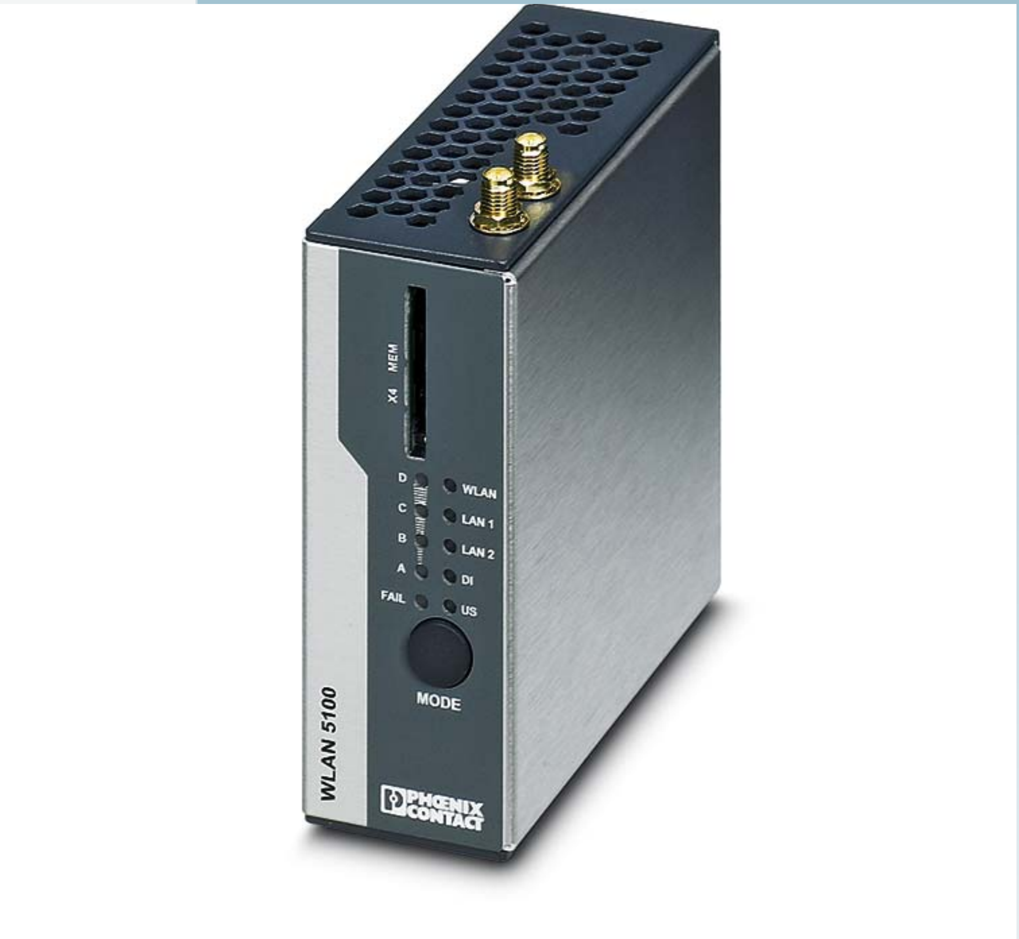


FL WLAN 511x

User manual

UM EN FL WLAN 511x

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual
FL WLAN 511x

2018-09-25

Designation:	UM EN FL WLAN 511x
Revision:	01
Order No.:	—

This user manual is valid for:

Designation	Order No.
FL WLAN 5110	1043193
FL WLAN 5111	1043201

Please observe the following information

User group of this manual

The use of products described in this user manual is oriented exclusively to:

- Electrically skilled persons or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.
- Qualified application programmers and software engineers, who are familiar with the safety concepts of automation technology as well as applicable standards and other regulations.

Explanation of symbols used and signal words

⚠ This symbol indicates hazards that could lead to personal injury. 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 by 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.

ℹ 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 General Terms and Conditions can be found on the Internet at:
phoenixcontact.com.

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

Subsidiaries

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

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY

Should you have any suggestions or recommendations for improving the content and layout of our user manual, please send your comments to:
tecdoc@phoenixcontact.com

General Terms and Conditions of Use for technical documentation

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

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

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

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

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

Note: Installation only by qualified specialist personnel

The product may only be installed, started up, and maintained by qualified specialist personnel who have been authorized to do so by the system operator. An electrician is someone who because of their education, experience, and instruction and their knowledge of relevant standards is able to assess all planned activities and recognize any possible dangers. Specialist personnel must read and understand this document and follow the instructions. You must comply with the applicable national regulations regarding the operation, function tests, repair, and maintenance of electronic devices.

WLAN 5110 – Industrial WLAN

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

- Reliable, safe, and fast communication with mobile or moving automation and production systems.
- Real-time access to network resources and maintenance information for increasing productivity and speeding up decision-making processes.

The WLAN modules in the 511x series offer maximum reliability, data throughput, and range. The WLAN 511x combines robust industrial technology with high 802.11n performance and modern MIMO (multiple input, multiple output) antenna technology in extremely compact metal housing. MIMO technology significantly increases the robustness, speed, and range of wireless communication. This is particularly noticeable under challenging industrial conditions.

A special feature of the WLAN 511x 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 5110 and the FL WLAN 5111.

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, and 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 to 36 V DC), 2 x RJ45 ports for LAN
- Configuration via WBM, SNMP, and CLI via SSH/Telnet
- Security functions in acc. with 802.11i: WPA2, WPA-PSK, TKIP, and AES
- Connections for two antennas (MIMO technology/connection method: RSMA/not supplied as standard)

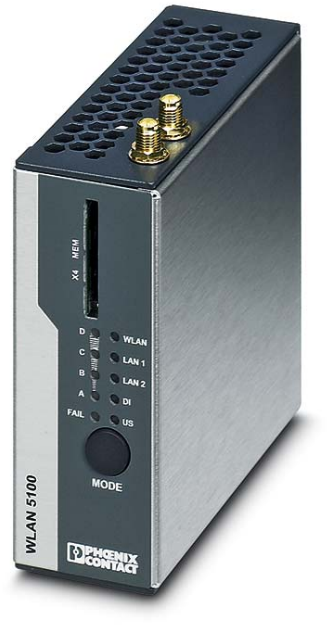


Figure 1-1 FL WLAN 511x

1.2 Country approvals and standards

1.2.1 FL WLAN 5110

The FL WLAN 5110 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 satisfies all the requirements of Directive 2014/53/EU:

– Additional information can be found in the manufacturer's declaration which is available in the e-shop at phoenixcontact.net/product/1043193.

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

> A current list including the national approvals is available in the e-shop at phoenixcontact.net/product/1043193.

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

Approvals for other countries are possible on request.

Phoenix Contact hereby declares that this wireless system complies with the basic requirements and other relevant regulations specified in Directive 2014/53/EU. The EU declaration of conformity can be accessed in the "Download" area via the following link: phoenixcontact.net/product/1043193.

1.2.2 Information on setting the equipment for using gain antennas

Compliance with regulations stipulates setting the transmission power to a level at which the emitted power does not exceed the permitted limit value. This value is 2.4 GHz for 20 dBm and 5 GHz for 23 dBm in Europe (EIRP). The following table lists the set value for Europe for the respective antenna under consideration of the antenna cable in the "Max. transmission power" column.

Table 1-1 Transmission power setting for FL WLAN 5110

Antenna	Frequency band in GHz	Gain in dBi	Antenna cable	Attenuation in dB	Max. transmission power in dBm
ANT-OMNI-2459-02 27 01 40 8	2.4	2.5	RAD-PIG-EF316-N-RSMA 2701402	1.0	16
	5	5		1.4	16
RAD-ISM-2400-ANT-VAN-3-0-RSMA 27 01 35 8	2.4	3	incl.	incl.	16
RAD-ISM-2400-ANT-OMNI-2-1-RSMA 27 01 36 2	2.4	2.1	incl.	incl.	16
RAD-ISM-2400-ANT-OMNI-6-0 28 85 91 9	2.4	6	RAD-PIG-RSMA/N-1.0* 2903264	0.8	15
ANT-OMNI-5900-01 27 01 34 7	5	5	RAD-PIG-RSMA/N-1.0* 2903264	1	16
ANT-DIR-2459-01 27 01 18 6	2.4	9	RAD-PIG-RSMA/N-1.0* 2903264	0.8	12
	5	9		1.1	11

Table 1-1 Transmission power setting for FL WLAN 5110

Antenna	Frequency band in GHz	Gain in dBi	Antenna cable	Attenuation in dB	Max. transmission power in dBm
ANT-DIR-5900-01 27 01 34 8	5	9	RAD-PIG-RSMA/N-1.0* 2903264	1.1	11
FL RUGGED BOX OMNI-1 27 01 43 0	2.4	2.5	RAD-PIG-EF316-N-RSMA 2701402	1	16
	5	5		1.4	16
FL RUGGED BOX OMNI-2 27 01 43 9	2.4	2.5	RAD-PIG-EF316-N-RSMA 2701402	1	16
	5	5		1.4	16
FL RUGGED BOX DIR-1 27 01 44 0	2.4	9	RAD-PIG-RSMA/N-3.0 2903266	2.4	12
	5	9		3.3	11

*When using the same cable type at a different length, the transmission power can be adapted in accordance with the cable losses.

1.2.3 FL WLAN 5111

The FL WLAN 5111 device, Order No. 1043201, can be used in the USA and Canada. It does not have CE approval and may not be operated in Europe. It is only available for export.

Furthermore, the following approvals have been performed and passed for the FL WLAN 5111 device (Order No. 1043201):

- FCC/CFR 47, Part 15 (USA)
- Radiocommunication Act R.S.C., 1985, c. R-2

1.2.3.1 FCC information

This device contains the following wlan module:

FCC ID	YG3-SXPCEAN2
IC-Nr	4720B-SXPCEAN2
HVIN (Hardware Version Identification Number)	SX-PCEAN2
FVIN (Firmware Version Identification Number)	1.0.3.0.2
PMN (Product Marketing Name)	SX-PCEAN2

NOTE:

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 or more 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.

NOTICE:

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

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

NOTICE:

This device complies with Part 15 of the FCC Rules and with Industry Canada licence-exempt RSS standard(s).

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.

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'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

NOTICE:

Changes or modifications made to this equipment not expressly approved by Phoenix Contact may void the FCC authorization to operate this equipment.

Information on radio frequency radiation exposure:

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Ce transmetteur ne doit pas etre place au meme endroit ou utilise simultanement avec un autre transmetteur ou antenne.

Table 1-2 Antenna list for use in USA and Canada

Antenna	Frequency band in GHz	Gain in dBi	Antenna cable	Attenuation in dB
ANT-OMNI-2459-02 27 01 40 8	2.4	2.5	RAD-PIG-EF316-N-RSMA 2701402	1.0
	5	5		1.4
RAD-ISM-2400-ANT-VAN-3-0-RSMA 27 01 35 8	2.4	3	incl.	incl.
RAD-ISM-2400-ANT-OMNI-2-1-RSMA 27 01 36 2	2.4	2.1	incl.	incl.
RAD-ISM-2400-ANT-OMNI-6-0 28 85 91 9	2.4	6	RAD-PIG-RSMA/N-1.0 2903264	0.8
ANT-DIR-2459-01 27 01 18 6	2.4	9	RAD-PIG-RSMA/N-1.0 2903264	0.8
	5	9		1.1
ANT-DIR-5900-01 27 01 34 8	5	9	RAD-PIG-RSMA/N-1.0 2903264	1.1

NOTE:

The use of antenna ANT-DIR-2459-01 is only allowed at a single chain operation on antenna port X5. Do not use this antenna at both antenna ports at the same time!

NOTE:

The FL WLAN 5111 (Ord-no. 1043201) operates on the non DFS channels only. It supports channel no. 36, 40, 44, 48, 149, 153, 157, 161, 165. Other channels cannot be selected.

1.3 Firmware

Table 1-3 Firmware functions

Firmware version	Functions
FW 3.x	First firmware version

Additional information on the latest firmware changes for the respective product can be found in the e-shop at phoenixcontact.com or at phoenixcontact.net/product/1043193.

2 Mounting/antenna configuration

2.1 Connections and operating elements

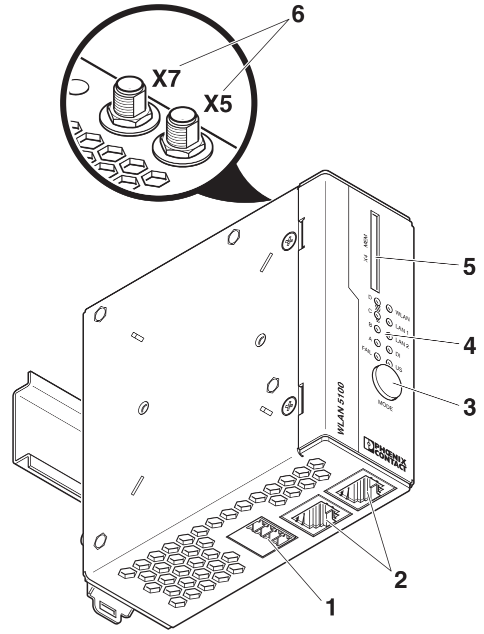


Figure 2-1 Connections and operating elements of the device

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

2.1.1 Electrical connection

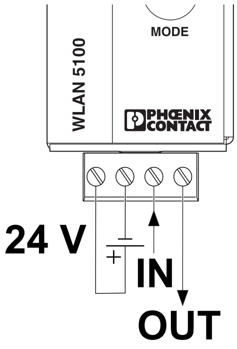


Figure 2-2 Connecting the supply voltage and the input/output

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 on the upper edge of the DIN rail, and snap the module into place by pushing it downward.

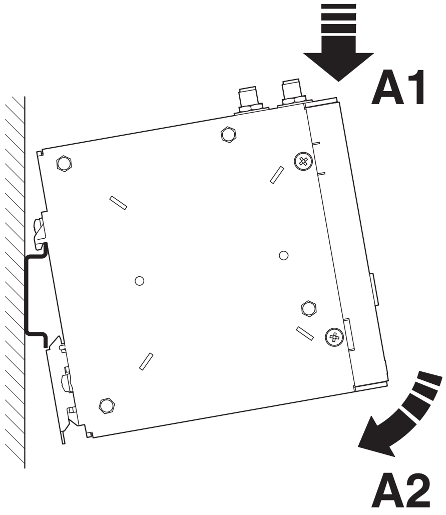


Figure 2-3 Snapping the module onto the DIN rail

2.1.2.2 Removal

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

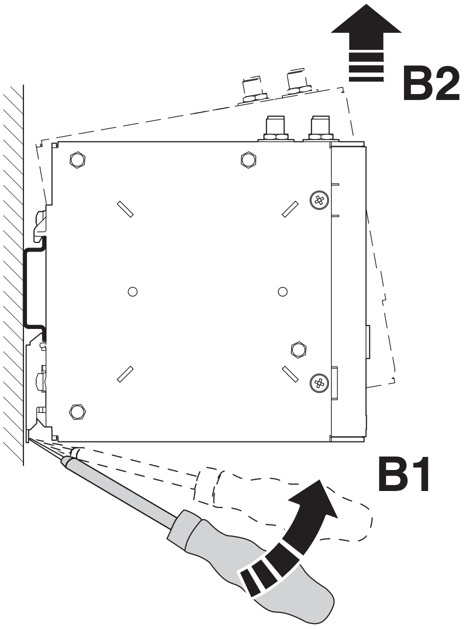


Figure 2-4 Removing the module from the DIN rail

2.1.2.3 Housing dimensions

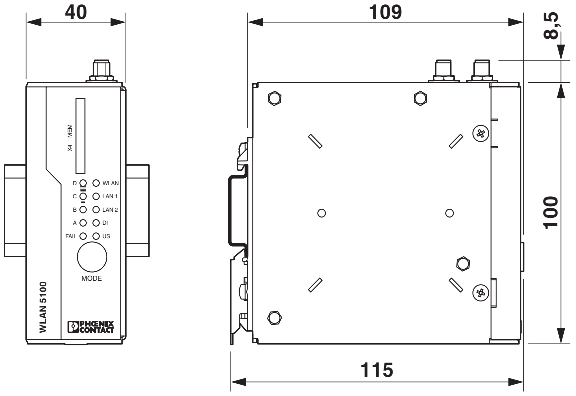


Figure 2-5 Housing dimensions without protruding parts in mm

2.1.3 Configuration of the antenna connections

NOTE: Damage to the device due to incorrect configuration

Always operate the device with the two antennas supplied or adapt the configuration accordingly if using fewer than two antennas.

The device is supplied ready for operation with two antennas by default. If you connect fewer antennas, you must configure the device accordingly in WBM. This can be done under “Advanced WLAN” -> “Antenna port configuration”.

Table 2-1 Configuration of the antenna connections

Number of antennas used	Designation of the antenna connection	Configuration
2 antennas	X5, X7	Default settings
1 antenna	X5	Configuration via WBM required

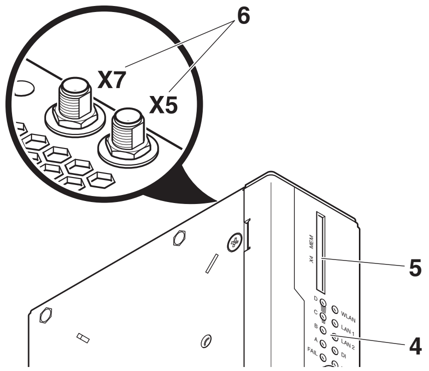


Figure 2-6 Assignment of the antenna connections

2.1.3.1 Antenna mounting distances

The WLAN 511x supports MIMO (multiple input, multiple output) antenna technology. Up to two antennas are used; they are connected to connections X5, 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.

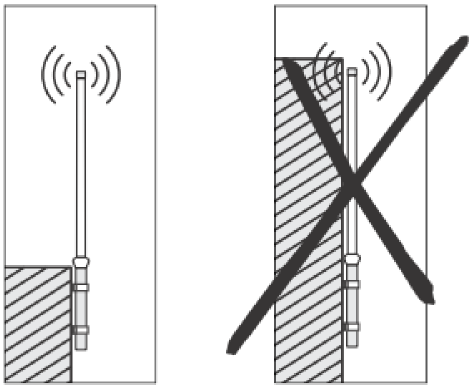


Figure 2-7 Correct and incorrect antenna mounting using an omnidirectional antenna as an example

Distance between the antennas

The distance between the two antennas of a device must be at least 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.

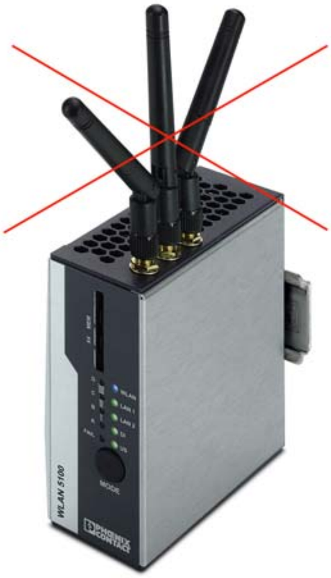


Figure 2-8 Do not screw several antennas onto the device

3 Startup and configuration

3.1 Safety and installation instructions

NOTE: Installation only by qualified personnel

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

NOTE: Electrostatic discharge

The devices contain components that can be damaged or destroyed by electrostatic discharge. When handling the devices, observe the necessary safety precautions against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and EN 61340-5-2.

NOTE: Statement regarding RF emission

This device should be installed and operated with a minimum distance of 20 cm between the emitter/antenna and your body.

NOTE: Demands on the power supply

The module is designed exclusively for operation with safety extra-low voltage (PELV/SELV).

NOTE: Do not open or modify the device. Do not repair the device yourself; replace it with an equivalent device instead. Repairs may only be carried out by the manufacturer. The manufacturer is not liable for damage resulting from noncompliance.

NOTE: Requirements for the current source

This device should only be operated with power supplies which meet the requirements of EN/IEC 60950-1 for limited power sources. Otherwise the device is to be operated in a housing which meets the requirements for fire protection enclosure according to EN/IEC 60950-1.

NOTE: Requirement for functional grounding

Mount the module on a grounded DIN rail. The module is grounded when it is snapped onto the DIN rail.

NOTE: Requirements for functional grounding in non-DIN rail mounting

Ensure proper (functional) grounding of the device.

NOTE: Requirement for mounting location

The prescribed mounting position is vertical on a horizontally mounted DIN rail. The vents may not be covered so that air can circulate freely. A gap of 3 cm between the vents of the housing is recommended.

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 or thermal stress that exceeds the specified thresholds.

3.2 Installation notes

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. Refer to the information in Section “Configuration of the antenna connections” on page 16.

Do not screw more than one omnidirectional antenna onto the device. The distance of the antenna sockets 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.

A typical startup of the WLAN device as an access point or client using the “Quick setup” feature is described below. 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 71.

3.3 Status and diagnostics indicators

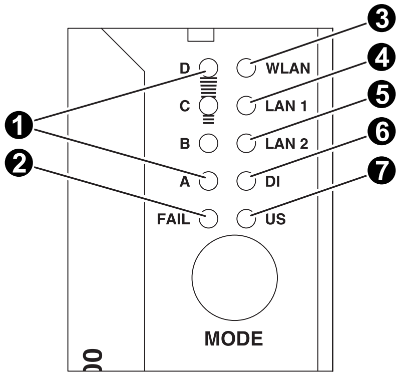


Figure 3-1 Status and diagnostics indicators

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 22.
   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 22).
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 22)
5. LAN2 status: green/yellow (see “Meaning of the LAN1/2 indicators” on Page 22)
6. DI: digital input set at connector X3 (see “Using the digital input and output” on Page 28)
7. US: supply voltage present

3.3.1 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
LAN2		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

3.3.2 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

3.4 Configuration using the MODE button

Typical operating settings for the FL WLAN 511x 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 23. A selection of the key settings is also available directly on the device.

3.4.1 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.

- Press 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 apply 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.

Table 3-3 Operating modes

Mode	Description	LEDs	A	B	C	D
1	Exit configuration mode without modifying the configuration.	A	●			
2	**Restore 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 via IP 192.168.0.254.	B+C		●	●	
7	**Restore 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	●			●

3.4.2 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 42.

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.

3.4.3 Connection to a PC

Proceed as follows to connect the WLAN 511x to your PC via the Ethernet interface without using BootP (default setting):

- Connect the device to a power supply.
- Press the MODE button immediately after booting (LEDs 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 511x receives the IP address 192.168.0.254.

3.4.4 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 of charge at phoenixcontact.net/products. The tool can also be found under “Help & Documentation” on the web page for the device, where it can be started directly.

Notes on BootP

During initial startup, the device sends 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 factory settings are restored, the device sends BootP requests until they are answered.

Requirements

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

3.4.5 Assigning the IP address 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 the “Run” button.

From the device:

- Set the device to mode 6 using the MODE button (see “Configuration using the MODE button” on page 22).
- 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.

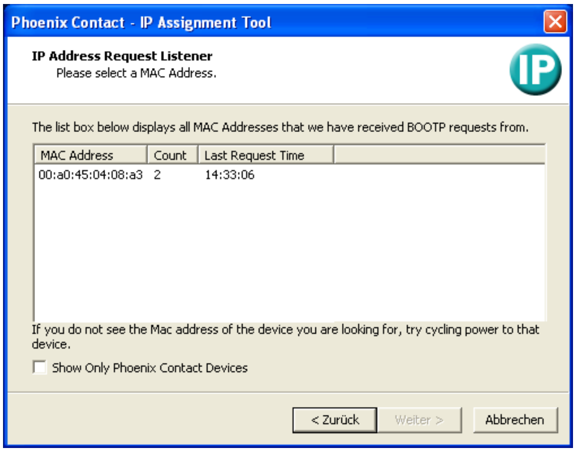
The program is mainly in English for international purposes. However, the program buttons change according to the country-specific settings.

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

- Click on the “Next” button.

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.



Phoenix Contact - IP Assignment Tool

IP Address Request Listener
Please select a MAC Address.

The list box below displays all MAC Addresses that we have received BOOTP requests from.

MAC Address	Count	Last Request Time
00:a0:45:04:08:a3	2	14:33:06

If you do not see the Mac address of the device you are looking for, try cycling power to that device.

□ Show Only Phoenix Contact Devices

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 want to assign an IP address.
- Click on the “Next” button.

Step 4: “Set IP Address”

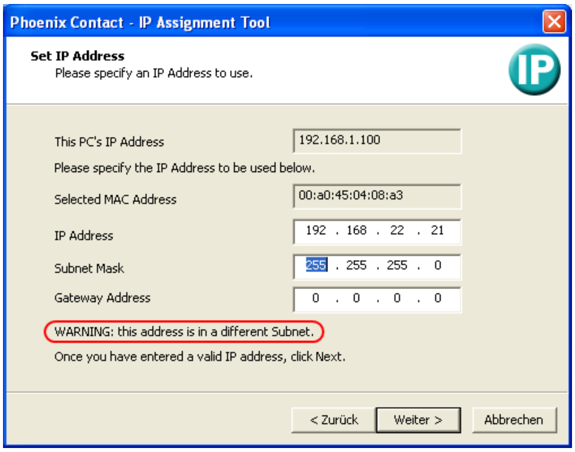
The following information is displayed in the window which opens:

– 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



Phoenix Contact - IP Assignment Tool

Set IP Address
Please specify an IP Address to use.

This PC's IP Address: 192.168.1.100

Please specify the IP Address to be used below.

Selected MAC Address: 00:a0:45:04:08:a3

IP Address: 192 . 168 . 22 . 21

Subnet Mask: 255 . 255 . 255 . 0

Gateway Address: 0 . 0 . 0 . 0

WARNING: this address is in a different Subnet.

Once you have entered a valid IP address, click Next.

Figure 3-3 “Set IP Address” window with incorrect settings

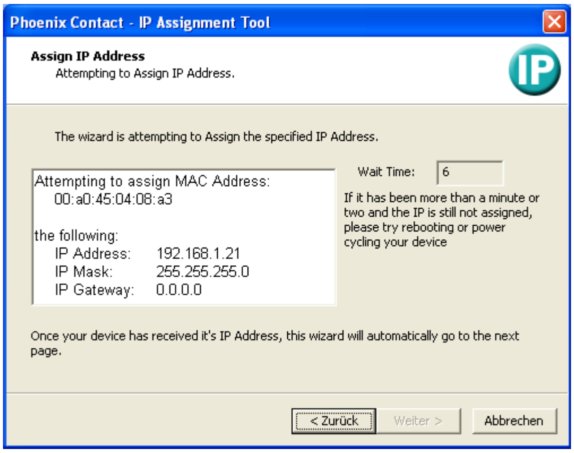
- Adjust the IP parameters according to your requirements.

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

- Click on the “Next” button and perform a voltage reset.

Step 5: “Assign IP Address”

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



Assign IP Address
Attempting to Assign IP Address.

The wizard is attempting to Assign the specified IP Address.

```
Attempting to assign MAC Address:
    00:a0:45:04:08:a3

the following:
    IP Address:     192.168.1.21
    IP Mask:        255.255.255.0
    IP Gateway:     0.0.0.0
```

Wait Time: 6

If it has been more than a minute or two and the IP is still not assigned, please try rebooting or power cycling your device

Once your device has received it's IP Address, this wizard will automatically go to the next page.

Figure 3-4 “Assign IP Address” window

Following successful transmission, the next window opens.

Step 6: completing 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 the “Back” button.

To exit IP address assignment:

- Click on the “Finish” button.

3.4.6 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.

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

Table 3-4 Function of the digital inputs/outputs [...]

Function	Digital input	Digital output
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

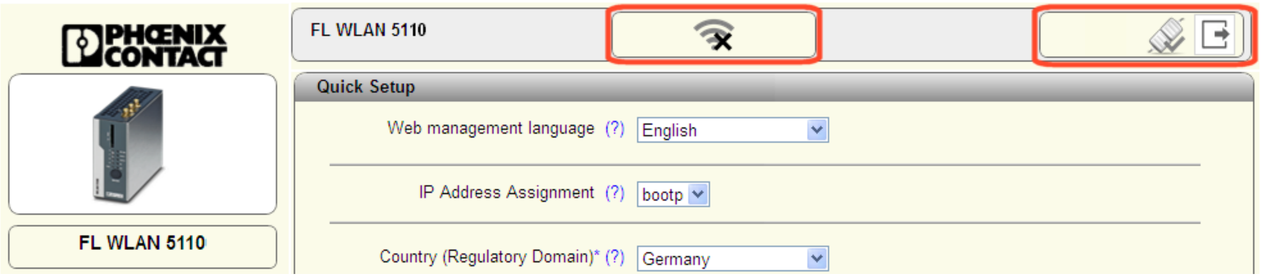
3.5 Startup via the web interface

WBM of the device is optimized for Mozilla Firefox.

3.5.1 General information in the web interface

3.5.1.1 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.



Web management language (?) English

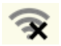
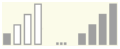
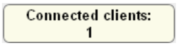
IP Address Assignment (?) bootp

Country (Regulatory Domain)* (?) Germany

Figure 3-5 Web page with overview icons

Meaning of the individual icons:

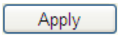
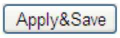
Table 3-5 Meaning of the icons

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

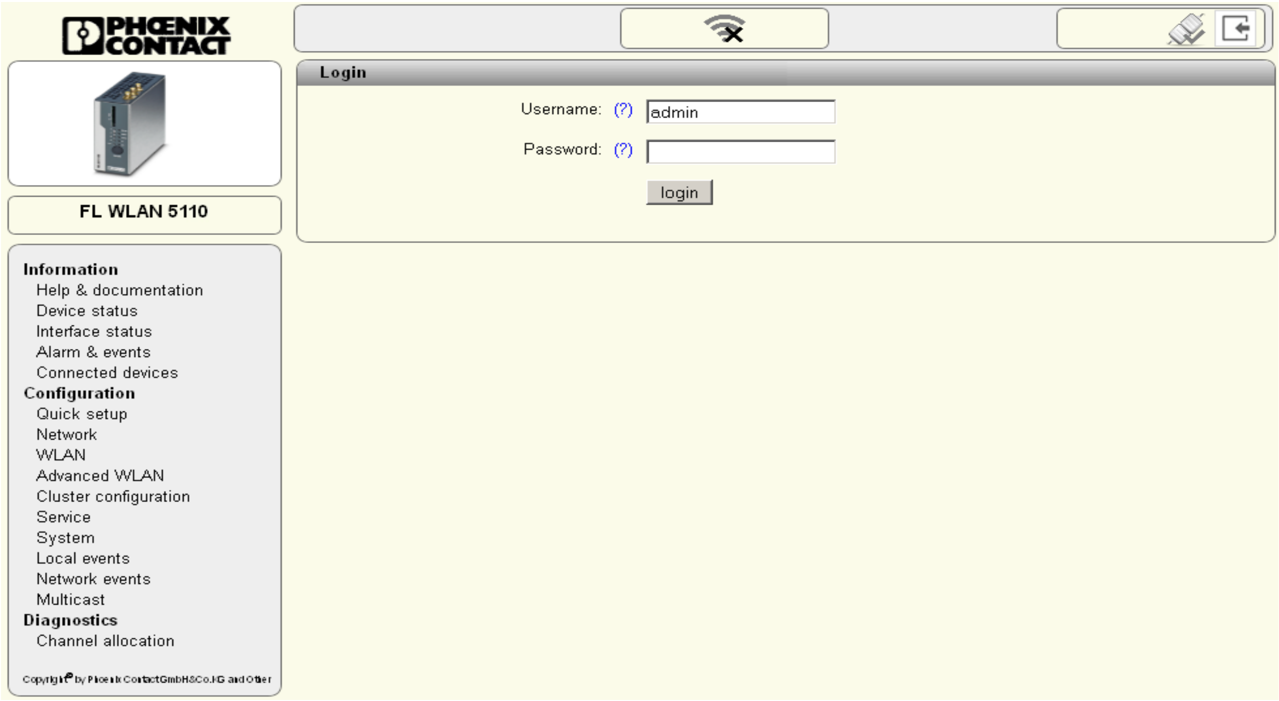
Icon	Meaning
	This button deletes the entries made since the last saved entry.
	This button applies the current settings, but does not save them.
	This button applies and saves the current settings.

3.6 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 22). 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 user name and “private” as the password.



Username: (?) admin

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 help text displayed when you move the mouse cursor over the (?) is shown in the selected language (only English at present).

IP parameter assignment

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

BootP: during initial startup, the device transmits BootP requests without interruption until it receives valid IP parameters. As soon as it receives a valid IP parameter, the device stops sending 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 IP parameters from a DHCP (Dynamic Host Configuration Protocol) server.

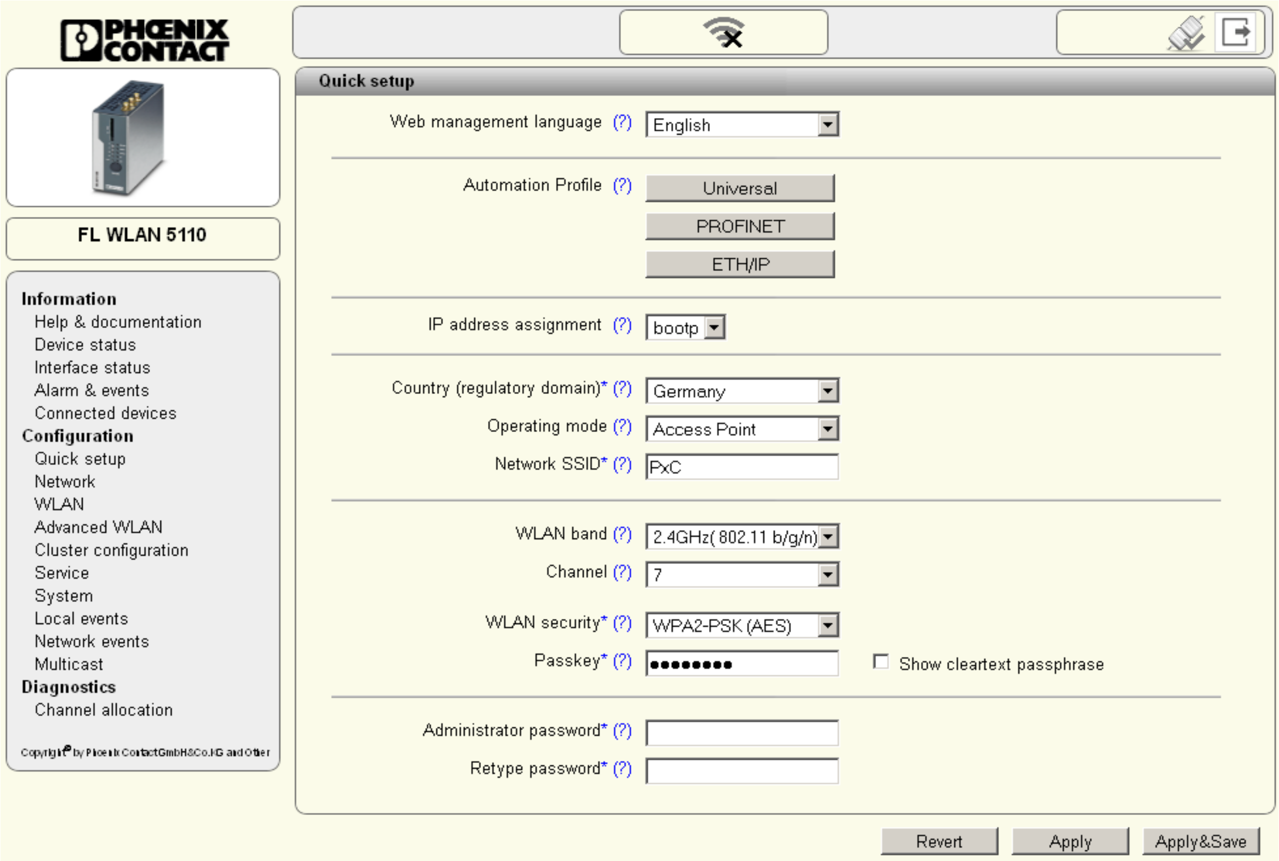
Country setting

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. Wireless approval is not necessarily available for each country that can be selected here.

Operating mode

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



Quick setup

Web management language (?) English

Automation Profile (?) Universal | PROFINET | ETH/IP

IP address assignment (?) bootp

Country (regulatory domain)* (?) Germany

Operating mode (?) Access Point

Network SSID* (?) PxC

WLAN band (?) 2.4GHz(802.11 b/g/n)

Channel (?) 7

WLAN security* (?) WPA2-PSK (AES)

Passkey* (?) ●●●●●●●● □ Show cleartext passphrase

Administrator password* (?)

Retype password* (?)

Figure 3-7 “Quick setup” web page

3.6.1 Operation as an access point

In access point mode, the FL WLAN 511x acts as the wireless interface in the overall network for one or more WLAN clients.

Automation Profile

There are three automation profiles which can be set by default in addition to the other settings required for WLAN.

If “PROFINET” is selected, “Profinet assistance mode” is activated. For details, please refer to Section “WLAN in PROFINET applications” on page 54. Please note that IP address assignment is set to DCP!

If “ETH/IP” is selected, enhanced multicast handling is activated. Details can be found in Section “EtherNet/IP™: optimizing multicast transmission” on page 55. Please observe that IP address assignment is switched to BootP!

If “Universal” is selected, “Profinet assistance mode” and “Multicast Enhancements” are disabled.

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, spaces, and the following characters are permitted: !$%@&/()=?[]{}+*-_<>

WLAN band

The radio 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 “Outdoor” check box must be selected.

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 set 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

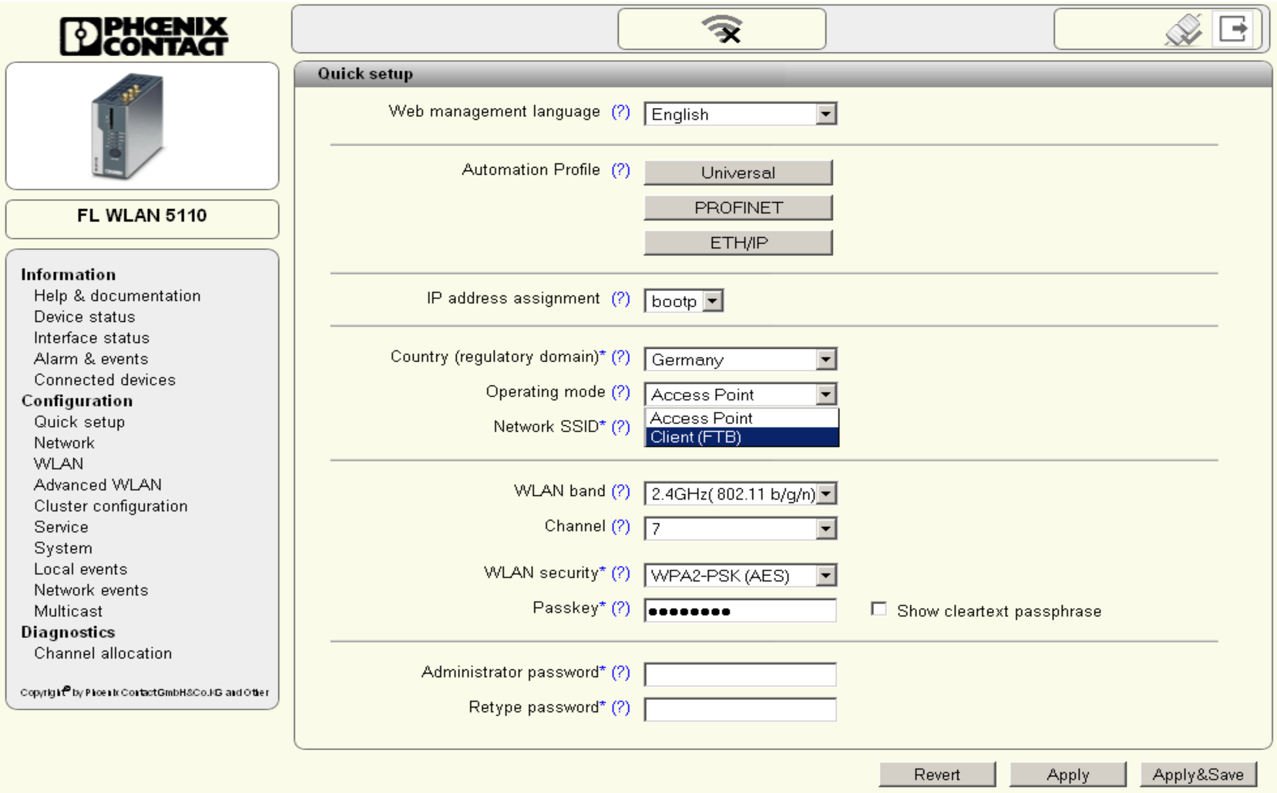
The password for accessing the web interface is changed under “Administrator password” and confirmed under “Retype password”. The change of password is applied when you log out and log back in again.

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.

3.6.2 Operation as a client

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



Quick setup

Web management language (?) English

Automation Profile (?)

IP address assignment (?) bootp

Country (regulatory domain)* (?) Germany

Operating mode (?) Access Point

Network SSID* (?)

WLAN band (?) 2.4GHz(802.11 b/g/n)

Channel (?) 7

WLAN security* (?) WPA2-PSK (AES)

Passkey* (?) ●●●●●●●●● □ Show cleartext passphrase

Administrator password* (?)

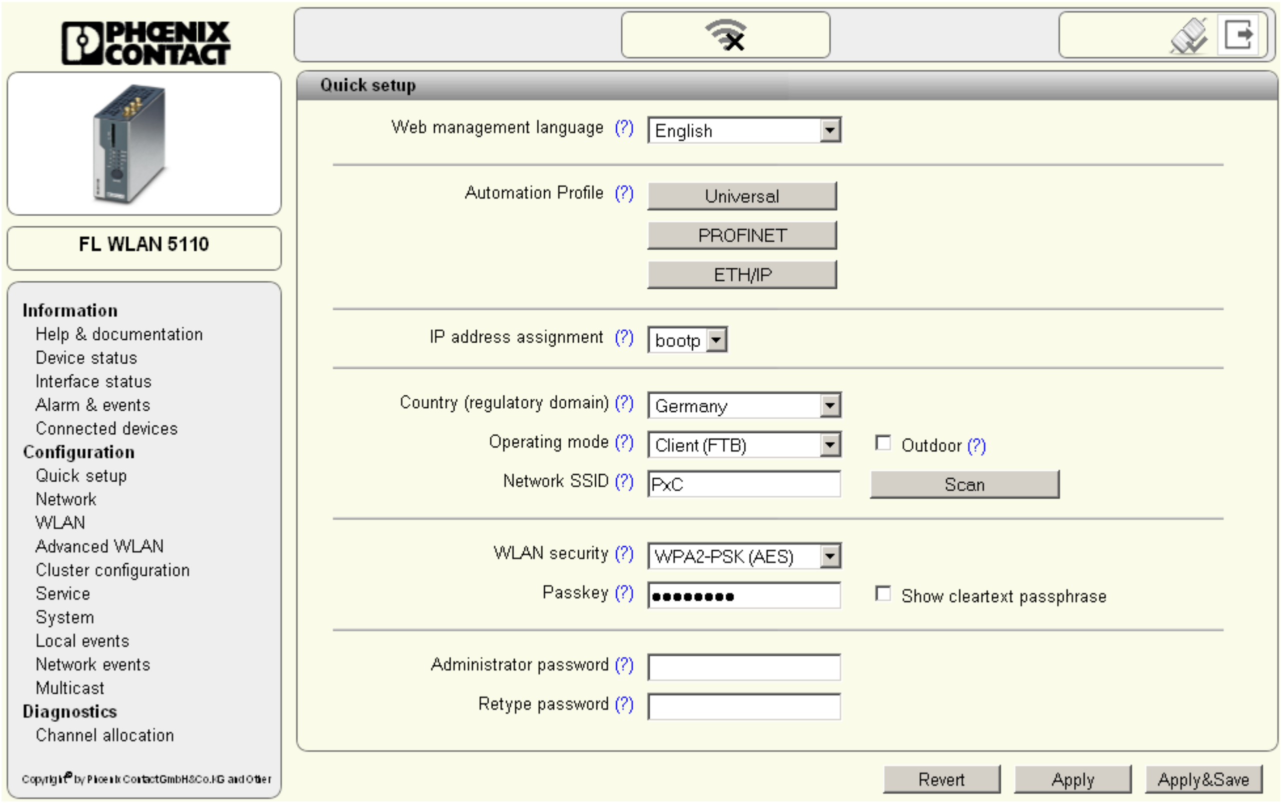
Retype password* (?)

Figure 3-8 Device configuration as a client

"Client (FTB)" mode is recommended when using another FL WLAN 511x as an access point. Other client modes are described in "Operating modes of the device" on page 44.

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.



Quick setup

Web management language (?) English

Automation Profile (?)

IP address assignment (?) bootp

Country (regulatory domain) (?) Germany

Operating mode (?) Client (FTB) □ Outdoor (?)

Network SSID (?) PxC

WLAN security (?) WPA2-PSK (AES)

Passkey (?) ●●●●●●●● □ Show cleartext passphrase

Administrator password (?)

Retype password (?)

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.

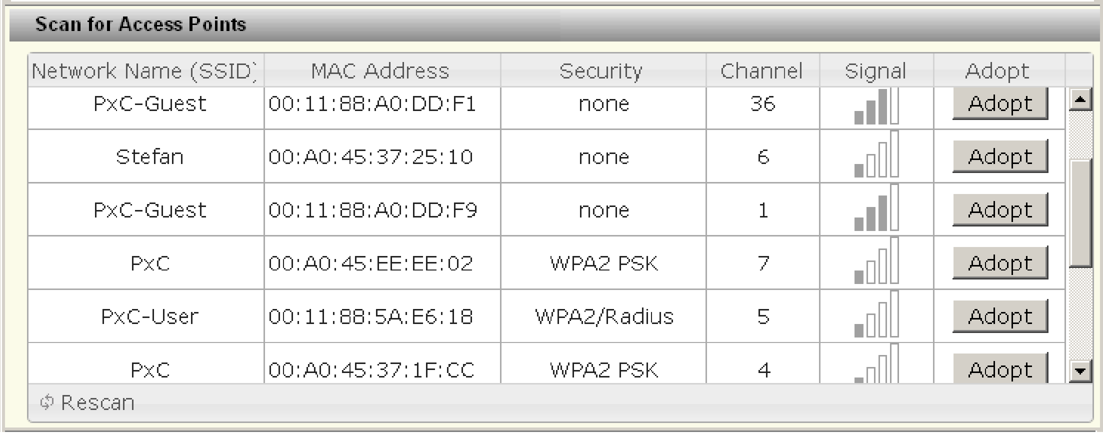
> In order to reach full data throughput under WLAN 802.11n, WPA2-PSK (AES) encryption must be used.

The network name can be up to 32 characters long. Letters, spaces, 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 the scan! All frequencies that can be used in the 2.4 GHz and 5 GHz band 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

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.

“Outdoor” check box

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, select the “Outdoor” check box.

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!

Note on WEP encryption:

WEP encryption can only be selected in client mode (FTB, MCB or SCB) under “WLAN”, “Security Mode”. The encryption quality depends on the key length.

64-bit: 5 alphanumeric characters or 10 hex numbers.

128-bit: 13 alphanumeric characters or 26 hex numbers.

It is specified in the access point.

NOTE: The WEP encryption method is compromised

The use of WEP is not recommended as it is not secure.

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.

3.7 SD card for saving the device configuration

The FL WLAN 511x 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 may be used (see “Ordering data” on page 91). 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 cards must have a minimum memory capacity of 256 MB. 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:

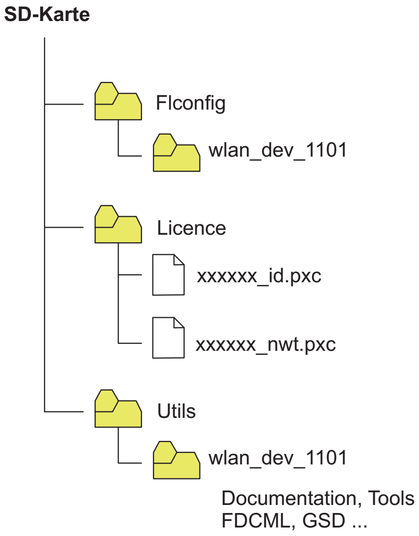


Figure 3-11 Structure on the SD card

3.7.1 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!

NOTE: As of FW 2.5, the firmware has a digital signature.
The FL WLAN 5111 device version, with the corresponding boot loader supplied on delivery, can then only be updated to (newer) FW versions that also have a signature.

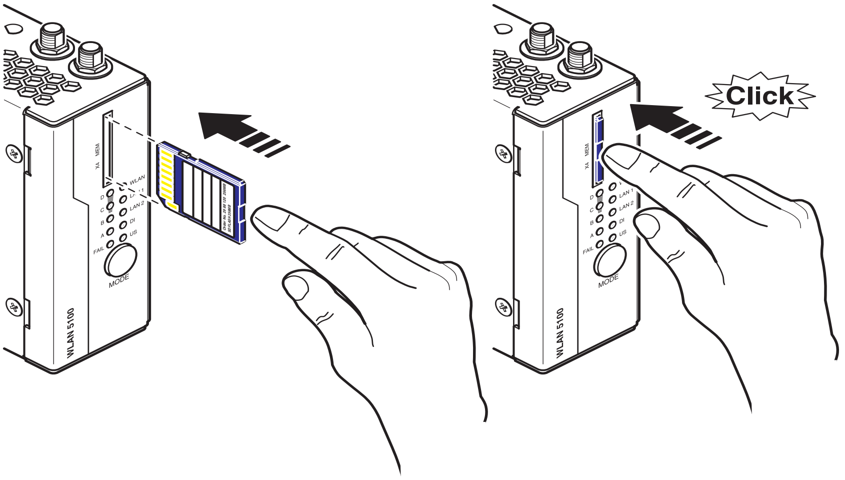


Figure 3-12 Inserting the SD card

The configuration data for the FL WLAN 511x 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.

3.7.2 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).

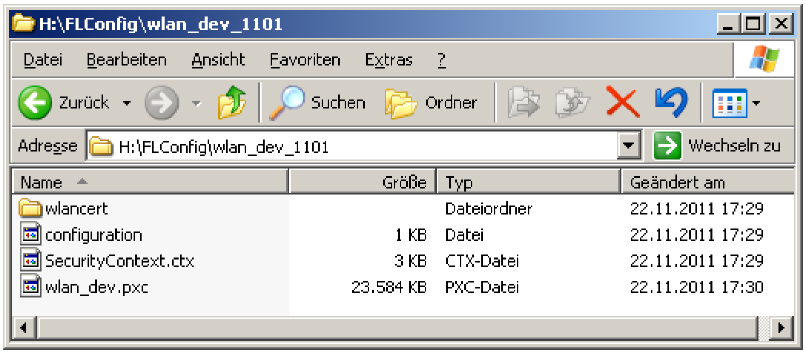
NOTE: Device downgrade

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 easily switch 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 511x can access it.



Adresse H:\FLConfig\wlan_dev_1101

Name	Größe	Typ	Geändert am
wlancert		Dateiordner	22.11.2011 17:29
configuration	1 KB	Datei	22.11.2011 17:29
SecurityContext.ctx	3 KB	CTX-Datei	22.11.2011 17:29
wlan_dev.pxc	23.584 KB	PXC-Datei	22.11.2011 17:30

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.

3.8 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.

3.8.1 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 done 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.

3.8.2 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 64).
- Start the TFT 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 done by clicking on the “Reset” button at the top of the “System” web window or by performing a voltage reset for the device.

3.8.3 Via SD card

- Make sure that the desired firmware version is located in the “FLConfig” folder. The new firmware file must be called “wlan_dev.pxc”.
- 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 display a running light and indicate that the firmware is being downloaded.

After rebooting, the new firmware version is available.

3.8.4 Via BootP/TFTP

This update method is used if the firmware on the device is no longer functional and a new version needs to be installed.

- Make sure that your PC has an active BootP and TFTP server.
- Enter the IP address of the TFTP server in the device WBM.
- 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.

3.9 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.

3.9.1 Operating mode: Access Point

In “Access Point” mode, the FL WLAN 511x 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 3.6.1 on page 33).

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 511x 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 72).

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 3.6.1 on page 33 and Section 4.1 on page 72.

3.9.2 Operating mode: Client

3.9.2.1 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.

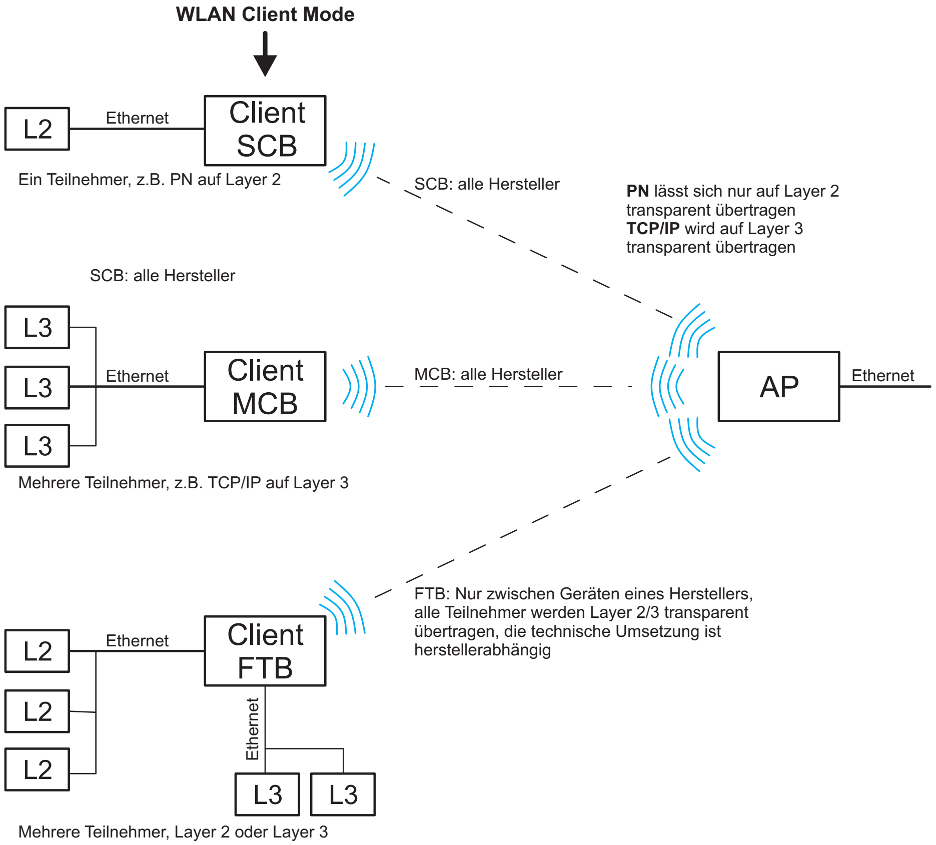

WLAN Client Mode
L2
Ethernet
Client SCB
Ein Teilnehmer, z.B. PN auf Layer 2
SCB: alle Hersteller
PN lässt sich nur auf Layer 2 transparent übertragen
TCP/IP wird auf Layer 3 transparent übertragen
SCB: alle Hersteller
L3
L3
L3
Ethernet
Client MCB
MCB: alle Hersteller
AP
Ethernet
Mehrere Teilnehmer, z.B. TCP/IP auf Layer 3
FTB: Nur zwischen Geräten eines Herstellers, alle Teilnehmer werden Layer 2/3 transparent übertragen, die technische Umsetzung ist herstellerabhängig
L2
L2
L2
Ethernet
Client FTB
Ethernet
L3
L3
Mehrere Teilnehmer, Layer 2 oder Layer 3

Figure 3-14 Overview of the various client modes

3.9.2.2 Operation as a single client

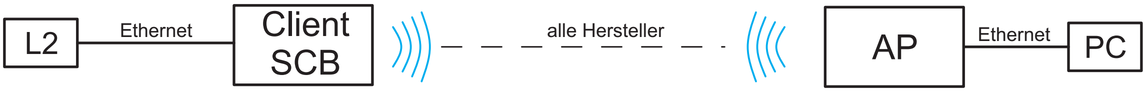


Figure 3-15 Diagram: single client mode

Properties:

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

Automatic SCB

> It is not necessary to manually enter the MAC or IP address of the connected device in the FL WLAN 511x. It requests these automatically.
>
> Only **one** wired 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 by 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 511x. This means that 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 in DHCP mode, the MAC address is transmitted to the FL WLAN 511x 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.

Manual SCB

If several Ethernet devices are connected to the Ethernet port of the FL WLAN 511x 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 511x can be accessed via WLAN.

3.9.2.3 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™.

3.9.2.4 Operation as a fully transparent bridge (default)

Properties:

- Connects several Ethernet devices (connected via Ethernet switches) to the access point on Layer 2.
- An FTB connection between the FL WLAN 511x 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.

3.9.3 Operating mode: Repeater

The FL WLAN 511x 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 3-16 on page 48 and Figure 3-18 on page 51. This repeater function allows for the creation of a linear structure. A meshed network or rings cannot be created.

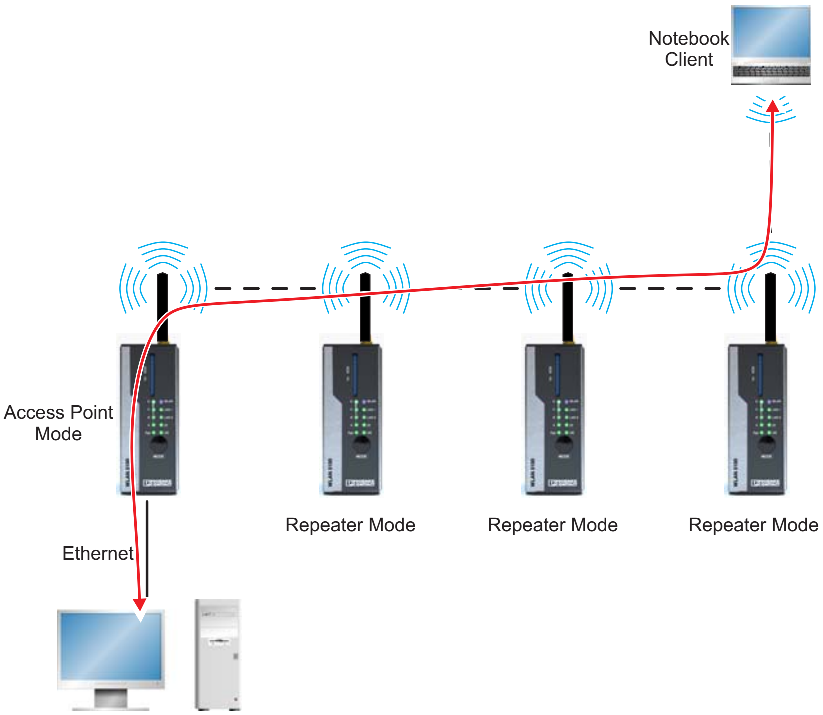


Figure 3-16 Communication via a repeater chain; enables WLAN coverage for complex topologies and connection at various locations

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 repeaters 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.

3.9.3.1 Configuration of Repeater mode

First, a FL WLAN 511x must be configured as an access point. The setting of this device mainly specifies 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.

Configuration of the access point

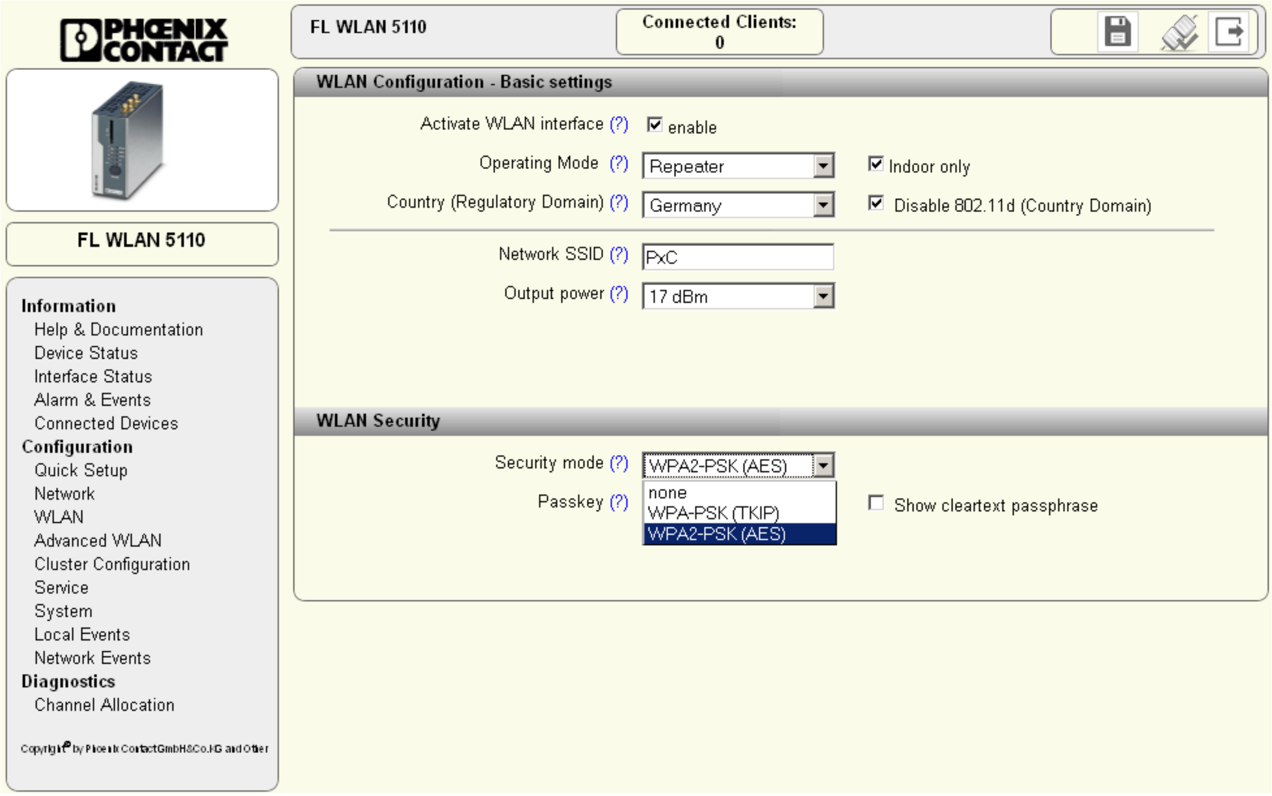
The configuration of an access point is described in “Operation as an access point” on page 33. Only “WPA-PSK (TKIP)”, “WPA2-PSK (AES)” or no encryption can be selected as the security mode.

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

Configuration of the repeater

> If the WLAN channel is to be changed after the network has been started up, this is done by means of configuration in the access point. All repeaters must then be restarted in order to ensure that the channel change is applied correctly.

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”.



FL WLAN 5110

Connected Clients: 0

WLAN Configuration - Basic settings

Activate WLAN interface (?) ☑ enable

Operating Mode (?) Repeater ☑ Indoor only

Country (Regulatory Domain) (?) Germany ☑ Disable 802.11d (Country Domain)

Network SSID (?) PxC

Output power (?) 17 dBm

WLAN Security

Security mode (?) WPA2-PSK (AES)

Passkey (?) □ Show cleartext passphrase

Figure 3-17 Configuration of the repeater

Network with several repeaters

For networks with several repeaters, it is recommended that the structure is specified by defining static MAC filters. This is done under “Static MAC Filter” in the “Advanced WLAN” menu for the individual devices.

Therefore by entering all the repeater MAC addresses that you do not want to connect in a blacklist, for example, you can ensure that only the desired repeater can log into another repeater. In contrast, all terminal devices that should establish a connection flexibly in the network can log in anywhere.

Connection establishment

Following configuration, the WLAN repeater 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.

Number of devices - data throughput

Multiple devices can be connected to all FL WLAN 511x 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. It is recommended that you connect a maximum of 2 - 3 repeaters in a line.

With respect to the clients connected via WLAN, repeater mode supports FTB, SCB, and MCB (see “Operation as a client” on page 35).

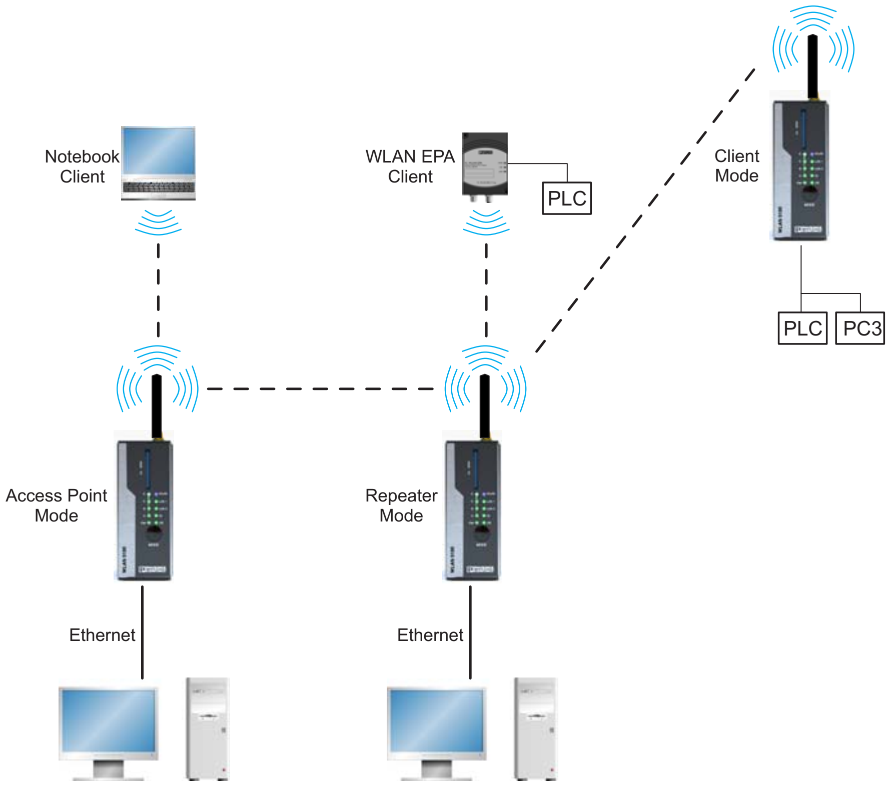


Figure 3-18 FL WLAN 511x in repeater mode: device connection via RJ45 or WLAN

All FL WLAN 511x 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.

When operating a repeater network at frequencies that require RADAR detection (Dynamic Frequency Selection, DFS), depending on the size of the network, the connection may be permanently interrupted. It is recommended that a repeater network is operated at frequencies that do not require DFS, e.g., the 2.4 GHz band.

3.9.4 Operating mode: Machine Admin

In “Machine Admin” mode, a network device can be accessed via WLAN using a panel PC or smartphone. 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 by a service technician, for example, who should deliberately not be able to access the entire network.

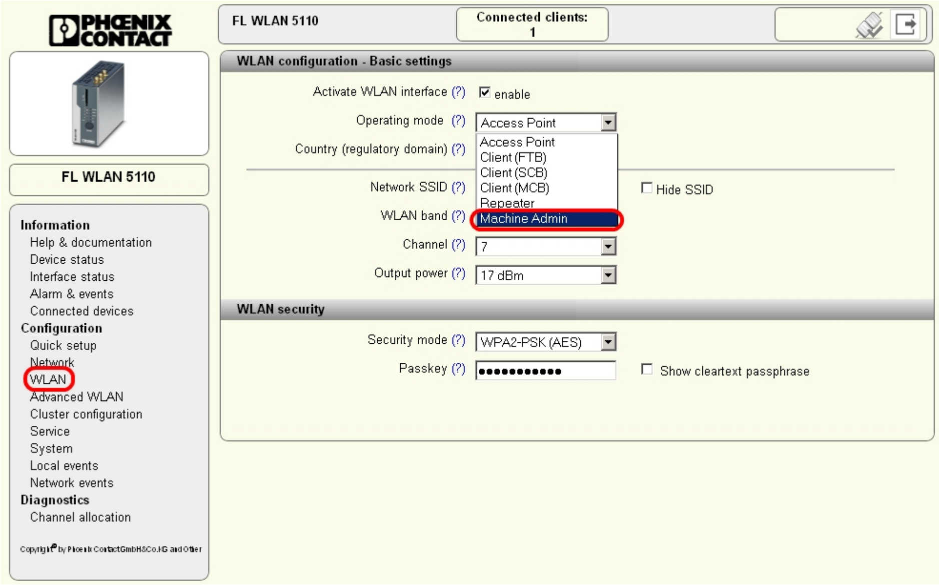
Parallel to this, the entire network can be accessed with password protection via the other SSID of normal access point mode.

3.9.4.1 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. This means that it is still possible to access the network via the access point and the network connected downstream via the SSID specified under “WLAN”. In addition, restricted access to a specific network device is possible 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.



FL WLAN 5110

Connected clients: 1

WLAN configuration - Basic settings

Activate WLAN interface (?) ☑ enable

Operating mode (?) Access Point

Access Point
Client (FTB)
Client (SCB)
Client (MCB)
Repeater
Machine Admin

Country (regulatory domain) (?)

Network SSID (?) □ Hide SSID

WLAN band (?)

Channel (?) 7

Output power (?) 17 dBm

WLAN security

Security mode (?) WPA2-PSK (AES)

Passkey (?) ●●●●●●●●●●● □ Show cleartext passphrase

Figure 3-19 “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 terminal device to be connected. Typically, the terminal device is a tablet PC, smartphone or notebook.

> If your terminal device is to be assigned an IP address via the WLAN 511x, the DHCP server must be configured first (see Section “DHCP server” on page 65). Usually, devices such as tablet PCs or smartphones expect dynamic IP address assignment via a DHCP server.

Passkey

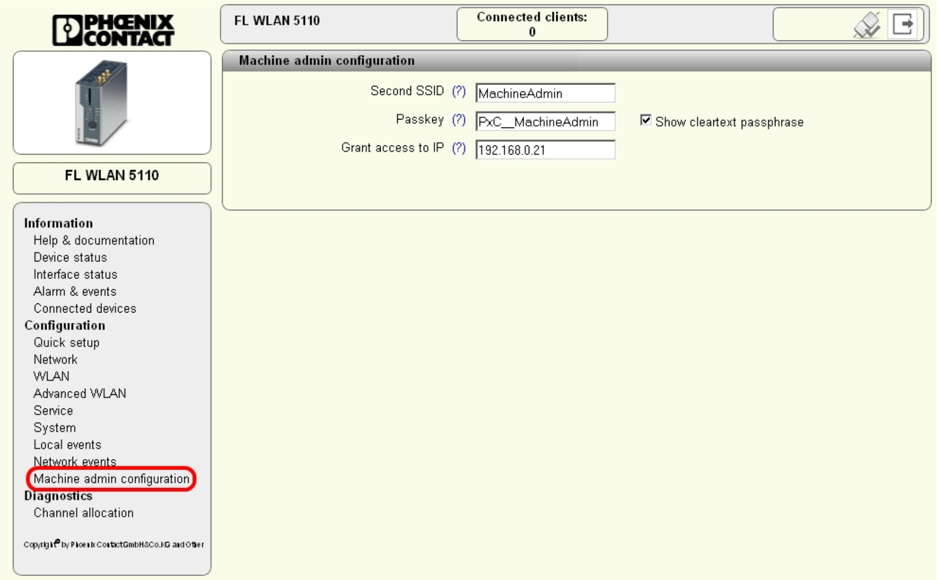
The encryption for “Machine Admin” access is entered here. The type of encryption always corresponds to that specified in access point mode. It is configured under “WLAN”, “Security mode”.

Between 8 and 63 characters should 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 511x enables the user to access exactly one device in the downstream network. This device is specified via its IP address. This address is entered under “Grant access to IP”.

> The IP address under “Grant access to IP” must be in the same IP address area as the WLAN 511x. See “Network configuration”.



Machine admin configuration

Second SSID (?) MachineAdmin

Passkey (?) PxC__MachineAdmin ☑ Show cleartext passphrase

Grant access to IP (?) 192.168.0.21

Figure 3-20 The required settings for maintenance access connection can be entered in the “Machine admin configuration” menu

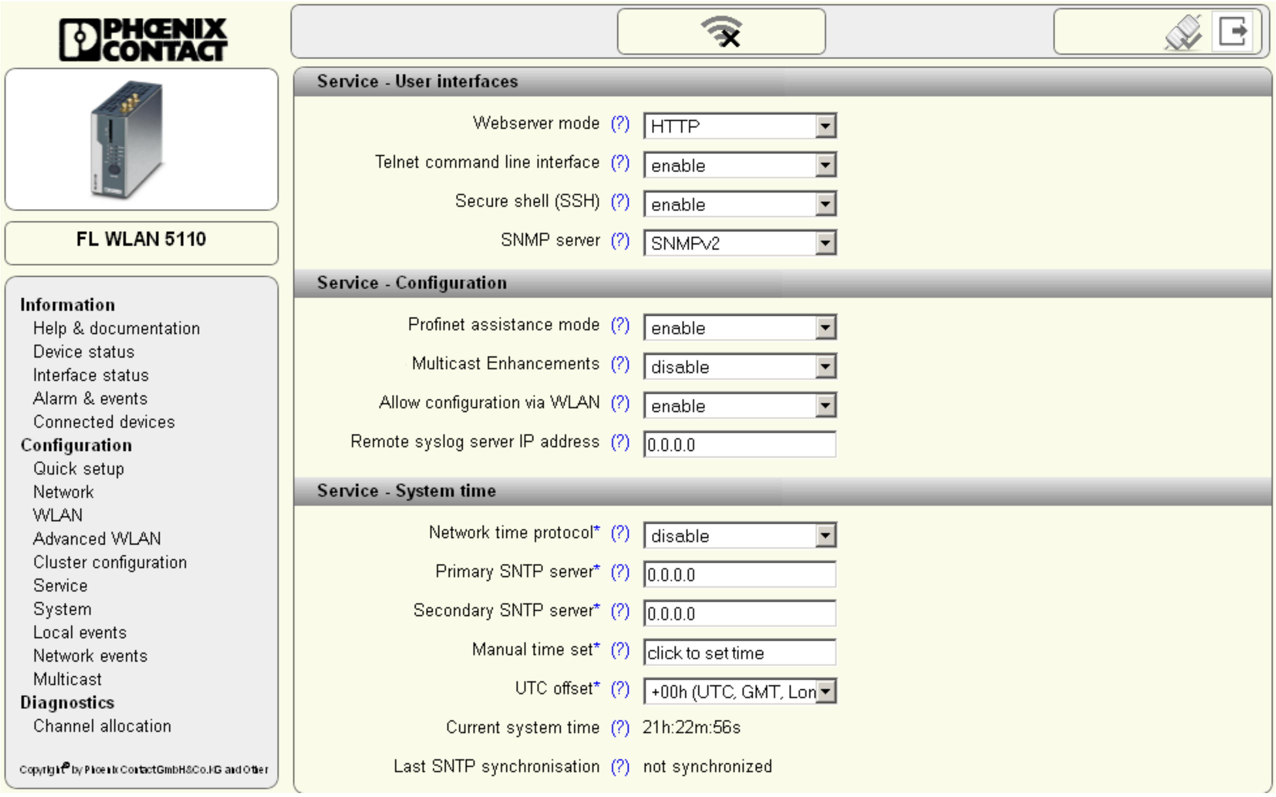
3.10 Profinet assistance mode

3.10.1 WLAN in PROFINET applications

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

3.10.1.1 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).



Service - User interfaces

Webserver mode	(?)	HTTP
Telnet command line interface	(?)	enable
Secure shell (SSH)	(?)	enable
SNMP server	(?)	SNMPv2

Service - Configuration

Profinet assistance mode	(?)	enable
Multicast Enhancements	(?)	disable
Allow configuration via WLAN	(?)	enable
Remote syslog server IP address	(?)	0.0.0.0

Service - System time

Network time protocol*	(?)	disable
Primary SNTP server*	(?)	0.0.0.0
Secondary SNTP server*	(?)	0.0.0.0
Manual time set*	(?)	click to set time
UTC offset*	(?)	+00h (UTC, GMT, Lon
Current system time	(?)	21h:22m:56s
Last SNTP synchronisation	(?)	not synchronized

Figure 3-21 PN assistance mode should be activated 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

3.10.1.2 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 5 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.

Please note that non-PROFINET traffic is considerably restricted by this setting. If your application does not permit such a restriction, it is recommended that you test the application without using Profinet assistance mode. Prioritization according to 802.11e will then apply, which may be sufficient depending on the data type. The PROFINET data will then experience the same prioritization as video or voice data, but higher prioritization than TCP/IP data traffic.

> When setting the PLC please note 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.

3.11 EtherNet/IP™: optimizing multicast transmission

“Ethernet/IP” automation profile

To improve multicast data transmission, specific settings can be made in WBM. In access point mode, the settings are made on the “Quick setup” page by selecting the “EtherNet/IP” automation profile. The client must also be a type FL WLAN 511x device and operated in FTB mode (standard settings). There is no need to select the “Ethernet/IP” automation profile on the client side.

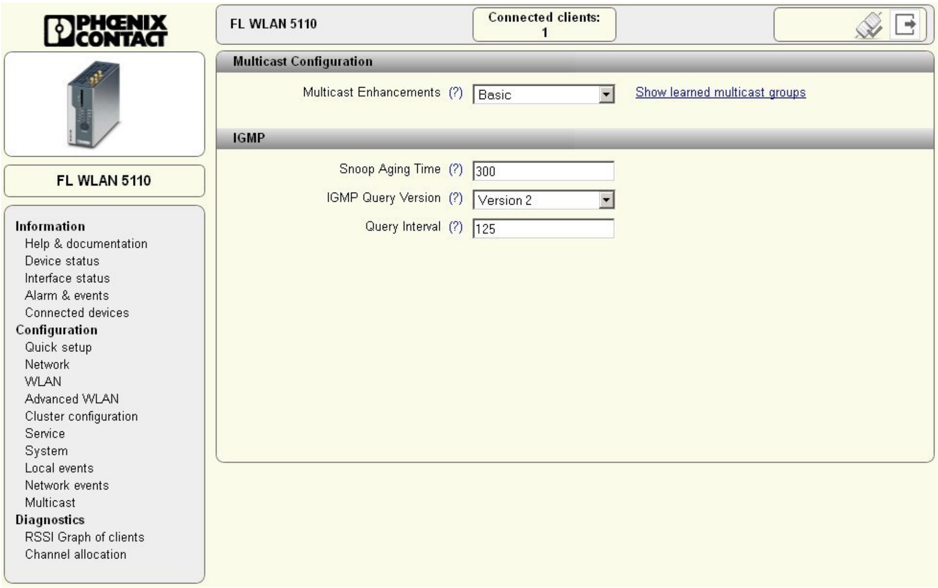
In “Basic” mode, “ETH/IP” activates an IGMPv2 querier (125 s query interval, 300 s timeout) as well as multicast enhancements. “Basic” means that IGMP snooping is activated, and learned multicast groups are tunneled in WLAN unicast telegrams via WLAN. In addition, the access point repeats the last query telegram on the WLAN side as soon as a new client logs on, in order to also learn its desired multicast groups as quickly as possible.

The basic advantage is tunneling all the IP multicast data on the WLAN side. This considerably reduces the amount of data on the wireless transmission via WLAN side, which improves system efficiency.

The profiles currently activated on the device can be found in WBM under “Service Configuration”.

Other settings

More detailed settings can be made under “Configuration”, “Multicast”, if required. See “Activating the preset multicast configuration by selecting the “Basic” profile” on page 56.



FL WLAN 5110 | Connected clients: 1

Multicast Configuration

Multicast Enhancements (?) Basic — Show learned multicast groups

IGMP

Snoop Aging Time (?) 300

IGMP Query Version (?) Version 2

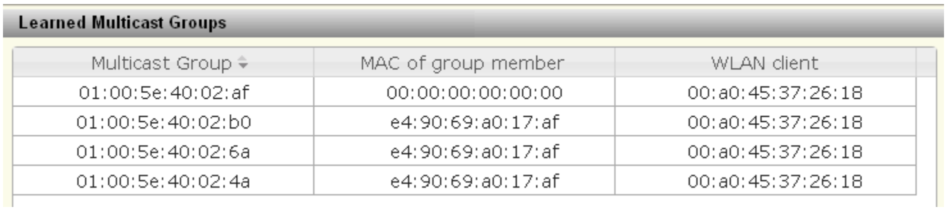
Query Interval (?) 125

Figure 3-22 Activating the preset multicast configuration by selecting the “Basic” profile

The “Basic” profile mentioned above can be selected under “Multicast Enhancements” or you can see whether settings have already been made via the CLI.

If a configuration has already been made via the CLI which does not correspond to the default settings, “CLI settings” is shown under “Multicast Enhancements” during later access via WBM. In this way, the user is informed that a different configuration has been made via the CLI. It is not overwritten by WBM as long as “CLI settings” is displayed. If no settings have been made via the CLI, “CLI settings” disappears when the web page is loaded again.

If multicast mode has been activated by clicking “Apply”, the device learns the existing multicast groups. These can be displayed in a table by clicking on the “Show learned multicast groups” link. See “The learned multicast groups are shown in a table” on page 56.



Learned Multicast Groups

Multicast Group ⇕	MAC of group member	WLAN client
01:00:5e:40:02:af	00:00:00:00:00:00	00:a0:45:37:26:18
01:00:5e:40:02:b0	e4:90:69:a0:17:af	00:a0:45:37:26:18
01:00:5e:40:02:6a	e4:90:69:a0:17:af	00:a0:45:37:26:18
01:00:5e:40:02:4a	e4:90:69:a0:17:af	00:a0:45:37:26:18

Figure 3-23 The learned multicast groups are shown in a table

The maximum number of learned multicast groups is limited to 32. The entry in the table might be deleted due to timeout, i.e., the query has not been answered with an IGMP membership report within the “Snoop Aging Time”.

Further details can be configured via the CLI, if required. For detailed information on general access to the CLI, please refer to “Access via the Command Line Interface (CLI)” on page 68. The parameters that can be set can be called directly via the CLI.

If permitted by your application, use unicast addressing instead of multicast addressing as early as the configuration stage for the controller and the other EtherNet/IP™ devices in the network in order to reduce the volume of data from the outset.

3.12 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.

3.12.1 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.

3.13 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 5 Mbps (see also Section 3.10.1.2 “PROFINET prioritization”).

3.14 Cluster management

For the simplified configuration of larger WLAN networks, the FL WLAN 511x 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.

3.14.1 Searching and selecting cluster devices

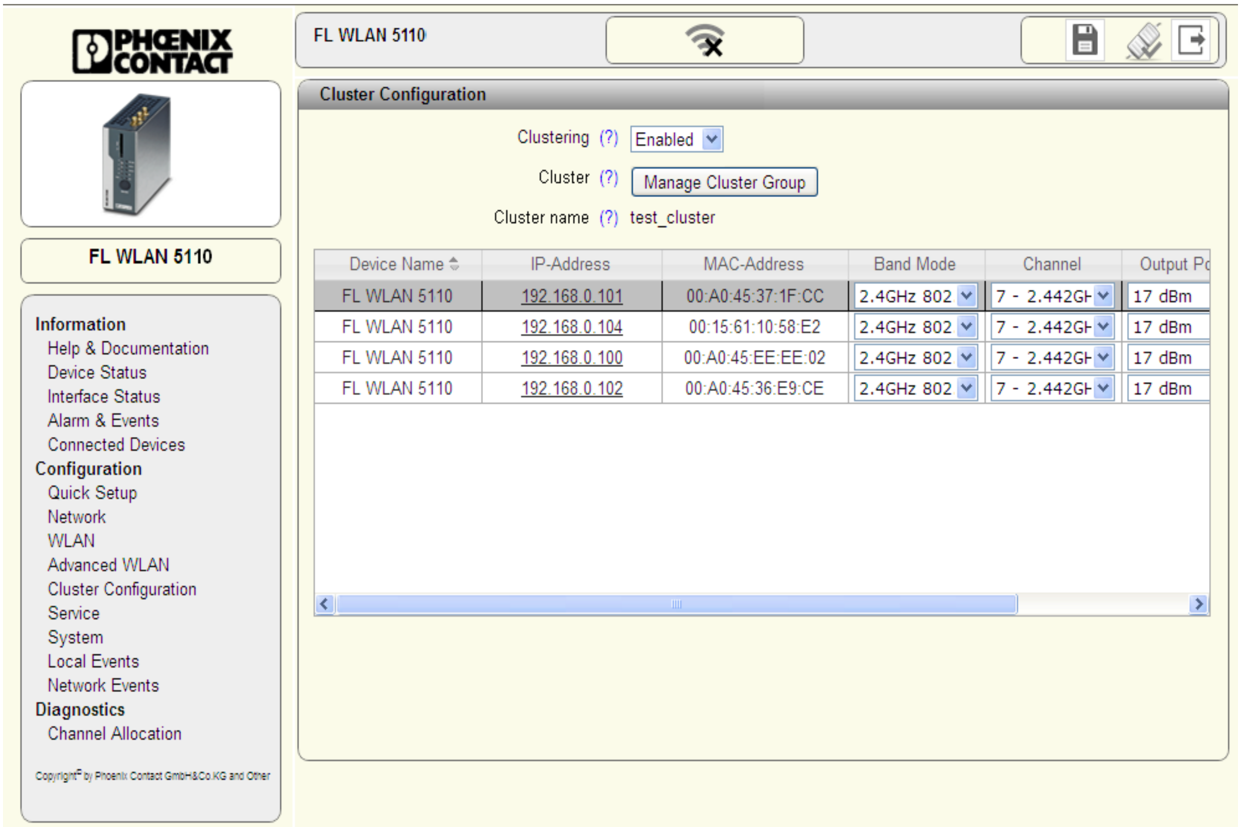
To configure a cluster, call a WLAN access point, which you intend to add to the cluster, via the corresponding IP address. The other FL WLAN 511x devices are connected to this device via the wired Ethernet network. They are in “Access Point” mode.

Only FL WLAN 511x 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 enabled (default) in the “Cluster Configuration” menu in order to apply the configuration. Clicking on the “Manage Cluster Group” button opens the “Cluster Group Configuration” pop-up window.

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



FL WLAN 5110

Cluster Configuration

Clustering (?) Enabled

Cluster (?) Manage Cluster Group

Cluster name (?) test_cluster

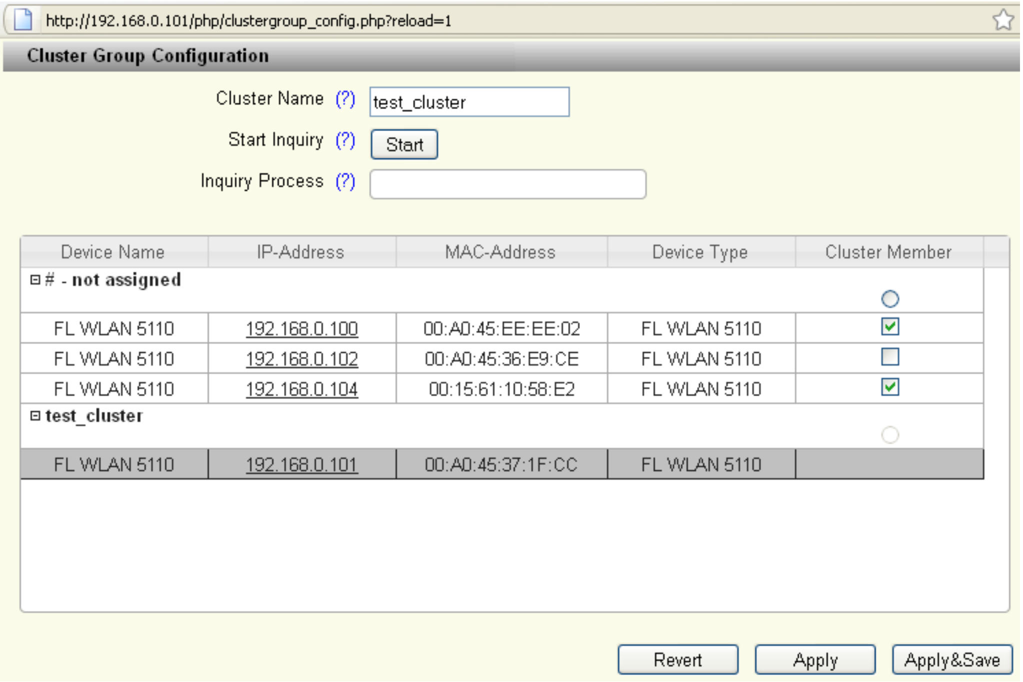
Device Name	IP-Address	MAC-Address	Band Mode	Channel	Output Pc
FL WLAN 5110	192.168.0.101	00:A0:45:37:1F:CC	2.4GHz 802	7 - 2.442GH	17 dBm
FL WLAN 5110	192.168.0.104	00:15:61:10:58:E2	2.4GHz 802	7 - 2.442GH	17 dBm
FL WLAN 5110	192.168.0.100	00:A0:45:EE:EE:02	2.4GHz 802	7 - 2.442GH	17 dBm
FL WLAN 5110	192.168.0.102	00:A0:45:36:E9:CE	2.4GHz 802	7 - 2.442GH	17 dBm

Figure 3-24 Assigning the cluster name – the table first shows the access point used for configuration by the user

Click on the “Start” button to start searching for other FL WLAN 511x 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 3-25 on page 60).

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



http://192.168.0.101/php/clustergroup_config.php?reload=1

Cluster Group Configuration

Cluster Name (?) test_cluster

Start Inquiry (?) Start

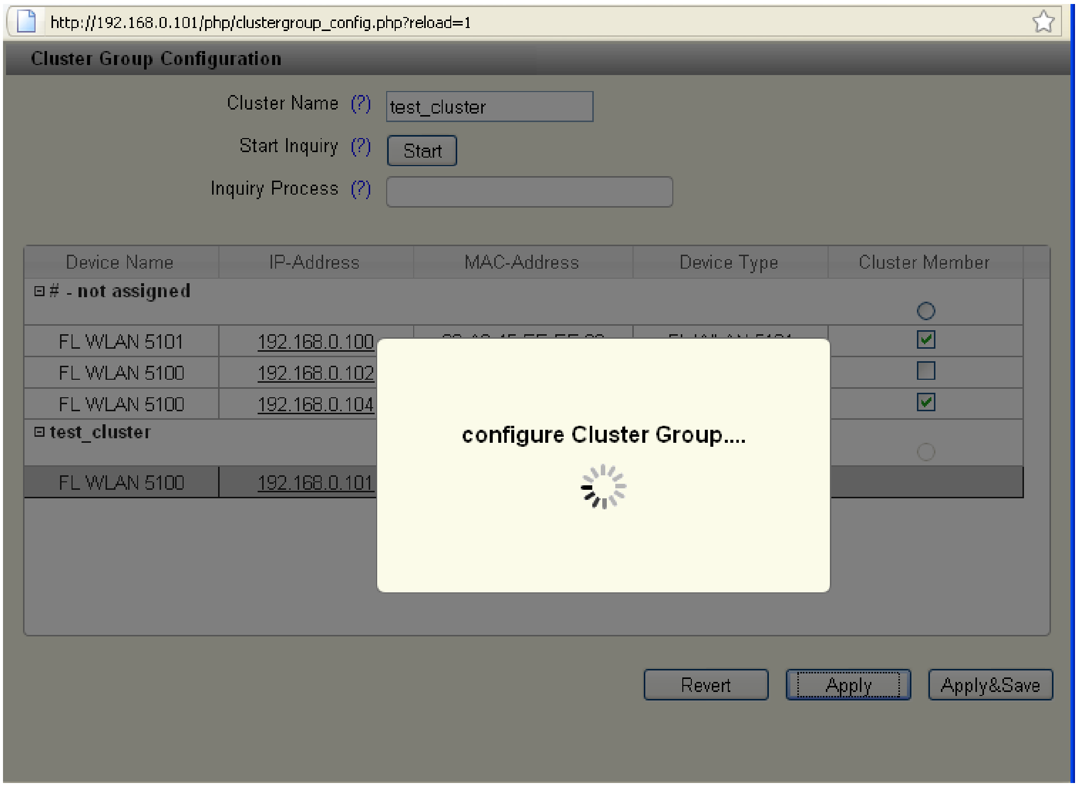
Inquiry Process (?)

Device Name	IP-Address	MAC-Address	Device Type	Cluster Member
⊟ # - not assigned				○
FL WLAN 5110	192.168.0.100	00:A0:45:EE:EE:02	FL WLAN 5110	☑
FL WLAN 5110	192.168.0.102	00:A0:45:36:E9:CE	FL WLAN 5110	☐
FL WLAN 5110	192.168.0.104	00:15:61:10:58:E2	FL WLAN 5110	☑
⊟ test_cluster				○
FL WLAN 5110	192.168.0.101	00:A0:45:37:1F:CC	FL WLAN 5110	

Figure 3-25 List of WLAN access points in the cable network

Once all desired access points have been selected by activating the corresponding check box, 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.



http://192.168.0.101/php/clustergroup_config.php?reload=1

Cluster Group Configuration

Cluster Name (?) test_cluster

Start Inquiry (?) Start

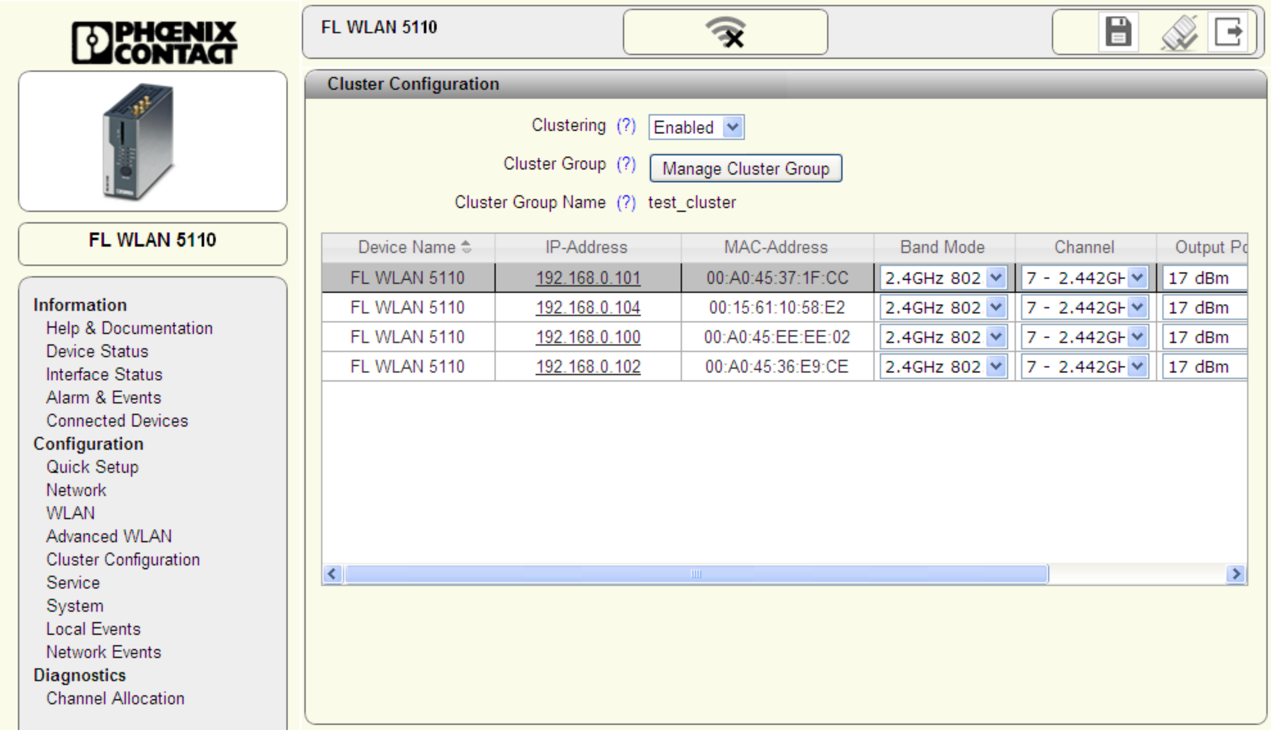
Inquiry Process (?)

Device Name	IP-Address	MAC-Address	Device Type	Cluster Member
⊟ # - not assigned				○
FL WLAN 5101	192.168.0.100			☑
FL WLAN 5100	192.168.0.102			□
FL WLAN 5100	192.168.0.104			☑
⊟ test_cluster				○
FL WLAN 5100	192.168.0.101			

configure Cluster Group....

Figure 3-26 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.



Cluster Configuration

Clustering (?) Enabled

Cluster Group (?) Manage Cluster Group

Cluster Group Name (?) test_cluster

Device Name	IP-Address	MAC-Address	Band Mode	Channel	Output Pc
FL WLAN 5110	192.168.0.101	00:A0:45:37:1F:CC	2.4GHz 802	7 - 2.442GH	17 dBm
FL WLAN 5110	192.168.0.104	00:15:61:10:58:E2	2.4GHz 802	7 - 2.442GH	17 dBm
FL WLAN 5110	192.168.0.100	00:A0:45:EE:EE:02	2.4GHz 802	7 - 2.442GH	17 dBm
FL WLAN 5110	192.168.0.102	00:A0:45:36:E9:CE	2.4GHz 802	7 - 2.442GH	17 dBm

Figure 3-27 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.

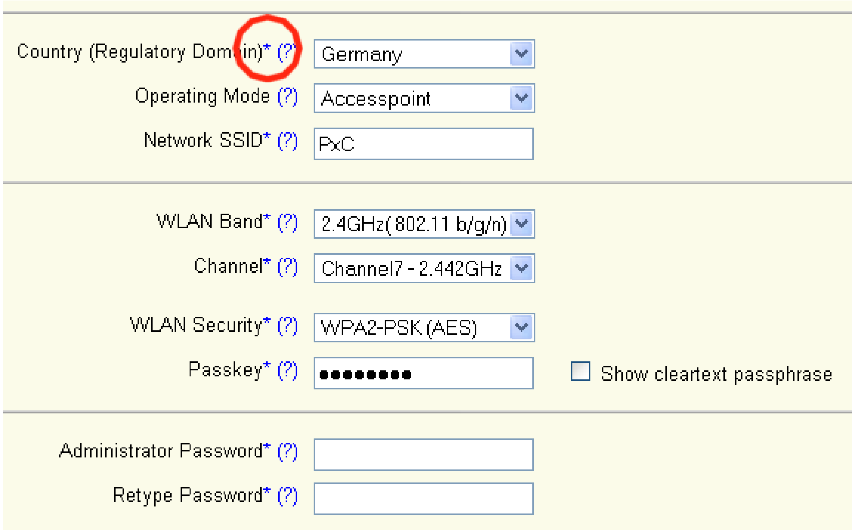
The configuration is stored to the device as the latest configuration by clicking on the floppy disk icon.

> Any parameter changes made to a device belonging to a cluster that are 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 the “Start” button. The new device appears in the list and can be added to the cluster via the check box under “Cluster Member”. Save the configuration with “Apply&Save”.

3.14.2 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 3-28 on page 63 if the function was previously activated on the “Cluster Configuration” web page) are transferred to the other access points in the cluster.



Country (Regulatory Domain)* (?) Germany

Operating Mode (?) Accesspoint

Network SSID* (?) PxC

WLAN Band* (?) 2.4GHz(802.11 b/g/n)

Channel* (?) Channel7 - 2.442GHz

WLAN Security* (?) WPA2-PSK (AES)

Passkey* (?) ●●●●●●●●● □ Show cleartext passphrase

Administrator Password* (?)

Retype Password* (?)

Figure 3-28 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

3.14.3 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.

3.15 Using file transfer

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

Table 3-7 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

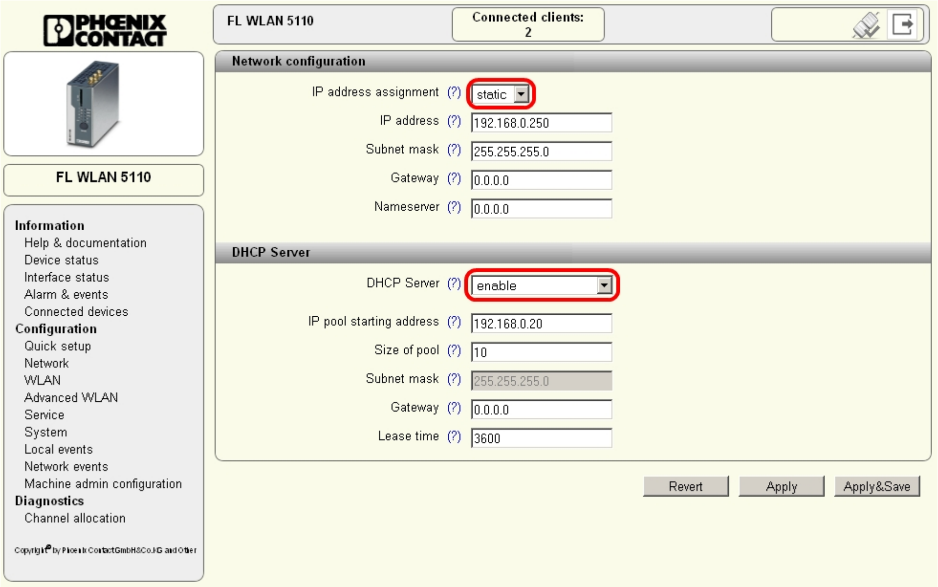
3.16 DHCP server

The FL WLAN 511x has a DHCP server. IP addresses can be assigned via WLAN or the Ethernet interface (copper). The DHCP server is deactivated by default upon delivery.

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.



Network configuration

IP address assignment (?) static
IP address (?) 192.168.0.250
Subnet mask (?) 255.255.255.0
Gateway (?) 0.0.0.0
Nameserver (?) 0.0.0.0

DHCP Server

DHCP Server (?) enable
IP pool starting address (?) 192.168.0.20
Size of pool (?) 10
Subnet mask (?) 255.255.255.0
Gateway (?) 0.0.0.0
Lease time (?) 3600

Figure 3-29 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 assigned IP address is leased. If the time has elapsed, the DHCP client can renew the IP parameters.

3.17 Event handling

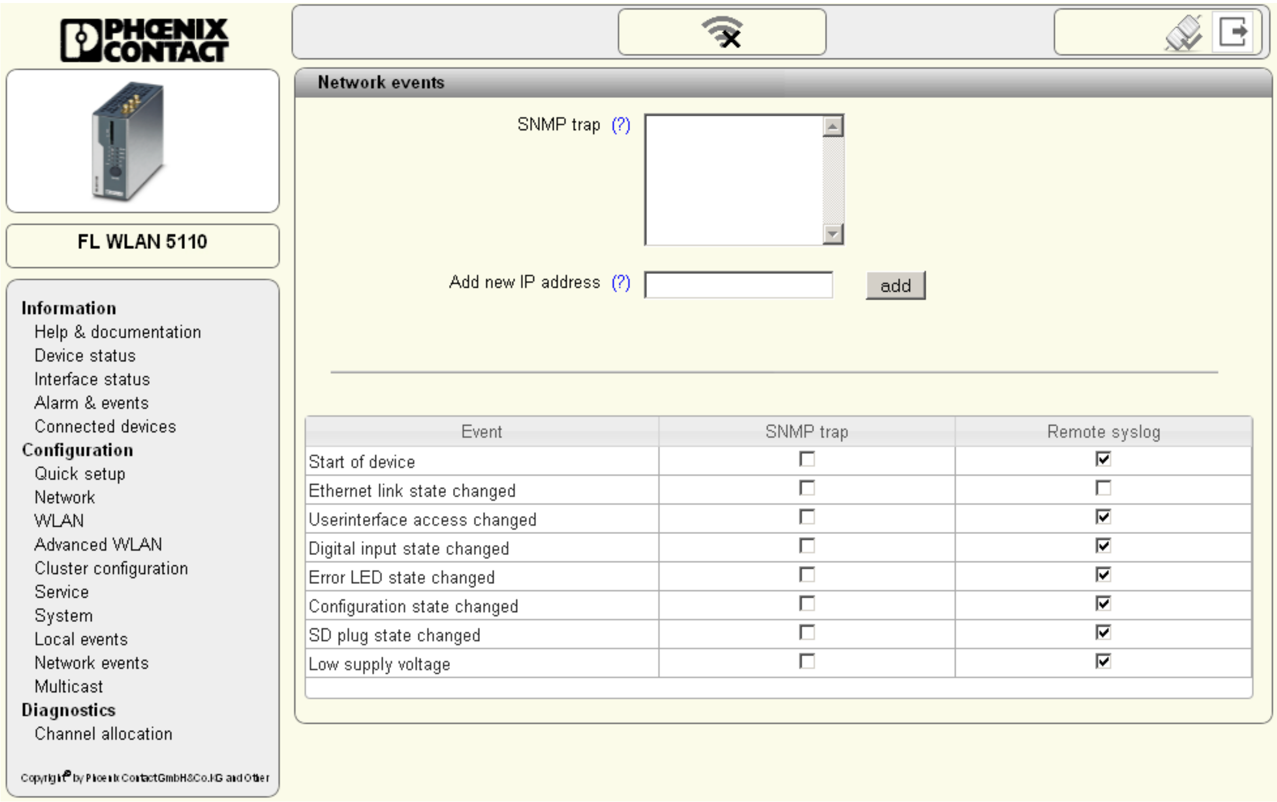
Various events trigger various reactions on the device:

Table 3-8 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		
Access to user interfaces failed	Yes, configurable	Always	Yes, configurable		
Digital input state change	Yes, configurable	Always	Yes, configurable		
Error LED state change	Yes, configurable	Always	Yes, configurable		
Configuration status changed	Yes, configurable	Always	Yes, configurable		
SD card state change	Yes, configurable	Always	Yes, configurable		
Power supply low level	Yes, configurable	Always	Yes, configurable		
WLAN interface on/off				Configurable, change when switching from off to on	Configurable, “High” = WLAN on “Low” = WLAN off
Force WLAN roaming				Set input to “High”	
Set digital output				Configurable, sets the digital output	
WLAN connected					Configurable in client mode, “High” = connected “Low” = not connected

3.17.1 Selecting network events in web-based management

Various events can be selected on the “Network 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.



SNMP trap (?)

Add new IP address (?)

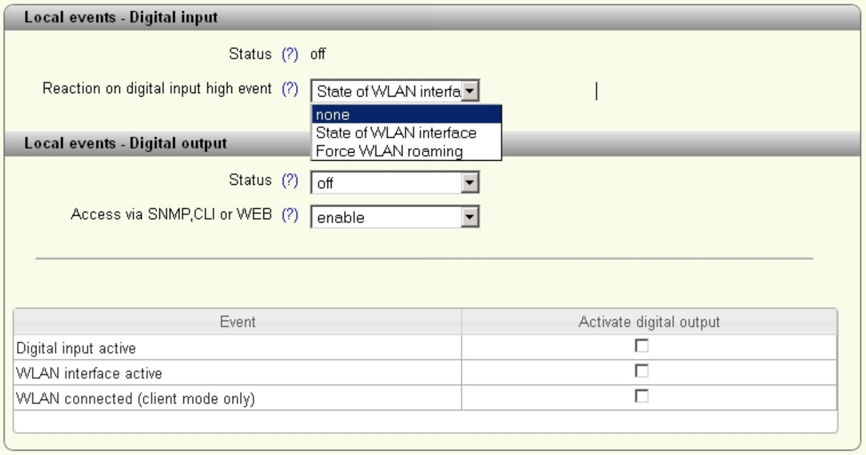
Event	SNMP trap	Remote syslog
Start of device	□	☑
Ethernet link state changed	□	□
Userinterface access changed	□	☑
Digital input state changed	□	☑
Error LED state changed	□	☑
Configuration state changed	□	☑
SD plug state changed	□	☑
Low supply voltage	□	☑

Figure 3-30 Possible network events available for selection

3.17.2 Digital input and output: selecting local events in web-based management

Various events relating to the digital input and output of the device can be configured on the “Local events” web page. Various functions can be triggered via the digital input. The digital output can be tested via the web page. The possible functions can also be activated.

Access to the digital output via SNMP, CLI or WEB can also be explicitly deactivated here.



Local events - Digital input

Status (?) off

Reaction on digital input high event (?) State of WLAN interfa

Local events - Digital output

Status (?) off

Access via SNMP,CLI or WEB (?) enable

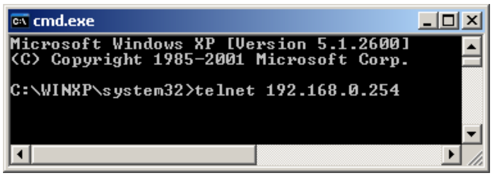
Event	Activate digital output
Digital input active	□
WLAN interface active	□
WLAN connected (client mode only)	□

Figure 3-31 Configuration of the digital input and output

3.18 Access via the Command Line Interface (CLI)

3.18.1 General access via a console (e.g., Windows)

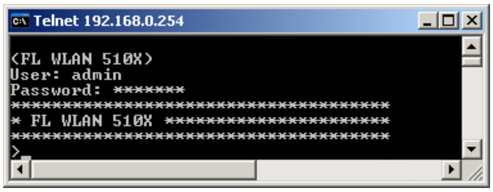
Enter “telnet IP address” in the console and confirm by pressing “Enter”. Please note that the device is delivered with BootP default settings. A static IP address must therefore be assigned in advance, for example.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINXP\system32>telnet 192.168.0.254
```

Now enter the user name and password and confirm each entry with “Enter”.



```
<FL WLAN 510X>
User: admin
Password: *******
*************************************
* FL WLAN 510X **********************
*************************************
>
```

You can now view and, if necessary, change the current settings of the individual parameters using the dedicated commands.

If you enter “?” you will receive a list of the accessible configurations for the respective current level.

You can access the respective level by entering the command followed by a space and a “?”. For example, “wlan ?”.

Below you will see an example based on the configuration of WLAN roaming parameters.

3.18.2 Configuration of client roaming via the CLI

By default, the device is prepared for roaming. Roaming is a client functionality and is used in client mode.

Please note that the device is already configured with roaming parameters. The adjustment of roaming parameters greatly depends on the environment of the WLAN application and its influence on the signal strength.

This section explains the configuration of a WLAN client in detail. As a starting point, the device is assumed to be in client mode. It is addressed via the CLI as described in the previous section.

Enter “wlan radio roaming ?” to go to the level for the client roaming settings. The configurable parameters are shown in a list.

The adjustable value range of the individual parameters can be read by entering the values listed under “Parameter” in the table. For example: “bgrnd-scan-thrsh ?”

The current value of the individual parameters can be read by entering “wlan radio roaming bgrnd-scan-thrsh” and then pressing “Enter”, for example.

You can change the value by entering “wlan radio roaming brgnd-scan-thrsh XX” and then pressing “Enter”, for example. “Set value to XX” is displayed to confirm the set value.

Please note that the setting of some values, particularly during roaming configuration, may require the device to be reset. This will take a moment. The LEDs on the front of the device signal this where applicable.

Table 3-9 CLI parameters

Function	Parameter	Description	Default value (value range)
Background scan threshold	bgrnd-scan-thrsh	RSSI level from which a background scan is started	-60 dBm (-1 to -94 dBm)
Background scan network idle time	bgrnd-scan-idle	Idle time for data traffic before the background scan is started	2 ms (1 to 5000 ms)
RSSI change delta background scan	rssi-chnge-delta	Delta RSSI before another background scan is started	4 dB (1 to 94 dB)
Roaming decision difference	roam-chnge-delta	Delta RSSI between the two access points at the client location	5 dB (-1 to -94 dB)
Forced roaming	force-scan-thrsh	Absolute value at which roaming is performed	-90 dBm (-1 to -94 dBm)
RSSI: Radio Signal Strength Indication, signal level in dB with reference to mW			

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 started on a PC without having to be installed 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 status of the digital inputs and outputs.
Interface status	
Interface status LAN	
	This area contains information regarding the current settings and status of the LAN interfaces.
Interface status WLAN	
	This area contains information regarding the current settings and status 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.

Configuration
Quick setup

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

Designation	Description
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	**Static:** a static IP address is assigned to this interface. **BootP:** during initial startup, the device transmits BootP requests without interruption until it receives valid IP parameters. As soon as it receives a valid IP parameter, the device stops sending 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 parameters that were last assigned via BootP. After the default settings are restored, the device sends BootP requests until they are answered. **DHCP**: dynamic request for IP parameters from a DHCP (Dynamic Host Configuration Protocol) server.
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	Access point: implements a WLAN wireless network for wirelessly connecting WLAN-compatible devices to an Ethernet network. 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.
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: spaces, !$@&/()=?[]{}+*-_<>
WLAN band	Selection of the frequency band. Other operating modes in acc. with IEEE 802.11 are available in the “Advanced WLAN” menu.

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

Designation	Description
Channel	**Channel selection:** possible channel selection depends on the setting made under “WLAN Band”. **Indoor Ch36…Ch48:** 4 channels can be freely selected. **Indoor Auto 8 / Indoor Auto 16:** the system selects the channels automatically (DFS). The connection may be interrupted during a channel switchover. **Automatic:** the device automatically selects a WLAN channel. **Note:** if the device is operated outdoors in the 5 GHz band, outdoor mode must be activated! This information is valid for Europe.
WLAN security	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.
Passkey	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 be at least eight characters long.
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.

Network
Network configuration

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

Designation	Description
Type of IP address assignment	**Static:** a static IP address is assigned to this interface. **BootP:** during initial startup, the device transmits BootP requests without interruption until it receives valid IP parameters. As soon as it receives a valid IP parameter, the device stops sending 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 parameters that were last assigned via BootP. After the default settings are restored, the device sends BootP requests until they are answered. **DHCP**: dynamic request for IP parameters from a DHCP (Dynamic Host Configuration Protocol) server.
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 the wired Ethernet interface as well as via 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 assigned 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	**Access point:** Implements a WLAN wireless network for wirelessly connecting WLAN-compatible devices to an Ethernet network. **Client:** Supports the wireless connection of Ethernet devices to an Ethernet network via a WLAN wireless network. **FTB mode**: Fully Transparent Bridge Supports Layer 2 transparent communication with multiple devices behind the WLAN client. **SCB mode:** Single Client Bridge Layer 2 transparent communication with one device behind the WLAN client (compatible with all access points). **MCB mode:** Multi Client Bridge Layer 3 (TCP/IP) transparent communication with multiple devices behind the WLAN client (compatible with most access points). **Repeaters** Access point with wireless connection to another access point (via virtual client). **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”.
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	Hide the SSID. 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.
WLAN band	Selection of the frequency band. Other operating modes in acc. with IEEE 802.11 are available in the “Advanced WLAN” menu.

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

Designation	Description
Channel	Channel selection: possible channel selection depends on the setting made under “WLAN Band”. **Indoor Ch36…Ch48:** 4 channels can be freely selected. **Indoor Auto 8 / Indoor Auto 16:** the system selects the channels automatically (DFS). The connection may be interrupted during a channel switchover. **Automatic:** the device automatically selects a WLAN channel. **Note:** if the device is operated outdoors in the 5 GHz band, outdoor mode must be activated! This information is valid for Europe.
Output power	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!
WLAN security	
Security mode	**None:** Operation without encryption puts network security at risk. **WPA-PSK (TKIP):** used by older devices that do not support WPA/AES. **WPA2-PSK (AES):** secure and faster for client roaming. **WPA2-EAP:** enables the use of authentication servers (AAA server, RADIUS server). In order to reach full data throughput under WLAN 802.11n, WPA2-PSK (AES) encryption must be used.
Passkey	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: $%@&/()=?[]{}+*-_<>.

Advanced WLAN	
Advanced WLAN configuration on the access point	
WLAN band	Selection of the frequency band.

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

Designation	Description
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	WiFi 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 0 deactivates RTS/CTS, 2312 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. Only change this parameter if the distance is over 3000 m! The setting must be the same for the access point and the client.
Antenna configuration	Select one of the possible antenna configurations for one or two antennas. Connect the antennas to the selected antenna connections. Antenna connections that are selected without antennas being connected may be damaged.
Cluster configuration	
Cluster configuration	

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

Designation	Description
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 already in the cluster. 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 check boxes. 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 only be accessed 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 5 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.
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	

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

Designation	Description
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.
User name	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
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”.

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

Designation	Description
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	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. After a firmware update or when another firmware image is selected, the device must be restarted. If the “Automatic reboot after upload” check box is activated, this will be carried out automatically on completion of the update.
Next active image	Another firmware image can be activated here. By default upon delivery, there is only one firmware image on the device. The firmware image only comes into effect once the device has been restarted. This is performed, for example, by clicking on the “Reset Device” button on the “System” web page.
SD card state	Shows whether an SD card is inserted in slot X4. The web page must be reloaded in order to display the current status. Note: only specially formatted SD cards from Phoenix Contact may be used.
Perform action	**Load configuration:** loads the device configuration stored on the SD card and executes it. **Save configuration:** saves the configuration to the “wal-n_5100.cfg” file on the SD card. **Save device independent configuration:** saves the device-independent parameters to the “wlan_5100.cfg” file on the SD card. **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.
Advanced configuration (pop-up window)	
Upload certificate	Upload certificate via HTTP: select a file by clicking on “Upload a file” or drag the file over this button. Alternatively, the certificate can be uploaded via a TFTP server.

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: spaces, !$%@&/()=?[]{}+*-_<>
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 IP address area as the WLAN 511x (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

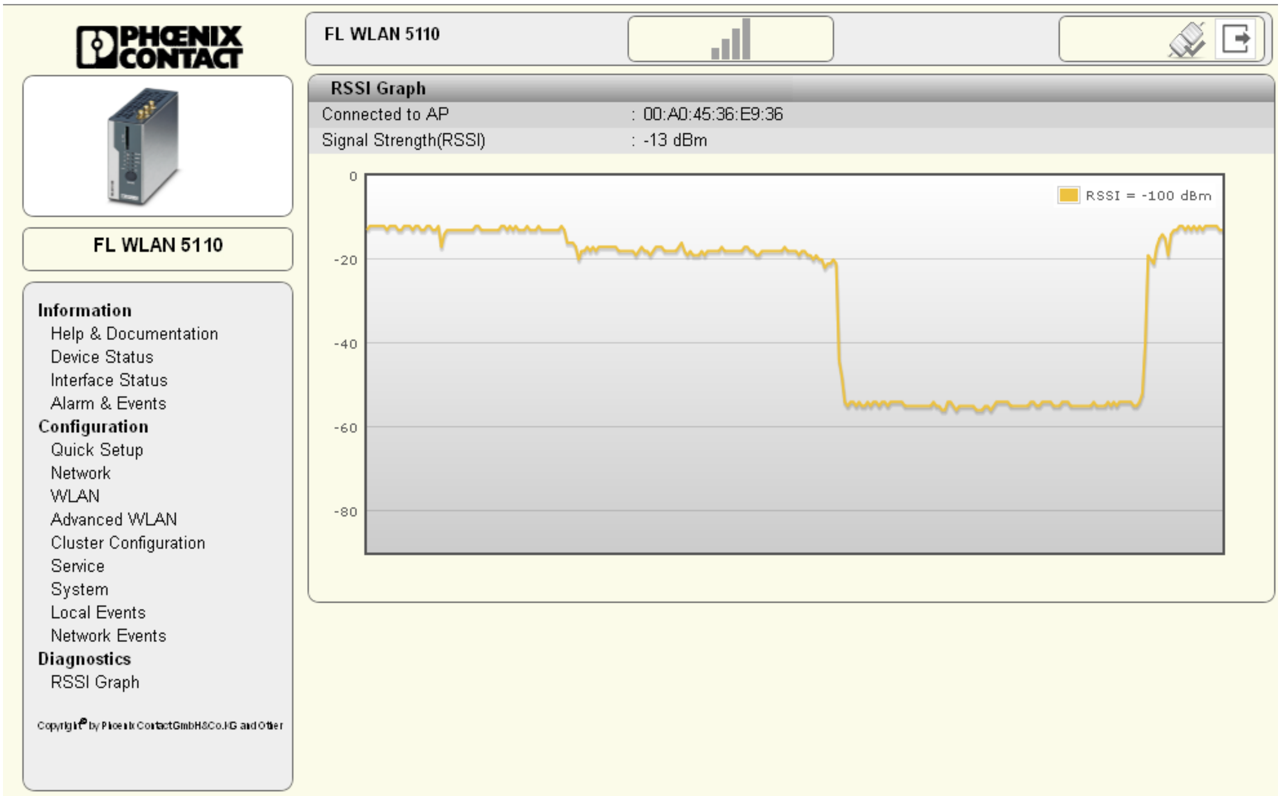
5.1 WLAN signal strength diagnostics in Client mode

If the FL WLAN 511x 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.



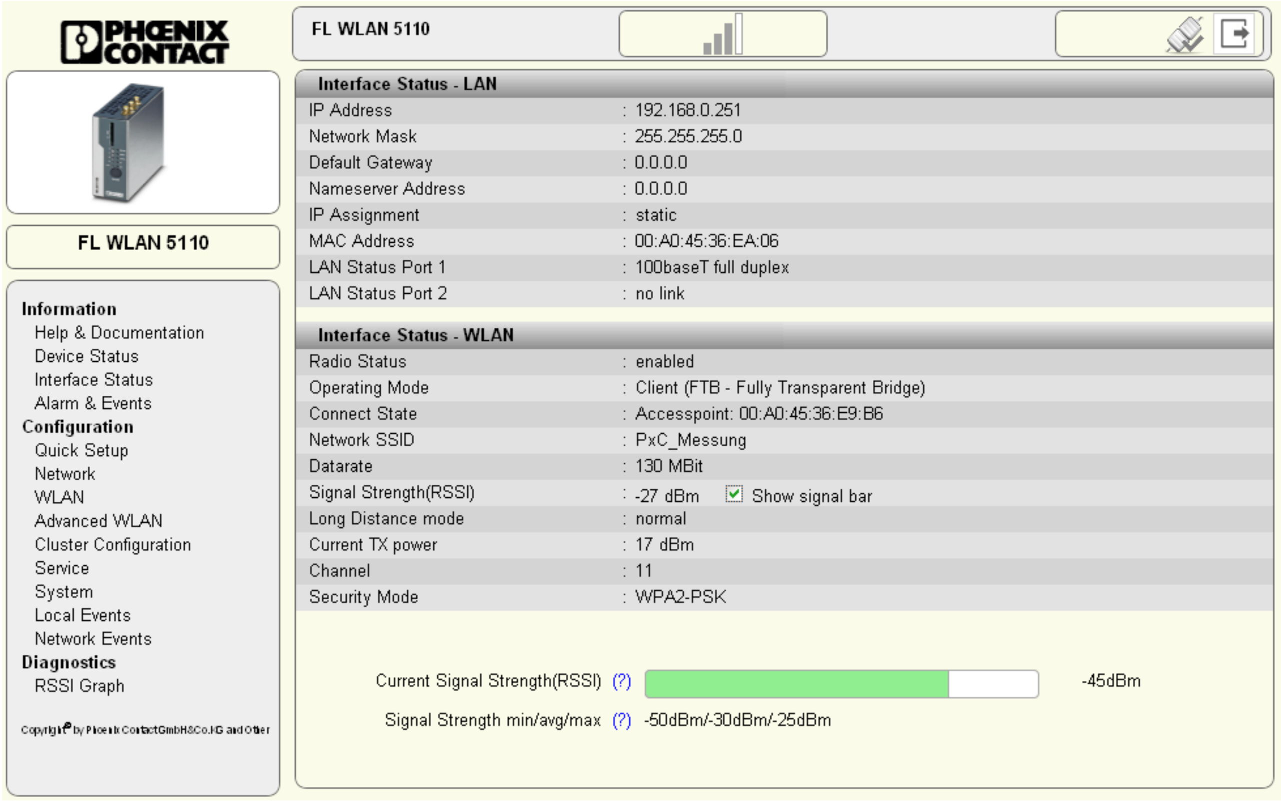
Connected to AP : 00:A0:45:36:E9:36
Signal Strength(RSSI) : -13 dBm

Figure 5-1 Display of the current WLAN signal strength in Client mode

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 in Client mode can be found in the “Interface Status – WLAN” menu. Here, the “Show signal bar” check box must be activated (see Figure 5-2). The check box 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.



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 ☑ Show signal bar
Long Distance mode	: normal
Current TX power	: 17 dBm
Channel	: 11
Security Mode	: WPA2-PSK

Current Signal Strength(RSSI) (?) -45dBm

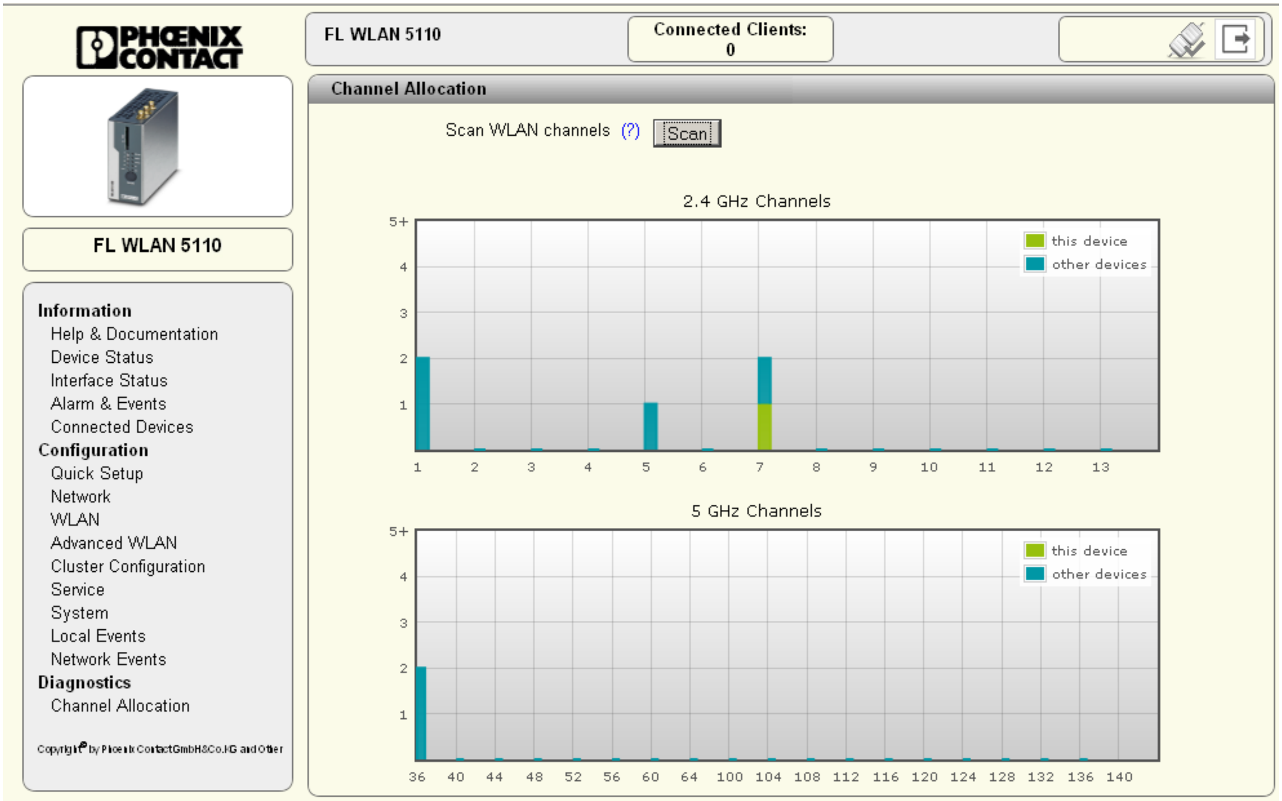
Signal Strength min/avg/max (?) -50dBm/-30dBm/-25dBm

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

5.2 WLAN channel assignment diagnostics in Access Point mode

If the FL WLAN 511x 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 as 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 the “Scan” button.



FL WLAN 5110

Connected Clients: 0

Channel Allocation

Scan WLAN channels (?) Scan

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

5.3 WLAN signal strength diagnostics in Access Point mode

If the FL WLAN 511x is in Access Point mode, the current WLAN signal strength of up to 10 connected clients (or repeaters) can be displayed. This function can be used to determine the signal strength when setting up wireless paths or when checking the signal strength during operation.

In Access Point mode, the current signal strength value of the connected client (or repeater) is displayed graphically and dynamically in the "Diagnostics" – "RSSI Graph of clients" menu.

The level indication is only changed reliably and dynamically during data traffic. During installation, a ping may be sent from a PC, for example, for this reason.

The RSSI (Radio Signal Strength Indication) value indicates the signal strength of the connected client at the access point location in dB. To differentiate between the individual devices, their MAC addresses are displayed. If any clients log off during the scan, the colors of the lines in the graphic move.

If the cursor of the PC mouse is outside the graphic, the current RSSI values are shown. If the cursor is moved over the graphic, the values of the graphs at the relevant position are shown. Clicking on the graphic stops the recording procedure and the display is frozen.

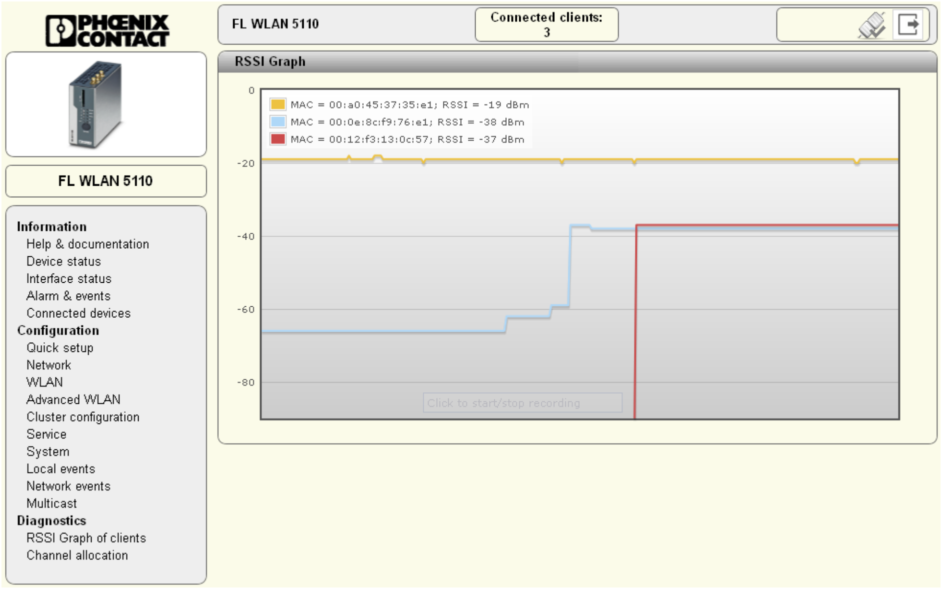


Figure 5-4 Display of the client signal strength at the access point

The value is only displayed and updated while the web page is open. Closing the web page will delete the display.

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) At very low temperatures, there may be a delay in the startup of the device when you operate the FL WLAN 511x in the extended temperature range from -40°C to +60°C. The supply voltage should not fall below 12 V DC.
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 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
Permissible voltage ranges	12 V DC to 32 V DC (HazLoc)
Current consumption at 24 V	200 mA
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 rate	10/100 Mbps
Segment length	100 m
Assignment of the IP address	BootP
Wireless interface	
Antenna connection	2 x RSMA female
Wireless standards for the FL WLAN 5110	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, in compliance with 802.11h

Interfaces [...]

Wireless standards for the FL WLAN 5111 (USA, Canada)	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
FL WLAN 5110: maximum transmission power at the RSMA connection (Europe)	For 802.11a: 16 dBm for 6-48 Mbps, 14.5 dBm for 54 Mbps For 802.11b: 17.5 dBm For 802.11g: 19 dBm for 6-36 Mbps, 16.5 dBm for 54 Mbps For 802.11an: 17 dBm for MCS 0, 13 dBm for MCS 15 For 802.11gn: 18.5 dBm for MCS 0, 15.5 dBm for MCS 15
FL WLAN 5111: maximum transmission power at the RSMA connection (USA/Canada)	For 802.11a: 15 dBm For 802.11b: 15 dBm (Ch.1), 17 dBm (Ch.2-Ch.10), 13.5 dBm (Ch.11) For 802.11g: : 16 dBm (Ch.1), 19 dBm (Ch.2-Ch.10), 14 dBm (Ch.11) For 802.11an: 16 dBm for MCS 0, 13 dBm for MCS 15 For 802.11gn: 18 dBm for MCS 0, 15.5 dBm for MCS 15 (Ch.2-Ch.10)
Receiver sensitivity at the RSMA connection	For 802.11a: -73 dBm for 54 Mbps, -90 dBm for 6 Mbps For 802.11an: -70 dBm for MCS7, -89 dBm for MCS0
Frequency range for the FL WLAN 5110	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 the FL WLAN 5111	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
Antennas	2 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 EN 60068-2-27/IEC 60068-2-27	30g, 11 ms half-sine shock pulse
Vibration resistance according to EN 60068-2-6/IEC 60068-2-6	5g, 10 - 150 Hz
Continuous shock according to EN60068-2-27/IEC60068-2-27	10g, 16 ms, 6000 shocks
Broadband noise according to EN 60068-2-64	Category 1, Class B

Conformance with EMC directives for the FL WLAN 5111	
Noise emission according to EN 55022	Class B
Radio interference field strengths according to EN 55022	Class B
Electrostatic discharge (ESD) according to EN 61000-4-2	Contact discharge: ±6 kV Air discharge: ±8 kV Indirect discharge: 6 kV
Electromagnetic fields according to IEC 61000-4-3	10 V/m
Conducted interference according to IEC 61000-4-6	10 V_{RMS}; 0.15 MHz - 80 MHz, 10 V
Fast transients (burst) according to IEC 61000-4-4	+-2.2kV
Surge voltages according to IEC 61000-4-5	+-1.0 kV asymmetrical +-0.5 kV (symmetrical)

Approvals for FL WLAN 5110	
Compliance with the “Safety of information technology equipment” test specification	DIN EN 60950 (VDE 0805, IEC 950)

EMC data for FL WLAN 5111	
Noise emission according to FCC/CFR 47, Part 15.107	Class B
Noise emission according to FCC/CFR 47, Part 15.109	Class B
Noise emission according to ICES-003 Issue 6 section 6.1	Class B
Noise emission according to ICES-003 Issue 6 section 6.2	Class B

Differences between this version and previous versions of the user manual

Rev. 00: no differences, initial version

6.1 Ordering data

Description	Order designation	Order No.
Access point, ETSI approval	FL WLAN 5110	1043193
Access point, FCC approval, only for use in the USA and Canada	FL WLAN 5111	1043201
SD memory card	SD FLASH 2GB	29 88 16 2
Factoryline Power over Ethernet splitter (PD) for separating power and data according to IEEE 802.3af and at, no configuration required, can be used with 10, 100, 1000 Mbps networks, 24 V DC output voltage	FL PD 1001 T GT	2891042
Omnidirectional antenna, 2.4 GHz / 5 GHz, gain 2.5 / 5 dBi, polarization linear vertical, beam width 2.4 GHz h/v 360°/30°, 5 GHz h/v 260°/16°, N (male), IP68	ANT-OMNI-2459-02	27 01 40 8
Omnidirectional antenna with protection against vandalism, 2.4 GHz, 3 dBi gain, IP55 degree of protection, 1.5 m cable length, RSMA (male) connection, h/v 360°/85° opening angle	RAD-ISM-2400-ANT-VAN-3-0-RSMA	27 01 35 8
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	27 01 36 2
Mounting material for wall mounting the OMNI omnidirectional antenna with protection against vandalism	RAD-ANT-VAN-MKT	28 85 87 0

Description [...]	Order designation	Order No.
Dual-band omnidirectional antenna with protection against vandalism; IP68 degree of 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	26 92 52 6
Directional antenna, 2.4/5 GHz, 9 dBi, linear vertical, N (female), IP67	ANT-DIR-2459-01	27 01 18 6
Directional antenna, 5 GHz, 9 dBi, ±45° dual slant, h/v 70°/60° opening angle, 2* N (female), IP67	ANT-DIR-5900-01	27 01 34 8
Omnidirectional antenna, 5 GHz, 5 dBi gain, linear vertical polarization, h/v 360°/25° opening angle, N (female), IP64	ANT-OMNI-5900-01	27 01 34 7
Adapter cable, 50 cm pigtail, N (female) -> RSMA (male), insertion loss: 0.75 dB for 2.4 GHz; 1.25 dB for 5 GHz, 50 ohm impedance	RAD-PIG-EF316-N-RSMA	27 01 40 2
Antenna cable, 0.5 m length; N (male) -> RSMA (male), 50 ohm impedance	RAD-PIG-RSMA/N-0.5	29 03 26 3
Antenna cable, 1 m length; N (male) -> RSMA (male), 50 ohm impedance	RAD-PIG-RSMA/N-1.0	29 03 26 4
Antenna cable, 2 m in length; N (male) -> RSMA (male), 50 ohm impedance	RAD-PIG-RSMA/N-2.0	29 03 26 5
Antenna cable, 3 m length; N (male) -> RSMA (male), 50 ohm impedance	RAD-PIG-RSMA/N-3.0	29 03 26 6
Antenna cable, 3 m length; N (male) -> N (male), attenuation approx. 0.45 dB/m for 2.4 GHz; 50 ohm impedance	RAD-CAB-EF393- 3M	28 67 64 9
Antenna cable, 5 m length; N (male) -> N (male), attenuation approx. 0.45 dB/m for 2.4 GHz; 50 ohm impedance	RAD-CAB-EF393- 5M	28 67 65 2
Antenna cable, 10 m length; N (male) -> N (male), attenuation approx. 0.45 dB/m for 2.4 GHz; 50 ohm impedance	RAD-CAB-EF393- 10M	28 67 66 5
Antenna cable, 15 m length; N (male) -> N (male), attenuation approx. 0.45 dB/m for 2.4 GHz; 50 ohm impedance	RAD-CAB-EF393- 15M	28 67 63 4
Adapter, RSMA (male) -> SMA (female); insertion loss: < 0.3 dB for 2.4 GHz	RAD-ADP-RSMA/F-SMA/F	28 84 53 8
Antenna barrier for installation in Ex Zone 2, separates and transmits HF signals with intrinsic safety (Ex i) to an antenna in Zone 0, 1 or 2; N (female) -> N (female), ATEX/IECEx approval	BAR-ANT-N-N-EX	2702198
Attachment plug with LAMBDA/4 technology as surge protection for coaxial signal interfaces. Connection: N connectors (socket/socket)	CN-LAMBDA/4-5.9-BB	28 38 49 0
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	29 03 18 2
COMBICON connector	MC 1,5/4-ST-3,5	18 40 38 2
Gray RJ45 connector set for linear cable (2 pieces)	FL PLUG RJ45 GR/2	27 44 85 6
Green RJ45 connector set for crossed cable (2 pieces)	FL PLUG RJ45 GN/2	27 44 57 1
Assembly tool for RJ45 connectors	FL CRIMPTOOL	27 44 86 9
Factory Manager startup/diagnostics software	FL SWT	28 31 04 4
Network monitoring with HMI/SCADA systems	FL SNMP OPC SERVER	28 32 16 6
Patch box 8 x RJ45 CAT5e, pre-assembled, can be retrofitted	FL PBX 8TX	28 32 49 6

Description [...]	Order designation	Order No.
Patch box 6 x RJ45 CAT5e and 4 SC-RJ, glass, pre-assembled, can be retrofitted	FL PBX 6TX/4FX	28 32 50 6
Patch cable, CAT5, pre-assembled, 0.3 m long, 10 pieces	FL CAT5 PATCH 0,3	28 32 25 0
Patch cable, CAT5, pre-assembled, 0.5 m long, 10 pieces	FL CAT5 PATCH 0,5	28 32 26 3
Patch cable, CAT5, pre-assembled, 1.0 m long, 10 pieces	FL CAT5 PATCH 1,0	28 32 27 6
Patch cable, CAT5, pre-assembled, 1.5 m long, 10 pieces	FL CAT5 PATCH 1,5	28 32 22 1
Patch cable, CAT5, pre-assembled, 2.0 m long, 10 pieces	FL CAT5 PATCH 2,0	28 32 28 9
Patch cable, CAT5, pre-assembled, 3.0 m long, 10 pieces	FL CAT5 PATCH 3,0	28 32 29 2
Patch cable, CAT5, pre-assembled, 5.0 m long, 10 pieces	FL CAT5 PATCH 5,0	28 32 58 0
Patch cable, CAT5, pre-assembled, 7.5 m long, 10 pieces	FL CAT5 PATCH 7,5	28 32 61 6
Patch cable, CAT5, pre-assembled, 10.0 m long, 10 pieces	FL CAT5 PATCH 10	28 32 62 9

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

☎ + 49 - (0) 52 35 - 3-00
🖷 + 49 - (0) 52 35 - 3-4 12 00
🖳 phoenixcontact.com
🌐 Worldwide locations:
www.phoenixcontact.com/salesnetwork

A Appendix for document lists

A 1 Technical appendix

A 1.1 Simple Network Management Protocol (SNMP)

A 1.1.1 General function

SNMP is a non-proprietary 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 terminals, 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 (Requests 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 (object name and parameters) is assigned to an object ID 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 and the password “private” is used 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

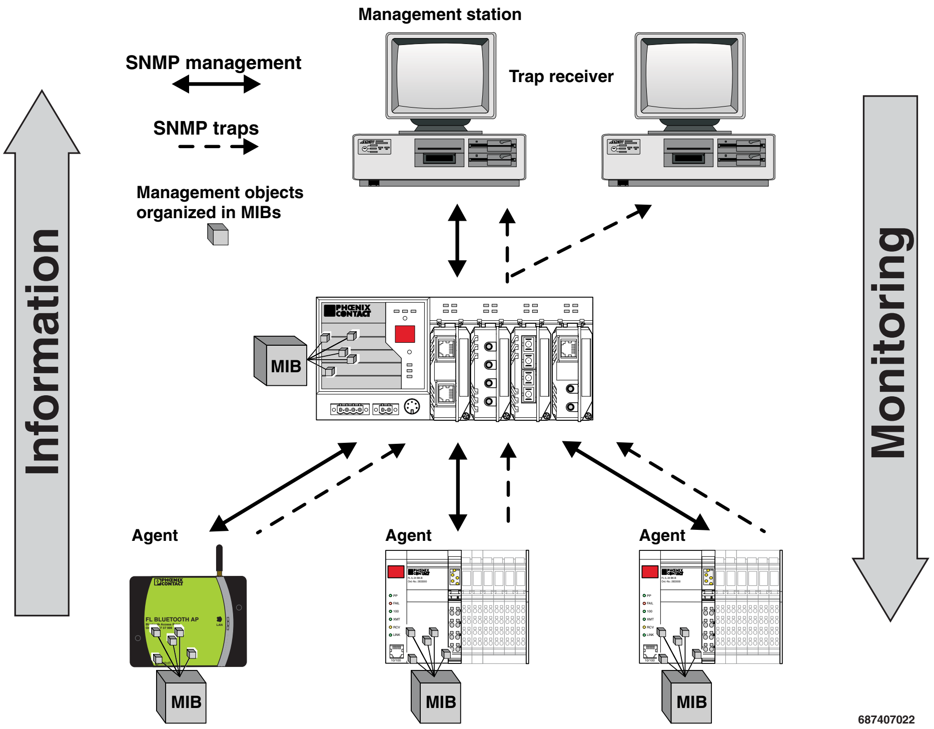


Figure 6-1 Schematic view of SNMP

A 1.1.2 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.

A 1.2 Setting the system time and using SNTP

A 1.2.1 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.

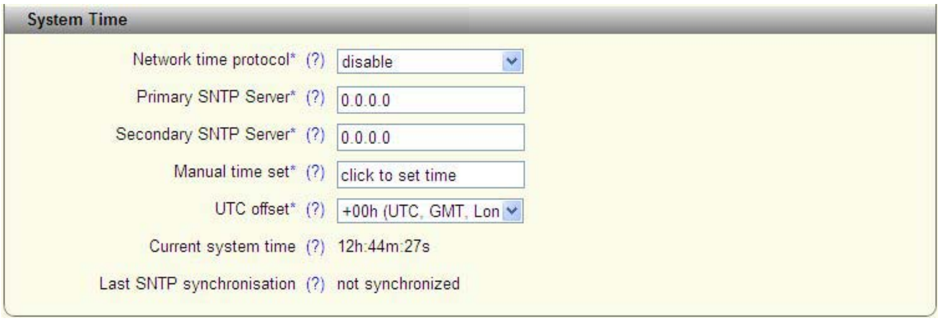
Time synchronization provides valuable assistance when evaluating error and event logs, as the use of time synchronization in various network components enables events to be assigned and analyzed more easily. Clients should therefore only be activated at the most extreme points of an NTP network.

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 therefore constantly corrected. In NTP, synchronization 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 therefore constantly corrected
- Synchronization is carried out in Universal Time Coordinated (UTC) format

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



System Time

Network time protocol*	(?)	disable
Primary SNTP Server*	(?)	0.0.0.0
Secondary SNTP Server*	(?)	0.0.0.0
Manual time set*	(?)	click to set time
UTC offset*	(?)	+00h (UTC, GMT, Lon
Current system time	(?)	12h:44m:27s
Last SNTP synchronisation	(?)	not synchronized

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.

B 1 List of figures

C 1 List of tables