FL EPA 2

User manual

UM EN FL EPA 2

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual
FL EPA 2

2018-02-21

Designation: UM EN FL EPA 2

Revision: 00

Order No.: —

This user manual is valid for:

Designation	Order No.
FL EPA 2	1005955
FL EPA 2 RSMA	1005957
FL BT EPA 2	1005869

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

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.

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.

Table of contents

1 FL EPA 2

1.1 Properties

The FL EPA 2 is an industrial wireless module for the wireless integration of industrial Ethernet and PROFINET devices in wired networks via WLAN and/or Bluetooth.

Typical applications for the FL EPA 2 include:

- Wireless network connection for industrial machines, devices and vehicles
- Ethernet cable replacement between moving machine parts

There are different ways of implementing the Bluetooth PAN profile in mobile devices. The implementation may be incompatible with the FL EPA 2. A Bluetooth PAN connection must be individually tested.

5 GHz WLAN cannot be used at the same time as 2.4 GHz WLAN or Bluetooth.

WLAN or Bluetooth?

WLAN is the preferred technology when it is important to integrate multiple devices with high data throughput and fast roaming.

Bluetooth offers particular advantages for applications requiring highly robust wireless connections or if precise channel planning is not possible.

1.1.1 Device versions

Three device versions are available:

–	FL EPA 2	Internal antenna, WLAN and Bluetooth	Order No. 1005955
–	FL EPA 2 RSMA	External antenna, WLAN and Bluetooth	Order No. 1005957
–	FL BT EPA 2	Internal antenna, Bluetooth (one device)	Order No. 1005869

Depending on the model, not all of the properties described above are available.

1.2 FL WLAN EPA ... country approvals

An up-to-date list of the country approvals can be found in the e-shop at

phoenixcontact.com.

2 Installation

CAUTION:
This device emits radio frequency (RF) energy in the ISM (Industrial, Scientific, Medical) band. Make sure that all medical devices used in proximity to this device meet appropriate susceptibility specifications for this type of RF energy.

NOTE:
This product is recommended for use in both industrial and domestic environments. Functional ground needs to be connected in industrial environments to comply with immunity requirements. For domestic environments the functional ground must be omitted if a shielded Ethernet cable is used, in order to meet the emission requirements.

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

2.1 General

NOTE:
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 is also required to read and understand this document and follow the instructions.

Observe the applicable national regulations regarding the operation, function tests, repair, and maintenance of electronic devices.

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

Observe the applicable regulations for using wireless devices outdoors.

2.2 Mechanical installation

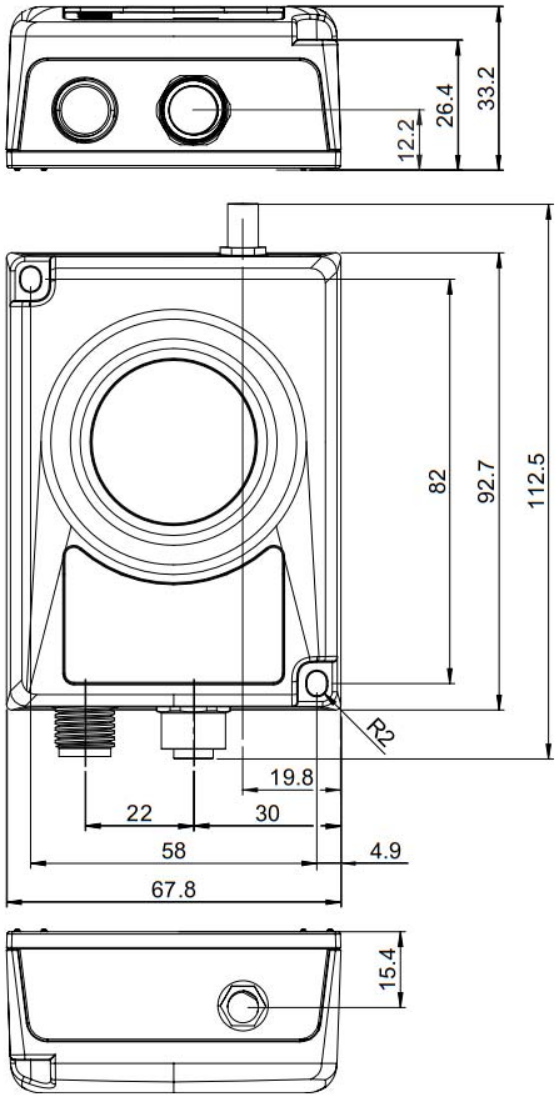


Figure 2-1 Assembly drawing (all dimensions in mm, antenna connection for the FL EPA 2 RSMA only)

2.2.1 DIN rail mounting

The FL EPA RMS mounting kit (Order No. 2701133) is available as an accessory for mounting the device on a 35 mm DIN rail.

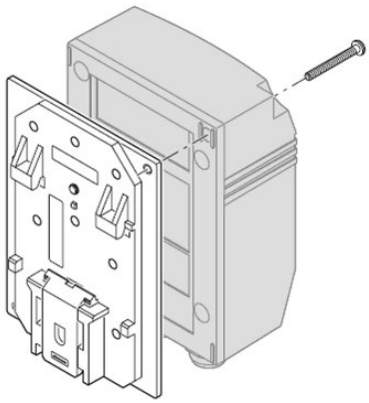


Figure 2-2 Fixing the EPA to the mounting kit for the DIN rail

- Use the two screws provided to fix the EPA to the base plate.
- Place the EPA with the adapter on the top edge of the DIN rail.
- Push the EPA towards the DIN rail until it snaps into place.
- For releasing the adapter from the DIN rail, pull the latch downwards using a screwdriver and simultaneously remove the EPA from the DIN rail.

2.2.2 Wall or mast mounting

The FL EPA WMS (Order No. 2701134) mounting kit can be used for EPA wall or mast mounting.

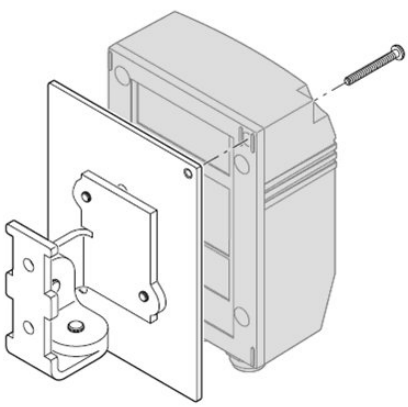


Figure 2-3 Fixing the EPA to the mounting kit for wall/mast mounting

- Use the two screws provided to fix the EPA to the base plate.
- The two 4.5 mm bore holes can be used for mounting. Two steel clamps are provided for mounting the EPA to a mast (25 mm ... 85 mm).

2.2.3 Connectors

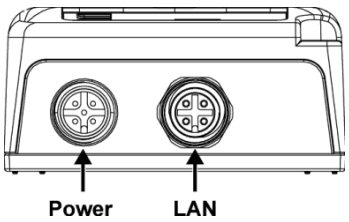
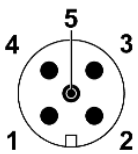


Figure 2-4 M12 connectors

Power connectors (M12 connectors, A-coded)

Table 2-1 M12 power connectors

Graphic	Pin	Function
	1	Power supply + (9 V DC ... 30 V DC)
	2	Digital input ground
	3	Power ground
	4	Digital input + (9 V DC ... 30 V DC)
	5	Functional ground

NOTE:
The signal line for the digital input must be carried in the same cable as power supply and functional ground if the line length exceeds 3 meters.

Table 2-2 LAN power connectors

Graphic	Pin	Function	Color coding (T568B)
	1	Transmit	Orange/white
	2	Receive	Green/white
	3	Transmit	Orange
	4	Receive	Green

2.3 Antenna connection (FL EPA 2 RSMA only)

The device is provided with an RSMA (female) antenna socket. Only use suitable antenna cables and adapters. The antenna socket may be damaged when trying to screw on wrong connectors.

Avoid the use of long and/or low-quality antenna cables. They cause additional attenuation and may reduce the range.

Torque the antenna cable to 1 Nm. Excessively high torques may damage the device.

2.4 LED indicators

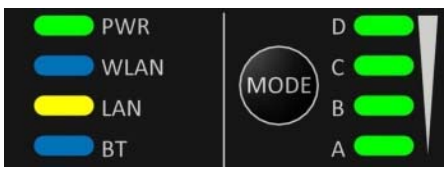


Figure 2-5 LED indicators

Table 2-3 Meaning of the LED indicators

LED	Color	Meaning
PWR	Off	No power
	Green	Normal operation
WLAN	Off	WLAN deactivated
	Flashing blue	Access Point mode: WLAN activated, no client connected
	Blue	Access Point mode: Connected to at least one client Client mode: Connected to Access Point
	Flashing blue rapidly	WLAN data activity (when connected)
	Flashing purple	Client mode: Scanning for Access Points
	Purple	Client mode: Connecting to a detected Access Point
	Red	Unrecoverable error
LAN	Off	No Ethernet connection
	Yellow	Ethernet link present
	Flashing yellow rapidly	Ethernet data activity (when connected)

Table 2-3 Meaning of the LED indicators (Fortsetzung)

LED	Color	Meaning
BT	Off	Bluetooth deactivated
	Flashing blue	NAP mode: Bluetooth activated, no client connected
	Blue	NAP mode: Connected to at least one PANU client PANU mode: Connected to NAP
	Flashing blue rapidly	Bluetooth data activity (when connected)
	Purple	PANU mode: Trying to connect to NAP
	Red	Unrecoverable error
A-B-C-D	Green	RSSI (received signal strength) or link quality

Table 2-4 Received signal strength indication via A-B-C-D LEDs

RSSI (WLAN client) / link quality (Bluetooth PANU)	A	B	C	D
No connection				
RSSI/link quality low	●			
RSSI/link quality sufficient	●	●		
RSSI/link quality good	●	●	●	
RSSI/link quality excellent	●	●	●	●

3 Configuration

There are different ways of configuring the EPAs for operation:

Easy Config (“MODE” button)

Typical operating modes, such as direct connection of two EPAs as a “wireless Ethernet cable”, can be directly activated via the “MODE” button on the EPA without the need for a PC. A detailed description can be found in Section 3.1 “Easy Config (“MODE” button)” on page 3-1.

Web-based management (WBM)

To use all the important options, the device has a web-based management using a web browser. This means that the current operating state can simply be displayed without the use of special software or the device can be configured.

For parameter description, please refer to Section “Web-based management” on page 4-1.

AT commands

All the EPA parameters can be modified or transmitted to the EPA in an automated manner, for example from a program of a controller. For development or testing purposes, AT commands can also be transmitted to the EPA via the web-based management using the web browser.

The AT command reference can be found, for example, in the web-based management application under the “Help” menu item.

3.1 Easy Config (“MODE” button)

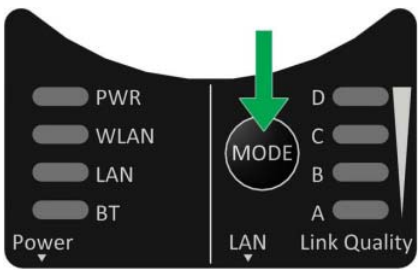


Figure 3-1 Control panel

The **“MODE”** button can be used to configure or reset the device.

The respective function is carried out when releasing the button (“falling edge”).

3.1.1 Using the “MODE” button

1. Switch on the device and wait for the Link Quality LEDs to light up and go out again. Then press and release the “MODE” button.

Step 1 must be carried out within 5 seconds after switching on the device.

2. Press the “MODE” button repeatedly to cycle through the Easy Config modes until the desired mode is indicated by the A-B-C-D LEDs.

Mode 2 is the first mode. Only suitable LED combinations are shown.

3. Press and hold the “MODE” button for at least two seconds, then release the button. This will confirm the selected mode and restart the device.

Step 3 must be carried out within 20 seconds after step 2. Otherwise the device will exit Easy Config setup and return to the previous settings.

3.1.2 Easy Config modes

Table 3-1 Received signal strength indication via the A-B-C-D LEDs

Mode	Role	RSSI (WLAN client) / link quality (Bluetooth PANU)	A	B	C	D
2	---	Reset configuration to factory defaults		●		
3	---	Reset IP settings to factory defaults	●	●		
4	Client	Wait for discovery and configuration			●	
5	WLAN AP	Configure the device as an Access Point, then discover devices in mode 4 and configure them accordingly as clients	●		●	
6	Bluetooth NAP	Configure the device as an Access Point, then discover devices in mode 4 and configure them accordingly as clients		●	●	
7	WLAN AP with PROFINET optimizations	Configure the device as an Access Point, then discover devices in mode 4 and configure them accordingly as clients	●	●	●	
8	Bluetooth NAP with PROFINET optimizations	Configure the device as an Access Point, then discover devices in mode 4 and configure them accordingly as clients				●
10	Add PROFINET optimizations only	Configure the device as an Access Point, then discover devices in mode 4 and configure them accordingly as clients		●		●

Modes 5 ... 8 are used for defining the operating mode of the network (WLAN/Bluetooth, with or without optimization for PROFINET operation). Set the device which will later act as an Access Point/NAP to the desired mode.

Configure the clients for mode 4. The Access Point or NAP then configures the devices in mode 4, matching the selected operating mode. As soon as a device is configured as a client, the device is restarted.

The Access Point scans for configurable devices for 120 s (the scan can be canceled by switching it off and on). The device is then also restarted. The connection is established automatically.

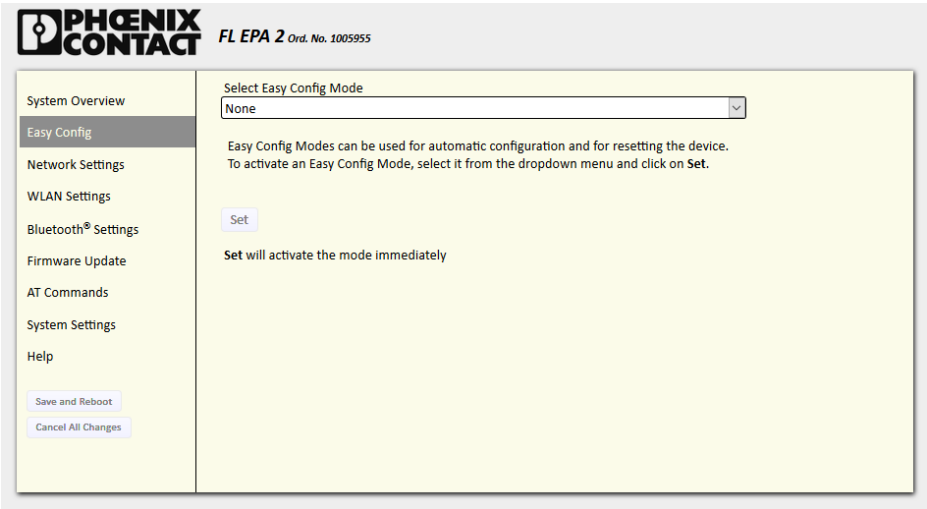


Figure 3-2 “Easy Config” web page

The Access Point retains the configured IP address. The clients/PANU are assigned the IP addresses in ascending order or - if not possible - in descending order.

Example: Based on the factory settings, the AP/NAP IP address is 192.168.0.254. The IP addresses 192.168.0.253, 252, … are then assigned to the clients.

If the AP has previously been configured to 192.168.3.50, it will retain this address. 192.168.3.51, 52, … are then assigned to the clients/PANU.

If several radio sets are used within a common backbone network, configuration via Easy Config may lead to the double assignment of IP addresses. This is due to the fact that each radio set starts with 192.168.0.254. In this case, assign unique addresses beforehand or subsequently using the web interface.

A WLAN connection is established on channel 6. The channel can also be changed subsequently using the Access Point web interface.

The connection is layer 2-transparent and thus also suitable for PROFINET.

For functionally safe communication, refer to the information in Section “Safety-related communication (PROFISafe/SafetyBridge)” on page 4-15.

4 Web-based management

4.1 General

The web-based management is accessed by pointing a web browser to the EPA IP address. The default IP address is 192.168.0.254. The computer accessing the web-based management must be in the same IP subnet as the wireless bridge.

The web-based management is designed for the current versions of Internet Explorer, Chrome, Firefox and Safari. Other browsers may not support the full functionality of the web-based management.

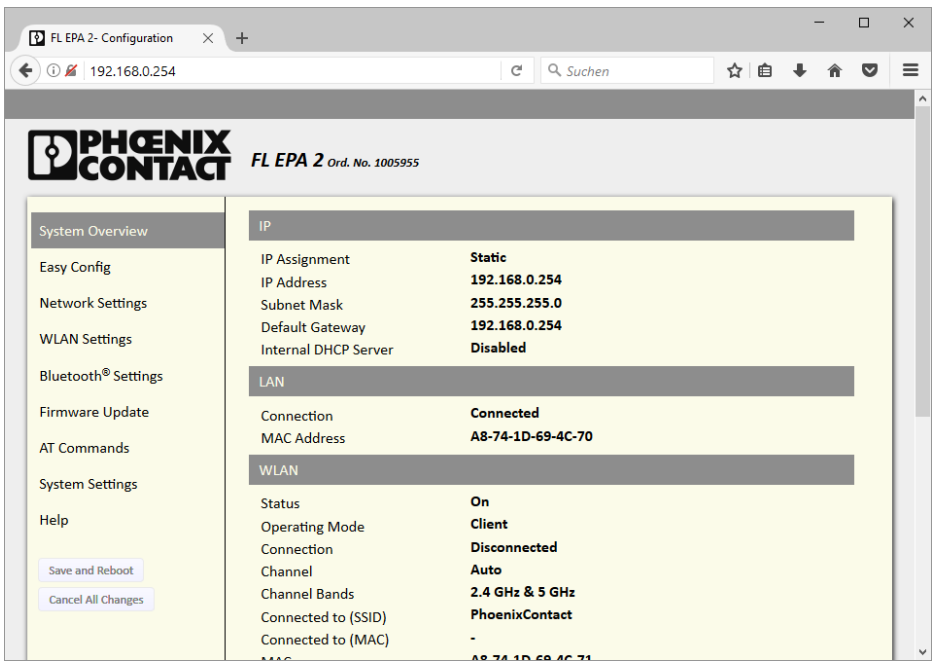


Figure 4-1 “System Overview” web page

All changes are activated using the “Safe and Reboot” button. The button will only be active if parameters have been changed. This also applies to changes made to the device on other web pages during this session. Selecting another menu item within the configuration pages does not discard the changes that have been made to the configuration. However, unsaved changes will be lost when closing the connection without pressing the “Safe and Reboot” button.

Using the “Cancel All Changes” button, all settings that have not yet been saved via “Safe and Reboot” will be discarded.

4.1.1 System overview

The “System Overview” page provides an overview of the current settings and connections.

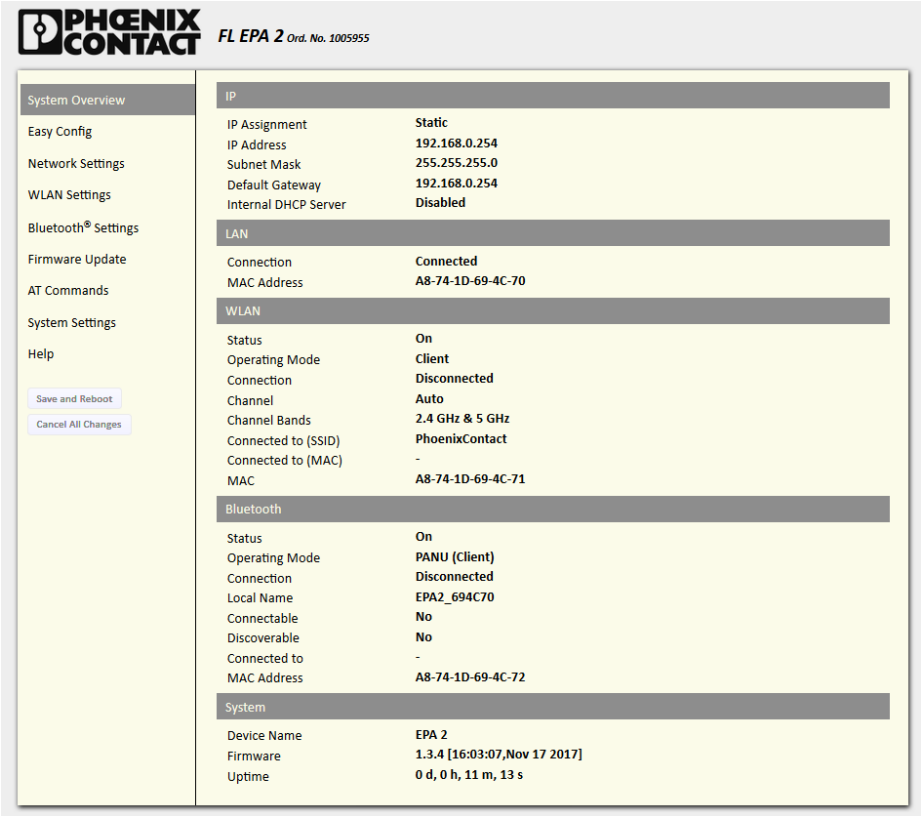


Figure 4-2 “System Overview” web page

4.1.2 Easy Config

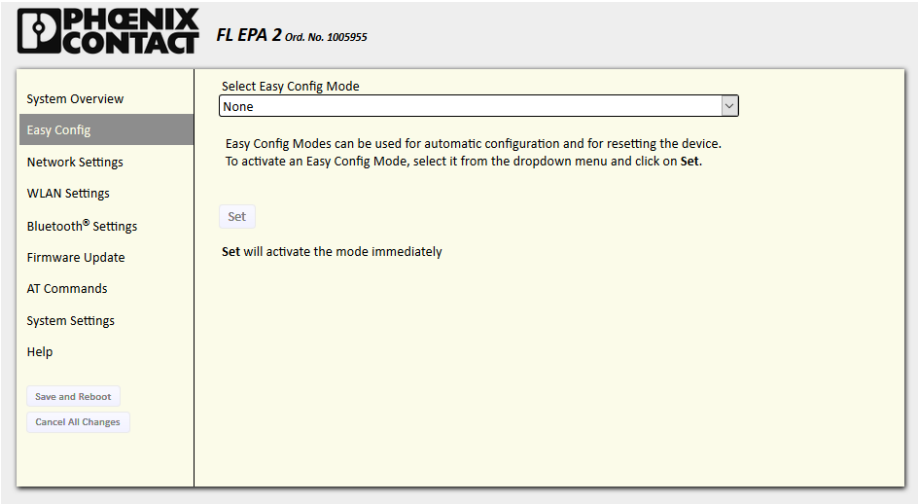


Figure 4-3 “Easy Config” web page

To activate an Easy Config mode, select it from the dropdown menu and click on “Set”.

For additional information, please refer to 3.1.2 on page 3-2.

4.1.3 Network settings

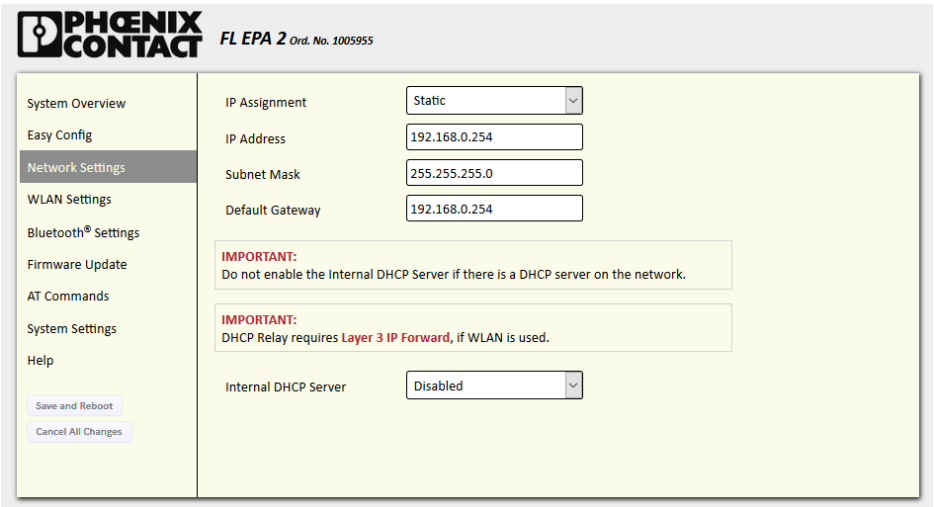


Figure 4-4 “Network Settings” web page

IP Assignment - Select whether the wireless module should use a static IP address or be assigned an IP address from an existing DHCP server.

IP Address - Static IP address field

Subnet Mask - Subnet mask when using a static IP address

Default Gateway - Default gateway when using a static IP address

Internal DHCP Server

Disabled: No internal DHCP functionality

DHCP Relay Enabled: DHCP requests from connected devices are forwarded using the DHCP relay protocol.

DHCP requests from connected devices are forwarded in both settings “Disabled” and “DHCP Relay”. Make sure that the selected protocol is supported by the DHCP server on the network. Select “Disabled” if in doubt. The behavior is then similar to that of a direct network connection.

DHCP Server Enabled: Activates the internal DHCP server. This option is only available if “IP Assignment” is set to “Static”.

The internal DHCP server will assign up to seven consecutive IP addresses, starting with the start address specified. If the device itself is located within the DCHP range, its IP address will be skipped and the next IP address will be assigned instead.

Do not enable this option if there is already a DHCP server on the network!

If the static IP address is changed, the browser is automatically redirected to the new address after clicking on “Save and Reboot”.

The automatic redirect function may not be supported by all browsers.

4.1.4 WLAN settings – Client mode

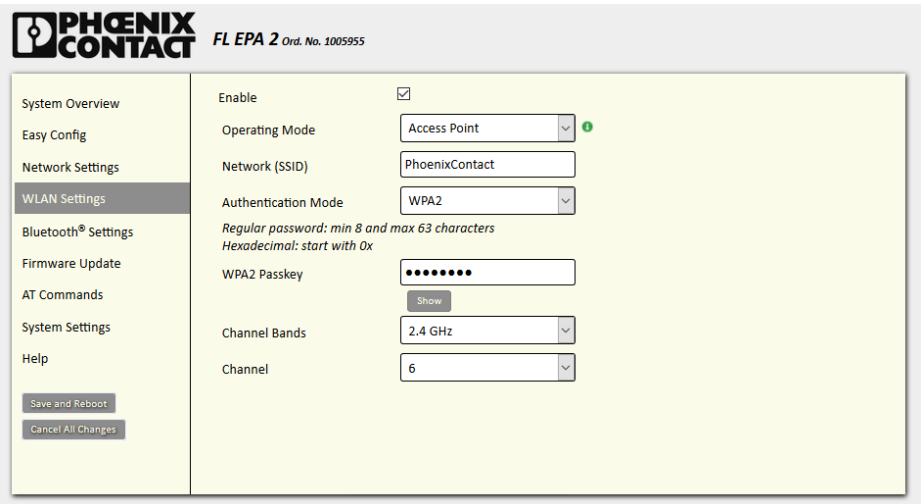


Figure 4-5 “WLAN Settings” web page

First select the operating mode (“Access Point” or “Client”). Depending on the selection, there are different input fields available.

Enable - Enable/disable the WLAN interface.

Operating Mode - Choose if the device should operate as a WLAN client or Access Point. Additional parameters will be visible, depending on the selection.

Channel Bands - “Client” mode only - Choose to scan for networks on either the 2.4 GHz or 5 GHz channel band, or on both (default).

Scan for Networks - Scans the selected frequency band for WLAN networks.
To connect to a network, select it from the dropdown menu after the scan has completed.

After pressing the button, all visible networks are shown in the “Select a network” dropdown menu, including the SSID, channel and received signal strength (RSSI).

Connect to SSID - To connect manually to a network, enter its SSID (network name) here. This can also be used if the network does not broadcast its SSID.

Authentication Mode - Select the authentication/encryption mode required by the network.

Open = No encryption (not recommended)

WPA2 = WPA2 PSK authentication with AES/CCMP encryption

Other authentication and encryption modes can be selected using AT commands.

WPA2 Passkey - Enter the WPA2 passkey for the network.

The WPA2 passkey must consist of 8 ... 63 characters from the following character set:

1234567890
abcdefghijklmnopqrstuvwxyzäöüß
ABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜ
!§$%&/()=?{[]}+*#'-_.:;@€<>|µ

The characters " (ASCII 34) and , (ASCII 44) and \ (ASCII 92) may not be used.

Channel - Select a specific channel to use when scanning for networks. Which channels are available depend on the “Channel Bands” setting.

Auto = All channels will be scanned (default).

4.1.4.1 Extended settings

Bridge mode (Client mode)

Layer 3 IP forward (default) -Several connected network devices support layer 3-transparent communication.

Several network devices can be connected behind the WLAN client. Communication can only be carried out on an IP basis. This mode is suitable for every WLAN-compliant Access Point.

Layer 2 tunnel - Connection with layer 2 transparency between two EPAs

This mode is suitable for all types of communication (e.g., PROFINET) and can also be used for several devices behind the wireless module. The performance is somewhat lower than in “Cloned MAC” mode. This mode can only be used between two EPA 2 modules.

Layer 2 cloned MAC only - Layer 2-transparent communication for one device

The device for which the MAC address needs to be entered supports layer 2-transparent communication (e.g., for PROFINET) with the network. This mode is suitable for every WLAN-compliant Access Point.

Cloned MAC Address - Enter the MAC address for “Layer 2 cloned MAC only” (see above).

4.1.5 WLAN settings - Access Point mode

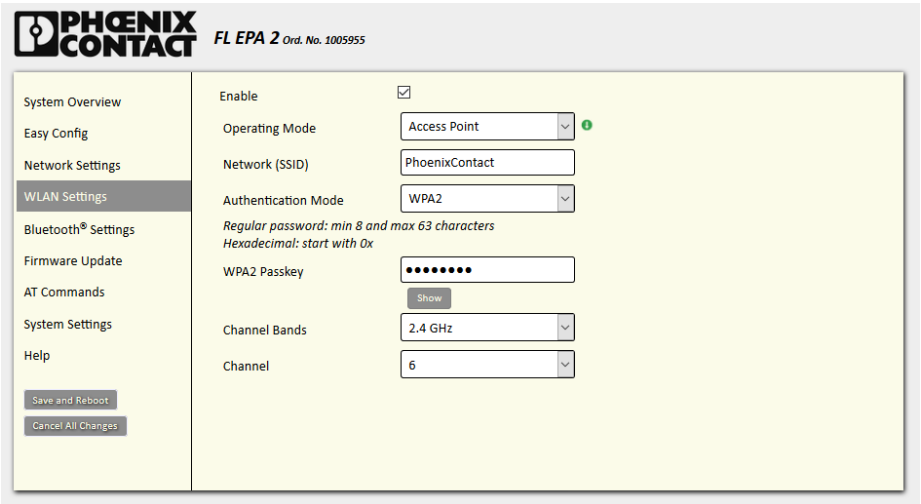


Figure 4-6 “WLAN Settings” web page

Settings for “Access Point” mode.

Network (SSID) - Enter an SSID (network name).

Authentication Mode - Select the authentication/encryption mode to use for the Access Point.

Open = No encryption (not recommended)

WPA2 = WPA2 PSK authentication with AES/CCMP encryption

Other authentication and encryption modes can be selected using AT commands.

WPA2 Passkey - Enter a string in plain text or hexadecimal format to use for authentication.

The WPA2 passkey must consist of 8 ... 63 characters from the following character set:

1234567890
abcdefghijklmnopqrstuvwxyzäöüß
ABCDEFGHIJKLMNOPQRSTUVWXYZÄÖÜ
!§$%&/()=?{[]}+*#'-_.:;@€<>|µ

The characters " (ASCII 34) and , (ASCII 44) and \ (ASCII 92) may not be used.

Make sure to use an individual and secure password.

Channel Bands, Channel

Select both a frequency band and channel for the Access Point (the client follows the Access Point settings).

4.1.6 Bluetooth settings - General

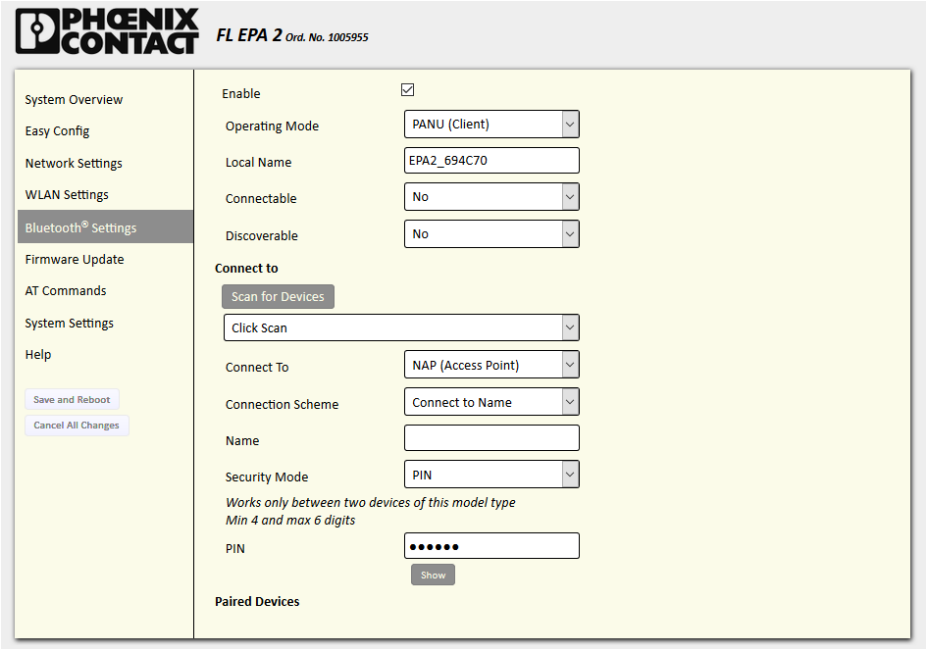


Figure 4-7 “Bluetooth Settings” web page

Enable - Enable/disable the Bluetooth interface.

Operating Mode - “PANU (Client)” = The device will operate as a Bluetooth PAN (Personal Area Network) User device. It can connect to another single Bluetooth PANU device or to a Bluetooth Network Access Point (NAP).

NAP (Access Point) = The device will operate as a Bluetooth Network Access Point. It can connect to up to seven Bluetooth PANU devices.

If several PANUs are used in conjunction with a single NAP, the available data throughput is divided between all PANUs.

Local Name - Identifies the device to other Bluetooth devices. If left blank, the device will use the default name including the last six characters of the MAC ID.

In “NAP” mode, the network (name) is entered here, to which PANUs may connect according to the “Connect to Name” connection scheme.

Connectable - Enable to make the device accept connection requests initiated by other Bluetooth devices.

Discoverable - Enable to make the device visible to scans of other Bluetooth devices.

Security Mode - Disabled = No encryption or authentication

PIN = Encrypted connection with PIN code protection. This mode only works between two devices of this type and manufacturer (not with third-party devices). PIN codes must consist of 4 ... 6 digits.

Just Works = Encrypted connection without PIN code

Paired Devices - Lists the Bluetooth devices connected to this device.

4.1.7 Bluetooth settings - Mode-specific

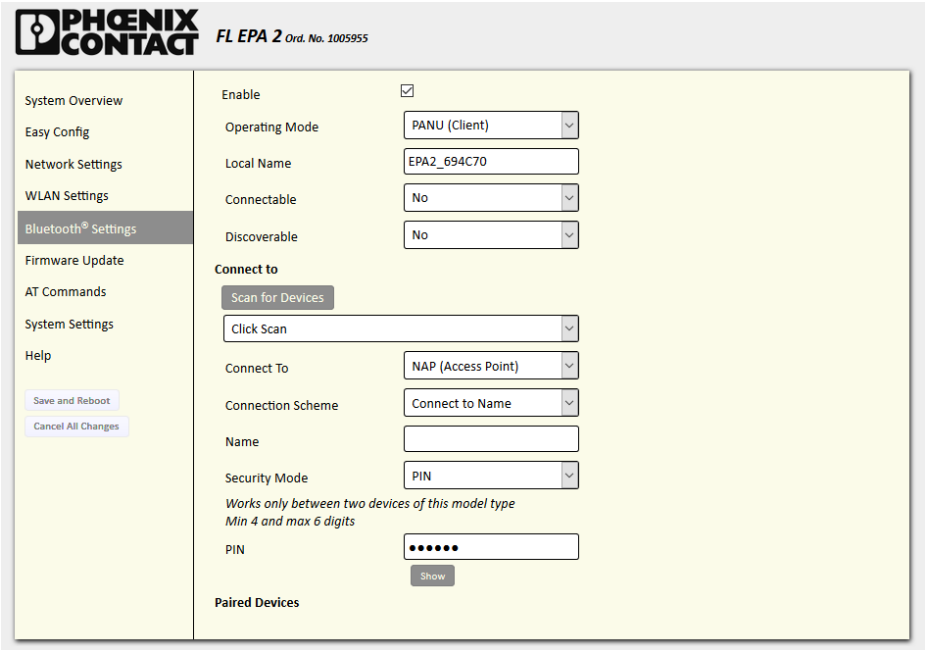


Figure 4-8 “Bluetooth Settings” web page

“PANU” mode only

Scan for Devices - Scans the environment for Bluetooth devices. To connect to a device, select it from the dropdown menu after scanning.

Connect To - Specifies if a NAP or PANU should be connected.

Connection Scheme - Choose whether to select a Bluetooth device by MAC address or name (“Local Name”) when connecting manually.

“NAP” mode only

List Nearby Devices - Lists Bluetooth devices discovered in the environment.

Connections can only be initiated in “PANU” mode.

4.1.7.1 Configuration examples

Connection in “Connect to MAC” mode

A Bluetooth connection based on MAC addresses is established quickly. In addition, devices do not need to be set to “Visible”, i.e., the Access Point (NAP) will respond to search requests from other Bluetooth devices.

When replacing a device, the configuration of other devices may need to be adapted.

Configuring the central device (“NAP”)

Assign a unique IP address on the “Network Settings” page.

Modify the following data on the “Bluetooth Settings” page:

- Operating Mode: NAP (Access Point)
- Connectable: Yes
- PIN: (unique key, 4 ... 6 digits, e.g., “123456”)
- Optional: Local Name (descriptive name for the radio cell)

Apply the settings with “Save and Reboot”.

Configuring the other devices

Assign a unique IP address on the “Network Settings” page.

Modify the following data on the “Bluetooth Settings” page:

- Connection Scheme: Connect to MAC
- PIN: Security key, identical to the NAP key
- Press the “Scan for Devices” button.

If the NAP is located in close proximity, the NAP address can be selected from the drop-down list after just a few seconds.

The MAC address of the Bluetooth module is two hex values higher than the MAC address printed on it.

Apply the settings with “Save and Reboot”.

Connection in “Connect to Name” mode

A connection based on the “Local Name” network name is established using the “Connect to Name” concept. This simplifies the replacement of devices, as the name, in contrast to the MAC address, can be configured freely. The name must be “Visible”, i.e., the device responds with its name during a Bluetooth scan.

Configuring the central device (“NAP”)

Assign a unique IP address on the “Network Settings” page.

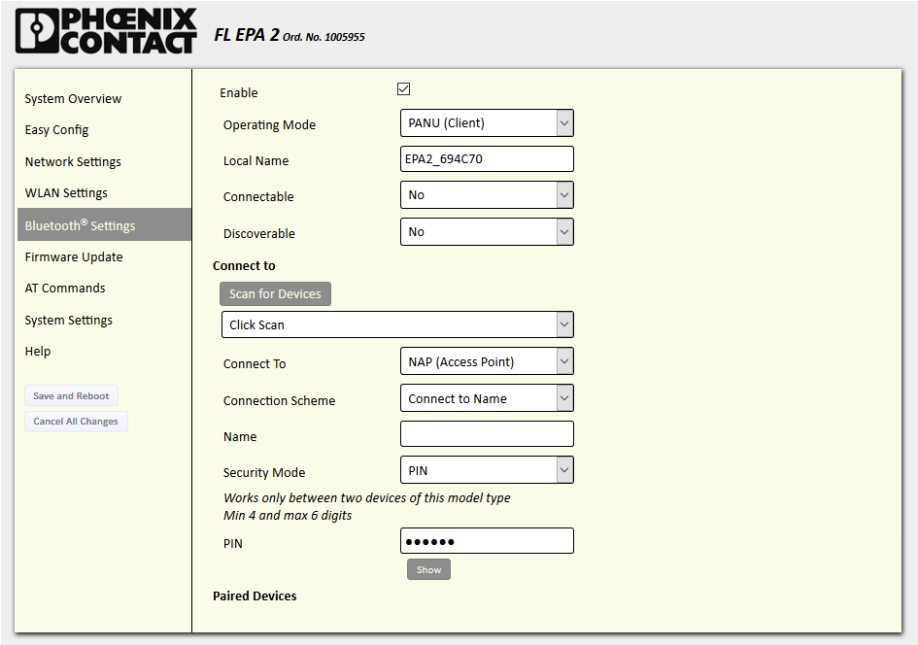


Figure 4-9 “Bluetooth Settings” web page

Modify the following data on the “Bluetooth Settings” page:

– Operating Mode: NAP (Access Point)
– Connectable: Yes
– Visible: Yes
– Local Name (descriptive name for the wireless cell)
– PIN: (unique key, 4 ... 6 digits, e.g., “123456”)

Apply the settings with “Save and Reboot”.

Configuring the client (“PANU”)

Assign a unique IP address on the “Network Settings” page.

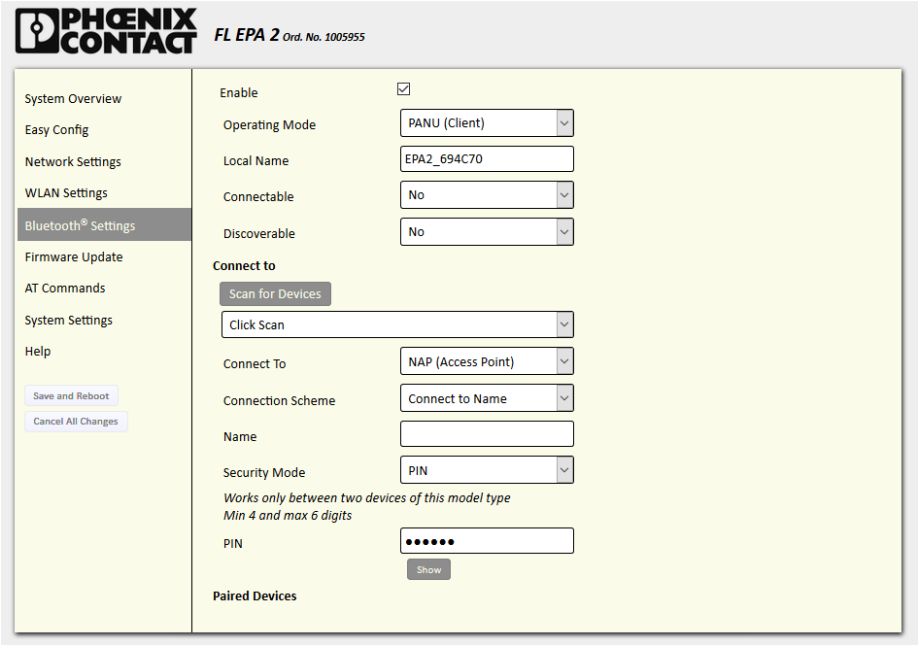


Figure 4-10 “Bluetooth Settings” web page

Modify the following data on the “Bluetooth Settings” page:

- Operating Mode: PANU (Client)
- Connect To: NAP (Access Point)
- Connection Scheme: “Connect to Name”
- Name: (“Local Name” of the NAP)
- Local Name (descriptive name for the wireless cell)
- PIN: (unique key, 4 to 6 digits, e.g., “123456”, identical to NAP)

Apply the settings with “Save and Reboot”.

After a few seconds, the client connects to the Access Point (NAP) if it is located in the radio range.

With this type of configuration, the NAP responds to any scanning device. Connection establishment is protected against unauthorized access using the PIN.

4.1.8 Firmware update

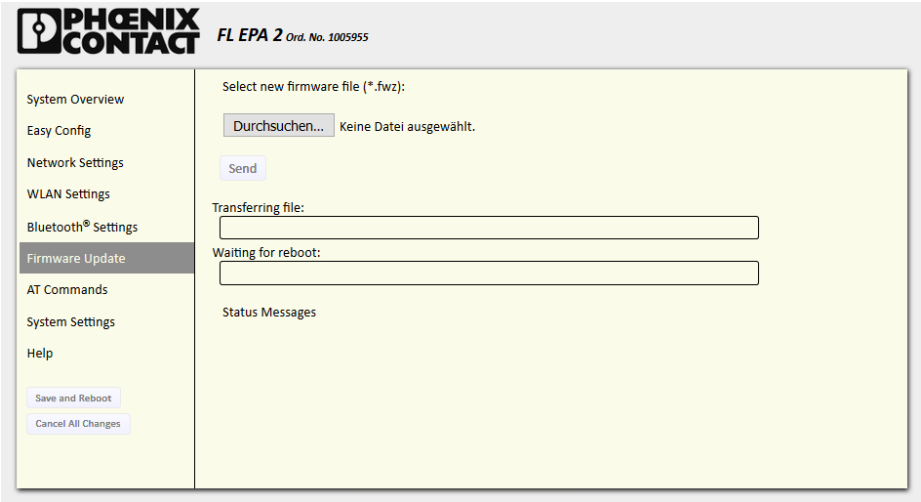


Figure 4-11 “Firmware Update” web page

Click on “Browse” to select a firmware file, then click on “Send” to download it to the device.

Both progress bars will turn green when the firmware update has been completed. Following firmware installation, the device restarts automatically.

4.1.9 AT commands

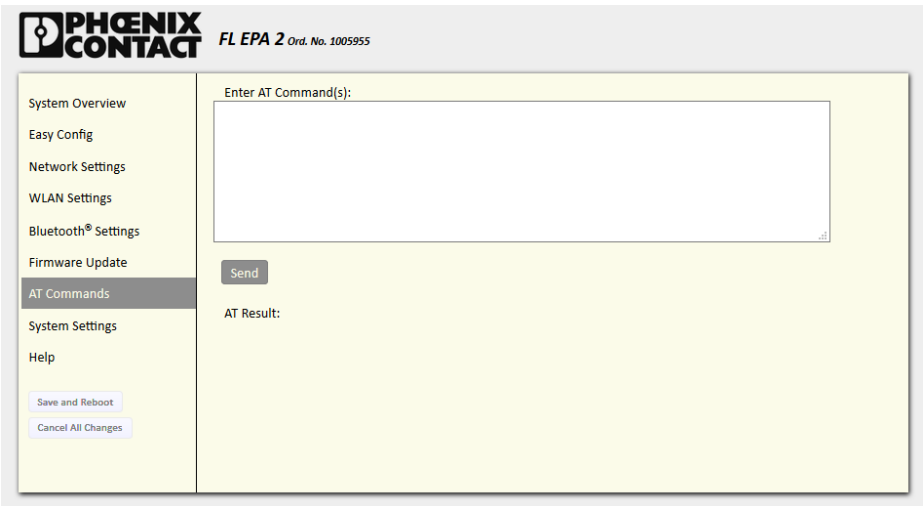


Figure 4-12 “AT Commands” web page

AT commands can be used for setting extended parameters that are not accessible via web-based management or to read out parameters in text format.

It is possible to simultaneously copy a set of commands into the input field.

Enter or paste the commands into the text field, then click on “Send”. The result codes will be displayed below the text field.

If a command cannot be processed (“Error”), it is also impossible to carry out subsequent commands.

The supported AT commands are described in the “Help” section of the web-based management and the Reference Manual for AT commands.

4.1.10 System settings

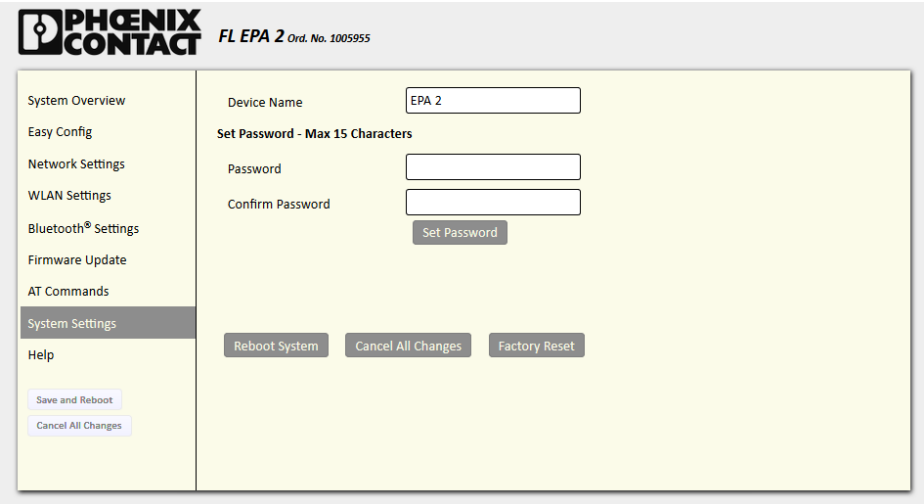


Figure 4-13 “System Settings” web page

Device Name - Enter a descriptive name for the device.

Password - Enter a password for accessing the web-based management.

Reboot System - Reboots the system without applying changes.

Cancel All Changes - Restores all parameters in the web-based management to the currently active values.

Factory Reset - Resets the device to the factory default settings and reboots.

Setting a secure password for the device is strongly recommended.

4.2 Restoring the factory defaults

The device can be restored to the factory default settings using any of the following methods:

- Press and hold the “MODE” button for >10 seconds and then release it.
- Execute Easy Config Mode 2.
- Click on “Factory Reset” on the “System Settings” page.

- Issue the “AT&F” command and reboot.

Table 4-1 Default settings (default upon delivery)

Network Settings	
IP Assignment	Static
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.254
WLAN Settings	
Operating Mode	Client
Channel Bands	2.4 GHz and 5 GHz
Authentication Mode	Open
Channel	Auto
Client Operating Mode	Layer 2 tunnel
Bluetooth Settings	
Operating Mode	PANU (Client)
Local Name	Generated from MAC address
Security Mode	Disabled
System Settings	
Password	-

Setting a secure password for the device is strongly recommended.

4.3 PROFINET communication

WLAN communication with PROFINET devices requires that “Bridge Mode” is set to “Layer 2 tunnel” on the “WLAN Settings” page using web-based management.

For WLAN and Bluetooth communication with PROFINET devices, it is recommended to enable the PROFINET optimizations. This can either be done using the EasyConfig mode or manually using an AT command.

Other real-time protocols

Profinet optimizations are also sensible when using other protocols with real-time requirements. Due to the large number of protocols, a general recommendation cannot be given here. To this end, it may be necessary to perform a test.

Bluetooth optimizations

The performance of a Bluetooth Access Point (NAP) can be improved by specifying the number of clients (PANU).

ATS2010=n (n=1…7, number of devices)

Execute the command on the “AT Commands” page using web-based management.

Safety-related communication (PROFISafe/SafetyBridge)

The PROFIBUS user organization has specified PROFIsafe for wireless transmission paths. Positive concept assessments have also been obtained from the BGIA (Professional Institute for Safety at Work) and TÜV (German Technical Inspectorate). Version 2.4 of the PROFIsafe profile describes the marginal conditions for the functionally safe transmission of data via WLAN and Bluetooth. In particular, security aspects for the configuration of wireless components and for safeguarding cyclic data exchange are specified.

Safety assessment regarding the safety-related communication also includes the protection against accidental or unauthorized changes to the configuration. Using the AT-command AT*AMPSM=1,1,1
all configuration interfaces (web-based management, AT command interface) are disabled.

Execute the command on the “AT Commands” page using the web-based management.

The command takes effect immediately. After that, it is no longer possible to modify other settings. Then the only way to access the device is by performing a factory reset via the “MODE” button (“B” mode).

Your therefore need to make sure that all necessary settings are made before disabling the interfaces.

Typical values for the monitoring time: >= 250 ms

To ensure a stable latency, the data load for a wireless path must never be higher than the transmission capacity of the wireless side. Problems rarely occur from the actual user data but sometimes from multicast or broadcast data. In time-critical applications we highly recommend to optimize data traffic using properly configured Managed Switches.

5 Technical data

Dimensions

Width	67.8 mm
Height	92.7 mm
Depth	33.2 mm
Note on dimensions	Without M12 connections

Ambient conditions

Ambient temperature (operation)	-40°C ... 65°C
Ambient temperature (storage/transport)	-40°C ... 85°C

Ambient conditions

Permissible humidity (operation)	Non-condensing
Permissible humidity (storage/transport)	Non-condensing
Degree of protection	IP65

Ethernet interface

Interface	Ethernet
Number	1
Connection method	M12 connector (D-coded, female)
Interface	Ethernet 10/100 Mbps
Number of interfaces	1
Connection method	M12 connector (D-coded, female)
Note on the connection method	Auto negotiation and auto crossing
Transmission speed	10/100 Mbps
Physical transmission method	Copper
Transmission length	100 m (per segment)

Wireless interface

Designation	Bluetooth
Wireless standard	Bluetooth 2.1 + EDR
Antenna connection method	(Internal)
Transmission power	10 dBm, maximum
Number of wireless interfaces	1 Bluetooth 2.1 + EDR
Wireless modules that can be connected	1
Supported profiles	PANU (NAP, PAN)

Wireless card

Number	1
Assembly instruction	Built-in

Antenna

Assembly instruction	Internal antenna
Number	1

Supply of the module electronics

Connection method	M12 connector (A-coded, male)
Supply voltage	24 V DC
Supply voltage range	9 V DC ... 30 V DC
Supply current	36 mA, typical (at 24 V DC)
Current consumption	190 mA, maximum (at 9 V DC)

Functions

Configuration	Web interface, MODE button, AT commands (TCP/IP), SSC
Security	PIN
	Non-discoverable

General

Mounting type	Wall mounting
Net weight	105 g
Wireless licenses	Belgium
	Bulgaria
	Denmark
	Germany
	Estonia
	Finland
	France
	Greece
	Great Britain
	Ireland
	Iceland
	Italy
	Canada
	Latvia
	Liechtenstein
	Lithuania
	Luxembourg
	Malta

	Netherlands
	Norway
	Austria
	Poland
	Portugal
	Romania
	Sweden
	Switzerland
	Slovakia
	Slovenia
	Spain
	Czech Republic
	Hungary
	USA
	Cyprus (Republic)

Standards and regulations

Mechanical tests	Shock according to EN 60068-2-27/IEC 60068-2-27, 3g, 11 ms, Half-sine shock pulse, vibration resistance according to EN 60068-2-6/IEC 60068-2-6

Classifications

eCl@ss

eCl@ss 4.0	27240409
eCl@ss 4.1	27240409
eCl@ss 5.0	27242215
eCl@ss 5.1	27250501
eCl@ss 6.0	27242208
eCl@ss 7.0	27242208
eCl@ss 8.0	19170101
eCl@ss 9.0	19170101

ETIM

ETIM 2.0	EC001423
ETIM 3.0	EC001423
ETIM 4.0	EC000515
ETIM 5.0	EC000515
ETIM 6.0	EC000515

UNSPSC

UNSPSC 6.01	20142601
UNSPSC 7.0901	20142601
UNSPSC 11	20142601
UNSPSC 12.01	20142601
UNSPSC 13.2	43201404

Accessories

Data cable assembled

Bus system cable - SAC-4P-M12MSD/ 2,0-931 - 1569391

Bus system cable, Ethernet CAT5 (100 Mbps), 4-pos., PUR halogen-free, RAL 5021 (water blue), shielded, straight M12 connector (D-coded) to free cable end, cable length: 2 m

Bus system cable - SAC-4P-M12MSD/ 5,0-931 - 1569401

Bus system cable, Ethernet CAT5 (100 Mbps), 4-pos., PUR halogen-free, RAL 5021 (water blue), shielded, straight M12 connector (D-coded) to free cable end, cable length: 5 m

Network cable - NBC-MSD/ 1,0-93E/R4AC SCO - 1407360

Network cable, Ethernet CAT5 (100 Mbps), 4-pos., PUR, RAL 5021 (water blue), shielded, straight M12 connector

SPEEDCON/IP67, D-coding, to straight RJ45/IP20 connector, cable length: 1 m

Network cable - NBC-MSD/ 2,0-93E/R4AC SCO - 1407361

Network cable, Ethernet CAT5 (100 Mbps), 4-pos., PUR, RAL 5021 (water blue), shielded, straight M12 connector

SPEEDCON/IP67, D-coding, to straight RJ45/IP20 connector, cable length: 2 m

Network cable - NBC-MSD/ 5,0-93E/R4AC SCO - 1407362

Network cable, Ethernet CAT5 (100 Mbps), 4-pos., PUR, RAL 5021 (water blue), shielded, straight M12 connector

SPEEDCON/IP67, D-coding, to RJ45/IP20 connector, cable length: 5 m

Data connector

RJ45 connector, degree of protection: IP20, number of positions: 8, 1 Gbps, CAT5 (IEC 11801:2002), material: PA, connection method: IDC

fast connection, connection cross section: 26- 23 AWG, cable outlet: straight, color: RAL 7042 (traffic gray A)

ter

Assembly adapter - FL EPA WMS - 2701134

Set for mounting devices with EPA design to wall or mast, including mast clips for a diameter of 25 mm ... 85 mm, can be moved on two axes for optimum alignment, stainless steel

cable

Sensor/actuator cable - SAC-4P- 2,0-PUR/M12FS - 1533576

Sensor/actuator cable, 4-pos., PUR halogen-free, RAL 7021 (black-gray), free cable end, to straight socket

M12, A-coded, cable length: 2 m

Sensor/actuator cable - SAC-4P- 3,0-PUR/M12FS - 1668111

Sensor/actuator cable, 4-pos., PUR halogen-free, RAL 7021 (black-gray), free cable end, to straight socket

M12, A-coded, cable length: 3 m

Sensor/actuator cable - SAC-4P- 5,0-PUR/M12FS - 1668124

Sensor/actuator cable, 4-pos., PUR halogen-free, RAL 7021 (black-gray), free cable end, to straight socket

M12, A-coded, cable length: 5 m

Sensor/actuator cable - SAC-4P- 10,0-PUR/M12FS - 1683002

Sensor/actuator cable, 4-pos., PUR halogen-free, RAL 7021 (black-gray), free cable end, to straight socket

M12, A-coded, cable length: 10 m

DIN rail adapter - FL EPA RMS - 2701133

Set for mounting devices with EPA design on a DIN rail

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

+49 5235 300

+49 5235 341200

phoenixcontact.com

Worldwide locations:
phoenixcontact.com/salesnetwork

HOTLINE:

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

+49 5281 9462888