

Anybus[®] WLAN Access Point IP67

USER MANUAL

SCM-1202-094 1.2 en-US ENGLISH



Important User Information

Disclaimer

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

HMS Industrial 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 Industrial Networks and is subject to change without notice. HMS Industrial 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 Industrial 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 Industrial Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Table of Contents

Page

1	Preface	3
1.1	About This Document	3
1.2	Document Conventions	3
1.3	Trademarks	3
2	Safety	4
2.1	General Safety Instructions	4
2.2	Intended Use	4
2.3	5 GHz Transmission Power Restriction (EU only)	5
3	Installation	6
3.1	Grounding	6
3.2	Overview	7
3.3	Wall Mounting	8
3.4	Pole Mounting	8
3.5	Power Connector (M12)	9
3.6	Ethernet Connector (M12)	9
3.7	Ethernet Cabling	10
3.8	LED Indicators	11
3.9	Factory Reset	11
4	Configuration	12
4.1	Overview	13
4.2	Basic Settings	14
4.3	Wireless Settings	17
4.4	Advanced Settings	22
4.5	Event Warning Settings	23
4.6	System Status	26
4.7	Administrator	28
5	Technical Data	31
5.1	Technical Specifications	31
5.2	Dimensions	32
A	Wireless Technology Basics	33

This page intentionally left blank

1 Preface

1.1 About This Document

This document describes how to install and configure Anybus WLAN Access Point IP67.

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

1.2 Document Conventions

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

1. First do this
2. Then do this

Bulleted lists are used for:

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

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

Program code and script examples

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

External link (URL): www.hms-networks.com



WARNING

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



Caution

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



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



Additional information which may facilitate installation and/or operation.

1.3 Trademarks

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

2 Safety

2.1 General Safety Instructions

**Caution**

This equipment emits RF energy in the ISM (Industrial, Scientific, Medical) band. Make sure that all medical devices used in proximity to this 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 prevention measures to avoid damage.



To prevent water intrusion, make sure that the unit is installed with the connectors on the bottom panel of the unit facing down.

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.

2.3 5 GHz Transmission Power Restriction (EU only)



Transmission power must be reduced for 5 GHz channels 149-165 when the unit is used in the EU.

To comply with the European Radio Equipment Directive (RED) the effective radiated power output for 5 GHz channels 149-165 (U-NII-3) must not exceed 25 mW (~14 dBm) when the unit is used in the EU.

To configure the unit for use within the EU, set **Tx Power** to **14 dBm** or less on the **Wireless 1 Options** page of the web configuration interface.

Wireless Settings --> Wireless Options

Wireless performance tuning

Radio:	<input type="button" value="Enabled"/>	<input type="button" value="Disabled"/>
Beacon Interval:	<input type="text" value="100"/>	
DTIM Interval:	<input type="text" value="1"/>	
Fragmentation Threshold:	<input type="text" value="2346"/>	
RTS Threshold:	<input type="text" value="2347"/>	
Tx Power:	<input type="text" value="14 dBm"/>	
Wireless Mode:	<input type="radio"/> 2.4G <input checked="" type="radio"/> 5G	

Fig. 1 Wireless Settings

3 Installation

The Anybus WLAN Access Point IP67 can be screw-mounted onto a stable flat surface using the included wall mounting kit. It can also be pole-mounted using the included adjustable steel band straps.

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.

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

Package Contents

After unpacking the access point, check the contents to be sure you have received all the components:

- Anybus WLAN Access Point IP67 (1 x)
- Wall mounting kit (1 x)
 - Mounting plate (1 x)
 - Screw 5.8 mm x 14.8 mm for fixed mounting plate (4 x)
 - Screw 6.3 mm x 25.3 mm for wall mount (4 x)
- Steel band strap (2 x)
- Antenna (2 x)
- Grounding cable (1x)
- Grounding screw with washer (2x)
- Startup Guide (1 x)

3.1 Grounding

When connecting a ground wire to the Anybus WLAN Access Point IP67, use the grounding screw on the unit. Use #20 AWG or larger copper core ground wire. The ground wire can be connected to a point on the bracket, pole, metal grounding plate, or directly to an earth termination. Make sure that there is a good electrical connection between the ground wire and the grounding point (no paint or isolating surface treatment).

3.2 Overview

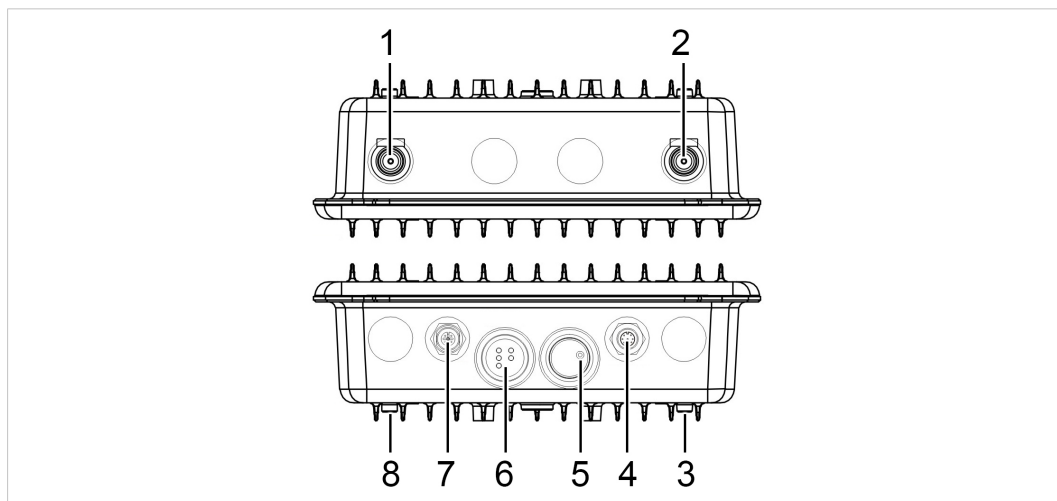


Fig. 2 Overview

- | | |
|------|-----------------------------------|
| 1, 2 | Antenna connector (N) |
| 3, 8 | Threaded hole for grounding screw |
| 4 | Ethernet connector (M12) |
| 5 | Reset button |
| 6 | LED indicators |
| 7 | Power connector (M12) |

3.3 Wall Mounting

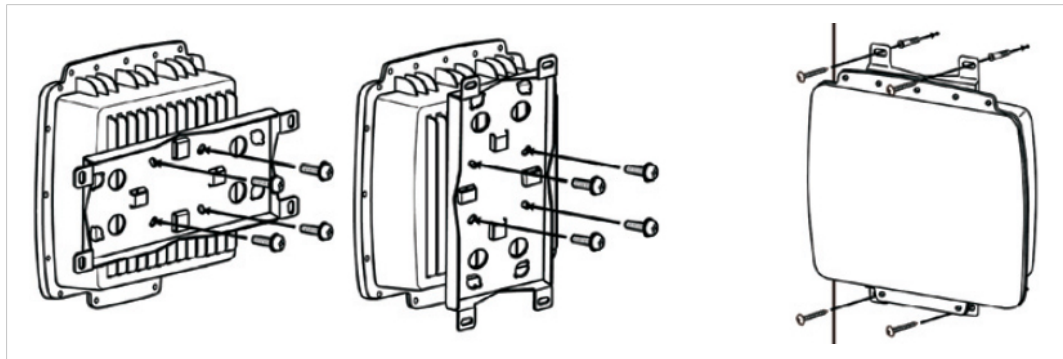


Fig. 3 Wall mounting

1. Attach the mounting plate to the back of the unit using the 4 included screws. The plate can be attached vertically or horizontally.
2. Hold the unit upright against the wall and fasten it with 4 screws through the apertures in the plate.

3.4 Pole Mounting

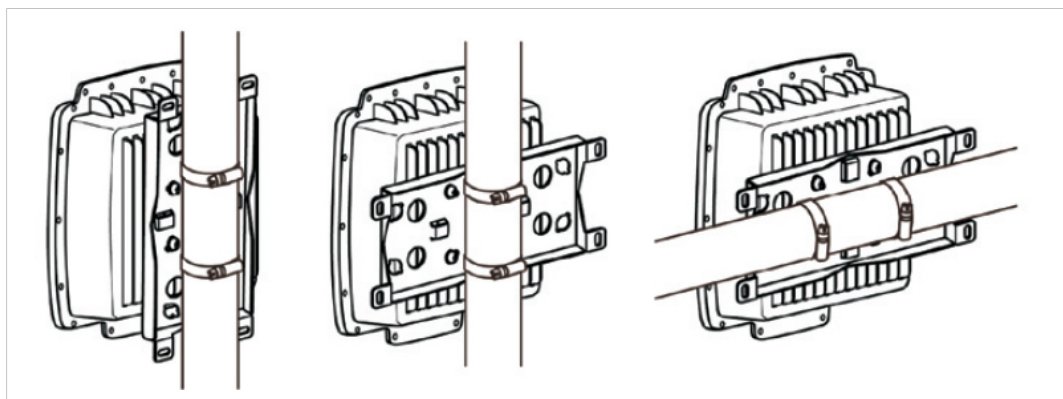


Fig. 4 Pole mounting

1. Attach the mounting plate to the back of the unit using the 4 included screws. The plate can be attached vertically or horizontally.
2. Thread the two supplied metal mounting straps through the large slots on the mounting plate and then put the straps around the pole.



To prevent water intrusion, make sure that the unit is installed with the connectors on the bottom panel of the unit facing down.


3.5 Power Connector (M12)

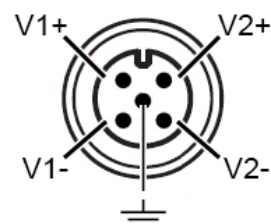
The power connector is a 5-pin A-coded M12 type connector that supports dual power inputs with a common ground connection.



Connecting power with reverse polarity or using the wrong type of power supply may damage the equipment. Make sure that the power supply is correctly connected and of the recommended type.

See also [Technical Data, p. 31](#) regarding power supply requirements.

Pin	Function
V1+	Power Input 1 +
V1-	Power Input 1 -
V2+	Power Input 2 +
V2-	Power Input 2 -
	Power Ground



3.6 Ethernet Connector (M12)

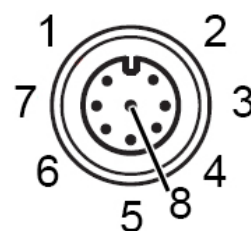
The Ethernet connector is an 8-pin A-coded M12 type connector. The Ethernet port supports PoE (Power over Ethernet) compliant with IEEE 802.3af.



A Power over Ethernet power source is not included with the equipment. The power source must be UL (UL 62368-1) certified for UL compliance, fully compliant with IEEE 802.3af, marked "Limited Power Source", "LPS" or "Class 2", and have a rated voltage of 48 VDC and output meeting ES1 (SELV) and PS2.

See also [Technical Data, p. 31](#) regarding power supply requirements.

Pin	Function
1	BI_DC+
2	BI_DD+
3	BI_DD-
4	BI_DA-
5	BI_DB+
6	BI_DA+
7	BI_DC-
8	BI_DB-



3.7 Ethernet Cabling

When planning a cable route from the access point (outdoors) to the power injector module (indoors), consider the following guidelines:

- Determine a building entry point for the cable.
- Determine if conduits, bracing, or other structures are required for safety or protection of the cable.
- For lightning protection at the power injector end of the cable, consider using a lightning arrestor immediately before the cable enters the building.
- Power cable and Ethernet cable are not included with the unit. The cables and connectors must be waterproof and installed by a professional.

3.8 LED Indicators

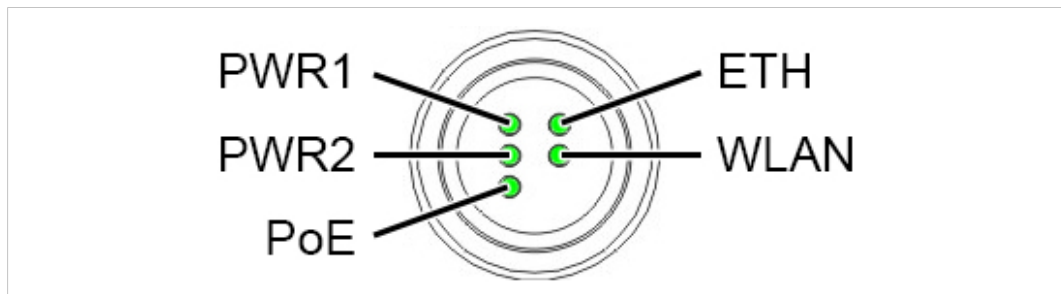


Fig. 5 LED indicators on bottom panel

PWR1	Green	Power supplied on Power Input 1
PWR2	Green	Power supplied on Power Input 2
PoE	Green	Power supplied on Ethernet port
ETH	Off	No LAN
	Green	LAN link established
	Green, flashing	LAN traffic
WLAN	Off	No WLAN
	Green	WLAN link established
	Green, flashing	WLAN traffic

3.9 Factory Reset

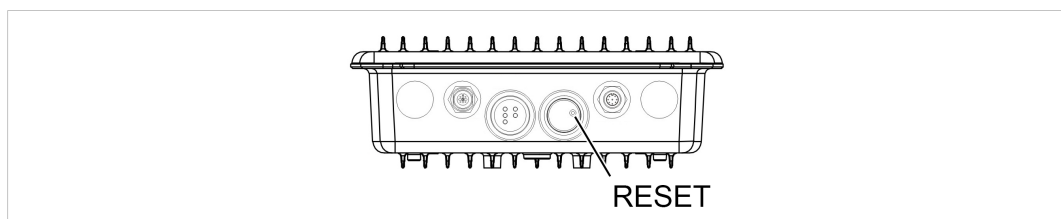


Fig. 6 Reset

To restore the factory default settings, press and hold **RESET** on the front panel until the power LED indicator(s) starts to flash, then release the button.

4 Configuration

Anybus WLAN Access Point IP67 is configured via a web interface which is accessed by pointing a web browser to the IP address of the unit. The computer accessing the web interface must be in the same IP subnet as the access point.

Default web interface settings

IP address	192.168.0.2
User ID	admin
Password	admin

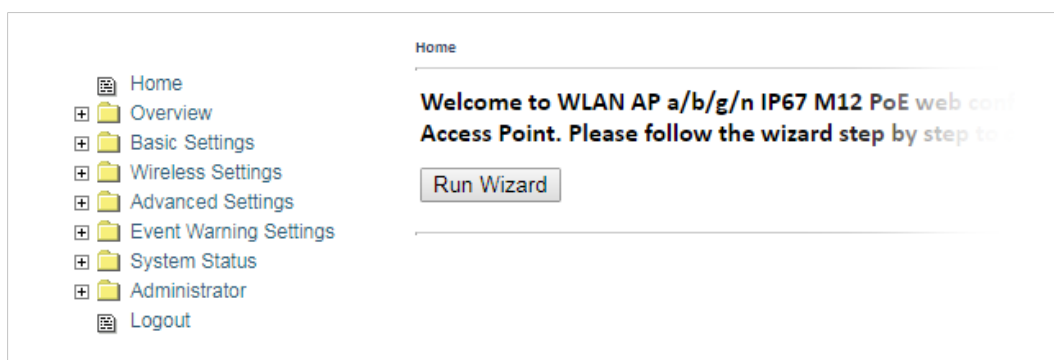


Fig. 7 Home page

Configuration Menu

Home	Click on Run Wizard to perform a quick basic configuration of the access point.
Overview	Basic information about the access point and the Ethernet and wireless networks
Basic Settings	Basic settings for the access point and the LAN interface
Wireless Settings	Basic settings for the WLAN interface
Advanced Settings	Advanced settings for the WLAN interface
Event Warning Settings	Settings for alarm messaging and fault indication
System Status	Detailed information about network connections and traffic
Administrator	Password settings, configuration backup, unit reset, etc.
Logout	Click to log out from the Anybus WLAN Access Point IP67.

4.1 Overview

Basic information about the access point and the Ethernet and wireless networks. These pages are read-only and have no editable settings.

4.1.1 System Info

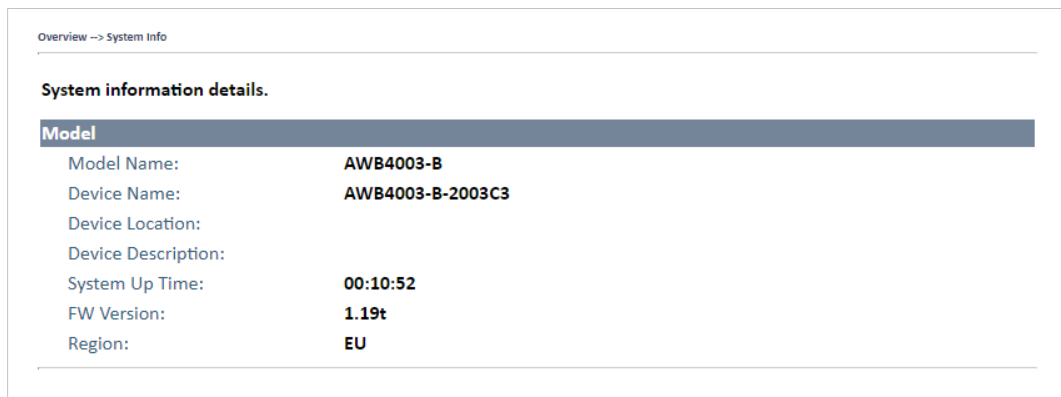


Fig. 8 System Info

4.1.2 LAN Info

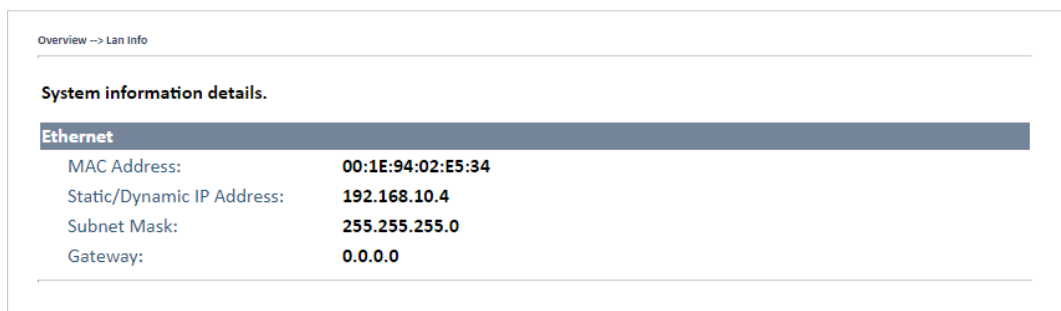


Fig. 9 LAN Info

4.1.3 Wireless Info

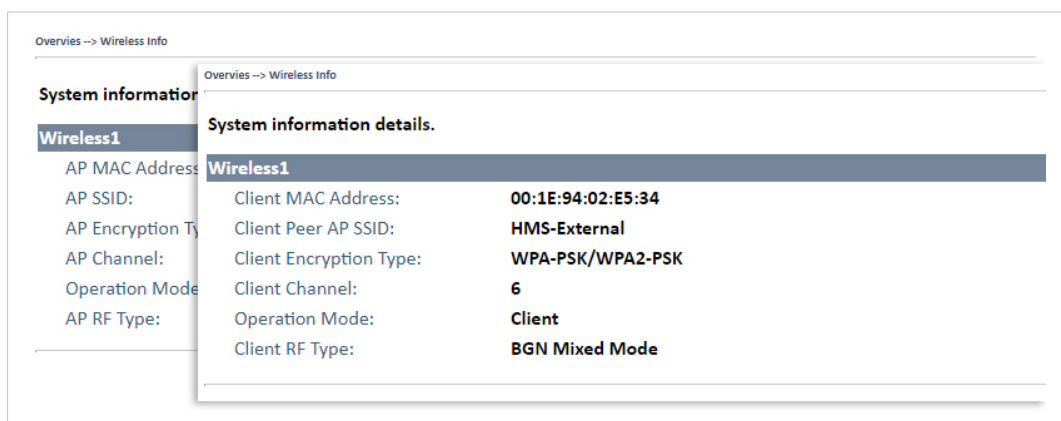


Fig. 10 Wireless Info (AP and client modes)

4.2 Basic Settings

Basic settings for the access point and the Ethernet (LAN) interface

4.2.1 System Info Settings

Basic Settings --> System Info Setting

Device Name:

Device Location:

Device Description:

Fig. 11 System Info Settings

Device Name	Define the name of the device
Device Location	Enter the location of the device
Device Description	Enter a description for the device

4.2.2 LAN Setting

Basic Settings --> LAN Setting

LAN settings of AP.

☐ Obtain an IP address automatically

☒ Use the following IP address

IP Address: . . .

Subnet Mask: . . .

Default Gateway: . . .

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses

Primary DNS: . . .

Secondary DNS: . . .

Web Protocol: ☒ HTTP ☐ HTTPS

Port:

Web Access Control: ☒ Wired ☒ Wireless

The AP can be setup as a DHCP server to distribute IP addresses to the WLAN network.

DHCP Server ☐ Enabled ☒ Disabled

Options

Starting IP address: . . .

Maximum Number of IPs:

Lease Time: hours

Fig. 12 LAN Setting

LAN Setting	
Obtain an IP address automatically	IP settings will be assigned automatically by the DHCP server in your network.
Use the following IP address	Manually assign IP address, subnet mask, and default gateway.
Obtain DNS server address automatically	Obtain a DNS server address from the DHCP server.
Use the following DNS server addresses	Set a primary and secondary DNS server address.
Web Protocol	Select HTTP (default) or HTTPS protocol for web access.
Port	Specify a port to use for web access. The default port is 80 for HTTP and 443 for HTTPS.
Web Access Control	Enable web access over the wired or wireless connections.
DHCP Server	When enabled, the device will act as DHCP server on your local network. Do not enable this function if there is an active DHCP server on the network.
Start IP Address	The starting IP address of the IP range assigned by the DHCP server.
Maximum Number of IPs	Limits the number of IP addresses allowed to access the device.
Lease Time (Hour)	The period of time that an IP address will be leased to a device.

4.2.3 Time Setting

Basic Settings --> Time Setting

Date/Time settings.

System time: **Thu Jul 04 2019 13:33:30**

NTP: ☒ **Enable**

NTP Server 1:

NTP Server 2: (optional)

Time Zone:

Synchronise: at :

Local Date: Year Month Day

Local Time: Hour Minute Second

Fig. 13 Time Setting

Time Setting	
NTP	Enables or disables NTP function
NTP Server 1	The primary NTP server
NTP Server 2	The secondary NTP server
Time Zone	Select the time zone you are located in
Synchronize	Specify the scheduled time for synchronization
Local Date	Set a local date manually
Local Time	Set a local time manually
Get Current Date & Time from Browser	Click to set the time from your browser

4.2.4 DIDO (Digital In/DigitalOut)

Basic Setting --> DIDO

DI		
DI 1	<input type="radio"/> On	<input checked="" type="radio"/> Off
DI 2	<input type="radio"/> On	<input checked="" type="radio"/> Off
DI 3	<input type="radio"/> On	<input checked="" type="radio"/> Off
DI 4	<input type="radio"/> On	<input checked="" type="radio"/> Off

DO		
DO 1	<input type="radio"/> On	<input checked="" type="radio"/> Off
DO 2	<input type="radio"/> On	<input checked="" type="radio"/> Off
DO 3	<input type="radio"/> On	<input checked="" type="radio"/> Off
DO 4	<input type="radio"/> On	<input checked="" type="radio"/> Off

Fig. 14 DIDO Setting

The initial state of the digital outputs **DO 1–4** can be set on this page. The default state is **Off**.

The digital inputs **DI 1–4** are read-only.

4.3 Wireless Settings

4.3.1 Wireless Settings

AP	Access Point mode. The unit will act as a central connection point which other wireless clients can connect to. This is the default mode.
AP-Client	Provides one-to-many MAC address mapping so that multiple stations behind the AP can transparently connect to the other AP even if they do not support WDS.
Client	The unit will function as a wireless client to connect your wired devices to a wireless network. This mode provides no access point services but supports 802.1X.
Bridge	In this mode, the device functions as a bridge between the network on its WAN port and the devices on its LAN port and those connected to it wirelessly.

Wireless settings – AP

Fig. 15 Wireless settings – AP

AP Settings	
Multiple SSID index	The device supports multiple SSIDs (network names) which are indexed 1 to 4. This dropdown selects the index of the SSID to configure in the following settings.
SSID	Enter an SSID for the network.
Channel	Select the WLAN channel to use for the access point. This channel will be used for all 4 SSIDs.
WDS-Master Mode	When enabled, the unit will act as a WDS master on this network.
AP Isolation	Prevents clients connected to the AP from communicating directly with each other.
Security options	None: no encryption WEP: WEP (Wired Equivalent Privacy) WPA Personal: WPA (Wi-Fi Protected Access) uses a pre-shared key for authentication. 802.1x: authentication through a RADIUS server. WPA Enterprise: WPA/WPA2 Personal with RADIUS authentication (802.1x). WPA Personal (FT): WPA2 Personal with fast roaming (802.11r). WPA Enterprise (FT): WPA2 Enterprise with fast roaming (802.11r).

See also [RADIUS Authentication, p. 21](#) and [WLAN Fast Roaming, p. 21](#)

Wireless settings - Client

Fig. 16 Wireless settings – Client

Wireless Settings - Client	
Peer AP SSID	Enter the SSID of the WLAN AP to connect to
Peer AP BSSID	Enter the BSSID (MAC address) of the WLAN AP (if required)
Site Survey	Click to scan for available wireless networks
WDS-Slave Mode	When enabled, the unit will act as a WDS slave on this network.
Security options	None: no encryption WEP: WEP (Wired Equivalent Privacy) WPA Personal: WPA (Wi-Fi Protected Access) uses a pre-shared key for authentication. 802.1x: authentication through a RADIUS server. WPA Enterprise: WPA/WPA2 Personal with RADIUS authentication (802.1x). WPA Personal (FT): WPA2 Personal with fast roaming (802.11r). WPA Enterprise (FT): WPA2 Enterprise with fast roaming (802.11r).

See also [RADIUS Authentication, p. 21](#) and [WLAN Fast Roaming, p. 21](#)

Wireless settings - Bridge

Operation mode of the AP should be set to "Bridge-mode" before these settings are changed.

WDS Mode:

Peer MAC Address 1: ☒ Enabled

Peer MAC Address 2: ☒ Enabled

Peer MAC Address 3: ☐ Enabled

Peer MAC Address 4: ☐ Enabled

Please enter the WLAN MAC Address you want to connect to.
Format example :
Local wireless MAC **00:30:11:20:05:64**

SSID: Channel:

Security Options

Security Type:

Auth Mode: ☐ WPAPSK ☐ WPA2PSK ☒ WPAPSK/WPA2PSK mix

Encryption Type: ☐ TKIP ☐ AES ☒ TKIP/AES mix

Shared Key: (8-64 characters)

Fig. 17 Wireless settings – Bridge

Wireless settings - Bridge	
WDS Mode	WDS can operate in Bridge Mode or Repeater Mode (see below).
Peer MAC Address	Enter the MAC address of each access point and check the Enable box.
SSID (Repeater Mode)	Enter an SSID (network name) for the network. All devices must use the same SSID.
Channel	Enter the WLAN channel to use for the network. All devices must use this channel.
Security options	None: no encryption WEP: WEP (Wired Equivalent Privacy) WPA/WPA2 Personal: WPA (Wi-Fi Protected Access) uses a pre-shared key for authentication that is shared between the access point and its clients.

WDS Bridge Mode

In this mode the AP forwards traffic between WDS links and an Ethernet port. The AP learns MAC addresses of up to 64 wireless or 128 wired and wireless network devices, which are connected to their respective Ethernet ports to limit the amount of forwarded data. Only data destined for stations which are known to reside on the peer Ethernet link, multicast data, or data with unknown destinations need to be forwarded to the peer AP via the WDS link. The peer WDS APs are based on the MAC addresses listed in **Peer MAC Address**.

When using WDS Bridge Mode:

- LAN IP address should use a different IP in the same network.
- Shut down all DHCP server functions of the AP
- Enable WDS.
- Each AP should have the same setting except **Peer MAC Address** which should be set to the MAC address of the other unit.
- The settings of security and channel must be the same.
- The distance of the AP should be limited within a certainty area.

WDS Repeater Mode

This mode extends the range of the wireless infrastructure by forwarding traffic between associated wireless stations and another repeater or AP connected to the wired LAN. The peer WDS APs are based on the MAC addresses listed in **Peer MAC Address 1–4**.

4.3.2 Wireless Options

Wireless Settings --> Wireless Options

Wireless performance tuning

Radio:

Beacon Interval: (msec, range:20~1000, default:100)

DTIM Interval: (range: 1~255, default:1)

Fragmentation Threshold: (range: 256~2346, default:2346)

RTS Threshold: (range: 1~2347, default:2347)

Tx Power:

Wireless Mode: ☒ 2.4G ☐ 5G

Max Client Threshold: (range: 1~2007, default 255)

Preamble: ☒ Long ☐ Short

SSID Broadcast: ☐ Disable ☒ Enable

Tx Multicast Rate:

HT Require: ☒ Disable ☐ Enable

HT Band Width: ☐ 20 MHz ☒ 20/40 MHz

HT Guard Interval: ☐ Long ☒ Short

HT Extension Channel:

HT Tx STBC: ☒ Disable ☐ Enable

HT Rx STBC: ☒ Disable ☐ Enable

HT LDPC: ☒ Disable ☐ Enable

Fig. 18 Wireless options

Wireless options	
Radio	Enable/disable the WLAN interface.
Wireless Mode	Select 2.4 GHz or 5 GHz operation.
SSID Broadcast	Select if the SSID of the unit should be broadcasted or not.
Beacon Interval	These settings are for advanced configuration only and should normally be left at their default values.
DTIM Interval	
Fragmentation Threshold	
RTS Threshold	
Preamble	
Tx Multicast Rate	
HT Require	
HT Band Width	
HT Guard Interval	
HT Extension Channel	
HT Tx STBC	
HT Rx STBC	
HT LDPC	

4.3.3 RADIUS Authentication

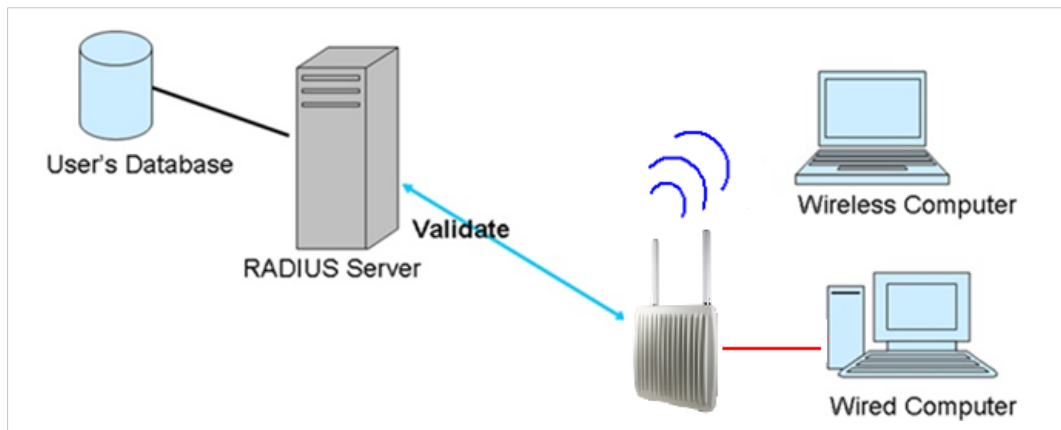


Fig. 19 Network with RADIUS authentication

RADIUS (Remote Authentication Dial-In User Service) is a widely deployed protocol that enables companies to authenticate and authorize remote users' access to a system or service from a central network server.

When you configure the remote access server for RADIUS authentication, the credentials of the connection request are passed to the RADIUS server for authentication and authorization. After the request is both authenticated and authorized, the RADIUS server sends an accept message back to the remote access server and the connection attempt is accepted. Otherwise, the RADIUS server sends a reject message back to the remote access server and the connection attempt is rejected.

4.3.4 WLAN Fast Roaming

The IEEE 802.11r fast roaming protocol, also known as Fast BSS Transition (FT), enables a WLAN client to roam quicker between 802.11r-enabled WLAN access points in the same mobility domain.

There are two methods for FT roaming: *Over-the-Air*, where the client communicates directly with the target access point, and *Over-the-DS*, where the client communicates through the current access point to another target access point.

Anybus WLAN Access Point IP67 can be configured to use IEEE 802.11r fast roaming with WPA personal or WPA Enterprise security in the access point and client modes. The mobility domain and a reassociation timeout value must be set.

Security Options

Security Type: WPA Personal(FT) ▼

Shared Key: (8-64 characters)

Mobility domain:

FT Roaming: ☒ Over-the-Air ☐ Over-the-DS

Reassociation timeout: (1000~65535 in ms)

Fig. 20 WPA Personal fast roaming settings

4.4 Advanced Settings

4.4.1 Filters

Advanced Settings --> Filters

Filters are used to allow or deny Wireless Clients from accessing the AP.

MAC Filters: ☒ Enabled ☐ Disabled

Options

☒ Only allow MAC address(es) listed below to connect to AP

☐ Only deny MAC address(es) listed below to connect to AP

Associated Clients: 00:30:11:19:43:2d Copy To 1

MAC Filter Table:

1.	00:30:11:19:43:2d	11.		21.	
2.		12.		22.	
3.		13.		23.	
4.		14.		24.	
5.		15.		25.	
6.		16.		26.	
7.		17.		27.	
8.		18.		28.	
9.		19.		29.	
10.		20.		30.	

Fig. 21 Filters

Allows you to set up MAC filters to allow or deny wireless clients to connect to the access point. You can add a MAC address manually or select one of the currently associated clients.

Filters	
MAC Filter	Enable/disable MAC filtering
Options	Select to allow or deny access for the listed MAC addresses
Associated Clients	Select the MAC address of a client, then use the Copy To dropdown to add it to the desired slot in the filter table.
MAC Filter Table	Enter MAC addresses to be filtered

4.4.2 Misc. Settings

Advanced Settings --> Misc. Settings

UPnP: ☒ Enable ☐ Disable

LLDP Protocol: ☒ Enable ☐ Disable

Fig. 22 Additional settings

Misc. Settings	
UPnP	Enables or disables UPnP
LLDP Protocol	Enables or disables the LLDP protocol

4.5 Event Warning Settings

The unit can be configured to issue notifications in various ways for selected events. Fill in the required settings on the following pages and check the corresponding box for each event to enable reporting.

4.5.1 System Log

Event Warning Settings -> System Log

Syslog Server Settings

Syslog Server IP:

Syslog Server Port: (0 represents default)

Syslog Event Types

Device Event Notification

Hardware Reset (Cold Start)	<input type="checkbox"/> Syslog
Software Reset (Warm Start)	<input type="checkbox"/> Syslog
Login Failed	<input type="checkbox"/> Syslog
IP Address Changed	<input type="checkbox"/> Syslog
Password Changed	<input type="checkbox"/> Syslog
Redundant Power Changed	<input type="checkbox"/> Syslog
Eth Link Status Changed	<input type="checkbox"/> Syslog
SNMP Access Failed	<input type="checkbox"/> Syslog
Wireless Client Associated	<input type="checkbox"/> Syslog
Wireless Client Disassociated	<input type="checkbox"/> Syslog
Client Mode Associated	<input type="checkbox"/> Syslog
Client Mode Disassociated	<input type="checkbox"/> Syslog
Client Mode Roaming	<input type="checkbox"/> Syslog

Fault Event Notification

Power 1 Fault	<input type="checkbox"/> Syslog
Power 2 Fault	<input type="checkbox"/> Syslog
Eth1 Link Down	<input type="checkbox"/> Syslog
Eth2 Link Down	<input type="checkbox"/> Syslog
DI1 ON->OFF	<input type="checkbox"/> Syslog
DI2 ON->OFF	<input type="checkbox"/> Syslog
DI3 ON->OFF	<input type="checkbox"/> Syslog
DI4 ON->OFF	<input type="checkbox"/> Syslog
DI1 OFF->ON	<input type="checkbox"/> Syslog
DI2 OFF->ON	<input type="checkbox"/> Syslog
DI3 OFF->ON	<input type="checkbox"/> Syslog
DI4 OFF->ON	<input type="checkbox"/> Syslog

Fig. 23 System log settings

Syslog Server Settings	
Syslog Server IP	Enter the IP address of a syslog server if you want the logs to be stored remotely. Leave this field blank to disable remote syslog.
Syslog Server Port	Specifies the syslog port. The default port is 514.

4.5.2 E-mail

Event Warning Settings --> E-mail

E-mail Server Settings

SMTP Server: (optional)

Server Port: (0 represents default)

☐ **My Server requires authentication**

User Name:

Password:

Sender Address:

E-mail Address 1:

E-mail Address 2:

E-mail Address 3:

E-mail Address 4:

Fig. 24 E-mail

E-mail Server Settings	
SMTP Server/Port	Enter the SMTP server address and port.
E-mail Address 1–4	Enter up to 4 email addresses that will receive the notifications.

Click the checkbox and enter authentication information if required by the SMTP server.

4.5.3 SNMP

Event Warning Settings --> SNMP Settings

SNMP Settings

SNMP Agent: ☒ Enable ☐ Disable

SNMP Trap Server 1:

SNMP Trap Server 2:

SNMP Trap Server 3:

SNMP Trap Server 4:

Community:

SysLocation:

SysContact:

Fig. 25 SNMP settings

SNMP Settings	
SNMP Agent	Enable/disable SNMP reporting
SNMP Trap Server 1-4	Enter the IP address of the SNMP server(s)
Community	As required
SysLocation	
SysContact	

4.5.4 Relay

Event Warning Settings -> Relay

Fault LED/Relay

Power 1 Fault	<input type="checkbox"/> Fault LED/Relay
Power 2 Fault	<input type="checkbox"/> Fault LED/Relay
Eth1 Link Down	<input type="checkbox"/> Fault LED/Relay
Eth2 Link Down	<input type="checkbox"/> Fault LED/Relay
DI1 ON->OFF	<input type="checkbox"/> Fault LED/Relay
DI2 ON->OFF	<input type="checkbox"/> Fault LED/Relay
DI3 ON->OFF	<input type="checkbox"/> Fault LED/Relay
DI4 ON->OFF	<input type="checkbox"/> Fault LED/Relay
DI1 OFF->ON	<input type="checkbox"/> Fault LED/Relay
DI2 OFF->ON	<input type="checkbox"/> Fault LED/Relay
DI3 OFF->ON	<input type="checkbox"/> Fault LED/Relay
DI4 OFF->ON	<input type="checkbox"/> Fault LED/Relay

Fig. 26 Fault LED/Relay settings

Select events that should trigger the Fault LED and relay output.

4.6 System Status

4.6.1 Wireless Link List

System Status -> Wireless Link List

List of connected wireless clients.

Mac Address	Rx Bytes	Rx Packets	Tx Bytes	Tx Packets	Rssi Quality	Bitrate	Link Type
00:30:11:19:43:2d	93748782	691347	57182	888	100 %	54.0 Mbps	Client

Refresh

Fig. 27 Wireless link list

Lists the wireless clients that are currently connected to the access point.

Click on **Refresh** to update the list.

4.6.2 DHCP Client List

System Status -> DHCP Client List

DHCP Clients List:

Hostname	Mac Address	IP Address	Expires In
None	00:30:11:19:43:2c	192.168.0.51	1 days 23:59:57

Fig. 28 DHCP client list

Lists the devices on your network that are receiving dynamic IP addresses from the built-in DHCP server.

4.6.3 Traffic/Port Status

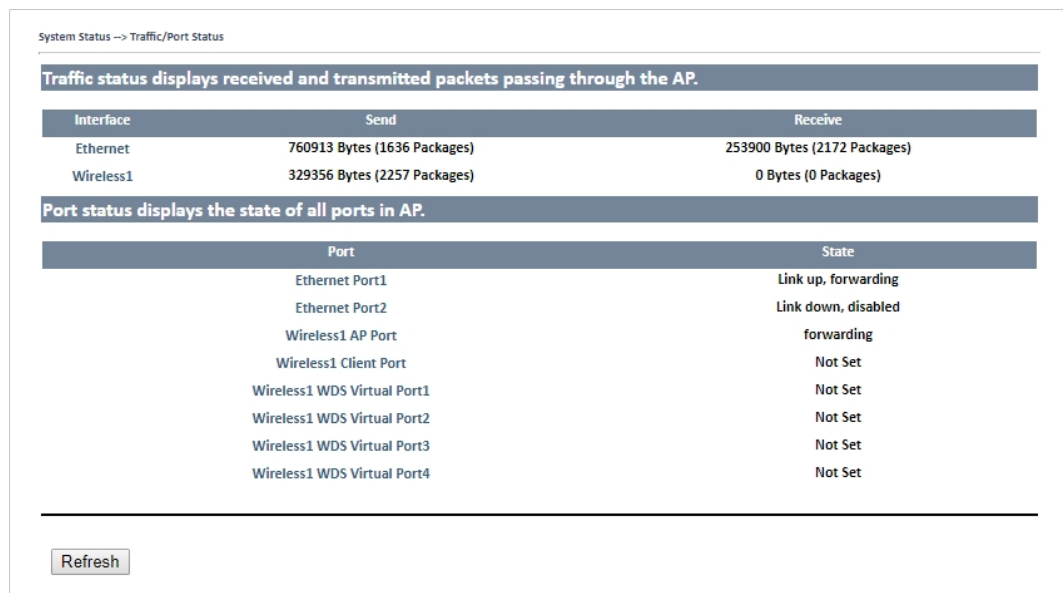


Fig. 29 Traffic/port status

Network traffic statistics for both received and transmitted packets through the Ethernet and wireless connections. The traffic counter will reset when the device is rebooted.

Click on **Refresh** to update the list.

4.6.4 System Log



Fig. 30 System log

Events and activities are logged continuously in the system log.

Click **Refresh** to renew the page or **Clear** to clear the log entries.

4.7 Administrator

4.7.1 Password

Fig. 31 Password

This page allows you to change the user ID and password for web access. The default user ID and password are both **admin**.



For security reasons the default password should always be changed.

Password	
Old Name	Enter the current user ID
Old Password	Enter the current password
New Name	Enter a new user ID. The user ID must consist of 1 to 15 characters and can only include A-Z, a-z, 0-9.
New Password	Enter the new password. The password must consist of 1 to 15 characters and can only include A-Z, a-z, 0-9.
Confirm New Password	Enter the new password again.

4.7.2 Configuration

Fig. 32 Configuration

This page allows you to save and restore configurations.

Configuration	
Download	Click to save the current configuration as a file on your computer.
Choose File/Upload	Click on Choose File to locate a saved configuration file, then click on Upload to install it. The unit will automatically validate the configuration file and then restart the unit with the uploaded configuration.

4.7.3 Firmware Upgrade

Fig. 33 Firmware upgrade

1. Download the firmware file from www.anybus.com/support and save it to your computer. Make sure that the file is the correct one for your access point model and version.
2. Click on **Choose File** and select the downloaded firmware file.
3. Click on **Start Upgrade** to apply the new firmware.

The unit will reboot automatically when the upgrade is completed.



Do not power off the unit while the upgrade is in progress as this may put the unit in an unrecoverable state.

4.7.4 Load Factory Default

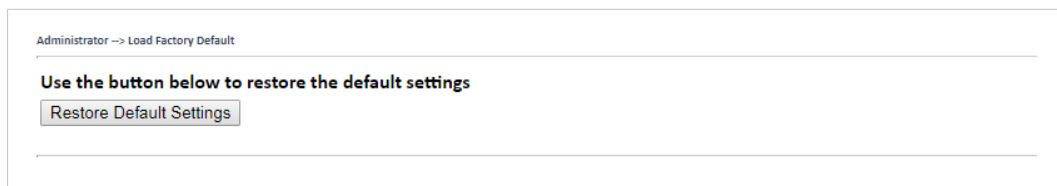


Fig. 34 Load factory default

Click on **Restore Default Settings** to restore the unit to the factory default settings.

4.7.5 Restart

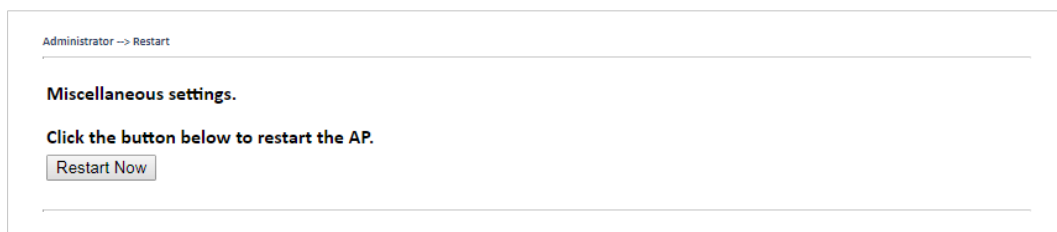


Fig. 35 Restart

Click on **Restart Now** to restart the unit.

5 Technical Data

5.1 Technical Specifications

Order code	AWB4004
Wireless antenna	External (N-type)
Wired interface	Ethernet
Ethernet port	10/100/1000Base-T(X) Auto MDI/MDX M12 8-pin female A-coded connector
Power connector	M12 5-pin female A-coded connector (dual power inputs in single connector)
Power supply	2 x 12–48 VDC
Power over Ethernet	44–57 VDC DTE Type1 according to IEEE 802.3af
Current consumption	Max. 0.75 A @ 12 VDC (9 W)
Dimensions (WxHxD)	310 x 87 x 310 mm
Weight	2.56 kg
Operating temperature	-25 to +70 °C
Storage temperature	-40 to +85 °C
Humidity	5 % to 95 % non-condensing
Mounting	Wall mount or pole mount
Housing	Metal
Protection class	IP67
Certifications	See datasheet

For more technical details and specifications, visit www.anybus.com/support.

Disposal and recycling



You must dispose of this product properly according to local laws and regulations. Because this product contains electronic components, it must be disposed of separately from household waste. When this product reaches its end of life, contact local authorities to learn about disposal and recycling options, or simply drop it off at your local HMS office or return it to HMS. For more information, see www.hms-networks.com.

5.2 Dimensions

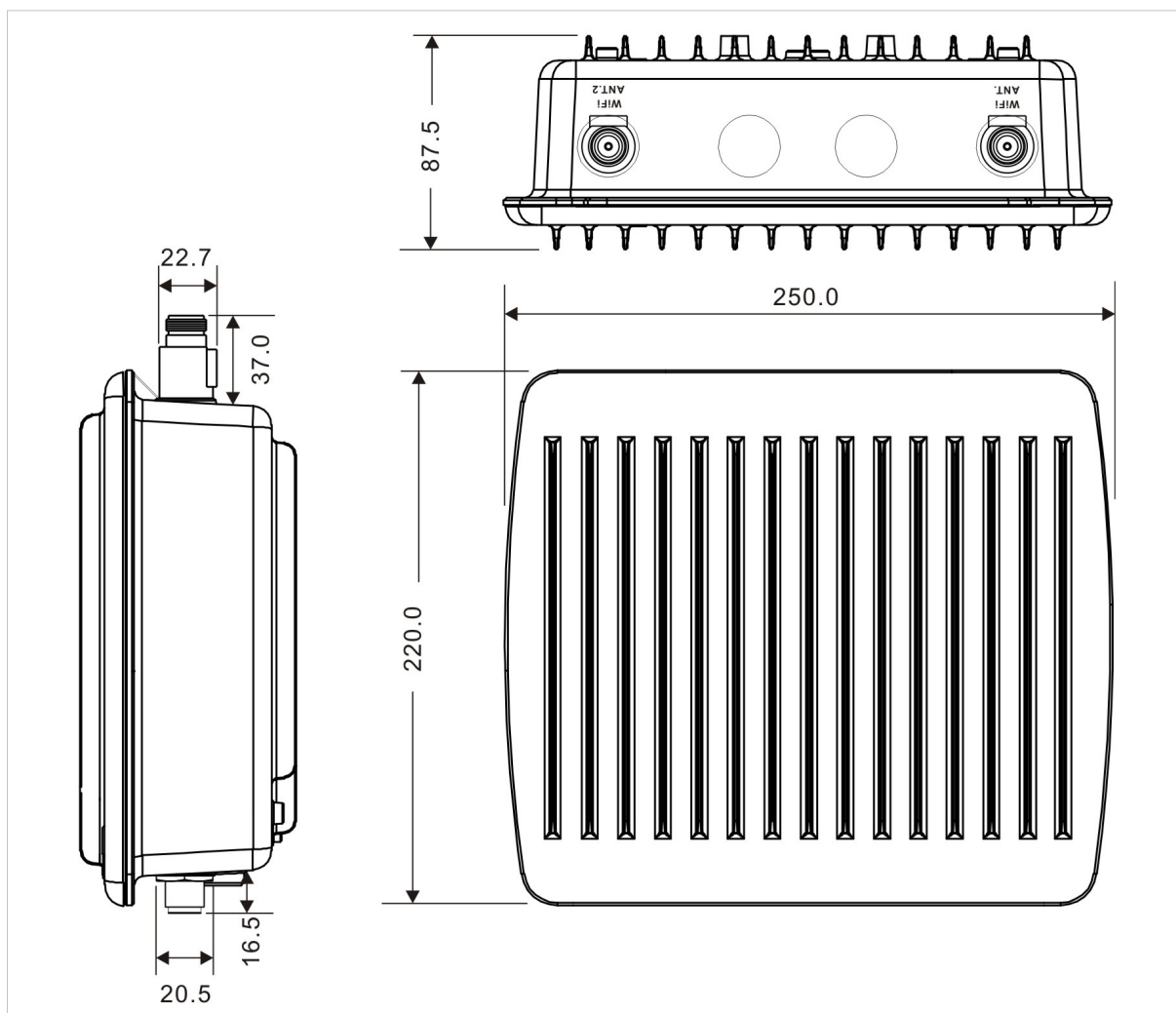


Fig. 36 Dimensions

All measurements are in mm.

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.

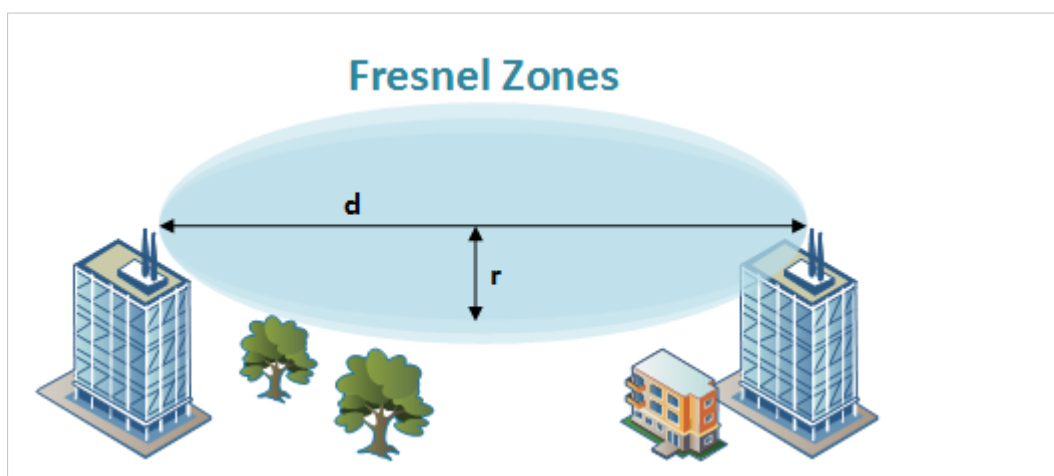


Fig. 37 Fresnel zones

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.

