

# Anybus<sup>®</sup> Wireless Bolt Serial<sup>™</sup>

## USER MANUAL

SCM-1202-143 1.11 en-US ENGLISH



---

# Important User Information

## Disclaimer

The information in this document is for informational purposes only. Please inform HMS Networks of any inaccuracies or omissions found in this document. HMS Networks disclaims any responsibility or liability for any errors that may appear in this document.

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the 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.

---

# Table of Contents

Page

<b>1</b>	<b>Preface .....</b>	<b>3</b>
1.1	About This Document .....	3
1.2	Document Conventions .....	3
1.3	Trademarks.....	3
<b>2</b>	<b>Safety .....</b>	<b>4</b>
2.1	General Safety Instructions .....	4
2.2	Intended Use.....	4
<b>3</b>	<b>Preparation.....</b>	<b>5</b>
3.1	General Information .....	5
3.2	When to Use Bluetooth and WLAN .....	5
<b>4</b>	<b>Installation.....</b>	<b>6</b>
4.1	Mechanical Installation .....	6
4.2	Connector.....	7
4.3	Cabling.....	8
4.4	Digital Input .....	8
4.5	RESET Button .....	9
<b>5</b>	<b>Configuration.....</b>	<b>10</b>
5.1	Web Interface .....	11
5.2	Use Cases .....	29
5.3	Set Up a Wireless Infrastructure .....	33
5.4	Factory Restore .....	36
<b>6</b>	<b>Technical Data .....</b>	<b>37</b>
6.1	Technical Specifications.....	37
<b>A</b>	<b>RS232/RS485 Electrical Connection .....</b>	<b>39</b>
A.1	RS485 Typical Connection .....	39
A.2	RS232 Typical Connection.....	39
<b>B</b>	<b>Wireless Technology Basics .....</b>	<b>40</b>
<b>C</b>	<b>Radio Antenna Patterns.....</b>	<b>41</b>
C.1	Azimuth (Horizontal) View .....	41
C.2	Vertical Views.....	42
C.3	Throughput Diagram.....	43

**This page intentionally left blank**

# 1 Preface

## 1.1 About This Document

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

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit [www.anybus.com/support](http://www.anybus.com/support).

## 1.2 Document Conventions

Numbered lists indicate tasks that should be carried out in sequence:

1. First do this
2. Then do this

Bulleted lists are used for:

- Tasks that can be carried out in any order
- Itemized information
- ▶ An action
  - and a result

**User interaction elements** (buttons etc.) are indicated with bold text.

```
Program code and script examples
```

Cross-reference within this document: [Document Conventions, p. 3](#)

External link (URL): [www.hms-networks.com](http://www.hms-networks.com)



### **WARNING**

Instruction that must be followed to avoid a risk of death or serious injury.



### **Caution**

Instruction that must be followed to avoid a risk of personal injury.



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



*Additional information which may facilitate installation and/or operation.*

## 1.3 Trademarks

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

## 2 Safety

### 2.1 General Safety Instructions

**Caution**

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

**Caution**

Minimum temperature rating of the cable to be connected to the field wiring terminals, 90 °C.

**Caution**

Use copper wire only for field wiring terminals.



This equipment 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 used if a shielded Ethernet cable is used, in order to meet emission requirements.



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

### 2.2 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.

## 3 Preparation

### 3.1 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.

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. 40](#).

### 3.2 When to Use Bluetooth and WLAN

#### Use Bluetooth when:

- The wireless link has an Bolt Serial at both ends.
- An interruption-free connection is more important than data throughput speed.
- Interference robustness is important – e.g. in an industrial environment.

#### 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.

## 4 Installation

### 4.1 Mechanical Installation

The device is intended to be mounted 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.

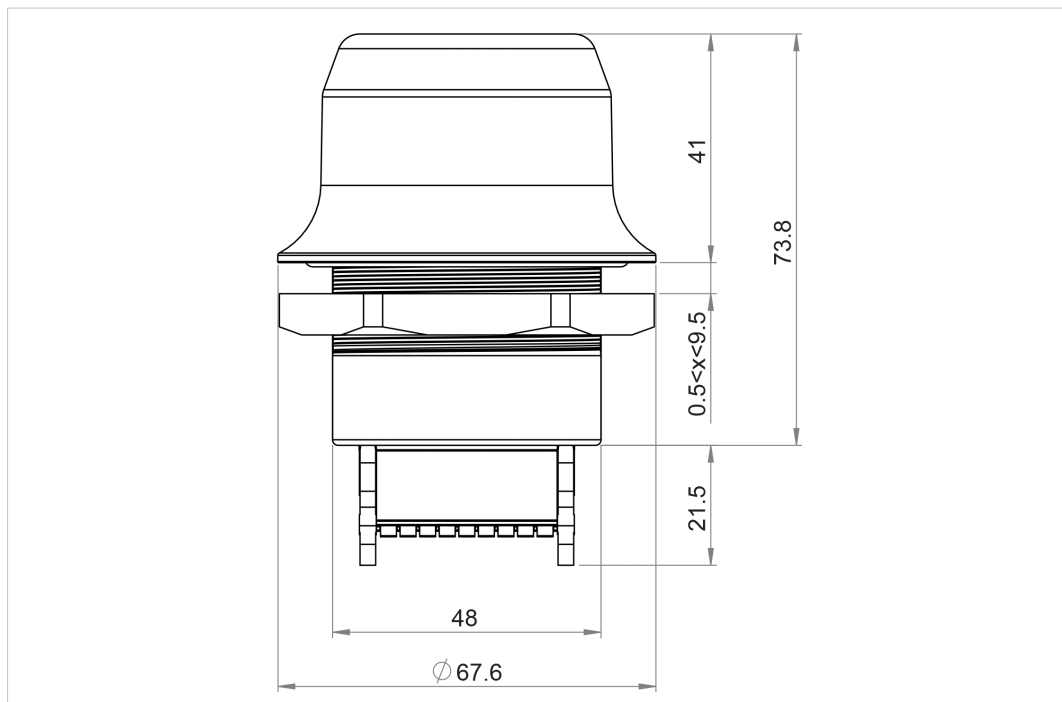
**Tightening torque:** 5 Nm  $\pm$ 10 %.



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



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



**Fig. 1** Installation drawing

All measurements are in mm.



## 4.2 Connector

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

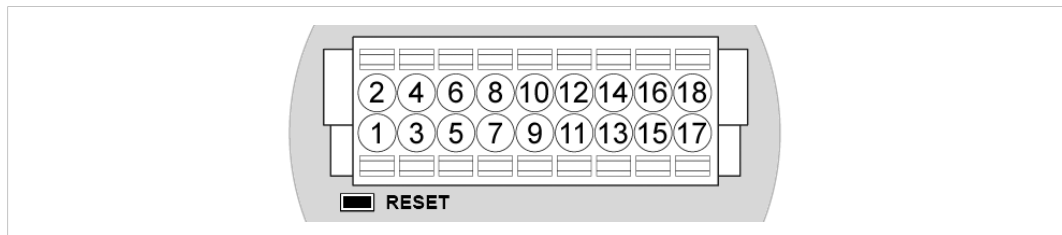


Fig. 2 Connector

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



*The Ethernet interface is intended for configuration purposes only. Bolt Serial is not designed for permanent Ethernet communication.*



*A and B marking differs between different devices, in this product A is TX+/RX+ or D+ and B is TX-/RX- or D-.*

For information about the correct connection type and termination, refer to [RS232/RS485 Electrical Connection, p. 39](#).

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 and CAN: 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      Not used for Bolt Serial.
14	RS232_CTS	RS-232 Clear To Send      Not used for Bolt Serial.
15	ISO_5V	Isolated 5 V for serial interface
16	RS232_GND/RS485_GND	Isolated Ground for Serial interface
17	CAN_L	CAN Low Not used for Bolt Serial.
18	CAN_H	CAN High Not used for Bolt Serial.

### Note:

- Use RS-485 when connecting multiple devices to a Bolt Serial.
- 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.
- RS485 Common signal reference ground (SC) is the RS485\_GND pin.

### 4.3 Cabling



*When using **Easy Config Modes**, the Bolt Serial that is to be configured as a Client does not need to be connected to the Ethernet wires. Only power and Serial wiring are used.*

To make an Ethernet, Serial and power connector cable for Anybus Wireless Bolt Serial:

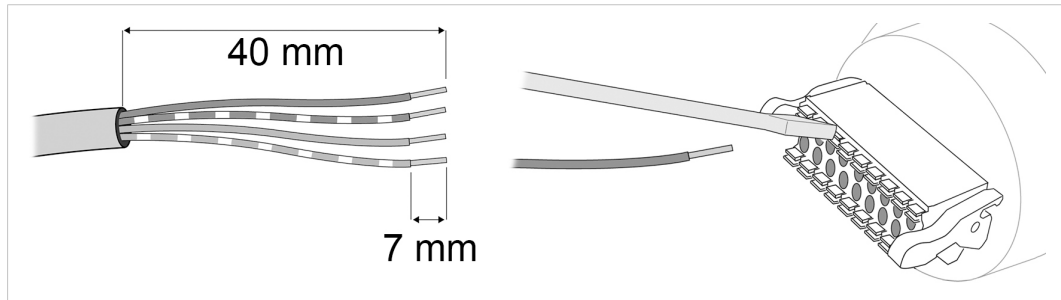


Fig. 3



*To maintain signal integrity, low emission and high immunity to EMI, untwist the twisted pair cable as little as possible.*

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, from the orange, orange/white, green and green/white wires.  
The shield and the other wires are not 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. 7](#).
5. Connect the wires from the Serial device to the connector in the same way as the Ethernet wiring.
6. Connect the wires from the power supply to the connector in the same way as the Ethernet wiring. **Make sure that polarity is not reversed.**

### 4.4 Digital Input

The digital input can be used to control roaming between Bluetooth access points (NAP). For more information, refer to the AT Reference Guide at [www.anybus.com/support](http://www.anybus.com/support).



If voltage is applied to the digital input for more than 10 seconds the unit will be reset to factory defaults.

## 4.5 RESET Button

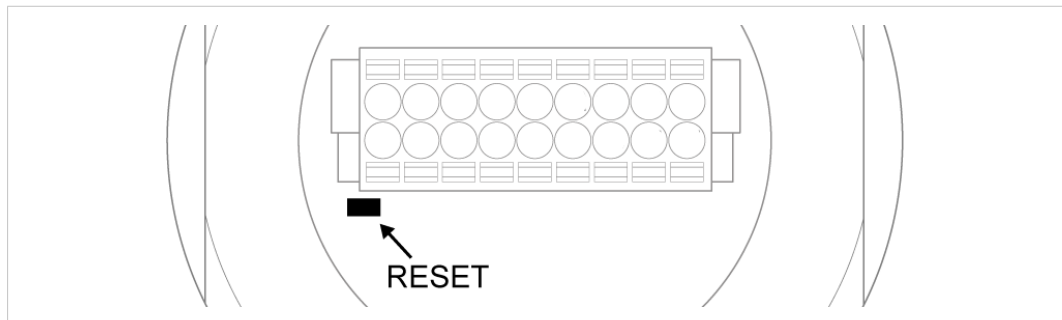


Fig. 4 RESET button

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.

### 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](http://www.anybus.com/support).

To enter Recovery Mode, press and hold **RESET** during startup.



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.

## 5 Configuration

Anybus Wireless Bolt Serial 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 Bolt Serial. The default address is **192.168.0.99**. The computer accessing the web interface must be in the same IP subnet as the Bolt Serial.



Fig. 5 Web interface

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 Reference Guide* or the **Help** page in the web interface for more information.

## 5.1 Web Interface

### 5.1.1 System Overview



Fig. 6 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.

<b>Save and Reboot</b>	This button will be enabled if the unit must be restarted to apply a change.
<b>Cancel All Changes</b>	Resets parameter changes that have not been applied.

## 5.1.2 Easy Config

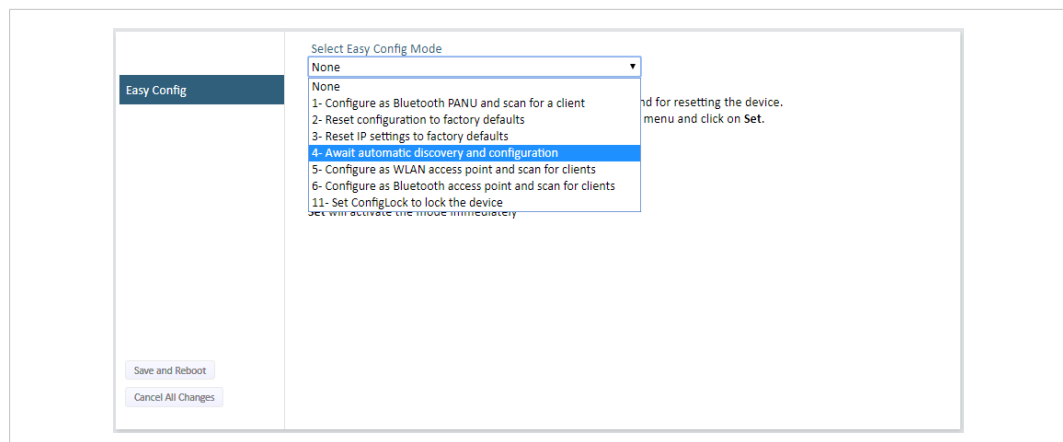
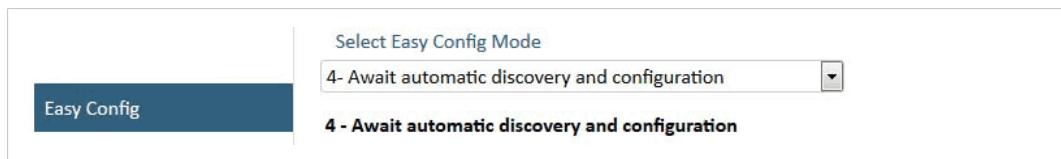


Fig. 7 Easy Config page

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

Easy Config Modes		
EC	Role	Description
1	Bluetooth PANU	Configure as Bluetooth client and scan for another client (PANU–PANU). Recommended setting for Bluetooth point-to-point communication. Listens for 40 seconds or until a configuration is established.  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.
2	–	Reset configuration to factory defaults.
3	–	Reset IP settings to factory defaults.
4	Client	Wait for automatic configuration. Listens for 120 seconds or until receiving a configuration. Configure units in mode 4 as clients. When mode 4 is used with mode 1, 5 or 6, Serial Settings TCP Mode Client is activated automatically.
5	WLAN AP	Restart as access point and connect clients. Mode 5 and 6 will time out after 120 seconds.
6	Bluetooth NAP	Modes 5 and 6 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.
11	(any)	Activate ConfigLock mode. Mode 7 will be added to the configuration without changing any other settings.  Mode 7 locks the unit in ConfigLock 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 RESETMODE button.

### Default Easy Config Mode

The screenshot shows a web interface for selecting an Easy Config Mode. On the left, there is a blue button labeled "Easy Config". To its right, there is a section titled "Select Easy Config Mode" which contains a dropdown menu. The dropdown menu is currently open, showing the selected option "4- Await automatic discovery and configuration". Below the dropdown, the text "4 - Await automatic discovery and configuration" is displayed in bold.

**Fig. 8** The default mode is Easy Config Mode 4

By default Wireless Bolt and Bridge starts in **Easy Config Mode 4**.

Configuration of Wireless Bolt and Bridge Clients can be performed wirelessly, via a PC connected to the Wireless Bolt or Bridge Access Point.

After factory reset, Wireless Bolt will by default start in Easy Config Mode 4, if there is no Ethernet connection.

When connection is established via the wireless interface, the Wireless Bolt or Bridge Client does not need to be connected with an Ethernet cable during configuration.

### 5.1.3 Network Settings

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

DHCP Interfaces: Wired Ethernet (selected), All, Wireless Interfaces

**IMPORTANT:**  
The internal DHCP server address 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

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

Save and Reboot

Cancel All Changes

Fig. 9 Network Settings page

<b>IP Assignment</b>	Select static or dynamic IP addressing (DHCP)
<b>IP Address</b>	Static IP address for the unit The browser should automatically be redirected to the new address after clicking on <b>Save and Reboot</b> (not supported by all browsers).
<b>Subnet Mask</b>	Subnet mask when using static IP
<b>Default Gateway</b>	Default gateway when using static IP
<b>Internal DHCP Server</b>	<p><b>Disabled:</b> No internal DHCP functionality</p> <p><b>DHCP Relay Enabled:</b> 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.</p> <p><b>DHCP Server Enabled:</b> Activates an internal DHCP server. This option is only available when IP Assignment is set to Static.</p> <p>To avoid IP address conflict if a DHCP server is already active on the network, use the <b>DHCP Interfaces</b> setting to limit the internal DHCP server to the correct interface.</p>



**DHCP Interfaces**

The **DHCP Interfaces** function is available when **Internal DHCP Server > DHCP Server Enabled** is selected.

**All:** By default, the DHCP Interfaces function is set to use all interfaces.

**Wired Ethernet:** The internal DHCP server only listens for clients on the wired Ethernet interface.

**Wireless Interfaces:** The internal DHCP server listens for clients on all supported wireless interfaces (WLAN/Bluetooth).

**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.

5.1.4 WLAN Settings - Client

WLAN Settings

Enable☒

Operating Mode

Client

Channel Bands

2.4 GHz 1, 6, 11

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

Advanced Settings

Bridge Mode

Layer 2 tunnel

Save and Reboot

Cancel All Changes

Fig. 10 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 settings will be available.
Channel Bands	Choose to scan only the 2.4 GHz or 5 GHz channel band, or both (default).
<div><div>i</div><div>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.</div></div>	
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. <b>Open</b> = 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).

### 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.

When using Layer 3 IP forward in an enterprise network, such as a Cisco Wireless LAN Controller, the connectivity may be reduced.

The cause may be:

- Multiple devices sharing a single wireless interface is not typically supported without special configuration.
- The network cannot enforce a 1-to-1 mapping of IP to MAC addresses and must allow propagation of broadcasted ARP messages over the wireless segment in order to route traffic to the bridged devices.

If this for security or performance reasons is not acceptable, a setup with a single Ethernet node connected to the Wireless Bridge is recommended.

#### Cloned MAC Address

The MAC address to use with **Layer 2 cloned MAC only** (see above).

#### Cloned IP Address

The IP address to use with **Layer 2 cloned MAC only** (see above).

### WLAN Roaming

Anybus Wireless Bolt Serial 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 *AT Commands Reference Guide* or 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. Anybus Wireless Bolt Serial 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 *AT Commands Reference Guide* or the **Help** page in the web interface for more information about how to use AT commands.

**Regulatory domains and WLAN channels**

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

### 5.1.5 WLAN Settings - Access Point

Fig. 11 WLAN Settings - Access Point

The following settings are specific for Access Point mode:

- |                               |  |
|-------------------------------|--|
| <b>Network (SSID)</b>         | Enter an SSID (network name) for the Bolt Serial.<br><br>If this entry is left blank, the unit will generate an SSID which includes the last 6 characters of the MAC ID.   |
| <b>Authentication Mode</b>    | Select the authentication/encryption mode to use for the access point.<br><br><b>Open</b> = No encryption or authentication<br><b>WPA2</b> = WPA2 PSK authentication with AES/CCMP encryption  |
| <b>WPA2 Passkey</b>           | Enter a string in plain text or hexadecimal format to use for authentication.<br><br>Regular (plain text) passwords must be between 8 and 63 characters.<br>All characters in the ASCII printable range (32–126) are allowed, except " (double quote) , (comma) and \ (backslash).<br><br>Hexadecimal passwords must start with 0x and be <b>exactly</b> 64 characters.<br>See also the example passwords below. |
| <b>Channel Bands, Channel</b> | Select the WLAN channel band and channel to use for the access point.<br><br>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:

uS78\_xpa&43

Example of hexadecimal password:

0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f



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

## 5.1.6 Bluetooth Settings – General

Fig. 12 Bluetooth Settings

<b>Enable</b>	Enable/disable the Bluetooth interface.
<b>Operating Mode</b>	<p><b>PANU (Client)</b> = 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.</p> <p><b>NAP (Access Point)</b> = The unit will operate as a Bluetooth Network Access Point. It can connect to up to 7 Bluetooth PANU devices.</p>
<b>Local Name</b>	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.
<b>Connectable</b>	Enable to make the unit accept connections initiated by other Bluetooth devices.
<b>Discoverable</b>	Enable to make the unit visible to other Bluetooth devices.
<b>Security Mode</b>	<p><b>Disabled</b> = No encryption or authentication.</p> <p><b>PIN</b> = 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.</p> <p><b>Just Works</b> = Encrypted connection without PIN code.</p>
<b>Paired Devices</b>	Lists the currently connected Bluetooth devices.

### 5.1.7 Bluetooth Settings – PANU Mode

The screenshot shows the 'Bluetooth Settings – PANU Mode' configuration window. On the left is a sidebar with 'Bluetooth Settings' highlighted. The main panel contains the following settings:

- Enable:** Checked.
- Operating Mode:** PANU (Client) (dropdown).
- Local Name:** bolt\_32b389 (text input).
- Connectable:** No (dropdown).
- Discoverable:** No (dropdown).
- Connect to (highlighted in red):**
  - Scan for Devices:** A button.
  - Click Scan:** A dropdown menu.
  - Connect To:** NAP (Access Point) (dropdown).
  - Connection Scheme:** Connect to Name (dropdown).
  - Name:** An empty text input field.
- Security Mode:** Just works (dropdown).
- Paired Devices:** A section header for a list of devices.

At the bottom left of the main panel are two buttons: 'Save and Reboot' and 'Cancel All Changes'.

Fig. 13 Bluetooth Settings – PANU

#### PANU mode only

<b>Scan for Devices</b>	Scans the network for discoverable Bluetooth devices. To connect to a device, select it from the dropdown menu when the scan has completed.
<b>Connect To</b>	Used when connecting manually to a NAP or PANU device.
<b>Connection Scheme</b>	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.
<b>MAC/Name</b>	MAC address or Name of the Bluetooth device to connect to.

### 5.1.8 Bluetooth Settings – NAP Mode

The screenshot displays the 'Bluetooth Settings – NAP Mode' configuration window. On the left, a sidebar shows 'Bluetooth Settings' as the active tab. The main configuration area includes the following options:

- Enable:** A checked checkbox.
- Operating Mode:** A dropdown menu set to 'NAP (Access Point)'.
- Local Name:** A text field containing 'bolt\_32b389'.
- Connectable:** A dropdown menu set to 'Yes'.
- Discoverable:** A dropdown menu set to 'Yes'.
- Bridge Mode:** A dropdown menu set to 'Standard', which is highlighted with a red rectangular box.
- Security Mode:** A dropdown menu set to 'Just works'.
- List Nearby Devices:** A button that is also highlighted with a red rectangular box.
- Click the button:** A dropdown menu below the 'List Nearby Devices' button, also highlighted with a red rectangular box.

At the bottom of the configuration area, there are two buttons: 'Save and Reboot' and 'Cancel All Changes'. Below the configuration area, there is a section labeled 'Paired Devices'.

Fig. 14 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.



## 5.1.9 Serial Settings

### Setting Up Serial Communication

The screenshot shows the 'Serial Settings' page in a configuration utility. On the left is a sidebar with navigation links: System Overview, Easy Config, Network Settings, WLAN Settings, Bluetooth Settings, **Serial Settings**, Firmware Update, AT Commands, System Settings, and Help. Below these are buttons for 'Save and Reboot' and 'Cancel All Changes'. The main area contains the following settings:

- Operating Mode: RS232
- Baud Rate: 9600
- Data Bits: 8
- Parity: None
- Stop Bits: 2
- Modbus Optimization: ☒
- TCP Mode: Server
- Modbus Gateway Mode: Modbus RTU
- TCP Port: 502
- Show Statistics: ☒

Below the settings are two statistics sections:

Serial Rx Statistics (Bytes)	
Buffer Size	512
Used	0
Total	0
Dropped	0
Overrun	0
Underrun	0

Serial Tx Statistics (Bytes)	
Buffer Size	3072
Used	0
Total	0
Dropped	0
Overrun	0
Underrun	0

Fig. 15 Example | Serial Settings, TCP Mode Server with Modbus TCP to Modbus RTU Gateway function enabled

The screenshot shows the 'Serial Settings' page in a configuration utility, similar to Fig. 15 but with different settings. The sidebar and buttons are the same. The main area contains the following settings:

- Operating Mode: RS232
- Baud Rate: 9600
- Data Bits: 8
- Parity: None
- Stop Bits: 2
- Modbus Optimization: ☒
- TCP Mode: Client
- TCP Server IP: 192.168.0.99
- TCP Port: 5005
- Show Statistics: ☒

Below the settings are two statistics sections:

Serial Rx Statistics (Bytes)	
Buffer Size	512
Used	0
Total	0
Dropped	0
Overrun	0
Underrun	0

Serial Tx Statistics (Bytes)	
Buffer Size	3072
Used	0
Total	0
Dropped	0
Overrun	0
Underrun	0

Fig. 16 Example | Serial Settings, TCP Mode Client



*To avoid timing problems if different baud rates are set on the master and the slaves, set the lowest baud rate on the master.*

#### Serial Settings

Operating Mode	Select a physical serial communication interface, <b>RS232</b> , <b>RS485</b> or <b>Off</b> .
Baud Rate	Specify the rate at which information is transferred in a communication channel. Select a baud rate. At baud rates up to 115200 baud, the module is ready to receive data within one bit after last bit is sent. At baud rates higher than 115200 baud, the module will be ready to receive data 7 micro seconds after the last bit is sent.
Data Bits	Specify the number of data bits to transmit. Select <b>5</b> , <b>6</b> , <b>7</b> or <b>8</b> bits. To transmit binary data, select 8 data bits.
Parity	Specify if parity should be used to detect code errors. <b>No parity</b> = No parity checking, parity bit is not transmitted. <b>Odd parity</b> = The parity bit is asserted or unasserted to obtain an odd number of mark bits. <b>Even</b> = Even parity checking.
Stop Bits	Specify the number of stop bits used to indicate the end of data transmission. Select stop bit <b>1</b> or <b>2</b> .
Modbus Optimization	When Modbus Optimization is selected, the communication is optimized to keep all Modbus packets together in one frame. This mode should only be enabled when communicating with MODBUS RTU devices.
TCP Mode	Select a TCP Mode from the dropdown menu: Client: The Bolt Serial acts as a client and establishes a connection to the TCP server. Server: The Bolt Serial acts as a server and listens for incoming connections from the TCP client.
TCP Server IP	When TCP Mode Client is selected, enter the TCP Server IP address.
Modbus Gateway Mode	When TCP Mode Server is enabled, select Modbus Gateway Mode to enable Modbus TCP to Modbus RTU gateway functionality.
TCP Port	When TCP Mode is active, enter the TCP Port number. Default port: 5005 When Modbus Gateway Mode is active, the port automatically changes to Modbus TCP port 502.
Show Statistics	Select Show Statistics to view Serial Rx and Tx statistics. Buffer Size: The bytes in the queue, handled with in the order they were received. Used: Part of the buffer used. Total: Total size of the buffer. Dropped: The number of dropped data packets. Overrun: Occur when the buffer is full, but still tries to handle incoming data traffic. Underrun: Occur when the incoming data traffic is at a lower speed than the outgoing data traffic.

### Serial Communication

The serial functionality is used to transfer serial data from one point on a wireless link to another.

The connection can be set up as a point-to-point link or a point-to-multipoint link.

A message sent from a *master* to a Bolt Serial is forwarded to all the connected *slaves*.

The *slave* response sent to the Bolt Serial is forwarded to the *master* but not to the other *slaves*.

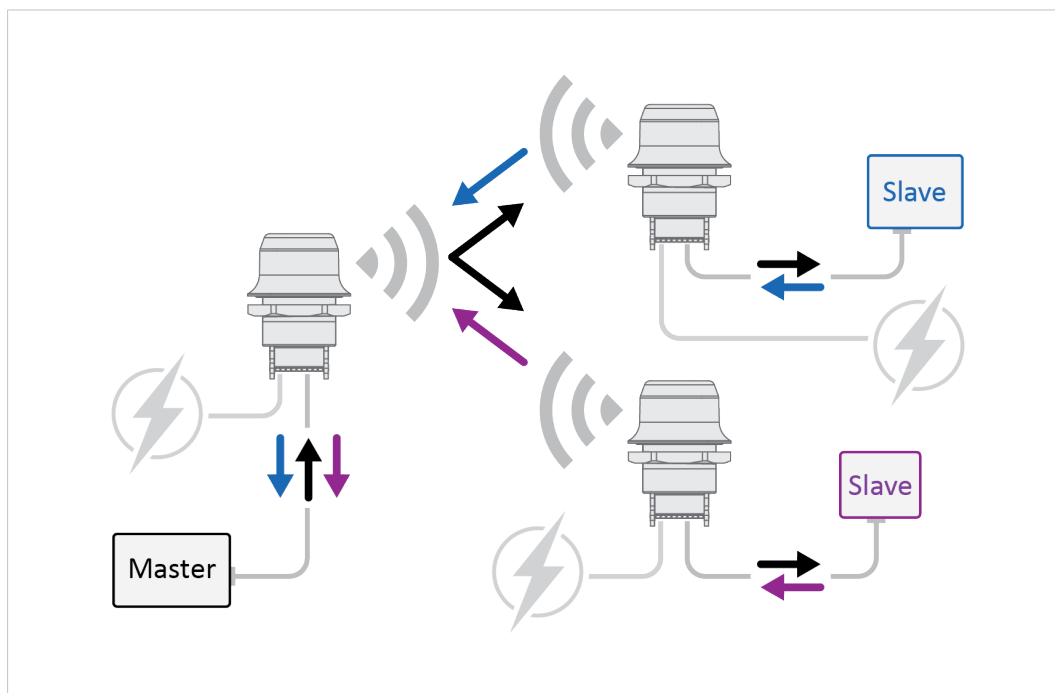


Fig. 17 Point-to-multipoint example | Message sent from master and response sent from slaves

#### 5.1.10 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.

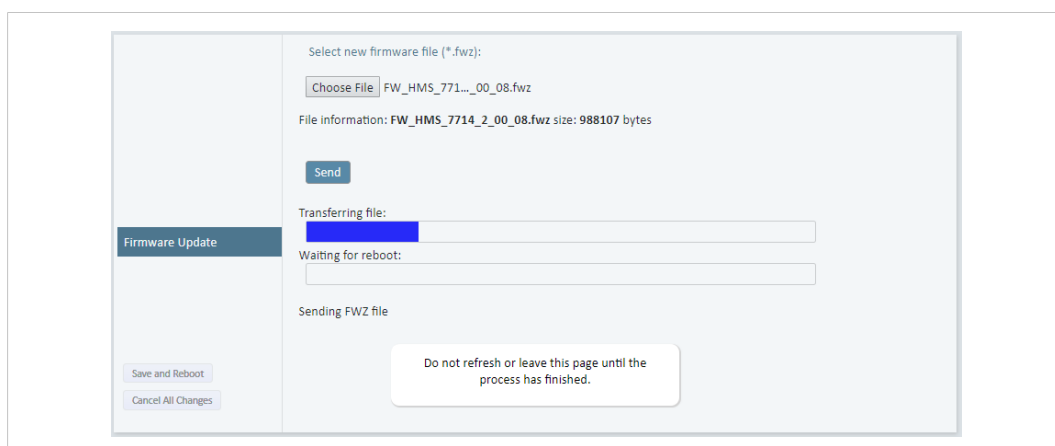
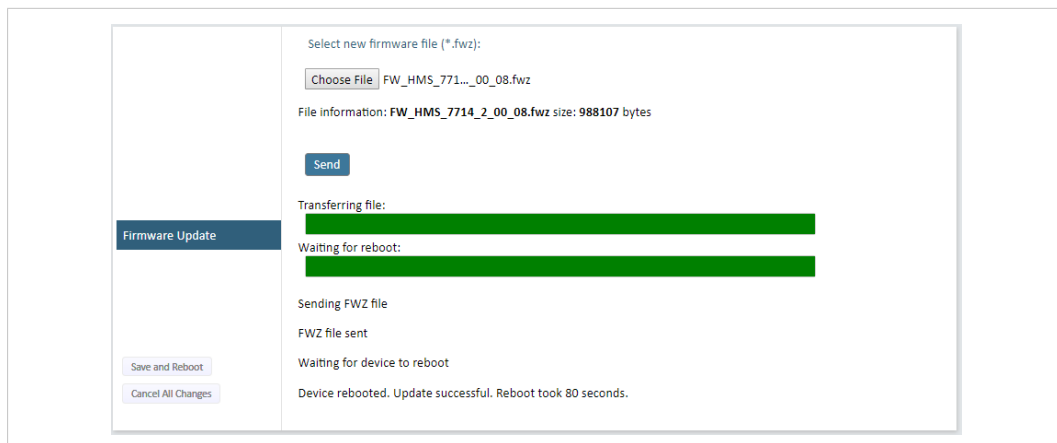


Fig. 18 Firmware update in progress

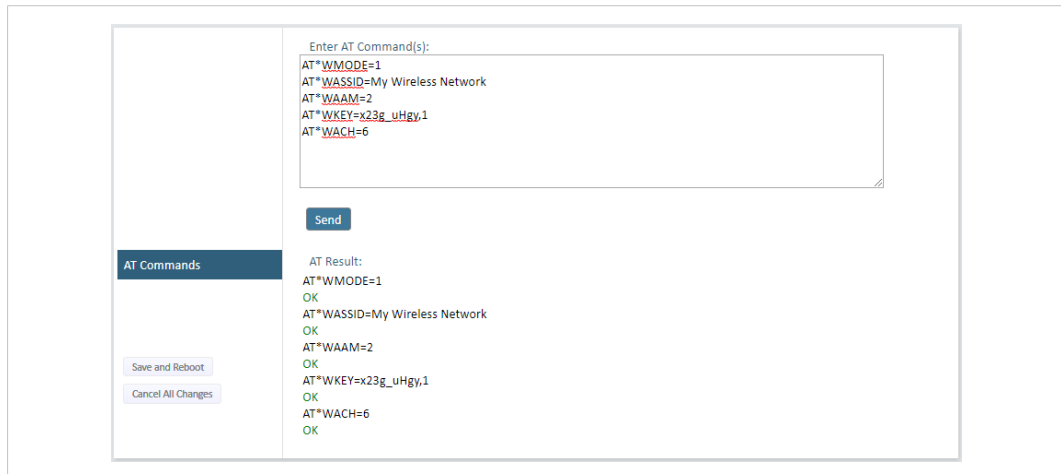
Both progress bars will turn green when the firmware update has been completed. The unit will then reboot automatically.



**Fig. 19** Firmware update completed

Updating the firmware will not change the configuration settings.

### 5.1.11 AT Commands



The screenshot displays a web interface for entering and executing AT commands. On the left, there is a sidebar with a button labeled "AT Commands" and two buttons at the bottom: "Save and Reboot" and "Cancel All Changes". The main area is divided into two sections. The top section, titled "Enter AT Command(s):", contains a text box with the following commands: `AT+WMODE=1`, `AT+WASSID=My Wireless Network`, `AT+WAAM=2`, `AT+WKEY=x23g_uHgy,1`, and `AT+WACH=6`. Below the text box is a "Send" button. The bottom section, titled "AT Result:", displays the output for each command: `AT+WMODE=1` OK, `AT+WASSID=My Wireless Network` OK, `AT+WAAM=2` OK, `AT+WKEY=x23g_uHgy,1` OK, and `AT+WACH=6` OK.

Fig. 20 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.

Click on **Help** for a complete list of supported AT commands.

5.1.12 System Settings

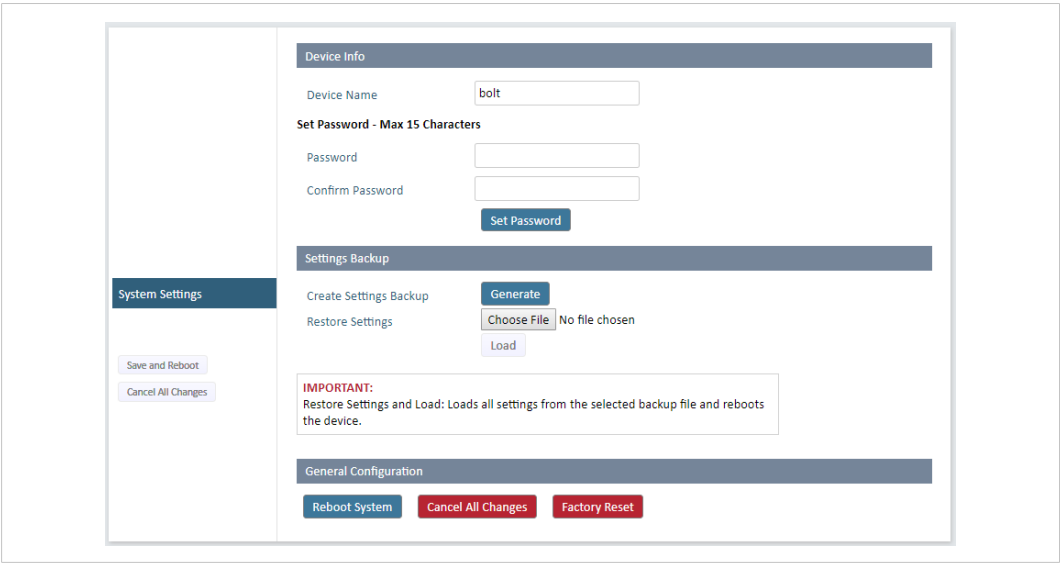



Fig. 21 System Settings

Device Info	
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.

Settings Backup	
Create Settings Backup	Click on <b>Generate</b> to save the current configuration to a file on your computer.
Restore Settings	Click on <b>Choose file</b> and select a previously saved configuration, then click on <b>Load</b> . The settings in the saved configuration will be applied and the unit will reboot.

General Configuration	
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.

## 5.2 Use Cases

### 5.2.1 Bolt Serial Point-to-Point Installation

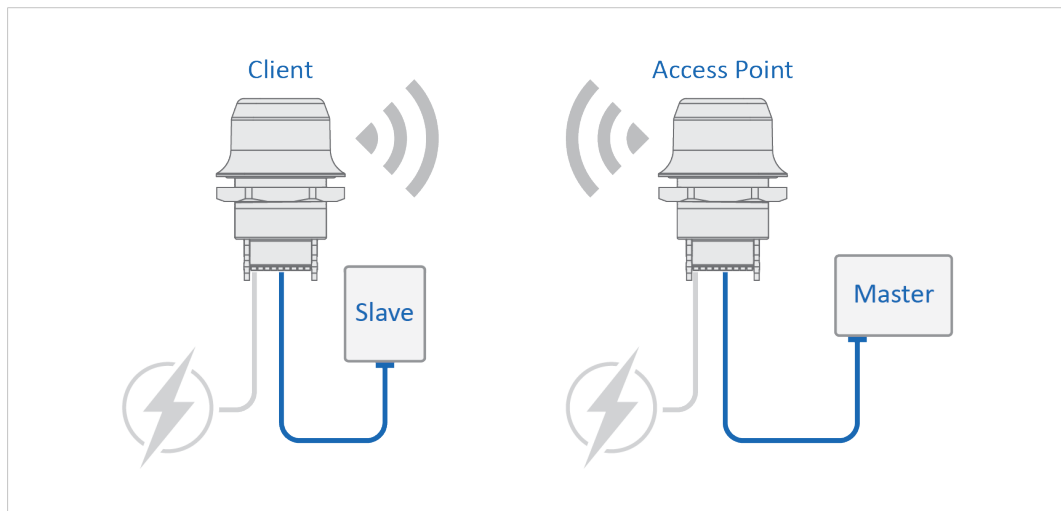


Fig. 22

Serial cable replacement is enabled by using two pieces of Bolt Serial which creates a wireless bridge for the serial communication.

### 5.2.2 Installing Multiple Bolt Serial

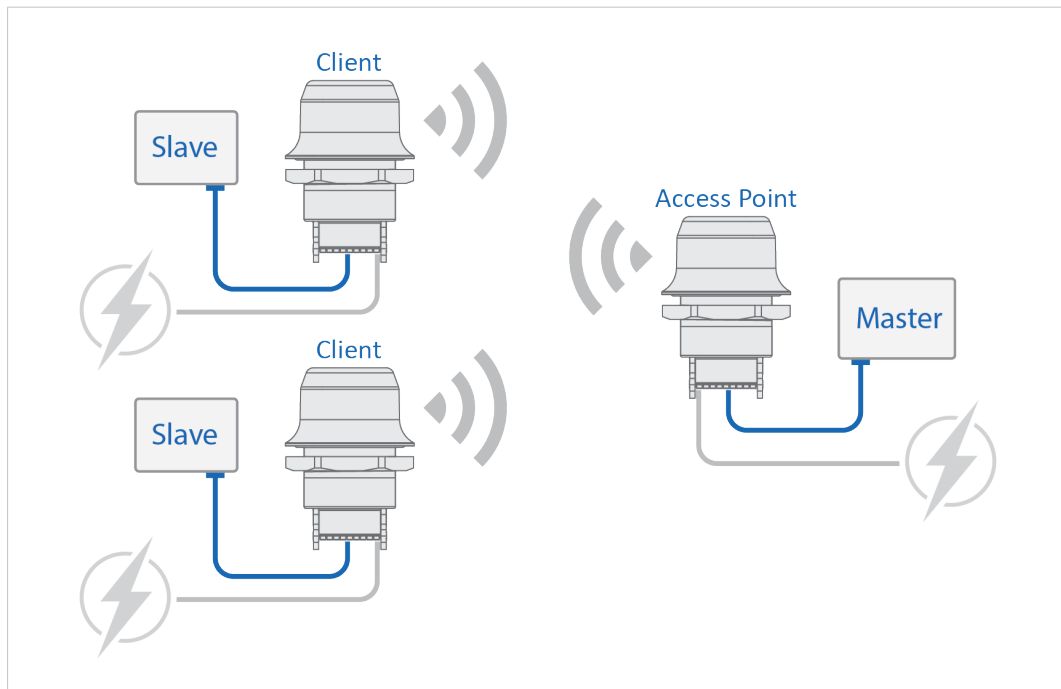


Fig. 23

When installing more than one Bolt Serial in the bridge, configure the Bolt Serial connected to the:

- *Master device as the Access Point (AP).*
- *Slave as a Client.*

### 5.2.3 Installing on a Modbus Network

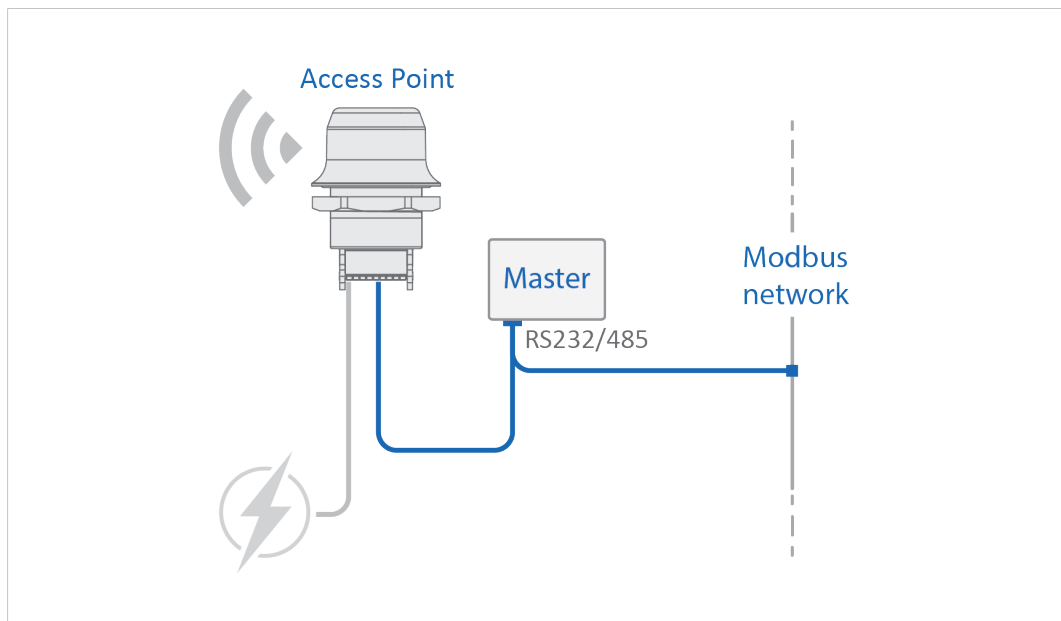


Fig. 24

When installing on a Modbus network, configure the Bolt Serial connected to the:

- *Master device as the Wireless Access point (AP).*
- *Slave as a Wireless Client.*

In the Bolt Serial access point web interface *Serial Settings tab*, select the **Modbus Optimization** checkbox.



### 5.2.4 Installing Using the Modbus TCP to RTU Gateway Function

The gateway function is transparent. When a command is sent on Modbus TCP it is translated to Modbus RTU. The response is translated back to Modbus TCP and delivered to the *Modbus TCP Client*.

It is possible to connect Bolt Serial to a pre-existing wireless infrastructure, such as the wireless network in a production facility.

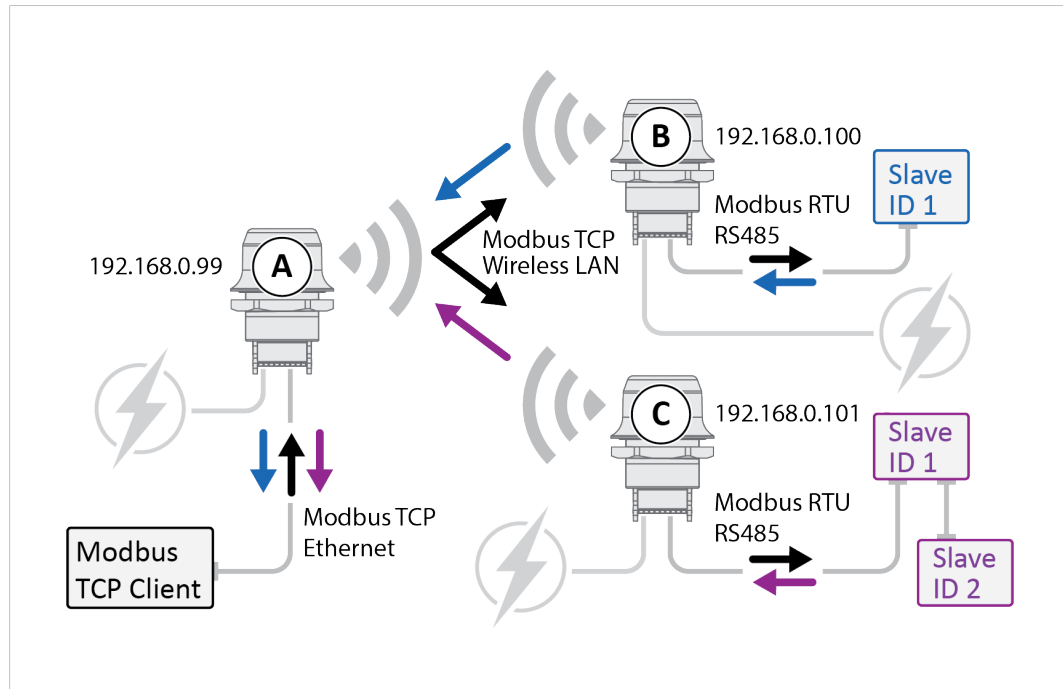


Fig. 25

- Configure *Bolt Serial A*, with IP address **192.168.0.99**, connected to the *Modbus TCP Client* as the *Access Point (AP)* or *Network Access Point (NAP)*.
- The *Modbus RTU Slave* connected to *Bolt Serial B* with IP address **192.168.0.100**.
- The other *Modbus RTU Slaves* are connected to *Bolt Serial C* with IP address **192.168.0.101**.
- The *Modbus RTU Slaves* are all Modbus Servers.

Configure the Modbus TCP Client to access the correct Modbus Slave:

- Slave ID 1 connected to *Bolt Serial Client B*:  
IP address 192.168.0.100 and unit identifier 1.
- Slave ID 1 connected to *Bolt Serial Client C*:  
IP address 192.168.0.101 and unit identifier 1.
- Slave ID 2 connected to *Bolt Serial Client C*:  
IP address 192.168.0.101 and unit identifier 2.

### 5.2.5 Bolt Serial TCP/IP Socket Protocol Description

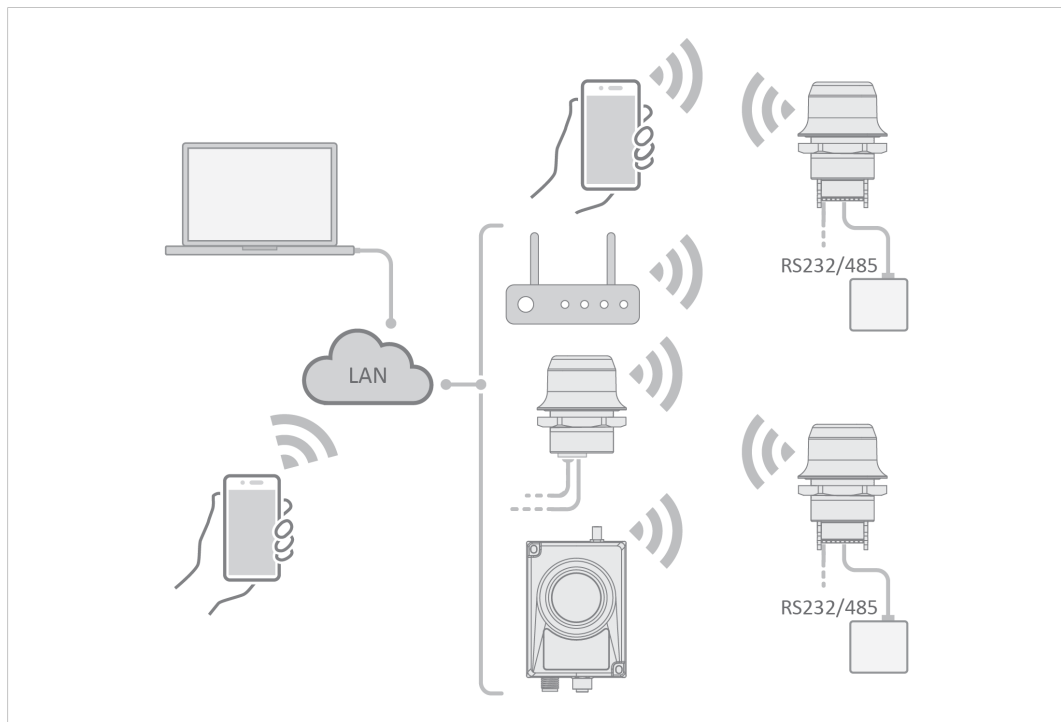


Fig. 26

The Bolt Serial may communicate with raw TCP/IP traffic and bridge the data to RS232 or RS485 on the serial port.

The Bolt Serial act as one of the endpoints in the TCP/IP communication. The other endpoint can be a PC program, tablet or phone application, PLC, controller or similar.

Using a virtual COM port (VCP) driver is also supported. Use a COM port redirector software that supports raw TCP/IP to enable wireless access to the devices over the network.

#### Procedure

To set up TCP/IP communication:

1. Establish IP connectivity between the devices using either WLAN or Bluetooth (PAN profile).
2. Do one of the following:
  - Open a TCP/IP socket towards the Bolt Serial.  
Use the configured TCP port number (default 5005).  
Up to 7 active sockets are supported simultaneously.
  - Configure the Bolt Serial as a TCP client to connect to a specific IP.

#### Result

Serial payload data can now be sent as is via the TCP socket to the Bolt Serial and transparently forwarded to the serial port.

Incoming data from the serial port is forwarded transparently to all open TCP sockets.

## 5.3 Set Up a Wireless Infrastructure

Connect two or more Bolt Serial units via WLAN or Bluetooth using Easy Config.

### 5.3.1 Connecting the Devices

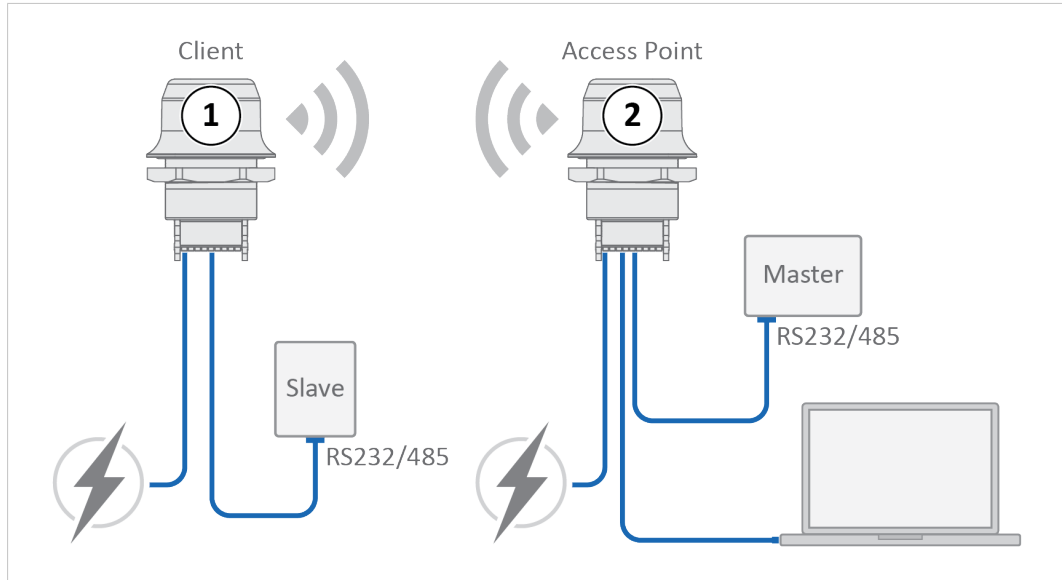


Fig. 27 Serial bridge example

1. Connect *Client unit 1* to a Serial device.
2. Connect *Access Point unit 2* to the master device.
3. Connect *Access Point unit 2* to your PC, with an Ethernet cable.
4. Connect *Access Point unit 2* to power.

### 5.3.2 Activate Easy Config

1. Navigate to the web interface of *Access Point unit 2*.  
The default address to *Access Point unit 2* is **192.168.0.99**.
2. Activate one of the following Easy Config Modes:
  - **Easy Config Mode 1** for Bluetooth PANU-PANU. Used for setting up point-to-point communication.
  - **Easy Config Mode 5** for WLAN
  - **Easy Config Mode 6** for Bluetooth
3. Connect *Client unit 1* to power.
  - *Client unit 1* starts up in **Easy Config Mode 4** and is open for automatic configuration during 120 seconds.
  - *Access Point unit 2* will discover and configure *Client unit 1* as a *Client* and configure itself as an *Access Point*.
  - *Client unit 1* will be assigned the first free IP address in the same Ethernet subnet as *Access Point unit 2*.  
The default address to the first *Client unit* is **192.168.0.100**.
  - If no connection is established during Easy Config Mode:
    - Ensure that *Client unit 1* is disconnected from Ethernet.
    - Disconnect *Client unit 1* from power and repeat Activate Easy Config step 5 and 6.

### 5.3.3 Adding More Bolt Serial Clients

When using **Easy Config Mode 1**, continue with Serial Configuration.

When using **Easy Config Mode 5** or **Easy Config Mode 6**, up to 6 additional Bolt Serial Clients can be added to the Serial bridge.

1. To add more *Client units*, repeat Connecting the Devices step 1 and the Activate Easy Config steps.
  - Each new *Client unit* will be assigned the next free IP address in the current Ethernet subnet.

### 5.3.4 Serial Configuration

From the PC connected to *Access Point unit 2*:

1. Navigate to the web interface of each Bolt Serial unit.
2. Select the **Serial Settings** tab.
3. Configure the serial port settings:

Operating mode	Specify the physical serial communication interface. Select <b>RS232</b> or <b>RS485</b> .
Baud rate	Select a baud rate to specify the rate at which information is transferred in a communication channel. To avoid timing problems if different baud rates are set on the master and the slaves, set the lowest baud rate on the master.
Data bits	Specify the number of data bits to transmit. Select <b>5</b> , <b>6</b> , <b>7</b> or <b>8</b> bits.
Parity	Specify if parity should be used to detect errors in code. Select <b>No parity</b> , <b>Odd parity</b> or <b>Even parity</b> .
Stop bits	Specify the number of stop bits used to indicate the end of data transmission. Select stop bit <b>1</b> or <b>2</b> .
Modbus Optimization	When Modbus Optimization is selected, the communication is optimized to keep all Modbus packets together in one frame. This mode should only be enabled when communicating with Modbus RTU devices.
TCP Mode	Select a TCP Mode from the dropdown menu: Client: Bolt Serial acts as a client and establishes a connection to the TCP server. Server: Bolt Serial acts as a server and listens for incoming connections from the TCP client.
TCP Server IP	When TCP Mode Client is enabled, enter the TCP Server IP address.
Modbus Gateway Mode	When TCP Mode Server is enabled, select Modbus Gateway Mode to enable Modbus TCP to Modbus RTU gateway functionality.
TCP Port	When TCP Mode is enabled, enter a TCP Port number. Default port: 5005 When Modbus Gateway Mode is active, the port automatically changes to Modbus TCP port 502.

### 5.3.5 Serial Installation

1. Connect each Bolt Serial unit to a device or machine equipped with a Serial port.  
For more information, refer to [Connector, p. 7](#) and [Cabling, p. 8](#).

## 5.4 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 pressed for >10 seconds and then releasing it

### Default Network Settings

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
DHCP Interfaces	All

### 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]
Connectable	No
Discoverable	No
Security Mode	Just works
Bluetooth LE	Operating Mode: Disabled Connectable: No Discoverable: No

### Default Serial Settings

Operating Mode	RS232
Baud Rate	57600 bits/s
Data bits	8
Stop bits	1
Parity	No parity
Modbus optimization	Off
TCP Mode	Server
Modbus Gateway Mode	Disabled
TCP port	5005

## 6 Technical Data

For complete technical specifications and regulatory compliance information please visit [www.anybus.com/support](http://www.anybus.com/support).

### 6.1 Technical Specifications

<b>Order code</b>	<b>AWB2010</b>	<b>AWB2011</b>
<b>Color</b>	Black	White top and black base
<b>Connector</b>	Included plug connector (2x9p; 3.5mm, Phoenix DFMC 1.5/9-ST-3.5, push-in spring connection).	
<b>Range</b>	Up to 100 meters free line of sight	
<b>Antenna</b>	One internal antenna. Dual-band 2,4GHz and 5GHz.	
<b>Temperature compatibility</b>	Operating: Shadow black and white: -40 to +65 °C Direct sunlight: Black -40 to +45 °C, White -40 to +65 °C Storage temperature: -40 to +85 °C	
<b>Weight</b>	81 g	
<b>Housing material</b>	Top: Valox 357X(f1) PBT/PC. Suitable for outdoor use with respect to exposure to ultraviolet light, water exposure and immersion in accordance with UL 746C. Bottom: Celanex: XFR 6840 GF15. PBT glass reinforced plastic.	
<b>IP protection class</b>	IP66, IP67 and UL NEMA 4X for top (outside the host), IP21 for bottom (inside the host).	
<b>Dimensions</b>	Diameter: 68 mm. Height: 75 mm (95 mm including connector). Outside height: 41 mm.	
<b>Mounting</b>	M50 screw and nut (50.5 mm hole needed).	
<b>Power</b>	9-30 VDC (-5% +20%), Cranking 12V (ISO 7637-2:2011 pulse 4). Reverse polarity protection. (Consumption: 0.7W idle, 1.7W max.)	
<b>Configuration</b>	Three different methods: 1. Accessing the built-in web pages in the product 2. Sending AT-commands via Telnet/Raw TCP and Serial 3. Using Easy Config modes.	
<b>Vibration compatibility</b>	Sinusoidal vibration test according to IEC 60068-2-6:2007 and with extra severities; Number of axes: 3 mutually perpendicular (X:Y:Z), Duration: 10 sweep cycles in each axes, Velocity: 1 oct/min, Mode: in operation, Frequency: 5-500 Hz, Displacement ±3.5 mm, Acceleration: 2g.  Shock test according to IEC 60068-2-27:2008 and with extra severities; Wave shape: half sine, Number of shocks: ±3 in each axes, Mode: In operation, Axes ± X,Y,Z, Acceleration: 30 g, Duration: 11 ms.	
<b>Humidity compatibility</b>	EN 600068-2-78: Damp heat, +40°C, 93% humidity for 4 days.	
<b>Digital input</b>	Usage: To control roaming between Bluetooth access points (NAP)	
<b>Wired interface</b>	Serial: RS232/485 Baud rate: 2.400 - 921.600 kbit/s, data bits 5-8, stop bits 1-2, parity None, Odd, Even. Transparent serial protocol transfer including support for Modbus-RTU.  Ethernet: 10/100BASE-T with automatic MDI/MDIX auto cross-over detection. For configuration only.	
<b>Wireless LAN</b>	<b>Wireless standards:</b> WLAN 802.11 a, b, g, n, d, r (fast roaming). <b>Operation modes:</b> Access point or Client <b>WiFi channels:</b> 2.4 GHz, channel 1-11 + 12-13 depending on regulatory domain scan. 5 GHz Access Point: 36-48 (U-NII-1), 5 GHz Client: 100-116 + 132-140 and 120-128 depending on regulatory domain scan. (U-NII-1, U-NII-2, U-NII-2e). <b>RF output power:</b> 13.75 dBm <b>Max number of slaves for access point:</b> 7 <b>Power consumption:</b> 54mA@24VDC <b>Net data throughput:</b> 20 Mbps. Link speed: max 65 Mbps (802.11n SISO) <b>Security:</b> WEP 64/128, WPA, WPA-PSK and WPA2, TKIP and AES/CCMP, LEAP, PEAP including MS-CHAP.	
<b>Classic Bluetooth</b>	<b>Wireless standards (profiles):</b> PANU & NAP <b>Operation modes:</b> Access point or Client <b>RF output power:</b> 9.75 dBm <b>Max number of slaves for access point:</b> 7 <b>Power consumption:</b> 36 mA@24VDC <b>Net data throughput:</b> ~1 Mbps <b>Bluetooth version support:</b> Classic Bluetooth v2.1 <b>Security:</b> Authentication & Authorization, Encryption & Data Protection, Privacy & Confidentiality, NIST Compliant, FIPS Approved	

**This page intentionally left blank**



# A RS232/RS485 Electrical Connection

**i** A and B marking differs between different devices, in this product A is TX+/RX+ or D+ and B is TX-/RX- or D-.

## A.1 RS485 Typical Connection

**i** The resistors on the Bolt Serial side are termination resistors which form an active termination of the RS485 line.

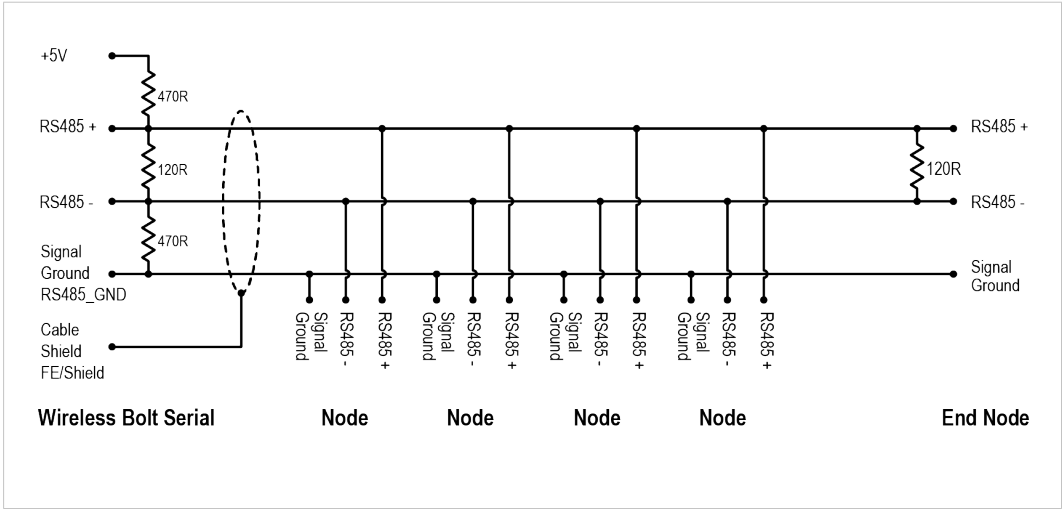


Fig. 28 RS485

## A.2 RS232 Typical Connection



Fig. 29 RS232

## 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.

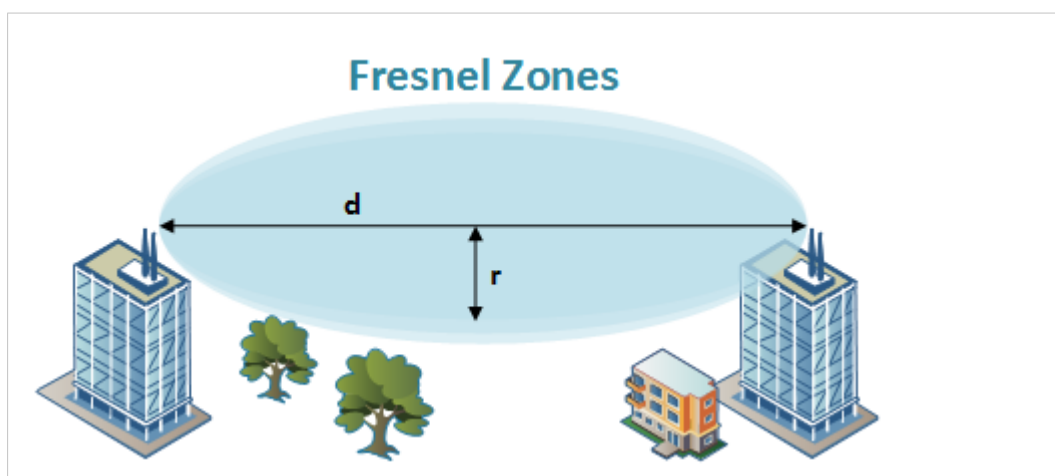


Fig. 30 Fresnel zones

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 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.

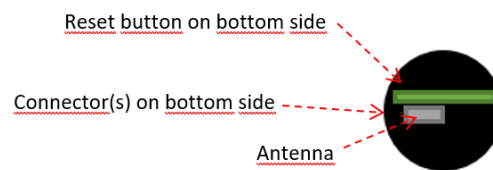
## C Radio Antenna Patterns

This section presents information about the radio antenna patterns for the Anybus Wireless Bolt.

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 Bolt, while maintaining the same distance.

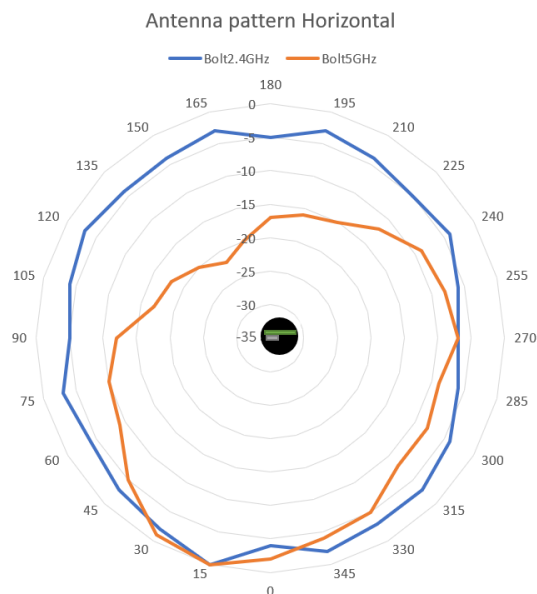
### C.1 Azimuth (Horizontal) View

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



(Bolt viewed from above, looking at the top logo)

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.



Limited gain for 5 GHz between 105° to 190°.

## C.2 Vertical Views

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

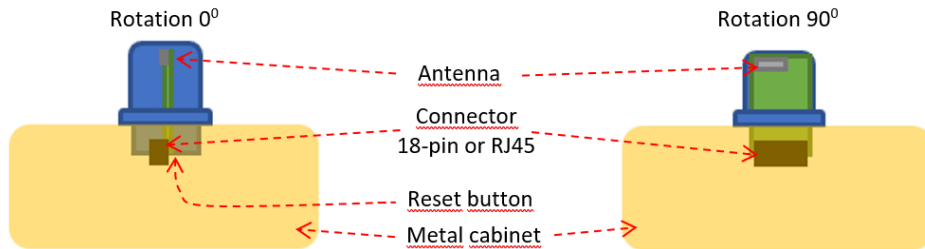
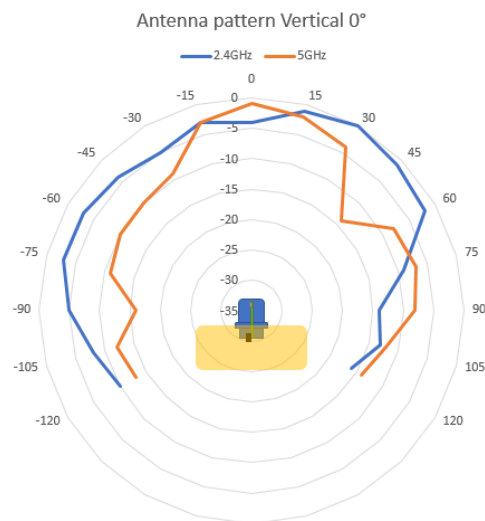
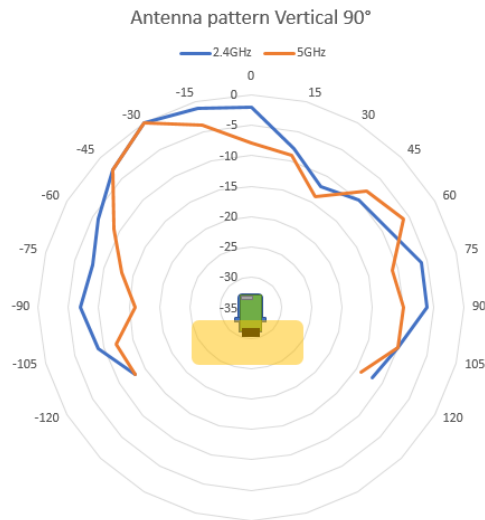


Diagram analysis: The vertical antenna gain is fairly omnidirectional for both frequencies. It is also clear to see that the metal cabinet where the Bolt is mounted will increase the gain “upwards” in reference to the surface where the Bolt is mounted. Thus the gain “downwards” is limited as expected.

### C.2.1 Front View – Vertical 0°



### C.2.2 Side View – Vertical 90°



### C.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 Anybus Wireless Bolt and the Anybus Wireless Bridge when using Wi-Fi (WLAN) 2.4 GHz.

