TECHDOCS

Manual

758-919

Wireless Access Point

Version 1.0.0

WAGO Kontakttechnik GmbH & Co. KG

Hansastraße 27
D-32423 Minden

Phone: +49 (0) 571/8 87 – 0
Fax: +49 (0) 571/8 87 – 1 69

E-Mail: info@wago.com

Web: www.wago.com

Technical Support

Phone: +49 (0) 571/8 87 – 4 45 55
Fax: +49 (0) 571/8 87 – 84 45 55

E-Mail: support@wago.com

Every conceivable measure has been taken to ensure the accuracy and completeness of this documentation. However, as errors can never be fully excluded, we always appreciate any information or suggestions for improving the documentation.

E-Mail: documentation@wago.com

We wish to point out that the software and hardware terms as well as the trademarks of companies used and/or mentioned in the present manual are generally protected by trademark or patent.

WAGO is a registered trademark of WAGO Verwaltungsgesellschaft mbH.

Table of Contents

1 Notes about this Documentation

Note

Always retain this documentation!
This documentation is part of the product. Therefore, retain the documentation during the entire service life of the product. Pass on the documentation to any subsequent user. In addition, ensure that any supplement to this documentation is included, if necessary.

This documentation applies to the Wireless Access Point 758-919

1.1 Copyright

1.2 Symbols

⚠ DANGER

Personal Injury!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

⚠ DANGER

Personal Injury Caused by Electric Current!
Indicates a high-risk, imminently hazardous situation which, if not avoided, will result in death or serious injury.

⚠ WARNING

Personal Injury!
Indicates a moderate-risk, potentially hazardous situation which, if not avoided, could result in death or serious injury.

⚠ CAUTION

Personal Injury!
Indicates a low-risk, potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

NOTICE

Damage to Property!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

NOTICE

Damage to Property Caused by Electrostatic Discharge (ESD)!
Indicates a potentially hazardous situation which, if not avoided, may result in damage to property.

Note

Important Note!
Indicates a potential malfunction which, if not avoided, however, will not result in damage to property.

Information

Additional Information:
Refers to additional information which is not an integral part of this documentation (e.g., the Internet).

1.3 Number Notation

Table 1: Number Notation

Number Code	Example	Note
Decimal	100	Normal notation
Hexadecimal	0x64	C notation
Binary	'100' '0110.0100'	In quotation marks, nibble separated with dots (.)

1.4 Font Conventions

Table 2: Font Conventions

Font Type	Indicates
italic	Names of paths and data files are marked in italic-type. e.g.: *C:\Program Files\WAGO Software*
Menu	Menu items are marked in bold letters. e.g.: **Save**
>	A greater-than sign between two names means the selection of a menu item from a menu. e.g.: **File** > **New**
Input	Designation of input or optional fields are marked in bold letters, e.g.: **Start of measurement range**
“Value”	Input or selective values are marked in inverted commas. e.g.: Enter the value “4 mA” under **Start of measurement range**.
[Button]	Pushbuttons in dialog boxes are marked with bold letters in square brackets. e.g.: **[Input]**
[Key]	Keys are marked with bold letters in square brackets. e.g.: **[F5]**

2 Important Notes

This section includes an overall summary of the most important safety requirements and notes that are mentioned in each individual section. To protect your health and prevent damage to devices as well, it is imperative to read and carefully follow the safety guidelines.

2.1 Legal Bases

2.1.1 Subject to Changes

WAGO Kontakttechnik GmbH & Co. KG reserves the right to provide for any alterations or modifications. WAGO Kontakttechnik GmbH & Co. KG owns all rights arising from the granting of patents or from the legal protection of utility patents. Third-party products are always mentioned without any reference to patent rights. Thus, the existence of such rights cannot be excluded.

2.1.2 Personnel Qualification

All sequences implemented on the device may only be carried out by electrical specialists with sufficient knowledge in installation and handling of electrical equipment. The electrical specialists must also be familiar with the current standards and guidelines valid for the device.

2.1.3 Intended Use

The intended use of this equipment is as a communication interface and gateway. The equipment receives and transmits data on various physical levels and connection types.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

2.1.4 Technical Condition of Specified Devices

The devices to be supplied ex works are equipped with hardware and software configurations, which meet the individual application requirements. These modules contain no parts that can be serviced or repaired by the user. The following actions will result in the exclusion of liability on the part of WAGO Kontakttechnik GmbH & Co. KG:

- Repairs,
- Changes to the hardware or software that are not described in the operating instructions,
- Improper use of the components.

Further details are given in the contractual agreements. Please send your request for modified and new hardware or software configurations directly to WAGO Kontakttechnik GmbH & Co. KG.

2.2 Special Use Conditions for ETHERNET Devices

If not otherwise specified, ETHERNET devices are intended for use on local networks. Please note the following when using ETHERNET devices in your system:

- Do not connect control components and control networks directly to an open network such as the Internet or an office network. WAGO recommends putting control components and control networks behind a firewall.
- In the control components close all ports and services not required by your application to minimize the risk of cyber attacks and to enhance cyber security.
  Only open ports and services during commissioning and/or configuration.
- Limit physical and electronic access to all automation components to authorized personnel only.
- Change the default passwords before first use! This will reduce the risk of unauthorized access to your system.
- Regularly change the passwords used! This will reduce the risk of unauthorized access to your system.
- If remote access to control components and control networks is required, use a Virtual Private Network (VPN).
- Regularly perform threat analyses. You can check whether the measures taken meet your security requirements.
- Use “defense-in-depth” mechanisms in your system's security configuration to restrict the access to and control of individual products and networks.

2.3 Storage, Assembly and Transport

Whenever possible, the components are to be stored in their original packaging. Likewise, the original packaging provides optimal protection during transport.

When assembling or repacking the components, the contacts must not be soiled or damaged. The components must be stored and transported in appropriate containers/packaging. Thereby, the ESD information is to be regarded.

2.4 Safety Advice (Precautions)

For installing and operating purposes of the relevant device to your system the following safety precautions shall be observed:

⚠ DANGER

Always use voltage sources with current limitation/safety extra-low voltage!
Only use power supply sources based on IEC/EN60950 Section 2.5 “Power sources with limited output” with the device. The output of the external power supply must be short-circuit protected. The output voltage of the external power supply shall not exceed 36 VDC.

⚠ WARNING

Do not use device in hazardous environments!
The device is only restricted for use in hazardous areas.

⚠ WARNING

Maintenance/Repair only by authorized specialists!
The device contains no parts that can be serviced by users. Always have all service, reconfiguration, maintenance or repair work performed by specialists authorized by WAGO.

⚠ DANGER

Do not work on components while energized!
All power sources to the device shall be switched off prior to performing any installation, repair or maintenance work.

⚠ CAUTION

Keep a distance of 20 cm to persons!
Install the device such that it is located at least 20 cm away from all persons during operation.

⚠ CAUTION

Radio frequency energy emission
This equipment emits 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.

NOTICE

Replace defective or damaged devices!
Replace defective or damaged device (e.g., in the event of deformed contacts), since the long-term functionality of fieldbus station involved can no longer be ensured.

NOTICE

Protect the components against materials having seeping and insulating properties!
The components are not resistant to materials having seeping and insulating properties such as: aerosols, silicones and triglycerides (found in some hand creams). If you cannot exclude that such materials will appear in the component environment, then install the components in an enclosure being resistant to the above-mentioned materials. Clean tools and materials are imperative for handling devices/modules.

NOTICE

Cleaning only with permitted materials!
Clean soiled contacts using oil-free compressed air or with ethyl alcohol and leather cloths.

NOTICE

Avoid electrostatic discharge!
The devices are equipped with electronic components that you may destroy by electrostatic discharge when you touch. Pay attention while handling the devices to good grounding of the environment (persons, job and packing).

Note

Functional earth
This product is recommended for use in both industrial and domestic environments. For industrial environments it is mandatory to use the functional earth connection to comply with immunity requirements. For domestic environments the functional earth must be omitted if a shielded Ethernet cable is used, in order to meet emission requirements.

Note

Device uses radio waves!
Never use the device in areas where operation of radio equipment is prohibited.

Note

Do not open the enclosure!
Never open the enclosure. Opening of the enclosure will nullify the guarantee, legal warranty and authorization for use.

⚠ WARNING

EXPLOSION HAZARD!
Substitution of any components may impair suitability for the explosive environment. When in hazardous locations, turn off power before replacing or wiring modules.

Do not disconnect equipment while the circuit is live or unless the area is known to be free of ignitable concentrations. Install in an enclosure considered representative of the intended use. To comply with directives, the equipment must be mounted in an IP54 enclosure.

⚠ WARNING

This device complies with Part 15 of the FCC Rules!
Operation is subject to the following 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!

3 Device Description

3.1 General Description

As a Wireless Access Point (WAP), the device makes it possible to integrate conventional ETHERNET devices in a wireless network. For this purpose, the device has a wired ETHERNET interface and another interface for radio communication. The device uses the integrated radio technology to transmit the data received on the ETHERNET interface. Conversely, the device uses the ETHERNET interface to send data received on the radio interface. As data transmission of ETHERNET packets occurs with a transparent protocol on Layer 2 of the OSI reference model, this provides for easy integration of all Ethernet-based fieldbuses, such as MODBUS/TCP, EtherNet/IP or PROFINET.

In combination with another function-related device, e.g., another WAP or Access Point (AP) of the same radio technology, the WAP can serve as a wireless replacement for ETHERNET cables. The WAP permits particularly robust, real-time radio connections over long distances. A suitable configuration can also prevent any degradation to other radio networks.

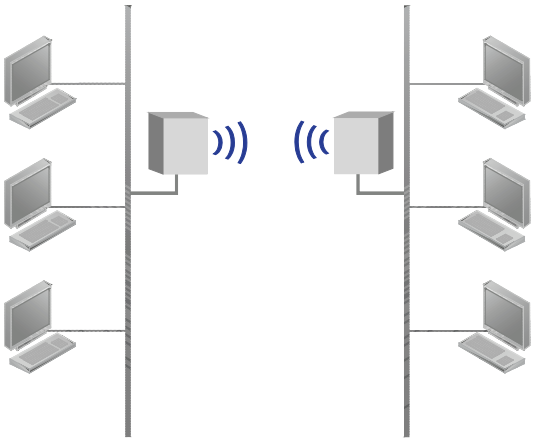

Figure 1: Wireless Transmission Between Two WAPs

An innovative operator control concept enables easy initiation of automatic configuration processes using a Mode membrane key on the device.
This can be used to configure a substitute cable link between two WAPs in only a few seconds, without using additional aids or hardware / software.

Status information and advanced device functions of the WAP can also be viewed and configured via a Web-based Management System (WBM).

Depending on the application, the unit can be operated in various modes.

Note

Restrictions

- The *Bluetooth*® PAN (Personal Area Network) may not work with your own devices. The reason is the different implementation of *Bluetooth*® by various manufacturers.
- 5 GHz WLAN cannot be used with 2.5 GHz WLAN or *Bluetooth*® at the same time.

Note

WLAN or *Bluetooth*®?

Choose WLAN if data throughput and wireless roaming are required or if there are only a few other devices transmitting in the area.

Choose *Bluetooth*® if stability and low latency are important and there are several other devices transmitting in the area.

3.2 View

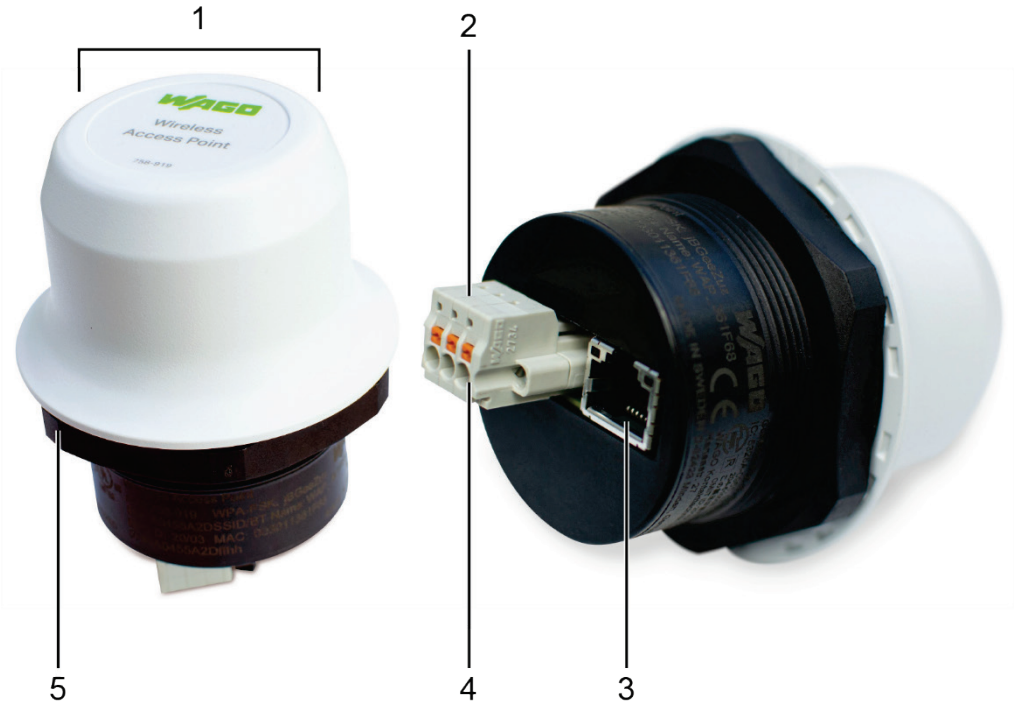

Figure 2: View

Table 3: Legend for Figure “View”

Pos.	Description	Details see Section
1	Antenna for WiFi and *Bluetooth*®	“Technical Data”
2	Power Connector (Art.-Nr. 2734-103/107-000)	-
3	ETHERNET Connector (RJ45, POE)	“Connectors”
4	RESET Button	“RESET Button”
5	Screw nut	“Technical Data”

3.3 Labeling

The device MAC address is included with other data on the device:

Figure 3: Marking – Type Plate Part 1 (Example)

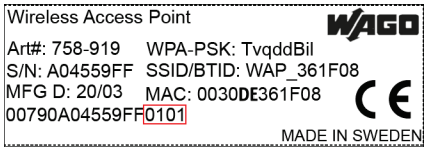

Figure 4: Marking – Type Plate Part 2 (Example)

Table 4: Legend for Figure “Label (Example)

No.	„Serial NO“ Description
01	Firmware version (left number sequence)
01	Hardware version (right number sequence)

3.4 Connectors

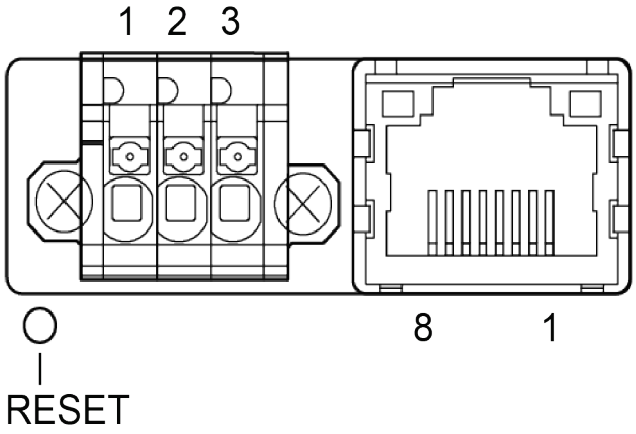

Figure 5: Connectors

NOTICE

Make sure that the power supply is connected correctly!
Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is connected correctly and of the recommended type!

See also Chapter „Technical Data“, regarding power supply requirements

Table 5: Power Connector (3-pin terminal block)

Pin	Function	
1	+	19 … 36 VDC
2	-	
3	Functional Earth (FE)	

Table 6: Ethernet Connector (RJ45 PoE)

Pin	Data	PoE	
1	TD+	A+	Positive power from alt. A PSE
2	TD-	A+	
3	RD+	A-	Negative power from alt. A PSE (with pin 6)
4		B+	Positive power from alt. B PSE
5		B+	
6	RD-	A-	Negative power from alt. A PSE (with pin 3)
7		B-	Negative power from alt. B PSE
8		B-	
Housing	Shield	Functional Earth (FE) via 1 nF capacitor and 1 MΩ bleeder resistor	

Shielded or unshielded Ethernet cables may be used.

3.5 RJ45 LED Indicators

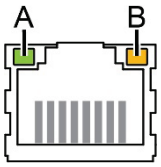

Figure 6: RJ45 LED indicators

Table 7: LED A – LINK/ACTIVITY

LED A – LINK/ACTIVITY	Function
Off	No Ethernet link or no power
Yellow	Ethernet link established
Yellow, flashing	Ethernet traffic

Table 8: LED B – STATUS

LED B – STATUS	Function
Off	No power
Blue	Connected on all configured wireless interfaces
Purple	Trying to connect to WLAN/Bluetooth access point
Blue, slow blink	Awaiting connections
Alternating blue/purple	Connected on one interface and trying to connect or awaiting connections on another
Purple, slow blink	Awaiting connections on one interface and trying to connect on another
Purple, fast blink	Scanning for Bluetooth devices or WLAN networks
Red, slow blink	No configured wireless interface
Red	Recoverable/unrecoverable fault

3.6 RESET Button

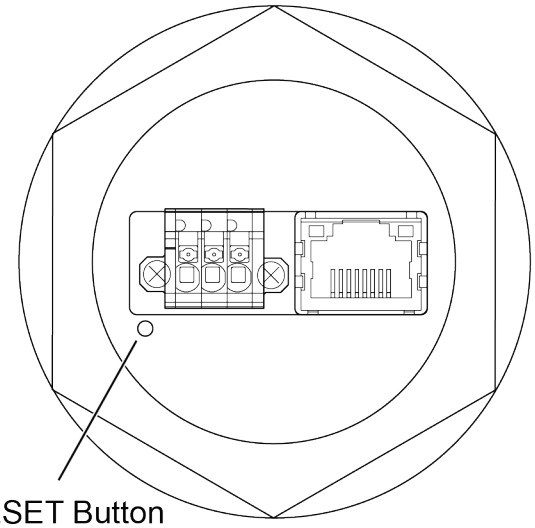

Figure 7: RESET Button

The RESET button is located on the bottom of the unit.

When the unit is powered on, press and hold RESET for > 10 seconds and then release it to reset to the factory default settings.

3.7 Technical Data

3.7.1 Hardware Specifications

Table 9: Hardware Specifications

Order Code	758-919
Color	White top and black base
Wired interface type	ETHERNET (RJ45 PoE)
ETHERNET connector	RJ45
Power connector	3-pole CAGE CLAMP® connector
Antenna	Internal dual-band 2.4 GHz and 5 GHz antenna
Maximum range	200 m (WLAN and Bluetooth©), see also section “Radio Antenna Patterns”
Operating temperature	- 40 … + 65 °C
Storage temperature	- 40 … + 85 °C
Humidity	EN 600068-2-78: Damp heat, + 40°C, 93% humidity for 4 days.
Dimensions	Height: 75 mm (91 mm with PS connector) Outside height: 41 mm Diameter: 68 mm
Weight	84 g
Protection class	Top (outside of host): IP66 / IP67 / UL NEMA 4X Base (inside of host): IP21
Mounting	M50 screw and nut (50.5 mm hole needed)
Power supply	19 … 36 VDC
Power over Ethernet	44 … 57 VDC DTE Type1 according to IEEE 802.3af
Power consumption	0.7 W idle, 1.7 W max.

3.7.2 Communication

Table 10: ETHERNET

Ethernet interface	10/100BASE-T with automatic MDI/MDIX auto cross-over detection.
Ethernet protocols	IP, TCP, UDP, HTTP, LLDP, ARP, DHCP Client/Server, DNS support. Transparent transfer of PROFINET IO, EtherNet/IP, Modbus-TCP or any other TCP/UDP based protocol.

Table 11: Wireless LAN

Wireless standards	IEEE 802.11 a, b, g, n, d, r
Operation modes	Access point or client
Fast roaming	IEEE 802.11r (client)
Max. number of clients for access point	7
WLAN channels	2.4 GHz Access Point: 1–11 2.4 GHz Client: 1–11 + 12 & 13 depending on regulatory domain scan 5 GHz Access Point: 36–48 (U-NII-1) 5 GHz Client: 36-48 + 100–116, 132–140, 120–128 depending on regulatory domain scan. (U- NII-1, U-NII-2, U-NII-2e)
RF output power	15 dBm EIRP
Power consumption	54 mA @ 24 VDC
Net data throughput	20 Mbps.
Link speed	Max 65 Mbps (802.11n SISO)
Security	WEP 64/128, WPA, WPA-PSK and WPA2, TKIP and AES/CCMP, LEAP, PEAP including MS-CHAP.

Table 12: Classic Bluetooth

Wireless standards (profiles)	PAN (PANU & NAP)
Operation modes	Access point or Client
Max. number of clients for Central	7
RF output power	11 dBm EIRP
Power consumption	36 mA @ 24 VDC
Net data throughput	~ 1 Mbps
Bluetooth version support	Classic Bluetooth v2.1
Security	Authentication & Authorization, Encryption & Data Protection, Privacy & Confidentiality, NIST Compliant, FIPS Approved.

Table 13: Bluetooth Low Energy

Wireless standards (profiles)	GATT
Operation modes	Central or Peripheral (pending)
Max. number of clients for Central	7
RF output power	7 dBm EIRP
Power consumption	36 mA @ 24 VDC
Net data throughput	~ 200 kbps
Bluetooth version support	Bluetooth 4.0 dual-mode
Security	AES-CCM cryptography

3.8 Approvals

The following approvals have been grated for the Wireless Access Point (758-919):

Conformity Marking

IC “Industry Canada” — IC: 5325A-0965, for indoor use only (5GHz)

FCC “Federal Communications Commission” / CFR 47 Part 15, ETS 300328 — FCC ID: PVH0965

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

UL E198726 for Use in Hazardous Locations
Cl I, Div 2, Group A, B, C, D, T4

204-510009.
この製品は屋内においてのみ使用可能です
CMIIT ID: 2016AJ1533

3.8.1 Radio Regulatory Compliance

FCC Compliance Statement

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

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. this device may not cause harmful interference, and
2. this device must accept any interference received, including interference that may cause undesired operation.

This product contains FCC ID: **PVH0965.**

NOTICE

Damage to Property!
Any changes or modifications not explicitly approved by WAGO Kontakttechnik GmbH & Co. KG could cause the module to cease to comply with FCC rules part 15, and thus void the user's authority to operate the equipment.

Industry Canada Statement

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

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 of the device.

This product contains IC ID: **5325A-0965.**

3.9 Selecting the Installation Location

In order to use all the functions of the device, a radio link must be established to a device having similar functions, for example a second device of the same type. If the two devices are relatively close to one another, that is, if the distance between them is considerably less than the potential range, the installation location and device alignment will have comparatively little impact on the radio link. If you wish to set up and maintain a radio link over the longest distance possible, however, certain requirements regarding the installation of the device and the ambient conditions must be fulfilled.

The distance between devices may not be too great. The maximum range can only be effective under optimal conditions. A lack of line-of-sight link, or mis-alignment of the devices will result in reduced range.

For a line-of-sight link, install the devices such that the antennas are aligned toward one another, i.e., the marked front side of the devices face one another.

If there is no line-of-sight link, but both devices have an unobstructed view of the same metallic or concrete surface (such as a building ceiling), a good radio link can be ensured through reflection.

If there is neither a line-of-sight link, nor a surface to use for reflection, for example between devices in different rooms, align the devices as for a line-of-sight link. The magnitude of the reduction in range for the devices in this case depends on the amount of material, e.g., brick walls, that the radio waves must pass through. In some circumstances, it may not be possible for the radio waves to penetrate certain obstacles, such as fire protection walls, at all.

Table 14: Selection of Installation Location

Ambient Conditions, Installation Location	Radio link possible?
Distance between devices is more than 400 m.	No
Line-of-sight link between devices that are about 200 m apart. Devices have been optimally installed and configured.	Yes
Two plaster or brick walls are located between the devices; distance between devices is around 30 m.	Yes. Links are also possible without line of sight, but the range is substantially reduced, depending on the obstacle (e.g., a wall).
A fire protection wall or a steel-reinforced concrete ceiling is located between the devices.	No. Reinforced concrete and other similar materials cannot be penetrated by radio waves when they are too thick.
The devices are located less than 50 m apart in a plant building, with the line of sight being obstructed by numerous machines or vehicles.	Possible. Building ceilings or other metallic or steel-reinforced large objects may permit an indirect link by reflecting the radio waves.

You can find more information in chapter “Radio Antenna Patterns”.

4 Installation

4.1 General Information

Make sure that you have all the necessary information about the capabilities and restrictions of your local network environment before installation.

The characteristics of the internal antenna should be considered when choosing the placement and orientation of the unit.

See also Chapter “Wireless Technology Basics”.

4.2 Limitations

Bluetooth PAN (Personal Area Network) may not work with some devices due to different implementations of Bluetooth by different manufacturers.

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

Note

Do not install antenna directly in front of metallic surfaces!
The front of the WAP, and hence the internal antenna, must not be located directly in front of metallic surfaces, as this can permanently degrade the radio capabilities of the antenna.

Note

Please note the installation conditions for hazardous location!
To comply with Hazardous Location directives, the device must be mounted in an IP54 enclosure. The antenna of the Wireless Access Point must be inside the housing.

4.3 Mechanical Installation

For optimal reception, wireless devices require a zone between them clear of objects that could otherwise obstruct or reflect the signal. A minimum distance of 50 cm between the devices should also be observed to avoid interference.

The device is intended to be mounted on top of a machine or cabinet through an M50 (50.5 mm) hole using the included sealing ring and nut.

The top mounting surface (in contact with the sealing) must be flat with a finish equivalent to Ra 3.2 or finer and cleaned and free from oils and greases.

Tightening torque: 5 Nm ±10 %

NOTICE

Make sure that the sealing ring is correctly placed!
Make sure that the sealing ring is correctly placed in the circular groove in the top part of the housing before tightening the nut.

NOTICE

Always hold the BOTTOM part of the unit when untightening the nut!
Always hold the BOTTOM part of the unit when untightening the nut, not the top part (the cap)!

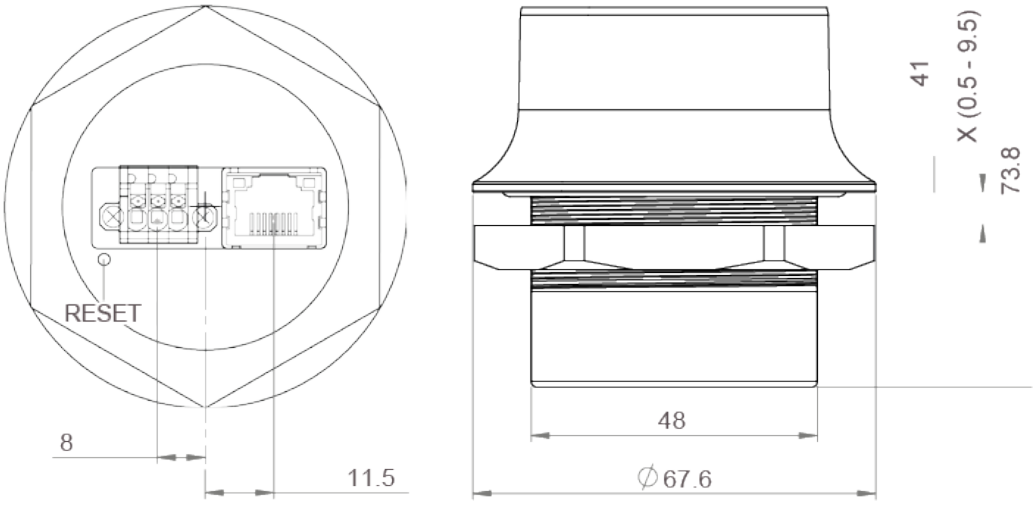

Figure 8: Installation drawing

All measurements are in mm.

5 Configuration

5.1 General

WAGO Wireless Access Point should normally be configured via the web interface. Parameters can be set individually or using one of the pre-configured Easy Config modes.

The web interface is accessed by pointing a web browser to the IP address of the Wireless Access Point. The default address is 192.168.0.99. The computer accessing the web interface must be in the same IP subnet as the Wireless Access Point.

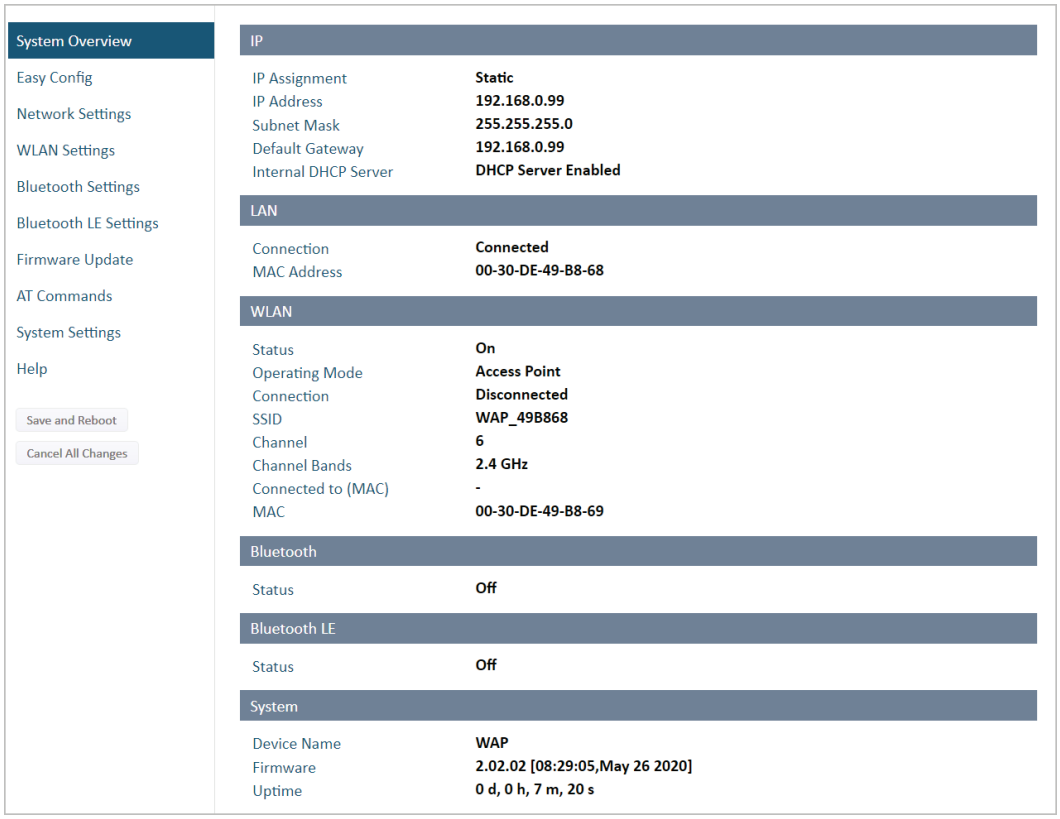

Figure 9: Web interface

The device is configured as a WiFi access point in factory default. The DHCP server is active and assigns IP addresses from 192.168.0.201 to 192.168.0.206 to WiFi clients.

Advanced configuration can be carried out by issuing AT (modem) commands through the web interface or over a Telnet or RAW TCP connection to port 8080. See the AT Commands or the Help page in the web interface for more information.

5.2 Web Interface

5.2.1 System Overview

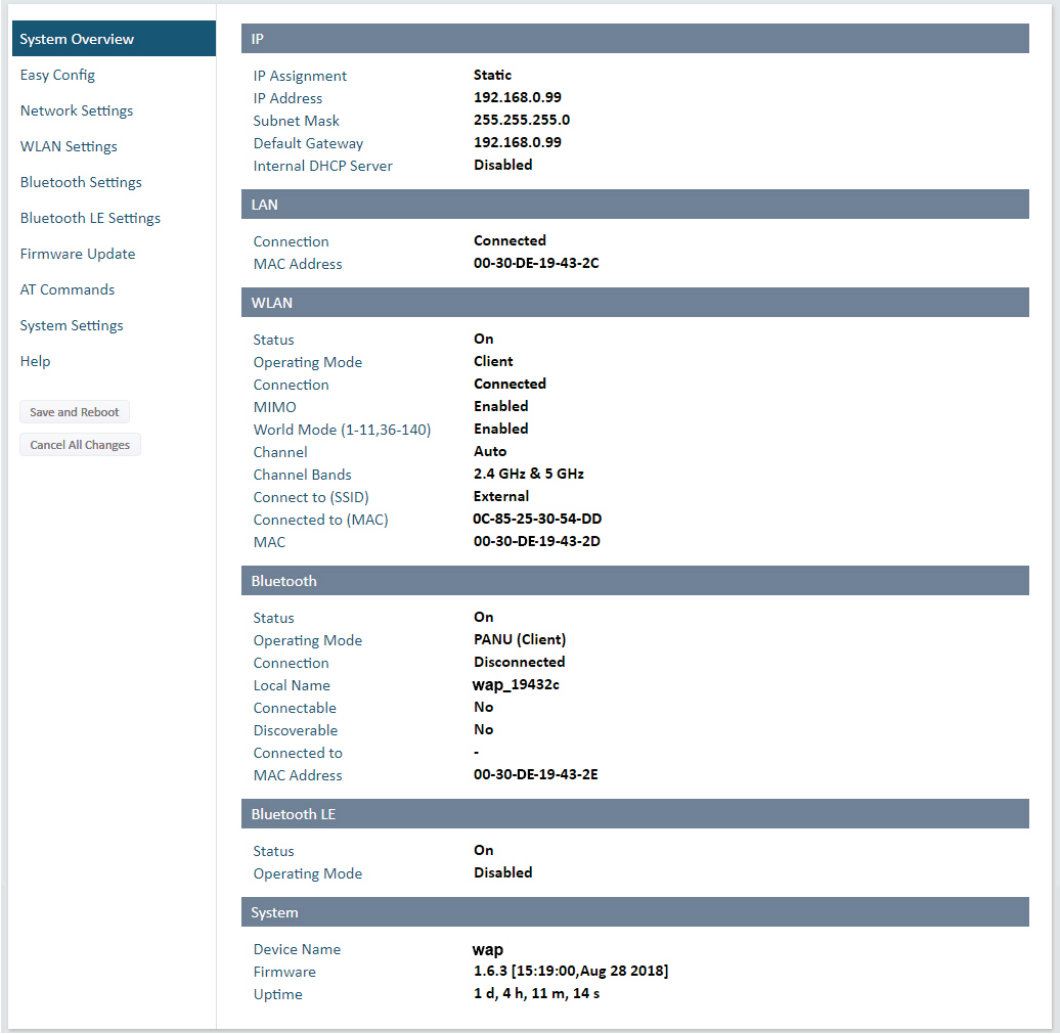

Figure 10: System Overview page

The **System Overview** page shows the current settings and connection status for the wired and wireless interfaces. The different parameters are explained in the descriptions of each settings page in this manual.

The **Help** page describes AT commands that can be used for advanced configuration.

Table 15: Buttons

Button	Description
[**Save and Reboot**]	This button will be enabled if the unit must be restarted to apply a change.
[**Cancel All Changes**]	Resets parameter changes that have not been applied.

5.2.2 Easy Config

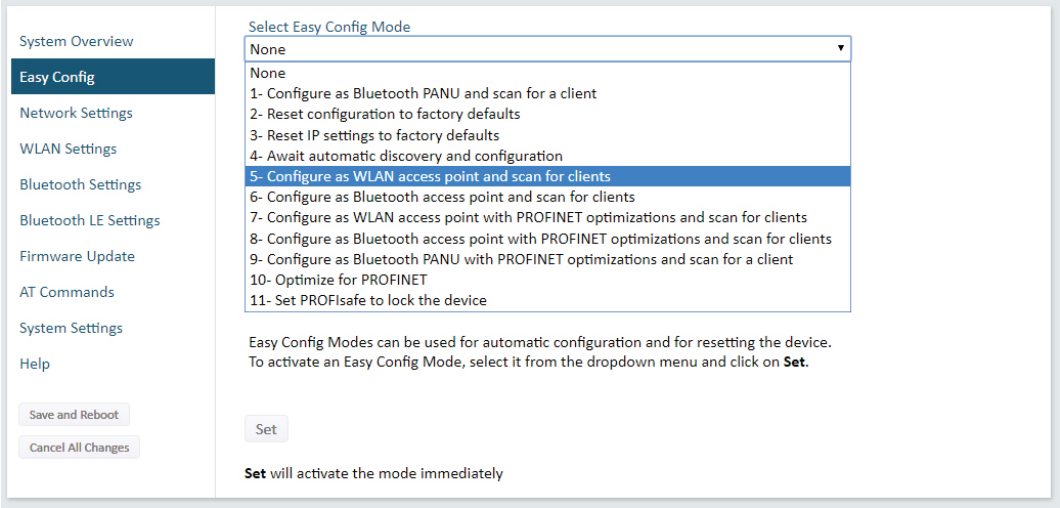

Figure 11: Easy Config page

To activate an Easy Config mode, select it from the dropdown menu and click on [**Set**]. The mode will be activated immediately.

Table 16: Easy Config Modes

EC	Role	Description
1	Bluetooth PANU	Configure as Bluetooth client and scan for another client (PANU–PANU).
2	-	Reset configuration to factory defaults.
3	-	Reset IP settings to factory defaults.
4	Client	Wait for automatic configuration. Configure units in mode 4 as clients.
5	WLAN AP	Configure units in mode 4 as clients. Restart as access point and connect clients.
6	Bluetooth NAP	
7	WLAN AP	Configure units in mode 4 as clients. Restart as access point and connect clients. Apply PROFINET optimization to all units.
8	Bluetooth NAP	
9	Bluetooth PANU	Configure as Bluetooth client and scan for another client (PANU–PANU). Apply PROFINET optimization to both units.
10	(any)	Apply PROFINET optimization and restart.
11	(any)	Enable PROFIsafe mode.

Notes:

- Mode 1 will scan for units in mode 4. When a unit in mode 4 is detected, the scanning unit will configure itself as a Bluetooth PANU client, send a connection configuration to the detected unit, and restart. The detected unit will also restart and attempt to connect to the first unit as a PANU client.
- Modes 5, 6, 7 and 8 will scan for units in mode 4. The detected units will be reconfigured as clients and the scanning unit will restart as an access point. The clients will then restart and connect to the access point.
- Modes 7 and 8 will additionally apply PROFINET optimization to all the units. PROFINET messages will then have priority over TCP/IP frames.

- Mode 11 locks the unit in PROFIsafe mode where the configuration cannot be changed without physical access. To cancel this mode the unit must be restored to factory defaults by pressing and holding the RESET button.
- Modes 10 and 11 will be added to the configuration without changing any other settings.
- Modes 1 and 9 will listen for 40 seconds or until a configuration is established.
- Modes 4 will listen for 120 seconds or until receiving a configuration.
- Modes 5, 6, 7 and 8 will time out after 120 seconds.

5.2.3 Network Settings

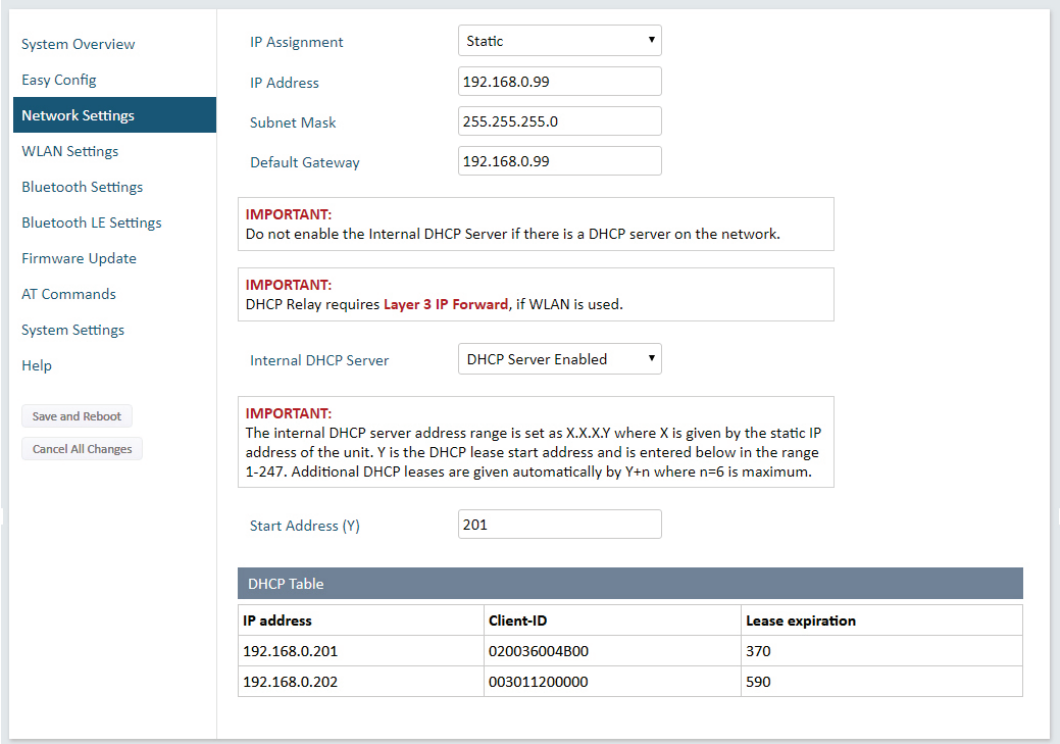

Figure 12: Network Settings page

Table 17: Network Settings page

Adjustment	Description
IP Assignment	Select static or dynamic IP addressing (DHCP).
IP Address	Static IP address for the unit. The browser should automatically be redirected to the new address after clicking on [**Save and Reboot**] (not supported by all browsers).
Subnet Mask	Subnet mask when using static IP
Default Gateway	Default gateway when using static IP
Internal DHCP Server	**Disabled:** No internal DHCP functionality **DHCP Relay Enabled:** The unit can receive a DHCP request on one interface and resend it to a DHCP server located on one of the other interfaces. Only a single DHCP server can be active for all the connected interfaces. If WLAN is used, the forwarding mode must be set to Layer 3 IP Forward. **DHCP Server Enabled:** Activates an internal DHCP server. This option is only available when IP Assignment is set to Static. Do not enable this option if there is already a DHCP server on the network!
Start Address (Y)	The internal DHCP server will assign up to 7 IP addresses starting from X.X.X.Y, where X is taken from the current static IP address setting, and Y is the value in **Start Address**. Already allocated addresses will be skipped, including the address of the unit itself. The subnet mask setting will be ignored. **Examples**: IP Address: 192.168.0.99, Start Address: 101 DHCP range = 192.168.0.101 – 192.168.0.107 IP Address: 192.168.0.103, Start Address: 101 DHCP range = 192.168.0.101 – 192.168.0.108 7 addresses are allocated but the address of the unit is skipped.

5.2.4 WLAN Settings – Client

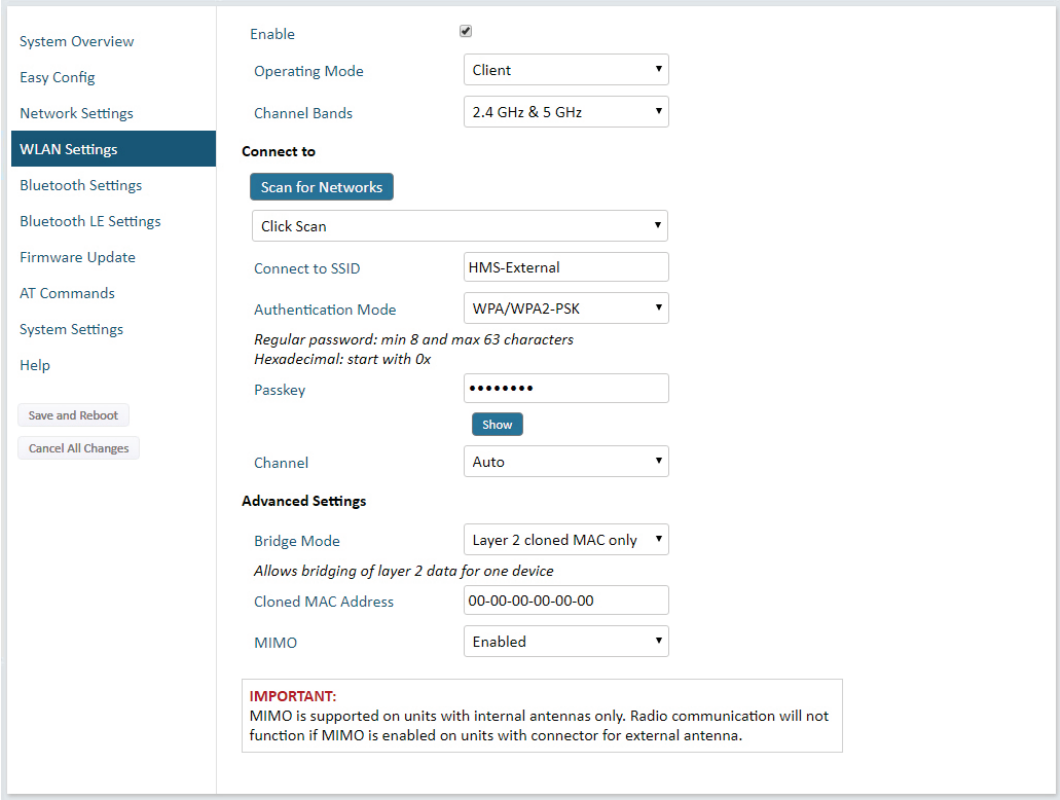

Figure 13: WLAN Settings – Client

Table 18: Network Settings page

Adjustment	Description
Enable	Enable/disable the WLAN interface.
Operating Mode	Choose operation as WLAN Client or Access Point. If Access Point is selected, additional settings will be available.
Channel Bands	Choose to scan only the 2.4 GHz or 5 GHz channel band, or both (default). **Note** **The unit can only communicate on one band at a time!** The unit can be configured to scan on both the 2.4 GHz and 5 GHz channel bands but can only communicate on one band at a time!
Scan for Networks	Click to scan the selected frequency band(s) for discoverable WLAN networks. Select a network from the dropdown menu to connect to it.
Connect to SSID	To connect manually to a network, enter its SSID (network name) here. This can be used if the network does not broadcast its SSID.
Authentication Mode	Select the authentication/encryption mode required by the network. **Open** = No encryption or authentication
Passkey	Enter the passkey when using “WPA/WPA2-PSK” or “WEP64/128”.
Username, Domain, Passphrase	Authentication details when using “LEAP” or “PEAP” (WPA2 Enterprise).
Channel	Select a specific channel to use when scanning for networks. **Auto** = all available channels will be scanned (default). See also “WLAN Channels and World Mode (Client Mode only)”.

Table 19: Advanced Settings

Adjustment	Description
Bridge Mode	**Layer 2 tunnel** = All layer 2 data will be bridged over WLAN. Use when multiple devices on both sides of an Ethernet network bridge must be able to communicate via WLAN (many-to-many). Only works between WAGO Wireless Access Point or WAGO Wireless ETHERNET Gateway devices. **Layer 2 cloned MAC only** = Layer 2 data from only a single MAC address (specified below) will be bridged over WLAN (many-to-one). **Layer 3 IP forward (default)** = IP data from all devices will be bridged over WLAN. This mode must be used when using the DHCP Relay function.
Cloned MAC Address	The MAC address to use with Layer 2 cloned MAC only (see above).

WLAN Roaming

WAGO Wireless Access Point supports Fast Roaming according to IEEE 802.11r. This enables a WLAN client to roam quicker between WLAN Access Points that have the same SSID and support

IEEE 802.11r. Fast Roaming is enabled as default but can be permanently disabled using AT commands.

See the Help page in the web interface for more information about how to set up WLAN roaming.

WLAN Channels and World Mode (Client Mode only)

Which channels are available for WLAN communication is restricted by the regulatory domain where the unit is operating. WAGO Wireless Access Point supports regulatory domain detection according to the IEEE 802.11d specification.

The unit is initially set in World Mode which enables only the universally allowed channels in the 2.4 GHz and 5 GHz bands (see the table below). World Mode can be disabled and additional channels added using AT commands. The unit will then search for country information during the scan. If the scan indicates that the unit is operating within either the European (ETSI) or North American (FCC) regulatory domains, the additional channels will be enabled. A new scan will be performed every hour to update the regulatory domain.

If no country information or conflicting information is detected, the unit will revert to World Mode. The unit must then be restarted to update the regulatory domain.

See the help page in the web interface for more information about how to use AT commands.

Table 20: Regulatory domains and WLAN channels

	2.4 GHz	5 GHz
WORLD	1 … 11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140
ETSI	1 … 11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140
FCC	1 … 11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140

Notes

- The maximum output power will be reduced on some channels depending on regulatory requirements.
- WLAN communication may take a longer time to establish during startup if World Mode is disabled and additional channels are used.

5.2.5 WLAN Settings – Access Point

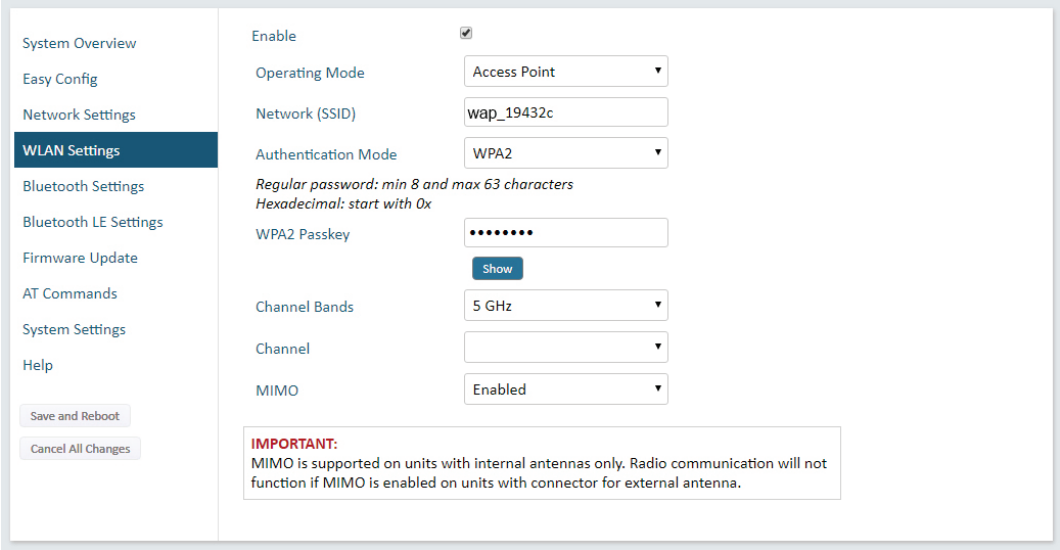

Figure 14: WLAN Settings - Access Point

The following settings are specific for Access Point mode:

Table 21: WLAN Settings - Access Point

Adjustment	Description
Enable	Enable/disable the WLAN interface.
Operating Mode	Choose operation as WLAN Client or Access Point. If Access Point is selected, additional settings will be available.
Network (SSID)	Enter an SSID (network name) for the Wireless Access Point. If this entry is left blank, the unit will generate an SSID which includes the last 6 characters of the MAC ID.
Authentication Mode	Select the authentication/encryption mode to use for the access point. **Open** = No encryption or authentication **WPA2** = WPA2 PSK authentication with AES/CCMP encryption
WPA2 Passkey	Enter a string in plain text or hexadecimal format to use for authentication. Regular (plain text) passwords must be between 8 and 63 characters. All characters in the ASCII printable range (32–126) are allowed, except " (double quote), (comma) and \ (backslash). Hexadecimal passwords must start with `0x` and be **exactly** 64 characters. See also the example passwords below.
Channel Bands, Channel	Select the WLAN channel band and channel to use for the access point. Valid channels are 1 to 11 for the 2.4 GHz band and 36, 40, 44, 48 for the 5 GHz band.

Password examples

For plain text passwords a combination of upper and lower case letters, numbers, and special characters is recommended.

Example of a strong plain text password:
`uS79_xpa&43`

Example of hexadecimal password:
`0x000102030405060708080a0b0c0d0e0f101112131415161718191a1b1c1d1e1f`

Note

Do not use the example passwords above in a live environment!

5.2.6 Bluetooth Settings – General

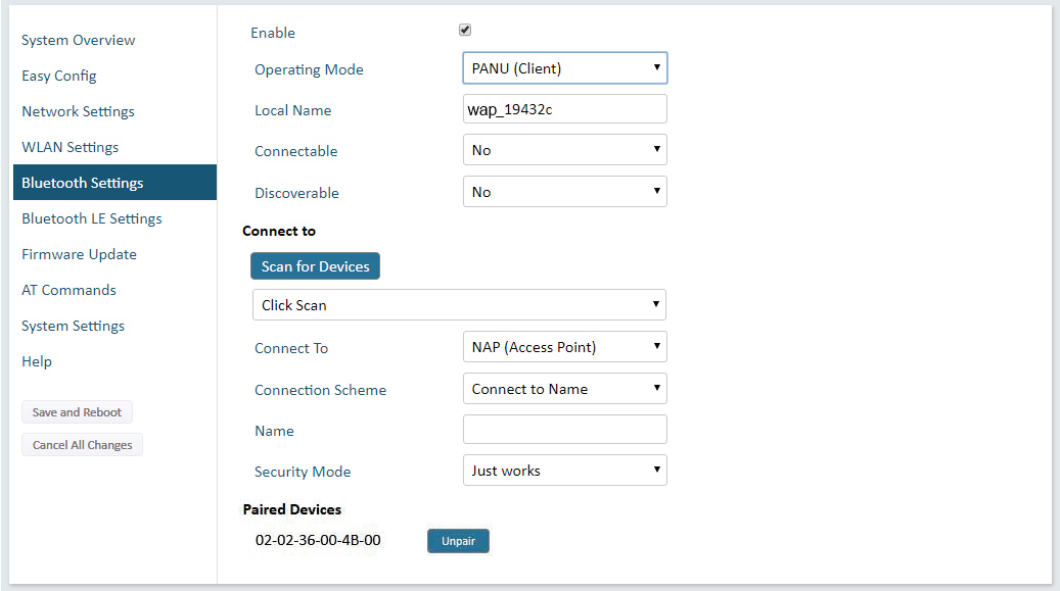

Figure 15: Bluetooth Settings

Table 22: Bluetooth Settings

Adjustment	Description
Enable	Enable/disable the Bluetooth interface.
Operating Mode	**PANU (Client)** = The unit 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 (Access Point)** = The unit will operate as a Bluetooth Network Access Point. It can connect to up to 7 Bluetooth PANU devices.
Local Name	Identifies the unit to other Bluetooth devices. If left blank, the unit will use a default name including the last 6 characters of the MAC ID.
Connectable	Enable to make the unit accept connections initiated by other Bluetooth devices.
Discoverable	Enable to make the unit visible to other Bluetooth devices.
Security Mode	**Disabled** = No encryption or authentication. **PIN** = Encrypted connection with PIN code security. This mode only works between two units of this type and brand (not with third-party devices). PIN codes must consist of 4 to 6 digits. **Just Works** = Encrypted connection without PIN code.
Paired Devices	Lists the currently connected Bluetooth devices.

Note

The settings for the PANU mode are as follows!
The settings for the PANU mode (Connect to) can be found in the following chapter!

5.2.7 Bluetooth Settings – PANU Mode

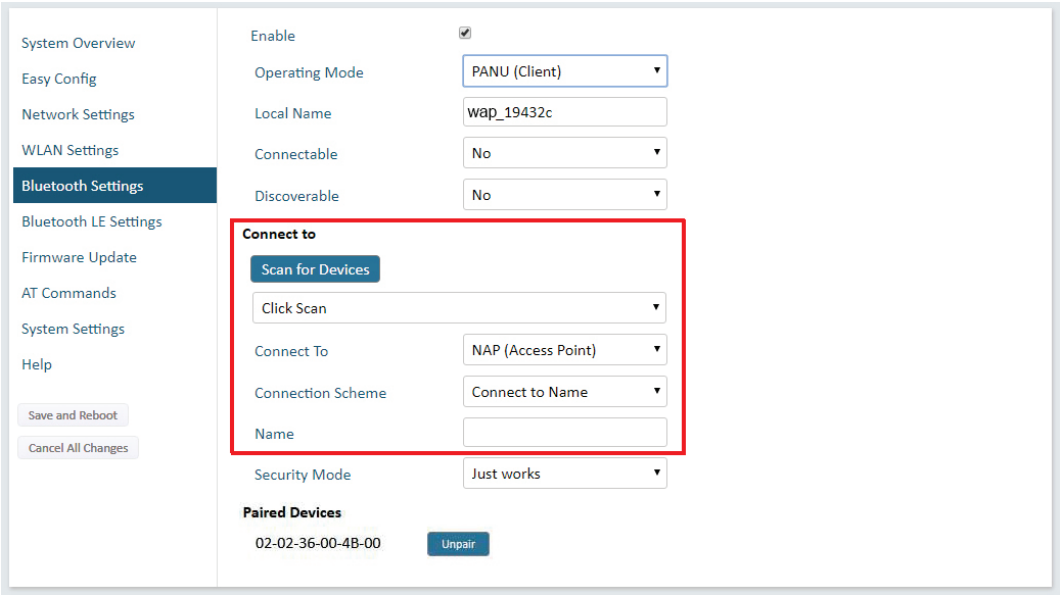

Figure 16: Bluetooth Settings – PANU Mode

Table 23: Bluetooth Settings – PANU Mode

Adjustment	Description
Scan for Devices	Scans the network for discoverable Bluetooth devices. To connect to a device, select it from the dropdown menu when the scan has completed.
Connect To	Used when connecting manually to a NAP or PANU device.
Connection Scheme	Choose whether to select a Bluetooth device by MAC address (default) or Name when connecting manually. Connecting to MAC will lock the connection to a specific hardware while connecting to Name allows for more flexibility.
MAC/Name	MAC address or Name of the Bluetooth device to connect to.

5.2.8 Bluetooth Settings – NAP Mode

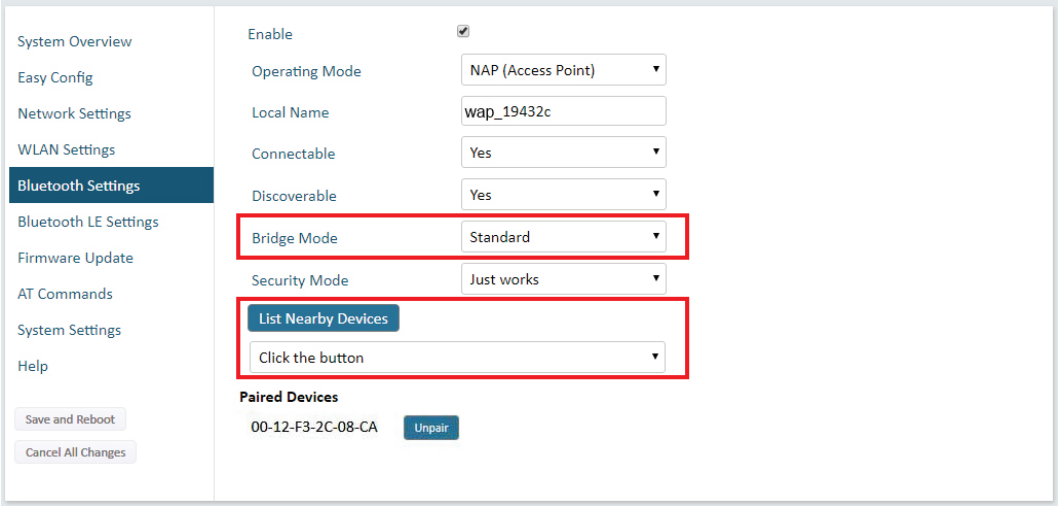

Figure 17: Bluetooth settings – NAP

Table 24: Bluetooth Settings – NAP Mode

Adjustment	Description
Bridge Mode	**Standard** = Default mode. **Layer 3 IP forward** = IP data will be bridged over Bluetooth. This mode must be used when connecting to an Android device over Bluetooth. The network must have an active DHCP server.
List Nearby Devices	Scans the network and lists discoverable Bluetooth devices. Pairing cannot be initiated in NAP mode.

5.2.9 Bluetooth LE Settings

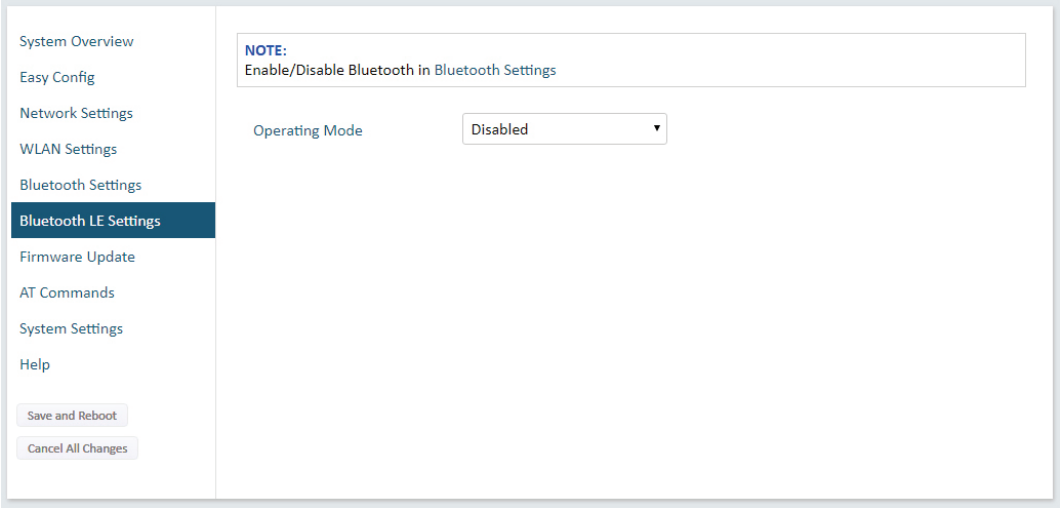

Figure 18: Bluetooth LE settings

Table 25: Bluetooth LE Settings

Adjustment	Description
Operating Mode	**Disabled** = Bluetooth LE disabled (default) **Central** = Bluetooth LE enabled

Please select **Help** in the main menu for more information about using Bluetooth LE with AT Commands.

Note

Bluetooth must be enabled!
Bluetooth must be enabled on the Bluetooth Settings page to use Bluetooth LE.!

5.2.10 Firmware Update

To update the firmware in the unit, click on **Browse** to select a downloaded firmware file, then click on **Send** to send it to the unit.

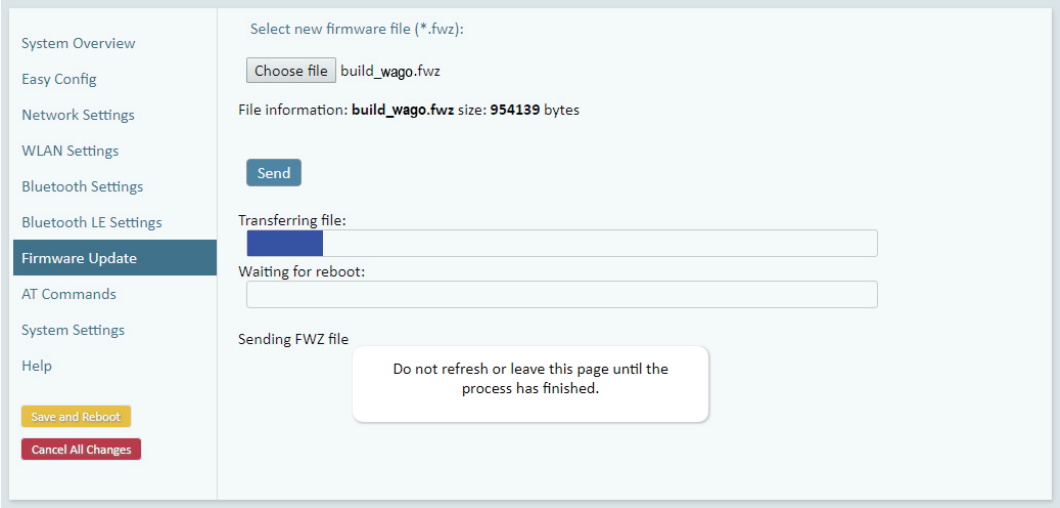

Figure 19: Firmware update in progress

Both progress bars will turn green when the firmware update has been completed. The unit will then reboot automatically.

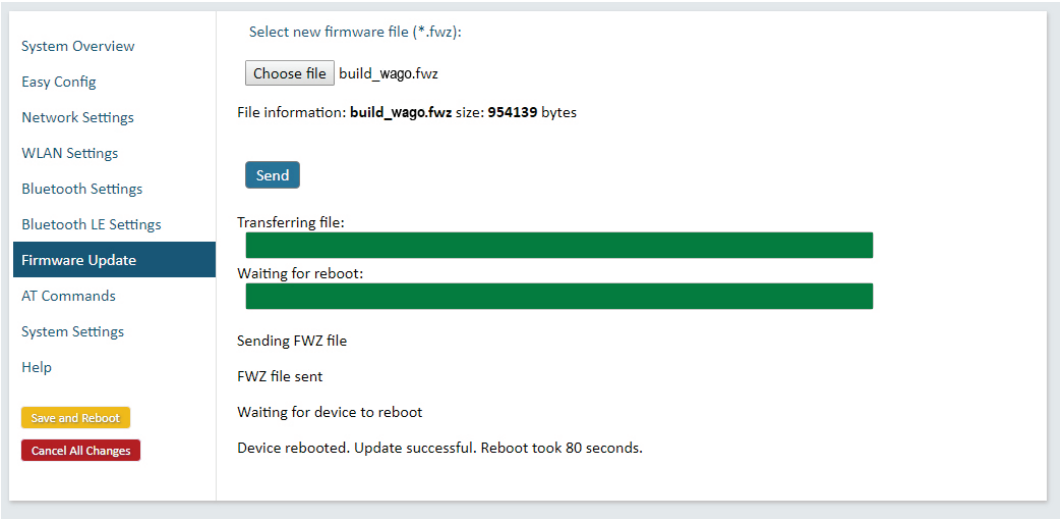

Figure 20: Firmware update completed

Updating the firmware will not change the configuration settings.

5.2.11 Configurations via AT Commands

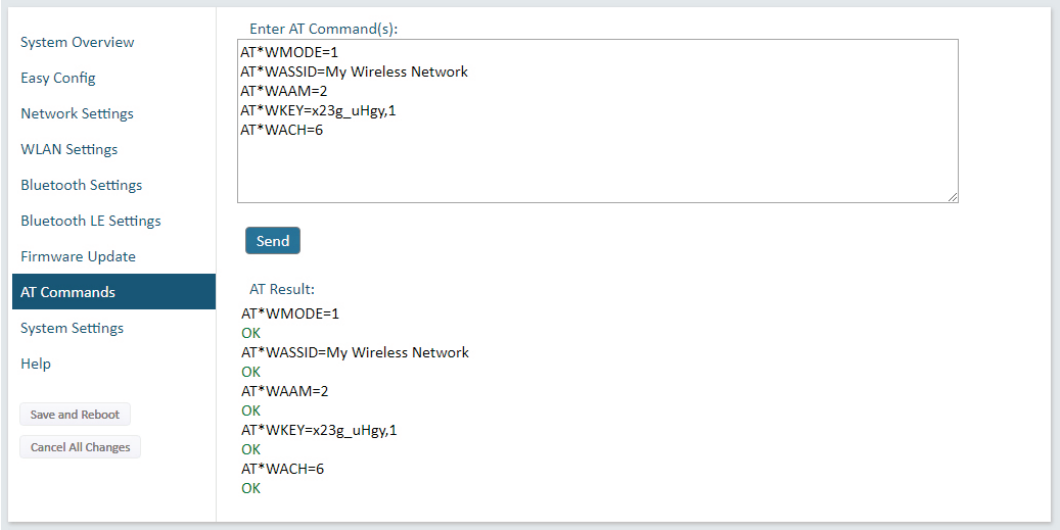

Figure 21: AT Commands

AT commands can be used for setting advanced parameters that are not accessible in the web interface, to read out parameters in text format, and for batch configuration using command scripts.

Enter or paste the commands into the text box, then click on [**Send**]. The result codes will be displayed below the text box.

Note

Overview of AT commands

A list of all AT commands is available on the “Help” page in the web interface.

5.2.12 System Settings

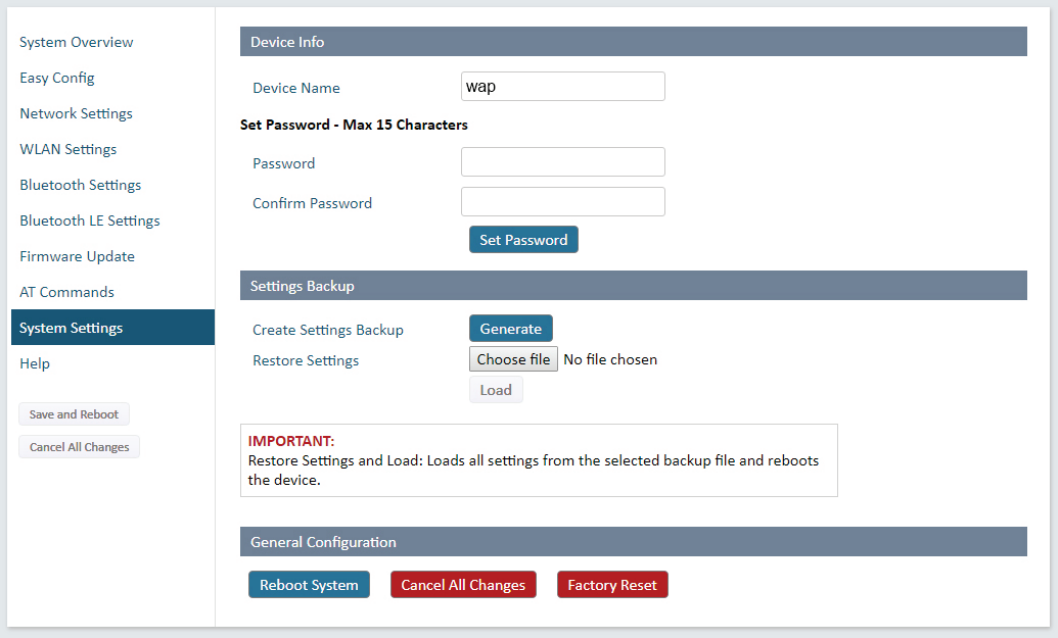

Figure 22: System Settings

Table 26: Device Info

Adjustment	Description
Device Name	Enter a descriptive name for the unit.
Password	Enter a password for accessing the web interface.
Confirm Password	Repeat the password entry.
[Set Password]	Click on [**Set Password**] to set the password.

Note

Secure password is recommended!

Setting a secure password for the unit is strongly recommended!

Table 27: Settings Backup

Adjustment	Description
Create Settings Backup	Click on [**Generate**] to save the current configuration to a file on your computer. Password is not included in backup file.
Restore Settings	Click on [**Choose file**] and select a previously saved configuration, then click on Load. The settings in the saved configuration will be applied and the unit will reboot.

Table 28: General Configuration

Adjustment	Description
[Reboot System]	Reboots the system without applying changes.
[Cancel All Changes]	Restores all parameters in the web interface to the currently active values.
[Factory Reset]	Resets the unit to the factory default settings and reboots.

5.3 Factory Restore

Any one of these actions will restore the factory default settings:

- Clicking on **Factory Restore** on the **System Settings** page.
- Executing **Easy Config Mode 2**.
- Issuing the AT command **AT&F** and then restarting the unit.
- Holding **RESET** pressed for >10 seconds and then releasing it.

Table 29: Default Network Settings

Adjustment	Description
IP Assignment	Static
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99
Internal DHCP Server	Enabled

Table 30: Default WLAN Settings

Adjustment	Description
Operating Mode	Access Point
Channel Bands	2.4 GHz
Authentication Mode	WPA2–PSK
Channel	6
WPA-PSK	See product printing
SSID	WAP_xxxxxx (last 6 hexadecimal numerals from MAC address)

Table 31: Default Bluetooth Settings

Adjustment	Description
Local Name	Generated from MAC address
Operating Mode	Off

6 Appendix

6.1 Configuration Examples

6.1.1 Ethernet Bridge via WLAN or Bluetooth® (Easy Config)

Figure 23: ETHERNET Bridge

This example describes how to connect two ETHERNET network segments via WLAN or *Bluetooth*® using Easy Config.

1. In the web interface of unit 1, activate **Easy Config Mode 4**. This unit will now be discoverable and open for automatic configuration.

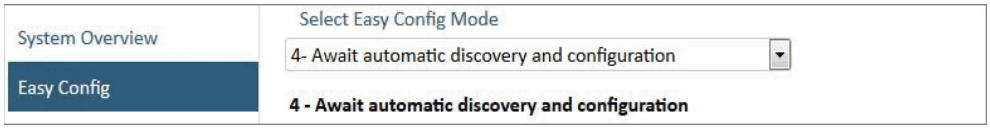

Figure 24: Easy Config Mode 4

2. In the web interface of unit 2, activate **Easy Config Mode 5** for WLAN or 6 for *Bluetooth*®. Unit 2 will now discover and configure unit 1 as a client and configure itself as an access point.

Figure 25: Easy Config Mode 5

Unit 1 will be assigned the first free IP address in the same Ethernet subnet as unit 2.

Adding More Devices
Up to 6 additional clients can be added by repeating the procedure. Each new client will be assigned the next free IP address in the current subnet.

6.1.2 PROFINET networking via Bluetooth®

Figure 26: ETHERNET Bridge

This example describes how to connect a PROFINET IO device and a PROFINET PLC over *Bluetooth*® using two Wireless Access Points and Easy Config.

The Wireless Access Points will be configured with PROFINET optimization, which means that PROFINET messages will have priority over TCP/IP frames.

See the respective documentation for the IO device and PLC on how to configure them for PROFINET communication.

Configuration

1. Reset both Wireless Access Points to the factory default settings.
2. Connect Wireless Access Point 1 to the IO device and Wireless Access Point 2 to the PLC.
3. Set Wireless Access Point 1 to Easy Config **Mode 4**.

This unit will now be discoverable and open for automatic configuration.

4. Set Wireless Access Point 2 to Easy Config **Mode 8.**

This unit should now automatically discover and configure unit 1 as a *Bluetooth*® client, and configure itself as an access point. Both units will be optimized for PROFINET.

The IO device should now be able to communicate with the PLC as if using a wired connection.

Adding More Devices
Up to 6 additional clients can be added by repeating the procedure. Each new client will be assigned the next free IP address in the current subnet.

Note

Note the IO cycle update time!
The IO cycle update time for each IO device must be set to ≥ 64 ms!

6.1.3 EtherNet/IP™ Networking via Bluetooth®

Configuration with Easy Config

Figure 27: EtherNet/IP wireless network

This example describes how to connect an EtherNet/IP IO device and an EtherNet/IP PLC over Bluetooth using two Wireless Access Points and Easy Config.

See the respective documentation for the IO device and PLC on how to configure them for EtherNet/IP communication.

Configuration

1. Reset both Wireless Access Points to the factory default settings.
2. Connect Wireless Access Point 1 to the IO device and Wireless Access Point 2 to the PLC.
3. Set Wireless Access Point 1 to Easy Config **Mode 4**.

This unit will now be discoverable and open for automatic configuration.

4. Set Wireless Access Point 2 to Easy Config **Mode 6.**

This unit should now automatically discover and configure unit 1 as a *Bluetooth*® client, and configure itself as an access point.

The IO device should now be able to communicate with the PLC as if using a wired connection.

Adding More Devices
Up to 6 additional clients can be added by repeating the procedure. Each new client will be assigned the next free IP address in the current subnet.

Note

Note the Requested Packet Interval (RPI)!
The Requested Packet Interval (RPI) for each IO device must be set to ≥ 64 ms!

6.1.4 Ethernet network to existing WLAN

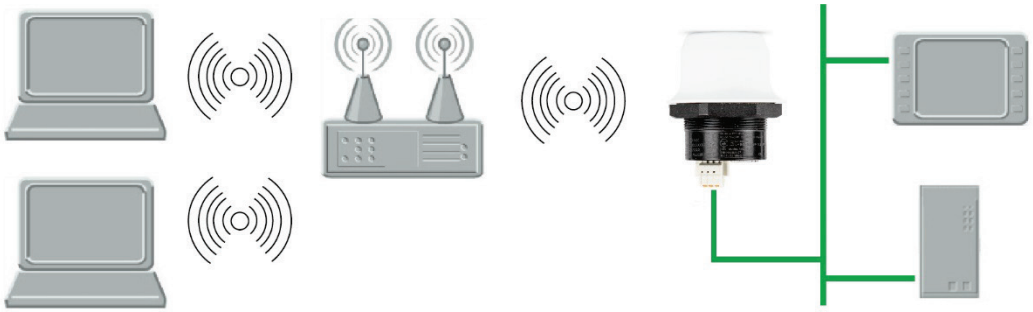

Figure 28: Connecting to a WLAN

This example describes how to connect a machine with an internal ETHERNET network to an existing WLAN.

This setup allows traffic on network layer 3, but not layer 2. This means that TCP/IP based protocols such as EtherNet/IP, Modbus TCP and BACnet can be used on the WLAN, but not protocols that use layer 2 traffic, such as PROFINET.

Configuration

1. Reset the Wireless Access Point to the factory default settings.
2. In **Network Settings**, configure the IP settings as required by the wireless network
3. If the network uses DHCP, select **DHCP Relay Enabled**.
4. In **WLAN Settings**, click on **Scan for Networks.**
5. When the scan has completed, select the wireless network from the dropdown list.
6. If required, select the authentication mode and enter the passkey for the wireless network.

Note

Note the WLAN Bridge Mode settings!
WLAN Bridge Mode must be set to Layer 3 IP forward (the default setting).

7. Click on [**Save and Reboot**].

The Ethernet network should now be able to access the WLAN access point.

6.1.5 Adding single Ethernet node to WLAN

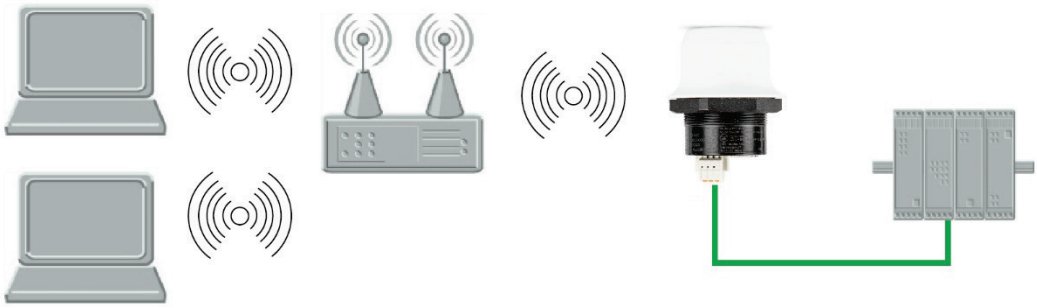

Figure 29: Adding WLAN connectivity

This example shows how to connect a PLC with an ETHERNET network interface to an existing WLAN with support for layer 2 and layer 3 traffic. The WLAN interface in the Wireless Access Point will clone the MAC address of the ETHERNET interface in the PLC.

Only a single ETHERNET node will be able to communicate via a third-party WLAN access point in this setup.

Configuration

1. Reset the Wireless Access Point to the factory default settings.
2. In **Network Settings**, configure the IP settings as required by the wireless network
3. In **WLAN Settings**, click on **Scan for Networks.**
4. When the scan has completed, select the wireless network from the dropdown list.
5. If required, select the authentication mode and enter the passkey for the wireless network.
6. Click on [**Save and Reboot]**.
7. Check the **System Overview** page to confirm that the WLAN connection is established before continuing.
   DO NOT SKIP THIS STEP! After the final steps of the configuration procedure the web interface may no longer be accessible from the network without doing a factory reset.
8. In **WLAN Settings**, set **Bridge Mode** to **Layer 2 cloned MAC only.**
9. Enter the MAC address of the PLC in the **Cloned MAC Address** field.
10. Click on [**Save and Reboot]**.

The Wireless Access Point will now function as a WLAN interface for the PLC using the MAC address of its ETHERNET interface.

6.1.6 Accessing PLC via WLAN from Handheld Device

Figure 30: Accessing a PLC from a handheld device using WLAN

This example describes how to use a Wireless Access Point to access the web interface of a PLC on a wired network from a tablet or smartphone which uses DHCP. The Wireless Access Point will function as a WLAN access point.

Please refer to the documentation for the handheld device and PLC on how to configure their respective network settings.

Configuration

1. Reset the Wireless Access Point to the factory default settings.

2. In **Network Settings**, configure the IP settings as required.

   - If the wired network uses DHCP, select **DHCP Relay Enabled**. The DHCP server on the network will now be able to allocate an IP address to the handheld device.

   - If the wired network uses static IP, select **DHCP Server Enabled** and set a Start Address for DHCP addressing. Make sure that the address range does not contain any existing addresses on the network.

The Wireless Access Point will now function as a DHCP server and allocate an IP address to the handheld device over WLAN.

Note

Do not enable the internal DHCP Server if one already exist!
Do not enable the internal DHCP Server if there is already a DHCP server on the network, as this may cause IP address conflicts!

3. In **WLAN Settings**, set **Operating Mode** to **Access Point.**

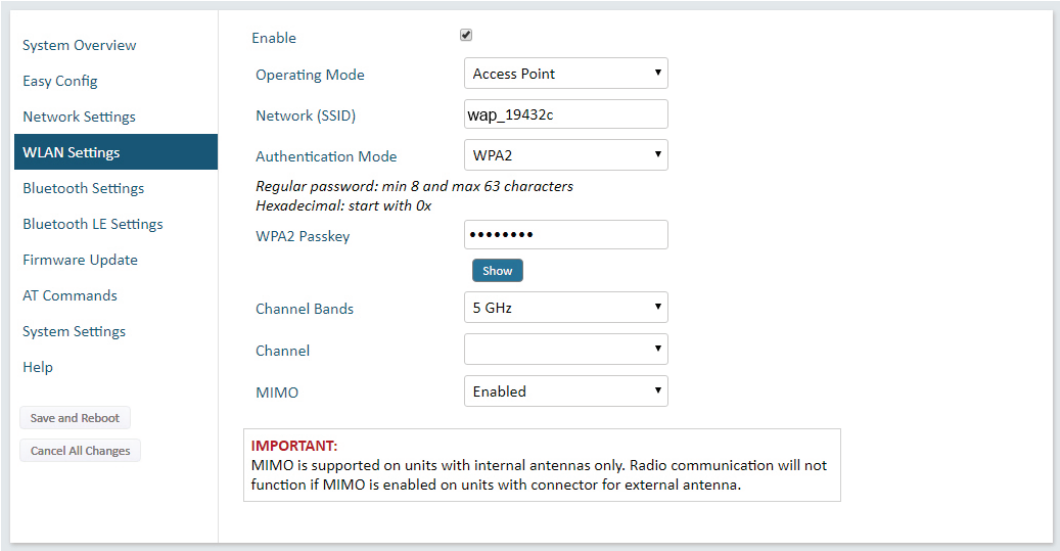

Figure 31: WLAN Settings

4. Enter a unique **SSID** (network name) for the new wireless network.

5. Set **Authentication Mode** to **WPA2** and enter a passkey.

6. Select a **Channel band** and a **Channel**.

7. Click on [**Save and Reboot**].

You should now be able to connect to the SSID of the Wireless Access Point on your handheld device and access the PLC by by entering its IP address in a browser.

6.2 Wireless Technology Basics

Wireless technology is based on the propagation and reception of electromagnetic waves. These waves respond in different ways in terms of propagation, dispersion, diffraction and reflection depending on their frequency and the medium in which they are travelling.

To enable communication there should optimally be an unobstructed line of sight between the antennas of the devices. However, the so called Fresnel Zones should also be kept clear from obstacles, as radio waves reflected from objects within these zones may reach the receiver out of phase, reducing the strength of the original signal (also known as phase cancelling).

Fresnel zones can be thought of as ellipsoid three-dimensional shapes between two wireless devices. The size and shape of the zones depend on the distance between the devices and on the signal wave length. As a rule of thumb, at least 60 % of the first (innermost) Fresnel zone must be free of obstacles to maintain good reception.

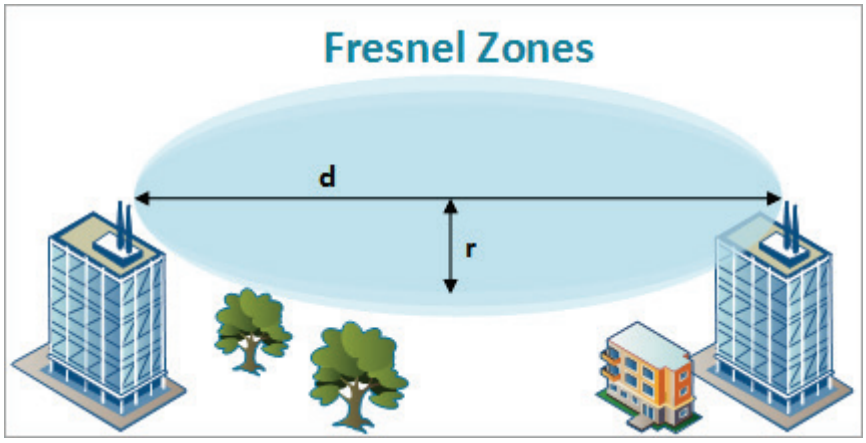

Figure 32: Fresnel zones

Table 32: Area to keep clear of obstacles (first Fresnel zone)

Distance	Fresnel zone radius (r)	
	2.4 GHz (WLAN or Bluetooth)	5 GHz (WLAN)
100 m	1.7 m	1.2 m
200 m	2.5 m	1.7 m
300 m	3.0 m	2.1 m
400 m	3.5 m	2.4 m

The wireless signal may be adequate even if there are obstacles within the Fresnel zones, as it always depends on the number and size of the obstacles and where they are located. This is especially true indoors, where reflections on metal objects may actually help the propagation of radio waves. To reduce interference and phase cancelling, the transmission power of the unit may in some cases have to be reduced to limit the range.

It is therefore recommended to use a wireless signal analysis tool for determining the optimal placement and configuration of a wireless device.

6.3 Radio Antenna Patterns

This section presents information about the radio antenna patterns for the Wireless Access Point (WAP).

The diagram scale shows relative RSSI values, where the outer ring represents maximum radio power and is labelled 0 dB. The inner rings represent the increasing attenuation in dB measured in different angles around the WAP, while maintaining the same distance.

6.3.1 Azimuth (Horizontal) View

This diagram shows the horizontal antenna pattern when looking at the WAP from above, i.e. looking at the top logo from above.

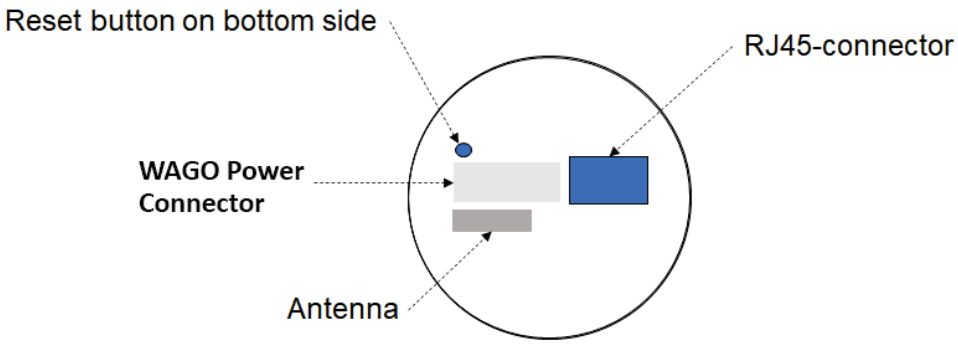

Figure 33: Azimuth (Horizontal) View

Diagram analysis: the diagram displays an omnidirectional antenna gain regarding 2.4 GHz (blue line) which is used for Bluetooth and Wireless LAN 2.4 GHz. However, it also shows that Wireless LAN 5 GHz (orange line) has a limited antenna gain in the approximate directions 105° to 190°, i. e. the 5 GHz range will be limited in this direction.

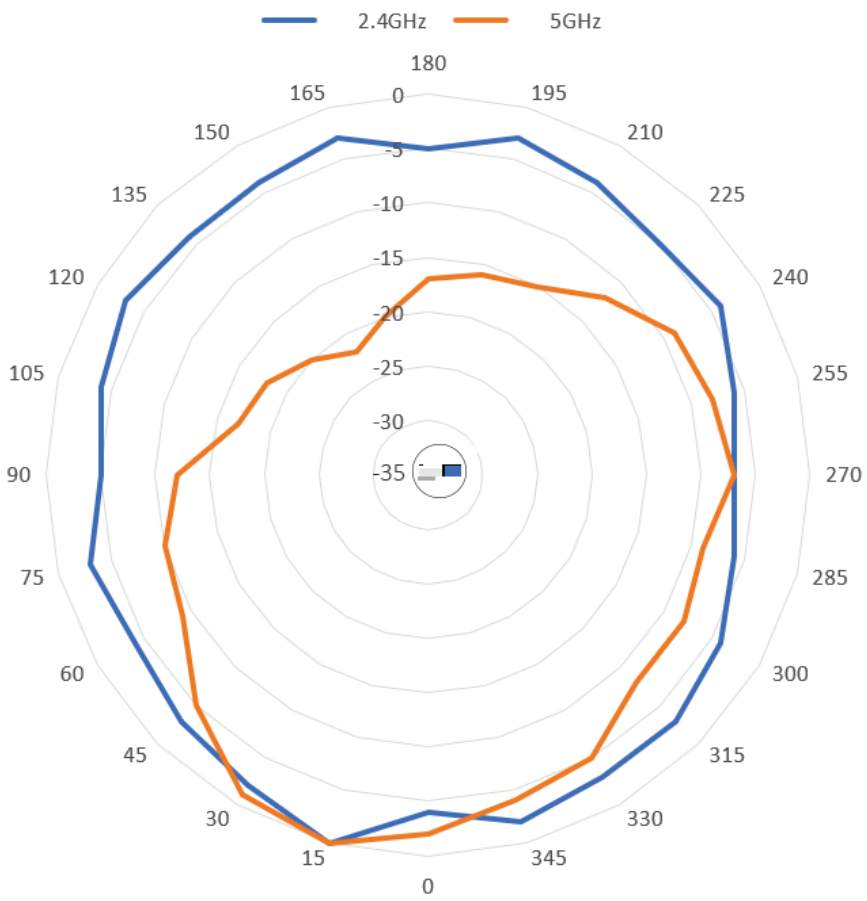

Figure 34: Antenna Pattern Horizontal

Note

Please note the information!
Limited gain for 5 GHz between 105° to 190°!

6.3.1.1 Front View – Vertical 0°

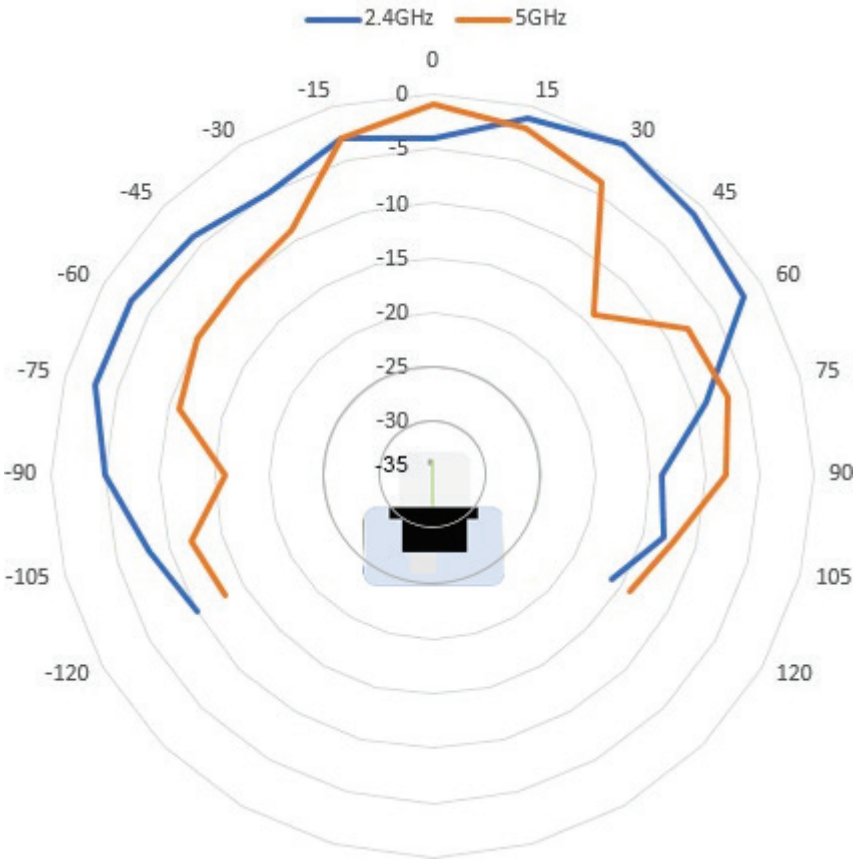

Figure 35: Front View – Vertical 0°

6.3.1.2 Side View – Vertical 90°

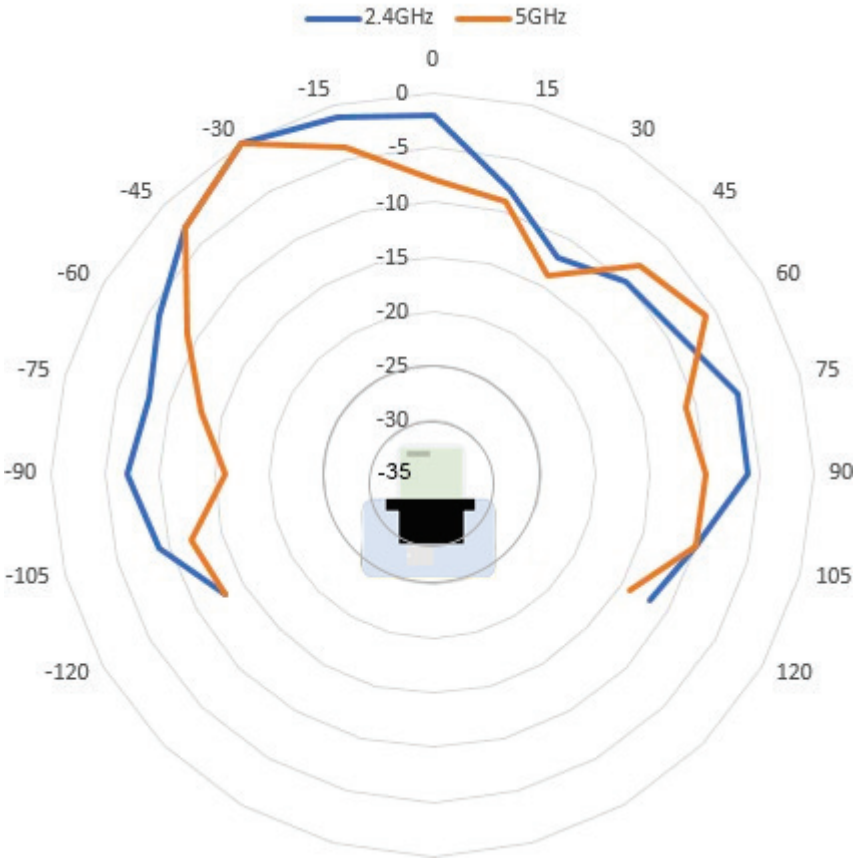

Figure 36: Side View – Vertical 90°

6.3.2 Vertical Views

These diagrams show the antenna pattern when looking at the WAP from the side in two different rotations, 0° and 90°. The WAP is mounted in a metal cabinet illustrated by the box below.

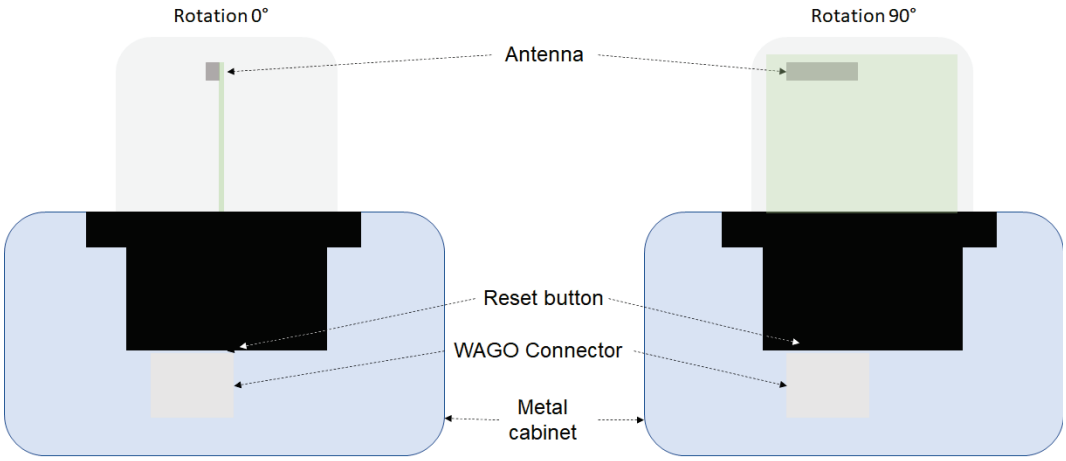

Figure 37: Vertical Views

Diagram analysis: The vertical antenna gain is fairly omnidirectional for both frequencies. It is also clear to see that the metal cabinet where the WAP is

mounted will increase the gain “upwards” in reference to the surface where the WAP is mounted. Thus the gain “downwards” is limited as expected.

6.3.3 Throughput Diagram

This diagram shows how data throughput decreases when distance increases. Note the huge difference between using a backshield to focus the radio energy, and not using a backshield. Using a backshield can greatly increase radio coverage if used correctly.

The diagram covers both the Wireless Access Point and the Wireless ETHERNET Gateway in a free field application.

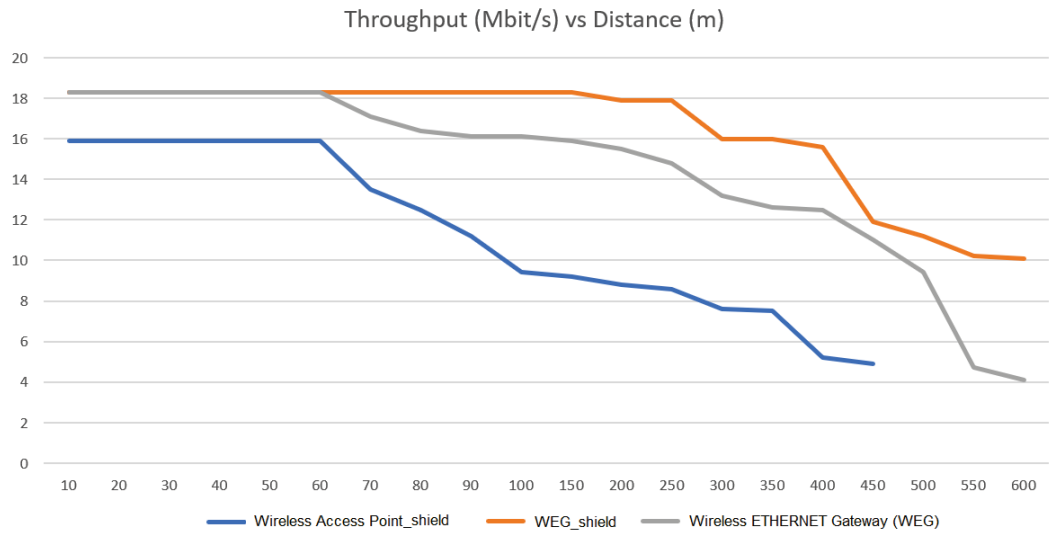

Figure 38: Throughput Diagram

6.4 Data Security for Radio Transmission

It is often assumed that wireless communication systems are less secure than line-connected systems. When used and operated correctly, wireless systems offer at least an equivalent level of security.

The following conditions must apply before an unauthorized user can obtain access to data exchanged via wireless communication:

1. The attacker must be familiar with the communication system in use and be within the operating range of the system.

2. Radio transmission must take place without the use of any security mechanisms offered by this technology or the attacker must have adequate means to determine the security code.

List of Figures

List of Tables