Anybus® Wireless Bolt™

USER MANUAL

SCM-1202-007 1.2 ENGLISH

Connecting Devices™

Important User Information

Liability

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

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

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

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

Intellectual Property Rights

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

Trademarks

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

Table of Contents

Page

This page intentionally left blank

1 Preface

1.1 About This Document

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

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

1.2 Related Documents

Document	Author	Document ID
Anybus Wireless Bolt Installation Guide	HMS	SCM-1202-006 (SP2139)
Anybus Wireless Bolt AT Commands Reference	HMS	SCM-1202-004

1.3 Document history

Version	Date	Description
1.0	2016-09-15	First release
1.1	2016-11-23	Minor additions and updates
1.2	2017-12-14	Added configuration example

1.4 Conventions

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

1. First do this
2. Then do this

Unordered (bulleted) lists are used for:

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

...and for action-result type instructions:

- This action...
  ➡ leads to this result

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

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

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

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

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

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

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

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

2 Description

Anybus Wireless Bolt combines Bluetooth® Classic/LE and WLAN 2.4 GHz/5 Ghz connectivity with Ethernet networking and optionally with serial RS-232/485 or CAN.

Bluetooth and WLAN (2.4 GHz) can be used simultaneously. Ethernet can be used at the same time as either the serial interface or the CAN interface. An internal DHCP server can be activated for dynamic IP addressing on a local network.

2.1 Intended Use

Typical applications for Anybus Wireless Bolt include:

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

Limitations

- Bluetooth PAN (Personal Area Network) cannot be used with iOS devices.
- Bluetooth PAN may not be compatible with some Android devices due to varying implementations of Bluetooth by different manufacturers.
- WLAN 5 GHz cannot be used at the same time as WLAN 2.4 GHz or Bluetooth.

3 Installation

Anybus Wireless Bolt should be mounted vertically (logo facing upwards) for best performance due to the characteristics of the internal antenna.

For optimal reception, wireless devices should be placed with a line of sight between them clear of obstructions. A minimum distance of 50 cm between the devices should be observed to avoid interference.

Make sure that you have all the necessary information about the capabilities and restrictions of your local network environment before installing the Anybus Wireless Bolt. Contact your network administrator if in doubt.

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

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

Mechanical Installation

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

Tightening torque: 5 Nm ±10 %

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

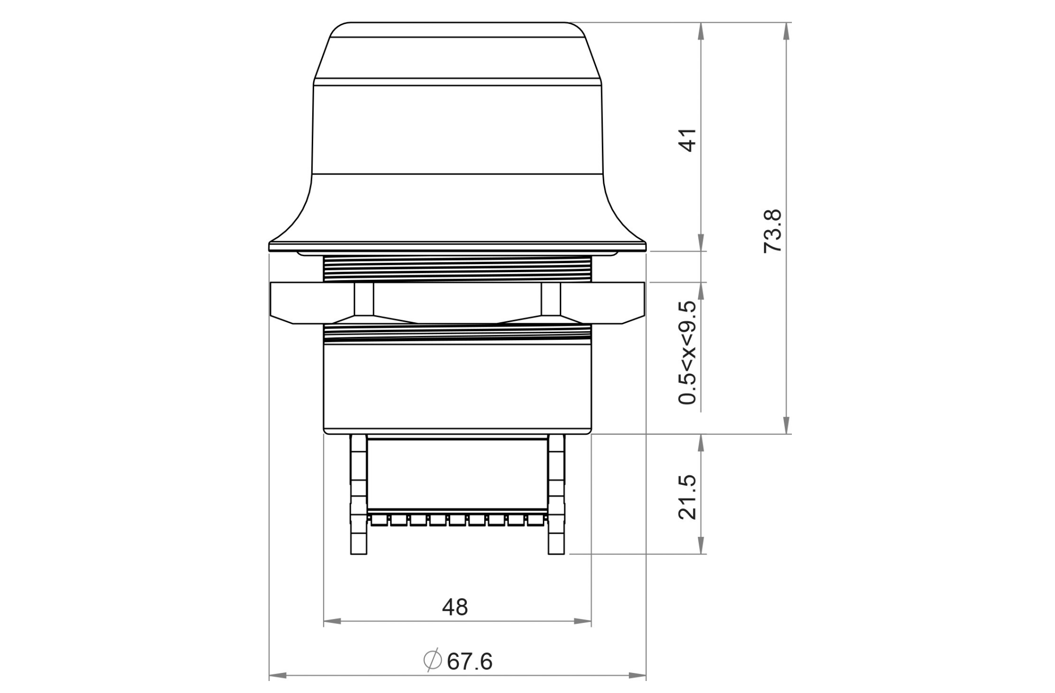


Fig. 1 Installation drawing

All measurements are in mm.

3.1 Connector Pinning

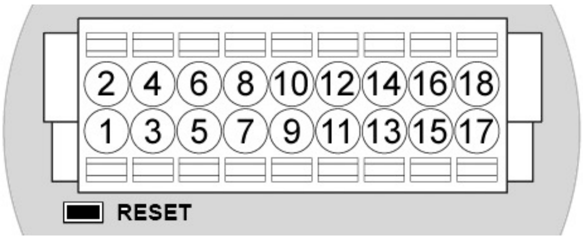


Fig. 2 Connector

Note the location of the **RESET** button when the connector is attached to the Wireless Bolt. Pin 1 will be the pin closest to the button.

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

Note:

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

3.2 Cabling

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

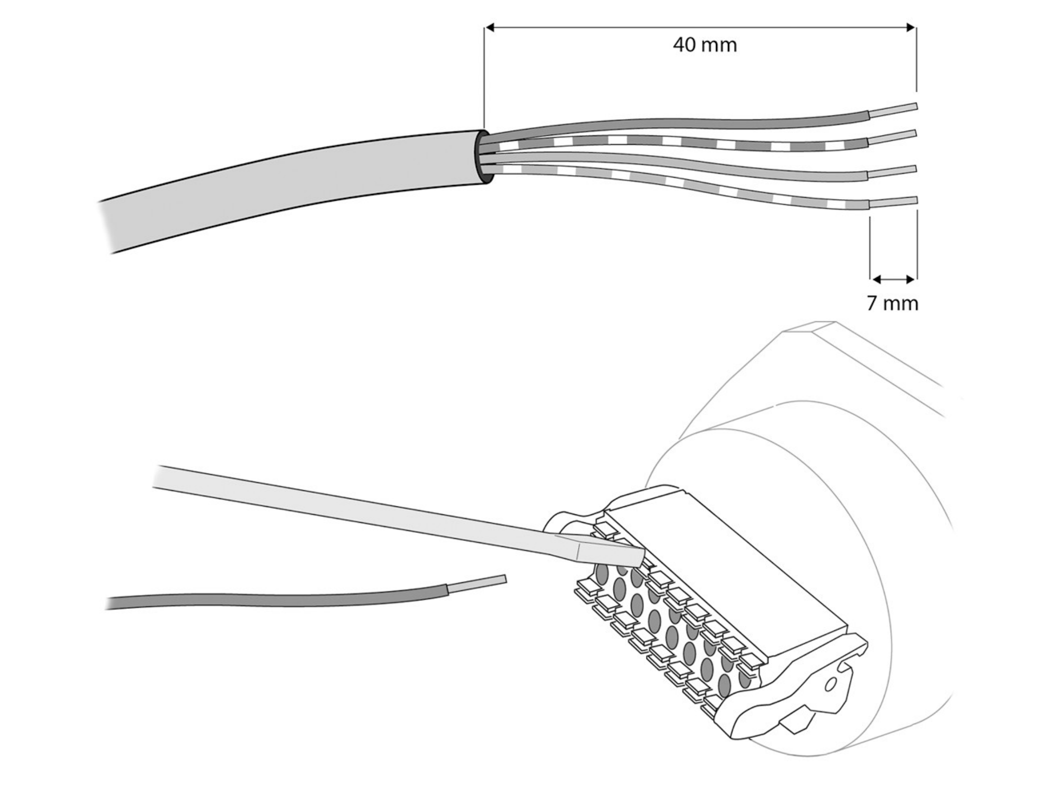


Fig. 3 Ethernet cable

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

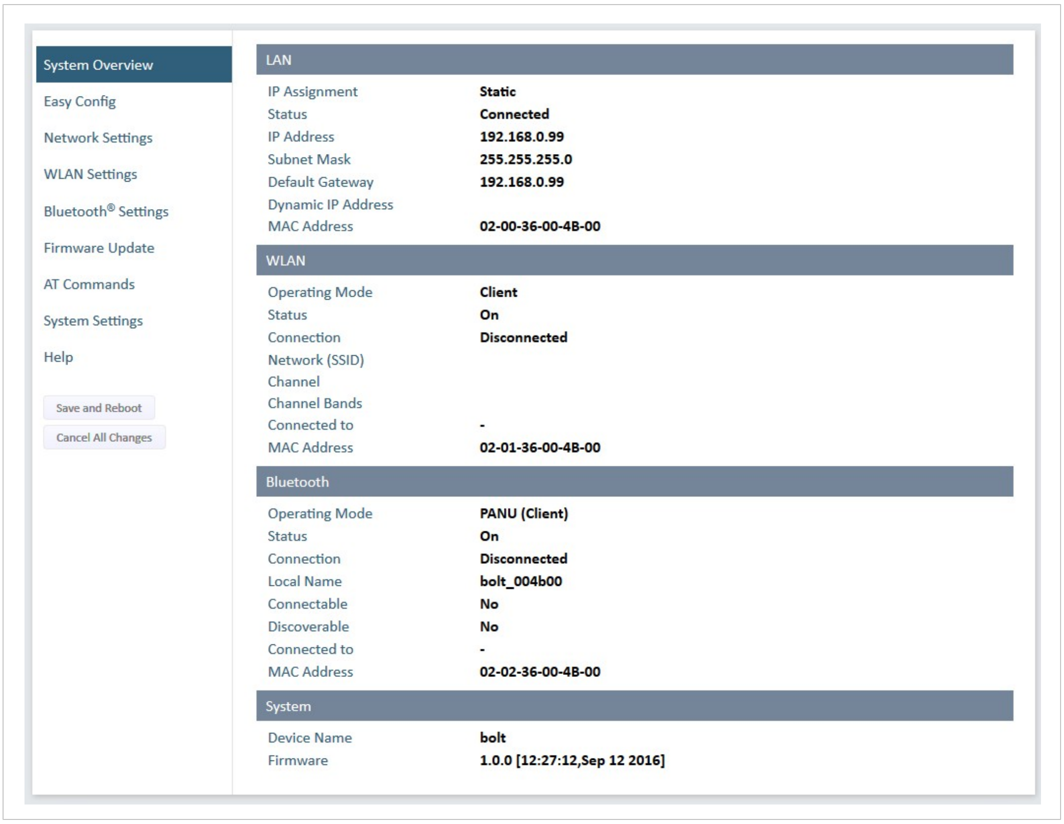
Connect the wires from the power supply to the connector in the same way as the Ethernet wiring. Make sure that polarity is not reversed.

4 Configuration

Anybus Wireless Bolt should normally be configured through the built-in web interface, either by setting individual parameters or by using a pre-configured **Easy Config** mode.

The web interface is accessed by pointing a web browser to the IP address of the internal web server in Wireless Bolt. The default address is **192.168.0.99**.

The start page of the web interface shows an overview of the current settings:



LAN	
IP Assignment	Static
Status	Connected
IP Address	192.168.0.99
Subnet Mask	255.255.255.0
Default Gateway	192.168.0.99
Dynamic IP Address	
MAC Address	02-00-36-00-4B-00

WLAN	
Operating Mode	Client
Status	On
Connection	Disconnected
Network (SSID)	
Channel	
Channel Bands	
Connected to	-
MAC Address	02-01-36-00-4B-00

Bluetooth	
Operating Mode	PANU (Client)
Status	On
Connection	Disconnected
Local Name	bolt_004b00
Connectable	No
Discoverable	No
Connected to	-
MAC Address	02-02-36-00-4B-00

System	
Device Name	bolt
Firmware	1.0.0 [12:27:12,Sep 12 2016]

Fig. 4 System Overview

If the Wireless Bolt needs to be restarted for a parameter change to come into effect, the **Save and Reboot** button will become enabled. To return to the current configuration without saving, click on **Cancel All Changes**.

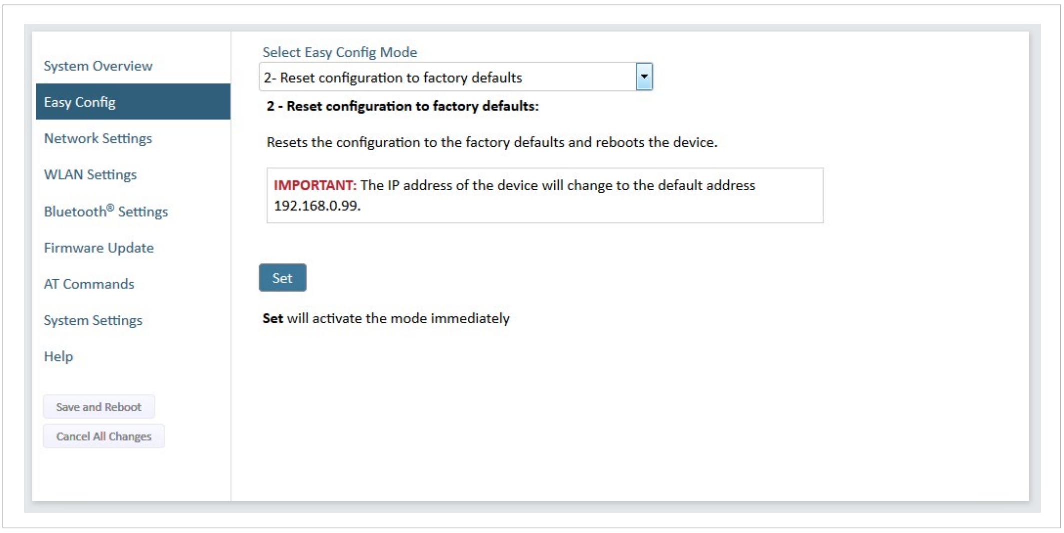
> ! The web interface is designed for the latest versions of Internet Explorer, Chrome, Firefox and Safari. Other browsers may not be supported.

Advanced Configuration

Advanced configuration can be carried out by entering AT (Hayes) command strings directly into the **AT Commands** tab in the web interface, or using a terminal emulator over a Telnet connection to port 8080. A reference manual describing the supported AT commands can be downloaded from www.anybus.com/support.

See also *AT Commands, p. 16*.

4.1 Easy Config

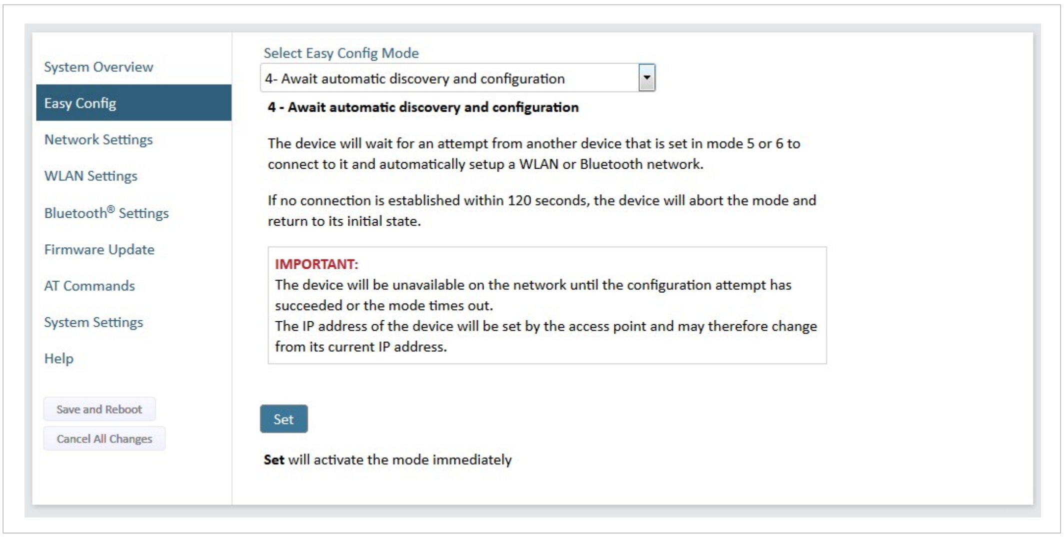


2 - Reset configuration to factory defaults:

Resets the configuration to the factory defaults and reboots the device.

IMPORTANT: The IP address of the device will change to the default address 192.168.0.99.

Set will activate the mode immediately



4 - Await automatic discovery and configuration

The device will wait for an attempt from another device that is set in mode 5 or 6 to connect to it and automatically setup a WLAN or Bluetooth network.

If no connection is established within 120 seconds, the device will abort the mode and return to its initial state.

IMPORTANT:
The device will be unavailable on the network until the configuration attempt has succeeded or the mode times out.
The IP address of the device will be set by the access point and may therefore change from its current IP address.

Set will activate the mode immediately

Fig. 5 Easy Config page

Easy Config allows you to quickly set up basic configurations of Anybus Wireless Bolt.

Modes 2 and 3 are used to reset the unit. Modes 4–6 are used in combination to automatically set up a WLAN or Bluetooth connection between two or more Wireless Bolts.

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

See also *Configuration Examples, p. 20*.

Easy Config Modes

Five Easy Config modes are available in the current firmware version. Additional modes may be implemented in future versions. Please visit www.anybus.com/support for the latest firmware updates and information.

Mode 2 - Reset configuration to factory defaults

Resets the configuration to the factory defaults and reboots the device.

See also *Factory Reset, p. 18*.

Mode 3 - Reset IP settings to factory defaults

Resets the IP settings to the factory defaults, clears the table holding the IP addresses of associated WLAN/ Bluetooth clients, and reboots the device.

> ! When resetting to factory defaults the IP address will be reset to 192.168.0.99. Associated devices may have to be reconfigured to avoid IP address conflicts.

Mode 4 - Await automatic discovery and configuration

Wait for an attempt from a device set in Mode 5 or 6 to connect. The connecting device will configure itself as an access point, and configure the device set in mode 4 as a client. The client device will automatically reboot with the new settings.

The mode will listen for 120 seconds or until the device has received a valid configuration from a device in Mode 5 or 6.

Mode 5 - Configure as WLAN access point and scan for clients

Scan for devices set in Mode 4. If at least one such device is discovered, the scanning device will configure itself as a WLAN access point and configure the other devices as clients. The client devices will then automatically reboot and connect to the access point.

The mode will continue scanning for 120 seconds. If no connection has been established within this period the device will return to its initial state. The mode can be run repeatedly to scan for additional devices.

The access point will automatically assign IP addresses within its own Ethernet subnet range to the clients. See also *Network Settings, p. 12*.

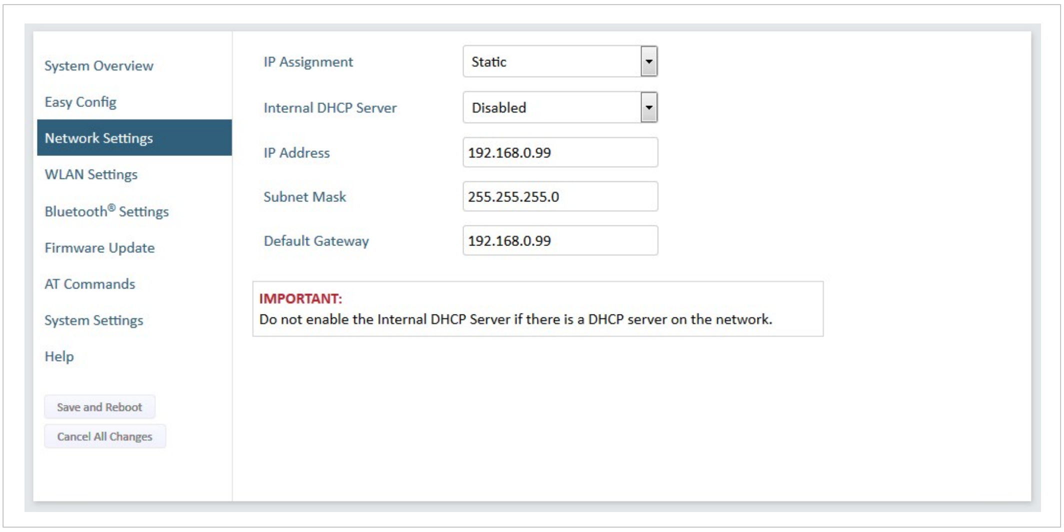
Mode 6 - Configure as Bluetooth access point and scan for clients

Same as Mode 5 but using Bluetooth. The device will be configured as a Bluetooth NAP.

Notes on using Easy Config modes 4–6:

- The devices will be unavailable on the network until the configuration attempt has succeeded or the mode times out.
- The IP address of a client may be changed by the configuration from the access point. Active browser sessions could therefore be lost.
- The devices will always use Bluetooth during the scanning phase. After that they will use either Bluetooth or WLAN depending on the selected mode.

4.2 Network Settings



IP Assignment: Static

Internal DHCP Server: Disabled

IP Address: 192.168.0.99

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.99

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

Fig. 6 Network Settings page

IP Assignment Select static or dynamic IP addressing (DHCP) for the Wireless Bolt.

Internal DHCP Server Activates an internal DHCP server which will assign IP addresses within the current subnet to devices that use DHCP.

Do not enable this option if there is already a DHCP server on the network!

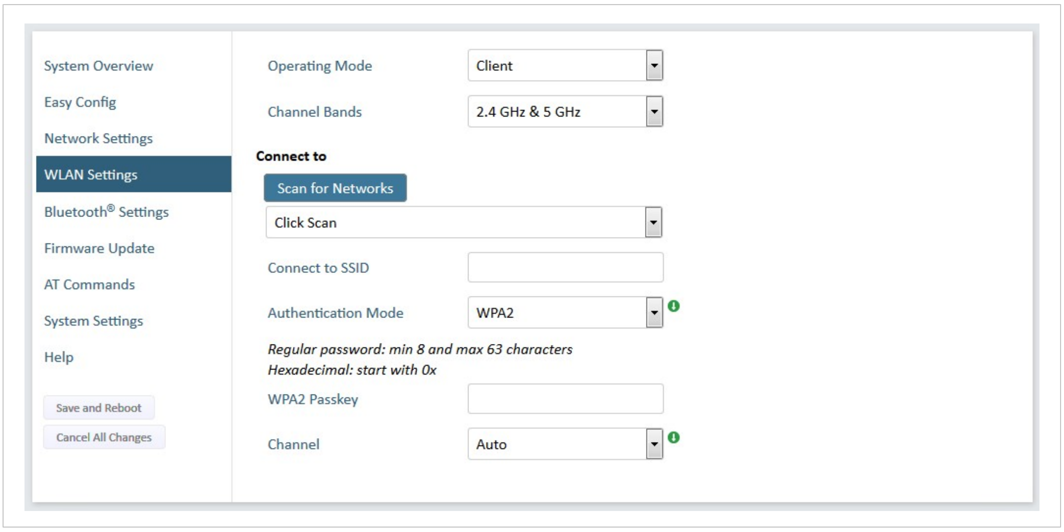
IP Address Static IP address for the Wireless Bolt

Subnet Mask Subnet mask when using static IP

Default Gateway Default gateway when using static IP

After clicking on **Save and Reboot** your web browser should automatically be redirected to the new IP address. The redirect function may not be supported by all browsers, in which case you will have to enter the new IP address in the browser to return to the web interface.

4.3 WLAN Settings



Operating Mode: Client

Channel Bands: 2.4 GHz & 5 GHz

Connect to

Click Scan

Connect to SSID:

Authentication Mode: WPA2

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

WPA2 Passkey:

Channel: Auto

Fig. 7 WLAN Settings – Client

Operating Mode
Choose if the Wireless Bolt should operate as a WLAN Client or Access Point. If Access Point is selected, additional parameters will be visible.

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

Anybus Wireless Bolt can be configured to scan on both the 2.4 GHz and 5 GHz channel bands, but it can only communicate on one band at a time.

Scan for Networks
Scans the currently active frequency band for discoverable WLAN networks. Select a network from the dropdown menu when the scan has completed.

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

Authentication Mode
Select the authentication/encryption mode required by the network.

Open = No encryption or authentication

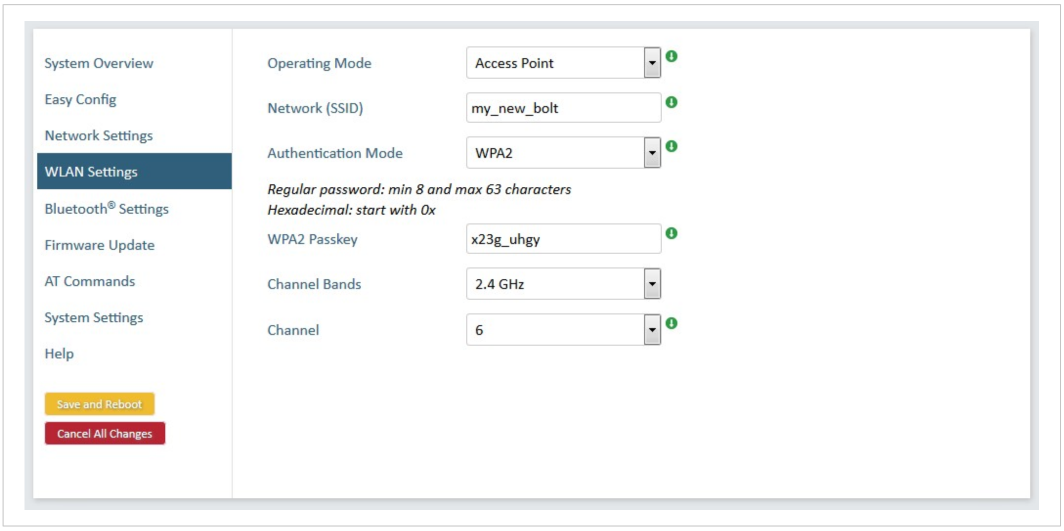
WPA2 = WPA2 PSK authentication with AES/CCMP encryption

Other authentication and encryption modes can be selected using AT commands. See the Anybus Wireless Bolt AT Commands Reference.

WPA2 Passkey
Enter the WPA2 passkey for the network (if required).

Channel
Select a specific channel to use when scanning for networks. Which channels are available depend on the **Channel Bands** setting.

Auto = all channels will be scanned (default).



Operating Mode: Access Point

Network (SSID): my_new_bolt

Authentication Mode: WPA2

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

WPA2 Passkey: x23g_uhgy

Channel Bands: 2.4 GHz

Channel: 6

Fig. 8 **WLAN Settings – Access Point**

Network (SSID)

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

If left blank, the unit will use the default SSID **bolt_xxyyzz**, where “xxyyzz” are the last 6 characters in the MAC ID.

Authentication Mode

Select the authentication/encryption mode to use for the access point.

Open = No encryption or authentication

WPA2 = WPA2 PSK authentication with AES/CCMP encryption

Other authentication and encryption modes can be selected using AT commands. See the Anybus Wireless Bolt AT Commands Reference.

WPA2 Passkey

Enter a string in plain text or hexadecimal format to use for authentication. If left empty, a passkey will be generated automatically.

The passkey will not be displayed after the setting is saved. To retrieve a lost passkey, use the `AT*WKEY?` command. See *AT Commands, p. 16*.

Regular (plain text) passkeys must be between 8 and 63 characters.
All characters in the ASCII printable range (ASCII 32–126) are allowed, except `"` (double quote) `,` (comma) and `\` (backslash). Hexadecimal passkeys must start with `0x` and be **exactly** 64 characters.

See also the example passkeys below.

Channel Bands, Channel

Select the WLAN channel band and channel to use for the access point.

Passkey examples

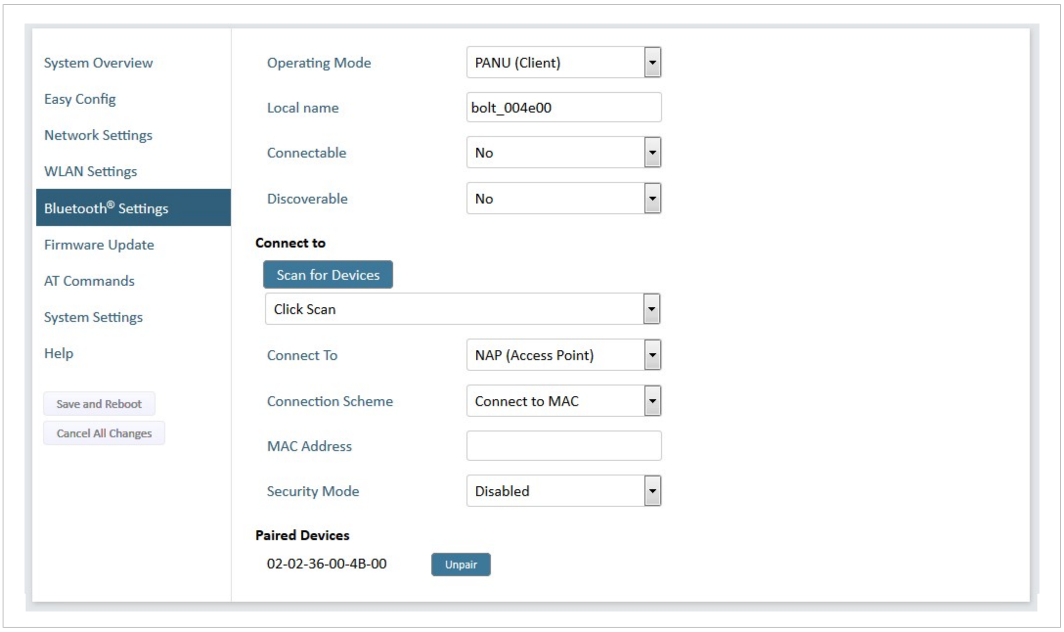
For plain text passkeys a combination of upper and lower case letters, numbers, and special characters is recommended.

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

Example of hexadecimal passkey:
`0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f`

! Do not use the example passkeys above in your installation!

4.4 Bluetooth Settings



Operating Mode: PANU (Client)

Local name: bolt_004e00

Connectable: No

Discoverable: No

Connect to

Click Scan

Connect To: NAP (Access Point)

Connection Scheme: Connect to MAC

MAC Address:

Security Mode: Disabled

Paired Devices

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

Fig. 9 Bluetooth Settings

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

The name identifying the unit to other Bluetooth devices. The default name is **bolt_xxyyzz**, where “xxyyzz” are the last 6 charaters in the MAC ID.

Connectable

Enable to make the unit accept connections initiated by other Bluetooth devices.

Discoverable

Enable to make the unit visible to other Bluetooth devices.

Security Mode

Disabled = No encryption or authentication.

PIN = Encrypted connection with PIN code security. This mode only works when connecting to another Wireless Bolt. PIN codes must consist of 4 to 6 digits.

Just Works = Encrypted connection without PIN code.

Paired Devices

Lists the currently connected Bluetooth devices.

PANU mode only

Scan for Devices

Scans the network for discoverable Bluetooth devices. To connect to a device, select it from the dropdown menu when the scan has completed.

Connect To

Used when connecting manually to a NAP or PANU device.

Connection Scheme

Choose whether to select a Bluetooth device by MAC address or name when connecting manually.

NAP mode only

List Nearby Devices

Scans the network and lists discoverable Bluetooth devices.
Pairing cannot be initiated in NAP mode.

4.5 Firmware Update

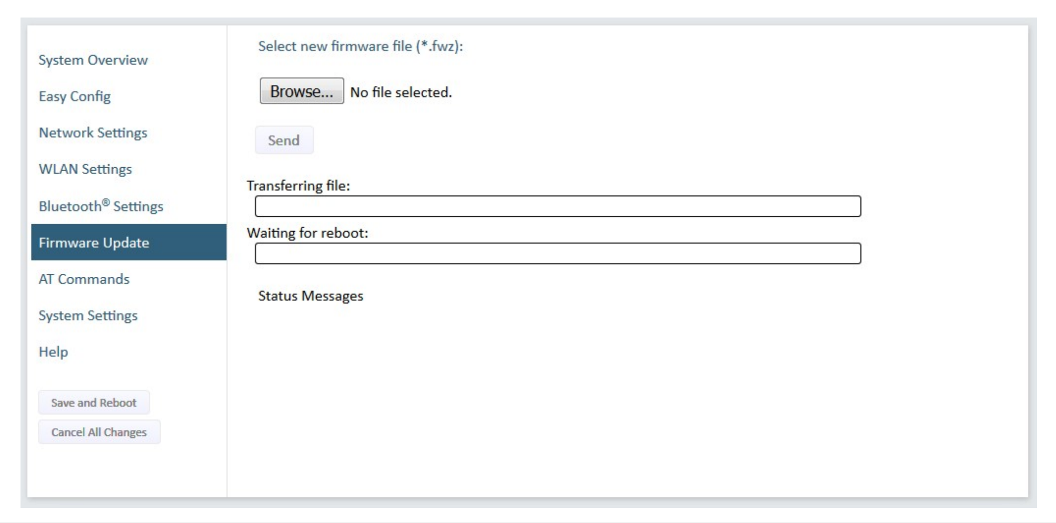
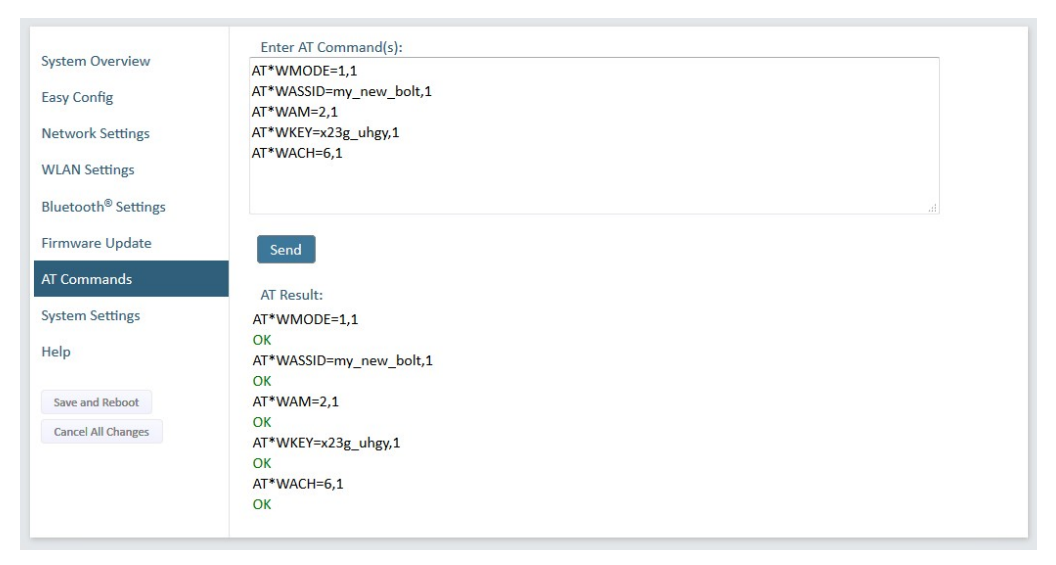


Fig. 10 Firmware Update

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

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

4.6 AT Commands



```
AT*WMODE=1,1
AT*WASSID=my_new_bolt,1
AT*WAM=2,1
AT*WKEY=x23g_uhgy,1
AT*WACH=6,1
```

```
AT*WMODE=1,1
OK
AT*WASSID=my_new_bolt,1
OK
AT*WAM=2,1
OK
AT*WKEY=x23g_uhgy,1
OK
AT*WACH=6,1
OK
```

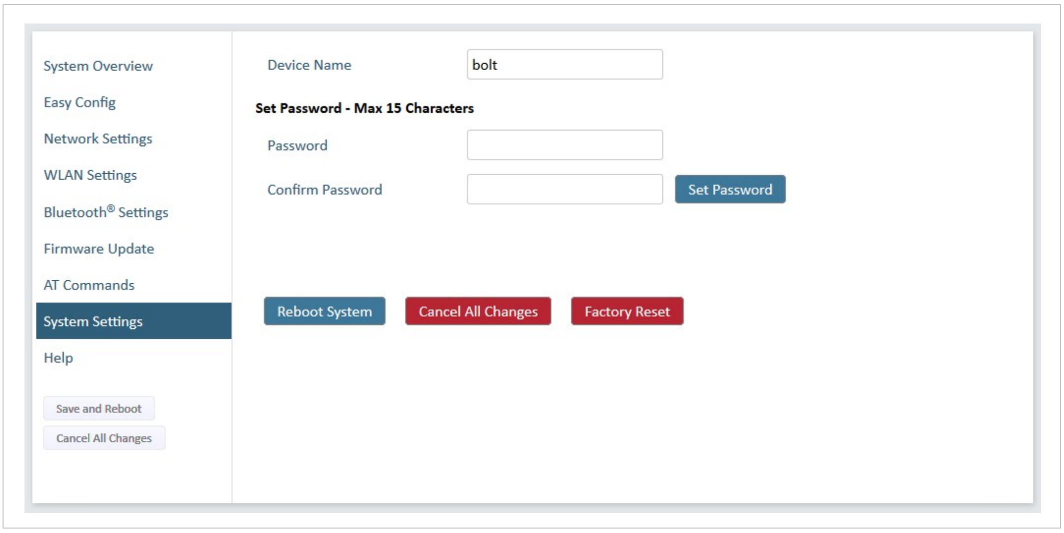
Fig. 11 AT Commands

AT commands can be used for setting parameters that are not available in the web interface, and for batch configuration using command scripts.

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

A reference manual describing all supported AT commands for Anybus Wireless Bolt can be downloaded from www.anybus.com/support.

4.7 System Settings



Device Name: bolt

Set Password - Max 15 Characters

Password

Confirm Password

Fig. 12 System Settings

Device Name Enter a descriptive name for the Wireless Bolt.

Password Enter a password for accessing the web interface.

Reboot System Reboots the system without applying changes.

Cancel All Changes Restores all parameters in the web interface to the currently active values.

Factory Reset Resets the unit to the factory default settings and reboots.

! Setting a secure password for the web interface is strongly recommended.

4.8 Factory Reset

Anybus Wireless Bolt can be reset to the factory default settings using either of the following methods:

- Press and hold the **Reset Button** for >10 seconds and then release it
- Execute **Easy Config Mode 2** through the web interface
- Issue the AT command **AT&F** and reboot

4.8.1 Factory Default Settings

Network Settings

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

WLAN Settings

Operating Mode	Client
Channel Bands	2.4 GHz & 5 GHz
Authentication Mode	Open
Channel	Auto

Bluetooth Settings

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

System Settings

Password	[empty]

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

4.8.2 Reset Button

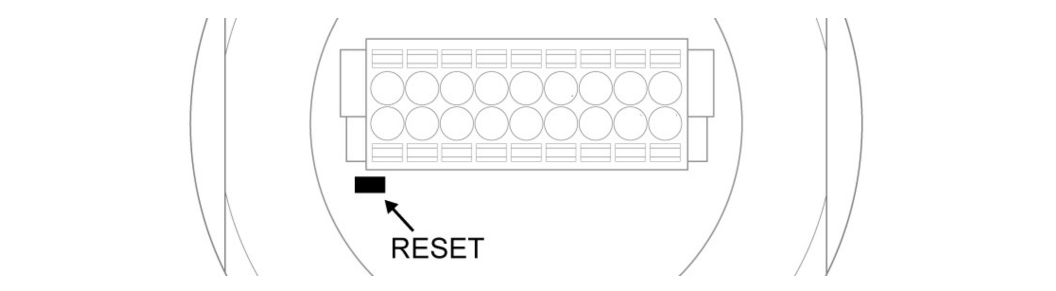


Fig. 13 Reset button

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

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

Recovery Mode

If the web interface cannot be accessed, the unit may be reset by starting in Recovery Mode and reinstalling the firmware using Anybus Firmware Manager II.

For instructions, please refer to the wizard in Anybus Firmware Manager II.

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

4.9 Configuration Examples

The following examples require a basic understanding of how to install Anybus Wireless Bolt and how to access and use the web interface. Please read the *Installation* and *Configuration* sections before you continue.

- All the examples start out from the factory default settings.
- Settings not mentioned in the examples should normally be left at their default values.
- The computer accessing the web interface must be in the same subnet as the Wireless Bolt that is being configured.

4.9.1 Setting up an Ethernet network bridge with Easy Config

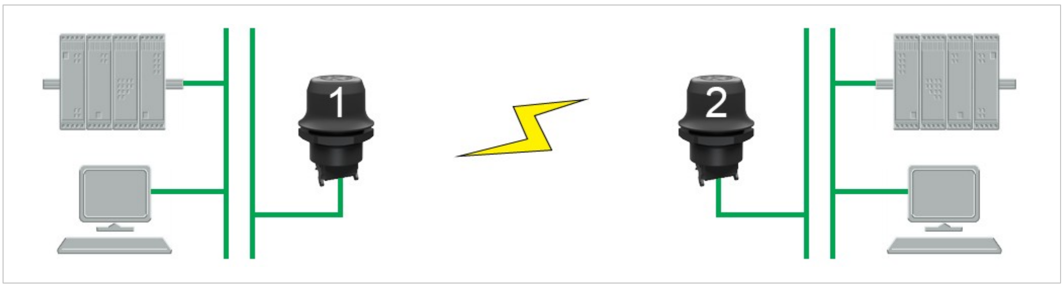
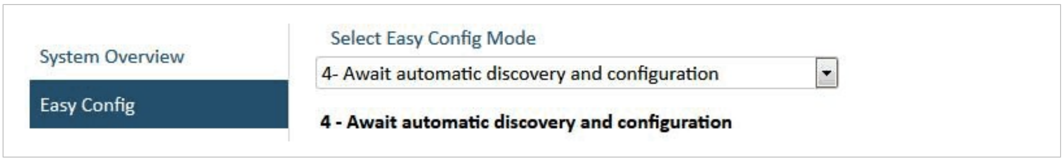


Fig. 14 Setting up a network bridge with Easy Config

This example describes how to connect two Ethernet network segments over WLAN or Bluetooth using two Wireless Bolts.

1. On Wireless Bolt 1, execute **Easy Config Mode 4**. This unit will now be discoverable and open for automatic configuration.



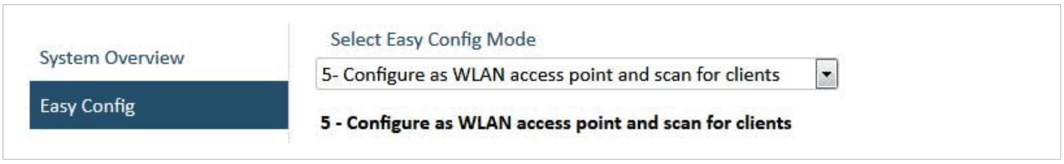
Select Easy Config Mode

4- Await automatic discovery and configuration

4 - Await automatic discovery and configuration

Fig. 15 Easy Config Mode 4

2. On Wireless Bolt 2, execute either **Easy Config Mode 5** for WLAN, or **6** for Bluetooth. This unit should now automatically discover and configure Wireless Bolt 1 as a WLAN or Bluetooth client.
   Wireless Bolt 1 will be assigned the first free IP address within the same Ethernet subnet as Wireless Bolt 2.



Select Easy Config Mode

5- Configure as WLAN access point and scan for clients

5 - Configure as WLAN access point and scan for clients

Fig. 16 Easy Config Mode 5

Adding More Devices

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

4.9.2 Accessing a PLC from a handheld device using WLAN

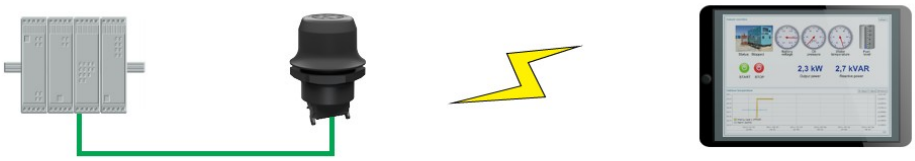


Fig. 17 Accessing a PLC from a handheld device using WLAN

This example describes how to access the web interface of a PLC from a tablet or smartphone using WLAN.

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

A: The PLC or network has an active DHCP server

1. **Network Settings:** Select **IP Assignment**: **Dynamic (DHCP)** and continue to step 3 below.

B: The PLC has a static IP address, no DHCP server on the network

1. Make sure that the IP addresses of the PLC and the Wireless Bolt are within the same Ethernet subnet.
2. **Network Settings:** Select **IP Assignment**: **Static** and enable **Internal DHCP Server**.
3. **WLAN Settings:** Select **Operating Mode** – **Access Point** and enter a unique SSID (network name) for the unit.

   Select an Authentication Mode and a WLAN channel if required by your network environment, otherwise leave them at the default settings.
4. Click on **Save and Reboot** to restart the Wireless Bolt with the new settings.
5. In the WLAN configuration of the handheld device, connect to the SSID (network name) of the Wireless Bolt.

   You should now be able access the web interface of the PLC by entering its IP address in the web browser on the handheld device.

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

4.9.3 PROFINET network communication over WLAN

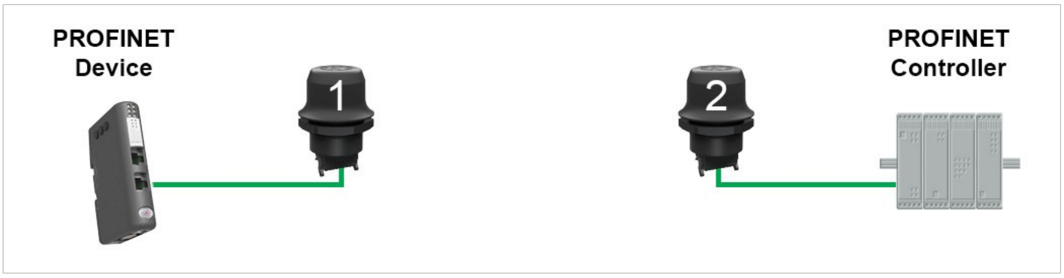


Fig. 18 PROFINET network using two Wireless Bolts

This example describes how to create a WLAN connection between a PROFINET device (slave) and a PROFINET controller (master) using two Wireless Bolts.

1. Reset the two Wireless Bolts to the factory default settings.
2. Change the IP address of one or both of the Wireless Bolts so that each unit has a unique IP address within the same subnet, e.g. 192.168.0.99 and 192.168.0.100.
3. On each of the Wireless Bolts, go to the **AT Commands** tab and enter the command `AT*WSBM=0` then click **Send**.

   This will change the WLAN bridging mode of the Wireless Bolt to *Layer 2 Tunnel Mode*, which is required for PROFINET traffic to be forwarded over WLAN.
4. Restart both Wireless Bolts.

The PROFINET device should now be able to communicate with the PROFINET controller as if using a wired connection. Please refer to the documentation for the respective units on how to configure PROFINET communication.

A Technical Data

General Specifications

Wired Interface type	Ethernet	Serial RS-232/485 + Ethernet	CAN + Ethernet
Order code	AWB2000	AWB2010	AWB2020
Range	Up to 100 meters		
Antenna	Built-in		
Operating temp.	-40 to +65 °C		
Weight	81 g		
Housing	Plastic (PBT glass-reinforced/PC-ABS)		
IP class	IP67 for top (outside of host), IP21 for bottom (inside host)		
Dimensions	Height: 70 mm (95 mm incl. connector, 41 mm outside) Diameter: 70 mm		
Mounting	M50 screw and nut (50.5 mm hole required)		
Connector	Included plug connector (2 x 9 pin 3.5 mm Phoenix DFMC 1.5/9-ST-3.5 push-in spring connection)		
Power supply	9–30 VDC (-5% +20%) Cranking 12 V (ISO 7637-2:2011 pulse 4) Polarity reversal protection		
Power consumption	0.7 W (idle) – 1.7 W (max)		
Browser support	Internet Explorer, Firefox, Chrome, Safari (latest stable versions)		
Configuration	Built-in web interface / Easy Config Modes / AT commands		
Vibration	Sinosodial vibration test according to IEC 60068-2-6:2007 and with extra severities; Number of axes: 3 mutually perpendicular (X:Y:Z), Duration: 10 sweep cycles in each axes, Velocity: 1 oct/min, Mode: in operation, Frequency: 5–500 Hz, Displacement ±3.5 mm, Acceleration: 2 G. Shock test according to IEC 60068-2-27:2008 and with extra severities; Wave shape: half sine, Number of shocks: ±3 in each axes, Mode: In operation, Axes ± X,Y,Z, Acceleration: 30 m/s^2 , Duration: 11 ms		
Humidity	EN 600068-2-78: Damp heat, +40 °C, 93 % humidity for 4 days		
Certifications	See Anybus Wireless Bolt Compliance Sheet		

Host Communication

Ethernet interface	10/100BASE-T, auto MDI/MDIX cross-over detection Supported protocols: IP, TCP, UDP, HTTP, LLDP, ARP, DHCP Client/Server, DNS support, PROFINET IO, EtherNet/IP, Modbus-TCP
Serial interface	Isolated RS-232/485 (max. 1 Mbit/s)
CAN interface	Isolated CAN (max. 1 Mbit/s)
Digital input	9–30 VDC (max. 3 m signal cable length)

WLAN Specifications

Wireless standards	WLAN 802.11a/b/g/d/e/i/h
Operation modes	Access Point or Client
2.4 GHz channels	1–11
5 GHz channels	36–48 (U-NII-1), 52–64 (U-NII-2), 100–140 (U-NII-2e)
RF output power	16 dBm
Max number of clients	7 (for access point)
Power consumption	54 mA @ 24 VDC (WLAN interface only)
Net data throughput	Up to 20 Mbit/s
Authentication	WPA/WPA2-PSK, LEAP, PEAP
Encryption	WEP64/128, TKIP, AES/CCMP

Bluetooth Specifications

Core specification	4.0
Wireless profiles	PAN (PANU & NAP)
Operation modes	Access Point or Client
RF output power	10 dBm
Max number of clients	7 (for access point)
Power consumption	36 mA @ 24 VDC (Bluetooth interface only)
Net data troughput	Up to 1 Mbit/s
Security	Authentication & Authorization, Encryption & Data Protection, Privacy & Confidentiality, NIST Compliant, FIPS Approved

This page intentionally left blank

Box 4126
300 04 Halmstad, Sweden

info@hms.se