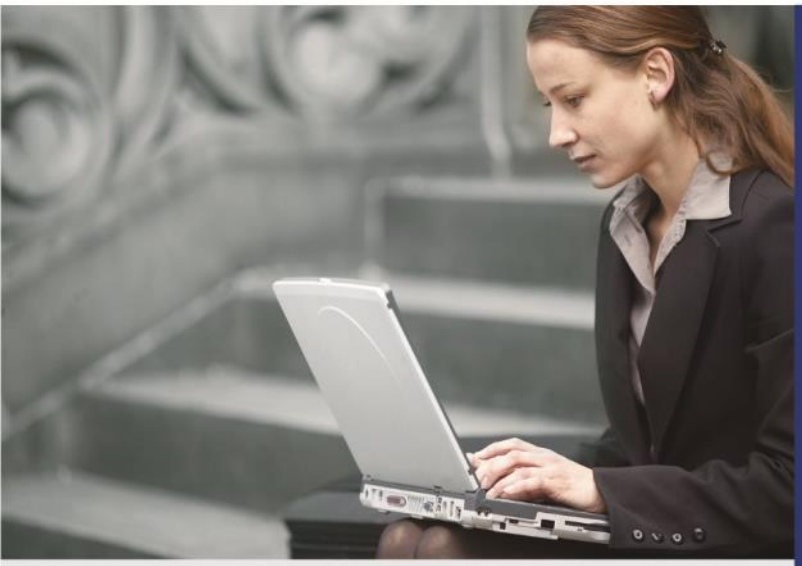
PLANET
Networking & Communication

User's Manual

Industrial 802.11ax Wireless Access Point with 5 10/100/1000T LAN Ports

► **IAP-1800AX & IAP-2400AX**



Copyright

The products and programs described in this User's Manual are licensed products of PLANET Technology, This User's Manual contains proprietary information protected by copyright, and this User's Manual and all accompanying hardware, software, and documentation are copyrighted.

No part of this User's Manual may be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form by any means, electronic or mechanical including photocopying, recording, or information storage and retrieval systems, for any purpose other than the purchaser's personal use, and without the prior express written permission of PLANET Technology.

Disclaimer

PLANET Technology does not warrant that the hardware will work properly in all environments and applications, and makes no warranty and representation, either implied or expressed, with respect to the quality, performance, merchantability, or fitness for a particular purpose.

PLANET has made every effort to ensure that this User's Manual is accurate; PLANET disclaims liability for any inaccuracies or omissions that may have occurred. Information in this User's Manual is subject to change without notice and does not represent a commitment on the part of PLANET. PLANET assumes no responsibility for any inaccuracies that may be contained in this User's Manual. PLANET makes no commitment to update or keep current the information in this User's Manual, and reserves the right to make improvements and/or changes to this User's Manual at any time without notice.

If you find information in this manual that is incorrect, misleading, or incomplete, we would appreciate your comments and suggestions.

Federal Communication Commission Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution:

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. To assure continued compliance, for example, use only shielded interface cables when connecting to computer or peripheral devices.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference
(2) This device must accept any interference received, including interference that may cause undesired operation.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHzHz band are restricted to indoor usage only.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20 cm (8 inches) during normal operation.

CE Compliance Statement

This device meets the RED 2014/53/EU requirements on the limitation of exposure of the general public to electromagnetic fields by way of health protection. The device complies with RF specifications when it is used at a safe distance of 20 cm from your body.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

WEEE regulation

To avoid the potential effects on the environment and human health as a result of the presence of hazardous substances in electrical and electronic equipment, end users of electrical and electronic equipment should understand the meaning of the crossed-out wheeled bin symbol. Do not dispose of WEEE as unsorted municipal waste and have to collect such WEEE separately.

Revision

User's Manual of PLANET Industrial 802.11ax Wireless Access Point with 5 10/100/1000T LAN Ports

Models: IAP-1800AX/IAP-2400AX

Rev.: 1.0 (July, 2022)

Part No. EM-IAP-1800AX_IAP-2400AX_v1.0

Table of Contents

Chapter 1. Product Introduction

Thank you for purchasing PLANET Industrial 802.11ax Wireless Access Point with 5 10/100/1000T LAN Ports, IAP-1800AX and IAP-2400AX. The descriptions of these models are as follows:

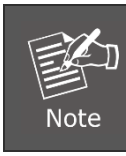
IAP-1800AX	Industrial Dual Band 802.11ax 1800Mbps Wireless Access Point with 5 10/100/1000T LAN Ports
IAP-2400AX	Industrial 5GHz 802.11ax 2400Mbps Wireless Access Point with 5 10/100/1000T LAN Ports

"**Industrial 802.11ax Wireless AP**" mentioned in the manual refers to the above models.

1.1 Package Contents

The package should contain the following:

Model / Item	IAP-1800AX	IAP-2400AX
Industrial 802.11ax Wireless AP	x 1	x 1
Quick Installation Guide	x 1	x 1
PLANET CloudViewer Quick Guide	x 1	x 1
Wall-mount Kit	x 1	x 1
Dual band Wi-Fi Antenna	x 2	x 4
Antenna Dust Cap	x 2	x 4
RJ45 Dust Cap	x 5	x 5



If any item is found missing or damaged, please contact your local reseller for replacement.

1.2 Product Overview

Ultra-high-speed Wi-Fi-6 Wireless LAN Solution with Environmentally Hardened Design

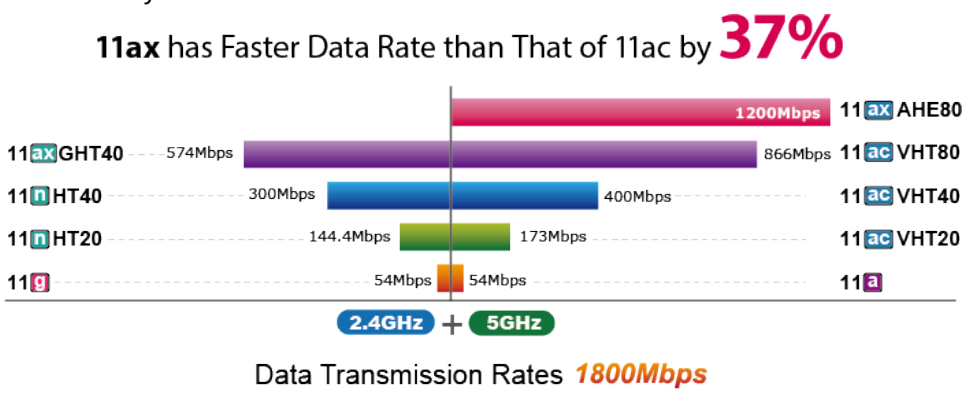
PLANET **IAP-1800AX Industrial Dual Band 802.11ax 1800Mbps Wireless Access Point with 5 10/100/1000T LAN Ports** is equipped with a rugged IP30 metal case for stable operation in heavy industrial environments. Thus, the IAP-1800AX**,** supporting **MU-MIMO, OFDMA, Seamless Roaming, Beamforming and BSS Coloring technology,** also provides a maximum wireless speed of **1200Mbps** in the 5GHz band and **600Mbps** in the 2.4GHz band. The maximum number of client users is up to 150, ensuring more secure and robust connectivity with the adoption of Wi-Fi 6 technology.

PLANET **IAP-2400AX Industrial 5GHz 802.11ax 2400Mbps Wireless Access Point with 5 10/100/1000T LAN Ports** is equipped with a rugged IP30 metal case for stable operation in heavy industrial environments. The IAP-2400AX supporting **MU-MIMO, OFDMA, Seamless Roaming, Beamforming and BSS Coloring** provides a maximum wireless speed of **2400Mbps** in the 5GHz band. The maximum number of client users is up to 150, ensuring more secure and robust connectivity with the adoption of Wi-Fi 6 technology.

As the IAP-1800AX/IAP-2400AX is able to operate under wide temperature range from -40 to 75 degrees C, it can be placed in almost any difficult environment. The IAP-1800AX/IAP-2400AX also allows either DIN rail or wall mounting for efficient use of cabinet space.

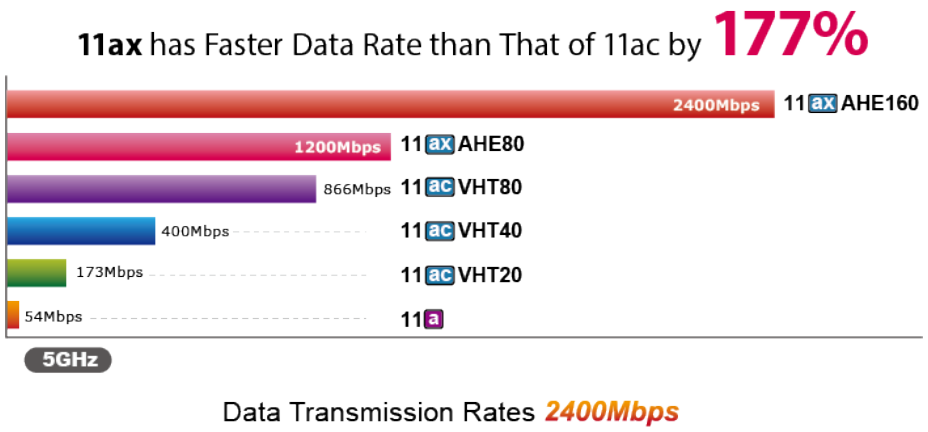
Super Power Dual Band WLAN Solution

The IAP-1800AX, adopting the IEEE 802.11ax Wi-Fi 6 standard, provides a high-speed transmission. The maximum wireless speed in 2.4GHz band is up to 11AXG_GHE40 of 574Mbps, and in the 5GHz band is up to 11AXA_AHE80 of 1201Mbps. Both the **2.4GHz and 5GHz** wireless connections can also be used simultaneously.



Super Power and Reliable 5GHz WLAN Solution

The IAP-2400AX, adopting the IEEE 802.11ax Wi-Fi 6 standard, provides a high-speed transmission. The maximum wireless speed in the 5GHz band is up to 11AXA_AHE80 of 1201Mbps.



Benefits of MU-MIMO, OFDMA, Seamless Roaming, Beamforming and BSS Coloring

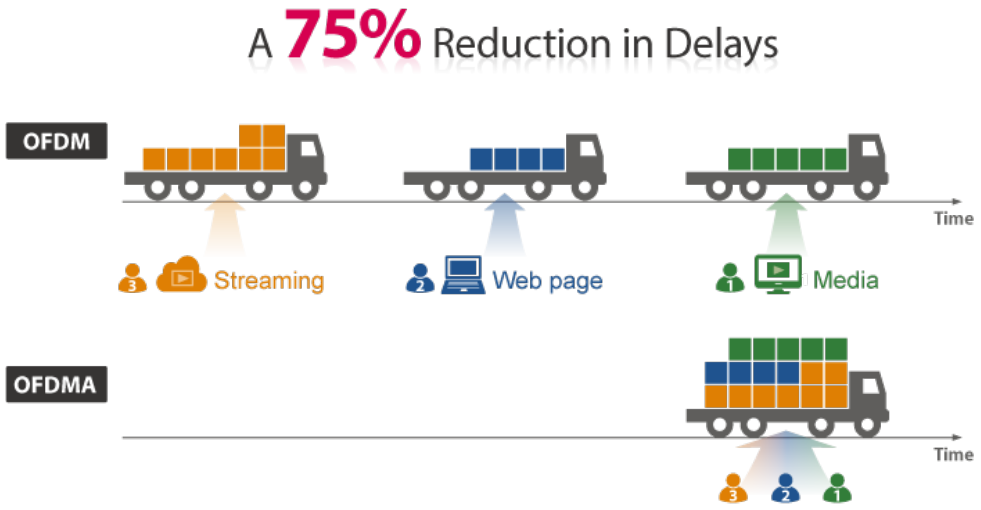
The IAP-1800AX/IAP-2400AX can be installed in public areas such as hotspots, airports and conferences as OFDMA, a multi-user version of OFDM, enables the concurrent AP to communicate (uplink and downlink) with multiple clients by assigning subsets of subcarriers called resource units (RUs) to the individual clients. With **MU-MIMO** and Seamless Roaming technologies, it provides a better Wi-Fi user experience, reducing the likelihood of users turning off Wi-Fi and putting more load on the cellular network. Beamforming is to improve your Wi-Fi signal when you are far away from your

Industrial 802.11ax Wireless AP. The **BSS color** is a numerical identifier of the BSS. 802.11ax radios are able to differentiate between BSSs using BSS color identifier when other radios transmit on the same channel.

These technologies also can solve Wi-Fi congestion issues in open work spaces and conference rooms. The IAP-1800AX/IAP-2400AX can offer more powerful throughput coverage of up to 150 client users.

■ **OFDMA (Orthogonal Frequency Division Multiple Access) Benefits**

- Helps transmit small and large packets together to reduce bandwidth burden and improve data transmission performance
- Transmitting data at the same time can effectively reduce the transmission delay for longer frame and low-speed transmission.
- Improves the overall traffic quality, and effectively uses bandwidth in an environment where multiple people use the Internet.
- Increases the number of devices that can be connected to the AP.
- Reduces the power consumption of the device by way of the use of low bandwidth.



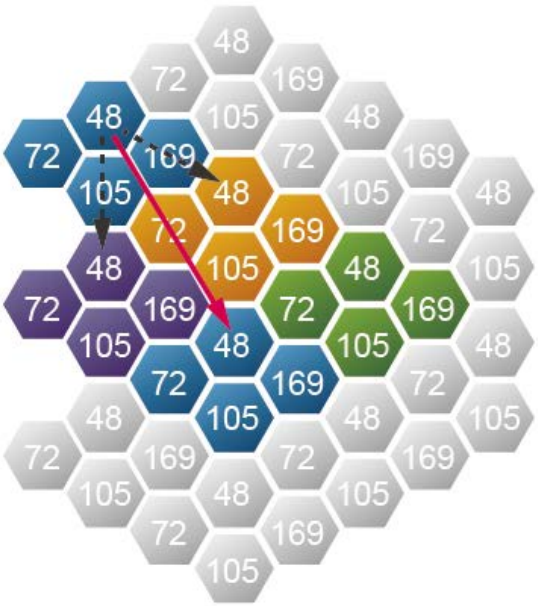
■ **Beamforming**

Beamforming is to improve your Wi-Fi signal when you are far away from your Industrial 802.11ax Wireless AP. When you use beamforming, Wi-Fi beamforming narrows the focus of that Industrial 802.11ax Wireless AP signal, sending it directly to your devices in a straight line, thus minimizing surrounding signal interference and increasing the strength of the signal that ultimately bring you the following benefits:

- Extend your Wi-Fi coverage
- Deliver a more stable Wi-Fi connection
- Deliver better Wi-Fi throughput
- Reduce Industrial 802.11ax Wireless AP interference

■ **BSS Coloring**

The BSS color is a numerical identifier of the BSS. 802.11ax radios are able to differentiate between BSSs using BSS color identifier when other radios transmit on the same channel. If the color is the same, this is considered to be an intra-BSS frame transmission. In other words, the transmitting radio belongs to the same BSS as the receiver. If the detected frame has a different BSS color from its own, then the STA considers that frame as an inter-BSS frame from an overlapping BSS.



WPA3 Next Generation Security for Your WLAN Solution

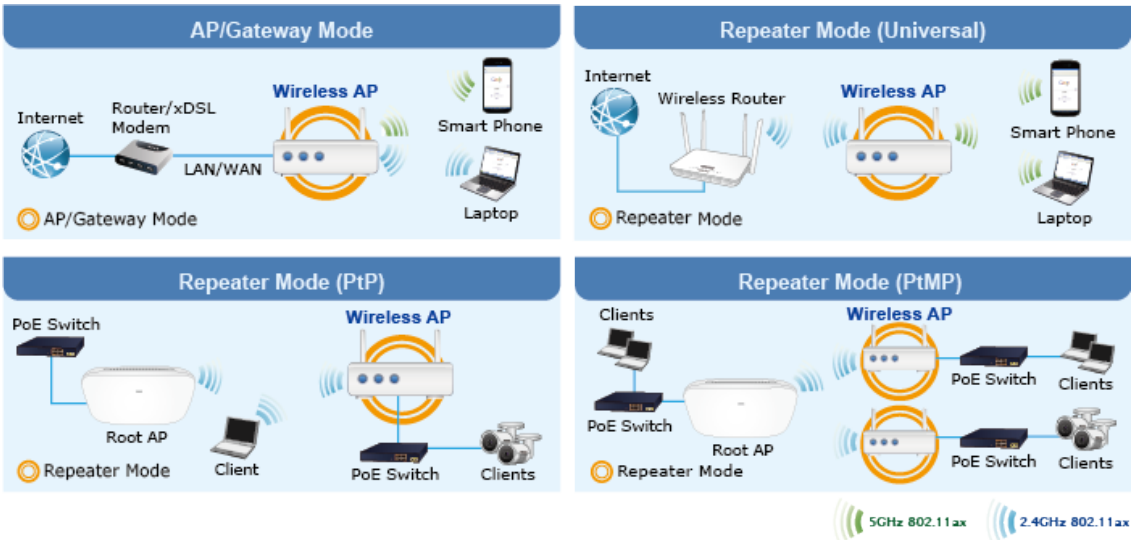
The WPA3 is the next generation Wi-Fi security technology that provides the most advanced security protocol to the market. WPA3 makes your connection more secure by preventing hackers from easily cracking your password no matter how simplified the password is. WPA3 can also provide more reliable password-based authentication, so it can better protect the security of individual users.

Advanced Security and Rigorous Authentication

The IAP-1800AX/IAP-2400AX supports WPA/WPA2/WPA3 wireless encryptions, suitable for the WPA2 Enterprise and WPA/WPA2 Enterprise where eavesdropping and unauthorized users or bandwidth occupied by unauthenticated wireless access can be effectively prevented. Furthermore, granting or denying access to the wireless LAN network based on the ACL (Access Control List) to any users can be pre-established by the administrator.

Multiple Operation Modes for Various Applications

The unit supports the simplified usage modes of AP and Gateway, through which they provide more flexibility for users when wireless network is established. Compared with general wireless access points, the IAP-1800AX/IAP-2400AX offers more powerful and flexible capability for wireless clients.



Optimized Efficiency in AP Management

The brand-new GUI configuration wizard helps the system administrator easily set up the IAP-1800AX/IAP-2400AX step by step. Besides, the built-in Wi-Fi analyzer provides real-time channel utilization to prevent channel overlapping to assure greater performance. With the automatic transmission power mechanism, distance control and scheduling reboot setting, the IAP-1800AX/IAP-2400AX is easy for the administrator to deploy and manage without on-site maintenance. Moreover, you can use PLANET NMS-500 or NMS-1000V AP control function to deliver wireless profiles to multiple APs simultaneously, thus making the central management simple.

Cybersecurity Network Solution to Minimize Security Risks

The IAP-1800AX/IAP-2400AX supports TLS protocols to provide strong protection against advanced threats. It includes a cybersecurity feature such as **SNMPv3** authentication, and so on to complement it as a security solution

User-friendly and Secure Management

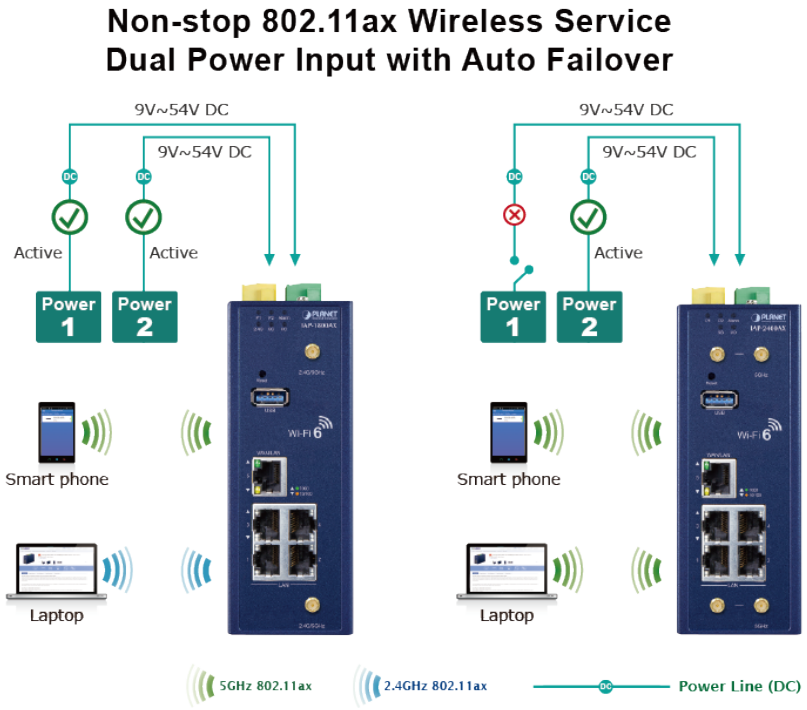
For efficient management, the IAP-1800AX/IAP-2400AX is equipped with Web and SNMP management interfaces.

- With the built-in **Web-based** management interface, the IAP-1800AX/IAP-2400AX offers an easy-to-use, platform-independent management and configuration facility.
- By supporting the standard SNMP protocol, the switch can be managed via any SNMP-based management software.

Moreover, the IAP-1800AX/IAP-2400AX offers secure remote management by supporting **TLSv1.3 protocols** and **SNMP v3** connections which encrypt the packet content at each session.

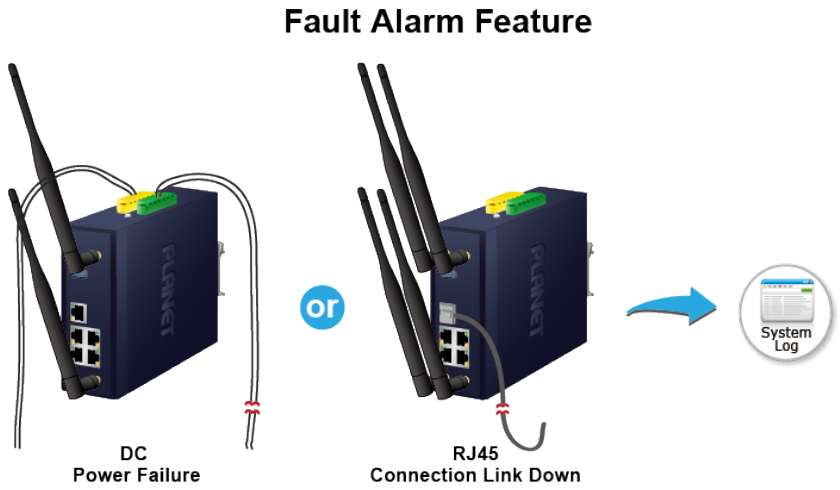
Dual Power Input for High Availability Network System

The IAP-1800AX/IAP-2400AX features a strong dual power input system with wide-ranging voltages (9V~54V DC) incorporated into customer's automation network to enhance system reliability and uptime. In the example below, when power supply 1 fails to work, the hardware failover function will be activated automatically to keep powering the IAP-1800AX/IAP-2400AX via power supply 2 alternatively without any loss of operation.



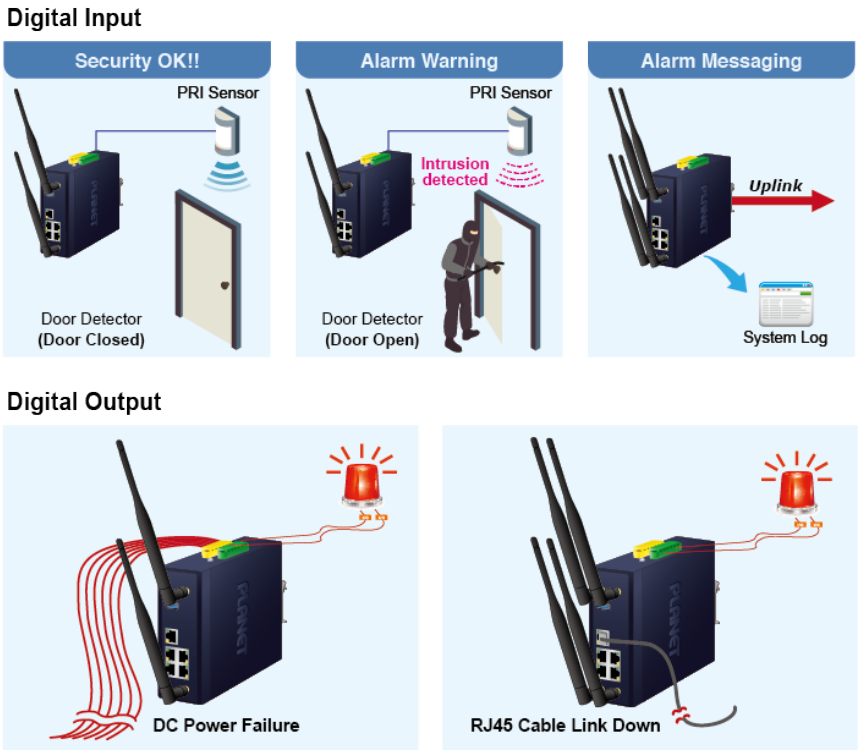
Effective Alarm Alert for Better Protection

The IAP-1800AX/IAP-2400AX supports a Fault Alarm feature which can alert the users when there is something wrong with the device. With this ideal feature, the users would not have to waste time finding where the issue is. It will help to save time and human resource.



Digital Input and Digital Output for External Alarm

The IAP-1800AX/IAP-2400AX supports Digital Input and Digital Output on its upper panel. This external alarm enables users to use Digital Input to detect and log external device status (such as door intrusion detector), and send event alarm to the administrators. The Digital Output could be used to alarm the administrators if the IAP-1800AX/IAP-2400AX port shows link down, link up or power failure.



Flexible and Easy Installation with Limited Space

The compact-sized IAP-1800AX/IAP-2400AX is specially designed to be installed in a narrow environment, such as a wall enclosure. It can be installed by fixed wall mounting or DIN rail, thereby making its usability more flexible and easier in any space-limited location.

* The above pictures are for illustration only.

1.3 Product Features

- **IAP-1800AX Physical Interfaces**
  - 4 x 10/100/1000BASE-T RJ45 LAN ports, auto-negotiation, auto MDI/MDI-X (Port 1 to Port 4)
  - 1 x 10/100/1000BASE-T RJ45 WAN/LAN port, auto-negotiation, auto MDI/MDI-X (Port 5)
  - 2 x dual-band (2.4GHz/5GHz) RP-SMA connectors with antennas
  - 1 USB 3.0 port for system configuration backup/upload and firmware upgrade
  - 1 x reset button for system factory default and reboot

- **IAP-2400AX Physical Interfaces**
  - 4 x 10/100/1000BASE-T RJ45 LAN ports, auto-negotiation, auto MDI/MDI-X (Port 1 to Port 4)
  - 1 x 10/100/1000BASE-T RJ45 WAN/LAN port, auto-negotiation, auto MDI/MDI-X (Port 5)
  - 4 x 5GHz band RP-SMA connectors with antennas
  - 1 USB 3.0 port for system configuration backup/upload and firmware upgrade
  - 1 x reset button for system factory default and reboot

- **LAN Port**
  - Hardware-based 10/100Mbps, half/full duplex and 1000Mbps full duplex mode, flow control and auto-negotiation, and auto MDI/MDI-X
  - Features Store-and-Forward mode with wire-speed filtering and forwarding rates
  - IEEE 802.3x flow control for full duplex operation and back pressure for half duplex operation
  - 10K jumbo frame
  - Automatic address learning and address aging

- **Industrial Case and Installation**
  - IP30 metal case protection
  - DIN-rail or wall-mount design
  - DC 9-54V, redundant power with reverse polarity protection
  - -40 to 75 degrees C operating temperature

- **Digital Input and Digital Output**
  - 2 Digital Input (DI)
  - 2 Digital Output (DO)
  - Integrate sensors into auto alarm system

- **Multiple Operation Modes Options**
  - Multiple operation modes: AP/Repeater and Gateway mode options

- **Industrial Compliant Wireless LAN**
  - Compliant with the IEEE 802.11a/b/g/n/an/ac/ax wireless technology(IAP-1800AX)
  - Compliant with the IEEE 802.11a/an/ac/ax wireless technology(IAP-2400AX)
- **IAP-1800AX RF Interface Characteristics**
  - 802.11ax 2T2R architecture with data rate of up to 1800Mbps (600Mbps in 2.4GHz and 1200Mbps in 5GHz)
  - High output power with multiply-adjustable transmit power control
- **IAP-2400AX RF Interface Characteristics**
  - 802.11ax 4T4R architecture with data rate of up to 2400Mbps (in 5GHz)
  - High output power with multiply-adjustable transmit power control
- **Secure Wireless Connection Features**
  - Full encryption supported: WPA3 Personal,WPA2/WPA3 Personal,WPA2 Personal (AES) ,WPA2 Personal (TKIP),WPA2 Personal (TKIP+AES),WPA/WPA2 Personal (AES) ,WPA/WPA2 Personal (TKIP) , WPA/WPA2 Personal (TKIP+AES) , WPA2 Enterprise, WPA/WPA2 Enterprise
  - MAC ACL
- **Wireless AP Mode Features**
  - Supports OFDMA (orthogonal frequency division multiple access)
  - Supports MU-MIMO (multi-user multiple-input multiple-output), Beamforming and BSS Coloring
  - WMM (Wi-Fi multimedia) provides higher priority to multimedia transmitting over wireless
  - Coverage threshold to limit the weak signal of clients occupying session
  - Real-time Wi-Fi channel analysis chart and client limit control for better performance
  - Terminal Seamless Roaming with 802.11k, 802.11v, and 802.11r
- **Gateway Mode Features**
  - Built-in RADIUS server/Client
  - Captive Portal
  - UPnP
  - IP routing protocol supports RIPv1/v2, OSPF
  - PLANET DDNS/Easy DDNS
  - SPI firewall, DDoS block, system security and NAT ALGs
  - MAC address/IP/Web filtering and QoS
  - DMZ and port forwarding
- **Easy Deployment and Management**
  - Supports PLANET AP Controllers in AP mode
  - Self-healing mechanism through system auto reboot setting

- System status monitoring through remote syslog server
- Gateway mode supports PLANET DDNS/Easy DDNS, Captive Portal, RADIUS Server/Client
- PLANET Smart Discovery Utility for deployment management
- PLANET NMS system and CloudViewer for deployment management

1.4 Product Specifications

■ IAP-1800AX

Product	IAP-1800AX	IAP-2400AX
Hardware Specifications		
Interfaces	5 10/100/1000BASE-T RJ45 Ethernet ports including 4 LAN ports (Ports 1 to 4) 1 WAN/LAN port (Port 5)	
Wireless Connector	Built-in two RP-SMA female connectors	Built-in four RP-SMA female connectors
USB Port	1 USB 3.0 port	
DI & DO Interfaces	2 Digital Input (DI): Level 0: -24V~2.1V (±0.1V) Level 1: 2.1V~24V (±0.1V) Input Load to 24V DC, 10mA max. 2 Digital Output (DO): Open collector to 24V DC, 100mA max.	
Connector	Removable 6-pin terminal block for power input Pin 1/2 for Power 1, Pin 3/4 for fault alarm, Pin 5/6 for Power 2	
Reset Button	< 5 sec: System reboot > 10 sec: Factory default	
Enclosure	IP30 metal case	
Dimensions (W x D x H)	50 x 135 x 135 mm	
Weight	773g	787g
Power Requirements – DC	9~54V DC, 1.8A	
Power Consumption	Max. 6.4 watts/ 21BTU (No Loading at DC 54V) Max.10.8 watts/ 36BTU (Full loading at DC 54V)	Max. 5.9 watts/ 20BTU (No Loading at DC 54V) Max.10.8 watts/ 36BTU (Full loading at DC 54V)
Installation	DIN-rail, desktop, wall-mounting	
LED Indicators	**System:** P1 (Green) P2 (Green) Alarm (Red) I/O (Red) **Ethernet Interfaces (Ports 1-4 LAN Port and Port 5 WAN/LAN Port):**	**System:** P1 (Green) P2 (Green) Alarm (Red) I/O (Red) **Ethernet Interfaces (Ports 1-4 LAN Port and Port 5 WAN/LAN Port):**

	1000 LNK/ACT (Green) 10/100 LNK/ACT (Amber) **Wi-Fi:** 2.4GHz(Green) 5GHz(Green)		1000 LNK/ACT (Green) 10/100 LNK/ACT (Amber) **Wi-Fi:** 5GHz(Green)
Wireless Specifications			
Wi-FI Standard	IEEE 802.11a/n/an/ac/ax 5GHz (2Tx2R) IEEE 802.11g/b/n/ax 2.4GHz (2Tx2R)		IEEE 802.11a/an/ac/ax 5GHz (4Tx4R)
Band Mode	2.4GHz & 5GHz concurrent mode		5GHz concurrent mode
Data Modulation	802.11ax: MIMO-OFDMA (BPSK / QPSK / 16QAM / 64QAM / 256QAM, 1024QAM) 802.11ac: MIMO-OFDM (BPSK / QPSK / 16QAM / 64QAM / 256QAM) 802.11a/g/n: OFDM (BPSK / QPSK / 16QAM / 64QAM) 802.11b: DSSS (DBPSK / DQPSK / CCK)		802.11ax: MIMO-OFDMA (BPSK / QPSK / 16QAM / 64QAM / 256QAM, 1024QAM) 802.11ac: MIMO-OFDM (BPSK / QPSK / 16QAM / 64QAM / 256QAM) 802.11a/g/n: OFDM (BPSK / QPSK / 16QAM / 64QAM)
Antenna	4 dBi 2.4GHz and 5GHz dual-band external antennas with RP-SMA male connectors for Wi-Fi		4 dBi external antennas with RP-SMA male connectors for Wi-Fi
Frequency Range	2.4GHz	America FCC: 2.412~2.462GHz Europe ETSI: 2.412GHz~2.472GHz	--
	5GHz	America FCC: 5.180~5.240GHz, 5.745~5.825GHz Europe ETSI: 5.180~5.700GHz	America FCC: 5.180~5.240GHz, 5.745~5.825GHz Europe ETSI: 5.180~5.700GHz
Operating Channels	2.4GHz	America FCC: 1~11 Europe ETSI: 1~13	--
	5GHz	America FCC: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140 Europe ETSI:	America FCC: Non-DFS: 36, 40, 44, 48, 149,153,157,161,165 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 132, 136, 140 Europe ETSI: Non-DFS: 36, 40, 44, 48 DFS: 52, 56, 60, 64, 100, 104, 108,

		Non-DFS: 36, 40, 44, 48 DFS: 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 5GHz channel list may vary in different countries according to their regulations.	112, 116, 120, 124, 128, 132, 136, 140 5GHz channel list may vary in different countries according to their regulations.
Channel Width	20MHz, 40MHz, 80MHz		20MHz, 40MHz, 80MHz, 160MHz
Data Transmission Rates	Transmit: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz Receive: 600 Mbps* for 2.4 GHz and 1200 Mbps* for 5 GHz ***The estimated transmission distance is based on the theory. The actual distance may vary in different environments.**		Transmit: 2400 Mbps* for 5 GHz Receive: 2400Mbps* for 5 GHz ***The estimated transmission distance is based on the theory. The actual distance may vary in different environments.**
Transmission Power	11b: 23dbm+/- 1.5dbm @11Mbps 11g: 20dbm+/- 1.5dbm @54Mbps 11g/n: 20dBm +/- 1.5dbm @MCS7, HT20 17dBm@MCS7,HT40 11a: 19.5dBm +/- 1.5dbm @54Mbps 11a/n: 19.5dBm+/- 1.5dbm @MCS7, HT20 17dBm@MCS7, HT40 11ac HT20: 20+/-1.5dBm @MCS8 11ac HT40: 17+/-1.5dBm @MCS9 11ac HT80: 14.5+/-1.5dBm @MCS9 11ax HT20: 20+/-1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9 11ax HT80: 14.5 +/- 1.5dBm @MCS11		11a: 19.5dBm +/- 1.5dbm @54Mbps 11a/n: 19.5dBm+/- 1.5dbm @MCS7, HT20 17dBm@MCS7, HT40 11ac HT20: 20+/-1.5dBm @MCS8 11ac HT40: 17+/-1.5dBm @MCS9 11ac HT80: 14.5+/-1.5dBm @MCS9 11ax HT20: 20+/-1.5dBm @MCS9 11ax HT40: 17 +/- 1.5dBm @MCS9 11ax HT80: 14.5 +/- 1.5dBm @MCS11
Receiver Sensitivity	11b: -99dBm @11Mbps 11g: -95dBm @54Mbps 11g/n: -90dBm @HT20, MCS7 -86dBm @HT40, MCS7 11a: -90Bm @54Mbps 11a/n: -85dBm @HT20, MCS7 -81dBm @HT40, MCS7 11ac: -90dBm +/- 2dBm @VHT20 MCS8 11ac: -85dBm +/- 2dBm @VHT40 MCS9 11ac: -68dBm +/- 2dBm @VHT80 MCS9 11ax: -61dBm +/- 2dBm @HE20 MCS11 11ax: -58dBm +/- 2dBm @HE40 MCS11		11a: -90Bm @54Mbps 11a/n: -85dBm @HT20, MCS7 -81dBm @HT40, MCS7 11ac: -90dBm +/- 2dBm @VHT20 MCS8 11ac: -85dBm +/- 2dBm @VHT40 MCS9 11ac: -68dBm +/- 2dBm @VHT80

	11ax: -55dBm +/- 2dBm @HE80 MCS11	MCS9 11ax: -61dBm +/- 2dBm @HE20 MCS11 11ax: -58dBm +/- 2dBm @HE40 MCS11 11ax: -55dBm +/- 2dBm @HE80 MCS11
Encryption Security	WPA3 Personal, WPA2/WPA3 Personal WPA2 Personal (AES), WPA2 Personal (TKIP), WPA2 Personal (TKIP+AES) WPA/WPA2 Personal (AES), WPA/WPA2 Personal (TKIP), WPA/WPA2 Personal (TKIP+AES) WPA2 Enterprise, WPA/WPA2 Enterprise	
Management Functions		
Basic Management Interfaces	Web browser SNMP v1, v2c PLANET Smart Discovery utility PLANET NMS controller supported	
Secure Management Interfaces	TLS 1.1, TLS 1.2, TLS 1.3 SNMP v3	
Operation Modes	Access Point (default) Gateway Repeater	
LAN	Static IP/* DHCP Client	
WAN	Static IP Dynamic IP PPPoE/PPTP/L2TP	
VLAN	IEEE 802.1Q VLAN (VID: 1~4094) SSID-to-VLAN mapping to up to 4 SSIDs	
Wireless Security	Enable/Disable SSID Broadcast Wireless MAC address filtering User Isolation	
Max. SSID	8 (4 per radio)	4
Max. Wireless Clients	150 (100 is suggested, depending on usage)	150 (100 is suggested, depending on usage)
Wi-Fi Advanced	Auto Channel Selection 5-level Transmit Power Control : ■ Max (100%) ■ Efficient (75%) ■ Enhanced (50%)	Auto Channel Selection 5-level Transmit Power Control : ■ Max (100%) ■ Efficient (75%) ■ Enhanced (50%)

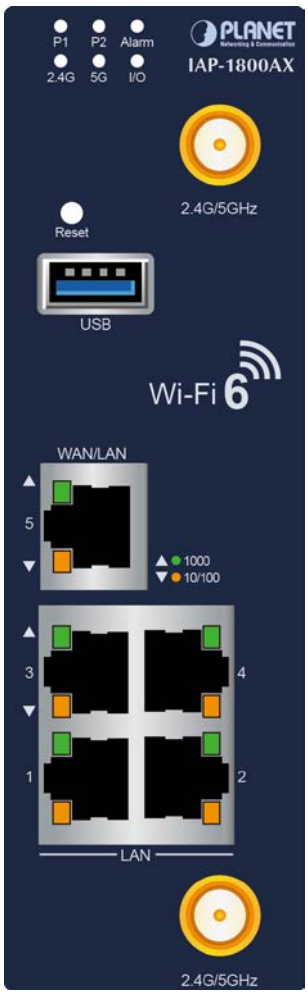
	■ Standard (25%) or Min (15%) Client Limit Control Coverage Threshold *Wi-Fi channel analysis chart Seamless Roaming Beamforming BSS Coloring 2.4GHz WLAN Partition 5GHz WLAN Partition RTS Threshold	■ Standard (25%) or Min (15%) Client Limit Control Coverage Threshold *Wi-Fi channel analysis chart Seamless Roaming Beamforming BSS Coloring 5GHz WLAN Partition RTS Threshold
Wireless Roaming	IEEE 802.11k, 802.11v, and 802.11r	
Wireless QoS	Supports Wi-Fi Multimedia (WMM)	
System Management	Setup wizard Remote management through PLANET DDNS/ Easy DDNS Configuration backup and restore Supports UPnP Supports IGMP Proxy Supports PPTP/L2TP/IPSec VPN Pass-through Supports Captive Portal, RADIUS Server/Client (Gateway mode) Diagnostics	
Status Monitoring	Dashboard System status/service Statistics Connection status	
Event Management	Remote System Log Local Event Log	
Self-healing	Supports auto reboot settings per day/hour	
Central Management	Applicable controllers: ● NMS-500, NMS-1000V ● Wireless Switch: WS-1032P, WS-2864PVR ● VPN Gateway: VR-300 series, IVR-300 series ● PLANET CloudViewer App	
Standards Conformance		
Regulatory Compliance	FCC Part 15 Class A, CE	
Environment		
Operating	Temperature: -40 ~ 75 degrees C Relative humidity: 5 ~ 90% (non-condensing)	
Storage	Temperature: -40 ~ 75 degrees C Relative humidity: 5 ~ 90% (non-condensing)	

Chapter 2. Physical Descriptions

2.1 Physical Descriptions

2.1.1 Front View

IAP-1800AX Front Panel



■ **LED Definition**

■ **System**

LED	Color	Function
P1	**Green**	**Lights** to indicate power 1 has power.
P2	**Green**	**Lights** to indicate power 2 has power.
Alarm	**Red**	**Lights** to indicate power or port failure
I/O	**Red**	Blinks to indicate input power or port has failed or DI has event.

■ **Wi-Fi**

LED	Color	Function
2.4G	**Green**	**Light** to indicate 2.4GHz Wi-Fi service is enabled.
5G	**Green**	**Light** to indicate 5GHz Wi-Fi service is enabled.

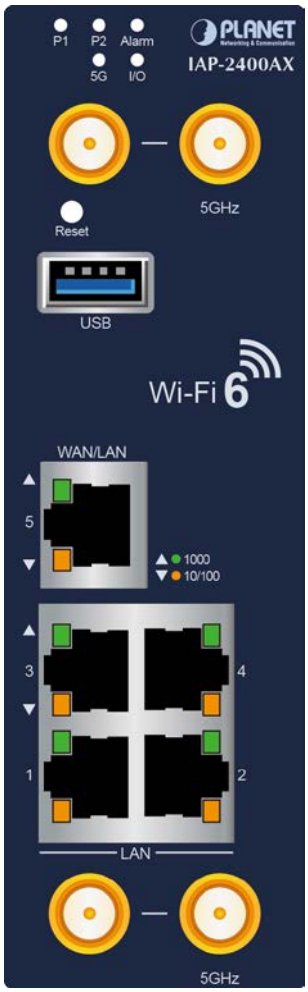
■ **LAN 10/100/1000BASE-T Interfaces (Ports 1 to 4)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**:	To indicate the link through that port is successfully established at **1000Mbps**.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**:	To indicate the link through that port is successfully established at **10/100Mbps**.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

■ **WAN/LAN 10/100/1000BASE-T Interface (Port 5)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**:	To indicate the link through that port is successfully established at **1000Mbps**.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**:	To indicate the link through that port is successfully established at **10/100Mbps**.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

IAP-2400AX Front Panel



■ LED Definition

■ System

LED	Color	Function
P1	**Green**	**Lights** to indicate power 1 has power.
P2	**Green**	**Lights** to indicate power 2 has power.
Alarm	**Red**	**Lights** to indicate power or port failure
I/O	**Red**	Blinks to indicate input power or port has failed or DI has event.

■ Wi-Fi

LED	Color	Function
5G	**Green**	**Light** to indicate 5GHz Wi-Fi service is enabled.

■ **LAN 10/100/1000BASE-T Interfaces (Ports 1 to 4)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**:	To indicate the link through that port is successfully established at **1000Mbps**.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**:	To indicate the link through that port is successfully established at **10/100Mbps**.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

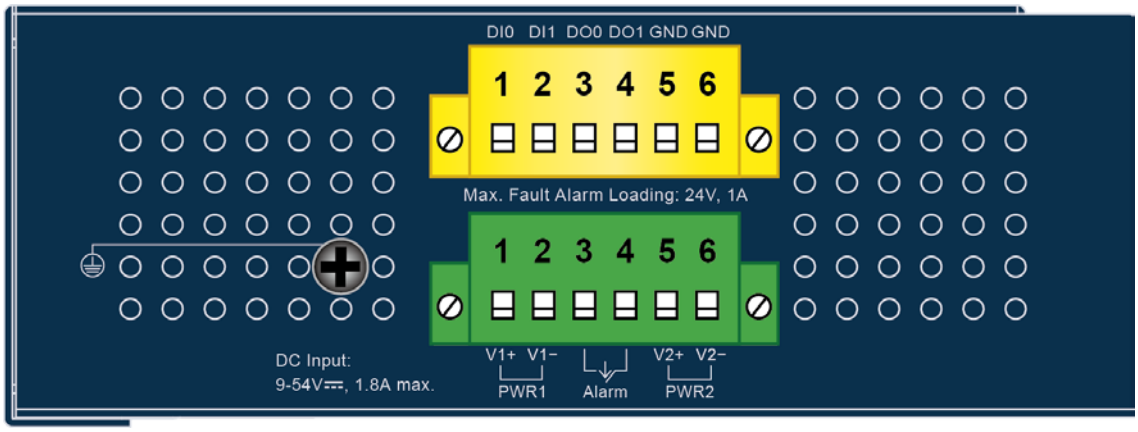
■ **WAN/LAN 10/100/1000BASE-T Interface (Port 5)**

LED	Color	Function	
1000 LNK/ACT	**Green**	**Lights**:	To indicate the link through that port is successfully established at **1000Mbps**.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
10/100 LNK/ACT	**Amber**	**Lights**:	To indicate the link through that port is successfully established at **10/100Mbps**.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

2.1.2 Top View

The Upper Panel of the Industrial 802.11ax Wireless AP consists of two terminal block connectors within 6 contacts. Please follow the steps below to insert the power wire.

IAP-1800AX/IAP-2400AX Top View

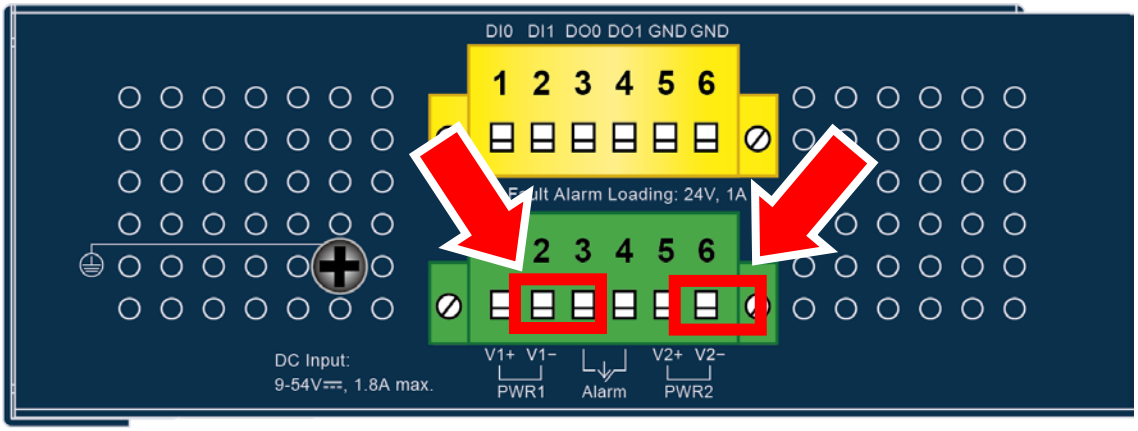


2.1.3 Wiring the Power Inputs

The 6-contact terminal block connector on the top panel of Industrial 802.11ax Wireless AP is used for two DC redundant power inputs. Please follow the steps below to insert the power wire.

When performing any of the procedures like inserting the wires or tightening the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

1. Industrial 802.11ax Wireless AP Input Voltage: 9-54V DC.
2. Insert positive/negative DC power wires into Contacts 1 and 2 for Power 1, or Contacts 5 and 6 for Power 2.



Note

To avoid damage, please make sure the input voltage is under the specification of the Industrial 802.11ax Wireless AP.

3. Tighten the wire-clamp screws for preventing the wires from loosening.

1	2	3	4	5	6
Power 1		Alarm		Power 2	
+	-			+	-

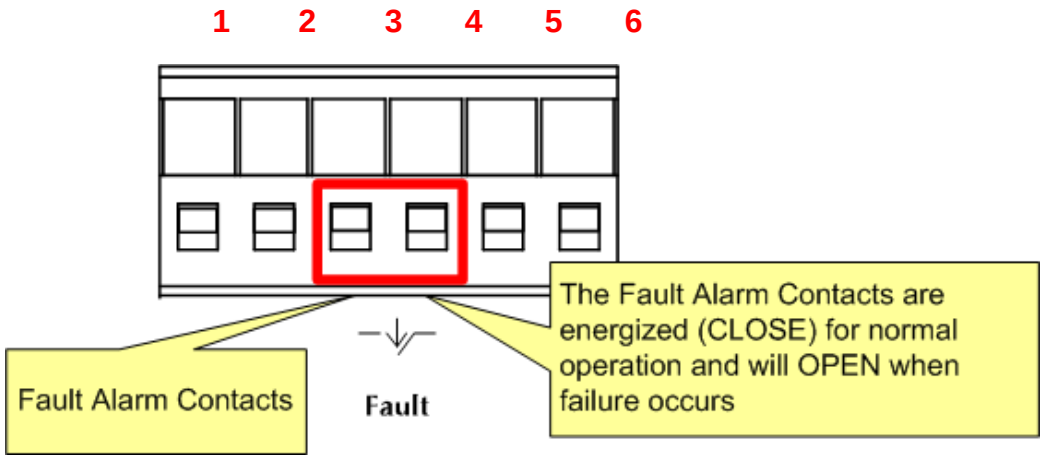
Note

The wire gauge for the terminal block should be in the range from **12** to **24** AWG.

PWR1 and PWR2 must provide the **same DC voltage** while operating with dual power input.

2.1.4 Wiring the Fault Alarm Contact

The fault alarm contacts are in the middle of the terminal block connector as the picture shows below. Inserting the wires, the Industrial 802.11ax Wireless AP will detect the fault status of the power failure or port failure, and then will form an open circuit. The following illustration shows an application example for wiring the fault alarm contacts.



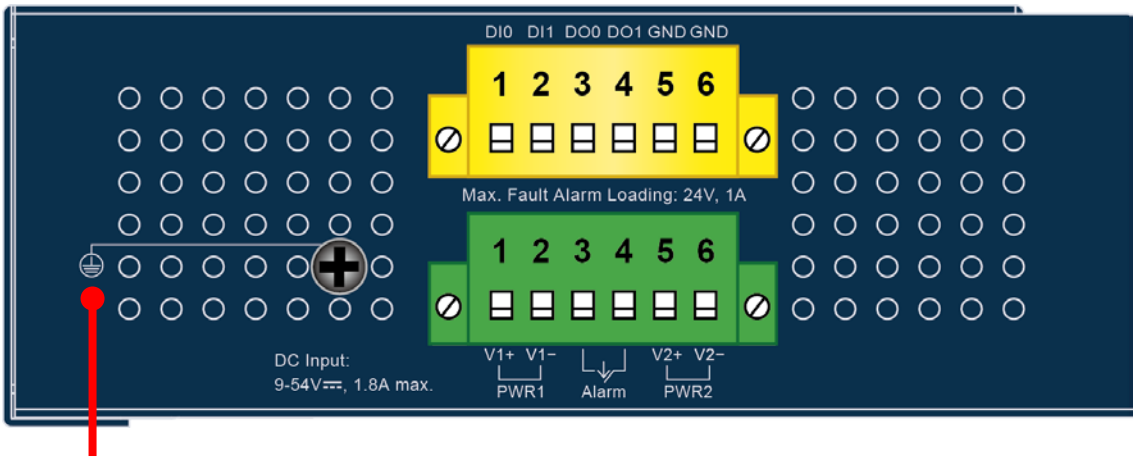
Insert the wires into the fault alarm contacts

Note

1. The wire gauge for the terminal block should be in the range between 12 and 24 AWG.
2. Alarm relay circuit accepts up to 24V, max. 1A currents.

2.1.5 Grounding the Device

Users **MUST** complete grounding wired with the device; otherwise, a sudden lightning could cause fatal damage to the device.



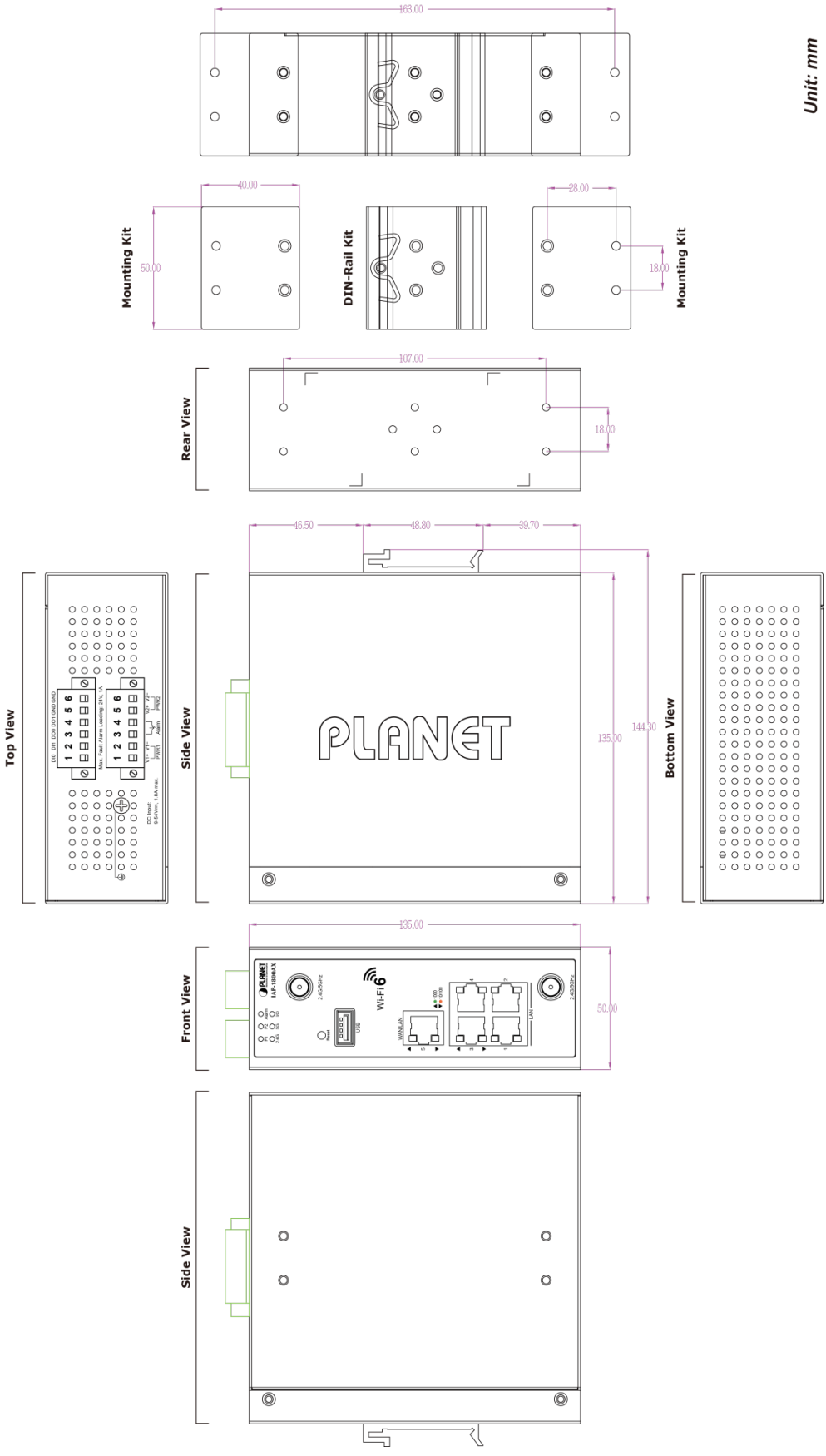
⏚ Earth Ground

Note

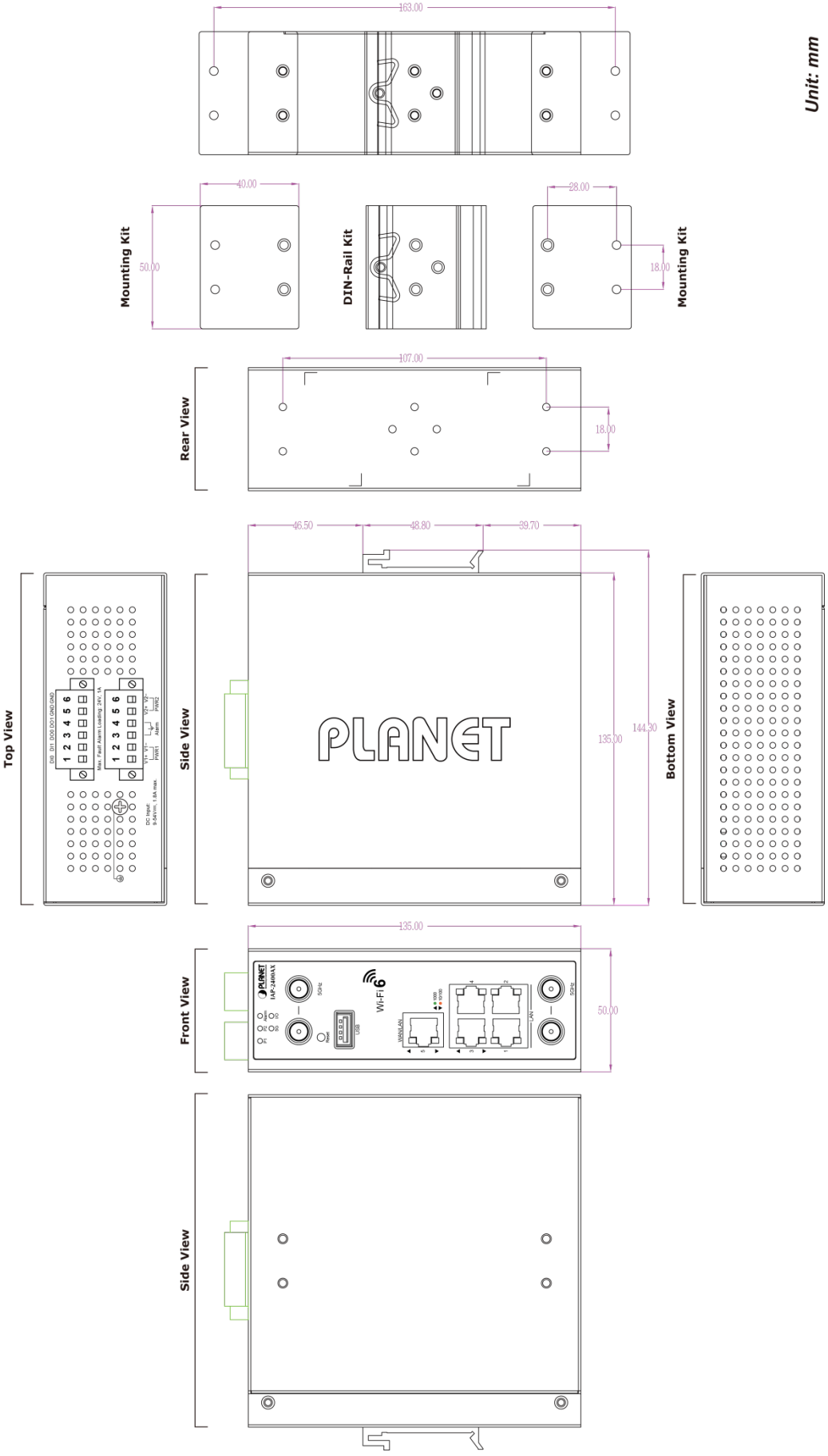
EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

2.1.6 Dimensions

IAP-1800AX Dimensions



IAP-2400AX Dimensions



2.2 Hardware Installation

This section describes how to install the Industrial 802.11ax Wireless AP. There are three methods to install the Industrial 802.11ax Wireless AP -- DIN-rail mounting, wall mounting and side wall mounting. Basic knowledge of networking is assumed.

Please read the following sections and perform the procedures in the order being presented.

(The device shown on this chapter is just a representation of the said device.)

2.2.1 DIN-rail Mounting

Step 1: Lightly slide the DIN-rail into the track.

Step 2: Check whether the DIN-rail is tightly on the track.

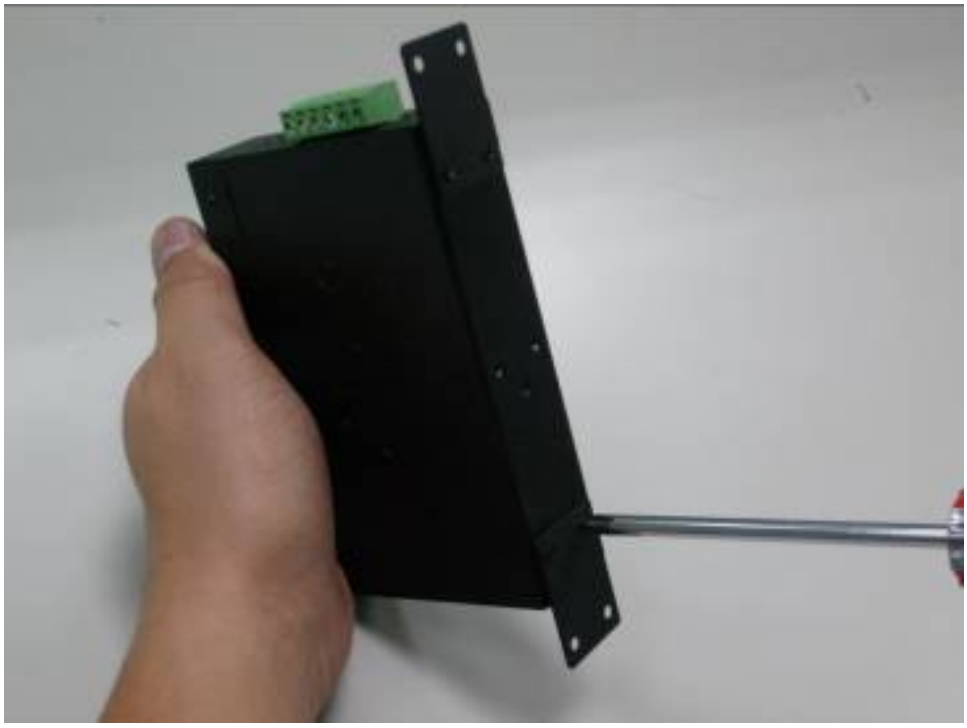
Step 3: Lightly remove the DIN-rail from the track.

2.2.2 Wall Mount Plate Mounting

To install the Industrial 802.11ax Wireless AP on the wall, please follow the instructions described below.

Step 1: Remove the DIN-rail from the Industrial 802.11ax Wireless AP. Use the screwdriver to loosen the screws to remove the DIN-rail.

Step 2: Place the wall-mount plate on the rear panel and use the screwdriver to screw the wall mount plate tightly on the Industrial 802.11ax Wireless AP.



Step 3: Use the hook holes at the corners of the wall mount plate to hang the Industrial 802.11ax Wireless AP on the wall.

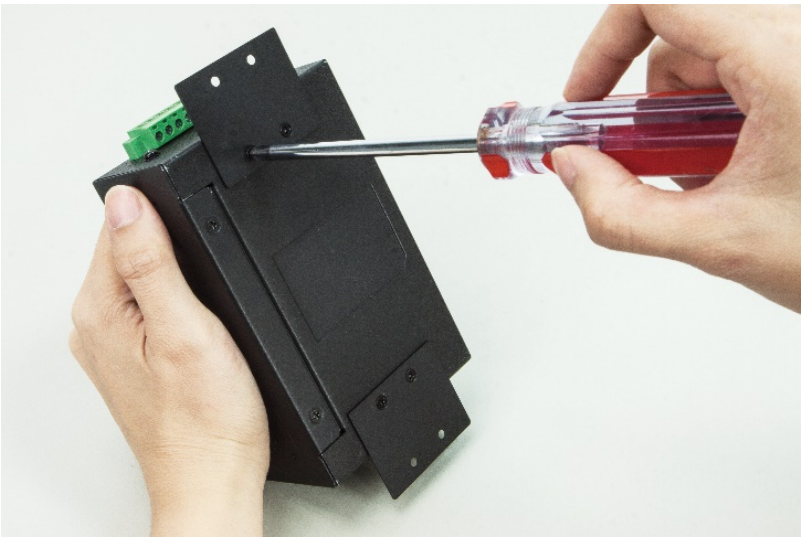
Step 4: To remove the wall mount plate, reverse the steps above.

2.2.3 Side Wall Mount Plate Mounting

To install the Industrial 802.11ax Wireless AP on the wall, please follow the instructions below.

Step 1: Remove the DIN-rail from the Industrial 802.11ax Wireless AP. Use the screwdriver to loosen the screws to remove the DIN-rail.

Step 2: Place the wall-mount plate on the side panel and use the screwdriver to screw the wall mount plate tightly on the Industrial 802.11ax Wireless AP.



Step 3: Use the hook holes at the corners of the wall mount plate to hang the Industrial 802.11ax Wireless AP on the wall.

Step 4: To remove the wall mount plate, reverse the steps above.

2.2.4 Wi-Fi Antenna Installation

Step 1: Fasten the antennas to the antenna connectors on the front panel of the Industrial 802.11ax Wireless AP.

Step 2: You can bend the antennas to fit your actual needs.

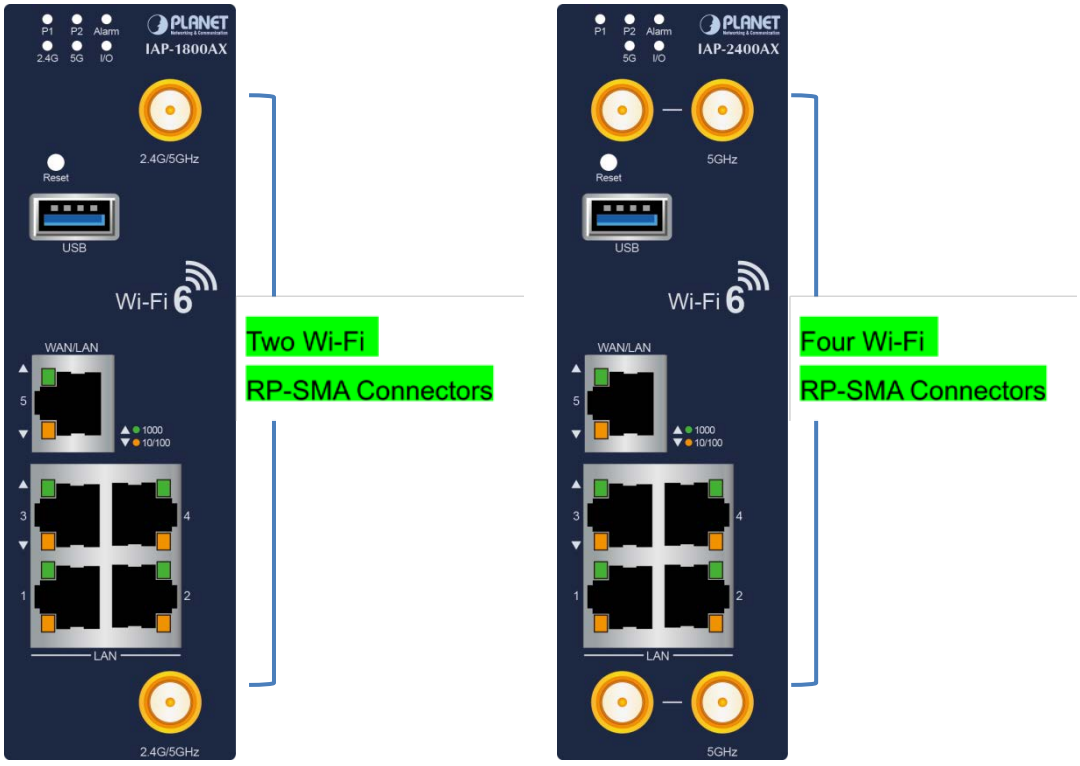


Figure 2-2: Industrial 802.11ax Wireless AP Front Panels

Chapter 3. Preparation

Before getting into the device's web UI, user has to check the network setting and configure PC's IP address.

3.1 System Requirements

- Workstations running Windows XP/2003/2008/2012/Vista/7/8/10/11, MAC OS X or later, Linux, UNIX, or other platforms are compatible with TCP/IP protocols.
- Workstations are installed with Ethernet NIC (Network Interface Card)
- **Serial Port Connection** (Terminal)
  - The above workstations come with **COM port** (DB9) or **USB-to-RS232** converter.
  - The above workstations have been installed with **terminal emulator**, such as Tera Term, PuTTY or Hyper Terminal included in Windows XP/2003.
  - **Serial cable** -- one end is attached to the RS232 serial port, while the other end to the console port of the Managed Metro Switch.
- **Ethernet Port Connection**
  - Network cables -- Use standard network (UTP) cables with RJ45 connectors.
  - The above PC is installed with Web browser.

It is recommended to use Chrome 98.0.xxx or above to access the Industrial 802.11ax Wireless AP. If the Web interface of the Industrial 802.11ax Wireless AP is not accessible, please turn off the anti-virus software or firewall and then try it again.

3.2 Manual Network Setup -- TCP/IP Configuration

The default IP address of the Industrial 802.11ax Wireless AP is **192.168.1.253**. And the default subnet mask is 255.255.255.0. These values can be changed as you want. In this guide, we use all the default values for description.

Connect the Industrial 802.11ax Wireless AP with your PC by plugging one end of an Ethernet cable in the LAN port of the AP and the other end in the LAN port of PC.

In the following sections, we'll introduce how to install and configure the TCP/IP correctly in **Windows 10**. And the procedures in other operating systems are similar. First, make sure your Ethernet Adapter is working, and refer to the Ethernet adapter manual if needed.

3.2.1 Configuring the IP Address Manually

Summary:

- Set up the TCP/IP Protocol for your PC.
- Configure the network parameters. The IP address is 192.168.1.xxx (If the default IP address of the Industrial 802.11ax Wireless AP is 192.168.1.253, the "xxx" can be configured to any number from 1 to 252.) and subnet mask is 255.255.255.0.

  1 Select **Use the following IP address**, and then configure the IP address of the PC.

  2 For example, the default IP address of the Industrial 802.11ax Wireless AP is 192.168.1.253, you may choose from 192.168.1.1 to 192.168.1.252.

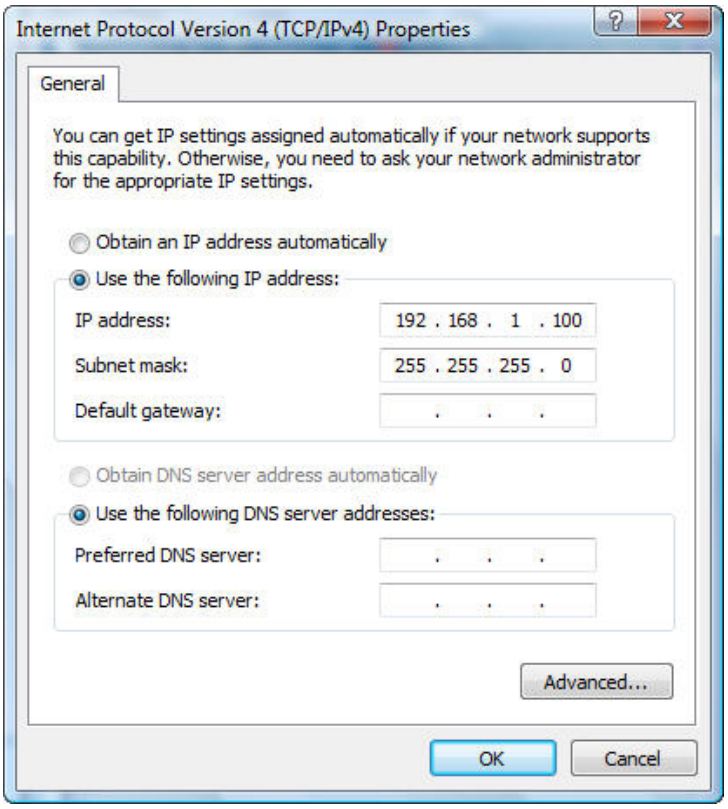


Figure 3-1: TCP/IP Setting

Now click **OK** to save your settings.

Now, you can run the ping command in the **command prompt** to verify the network connection between your PC and the AP. The following example is in **Windows 10** OS. Please follow the steps below:

1. Click on **Start > Run**.

2. Type "**cmd**" in the Search box.

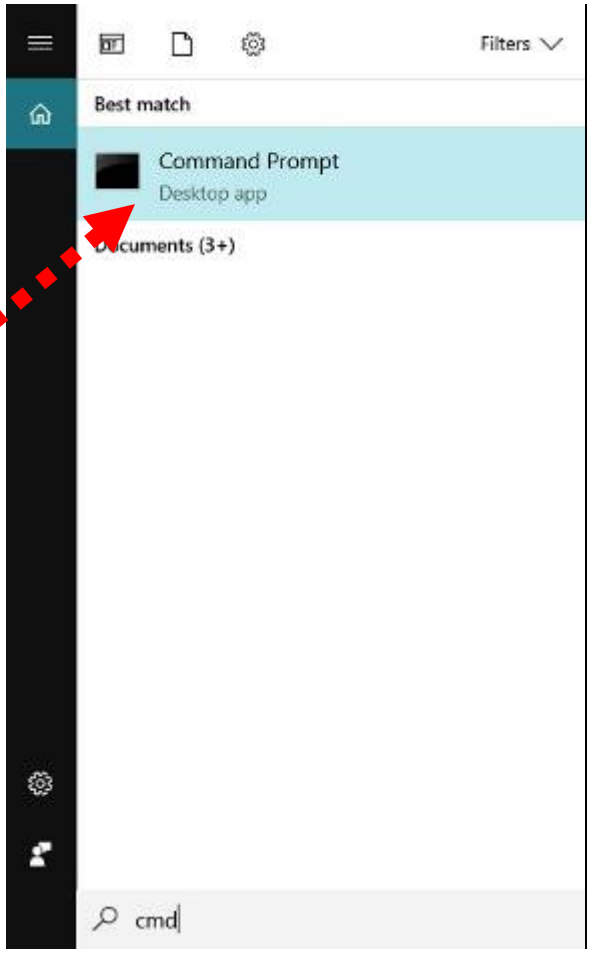


Figure 3-2: Windows Start Menu

3. Open a command prompt, type ping **192.168.1.253** and then press **Enter**.

◆ If the result displayed is similar to **Figure 3-3**, it means the connection between your PC and the AP has been established well.

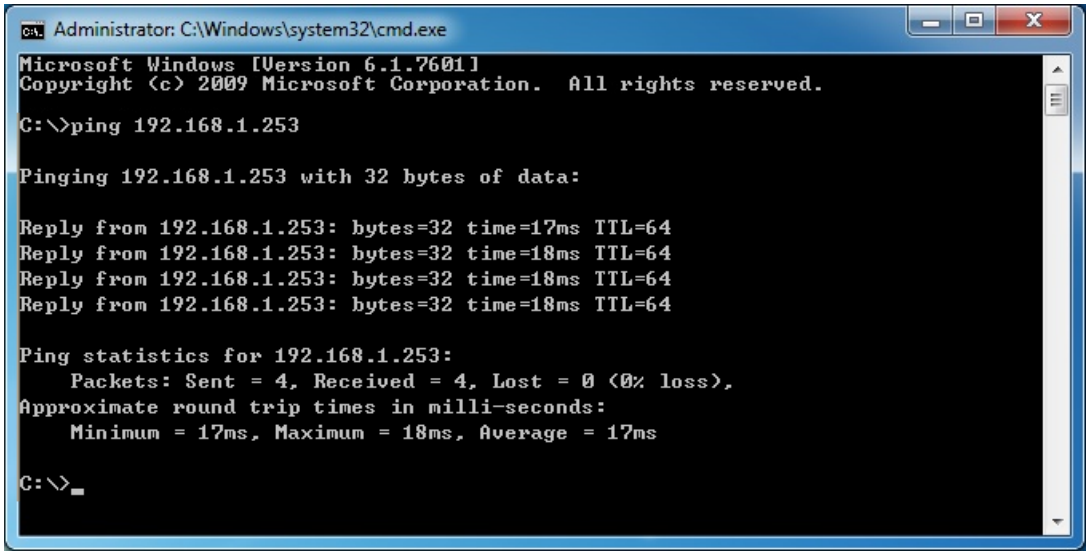


Figure 3-3: Successful Result of Ping Command

- If the result displayed is similar to **Figure 3-4**, it means the connection between your PC and the AP has failed.

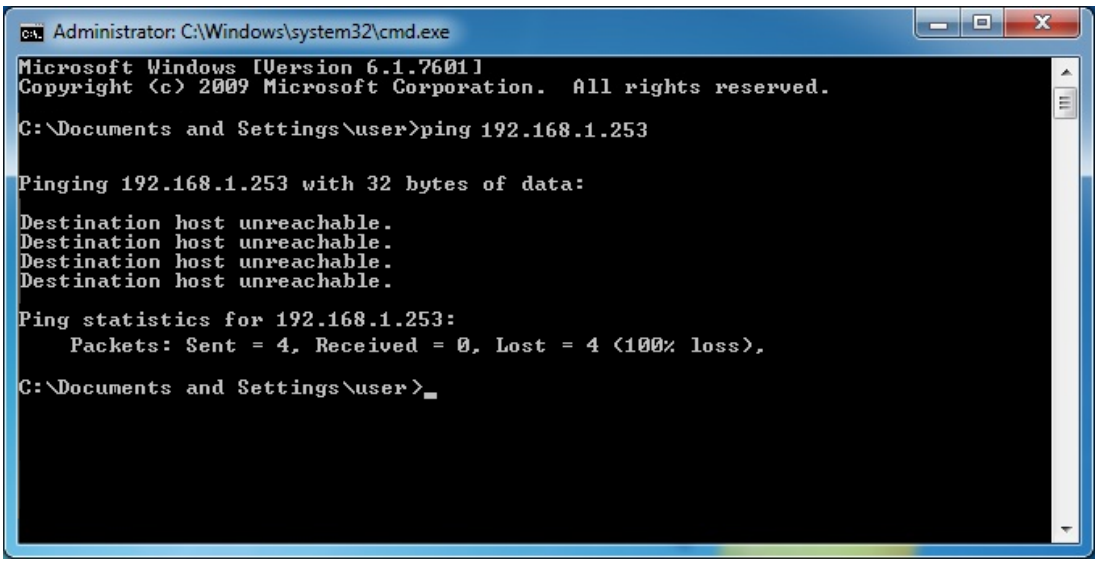


Figure 3-4: Failed Result of Ping Command

If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your AP. Some firewall software programs may block a DHCP request on newly installed adapters.

3.3 PLANET Smart Discovery Utility

For easily listing the Industrial 802.11ax Wireless AP in your Ethernet environment, the search tool -- PLANET Smart Discovery Utility -- is an ideal solution.

The following installation instructions are to guide you to running the PLANET Smart Discovery Utility.

1. Download the PLANET Smart Discovery Utility in administrator PC.
2. Run this utility as the following screen appears.

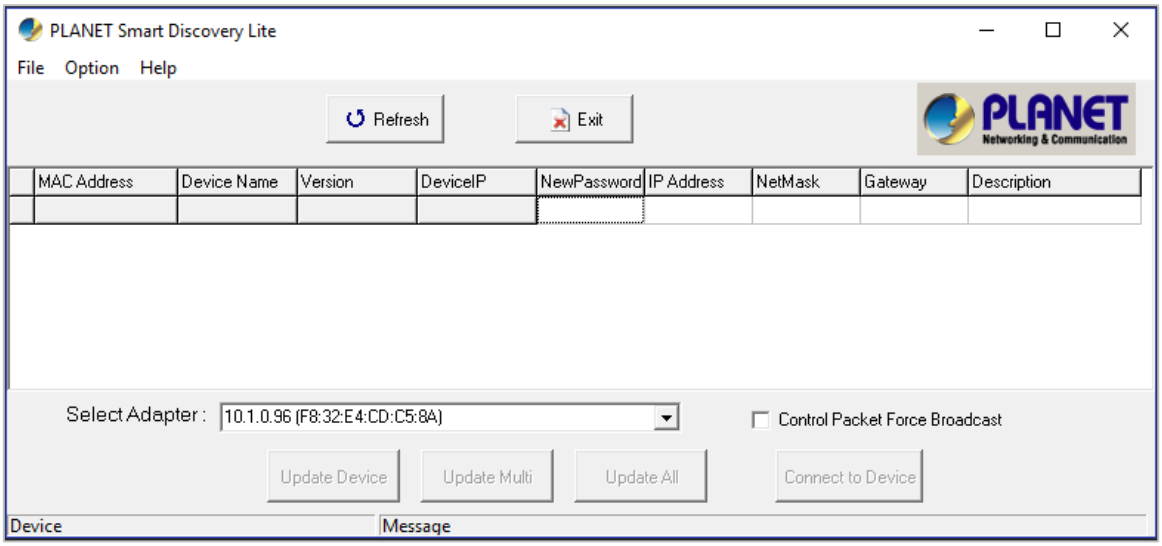


Figure 3-5: PLANET Smart Discovery Utility Screen

Note

If there are two LAN cards or above in the same administrator PC, choose a different LAN card by using the **"Select Adapter"** tool.

3. Press the **"Refresh"** button for the currently connected devices in the discovery list as the screen shows below:

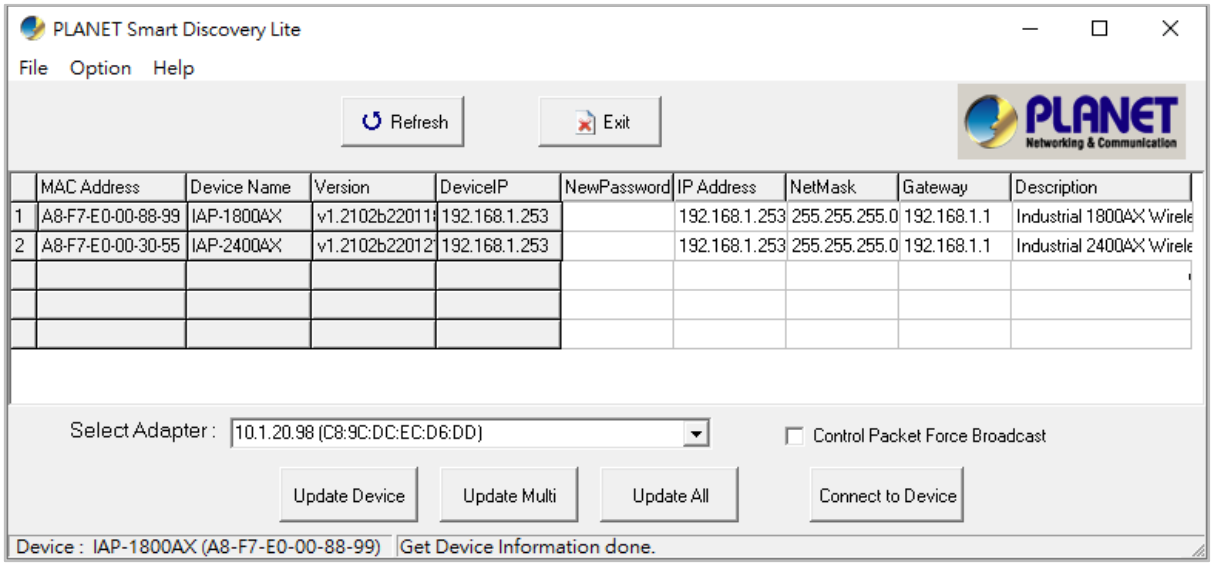


Figure 3-6: PLANET Smart Discovery Utility Screen

1. This utility shows all necessary information from the devices, such as MAC address, device name, firmware version, and device IP subnet address. It can also assign new password, IP subnet address and description to the devices.

2. After setup is completed, press the "**Update Device**", "**Update Multi**" or "**Update All**" button to take effect. The functions of the 3 buttons above are shown below:
   - **Update Device**: use current setting on one single device.
   - **Update Multi:** use current setting on choose multi-devices.
   - **Update All:** use current setting on whole devices in the list.

   The same functions mentioned above also can be found in "**Option**" tools bar.

3. To click the "**Control Packet Force Broadcast**" function, it allows you to assign a new setting value to the device under a different IP subnet address.

4. Press the "**Connect to Device**" button and the Web login screen appears.

Press the "**Exit**" button to shut down the PLANET Smart Discovery Utility.

3.4 Starting Setup in the Web UI

It is easy to configure and manage the Industrial 802.11ax Wireless AP with the web browser.

Step 1. To access the configuration utility, open a web-browser and enter the default IP address http://192.168.1.253 in the web address field of the browser.

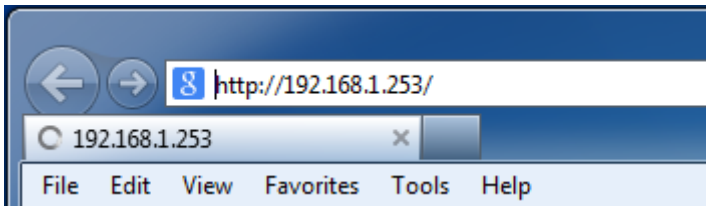


Figure 3-7: Login by Default IP Address

Step 2. When the login window pops up, please enter username and password. The default username and password are "**admin**". Then click the **LOGIN** button to continue.

Note

The following web screen is based on the IAP-1800AX; the display of the IAP-2400AX is the same as that of the IAP-1800AX.

Figure 3-8: Login Window

Default IP Address: **192.168.1.253**

Default Password: **admin**

Note

If the above screen does not pop up, it may mean that your web browser has been set to a proxy. Go to Tools menu> Internet Options> Connections> LAN Settings on the screen that appears, uncheck **Using Proxy** and click **OK** to finish it.

Chapter 4. Web-based Management

This chapter delivers a detailed presentation of Industrial 802.11ax Wireless AP's functionalities and allows you to manage the Industrial 802.11ax Wireless AP with ease.

Figure 4-1: Main Web Page

■ Main Menu

The main menu displays the product name, function menu, and main information in the center. Via the Web management, the administrator can set up the device by selecting the functions those listed in the function menu and button as shown in Figures 4-2 and 4-3.

Figure 4-2: Function Menu

Object	Description
System	Provides system information of the Industrial 802.11ax Wireless AP.
Network	Provides WAN, LAN and network configuration of the Industrial 802.11ax Wireless AP.
Security	Provides firewall and security configuration of the Industrial 802.11ax Wireless AP **(Available at Gateway mode)**.

Wireless	Provides wireless configuration of the Industrial 802.11ax Wireless AP.
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the Industrial 802.11ax Wireless AP.

Figure 4-3: Function Button

Object	Description
	Click the "**Refresh button**" to refresh the current web page.
	Click the "**Logout button**" to log out the web UI of the Industrial 802.11ax Wireless AP.

4.1 System

Use the system menu items to display and configure basic administrative details of the Industrial 802.11ax Wireless AP. The System menu shown in Figure 4-4 provides the following features to configure and monitor system.

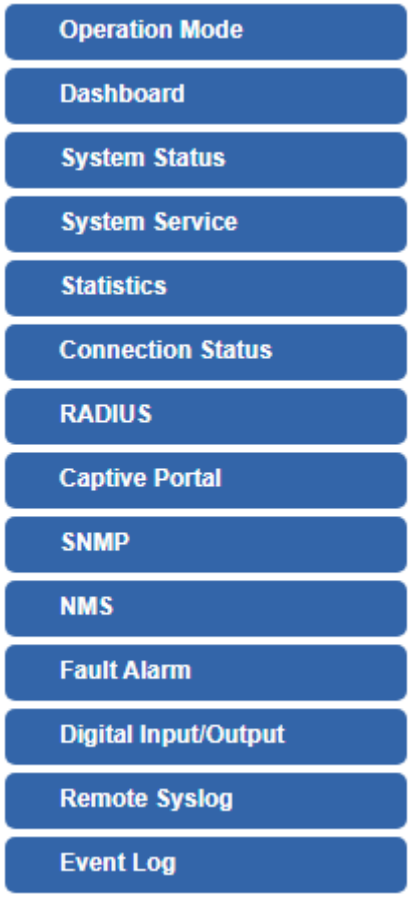


Figure 4-4: System Menu

Object	Description
Operation Mode	The Wizard will guide the user to configuring the Industrial 802.11ax Wireless AP easily and quickly.
Dashboard	The overview of system information includes connection, port, and system status.
System Status	Display the status of the system, Device Information, LAN and WAN.
System Service	Display the status of the system, Secured Service and Server Service.
Statistics	Display statistics information of network traffic of LAN and WAN.
Connection Status	Display the DHCP client table and the ARP table.

RADIUS	Enable/Disable RADIUS on Industrial 802.11ax Wireless APs.
Captive Portal	Enable/Disable Captive Portal on Industrial 802.11ax Wireless APs.
SNMP	Display SNMP system information.
NMS	Enable/Disable NMS on Industrial 802.11ax Wireless APs.
Fault Alarm	One relay output for power failure. Alarm relay current carry ability.
Digital Input/output	Digital Input/output Control Configuration page.
Remote Syslog	Enable Captive Portal on Industrial 802.11ax Wireless APs.
Event Log	Display Event Log information.

4.1.1 Operation Mode

The Wizard guides you to configuring the Industrial 802.11ax Wireless AP in a different mode, including AP, gateway and repeater modes.

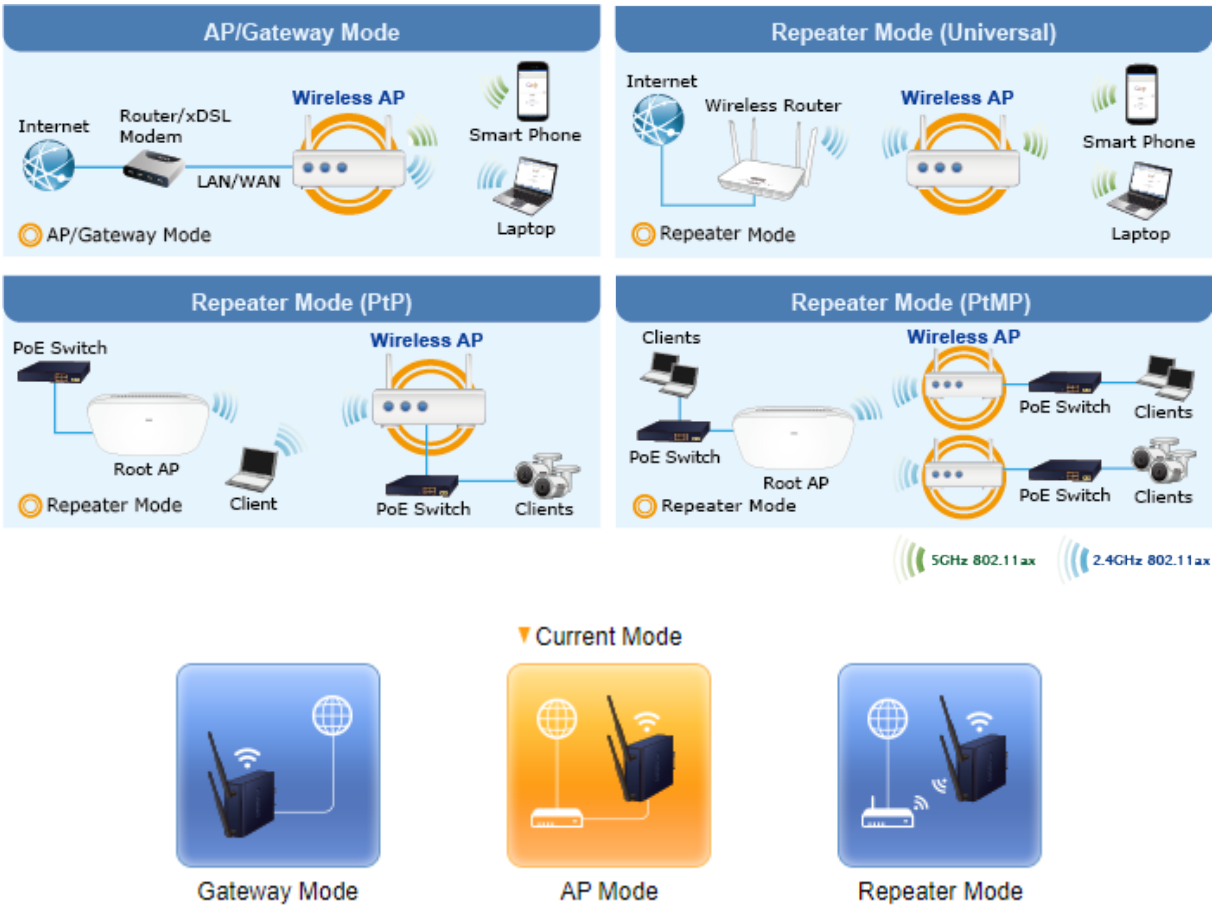


Figure 4-5: Operation Mode

Note

The default operation mode is **AP Mode**.

4.1.2 Gateway Mode (Router)

Click "**Wizard**" → "**Gateway Mode**" and the following page will be displayed. This section allows you to configure the Gateway mode.

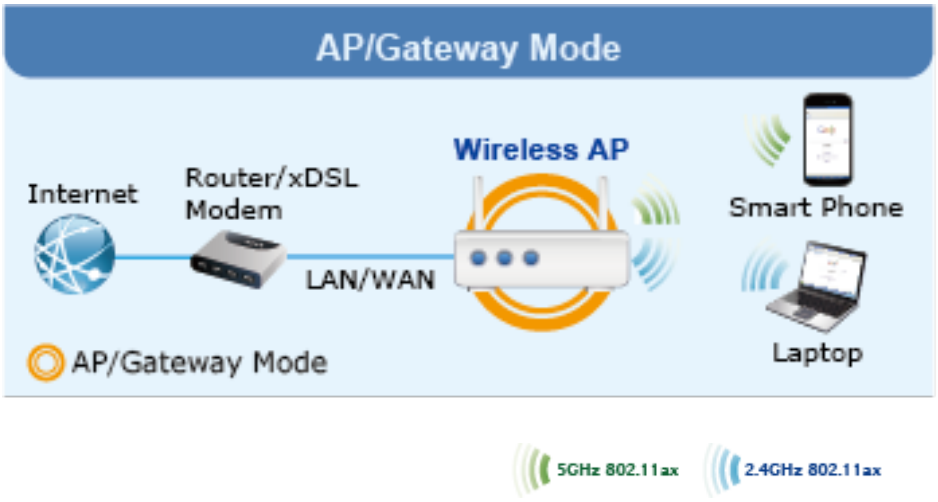


Figure 4-6: Setup Wizard

Step 1: Operation Mode

Select operation Mode.

Step 2: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown in Figure 4-7.

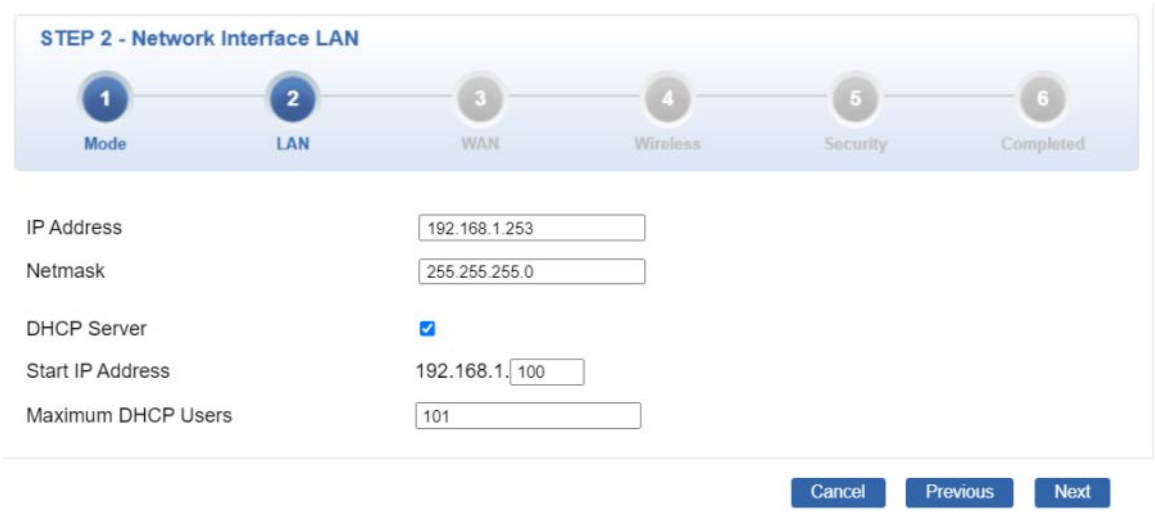


Figure 4-7: Setup Wizard – LAN Configuration

Object	Description
IP Address	Enter the IP address of your Industrial 802.11ax Wireless AP. The default is 192.168.1.1.
Subnet Mask	An address code that determines the size of the network. Normally use 255.255.255.0 as the subnet mask.
DHCP Server	By default, the DHCP Server is enabled. If user needs to disable the function, please uncheck the box.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the Industrial 802.11ax Wireless AP.
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the Industrial 802.11ax Wireless AP will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
Next	Press this button to the next step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Step 3: WAN Interface

The Industrial 802.11ax Wireless AP supports two access modes on the WAN side shown in Figure 4-8.

Figure 4-8: Setup Wizard – WAN 1 Configuration

Mode 1 -- Static IP

Select **Static IP Address** if all the Internet port's IP information is provided to you by your ISP. You will need to enter the **IP Address**, **Netmask**, **Default Gateway** and **DNS Server** provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Industrial 802.11ax Wireless AP will not accept the IP address if it is not in this format. The setup is shown in Figure 4-9.

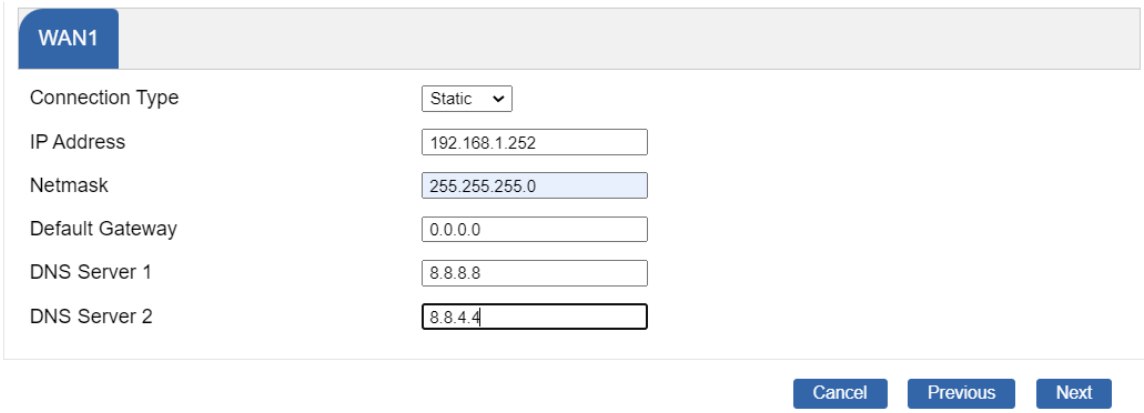


Figure 4-9: WAN Interface Setup – Static IP Setup

Object	Description

IP Address	Enter the IP address assigned by your ISP.
Netmask	Enter the Netmask assigned by your ISP.
Default Gateway	Enter the Gateway assigned by your ISP.
DNS Server	The DNS server information will be supplied by your ISP.
Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Mode 2 -- DHCP Client

Select DHCP Client to obtain IP Address information automatically from your ISP. The setup is shown in Figure 4-10.

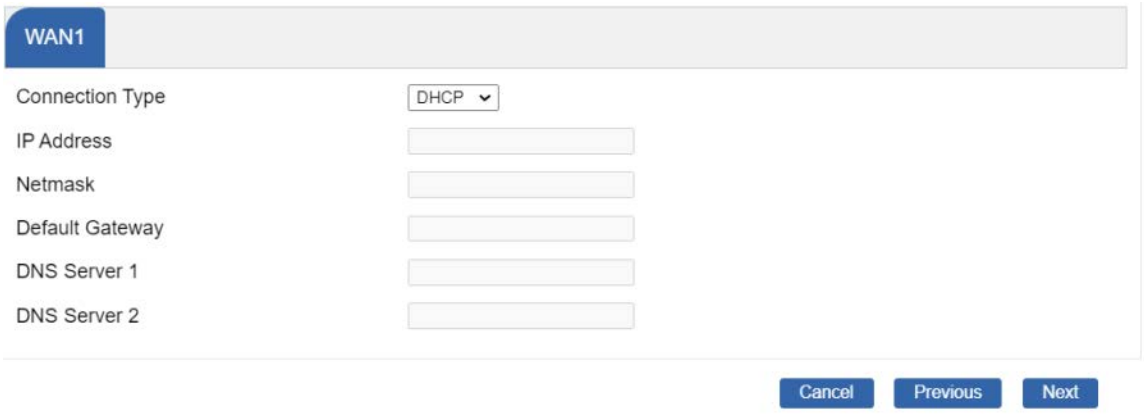


Figure 4-10: WAN Interface Setup – DHCP Setup

Step 4: Network Interface Wireless

Set up the Security Settings as shown in Figure 4-11.

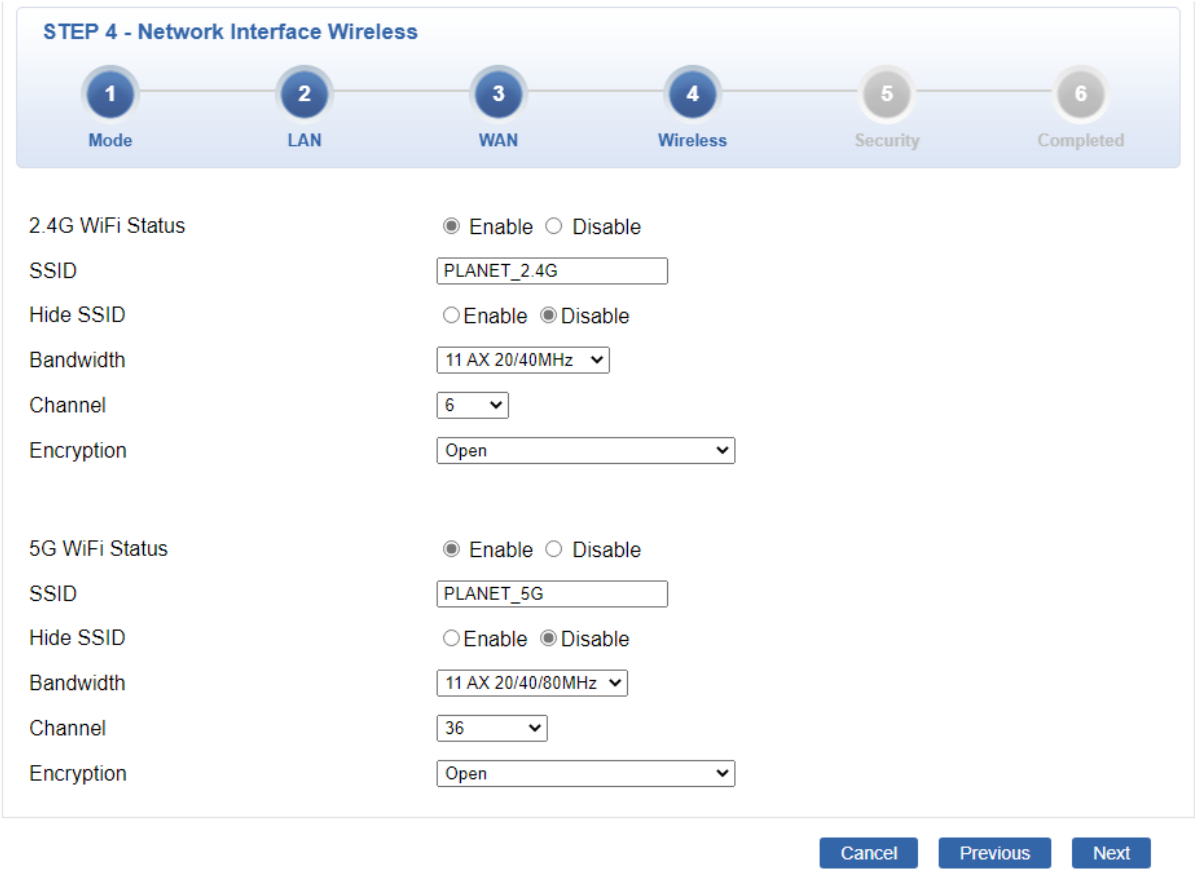


Figure 4-11: Network Setup

Step 5: Security Setting

Set up the Security Settings as shown in Figure 4-12.

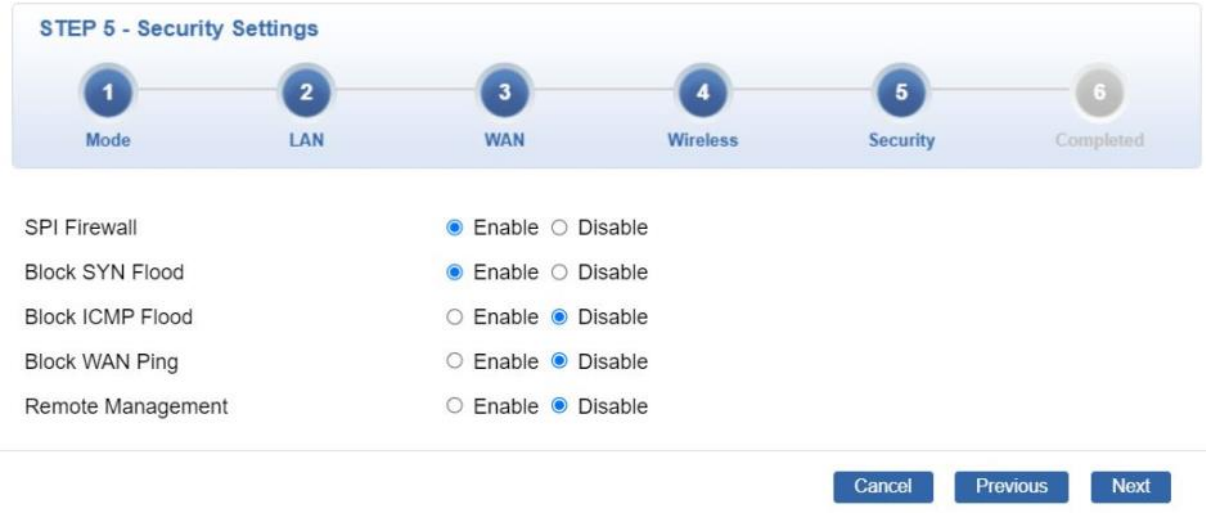


Figure 4-12: Setup Wizard –Security Setting

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. The default configuration is enabled.
Block SYN Flood	SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on. The default configuration is enabled.
Block ICMP Flood	ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack. The default configuration is disabled.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
Remote Management	Enable the function to allow the web server access of the Industrial 802.11ax Wireless AP from the Internet network. The default configuration is disabled.
Next	Press this button for the next step.
Previous	Press this button for the previous step.
Cancel	Press this button to undo any changes made locally and revert to previously saved values.

Step 6: Setup Completed

The page will show the summary of LAN, WAN and Security settings as shown in Figure 4-13.

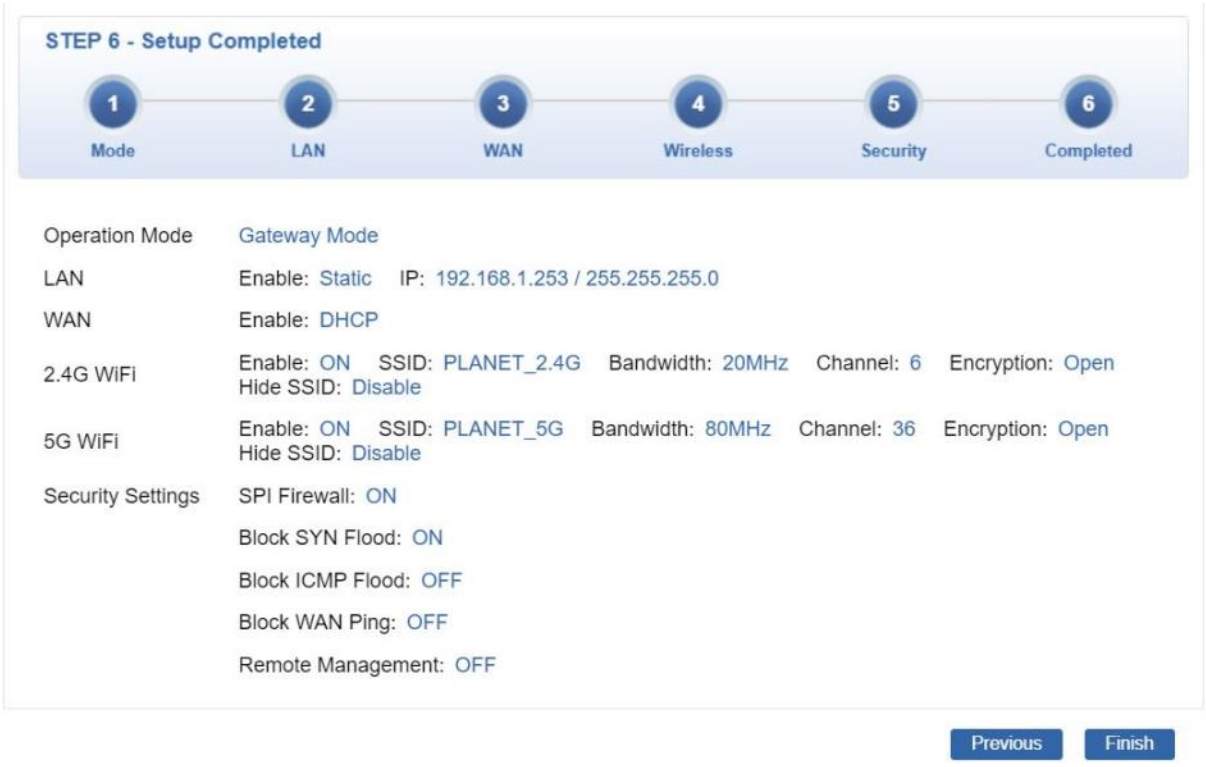


Figure 4-13: Setup Wizard – Setup Completed

Object	Description
Finish	Press this button to save and apply changes.
Previous	Press this button for the previous step.

4.1.3 Dashboard

The dashboard provides an overview of system information including connection, port, and system status as shown in Figure 4-14.

Figure 4-14: Dashboard

Port Status

Object	Description
	Ethernet port is in use.
	Ethernet port is not in use.

Wireless Status

Object	Description
	Wireless is in use.
	Wireless is not in use.

System Information

Object	Description
CPU	Display the CPU loading
Memory	Display the memory usage

4.1.4 System Status

This page displays system information as shown in Figure 4-15.

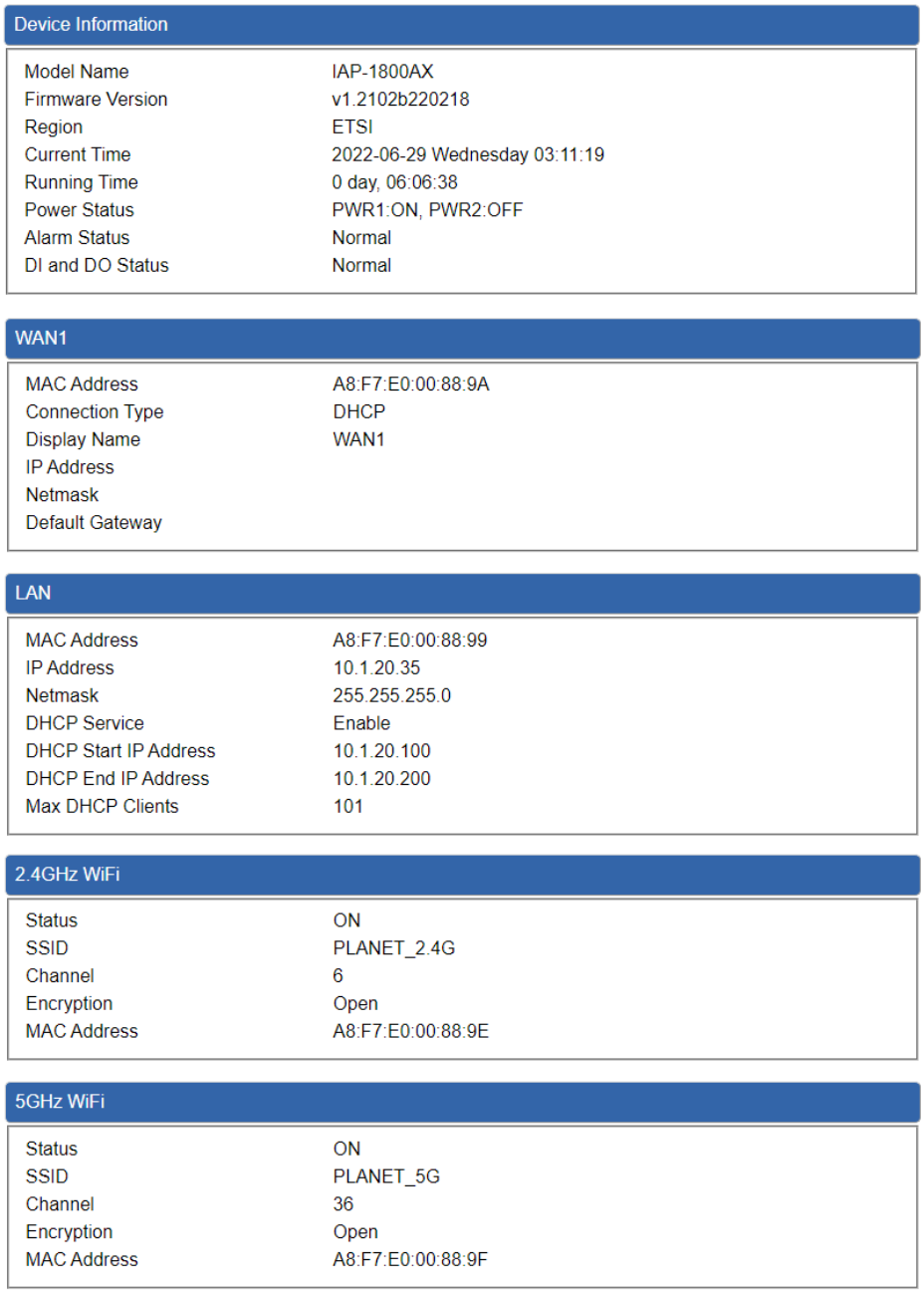


Figure 4-15: Status

4.1.5 System Service

This page displays the number of packets that pass through the Industrial 802.11ax Wireless AP on the WAN and LAN. The statistics are shown in Figure 4-16.

Server Service

#	Action	Service	Status
1	Enabled	DHCP Service	DHCP Table: 5
2	Disabled	DDNS Service	Not enabled
3	Disabled	Quality of Service	
4	Disabled	RADIUS Service	
5	Disabled	Captive Portal	
6	Enabled	2.4G WiFi	SSID: PLANET_2.4G
7	Enabled	5G WiFi	SSID: PLANET_5G

Secured Server Service

#	Action	Service	Status
1	Enabled	Cyberseurity	TLS 1.1, TLS 1.2, TLS 1.3
2	Enabled	SPI Firewall	
3	Disabled	MAC Filtering	(Active / Maximum Entries) 0 / 32
4	Disabled	IP Filtering	(Active / Maximum Entries) 0 / 32
5	Disabled	Web Filtering	(Active / Maximum Entries) 0 / 32

Figure 4-16: Service

4.1.6 Statistics

This page displays the number of packets that pass through the Industrial 802.11ax Wireless AP on the WAN and LAN. The statistics are shown in Figure 4-17.

Figure 4-17: Statistics

4.1.7 Connection Status

The page will show the DHCP Table and ARP Table. The status is shown in Figure 4-18.

DHCP Table

Name	IP Address	MAC Address	Expiration Time

ARP Table

IP Address	MAC Address	ARP Type
192.168.1.11	00:30:4f:9e:b7:df	dynamic
192.168.1.188	00:05:1b:c5:51:14	dynamic
192.168.1.239	a8:f7:e0:6a:a3:a4	dynamic
192.168.1.1	00:e0:53:00:12:01	dynamic

Figure 4-18: Connection Status

4.1.8 RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a security authentication client/server protocol that supports authentication, authorization and accounting. The RADIUS Server page is shown in Figure 4-19.

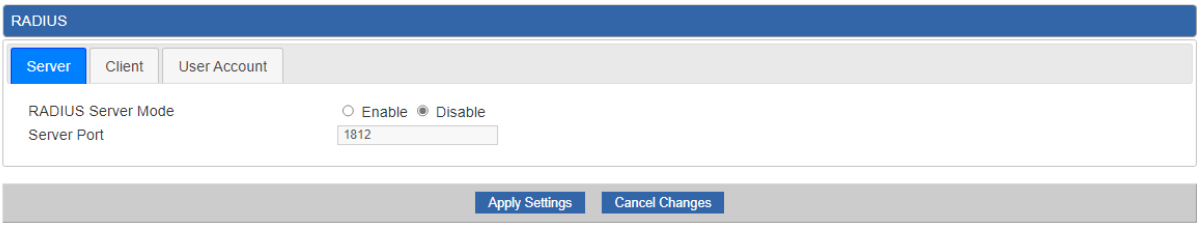


Figure 4-19: RADIUS

Object	Description
RADIUS	Disable or enable the RADIUS function. The default configuration is disabled.
Server Port	Default: 1812

4.1.9 Captive Portal

Captive portal service gives the ability to organize a public (or guest) Wi-Fi zone with user authorization. A captive portal is the authorization page that forcibly redirects users who connect to the public network before accessing the Internet. The Captive portal page is shown in Figure 4-20.

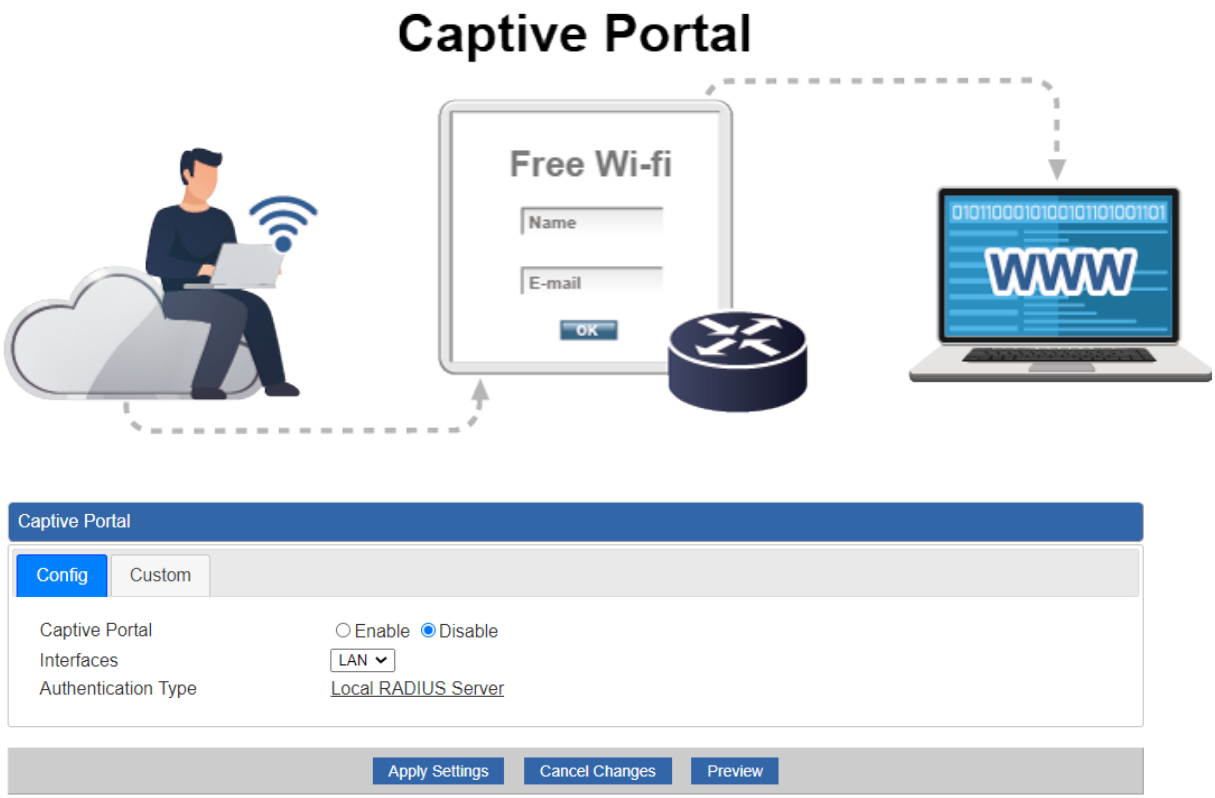


Figure 4-20: Captive Portal

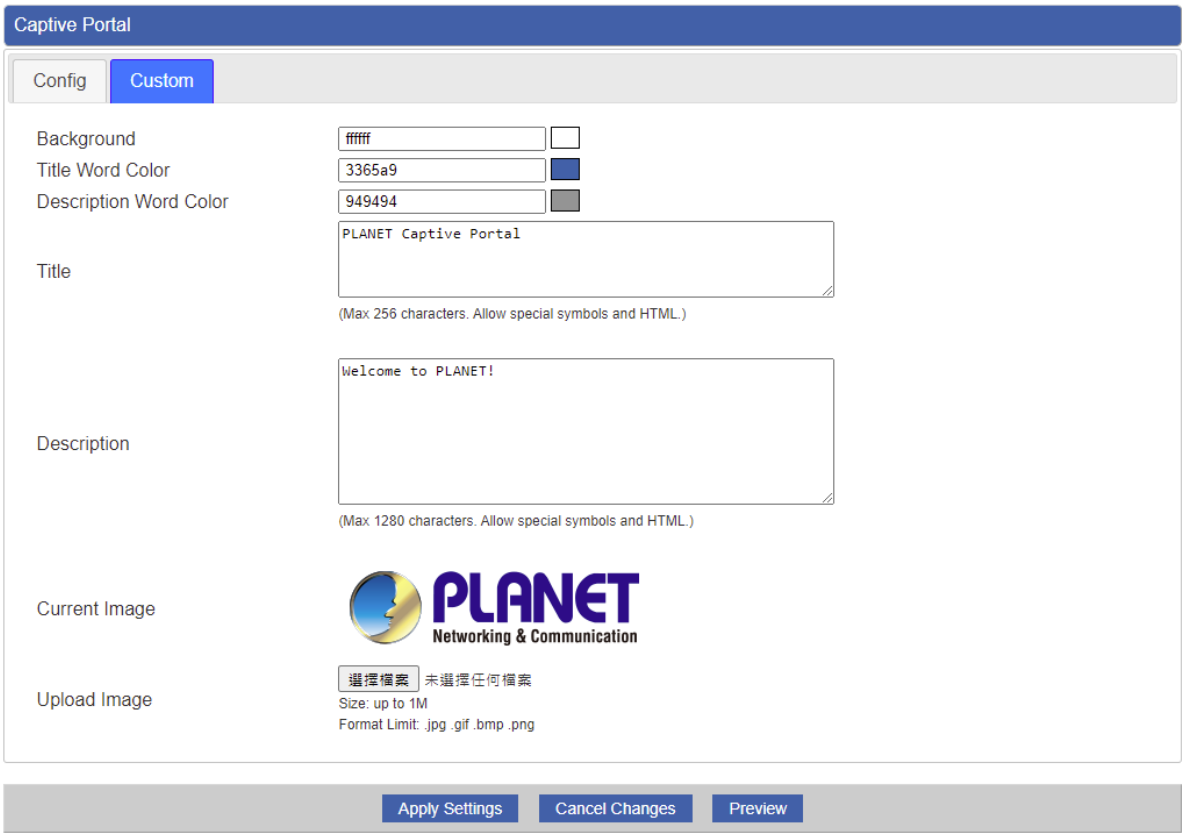
Object	Description
Captive Portal	Disable or enable the Captive Portal function. The default configuration is disabled.

Note

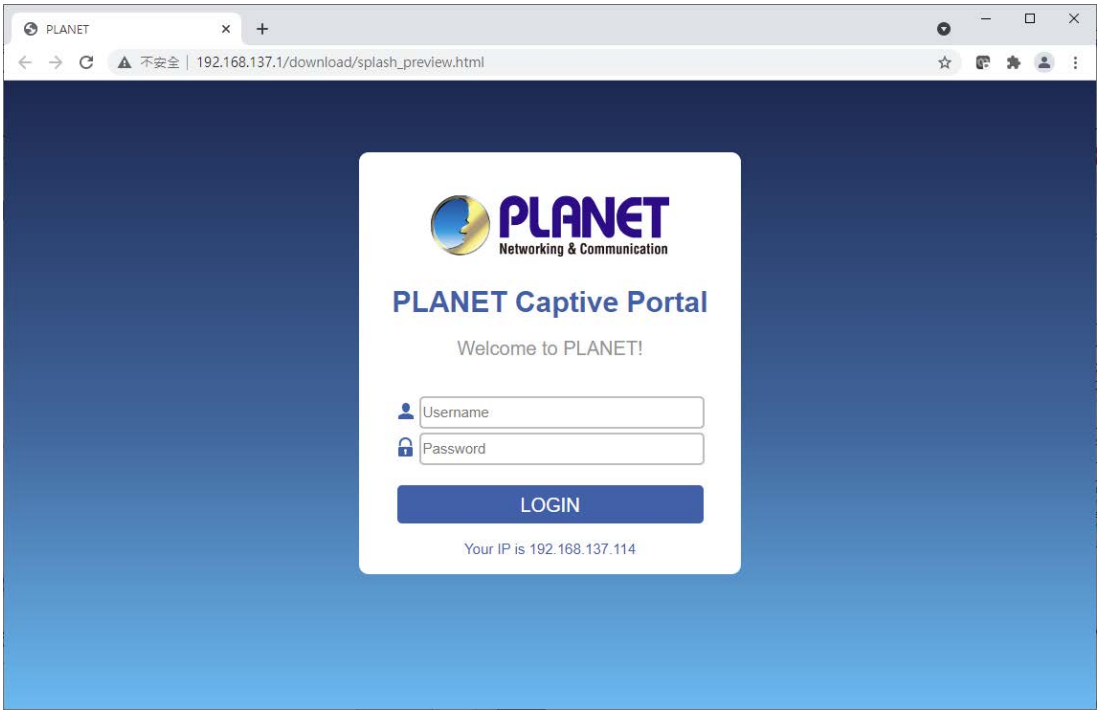
Captive Portal function can be only configured at **Gateway Mode**

Customizing the Custom Captive Portal Web Page

1. Click **Custom**



2. After configure and upload image, click **Apply Settings** button
3. Click **Preview** to check the Captive Portal login page



4.1.10 SNMP

This page provides SNMP setting of the Industrial 802.11ax Wireless AP as shown in Figure 4-21.

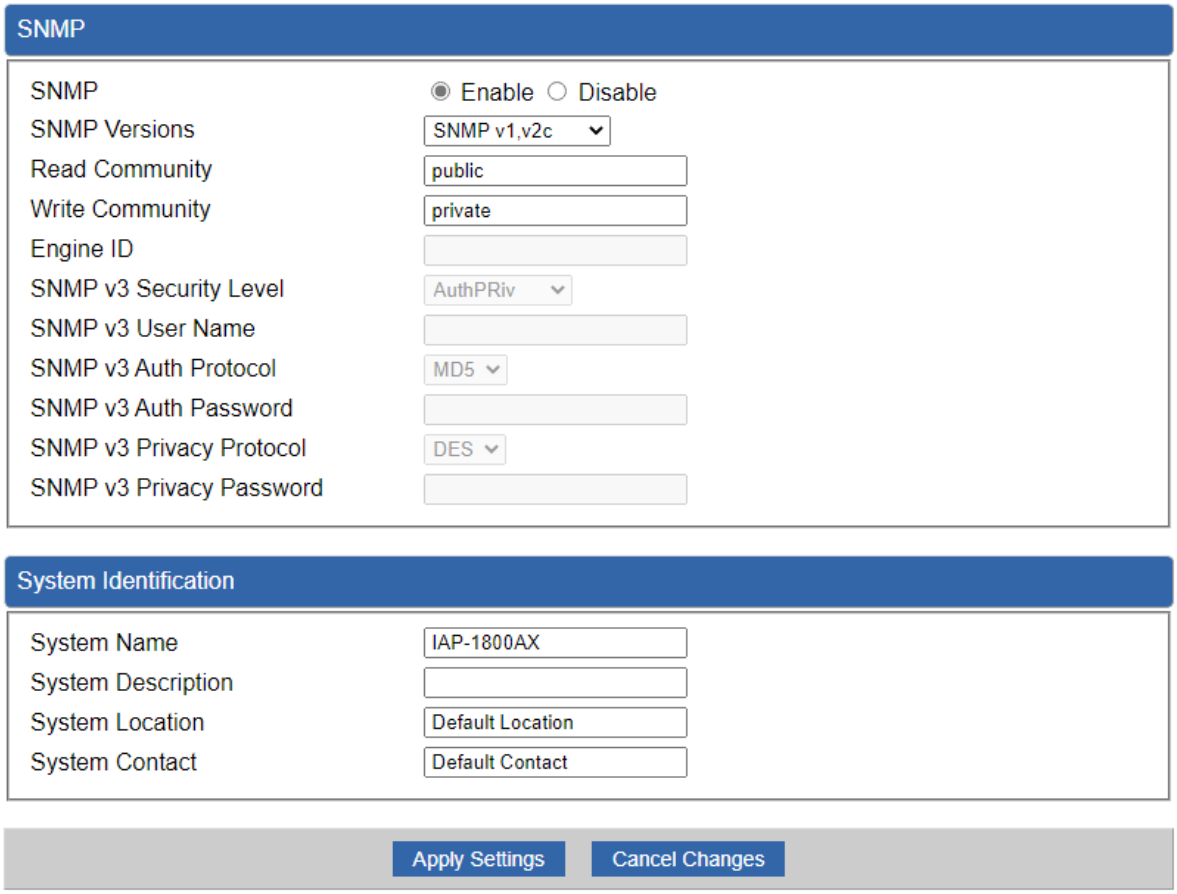


Figure 4-21: SNMP

Object	Description
Enable SNMP	Disable or enable the SNMP function. The default configuration is enabled.
Read/Write Community	Allows entering characters for SNMP Read/Write Community of the Industrial 802.11ax Wireless AP.
System Name	Allows entering characters for system name of the Industrial 802.11ax Wireless AP.
System Location	Allows entering characters for system location of the Industrial 802.11ax Wireless AP.
System Contact	Allows entering characters for system contact of the Industrial 802.11ax Wireless AP.
Apply Settings	Press this button to save and apply changes.
Cancel Changes	Press this button to undo any changes made locally and revert to previously saved values.

4.1.11 NMS

The CloudViewer Server – Internet screens – is shown in Figure 4-22.

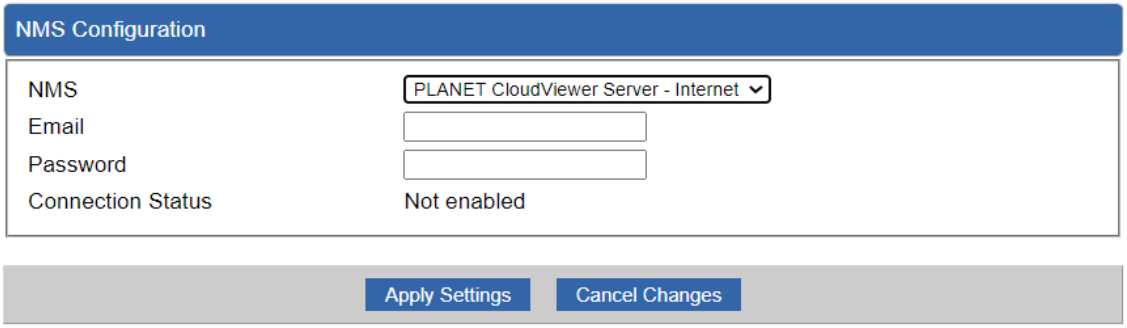
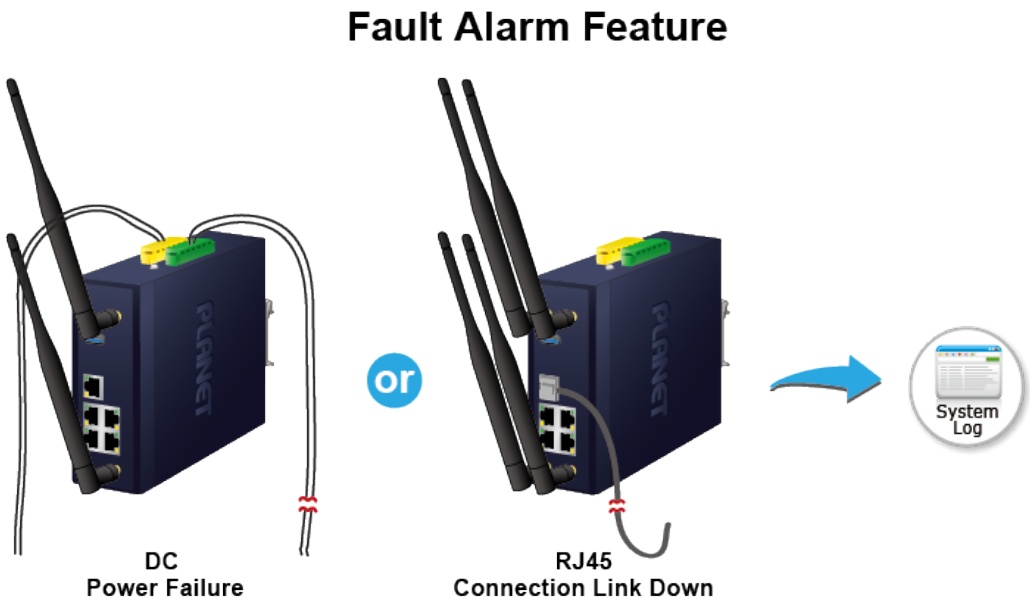


Figure 4-22: CloudViewer Server

Object	Description
Email	The email is registered on CloudViewer Server
Password	The password of your CloudViewer account
Connection Status	Indicates the status of connecting CloudViewer Server

4.1.12 Fault Alarm

The Industrial 802.11ax Wireless AP supports a Fault Alarm feature which can alert the users when there is something wrong with the device. With this ideal feature, the users would not have to waste time finding where the issue is. It will help to save time and human resource.



This page provides fault alarm setting as shown below.

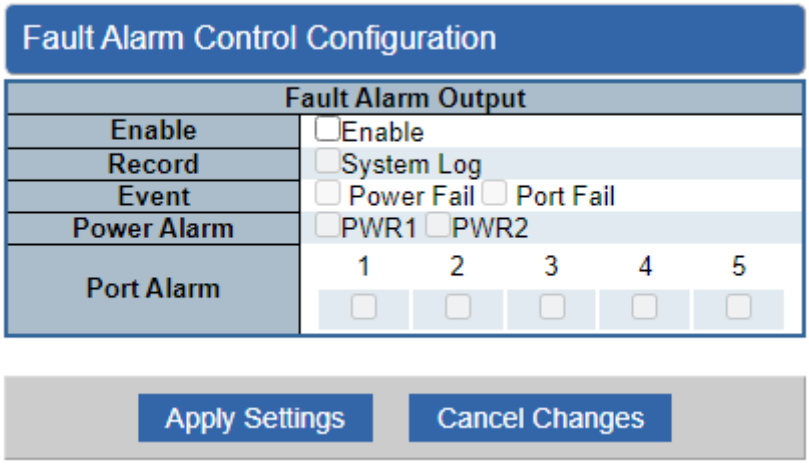


Figure 4-23: Fault Alarm

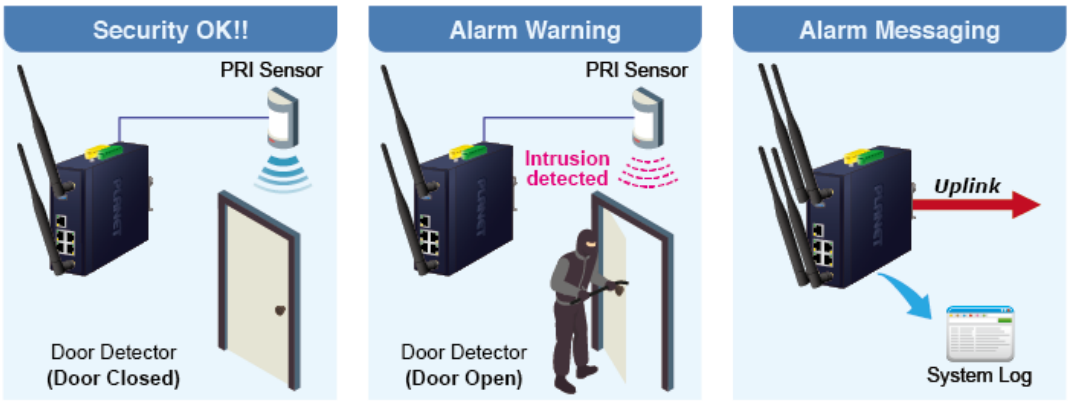
Object	Description
• **Enable**	Controls whether Fault Alarm is enabled.
• **Record**	Controls whether Record is sending System log or SMS.
• **Event**	Controls whether Port Failure or Power Failure or both is/are detected.

• **Power Alarm**	Controls whether faulty PWR1 or faulty PWR2 or both is/are detected.
• **Port Alarm**	Controls which port or all is/are detected for fault.

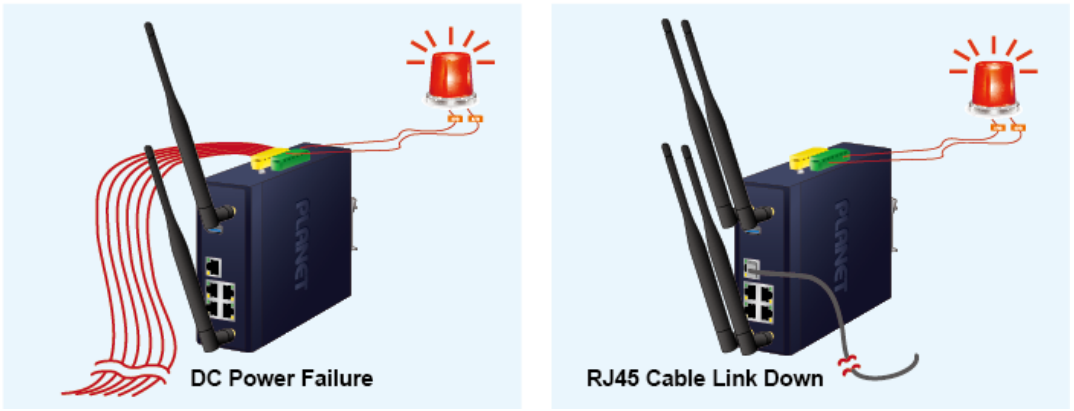
4.1.13 Digital Input / Output

The Industrial 802.11ax Wireless AP supports Digital Input and Digital Output on its upper panel. This external alarm enables users to use Digital Input to detect and log external device status (such as door intrusion detector), and send event alarm to the administrators. The Digital Output could be used to alarm the administrators if the Industrial 802.11ax Wireless AP port shows link down, link up or power failure.

Digital Input



Digital Output



This page provides Digital Input / Output setting as shown below.

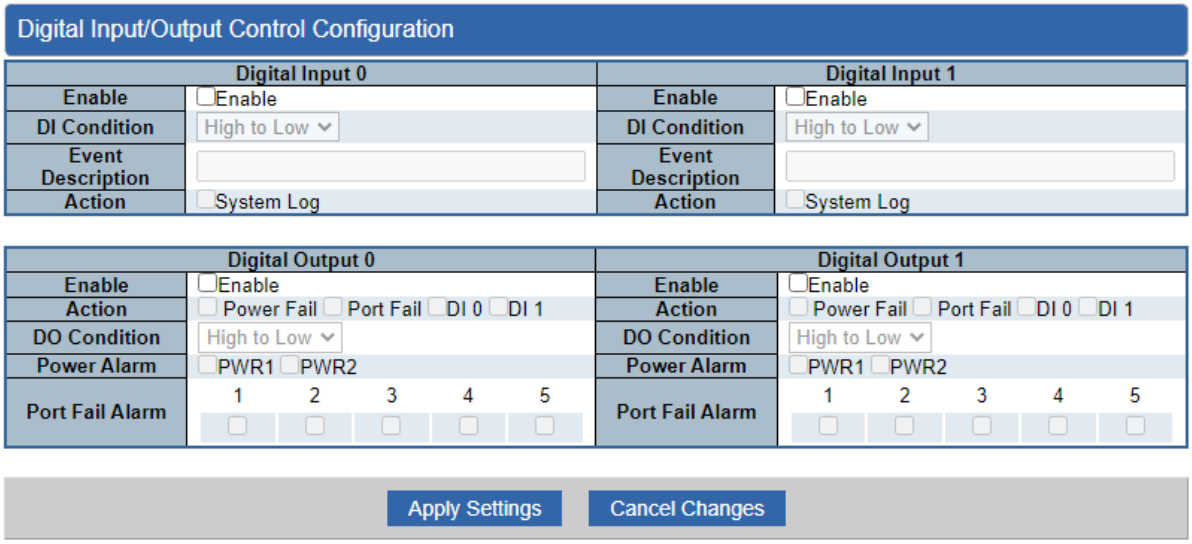


Figure 4-24: Digital Input / Output

Object	Description
• **Enable**	Check the Enable checkbox to enable Digital Input / output function. Uncheck the Enable checkbox to disable Digital input / output function.
• **Condition**	**As Digital Input:** Allows user to select High to Low or Low to High. This means a signal received by system is from High to Low or from Low to High. It will trigger an action that logs a customized message or issue the message from the switch. **As Digital Output:** Allows user to select High to Low or Low to High. This means that when the switch is power-failed or port-failed, the system will issue a High or Low signal to an external device such as an alarm.
• **Event Description**	Allows user to set a customized message for Digital Input function alarm.
• **Action**	**As Digital Input:** Allows user to record alarm message to System log, syslog or issues out via SNMP Trap or SMTP. By default, SNMP Trap and SMTP are disabled. Please enable them first if you want to issue alarm message via them. **As Digital Output:** Allows user to monitor an alarm from port failure, power failure, Digital Input 0 (DI 0) and Digital Input 1(DI 1) which mean if Digital

	Output has detected these events, then Digitial Output would be triggered according to the setting of Condition.
• **Power Alarm**	Allows user to choose which power module that needs to be monitored.
• **Port Alarm**	Allows user to choose which port that needs to be monitored.

4.1.14 Remote Syslog

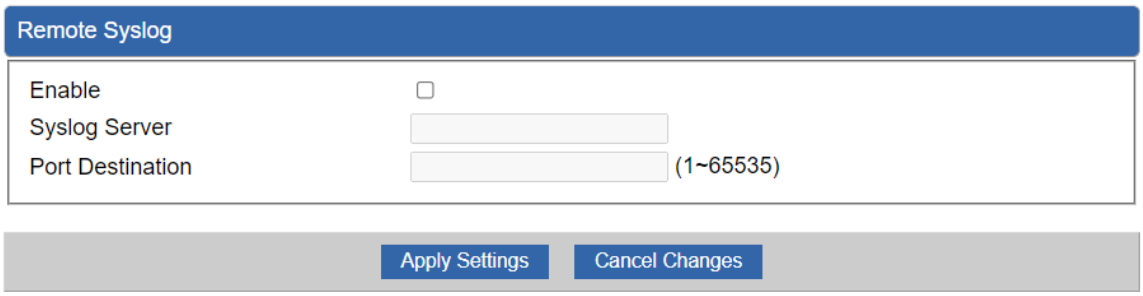


Figure 4-25: Remote Syslog

Object	Description
Enable Remote Syslog	Enable Captive Portal on Industrial 802.11ax Wireless APs

4.1.15 Event Log

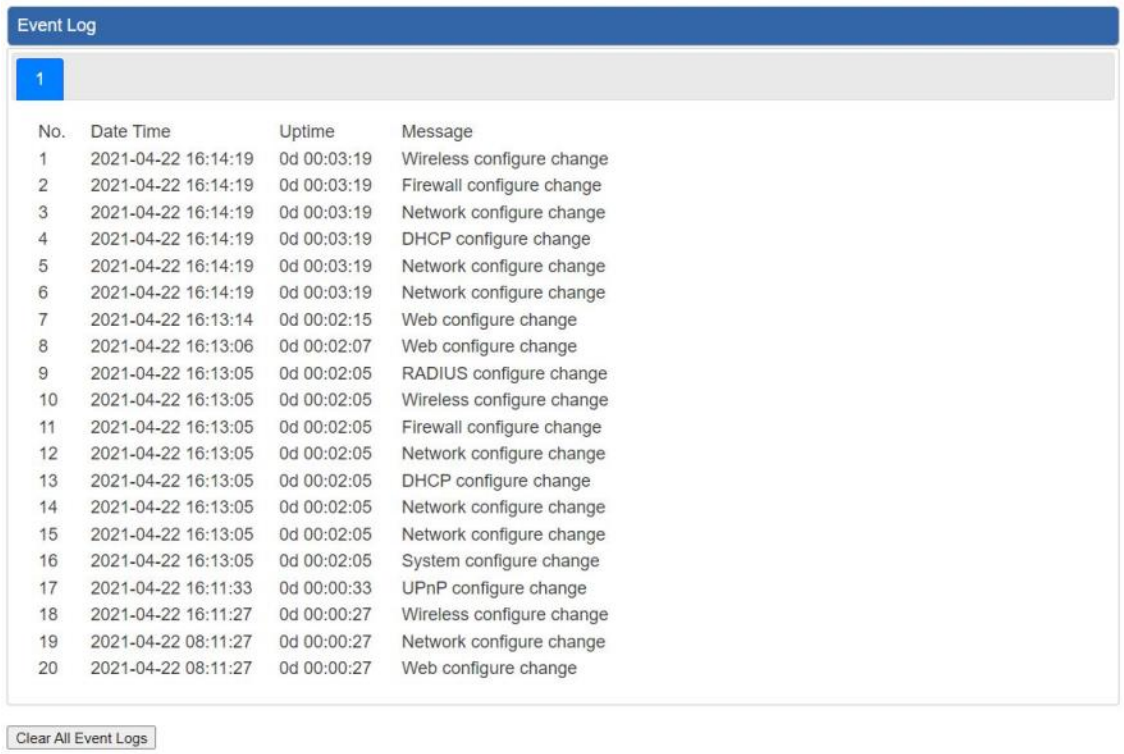


Figure 4-26: Event Log

Object	Description
Event Log	Display Event Log information.

4.2 Network

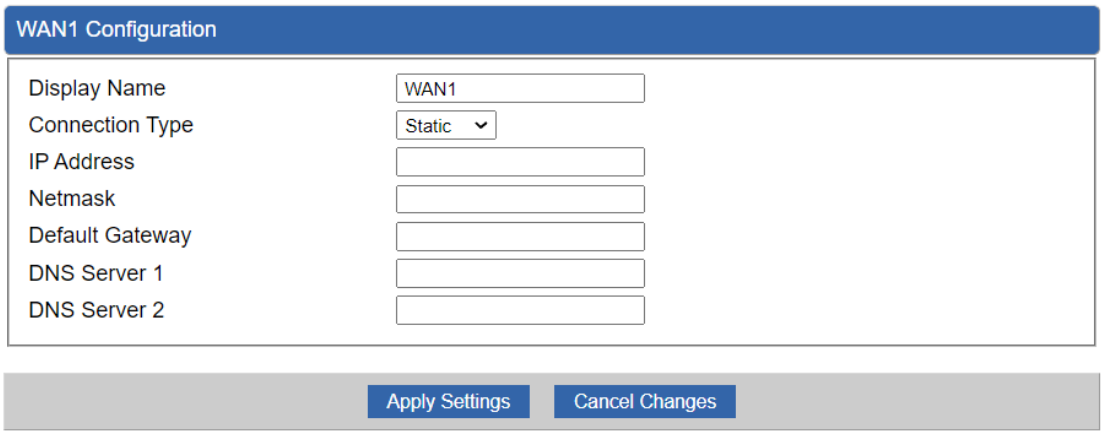
The Network function provides WAN, LAN and network configuration of the Industrial 802.11ax Wireless AP as shown in Figure 4-27.

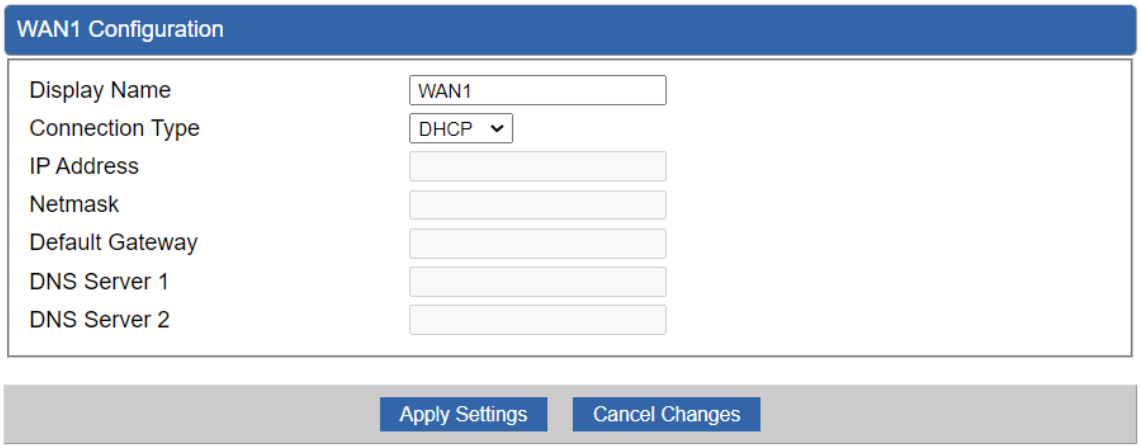
Figure 4-27: Network Menu

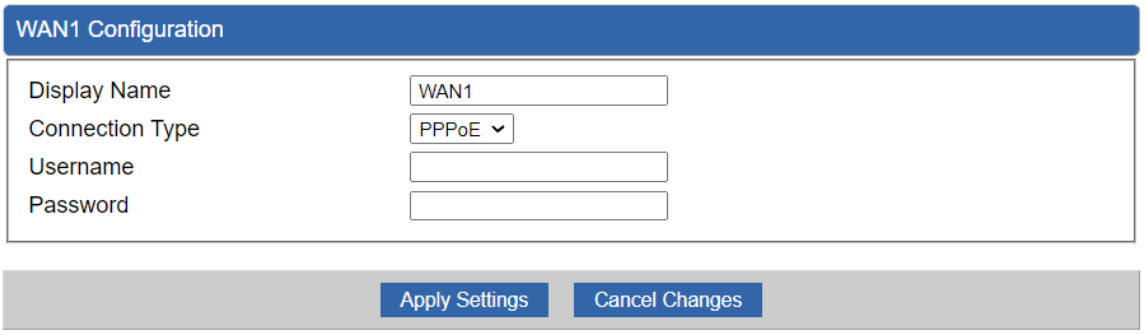
Object	Description
WAN	Allows setting WAN interface.
LAN	Allows setting LAN interface.
UPnP	Disable or enable the UPnP function. The default configuration is disabled.
Routing	Allows setting Route.
RIP	Disable or enable the RIP function. The default configuration is disabled.
OSPF	Disable or enable the OSPF function. The default configuration is disabled.
IGMP	Disable or enable the IGMP function. The default configuration is disabled.
IPv6	Allows setting IPv6 WAN interface.
DHCP	Allows setting DHCP Server.
DDNS	Allows setting DDNS and PLANET DDNS.

4.2.1 WAN

This page is used to configure the parameters for Internet network which connects to the WAN port of the Industrial 802.11ax Wireless AP as shown in Figure 4-28. Here you may select the access method by clicking the item value of WAN access type.







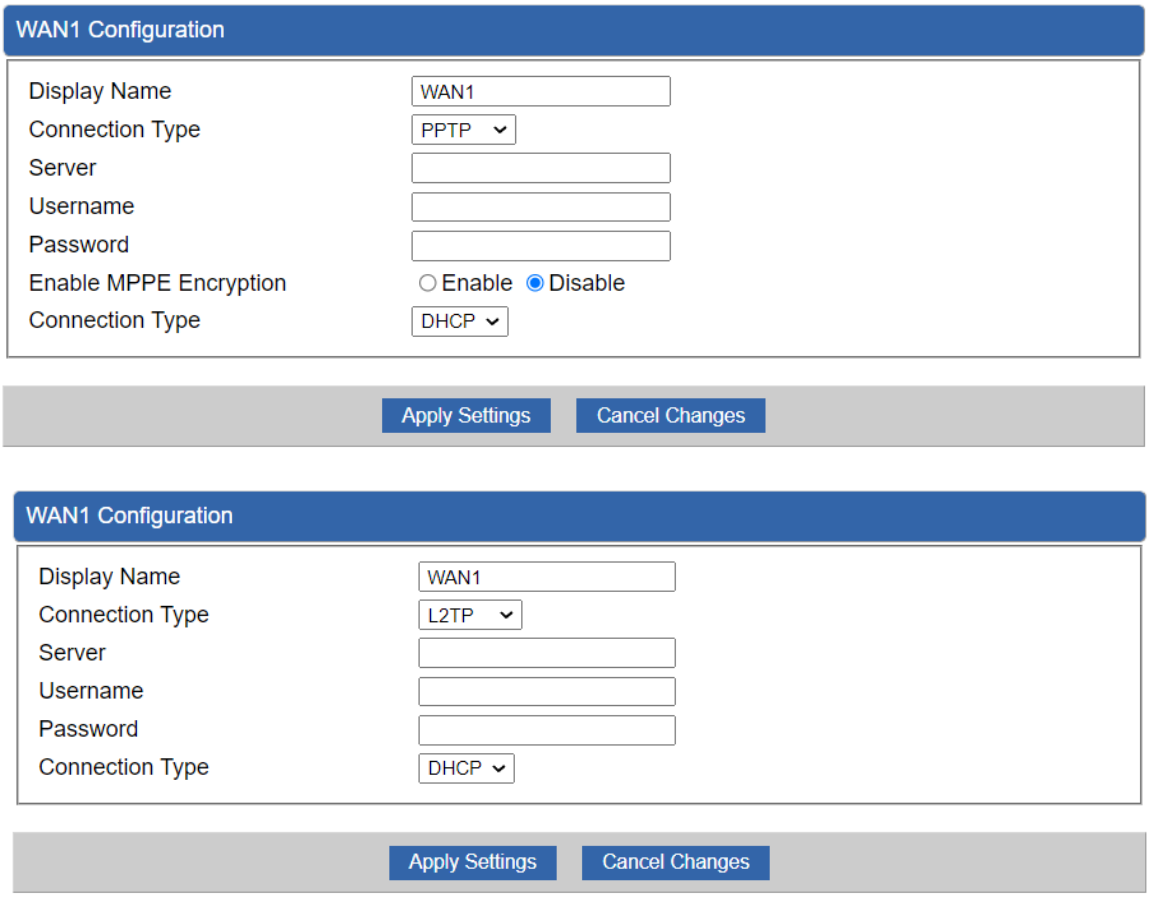


Figure 4-28: WAN

Object	Description	
WAN Access Type	Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.	
	Static	Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet Service Provider). You will need to enter the IP address, Netmask, Gateway, and DNS Server provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which are four octets separated by a dot (x.x.x.x). The Industrial 802.11ax Wireless AP will not accept the IP address if it is not in this format. **IP Address** Enter the IP address assigned by your ISP. **Netmask** Enter the Subnet Mask assigned by your ISP. **Gateway**

Object		Description
		Enter the Gateway assigned by your ISP. **DNS Server** The DNS server information will be supplied by your ISP.
	DHCP	Select DHCP Client to obtain IP Address information automatically from your ISP.
	PPPoE	Select PPPOE if your ISP is using a PPPoE connection and provide you with PPPoE user name and password info.
	PPTP	Enable or disable PPTP to pass through PPTP communication data.
	L2TP	Enable or disable L2TP to pass through L2TP communication data.

Note

WAN IP, whether obtained automatically or specified manually, should NOT be on the same IP net segment as the LAN IP; otherwise, the Industrial 802.11ax Wireless AP will not work properly. In case of emergency, press the hardware-based "Reset" button.

4.2.2 LAN

This page is used to configure the parameters for local area network which connects to the LAN port of your Industrial 802.11ax Wireless AP as shown in Figure 4-29. Here you may change the settings for IP address, subnet mask, DHCP, etc.

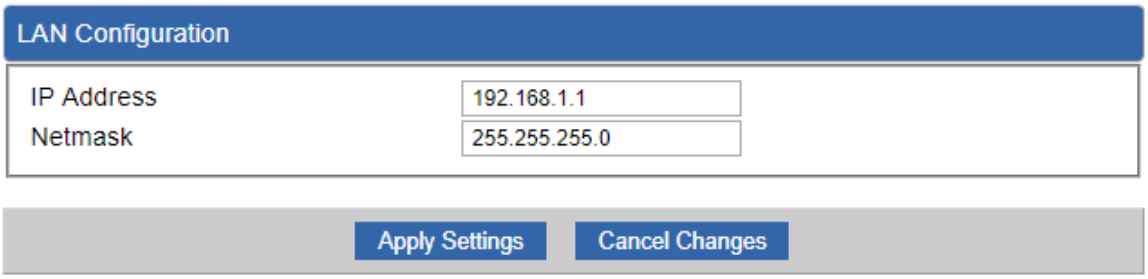


Figure 4-29: LAN Setup

Object	Description
IP Address	The LAN IP address of the Industrial 802.11ax Wireless AP and default is **192.168.1.1**.
Net Mask	Default is **255.255.255.0**.

4.2.3 UpnP

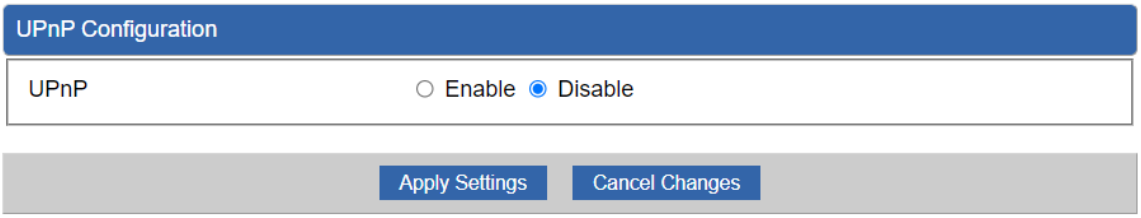


Figure 4-30: UpnP

Object	Description
UpnP	Set the function as enable or disable

4.2.4 Routing

Please refer to the following sections for the details as shown in Figures 4-31 and 4-32.

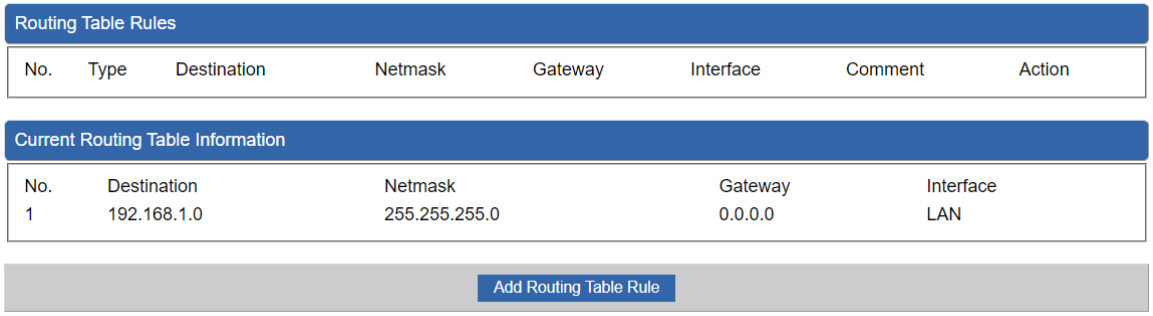


Figure 4-31: Routing table

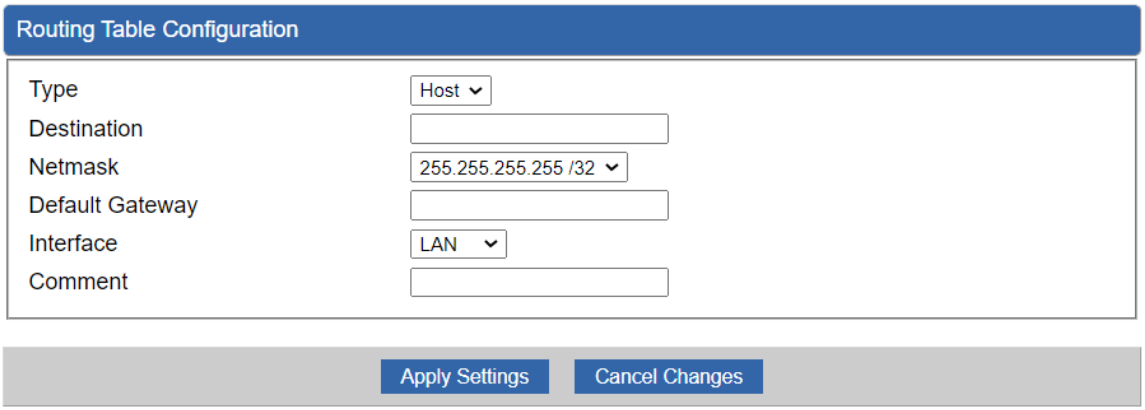


Figure 4-32: Routing setup

Routing tables contain a list of IP addresses. Each IP address identifies a remote Industrial 802.11ax Wireless AP (or other network gateway) that the local Industrial 802.11ax Wireless AP is configured to recognize. For each IP address, the routing table additionally stores a network mask and other data that specifies the destination IP address ranges that remote device will accept.

Object	Description
Type	There are two types: Host and Net. When the Net type is selected, user does not need to input the Gateway.
Destination	The network or host IP address desired to access.
Netmask	The subnet mask of destination IP.
Default Gateway	The gateway is the Industrial 802.11ax Wireless AP or host's IP address to which packet was sent. It must be the same network segment with the WAN or LAN port.
Interface	Select the interface that the IP packet must use to transmit out of the Industrial 802.11ax Wireless AP when this route is used.
Comment	Enter any words for recognition.

4.2.5 RIP

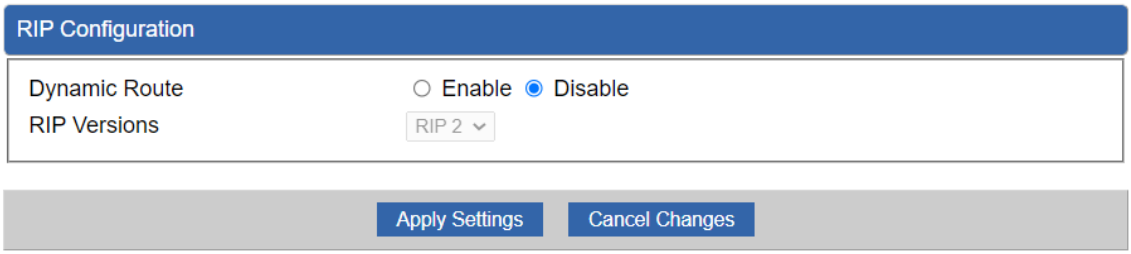


Figure 4-33: RIP

Object	Description
Dynamic Route	Disable or enable the RIP function.
RIP Versions	Set RIP Versions.

4.2.6 OSPF

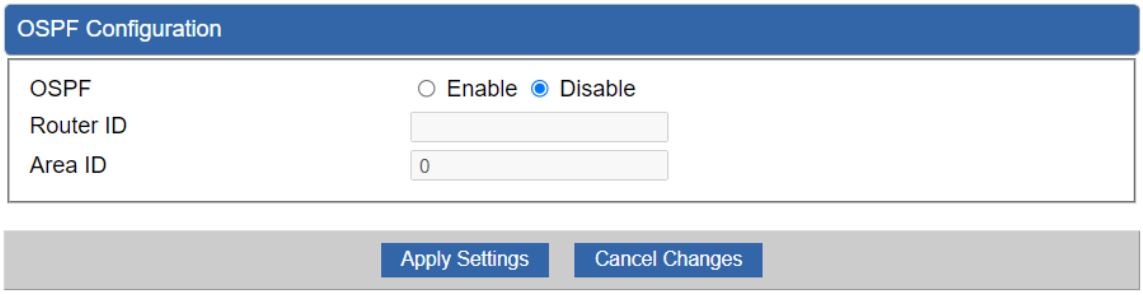


Figure 4-34: OSPF

Object	Description
OSPF	Enable the OSPF function.
Router ID	Set Router ID.
Area ID	Set Area ID.

4.2.7 IGMP

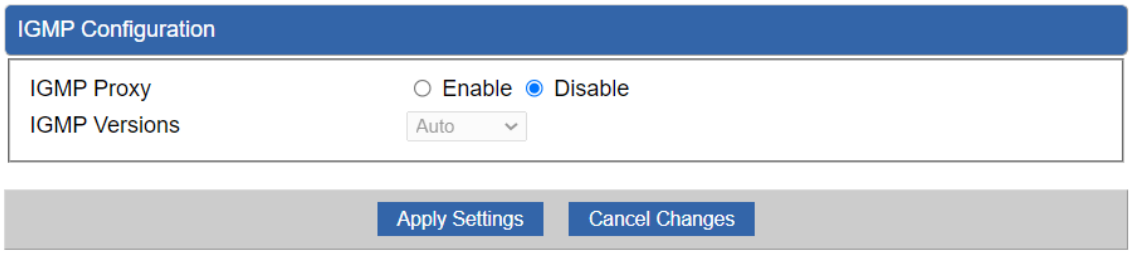
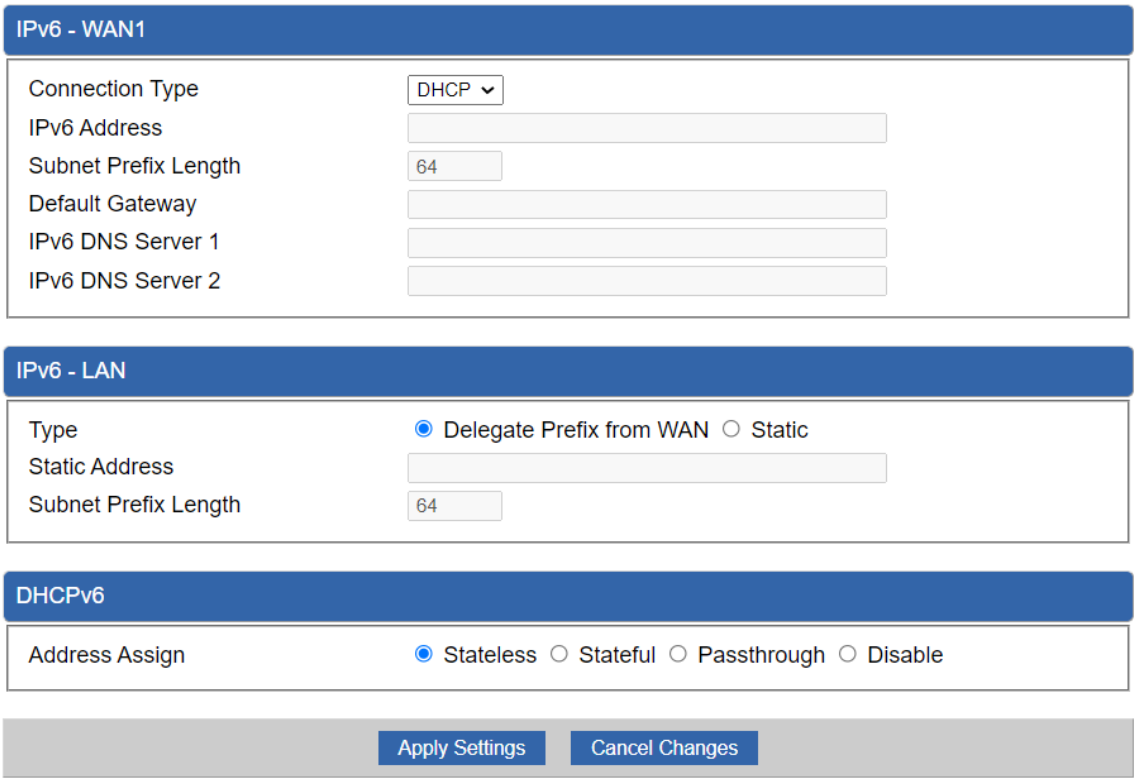


Figure 4-35: IGMP

Object	Description
IGMP	Enable the IGMP function.
IGMP Versions	Select the GMP Versions

4.2.8 IPv6

This page is used to configure parameter for IPv6 internet network which connects to WAN port of the Industrial 802.11ax Wireless AP as shown in Figure 4-36. It allows you to enable IPv6 function and set up the parameters of the Industrial 802.11ax Wireless AP's WAN. In this setting you may change WAN connection type and other settings.



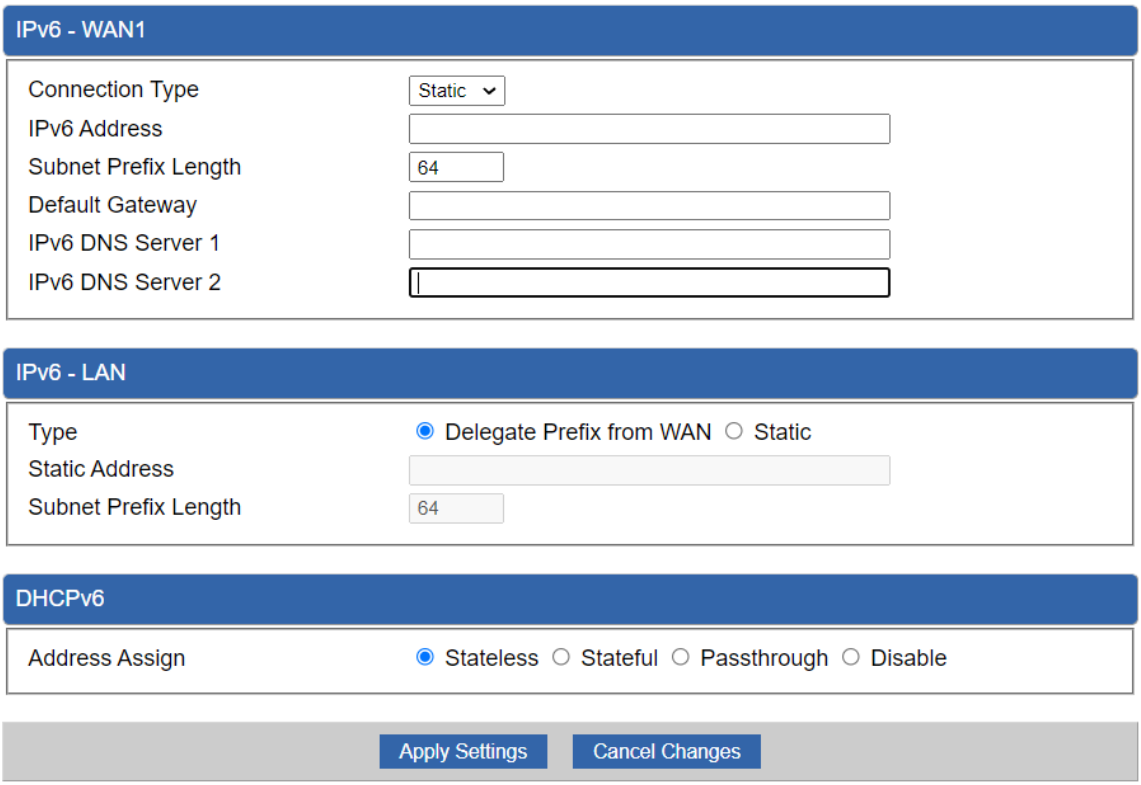


Figure 4-36: IPv6 WAN setup

Object	Description
Connection Type	Select IPv6 WAN type either by using DHCP or Static.
IPv6 Address	Enter the WAN IPv6 address.
Subnet Prefix Length	Enter the subnet prefix length.
Default Gateway	Enter the default gateway of the WAN port.
IPv6 DNS Server 1	Input a specific DNS server.
IPv6 DNS Server 2	Input a specific DNS server.

4.2.9 DHCP

The DHCP service allows you to control the IP address configuration of all your network devices. When a client (host or other device such as networked printer, etc.) joins your network it will automatically get a valid IP address from a range of addresses and other settings from the DHCP service. The client must be configured to use DHCP; this is something called "automatic network configuration" and is often the default setting. The setup is shown in Figure 4-37.

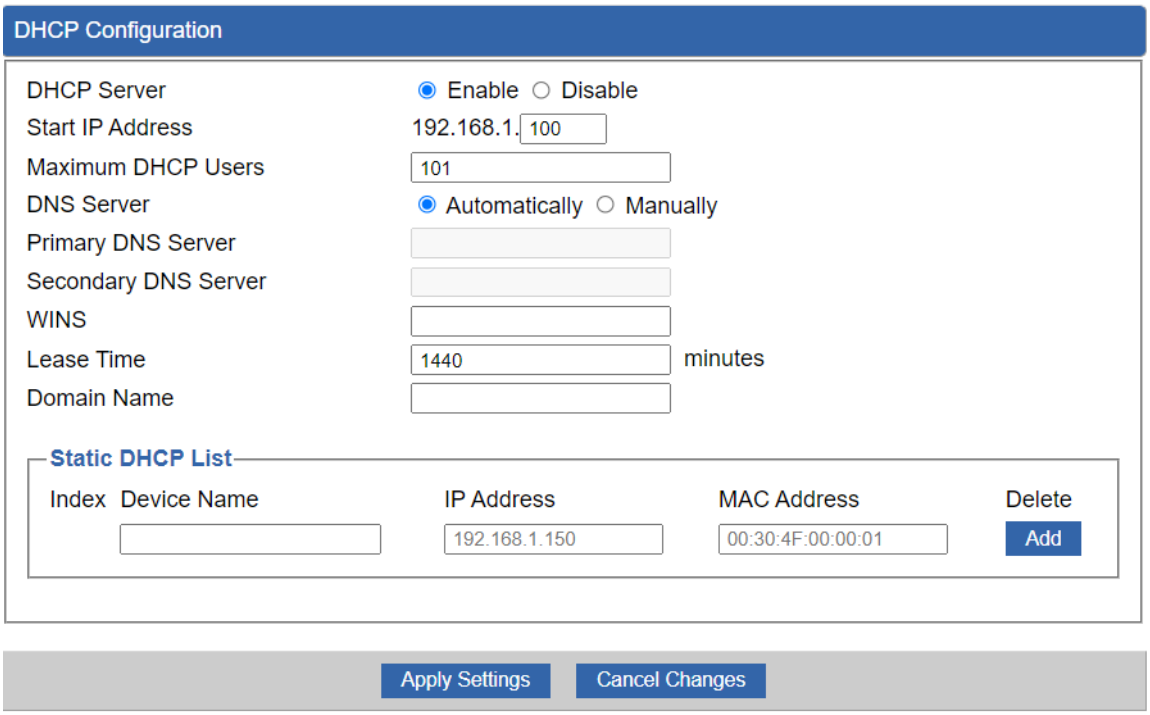


Figure 4-37: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the Industrial 802.11ax Wireless AP will assign IP addresses to the DHCP clients automatically. If user needs to disable the function, please set it as disable.
Start IP Address	By default, the start IP address is 192.168.1.100. Please do not set it to the same IP address of the Industrial 802.11ax Wireless AP.
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the Industrial 802.11ax Wireless AP will provide DHCP client with IP address from 192.168.1.100 to 192.168.1.200 when the start IP address is 192.168.1.100.
DNS Server	By default, it is set as Automatically, and the DNS server is the Industrial 802.11ax Wireless AP's LAN IP address.

Object	Description
	If user needs to use specific DNS server, please set it as Manually, and then input a specific DNS server.
Primary/Secondary DNS Server	Input a specific DNS server.
WINS	Input a WINS server if needed.
Lease Time	Set the time for using one assigned IP. After the lease time, the DHCP client will need to get new IP addresses from the Industrial 802.11ax Wireless AP. Default is 1440 minutes.
Domain Name	Input a domain name for the Industrial 802.11ax Wireless AP.

4.2.10 DDNS

The Industrial 802.11ax Wireless AP offers the DDNS (Dynamic Domain Name System) feature, which allows the hosting of a website, FTP server, or e-mail server with a fixed domain name (named by yourself) and a dynamic IP address, and then your friends can connect to your server by entering your domain name no matter what your IP address is. Before using this feature, you need to sign up for DDNS service providers such as **PLANET DDNS (**http://www.planetddns.com**)** and set up the domain name of your choice.

PLANET DDNS website provides a free DDNS (Dynamic Domain Name Server) service for PLANET devices. Whether the IP address used on your PLANET device supporting DDNS service is fixed or dynamic, you can easily connect the devices anywhere on the Internet with a meaningful or easy-to-remember name you gave. PLANET DDNS provides two types of DDNS services. One is **PLANET DDNS** and the other is **PLANET Easy DDNS** as shown in Figure 4-38.

PLANET DDNS

For example, you've just installed a PLANET IP camera with dynamic IP like 210.66.155.93 in the network. You can name this device as “Mycam1” and register a domain as Mycam1.planetddns.com at PLANET DDNS (http://www.planetddns.com). Thus, you don't need to memorize the exact IP address but just the URL link: Mycam1.planetddns.com.

PLANET Easy DDNS

PLANET Easy DDNS is an easy way to help user to get your Domain Name with just one click. You can just log in to the Web Management Interface of your devices, say, your Industrial 802.11ax Wireless AP, and check the DDNS menu and just enable it. You don’t need to go to http://www.planetddns.com to apply for a new account. Once you enabled the Easy DDNS, your

PLANET Network Device will use the format PLxxxxxx where xxxxxx is the last 6 characters of your MAC address that can be found on the Web page or bottom label of the device. (For example, if the Industrial 802.11ax Wireless AP's MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)

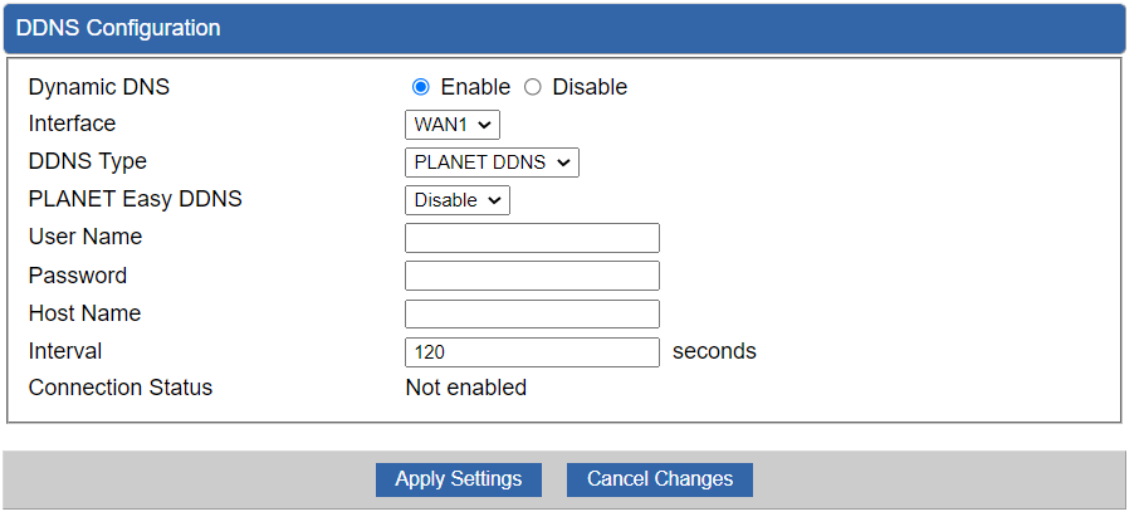


Figure 4-38: PLANET DDNS

Object	Description
DDNS Service	By default, the DDNS service is disabled. If user needs to enable the function, please set it as enable.
Interface	User is able to select the interface for DDNS service. By default, the interface is WAN 1.
DDNS Type	There are three options: 1. PLANET DDNS: Activate PLANET DDNS service. 2. DynDNS: Activate DynDNS service. 3. NOIP: Activate NOIP service. Note that please first register with the DDNS service and set up the domain name of your choice to begin using it.
Easy DDNS	When the PLANET DDNS service is activated, user is able to select to enable or disable Easy DDNS. When this function is enabled, DDNS hostname will appear automatically. User doesn't go to http://www.planetddns.com to apply for a new account.
User Name	The user name is used to log into DDNS service.
Password	The password is used to log into DDNS service.

Object	Description
Host Name	The host name as registered with your DDNS provider.
Interval	Set the update interval of the DDNS function.
Connection Status	Show the connection status of the DDNS function.

4.3 Security

The Security menu provides Firewall, Access Filtering and other functions as shown in Figure 4-39. Please refer to the following sections for the details.

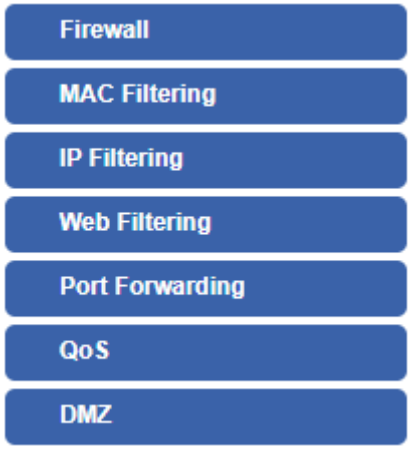


Figure 4-39: Security menu

Object	Description
Firewall	Allows setting DoS (Denial of Service) protection as enable.
MAC Filtering	Allows setting MAC Filtering.
IP Filtering	Allows setting IP Filtering.
Web Filtering	Allows setting Web Filtering.
Port Forwarding	Allows setting Port Forwarding.
QoS	Allows setting Qos.
DMZ	Allows setting DMZ.

4.3.1 Firewall

A "Denial-of-Service" (DoS) attack is characterized by an explicit attempt by hackers to prevent legitimate users of a service from using that service. The Industrial 802.11ax Wireless AP can prevent specific DoS attacks as shown in Figure 4-40.

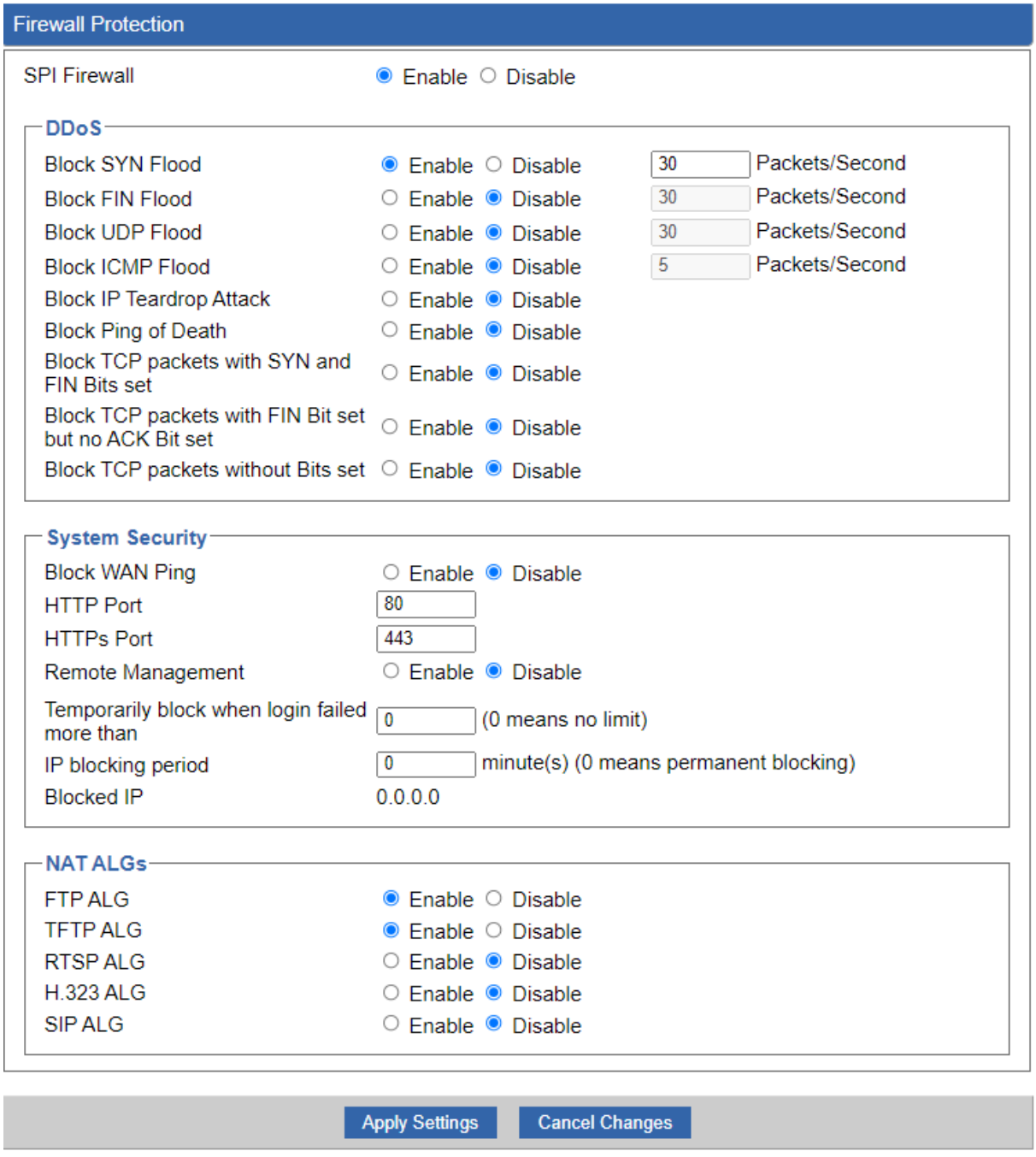


Figure 4-40: Firewall

Object	Description
SPI Firewall	The SPI Firewall prevents attack and improper access to network resources. The default configuration is enabled.

Block SYN Flood	SYN Flood is a popular attack way. DoS and DDoS are TCP protocols. Hackers like using this method to make a fake connection that involves the CPU, memory, and so on. The default configuration is enabled.
Block FIN Flood	If the function is enabled, when the number of the current FIN packets is beyond the set value, the Industrial 802.11ax Wireless AP will start the blocking function immediately. The default configuration is disabled.
Block UDP Flood	If the function is enabled, when the number of the current UPD-FLOOD packets is beyond the set value, the Industrial 802.11ax Wireless AP will start the blocking function immediately. The default configuration is disabled.
Block ICMP Flood	ICMP is kind of a pack of TCP/IP; its important function is to transfer simple signal on the Internet. There are two normal attack ways which hackers like to use, Ping of Death and Smurf attack. The default configuration is disabled.
IP TearDrop	If the function is enabled, the Industrial 802.11ax Wireless AP will block Teardrop attack that is targeting on TCP/IP fragmentation reassembly codes.
Ping Of Death	If the function is enabled, the Industrial 802.11ax Wireless AP will block Ping of Death attack that aims to disrupt a targeted machine by sending a packet larger than the maximum allowable size causing the target machine to freeze or crash.
TCP packets with SYN and FIN Bits set	Set the function as enable or disable.
TCP packets with FIN Bit set but no ACK Bit set	Set the function as enable or disable.
TCP packets without Bits set	Set the function as enable or disable.
Block WAN Ping	Enable the function to allow the Ping access from the Internet network. The default configuration is disabled.
HTTP Port	The default is 80.
HTTPs Port	The default is 443.
Remote Management	Enable the function to allow the web server access of the Industrial 802.11ax Wireless AP from the Internet network. The default configuration is disabled.

Temporarily block when login failed	The default is 0. (0 means no limit).
IP blocking period	The default is 0. (0 means permanent blocking).
Blocked IP	0.0.0.0.
FTP ALG	Set the function as enable or disable.
TFTP ALG	Set the function as enable or disable.
RTSP ALG	Set the function as enable or disable.
H.323 ALG	Set the function as enable or disable.
SIP ALG	Set the function as enable or disable.

4.3.2 MAC Filtering

Entries in this table are used to restrict certain types of data packets from your local network or Internet through the Industrial 802.11ax Wireless AP. Use of such filters can be helpful in securing or restricting your local network as shown in Figure 4-41.

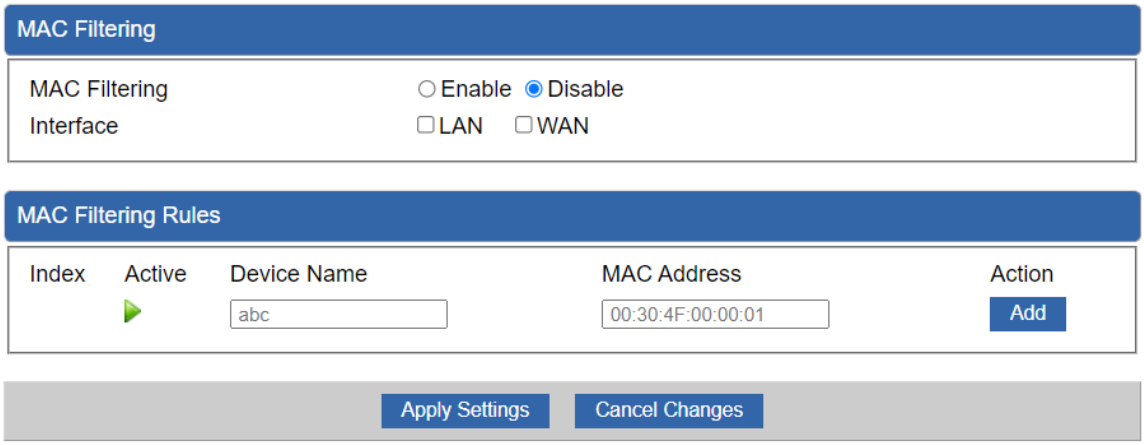


Figure 4-41: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. When the function is enabled, the Industrial 802.11ax Wireless AP will block traffic of the MAC address on the list.
Interface	Select the function works on LAN, WAN or both. If you want to block a LAN device's MAC address, please select LAN, vice versa.
MAC Address	Input a MAC address you want to control, such as A8:F7:E0:00:06:62.
Add	When you input a MAC address, please click the "Add" button to add it into the list.

4.4.3 IP Filtering

IP Filtering is used to deny LAN users from accessing the public IP address on internet as shown in Figure 4-42. To begin blocking access to an IP address, enable IP Filtering and enter the IP address of the web site you wish to block.

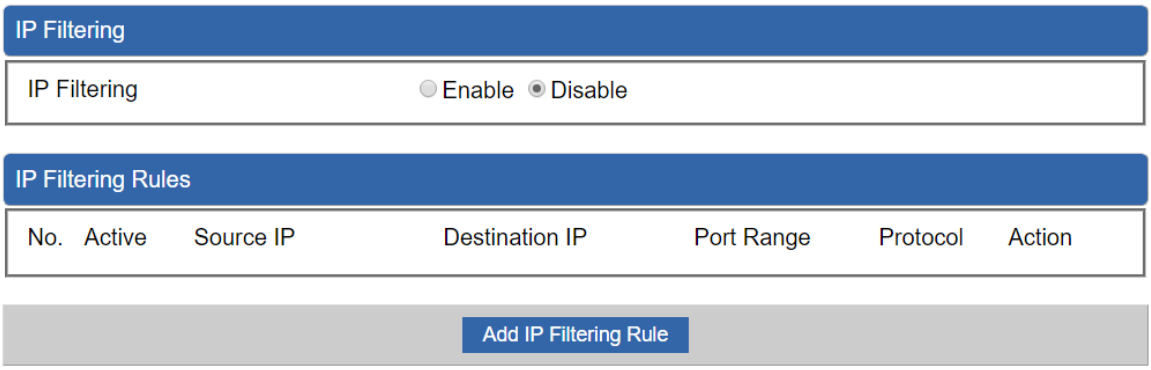


Figure 4-42: IP Filtering

Object	Description
IP Filtering	Set the function as enable or disable.
Add IP Filtering Rule	Go to the Add Filtering Rule page to add a new rule.

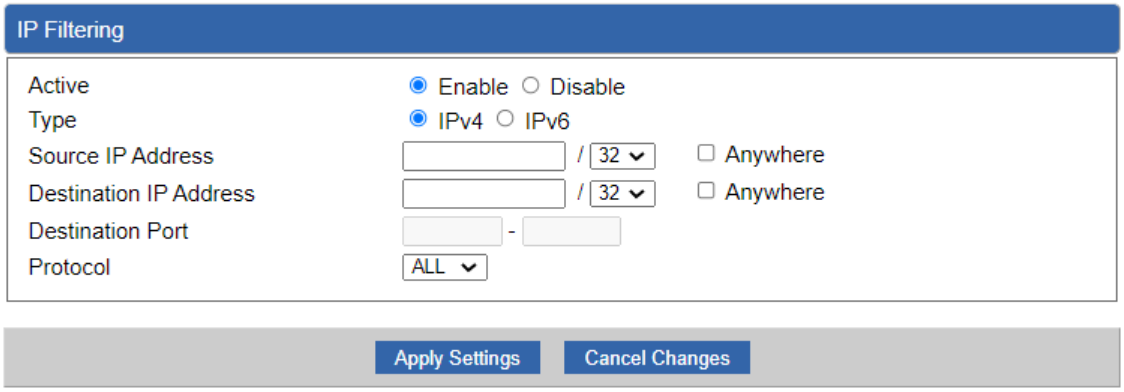


Figure 4-43: IP Filter Rule Setting

Object	Description
Active	Set the rule as enable or disable.
Type	Set the type as IPv4 or IPv6.
Source IP Address	Input the IP address of LAN user (such as PC or laptop) which you want to control.
Anywhere (of source IP Address)	Check the box if you want to control all LAN users.

Object	Description
Destination IP Address	Input the IP address of web site which you want to block.
Anywhere (of destination IP Address)	Check the box if you want to control all web sites, meaning the LAN user can't visit any web site.
Destination Port	Input the port of destination IP Address which you want to block. Leave it as blank if you want to block all ports of the web site.
Protocol	Select the protocol type (TCP, UDP or all). If you are unsure, please leave it to the default all protocol.

4.3.4 Web Filtering

Web filtering is used to deny LAN users from accessing the internet as shown in Figure 4-44. Block those URLs which contain keywords listed below.

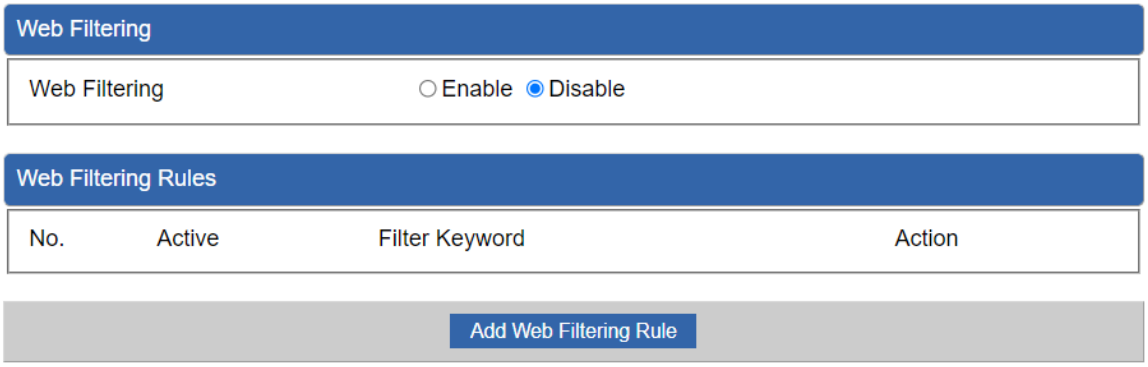


Figure 4-44: Web Filtering

Object	Description
Web Filtering	Set the function as enable or disable.
Add Web Filtering Rule	Go to the Add Web Filtering Rule page to add a new rule.

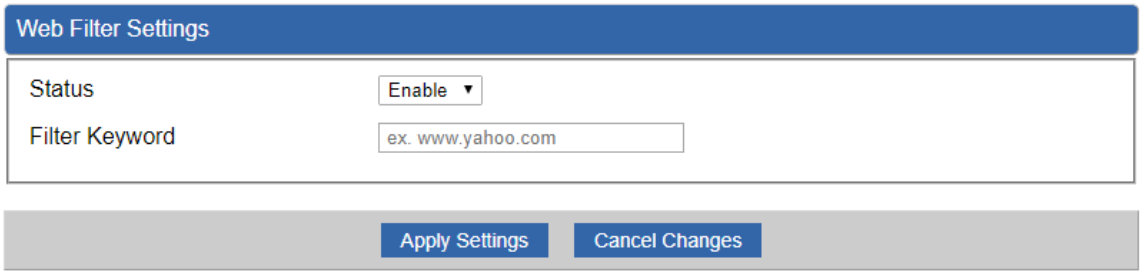


Figure 4-45: Web Filtering Rule Setting

Object	Description
Status	Set the rule as enable or disable.
Filter Keyword	Input the URL address that you want to filter, such as www.yahoo.com.

4.3.5 Port Forwarding

Entries in this table allow you to automatically redirect common network services to a specific machine behind the NAT firewall as shown in Figure 4-46. These settings are only necessary if you wish to host some sort of server like a web server or mail server on the private local network behind your Industrial 802.11ax Wireless AP's NAT firewall.

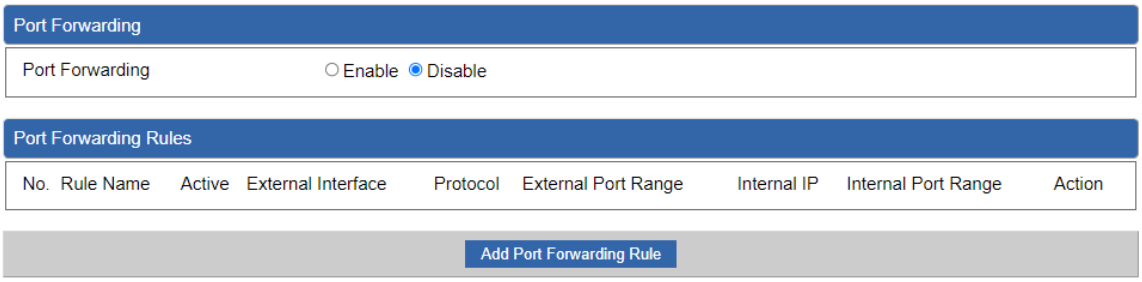


Figure 4-46: Port Forwarding

Object	Description
Port Forwarding	Set the function as enable or disable.
Add Port Forwarding Rule	Go to the Add Port Forwarding Rule page to add a new rule.

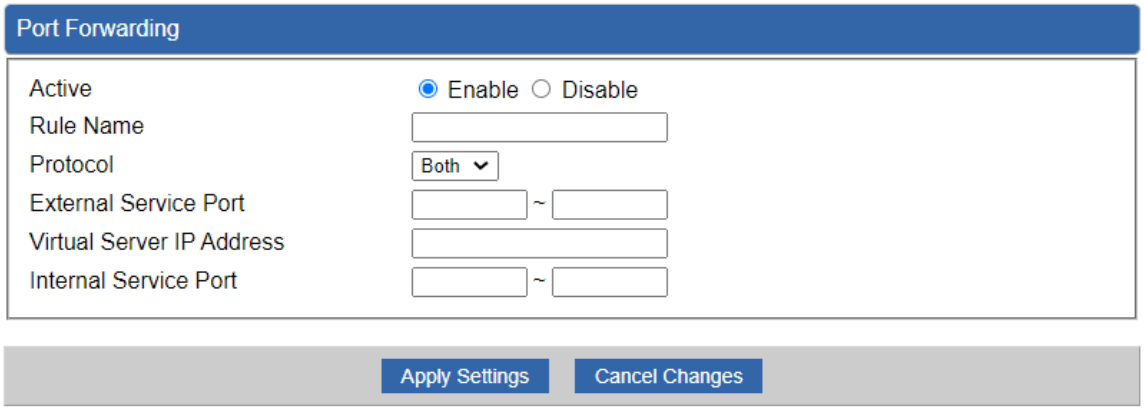


Figure 4-47: Port Forwarding Rule Setting

Object	Description
Active	Set the function as enable or disable.
Rule Name	Enter any words for recognition.
Protocol	Select the protocol type (TCP, UDP or both). If you are unsure, please leave it to the default both protocols.
External Service Port	Enter the external ports you want to control. For TCP and UDP services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both

Object	Description
	the start and finish fields.
Virtual Server IP Address	Enter the local IP address.
Internal Service Port	Enter local ports you want to control. For TCP and UDP Services, enter the beginning of the range of port numbers used by the service. If the service uses a single port number, enter it in both the start and finish fields.

4.3.6 QoS

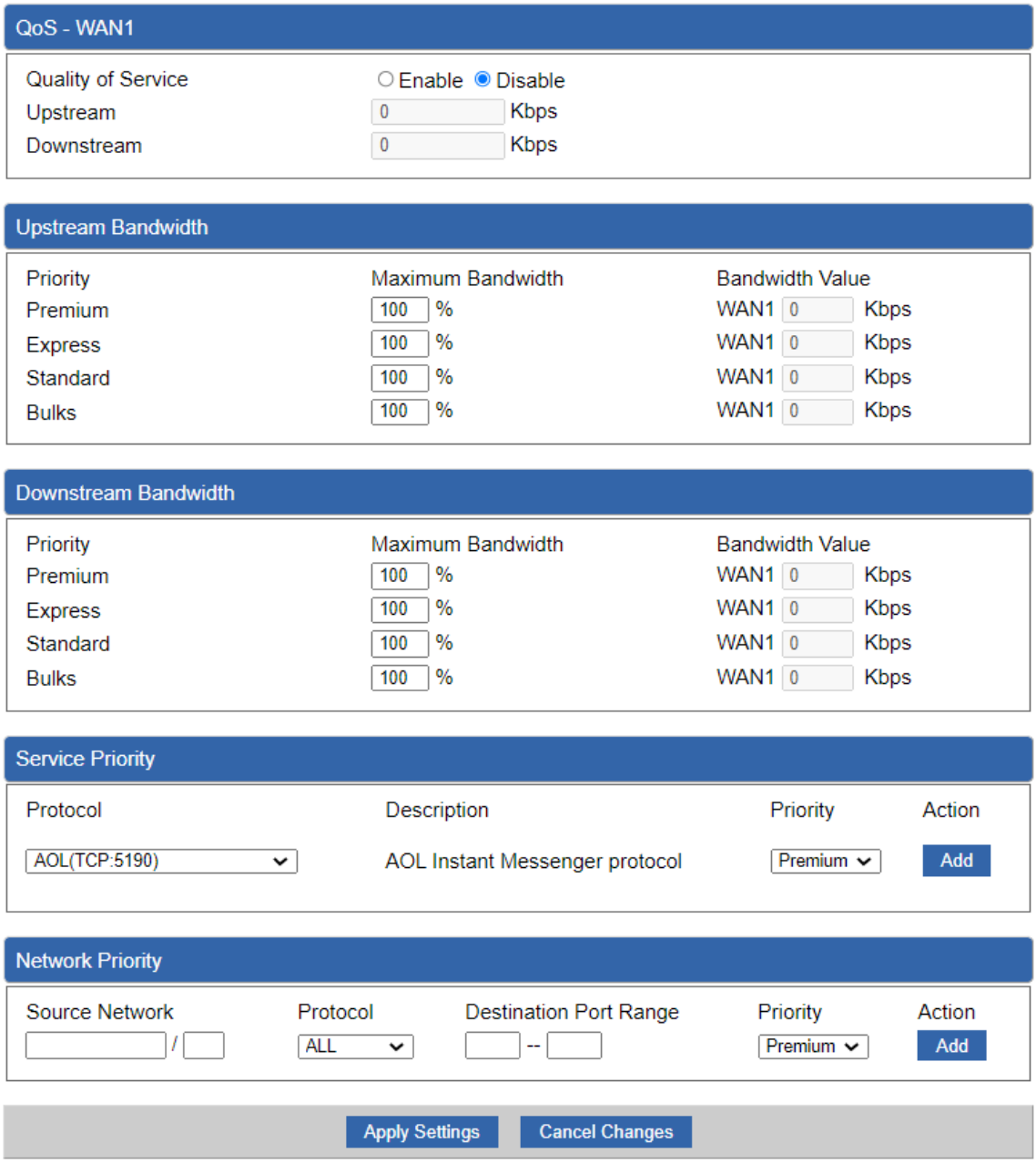


Figure 4-48: QoS Setting

Object	Description
QoS - WAN1	Enable/disable QoS function.
Upstream Bandwidth	Setting Upstream Bandwidth.
Downstream Bandwidth	Setting Downstream Bandwidth.
Service Priority	Setting Service Priority.
Network Priority	Setting Network Priority.

4.3.7 DMZ

A Demilitarized Zone is used to provide Internet services without sacrificing unauthorized access to its local private network as shown in Figure 4-49.Typically, the DMZ host contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.

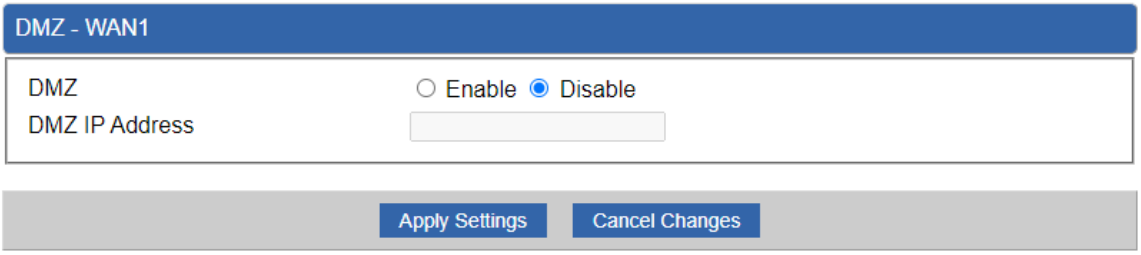


Figure 4-49: DMZ

Object	Description
DMZ	Set the function as enable or disable. If the DMZ function is enabled, it means that you set up DMZ at a particular computer to be exposed to the Internet so that some applications/software, especially Internet/online game can have two way connections.
DMZ IP Address	Enter the IP address of a particular host in your LAN which will receive all the packets originally going to the WAN port/Public IP address above.

4.4 Wireless

The Wireless menu provides the following features for managing the system

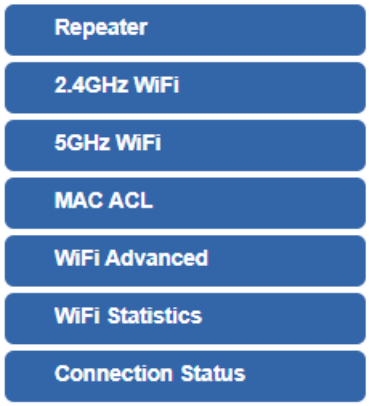
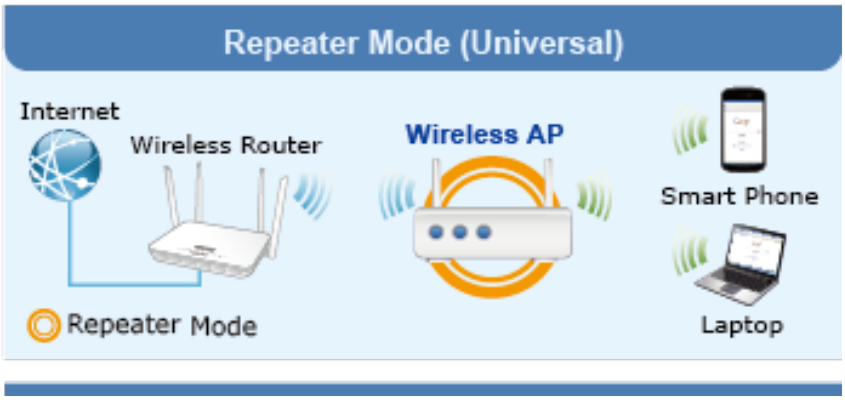


Figure 4-50: Wireless Menu

Object	Description
Repeater	Allow to configure Repeater.
2.4G Wi-Fi	Allow to configure 2.4G Wi-Fi.
5G Wi-Fi	Allow to configure 5G Wi-Fi.
MAC ACL	Allow configure MAC ACL.
Wi-Fi Advanced	Allow to configure advanced setting of Wi-Fi.
Wi-Fi Statistics	Display the statistics of Wi-Fi traffic.
Connection Status	Display the connection status.

4.4.1 Repeater



This page allows the user to define Repeater

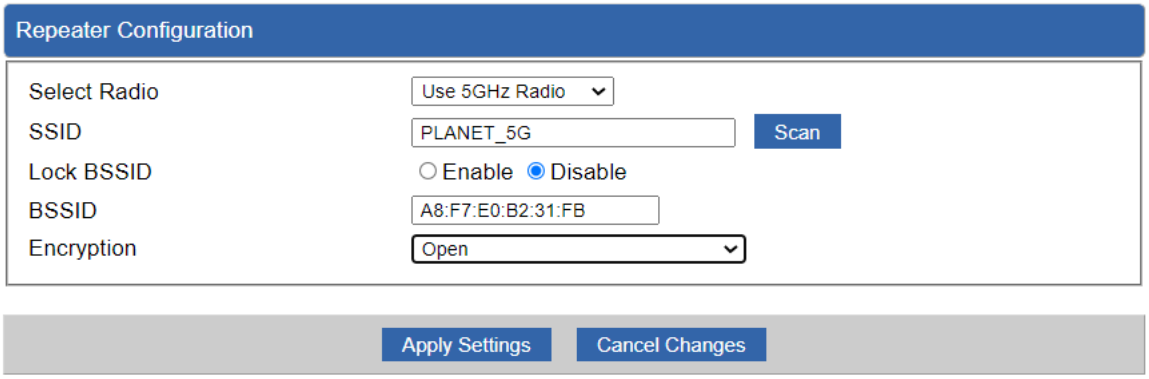


Figure 4-51: Repeater

Object	Description
Select Radio	Select "**2.4GHz**" or "**5GHz**" wireless LAN.
SSID (Wireless Name)	Enter the root AP's SSID or press "**Scan**" to select.
Lock BSSID	Enable/disable to lock the root AP's MAC address.
BSSID	The root AP's MAC address
Encryption	Select the wireless encryption of root AP. The default is "**Open**"

4.4.2 2.4G Wi-Fi

This page allows the user to define 2.4G Wi-Fi.

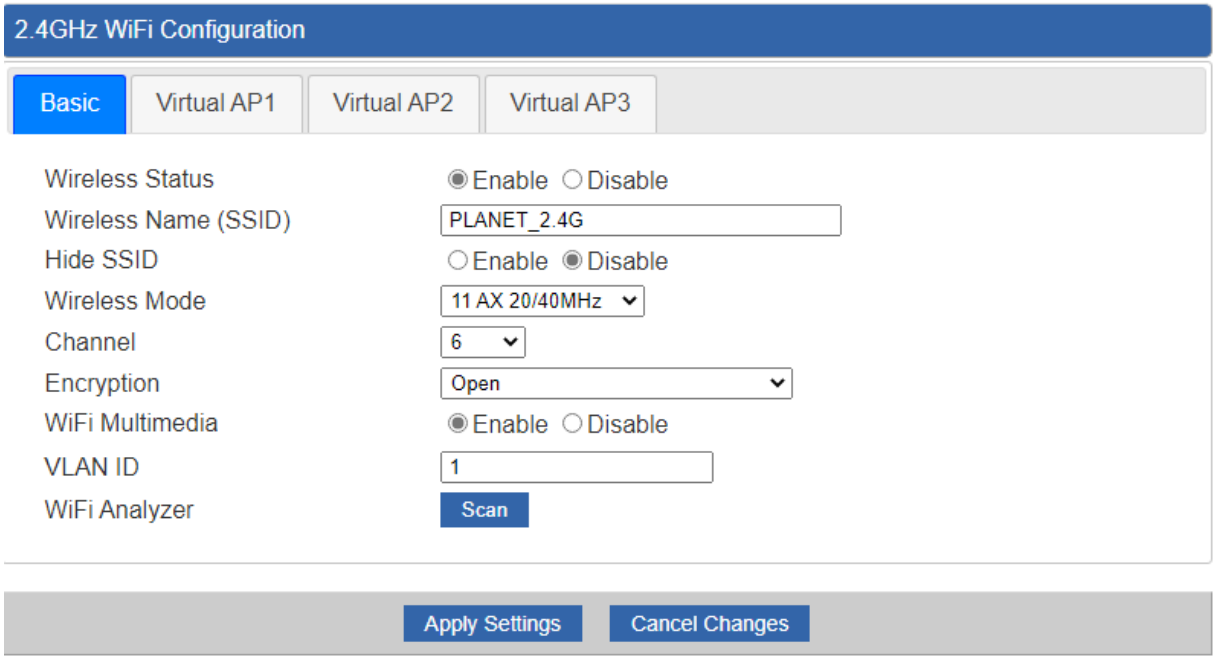


Figure 4-52: 2.4G Wi-Fi

Object	Description
Wireless Status	Allows user to enable or disable 2.4G Wi-Fi.
Wireless Name (SSID)	It is the wireless network name. The default 2.4G SSID is "PLANET_2.4G".
Hide SSID	Allows user to enable or disable SSID.
Wireless Mode	Select the operating wireless mode.
Channel	It shows the channel of the CPE. Default 2.4GHz is channel 6.
Encryption	Select the wireless encryption. The default is "**Open**".
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function.
VLAN ID	Setting VLAD ID.

4.4.3 5G Wi-Fi

This page allows the user to define 5G Wi-Fi.

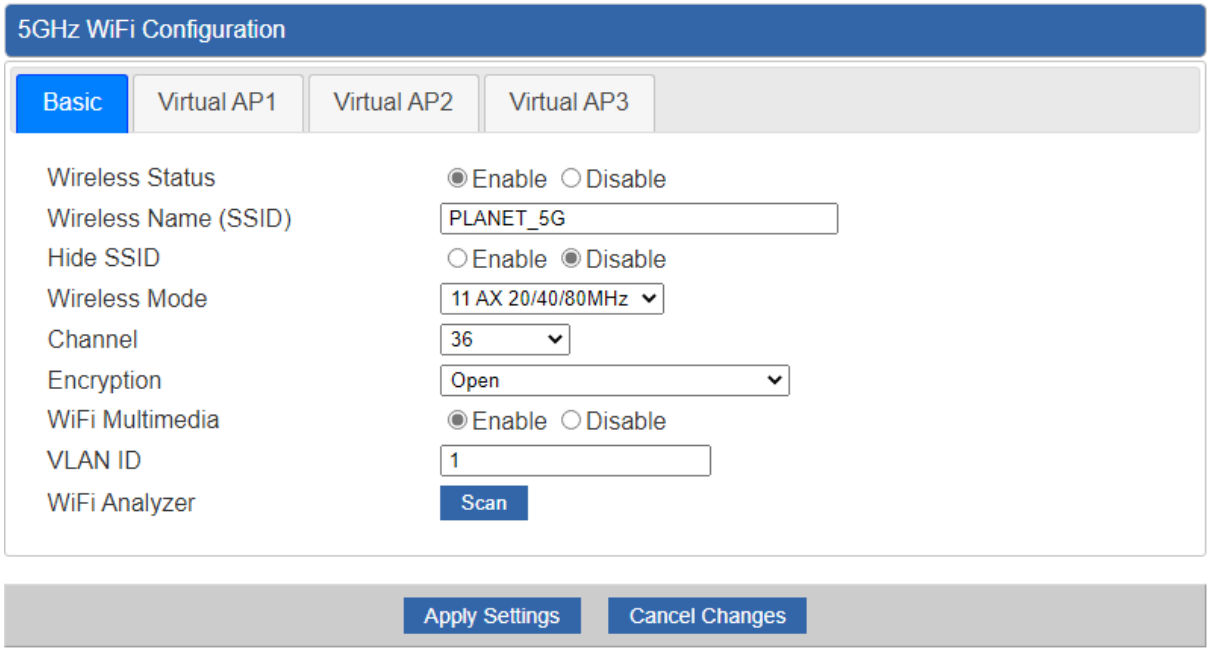


Figure 4-53: 5G Wi-Fi

Object	Description
Wireless Status	Allows user to enable or disable 5G Wi-Fi.
Wireless Name (SSID)	It is the wireless network name. The default 5G SSID is "PLANET_5G".
Hide SSID	Allows user to enable or disable SSID.
Wireless Mode	Select the operating wireless mode.
Channel	It shows the channel of the CPE. Default 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is "**Open**".
Wi-Fi Multimedia	Enable/Disable WMM (Wi-Fi Multimedia) function.
VLAN ID	Setting VLAD ID.

4.4.4 MAC ACL

This page allows the user to define MAC ACL.

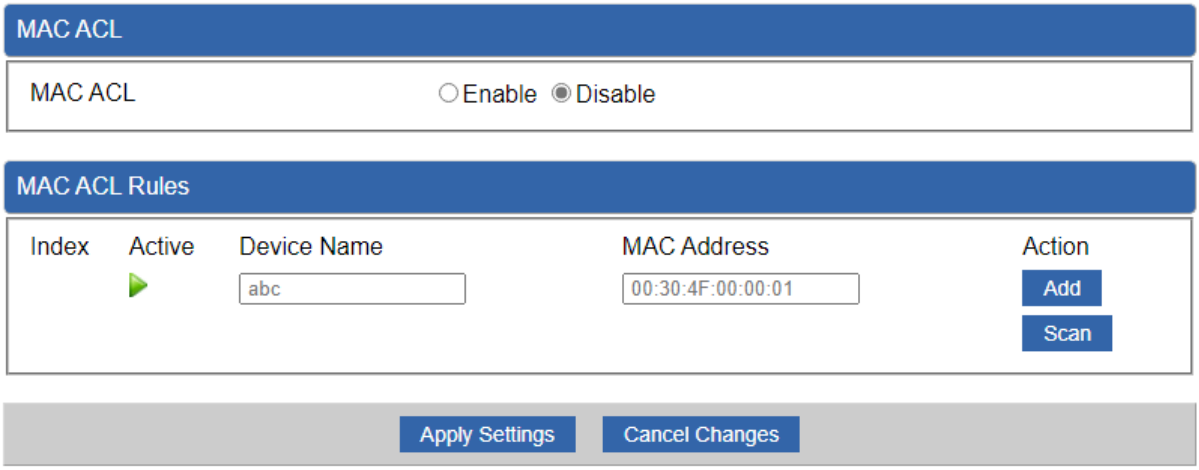


Figure 4-54: MAC ACL

Object	Description
Active	Allows the devices to pass in the rule.
Device Name	Set an allowed device name.
MAC Address	Set an allowed device MAC address.
Add	Press the "**Add**" button to add end-device that is scanned from wireless network and mark them.
Scan	Connect to client list.

4.4.5 Wi-Fi Advanced

This page allows the user to define advanced setting of Wi-Fi.

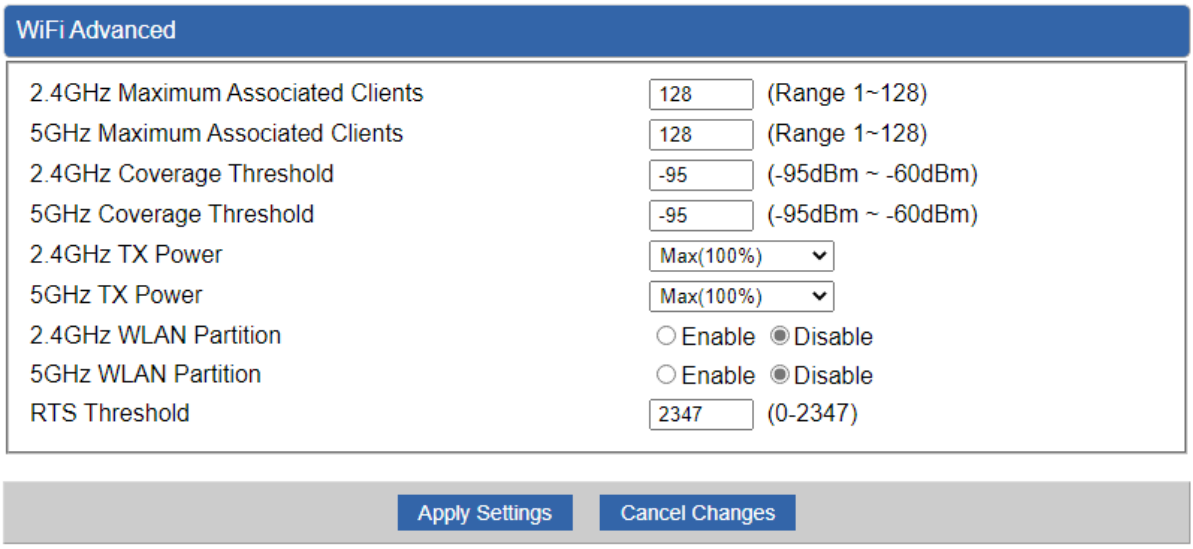


Figure 4-55: Wi-Fi Advanced

Object	Description
2.4GHz Maximum Associated Clients	The maximum users are 128.
5GHz Maximum Associated Clients	The maximum users are 128.
2.4G Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -95dBm.
5G Coverage Threshold	The coverage threshold is to limit the weak signal of clients occupying session. The default is -95dBm.
2.4G TX Power	The range of transmit power is **Max (100%)**, **Efficient (75%)**, **Enhanced (50%), Standard (25%)** or **Min (15%)**. In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power.
5G TX Power	The range of transmit power is **Max (100%)**, **Efficient (75%)**, **Enhanced (50%), Standard (25%)** or **Min (15%)**. In case of shortening the distance and the coverage of the wireless network, input a smaller value to reduce the radio transmission power.
2.4GHz WLAN Partition	Set the function as enable or disable.
5GHz WLAN Partition	Set the function as enable or disable.
RTS Threshold	Enable or Disable RTS/CTS protocol. It can be used in the following scenarios and used by Stations or Wireless AP.

	1) When medium is too noisy or lots of interferences are present. If the AP/Station cannot get a chance to send a packet, the RTS/CTS mechanism can be initiated to get the packet sent. 2) In mixed mode, the hidden node problem can be avoided. The default value is **2347**.

4.4.6 Wi-Fi Statistics

This page shows the statistics of Wi-Fi traffic.

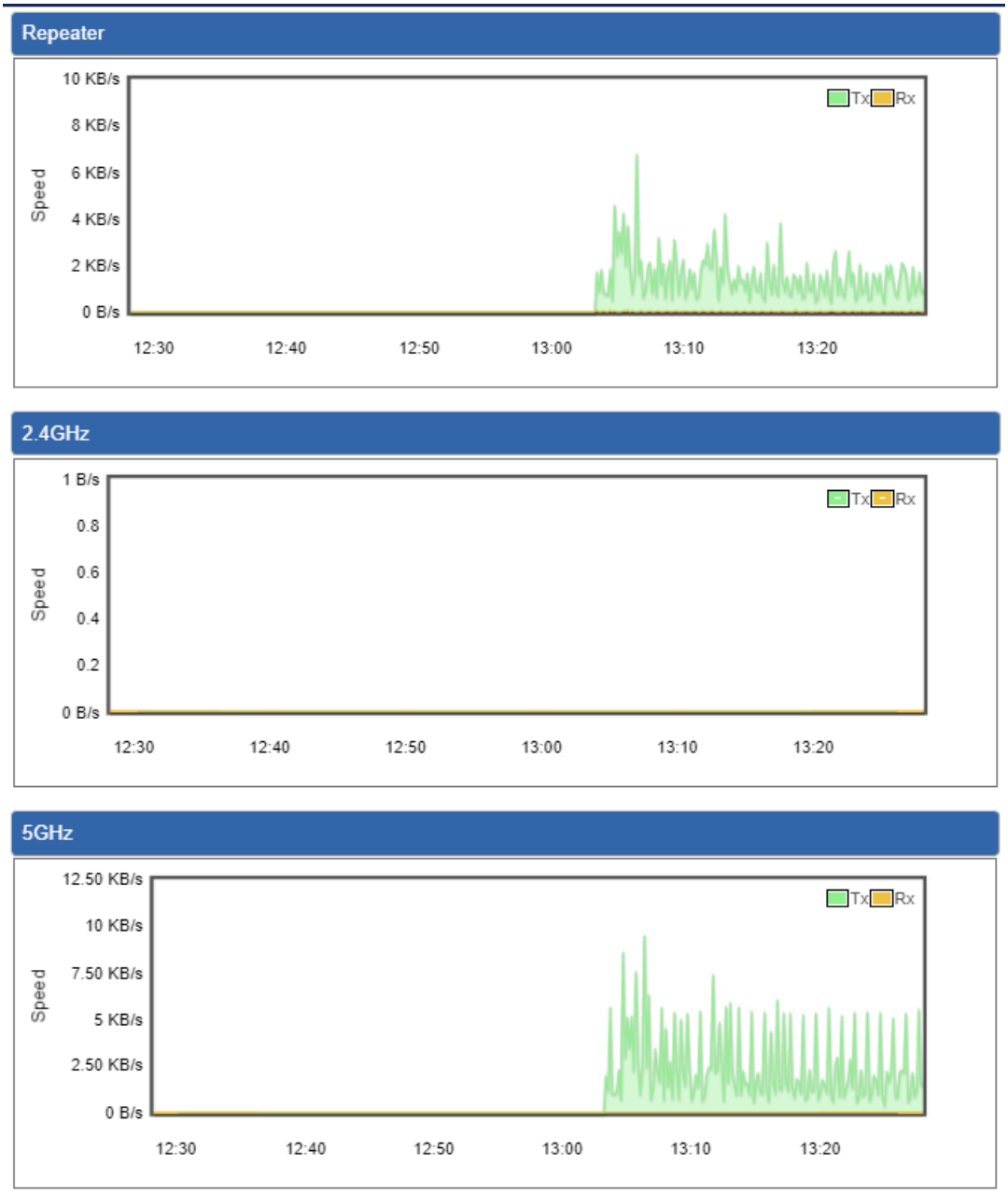


Figure 4-56: Wi-Fi Statistics

4.4.7 Connection Status

This page shows the host names and MAC address of all the clients in your network

Figure 4-57: Connection Status

Object	Description
Name	Display the host name of connected clients.
MAC Address	Display the MAC address of connected clients.
Signal	Display the connected signal of connected clients.
Connected Time	Display the connected time of connected clients.

4.5 Maintenance

The Maintenance menu provides the following features for managing the system

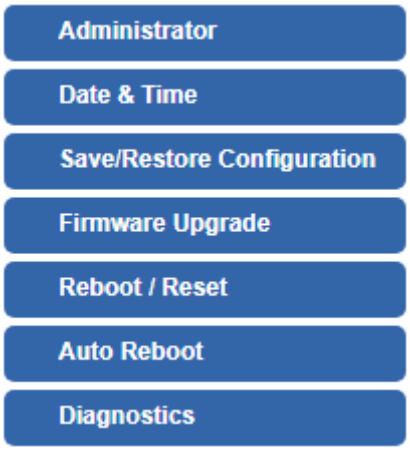


Figure 4-58: Maintenance

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the Industrial 802.11ax Wireless AP's configuration to local or USB sticker. Restore the Industrial 802.11ax Wireless AP's configuration from local or USB sticker.
Firmware Upgrade	Upgrade the firmware from local or USB storage.
Reboot / Reset	Reboot or reset the system.
Auto Reboot	Allows setting auto-reboot schedule.
Diagnostics	Allows you to issue ICMP PING packets to troubleshoot IP.

4.5.1 Administrator

To ensure the Industrial 802.11ax Wireless AP's security is secure, you will be asked for your password when you access the Industrial 802.11ax Wireless AP's Web-based utility. The default user name and password are "**admin**". This page will allow you to modify the user name and passwords as shown in Figure 4-59.

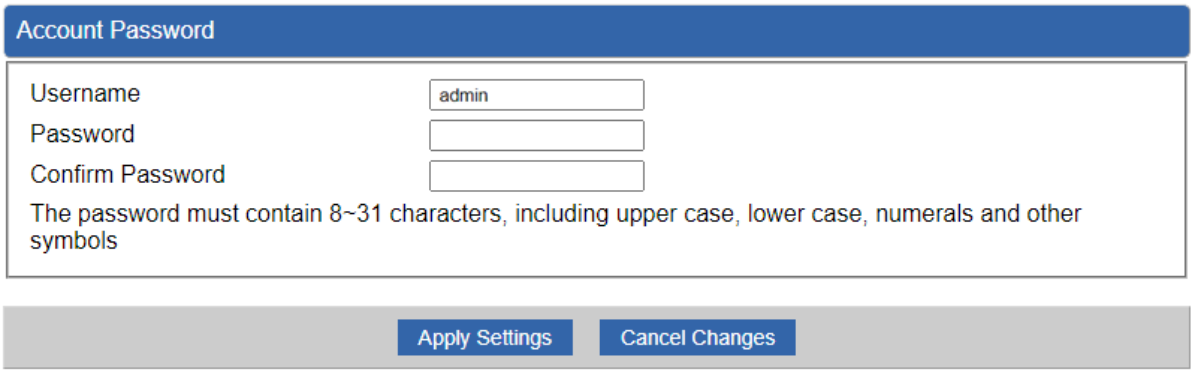


Figure 4-59: Administrator

Object	Description
Username	Input a new username.
Password	Input a new password.
Confirm Password	Input password again.

4.5.2 Date and Time

This section assists you in setting the system time of the Industrial 802.11ax Wireless AP. You are able to either select to set the time and date manually or automatically obtain the GMT time from Internet as shown in Figure 4-60.

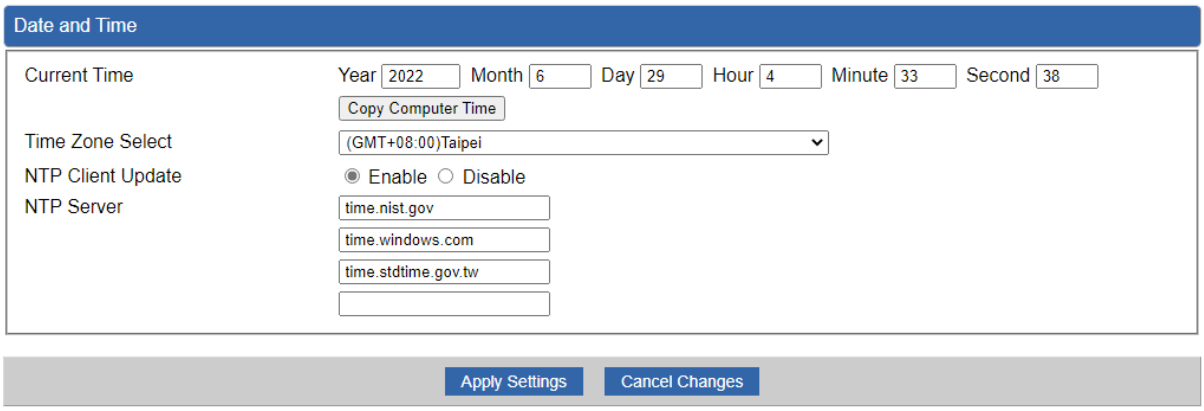


Figure 4-60: Date and Time

Object	Description

Current Time	Show the current time. User is able to set time and date manually.
Time Zone Select	Select the time zone of the country you are currently in. The Industrial 802.11ax Wireless AP will set its time based on your selection.
NTP Client Update	Once this function is enabled, Industrial 802.11ax Wireless AP will automatically update current time from NTP server.
NTP Server	User may use the default NTP sever or input NTP server manually.

4.5.3 Saving/Restoring Configuration

This page shows the status of the configuration. You may save the setting file to either USB storage or PC and load the setting file from USB storage or PC as Figure 4-61 is shown below:

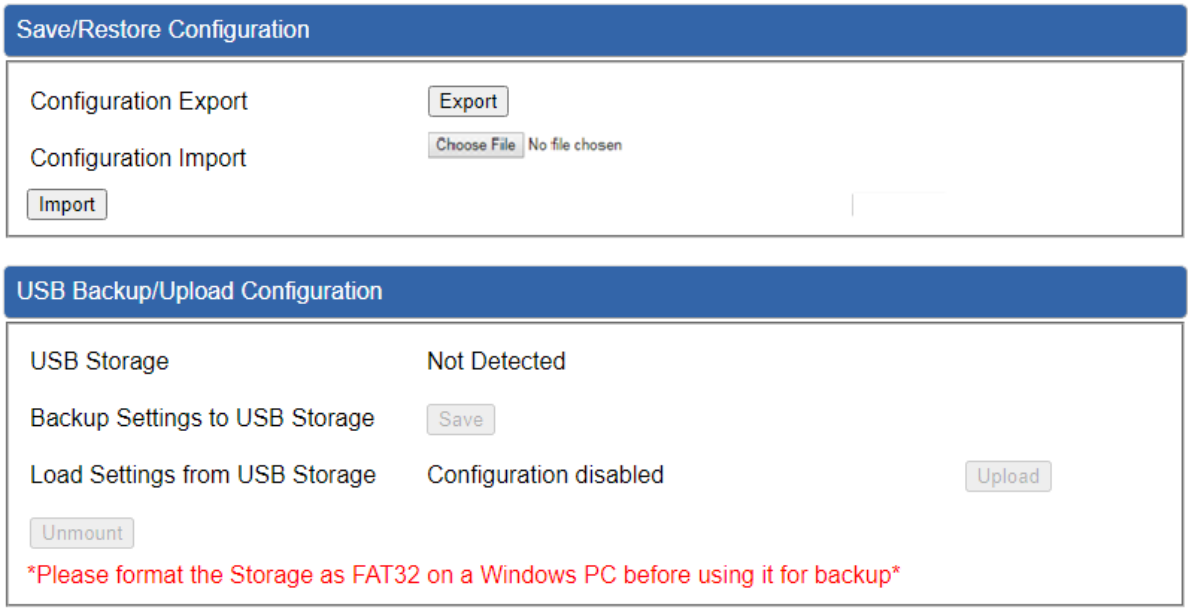


Figure 4-61: Save/Restore Configuration

■ **Save Setting to PC**

Object	Description
Configuration Export	Press the Export button to save setting file to PC.
Configuration Import	Press the Choose File button to select the setting file, and then press the Import button to upload setting file from PC.

■ **Save Setting to USB Storage**

Object	Description

Object	Description
USB Storage	The status of USB storage.
Backup Settings to USB Storage	Press the Save button to save setting file to USB storage.
Load Settings from USB Storage	Press the Upload button to upload setting file from USB storage.
Unmount	Before removing the USB storage from the VPN Security Gateway, please press the Umount button first.

4.5.4 Firmware Upgrading

This page provides the firmware upgrade of the Industrial 802.11ax Wireless AP as shown in Figure 4-62.

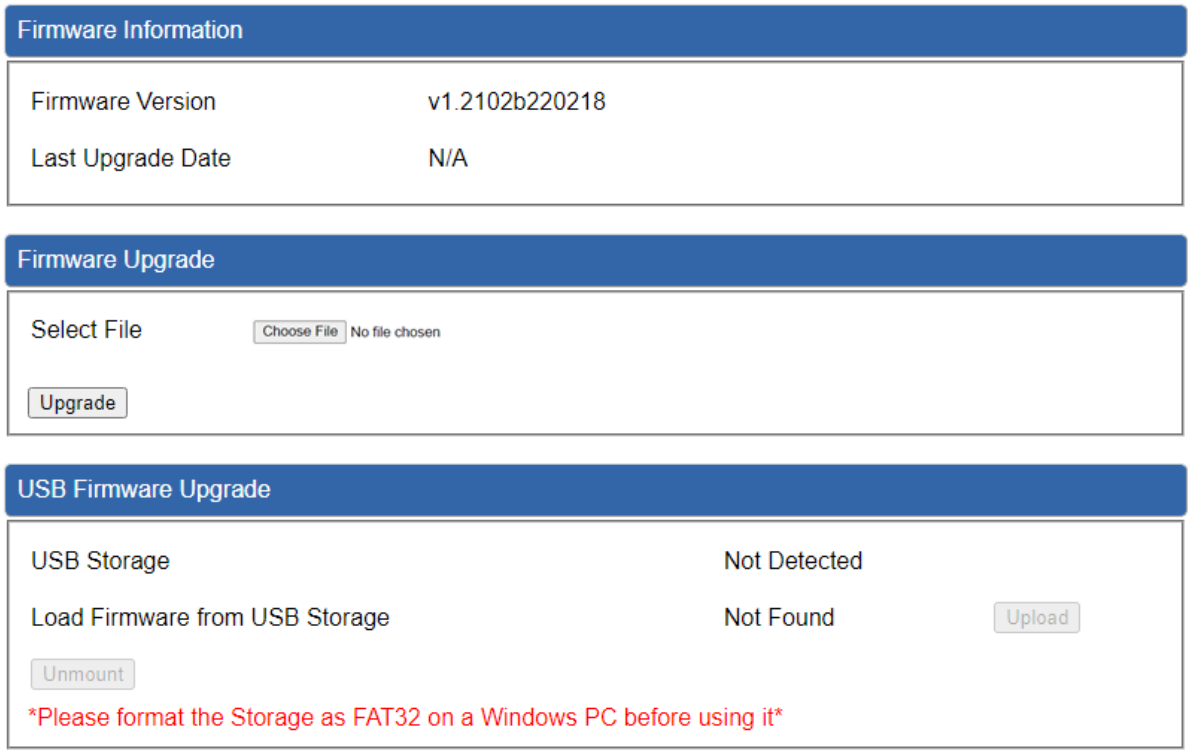


Figure 4-62: Firmware upgrade

Object	Description
Choose File	Press the button to select the firmware.
Upgrade	Press the button to upgrade firmware to system.

4.5.5 Reboot / Reset

This page enables the device to be rebooted from a remote location. Once the Reboot button is pressed, users have to re-log in the Web interface as Figure 4-63 is shown below:

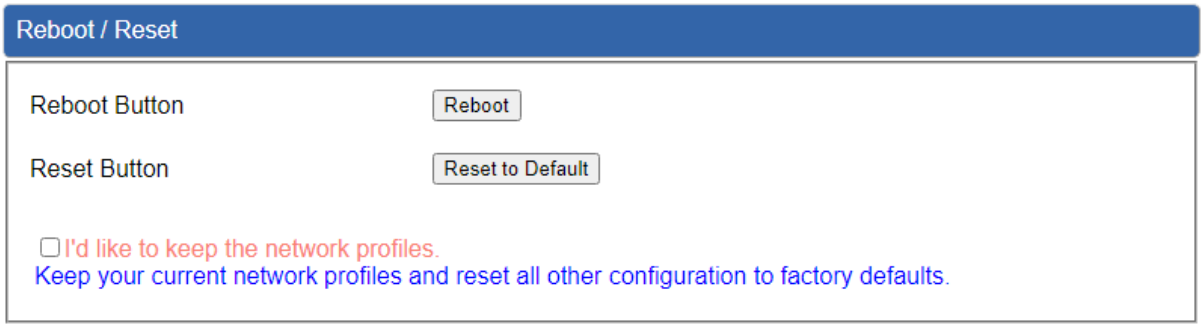


Figure 4-63: Reboot/Reset

Object	Description
Reboot	Press the button to reboot system.
Reset	Press the button to restore all settings to factory default settings.
I'd like to keep the network profiles.	Check the box and then press the Reset to Default button to keep the current network profiles and reset all other configurations to factory defaults.

4.5.6 Auto Reboot

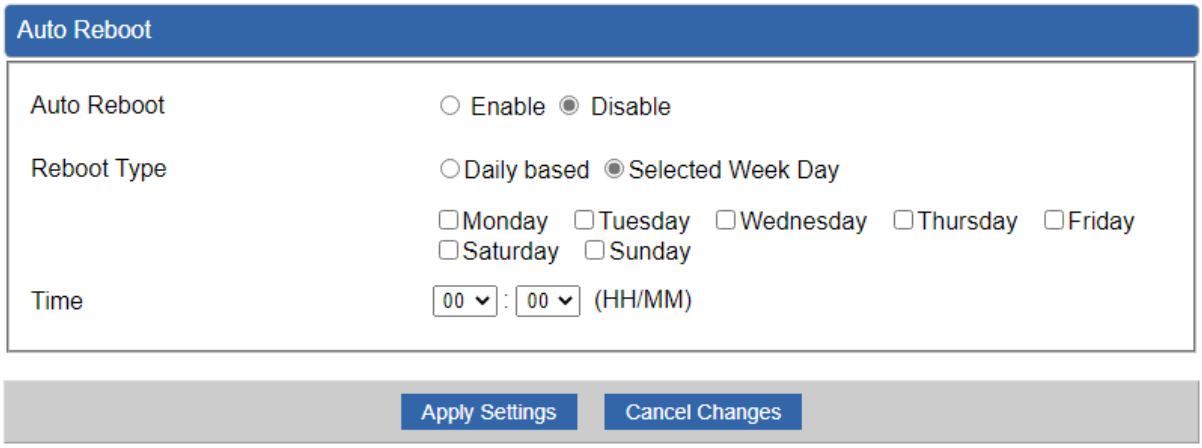


Figure 4-64: Auto Reboot

Object	Description
Auto Reboot	Disable or enable the Auto Reboot function.
Reboot Type	Set the function type.
Time	Select reboot time for clock.

4.5.7 Diagnostics

The page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press “Ping”, ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The Page refreshes automatically until responses to all packets are received, or until a timeout occurs. The ICMP Ping is shown in Figure 4-65.

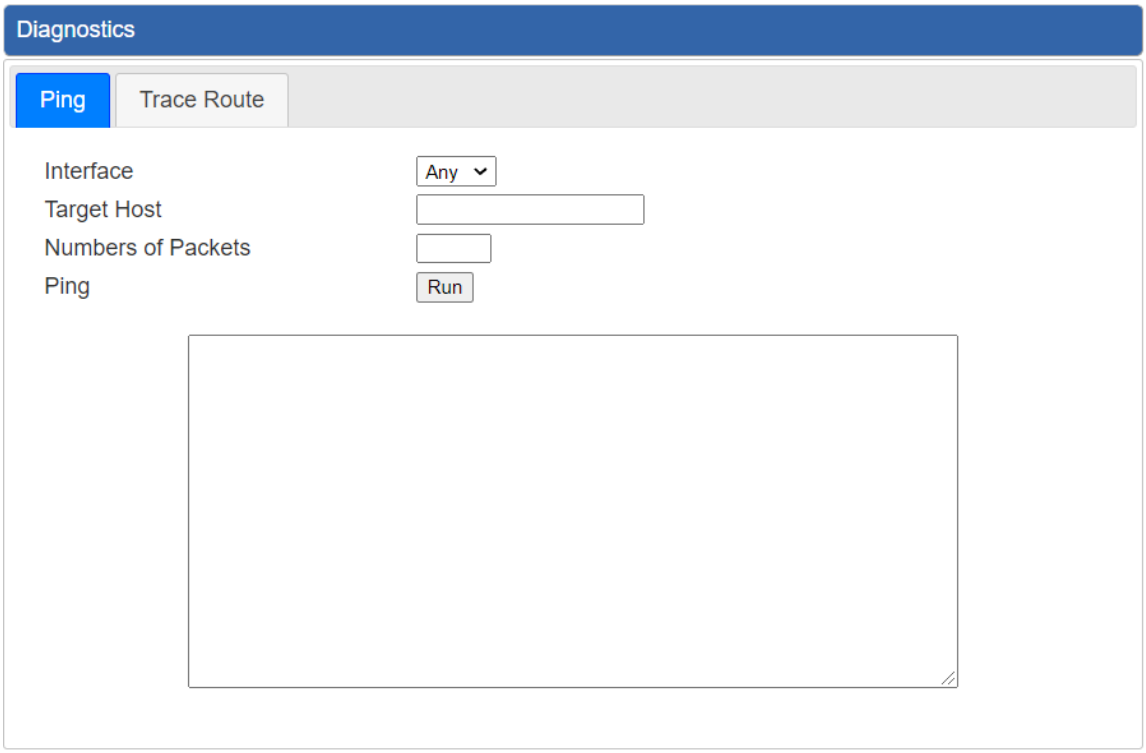


Figure 4-65: Ping

Object	Description
Interface	Select an interface of the Industrial 802.11ax Wireless AP.
Target Host	The destination IP Address or domain.
Number of Packets	Set the number of packets that will be transmitted; the maximum is 100.
Ping	The time of ping.

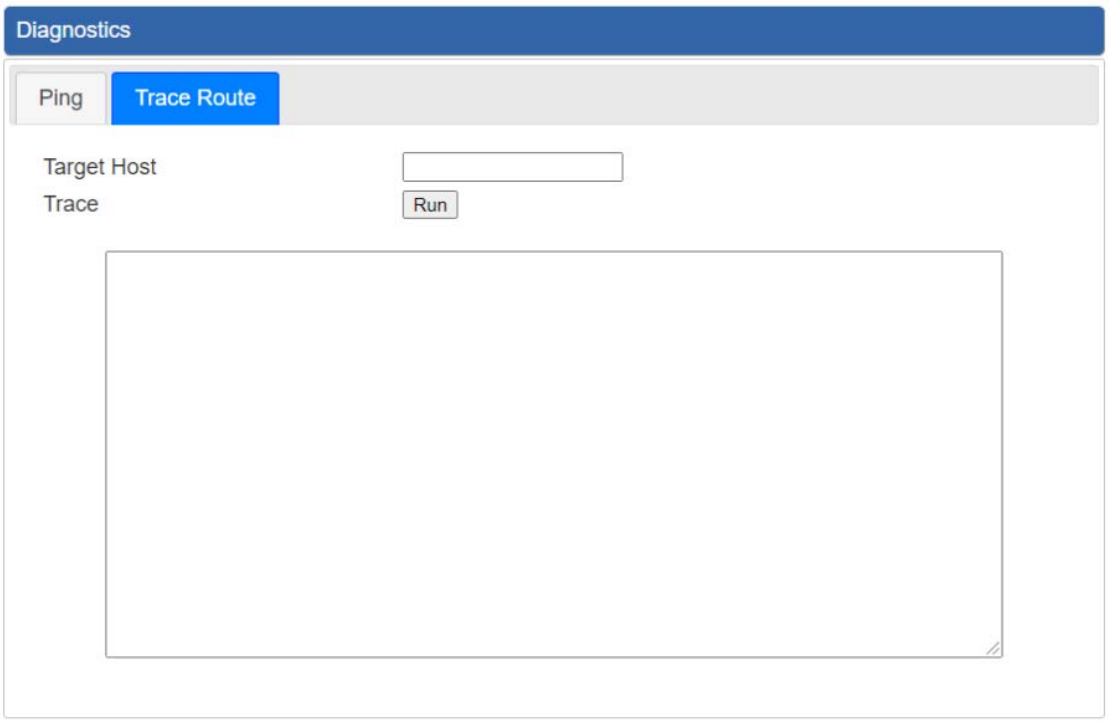


Figure 4-66: Trace Route

Object	Description
Target Host	The destination IP Address or domain.
Trace	The time of ping.

Note

Be sure the target IP address is within the same network subnet of the Industrial 802.11ax Wireless AP, or you have to set up the correct gateway IP address.

Chapter 5. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the Industrial 802.11ax Wireless AP is configured to "**default**".

Note

Some laptops are equipped with a "Wireless ON/OFF" switch for the internal wireless LAN. Make sure the hardware wireless switch is switched to "ON" position.

5.1 Windows 7/8/10/11 (WLAN AutoConfig)

WLAN AutoConfig service is built-in in Windows 7 that can be used to detect and connect to wireless network. This built-in wireless network connection tool is similar to wireless zero configuration tool in Windows XP.

Step 1: Right-click on the **network icon** displayed in the system tray

Figure 5-1: Network Icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [**default**]

(2) Click the [**Connect**] button

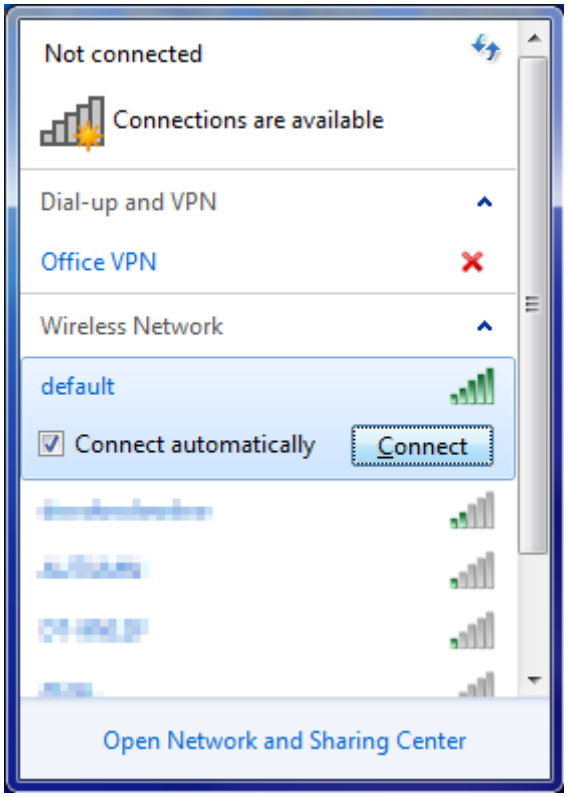


Figure 5-2: WLAN AutoConfig

Note

If you will be connecting to this Industrial 802.11ax Wireless AP in the future, check [**Connect automatically**].

Step 4: Enter the **encryption key** of the wireless AP

(1) The Connect to a Network box will appear.

(2) Enter the encryption key that is configured in section 5.7.2.1

(3) Click the [OK] button.

Figure 5-3: Typing the Network Key

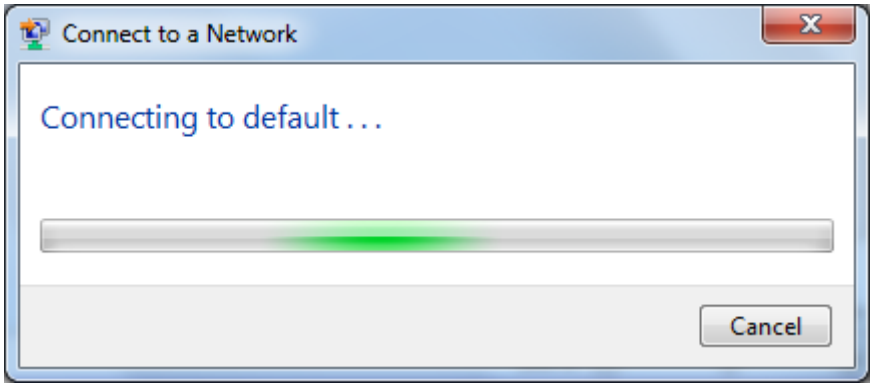


Figure 5-4: Connecting to a Network

Step 5: Check if "**Connected**" is displayed.

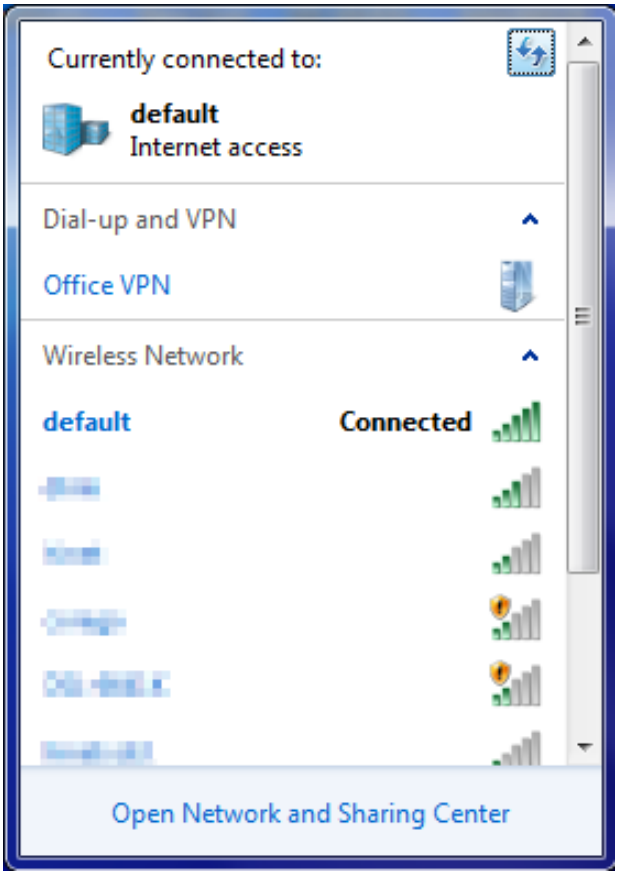


Figure 5-5: Connected to a Network

5.2 Mac OS X 10.x

In the following sections, the default SSID of the Industrial 802.11ax Wireless AP is configured to "default".

Step 1: Right-click on the **network icon** displayed in the system tray

The AirPort Network Connection menu will appear.

Figure 5-6: Mac OS – Network Icon

Step 2: Highlight and select the wireless network (SSID) to connect

(1) Select and SSID [**default**].

(2) Double-click on the selected SSID.

Figure 5-7: Highlighting and Selecting the Wireless Network

Step 4: Enter the **encryption key** of the wireless AP

(1) Enter the encryption key that is configured in section 5.7.2.1

(2) Click the [OK] button.

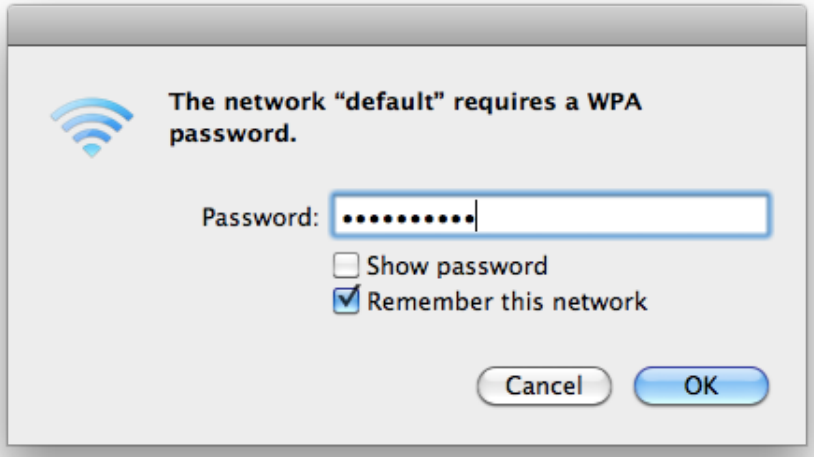


Figure 5-8: Enter the Password

Note

If you will be connecting to this Industrial 802.11ax Wireless AP in the future, check [**Remember this network**].

Step 5: Check if the AirPort is connected to the selected wireless network.

If "Yes", then there will be a "check" symbol in front of the SSID.

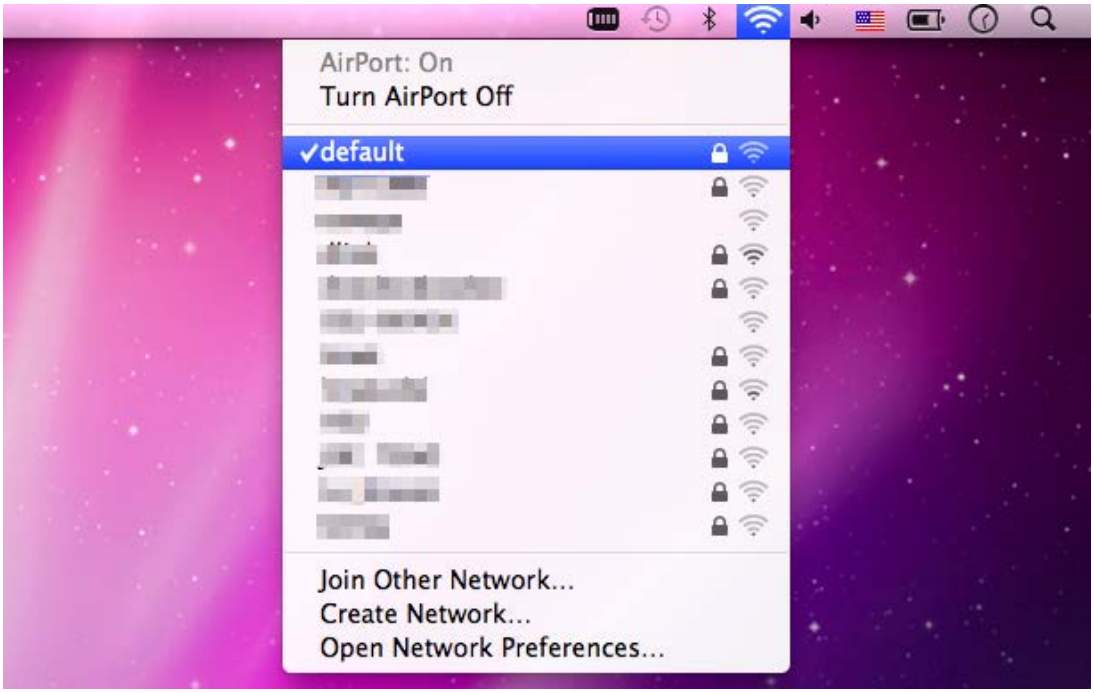


Figure 5-9: Connected to the Network

There is another way to configure the MAC OS X wireless settings:

Step 1: Click and open the [**System Preferences**] by going to **Apple** > **System Preference** or **Applications**

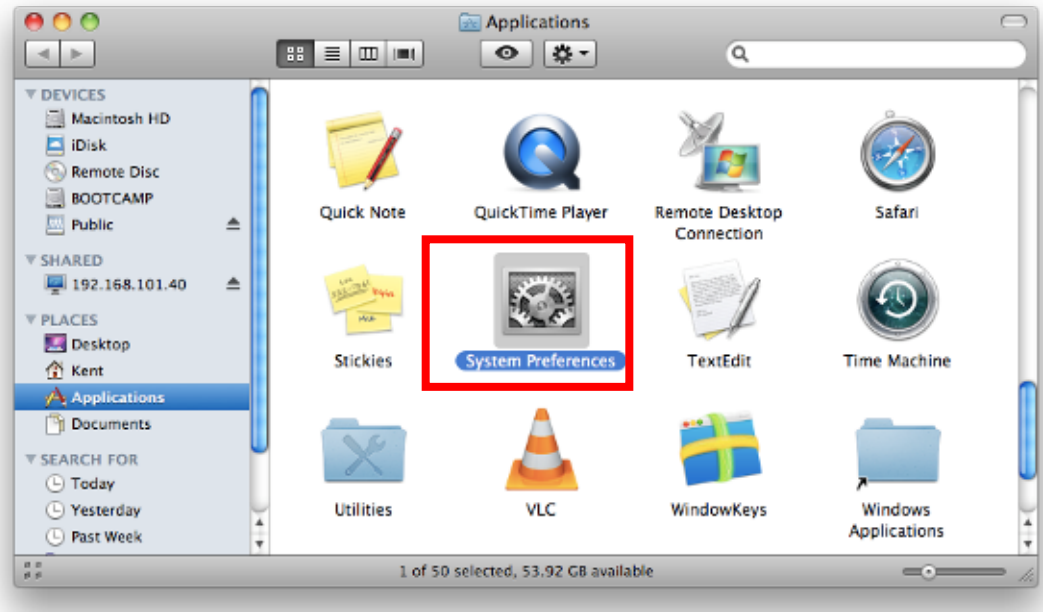


Figure 5-10: System Preferences

Step 2: Open **Network Preference** by clicking on the [**Network**] icon

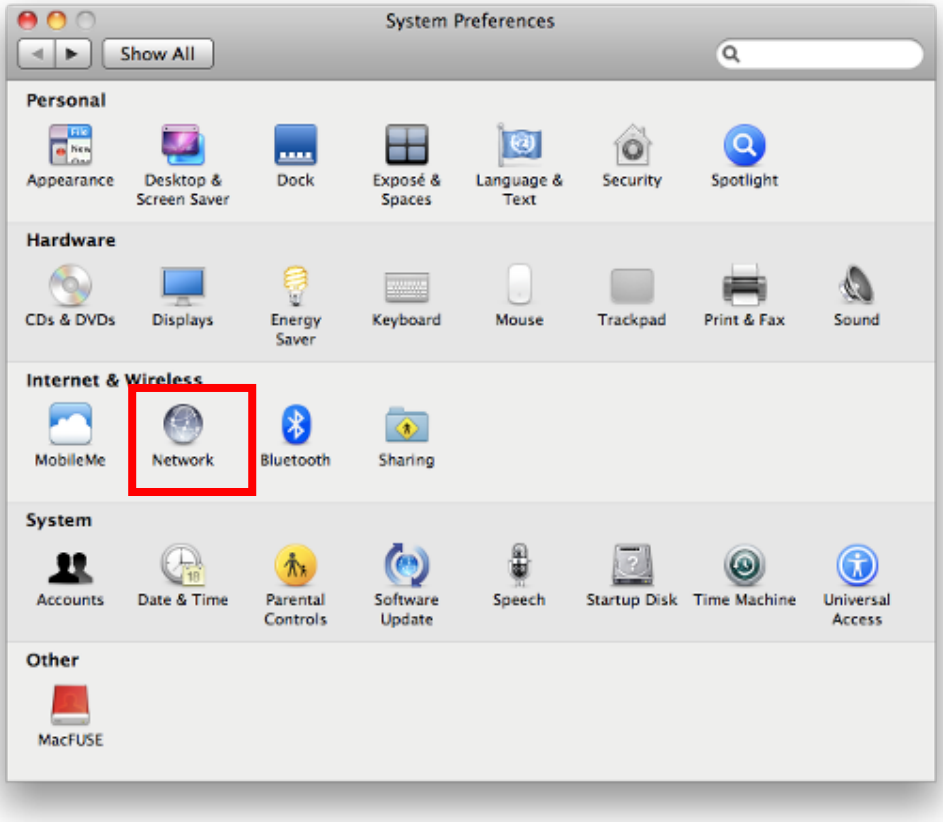


Figure 5-2: System Preferences -- Network

Step 3: Check Wi-Fi setting and select the available wireless network

(1) Choose the **AirPort** on the left menu (make sure it is ON)

(2) Select Network Name [**default**] here

If this is the first time to connect to the Wireless AP, it should show “No network selected”.

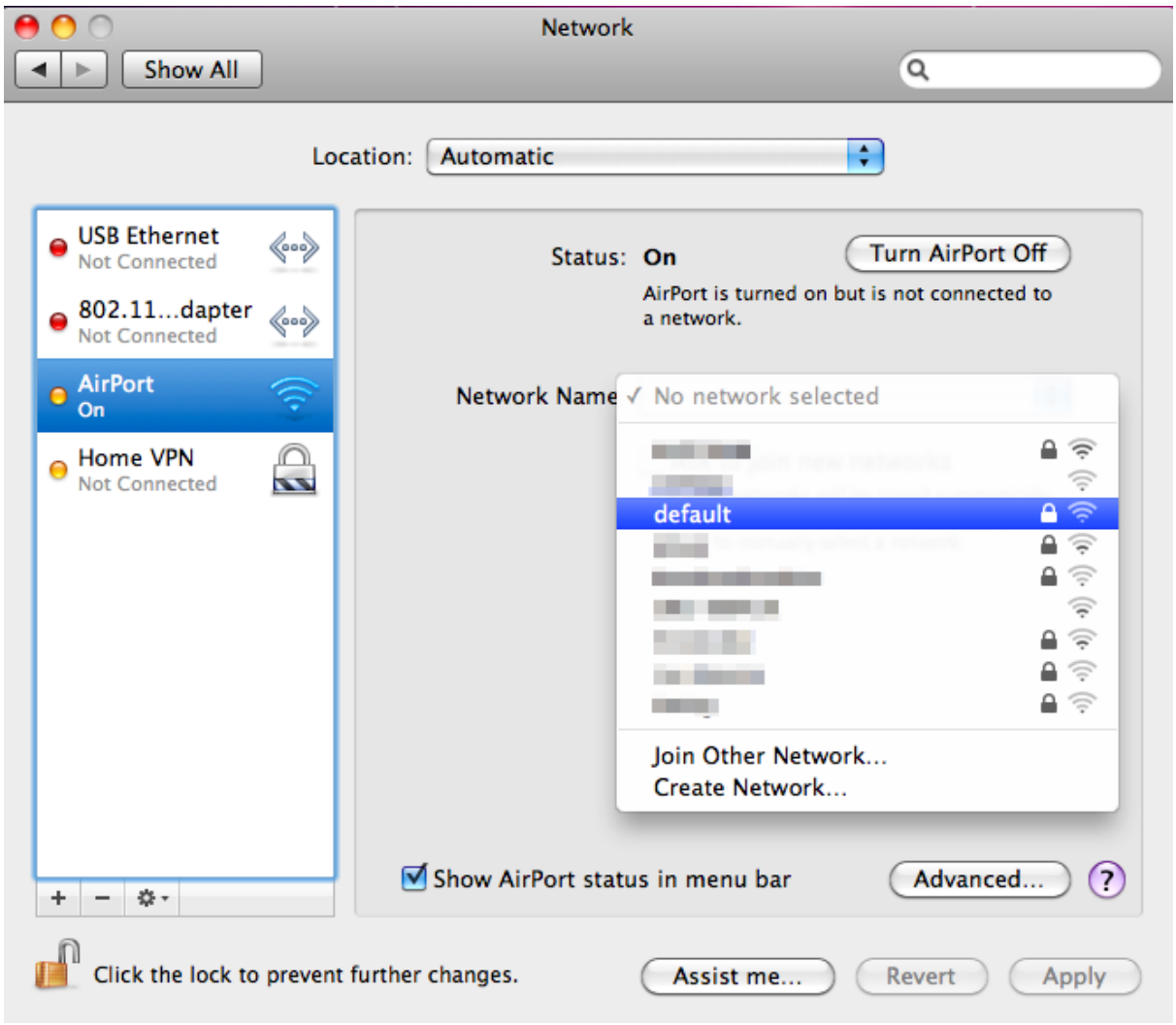


Figure 5-12: Selecting the Wireless Network

5.3 iPhone/iPod Touch/iPad

In the following sections, the **default SSID** of the WDAP series is configured to "**default**".

Step 1: Tap the [**Settings**] icon displayed in the home screen

Figure 5-3: iPhone – Settings icon

Step 2: Check Wi-Fi setting and select the available wireless network

(1) Tap [**General**] \ [**Network**]

(2) Tap [**Wi-Fi**]

If this is the first time to connect to the Industrial 802.11ax Wireless AP, it should show "Not Connected".

Figure 5-4: Wi-Fi Setting

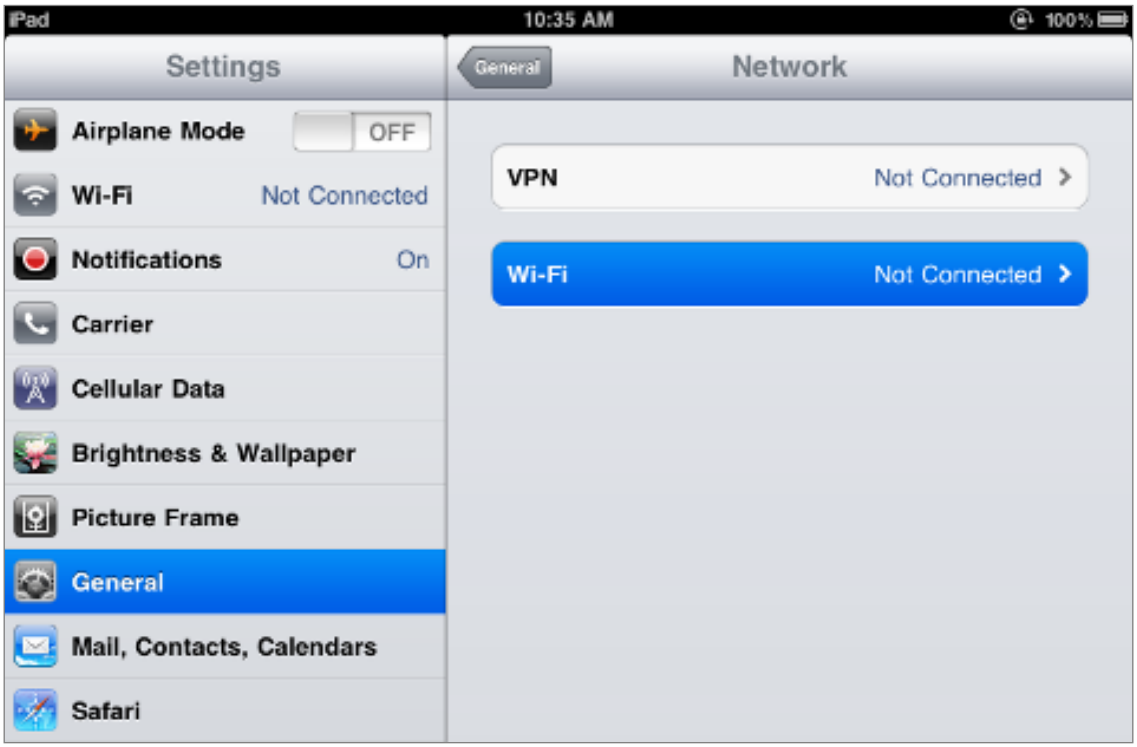


Figure 5-5: Wi-Fi Setting – Not Connected

Step 3: Tap the target wireless network (SSID) in "**Choose a Network…**"

(1) Turn on Wi-Fi by tapping "**Wi-Fi**"

(2) Select SSID [**default**]

Figure 5-6: Turning on Wi-Fi

Step 4: Enter the **encryption key** of the Wireless AP

(1) The password input screen will be displayed.

(2) Enter the encryption key that is configured in section 5.7.2.1

(3) Tap the [**Join**] button.

Figure 5-17: iPhone -- Entering the Password

Step 5: Check if the device is connected to the selected wireless network.

If “Yes”, then there will be a “check” symbol in front of the SSID.

Figure 5-18: iPhone -- Connected to the Network

Appendix A: DDNS Application

Configuring PLANET DDNS steps:

Step 1: Visit DDNS provider's web site and register an account if you do not have one yet. For example, register an account at http://planetddns.com

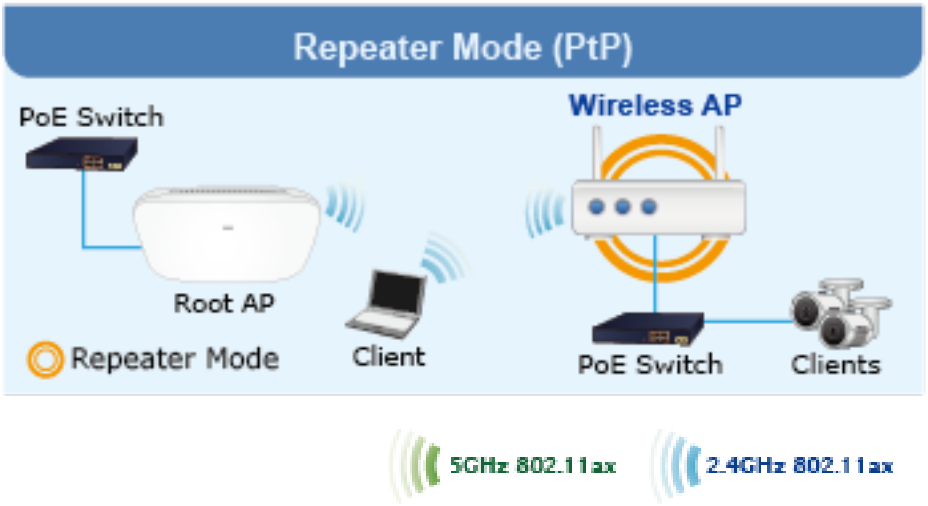
Step 2: Enable DDNS option through accessing web page of the device.

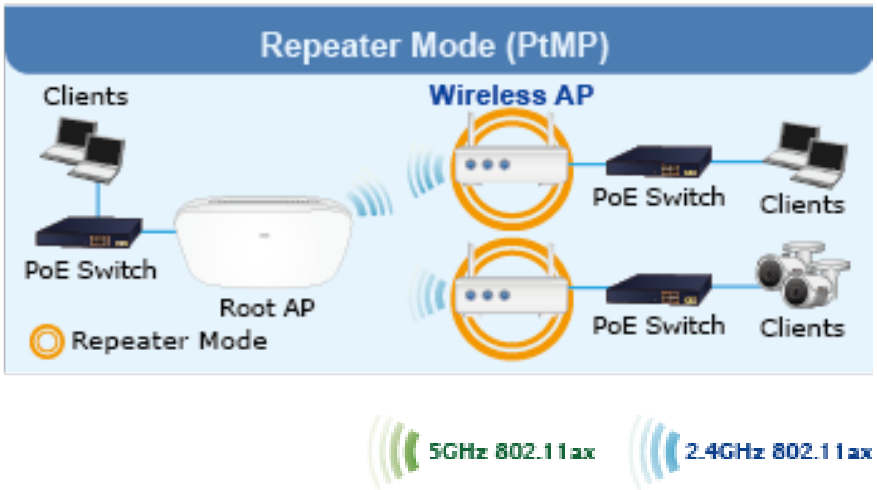
Step 3: Input all DDNS settings.

Appendix B: FAQs

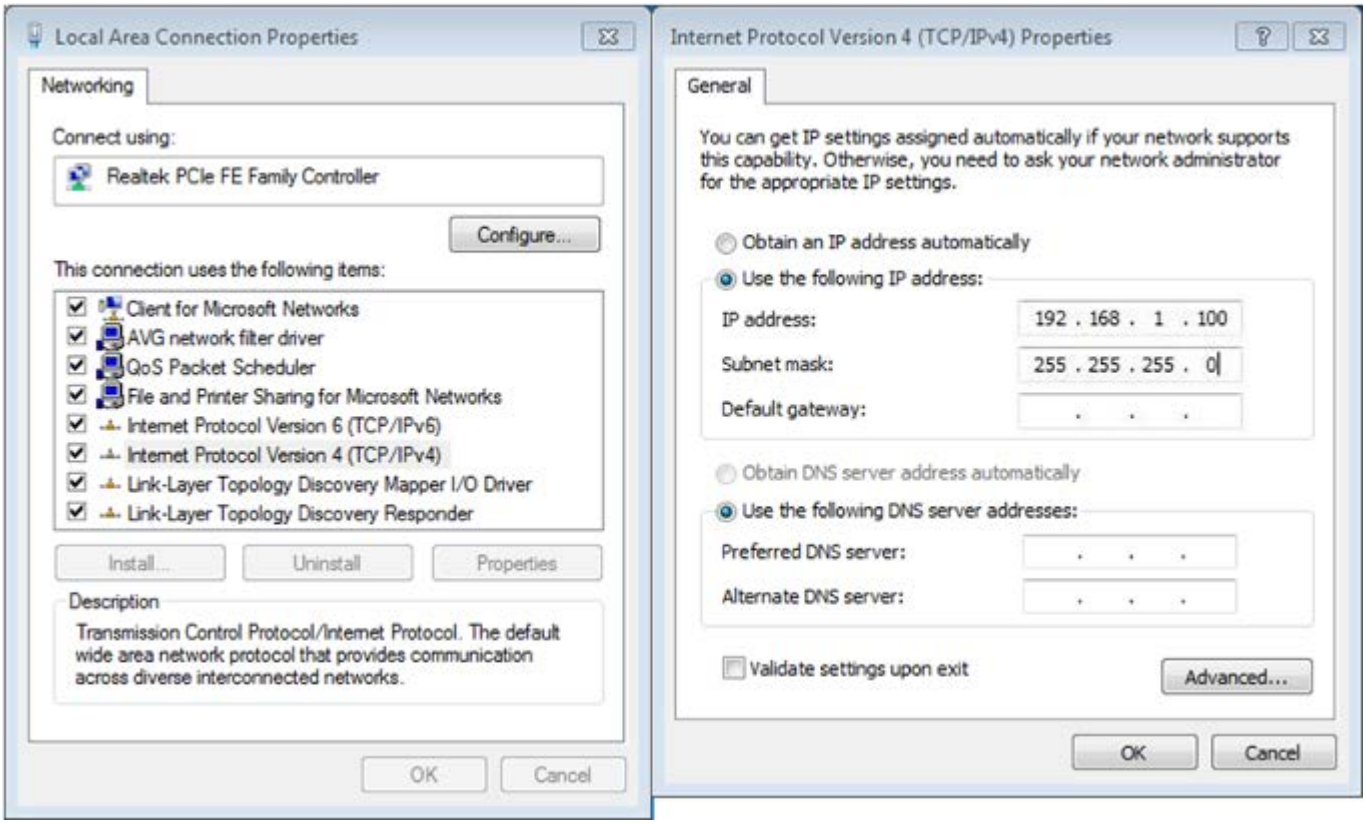
Q1: How to Set Up the AP Client Connection

Topology:

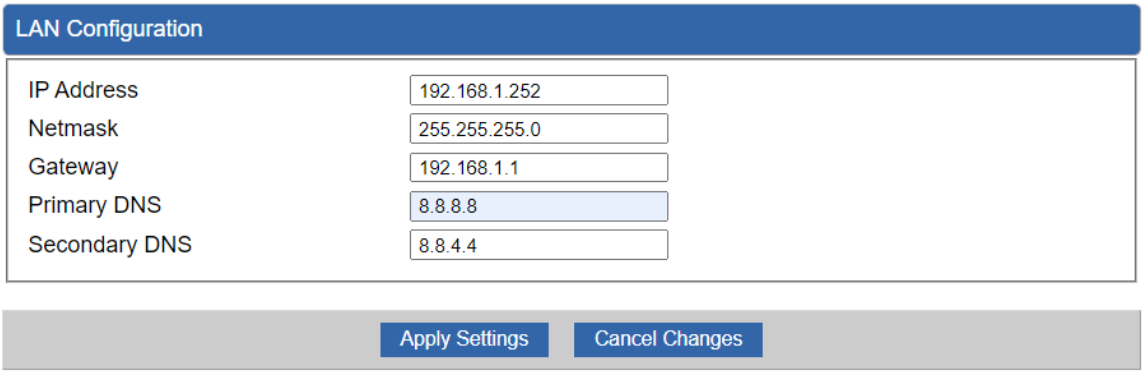




Step 1. Use static IP in the PCs that are connected with AP-1(Site-1) and AP-2(Site-2). In this case, Site-1 is "**192.168.1.100**", and Site-2 is "**192.168.1.200**".



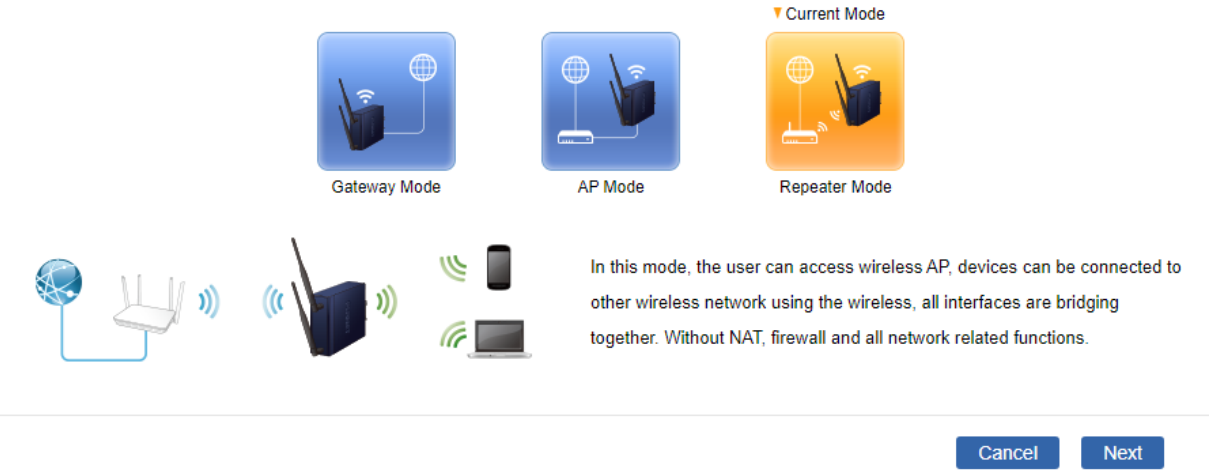
Step 2. In AP-2, change the default IP to the same IP range but different from AP-1. In this case, the IP is changed to **192.168.1.252**.



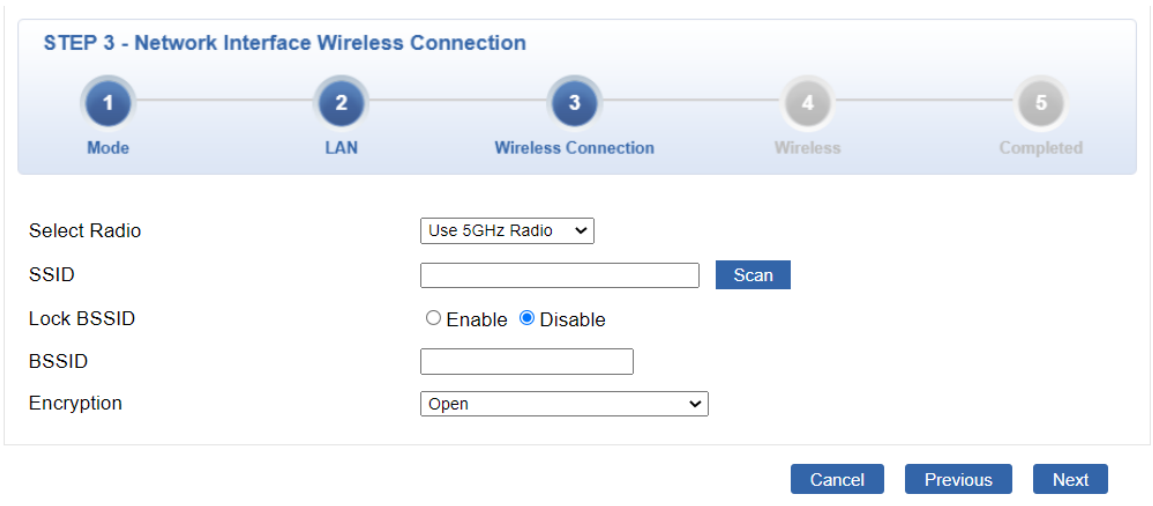
Step 3. In AP-1, go to "**Wizard**" to configure it to **AP Mode**. In AP-2, configure it to **Repeater Mode**.

AP-1

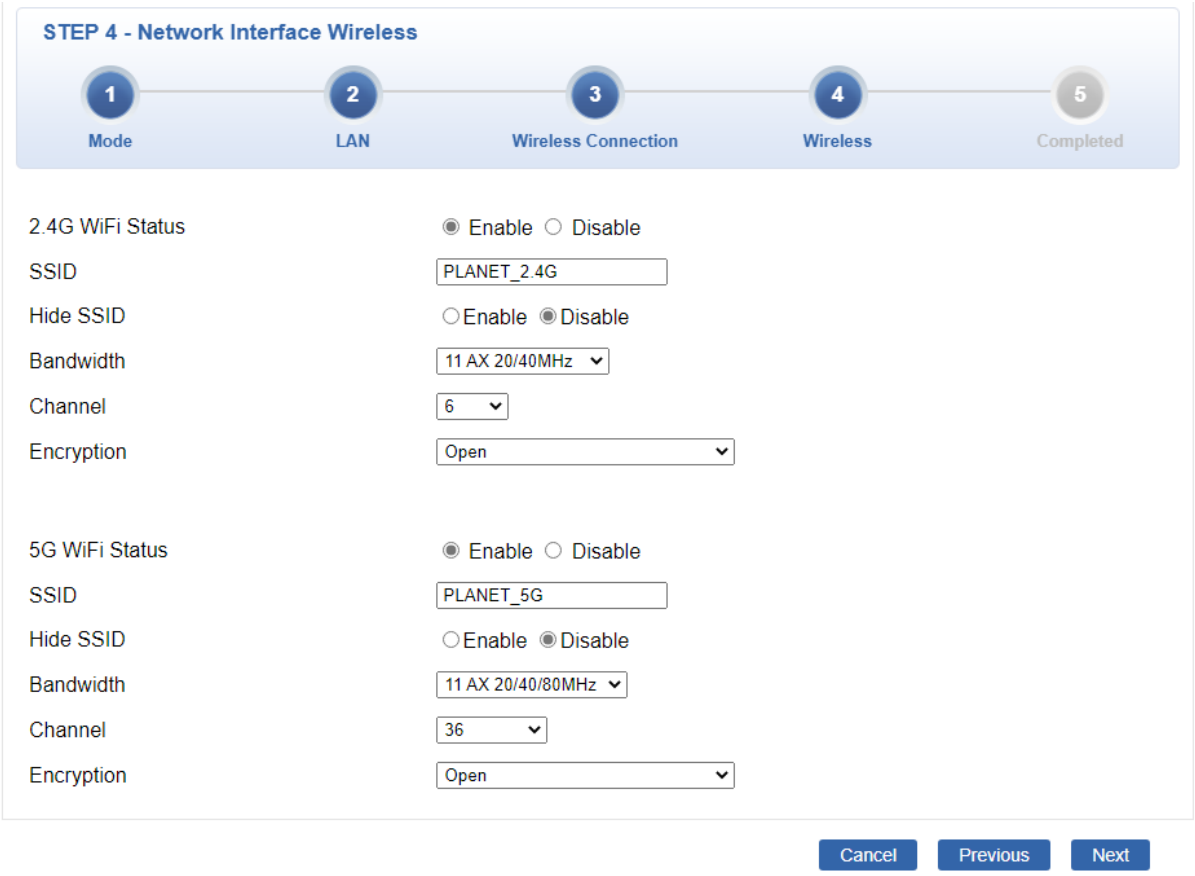
AP-2



Step 4. In AP-2, press "**Scan "** to search the AP-1. You can also enter the MAC address, SSID, encryption and bandwidth if you know what they are.

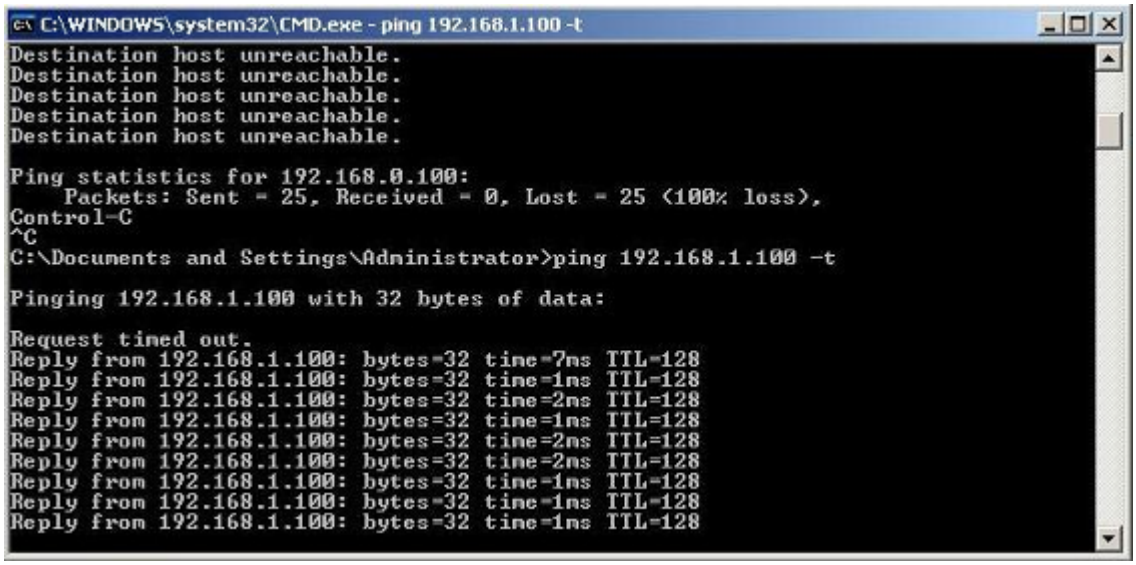


Step 5. Click "**Next**" to finish the setting.

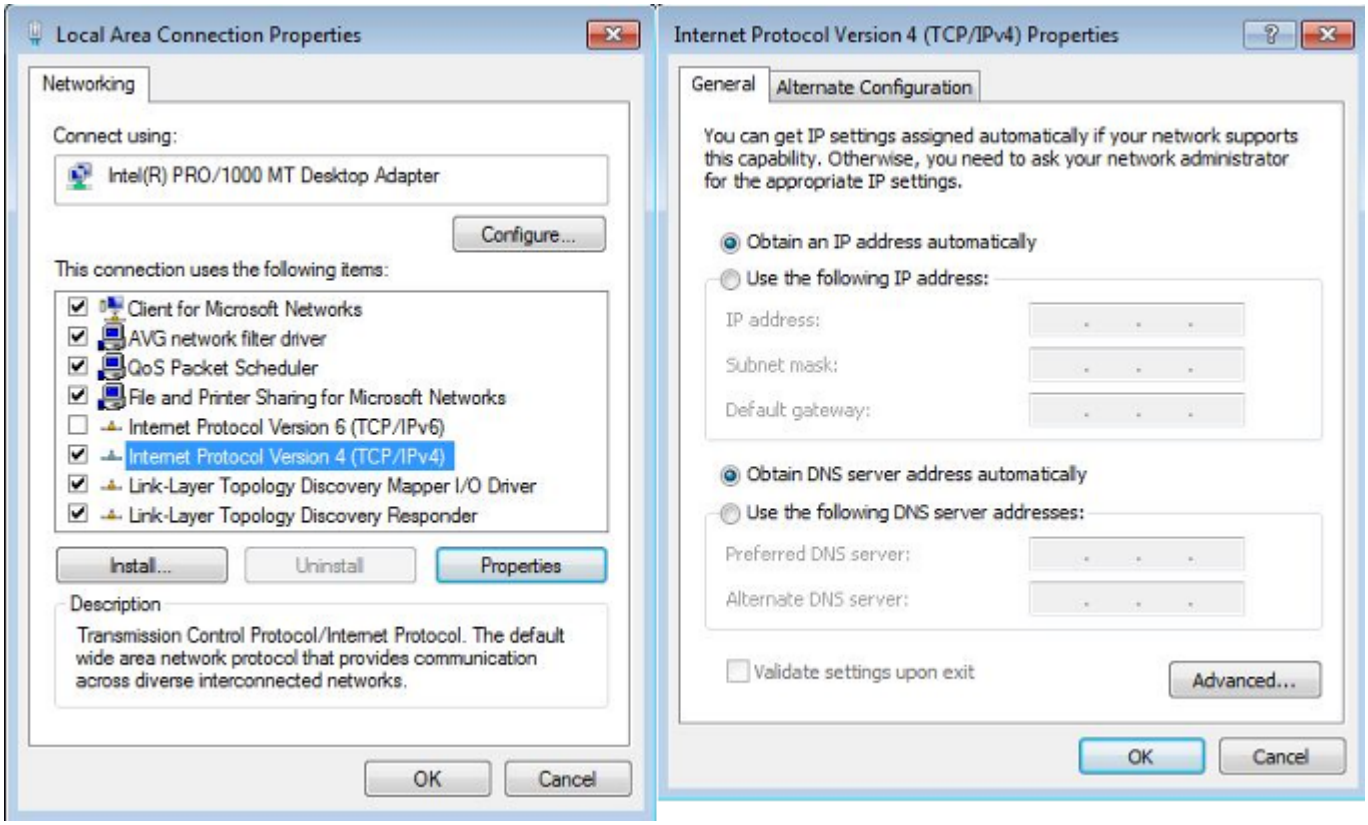


Step 6.Setup Completed

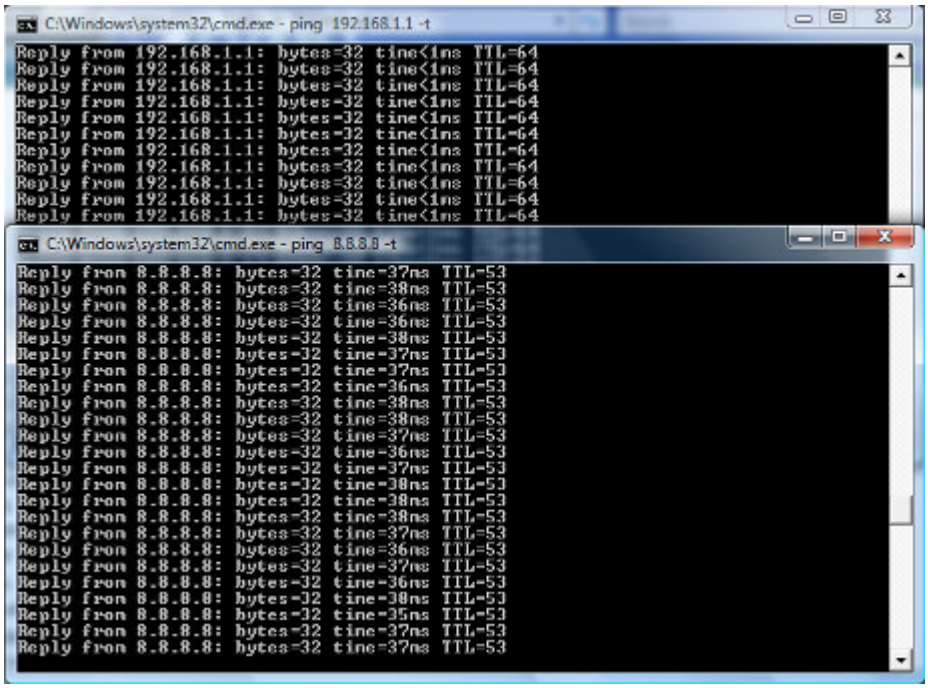
Step 7. Use command line tool to ping each other to ensure the link is successfully established. From Site-1, ping 192.168.1.200; and in Site-2, ping 192.168.1.100.



Step 8. Configure the TCP/IP settings of Site-2 to "**Obtain an IP address automatically**".



Step 9. Use command line tool to ping the DNS (e.g., Google) to ensure Site-2 can access internet through the wireless connection.



Note

The following hints should be noted:

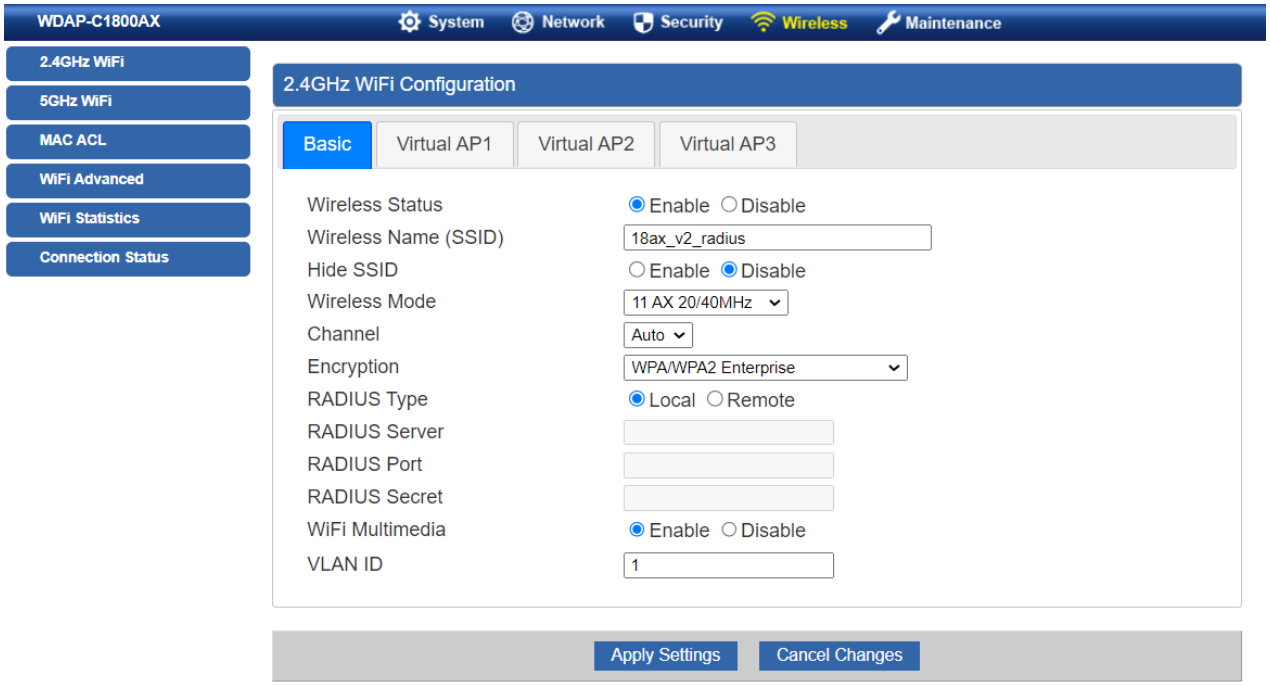
1) The encryption method must be the same as that of both sites if configured.
2) Both sites should be Line-of-Sight.
3) For the short distance connection less than 1km, please reduce the "RF Output Power" of both sites.
4) For the long distance connection over 1km, please adjust the "Distance" to the actual distance or double the actual distance.

Q2: How to tweak, change design or configure login information needed for the Captive Portal?

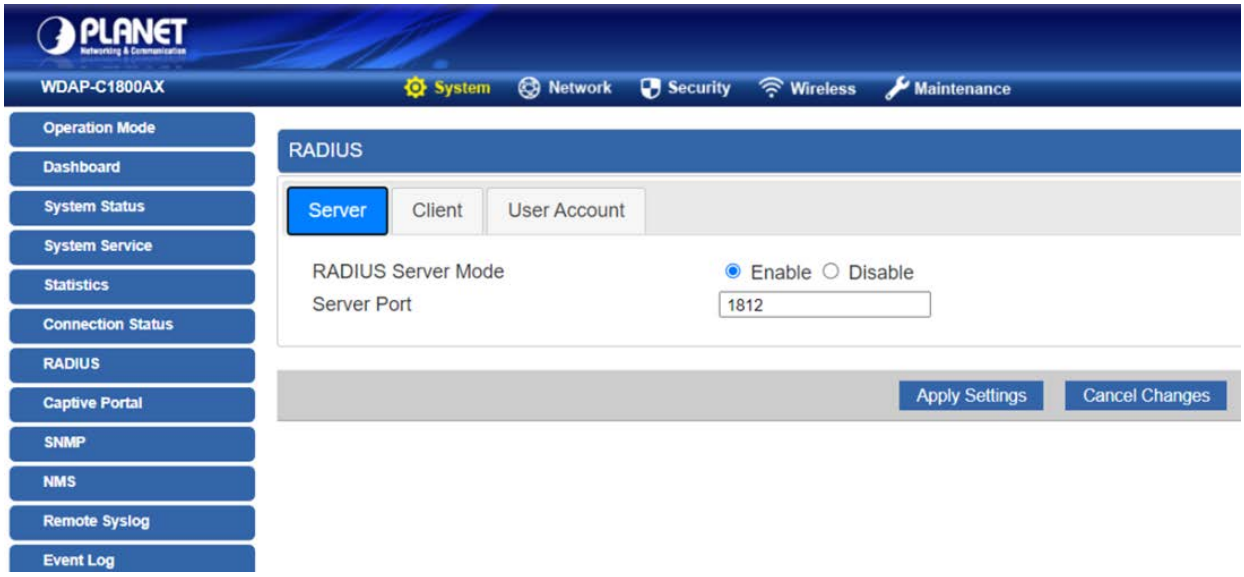
Step 1. Wi-Fi user client connect to AP local RADIUS Server.

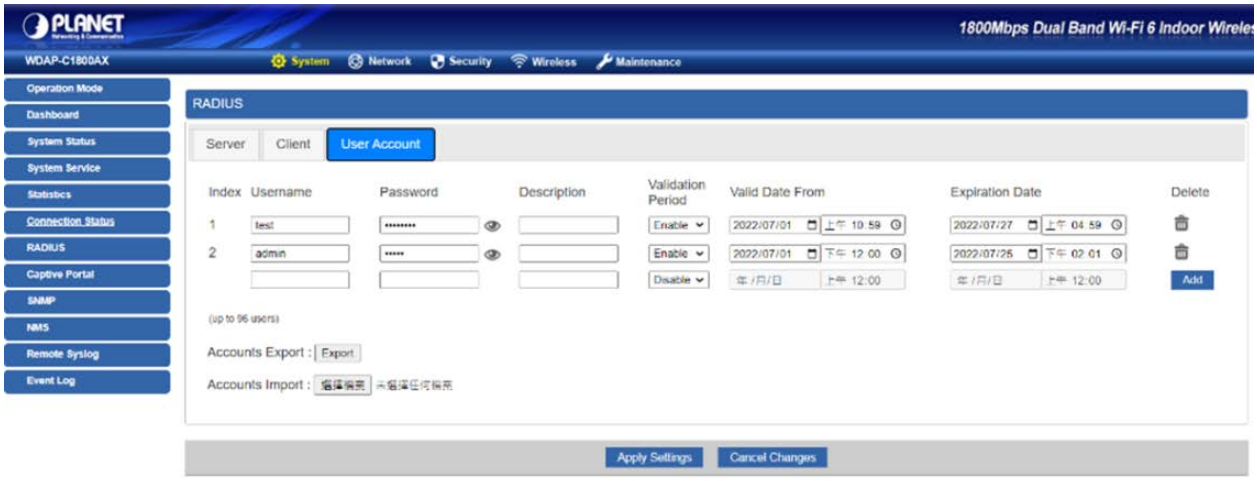
Step 2. Add user account for example: test/1qaz!QAZ & admin/12345.

Step 3.WI-FI setup web page.

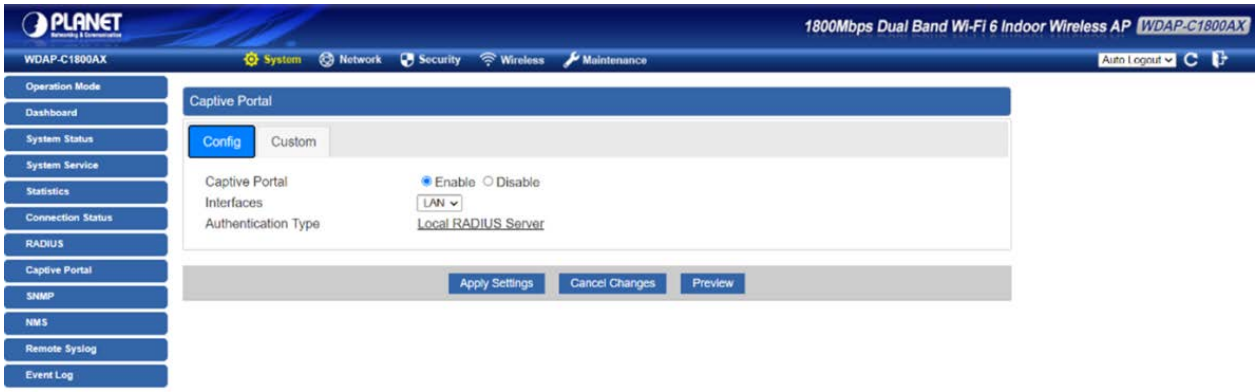


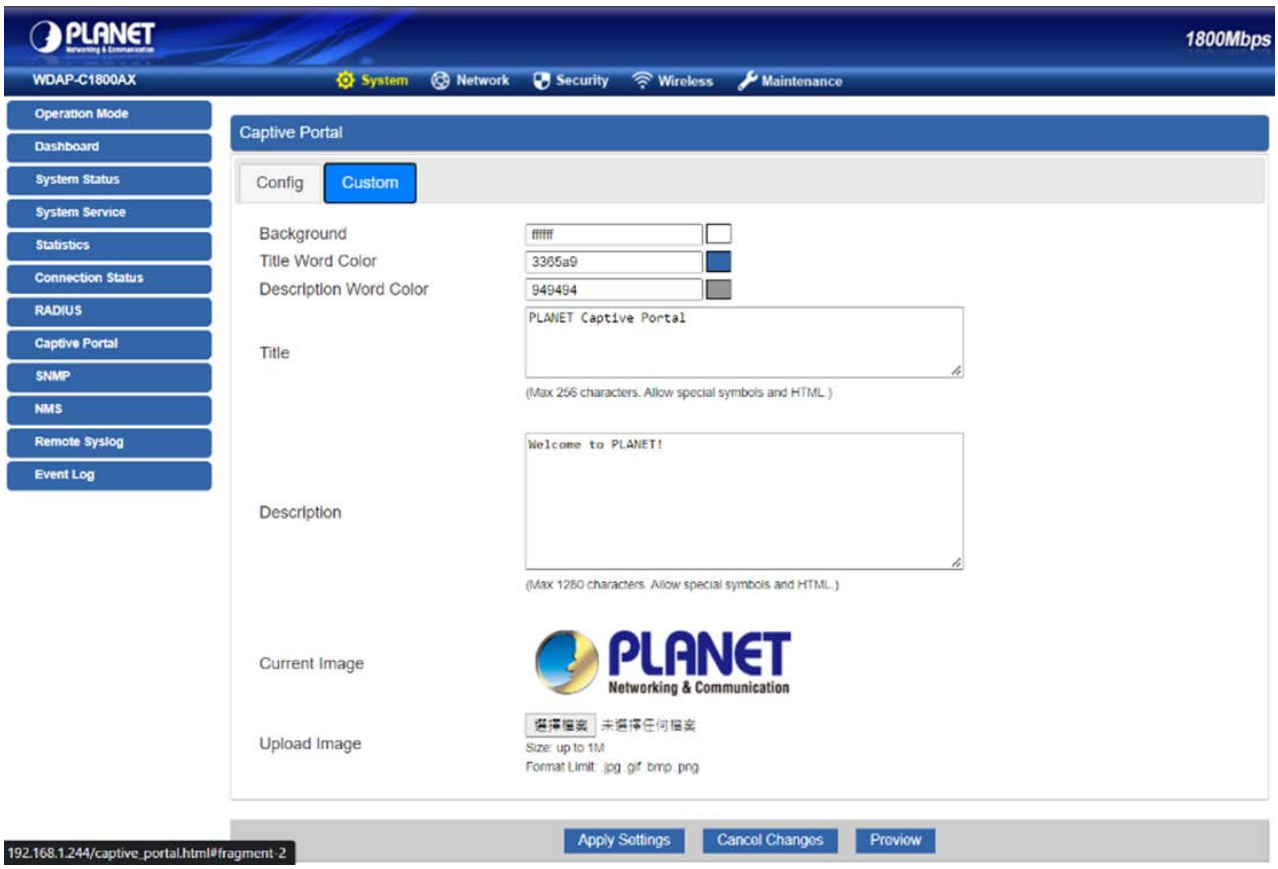
Step 4.Radius server setup web page.





Step 5.Captive Portal setup web page.



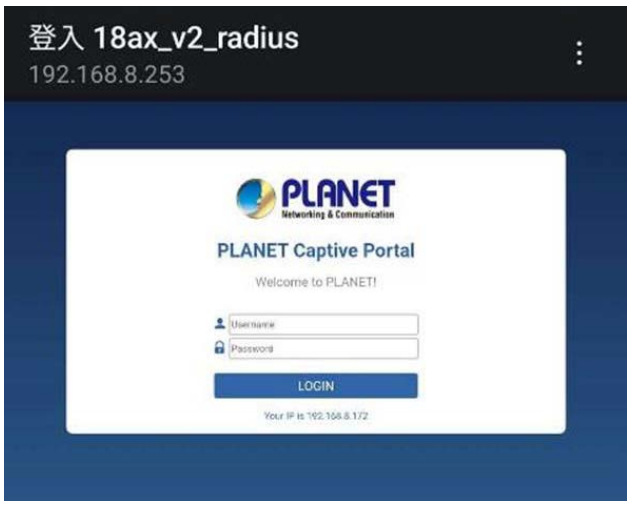


Step 6.Setup Completed.

Step 7.The WIFI client connects to the WI-FI AP then input the username and password.

Step 7. The WIFI client connects to the WI-FI AP then input the username, password and select without CA verification required.

Step 8. The Captive Portal login screen appears, input the username and password then the WIFI client can access the Internet.


登入 18ax_v2_radius
192.168.8.253
PLANET
Networking & Communication
PLANET Captive Portal
Welcome to PLANET!
Username
Password
LOGIN
Your IP is 192.168.8.172

Appendix C: Troubleshooting

If you find the AP is working improperly or stop responding to you, please read this troubleshooting first before contacting the dealer for help. Some problems can be solved by yourself within a very short time.

Scenario	Solution
The AP is not responding to me when I want to access it by Web browser.	a. Please check the connection of the power cord and the Ethernet cable of this AP. All cords and cables should be correctly and firmly inserted into the AP. b. If all LEDs on this AP are off, please check the status of power adapter, and make sure it is correctly powered. c. You must use the same IP address section which AP uses. d. Are you using MAC or IP address filter? Try to connect the AP by another computer and see if it works; if not, please reset the AP to the factory default settings by pressing the 'reset' button for over 7 seconds. e. Use the Smart Discovery Tool to see if you can find the AP or not. f. If you did a firmware upgrade and this happens, contact your dealer of purchase for help. g. If all the solutions above don't work, contact the dealer for help.
I can't get connected to the Internet.	a. Go to 'Status' -> 'Internet Connection' menu on the Industrial 802.11ax Wireless AP connected to the AP, and check Internet connection status. b. Please be patient. Sometimes Internet is just that slow. c. If you've connected a computer to Internet directly before, try to do that again, and check if you can get connected to Internet with your computer directly attached to the device provided by your Internet service provider. d. Check PPPoE / L2TP / PPTP user ID and password entered in the Industrial 802.11ax Wireless AP's settings again. e. Call your Internet service provider and check if there's something wrong with their service.

Scenario	Solution
	f. If you just can't connect to one or more website, but you can still use other internet services, please check URL/Keyword filter. g. Try to reset the AP and try again later. h. Reset the device provided by your Internet service provider too. i. Try to use IP address instead of host name. If you can use IP address to communicate with a remote server, but can't use host name, please check DNS setting.
I can't locate my AP by my wireless device.	a. 'Broadcast ESSID' set to off? b. Both two antennas are properly secured. c. Are you too far from your AP? Try to get closer. d. Please remember that you have to input ESSID on your wireless client manually, if ESSID broadcast is disabled.
File downloading is very slow or breaks frequently.	a. Internet is slow sometimes. Please be patient. b. Try to reset the AP and see if it's better after that. c. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. d. If this never happens before, call you Internet service provider to know if there is something wrong with their network.
I can't log into the web management interface; the password is wrong.	a. Make sure you're connecting to the correct IP address of the AP. b. Password is case-sensitive. Make sure the 'Caps Lock' light is not illuminated. c. If you really forget the password, do a hard reset.
The AP becomes hot	a. This is not a malfunction, if you can keep your hand on the AP's case. b. If you smell something wrong or see the smoke coming out from AP or A/C power adapter, please disconnect the AP and power source from utility power (make sure it's safe before you're doing this), and call your dealer of purchase for help.

Appendix D: Glossary

- **802.11ax** - 802.11ax is a wireless networking standard in the 802.11 family by adding OFDMA, MU-MIMO (which is marketed under the brand name Wi-Fi 6), developed in the IEEE Standards Association process, providing high-throughput wireless local area networks (WLANs) on the 5GHz band 20、40、80、160MHz.
- **802.11ac** - 802.11ac is a wireless networking standard in the 802.11 family by adding MU-MIMO (which is marketed under the brand name Wi-Fi 5), developed in the IEEE Standards Association process, providing high-throughput wireless local area networks (WLANs) on the 5GHz band.
- **802.11n -** 802.11n builds upon previous 802.11 standards by adding MIMO (multiple-input multiple-output). MIMO uses multiple transmitter and receiver antennas to allow for increased data throughput via spatial multiplexing and increased range by exploiting the spatial diversity, perhaps through coding schemes like Alamouti coding. The Enhanced Wireless Consortium (EWC) [3] was formed to help accelerate the IEEE 802.11n development process and promote a technology specification for interoperability of next-generation wireless local area networking (WLAN) products.
- **802.11a** - 802.11a was an amendment to the IEEE 802.11 wireless local network specifications that defined requirements for an orthogonal frequency division multiplexing (OFDM) communication system. It was originally designed to support wireless communication in the unlicensed national information infrastructure (U-NII) bands (in the 5–6 GHz frequency range) as regulated in the United States by the Code of Federal Regulations, Title 47, Section 15.407.
- **802.11b -** The 802.11b standard specifies a wireless networking at 11 Mbps using direct-sequence spread-spectrum (DSSS) technology and operating in the unlicensed radio spectrum at 2.4GHzHz, and WEP encryption for security. 802.11b networks are also referred to as Wi-Fi networks.
- **802.11g -** specification for wireless networking at 54 Mbps using direct-sequence spread-spectrum (DSSS) technology, using OFDM modulation and operating in the unlicensed radio spectrum at 2.4GHzHz, and backward compatibility with IEEE 802.11b devices, and WEP encryption for security.
- **DDNS** (**D**ynamic **D**omain **N**ame **S**ystem) **-** The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP** (**D**ynamic **H**ost **C**onfiguration **P**rotocol) **-** A protocol that automatically configure the

TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.

- **DMZ** (**Dem**ilitarized **Z**one) **-** A Demilitarized Zone allows one local host to be exposed to the Internet for a special-purpose service such as Internet gaming or videoconferencing.
- **DNS** (**D**omain **N**ame **S**ystem) **-** An Internet Service that translates the names of websites into IP addresses.
- **Domain Name -** A descriptive name for an address or group of addresses on the Internet.
- **DSL** (**D**igital **S**ubscriber **L**ine) **-** A technology that allows data to be sent or received over existing traditional phone lines.
- **MTU** (**Maximum Transmission Unit**) **-** The size in bytes of the largest packet that can be transmitted.
- **NAT** (**N**etwork **A**ddress **T**ranslation) **-** NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE** (**P**oint to **P**oint **P**rotocol **o**ver **E**thernet) **-** PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID -** A **S**ervice **S**et **Id**entification is a thirty-two character (maximum) alphanumeric key identifying a wireless local area network. For the wireless devices in a network to communicate with each other, all devices must be configured with the same SSID. This is typically the configuration parameter for a wireless PC card. It corresponds to the ESSID in the wireless Access Point and to the wireless network name.
- **WEP** (**W**ired **E**quivalent **P**rivacy) **-** A data privacy mechanism based on a 64-bit or 128-bit or 152-bit shared key algorithm, as described in the IEEE 802.11 standard.
- **Wi-Fi -** A trade name for the 802.11b wireless networking standard, given by the Wireless Ethernet Compatibility Alliance (WECA, see http://www.wi-fi.net), an industry standards group promoting interoperability among 802.11b devices.
- **WLAN** (**W**ireless **L**ocal **A**rea **N**etwork) **-** A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

EC Declaration of Conformity

English	Hereby, PLANET Technology Corporation, declares that this 11ac Wireless AP is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.	Lietuviškai	Šiuo PLANET Technology Corporation,, skelbia, kad 11ac Wireless AP tenkina visus svarbiausius 2014/53/EU direktyvos reikalavimus ir kitas svarbias nuostatas.
Česky	Společnost PLANET Technology Corporation, tímto prohlašuje, že tato 11ac Wireless AP splňuje základní požadavky a další příslušná ustanovení směrnice 2014/53/EU.	Magyar	A gyártó PLANET Technology Corporation, kijelenti, hogy ez a 11ac Wireless AP megfelel az 2014/53/EU irányelv alapkövetelményeinek és a kapcsolódó rendelkezéseknek.
Dansk	PLANET Technology Corporation, erklærer herved, at følgende udstyr 11ac Wireless AP overholder de væsentlige krav og øvrige relevante krav i direktiv 2014/53/EU	Malti	Hawnhekk, PLANET Technology Corporation, jiddikjara li dan 11ac Wireless AP jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 2014/53/EU
Deutsch	Hiermit erklärt PLANET Technology Corporation, dass sich dieses Gerät 11ac Wireless AP in Übereinstimmung mit den grundlegenden Anforderungen und den anderen relevanten Vorschriften der Richtlinie 2014/53/EU befindet". (BMWi)	Nederlands	Hierbij verklaart , PLANET Technology orporation, dat 11ac Wireless AP in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 2014/53/EU
Eestikeeles	Käesolevaga kinnitab PLANET Technology Corporation, et see 11ac Wireless AP vastab Euroopa Nõukogu direktiivi 2014/53/EU põhinõuetele ja muudele olulistele tingimustele.	Polski	Niniejszym firma PLANET Technology Corporation, oświadcza, że 11ac Wireless AP spełnia wszystkie istotne wymogi i klauzule zawarte w dokumencie „Directive 2014/53/EU.
Ελληνικά	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* , PLANET Technology Corporation, *ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ* 11ac Wireless AP*ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ* 2014/53/EU	Português	PLANET Technology Corporation, declara que este 11ac Wireless AP está conforme com os requisitos essenciais e outras disposições da Directiva 2014/53/EU.

Español	Por medio de la presente, PLANET Technology Corporation, declara que 11ac Wireless AP cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 2014/53/EU	Slovensky	Výrobca PLANET Technology Corporation, týmto deklaruje, že táto 11ac Wireless AP je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 2014/53/EU.
Français	Par la présente, PLANET Technology Corporation, déclare que les appareils du 11ac Wireless AP sont conformes aux exigences essentielles et aux autres dispositions pertinentes de la directive 2014/53/EU	Slovensko	PLANET Technology Corporation, s tem potrjuje, da je ta 11ac Wireless AP skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 2014/53/EU
Italiano	Con la presente , PLANET Technology Corporation, dichiara che questo 11ac Wireless AP è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 2014/53/EU.	Suomi	PLANET Technology Corporation, vakuuttaa täten että 11ac Wireless AP tyyppinen laite on direktiivin 2014/53/EU oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo PLANET Technology Corporation, apliecina, ka šī 11ac Wireless AP atbilst Direktīvas 2014/53/EU pamatprasībām un citiem atbilstošiem noteikumiem.	Svenska	Härmed intygar, PLANET Technology Corporation, att denna 11ac Wireless AP står i överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 2014/53/EU.