Anybus® Wireless Bridge II™

USER MANUAL

SCM-1202-032 1.0 ENGLISH

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.

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 Bridge II.

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 Bridge II Installation Guide	HMS	SCM-1202-013 (SP2167)
Anybus Wireless Bridge II AT Commands Reference	HMS	SCM-1202-004

1.3 Document history

Version	Date	Description
1.0	2017-03-31	First public release

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 Bridge II provides wireless communication over WLAN and/or Bluetooth® to wired networks.

Typical applications for Anybus Wireless Bridge II include:

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

WLAN or Bluetooth?

Choose WLAN when data throughput and seamless roaming are most important and there are few other radio emitting devices in the environment.

Choose Bluetooth if connection robustness and low latency are most important, and in environments with many other radio emitters.

Limitations

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

3 Installation

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

! This product is recommended for use in both industrial and domestic environments. For industrial environments it is mandatory to use the functional earth connection to comply with immunity requirements. For domestic environments the functional earth must be omitted if a shielded Ethernet cable is used, in order to meet emission requirements.

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

3.1 General

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

The characteristics of the internal antenna should be considered when choosing the placement and orientation of the unit (unless an external antenna is used).

See *Technical Data, p. 28* for details about the antenna characteristics.

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

See also *Wireless Technology Basics, p. 27*.

3.2 Mechanical Installation

Anybus Wireless Bridge II can be screw-mounted directly onto a flat surface or mounted on a standard DIN rail using the optional DIN mounting kit.

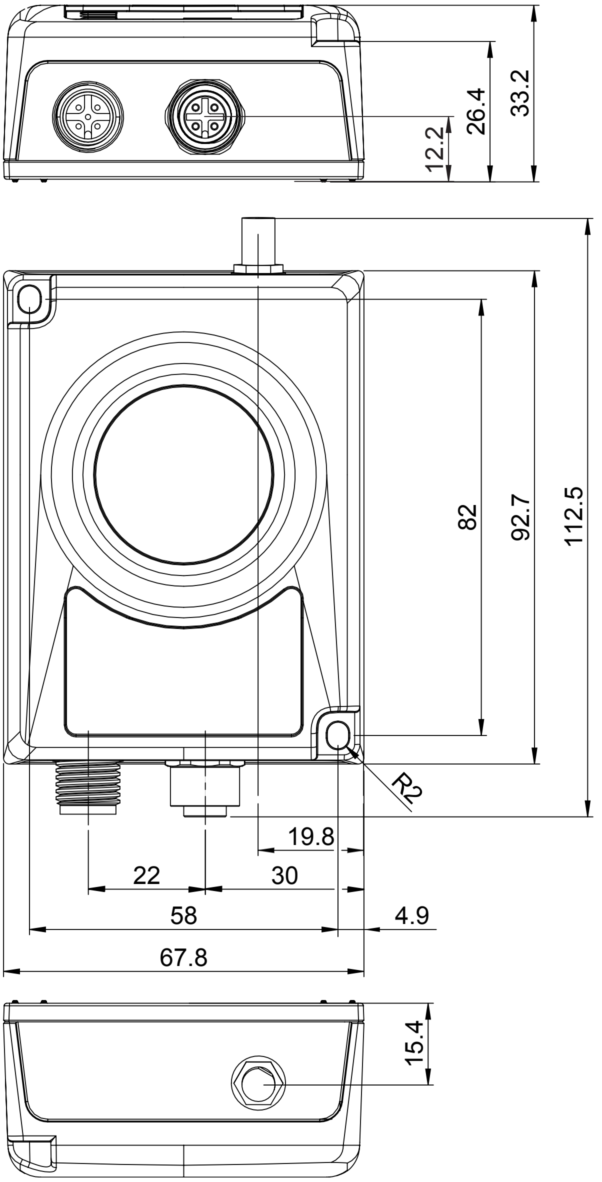


Fig. 1 Installation drawing

All measurements are in mm.

3.3 Connectors

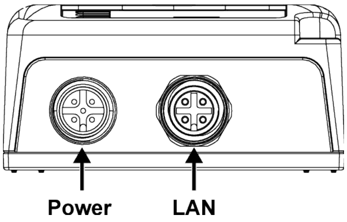
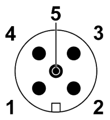


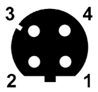
Fig. 2 M12 connectors

Power Connector (A-coded male M12)

	Pin	Function
	1	Power + (9–30 V)
	2	Digital Input Ground
	3	Power Ground
	4	Digital Input + (9–30 V)
	5	Functional Earth

! Signal wiring for the digital input must be carried in the same cable as power and functional earth if wiring length exceeds 3 meters.

LAN Connector (D-coded female M12)

	Pin	Function	Color coding (T568B)
	1	Transmit +	Orange/White
	2	Receive +	Green/White
	3	Transmit -	Orange
	4	Receive -	Green

3.4 LED Indicators

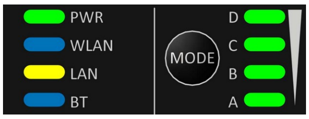


Fig. 3 LED indicators

PWR	Off	No power
	Green	Normal operation
WLAN	Off	WLAN disabled or no power
	Blue	Access Point mode: Connected to at least one client Client mode: Connected to access point
	Blue, flickering	WLAN data activity (when connected)
	Purple, blinking	Client mode: Scanning for access points
	Purple	Client mode: Connecting to a detected access point
	Red	Unrecoverable error
LAN	Off	No Ethernet connection
	Yellow	Ethernet link present
	Yellow, flickering	Ethernet data activity (when connected)
BT	Off	Bluetooth disabled or no power
	Blue	NAP mode: Connected to at least one PANU client PANU mode: Connected to NAP
	Blue, flickering	Bluetooth data activity (when connected)
	Purple	PANU mode: Trying to connect to NAP
	Red	Unrecoverable error
A-B-C-D	Green	RSSI (received signal strength) or Link Quality See also *Easy Config, p. 11*.

RSSI (WLAN Client) / Link Quality (Bluetooth PANU)	**A**	**B**	**C**	**D**
No connection				
RSSI/Link Quality < 25 %	●			
RSSI/Link Quality 25–50 %	●	●		
RSSI/Link Quality 50–75 %	●	●	●	
RSSI/Link Quality > 75 %	●	●	●	●

Additional LED indications are used when the unit is in Recovery Mode.
See *Recovery Mode LED Indications, p. 24*.

4 Configuration

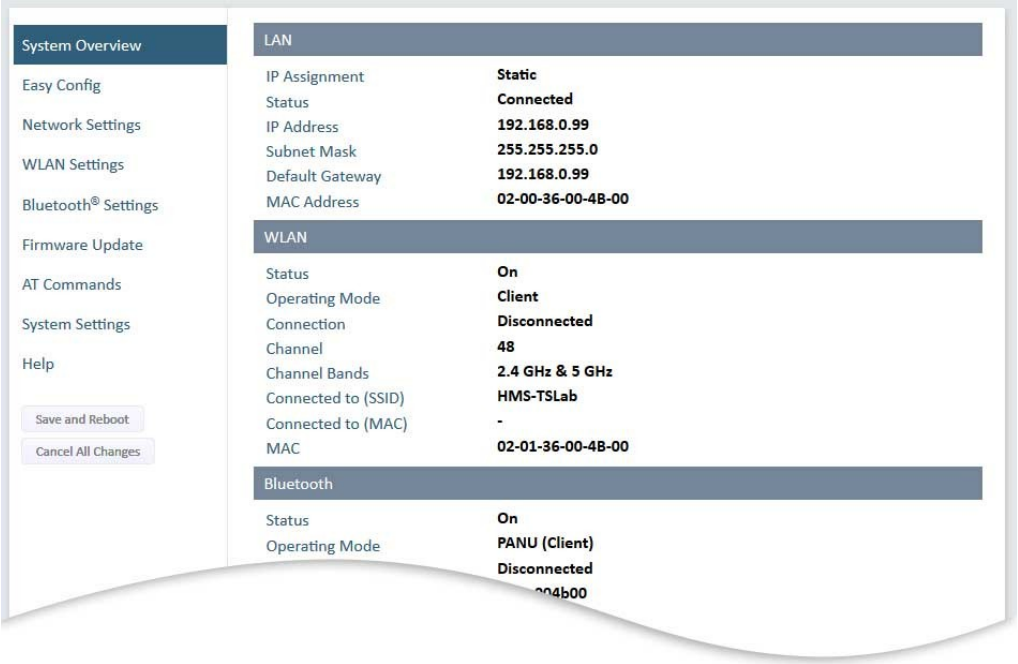
4.1 General

Anybus Wireless Bridge II should normally be configured via the web interface or using one of the pre-configured **Easy Config** modes.

Advanced configuration can be carried out by issuing AT (modem) commands through the web interface or over a Telnet or RAW TCP connection to port 8080. The **Help** page in the web interface includes a list of all supported AT commands.

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

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



LAN

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

WLAN

Status	On
Operating Mode	Client
Connection	Disconnected
Channel	48
Channel Bands	2.4 GHz & 5 GHz
Connected to (SSID)	HMS-TSLab
Connected to (MAC)	-
MAC	02-01-36-00-4B-00

Bluetooth

Status	On
Operating Mode	PANU (Client)
	Disconnected
	004b00

Fig. 4 Web interface

4.2 Easy Config

1. Power on the unit and wait for the Link Quality LEDs to light up and go out again, then press and release the **MODE** button.

   Step 1 must be carried out within 5 seconds of startup.

2. Press **MODE** repeatedly to cycle through the Easy Config modes until the desired mode is indicated by the A-B-C-D LEDs.

   Mode 2 is the first mode, which means that the number of required button presses are always one less than the mode number.

3. Press and hold **MODE** for 2 seconds, then release the button. This will confirm the selected mode and restart the unit.

   Step 3 must be carried out within 20 seconds of step 2, otherwise the unit will exit Easy Config setup and return to the previous settings.

4.2.1 Easy Config Modes

Mode	Role	Description	A	B	C	D
2	—	Reset configuration to factory defaults		●		
3	—	Reset IP settings to factory defaults	●	●		
4	Client	Wait for discovery and configuration			●	
5	WLAN AP	Discover units in Mode 4 and configure them as clients	●		●	
6	Bluetooth NAP			●	●	

Modes 4, 5 and 6 are used in combination to automatically set up a WLAN or Bluetooth network with units of this type.

Modes 5 and 6 will scan for units in Mode 4. Each detected unit in Mode 4 will be reconfigured as a client, and the scanning unit will be configured as an access point. The clients will then restart and connect to the access point.

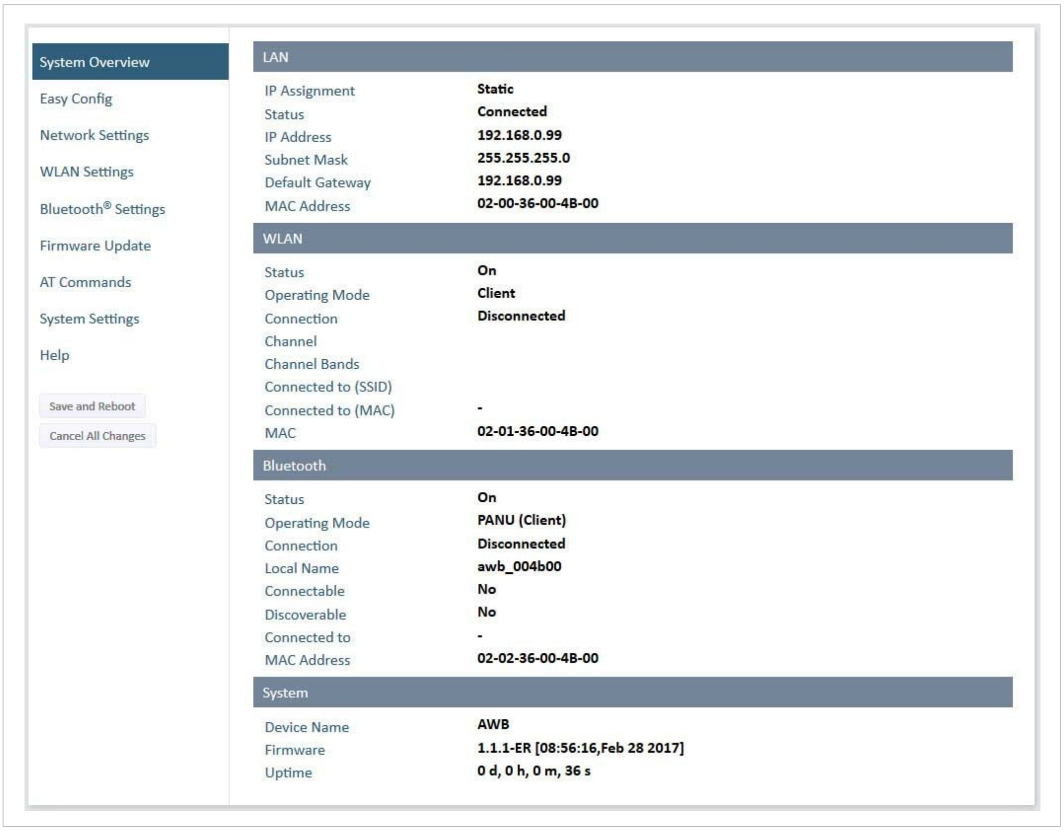
Mode Timeout

- Mode 5 and 6 will scan for 120 seconds. The mode can be activated repeatedly to scan for additional units.
- Mode 4 will listen for 120 seconds, or until it has received a valid configuration from a unit scanning in Mode 5 or 6.

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

4.3 Web Interface

4.3.1 System Overview



LAN

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

WLAN

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

Bluetooth

Status	On
Operating Mode	PANU (Client)
Connection	Disconnected
Local Name	awb_004b00
Connectable	No
Discoverable	No
Connected to	-
MAC Address	02-02-36-00-4B-00

System

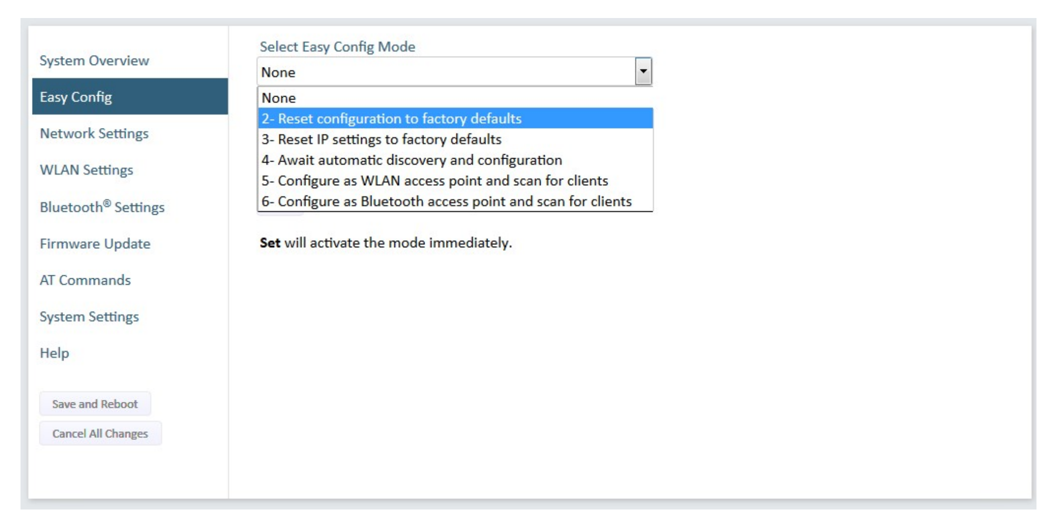
Device Name	AWB
Firmware	1.1.1-ER [08:56:16,Feb 28 2017]
Uptime	0 d, 0 h, 0 m, 36 s

Fig. 5 System Overview page

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

To go back to the current configuration without saving changes, click on **Cancel All Changes.**

4.3.2 Easy Config


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

Select Easy Config Mode: None

Set will activate the mode immediately.

Fig. 6 **Easy Config page**

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

Easy Config Modes

Mode	Role	Description	A	B	C	D
2	—	Reset configuration to factory defaults		●		
3	—	Reset IP settings to factory defaults	●	●		
4	Client	Wait for discovery and configuration			●	
5	WLAN AP	Discover units in Mode 4 and configure them as clients	●		●	
6	Bluetooth NAP			●	●	

Modes 4, 5 and 6 are used in combination to automatically set up a WLAN or Bluetooth network with units of this type.

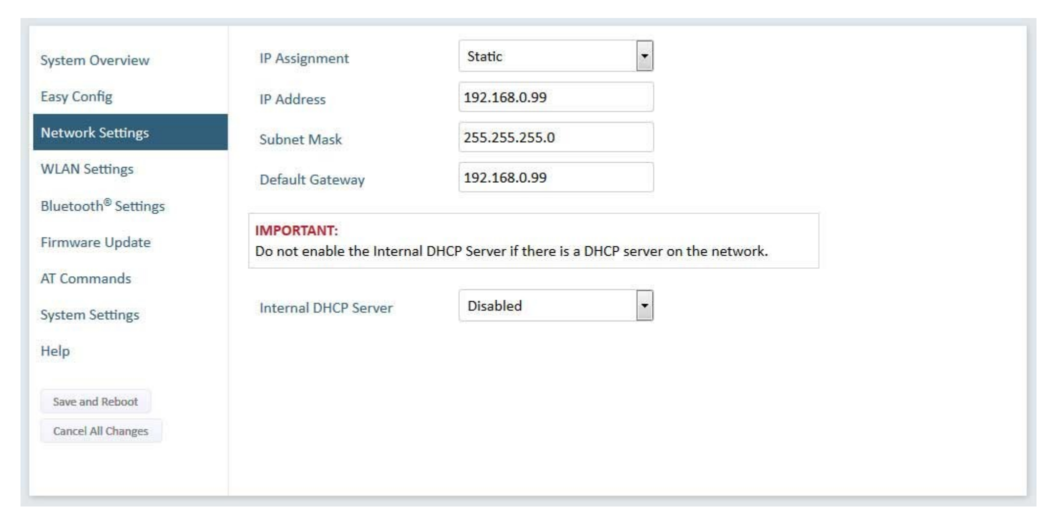
Modes 5 and 6 will scan for units in Mode 4. Each detected unit in Mode 4 will be reconfigured as a client, and the scanning unit will be configured as an access point. The clients will then restart and connect to the access point.

Mode Timeout

- Mode 5 and 6 will scan for 120 seconds. The mode can be activated repeatedly to scan for additional units.
- Mode 4 will listen for 120 seconds, or until it has received a valid configuration from a unit scanning in Mode 5 or 6.

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

4.3.3 Network Settings



IP Assignment: Static

IP Address: 192.168.0.99

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.0.99

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

Internal DHCP Server: Disabled

Fig. 7 Network Settings page

IP Assignment Select static or dynamic IP addressing (DHCP)

IP Address Static IP address for the unit

Subnet Mask Subnet mask when using static IP

Default Gateway Default gateway when using static IP

Internal DHCP Server **Disabled:** No internal DHCP functionality

DHCP Relay Enabled: The unit can receive a DHCP request on one interface and resend it to a DHCP server located on one of the other interfaces. Only a single DHCP server can be active for all the connected interfaces.

DHCP Server Enabled: Activates an internal DHCP server. This option is only available if IP Assignment is set to static.

The internal DHCP server will assign up to 7 consecutive IP addresses in the subnet specified by the netmask, starting from x.x.x.1. If the unit itself is located within the DCHP range, its IP address will be skipped and the next IP address will be assigned instead. The last assigned IP address will then be x.x.x.8.

Example 1: (Netmask 255.255.255.0)
Device IP address: 192.168.0.99
DHCP Server addresses: 192.168.0.1 - 192.168.0.7

Example 2: (Netmask 255.255.255.0)
Device IP address: 192.168.0.3
DHCP Server addresses: 192.168.0.1 - 192.168.0.8 (excluding 192.168.0.3)

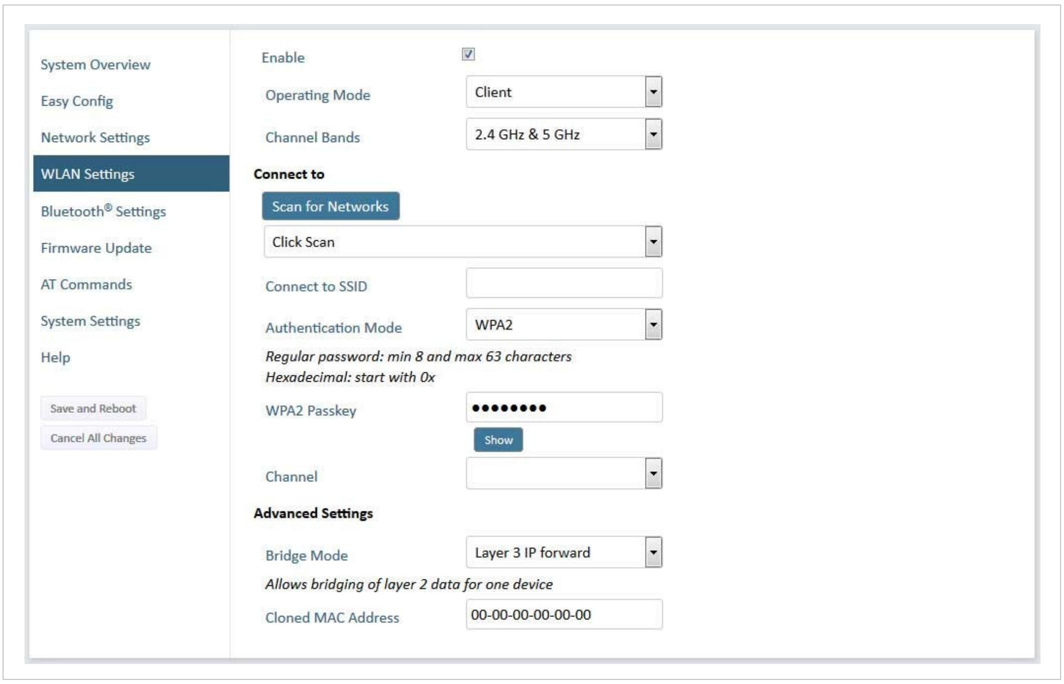
Example 3: (Netmask 255.255.0.0)
Device IP address: 192.168.5.5
DHCP Server addresses: 192.168.0.1 - 192.168.0.7

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

If the static IP address is changed the browser should automatically be redirected to the new address after clicking on **Save and Reboot.**

ⓘ *The automatic redirect function may not be supported by all browsers.*

4.3.4 WLAN Settings – Client Mode



Enable ☑

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:

Advanced Settings

Bridge Mode: Layer 3 IP forward

Allows bridging of layer 2 data for one device

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

Fig. 8 WLAN Settings – Client

Enable
Enable/disable the WLAN interface.

Operating Mode
Choose if the unit 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 either the 2.4 GHz or 5 GHz channel band, or on both (default). The unit must be rebooted to enable the new setting.

The unit can be configured to scan on both the 2.4 GHz and 5 GHz channel bands but can only communicate on one band at a time.

Scan for Networks
Scans the currently active frequency band for discoverable WLAN networks. To connect to a network, select it from the dropdown menu after 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

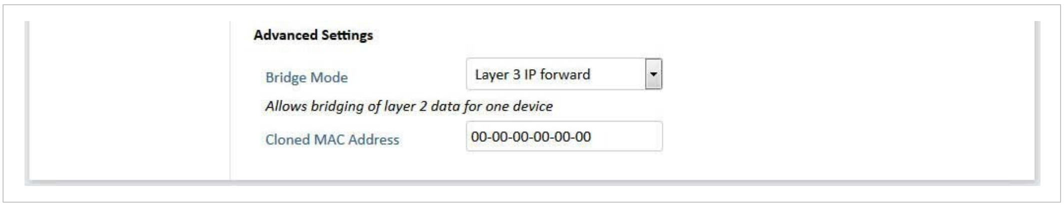
WPA2 = WPA2 PSK authentication with AES/CCMP encryption

Other authentication and encryption modes can be selected using AT commands.

WPA2 Passkey
Enter the WPA2 passkey for the network.

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

Auto = all channels will be scanned (default).



Advanced Settings

Bridge Mode: Layer 3 IP forward

Allows bridging of layer 2 data for one device

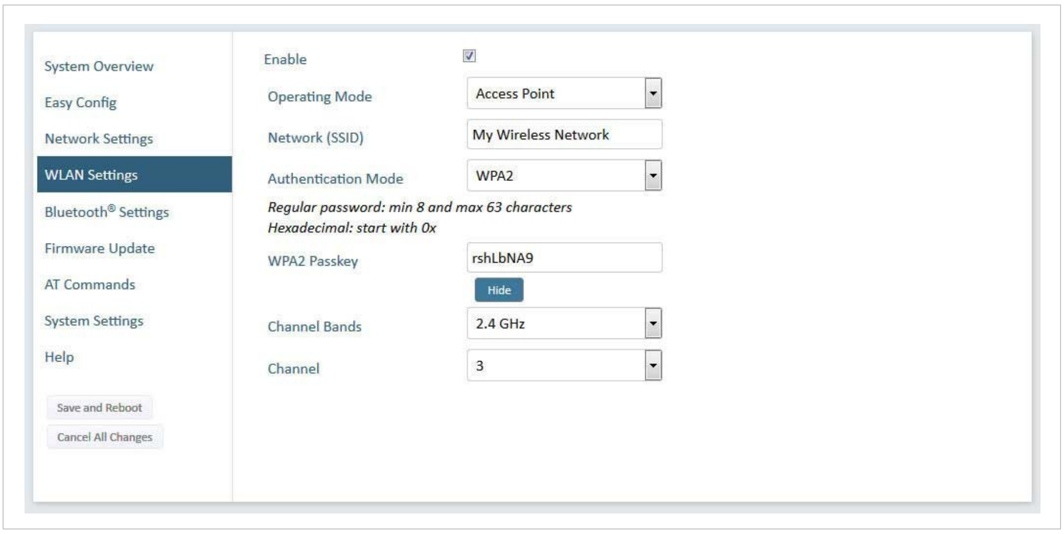
Cloned MAC Address: 00-00-00-00-00-00

Fig. 9 WLAN Client – Advanced Settings

Advanced Settings

Bridge Mode	**Layer 2 tunnel** = All layer 2 data will be bridged over WLAN. This mode should be used when multiple devices on both sides of an Ethernet network bridge must be able to communicate via WLAN (many-to-many). **Layer 2 cloned MAC only** = Layer 2 data from only a single MAC address (specified below) will be bridged over WLAN (many-to-one). **Layer 3 IP forward** (default) = IP data from all devices will be bridged over WLAN.
Cloned MAC Address	The MAC address to use with **Layer 2 cloned MAC only** (see above).

4.3.5 WLAN Settings – Access Point Mode



Enable ☑

Operating Mode: Access Point

Network (SSID): My Wireless Network

Authentication Mode: WPA2

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

WPA2 Passkey: rshLbNA9

Channel Bands: 2.4 GHz

Channel: 3

Fig. 10 WLAN Settings – Access Point

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

Network (SSID)

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

If this entry is left blank, the unit will generate an SSID which includes the last 6 characters of the MAC ID.

Authentication Mode

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

Open = No encryption or authentication

WPA2 = WPA2 PSK authentication with AES/CCMP encryption

Other authentication and encryption modes can be selected using AT commands.

WPA2 Passkey

Enter a string in plain text or hexadecimal format to use for authentication.

Regular (plain text) passwords must be between 8 and 63 characters.
All characters in the ASCII printable range (32–126) are allowed, except
`"` (double quote) `,` (comma) and `\` (backslash).

Hexadecimal passwords must start with `0x` and be **exactly** 64 characters.

See also the example passwords below.

Channel Bands, Channel

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

Password examples

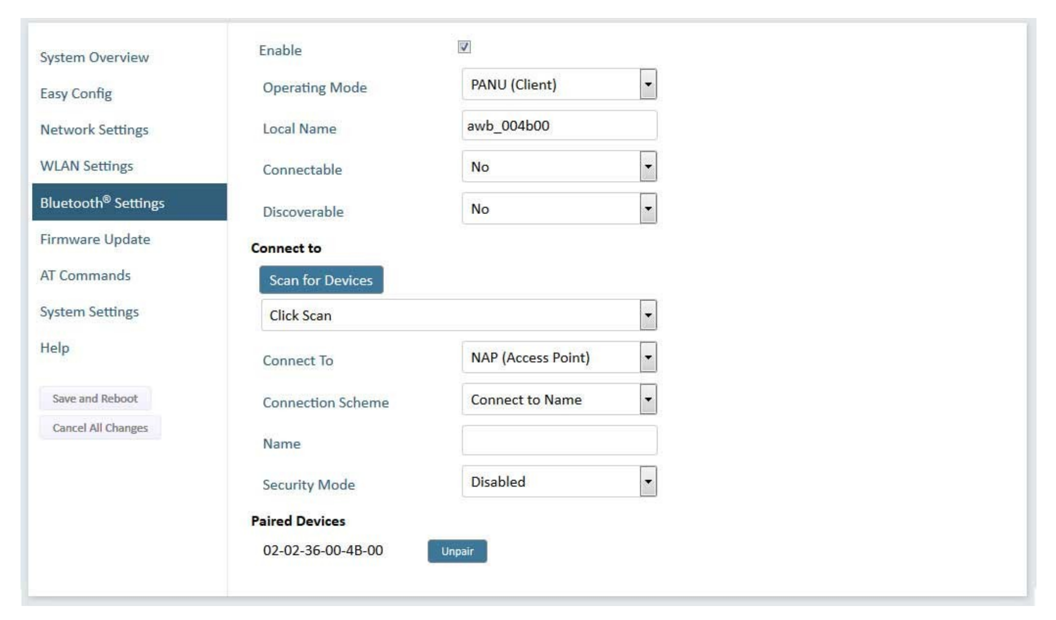
For plain text passwords a combination of upper and lower case letters, numbers, and special characters is recommended.

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

Example of hexadecimal password:
`0x000102030405060708090a0b0c0d0e0f101112131415161718191a1b1c1d1e1f`

! Do not use the example passwords above in a real installation!

4.3.6 Bluetooth Settings – General



Enable ☑

Operating Mode: PANU (Client)

Local Name: awb_004b00

Connectable: No

Discoverable: No

Connect to

Click Scan

Connect To: NAP (Access Point)

Connection Scheme: Connect to Name

Name:

Security Mode: Disabled

Paired Devices

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

Fig. 11 Bluetooth Settings

Enable
Enable/disable the Bluetooth interface.

Operating Mode
PANU (Client) = The unit will operate as a Bluetooth PAN (Personal Area Network) User device. It can connect to another single Bluetooth PANU device or to a Bluetooth Network Access Point.

NAP (Access Point) = The unit will operate as a Bluetooth Network Access Point. It can connect to up to 7 Bluetooth PANU devices.

Local Name
Identifies the unit to other Bluetooth devices. If left blank, the unit will use a default name including the last 6 characters of the MAC ID.

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

Discoverable
Enable to make the unit visible to other Bluetooth devices.

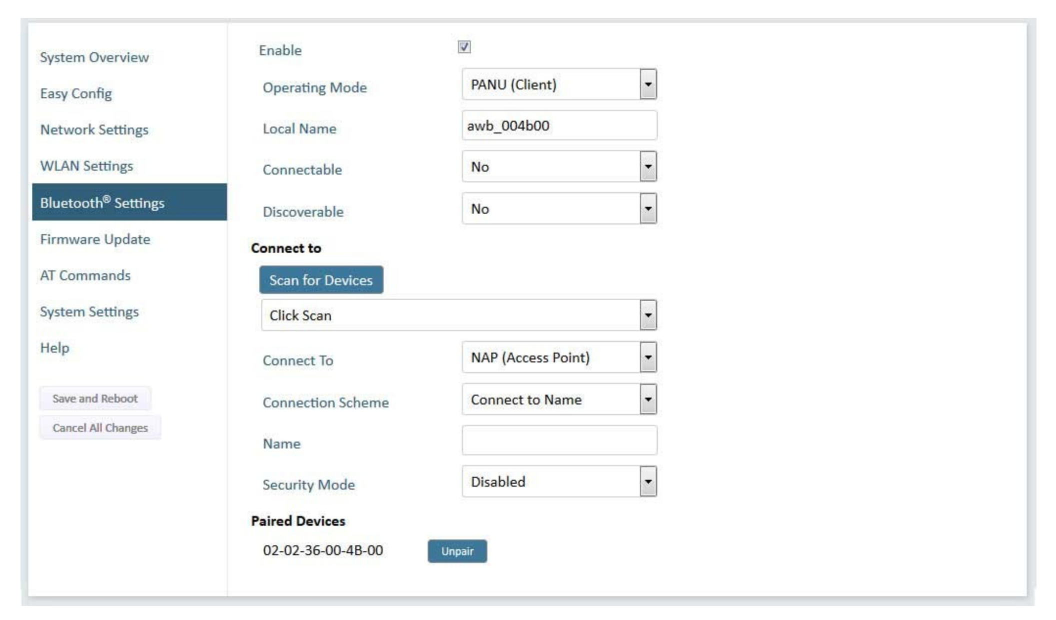
Security Mode
Disabled = No encryption or authentication.

PIN = Encrypted connection with PIN code security. This mode only works between two units of this type and brand (not with third-party devices). PIN codes must consist of 4 to 6 digits.

Just Works = Encrypted connection without PIN code.

Paired Devices
Lists the currently connected Bluetooth devices.

4.3.7 Bluetooth Settings – Mode Specific



Enable ☑

Operating Mode: PANU (Client)

Local Name: awb_004b00

Connectable: No

Discoverable: No

Connect to

Click Scan

Connect To: NAP (Access Point)

Connection Scheme: Connect to Name

Name:

Security Mode: Disabled

Paired Devices

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

Fig. 12 Bluetooth Settings

PANU 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.

4.3.8 Firmware Update

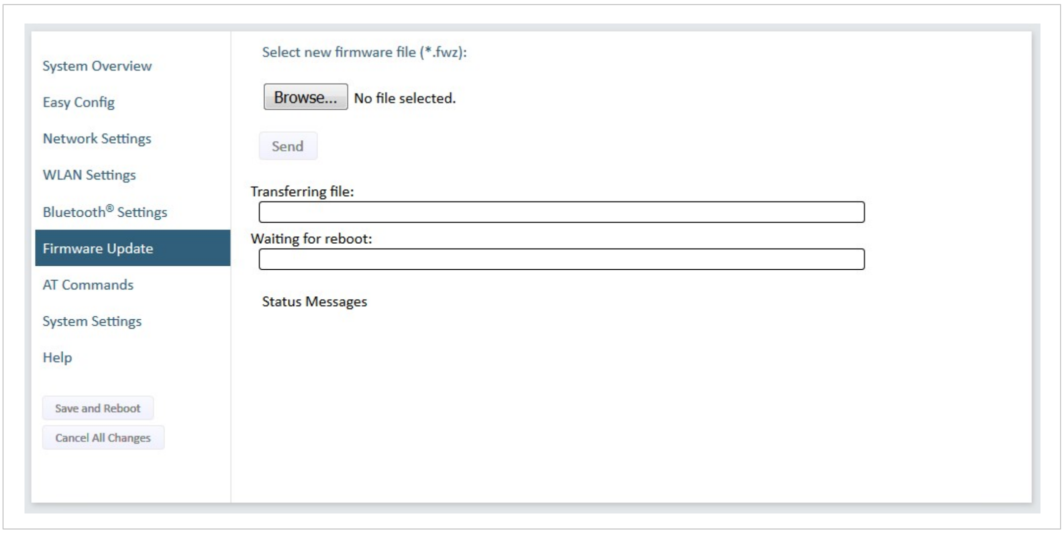
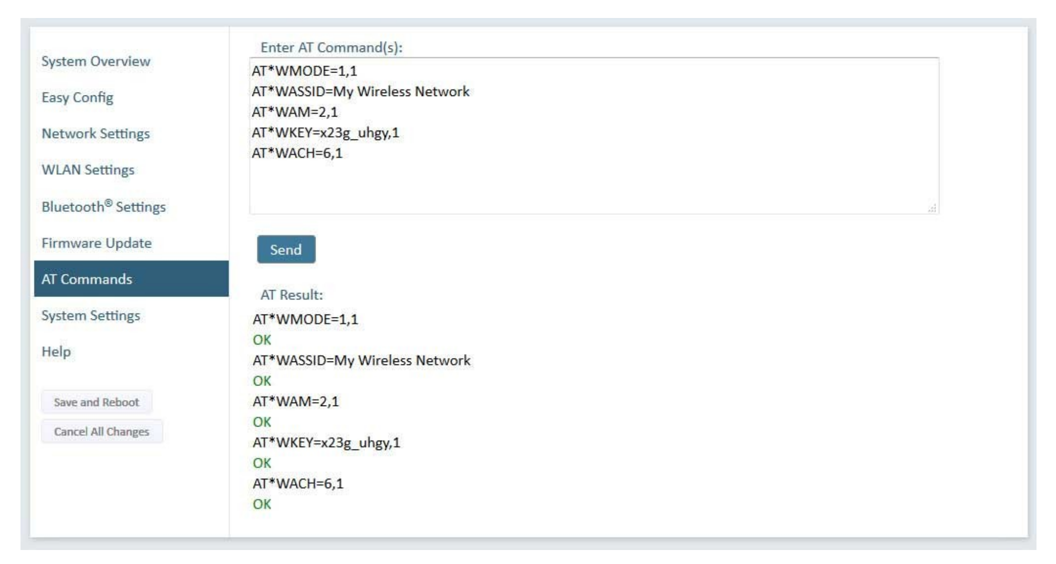


Fig. 13 Firmware Update

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

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

4.3.9 AT Commands



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

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

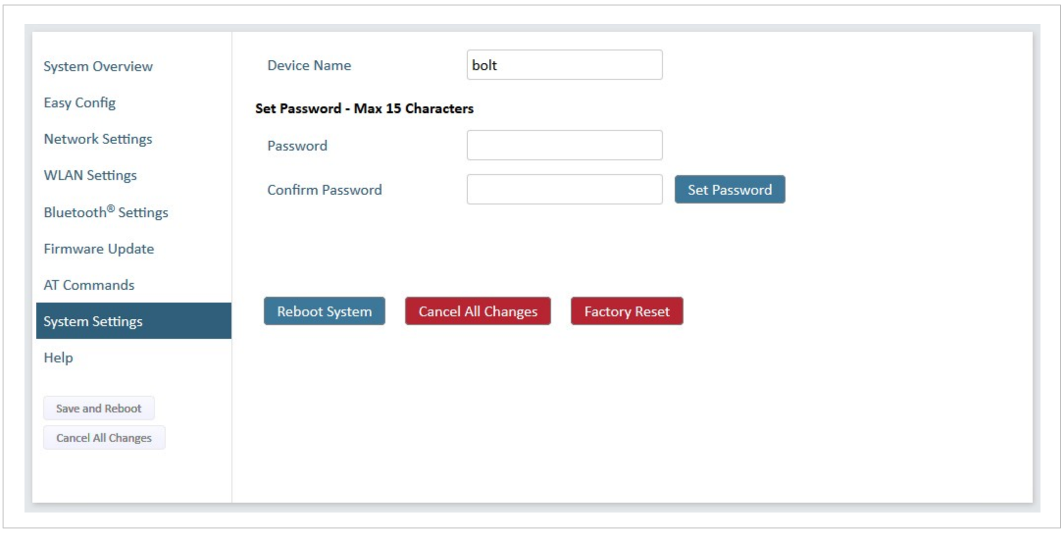
Fig. 14 AT Commands

AT commands can be used for setting advanced parameters that are not accessible in the web interface, to read out parameters in text format, and for batch configuration using command scripts.

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

The supported AT commands are described in the **Help** section of the web interface and in the *AT Commands Reference Manual*.

4.3.10 System Settings



Device Name bolt

Fig. 15 System Settings

Device Name Enter a descriptive name for the unit.

Password Enter a password for accessing the web interface.

Reboot System Reboots the system without applying changes.

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

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

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

4.4 Factory Restore

The unit can be restored to the factory default settings using any of the following methods:

- Press and hold the **MODE** button for >10 seconds and then release it
- Execute **Easy Config Mode 2**
- Click on **Factory Restore** on the **System Settings** page
- Issue the AT command **AT&F** and reboot

Default Network Settings

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

Default WLAN Settings

Operating Mode	Client
Channel Bands	2.4 GHz & 5 GHz
Authentication Mode	Open
Channel	Auto
Bridge Mode	Layer 2 tunnel

Default Bluetooth Settings

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

Default System Settings

Password	[empty]

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

4.5 MODE Button

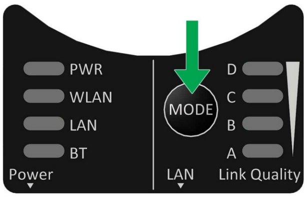


Fig. 16 Overlay

The **MODE** button can be used to restart or reset the unit as well as for selecting Easy Config modes. See *Easy Config, p. 11*.

- ► When the unit is powered on, press and hold **MODE** for >10 seconds and then release it to reset to the factory default settings.

  See *Factory Restore, p. 23*.

- ► Press and hold **MODE** while applying power to boot into *Recovery Mode*.

  Recovery Mode can be used to reinstall firmware using an external application if the web interface cannot be accessed. Please refer to the support website for more information.

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

Recovery Mode LED Indications

In Recovery Mode the LEDs will indicate firmware update status.

PWR	Green	Firmware update in progress
	Green, blinking	Waiting for valid firmware
WLAN + BT	Alternating red/blue	Firmware update in progress

4.6 Configuration Examples

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

- All the examples start out from the factory default settings.
- Settings not mentioned in the examples should be left at their default values.
- The computer accessing the web interface of a unit must be in the same subnet as that unit.

Easy Config: Ethernet Bridge over WLAN

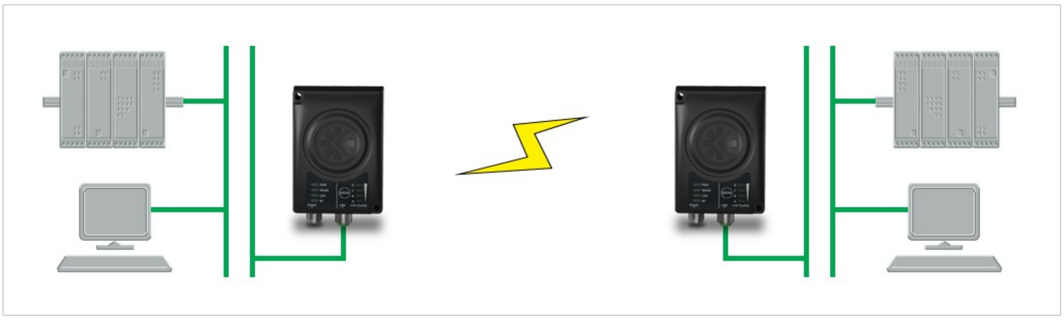
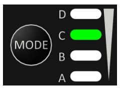


Fig. 17 Setting up a network bridge with Easy Config

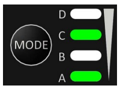
This example describes how to bridge two Ethernet network segments over WLAN. The units are configured using only their **MODE** buttons.



1. Power on the first unit and wait for the LEDs to light up and go out, then press **MODE** and release it immediately.
2. Press **MODE** repeatedly until only LED **C** is lit (Easy Config Mode 4), then confirm by pressing and holding **MODE** for 2 seconds.

   This unit will now be discoverable and open for automatic configuration.
3. Power on the second unit and wait for the LEDs to light up and go out, then press and release **MODE**.
4. Press **MODE** repeatedly on the second unit until **A** + **C** are lit (Easy Config Mode 5), then confirm by pressing and holding **MODE** for 2 seconds.

   This unit should now automatically discover and configure the other unit as a WLAN client.



PROFINET communication

WLAN communication with PROFINET devices requires that **Bridge Mode** is set to **Layer 2 tunnel** on the **WLAN Settings** page of the web interface.

This page intentionally left blank

A Wireless Technology Basics

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

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

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

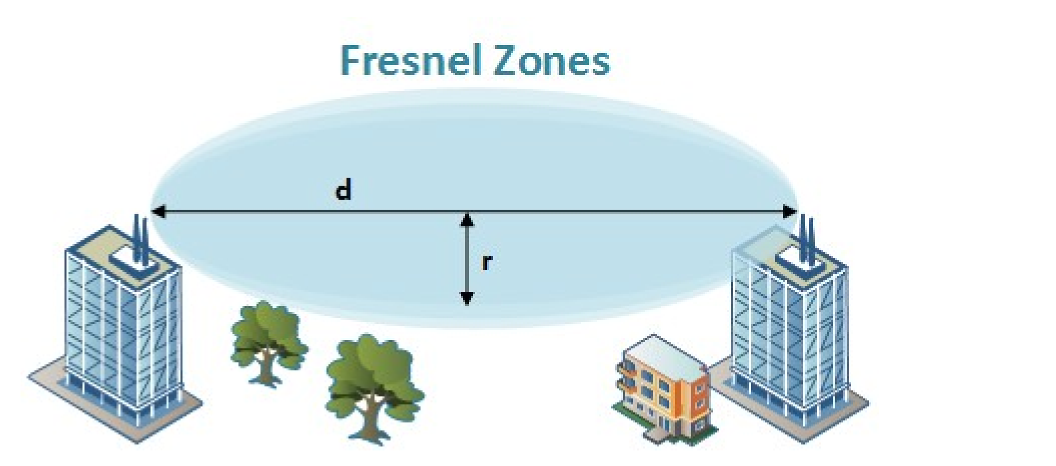


Fig. 18 Fresnel zones

Area to keep clear of obstacles (first Fresnel zone)

Distance (d)	Fresnel zone radius (r)	
	2.4 GHz (WLAN or Bluetooth)	5 GHz (WLAN)
100 m	1.7 m	1.2 m
200 m	2.5 m	1.7 m
300 m	3.0 m	2.1 m
400 m	3.5 m	2.4 m

The wireless signal may be adequate even if there are obstacles within the Fresnel zones, as it always depends on the number and size of the obstacles and where they are located. This is especially true indoors, where reflections on metal objects may actually help the propagation of radio waves. To reduce interference and phase cancelling, the range may also need to be limited by reducing the transmission power. For determining the optimal configuration and placement of wireless devices it is therefore recommended to use a wireless signal analysis tool.

B Technical Data

B.1 Technical Specifications

General Specifications

Order code	AWB3000	AWB3010
Antenna	Internal	External
Maximum range	400 m (WLAN and Bluetooth) *Using an external antenna does not extend the range but allows separate placement of antenna and unit (e.g. if unit is placed in an enclosure).*	
Wired Interface type	Ethernet	
Dimensions (LxWxH)	93 x 68 x 33.2 mm	
Weight	120 g	
Operating temperature	-30 to +65 °C	
Storage temperature	-40 to +85 °C	
Vibration	Sinusoidal vibration test according to IEC 60068-2-6:2007 and with extra severities. Shock test according to IEC 60068-2-27:2008 and with extra severities. See Anybus Wireless Bridge II Compliance Sheet for details.	
Humidity	EN 600068-2-78: Damp heat, +40 °C, 93 % humidity for 4 days	
Housing	Plastic (Bayblend FR3010)	
Protection class	IP65	
Mounting	Screw mount or DIN rail using optional clip	
Power connector	M12 male A-coded	
Ethernet connector	M12 female D-coded	
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)	
Configuration	Push-button, web interface, AT commands	
Browser support	Internet Explorer, Firefox, Chrome, Safari (current stable versions)	
Certifications	See Anybus Wireless Bridge II Compliance Sheet.	

Host Communication

Ethernet interface	10/100BASE-T, auto MDI/MDIX cross-over detection Supports all common Ethernet protocols based on TCP/IP including the industrial protocols EtherNet/IP, Modbus TCP, BACnet/IP and Profinet IO.
Digital input	9–30 VDC Signal cable length must be <3 m if separate from power supply cable.

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	Access Point: 36–48 (U-NII-1) Client: 36–140 (U-NII-1, U-NII-2A, U-NII-2C)
RF output power	16 dBm
Max number of clients	7 (for access point)
Power consumption	54 mA @ 24 VDC (WLAN interface only)
Data throughput	Gross data throughput: 54 Mbit/s Net data througput: 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

B.2 Internal Antenna Characteristics

Anybus Wireless Bridge II has 3 independent quarter wave monopole antennas. The following radiation diagrams and tables show the characteristics of the different antennas as measured under laboratory test conditions. The diagrams can be used as a general guide for finding the optimal placement and orientation of the units.

The diagrams use a color spectrum from violet to red to indicate signal gain. The closer to the red end of the spectrum, the stronger the signal.

2.4 GHz Section of Dual Band Antenna

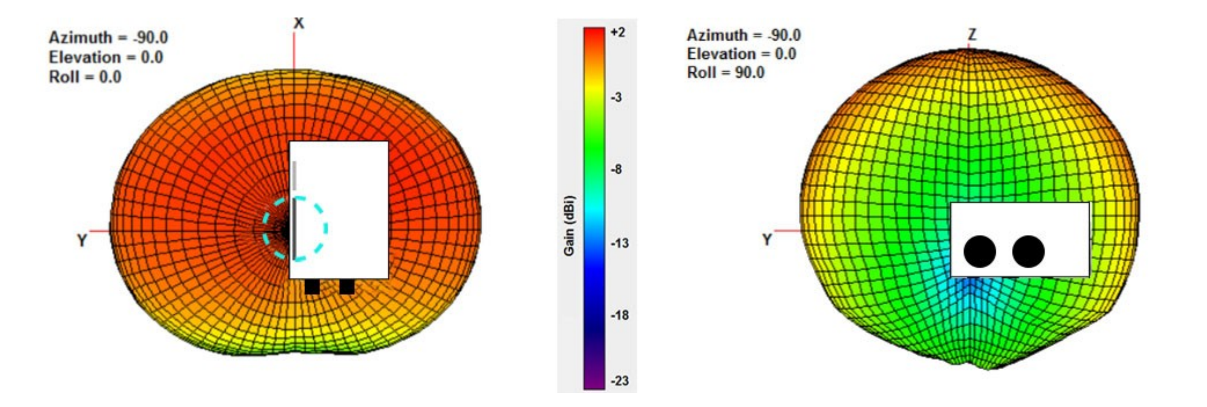


Fig. 19 2.4 GHz antenna gain and directivity in horizontal and vertical planes

Test	Antenna	Section	F	Avg Gain	Peak Gain	Dir	Comment
#	Dual band	2.4GHz	MHz	dBi %	dBi	dB	In Plastic Box
148			2400	-2.78 52.7	+1.61	4.3	
149			2440	-2.24 60.5	+1.80	3.9	
150			2485	-1.89 64.7	+2.00	3.9	

5 GHz Section of Dual Band Antenna

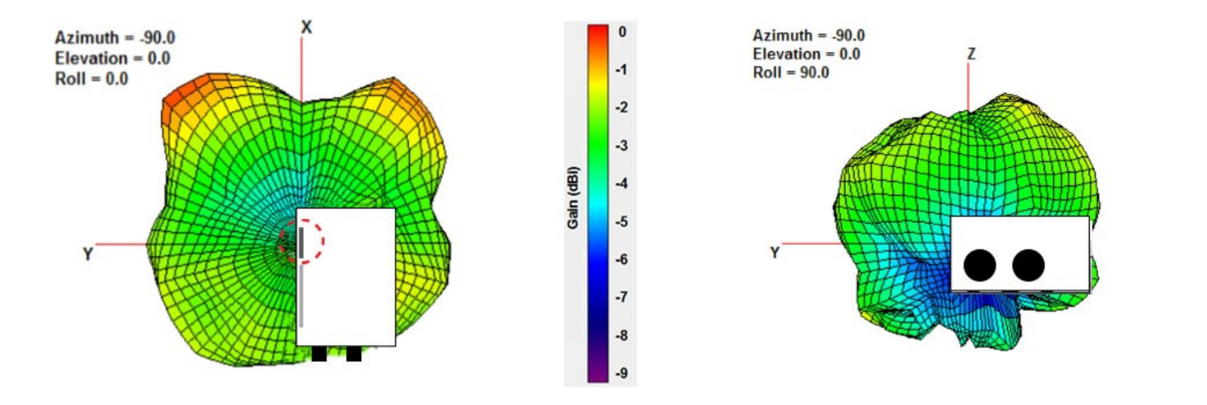


Fig. 20 5 GHz antenna gain and directivity in horizontal and vertical planes

Test	Antenna	Section	F	Avg Gain	Peak Gain	Dir	Comment
#	Dual band	5GHz	MHz	dBi %	dBi	dB	In Plastic Box
151			5150	-4.80 33.1	-2.48	2.3	
152			5250	-3.42 45.5	-0.75	2.7	
153			5400	-3.13 48.6	-0.14	3.0	
154			5600	-1.96 63.7	+0.48	2.4	

2.4 GHz MIMO Antenna

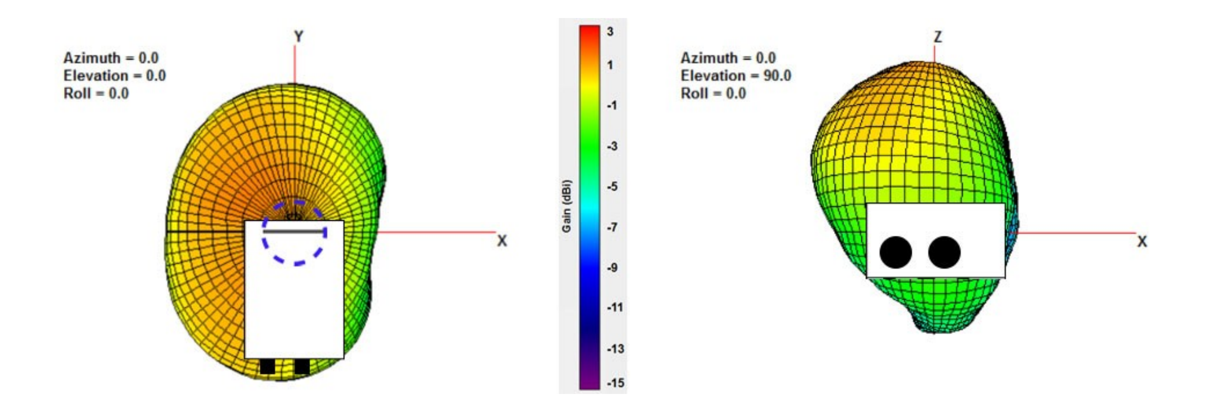


Fig. 21 2.4 GHz MIMO antenna gain and directivity in horizontal and vertical planes

Test	Antenna	Section	F	Avg Gain	Peak Gain	Dir	Comment
#	MIMO	-	MHz	dBi %	dBi	dB	In Plastic Box
168			2400	-1.95 63.8	+2.66	4.6	
169			2440	-1.65 68.4	+2.88	4.5	
170			2485	-1.42 72.1	+2.76	4.2	

This page intentionally left blank

Box 4126
300 04 Halmstad, Sweden

info@hms.se