

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

**USER MANUAL**

SCM-1202-143  
Version 2.0  
Publication date 2022-04-07



## 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.

Copyright © 2021 HMS Networks

### **Contact Information**

Postal address:  
Box 4126  
300 04 Halmstad, Sweden

E-Mail: [info@hms.se](mailto:info@hms.se)

# Table of Contents

<b>1. Preface</b> .....	<b>1</b>
1.1. About This Document .....	1
1.2. Document Conventions .....	1
1.3. Trademarks .....	2
<b>2. Safety</b> .....	<b>3</b>
2.1. General Safety .....	3
2.2. Intended Use .....	3
<b>3. Preparation</b> .....	<b>4</b>
3.1. Support and Resources .....	4
3.2. Network Environment .....	4
3.3. Placement .....	4
3.4. When to Use Bluetooth or WLAN .....	4
3.5. Bluetooth Limitations .....	4
3.6. I/O-Data Cycle Time Considerations .....	5
<b>4. Installation</b> .....	<b>6</b>
4.1. Mechanical Installation .....	6
4.2. Connector .....	7
4.3. Cabling .....	8
4.4. Reset Button .....	9
<b>5. Configuration</b> .....	<b>10</b>
5.1. Bolt Serial Built-In Web Interface .....	10
5.2. Access the Built-In Web Interface .....	11
5.2.1. Required IP Address Settings .....	11
5.2.2. Log In to the Built-In Web Interface .....	12
5.3. To Save and Reboot .....	13
5.4. Factory Default Settings .....	14
5.5. Configuration Methods .....	15
5.6. Wireless Configuration via Access Point Unit .....	15
5.7. Configuration with Easy Config .....	16
5.7.1. Available Easy Config Modes .....	16
5.7.2. Easy Config Modes Time Considerations .....	16
5.7.3. How to Activate an Easy Config Mode .....	17
5.8. Configuration with AT Commands .....	18
5.8.1. Enable Fast Roaming with AT Commands .....	19
5.8.2. Digital Input .....	19
5.8.3. Add Additional WLAN Channels with AT Commands .....	20
5.9. Configure Settings in the Built-In Web Interface .....	22
5.9.1. Network Settings .....	22
5.9.2. Layer 3 IP Forward Connectivity Considerations .....	23
5.9.3. WLAN Settings General .....	24
5.9.4. WLAN Settings for Client .....	25
5.9.5. WLAN Roaming .....	25
5.9.6. WLAN Channels and World Mode .....	26
5.9.7. WLAN Settings for Access Point .....	27
5.9.8. WLAN Advanced Settings .....	28
5.9.9. Bluetooth Settings General .....	29
5.9.10. Bluetooth Settings for PANU Mode .....	30
5.9.11. Bluetooth Settings for NAP Mode .....	31

5.9.12. Set Up Serial Communication .....	32
5.9.13. Serial Communication .....	35
5.9.14. System Settings .....	36
<b>6. Use Cases .....</b>	<b>37</b>
6.1. Bolt Serial Point-to-Point Installation .....	37
6.2. Set Up Wireless Infrastructure .....	38
6.3. Installing Multiple Bolt Serial Units .....	40
6.4. Installing on a Modbus Network .....	41
6.5. Installing Using the Modbus TCP to RTU Gateway Function .....	42
6.6. Bolt Serial TCP/IP Socket Protocol Description .....	43
<b>7. Verify Operation .....</b>	<b>44</b>
7.1. Network Connection Status .....	44
<b>8. Maintenance .....</b>	<b>45</b>
8.1. Firmware Update .....	45
8.2. Settings Backup .....	47
8.2.1. Create Settings Backup File .....	47
8.2.2. Restore Settings From Backup File .....	47
<b>9. Troubleshooting .....</b>	<b>48</b>
9.1. Reset Button .....	48
9.2. Recovery Mode .....	49
9.3. Reset to Factory Default .....	50
<b>10. Technical Data .....</b>	<b>52</b>
10.1. Technical Specifications .....	52
<b>11. Reference Guides .....</b>	<b>54</b>
11.1. RS232/RS485 Electrical Connection .....	54
11.2. Wireless Technology Basics .....	55
11.3. Radio Antenna Patterns .....	56

# 1. Preface

## 1.1. About This Document

This document 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

### Lists

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

### User Interaction Elements

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

### Program Code and Scripts

```
Program code and script examples
```

### Cross-References and Links

Cross-reference within this document: [Document Conventions \(page 1\)](#)

External link (URL): [www.anybus.com](http://www.anybus.com)

### Safety Symbols



#### DANGER

Instructions that must be followed to avoid an imminently hazardous situation which, if not avoided, will result in death or serious injury.



#### WARNING

Instructions that must be followed to avoid a potential hazardous situation that, if not avoided, could result in death or serious injury.



#### CAUTION

Instruction that must be followed to avoid a potential hazardous situation that, if not avoided, could result in minor or moderate injury.



#### IMPORTANT

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.

## Information Symbols



### NOTE

Additional information which may facilitate installation and/or operation.



### TIP

Helpful advice and suggestions.

## 1.3. Trademarks

Anybus® is a registered trademark and Wireless Bolt Serial™ is a trademark of HMS Networks AB.

All other trademarks are the property of their respective holders.

## 2. Safety

### 2.1. General 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 equipment meet appropriate susceptibility specifications for this type of RF energy.

**CAUTION**

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

**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.

**CAUTION**

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.

### 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. Support and Resources

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

**TIP**

Have the product article number available, to search for the product specific support web page. You find the product article number on the product cover.

### 3.2. Network Environment

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

### 3.3. Placement

#### Antenna Considerations

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

See also [Internal Antenna Characteristics](#).

#### Required Distance Between Devices

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

See [Wireless Technology Basics \(page 55\)](#).

### 3.4. When to Use Bluetooth or WLAN

#### Use Bluetooth when:

- The wireless link has an Anybus Wireless Bolt or Anybus Wireless Bridge II 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.

### 3.5. Bluetooth Limitations

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

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

### 3.6. I/O-Data Cycle Time Considerations

Based on recommendations from industrial equipment suppliers, such as Rockwell and Siemens, use the following minimum I/O data cycle times for PROFINET and EtherNet/IP networks:

- Wireless link Point-to-Point with Bluetooth PANU-PANU or Wi-Fi Access Point to Station: 32 ms
- Wireless link with Access Point and up to 4 wireless clients/stations, Bluetooth or Wi-Fi: 64 ms

## 4. Installation

### 4.1. Mechanical Installation

#### Placement

- The device is intended to be mounted on top of a machine or cabinet through an M50 (50.5mm) 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.

#### Installation

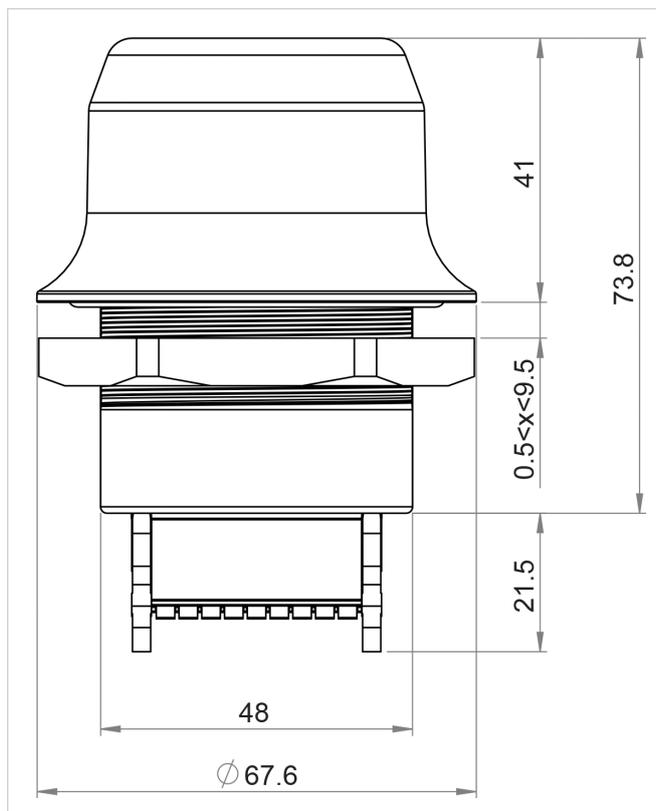
**IMPORTANT**

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

**IMPORTANT**

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

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



All measurements are in mm.

Figure 1. Installation drawing

## 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.

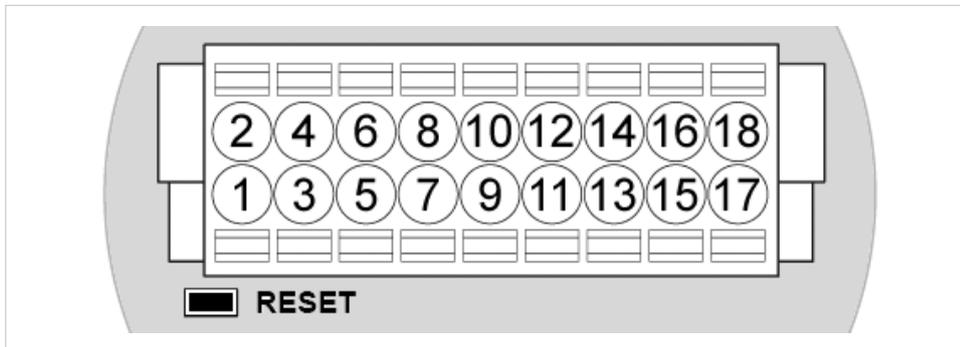


Figure 2. 18-Pin connector

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 **RESET** button.



### NOTE

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



### NOTE

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 \(page 54\)](#).

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 Wireless Bolt Serial.)
14	RS232_CTS	RS-232 Clear To Send (Not used for Wireless 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 Wireless Bolt Serial.)
18	CAN_H	CAN High (Not used for Wireless 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

### Before You Begin

**NOTE**

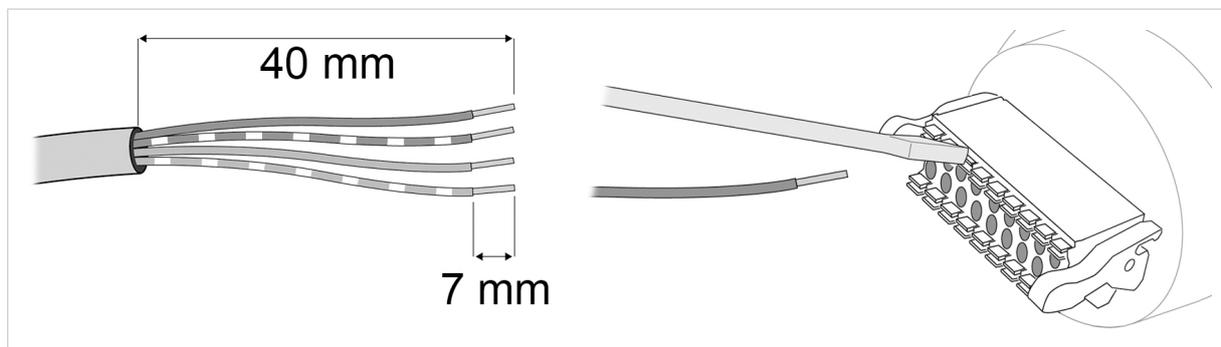
When using **Easy Config Modes**, the Bolt Serial that is to be configured as a Client does not need to be connected to the Ethernet wires. Only power and Serial wiring are used.

**NOTE**

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

### Procedure

#### Create connector cable for Bolt Serial



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 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 \(page 7\)](#).
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.

**NOTE**

Ensure that polarity is not reversed.

### 4.4. Reset Button

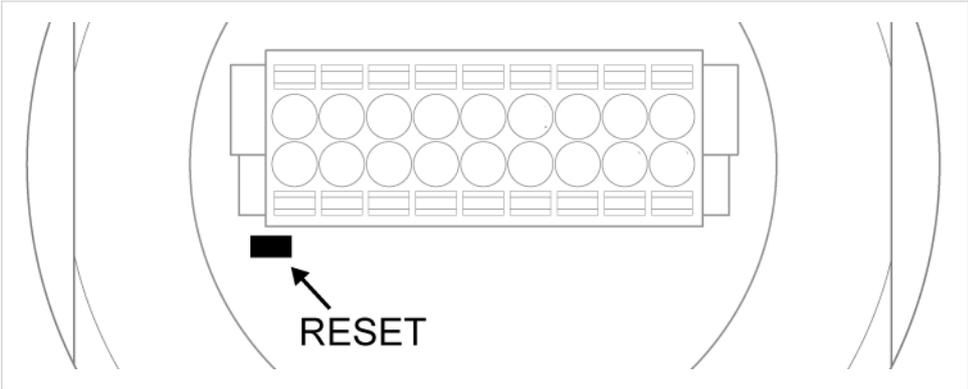


Figure 3. Reset button

The **Reset** button is located on the bottom of the Bolt Serial.

## 5. Configuration

### 5.1. Bolt Serial Built-In Web Interface

The Bolt Serial built-in web interface is used to configure, maintain and troubleshoot the Bolt Serial. Parameters can be set individually or using pre-configured Easy Config modes.

The web interface is accessed by pointing a web browser to the IP address of the unit.

The default address is 192.168.0.99.

See also [Access the Built-In Web Interface \(page 11\)](#).

System Overview	
Easy Config	
Network Settings	
WLAN Settings	
Bluetooth Settings	
Bluetooth LE Settings	
Firmware Update	
AT Commands	
System Settings	
Help	
Save and Reboot	
Cancel All Changes	
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
World Mode (1-11,36-140)	Enabled
Channel	Auto
Channel Bands	2.4 GHz & 5 GHz
Connect 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
Bluetooth LE	
Status	On
Operating Mode	Disabled
System	
Device Name	awb
Firmware	1.6.3 [15:19:00, Aug 28 2018]
Uptime	1 d, 4 h, 11 m, 14 s

Figure 4. System Overview page example

The **System Overview** page shows current settings and network connection status.

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

## 5.2. Access the Built-In Web Interface

### 5.2.1. Required IP Address Settings

To be able to access the Bolt Serial built-in web interface you may need to adjust the IP settings, choose one of the following methods.

The Bolt Serial default IP address is 192.168.0.99.

#### Option 1 - Set a Static IP Address on Your PC



On the PC accessing the Bolt Serial built-in web interface, set a static IP address within the same IP address range as the Bolt Serial IP address.

Note that when you change to a static IP address on your PC, internet access is lost.

#### Option 2 - Change the IP Address on the Bolt Serial Ethernet port



Use the software application HMS IPconfig to find and change the IP address on the Bolt Serial Ethernet port, to one within the same IP address range as the PC accessing the Bolt Serial built-in web interface.

To download the installation files, please visit [www.anybus.com/support](http://www.anybus.com/support) and enter the product article number to search for the Bolt Serial support web page. You find the product article number on the product cover.

#### Result

Now you can enter the Bolt Serial IP address in your web browser and search to access the built-in web interface login page.

See [Log In to the Built-In Web Interface \(page 12\)](#).

## 5.2.2. Log In to the Built-In Web Interface

The Bolt Serial built-in web interface can be accessed from a standard web browsers.

### Before You Begin



#### IMPORTANT

Before installing Bolt Serial on a network, change the default administrator password.



#### IMPORTANT

Before installing the Bolt Serial on a network, change the Bolt Serial default username and password.



#### NOTE

The Bolt Serial comes with a default username and password. The default username is admin, written in lowercase letters. You find the default password on the Bolt Serial product housing.



#### NOTE

The Bolt Serial default IP address is 192.168.0.99.

### Procedure

#### Login to the Bolt Serial built-in web interface

1. Open a web browser.
2. Click to select the **Address bar** and enter the Bolt Serial IP address.



Figure 5. Enter IP address in web browser

3. Press **Enter**.  
The built-in web interface login screen appears.
4. Enter the **Password** and click **Sign in**.

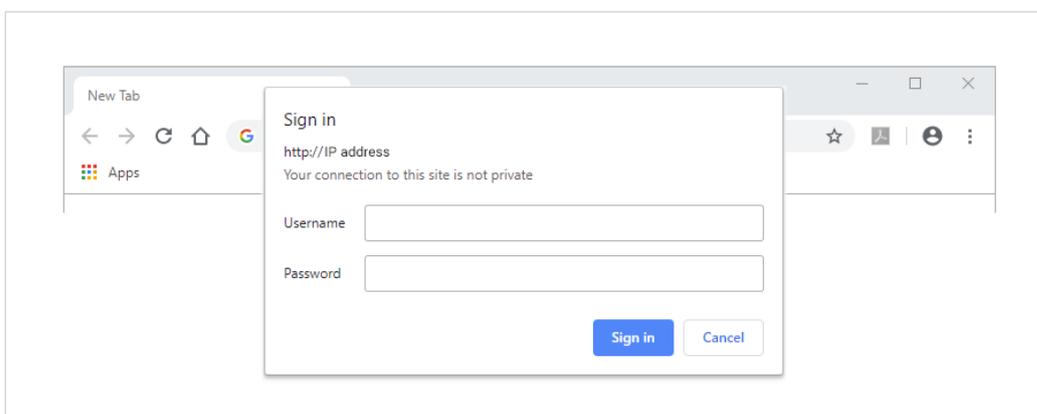


Figure 6. Built-in web interface login screen

## Result

You are logged in to the **System Overview** page.

The screenshot shows the 'System Overview' page with a sidebar menu on the left and a main content area on the right. The sidebar menu includes 'System Overview', 'Easy Config', 'Network Settings', 'WLAN Settings', 'Bluetooth Settings', 'Bluetooth LE Settings', 'Firmware Update', 'AT Commands', 'System Settings', and 'Help'. Below the menu are two buttons: 'Save and Reboot' and 'Cancel All Changes'. The main content area is divided into three sections: 'IP', 'LAN', and 'WLAN', each with a list of settings and their values.

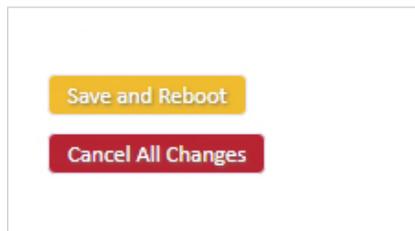
IP	
IP Assignment	Static
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99
Internal DHCP Server	Disabled

LAN	
Connection	Connected
MAC Address	00-30-11-19-43-2C

WLAN	
Status	On
Operating Mode	Client
Connection	Connected
MIMO	Enabled
World Mode (1-11,36-140)	Enabled
Channel	Auto
Channel Bands	2.4 GHz & 5 GHz

Figure 7. System Overview page

## 5.3. To Save and Reboot



### Cancel Changes

To cancel changes you have made to the settings:

- In the left sidebar menu, click **Cancel All Changes**.

To restore settings, see [Restore Settings From Backup File \(page 47\)](#).

### Apply Changes

- To apply changes, click **Save and Reboot** in the left sidebar menu. Bolt Serial restarts for the changes to take effect.

## 5.4. Factory Default Settings

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

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

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

## 5.5. Configuration Methods

There are different methods available for configuring the Bolt Serial.

### Built-In Web Interface Settings

Bolt Serial can be configured via the settings in the built-in web interface.

See [Configure Settings in the Built-In Web Interface \(page 22\)](#).

### Easy Config Modes

Bolt Serial can be configured using one of the pre-configured Easy Config modes.

See [Configuration with Easy Config \(page 16\)](#).

### AT Commands

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.

For more information about how to use the AT commands, navigate to the built-in web interface **Help** page or see the AT Commands Reference Guide.

See also [Configuration with AT Commands \(page 18\)](#).

## 5.6. Wireless Configuration via Access Point Unit

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

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.

## 5.7. Configuration with Easy Config

### 5.7.1. Available Easy Config Modes

Bolt Serial may be configured using one of the pre-configured Easy Config modes.



#### NOTE

By default, the unit starts in **Easy Config Mode 4**. The unit awaits automatic configuration during 120 seconds or until receiving a configuration.



#### NOTE

To cancel Easy Config mode 11, the unit must be reset to factory default settings. See [Reset to Factory Default \(page 50\)](#)

Table 1. Easy Config modes

EC	Role	Description
1	Bluetooth PANU	Used for setting up point-to-point communication. The unit scans for another unit in Config Mode 4. The unit listens for 40 seconds or until a configuration is established. When a unit in mode 4 is detected: The scanning unit configures itself as a Bluetooth PANU Client, sends a connection configuration to the detected unit, and restarts. The detected unit restarts and attempt to connect to the first unit as a PANU Client.
2	N/A	Reset configuration to factory defaults.
3	N/A	Reset IP settings to factory defaults.
4	Client	Configure units in mode 4 as Clients. Wait for automatic configuration. The unit listens for 120 seconds or until receiving a configuration. When mode 4 is used with mode 1, 5 or 6, Serial Settings TCP Mode Client is activated automatically.
5	WLAN AP	The unit scans for other units in Config Mode 4 and configure them as Clients. Timeout occur after 120 seconds.
6	Bluetooth NAP	Restart as Access Point and connect Clients.
11	(any)	Enable PROFIsafe mode. The unit is locked in PROFIsafe mode. No other configuration settings are changed.

The Easy Config modes are also described when selected in the built-in web interface. See [How to Activate an Easy Config Mode \(page 17\)](#).

### 5.7.2. Easy Config Modes Time Considerations

Table 2. Easy Config modes time considerations

Mode	Timeout
1 and 9	The unit listens for 40 seconds or until a configuration is established.
4	The unit listens for 120 seconds or until receiving a configuration.
5, 6, 7 and 8	The unit scans for 120 seconds, then timeout occur.

### 5.7.3. How to Activate an Easy Config Mode

#### Activate an Easy Config Mode in the Built-In Web Interface

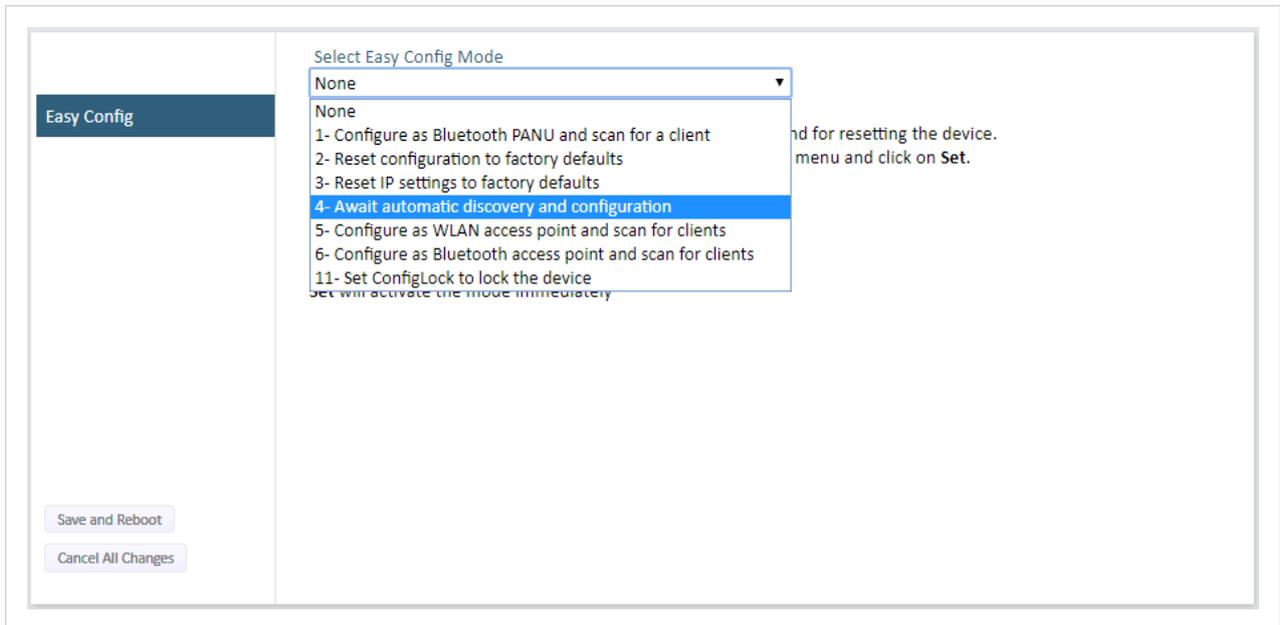


Figure 8. Built-in web interface Easy Config menu

1. In the built-in web interface, navigate to the **Easy Config** page.
2. To activate an Easy Config mode, select it from the drop-down menu and click **Set**. See also [Available Easy Config Modes \(page 16\)](#). The selected mode is activated immediately.

## 5.8. Configuration with AT Commands

Advanced configuration can be carried out by issuing AT commands via the web interface or over a Telnet or RAW TCP connection to port 8080 or over serial interface.

Use AT commands to setting advanced parameters, that are not accessible in the Bolt Serial built-in web interface.

AT commands can be used to read out parameters in text format and for batch configuration using command scripts.

For a complete list of supported AT commands, click **Help** in the built-in web interface. See also the AT Commands Reference Guide at [www.anybus.com/support](http://www.anybus.com/support).

### Procedure

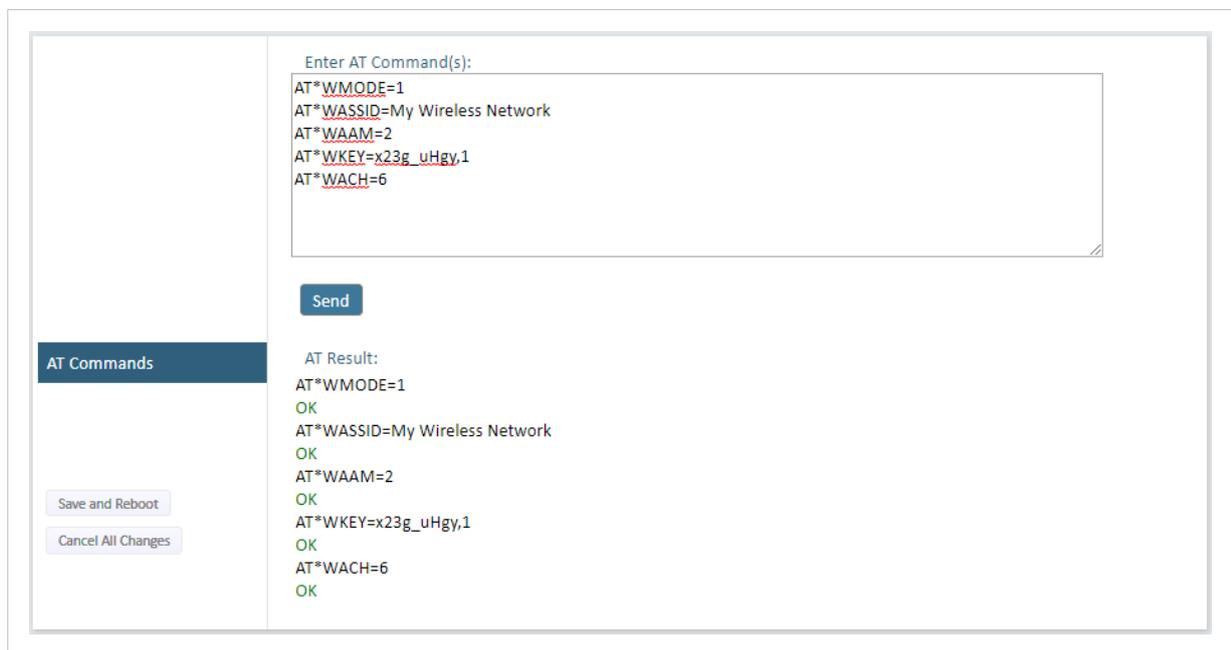


Figure 9. AT Commands and AT Results

1. Enter or paste the AT commands into the **Enter AT Command(s)** text field.
2. Click **Send**.
3. The result codes are displayed in the **AT Result** panel.

### 5.8.1. Enable Fast Roaming with AT Commands

Fast Roaming is only used for Client Mode.

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

#### Procedure

Enable or Disable Fast Roaming.

1. To Enable or Disable Fast Roaming, change the value of register **4004**.

- Enable Fast Roaming:

```
ATS4004=1
```

- Disable Fast Roaming:

```
ATS4004=0
```

2. For the command to take effect, reboot the Bolt Serial.

Send the Reboot device AT Command:

```
AT*AMREBOOT
```

For more information about how to set up WLAN roaming, see the AT Commands Reference Guide or the **Help** page in the built-in web interface.

### 5.8.2. Digital Input

The digital input can be used to control roaming between Bluetooth access points (NAP).

For more information, refer to the AT Commands Reference Guide at [www.anybus.com/support](http://www.anybus.com/support).



#### IMPORTANT

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

### 5.8.3. Add Additional WLAN Channels with AT Commands

WLAN Channels and World Mode is only used for Client Mode.

World Mode can be disabled and additional channels added using AT commands.



#### NOTE

When World Mode is disabled and additional channels are used, WLAN communication may take a longer time to establish during startup.

When using additional channels:

- The unit will 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.

For more information about how to use AT commands, see the AT Commands Reference Guide or the **Help** page in the web interface.

For information on possible channels to include, see [WLAN Channels and World Mode \(page 26\)](#).

#### Procedure

Enable or Disable World Mode and add WLAN channels.

1. To Enable or Disable World Mode.

- Enable World Mode

```
AT*WMM=1
```

- Disable World Mode:

```
AT*WMM=0
```

2. To include WLAN channels for connection and roaming, use the AT Command **AT\*WSCHL=<channel\_list>,<store>**.

Example 1. Add 2.4 GHz channels

2.4 GHz system with Access Points in channel 1, 6 and 11. There is no 5 GHz channels.

```
AT*WSCHL=1,6,11,1
```

Example 2. Add both 2.4 GHz and 5 GHz channels

2.4 GHz channels: 1, 6 and 11

5 GHz channels: 36, 40, 44, 48

```
AT*WSCHL=1,6,11,36,40,44,48,1
```

3. For the change to take effect, reboot the Bolt Serial.  
Send the Reboot device AT Command:

```
AT*AMREBOOT
```

## 5.9. Configure Settings in the Built-In Web Interface

### 5.9.1. Network Settings

The screenshot displays the Network Settings page. On the left, there is a sidebar with a 'Network Settings' tab and two buttons: 'Save and Reboot' (yellow) and 'Cancel All Changes' (red). The main content area contains the following settings:

- IP Assignment:** Static (dropdown menu)
- IP Address:** 192.168.0.99 (text input)
- Subnet Mask:** 255.255.255.0 (text input)
- Default Gateway:** 192.168.0.99 (text input)

Two important warnings are displayed in red boxes:

- 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.

Below the warnings, the following settings are visible:

- Internal DHCP Server:** DHCP Server Enabled (dropdown menu with a green info icon)
- DHCP Interfaces:** Wired Ethernet (dropdown menu with a green info icon). A dropdown menu is open showing options: All, Wired Ethernet (highlighted), and Wireless Interfaces.

Another important warning is shown:

- 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.

The **Start Address (Y)** is set to 201 (text input).

A **DHCP Table** is shown with the following data:

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

Figure 10. Network Settings page

Setting	Description
IP Assignment	Select static or dynamic IP addressing (DHCP).
IP Address	Static IP address for the unit. When you click <b>Save and Reboot</b> , the browser is redirected to the new address (not supported by all browsers).
Subnet Mask	Subnet mask when using static IP.
Default Gateway	Default gateway when using static IP.
Internal DHCP Server	<b>Disabled:</b> No internal DHCP functionality. <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. <b>DHCP Server Enabled:</b> Activates an internal DHCP server. This option is only available when IP Assignment is set to Static. To avoid IP address conflict if a DHCP server is already active on the network, use the DHCP Interfaces setting to limit the internal DHCP server to the correct interface.
DHCP Interfaces	The DHCP Interfaces function is available when <b>Internal DHCP Server &gt; DHCP Server Enabled</b> is selected. <b>All:</b> By default, the DHCP Interfaces function is set to use all interfaces. <b>Wired Ethernet:</b> The internal DHCP server only listens for clients on the wired Ethernet interface. <b>Wireless Interfaces:</b> 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 <b>X.X.X.Y</b> . <b>X</b> is taken from the current static IP address setting, and <b>Y</b> is the value in <b>Start Address</b> . Already allocated addresses will be skipped, including the address of the unit itself. The subnet mask setting is ignored.

Setting	Description
	Example 3. Start address 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.

### 5.9.2. Layer 3 IP Forward Connectivity Considerations

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.

### 5.9.3. WLAN Settings General

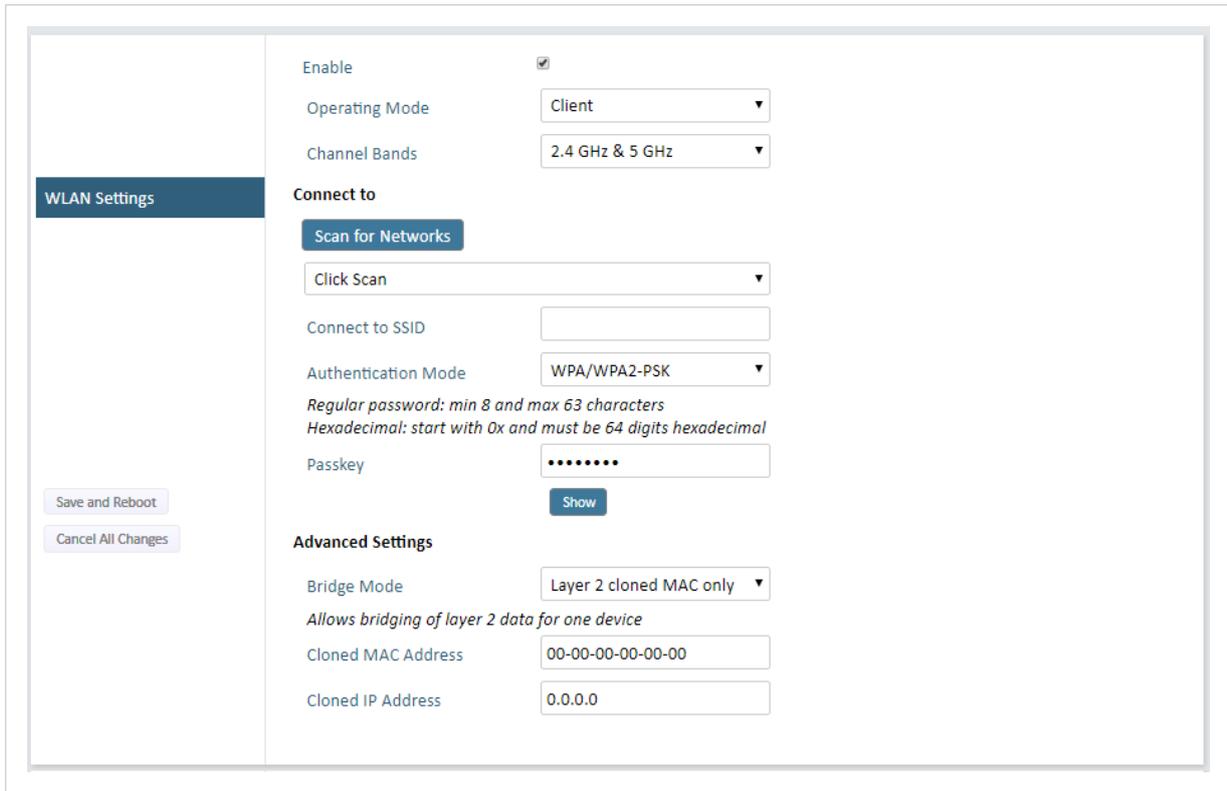


Figure 11. WLAN Settings page

Setting	Description
Enable	Enable/disable the WLAN interface.
Operating Mode	Choose operation as WLAN <b>Client</b> or <b>Access Point</b> . When <b>Access Point</b> is selected, additional settings will be available.
Channel Bands	<div style="border: 1px solid gray; padding: 5px; margin-bottom: 5px;">  <b>NOTE</b> 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> Choose to scan only the 2.4 GHz or 5 GHz channel band, or both (default).

### 5.9.4. WLAN Settings for Client

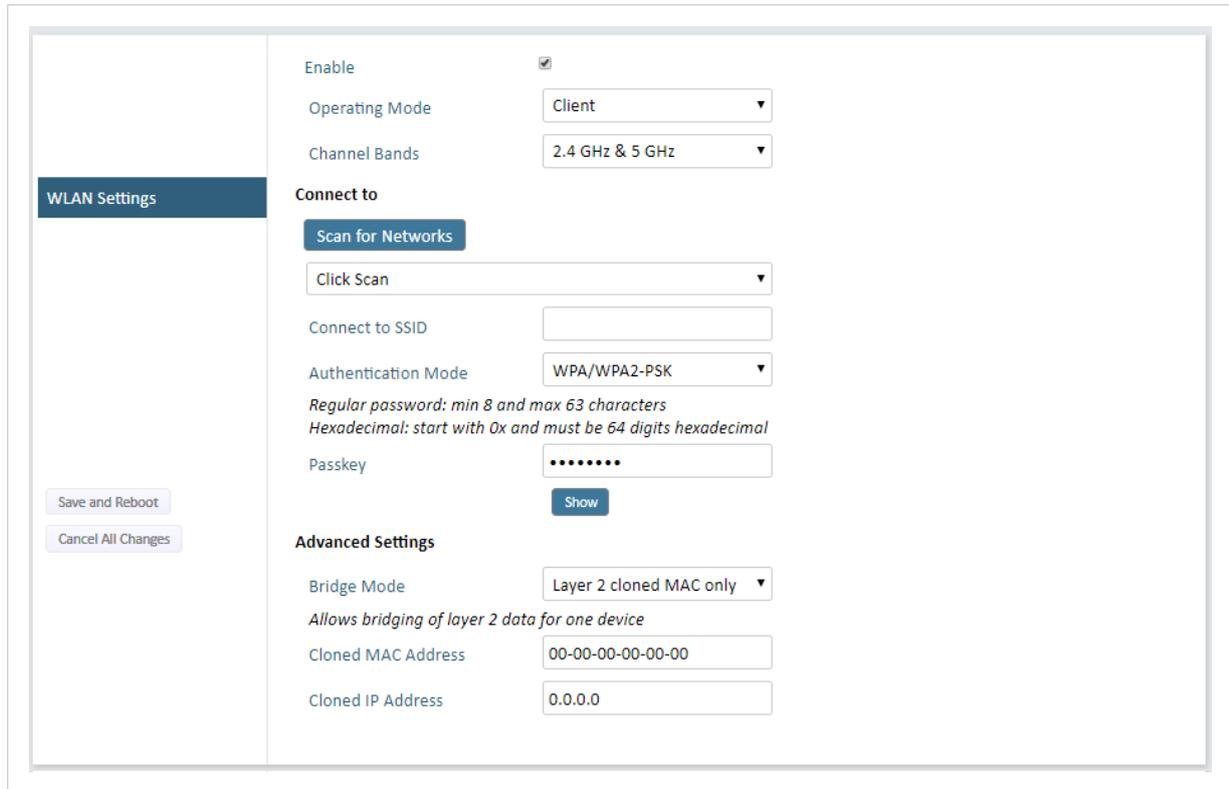


Figure 12. WLAN Settings page

#### Connect to settings for Client

Setting	Description
Scan for Networks	To scan the selected frequency band(s) for discoverable WLAN networks, click <b>Scan for Networks</b> . Select a network from the drop-down 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. When <b>Open</b> is selected there is no encryption or authentication.
Passkey	When using WPA/WPA2-PSK or WEP64/128, enter the passkey.
Username, Domain, Passphrase	Authentication details when using LEAP or PEAP (WPA2 Enterprise).

### 5.9.5. WLAN Roaming

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.

See also [Enable Fast Roaming with AT Commands \(page 19\)](#).

### 5.9.6. WLAN Channels and World Mode

WLAN Channels and World Mode is only used for Client Mode.



#### NOTE

The maximum output power will be reduced on some channels depending on regulatory requirements.

Which channels are available for WLAN communication is restricted by the regulatory domain where the unit is operating.

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.

Table 3. Regulatory domains and WLAN channels

Domain	2.4 GHz	5 GHz
WORLD	1-11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140
ETSI	1-11, 12, 13	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165
FCC	1-11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140

See also [Add Additional WLAN Channels with AT Commands \(page 20\)](#).

### 5.9.7. WLAN Settings for Access Point

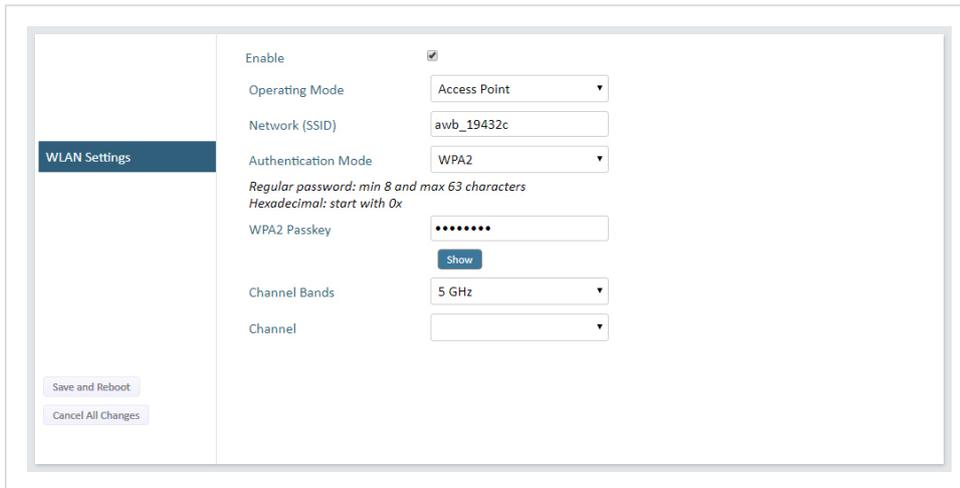


Figure 13. WLAN Settings page

#### Connect to settings for Access Point

The following settings are specific for Access Point mode:

Setting	Description
Network (SSID)	Enter an SSID (network name) for the Bolt Serial. 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. When <b>Open</b> is selected there is no encryption or authentication. When <b>WPA2</b> is selected WPA2 PSK authentication with AES/CCMP encryption is used.
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 <a href="#">WPA2 Password Examples (page 27)</a> .
Channel Bands, Channel	Select the WLAN channel band and channel to use for the Access Point. Valid channels are 1 to 11 for the 2.4 GHz band and 36, 40, 44, 48 for the 5 GHz band.

#### WPA2 Password Examples

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

#### Example 4. Plain text password

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&mp;43**

#### Example 5. Hexadecimal password example

**0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f**

### 5.9.8. WLAN Advanced Settings

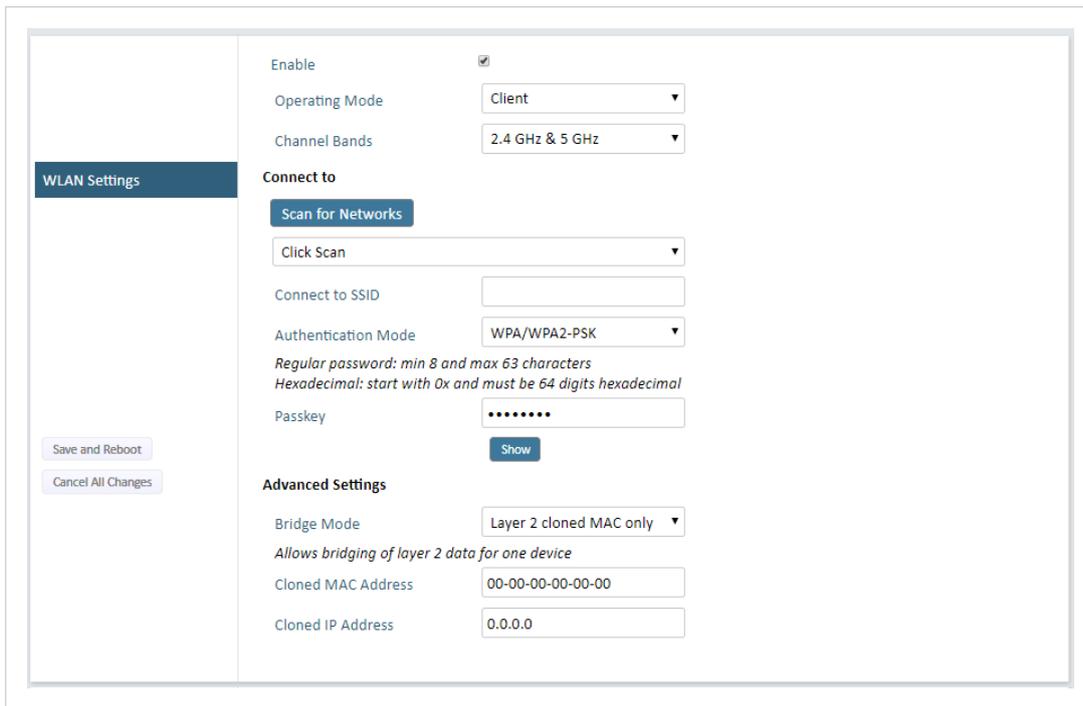


Figure 14. WLAN Settings page

#### Advanced Settings

Setting	Description
Bridge Mode	<p><b>Layer 2 tunnel:</b> 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.</p> <p><b>Layer 2 cloned MAC only:</b> Layer 2 data from only a single MAC address (specified below) will be bridged over WLAN (many-to-one).</p> <p><b>Layer 3 IP forward:</b> Default setting. IP data from all devices will be bridged over WLAN. This mode must be used when using the DHCP Relay function. See <a href="#">Layer 3 IP Forward Connectivity Considerations (page 23)</a>.</p>
Cloned MAC Address	The MAC address to use with <b>Layer 2 cloned MAC only</b> .
Cloned IP Address	The IP address to use with <b>Layer 2 cloned MAC only</b> .

### 5.9.9. Bluetooth Settings General

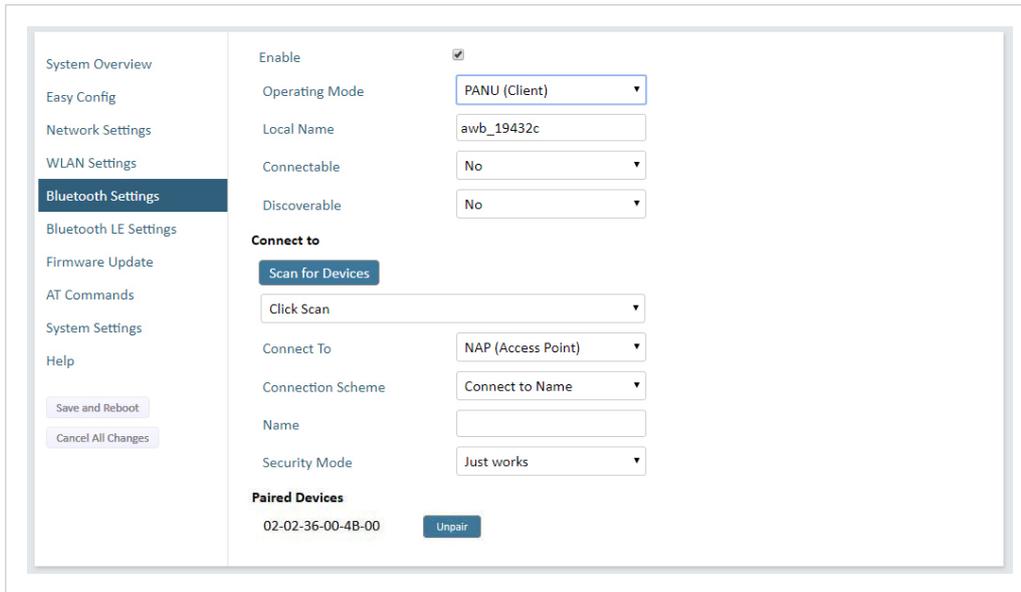


Figure 15. Bluetooth Settings page

#### General settings

Setting	Description
Enable	Enable/disable the Bluetooth interface.
Operating Mode	<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. <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.
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.

#### Connect to settings

Setting	Description
Security Mode	<b>Disabled:</b> No encryption or authentication. <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. <b>Just Works:</b> Encrypted connection without PIN code.

#### Paired devices

The currently connected Bluetooth devices DHCP Client-ID are listed in the **Paired devices** panel.

To unpair a devices, click **Unpair**.

### 5.9.10. Bluetooth Settings for PANU Mode

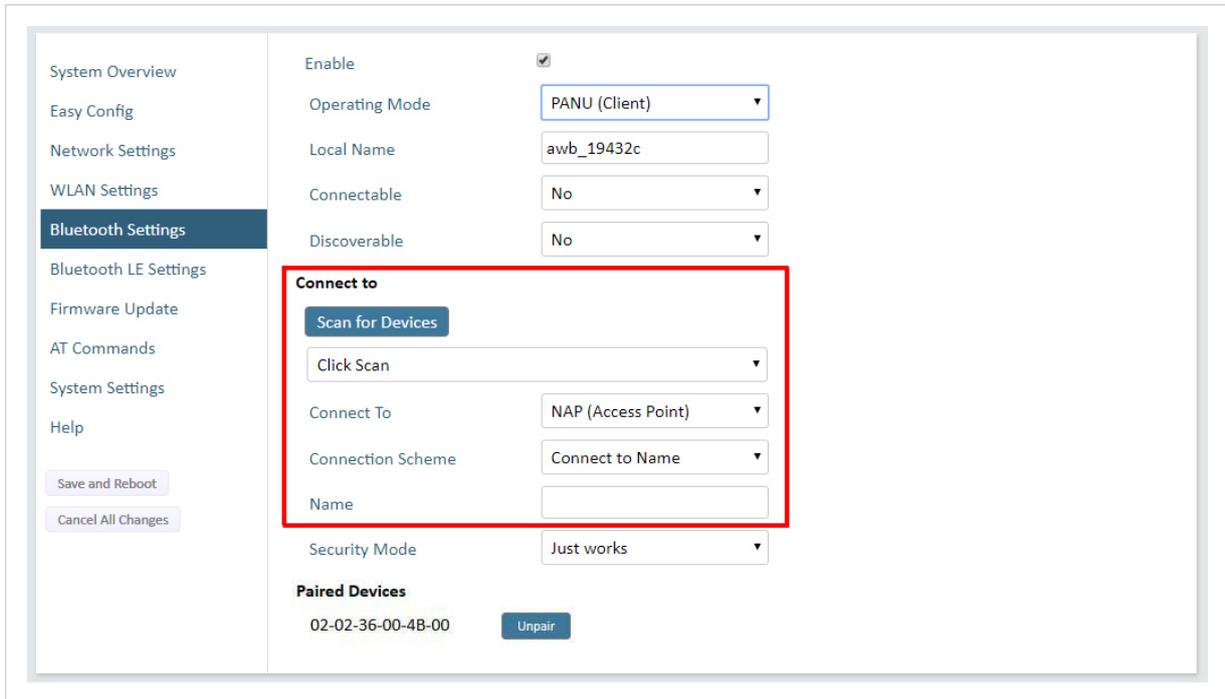


Figure 16. Bluetooth Settings page

#### Connect to settings for PANU Mode

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

### 5.9.11. Bluetooth Settings for NAP Mode

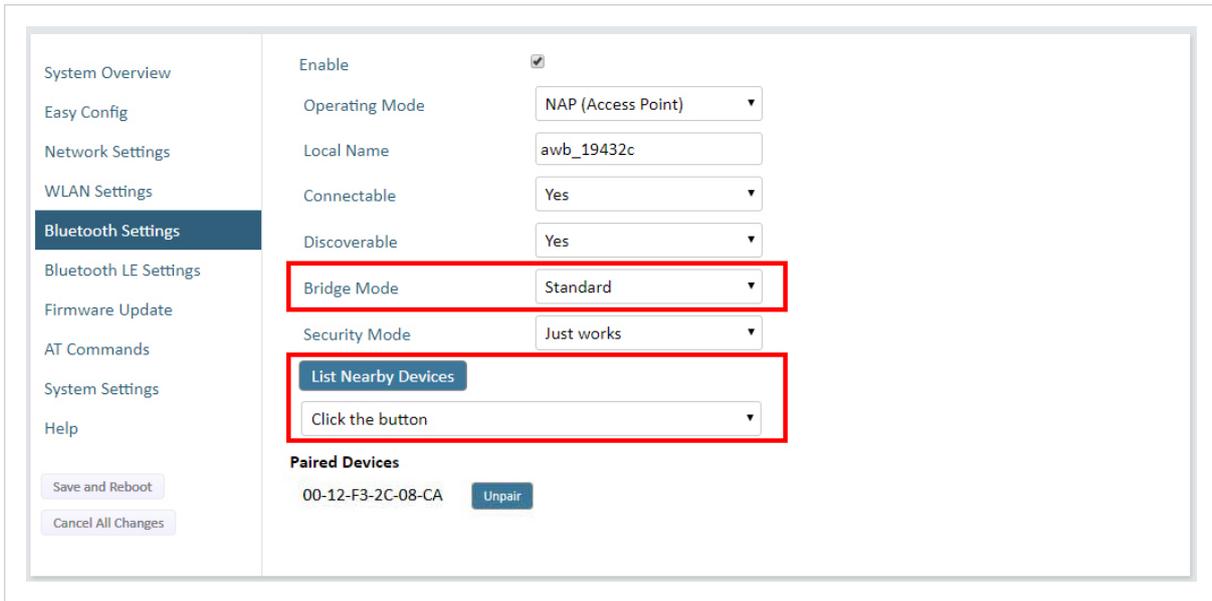


Figure 17. Bluetooth Settings page

#### Bluetooth Settings for NAP Mode

Setting	Description
Bridge Mode	<b>Standard:</b> 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.

### 5.9.12. Set Up Serial Communication

- System Overview
- Easy Config
- Network Settings
- WLAN Settings
- Bluetooth Settings
- Serial Settings
- Firmware Update
- AT Commands
- System Settings
- Help

Save and Reboot

Cancel All Changes

Operating Mode		RS232 ▼
Baud Rate		9600 ▼
Data Bits		8 ▼
Parity		None ▼
Stop Bits		2 ▼
Modbus Optimization		<input checked="" type="checkbox"/>
TCP Mode		Server ▼
Modbus Gateway Mode		Modbus RTU ▼
TCP Port		502
Show Statistics		<input checked="" type="checkbox"/>

Serial Rx Statistics (Bytes)

Buffer Size	<b>512</b>
Used	<b>0</b>
Total	<b>0</b>
Dropped	<b>0</b>
Overrun	<b>0</b>
Underrun	<b>0</b>

Serial Tx Statistics (Bytes)

Buffer Size	<b>3072</b>
Used	<b>0</b>
Total	<b>0</b>
Dropped	<b>0</b>
Overrun	<b>0</b>
Underrun	<b>0</b>

Serial Settings example, TCP Mode Server with Modbus TCP to Modbus RTU Gateway function enabled

Figure 18. Serial Settings page, TCP Mode Server

The screenshot shows the 'Serial Settings' page. On the left is a navigation menu with 'Serial Settings' highlighted. The main area contains configuration fields: Operating Mode (RS232), Baud Rate (9600), Data Bits (8), Parity (None), Stop Bits (2), Modbus Optimization (checked), TCP Mode (Client), TCP Server IP (192.168.0.99), TCP Port (5005), and Show Statistics (checked). Below these are two statistics tables: 'Serial Rx Statistics (Bytes)' and 'Serial Tx Statistics (Bytes)'. Both tables show Buffer Size (512 for Rx, 3072 for Tx) and all other metrics (Used, Total, Dropped, Overrun, Underrun) as 0.

Serial Settings example, TCP Mode Client enabled

Figure 19. Serial Settings page, TCP Mode Client

### Serial Settings

 **NOTE** To avoid timing problems when different baud rates are set on the Master and the Slaves, set the lowest baud rate on the Master.

Setting	Description
Operating Mode	Select a physical serial communication interface, <b>RS232</b> , <b>RS422</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.

Setting	Description
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.

### 5.9.13. Serial Communication

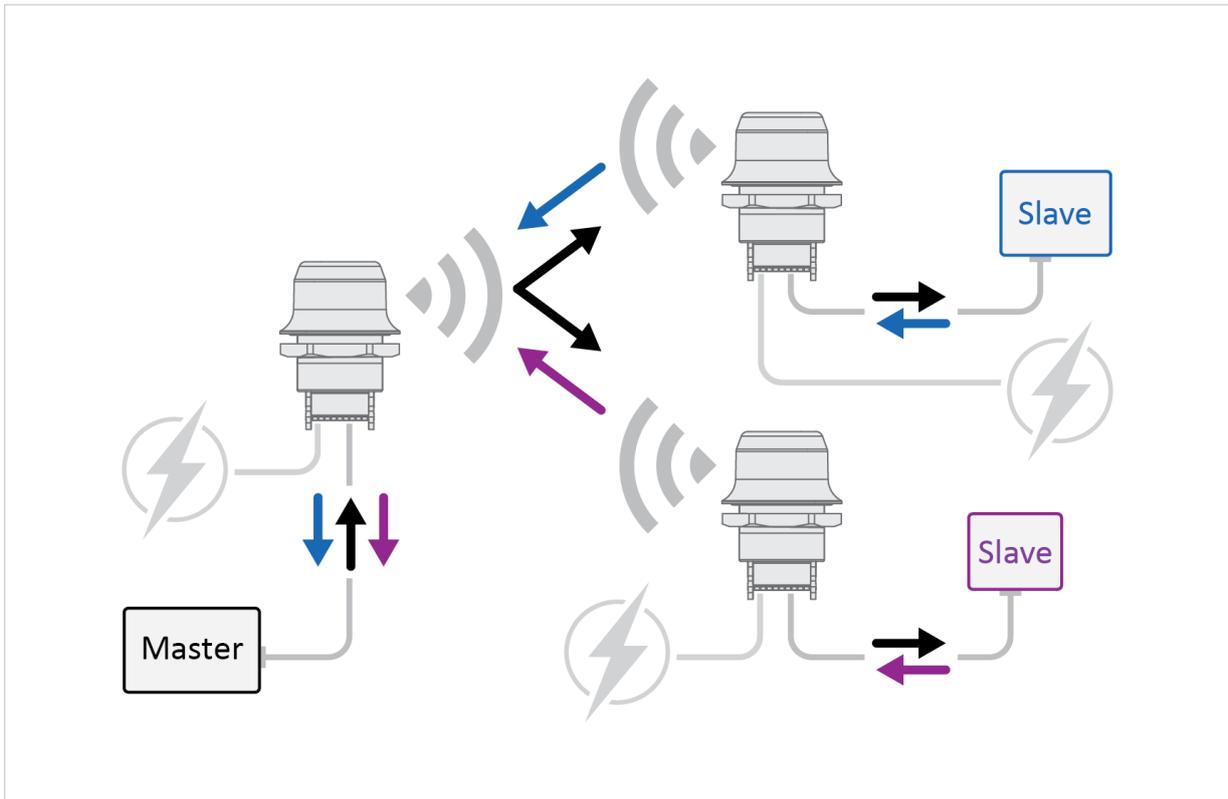
The serial functionality is used to transfer serial data from one point on a wireless link to another.

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.

Example 6. Point-to-multipoint link



Message sent from Master and response sent from Slaves

### 5.9.14. System Settings



**NOTE**

Setting a secure password for the unit is strongly recommended.

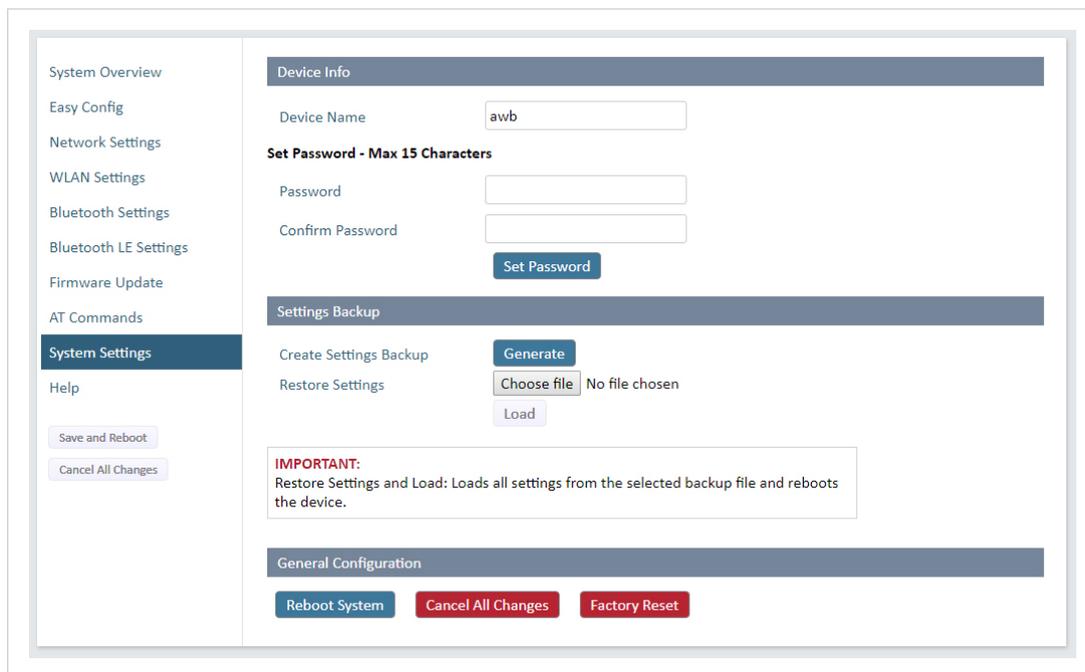


Figure 20. System Settings page

#### Device Info

Setting	Description
Device Name	Enter a descriptive name for the unit.
Password	Enter a password for accessing the web interface.

#### Settings Backup

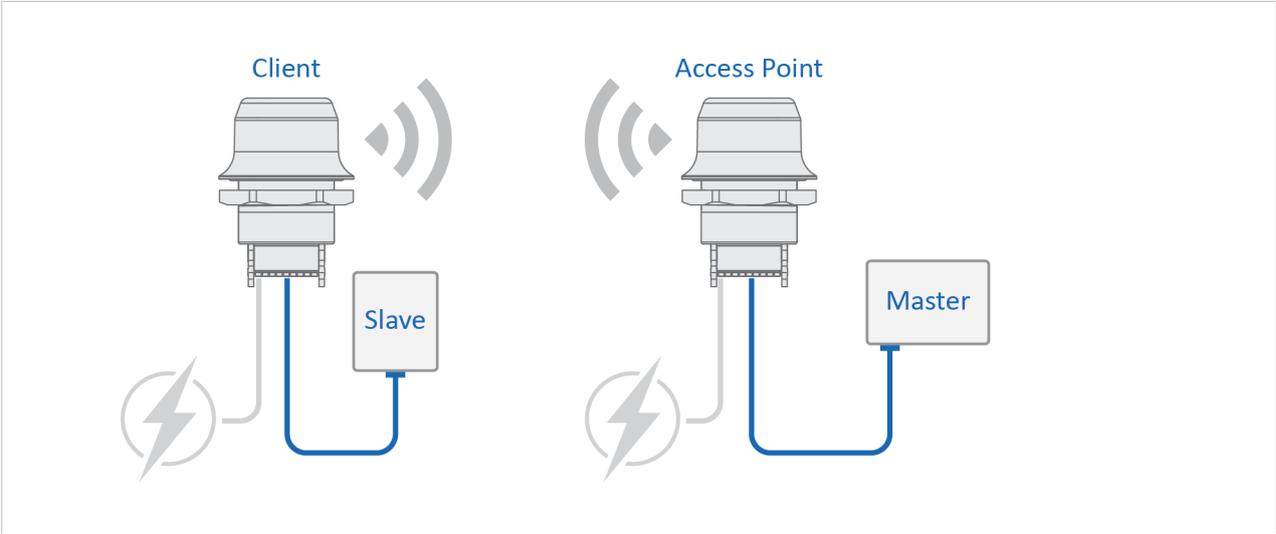
Setting	Description
Create Settings Backup	Click Generate to save the current configuration to a file on your computer.
Restore Settings	Click Choose file and select a previously saved configuration, then click Load. The settings in the saved configuration will be applied and the unit will reboot.

#### General Configuration

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

# 6. Use Cases

## 6.1. Bolt Serial Point-to-Point Installation



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

Figure 21. Bolt Serial Point-to-Point Installation

## 6.2. Set Up Wireless Infrastructure

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

### Procedure

#### Connecting the Devices

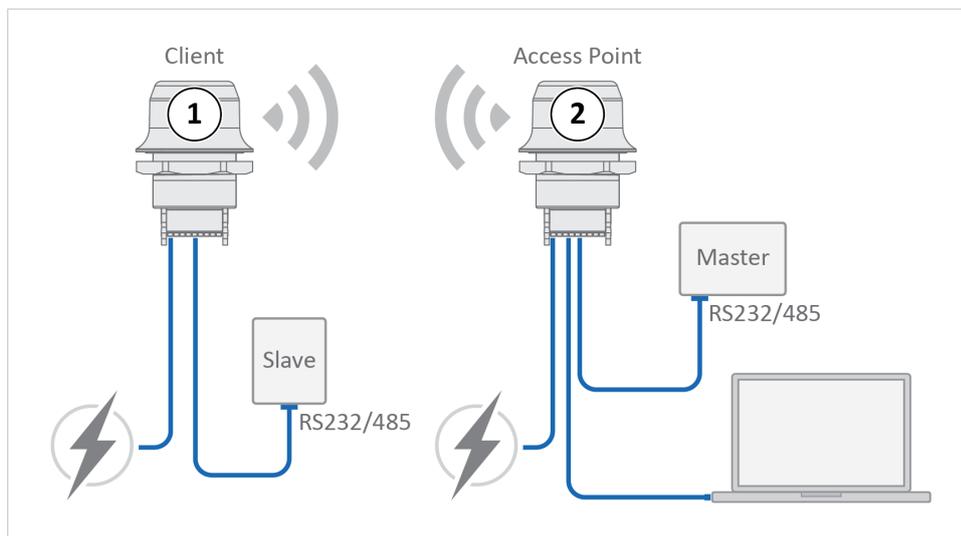


Figure 22. Serial bridge

1. Connect Client 1 to a Slave serial device. See also [Connect to LAN, Serial and Power](#).
2. Connect Access Point 2 to the Master device.
3. Connect Access Point 2 to your PC, with an Ethernet cable.
4. Connect Access Point 2 to power.

#### Activate Easy Config

1. Navigate to the web interface of Access Point 2.  
The default address to Access Point unit 2 is 192.168.0.99.
2. Activate one of the following Easy Config Modes:

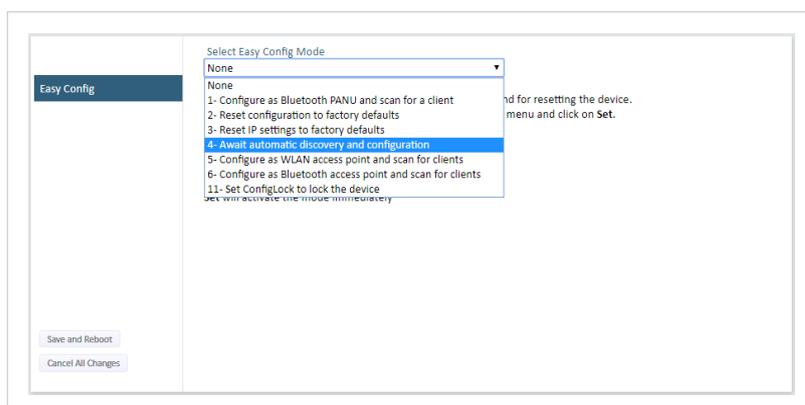


Figure 23. Easy Config modes menu

- 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 1 to power.
4. Automatic configuration of the units starts:
  - Client 1 starts up in Easy Config Mode 4 and is open for automatic configuration during 120 seconds.
  - Access Point 2 will discover and configure Client 1 as a Client and configure itself as an Access Point.
  - Client 1 will be assigned the first free IP address in the same Ethernet subnet as Access Point 2.  
The default address to Client 1 is 192.168.0.100.

#### Troubleshooting if no connection is established during Easy Config Mode

- Ensure that Client 1 is disconnected from Ethernet.
- Disconnect Client 1 from power and repeat the steps to activate Easy Config.

#### Add Additional Bolt Serial Clients

Option when using Easy Config Mode 1: Continue with the configuration, see [Serial Configuration \(page 40\)](#).

Option when using Easy Config Mode 5 or 6: You can add up to 6 additional Bolt Serial Clients to the serial bridge.

To add additional Clients:

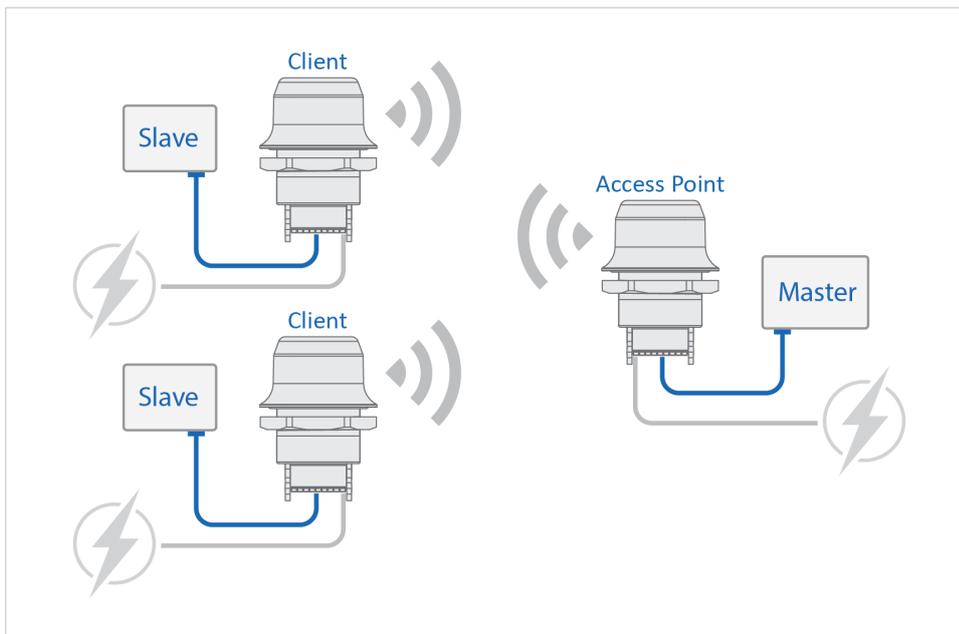


Figure 24. Serial bridge

1. Connect the Client to a serial device.
2. Automatic configuration of the Client starts.  
The Client will be assigned the next free IP address in the current Ethernet subnet.
3. To add more Clients, repeat step 1 and 2.

## Serial Configuration

System Overview	Operating Mode	RS232
Easy Config	Baud Rate	9600
Network Settings	Data Bits	8
WLAN Settings	Parity	None
Bluetooth Settings	Stop Bits	2
<b>Serial Settings</b>	Modbus Optimization	<input checked="" type="checkbox"/>
Firmware Update	TCP Mode	Client
AT Commands	TCP Server IP	192.168.0.99
System Settings	TCP Port	5005
Help	Show Statistics	<input checked="" type="checkbox"/>

Figure 25. Serial port settings example

1. From the PC connected to Access Point 2, navigate to the built-in web interface of each Bolt Serial Client.
2. Select the **Serial Settings** tab.
3. Configure the serial port settings, see [Set Up Serial Communication \(page 32\)](#).

## 6.3. Installing Multiple Bolt Serial Units

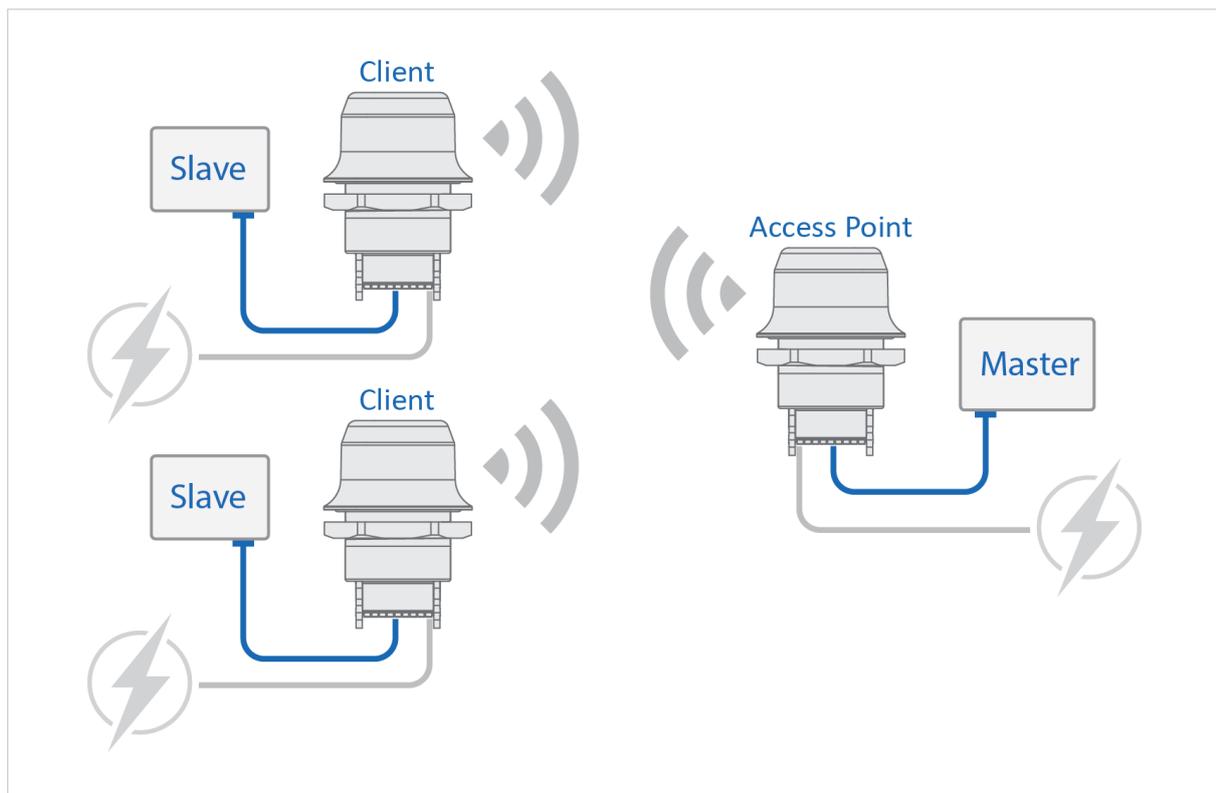


Figure 26. Installing Multiple Bolt Serial

When installing more than one Bolt Serial in the network infrastructure, configure the unit connected to the:

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

## 6.4. Installing on a Modbus Network

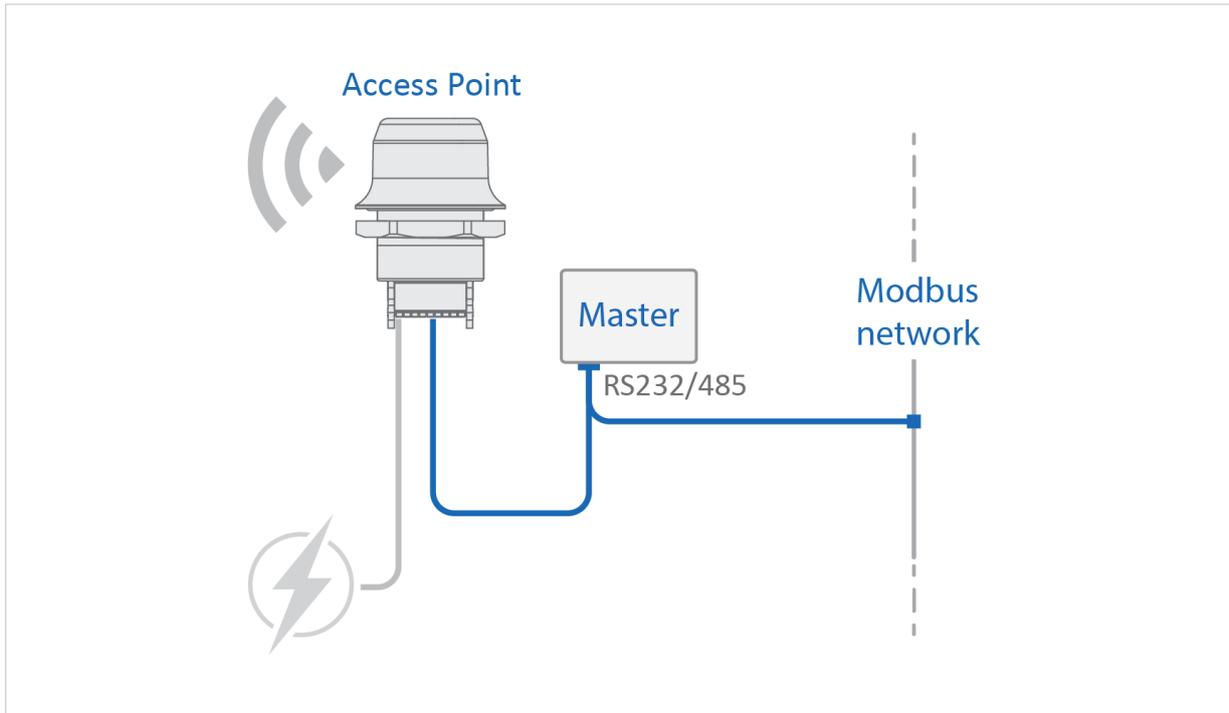


Figure 27. Access Point on Modbus network

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.

Modbus Optimization:

- In the Bolt Serial Access Point built-in web interface **Serial Settings** page, select the **Modbus Optimization** checkbox.

## 6.5. 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.

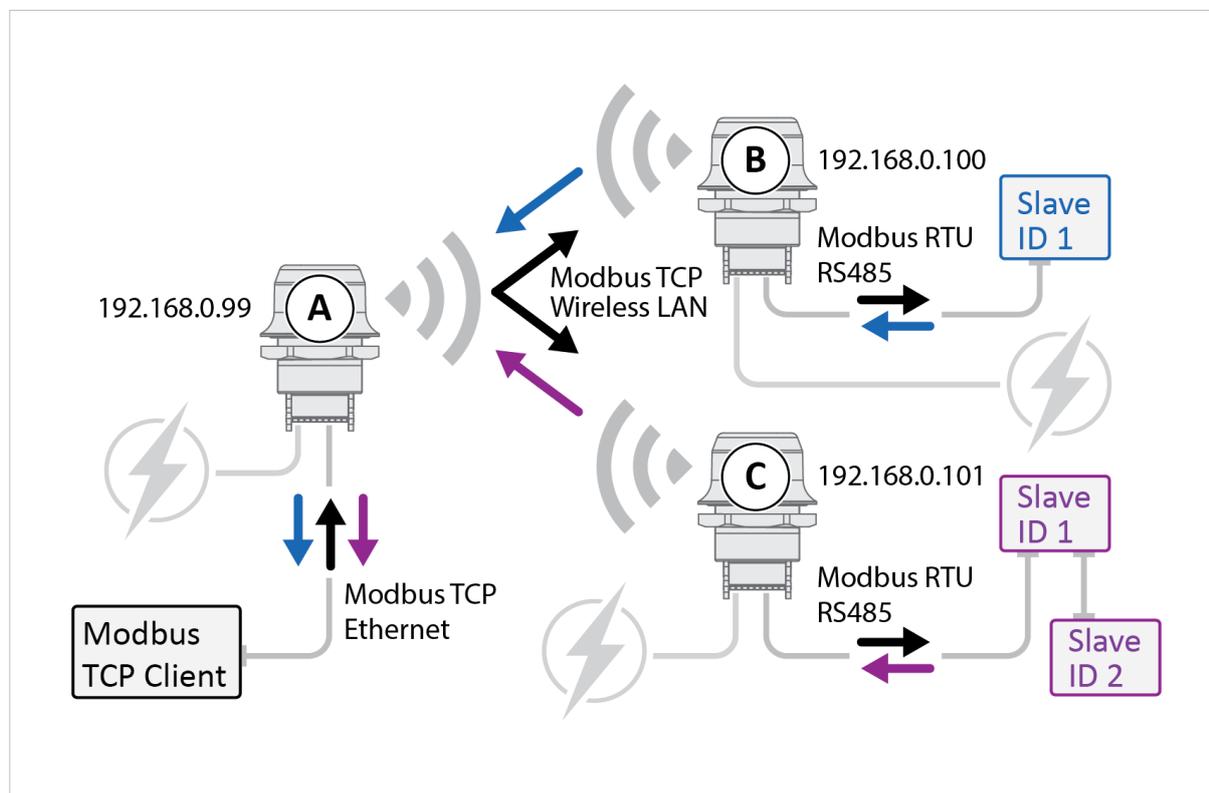


Figure 28. Serial bridge, Modbus RTU to RTU Gateway function

### Bolt Serial Access Point Unit

- 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).

### Connect the Modbus RTU Slaves

The Modbus RTU Slaves are all Modbus Servers.

- One of the Modbus RTU Slaves is 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.

### Modbus TCP Client Configuration

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

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

## 6.6. Bolt Serial TCP/IP Socket Protocol Description

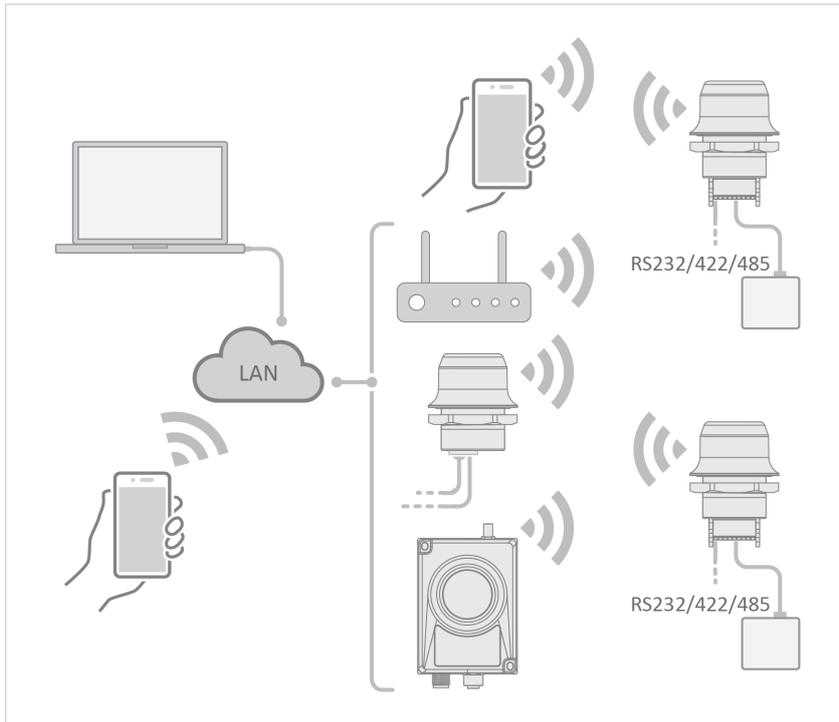


Figure 29. Bridge data to the Bolt Serial port

The Bolt Serial may communicate with raw TCP/IP traffic and bridge the data to RS232, RS422 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.

### 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.

# 7. Verify Operation

## 7.1. Network Connection Status

The **System Overview** page shows current settings and network connection status.

The screenshot displays the 'System Overview' page with a left-hand navigation menu and a main content area. The navigation menu includes: System Overview (selected), Easy Config, Network Settings, WLAN Settings, Bluetooth Settings, Bluetooth LE Settings, Firmware Update, AT Commands, System Settings, Help, Save and Reboot, and Cancel All Changes. The main content area is divided into several sections:

- 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; World Mode (1-11,36-140): Enabled; Channel: Auto; Channel Bands: 2.4 GHz & 5 GHz; Connect 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.
- Bluetooth LE:** Status: On; Operating Mode: Disabled.
- System:** Device Name: awb; Firmware: 1.6.3 [15:19:00, Aug 28 2018]; Uptime: 1 d, 4 h, 11 m, 14 s.

Figure 30. System Overview page example

## 8. Maintenance

### 8.1. Firmware Update

#### Before You Begin

**NOTE**

The configuration settings are not affected when updating firmware.

#### Download the Firmware Update File

1. Download the firmware update file from [www.anybus.com/support](http://www.anybus.com/support).
2. Connect Bolt Serial to your computer, refer to [Connecting to PC and Power](#).

#### Procedure

Update the Bolt Serial firmware.

The screenshot shows a web interface for firmware updates. On the left, there is a dark blue button labeled 'Firmware Update'. On the right, there is a form titled 'Firmware Update'. The form contains the following elements:

- A header bar with the text 'Firmware Update'.
- A label 'Current Version' with the value '0.0.0-latest-dev'.
- A label 'Firmware File' with a 'Choose File' button and the text 'No file chosen'.
- A 'Send' button.

Figure 31. Firmware Update, Choose file

1. Click **Choose File**.
2. In the **Open** dialog box, browse to and select the firmware update file and click **Open**.
3. To start the file transfer, click **Send**.

**NOTE**

Do not refresh or leave the Firmware Update page until the process has finished.

### Firmware update progress

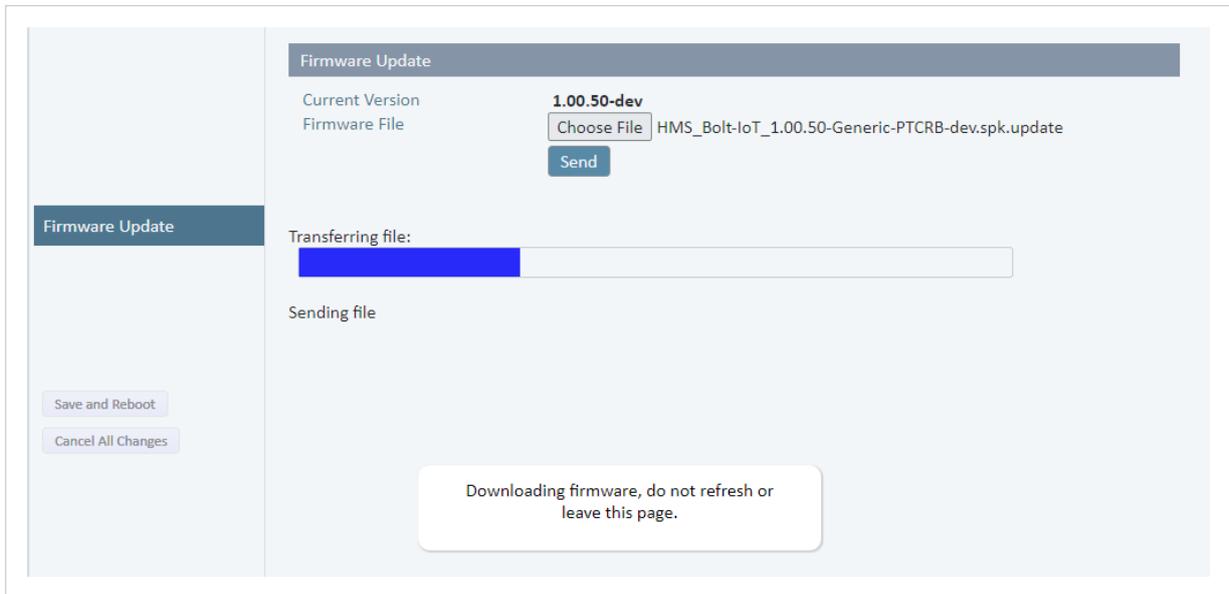


Figure 32. Firmware Update, Transferring file

- The progress bar, Transferring file, indicates the progress of the file transfer. Status messages show the progress of the firmware update stages.
- When the file transfer is finished, the progress bar turns green.

### Reboot

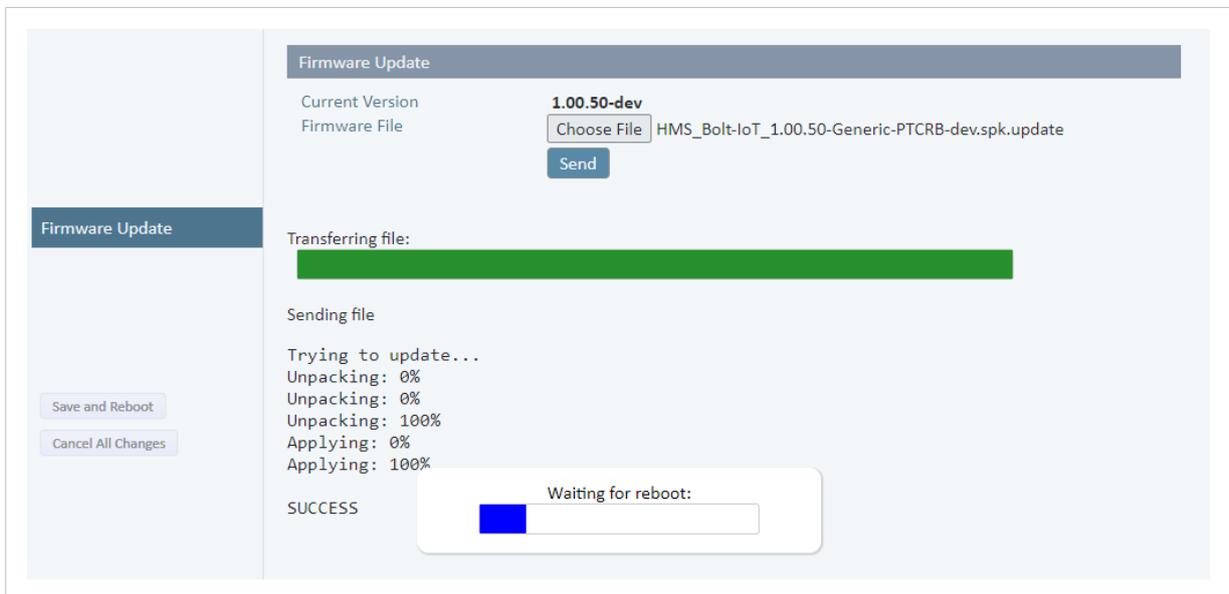
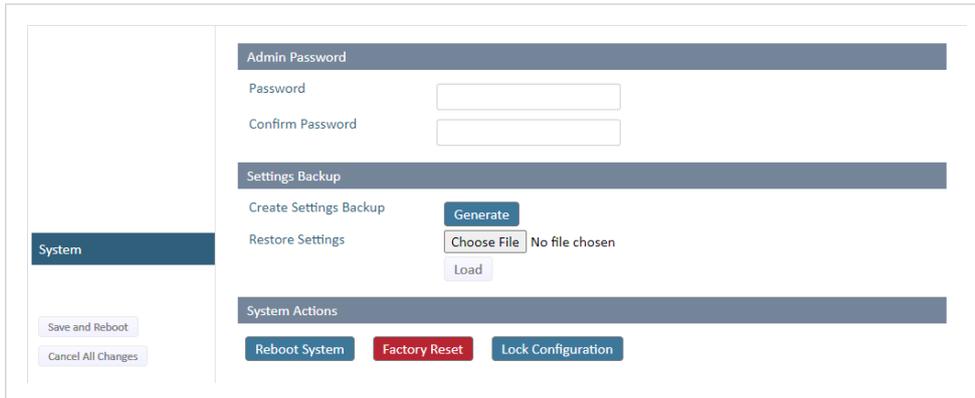


Figure 33. Firmware Update, Waiting for reboot

- When the firmware update is finished, Bolt Serial automatically reboots for the updates to take effect. The progress bar, Waiting for reboot, indicates the progress.
- When the reboot is complete, the web browser automatically redirects to the **System Overview** page.

## 8.2. Settings Backup

### 8.2.1. Create Settings Backup File



The screenshot shows the 'System' page of a device's web interface. On the left, there is a sidebar with 'System' selected. Below it are buttons for 'Save and Reboot' and 'Cancel All Changes'. The main content area is divided into three sections: 'Admin Password' with fields for 'Password' and 'Confirm Password'; 'Settings Backup' with a 'Generate' button and a 'Restore Settings' section containing a 'Choose File' button, the text 'No file chosen', and a 'Load' button; and 'System Actions' with buttons for 'Reboot System', 'Factory Reset', and 'Lock Configuration'.

Figure 34. System page

#### Create Settings Backup

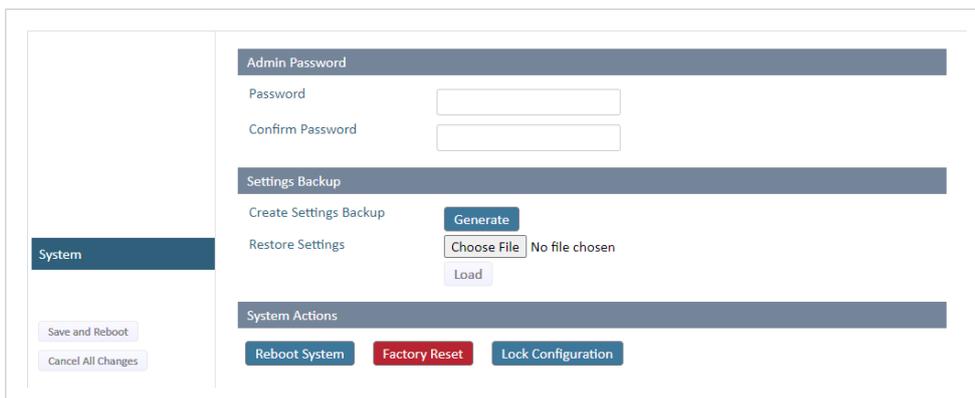
- To save the current configuration in a backup file, click **Generate**.  
A backup file is automatically downloaded and saved in the Downloads folder on your PC.

### 8.2.2. Restore Settings From Backup File



#### IMPORTANT

When you restore settings from a backup file, all the current settings are overwritten by the settings loaded from the backup file.



This screenshot is identical to Figure 34, showing the 'System' page. The focus is on the 'Restore Settings' section within the 'Settings Backup' area, which includes the 'Choose File' button, the text 'No file chosen', and the 'Load' button.

Figure 35. Restore Settings from a backup file

#### Restore settings from a backup file

- Click **Choose file**.
- Browse to and select your backup file.
- Click **Load**.  
The Bolt Serial reboot automatically, for the settings loaded from the backup file to take effect.

# 9. Troubleshooting

## 9.1. Reset Button

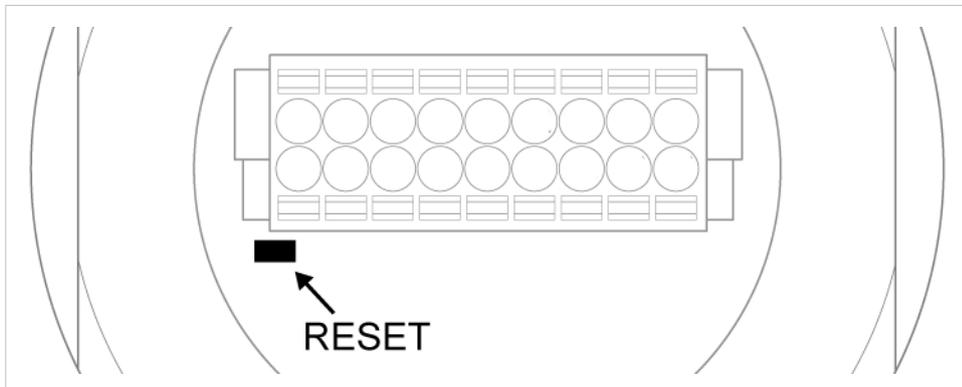


Figure 36. Reset button

The **Reset** button is located on the bottom of the Bolt Serial.

## 9.2. Recovery Mode

If the built-in web interface cannot be accessed, the unit can be reset by starting in Recovery Mode and reinstalling the firmware.

### Before You Begin



#### IMPORTANT

Use Recovery Mode only when the unit is unresponsive and the built-in web interface cannot be accessed. Firmware updates should normally be carried out through the built-in web interface.

### Procedure

#### To enter Recovery Mode

1. Press and hold **MODE** button during startup.

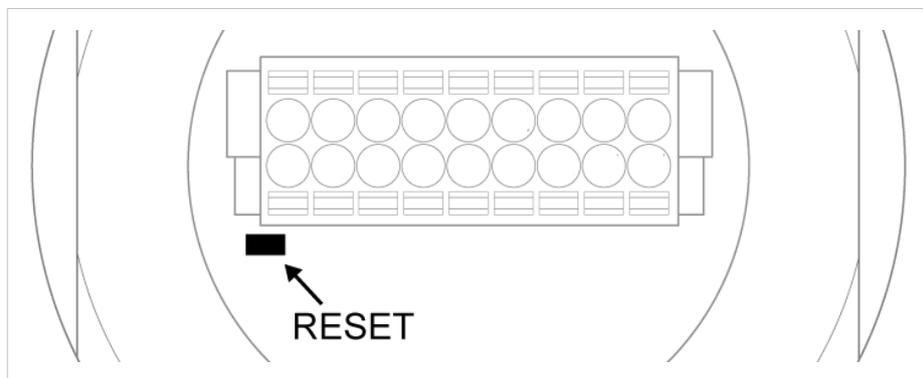


Figure 37. RESET button

2. Bolt Serial enters Recovery Mode.

#### To Reinstall the Firmware

1. To reinstall the firmware, you need Anybus Firmware Manager II. Download Anybus Firmware Manager II from [www.anybus.com/support](http://www.anybus.com/support).
2. Install Anybus Firmware Manager II on your PC.
3. Launch Anybus Firmware Manager II and follow the instructions to reinstall the firmware.

## 9.3. Reset to Factory Default

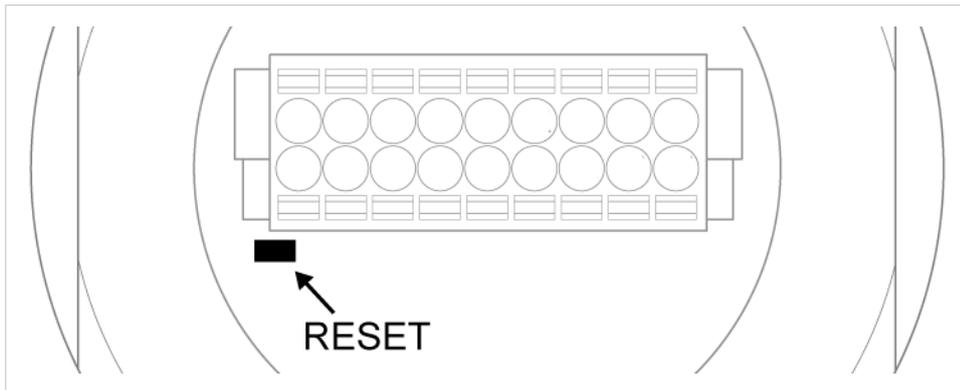


### IMPORTANT

If there is no Ethernet connection available after a factory reset, the Bolt Serial starts in the default Easy Config Mode 4.

Any one of these actions will restore the unit to factory default settings.

### Reset Using the RESET Button



Press and hold **RESET** for >10 seconds and then release it.

### Reset Via the Built-In Web Interface

Device Info

Device Name

Set Password - Max 15 Characters

Password

Confirm Password

Settings Backup

Create Settings Backup

Restore Settings  No file chosen

**IMPORTANT:**  
Restore Settings and Load: Loads all settings from the selected backup file and reboots the device.

General Configuration

Launch the built-in web interface > On the **System Settings** page, click **Factory Restore**.

### Reset Using Easy Config

To reset Bolt Serial to factory default, execute Easy Config Mode 2.

See [Activate an Easy Config Mode in the Built-In Web Interface \(page 17\)](#).

### **Reset Using AT Command**

To reset Bolt Serial to factory default, issue the AT command **AT&F** and then restart the unit.

See [Configuration with AT Commands \(page 18\)](#).

### **Reset Using Digital Input**

To reset Bolt Serial to factory default, apply voltage to the digital input for >10 seconds.

See [Connector \(page 7\)](#).

## 10. Technical Data

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

### 10.1. Technical Specifications

Order code	AWB2010	AWB2011
Color	Black	White top and black base
Connector	Included plug connector (2x9p; 3.5mm, Phoenix DFMC 1.5/9-ST-3.5, push-in spring connection).	
Range	Up to 100 meters free line of sight	
Antenna	One internal antenna. Dual-band 2,4GHz and 5GHz.	
Temperature compatibility	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	
Weight	81 g	
Housing material	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.	
IP protection class	IP66, IP67 and UL NEMA 4X for top (outside the host), IP21 for bottom (inside the host).	
Dimensions	Diameter: 68 mm. Height: 75 mm (95 mm including connector). Outside height: 41 mm.	
Mounting	M50 screw and nut (50.5 mm hole needed).	
Power	9-30 VDC (-5% +20%), Cranking 12V (ISO 7637-2:2011 pulse 4). Reverse polarity protection. (Consumption: 0.7W idle, 1.7W max.)	
Configuration	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.	
Vibration compatibility	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 $\pm 3.5$ mm, Acceleration: 2g. Shock test according to IEC 60068-2-27:2008 and with extra severities; Wave shape: half sine, Number of shocks: $\pm 3$ in each axes, Mode: In operation, Axes $\pm X,Y,Z$ , Acceleration: 30 g, Duration: 11 ms.	
Humidity compatibility	EN 600068-2-78: Damp heat, +40°C, 93% humidity for 4 days.	
Digital input	Usage: To control roaming between Bluetooth access points (NAP)	
Wired interface	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.	
Wireless LAN	Wireless standards: WLAN 802.11 a, b, g, n, d, r (fast roaming). Operation modes: Access point or Client WiFi channels: 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). RF output power: 13.75 dBm Max number of slaves for Access Point: 7 Power consumption: 54mA@24VDC Net data throughput: 20 Mbps. Link speed: max 65 Mbps (802.11n SISO) Security: WEP 64/128, WPA, WPA-PSK and WPA2, TKIP and AES/CCMP, LEAP, PEAP including MS-CHAP.	
Classic Bluetooth	Wireless standards (profiles): PANU & NAP Operation modes: Access point or Client	

Order code	AWB2010	AWB2011
	RF output power: 9.75 dBm Max number of slaves for Access Point: 7 Power consumption: 36 mA@24VDC Net data throughput: ~1 Mbps Bluetooth version support: Classic Bluetooth v2.1 Security: Authentication & Authorization, Encryption & Data Protection, Privacy & Confidentiality, NIST Compliant, FIPS Approved	

# 11. Reference Guides

## 11.1. RS232/RS485 Electrical Connection



**NOTE**

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

### RS232 Typical Connection

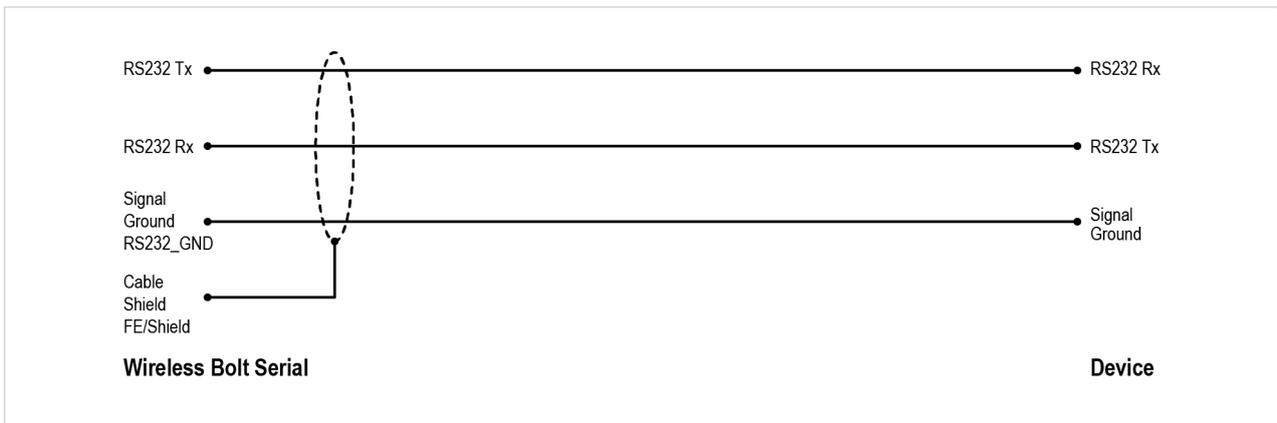


Figure 38. RS232 Typical Connection

### RS485 Typical Connection



**NOTE**

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

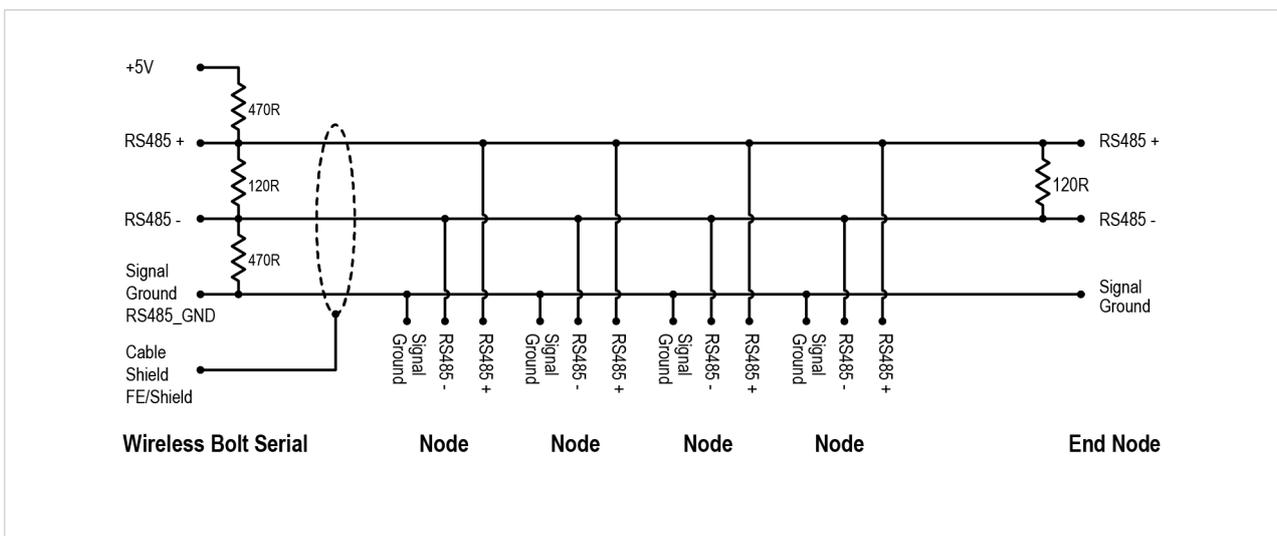


Figure 39. RS485 Typical Connection

## 11.2. Wireless Technology Basics

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

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

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

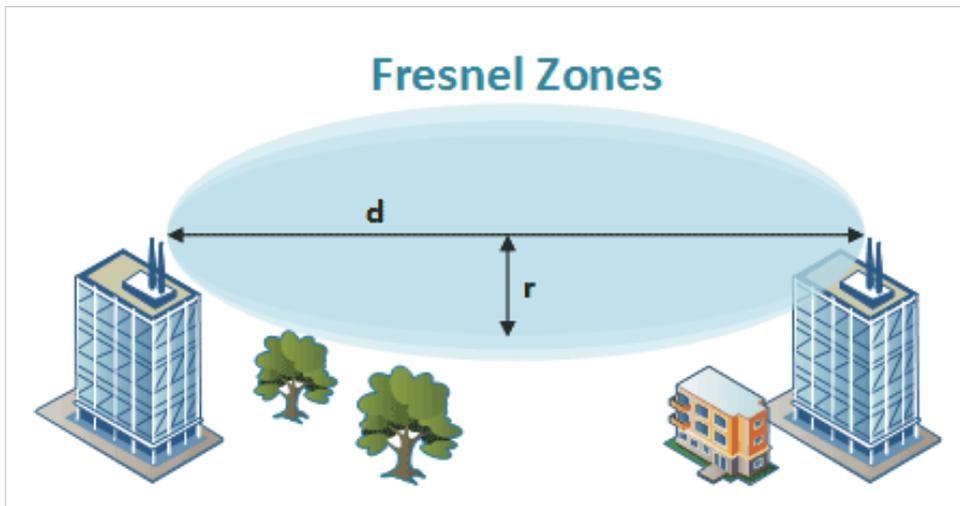


Figure 40. Fresnel zones

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.

### 11.3. 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.

#### 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.

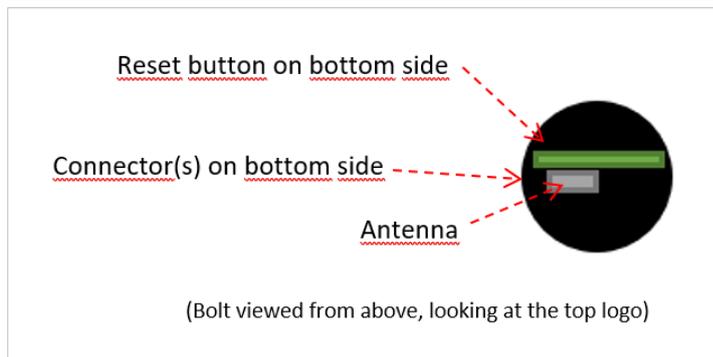


Figure 41. Bolt top view

#### Diagram Analysis



#### NOTE

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

The diagram displays an omnidirectional antenna gain regarding 2.4 GHz (blue line) which is used for Bluetooth and Wireless LAN 2.4 GHz.

It also shows that Wireless LAN 5 GHz (orange line) has a limited antenna gain in the approximate directions 105° to 190°, i.e. the 5 GHz range will be limited in this direction.

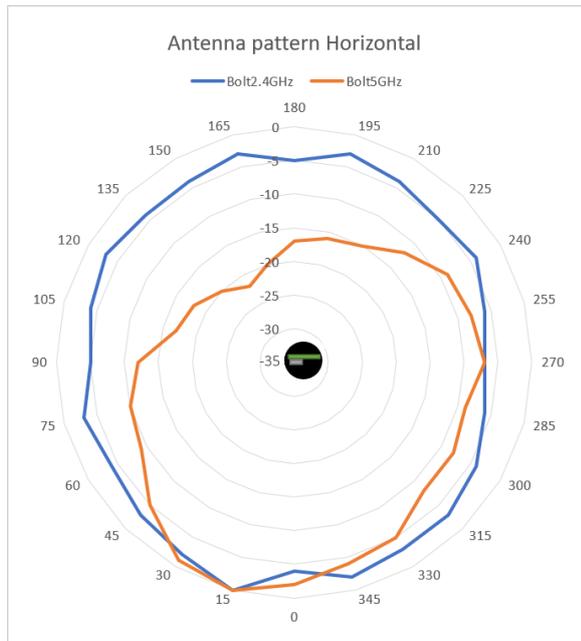


Figure 42. Antenna pattern Horizontal

### 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.

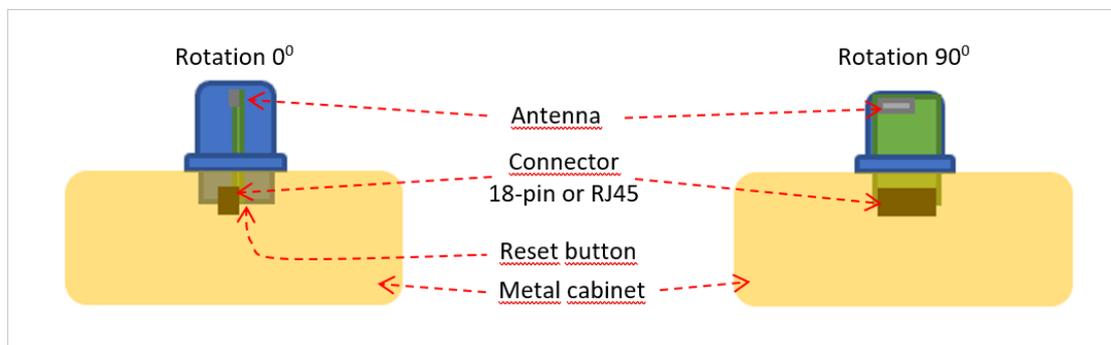


Figure 43. Antenna pattern, Bolt rotation 0° and 90°

### 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.

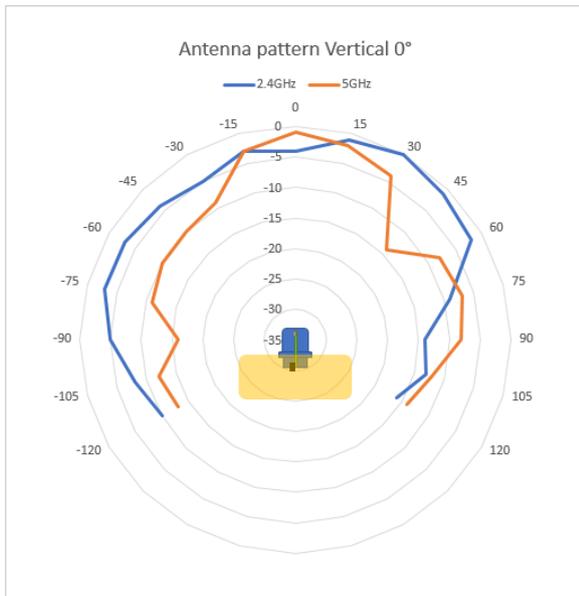


Figure 44. Front View – Vertical 0°

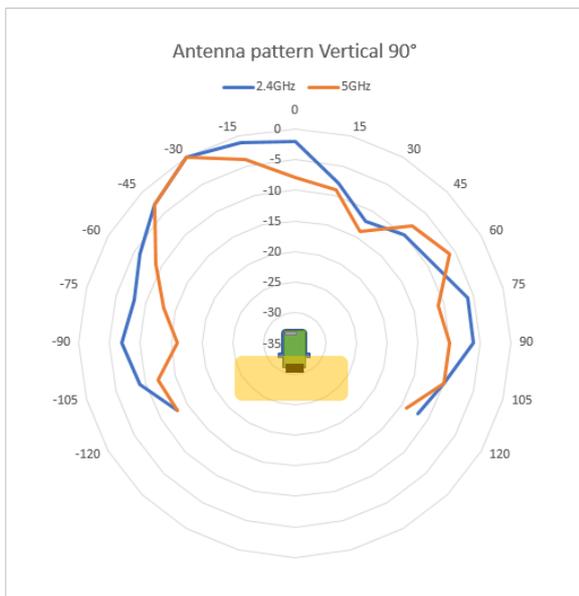


Figure 45. Side View – Vertical 90°

### Throughput Diagram

This diagram shows how data throughput decreases when distance increases.

The huge difference between using a back shield to focus the radio energy, and not using a back shield. Using a back shield 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.

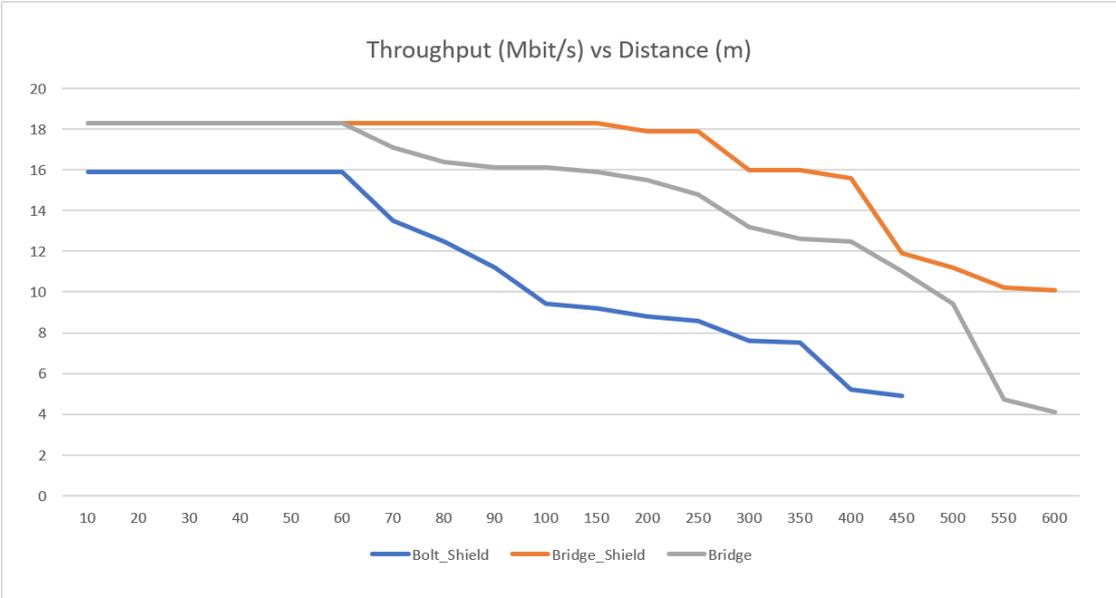


Figure 46.

This page is intentionally left blank.

# Mouser Electronics

Authorized Distributor

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

[HMS Networks:](#)

[AWB2010-B](#) [AWB2011-B](#)