ENGLISH

Anybus® Wireless Access Point IP30 with Mesh

USER MANUAL

SCM-1202-155
Version 1.1
Publication date 2022-06-02

Important User Information

Disclaimer

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

HMS Networks reserves the right to modify its products in line with its policy of continuous product development. The information in this document shall therefore not be construed as a commitment on the part of HMS Networks and is subject to change without notice. HMS Networks makes no commitment to update or keep current the information in this document.

The data, examples and illustrations found in this document are included for illustrative purposes and are only intended to help improve understanding of the functionality and handling of the product. In view of the wide range of possible applications of the product, and because of the many variables and requirements associated with any particular implementation, HMS Networks cannot assume responsibility or liability for actual use based on the data, examples or illustrations included in this document nor for any damages incurred during installation of the product. Those responsible for the use of the product must acquire sufficient knowledge in order to ensure that the product is used correctly in their specific application and that the application meets all performance and safety requirements including any applicable laws, regulations, codes and standards. Further, HMS Networks will under no circumstances assume liability or responsibility for any problems that may arise as a result from the use of undocumented features or functional side effects found outside the documented scope of the product. The effects caused by any direct or indirect use of such aspects of the product are undefined and may include e.g. compatibility issues and stability issues.

Contact Information

Postal address:
Box 4126
300 04 Halmstad, Sweden

E-Mail: info@hms.se

Table of Contents

1. Preface 1
1.1. About This Document 1
1.2. Document Conventions 1
1.3. Trademarks 2

2. Safety 3
2.1. General Safety 3
2.2. Intended Use 3

3. Preparation 4
3.1. Support and Resources 4

4. Installation 5
4.1. DIN Rail Mounting 5
4.2. Connect Ground Screw 6
4.3. Connect to Power 6
4.3.1. Connect to Power via Terminal Block 7
4.3.2. Connect to Power via Ethernet PoE 8
4.4. Connect to Ethernet 9
4.5. Connect Antennas 9

5. Configuration 10
5.1. Before You Begin Configuration 10
5.2. Access the Web Management Interface 10
5.3. Configure the Country/Region Settings 11
5.4. Submit and Save Configuration 11
5.5. Factory Reset 12
5.6. System 13
5.6.1. Information 13
5.6.2. Login Setting 13
5.6.3. Network Setting 13
5.6.4. Date and Time 14
5.6.5. DHCP Server 14
5.7. Ethernet Port 15
5.7.1. Port Status 15
5.7.2. Port Setting 15
5.7.3. Traffic Control 15
5.8. Wireless LAN 16
5.8.1. WLAN Status 16
5.8.2. WLAN Setting 17
5.8.3. Multi SSID 19
5.8.4. Mesh Settings 20
5.8.5. WLAN Security 21
5.8.6. Advanced 21
5.8.7. Radius Server 22
5.8.8. Certificate File (Client Mode) 22
5.9. Security 22
5.9.1. Access Control 22
5.9.2. Outbound Firewall 22
5.9.3. NAT Setting 23
5.9.4. OpenVPN 24
5.9.5. IPSec Setting 25

5.9.6. L2TP Setting 25
5.10. Warning 26
5.10.1. Ping Watchdog 26
5.10.2. Syslog Setting 26
5.11. Diagnostics 27
5.11.1. Event Logs 27
5.11.2. ARP Table 27
5.11.3. Ping 27
5.11.4. Trace Route 28
5.11.5. Network Statistics 28
5.11.6. Association List 28
5.12. Backup/Restore 28
5.12.1. WEB Backup and Restore 28
5.13. Firmware Upgrade 29
5.13.1. WEB Firmware Upgrade 29
5.14. Reset to Default 30

6. Verify Operation 31
6.1. Front Panel LED 31

7. Technical Data 32
7.1. Technical Specifications 32

8. Reference Guides 33
8.1. Wireless Technology Basics 33

1. Preface

1.1. About This Document

This document describes how to install and configure Anybus® Wireless Access Point IP30 with Mesh.

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

1.2. Document Conventions

Lists

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

1. First do this
2. Then do this

Bulleted lists are used for:

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

User Interaction Elements

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

Program Code and Scripts

```
Program code and script examples
```

Cross-References and Links

Cross-reference within this document: Document Conventions

External link (URL): www.anybus.com

Safety Symbols

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

WARNING
Instruction à suivre pour éviter tout risque de décès ou de blessure grave.

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

CAUTION
Instruction à suivre pour éviter tout risque de blessure.

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

Information Symbols

NOTE
Additional information which may facilitate installation and/or operation.

TIP
Helpful advice and suggestions.

1.3. Trademarks

Anybus® is a registered trademark of HMS Networks.

All other trademarks mentioned in this document are the property of their respective holders.

2. Safety

2.1. General Safety

CAUTION
Ensure that the power supply is turned off before connecting it to the equipment.

CAUTION
Assurez-vous que l'alimentation électrique est coupée avant de la brancher sur l'équipement.

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

CAUTION
Le fait de brancher l'alimentation avec une polarité inversée ou d'utiliser le mauvais type d'alimentation peut endommager l'équipement. Assurez-vous que l'alimentation électrique est correctement branchée et conforme au type recommandé.

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

CAUTION
Cet équipement contient des pièces qui peuvent être endommagées par une décharge électrostatique (ESD). Appliquez les mesures de prévention ESD pour éviter les dommages.

2.2. Intended Use

The intended use of this equipment is to provide wireless LAN connectivity. The equipment receives and transmits data on various physical levels and connection types.

If this equipment is used in a manner not specified by the manufacturer, the protection provided by the equipment may be impaired.

3. Preparation

3.1. Support and Resources

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

TIP

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

4. Installation

4.1. DIN Rail Mounting

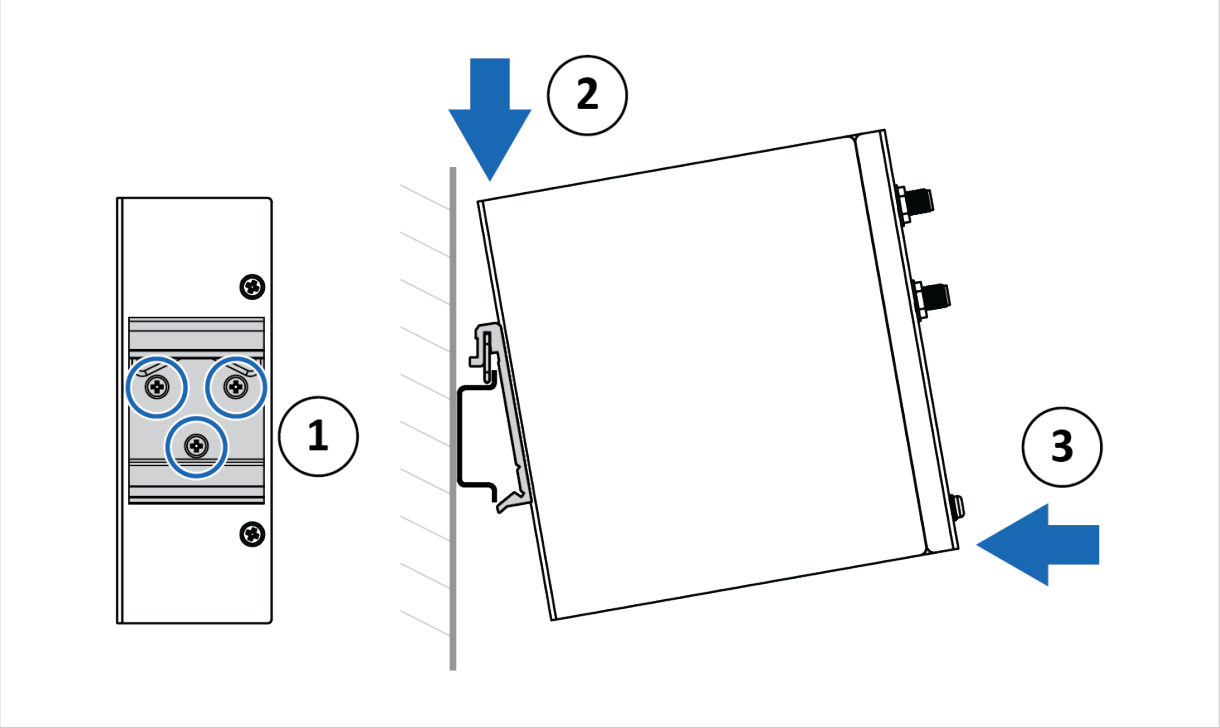


Figure 1. DIN rail mounting option

1. Fasten the DIN clip with 3 (M3x6 flat head) screws on the rear side of the access point.
2. Insert the upper end of the DIN rail clip into the DIN rail.
3. Push the bottom of the DIN rail clip into the DIN rail.

4.2. Connect Ground Screw

IMPORTANT
To avoid system damage, the equipment should be connected to ground.

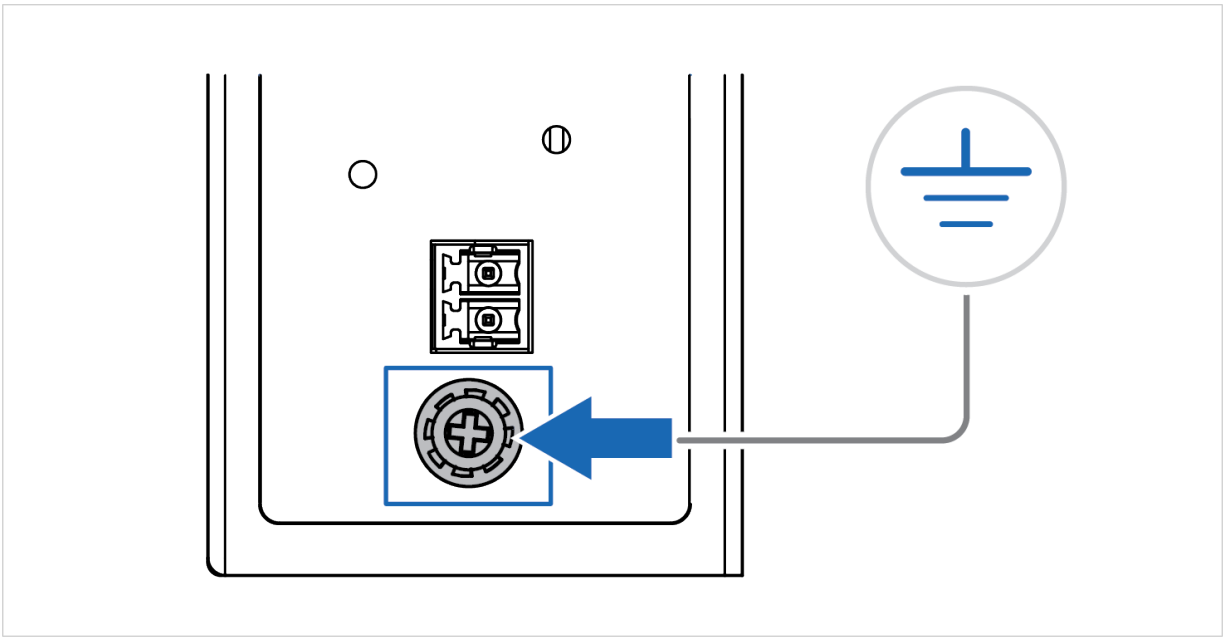


Figure 2. Connect ground screw

- Establish a direct connection between the ground screw and the grounding surface prior to connecting devices.

4.3. Connect to Power

CAUTION
Ensure that the power supply is turned off before connecting it to the equipment.

CAUTION
Assurez-vous que l'alimentation électrique est coupée avant de la brancher sur l'équipement.

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

CAUTION
Le fait de brancher l'alimentation avec une polarité inversée ou d'utiliser le mauvais type d'alimentation peut endommager l'équipement. Assurez-vous que l'alimentation électrique est correctement branchée et conforme au type recommandé.

4.3.1. Connect to Power via Terminal Block

IMPORTANT
Use a power supply of 10-60 VDC for terminal block and 48 VDC for PoE.

Max power consumption: 11.5 W

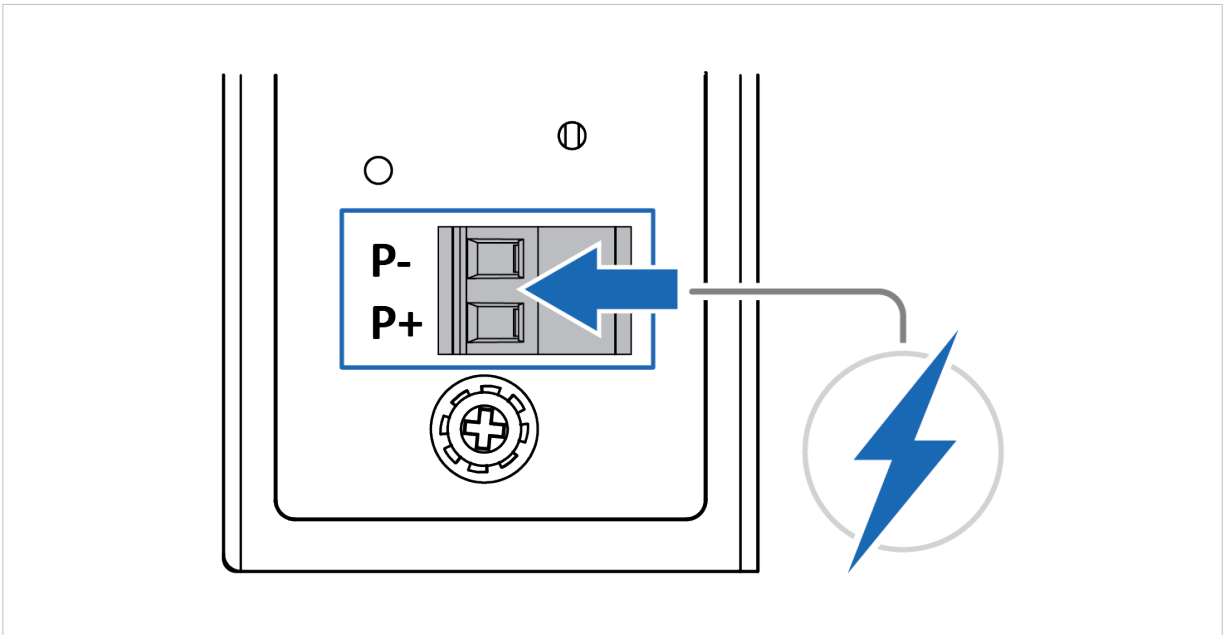


Figure 3. Connect to power via terminal blo

P-	10-60 VDC (terminal block) Max. 11.5 W
P+	

1. Insert the positive and negative wires into the *P-* and *P+* contact on the terminal block.
2. Tighten the 2 wire-clamp screws.
3. Connect the power wires to a DC power supply.

4.3.2. Connect to Power via Ethernet PoE

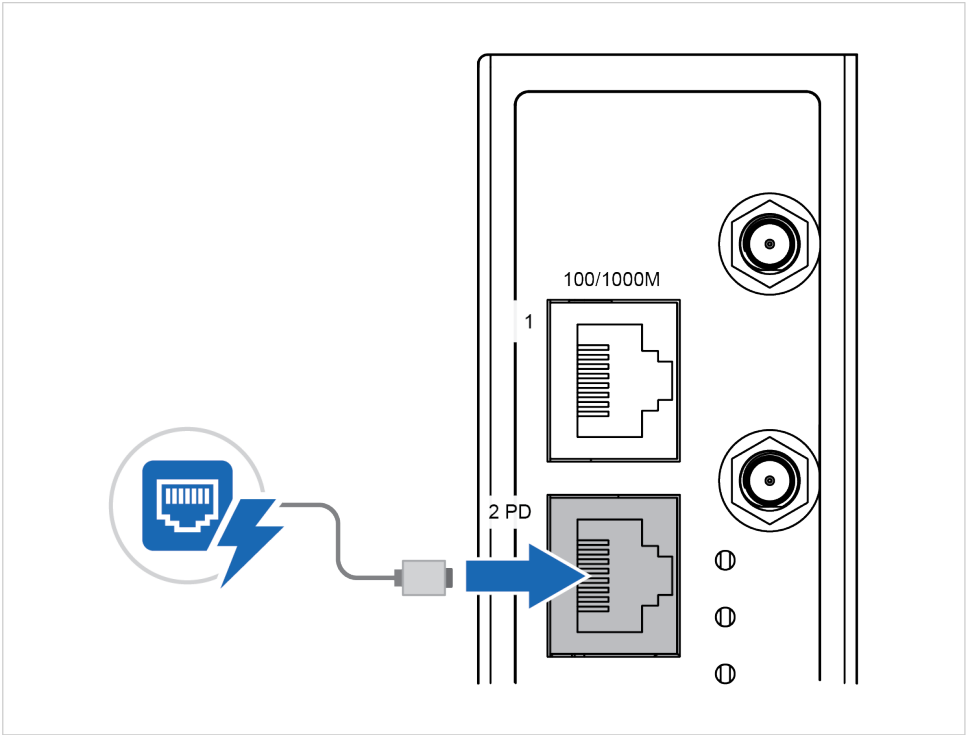


Figure 4. Connect to power via Ethernet PoE

Port	Function	Power
2 PD	WAN 1 Gbit/s PoE enabled	IEEE 802.3af (48 VDC PoE)

- Connect the access point to an Ethernet network via the WAN PoE enabled port.

4.4. Connect to Ethernet

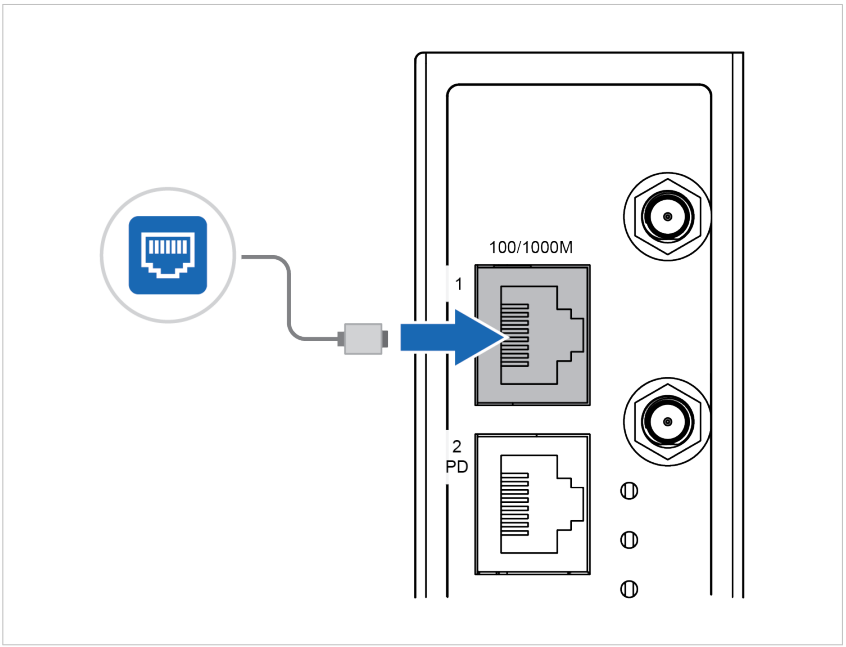
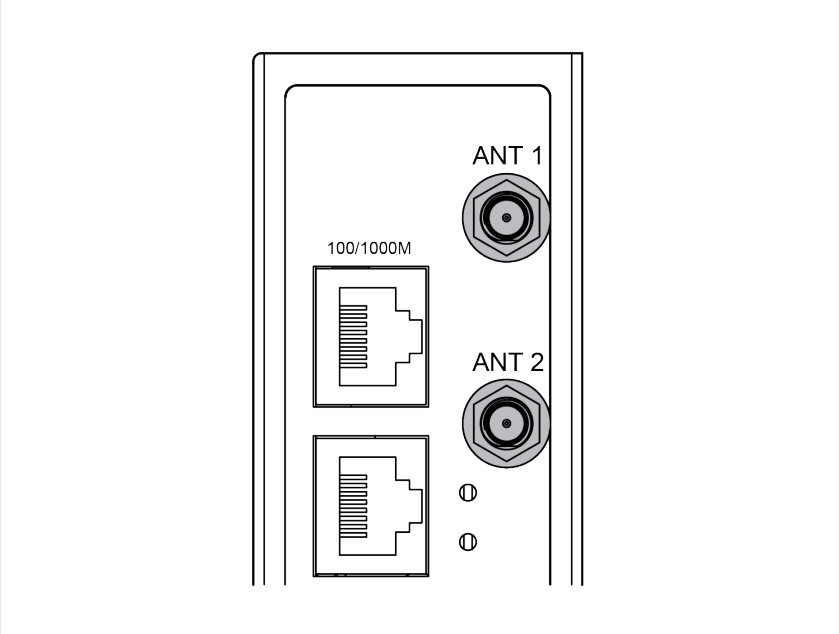


Figure 5. Connect to Ethernet

Port	Function	Speed
1	LAN	1 Gbit/s

- Connect the access point to an Ethernet network via the LAN port.

4.5. Connect Antennas



Placement	Type
ANT 1	WLAN 1, RP-SMA connector, female
ANT 2	WLAN 2, RP-SMA connector, female

5. Configuration

5.1. Before You Begin Configuration

The access point is configured through web management.

NOTE
The switch default IP address is **http://192.168.10.1/**.

NOTE
The default switch login user name is **admin** and the password is **admin**.

5.2. Access the Web Management Interface

Prepare for configuring the switch settings via the web management interface.

Before You Begin

1. Connect the access point to your computer.
2. Connect the access point to power.
3. To link your computer with the access point, make sure that the IP address of the computer is located in the same subnet as the switch default IP address.

Procedure

Access the web management interface:

1. In your browser, type **http://IP address** and press **Enter**.
   The web-based management interface login screen appears.
2. In the login screen, enter user name and password.
3. Click **OK**.
   The web-based management interface welcome page appears.

To Do Next

- Configure the access point.

5.3. Configure the Country/Region Settings

IMPORTANT
To comply with the Radio Equipment Directive (RED) and local radio regulations you must configure the country/region settings before the access point is brought into use.

Procedure

Configure the Country settings.

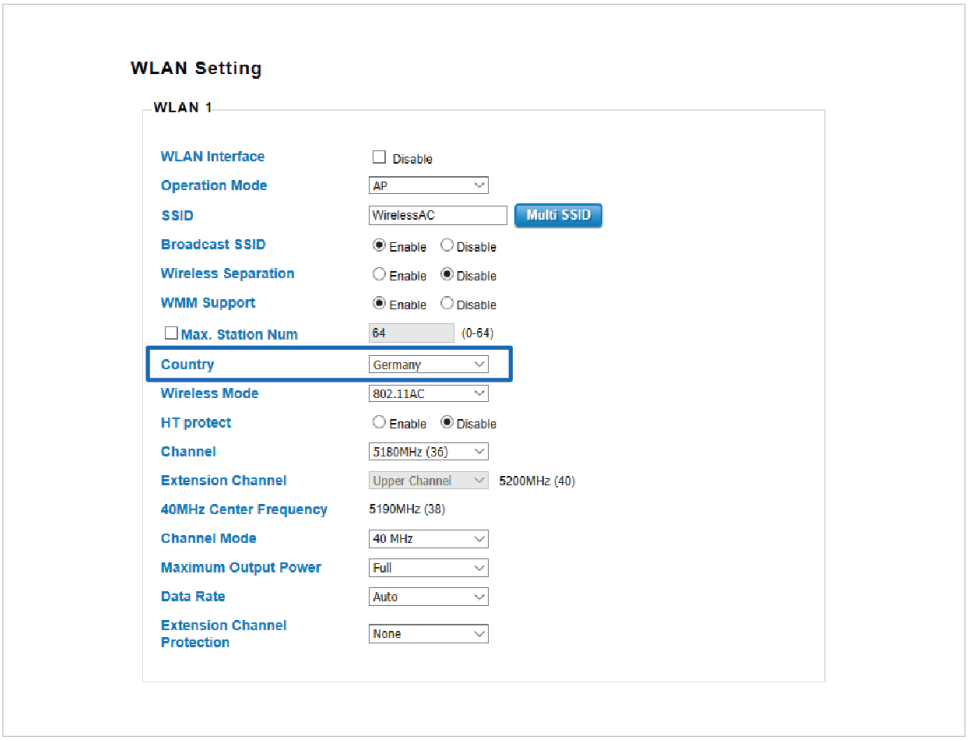


Figure 6. Country settings

In the web management interface:

1. Navigate to the **WLAN Settings** tab.
2. Select your country/region from the **Country** drop-down menu.
3. Press **Submit** button for the setting to take effect.

5.4. Submit and Save Configuration

To apply changes made on a configuration page/tab, click **Submit** at the bottom of the page.

To discard the changes, click **Cancel**.

Some pages have additional buttons that are described in the respective sections in this manual.

To save changed settings permanently, click **Save** at the top of the configuration page. The recent changes will otherwise be discarded if the access point is rebooted.

Figure 7. Web Management Inteface, top menu

5.5. Factory Reset

Reset the access point to its factory settings.

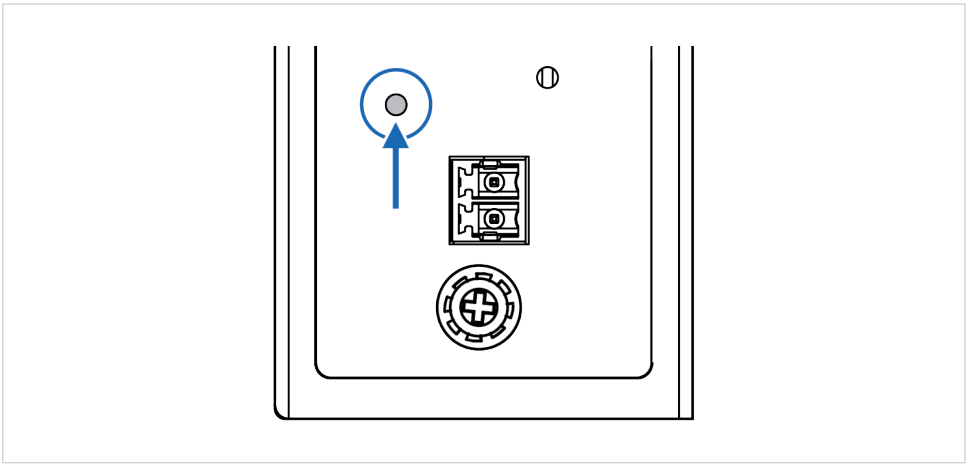


Figure 8. Factory reset button

1. Ensure that the access point is powered on.
2. Use a pointed object, such as a ballpoint pen, to press and hold the reset button for >10 seconds.

Result

- Once the reset button is released, the access point reboots automatically.
- When the access point has successfully rebooted, the SYS LED turns green.

5.6. System

5.6.1. Information

Figure 9. System configuration page

System Name	Name of the unit Default: AP
System Description	A short description of the unit for easier identification Default: WLAN AP
Software Version	The currently installed firmware version
MAC Address	MAC address of the Ethernet network interface
IP Address	IP Address of the Ethernet network interface
Subnet Mask	Subnet mask of the Ethernet network interface

5.6.2. Login Setting

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

User Name / Guest Name	Names for the normal user account and the guest account Default: admin/guest
New Password	Enter a password for accessing the web interface
Confirm Password	Re-type the new password again to confirm it

5.6.3. Network Setting

Table 1. IPv4 Configuration

IP Assignment/Type	Select static or dynamic IP addressing (DHCP)
IP Address	Static IP address for the unit Default: 192.168.10.1
Subnet Mask	Subnet mask when using static IP Default: 255.255.255.0
Gateway IP Address	Default gateway when using static IP Default: 0.0.0.0.
DNS 1	IP address of primary DNS server when using static IP
DNS 2	IP address of secondary DNS server when using static IP

Table 2. WAN Setting (Router Mode)

WAN Access Type	Select static or dynamic IP addressing (DHCP)
IP Address	Static IP address for the unit Default: 192.168.1.1
Subnet Mask	Subnet mask when using static IP Default: 255.255.255.0
Gateway IP Address	Default gateway when using static IP Default: 0.0.0.0.
DNS 1	IP address of primary DNS server when using static IP
DNS 2	IP address of secondary DNS server when using static IP

5.6.4. Date and Time

Current Time	Set the date and time manually
Get PC Time	Click to update the date and time from the connected PC
Time Zone	Select the desired time zone
NTP	When enabled, the date and time will be updated automatically from a specified NTP server. Select an NTP server in the dropdown list or enter the IP address for the NTP server.

5.6.5. DHCP Server

IMPORTANT
Do not enable DHCP Server if there is already an active DHCP server on the network, as this may result in IP address conflicts.

DHCP Setting	Enable/disable the internal DHCP server
IP Address Start	Set the range of IP addresses that can be allocated by the DHCP Server
IP Address End	
Subnet Mask	Subnet mask for the DHCP Server Default: 255.255.255.0
Gateway	Default gateway for the DHCP Server.
WIN S1	IP address for primary WINS Server
WIN S2	IP address for secondary WINS Server
Primary DNS Server	IP address of primary DNS server
Secondary DNS Server	IP address of secondary DNS server
Lease Time	Maximum DHCP lease time in minutes (range: 15-44640 minutes) Default: 1440

Table 3. DHCP Leased Entries

IP Address	IP address assigned by the DNS server
MAC Address	MAC Address of the node
Time to expire(s)	Remaining DHCP lease time for the node

5.7. Ethernet Port

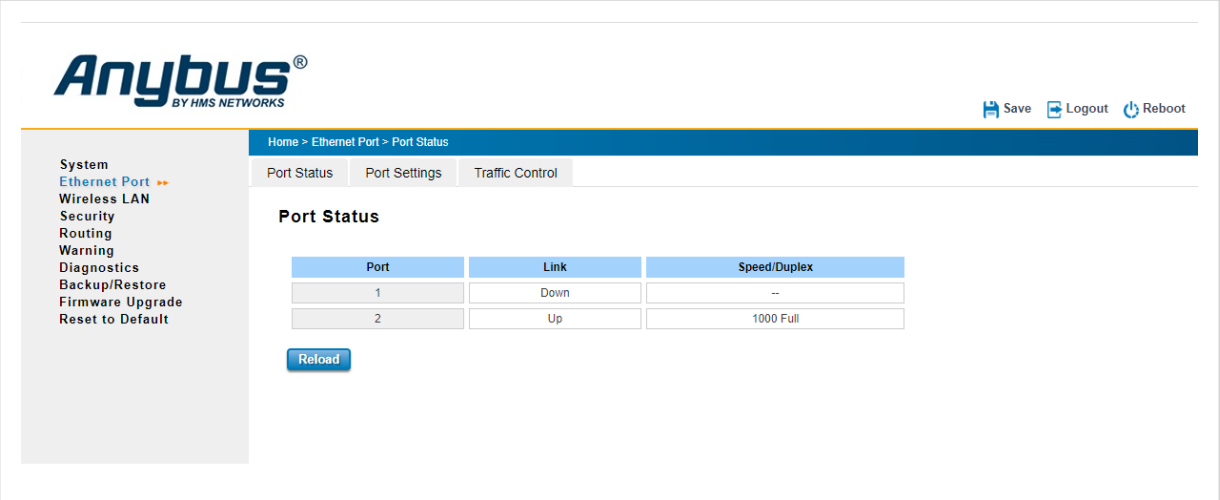


Figure 10. Ethernet Port configuration page

5.7.1. Port Status

Port	Ethernet port number (label)
Link	Link Up = Ethernet link established Link Down = no Ethernet link
Speed/Duplex	Speed (10/100/1000 Mbit/s) and duplex mode (Half/Full) for the port.

5.7.2. Port Setting

Port	Ethernet port number (label)
State	Enable or disable this port Default: Enable
Speed/Duplex	Select the speed and duplex mode for the port. Ports 1–2 (Gigabit Ethernet) can be set to AutoNegotiation (1 Gbit/s), 100 Full and 100 Half. Default: AutoNegotiation

5.7.3. Traffic Control

Enable Traffic Control	Enable/disable traffic control
Outgoing Rate Limit	Maximum outgoing data rate Default: 1024000 kbit/s
Outgoing Burst	Maximum outgoing burst size Default: 20 kBytes

5.8. Wireless LAN

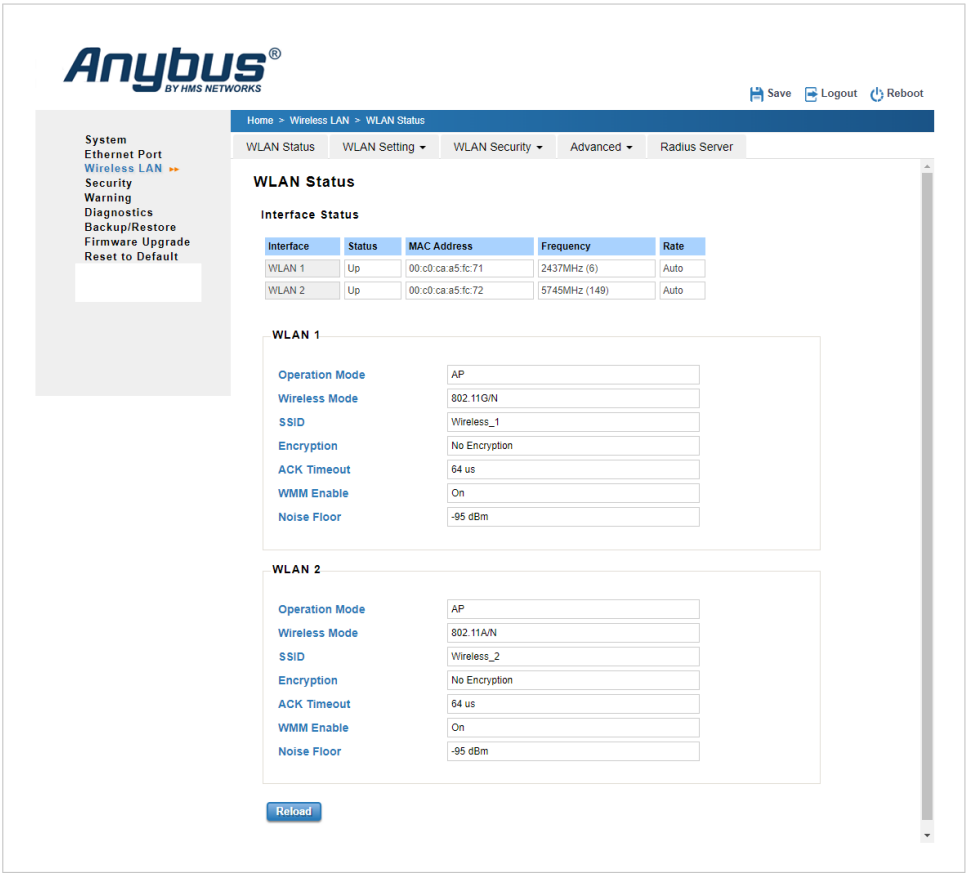


Figure 11. WLAN configuration page

5.8.1. WLAN Status

Operation Mode	Operation mode of the WLAN interface. See WLAN Setting (page 17).
Wireless Mode	WLAN mode
SSID	SSID of the WLAN interface
Encryption	Encryption mode used
ACK Timeout	For long distance connections, typically point-to-point, acknowledgment (ACK) timeout can be set manually to avoid excessive retransmitting.
WMM Enable	WMM enabled/disabled
Noise Floor	Background noise level (dBm)

5.8.2. WLAN Setting

IMPORTANT
To comply with the European Radio Equipment Directive (RED) and local radio regulations you must configure the country/region settings before the access point is brought into use.

Table 4. Common Settings

WLAN Interface	Check the box to **disable** the WLAN interface.
Operation Mode	Select the operation mode for the WLAN interface: AP (access point), Wireless Client, WDS-AP, or WDS-Client. Default: AP
SSID	Enter the SSID of the currently selected wireless network. If the SSID of the desired network is not broadcasted it can be entered here manually. Default: Wireless
WMM Support	Enhances quality of service (QoS) on the wireless network by prioritizing data packets depending on category. Default: Enable
Country	Select the country or region where the wireless access point is operating.
Wireless Mode	Select the wireless mode (protocol). Default: 802.11g/n
Channel Mode	Select 20 MHz, 20/40 MHz or 40 MHz channel bandwidth. Default: 20 MHz
Maximum Output Power	Transmission output power can be set in stages from minimum to full power. Default: Half
Data Rate	Data transmission rate. Default: Auto
Extension Channel Protection	Enable CTS-Self or RTS-CTS channel protection. Default: None

The following additional settings are specific for each operation mode.

Table 5. AP (Access Point)

Multi SSID	Click to configure multiple profiles. See Multi SSID (page 19).
Broadcast SSID	Enable/disable broadcasting the SSID on the network. Default: Enable
Wireless Separation	When enabled, wireless clients connected to the access point cannot communicate directly with each other. Default: Disable
Max Station Num	The maximum number of clients allowed to connect to the access point.
HT Protect	Enable High Throughput protection. Default: Disabled
Channel	Select WLAN channel. Default: 2437MHz (Channel 6)
Extension Channel	Available in 802.11n mode when the bandwidth is set to 20/40 MHz or 40 MHz, and in 802.11ac mode when bandwidth is set to 40 MHz or 80 MHz. A lower or upper extension channel will be set by the router based on the selected control channel. If the selected control channel is in the middle range of the channel band, the user can choose between the upper or lower extension channel.

Table 6. Wireless Client

Site Survey	Click to scan for wireless networks, select the desired network from the **Wireless Site Survey** list, then click Selected to connect the network.

Table 7. WDS-AP

Broadcast SSID	Enable/disable broadcasting the SSID on the network. Default: Enable
Wireless Separation	When enabled, wireless clients connected to the access point cannot communicate directly with each other. Default: Disable
Max Station Num	The maximum number of clients allowed to connect to the access point.
HT Protect	Enable High Throughput protection. Default: Disabled

Table 8. WDS-AP

Broadcast SSID	Enable/disable broadcasting the SSID on the network. Default: Enable
Wireless Separation	When enabled, wireless clients connected to the access point cannot communicate directly with each other. Default: Disabled
Max Station Num	The maximum number of clients allowed to connect to the access point.
HT Protect	Enable High Throughput protection. Default: Disabled
Channel	Select WLAN channel. Default: 2437MHz (Channel 6)
Extension Channel	Available in 802.11n mode when the bandwidth is set to 20/40 MHz or 40 MHz, and in 802.11ac mode when bandwidth is set to 40 MHz or 80 MHz. A lower or upper extension channel will be set by the access point based on the selected control channel. If the selected control channel is in the middle range of the channel band, the user can choose between the upper or lower extension channel.

Table 9. WDS-Client

Site Survey	Click to scan for wireless networks, select the desired network from the **Wireless Site Survey** list, then click **Selected** to connect the network.
AP MAC Address	Enter the MAC address of the WDS-AP to connect to.

5.8.3. Multi SSID

The access point can have multiple active WLAN profiles with individual SSIDs and authentication settings.

Profile 1 is the default profile and is always enabled.

To set up a profile: check the box to enable the profile, then click on the profile name.

Figure 12. WLAN Profiles

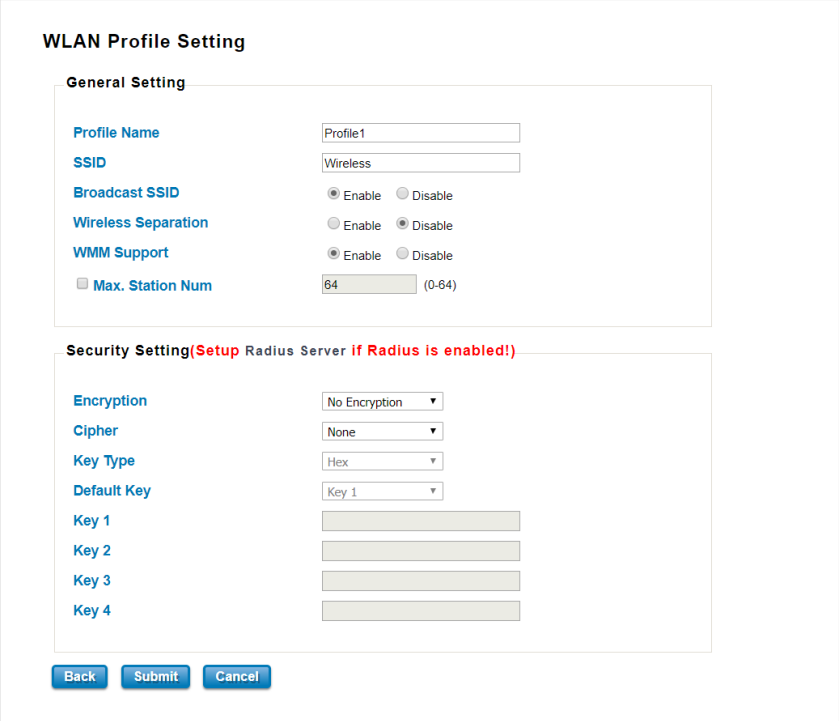


Figure 13. WLAN profile settings

Table 10. Multi SSID

Profile Name	Name of the profile
SSID	SSID (network name) for the profile
Security	Security mode to use for the profile
Enable	Check the box to enable the profile

Security settings are set individually for each WLAN profile. The security settings for the default profile (Profile 1) can also be set on the WLAN Security page.

Table 11. Security Setting

Profile Name	Enter a name for the profile. Default: Profile1	No encryption or authentication
SSID	Enter an SSID (network name) for the access point. Default: Wireless	
Broadcast SSID	Enable/disable broadcasting the SSID on the network. Default: Enable	
Max Station Number	The maximum number of clients allowed to connect to the access point.	
Encryption	**No encryption**	
	WEP	Data encryption and shared key
	WPA Enterprise WPA2 Enterprise WPA & WPA2 Enterprise	WPA-Enterprise Uses a RADIUS server for authentication.
	WPA-PSK WPA2-PSK WPA-PSK & WPA2-PSK	WPA-Personal/Pre-Shared Key Uses a password or passphrase for authentication.
Cipher	**None**	Can only be combined with **No encryption**
	64 bits WEP	Used with WEP authentication
	128 bits WEP	
	TKIP	Used with WPA-PSK authentication
	AES	Used with WPA2-PSK authentication
Key Type	Select hexadecimal or ASCII format for WEP keys. Default: Hex	
Default Key	Select the default key. Default: Key 1	
Key 1~4	Enter the encryption keys.	

5.8.4. Mesh Settings

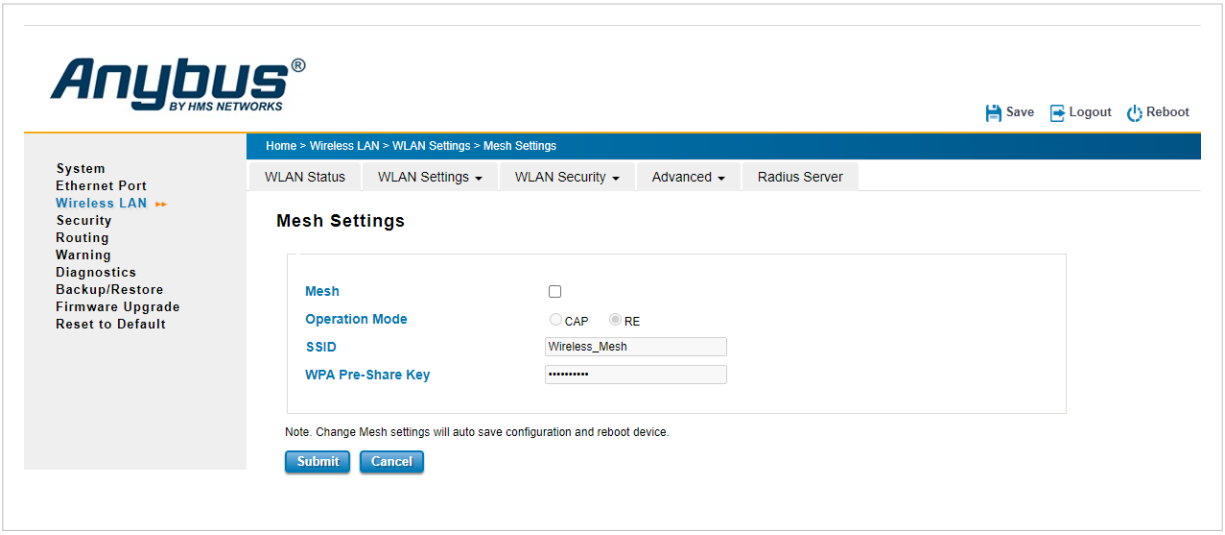


Figure 14. Mesh Settings

Mesh	To enable Mesh, select the checkbox.
Operation Mode	Select Operation Mode if the access point will work as a central AP (CAP; wired) or range extender (RE; wirelessly connected).
SSID	SSID of the mesh network. Default: Wireless_Mesh
WPA Pre-Shared Key	Uses a password or passphrase for authentication.

5.8.5. WLAN Security

The security settings on the WLAN Security page only apply to the default profile (Profile 1).

Encryption	**No encryption**	No encryption or authentication
	WEP	Data encryption and shared key
	WPA with RADIUS WPA2 with RADIUS WPA & WPA2 with RADIUS	WPA-Enterprise Uses a RADIUS server for authentication.
	WPA-PSK WPA2-PSK WPA-PSK & WPA2-PSK	WPA-Personal/Pre-Shared Key Uses a password or passphrase for authentication.
Cipher	**None**	Can only be combined with **No encryption**
	64 bits WEP	Used with WEP encryption
	128 bits WEP	
	TKIP	Used with WPA-PSK authentication
	AES	Used with WPA2-PSK authentication
Key Type	Select hexadecimal or ASCII format for WEP keys. Default: Hex	
Default Key	Select the default key. Default: Key 1	
Key 1~4	Enter the encryption keys.	

5.8.6. Advanced

IMPORTANT

Normally these settings are left at the default values. Incorrect settings may reduce performance or prevent communication with the device.

IMPORTANT

If only one antenna is used for WLAN, the antenna must be connected to **WLAN 1**.

A-MPDU/A-MSDU aggregation	Can improve performance in AP mode. Do not enable this function if the wireless clients do not support A-MPDU/A-MSDU aggregation.
Short GI	Short guard interval can improve the data rate. The guard interval is used to introduce immunity to propagation delays, echoes and reflections, to which digital data is normally very sensitive.
RTS Threshold	Threshold value for triggering a RTS/CTS handshake. Default: 2347 (bytes)
Fragment Threshold	The maximum size for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance. Default: 2346 (bytes)
Beacon Interval	The interval between broadcast packets. Default: 100 (ms)
DTIM Interval	The interval between Delivery Traffic Indication Messages. Default: 1 (frame)
Preamble Type	Preamble Type controls the additional data header strings that are used to check for data transmission errors. Default: Long
IGMP Snooping	IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the AP. IGMP Snooping provides the ability to limit multicast traffic so that it travels only to those end destinations that require that traffic. Default: Enable
Antenna Number	Select the number of antennas to use. This setting must be set to **One Antenna** if only a single antenna is used. Antenna 1 is active when **One Antenna** is selected. Default: Two Antenna

5.8.7. Radius Server

IP Address	IP address for the RADIUS server
Server Port	UDP port for the RADIUS server Default: 1812
Shared Key	Shared key for authentication

5.8.8. Certificate File (Client Mode)

Delete User Key	Delete the currently selected RADIUS server certificate
Upload User Key	Upload a certificate file from a specified file location

5.9. Security

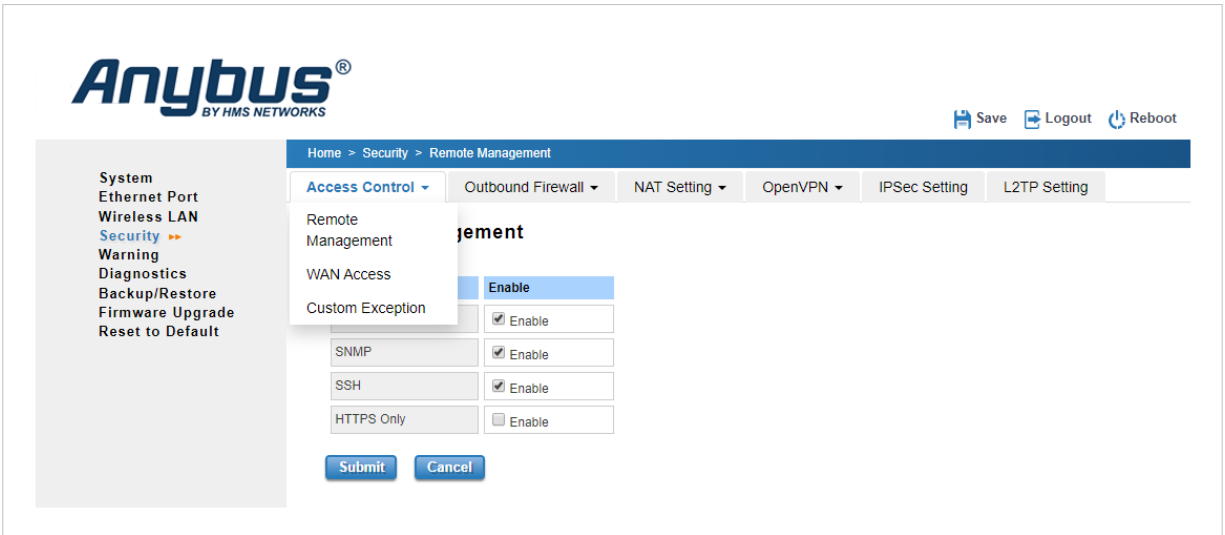


Figure 15. Security configuration page

5.9.1. Access Control

Table 12. Remote Management

Telnet	Allow remote login and configuration of the device using Telnet.
SNMP	Allow remote login and configuration of the device using SNMP.
SSH	Allow remote login and configuration of the device using SSH.
HTTPS Only	Require SSL/TLS encryption for access to the web configuration interface.

WAN Access

Access from the WAN can be enabled for Web (HTTP/HTTPS), Telnet, SSH and/or SNMP.

Custom Exception

Access to the configuration can be restricted to specific IP addresses and port ranges.

5.9.2. Outbound Firewall

Firewall rules for outbound traffic can be set up based on source and destination IP address, source port range, destination port range, and protocol (TCP/UDP).

5.9.3. NAT Setting

Port Forwarding	Check the box to enable port forwarding.
Public Port Range	Range of public TCP/UDP ports for this entry
IP Address	IP address that traffic on the public ports will be redirected to
Protocol	Allow only TCP or UDP packets, or both (default)
Port Range	Target port range
Comment	Enter a description of this entry (optional).

Table 13. DMZ

DMZ	Check the box to enable DMZ.
DMZ Host IP Address	IP address of the DMZ host

Table 14. N to 1 NAT

NAPT enable	To enable NAPT for WAN1 and/or WWAN, select the checkbox/checkboxes.
Port Mapping Policy	Reuse: Use the same port number when the same remote device re connect. Randomize: Change the port number randomly for each connection attempt. Default: Reuse

Table 15. 1 to 1 NAT

1 to 1 NAT	Check the box to enable 1 to 1 NAT
Local IP Address	Target IP Address
WAN IP Address	Incoming IP Address
Comment	Enter a description of this entry (optional).

5.9.4. OpenVPN

Table 16. OpenVPN Status

Enabled	OpenVPN enabled/disabled
Connection Status	OpenVPN connection status

Table 17. OpenVPN Client

Enable VPN Client	Check the box to enable VPN Client
Encryption Mode	Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Primary IP address of the VPN server
Server 2	Secondary IP Address of the VPN server
Port	VPN port number (1–65535) Default: 1194
Tunnel Protocol	Select TCP or UDP
Encryption Cipher	Select encryption cipher
Hash Algorithm	Select hash algorithm
ping-timer-rem	Prevents unnecessary restart of server/client on network failure. Default: Enable
persist-tun	Keep tun (layer 3) device linkup after keepalive timeout. Default: Enable
persist-key	Keep the first used key if VPN restarts after keepalive timeout. Default: Enable
LZO Compression	Uses compression of data to decrease the traffic (CPU intensive). Default: Disable
Keepalive	Detect connection status Default: Enable
Ping Interval	Interval between pings (1–99999 seconds). Default: 10
Retry Timeout	Time between retries after failed ping (1–99999 seconds). Default: 60
nobind	When enabled, source ports will be assigned randomly.
ifconfig	Local/remote IP addresses for the VPN tunnel
Route	Route IP address and netmask. This is the target IP domain that can be accessed through the VPN tunnel.
Save Log File	Click **Save...** to save the VPN Client Log.

Table 18. OpenVPN Server

Enable VPN Server	Check the box to enable VPN Server
Encryption Mode	Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Primary IP address of the VPN server
Server 2	Secondary IP Address of the VPN server
Port	VPN port number (1–65535) Default: 1194
Tunnel Protocol	Select TCP or UDP
Encryption Cipher	Select encryption cipher
Hash Algorithm	Select hash algorithm
ping-timer-rem	Prevents unnecessary restart of server/client on network failure. Default: Enable
persist-tun	Keep tun (layer 3) device linkup after keepalive timeout. Default: Enable
persist-key	Keep the first used key if VPN restarts after keepalive timeout. Default: Enable
LZO Compression	Uses compression of data to decrease the traffic (CPU intensive). Default: Disable
Keepalive	Detect connection status Default: Enable
Ping Interval	Interval between pings (1–99999 seconds). Default: 10
Retry Timeout	Time between retries after failed ping (1–99999 seconds). Default: 60
ifconfig	Local/remote IP addresses for the VPN tunnel
Route	Route IP address and netmask. This is the target IP domain that can be accessed through the VPN tunnel.
Save Log File	Click **Save...** to save the VPN Server Log.

Table 19. OpenVPN User

User name	Set up a username for an OpenVPN user.

Password/confirm password	Set up a password for an OpenVPN user.
Remote Network	IP address of the remote network.
Remote Netmask	Subnet mask of the remote network.

To edit an existing OpenVPN profile, select the profile checkbox and click **Edit**.

Table 20. OpenVPN Certificate

Delete VPN Key	Delete the selected certificate.
Upload VPN Key	Upload a certificate file from a specified file location
Generate TLS keys	To create TLS keys, click Generat. The TLS keys encrypts data sent between the TLS client and server.
Generate Static Key	To create static key for data encryption, click Generat. A static key is used more than once over a long period of time.
Download CA	To download a certification authority (CA) for authentication of the CA signature on the server certificate, click Download.
Download Client Cert	To download a client certificate, click Download. The client certificate is used by client systems to make authenticated requests to a remote server.
Download Client Key	To download a client key for authentication of client identity, click Download.
Download Static Key	To download a static key for data encryption, click Download.

5.9.5. IPSec Setting

Enable IPsec	Check the box to enable IPsec
IPsec Status	IPsec connection status.
Exchange Mode	Select Main or Aggressive mode
Authentication Method	Default: PSK
Pre-shared key	Default: No default key
IPsec Cipher Suites	Default: AES128-SHA1-DH2
Local IP	IP Address of the local side of the tunnel. Use 0.0.0.0 if WAN uses DHCP.
Local Subnet	IPsec local protected subnet/netmask. Example: 192.168.10.0/24
Remote Host	IP adress of the IPsec remote host. Use 0.0.0.0 if remote host uses DHCP
Remote Subnet	IPsec remote protected subnet/netmask. Example: 192.168.10.0/24

5.9.6. L2TP Setting

L2TP Server	To enable L2TP Server, select the checkbox.
Local IP Address	Local virtual IP address of the L2TP server.
Offered IP Range	Enter the start and end IP address of the L2TP client IP address range.

Table 21. Authentication

Authentication Method	PAP/CHAP selectable

Table 22. User

User Name	Enter a new user name here.
Password	Enter a new password here.

5.10. Warning

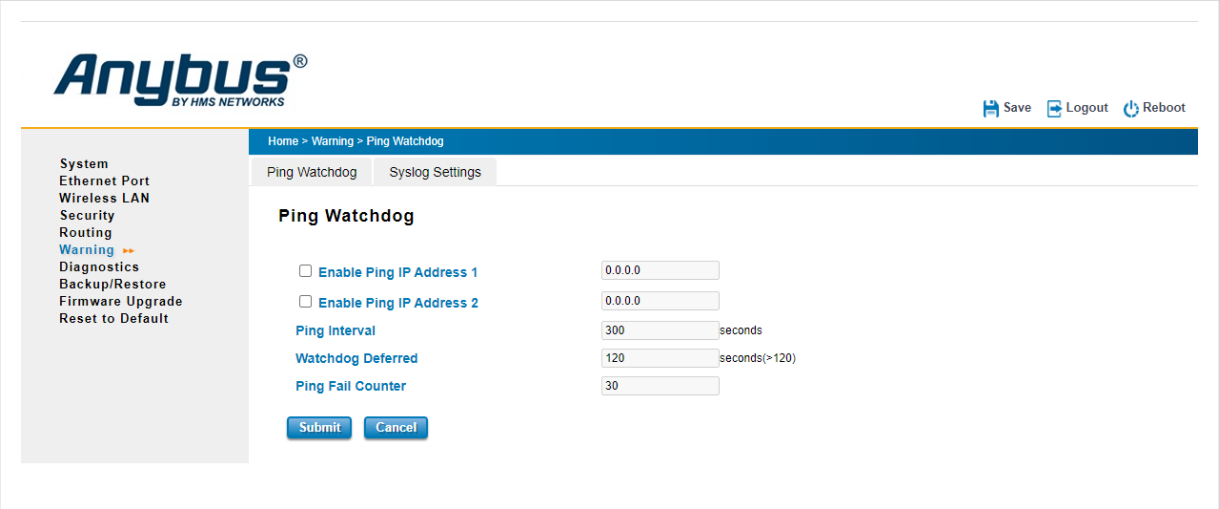


Figure 16. Warning configuration page

5.10.1. Ping Watchdog

The Access Point can be configured to regularly ping another device on the network.

If the remote device is not reachable, the access point will reboot.

Enable Ping IP Address	Two IP addresses can be set up as targets. The Access Point will send a ping command to each of them at the interval configured below.
Ping Interval	The interval between each ping. Default: 300 (seconds)
Watchdog Deferred	The delay before the Access Point reboots after the number of failed pings have been reached. Default: 120 (seconds)
Ping Fail Counter	The number of consecutive failed pings that will indicate a lost connection. Default: 30

5.10.2. Syslog Setting

Enable Remote Syslog Server	Check the box to enable sending system logs to a syslog server on the network.
IP Address	The IP address of the syslog server.
Port	The port number of the syslog server Default: 514

5.11. Diagnostics

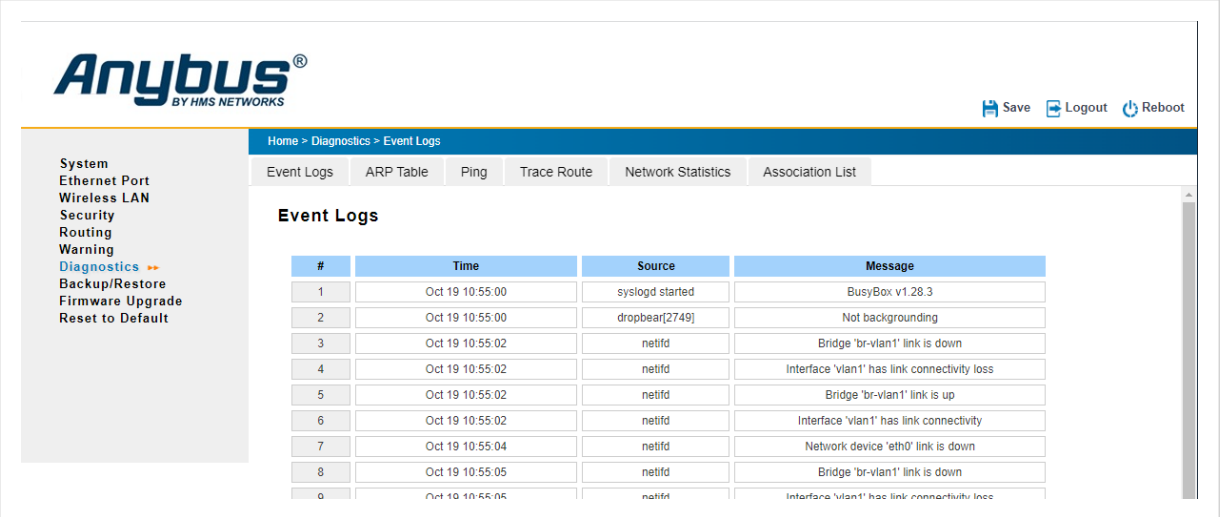


Figure 17. Diagnostics configuration page

5.11.1. Event Logs

#	Index
Time	Event time (uses the date/time setting of the Anybus Industrial WLAN Access Point)
Source	Event source
Message	Event message

5.11.2. ARP Table

This page shows the active ARP table for the Access Point.

The ARP table contains recently cached MAC addresses of devices that have been communicating with the access point.

5.11.3. Ping

Can be used to test connectivity by sending ping packets to a remote host.

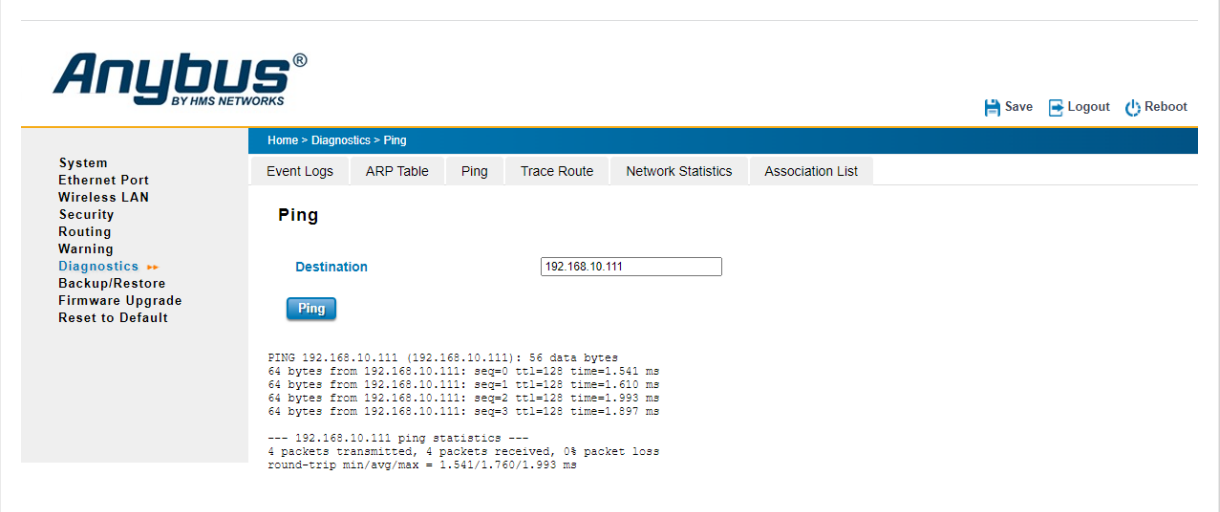


Figure 18. Ping tool

5.11.4. Trace Route

Can be used to diagnose the connection to a remote host using the traceroute command.

5.11.5. Network Statistics

Statistics for transmitted and received packets on the WLAN interface/cellular interface.

5.11.6. Association List

Shows the status of connected wireless clients when the access point is in Access Point mode.

SSID	The SSID used by the client
MAC Address	The MAC Address of the client
Signal Strength	Connection signal strength
Noise Floor	Background noise level
Connection Time	The time when the client connected to the AP
Last IP	The IP Address of the client.
Action	Select **kick** to immediately disconnect the client.

5.12. Backup/Restore

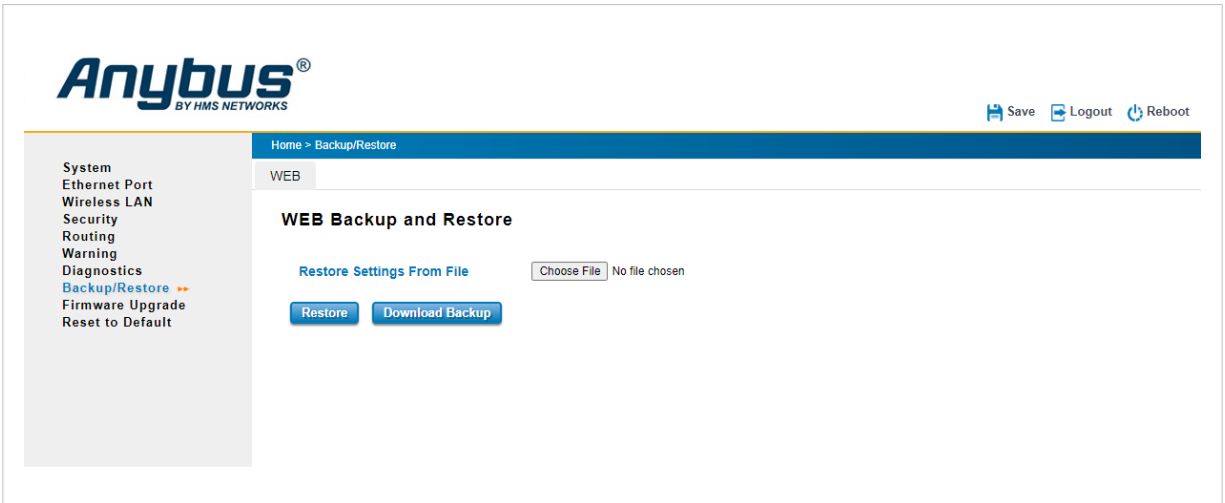


Figure 19. Backup/Restore page

The configuration settings can be saved and restored over the current network connection (WEB).

After restoring a configuration, you will be asked to log in to the access point again.

5.12.1. WEB Backup and Restore

To save the current configuration:

1. Click on **Download Backup** to open a file dialog.
2. Click on Save to save the configuration to a location on your computer.

To restore a saved configuration:

1. Click on **Choose file** to open a file dialog.
2. Select the configuration file and click on **Open**.
3. Click on **Restore** to apply the configuration.

5.13. Firmware Upgrade

IMPORTANT
Do not disconnect the Access Point while the upgrade procedure is running.

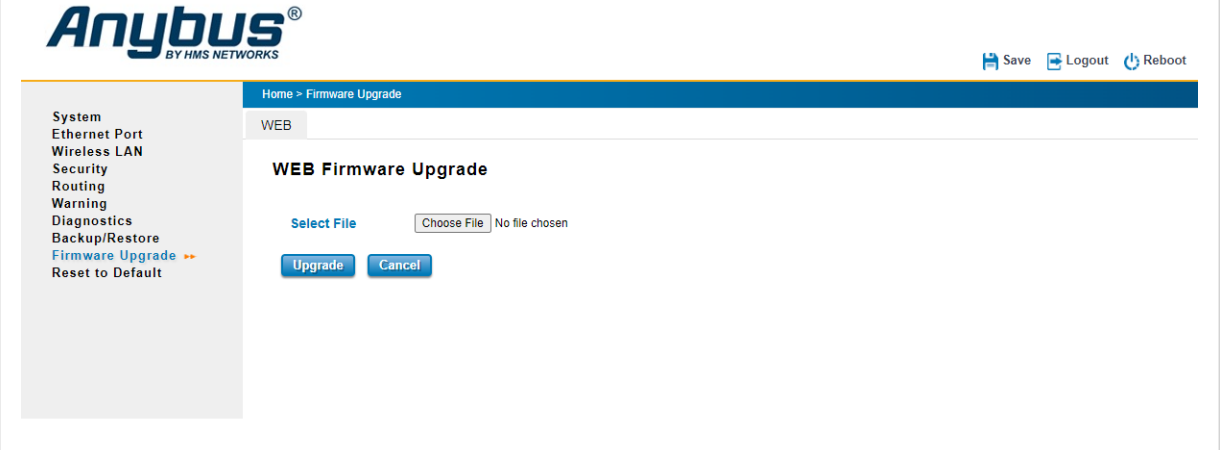


Figure 20. Firmware Upgrade page

The firmware of the Access Point can be upgraded over the current network connection (WEB).

The latest firmware can be downloaded from www.anybus.com/support.

5.13.1. WEB Firmware Upgrade

1. Click on **Choose file** to open a file dialog.
2. Select the firmware file and click on **Open**.
3. Click on **Upgrade** to start the firmware upgrade procedure.
   The Anybus Industrial WLAN Access Point will reboot automatically when the upgrade procedure has finished.

5.14. Reset to Default

IMPORTANT
The IP address of the access point will be reset to the default address 192.168.10.1.

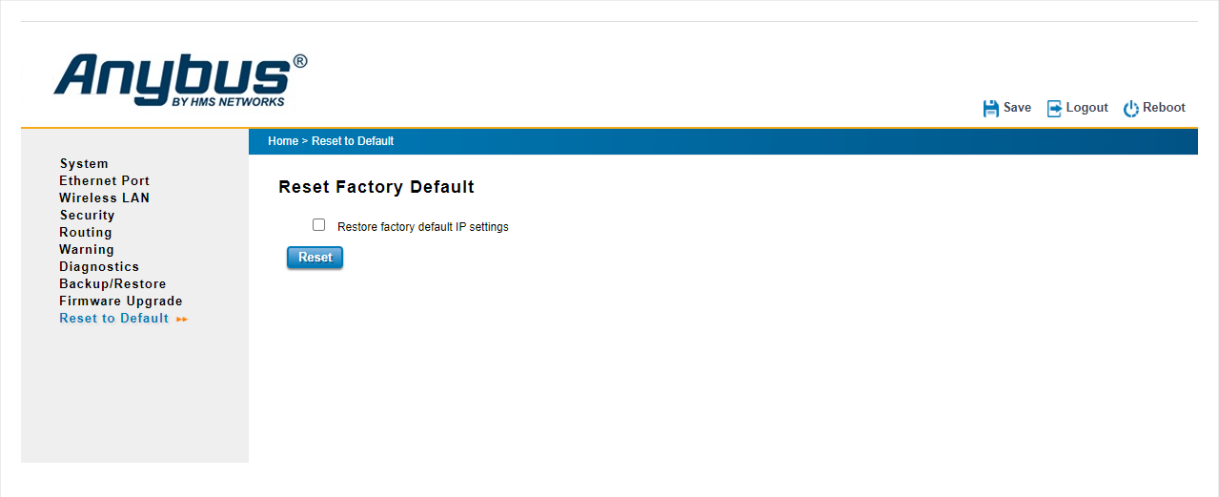


Figure 21. Factory Reset page

Click on **Reset** to restore the factory settings. The current IP settings will be kept if the box Restore factory default IP setting is unchecked.

6. Verify Operation

6.1. Front Panel LED

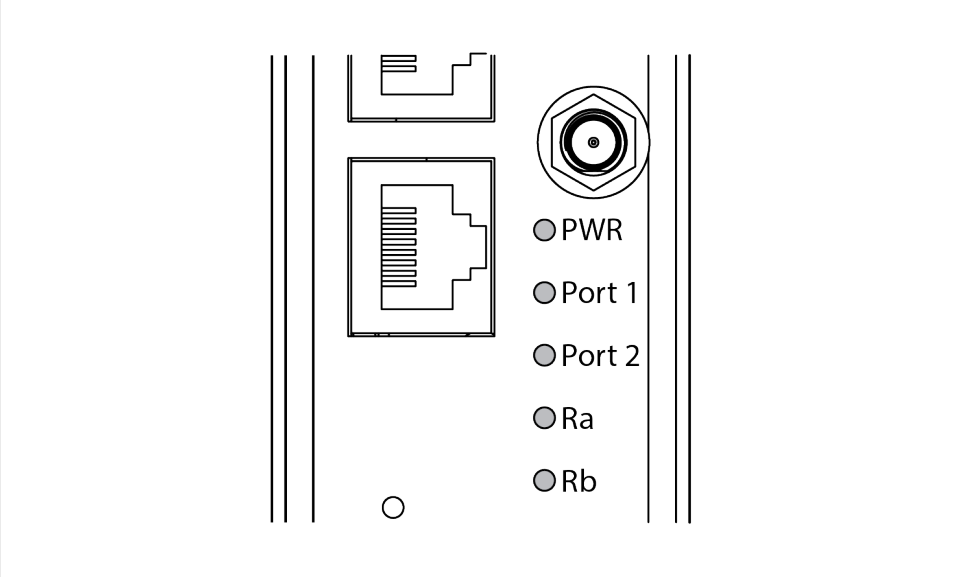


Figure 22. Front Panel LED

Table 23. Front Panel LED status indications

LED	Status	Description
PWR	Green On	DC-IN Power is On
	Off	No Power in DC-IN
Port 1-2	Green On	Link is established
	Green Blinking	Packets transmitting/receiving
	Off	Link is inactive
Ra 2.4 GHz Radio LED	Green On	AP: Radio enabled Mesh: Mesh enabled
	Green Blinking	AP: STA connected Mesh: Uplink is active
	Off	AP: STA disconnected, radio disabled Mesh: No signal
Rb 5 GHz Radio LED	Green On	AP: Radio enabled Mesh: Signal is strong
	Green Blinking	AP: STA connected Mesh: Signal is weak
	Off	AP: STA disconnected, radio disabled Mesh: No signal

7. Technical Data

7.1. Technical Specifications

Order code	AWB5141 WLAN AP, IP30, with mesh
Ethernet connector	RJ45
Power supply	10-60 VDC (terminal block) or IEEE 802.3af (48 VDC PoE) Max. 11.5 W
WLAN 2.4 GHz	Maximum RF transmitted power: IEEE 802.11b: 21 ±2 dBm IEEE 802.11g: 22 ±2 dBm IEEE 802.11n: 21 ±2 dBm
WLAN 5 GHz	Maximum RF transmitted power: IEEE 802.11a: 21.5 ±2 dBm IEEE 802.11an: 21.5 ±2 dBm IEEE 802.11ac: 21.5 ±2 dBm
Dimensions	200 x 51 x 126 mm (W x H x D) without DIN mounting clip
Weight	660 g
Housing material	Metal
IP protection class	IP30
Mounting	DIN rail mount
Operating temperature	-40 °C to 70 °C, 5–95 % RH non-condensing

Additional technical data and information related to the installation and use of this product can be found at www.anybus.com/support.

8. Reference Guides

8.1. Wireless Technology Basics

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

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

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

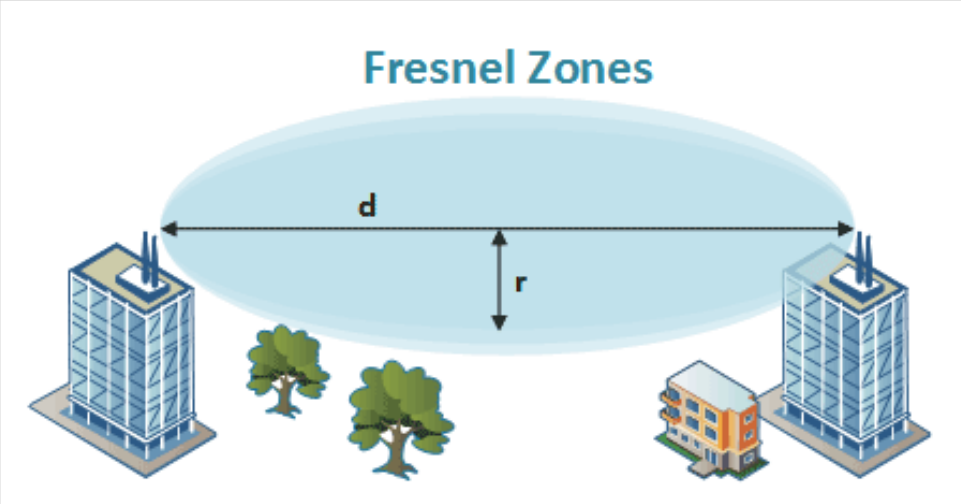


Figure 23. Fresnel zones

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.

This page is intentionally left blank.

This page is intentionally left blank.

This page is intentionally left blank.