Anybus® Wireless Bolt™

USER MANUAL

SCM-1202-007-EN 2.5 ENGLISH

Connecting Devices™

Important User Information

Liability

Every care has been taken in the preparation of this document. Please inform HMS Industrial Networks AB of any inaccuracies or omissions. The data and illustrations found in this document are not binding. We, HMS Industrial Networks AB, reserve the right to modify our products in line with our policy of continuous product development. The information in this document is subject to change without notice and should not be considered as a commitment by HMS Industrial Networks AB. HMS Industrial Networks AB assumes no responsibility for any errors that may appear in this document.

There are many applications of this product. Those responsible for the use of this device must ensure that all the necessary steps have been taken to verify that the applications meet all performance and safety requirements including any applicable laws, regulations, codes, and standards.

HMS Industrial Networks AB will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features, timing, or functional side effects found outside the documented scope of this product. The effects caused by any direct or indirect use of such aspects of the product are undefined, and may include e.g. compatibility issues and stability issues.

The examples and illustrations in this document are included solely for illustrative purposes. Because of the many variables and requirements associated with any particular implementation, HMS Industrial Networks AB cannot assume responsibility for actual use based on these examples and illustrations.

Intellectual Property Rights

HMS Industrial Networks AB has intellectual property rights relating to technology embodied in the product described in this document. These intellectual property rights may include patents and pending patent applications in the USA and other countries.

Anybus® is a registered trademark and Wireless Bolt™ is a trademark of HMS Industrial Networks AB. All other trademarks mentioned in this document are the property of their respective holders.

Table of Contents

Page

This page intentionally left blank

1 Preface

1.1 About This Document

This manual describes how to install and configure Anybus Wireless Bolt.

For additional related documentation and file downloads, please visit the Anybus support website at www.anybus.com/support.

Included Additional Files

SCM-1202-061	UL Ord.Loc. compliance information
SCM-1202-062	UL Haz.Loc. compliance information
SCM-1202-063	ATEX compliance information

1.2 Document History

Version	Date	Description
1.0	2016-09-15	First release
1.1	2016-11-23	Minor additions and updates
1.2	2017-12-14	Added configuration example
2.0	2017-04-19	Updated for SP1
2.1	2017-07-06	Added Bluetooth bridge mode
2.2	2017-10-04	Updated for SP2
2.3	2017-10-18	Updated compliance info
2.4	2017-12-21	Updated for FW 1.3.9
2.5	2018-02-02	Minor update

1.3 Document Conventions

Ordered lists are used for instructions that must be carried out in sequence:

1. First do this
2. Then do this

Unordered (bulleted) lists are used for:

- Itemized information
- Instructions that can be carried out in any order

...and for action-result type instructions:

► This action...

  ➡ leads to this result

Bold typeface indicates interactive parts such as connectors and switches on the hardware, or menus and buttons in a graphical user interface.

```
Monospaced text is used to indicate program code and other
kinds of data input/output such as configuration scripts.
```

This is a cross-reference within this document: *Document Conventions, p. 4*

This is an external link (URL): www.hms-networks.com

ⓘ *This is additional information which may facilitate installation and/or operation.*

! This instruction must be followed to avoid a risk of reduced functionality and/or damage to the equipment, or to avoid a network security risk.

⚠ **Caution**
This instruction must be followed to avoid a risk of personal injury.

⚠ **WARNING**
This instruction must be followed to avoid a risk of death or serious injury.

2 Description

2.1 Product Description

Anybus Wireless Bolt provides wireless communication over WLAN and/or Bluetooth® to wired networks.

Typical applications for Anybus Wireless Bolt include:

- Adding wireless cloud connectivity to industrial devices
- Accessing devices from a laptop, smartphone or tablet
- Ethernet cable replacement between devices

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.

2.2 Bluetooth or WLAN?

Use Bluetooth when...

- ...the wireless link has an Anybus Wireless Bridge II or Anybus Wireless Bolt at both ends.
- ...an interruption-free connection is more important than data throughput speed.
- ...interference robustness is important – e.g. in an industrial environment.
- ...a Profinet I/O cycle time or EtherNet/IP RPI of 64 ms or more is acceptable.

Use WLAN when...

- ...connecting to other types of wireless devices or a WLAN infrastructure.
- ...high data throughput speed is more important than connection reliability.
- ...large file transfers are expected.
- ...WLAN channel frequency planning is possible.
- ...a low Profinet I/O cycle time or EtherNet/IP RPI is desired.

2.3 Model Name – Certification Identifier

The model name is used to identify the product for various certifications. It consists of a model prefix followed by two designators for the specific interface configuration and functionality.

Prefix	AWB2	Anybus Wireless Bolt
Interface configuration	A	Interface 18-pin plug
Functionality	A B C	Ethernet Ethernet and RS232/485 Ethernet and CAN

Example: AWB2AA = Anybus Wireless Bolt with18-pin connector and Ethernet networking only.

3 Installation

3.1 Safety

⚠ **Caution**
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.

! 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.

! This product contains parts that can be damaged by electrostatic discharge (ESD). Use ESD prevention measures to avoid damage.

See also additional safety instructions in the included compliance information.

3.2 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 *Technical Data, p. 34* for details about the antenna characteristics.

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.

See also *Wireless Technology Basics, p. 33*.

3.3 Mechanical Installation

Anybus Wireless Bolt 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.

Tightening torque: 5 Nm ±10 %

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

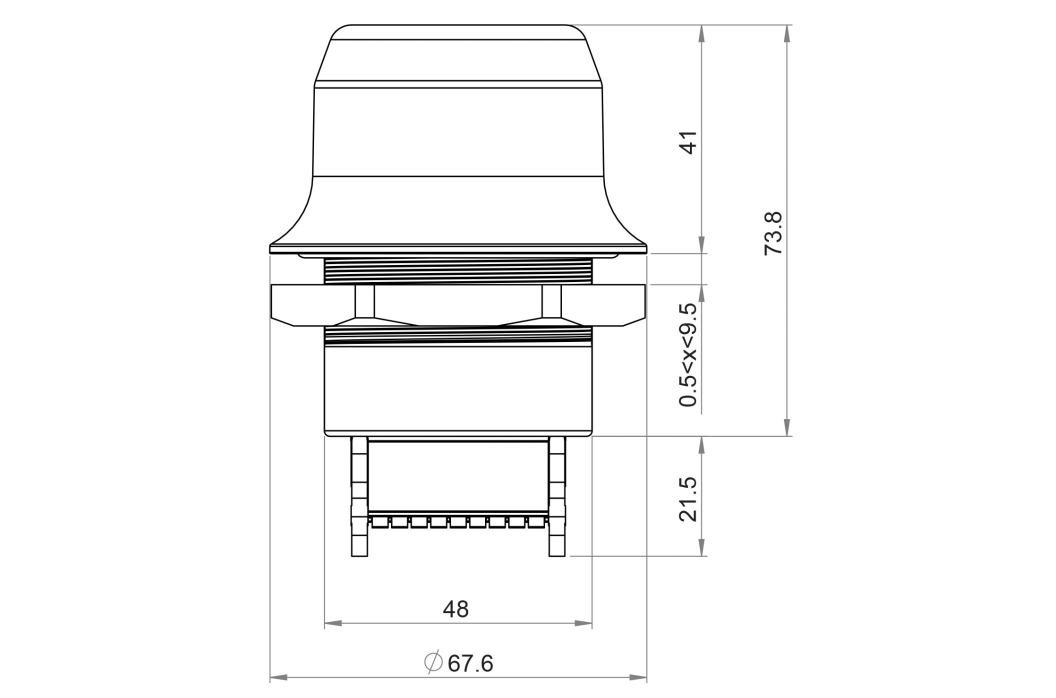


Fig. 1 Installation drawing

All measurements are in mm.

3.4 Connector

The 18-pin connector is common for all models of the Anybus Wireless Bolt. Some pins may have a different function depending on model. Unused pins should not be connected.

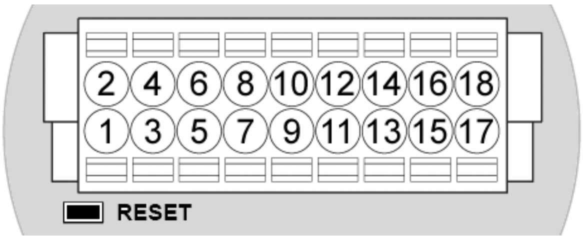


Fig. 2 Connector

The location of the **RESET** button can be used as a reference for the pin numbering when the connector is attached to the Wireless Bolt. Pin 1 will be the pin closest to the button.

Pin	Name	Description
1	VIN	Power + (9–30 V)
2	GND	Power Ground
3	DI	Digital input + (9–30 V)
4	DI_GND	Digital input ground
5	ETN_RD+	Ethernet receive + (white/orange)
6	ETN_RD-	Ethernet receive - (orange)
7	ETN_TD-	Ethernet transmit - (green)
8	ETN_TD+	Ethernet transmit + (white/green)
9	RS485_B	RS-485 B Line
10	FE/Shield	Ethernet: Functional Earth Serial: Functional Earth and Shield
11	RS232_TXD	RS-232 Transmit
12	RS485_A/RS232_RXD	RS-485 A Line / RS-232 Receive
13	RS232_RTS	RS-232 Request To Send
14	RS232_CTS	RS-232 Clear To Send
15	ISO_5V	Isolated 5 V for serial interface
16	ISO_GND	Isolated Ground for serial interface
17	CAN_L	CAN Low
18	CAN_H	CAN High

Note:

- The Ethernet wire colors refer to the **T568A** standard.
- If using a shielded Ethernet cable the shield must be unconnected.
- RS-232 and RS-485 cannot be used at the same time.
- Use termination for RS-485 and CAN when required.

3.5 Cabling

To make an Ethernet connector cable for the Anybus Wireless Bolt:

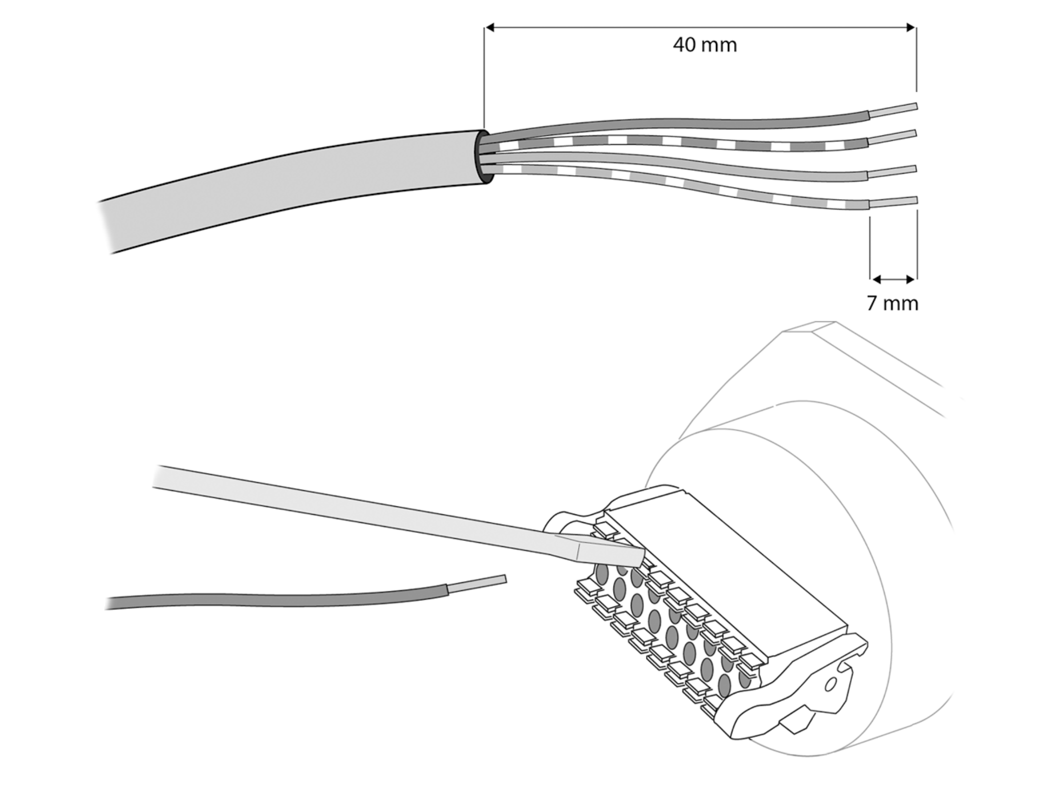


Fig. 3 Ethernet cable

1. Cut off one of the connectors on a standard Cat5e or Cat6 Ethernet cable.
2. Strip off about 40 mm (1½ inch) of the cable jacket and untwist the orange, orange/white, green and green/white wires. The other wires will not be used.
3. Strip off about 7 mm (¼ inch) of the isolation on each wire.
4. Push the pin spring release next to each socket on the connector and insert the correct wire end according to *Connector, p. 9*.

Connect the wires from the power supply in the same way as the Ethernet wiring. Make sure that polarity is not reversed.

4 Configuration

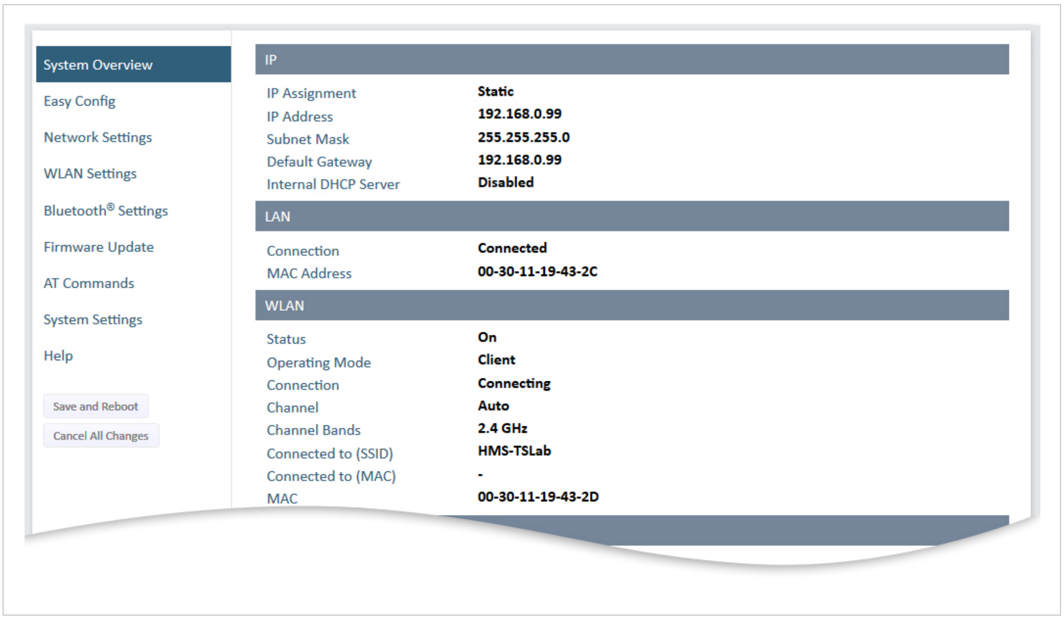
4.1 General

Anybus Wireless Bolt should normally be configured via the web interface. Parameters can be set individually or using one of the pre-configured **Easy Config** modes.

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.

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

> **!** The web interface is designed for the current stable versions of Internet Explorer, Chrome, Firefox and Safari. Other browsers may not support the full functionality of the web interface.



IP	
IP Assignment	Static
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99
Internal DHCP Server	Disabled
LAN	
Connection	Connected
MAC Address	00-30-11-19-43-2C
WLAN	
Status	On
Operating Mode	Client
Connection	Connecting
Channel	Auto
Channel Bands	2.4 GHz
Connected to (SSID)	HMS-TSLab
Connected to (MAC)	-
MAC	00-30-11-19-43-2D

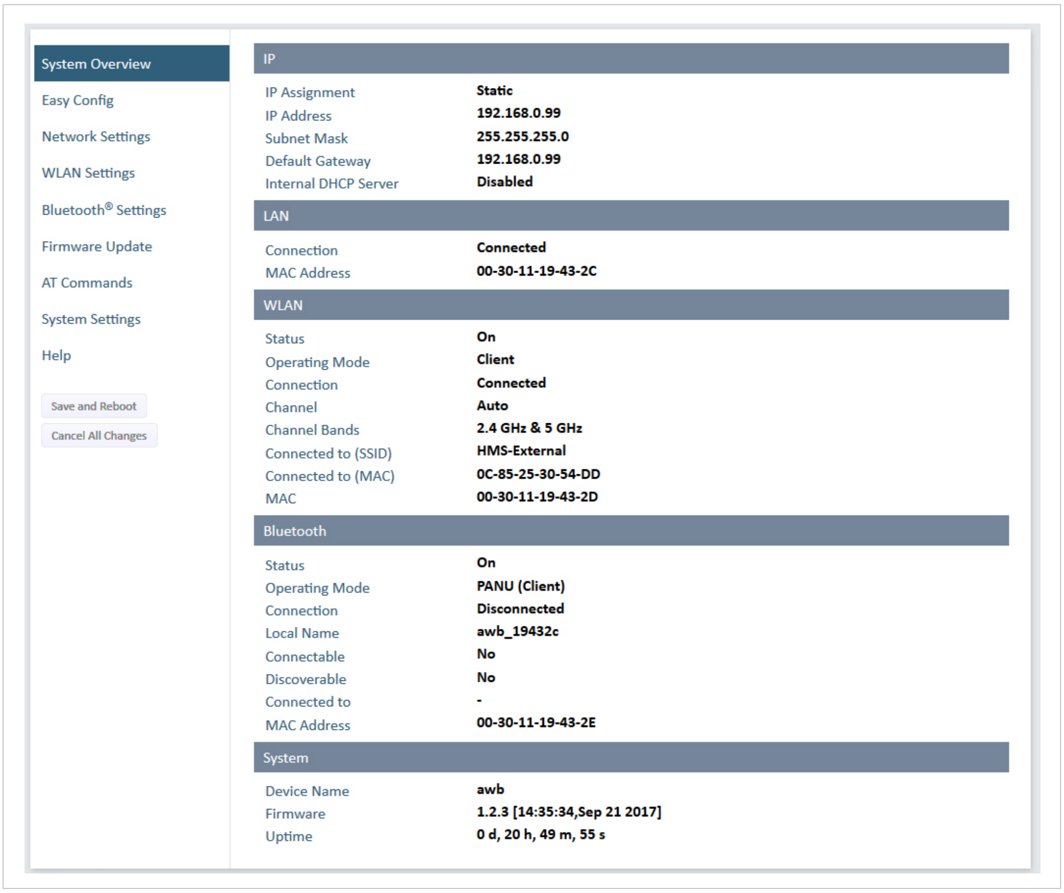
Fig. 4 Web interface

4.2 Web Interface

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

> ! The web interface is designed for the current stable versions of Internet Explorer, Chrome, Firefox and Safari. Other browsers may not support the full functionality of the web interface.

4.2.1 System Overview



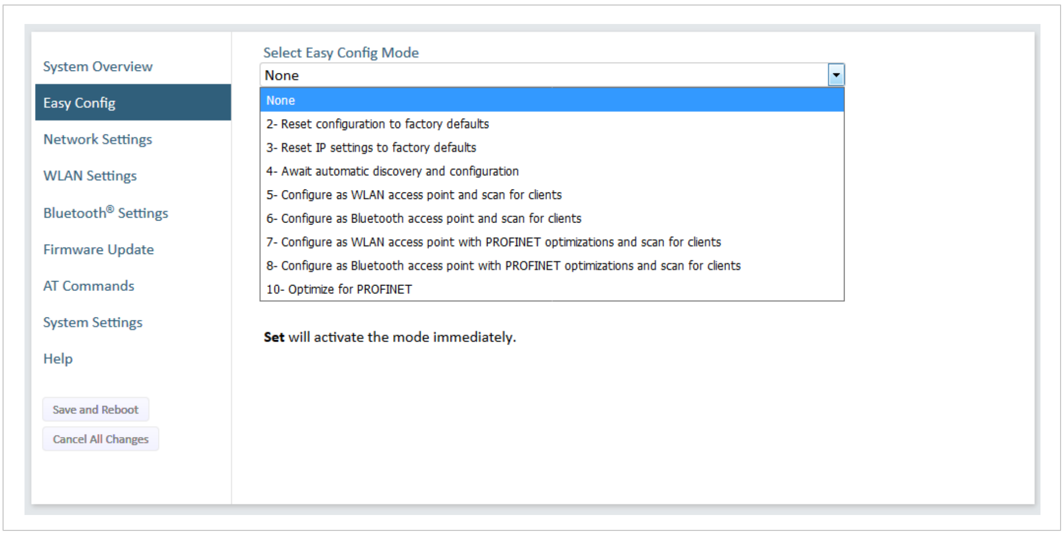
IP	
IP Assignment	Static
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99
Internal DHCP Server	Disabled
LAN	
Connection	Connected
MAC Address	00-30-11-19-43-2C
WLAN	
Status	On
Operating Mode	Client
Connection	Connected
Channel	Auto
Channel Bands	2.4 GHz & 5 GHz
Connected to (SSID)	HMS-External
Connected to (MAC)	0C-85-25-30-54-DD
MAC	00-30-11-19-43-2D
Bluetooth	
Status	On
Operating Mode	PANU (Client)
Connection	Disconnected
Local Name	awb_19432c
Connectable	No
Discoverable	No
Connected to	-
MAC Address	00-30-11-19-43-2E
System	
Device Name	awb
Firmware	1.2.3 [14:35:34,Sep 21 2017]
Uptime	0 d, 20 h, 49 m, 55 s

Fig. 5 System Overview page

The **Save and Reboot** button will become enabled if the unit must be restarted for a parameter change to come into effect.

To revert to the currently active configuration without saving the parameter changes, click on **Cancel All Changes**.

4.2.2 Easy Config


System Overview
Easy Config
Network Settings
WLAN Settings
Bluetooth® Settings
Firmware Update
AT Commands
System Settings
Help
Save and Reboot
Cancel All Changes
Select Easy Config Mode
None
None
2- Reset configuration to factory defaults
3- Reset IP settings to factory defaults
4- Await automatic discovery and configuration
5- Configure as WLAN access point and scan for clients
6- Configure as Bluetooth access point and scan for clients
7- Configure as WLAN access point with PROFINET optimizations and scan for clients
8- Configure as Bluetooth access point with PROFINET optimizations and scan for clients
10- Optimize for PROFINET

Set will activate the mode immediately.

Fig. 6 Easy Config page

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

Easy Config Modes

Mode	Role	Description
2	—	Reset configuration to factory defaults.
3	—	Reset IP settings to factory defaults.
4	Client	Wait for automatic configuration.
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 optimizations to all units.
8	Bluetooth NAP	
10	—	Apply PROFINET optimizations and restart.

Modes 5 – 8 will scan for units in mode 4. 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.

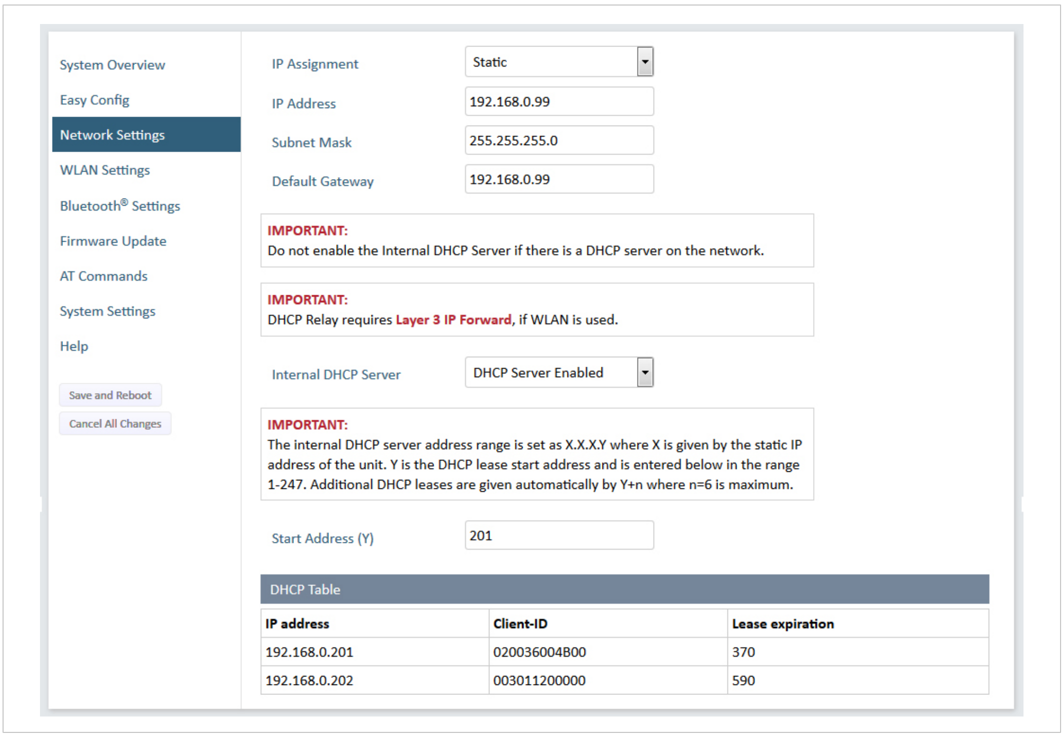
Modes 7 and 8 will additionally apply PROFINET optimization to all the units. PROFINET messages will then have priority over TCP/IP frames.

Mode Timeout

- Modes 5 – 8 will time out after 120 seconds. Apply the mode again to repeat the scan.
- Mode 4 will listen for 120 seconds or until receiving a configuration.

! The IP address of a client may be changed by the configuration from the access point. Active browser sessions could therefore be lost.

4.2.3 Network Settings



IP Assignment: Static

IP Address: 192.168.0.99

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.99

IMPORTANT:
Do not enable the Internal DHCP Server if there is a DHCP server on the network.

IMPORTANT:
DHCP Relay requires Layer 3 IP Forward, if WLAN is used.

Internal DHCP Server: DHCP Server Enabled

IMPORTANT:
The internal DHCP server address range is set as X.X.X.Y where X is given by the static IP address of the unit. Y is the DHCP lease start address and is entered below in the range 1-247. Additional DHCP leases are given automatically by Y+n where n=6 is maximum.

Start Address (Y): 201

DHCP Table

IP address	Client-ID	Lease expiration
192.168.0.201	020036004B00	370
192.168.0.202	003011200000	590

Fig. 7 Network Settings page

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.

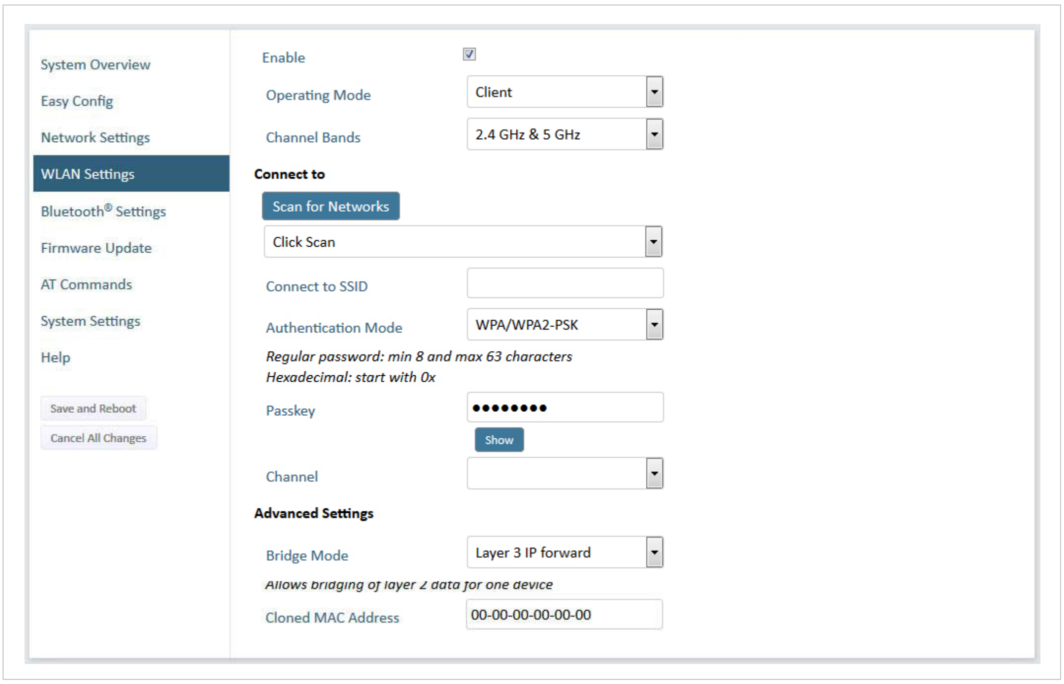
DHCP Server Enabled: Activates an internal DHCP server. This option is only available when IP Assignment is set to Static.
Do not enable this option if there is already a DHCP server on the network!

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.

4.2.4 WLAN Settings – Client Mode



Enable ☑

Operating Mode: Client

Channel Bands: 2.4 GHz & 5 GHz

Connect to

Scan for Networks

Click Scan

Connect to SSID:

Authentication Mode: WPA/WPA2-PSK

Regular password: min 8 and max 63 characters
Hexadecimal: start with 0x

Passkey: ••••••••

Show

Channel:

Advanced Settings

Bridge Mode: Layer 3 IP forward

Allows bridging of layer 2 data for one device

Cloned MAC Address: 00-00-00-00-00-00

Fig. 8 WLAN Settings – Client

Enable Enable/disable the WLAN interface.

Operating Mode Choose operation as WLAN Client or Access Point. If Access Point is selected, additional parameters will be visible.

Channel Bands Choose to scan on only the 2.4 GHz or 5 GHz channel band, or on both (default). The unit must be rebooted to enable the new setting.

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.

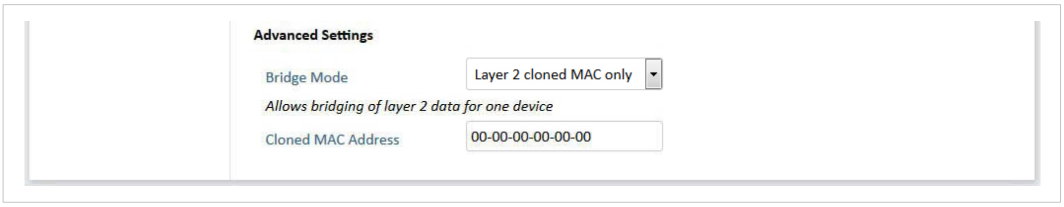
Connect to SSID To connect manually to a network, enter its SSID (network name) here. This can be used if the network does not broadcast its SSID.

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. Which channels are available depend on the **Channel Bands** setting.
Auto = all channels will be scanned (default).



Advanced Settings

Bridge Mode: Layer 2 cloned MAC only

Allows bridging of layer 2 data for one device

Cloned MAC Address: 00-00-00-00-00-00

Fig. 9 WLAN Client – Advanced Settings

Advanced Settings

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 Anybus Wireless Bolt or Wireless Bridge II 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).

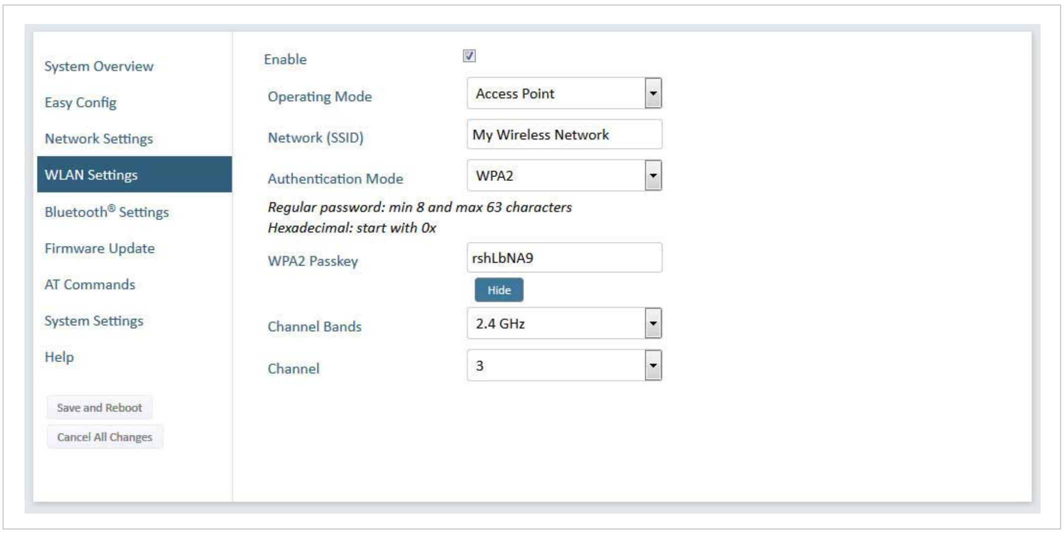
Layer 3 IP forward (default) = IP data from all devices will be bridged over WLAN.

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).

4.2.5 WLAN Settings – Access Point Mode



Enable ☑

Operating Mode: Access Point

Network (SSID): My Wireless Network

Authentication Mode: WPA2

Regular password: min 8 and max 63 characters
Hexadecimal: start with 0x

WPA2 Passkey: rshLbNA9

Channel Bands: 2.4 GHz

Channel: 3

Fig. 10 WLAN Settings – Access Point

The following settings are specific when Access Point mode is selected.

Network (SSID)

Enter an SSID (network name) for the Wireless Bolt.

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.

Password examples

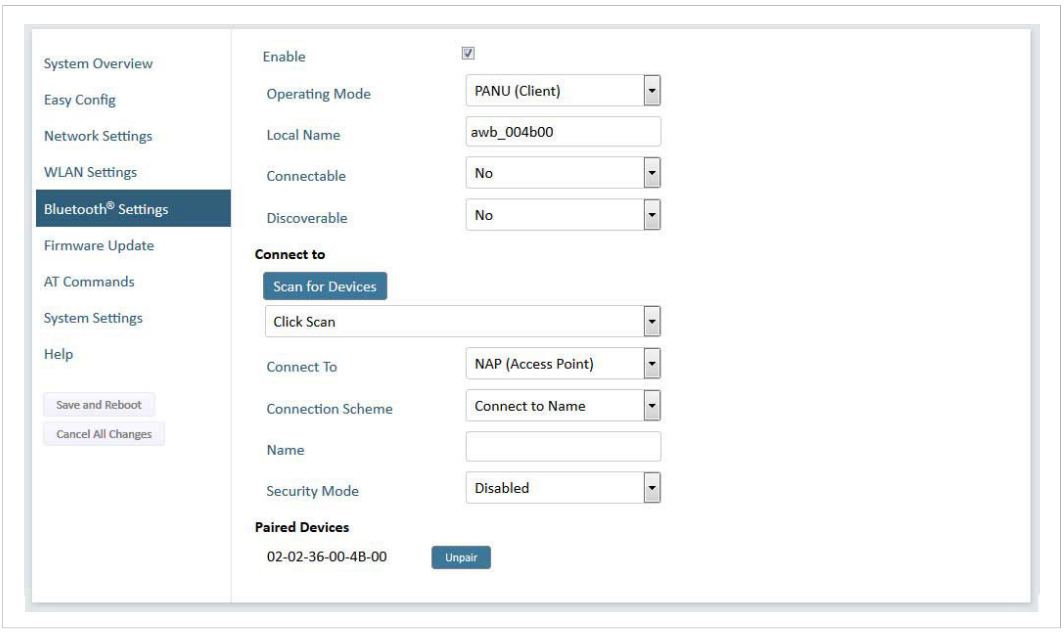
For plain text passwords a combination of upper and lower case letters, numbers, and special characters is recommended.

Example of a strong plain text password:
`uS78_xpa&43`

Example of hexadecimal password:
`0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f`

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

4.2.6 Bluetooth Settings – General



Enable ☑

Operating Mode: PANU (Client)

Local Name: awb_004b00

Connectable: No

Discoverable: No

Connect to

Connect To: NAP (Access Point)

Connection Scheme: Connect to Name

Name:

Security Mode: Disabled

Paired Devices

02-02-36-00-4B-00

Fig. 11 Bluetooth Settings

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.

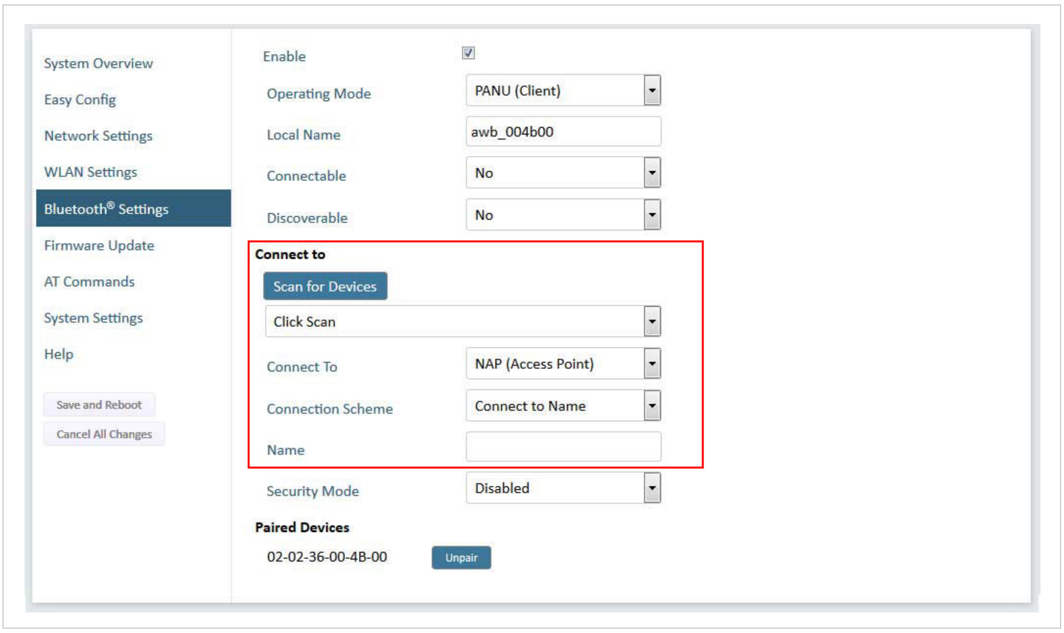
Security Mode
Disabled = No encryption or authentication.

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.

4.2.7 Bluetooth Settings – PANU Mode



Enable ☑

Operating Mode: PANU (Client)

Local Name: awb_004b00

Connectable: No

Discoverable: No

Connect to

Click Scan

Connect To: NAP (Access Point)

Connection Scheme: Connect to Name

Name:

Security Mode: Disabled

Paired Devices

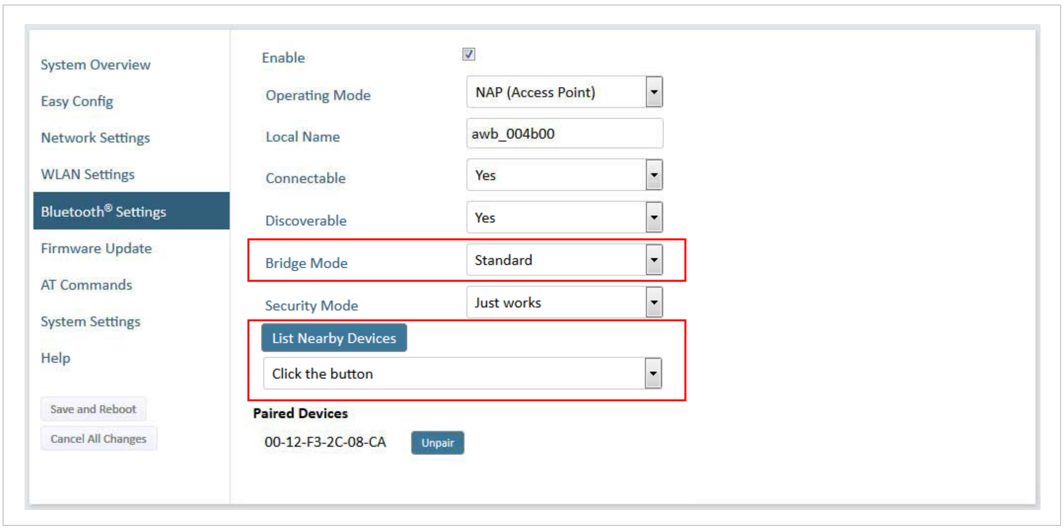
02-02-36-00-4B-00

Fig. 12 Bluetooth Settings – PANU

PANU mode only

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 or name when connecting manually.
Name	Name of the Bluetooth device to connect to.

4.2.8 Bluetooth Settings – NAP Mode



Enable ☑

Operating Mode: NAP (Access Point)

Local Name: awb_004b00

Connectable: Yes

Discoverable: Yes

Bridge Mode: Standard

Security Mode: Just works

Click the button

Paired Devices

00-12-F3-2C-08-CA

Fig. 13 Bluetooth settings – NAP

NAP mode only

Bridge Mode

Standard = Default mode.

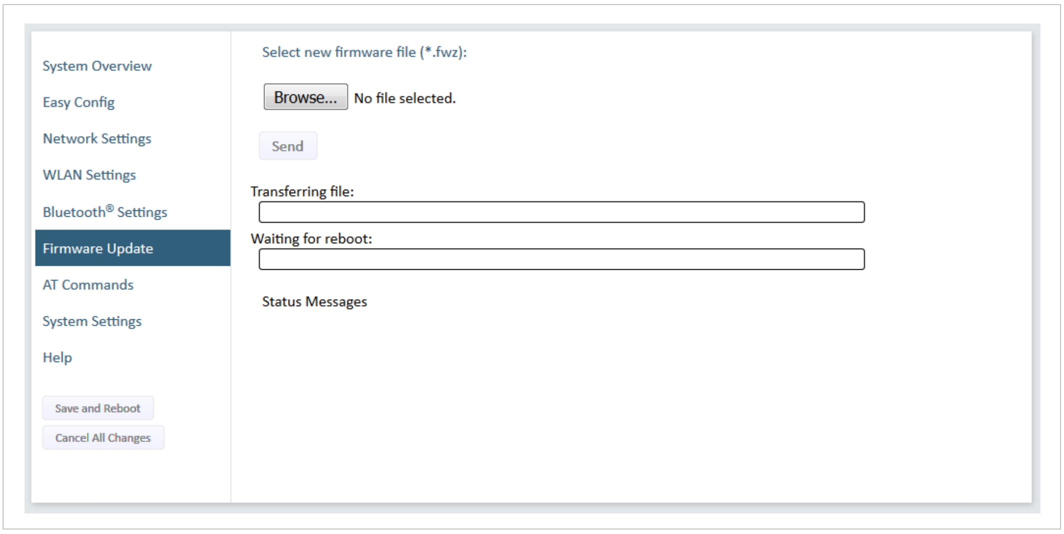
Layer 3 IP forward = IP data will be bridged over Bluetooth.

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.

4.2.9 Firmware Update



Select new firmware file (*.fwz):

No file selected.

Transferring file:

Waiting for reboot:

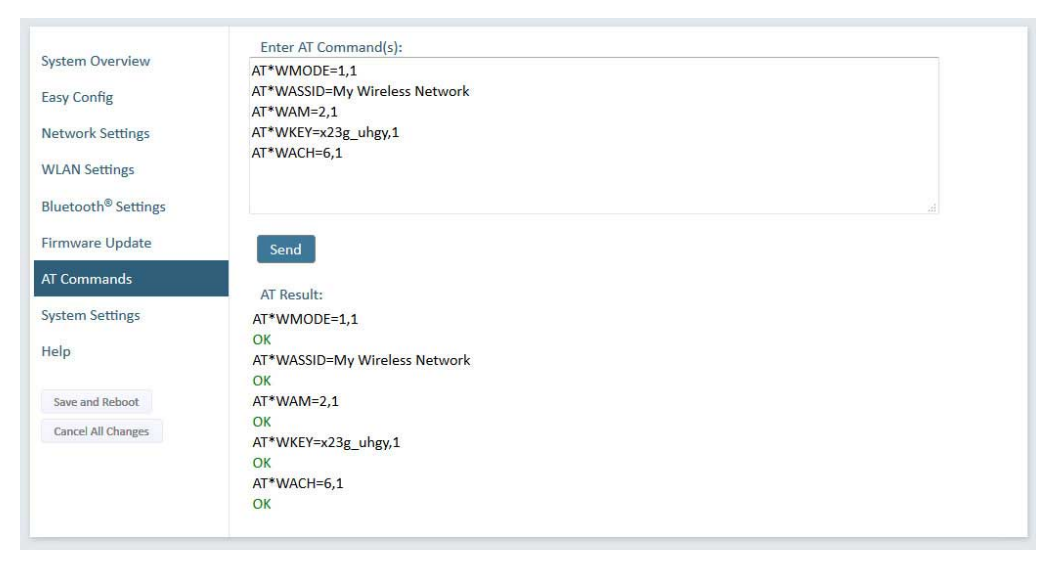
Status Messages

Fig. 14 Firmware Update

Click on **Browse** to select a firmware file, then click on **Send** to download it to the unit.

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

4.2.10 AT Commands



```
AT*WMODE=1,1
AT*WASSID=My Wireless Network
AT*WAM=2,1
AT*WKEY=x23g_uhgy,1
AT*WACH=6,1
```

```
AT*WMODE=1,1
OK
AT*WASSID=My Wireless Network
OK
AT*WAM=2,1
OK
AT*WKEY=x23g_uhgy,1
OK
AT*WACH=6,1
OK
```

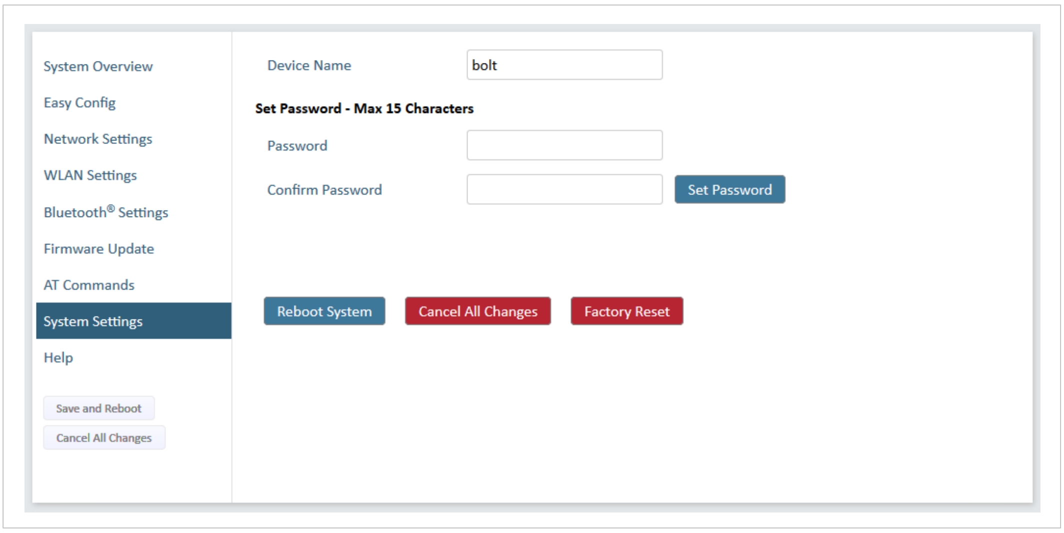
Fig. 15 AT Commands

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.

See the *AT Commands Reference Guide* for a complete list of supported AT commands.

4.2.11 System Settings



Device Name: bolt

Set Password - Max 15 Characters

Password

Confirm Password

Fig. 16 System Settings

Device Name Enter a descriptive name for the unit.

Password Enter a password for accessing the web interface.

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.

! Setting a secure password for the unit is strongly recommended.

4.3 Factory Restore

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

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

Default Network Settings

IP Assignment	Static
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99

Default WLAN Settings

Operating Mode	Client
Channel Bands	2.4 GHz & 5 GHz
Authentication Mode	WPA/WPA2–PSK
Channel	Auto
Bridge Mode	Layer 3 IP forward

Default Bluetooth Settings

Operating Mode	PANU (Client)
Local Name	[generated from MAC address]
Security Mode	Just works

Default System Settings

Password	[empty]

> ! Setting a secure password for the unit is strongly recommended.

4.4 RESET Button

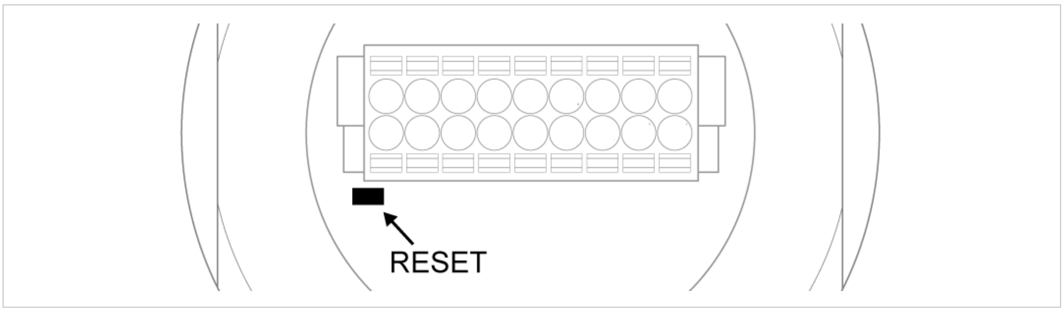


Fig. 17

The **RESET** button is located on the bottom of the unit next to the connector.

- ► Press and hold the button for >10 seconds and then release it to reset to the factory default settings (when the unit is powered on).
- ► Press and hold the button during startup to enter *Recovery Mode*.

Recovery Mode

If the web interface cannot be accessed, the unit can be reset by starting in Recovery Mode and reinstalling the firmware using Anybus Firmware Manager II, which can be downloaded from www.anybus.com/support.

> ! Firmware updates should normally be carried out through the web interface. Recovery Mode should only be used if the unit is unresponsive and the web interface cannot be accessed.

This page intentionally left blank

A Configuration Examples

The following examples require that you have installed the Anybus Wireless Bolt and that you understand how to access and use the web interface.

- All the examples start out from the factory default settings.
- Settings not mentioned in the examples should be left at their default values.
- The computer accessing the web interface of a Wireless Bolt must be connected to its Ethernet interface and have an IP address within the same subnet.

A.1 Ethernet Bridge via WLAN or Bluetooth (Easy Config)

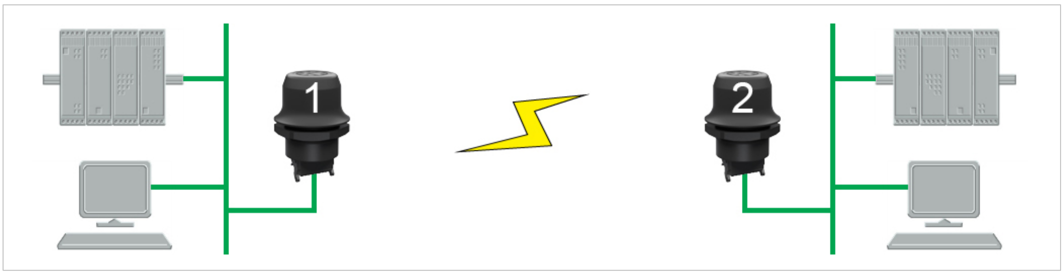
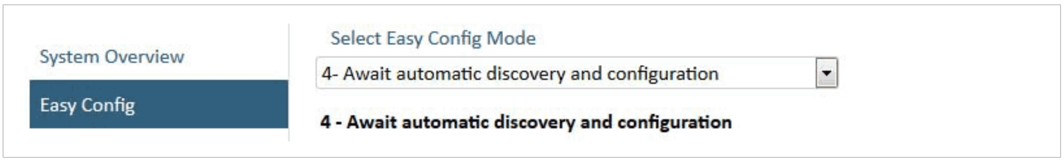


Fig. 18 Ethernet bridge

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.



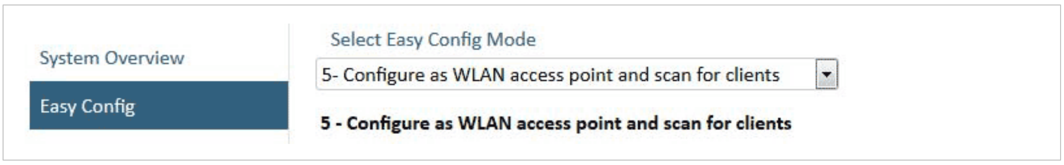
Select Easy Config Mode

4- Await automatic discovery and configuration

4 - Await automatic discovery and configuration

Fig. 19 Easy Config Mode 4

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



Select Easy Config Mode

5- Configure as WLAN access point and scan for clients

5 - Configure as WLAN access point and scan for clients

Fig. 20 Easy Config Mode 5

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

Adding More Devices

Up to 6 additional clients can be added to the access point by repeating the procedure. Each new client will be assigned the next free IP address within the current subnet.

A.2 PROFINET networking via Bluetooth (Easy Config)

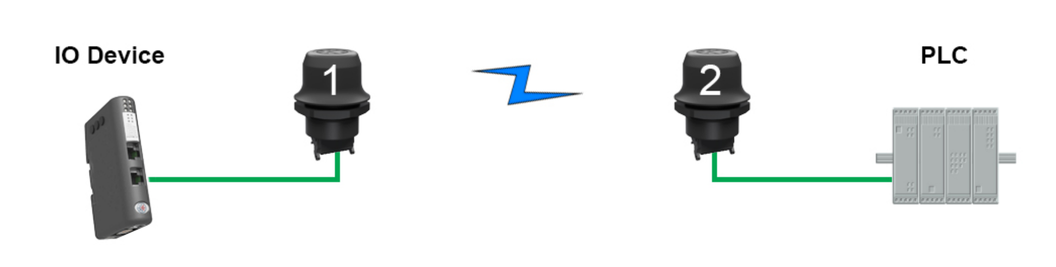


Fig. 21 PROFINET wireless network

This example describes how to connect a PROFINET IO device and a PROFINET PLC via Bluetooth using two Wireless Bolts and Easy Config.

Configuration

Please refer to the documentation for the IO device and the PLC regarding how to configure PROFINET communication.

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

   This unit will now be discoverable and open for automatic configuration.
4. Set Wireless Bolt 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 to the access point by repeating the procedure. Each new client will be assigned the next free IP address within the current subnet.

> **!** The IO cycle update time for each IO device must be set to ≥ 64 ms.

A.3 EtherNet/IP networking via Bluetooth (Easy Config)

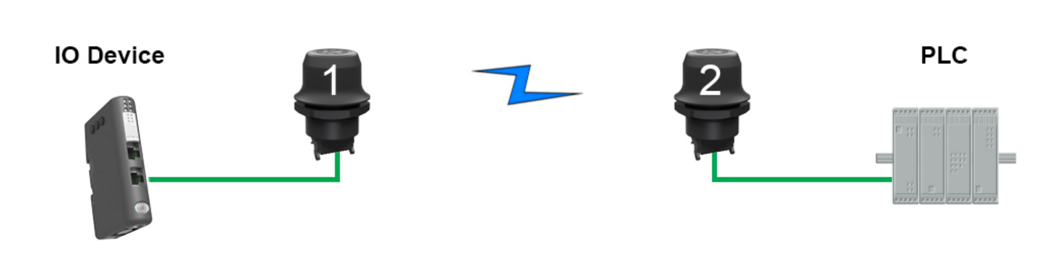


Fig. 22 EtherNet/IP wireless network

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

Configuration

Please refer to the documentation for the IO device and PLC regarding how to configure EtherNet/IP communication.

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

   This unit will now be discoverable and open for automatic configuration.
4. Set Wireless Bolt 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 to the access point by repeating the procedure. Each new client will be assigned the next free IP address within the current subnet.

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

A.4 Connecting an Ethernet network to an existing WLAN

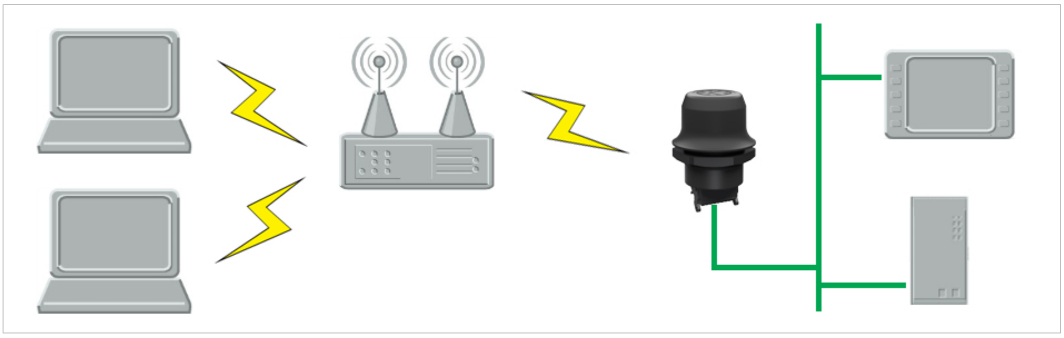


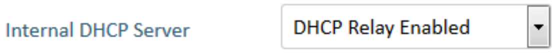
Fig. 23 **Connecting to a WLAN**

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 Bolt 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**.



Internal DHCP Server 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.

> **!** 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.

A.5 Adding wireless connectivity to a single Ethernet node

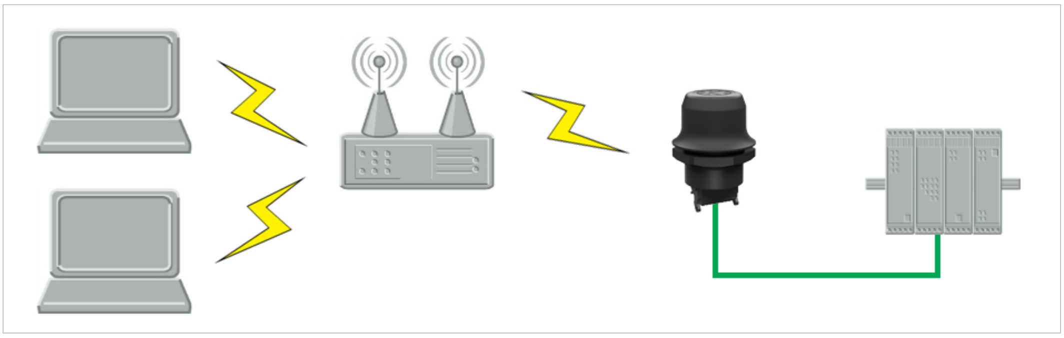


Fig. 24 Adding WLAN connectivity

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

Only a single Ethernet node can communicate via a third-party WLAN access point in this setup.

Configuration

1. Reset the Wireless Bolt 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 Bolt will now function as a WLAN interface for the PLC using the MAC address of its Ethernet interface.

A.6 Accessing a PLC from a handheld device over WLAN

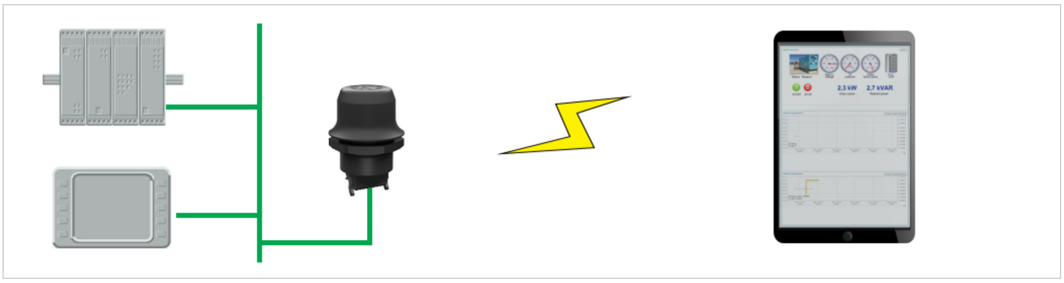


Fig. 25 Accessing a PLC from a handheld device using WLAN

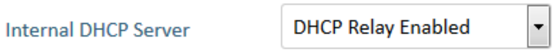
This example describes how to use a Wireless Bolt to allow access to the web interface of a PLC or other device on a wired network from a tablet or smartphone that uses dynamic IP addressing (DHCP). The Wireless Bolt will operate as a WLAN access point.

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

Configuration

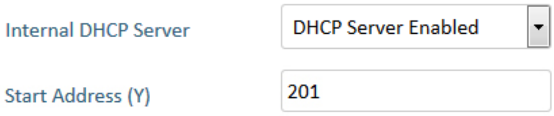
1. Reset the Wireless Bolt to the factory default settings.
2. In **Network Settings**, configure the IP settings as required by the wired network.

   If the network uses DHCP, set **Internal DHCP Server** to **DHCP Relay Enabled**.

   Internal DHCP Server: DHCP Relay Enabled

   If the network has no active DHCP server, set **Internal DHCP Server** to **DHCP Server Enabled**. The Wireless Bolt will now act as DHCP server on the network.

   Internal DHCP Server: DHCP Server Enabled

   Start Address (Y): 201

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

   See also *Network Settings, p. 14* for an explanation of the internal DHCP server.

3. In **WLAN Settings**, set **Operating Mode** to **Access Point**.
4. Enter a new unique **SSID** for the new wireless network.
5. Set **Authentication Mode** to **WPA2** end 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 Bolt on your handheld device and access the PLC by by entering its IP address in a browser.

B 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.

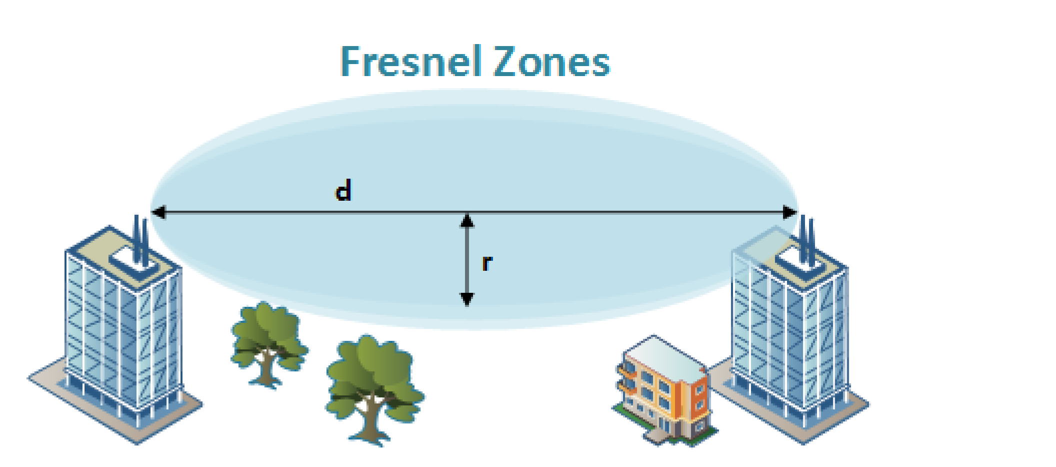


Fig. 26 Fresnel zones

Area to keep clear of obstacles (first Fresnel zone)

Distance (d)	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 range may also need to be limited by reducing the transmission power. For determining the optimal configuration and placement of wireless devices it is therefore recommended to use a wireless signal analysis tool.

C Technical Data

C.1 Technical Specifications

Order code	AWB2000	AWB2010	AWB2020
Wired Interface type	Ethernet	Serial RS-232/485 + Ethernet	CAN + Ethernet
Wireless antenna	Internal		
Maximum range	100 m (WLAN and Bluetooth)		
Communication	See Anybus Wireless Bolt Datasheet		
Dimensions	Height: 70 mm (95 mm incl. connector, 41 mm outside) Diameter: 70 mm		
Weight	81 g		
Operating temperature	-40 to +65 °C		
Storage temperature	-40 to +85 °C		
Humidity	EN 600068-2-78: Damp heat, +40 °C, 93 % humidity for 4 days		
Housing	Plastic		
Protection class	IP67 / TYPE 4X for top part (outside of host) IP21 for bottom part (inside of host)		
Mounting	M50 screw and nut (50.5 mm hole required)		
Connector	Included plug connector		
Power supply	9–30 VDC (-5 % +20 %) Cranking 12 V (ISO 7637-2:2011 pulse 4) Reverse polarity protection		
Power consumption	0.7 W (idle) – 1.7 W (max)		
Certifications	See www.anybus.com/support and the compliance information appended to the User Manual.		

C.2 Internal Antenna Characteristics

The following radiation diagrams show the characteristics of the internal 2.4 GHz antenna as measured under laboratory test conditions. The diagrams should be regarded as a general guide for finding the optimal placement and orientation of the units.

2.4 GHz Antenna Characteristics

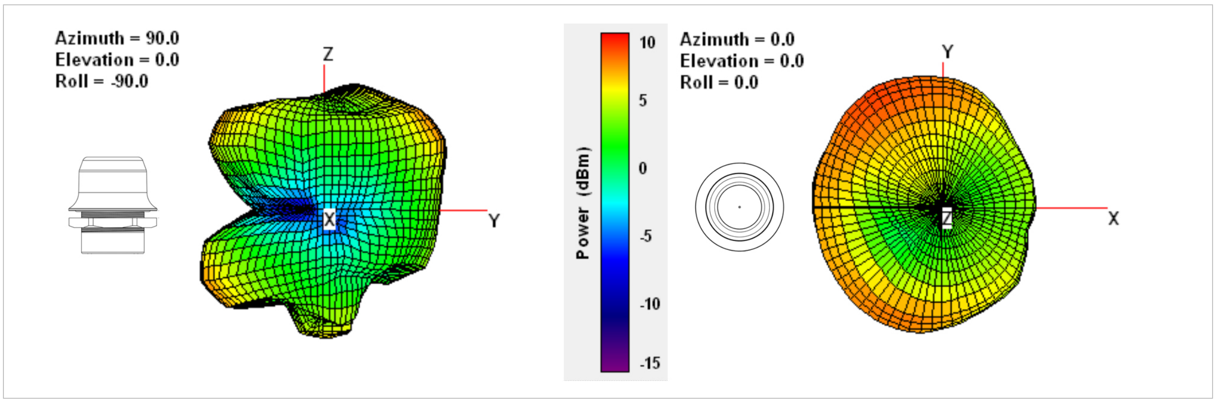


Fig. 27 2.4 GHz antenna gain and directivity in horizontal and vertical planes

This page intentionally left blank

Box 4126
300 04 Halmstad, Sweden

info@hms.se