web-based management opens.

Figure 3-1 Login area



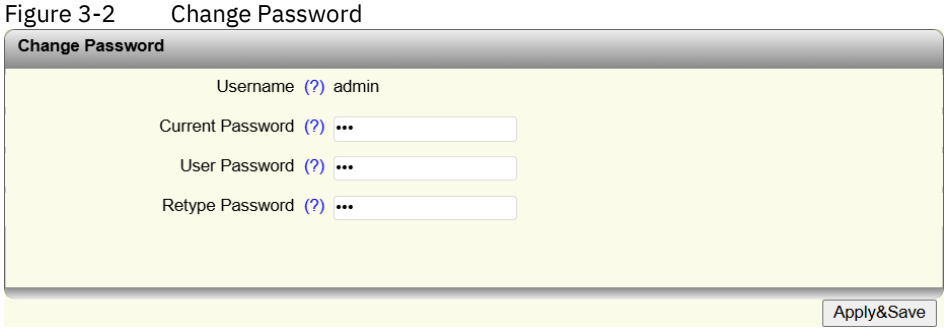
- Click on “Login” and log in using your access data.

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

Up to ten users each can log in at the same time either via web-based management or CLI.

When you use the device for the first time, the following dialog is displayed:

Figure 3-2 Change Password



NOTE: Change initial password

- Before using the device for the first time, you must change the password of the user “admin”.

  The new password must meet the following criteria:
  - at least 10 characters
  - at least one special character
  - at least one digit
  - at least one uppercase and lowercase letter
- Enter the current password and the new password twice and click on “Apply&Save”.

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” on page 34).

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 (WBM) is split into the following areas:

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

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

3.1.3 Icons and buttons in web-based management

At the top and bottom of WBM are icons and buttons that provide an overview of important device functions (see Figure 3-4).

Figure 3-4 WBM with icons (selection)

Table 3-1 Explanation of icons

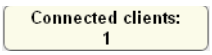
Icon	Explanation
	The WLAN interface is deactivated.
	The device operating mode is “Client”. There is no WLAN connection to an access point.
	The device operating mode is “Client”. There is a WLAN connection to an access point. The number of bars indicates the signal strength of the connection: The more 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.
	An administrator is currently logged into the device. The icon is also the logout button.

Table 3-1 Explanation of icons

Icon	Explanation
	An administrator is currently not logged into the device. The icon is also the login button.
	The active configuration differs from the saved configuration for the device. To save the current 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: Changing the initial password** With the initial password, unauthorized access is possible. – Change the administrator password immediately after the first login. – Do not share the password.

Table 3-2 Explanation of the buttons

Button	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.

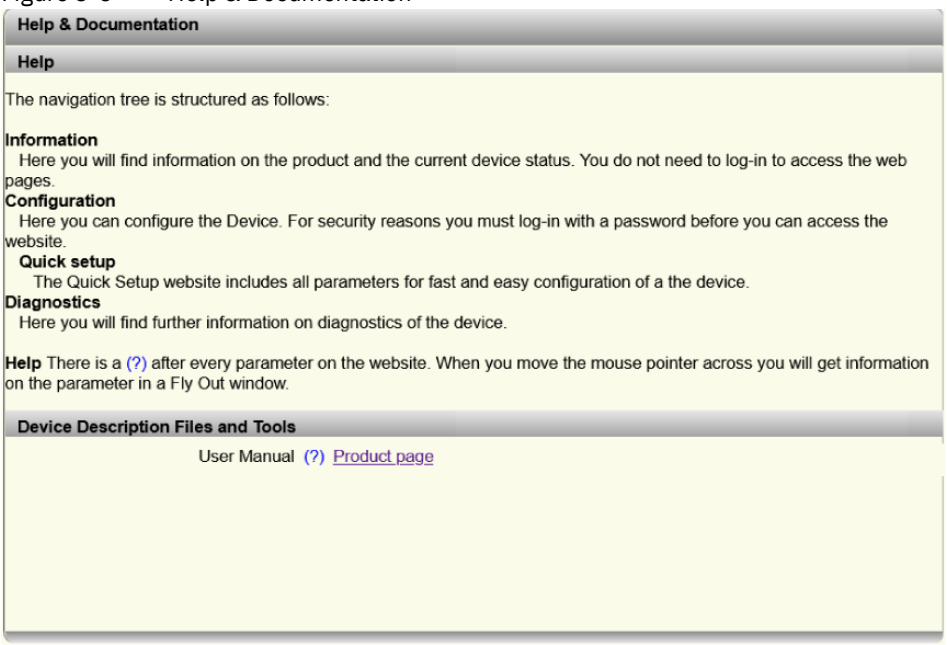
3.2 WBM Information area

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” on page 23) and log in.
- Click on “Information, Help & Documentation”.

Figure 3-5 Help & Documentation



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

– User Manual: Click on “Product page” to be brought to 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” on page 23) and log in.
- Click on “Information, Device Status”.

Figure 3-6 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” on page 23) and log in.
- Click on “Information, Local Diagnostics”.

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

Figure 3-7 Local Diagnostics (FL WLAN 101x/201x)

Local Diagnostics		
Power Supply		
US	:	Supply Voltage (green LED)
Ethernet		
LAN	:	There is a link LED for each port.
WLAN		
WLAN	:	WLAN active (blue LED/purple while scanning)
RSSI	:	Signal Strength LED (green/orange)

3.2.4 Alarm & 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 3000 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 the “Persistent Event Logging” item on the “Service” page (see “Service” on page 48).

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Information, Alarm & Events”.

Figure 3-8 Alarm & Events

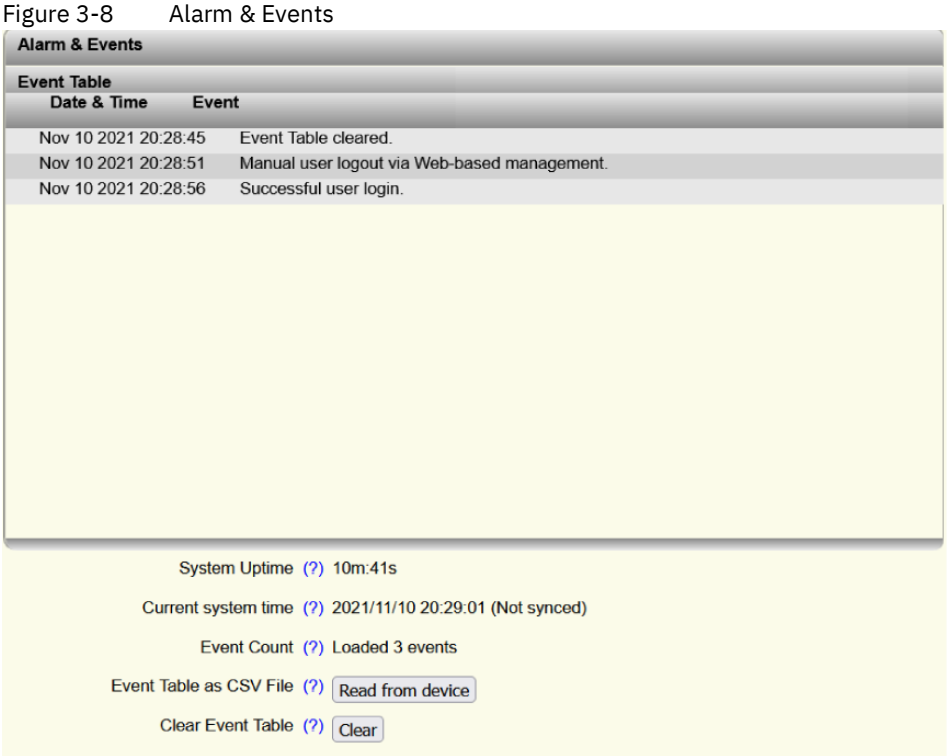


Table 3-3 Alarm & Events: Parameters

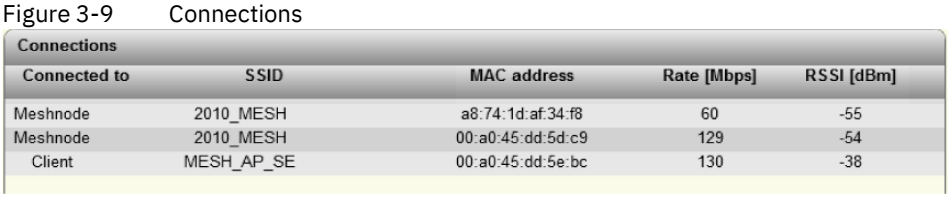
Parameter	Description
System Uptime	How long the device has been in operation since the last restart is displayed here.
Current system time	The current system time is displayed here. If the time is not synchronized, there may be discrepancies between the system time and the actual time (see “Service” on page 48).
Event Count	The number of currently loaded events in the event table is displayed here.
Event Table as CSV File	Click on “Read from device” to download the currently displayed Event Table as a CSV file and save it.
Clear Event Table	Click on “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” on page 23) and log in.
- Click on “Information, Connections”.

Figure 3-9 Connections



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” on page 23) and log in.
- Click on “Information, Interface Status”.

Figure 3-10 Interface Status: LAN

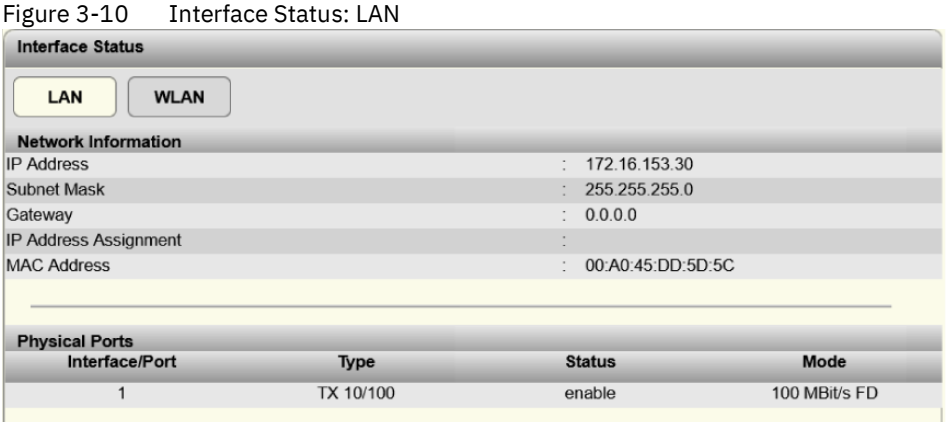
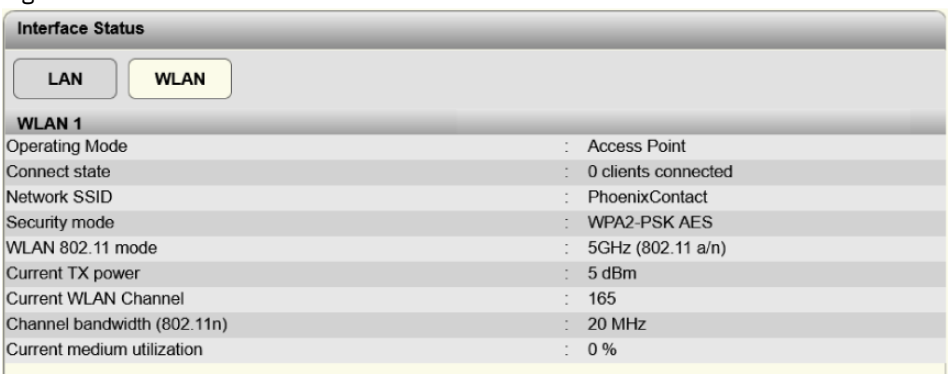


Figure 3-11 Interface Status: WLAN



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” on page 23) and log in.
- Click on “Configuration, My Profile”.

Figure 3-12 My Profile

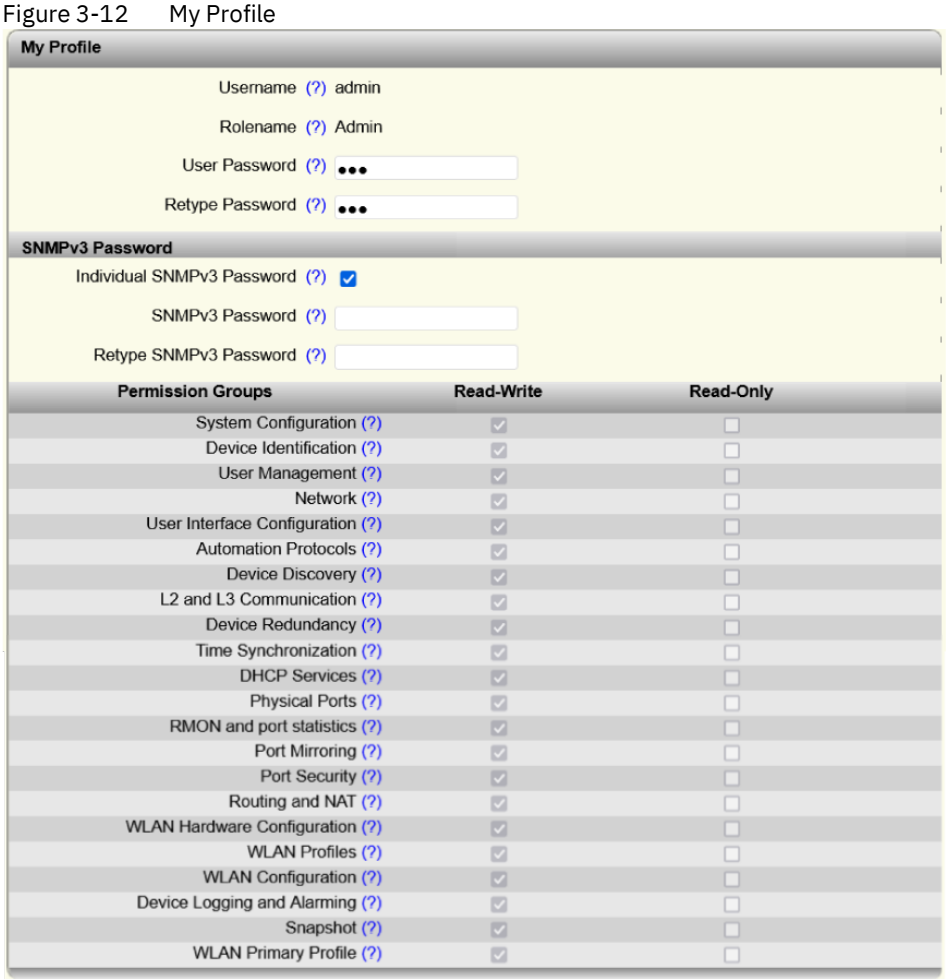


Table 3-4 My Profile: Parameters

Parameter	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.
	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

Table 3-5 SNMPv3 Password: Parameters

Parameter	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.
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” on page 53).

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” on page 23) and log in.
- Click on “Configuration, User Management”.

Figure 3-13 User Management

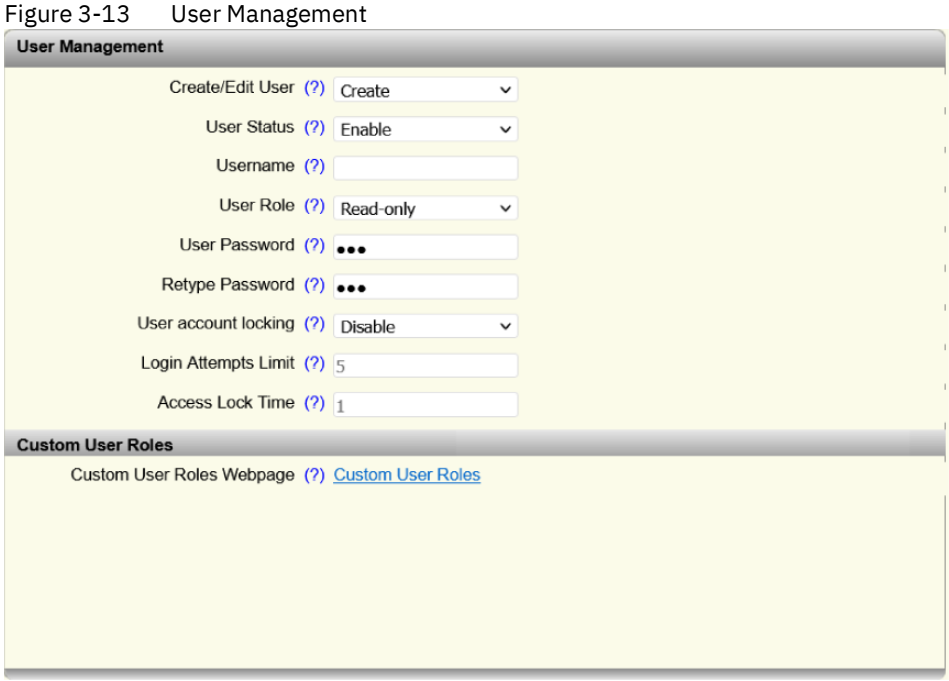


Table 3-6 User Management: Parameters

Parameter	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 on “Delete” to delete the currently selected user account. This action cannot be undone. The “admin” user account cannot be deleted.
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 can no longer be changed.

Table 3-6 User Management: Parameters

Parameter	Description
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” on page 37).
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 1 and 100.
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 1 and 1440 minutes.

User Management: Custom User Roles

Table 3-7 Custom User Roles: Parameters

Parameter	Description
Custom User Roles Web-page	Click on “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” on page 37).

Pop-up window: Custom User Roles

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

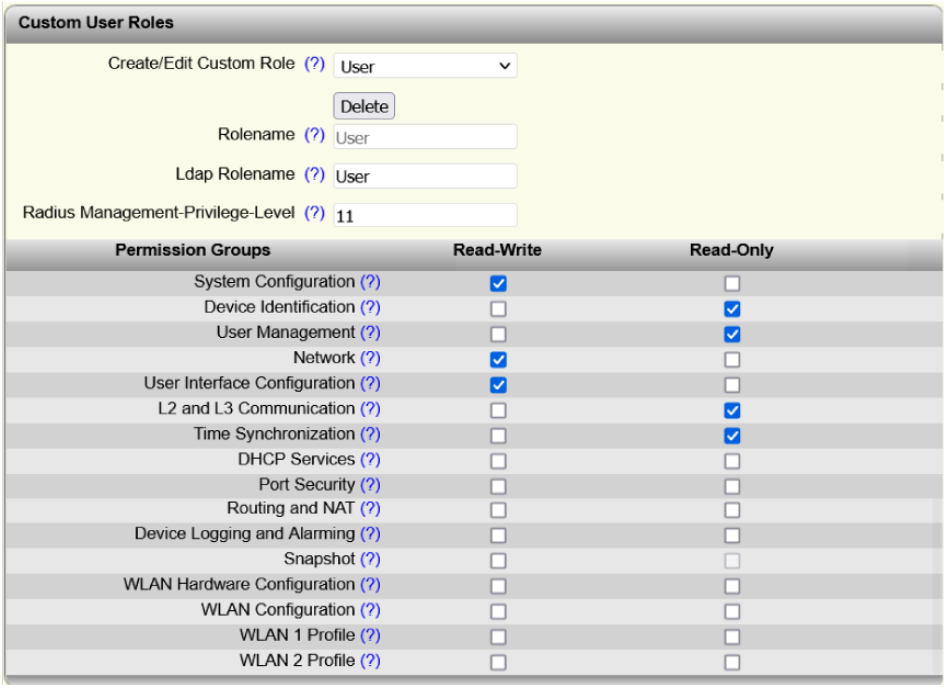


Table 3-8 Pop-up window: Custom User Roles: Parameters

Parameter	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 on “Delete” to delete the currently selected role. This action cannot be undone. The preconfigured roles “Admin”, “Expert”, and “Read-only” cannot be deleted.
Rolename	Enter the desired name for the user role in the text field. The name for the user role can be up to 32 characters long. Letters, numbers, and the following special characters are permitted: -_.@. Once the role name has been created, it can no longer be changed.

Table 3-8 Pop-up window: Custom User Roles: Parameters

Parameter	Description
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 “Security” on page 53.
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 “RADIUS certificates” on page 125.
Permission Groups	In the table, you can assign and edit the read and write permissions for user-defined user roles. The predefined permissions of the “Admin”, “Expert”, and “Read-only” roles available by default cannot be changed. – Read-Write: Activate the respective check box to assign read and write permissions for the function group to the selected user role. – Read-Only: Activate 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.

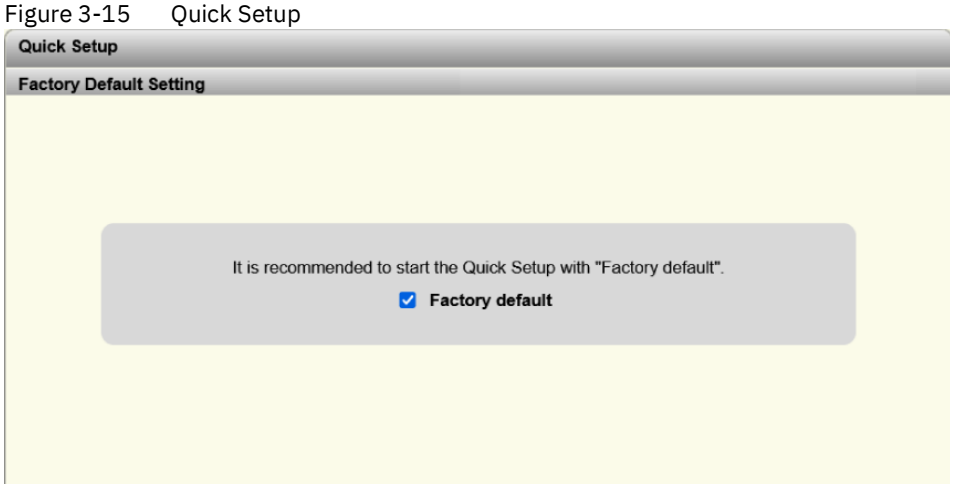
For further information on user roles and permissions, see “Creating user roles” on page 74.

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” on page 23) and log in.
- Click on “Configuration, Quick Setup”.

Figure 3-15 Quick Setup



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

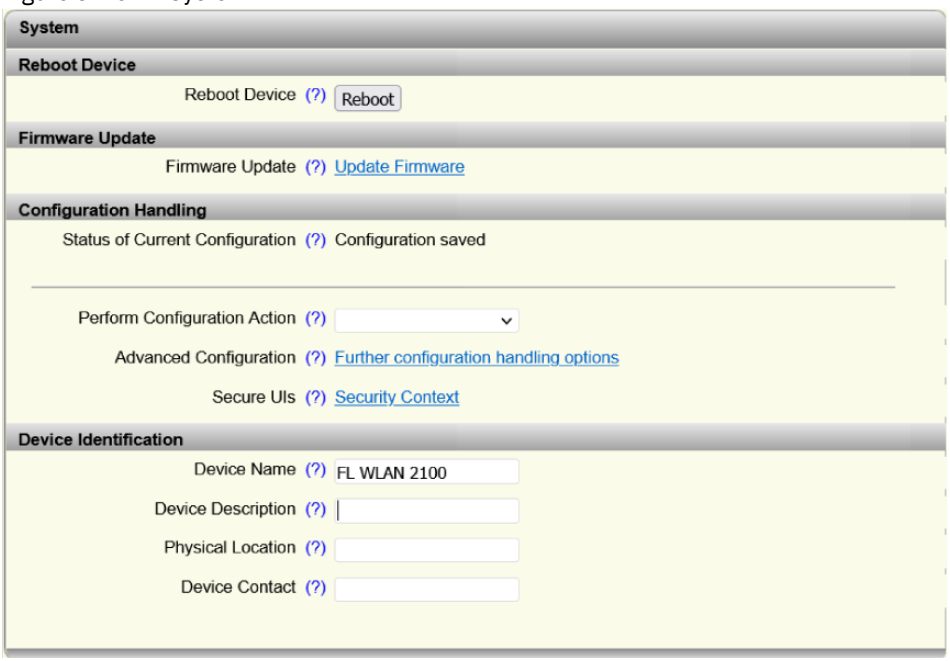
- Click on “Next” and follow the setup instructions.

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” on page 23) and log in.
- Click on “Configuration, System”.

Figure 3-16 System



System: Reboot Device

Table 3-9 Reboot Device: Parameters

Parameter	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

Table 3-10 Firmware Update: Parameters

Parameter	Description
Firmware Update	Click on “Update Firmware” to perform a firmware update. For further information, refer to Section “Firmware Update” on page 67.

System: Configuration Handling

Table 3-11 Configuration Handling: Parameters

Parameter	Description
Status of Current Configuration	The status of the current configuration is displayed here. – Configuration saved: The current configuration is saved to the device. – Configuration modified but not saved: The active configuration has been changed, but not yet saved to the device. Click on “Apply&Save” to save the configuration to the device.
Perform Configuration Action	Select an option from the drop-down list. – Factory Default: The action resets the device configuration to the factory default state. – Save Configuration: The action saves the active configuration to the device. The settings made are retained after a voltage reset. – Reload Configuration: The action loads the most recently saved configuration and applies it. The configuration might have been saved using “Save Configuration” or the “Apply&Save” button.
Advanced Configuration	Click on “Further configuration handling options” to open the “File Transfer” pop-up window (see “File Transfer” on page 69).
Secure UIs	Click on “Security Context” to open the “Security Context” pop-up window (see “Pop-up window: Security Context” on page 55).

System: Device Identification

Table 3-12 Device Identification: Parameters

Parameter	Description
	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.
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” on page 23) and log in.
- Click on “Configuration, Network”.

Figure 3-17 Network

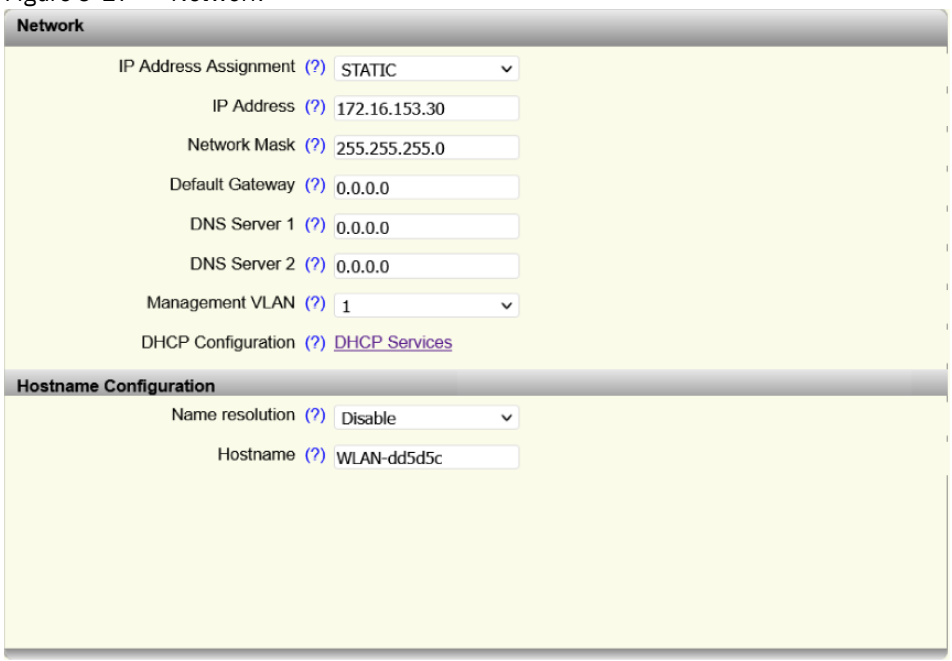


Table 3-13 Network: Parameters

Parameter	Description
	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 the PROFINET engineering tool or controller For further information on IP address assignment, see “Assigning the IP address” on page 15.
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.

Table 3-13 Network: Parameters

Parameter	Description
Default Gateway	This option is only available if you selected “STATIC” for “IP Address Assignment”. Enter the default gateway.
DNS Server 1	Here, enter the IP address of the primary DNS server.
DNS Server 2	Here, enter the IP address of the secondary DNS server.
Management VLAN	Select the VLAN in which web-based management is to be accessible. The 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	Click on “DHCP Services” to open the “DHCP Service” pop-up window (see “DHCP services” on page 119).

Network: Hostname Configuration

Table 3-14 Hostname Configuration: Parameters

Parameter	Description
Name resolution	Select whether you want to activate DNS name resolution via mDNS and LLMNR. When you activate the function, you can also access the device via the host name (e.g., http://WLAN-dd5d5c.local/).
Hostname	Here, enter the host name of your device. The host name must be between two and 63 characters long. Alphanumeric characters and dashes are permitted. A host name must not start with a dash.

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” on page 23) and log in.
- Click on “Configuration, WLAN Setting”.

Figure 3-18 WLAN Setting

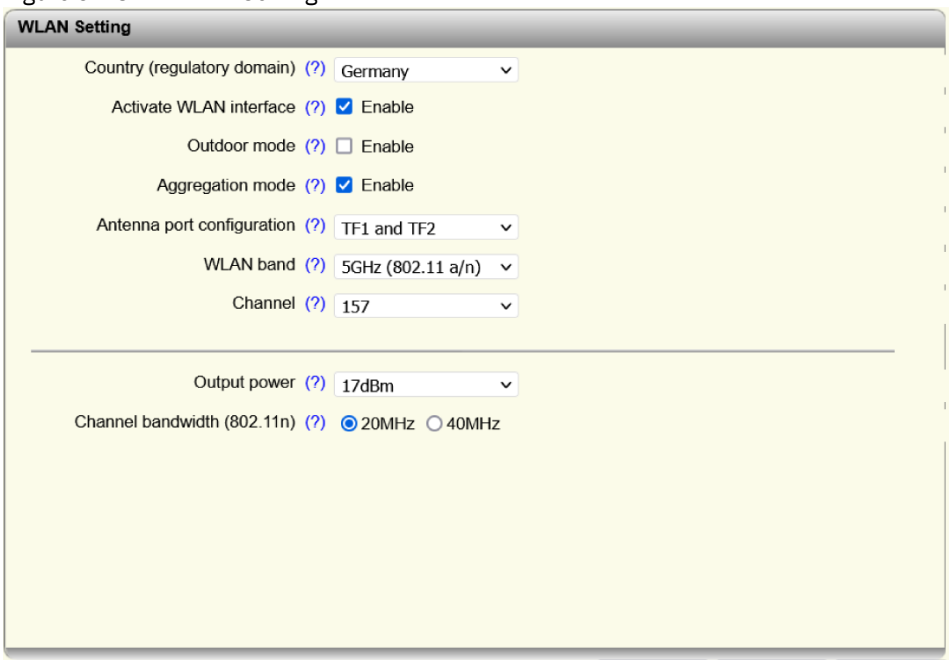


Table 3-15 WLAN Setting: Parameters

Parameter	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. Observe the various country-specific approvals for the device versions. For further information on this, refer to the corresponding installation manual.
Activate WLAN interface	Select the check box to activate the WLAN interface. If the WLAN interface is deactivated, no communication can take place over the interface.
Outdoor mode	Activate the check box if the device will be used outdoors. You must activate the check box if you plan to operate the device outdoors in Europe and use the 5 GHz band. The device will then be operated on the prescribed DFS (Dynamic Frequency Selection) channels.
Aggregation mode	Activate the check box to combine multiple data packets. This increases the user data component of a WLAN packet and the utilization of the transmission capacity.
Antenna port configuration	This option is only available on the FL WLAN 101x and 201x. 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) – 5 GHz (802.11 a) – 5 GHz (802.11 a/n) 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” on page 82).

Table 3-15 WLAN Setting: Parameters

Parameter	Description
Channel	Here, select the desired channel or select “Automatic” to have the device pick the channel automatically. Depending on the option you selected in the previous parameters, there will be different channels to choose from. 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” on page 82).
Output power	Here, select the desired transmission power. – FL WLAN 110x/210x: The transmission power is the effectively radiated power including the antenna gain. – FL WLAN 101x/201x: 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.
Channel bandwidth	Activate the desired radio button for the channel bandwidth. – 20MHz: The device is operated on one channel. – 40MHz: The device is operated on two channels (channel bonding). This increases the data rate, but requires two channels.

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.

When configuring two virtual wireless interfaces, you should always configure “WLAN 2” as an access point. You can optionally configure “WLAN 1” as an access point or a client.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.

Figure 3-19 WLAN Interface

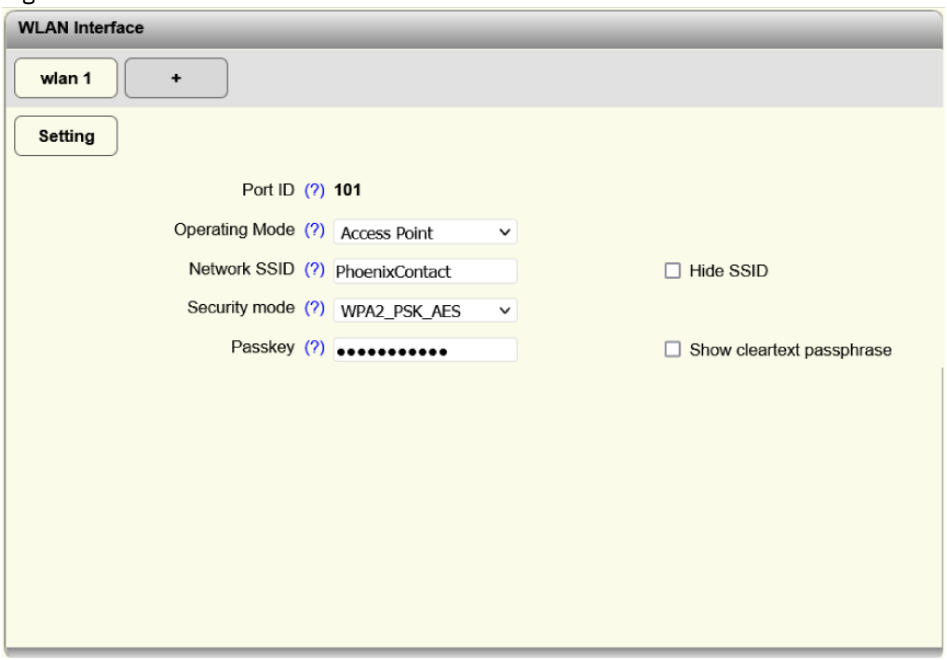


Table 3-16 WLAN Interface: Parameters

Parameter	Description
Operating Mode	Here, select the desired operating mode. – Access Point – Client (Fully transparent bridge) – Client (Single client bridge) – Client (Multi client bridge) – Mesh (only FL WLAN 2xxx) – Client (NAT) For further information about the various operating modes and the respective setting options, see “Device operating modes” on page 79.

The other parameters on this page depend on the selected operating mode and are dealt with in the corresponding section (see “Device operating modes” on page 79).

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
Deactivate unused interfaces to prevent unauthorized access.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, Service”.

Figure 3-20 Service

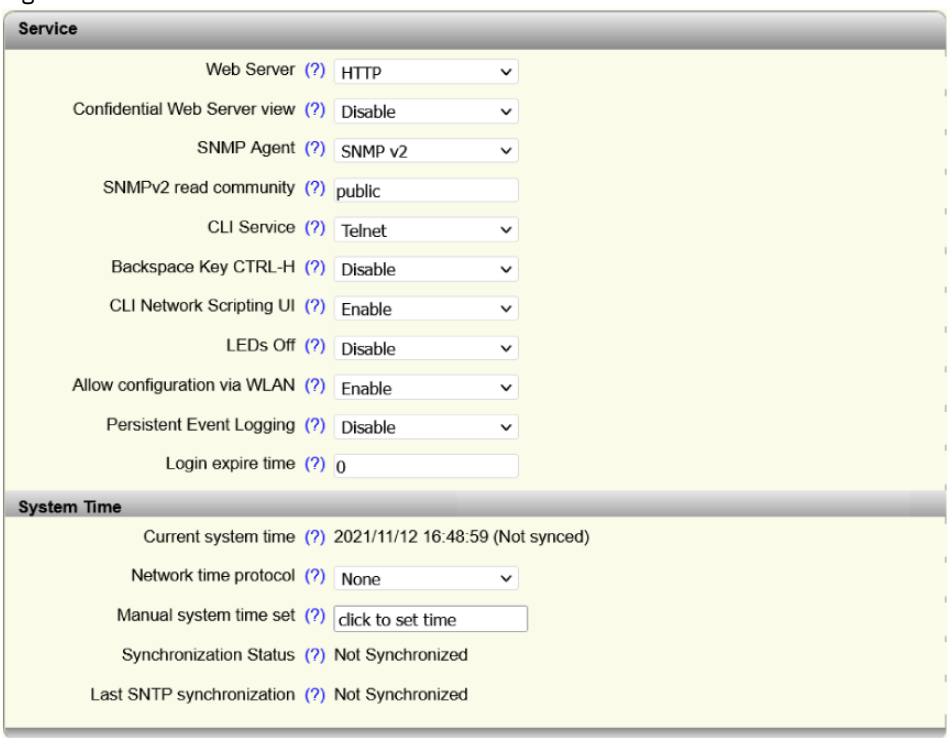


Table 3-17 Service: Parameters

Parameter	Description
Web Server	Here, select whether the web server functionality should be activated. – Disable: The web server is deactivated. Access to web-based management is deactivated. – HTTP: The web server is activated in “HTTP” mode. The connection is not secured. – HTTPS: The web server is activated in “HTTPS” mode. Use “https://” to access web-based management. The connection is secured. If you deactivate the web server, web-based management can no longer be accessed.
Confidential Web Server view	Here, select 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 other areas is controlled using user roles (see “User Management” on page 34). – Enable: Web-based management is only visible with previous login.
SNMP Agent	Here, select the SNMP server functionality (see “SNMP – Simple Network Management Protocol” on page 131). – Disabled: The SNMP server is deactivated. – SNMP v2: The SNMP server is activated in “SNMP v2” mode. SNMP v1 is also supported in this mode. – SNMP v3: The SNMP server is activated in “SNMP v3” mode. **NOTE: Network security** SNMPv2 is not a secure encryption method.
SNMPv2 read community	This option is only available if you selected “SNMP v2” for “SNMP Agent”. Here, enter the string for the SNMPv2 read community. This password must be entered for read access to objects.
CLI Service	Here, select whether entry of CLI commands via Telnet or Secure Shell should be activated. – Disable: Entry of CLI commands is deactivated. – Telnet: Entry of CLI commands via Telnet is activated. – SSH: Entry of CLI commands via Secure Shell (SSH) is activated. For information about configuration and diagnostics via the Command Line Interface (CLI), refer to the separate manual at phoenixcontact.com/qr/<item_number>.

Table 3-17 Service: Parameters

Parameter	Description
Backspace Key CTRL-H	Here, select 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 activate this option, you can instead use the Ctrl+H key combination in your terminal program to delete the last character.
CLI Network Scripting UI	– Disable: Transmission of CLI commands via the network is deactivated. – Enable: Transmission of CLI commands via the network is activated.
LEDs Off	Here, select whether the LEDs on the device should be active. – Select “Enable” to deactivate the LEDs. – Select “Disable” to activate the LEDs.
Allow configuration via WLAN	Here, select whether configuration via the WLAN interface should be possible. If you deactivate 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	Here, select whether the persistent storage of events should be activated. Persistent storage means that events are not deleted when the device is restarted.
Login expire time	Here, enter the time until automatic logout. You can set a number between 30 and 3600 seconds. The default is 1200 seconds. If you set a value of “0”, automatic logout is deactivated.

Service: System Time

Table 3-18 System Time: Parameters

Parameter	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 is not 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.
Network time protocol	Here, select a protocol for synchronizing the time via a web server. – None: No synchronization via a 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". Here, enter the IP address of your SNTP server. 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". Here, enter a description of your SNTP server.
Secondary SNTP server	This option is only available if you selected "Unicast" for "Network time protocol". Here, enter the IP address of your secondary SNTP server. SNTP stands for Simple Network Time Procotol 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". Here, enter a description of your secondary SNTP server.

Table 3-18 System Time: Parameters

Parameter	Description
UTC offset	This option is only available if you selected “Unicast” or “Broadcast” for “Network time protocol”. Here, enter the difference from the coordinated world time (UTC) for your time zone.
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” on page 23) and log in.
- Click on “Configuration, Multicast Filtering”.

Figure 3-21 Multicast Filtering

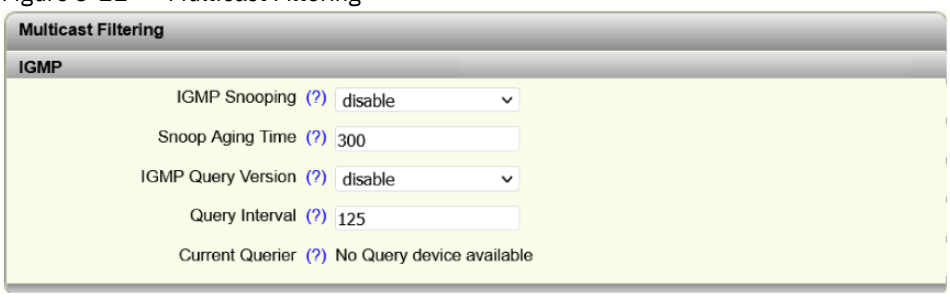


Table 3-19 Multicast Filtering: Parameters

Parameter	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 3600 (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.

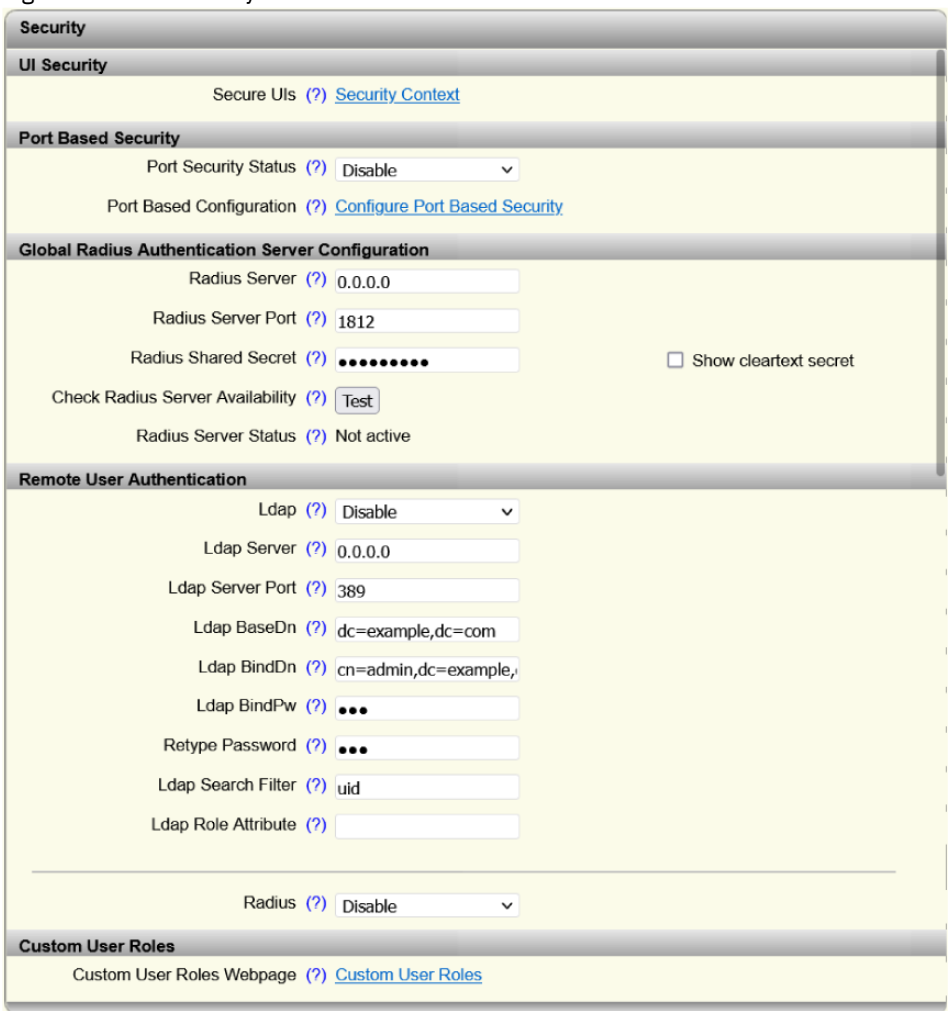
3.3.10 Security

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

NOTE: Network security
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.com/qr/<item_number>.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, Security”.

Figure 3-22 Security



Security: UI Security

Table 3-20 UI Security: Parameters

Parameter	Description
Secure UIs	Click on “Security Context” to open the “Security Context” pop-up window (see “Pop-up window: Security Context” on page 55). Here, you can create the necessary keys and certificates for operation with HTTPS and SSH.

Pop-up window: Security Context

Figure 3-23 Pop-up window: Security Context.

Table 3-21 Pop-up window: Security Context: Parameters

Parameter	Description
Create new context	Click on “Generate” to create all the necessary keys and certificates for operation with HTTPS and SSH.
Current state	The current availability of the security context is displayed here.
Root CA	Click on “cecert.cer” to download the root CA certificate created for the installation from the device.
Advanced Configuration	Click on “File Transfer” to open the “File Transfer” pop-up window (see “File Transfer” on page 69).
Customer CA state	The current status of the customer CA certificate is displayed here. You can store a self-signed certificate. Your browser’s security warnings will then no longer be triggered.
Delete Customer CA	Click on “Delete” to delete your self-signed certificate.

Security: Port Based Security

Table 3-22 Port Based Security: Parameters

Parameter	Description
Port Security Status	Select whether port-based security should be activated globally.
Port Based Configuration	Click on “Configure Port Based Security” to open the “Port Based Security” pop-up window (see “Pop-up window: Port Based Security” on page 55).

Pop-up window: Port Based Security

All the 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 Security” on page 55).

Settings in this pop-up window are only possible if you selected “Access Point” as the device operating mode (see “Device operating modes” on page 79).

Figure 3-24 Pop-up window: Port Based Security

Table 3-23 Pop-up window: Port Based Security: Parameters

Parameter	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: 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 addresses are on the allowlist are allowed. – Pass: All WLAN devices with an unknown MAC address are allowed. WLAN devices whose MAC addresses are on the denylist are blocked. – IP-allowlist: Data traffic is blocked, with the exception of the IP addresses on the list. The target IP and TCP/UDP port are considered here (all or 1–65535).
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”.

Security: Global Radius Authentication Server Configuration

Table 3-24 Global Radius Authentication Server Configuration: Parameters

Parameter	Description
Radius Server	Here, enter the IP address of the RADIUS server.
Radius Server Port	Here, enter the port of the RADIUS server.
Radius Shared Secret	Here, enter the shared secret that is required for encrypted communication with the RADIUS server. The shared secret must not exceed 128 characters.
Check Radius Server Availability	Click on “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.

For further information about RADIUS certificates, see “RADIUS certificates” on page 125.

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.

Table 3-25 Remote User Authentication: Parameters

Parameter	Description
	Select whether LDAP server-based user authentication should be activated.
Ldap Server	Here, enter the address of the LDAP server as an IP address or DNS name.
Ldap Server Port	Here, enter the TCP port for the connection to the LDAP server (default: 389). An encrypted connection to the LDAP server (e.g., via SSL/TLS and Port 636) is not currently supported by the device.
Ldap BaseDn	Here, enter the LDAP Base Distinguished Name. The BaseDN describes the base address or the storage location under which the user data is stored in the directory on the LDAP server.
Ldap BindDn	Here, enter the LDAP Bind Distinguished Name. The BindDn is the user name for logging into the device on the LDAP server in order to be able to perform operations on the LDAP server such as browsing user data.
Ldap BindPw	Here, enter the LDAP Bind Password. The Bind password is required for authenticating the device on the LDAP server. This password is linked to the BindDn.
Retype Password	Here, enter the Bind password again.

Table 3-25 Remote User Authentication: Parameters

Parameter	Description
Ldap Search Filter	Here, enter the server attribute under which the user name is to be found when logging into the server. Optional: With the wildcard operator {0}, you can define the part of the attribute that is to be entered during login (e.g., mail={0}@phoenixcontact.com).
Ldap Role Attributes	Here, enter the attribute under which the designation of the user roles is stored on the LDAP server. This attribute is mapped to the device with a local role designation so that rights can be assigned to a user. On the “Custom User Roles” page, you can map the LDAP role name from the server to a local user role under “Ldap Rolename” (see “Pop-up window: Custom User Roles” on page 37).
Radius	Here, select whether RADIUS server-based user authentication should be activated. To establish a connection to the RADIUS server, the settings under “Global Radius Authentication Server Configuration” are used (see “Security: Global Radius Authentication Server Configuration” on page 57).

Security: Custom User Roles

Table 3-26 Custom User Roles: Parameters

Parameter	Description
Custom User Roles Webpage	Click on “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” on page 37).

3.4 WBM Diagnostics area

3.4.1 Channel Allocation (only Access Point operating mode): WLAN channel assignment diagnostics

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.

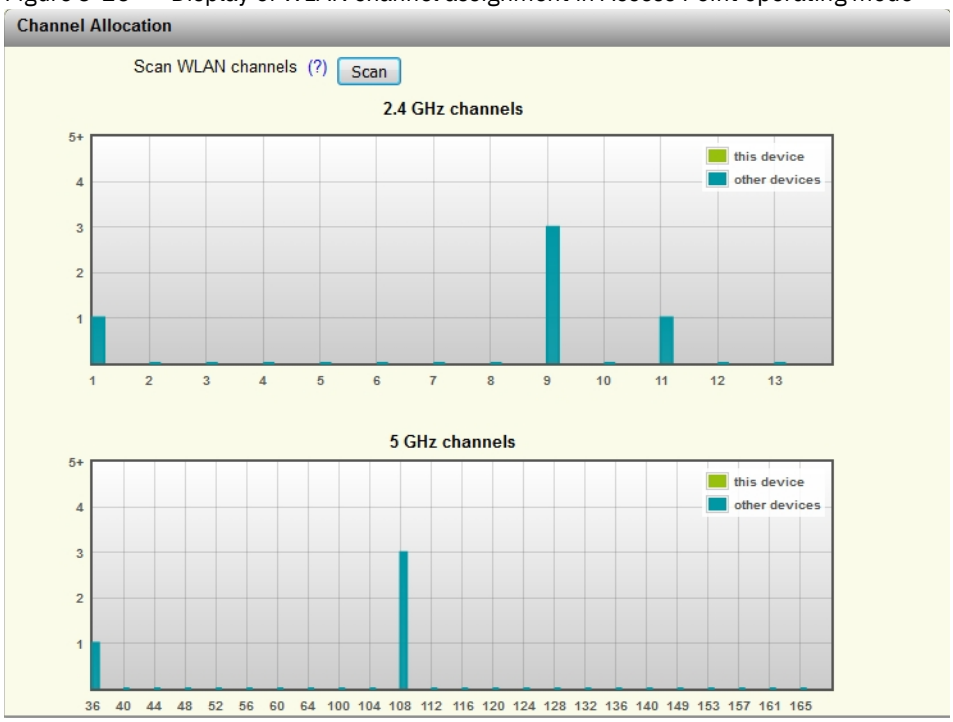
Requirement:

The device is in Access Point operating mode.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Diagnostics, Channel Allocation”.
- Click on the “Scan” button.

↪ WLAN networks in range are displayed as graphs.

Figure 3-25 Display of WLAN channel assignment in Access Point operating mode



3.4.2 RSSI Graph: WLAN signal strength diagnostics

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” on page 23) and log in.
- Click on “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 3-26 Display of the current WLAN signal strength in Client mode

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

The RSSI graph can display values from a maximum of 10 devices simultaneously.

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).

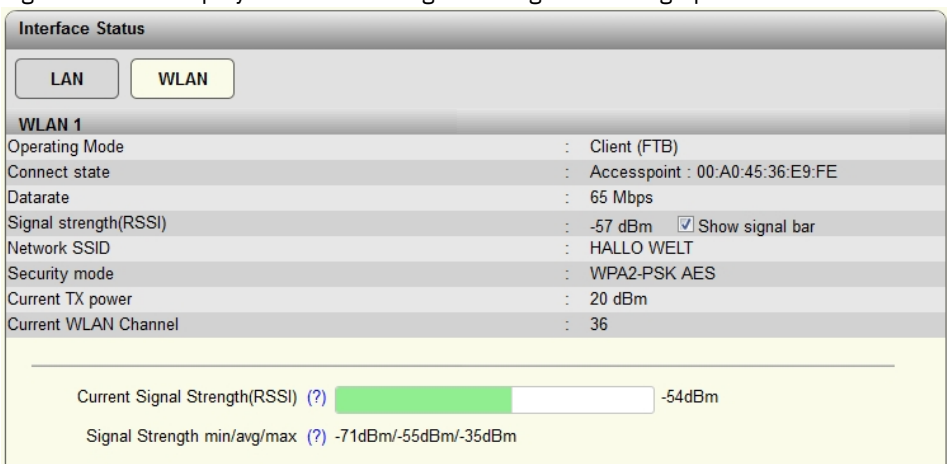
- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Information, Interface Status, WLAN”.
- Activate the “Show signal bar” check box (see Figure 3-27).

↪ 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 3-27 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” on page 23) and log in.
- Click on “Diagnostics, Trap Manager”.

Figure 3-28 Trap Manager

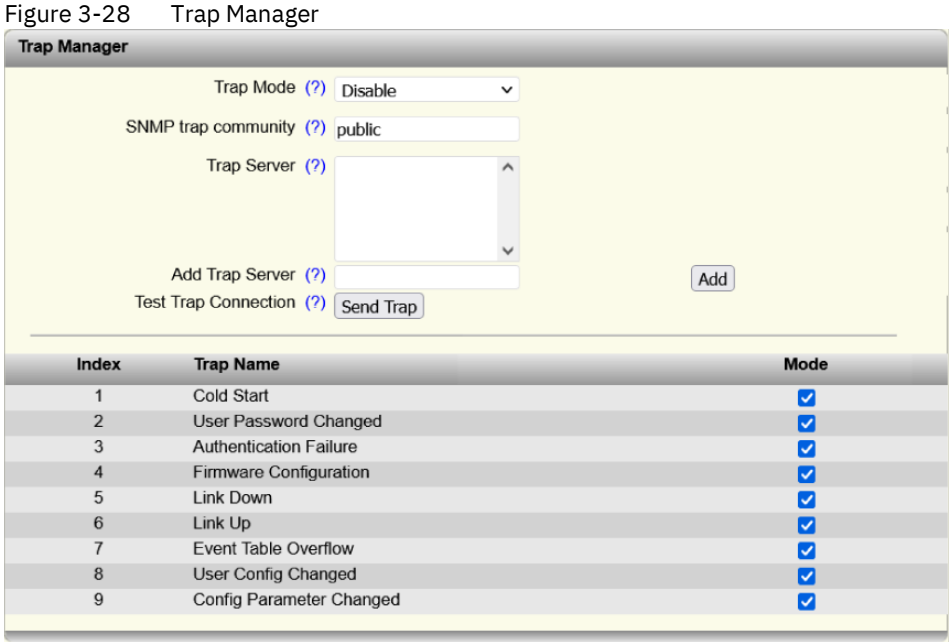


Table 3-27 Trap Manager: Parameters

Parameter	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 on “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: Diagnostics using snapshot

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.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Diagnostics, Snapshot”.
- Click on the “Snapshot” button.

↪ The snapshot of the device is created.

- Click on “File transfer” to download the snapshot (see “File Transfer” on page 69).

Figure 3-29 Snapshot

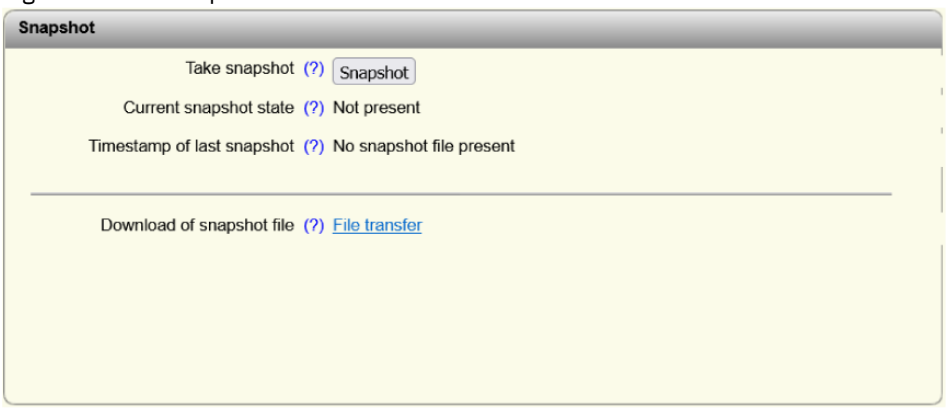


Table 3-28 Snapshot: Parameters

Parameter	Description
Take snapshot	Click on “Snapshot” to create a snapshot of the current device configuration.
Current snapshot state	The snapshot status is displayed here (e.g., whether it 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 on “File transfer” to download the snapshot (see “File Transfer” on page 69).

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” on page 23) and log in.
- Click on “Diagnostics, Syslog”.

Figure 3-30 Syslog

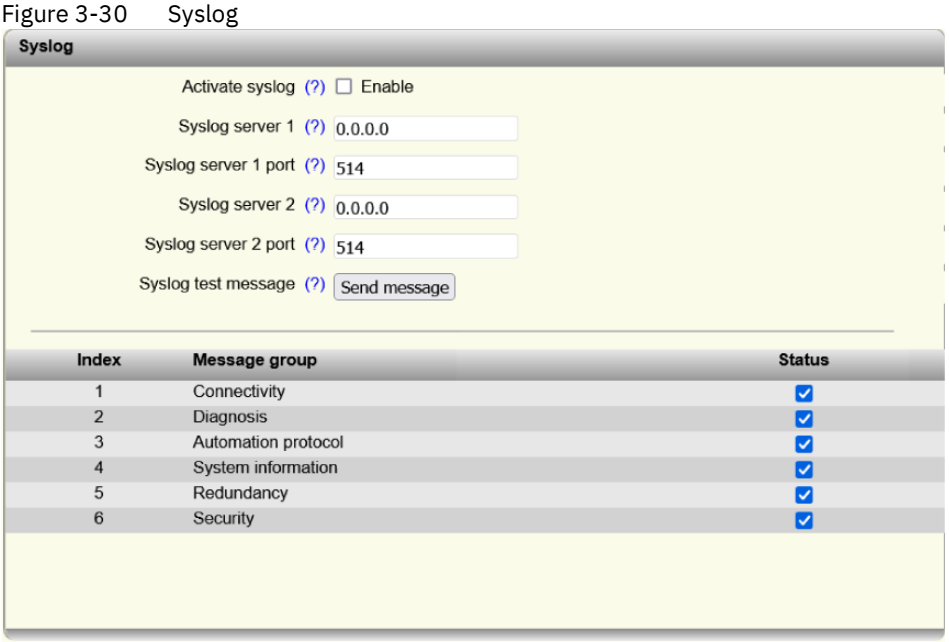


Table 3-29 Syslog: Parameters

Parameter	Description
Activate syslog	Select the check box to activate the Syslog functionality.
Syslog server 1	Here, enter the IP address or the DNS name of the first Syslog server.
Syslog server 1 port	Here, enter the UDP port of the first Syslog server. Default: 514
Syslog server 2	Here, enter the IP address or the DNS name of the second Syslog server.
Syslog server 2 port	Here, enter the UDP port of the second Syslog server. Default: 514
Syslog test message	Click on “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	Activate the check boxes in the “Status” column to select those categories whose events are to be sent to the Syslog server.

Figure 3-31 Received data on a Syslog recipient (example)

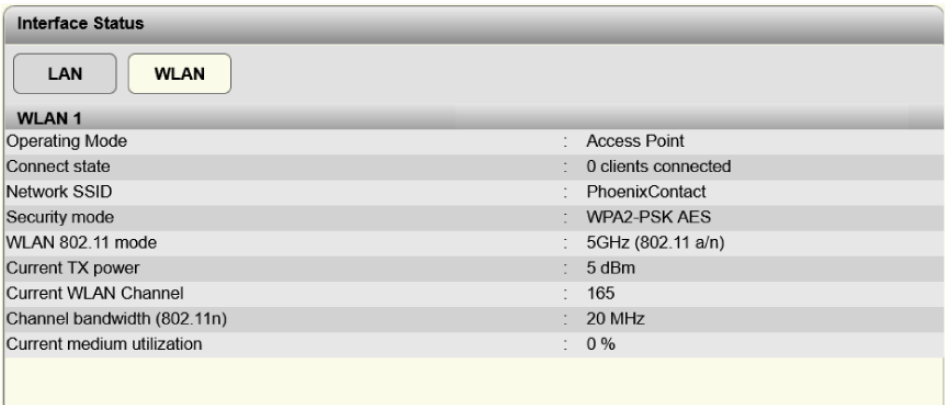
Date/Time UTC	Host Name	Message
2020-07-13 11:26:44.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | Channel: 6 | RSSI: -72 dBm | MU: 2 %
2020-07-13 11:26:43.	192.168.0.100	Port: 101 | Mode FTB | AP-MAC: 00:A0:45:A5:85:49 | SSID: Test1 | Bitrate: 72 Mbps | 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” on page 23) and log in.
- Click on “Information, Interface Status, WLAN”.

Figure 3-32 Interface Status: Channel assignment



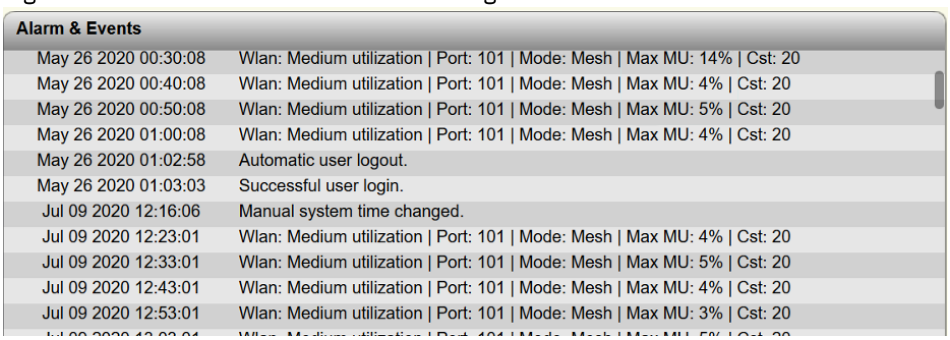
↪ The “Current medium utilization” option shows you the current channel assignment.

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 10 minutes in percent in the event log.

- Click on “Information, Alarm & Events”.

Figure 3-33 Alarm & Events: Channel assignment



– Max MU: The channel assignment is determined in the device every 5 seconds. The highest of these values over a time of 10 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.

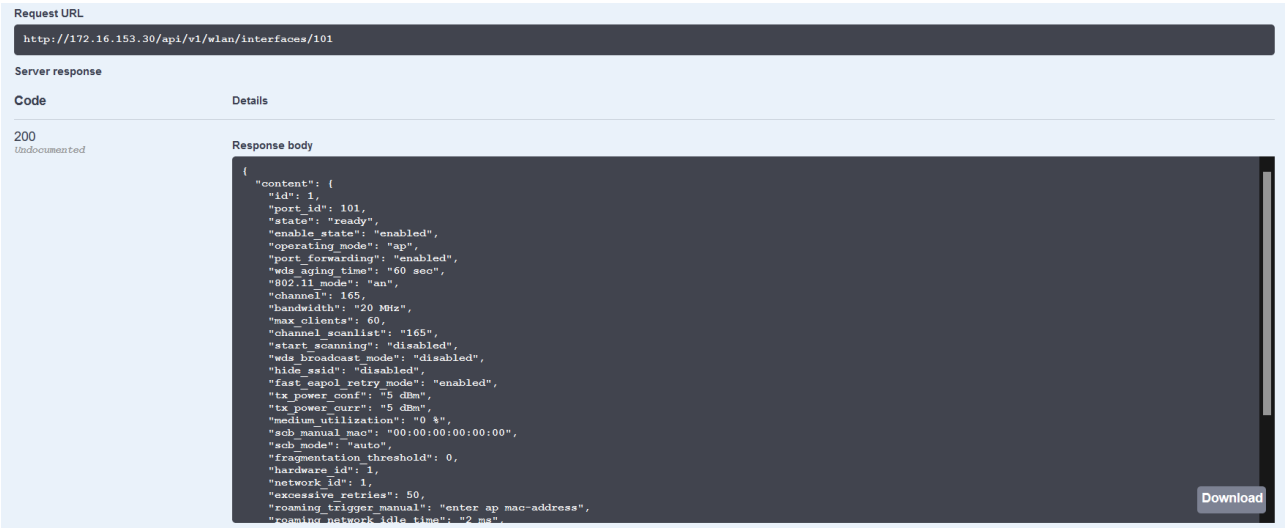
3.5 REST API

The FL WLAN 1000/2000 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 page “<Device_IP_address>/api/v1”, for example, “172.16.153.30/api/v1”.

Figure 3-34 Visualization of the connection data read out for a WLAN connection (example)



In the example shown here (Figure 3-34), the connection data read out for a WLAN connection is displayed via the 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” on page 23) and log in.
- Click on “Configuration, System”.
- Click on “Update Firmware”.

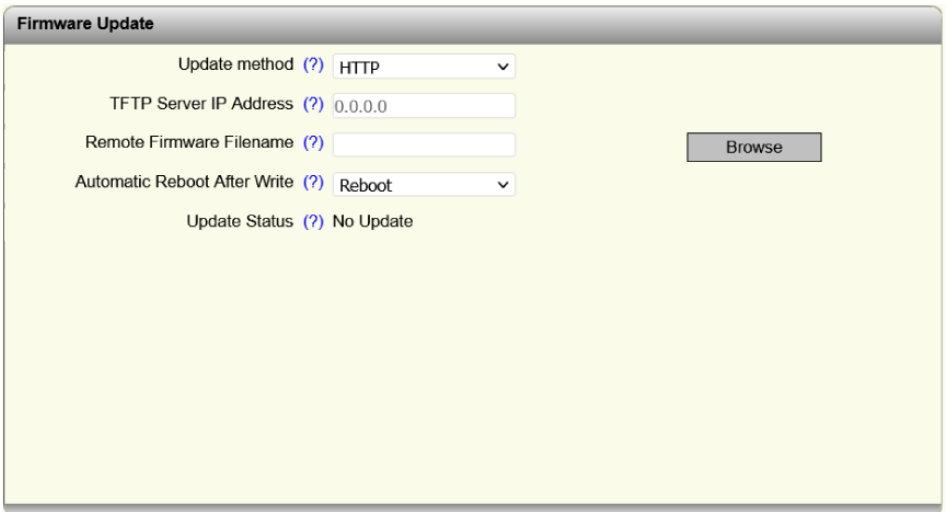
↳ The “Firmware Update” dialog opens.

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

3.6.1 Update via HTTP

- Select “HTTP” for “Update method”.

Figure 3-35 Update via HTTP



- Click on “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 on “Apply”.

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

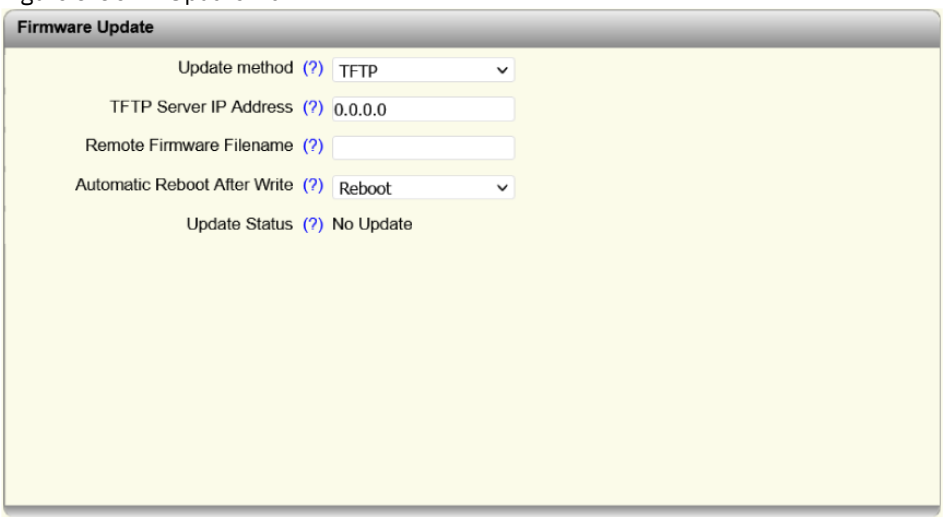
- Wait until “Update Status” shows the message “Firmware Update successful”.
- Close the “Firmware Update” window.

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

3.6.2 Update via TFTP

- Select “TFTP” for “Update method”.

Figure 3-36 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 on “Apply”.

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

- Wait until “Update Status” shows the message “Firmware Update successful”.
- 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” on page 23) and log in.
- Click on “Configuration, System”.
- Click on “Further configuration handling options”.

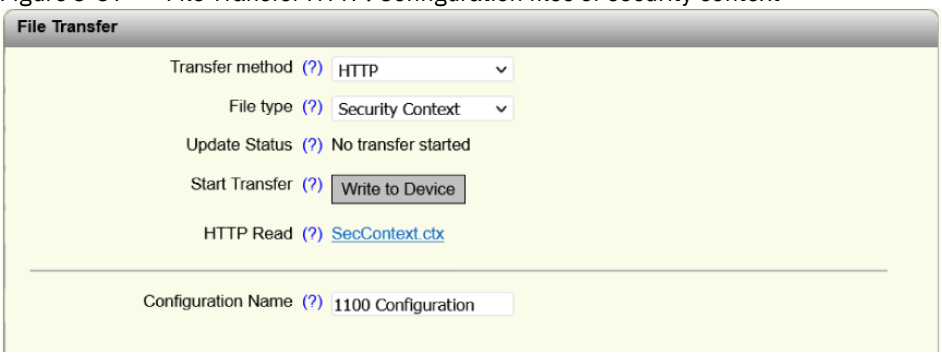
↪ The “File Transfer” pop-up window opens.

3.7.1 Transfer via HTTP

- Select “HTTP” for “Transfer method”.

Transferring configuration files or security context

Figure 3-37 File Transfer HTTP: Configuration files or security context

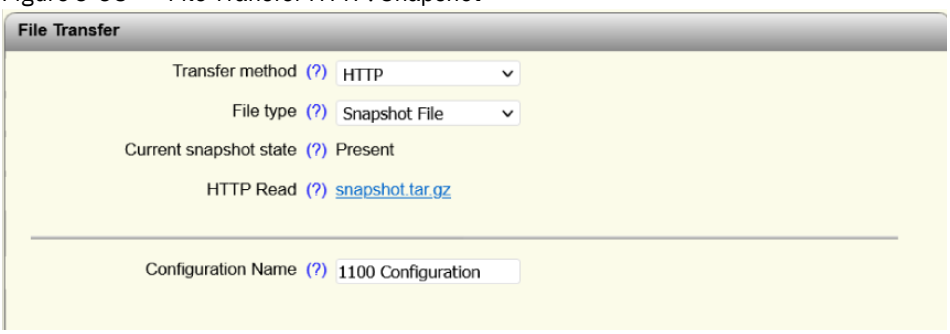


- Select the “Configuration” or “Security Context” option for “File type”.
- Optionally, enter a name for your configuration or your security context in “Configuration Name”.
- Click on “Write to Device” to select a file on your PC that is to be transferred to the device.
- Click on the “config.cfg” link to download the active configuration to your PC.

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

Transferring snapshot files

Figure 3-38 File Transfer HTTP: Snapshot



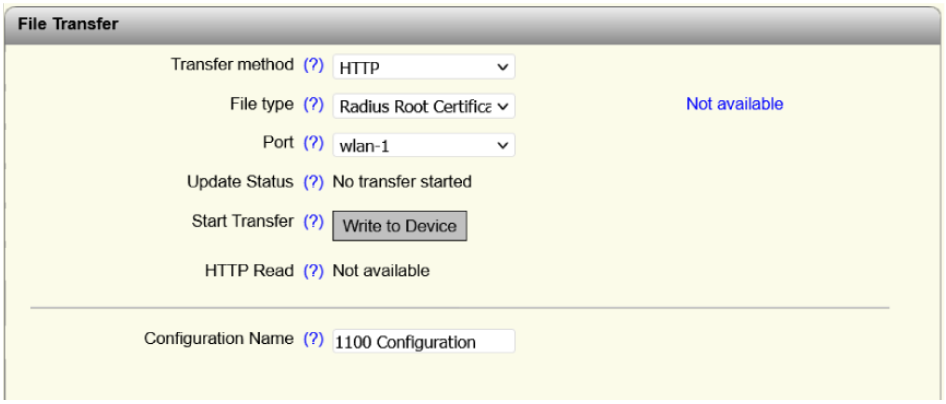
First you need to create a snapshot (see “Snapshot: Diagnostics using snapshot” on page 63).

- Select “Snapshot” for “File type”.
- Optionally, enter a name for your snapshot file in “Configuration Name”.
- Click on “snapshot.tar.gz” to download the snapshot to your PC.

↪ The snapshot file is downloaded to your PC.

Transferring RADIUS root certificates

Figure 3-39 File Transfer HTTP: RADIUS root certificate

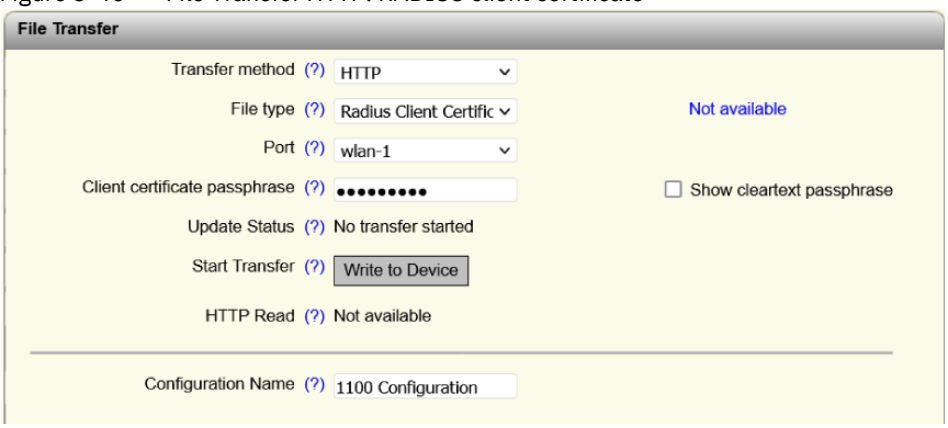


- Select the “Radius Root Certificate” option for “File type”.
- For “Port”, select the port for which the RADIUS root certificate is to be installed.
- Optionally, enter a name for your RADIUS root certificate in “Configuration Name”.
- Click on “Write to Device” to select a file on your PC that is 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 3-40 File Transfer HTTP: RADIUS client certificate



- 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.
- Optionally, enter a name for your RADIUS client certificate in “Configuration Name”.
- Click on “Write to Device” to select a file on your PC that is to be transferred to the device.

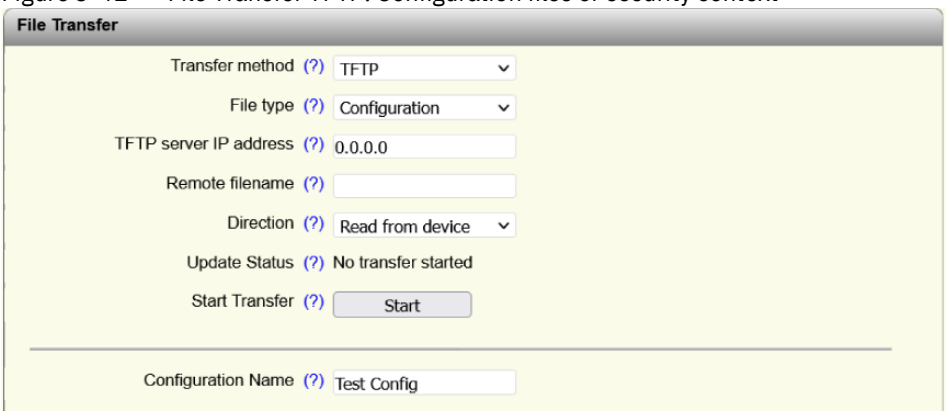
↳ The selected file is uploaded and installed at the selected port. The current status is displayed under “Update Status”.

3.7.2 Transfer via TFTP

- Select “TFTP” for “Transfer method”.

Transferring configuration files or security context

Figure 3-41 File Transfer TFTP: Configuration files or security context

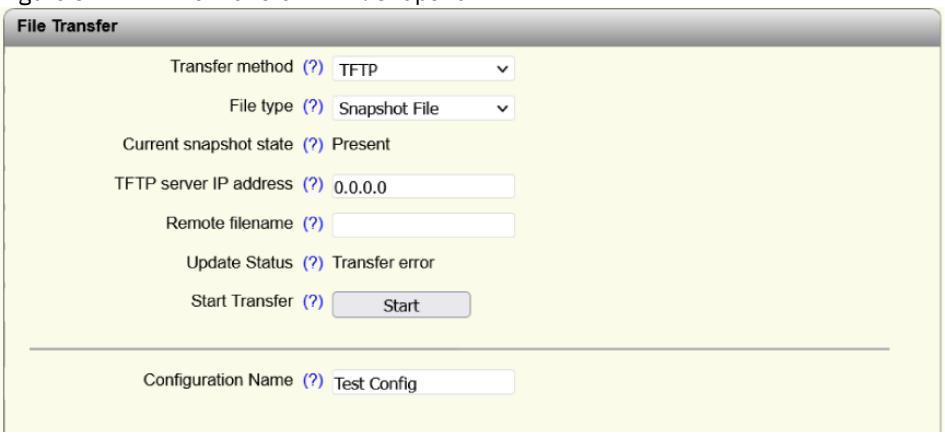


- Select the “Configuration” or “Security Context” option for “File type”.
- For “TFTP server IP address”, enter the IP address of the TFTP server.
- For “Remote filename”, specify the file name including file extension. The file extension is *.cfg for a configuration file or *.ctx for a security context.
- 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 security context in “Configuration Name”.
- Click on “Start” to start the transfer.

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

Transferring snapshot files

Figure 3-42 File Transfer TFTP: Snapshot



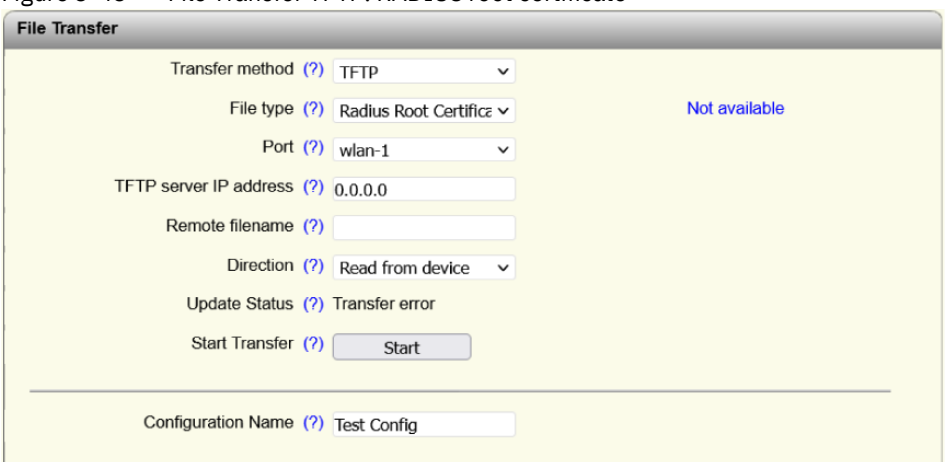
First you need to create a snapshot (see “Snapshot: Diagnostics using snapshot” on page 63).

- Select “Snapshot” for “File type”.
- 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 on “Start” to download the snapshot to your PC.

↪ The snapshot file is downloaded to your PC. The current status is displayed under “Update Status”.

Transferring RADIUS root certificates

Figure 3-43 File Transfer TFTP: RADIUS root certificate



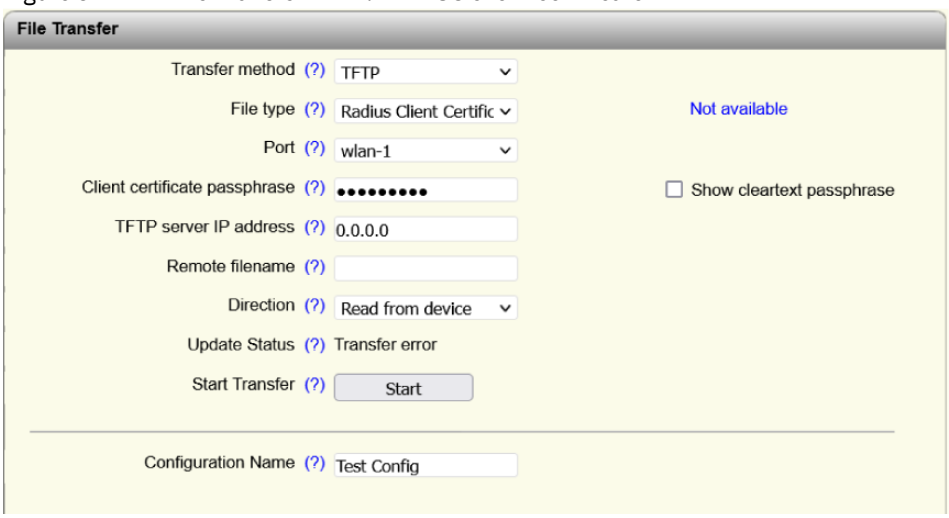
- Select the “Radius Root Certificate” option for “File type”.
- For “Port”, select the port for which the RADIUS root certificate is to be installed.
- For “TFTP server IP address”, enter the IP address of the TFTP server.

- 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 on “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 3-44 File Transfer TFTP: RADIUS client certificate



- 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 “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.
- For “Client certificate passphrase”, enter the password that can be used to decrypt the client certificate.
- Optionally, enter a name for your RADIUS client certificate in “Configuration Name”.
- Click on “Start” to upload the file to the device.

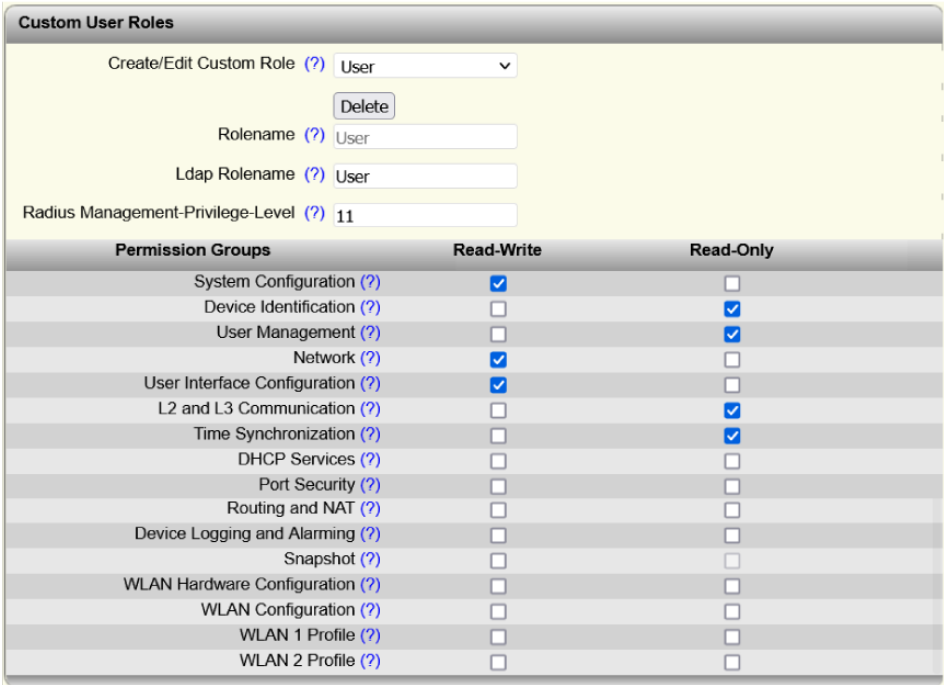
↳ The selected file is uploaded and installed at the selected port. The current status is displayed under “Update Status”.

3.8 Creating user roles

As of firmware version 2.70, 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” on page 23) and log in.
- Click on “Configuration, User Management”.
- Click on “Custom User Roles”.

Figure 3-45 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.

Table 3-30 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
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

Table 3-30 Custom User Roles: Explanation of permission groups

Permission group	Description
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”.
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

Table 3-30 Custom User Roles: Explanation of permission groups

Permission group	Description
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)”, “Repeater” (with two virtual wireless interfaces), and “Mesh” (only FL WLAN 2xxx) operating modes. “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” on page 23) and log in.
- Click on “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” on page 82).

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 applica-

tions 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)” on page 83 and “Operation as a fully transparent bridge” on page 95).

4.1.2 Configuring an access point

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.

Figure 4-1 Configuring an access point

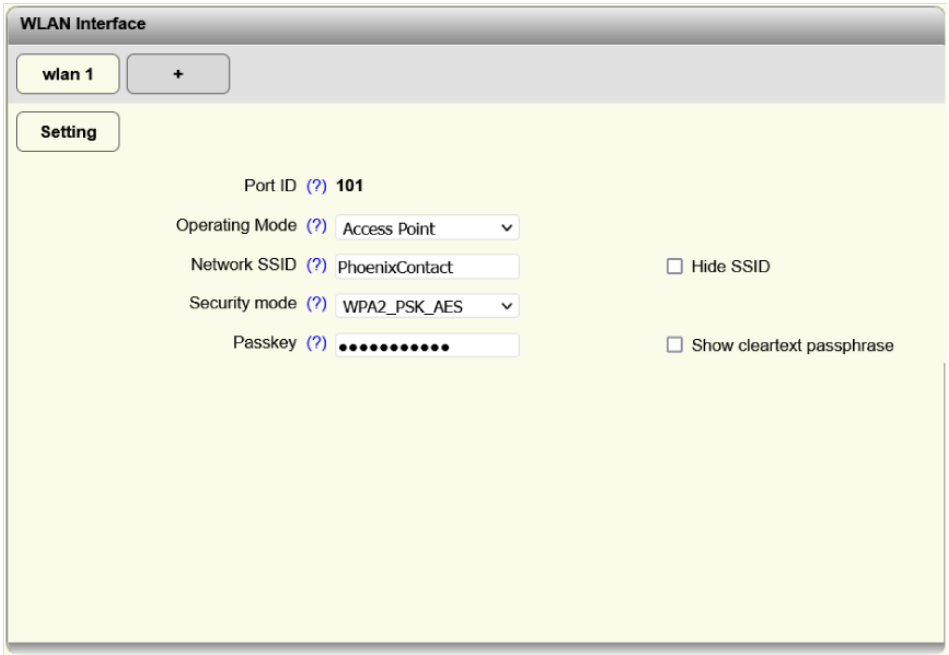


Table 4-1 Configuring an access point: Parameters

Parameter	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. – 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” on page 125).
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between 8 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 on “Link to radius server configuration” to open the “Security” page. Here you can configure the RADIUS server for authentication (see “Security” on page 53 and “RADIUS certificates” on page 125).

- On the “WLAN Interface” page, set the “Access Point” option for “Operating Mode”.
- Define the parameters as desired and click on “Apply&Save”.

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

4.2 Operating mode: Client

4.2.1 Roaming

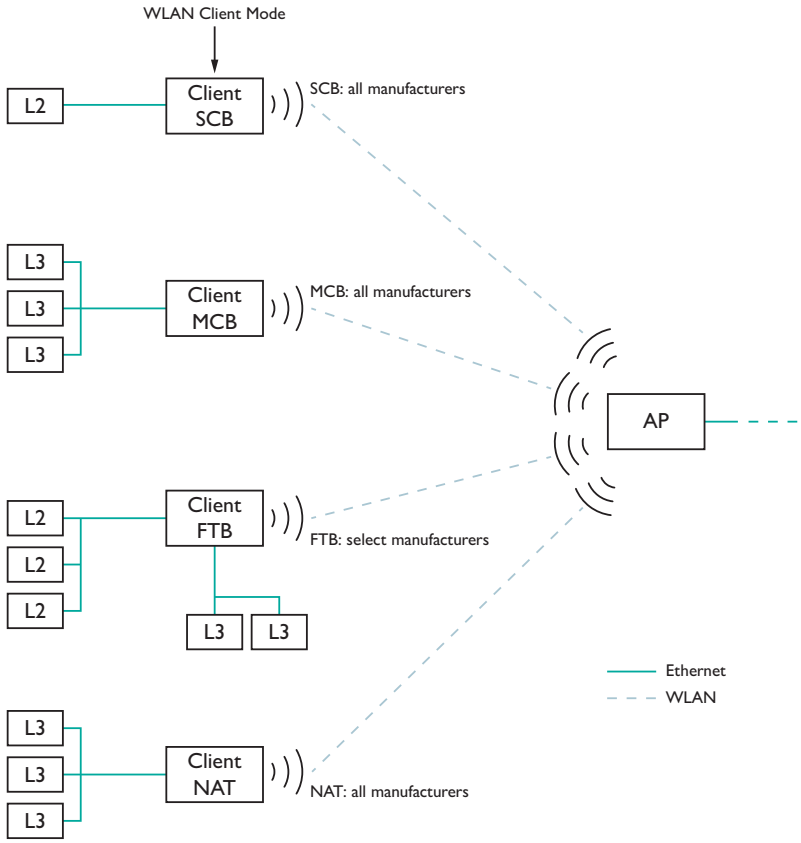
The process where a WLAN client switches from one access point to another is known as roaming. The roaming speed varies depending on the type of client used. A notebook, for example, will need quite a long time. For applications where roaming needs to be carried out in a fraction of a second, you must 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 1000/2000 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 Figure 4-7).

4.2.2 Compatibility between different WLAN device manufacturers

The following describes points relating to the client configuration that should be noted 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.

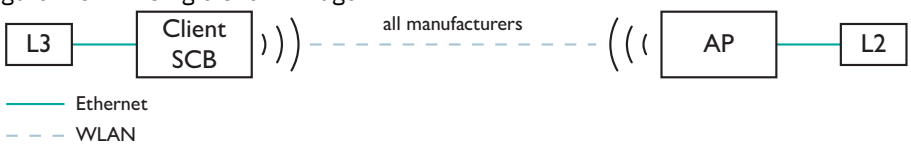
The “Client (NAT)” operating mode supports devices that are NAT-compatible, regardless of the manufacturer. The “1:1 NAT” and “IP Masquerading” NAT functions are available. “1:1 NAT” lets you connect one device per IP address, “IP Masquerading” lets you connect several (see “Operating mode: Client (NAT)” on page 98).

The “Client (FTB)” operating mode, on the other hand, only supports communication between a single manufacturer’s devices. The technical implementation varies from manufacturer to manufacturer. You can connect several network devices to a device with the “Client (FTB)” operating mode.

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 access point on Layer 2 via WLAN.

To use access via SCB port forwarding, the WLAN device only learns one IP address for the MAC address. Therefore, make sure that the connected computer uses one IP address only. If the computer uses several addresses, the access rule may not apply.

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.

Example of static IP:

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. 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.

Example of DHCP/BOOTP/DCP:

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

If you connect several Ethernet devices in automatic SCB mode, it is possible that the MAC address of an unwanted device is entered automatically, even during later operation. To avoid this, it is recommended that you use manual SCB mode.

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” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.

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

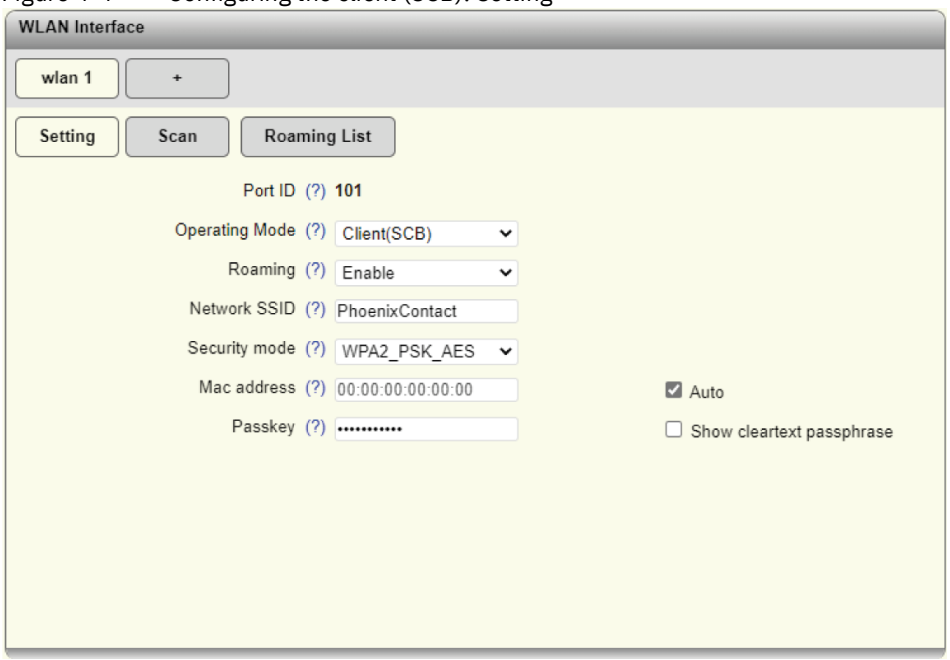


Table 4-2 Configuring the client (SCB): Setting: Parameters

Parameter	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.

Table 4-2 Configuring the client (SCB): Setting: Parameters

Parameter	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. – WEP: This option is not recommended because of its security features. – WPA2-EAP: This encryption method is used for RADIUS authentication (see “RADIUS certificates” on page 125). For further information about the parameters available for this encryption method, see “Encryption: WPA2-EAP and FT-EAP” on page 87. – 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” on page 87. **NOTE: Network security** If you select “None”, the data is sent without encryption. This option puts network security at risk.
Mac address	Here, enter the desired IP address for a manual assignment. For an automatic IP address assignment, activate the “Auto” check box.
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between 8 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

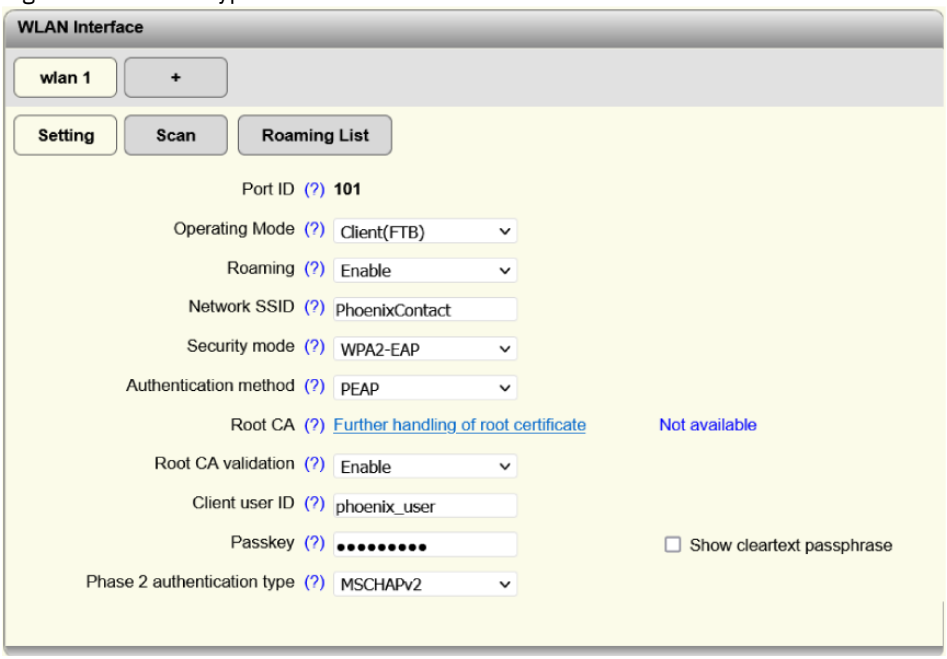


Table 4-3 Encryption: WPA2-EAP and FT-EAP: Parameters

Parameter	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.
Root CA	Click on "Further handling of root certificate" to open the "File Transfer" pop-up window. Here, you can upload a root certificate (see "File Transfer" on page 69).
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** If you select "Disable", the server identity will not be validated. This option is not secure.

Table 4-3 Encryption: WPA2-EAP and FT-EAP: Parameters

Parameter	Description
Client certificate	This option is only available if you selected “TLS” for “Authentication method”. Click on “Further handling of client certificate” to open the “File Transfer” pop-up window. Here, you can upload a client certificate (see “File Transfer” on page 69).
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 on “Apply&Save”.

↳ A WLAN device can now use the defined access data to connect to the wireless interface.

- Click on “Scan”.

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

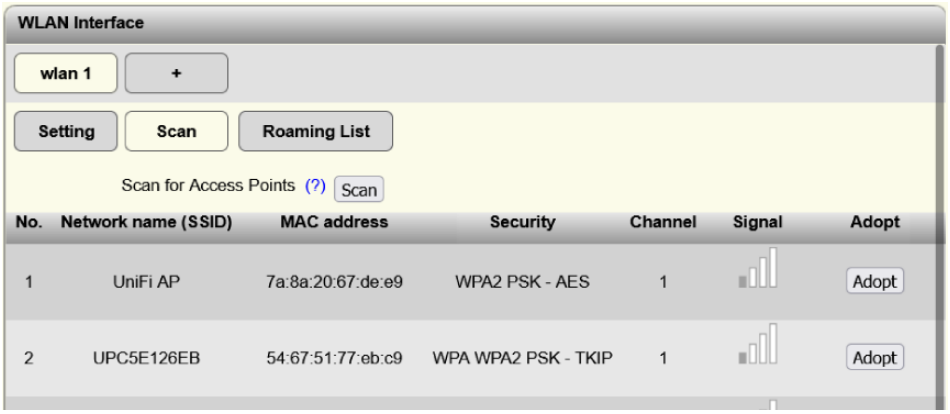


Table 4-4 Configuring the client (SCB): Scan: Parameters

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

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

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

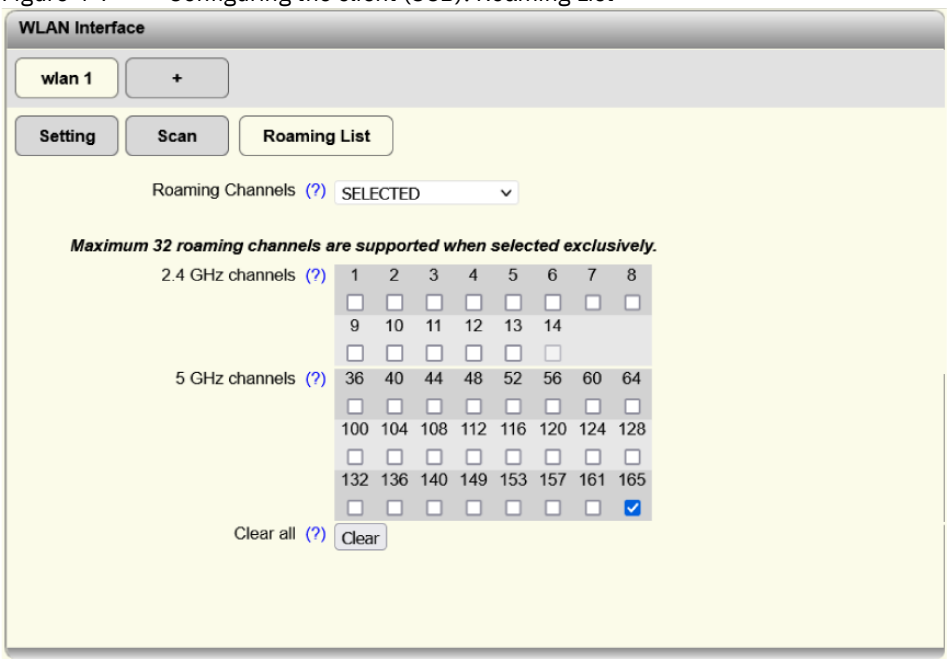


Table 4-5 Configuring the client (SCB): Roaming List: Parameters

Parameter	Description
Roaming Channels	Select whether the device should search all available channels or just selected channels for networks. The more channels you select, the longer will roaming take. Select only 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 on “Clear all” to deactivate all check boxes in the 2.4 GHz and 5 GHz ranges.

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

The more channels you select, the longer will roaming take. Select only 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 on “Apply&Save”.

4.2.4 Operation as a 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. These include, for example, TCP/IP but not PROFINET or Ethernet/IP.

4.2.4.2 Configuring the client (MCB)

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.

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

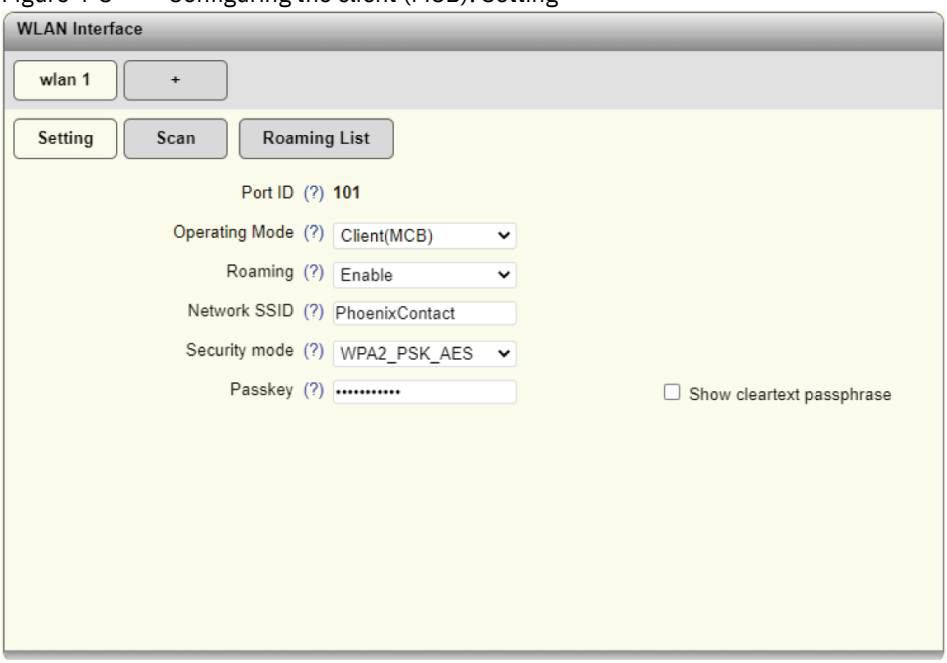


Table 4-6 Configuring the client (MCB): Setting: Parameters

Parameter	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).

Table 4-6 Configuring the client (MCB): Setting: Parameters

Parameter	Description
Network SSID	Here, enter the desired network SSID. The SSID is the network ID by means of which WLAN devices 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. – WEP: Only available in “Client” (FTB, MCB, SCB) operating mode. This option is not recommended because of its security features. – WPA2-EAP: This encryption method is used for RADIUS authentication (see “RADIUS certificates” on page 125). For further information about the parameters available for this encryption method, see “Encryption: WPA2-EAP and FT-EAP” on page 87. – 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” on page 87. – Advanced config: Select this option if you already configured encryption on another interface (e.g., via CLI). **NOTE: Network security** If you select “None”, the data is sent without encryption. This option puts network security at risk.

Table 4-6 Configuring the client (MCB): Setting: Parameters

Parameter	Description
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between 8 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 on “Apply&Save”.

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

- Click on “Scan”.
- Click on “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 Figure 4-6).
- Click on “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.
- Click on “Roaming List”.
- Select whether the device should search all available channels or just selected channels for networks (see Figure 4-7).

The more channels you select, the longer will roaming take. Select only 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 on “Apply&Save”.

4.2.5 Operation as a fully transparent bridge

4.2.5.1 General information

Properties:

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

Connection is only possible with devices (access points) that support the same fully transparent bridge mode. As a rule, this is only possible with devices from the same manufacturer.

4.2.5.2 Configuring the client (FTB)

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.

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

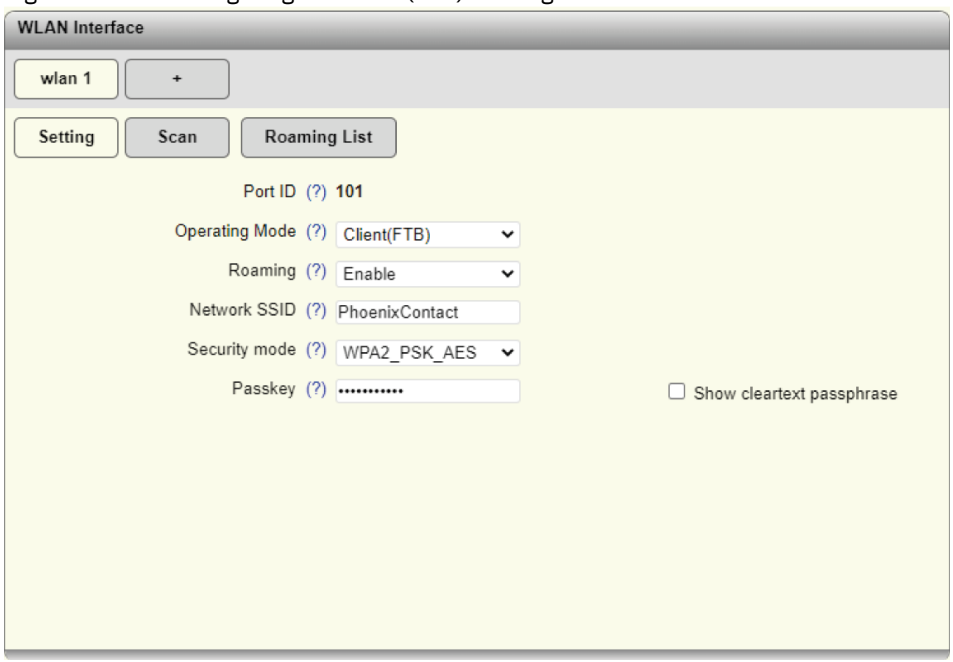


Table 4-7 Configuring the client (FTB): Setting: Parameters

Parameter	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). – Advanced config: Select this option if you already configured roaming on another interface (e.g., via CLI).

Table 4-7 Configuring the client (FTB): Setting: Parameters

Parameter	Description
Network SSID	Here, enter the desired network SSID. The SSID is the network ID by means of which WLAN devices 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. – WEP: This option is not recommended because of its security features. – WPA2-EAP: This encryption method is used for RADIUS authentication (see “RADIUS certificates” on page 125). For further information about the parameters available for this encryption method, see “Encryption: WPA2-EAP and FT-EAP” on page 87. – 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” on page 87.
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between 8 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 on “Apply&Save”.

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

- Click on “Scan”.

- Click on “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 Figure 4-6).
- Click on “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.
- Click on “Roaming List”.
- Select whether the device should search all available channels or just selected channels for networks (see Figure 4-7).

The more channels you select, the longer will roaming take. Select only 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 on “Apply&Save”.

4.3 Operating mode: Client (NAT)

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

You can configure at most one virtual interface in the “Client (NAT)” operating mode.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.
- On the “WLAN Interface” page, set the “Client (NAT)” option for “Operating Mode”.

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

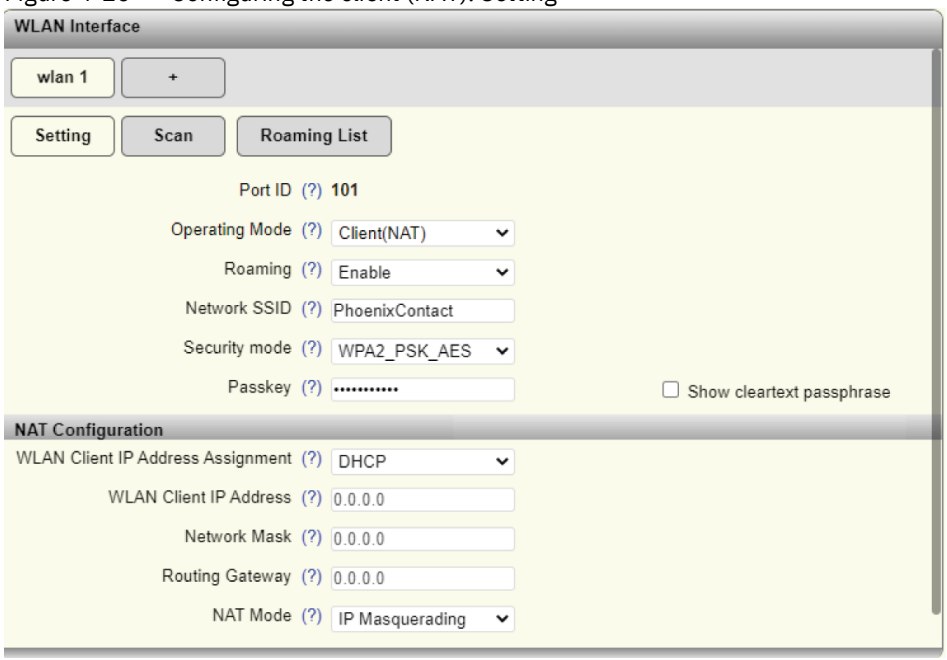


Table 4-8 Configuring the client (NAT): Setting: Parameters

Parameter	Description
Port ID	The internal port ID of the wireless interface is displayed here.
Operating Mode	Set 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. – 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).

Table 4-8 Configuring the client (NAT): Setting: Parameters

Parameter	Description
Network SSID	Here, enter the desired network SSID. The SSID is the network ID by means of which WLAN devices 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. – WEP: This option is not recommended because of its security features. – WPA2-EAP: This encryption method is used for RADIUS authentication (see “RADIUS certificates” on page 125). For further information about the parameters available for this encryption method, see “Encryption: WPA2-EAP and FT-EAP” on page 87. – 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” on page 87.
Passkey	Here, enter a pre-shared key that is used for authentication and encryption. The pre-shared key can be between 8 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

Table 4-9 Setting: NAT Configuration: Parameters

Parameter	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 services” on page 119).
WLAN Client IP Address	This option is only available if you selected “STATIC” for “WLAN Client IP Address Assignment”. Here, enter the IP address of the WLAN client.
Network Mask	This option is only available if you selected “STATIC” for “WLAN Client IP Address Assignment”. Here, enter the subnet mask of the target network to which the static route refers.
Routing Gateway	This option is only available if you selected “STATIC” for “WLAN Client IP Address Assignment”. Here, enter the IP address of the routing gateway.
NAT Mode	Set the desired NAT mode. Confirm your selection by clicking on “Apply”. – 1-to-1 NAT: For further information, see “Configuring 1:1 NAT” on page 101. – IP Masquerading: For further information, see “Configuring IP masquerading” on page 105.

The other parameters on this page depend on the selected NAT mode and are dealt with in the corresponding sections (see “Configuring 1:1 NAT” on page 101 and “Configuring IP masquerading” on page 105).

4.3.1 Configuring 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:

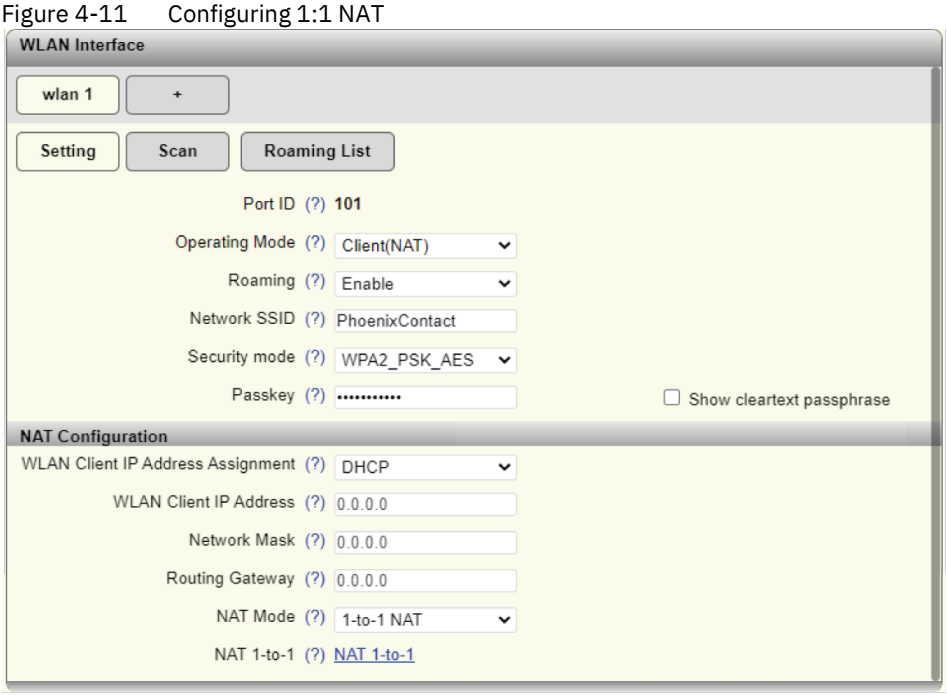
– No route or gateway configuration necessary in the WAN
– Communication can be established from both the LAN and WAN
– Not restricted to dedicated protocols

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 on “Apply”.

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

- Click on “NAT 1-to-1” to open the “1-to-1 NAT Configuration” pop-up window.

Pop-up window: 1-to-1 NAT Configuration

Figure 4-12 Pop-up window: 1-to-1 NAT Configuration

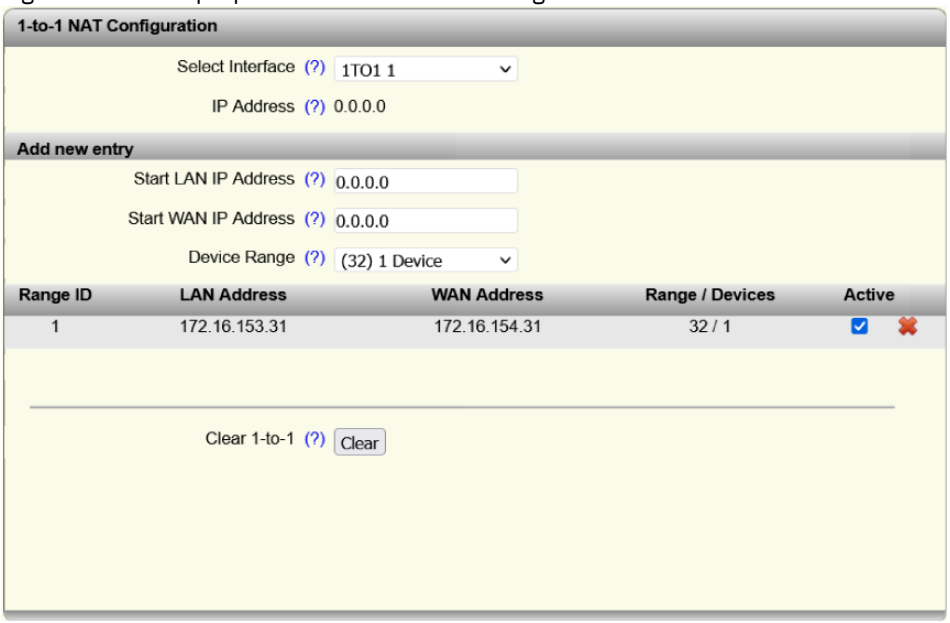


Table 4-10 1-to-1 NAT Configuration: Parameters

Parameter	Description
Select Interface	The interface is displayed here. There is only ever one interface available.
IP Address	The IP address of the WLAN client is displayed here.
Start LAN IP Address	Here, enter the start IP address of the area that is to be translated.
Start WAN IP Address	Here, enter the start IP address of the area that is to be translated to. 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	Here, select the number of IP addresses that are to be translated.
Clear 1-to-1	Click on “Clear” to delete the complete table for the selected interface.

- Set the parameters as desired.
- Click on “Apply” to populate the table with the entered data.
- To populate the table with more data, enter the desired parameters again and click on “Apply”.
- Close the “1-to-1 NAT Configuration” pop-up window.
- Click on “Scan”.
- Click on “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 Figure 4-6).

- Click on “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.
- Click on “Roaming List”.
- Select whether the device should search all available channels or just selected channels for networks (see Figure 4-7).

The more channels you select, the longer will roaming take. Select only 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 on “Apply&Save”.

4.3.1.2 Example configuration

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

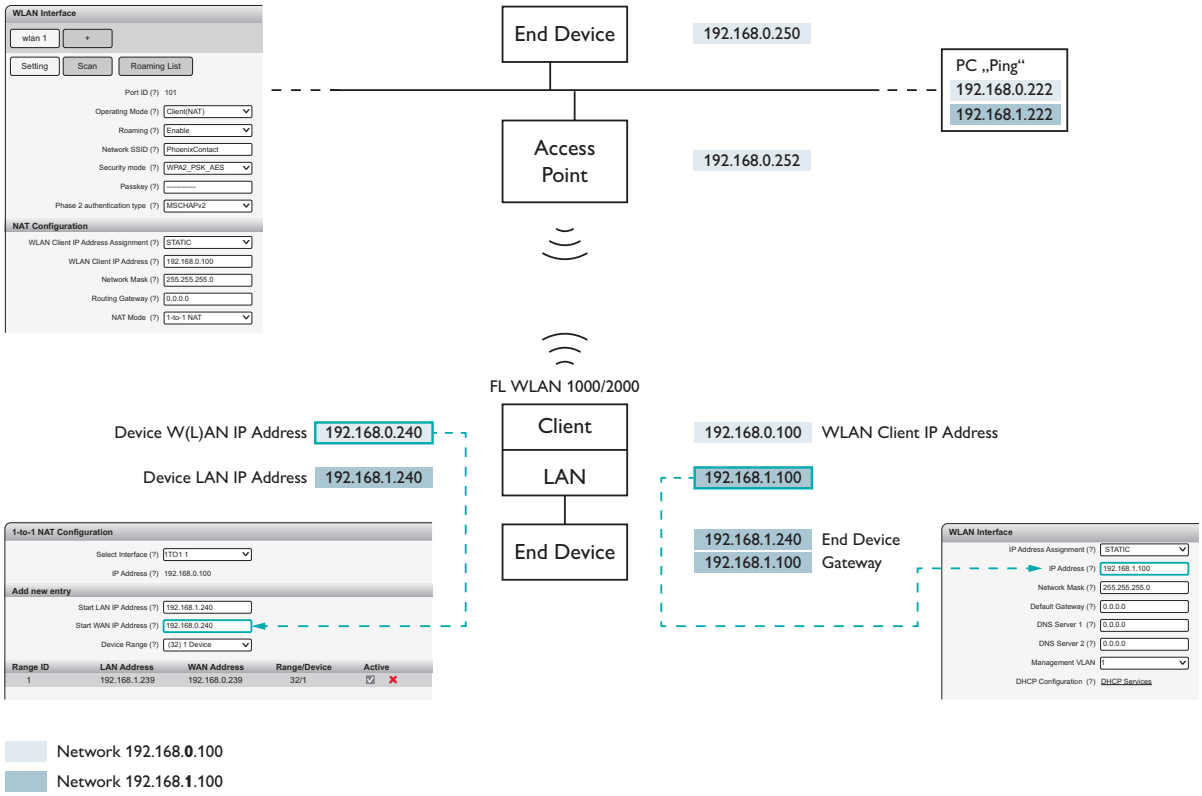
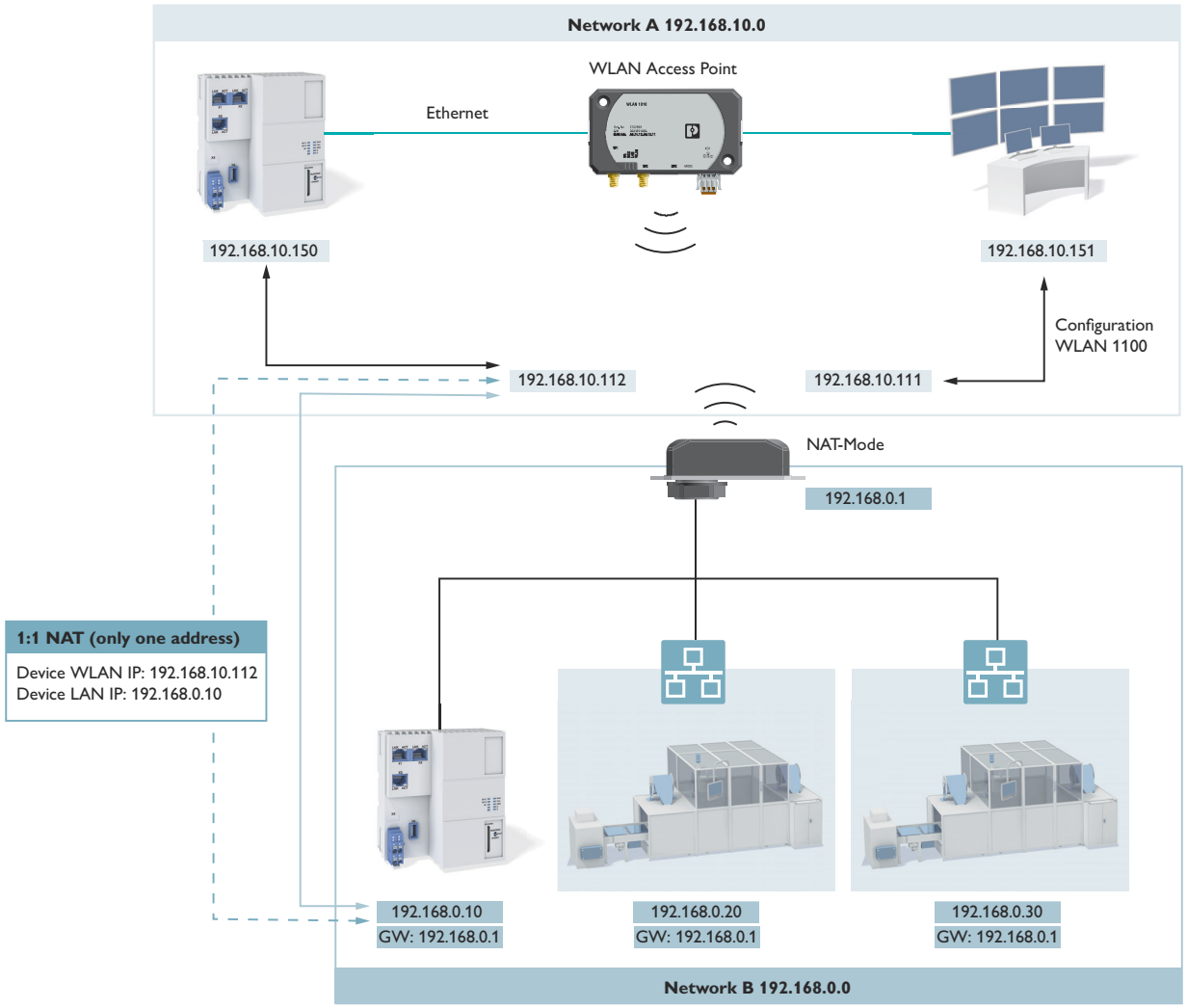


Figure 4-14 1:1-NAT: Example configuration 2



4.3.2 Configuring 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.

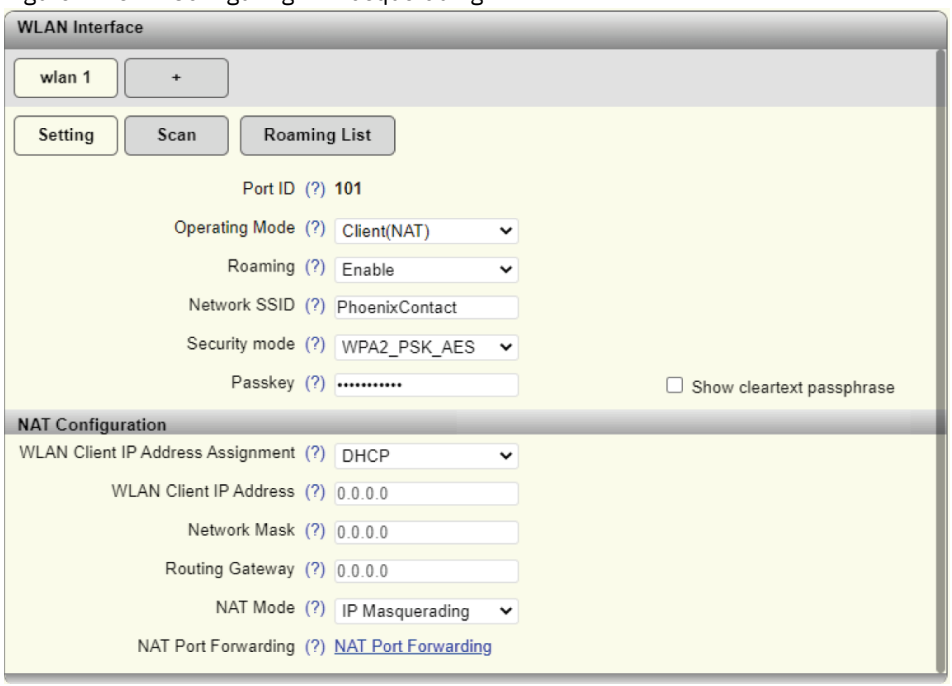
Disadvantage:

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

4.3.2.1 Configuring IP masquerading

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.

Figure 4-15 Configuring IP masquerading



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

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

- Click on “NAT Port Forwarding” to open the “IP Masquerading Configuration” pop-up window.

Pop-up window: IP Masquerading Configuration

Figure 4-16 Pop-up window: IP Masquerading Configuration

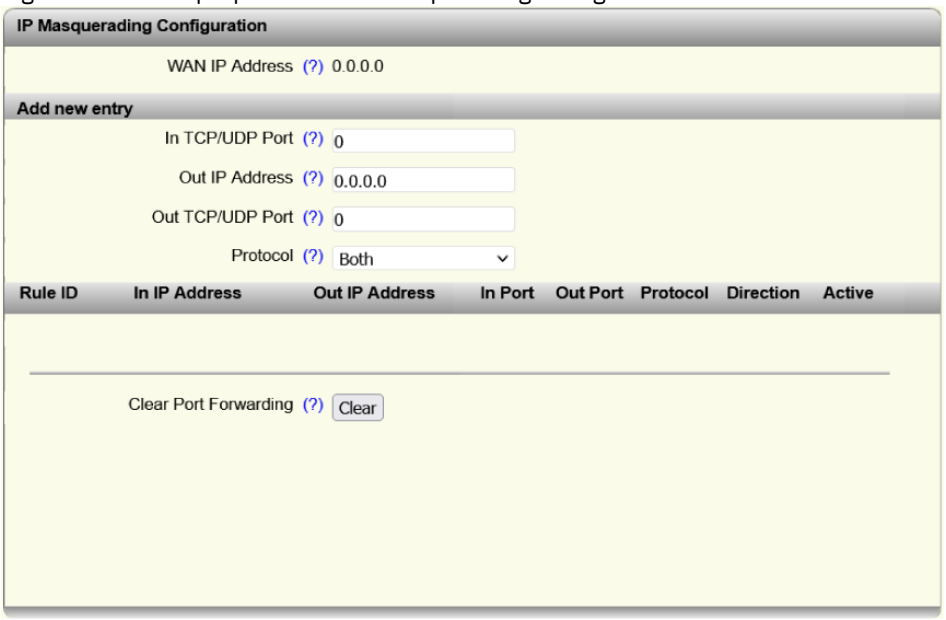


Table 4-11 IP Masquerading Configuration: Parameters

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

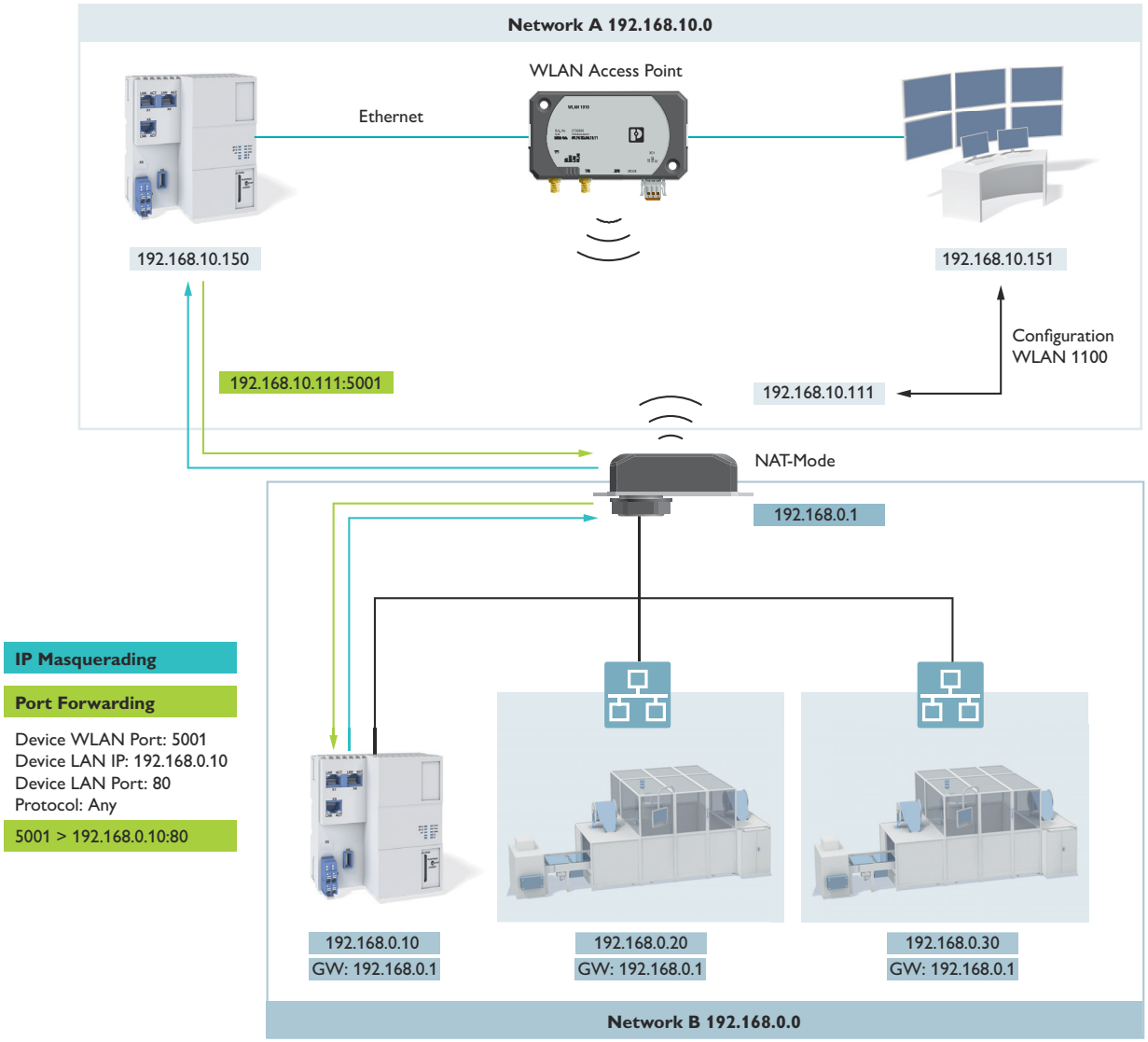
- Click on “Scan”.
- Click on “Scan” to search for available access points. Available access points are displayed in the table with information such as the SSID or the signal strength (see Figure 4-6).
- Click on “Adopt” next to the desired access point to apply the access point settings. The SSID as well as the encryption settings are applied.
- Click on “Roaming List”.
- Select whether the device should search all available channels or just selected channels for networks (see Figure 4-7).

The more channels you select, the longer will roaming take. Select only 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 on “Apply&Save”.

4.3.2.2 Example configuration

Figure 4-17 IP masquerading: Example configuration



4.4 Operating mode: Repeater

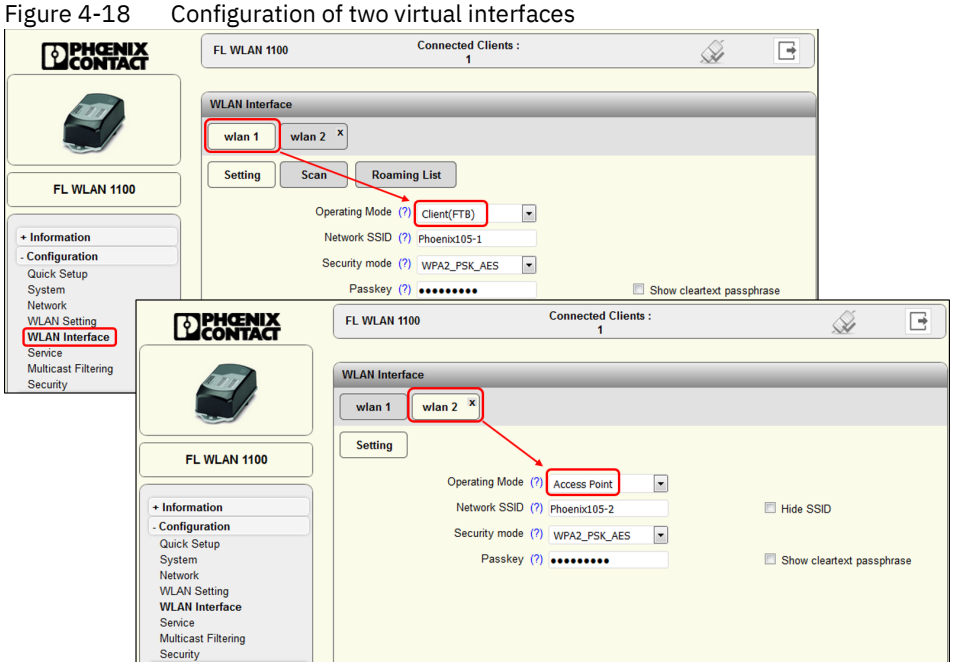
The devices have two virtual wireless interfaces, which can be individually configured. Two access points or, alternatively, one access point and one client, can be configured at the same time. You can regard the combination of access point and client as a repeater. In the “Quick Setup” menu, you can configure both virtual wireless interfaces under “Repeater” (see “Quick Setup” on page 39). The “WLAN Interface” menu shows both virtual wireless interfaces separately, without using the term “Repeater” (see “WLAN Interface” on page 46). 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”.

4.4.1 Configuration example

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.
- Configure the first interface as a client and the second interface as an access point.
  – Set “Client” once and “Access Point” once for “Operating Mode”.

Figure 4-18 Configuration of two virtual interfaces

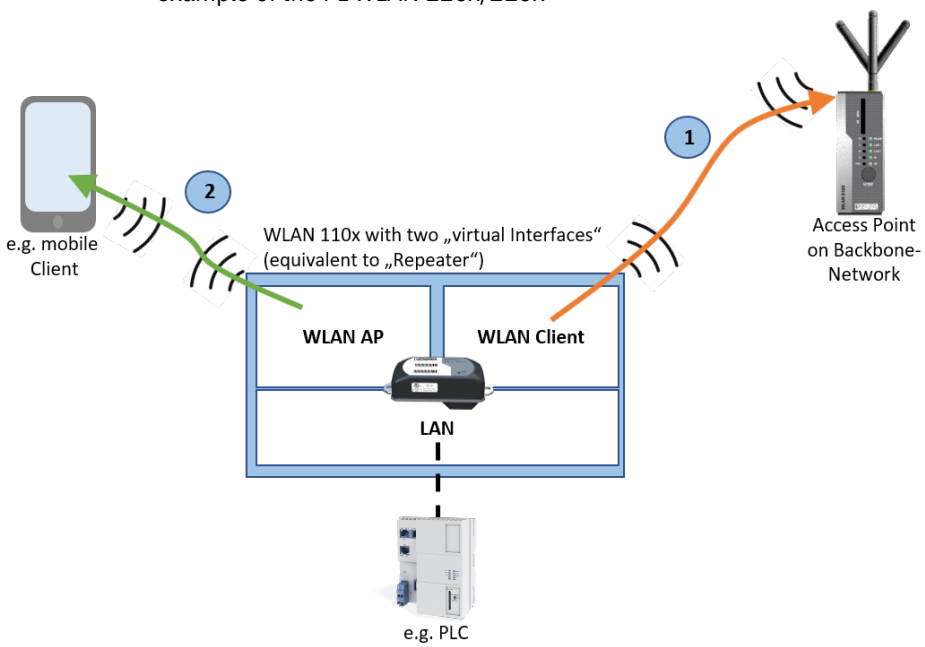


When configuring two virtual wireless interfaces, you should always configure “WLAN 2” as an access point. You can optionally configure “WLAN 1” as an access point or a client.

4.4.2 Properties of two virtual wireless interfaces

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

Figure 4-19 Structural representation of both wireless and cable interfaces using the example of the FL WLAN 110x/210x



Up to FW 2.40

The connection (1) between the WLAN client and the higher-level access point must be established. Only then will the WLAN access point of the WLAN device be available. Now, the connection (2) to additional clients is established (see Figure 4-19).

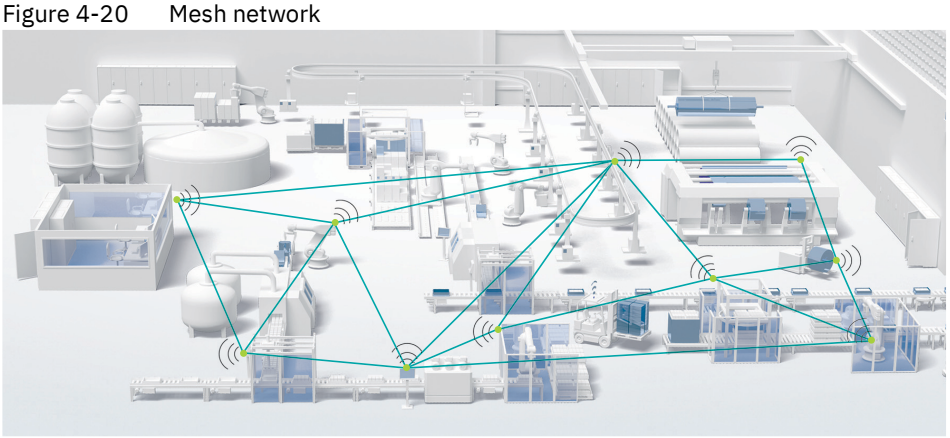
As of FW 2.50

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 voltage reset of the device (see Figure 4-19).

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.

4.5 Operating mode: Mesh (only FL WLAN 2xxx)

Figure 4-20 Mesh network



Requirement:

Devices of the type FL WLAN 2010/2011 or FL WLAN 2100/2101 with firmware version 2.60 or higher

The “Mesh” operating mode is a proprietary mode by Phoenix Contact that only supports wireless communication between the specified device types.

If you want to connect other devices to the mesh network, you can configure a secondary WLAN interface as an access point. You can then connect further devices via the access point (see “Setting up a secondary WLAN interface as an access point” on page 116).

4.5.1 Mesh functions and best practice

The main mesh function of the FL WLAN 2xxx devices is to provide wireless communication between various locations. The access point infrastructure used as standard is not used for this. The user can set up a “private” network, which is set up isolatedly and separated from a company network. The mesh functionality uses standard WLAN principles for the communication and behaves like a typical infrastructure in WLAN networks.

- All nodes in the mesh network use the same frequency and the same channel. It is important before startup to be mindful of the utilization of the channel that is to be used. The channel utilization should be less than 30%. The lower the channel utilization, the higher the network performance.
- In order for the mesh network to be able to establish itself autonomously and detect other nodes as mesh nodes, the over-the-air baud rate from node to node in 802.11n mode must be at least 54 Mbps. In most cases, this baud rate can be achieved if the RSSI between nodes is –65 dBm or better. If the baud rate is not achieved, these nodes will not be detected as potential mesh nodes.
- Best practice: Set the same frequency and the same channel for all nodes. Further, reduce the roaming scan list so that only the channel in use is scanned. This reduces the utilization of the modules and makes communication more efficient. Automatic channel selection is not recommended here.
- Avoid any sudden disconnection of the power supply. In some cases this could delay the recalculation of the transmission paths.

– If you configure a WLAN device for the “Mesh” operating mode that was previously used in another operating mode, you should first reset the device to the default settings (see “Resetting to the default settings” on page 14). This will reset all the settings made.

4.5.2 Limits of mesh

Simultaneous startup of multiple nodes

Any attempt to start up multiple mesh nodes **at one time** and **in one place**, for example, by switching on the power supply for all of them simultaneously, may result in channel overload.

– Background: Each mesh node exchanges a number of security keys with each other node in its environment when starting. Switching on all the nodes simultaneously can cause heavy data traffic due to the high number of exchanged keys.
– Remedy: Start the mesh nodes with a time delay. The individual nodes then request the security keys on a staggered basis.

Number of mesh nodes at a location

You can use many mesh nodes in a network. The number of mesh nodes that can connect directly to each other is, however, restricted. This is due to how encryption is handled internally. Each node exchanges a security key with each other node. Make sure, wherever possible, to operate a **maximum of 20 nodes** at a location.

In total, however, you can connect many more nodes to the same mesh network. However, they should not all need to be able to exchange data directly. Achieve this by means of structural separation, if a physical separation is not sufficient. Alternatively, you can also reduce the transmission power by a certain and appropriate amount as a way of reducing the range of the nodes.

Using 5 GHz (only FL WLAN 2010 and FL WLAN 2100)

According to applicable guidelines, Mesh cannot be used on 5 GHz channels that require DFS (Dynamic Frequency Selection/radar detection). For the devices FL WLAN 2010 (item number 1119246) and FL WLAN 2100 (item number 2702535), it appears as if all 5 GHz channels could be selected. This is not the case, even if no error message appears. Use only the 5 GHz channels 36 to 48 (only for indoor areas) for the configuration in European countries.

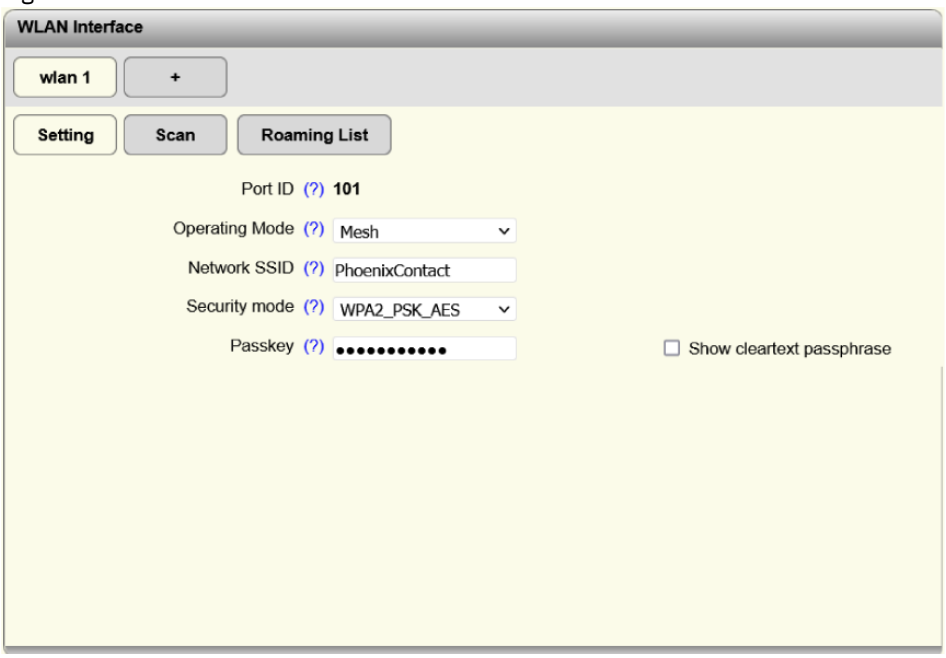
4.5.3 Setting up FL WLAN 2xxx for Mesh

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, Network”.
- In the “IP Address Assignment” drop-down list, select the “STATIC” option.
- Assign a static IP address and a subnet mask.
- Click on “Apply&Save”.
- Click on “Configuration, WLAN Setting”.

Figure 4-21 WLAN Setting

- Activate the “Activate WLAN interface” check box.
- For “Channel”, select the desired channel.
- Define the other parameters as desired and click on “Apply&Save” (see “WLAN Setting” on page 44).
- Click on “Configuration, WLAN Interface”.

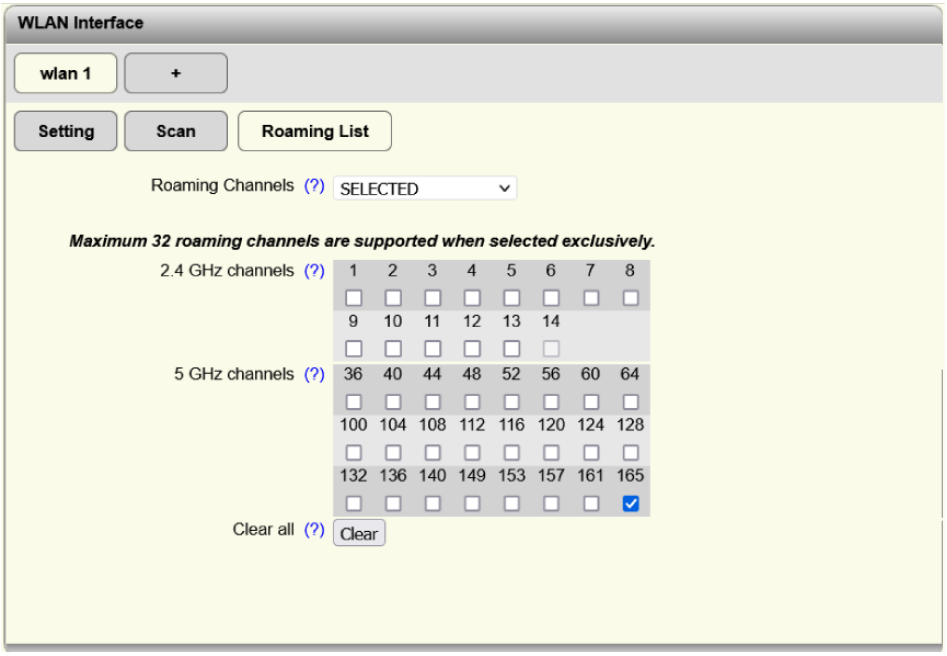
Figure 4-22 WLAN Interface



- In the “Operating Mode” drop-down list, select the “Mesh” option.
- Enter the desired SSID in the “Network SSID” input field. The SSID can be up to 32 characters long. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space.
- In the “Security mode” drop-down list, select the desired encryption method.

To enable a high security standard and efficient communication within the mesh network, you can only select “WPA2_PSK_AES” here.

Figure 4-23 WLAN Interface: Roaming List



- Click on “Roaming List”.
- In the “Roaming Channels” drop-down list, select the “SELECTED” option.
- Activate the check box for the channel you set on the “WLAN Setting” page.
- Click on “Apply&Save”.

Repeat these steps for all devices of the type FL WLAN 2xxx that you want to add to the mesh network. Make sure to make the same settings.

Once you have made the settings in other devices, you can see an overview of all configured devices:

- Click on “Information, Connections”.

If you cannot see all the configured devices, make sure that the settings are the same in all the devices.

4.5.4 Setting up a secondary WLAN interface as an access point

If you want to connect other devices to the mesh network, you can configure a secondary WLAN interface as an access point.

The secondary WLAN interface uses the same frequency and the same channel as the mesh network, because the device uses the same WLAN card for both interfaces.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.
- Click on “+” to activate the “WLAN 2” interface.

The only available mode in the “Operating Mode” drop-down list is “Access Point”.

- Enter the desired SSID in the “Network SSID” input field. The SSID can be up to 32 characters long. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~| and space.
- In the “Security mode” drop-down list, select the desired encryption method.
- Enter the desired password in the “Passkey” input field. The password can be 8 to 64 characters long. Letters, numbers, and the following special characters are permitted: $%@&/\()=?![]{}+*-_<>#^.,:~|.
- Click on “Apply&Save”.

↪ Additional devices can now connect to the mesh network via the access point.

On devices that should be connected to the mesh network via the access point, set a static IP address or activate a DHCP server in the mesh network (see “DHCP services” on page 119).

4.5.5 Mesh: Diagnostics

4.5.5.1 Channel utilization

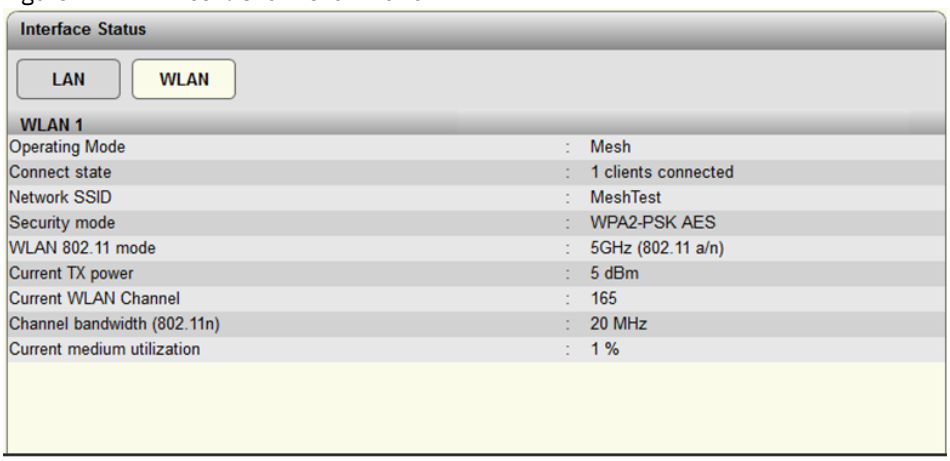
You can display the total utilization of the selected channel.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Information, Interface Status, WLAN”.

The specified percentage reflects the interpretation of the utilization of the specific module you are logged into. The utilization may vary slightly from device to device.

The item “Current medium utilization” shows the total utilization of the selected channel. For WLAN communication, the utilization should not exceed 30%.

Figure 4-24 Mesh: Channel utilization

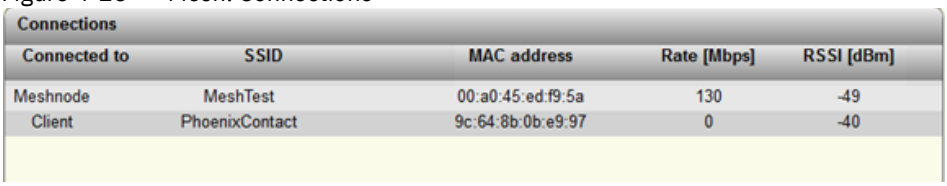


4.5.5.2 Connections

You can display all the connected devices and view further information about them. This includes the network they are assigned to, the baud rate, and the RSSI.

- Open web-based management (see “Accessing web-based management” on page 23) and log in.
- Click on “Information, Connections”.

Figure 4-25 Mesh: Connections



4.5.5.3 MAC addresses

For technical reasons, all WLAN devices within a mesh network have different MAC addresses **internally**. This information can be used for data analysis (e.g., snapshot data). It is not relevant for normal operation.

The following table shows a sample assignment of various MAC addresses to a device.

Table 4-12 Mesh: Overview of MAC addresses

Device	MAC address	Description	Detail
FL WLAN 2101	A8:74:1D:74:B0:84	MAC address printed on device	
FL WLAN 2101	A8:74:1D:74:B0:85	MAC address of LAN	1 byte higher than MAC address printed on device
FL WLAN 2101	A8:74:1D:74:B0:88	MAC address of internal mesh VLAN (not used in customer applications)	4 bytes higher than MAC address printed on device
FL WLAN 2101	A8:74:1D:74:B0:89	MAC address of WLAN card	5 bytes higher than MAC address printed on device

5 DHCP services

5.1 Activating DHCP services

The devices FL WLAN 110x/210x and FL WLAN 101x/201x 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.

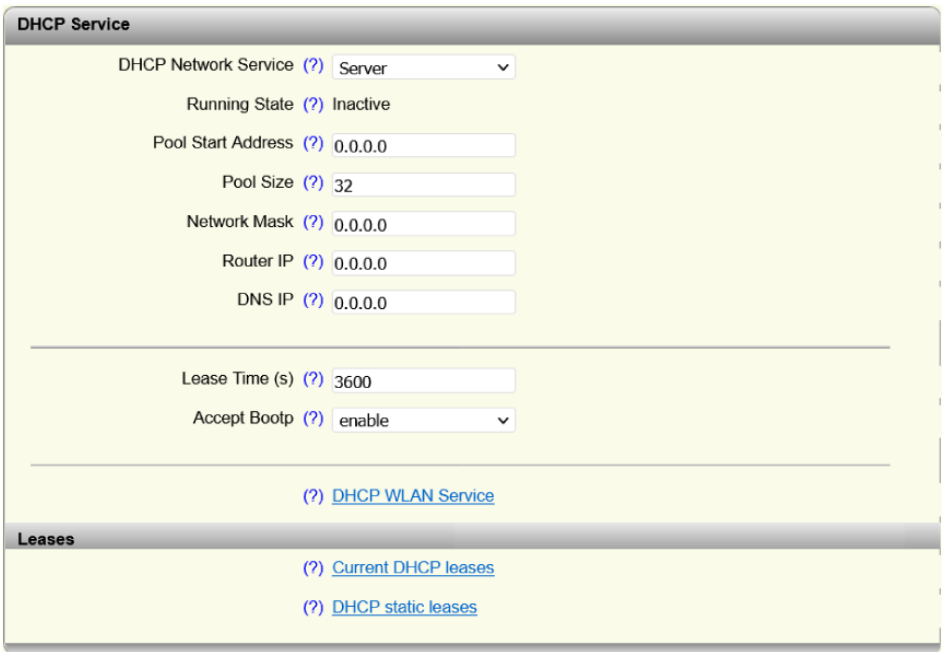
- Click on “Configuration, Network”.
- In the “IP Address Assignment” drop-down list, select the “STATIC” option.

↪ The “DHCP Configuration” menu item appears.

- Click on “DHCP Services”.

DHCP Service

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 on “Apply”.

5.2 Activating the global DHCP server on all interfaces

You can assign IP addresses via DHCP for all interfaces, on the cable side via LAN as well as 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 services” on page 119).
- You can now set the following parameters:

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

Table 5-1 DHCP Service: Parameters

Parameter	Description
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	Here, enter the first IP address of the DHCP server address pool. 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	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.
Lease Time (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”.
Accept Boot	Here, select 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.

Table 5-1 DHCP Service: Parameters

Parameter	Description
DHCP WLAN Service	Click on “DHCP WLAN Service” to open the “DHCP WLAN Service” pop-up window (see “Pop-up window: DHCP WLAN Service” on page 121).
Current DHCP leases	Click on “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” on page 123).
DHCP static leases	Click on “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” on page 123).

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

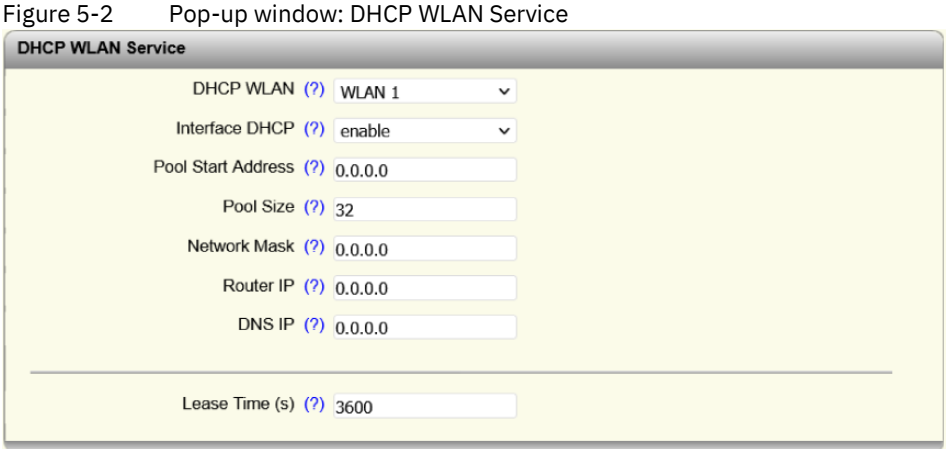
By means of the configuration described below, IP addresses can be assigned via DHCP via the WLAN interface(s) only, but not via the cable-side LAN interface.

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 services” on page 119).
- Do not enter an IP address for “Pool Start Address”. No IP addresses will then be assigned via the LAN interface.
- Click on “DHCP WLAN Services”.

Pop-up window: DHCP WLAN Service

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



- You can now set the following parameters:

Table 5-2 DHCP WLAN Service: Parameters

Parameter	Description
DHCP WLAN	Here, select the desired WLAN interface. You may need to configure the WLAN interfaces first (see “WLAN Interface” on page 46).
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 “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	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.
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 each other. If that is the case, the address is output on one interface only.

Observe the following notes:

- DHCP requests on inactive interfaces (WLAN 1, WLAN 2) are not responded to.
- 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.

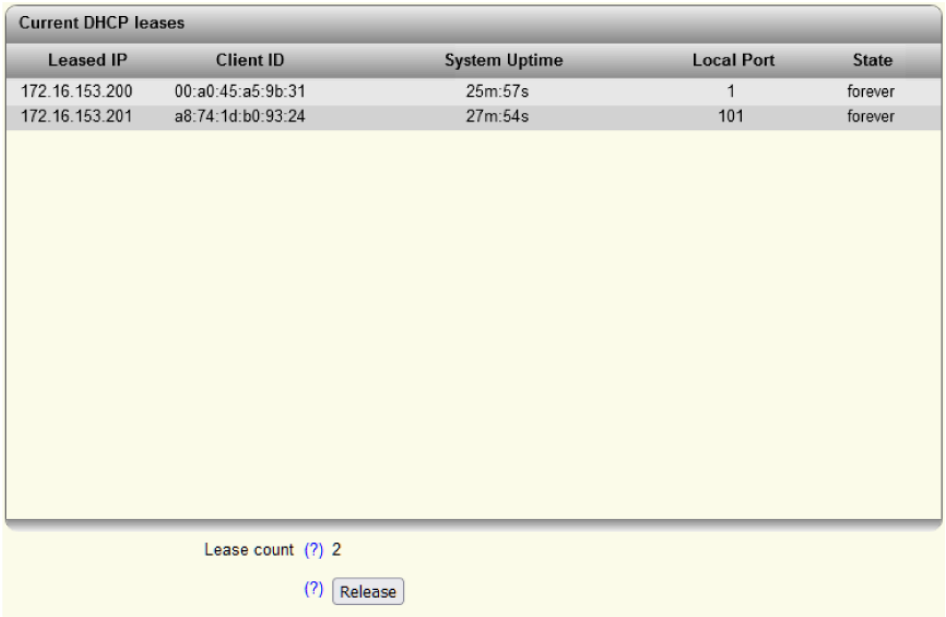
5.4 Diagnostics

- Activate the DHCP server (see “Activating DHCP services” on page 119).

Pop-up window: Current DHCP leases

- Click on “Current DHCP leases”.

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



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

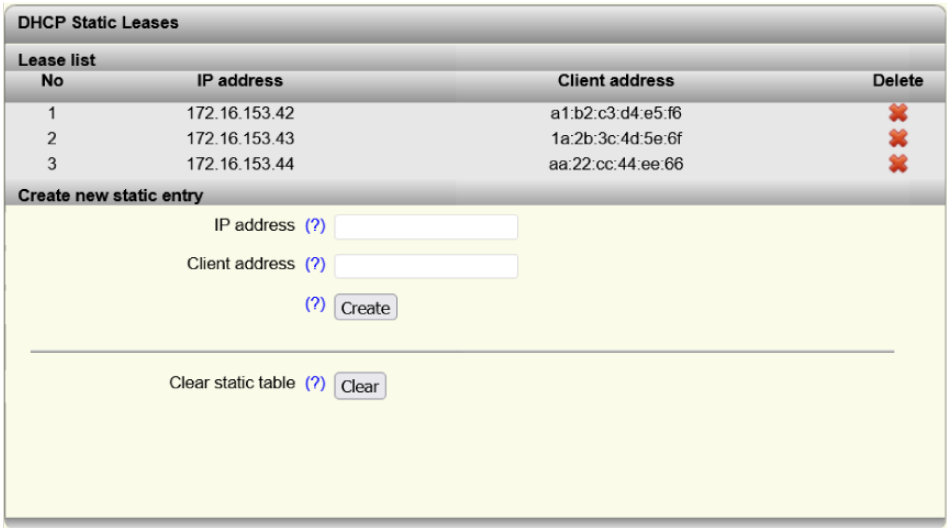
Table 5-3 Current DHCP leases: Parameters

Parameter	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 on “Release” to release unused entries again.

Pop-up window: DHCP Static Leases

- Click on “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.

Table 5-4 DHCP Static Leases: Parameters

Parameter	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

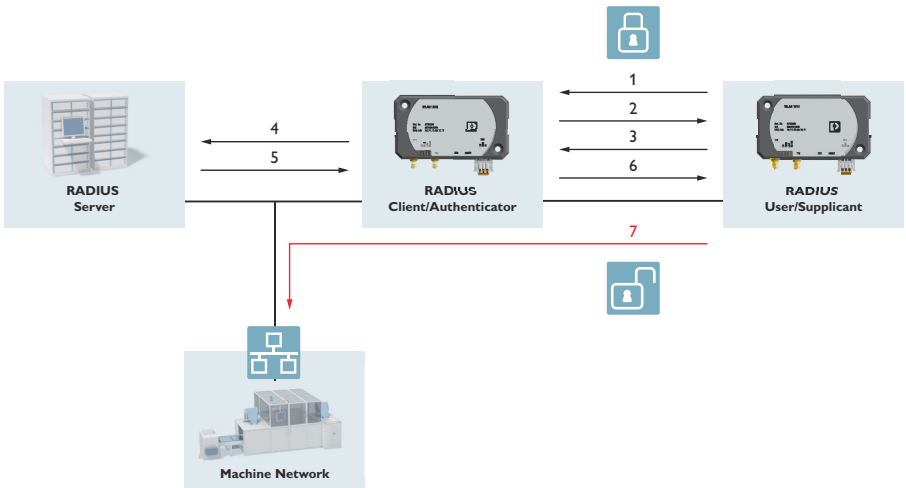
RADIUS stands for “Remote Authentication Dial-in User Service”. It is a client/server protocol that is also referred to as a “triple-A” protocol. The three “A”s stand for authentication, authorization, and accounting.

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.

6.1.1 Sequence of the 802.1X authentication process

Figure 6-1 802.1X RADIUS process (simplified)

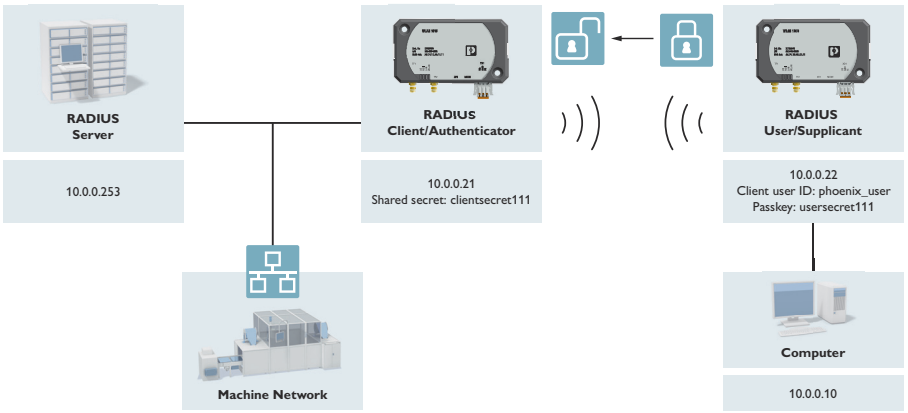


1. The supplicant sends a start packet to the authenticator.
2. The authenticator asks the supplicant for the access data.
3. The supplicant sends the access data to the authenticator.
4. The authenticator sends the supplicant’s access data as well as its own access data to the RADIUS server.
5. The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

6.2 Example configuration

Figure 6-2 RADIUS: Example configuration



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

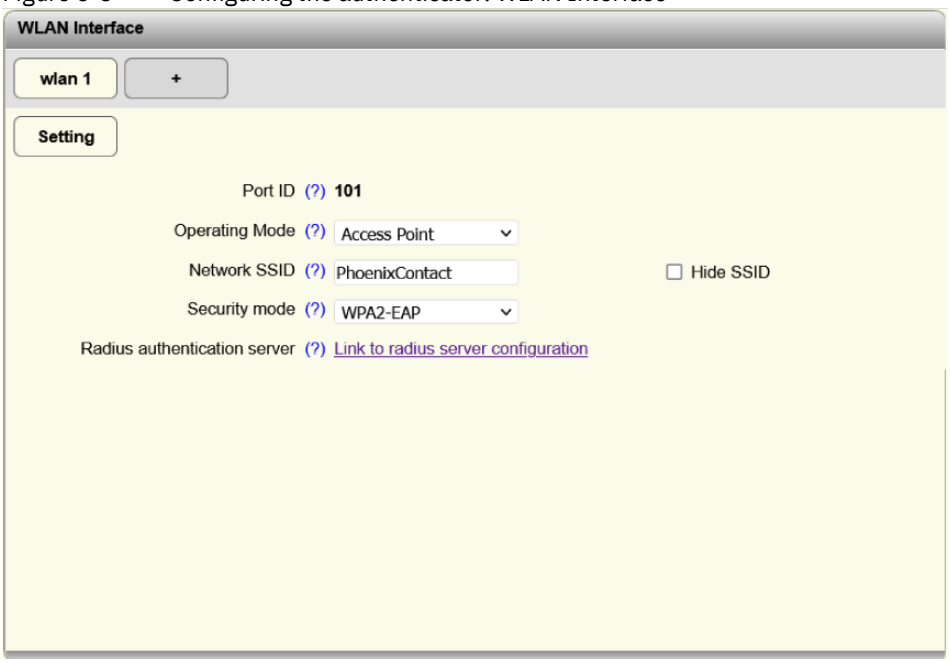
– Authenticator's access data:
  – IP address of authenticator: 10.0.0.21
  – Shared secret of authenticator: clientsecret111
– Supplicant's access data:
  – User name: phoenix_user
  – Passkey: usersecret111

6.3 Configuring RADIUS

6.3.1 Configuring the authenticator

- Open web-based management on the authenticator (see "Accessing web-based management" on page 23) and log in.
- Click on "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 on “Configuration, Security”.

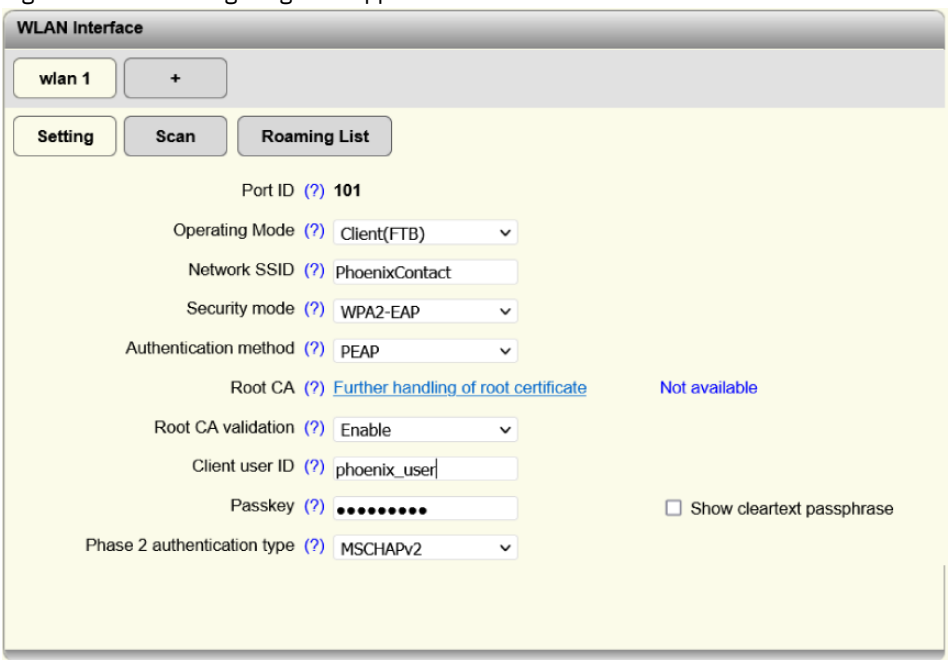
Figure 6-4 Configuring the authenticator: Security

- 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 on “Apply&Save” to save your settings.

6.3.2 Configuring the supplicant

- Open web-based management on the supplicant (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.

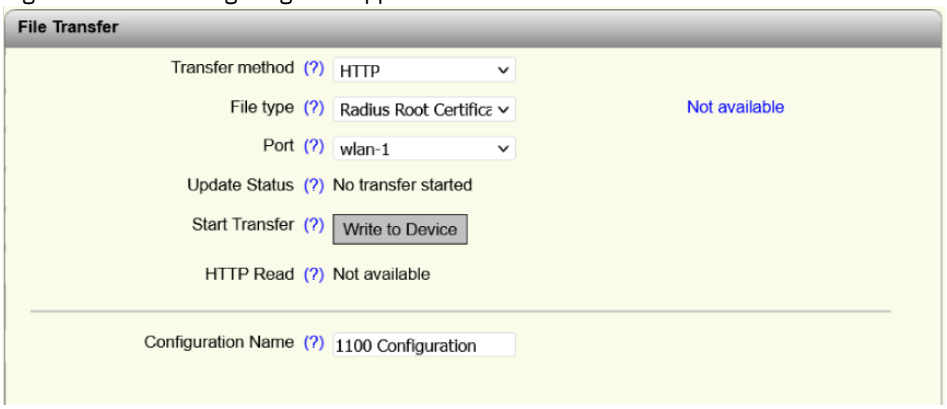
Figure 6-5 Configuring the supplicant: WLAN Interface



- 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 on “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” on page 69.

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 on “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” on page 69).

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.

6.3.3 Deactivating server identity verification

You can deactivate server identity verification. The server identity is then not validated.

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

- Open web-based management on the supplicant (see “Accessing web-based management” on page 23) and log in.
- Click on “Configuration, WLAN Interface”.
- For “Authentication method”, select “PEAP”.
- For “Root CA validation”, select “Disable”.

7 SNMP – Simple Network Management Protocol

7.1 General function

The Simple Network Management Protocol (SNMP) is a manufacturer-independent standard for Ethernet management. It defines commands for reading and writing information and defines formats for error and status messages. SNMP is also a structured model that consists of agents, 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.

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.com/qr/<item_number>.

- Download the current firmware for this.
- Unzip the firmware.
- Navigate to the folder “FL_WLAN_110X_MIBs_[version_and_date].zip”.
- Open the “FL-MGD-INFRASTRUCT-MIB.mi2” file with an editor of your choice.

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

7.2 SNMP interface

All Factoryline components have an SNMP agent. The agent of the device manages the Management Information Base II (MIB 2) in accordance with RFC 1213.

Via the Simple Network Management Protocol, network management stations, such as a PC with the Network Manager, can read and change the configuration and diagnostic data of the network devices. You can use any SNMP tools or network management tools to access Factoryline products via SNMP. To do this, you must make the MIBs supported by the respective device available to the SNMP management tools.

On the one hand, these are globally valid MIBs, which are defined and described in Requests for Comments (RFCs). For example, this includes MIB 2 in accordance with RFC 1213, which is supported by all SNMP-capable network devices. On the other hand, manufacturers can define their own private SNMP objects, which are then assigned to a private manufacturer range in the large SNMP object tree. Manufacturers are responsible for their own private (enterprise) areas. For example, they may assign an object (object name and parameters) to an object ID and publish it only once. If this object is then no longer needed, it is labeled as expired, but it cannot be reused, for example, 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.

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. In the delivery state, 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.

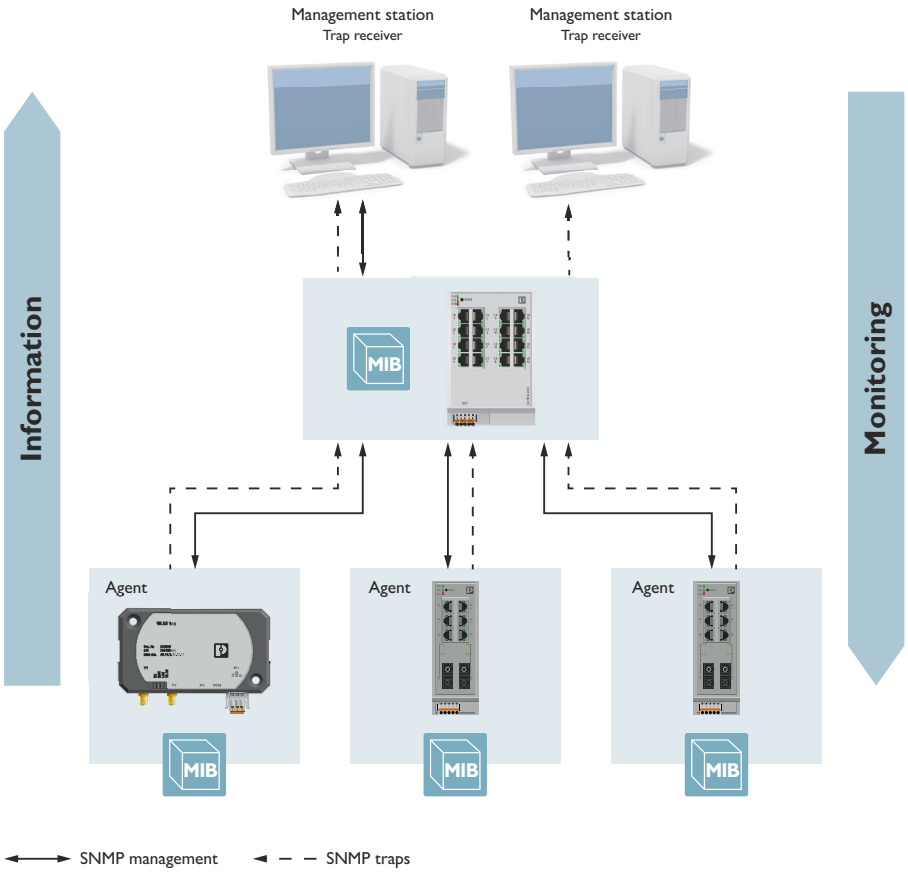
7.2.1 Management Information Base (MIB)

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.

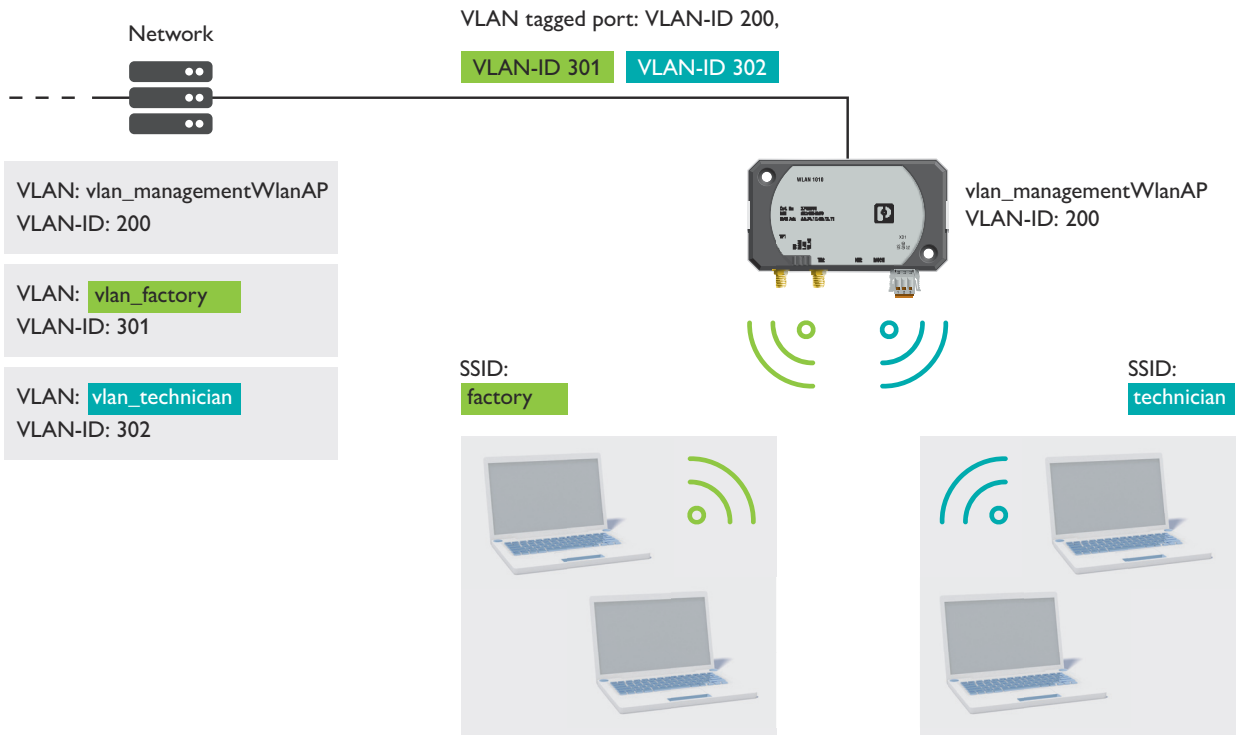
Figure 7-1 Schematic view of SNMP management



8 VLAN – Virtual Local Area Network

8.1 Configuration example

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



In the use case described in Figure 8-1, 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 Figure 8-1:

Once you send 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
```

A Revision history

Revision	Date	Contents
00	2022-02-25	First publication of the firmware manual – Update to firmware version 2.70
01	2022-04-12	– Correction in Section “Syslog for diagnostic purposes” – New graphics in Section “Device operating modes” – Addition in Section “RADIUS certificates”
02	2023-05-17	– Update to firmware version 2.71 – New section: “VLAN – Virtual Local Area Network” – Addition of a number of notes in Section “Accessing web-based management”
03	2025-07-21	– Update to firmware version 3.47 – Changes in section “Delivery state/default settings” – Addition in Section “Accessing web-based management”: Changing the password before first use.

The changes to the firmware can be found in the respective release notes available to download with the firmware in the online shop.

B Appendix for document lists

B 1 List of figures

Section 1

Section 2

Section 3

Section 4

Section 5

Section 6

Section 7

Section 8

Appendix A

Appendix B

B 2 List of tables

Section 1

Section 2

Section 3

Section 4

Section 5

B 3 Index

Numerics

A

B

C

D

E

F

I

L

M

N

O

Q

R

S

T

U

W

Please observe the following notes

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 modifications 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.

Phoenix Contact reserves the right to register its own intellectual property rights for the product identifications of Phoenix Contact products that are used here. Registration of such intellectual property rights by third parties is prohibited.

Other product identifications may be afforded legal protection, even where they may not be indicated as such.

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:
phoenixcontact.com/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

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

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

109065_en_03
Item No. –03