



UM EN FL WLAN 5100

User manual
UM EN FL WLAN 5100

User manual

UM EN FL WLAN 5100

2013-06-05

Designation: UM EN FL WLAN 5100

Revision: 04

Order No.: —

This user manual is valid for:

Designation	Revision	Order No.
FL WLAN 5100		2700718
FL WLAN 5101		2701093

Please observe the following notes

User group of this manual

The use of products described in this manual is oriented exclusively to qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.

Explanation of symbols used and signal words



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety measures that follow this symbol to avoid possible injury or death.

There are three different categories of personal injury that are indicated with a signal word.

DANGER This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.



This symbol together with the signal word **NOTE** and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.



This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

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:

www.phoenixcontact.com

Make sure you always use the latest documentation.

It can be downloaded at:

www.phoenixcontact.net/catalog

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 www.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

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 technical 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 data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed.

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

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

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.

Table of contents

1	Technical description	8
1.1	General description	8
1.2	FL WLAN 510x country registrations	9
1.2.1	FL WLAN 5100	9
1.2.2	FL WLAN 5101	9
1.3	Firmware	12
2	Mounting	13
2.1	Connections and operating elements	13
2.1.1	Electrical connection	14
2.1.2	Mounting	14
3	Startup and configuration	19
3.1	Status and diagnostic indicators	20
3.1.1	Meaning of the LAN1/2 indicators	21
3.1.2	Meaning of the LEDs as signal quality indicators in client mode	21
3.2	Configuration using the MODE button	21
3.2.1	General sequence	22
3.2.2	Changing the firmware image using the MODE button	23
3.2.3	Connection to a PC	24
3.2.4	Assigning the IP address via BootP (with IPAssign)	25
3.2.5	IP address assignment using IPAssign.exe	25
3.2.6	Using the digital input and output	28
3.3	Startup via the web interface	28
3.3.1	General information in the web interface	29
3.4	Quick setup	31
3.4.1	Operation as an access point	34
3.4.2	Operation as a client	36
3.5	SD card for saving the device configuration	40
3.5.1	Inserting the SD card	41
3.5.2	Saving the device configuration	42
3.6	Firmware update.....	43
3.6.1	HTTP	43
3.6.2	TFTP	43
3.6.3	Via SD card	43
3.6.4	Via BootP/TFTP	44
3.7	Operating modes of the device.....	45
3.7.1	Operating mode: access point	45
3.7.2	Operating mode: client	46
3.7.3	Operating mode: repeater	49
3.7.4	Operating mode: machine admin	52

3.8	PROFINET assistance mode.....	54
3.8.1	WLAN in PROFINET applications	54
3.9	Wi-Fi Protected Setup (WPS)	56
3.9.1	Running WPS using the MODE button	56
3.10	Quality of service	56
3.11	Cluster management	57
3.11.1	Searching and selecting cluster devices	57
3.11.2	Identifying cluster-relevant parameters in the web interface	62
3.11.3	Properties of cluster management	63
3.12	Using file transfer.....	63
3.13	DHCP server	64
3.14	Event handling.....	65
3.14.1	Selecting events in web-based management	66
4	Menu/functions	69
4.1	Parameter list for the configuration	70
5	Diagnostics	83
5.1	WLAN signal strength diagnostics on the client.....	83
5.2	Diagnostics of WLAN channel assignment on the access point	85
6	Technical data	87
6.1	Ordering data	89

WLAN 5100 – next generation industrial WLAN

Industrial WLAN network solutions from Phoenix Contact open up new possibilities for creating production and logistics processes more efficiently, reliably, and simply. The fields of application are:

- Reliable, safe and fast communication with mobile or moving automation and production systems.
- Realtime access to network resources and service information for increasing productivity and accelerating decision processes.

The WLAN modules in the 510x series offer maximum reliability, data throughput, and range. The new WLAN 510x combines rugged industrial technology with high 802.11n performance and modern MiMo (multiple input, multiple output) antenna technology in extremely compact metal housing. MiMo technology with three antennas significantly increases the ruggedness, speed, and range of your wireless communication. This is particularly noticeable under challenging industrial conditions.

A special feature of the WLAN 510x modules is their quick and easy configuration. The configuration of a WLAN access point is automatically distributed to all other access points in the WLAN network using the cluster management function. At the touch of a button, WLAN clients can also be integrated easily into the WLAN network without configuration thanks to WPS (Wi-Fi Protected Setup).

1 Technical description



Unless otherwise expressly stated, all information provided in this user manual always applies to both the FL WLAN 5100 and the FL WLAN 5101.

1.1 General description

Compact wireless access point/client with the following properties:

- Operation as a WLAN access point, repeater or client
- Supports WLAN 802.11 standards: a, b, g, n
- Operation in the ISM band at 2.4 GHz frequency or in the 5 GHz band
- IP20 degree of protection
- Connections: COMBICON for supply voltage (10 ... 36 V DC), 2 x RJ45 ports for LAN
- Configuration via WBM, SNMP, and CLI via SSH/Telnet
- Security functions: 802.11i: WPA2, WPA-PSK, TKIP, AES
- Connections for three antennas (MiMo technology/connection method: RSMA/not supplied as standard)



Figure 1-1 FL WLAN AP 5100

1.2 FL WLAN 510x country registrations

1.2.1 FL WLAN 5100

The FL WLAN 5100 is a WLAN device with access point and client functionality. The device uses the WLAN standard in the license-free 2.4 GHz and 5 GHz bands which are free of charge.

The device meets all the requirements of R&TTE directive 1999/5/EC (Europe):

- EMC according to EN 61000-6-2:2005
- Safety according to EN 60950-1:2006+A11
- Health according to EN 50371
- EN 301 893 V1.5.1 (5 GHz), EN 300 328 V1.7.1 (2.4 GHz), EN 301 489-01 V1.8.1, and EN 301 489-17 V2.1.1

Depending on the maximum possible transmission power, device operation must be approved or registered in some countries. Furthermore, there may be a usage restriction on the transmission power.



An up-to-date list of the country registrations can be found in the e-shop at phoenixcontact.com.



Make sure you observe the regulations of the relevant regulatory domain for device operation in all countries.

Approvals for other countries are available on request.

1.2.2 FL WLAN 5101



The FL WLAN 5101 device, Order No. 2701093, does not have CE approval and may not be operated in Europe. It is only available for export.

In addition, the following approvals have been performed and passed for the FL WLAN 5101 device (Order No. 2701093):

- FCC/CFR 47, Part 15 (USA)
- RSS 210 (Canada)

1.2.2.1 FCC information

FCC Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

To comply with FCC part 15 rules in the United States, the system must be professionally installed to ensure compliance with the Part 15 certification. It is the responsibility of the operator and professional installer to ensure that only certified systems are deployed in the United States. The use of the system in any other combination (such as co-located antennas transmitting the same information) is expressly for bidden.

FCC Caution

Any changes or modifications not expressly approved by the party responsible for compliance could void the users authority to operate this equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

For product available in the USA/Canada market, only channel 1~11@2.4GHz can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

If this device is going to be operated in 5.15~5.25GHz frequency range, it is restricted in indoor environment only.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

IC Statement

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B conforme à la norme NMB-003 du Canada.

This device complies with Industry Canada license-exempt RSS standard(s). Operation this subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes: (1) l'appareil ne doit pas produire de brouillage, et (2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

For product available in the USA/Canada market, only channel 1~11 can be operated. Selection of other channels is not possible.

This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Under Industry Canada regulations, this radio transmitter may only operate using an antenna of a type and maximum (or lesser) gain approved for the transmitter by Industry Canada. To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that necessary for successful communication.

This radio transmitter (identify the device by certification number, or model number if Category II) has been approved by Industry Canada to operate with the antenna types listed below with the maximum permissible gain and required antenna impedance for each antenna type indicated. Antenna types not included in this list, having a gain greater than the maximum gain indicated for that type, are strictly prohibited for use with this device.

The device could automatically discontinue transmission in case of absence of information to transmit, or operational failure. Note that this is not intended to prohibit transmission of control or signaling information or the use of repetitive codes where required by the technology.

Dynamic Frequency Selection (DFS) for devices operating in the bands 5250-5350 MHz, 5470-5600 and 5650-5725 MHz.

The maximum antenna gain permitted for devices in the band 5725-5825 MHz shall comply with the e.i.r.p. limits specified for point-to-point and non point-to-point operation as appropriate.

Users should also be advised that high-powers radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

IMPORTANT NOTE:

IC Radiation Exposure Statement:

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between radiator & your body.

This module is intended for OEM integrator. The OEM integrator is still responsible for the IC compliance requirement of the product, which integrates this module.

20cm minimum distance has to be able to be maintained between the antenna and the users for the host this module is integrated into. Under such configuration, the IC RSS-102 radiation exposure limits set forth for a population/uncontrolled environment can be satisfied.

Any changes or modifications not expressly approved by the manufacturer could void the users authority to operate this equipment.

1.3 Firmware

Table 1-1

Firmware version	Functionality
FW 1.60	The "machine admin mode" (second SSID) and DHCP server functions are available as of this FW version.

2 Mounting

2.1 Connections and operating elements

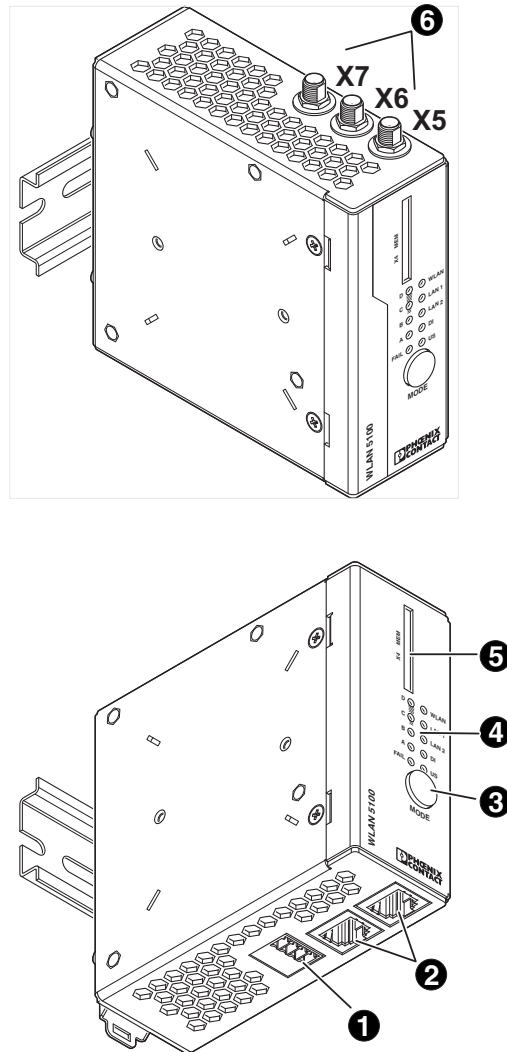


Figure 2-1 Connections and operating elements of the device

1. COMBICON connections for supply voltage and one digital input or output (X3)
2. Two RJ45 Ethernet connections with 100 Mbps (X1, X2)
3. Mode button for setting various pre-configured states
4. Status and diagnostic LEDs
5. Slot for optional SD memory card (X4)
6. RSMA antenna connections (female) (X5, X6, X7)

2.1.1 Electrical connection

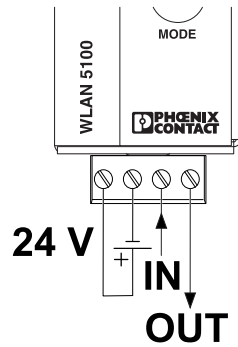


Figure 2-2 Connecting the supply voltage and the input/output

2.1.2 Mounting



When using remote antennas, always keep the antenna cable as short as possible to avoid an attenuation of the wireless signal.



Preferably use the mounting position illustrated in the following graphic.

2.1.2.1 DIN rail mounting

Use the DIN rail guide to position the module onto the upper edge of the DIN rail, and snap the module into place by pushing it downward.

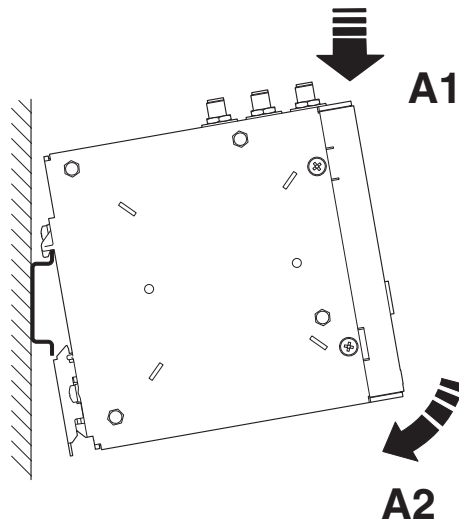


Figure 2-3 Snapping the module onto the DIN rail

2.1.2.2 Removal

Insert a suitable tool (e.g., flat-bladed screwdriver) into the latch and pull the latch downward (B1).

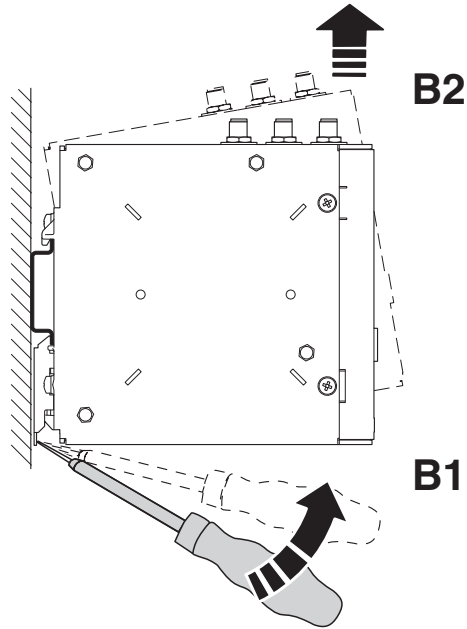


Figure 2-4 Removing the module from the DIN rail

2.1.2.3 Housing dimensions

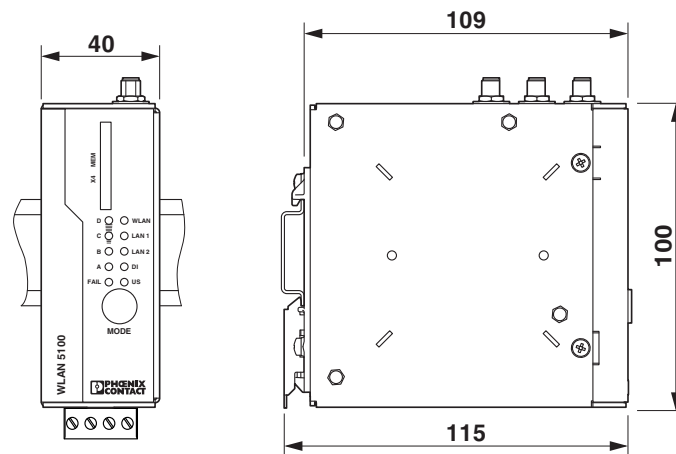


Figure 2-5 Housing dimensions with protruding parts in mm

2.1.2.4 Wall mounting



Preferably use the mounting position illustrated in the following graphic.

The FL WLAN 5100 PA mounting kit (Order No. 2701092) can be used to mount the device on a wall.

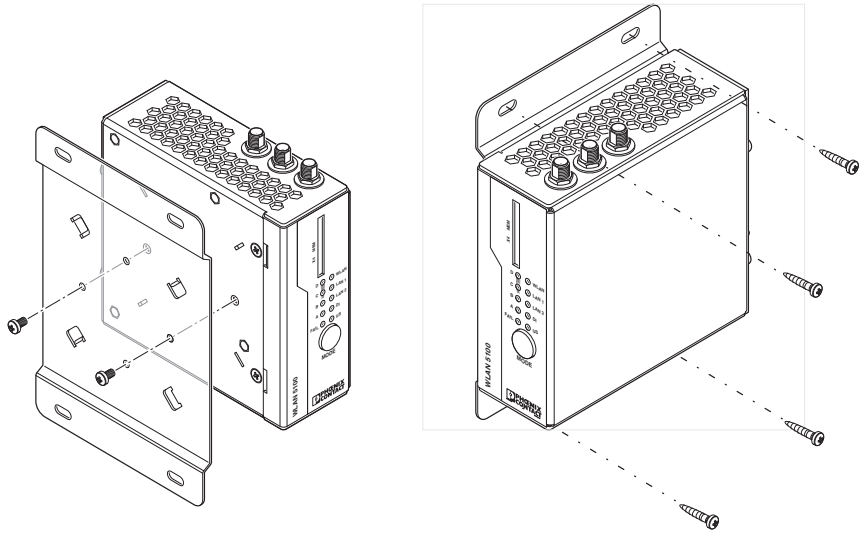


Figure 2-6 Securing the mounting kit

Use the two screws provided to secure the device to the base plate.
The two 4.5 mm bore holes can be used for mounting.

2.1.2.5 Dimensions of the mounting kit and drill hole template

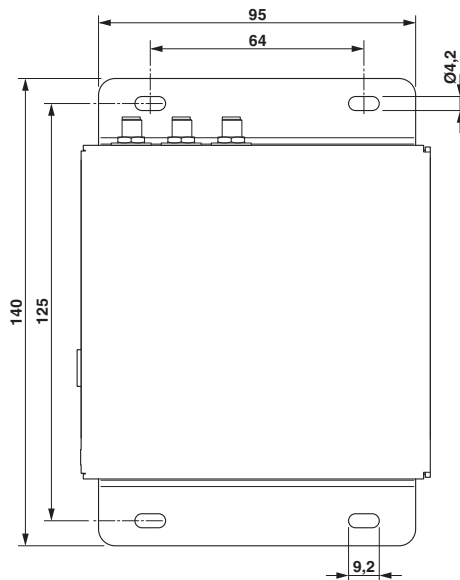


Figure 2-7 Dimensions of the mounting kit and drill hole template in mm

2.1.2.6 Mounting in the IP65 housing

Phoenix Contact offers an IP65 housing (FL RUGGED BOX OMNI-1) specifically for use in conjunction with the FL WLAN 510x. Three omnidirectional antennas (dual band, 2.4 GHz, and 5 GHz) are supplied as standard with the housing. They are screwed directly onto the housing. Also included are three antenna connecting cables, the necessary DIN rail (144 mm), plus cable feed-throughs. The WLAN access point is not supplied as standard.

Housing dimensions of FL RUGGED BOX OMNI-1

Width: 180 mm

Height: 250 mm

Depth: 140 mm



Figure 2-8 IP65 protective housing with antennas and cable feed-throughs

Additional rugged box versions can be found at phoenixcontact.com:

FL RUGGED BOX, Order No. 2701204

FL RUGGED BOX OMNI-2, Order No. 2701439

FL RUGGED BOX DIR-1, Order No. 2701440

2.1.2.7 Antenna mounting distances

The WLAN 510x supports the MIMO (multiple input multiple output) antenna technology. Up to three antennas are used which are connected to connections X5, X6, X7. The antennas should be connected via an antenna cable outside the control cabinet, so they can radiate

well into the area. This means that the radiating element of the antenna should not be located too close to conductive objects, if possible. Keep a distance of more than 200 mm, if possible. Smaller distances are possible, however, they may affect radiation.

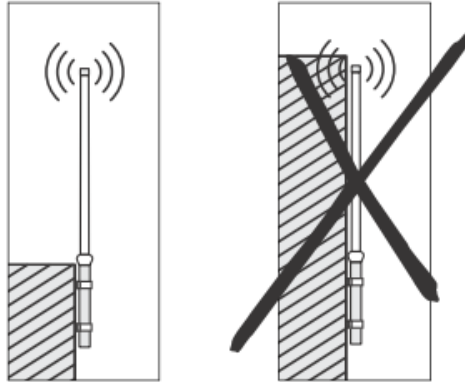


Figure 2-9 Correct and wrong antenna mounting using an omnidirectional antenna as an example

Distance of the antennas from one another

The distance between the three antennas of a device must at least be 80 mm each to ensure decoupling of the data streams that are transmitted in parallel (MIMO technology). If larger distances of approximately 200 mm to 500 mm between the antennas are mechanically feasible, this may lead to further improvement.

For the same reason, antennas should not be screwed directly onto the device.



Figure 2-10 Do not screw several antennas onto the device.

3 Startup and configuration

Installation notes

The category 3 device is designed for installation in the potentially explosive area of zone 2. It meets the requirements of EN 60079-0:2009 and EN 60079-15:2010.

Installation, operation, and servicing may only be carried out by qualified electricians. Follow the installation instructions as described. When installing and operating the device, the applicable regulations and safety directives (including national safety directives), as well as general technical regulations, must be observed. The safety data is provided in this user manual and on the certificates (conformity assessment, additional approvals where applicable).

Do not open or modify the device. Do not repair the device yourself but replace it with an equivalent device. Repairs may only be performed by the manufacturer. The manufacturer is not liable for harm resulting from noncompliance.

The IP20 degree of protection (IEC 60529/EN 60529) of the device is intended for use in a clean and dry environment. Do not subject the device to mechanical and/or thermal loads that exceed the specified limits.

The device is not suitable for installation in zone 22.

If, however, you wish to use the device in zone 22, it must be installed in a housing that complies with EN 60079-0. In doing so, observe the maximum surface temperatures. Adhere to the requirements of EN 60079-14.

Installation in zone 2

Observe the specified conditions for use in potentially explosive areas! When installing the device, use an appropriate and approved housing with a minimum protection of IP54. At the same time, observe EN 60079-14 requirements.

Only devices which are designed for operation in zone 2 and are suitable for the conditions at the installation location may be connected to the supply and signal circuits in zone 2.

In potentially explosive areas, only connect and disconnect cables when the power is disconnected.

You must only work on the device if it has been ensured that there is no explosive environment.

The device must be stopped and immediately removed from the Ex area if it is damaged, was subjected to an impermissible load, stored incorrectly or if it malfunctions.

In addition for FL WLAN 5100:

Ensure that the radiated wireless power is neither bundled (focused) by the antenna itself nor by any inserts in the environment of the antenna, and that it cannot enter neighboring zones 1 or 0. Please refer to the technical data for the transmission power.

Application note:

The HF antenna cable must be suitable for the ambient conditions and should be installed in a way that it is protected against mechanical damage, corrosion, chemical stress, and the effects of heat or UV radiation. The same applies to the antenna which is connected to the cable and which functions as a cable termination.

The antenna must meet the requirements of EN 60079-0 with regard to housing and electrostatic discharge.



NOTE:

The device must only ever be operated when an antenna is present at the activated antenna connection. The antenna connections can be deactivated under “Advanced WLAN” in the web interface.



Do not screw more than one omnidirectional antenna onto the device. The distance of the antenna connectors has been optimized for installation in control cabinets and the use of antenna cables. To ensure decoupling the distance between the antennas should be at least 80 mm. A larger distance may improve the performance of the device.

This section describes a typical startup of the WLAN device as an access point or client using the “Quick Setup” feature. A standard WLAN network can be established in this way. For special applications and configuration, further details can be found in “Menu/functions” on page 69.

3.1 Status and diagnostic indicators

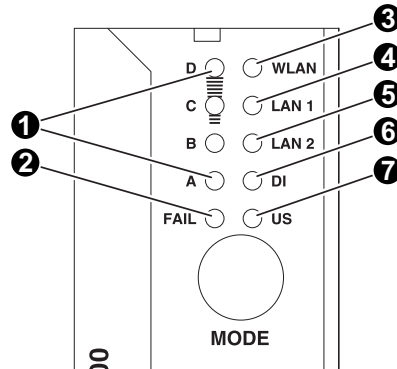


Figure 3-1 Status and diagnostic indicators

1. LEDs A, B, C, and D indicate the relevant state of the device while it is being configured using the MODE button. For details, see the sticker on the side of the device or “Configuration using the MODE button” on page 21.
In WLAN operation as a client, the LEDs indicate the signal strength of the connected device (see “Meaning of the LEDs as signal quality indicators in client mode” on page 21).
2. Fail:
Lights up red if no configuration has been received in WPS mode, the link quality LEDs also flash yellow.
3. WLAN status:
WLAN connection established (blue)
Whether data transmission occurs depends on whether the passwords and certificates are valid. A WLAN connection can therefore exist even if data cannot be transmitted. If WLAN authentication fails, this is indicated in the log file.
Half duplex data transmission: blue; if flashing, data transmission is active

Connection establishment (purple): only in client mode during a scan/connection establishment or when a channel is selected automatically in access point mode
 Green LED: if the WLAN interface is in idle mode (e.g., between scans in client mode or when the radar check is performed at 5 GHz in access point mode)

4. LAN1 status: green/yellow (see “Meaning of the LAN1/2 indicators” on page 21)
5. LAN2 status: green/yellow (see “Meaning of the LAN1/2 indicators” on page 21)
6. DI: digital input set at connector X3 (see “Using the digital input and output” on page 28)
7. US: supply voltage present

3.1.1 Meaning of the LAN1/2 indicators

Table 3-1 Meaning of the LAN1/2 indicators

Des.	Color	Status	Meaning
LAN 1		OFF	No Ethernet connection at port 1
	Green	ON	Ethernet connection in full duplex mode
		Flashing	Ethernet communication in full duplex mode
	Yellow	ON	Ethernet connection in half duplex mode
Flashing		Ethernet communication in half duplex mode	
LAN 2		OFF	No Ethernet connection at port 2
	Green	ON	Ethernet connection in full duplex mode
		Flashing	Ethernet communication in full duplex mode
	Yellow	ON	Ethernet connection in half duplex mode
Flashing		Ethernet communication in half duplex mode	

3.1.2 Meaning of the LEDs as signal quality indicators in client mode

Table 3-2 Meaning of LEDs A to D in client mode

LED	Meaning
OFF	No WLAN connection
A	Poor link quality
A+B	Good link quality
A+B+C	Optimum link quality
A+B+C+D	Excellent link quality

3.2 Configuration using the MODE button

Typical operating settings for the FL WLAN 510x can be set using the MODE button on the front of the device. The possible settings can be found in table “Operating modes” on page 22. A selection of the key settings is also available directly on the device.

3.2.1 General sequence

- Connect the device to the power supply.
- The device is started, and the status can be tracked by observing the yellow LEDs “A B C D”: the boot process is completed when the last LED “D” goes out. You then have 5 seconds to switch the device to configuration mode via the MODE button.
- Push the MODE button for about 1 second in order to switch the device to configuration mode. The yellow flashing LED A indicates that the device is in configuration mode.



If the MODE button is not pressed for an extended period in active configuration mode, configuration mode is exited automatically after 5 minutes and the device is started with its previous settings.

- Select the desired operating mode by pressing the MODE button until the corresponding LED combination lights up. Once you have scrolled through all the LED combinations (operating modes), the selection automatically starts again from the beginning.
- After selecting the desired operating mode, exit the configuration by pressing the MODE button (for about 1 second) until the four LEDs light up. The mode is set, and the device starts up with the corresponding settings.

During configuration with the MODE button, not all parameters are rewritten, only those necessary for the operating mode. Some settings can therefore be made beforehand via the web interface or via SNMP and will still be effective after configuration with the MODE button.

If the module has been previously configured, we recommend restoring the device's default settings before configuring the device via the MODE button. This action is also performed via the MODE button. This ensures that the initial configuration is recognized.

Table 3-3 Operating modes

Mode	Description	LEDs	A	B	C	D
1	Exit configuration mode without modifying the configuration.	A	●			
2	Restoring default settings (factory defaults)	B		●		
3	PROFINET assistance mode: allows DCP (Discovery Control Protocol) to be used in PROFINET environments. PROFINET data is transmitted with top priority (see “PROFINET assistance mode” on page 54).	A+B	●	●		
6	Static IP (temporary DHCP server): as a DHCP server, the device assigns an IP address to a device connected via the Ethernet network. An address is assigned only once in order to easily supply a single device with an IP address (e.g., a PC that is connected for configuration purposes). In this mode, the device can be accessed under IP 192.168.0.254.	B+C		●	●	

Table 3-3 Operating modes [...]

Mode	Description	LEDs	A	B	C	D
7	Restoring IP setting to default setting (BootP request through to assigning an IP address). The other settings specifically made on the device are retained.	A+B+C	●	●	●	
8	Restoring the device to the basic settings specified by the user.	D				●
9	WPS client	A+D	●			●

3.2.2 Changing the firmware image using the MODE button



NOTE:

By default, there is only one firmware image on the device. If, however, the switchover procedure described here is carried out, the device will no longer start as there is no firmware image present. This can be seen when the four link quality LEDs do not go out one after the other.

In this case, the switchover procedure must be repeated again so that the device is started with the original firmware image.

For information on how to load a second firmware image, please refer to “Firmware update” on page 43.

The device can accommodate two complete firmware versions (dual image). You can switch between these two versions. To do this, proceed as follows:

- Switch off the power supply.
- Press and hold down the MODE button.
- Switch on the power supply.
- Release the MODE button within five seconds once the link quality LEDs (A+B+C+D) have started to flash yellow.

The device now switches the firmware image and reboots.

3.2.3 Connection to a PC

Proceed as follows to connect the WLAN 510x to your PC via the Ethernet interface without using BootP (default setting):

- Connect the device to a power supply.
- Press the mode button right after the booting (LED A - D off) until LED A flashes.
- Press the MODE button briefly several times to select mode "BC" (LED).
- Confirm the mode by pressing the MODE button longer (> 2 sec).
- The temporary DHCP server automatically assigns an IP address to the configuration PC. The FL WLAN 510x receives the IP address 192.168.0.254.

3.2.4 Assigning the IP address via BootP (with IPAssign)

This section explains IP address assignment using the “IP Assignment Tool” Windows software (IPAssign.exe). This software can be downloaded free or charge at phoenixcontact.net/catalog. The tool can also be found under “Help & Documentation” on the web page for the device, where it can be started directly.

Notes for BootP

During initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. As soon as it receives a valid IP address, the device stops sending BootP requests.

After receiving a BootP reply, the device no longer sends BootP requests. Following a restart, a device that was previously configured sends three BootP requests; if these requests are not answered, the device starts with the IP address that was last assigned via BootP. After the default settings are restored, the device sends BootP requests until they are answered.

Requirements

The device is connected to a computer using a Microsoft Windows operating system.

3.2.5 IP address assignment using IPAssign.exe

Step 1: downloading and executing the program

You can either load the tool from the Internet or from the device itself.

From the Internet:

- On the Internet, select the link phoenixcontact.net/products.
- Enter the order number 2701094 or IPASSIGN in the search field, for example.

The BootP IP addressing tool can be found under “Configuration file”.

- Double-click on the “IPAssign.exe” file.
- In the window that opens, click on “Run”.

From the device:

- Set the device to mode 6 using the MODE button (see “Configuration using the MODE button” on page 21).
- Using a browser, go to IP address 192.168.0.254. In web-based management, you can start the program by double-clicking on it under “Help & Documentation”.

Step 2: “IP Assignment Wizard”



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

The program opens and the start screen of the addressing tool appears.

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

The start screen displays the IP address of the PC. This helps when addressing the device in the following steps.

- Click on “Next”.

Step 3: “IP Address Request Listener”

All devices sending a BootP request are listed in the window which opens. These devices are waiting for a new IP address.

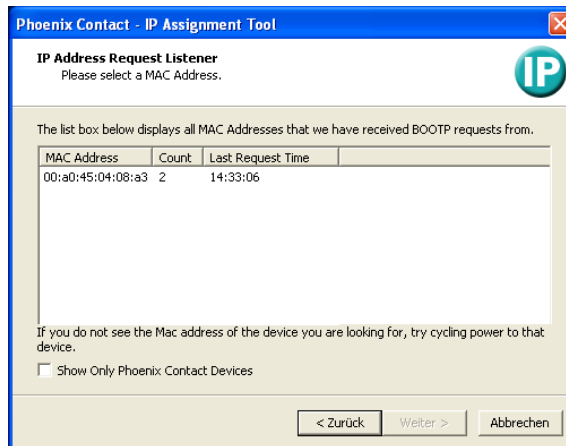


Figure 3-2 “IP Address Request Listener” window

In this example, the device has MAC ID 00.A0.45.04.08.A3.

- Select the device to which you would like to assign an IP address.
- Click on “Next”.

Step 4: “Set IP Address”

The following information is displayed in the window which opens:

- IP address of the PC
- MAC address of the selected device
- IP parameters of the selected device (IP address, subnet mask, and gateway address)
- Any incorrect settings

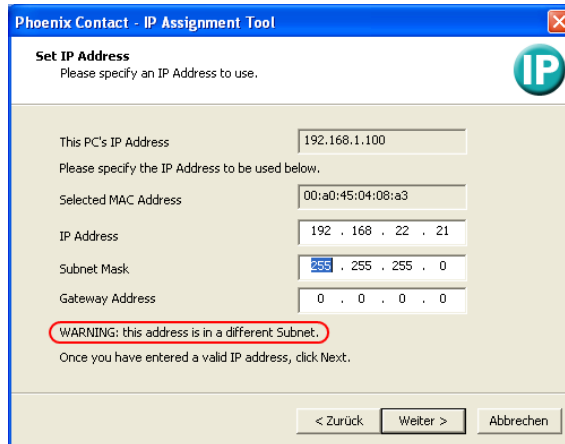


Figure 3-3 "Set IP Address" window with incorrect settings

- Adjust the IP parameters according to your requirements.

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

- Click on "Next" and perform a voltage reset.

Step 5: "Assign IP Address"

The program attempts to transmit the IP parameters set to the device.

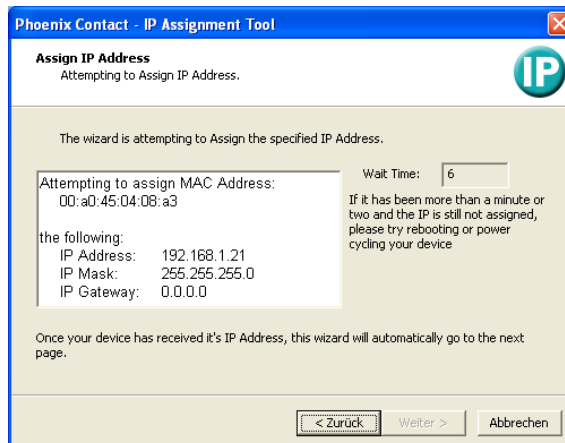


Figure 3-4 "Assign IP Address" window

Following successful transmission, the next window opens.

Step 6: finishing IP address assignment

The window that opens informs you that IP address assignment has been successfully completed. It gives an overview of the IP parameters that have been transmitted to the device with the MAC address shown.

To assign IP parameters for additional devices:

- Click on "Back".

To exit IP address assignment:

- Click on “Finish”.

3.2.6 Using the digital input and output

The functions of the input/output are generally available or need to be activated by the user by means of configuration. The following table shows the possible options.



Please note that the majority of functions that relate to the digital input can be activated simultaneously.

If you activate the “Show status of WLAN interface” function for the digital output, the “Status change via SNMP” and “Status change via WBM” functions will be deactivated automatically.

The “Show status of WLAN interface” function sets the output to “ON” if a WLAN link is present.

Table 3-4 Function of the digital inputs/outputs

Function	Digital input	Digital output
Status request via SNMP	Yes, always	Yes, always
Status change via SNMP		Yes, via configuration
Status request via WBM	Yes, always	Yes, always
Status change via WBM		Yes, via configuration
Send SNMP trap when input is set	Yes, via configuration	
Trigger WLAN roaming	Yes, via configuration	
Switch WLAN interface on/off	Yes, via configuration	
Show status of WLAN interface		Yes, via configuration

3.3 Startup via the web interface



WBM of the device is optimized for Internet Explorer 8.0 or later

3.3.1 General information in the web interface

3.3.1.1 Web interface icons

There are a few icons at the top of the web page (marked in red in the graphic below), which provide an overview of important device functions.



Figure 3-5 Web page with overview icons

Meaning of the individual icons:

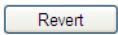
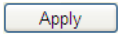
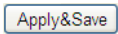
Table 3-5 Meaning of the icons

Icon	Meaning
	The WLAN interface is deactivated.
	The device is in "Client" mode and there is no WLAN connection to an access point at present.
	The device is in "Client" mode and connected to an access point. The bars indicate the signal strength of the access point for reception. One bar: poor link quality Two bars: good link quality Three bars: optimum link quality Four bars: excellent link quality
	The device is in "Access Point" mode and connected to a number of clients. The number of connected clients is displayed. If "0" is displayed, there is no connection to a client.
	Connection status: connected Indicates whether the PC with the browser has an active connection to the device.
	Connection status: disconnected During a configuration change or in the event that a configuration change has been made via WLAN and the connection has been disabled.
	An administrator is logged into the device. The icon also acts as the logout button.
	An administrator is not logged in at present. The icon also acts as the login button.
	The active configuration differs from the saved configuration for the device. To save the active configuration, simply click on the icon.

Web interface buttons

Meaning of the individual buttons:

Table 3-6 Meaning of the buttons

Icon	Meaning
	This button deletes the entries made since the last saved entry
	This button applies the current settings, but does not save them
	This button applies and saves the current settings

3.4 Quick setup

The “Quick Setup” feature on the web page allows you to quickly configure the minimum requirements of a WLAN network. The procedure is described below.

Establishing a connection to the device

- Connect the device to the supply voltage and connect it to the PC via an Ethernet cable.
- Set the device to mode 6 using the MODE button (see “Configuration using the MODE button” on page 21). As a DHCP server, the device assigns an IP address to the PC connected via the Ethernet network. Make sure that your PC is ready for IP assignment using DHCP.
- Using a browser, go to IP address 192.168.0.254. In web-based management, select “Quick Setup”.
- Login: enter “admin” as the username and “private” as the password.

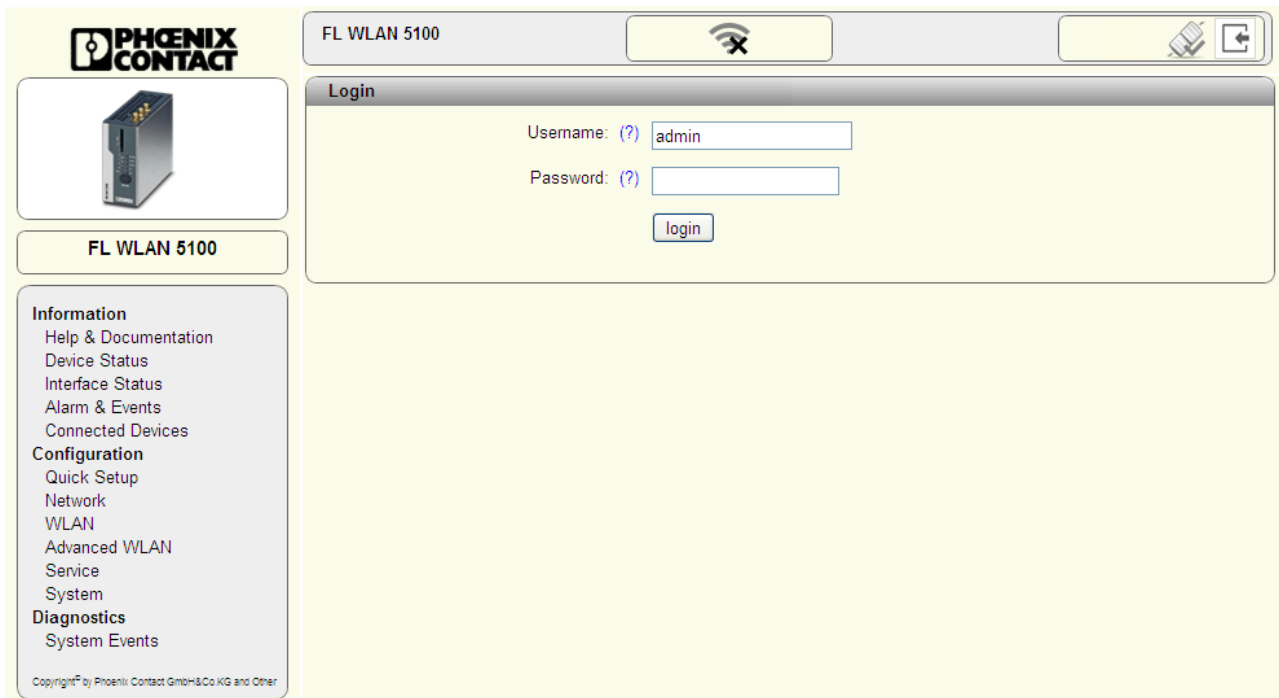


Figure 3-6 “Login” web page

On the web page, you can set all the necessary configurations for a standard WLAN network.

Language selection

First, select the language for user management, the web page interface. The help text displayed when you move the mouse cursor over the (?) is shown in the selected language.

IP address assignment

Static: The static IP address, subnet mask, and gateway address can be set here.

BootP: during initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. As soon as it receives a valid IP address, the device stops sending BootP requests.

After receiving a BootP reply, the device no longer sends BootP requests. Following a restart, a device that was previously configured sends three BootP requests; if these requests are not answered, the device starts with the IP address that was last assigned via BootP. After the default settings are restored, the device sends BootP requests until they are answered.

DHCP: dynamic request for an IP address from a DHCP (Dynamic Host Configuration Protocol) server.

Country setting

Under “Country”, select the country in which the device is operated. By selecting the country, regulatory features in terms of the frequency usage of the device are automatically taken into consideration.



The settings primarily affect the device when it is used in the 5 GHz WLAN band. A wireless license is not necessarily available for each country that can be selected here.

Operating mode

Under “Operating Mode”, you can define whether the device assumes the function of an access point or a client in the network.

The screenshot displays the 'Quick Setup' web page for the FL WLAN 5100 device. The page is divided into a left sidebar and a main configuration area. The sidebar contains a navigation menu with sections: Information (Help & Documentation, Device Status, Interface Status, Alarm & Events, Connected Devices), Configuration (Quick Setup, Network, WLAN, Advanced WLAN, Cluster Configuration, Service, System, Local Events, Network Events), and Diagnostics (Channel Allocation). The main configuration area is titled 'Quick Setup' and contains the following fields:

- Web management language (?): English (dropdown)
- IP Address Assignment (?): static (dropdown)
- IP Address (?): 192.168.0.254 (text input)
- Subnet Address (?): 255.255.255.0 (text input)
- Gateway Address (?): 0.0.0.0 (text input)
- Country (Regulatory Domain)* (?): Germany (dropdown)
- Operating Mode (?): Accesspoint (dropdown)
- Network SSID* (?): PxC (text input)
- WLAN Band (?): 2.4GHz(802.11 b/g/n) (dropdown)
- Channel (?): Channel7 - 2.442GHz (dropdown)
- WLAN Security* (?): WPA2-PSK (AES) (dropdown)
- Passkey* (?): [masked] (text input) with a checkbox for 'Show cleartext passphrase'
- Administrator Password* (?): [masked] (text input)
- Retype Password* (?): [masked] (text input)

At the bottom right of the configuration area, there are three buttons: 'Revert', 'Apply', and 'Apply&Save'.

Figure 3-7 “Quick Setup” web page

3.4.1 Operation as an access point

In access point mode, the WLAN 510x forms the wireless interface in the overall network for one or more WLAN clients.

Network SSID

The network SSID is used to identify the network to which the WLAN clients connect wirelessly. The name entered here for an access point enables all WLAN clients with the same SSID to connect to the access point using the correct encryption.

The network name can be up to 32 characters long. Letters, numbers, and the following characters are permitted: \$%&/()=?[]{}+*-_<>

WLAN Band

The wireless frequency at which the WLAN network is operated is specified at the access point. Under "WLAN Band", first select whether your network should be operated in the 2.4 GHz band or in the 5 GHz band. In doing so, observe any company specifications for frequency planning.

Channel

2.4 GHz band

Where possible, you should select a free frequency or observe any specifications relating to the company premises. Channels 1, 6, and 11 are typically used in order to avoid interference between devices caused by channel overlap.

5 GHz band

Operation inside buildings:

Indoor Ch36...Ch48: in this area, one of the four channels can be freely selected and is available without any interruptions.

Indoor 8 channels automatically/indoor 16 channels automatically:

The system automatically selects the channels (Dynamic Frequency Selection, DFS). In doing so, the connection may be interrupted during a channel switchover or in the event of radar detection.

Operation outdoors:

If your application is located outdoors, the checkmark must be deselected from "Indoor".

In "Outdoor" mode, the wireless channel is automatically selected in the system (Dynamic Frequency Selection, DFS). In doing so, the connection may be interrupted for at least one minute during a channel switchover.



NOTE: This operating mode is prescribed by law within the EU for outdoor operation and must be used.

Encryption

WLAN Security:

WPA2-PSK (AES) offers the highest security standard in encryption.

WPA2-EAP (for use in enterprise/IT environments with central authentication) can be defined in the “WLAN” menu. WPA-PSK (TKIP) is available as an alternative. Other encryption options are available in the “WLAN” menu or via the CLI interface.

We strongly recommend using secure encryption in order to protect your network against unauthorized access. Where possible, use WPA2 with AES.



NOTE: If you select WPA-TKIP, rather than high data rates, WLAN standard 802.11n prescribes the use of 54 Mbps, maximum.



In order to reach full data throughput under WLAN 802.11n, WPA2-PSK (AES) encryption must be used.

Passkey

Enter a key which will be used by the device during the initialization of WPA encryption.

Note: for maximum security, a random alphanumeric string (up to 63 characters) should be used. Letters, numbers, and the following characters are permitted: \$%&@&/()=?[]{}+*_-<>. The password must contain at least eight characters.

Administrator Password

The password for accessing the web interface is changed under “Administrator Password” and confirmed under “Retype Password”. The change of password is applied when you log out and log back in again.

The change is only applied when you click on “Apply”. To permanently save the change beyond a device restart, click on “Apply&Save”.



We strongly recommend that you change the administrator password the first time you use the device in order to avoid unauthorized access to the web interface.

3.4.2 Operation as a client

In client (FTB) mode, the device forms the wireless interface of a distributed device. One or more WLAN clients can be connected to a WLAN access point.

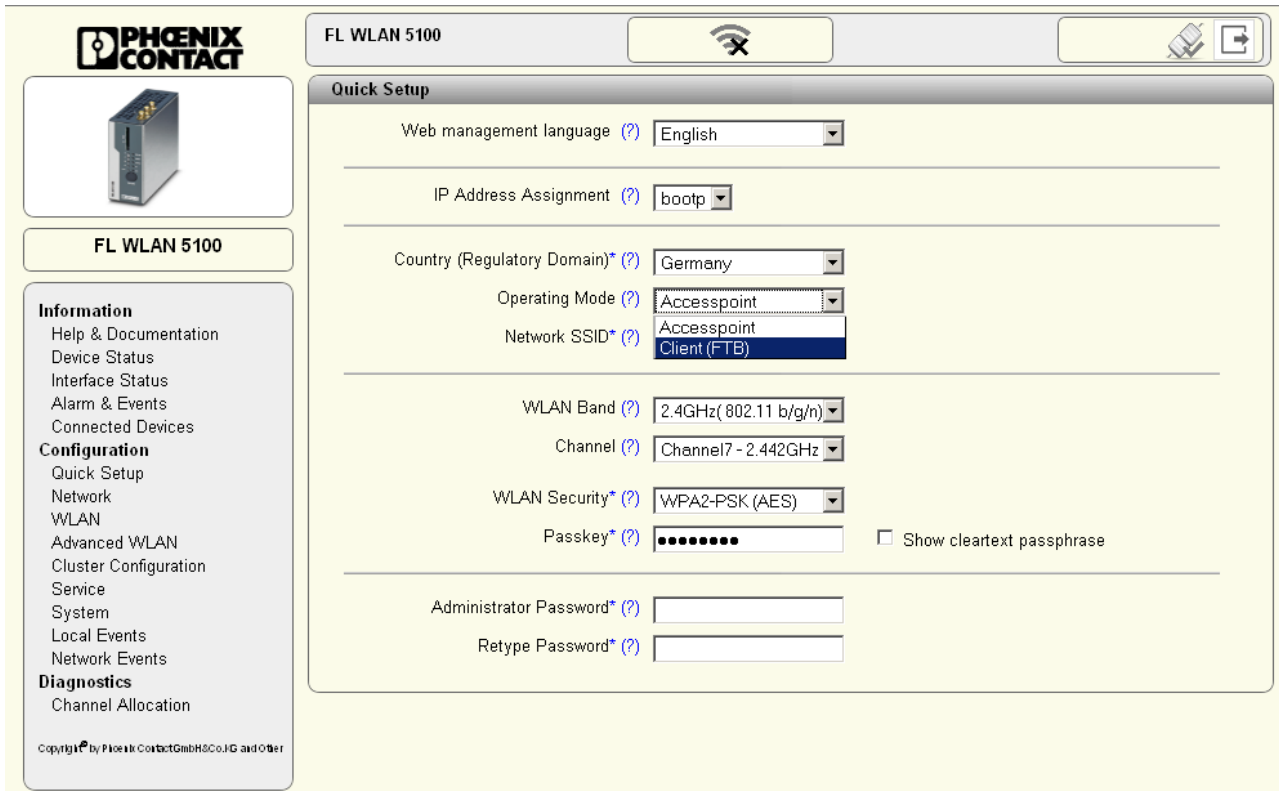


Figure 3-8 Device configuration as a client



“Client (FTB)” mode is recommended when using another FL WLAN 510x as an access point. Other client modes are described in “Operating modes of the device” on page 45.

Confirm your selection with “Apply” or “Apply&Save”.



The WLAN wireless interface is activated automatically by clicking on “Apply” in the “Quick Setup” menu. It is deactivated by default.

The screenshot shows the 'Quick Setup' web page for a Phoenix Contact FL WLAN 5100 device. The page is titled 'FL WLAN 5100' and features a navigation menu on the left with sections for Information, Configuration, and Diagnostics. The main content area is titled 'Quick Setup' and contains the following fields and options:

- Web management language (?): English
- IP Address Assignment (?): bootp
- Country (Regulatory Domain) (?): Germany
- Operating Mode (?): Client (FTB) Indoor
- Network SSID (?): PxC
- WLAN Security (?): WPA2-PSK (AES)
- Passkey (?): [masked] Show cleartext passphrase
- Administrator Password (?): [empty field]
- Retype Password (?): [empty field]

At the bottom right of the 'Quick Setup' section, there are three buttons: 'Revert', 'Apply', and 'Apply&Save'.

Figure 3-9 “Quick Setup” web page after selecting client mode

Network SSID

The network SSID is used to identify the network to which the WLAN clients connect wirelessly. The name entered here allows the WLAN client to search for an access point with the same SSID. When using the correct encryption, a connection can be established with the access point.



In order to reach full data throughput under WLAN 802.11n, WPA2-PSK (AES) encryption must be used.

The network name can be up to 32 characters long. Letters, numbers, and the following characters are permitted: \$%&/()=?[]{}+*-_<>

If the SSID of the access point with which the wireless connection is to be established is known, it can be entered in the “Network SSID” field.

“Scan” button

An alternative to typing in the SSID, is to click on the “Scan” button and search for WLAN access points that can be reached. Please note that any existing connections will be interrupted during scanning. All frequencies that can be used in the 2.4 GHz and 5 GHz band (see “Indoor” checkbox) are scanned for access points.

Scan for Access Points					
Network Name (SSID)	MAC Address	Security	Channel	Signal	Adopt
PxC-Guest	00:11:88:A0:DD:F1	none	36		Adopt
Stefan	00:A0:45:37:25:10	none	6		Adopt
PxC-Guest	00:11:88:A0:DD:F9	none	1		Adopt
PxC	00:A0:45:EE:EE:02	WPA2 PSK	7		Adopt
PxC-User	00:11:88:5A:E6:18	WPA2/Radius	5		Adopt
PxC	00:A0:45:37:1F:CC	WPA2 PSK	4		Adopt

⊕ Rescan

Figure 3-10 Display of WLAN access points received by the client

A list of the WLAN access points found is displayed in a separate window. The SSID for setting the client can be applied by clicking on “Adopt”. The key must be known and entered as described below.

“Indoor” checkbox

When set, the “Indoor” checkbox means that the outdoor frequencies of the 5 GHz band are not scanned. This significantly reduces the scan time.

For regulatory reasons, not all frequencies in the 5 GHz band may be used outdoors. If your WLAN application is located outdoors and is operated in the 5 GHz band, uncheck the “Indoor” checkbox.



Specific operating modes are prescribed by law for the 5 GHz frequency range in the case of outdoor operation. Please make sure that the correct country settings are also used on the WLAN access point side.

Encryption

WLAN Security:

WPA2-PSK (AES) offers the highest security standard in encryption. WPA-PSK (TKIP) is available as an alternative. Other encryption options are available in the “WLAN” menu.

We strongly recommend using secure encryption in order to protect your network against unauthorized access.



In order to reach full data throughput under WLAN 802.11n, WPA2-PSK (AES) encryption must be used.

Passkey

Enter a key which will be used by the device during the initialization of WPA encryption.

Note: for maximum security, a random alphanumeric string (up to 63 characters) should be used. Letters, numbers, and the following characters are permitted: \$%&@&/()=?[]{}+*_-<>.

After clicking on “Apply”, the client automatically establishes a connection to the access point.

If this does not happen, check that the entries for the SSID, network security, and passkey match those of the access point. If the security of the installation permits it, a test run without using encryption can simplify startup. However, during operation secure encryption should be activated.

Administrator Password

The password for accessing the web interface is changed under “Administrator Password” and confirmed under “Retype Password”.

The change is only applied when you click on “Apply”. To permanently save the change beyond a device restart, click on “Apply&Save”.



We strongly recommend that you change the administrator password the first time you use the device in order to avoid unauthorized access to the web interface.

3.5 SD card for saving the device configuration

The FL WLAN 510x uses an SD card as an external storage medium. The SD card can be used to back up the device configuration and to transfer the configuration to other devices.



Only SD cards from Phoenix Contact can be used (see “Ordering data” on page 89). Do **not** delete the existing license key on SD cards from Phoenix Contact.

The device can be operated with or without an SD card. The SD card must have a minimum memory capacity of 256 Mbyte. The SD cards can be read and written by a PC. Additional data/project data which is not needed or used by the device can also be archived on the SD card.

After you have saved the configuration, the SD card has the following structure:

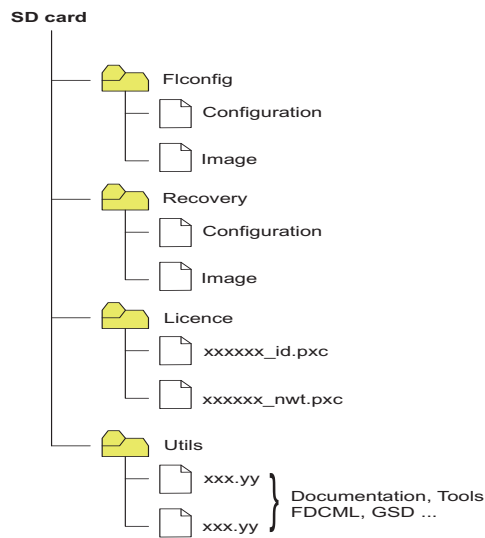


Figure 3-11 Structure on the SD card

3.5.1 Inserting the SD card

Insert the card into the device as shown in the figure below until it engages with a click.



NOTE: If an SD card with a configuration file is inserted when the device is booted, this configuration (including the firmware version) is applied and the previous configuration is overwritten in the internal memory.



NOTE: If an SD card without firmware image is detected during a boot process or a firmware update was carried out prior to booting, the boot process will take longer as the firmware has to be copied from the device to the SD card first. Do not remove the SD card until the last "boot LED" has gone out.

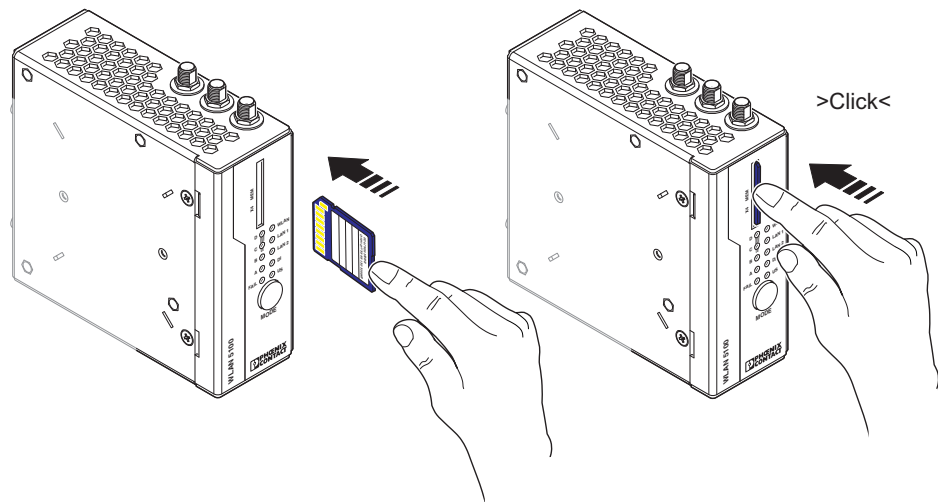


Figure 3-12 Inserting the SD card

The configuration data for the FL WLAN 510x can be saved to the SD card and downloaded from the SD card to the WLAN device. The "Perform action" menu for this purpose is located under "System" in the web interface.



The device can also be operated without an SD card. The configuration is also stored in the internal memory of the device.

3.5.2 Saving the device configuration

The active device configuration is saved to the SD card. This configuration can then also be transferred to another device. In addition to the configuration, the current firmware image is also stored on the SD card. This too is read from the card after power up if it differs from the internal firmware image (present on the device).



NOTE: Device downgrade

If there is an older version of the device firmware on the SD card, on a power up, the older firmware version on the card will be installed if the SD card is inserted and the newer device firmware will therefore be overwritten. This function ensures 1:1 function compatibility in the event of device replacement.

In the case of a newer device, the dual image concept can be used if necessary to switch easily to the second, newer image in the AP.

Note: loading the device configuration

The device configuration is loaded from the SD card to the WLAN device. The WLAN configuration must be saved to the SD card in a folder with the name “FLConfig” so that the WLAN 510x can access it.

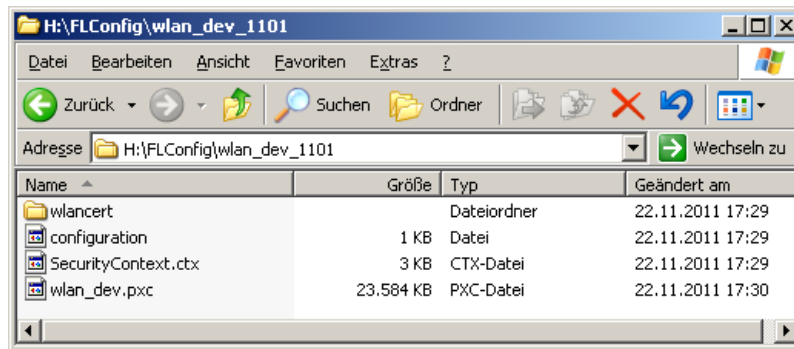


Figure 3-13 Folder for saving the configuration file on the SD card

All configuration data is saved, with the exception of some parameters that should not be overwritten when the configuration data is later transferred to other devices via the SD card.

3.6 Firmware update

A firmware update can be performed directly via the web interface.

- To do so, select “Update Firmware” under the “System” menu item.
- A “Firmware Update” pop-up window allows you to choose whether to update the firmware via “HTTP” or “TFTP”.



Note: Please keep in mind that the configuration settings of the device may be lost when you downgrade the firmware.

3.6.1 HTTP

- Select “HTTP” and click on the “Upload a file” button. Then select the folder containing the new firmware. The new firmware file is a “.pxc” file.

The firmware is loaded, and the update status is indicated by a progress bar.

“Update finished” is displayed as the status when the update is completed.

- Close the “Firmware Update” window.

To activate the new firmware, the device must be restarted. This can be activated by clicking on the “Auto Reboot” or “Reset” button at the top of the “System” web window or by performing a voltage reset for the device.

3.6.2 TFTP

- Select “TFTP” and enter the IP address of the TFTP server in the window provided for this purpose. In the “Remote firmware filename” window, enter the path and name of the firmware file (see also “Using file transfer” on page 63).
- Start the TFTP file transfer by clicking on the upload button.
- Close the “Firmware Update” window.
- To activate the new firmware, the device must be restarted. This can be activated by clicking on the “Reset” button at the top of the “System” web window or by performing a voltage reset for the device.

3.6.3 Via SD card

- Make sure that the desired firmware version is located in the “FLConfig” folder. The new firmware file is a “.pxc” file.
- Switch off the device on which you wish to install the new firmware, e.g., by interrupting the power supply.
- Now insert the SD card into the device.
- Switch on the device with the card inserted.
- LEDs A - D form a light sequence and indicate that the firmware is being downloaded.

After rebooting, the new firmware version is available.

3.6.4 Via BootP/TFTP



This update method is used if the firmware on the device is no longer compatible in terms of function and a new version needs to be installed.

- Make sure that your PC has an active BootP and TFTP server.
- Configure the TFTP server with the IP addresses assigned via BootP.
- Place the desired firmware image in the corresponding folder of the TFTP server.
- Connect the device and your PC via an Ethernet cable.
- Switch off the device on which you wish to install the new firmware, e.g., by interrupting the power supply.
- Switch on the device while holding down the MODE button. Do not release the button until the LEDs change from yellow to green.

3.7 Operating modes of the device

The device supports “Access Point”, “Client”, “Repeater”, and “Machine Admin” modes. “Client” mode is subdivided into three options: “FTB - Fully Transparent Bridge”, “SCB - Single Client Bridge” and “MCB - Multi Client Bridge”. Each operating mode supports different applications.

3.7.1 Operating mode: access point

In “Access Point” mode, the FL WLAN 510x represents the wireless interface of an Ethernet network. WLAN devices can be connected wirelessly to a network via this access point.

Important parameters

The WLAN network, which is represented by 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 that network security is protected against unauthorized access via the WLAN interface (according to IEEE 802.11i), secure encryption must also be used (see Section 3.4.1 on page 34).

The network name and encryption are defined in the access point. They can be entered via the web interface.

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

If WLAN access is to take place at several points in an Ethernet network or a wide area is to be covered, multiple WLAN access points are used which are connected to the network. If all of these access points use the same SSID and encryption, a connected WLAN client can switch between the access points.

Roaming

The process where a WLAN client switches from one access point to another is known as roaming. The speed of roaming varies depending on the type of client used. Roaming is rather slow in the case of a notebook. For applications where roaming needs to be carried out in a fraction of a second, industrial WLAN clients must definitely be used. Roaming is primarily defined via the client. Access points are effective due to their physical location, set transmission power, and antenna. They make sure that there is sufficient network coverage available at every location. The FL WLAN 510x is already optimized for fast roaming in client mode. The user can only improve effectiveness by restricting channels via the “Roaming search list” under “Advanced WLAN configuration” (see Section 4.1 on page 70).

Network planning

The frequencies to be specified for the wireless channels are also defined via the access point, ideally as early as the WLAN network planning stage. 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 to a greater or lesser extent depending on how much data the application requests via the individual clients. If the application has time requirements, the number of clients must also be taken into consideration. For example, for

PROFINET applications, it is recommended that the number of clients per access point is reduced to a few devices. This can be achieved by using multiple access points and assigning different frequencies and SSIDs.

The configuration of an access point is described step by step in Section 3.4.1 on page 34 and Section 4.1 on page 70.

3.7.2 Operating mode: client

3.7.2.1 Compatibility between different WLAN device manufacturers

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

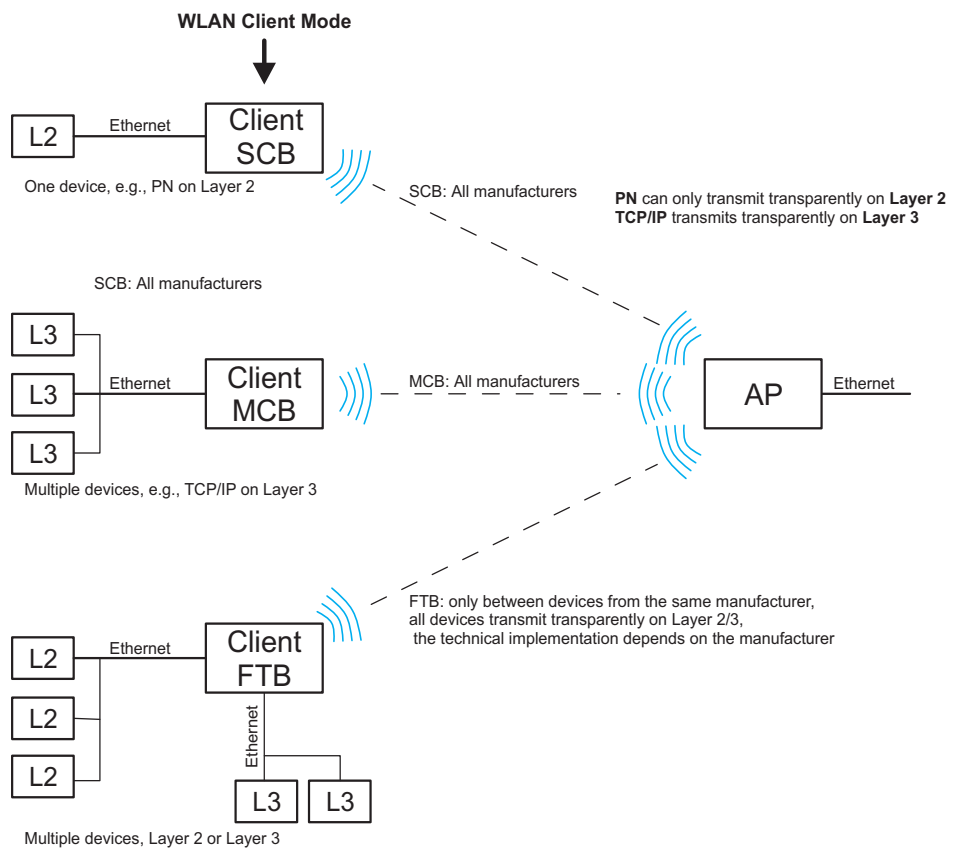


Figure 3-14 Overview of the various client modes

3.7.2.2 Operation as a single client

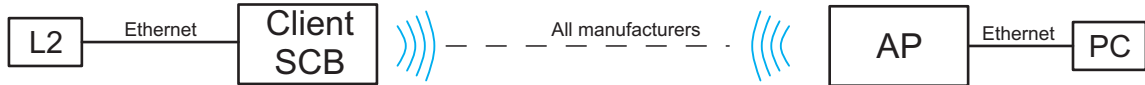


Figure 3-15 Diagram: single client mode

Properties:

- Transparently connects an Ethernet device to the access point on Layer 2 via WLAN.

3.7.2.2.1 Automatic SCB



It is not necessary to manually enter the MAC or IP address of the connected device in the FL WLAN 510x. It requests these automatically.

Only **one** cable-based device may be connected in SCB mode.

Example of static IP:

An Ethernet device (L2) with static IP address is connected to the copper port of the FL WLAN 510x (in SCB mode).

A ping is sent or the IP address of the Ethernet device (L2) behind the client is addressed via a browser from the PC that is connected to the access point on the other side.

A broadcast is sent to all devices. Device L2 responds. The first response (ARP reply) is not sent back via the WLAN wireless interface of the FL WLAN 510x. This means, a timeout is received on the PC side following the first ping/browser call, i.e., not a response. All other calls are answered.

Old ARP tables (in the PC) can be deleted 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 running in DHCP mode, the MAC address is always transmitted to the FL WLAN 510x and beyond.



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

3.7.2.2.2 Manual SCB

If several Ethernet devices are connected to the Ethernet port of the FL WLAN 510x 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 the web interface.

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, the data is transmitted transparently on Layer 2. Only the device whose MAC address is entered for FL WLAN 510x can be accessed via WLAN.

3.7.2.3 Operation as a multi-client

Properties:

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

3.7.2.4 Operation as a fully transparent bridge (default)

Properties:

- Connects several Ethernet devices (connected via Ethernet switches) to the access point on Layer 2.

Operation as a fully transparent bridge is possible between the following devices:

FL WLAN 510x – FL WLAN 510x
FL WLAN 510x – FL WLAN XX AP/DAP 802-11
FL WLAN 510x – FL WLAN 24 EC 802-11

Operation as a fully transparent bridge is not possible between the following devices:

FL WLAN 510x – FL WLAN 24 AP 802-11 XDB
FL WLAN 24 EC 802-11 – FL WLAN 24 AP 802-11 XDB
FL WLAN 24 AP 802-11 XDB – FL WLAN xx AP/DAP 802-11

- An FTB connection between the FL WLAN 510x and the device (access point) of a third party manufacturer can only work if the latter uses the same, non-standardized implementation. This is possible, but rather unlikely. More detailed information regarding interoperability in FTB mode with other manufacturers cannot be provided.

3.7.3 Operating mode: repeater

The FL WLAN 510x offers repeater functionality. This means that several devices in one line can be connected via WLAN. One or more clients can log onto the individual devices in this repeater chain. These can be connected via WLAN or the Ethernet copper ports. See Figure 3-3 on page 49 and Figure 3-5 on page 51. This repeater function allows for the creation of a linear structure. A meshed network or rings cannot be created.

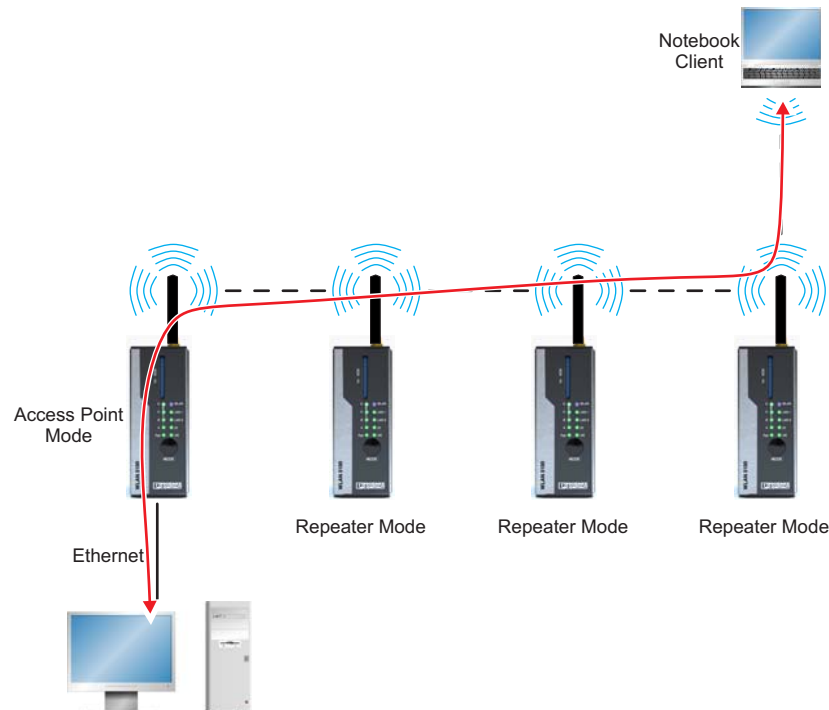


Figure 3-3 Communication via a repeater chain; enables WLAN coverage for complex topologies and connection at various locations

Properties:

- The repeater acts as a logical dual device with a client (FTB) and an access point. The repeater can therefore connect to every AP.
- All access points run on the same WLAN channel.
- In repeater mode, the data rate is at least halved as each data packet is received and sent.
- The coverage area of a WLAN network is enlarged.
- The configuration matches that of a client.
- Only with PSK encryption.

3.7.3.1 Configuration of repeater mode

First, a FL WLAN 510x must be configured as an access point. The device settings mainly determines the encryption, the SSID, and the wireless channel with which the entire repeater system operates. The other devices, which are configured as repeaters below, search for this SSID on all wireless channels.

3.7.3.1.1 Configuration of the access point

The configuration of an access point is described in “Operation as an access point” on page 34. Only “WPA-PSK (TKIP)”, “WPA2-PSK (AES)” or no encryption can be selected as the security mode.



In order to reach full data throughput under WLAN 802.11n, WPA2-PSK (AES) encryption must be used.

3.7.3.1.2 Configuration of the repeater

In the “WLAN” menu, “Repeater” is selected as the “Operating Mode” and confirmed with “Apply&Save”. The “SSID”, “Security mode”, and “Passkey” are then entered and confirmed with “Apply&Save”.

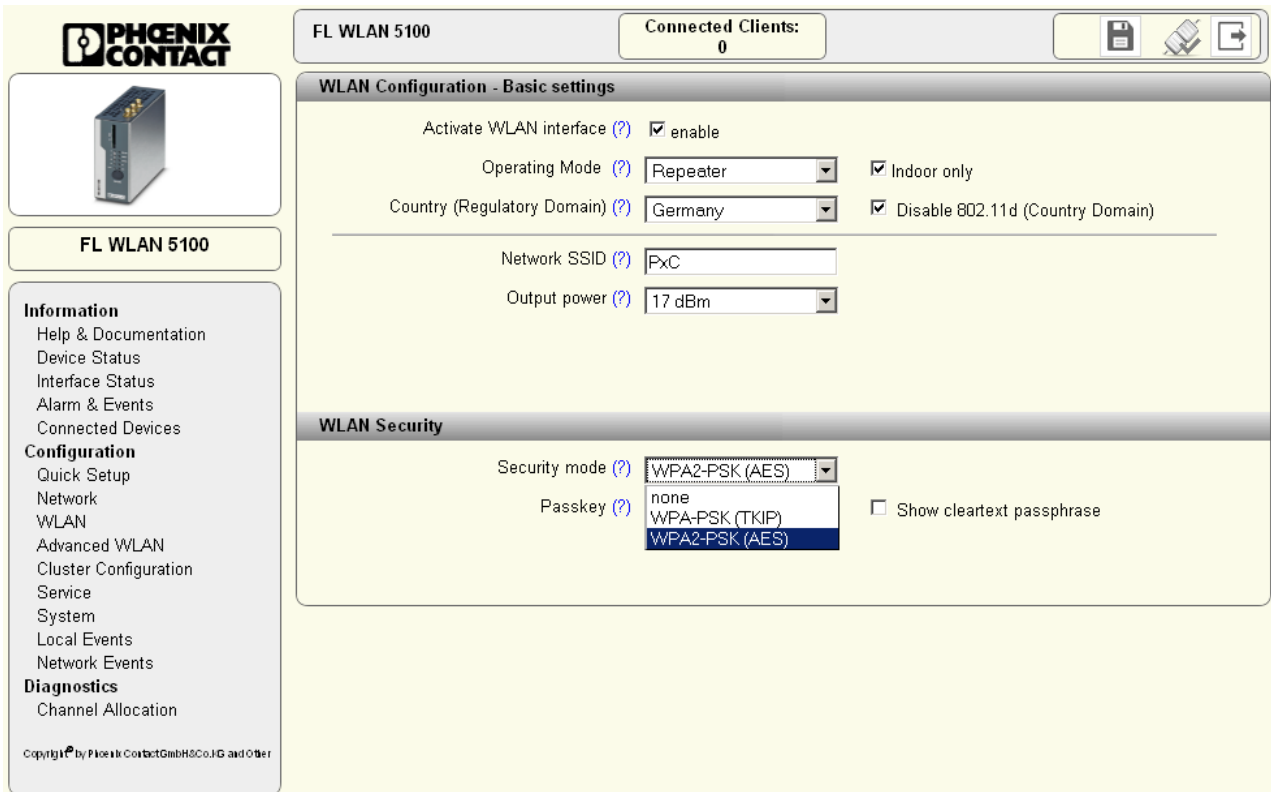


Figure 3-3 Configuration of the repeater

The WLAN repeater now scans for the corresponding SSID and establishes the connection. The “WLAN” LED lights up blue after successful connection establishment. The MAC address of the connected device and information regarding the connection quality are displayed in the “Interface Status (WLAN)” menu.

3.7.3.1.4 Number of devices - data throughput

Multiple devices can be connected to all FL WLAN 510x devices in repeater mode via the Ethernet port or the WLAN wireless interface. In repeater mode, the data is transmitted sequentially via a single wireless channel. This means that the overall data rate that can be achieved decreases as the number of devices and repeaters increases. The data throughput that can be achieved is dependent on these factors, on the potential use of the wireless channel by other devices, as well as on the distance between the individual devices. As a result, no general statement can be made as to the possible data throughput amount.

With respect to the clients connected via WLAN, repeater mode supports FTC, SCB, and MCB (see Section “Operation as a client” on page 36 and Section “Wi-Fi Protected Setup (WPS)” on page 56).

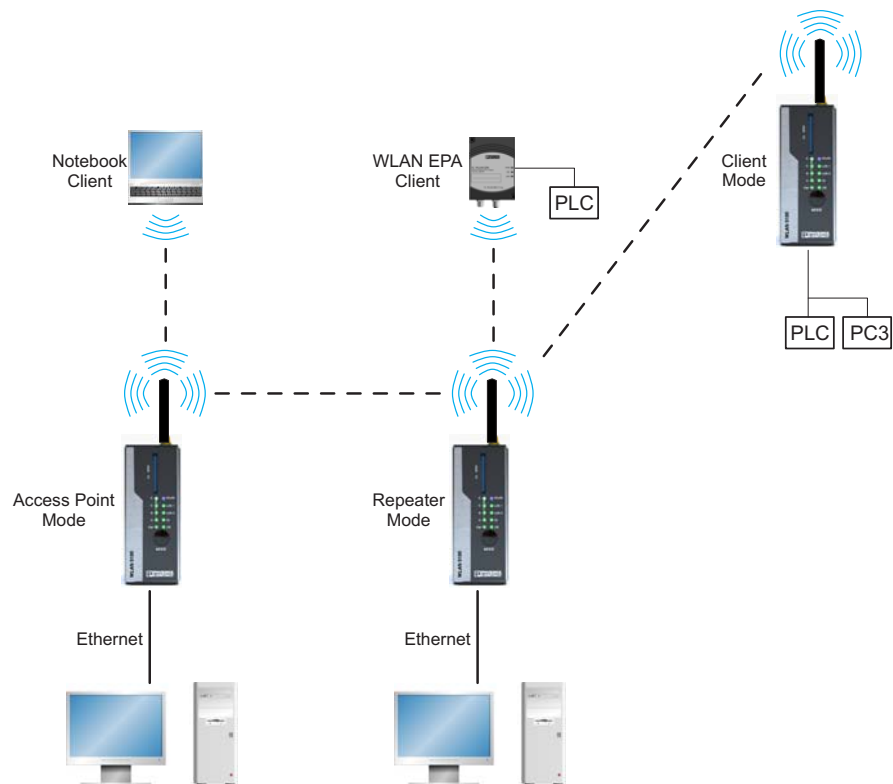


Figure 3-5 FL WLAN 510x in repeater mode: device connection via RJ45 or WLAN



All FL WLAN 510x devices in a network that are configured as repeaters operate with one SSID, one security mode, and one passkey. The same applies to the clients that are connected to the repeaters via WLAN. All devices use a single wireless channel.



The use of WPS is not supported in repeater mode.

3.7.4 Operating mode: machine admin

In “Machine Admin mode”, a network device can be accessed via WLAN using a panel PC or smart phone. A second SSID which enables password-protected access to exactly one device in the network is assigned for this access. During configuration, this device is specified by entering its IP address. This mode is intended for maintenance access of a service technician, for example, who should deliberately not be able to access the entire network.

In parallel, the entire network can be accessed password-protected via the other SSID of normal access point mode.

3.7.4.1 Configuration of “Machine Admin” mode



When using “Machine Admin” mode, “PROFINET assistance mode” cannot be enabled.

“Machine Admin” mode is activated on the web interface under “WLAN”, “Operating mode”. When selecting “Machine Admin” mode, “Access Point” mode automatically runs in parallel. The network via the access point and the connected network are therefore still available via the SSID specified under “WLAN”. In addition, restricted access to a specific network device is enabled using a different SSID.

This access is configured under “Machine admin configuration”. This menu item is shown in the menu on the left after selecting “Machine Admin” mode.

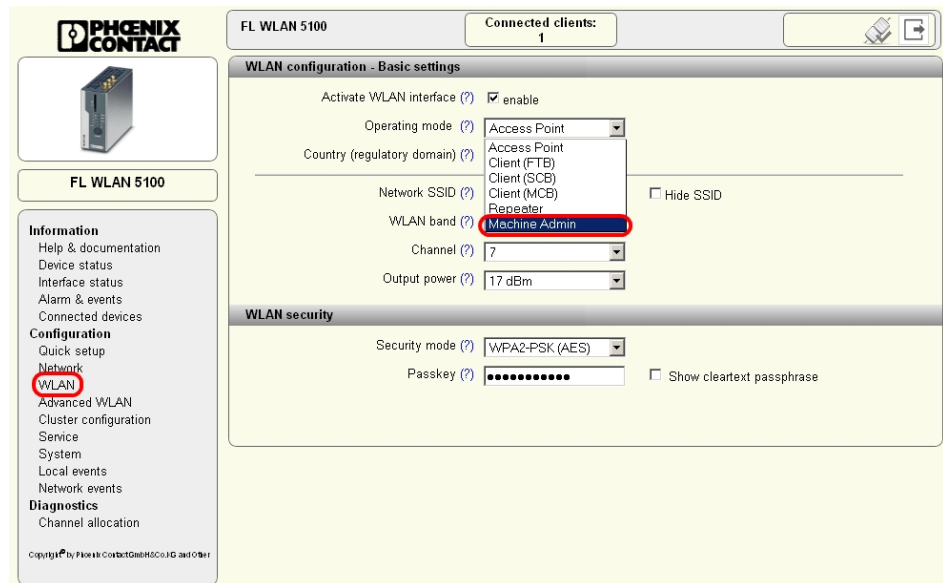


Figure 3-6 “Machine Admin” mode can be selected on the “WLAN” page.

Second SSID

Open the “Machine admin configuration” page. First, enter a network name in the “Second SSID” field. This name is used to identify the administrator network. The name is displayed on the “WLAN” page and can be selected by the termination device to be connected. Typically, the termination device is a tablet PC, smart phone, or notebook.



If your termination device is to be assigned an IP address via the WLAN 510x, the DHCP server must be configured first (see Section “DHCP server” on page 64). Usually, devices like tablet PCs or smart phones expect temporary IP address assignment via a DHCP server.

Passkey

In this field, encryption for “Machine Admin” access is entered. The type of encryption always corresponds to that specified in access point mode. It is configured under “WLAN”, “Security mode”.

8 to 63 characters may be used. Letters, numbers, and the following characters are permitted: \$%&/()=?[]{}+*-_<>.

Grant access to IP

“Machine admin” access via the WLAN interface (second SSID) of the WLAN 510x enables the user to access exactly one device in the connected network. This device is specified via its IP address. This address is entered under “Grant access to IP”.



The IP addresses under “Grant access to IP” must be in the same address area as the WLAN 510x. See “Network configuration”.

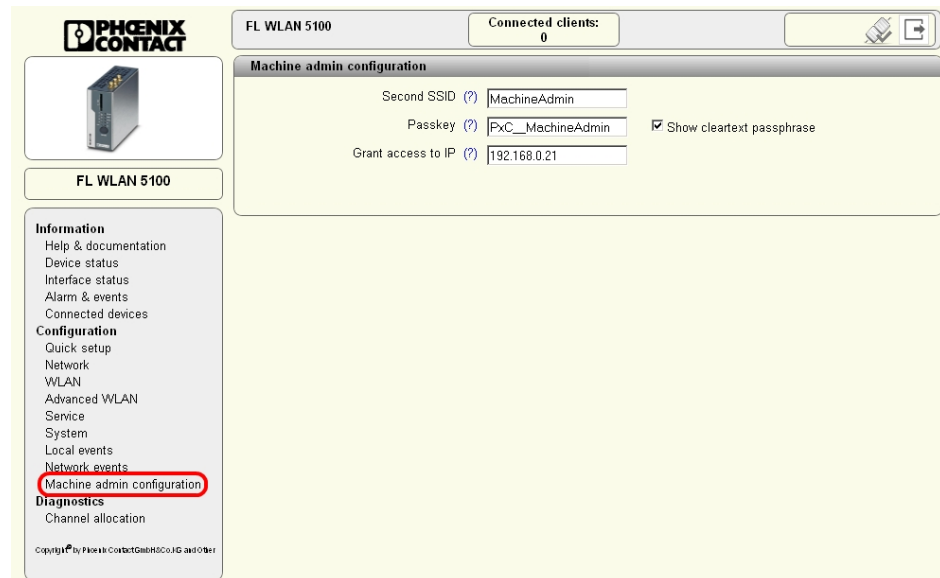


Figure 3-7 The required settings for maintenance access connection can be entered in the “Machine admin configuration” menu

3.8 PROFINET assistance mode

3.8.1 WLAN in PROFINET applications

The use of WLAN in PROFINET applications means that certain individual parameters must be observed. PROFINET places high demands on prompt data transmission, also via the WLAN interface.

3.8.1.1 Activating PROFINET assistance mode

“PROFINET assistance mode” can be activated in the web menu under “Service Configuration”. Alternatively, “PROFINET assistance mode” can also be activated using the MODE button (mode 3).

The screenshot displays the web configuration interface for a Phoenix Contact FL WLAN 5100 device. The interface is organized into several sections:

- Service User Interfaces:** Contains settings for Webserver mode (HTTP), Telnet Command Line Interface (enable), Secure Shell (SSH) (enable), and SNMP Server (SNMPv2).
- Service Configuration:** This section is highlighted and contains the 'Profinet assistance mode' dropdown menu, which is currently set to 'enable'. Other options include 'Disable configuration from WLAN' (checkbox) and 'Remote Syslog Server IP Address' (0.0.0.0).
- System Time:** Contains settings for Network time protocol* (disable), Primary and Secondary SNTP Servers (0.0.0.0), Manual time set* (click to set time), and UTC offset* (+00h UTC, GMT, Lon). It also displays the current system time as 18h:37m:47s and the last SNTP synchronisation status as 'not synchronized'.

At the bottom of the configuration area, there are three buttons: 'Revert', 'Apply', and 'Apply&Save'. A left-hand navigation menu includes sections for Information, Configuration, and Diagnostics.

Figure 3-8 “PROFINET assistance mode” should be enabled in PROFINET applications

The following settings are activated in “PROFINET assistance mode”:

1. IP address assignment is via DCP
2. PROFINET data is transmitted with top priority

3.8.1.2 PROFINET prioritization

In “PROFINET assistance mode”, prioritization based on the PROFINET Ethertype is performed in addition to prioritization based on the VLAN tag and 802.11e. Here, PROFINET packets are transmitted with top priority over all other Ethernet packets via the WLAN interface (strict prioritization). The remaining traffic not labeled as PROFINET is limited to a maximum data throughput of 10 Mbps. Reliable PROFINET communication is therefore also ensured in the event of a higher broadcast and multicast load as well as other high-priority data on the Ethernet interface.



When setting the PLC please observe that the PROFINET update time must also be adjusted according to the number of PROFINET devices. The more PROFINET devices used in the WLAN network, the higher the required PROFINET update time.

3.9 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup (WPS) is a standard developed by the Wi-Fi Alliance intended to help users easily set up a wireless network including the encryption method or to easily add devices.

3.9.1 Running WPS using the MODE button



Please note that the WPS function is disabled automatically after 120 seconds for security reasons.



Make sure you only ever set one access point to WPS mode. This will prevent clients connecting to an incorrect access point.



Please note that the WPS function cannot be used if certificates are used.

Sequence:

- Activate the “WPS Access Point” function for the access point on the “Advanced WLAN” web page. The access point can now be accessed by clients for 120 seconds, during this time the link quality LEDs flash yellow. Once this time has elapsed, the device returns to configuration mode.
- Select “WPS Client” mode for the client using the MODE button. The client can now be accessed by access points for 120 seconds, during this time the link quality LEDs flash yellow. Once this time has elapsed, the device returns to configuration mode. If the device has received valid configuration parameters, the link quality LEDs flash green; if no configuration was received, the link quality LEDs flash yellow and the error LED lights up red.

3.10 Quality of service

The device supports Quality of Service (QoS) in the following way:

- The use of QoS is supported both according to IEEE 802.1p and according to IEEE 802.11e.
- The device evaluates IP ToS and VLAN tags.
- If the device is operating in **PROFINET assistance mode**, the PROFINET packets are classed as high priority based on their Ethertype value. Strict prioritization is used. “Non-PROFINET traffic” is now limited to a maximum data throughput of 10 Mbps.

3.11 Cluster management

For the simplified configuration of larger WLAN networks, the FL WLAN 510x offers cluster management. This functionality enables WLAN access points within a network to be configured clearly and quickly. They are grouped together into a cluster.

3.11.1 Searching and selecting cluster devices

To configure a cluster, call a WLAN access point, which you intend to add to the cluster, via the corresponding IP address. The other FL WLAN 510x devices are connected to this device via the cable-based Ethernet network. They are in “Access Point” mode.



Only FL WLAN 510x series devices can be grouped into a cluster.

The access point whose web interface you are viewing is fully configured. These parameters are later transferred to all access points that belong to the cluster. Parameters can also be modified later, some individually for each device.

The “Clustering” parameter must be activated (default) in the “Cluster Configuration” menu in order to apply the configuration. Clicking on “Manage Cluster Group” opens the “Cluster Group Configuration” pop-up window.

First, enter a name for the future cluster under “Cluster Name”. Confirm with “Apply”.

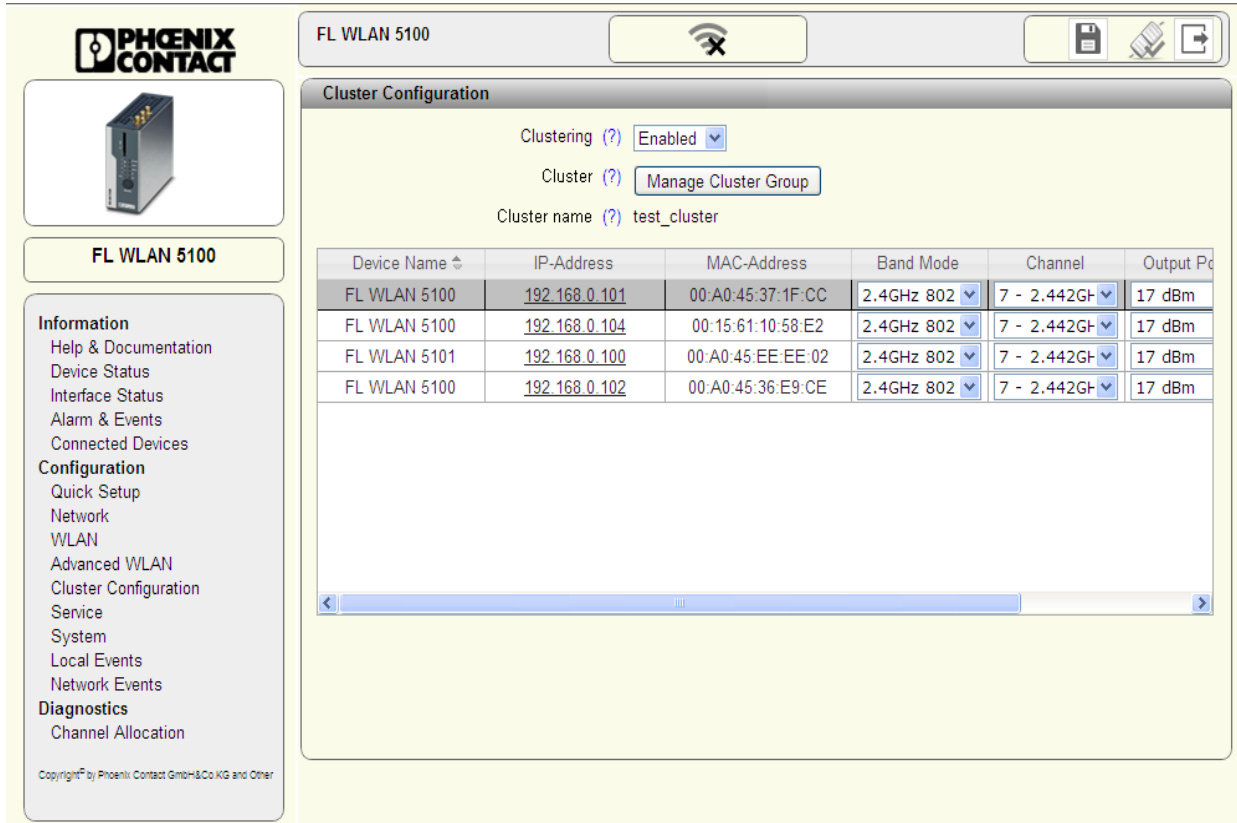


Figure 3-9 Assigning the cluster name - the table first shows the access point used for configuration by the user

Click on “Start” to start searching for other FL WLAN 510x type access points on the cable side. After completing the inquiry scan, a list of available access points is displayed. The access point used for configuration is displayed in the last row on a gray background.

The access points that will be added to the cluster are now selected in the last column, “Cluster Member” (see Figure 3-10 on page 59).



Up to 20 access points can be grouped into a cluster. An Ethernet network can have several clusters.

Cluster Group Configuration

Cluster Name (?)

Start Inquiry (?)

Inquiry Process (?)

Device Name	IP-Address	MAC-Address	Device Type	Cluster Member
not assigned				
FL WLAN 5101	192.168.0.100	00:A0:45:EE:EE:02	FL WLAN 5101	<input checked="" type="checkbox"/>
FL WLAN 5100	192.168.0.102	00:A0:45:36:E9:CE	FL WLAN 5100	<input type="checkbox"/>
FL WLAN 5100	192.168.0.104	00:15:61:10:58:E2	FL WLAN 5100	<input checked="" type="checkbox"/>
test_cluster				
FL WLAN 5100	192.168.0.101	00:A0:45:37:1F:CC	FL WLAN 5100	<input type="checkbox"/>

Figure 3-10 List and configuration options for the cluster created

Once all desired access points have been selected by activating the corresponding checkbox, click on “Apply” to start creating and configuring the cluster.

The configuration of the preset access point is transferred to all the other devices. The process can take a little time depending on the number of access points in the cluster.

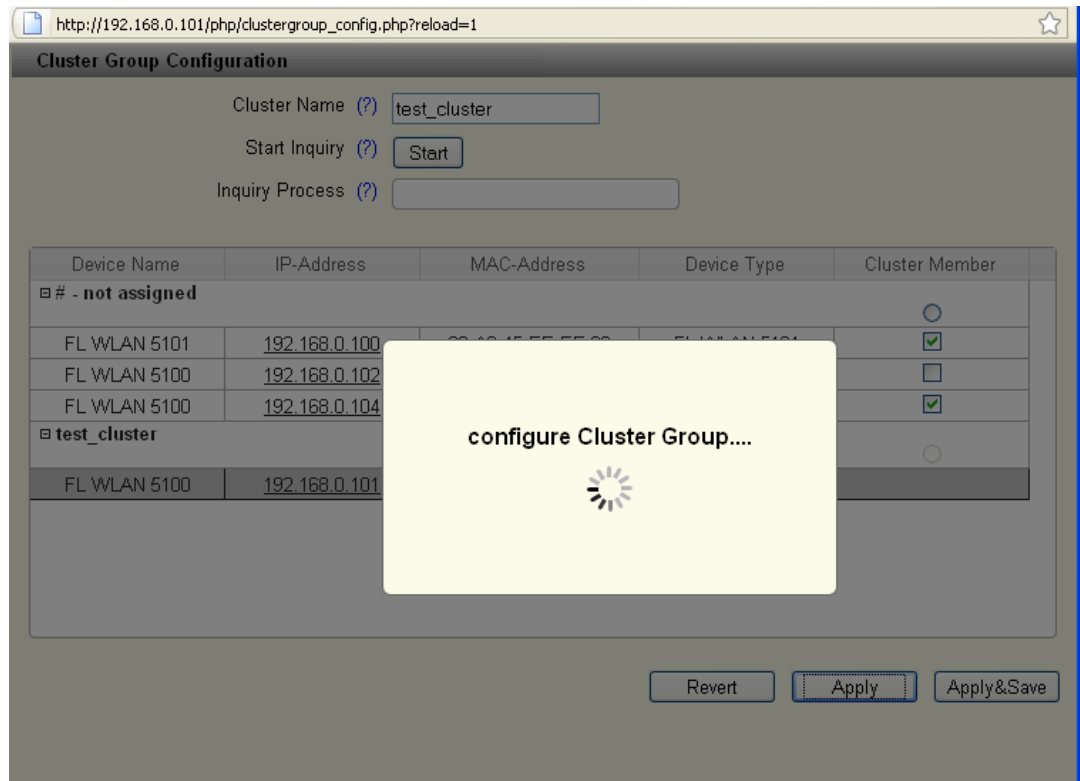


Figure 3-11 Automatic configuration of the selected cluster

A table containing all the access points belonging to the cluster then appears in the “Cluster Configuration” window. They can be identified by their IP address or MAC address.

FL WLAN 5100

Cluster Configuration

Clustering (?) Enabled

Cluster Group (?) Manage Cluster Group

Cluster Group Name (?) test_cluster

Device Name	IP-Address	MAC-Address	Band Mode	Channel	Output Power
FL WLAN 5100	192.168.0.101	00:A0:45:37:1F:CC	2.4GHz 802	7 - 2.442GHz	17 dBm
FL WLAN 5100	192.168.0.104	00:15:61:10:58:E2	2.4GHz 802	7 - 2.442GHz	17 dBm
FL WLAN 5101	192.168.0.100	00:A0:45:EE:EE:02	2.4GHz 802	7 - 2.442GHz	17 dBm
FL WLAN 5100	192.168.0.102	00:A0:45:36:E9:CE	2.4GHz 802	7 - 2.442GHz	17 dBm

Figure 3-12 List and configuration options for the cluster created

The parameters that can be adjusted individually, if necessary, to achieve full wireless coverage can be edited in the table: frequency band, channel, and transmission power. The number of WLAN clients connected to the relevant access point can be seen in the right-hand column of the table.

The configuration is stored to the device as the latest configuration by clicking on the diskette icon.



Any parameter changes made to a device belonging to a cluster and saved will be automatically transferred to the other devices in the cluster. However, the parameters listed in the "Cluster Configuration" table can be configured individually.

Access points can be integrated into a cluster at a later time. To do this, enter the name of the existing cluster under "Cluster Name" in the "Cluster Group Configuration" window. An inquiry scan is triggered by clicking on "Start". The new device appears in the list and can be added to the cluster via the checkbox under "Cluster Member". Save the configuration with "Apply&Save".

3.11.2 Identifying cluster-relevant parameters in the web interface

In cluster management, the parameters of an access point marked with an (*) in the web interface (see red marking in Figure 3-13 on page 62 if the function was previously activated on the “Cluster Configuration” web page) are transferred to the other access points in the cluster.

The screenshot shows a web interface for configuring an access point. The parameters are grouped into sections. The first section includes:

- Country (Regulatory Domain)* (?) with a dropdown menu set to 'Germany'. This label is circled in red.
- Operating Mode (?) with a dropdown menu set to 'Accesspoint'.
- Network SSID* (?) with a text input field containing 'PxC'.

 The second section includes:

- WLAN Band* (?) with a dropdown menu set to '2.4GHz(802.11 b/g/n)'.
- Channel* (?) with a dropdown menu set to 'Channel7 - 2.442GHz'.
- WLAN Security* (?) with a dropdown menu set to 'WPA2-PSK (AES)'.
- Passkey* (?) with a text input field containing ten dots and a checkbox labeled 'Show cleartext passphrase'.

 The third section includes:

- Administrator Password* (?) with a text input field.
- Retype Password* (?) with a text input field.

Figure 3-13 Cluster information in WBM

An access point that is part of a cluster indicates this in the web interface as well as the following cluster information:

- Name of the access point
- MAC address
- IP address

The following information is exchanged within a cluster:

- WLAN SSID
- Security settings (access control list, MAC address filter)
- User names and passwords
- QoS settings
- WLAN settings

The following information can also be viewed within a cluster:

- Diagnostic information
- Connected clients

3.11.3 Properties of cluster management

- The members of a cluster have the same cluster name and the same administrator password.
- The cluster configuration can be changed by any cluster member.
- The members of the cluster automatically load the latest configuration.
- IP addresses are not assigned via cluster management.
- Up to 20 access points can belong to a cluster.
- Individual settings can only be made to cluster members if these particular members can be accessed.
- The individual settings of specific devices are not saved “in” the cluster and therefore, in the case of device replacement, cannot be transferred to the replaced device.
- Devices that were offline when a change was made to the configuration in the cluster detect that the cluster configuration was changed as soon as they go online again and apply the new configuration automatically.
- When a cluster-relevant change to the configuration of a device is saved this triggers saving on all cluster members.

3.12 Using file transfer

Various files can be transferred between the configuration PC and the device using HTTP(s) or TFTP:

Table 3-1 File transfer

File	Upload	Download
Device documentation		Yes
SNMP MIB files		Yes
Security context	Yes	Yes
CA root certificate	Yes	Yes
Client certificates	Yes	Yes
Event log files		Yes
Firmware files	Yes	
Device configuration	Yes	Yes

3.13 DHCP server

The FL WLAN 510x has a DHCP server. IP addresses can be assigned via WLAN or the Ethernet interface (copper). By default upon delivery, the DHCP server is deactivated.

The “DHCP Server” item can be found in the “Network” menu under “Configuration”. Configuration is performed here.

DHCP server

To activate the DHCP server, IP address assignment must be set to “static” under “Network configuration”. After selecting “enable”, the following parameters can be configured.

The screenshot shows the web interface for the FL WLAN 5100. The main content area is titled "Network configuration" and "DHCP Server". In the "Network configuration" section, the "IP address assignment" dropdown menu is set to "static" and is highlighted with a red box. Below it, the "IP address" is 192.168.0.250, "Subnet mask" is 255.255.255.0, "Gateway" is 0.0.0.0, and "Nameserver" is 0.0.0.0. In the "DHCP Server" section, the "DHCP Server" dropdown menu is set to "enable" and is also highlighted with a red box. Below it, the "IP pool starting address" is 192.168.0.20, "Size of pool" is 10, "Subnet mask" is 255.255.255.0, "Gateway" is 0.0.0.0, and "Lease time" is 3600. At the bottom right, there are buttons for "Revert", "Apply", and "Apply&Save".

Figure 3-14 To use the DHCP server, IP address assignment must be set to “static”

IP pool starting address

The first IP address to be assigned by the DHCP server is entered here.

Size of pool

The number of DHCP clients which may receive an address is entered here. The number can be between 1 and 1000.

Subnet mask

The settings of the local subnet mask from the “Subnet mask” field under “Network configuration” are automatically entered in this field. The subnet mask is assigned by the DHCP server.

Gateway

Assignment of the gateway in format 0.0.0.0

Lease time

Time interval in seconds during which the IP address is valid.

3.14 Event handling

Various events trigger various reactions on the device:

Table 3-2 Event handling

Event	SNMP trap	Internal Syslog entry	Send to external Syslog server	Set digital output	Error LED lights up
Device start	Yes, configurable	Always	Yes, configurable		
Link up/link down	Yes, configurable	Always	Yes, configurable		
IPAssign tool download		Always	Yes, configurable		
User login failed	Yes, configurable	Always	Yes, configurable		
Power supply low level	Yes, configurable	Always	Yes, configurable		
Error LED ON/OFF	Yes, configurable	Yes	Yes, configurable		
Client connected/not connected	Yes, configurable	Always	Always		
Roaming performed	Yes, configurable	Always	Yes, configurable		
Client mode changed	Yes, configurable	Always	Yes, configurable	Yes, configurable	Yes, configurable

3.14.1 Selecting events in web-based management

Various events can be selected on the “System Events” web page, the occurrence of which generates an external Syslog entry or sends an SNMP trap. In addition, the SNMP trap receivers are defined here.

The screenshot displays the web-based management interface for a Phoenix Contact FL WLAN 5100 device. The main content area is titled "System Events" and includes a configuration section for SNMP traps. A dropdown menu is open, showing two IP addresses: 10.10.2.23 and 192.162.2.57. Below this, there is a text input field for "Add new IP address" and an "add" button. At the bottom of the configuration area is a table with the following data:

Event	SNMP Trap	Remote Syslog
Start of device	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Ethernet link state changed	<input type="checkbox"/>	<input type="checkbox"/>
Userinterface access changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Digital Input state changed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Error LED state changed	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Configuration state changed	<input type="checkbox"/>	<input checked="" type="checkbox"/>
SD plug state changed	<input type="checkbox"/>	<input checked="" type="checkbox"/>

At the bottom right of the page, there are three buttons: "Revert", "Apply", and "Apply&Save".

Figure 3-15 Possible system events that can be selected

4 Menu/functions

The web interface is split into three main areas, each containing several thematically structured web pages.

Area: Information

This area contains information on the product and the current device status. You do not have to log in to access the web pages.

Area: Configuration

You can configure the device in this area. For security reasons, you must log in with a password before accessing the web pages.

Web page: Quick Setup

All the main parameters are grouped together on the “Quick Setup” web page in order to enable quick and easy configuration of a WLAN standard network or WLAN client adapter.

Area: Diagnostics

All information regarding the diagnostics of wireless connections can be found in this area.

Help

On web pages, a (?) appears after each parameter. When you place the mouse pointer over it, information regarding the parameter is displayed in a flyout window.

4.1 Parameter list for the configuration

Table 4-1 Parameter list for Information page

Designation	Description
Help & Documentation	
Documentation & SD Card	
Documentation of the device (PDF)	The latest documentation for the device can be downloaded here as a PDF file.
Device Description Zip (SNMP, SGML)	ZIP file for the device description (SNMP, SGML)
IP Assignment Tool	The IP Assignment Tool can be downloaded from the device here. It can be installed on a PC and used for IP address assignment.
Device Status	
Device Identification	
	This area contains important static information regarding the WLAN device, especially its hardware and firmware version.
System Status	
	This area contains dynamic information regarding the WLAN device, such as the system time, operating time since the last voltage reset, and the states of the digital inputs and outputs.
Interface Status	
Interface Status LAN	
	This area contains information regarding the current settings and states of the LAN interfaces.
Interface Status WLAN	
	This area contains information regarding the current settings and states of the WLAN interfaces. Note on client mode: "Show RSSI" displays a bar graph for antenna alignment.
Alarm & Events	
Alarm & Events	
	A chronologically ordered table overview displays the event messages of the device. The complete log file can be downloaded via a link.
Connected Devices	
	Only in access point mode: the connected devices (client mode) and their parameters are displayed in table format.

Table 4-1 Parameter list for Information page [...]

Designation	Description
Configuration	
Quick Setup	
Quick Setup - any configuration on this page always activates the WLAN interface.	
Web management language	Select the language for the web interface. Enable cookies in your browser. Otherwise, the language will be reset to English when you log in again.
IP Address Assignment	<p>Static: a static IP address is assigned to this interface.</p> <p>BootP: during initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. As soon as it receives a valid IP address, the device stops sending BootP requests.</p> <p>After receiving a BootP reply, the device no longer sends BootP requests. Following a restart, a device that was previously configured sends three BootP requests; if these requests are not answered, the device starts with the IP address that was last assigned via BootP. After the default settings are restored, the device sends BootP requests until they are answered.</p> <p>DHCP: dynamic request for an IP address from a DHCP (Dynamic Host Configuration Protocol) server.</p>
Country (Regulatory Domain)	Select the country in which the device is operated from the list. You will then only be able to configure the parameters that are permissible for this specific country.
Operating Mode	<p>Access point: implements a WLAN wireless network for wirelessly connecting WLAN-compatible devices to an Ethernet network.</p> <p>Client (FTB): supports the wireless connection of Ethernet devices to an Ethernet network via a WLAN wireless network. "Fully Transparent Bridge (FTB)" mode supports Layer 2 transparent communication with multiple devices behind the WLAN client. Other client modes are available in the "WLAN" menu.</p>
Network SSID	The SSID is the network ID via which clients are assigned to the access points. It can be a maximum of 32 characters long. Letters, numbers, and the following characters are permitted: \$@&/()=?[]{}+*-_<>.
WLAN Band	Selection of the frequency band. Other operating modes according to IEEE 802.11 are available in the "Advanced WLAN" menu.

Table 4-1 Parameter list for Information page [...]

Designation	Description
Channel	<p>Channel selection: possible channel selection depends on the setting made under “WLAN Band”.</p> <p>Indoor Ch36...Ch48: 4 channels can be freely selected.</p> <p>Indoor 8 channels automatically/indoor 16 channels automatically: the system selects the channels automatically (DFS). The connection may be interrupted during a channel switchover.</p> <p>Automatic: The device automatically selects a WLAN channel.</p> <p>Note: if the device is operated outdoors in the 5 GHz band, outdoor mode must be activated.</p> <p>This information is valid for Europe.</p>
WLAN Security	<p>WPA2-PSK (AES) offers the highest security standard. Other encryption options are available in the “WLAN” section. In order to reach full data throughput under WLAN 802.11n, WPA2-PSK (AES) encryption must be used.</p>
Passkey	<p>Key during the initialization of WPA encryption. Note: for maximum security, a random alphanumeric string (up to 63 characters) should be used. Letters, numbers, and the following characters are permitted: \$%&/()=?[]{}+*-_<>. The password must contain at least eight characters.</p>
Administrator Password	<p>It is recommended that you enter a new password to prevent any manipulation of the device. The new password must be between 8 and 14 characters long.</p> <p>The new password is not activated until you log out and log back in again.</p>
Retype Password	<p>Retype the new password you wish to use.</p>

Table 4-1 Parameter list for Information page [...]

Designation	Description
Network	
Network configuration	
Type of IP address assignment	<p>Static: a static IP address is assigned to this interface. BootP: during initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. As soon as it receives a valid IP address, the device stops sending BootP requests.</p> <p>After receiving a BootP reply, the device no longer sends BootP requests. Following a restart, a device that was previously configured sends three BootP requests; if these requests are not answered, the device starts with the IP address that was last assigned via BootP. After the default settings are restored, the device sends BootP requests until they are answered.</p> <p>DHCP: dynamic request for an IP address from a DHCP (Dynamic Host Configuration Protocol) server.</p>
IP address	Entry of the static IP address in format 192.168.0.254.
Subnet mask	Entry of the static subnet mask in format 255.255.255.0.
Gateway	Assignment of the gateway in format 0.0.0.0
Nameserver	If a name server is used, the destination address is entered here in format 0.0.0.0.
DHCP Server	
DHCP Server	The DHCP server assigns IP parameters to network devices. This is performed via both methods the cable-based Ethernet interface and WLAN. To activate the function, "IP address assignment" must be set to "static" first.
IP pool starting address	The first IP address to be assigned by the DHCP server is entered here.
Size of pool	The number of DHCP clients which may receive an address is entered here. The number can be between 1 and 1000.
Subnet mask	The DHCP server uses the local subnet mask. It is configured under "Network configuration".
Gateway	Assignment of the gateway in format 0.0.0.0
Lease time	Time interval in seconds during which the IP address is valid.
WLAN	
WLAN Configuration - Basic settings	
Activate WLAN interface	The disabled WLAN interface prevents any communication at the wireless interface.

Table 4-1 Parameter list for Information page [...]

Designation	Description
Operating mode	<p>Access point: implements a WLAN wireless network for wirelessly connecting WLAN-compatible devices to an Ethernet network.</p> <p>Client: supports the wireless connection of Ethernet devices to an Ethernet network via a WLAN wireless network.</p> <p>FTB mode: Fully Transparent Bridge Supports Layer 2 transparent communication with multiple devices behind the WLAN client.</p> <p>SCB mode: Single Client Bridge Layer 2 transparent communication with one device behind the WLAN client (compatible with all access points).</p> <p>MCB mode: Multi Client Bridge Layer 3 (TCP/IP) transparent communication with multiple devices behind the WLAN client (compatible with most access points).</p> <p>Repeater Access point with wireless connection to another access point (via virtual client).</p> <p>Machine Admin In addition to access point functionality, this access enables another specific service access via WLAN. It is restricted to a specific IP address in the network. Confirming this mode with “Apply&Save” enables “Machine admin configuration” under “Configuration”.</p>
Country (regulatory domain)	When a country is selected, regulatory conditions such as special wireless channels are taken into consideration.
Network SSID	The SSID is the network ID via which clients are assigned to the access points. It can be a maximum of 32 characters long. Letters, numbers, and the following characters are permitted: \$%@&/()=?[]{}+*-_<>.
Hide SSID	<p>Hide the SSID.</p> <p>If “Hide SSID” is used when the access point is operating on a 5 GHz DFS channel, please note that because the clients may not actively scan this area and due to passive scans and the missing SSID in the beacons of the access point it may not be possible to find the correct access point.</p>
WLAN band	Selection of the frequency band. Other operating modes according to IEEE 802.11 are available in the “Advanced WLAN” menu.

Table 4-1 Parameter list for Information page [...]

Designation	Description
Channel	<p>Channel selection: possible channel selection depends on the setting made under "WLAN band".</p> <p>Indoor Ch36...Ch48: 4 channels can be freely selected.</p> <p>Indoor 8 channels automatically/indoor 16 channels automatically: the system selects the channels automatically (DFS). The connection may be interrupted during a channel switchover.</p> <p>Automatic: The device automatically selects a WLAN channel.</p> <p>Note: if the device is operated outdoors in the 5 GHz band, outdoor mode must be activated.</p> <p>This information is valid for Europe.</p>
Output power	<p>Selection of the transmission power at the antenna connection. Maximum corresponds to the maximum transmission power that can be output by the wireless module or which is permitted by regulations. Note: antenna gain and cable attenuation must be taken into consideration by the user.</p>
WLAN Security	
Security Mode	<p>None: operation without encryption puts network security at risk.</p> <p>WPA-PSK (TKIP): used by older devices that do not support WPA/AES.</p> <p>WPA2-PSK (AES): secure and faster for client roaming.</p> <p>WPA2-EAP: enables the use of authentication servers (AAA server, RADIUS server).</p> <p>In order to reach full data throughput under WLAN 802.11n, WPA2-PSK (AES) encryption must be used.</p>
Passkey	<p>Key during the initialization of WPA encryption. Note: for maximum security, a random alphanumeric string (up to 63 characters) should be used. Letters, numbers, and the following characters are permitted: \$%@&/()=?[]{}+*-_<>.</p>

Table 4-1 Parameter list for Information page [...]

Designation	Description
Advanced WLAN	
Advanced WLAN configuration on the access point	
WLAN band	Selection of the frequency band.
Channel Bandwidth (802.11n)	20 MHz: operation of the device on one wireless channel. 40 MHz: operation of the device on two wireless channels (channel bonding). As such, an increased data rate is achieved, but two wireless channels are used.
Static MAC Filter	As an additional security criterion for restricting access, the MAC addresses of devices can be used here to permit or refuse access. Please note that WPS cannot be activated if using a MAC filter.
Roaming search list	Selecting a limited number of channels reduces the client scan time when searching for another access point and speeds up roaming.
Transmit data rate	Limits the data rate to a maximum.
802.11f (IAPP)	Exchange of roaming information between access points. Should be activated; deactivation may be necessary when using seamless roaming clients.
WiFi Protected Setup	Wi-Fi Protected Setup (WPS) supports simplified client security configuration. Clicking on "Activate WPS" activates WPS for 120 seconds. Please note that WPS cannot be used in conjunction with MAC filters.
STBC	Space Time Block Coding is a method for increasing transmission resilience by means of redundant transmission paths in standard 802.11n. STBC must be supported by the client.
RTS/CTS threshold	Packets whose size exceeds the specified value are transmitted with an acknowledgment mechanism in order to avoid collisions. The total bandwidth of the WLAN can be increased if several clients use the same access point. The value 2312 deactivates RTS/CTS, 0 activates it for all packets.
Fragmentation	Data packets whose size exceeds the specified value are fragmented. In RF environments with a lot of interference, the number of repeated packets can therefore be reduced. The value 0 deactivates fragmentation.
Long distance mode (> 3000 m)	Wireless connections over large distances (> 3000 m) require the timeout configuration to be modified. Change this parameter only if the distance is over 3000 m. The setting must be the same for the access point and the client.

Table 4-1 Parameter list for Information page [...]

Designation	Description
Antenna configuration	Selection of the desired antenna connections X5, X6, X7. Only activate the connections to which an antenna is connected. Activated antenna connections can be damaged if an antenna is not connected. Terminate unused connections with 50 ohms.
Cluster Configuration	
Cluster Configuration	
Clustering	Clustering can be used to configure several access points in the same subnetwork for one WLAN network centrally as a group. The parameters marked with (*) are then synchronized automatically between all access points belonging to the cluster.
Cluster	Opens a window in which you can configure the cluster.
Cluster Name	Name of the cluster, can be configured under "Cluster".
Cluster Configuration	
Start Inquiry	Searches for devices that can be picked up in the cluster or are ready. The devices must belong to the same subnetwork.
Table for cluster configuration	Additional (as yet unassigned) devices can be assigned to the current cluster via the checkboxes. You can assign the device you are currently logged into (gray) to another cluster via the radio button.
Service	
Service - User Interface	
Webserver mode	Selection of "Webserver mode": HTTPS (security certificate), HTTP (standard, unsecured). Note: "Disable" deactivates the web interface. When confirmed with "Apply&Save", the device can be accessed only via the CLI. Telnet or SSH must be activated beforehand.
Telnet Command Line Interface	Configuration of the device via Telnet
Secure Shell (SSH)	Configuration via Secure Shell (SSH)
SNMP Server	Selection of SNMP mode: SNMPv2, SNMPv3 or SNMP deactivated.
Service Configuration	
PROFINET assistance mode	IP address assignment via DCP supported. If the device is operating in PROFINET assistance mode , the PROFINET packets are classed as high priority based on their Ethertype value. Strict prioritization is used. "Non-PROFINET traffic" is now limited to a maximum data throughput of 10 Mbps.
Allow configuration via WLAN	If activated, the device can be configured via its WLAN interface (must be deactivated for PROFIsafe applications). The configuration interfaces (WBM, SNMP, CLI via Telnet/SSH) are still available via Ethernet.

Table 4-1 Parameter list for Information page [...]

Designation	Description
Remote Syslog Server IP Address	Diagnostic messages are redirected to the device with the specified IP address. The IP address 0.0.0.0 deactivates the forwarding of messages to the Syslog server.
System Time	
Network time protocol	If the time synchronization of an existing time server is to be used, it must be activated here.
Primary SNMP Server	Entry of the IP address of the primary SNTP server.
Secondary SNMP Server	Entry of the IP address of the secondary SNTP server.
Manual time set	The system time is set here if an SNTP server is not available.
UTC offset	Selection of the time zone. For the times in the event table, for example, make sure that the system time corresponds to Greenwich Mean Time. The current local time is based on the system time and the "UTC Offset". Where necessary, the switch between daylight savings and standard time must be taken into consideration.
Current system time	Display of the current system time
Last SNTP synchronization	If an SNTP server is available in the network, the time is automatically applied from this server if "Network time protocol" is activated. The time of the last synchronization is displayed here.
System	
System	
Reset Device	The device is restarted. Existing WLAN connections are interrupted.
Username	Administrator name
Administrator password	It is recommended that you enter a new password to prevent any manipulation of the device. The new password must be between 8 and 14 characters long. The new password is not activated until you log out and log back in again.
Retype password	Retype the new password you wish to use.
Security context	Open the window for configuring security certificates here.
Security context (pop-up window)	
Upload certificate	Choose whether to upload the safety certificate via TFTP or HTTP.
Direction	Download: WLAN device to local PC (host); Upload: local PC (host) to WLAN device
TFTP server IP address	In the case of TFTP, the file name and path of the TFTP server must be specified here.
Generate new	Generate a new certificate.
SSH hostkey	Host key for the SSH session

Table 4-1 Parameter list for Information page [...]

Designation	Description
Device name	Enter the device name here that will be displayed in the web interface under "Device status".
Device description	Enter the description here that will be displayed in the web interface under "Device status".
Physical location	Enter the location here that will be displayed in the web interface under "Device status".
Device contact	Enter the desired contact address here that will be displayed in the web interface under "Device status".
Firmware update	Select the type of firmware update: TFTP or HTTP
Firmware update (pop-up window)	
Upload protocol	Choose whether the firmware update should be carried out via TFTP or HTTP.
Remote firmware filename	In the case of TFTP, the file name and path of the TFTP server must be specified here.
Current active image	<p>Display of the current active firmware version. Two firmware images can be stored on the WLAN device. The image displayed here is the active one.</p> <p>After a firmware update or when another firmware image is selected, the device must be restarted. If the "Automatic reboot after upload" checkbox is activated, this will be carried out automatically on completion of the update.</p>
Next active image	Another firmware image can be activated here. By default, there is only one firmware image on the device.
SD card state	<p>Shows whether an SD card is inserted in slot X4. The web page must be reloaded in order to display the current status.</p> <p>Note: only specially formatted SD cards from Phoenix Contact can be used.</p>
Perform action	<p>Load configuration: loads the device configuration stored on the SD card and executes it.</p> <p>Save configuration: Save device independent configuration: saves the device-independent parameters to the wlan_5100.cfg file on the SD card.</p> <p>Save client configuration: the device that is in access point mode can save the corresponding client configuration here. The SD card can then be used to configure the client that corresponds to the access point.</p>
Advanced configuration (pop-up window)	
Upload certificate	<p>Upload certificate via HTTP: select a file by clicking on "Upload a file" or drag the file over this button.</p> <p>Alternatively, the certificate can be uploaded via a TFTP server.</p>

Table 4-1 Parameter list for Information page [...]

Designation	Description
Direction	Download: from device to local PC (host) Upload: from PC (host) to device
TFTP server IP address	Enter the TFTP server address.
Current configuration	Download the configuration from the device by selecting the "wlan_5100.cfg" file.
Configuration name	The active configuration can be assigned a name here.
Customer default configuration	A customer-specific configuration can be downloaded to the device or from the device here. This configuration can also be activated via the MODE button.
Device independent configuration	A configuration can be downloaded to the device or from the device here, which only stores the general settings and not device-specific data.
Local Events	
Local events - digital input	
Status	Current state of the digital input (connection X3).
Reaction on digital input high event	Definition of the action that is triggered when the digital input is set to "High".
Local events - digital output	
Status	The digital output can be set here for test purposes via the web interface. To do this, "Access" must be activated.
Access	Activation of access via SNMP, CLI or the web interface. If this is not desired, access should be deactivated here. Access is then only possible via the event table.
Network Events	
Network events	
SNMP trap	In this area, you can select which system events should be recorded and on which interface they should be output. They can be output in the Syslog server or as an SNMP trap.
Add new IP address	Add a new trap receiver to the list.
Machine admin configuration	
Machine admin configuration	
Second SSID	This second SSID (network ID in addition to the SSID of the access point) is used to assign a service access to the access point. The SSID can be a maximum of 32 characters long. Letters, numbers, and the following characters are permitted: \$%&/()=?[]{}+*-_<>.
Passkey	For encryption of the "machine admin network". Note: for maximum security, a random alphanumeric string (up to 63 characters) should be used. Letters, numbers, and the following characters are permitted: \$%&/()=?[]{}+*-_<>. The password must be at least eight characters long.

Table 4-1 Parameter list for Information page [...]

Designation	Description
Grant access to IP	The IP address of the device in the network which should be accessible via "Machine Admin" mode (second SSID) is entered here. Note: It must be in the same address area as the WLAN 510x (see "Network configuration").
Diagnostics	
Channel allocation	
Graphic	In access point mode, the "Channel Allocation" web page displays a graphical overview of the channels occupied by WLAN systems. The data displayed is cleared when the web page is exited.
RSSI graph	
Graphic	In client mode, the "RSSI Graph" web page has a graphical RSSI logger which displays the time curve for the RSSI values on the client. The data displayed is cleared when the web page is exited.

5 Diagnostics

5.1 WLAN signal strength diagnostics on the client

If the FL WLAN 510x is in client or repeater mode, the current WLAN signal strength of the connected access point (or repeater) 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 an access point at various locations (e.g., mobile clients) or to determine the optimum alignment of an antenna in the case of a radio link.

In client mode, the current signal strength value of the connected access point (or repeater) is displayed graphically and dynamically in the “Diagnostics” – “RSSI Graph” menu. The RSSI (Radio Signal Strength Indication) value indicates the signal strength of the connected access point at the client location in dB.

The MAC address of the connected access point and the current WLAN signal strength (RSSI) are displayed at the top of the window.

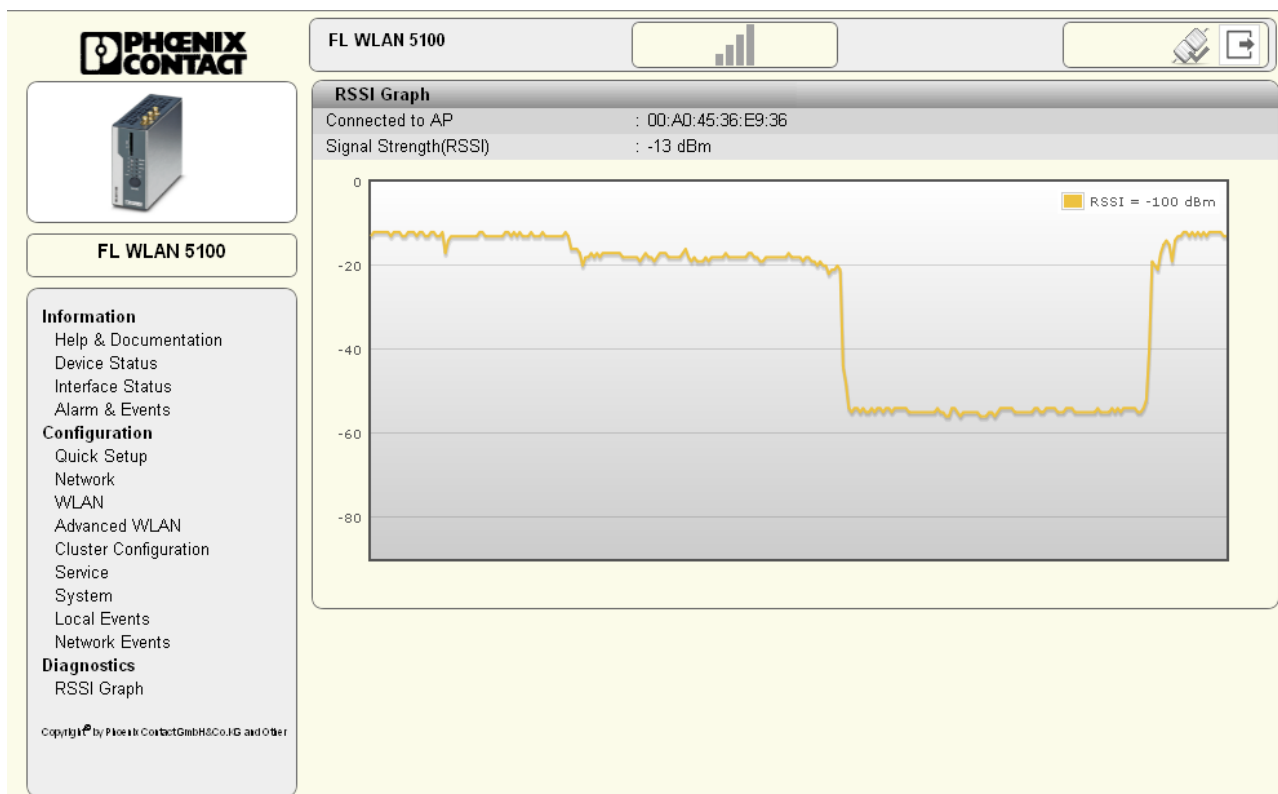


Figure 5-1 Display of the current WLAN signal strength on the client



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

Another option for dynamically displaying the signal strength of the access point on the client can be found in the "Interface Status – WLAN" menu. Here, the "Show signal bar" checkbox must be activated (see Figure 5-2). The checkbox can only be activated if a connection already exists.

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. Measurement is stopped when you exit the web page.

The screenshot shows the web interface for the FL WLAN 5100. On the left is a navigation menu with sections for Information, Configuration, and Diagnostics. The main content area is titled 'FL WLAN 5100' and contains two sections: 'Interface Status - LAN' and 'Interface Status - WLAN'. The WLAN section includes a 'Show signal bar' checkbox which is checked. Below the status tables, there is a bar graph showing the current signal strength (RSSI) as -45dBm, with a range of -50dBm to -25dBm.

Interface Status - LAN	
IP Address	: 192.168.0.251
Network Mask	: 255.255.255.0
Default Gateway	: 0.0.0.0
Nameserver Address	: 0.0.0.0
IP Assignment	: static
MAC Address	: 00:A0:45:36:EA:06
LAN Status Port 1	: 100baseT full duplex
LAN Status Port 2	: no link

Interface Status - WLAN	
Radio Status	: enabled
Operating Mode	: Client (FTB - Fully Transparent Bridge)
Connect State	: Accesspoint: 00:A0:45:36:E9:B6
Network SSID	: PxC_Messung
Datarate	: 130 MBit
Signal Strength(RSSI)	: -27 dBm <input checked="" type="checkbox"/> Show signal bar
Long Distance mode	: normal
Current TX power	: 17 dBm
Channel	: 11
Security Mode	: WPA2-PSK

Current Signal Strength(RSSI) (?) -45dBm
 Signal Strength min/avg/max (?) -50dBm/-30dBm/-25dBm

Figure 5-2 Display of the current signal strength as a bar graph

5.2 Diagnostics of WLAN channel assignment on the access point

If the FL WLAN 510x is in access point 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 in a graphic. In this way, you can find a free channel for your own WLAN network, for example.

In access point mode, the WLAN networks that are within range are displayed in the “Diagnostics” – “Channel Allocation” menu when you click on “Scan”.

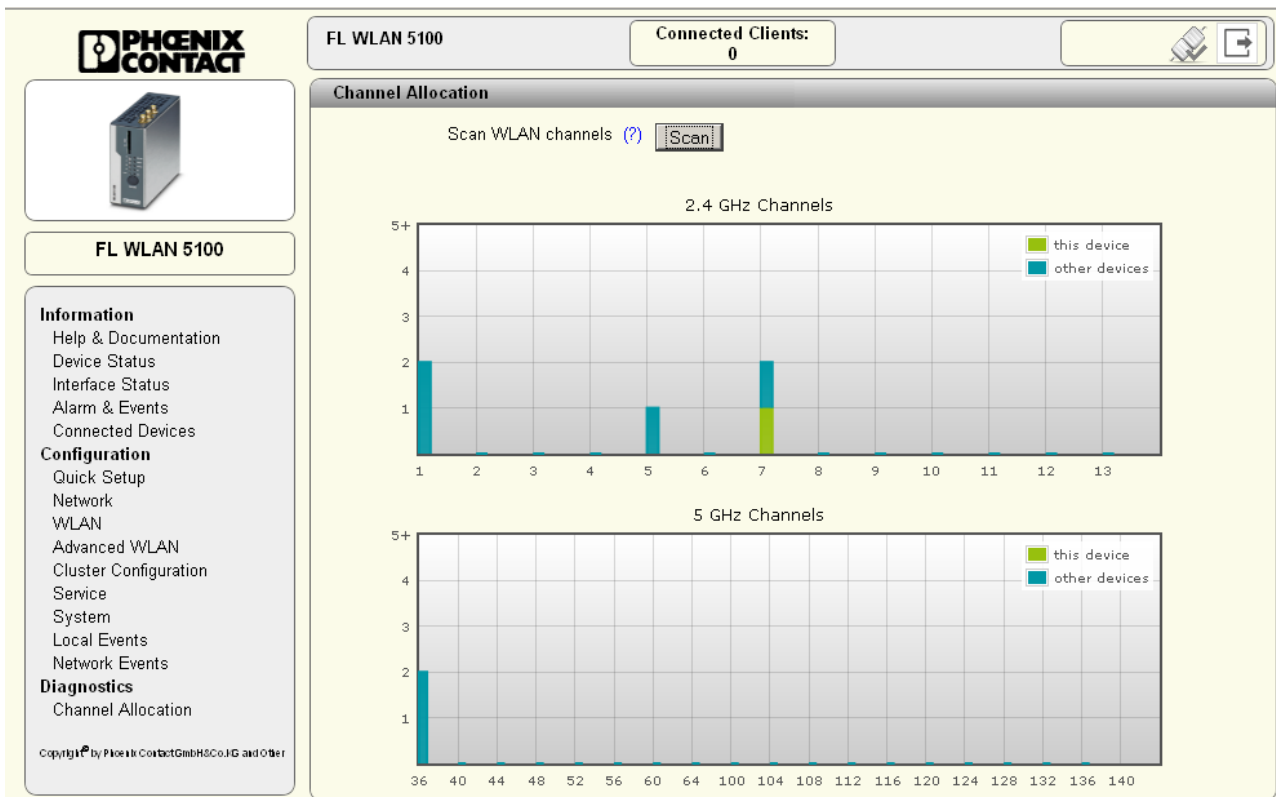


Figure 5-3 Display of WLAN channel assignment on the access point

6 Technical data

General data	
Function	WLAN Ethernet access point/client/repeater
Housing dimensions (width x height x depth) in mm	
External dimensions without antenna connections	40 x 100 x 109
External dimensions with antenna connections	40 x 109 x 109
Permissible operating temperature	-25°C to 60°C (extended temperature range available on request)
	<div style="border: 1px solid black; padding: 5px; display: inline-block;">  <p>At very low temperatures, there may be a delay in the start up of the device when you operate the FL WLAN 510x in the extended temperature range from -40°C to +60°C. The supply voltage should not fall below 12 V DC.</p> </div>
Permissible storage temperature	-40°C to 80°C
Degree of protection	IP20
Humidity	
Operation	10% to 95%, non-condensing
Storage	10% to 95%, non-condensing
Air pressure	
Operation	800 hPa to 1080 hPa, up to 2000 m above sea level
Storage	660 hPa to 1080 hPa, up to 3500 m above sea level
Mounting position	Perpendicular to a DIN rail
Connection to protective earth ground	By means of the DIN rail
Configuration	Web-based management via http or https, SNMPv2/v3, CLI via Telnet/SSH, password-protected
Weight	418 g
Supply voltage	
Connection	Via MINI-COMBICON; maximum conductor cross section = 1.5 mm ²
Nominal value	24 V DC/PELV
Permissible voltage range	10 V DC to 36 V DC
Current consumption at 24 V	200 mA
Power over Ethernet	
Protection class	III, IEC 61140, EN 61140, VDE 0140-1
Interfaces	
RJ45 Ethernet interface	
Number	2
Connection format	RJ45 socket on the device
Data transmission speed	10/100 Mbps
Segment length	100 m
IP address assignment	BootP
Wireless interface	
Antenna connection	3 x RSMA female

FL WLAN 510x

Interfaces [...]	
Wireless standards for FL WLAN 5100	IEEE 802.11a/b/g/h/n Automatic or manual channel selection 2.4 GHz: 13 channels according to 802.11b/g 5 GHz: up to 19 channels according to 802.11a according to standard 802.11h
Wireless standards for FL WLAN 5101	IEEE 802.11a/b/g/h/n Automatic or manual channel selection 2.4 GHz: 11 channels according to 802.11b/g 5 GHz: up to 9 channels according to 802.11a
Maximum transmission power at the RSMA connection	For 802.11a: 20 dBm at 6 Mbps, 18 dBm at 54 Mbps For 802.11b: 19 dBm For 802.11g: 19 dBm at 6 Mbps, 18 dBm at 54 Mbps For 802.11an: max. 19 dBm at MCS 0, 15 dBm at MCS 15 For 802.11gn: max. 18 dBm at MCS 0, 15 dBm at MCS 15
Receiver sensitivity at the RSMA connection	For 802.11a: -84 dBm at 54 Mbps, -97 dBm at 6 Mbps For 802.11b: -97 dBm at 11 Mbps, -97 dBm at 1 Mbps For 802.11g: -84 dBm at 54 Mbps, -97 dBm at 6 Mbps For 802.11n: -76 dBm at MCS15, -97 dBm at MCS0
Frequency range for FL WLAN 5100	2.4 to 2.48 GHz (IEEE 802.11b/g) 5.15 to 5.35 GHz/5.47 to 5.725 GHz (IEEE 802.11a/h)
Frequency range for FL WLAN 5101	2.4 to 2.48 GHz (IEEE 802.11b/g) 5.15 to 5.35 GHz/5.725 to 5.85 GHz (IEEE 802.11a)
Modulation method	802.11b: DSSS, 802.11 a/g/n: OFDM
Roaming	Supports roaming in client mode
Antennas	3 x RSMA connection, no antennas supplied as standard
Impedance	50 Ohm
Digital input	
Number	1
Logic "1" voltage level	> 10 V DC to 36 V DC
Logic "0" voltage level	< 5 V DC
Digital output	
Number	1
Output voltage	= supply voltage minus 1 V
Output current	0.5 A, maximum

Filter/encryption	
Encryption/authentication	None WPA/PSK and WPS2/PSK, WPA/PSK 802.11i with TKIP or AES/CCMP WPA/RADIUS with TKIP or AES/CCMP, WPA/RADIUS and WPA2/RADIUS

Mechanical tests	
Shock test according to DIN EN 60068-2-29	25g, when there is a half-wave of 30 ms
Vibration resistance according to DIN EN 60068-2-6	Operation: 5g, 10 - 500 Hz

Conformance with EMC directives for FL WLAN 5100	
Noise emission according to EN 55022	Class B
Radio interference field strengths according to EN 55022	Class a
Electrostatic discharge (ESD) according to EN 61000-4-2	Contact discharge: ±6 kV Air discharge: ±8 kV
Electromagnetic fields according to IEC 61000-4-3	10 V/m; Criterion A

Conformance with EMC directives for FL WLAN 5100

Conducted interference according to IEC 61000-4-6	10 V _{RMS} ; Criterion A
Fast transients (burst) according to IEC 61000-4-4	Data lines: 1 kV; Criterion B Power supply lines: 0.5 kV; Criterion B
Surge voltages according to IEC 61000-4-5	Data lines: ±2.2 kV asymmetrical; Criterion B Power supply lines: ±2.2 kV symmetrical/asymmetrical; Criterion B

Approvals for FL WLAN 5100

Compliance with the "Safety of information technology equipment" test specifications	DIN EN 60950 (VDE 0805, IEC 950)
--	----------------------------------

Differences between this version and previous versions of the user manual

- Rev. 00: no differences, initial version
- Rev. 01: valid for firmware Version 1.50 or later
- Rev. 02: smaller adaptations
- Rev. 03: valid for firmware Version 1.60 or later

6.1 Ordering data

Description	Order designation	Order No.
Access point, ETSI approval	FL WLAN 5100	2700718
Access point, FCC approval, only for use in the USA and Canada	FL WLAN 5101	2701093
Mounting bracket/panel adapter	FL WLAN 5100 PA	2701092
SD memory card	SD FLASH 512 MB	2988146
IP65 protective housing with three dual-band antennas (for 2.4 GHz and 5 GHz) and three connecting cables (access point not included), plus a 144 mm long DIN rail	FL RUGGED BOX OMNI-1	2701430
Control box for rugged construction of wireless systems for industrial applications, IP65, 25 x 18 x 13 cm, polycarbonate material, gray, drilled, including DIN rail, plugs, and screw connections, without devices	FL RUGGED BOX	2701204
Control box set for constructing wireless systems for industrial applications, including three 2.4/5 GHz, IP65 omnidirectional antennas that can be directly screwed on, with DIN rail, plugs, and screw connections, with 100 ... 240 V power supply unit, without devices	FL RUGGED BOX OMNI-2	2701439
Control box set for constructing wireless systems for industrial applications, including panel antenna and 3m antenna cable for 2.4/5 GHz, IP65, with DIN rail, plugs, and screw connections, with 100 ... 240 V power supply unit, without devices	FL RUGGED BOX DIR-1	2701440
Omnidirectional antenna, 2.4 GHz/5 GHz, 2.5/5 dBi gain, linear vertical polarization, 2.4 GHz h/v 360°/30°, 5 GHz h/v 260°/16° opening angle, N (male), IP68	ANT-OMNI-2459-02	2701408
Omnidirectional antenna with protection against vandalism, 2.4 GHz, 3 dBi gain, IP55 protection, 1.5 m cable length, RSMA connection (male), h/v 360°/85° opening angle	RAD-ISM-2400-ANT-VAN-3-0-RSMA	2701358

Description [...]	Order designation	Order No.
Omnidirectional antenna, 2,4 GHz, 2 dBi, linear vertical, 1.5 m cable, RSMA (male), IP65, 50 Ω impedance	RAD-ISM-2400-ANT-OMNI-2-1-RSMA	2701362
Omnidirectional antenna with protection against vandalism, 2.4 GHz, 3 dBi gain, IP55 protection, 1.5 m cable length, SMA connection (male), h/v 360°/85° opening angle	RAD-ISM-2400-ANT-VAN-3-0-SMA	2885867
Omnidirectional antenna with protection against vandalism, 2.4 GHz, 3 dBi gain, IP55 degree of protection, 1.5 m cable length, MCX connection (male), h/v 360°/85° opening angle	RAD-ISM-2400-ANT-VAN-3-1-MCX	2885702
Mounting material for wall mounting the omnidirectional antenna with protection against vandalism	RAD-ANT-VAN-MKT	2885870
Omnidirectional antenna, 2.4 GHz, 6 dBi, linear vertical, h/v 360°/20° opening angle, N (female), IP65, salt water resistant	RAD-2400-ANT-OMNI-6-0-SW	2903219
Dual-band omnidirectional antenna with protection against vandalism; IP68 protection; frequency band/gain: 2.4 GHz/up to 6 dBi, 5 GHz/up to 8 dBi; EN 50155; temperature range: -40°C to +80°C; N (f) connection; 1 m long adapter cable, N (m) - SMA (m) connection	RAD-ISM-2459-ANT-FOOD-6-0	2692526
Panel antenna, 2.4/5 GHz, 9 dBi, linear vertical, N (female), IP67	ANT-DIR-2459-01	2701186
Panel antenna, 5 GHz, 9 dBi, +/- 45° dual slant, h/v 70°/60° opening angle, 2 x N (female), IP67	ANT-DIR-5900-01	2701348
Omnidirectional antenna, 5 GHz, 5 dBi gain, linear vertical polarization, h/v 360°/25° opening angle, N (female), IP64	ANT-OMNI-5900-01	2701347
Parabolic antenna, IP65 protection, 19 dBi gain, linear vertical, N (female) connection, 50 Ω impedance, h/v 17°/11° opening angle	RAD-ISM-2400-ANT-PAR-19-0	2867885
Panel antenna, 5 GHz, 18 dBi gain, N (female) connection, IP55	RAD-ISM-5000-ANT-PAR-18-N	5606613
Parabolic antenna, 5 GHz, 22 dBi gain, N (female) connection, IP55	RAD-ISM-5000-ANT-PAR-22-N	5606174
Adapter cable, pigtail 50 cm, N (female) -> RSMA (male), insertion loss 0.75 dB at 2.4 GHz; 1.25 dB at 5 GHz, impedance 50 ohms	RAD-PIG-EF316-N-RSMA	2701402
Antenna cable, 0.5 m in length; N (male) -> RSMA (male), impedance 50 ohms	RAD-PIG-RSMA/N-0.5	2903263
Antenna cable, 1 m in length; N (male) -> RSMA (male), impedance 50 ohms	RAD-PIG-RSMA/N-1.0	2903264
Antenna cable, 2 m in length; N (male) -> RSMA (male), impedance 50 ohms	RAD-PIG-RSMA/N-2.0	2903265
Antenna cable, 3 m in length; N (male) -> RSMA (male), impedance 50 ohms	RAD-PIG-RSMA/N-3.0	2903266
Antenna cable, 3 m in length; N (male) -> N (male), attenuation approx. 0.45 dB at 2.4 GHz; impedance 50 ohms	RAD-CAB-EF393- 3M	2867649
Antenna cable, 5 m in length; N (male) -> N (male), attenuation approx. 0.45 dB at 2.4 GHz; impedance 50 ohms	RAD-CAB-EF393- 5M	2867652
Antenna cable, 10 m in length; N (male) -> N (male), attenuation approx. 0.45 dB at 2.4 GHz; impedance 50 ohms	RAD-CAB-EF393- 10M	2867665
Antenna cable, 15 m in length; N (male) -> N (male), attenuation approx. 0.45 dB at 2.4 GHz; impedance 50 ohms	RAD-CAB-EF393- 15M	2867634

Description [...]	Order designation	Order No.
Adapter, RSMA (male) -> SMA (female); insertion attenuation <0.3 dB at 2.4 GHz	RAD-ADP-RSMA/F-SMA/F	2884538
Attachment plug with LAMBDA/4 technology as surge protection for coaxial signal interfaces. Connection: N connectors (socket/socket).	CN-LAMBDA/4-5.9-BB	2838490
Vulcanizing sealing tape for external protection of adapters, cable connections, etc. against the effects of weather, roll length: 3 m	RAD-TAPE-SV-19-3	2903182
COMBICON plug	MC 1,5/4-ST-3,5	1840382
Gray RJ45 plug set for linear cable (2 pieces)	FL PLUG RJ45 GR/2	2744856
Green RJ45 plug set for crossed cable (2 pieces)	FL PLUG RJ45 GN/2	2744571
Assembly tool for RJ45 plugs	FL CRIMPTOOL	2744869
Factory Manager startup/diagnostics software	FL SWT	2831044
Network monitoring with HMI/SCADA systems	FL SNMP OPC SERVER	2832166
Patchbox 8 x RJ45 CAT5e, pre-assembled, can be retrofitted	FL PBX 8TX	2832496
Patchbox 6 x RJ45 CAT5e and 4 SC-RJ, glass, pre-assembled, can be retrofitted	FL PBX 6TX/4FX	2832506
Patch cable, CAT5, pre-assembled, 0.3 m long, 10 pieces	FL CAT5 PATCH 0,3	2832250
Patch cable, CAT5, pre-assembled, 0.5 m long, 10 pieces	FL CAT5 PATCH 0,5	2832263
Patch cable, CAT5, pre-assembled, 1.0 m long, 10 pieces	FL CAT5 PATCH 1,0	2832276
Patch cable, CAT5, pre-assembled, 1.5 m long, 10 pieces	FL CAT5 PATCH 1,5	2832221
Patch cable, CAT5, pre-assembled, 2.0 m long, 10 pieces	FL CAT5 PATCH 2,0	2832289
Patch cable, CAT5, pre-assembled, 3.0 m long, 10 pieces	FL CAT5 PATCH 3,0	2832292
Patch cable, CAT5, pre-assembled, 5.0 m long, 10 pieces	FL CAT5 PATCH 5,0	2832580
Patch cable, CAT5, pre-assembled, 7.5 m long, 10 pieces	FL CAT5 PATCH 7,5	2832616
Patch cable, CAT5, pre-assembled, 10.0 m long, 10 pieces	FL CAT5 PATCH 10	2832629

PHOENIX CONTACT GmbH & Co. KG
 Flachmarktstr. 8
 32825 Blomberg
 Germany



+ 49 - (0) 52 35 - 3-00



+ 49 - (0) 52 35 - 3-4 12 00



www.phoenixcontact.com



Worldwide locations:
www.phoenixcontact.com/salesnetwork

HOTLINE:

If there are any problems that cannot be solved using this documentation, please call our hotline:



+ 49 - (0) 52 81 - 946 2888

7 Technical appendix

7.1 Simple Network Management Protocol (SNMP)

7.1.1 General function

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 relevant Management Information Base (MIB) and a manager. The manager is a software tool that is executed on a network management station. The agents are located inside switches, bus terminal modules, routers and other devices that support SNMP. The task of the agents is to collect and provide data in the MIB. The manager regularly requests and displays this information. The devices can be configured by writing data from the manager to the MIB. In the event of an emergency, the agents can also send messages (traps) directly to the manager.



All configuration modifications, which are to take effect after a device restart, must be saved permanently.

SNMP interface

All managed Factoryline components have an SNMP agent. This device agent manages Management Information Base II (MIB 2) according to RFC1213 and private SNMP objects from the Phoenix Contact MIB (PXC-WLAN-MIB).

Network management stations, such as a PC with Factory Manager, can read and modify configuration and diagnostic data from network devices via the Simple Network Management Protocol. In addition, any SNMP tools or network management tools can be used to access Factoryline products via SNMP. To do this, the MIBs supported by the relevant device must be made available to the SNMP management tools.

On the one hand, these are globally valid MIBs, which are specified and described in RFCs (Request for Comments). This includes, for example, MIB2 according to RFC1213, which is supported by all SNMP-compatible network devices. On the other hand, manufacturers can specify their own SNMP objects, which are then assigned to a private manufacturer area in the large SNMP object tree. Manufacturers are then responsible for their own private (enterprise) areas, i.e., they must ensure that only one object is assigned to an object ID (object name and parameters) and can be published. If an object is no longer needed, it can be labeled as “expired”, but it cannot be reused with other parameters under any circumstances.

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

Reading SNMP objects is not password-protected. However, a password is required for read access in SNMP, but this is set to “public”, which is usual for network devices, and cannot be modified. By default upon delivery, the password for write access is “private” and can be changed by the user.



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

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

Management Information Base (MIB)

Database which contains all the data (objects and variables) required for network management.

Agent

An agent is a software tool, which 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 a request of a manager or on the occurrence of a specific event, the agent transmits the collected information to the management station.

Schematic view of SNMP management

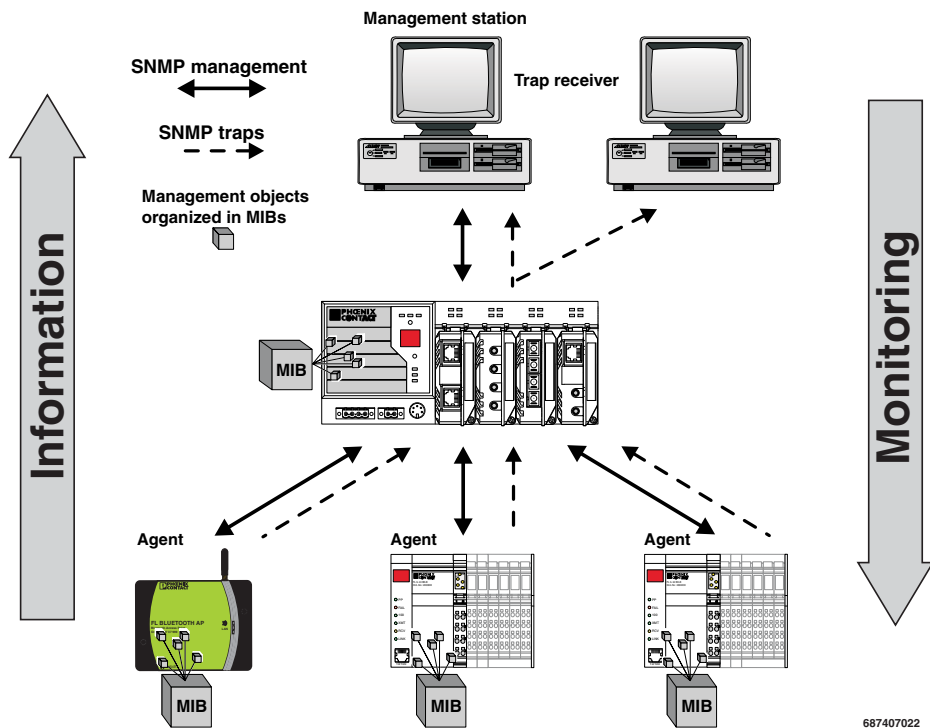


Figure 6-1 Schematic view of SNMP

687407022

7.1.2 Supported MIBs and SNMP versions

The device supports SNMP Versions V2 and V3.

The device supports the following MIBs: MIB II and the “PXC-WLAN5100 MIB”. The full complement of MIB files can be found at www.phoenixcontact.com or MIBs can be downloaded under “Help & Documentation” in web-based management for the device.

Up to ten trap receivers can be configured.

7.2 Setting the system time and using SNTP

7.2.1 General information on SNTP

The Simple Network Time Protocol (SNTP) is defined in RFC 4330 (SNTP clients in automation technology) and is used to synchronize the internal system time with any NTP server, which represents the “timer”, i.e., the universal time. The aim is to synchronize all the components in a network with the universal time and to thereby create a uniform time base.

Time synchronization provides valuable assistance when evaluating error and event logs, as the use of time synchronization in various network components enables events to be assigned and analyzed more easily. Clients should therefore only be activated at the most extreme points of an NTP network.

Time synchronization is carried out at fixed synchronization intervals known as polling intervals. The client receives a correction time by means of an SNTP server, with the packet runtime for messages between the client and server being integrated in the time calculation in the client. The local system time of the client is thus constantly corrected. Synchronization in the NTP is carried out in Universal Time Coordinated (UTC) format.

The current system time is displayed as Universal Time Coordinates (UTCs). This means that the displayed system time corresponds to Greenwich Mean Time. The system time and the “UTC offset” provide the current local time. The device supports the use of the SNTP protocol only in client mode, i.e., devices or other network components only ever receive a time from a time server, but do not transmit their own times.

- Each client synchronizes its system time with that of an SNTP server
- Time synchronization is carried out at fixed synchronization intervals
- The local system time of the client is thus constantly corrected.
- Synchronization is carried out in Universal Time Coordinated (UTC) format

The corresponding web page is located under “Configuration/Service/System Time”.

Figure 6-2 “System Time” web page



For the times in the event table, for example, make sure that the system time corresponds to Greenwich Mean Time. The current local time is based on the system time and the “UTC offset”. Where necessary, the switch between daylight savings and standard time must be taken into consideration.

Configuration sequence

- Activate the SNTP function (enable)
- Set the desired time zone with “UTC offset”
- Select the operating mode. Choose between:
Unicast mode: the client receives its time from a fixed SNTP primary server.
Broadcast mode: the client receives its time from broadcast messages, which were transmitted by an NTP server and sent to several clients.



Manual configuration: the module has a realtime clock with buffer battery. This means that the clock continues running even without an external power supply. Manual configuration is recommended for the certificate to be validated. Please note that it is not possible to automatically switch between daylight savings and standard time.