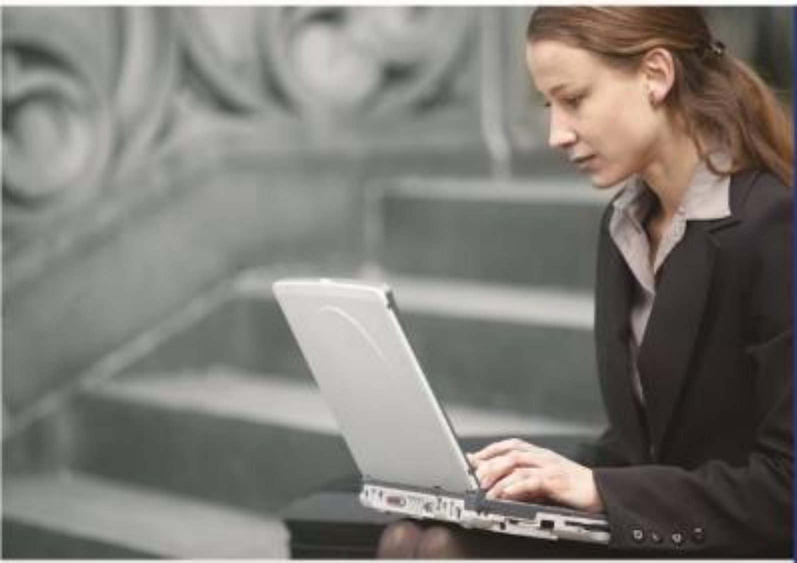
User's Manual

Industrial Dual Band 802.11be 3600Mbps Wireless Access Point with 5 10/100/1000T LAN Ports

- ► IAP-3600BE
- ► IAP-3600BE-4PF



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.

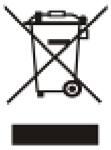
CE Compliance Statement

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 Dual Band 802.11be 3600Mbps Wireless Access Point with 5 10/100/1000T LAN Ports

Models: IAP-3600BE and IAP-3600BE-4PF

Rev.: 1.0 (August, 2025)

Part No. EM-IAP-3600BE_IAP-3600BE-4PF_v1.0

Table of Contents

Chapter 1. Product Introduction

Thank you for purchasing PLANET IAP-3600BE or IAP-3600BE-4PF Industrial Dual Band 802.11be 3600Mbps Wireless Access Point with 5 10/100/1000T LAN Ports, The descriptions of these models are as follows:

IAP-3600BE	Industrial Dual Band 802.11be 3600Mbps Wireless Access Point with 5 10/100/1000T LAN Ports
IAP-3600BE-4PF	Industrial Dual Band 802.11be 3600Mbps Wireless Access Point with 4-Port 802.3at PoE+

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

1.1 Package Contents

The package should contain the following:

Model **Item**	**IAP-3600BE**	**IAP-3600BE-4PF**
Industrial 802.11be Wireless AP	x 1	x 1
Quick Installation Guide	x 1	x 1
PLANET CloudNMS Quick Guide	x 1	x 1
Wall-mount Kit	x 1	x 1
Dual band Wi-Fi Antenna	x 2	x 2
Antenna Dust Cap	x 2	x 2
RJ45 Dust Cap	x 5	x 5
SFP Cap	--	1

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

1.2 Product Overview

Ultra-high-speed Wi-Fi 7 Wireless LAN Solution with Environmentally Hardened Design

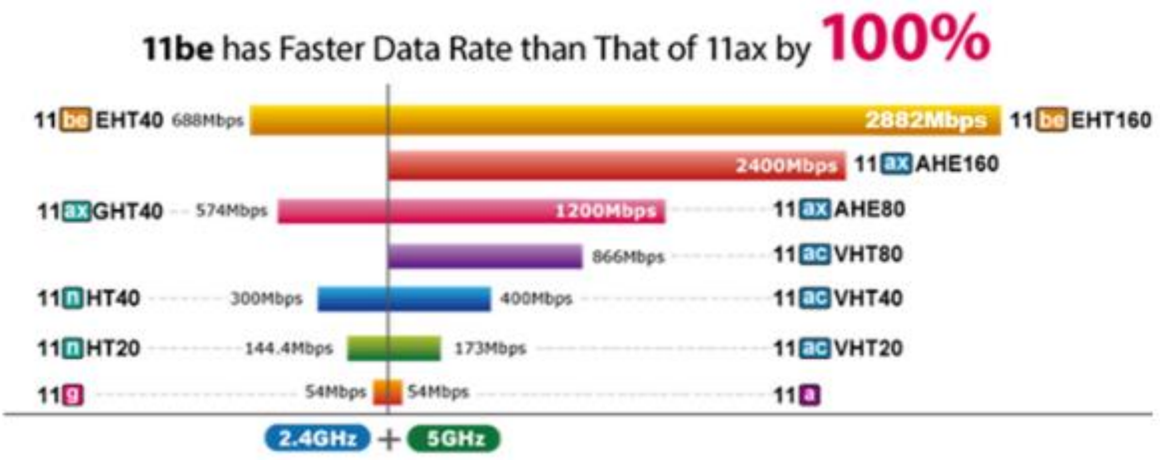
The PLANET IAP-3600BE Series Industrial Dual Band 802.11be Wireless Access Point comes with 5 × 10/100/1000T LAN ports. The IAP-3600BE-4PF model features 4 × 1000T 802.3at PoE LAN ports with a total PoE budget of 120 watts, and 1 × 1GBASE-X SFP WAN/LAN slot for flexible connectivity. Both models feature a rugged IP30-rated metal enclosure, ensuring robust performance in harsh industrial environments. Integrated with **Wi-Fi 7 (802.11be) technology**, the IAP-3600BE Series delivers exceptional wireless speeds of up to **2882 Mbps** on the 5GHz band and **688 Mbps** on the 2.4GHz band.

It supports advanced wireless capabilities including **4096-QAM**, **Multi-Link Operation (MLO)**, **MU-MIMO**, **MU-OFDMA**, and **beamforming**, enabling lower latency, greater bandwidth efficiency, and highly stable multi-user connections. Supporting up to **256 concurrent client devices**, the IAP-3600BE Series is the ideal wireless solution for mission-critical industrial applications requiring ultra-fast, reliable, and secure connectivity.

Designed to operate in extreme environments, the IAP-3600BE Series supports a wide temperature range from -40 to 70 degree C, making it ideal for deployment in harsh and demanding conditions. It also features flexible installation options with both DIN rail and wall-mount support, maximizing space efficiency within industrial cabinets.

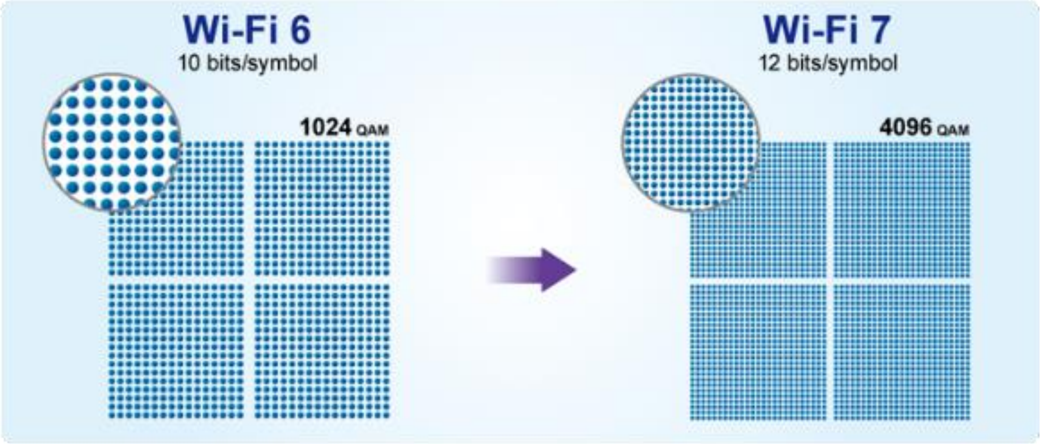
High-Performance Dual Band Wi-Fi 7 Solution

The IAP-3600BE Series, compliant with the latest IEEE 802.11be Wi-Fi 7 standard, delivers ultra-high-speed and low-latency wireless connectivity. It supports maximum data rates of up to **688Mbps on the 2.4GHz band** (40MHz) and **2882Mbps on the 5GHz band** (160MHz), enabling lightning-fast transmission across both frequency bands. With **dual-band concurrent operation**, users can benefit from improved bandwidth, reduced congestion, and more stable connections in high-density environments.



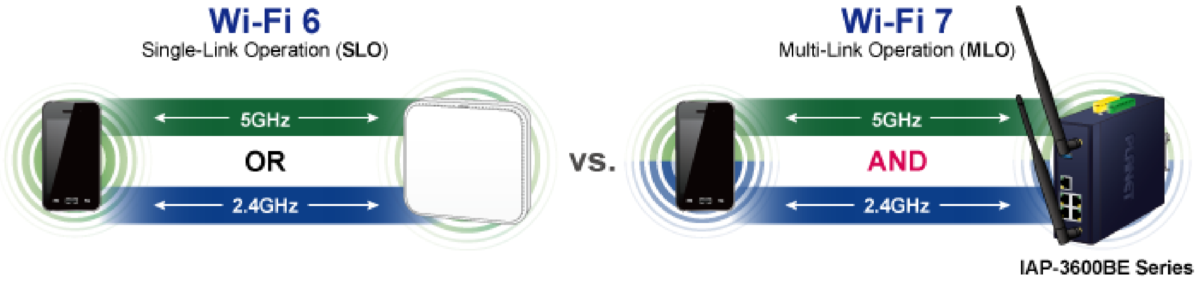
Boost Network Throughput with 4096-QAM

With 4096-QAM encoding, the IAP-3600BE Series transmits more data per signal, increasing throughput and making it ideal for high-bandwidth applications such as 4K/8K video streaming, AR/VR experiences, and real-time cloud services while maintaining a stable and efficient network connection.



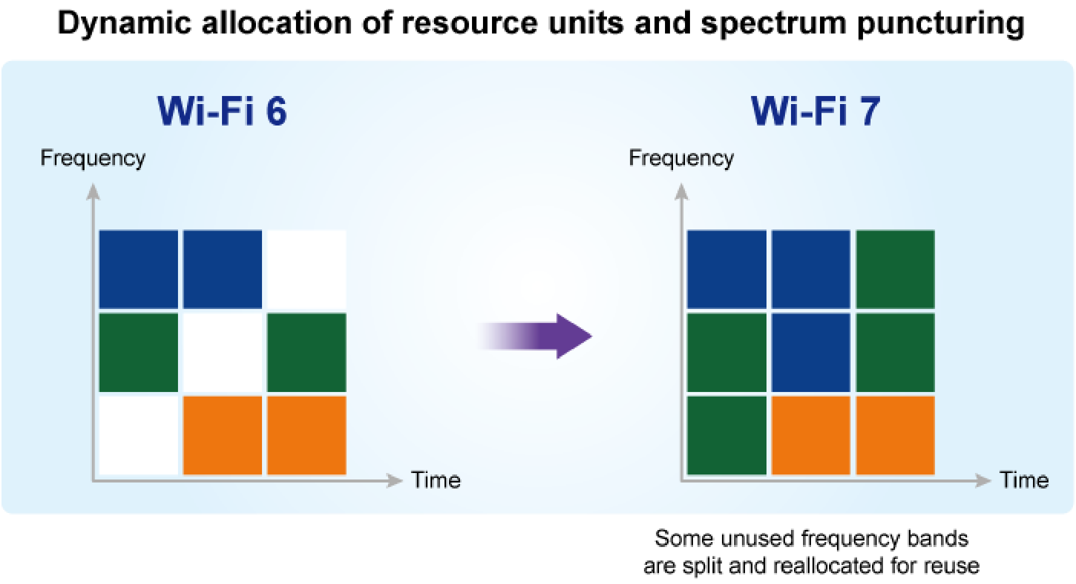
Seamless Connectivity and Peak Network Performance

Designed for robust dual-band operation, the IAP-3600BE Series ensures seamless connectivity across both 2.4 GHz and 5 GHz frequencies. This design guarantees consistent data transfer and stable connections even in interference-prone, high-density scenarios, delivering the reliability demanded by modern commercial applications.



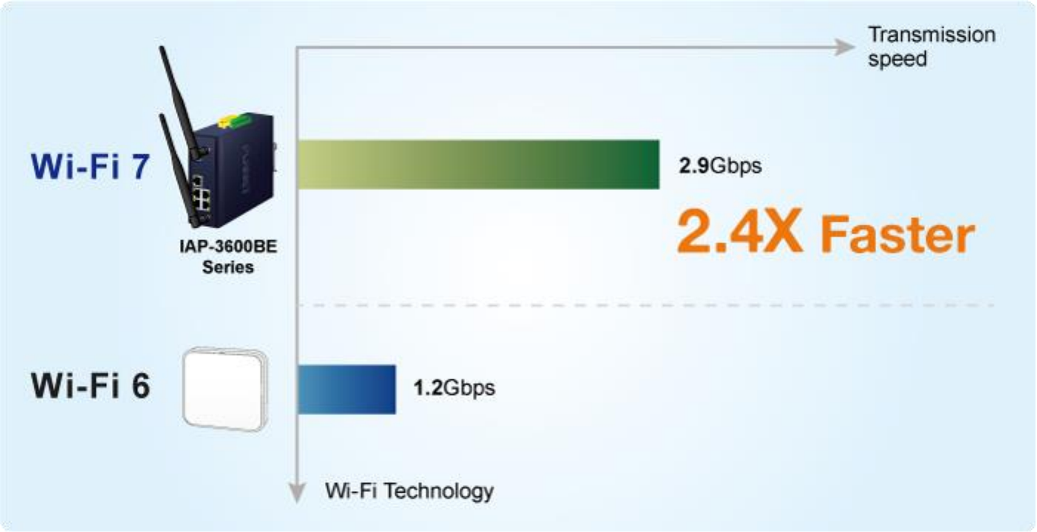
Optimize Spectrum Utilization

Employing advanced techniques such as dynamic allocation of resource units and spectrum puncturing, the IAP-3600BE Series minimizes spectrum waste and maximizes efficiency in densely-populated wireless environments, further enhancing overall network performance and business productivity.


Dynamic allocation of resource units and spectrum puncturing
Wi-Fi 6
Frequency
Time
Wi-Fi 7
Frequency
Time
Some unused frequency bands are split and reallocated for reuse

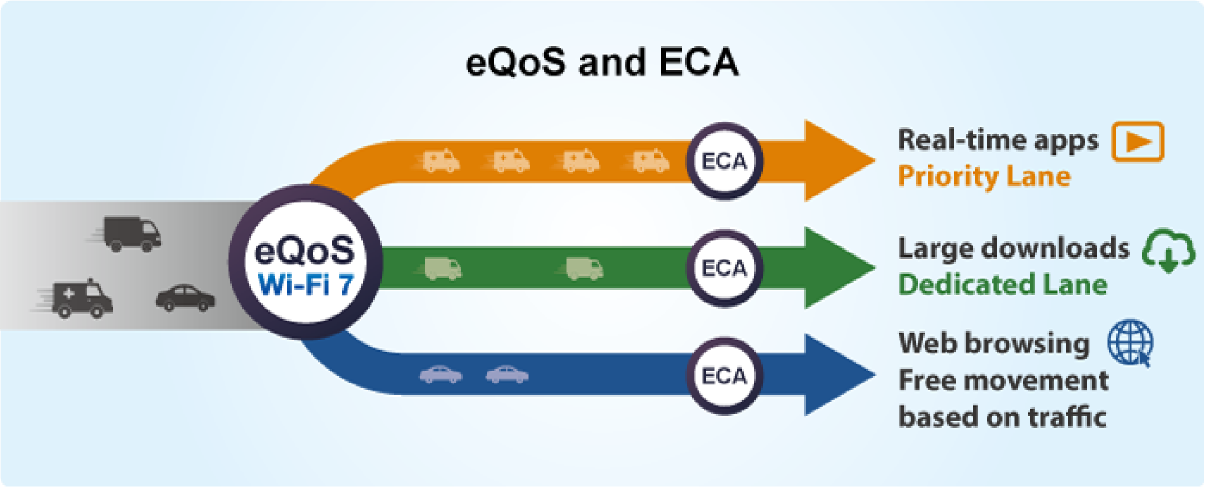
Business-Oriented Wi-Fi 7 Performance in Industrial Environments

The **IAP-3600BE Series** is purpose-built for enterprise and industrial applications, prioritizing network stability, high performance, and environmental durability. Supporting the latest **Wi-Fi 7 (802.11be)** standard, it delivers impressive wireless speeds of up to **2882Mbps on the 5GHz band** and **688Mbps on the 2.4GHz band**, providing nearly **2.4 times the throughput of Wi-Fi 6** in real-world scenarios.



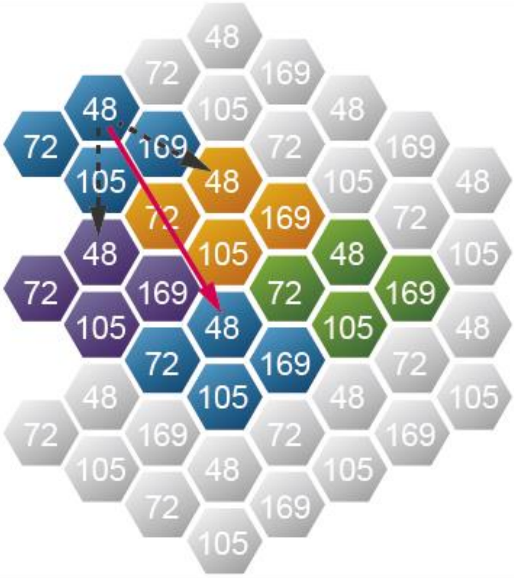
Ultra-low Latency and Jitter for Real-time Industrial Applications

Equipped with advanced Quality of Service (eQoS) and enhanced channel access mechanisms, the **IAP-3600BE Series** intelligently prioritizes latency-sensitive data traffic, minimizing delay and jitter. This ensures consistent, real-time performance for mission-critical applications such as **remote machine control, industrial AR/VR**, **video surveillance**, and **low-latency communication in automation systems**.



Precision Interference Control for Seamless Industrial Connectivity

The **IAP-3600BE Series** incorporates **BSS Coloring** technology to intelligently differentiate overlapping basic service sets (BSS), effectively minimizing co-channel interference and maintaining stable wireless connections in high-density environments. Additionally, **beamforming** enhances signal strength and coverage by directing Wi-Fi signals toward active client devices, ensuring consistent performance throughout industrial deployment zones.

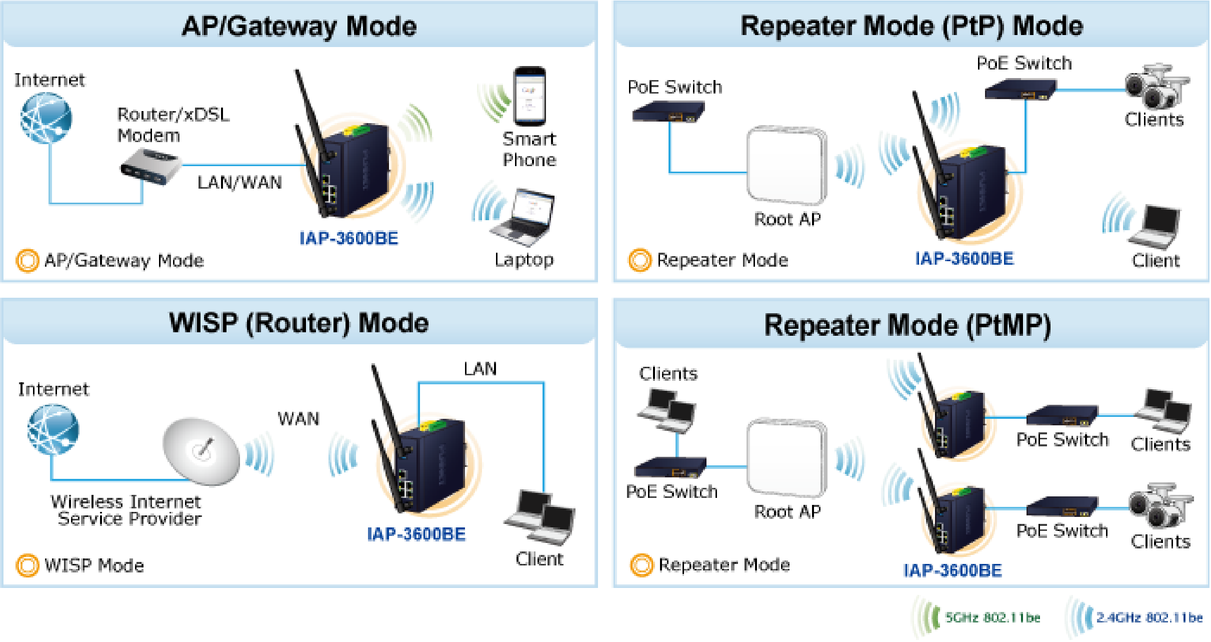


Advanced Wireless Security for Industrial Networks

The **IAP-3600BE Series** supports advanced wireless encryption standards including **WPA3-PSK**, **WPA2-PSK**, and **WPA/WPA2-Enterprise**, providing strong data protection and preventing unauthorized network access. For enhanced access control, administrators can configure **predefined Access Control Lists (ACLs)**, making it a reliable and secure solution for sensitive industrial and enterprise applications.

Flexible Deployment Modes and Centralized Management

The **IAP-3600BE Series** supports multiple operation modes—including **Access Point, Gateway, Repeater, and WISP**—to flexibly adapt to a wide range of industrial and enterprise deployment scenarios, whether establishing a new infrastructure or upgrading an existing one. With **intuitive remote management via the PLANET CloudNMSPro app and centralized NMS**, it streamlines installation, monitoring, and ongoing maintenance across distributed networks.



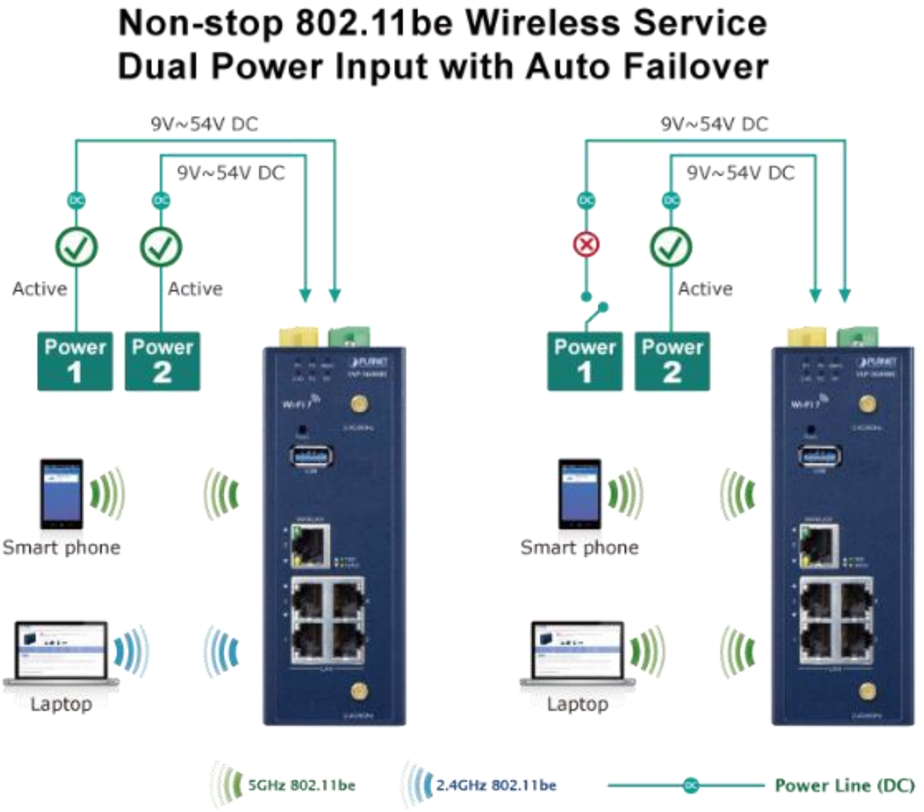
Home Dashboard for Wi-Fi Status
CloudViewer Pro
Setup Wizard for Multiple Modes

Built-in Cybersecurity Features for Industrial Network Protection

The **IAP-3600BE Series** supports **TLS v1.3** for secure remote access and encrypted management traffic, ensuring strong protection against modern cyber threats. It also includes enterprise-grade security features such as **SNMPv3 with authentication and encryption**, **Access Control Lists (ACLs)**, **WPA3 encryption**, and **802.1X authentication**, forming a comprehensive defense against unauthorized access and data breaches.

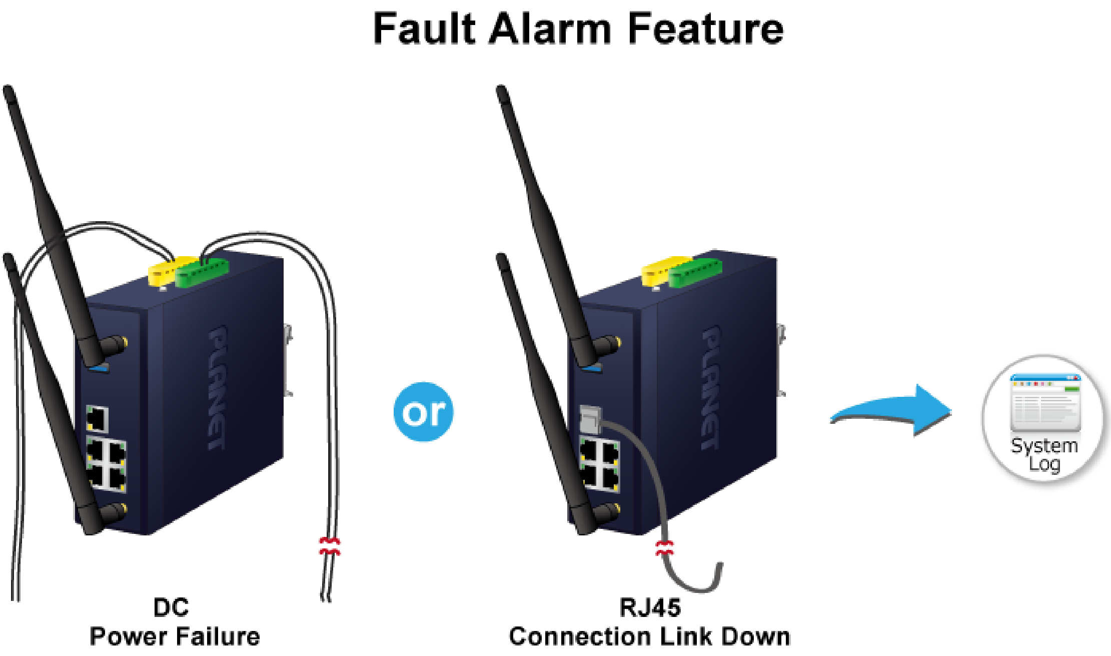
Dual Power Input for High Availability Network System

The IAP-3600BE Series features a strong dual power input system with wide-ranging voltages (IAP-3600BE support 9V~54V DC and IAP-3600BE-4PF support 48V~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-3600BE Series via power supply 2 alternatively without any loss of operation.



Effective Alarm Alert for Better Protection

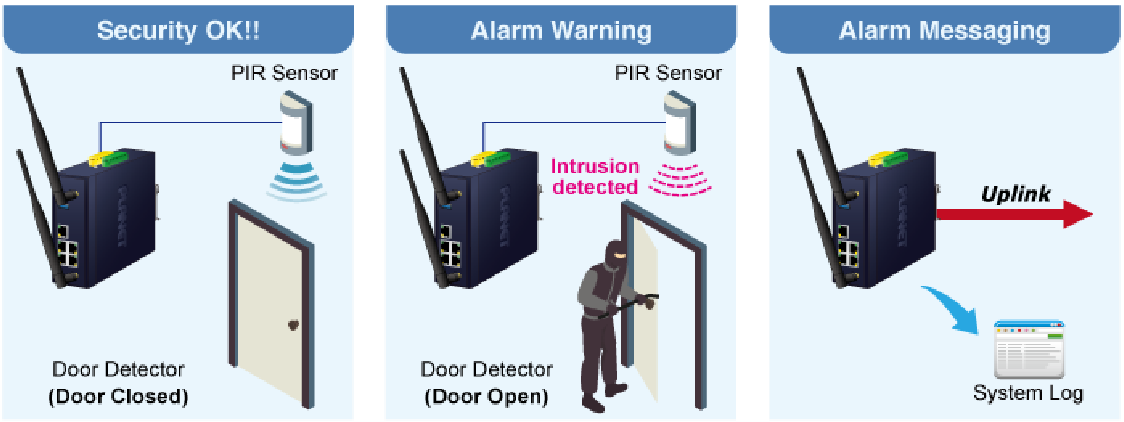
The IAP-3600BE Series supports a Fault Alarm feature which can alert the users when there is something wrong with the device. With this ideal feature, the users would not have to waste time finding where the issue is. It will help to save time and human resource.



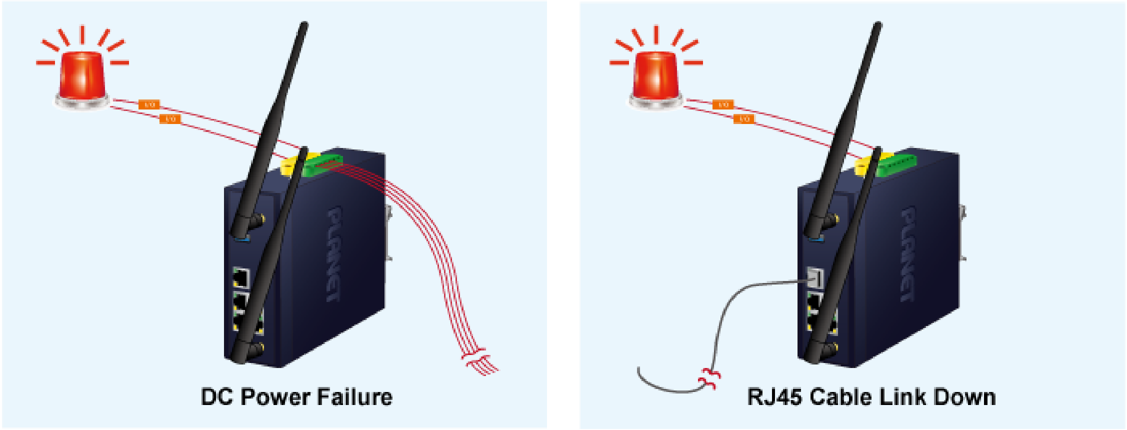
Digital Input and Digital Output for External Alarm

The IAP-3600BE Series 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-3600BE Series port shows link down, link up or power failure.

Digital Input



Digital Output



Flexible and Easy Installation with Limited Space

The compact-sized IAP-3600BE Series 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.

Optional installation method

DIN-rail Mounting
Wall Mounting
Side Wall Mounting (Space saving)

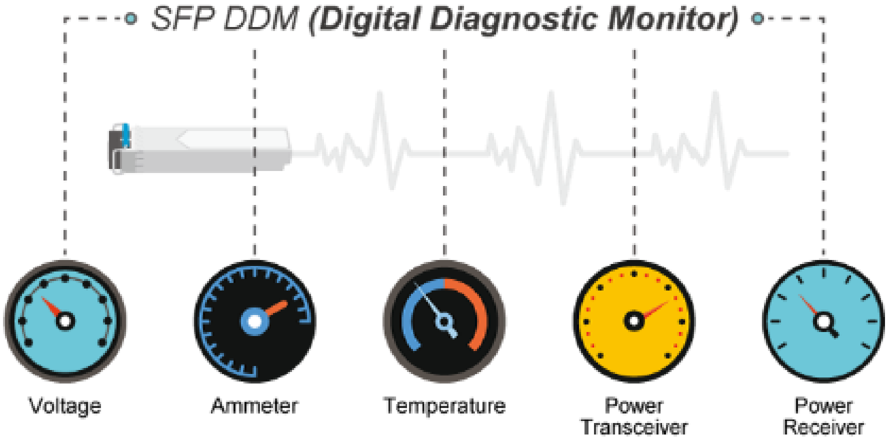
* The above pictures are for illustration only.

Flexible WAN interface Enables Extension of Network Deployment

The IAP-3600BE-4PF provides both copper and fiber connectors for WAN interface. With one SFP slot, it supports fiber extension for FTTX application. It allows the administrator to flexibly choose the suitable SFP transceiver according to the transmission distance required to extend the network efficiently. The distance can be extended from 550 meters to 2 kilometers (multi-mode fiber) and 10/20/40/80/120 kilometers (single-mode fiber or WDM fiber). They are well suited for applications to uplink to backbone switch and monitoring center in long distance.

Intelligent SFP Diagnosis Mechanism

The IAP-3600BE-4PF supports SFP-DDM (digital diagnostic monitor) function that greatly helps network administrator to easily monitor real-time parameters of the SFP, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage.



Built-in Unique PoE Functions for Powered Devices Management

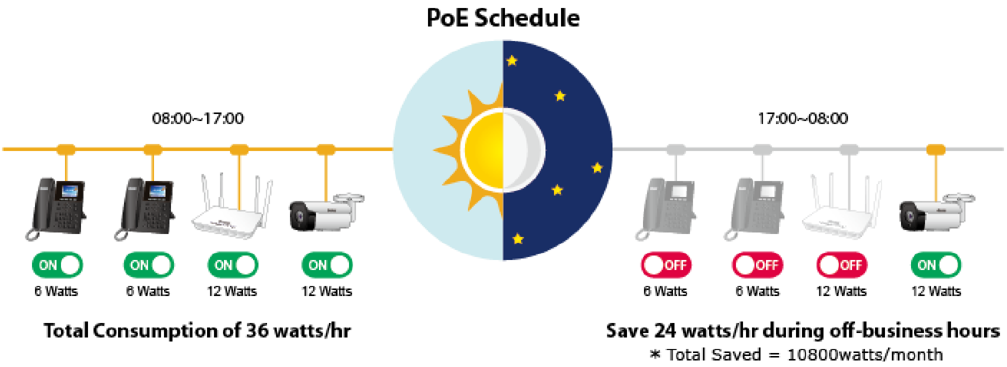
The IAP-3600BE-4PF is capable of having a maximum of up to 120 watts of power output and can deliver **up to 36W** for each port. It also features the following special PoE management functions.

PoE Usage Monitoring

With PoE usage monitoring, it can show the PoE loading of each port, total PoE power usage and system status, such as overload, low voltage, over voltage and high temperature. User can obtain detailed information about the real-time PoE working condition of the IAP-3600BE-4PF directly.

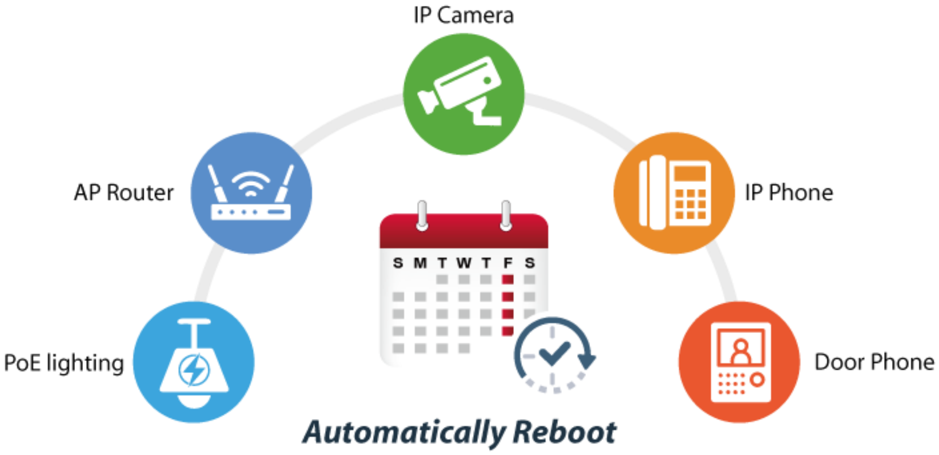
PoE Schedule

Under the trend of energy saving worldwide and contributing to environmental protection, the IAP-3600BE-4PF can effectively control the power supply besides its capability of giving high watts power. The “PoE schedule” function helps you to enable or disable PoE power feeding for each PoE port during specified time intervals and it is a powerful function to help SMBs or enterprises save power and budget. It also increases security by powering off PDs that should not be in use during non-business hours.



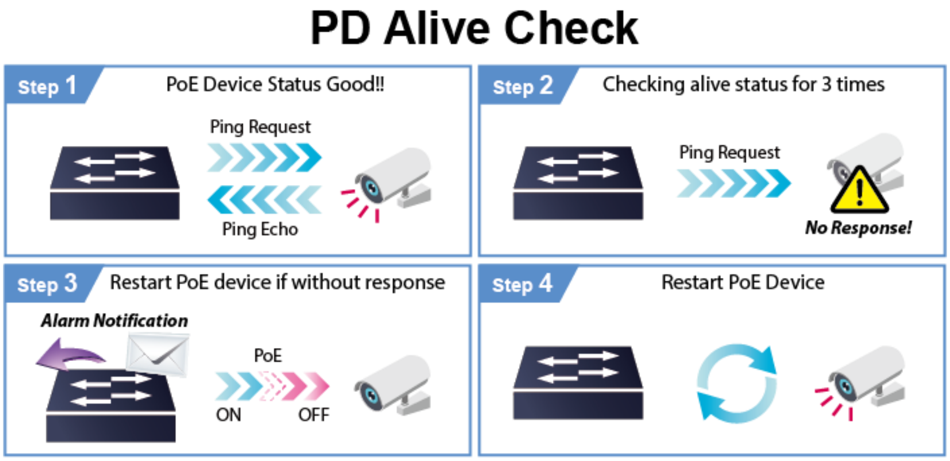
Scheduled Power Recycling

The IAP-3600BE-4PF allows each of the connected PoE IP cameras or PoE wireless access points to reboot at a specific time each week. Therefore, it will reduce the chance of IP camera or AP crash resulting from buffer overflow.



PD Alive Check

The IAP-3600BE-4PF can be configured to monitor connected PD status in real time via ping action. Once the PD stops working and responding, the IAP-3600BE-4PF will resume the PoE port power and bring the PD back to work. It will greatly enhance the network reliability through the PoE port resetting the PD's power source and reducing administrator management burden.



1.3 Product Features

- **Physical Interfaces**
  - 4 x 10/100/1000BASE-T RJ45 LAN ports, auto-negotiation, auto MDI/MDI-X (Port 1 to Port 4)
  - 4 x 10/100/1000BASE-T RJ45 LAN ports with 4-port IEEE 802.3at PoE+ injector function (Fo IAP-3600BE-4PF)
  - 1 x 10/100/1000BASE-T RJ45 WAN/LAN port, auto-negotiation, auto MDI/MDI-X (Port 5)
  - 1 x 1000BASE-X SFP interface WAN/LAN port(Fo IAP-3600BE-4PF)
  - 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

- **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(Fo IAP-3600BE)
  - DC 48-54V, redundant power with reverse polarity protection(Fo IAP-3600BE-4PF)
  - -40 to 70 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 mode, WISP mode and Gateway mode options

- **Industrial-Grade Wireless LAN Compliance**
  - Supports Wi-Fi 7 (IEEE 802.11be), the latest generation of wireless networking technology
  - Backward compatible with 2.4GHz (802.11b/g/n/ax/be), 5GHz (802.11a/n/ac/ax/be) frequency bands

RF Interface Characteristics

- 802.11be 2T2R architecture with data rates up to 3600Mbps (688Mbps in 2.4GHz and 2882Mbps in 5GHz)
- High output power with multi-level 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-based Access Control Lists (ACL) for enhanced device-level security

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
- NEW: Supports Wi-Fi 7 enhancements, including:
  - 4096-QAM for higher data rates
  - Multi-Link Operation (MLO) for simultaneous multi-band transmission

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
- PLANET Smart Discovery Utility for deployment management
- PLANET NMS system and CloudNMS for deployment management

- **Power over Ethernet**
  - Complies with IEEE 802.3at Power over Ethernet Plus, end-span PSE
  - Backward compatible with IEEE 802.3af Power over Ethernet
  - Up to 4 ports of IEEE 802.3af / 802.3at devices powered
  - Supports PoE power up to 36 watts for each PoE port
  - Auto detects powered device (PD)
  - Circuit protection prevents power interference between ports
  - PoE management
  - Total PoE power budget control

    - Per port PoE function enable/disable
    - PoE port power feeding priority
    - Per PoE port power limitation
    - PD classification detection
    - PD alive check

1.4 Product Specifications

Product	IAP-3600BE	IAP-3600BE-4PF
Hardware Specifications		
Copper Ports	5 10/100/1000BASE-T RJ45 Ethernet ports including • 4 LAN ports (Ports 1 to 4) • 1 WAN/LAN port (Port 5)	
Fiber Port	--	1 1000BASE-X SFP slot including 1 WAN/LAN port (Port 6)
Wireless Connector	Built-in two 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	881g	905g
Power Requirements – DC	9~54V DC, 1.8A	48~54V DC, 3.5A
Power Consumption	Max. 6.48 watts/ 22.09BTU (No Loading at DC 54V) Max.11.88 watts/ 40.51BTU (Full loading at DC 54V)	Max. 9.18 watts/ 31.3BTU (No Loading at DC 54V) Max.142.8 watts/ 486.94BTU (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):** 1000 LNK/ACT (Green) 10/100 LNK/ACT (Amber) **Wi-Fi:**	**System:** P1 (Green) P2 (Green) Alarm (Red) I/O (Red) **Ethernet Interfaces (Ports 1-4 Ports):** 10/100/1000 LNK/ACT (Green) PoE-in-Use (Amber) **Ethernet Interfaces (Port 5 WAN/LAN Port):**

	2.4GHz(Green)
	5GHz(Green)
		10/100/1000 LNK/ACT (Green)
		1000 LNK (Amber)
		1000BASE-X SFP Interfaces (Port 6):
		LNK/ACT (Green)
		Wi-Fi:
		2.4GHz(Green)
		5GHz(Green)

Wireless Specifications		
Wi-Fi Standard	IEEE 802.11a/n/an/ac/ax/be 5GHz (2Tx2R) IEEE 802.11g/b/n/ax/be 2.4GHz (2Tx2R)	
Band Mode	2.4GHz & 5GHz concurrent mode	
Data Modulation	802.11be: MIMO-OFDM/OFDMA (BPSK / QPSK / 16QAM / 64QAM / 256QAM / 1024QAM / 4096QAM) 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)	
Antenna	4 dBi 2.4GHz and 5GHz dual-band 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
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: 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.
Channel Width	20MHz, 40MHz, 80MHz, 160MHz	
Data Transmission Rates	Transmit: 688 Mbps* for 2.4 GHz and 2882 Mbps* for 5 GHz Receive: 688 Mbps* for 2.4 GHz and 2882 Mbps* for 5 GHz ***The estimated transmission distance is based on the theory. The**	

	actual distance may vary in different environments.
Transmission Power	**2.4 GHz:** 11b CCK：1 M 23.5 dBm ±2 dB；11 M 23.5 dBm ±2 dB。 11g OFDM：54 M 20.5 dBm ±2 dB 11n HT20：MCS0 21 dBm ±2 dB；MCS7 19 dBm ±2 dB 11n HT40：MCS0 20 dBm ±2 dB；MCS7 18 dBm ±2 dB 11ax HE-SU40：MCS0 21 dBm ±2 dB；MCS11 17.5 dBm ±2 dB 11be EHTMU-SU40：MCS0 21 dBm ±2 dB；MCS13 16.5 dBm ±2 dB **5 GHz:** 11a OFDM：6 M 23 dBm ±1.5 dB；54 M 20.5 dBm ±1.5 dB 11ac VHT20：MCS0 21.5 dBm ±1.5 dB；MCS8 19 dBm ±1.5 dB 11ax HE-SU20：MCS0 21.5 dBm ±1.5 dB；MCS11 18.5 dBm ±1.5 dB 11be EHTMU-SU20：MCS0 21.5 dBm ±1.5 dB；MCS13 17 dBm ±1.5 dB 11ac VHT40：MCS0 21 dBm ±1.5 dB；MCS9 19 dBm ±1.5 dB 11ax HE-SU40：MCS0 21 dBm ±1.5 dB；MCS11 18.5 dBm ±1.5 dB 11be EHTMU-SU40：MCS0 21 dBm ±1.5 dB；MCS13 16.5 dBm ±1.5 dB 11ac VHT80：MCS0 21 dBm ±1.5 dB；MCS9 18 dBm ±1.5 dB 11ax HE-SU80：MCS0 21 dBm ±1.5 dB；MCS11 17.5 dBm ±1.5 dB 11be EHTMU-SU80：MCS0 21 dBm ±1.5 dB；MCS13 16 dBm ±1.5 dB 11ac VHT160：MCS0 20 dBm ±1.5 dB；MCS9 16 dBm ±1.5 dB 11ax HE-SU160：MCS0 20 dBm ±1.5 dB；MCS11 15 dBm ±1.5 dB 11be EHTMU-SU160：MCS0 20 dBm ±1.5 dB；MCS13 13 dBm ±1.5 dB
Receiver Sensitivity	**2.4 GHz** 11b CCK 11 M: -93 11g OFDM 54 M: -77 11n HT20 MCS7: -74 11n HT40 MCS7: -71 11ax HE20 MCS11: -62 11ax HE40 MCS11: -59 11be EHT20 MCS13: -61 11be EHT40 MCS13: -58 **5 GHz** 11a OFDM 54 M: -77 11n HT20 MCS7: -74 11n HT40 MCS7: -71 11ac VHT20 MCS9: -63 11ac VHT40 MCS9: -60 11ac VHT80 MCS9: -57 11ac VHT160 MCS9: -54 11ax HE20 MCS11: -63 11ax HE40 MCS11: -60 11ax HE80 MCS11: -57 11ax HE160 MCS11: -54 11be EHT20 MCS13: -61 11be EHT40 MCS13: -58 11be EHT80 MCS13: -55 11be EHT160 MCS13: -52
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	
Power over Ethrenet		
PoE Standard	--	IEEE 802.3af / 802.3at PoE+ PSE
PoE Power Supply Type	--	End-span
PoE Power Output	--	Per port 54V DC, 35 watts (max.)
Power Pin Assignment	--	1/2 (+), 3/6 (-)
PoE Power Budget	--	120 watts (max.)
Max. Number of Class 4 PDs	--	4
PoE Management	--	PD Alive Check Scheduled Power Recycling PoE Schedule PoE Usage Monitoring
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	Gateway Mode WISP Mode Access Point Mode (default) Repeater Mode (Future features)	
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)	
Max. Wireless Clients	Up to **256 clients** (128 is suggested, depending on usage)	
Wi-Fi Advanced	Auto Channel Selection 5-level Transmit Power Control : ■ Max (100%)	

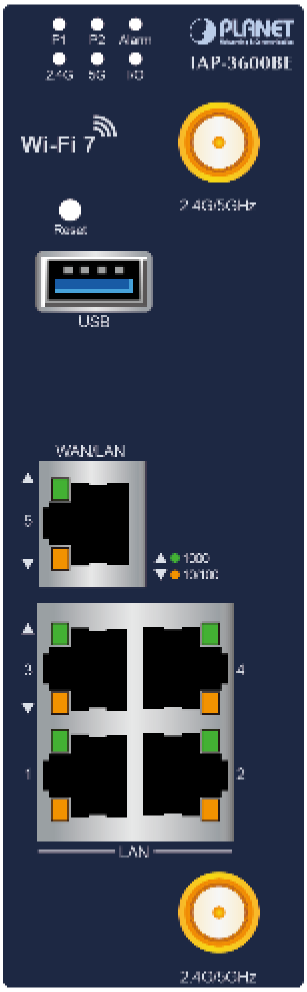
	■ Efficient (75%) ■ Enhanced (50%) ■ Standard (25%) or Min (15%) Client Limit Control Coverage Threshold *Wi-Fi channel analysis chart Seamless Roaming Beamforming BSS Coloring 2.4GHz WLAN Partition 5GHz WLAN Partition RTS Threshold
Wireless Roaming	IEEE 802.11k, 802.11v, and 802.11r
Wireless QoS	Supports 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 ● VPN Gateway: VR-300 series, IVR-300 series ● PLANET CloudNMS App, CloudNMSPro, CloudNMS.
Standards Conformance	
Regulatory Compliance	FCC Part 15 Class A, CE
Environment	
Operating	Temperature: -40 ~ 70 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-3600BE 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.

■ **WIFI**

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.

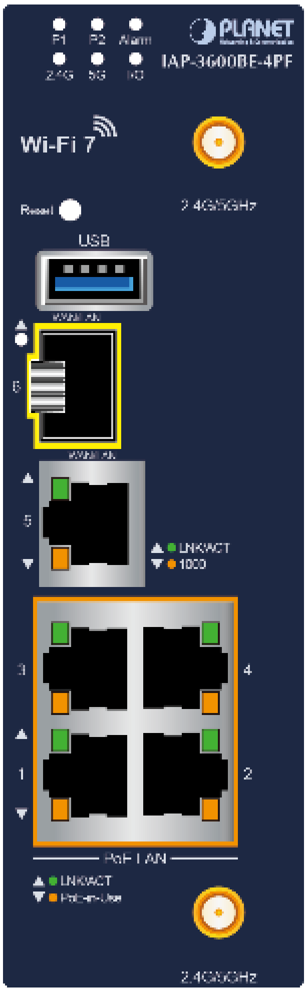
■ **LAN 10/100/1000BASE-T Interface (Port-1 to Port-4)**

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 Interfaces (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-3600BE-4PF 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.

WIFI

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 Interface (Port-1 to Port-4)

LED	Color	Function	
10/100/1000 LNK/ACT	Green	**Lights**:	To indicate that the port is operating at 1000Mbps,100Mbps or 10Mbps.
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.
PoE-In-use	Amber	**Lights**:	To indicate the port is providing DC in-line power.
		Off:	To indicate the connected device is not a PoE PD.

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

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

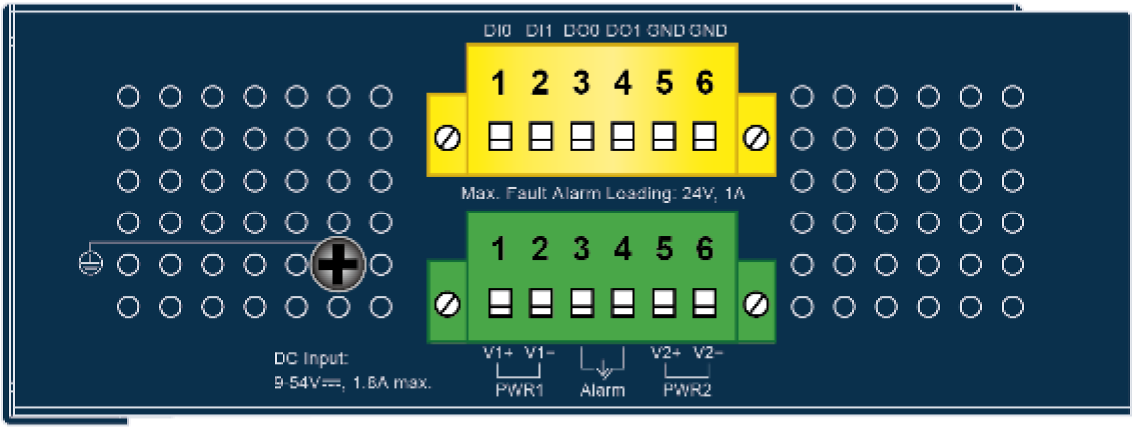
■ WAN/LAN 1000BASE-X Interfaces (Port-6)

LED	Color	Function	
1000 LNK/ACT	Green	**Lights**:	To indicate that the port is operating at 1000Mbps
		Blinks:	To indicate that the switch is actively sending or receiving data over that port.

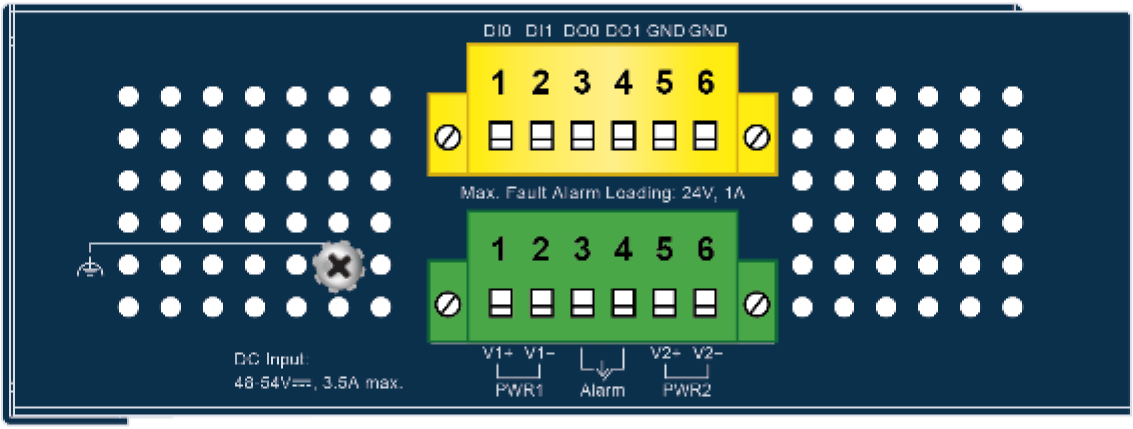
2.1.2 Top View

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

IAP-3600BE Top View



IAP-3600BE-4PF Top View

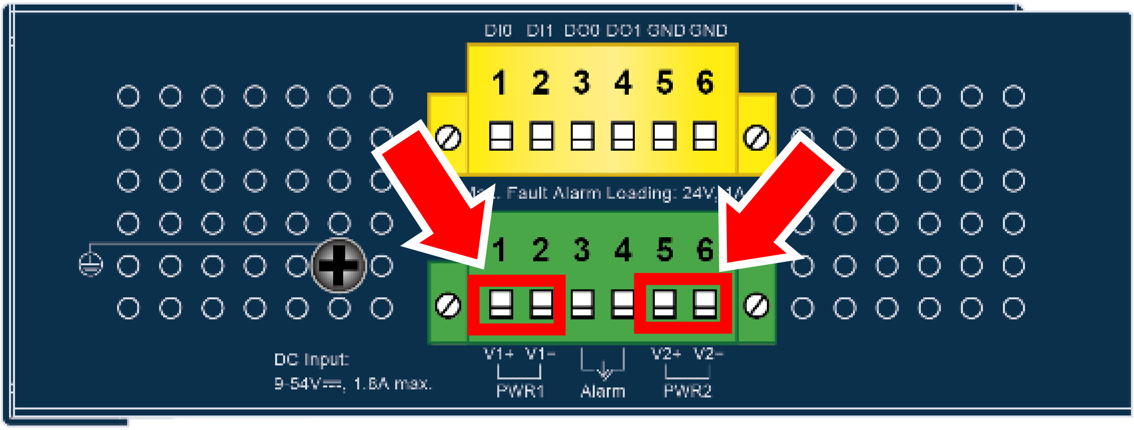


2.1.3 Wiring the Power Inputs

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

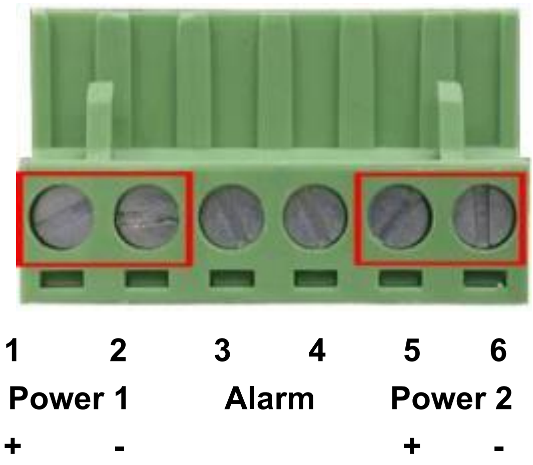
When performing any of the procedures like inserting the wires or tightening the wire-clamp screws, make sure the power is OFF to prevent from getting an electric shock.

1. Industrial 802.11be Wireless AP Input Voltage: (IAP-3600BE: 9-54V DC, IAP-3600BE-4PF: 48-54V DC)
2. Insert positive/negative DC power wires into Contacts 1 and 2 for Power 1, or Contacts 5 and 6 for Power 2.



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

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



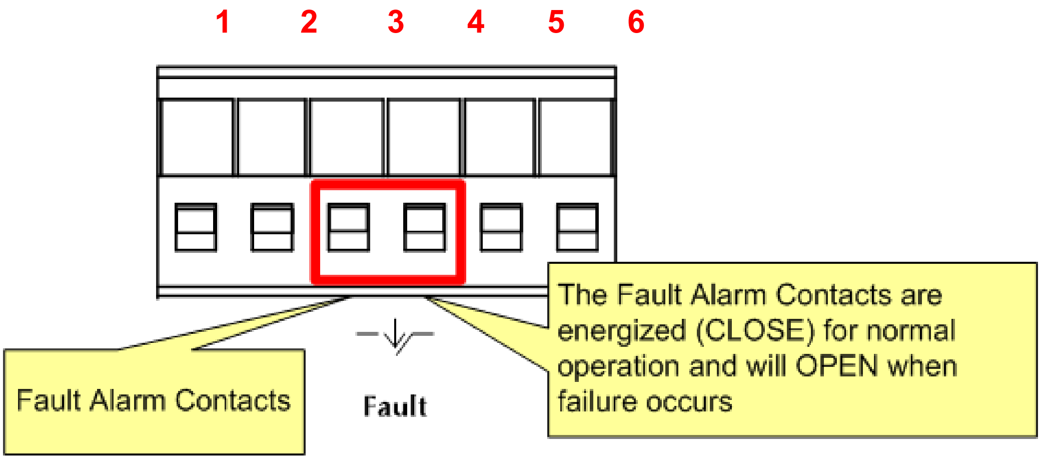
Note

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 802.11be 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.


1
2
3
4
5
6
Fault Alarm Contacts
Fault
The Fault Alarm Contacts are energized (CLOSE) for normal operation and will OPEN when failure occurs

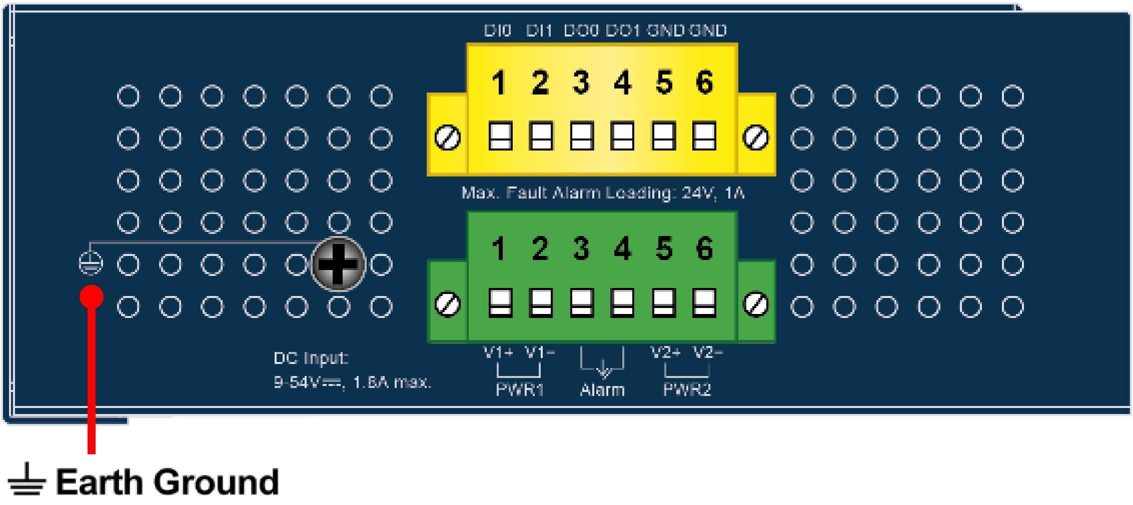
Insert the wires into the fault alarm contacts

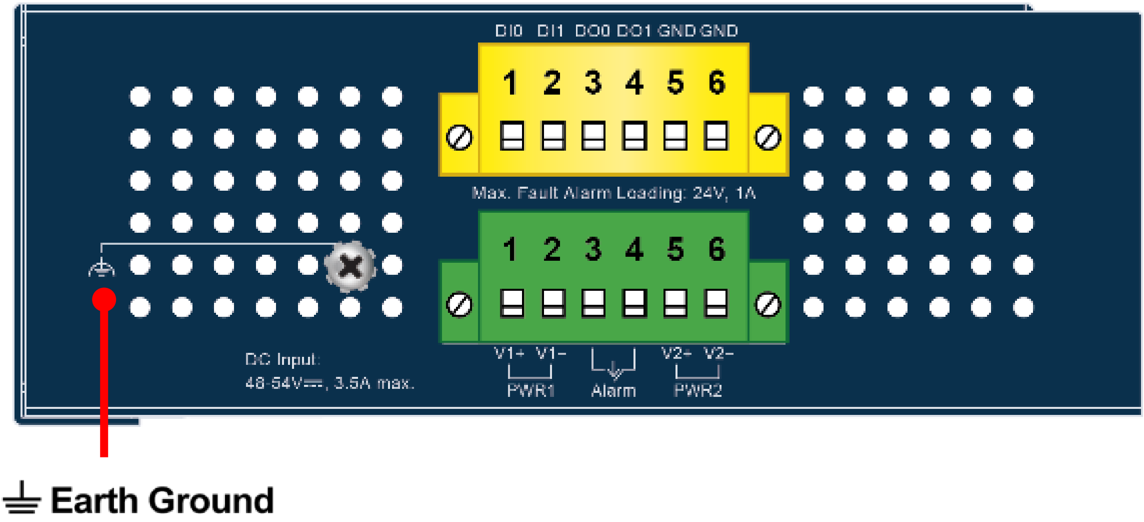
Note

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.



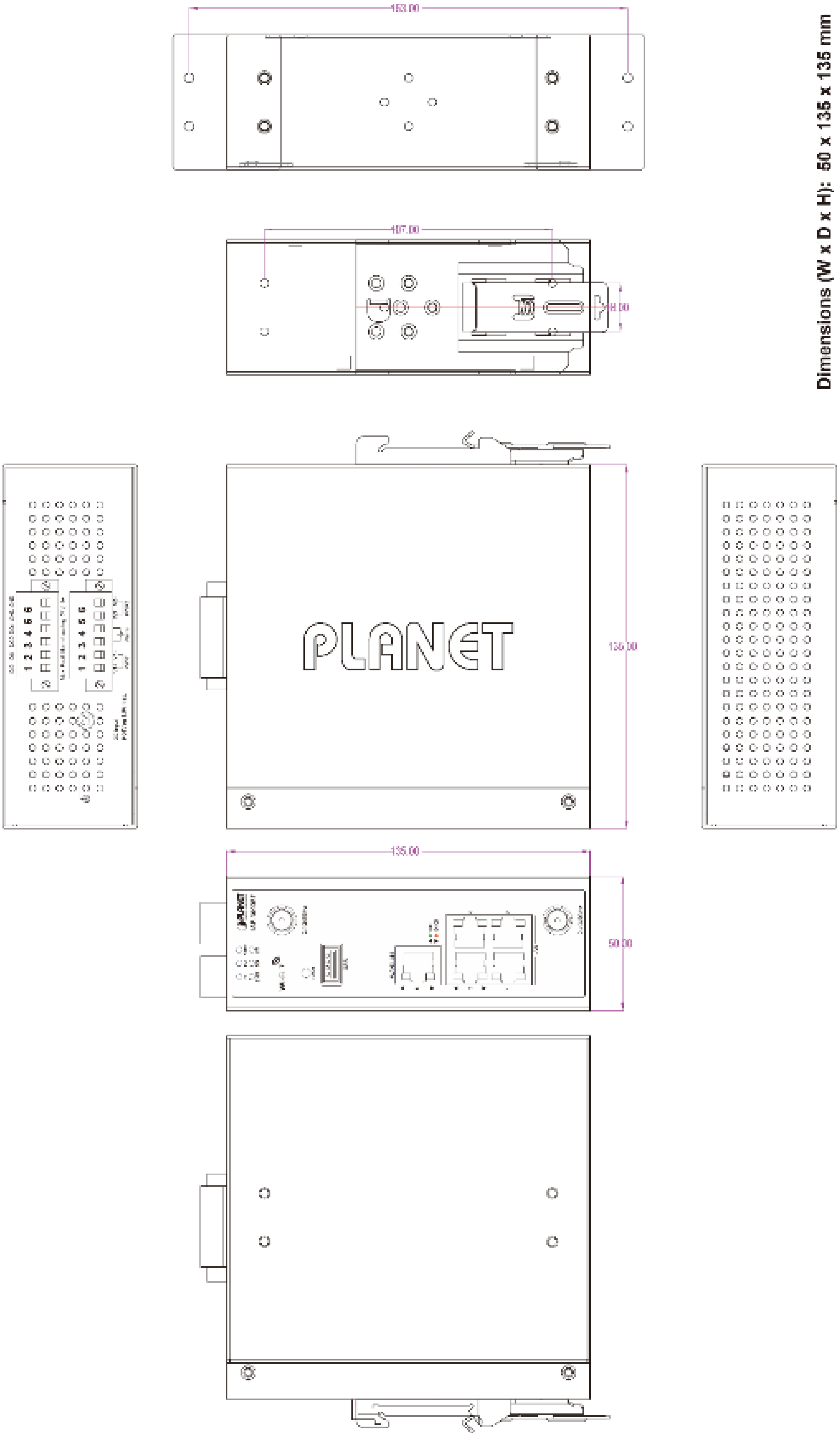


Note

EMD (Lightning) DAMAGE IS NOT COVERED UNDER WARRANTY.

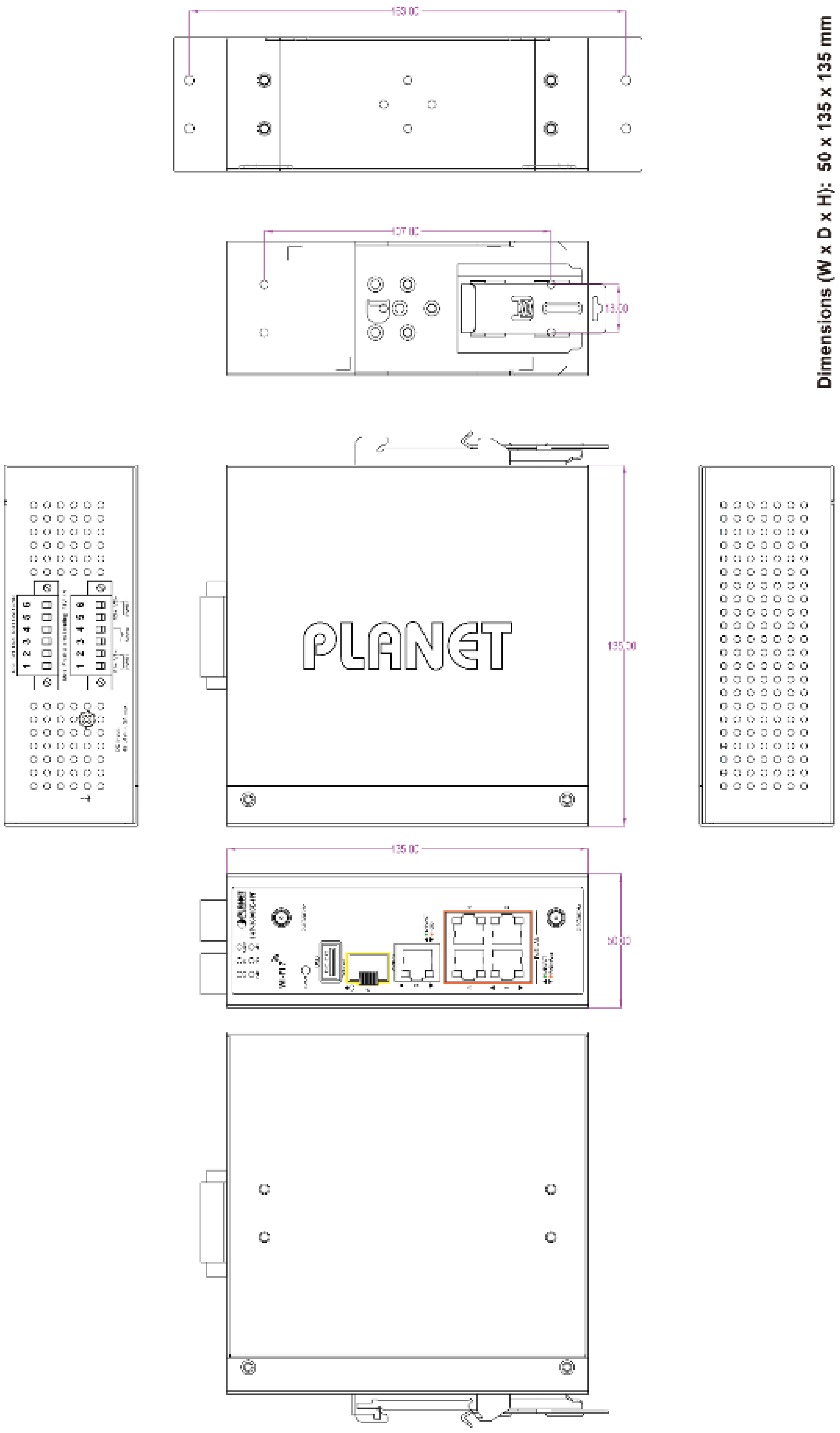
2.1.6 Dimensions

IAP-3600BE Dimensions



Dimensions (W x D x H): 50 x 135 x 135 mm

IAP-3600BE-4PF Dimensions



Dimensions (W x D x H): 50 x 135 x 135 mm

2.2 Hardware Installation

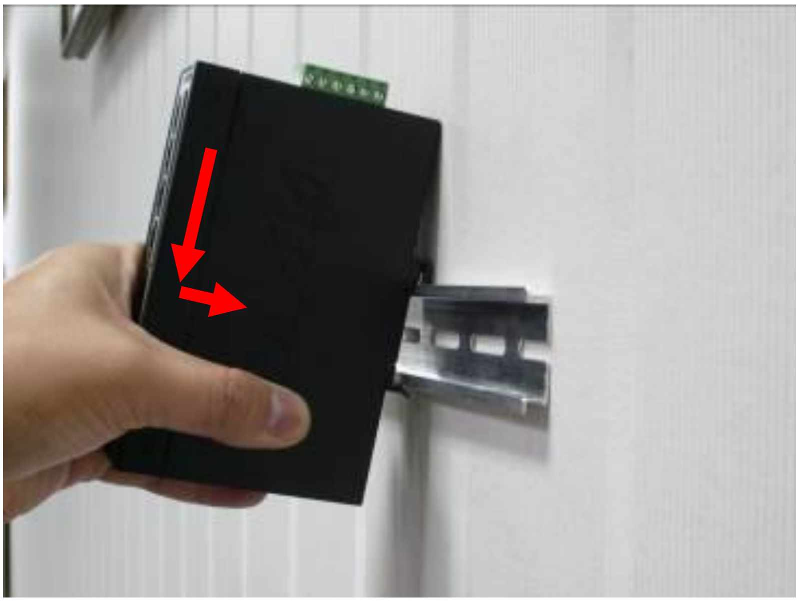
This section describes how to install the Industrial 802.11be Wireless AP. There are three methods to install the Industrial 802.11be Wireless AP -- DIN-rail mounting, wall mounting and side wall mounting. Basic knowledge of networking is assumed.

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.)

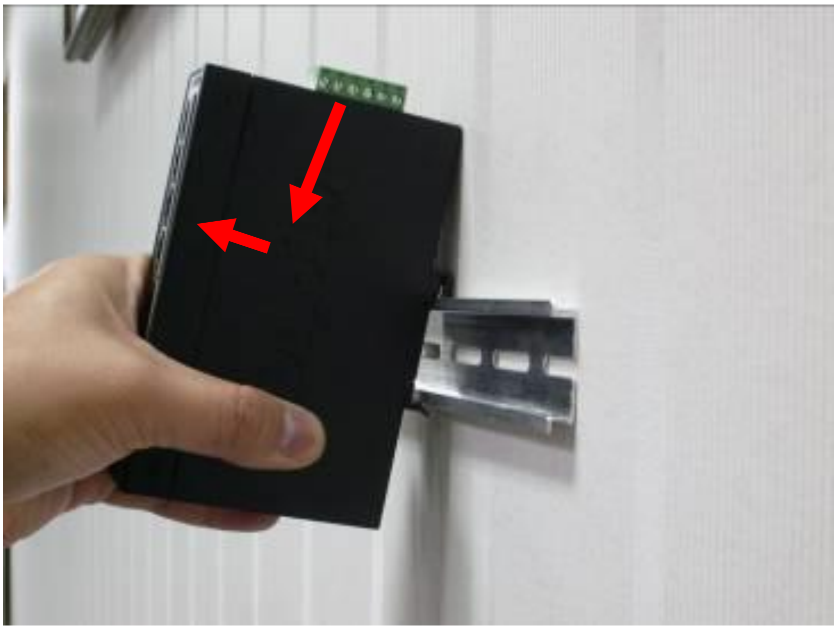
2.2.1 DIN-rail Mounting

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.

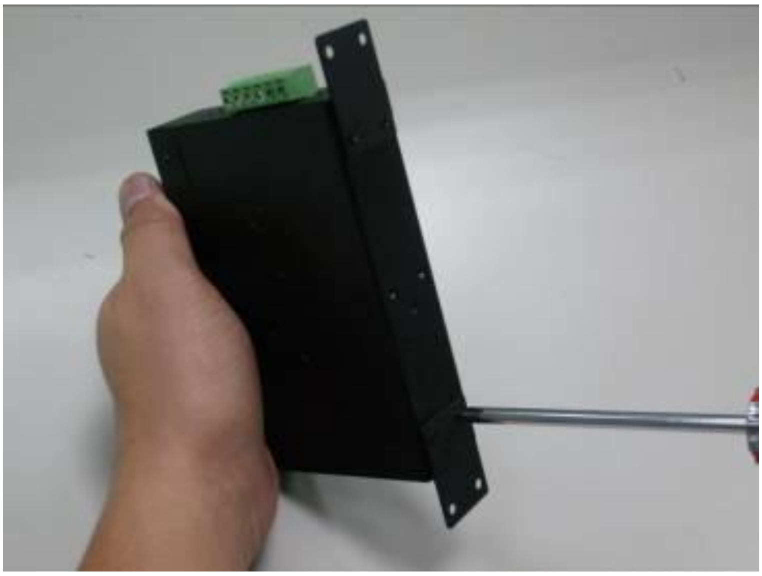


2.2.2 Wall Mount Plate Mounting

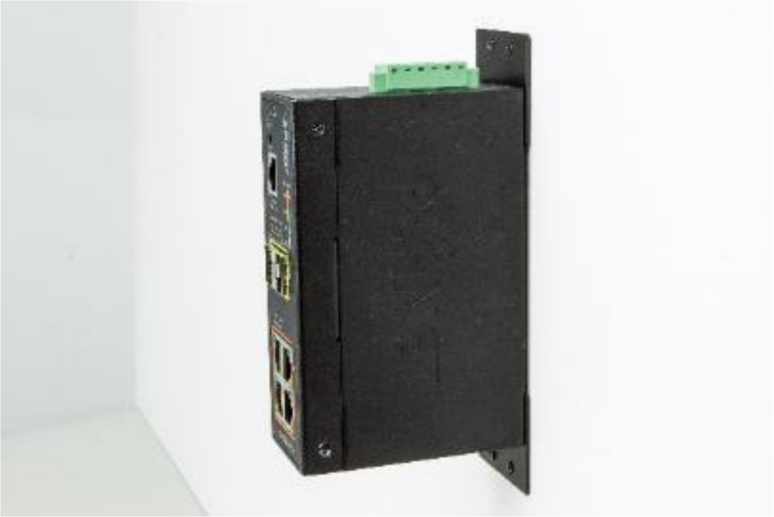
To install the Industrial 802.11be Wireless AP on the wall, please follow the instructions described below.

Step 1: Remove the DIN-rail from the Industrial 802.11be 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 802.11be Wireless AP.



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



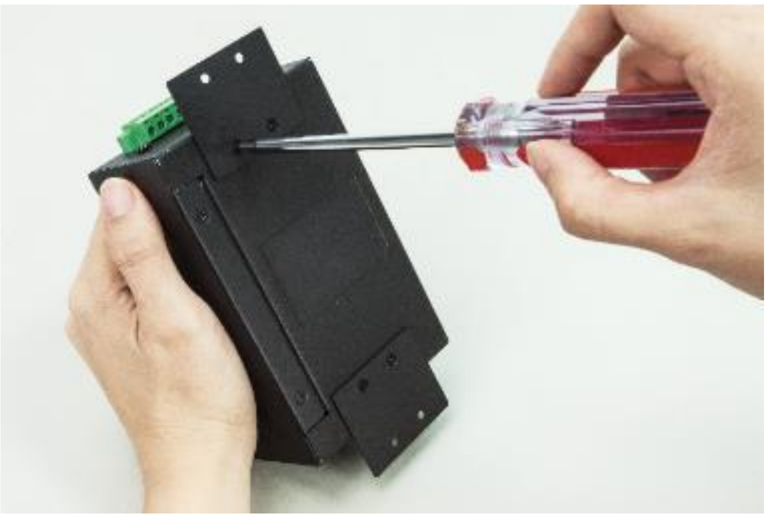
Step 4: To remove the wall mount plate, reverse the steps above.

2.2.3 Side Wall Mount Plate Mounting

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

Step 1: Remove the DIN-rail from the Industrial 802.11be 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 802.11be Wireless AP.



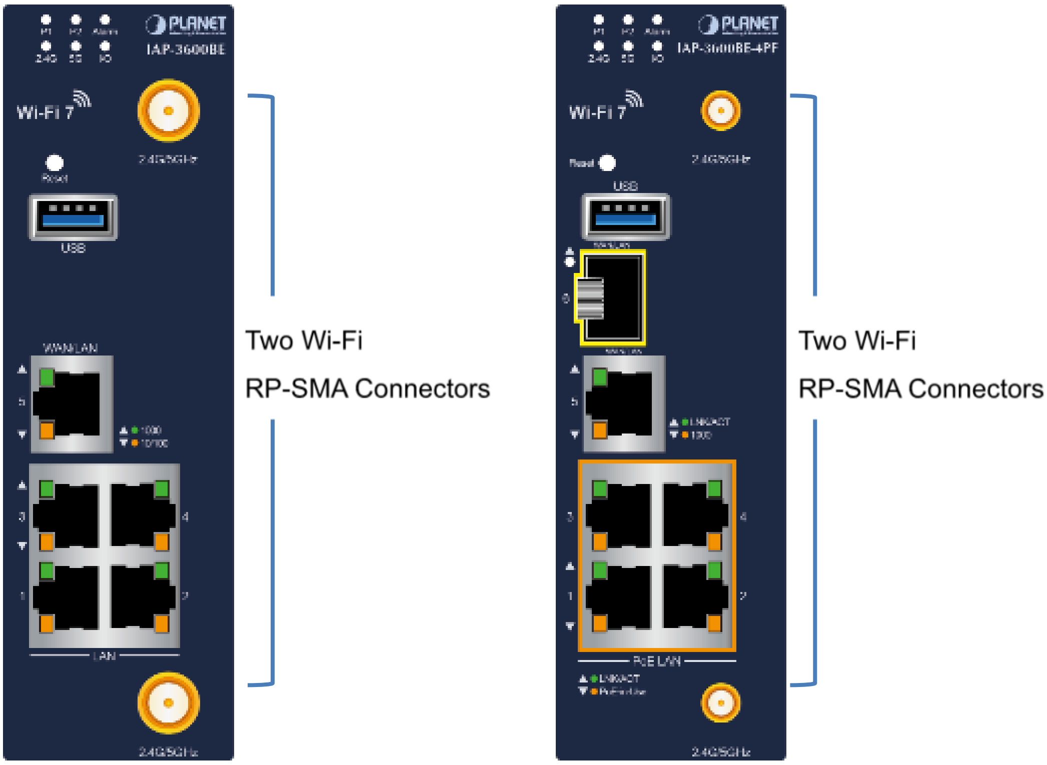
Step 3: Use the hook holes at the corners of the wall mount plate to hang the Industrial 802.11be Wireless AP on the wall.

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 802.11be Wireless AP.

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



Two Wi-Fi RP-SMA Connectors

Two Wi-Fi RP-SMA Connectors

Figure 2-2: Industrial 802.11be 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 7/8/10/11, macOS 10.12 or later, Linux Kernel 2.6.18 or later, or other modern operating system 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.

Note

It is recommended to use Google Chrome, Microsoft Edge or Mozilla Firefox to access the Industrial 802.11be Wireless AP. If the Web interface of the Industrial 802.11be 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 802.11be 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 802.11be 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.

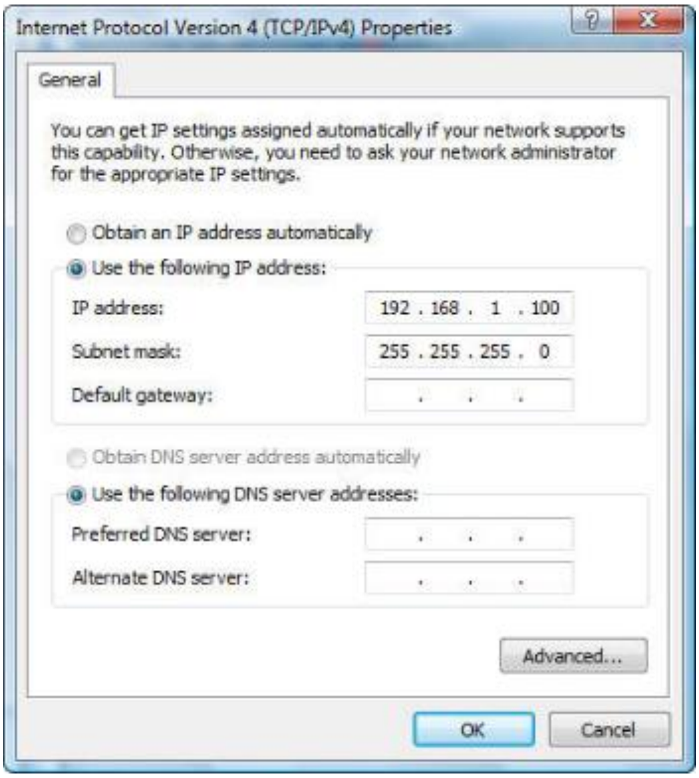
In the following sections, we'll introduce how to install and configure the TCP/IP correctly in **Windows 10**. And the procedures in other operating systems are similar. First, make sure your Ethernet Adapter is working, and refer to the Ethernet adapter manual if needed.

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 802.11be 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 802.11be Wireless AP is 192.168.1.253, you may choose from 192.168.1.1 to 192.168.1.252.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 100

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

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.

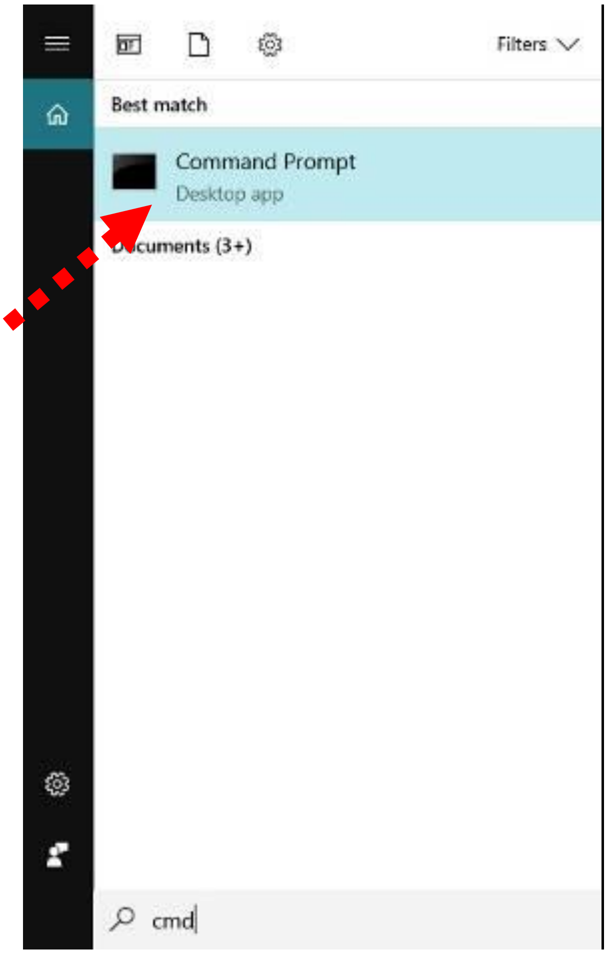
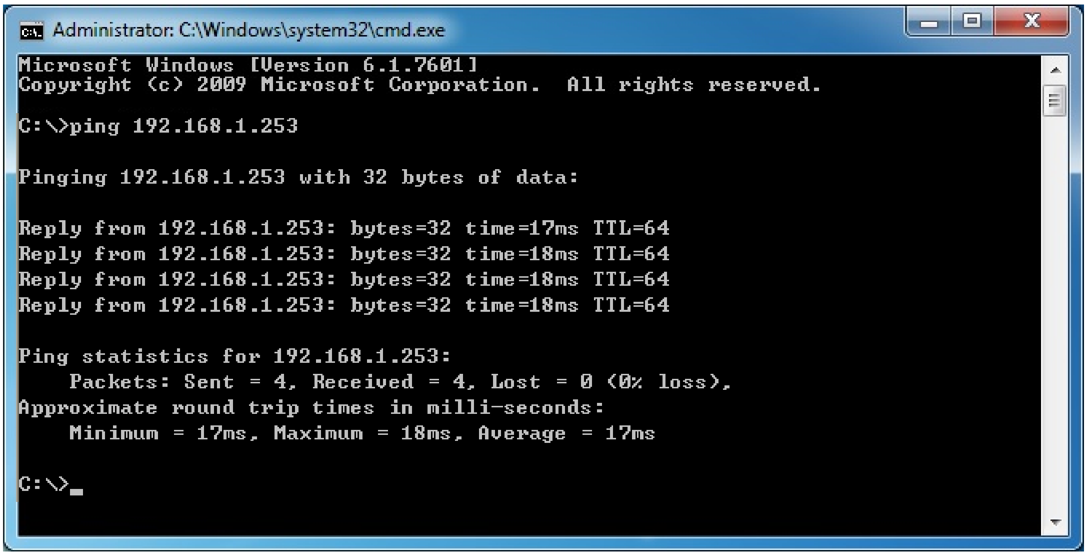


Figure 3-2: Windows Start Menu

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

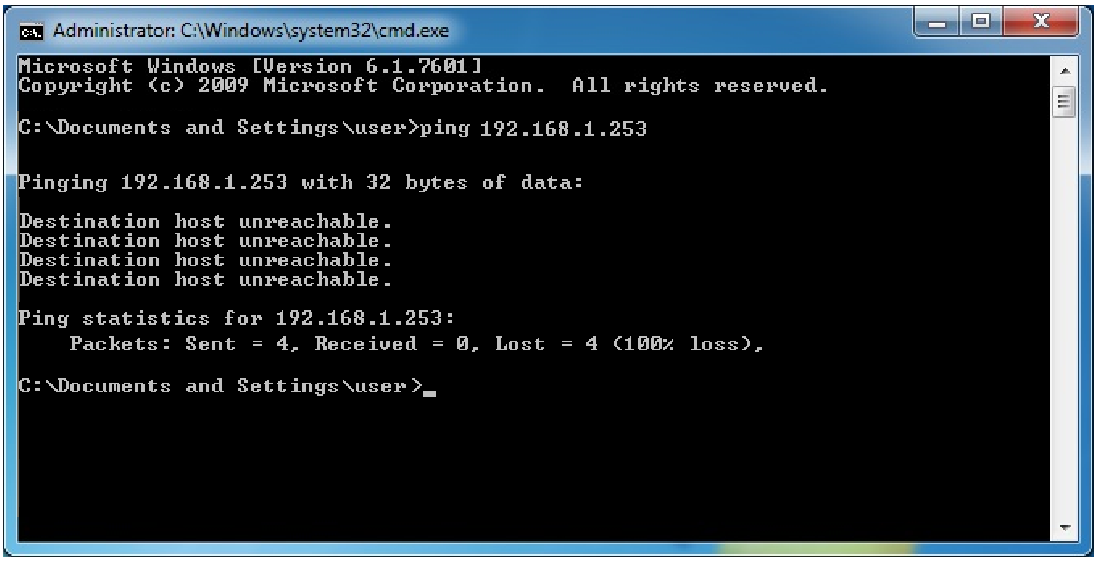
- If the result displayed is similar to **Figure 3-3**, it means the connection between your PC and the AP has been established well.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Reply from 192.168.1.253: bytes=32 time=17ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64
Reply from 192.168.1.253: bytes=32 time=18ms TTL=64

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 17ms, Maximum = 18ms, Average = 17ms

C:\>_
```

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.



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Documents and Settings\user>ping 192.168.1.253

Pinging 192.168.1.253 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.1.253:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\user>
```

Figure 3-4: Failed Result of Ping Command

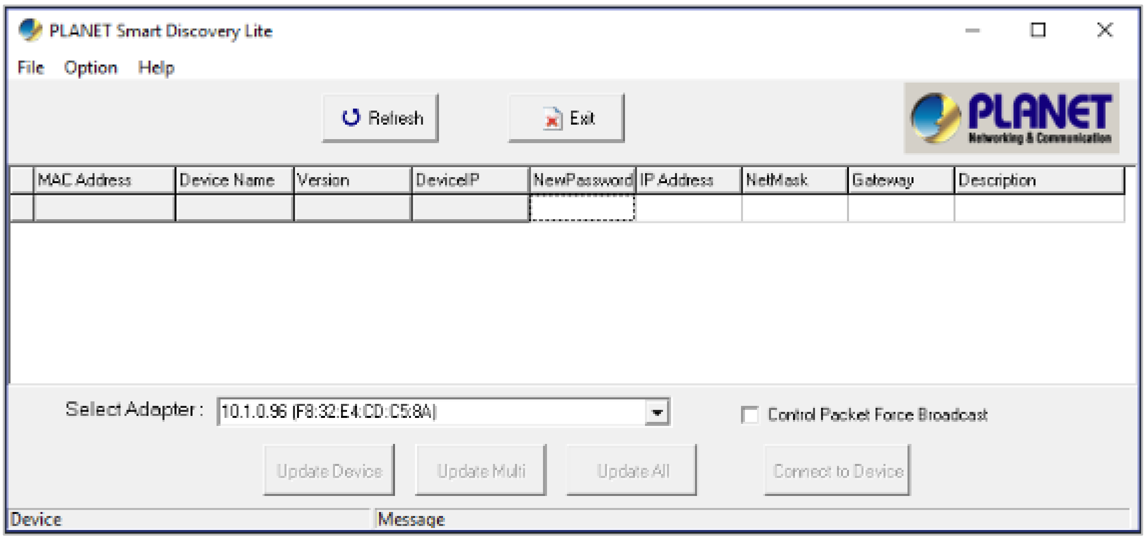
If the address is 0.0.0.0, check your adapter installation, security settings, and the settings on your AP. Some firewall software programs may block a DHCP request on newly installed adapters.

3.3 PLANET Smart Discovery Utility

For easily listing the Industrial 802.11be 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.


PLANET Smart Discovery Lite
File
Option
Help
Refresh
Exit
PLANET Networking & Communication
Control Packet Force Broadcast
Update Device
Update Multi
Update All
Connect to Device

	MAC Address	Device Name	Version	DeviceIP	NewPassword	IP Address	NetMask	Gateway	Description

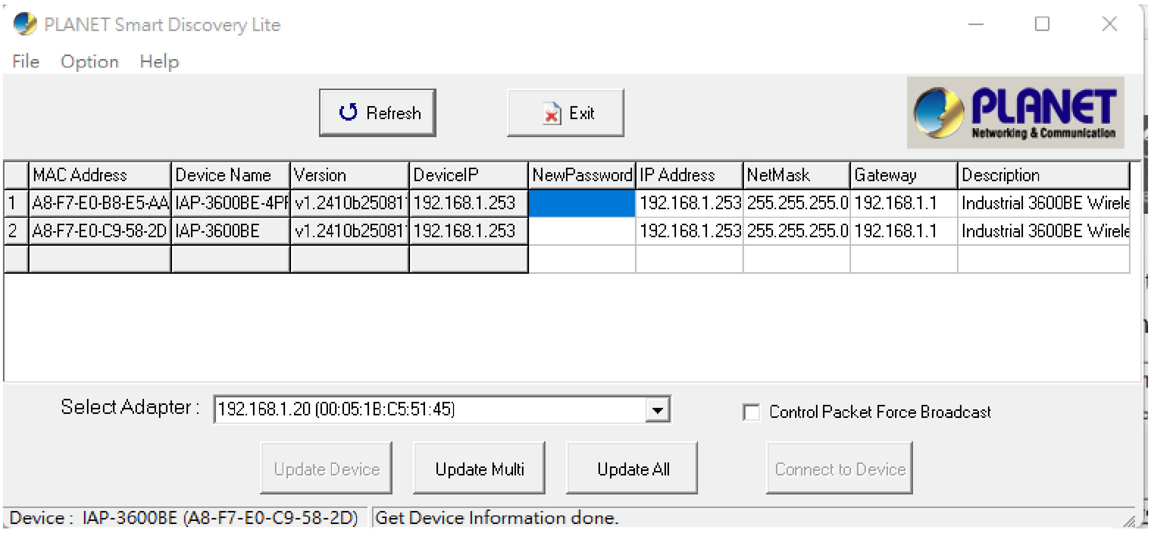
Select Adapter : 10.1.0.96 (F8:32:E4:CD:C5:8A)

Device | Message

Figure 3-5: PLANET Smart Discovery Utility Screen

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:


PLANET Smart Discovery Lite
File
Option
Help
Refresh
Exit
PLANET Networking & Communication
Control Packet Force Broadcast
Update Device
Update Multi
Update All
Connect to Device

	MAC Address	Device Name	Version	DeviceIP	NewPassword	IP Address	NetMask	Gateway	Description
1	A8-F7-E0-B8-E5-AA	IAP-3600BE-4PF	v1.2410b250811	192.168.1.253		192.168.1.253	255.255.255.0	192.168.1.1	Industrial 3600BE Wirele
2	A8-F7-E0-C9-58-2D	IAP-3600BE	v1.2410b250811	192.168.1.253		192.168.1.253	255.255.255.0	192.168.1.1	Industrial 3600BE Wirele

Select Adapter : 192.168.1.20 (00:05:1B:C5:51:45)

Device : IAP-3600BE (A8-F7-E0-C9-58-2D) | Get Device Information done.

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 802.11be Wireless AP with the web browser.

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

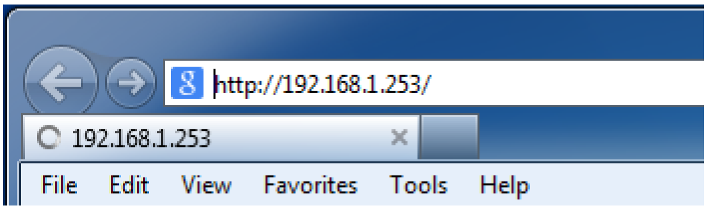


Figure 3-7: Login by Default IP Address

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

Note

The following web screen is based on the IAP-3600BE; the display of the IAP-3600BE-4PF is the same as that of the IAP-3600BE.

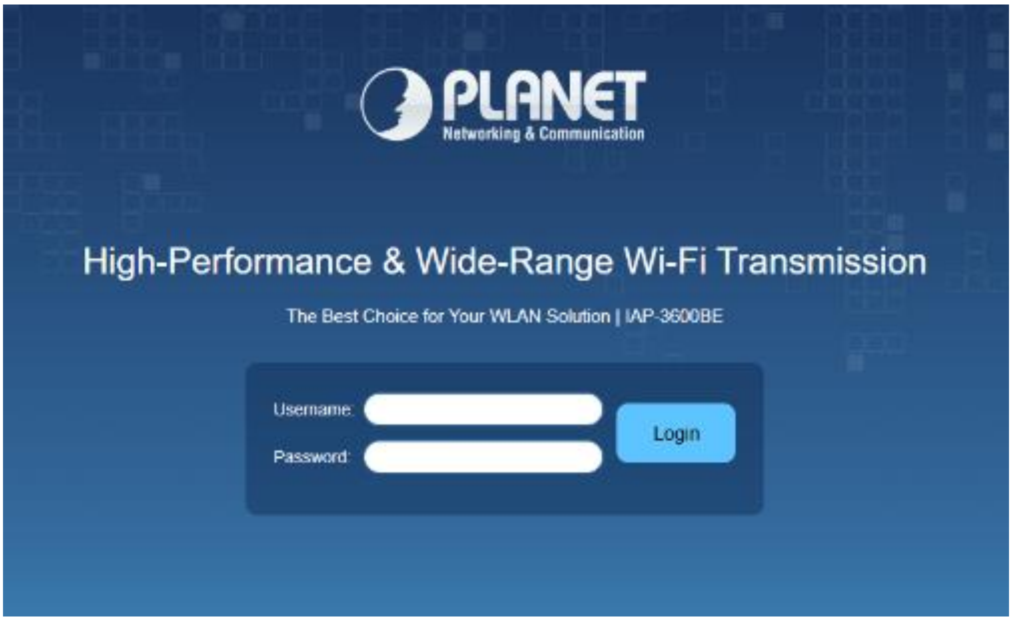
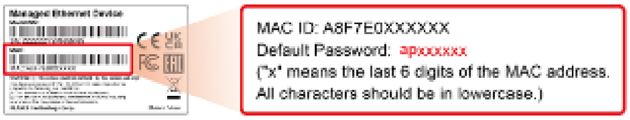

PLANET
Networking & Communication
High-Performance & Wide-Range Wi-Fi Transmission
The Best Choice for Your WLAN Solution | IAP-3600BE
Username:
Password:
Login

Figure 3-8: Login Window

Default Username: **admin**
Default Password: **ap + the last 6 characters of the MAC ID in lowercase**
Default 2.4GHz SSID: **PLANET_2.4G**
Default 5GHz SSID: **PLANET_5G**

Find the MAC ID on your device label. The default password is "ap" followed by the last six lowercase characters of the MAC ID.



MAC ID: A8F7E0XXXXXX

Default Password: apxxxxxx

("x" means the last 6 digits of the MAC address.

All characters should be in lowercase.)

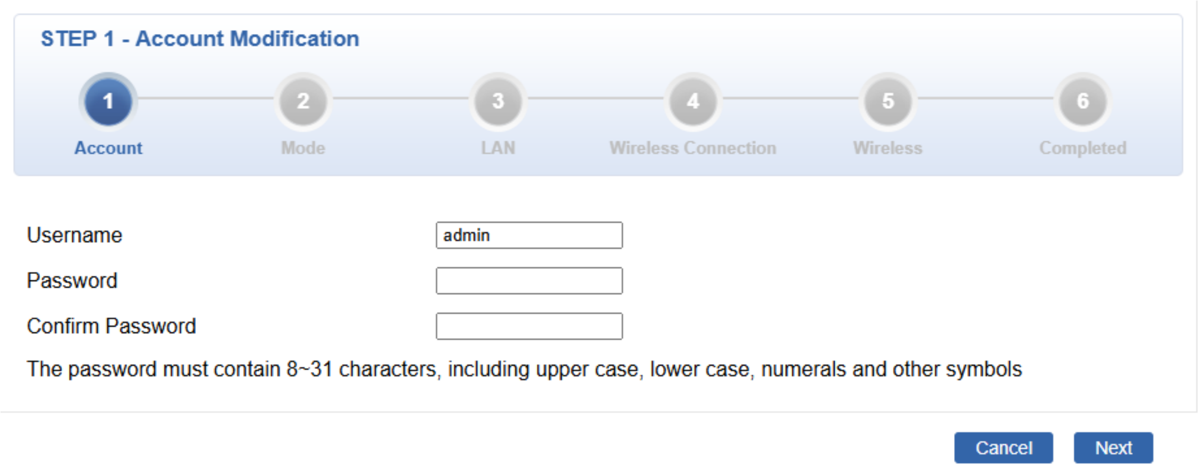
Figure 3-9: MAC ID

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.

Please follow the wizard to do the first-time account modification.

The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols


STEP 1 - Account Modification

Username	admin
Password	
Confirm Password	

The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols

Note

Administrators are strongly suggested to change the default admin and password to ensure system security.

Chapter 4. Web-based Management

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

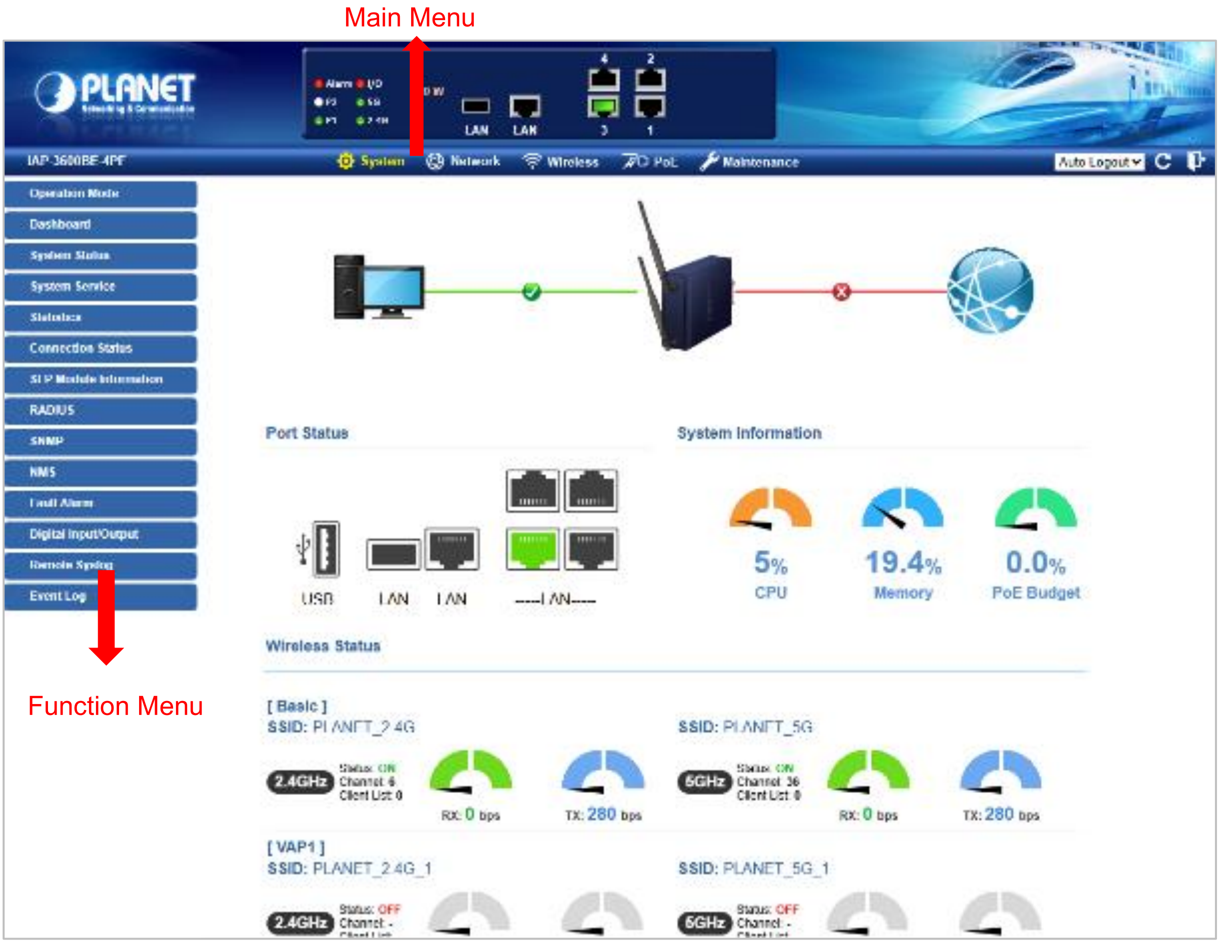


Figure 4-1: Main Web Page

- **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.

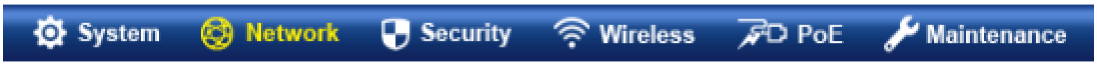


Figure 4-2: Function Menu

Object	Description
System	Provides system information of the Industrial 802.11be Wireless AP.
Network	Provides WAN, LAN and network configuration of the Industrial 802.11be Wireless AP.
Wireless	Provides wireless configuration of the Industrial 802.11be Wireless AP.
PoE	Provides PoE Management configuration of industrial wall-mount Gigabit router. (For IAP-3600BE-4PF only)
Maintenance	Provides firmware upgrade and setting file restore/backup configuration of the Industrial 802.11be 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 802.11be Wireless AP.

4.1 System

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

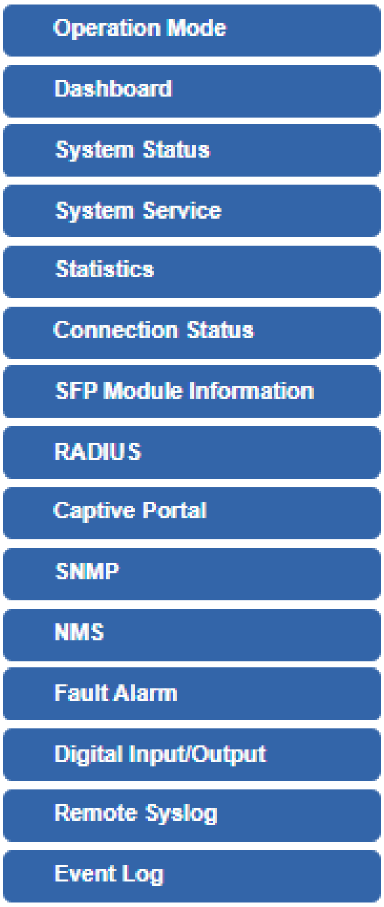


Figure 4-4: System Menu

Object	Description
Operation Mode	The Wizard will guide the user to configuring the Industrial 802.11be 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.
SFP Module Information	Display the physical or operational status of an SFP module via the SFP Module Information page
RADIUS	Enable/Disable RADIUS on Industrial 802.11be Wireless APs.
Captive Portal	Enable/Disable Captive Portal on Industrial 802.11be Wireless APs.
SNMP	Display SNMP system information.
NMS	Enable/Disable NMS on Industrial 802.11be 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 802.11be Wireless APs.
Event Log	Display Event Log information.

4.1.1 Wizard

The Wizard will guide the user to configuring the Gateway easily and quickly. There are different procedures in different operation modes. According to the operation mode you switch to, please follow the instructions below to configure the Gateway via Setup Wizard as shown below:

4.1.2 Operation Mode

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

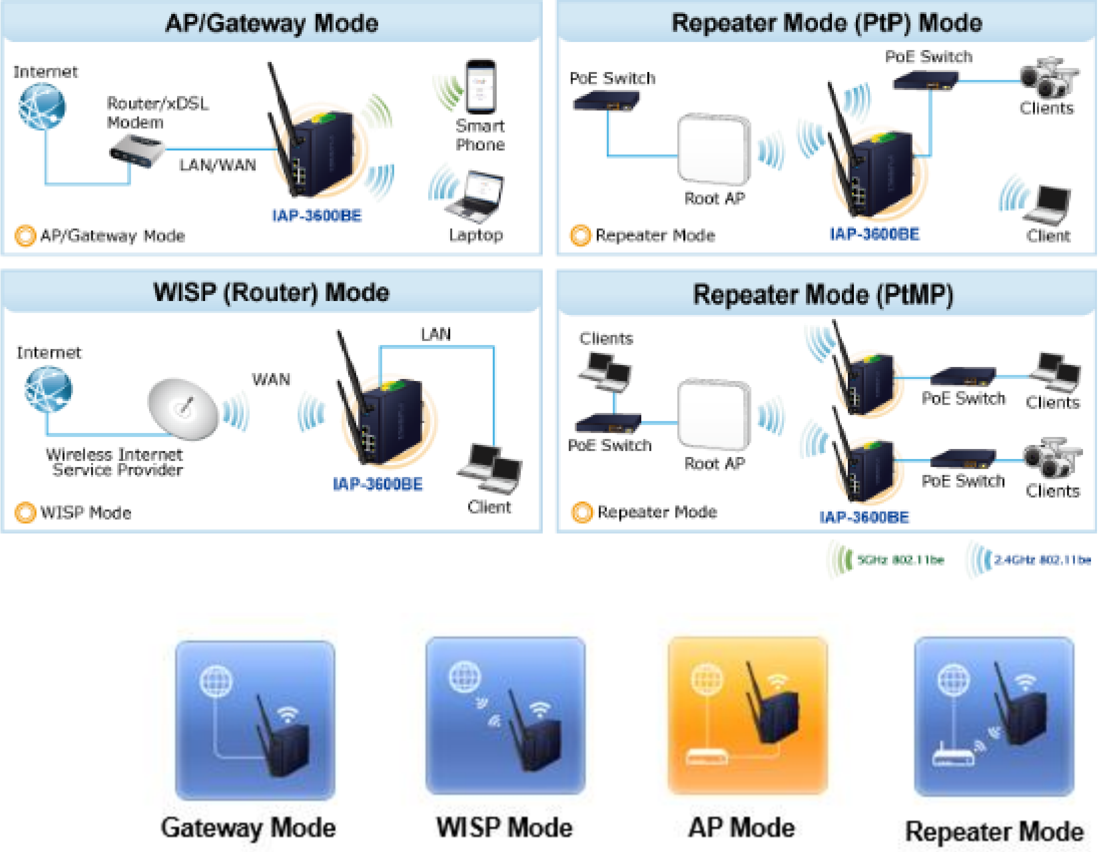
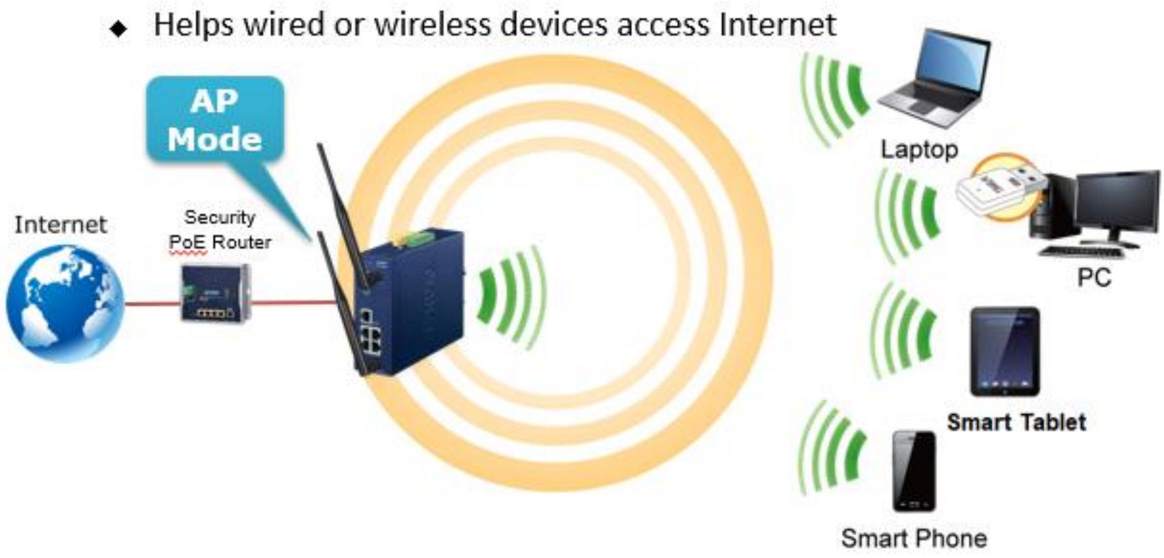


Figure 4-5: Operation Mode

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

4.1.3 AP Mode(Access Point Mode)

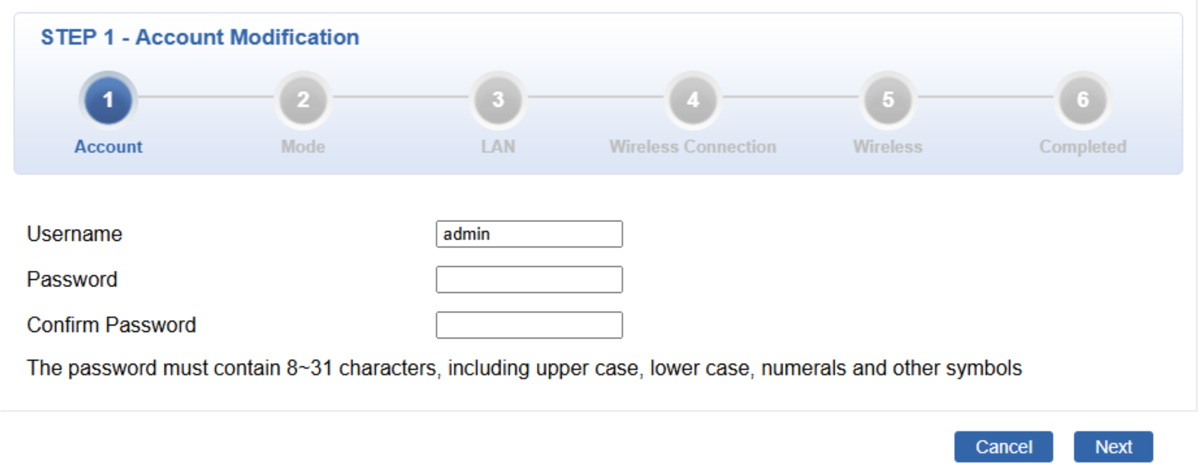
Click “**Wizard**” → “**AP Mode**”(Default) and the following page will be displayed. This section allows you to configure the AP mode.



Step 1: Account Modification

Please follow the wizard to do the first-time account modification.

The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols


STEP 1 - Account Modification

Username	admin
Password	
Confirm Password	

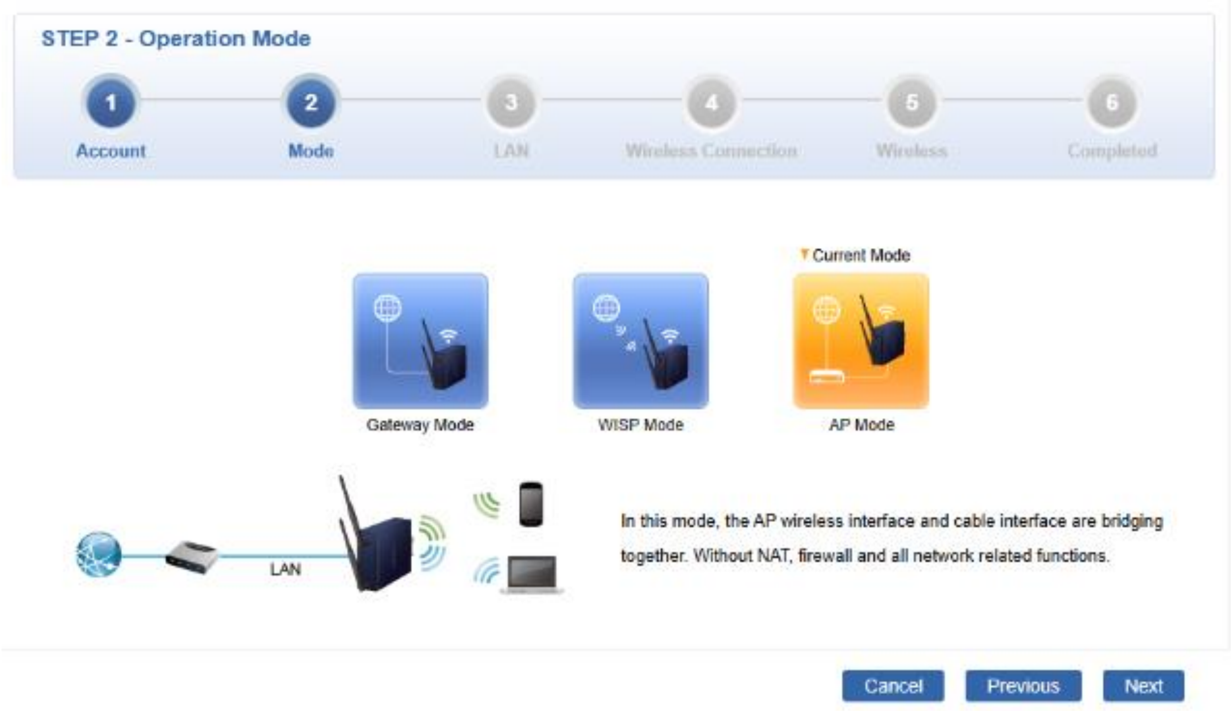
The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols

Note

Administrators are strongly suggested to change the default admin and password to ensure system security.

Step 2: Operation Mode

Select the AP Mode.

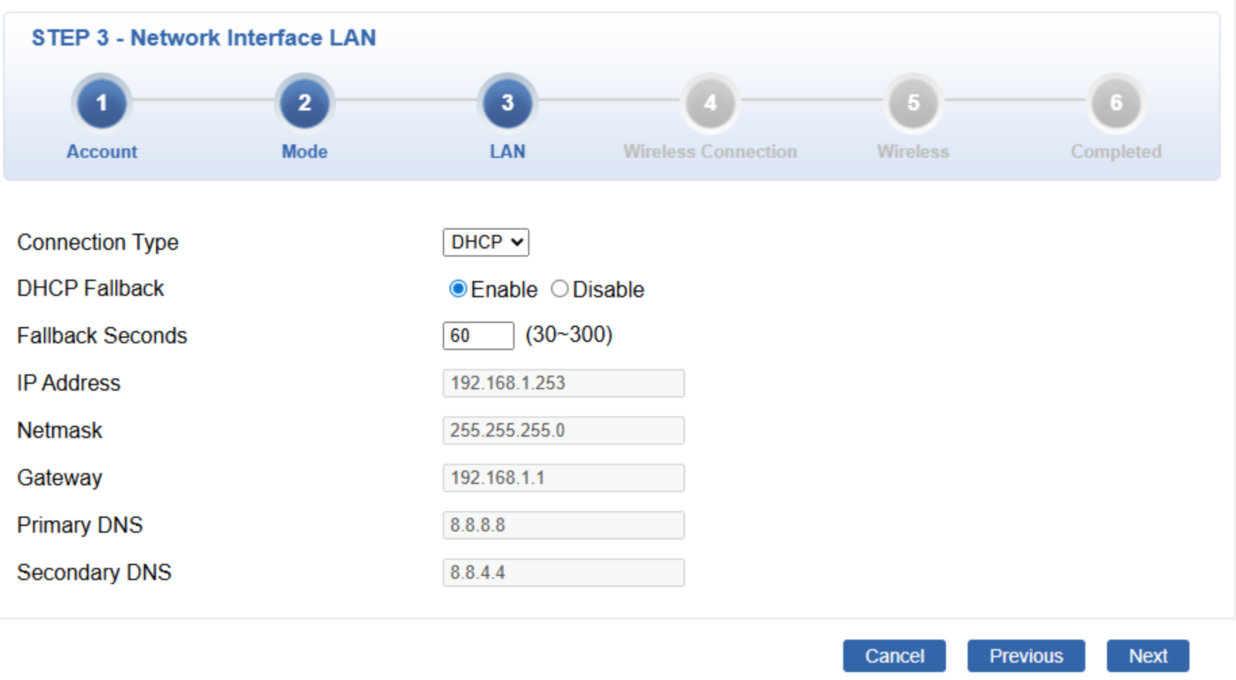


STEP 2 - Operation Mode

In this mode, the AP wireless interface and cable interface are bridging together. Without NAT, firewall and all network related functions.

Step 3: LAN Interface

Set up the IP Address and Subnet Mask for the LAN interface as shown below.



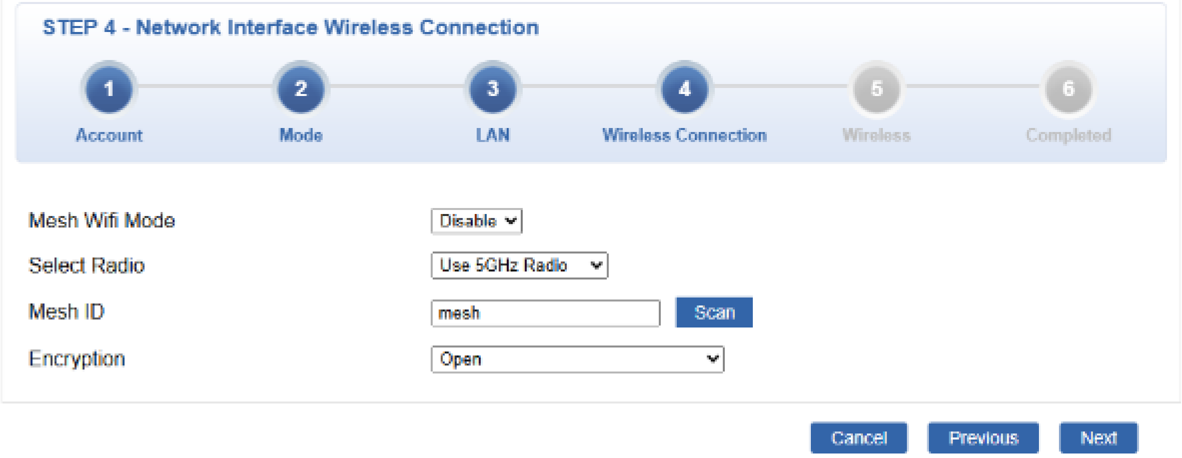
STEP 3 - Network Interface LAN

Connection Type	DHCP
DHCP Fallback	● Enable ○ Disable
Fallback Seconds	60 (30~300)
IP Address	192.168.1.253
Netmask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4

Object	Description
IP Address	Enter the IP address of your VPN Security Gateway The default is 192.168.1.1.
Netmask	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 VPN Security Gateway
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the VPN Security Gateway 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.

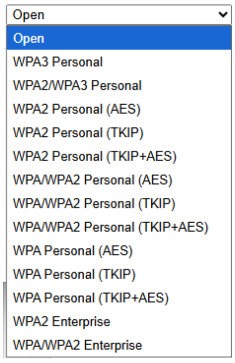
Step 4: Wireless Connection

Set up the Wireless Connection as shown below.


STEP 4 - Network Interface Wireless Connection

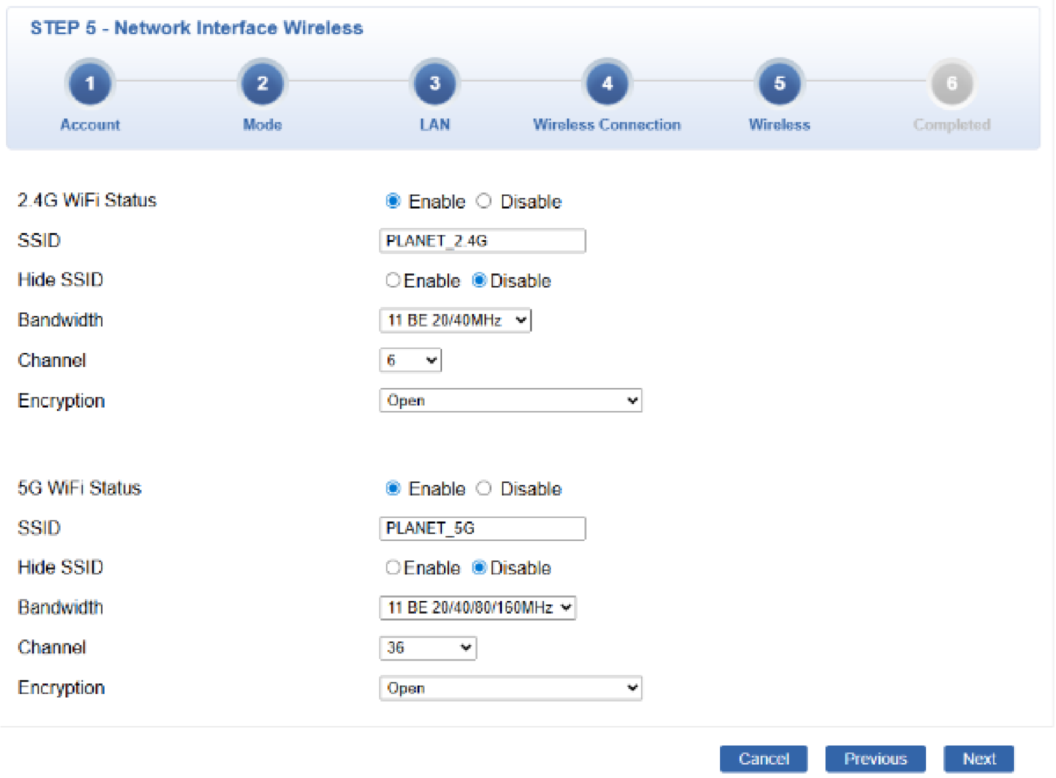
Mesh Wifi Mode: Disable
Select Radio: Use 5GHz Radio
Mesh ID: mesh
Encryption: Open

Figure: Setup Wizard –Mesh set up

Object	Description
Mesh Wi-Fi Mode	Select the Mesh role for Master or Node to enable Mesh function. The default configuration is disabled.
Select Radio	Select 2.4GHz or 5GHz for MESH ID radio.
Mesh ID	Enter the Mesh ID, just like SSID, or use the Scan button to discover Mesh ID from the Master/Node Mesh AP.
Encryption	Selector is for the encryption for the sake of security.  Open Open 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) WPA Personal (AES) WPA Personal (TKIP) WPA Personal (TKIP+AES) WPA2 Enterprise WPA/WPA2 Enterprise
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 5: Wireless

Set up the Network Interface Wireless as shown below.



STEP 5 - Network Interface Wireless

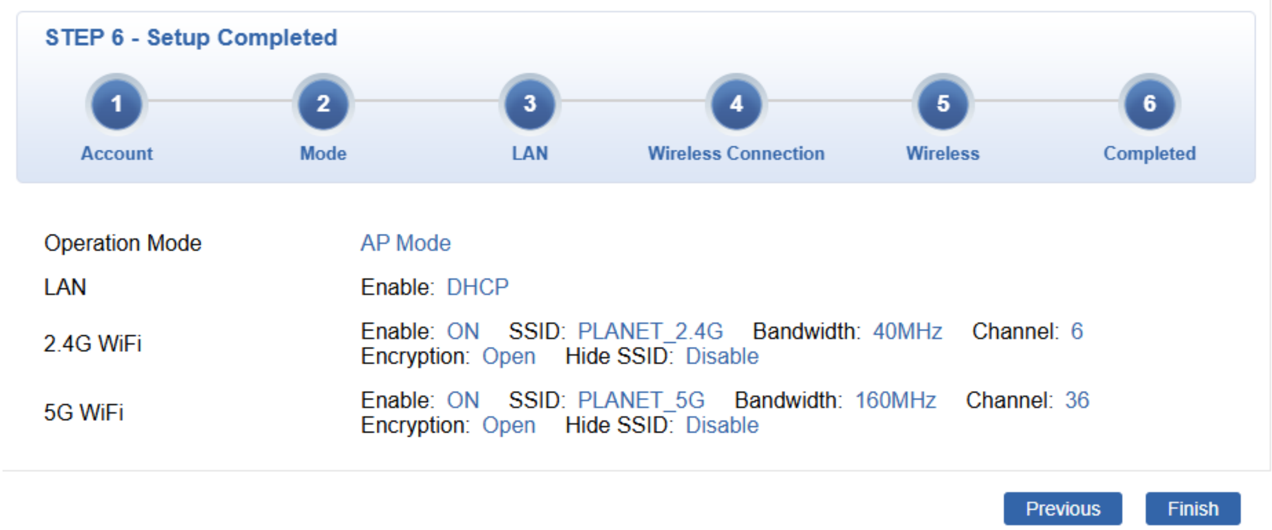
2.4G WiFi Status	● Enable ○ Disable
SSID	PLANET_2.4G
Hide SSID	○ Enable ● Disable
Bandwidth	11 BE 20/40MHz
Channel	6
Encryption	Open
5G WiFi Status	● Enable ○ Disable
SSID	PLANET_5G
Hide SSID	○ Enable ● Disable
Bandwidth	11 BE 20/40/80/160MHz
Channel	36
Encryption	Open

Object	Description
2.4G Wireless Status	Allows user to enable or disable 2.4G Wi-Fi
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
Bandwidth	Select the operating channel width, “**20MHz**” or “**40MHz**”
Channel	It shows the channel of the CPE. Default 2.4GHz is channel 6.
Encryption	Select the wireless encryption. The default is “**Open**”

Object	Description
5G Wireless Status	Allows user to enable or disable 5G Wi-Fi
SSID	It is the wireless network name. The default 5G SSID is “PLANET_5G”
Hide SSID	Allows user to enable or disable SSID
Bandwidth	Select the operating channel width, “**20MHz**” or “**40MHz**” or “**80MHz**” or “**160MHz**”
Channel	It shows the channel of the CPE. Default 5GHz is channel 36.
Encryption	Select the wireless encryption. The default is “**Open**”

Step 6: Completed

The page will show the completed settings shown below.



STEP 6 - Setup Completed

Operation Mode AP Mode

LAN Enable: DHCP

2.4G WiFi Enable: ON SSID: PLANET_2.4G Bandwidth: 40MHz Channel: 6 Encryption: Open Hide SSID: Disable

5G WiFi Enable: ON SSID: PLANET_5G Bandwidth: 160MHz Channel: 36 Encryption: Open Hide SSID: Disable

Figure: Setup Wizard – Setup Completed

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

4.1.4 Gateway Mode (Router)

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

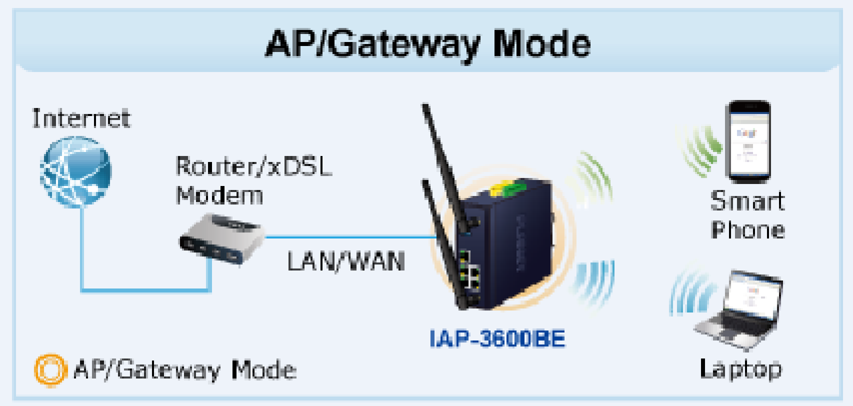
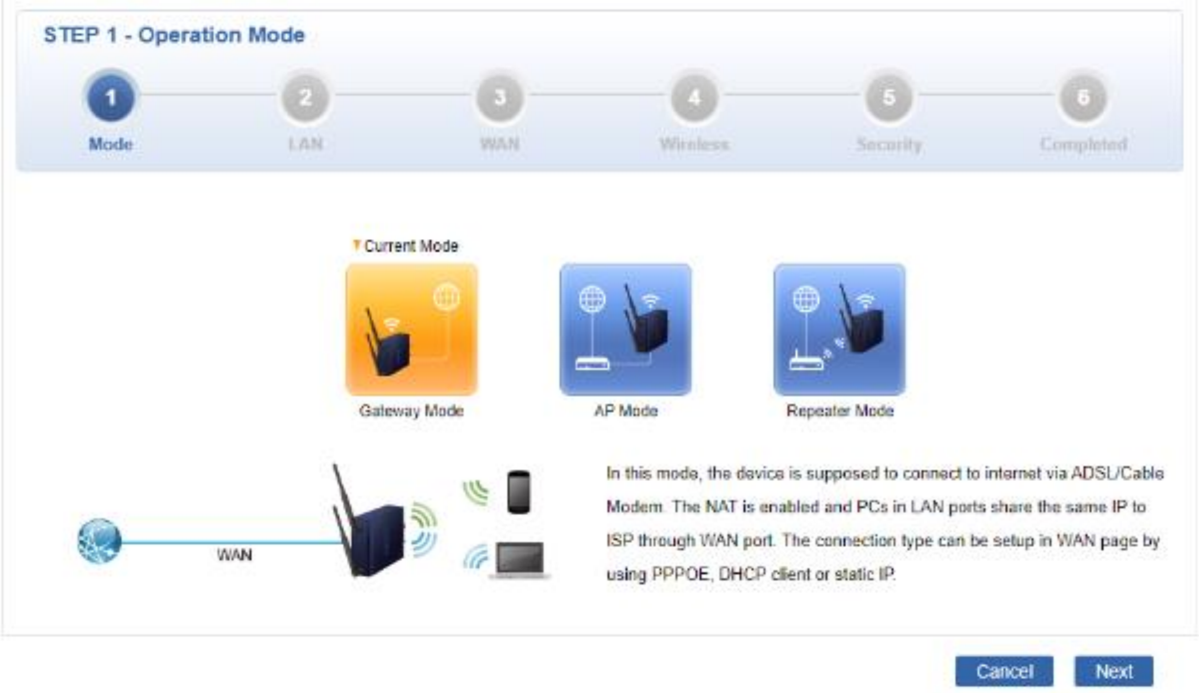


Figure 4-6: Setup Wizard

Step 1: Operation Mode

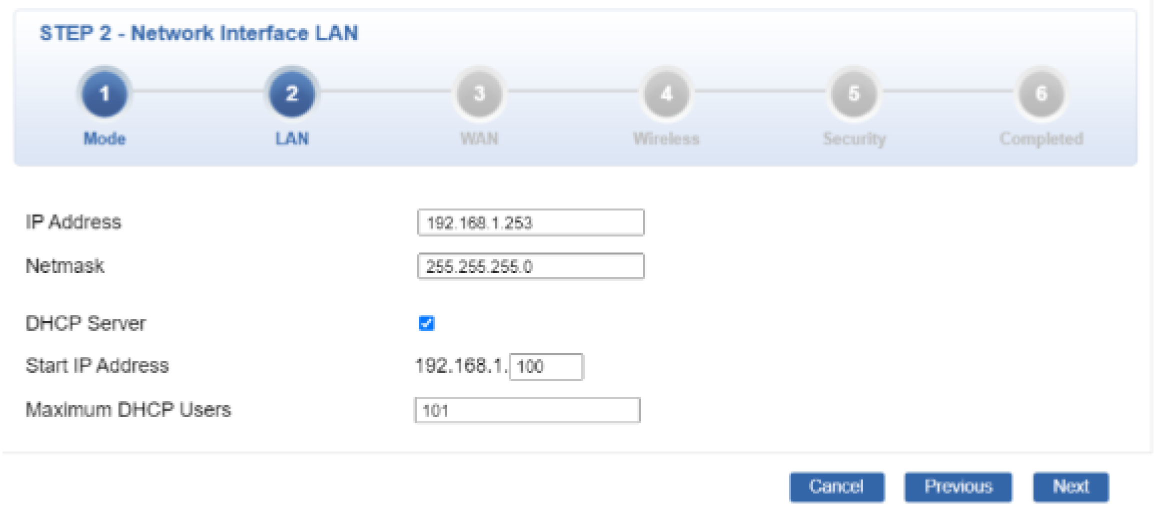
Select the Gateway Mode.



In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN ports share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using PPPOE, DHCP client or static IP.

Step 2: LAN Interface

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



IP Address 192.168.1.253

Netmask 255.255.255.0

DHCP Server ☑

Start IP Address 192.168.1. 100

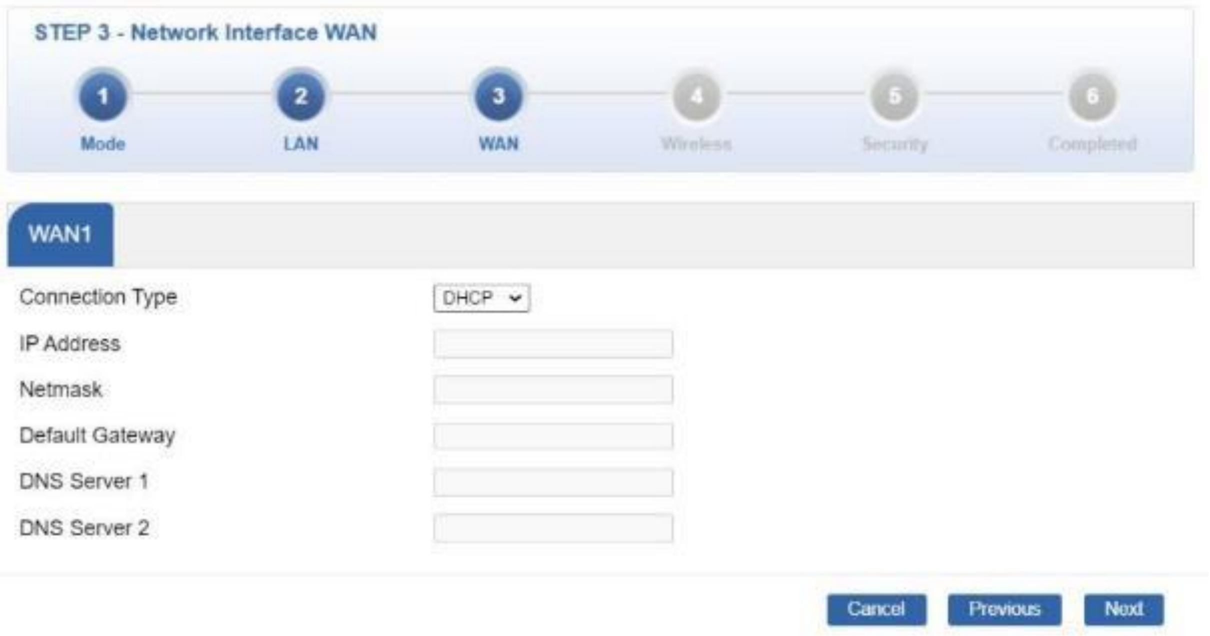
Maximum DHCP Users 101

Figure 4-7: Setup Wizard – LAN Configuration

Object	Description
IP Address	Enter the IP address of your Industrial 802.11be 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 802.11be Wireless AP.
Maximum DHCP Users	By default, the maximum DHCP users are 101, which means the Industrial 802.11be 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 802.11be Wireless AP supports two access modes on the WAN side shown in Figure 4-8.



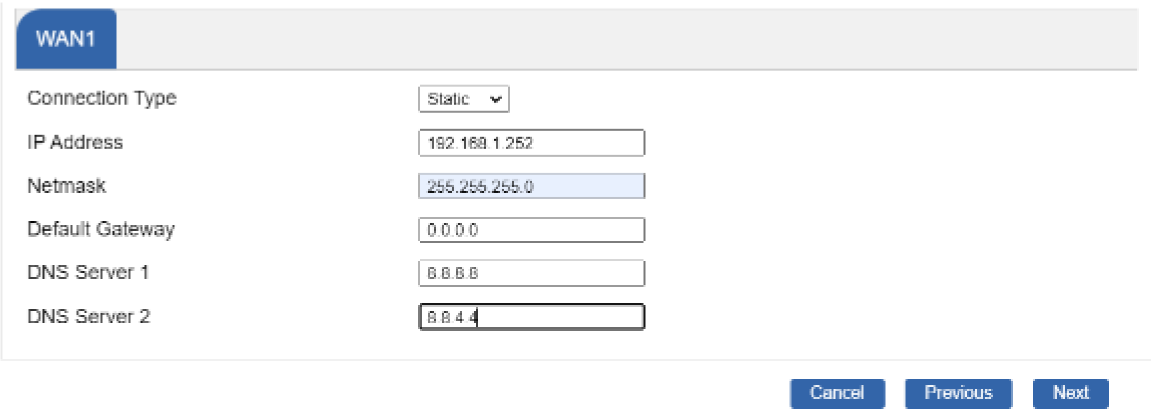
STEP 3 - Network Interface WAN

Connection Type	DHCP
IP Address	
Netmask	
Default Gateway	
DNS Server 1	
DNS Server 2	

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 802.11be Wireless AP will not accept the IP address if it is not in this format. The setup is shown in Figure 4-9.



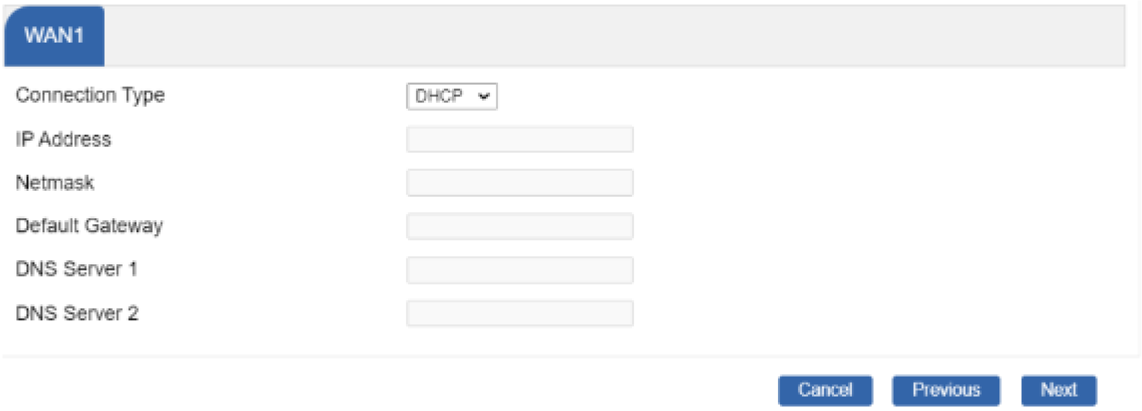
Connection Type	Static
IP Address	192.168.1.252
Netmask	255.255.255.0
Default Gateway	0.0.0.0
DNS Server 1	8.8.8.8
DNS Server 2	8.8.4.4

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.



WAN1

Connection Type: DHCP

IP Address

Netmask

Default Gateway

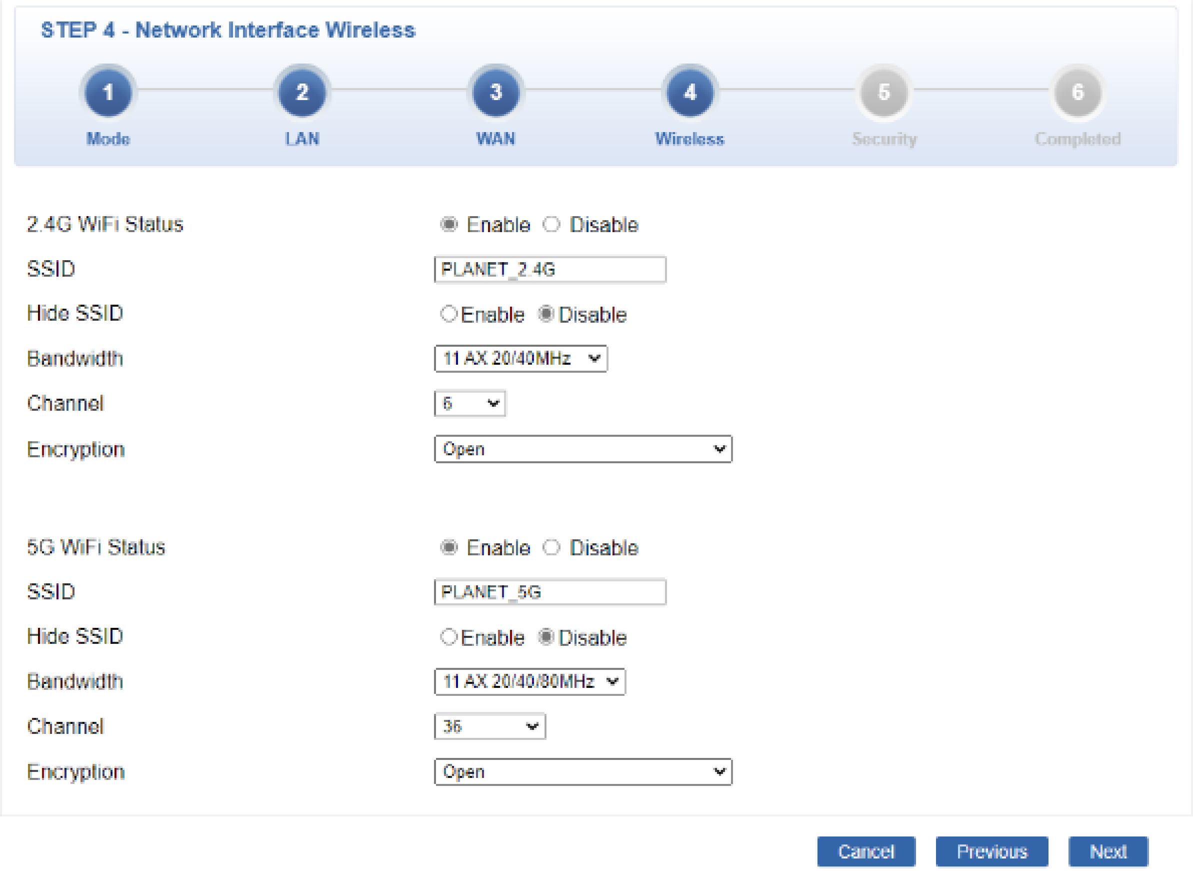
DNS Server 1

DNS Server 2

Figure 4-10: WAN Interface Setup – DHCP Setup

Step 4: Network Interface Wireless

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

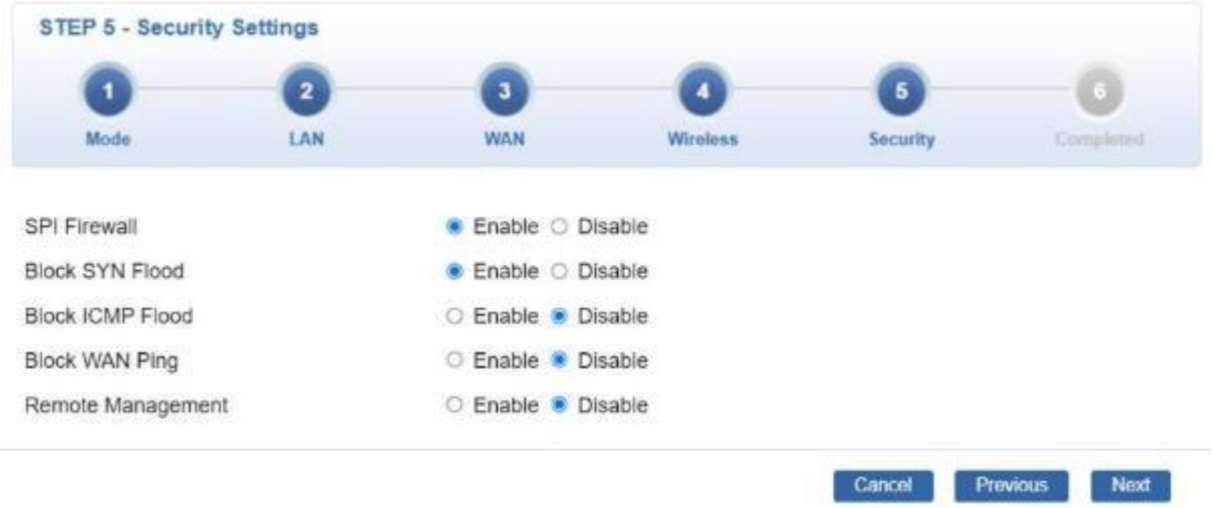


2.4G WiFi Status	● Enable ○ Disable
SSID	PLANET_2.4G
Hide SSID	○ Enable ● Disable
Bandwidth	11 AX 20/40MHz
Channel	6
Encryption	Open
5G WiFi Status	● Enable ○ Disable
SSID	PLANET_5G
Hide SSID	○ Enable ● Disable
Bandwidth	11 AX 20/40/80MHz
Channel	36
Encryption	Open

Figure 4-11: Network Setup

Step 5: Security Setting

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



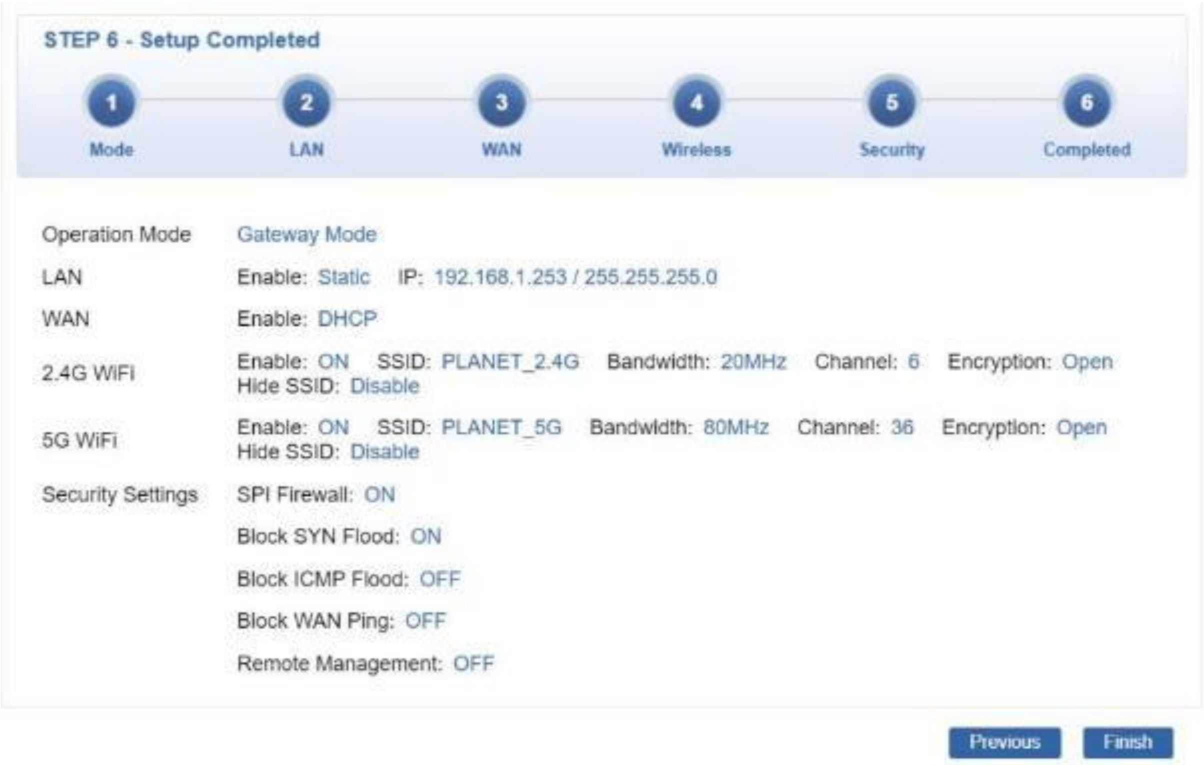
SPI Firewall	● Enable ○ Disable
Block SYN Flood	● Enable ○ Disable
Block ICMP Flood	○ Enable ● Disable
Block WAN Ping	○ Enable ● Disable
Remote Management	○ Enable ● Disable

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 802.11be 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.



Operation Mode: Gateway Mode

LAN: Enable: Static IP: 192.168.1.253 / 255.255.255.0

WAN: Enable: DHCP

2.4G WiFi: Enable: ON SSID: PLANET_2.4G Bandwidth: 20MHz Channel: 6 Encryption: Open Hide SSID: Disable

5G WiFi: Enable: ON SSID: PLANET_5G Bandwidth: 80MHz Channel: 36 Encryption: Open Hide SSID: Disable

Security Settings: SPI Firewall: ON

Block SYN Flood: ON

Block ICMP Flood: OFF

Block WAN Ping: OFF

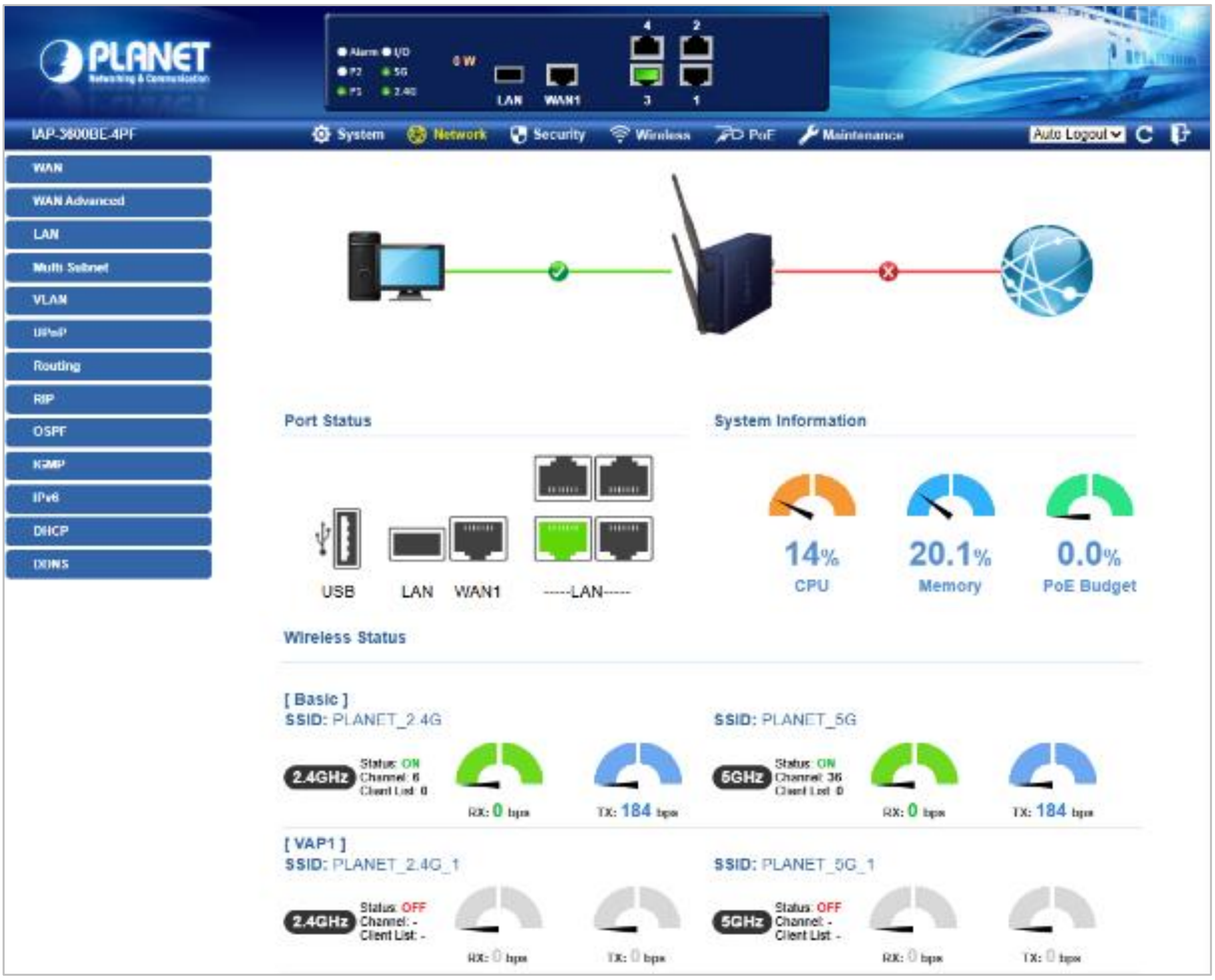
Remote Management: OFF

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.

4.1.5 Dashboard

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



[Basic]
SSID: PLANET_2.4G
2.4GHz Status: ON Channel: 6 Client List: 0 RX: 0 bps TX: 184 bps

SSID: PLANET_5G
5GHz Status: ON Channel: 36 Client List: 0 RX: 0 bps TX: 184 bps

[VAP1]
SSID: PLANET_2.4G_1
2.4GHz Status: OFF Channel: - Client List: - RX: 0 bps TX: 0 bps

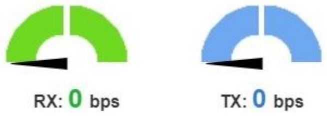
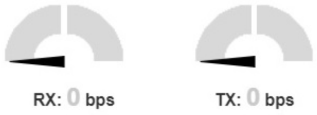
SSID: PLANET_5G_1
5GHz Status: OFF Channel: - Client List: - RX: 0 bps TX: 0 bps

Figure 4-14: Dashboard

Port Status

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

Wireless Status

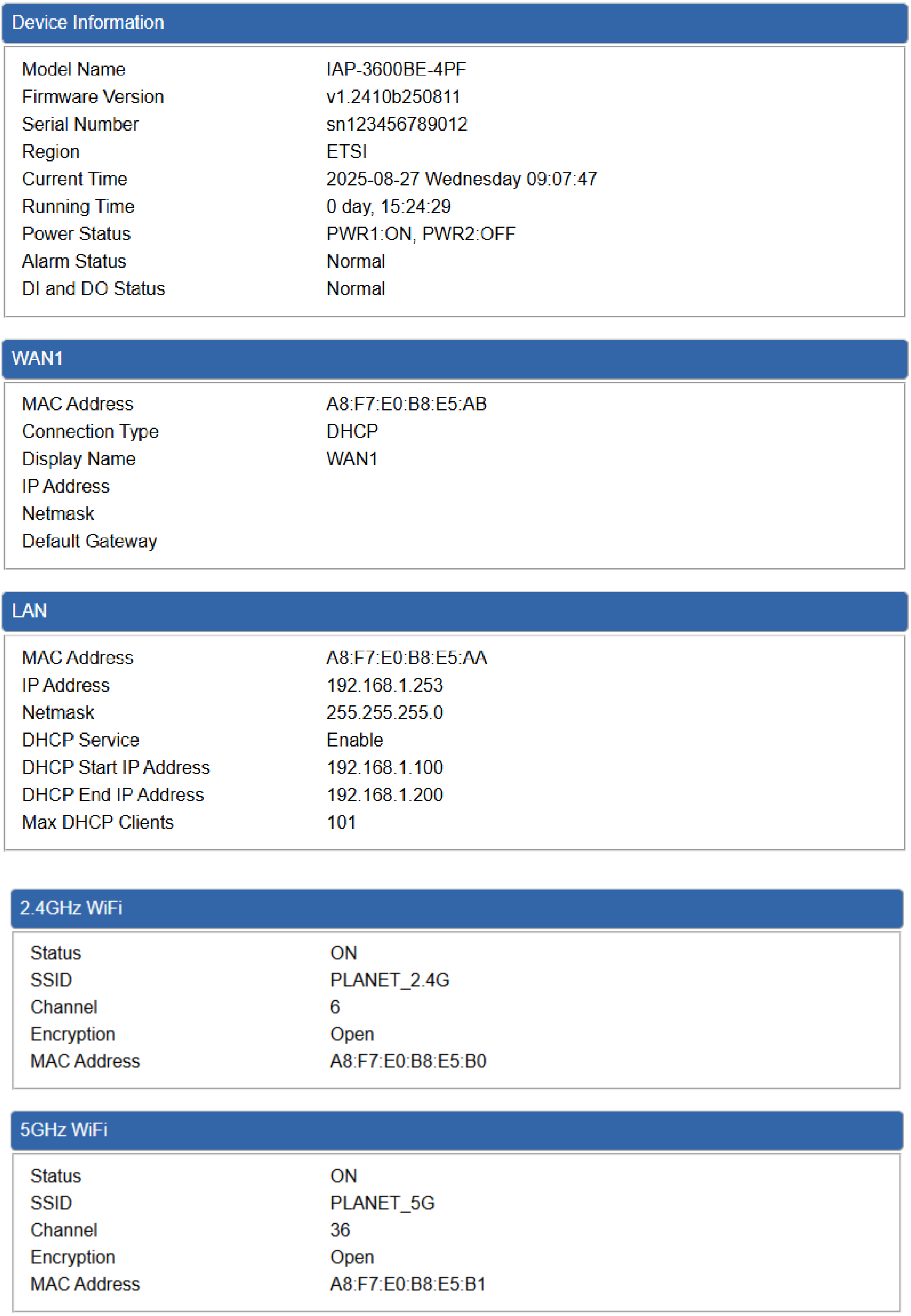
Object	Description
 RX: 0 bps TX: 0 bps	Wireless is in use.
 RX: 0 bps TX: 0 bps	Wireless is not in use.

System Information

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

4.1.6 System Status

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



Device Information

Model Name	IAP-3600BE-4PF
Firmware Version	v1.2410b250811
Serial Number	sn123456789012
Region	ETSI
Current Time	2025-08-27 Wednesday 09:07:47
Running Time	0 day, 15:24:29
Power Status	PWR1:ON, PWR2:OFF
Alarm Status	Normal
DI and DO Status	Normal

WAN1

MAC Address	A8:F7:E0:B8:E5:AB
Connection Type	DHCP
Display Name	WAN1
IP Address	
Netmask	
Default Gateway	

LAN

MAC Address	A8:F7:E0:B8:E5:AA
IP Address	192.168.1.253
Netmask	255.255.255.0
DHCP Service	Enable
DHCP Start IP Address	192.168.1.100
DHCP End IP Address	192.168.1.200
Max DHCP Clients	101

2.4GHz WiFi

Status	ON
SSID	PLANET_2.4G
Channel	6
Encryption	Open
MAC Address	A8:F7:E0:B8:E5:B0

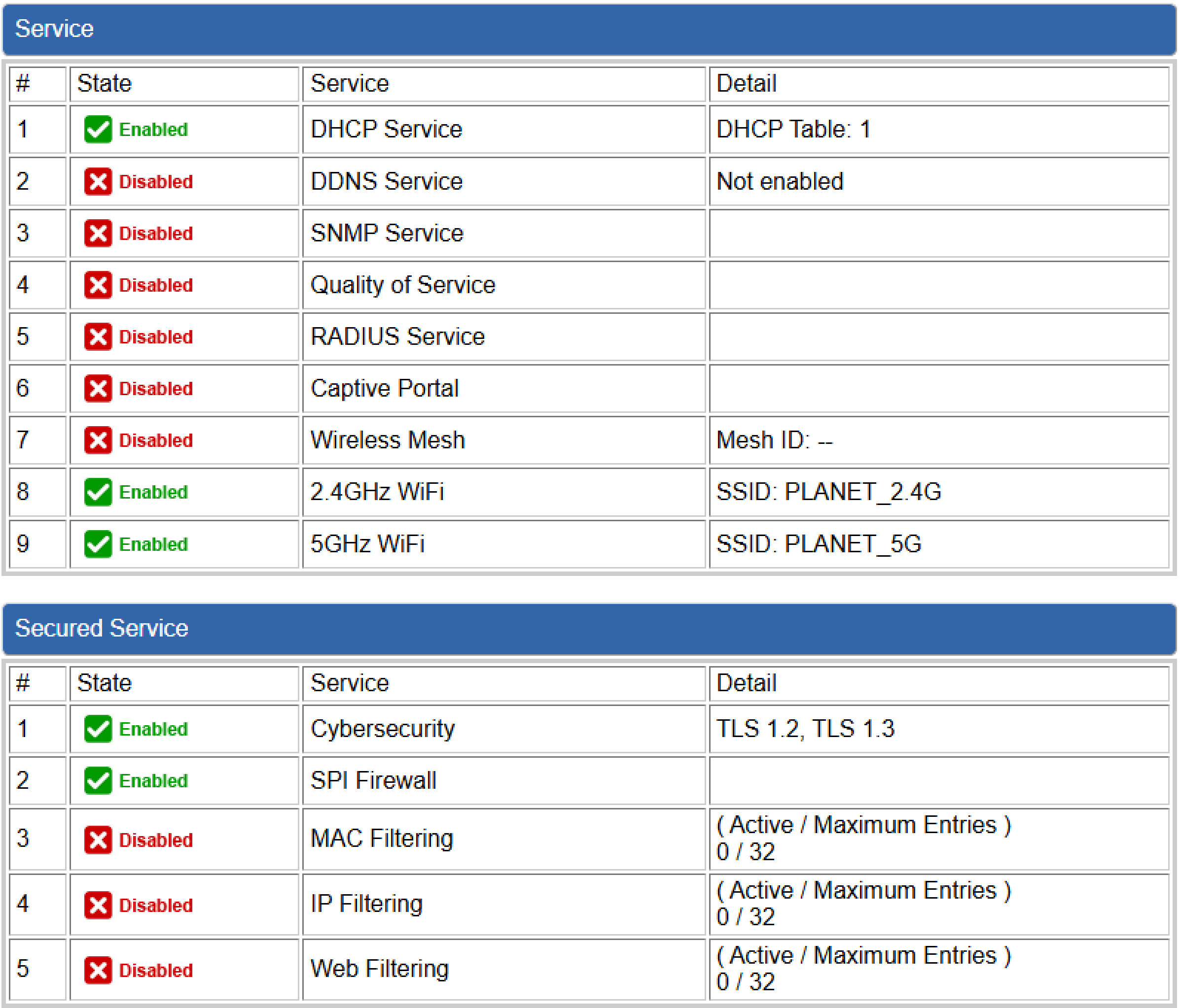
5GHz WiFi

Status	ON
SSID	PLANET_5G
Channel	36
Encryption	Open
MAC Address	A8:F7:E0:B8:E5:B1

Figure 4-15: Status

4.1.7 System Service

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



Service

#	State	Service	Detail
1	✓ Enabled	DHCP Service	DHCP Table: 1
2	✗ Disabled	DDNS Service	Not enabled
3	✗ Disabled	SNMP Service	
4	✗ Disabled	Quality of Service	
5	✗ Disabled	RADIUS Service	
6	✗ Disabled	Captive Portal	
7	✗ Disabled	Wireless Mesh	Mesh ID: --
8	✓ Enabled	2.4GHz WiFi	SSID: PLANET_2.4G
9	✓ Enabled	5GHz WiFi	SSID: PLANET_5G

Secured Service

#	State	Service	Detail
1	✓ Enabled	Cybersecurity	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

4.1.8 Statistics

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

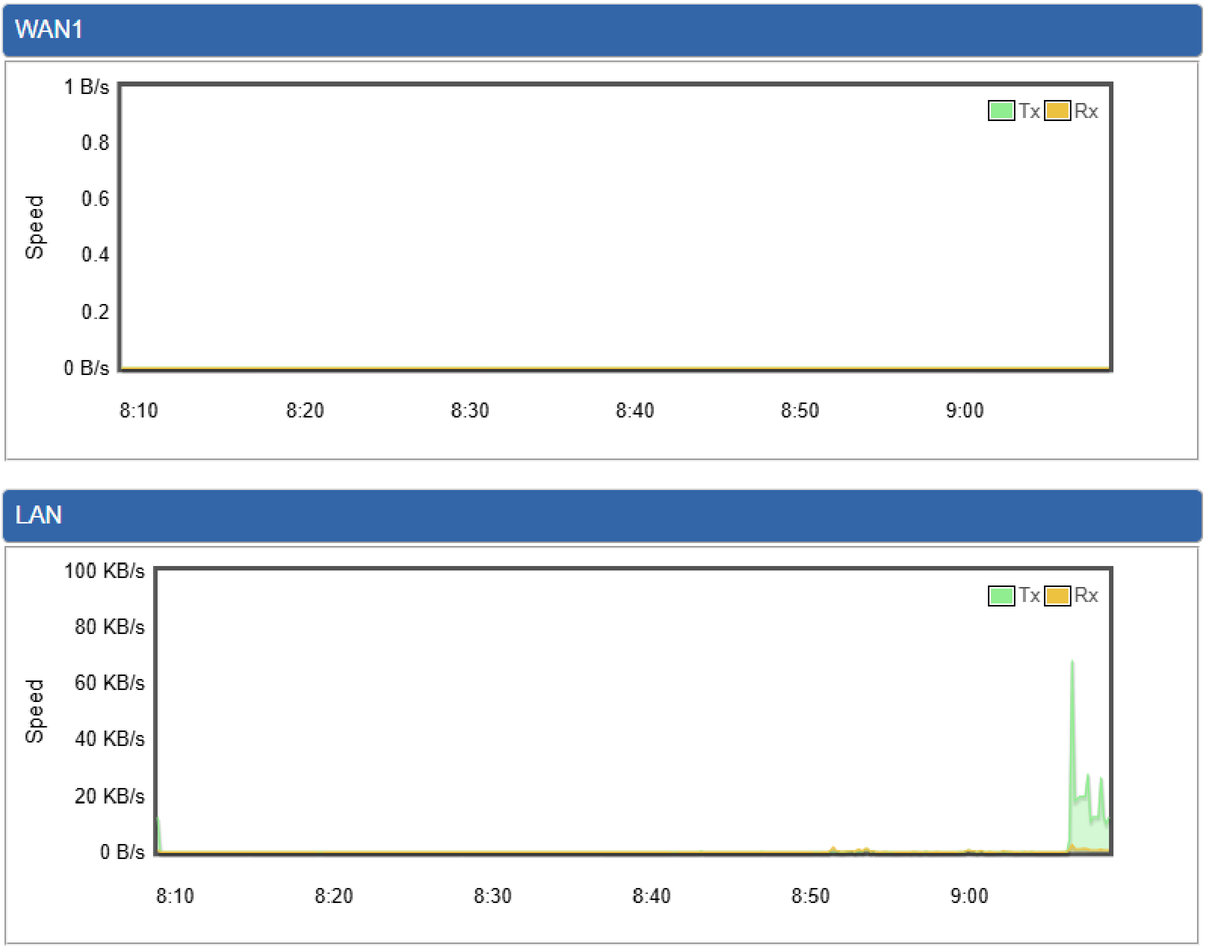
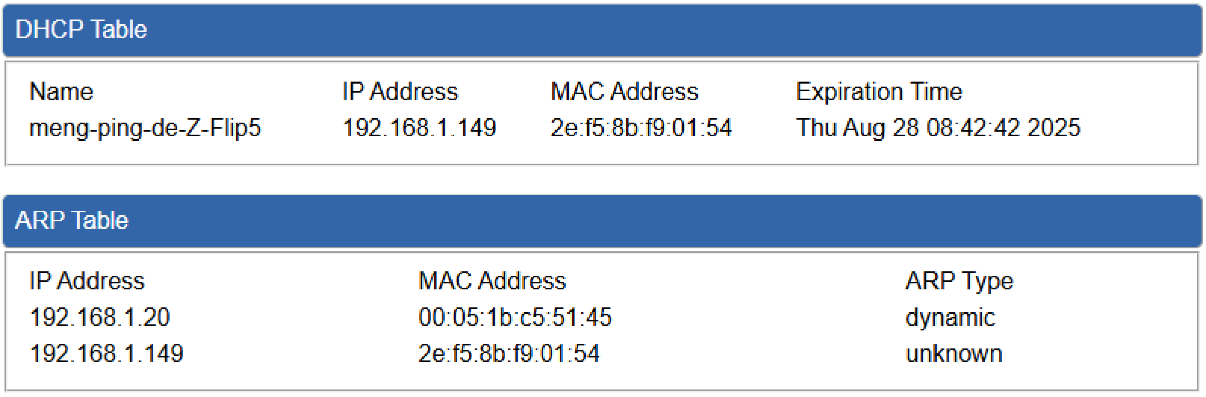


Figure 4-17: Statistics

4.1.9 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
meng-ping-de-Z-Flip5	192.168.1.149	2e:f5:8b:f9:01:54	Thu Aug 28 08:42:42 2025

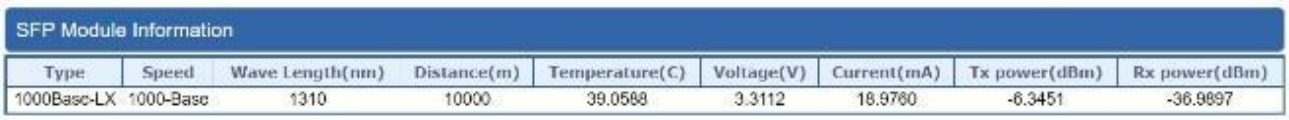
ARP Table

IP Address	MAC Address	ARP Type
192.168.1.20	00:05:1b:c5:51:45	dynamic
192.168.1.149	2e:f5:8b:f9:01:54	unknown

Figure 4-18: Connection Status

4.1.10 SFP Module Information

This page shows the operational status, such as the transceiver type, speed, wavelength, optical output power, optical input power, temperature, laser bias current and transceiver supply voltage in real time. The SFP Module Information page is shown below.



SFP Module Information

Type	Speed	Wave Length(nm)	Distance(m)	Temperature(C)	Voltage(V)	Current(mA)	Tx power(dBm)	Rx power(dBm)
1000Base-LX	1000-Base	1310	10000	39.0588	3.3112	18.9760	-6.3451	-36.9897

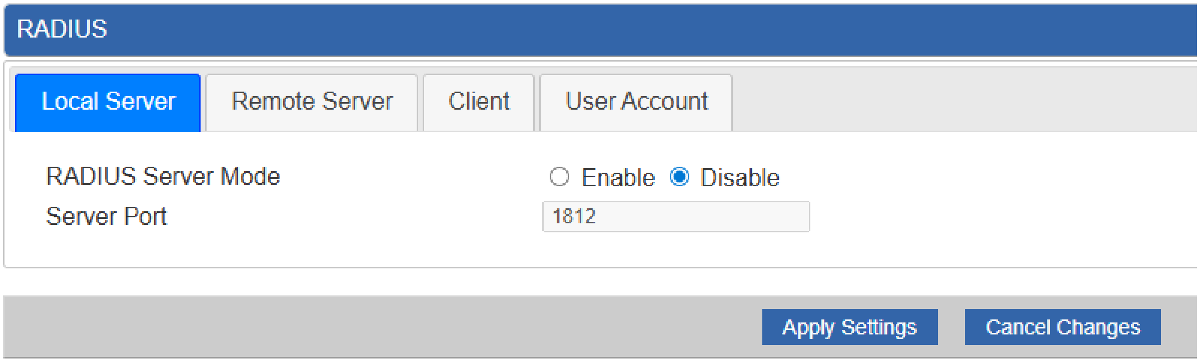
Figure 4.1-1 SFP Module Information

Object	Description
Type	Display the type of current SFP module; the possible types are: ■ 1000BASE-SX ■ 1000BASE-LX
Speed	Display the speed of current SFP module; the speed value or description is obtained from the SFP module. Different vendors' SFP modules might show different speed information.
Wave Length (nm)	Display the wavelength of current SFP module; the wavelength value is obtained from the SFP module. Use this column to check if the wavelength values of two nodes match while the fiber connection fails.
Distance (m)	Display the support distance of current SFP module; the distance value is obtained from the SFP module.
Temperature (C) **– SFP DDM Module Only**	Display the temperature of current SFP DDM module; the temperature value is gotten from the SFP DDM module.
Voltage (V) **– SFP DDM Module Only**	Display the voltage of current SFP DDM module; the voltage value is gotten from the SFP DDM module.
Current (mA) **– SFP DDM Module Only**	Display the ampere of current SFP DDM module; the ampere value is gotten from the SFP DDM module.
TX power (dBm) **– SFP DDM Module Only**	Display the TX power of current SFP DDM module; the TX power value is gotten from the SFP DDM module.
RX power (dBm) **– SFP DDM Module Only**	Display the RX power of current SFP DDM module; the RX power value is gotten from the SFP DDM module.

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

4.1.11 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.



RADIUS Server Mode ○ Enable ● Disable

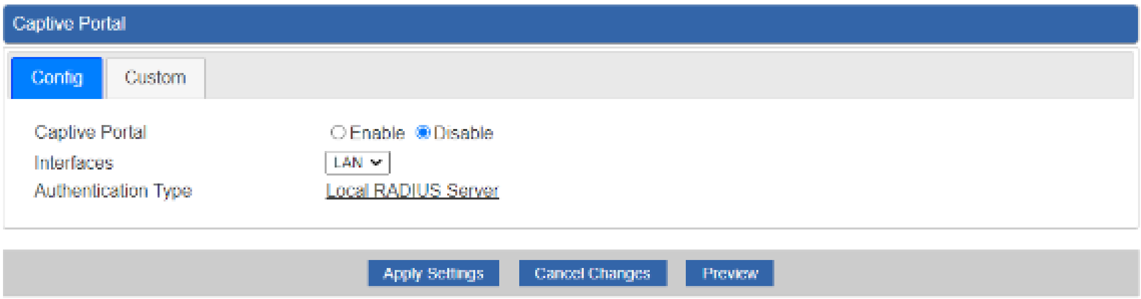
Server Port 1812

Figure 4-19: RADIUS

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

4.1.12 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.



Captive Portal ○ Enable ● Disable
Interfaces LAN
Authentication Type Local RADIUS Server

Figure 4-20: Captive Portal

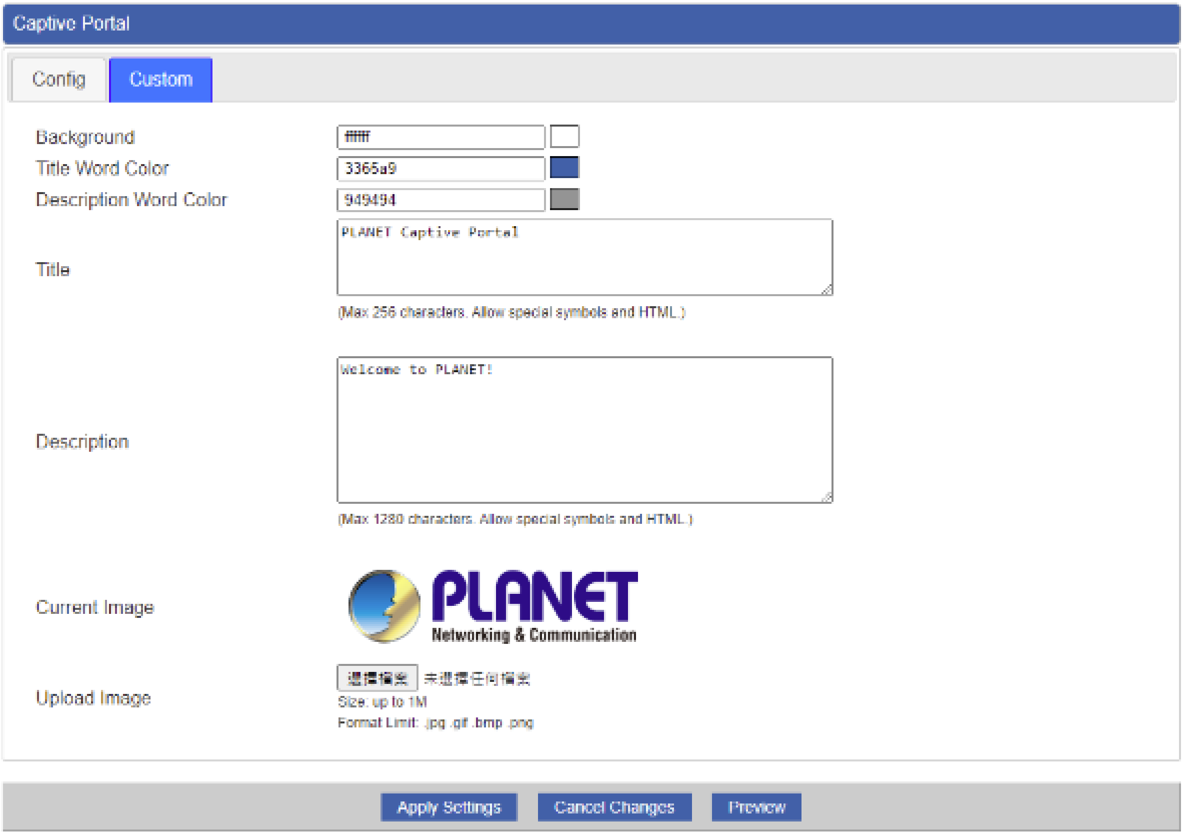
Object	Description
Captive Portal	Disable or enable the Captive Portal function. The default configuration is disabled.

Note

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

Customizing the Custom Captive Portal Web Page

1. Click **Custom**



Captive Portal

Background: ffffff

Title Word Color: 3365a9

Description Word Color: 949494

Title: PLANET Captive Portal

(Max 256 characters. Allow special symbols and HTML.)

Description: Welcome to PLANET!

(Max 1280 characters. Allow special symbols and HTML.)

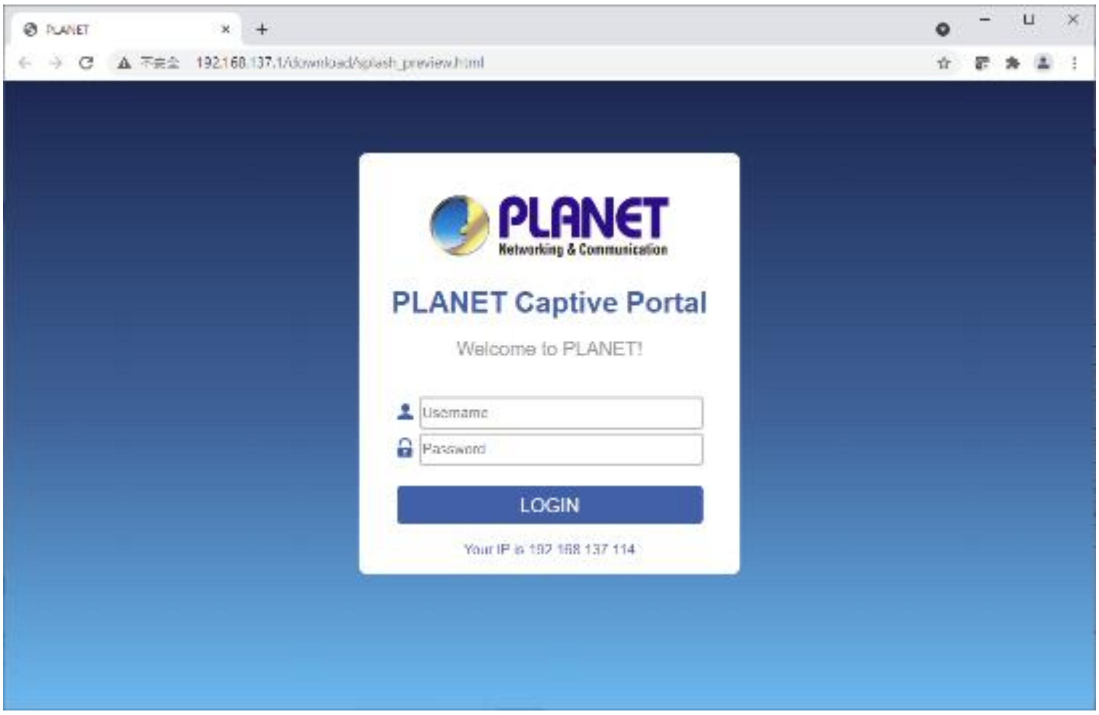
Current Image

Upload Image: 選擇檔案 未選擇任何檔案

Size: up to 1M

Format Limit: .jpg .gif .bmp .png

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



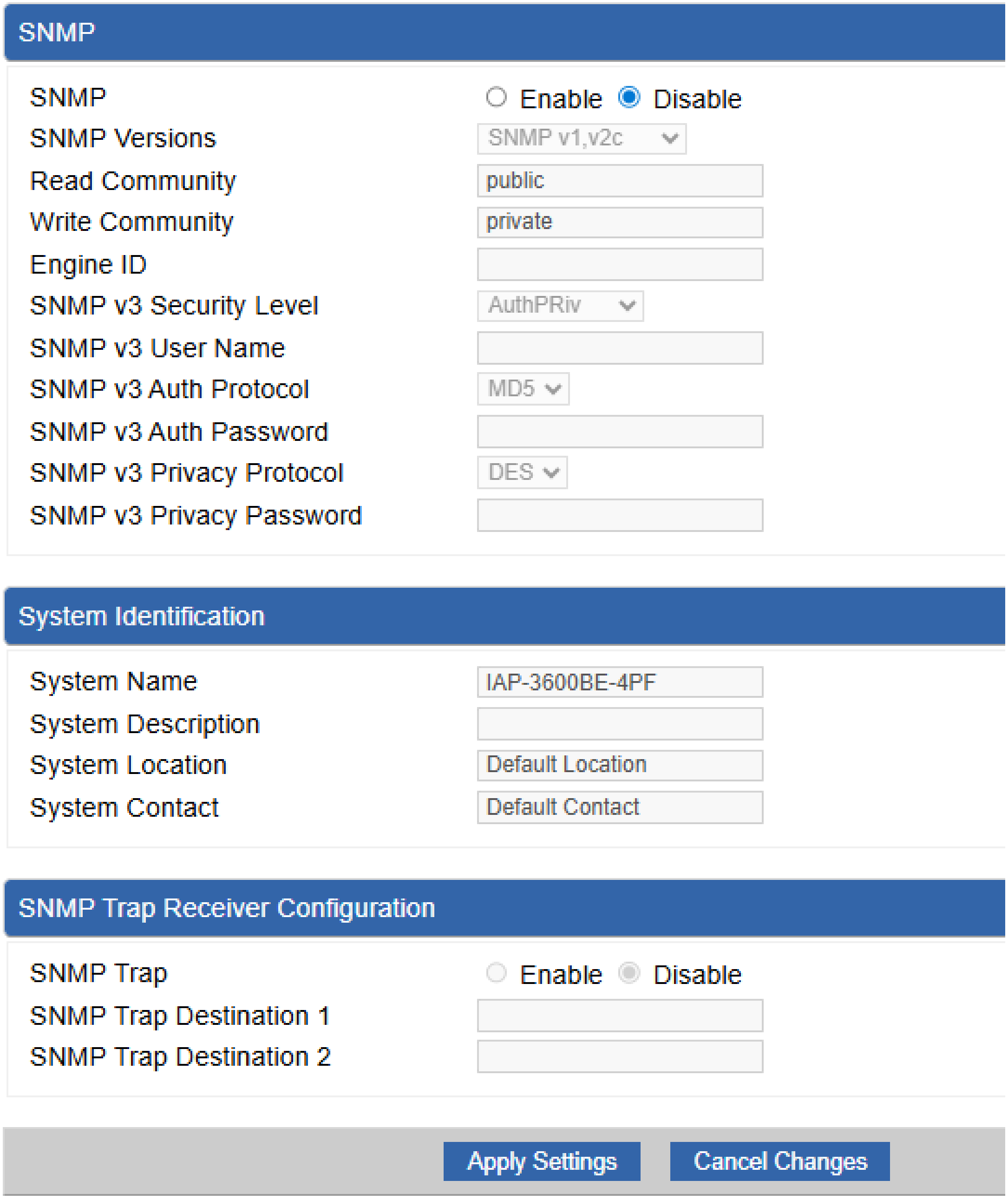
PLANET Captive Portal

Welcome to PLANET!

Your IP is 192.168.137.114

4.1.13 SNMP

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



SNMP

SNMP	○ Enable ● Disable
SNMP Versions	SNMP v1,v2c
Read Community	public
Write Community	private
Engine ID	
SNMP v3 Security Level	AuthPRiv
SNMP v3 User Name	
SNMP v3 Auth Protocol	MD5
SNMP v3 Auth Password	
SNMP v3 Privacy Protocol	DES
SNMP v3 Privacy Password	

System Identification

System Name	IAP-3600BE-4PF
System Description	
System Location	Default Location
System Contact	Default Contact

SNMP Trap Receiver Configuration

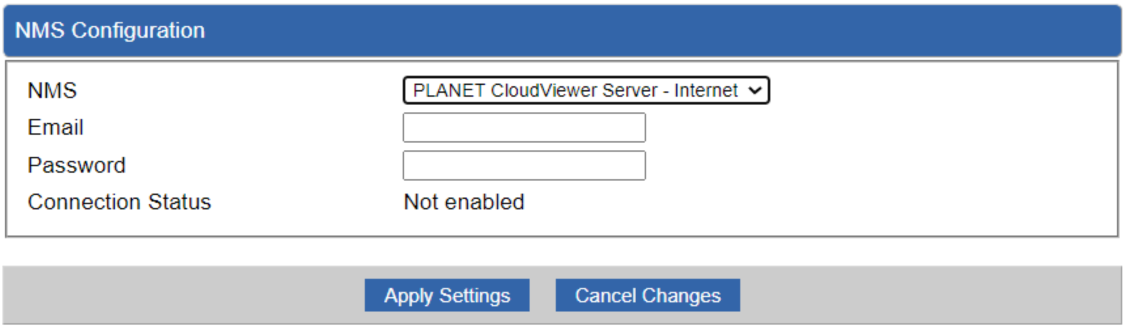
SNMP Trap	○ Enable ● Disable
SNMP Trap Destination 1	
SNMP Trap Destination 2	

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 802.11be Wireless AP.
System Name	Allows entering characters for system name of the Industrial 802.11be Wireless AP.
System Location	Allows entering characters for system location of the Industrial 802.11be Wireless AP.
System Contact	Allows entering characters for system contact of the Industrial 802.11be 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.

4.1.14 NMS

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



NMS Configuration

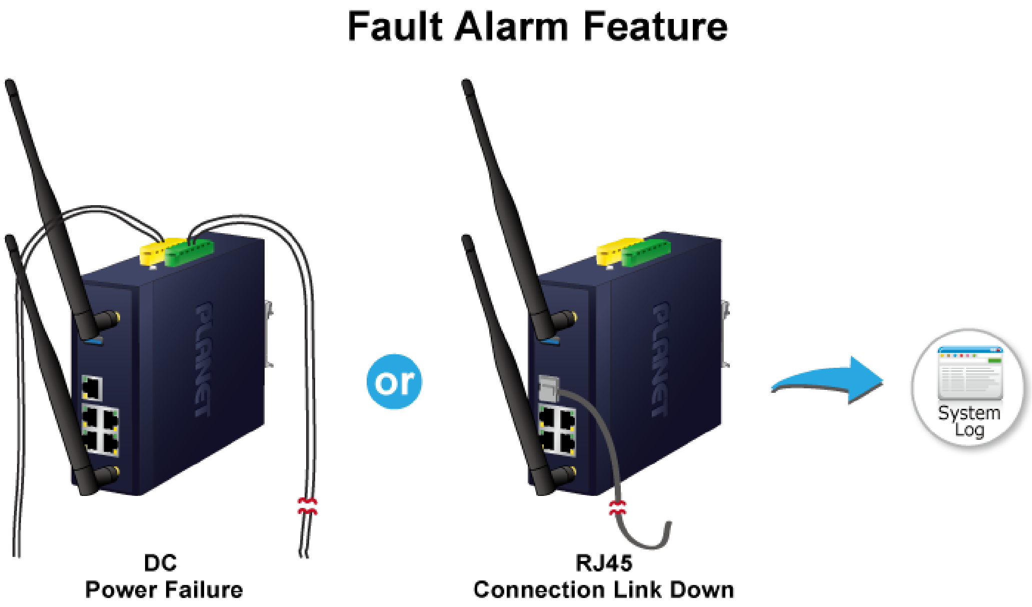
NMS	PLANET CloudViewer Server - Internet
Email	
Password	
Connection Status	Not enabled

Figure 4-22: CloudNMS Server

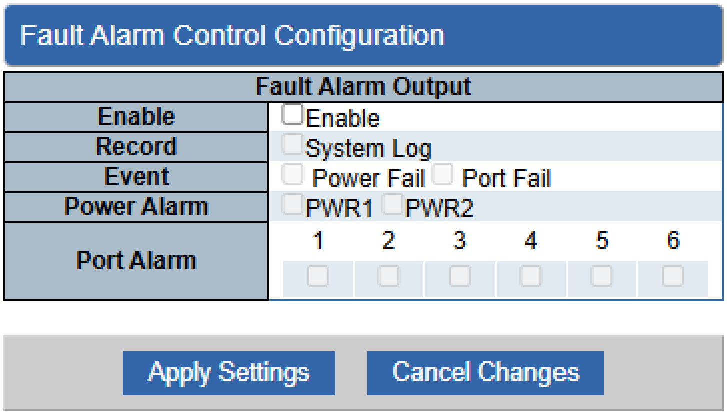
Object	Description
Email	The email is registered on CloudNMS Server
Password	The password of your CloudNMS account
Connection Status	Indicates the status of connecting CloudNMS Server

4.1.15 Fault Alarm

The Industrial 802.11be 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.



Fault Alarm Control Configuration

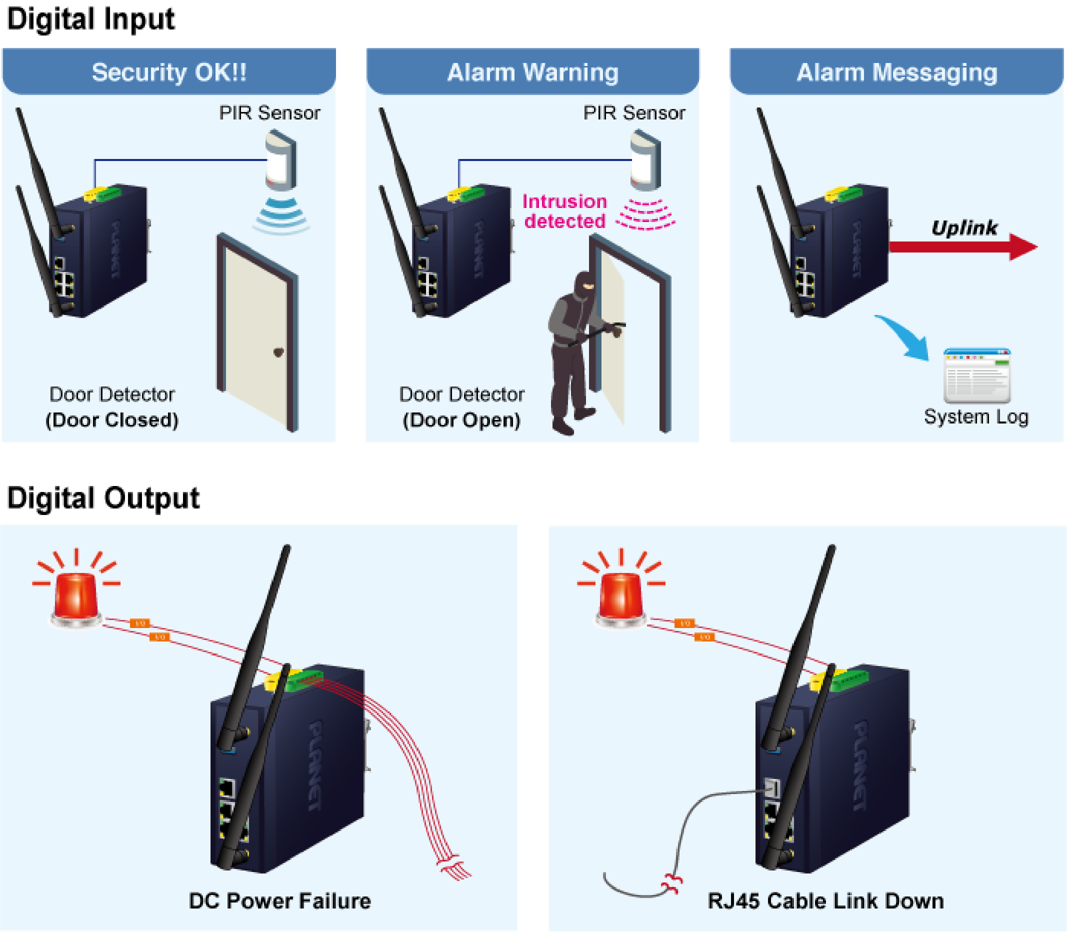
Fault Alarm Output						
Enable	□ Enable					
Record	□ System Log					
Event	□ Power Fail □ Port Fail					
Power Alarm	□ PWR1 □ PWR2					
Port Alarm	1	2	3	4	5	6
	□	□	□	□	□	□

Figure 4-23: Fault Alarm

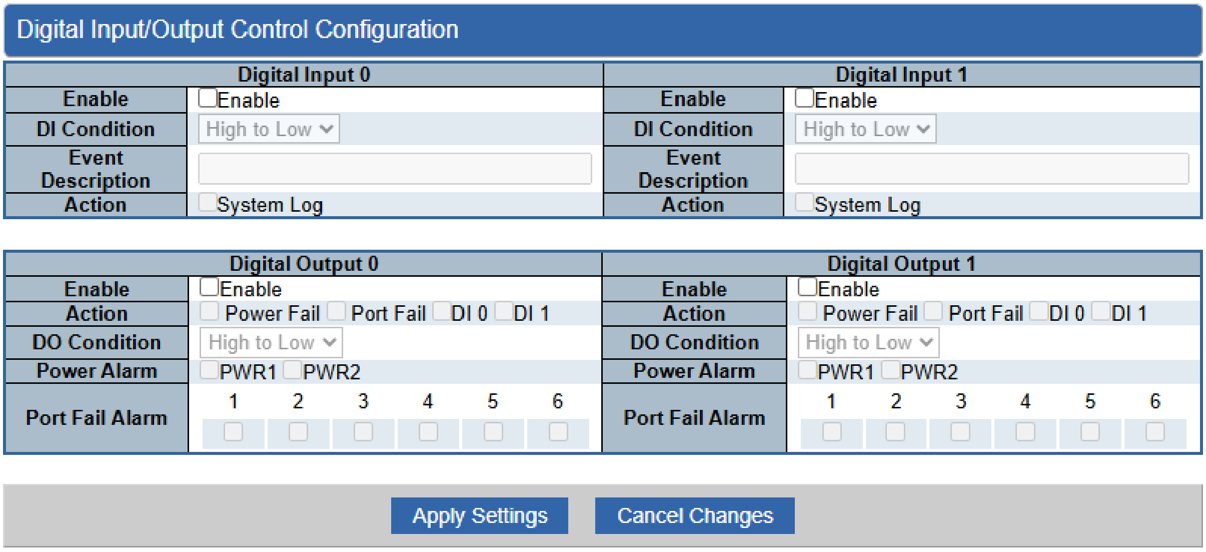
Object	Description
• **Enable**	Controls whether Fault Alarm is enabled.
• **Record**	Controls whether Record is sending System log or SMS.
• **Event**	Controls whether Port Failure or Power Failure or both is/are detected.
• **Power Alarm**	Controls whether faulty PWR1 or faulty PWR2 or both is/are detected.
• **Port Alarm**	Controls which port or all is/are detected for fault.

4.1.16 Digital Input / Output

The Industrial 802.11be 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 802.11be Wireless AP port shows link down, link up or power failure.



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



Digital Input/Output Control Configuration

Digital Input 0		Digital Input 1	
Enable	□ Enable	Enable	□ Enable
DI Condition	High to Low	DI Condition	High to Low
Event Description		Event Description	
Action	□ System Log	Action	□ System Log

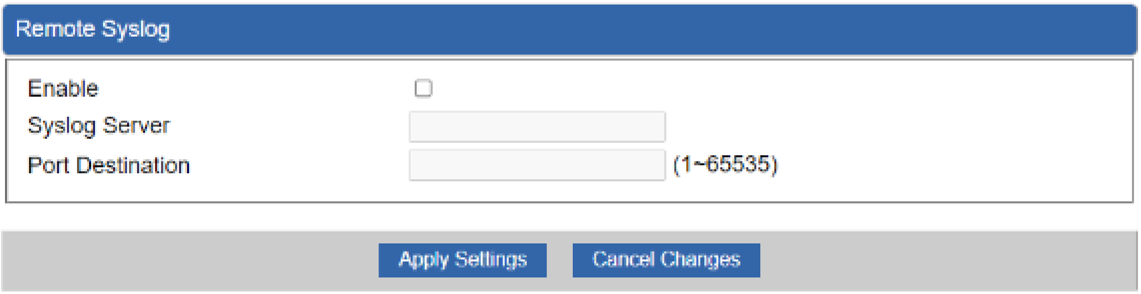
Digital Output 0		Digital Output 1	
Enable	□ Enable	Enable	□ Enable
Action	□ Power Fail □ Port Fail □ DI 0 □ DI 1	Action	□ Power Fail □ Port Fail □ DI 0 □ DI 1
DO Condition	High to Low	DO Condition	High to Low
Power Alarm	□ PWR1 □ PWR2	Power Alarm	□ PWR1 □ PWR2
Port Fail Alarm	1 2 3 4 5 6 □ □ □ □ □ □	Port Fail Alarm	1 2 3 4 5 6 □ □ □ □ □ □

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.

4.1.17 Remote Syslog



Remote Syslog

Enable □

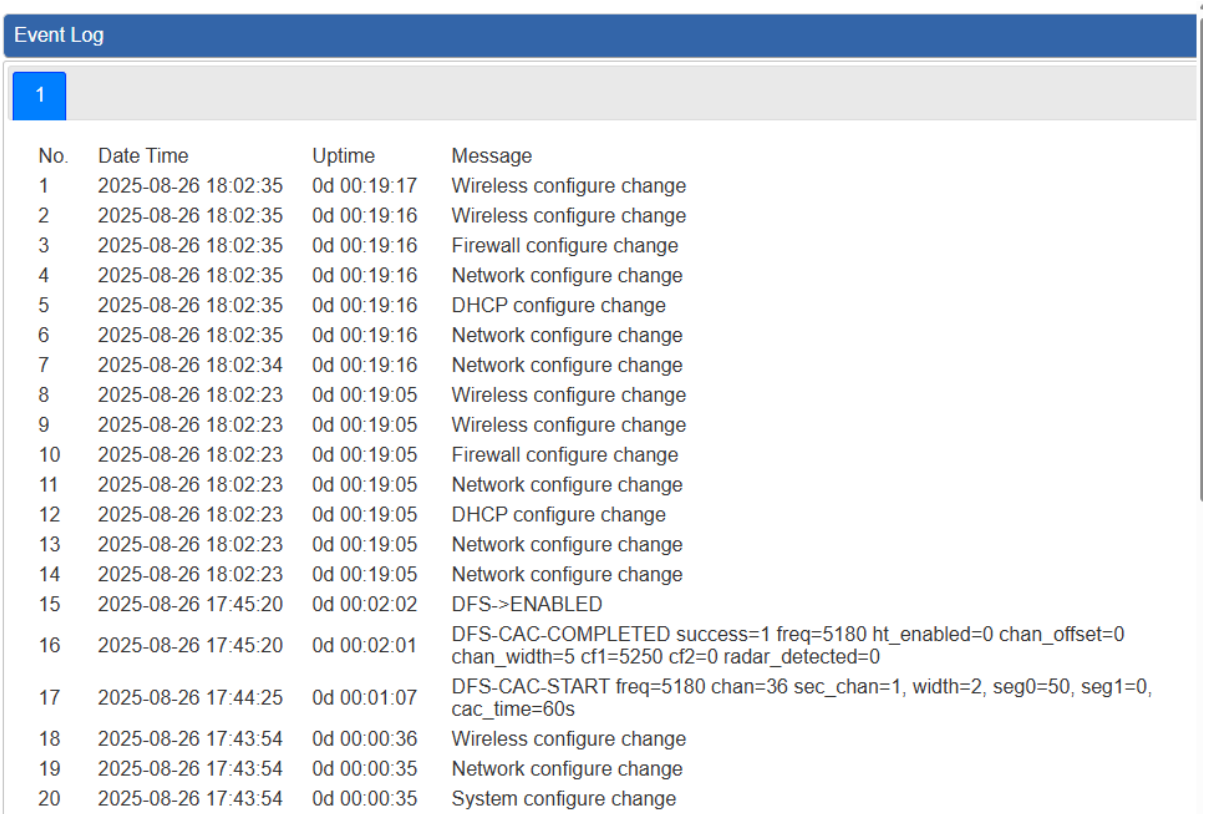
Syslog Server

Port Destination (1~65535)

Figure 4-25: Remote Syslog

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

4.1.18 Event Log



No.	Date Time	Uptime	Message
1	2025-08-26 18:02:35	0d 00:19:17	Wireless configure change
2	2025-08-26 18:02:35	0d 00:19:16	Wireless configure change
3	2025-08-26 18:02:35	0d 00:19:16	Firewall configure change
4	2025-08-26 18:02:35	0d 00:19:16	Network configure change
5	2025-08-26 18:02:35	0d 00:19:16	DHCP configure change
6	2025-08-26 18:02:35	0d 00:19:16	Network configure change
7	2025-08-26 18:02:34	0d 00:19:16	Network configure change
8	2025-08-26 18:02:23	0d 00:19:05	Wireless configure change
9	2025-08-26 18:02:23	0d 00:19:05	Wireless configure change
10	2025-08-26 18:02:23	0d 00:19:05	Firewall configure change
11	2025-08-26 18:02:23	0d 00:19:05	Network configure change
12	2025-08-26 18:02:23	0d 00:19:05	DHCP configure change
13	2025-08-26 18:02:23	0d 00:19:05	Network configure change
14	2025-08-26 18:02:23	0d 00:19:05	Network configure change
15	2025-08-26 17:45:20	0d 00:02:02	DFS->ENABLED
16	2025-08-26 17:45:20	0d 00:02:01	DFS-CAC-COMPLETED success=1 freq=5180 ht_enabled=0 chan_offset=0 chan_width=5 cf1=5250 cf2=0 radar_detected=0
17	2025-08-26 17:44:25	0d 00:01:07	DFS-CAC-START freq=5180 chan=36 sec_chan=1, width=2, seg0=50, seg1=0, cac_time=60s
18	2025-08-26 17:43:54	0d 00:00:36	Wireless configure change
19	2025-08-26 17:43:54	0d 00:00:35	Network configure change
20	2025-08-26 17:43:54	0d 00:00:35	System configure change

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 802.11be Wireless AP as shown in Figure 4-27.

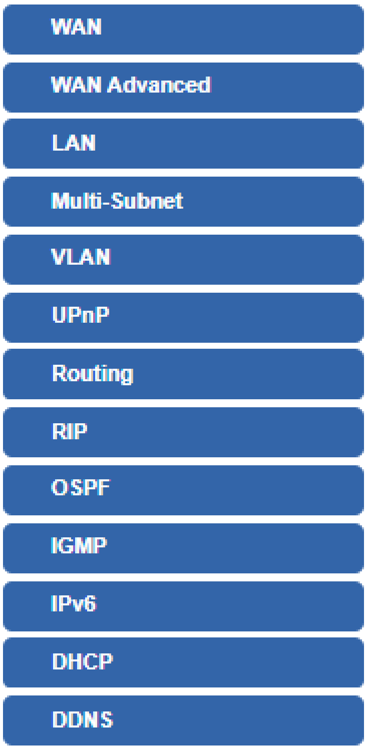


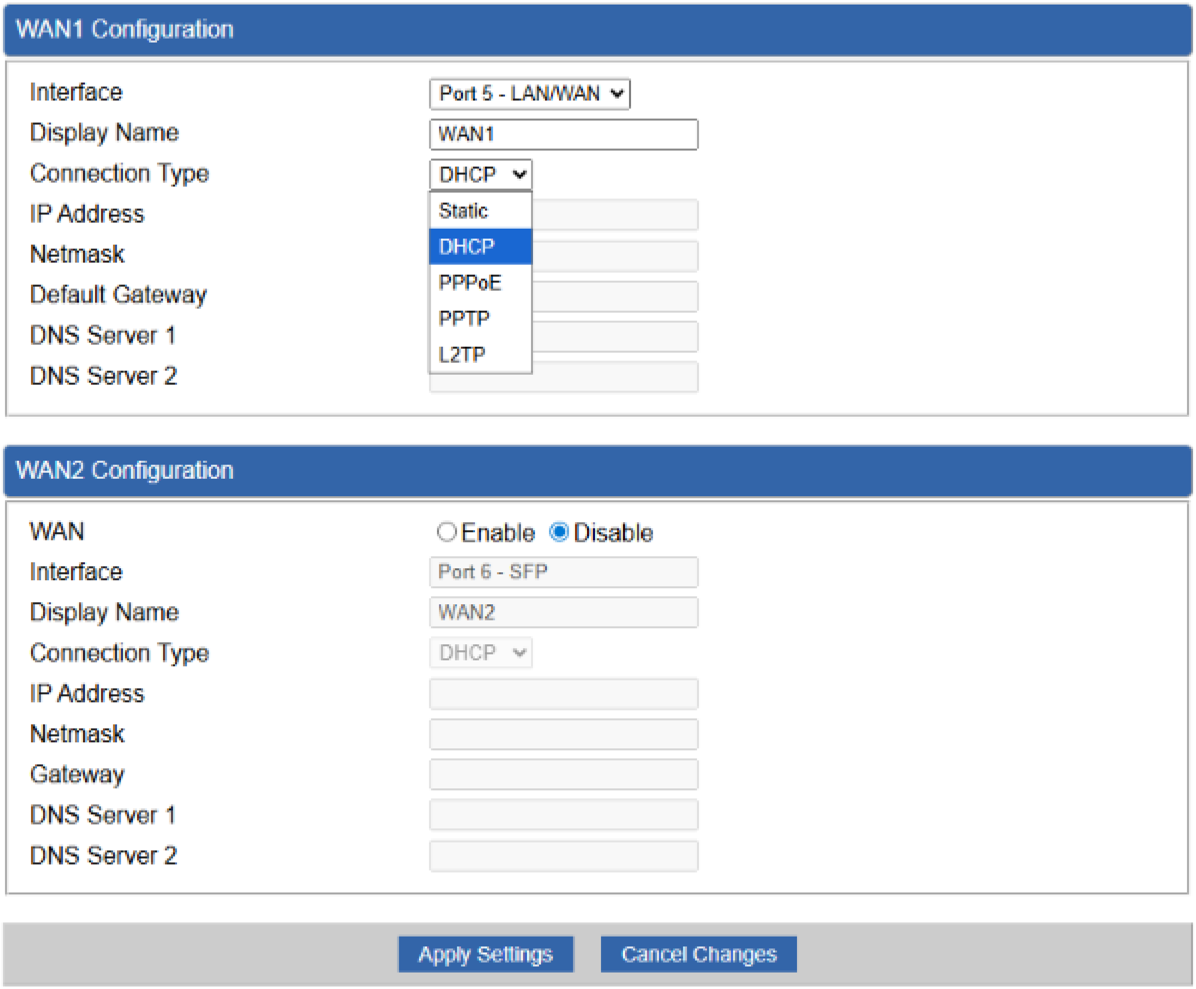
Figure 4-27: Network Menu

Object	Description
WAN	Allows setting WAN interface.
WAN Advanced	Allows setting WAN Advanced settings.
LAN	Allows setting LAN interface.
Multi-Subnet	Allows setting Multi-Subnet1 ~ Subnet4 interface.
VLAN	Disable or enable the VLAN function. The default configuration is disabled.
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 802.11be Wireless AP as shown in Figure 4-28. Here you may select the access method by clicking the item value of WAN access type.



WAN1 Configuration

Interface	Port 5 - LAN/WAN
Display Name	WAN1
Connection Type	DHCP
IP Address	
Netmask	
Default Gateway	
DNS Server 1	
DNS Server 2	

WAN2 Configuration

WAN	○ Enable ● Disable
Interface	Port 6 - SFP
Display Name	WAN2
Connection Type	DHCP
IP Address	
Netmask	
Gateway	
DNS Server 1	
DNS Server 2	

Figure 4-28: WAN

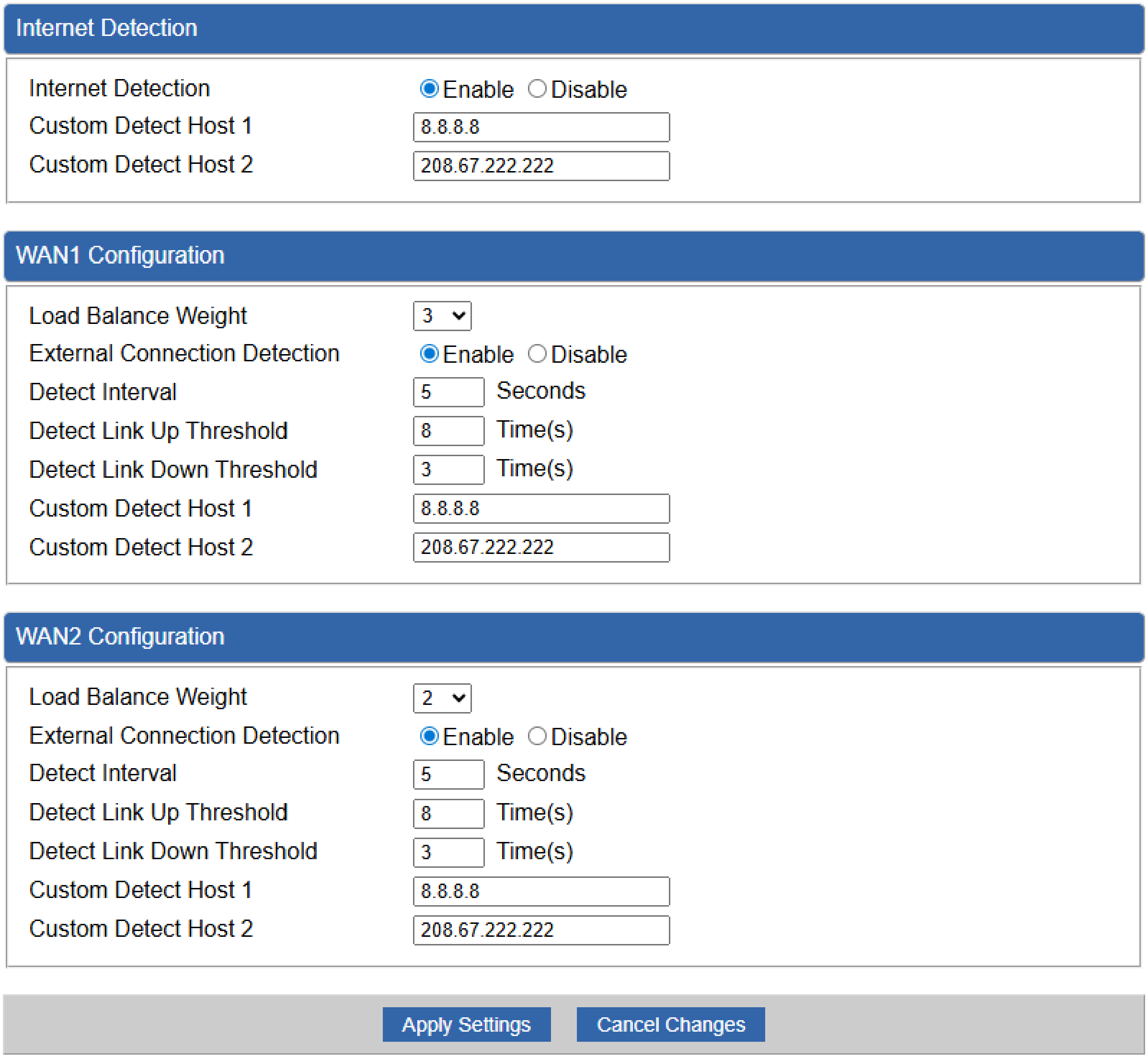
Object	Description	
WAN Access Type	Please select the corresponding WAN Access Type for the Internet, and fill out the correct parameters from your local ISP in the fields which appear below.	
	Static	Select Static IP Address if all the Internet ports' IP information is provided to you by your ISP (Internet 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 802.11be 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** 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 802.11be Wireless AP will not work properly. In case of emergency, press the hardware-based "Reset" button.

4.2.2 WAN Advanced

This page is used to configure the advanced parameters for Internet area network which connects to the WAN port of your VPN Security Gateway as shown below. Here you may change the setting for Load Balance Weight, Detect Interval, Detect Linkup Threshold, etc.



Internet Detection

Internet Detection	● Enable ○ Disable
Custom Detect Host 1	8.8.8.8
Custom Detect Host 2	208.67.222.222

WAN1 Configuration

Load Balance Weight	3
External Connection Detection	● Enable ○ Disable
Detect Interval	5 Seconds
Detect Link Up Threshold	8 Time(s)
Detect Link Down Threshold	3 Time(s)
Custom Detect Host 1	8.8.8.8
Custom Detect Host 2	208.67.222.222

WAN2 Configuration

Load Balance Weight	2
External Connection Detection	● Enable ○ Disable
Detect Interval	5 Seconds
Detect Link Up Threshold	8 Time(s)
Detect Link Down Threshold	3 Time(s)
Custom Detect Host 1	8.8.8.8
Custom Detect Host 2	208.67.222.222

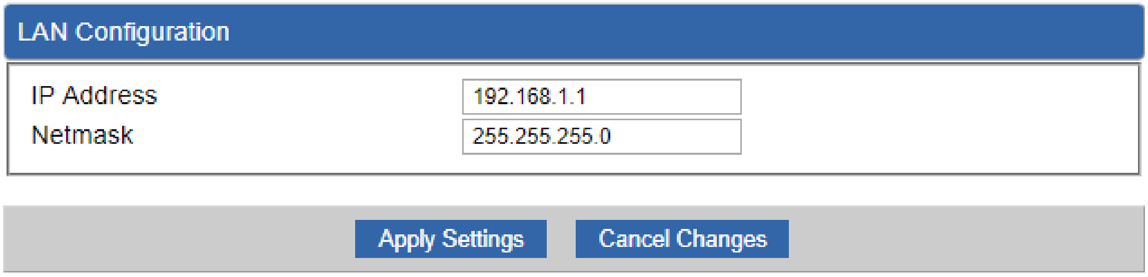
Figure 4.2-1 WAN Advanced Configuration

Object	Description
Load Balance Weight	Load Balance Weight allows you to set a relative weight (from 1 - 10) for each WAN port.
External Connection Detection	Enable to detect the status of WAN connection.
Detect Interval	Set the detect interval as you need. The recommended value is 5 (default).
Detect Link Up	Set the times for detecting link up.

Object	Description
Threshold	The recommended value is 8 (default).
Detect Link Down Threshold	Set the times for detecting link down. The recommended value is 3 (default).
Custom Detect Host	The host is used to check whether the internet connection is alive or not.

4.2.3 LAN

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



LAN Configuration

IP Address: 192.168.1.1

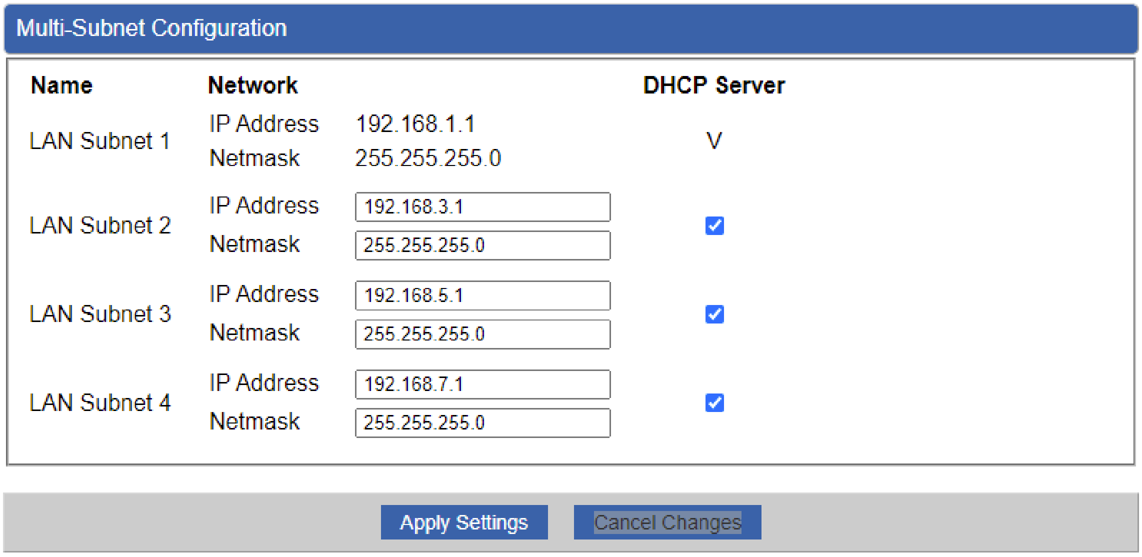
Netmask: 255.255.255.0

Figure 4-29: LAN Setup

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

4.2.4 Multi-Subnet

This page provides multi-subnet setting as shown below.



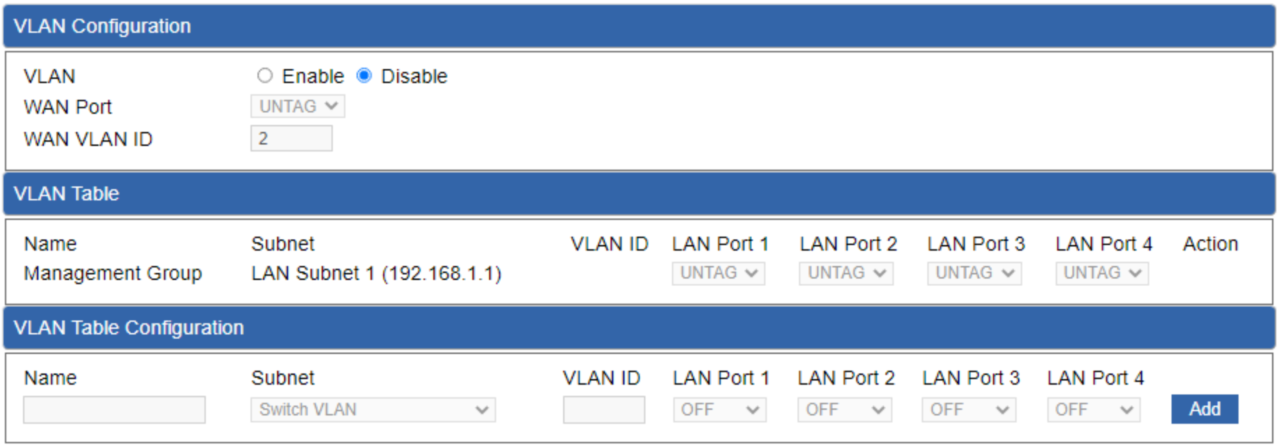
Multi-Subnet Configuration

Name	Network		DHCP Server
LAN Subnet 1	IP Address Netmask	192.168.1.1 255.255.255.0	V
LAN Subnet 2	IP Address Netmask	192.168.3.1 255.255.255.0	☑
LAN Subnet 3	IP Address Netmask	192.168.5.1 255.255.255.0	☑
LAN Subnet 4	IP Address Netmask	192.168.7.1 255.255.255.0	☑

Figure 4.2-2 Multi-Subnet Configuration

4.2.5 VLAN

Please refer to the following sections for the details as shown below.



VLAN Configuration

VLAN	○ Enable ● Disable
WAN Port	UNTAG
WAN VLAN ID	2

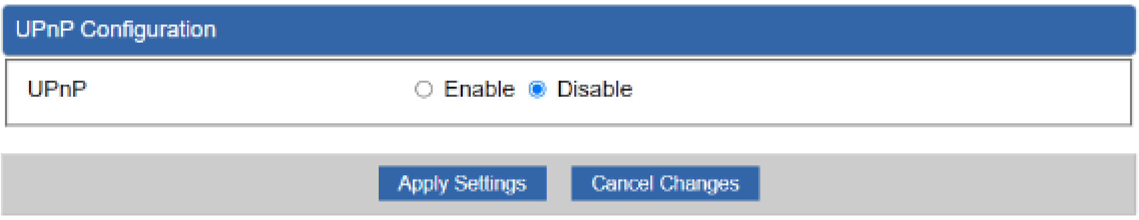
VLAN Table

Name	Subnet	VLAN ID	LAN Port 1	LAN Port 2	LAN Port 3	LAN Port 4	Action
Management Group	LAN Subnet 1 (192.168.1.1)		UNTAG	UNTAG	UNTAG	UNTAG	

VLAN Table Configuration

Name	Subnet	VLAN ID	LAN Port 1	LAN Port 2	LAN Port 3	LAN Port 4	
	Switch VLAN		OFF	OFF	OFF	OFF	Add

4.2.6 UPnP


UPnP Configuration

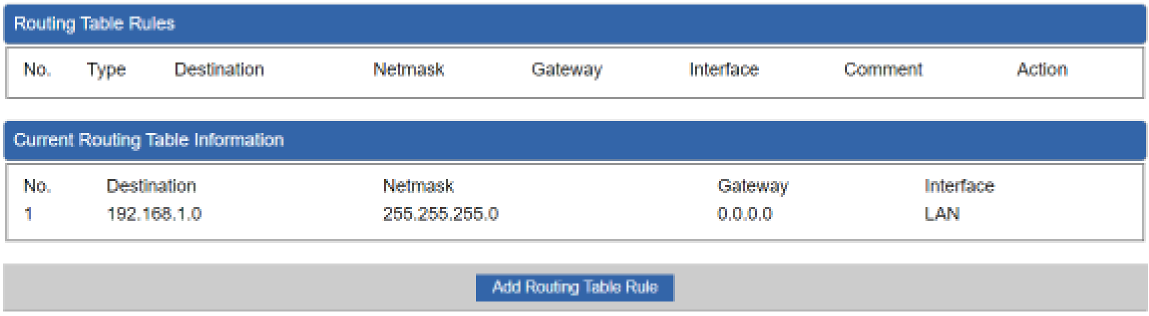
UPnP ○ Enable ● Disable

Figure 4-30: UpnP

Object	Description
UpnP	Set the function as enable or disable

4.2.7 Routing

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



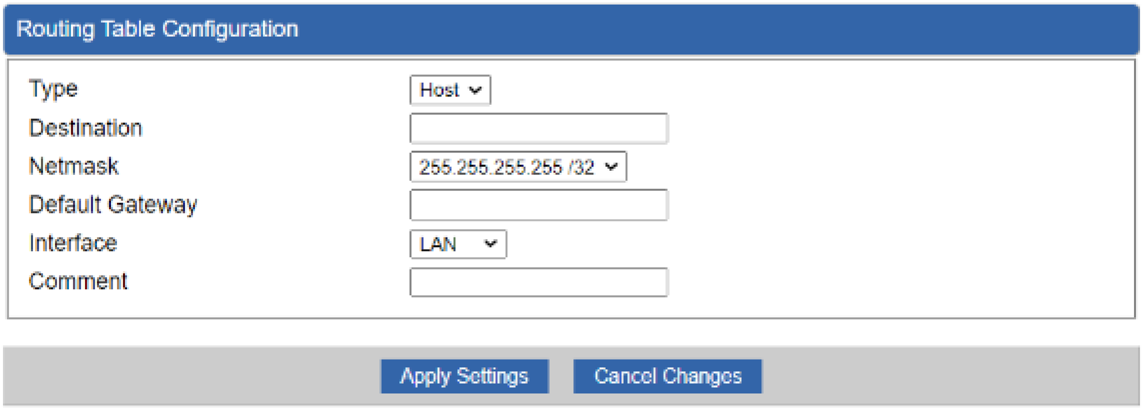
Routing Table Rules

No.	Type	Destination	Netmask	Gateway	Interface	Comment	Action

Current Routing Table Information

No.	Destination	Netmask	Gateway	Interface
1	192.168.1.0	255.255.255.0	0.0.0.0	LAN

Figure 4-31: Routing table



Routing Table Configuration

Type	Host
Destination	
Netmask	255.255.255.255 /32
Default Gateway	
Interface	LAN
Comment	

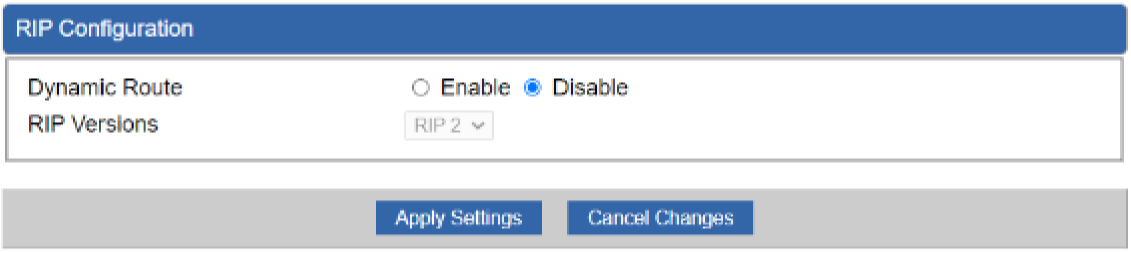
Figure 4-32: Routing setup

Routing tables contain a list of IP addresses. Each IP address identifies a remote Industrial 802.11be Wireless AP (or other network gateway) that the local Industrial 802.11be 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 802.11be 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.

Object	Description
Interface	Select the interface that the IP packet must use to transmit out of the Industrial 802.11be Wireless AP when this route is used.
Comment	Enter any words for recognition.

4.2.8 RIP



RIP Configuration

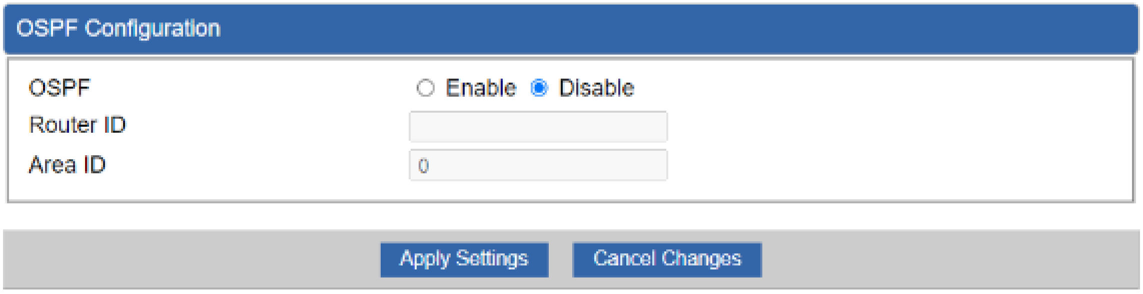
Dynamic Route ○ Enable ● Disable

RIP Versions RIP 2

Figure 4-33: RIP

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

4.2.9 OSPF



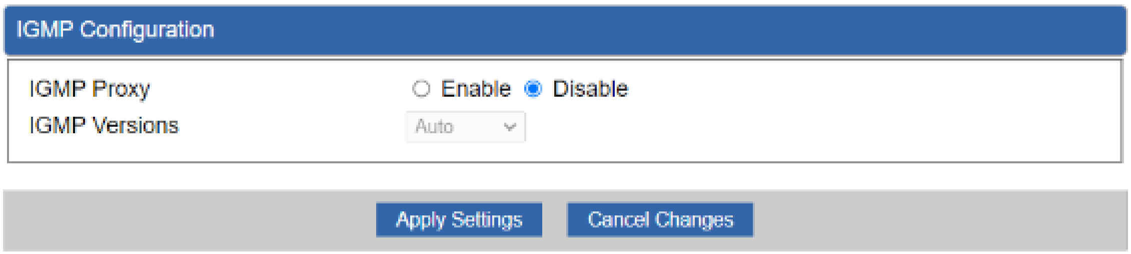
OSPF Configuration

OSPF	○ Enable ● Disable
Router ID	
Area ID	0

Figure 4-34: OSPF

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

4.2.10 IGMP



IGMP Configuration

IGMP Proxy ○ Enable ● Disable

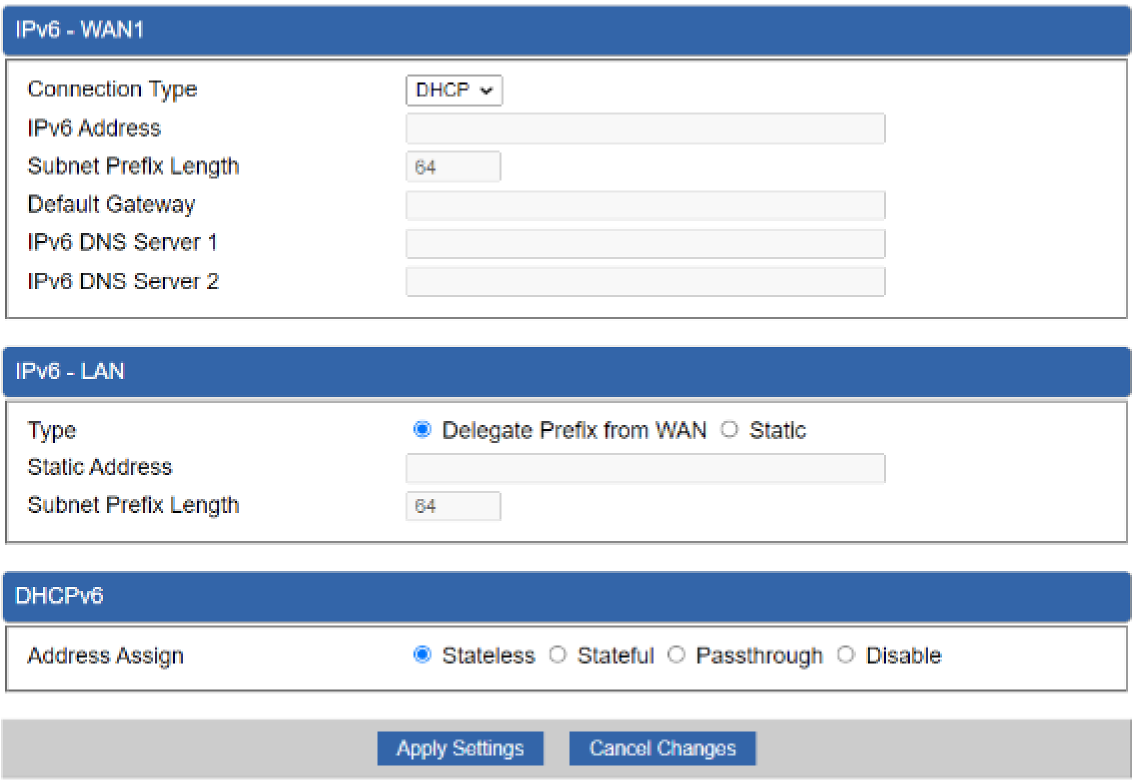
IGMP Versions Auto

Figure 4-35: IGMP

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

4.2.11 IPv6

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



IPv6 - WAN1

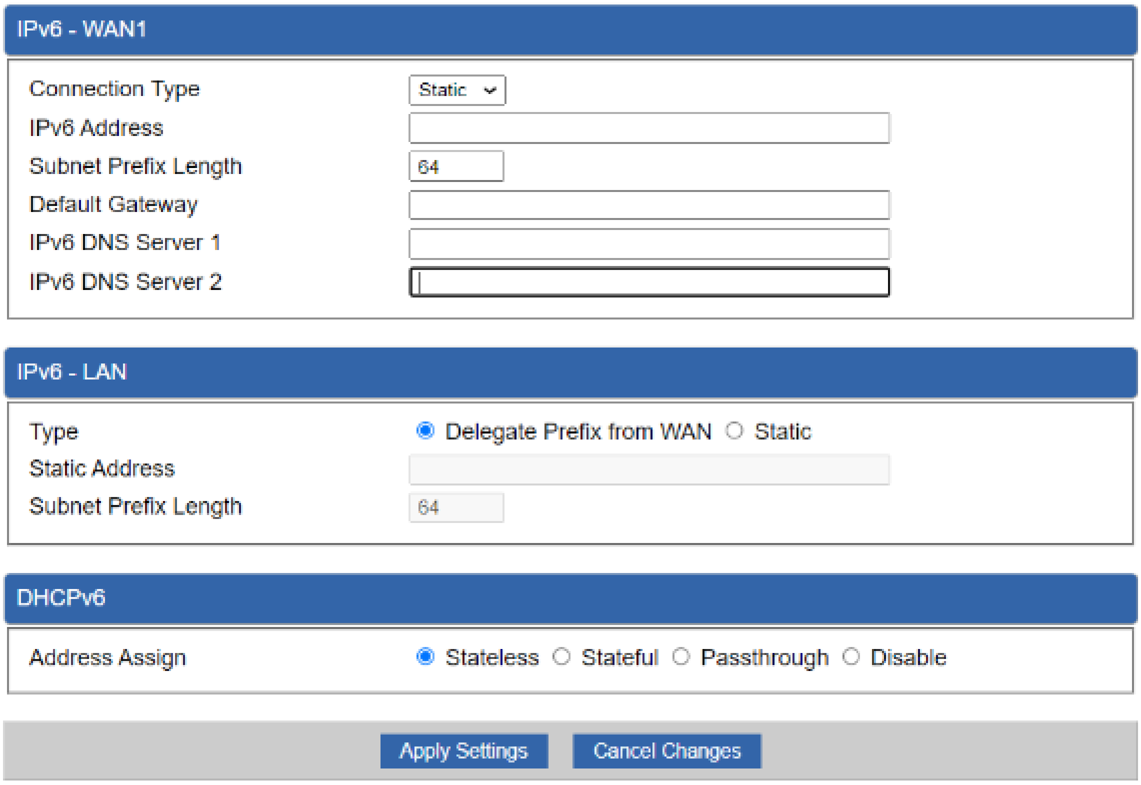
Connection Type	DHCP
IPv6 Address	
Subnet Prefix Length	64
Default Gateway	
IPv6 DNS Server 1	
IPv6 DNS Server 2	

IPv6 - LAN

Type	● Delegate Prefix from WAN ○ Static
Static Address	
Subnet Prefix Length	64

DHCPv6

Address Assign	● Stateless ○ Stateful ○ Passthrough ○ Disable



IPv6 - WAN1

Connection Type	Static
IPv6 Address	
Subnet Prefix Length	64
Default Gateway	
IPv6 DNS Server 1	
IPv6 DNS Server 2	

IPv6 - LAN

Type	● Delegate Prefix from WAN ○ Static
Static Address	
Subnet Prefix Length	64

DHCPv6

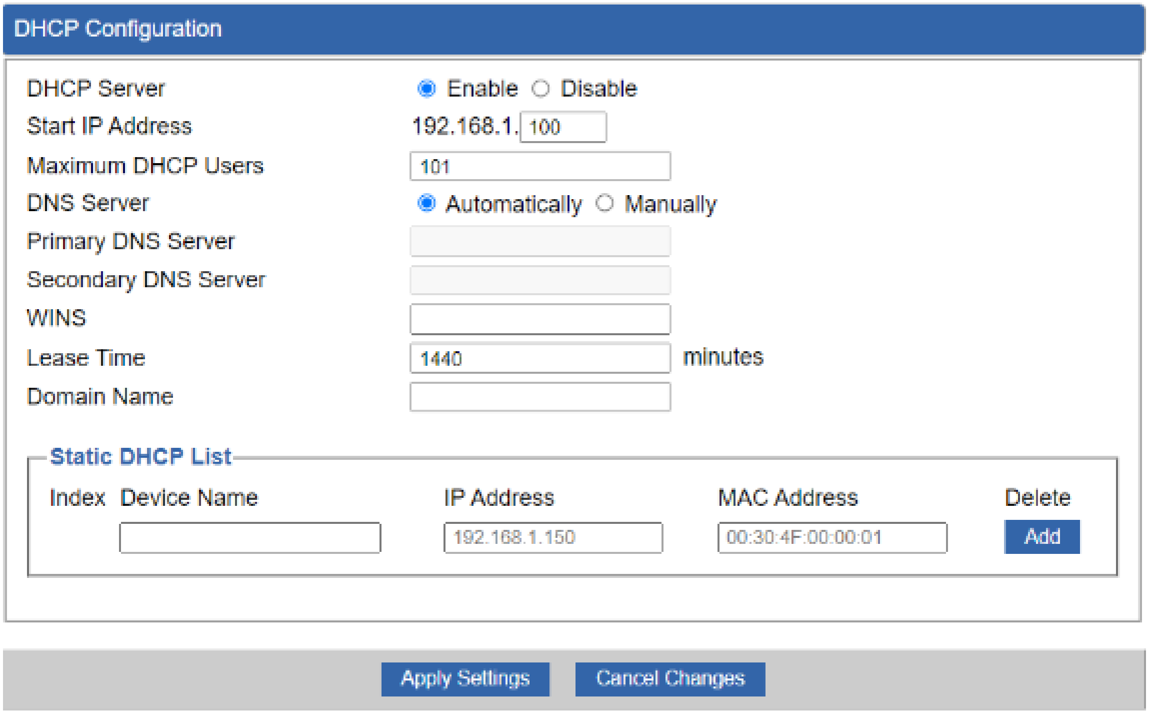
Address Assign	● Stateless ○ Stateful ○ Passthrough ○ Disable

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.

4.2.12 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.



DHCP Configuration

DHCP Server ● Enable ○ Disable
Start IP Address 192.168.1. 100
Maximum DHCP Users 101
DNS Server ● Automatically ○ Manually
Primary DNS Server
Secondary DNS Server
WINS
Lease Time 1440 minutes
Domain Name

Static DHCP List

Index	Device Name	IP Address	MAC Address	Delete
		192.168.1.150	00:30:4F:00:00:01	Add

Figure 4-37: DHCP

Object	Description
DHCP Service	By default, the DHCP Server is enabled, meaning the Industrial 802.11be 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 802.11be Wireless AP.
Maximum DHCP Users	By default, the maximum DHCP users are 101, meaning the Industrial 802.11be 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 802.11be 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 802.11be Wireless AP. Default is 1440 minutes.
Domain Name	Input a domain name for the Industrial 802.11be Wireless AP.

4.2.13 DDNS

The Industrial 802.11be 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 (**https://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.

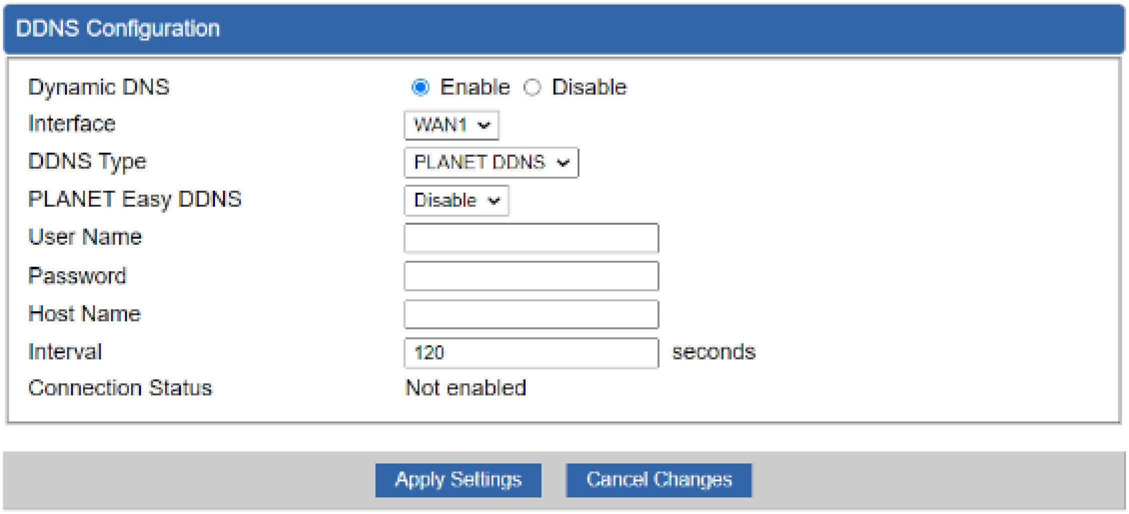
PLANET DDNS

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 (https://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 802.11be Wireless AP, and check the DDNS menu and just enable it. You don’t need to go to https://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 802.11be Wireless AP’s MAC address is A8-F7-E0-81-96-C9, it will be converted into pt8196c9.planetddns.com)



DDNS Configuration

Dynamic DNS	● Enable ○ Disable
Interface	WAN1
DDNS Type	PLANET DDNS
PLANET Easy DDNS	Disable
User Name	
Password	
Host Name	
Interval	120 seconds
Connection Status	Not enabled

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 https://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.
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.

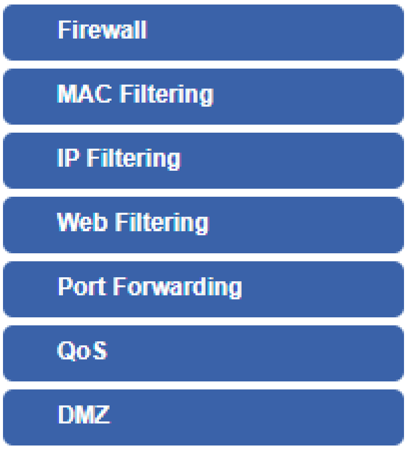
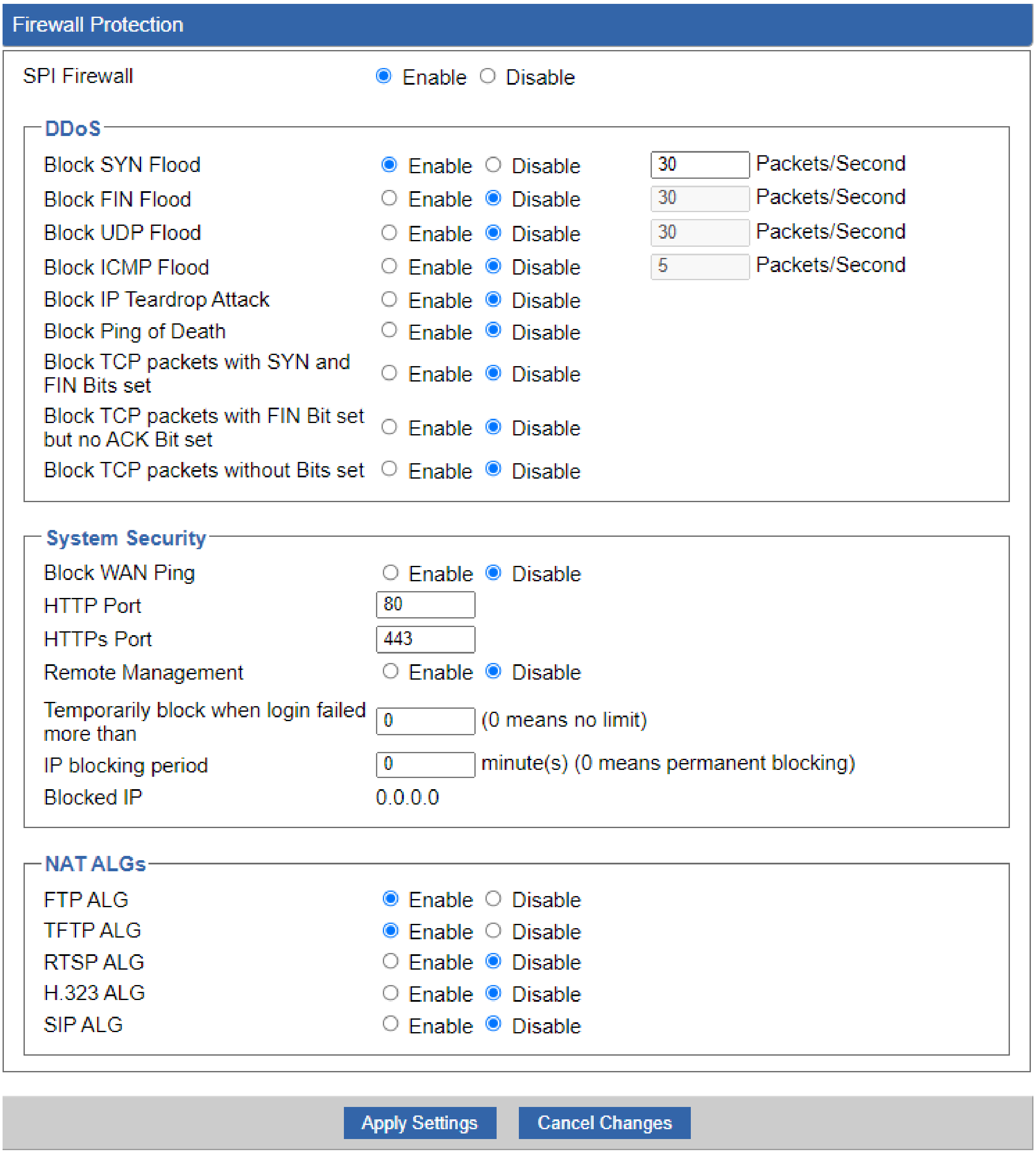


Figure 4-39: Security menu

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 802.11be Wireless AP can prevent specific DoS attacks as shown in Figure 4-40.



Firewall Protection

SPI Firewall	● Enable ○ Disable	

DDoS

Block SYN Flood	● Enable ○ Disable	30 Packets/Second
Block FIN Flood	○ Enable ● Disable	30 Packets/Second
Block UDP Flood	○ Enable ● Disable	30 Packets/Second
Block ICMP Flood	○ Enable ● Disable	5 Packets/Second
Block IP Teardrop Attack	○ Enable ● Disable	
Block Ping of Death	○ Enable ● Disable	
Block TCP packets with SYN and FIN Bits set	○ Enable ● Disable	
Block TCP packets with FIN Bit set but no ACK Bit set	○ Enable ● Disable	
Block TCP packets without Bits set	○ Enable ● Disable	

System Security

Block WAN Ping	○ Enable ● Disable
HTTP Port	80
HTTPs Port	443
Remote Management	○ Enable ● Disable
Temporarily block when login failed more than	0 (0 means no limit)
IP blocking period	0 minute(s) (0 means permanent blocking)
Blocked IP	0.0.0.0

NAT ALGs

FTP ALG	● Enable ○ Disable
TFTP ALG	● Enable ○ Disable
RTSP ALG	○ Enable ● Disable
H.323 ALG	○ Enable ● Disable
SIP ALG	○ Enable ● Disable

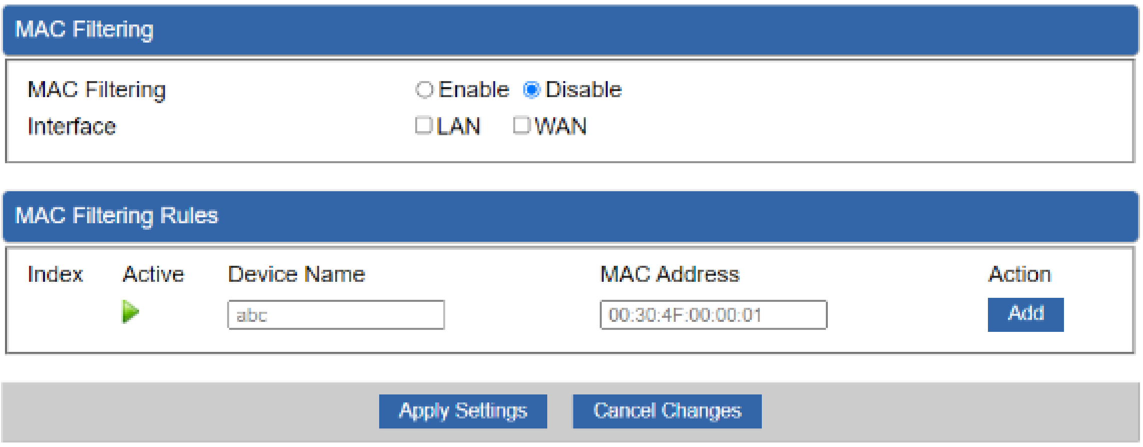
Figure 4-40: Firewall

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 802.11be 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 802.11be 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 Tear Drop	If the function is enabled, the Industrial 802.11be 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 802.11be 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 802.11be 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 802.11be Wireless AP. Use of such filters can be helpful in securing or restricting your local network as shown in Figure 4-41.



MAC Filtering

MAC Filtering ○ Enable ● Disable

Interface □ LAN □ WAN

MAC Filtering Rules

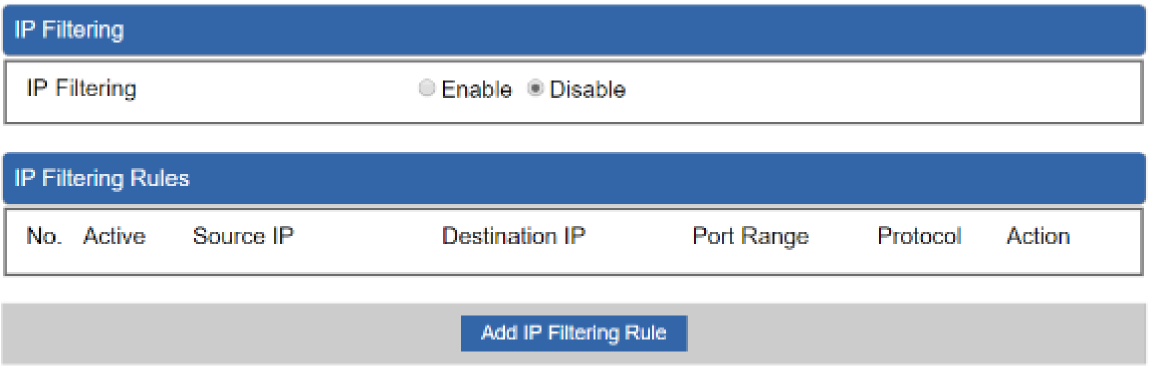
Index	Active	Device Name	MAC Address	Action
	▶	abc	00:30:4F:00:00:01	Add

Figure 4-41: MAC Filtering

Object	Description
Enable MAC Filtering	Set the function as enable or disable. When the function is enabled, the Industrial 802.11be 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.

4.3.3 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.



IP Filtering

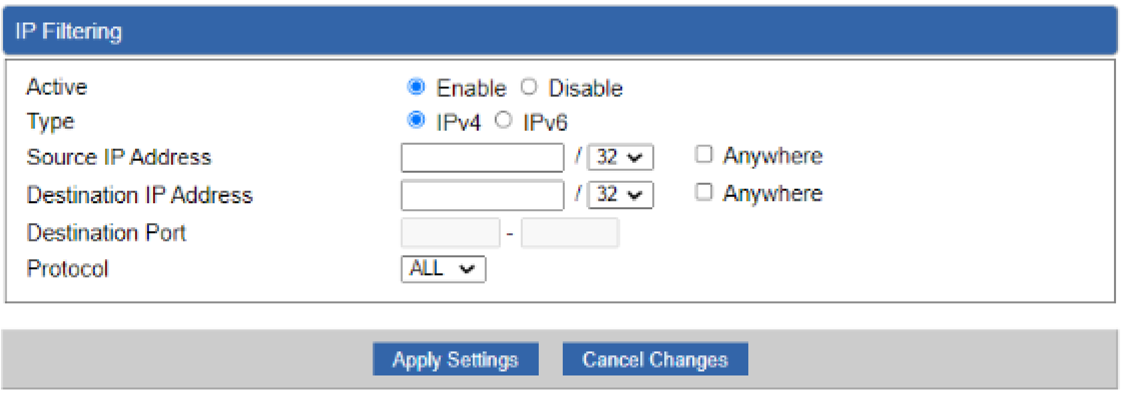
IP Filtering ○ Enable ● Disable

IP Filtering Rules

No.	Active	Source IP	Destination IP	Port Range	Protocol	Action

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.



IP Filtering

Active ● Enable ○ Disable

Type ● IPv4 ○ IPv6

Source IP Address [ ] / 32 □ Anywhere

Destination IP Address [ ] / 32 □ Anywhere

Destination Port [ ] - [ ]

Protocol ALL

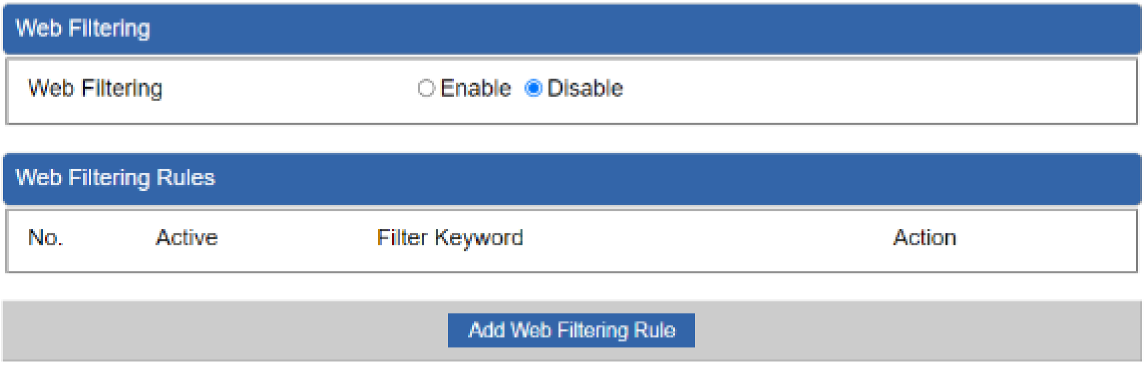
Figure 4-43: IP Filter Rule Setting

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	Check the box if you want to control all LAN users.

Object	Description
Address)	
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.



Web Filtering

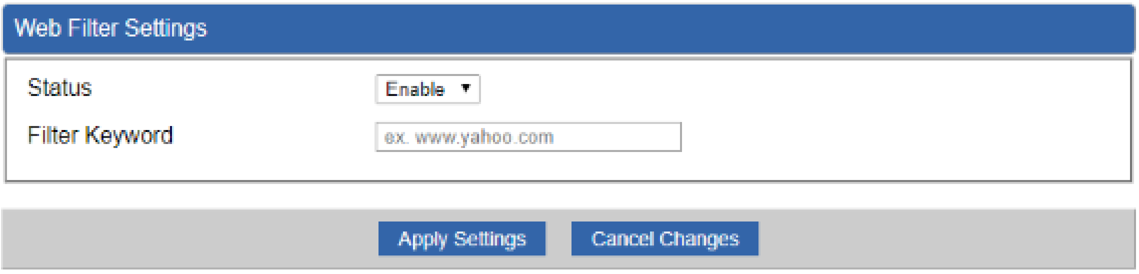
Web Filtering ○ Enable ● Disable

Web Filtering Rules

No.	Active	Filter Keyword	Action

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.



Web Filter Settings

Status: Enable

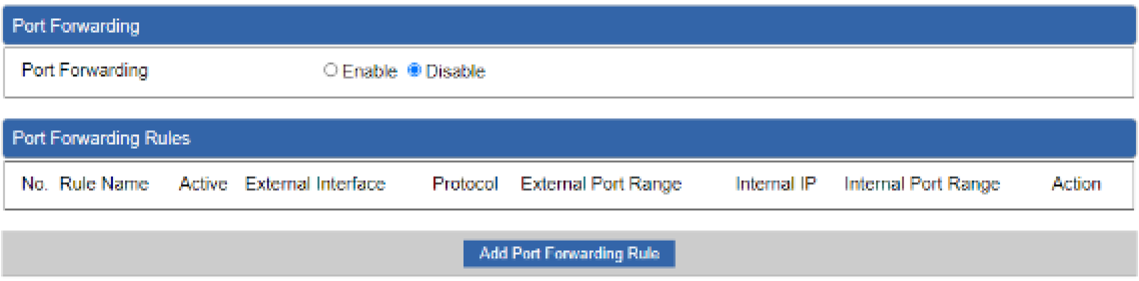
Filter Keyword: ex. www.yahoo.com

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 802.11be Wireless AP's NAT firewall.



Port Forwarding

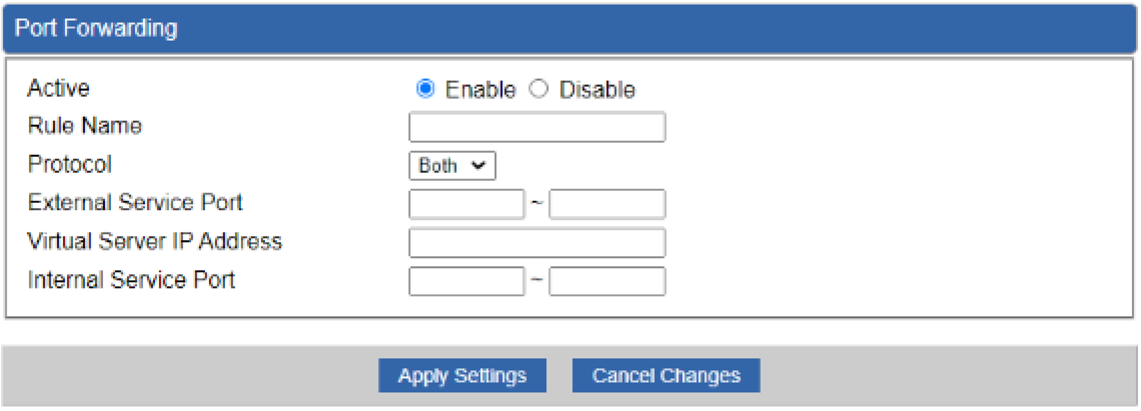
Port Forwarding ○ Enable ● Disable

Port Forwarding Rules

No.	Rule Name	Active	External Interface	Protocol	External Port Range	Internal IP	Internal Port Range	Action

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.



Port Forwarding

Active ● Enable ○ Disable

Rule Name

Protocol Both

External Service Port ~

Virtual Server IP Address

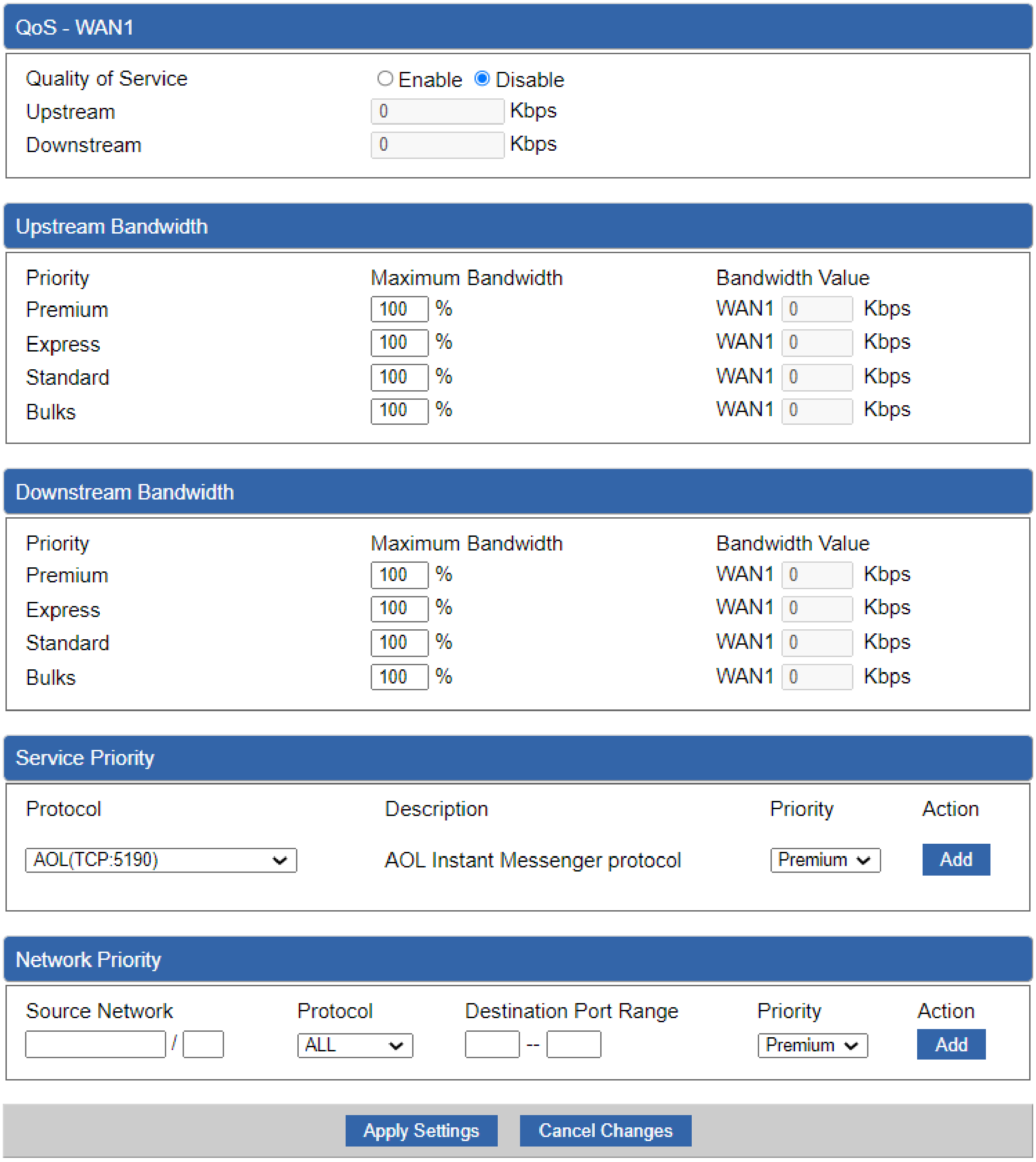
Internal Service Port ~

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

Object	Description
	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.
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



QoS - WAN1

Quality of Service	○ Enable ● Disable
Upstream	0 Kbps
Downstream	0 Kbps

Upstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	100 %	WAN1 0 Kbps
Express	100 %	WAN1 0 Kbps
Standard	100 %	WAN1 0 Kbps
Bulks	100 %	WAN1 0 Kbps

Downstream Bandwidth

Priority	Maximum Bandwidth	Bandwidth Value
Premium	100 %	WAN1 0 Kbps
Express	100 %	WAN1 0 Kbps
Standard	100 %	WAN1 0 Kbps
Bulks	100 %	WAN1 0 Kbps

Service Priority

Protocol	Description	Priority	Action
AOL(TCP:5190)	AOL Instant Messenger protocol	Premium	Add

Network Priority

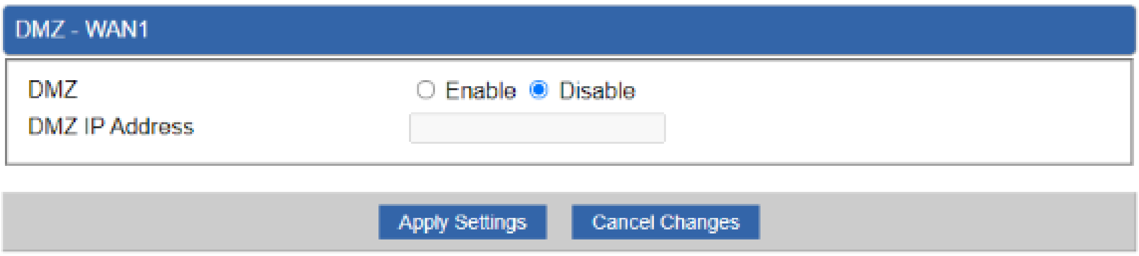
Source Network	Protocol	Destination Port Range	Priority	Action
/	ALL	--	Premium	Add

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.



DMZ - WAN1

DMZ ○ Enable ● Disable

DMZ IP Address

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

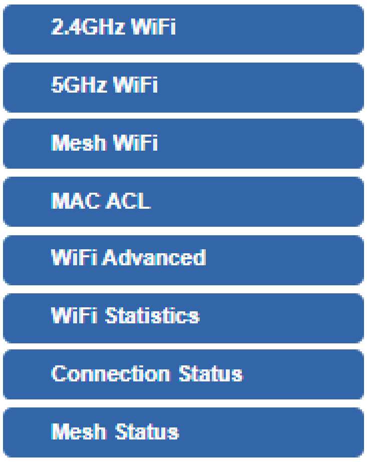
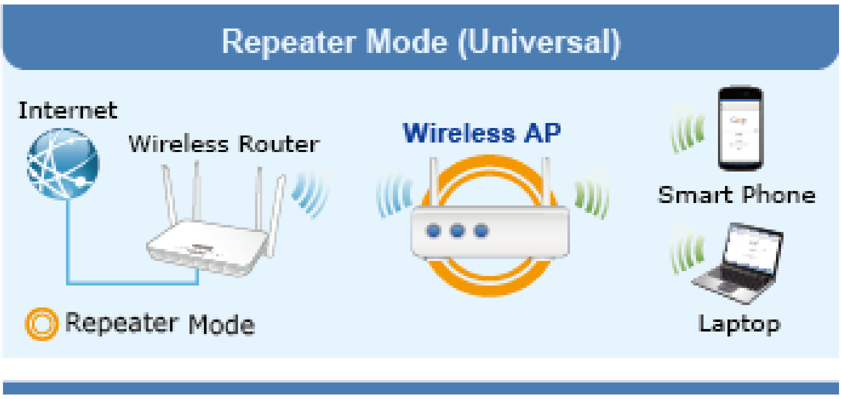


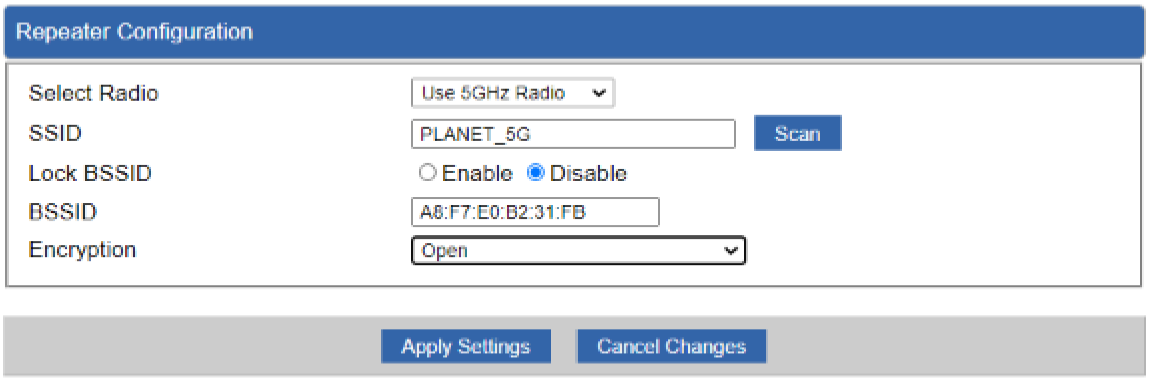
Figure 4-50: Wireless Menu

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


Repeater Configuration

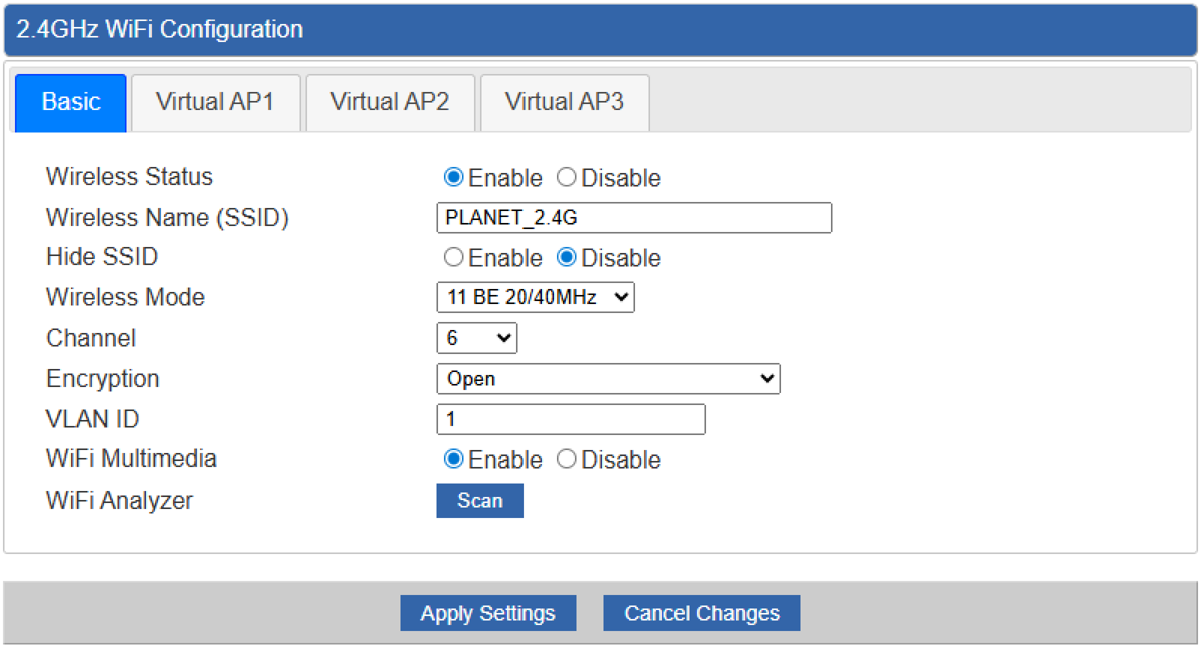
Select Radio	Use 5GHz Radio
SSID	PLANET_5G
Lock BSSID	○ Enable ● Disable
BSSID	A8:F7:E0:B2:31:FB
Encryption	Open

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.



2.4GHz WiFi Configuration

Wireless Status ● Enable ○ Disable

Wireless Name (SSID) PLANET_2.4G

Hide SSID ○ Enable ● Disable

Wireless Mode 11 BE 20/40MHz

Channel 6

Encryption Open

VLAN ID 1

WiFi Multimedia ● Enable ○ Disable

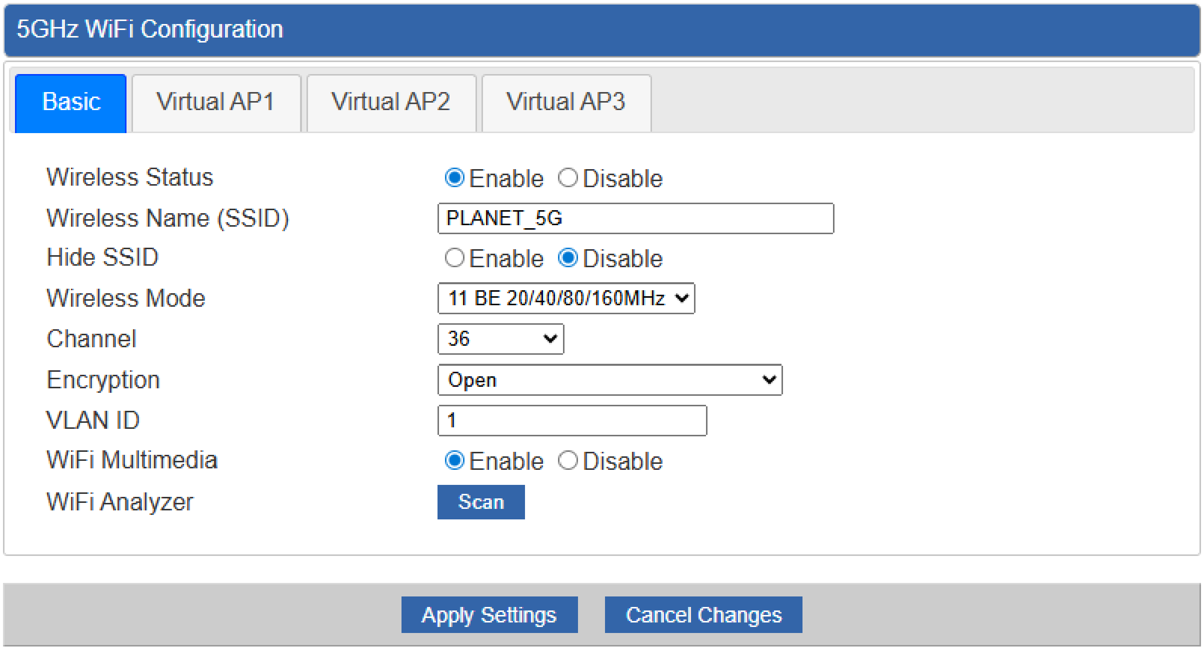
WiFi Analyzer Scan

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.



Wireless Status ● Enable ○ Disable

Wireless Name (SSID) PLANET_5G

Hide SSID ○ Enable ● Disable

Wireless Mode 11 BE 20/40/80/160MHz

Channel 36

Encryption Open

VLAN ID 1

WiFi Multimedia ● Enable ○ Disable

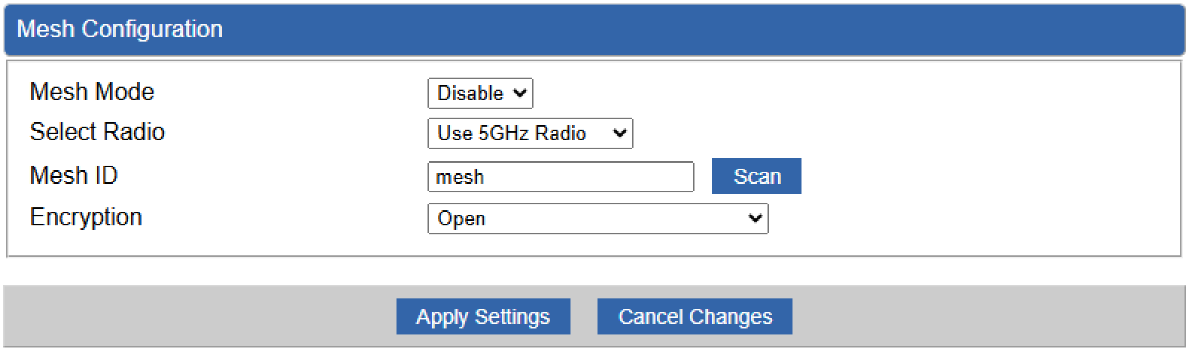
WiFi Analyzer

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 Mesh WiFi

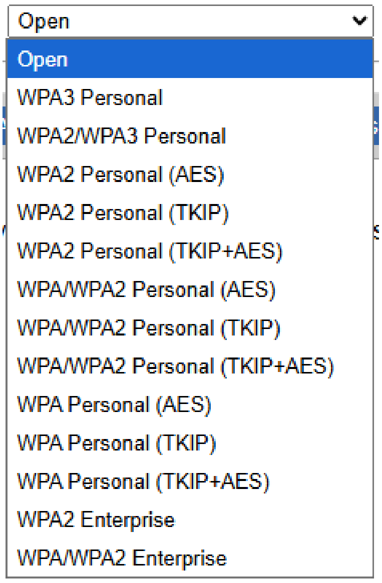
This page allows the user to define Mesh WiFi.



Mesh Configuration

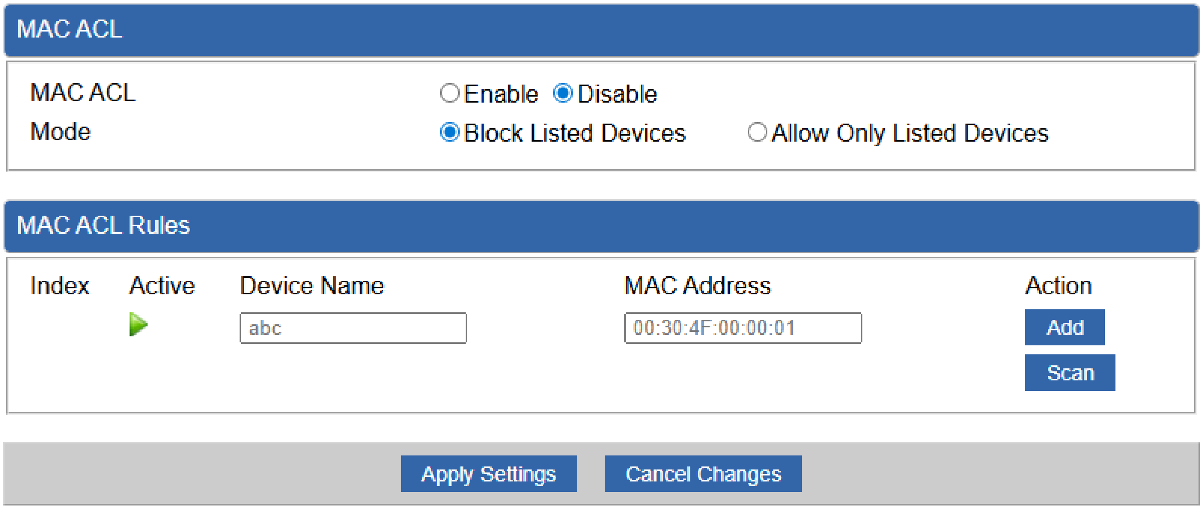
Mesh Mode	Disable
Select Radio	Use 5GHz Radio
Mesh ID	mesh
Encryption	Open

Note: For Mesh to work properly, all devices in the Mesh network must use the same Mesh ID, security key, and wireless channel.

Object	Description
Mesh Mode	Select the Mesh Mode.
Select Radio	Select the Select Radio, default is Use 5GHz Radio.
Mesh ID	Scan the Mesh ID.
Encryption	Select the Encryption.  Open Open 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) WPA Personal (AES) WPA Personal (TKIP) WPA Personal (TKIP+AES) WPA2 Enterprise WPA/WPA2 Enterprise

4.4.5 MAC ACL

This page allows the user to define MAC ACL.



MAC ACL

MAC ACL ○ Enable ● Disable

Mode ● Block Listed Devices ○ Allow Only Listed Devices

MAC ACL Rules

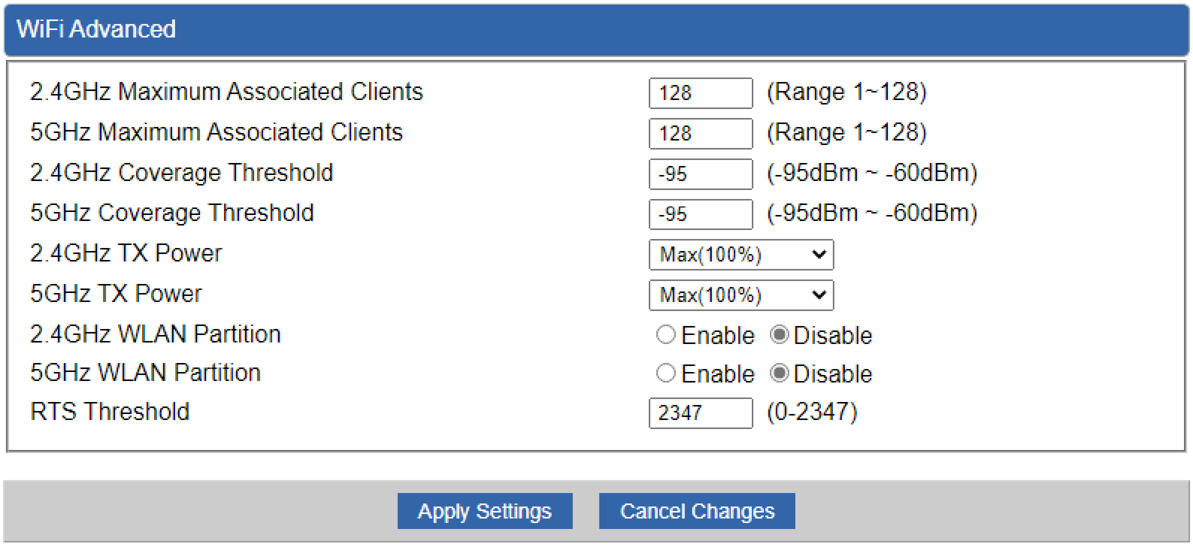
Index	Active	Device Name	MAC Address	Action
	▶	abc	00:30:4F:00:00:01	Add Scan

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.

4.4.6 Wi-Fi Advanced

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



WiFi Advanced

2.4GHz Maximum Associated Clients	128 (Range 1~128)
5GHz Maximum Associated Clients	128 (Range 1~128)
2.4GHz Coverage Threshold	-95 (-95dBm ~ -60dBm)
5GHz Coverage Threshold	-95 (-95dBm ~ -60dBm)
2.4GHz TX Power	Max(100%)
5GHz TX Power	Max(100%)
2.4GHz WLAN Partition	○ Enable ● Disable
5GHz WLAN Partition	○ Enable ● Disable
RTS Threshold	2347 (0-2347)

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**.

4.4.7 Wi-Fi Statistics

This page shows the statistics of Wi-Fi traffic.

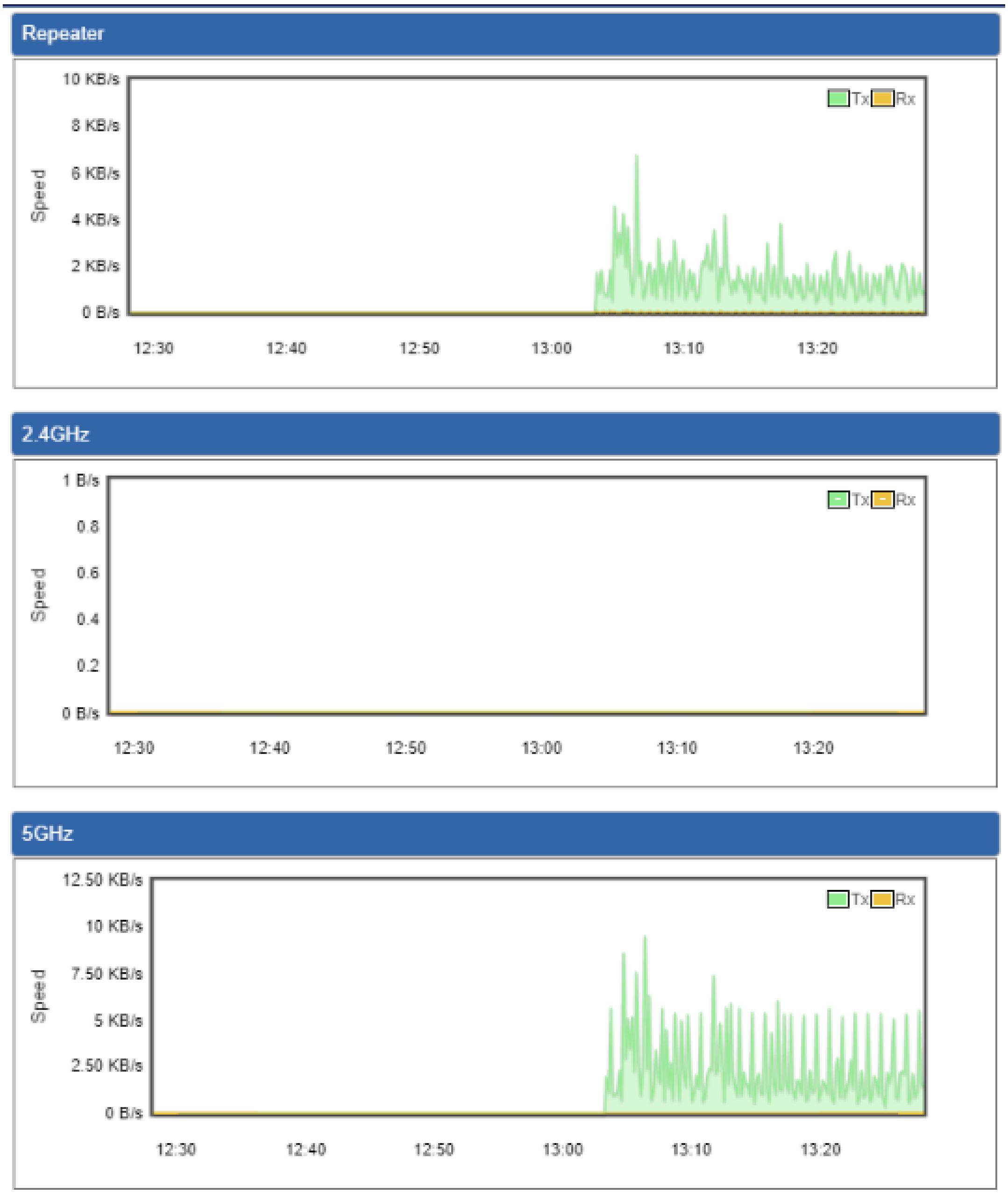
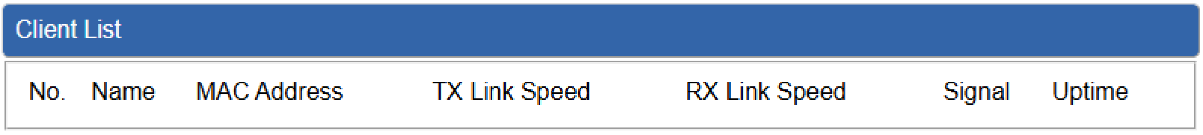


Figure 4-56: Wi-Fi Statistics

4.4.8 Connection Status

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



Client List

No.	Name	MAC Address	TX Link Speed	RX Link Speed	Signal	Uptime

Figure 4-57: Connection Status

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

4.5 PoE

(For IAP-3600BE-4PF Only)

The PoE menu provides the following features for managing the system.

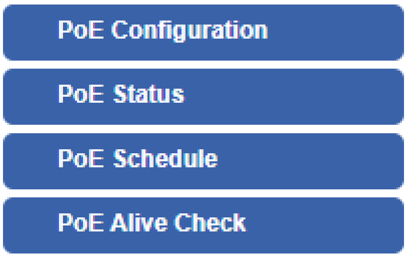
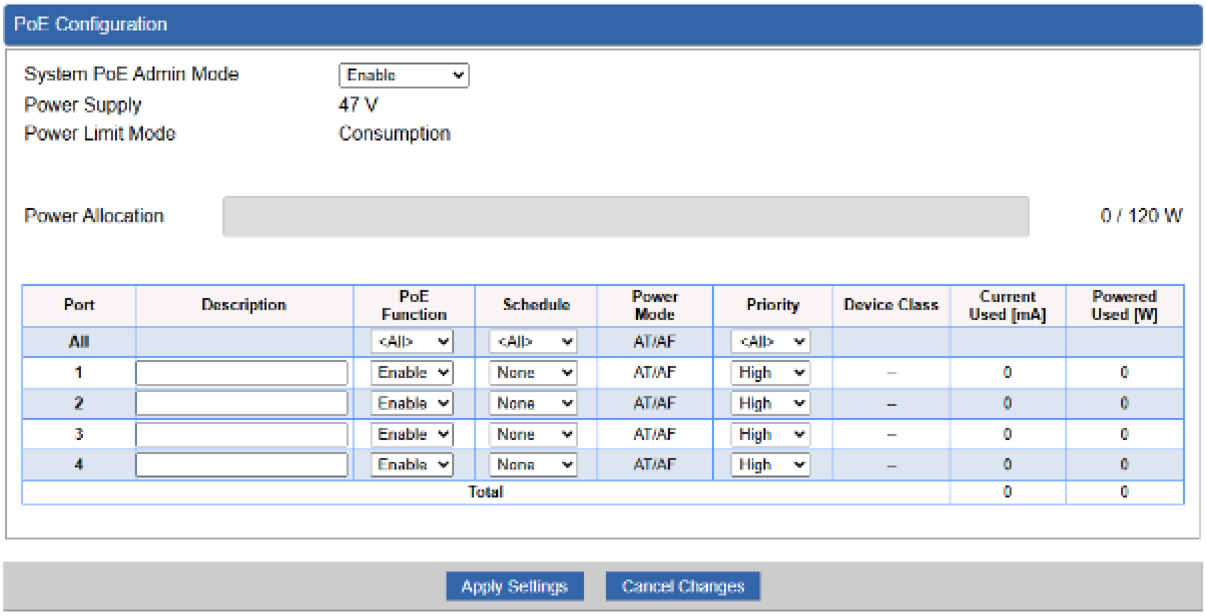


Figure 4.5-1 PoE Menu

Object	Description
PoE Configuration	Allows to centralize management of PoE power for PDs.
PoE Status	Displays the current PoE usage.
PoE Schedule	Allows centralizing management of PoE power for providing schedule.
PD Alive Check	Allows centralizing management of PoE power for checking PDs alive.

4.5.1 PoE Configuration

This section allows the user to inspect and configure the current PoE configuration setting.



PoE Configuration

System PoE Admin Mode	Enable
Power Supply	47 V
Power Limit Mode	Consumption

Power Allocation 0 / 120 W

Port	Description	PoE Function	Schedule	Power Mode	Priority	Device Class	Current Used [mA]	Powered Used [W]
All		<All>	<All>	AT/AF	<All>			
1		Enable	None	AT/AF	High	–	0	0
2		Enable	None	AT/AF	High	–	0	0
3		Enable	None	AT/AF	High	–	0	0
4		Enable	None	AT/AF	High	–	0	0
Total							0	0

Figure 4.5-2 PoE configuration

Object	Description
• **System PoE Admin Mode**	Allows user to enable or disable PoE function. It will cause all of PoE ports to supply or not to supply power.
• **PoE Function**	There are three modes for PoE mode. ■ **Enable**: enable PoE function.. ■ **Disable**: disable PoE function. ■ **Schedule: enable PoE function in schedule mode.**
• **Schedule**	Indicates the scheduled profile mode. Possible profiles are: ■ **Profile1** ■ **Profile2** ■ **Profile3** ■ **Profile4**
• **Priority**	The Priority represents PoE ports priority. There are three levels of power priority named **Low**, **High** and **Critical**. The priority is used in case the total power consumption is over the total power budget. In this case, the port with the lowest priority will be turned off, and power for the port of higher priority will be offered.
• **Device Class**	Displays the class of the PD attached to the port, as established by

	the classification process. Class 0 is the default for PDs. The PD is powered based on PoE Class level if the system is working in Classification mode. The PD will return to Class 0 to 4 in accordance with the maximum power
• **Current Used [mA]**	The **Power Used** shows how much current the PD currently is using.
• **Powered Used [W]**	The **Power Used** shows how much power the PD currently is using.

4.5.2 PoE Status

This section provides per port PoE status.

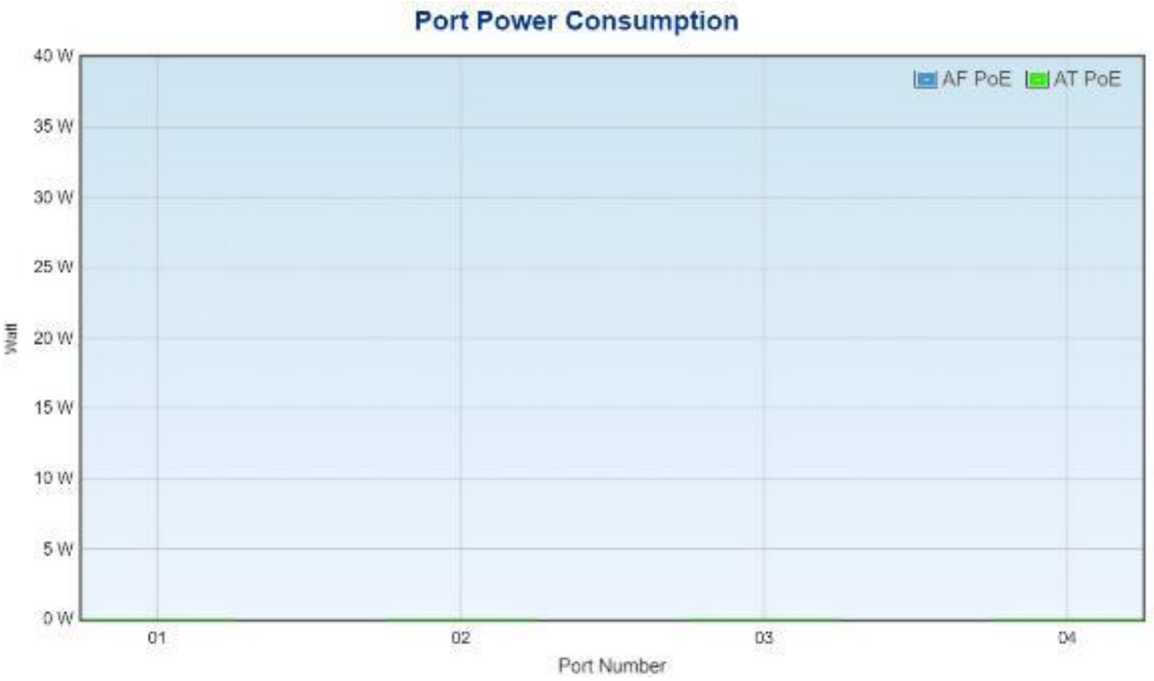
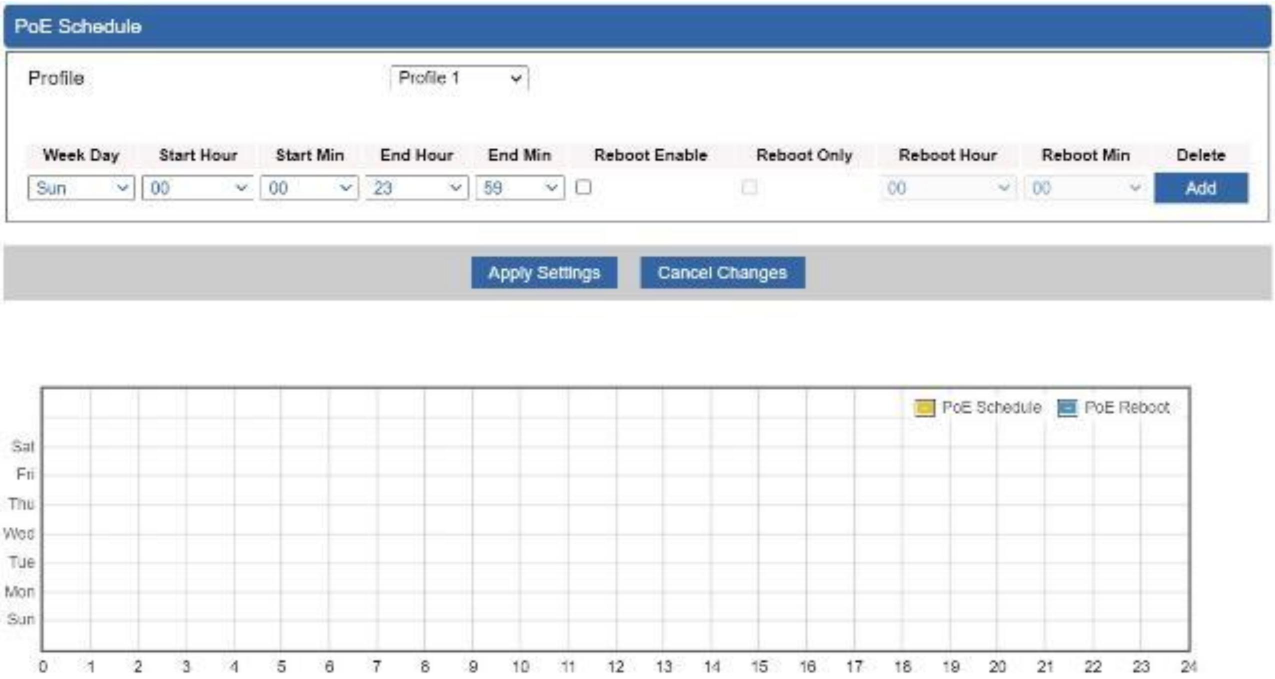


Figure 4.5-3 Port Power Consumption

4.5.3 PoE Schedule

This page allows the user to define PoE schedule and scheduled power recycling.

Please press the **Add New Rule** button to start setting PoE Schedule function. You have to set PoE schedule to profile and then go back to PoE Port Configuration, and select “**Schedule**” mode from per port “**PoE Mode**” option to enable you to indicate which schedule profile could be applied to the PoE port.



PoE Schedule

Profile: Profile 1

Week Day	Start Hour	Start Min	End Hour	End Min	Reboot Enable	Reboot Only	Reboot Hour	Reboot Min	Delete
Sun	00	00	23	59	□	□	00	00	Add

Apply Settings | Cancel Changes

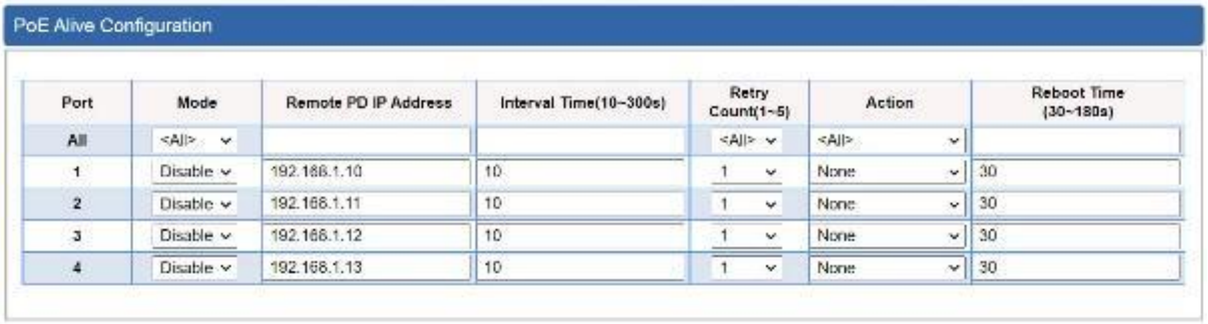
Figure 4.5-4 PoE schedule Configuration

Object	Description
• **Profile**	Set the schedule profile mode. Possible profiles are: **Profile1** **Profile2** **Profile3** **Profile4**
• **Week Day**	Allows user to set week day for defining PoE function by enabling it on the day.
• **Start Hour**	Allows user to set what hour PoE function does by enabling it.
• **Start Min**	Allows user to set what minute PoE function does by enabling it.
• **End Hour**	Allows user to set what hour PoE function does by disabling it.

• **End Min**	Allows user to set what minute PoE function does by disabling it.
• **Reboot Enable**	Allows user to enable or disable the whole PoE port reboot by PoE reboot schedule. Please note that if you want PoE schedule and PoE reboot schedule to work at the same time, please use this function, and don't use **Reboot Only** function. This function offers administrator to reboot PoE device at an indicated time if administrator has this kind of requirement.
• **Reboot Only**	Allows user to reboot PoE function by PoE reboot schedule. Please note that if administrator enables this function, PoE schedule will not set time to profile. This function is just for PoE port to reset at an indicated time.
• **Reboot Hour**	Allows user to set what hour PoE reboots. This function is only for PoE reboot schedule.
• **Reboot Min**	Allows user to set what minute PoE reboots. This function is only for PoE reboot schedule.

4.5.4 PD Alive Check

The VPN Router can be configured to monitor connected PD's status in real-time via ping action. Once the PD stops working and without response, the PoE Switch is going to restart PoE port power, and bring the PD back to work. It will greatly enhance the reliability and reduces administrator management burden.



PoE Alive Configuration

Port	Mode	Remote PD IP Address	Interval Time(10~300s)	Retry Count(1~5)	Action	Reboot Time (30~180s)
All	<All>			<All>	<All>	
1	Disable	192.168.1.10	10	1	None	30
2	Disable	192.168.1.11	10	1	None	30
3	Disable	192.168.1.12	10	1	None	30
4	Disable	192.168.1.13	10	1	None	30

Figure 4.5-5 PoE Alive Configuration

Object	Description
• **Mode**	Allows user to enable or disable per port PD Alive Check function. By default, all ports are disabled.
• **Remote PD IP Address**	This column allows user to set PoE device IP address for system making ping to the PoE device. Please note that the PD's IP address must be set to the same network segment with the PoE Switch.
• **Interval Time (10~300s)**	This column allows user to set how long system should issue a ping request to PD for detecting whether PD is alive or dead. Interval time range is from 10 seconds to 300 seconds.
• **Retry Count (1~5)**	This column allows user to set the number of times system retries ping to PD. For example, if we set count 2, it means that if system retries ping to the PD and the PD doesn't response continuously, the PoE port will be reset.
• **Action**	Allows user to set which action will be applied if the PD is without any response. The PoE Switch Series offers the following 3 actions: ■ **PD Reboot:** It means system will reset the PoE port that is connected to the PD. ■ **PD Reboot & Alarm:** It means system will reset the PoE port and issue an alarm message via Syslog. ■ **Alarm:** It means system will issue an alarm message via Syslog.
• **Reboot Time (30~180s)**	This column allows user to set the PoE device rebooting time as there are so many kinds of PoE devices on the market and they have a different rebooting time.

	The PD Alive-check is not a defining standard, so the PoE device on the market doesn’t report reboot done information to the PoE Switch. Thus, user has to make sure how long the PD will take to finish booting, and then set the time value to this column. System is going to check the PD again according to the reboot time. If you are not sure of the precise booting time, we suggest you set it longer.

4.6 Maintenance

The Maintenance menu provides the following features for managing the system

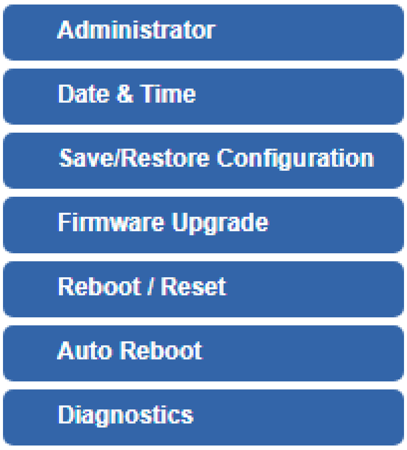
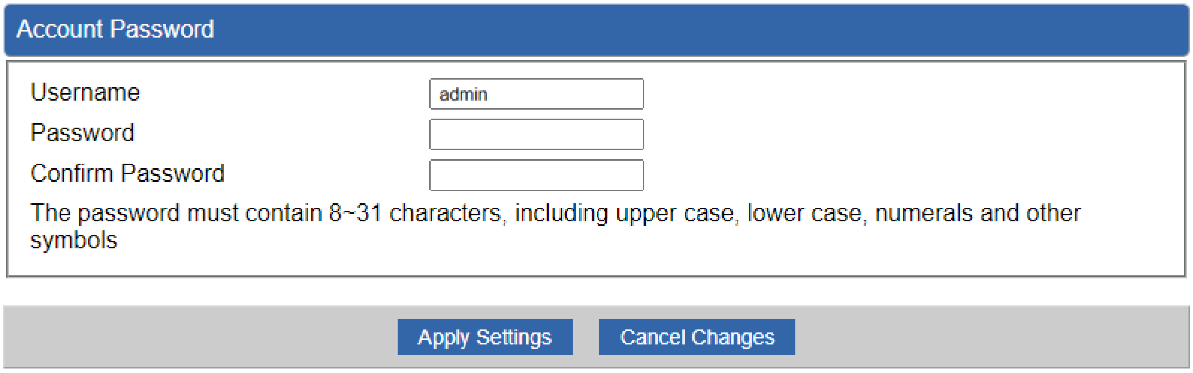


Figure 4-58: Maintenance

Object	Description
Administrator	Allows changing the login username and password.
Date & Time	Allows setting Date & Time function.
Save/Restore Configuration	Export the Industrial 802.11be Wireless AP's configuration to local or USB sticker. Restore the Industrial 802.11be 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.

4.6.1 Administrator

To ensure the Industrial 802.11be Wireless AP's security is secure, you will be asked for your password when you access the Industrial 802.11be 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.



Account Password

Username	admin
Password	
Confirm Password	

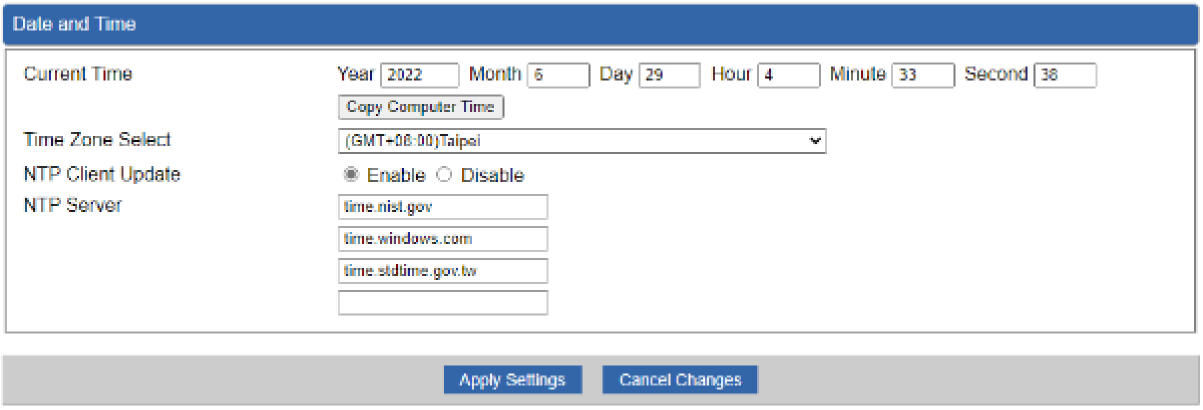
The password must contain 8~31 characters, including upper case, lower case, numerals and other symbols

Figure 4-59: Administrator

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

4.6.2 Date and Time

This section assists you in setting the system time of the Industrial 802.11be 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.



Date and Time

Current Time: Year 2022 Month 6 Day 29 Hour 4 Minute 33 Second 38

Time Zone Select: (GMT+08:00)Taipei

NTP Client Update: ● Enable ○ Disable

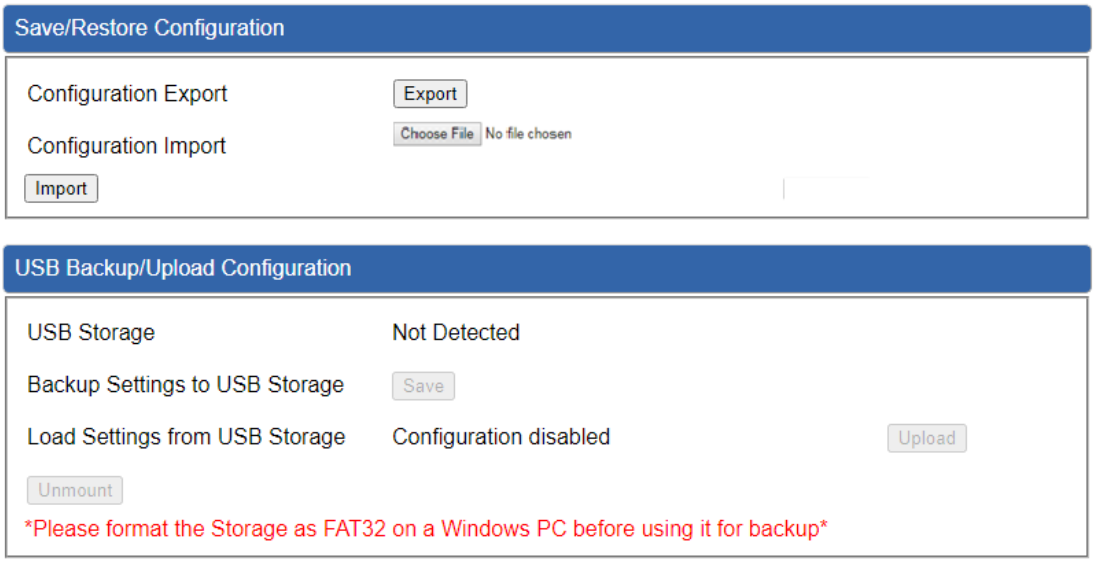
NTP Server: time.nist.gov
time.windows.com
time.stdtime.gov.tw

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 802.11be Wireless AP will set its time based on your selection.
NTP Client Update	Once this function is enabled, Industrial 802.11be Wireless AP will automatically update current time from NTP server.
NTP Server	User may use the default NTP sever or input NTP server manually.

4.6.3 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:



Save/Restore Configuration

Configuration Export: Export

Configuration Import: Choose File No file chosen

Import

USB Backup/Upload Configuration

USB Storage: Not Detected

Backup Settings to USB Storage: Save

Load Settings from USB Storage: Configuration disabled Upload

Unmount

Please format the Storage as FAT32 on a Windows PC before using it for backup

Figure 4-61: Save/Restore Configuration

- **Save Setting to PC**

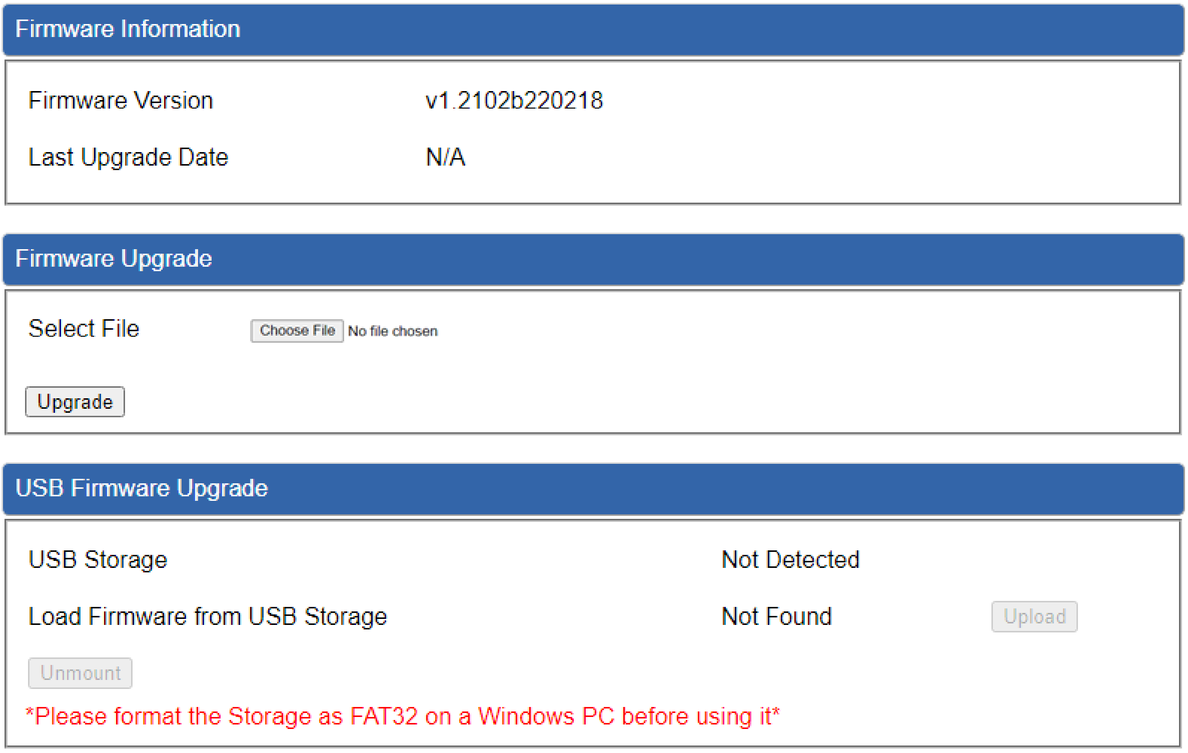
Object	Description
Configuration Export	Press the Export button to save setting file to PC.
Configuration Import	Press the Choose File button to select the setting file, and then press the Import button to upload setting file from PC.

- **Save Setting to USB Storage**

Object	Description
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.

4.6.4 Firmware Upgrading

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



Firmware Information

Firmware Version	v1.2102b220218
Last Upgrade Date	N/A

Firmware Upgrade

Select File [Choose File] No file chosen

[Upgrade]

USB Firmware Upgrade

USB Storage	Not Detected	
Load Firmware from USB Storage	Not Found	[Upload]

[Unmount]

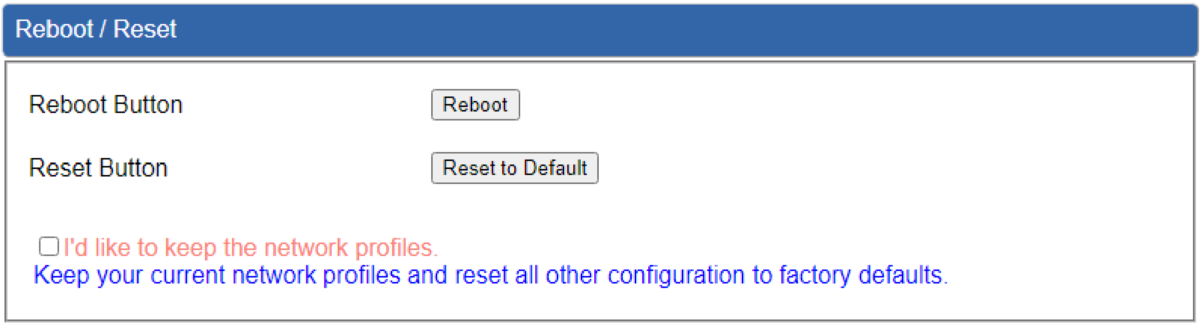
Please format the Storage as FAT32 on a Windows PC before using it

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.

4.6.5 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:



Reboot / Reset

Reboot Button Reboot

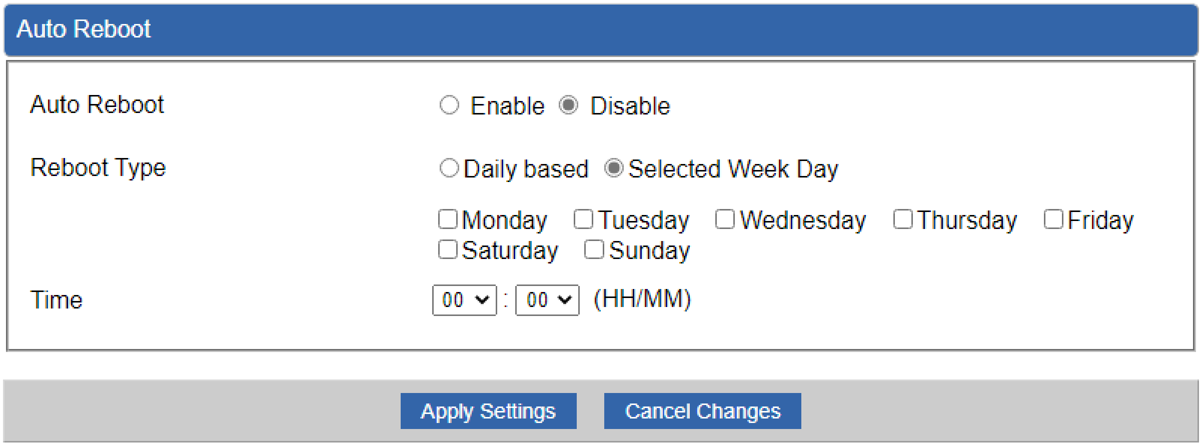
Reset Button Reset to Default

□ I'd like to keep the network profiles.
Keep your current network profiles and reset all other configuration to factory defaults.

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.

4.6.6 Auto Reboot



Auto Reboot

Auto Reboot ○ Enable ● Disable

Reboot Type ○ Daily based ● Selected Week Day

□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

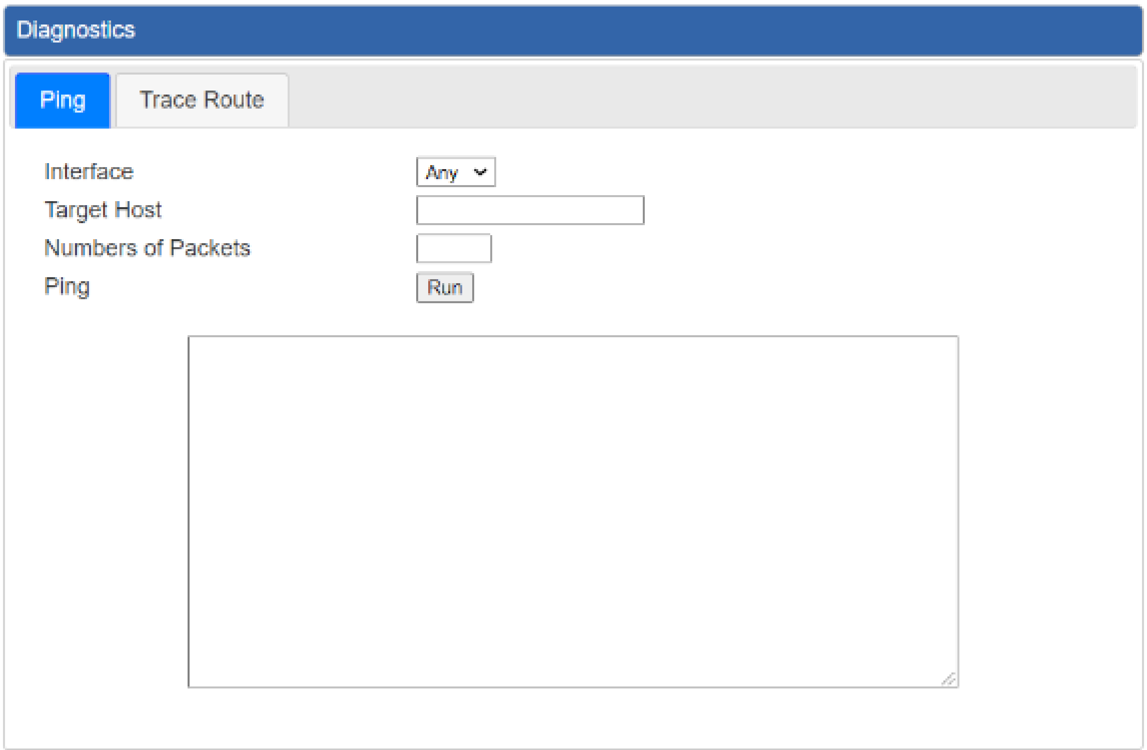
Time 00 : 00 (HH/MM)

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.

4.6.7 Diagnostics

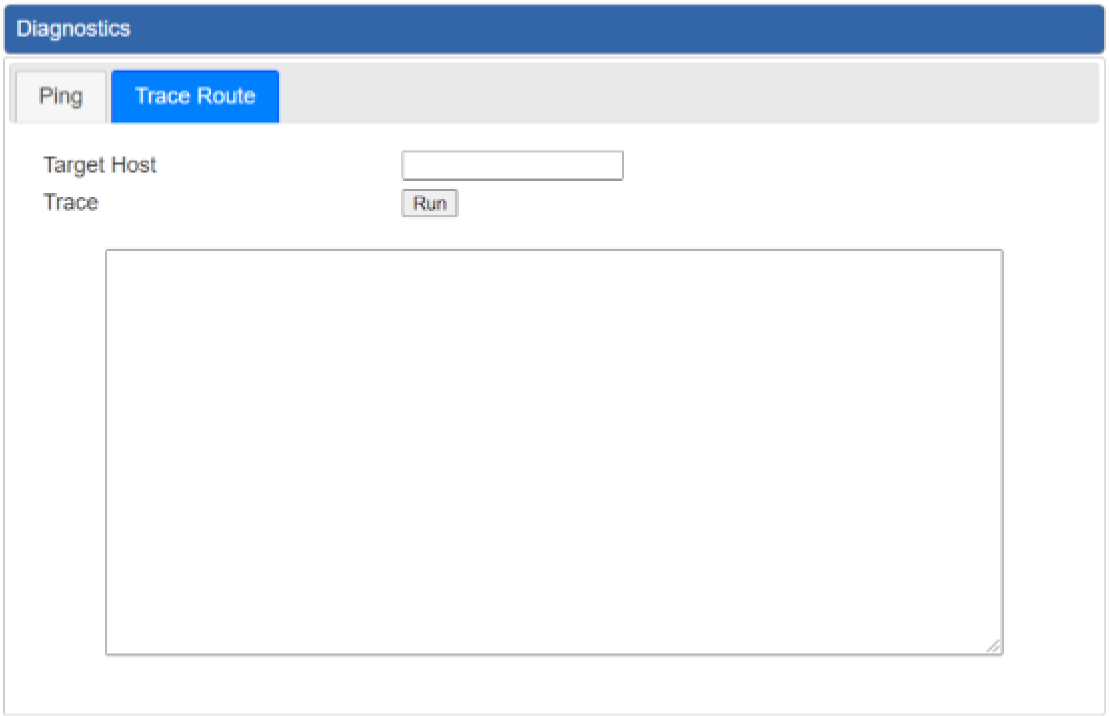
The page allows you to issue ICMP PING packets to troubleshoot IP connectivity issues. After you press “Ping”, ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The Page refreshes automatically until responses to all packets are received,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


Diagnostics

Interface: Any
Target Host:
Numbers of Packets:
Ping: Run

Figure 4-65: Ping

Object	Description
Interface	Select an interface of the Industrial 802.11be 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.



Diagnostics

Target Host

Trace Run

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 802.11be Wireless AP, or you must 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 802.11be Wireless AP is configured to “**default**”.

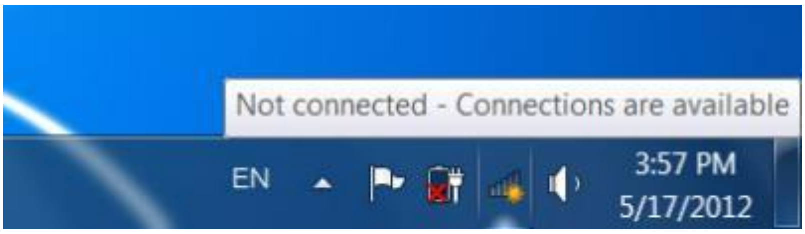
Note

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



Not connected - Connections are available

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

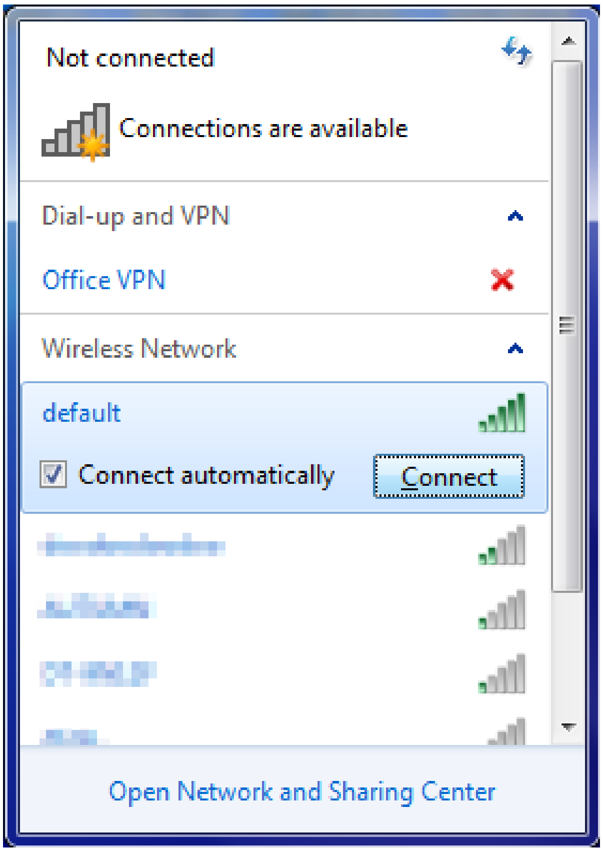


Figure 5-2: WLAN AutoConfig

Note

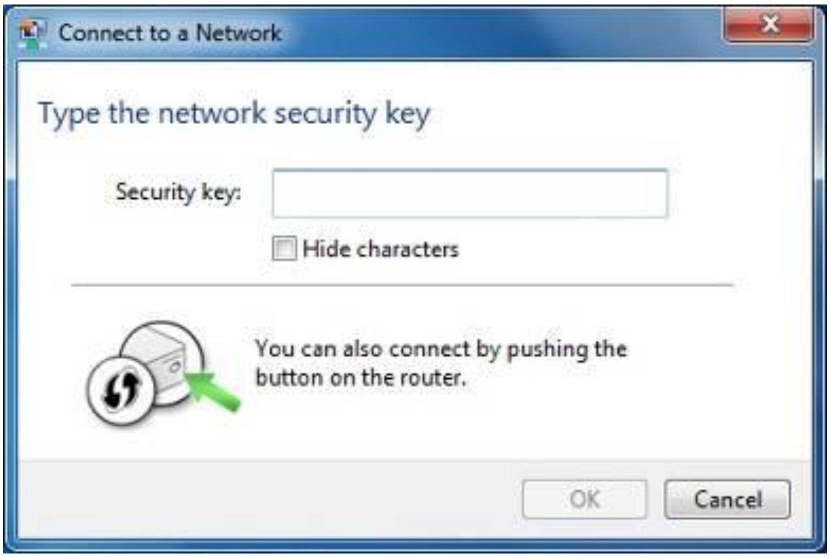
If you will be connecting to this Industrial 802.11be Wireless AP in the future, check [**Connect automatically**].

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

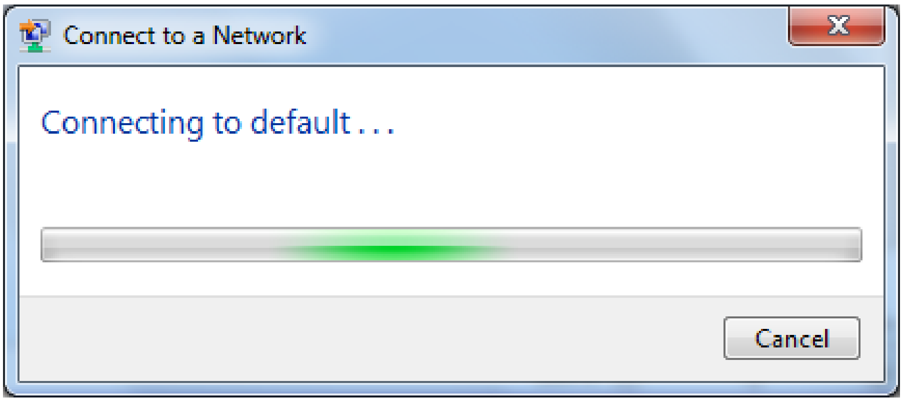
(3) Click the [OK] button.



Type the network security key

You can also connect by pushing the button on the router.

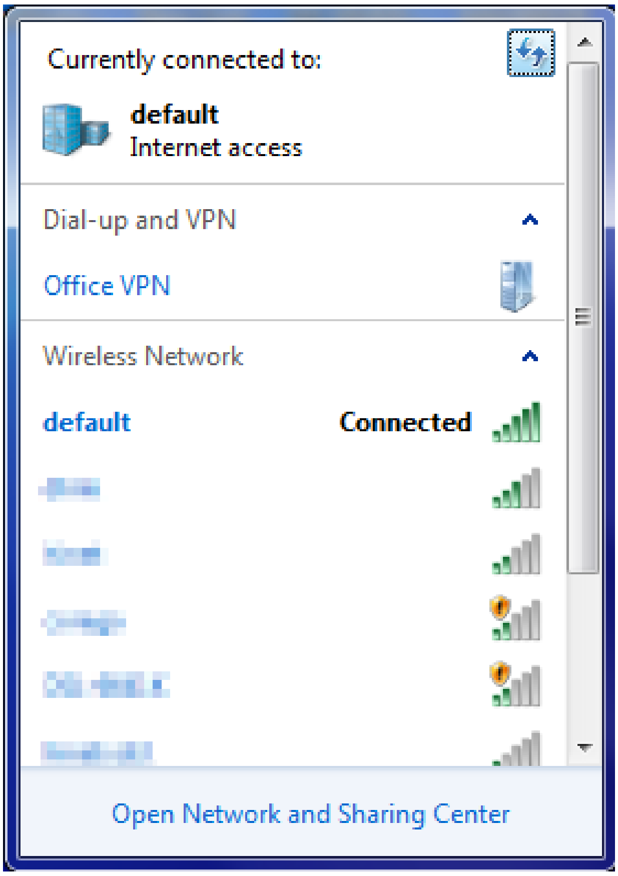
Figure 5-3: Typing the Network Key



Connecting to default . . .

Figure 5-4: Connecting to a Network

Step 5: Check if “**Connected**” is displayed.



Currently connected to:

default
Internet access

Dial-up and VPN

Office VPN

Wireless Network

default **Connected**

Open Network and Sharing Center

Figure 5-5: Connected to a Network

5.2 Mac OS X 10.x

In the following sections, the default SSID of the Industrial 802.11be 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.

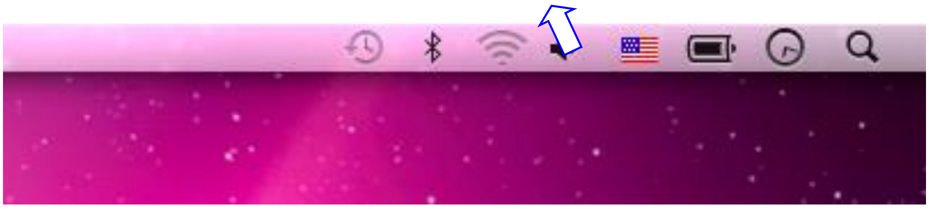
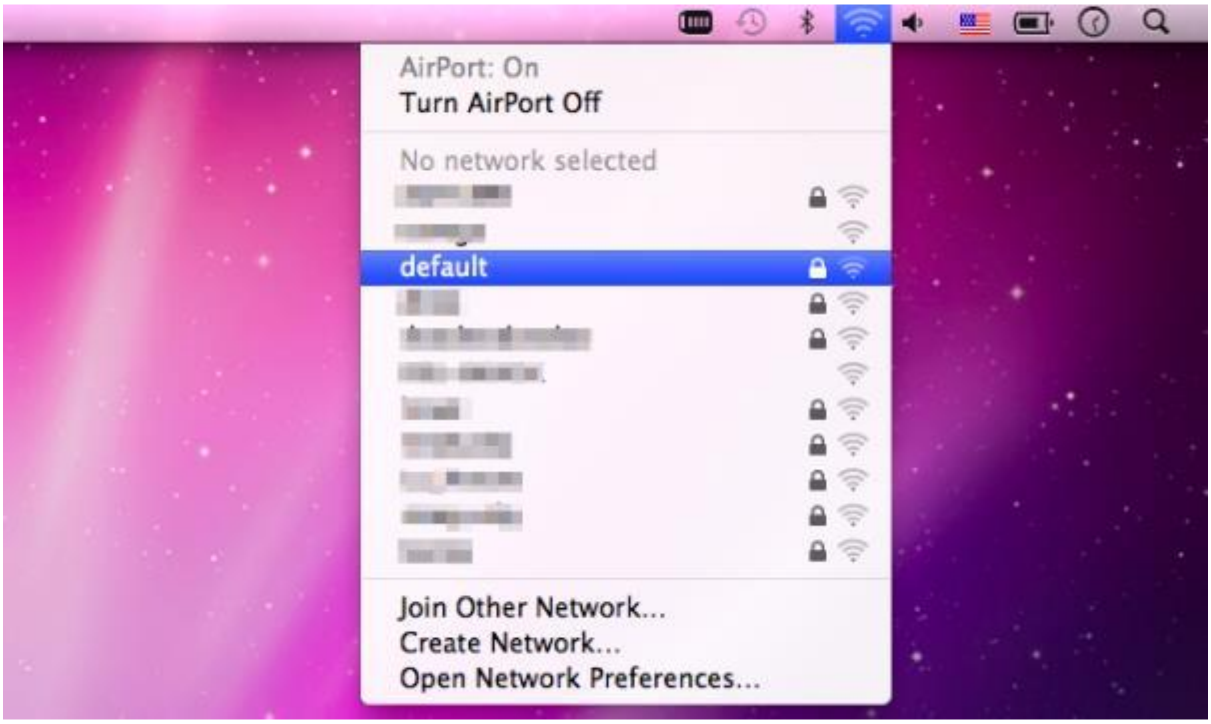


Figure 5-6: Mac OS – Network Icon

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

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

(2) Double-click on the selected SSID.



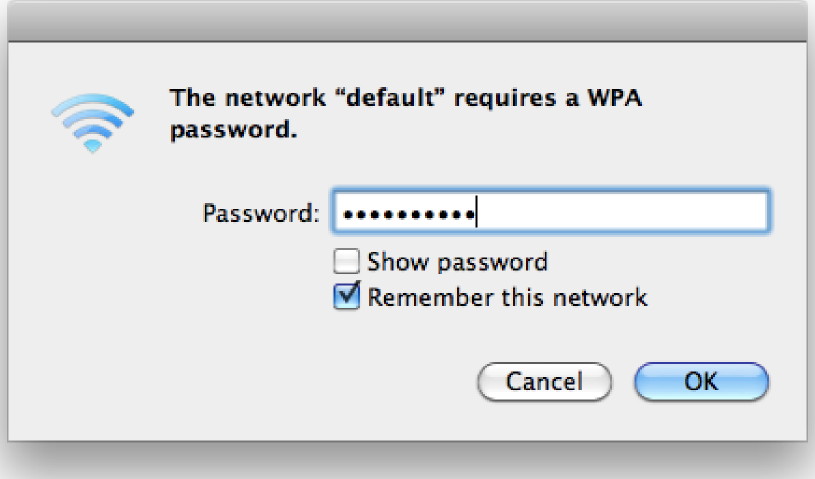
AirPort: On
Turn AirPort Off
No network selected
default
Join Other Network...
Create Network...
Open Network Preferences...

Figure 5-7: Highlighting and Selecting the Wireless Network

Step 3: 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.



The network "default" requires a WPA password.

Password: ●●●●●●●●●●

□ Show password

☑ Remember this network

Figure 5-8: Enter the Password

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

Step 4: 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.

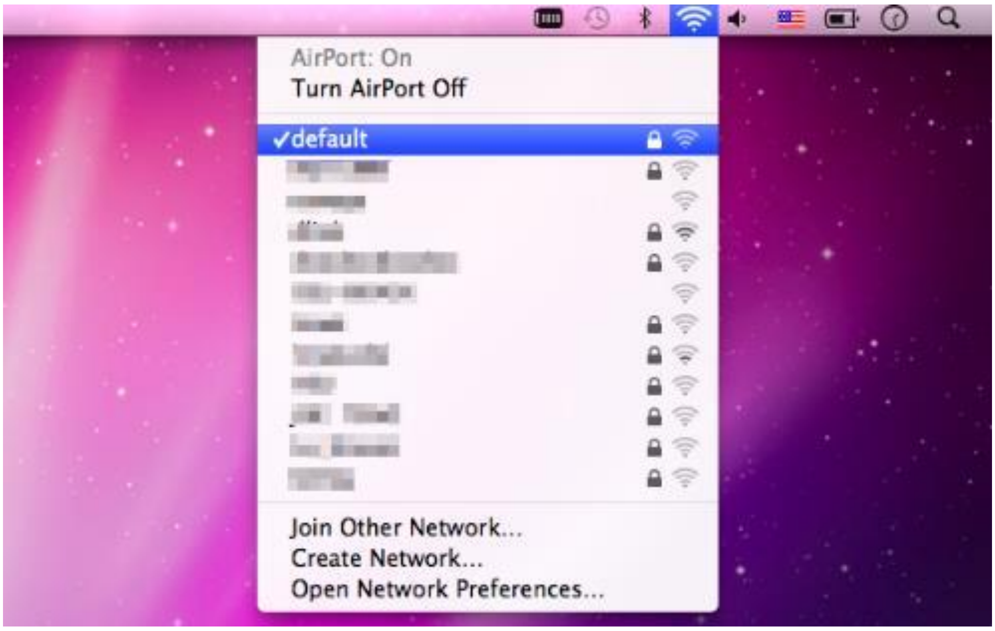


Figure 5-9: Connected to the Network

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**

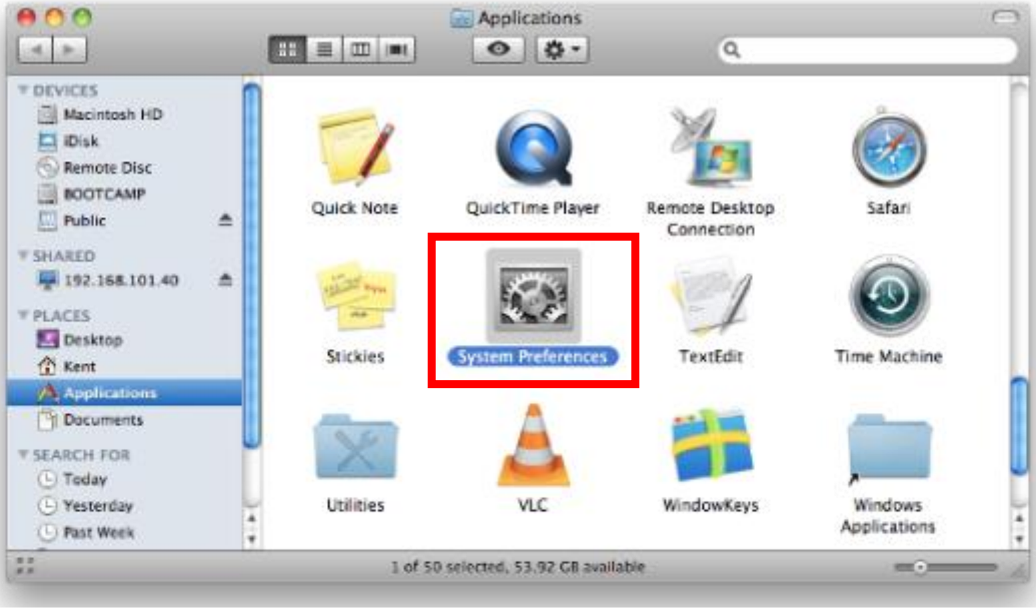


Figure 5-10: System Preferences

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

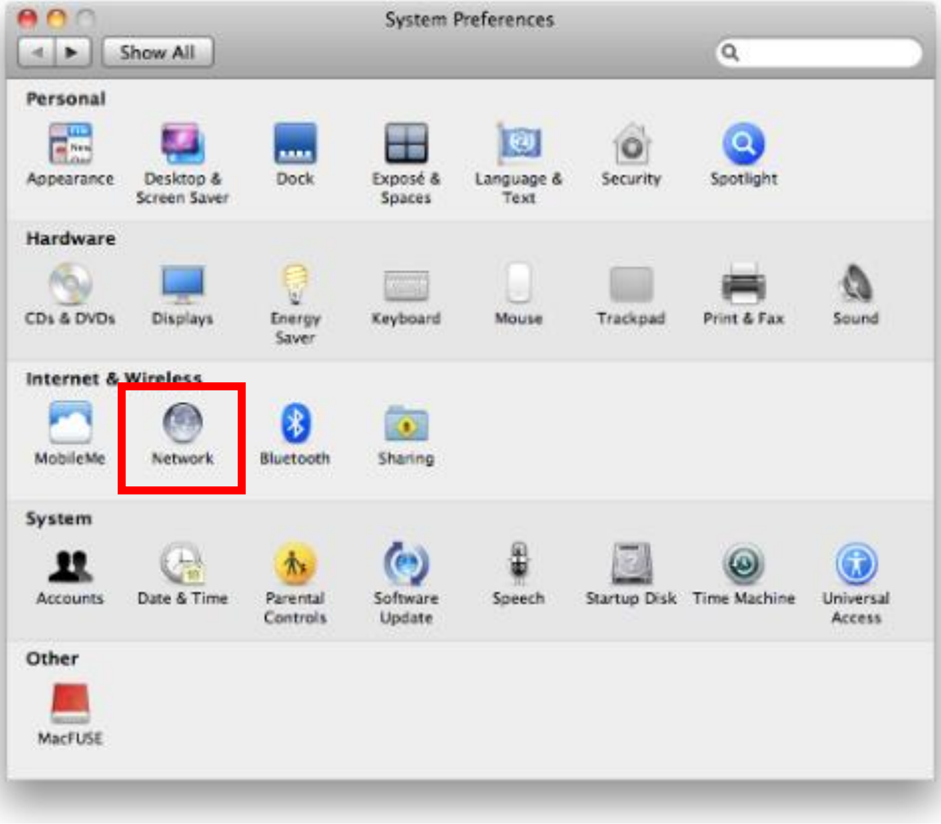


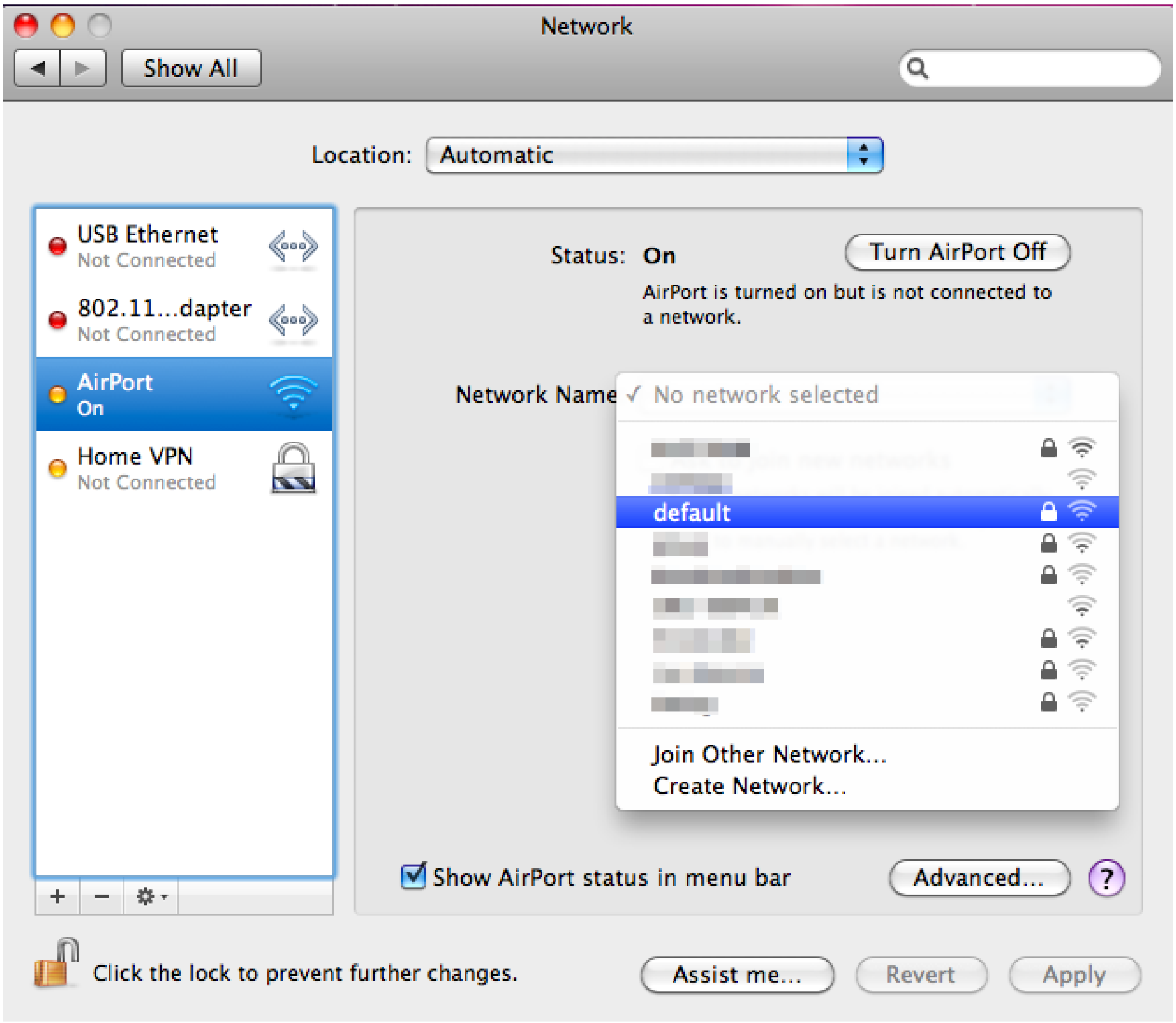
Figure 5-2: System Preferences -- Network

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".



Location: Automatic

Status: On

AirPort is turned on but is not connected to a network.

Network Name ✓ No network selected

☑ Show AirPort status in menu bar

Click the lock to prevent further changes.

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

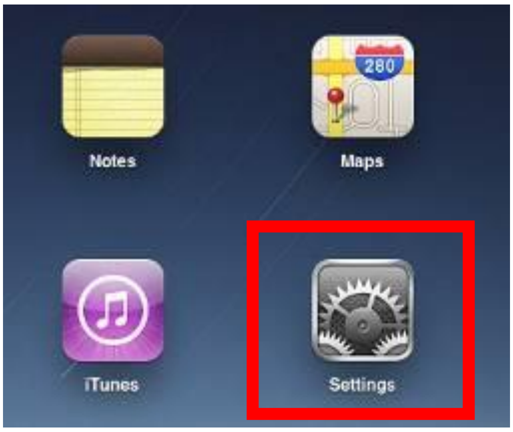


Figure 5-3: iPhone – Settings icon

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 802.11be Wireless AP, it should show “Not Connected”.

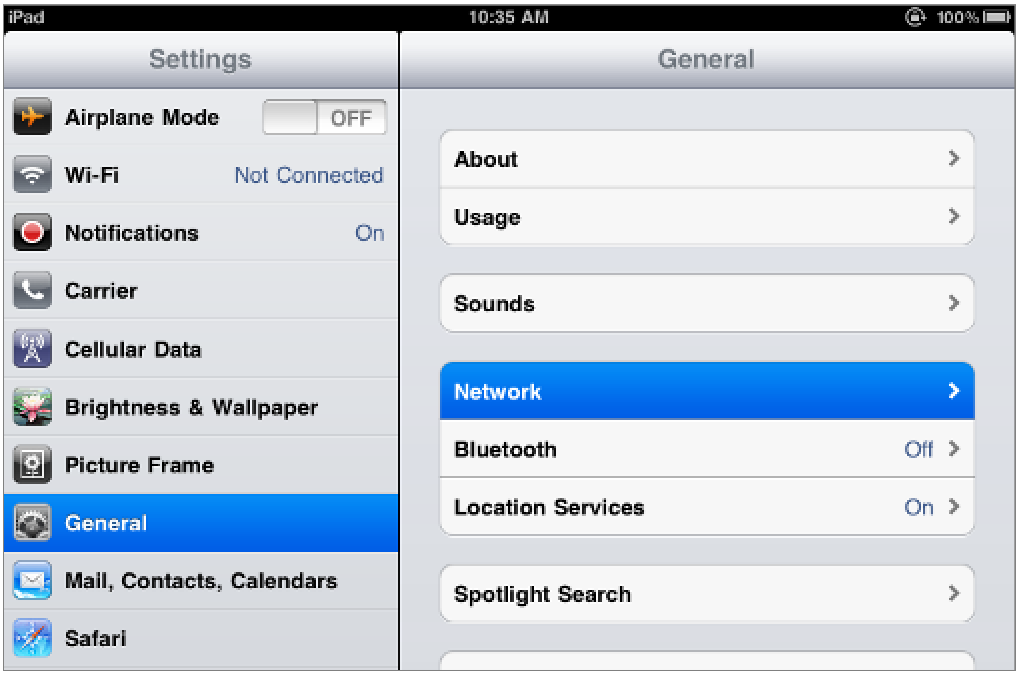
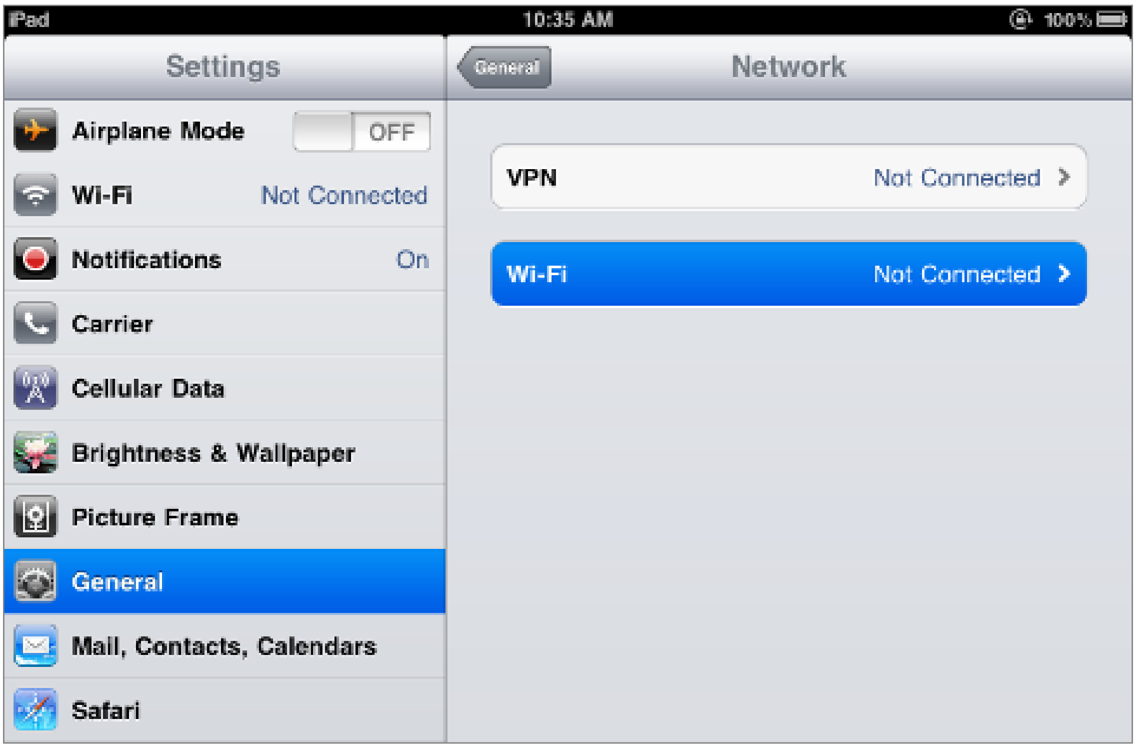


Figure 5-4: Wi-Fi Setting



iPad 10:35 AM 100%

Settings

Airplane Mode OFF

Wi-Fi Not Connected

Notifications On

Carrier

Cellular Data

Brightness & Wallpaper

Picture Frame

General

Mail, Contacts, Calendars

Safari

General Network

VPN Not Connected

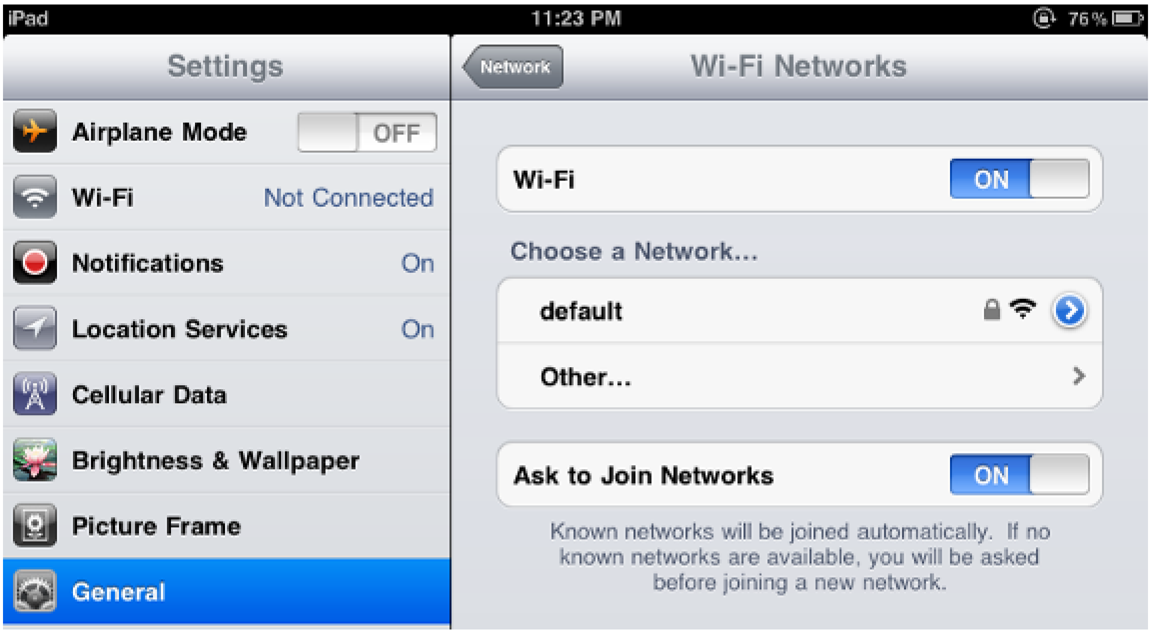
Wi-Fi Not Connected

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**]



iPad 11:23 PM 76%

Settings

Airplane Mode OFF

Wi-Fi Not Connected

Notifications On

Location Services On

Cellular Data

Brightness & Wallpaper

Picture Frame

General

Network Wi-Fi Networks

Wi-Fi ON

Choose a Network...

default

Other...

Ask to Join Networks ON

Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

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.

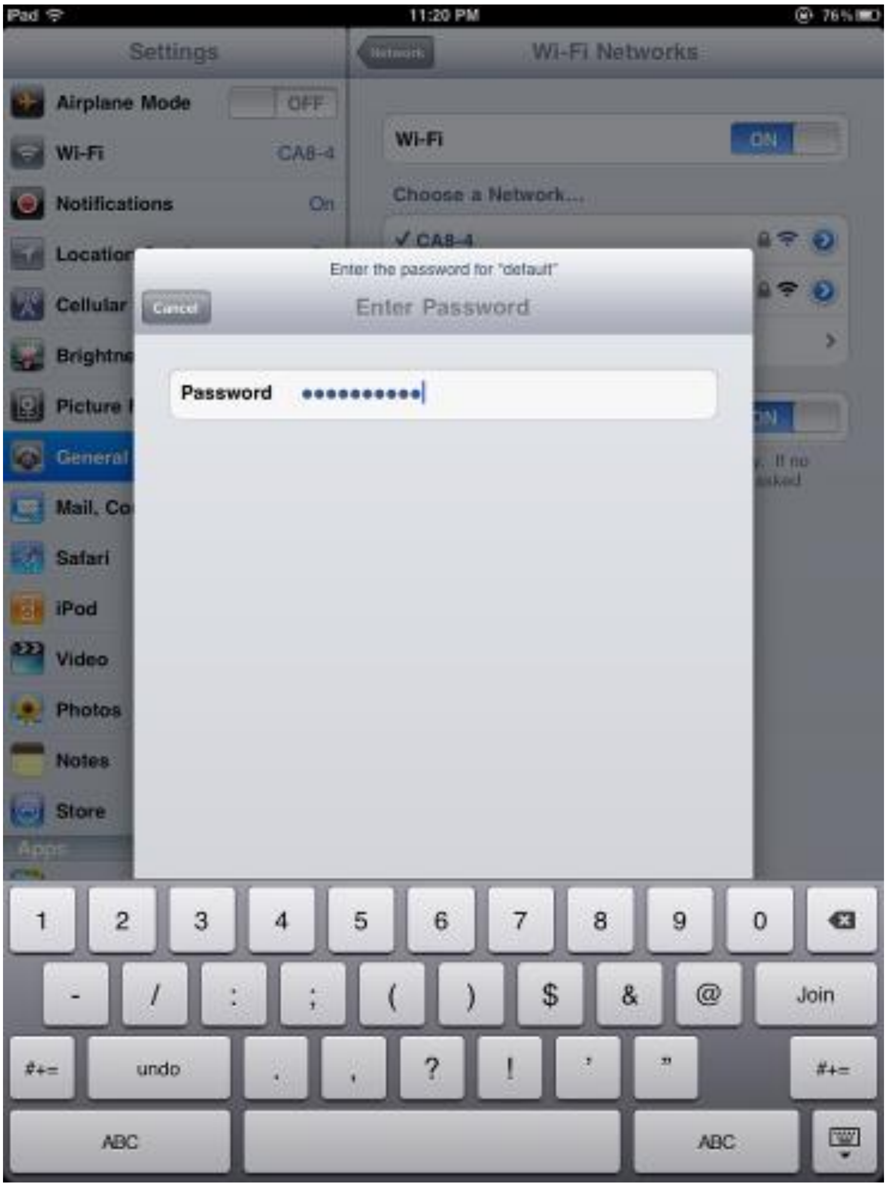
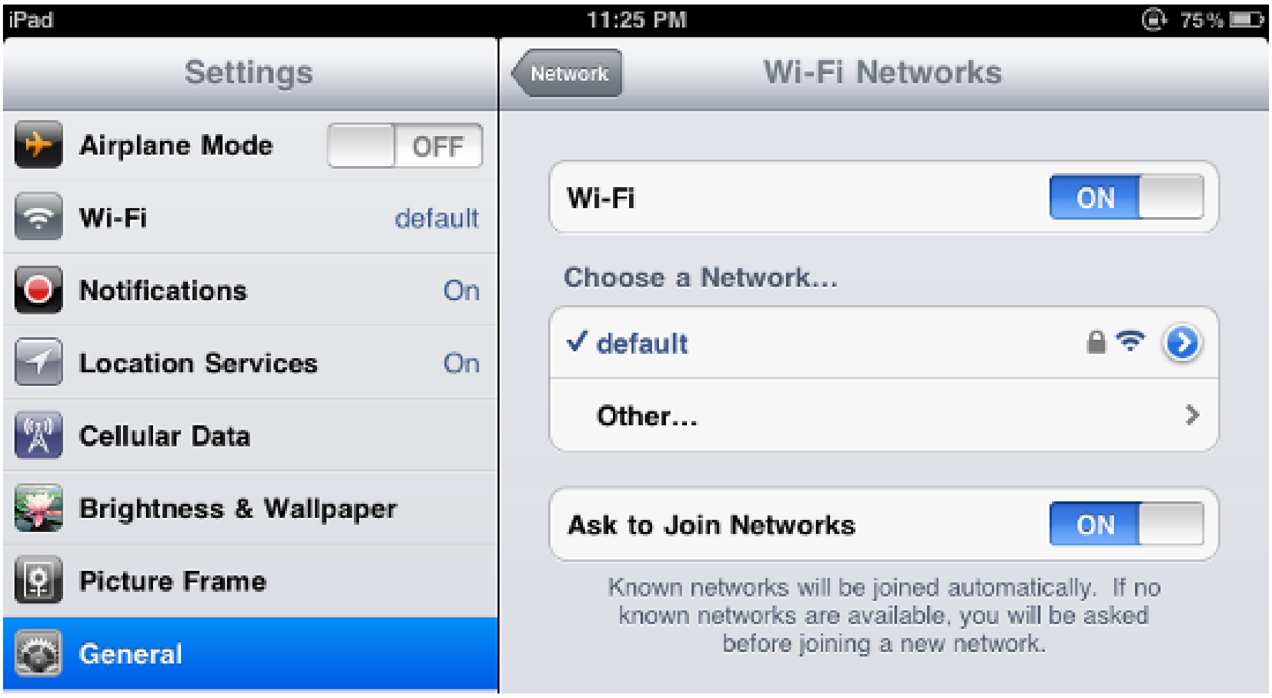


Figure 5-17: iPhone -- Entering the Password

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.



Known networks will be joined automatically. If no known networks are available, you will be asked before joining a new network.

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

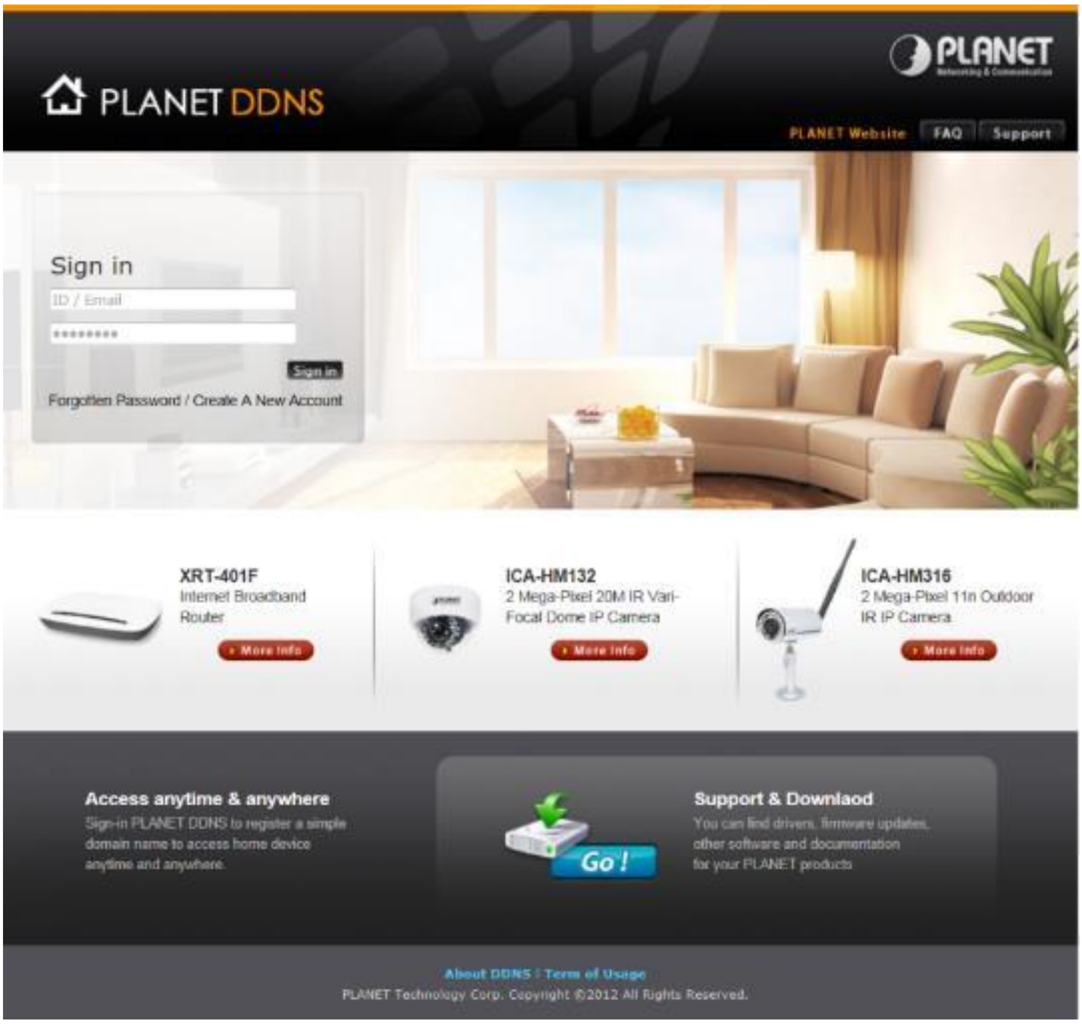
Appendix A: DDNS Application

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 https://planetddns.com

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

Step 3: Input all DDNS settings.



XRT-401F
Internet Broadband Router

ICA-HM132
2 Mega-Pixel 20M IR Vari-Focal Dome IP Camera

ICA-HM316
2 Mega-Pixel 11n Outdoor IR IP Camera

Access anytime & anywhere
Sign-in PLANET DDNS to register a simple domain name to access home device anytime and anywhere.

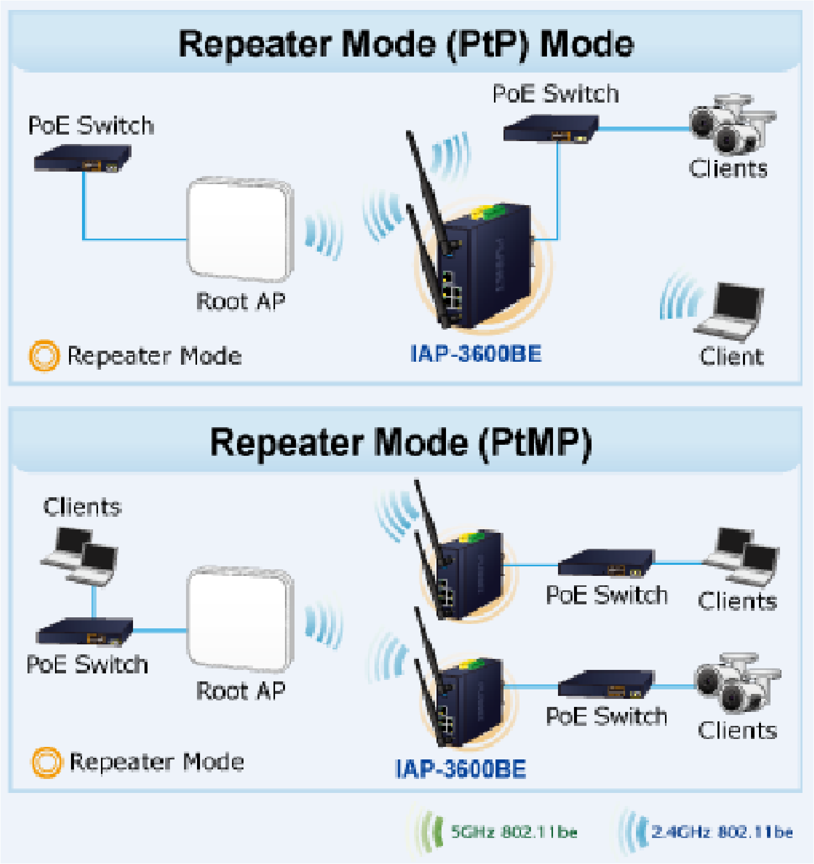
Support & Downlaod
You can find drivers, firmware updates, other software and documentation for your PLANET products

PLANET Technology Corp. Copyright ©2012 All Rights Reserved.

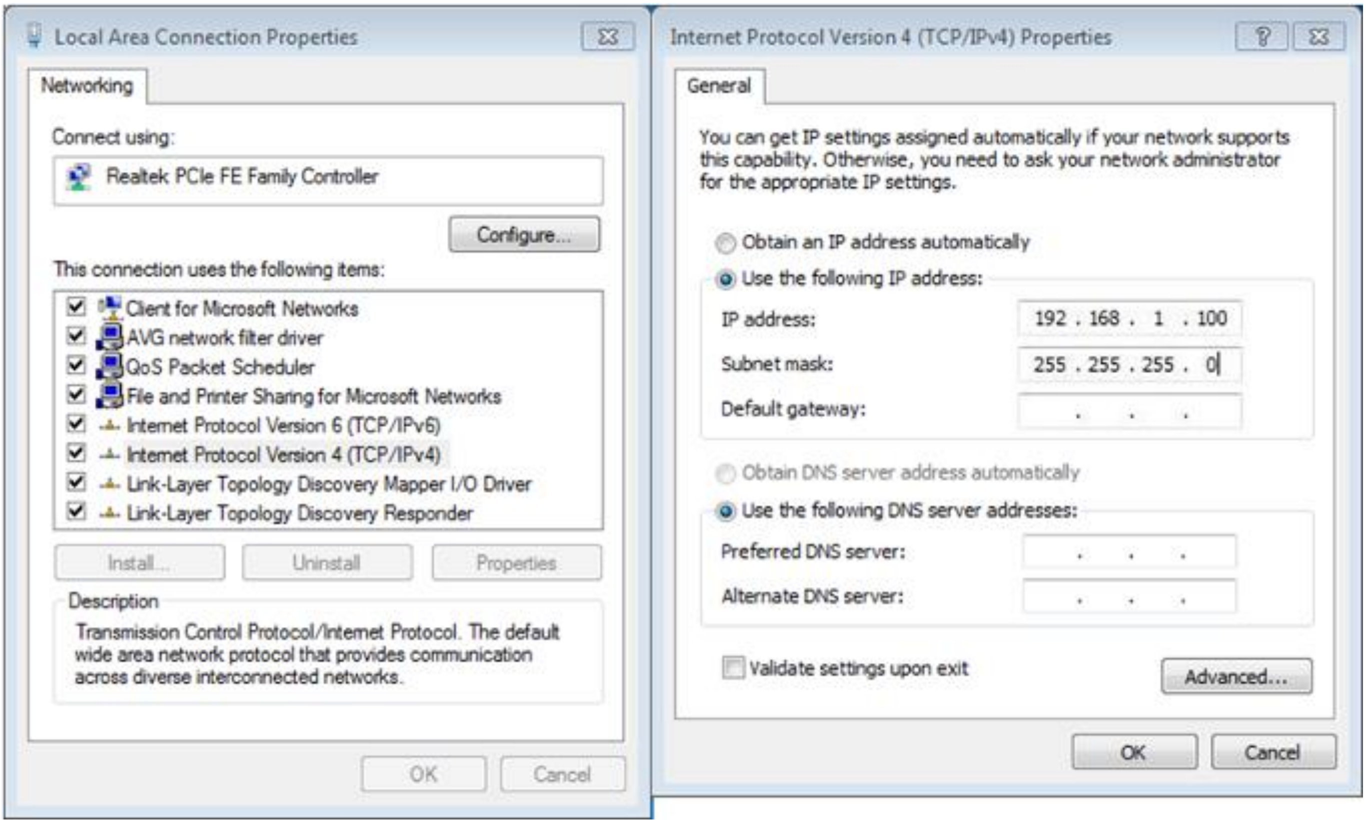
Appendix B: FAQs

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**".



Local Area Connection Properties

Networking

Connect using:

Realtek PCIe FE Family Controller

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ AVG network filter driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address:	192 . 168 . 1 . 100
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

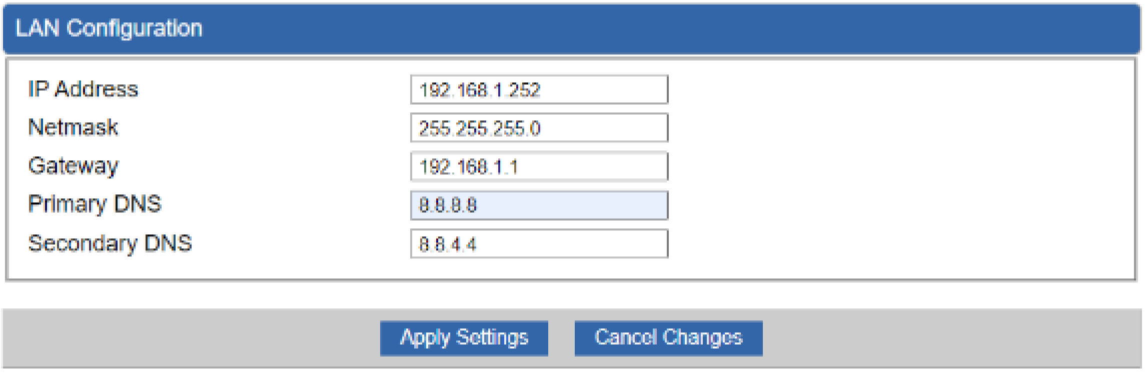
Preferred DNS server:	. . .
Alternate DNS server:	. . .

□ Validate settings upon exit

Advanced...

OK Cancel

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**.



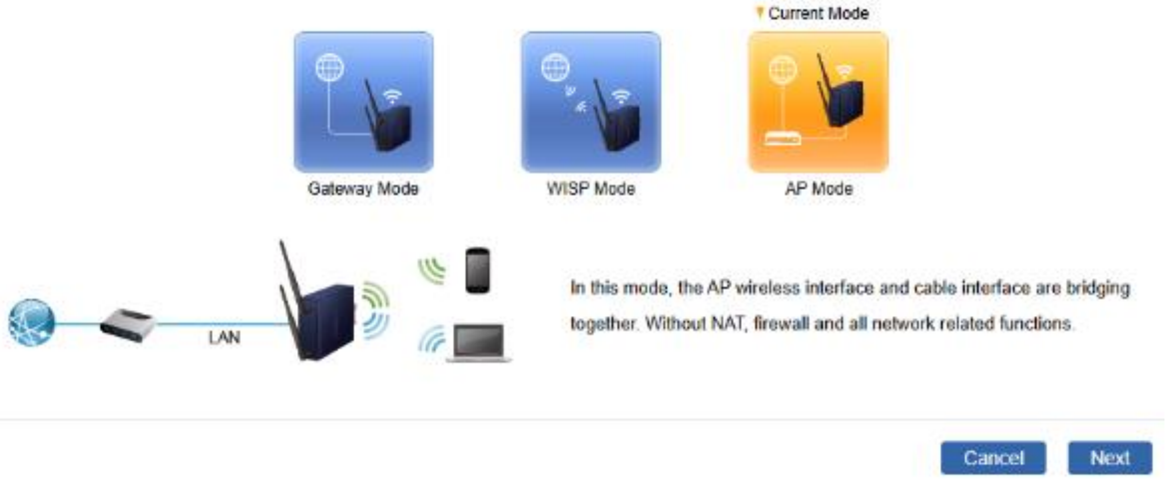
LAN Configuration

IP Address	192.168.1.252
Netmask	255.255.255.0
Gateway	192.168.1.1
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4

Apply Settings Cancel Changes

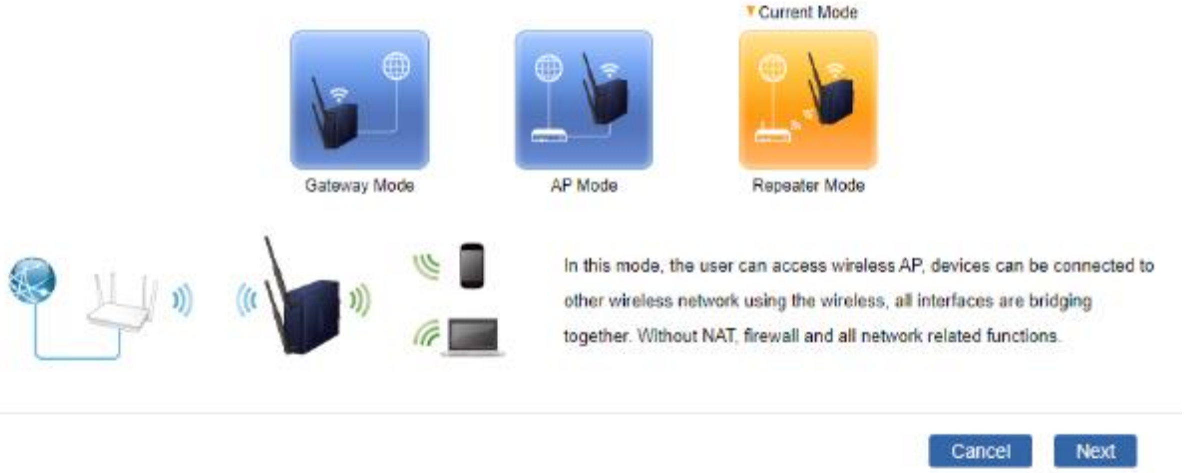
Step 3. In AP-1, go to “**Wizard**” to configure it to **AP Mode**. In AP-2, configure it to **Repeater Mode**.

AP-1



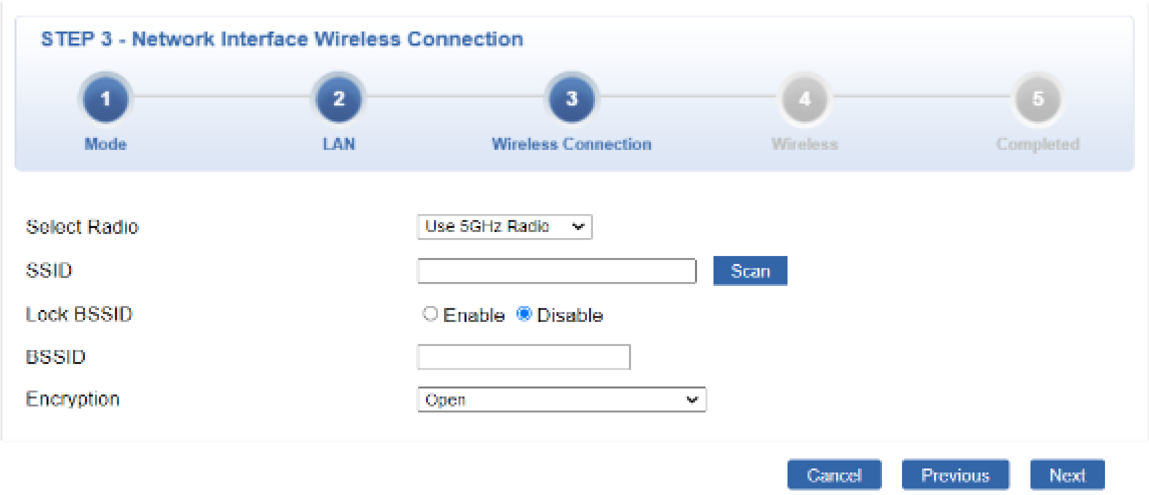
In this mode, the AP wireless interface and cable interface are bridging together. Without NAT, firewall and all network related functions.

AP-2



In this mode, the user can access wireless AP, devices can be connected to other wireless network using the wireless, all interfaces are bridging together. Without NAT, firewall and all network related functions.

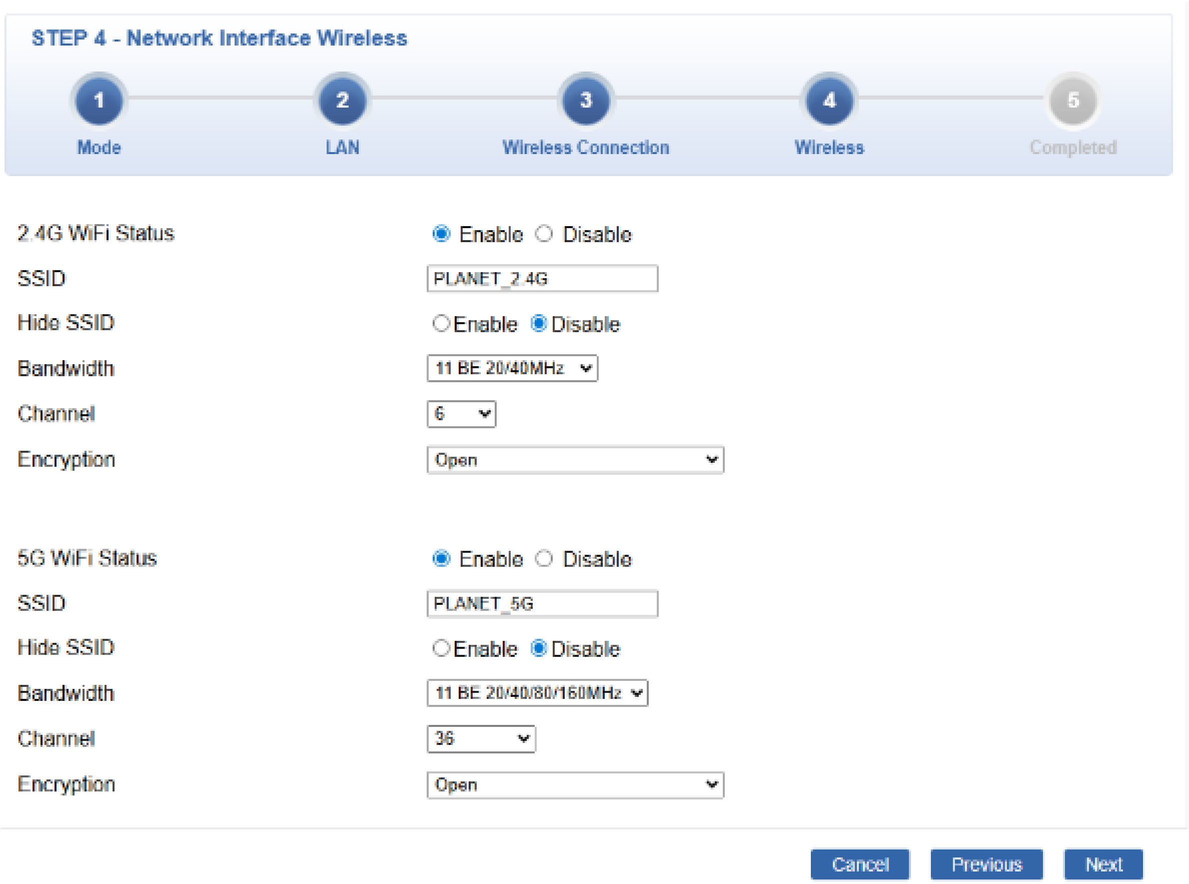
Step 4. In AP-2, press “**Scan “** to search the AP-1. You can also enter the MAC address, SSID, encryption and bandwidth if you know what they are.



STEP 3 - Network Interface Wireless Connection

Select Radio	Use 5GHz Radio
SSID	Scan
Lock BSSID	○ Enable ● Disable
BSSID	
Encryption	Open

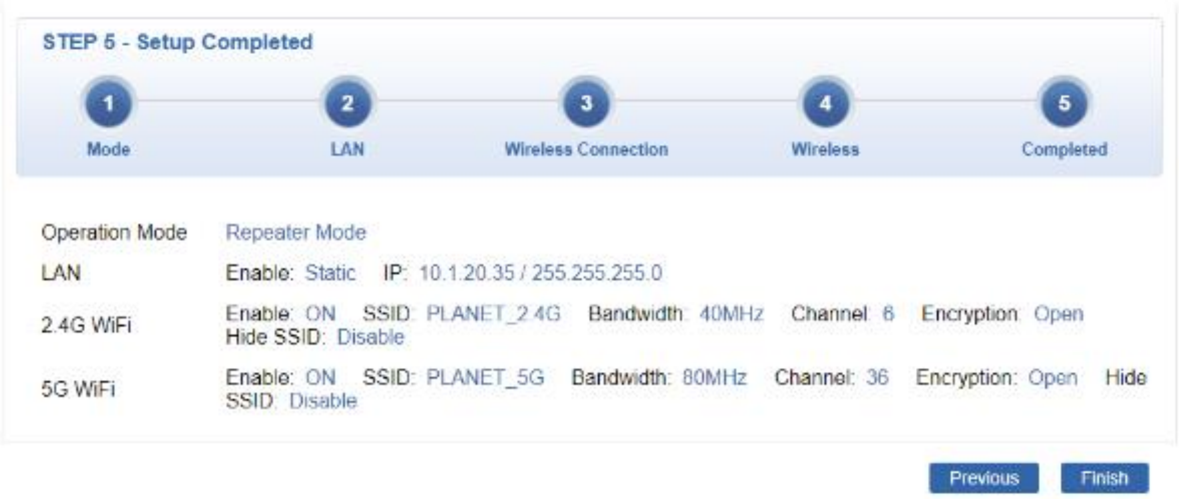
Step 5. Click “**Next**” to finish the setting.



STEP 4 - Network Interface Wireless

2.4G WiFi Status	● Enable ○ Disable
SSID	PLANET_2.4G
Hide SSID	○ Enable ● Disable
Bandwidth	11 BE 20/40MHz
Channel	6
Encryption	Open
5G WiFi Status	● Enable ○ Disable
SSID	PLANET_5G
Hide SSID	○ Enable ● Disable
Bandwidth	11 BE 20/40/80/160MHz
Channel	36
Encryption	Open

Step 6.Setup Completed



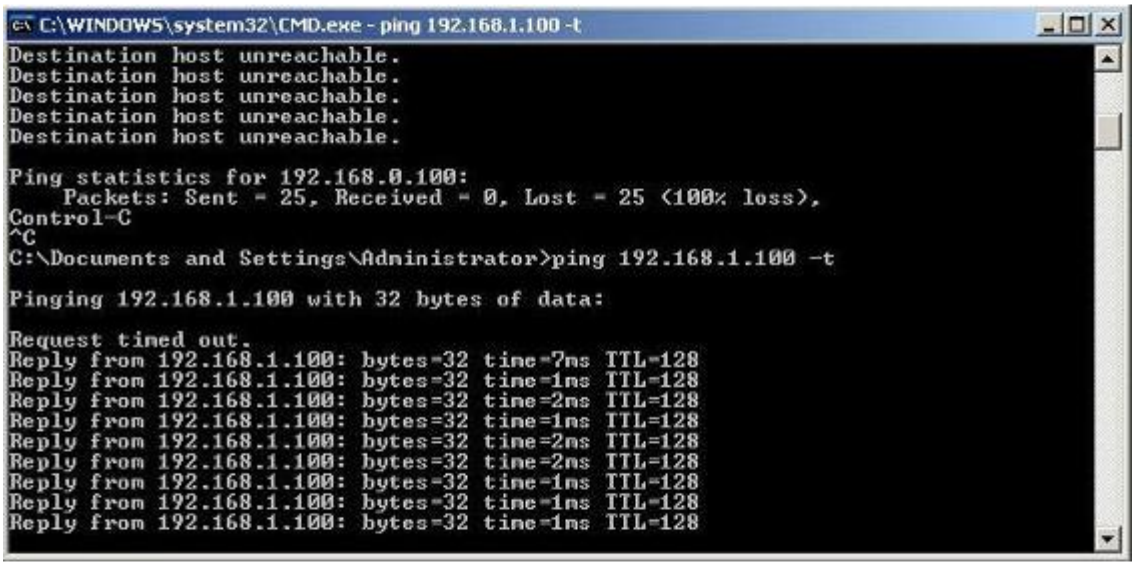
Operation Mode Repeater Mode

LAN Enable: Static IP: 10.1.20.35 / 255.255.255.0

2.4G WiFi Enable: ON SSID: PLANET_2.4G Bandwidth: 40MHz Channel: 6 Encryption: Open Hide SSID: Disable

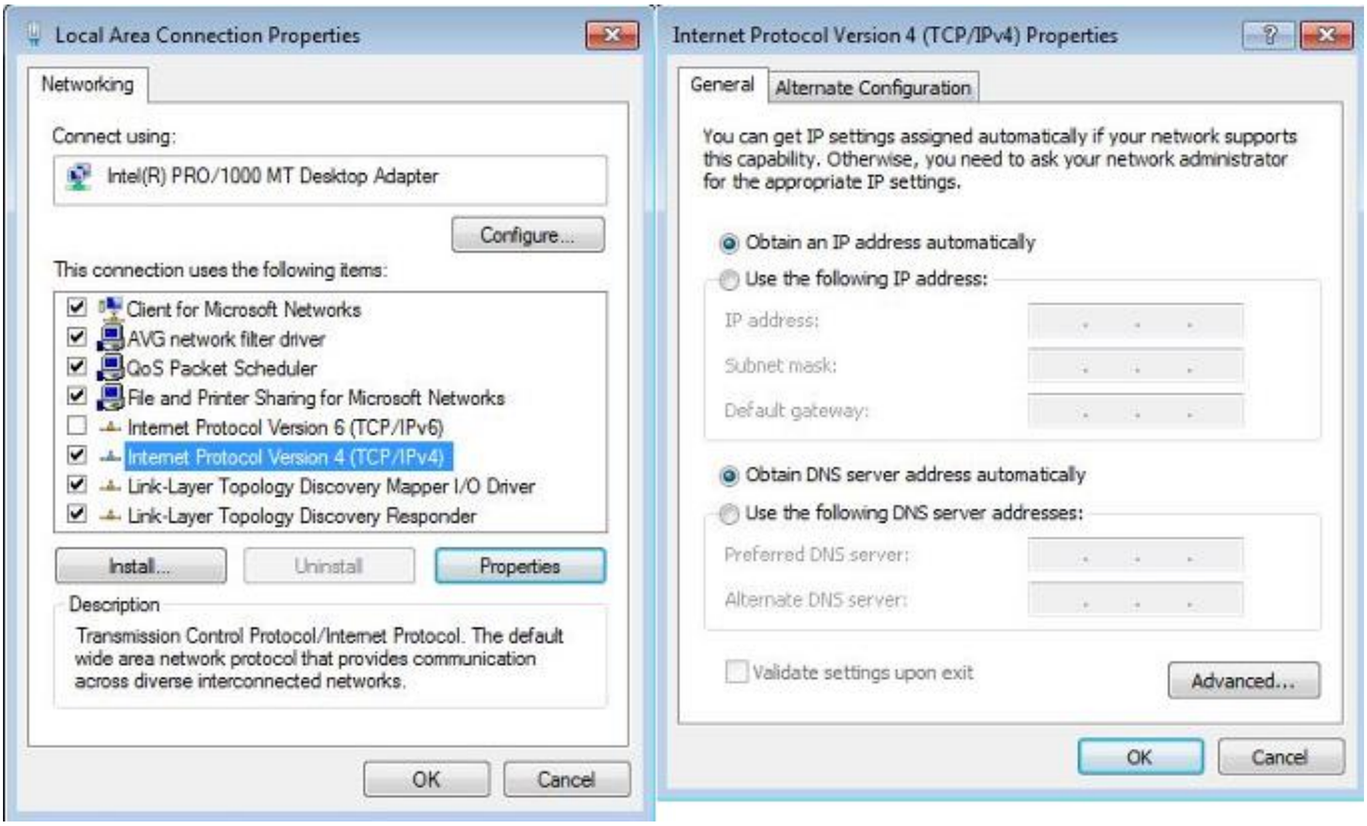
5G WiFi Enable: ON SSID: PLANET_5G Bandwidth: 80MHz Channel: 36 Encryption: Open Hide SSID: Disable

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.



```
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 192.168.0.100:
    Packets: Sent = 25, Received = 0, Lost = 25 (100% loss),
Control-C
^C
C:\Documents and Settings\Administrator>ping 192.168.1.100 -t

Pinging 192.168.1.100 with 32 bytes of data:

Request timed out.
Reply from 192.168.1.100: bytes=32 time=7ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=2ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
Reply from 192.168.1.100: bytes=32 time=1ms TTL=128
```

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



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ AVG network filter driver
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- □ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... Uninstall Properties

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

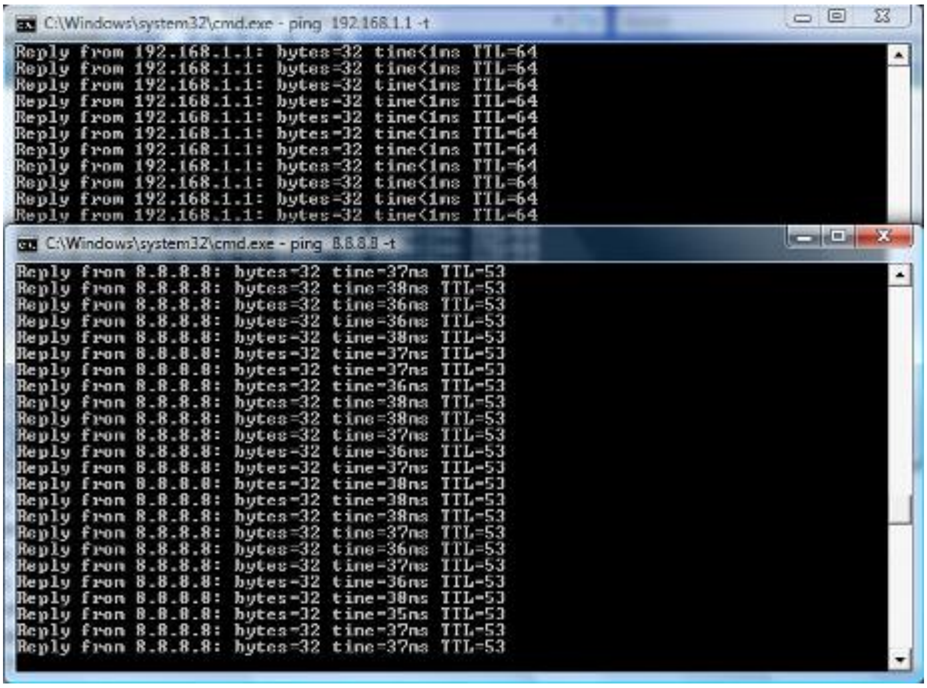
Alternate DNS server: . . .

□ Validate settings upon exit

Advanced...

OK Cancel

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



C:\Windows\system32\cmd.exe - ping 192.168.1.1 -t

```
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
Reply from 192.168.1.1: bytes=32 time<1ms TTL=64
```

C:\Windows\system32\cmd.exe - ping 8.8.8.8 -t

```
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=36ms TTL=53
Reply from 8.8.8.8: bytes=32 time=38ms TTL=53
Reply from 8.8.8.8: bytes=32 time=35ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
Reply from 8.8.8.8: bytes=32 time=37ms TTL=53
```

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.

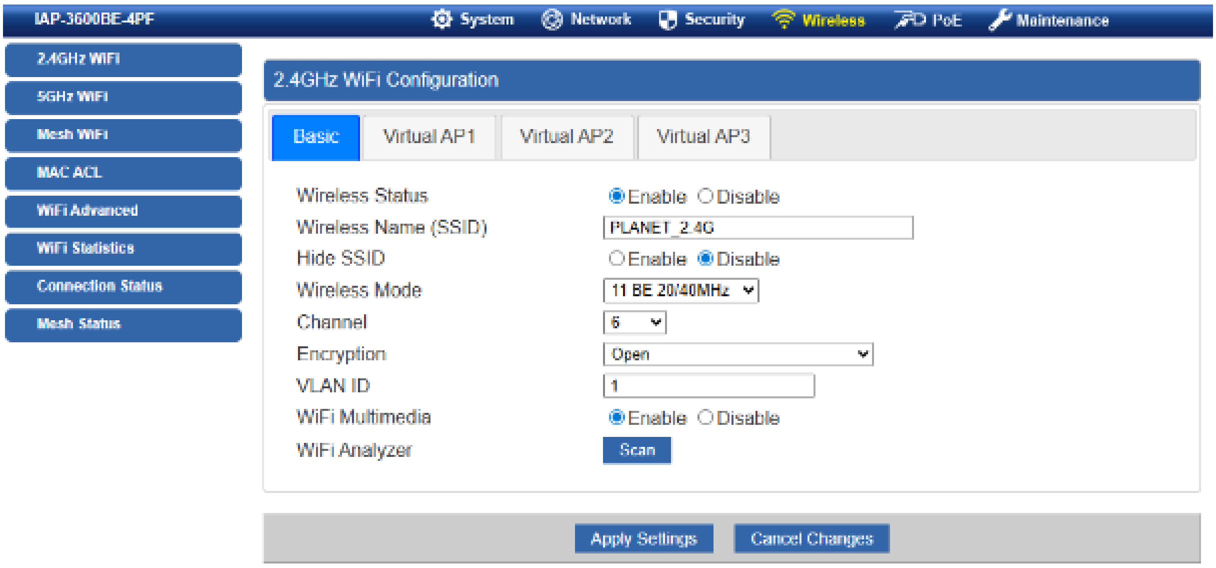
4) For the long distance connection over 1km, please adjust the "Distance" to the actual distance or double the actual distance.

Q2: How to tweak or 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.



2.4GHz WiFi Configuration

Wireless Status ● Enable ○ Disable

Wireless Name (SSID) PLANET_2.4G

Hide SSID ○ Enable ● Disable

Wireless Mode 11 BE 20/40MHz

Channel 6

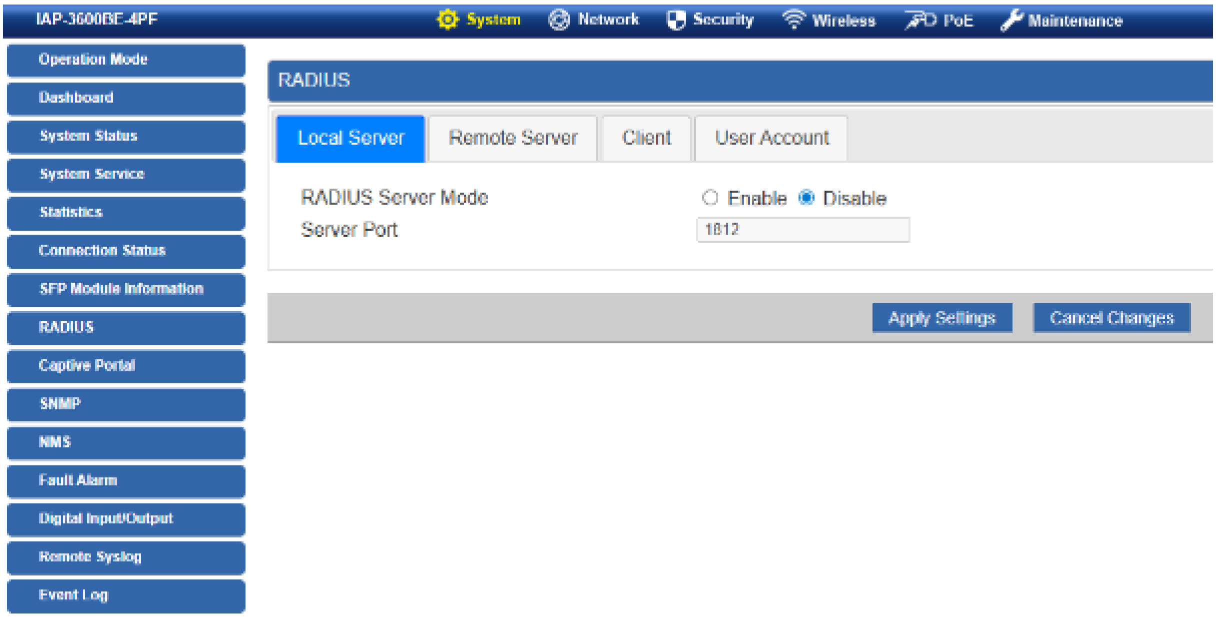
Encryption Open

VLAN ID 1

WiFi Multimedia ● Enable ○ Disable

WiFi Analyzer Scan

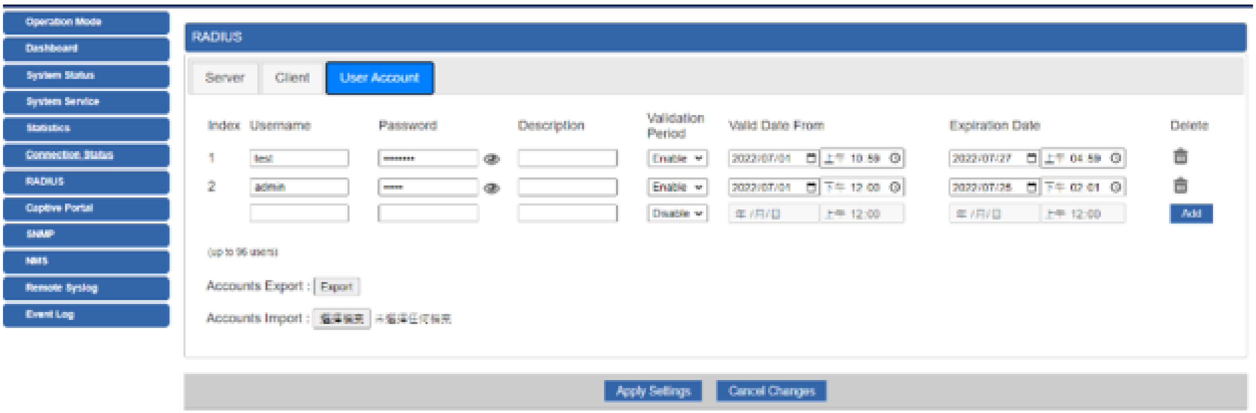
Step 4. Radius server setup web page.



RADIUS

RADIUS Server Mode ○ Enable ● Disable

Server Port 1812



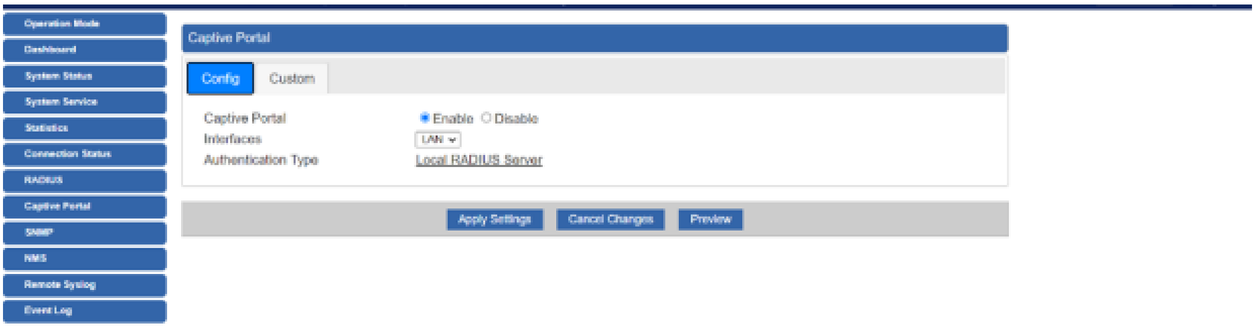
Index	Username	Password	Description	Validation Period	Valid Date From	Expiration Date	Delete
1	test	••••••••		Enable	2022/07/01 上午 10:59	2022/07/27 上午 04:59	🗑
2	admin	•••••		Enable	2022/07/01 下午 12:00	2022/07/26 下午 02:01	🗑
				Disable	年/月/日 上午 12:00	年/月/日 上午 12:00	Add

(up to 96 users)

Accounts Export : Export

Accounts Import : 選擇檔案 未選擇任何檔案

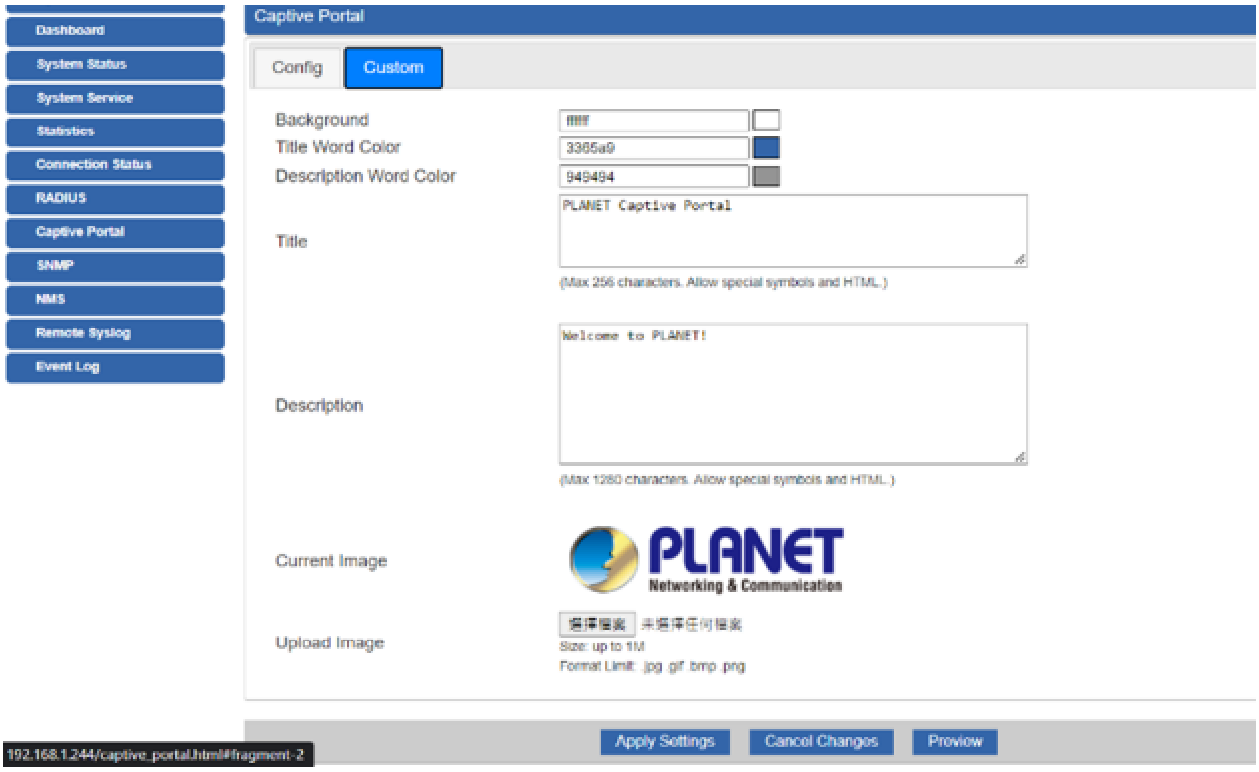
Step 5. Captive Portal setup web page.



Captive Portal ● Enable ○ Disable

Interfaces LAN

Authentication Type Local RADIUS Server



Background ffffff

Title Word Color 3365a9

Description Word Color 949494

Title PLANET Captive Portal

(Max 256 characters. Allow special symbols and HTML.)

Description Welcome to PLANET!

(Max 1280 characters. Allow special symbols and HTML.)

Current Image

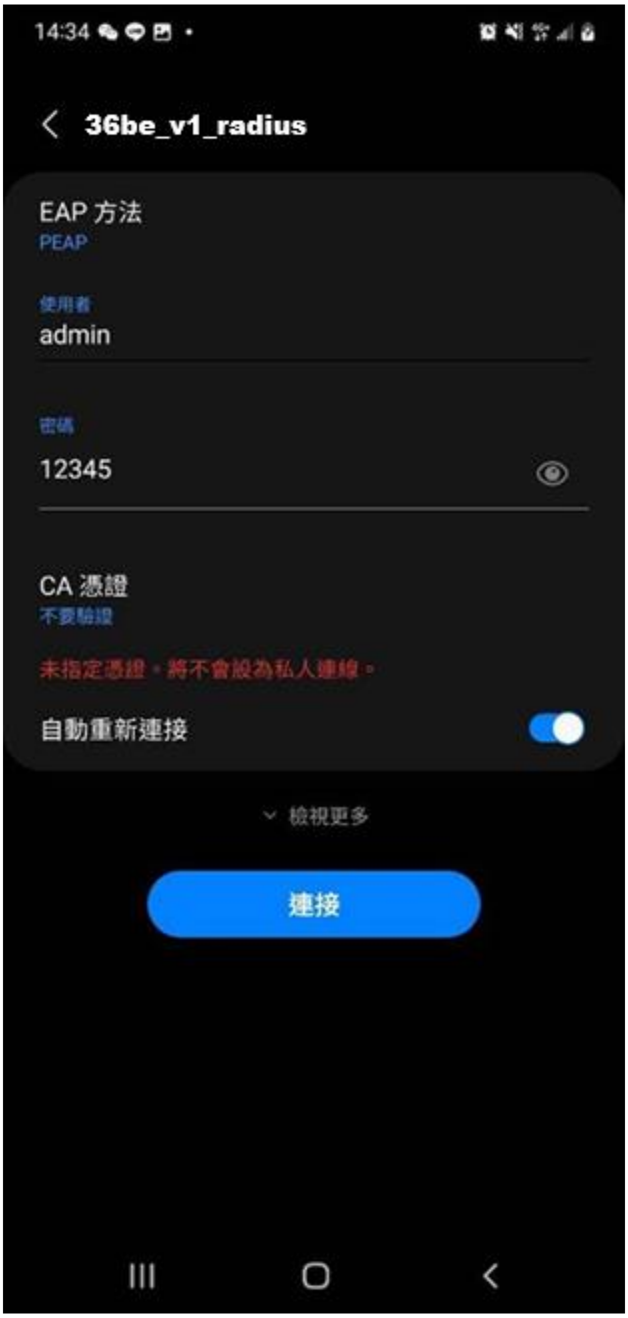
Upload Image 選擇檔案 未選擇任何檔案

Size: up to 1M

Format Limit: .jpg .gif .bmp .png

Step 6. Setup Completed.

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



14:34

36be_v1_radius

EAP 方法
PEAP

使用者
admin

密碼
12345

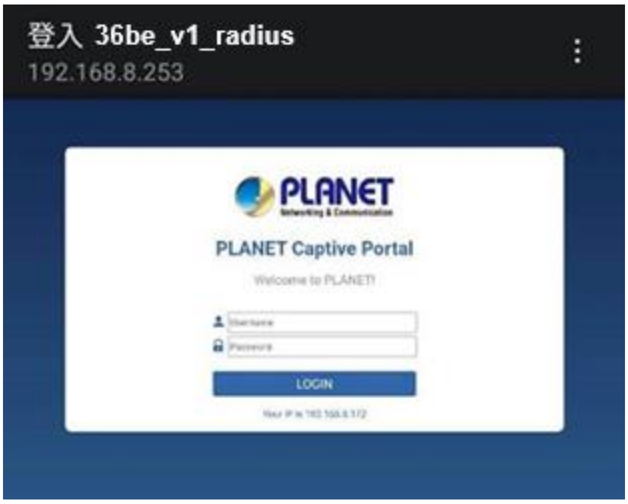
CA 憑證
不要驗證

未指定憑證。將不會設為私人連線。

自動重新連接

Step 8. The WIFI client connects to the WI-FI AP then input the username, password and select without CA verification required.

Step 9. The Captive Portal login screen appears, input the username and password then the WIFI client can access the Internet.



登入 36be_v1_radius
192.168.8.253

PLANET Captive Portal

Welcome to PLANET!

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 802.11be 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 802.11be 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

- **802.11be –** 802.11be, also known as Wi-Fi 7, is the latest wireless networking standard in the IEEE 802.11 family. It enhances and extends previous technologies such as OFDMA and MU-MIMO, and introduces advanced features like Multi-Link Operation (MLO) and 4096-QAM. Operating across the 2.4GHz and 5GHz bands, 802.11be supports channel bandwidths up to 160MHz, delivering significantly higher throughput, lower latency, and improved efficiency for next-generation wireless local area networks (WLANs).

- **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 https://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*	Português	PLANET Technology Corporation, declara que este 11ac Wireless AP está conforme com os requisitos essenciais e outras disposições da Directiva

	ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 2014/53/EU		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.