ENGLISH

Anybus® Wireless Bolt Ethernet 18-Pin™

USER MANUAL

SCM-1202-007
Version 3.10
Publication date 2025-07-10

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.

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden

E-Mail: info@hms.se

Table of Contents

1. Preface

1.1. About This Document

This document describes how to install and configure Anybus® Wireless Bolt Ethernet 18-Pin™.

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.hms-networks.com/technical-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.hms-networks.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 Ethernet 18-Pin™ 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. Cybersecurity

3.1. General Cybersecurity

IMPORTANT
To physically secure equipment and to prevent unauthorized access, it is recommended to install the equipment in a environment with access control.

IMPORTANT
To maintain the cybersecurity of the Bolt 18-Pin, only connect its Local Area Network (LAN) port to a trusted network.

Networks that are outside your security measures, such as firewalls and network administration, are considered untrusted. These networks are more vulnerable to unauthorized access and other security threats.

Examples of trusted networks include:

- Internal Company Local Area Networks (LANs): Managed and secured by the IT department.
- Industrial Control System (ICS) Networks: Used to control and monitor industrial processes, and can be isolated from other networks.
- Direct Connections: For example, a laptop connected with a LAN cable directly to the Bolt 18-Pin.

IMPORTANT
The Bolt 18-Pin can be manipulated through the digital input without authentication.

To maintain the cybersecurity of the Bolt 18-Pin, only connect its digital input to trusted devices.

Unauthenticated or unmonitored devices are considered untrusted and more vulnerable to unauthorized access and other security threats.

For a device to be considered trusted, it must come from reputable sources that follow security policies.

Trusted devices are verified and regularly monitored to ensure they do not pose a security risk.

IMPORTANT
To reduce the risk of sensitive data exposure, always perform a factory reset before decommissioning the equipment.

A factory reset will reset any on-site made configuration changes and revert the Bolt 18-Pin to the default settings of the latest installed firmware version.

3.2. Security Advisories

For cybersecurity reasons, stay informed about new vulnerabilities and follow the recommended actions.

HMS Networks Security Advisories includes information about our product vulnerabilities and available solutions.

You find our Safety Advisories at www.hms-networks.com/cybersecurity/security-advisories.

3.3. How to Report a Vulnerability

HMS Networks place the utmost importance on the security of our products and systems, however, despite all the measures we take, it cannot be excluded that vulnerabilities persist.

To report a potential vulnerability in an HMS product or service, please visit www.hms-networks.com/cybersecurity/report-a-vulnerability and follow the instructions.

3.4. Product Cybersecurity Context

3.4.1. Bolt 18-Pin Interfaces

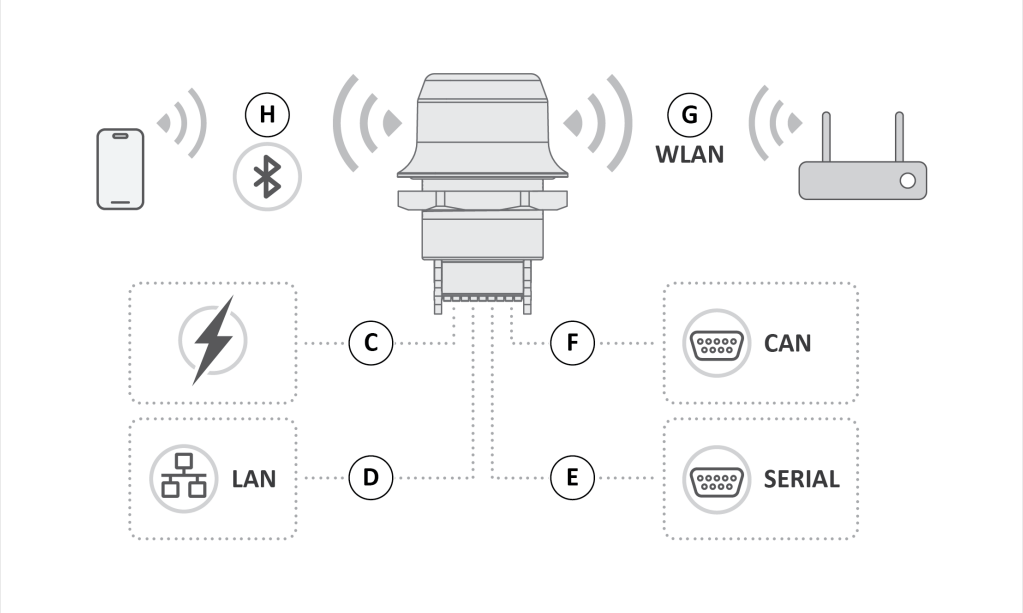


Figure 1. Bolt 18-Pin interfaces

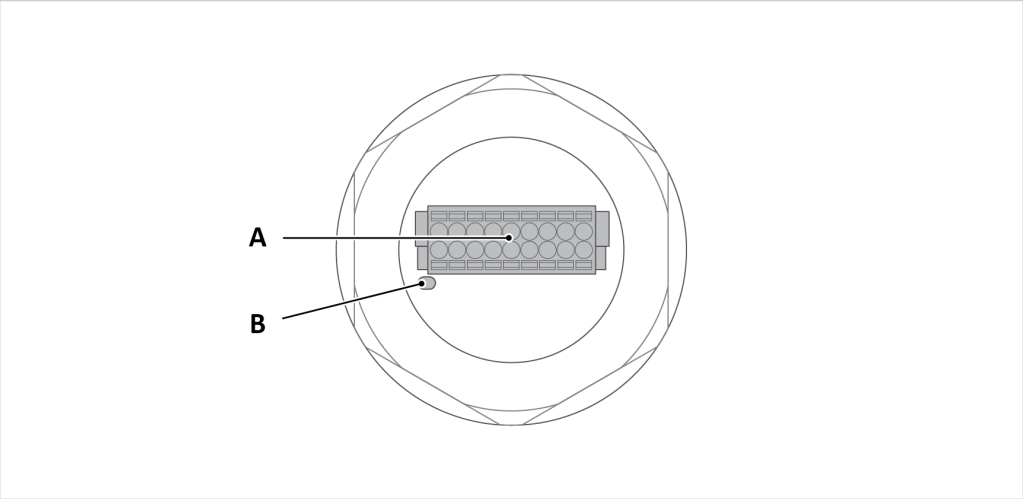


Figure 2. Bolt 18-Pin External parts

A. 18-pin socket connector
B. Reset button
C. Voltage Input (VIN) power, and Digital input interfaces
D. LAN interface
E. Serial RS232/RS485 interface
F. CAN interface
G. Bluetooth interface
H. WLAN interface

3.4.2. Services

Service	Description	Default Interface	Default Setting	Configurable Service
HTTP (Hypertext Transfer Protocol)	Enables configuration of the equipment over a network.	LAN	Restricted to local network only.	Restricted to local network only/ unrestricted.
DHCP (Dynamic Host Configuration Protocol) Server	Used to automatically assigns IP addresses and other network settings to devices on a network.	Applicable to all interfaces.	Off	Yes
Ping	Used by network devices to identify and locate other devices on a network.	Applicable to all interfaces.	On	No
Ethernet Tunnel	Used for tunneling of Ethernet Protocol Data Units (PDUs) between Anybus Wireless Bolt or Anybus Wireless Bridge II devices. Uses EtherType 0x6789.	Applicable to all interfaces.	Off	Yes
AT Command Interface on TCP/IP	Used for configuring the equipment. Default TCP port: 8080	LAN	Restricted to local network only.	Restricted to local network only/ unrestricted.
AT Command Interface on Ethernet	Used for configuring the equipment. Default EtherType: 0x0666	LAN	On	Yes

4. Preparation

4.1. Support and Resources

For additional documentation and software downloads, FAQs, troubleshooting guides and technical support, please visit www.hms-networks.com/technical-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.

4.2. Network Environment

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

4.3. Placement for Optimal Reception

Antenna Considerations

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

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 wireless devices should be observed.

See Wireless Technology Basics (page 71).

Required Distance Between Device and Human

At least 20 cm separation distance between the device and the user's body must be maintained at all times.

4.4. 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.
- 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.

4.5. 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.

4.6. 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

5. Installation

5.1. Mechanical Installation

Placement

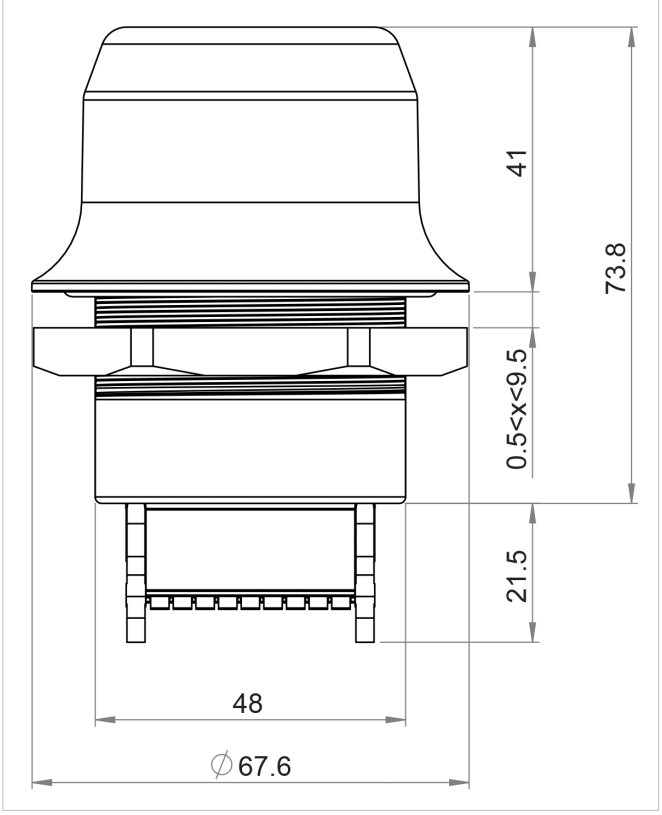
- The device is intended to be mounted on top of a machine or cabinet through an M50 (50.5mm) hole using the included sealing ring and nut.
- The top mounting surface, in contact with the sealing, must be flat with a finish equivalent to Ra 3.2 or finer and cleaned and free from oils and greases.

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 ±10 %



All measurements are in mm.

Figure 3. Installation drawing

5.2. 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.

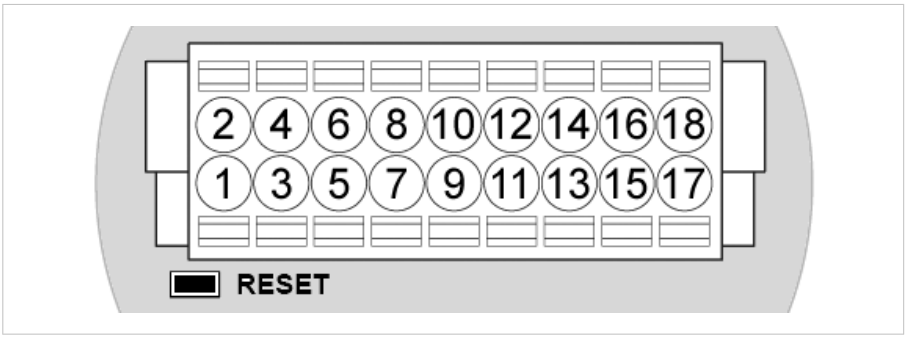


Figure 4. 18-Pin connector

The location of the **RESET** button can be used as a reference for the pin numbering when the connector is attached to the Bolt 18-Pin. Pin 1 will be the pin closest to the **RESET** button.

For information about the correct connection type and termination, refer to .

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
14	RS232_CTS	RS-232 Clear To Send
15	ISO_5V	Isolated 5 V for serial interface
16	RS232_GND/RS485_GND	Isolated Ground for Serial interface
17	CAN_L	CAN Low
18	CAN_H	CAN High

Note:

- 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.

5.3. Cabling

Before You Begin

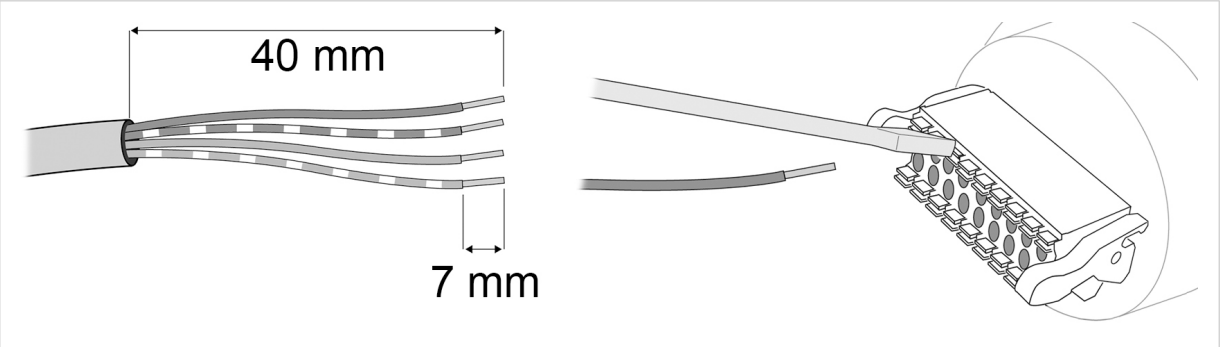
RJ-45 Adapter

An Ethernet adapter with an RJ45 female connector can be ordered as an accessory.

Please contact your sales representative for more information.

Procedure

Create connector cable for Bolt 18-Pin



1. Cut off one of the connectors on a standard Cat5e or Cat6 Ethernet cable.
2. Strip off about 40 mm (1½ inch) of the cable jacket and untwist the orange, orange/white, green and green/white wires.
   The other wires 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 10).
5. 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.

5.4. Reset Button

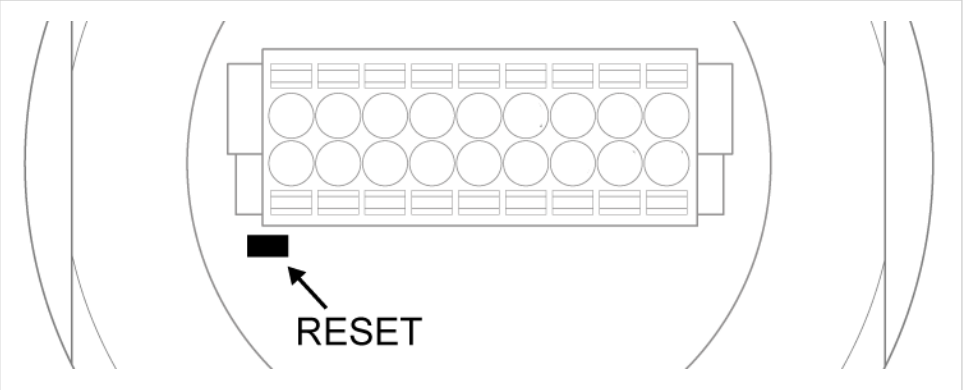


Figure 5. Reset button

The **Reset** button is located on the bottom of the Bolt 18-Pin.

6. Configuration

6.1. Available Easy Config Modes

Bolt 18-Pin may be configured using one of the pre-configured Easy Config modes.

NOTE
To cancel Easy Config mode 11, the unit must be reset to factory default settings. See Reset to Factory Default (page 65)

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 120 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.
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.
7	WLAN AP	The unit scans for other units in Config Mode 4 and configure them as Clients. Timeout occur after 120 seconds.
8	Bluetooth NAP	Restart as Access Point and connect Clients. Apply PROFINET optimization to all units. PROFINET messages will have priority over TCP/IP frames.
9	Bluetooth PANU	Configure unit as a Client and scan for another Client (PANU to PANU). Apply PROFINET optimization to both units. The unit listens for 120 seconds or until a configuration is established.
10	(any)	Apply PROFINET optimization and restart. No other configuration settings are changed.
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.

6.2. Bolt 18-Pin Built-In Web Interface

The Bolt 18-Pin built-in web interface is used to configure, maintain and troubleshoot the Bolt 18-Pin. 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 16).

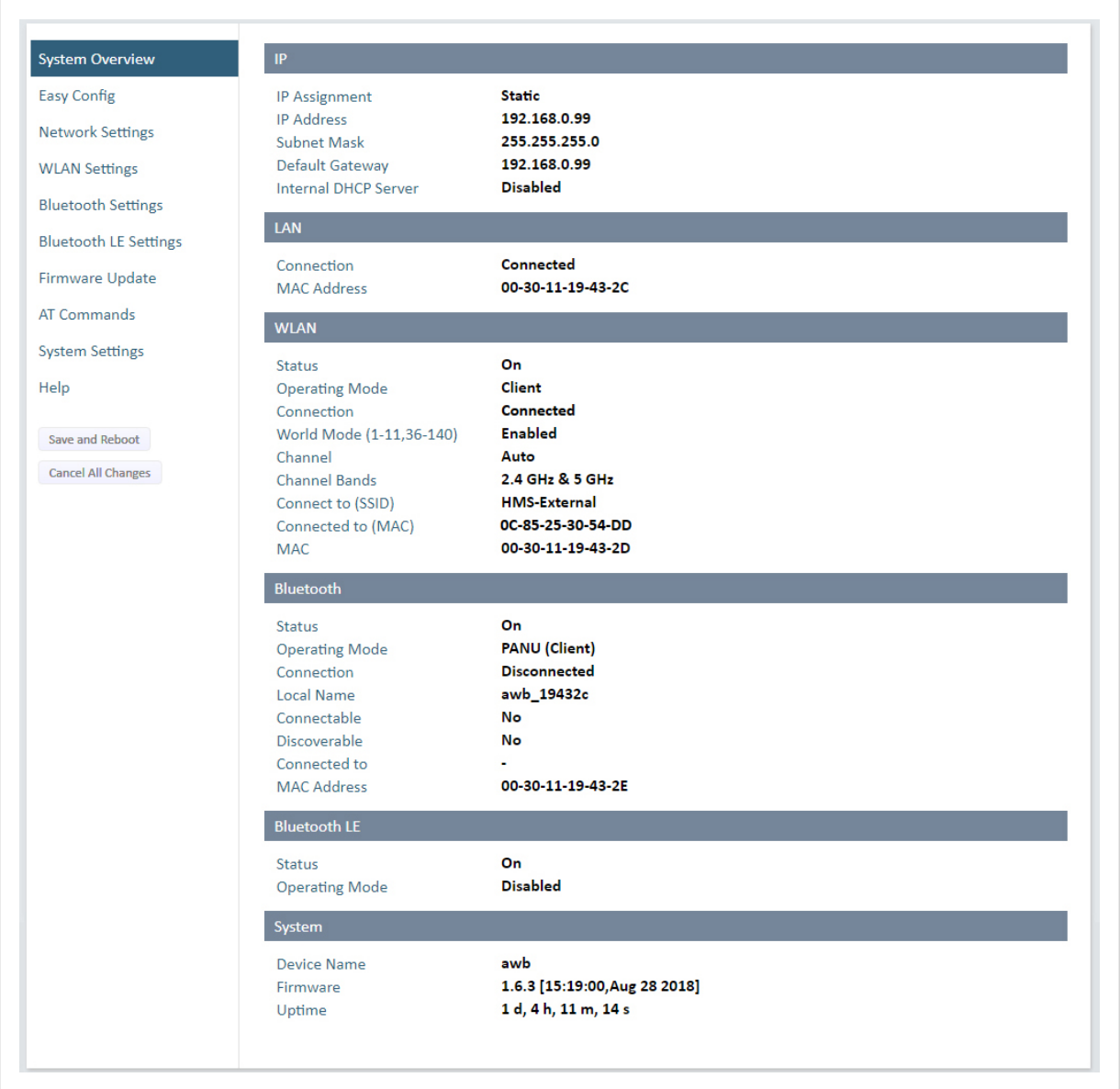


Figure 6. System Overview page example

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.

6.3. Connect to Configure

Initial Setup and Factory Reset

For initial setup or after a factory reset: To configure the Bolt 18-Pin using its built-in web interface, it must be connected to a PC via an Ethernet cable.

Procedure

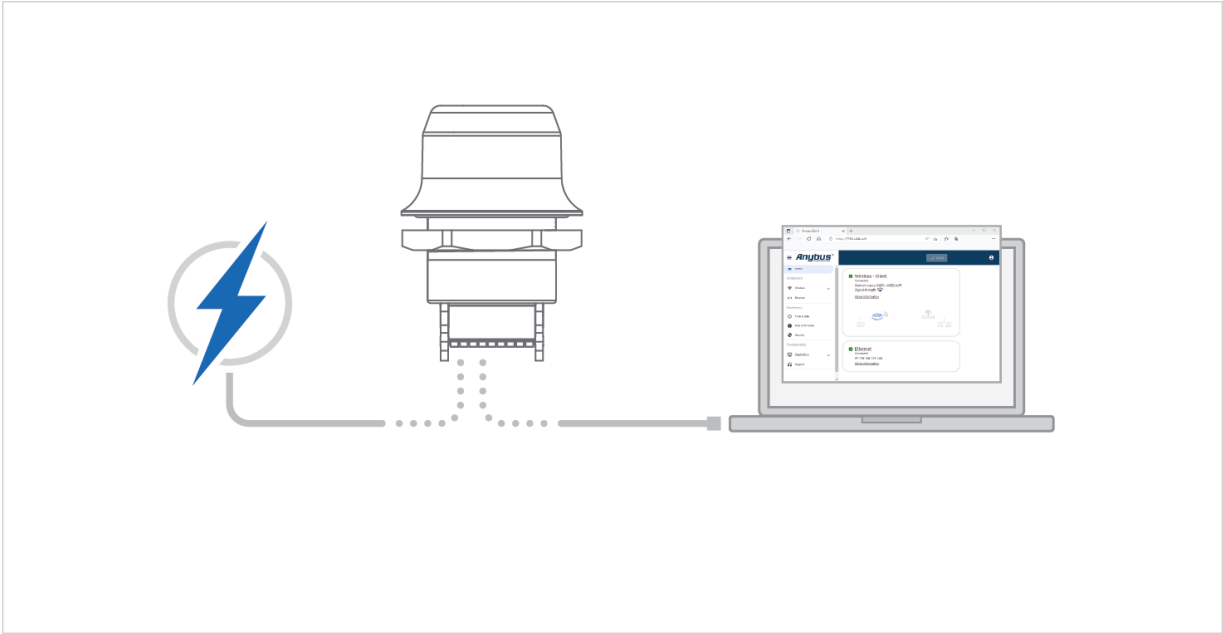


Figure 7. Connect to PC and Power

1. Connect the Bolt 18-Pin Ethernet port to your PC.
2. Connect the Bolt 18-Pin Power connector to a power supply.

When Connected to Wi-Fi Network

Once connected to a Wi-Fi network after initial setup, you can configure the Bolt 18-Pin wirelessly through the web interface — just ensure that **Local Configuration** is disabled.

See Local Configuration (page 44).

6.4. Access the Built-In Web Interface

NOTE
By default, **Local configuration** is enabled, which restricts access to the Bolt 18-Pin built-in web interface.

For a device to access the Bolt 18-Pin built-in web interface, connect it directly to the Bolt 18-Pin LAN (Local Area Network) port.

See also Local Configuration (page 44).

6.4.1. Required IP Address Settings

To be able to access the Bolt 18-Pin built-in web interface you may need to adjust the IP settings, choose one of the following methods.

NOTE
The Bolt 18-Pin default IP address is 192.168.0.99 and the subnet mask is 255.255.255.0.

Option 1- Set a Static IP Address on Your PC

NOTE
When you change to a static IP address on your PC, internet access may be lost.

On the PC accessing the Bolt 18-Pin built-in web interface, set a static IP address within the same IP address range as the Bolt 18-Pin IP address.

Option 2 - Change the IP Address on the Bolt 18-Pin Ethernet port

Use the software application HMS IPconfig to find and change the IP address on the Bolt 18-Pin Ethernet port, to one within the same IP address range as the PC accessing the Bolt 18-Pin built-in web interface.

To download the installation files, please visit www.hms-networks.com/technical-support and enter the product article number to search for the Bolt 18-Pin support web page. You find the product article number on the product cover.

Result

Now you can enter the Bolt 18-Pin IP address in your web browser and access the built-in web interface login page.

6.4.2. Login to the Built-In Web Interface

The Bolt 18-Pin built-in web interface can be accessed from a standard web browser.

Before You Begin

NOTE
The Bolt 18-Pin default IP address is 192.168.0.99 and the subnet mask is 255.255.255.0.

Procedure

Login to the Bolt 18-Pin built-in web interface:

1. Open a web browser.
2. Click to select the **Address bar** and enter http:// and the Bolt 18-Pin IP address.

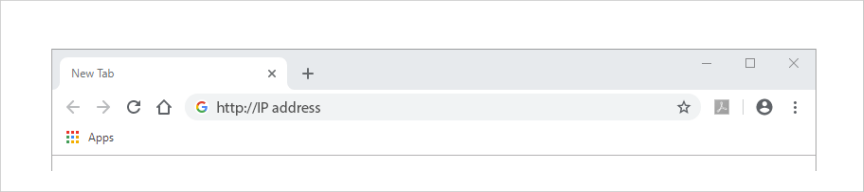


Figure 8. Enter IP address in web browser

3. Press **Enter**.
   The Bolt 18-Pin built-in web interface login screen appears.
4. Enter the **Password** and click **Sign in**.

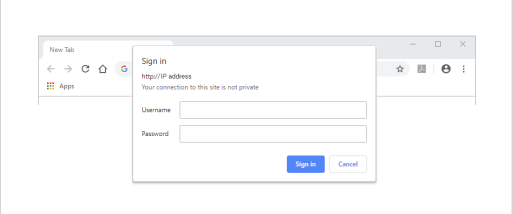


Figure 9. Built-in web interface login screen

Result

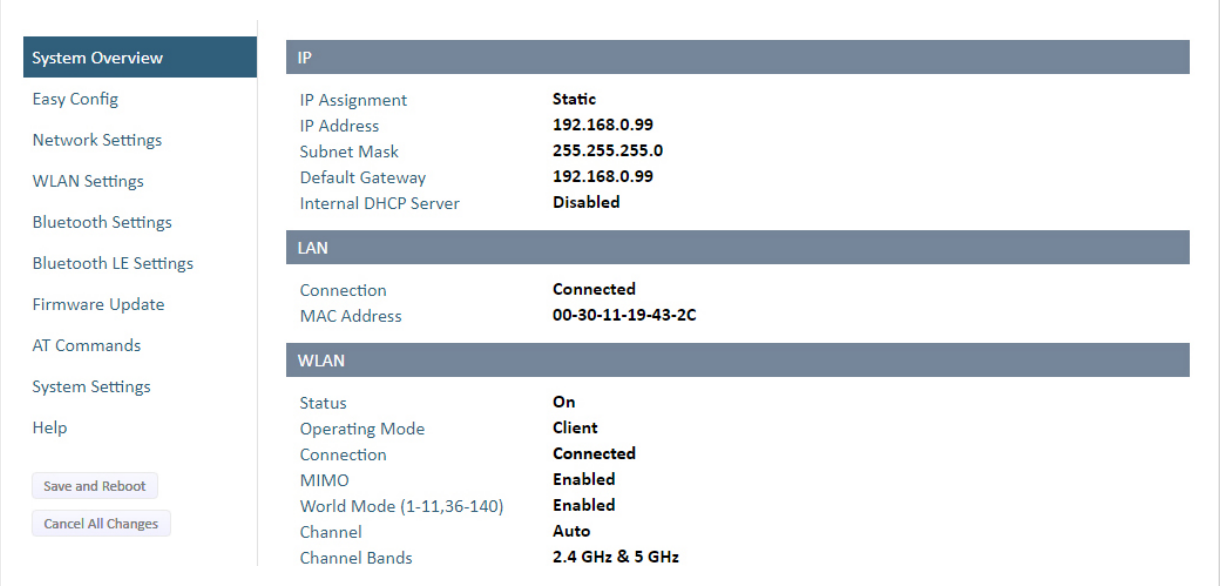
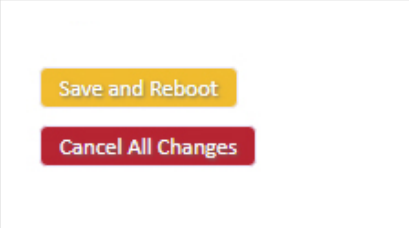


Figure 10. **System Overview** page

6.5. 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 62).

Apply Changes

To apply changes, click **Save and Reboot** in the left sidebar menu.

Bolt 18-Pin restarts for the changes to take effect.

6.6. 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]
Pairing Mode	Enabled
Connectable	No
Discoverable	No
Security Mode	Just works

6.7. Configuration Methods

There are different methods available for configuring the Bolt 18-Pin.

Built-In Web Interface Settings

Bolt 18-Pin can be configured via the settings in the built-in web interface.

See Configure Settings in the Built-In Web Interface (page 29).

Easy Config Modes

Bolt 18-Pin can be configured using one of the pre-configured Easy Config modes.

See Configuration with Easy Config (page 21).

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 25).

6.8. Configuration with Easy Config

6.8.1. Available Easy Config Modes

Bolt 18-Pin may be configured using one of the pre-configured Easy Config modes.

NOTE
To cancel Easy Config mode 11, the unit must be reset to factory default settings. See Reset to Factory Default (page 65)

Table 2. 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 120 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.
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.
7	WLAN AP	The unit scans for other units in Config Mode 4 and configure them as Clients. Timeout occur after 120 seconds.
8	Bluetooth NAP	Restart as Access Point and connect Clients. Apply PROFINET optimization to all units. PROFINET messages will have priority over TCP/IP frames.
9	Bluetooth PANU	Configure unit as a Client and scan for another Client (PANU to PANU). Apply PROFINET optimization to both units. The unit listens for 120 seconds or until a configuration is established.
10	(any)	Apply PROFINET optimization and restart. No other configuration settings are changed.
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.

6.8.2. Easy Config Modes Time Considerations

Table 3. 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.

6.8.3. Easy Config Configuration Steps

In this topic we describe the general procedure for configuring units using Easy Config modes. For specific use case examples, see Use Cases (page 46).

Configuration Steps

1. Connect the LAN port on the first Unit to your PC.
2. Power on Unit 1.
3. Login to the Built-In Web Interface of Unit 1.
4. On the **Easy Config** page, select the desired Easy Config mode from the **Select Easy Config** drop-down menu.

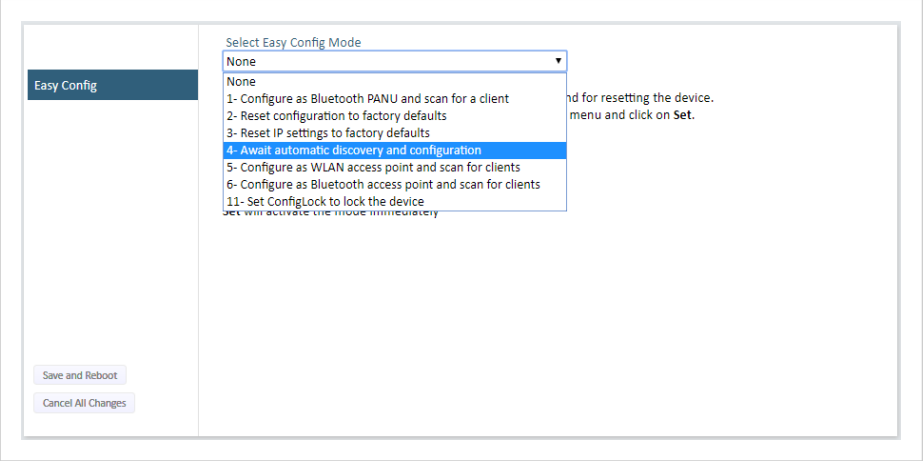


Figure 11. Easy Config Modes menu

Table 4. Available Easy Config Modes

EC	Role	Description
1	Bluetooth PANU	Configure as Bluetooth Client and scan for another Client (PANU–PANU). Timeout occur after 120 seconds.
2	–	Reset configuration to factory defaults.
3	–	Reset IP settings to factory defaults.
4	Client	Wait for automatic configuration. Configure units in Mode 4 as Clients.
5	WLAN AP	Configure units in mode 4 as clients. Restart as Access Point and connect Clients. Timeout occur after 120 seconds.
6	Bluetooth NAP	
11	(any)	Enable PROFIsafe mode.

5. Click **Set**.
   The Easy Config mode is activated immediately.

Add Additional Units

When using Easy Config Mode 5 or 6, up to seven additional Units can be added.

NOTE
When using Easy Config mode 4, the next unit to be added must be set up within 120 seconds after the first unit was restarted.

Each new Client unit will be assigned the next free IP address in the current Ethernet subnet.

To add a Unit, repeat the configuration steps.

Confirm Connection

When using one of the Easy Config Modes to connect two units, you need to confirm the connection between them.

For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. On the **Easy Config** page for each unit, a dialog window appears showing an **Easy Config confirmation** code.

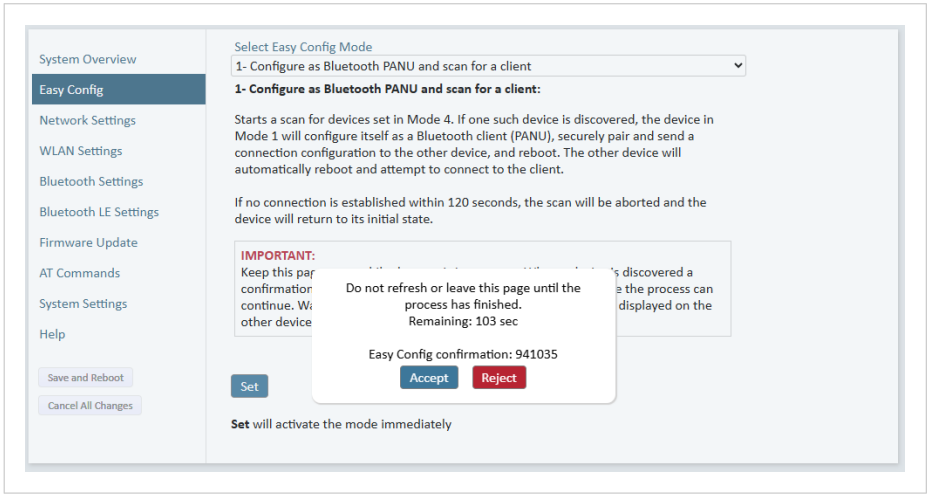


Figure 12. Easy Config page, confirmation dialog window

2. Compare the codes displayed in the dialog windows of both units to ensure they are identical.

- To allow Unit 2 to connect to and configure Unit 1, click **Accept** for each unit.

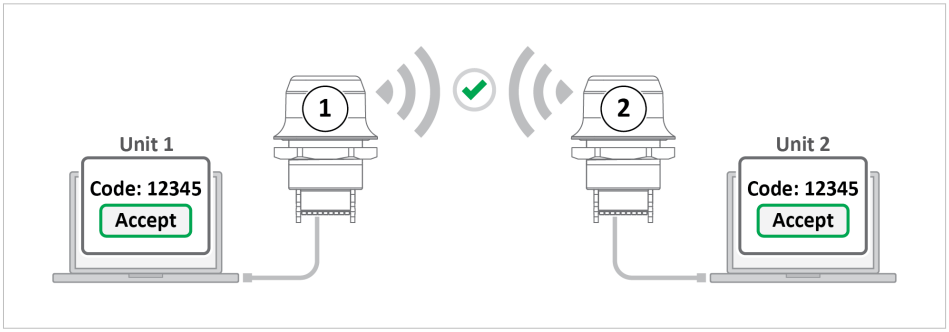


Figure 13. Codes match, Accept

- If Unit 2 detects a device other than the Bolt 18-Pin Unit 1, the dialog window appears only on Unit 2. Then, click **Reject**.
  Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.

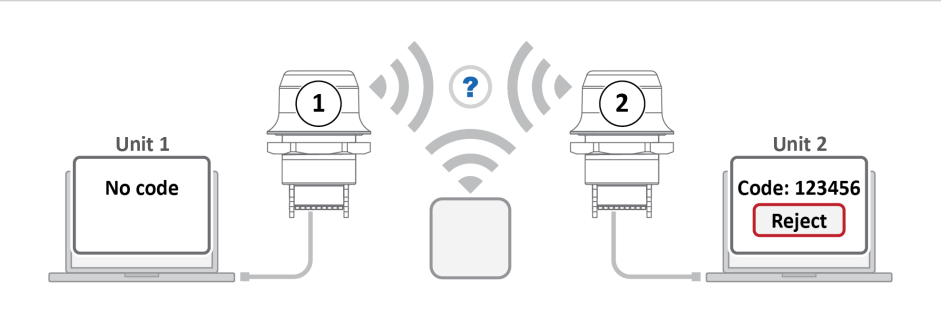


Figure 14. Code appear for one unit only, Reject

- If the codes do not match, click **Reject** for each unit.
  Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

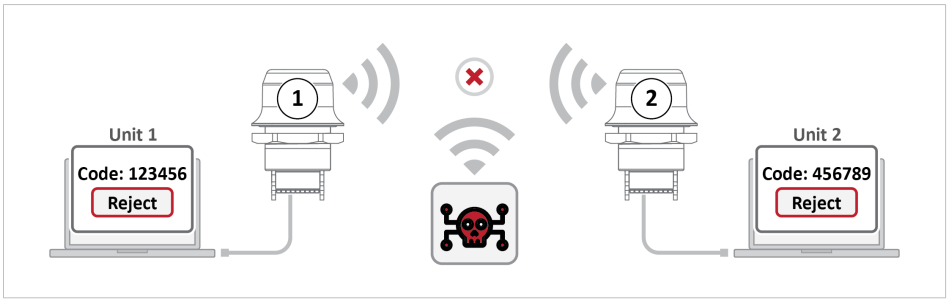


Figure 15. Codes do not match, Reject

Configure Additional Settings

To configure additional settings, log in to the built-in web interface for each unit you want to configure.

See Configure Settings in the Built-In Web Interface (page 29)

6.9. 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 18-Pin 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.hms-networks.com/technical-support.

Procedure

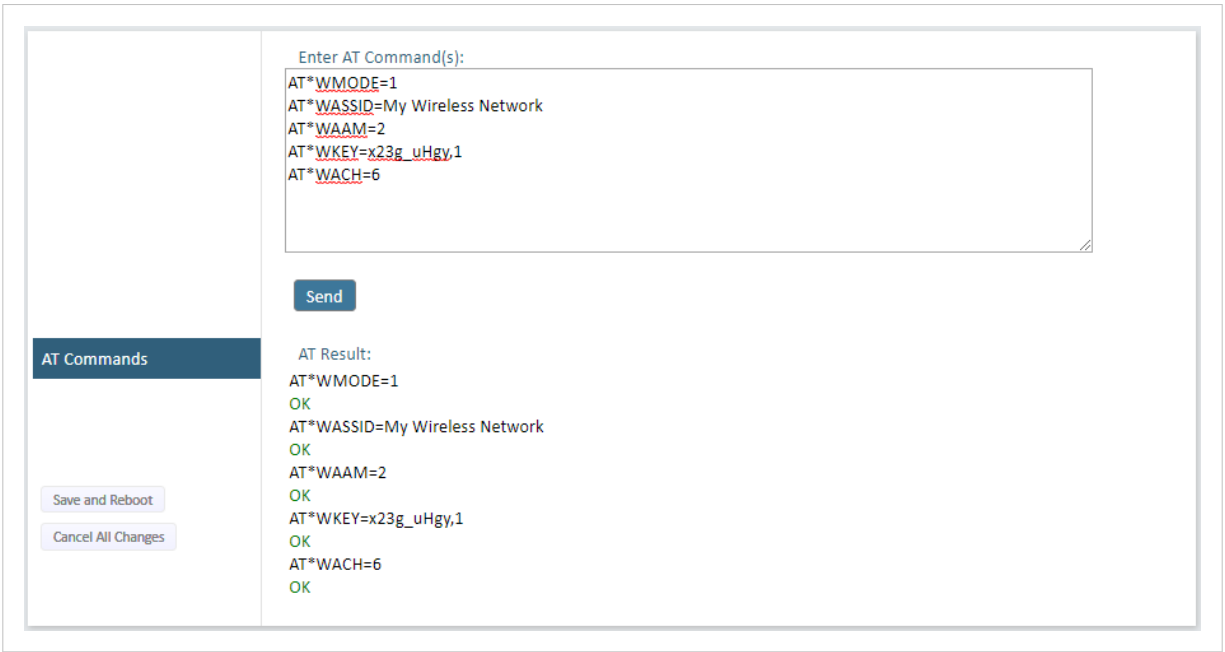


Figure 16. AT Commands and AT Results

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.

6.9.1. 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 18-Pin.
   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.

6.9.2. 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.hms-networks.com/technical-support.

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

6.9.3. 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 35).

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*WWM=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 18-Pin.
   Send the Reboot device AT Command:

```
AT*AMREBOOT
```

6.9.4. To Use Bluetooth LE With AT Commands

For information about using Bluetooth LE, refer to the AT Commands Reference Guide or the **Help** page in the built-in web interface.

6.10. Configure Settings in the Built-In Web Interface

6.10.1. Network Settings

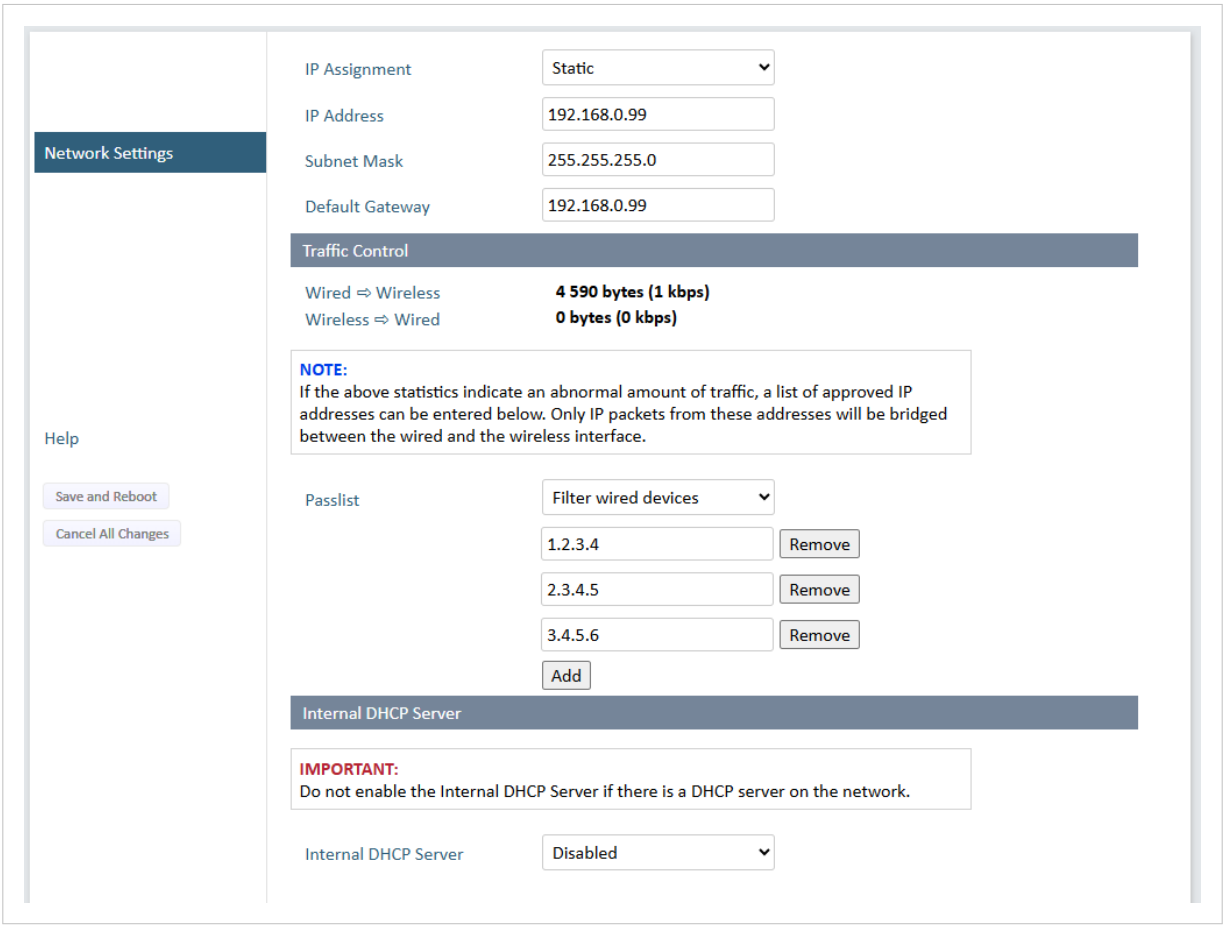


Figure 17. Network Settings page

Setting	Description
IP Assignment	Select static or dynamic IP addressing (DHCP).
IP Address	Static IP address for the unit. When you click **Save and Reboot**, 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.
Traffic Control	**Wired to Wireless** and **Wireless to Wired** Bytes Counter: Used to monitor and measure the amount of data being received and transmitted by the Bolt 18-Pin. Pass list: Used to specify which IP addresses have access to the Bolt 18-Pin.
Internal DHCP Server	**Disabled**: No internal DHCP functionality. **DHCP Relay Enabled**: The unit can receive a DHCP request on one interface and resend it to a DHCP server located on one of the other interfaces. Only a single DHCP server can be active for all the connected interfaces. If WLAN is used, the forwarding mode must be set to Layer 3 IP Forward. **DHCP Server Enabled**: Activates an internal DHCP server. This option is only available when IP Assignment is set to Static. 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 **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.

Setting	Description
	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**. **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 is ignored.
	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.

6.10.2. Traffic Control

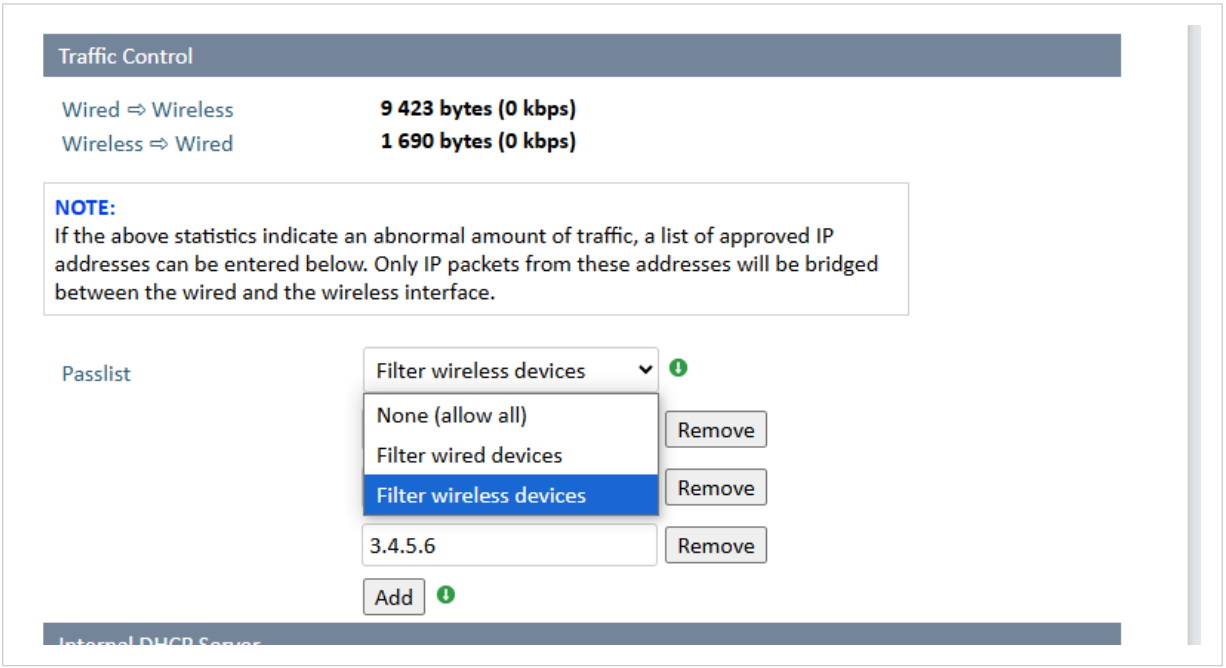


Figure 18. Network Settings, Traffic Control

Bytes Counter

> **IMPORTANT**
> Monitoring unusual traffic patterns can help detect potential security threats and identify unauthorized data transfers or potential intrusions.

Use the byte counter to monitor and measure the amount of data being received and transmitted by the Bolt 18-Pin.

Passlist

> **IMPORTANT**
> A pass list is used to specify which IP addresses have access to the connected network.
>
> Only IP traffic from sources on the passlist is allowed; all other IP traffic is blocked.
>
> Other Ethernet traffic, such as PROFINET over Layer 2, is still bridged from the Bolt 18-Pin.
>
> Restricting access to only trusted sources can help improve security.

By default all traffic is permitted, **Traffic Control None (allow all)** is selected.

Procedure

1. From the **Passlist** menu, select:
   - **Filter wired devices**, to filter devices connected to the Bolt 18-Pin via Ethernet.
   - **Filter wireless devices**, to filter devices wirelessly connected to the Bolt 18-Pin.
2. In the input field, enter the trusted IP address.
3. To add more sources, click **Add**.
   You can add up to 5 sources.

6.10.3. 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.

6.10.4. WLAN Settings General

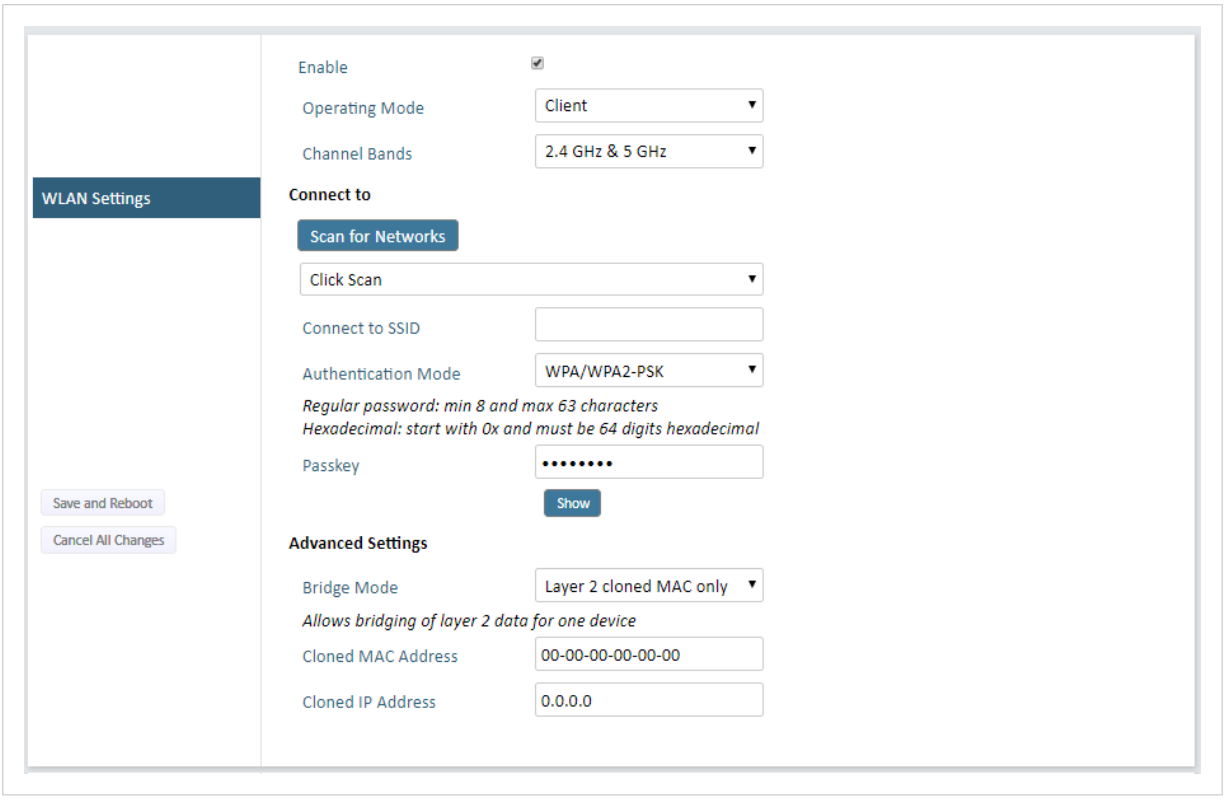


Figure 19. WLAN Settings page

Setting	Description
Enable	Enable/disable the WLAN interface.
Operating Mode	Choose operation as WLAN **Client** or **Access Point**. When **Access Point** is selected, additional settings will be available.
Channel Bands	**NOTE** 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. Choose to scan only the 2.4 GHz or 5 GHz channel band, or both (default).

6.10.5. WLAN Settings for Client

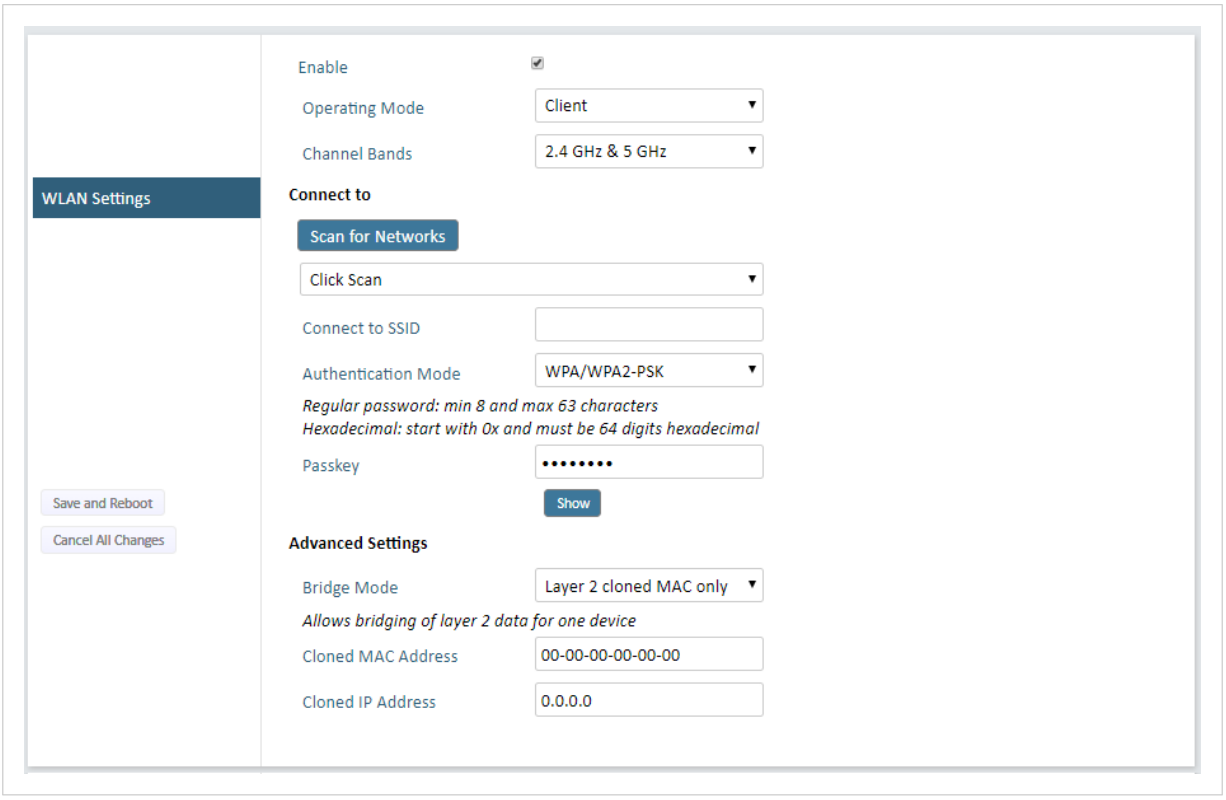


Figure 20. WLAN Settings page

Connect to settings for Client

Setting	Description
Scan for Networks	To scan the selected frequency band(s) for discoverable WLAN networks, click **Scan for Networks**. 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, **Open**, **WEP64/128**, or **WPA/WPA2-PSK**. **Open**: Not secure. No password or encryption is used. **WEP64/128**: Basic security. Use only if needed for compatibility with legacy devices. **WPA/WPA2-PSK**: Recommended for most networks. WPA2 is more secure than WPA.
Passkey	When using **WPA/WPA2-PSK** or **WEP64/128**, enter the passkey.

6.10.6. WLAN Roaming

Bolt 18-Pin 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 26).

6.10.7. 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 18-Pin supports regulatory domain detection and channel settings for FCC and ETSI according to the IEEE 802.11d specification.

Table 5. 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 (European Telecommunications Standards Institute)	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 (Federal Communications Commission)	1-11	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140

6.10.8. WLAN Settings for Access Point

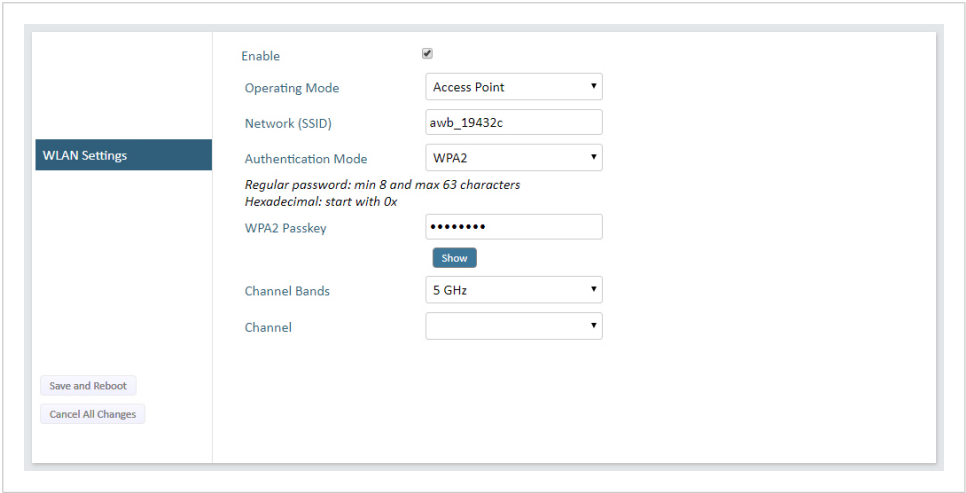


Figure 21. WLAN Settings page

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 18-Pin. 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 **Open** is selected there is no encryption or authentication. When **WPA2** 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 WPA2 Password Examples (page 36).
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&43**

Example 5. Hexadecimal password example

0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f

6.10.9. WLAN Advanced Settings

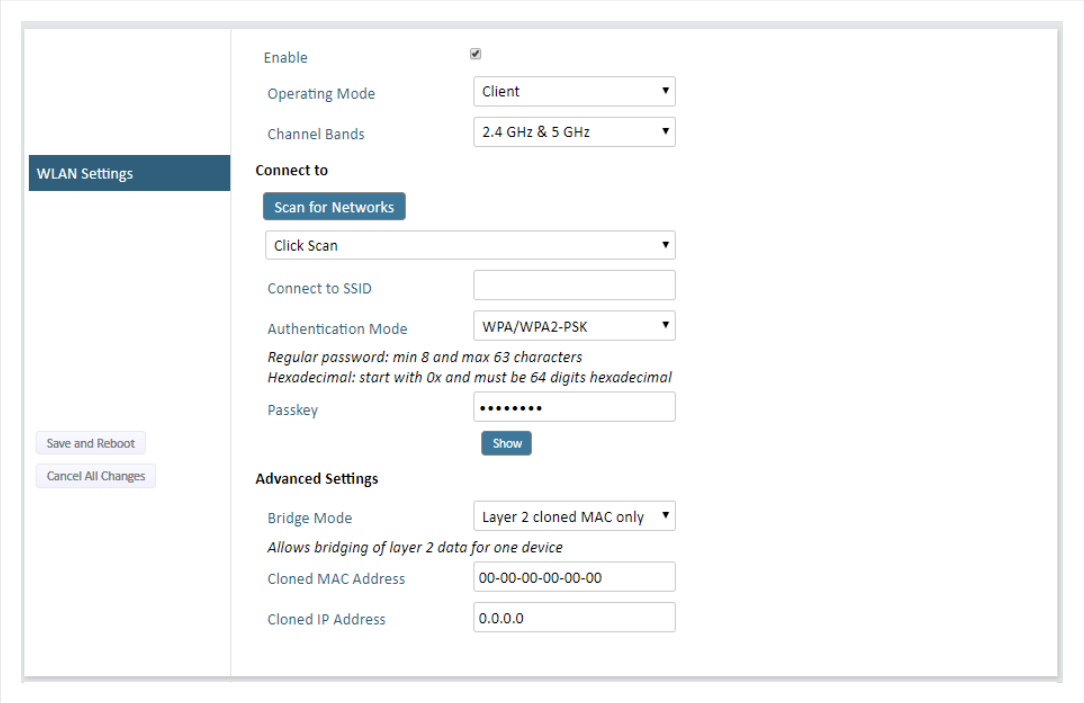


Figure 22. WLAN Settings page

Advanced Settings

Setting	Description
Bridge Mode	**Layer 2 tunnel**: All layer 2 data will be bridged over WLAN. Use when multiple devices on both sides of an Ethernet network bridge must be able to communicate via WLAN (many-to-many). Only works between 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 setting. IP data from all devices will be bridged over WLAN. This mode must be used when using the DHCP Relay function. See Layer 3 IP Forward Connectivity Considerations (page 32).
Cloned MAC Address	The MAC address to use with **Layer 2 cloned MAC only**.
Cloned IP Address	The IP address to use with **Layer 2 cloned MAC only**.

6.10.10. Bluetooth Settings General

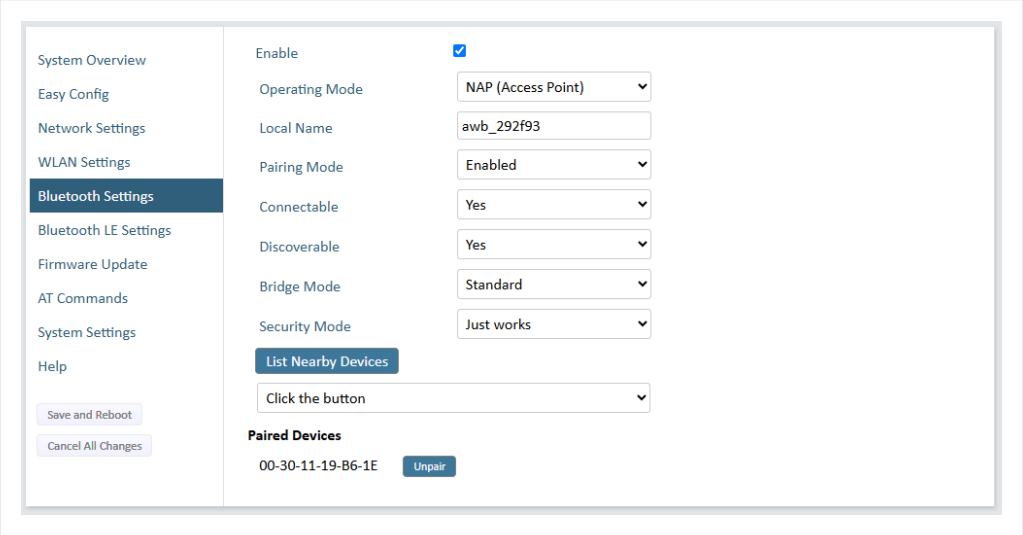


Figure 23. Bluetooth Settings page

General settings

Setting	Description
Enable	Enable/disable the Bluetooth interface.
Operating Mode	**PANU (Client)**: The unit will operate as a Bluetooth PAN (Personal Area Network) User device. It can connect to another single Bluetooth PANU device or to a Bluetooth Network Access Point. **NAP (Access Point)**: The unit will operate as a Bluetooth Network Access Point. It can connect to up to 7 Bluetooth PANU devices.
Local Name	Identifies the unit to other Bluetooth devices. If left blank, the unit will use a default name including the last 6 characters of the MAC ID.
Pairing Mode	**Enabled**: The Bolt 18-Pin allows other Bluetooth devices to pair with it. **Disabled**: The Bolt 18-Pin does not allow other Bluetooth devices to pair with it.
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	**Disabled**: No encryption or authentication. **PIN**: Encrypted connection with PIN code security. This mode only works between two units of this type and brand (not with third-party devices). PIN codes must consist of 4 to 6 digits. **Just Works**: Encrypted connection without PIN code.

Paired devices

The Bluetooth MAC addresses of the connected devices are listed in the **Paired devices** panel.

To unpaire a devices, click **Unpaire**.

6.10.11. Bluetooth Settings for PANU Mode

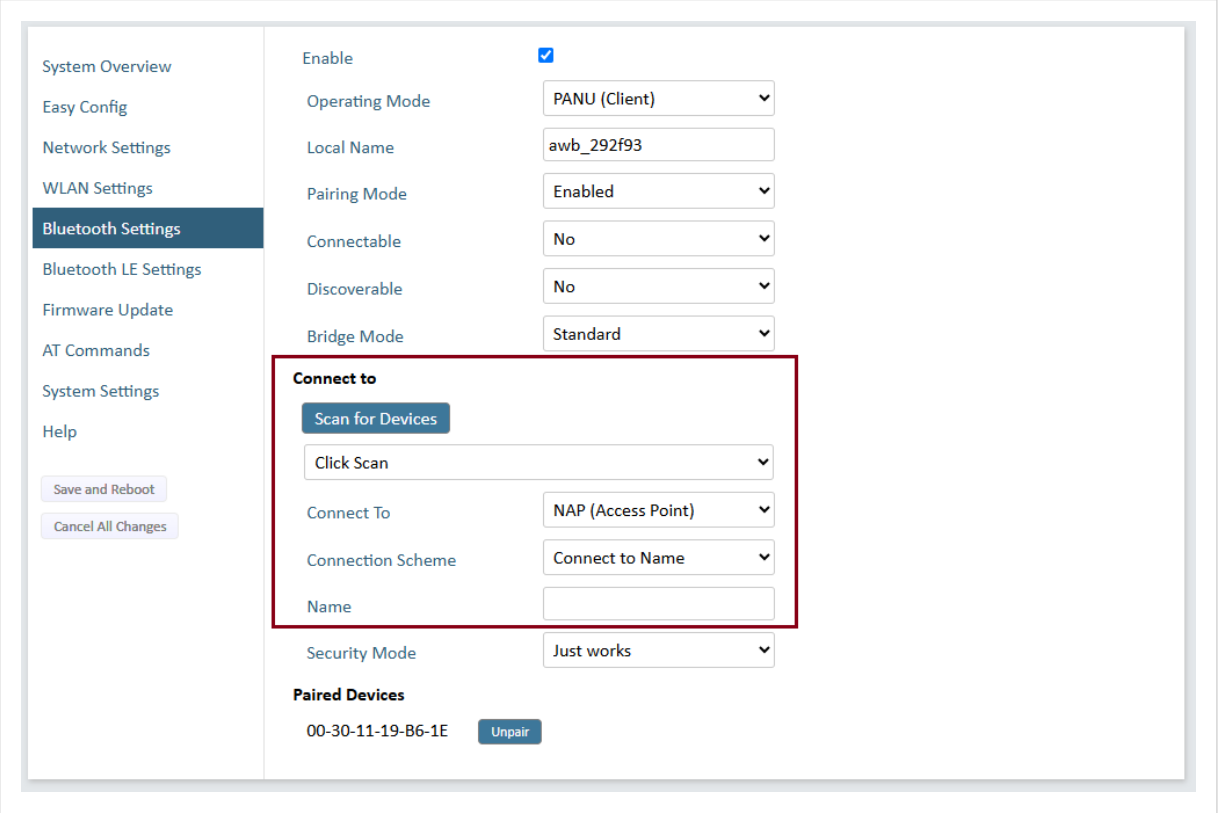


Figure 24. Bluetooth Settings page

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.

6.10.12. Bluetooth Settings for NAP Mode

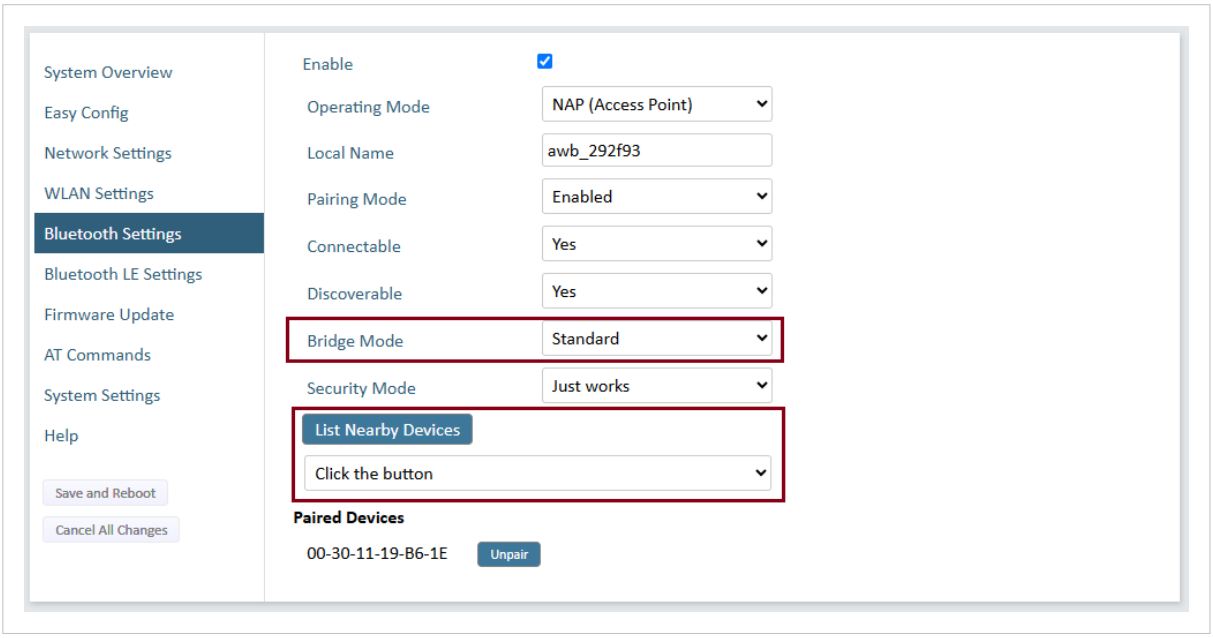


Figure 25. Bluetooth Settings page

Bluetooth Settings for NAP Mode

Setting	Description
Bridge Mode	**Standard** • Default mode. • Bridge data between devices without performing IP-level forwarding. **Layer 3 IP forward** • IP data is forwarded over Bluetooth. • Use when connecting to an Android device over Bluetooth. • Ensure the network has an active DHCP server to assign IP addresses.
List Nearby Devices	Scans the network and lists discoverable Bluetooth devices. Pairing cannot be initiated in NAP mode.

6.10.13. Bluetooth Settings for SPP Mode

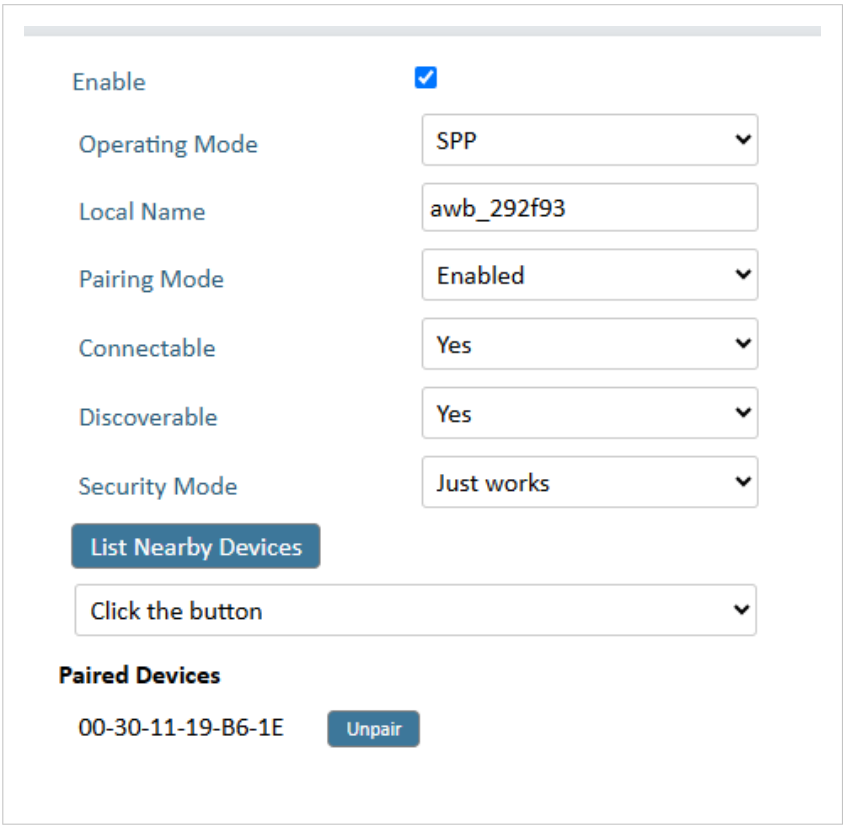


Figure 26. Bluetooth page, Operation Mode SPP enabled

There are no specific settings required for **Operating Mode SPP** mode.

Once paired, Bolt 18-Pin enable serial/CAN communication.

List Nearby Devices
To scans the network and list discoverable Bluetooth devices, click **List Nearby Devices**

Pairing cannot be initiated in **SPP** mode.

6.10.14. Bluetooth LE Settings

1. On the **Bluetooth Settings** page, enable **Bluetooth LE**.
2. On the **Bluetooth LE Settings** page, configure the Bluetooth LE settings.

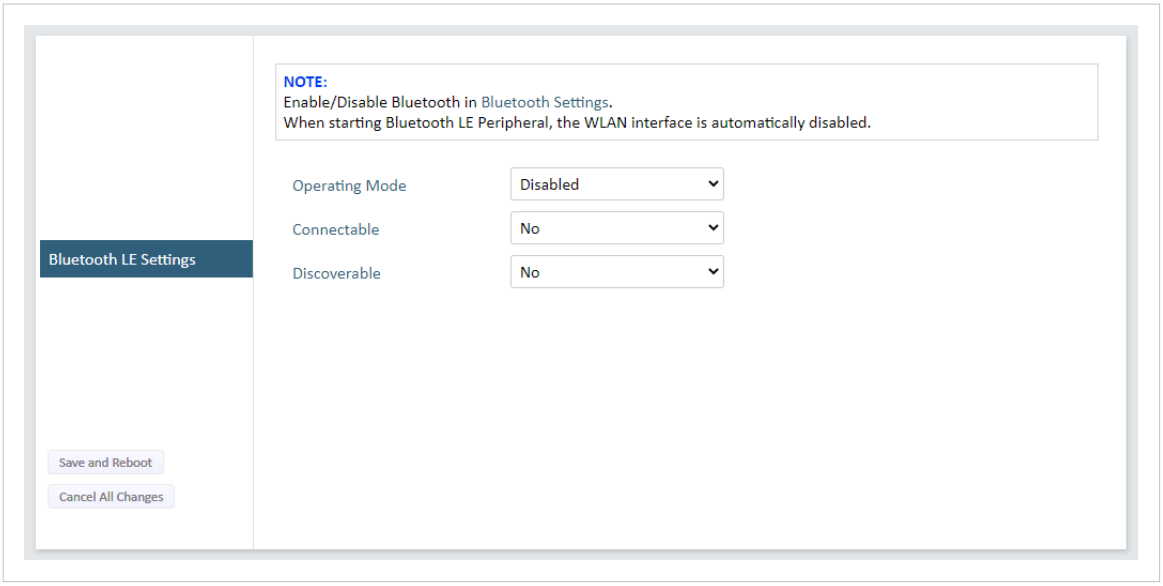


Figure 27. **Bluetooth LE Settings** page

Setting	Description
Operating Mode	**Disabled**: Bluetooth LE disabled (default) **Central**: Bluetooth LE Central operating mode enabled **Peripheral**: Bluetooth LE Peripheral operating mode enabled. This requires that the WLAN interface is disabled.
Connectable	**No**: Connectable is disabled (default) **Yes**: Enables the Wireless Bridge II Serial to search, connect and transfer data with another Bluetooth-capable device.
Discoverable	**No**: Discoverable is disabled (default) **Yes**: Enables the Wireless Bridge II Serial to pair with another Bluetooth-capable device.

6.10.15. System Settings

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

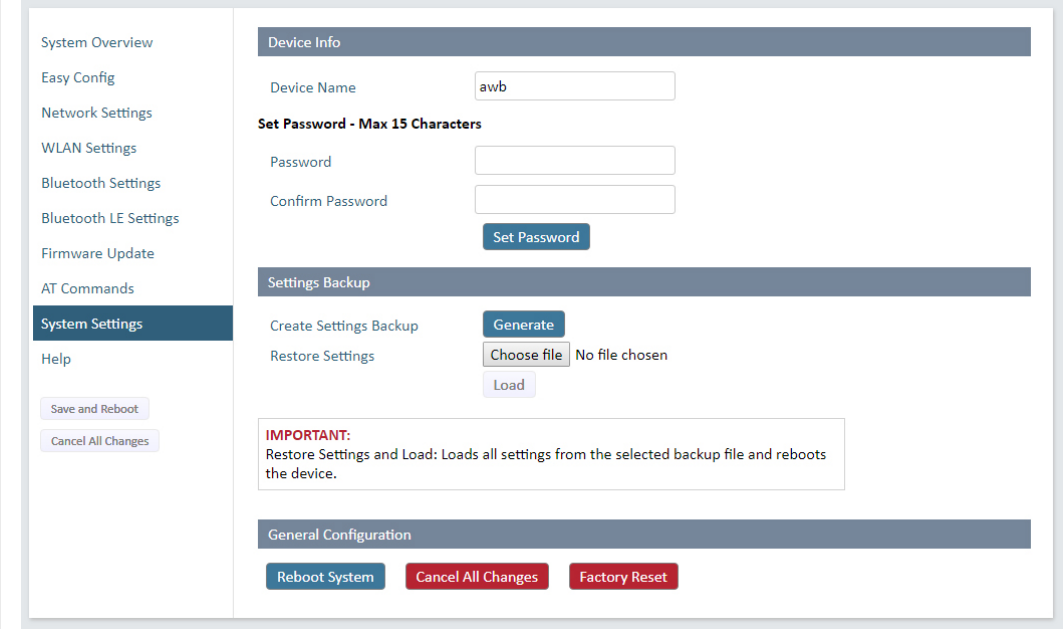


Figure 28. System Settings page

Device Info

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

Local Configuration

IMPORTANT

You should only disable **Local configuration** if the Bolt 18-Pin is connected to trusted networks via routers or the wireless interface, and there are cybersecurity measures in place to protect the networks and connected devices from unauthorized access.

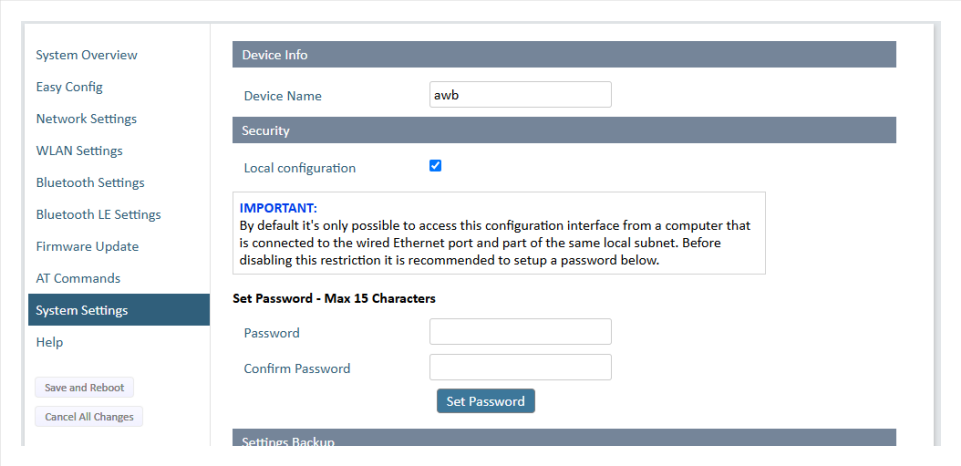


Figure 29. System Settings page, Security, Local configuration

By default, the **Local configuration** checkbox is selected, which restricts access to the Bolt 18-Pin built-in web interface.

This ensures only requests originating from the wired Ethernet interface and within the same sub network as the Bolt 18-Pin are permitted to access the built-in web interface.

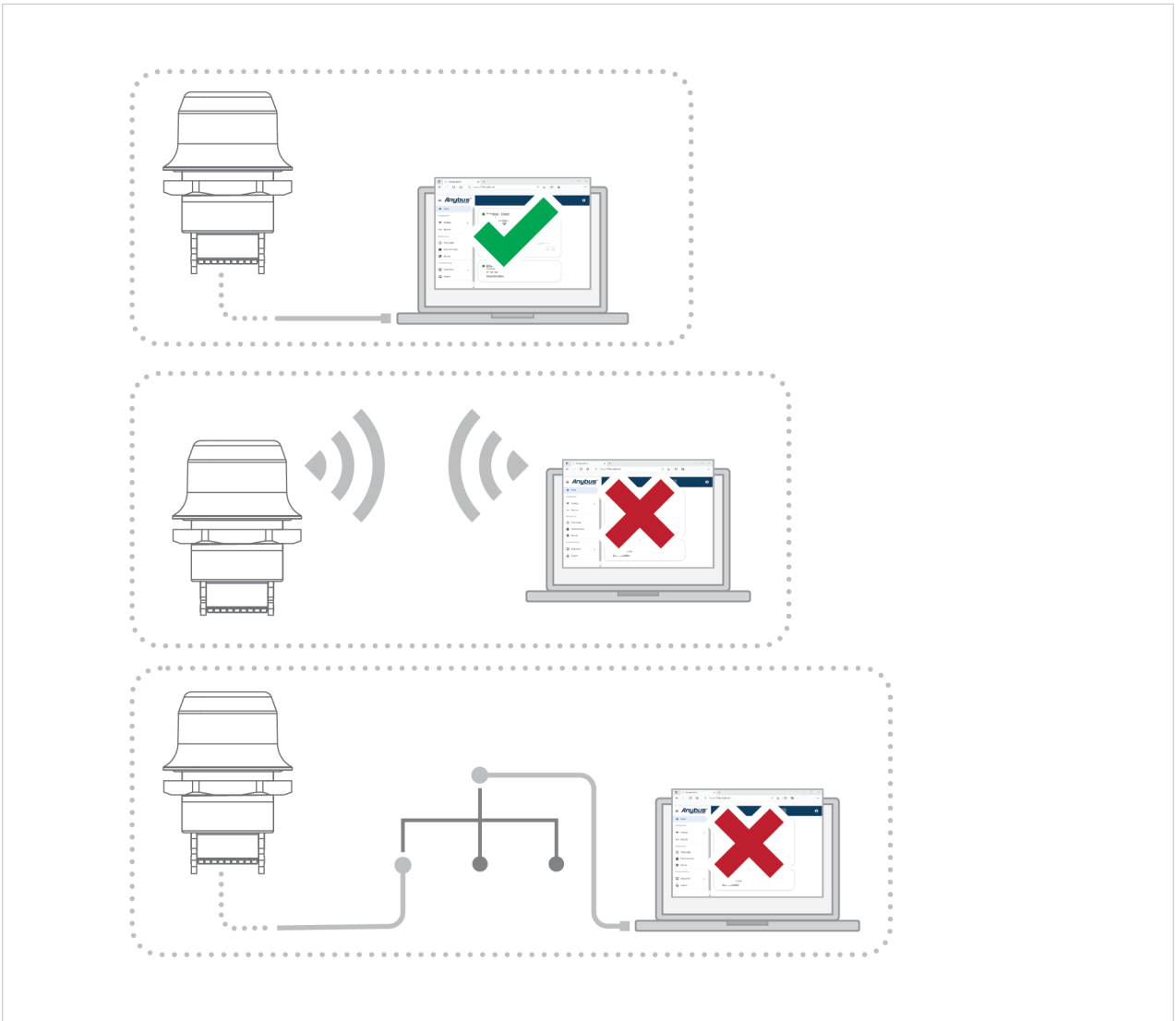


Figure 30. Direct LAN connection required for Bolt 18-Pin built-in web interface access

For a device to access the Bolt 18-Pin built-in web interface, connect it directly to the Bolt 18-Pin LAN (Local Area Network) port,

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.

7. Use Cases

7.1. Ethernet Bridge via WLAN or Bluetooth

Configuration with Easy Config

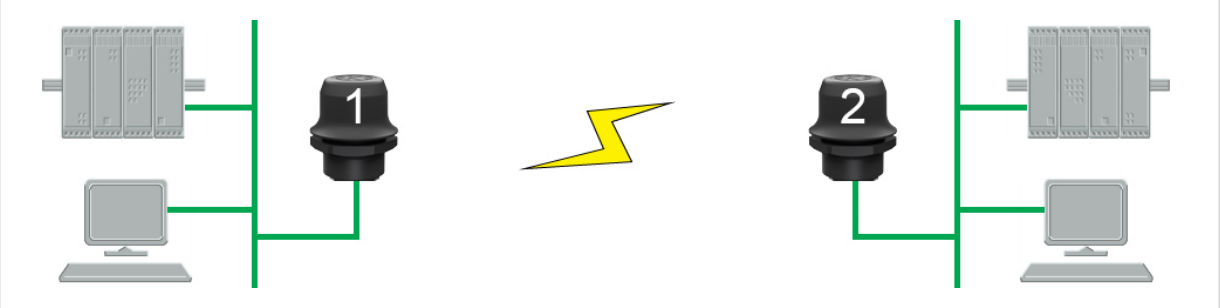


Figure 31. Ethernet bridge

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

Procedure

Activate Easy Config Mode

1. In the web interface of Unit 1, activate **Easy Config Mode 4**.
   This Unit 1 isl now discoverable.

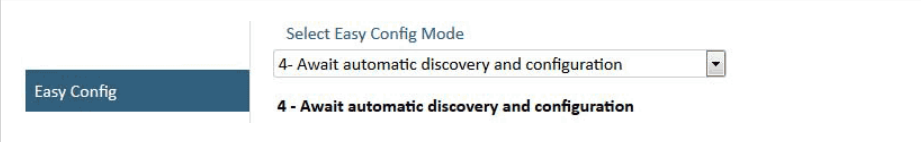


Figure 32. Easy Config Mode 4

2. In the web interface of Unit 2, activate **Easy Config Mode 5** for WLAN or **6** for Bluetooth.

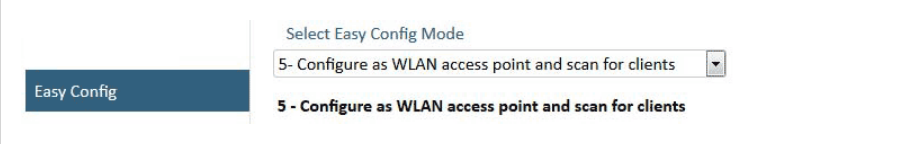
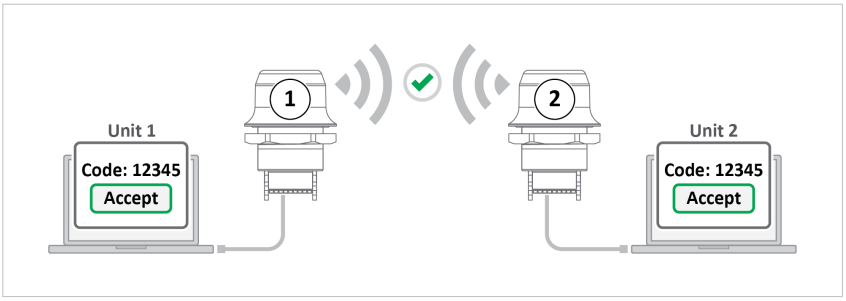


Figure 33. Easy Config Mode 5

Confirm Connection



For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. On the **Easy Config** page for each unit, a dialog window appears showing an **Easy Config confirmation** code.
2. Compare the codes displayed in the dialog windows of both units to ensure they are identical.
   - To allow Unit 2 to connect to and configure Unit 1, click **Accept** for each unit,
   - If Unit 2 cannot discover Unit 1, the dialog window only appear on Unit 2. Then, click **Reject**.
     Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.
   - If the codes do not match, click **Reject**.
     Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

Result

- Unit 1 is now open for automatic configuration.
- Unit 2 will now discover and configure Unit 1 as a client and configure itself as an access point.
- Unit 1 will be assigned the first free IP address in the same Ethernet subnet as Unit 2.

Add Additional Units

To add a Client Unit, repeat the configuration steps.

- You can add up to 6 additional Clients, by repeating the procedure.
- Each new Client will be assigned the next free IP address in the current subnet.

7.2. PROFINET Networking Via Bluetooth

Configuration with Easy Config

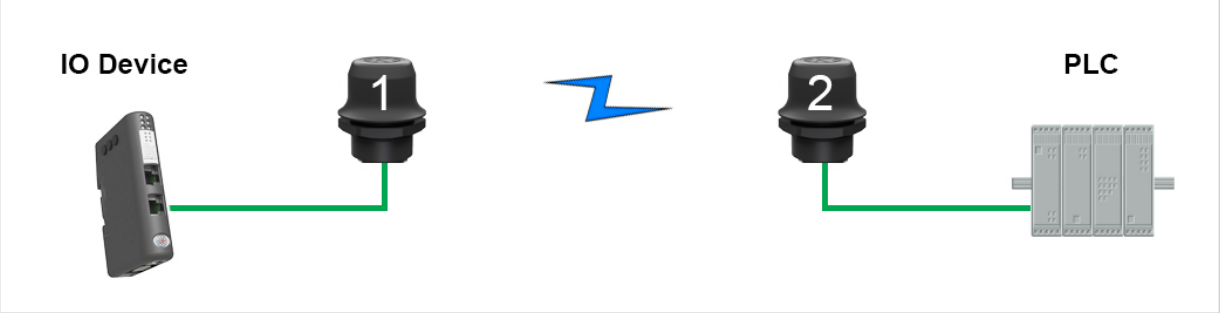


Figure 34. PROFINET wireless network

This example describes how to connect a PROFINET IO device and a PROFINET PLC over Bluetooth using two Bolt 18-Pins and Easy Config.

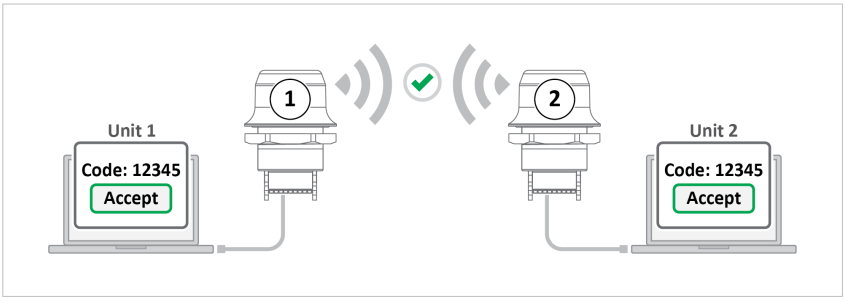
The Bolt 18-Pins are configured with PROFINET optimization. This means that PROFINET messages have priority over TCP/IP frames.

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

Activate Easy Config Mode

1. Reset both units to the factory default settings.
2. Connect Unit 1 to the IO device and Unit 2 to the PLC.
3. Set Unit 1 to Easy Config Mode 4.
   Unit 1 is now discoverable.
4. Set Unit 2 to Easy Config Mode 8.

Confirm Connection



For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. On the **Easy Config** page for each unit, a dialog window appears showing an **Easy Config confirmation** code.

2. Compare the codes displayed in the dialog windows of both units to ensure they are identical.
   - To allow Unit 2 to connect to and configure Unit 1, click **Accept** for each unit,
   - If Unit 2 cannot discover Unit 1, the dialog window only appear on Unit 2. Then, click **Reject**.
     Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.
   - If the codes do not match, click **Reject**.
     Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

Result

- Unit 1 is now open for automatic configuration.
- Unit 2 will now automatically discover and configure Unit 1 as a Bluetooth Client, and configure itself as an Access Point.
- Both units are optimized for PROFINET.
- The IO device will now be able to communicate with the PLC as if using a wired connection.

Add Additional Units

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

To add a Client Unit, repeat the configuration steps.

- You can add up to 6 additional Clients, by repeating the procedure.
- Each new Client will be assigned the next free IP address in the current subnet.

7.3. EtherNet/IP Networking Via Bluetooth

Configuration with Easy Config

Figure 35. EtherNet/IP wireless network

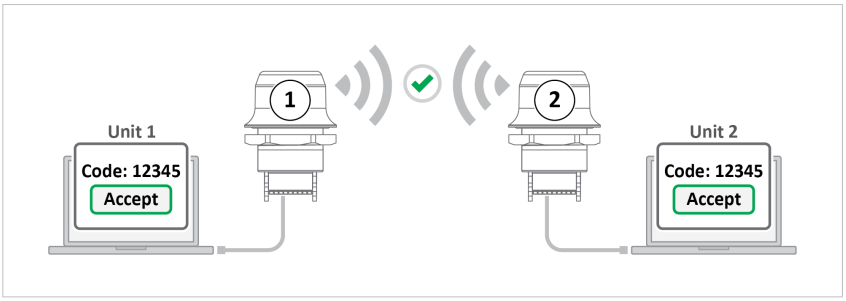
This example describes how to connect an EtherNet/IP IO device and an EtherNet/IP PLC over Bluetooth using two Wireless Bridges and Easy Config.

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

Activate Easy Config Mode

1. Reset both units to the factory default settings.
2. Connect Unit 1 to the IO device.
3. Connect Unit 2 to the PLC.
4. Set Unit 1 to Easy Config Mode 4.
   Unit 1 is now be discoverable.
5. Set Unit 2 to Easy Config Mode 6

Confirm Connection



For cybersecurity reasons, the following steps are implemented to ensure the correct devices are connected:

1. On the **Easy Config** page for each unit, a dialog window appears showing an **Easy Config confirmation** code.
2. Compare the codes displayed in the dialog windows of both units to ensure they are identical.
   - To allow Unit 2 to connect to and configure Unit 1, click **Accept** for each unit,
   - If Unit 2 cannot discover Unit 1, the dialog window only appear on Unit 2. Then, click **Reject**.
     Ensure that no other nearby Bluetooth devices are in pairing mode, then redo the Easy Config procedure.
   - If the codes do not match, click **Reject**.
     Verify that there are no unauthorized or potentially harmful devices in the area, then redo the Easy Config procedure.

Result

- Unit 1 is now open for automatic configuration.
- Unit 2 will automatically discover and configure Unit 1 as a Bluetooth Client, and configure itself as an Access Point.
- The IO device will now be able to communicate with the PLC as if using a wired connection.

Add Additional Units

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

To add a Client Unit, repeat the configuration steps.

- You can add up to 6 additional Clients, by repeating the procedure.
- Each new Client will be assigned the next free IP address in the current subnet.

7.4. Ethernet Network to Existing WLAN

Figure 36. Connecting to a WLAN

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

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

Before You Begin

- When using this set up in an enterprise network, read the connectivity consideration information before you start. Layer 3 IP Forward Connectivity Considerations (page 32).

Configuration

1. Reset the Bolt 18-Pin to the factory default settings.
2. In **Network Settings**, configure the IP settings as required by the wireless network.
3. If the network uses DHCP, select **DHCP Relay Enabled**.

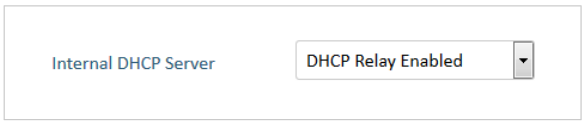


Figure 37. DHCP Relay Enabled

WLAN Settings for Small Office/Home Office Network

When the setup is used in a small office/home office network, follow these steps:

1. In **WLAN Settings**, select **Layer 3 IP forward** (default setting) from the **Bridge Mode** drop-down list.
2. In **WLAN Settings**, click **Scan for Networks**.
3. When the scan is completed, select the wireless network from the drop-down list.
4. If required, select the authentication mode and enter the passkey for the wireless network.
5. Click **Save and Reboot**.
   The Ethernet network will now be able to access the WLAN Access Point.

WLAN Settings for Enterprise Network

When the setup is used in an enterprise network, follow these steps:

1. In WLAN Settings, set **Bridge Mode** to **Layer 2 cloned MAC only**.

2. In the **Cloned MAC Address** field, enter the MAC address of the PLC.
3. In the **Cloned IP Address** field, enter the IP address of the PLC.
4. Click **Save and Reboot**.
   The Bolt 18-Pin will now function as a WLAN interface for the PLC using the MAC address of its Ethernet interface.

7.5. Adding Single Ethernet Node to WLAN

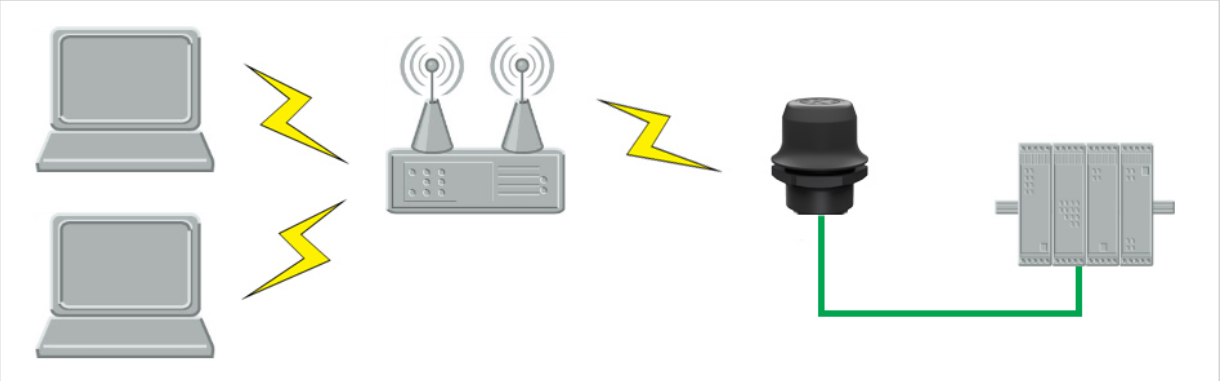


Figure 38. Adding WLAN connectivity

This example describehows how to connect a PLC with an Ethernet network interface to an existing WLAN with support for layer 2 and layer 3 traffic. The WLAN interface in the Bolt 18-Pin will clone the MAC address of the Ethernet interface in the PLC.

Only a single Ethernet node will be able to communicate via a third-party WLAN Access Point in this setup.

Configuration

1. Reset the Bolt 18-Pin to the factory default settings.
2. In **Network Settings**, configure the IP settings as required by the wireless network.
3. In WLAN Settings, click on **Scan for Networks**.
4. When the scan is completed, select the wireless network from the drop-down list.
5. If required, select the authentication mode and enter the passkey for the wireless network.
6. Click **Save and Reboot**.
7. To ensure that the WLAN connection is established, check the **System Overview** page.

> **NOTE**
> It is important that the WLAN connection is established before you proceed with the next configuration step. When the final configuration step is done, the built-in web interface may no longer be accessible from the network without performing a factory reset.

8. In **WLAN Settings**, set **Bridge Mode** to **Layer 2 cloned MAC only**.
9. In the **Cloned MAC Address** field, enter the PLC MAC address.
10. In the **Cloned IP Address** field, enter the PLC IP address.
11. Click **Save and Reboot**.
    The Bolt 18-Pin will now function as a WLAN interface for the PLC using the MAC address of its Ethernet interface.

7.6. Access PLC from Handheld Device via WLAN

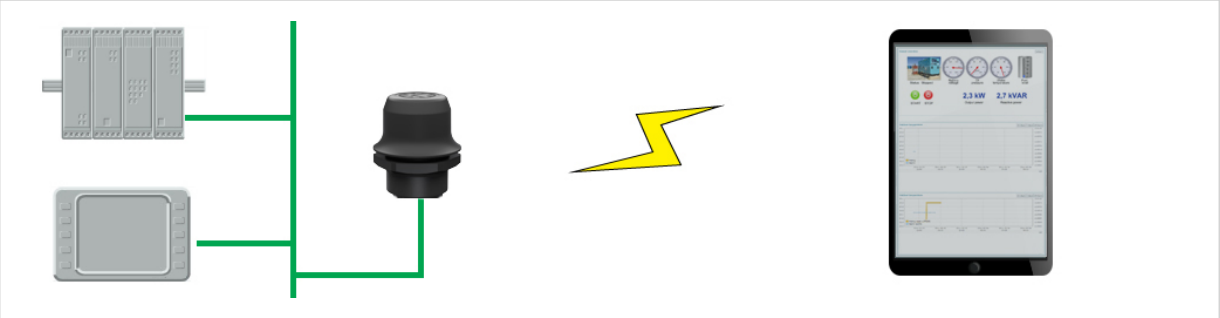


Figure 39. Access a PLC from a handheld device using WLAN

This example describes how to use a Bolt 18-Pin to access the web interface of a PLC on a wired network from a tablet or smartphone which uses DHCP. The Bolt 18-Pin will function as a WLAN Access Point.

Before You Begin

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

Configuration

1. Reset the Bolt 18-Pin to the factory default settings.
2. In **Network Settings**, configure the IP settings as required:

Option if the wired network uses DHCP

a. Select **DHCP Relay Enabled**.

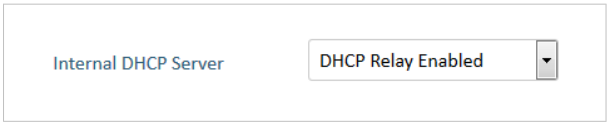


Figure 40. DHCP Relay Enabled

Option if the wired network uses static IP

IMPORTANT
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.

a. Select **DHCP Server Enabled**.
b. Select an interface from the **DHCP Interfaces** drop-down menu.

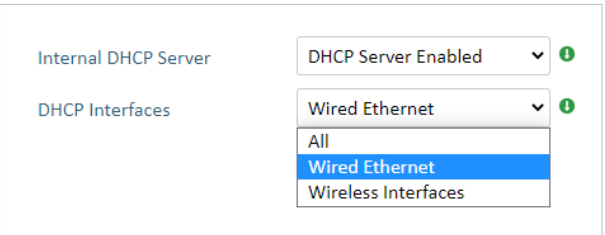


Figure 41. DHCP Interfaces, Wired Ethernet

c. Enter a Start Address for DHCP addressing. Ensure that the address range does not contain any existing addresses on the network.

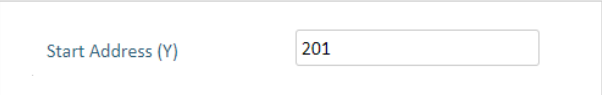


Figure 42. Start Address for DHCP addressing

The Bolt 18-Pin will now function as a DHCP server and allocate an IP address to the handheld device over WLAN.

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

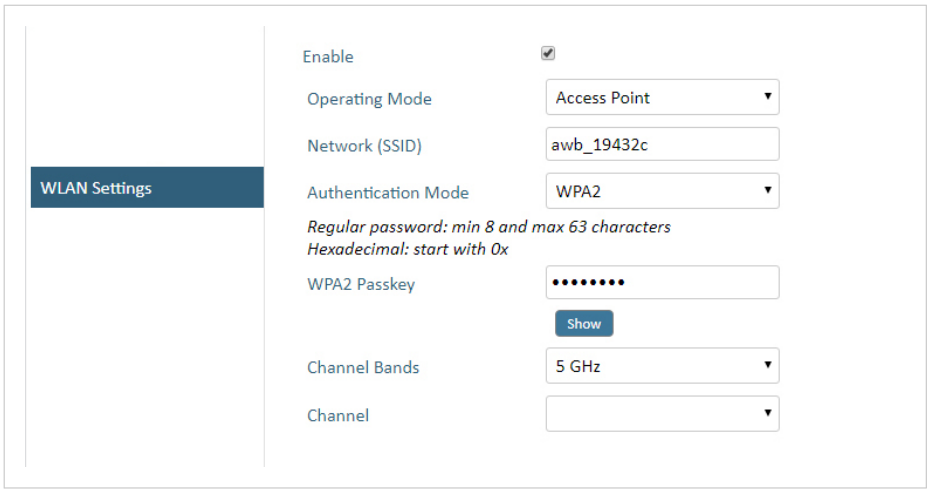


Figure 43. WLAN Settings

4. Enter a unique **Network (SSID)**, network name, for the new wireless network.
5. Set **Authentication Mode** to **WPA2** and enter a passkey.
6. Select a **Channel band** and a **Channel**.
7. Click **Save and Reboot**.
   You should now be able to connect to the SSID of the Bolt 18-Pin on your handheld device and access the PLC by by entering its IP address in a browser.

8. Verify Operation

8.1. Network Connection Status

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

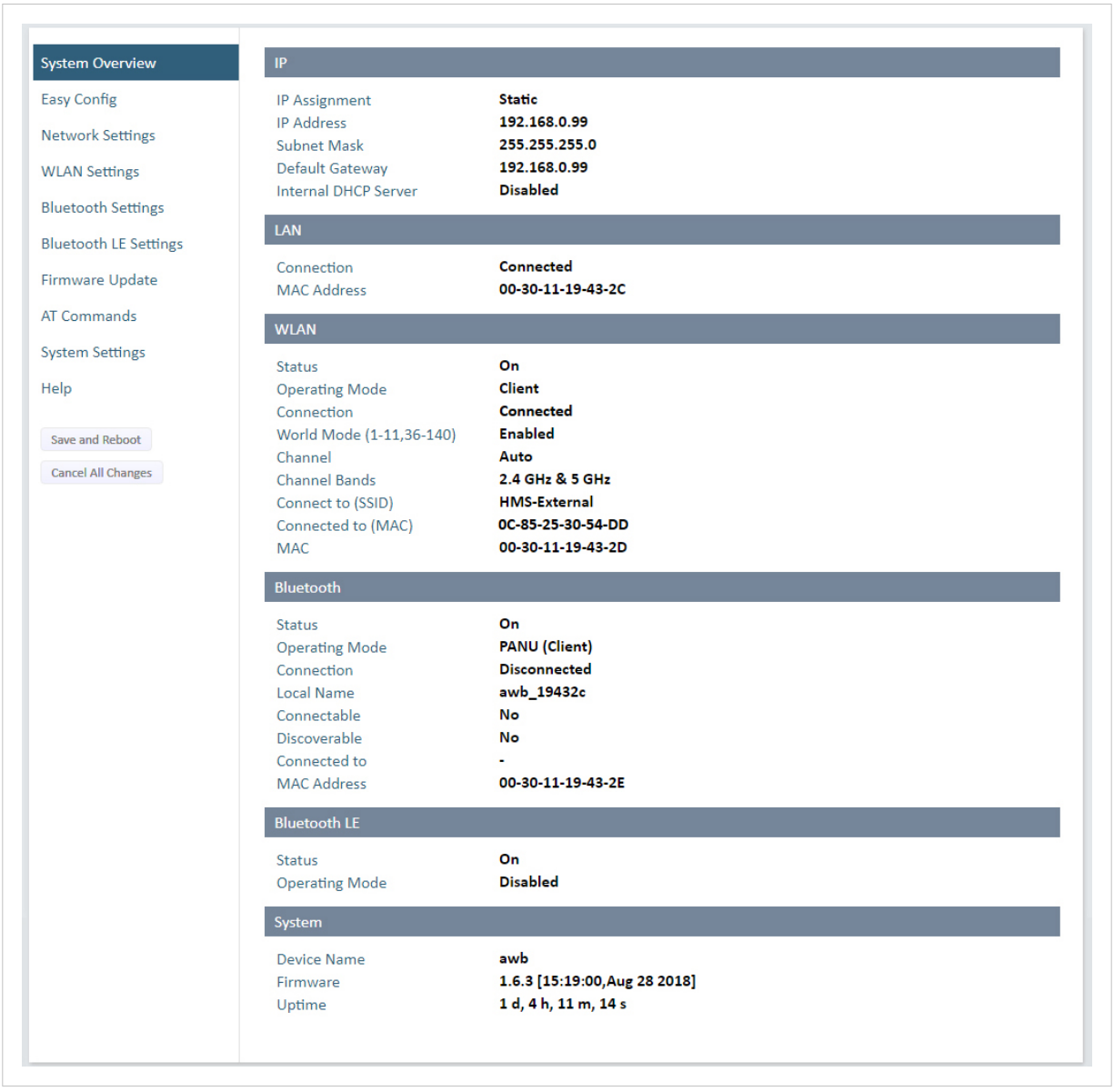


Figure 44. System Overview page example

9. Maintenance

9.1. Firmware Management

9.1.1. Automatically Check for Firmware Updates

By default **Automatic Update Mode** is **Disabled**.

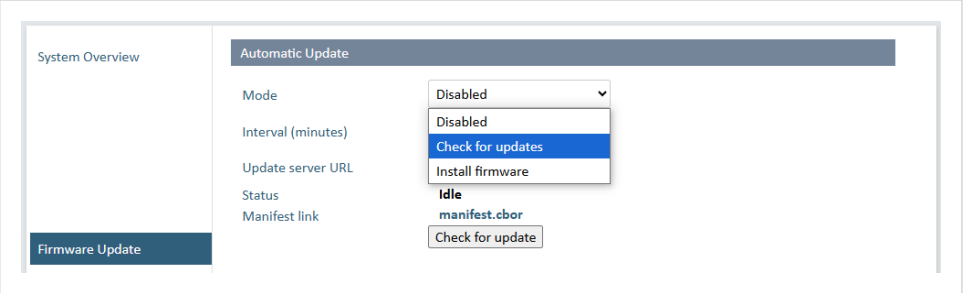


Figure 45. Automatic Update Mode menu, Check for updates

Check for Updates Settings

1. From the **Mode** menu, select **Check for Updates**.
2. In the **Interval** field, specify the frequency in minutes (0-10 000) at which the Bolt 18-Pin should check for new firmware updates.
   The Bolt 18-Pin checks for updates at each boot, and then periodically at the configured interval.
   For the Bolt 18-Pin to check for updates only at boot, set the interval to 0.
3. By default, the firmware is downloaded from a vendor-operated upgrade server.
   To use your own update server, enter its URL in the the **Manifest URL** field. The firmware will be downloaded automatically from this address.

Automated Firmware Search and Download

The Bolt 18-Pin will check for new firmware every [specified number] hour(s).

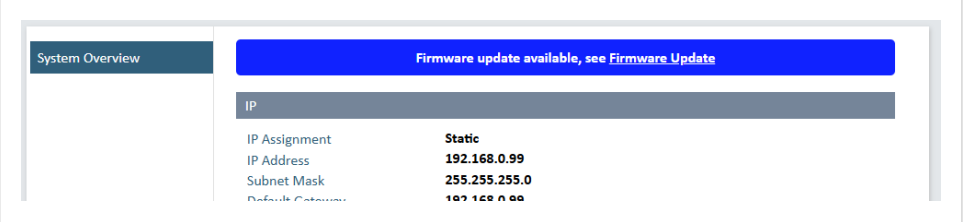


Figure 46. Firmware update available banner

If an firmware update is available, a banner appear below the header indicating that new firmware is ready for installation.

Firmware Installation

To install the firmware, click **Install firmware**.

The firmware is downloaded and installed.

When the firmware installation is completed, the progress bar turn green and the Bolt 18-Pin automatically reboots.

9.1.2. Automatically Update Firmware

By default **Automatic Update Mode** is **Disabled**.

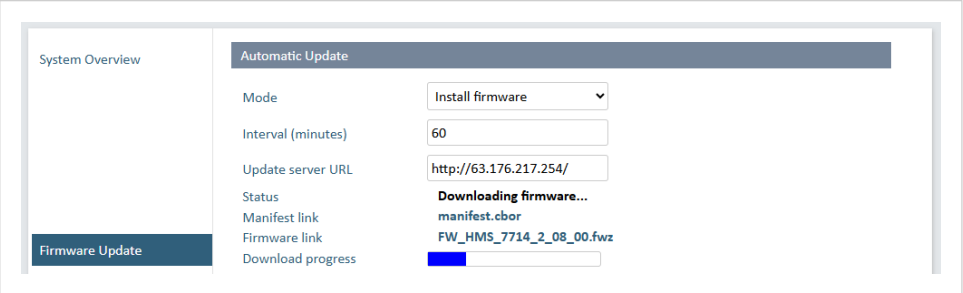


Figure 47. Automatic Update Mode menu, Install firmware

Procedure

1. From the **Mode** menu, select **Install firmware**.
2. In the **Interval** field, enter how often, in minutes, the Bolt 18-Pin should check for new firmware updates. For the Bolt 18-Pin to check for updates on each boot, enter 0.

Result

The Bolt 18-Pin will check for new firmware every [specified interval] hour(s).

If an update is available, it is automatically downloaded and installed.

The Bolt 18-Pin automatically reboots, for the upgrade to take effect.

9.1.3. Manually Update Firmware

Before You Begin

NOTE
For manual firmware installation to work, make sure **Automatic Update Mode** is **Disabled**.

NOTE
The configuration settings are not affected when updating firmware.

Download the Firmware Update File

1. Download the firmware update file from www.hms-networks.com/technical-support.
2. Connect Bolt 18-Pin to your computer, refer to Connect to Configure (page 15).

Procedure

Update the Bolt 18-Pin firmware.

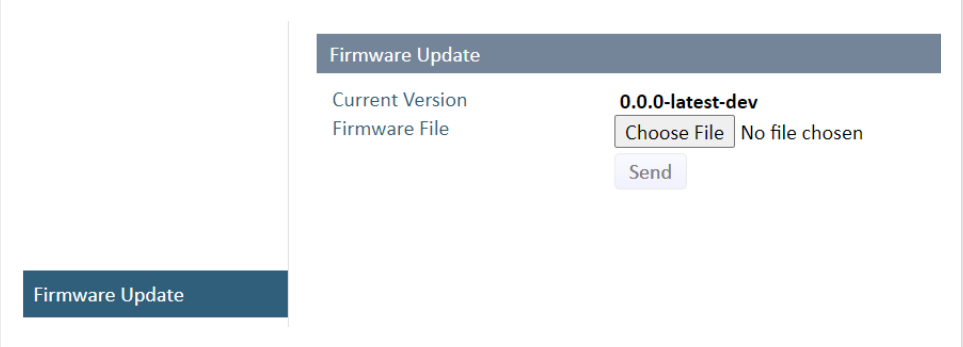


Figure 48. Firmware Update, Choose file

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

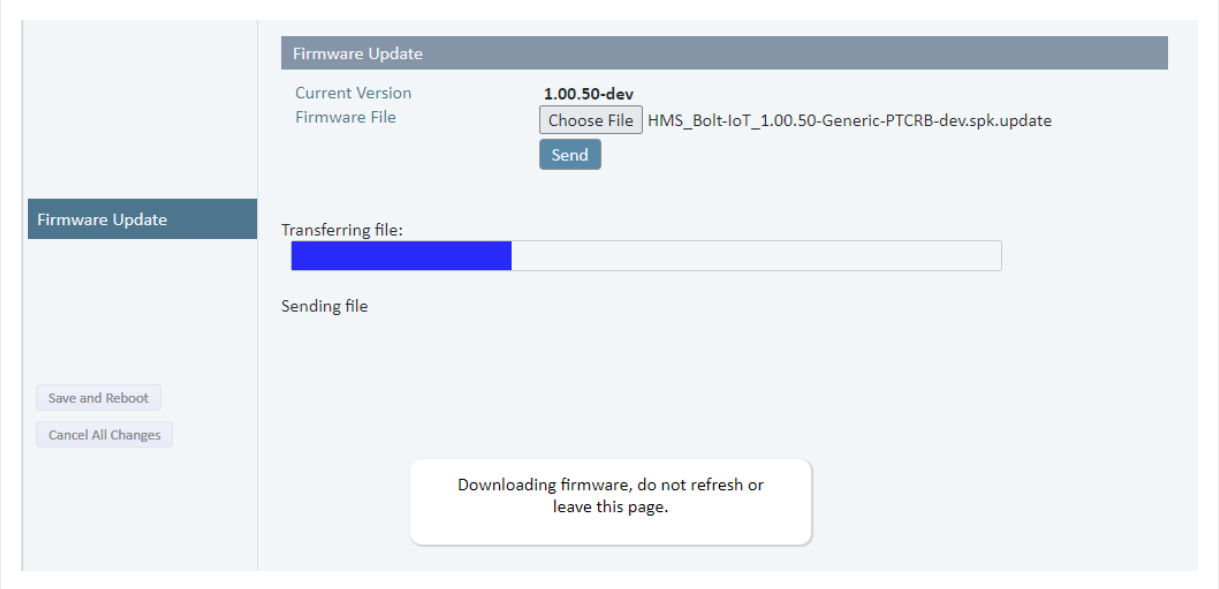


Figure 49. Firmware Update, Transferring file

- 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

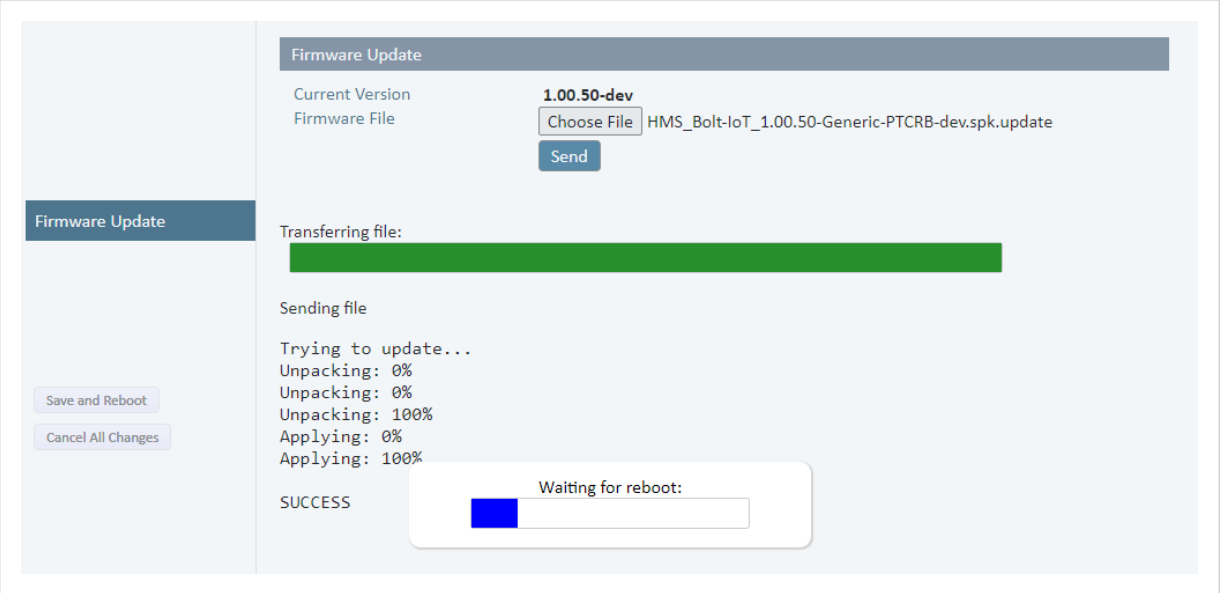


Figure 50. Firmware Update, Waiting for reboot

- When the firmware update is finished, Bolt 18-Pin 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.

9.2. Settings Backup

9.2.1. Create Settings Backup File

IMPORTANT
The Administrator Password is not saved in the settings backup file.

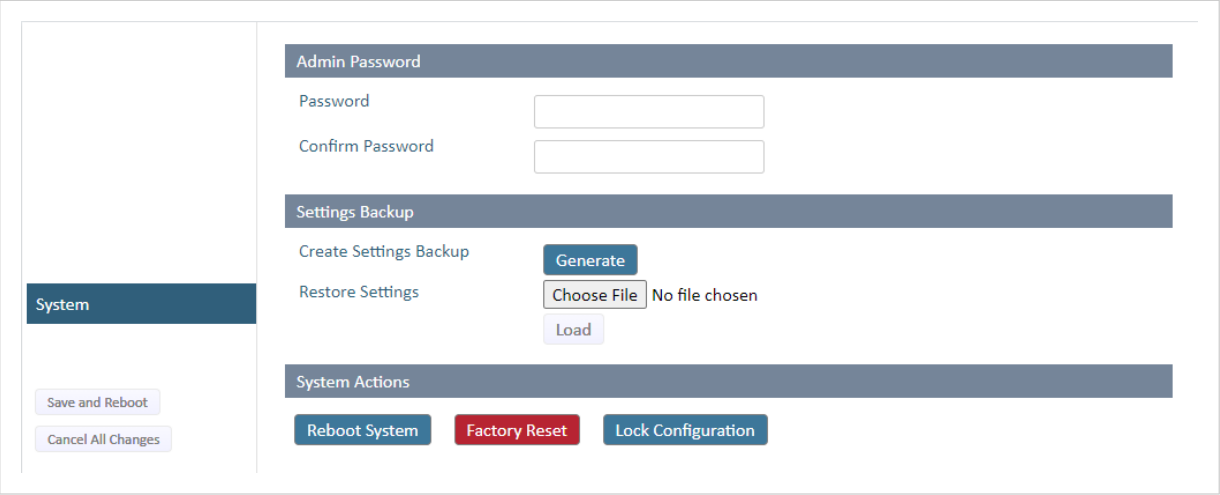


Figure 51. System page

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.

9.2.2. Restore Settings From Backup File

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

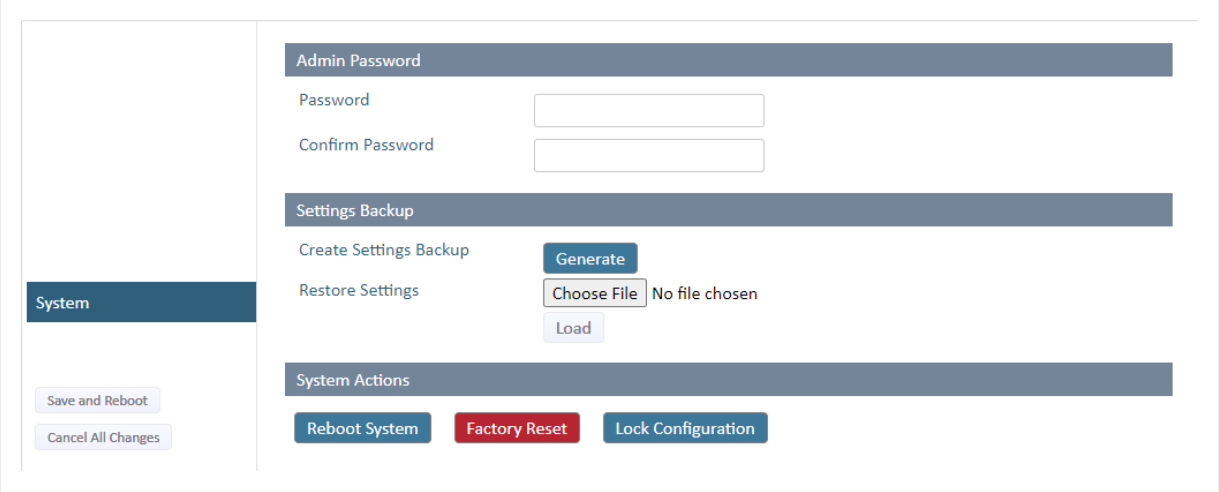


Figure 52. Restore Settings from a backup file

Restore settings from a backup file

1. Click **Choose** file.
2. Browse to and select your backup file.
3. Click **Load**.
   The Bolt 18-Pin reboot automatically, for the settings loaded from the backup file to take effect.

10. Troubleshooting

10.1. Reset Button

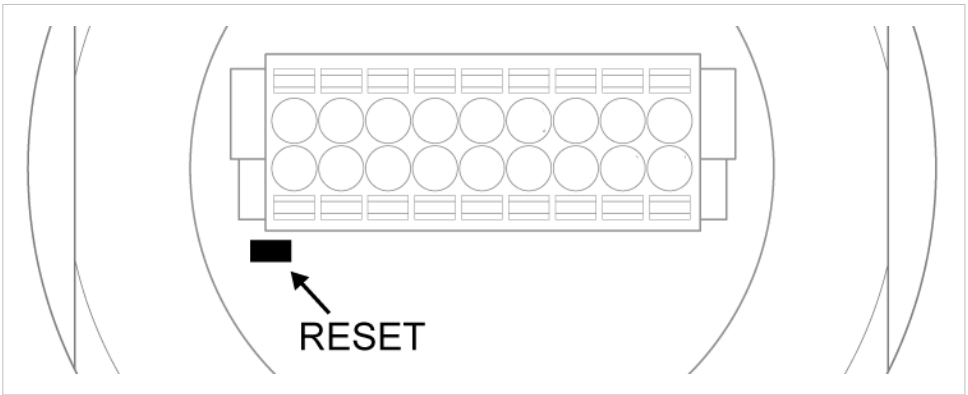


Figure 53. Reset button

The **Reset** button is located on the bottom of the Bolt 18-Pin.

10.2. 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.

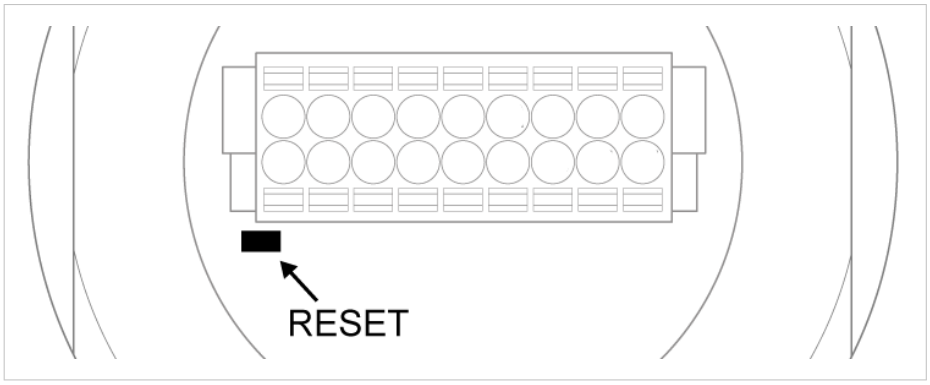


Figure 54. RESET button

2. Bolt 18-Pin enters Recovery Mode.

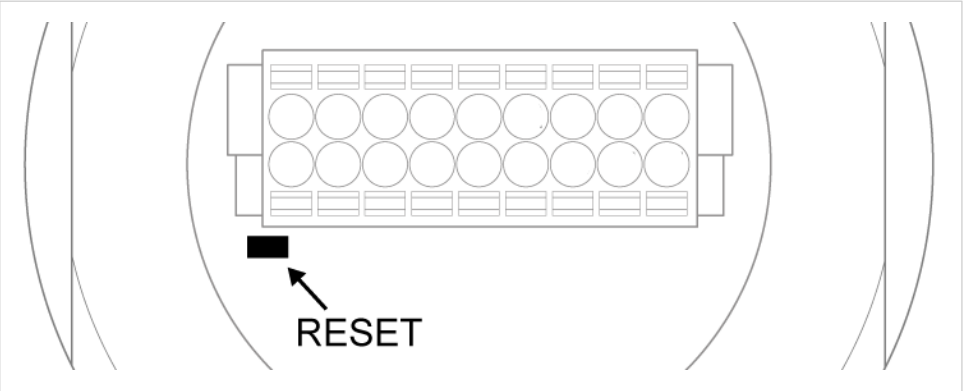
To Reinstall the Firmware

1. To reinstalling the firmware, you need Anybus Firmware Manager II.
   Download Anybus Firmware Manager II from www.hms-networks.com/technical-support.
2. Install Anybus Firmware Manager II on your PC.
3. Launch Anybus Firmware Manager II and follow the instructions to reinstall the firmware.

10.3. Reset to Factory Default

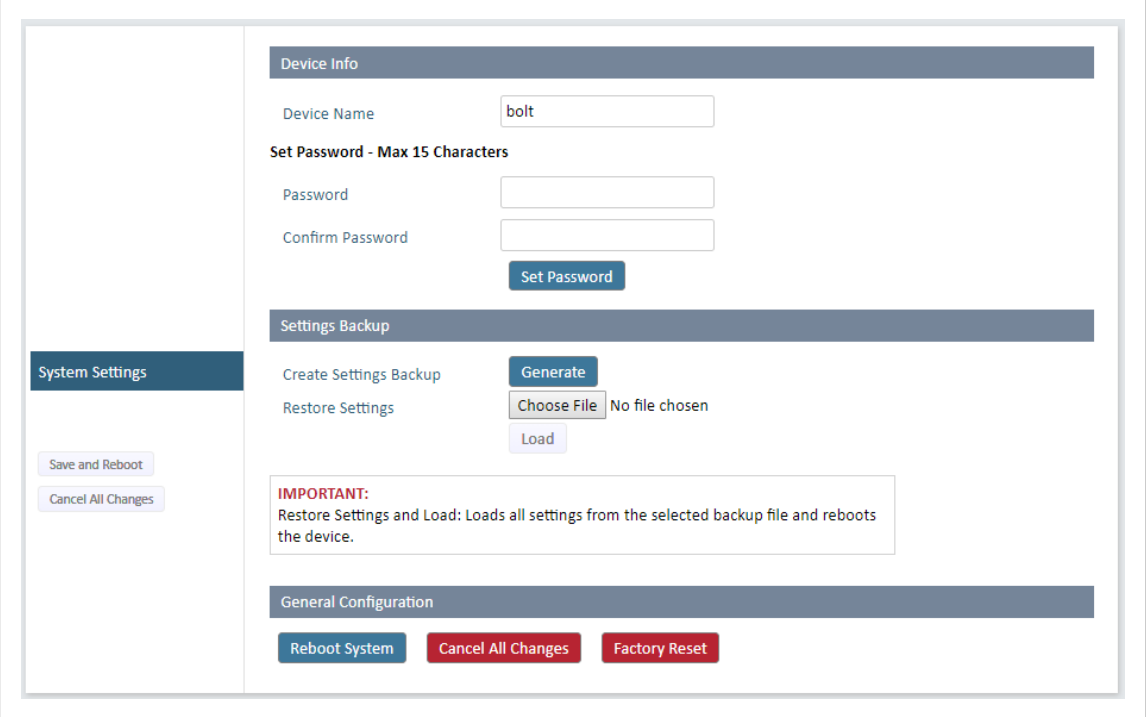
Any one of these actions will restore the unit to factory default settings.

Reset Using the RESET Button



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

Reset Via the Built-In Web Interface



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

Reset Using Easy Config

To reset Bolt 18-Pin to factory default, execute Easy Config Mode 2.

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

Reset Using AT Command

To reset Bolt 18-Pin to factory default, issue the AT command **AT&F** and then restart the unit.

See Configuration with AT Commands (page 25).

Reset Using Digital Input

To reset Bolt 18-Pin to factory default, apply voltage to the digital input for >10 seconds.

See Connector (page 10).

11. End Product Life Cycle

11.1. Secure Data Disposal

IMPORTANT
To reduce the risk of sensitive data exposure, always perform a factory reset before decommissioning the equipment.

A factory reset will reset any on-site made configuration changes and revert the Bolt 18-Pin to the default settings of the latest installed firmware version.

12. Technical Data

12.1. Hardware Specifications

Order code	AWB2000	AWB2001
Color	Black	White top and black base
Wired interface type	Ethernet	
Connector	Included plug connector	
Antenna	Internal dual-band 2.4 GHz and 5 GHz antenna	
Maximum range	100 m (WLAN and Bluetooth)	
Operating temperature	Shadow: -40 to +65 °C Direct sunlight: -40 to +45 °C	Shadow: -40 to +65 °C Direct sunlight: -40 to +65 °C
Storage temperature	-40 to +85 °C	
Humidity	EN 600068-2-78: Damp heat, +40°C, 93% humidity for 4 days	
Vibration	See datasheet	
Dimensions	Height: 75 mm (95 mm incl. connector, 41 mm outside) Diameter: 68 mm	
Weight	81 g	
Housing material	Plastic (see datasheet for details)	
Protection class	Top (outside of host): IP66 / IP67 / UL Type 4X Base (inside of host): IP21	
Mounting	M50 screw and nut (50.5 mm hole needed)	
Power supply	9–30 VDC (-5 % +20 %) Cranking 12 V (ISO 7637-2:2011 pulse 4) Reverse polarity protection	
Power consumption	0.7 W idle, 1.7 W max.	

12.2. Communication

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

Wireless LAN	
Wireless standards	IEEE 802.11 a, b, g, n, d, r
Operation modes	Access point or client
Fast roaming	IEEE 802.11r (client)
Max. number of clients for access point	7
WLAN channels	2.4 GHz Access Point: 1–11 2.4 GHz Client: 1–11 + 12 & 13 depending on regulatory domain scan 5 GHz Access Point: 36–48 (U-NII-1) 5 GHz Client: 36-48 + 100–116, 132–140, 120–128 depending on regulatory domain scan. (U-NII-1, U-NII-2, U-NII-2e)
RF output power	18 dBm EIRP (including max antenna gain 3 dBi)
Power consumption	54 mA @ 24 VDC
Net data throughput	20 Mbps.
Link speed	Max 65 Mbps (802.11n SISO)
Security	WEP 64/128, WPA, WPA-PSK and WPA2, TKIP and AES/CCMP, LEAP, PEAP including MS-CHAP

Classic Bluetooth	
Wireless standards (profiles)	PAN (PANU & NAP)
Operation modes	Access point or Client
Max. number of clients for access point	7
RF output power	14 dBm EIRP (including max antenna gain 3 dBi)
Power consumption	36 mA @ 24 VDC
Net data throughput	~1 Mbps
Bluetooth version support	Classic Bluetooth v2.1
Security	Authentication & Authorization, Encryption & Data Protection, Privacy & Confidentiality, NIST Compliant, FIPS Approved

Bluetooth Low Energy	
Wireless standards (profiles)	GATT
Operation modes	Central or Peripheral (pending)
Max. number of clients for Central	7
RF output power	10 dBm EIRP (including max antenna gain 3 dBi)
Power consumption	36 mA @ 24 VDC
Net data throughput	~200 kbps
Bluetooth version support	Bluetooth 4.0 dual-mode
Security	AES-CCM cryptography

13. Reference Guides

13.1. RS232/RS485 Electrical Connection

RS232 Typical Connection

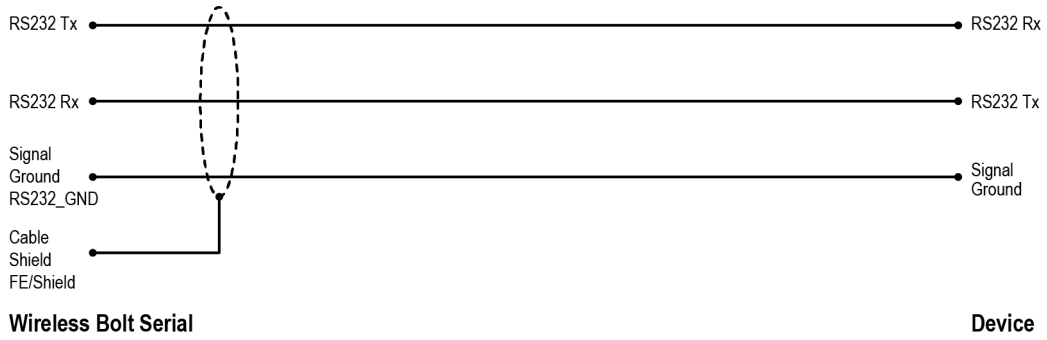


Figure 55. RS232 Typical Connection

RS485 Typical Connection

NOTE
The resistors on the Bolt 18-Pin side are termination resistors which form an active termination of the RS485 line.

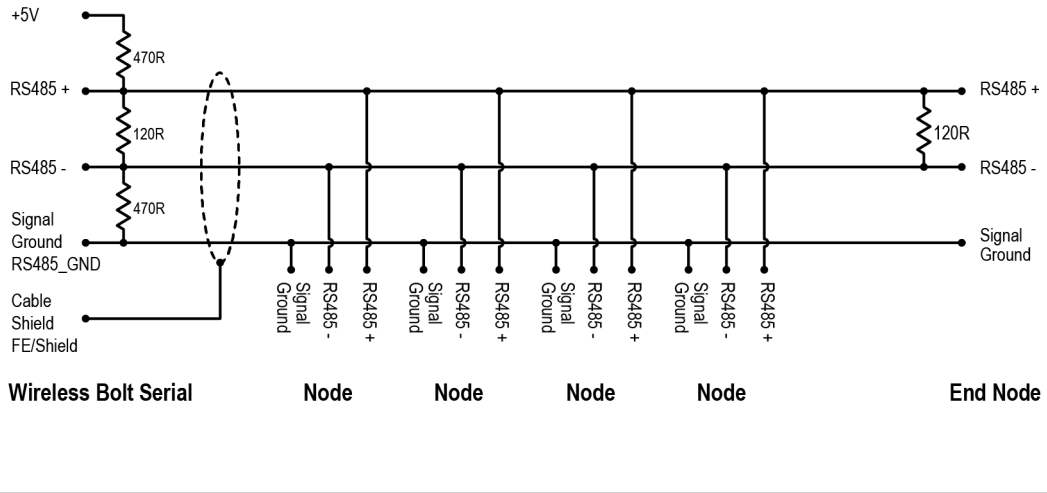


Figure 56. RS485 Typical Connection

13.2. 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.

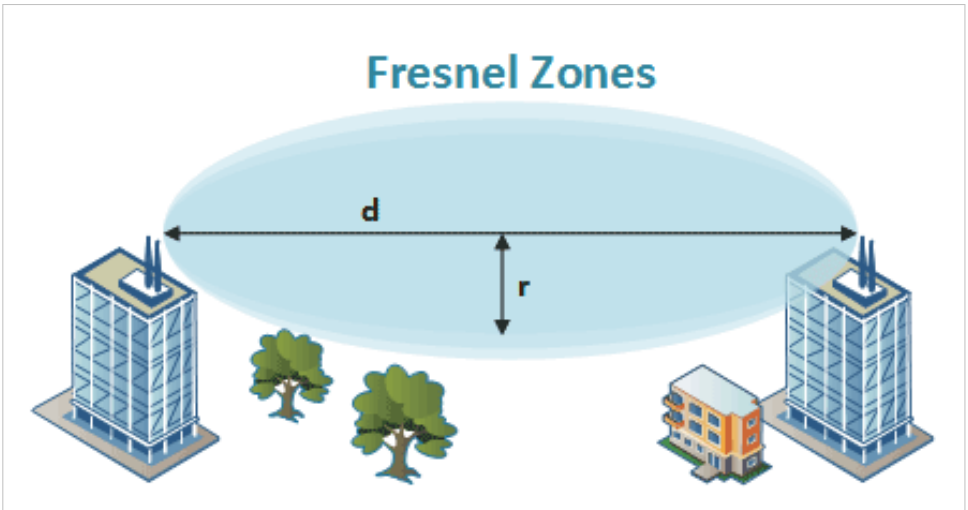


Figure 57. Fresnel zones

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.

13.3. 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.

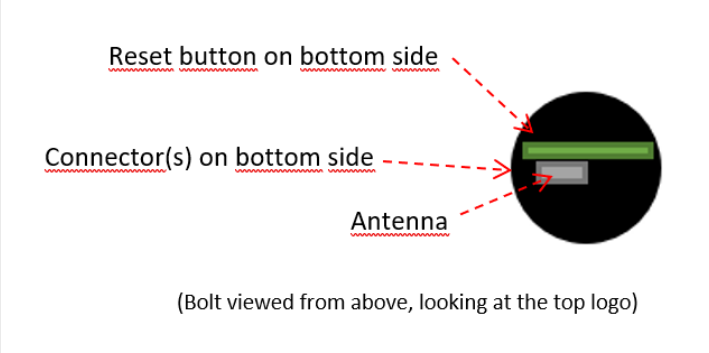


Figure 58. Bolt top view

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.

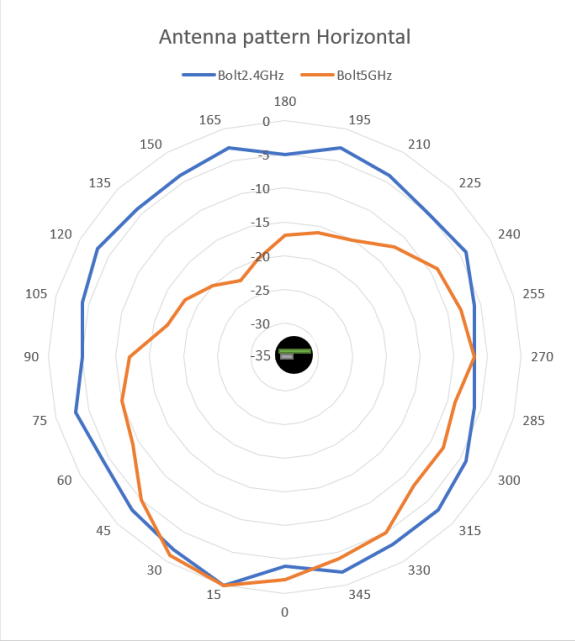


Figure 59. Antenna pattern Horizontal

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.

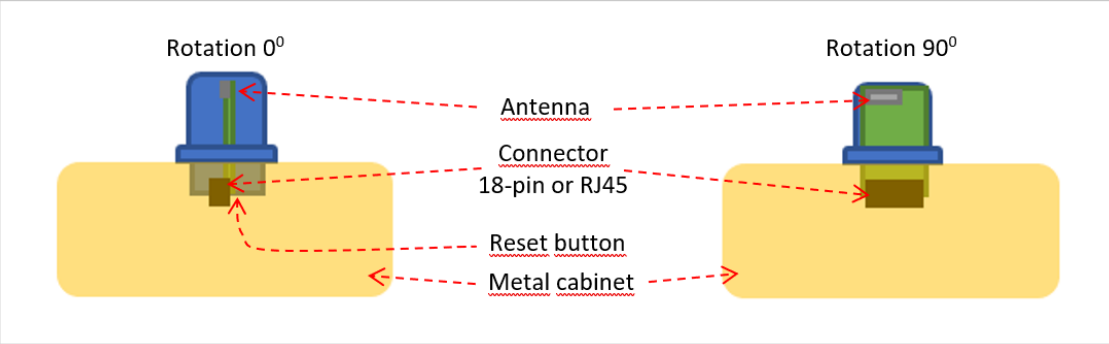


Figure 60. Antenna pattern, Boltrotation 0° and 90°

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.

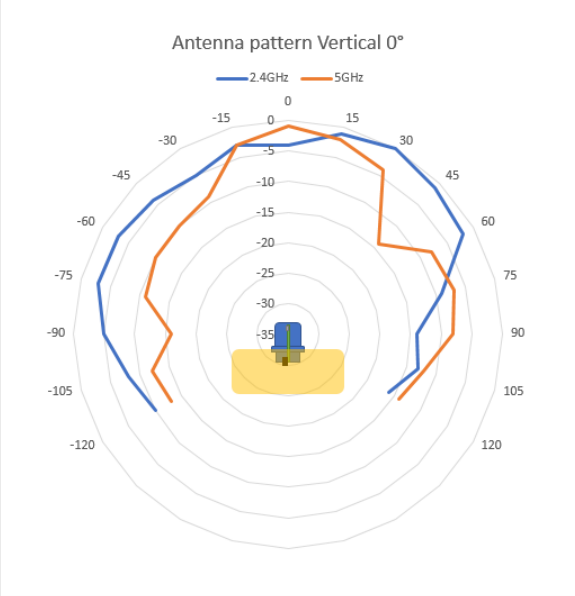


Figure 61. Front View – Vertical 0°

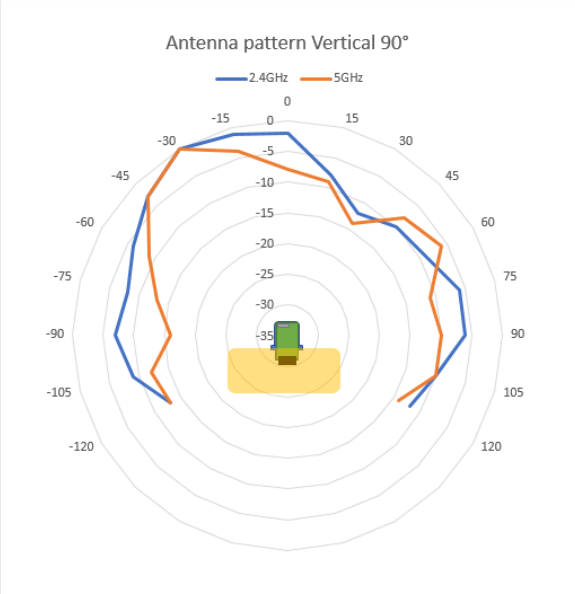


Figure 62. Side View – Vertical 90°

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.

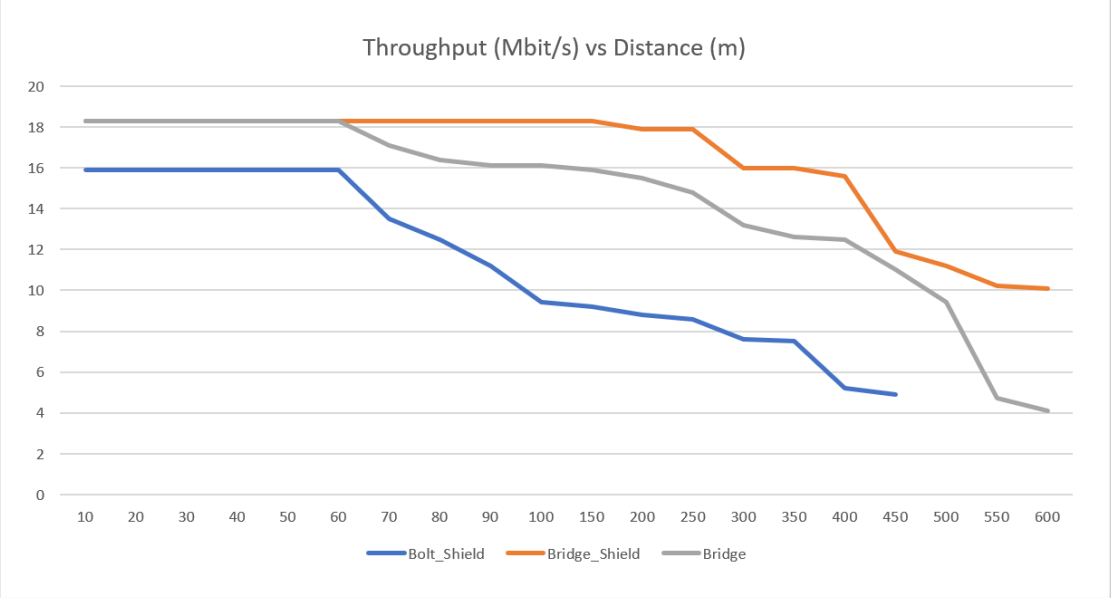

Throughput (Mbit/s) vs Distance (m)
20
18
16
14
12
10
8
6
4
2
0
10 20 30 40 50 60 70 80 90 100 150 200 250 300 350 400 450 500 550 600
Bolt_Shield
Bridge_Shield
Bridge

Figure 63.