PLANET
Networking & Communication

User's Manual

1750Mbps 11ac Dual Band Wall Mount Enterprise Wireless AP

► **WDAP-1750AC**

www.PLANET.com.tw

Copyright

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

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

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.

Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Federal Communication Commission (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.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/CE OF THE EUROPEAN PARLIAMENT AND THE COUNCIL OF 9 March 1999 on radio equipment and telecommunication terminal equipment and the mutual recognition of their conformity (R&TTE). The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) as of April 8, 2000.

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.

National Restrictions

This device is intended for home and office use in all EU countries (and other countries following the EU directive 1999/5/EC) without any limitation except for the countries mentioned below:

Country	Restriction	Reasons/remarks
Bulgaria	None	General authorization required for outdoor use and public service
France	Outdoor use; limited to 10 mW e.i.r.p. within the band 2454-2483.5 MHz	Military Radiolocation use. Refarming of the 2.4 GHz band has been ongoing in recent years to allow current relaxed regulation. Full implementation planned 2012
Italy	None	If used outside of own premises, general authorization is required
Luxembourg	None	General authorization required for network and service supply(not for spectrum)
Norway	Implemented	This subsection does not apply for the geographical area within a radius of 20 km from the centre of Ny-Ålesund
Russian Federation	None	Only for indoor applications

Note: Please don't use the product outdoors in France.

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 Manual of PLANET 1750Mbps 802.11ac Dual Band Wall Mount Wireless Access Point

Model: WDAP-1750AC

Rev: 1.0 (Nov., 2014)

Part No. EM-WDAP-1750AC_v1.0 (2081-E11030-000)

CONTENTS

FIGURES

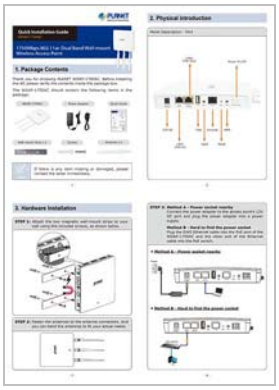
Chapter 1. Product Introduction

1.1 Package Contents

Thank you for choosing PLANET WDAP-1750AC. Before installing the AP, please verify the contents inside the package box.

WDAP-1750AC

Quick Guide



Antenna x 3

Wall-mount Strip x 2

Screws

Power Adapter

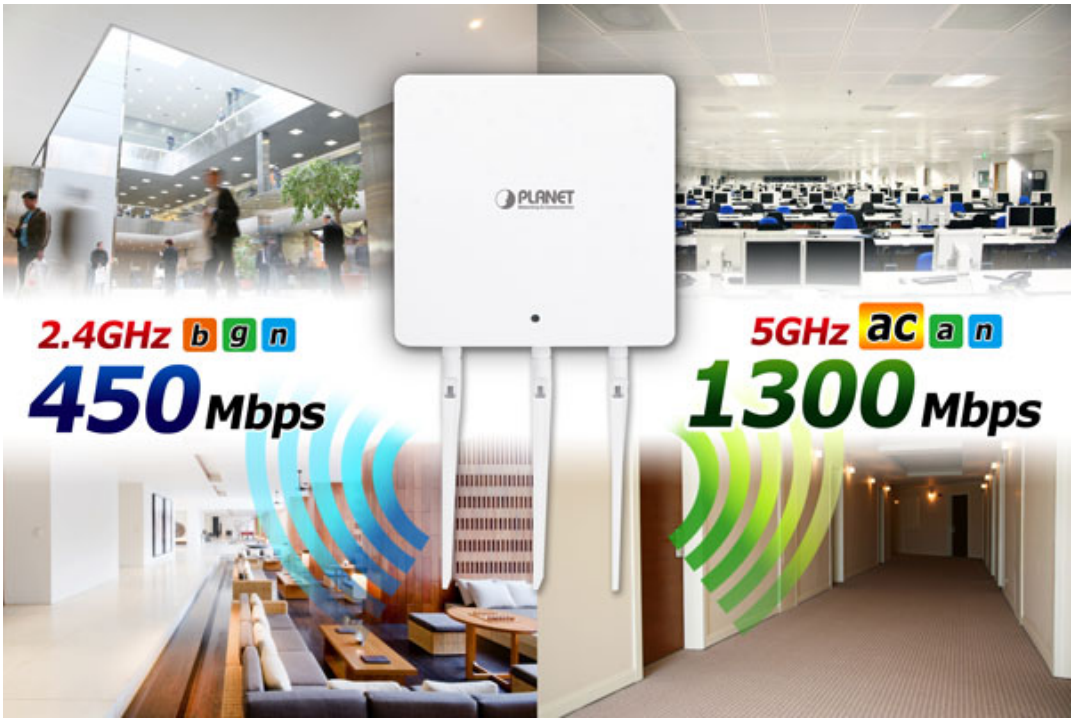
Note

If there is any item missing or damaged, please contact the seller immediately.

1.2 Product Description

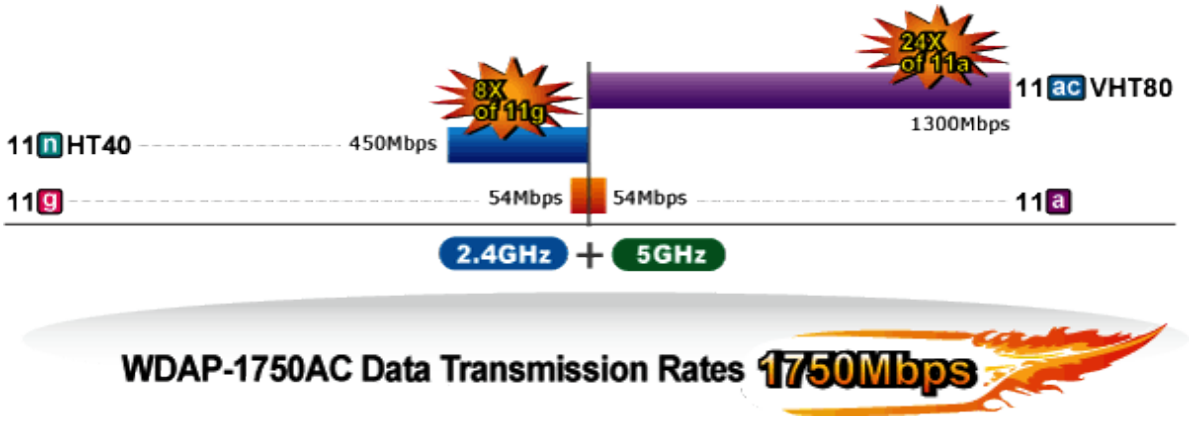
Ultra-high-speed, Next-generation Enterprise Wireless

PLANET WDAP-1750AC is an enterprise PoE access point with the latest 802.11ac wireless technology, advanced management features and superior encryption standard yet cost-effective. Meeting enterprise demand, the WDAP-1750AC has enhanced security and management features including multiple SSIDs, IEEE 802.1Q VLAN, WPA / WPA2-enterprise security, RADIUS MAC authentication and so forth. With the multiple reversed-polarity SMA male antenna connectors, the WDAP-1750AC is able to connect its suitable external antenna and booster wirelessly.



Extraordinary 11ac Dual Band Wireless Technology

The WDAP-1750AC supports IEEE 802.11a/b/g/n/ac dual band standards with 3T3R MIMO technology; therefore, it provides the wireless speed up to 450+1300Mbps, which is 24X faster than the 11a access point at 5GHz frequency and 8X faster than the 11g access point at 2.4GHz frequency. The incredible wireless speed makes it ideal for handling multiple HD movie streams, high-resolution on-line games, stereo music, VoIPs and data streams at the same time stably and smoothly.

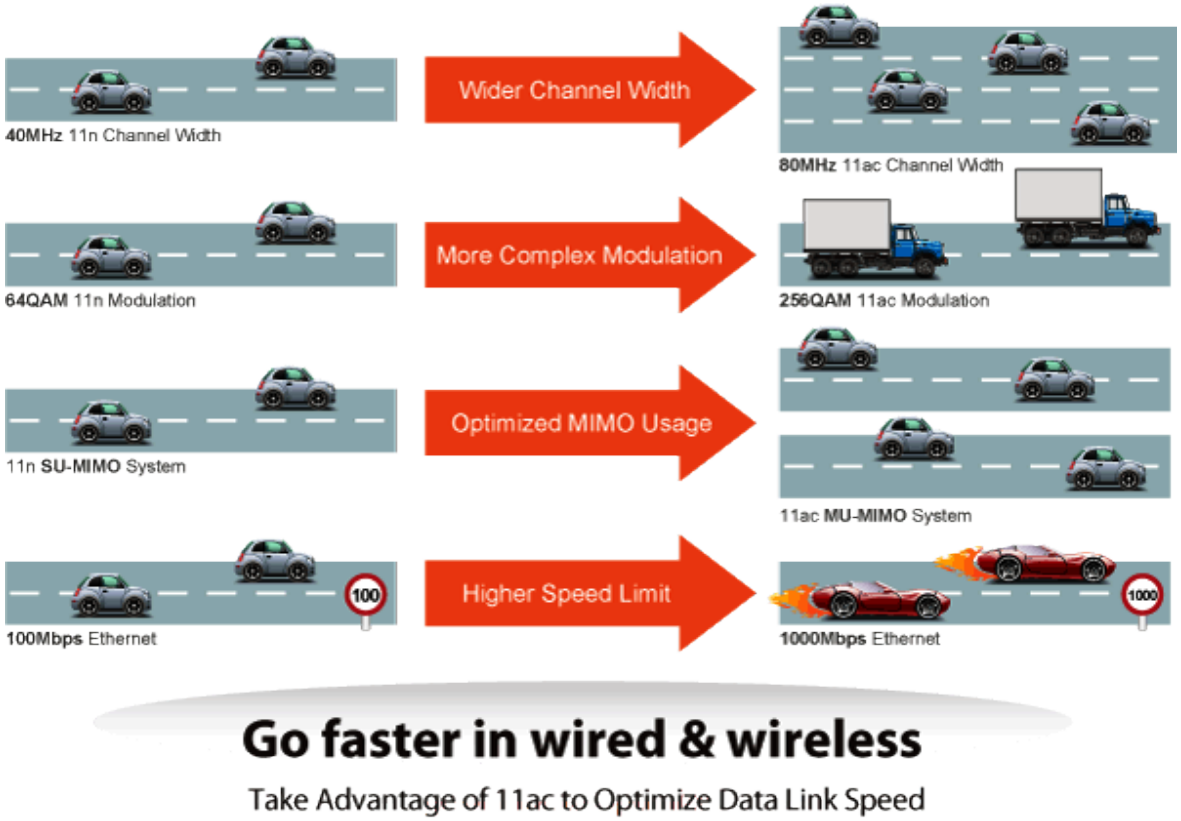


Secured and Managed Enterprise-class WLAN

With support for high-level encryption mechanism, the WDAP-1750AC can effectively prevent your information from eavesdropping by unauthorized users. Allowing multiple different SSIDs to be used simultaneously and cooperating with the VLAN support, the WDAP-1750AC helps network administrators define separate wireless subnets for various class-of-service and security policies.

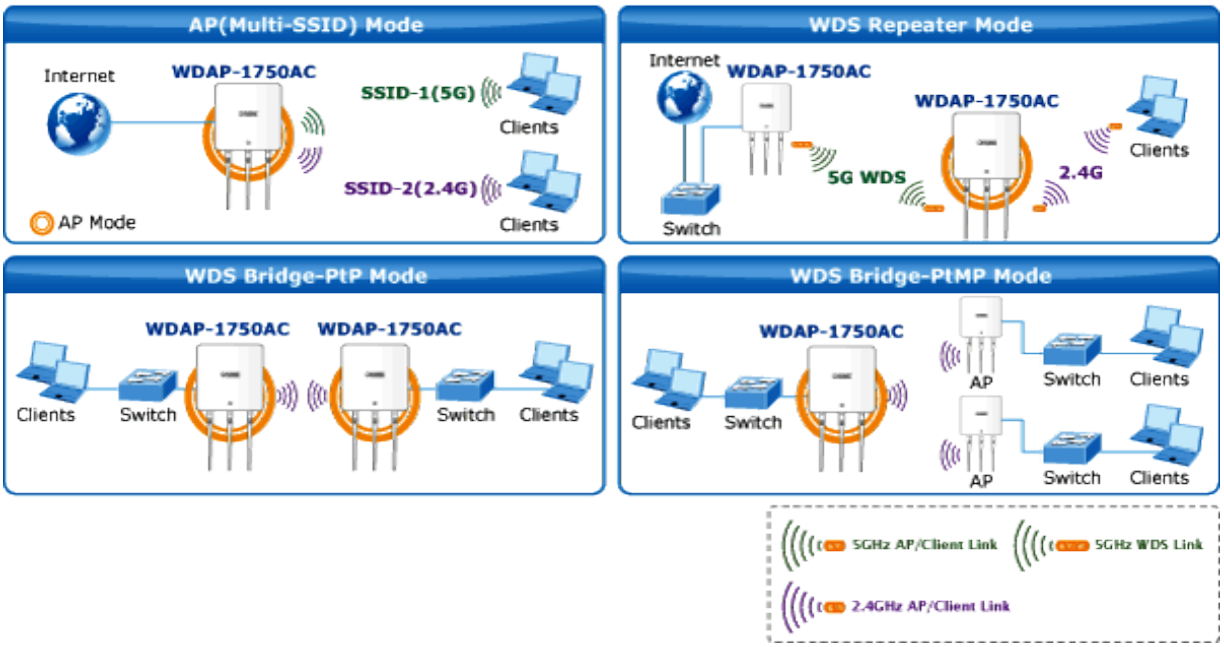
11ac Innovations Bring Excellent Data Link Speed

The WDAP-1750AC has 3 detachable highly-sensitive antennas which provide stronger signal and excellent coverage even in the wide-ranging or bad environment. With adjustable transmit power option, the administrator can flexibly reduce or increase the output power for various environments, thus reducing interference to achieve maximum performance. To provide extremely high-speed user experience, the WDAP-1750AC adopts IEEE 802.11ac technology to extend the 802.11n 40MHz channel binding to 80MHz and the implementation of 256-QAM modulation where higher transmitting/receiving rates go up to 1300Mbps in 5GHz less interference frequency band. In addition, the WDAP-1750AC is equipped with Gigabit LAN port to eliminate the restriction of 100Mbps Fast Ethernet wired connection to let users fully enjoy the high speed provided by wireless. The IEEE 802.11ac also optimizes MU-MIMO (Multi-User MIMO) mechanism to serve multiple devices simultaneously.



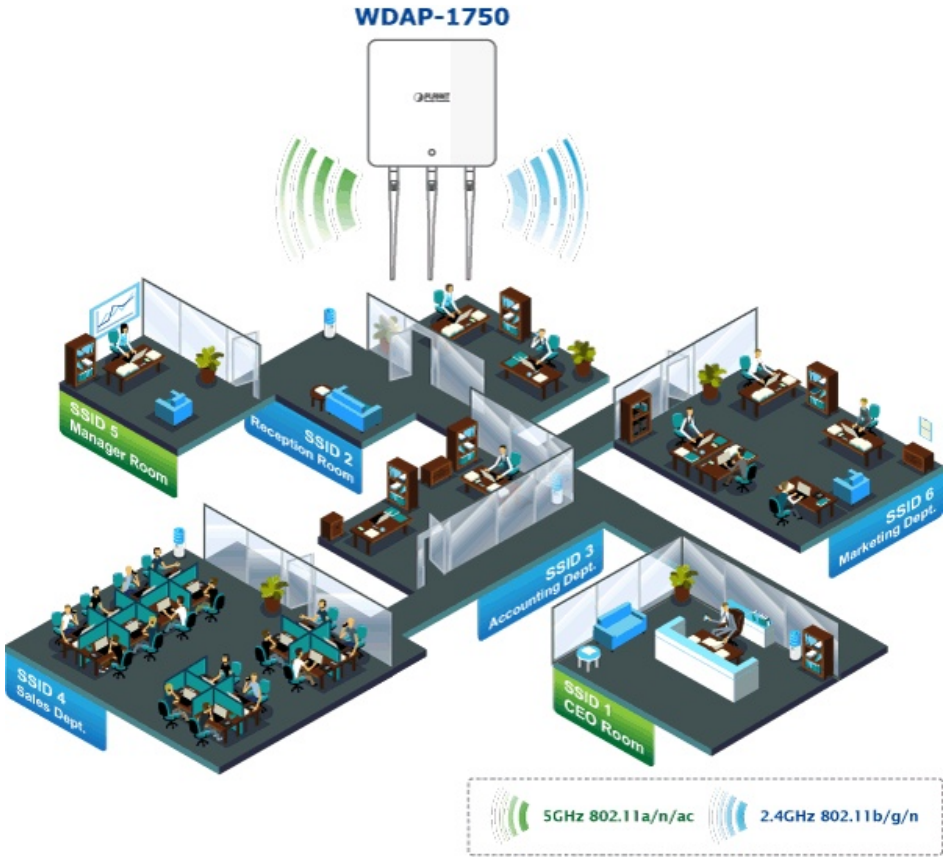
Multiple Operation Modes for Various Applications

The WDAP-1750AC supports AP, WDS Bridge, and Repeater modes, through which it provides more flexibility for users when wireless network is established. Compared with general wireless access point, the WDAP-1750AC offers more powerful and flexible capability for wireless clients.



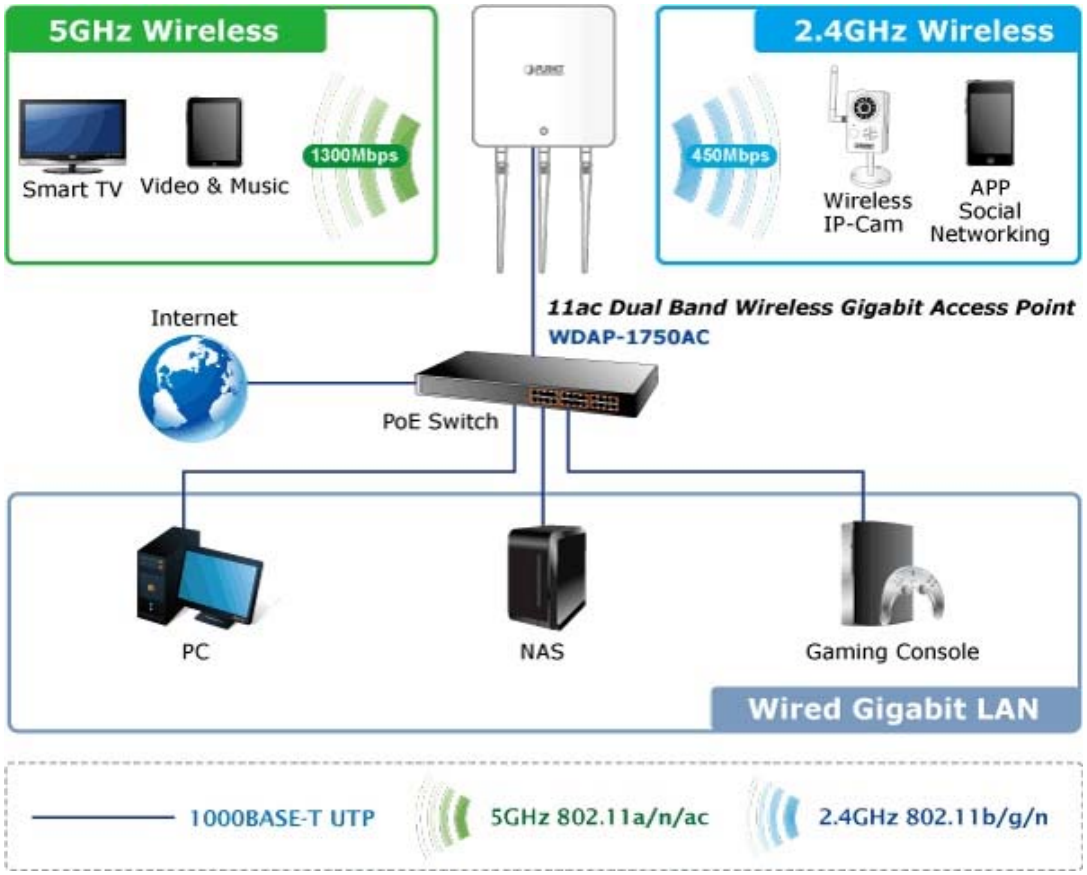
Wireless Security Encryption and Wireless Value-added Features

In aspect of security, besides 64/128-bit WEP encryption, the WDAP-1750AC is integrated with WPA / WPA2, WPA-PSK / WPA2-PSK and 802.1x Radius authority to secure and protect your wireless LAN. It provides the wireless MAC filtering and SSID broadcast control to consolidate the wireless network security and prevent unauthorized wireless connection. Being an access point, the WDAP-1750AC supports the VLAN function to allow multiple SSIDs (32 sets of SSIDs) to access Internal VLAN topology. Moreover, its Wi-Fi Multimedia (WMM) mechanism provides enhanced QoS over wireless connection for better performance in multimedia transmission like on-line gaming and video streaming, which are classified as a top priority.



Extreme High Speed and Dual Band Make Wi-Fi transmission More Powerful

The WDAP-1750AC delivers the dual band technology to avoid signal interference and ensure the best Wi-Fi performance. It allows you to check e-mail and surf the Internet via the 2.4GHz band and simultaneously watch high-definition (HD) video or any other multimedia application via 5GHz band. Moreover, the Gigabit Ethernet port of the WDAP-1750AC offers ultra-fast wired connections that utilize the maximum wireless bandwidth; therefore, users will have real wireless speed over 100Mbps. With outstanding stability of high-speed wireless transmission, the WDAP-1750AC can provide users with excellent experience in multimedia streaming with your mobile devices anywhere, anytime.



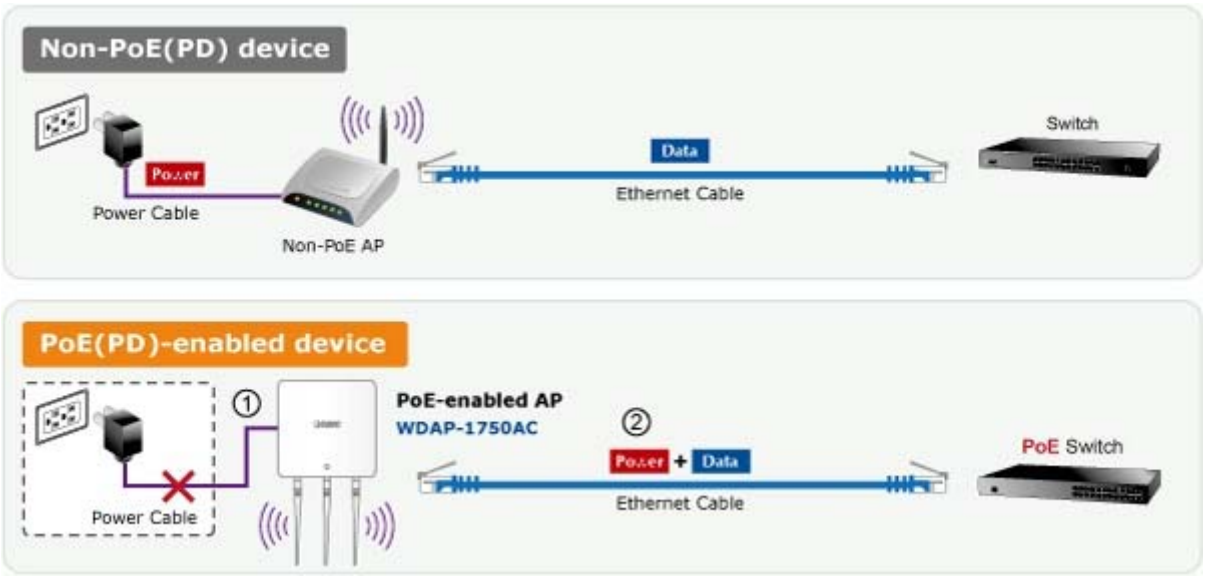
Wall-mount Design Perfect for Room Installation

The WDAP-1750AC is adopted with the latest 802.11ac technology to provide extreme high-speed wireless experience for users. With the stylish wall-mount design, you don't need to spend extra time and cost to deploy the wireless network. Its sleek and fashionable appearance adapted to the room can match any decor without affecting the original interior design. Furthermore, the WDAP-1750AC supports standard 802.3at PoE power scheme, effectively reducing the cabling cost. The WDAP-1750AC, with the SNMP supported, brings the most convenience to system administrators or machine operators. No expensive instruments or complex back-end subscriber managed systems are required for deployment.

Flexible Deployment with PoE Feature

Compliant with the IEEE 802.3at Power over Ethernet standard, the WDAP-1750AC can be powered and networked by a single UTP cable. It thus reduces the needs of extra cables and dedicated electrical outlets on

the wall, ceiling or any other place where it is difficult to reach. The wireless network deployment becomes more flexible and worry-free from the power outlet locations. As it is a highly-reliable industrial wall-mount design, the WDAP-1750AC can be firmly installed on the wall conveniently.



Easy Installation and Management

With user-friendly Web UI, the WDAP-1750AC is easy to install, even for users who never experience setting up a wireless network. Furthermore, with SNMP-based management interface, the WDAP-1750AC is convenient to be managed and configured remotely in a small business wireless network.

1.3 Product Features

- **Standard Compliant Hardware Interface**
  - Complies with IEEE 802.11ac (draft 2.0) and IEEE 802.11a/b/g/n standards
  - 2 x 10/100/1000BASE-TX port with PoE supporting 802.3at and 802.3af PSE (Power Sourcing Equipment).
  - IEEE standard 802.3af/at PoE design
- **RF Interface Characteristics**
  - Features 2.4GHz (802.11b/g/n) and 5GHz (802.11a/n/ac) concurrent dual band for more efficiency of carrying high load traffic
  - 3T3R MIMO technology for enhanced throughput and coverage
  - Provides multiple adjustable transmit power control
  - High speed up to 1.75Gbps (450Mbps for 2.4GHz + 1300Mbps for 5GHz) wireless data rate
- **Comprehensive Wireless Advanced Features**
  - Multiple Wireless Modes: AP,WDS PtP/ PtMP, and WDS Repeater
  - Supports up to 32 multiple-SSIDs (2.4GHz + 5GHz) to allow users to access different networks through a single AP
  - Supports VLAN function to limit the clients to access the specific internal network resource
  - Supports WMM (Wi-Fi Multimedia) and wireless QoS to enhance the efficiency of multimedia application
  - Supports wireless schedule to automatically enable or disable the wireless function based on predefined schedule. *Future firmware supports
- **Secure Network Connection**
  - Advanced security: 64/128-bit WEP, WPA / WPA2, WPA-PSK / WPA2-PSK (TKIP/AES encryption) and 802.1x Radius Authentication
  - Supports MAC address Filtering
- **Easy Installation & Management**
  - Flexible Deployment with Standard 802.3at PoE/ PD supported
  - Web-based configuration of HTTP/HTTPS/SSH/CLI
  - SNMP-based management interface
  - System status monitoring includes DHCP Client, System Log

1.4 Product Specifications

Product	**WDAP-1750AC**	
Hardware Specifications		
Interfaces	LAN 1 (PoE In)	10/100/1000BASE-T Auto MDI/MDI-X RJ45 port
	LAN 2 (PoE Out)	10/100/1000BASE-T Auto MDI/MDI-X RJ45 port with 802.3af PoE injector
	USB	USB port for system log and system configuration file
	Console	1 x RS-232-to-RJ45 serial port (115200, 8, N, 1)
Antennas	Gain	3 x 2dBi RP-SMA (Male) dual-band antenna
Button / Switch	Reset	Press over 5 seconds to reset the device to factory default
	WPS	Press for 1~2 seconds to activate WPS function
	Eject	Eject an attached USB device
	Switch	Power ON/Off switch
LED Indicators	PWR Allow LED to turn off via software control	
Material	Plastic	
Dimensions (WxDxH)	182 x 182 x 30mm	
Weight	470g	
Power Requirements	■ DC Input: 12V DC, 4A ■ PoE Input: IEEE 802.3at PoE+, 48~56V DC in-line power	
ESD Protection	±8kV air-gap discharge, ±4kV contact discharge	
Mounting	Wall mount / Desktop	
Wireless Interface Specifications		
Standard	IEEE 802.11ac (draft 2.0) 5GHz IEEE 802.11a/n 5GHz IEEE 802.11b/g/n 2.4GHz	
Antenna Structure	802.11ac: 3T3R MU-MIMO 802.11n: 3T3R MIMO	
Modulation	DSSS	
Data Modulation	802.11ac: OFDM (BPSK / QPSK / 16QAM / 64QAM / 256QAM) 802.11a/g/n: OFDM (BPSK / QPSK / 16QAM / 64QAM) 802.11b: DSSS (DBPSK / DQPSK / CCK)	
Band Mode	2.4G / 5G concurrent mode	
Frequency Range	2.4GHz	America/ FCC: 2.412~2.462GHz Europe/ ETSI: 2.412~2.484GHz
	5GHz	America/ FCC: 5.180~5.240GHz, 5.725~5.850GHz Europe/ ETSI: 5.180~5.240GHz
Operating Channels	2.4GHz	America/ FCC: 1~11 Europe/ ETSI: 1~13
	5GHz	America/ FCC: 36, 40, 44, 48, 149, 153, 157, 161, 165 Europe/ ETSI:

		36, 40, 44, 48 5GHz channel list will vary in different countries according to their regulations.
Channel Width	802.11ac: 20/40/80MHz 802.11n: 20/40MHz	
Transmission Distance	802.11ac (draft): up to 30m 802.11n: up to 70m 802.11g: up to 30m The estimated transmission distance is based on the theory. The actual distance will vary in different environments.	
Max. RF Power	**5GHz:** 802.11a 22dBm@6Mbps 22dBm@9Mbps 22dBm@12Mbps 22dBm@18Mbps 22dBm@24Mbps 21dBm@36Mbps 19dBm@48Mbps 18dBm@54Mbp 802.11an(5G) 27.5dBm@MCS0/8/16 26.5dBm@MCS1/9/17 26.5dBm@MCS2/10/18 25.5dBm@MCS3/11/19 25.5dBm@MCS4/12/20 24.5dBm@MCS5/13/21 23.5dBm@MCS6/14/22 22.5dBm@MCS7/15/23 802.11ac 27.5dBm@MCS0 26.5dBm@MCS1 26.5dBm@MCS2 25.5dBm@MCS3 25.5dBm@MCS4 24.5dBm@MCS5 23.5dBm@MCS6 22.5dBm@MCS7 20.5dBm@MCS8 19.5dBm@MCS9	**2.4GHz:** 802.11b 23dBm@1Mbps 23dBm@2Mbps 23dBm@5.5Mbps 23dBm@11Mbps 802.11g 23dBm@6Mbps 23dBm@9Mbps 23dBm@12Mbps 23dBm@18Mbps 23dBm@24Mbps 22dBm@36Mbps 20dBm@48Mbps 19dBm@54Mbps 802.11gn (2.4G) 27.5dBm@MCS0/8/16 26.5dBm@MCS1/9/17 26.5dBm@MCS2/10/18 26.5dBm@MCS3/11/19 25.5dBm@MCS4/12/20 24.5dBm@MCS5/13/21 23.5dBm@MCS6/14/22 22.5dBm@MCS7/15/23
Receive Sensitivity	**5GHz:** 802.11a: -71dBm @ 54Mbps 802.11n (HT20): -87dBm @ MCS0, -67dBm @ MCS7 802.11n (HT40): -84dBm @ MCS0, -63dBm @ MCS7 802.11ac (VHT20): -64dBm @ MCS9	

	802.11ac (VHT40): -61dBm @ MCS9 802.11ac (VHT80): -58dBm @ MCS9
	2.4GHz: 802.11b: -90dBm @1Mbps 802.11g: -70dBm @54Mbps 802.11n (HT20/40): -87dBm @MCS0 802.11n (HT20/40): -67dBm @MCS7
Software Features	
Wireless Mode	■ AP (Access Point) ■ WDS PTP (Point to Point) ■ Repeater (WDS + AP) ■ WDS PTMP (Point to Multipoint)
Encryption Security	■ WEP (64/128-bit) encryption security ■ WPA / WPA2 (TKIP/AES) ■ WPA-PSK / WPA2-PSK (TKIP/AES) ■ 802.1x Authenticator (MD5/TLS/TTLS/PEAP/EAP-FAST, EAP-SIM/MAC Authentication)
Wireless Security	Wireless MAC address filtering, up to 256 entries
	Supports WPS (Wi-Fi Protected Setup)
	Enable/ Disable SSID Broadcast
Wireless Advanced	WMM (Wi-Fi Multimedia), Max. Associated Station Number
	Multiple SSIDs: up to 16 at 2.4GHz and 16 at 5GHz
	Wireless Isolation: Enable it to isolate each connected wireless client from communicating with each other
	WLAN L2 isolation (AP mode)
	Provides wireless statistics
	Tx power control adjustment by %: 10%, 25%, 50%, 75%, 90%, 100%
	Auto-channel: Automatically selecting lease congested channel
Max. Clients	Wired: 253 2.4GHz Wireless: 50 5GHz Wireless: 50
LAN	Built-in DHCP server supporting static IP address distribution
	Supports UPnP
	Supports 802.1Q VLAN, SSID and Ethernet port-based tag/untag VID from 1~4094
System Management	Web-based (HTTP/HTTPS) management interface
	SNMP v1,v2c,v3
	SNTP synchronization
	Firmware upgrade via WEB, USB and FTP
	Supports scheduling reboot
	Supports Smart Discovery Utility*
	Local RADIUS: Radius server built-in with 256 accounts support

Standards Conformance	
IEEE Standards	IEEE 802.11ac (draft 2.0, 3T3R, up to 1300Mbps) IEEE 802.11n (3T3R, up to 450Mbps) IEEE 802.11g IEEE 802.11b IEEE 802.11i IEEE 802.3 10BASE-T IEEE 802.3u 100BASE-TX IEEE 802.3ab 1000BASE-T IEEE 802.3x Flow Control
SNMP MIBs	IEEE 802.11 MIB IEEE 802.1AE LLDP-MIB Bridge MIB Interface MIB
Other Protocols and Standards	CSMA/CA, CSMA/CD, TCP/IP, DHCP, ICMP, SNTP
Environment & Certification	
Temperature	Operating: 0 ~ 50 degrees C Storage: -20 ~ 60 degrees C
Humidity	Operating: 10 ~ 90% (non-condensing) Storage: 5 ~ 90% (non-condensing)
Regulatory	FCC, CE

Chapter 2. Hardware Installation

Please follow the instructions below to connect WDAP-1750AC to the existing network devices and your computers.

2.1 Product Outlook

- **Dimensions**: **(W x D x H)**

  182 x 30 x 182 mm

- **Weight :**

  470g

Figure 2-1 WDAP-1750AC

2.1.1 Panel Layout

Figure 2-2 shows the hardware interface of the WDAP-1750AC.

Hardware Interface

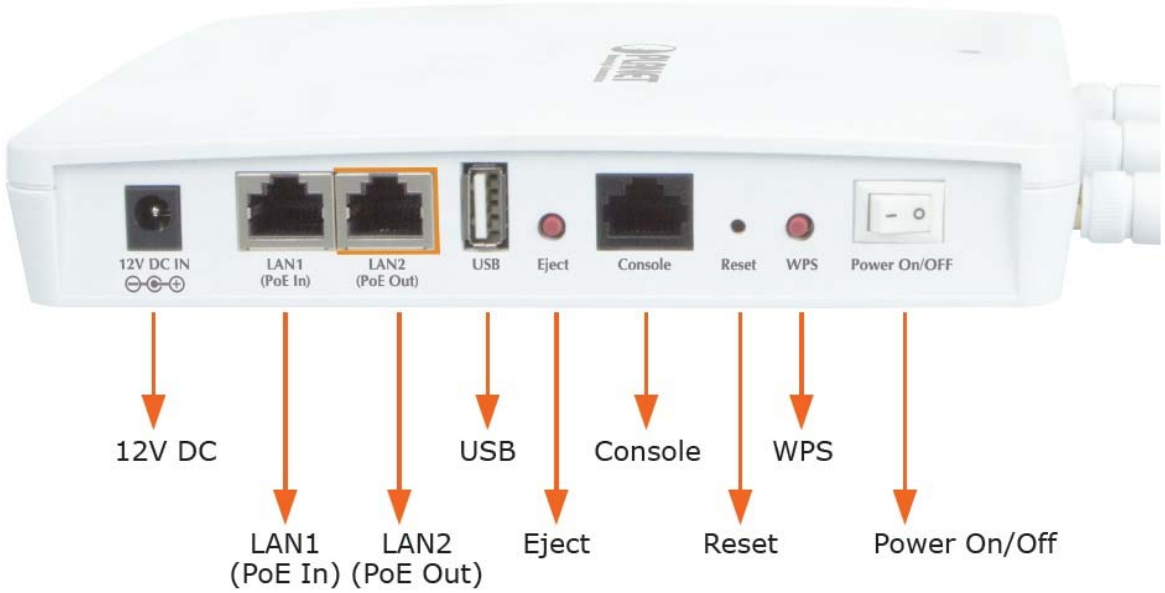


Figure 2-2 WDAP-1750AC Panel Layout

2.1.2 Hardware Description

Port definition

Object	Description
12V DC	12V DC port to connect the power adapter
LAN1 (PoE In)	LAN port with IEEE 802.3at Power over Ethernet (PoE) to power on the device.
LAN2 (PoE Out)	LAN port with IEEE 802.3af Power over Ethernet (PoE) OUT to supply power to the POE IP-CAM.
USB	USB Port for system log
Eject	Eject an attached USB device
Console	Connect a management console
Reset	To restore to the factory default setting, press and hold the Reset Button over 7 seconds, and then release it.
WPS	Wi-Fi Protected Setup (WPS) button
Power On/Off	Switch the access point on/off

LED definition

LED STATUS	FUNCTION
Off	The access point is off.
Blue	The access point is on.
Amber	The access point is starting up.
Flashing Amber	The access point cannot establish a connection to the network.
Flashing Amber and Blue	The access point is experiencing a problem of starting up. The access point will restart.

Chapter 3. Connecting to the AP

3.1 System Requirements

- Broadband Internet Access Service (Cable/xDSL/Ethernet connection)
- One IEEE 802.3at PoE switch (supply power to the WDAP-1750AC)
- PCs with a working Ethernet Adapter and an Ethernet cable with RJ45 connectors
- PCs running Windows 98/ME, NT4.0, 2000/XP, Windows Vista / Win 7, MAC OS 9 or later, Linux, UNIX or other platforms are compatible with **TCP/IP** protocols

Note

1. The AP in the following instructions refers to PLANET WDAP-1750AC.
2. It is recommended to use Internet Explore 7.0 or above to access the AP.

3.2 Installing the AP

Before installing the AP, make sure your PoE switch is connected to the Internet through the broadband service successfully at this moment. If there is any problem, please contact your local ISP. After that, please install the AP according to the following steps. Don't forget to pull out the power plug and keep your hands dry.

Step 1. Attach the two magnetic wall-mount strips to your wall using the included screws, as shown below..

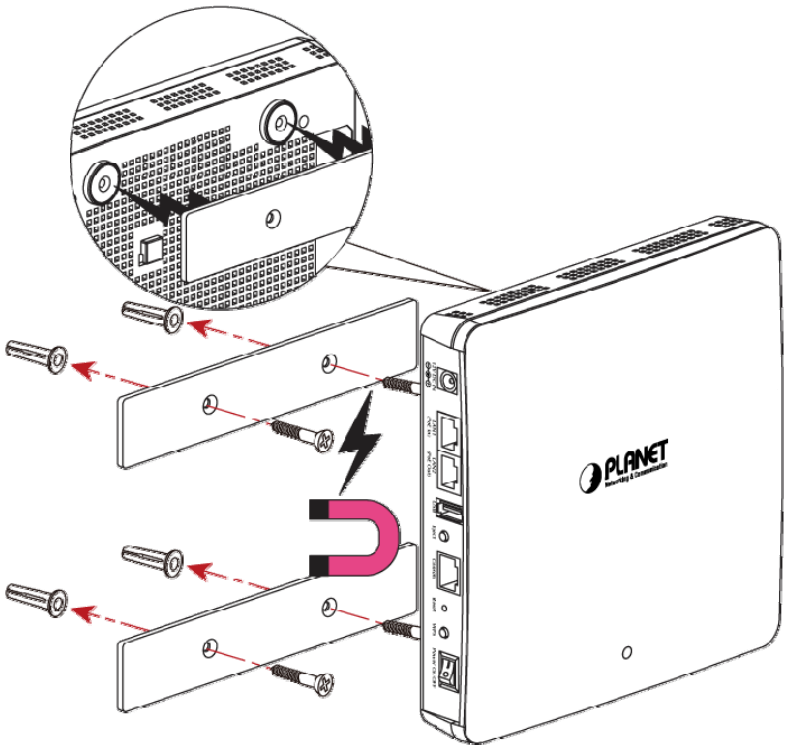


Figure 3-1 WDAP-1750AC Installation Diagram 1

Step 2. Fasten the antennas to the antenna connectors. And you can bend the antennas to fit your actual needs.

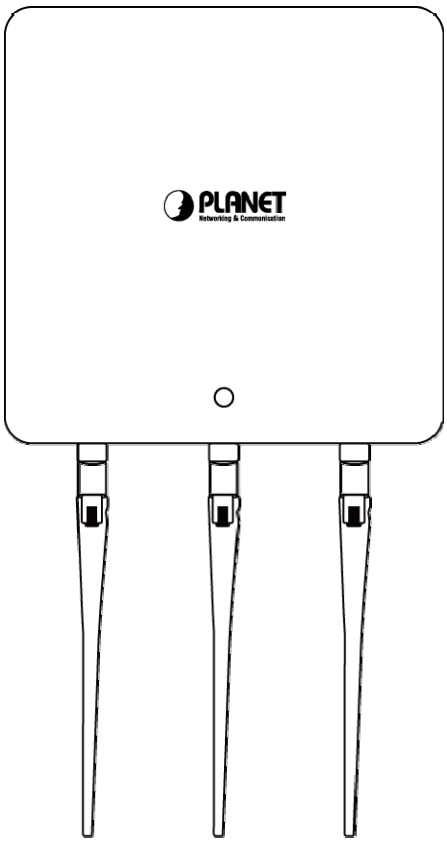


Figure 3-2 WDAP-1750AC Installation Diagram 2

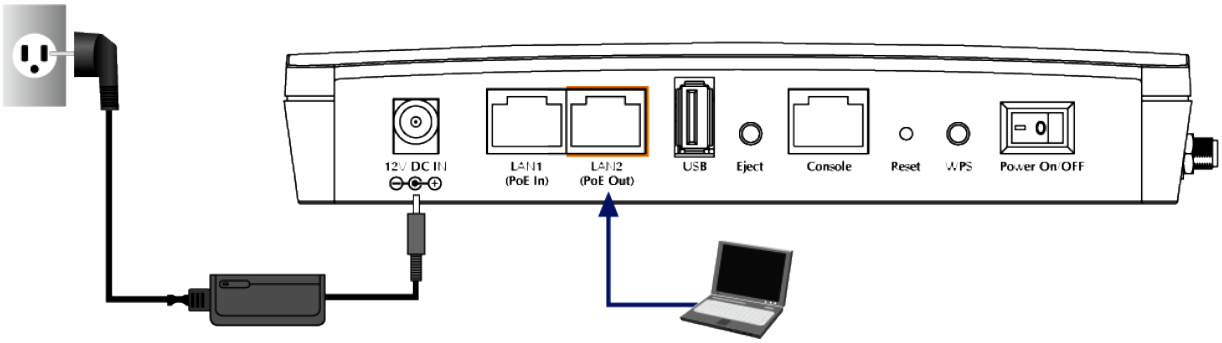
Step 3. Method A - Power socket nearby

Connect he power adapter to the access point's 12V DC port and plug the power adapter into a power source.

Method B – Hard to find the power socket

Plug the RJ45 Ethernet cable into the PoE port of the WDAP-1750AC and the other end of Ethernet cable into the PoE switch.

Method A - Power socket nearby



Method B - Hard to find the power socket

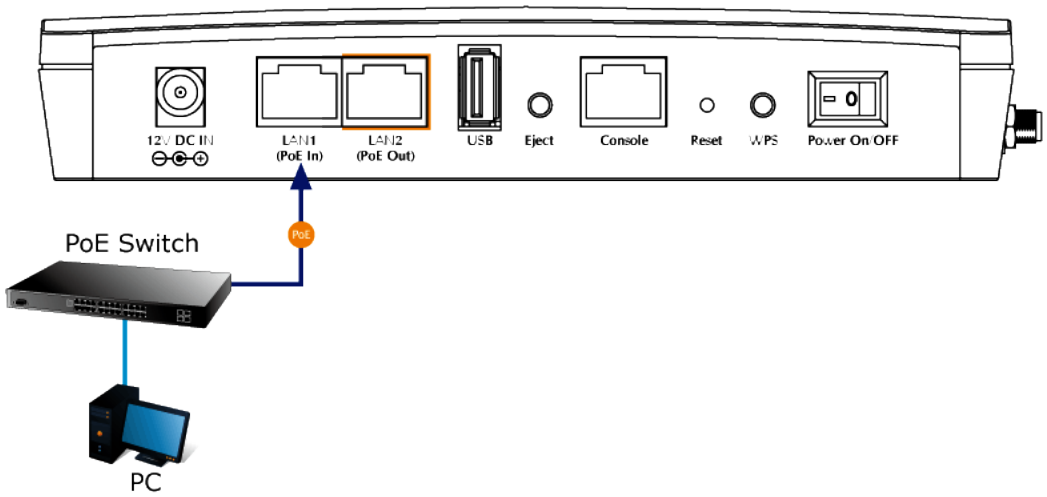


Figure 3-3 WDAP-1750AC Installation Diagram 3

Chapter 4. Quick Installation Guide

This chapter will show you how to configure the basic functions of your AP within minutes.

Note

A computer with wired Ethernet connection to the Wireless AP is required for the first-time configuration.

4.1 Manual Network Setup - TCP/IP Configuration

The default IP address of the WDAP-1750AC 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 WDAP-1750AC with your PC by an Ethernet cable plugging in LAN port on one side and in LAN port of PC on the other side. Please power on the WDAP-1750AC by PoE switch through the PoE port.

In the following sections, we'll introduce how to install and configure the TCP/IP correctly in **Windows 7**. 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.

4.1.1 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 WDAP-1750AC is 192.168.1.253, and the DSL router is 192.168.1.254, the "xxx" can be configured to any number from 1 to 252), Subnet Mask is 255.255.255.0.

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

2 For example, as the default IP address of the WDAP-1750AC is 192.168.1.253 and the DSL router is 192.168.1.254, you may choose from 192.168.1.1 to 192.168.1.252.

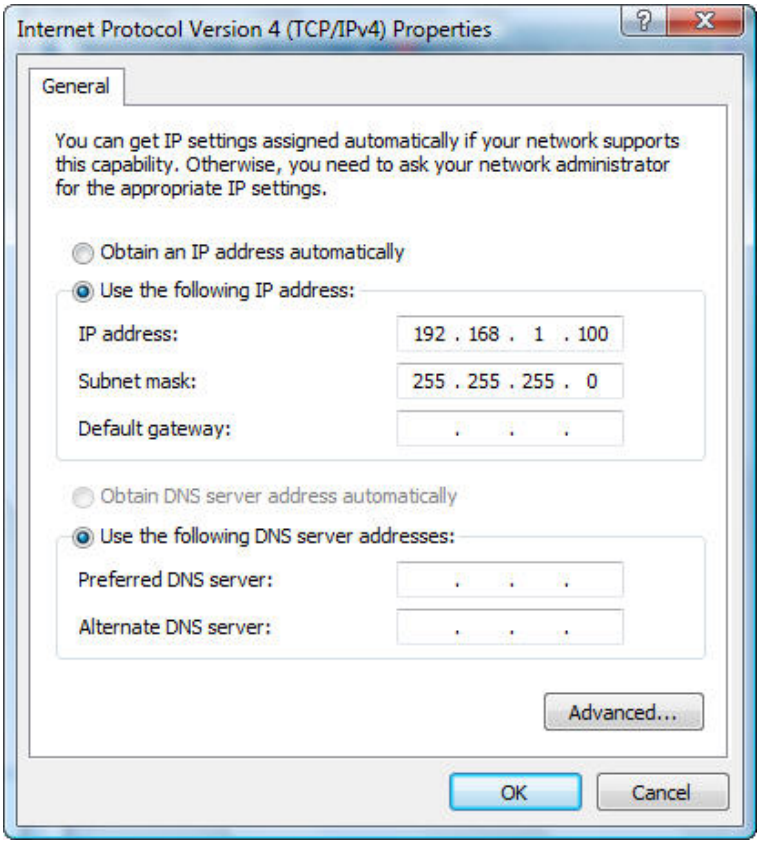


Figure 4-1 TCP/IP Setting

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 7** OS. Please follow the steps below:

1. Click on **Start > Run**.
2. Type "**cmd**" in the Search box.

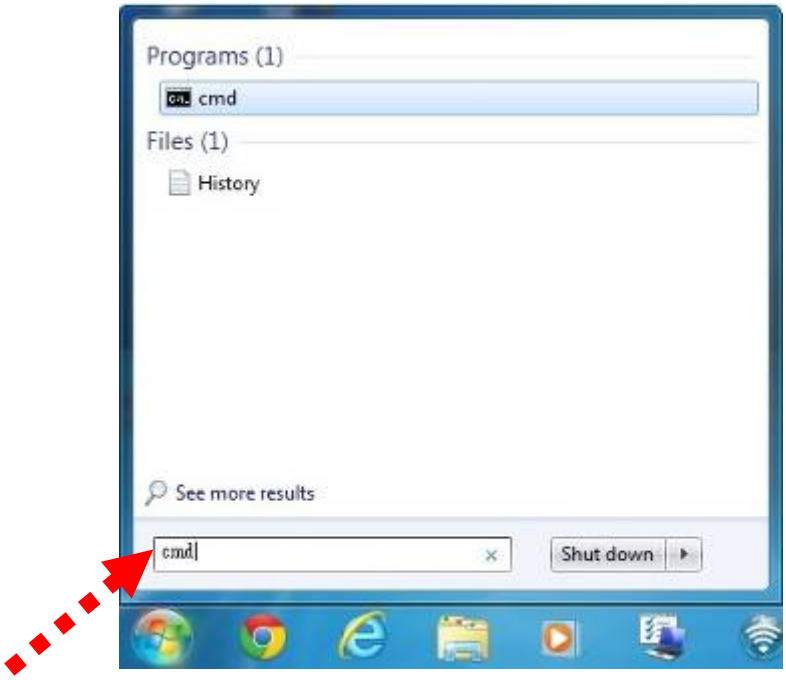


Figure 4-2 Windows Start Menu

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

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

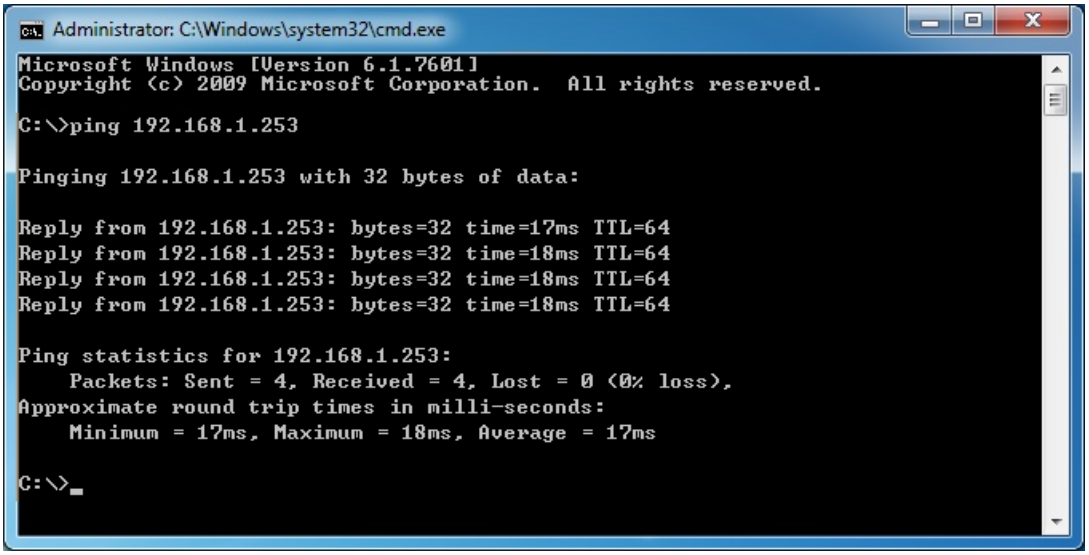


Figure 4-3 Successful Result of Ping Command

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

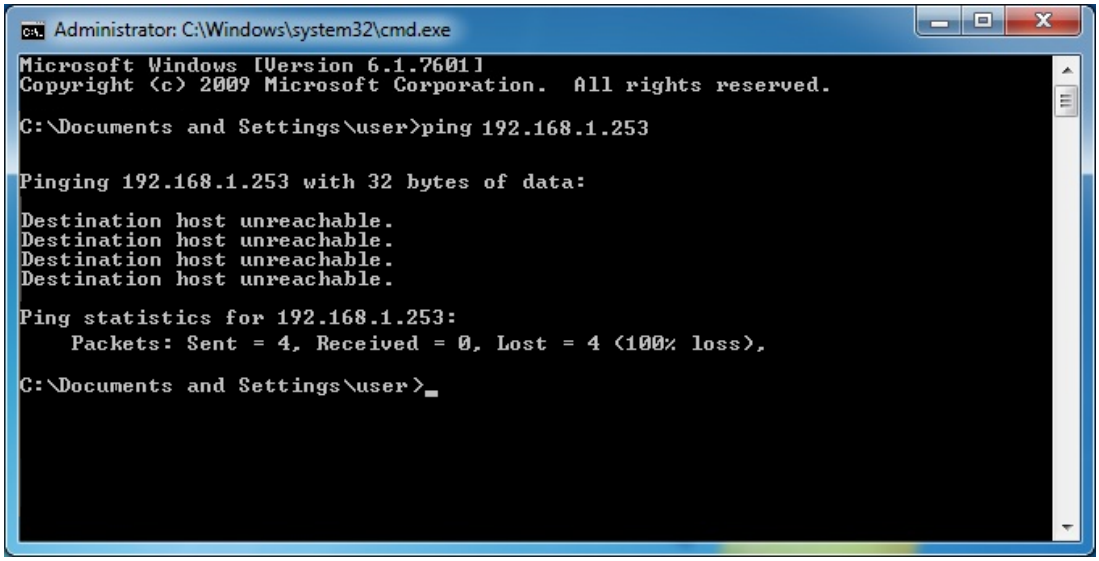


Figure 4-4 Failed Result of Ping Command

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.

4.2 Starting Setup in the Web UI

It is easy to configure and manage the AP with the web browser.

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

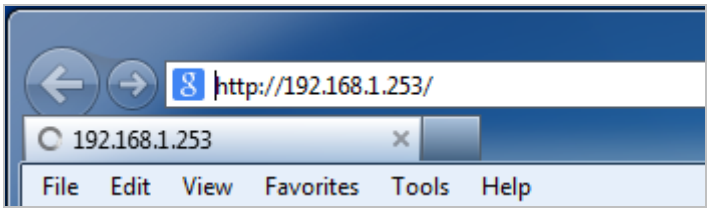


Figure 4-5 Login by default IP address

After a moment, a login window will appear. Enter **admin** for the User Name and Password, both in lower case letters. Then click the **OK** button or press the **Enter** key.

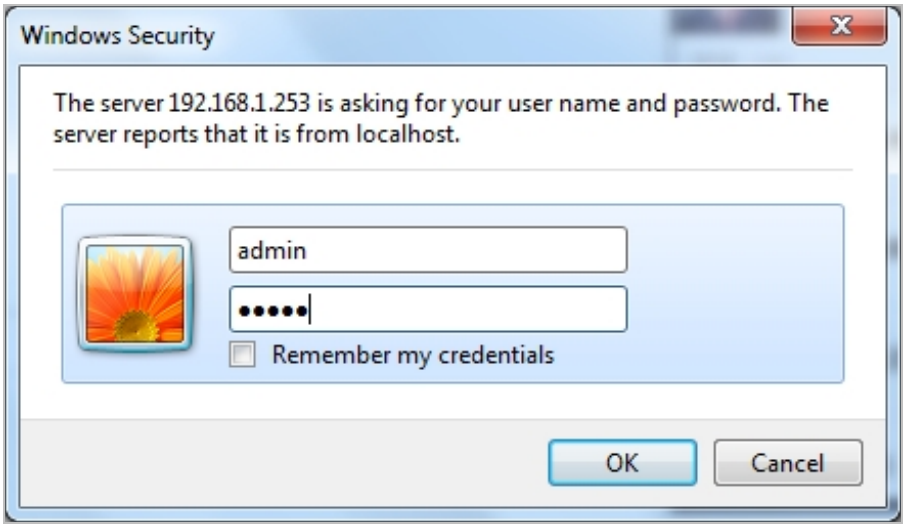


Figure 4-6 Login Window

Default IP Address: **192.168.1.253**

Default User name: **admin**

Default Password: **admin**

Note

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

4.3 Basic Settings

The instructions below will help you to configure the following basic settings of the access point:

- **LAN IP Address**
- **2.4GHz & 5GHz SSID & Security**
- **Administrator Name & Password**
- **Time & Date**

Note

It is recommended you configure these settings before using Planet WDAP-1750AC.

4.3.1 LAN IP Address

1. To change the access point's LAN IP address, go to "Network Settings" > "LAN-side IP Address" and you will see the screen below.

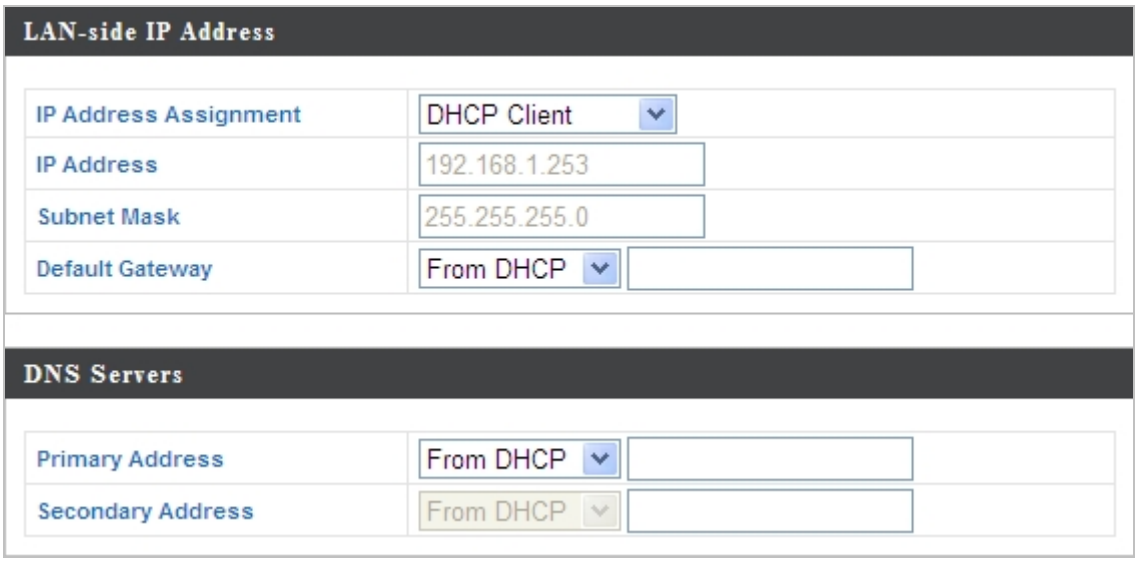


Figure 4-7 Basic Settings **-** DHCP

2. Enter the IP address settings you want to use for your access point. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click "Apply" to save the changes and wait a few moments for the access point to reload.

Note

When you change your access point's IP address, you need to use the new IP address to access the browser based configuration interface instead of the default IP 192.168.1.253.

4.3.2 2.4GHz & 5GHz SSID & Security

1. To change the SSID of your WDAP-1750AC's 2.4GHz wireless network(s), go to "Wireless Setting" > "2.4GHz 11bgn" > "Basic". Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field and click "Apply".

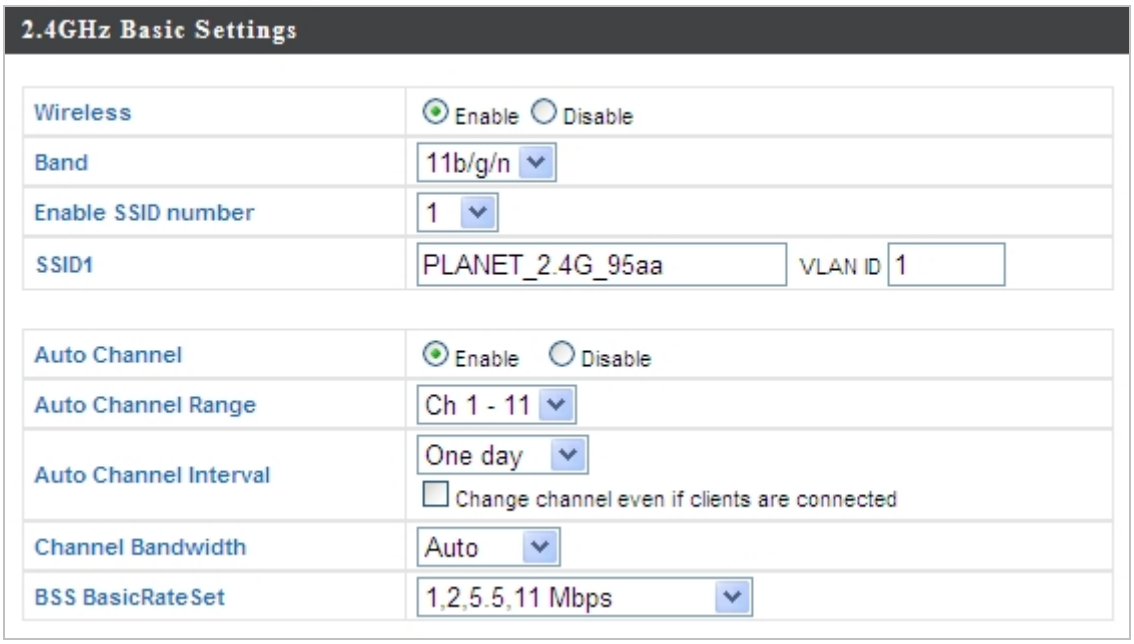


Figure 4-8 Basic Settings - Wireless settings

2. Go to **"Wireless Setting" > "5GHz 11ac 11an"** and repeat steps**1** for the access point's 5GHz wireless network.

4.3.3 Administrator Name & Password

1. To change the administrator name and password for the browser based configuration interface, go to **"Management" > "Admin"**.

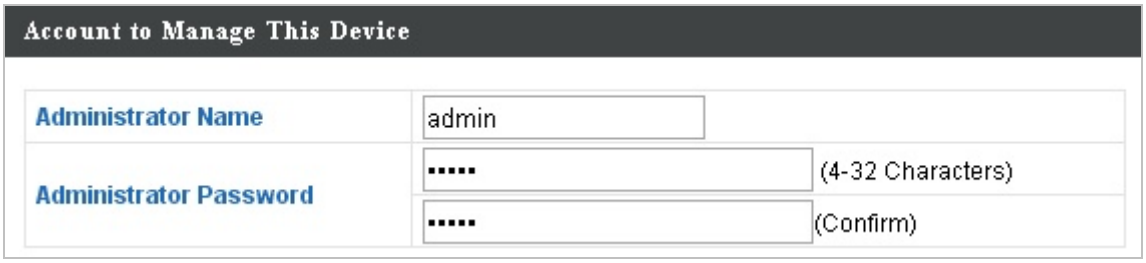


Figure 4-9 Basic Settings - Administrator setting

2. Complete the "Administrator Name" and "Administrator Password" fields and click "Apply".

4.3.4 Time & Date

1. To set the correct time for your access point, go to **"Management" > "Date and Time"**.

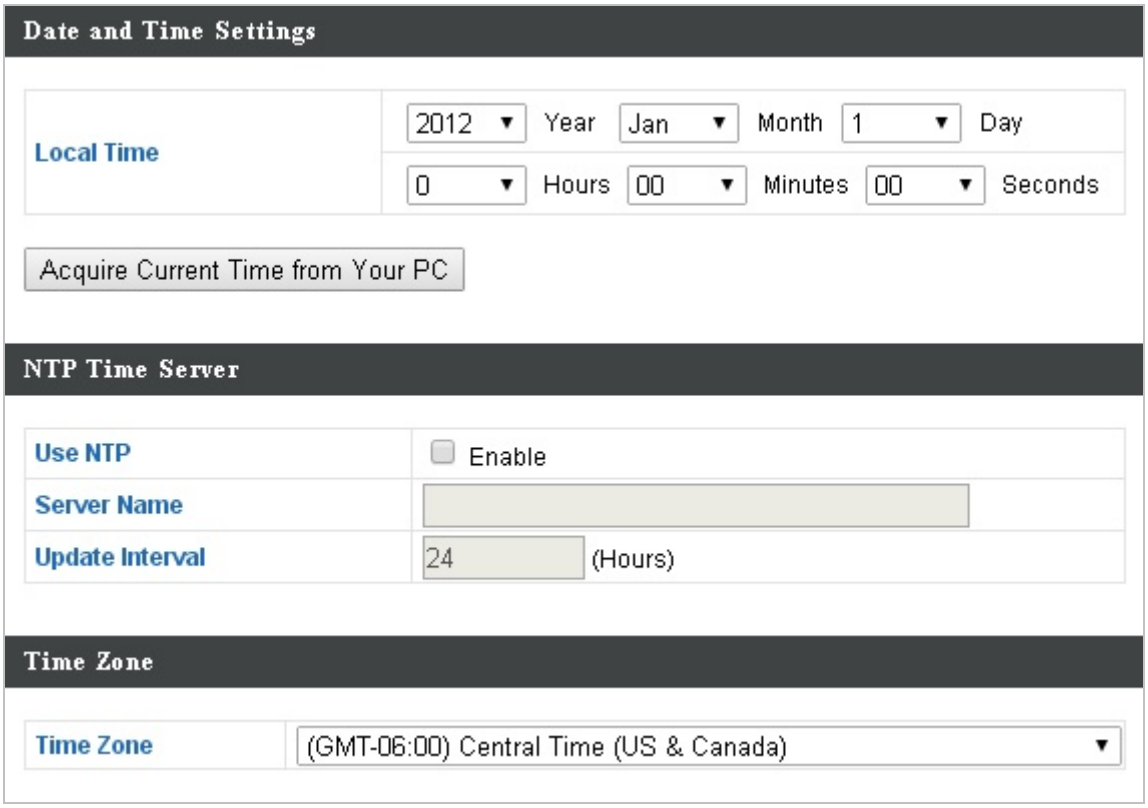


Figure 4-10 Basic Settings - Time & Date

2. Set the correct time and time zone for your access point using the drop down menus. The access point also supports **NTP** (Network Time Protocol) so alternatively you can enter the host name or IP address of a time server. Click "**Apply**" when you are finished.

You can also use the "**Acquire Current Time from your PC**" button if you wish to set the access point to the same time as your PC.

Chapter 5. Configuring the AP

This chapter delivers a detailed presentation of AP's functionalities and features under 5 main menus below, allowing you to manage the AP with ease.

5.1 Information

5.1.1 System Information

The "System Information" page displays basic system information about the access point.

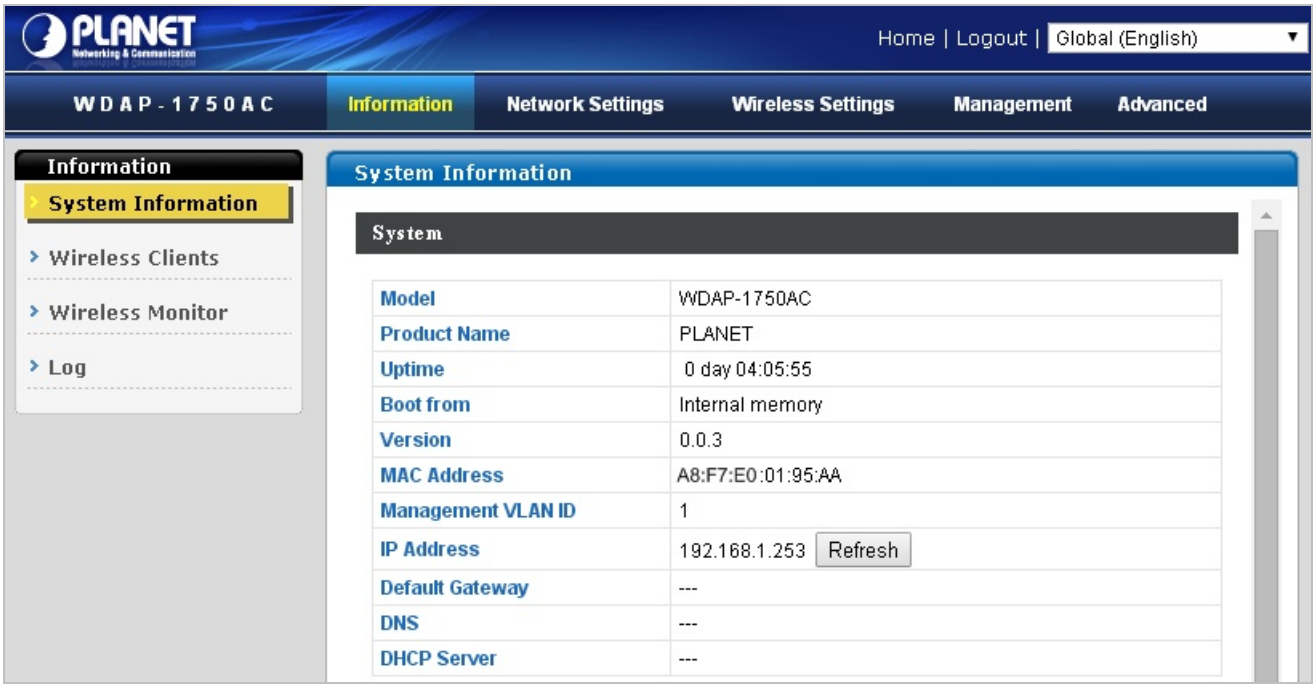


Figure 5-1 Information - Main Menu

The page includes the following information:

Object	Description
Model	Displays the model number of the access point.
Product Name	Displays the product name for reference, which consists of "AP" plus the MAC address.
Uptime	Displays the total time since the device was turned on.
Boot From	Displays information for the booted hardware, booted from either USB or internal memory.
MAC Address	Displays the access point's MAC address.
Management VLAN ID	Displays the management VLAN ID.
Runtime Code Version	Displays the runtime code version.
IP Address	Displays the IP address of this device. Click "Refresh" to update this

	value.
Default Gateway	Displays the IP address of the default gateway.
DNS	IP address of DNS (Domain Name Server)
DHCP Server	IP address of DHCP Server.
Wired LAN Port	Specifies which LAN port (1 or 2).
Status	Displays the status of the specified LAN port (connected or disconnected).
VLAN Mode/ID	Displays the VLAN mode (tagged or untagged) and VLAN ID for the specified LAN port.
Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled or disabled).
MAC Address	Displays the access point's MAC address.
Channel	Displays the channel number the specified wireless frequency is using for broadcast.
Transmit Power	Displays the wireless radio transmitting power level as a percentage.
SSID	Displays the SSID name(s) for the specified frequency.
Authentication Method	Displays the authentication method for the specified SSID.
Encryption Type	Displays the encryption type for the specified SSID.
VLAN ID	Displays the VLAN ID for the specified SSID.
Additional Authentication	Displays the additional authentication type for the specified SSID. See IV-3. Wireless Settings
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID.
Refresh	Click to refresh all information.

5.1.2 Wireless Clients

The "**Wireless Clients**" page displays information about all wireless clients connected to the access point on the 2.4GHz or 5GHz frequency.

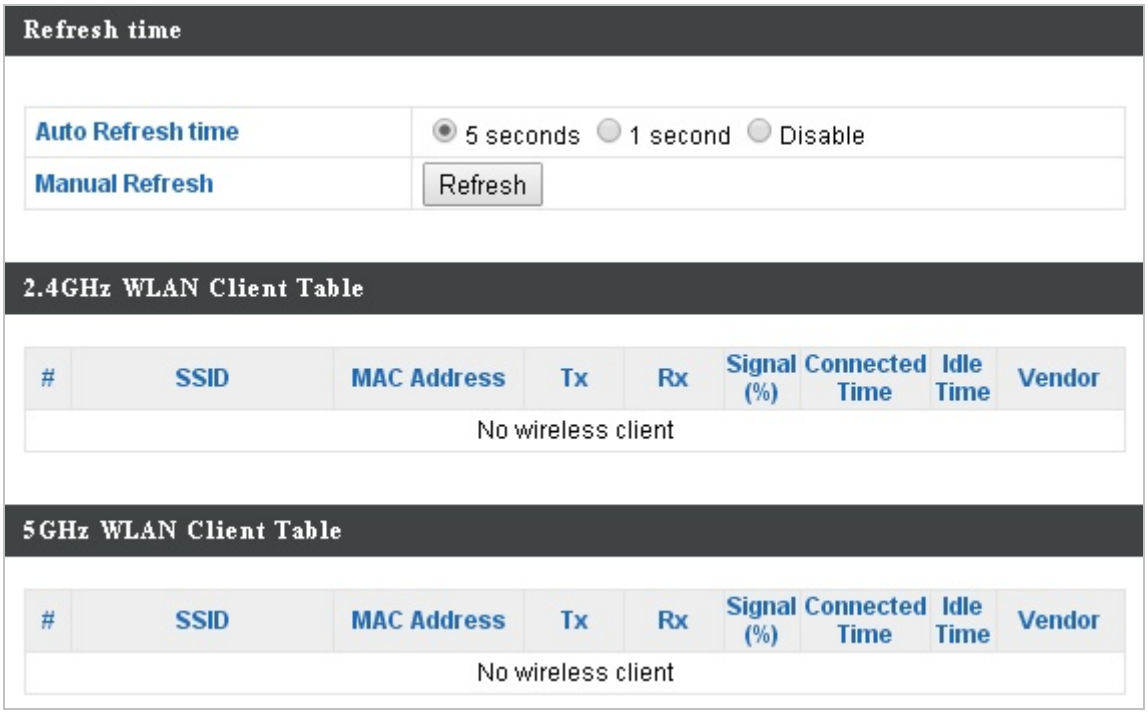


Figure 5-2 Information - Wireless Clients

The page includes the following information:

Object	Description
Auto Refresh Time	Select a time interval for the client table list to automatically refresh.
Manual Refresh	Click refresh to manually refresh the client table.
SSID	Displays the SSID which the client is connected to.
MAC Address	Displays the MAC address of the client.
Tx	Displays the total data packets transmitted by the specified client.
Rx	Displays the total data packets received by the specified client.
Signal (%)	Displays the wireless signal strength for the specified client.
Connected Time	Displays the total time the wireless client has been connected to the access point.
Idle Time	Client idle time is the time for which the client has not transmitted any data packets i.e. is idle.
Vendor	The vendor of the client's wireless adapter is displayed here.

5.1.3 Wireless Monitor

Wireless Monitor is a tool built into the access point to scan and monitor the surrounding wireless environment. Select a frequency and click "**Scan**" to display a list of all SSIDs within range along with relevant details for each SSID.

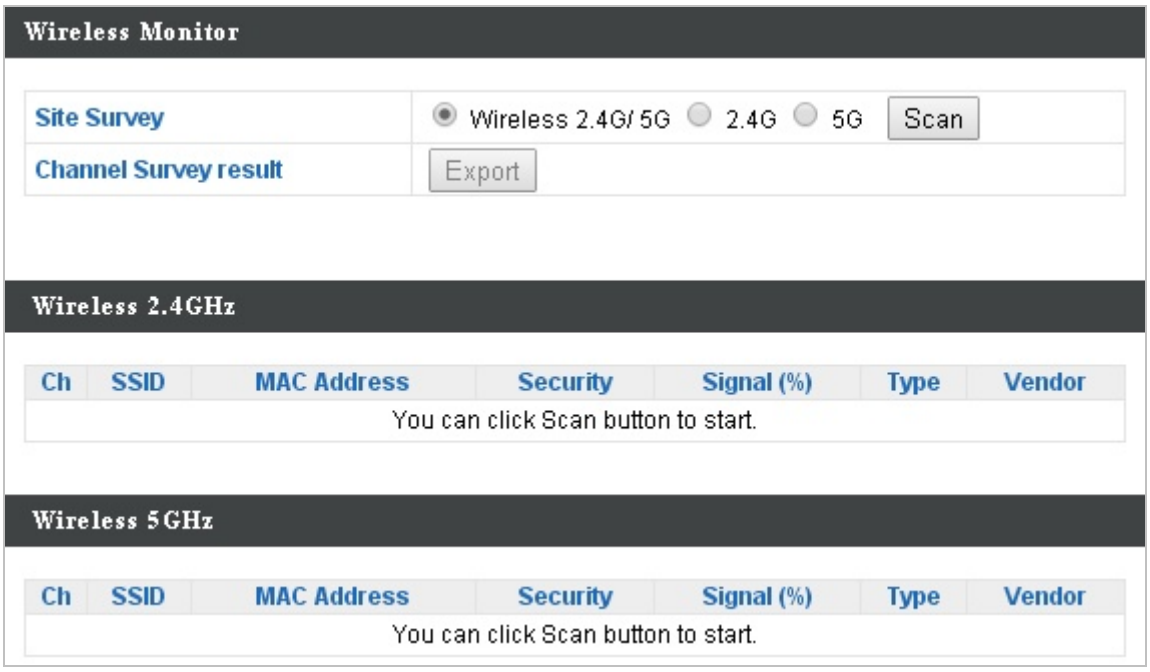


Figure 5-3 Information - Wireless Monitor

The page includes the following fields:

Object	Description
Channel Survey	Select which frequency (or both) to scan, and click "**Scan**" to begin.
Channel Survey Result	After a scan is complete, click "**Export**" to save the results to local storage.
Ch	Displays the channel number used by the specified SSID.
SSID	Displays the SSID identified by the scan.
MAC Address	Displays the MAC address of the wireless router/access point for the specified SSID.
Security	Displays the authentication/encryption type of the specified SSID.
Signal (%)	Displays the current signal strength of the SSID.
Type	Displays the 802.11 wireless networking standard(s) of the specified SSID.
Vendor	Displays the vendor of the wireless router/access point for the specified SSID.

5.1.4 Log

The system log displays system operation information such as up time and connection processes. This information is useful for network administrators.

Figure 5-4 Information - Log

The page includes the following fields:

Object	Description
Save	Click to save the log as a file on your local computer.
Clear	Clear all log entries.
Refresh	Refresh the current log.

5.2 Networking Settings

5.2.1 LAN-side IP Address

The "**LAN-side IP Address**" page allows you to configure your access point on your Local Area Network (LAN). You can enable the access point to dynamically receive an IP address from your router's DHCP server or you can specify a static IP address for your access point, as well as configure DNS servers.

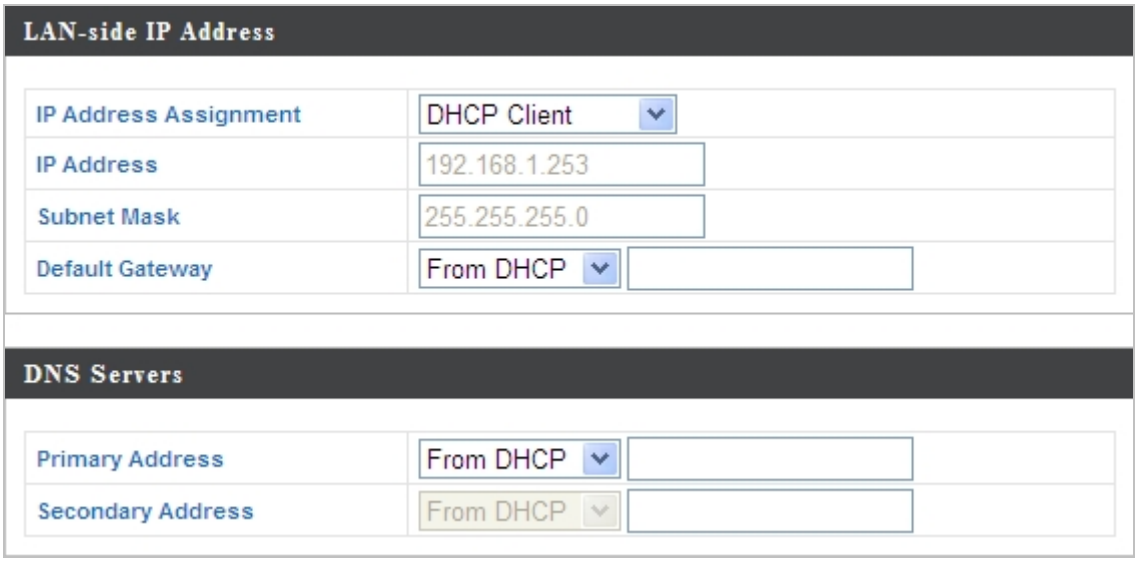


Figure 5-5 Network Settings - LAN-side IP Address

The page includes the following fields:

Object	Description
IP Address Assignment	■ Select "**DHCP Client**" for your access point to be assigned a dynamic IP address from your router's DHCP server. ■ Select "**Static IP**" to manually specify a static/fixed IP address for your access point (below).
IP Address	Specify the IP address here. This IP address will be assigned to your access point and will replace the default IP address.
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select "**From DHCP**" to get default gateway from your DHCP server or "User-Defined" to enter a gateway manually. For static IP users, the default value is blank.

DHCP users can select to get DNS servers' IP address from DHCP or manually enter a value. For static IP users, the default value is blank.

Object	Description
Primary Address	DHCP users can select "**From DHCP**" to get primary DNS server's IP address from DHCP or "User-Defined" to manually enter a value. For static IP users, the default value is blank.
Secondary Address	DHCP users can select "**From DHCP**" to get secondary DNS server's IP address from DHCP or "User-Defined" to manually enter a value. For static IP users, the default value is blank.

5.2.2 LAN Port

The "**LAN Port**" page allows you to configure the settings for your access point's two wired LAN (Ethernet) ports.

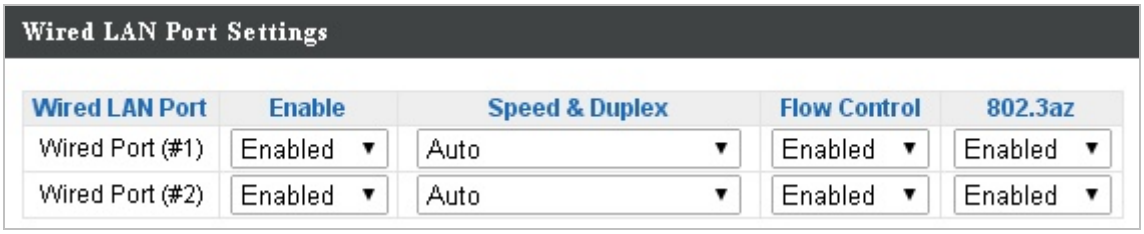


Figure 5-6 Network Settings - LAN Port

The page includes the following fields:

Object	Description
Wired LAN Port	Identifies LAN port 1 or 2.
Enable	Enable/disable specified LAN port.
Speed & Duplex	Select a speed and duplex type for specified LAN port, or use the "**Auto**" value. LAN ports can operate up to 1000Mbps and full-duplex enables simultaneous data packets transfer/receive.
Flow Control	Enable/disable flow control. Flow control can pause new session request until current data processing is complete, in order to avoid device overloads under heavy traffic.
802.3az	Enable/disable 802.3az. 802.3az is an Energy Efficient Ethernet feature which disables unused interfaces to reduce power usage.

5.2.3 VLAN

The "**VLAN**" (Virtual Local Area Network) enables you to configure VLAN settings. A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other. VLAN IDs 0 – 4094 are supported.

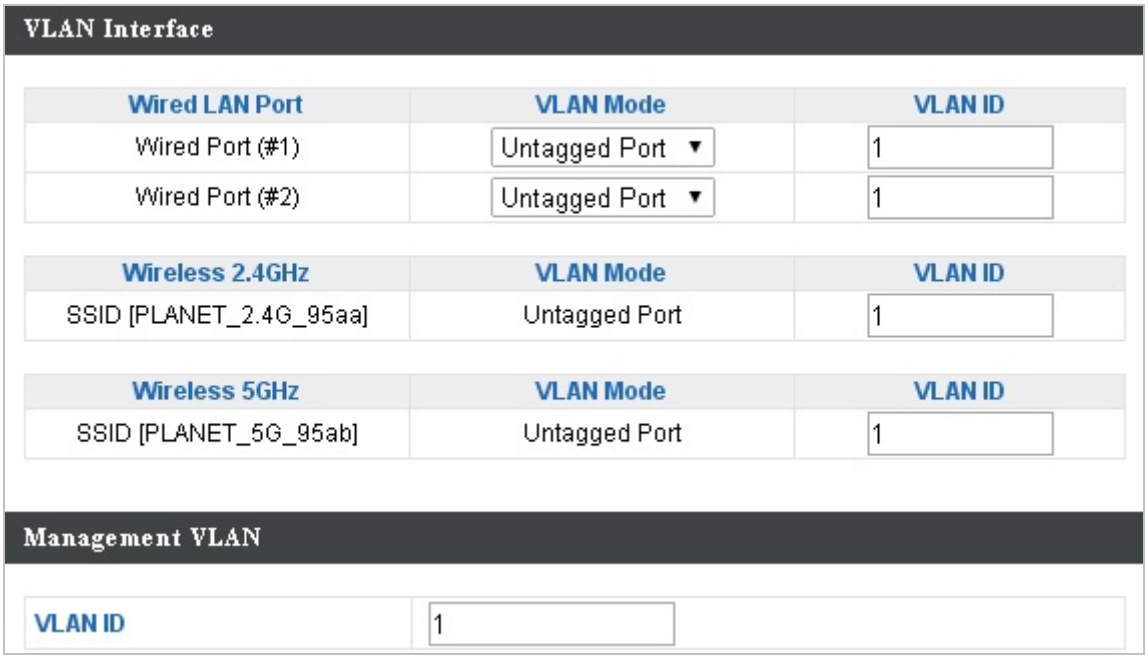


Figure 5-7 Network Settings **-** VLAN

The page includes the following fields:

Object	Description
Wired LAN Port/Wireless	Identifies LAN port 1 or 2, or wireless SSIDs (2.4GHz or 5GHz).
VLAN Mode	Select "**Tagged Port**" or "**Untagged Port**" for specified LAN/wireless interface.
VLAN ID	Set a VLAN ID for specified interface, if "**Untagged Port**" is selected.
Management VLAN ID	Specify the VLAN ID of the subnet. Hosts belonging to the subnet can only communicate with other hosts on the same subnet.

5.3 Wireless Settings

5.3.1 2.4GHz 11bgn Basic Settings

The "**2.4GHz 11bgn**" menu allows you to view and configure information for your access point's 2.4GHz wireless network across four categories: Basic, Advanced, Security and WDS.

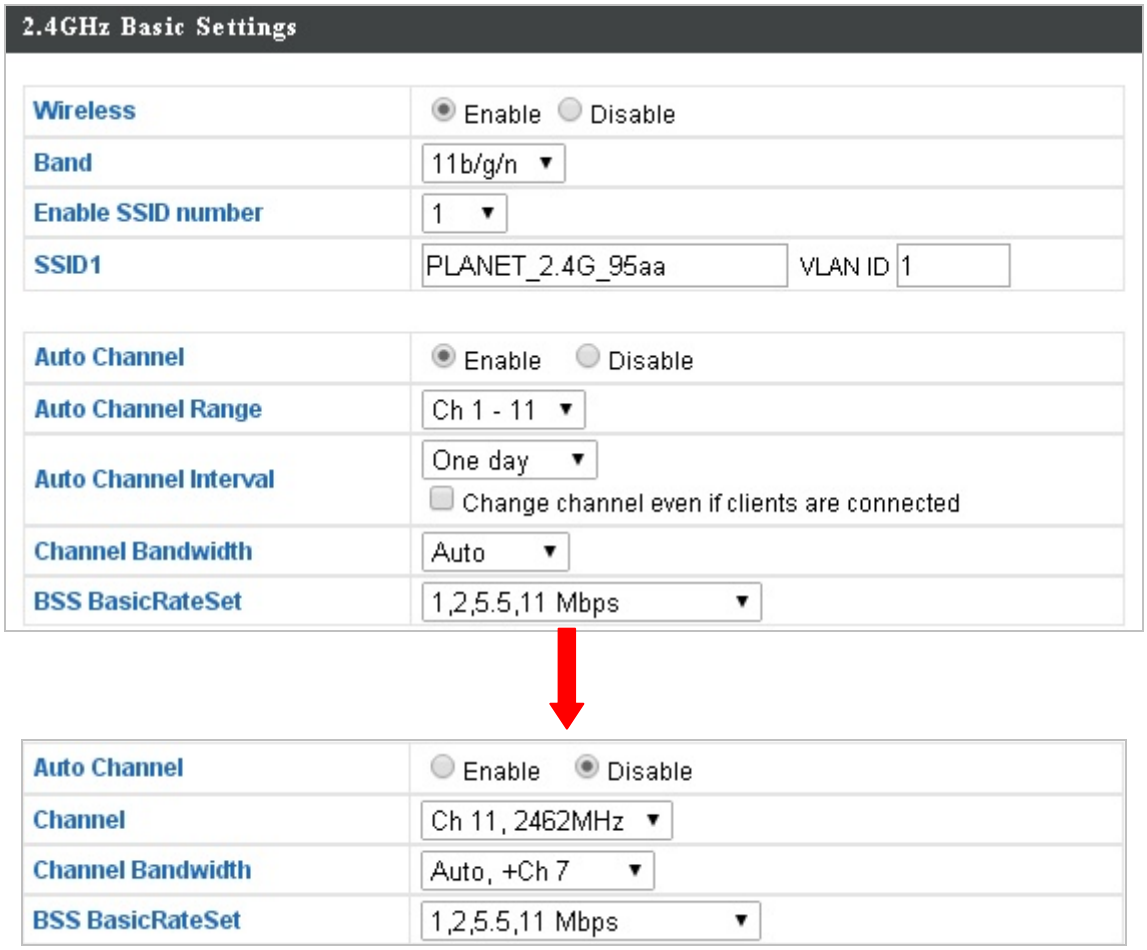


Figure 5-8 2.4GHz Wireless Settings

The page includes the following fields:

Object	Description
Wireless	Enable or disable the access point's 2.4GHz wireless radio. When disabled, no 2.4GHz SSIDs will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g and 802.11n can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 2.4GHz frequency from the drop-down menu. A maximum of **16** can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.

Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel Bandwidth	Set the channel bandwidth: ■ **20MHz** (lower performance but less interference) ■ **40MHz** (higher performance but potentially higher interference) ■ **Auto** (automatically select based on interference level).
BSS Basic Rate Set	Set a Basic Service Set (BSS) rate: this is the transmission rate for controlling communication frames for wireless clients.

When auto channel is disabled, select a wireless channel manually:

Object	Description
Channel Interval	Select a wireless channel from 1 – 11.
Channel Bandwidth	Set the channel bandwidth: ■ 20MHz (lower performance but less interference), ■ 40MHz (higher performance but potentially higher interference) ■ Auto (automatically select based on interference level).
BSS Basic Rate Set	Set a Basic Service Set (BSS) rate: this is the transmission rate for controlling communication frames for wireless clients.

5.3.2 Advanced

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

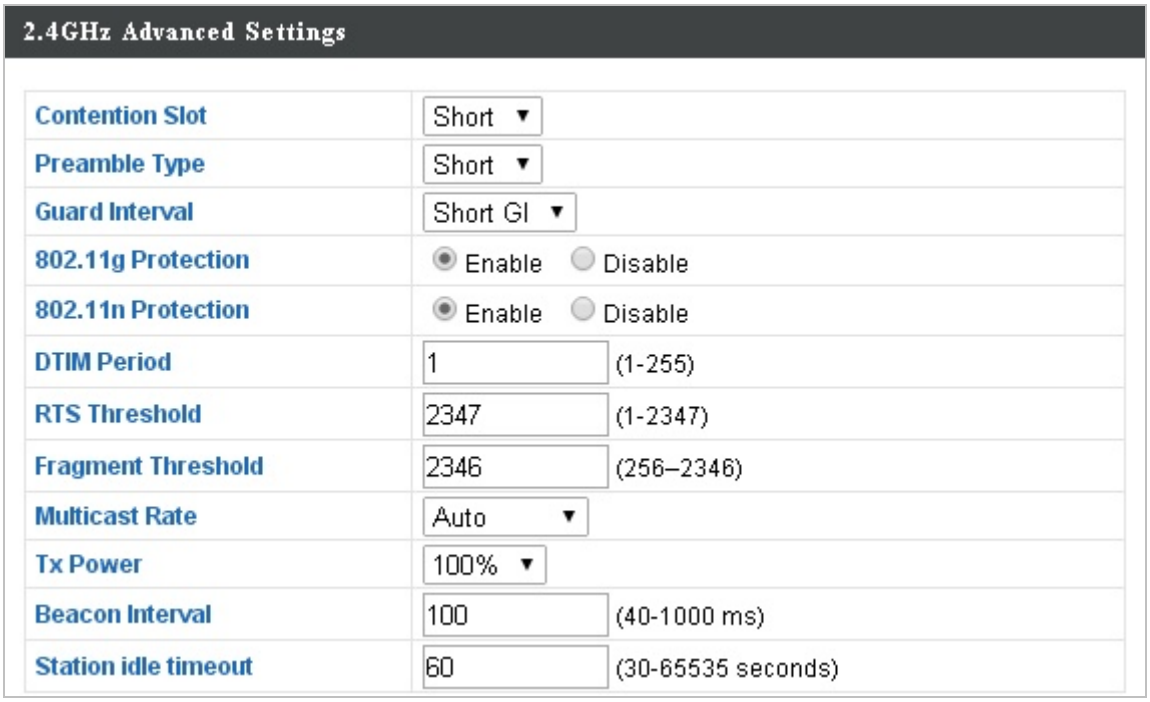


Figure 5-9 2.4GHz Wireless Settings **-** Advanced

The page includes the following fields:

Object	Description
Contention Slot	Select “Short” or “Long” – this value is used for contention windows in WMM.
Preamble Type	Set the wireless radio preamble type. The default value is “**Short Preamble**”.
Guard Interval	Set the guard interval.
802.11g Protection	Enable/disable 802.11g protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is **1**.

RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is **2346**.
Multicast Rate	Set the transfer rate for multicast packets or use the “Auto” setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is **100**.
Station Idle Timeout	Set the time for access point which the client has not transmitted any data packets

Note Changing these settings can adversely affect the performance of your access point.

5.3.3 Security

The access point provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

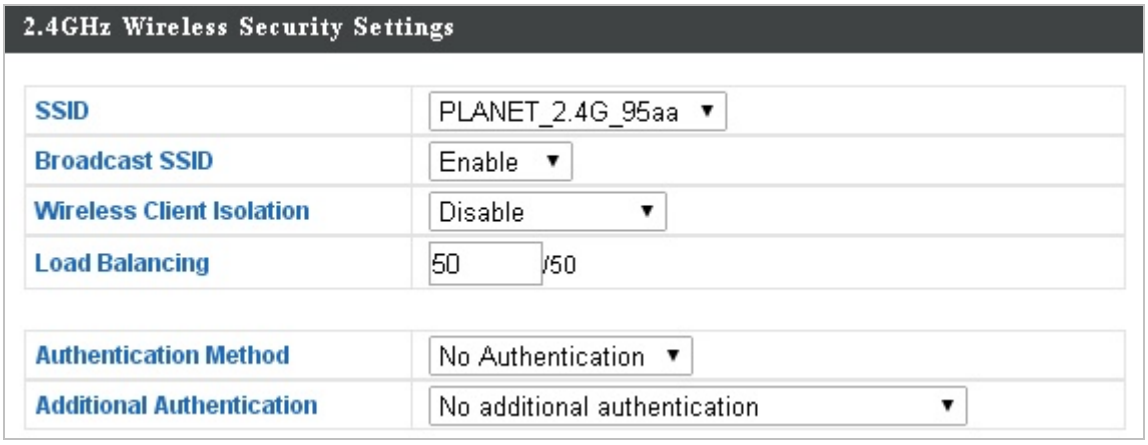


Figure 5-10 2.4GHz Wireless Settings **-** Security

The page includes the following fields:

Object	Description
SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. ■ When **enabled**, the SSID will be visible to clients as an available Wi-Fi network.

	■ When **disabled**, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method.
Additional Authentication	Select an additional authentication method from the drop down menu.

■ **No Authentication**

Authentication is disabled and no password/key is required to connect to the access point.

Note

Disabling wireless authentication is NOT recommended. When disabled, anybody within range can connect to your device's SSID.

■ **WEP**

WEP (Wired Equivalent Privacy) is a basic encryption type. For a higher level of security consider using WPA encryption.

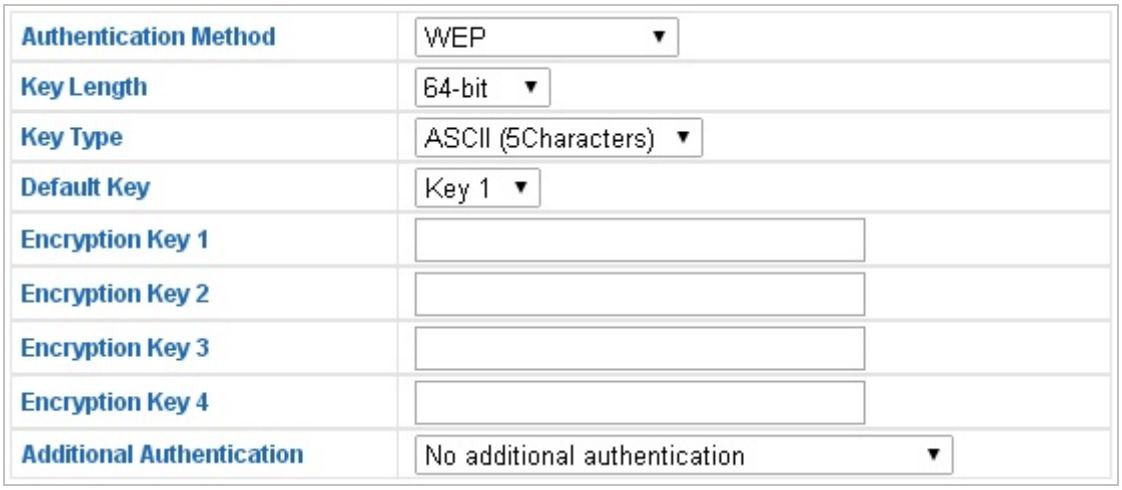


Figure 5-11 2.4GHz Wireless Settings **-** WEP

The page includes the following fields:

Object	Description
Key Length	Select **64-bit** or **128-bit**. 128-bit is more secure than 64-bit and is recommended.
Key Type	Choose from “ASCII” (any alphanumerical character 0-9, a-z and A-Z) or “Hex” (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key (1 – 4 below) is the default key. For security purposes, you can set up to four keys (below) and change which is the default key.
Encryption Key 1 – 4	Enter your encryption key/password according to the format you selected above.

■ **IEEE802.1x/EAP**

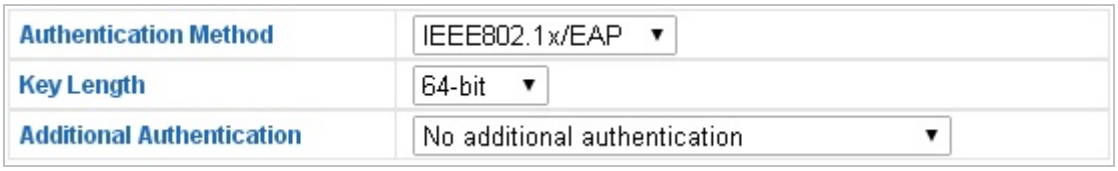


Figure 5-12 2.4GHz Wireless Settings - IEEE802.1x/EAP

The page includes the following fields:

Object	Description
Key Length	Select 64-bit or 128-bit. 128-bit is more secure than 64-bit and is recommended.

■ **WPA-PSK**

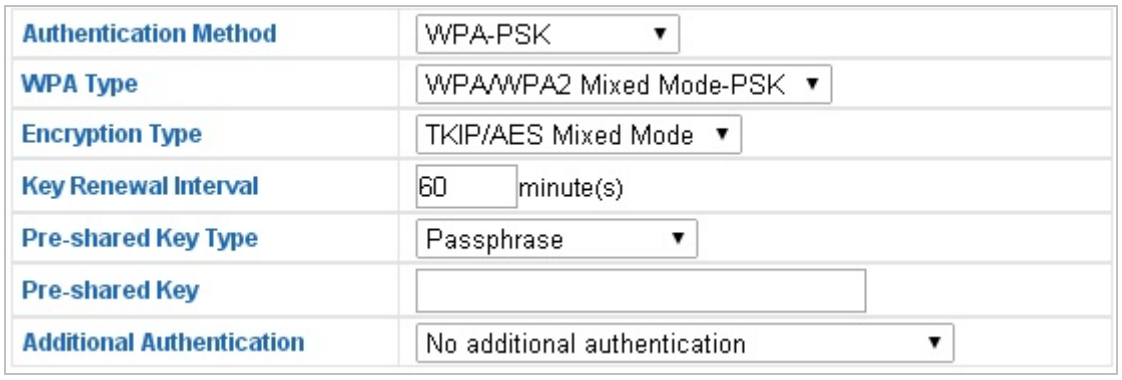


Figure 5-13 2.4GHz Wireless Settings - WPA-PSK

The page includes the following fields:

Object	Description
WPA Type	Select from **WPA/WPA2 Mixed Mode-PSK**, **WPA2** or **WPA** only. WPA2 is safer than WPA only, but not supported by all wireless clients. Please

	make sure your wireless client supports your selection.
Encryption	Select "**TKIP/AES Mixed Mode**" or "**AES**" encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.
Pre-Shared Key Type	Choose from "Passphrase" (8 – 63 alphanumeric characters) or "Hex" (up to 64 characters from 0-9, a-f and A-F).
Pre-Shared Key	Please enter a security key/password according to the format you selected above.

■ **WPA-EAP**

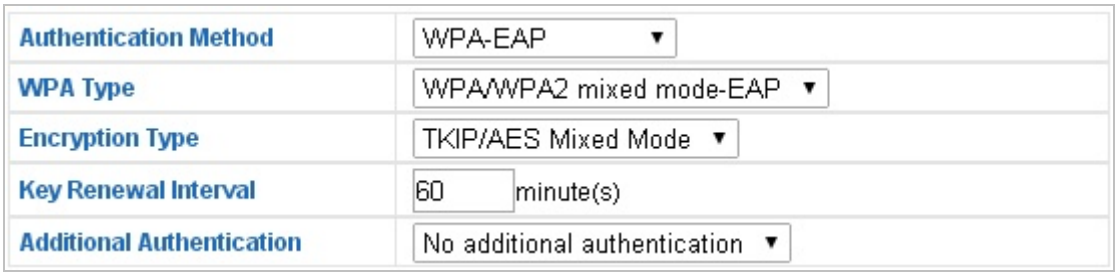


Figure 5-14 2.4GHz Wireless Settings **-** WPA-EAP

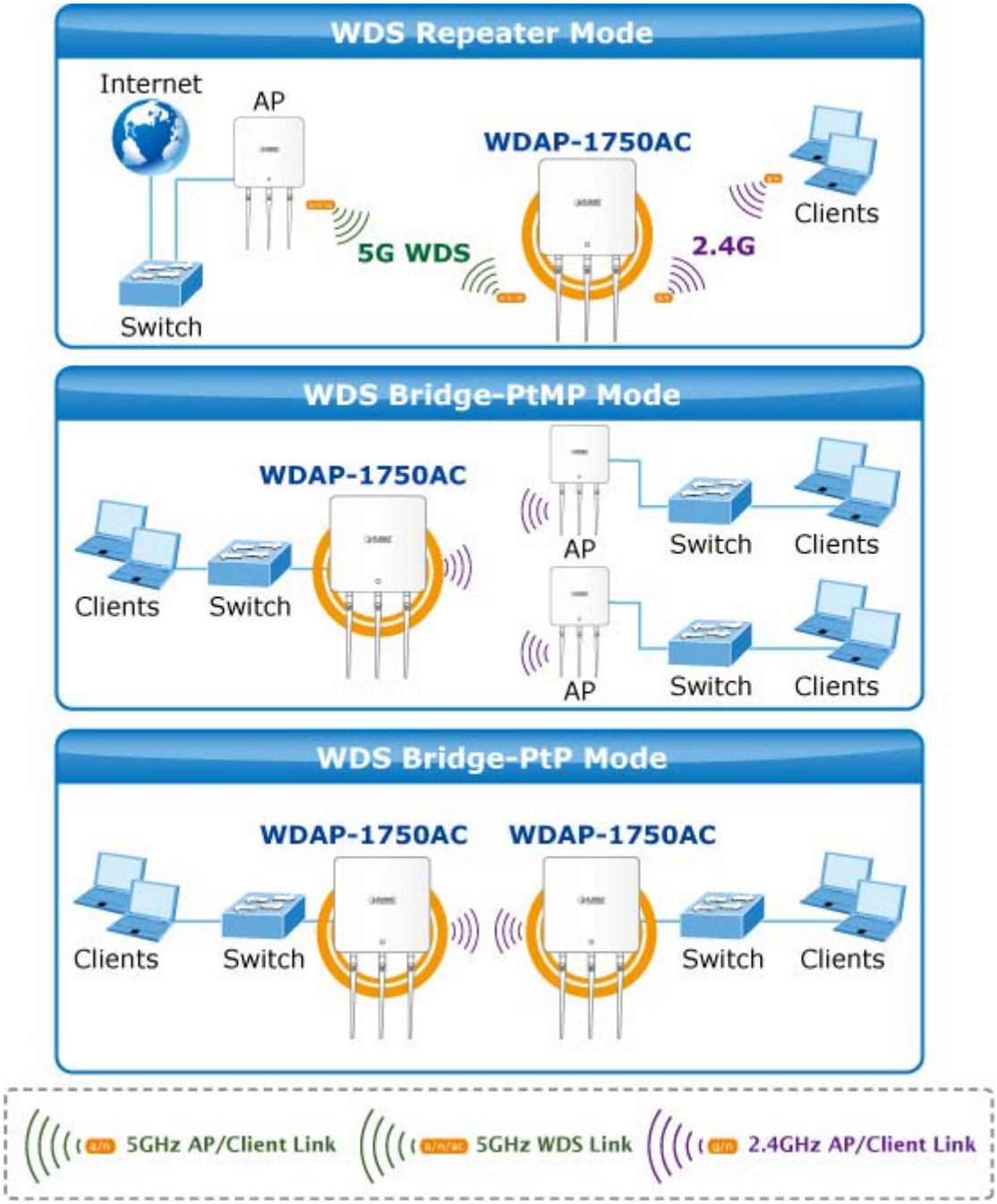
■ **Additional Authentication**

Additional wireless authentication methods can also be used:

Object	Description
MAC address filters	Restrict wireless clients access based on MAC address specified in the MAC filter table.
MAC-RADIUS Authentication	Restrict wireless clients access based on MAC address via a RADIUS server, or password authentication via a RADIUS server.
MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If you select "**Use the following password**", enter the password in the field below. The password should match the "**Shared Secret**".
MAC Filter & MAC-RADIUS Authentication	Restrict wireless clients access using both of the above MAC filtering and RADIUS authentication methods

5.3.4 WDS

Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network.



WDS settings can be configured as shown below. When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.

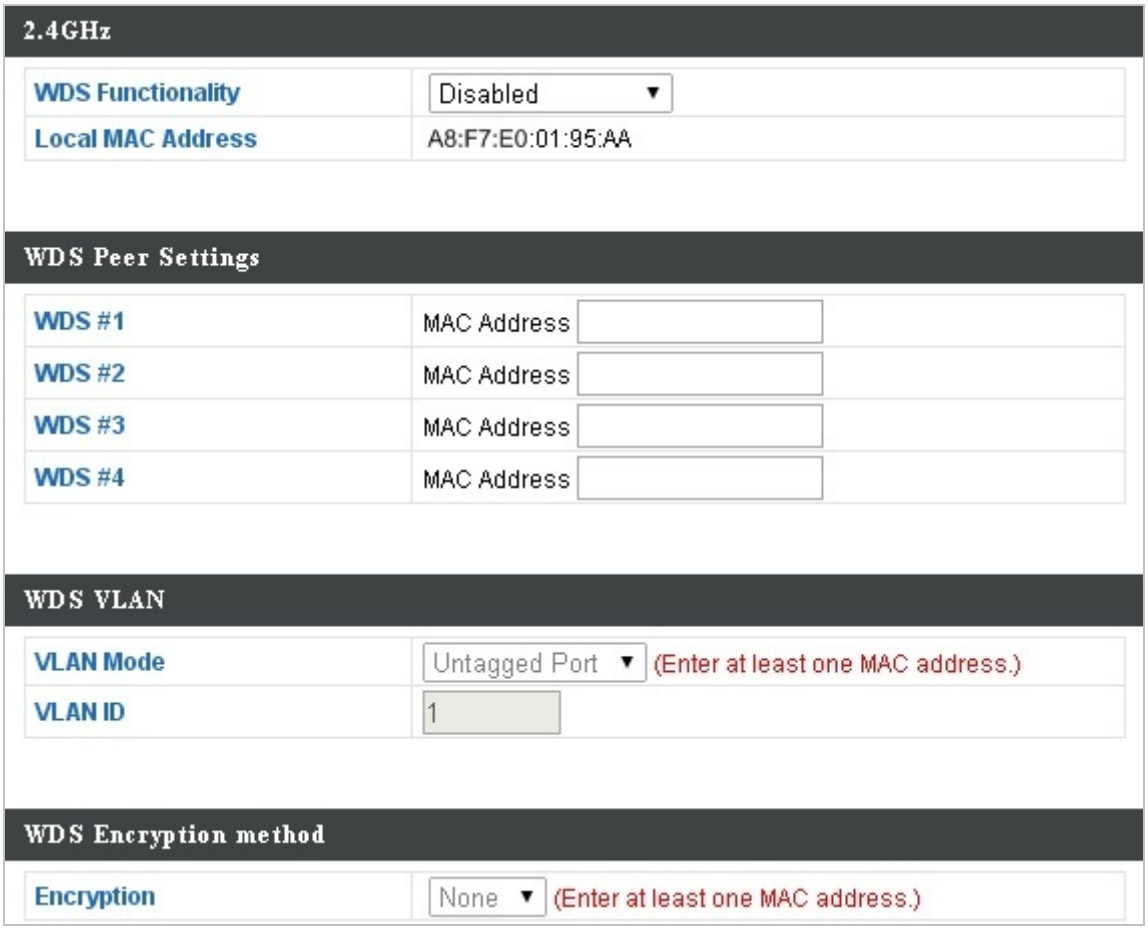


Figure 5-15 2.4GHz Wireless Settings **-** WDS

The page includes the following fields:

Object	Description
WDS Functionality	Select "**WDS with AP**" to use WDS or "**WDS Dedicated Mode**" to use WDS and also block communication with regular wireless clients. When WDS is used, each access point should be configured with corresponding MAC addresses, wireless channel and WEP key.
Local MAC Address	Displays the MAC address of your access point.
WDS #	Enter the MAC address for up to four other WDA devices you wish to connect.
VLAN Mode	Specify the WDS VLAN mode.
VLAN ID	Specify the WDS VLAN ID.
Encryption	Select whether to use "**None**" or "**AES**" encryption and enter a pre-shared key for AES.

Note

WDS must be configured on each access point, using **correct MAC addresses**.
All access points should use the **same wireless channel** and **WEP key**.

5.3.5 5GHz 11ac 11an Basic Settings

The "**5GHz 11ac 11an**" menu allows you to view and configure information for your access point's 5GHz wireless network across four categories: **Basic**, **Advanced**, **Security** and **WDS**.

The "**Basic**" screen displays basic settings for your access point's 5GHz Wi-Fi network (s).

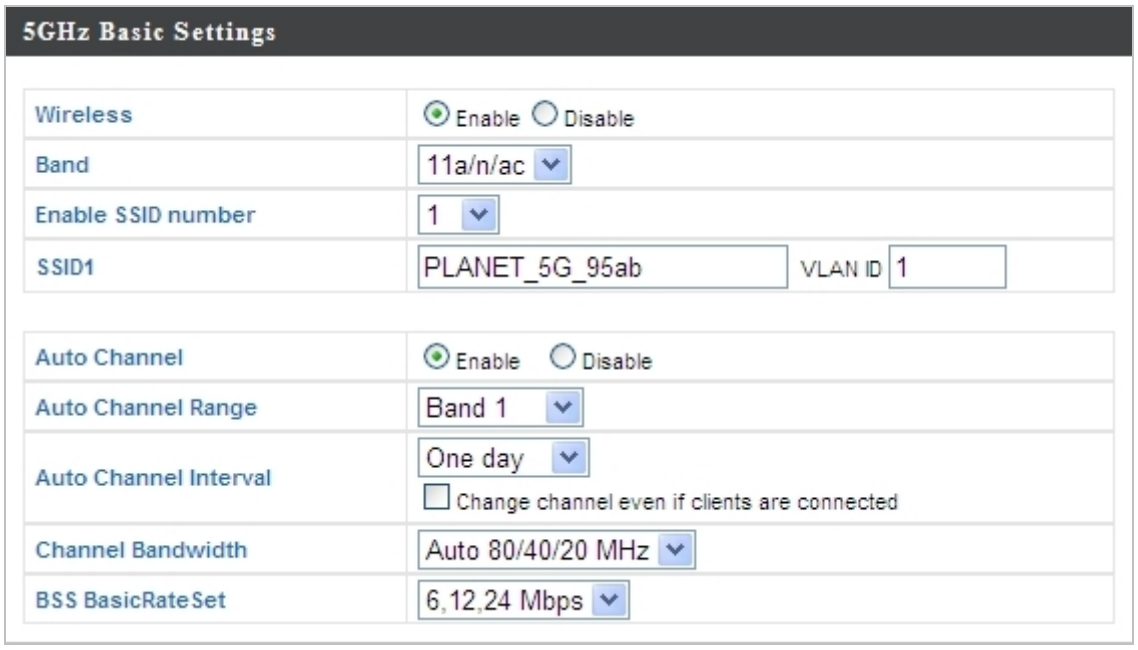


Figure 5-16 5GHz Wireless Settings

The page includes the following fields:

Object	Description
Wireless	Enable or disable the access point's 5GHz wireless radio. When disabled, no 5GHz SSIDs will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11a, 802.11n and 802.11ac can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 5GHz frequency from the drop-down menu. A maximum of **16** can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 5GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.

Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "**Change channel even if clients are connected**" box according to your preference.
Channel Bandwidth	Set the channel bandwidth: ■ **20MHz** (lower performance but less interference) ■ **Auto 40/20MHz** ■ **Auto 80/40/20MHz** (automatically select based on interference level).
BSS Basic Rate Set	Set a Basic Service Set (BSS) rate: this is the transmission rate for controlling communication frames for wireless clients.

When auto channel is disabled, select a wireless channel manually:

Object	Description
Channel Interval	Select a wireless channel.
Channel Bandwidth	Set the channel bandwidth: ■ 20MHz (lower performance but less interference) ■ Auto 40/20MHz ■ Auto 80/40/20MHz (automatically select based on interference level).
BSS Basic Rate Set	Set a Basic Service Set (BSS) rate: this is the transmission rate for controlling communication frames for wireless clients.

5.3.6 Advanced

These settings are for experienced users only. Please do not change any of the values on this page unless you are already familiar with these functions.

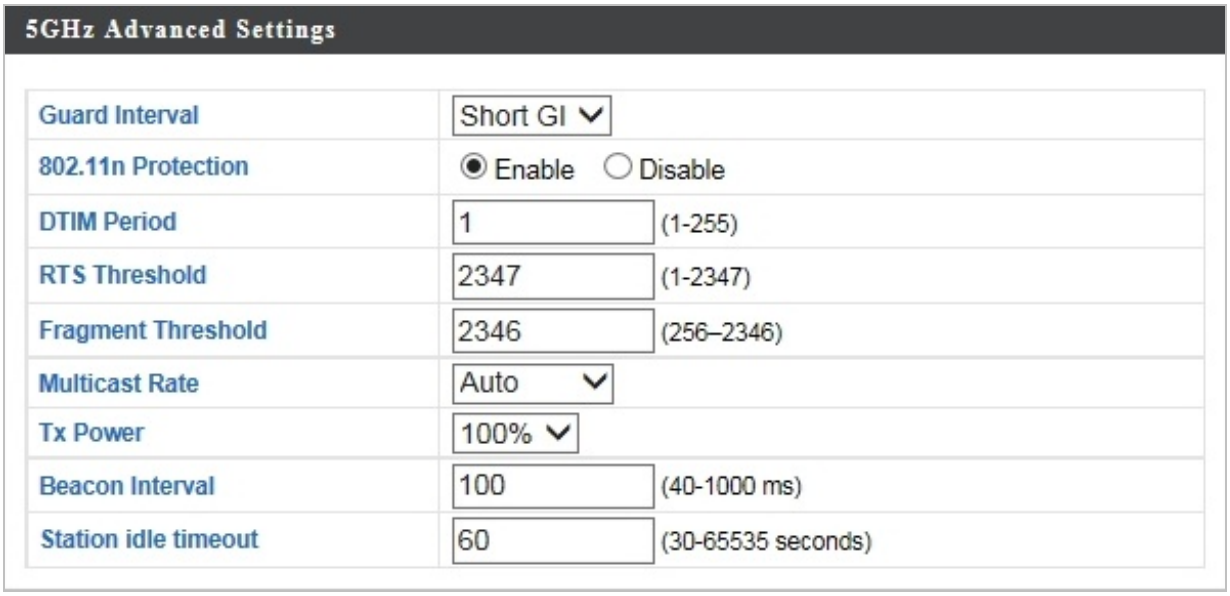


Figure 5-17 5GHz Wireless Settings **-** Advanced

The page includes the following fields:

Object	Description
Guard Interval	Set the guard interval.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is **1**.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is **2347**.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is **2346**.
Multicast Rate	Set the transfer rate for multicast packets or use the "**Auto**" setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is **100**.
Station Idle Timeout	Set the time for access point which the client has not transmitted any data packets

Changing these settings can adversely affect the performance of your access point.

5.3.7 Security

The access point provides various security options (wireless data encryption). When data is encrypted, information transmitted wirelessly cannot be read by anyone who does not know the correct encryption key.

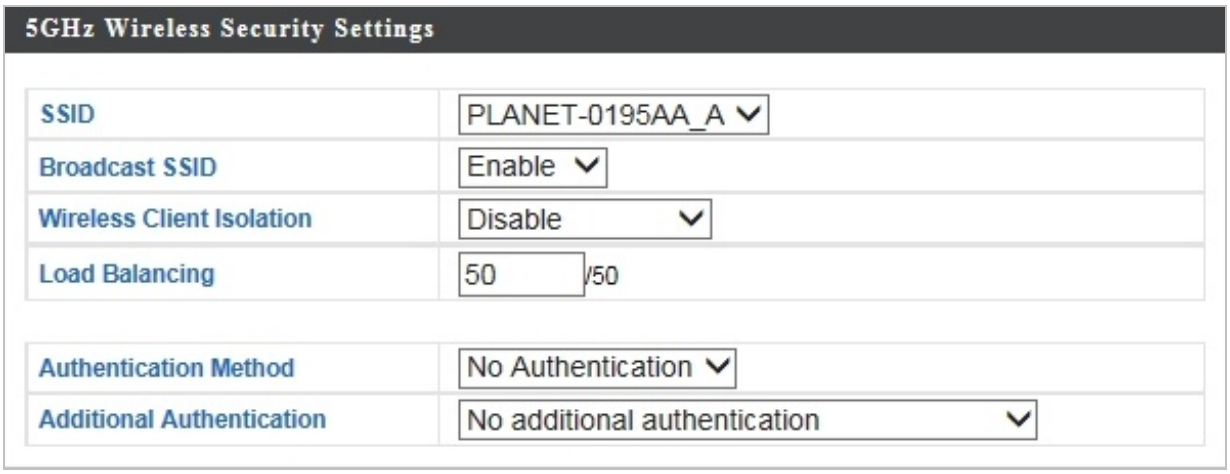


Figure 5-18 5GHz Wireless Settings **-** Security

The page includes the following fields:

Object	Description
SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	**Enable** or **disable** SSID broadcast. ■ When enabled, the SSID will be visible to clients as an available Wi-Fi network. ■ When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	**Enable** or **disable** wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method.
Additional Authentication	Select an additional authentication method from the drop down menu.

■ **No Authentication**

Authentication is disabled and no password/key is required to connect to the access point.

Note

Disabling wireless authentication is **NOT recommended**. When disabled, anybody within range can connect to your device's SSID.

■ **WEP**

WEP (Wired Equivalent Privacy) is a basic encryption type. For a higher level of security consider using WPA encryption.

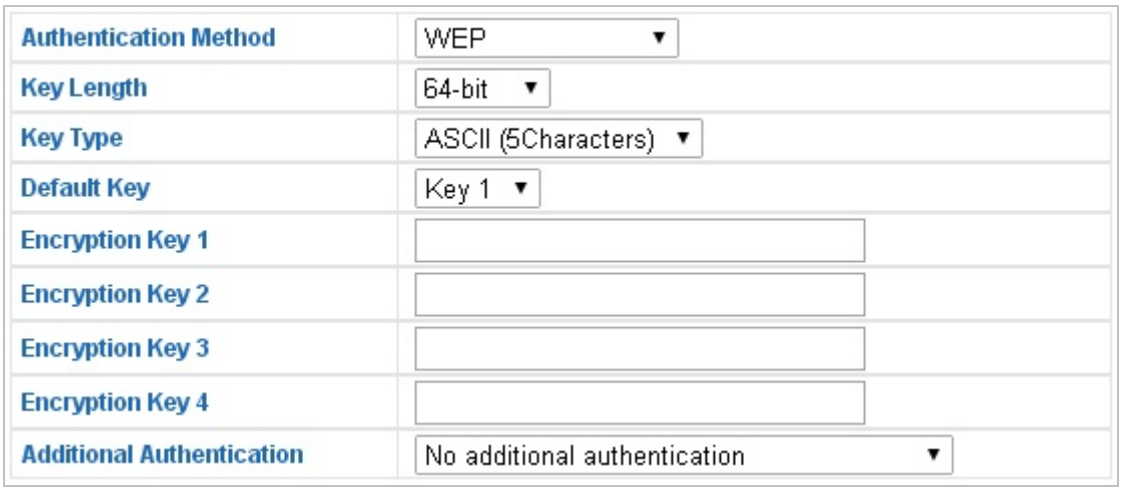


Figure 5-19 5GHz Wireless Settings - WEP

The page includes the following fields:

Object	Description
Key Length	Select **64-bit** or **128-bit**. 128-bit is more secure than 64-bit and is recommended.
Key Type	Choose from "ASCII" (any alphanumerical character 0-9, a-z and A-Z) or "Hex" (any characters from 0-9, a-f and A-F).
Default Key	Select which encryption key (1 – 4 below) is the default key. For security purposes, you can set up to four keys (below) and change which is the default key.
Encryption Key 1 – 4	Enter your encryption key/password according to the format you selected above.

■ **IEEE802.1x/EAP**

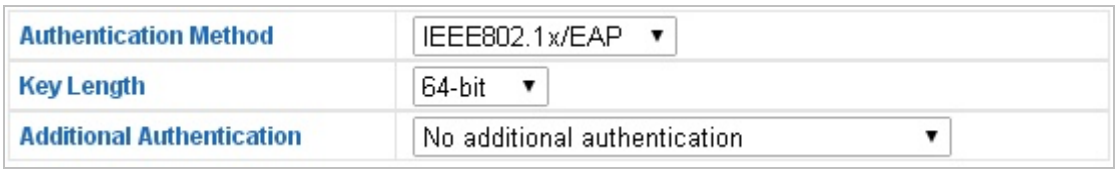


Figure 5-20 5GHz Wireless Settings - IEEE802.1x/EAP

The page includes the following fields:

Object	Description
Key Length	Select **64-bit** or **128-bit**. 128-bit is more secure than 64-bit and is recommended.

■ **WPA-PSK**

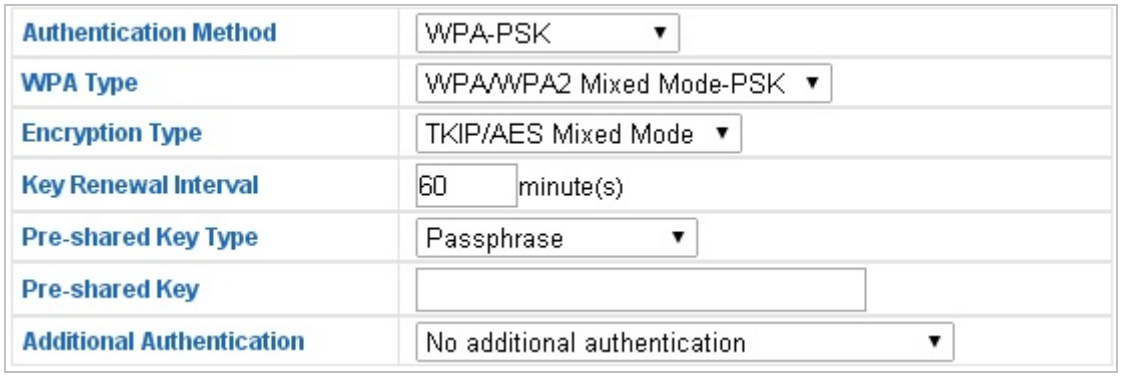


Figure 5-21 5GHz Wireless Settings - WPA-PSK

The page includes the following fields:

Object	Description
WPA Type	Select from **WPA/WPA2 Mixed Mode-PSK**, **WPA2** or **WPA only**. WPA2 is safer than WPA only, but not supported by all wireless clients. Please make sure your wireless client supports your selection.
Encryption	Select "**TKIP/AES Mixed Mode**" or "**AES**" encryption type.
Key Renewal Interval	Specify a frequency for key renewal in minutes.
Pre-Shared Key Type	Choose from "Passphrase" (8 – 63 alphanumeric characters) or "Hex" (up to 64 characters from 0-9, a-f and A-F).
Pre-Shared Key	Please enter a security key/password according to the format you selected above.

■ **WPA-EAP**

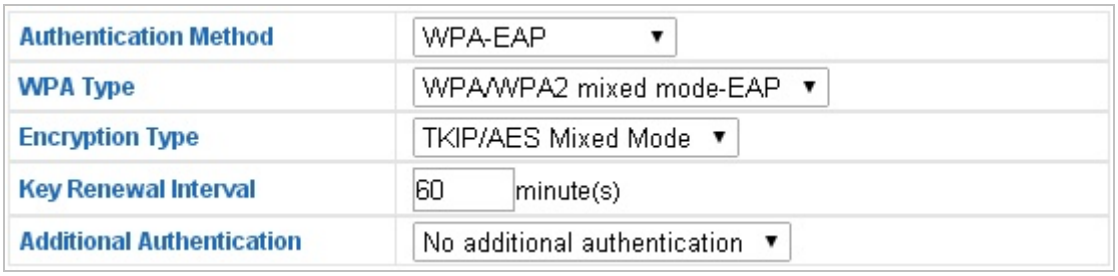


Figure 5-22 5GHz Wireless Settings - WPA-EAP

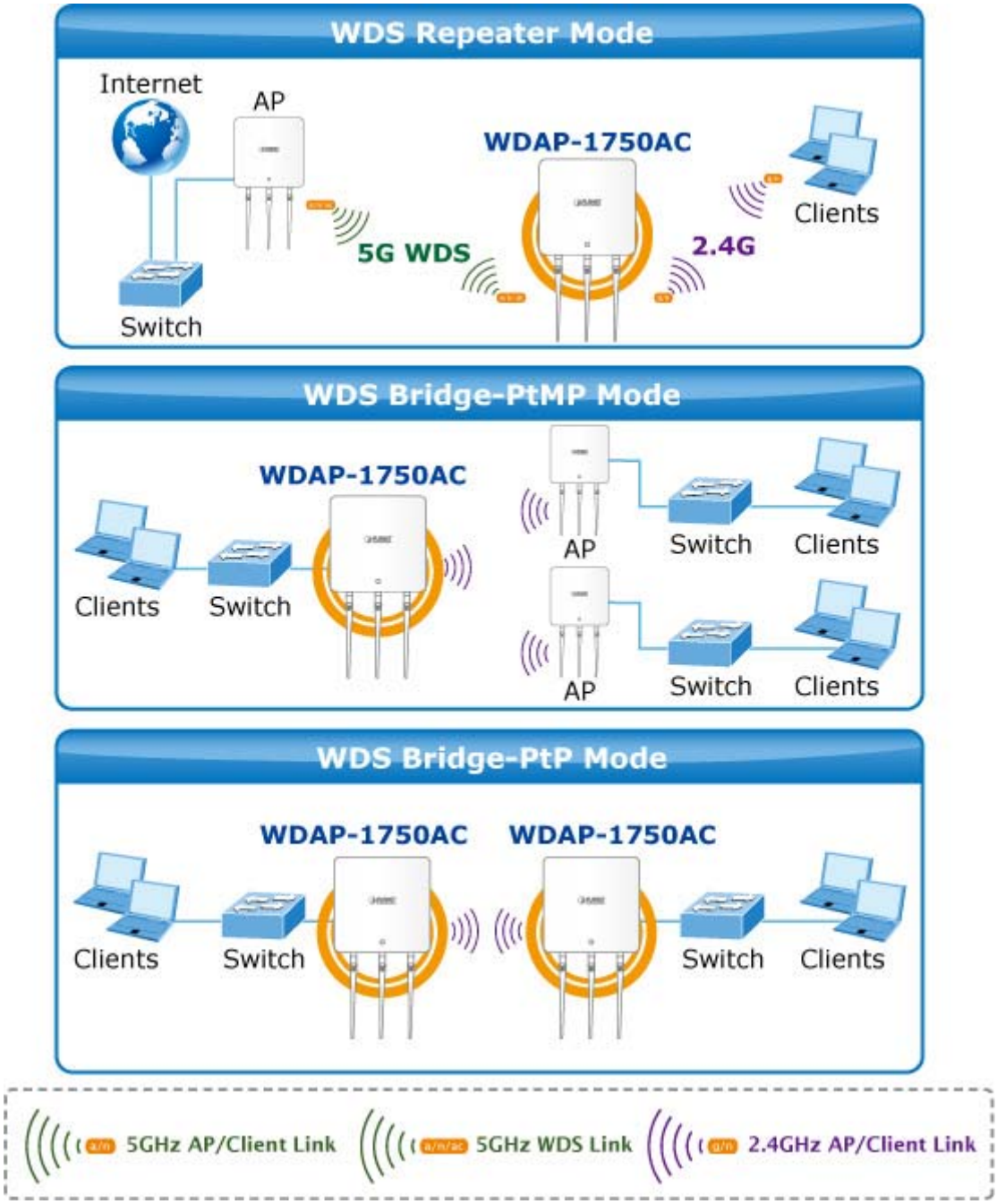
■ **Additional Authentication**

Additional wireless authentication methods can also be used:

Object	Description
MAC Address Filters	Restrict wireless clients access based on MAC address specified in the MAC filter table.
MAC-RADIUS Authentication	Restrict wireless clients access based on MAC address via a RADIUS server, or password authentication via a RADIUS server.
MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If you select "**Use the following password**", enter the password in the field below. The password should match the "Shared Secret".
MAC Filter & MAC-RADIUS Authentication	Restrict wireless clients access using both of the above MAC filtering and RADIUS authentication methods

5.3.8 WDS

Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network.



WDS settings can be configured as shown below. When using WDS, configure the IP address of each access point to be in the same subnet and ensure there is only one active DHCP server among connected access points, preferably on the WAN side.

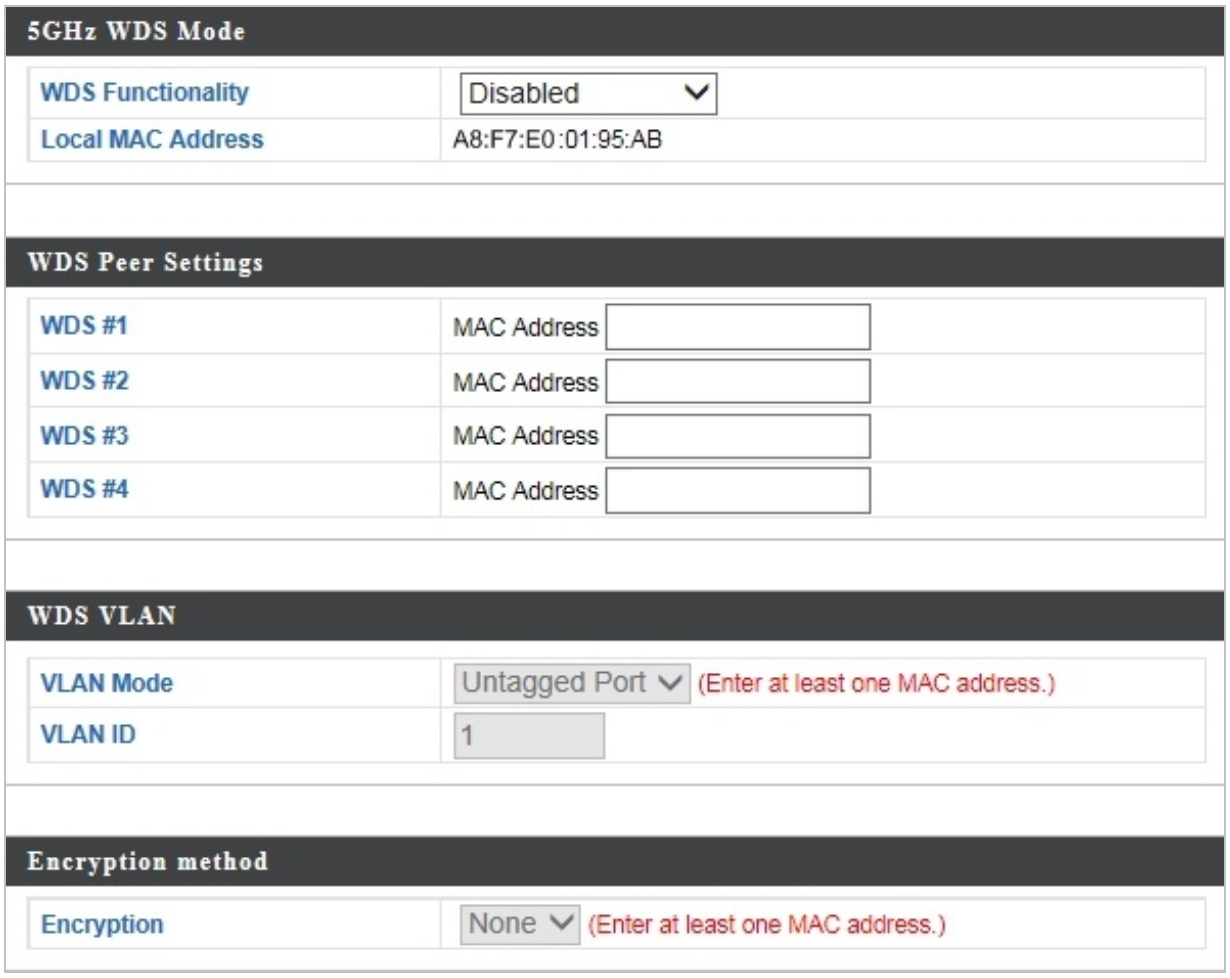


Figure 5-23 5GHz Wireless Settings **-** WDS

The page includes the following fields:

Object	Description
WDS Functionality	Select "**WDS with AP**" to use WDS or "**WDS Dedicated Mode**" to use WDS and also block communication with regular wireless clients. When WDS is used, each access point should be configured with corresponding MAC addresses, wireless channel and WEP key.
Local MAC Address	Displays the MAC address of your access point.
WDS #	Enter the MAC address for up to four other WDA devices you wish to connect.
VLAN Mode	Specify the WDS VLAN mode.
VLAN ID	Specify the WDS VLAN ID.
Encryption	Select whether to use "None" or "AES" encryption and enter a pre-shared key for AES.

Note

WDS must be configured on each access point, using correct MAC addresses.

All access points should use the **same wireless channel** and **WEP key**.

5.3.9 WPS

Wi-Fi Protected Setup (WPS) is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the device or from within the device's firmware/configuration interface (known as **PBC** or "**Push Button Configuration**").

When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "**PIN code WPS**" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

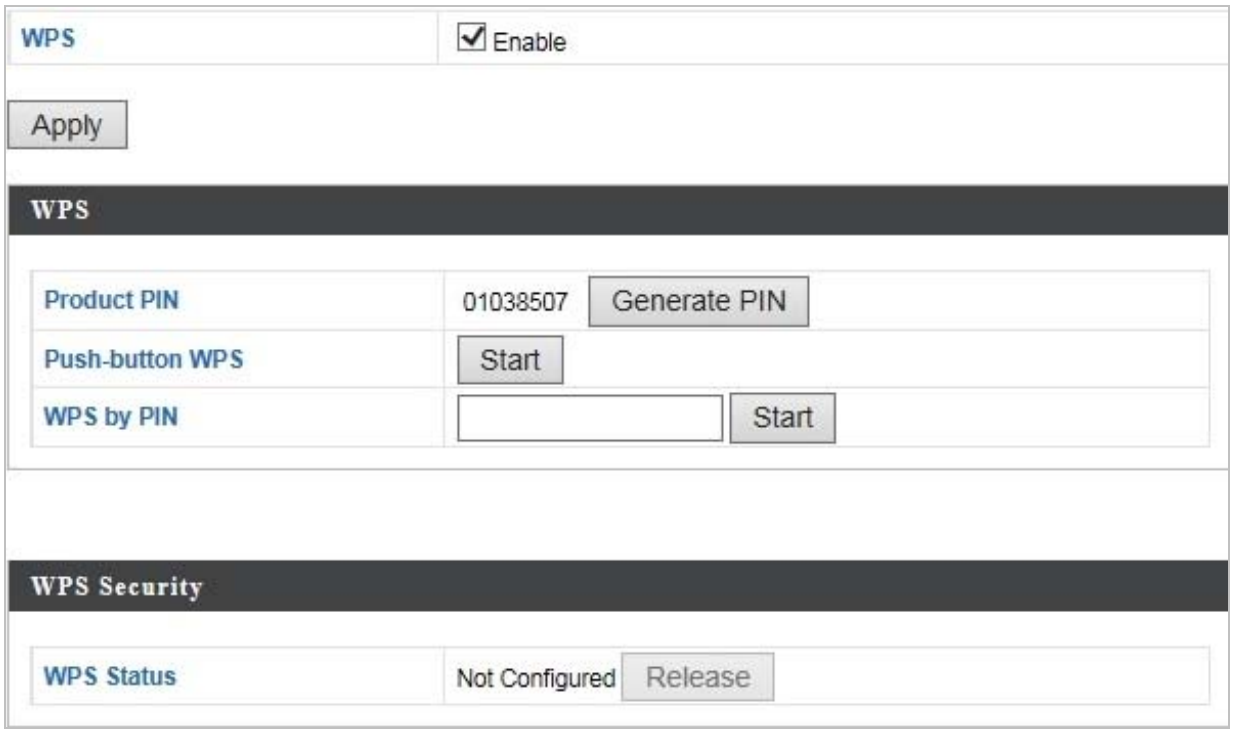


Figure 5-24 WPS

The page includes the following fields:

Object	Description
WPS	Check/uncheck this box to enable/disable WPS functionality. WPS must be disabled when using MAC-RADIUS authentication
Product PIN	Displays the WPS PIN code of the device, used for PIN code WPS. You will be required to enter this PIN code into another WPS device for PIN code WPS. Click "Generate PIN" to generate a new WPS PIN code.
Push-button WPS	Click "**Start**" to activate WPS on the access point for approximately **2 minutes**. This has the same effect as physically pushing the access point's WPS button.
WPS by PIN	Enter the PIN code of another WPS device and click "**Start**" to attempt to establish a WPS connection for approximately **2 minutes**.
WPS Status	WPS security status is displayed here. Click "**Release**" to clear the existing status.

5.3.10 RADIUS Settings

The RADIUS sub menu allows you to configure the access point's RADIUS server settings, categorized into three submenus: **RADIUS settings**, **Internal Server** and **RADIUS accounts**.

A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

The access point can utilize both a primary and secondary (backup) RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz). External RADIUS servers can be used or the access point's internal RADIUS server can be used.

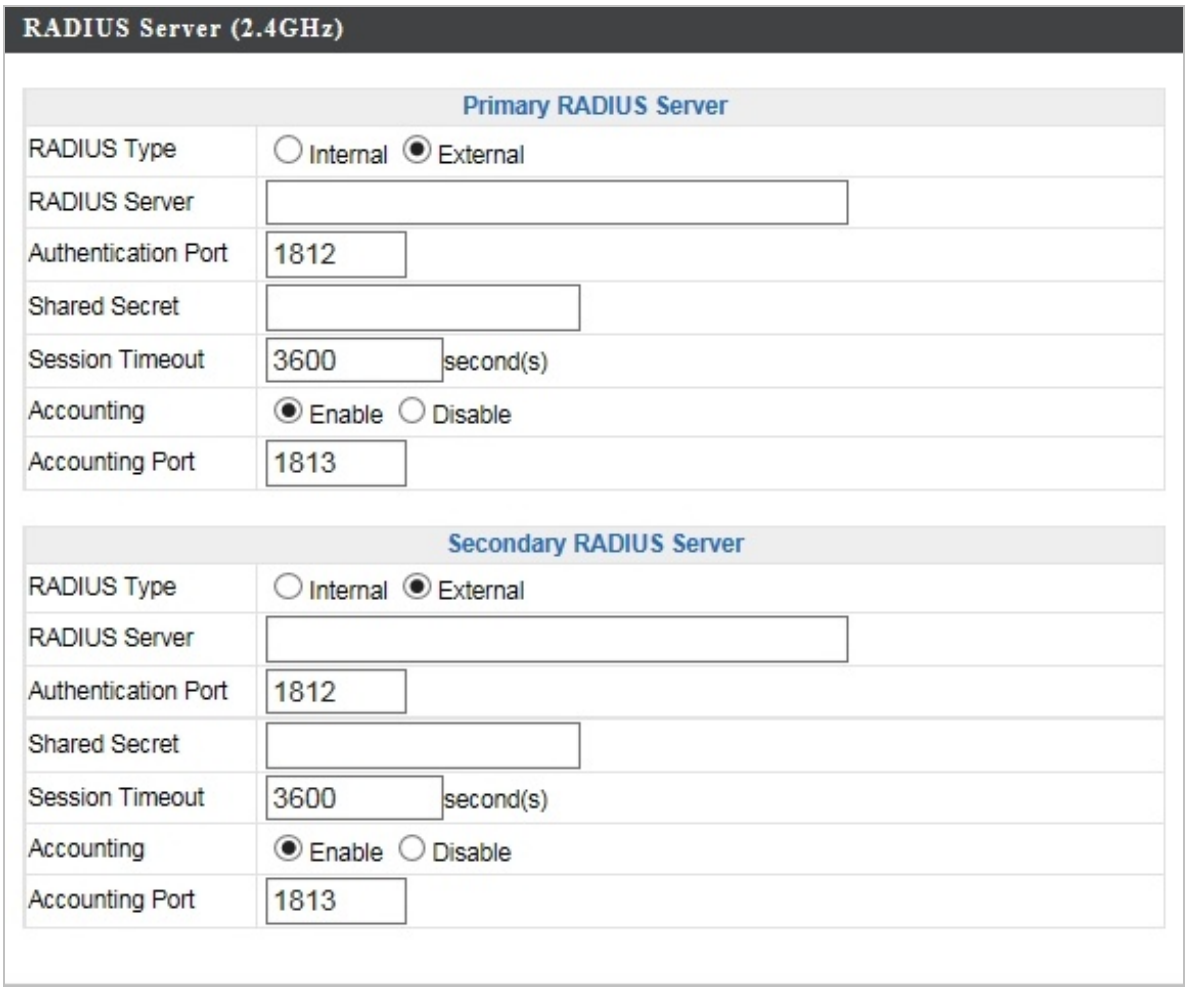


Figure 5-25 RADIUS Settings

The page includes the following fields:

Object	Description
RADIUS Type	Select "**Internal**" to use the access point's **built-in RADIUS server** or "**external**" to use an external RADIUS server.
RADIUS Server	Enter the RADIUS server host IP address.
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between **1** and **65535**.

Shared Secret	Enter a shared secret/password between 1 and 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between **0 and 86400**.
Accounting	Enable or disable RADIUS accounting.
Accounting Port	When accounting is enabled (above), set the UDP port used in the accounting protocol of the RADIUS server. Value must be between **1 and 65535**.

5.3.11 Internal Server

The access point features a built-in RADIUS server which can be configured as shown below.

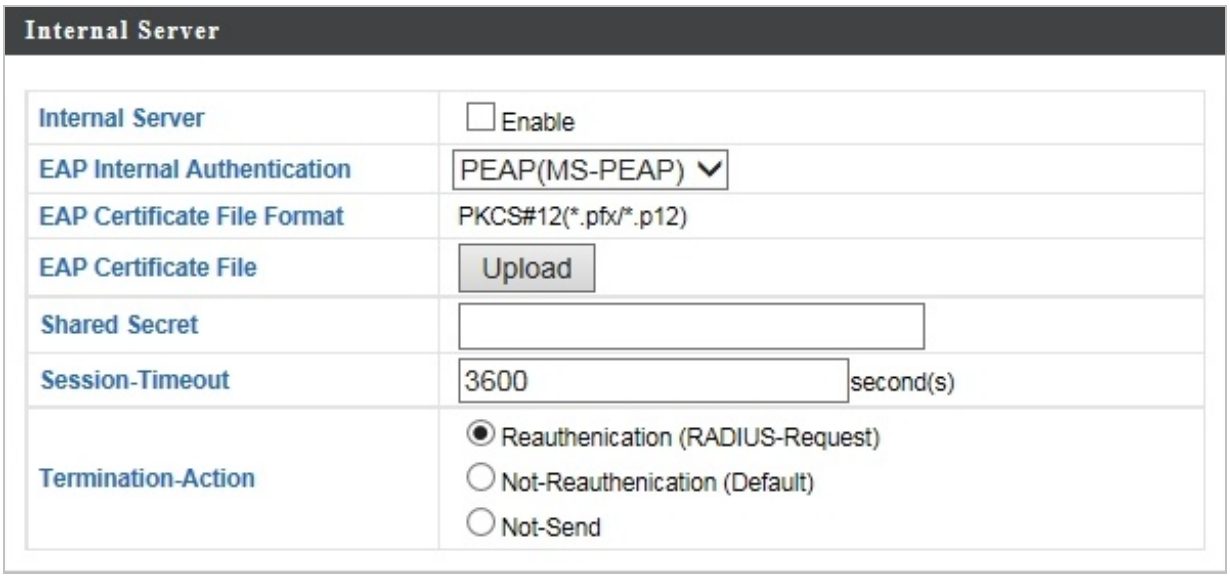


Figure 5-26 Internal Server

The page includes the following fields:

Object	Description
Internal Server	Check/uncheck to enable/disable the access point's internal RADIUS server.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
EAP Certificate File Format	Displays the EAP certificate file format: PCK#12(*.pfx/*.p12)
EAP Certificate File	Click "**Upload**" to open a new window and select the location of an EAP certificate file to use. If no certificate file is uploaded, the internal RADIUS server will use a self-made certificate.
Shared Secret	Enter a shared secret/password for use between the internal RADIUS server and RADIUS client. The shared secret should be 1 to 99 characters in length.
Session Timeout	Set a duration of session timeout in seconds between 0 to 86400.
Termination Action	Select a termination-action attribute: "**Reauthentication**" sends a RADIUS request to the access point, "**Not-Reathentication**" sends a default

	termination-action attribute to the access point, “**Not-Send**” no termination-action attribute is sent to the access point.

5.3.12 RADIUS Accounts

The internal RADIUS server can authenticate up to 256 user accounts. The “RADIUS Accounts” page allows you to configure and manage users.

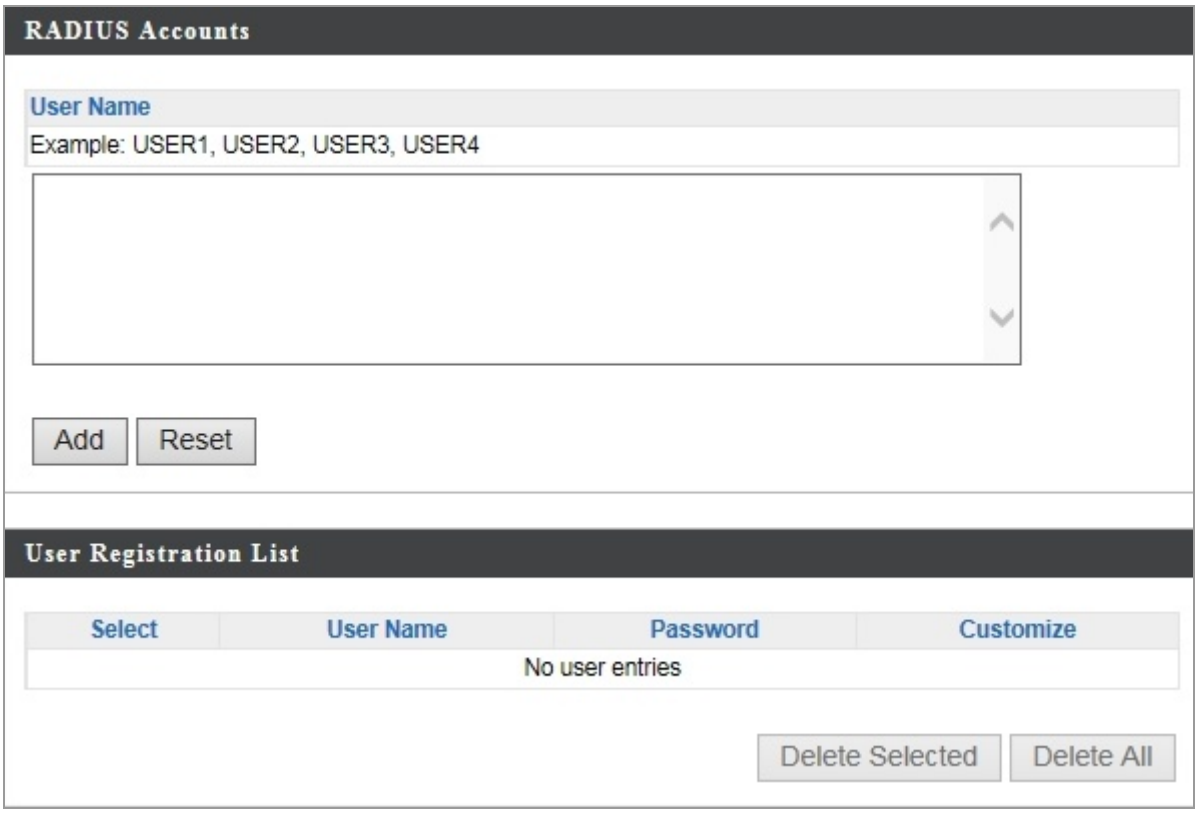


Figure 5-27 RADIUS Accounts

Press “**Add**” and “**Edit**”, the page includes the following fields:

Object	Description
User Name	Enter a user name here.
Add	Click “**Add**” to add the user to the user registration list.
Reset	Clear text from the user name box.
Select	Check the box to select a user.
User Name	Displays the user name.
Password	Displays if specified user name has a password (configured) or not (not configured).
Customize	Click “**Edit**” to open a new field to set/edit a password for the specified user name (below).
Delete Selected	Delete selected user from the user registration list.
Delete All	Delete all users from the user registration list.

5.3.13 MAC Filter

Mac filtering is a security feature that can help to prevent unauthorized users from connecting to your access point.

This function allows you to define a list of network devices permitted to connect to the access point. Devices are each identified by their unique MAC address. If a device which is not on the list of permitted MAC addresses attempts to connect to the access point, it will be denied.

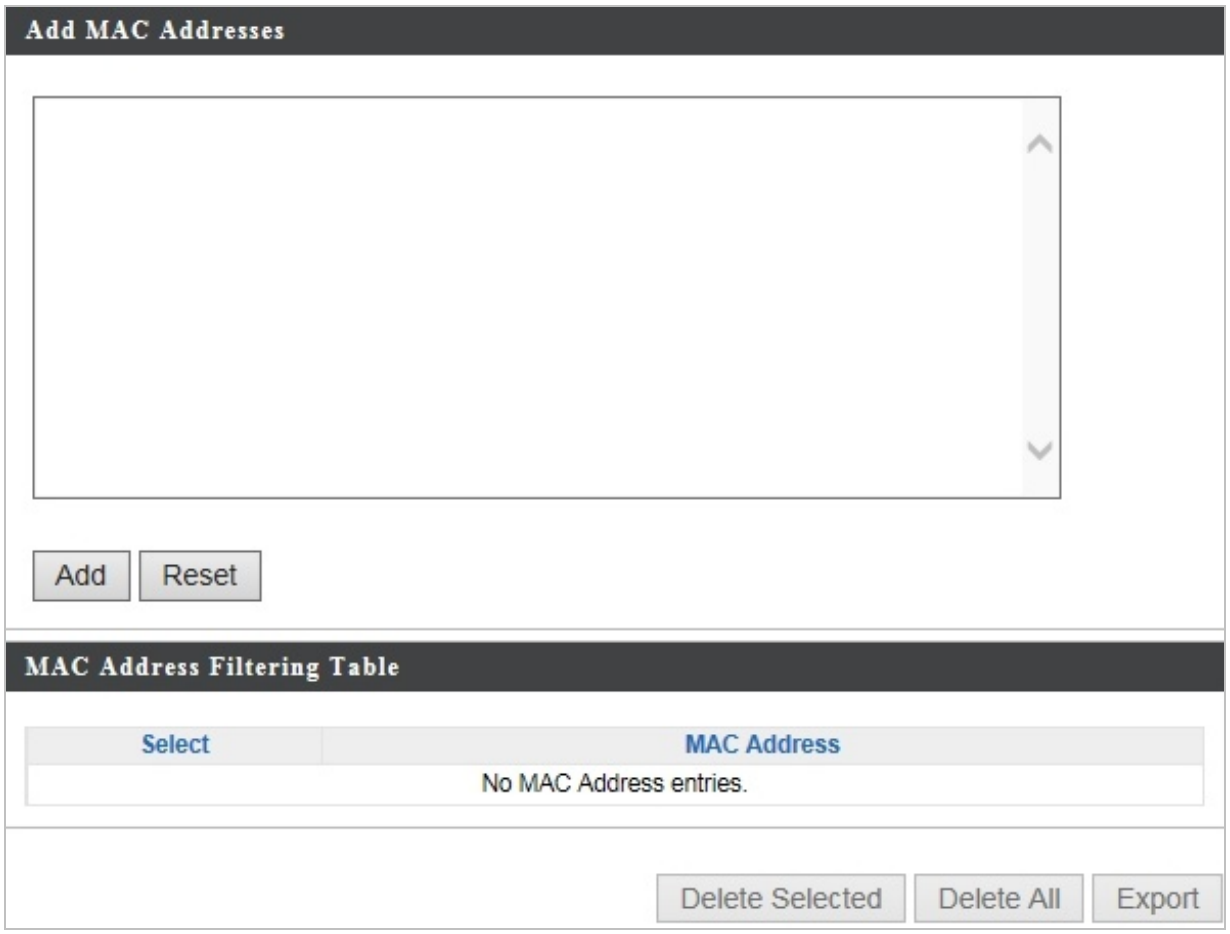


Figure 5-28 MAC Filter

The page includes the following fields:

Object	Description
Add MAC Address	Enter a MAC address of computer or network device manually without dashes or colons, e.g., for MAC address 'aa-bb-cc-dd-ee-ff' enter 'aabbccddeeff'.
Add	Click "**Add**" to add the MAC address to the MAC address filtering table.
Reset	Clear all fields.

MAC address entries will be listed in the "**MAC Address Filtering Table**". Select an entry using the "Select" checkbox.

Object	Description

Select	Delete selected or all entries from the table.
MAC Address	The MAC address is listed here.
Delete Selected	Delete the selected MAC address from the list.
Delete All	Delete all entries from the MAC address filtering table.
Backup	Click "**Backup**" to save a copy of the MAC filtering table. A new window will pop up for you to select a location to save the file.

5.3.14 WMM

Wi-Fi Multimedia (WMM) is a Wi-Fi Alliance interoperability certification based on the IEEE 802.11e standard, which provides Quality of Service (QoS) features to IEE 802.11 networks. WMM prioritizes traffic according to four categories: **background**, **best effort**, **video** and **voice**.

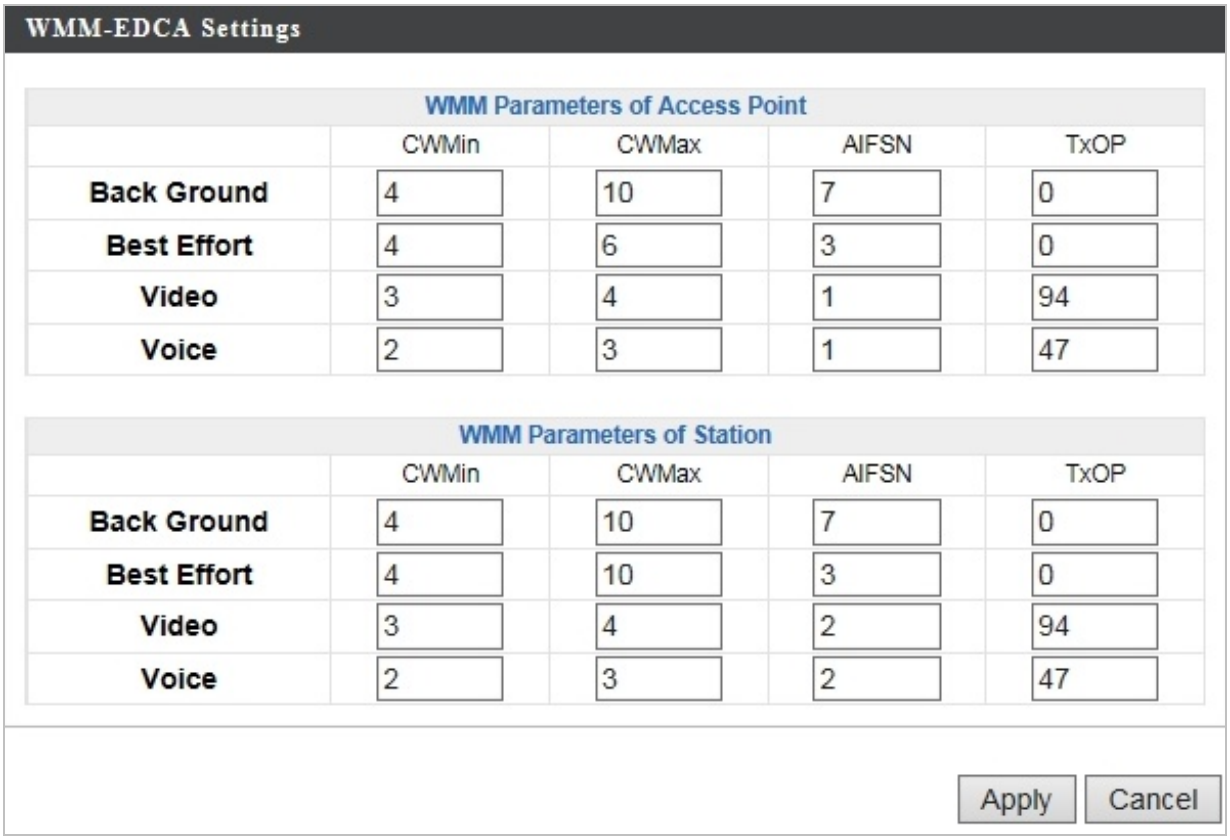


Figure 5-29 WMM

Configuring WMM consists of adjusting parameters on queues for different categories of wireless traffic. Traffic is sent to the following queues:

Object	Description	
Background	Low Priority	High throughput, non time sensitive bulk data e.g. FTP
Best Effort	Medium Priority	Traditional IP data, medium throughput and delay.
Video	High Priority	Time sensitive video data with minimum time delay.
Voice	High Priority	Time sensitive data such as VoIP and streaming media

		with minimum time delay.

Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can further be adjusted manually:

Object	Description
CWMin	Minimum Contention Window (milliseconds): This value is input to the initial random backoff wait time algorithm for retry of a data frame transmission. The backoff wait time will be generated between 0 and this value. If the frame is not sent, the random backoff value is doubled until the value reaches the number defined by CWMax (below). Valid values are 1,3,7,15,31,63,127,255,511 or 1024. The CWMin value must be lower than the CWMax value. The contention window scheme helps to avoid frame collisions and determine priority of frame transmission. A shorter window has a higher probability (priority) of transmission.
CWMax	Maximum Contention Window (milliseconds): This value is the upper limit to random backoff value doubling (see above). Valid values are 1,3,7,15,31,63,127,255,511 or 1024.
AIFSN	Arbitration Inter-Frame Space (milliseconds): Specifies additional time between when a channel goes idle and the AP/client sends data frames. Traffic with a lower AIFSN value has a higher priority.
TxOP	Transmission Opportunity (milliseconds): The maximum interval of time an AP/client can transmit. This makes channel access more efficiently prioritized. A value of 0 means only one frame per transmission. A greater value effects higher priority.

5.4 Management

5.4.1 Admin

You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.

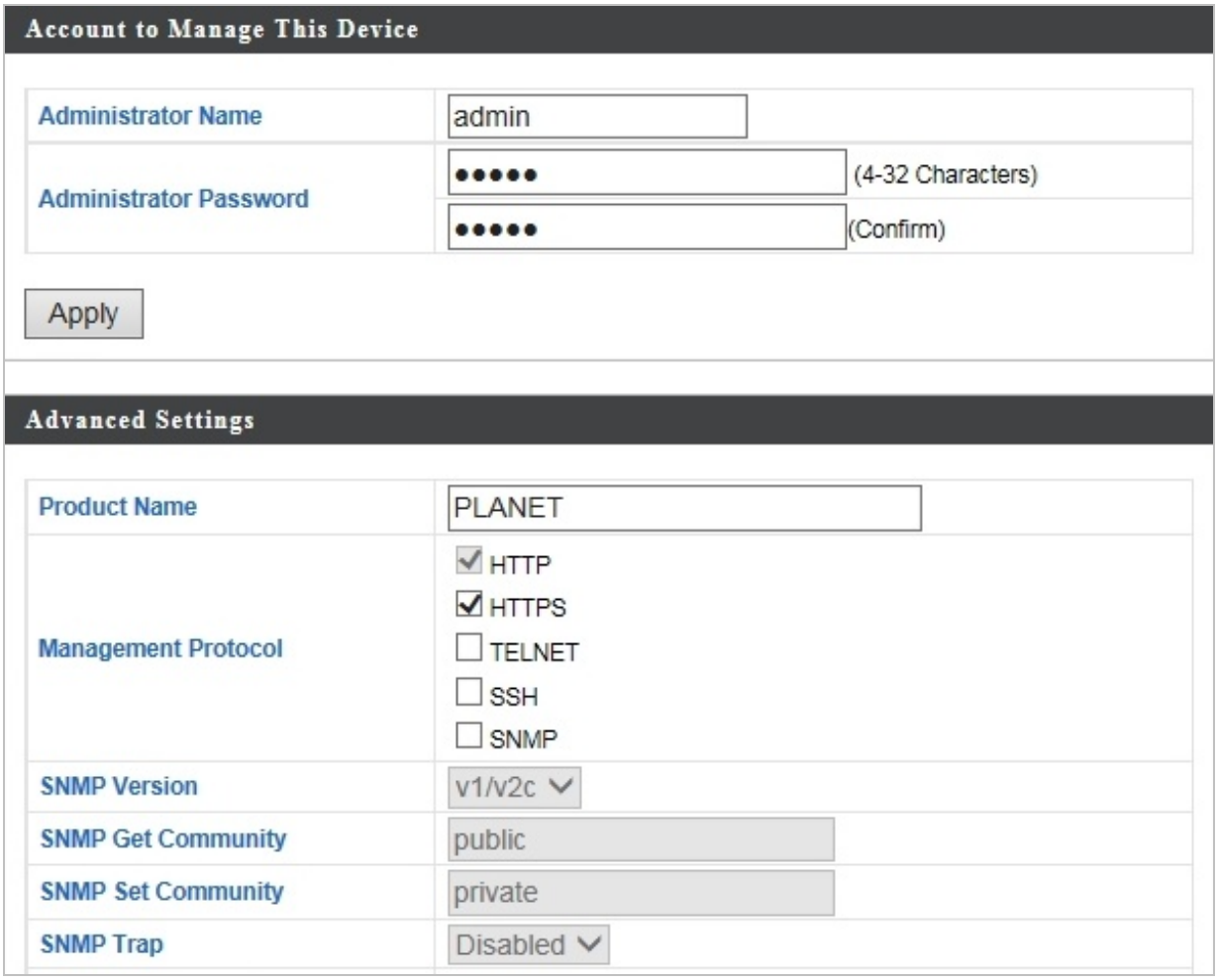


Figure 5-30 Admin

The page includes the following fields:

Object	Description
Administrator Name	Set the access point's administrator name. This is used to log in to the browser based configuration interface.
Administrator Password	Set the access point's administrator password. This is used to log in to the browser based configuration interface.
Product Name	Edit the product name according to your preference. This name is used for reference purposes.
Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below). When SNMP is enabled, complete the SNMP fields below.
SNMP Version	Select SNMP version appropriate for your SNMP manager.

SNMP Get Community	Enter an SNMP Get Community name for verification with the SNMP manager for SNMP-GET requests.
SNMP Set Community	Enter an SNMP Set Community name for verification with the SNMP manager for SNMP-SET requests.
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of network errors.
SNMP Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests.
SNMP Trap Manager	Specify the IP address or sever name (maximum 128 characters) of the SNMP manager.

- **HTTP:** Internet browser HTTP protocol management interface
- **HTTPS:** Internet browser HTTPS protocol management interface
- **TELNET:** Client terminal with Telnet protocol management interface
- **SSH:** Client terminal with SSH protocol version 1 or 2 management interface
- **SNMP:** Network management protocol. SNMPv1, v2 & v3 protocol supported. SNMPv2 can be used with community based authentication. SNMPv3 uses user-based security model (UM) architecture.
- **FTPD:** Third-party FTP server.
- **SNMP:** Third-party TFTP server.

5.4.2 Date and Time

You can configure the time zone settings of your access point here. The date and time of the device can be configured manually or can be synchronized with a time server.

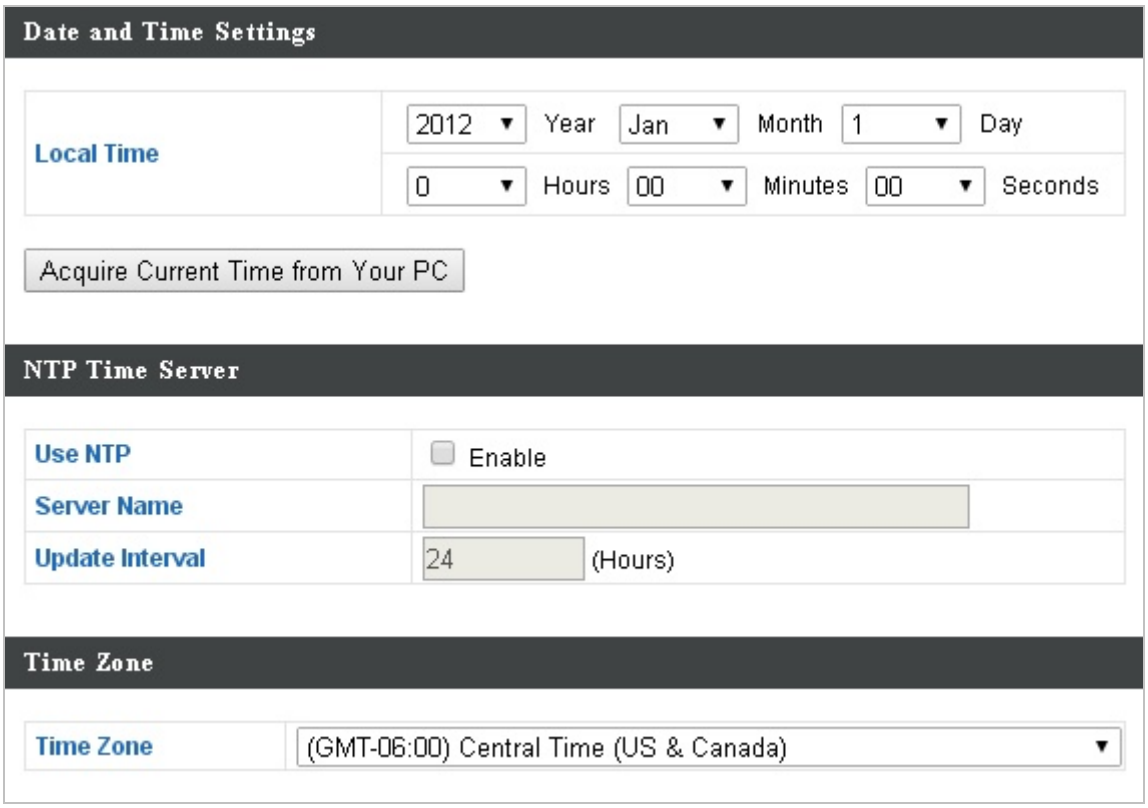


Figure 5-31 Time and Date

The page includes the following fields:

Object	Description
Local Time	Set the access point's date and time manually using the drop-down menus.
Acquire Current Time from your PC	Click "Acquire Current Time from Your PC" to enter the required values automatically according to your computer's current time and date.
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server.
Time Zone	Select the time zone of your country/ region. If your country/region is not listed, please select another country/region whose time zone is the same as yours.

5.4.3 Syslog Server

The system log can be sent to a server or to attached USB storage.

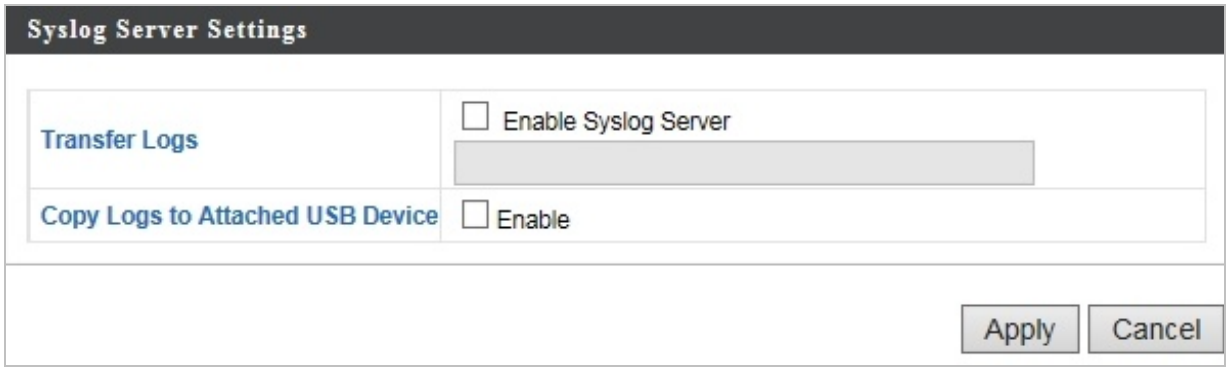


Figure 5-32 Syslog Server

The page includes the following fields:

Object	Description
Transfer Logs	Check/uncheck the box to enable/disable the use of a syslog server, and enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters.
Copy Logs to Attached USB Device	Check/uncheck the box to enable/disable copying logs to attached USB storage.
Transfer Logs	Check/uncheck the box to enable/disable the use of a syslog server, and enter a host name, domain or IP address for the server, consisting of up to 128 alphanumeric characters.

5.4.4 I'm Here

The access point features a built-in buzzer which can sound on command using the "I'm Here" page. This is useful for network administrators and engineers working in complex network environments to locate the access point.

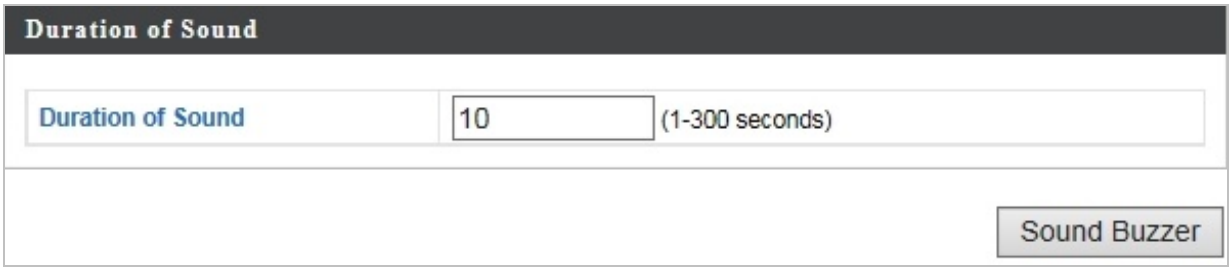


Figure 5-33 I'm Here

The page includes the following fields:

Object	Description
Duration of Sound	Set the duration for which the buzzer will sound when the "Sound Buzzer" button is clicked.
Sound Buzzer	Activate the buzzer sound for the above specified duration of time.

5.5 Advanced

5.5.1 LED Settings

The access point's LEDs can be manually enabled or disabled according to your preference.

Figure 5-34 LED Settings

The page includes the following fields:

Object	Description
Power LED	Select on or off.
Diag LED	Select on or off.

5.5.2 Update Firmware

The "**Firmware**" page allows you to update the system firmware to a more recent version. Updated firmware versions often offer increased performance and security, as well as bug fixes. You can download the latest firmware from the PLANET website.

Figure 5-35 Update Firmware

The page includes the following fields:

Object	Description
Update Firmware From	Select to upload firmware from your local computer or from an attached USB device.

Firmware Update File	Click “**Browse**” to open a new window to locate and select the firmware file in your computer.
Update	Click “**Update**” to upload the specified firmware file to your access point.

5.5.3 Save/Restore Settings

The access point’s “Save/Restore Settings” page enables you to save/backup the access point’s current settings as a file to your local computer or a USB device attached to the access point, and restore the access point to previously saved settings.

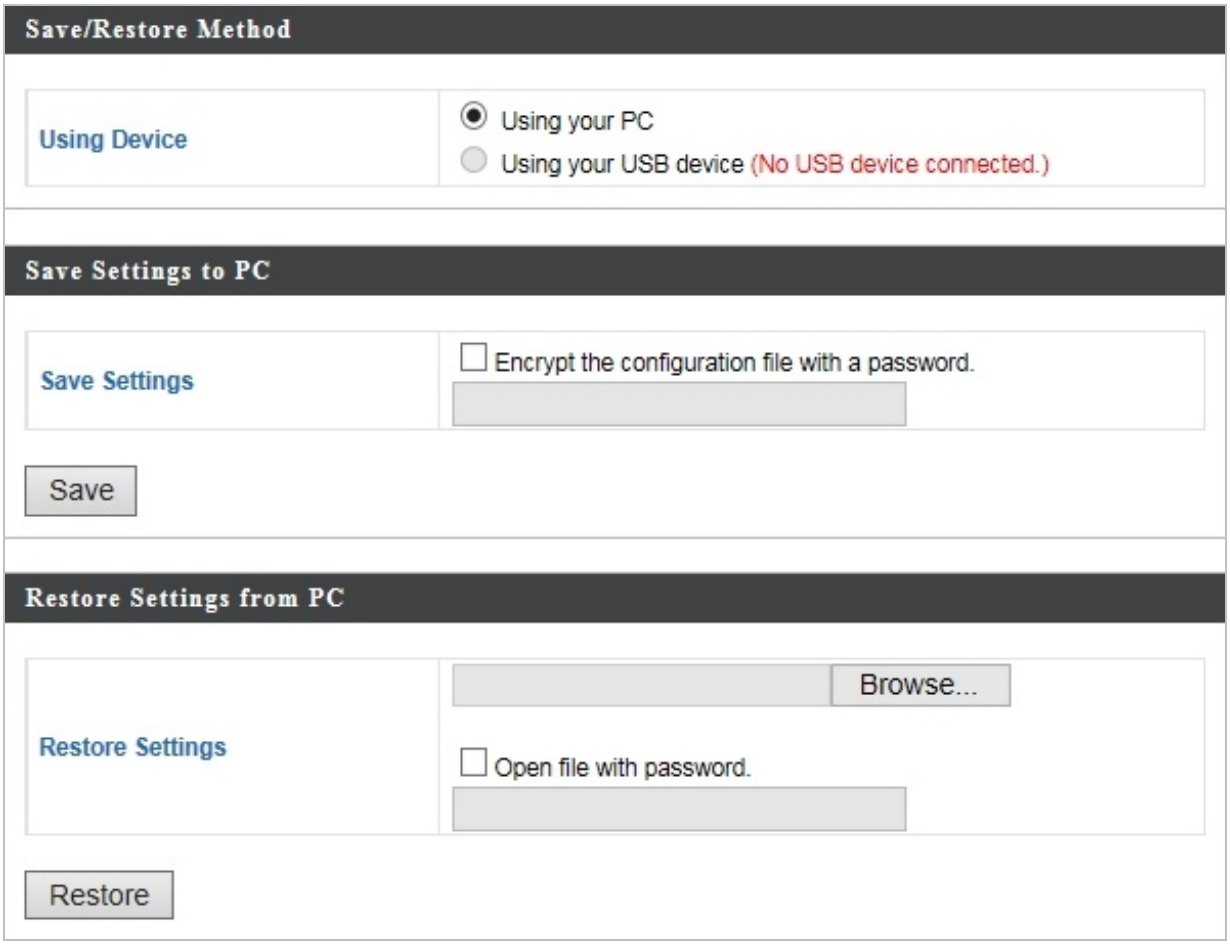


Figure 5-36 Save/Restore Settings

The page includes the following fields:

Object	Description
Using Device	Select to save the access point’s settings to your local computer or to an attached USB device.
Save Settings	Click “**Save**” to save settings and a new window will open to specify a location to save the settings file. If saving settings to your computer, you can also check the “**Encrypt the configuration file with a password**” box and enter a password to protect the file in the field underneath, if you wish.

Restore Settings	Click the browse button to find a previously saved settings file and then click "**Restore**" to replace your current settings. If your settings file is encrypted with a password, check the "**Open file with password**" box and enter the password in the field underneath.

5.5.4 Factory Default

If the access point malfunctions or is not responding, then it is recommended that you reboot the device or reset the device back to its factory default settings. You can reset the access point back to its default settings using this feature if the location of the access point is not convenient to access the reset button.

Figure 5-37 Factory Default

The page includes the following fields:

Object	Description
Factory Default	Click "**Factory Default**" to restore settings to the factory default. A pop-up window will appear and ask you to confirm.

Note: After resetting to factory defaults, please wait for the access point to reset and restart.

5.5.5 Reboot

If the access point malfunctions or is not responding, then it is recommended that you reboot the device or reset the access point back to its factory default settings. You can reboot the access point remotely using this feature.

Figure 5-38 Reboot

The page includes the following fields:

Object	Description
Reboot	Click "**Reboot**" to reboot the device. A countdown will indicate the progress of the reboot.

Chapter 6. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the WDAP-1750AC is configured to "**default**".

6.1 Windows XP (Wireless Zero Configuration)

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

Figure 6-1 System Tray – Wireless Network Icon

Step 2: Select [**View Available Wireless Networks**]

Step 3: Highlight and select the wireless network (SSID) to connect

(1) Select SSID [default]

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

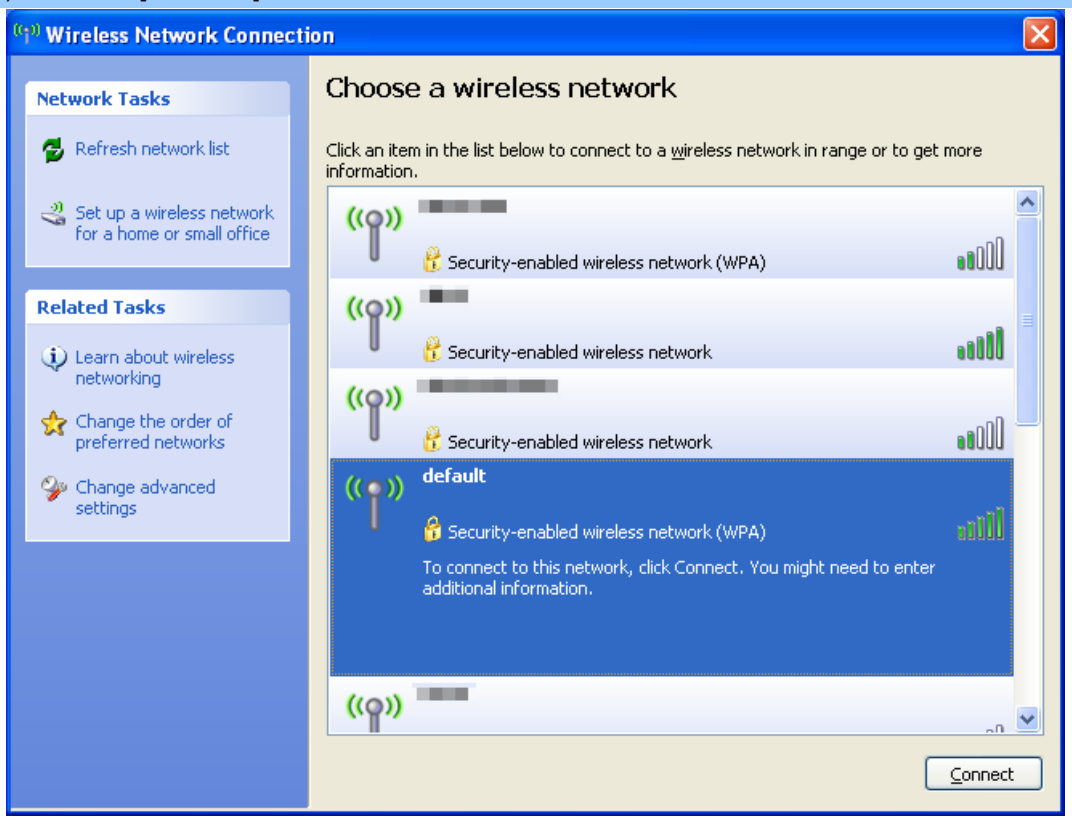


Figure 6-2 Choose a wireless network

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

(1) The Wireless Network Connection box will appear

(2) Enter the encryption key that is configured in section 5.3.3

(3) Click the [Connect] button

Figure 6-3 Enter the network key

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

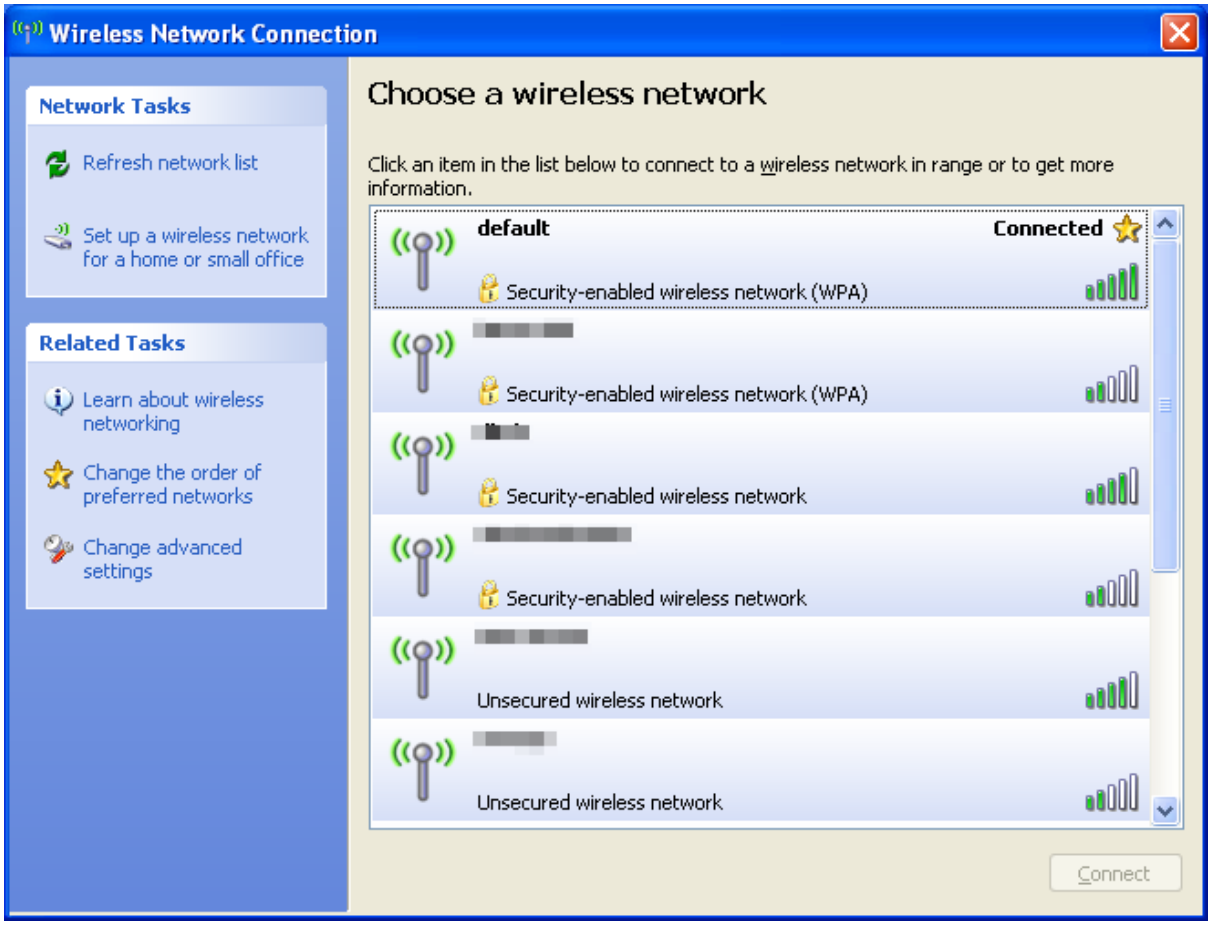


Figure 6-4 Choose a wireless network -- Connected

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.

6.2 Windows 7 (WLAN AutoConfig)

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

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

Figure 6-5 Network icon

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

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

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

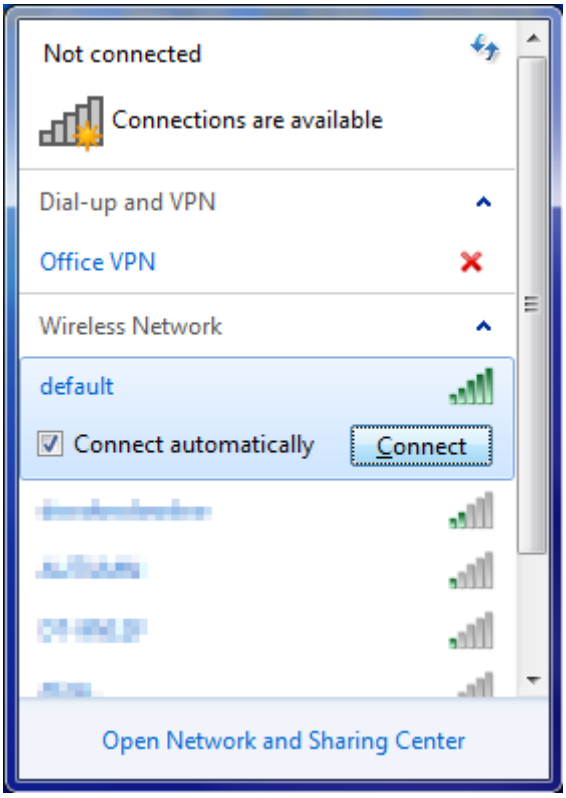


Figure 6-6 WLAN AutoConfig

Note

If you will be connecting to this 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 5.3.3

(3) Click the [OK] button

Figure 6-7 Type the network key

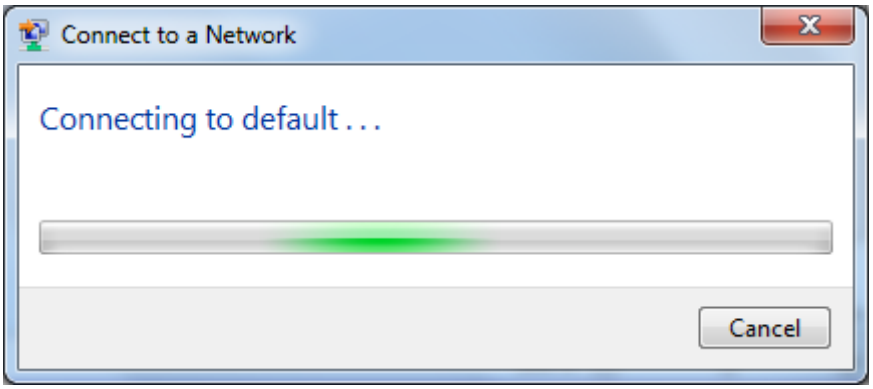


Figure 6-8 Connecting to a Network

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

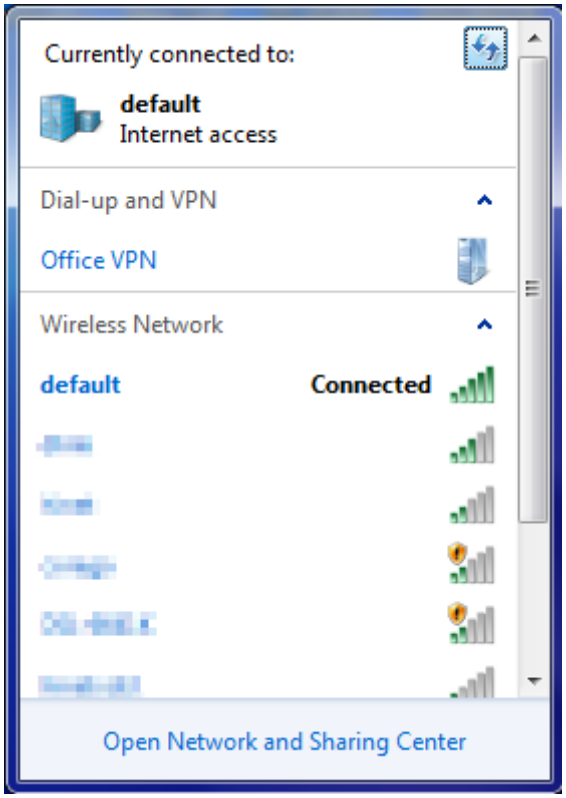


Figure 6-9 Connected to a Network

6.3 Mac OS X 10.x

In the following sections, the default SSID of the WDAP-1750AC is configured to “default”.

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

The AirPort Network Connection menu will appear

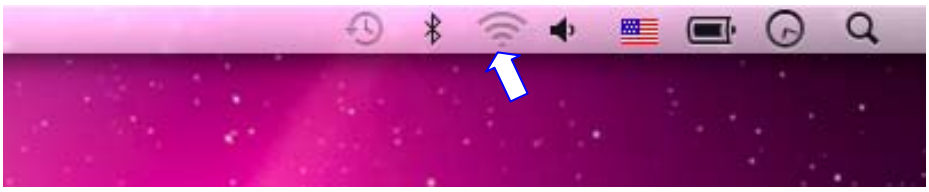


Figure 6-10 Mac OS – Network icon

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

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

(2) Double-click on the selected SSID

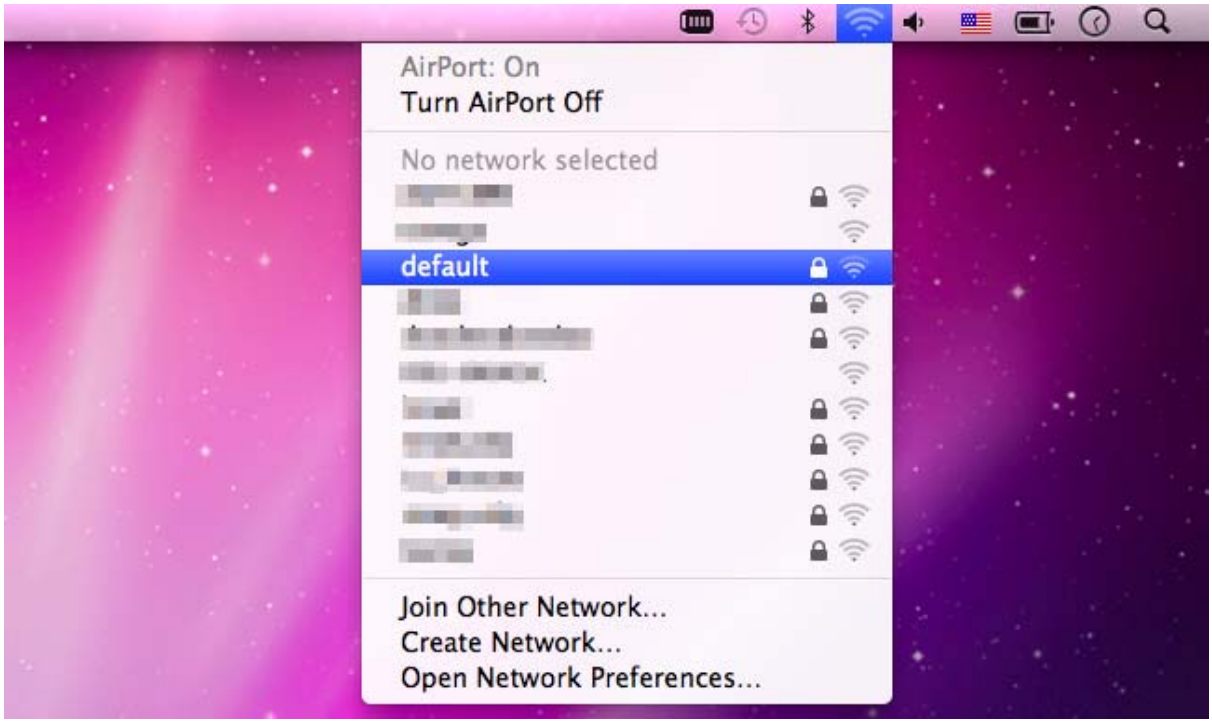


Figure 6-11 Highlight and select the wireless network

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

(1) Enter the encryption key that is configured in section 5.3.3

(2) Click the [OK] button

Figure 6-12 Enter the Password

Note

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

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

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

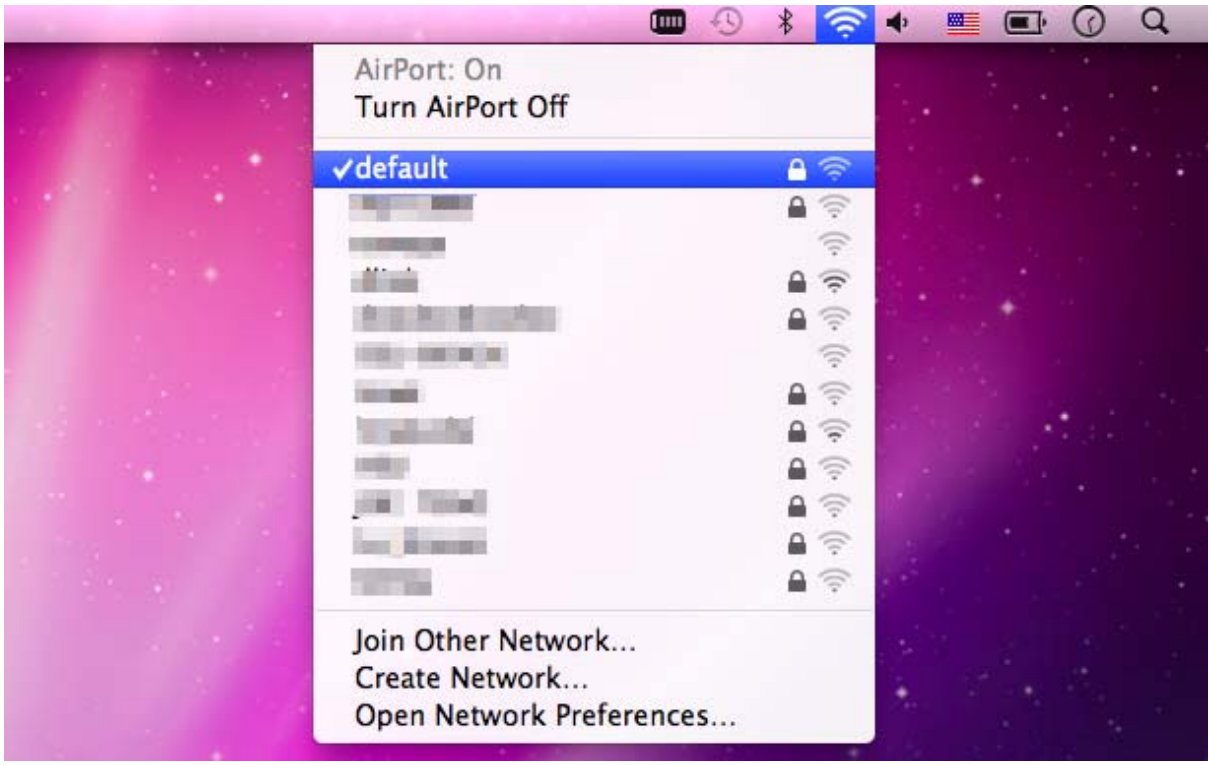


Figure 6-13 Connected to the Network

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**

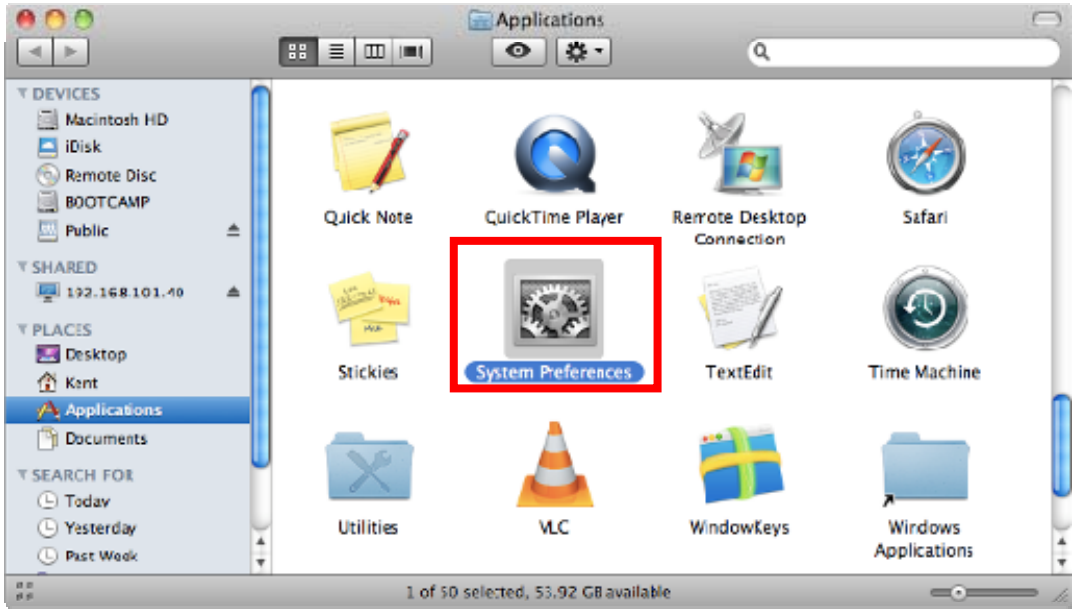


Figure 6-14 System Preferences

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

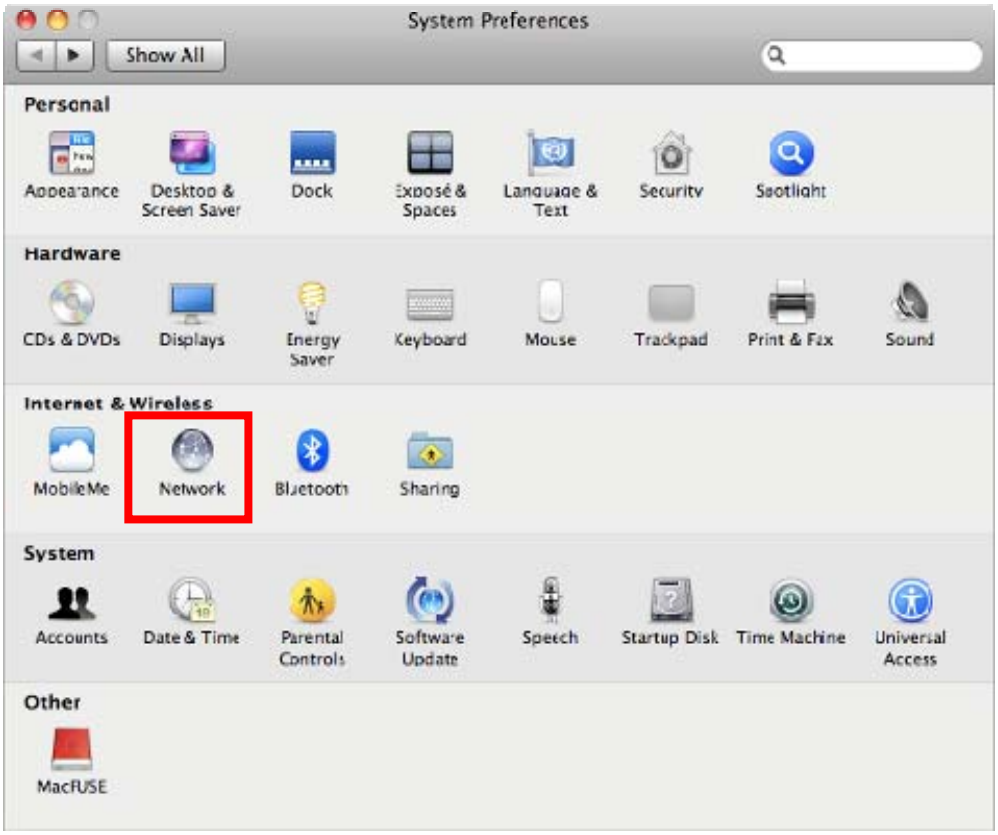


Figure 6-15 System Preferences -- Network

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 “Not network selected”.

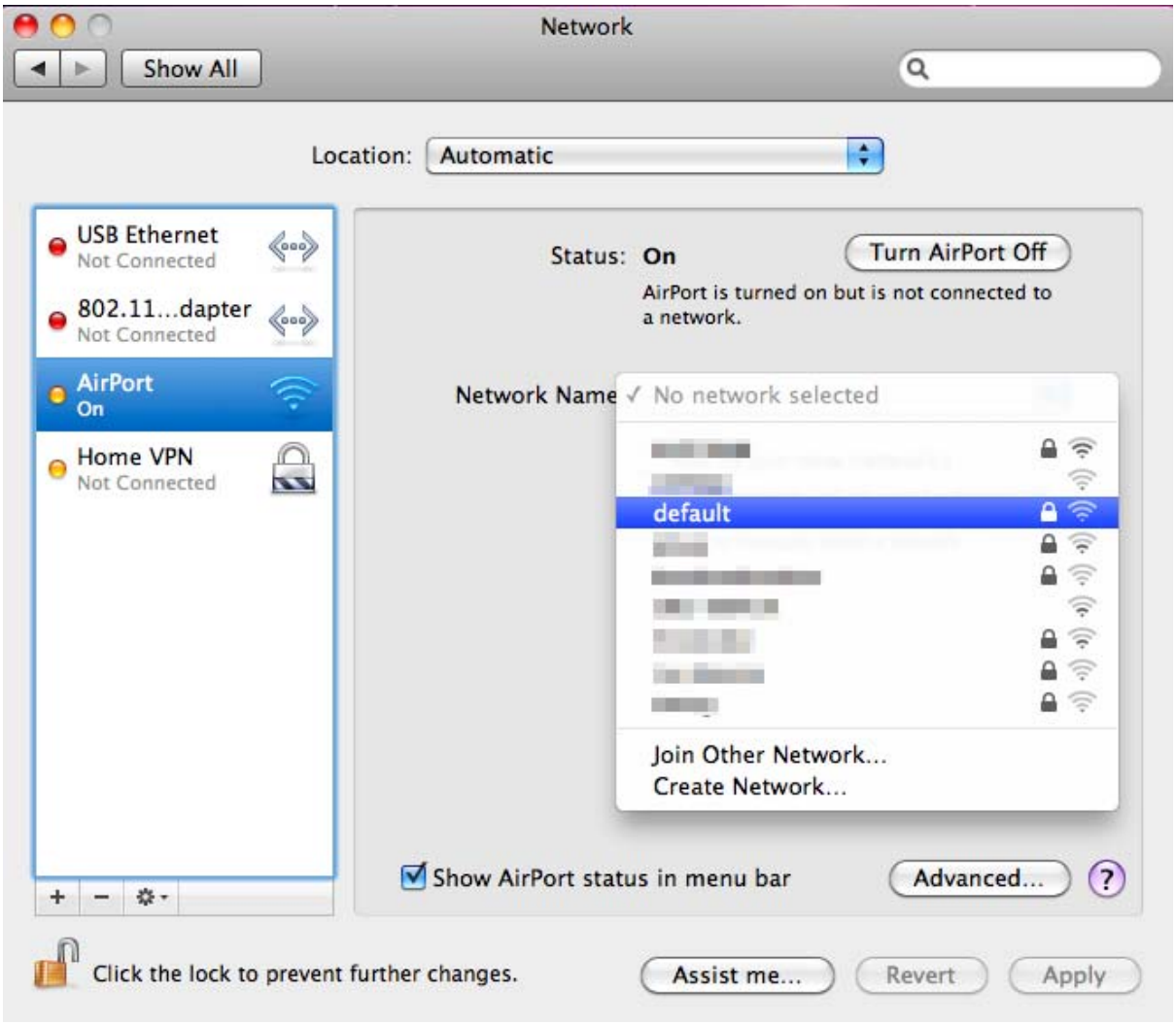


Figure 6-16 Select the Wireless Network

6.4 iPhone / iPod Touch / iPad

In the following sections, the **default SSID** of the WDAP-1750AC is configured to "**default**".

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

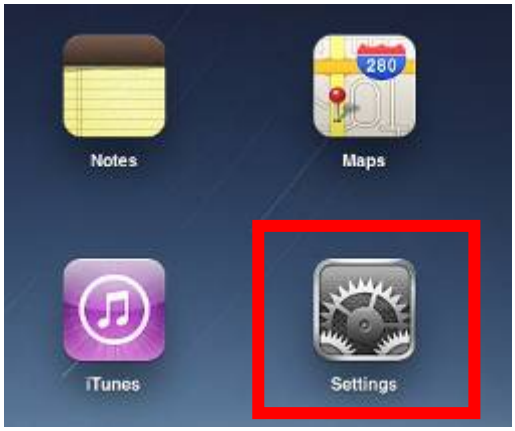


Figure 6-17 iPhone – Settings icon

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

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

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

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

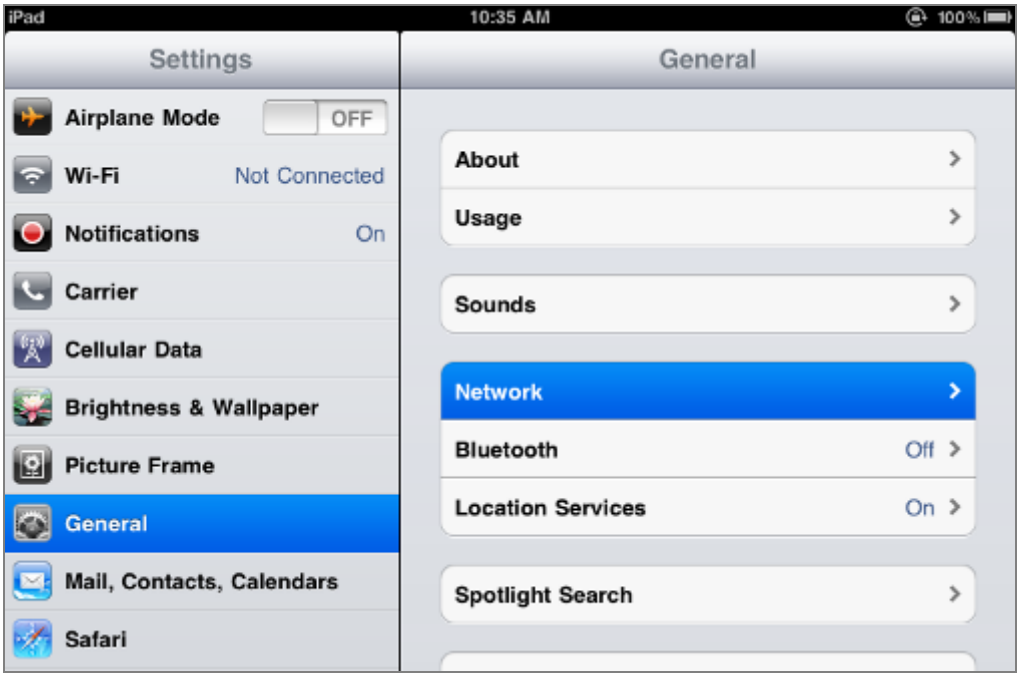


Figure 6-18 Wi-Fi Setting

Figure 6-19 Wi-Fi Setting – Not Connected

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

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

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

Figure 6-20 Turn 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 5.3.3

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

Figure 6-21 iPhone -- Enter 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 the front of the SSID.

Figure 6-22 iPhone -- Connected to the Network

Appendix A: Planet Smart Discovery Utility

To easily list the WDAP-1750AC in your Ethernet environment, the Planet Smart Discovery Utility from user's manual CD-ROM is an ideal solution.

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

Step 1: Deposit the **Planet Smart Discovery Utility** in administrator PC.

Step 2: Run this utility and the following screen appears.

Step 3: Press **"Refresh"** button for the current connected devices in the discovery list as shown in the following screen:

Step 3: Press **"Connect to Device"** button and then the Web login screen appears.

Note

The fields in white background can be modified directly and then you can apply the new setting by clicking the "**Update Device**" button.

Appendix B: 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 to 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 (pressing '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 router 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 router's settings again. e. Call your Internet service provider and check if there's something wrong with their service. 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. Are you using QoS function? Try to disable it and try again. b. Internet is slow sometimes. Please be patient. c. Try to reset the AP and see if it's better after that. d. Try to know what computers do on your local network. If someone's transferring big files, other people will think Internet is really slow. e. 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 hardware 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 C: Glossary

- **802.11ac** - 802.11ac is a wireless networking standard in the 802.11 family (which is marketed under the brand name Wi-Fi), developed in the IEEE Standards Association process, providing high-throughput wireless local area networks (WLANs) on the 5 GHz 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 2.4GHz, 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 2.4GHz, 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** (**De**militarized **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.
- **ISP** (**I**nternet **S**ervice **P**rovider) **-** A company that provides access to the Internet.

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

EC Declaration of Conformity

For the following equipment:

*Type of Product: 1750Mbps 802.11ac Dual Band Wall Mount Enterprise Wireless Access Point
*Model Number: WDAP-1750AC

* Produced by:
Manufacturer‘s Name : **Planet Technology Corp.**
Manufacturer‘s Address: 10F., No.96, Minquan Rd., Xindian Dist.,
New Taipei City 231, Taiwan (R.O.C.)

is here with confirmed to comply with the requirements set out in the Council Directive on the Approximation of the Laws of the Member States relating to 1999/5/EC R&TTE.
For the evaluation regarding the R&TTE the following standards were applied:

EN 300 328	V1.8.1	(2012-06)
EN 301 489-17	V2.2.1	(2012-09)
EN 301 489-1	V1.9.2	(2011-09)
EN 301 893	V1.7.1	(2012-06)
EN 60950-1		(2006+A11:2009+A1:2010+A12:2011)

Responsible for marking this declaration if the:

☒ **Manufacturer** ☐ **Authorized representative established within the EU**

Authorized representative established within the EU (if applicable):

Company Name: **Planet Technology Corp.**

Company Address: **10F., No.96, Minquan Rd., Xindian Dist., New Taipei City 231, Taiwan (R.O.C.)**

Person responsible for making this declaration

Name, Surname **Kent Kang**

Position / Title : **Product Manager**

Taiwan	**5 Dec., 2014**	
Place	*Date*	*Legal Signature*

PLANET TECHNOLOGY CORPORATION

e-mail: sales@planet.com.tw http://www.planet.com.tw
10F., No.96, Minquan Rd., Xindian Dist., New Taipei City, Taiwan, R.O.C.
Tel:886-2-2219-9518 Fax:886-2-2219-9528

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 1999/5/EC.	**Lietuviškai**	Šiuo **PLANET Technology Corporation,**, skelbia, kad **11ac Wireless AP** tenkina visus svarbiausius 1999/5/EC 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 1999/5/EC.	**Magyar**	A gyártó **PLANET Technology Corporation**, kijelenti, hogy ez a **11ac Wireless AP** megfelel az 1999/5/EK 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 1999/5/EF	**Malti**	Hawnhekk, **PLANET Technology Corporation,** jiddikjara li dan **11ac Wireless AP** jikkonforma mal-ħtiġijiet essenzjali u ma provvedimenti oħrajn relevanti li hemm fid-Dirrettiva 1999/5/EC
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 1999/5/EG 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 1999/5/EG
Eestikeeles	Käesolevaga kinnitab **PLANET Technology Corporation,** et see **11ac Wireless AP** vastab Euroopa Nõukogu direktiivi 1999/5/EC 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 1999/5/EC”.
Ελληνικά	*ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ* , **PLANET Technology Corporation,** *ΔΗΛΩΝΕΙ ΟΤΙ ΑΥΤΟ* **11ac Wireless AP***ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ*	**Português**	**PLANET Technology Corporation**, declara que este **11ac Wireless AP** está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
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 1999/5/CE	**Slovensky**	Výrobca **PLANET Technology Corporation,** týmto deklaruje, že táto **11ac Wireless AP** je v súlade so základnými požiadavkami a ďalšími relevantnými predpismi smernice 1999/5/EC.
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 1999/5/CE	**Slovensko**	**PLANET Technology Corporation**, **s tem potrjuje,** da je ta **11ac Wireless AP** skladen/a z osnovnimi zahtevami in ustreznimi določili Direktive 1999/5/EC.
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 1999/5/CE.	**Suomi**	**PLANET Technology Corporation,** vakuuttaa täten että **11ac Wireless AP** tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Latviski	Ar šo **PLANET Technology Corporation,** apliecina, ka šī **11ac Wireless AP** atbilst Direktīvas 1999/5/EK 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 1999/5/EG.