

User's Manual

1750Mbps 11ac Dual Band Ceiling-mount Enterprise Wireless Access Point

▶ WDAP-C1750



Copyright

Copyright © 2016 by PLANET Technology Corp. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of PLANET.

PLANET makes no representations or warranties, either expressed or implied, with respect to the contents hereof and specifically disclaims any warranties, merchantability or fitness for any particular purpose. Any software described in this manual is sold or licensed "as is". Should the programs prove defective following their purchase, the buyer (and not PLANET, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, PLANET reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation to notify any person of such revision or changes.

All brand and product names mentioned in this manual are trademarks and/or registered trademarks of their respective holders.

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.



IMPORTANT SAFETY PRECAUTIONS:

This device requires professional installation.

Revision

User Manual of PLANET 1750Mbps 802.11ac Dual Band Ceiling-mount Enterprise Wireless Access Point

Model: WDAP-C1750

Rev: 1.0 (Apr., 2016)

Part No. EM-WDAP-C1750_v1.0

CONTENTS

Chapter 1.Product Introduction	1
1.1 Package Contents	1
1.2 Product Description	2
1.3 Product Features	5
1.4 Product Specifications	7
Chapter 2.Hardware Installation	11
2.1 Product Outlook	11
2.1.1 Panel Layout.....	12
2.1.2 Hardware Description.....	13
Chapter 3.Connecting to the AP	14
3.1 System Requirements	14
3.2 Installing the AP	14
Chapter 4.Quick Installation Guide	18
4.1 Manual Network Setup - TCP/IP Configuration	18
4.1.1 Configuring the IP Address Manually.....	18
4.2 Starting Setup in the Web UI	21
4.3 Basic Settings	22
4.3.1 LAN IP Address.....	22
4.3.2 2.4GHz & 5GHz SSID & Security.....	23
4.3.3 Administrator Name & Password.....	23
4.3.4 Time & Date.....	24
Chapter 5.Configuring the AP	25
5.1 Information	25
5.1.1 System Information.....	25
5.1.2 Wireless Clients.....	27
5.1.3 Wireless Monitor.....	28
5.1.4 DHCP Clients.....	29
5.1.5 Log.....	30
5.2 Networking Settings	31
5.2.1 LAN-side IP Address.....	31
5.2.2 LAN Port.....	32
5.2.3 VLAN.....	33
5.3 Wireless Settings	34
5.3.1 2.4GHz 11bgn Basic Settings.....	34
5.3.2 Advanced.....	36
5.3.3 Security.....	37

5.3.4	WDS.....	41
5.3.5	5GHz 11ac 11an Basic Settings	43
5.3.6	Advanced.....	44
5.3.7	Security.....	46
5.3.8	WDS.....	50
5.3.9	WPS.....	52
5.3.10	RADIUS Settings	53
5.3.11	Internal Server	54
5.3.12	RADIUS Accounts.....	55
5.3.13	MAC Filter.....	56
5.3.14	WMM.....	57
5.3.15	Schedule.....	59
5.3.16	Traffic Shaping.....	60
5.4	Management	61
5.4.1	Admin.....	61
5.4.2	Date and Time	63
5.4.3	Syslog Server	64
5.4.4	Ping Test	64
5.4.5	I'm Here	65
5.5	Advanced	65
5.5.1	Reboot Schedule	65
5.5.2	LED Settings.....	66
5.5.3	Update Firmware	66
5.5.4	Save/Restore Settings.....	67
5.5.5	Factory Default	68
5.5.6	Reboot	69
5.6	Operation Mode	70
5.6.1	AP Mode	70
5.6.2	Repeater Mode.....	70
5.6.3	AP Controller Mode	72
5.6.4	Managed AP Mode	73

Chapter 6.NMS74

6.1	Dashboard.....	75
6.2	Zone Plan	75
6.3	NMS Monitor	76
6.3.1	Managed AP	76
6.3.2	Managed AP Group	78
6.3.3	Active WLAN.....	78
6.3.4	Active WLAN Group.....	79
6.3.5	Active Clients	79
6.3.6	All Events/Activities.....	79

6.4	NMS Settings	80
6.4.1	Access Point	80
6.4.2	WLAN.....	86
6.4.3	RADIUS	88
6.4.4	Access Control.....	92
6.4.5	Zone Edit	93
6.4.6	Firmware Upgrade	94
6.4.7	Advanced.....	94
6.5	Local Network.....	95
6.6	Local Settings.....	95
6.7	Toolbox.....	96
Chapter 7.	Quick Connection to a Wireless Network	97
7.1	Windows XP (Wireless Zero Configuration).....	97
7.2	Windows 7 (WLAN AutoConfig).....	99
7.3	Mac OS X 10.x.....	102
7.4	iPhone/iPod Touch/iPad	106
Appendix A:	Planet Smart Discovery Utility.....	109
Appendix B:	Troubleshooting.....	110
Appendix C:	Glossary.....	112

FIGURES

FIGURE 2-1 WDAP-C1750 – TRIPLE VIEW	11
FIGURE 2-2 WDAP-C1750 FRONT PANEL LAYOUT	12
FIGURE 2-3 WDAP-C1750 SIDE PANEL LAYOUT	12
FIGURE 3-1 WDAP-C1750 INSTALLATION DIAGRAM 1	15
FIGURE 3-2 WDAP-C1750 INSTALLATION DIAGRAM 2	15
FIGURE 3-3 WDAP-C1750 T-RAIL MOUNT DIAGRAM 1	16
FIGURE 3-4 WDAP-C1750 T-RAIL MOUNT DIAGRAM 2	17
FIGURE 3-5 WDAP-C1750 INSTALLATION – CONNECT TO PoE SWITCH	17
FIGURE 4-1 TCP/IP SETTING	19
FIGURE 4-2 WINDOWS START MENU	19
FIGURE 4-3 SUCCESSFUL RESULT OF PING COMMAND	20
FIGURE 4-4 FAILED RESULT OF PING COMMAND	20
FIGURE 4-5 LOGIN BY DEFAULT IP ADDRESS	21
FIGURE 4-6 LOGIN WINDOW	21
FIGURE 4-7 BASIC SETTINGS - DHCP	22
FIGURE 4-8 BASIC SETTINGS - WIRELESS SETTINGS	23
FIGURE 4-9 BASIC SETTINGS - ADMINISTRATOR SETTING	23
FIGURE 4-10 BASIC SETTINGS - TIME & DATE	24
FIGURE 5-1 INFORMATION - MAIN MENU	25
FIGURE 5-2 INFORMATION -- WIRELESS CLIENTS	27
FIGURE 5-3 INFORMATION -- WIRELESS MONITOR	28
FIGURE 5-4 INFORMATION – DHCP CLIENTS	29
FIGURE 5-5 INFORMATION -- LOG	30
FIGURE 5-6 NETWORK SETTINGS -- LAN-SIDE IP ADDRESS	31
FIGURE 5-7 NETWORK SETTINGS -- LAN PORT	32
FIGURE 5-8 NETWORK SETTINGS -- VLAN	33
FIGURE 5-9 2.4GHZ WIRELESS SETTINGS	34
FIGURE 5-10 2.4GHZ WIRELESS SETTINGS -- ADVANCED	36
FIGURE 5-11 2.4GHZ WIRELESS SETTINGS -- SECURITY	37
FIGURE 5-12 2.4GHZ WIRELESS SETTINGS -- WEP	38
FIGURE 5-13 2.4GHZ WIRELESS SETTINGS -- IEEE802.1X/EAP	39
FIGURE 5-14 2.4GHZ WIRELESS SETTINGS -- WPA-PSK	39
FIGURE 5-15 2.4GHZ WIRELESS SETTINGS -- WPA-EAP	40
FIGURE 5-16 2.4GHZ WIRELESS SETTINGS -- WDS	42
FIGURE 5-17 5GHZ WIRELESS SETTINGS	43
FIGURE 5-18 5GHZ WIRELESS SETTINGS - ADVANCED	45
FIGURE 5-19 5GHZ WIRELESS SETTINGS -- SECURITY	46
FIGURE 5-20 5GHZ WIRELESS SETTINGS -- WEP	47
FIGURE 5-21 5GHZ WIRELESS SETTINGS -- IEEE802.1X/EAP	48
FIGURE 5-22 5GHZ WIRELESS SETTINGS -- WPA-PSK	48
FIGURE 5-23 5GHZ WIRELESS SETTINGS -- WPA-EAP	49
FIGURE 5-24 5GHZ WIRELESS SETTINGS -- WDS	51

FIGURE 5-25 WPS	52
FIGURE 5-26 RADIUS SETTINGS	53
FIGURE 5-27 INTERNAL SERVER	54
FIGURE 5-28 RADIUS ACCOUNTS	55
FIGURE 5-29 MAC FILTER	56
FIGURE 5-30 WMM	57
FIGURE 5-31 SCHEDULE	59
FIGURE 5-32 TRAFFIC SHAPING	60
FIGURE 5-33 ADMIN	61
FIGURE 5-34 TIME AND DATE	63
FIGURE 5-35 SYSLOG SERVER	64
FIGURE 5-36 PING TEST	64
FIGURE 5-37 I'M HERE	65
FIGURE 5-38 REBOOT SCHEDULE	65
FIGURE 5-39 LED SETTINGS	66
FIGURE 5-40 UPDATE FIRMWARE	66
FIGURE 5-41 SAVE/RESTORE SETTINGS	67
FIGURE 5-42 FACTORY DEFAULT	68
FIGURE 5-43 REBOOT	69
FIGURE 5-44 AP MODE	70
FIGURE 5-45 REPEATER MODE	71
FIGURE 5-46 REPEATER MODE -- SITE SURVEY	71
FIGURE 5-47 AP CONTROLLER MODE	72
FIGURE 5-48 MANAGED AP MODE	73
FIGURE 6-1 DASHBOARD	75
FIGURE 6-2 ZONE PLAN	76
FIGURE 6-3 NMS MONITOR—MANAGED AP	76
FIGURE 6-4 NMS MONITOR—MANAGED AP GROUP	78
FIGURE 6-5 NMS MONITOR—ACTIVE WLAN	78
FIGURE 6-6 NMS MONITOR—ACTIVE WLAN GROUP	79
FIGURE 6-7 CLIENTS—ACTIVE CLIENTS	79
FIGURE 6-8 INFORMATION—ALL EVENTS/ACTIVITIES	80
FIGURE 6-9 NMS SETTINGS—ACCESS POINT	80
FIGURE 6-10 NMS SETTINGS—ACCESS POINT BASIC SETTINGS	81
FIGURE 6-11 NMS SETTINGS—ACCESS POINT VLAN SETTINGS	82
FIGURE 6-12 NMS SETTINGS—ACCESS POINT RADIO SETTINGS	83
FIGURE 6-13 NMS SETTINGS—ACCESS POINT ADVANCED SETTINGS	84
FIGURE 6-14 NMS SETTINGS—ACCESS POINT PROFILE SETTINGS	85
FIGURE 6-15 NMS SETTINGS—WLAN	86
FIGURE 6-16 NMS SETTINGS—WLAN SETTINGS	87
FIGURE 6-17 NMS SETTINGS—WLAN GROUP SETTINGS	88
FIGURE 6-18 NMS SETTINGS—EXTERNAL RADIUS SERVER	89
FIGURE 6-19 NMS SETTINGS—INTERNAL RADIUS SERVER	90
FIGURE 6-20 NMS SETTINGS—RADIUS ACCOUNT	91
FIGURE 6-21 NMS SETTINGS—ACCESS CONTROL	92

FIGURE 6-22 NMS SETTINGS—ZONE EDIT	93
FIGURE 6-23 NMS SETTINGS—FIRMWARE UPGRADE	94
FIGURE 6-24 NMS SETTINGS—ADVANCED	94
FIGURE 6-25 LOCAL NETWORK	95
FIGURE 6-26 LOCAL SETTINGS	95
FIGURE 6-27 TOOLBOX.....	96
FIGURE 7-1 SYSTEM TRAY – WIRELESS NETWORK ICON	97
FIGURE 7-2 CHOOSE A WIRELESS NETWORK	97
FIGURE 7-3 ENTER THE NETWORK KEY.....	98
FIGURE 7-4 CHOOSE A WIRELESS NETWORK -- CONNECTED	98
FIGURE 7-5 NETWORK ICON	99
FIGURE 7-6 WLAN AUTOCONFIG	99
FIGURE 7-7 TYPE THE NETWORK KEY	100
FIGURE 7-8 CONNECTING TO A NETWORK	100
FIGURE 7-9 CONNECTED TO A NETWORK.....	101
FIGURE 7-10 MAC OS – NETWORK ICON	102
FIGURE 7-11 HIGHLIGHT AND SELECT THE WIRELESS NETWORK.....	102
FIGURE 7-12 ENTER THE PASSWORD	103
FIGURE 7-13 CONNECTED TO THE NETWORK	103
FIGURE 7-14 SYSTEM PREFERENCES	104
FIGURE 7-15 SYSTEM PREFERENCES -- NETWORK.....	104
FIGURE 7-16 SELECT THE WIRELESS NETWORK.....	105
FIGURE 7-17 IPHONE – SETTINGS ICON.....	106
FIGURE 7-18 WI-FI SETTING	106
FIGURE 7-19 WI-FI SETTING – NOT CONNECTED	107
FIGURE 7-20 TURN ON WI-FI.....	107
FIGURE 7-21 IPHONE -- ENTER THE PASSWORD	108
FIGURE 7-22 IPHONE -- CONNECTED TO THE NETWORK	108

Chapter 1. Product Introduction

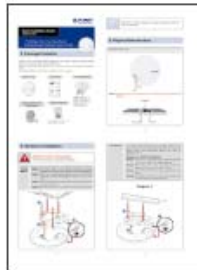
1.1 Package Contents

Thank you for choosing PLANET WDAP-C1750. Before installing the AP, please verify the contents inside the package box.

WDAP-C1750



Quick Guide



T-rail Mounting Kit



- Plastic spacer x 2
- Long T-rail clip x 2
- Short T-rail clip x 2
- Long screw x 2
- Short screw x 2

**Mounting Bracket with
Thumb Screw**



Ceiling Mounting Kit



- Self-tapping screw x 4
- Screw anchor x 4



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

1.2 Product Description

Ultra-high-speed, Enterprise-class Wireless LAN Solution

To meet enterprise demand, PLANET WDAP-C1750 has enhanced security and management features including **SSID-based VLAN**, **SNMP**, internal **RADIUS Server** and cost-effective **NMS (Network Management System)**. With **3T3R MIMO IEEE 802.11ac** dual-band technology, the WDAP-C1750 provides extreme wireless speed up to **450 + 1300Mbps** (2.4GHz + 5GHz). The incredible wireless speed makes it ideal for handling multiple HD video streams, VoIPs and data sessions stably at the same time, specifically designed for SMBs, hotels, hospitals or anywhere with high-density network application.



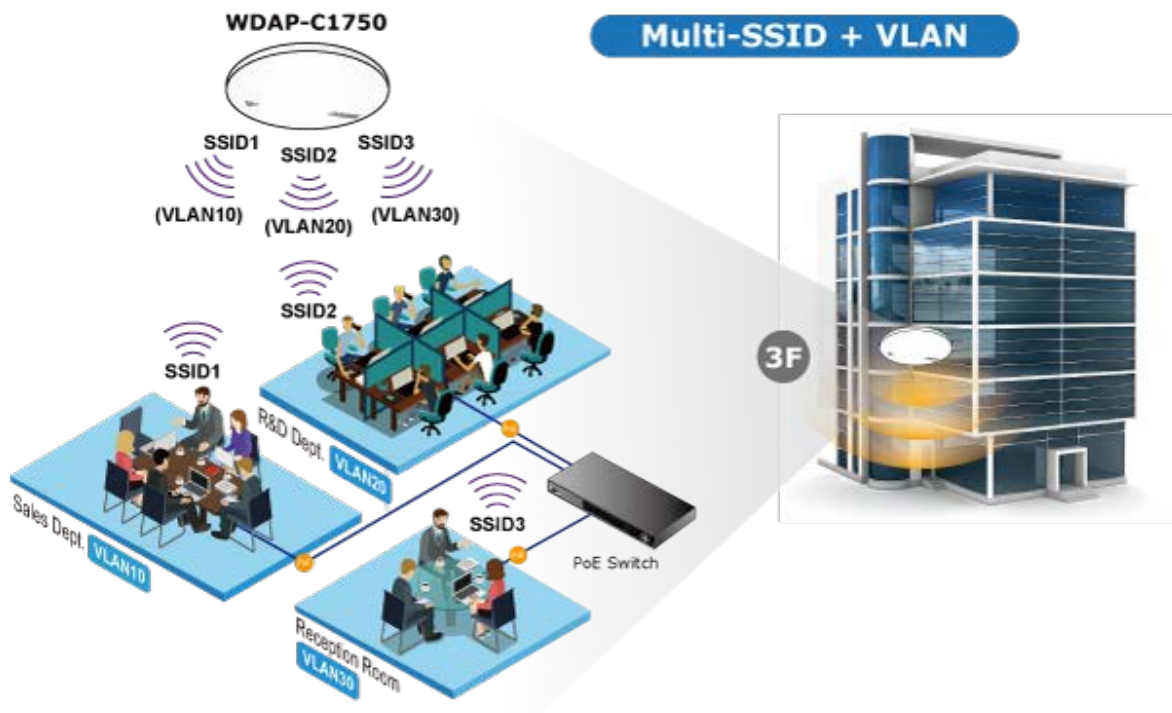
Central Management with NMS

The WDAP-C1750 with **NMS (Network Management System)** permits users to monitor and manage their entire operations when in the operation mode. When entering the NMS control platform, the dashboard displays an at-a-glance view of their wireless networks including system information, managed AP, managed AP group and active client list with real-time scanning. The graphical zone plan showing the wireless coverage including heat maps, devices and location can be customized with the floor map you uploaded. With NMS, any WDAP-C1750 can be the controller of a manageable wireless network.



Secure and Manageable Wireless Network

Besides the WEP/WPA/WPA2 encryption for stations, the WDAP-C1750 is integrated with an internal RADIUS server and MAC-based ACL to authenticate and protect your wireless LAN to prevent unauthorized wireless connections. For management purposes, the WDAP-C1750 enables the system administrator to remotely monitor the wireless network status through the SNMP and the syslog server, and the IEEE 802.1Q tagged VLAN to be mapped to multiple SSIDs (16 sets of SSIDs per radio) to distinguish the wireless access in the Internal VLAN topology. The tagged VLAN also allows to be transmitted across the WDS connection and thus it is the best Wireless LAN solution to enterprises to isolate traffic guests from internal usage.



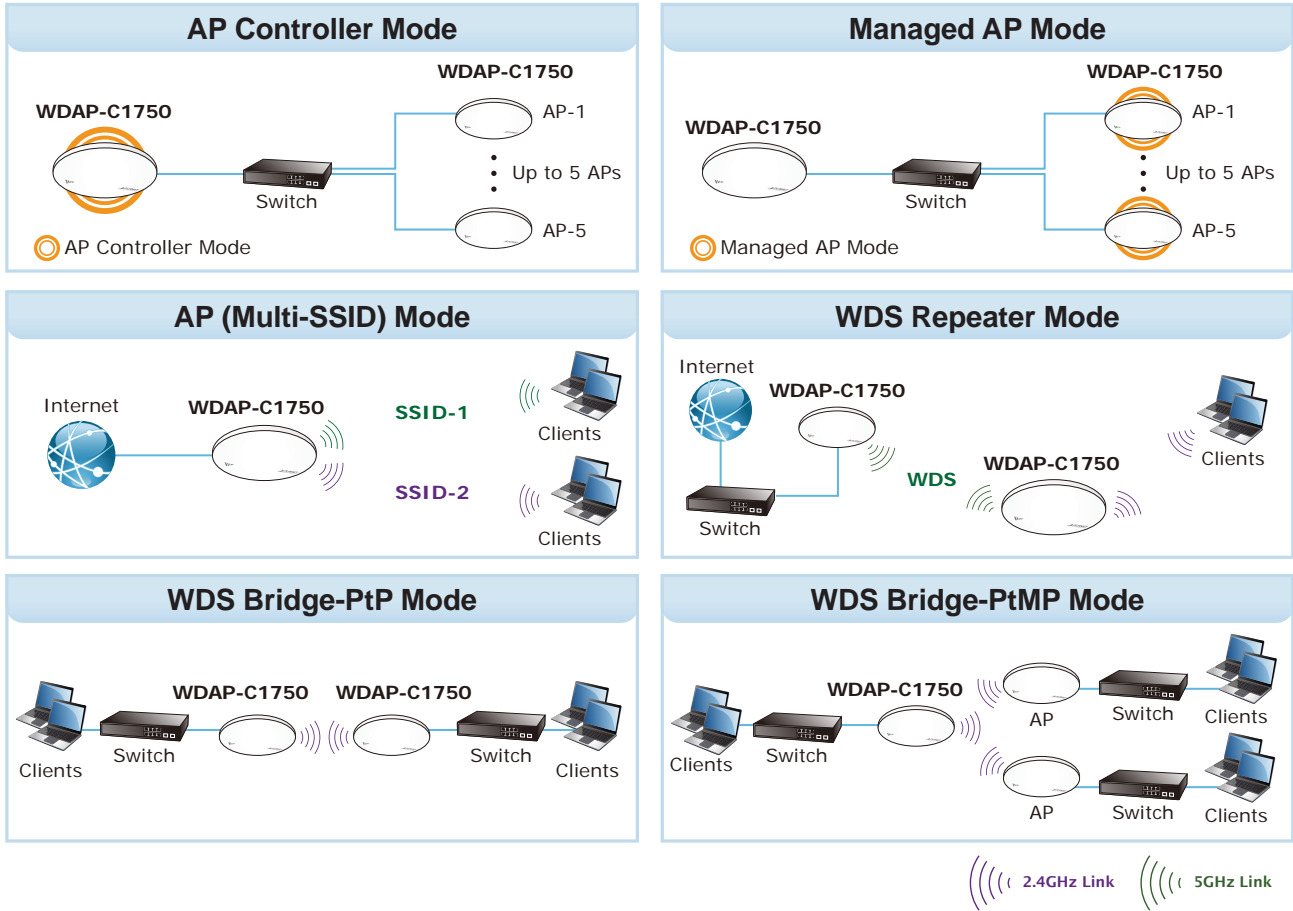
T-rail Ceiling-mount Design Perfect for Office

The WDAP-C1750 has an elegant, ultra slim, durable ceiling-mount housing, which provides more flexible deployment options for enterprises. By supporting the standard IEEE 802.3at PoE PD power scheme, the WDAP-C1750 can be powered and networked by a single UTP cable, effectively eliminating the needs of dedicated electrical outlets on the ceiling and reducing the cabling cost. Furthermore, the system administrator is able to arrange PoE schedule by using the managed PoE switch. Besides the standard ceiling-mounting kit, the WDAP-C1750 provides an extra T-rail mounting kit allowing IT engineers to easily hang bulky APs without any construction.



Multiple Operation Modes for Various Applications

In the aspect of management, the WDAP-C1750 supports AP Controller and Managed AP modes in NMS scheme. The WDAP-C1750 being an AP Controller is able to centrally manage up to 5 WDAP-C1750 units acting as managed APs. As to common wireless application, it supports WDS Bridge PtP, WDS Bridge PtMP and Repeater modes, through which it provides more flexibility for users when wireless network is established. Compared with general wireless access point, the WDAP-C1750 offers more powerful and flexible capability for wireless clients.



1.3 Product Features

- **Standard Compliant Hardware Interface**
 - Complies with IEEE 802.11ac and IEEE 802.11a/b/g/n standards
 - 1 x 10/100/1000BASE-T port with IEEE 802.3at PoE PD supported
 - 1 x micro USB 2.0 port for image upgrade and configuration backup/restore
- **RF Interface Characteristics**
 - 2.4GHz (802.11b/g/n) and 5GHz (802.11a/n/ac) concurrent dual band for more efficiency of carrying high traffic loads
 - 3T3R MIMO technology for enhanced throughput and coverage
 - Provides multiple adjustable transmit power control
 - Wireless data transfer rate of up to 1.75Gbps (450Mbps at 2.4GHz + 1300Mbps at 5GHz)
- **Comprehensive Wireless Advanced Features**
 - Multiple Wireless Modes: AP, Repeater, WDS PtP, WDS PtMP
 - NMS Operation Modes: AP Controller, Managed AP
 - Supports up to 16 multi-SSIDs per radio (32 multi-SSIDs per AP)
 - Supports SSID-based VLAN, tagged VLAN over WDS connection
 - Supports WMM (Wi-Fi Multimedia) and wireless QoS to enhance the efficiency of multimedia application

- Self-healing (Schedule Reboot) mechanism for reliable connection
- Multicast rate adaptation guarantees wireless bandwidth and service quality
- Load balancing achieved through the defined number of associated clients per SSID or station idle timeout control

➤ **Secure Network Connection**

- Advanced security for clients: 64/128-bit WEP, WPA/WPA2, WPA-PSK/WPA2-PSK (TKIP/AES encryption) and 802.1x RADIUS authentication
- Supports WPS (Wi-Fi Protected Setup)
- Built-in RADIUS server for authenticating up to 256 user accounts
- Supports MAC address filtering up to 256 entries
- Wireless Isolation between SSIDs or clients connected to the same SSID

➤ **Easy Installation & Management**

- Ultra slim and durable ceiling-mount design with extra T-rail mounting kit provided for office environment
- Flexible deployment with standard IEEE 802.3at PoE PD supported
- Web-based configuration through HTTP/HTTPS/SSH/CLI interface
- SNMP-based management interface
- Central management with firmware-based NMS (Network Management System) interface
- Diagnostic LED and built-in buzzer will sound temporarily to help identify and locate the AP
- Supports Syslog Server for sending syslog messages to the external servers for remote tracking
- System status monitoring includes DHCP Client and System Log

➤ **NMS Management Features**

- Supports up to 5 managed APs with no additional wireless AP controller
- Dashboard display for the system, AP, AP group and associated client information
- Zone Plan with heat map view allows user to upload customized floor plan
- AP Cluster Management and AP Cluster provisioning
- AP bulk firmware upgrade
- AP/Client status monitoring

1.4 Product Specifications

Product	WDAP-C1750 1750Mbps 802.11ac Dual Band Ceiling-mount Enterprise Wireless Access Point	
Hardware Specifications		
Interfaces	LAN	1 x 10/100/1000BASE-T RJ45 port Auto-negotiation and auto MDI/MDI-X
	USB	1 x micro USB 2.0 port
Antennas	Gain	Internal PIFA antenna (3 x 2.4GHz 4dBi, 3 x 5GHz 5dBi)
Button	Reset button	
LED Indicators	PWR/Diag LED Allow LED to turn off via software control	
Other	Internal buzzer	
Material	Plastic front panel, metal rear panel	
Dimensions (Φ x H)	208 x 31.5 mm	
Weight	590g	
Power Requirements	PoE: 802.3at PoE-PD Class 4 12V DC, 2A (not included in the standard package)	
Power Consumption (Max.)	15W, 19.2W (with USB)	
Mounting	Ceiling mount	
Wireless Interface Specifications		
Standard	IEEE 802.11ac 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	<u>America -- FCC:</u> 36, 40, 44, 48, 149, 153, 157, 161, 165 <u>Europe -- ETSI:</u> 36, 40, 44, 48 <i>5GHz channel list will vary in different countries according to their regulations.</i>
Channel Width	802.11ac: 20/40/80MHz	

	802.11n: 20/40MHz
Transmission Speed	450 + 1300Mbps (2.4GHz + 5GHz)
Transmission Distance	802.11ac: up to 35m 802.11n: up to 70m 802.11a/b/g: up to 30m <i>The estimated transmission distance is based on the theory. The actual distance will vary in different environments.</i>
Max. RF Power (limited by local regulation)	5GHz: 802.11ac (VHT20/40/80): 27.5dBm @MCS0 802.11ac (VHT20/40/80): 22.5dBm @MCS7 802.11ac (VHT20/40/80): 19.5dBm @MCS9 802.11n (HT20/40): 27.5dBm @MCS0/MCS8 802.11n (HT20/40): 22.5dBm @MCS7/MCS15 802.11a: 26.5dBm @6Mbps 22.5dBm @54Mbps
	2.4GHz: 802.11n (HT20/40): 27.5dBm @MCS0 802.11n (HT20/40): 22.5dBm @MCS7 802.11g: 27.5dBm @6Mbps 802.11g: 23.5dBm @54Mbps 802.11b: 27.5dBm @1Mbps
Receive Sensitivity	5GHz: 802.11ac (VHT20/40/80): -84dBm @MCS0 802.11ac (VHT20/40/80): -58dBm @MCS9 802.11n (HT20): -90dBm @MCS0, -70dBm @MCS7 802.11n (HT40): -87dBm @MCS0, -68dBm @MCS7 802.11a: -90dBm @6Mbps 802.11a: -71dBm @54Mbps
	2.4GHz: 802.11n (HT20/40): -83dBm @MCS0 802.11n (HT20/40): -66dBm @MCS7 802.11g: -86dBm @54Mbps 802.11g: -72dBm @54Mbps 802.11b: -93dBm @1Mbps 802.11b: -85dBm @11Mbps
Software Features	
Operation Mode (NMS)	<ul style="list-style-type: none"> ■ AP Controller ■ Managed AP
Wireless Mode	<ul style="list-style-type: none"> ■ AP (Access Point) ■ WDS PTP (Point to Point) ■ Repeater ■ WDS PTMP (Point to Multipoint)
Encryption Security	<ul style="list-style-type: none"> ■ WEP (64/128-bit) encryption security ■ WPA/WPA2 (TKIP/AES) ■ WPA-PSK/WPA2-PSK (TKIP/AES) ■ 802.1x authentication
Wireless Security	Wireless MAC address filtering up to 256 entries
	Wireless Client Isolation: STA separator, SSID separator
	Supports WPS (Wi-Fi Protected Setup)
	Enable/Disable SSID broadcast

Wireless Advanced	6-level adjustable Tx power (100%, 90%, 75%, 50%, 25%, 10%)
	Multiple SSIDs: up to 16 at 2.4GHz and 16 at 5GHz
	Tagged VLAN per SSID, tagged VLAN over WDS
	Auto-channel selection: enables an AP to determine the best channel available
	Rogue AP detection
	Provides wireless statistics for system administrator monitoring
Max. Clients	Wired: 253 2.4GHz Wireless: 50 5GHz Wireless: 50
Max. WDS Peers	Up to 4 at 2.4GHz and 4 at 5GHz
QoS	IEEE 802.11e WMM (Wi-Fi Multimedia)
	Station Idle Timeout: Enables and configures it to prevent inactivated clients from occupying the connection.
	AP Load Balancing: To balance the distribution of wireless client connections across multiple APs.
	Supports multicast rate adaptation mechanism to guarantee the wireless bandwidth and service quality.
LAN	Static IP, DHCP Client, DHCP Server
	Supports 802.1d Spanning Tree (RTSP)
	Supports 802.1Q tagged/untagged VLAN (VID: 1-4095)
System Management	NMS firmware-based management interface: <ul style="list-style-type: none"> ■ Supports up to 5 managed APs with no additional wireless controller ■ Features dashboard and zone plan with heat map, AP cluster management, AP bulk firmware upgrade, AP/client status monitoring
	Web-based (HTTP/HTTPS/SSH/CLI) management interface
	SNMP v1, v2c, v3 management interface
	Built-in RADIUS server with EAP authentication (MS-PEAP)
	User account up to 256
	SNTP synchronization
	Easy firmware upgrade
	Supports self-healing (schedule reboot) mechanism for reliable connection
	Supports PLANET Smart Discovery Utility
	Supports system log and syslog server
Standards Conformance	
IEEE Standards	IEEE 802.11ac (wave 1, 3T3R, up to 1300Mbps)
	IEEE 802.11n (3T3R, up to 450Mbps)
	IEEE 802.11g
	IEEE 802.11a
	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
	IEEE 802.3az Energy Efficient Ethernet

	IEEE 802.3at Power over Ethernet plus
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-C1750 to the existing network devices and your computers.

2.1 Product Outlook

- **Dimensions: (Φ x H)**
208 x 31.5 mm
- **Weight :**
590g



Figure 2-1 WDAP-C1750 – Triple View

2.1.1 Panel Layout

Figure 2-2 and Figure 2-3 show the hardware interface of the WDAP-C1750.

Hardware Interface

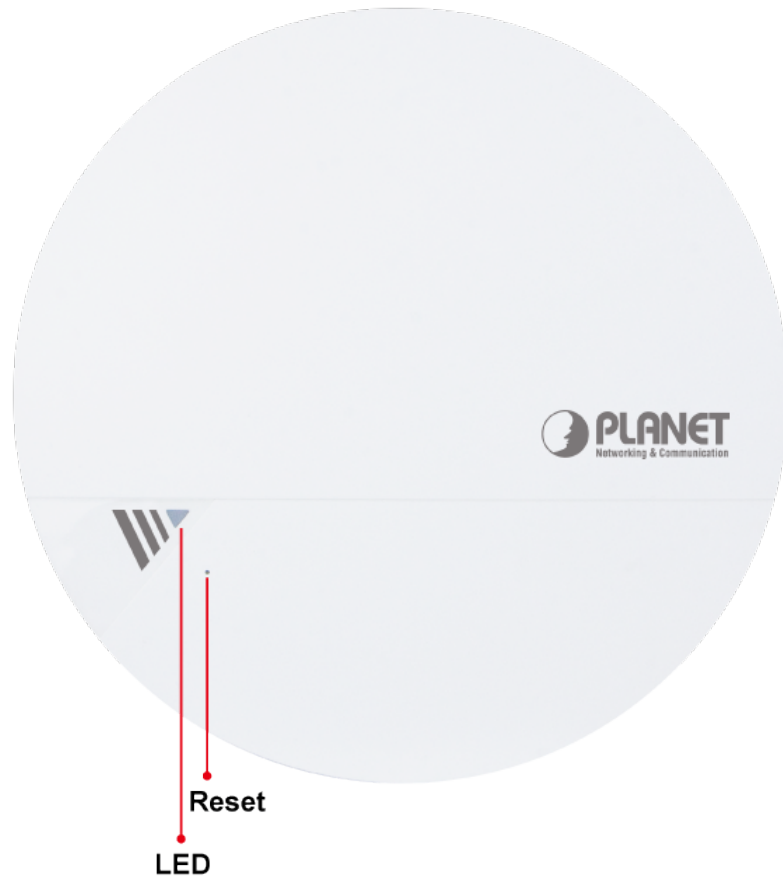


Figure 2-2 WDAP-C1750 Front Panel Layout

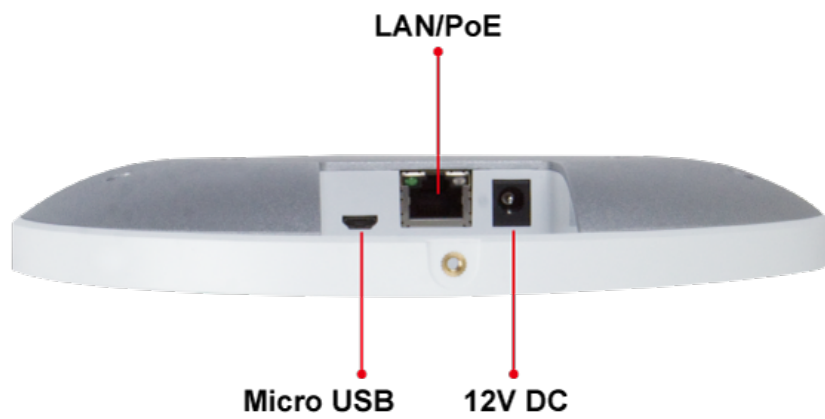


Figure 2-3 WDAP-C1750 Side Panel Layout

2.1.2 Hardware Description

Port definition

Object	Description
12V DC	DC port supports 12V DC/2A power adapter. The WDAP-C1750 can be powered by 802.3at PoE switch. The power adapter is not included in the standard package and should be purchased separately if required.
LAN/PoE	LAN port with Power over Ethernet (PoE) IN.
Micro USB	Connect any USB memory stick to the micro USB 2.0 port for firmware image upgrade and system configuration file backup/restore.
Reset	To restore to the factory default setting, press and hold the Reset Button by using the paper clip for at least 8 seconds, and then release it.

LED definition

LED Color	LED STATUS	FUNCTION
Purple	On	The system is initializing.
Blue	On	The access point is finished initializing and ready.
	Off	The access point is powered off or LED is disabled.
	Slow Flashing	Firmware upgrade in progress.
	Fast Flashing	Resetting to factory defaults in progress.

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-C1750)
- 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



1. The AP in the following instructions refers to PLANET WDAP-C1750.
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.

For Wooden Ceilings

1. Place the mounting bracket to a ceiling in your desired location and use the four self-tapping screws included in the ceiling mounting kit to fix it into place.
2. Attach the AP to the mounting bracket by aligning the grooves in the AP to the ceiling mount.
3. Secure the AP firmly in place using the thumb screw.

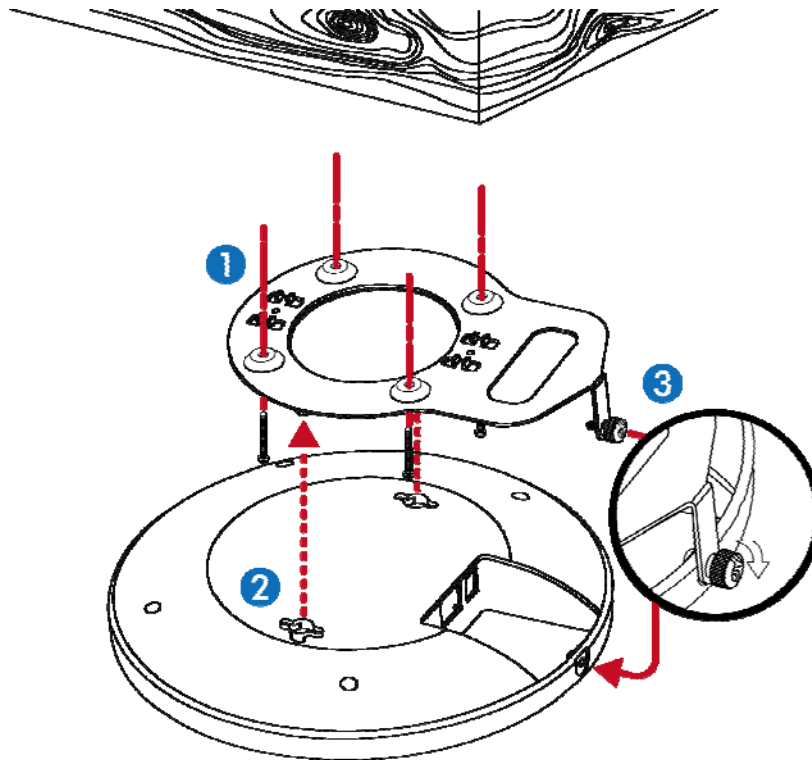


Figure 3-1 WDAP-C1750 Installation Diagram 1

For Other Ceilings

1. Drill four holes in your ceiling using the mounting bracket as a guide, and insert the four screw anchors.
2. Align the mounting bracket with your screw anchors and use the four self-tapping screws to fix it into place.
3. Attach the AP to the mounting bracket by aligning the grooves in the AP.
4. Secure the AP firmly in place using the thumb screw.

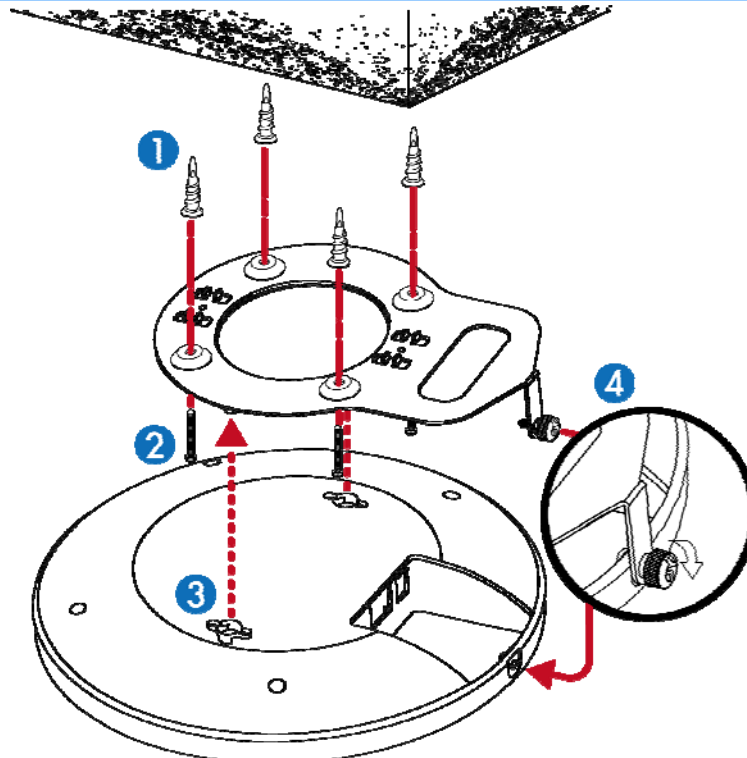


Figure 3-2 WDAP-C1750 Installation Diagram 2

T-rail Mount

To mount the AP to a T-rail, you need to select a T-rail clip whose size must go with the width of the T-rail. Please follow the instructions below and refer to Diagram 1 or 2.

Diagram 1: Tight-fit installation

1. Attach the T-rail clips to the mounting bracket using the included two **short screws**.
2. Attach the AP to the mounting bracket by aligning it with the grooves in the AP.
3. Secure the AP firmly in place using the thumb screw.
4. Hang the AP onto the T-rail on the ceiling with the assembled mounting bracket.

Diagram 2: Retention gap installation

1. Pre-assemble the T-rail clips and the plastic spacers to the mounting bracket using the included two **long screws**.
2. Attach the AP to the mounting bracket by aligning the grooves in the AP.
3. Secure the AP firmly in place using the thumb screw.
4. Hang the AP onto the ceiling via T-rail with assembled mounting bracket.

Diagram 1

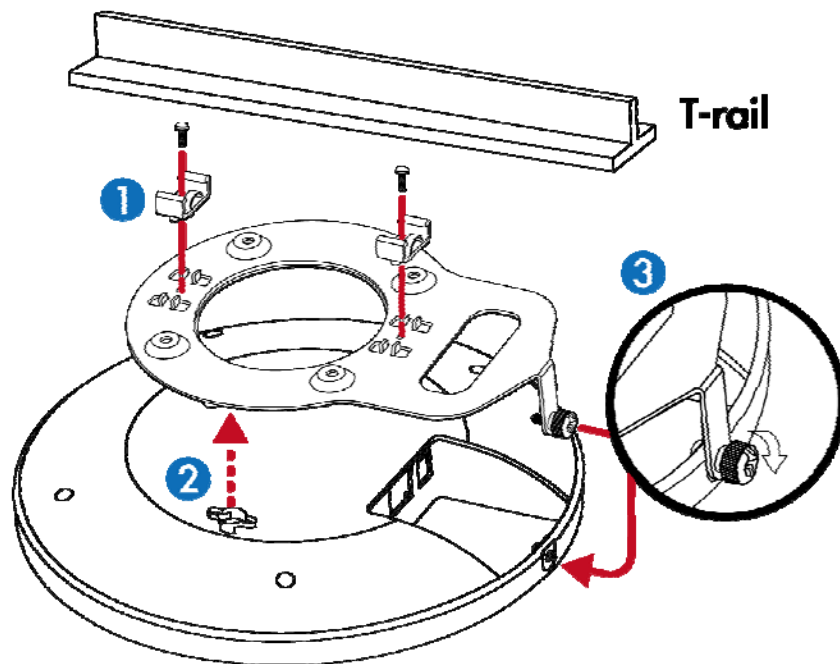


Figure 3-3 WDAP-C1750 T-rail Mount Diagram 1

Diagram 2

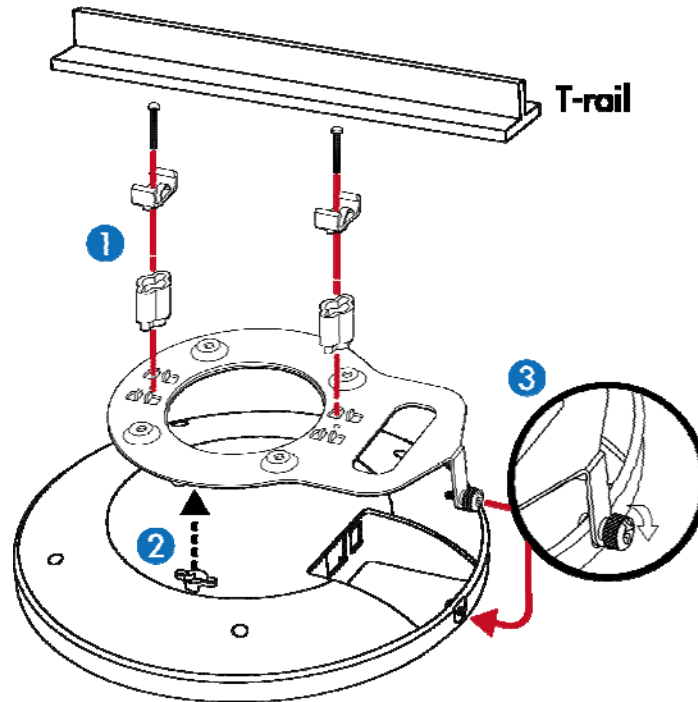


Figure 3-4 WDAP-C1750 T-rail Mount Diagram 2

Step 2.

Plug the RJ45 Ethernet cable into the PoE port of the WDAP-C1750 and the other end of Ethernet cable into the PoE switch.

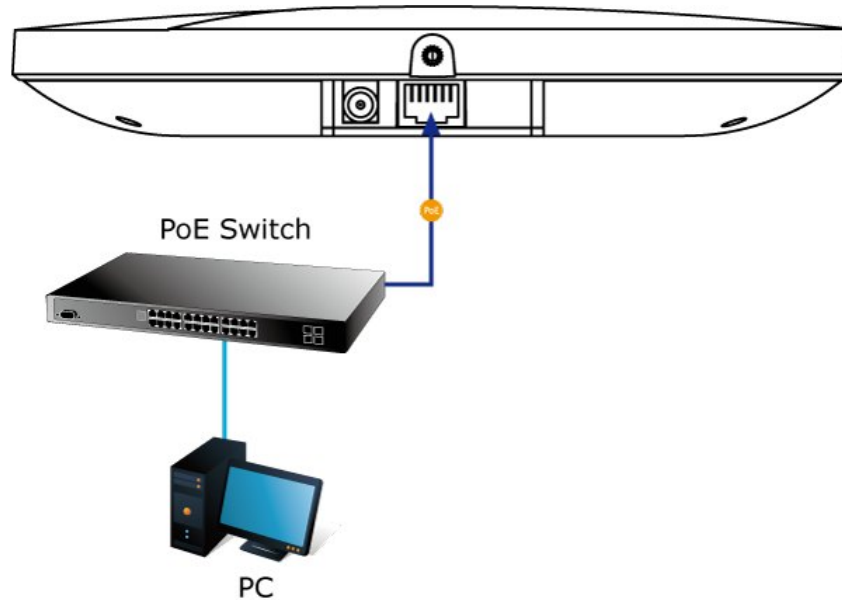


Figure 3-5 WDAP-C1750 Installation – connect to PoE switch

Chapter 4. Quick Installation Guide

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



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-C1750 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-C1750 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-C1750 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-C1750 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-C1750 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.

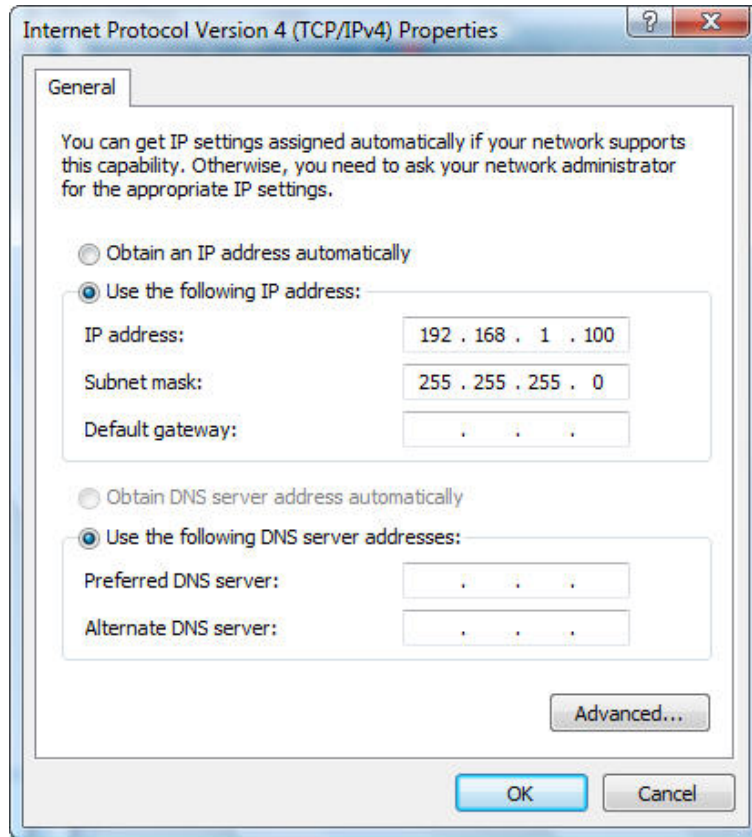


Figure 4-1 TCP/IP Setting

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.

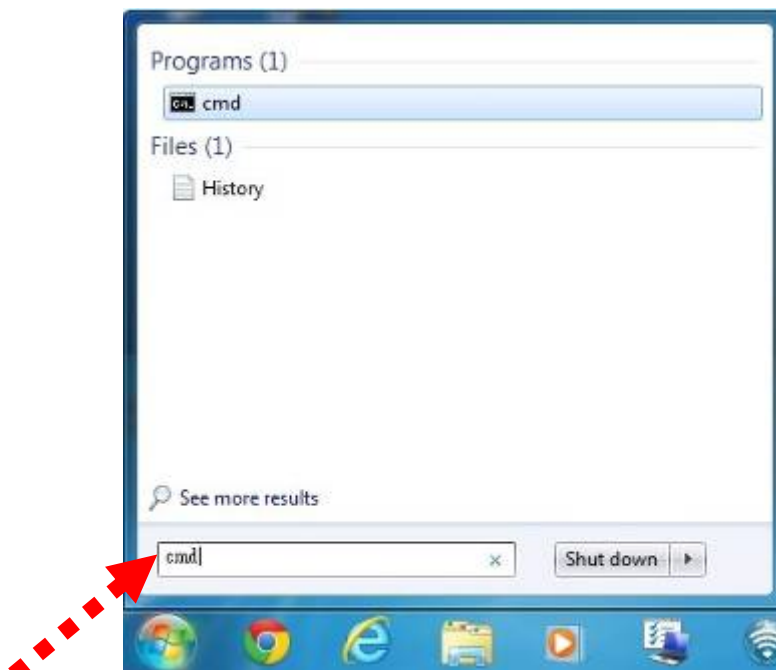


Figure 4-2 Windows Start Menu

- 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.

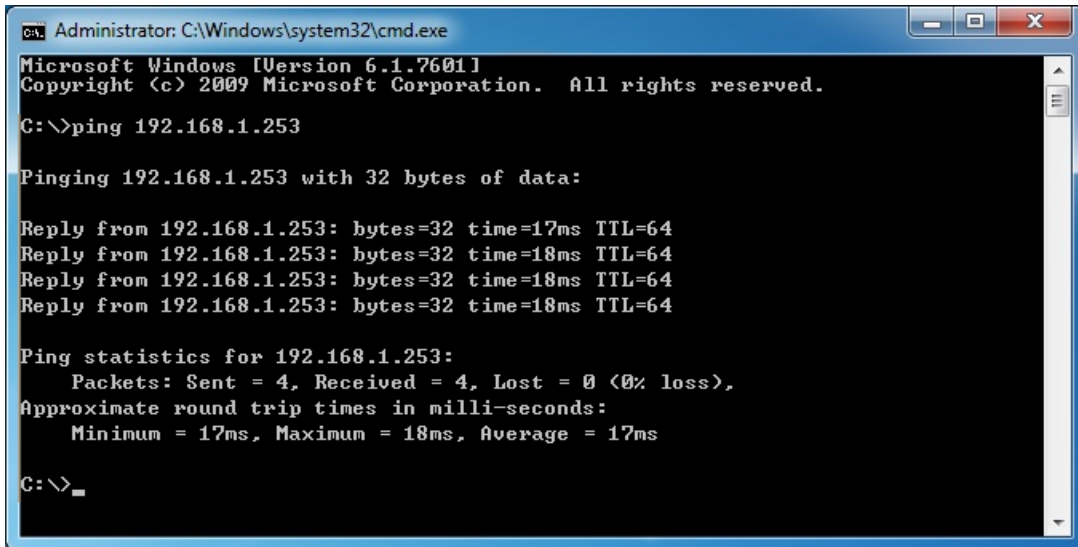


Figure 4-3 Successful Result of Ping Command

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

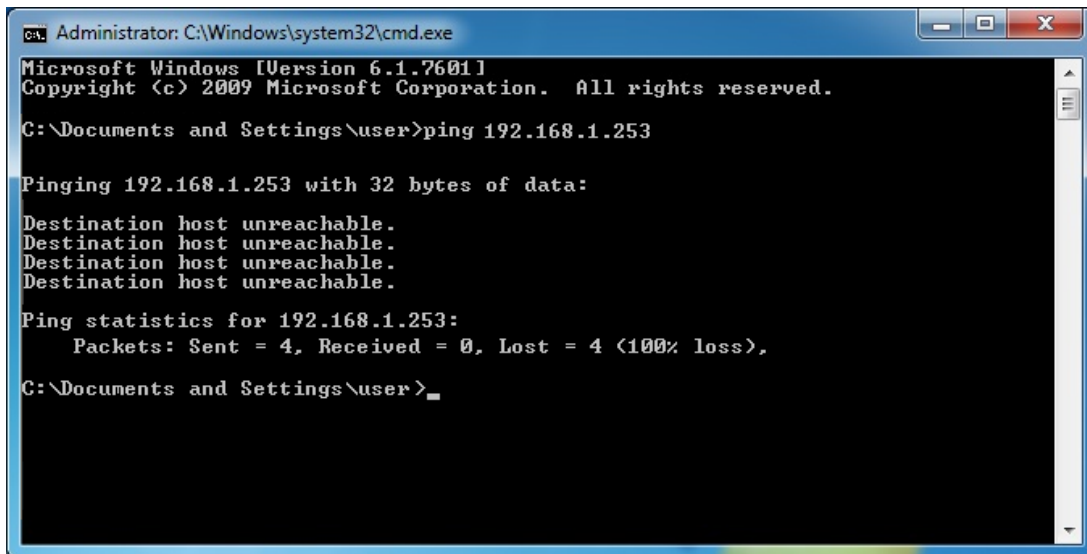


Figure 4-4 Failed Result of Ping Command

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.

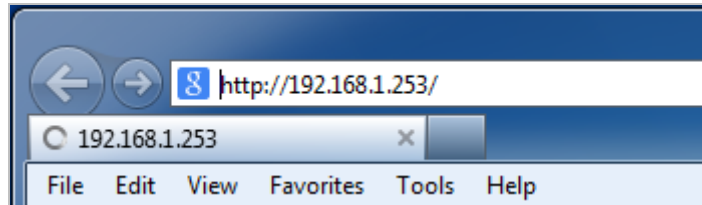


Figure 4-5 Login by default IP address

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.

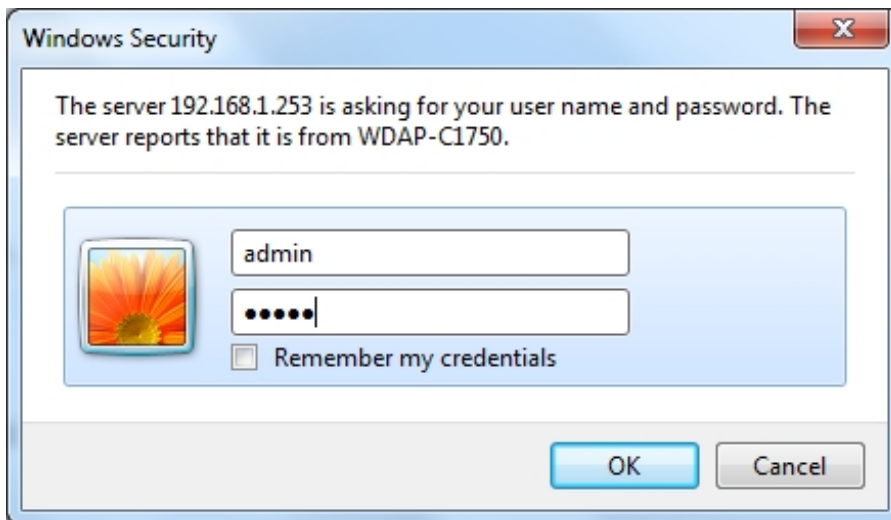


Figure 4-6 Login Window

Default IP Address: **192.168.1.253**

Default User name: **admin**

Default Password: **admin**



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



It is recommended you configure these settings before using Planet WDAP-C1750.

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.

LAN-side IP Address	
IP Address Assignment	DHCP Client <input type="button" value="v"/>
IP Address	192.168.1.253
Subnet Mask	255.255.255.0
Default Gateway	From DHCP <input type="button" value="v"/> <input type="text" value=""/>
Primary DNS Address	From DHCP <input type="button" value="v"/> <input type="text" value="0.0.0.0"/>
Secondary DNS Address	From DHCP <input type="button" value="v"/> <input type="text" value="0.0.0.0"/>

Figure 4-7 Basic Settings - DHCP

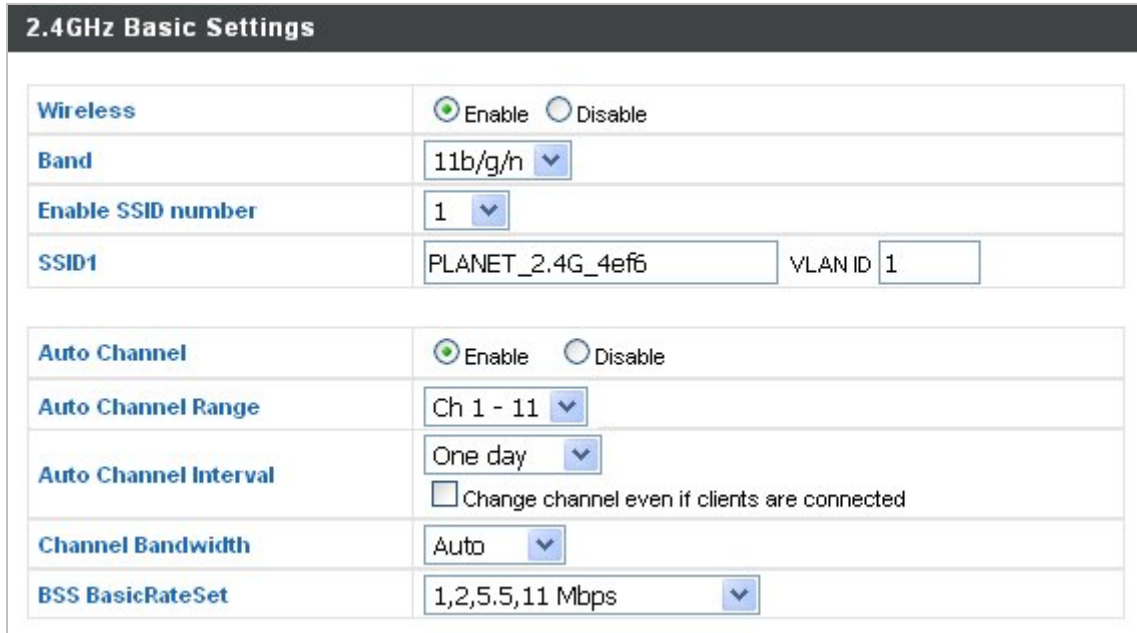
2. Enter the IP address settings you want to use for your access point. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click “Apply” to save the changes and wait a few moments for the access point to reload.



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-C1750'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".



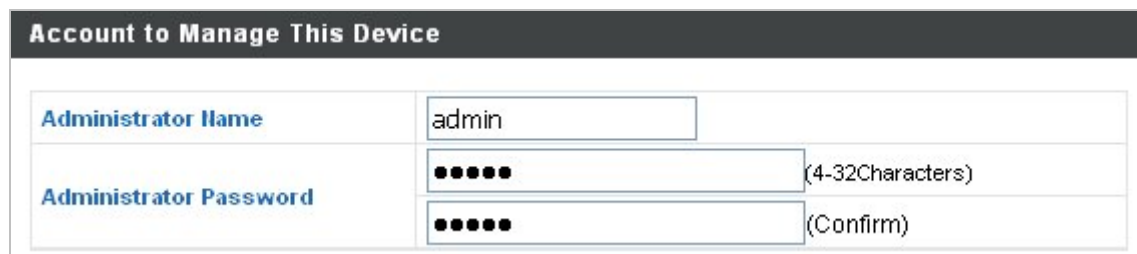
2.4GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11b/g/n
Enable SSID number	1
SSID1	PLANET_2.4G_4ef6
VLAN ID	1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Ch 1 - 11
Auto Channel Interval	One day
	<input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto
BSS BasicRateSet	1,2,5.5,11 Mbps

Figure 4-8 Basic Settings - Wireless settings

2. Go to "Wireless Setting" > "5GHz 11ac 11an" and repeat step 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".



Account to Manage This Device	
Administrator Name	admin
Administrator Password	••••• (4-32Characters)
	••••• (Confirm)

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”.

Date and Time Settings	
Local Time	2012 <input type="button" value="v"/> Year Jan <input type="button" value="v"/> Month 1 <input type="button" value="v"/> Day 0 <input type="button" value="v"/> Hours 00 <input type="button" value="v"/> Minutes 00 <input type="button" value="v"/> Seconds
<input type="button" value="Acquire Current Time from Your PC"/>	
NTP Time Server	
Use NTP	<input type="checkbox"/> Enable
Server Name	User-Defined <input type="button" value="v"/> <input style="width: 100%;" type="text"/>
Update Interval	24 <input type="button" value="v"/> (Hours)
Time Zone	
Time Zone	(GMT-06:00) Central Time (US & Canada) <input type="button" value="v"/>

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.

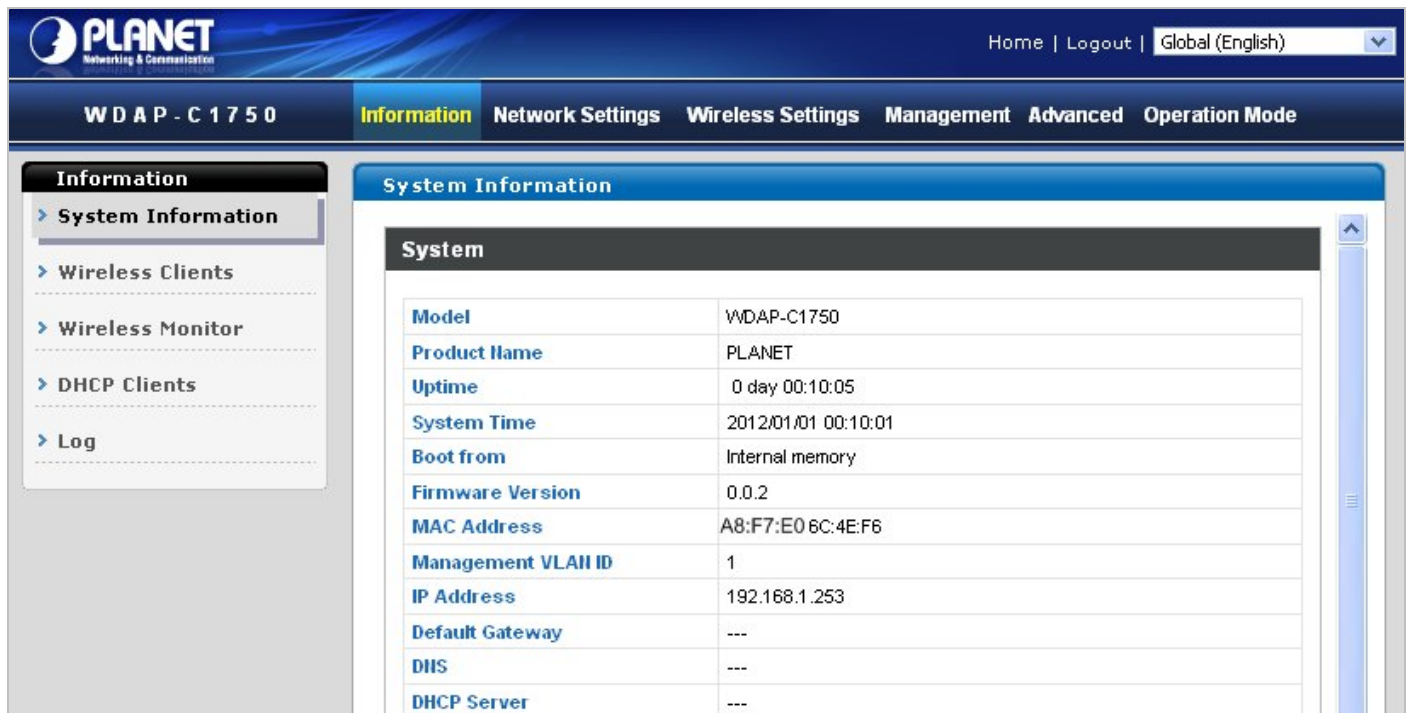


Figure 5-1 Information - Main Menu

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.
Firmware Version	Displays the firmware version.
MAC Address	Displays the access point’s MAC address.
Management VLAN ID	Displays the management VLAN ID.

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 the LAN port.
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.

Refresh Time

Auto Refresh Time	<input checked="" type="radio"/> 5 seconds <input type="radio"/> 1 second <input type="radio"/> Disable
Manual Refresh	<input type="button" value="Refresh"/>

2.4GHz WLAN Client Table

#	SSID	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time	Vendor
No wireless client								

5GHz WLAN Client Table

#	SSID	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time	Vendor
No wireless client								

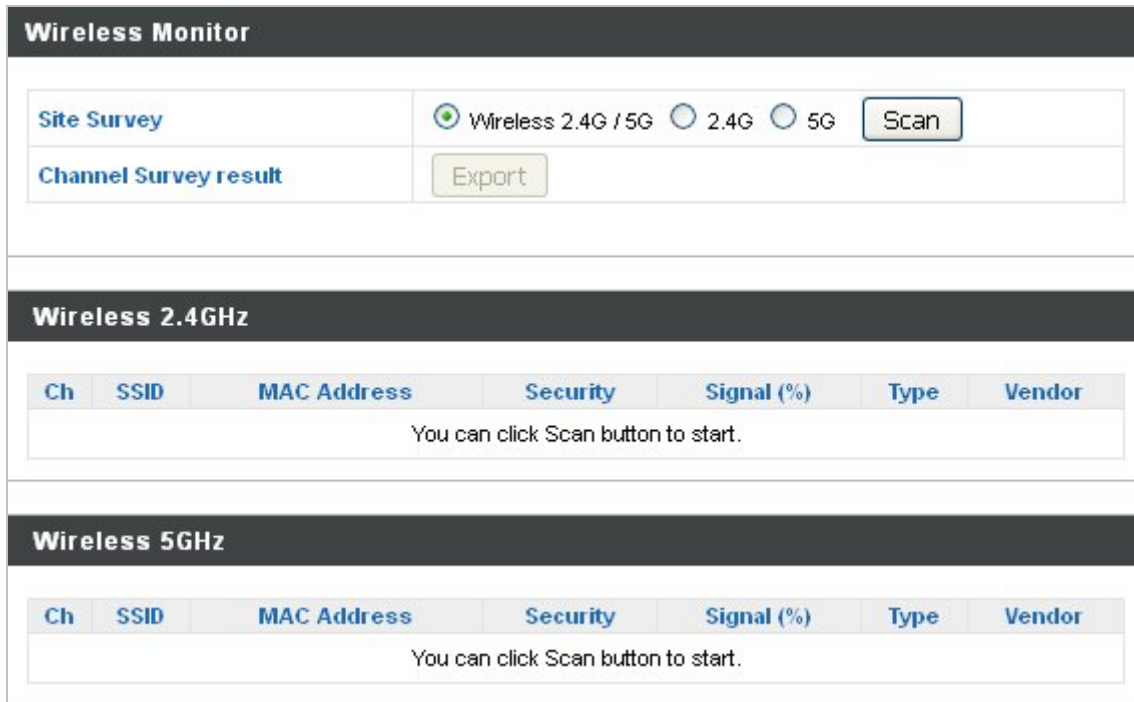
Figure 5-2 Information -- Wireless Clients

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.



The screenshot shows the 'Wireless Monitor' interface. At the top, there is a 'Site Survey' section with radio buttons for 'Wireless 2.4G / 5G' (selected), '2.4G', and '5G', and a 'Scan' button. Below it is a 'Channel Survey result' section with an 'Export' button. The interface is divided into two main sections: 'Wireless 2.4GHz' and 'Wireless 5GHz'. Each section contains a table with columns: Ch, SSID, MAC Address, Security, Signal (%), Type, and Vendor. Both tables currently display the text 'You can click Scan button to start.'

Figure 5-3 Information -- Wireless Monitor

The page includes the following fields:

Object	Description
Site 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 DHCP Clients

This table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.

DHCP Clients

This table shows the assigned IP address, MAC address and expiration time for each DHCP leased client.

DHCP Client Table		
IP Address	MAC Address	Expiration Time
No DHCP client		

Figure 5-4 Information – DHCP Clients

The page includes the following fields:

Object	Description
IP Address	Displays the IP Address of DHCP client.
MAC Address	Displays the MAC address of the DHCP client.
Expiration Time	The length of time for the IP address lease.

5.1.5 Log

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



Figure 5-5 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.

LAN-side IP Address	
IP Address Assignment	DHCP Client <input type="button" value="v"/>
IP Address	192.168.1.253
Subnet Mask	255.255.255.0
Default Gateway	From DHCP <input type="button" value="v"/> <input type="text"/>
Primary DNS Address	From DHCP <input type="button" value="v"/> 0.0.0.0
Secondary DNS Address	From DHCP <input type="button" value="v"/> 0.0.0.0

Figure 5-6 Network Settings -- LAN-side IP Address

The page includes the following fields:

Object	Description
IP Address Assignment	<ul style="list-style-type: none"> ■ Select “Static IP” to manually specify a static/fixed IP address for your access point (below). ■ Select “DHCP Client” for your access point to be assigned a dynamic IP address from your router’s DHCP server. ■ Select “DHCP Server” for your access point to assign a IP address for the clients.
IP Address	<p>Specify the IP address here.</p> <p>This IP address will be assigned to your access point and will replace the default IP address.</p>
Subnet Mask	<p>Specify a subnet mask.</p> <p>The default value is 255.255.255.0</p>
Default Gateway	<p>For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually.</p> <p>For static IP users, the default value is blank.</p>

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 DNS Address	DNS	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 DNS Address	DNS	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 5-7 Network Settings -- LAN Port

The page includes the following fields:

Object	Description
Wired LAN Port	Identifies 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 1 – 4095 are supported.

VLAN Interface		
Wired LAN Port	VLAN Mode	VLAN ID
LAN1	Untagged Port <input type="button" value="v"/>	1
Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [PLANET_2.4G_4ef6]	Untagged Port	1
Wireless 5GHz	VLAN Mode	VLAN ID
SSID [PLANET_5G_4ef7]	Untagged Port	1
Management VLAN		
VLAN ID	1	

Figure 5-8 Network Settings -- VLAN

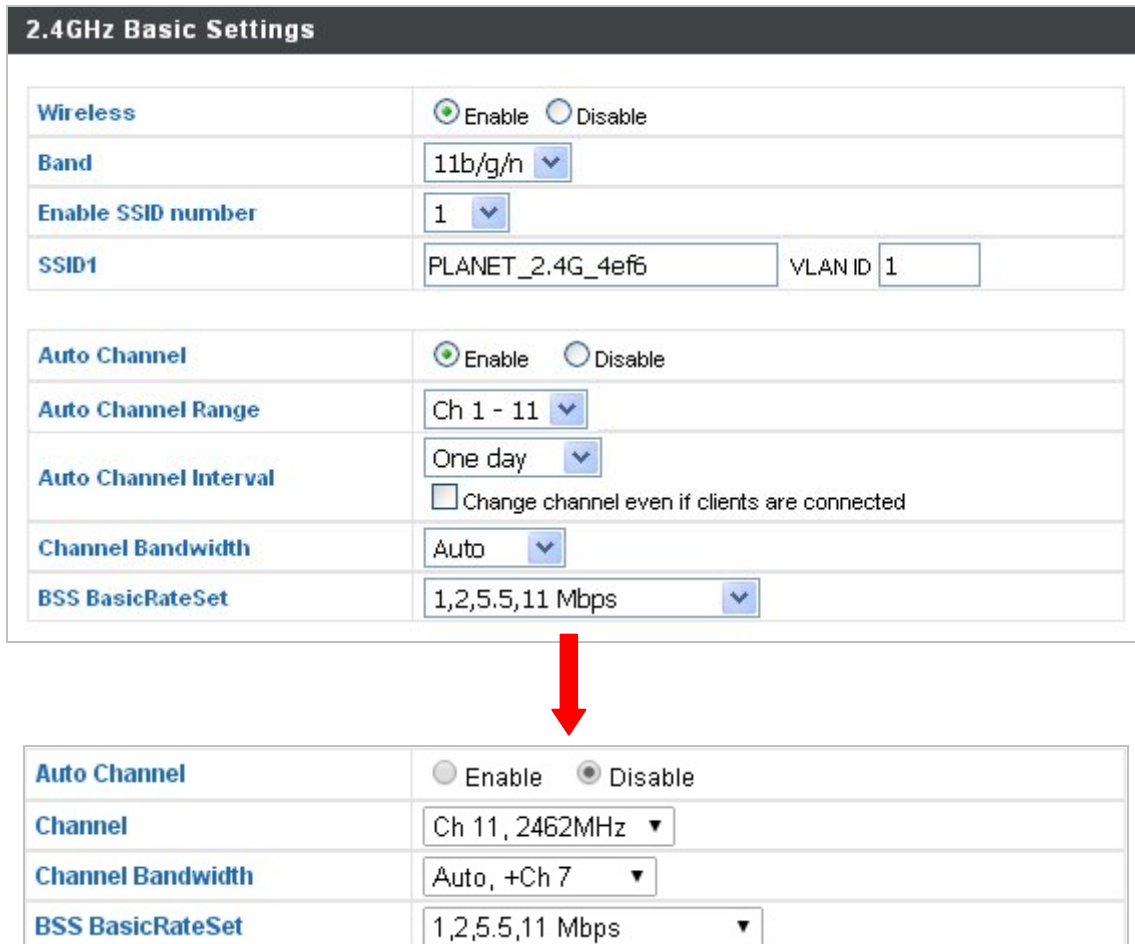
The page includes the following fields:

Object	Description
Wired LAN Port/Wireless	Identifies LAN port 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.



2.4GHz Basic Settings	
Wireless	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Band	11b/g/n
Enable SSID number	1
SSID1	PLANET_2.4G_4ef6 VLAN ID 1
Auto Channel	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Auto Channel Range	Ch 1 - 11
Auto Channel Interval	One day <input type="checkbox"/> Change channel even if clients are connected
Channel Bandwidth	Auto
BSS BasicRateSet	1,2,5.5,11 Mbps

Auto Channel	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Channel	Ch 11, 2462MHz
Channel Bandwidth	Auto, +Ch 7
BSS BasicRateSet	1,2,5.5,11 Mbps

Figure 5-9 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	<p>Enable/disable auto channel selection.</p> <p>Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz frequency based on availability and potential interference.</p> <p>When disabled, select a channel manually as shown in the next table.</p>
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	<p>Specify a frequency for how often the auto channel setting will check/reassign the wireless channel.</p> <p>Check/uncheck the "Change channel even if clients are connected" box according to your preference.</p>
Channel Bandwidth	<p>Set the channel bandwidth:</p> <ul style="list-style-type: none"> ■ 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	<p>Set the channel bandwidth:</p> <ul style="list-style-type: none"> ■ 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.

2.4GHz Advanced Settings	
Contention Slot	Short <input type="button" value="v"/>
Preamble Type	Short <input type="button" value="v"/>
Guard Interval	Short GI <input type="button" value="v"/>
802.11g Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
802.11n Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Period	<input type="text" value="1"/> (1-255)
RTS Threshold	<input type="text" value="2347"/> (1-2347)
Fragment Threshold	<input type="text" value="2346"/> (256-2346)
Multicast Rate	Auto <input type="button" value="v"/>
Tx Power	100% <input type="button" value="v"/>
Beacon Interval	<input type="text" value="100"/> (40-1000 ms)
Station Idle Timeout	<input type="text" value="60"/> (30-65535 seconds)

Figure 5-10 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



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.

2.4GHz Wireless Security Settings

SSID	PLANET_2.4G_4ef6 ▾
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
Load Balancing	50 / 50
Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

Figure 5-11 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. <ul style="list-style-type: none"> ■ When enabled, the SSID will be visible to clients as an available Wi-Fi network.

	<ul style="list-style-type: none"> 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. <p>A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.</p>
Wireless Client Isolation	<p>Enable or disable wireless client isolation.</p> <p>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.</p>
Load Balancing	<p>Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50 per radio).</p>
Authentication Method	<p>Select an authentication method from the drop down menu and refer to the information below appropriate for your method.</p>
Additional Authentication	<p>Select an additional authentication method from the drop down menu.</p>

■ **No Authentication**

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



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.

Authentication Method	WEP ▼
Key Length	64-bit ▼
Key Type	ASCII (5Characters) ▼
Default Key	Key 1 ▼
Encryption Key 1	<input type="text"/>
Encryption Key 2	<input type="text"/>
Encryption Key 3	<input type="text"/>
Encryption Key 4	<input type="text"/>
Additional Authentication	No additional authentication ▼

Figure 5-12 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 alphanumeric 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

Authentication Method	IEEE802.1x/EAP ▼
Key Length	64-bit ▼
Additional Authentication	No additional authentication ▼

Figure 5-13 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

Authentication Method	WPA-PSK ▼
WPA Type	WPA/WPA2 Mixed Mode-PSK ▼
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase ▼
Pre-shared Key	<input type="text"/>
Additional Authentication	No additional authentication ▼

Figure 5-14 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**

Authentication Method	WPA-EAP ▼
WPA Type	WPA/WPA2 mixed mode-EAP ▼
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)
Additional Authentication	No additional authentication ▼

Figure 5-15 2.4GHz Wireless Settings -- WPA-EAP

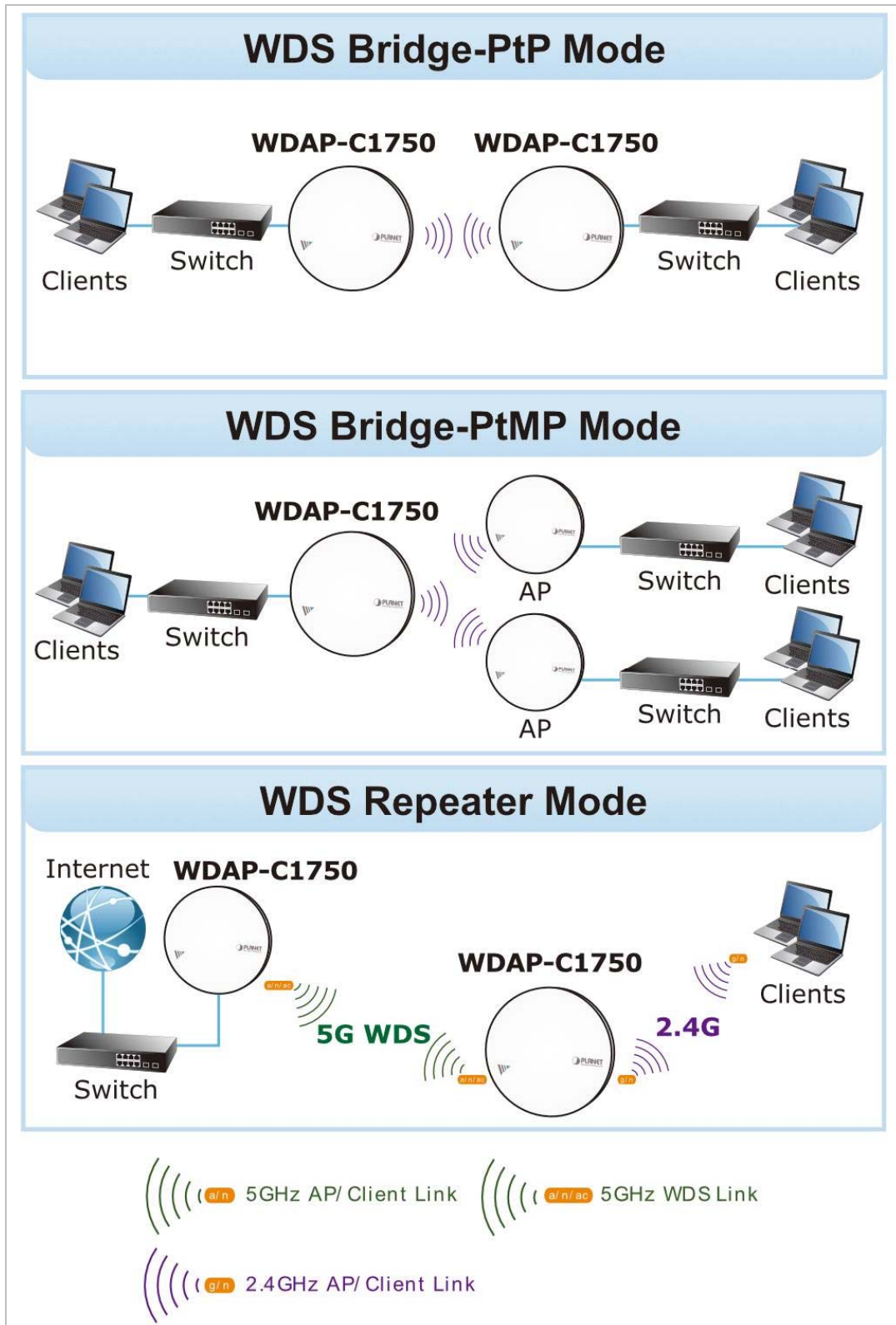
■ **Additional Authentication**

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 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.

2.4GHz	
WDS Functionality	Disabled <input type="button" value="v"/>
Local MAC Address	A8:F7:E0:06:07:46
WDS Peer Settings	
WDS #1	MAC Address <input type="text"/>
WDS #2	MAC Address <input type="text"/>
WDS #3	MAC Address <input type="text"/>
WDS #4	MAC Address <input type="text"/>
WDS VLAN	
VLAN Mode	Untagged Port <input type="button" value="v"/> (Enter at least one MAC address.)
VLAN ID	1 <input type="text"/>
WDS Encryption method	
Encryption	None <input type="button" value="v"/> (Enter at least one MAC address.)

Figure 5-16 2.4GHz Wireless Settings -- WDS

The page includes the following fields:

Object	Description
WDS Functionality	Select “ WDS with AP ” to use WDS or “ Dedicated WDS ” 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 WDS 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.



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 11n Basic Settings

The “5GHz 11ac 11n” 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).

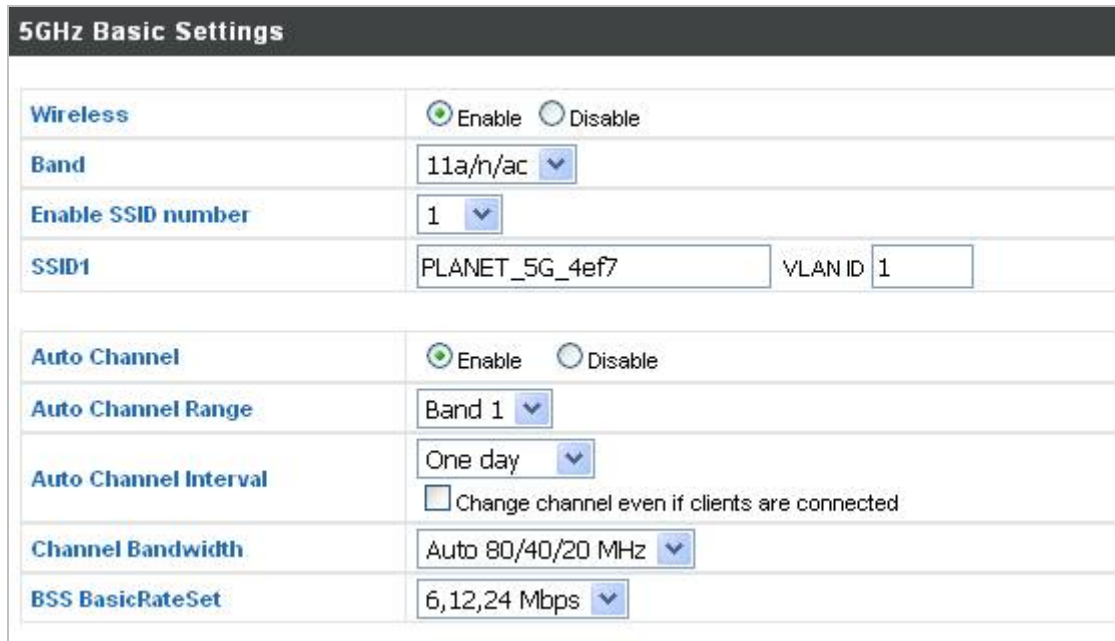


Figure 5-17 5GHz Wireless Settings

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: <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ■ 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.

5GHz Advanced Settings	
Guard Interval	Short GI <input type="button" value="v"/>
802.11n Protection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256-2346)
Multicast Rate	Auto <input type="button" value="v"/>
Tx Power	100% <input type="button" value="v"/>
Beacon Interval	100 (40-1000 ms)
Station Idle Timeout	60 (30-65535 seconds)

Figure 5-18 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.

5GHz Wireless Security Settings	
SSID	PLANET_5G_4ef7 <input type="button" value="v"/>
Broadcast SSID	Enable <input type="button" value="v"/>
Wireless Client Isolation	Disable <input type="button" value="v"/>
Load Balancing	50 /50
Authentication Method	No Authentication <input type="button" value="v"/>
Additional Authentication	No additional authentication <input type="button" value="v"/>

Figure 5-19 5GHz Wireless Settings -- Security

The page includes the following fields:

Object	Description
SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	<p>Enable or disable SSID broadcast.</p> <ul style="list-style-type: none"> ■ 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. <p>A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.</p>
Wireless Client Isolation	<p>Enable or disable wireless client isolation.</p> <p>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.</p>
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50 per radio).
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.



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.

Authentication Method	WEP ▼
Key Length	64-bit ▼
Key Type	ASCII (5Characters) ▼
Default Key	Key 1 ▼
Encryption Key 1	<input type="text"/>
Encryption Key 2	<input type="text"/>
Encryption Key 3	<input type="text"/>
Encryption Key 4	<input type="text"/>
Additional Authentication	No additional authentication ▼

Figure 5-20 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

Authentication Method	IEEE802.1x/EAP ▼
Key Length	64-bit ▼
Additional Authentication	No additional authentication ▼

Figure 5-21 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

Authentication Method	WPA-PSK ▼
WPA Type	WPA/WPA2 Mixed Mode-PSK ▼
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase ▼
Pre-shared Key	<input type="text"/>
Additional Authentication	No additional authentication ▼

Figure 5-22 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

Authentication Method	WPA-EAP ▼
WPA Type	WPA/WPA2 mixed mode-EAP ▼
Encryption Type	TKIP/AES Mixed Mode ▼
Key Renewal Interval	60 minute(s)
Additional Authentication	No additional authentication ▼

Figure 5-23 5GHz Wireless Settings -- WPA-EAP

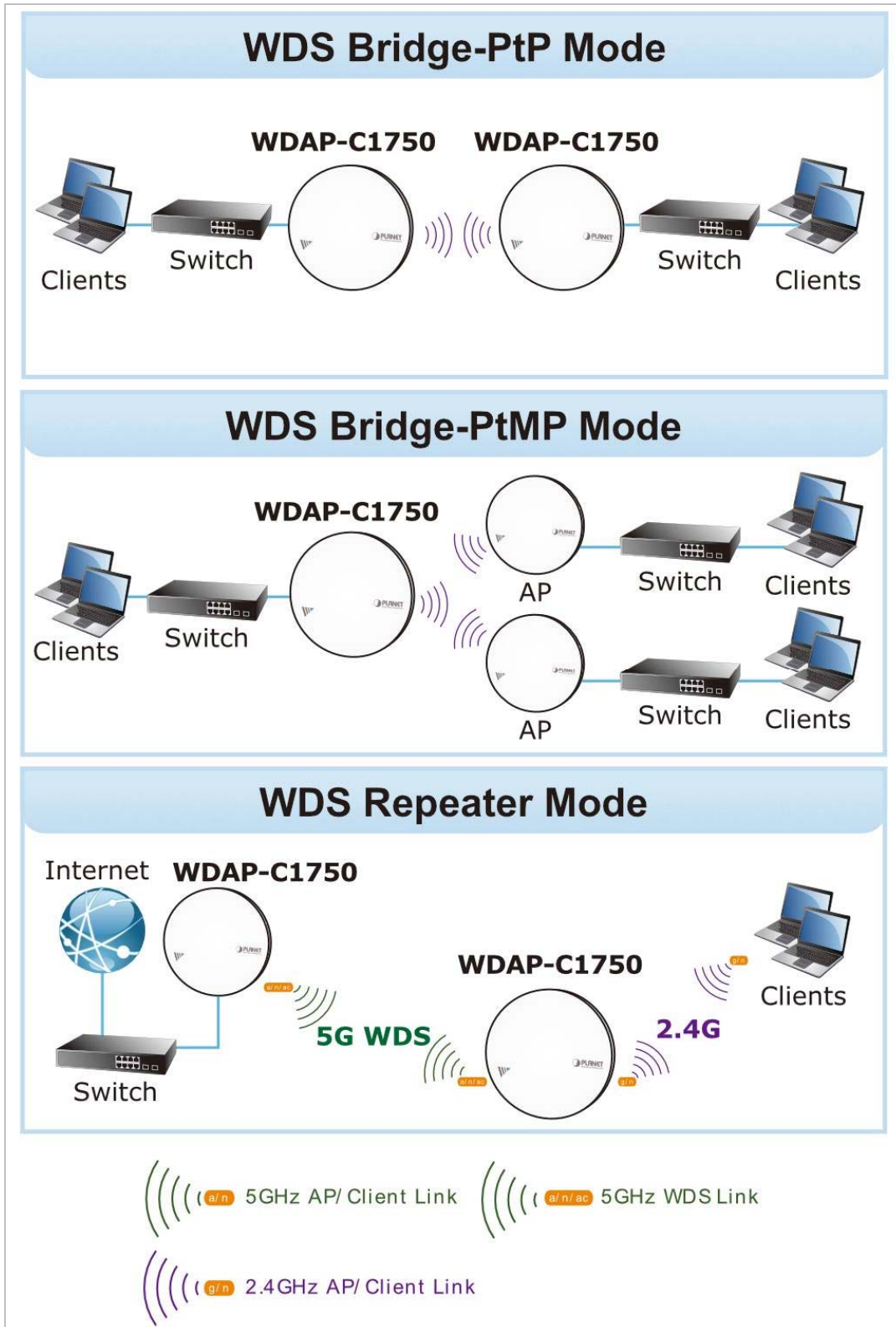
■ Additional Authentication

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 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.

5GHz WDS Mode	
WDS Functionality	Disabled <input type="button" value="v"/>
Local MAC Address	A8:F7:E0:06:07:46
WDS Peer Settings	
WDS #1	MAC Address <input type="text"/>
WDS #2	MAC Address <input type="text"/>
WDS #3	MAC Address <input type="text"/>
WDS #4	MAC Address <input type="text"/>
WDS VLAN	
VLAN Mode	Untagged Port <input type="button" value="v"/> (Enter at least one MAC address.)
VLAN ID	1 <input type="text"/>
Encryption method	
Encryption	None <input type="button" value="v"/> (Enter at least one MAC address.)

Figure 5-24 5GHz Wireless Settings -- WDS

The page includes the following fields:

Object	Description
WDS Functionality	Select “WDS with AP” to use WDS or “Dedicated WDS” 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.



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.

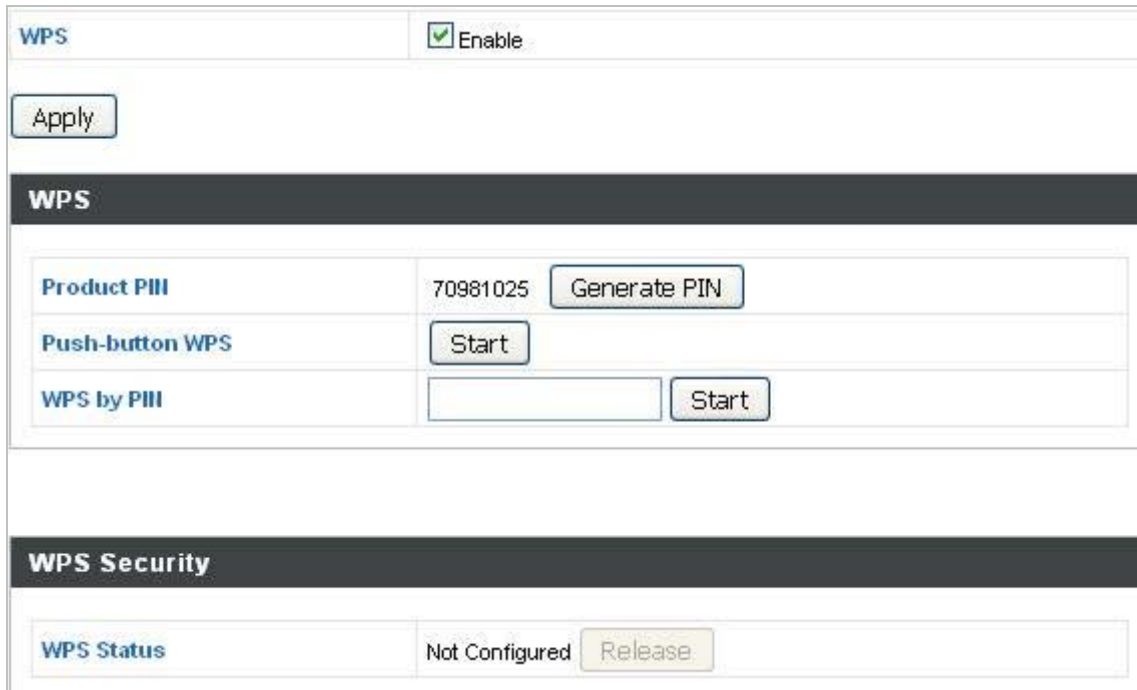


Figure 5-25 WPS

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.

RADIUS Server (2.4GHz)

Primary RADIUS Server

RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input style="width: 90%;" type="text"/>
Authentication Port	<input style="width: 50%;" type="text" value="1812"/>
Shared Secret	<input style="width: 80%;" type="text"/>
Session Timeout	<input style="width: 50%;" type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input style="width: 50%;" type="text" value="1813"/>

Secondary RADIUS Server

RADIUS Type	<input type="radio"/> Internal <input checked="" type="radio"/> External
RADIUS Server	<input style="width: 90%;" type="text"/>
Authentication Port	<input style="width: 50%;" type="text" value="1812"/>
Shared Secret	<input style="width: 80%;" type="text"/>
Session Timeout	<input style="width: 50%;" type="text" value="3600"/> second(s)
Accounting	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Accounting Port	<input style="width: 50%;" type="text" value="1813"/>

Figure 5-26 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 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.

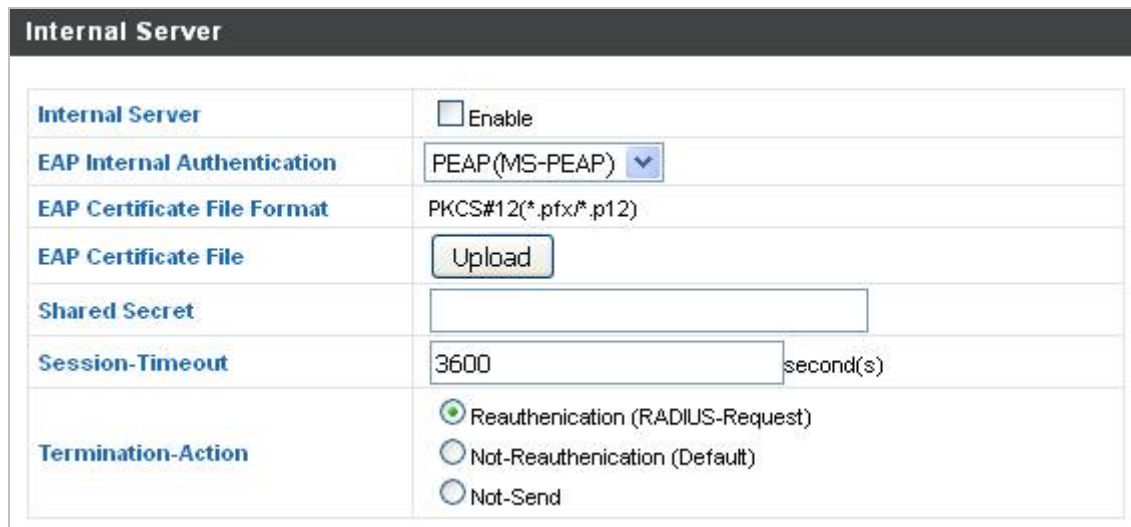


Figure 5-27 Internal Server

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.

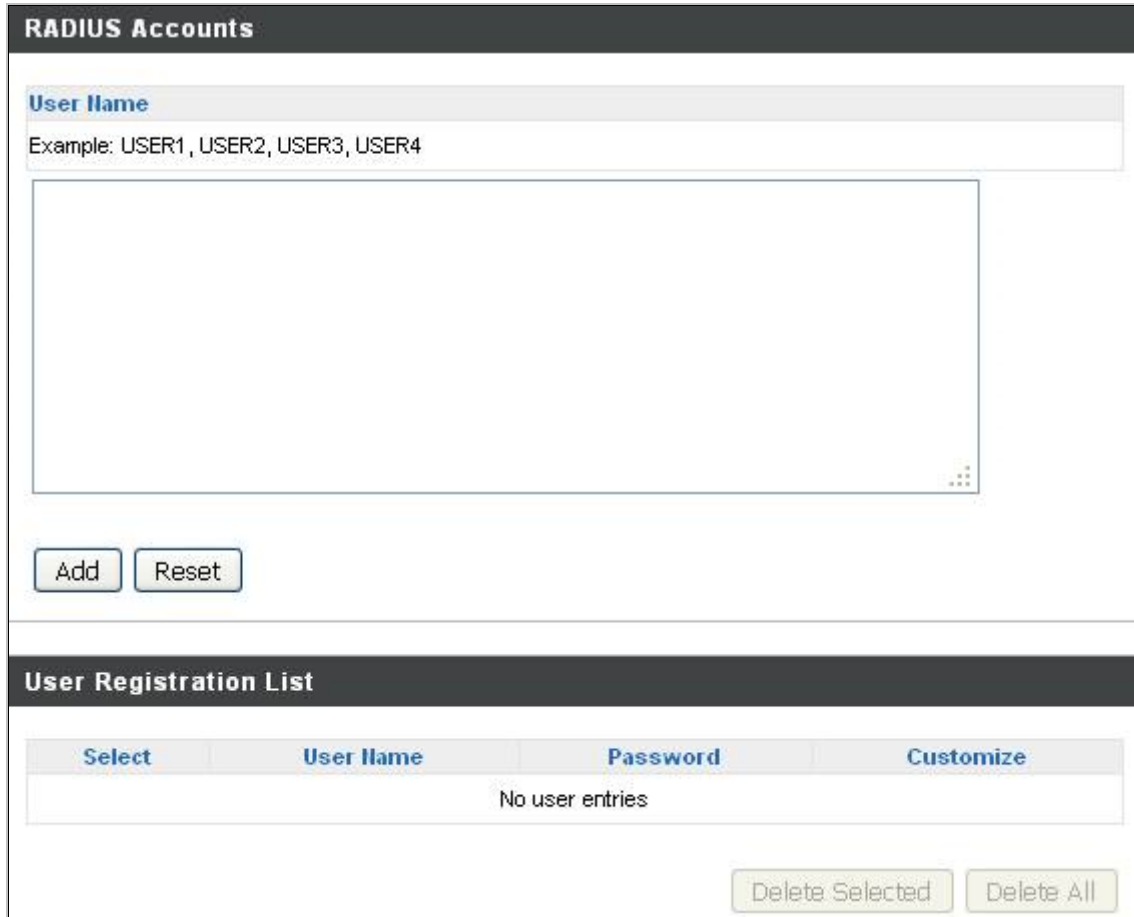


Figure 5-28 RADIUS Accounts

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. Up to 256 entries can be added to the list.

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.

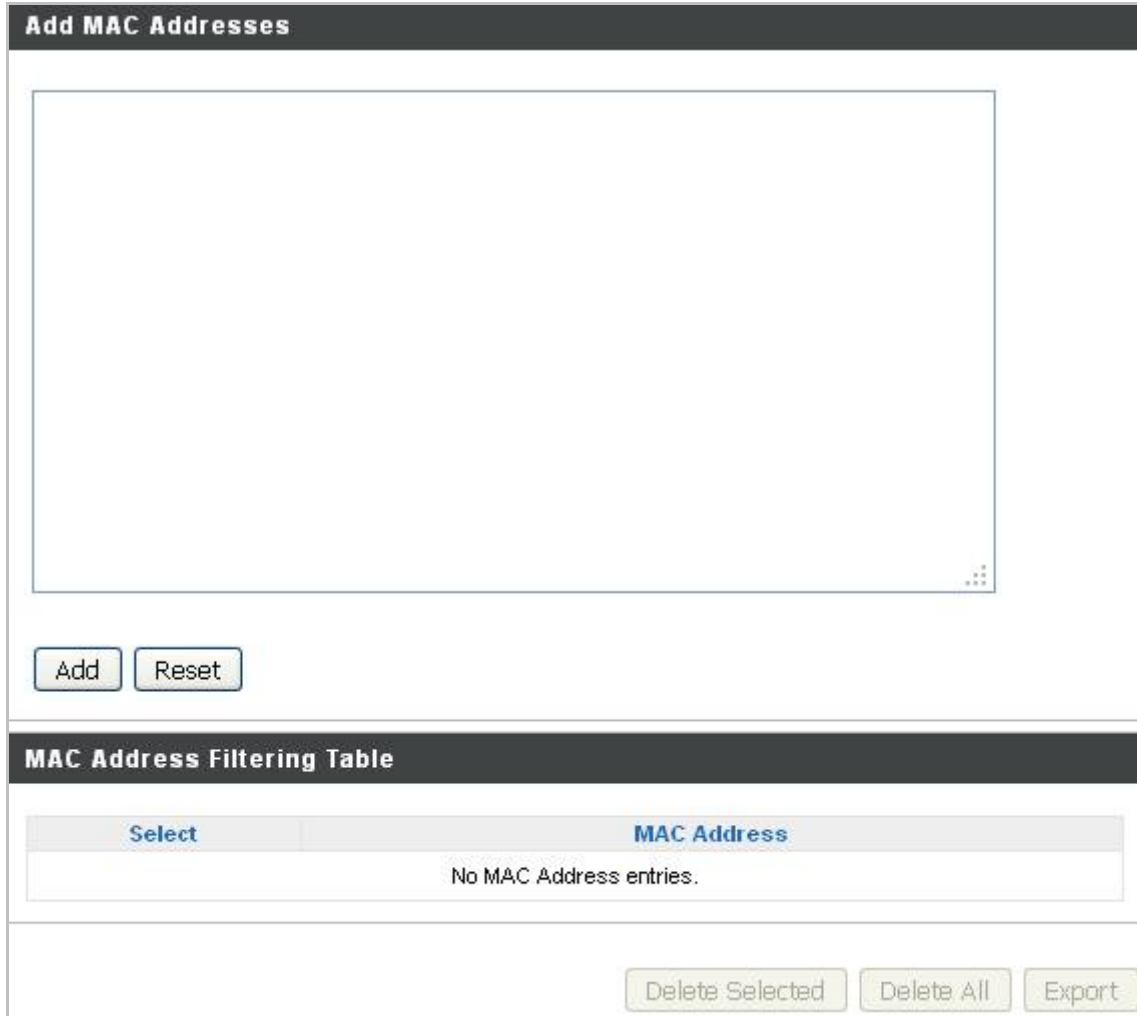


Figure 5-29 MAC Filter

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 IEEE 802.11 networks. WMM prioritizes traffic according to four categories: **background**, **best effort**, **video** and **voice**.

WMM-EDCA Settings

WMM Parameters of Access Point				
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	6	3	0
Video	3	4	1	94
Voice	2	3	1	47

WMM Parameters of Station				
	CWMin	CWMax	AIFSN	TxOP
Back Ground	4	10	7	0
Best Effort	4	10	3	0
Video	3	4	2	94
Voice	2	3	2	47

Figure 5-30 WMM

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

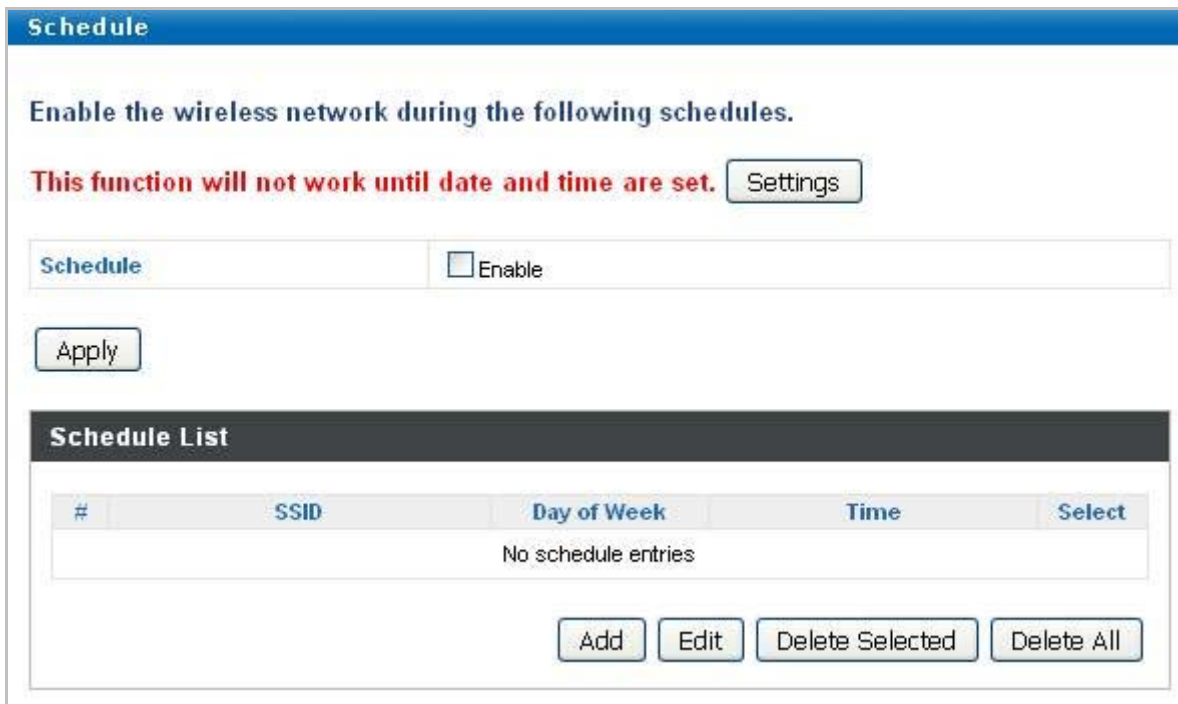
Object	Description	
Background	Low Priority	High throughput, non time sensitive bulk data e.g. FTP
Best Effort	Medium Priority	Traditional IP data, medium throughput and delay.
Video	High Priority	Time sensitive video data with minimum time delay.
Voice	High Priority	Time sensitive data such as VoIP 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	<p>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).</p> <p>Valid values are 1,3,7,15,31,63,127,255,511 or 1024.</p> <p>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.</p>
CWMax	<p>Maximum Contention Window (milliseconds): This value is the upper limit to random backoff value doubling (see above).</p> <p>Valid values are 1,3,7,15,31,63,127,255,511 or 1024.</p>
AIFSN	<p>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.</p>
TxOP	<p>Transmission Opportunity (milliseconds): The maximum interval of time an AP/client can transmit. This makes channel access more efficiently prioritized.</p> <p>A value of 0 means only one frame per transmission.</p> <p>A greater value effects higher priority.</p>

5.3.15 Schedule

The schedule feature allows you to automate the wireless network for specified times. Check/uncheck the box “Enable Wireless Schedule” to enable/disable the wireless scheduling function.



Schedule

Enable the wireless network during the following schedules.

This function will not work until date and time are set. [Settings](#)

Schedule Enable

[Apply](#)

Schedule List

#	SSID	Day of Week	Time	Select
No schedule entries				

[Add](#) [Edit](#) [Delete Selected](#) [Delete All](#)

Figure 5-31 Schedule



The **Date and Time** must be set before enable this function. And reload your WiFi adapter to get the SSID successfully.

5.3.16 Traffic Shaping

The traffic shaping function allows you to regulate network data transfer to ensure or prioritize performance by limiting uplink and downlink speeds according to SSID.

Traffic Shaping for ssid(2.4GHz)

Enable

Unlimited : 0 Mbps

Down Link/Up Link Maximum : 1024 Mbps

SSID	Down Link	Up Link
PLANET_2.4G_4ef6	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_2	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_3	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_4	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_5	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_6	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_7	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_8	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_9	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_10	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_11	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_12	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_13	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_14	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_15	0 Mbps	0 Mbps
PLANET_2.4G_4ef6_16	0 Mbps	0 Mbps

Figure 5-32 Traffic Shaping

Object	Description
Enable	Check/uncheck to enable or disable unlimited transfer speed.
Downlink/Uplink Maximum	Specify the maximum down/uplink capacity in Mbps.
Downlink	Enter a downlink limit in MB for the listed SSID.
Uplink	Enter an uplink limit in MB for the listed SSID.

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.

Account to Manage This Device	
Administrator Name	<input type="text" value="admin"/>
Administrator Password	<input type="password" value="•••••"/> (4-32Characters)
	<input type="password" value="•••••"/> (Confirm)
<input type="button" value="Apply"/>	
Advanced Settings	
Product Name	<input type="text" value="PLANET"/>
Management Protocol	<input checked="" type="checkbox"/> HTTP <input checked="" type="checkbox"/> HTTPS <input type="checkbox"/> TELNET <input type="checkbox"/> SSH <input type="checkbox"/> SNMP
SIIMP Version	<input type="text" value="v1/v2c"/>
SIIMP Get Community	<input type="text" value="public"/>
SIIMP Set Community	<input type="text" value="private"/>
SIIMP V3 Name	<input type="text" value="admin"/>
SIIMP V3 Password	<input type="password" value="••••••••"/>
SIIMP Trap	<input type="text" value="Disabled"/>
SIIMP Trap Community	<input type="text" value="public"/>
SIIMP Trap Manager	<input type="text"/>
<input type="button" value="Apply"/>	

Figure 5-33 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.

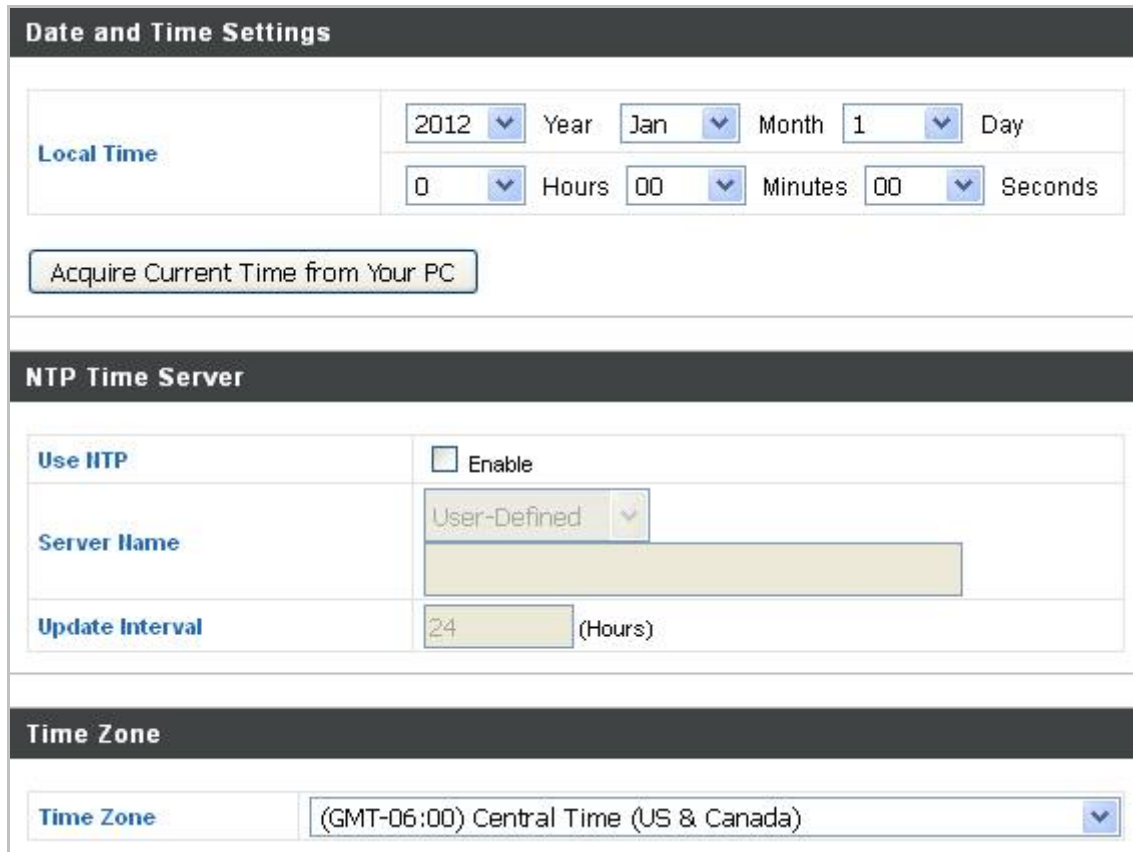


Figure 5-34 Time and Date

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.

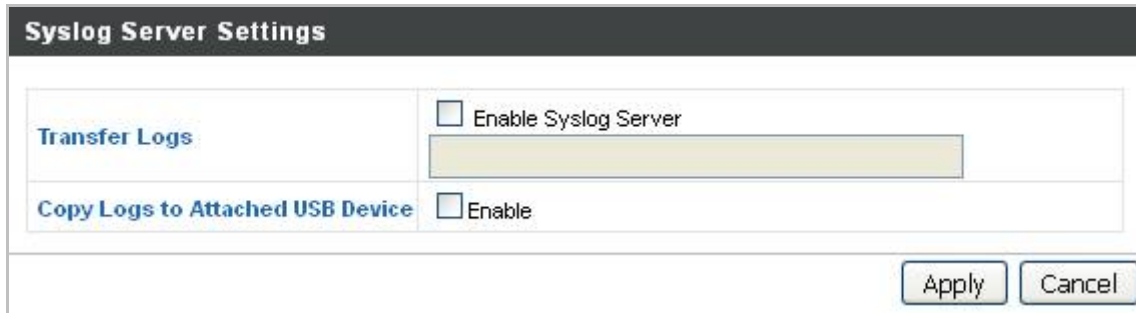


Figure 5-35 Syslog Server

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.

5.4.4 Ping Test

The access point includes a built-in ping test function. Ping is a computer network administration utility used to test whether a particular host is reachable across an IP network and to measure the round-trip time for sent messages.



Figure 5-36 Ping Test

The page includes the following fields:

Object	Description
Destination Address	Enter the address of the host.
Execute	Click “Execute” to ping the host.

5.4.5 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 5-37 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 Reboot Schedule

This function allows you to enable and configure system reboot schedule. The device can regularly reboot according to the reserved time when connecting to the Internet.

Figure 5-38 Reboot Schedule



The **Date and Time** must be set before enable this function.

5.5.2 LED Settings

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

LED Settings	
Power LED	<input checked="" type="radio"/> On <input type="radio"/> Off
Diag LED	<input checked="" type="radio"/> On <input type="radio"/> Off
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 5-39 LED Settings

The page includes the following fields:

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

5.5.3 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.

Firmware Location	
Update firmware from	<input checked="" type="radio"/> a file on your PC <input type="radio"/> a file on an attached USB device (No USB device connected.)
Update Firmware from PC	
Firmware Update File	<input type="button" value="Browse..."/> No file selected.
<input type="button" value="Update"/>	

Figure 5-40 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.

5.5.4 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.

Save/Restore Method

Using Device

Using your PC
 Using your USB device (No USB device connected.)

Save Settings to PC

Save Settings

Encrypt the configuration file with a password.

Restore Settings from PC

Restore Settings

No file selected.
 Open file with password.

Figure 5-41 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.

5.5.5 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 5-42 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.



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

5.5.6 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.



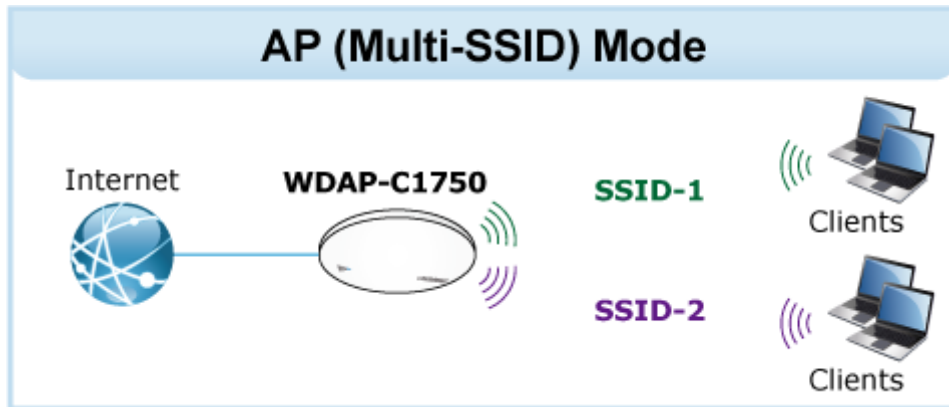
Figure 5-43 Reboot

The page includes the following fields:

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

5.6 Operation Mode

5.6.1 AP Mode

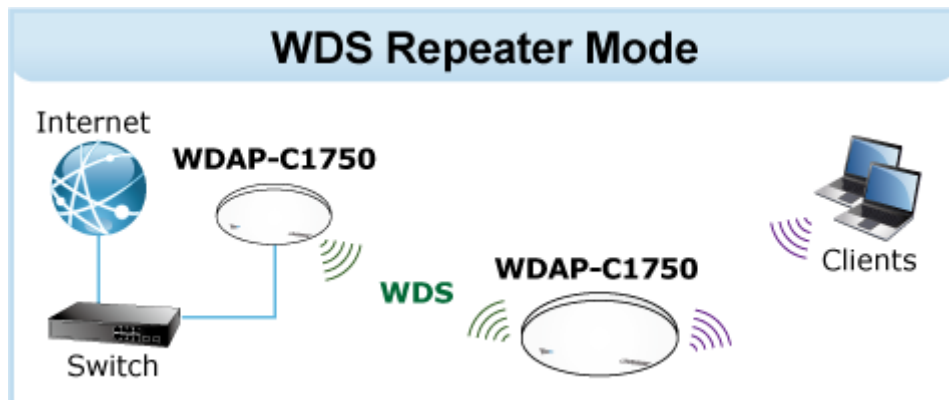


The default setting is AP mode.

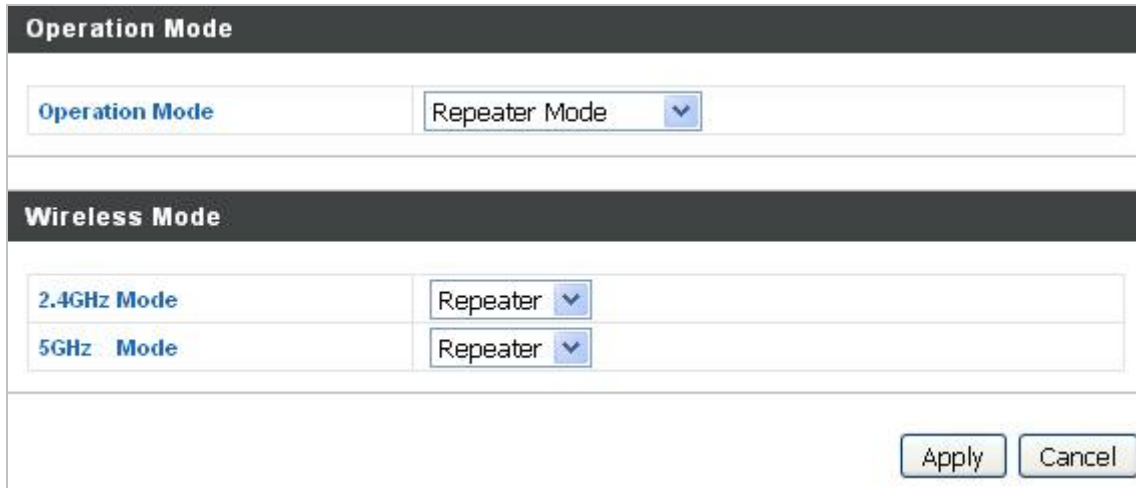
Operation Mode	
Operation Mode	AP Mode <input type="button" value="v"/>
Wireless Mode	
2.4GHz Mode	Access Point <input type="button" value="v"/>
5GHz Mode	Access Point <input type="button" value="v"/>
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 5-44 AP Mode

5.6.2 Repeater Mode



Select "Repeater mode" and the WDAP-C1750 will be configured as a repeater to extend the wireless signal.



Operation Mode

Operation Mode: Repeater Mode

Wireless Mode

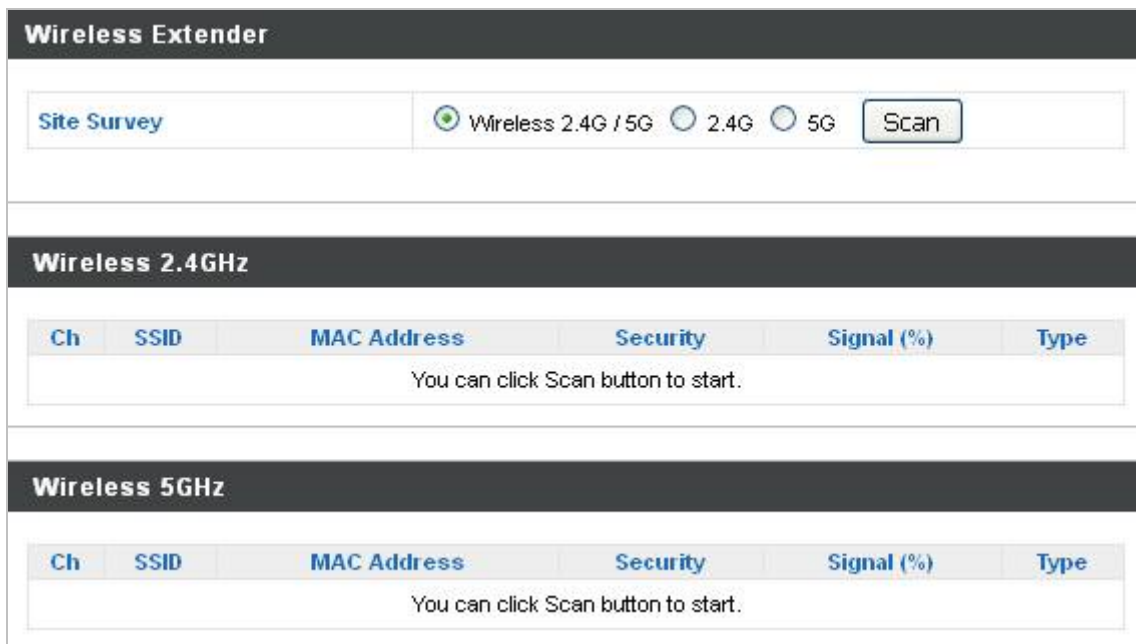
2.4GHz Mode: Repeater

5GHz Mode: Repeater

Apply Cancel

Figure 5-45 Repeater Mode

After configured as Repeater mode, please choose **Wireless Settings** to site survey the root AP. And select the one you want to connect then enter the authentication.



Wireless Extender

Site Survey: Wireless 2.4G / 5G 2.4G 5G Scan

Wireless 2.4GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type
You can click Scan button to start.					

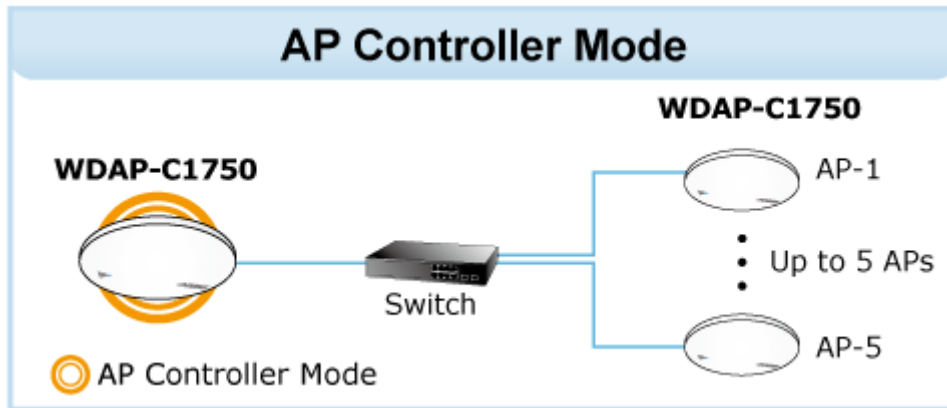
Wireless 5GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type
You can click Scan button to start.					

Figure 5-46 Repeater Mode -- Site Survey

5.6.3 AP Controller Mode

This mode is enabled under the NMS (Network Management System) structure. Please refer to Chapter 6 for further information and detail configuration.



Select "AP Controller Mode" to configure WDAP-C1750 as an AP controller.

Operation Mode	
Operation Mode	AP Controller Mode ▼
Wireless Mode	
2.4GHz Mode	Access Point ▼
5GHz Mode	Access Point ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

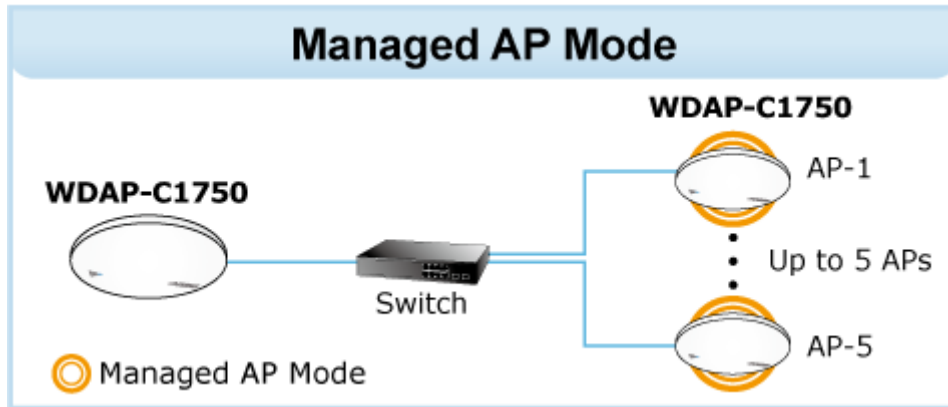
Figure 5-47 AP Controller Mode



When the "AP Controller Mode" is enabled, the wireless will be disabled automatically to reduce its CPU loading, once you have finished configuring all managed APs, you can manually enable its wireless or configured it back to "Access Point" mode.

5.6.4 Managed AP Mode

This mode is enabled under the NMS (Network Management System) structure. Please refer to Chapter 6 for further information and detail configuration.



Select "**Managed AP Mode**" to configure WDAP-C1750 as a managed AP.

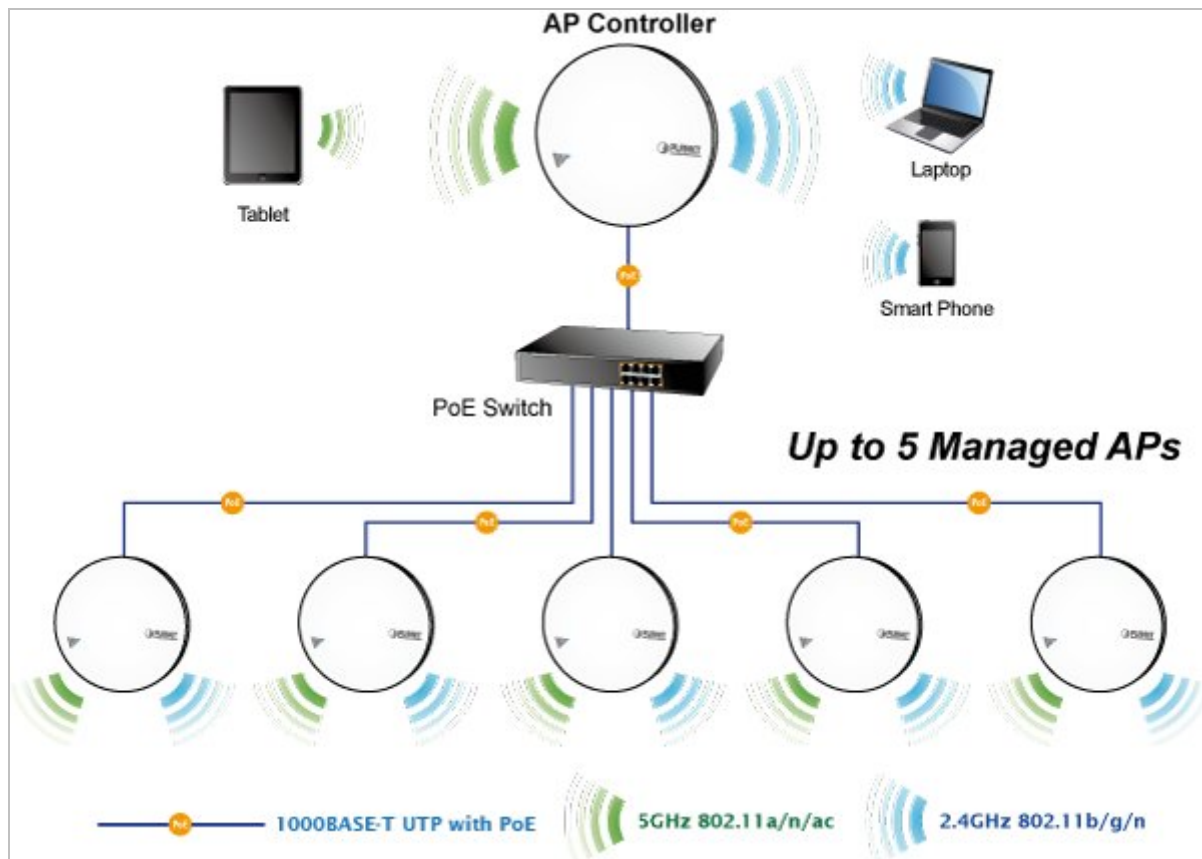
Operation Mode	
Operation Mode	Managed AP mode ▼
Wireless Mode	
2.4GHz Mode	Access Point ▼
5GHz Mode	Access Point ▼
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

Figure 5-48 Managed AP Mode

Chapter 6.NMS

The Network Management System (NMS) supports the central management of a group of access points, otherwise known as an AP Array. NMS can be installed on one access point and support up to 5 access points with no additional wireless controller required, reducing costs and facilitating efficient remote AP management.

Access points can be deployed and configured according to requirements, creating a powerful network architecture which can be easily managed and expanded in the future, with an easy to use interface and a full range of functionality – ideal for small and mid-sized office environments. A secure WLAN can be deployed and administered from a single point, minimizing cost and complexity.

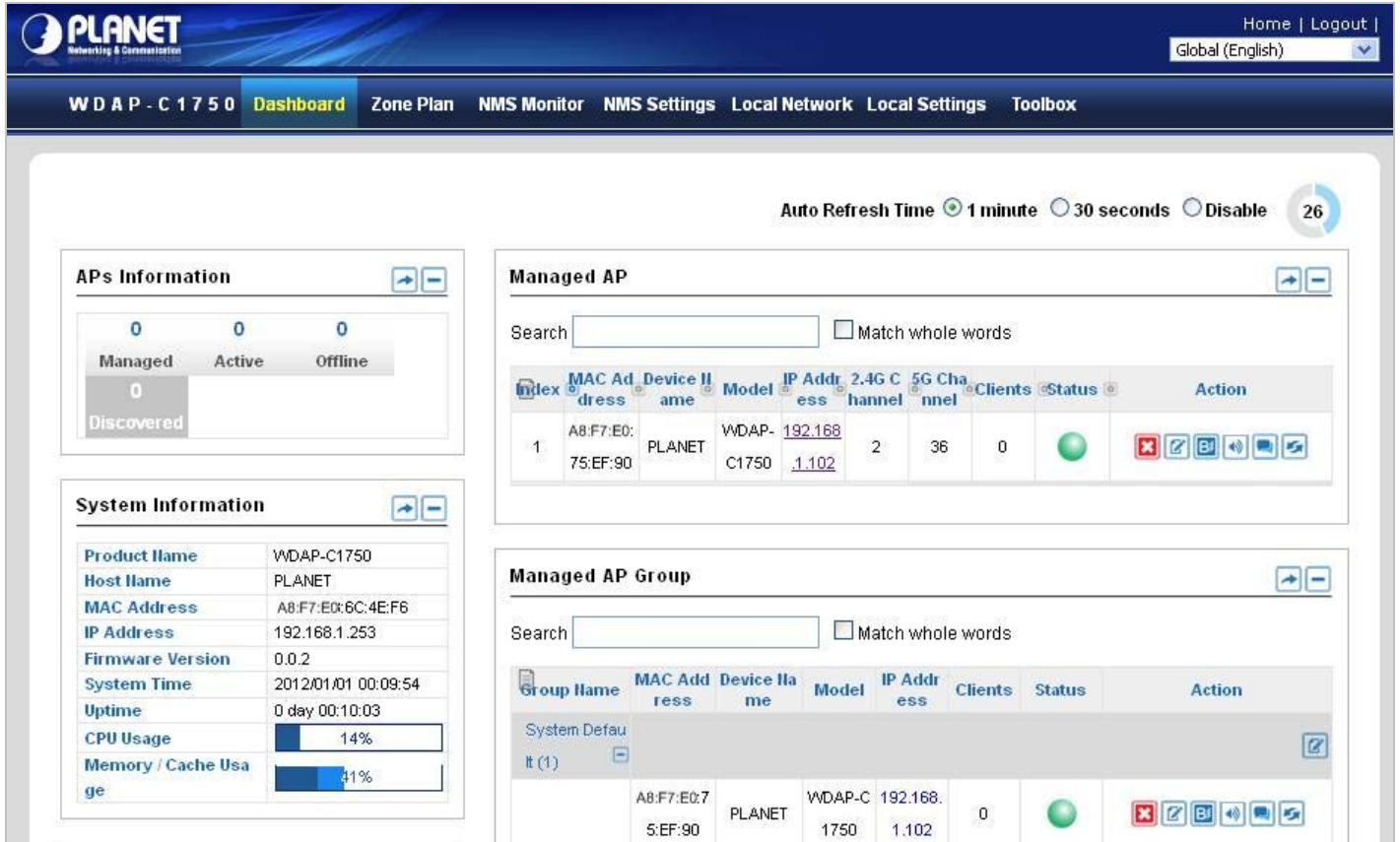


Go to “**Operation Mode**” and select “**AP Controller Mode**” from the drop down menu. And click **Apply** to save the setting. You will see at the NMS Dashboard after reboots. If you want to configure your WDAP-C1750 as **Managed AP Mode**, go to “**Operation Mode**” and select “**Managed AP Mode**” from the drop down menu. And click **Apply** to save the setting.

One AP (access point) is designated as the AP Controller (master) and other connected APs are automatically designated as Managed APs (slaves). Using PLANET NMS you can monitor, configure and manage all Managed APs (up to 5) from the single AP Controller.

6.1 Dashboard

The **Dashboard** panel displays an overview of your network and key system information, with quick links to access configuration options for **Managed AP** and **Managed AP Group**. Each panel can be refreshed, collapsed or moved according to your preference.



The dashboard interface includes a top navigation bar with the following menu items: **W D A P - C 1 7 5 0**, **Dashboard**, **Zone Plan**, **NMS Monitor**, **NMS Settings**, **Local Network**, **Local Settings**, and **Toolbox**. The top right corner features **Home | Logout |** and a language dropdown set to **Global (English)**.

At the top right of the dashboard area, there is an **Auto Refresh Time** control with options for **1 minute** (selected), **30 seconds**, and **Disable**, along with a refresh icon and the number **26**.

The dashboard is divided into four main sections:

- APs Information:** Shows counts for **Managed** (0), **Active** (0), and **Offline** (0) APs. A **Discovered** count of 0 is also shown.
- System Information:** A table of system details:

Product Name	WDAP-C1750
Host Name	PLANET
MAC Address	A8:F7:E0:6C:4E:F6
IP Address	192.168.1.253
Firmware Version	0.0.2
System Time	2012/01/01 00:09:54
Uptime	0 day 00:10:03
CPU Usage	14%
Memory / Cache Usage	41%
- Managed AP:** A search bar with a **Match whole words** checkbox. Below is a table of managed APs:

Index	MAC Address	Device Name	Model	IP Address	2.4G Channel	5G Channel	Clients	Status	Action
1	A8:F7:E0:75:EF:90	PLANET	WDAP-C1750	192.168.1.102	2	36	0	●	[Icons]
- Managed AP Group:** A search bar with a **Match whole words** checkbox. Below is a table of managed AP groups:

Group Name	MAC Address	Device Name	Model	IP Address	Clients	Status	Action
System Default (1)	A8:F7:E0:75:EF:90	PLANET	WDAP-C1750	192.168.1.102	0	●	[Icons]

Figure 6-1 Dashboard

6.2 Zone Plan

Zone Plan displays a customizable live map of Managed APs for a visual representation of your network coverage. Each AP icon can be moved around the map, and a background image can be uploaded for user-defined location profiles using **NMS Settings** → **Zone Edit**. Options can be configured using the menu on the right side and signal strength is displayed for each AP.

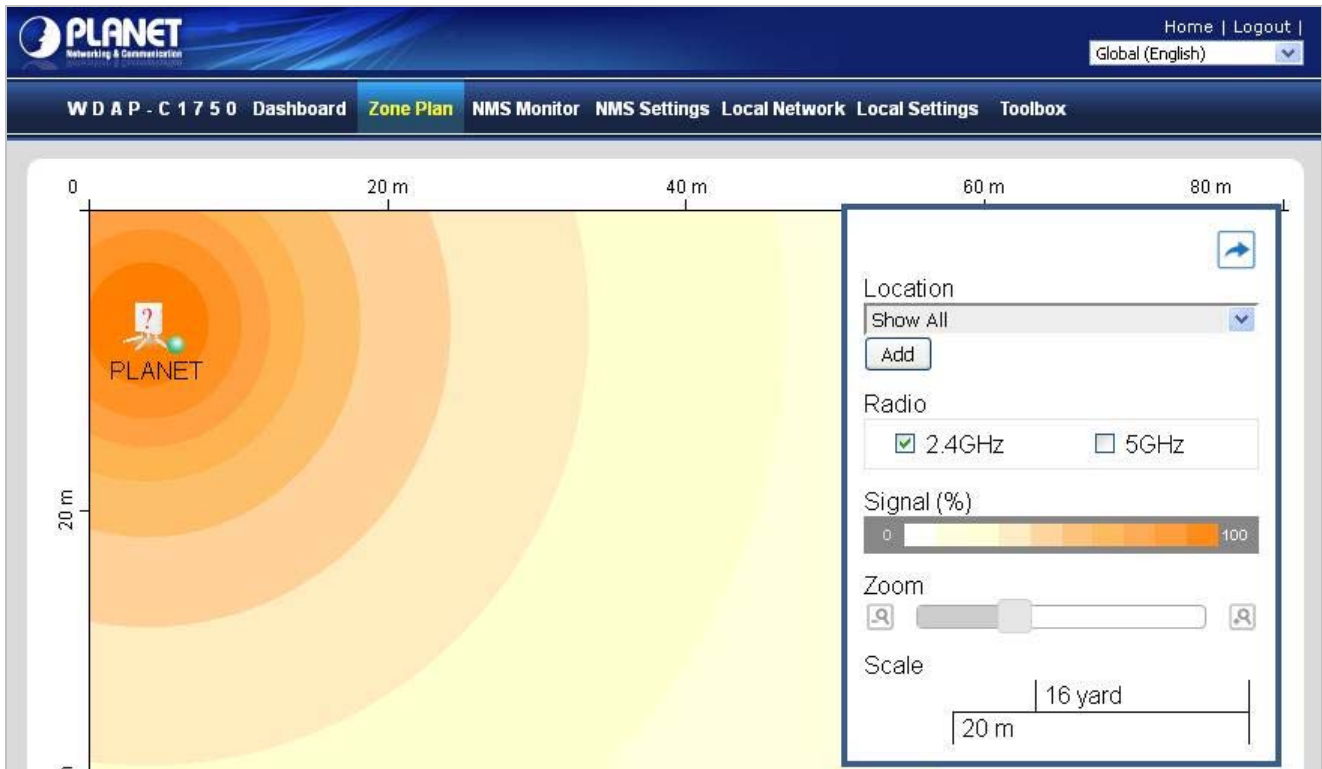


Figure 6-2 Zone Plan

6.3 NMS Monitor

The **NMS Monitor** panel provides more detailed monitoring information about the AP Array than found on the Dashboard, grouped according to categories in the menu down the left side.

6.3.1 Managed AP

Displays information about each Managed AP in the local network: Index (reference number), MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each access point, and Status (connected, connecting or disconnected).









Figure 6-3 NMS Monitor—Managed AP

The search function can be used to locate a specific Managed AP. Type in the search box and the list will update.

Search Match whole words

Icon Status

Icon	Color	STATUS	Definition
	Grey	Disconnected	Managed AP is disconnected. Please check the network connection and ensure the Managed AP is in the same IP subnet as the AP Controller.
	Red	Authentication Failed Or Incompatible NMS Version	System security must be the same for all access points in the AP array. Please check security settings Access points must use the same version of NMS: the managed AP will not be able to make configurations. Please use the AP Controller's firmware upgrade function.
	Orange	Configuring or Upgrading	Please wait while the Managed AP makes configurations or while the firmware is upgrading.
	Yellow	Connecting	Please wait while Managed AP is connecting.
	Green	Connected	Managed AP is connected.
	Blue	Waiting for Approval	Managed AP is waiting for approval. Note: Eight Managed APs are supported. Additional APs will display this status until an existing Managed AP is removed.

Each Managed AP has “**Action**” icons with the following functions:



1. Disallow

Remove the Managed AP from the AP array and disable connectivity.

2. Edit

Edit various settings for the Managed AP.

3. Blink LED

The Managed AP's LED will flash temporarily to help identify and locate access points.

4. Buzzer

The Managed AP's buzzer will sound temporarily to help identify and locate access points.

5. Network Connectivity

Go to the “Network Connectivity” panel to perform **Trace Route**.

6. Restart

Restarts the Managed AP.

6.3.2 Managed AP Group

Managed APs can be grouped according to your requirements. Managed AP Group displays information about each Managed AP group in the local network: Group Name, MAC Address, Device Name, Model, IP Address, 2.4GHz & 5GHz Wireless Channel Number, No. of Clients connected to each access point, and Status (connected or disconnected).

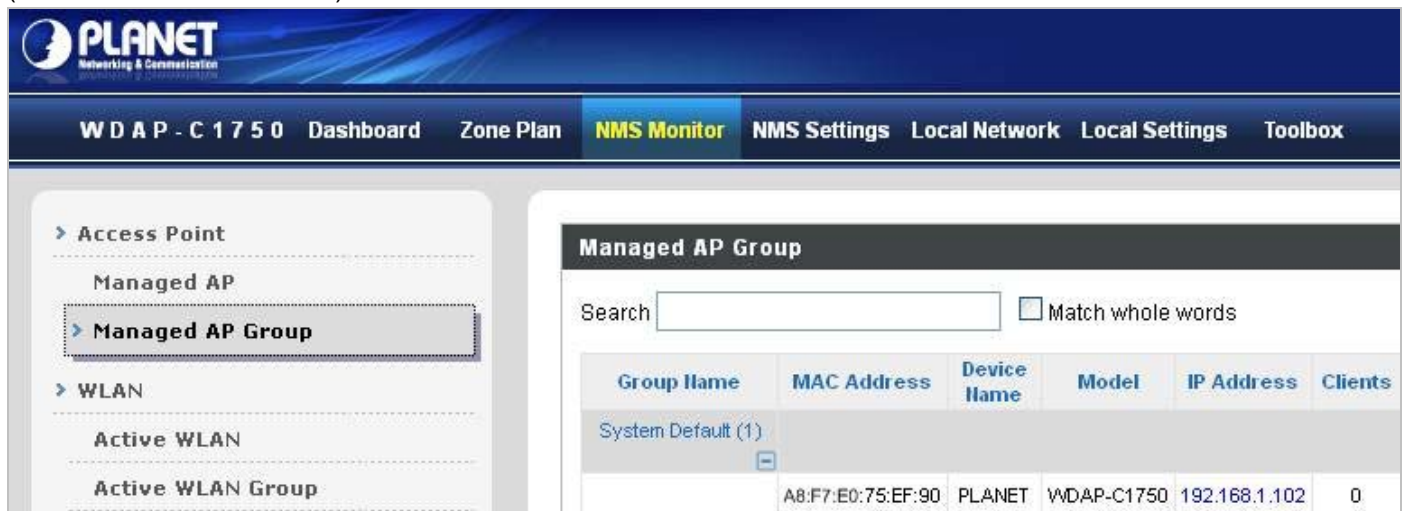


Figure 6-4 NMS Monitor—Managed AP Group

To edit Managed AP Groups, please go to **NMS Settings → Access Point**

6.3.3 Active WLAN

Displays information about each SSID in the AP Array: Index (reference number), Name/SSID, VLAN ID, Authentication, Encryption, IP Address and Additional Authentication.

To configure encryption and VLAN for Managed APs, please go to **NMS Settings → WLAN**.



Figure 6-5 NMS Monitor—Active WLAN

6.3.4 Active WLAN Group

WLAN groups can be created according to your preference. Active WLAN Group displays information about WLAN group: Group Name, Name/SSID, VLAN ID, Authentication, Encryption, IP Address and Additional Authentication.



Group Name	Name/SSID	VLAN ID	Authentication	Encryption	Additional Authentication
C1750_10F (0)					

Empty

Figure 6-6 NMS Monitor—Active WLAN Group

6.3.5 Active Clients

Displays information about clients currently connected to the AP Array: Index (reference number), Client MAC Address, AP MAC Address, WLAN (SSID), Radio (2.4GHz or 5GHz), Signal Strength received by Client, Connected Time, Idle Time, Tx & Rx (Data transmitted and received by Client in KB), and the Vendor of the client device.



Index	Client MAC Address	AP MAC Address	WLAN	Radio	Signal(%)	Connected Time	Idle Time	Tx(KB)	Rx(KB)	Vendor
1	C0:F8:DA:03:B9:86	80:1F:02:75:EF:90	PLANET_2.4G_e190	2.4GHz	100	6 secs	0	14.724	23.947	Hon Hai Precision Ind. Co.,Ltd.

Figure 6-7 Clients—Active Clients

6.3.6 All Events/Activities

Displays a log of time-stamped events for each access point in the Array – use the drop down menu to select an access point and view the log.

All Events/Activities				
Search <input type="text"/>		<input type="checkbox"/> Match whole words		
ID	Date and Time	Severity	Users	Events/Activities
4	2012/01/01 00:01:07	undefined	undefined	Managed AP(80:1F:02:75:EF:90) connect successfully
3	2012/01/01 00:00:20	undefined	undefined	Managed AP(80:1F:02:75:EF:90) start NMS WTP service successfully
2	2012/01/01 00:00:31	undefined	undefined	Managed AP(80:1F:02:75:EF:90) start NMS WTP service successfully
1	2012/01/01 00:00:44	undefined	undefined	Managed AP(80:1F:02:75:EF:90) start NMS WTP service successfully

Save Refresh



Figure 6-8 Information—All Events/Activities

6.4 NMS Settings

NMS Settings provides extensive configuration options for the AP Array. You can manage each access point, assign access points into groups, manage WLAN, RADIUS as well as upgrade firmware across multiple access points. The **Zone Plan** can also be configured using “**Zone Edit**”.

6.4.1 Access Point

Displays information about each access point and access point group in the local network and allows you to edit access points and edit or add access point groups.

Access Point										
Search <input type="text"/>		<input type="checkbox"/> Match whole words								
<input type="checkbox"/>	Index	MAC Address	Device Name	Model	AP Group	2.4G Channel	5G Channel	2.4G Tx Power	5G Tx Power	Status Action
<input type="checkbox"/>	1	A8:F7:E0:75:EF:90	PLANET	WDAP-C1750	System Default	2	36	Full	Full	 

Refresh Edit Delete Selected Delete All

Access Point Group								
Search <input type="text"/>		<input type="checkbox"/> Match whole words						
<input type="checkbox"/>	Group Name	AP Members	2.4G WLAN Profile	5G WLAN Profile	2.4G Guest Network Profile	5G Guest Network Profile	RADIUS Profile	Access Control Profile
<input type="checkbox"/>	System Default	1	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled

Add Edit Clone Delete Selected Delete All

Access Point Settings	
Auto Approve	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Apply

Figure 6-9 NMS Settings—Access Point

The Status icon displays grey (disconnected), red (authentication failed/incompatible NMS version), orange (upgrading firmware), yellow (connecting), green (connected) or blue (waiting for approval) for each individual Managed AP.

Select an access point or access point group using the checkboxes and click “Edit” to make configurations, or click “Add” to add a new access point group. You can also use Profile Settings to assign the access point to WLAN, RADIUS and Access Control groups independently from Access Point Group settings.

Check the “Override Default Settings” box to use different individual settings for access points assigned to AP Groups

6.4.1.1. Basic Settings

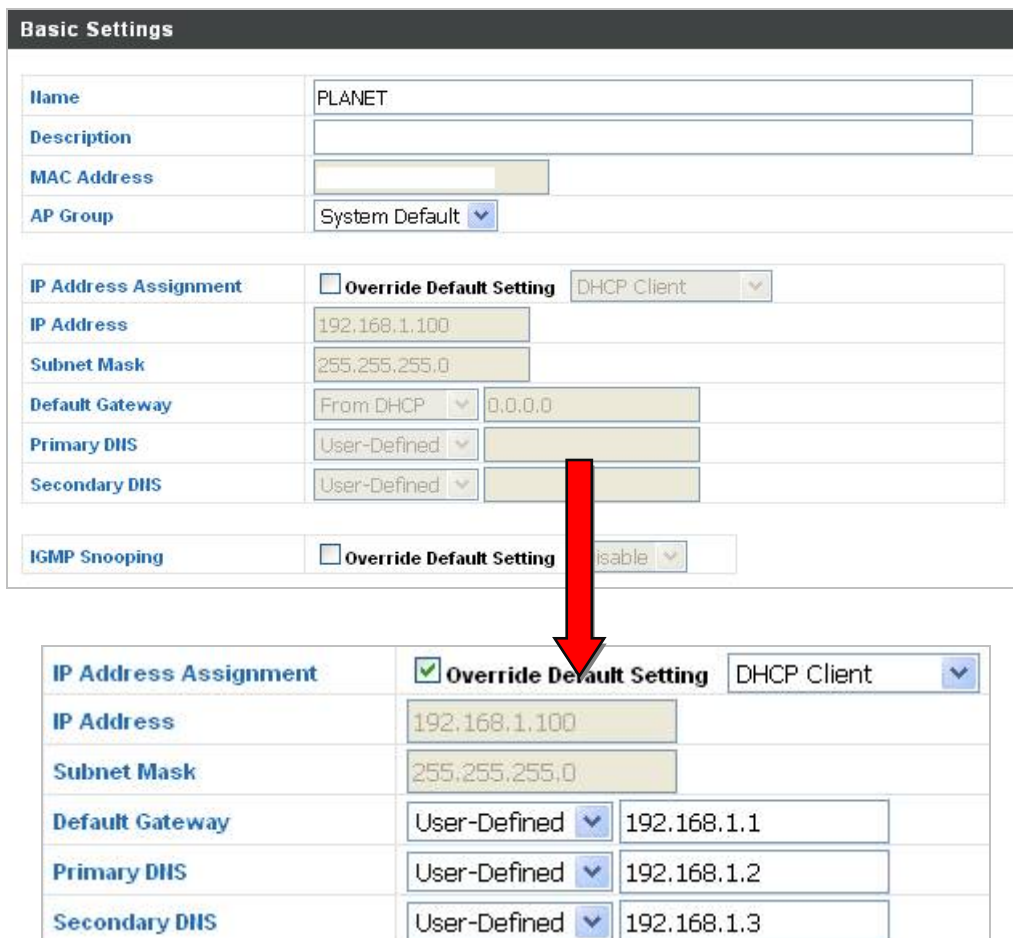


Figure 6-10 NMS Settings—Access Point Basic Settings

Object	Description
Name	Edit the access point name. The default name is PLANET.
Description	Enter a description of the access point for reference, e.g., 2nd Floor Office.
MAC Address	Displays MAC address.
AP Group	Use the drop-down menu to assign the AP to an AP Group. You can edit AP Groups from the NMS Settings → Access Point page.
IP Address Assignment	Select “DHCP Client” for your access point to be assigned a dynamic IP address from your router’s DHCP server, or select

	<p>“Static IP Address” to manually specify a static/fixed IP address for your access point (below). Check the box “Override Default Setting” if the AP is a member of an AP Group and you wish to use a different setting than the AP Group setting.</p>
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.
Primary DNS	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 DNS	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.

6.4.1.2. VLAN Settings

VLAN Settings

Wired LAN Port	VLAN Mode	VLAN ID
Wired Port(#1)	<input checked="" type="checkbox"/> Override Default Setting Untagged Port	<input type="checkbox"/> Override Default Setting 1
Wired Port(#2)	<input type="checkbox"/> Override Default Setting Untagged Port	<input type="checkbox"/> Override Default Setting 1
Management VLAN ID	<input type="checkbox"/> Override Default Setting 1	

Figure 6-11 NMS Settings—Access Point VLAN Settings

Object	Description
Wired Port	Identifies LAN port.
VLAN Mode	Check the box “ Override Default Setting ” if the AP is a member of an AP Group and you wish to use a different setting than the AP Group setting. Select “ Untagged Port ” or “ Tagged Port ” specified LAN 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.

6.4.1.3. Radio Settings

Radio Settings		
	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Wireless	<input type="checkbox"/> Override Default Setting Enable	<input type="checkbox"/> Override Default Setting Enable
Band	<input type="checkbox"/> Override Default Setting 11b/g/n	<input type="checkbox"/> Override Default Setting 11a/n
Auto Channel	<input type="checkbox"/> Override Default Setting Enable	<input type="checkbox"/> Override Default Setting Enable
Auto Channel Range	<input type="checkbox"/> Override Default Setting Ch 1 - 11	<input type="checkbox"/> Override Default Setting Band 1
Auto Channel Interval	<input type="checkbox"/> Override Default Setting One day <input type="checkbox"/> Change channel even if clients are connected	<input type="checkbox"/> Override Default Setting One day <input type="checkbox"/> Change channel even if clients are connected
Channel	<input type="checkbox"/> Override Default Setting Ch 11, 2462MHz	<input type="checkbox"/> Override Default Setting Ch 36, 5.18GHz
Channel Bandwidth	<input type="checkbox"/> Override Default Setting 20 MHz	<input type="checkbox"/> Override Default Setting 20 MHz
BSS BasicRateSet	<input type="checkbox"/> Override Default Setting 1,2,5,5,11 Mbps	<input type="checkbox"/> Override Default Setting 6,12,24 Mbps

Figure 6-12 NMS Settings—Access Point Radio Settings

Object	Description
Wireless	Enable or disable the access point's 2.4GHz or 5GHz wireless radio. When disabled, no SSIDs on that frequency will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g, 802.11n & 802.11ac can be selected.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 2.4GHz or 5GHz frequency based on availability and potential interference. When disabled, select a channel manually.
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 or use Auto (automatically select based on interference level).
BSS Basic Rate Set	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

6.4.1.4. Advanced Settings

The advanced 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.

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
Contention Slot	<input type="checkbox"/> Override Default Setting Short	
Preamble Type	<input type="checkbox"/> Override Default Setting Short	
Guard Interval	<input type="checkbox"/> Override Default Setting Short GI	<input type="checkbox"/> Override Default Setting Short GI
802.11n Protection	<input type="checkbox"/> Override Default Setting Enable	<input type="checkbox"/> Override Default Setting Enable
CE Adaptive	<input type="checkbox"/> Override Default Setting Disable	
DTIM Period	<input type="checkbox"/> Override Default Setting 1 (1-255)	<input type="checkbox"/> Override Default Setting 1 (1-255)
RTS Threshold	<input type="checkbox"/> Override Default Setting 2347 (1-2347)	<input type="checkbox"/> Override Default Setting 2347 (1-2347)
Fragment Threshold	<input type="checkbox"/> Override Default Setting 2346 (256-2346)	<input type="checkbox"/> Override Default Setting 2346 (256-2346)
Multicast Rate	<input type="checkbox"/> Override Default Setting Auto	<input type="checkbox"/> Override Default Setting Auto
Tx Power	<input type="checkbox"/> Override Default Setting 100%	<input type="checkbox"/> Override Default Setting 100%
Beacon Interval	<input type="checkbox"/> Override Default Setting 100 (40-1000 ms)	<input type="checkbox"/> Override Default Setting 100 (40-1000 ms)
Station idle timeout seconds)	<input type="checkbox"/> Override Default Setting 60 (30-65535 seconds)	<input type="checkbox"/> Override Default Setting 60 (30-65535 seconds)

Figure 6-13 NMS Settings—Access Point Advanced Settings

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 preamble type in 802.11 based wireless communications defines the length of the CRC (Cyclic Redundancy Check) block for communication between the access point and roaming wireless adapters. The default value is “Short”.
Guard Interval	Set the guard interval. A shorter interval can improve performance.
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 interval for keep alive messages from the access point to a wireless client to verify if the station is still alive/active.



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

6.4.1.5. Profile Settings

Profile Settings

	Radio B/G/N (2.4 GHz)	Radio A/N/AC (5.0 GHz)
WLAN Group	<input type="checkbox"/> Override Default Setting Disable ▾	<input type="checkbox"/> Override Default Setting Disable ▾
RADIUS Group	<input type="checkbox"/> Override Default Setting Disable ▾	
MAC Access Control Group	<input type="checkbox"/> Override Default Setting Disable ▾	

Figure 6-14 NMS Settings—Access Point Profile Settings

Object	Description
WLAN Group	Assign the access point's 2.4GHz or 5GHz SSID(s) to a WLAN Group. You can edit WLAN groups in NMS Settings → WLAN .
RADIUS Group	Assign the access point's 2.4GHz SSID(s) to a RADIUS group. You can edit RADIUS groups in NMS Settings → RADIUS .
Access Control Group	Assign the access point's 2.4GHz SSID(s) to a RADIUS group. You can edit RADIUS groups in NMS Settings → Access Control .

6.4.2 WLAN

Displays information about each WLAN and WLAN group in the local network and allows you to add or edit WLAN & WLAN Groups. When you add a WLAN Group, it will be available for selection in **NMS Settings** → **Access Point & Access Point Group** settings.

WLAN

Search Match whole words

<input type="checkbox"/>	Name/SSID	VLAN ID	Authentication	Encryption	Additional Authentication
<input type="checkbox"/>	C1750_2.4G	1	WPA2PSK	AES	No additional authentication
<input type="checkbox"/>	C1750_5G	1	WPA1PSK/WPA2PSK	TKIP/AES	No additional authentication

WLAN Groups

Search Match whole words

<input type="checkbox"/>	Group Name	WLAN members	WLAN member list	Used AP	Used AP Group
<input type="checkbox"/>	C1750_10F	0			

Figure 6-15 NMS Settings—WLAN

6.4.2.1. WLAN Settings

Select a WLAN or WLAN Group using the check-boxes and click **“Edit”** or click **“Add”** to add a new WLAN or WLAN Group.

WLAN Settings	
Name/ESSID	OFFICE
Description	10 floor office
VLAN ID	1
Broadcast SSID	Enable
Wireless Client Isolation	Disable
Load Balancing	50 /50
Authentication Method	WPA-PSK
WPA Type	WPA2 Only
Encryption Type	AES
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase
Pre-shared Key	abcd1234
Additional Authentication	No additional authentication

Apply Cancel

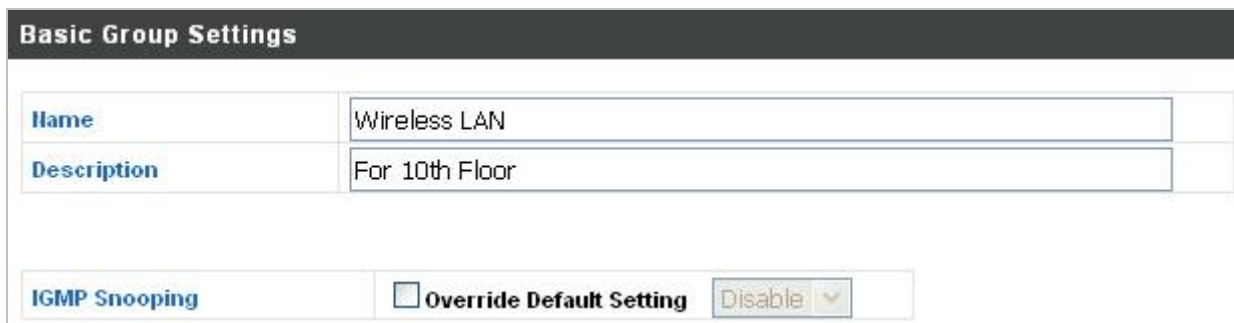
Figure 6-16 NMS Settings—WLAN Settings

Object	Description
Name/ESSID	Edit the WLAN name (SSID).
Description	Enter a description of the SSID for reference e.g. 2nd Floor Office HR.
SSID	Select which SSID to configure security settings for.
VLAN ID	Specify the VLAN ID.
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.
Additional Authentication	Select an additional authentication method from the drop-down menu.

6.4.2.2. WLAN Group Settings

When you add a WLAN Group, it will be available for selection in **NMS Settings** → **Access Point Group** settings.



The screenshot shows the 'Basic Group Settings' form. It includes two text input fields: 'Name' with the value 'Wireless LAN' and 'Description' with the value 'For 10th Floor'. Below these fields is a section for 'IGMP Snooping' with an unchecked checkbox for 'Override Default Setting' and a dropdown menu currently set to 'Disable'.

Figure 6-17 NMS Settings—WLAN Group Settings

Object	Description
Name	Edit the WLAN Group name.
Description	Enter a description of the WLAN Group for reference, e.g., 2nd Floor Office HR Group.
Members	Select SSIDs to include in the group using the checkboxes and assign VLAN IDs.

6.4.3 RADIUS

Displays information about External & Internal RADIUS Servers, Accounts and Groups, and allows you to add or edit RADIUS Servers, Accounts & Groups. When you add a RADIUS Group, it will be available for selection in **NMS Settings** → **Access Point & Access Point Group** settings.

6.4.3.1. External RADIUS Server

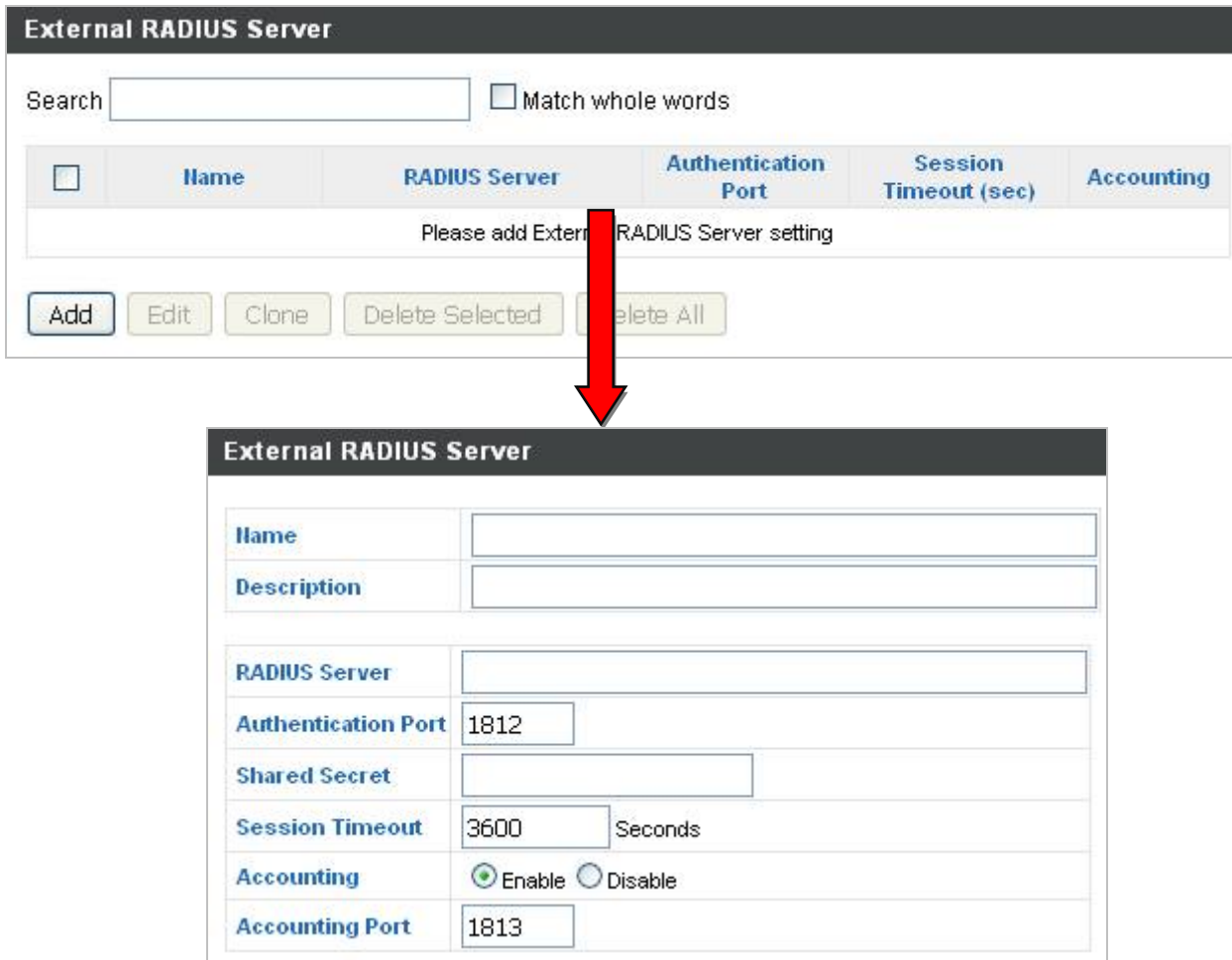


Figure 6-18 NMS Settings—External RADIUS Server

Object	Description
Name	Enter a name for the RADIUS Server.
Description	Enter a description of the RADIUS Server for reference.
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 1 to 65535.
Shared Secret	Enter a shared secret/password between 1 and 99 characters in length.
Session Timeout	Set 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.

6.4.3.2. Internal RADIUS Server

Upload EAP Certificate File

EAP Certificate File Format	PKCS#12(*.pfx/*.p12)
Upload EAP Certificate File	<input type="button" value="Browse..."/> No file selected.
Password of EAP Certificate File	<input type="text"/>

Internal RADIUS Server

Name	<input type="text"/>
Description	<input type="text"/>
EAP Internal Authentication	PEAP(MS-PEAP) <input type="button" value="v"/>
Shared Secret	<input type="text"/>
Session-Timeout	<input type="text" value="3600"/> Seconds
Termination-Action	<input checked="" type="radio"/> Reauthentication (RADIUS-Request) <input type="radio"/> Not-Reauthentication (Default) <input type="radio"/> Not-Send

Figure 6-19 NMS Settings—Internal RADIUS Server

Object	Description
EAP Certificate File Format	Displays the EAP certificate file format: PKCS#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.
Name	Enter a name for the Internal RADIUS Server.
Description	Enter a description of the RADIUS Server for reference.
RADIUS Server	Enter the RADIUS server host IP address.
EAP Internal Authentication	Select EAP internal authentication type from the drop down menu.
Shared Secret	Enter a shared secret/password between 1 to 99 characters in length.
Session Timeout	Set duration of session timeout in seconds between 0 and 86400.
Termination Action	Select a termination-action attribute: “Reauthentication” sends a RADIUS request to the access point, “Not-Reauthentication”

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

6.4.3.3. RADIUS Accounts

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

RADIUS Accounts

User Name

Example: USER1, USER2, USER3, USER4

User Registration List

User Name	Password	Description	Action
Please add Account(s)			

Figure 6-20 NMS Settings—RADIUS Account

Object	Description
User Name	Enter the user names here, separated by commas.
Add	Click “Add” to add the user to the user registration list.
Reset	Clear text from the user name box.
Delete Selected	Delete selected user from the user registration list.
Delete All	Delete all users from the user registration list.

6.4.4 Access Control

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.

The MAC address filtering table is displayed below.




Figure 6-21 NMS Settings—Access Control

Object	Description
Add MAC Address	Enter a MAC address of computer or network device manually e.g. 'aa-bb-cc-dd-ee-ff' or enter multiple MAC addresses separated with commas, e.g. 'aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg'
Add	Click “ Add ” to add the MAC address to the MAC address filtering table.
Reset	Clear all fields.

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.

6.4.5 Zone Edit

You can upload the sketch map for the radio coverage and location planning. Press “Add” to upload the map image.

Zone Edit

Search Match whole words

655360 bytes Available (655360 bytes Total)

<input type="checkbox"/>	Name/Location	Map	Map Size	Number of APs
Please add Zone Edit setting				



Upload Zone Image

Map Image File No file selected.

Member(s) Settings




Name/Location	<input type="text"/>															
Description	<input type="text"/>															
	Search <input type="text"/> <input type="checkbox"/> Match whole words															
Member(s)	<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 5%;"></th> <th style="width: 30%;">MAC Address</th> <th style="width: 20%;">Device Name</th> <th style="width: 20%;">Model</th> <th style="width: 25%;">Status</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>System Default</td> <td></td> <td></td> <td></td> </tr> <tr> <td><input type="checkbox"/></td> <td>A8:F7:E0:75:EF:90</td> <td>PLANET</td> <td>WDAP-C1750</td> <td style="text-align: center;"></td> </tr> </tbody> </table>		MAC Address	Device Name	Model	Status	<input type="checkbox"/>	System Default				<input type="checkbox"/>	A8:F7:E0:75:EF:90	PLANET	WDAP-C1750	
	MAC Address	Device Name	Model	Status												
<input type="checkbox"/>	System Default															
<input type="checkbox"/>	A8:F7:E0:75:EF:90	PLANET	WDAP-C1750													

Figure 6-22 NMS Settings—Zone Edit

6.4.6 Firmware Upgrade

Firmware Upgrade allows you to upgrade firmware to Access Point Groups. First, upload the firmware file from a local disk or external FTP server: locate the file and click “**Upload**” or “**Check**”. The table below will display the Firmware Name, Firmware Version, NMS Version, Model and Size.

Then click “**Upgrade All**” to upgrade all access points in the Array or select Access Point groups from the list using checkboxes and click “**Upgrade Selected**” to upgrade only selected access points.

Firmware Upgrade

Update firmware from: Local External FTP Server

Firmware File: No file selected.

Timeout: Seconds

Firmware Name	Firmware Version	NMS Version	Model	Size (bytes)

Access Point Group

	Group Name	MAC Address	Device Name	Model	IP Address	Status	Firmware Version	NMS Version	Progress
	System Default (1)								
<input type="checkbox"/>		A8:F7:E0:75:EF:90	PLANET	WDAP-C1750	192.168.1.100	●	0.0.2	1.0.4.0	0%

Figure 6-23 NMS Settings—Firmware Upgrade

6.4.7 Advanced

Configure the NMS system login name and password.

System Security

NMS Security Name

NMS Security Key (8~16 Characters)

Sync NMS Security with Active Managed APs Enable

*Before changing NMS Security Name and Key, please make sure all Managed APs are connected; all other configuration update is complete, and status color is green.

Figure 6-24 NMS Settings—Advanced

6.5 Local Network

Local Network settings are for your AP Controller. You can configure the IP address and DHCP server of the AP Controller in addition to 2.4GHz & 5GHz Wi-Fi and security, with WPS, RADIUS server, MAC filtering and WMM settings also available.

Please refer to the Chapter 5.2 and 5.3 for more information.

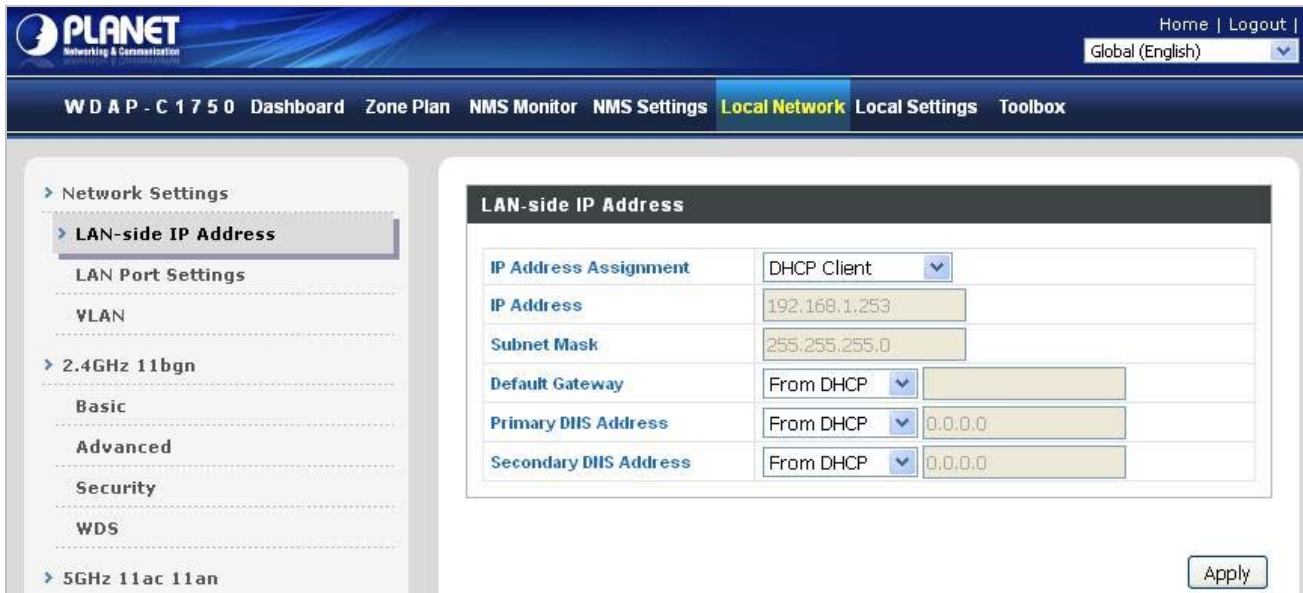


Figure 6-25 Local Network

6.6 Local Settings

Local Settings are for your AP Controller. You can set the operation mode and view network settings (clients and logs) specifically for the AP Controller, as well as other management settings such as date/time, admin accounts, firmware and reset.

Please refer to the Chapter 5.4 and 5.5 for more information.

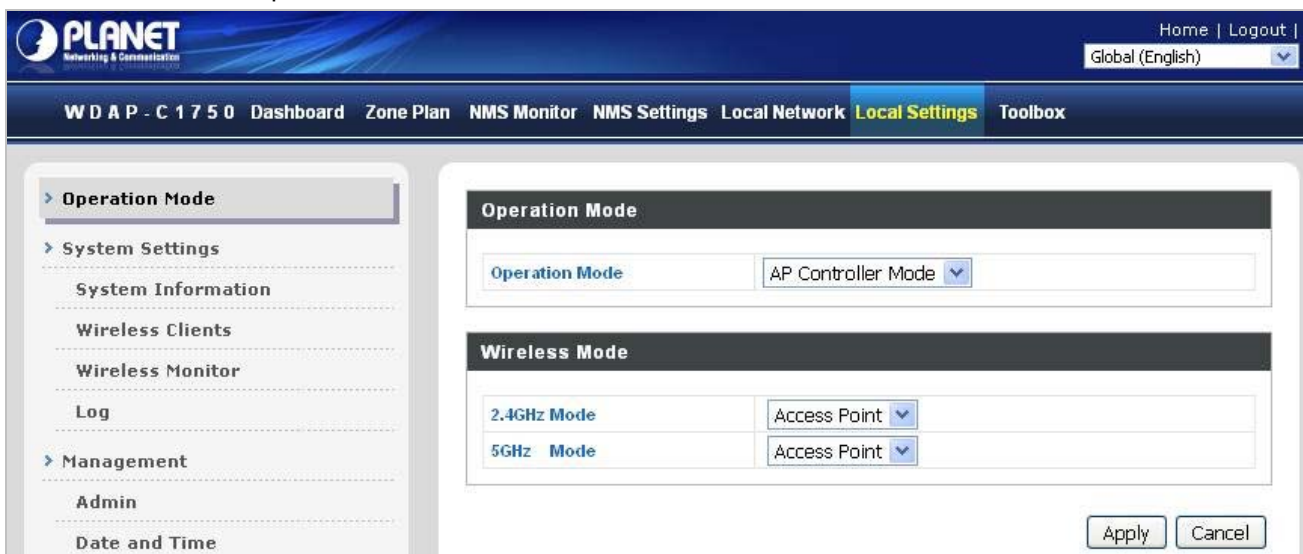


Figure 6-26 Local Settings

6.7 Toolbox

The Toolbox panel provides the network diagnostic tool **Ping** and **Trace Route**.

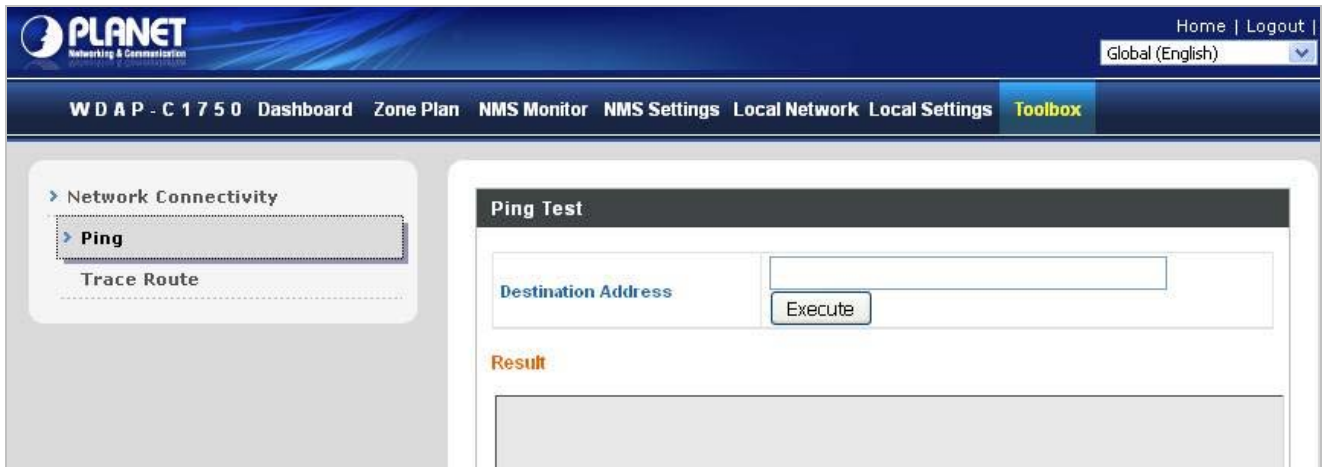


Figure 6-27 Toolbox

Chapter 7. Quick Connection to a Wireless Network

In the following sections, the **default SSID** of the WDAP-C1750 is configured to “**default**”.

7.1 Windows XP (Wireless Zero Configuration)

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



Figure 7-1 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

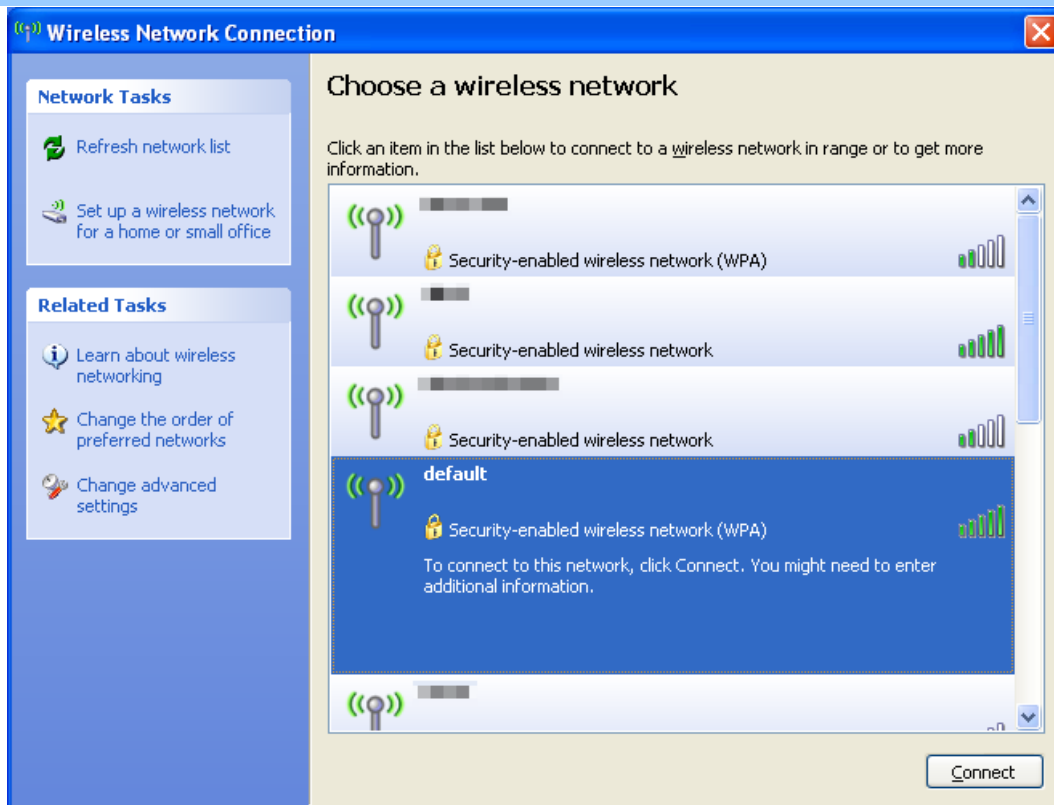


Figure 7-2 Choose a wireless network

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

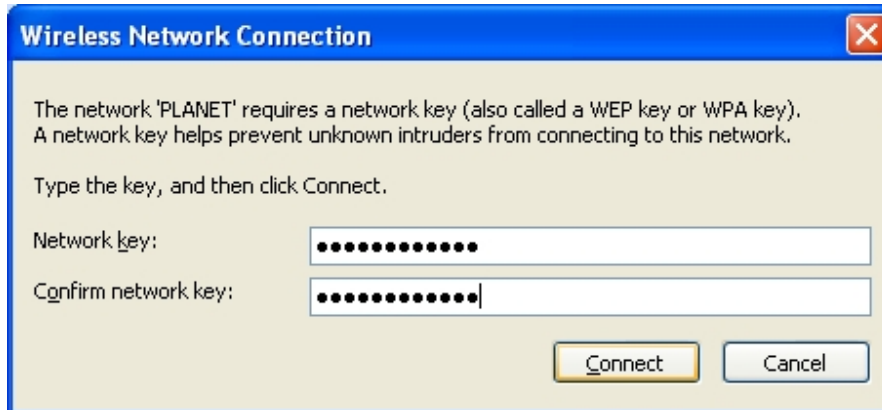


Figure 7-3 Enter the network key

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

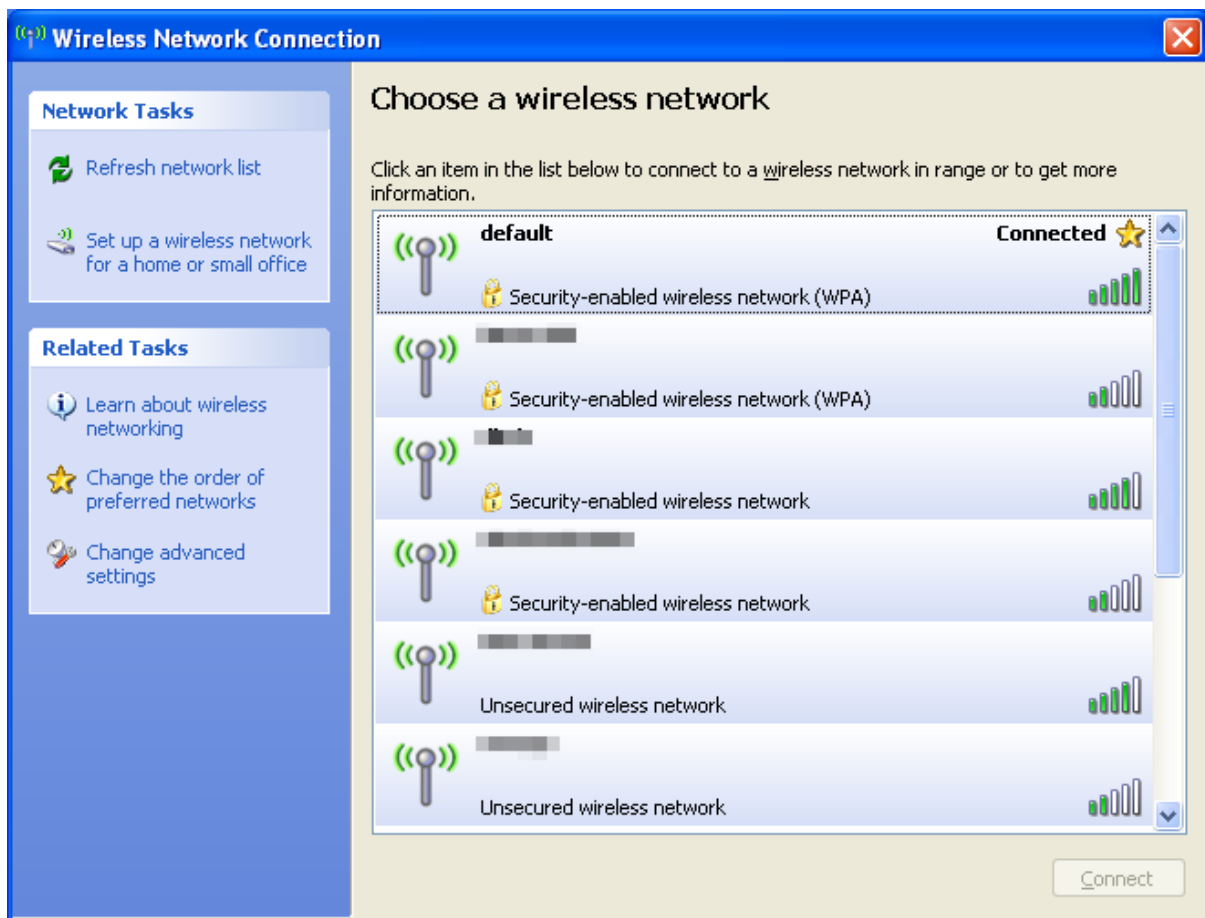


Figure 7-4 Choose a wireless network -- Connected



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.

7.2 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 7-5 Network icon

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

- (1) Select SSID [default]
- (2) Click the [Connect] button

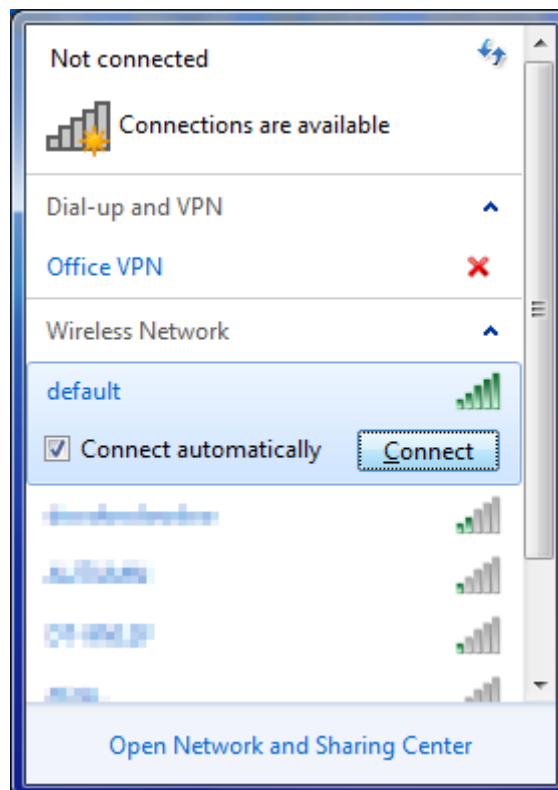


Figure 7-6 WLAN AutoConfig



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 7-7 Type the network key

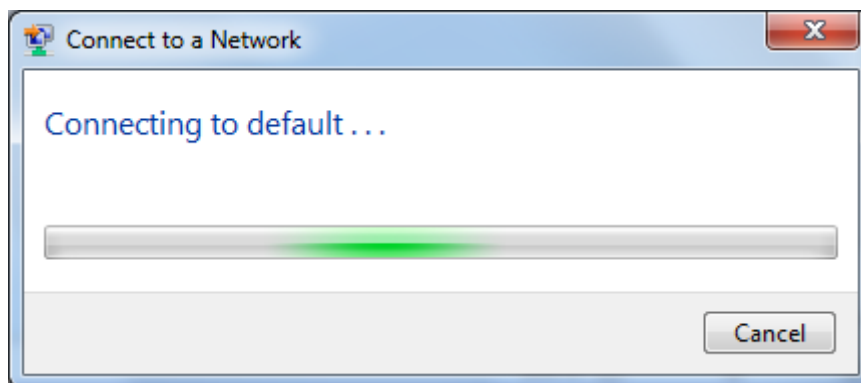


Figure 7-8 Connecting to a Network

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

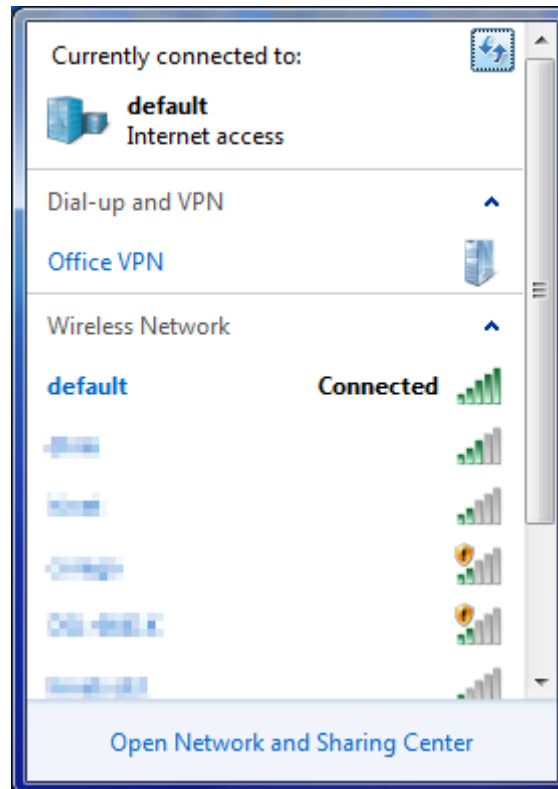


Figure 7-9 Connected to a Network

7.3 Mac OS X 10.x

In the following sections, the default SSID of the WDAP-C1750 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 7-10 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 7-11 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

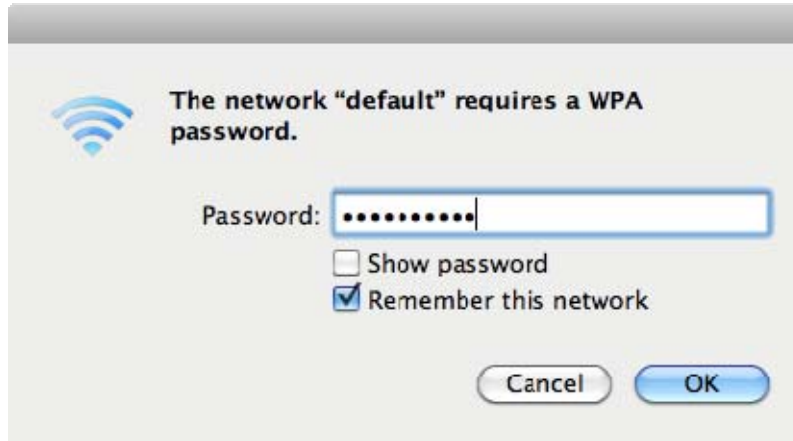


Figure 7-12 Enter the Password



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.

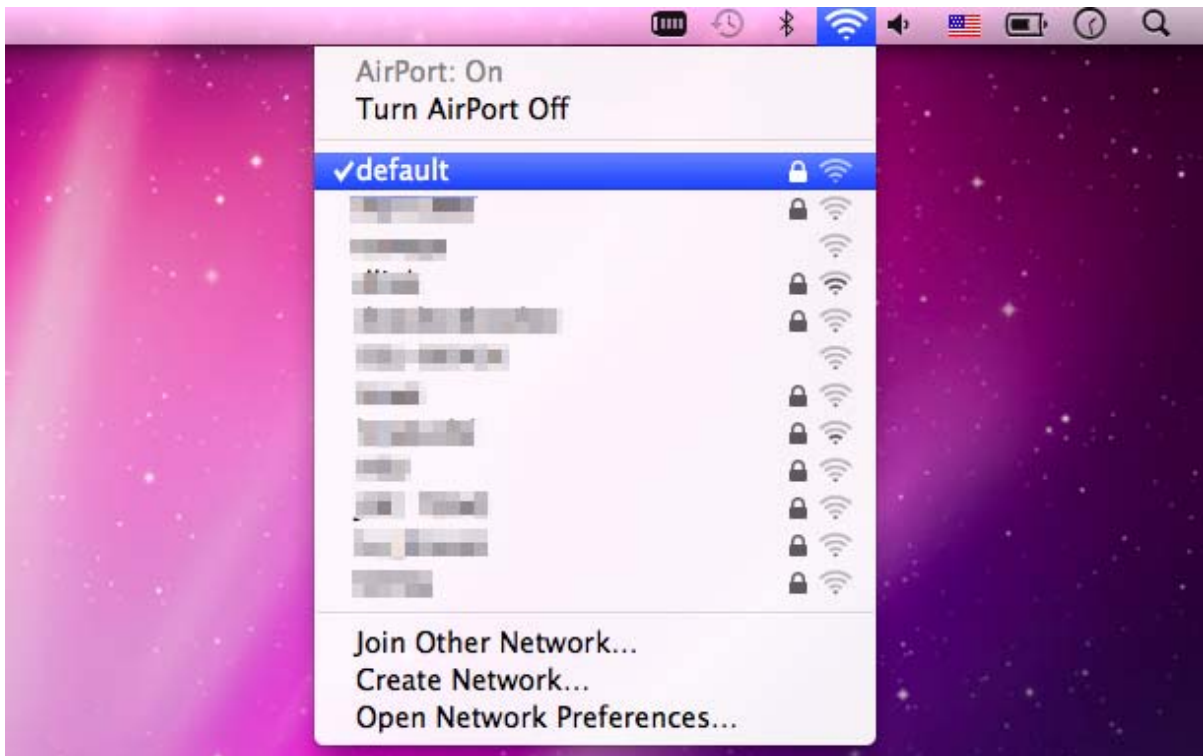


Figure 7-13 Connected to the Network

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**

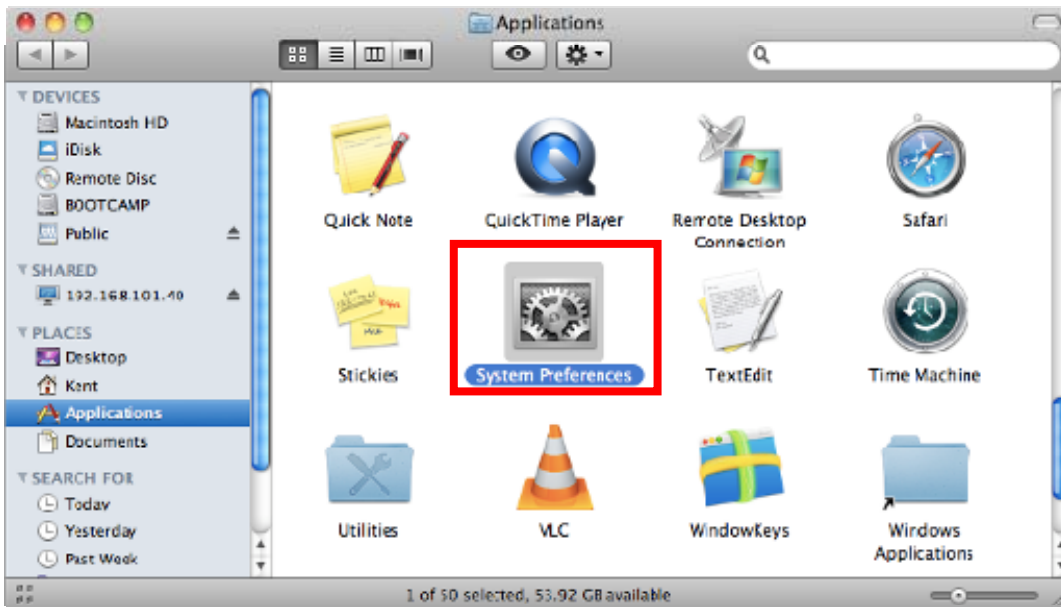


Figure 7-14 System Preferences

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

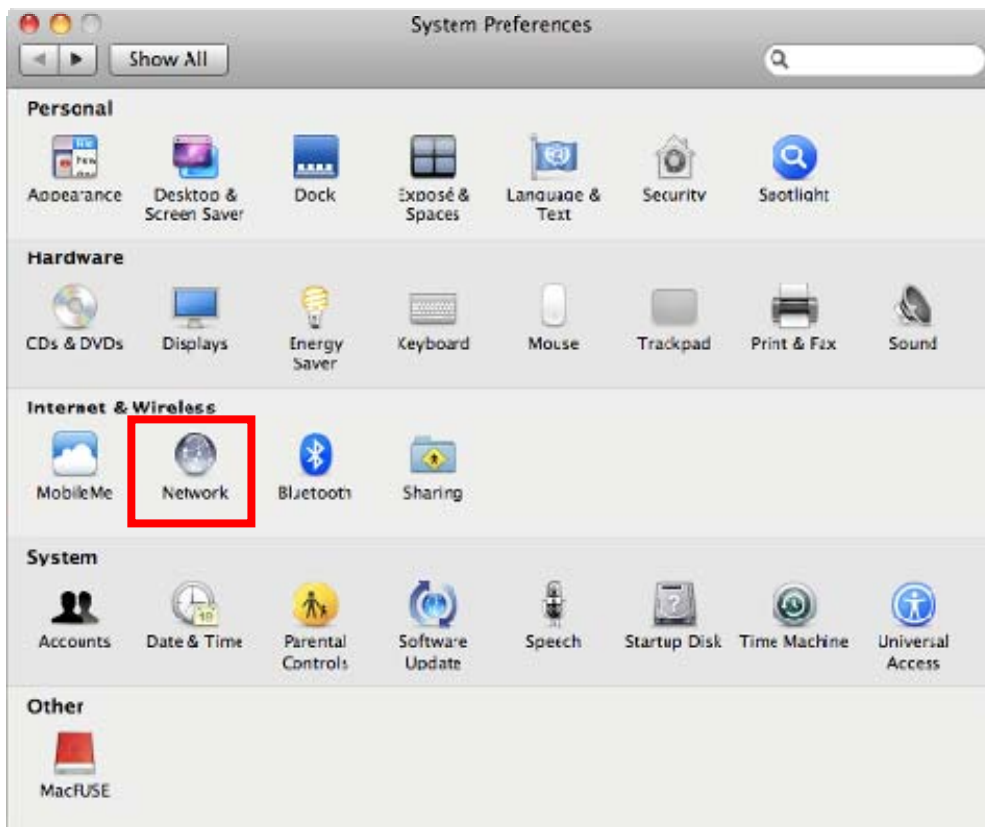


Figure 7-15 System Preferences -- Network

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

- (1) Choose the **AirPort** on the left side of the menu (make sure it is ON)
- (2) Select Network Name [**default**] here

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

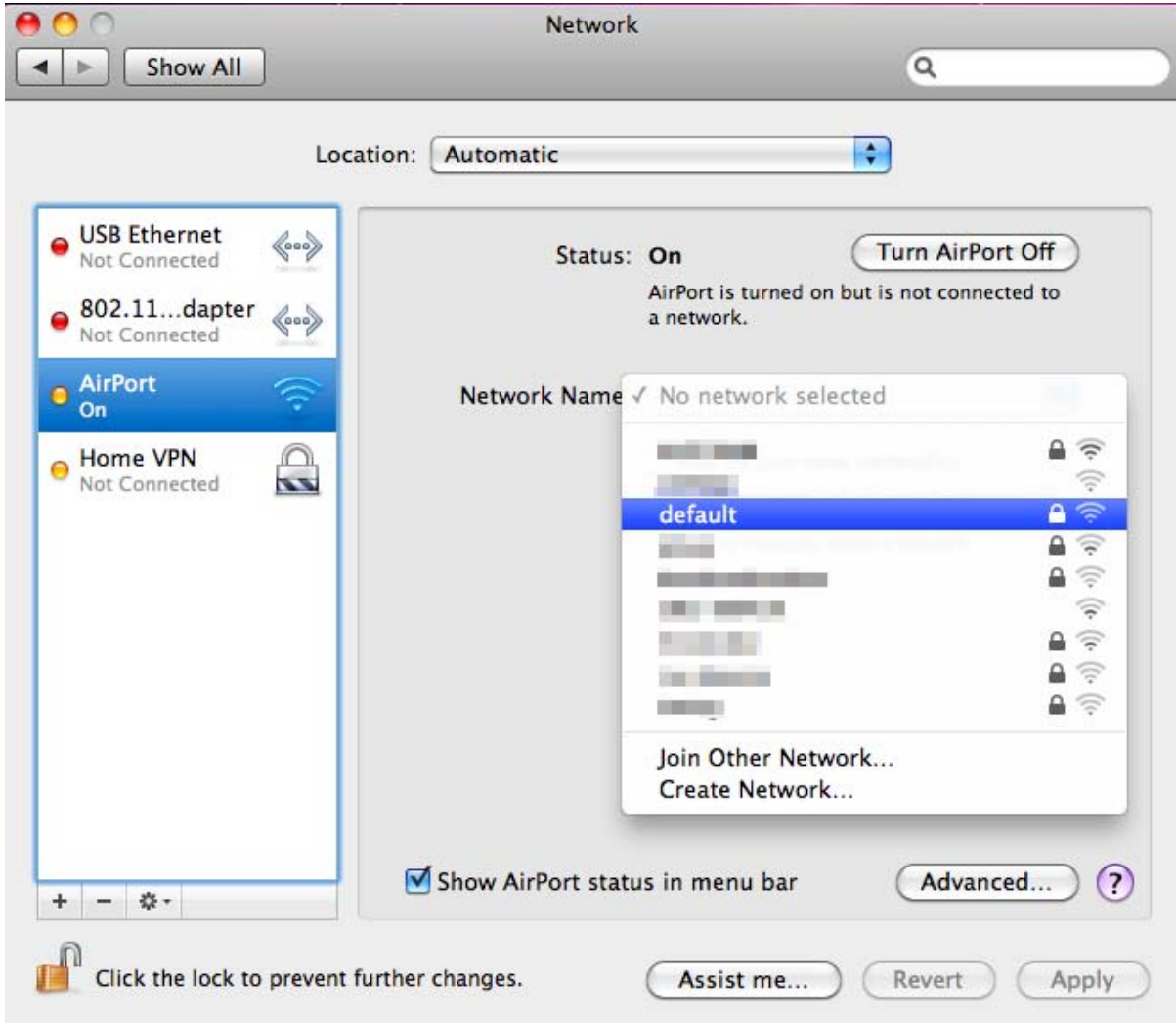


Figure 7-16 Select the Wireless Network

7.4 iPhone/iPod Touch/iPad

In the following sections, the **default SSID** of the WDAP-C1750 is configured to “**default**”.

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

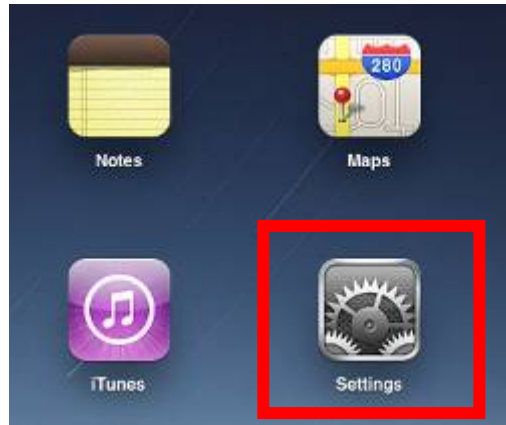


Figure 7-17 iPhone – Settings icon

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 7-18 Wi-Fi Setting

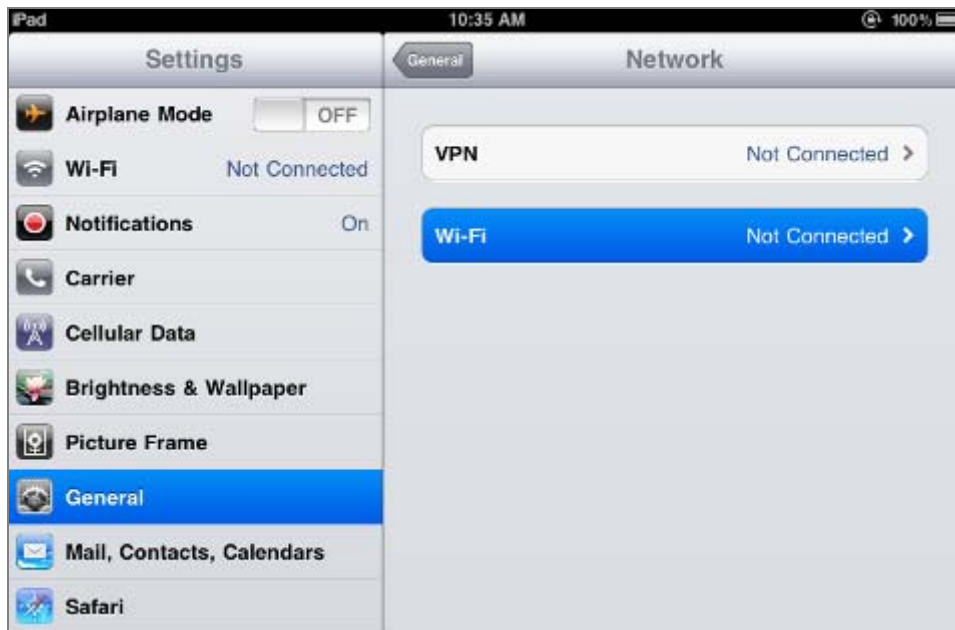


Figure 7-19 Wi-Fi Setting – Not Connected

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 7-20 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

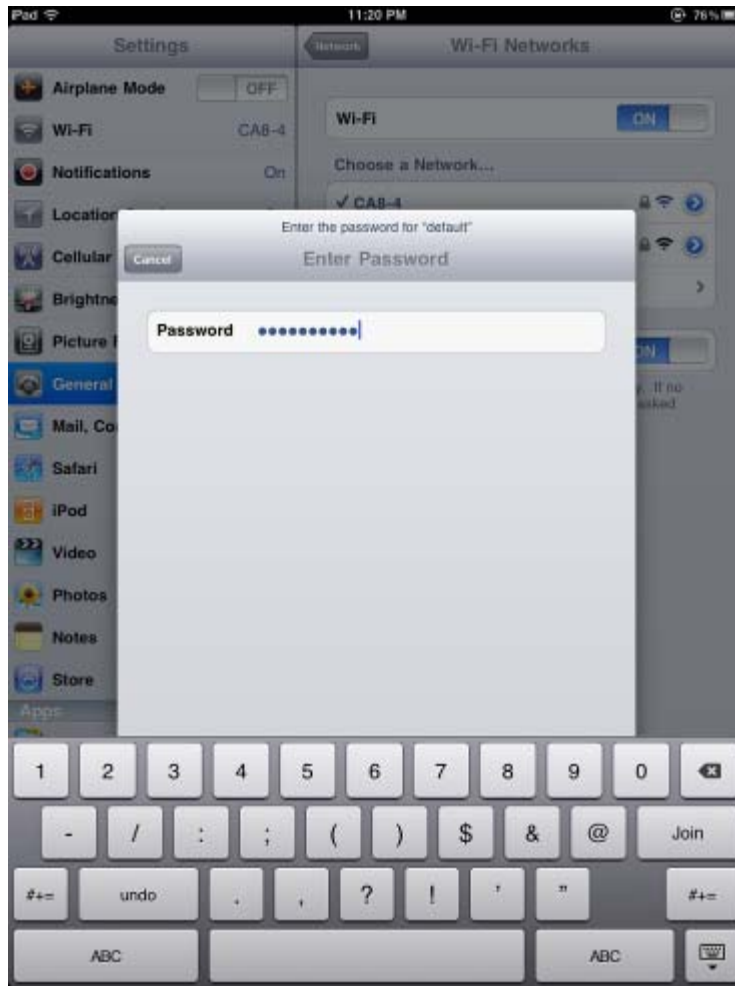


Figure 7-21 iPhone -- Enter the Password

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 7-22 iPhone -- Connected to the Network

Appendix A: Planet Smart Discovery Utility

To easily list the WDAP-C1750 in your Ethernet environment, the Planet Smart Discovery Utility is an ideal solution. The utility is available at: http://www.planet.com.tw/en/product/images/48590/Planet_Utility.zip

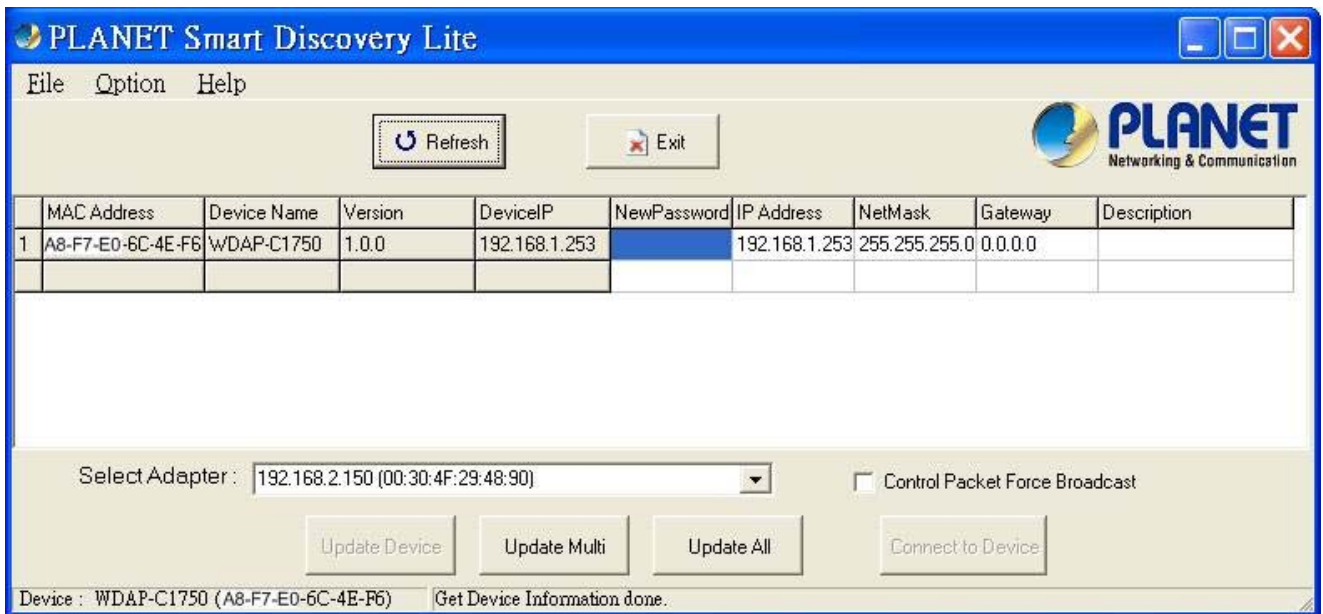
The following installation instructions guide you to running the Planet Smart Discovery Utility.

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

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



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



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



The fields in the 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.

	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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.	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 (Dynamic Domain Name System)** - The capability of assigning a fixed host and domain name to a dynamic Internet IP Address.
- **DHCP (Dynamic Host Configuration Protocol)** - A protocol that automatically configure the TCP/IP parameters for the all the PC(s) that are connected to a DHCP server.
- **DMZ (Demilitarized Zone)** - 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 (Domain Name System)** - 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 (Digital Subscriber Line)** - A technology that allows data to be sent or received over existing traditional phone lines.
- **ISP (Internet Service Provider)** - 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 (Network Address Translation)** - NAT technology translates IP addresses of a local area network to a different IP address for the Internet.
- **PPPoE (Point to Point Protocol over Ethernet)** - PPPoE is a protocol for connecting remote hosts to the Internet over an always-on connection by simulating a dial-up connection.
- **SSID - A Service Set Identification** 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 (Wired Equivalent Privacy)** - 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 (Wireless Local Area Network)** - A group of computers and associated devices communicate with each other wirelessly, which network serving users are limited in a local area.

EC Declaration of Conformity

English	Hereby, PLANET Technology Corporation , declares that this 11ac Wireless AP is in compliance with the essential requirements and other relevant provisions of Directive 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 rilevanti 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". (BMW i)	Nederlands	Hierbij verklaart, PLANET Technology Corporation , 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/CE”.
Ελληνικά	<i>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</i>	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.