



FL WLAN 1100/1101

User manual

UM EN FL WLAN 1000

User manual

FL WLAN 1100/1101

2017-05-03

Designation: UM EN FL WLAN 1000

Revision: 01

Order No.: —

This user manual is valid for:

Designation

FL WLAN 1100

FL WLAN 1101

Order No.

2702534

2702538

Please observe the following notes

User group of this manual

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

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

Explanation of symbols used and signal words



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

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

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

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

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



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



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

How to contact us

Internet

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

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 improvement of the contents and layout of our manuals, please send your comments to:

tecdoc@phoenixcontact.com

Please observe the following notes

General terms and conditions of use for technical documentation

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

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

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

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

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

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

Table of Contents

1	Technical description	7
1.1	General description	7
1.2	FL WLAN 110x country registrations	8
1.2.1	FL WLAN 1100	8
1.2.2	FL WLAN 1101	8
1.3	Firmware	10
2	Mounting/antenna configuration	11
2.1	Connections and operating elements	11
2.1.1	Housing dimensions	12
2.1.2	Electrical connection	12
2.1.3	Mounting the device on a level surface	14
2.1.4	Mounting the device with cable feed-through and seal	16
3	Startup and configuration	19
3.1	Delivery state/factory settings.....	19
3.1.1	Meaning of diagnostic and status indicators	19
3.1.2	General sequence for startup	20
3.1.3	Assigning the IP address via BootP (with IPAssign)	21
3.1.4	Assigning the IP address using IPAssign.exe	21
3.1.5	Reset to the factory settings	23
3.2	Startup via the web interface	24
3.2.1	General information in the web interface	24
3.2.2	Quick Setup	25
3.3	Operating modes of the device.....	27
3.3.1	Operating mode: Access Point	27
3.3.2	Operating mode: Client	28
3.3.3	Operating mode: Repeater	31
3.4	Firmware update.....	32
3.4.1	HTTP	32
3.4.2	TFTP	32
4	Configuration and diagnostics via Command Line Interface (CLI) 33	
4.1	Using the Command Line Interface (CLI).....	33
4.2	Access to the CLI	33
4.3	Basic principles for using CLI commands	34
4.4	Command syntax	34
4.5	Using the CLI Help.....	35

4.6	Auto-completion of commands.....	36
4.7	Using the CLI Network Scripting UI.....	36
5	Diagnostics	39
5.1	WLAN signal strength diagnostics in client mode	39
5.2	WLAN channel assignment diagnostics in access point mode	41
5.3	WLAN signal strength diagnostics in access point mode	41
6	Technical data	43
6.1	Ordering data	46

1 Technical description



Unless otherwise expressly stated, all information provided in this user manual always applies to both the FL WLAN 1100 and the FL WLAN 1101.

1.1 General description

Robust, compact WLAN module with integrated antennas:

- Turnkey solution with integrated antenna and wireless module in a single device
- Space savings in the control cabinet, optimized for mounting directly on machines, mobile units or control cabinets
- Fast and reliable wireless communication, thanks to powerful MIMO antennas
- Quick and easy connection, thanks to single-hole mounting
- Extremely robust housing, shock-proof according to IK08
- Operation as a WLAN access point, client or repeater
- Supports WLAN 802.11 standards a, b, g, and n
- Operation in the 2.4 GHz and 5 GHz band



Figure 1-1 FL WLAN 1100

1.2 FL WLAN 110x country registrations

1.2.1 FL WLAN 1100

The FL WLAN 1100 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. It is approved for use in Europe.



An up-to-date list of additional country registrations can be found in the e-shop at phoenixcontact.net/product/2702534.



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

Approvals for other countries are available on request.

1.2.2 FL WLAN 1101



The FL WLAN 1101 device, Order No. 2702538, 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 1101 device:

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

1.2.2.1 FCC information

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

NOTICE:

This Class A digital apparatus complies with Canadian ICES-003. Cet appareil numérique de la classe A 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 GmbH & Co. KG may void the FCC authorization to operate this equipment.

Radiofrequency radiation exposure Information:

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 être placé au même endroit ou utilisé simultanément avec un autre transmetteur ou antenne.

1.3 Firmware

Table 1-1

Firmware version	Functions
FW 1.0x	Initial 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/2702534.

2 Mounting/antenna configuration

2.1 Connections and operating elements

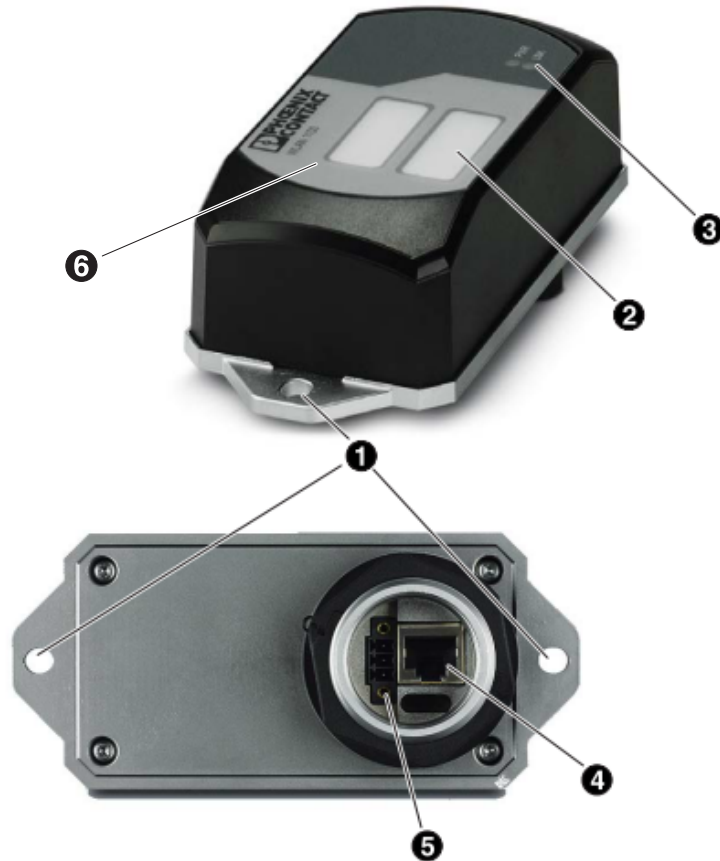


Figure 2-1 Connections and operating elements of the device

1. Mounting holes
2. Marking fields
3. Status and diagnostic LEDs
4. Ethernet connection in RJ45 format with 100 Mbps
5. Connections for supply voltage and one digital input via COMBICON
6. Two integrated WLAN antennas

2.1.1 Housing dimensions

The outside dimensions of the FL WLAN 1100 and FL WLAN 1101 devices are 62.8 mm x 36.5 mm x 113.2 mm (width x height x depth).

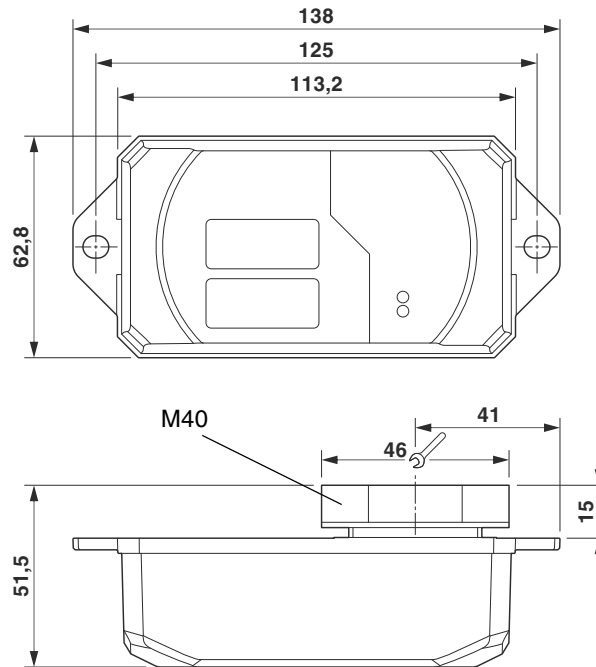


Figure 2-2 Housing dimensions and distances

2.1.2 Electrical connection

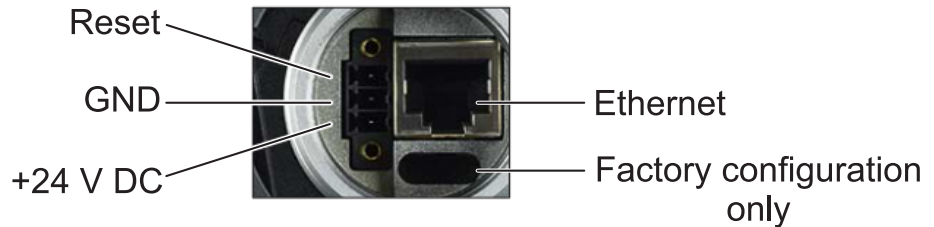


Figure 2-3 Connection of the supply voltage, Ethernet, and the reset input

The supplied connector is an FMC 1,5/ 3-STF-3,5 (Order No. 1966101).



A cable with a cross section of 0.75 mm² and a trapezoidal or square crimped ferrule that is 10 mm long is recommended.
Always use the appropriate conductor cross section and ferrules to ensure that the cable is fixed securely.

Table 2-1 Connection data for the connector

Conductor cross section solid/stranded min.	0.2 mm ²
Conductor cross section solid/stranded max.	1.5 mm ²
Conductor cross section stranded with ferrule without plastic sleeve min.	0.25 mm ²
Conductor cross section stranded with ferrule without plastic sleeve max.	1.5 mm ²
Conductor cross section stranded with ferrule with plastic sleeve min.	0.25 mm ²
Conductor cross section stranded with ferrule with plastic sleeve max.	0.75 mm ²
Conductor cross section AWG min.	24
Conductor cross section AWG max.	16
Conductor cross section AWG min. according to UL/CUL	24
Conductor cross section AWG max. according to UL/CUL	16

2.1.2.1 Assignment of the RJ45 Ethernet connectors

Table 2-2 Pin assignment of RJ45 connectors

Pin number	10Base-T/10 Mbps	100Base-T/100 Mbps
1	TD+ (transmit)	TD+ (transmit)
2	TD- (transmit)	TD- (transmit)
3	RD+ (receive)	RD+ (receive)
4	-	-
5	-	-
6	RD- (receive)	RD- (receive)
7	-	-
8	-	-

2.1.2.2 Grounding of the device 



Grounding protects people and machines against hazardous voltages. To avoid these dangers, as far as possible, correct grounding, taking the local conditions into account, is vital.



Functional grounding of the device:
The device must be connected to ground (functional earth ground) via the metal part of the housing. If this is not possible, ensure a low-resistance ground connection (functional earth ground) for the shielding of the Ethernet cable.

FL WLAN 1100 and FL WLAN 1101: it is recommended that the base plate of the device is grounded by connecting the mounting screws to a grounded metal surface (functional earth ground/FE).

If this is not possible, e.g., because the device is installed on a plastic surface, you must make sure that the Ethernet cable is properly shielded. This is particularly important if the housing is not grounded by other means, e.g., via the base plate.

2.1.3 Mounting the device on a level surface

The devices in the FL WLAN 110x series are designed for external mounting on control cabinets, machines, automatic guided vehicle (AGV) systems or similar equipment.

To mount the device on a level surface, a bore hole is required for the mounting flange (40 mm in diameter). The nut must be tightened (8 - 10 Nm maximum) to ensure a tight seal. The device can be additionally secured to the surface with two screws (M6). When using this additional screw connection, make sure that the entire system is sealed tight.

The device can be installed in any mounting position.

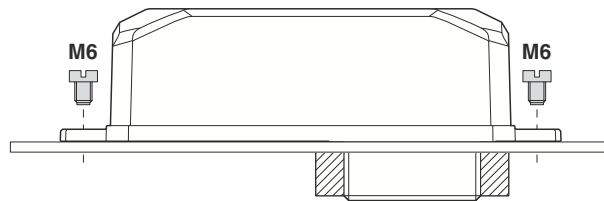


Figure 2-4 Mounting on a level surface

2.1.3.1 Drill hole template

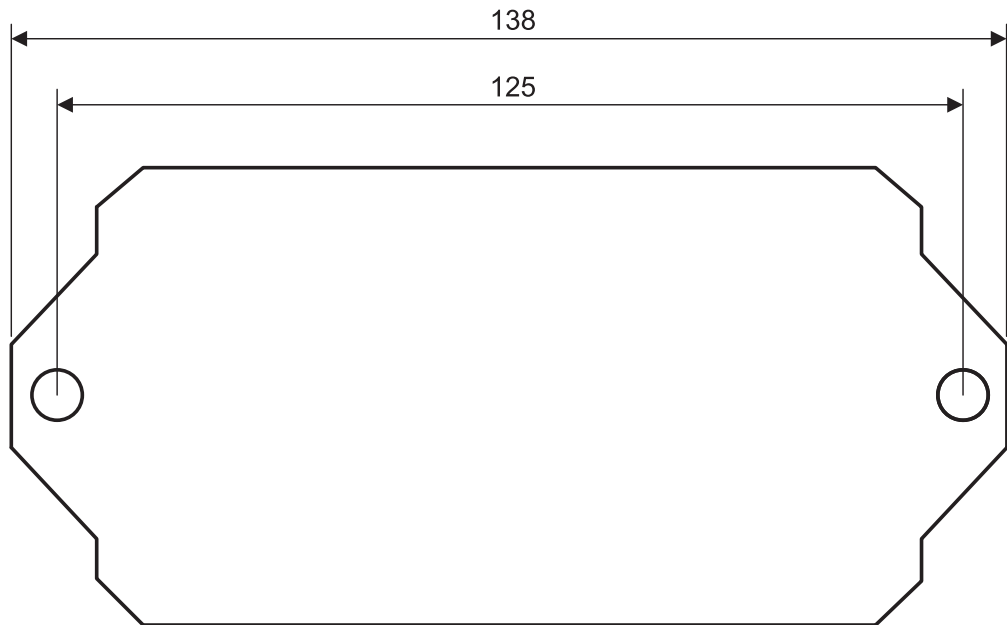


Figure 2-5 Drill hole template (original size)

2.1.4 Mounting the device with cable feed-through and seal

When mounting the device outside the control cabinet (e.g., on a mounting bracket), a cable feed-through with seal can be used to seal the connection dome for the supply line. The metal cable feed-through (FL M32 ADAPTER, Order No. 2702544) screws into the M32 internal thread of the FL WLAN 1100 connection dome. The FL WLAN 1100 is therefore sealed to IP54 even outdoors.

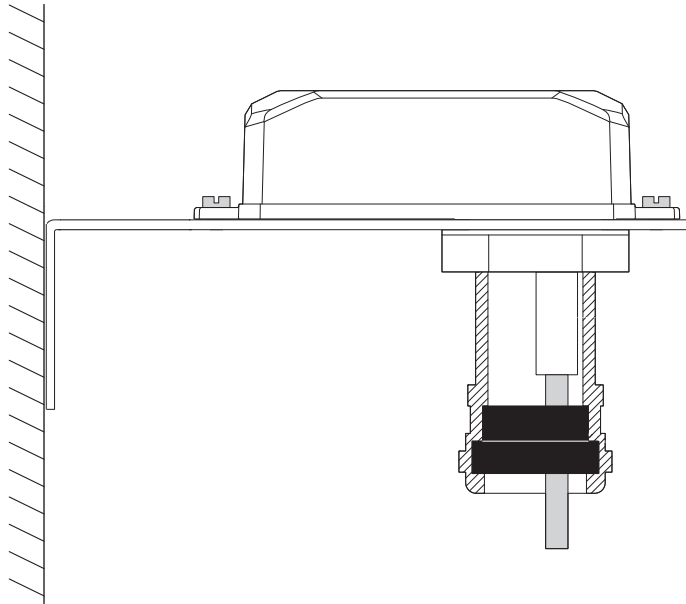


Figure 2-6 Mounting on a mounting bracket. If the device is not mounted directly on a control cabinet, use the FL M32 ADAPTER (Order No. 2702544) to create the seal.

2.1.4.1 Handling the FL M32 ADAPTER

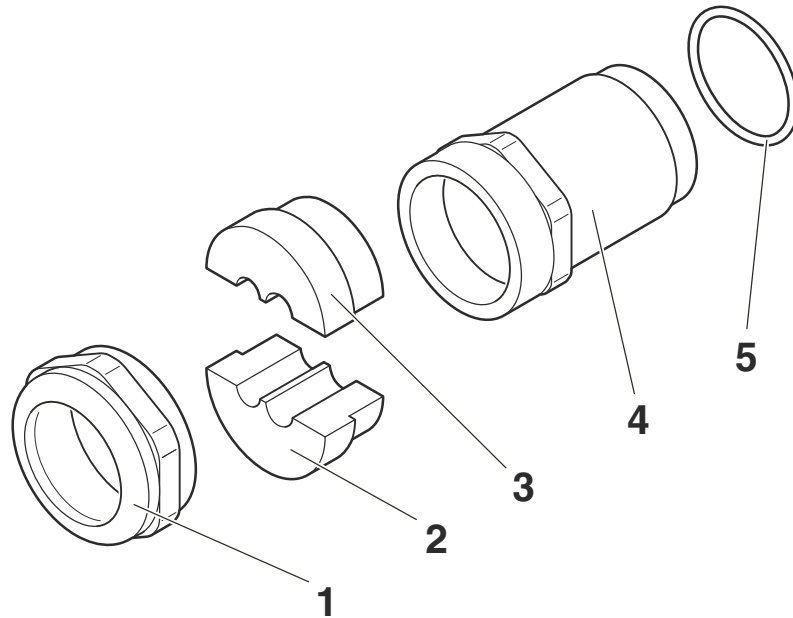


Figure 2-7 Handling the FL M32 ADAPTER

2.1.4.2 Tightness of seal, retention, and strain relief (in accordance with EN 50262)

Tightening torque (double nipple): 15 Nm for M32

Tightening torque (pressure screw): 20 Nm for Pg29

Tightness of seal for 7 mm hole pattern and 8.5 mm for cable:

IP65 protection is achieved in accordance with DIN EN 60529(2014.09) if the difference between the cable diameter and hole is less than 10%.

If both are the same, IP68 can be achieved up to 10 bar with defined "retention" in accordance with EN 50262 Class A. The tightness of seal and strain relief depend on the cable used.

2.1.4.3 Mounting taking the internal antennas into consideration

The FL WLAN 1100 has two internal antennas which transmit through the plastic housing. This must be taken into consideration when mounting the device: in order to ensure that the WLAN signal can be transmitted via the built-in antennas, the device must not be installed inside control cabinets or other metal housings.



The devices in the FL WLAN 110x series have internal antennas for WLAN communication. The device should therefore be mounted on the outside of metal objects so as to ensure that the WLAN signal can be transmitted.

In order to optimize the device's performance with respect to transmission, the same rules that apply when mounting antennas should be observed. An important criterion here is the lateral distance from conductive surfaces. These surfaces can influence the radio propagation (directional characteristics of the antenna) due to reflections and interference.

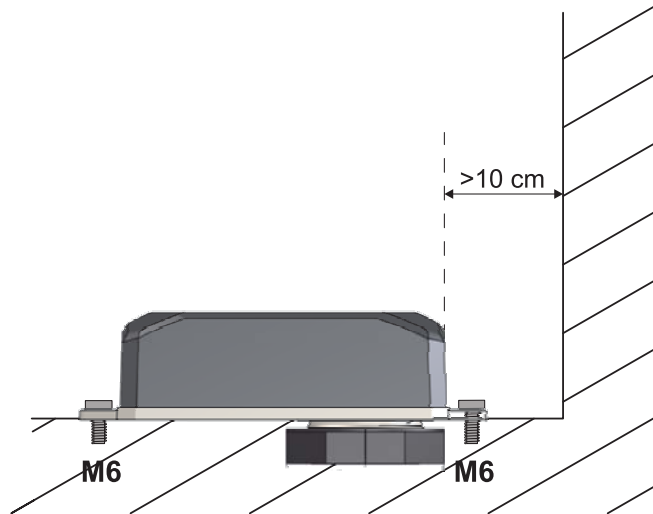


Figure 2-8 Mounting distance from lateral conductive surfaces

Due to its internal antennas, the device should not be located too close to conductive objects, if possible. Keep a distance of more than 100 mm, if possible. Smaller distances are possible, but they may adversely affect transmission.

3 Startup and configuration

3.1 Delivery state/factory settings

By default upon delivery or after the system is reset to the factory settings, the following functions and properties are available:

- The user name is: “admin”
- The password is: “private”
- All IP parameters are deleted. The device has no valid IP address
- BootP is activated

Installation notes

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.



NOTE: Statement regarding RF emission

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

3.1.1 Meaning of diagnostic and status indicators

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

Table 3-1 Meaning of diagnostic and status indicators

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

*WLAN connection established (blue):

Whether data transmission occurs depends on whether the passwords and certificates are valid. A WLAN connection can therefore exist even if data cannot be transmitted. If WLAN authentication fails, this is indicated in the log file.

3.1.2 General sequence for startup

During startup, supply the device with operating voltage (nominal value: 24 V DC). The assignment of the connector is shown in Unknown source of cross-reference.

In order to start up the device, the device must first be assigned an IP address. This is done via BootP. The IP address is allocated by a corresponding server in the network or a PC tool (see "Assigning the IP address using IPAssign.exe" on page 21 or "Assigning the IP address using IPAssign.exe" on page 21). The device can then be configured via the web interface (WBM) or the Command Line Interface (CLI).

In any case, the device must be connected via its Ethernet interface and an appropriate cable (RJ45 connector) to the device used for configuration.

By default upon delivery (factory settings), the WLAN interface is deactivated for security reasons. Configuration via the WLAN interface is therefore not possible in this state.

The device can be configured by setting all parameters via the web interface (see "Startup via the web interface" on page 24) or the Command Line Interface (CLI). In order to do this, the device must first be assigned an IP address. The factory default setting is BootP.

3.1.3 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/product/2702534. 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.

3.1.4 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 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.

Step 2: “IP Assignment Wizard”



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

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

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

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

- Click on 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.

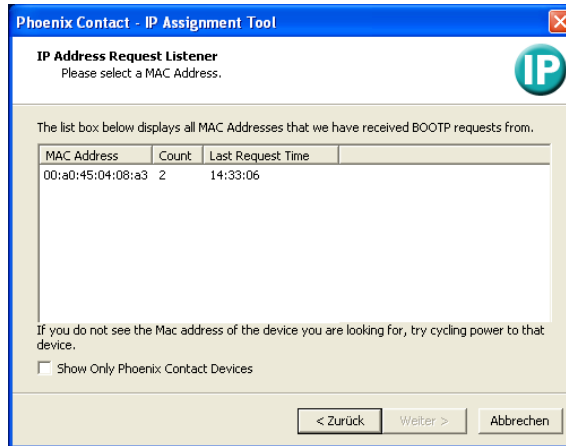


Figure 3-1 “IP Address Request Listener” window

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

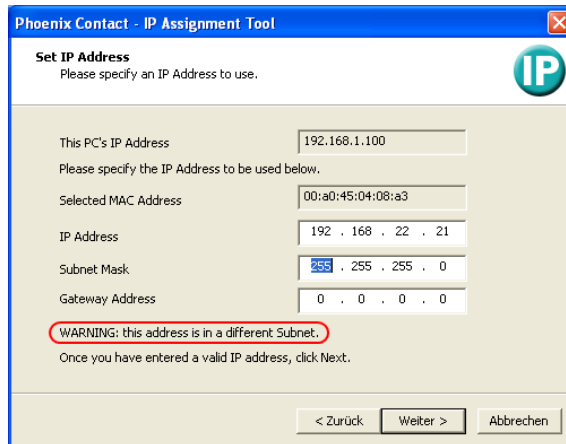


Figure 3-2 “Set IP Address” window with incorrect settings

- 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.

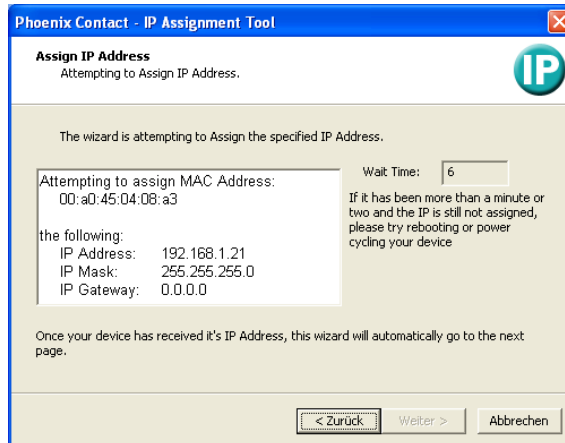


Figure 3-3 “Assign IP Address” window

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.

3.1.5 Reset to the factory settings

The device has a digital input. This digital input on the device is used exclusively to reset the device to the factory settings.

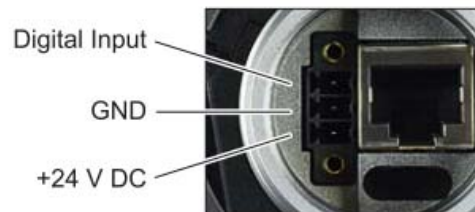


Figure 3-4 Connection of the supply voltage and the digital input on the bottom of the device

3.1.5.1 Detailed instructions for resetting the device to the factory settings:

Connect the device to the supply voltage.

As soon as the device has started up and is ready for operation, you have 1 minute to reset the device to the factory settings. To do this, the digital input must be supplied with voltage equivalent to the operating voltage. The operating voltage must be applied at the digital input for at least 5 seconds. The device is then reset to the factory settings and restarted.

3.2 Startup via the web interface



WBM of the device is optimized for Mozilla Firefox.

3.2.1 General information in the web interface

3.2.1.1 Web interface icons

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

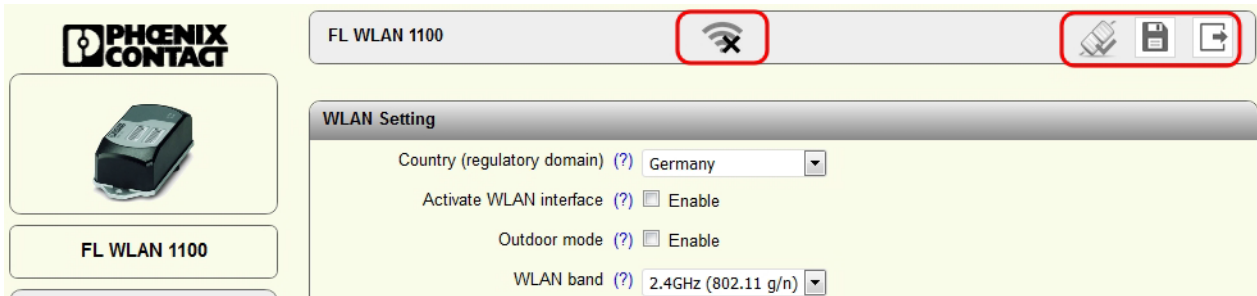







Figure 3-5 Web page with overview icons

Meaning of the individual icons:

Table 3-2 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.

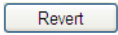
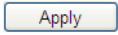
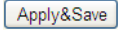
Table 3-2 Meaning of the icons [...]

Icon	Meaning
	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 3-3 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.

3.2.2 Quick Setup

The “Quick Setup” feature on the web page allows you to quickly configure the minimum requirements of a WLAN network. You are guided through the individual menus by a wizard. 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.
- In order to address the device, an IP address is assigned to it via BootP. To do this, an appropriate tool is needed on the PC (for details, see “Assigning the IP address via BootP (with IPAssign)” on page 21).
- Using a browser, go to the assigned IP address.
- In web-based management, select “Quick Setup”.

- Login: enter “admin” as the user name and “private” as the password.

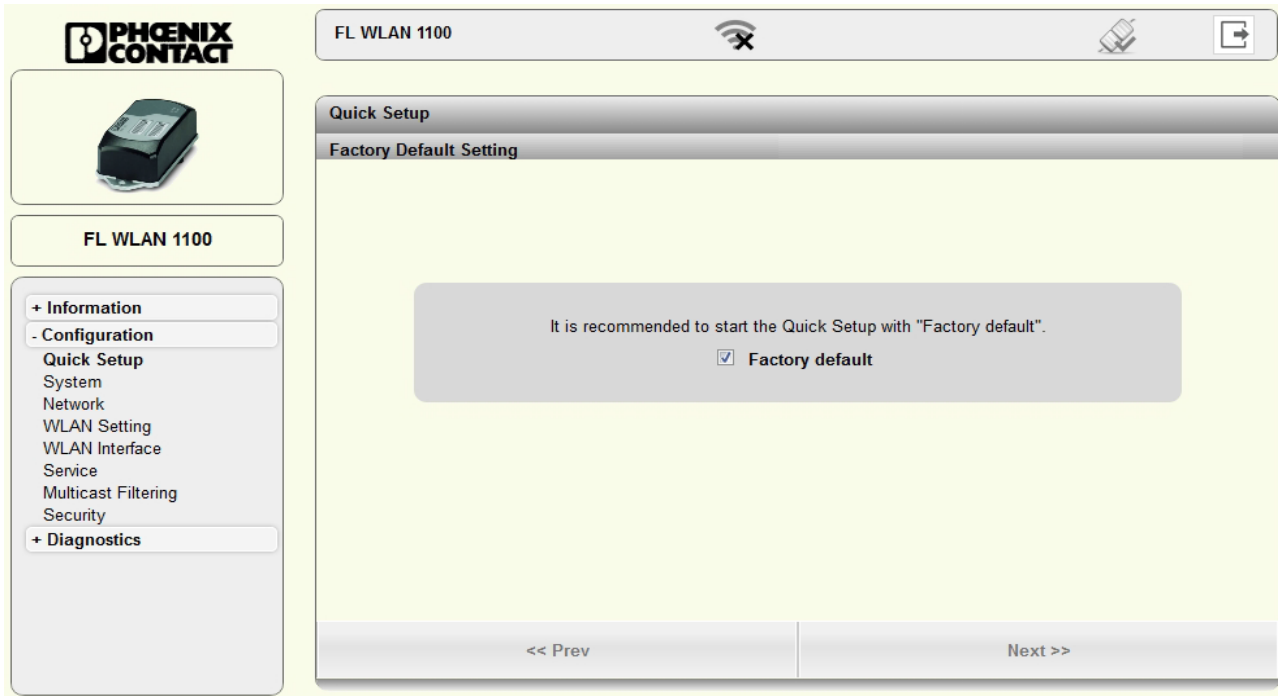


Figure 3-6 “Login” web page

On the “Quick Setup” page, a wizard guides you through all the relevant parameters for basic configuration. Please note the option on the first page to configure the device from the factory settings (“Factory default”). If you select this option, all configuration settings previously made will be deleted.

At the end of the wizard, you are prompted to confirm all the settings that have been made. The device is then rebooted again in order to apply all the settings.

3.3 Operating modes of the device

The device supports “Access Point”, “Client”, and “Repeater” 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.

3.3.1 Operating mode: Access Point

In “Access Point” mode, the FL WLAN 110x 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.

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 110x is already optimized for fast roaming in Client mode. The user can only improve effectiveness by restricting channels via the “Roaming list” under “WLAN interface”.

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.

3.3.2 Operating mode: Client

3.3.2.1 Compatibility between different WLAN device manufacturers

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

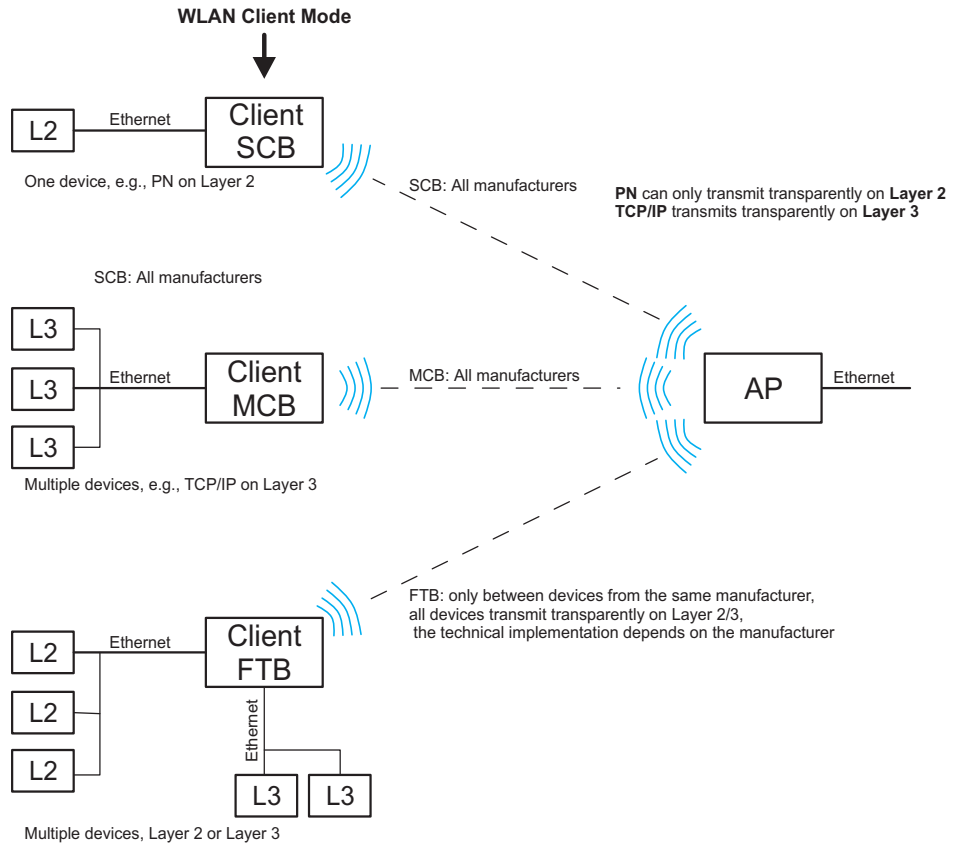


Figure 3-7 Overview of the various client modes

3.3.2.2 Operation as a single client

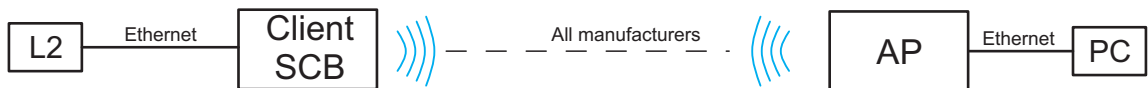


Figure 3-8 Diagram: single client mode

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 110x. 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 110x (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.

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 110x 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 110x 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 110x can be accessed via WLAN.

3.3.2.3 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 Ether-Net/IP™.

3.3.2.4 Operation as a fully transparent bridge (default)

Properties:

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



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

- An FTB connection between the FL WLAN 110x 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.

3.3.3 Operating mode: Repeater

The FL WLAN 110x 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. This repeater function allows for the creation of a linear structure. A meshed network or rings cannot be created.



It is recommended that no more than two repeaters are operated in a line, as the transmission speed is drastically reduced.

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.

3.3.3.1 Configuration of Repeater mode

Configuration of the repeater



All FL WLAN 110x 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.

3.4 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.

3.4.1 HTTP

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

The firmware is loaded, and “Update in progress...” indicates the update status.

“Firmware Update successful” 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 is done automatically if the corresponding preset was left enabled in the “Firmware Update” pop-up window.

3.4.2 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.
- Start the TFTP file transfer by clicking on the “Apply” 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.

4 Configuration and diagnostics via Command Line Interface (CLI)

4.1 Using the Command Line Interface (CLI)

The Command Line Interface (CLI) is a text-based tool that can be used to configure and diagnose the device. The CLI is accessed by means of a connection via Telnet (factory default) or SSH. The configuration of the CLI service via the device's web-based management is described in "Assigning the IP address via BootP (with IPAssign)" on page 21.

4.2 Access to the CLI

The CLI is accessed via a Telnet connection (factory default) or SSH connection from a management host, e.g., a PC. For example, the Windows command prompt or the PuTTY freeware tool can be used as an input terminal.

The device requires an IP address and a subnet mask in order to access the CLI. The configuration of the device network parameters is described in "Assigning the IP address via BootP (with IPAssign)" on page 21.

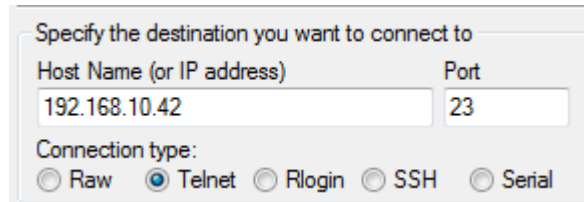


Figure 4-1 Configuration of a Telnet connection in PuTTY

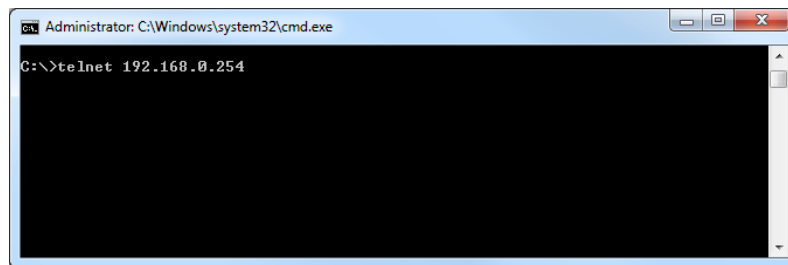


Figure 4-2 Initialize a connection with Windows

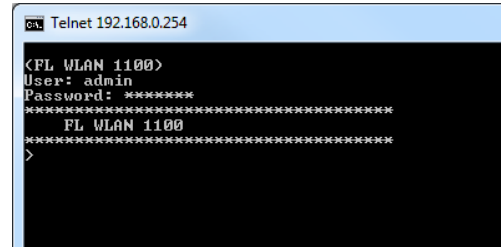


Figure 4-3 Command terminal in Windows command prompt

4.3 Basic principles for using CLI commands

In this section, the **CLI command names** are written in bold. *CLI parameters* are written in italics and must be replaced by appropriate values (e.g., names or numbers). If a command has several parameters, the order of these must be strictly observed.

The parameters of a command may be mandatory, optional or a selection of values (see Table “Structure of CLI commands” on page 34).

Table 4-1 Structure of CLI commands

Symbol	Example	Description
< > Angle brackets	<Value>	Denotes a mandatory parameter that must be entered in place of the brackets
[] Square brackets	[Value]	Denotes an optional parameter that can be entered in place of the brackets
{ } Braces	{choice1 choice2}	Denotes the mandatory selection of a value from a given list of values
Vertical bar	choice1 choice2	Separates mutually exclusive selection options
[{ }] Braces within square brackets	[{choice 1 choice 2}]	Denotes a selection within an optional parameter

4.4 Command syntax

A command consists of one or more terms which can be followed by one or more parameters. These parameters can be mandatory or optional values.

Some commands, e.g., **show network** or **clear config**, do not require parameters. Other commands, e.g., **network parms**, require values to be specified after the command name. The parameters must be entered in the specified order, whereby optional parameters always follow mandatory parameters.

The following example illustrates the syntax using the command **network parms**:

network parms <ipaddr> <netmask> [gateway]

- **network parms** is the command name.
- <ipaddr> and <netmask> are parameters and represent mandatory values, which must be specified after the entry of the command name.
- [gateway] is an optional parameter, which means that a value does not have to be specified.

The following examples illustrate the correct syntax for entering the **network parms** command:

network parms 192.168.10.42 255.255.255.0

network parms 192.168.10.42 255.255.255.0 192.168.10.0

The following examples illustrate incorrect syntax for entering the **network parms** command:

network parms 192.168.10.42 - missing mandatory parameter

network parms 255.255.255.0 - missing mandatory parameter

network parms 255.255.255.0 192.168.10.42 - incorrect parameter sequence

4.5 Using the CLI Help

Entering a question mark (?) in the command prompt displays a list of all the commands currently available together with a brief description.

Table 4-2 Structure of CLI commands

Command	Description
?	Display available commands

Typing a question mark (?) after each entry displays all the available command names or parameters from this point on.

```
>spanning-tree

port          Configure spanning tree port parameter.
max-age       Configure bridge maximum aging time.
fwd-delay     Configure bridge forward delay.
hello-time    Configure bridge hello time.
bdg-prio      Configure bridge priority.
frd           Configure fast ring detection.
lts           Configure large tree support.
status        Select spanning tree status.

>spanning-tree bdg-prio
```

If the Help output displays a parameter in angle brackets, this parameter must be replaced by a value. Example:

<ipaddr> Enter the IP address

```
>network parms
<ipaddress>      Enter IP address.
>network parms 192.168.10.43
```

If at any point there are no further command names or parameters available or further parameters are optional, the following message appears in the output prompting you to execute the command that was entered:

<cr> Press Enter to execute the command

```
>show mrp
<cr>              Press Enter to execute the command.
>show mrp
OK
```

4.6 Auto-completion of commands

The Autocomplete command is an additional way of writing a command, provided enough letters have already been entered to clearly identify the command name. As soon as enough letters have been entered, press space or TAB to automatically complete the words.

```
>spanning-tree f
  2 Possibilities:
    fwd-delay
    frd
>spanning-tree fwd-delay
```

4.7 Using the CLI Network Scripting UI

The CLI Network Scripting UI enables CLI commands from scripts to be loaded onto the device via the network. This means that the device can be configured and diagnosed using a URL via PC or from a controller. Each command that is entered is confirmed by the device, either with OK (config commands) or by outputting the device data (show commands).

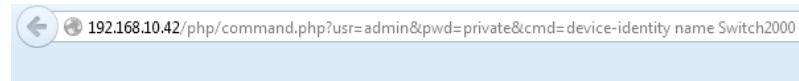
The command entry must follow a specific syntax:

`http://ipaddress/php/command.php?usr=username&pwd=password&cmd=cli_command_1 | cli_command_2 |`

The following examples illustrate the correct syntax for entering commands via the CLI Network Scripting UI:

Example: changing the device name

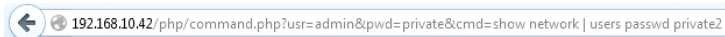
`http://192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=device-identity name Device2000`



OK

Example: displaying the network parameters and changing the user password

`http://192.168.10.42/php/command.php?usr=admin&pwd=private&cmd=show network | users passwd private2`



OK IP Assignment : bootp IP Address : 192.168.10.42 Network Mask : 255.255.255.0 Default Gateway : 0.0.0.0 Management VLAN : 1 ACD Mode : None ERROR

5 Diagnostics

5.1 WLAN signal strength diagnostics in client mode

If the FL WLAN 1000/2000 is in client or repeater mode, the current WLAN signal strength of the connected access point (or repeater) can be displayed. This function can be used to determine the signal strength when setting up wireless paths.

Thanks to the dynamic display, it is possible to determine the signal strength of an access point at various locations (e.g., mobile clients) or to determine the optimum alignment of an antenna in the case of a radio link.

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

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

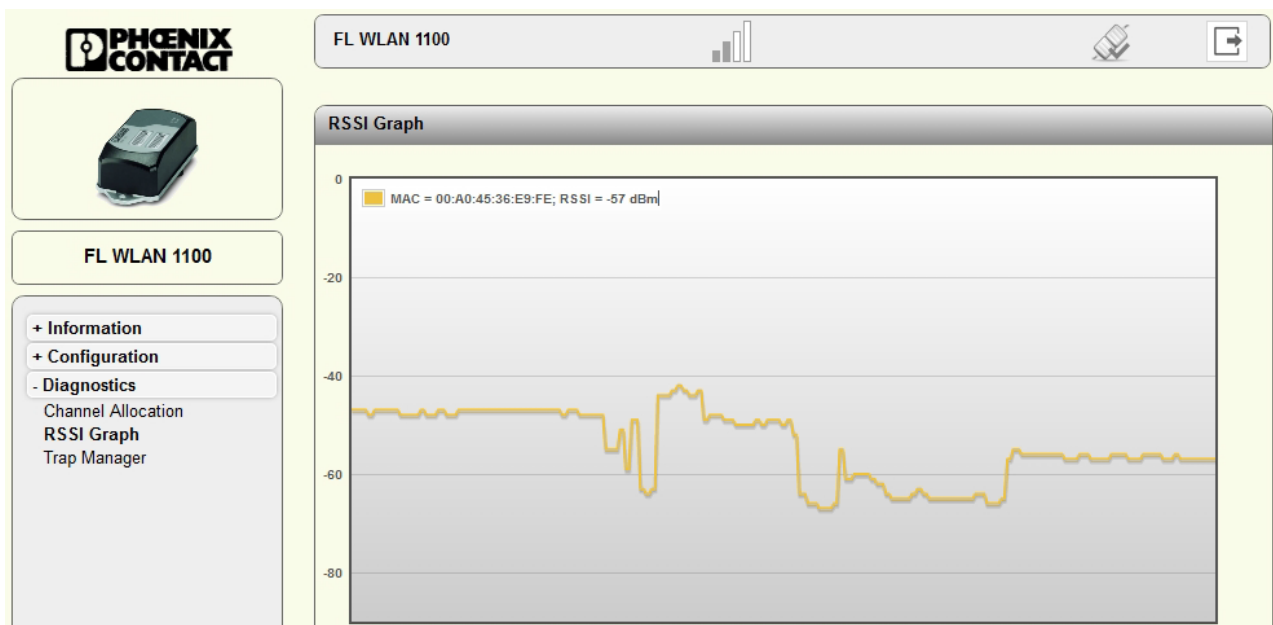


Figure 5-1 Display of the current WLAN signal strength in client mode



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.

The screenshot shows the web interface for a Phoenix Contact device. On the left, there is a navigation menu with sections: Information, Configuration, and Diagnostics. The main content area is titled 'FL WLAN 1100' and shows the 'Interface Status' for 'WLAN 1'. The status table includes: Operating Mode (Client (FTB)), Connect state (Accesspoint : 00:A0:45:36:E9:FE), Datarate (65 Mbps), Signal strength(RSSI) (-57 dBm), Network SSID (HALLO WELT), Security mode (WPA2-PSK AES), Current TX power (20 dBm), and Current WLAN Channel (36). Below the table, a bar graph shows the 'Current Signal Strength(RSSI)' as a green bar, with the value '-54dBm' displayed to its right. Below the bar graph, the 'Signal Strength min/avg/max' values are listed as '-71dBm/-55dBm/-35dBm'.

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 1000/2000 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.

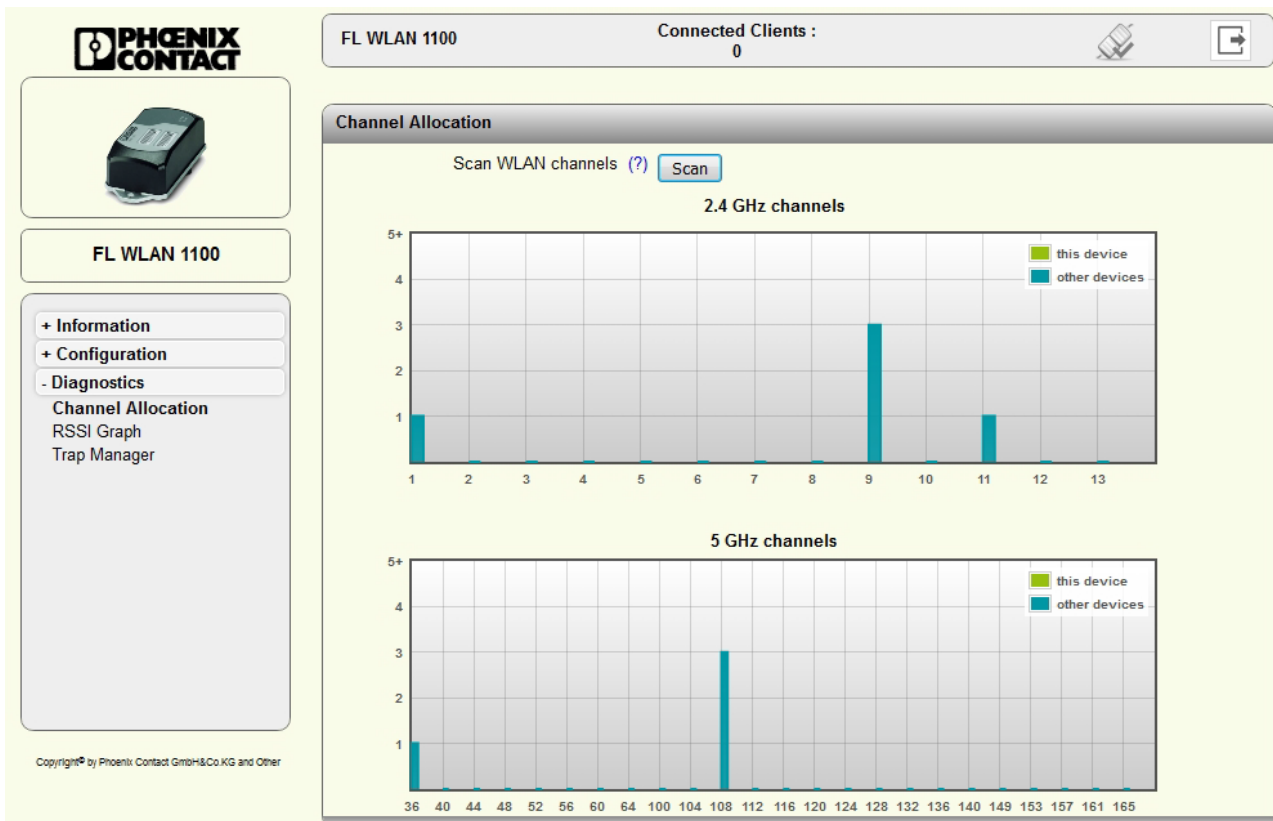


Figure 5-3 Display of WLAN channel assignment at the access point

5.3 WLAN signal strength diagnostics in access point mode

If the FL WLAN 1000/2000 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.

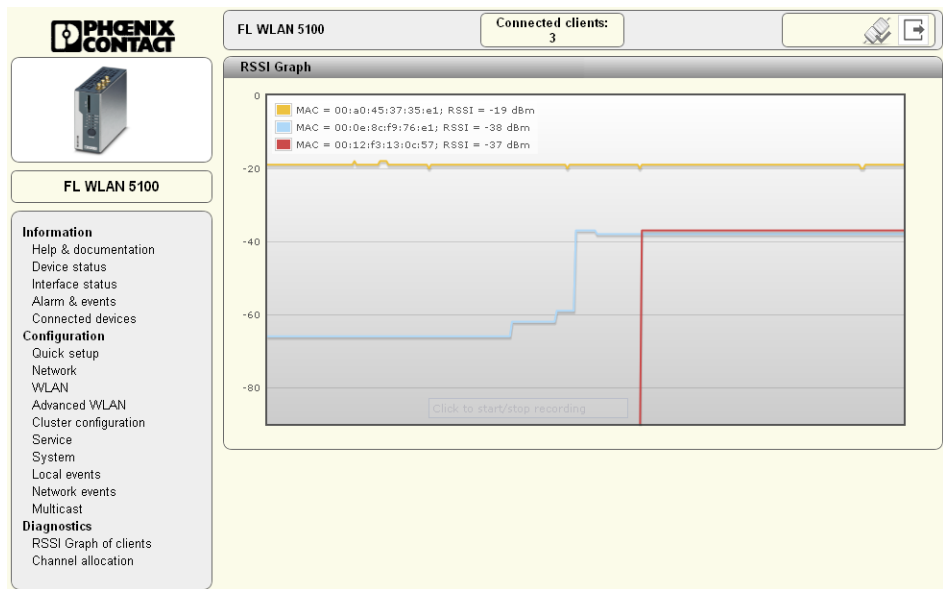


Figure 5-4 Display of the client signal strength at the access point



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

6 Technical data

General data	
Function	WLAN Ethernet access point/client/repeater, 2.4 GHz, 5 GHz, internal MIMO antennas
Housing dimensions (width x height x depth) in mm	
Mounting dimensions outside, without mounting clips	62,8 x 36,5 x 113,2 mm
Permissible operating temperature	0°C to 60°C
Permissible storage temperature	0°C to 70°C
Degree of protection	IP54
Humidity	
Operation	5% to 95%, non-condensing
Storage	5% 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	Any
Connection to protective earth ground	By means of lower housing part or additional screw connection
Configuration	Web-based management via http or https, SNMPv2/v3, CLI via Telnet/SSH, password-protected
Degree of pollution	2
Overvoltage category	none
Weight	340 g
Supply voltage	
Type of connection	Via MINI COMBICON Push-in spring connection Conductor cross section solid min.: 0.2 mm ² Conductor cross section solid max.: 1.5 mm ² Conductor cross section stranded min.: 0.2 mm ² Conductor cross section stranded max.: 1.5 mm ² Conductor cross section stranded with ferrule without plastic sleeve min.: 0.25 mm ² Conductor cross section stranded with ferrule without plastic sleeve max.: 1.5 mm ² Conductor cross section stranded with ferrule with plastic sleeve min.: 0.25 mm ² Conductor cross section stranded with ferrule with plastic sleeve max.: 0.75 mm ² Conductor cross section AWG min.: 24 Conductor cross section AWG max.: 16 AWG according to UL/CUL min.: 24 AWG according to UL/CUL max.: 16 Stripping length: 10 mm
Note on connection method	Recommended conductor cross section: 0.75 mm ² Recommended ferrule: connection length 10 Recommended crimping pliers: trapezoidal or square

FL WLAN 1100/1101

Supply voltage [...]

Nominal value	24 V DC / SELV
Range of supply voltages	18 V DC - 32 V DC, PELV/SELV
Current consumption at 24 V	120 mA typical @24 VDC 250 mA typical @18 V DC

Functions

Operating modes	Access Point / Client Adapter / Repeater
Configuration	Web-based Management, automated CLI
Quality of Service (QoS)	yes
Security	802.11i, WPA PSK, WPA2, AES, TKIP, MAC filter

Interfaces

RJ45 Ethernet interface

Number	1
Connection format	RJ45 socket on the device, Autonegotiation and Autocrossing
Data transmission speed	10/100 Mbps
Segment length	100 m
Assignment of the IP address	BootP

Wireless interface

Antenna connection	2 internal antennas, MIMO, permanently installed
Wireless standards for FL WLAN 1100 (Europa ETSI)	IEEE 802.11a/b/g/n, up to 300 Mbps
Wireless standards for FL WLAN 1101 (USA, Canada FCC/IC)	IEEE 802.11a/b/g/1
Wireless modules that can be connected	10 (in Access Point mode max. 2 SSIDs)
Gain	5 dBi

Security

Security mechanism	802.11i, WPA PSK, WPA2, AES, TKIP, MAC filter
--------------------	---

FL WLAN 1100 Regulatory Domain: Europe (ETSI)

Mode	Bandwidth (MHz)	Channel (at 40 MHz: central channel)	Maximum transmission power emitted (EIRP)
802.11b	20	1 to 13	20
802.11g	20	1 to 13	20
802.11n	20	1 to 13	20
	40	3 to 11	19
802.11a	20	36 to 140	18
802.11na	20	36 to 64	18
		100 to 140	19
	40	38 to 62	17
		102 to 138	17

FL WLAN 1101 Regulatory Domain: USA/Canada (FCC/IC)

Mode	Bandwidth (MHz)	Channel (at 40 MHz: central channel)	Maximum transmission power emitted (EIRP)
802.11b	20	1 to 20	20

802.11g	20	1 to 11	20
802.11ng	20	1	20
		2 to 10	20
		11	18
		3	14
		4 to 8	20
802.11a	40	9	12
		36 to 165	18
		36 to 64	18
802.11na	20	100 to 165	19
		38 to 62	17
	40	102 to 159	17

Mechanical tests

Shock testing according to DIN EN 60068-2-27/IEC 60068-2-27	30g, 11 ms half-sine shock pulse
Vibration resistance according to DIN EN 60068-2-6/IEC 60068-2-6	5g, 10 -150 Hz
Continuous shock according to EN 60068-2-27/IEC 60068-2-27	10g, 16 ms, 6000 shocks
Broadband noise according to EN 60068-2-64	Category 1, Class A

Conformance with EMC directives for the FL WLAN 1100

Noise emission according to EN 55022	Class B
Electrostatic discharge (ESD) according to EN 61000-4-2	Contact discharge: ±4 kV Indirect discharge: ±6 kV
Electromagnetic fields according to IEC 61000-4-3	80 MHz - 1000 MHz, 10 V/m 1000 MHz - 6000 MHz, 3 V/m
Conducted interference according to IEC 61000-4-6	0,15 MHz - 80 MHz, 10 V
Fast transients (burst) according to IEC 61000-4-4	± 2.2 kV
Surge voltages according to IEC 61000-4-5	± 0,5 kV symmetrical ± 1 kV asymmetrical

EMC data for FL WLAN 1101

Emitted interference in acc. to FCC/CFR 47, Part 15.107	Class B
Emitted interference in acc. to FCC/CFR 47, Part 15.109	Class A
Emitted interference in acc. to ICES-003 Issue 6 section 6.1	Class B
Emitted interference in acc. to ICES-003 Issue 6 section 6.2	Class A

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 1100	2702534
Access point, FCC approval, only for use in the USA and Canada	FL WLAN 1101	2702538
RJ45 connector, degree of protection: IP20, number of positions: 8, 1 Gbps, CAT5 (IEC 11801:2002), material: zinc die-cast, connection method: IDC fast connection, connection cross section: 26 - 24 AWG, cable outlet: straight	CUC-IND-C1ZNI-S/R4IE8	1421607
Plug, nominal current: 8 A, rated voltage (III/2): 160 V, number of positions: 3, pitch: 3.5 mm, connection method: Push-in spring connection, color: green, contact surface: tin	FMC 1,5/ 3-STF-3,5	1966101
FL M32 ADAPTER	FL M32 ADAPTER	2702544
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
 Flachmarktstr. 8
 32825 Blomberg
 Germany



+ 49 5235 3-00



+ 49 5235 3-41200



www.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.

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

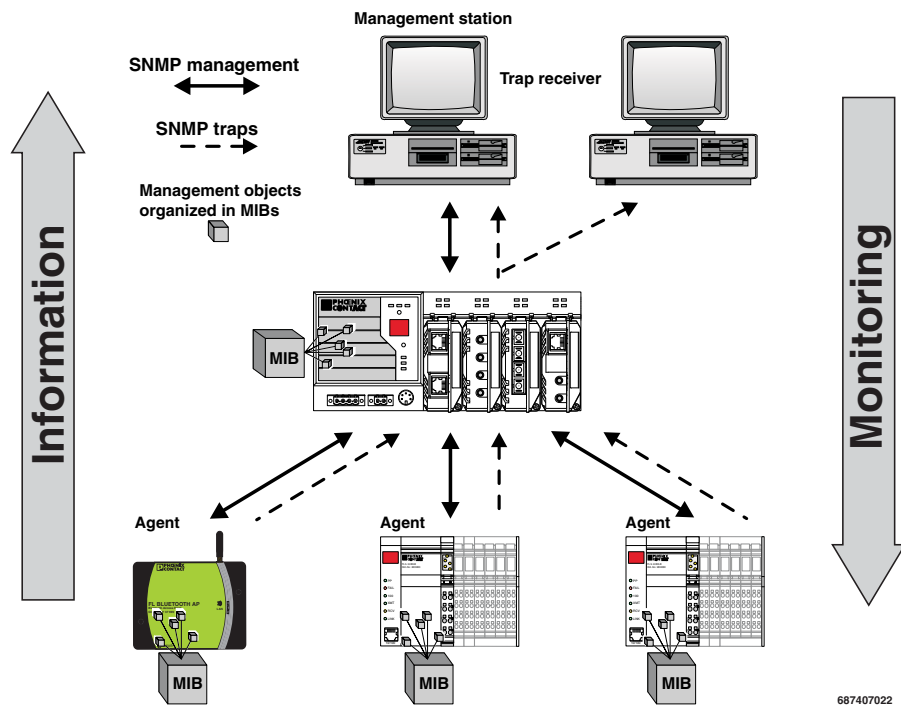


Figure 6-1 Schematic view of SNMP

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. 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.

B 1 List of figures

Figure 1-1:	FL WLAN 1100	7
Figure 2-1:	Connections and operating elements of the device	11
Figure 2-2:	Housing dimensions and distances	12
Figure 2-3:	Connection of the supply voltage, Ethernet, and the reset input	12
Figure 2-4:	Mounting on a level surface	14
Figure 2-5:	Drill hole template (original size)	15
Figure 2-6:	Mounting on a mounting bracket. If the device is not mounted directly on a control cabinet, use the FL M32 ADAPTER (Order No. 2702544) to create the seal.	16
Figure 2-7:	Handling the FL M32 ADAPTER	17
Figure 2-8:	Mounting distance from lateral conductive surfaces	18
Figure 3-1:	“IP Address Request Listener” window	22
Figure 3-2:	“Set IP Address” window with incorrect settings	22
Figure 3-3:	“Assign IP Address” window	23
Figure 3-4:	Connection of the supply voltage and the digital input on the bottom of the device	23
Figure 3-5:	Web page with overview icons	24
Figure 3-6:	“Login” web page	26
Figure 3-7:	Overview of the various client modes	28
Figure 3-8:	Diagram: single client mode	28
Figure 4-1:	Configuration of a Telnet connection in PuTTY	33
Figure 4-2:	Initialize a connection with Windows	33
Figure 4-3:	Command terminal in Windows command prompt	34
Figure 5-1:	Display of the current WLAN signal strength in client mode	39
Figure 5-2:	Display of the current signal strength as a bar graph	40
Figure 5-3:	Display of WLAN channel assignment at the access point	41
Figure 5-4:	Display of the client signal strength at the access point	42
Figure 6-1:	Schematic view of SNMP	48

C 1 List of tables

Table 1-1:	10
Table 2-1:	Connection data for the connector.....	13
Table 2-2:	Pin assignment of RJ45 connectors	13
Table 3-1:	Meaning of diagnostic and status indicators	19
Table 3-2:	Meaning of the icons.....	24
Table 3-3:	Meaning of the buttons	25
Table 4-1:	Structure of CLI commands	34
Table 4-2:	Structure of CLI commands	35

Mouser Electronics

Authorized Distributor

Click to View Pricing, Inventory, Delivery & Lifecycle Information:

[Phoenix Contact:](#)

[2702538](#) [2702534](#) [2702544](#)