USER MANUAL

WAP-EN Series

Wireless Access Points

Version 1.3.0 June 2018

FCC Compliance

This equipment has been tested and found to comply with the limits for a Class B Digital Device, pursuant to part 15 of the 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 instruction, may cause harmful interference to radio communication. 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:

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

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

To comply with the FCC RF exposure compliance requirements, this device and its antenna must not be co-located or operating to conjunction with any other antenna or transmitter.
This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Copyright

NOTE: This document is subject to change without notice.

Protect Our Environment

This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling center and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law.

CONTENTS

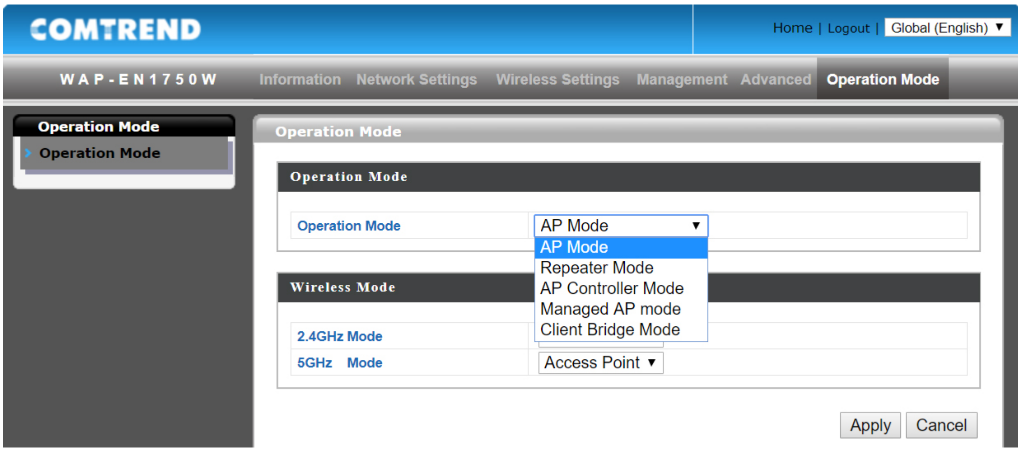
Overview

The default mode for your EN-Series access point is “AP Mode”.

AP Mode is a regular access point for your network.

Some EN-Series access points can also function as an **AP Controller,** acting as a designated “Master” for an array of “Slave” access points. (Up to a maximum of 5 remote access points)

Managed AP Mode acts like a “Slave” access point in an access point array. (Controlled by the AP Controller “Master” or WLC-6404 Wireless Access Point Controller)



Operation Mode

Operation Mode: AP Mode

Wireless Mode

2.4GHz Mode

5GHz Mode: Access Point

The user interface will change depending on which mode is selected.

This manual will cover the AP Mode functions only.

{Image will vary slightly from device models to device models}

{Available frequencies will vary from device models to device models}

I. Browser Based Configuration Interface

The browser-based configuration interface enables you to configure the access point's advanced features. The device features a range of advanced functions such as MAC filtering, MAC RADIUS authentication, VLAN configurations, up to 16-32 SSIDs and many more. To access the browser-based configuration interface:

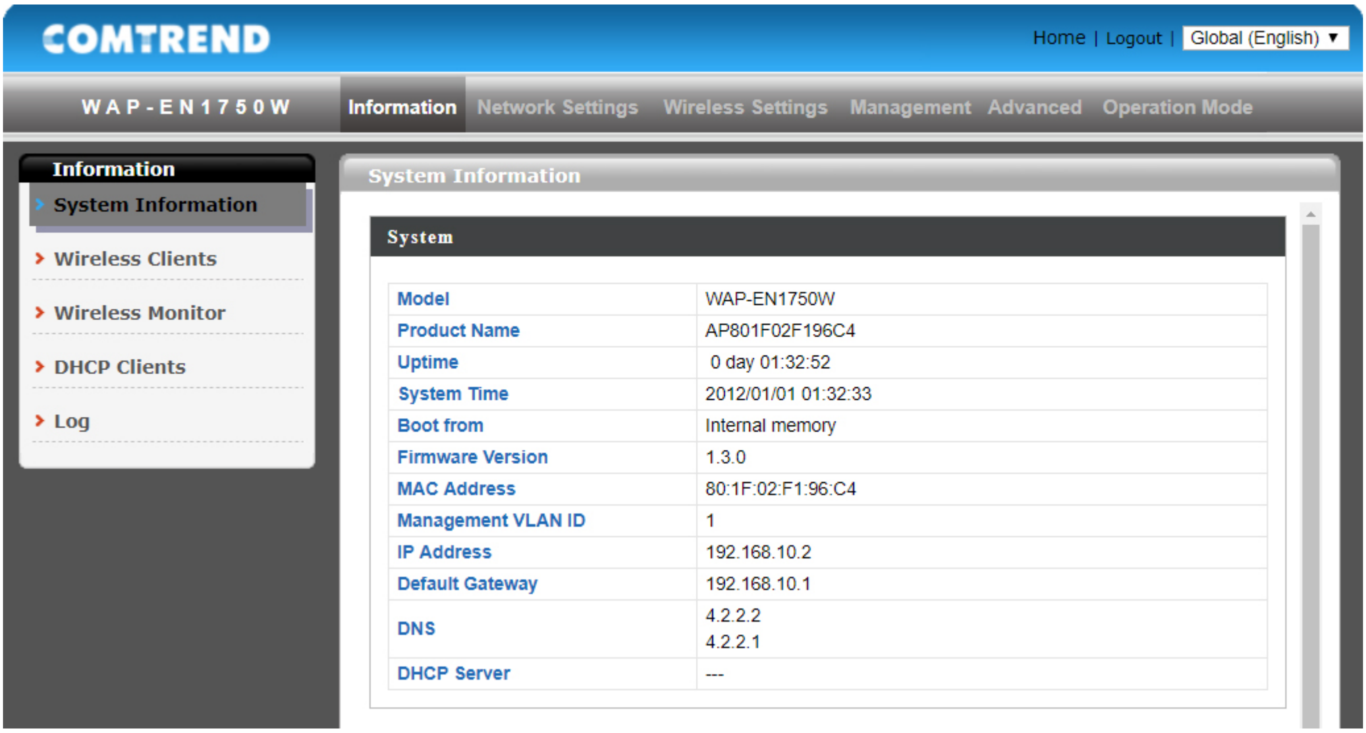
1. Connect a computer to your access point using an Ethernet cable.

2. Enter your access point's IP address in the URL bar of a web browser. If no DHCP Services is discovered, the access point's default IP address is **192.168.2.2 or 192.168.2.1.**

3. You will be prompted for a username and password. The default username is "admin" and the default password is "admin" or "1234", though it was recommended that you change the password.

If you cannot remember your password, reset the access point back to its factory default settings. Refer to the Quick Installation Guide for instructions on how to factory reset your device.

4. You will arrive at the "System Information" screen shown below.

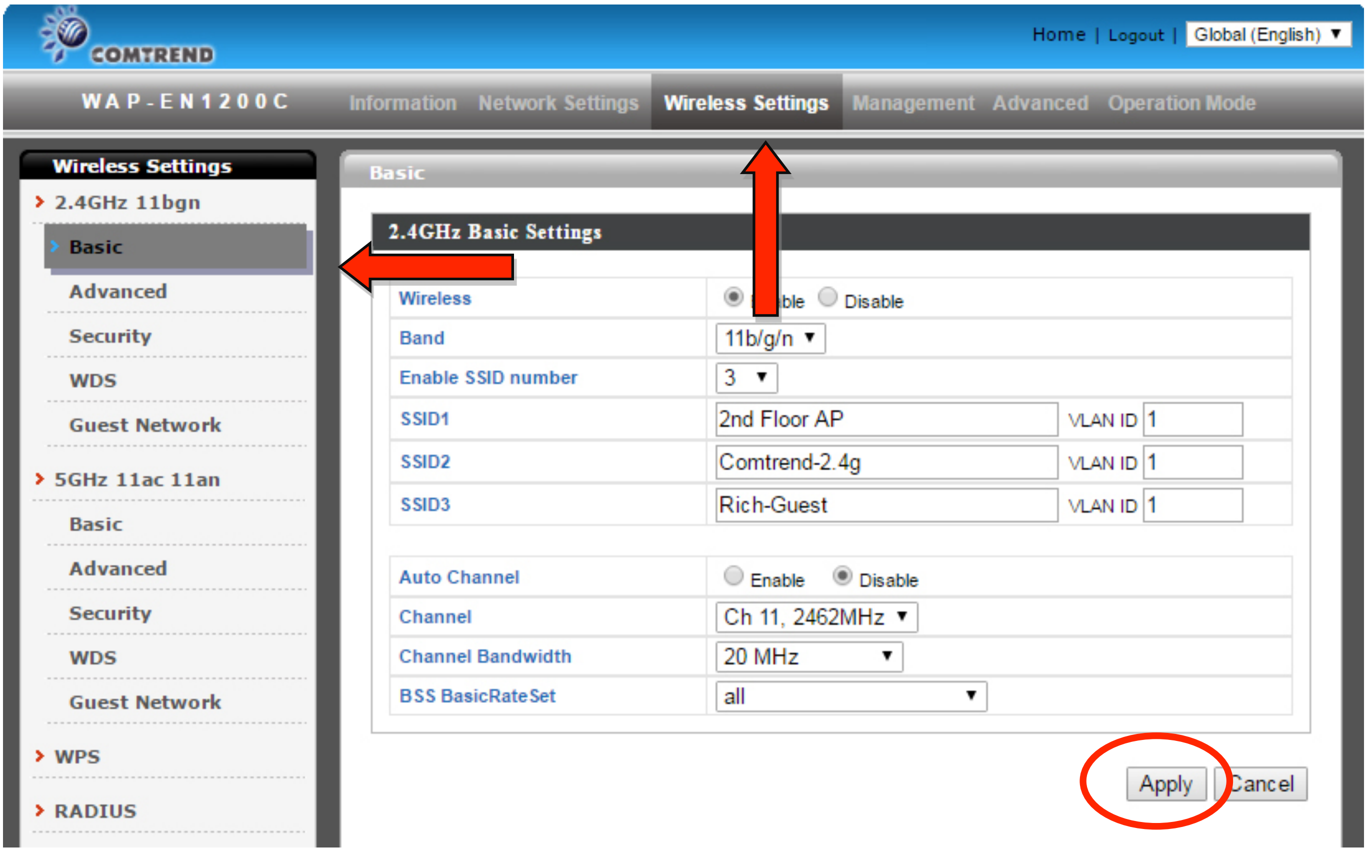


System Information

System

Model	WAP-EN1750W
Product Name	AP801F02F196C4
Uptime	0 day 01:32:52
System Time	2012/01/01 01:32:33
Boot from	Internal memory
Firmware Version	1.3.0
MAC Address	80:1F:02:F1:96:C4
Management VLAN ID	1
IP Address	192.168.10.2
Default Gateway	192.168.10.1
DNS	4.2.2.2 4.2.2.1
DHCP Server	---

5. Use the menu across the top and down the left side to navigate.



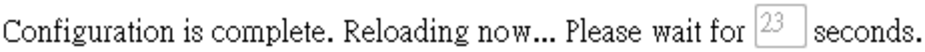
2.4GHz Basic Settings

Wireless	● ble ○ Disable		
Band	11b/g/n		
Enable SSID number	3		
SSID1	2nd Floor AP	VLAN ID	1
SSID2	Comtrend-2.4g	VLAN ID	1
SSID3	Rich-Guest	VLAN ID	1

Auto Channel	○ Enable ● Disable
Channel	Ch 11, 2462MHz
Channel Bandwidth	20 MHz
BSS BasicRateSet	all

6. Click "Apply" to save changes and reload the access point, or "Cancel" to cancel changes.

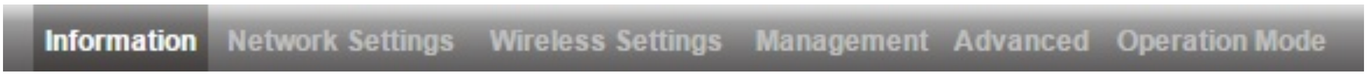
Please wait a few seconds for the access point to reload after you "Apply" changes, as shown below.



Configuration is complete. Reloading now... Please wait for 23 seconds.

7. Refer to the following chapters for full descriptions of the browser-based configuration interface features.

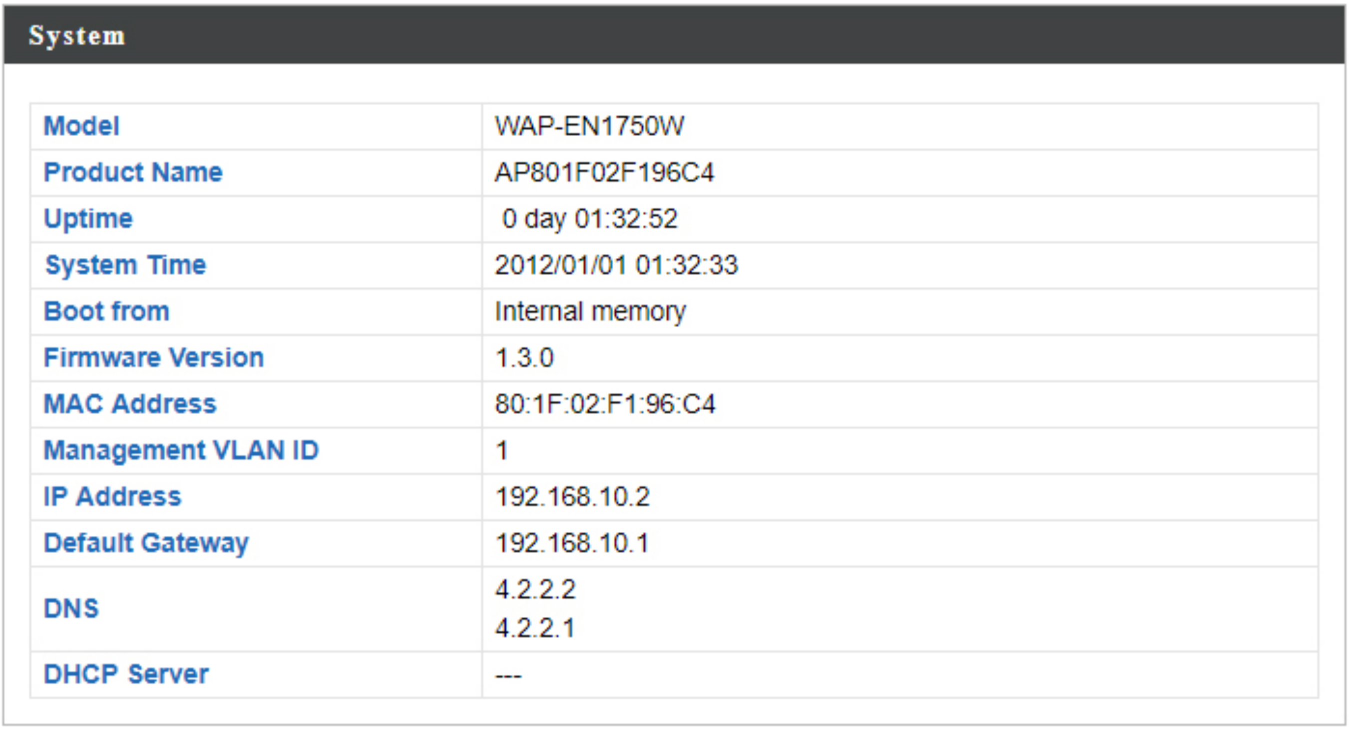
I-1. Information



Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

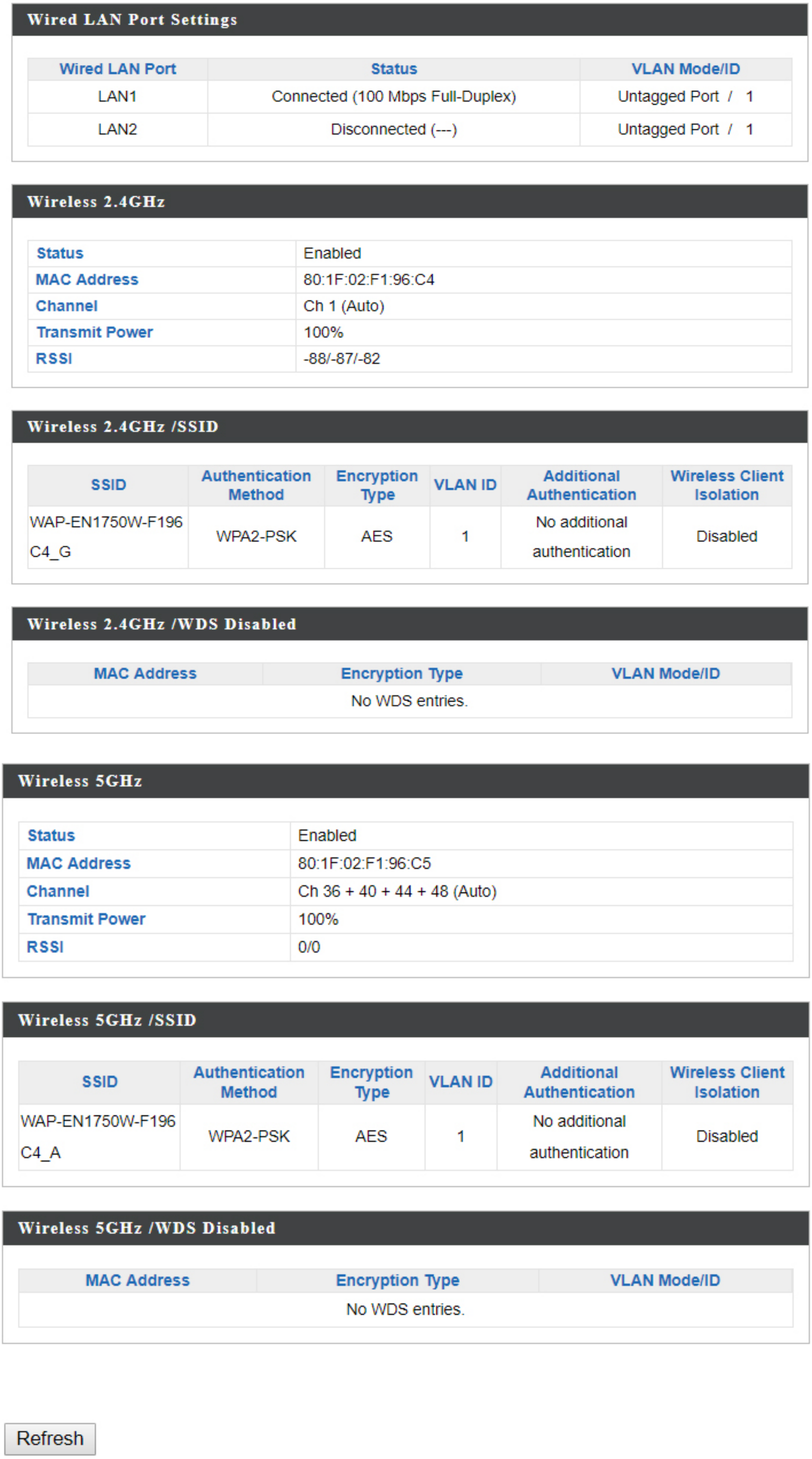
I-1-1. System Information

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



System

Model	WAP-EN1750W
Product Name	AP801F02F196C4
Uptime	0 day 01:32:52
System Time	2012/01/01 01:32:33
Boot from	Internal memory
Firmware Version	1.3.0
MAC Address	80:1F:02:F1:96:C4
Management VLAN ID	1
IP Address	192.168.10.2
Default Gateway	192.168.10.1
DNS	4.2.2.2 4.2.2.1
DHCP Server	---



Wired LAN Port Settings

Wired LAN Port	Status	VLAN Mode/ID
LAN1	Connected (100 Mbps Full-Duplex)	Untagged Port / 1
LAN2	Disconnected (---)	Untagged Port / 1

Wireless 2.4GHz

Status	Enabled
MAC Address	80:1F:02:F1:96:C4
Channel	Ch 1 (Auto)
Transmit Power	100%
RSSI	-88/-87/-82

Wireless 2.4GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
WAP-EN1750W-F196C4_G	WPA2-PSK	AES	1	No additional authentication	Disabled

Wireless 2.4GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
	No WDS entries.	

Wireless 5GHz

Status	Enabled
MAC Address	80:1F:02:F1:96:C5
Channel	Ch 36 + 40 + 44 + 48 (Auto)
Transmit Power	100%
RSSI	0/0

Wireless 5GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
WAP-EN1750W-F196C4_A	WPA2-PSK	AES	1	No additional authentication	Disabled

Wireless 5GHz /WDS Disabled

MAC Address	Encryption Type	VLAN Mode/ID
	No WDS entries.	

System	
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
System Time	Displays the System Time of the Device
Boot From	Displays information for the booted hardware
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 Settings	
Wired LAN Port	Specifies which LAN port
Status	Displays the status of the LAN port (connected or disconnected)
VLAN Mode/ID	Displays the VLAN mode (tagged or untagged) and VLAN ID for the LAN port. See **I-2-3. VLAN**

Wireless 2.4GHz (5GHz)	
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 transmit power level as a percentage
RSSI	Displays Receiver Signal Strength Indicator

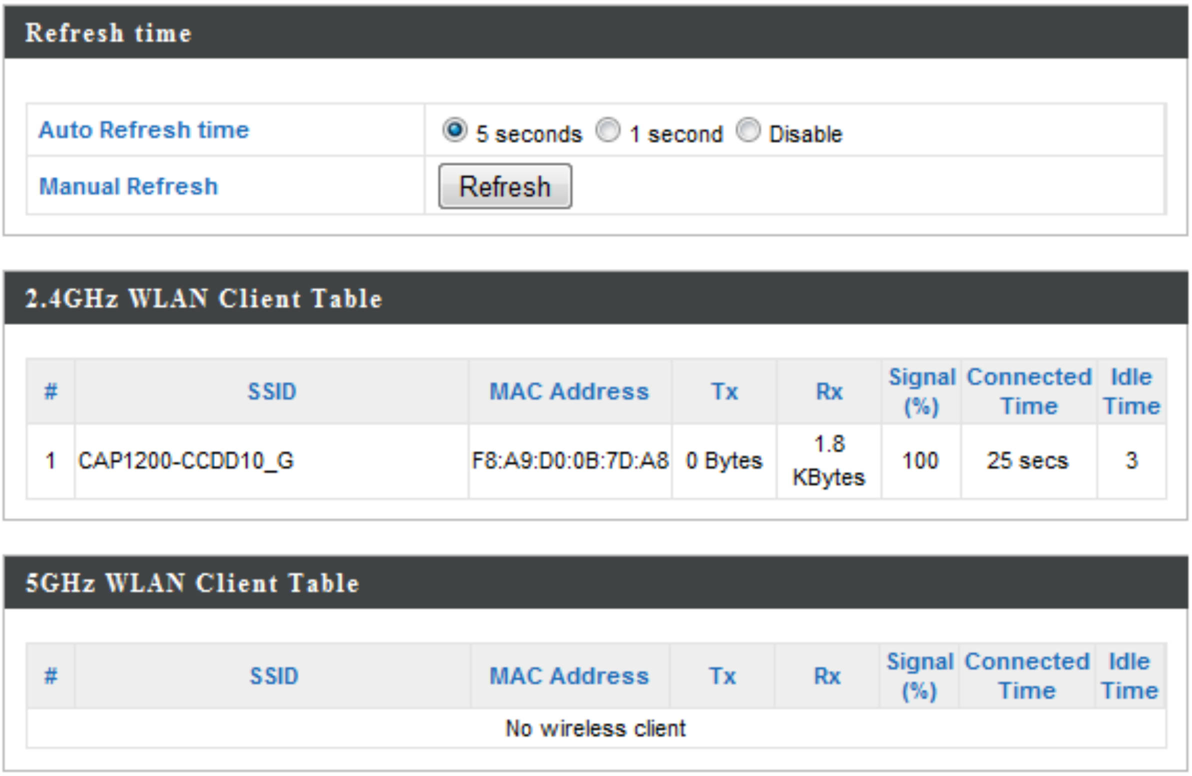
Wireless 2.4GHz (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency
Authentication Method	Displays the authentication method for the specified SSID. See **I-3. Wireless Settings**
Encryption Type	Displays the encryption type for the specified SSID. See **I-3. Wireless Settings**
VLAN ID	Displays the VLAN ID for the specified SSID. See **I-2-3. VLAN**
Additional Authentication	Displays the additional authentication type for the specified SSID. See **I-3. Wireless Settings**
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID. See **I-2-3. VLAN**

Wireless 2.4GHz (5GHz) / WDS Status	
MAC Address	Displays the peer access point’s MAC address
Encryption Type	Displays the encryption type for the specified WDS. See **I-3-1-4. WDS**
VLAN Mode/ID	Displays the VLAN ID for the specified WDS. See **I-3-1-4. WDS**

Refresh	Click to refresh all information

I-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	● 5 seconds ○ 1 second ○ Disable
Manual Refresh	Refresh

2.4GHz WLAN Client Table

#	SSID	MAC Address	Tx	Rx	Signal (%)	Connected Time	Idle Time
1	CAP1200-CCDD10_G	F8:A9:D0:0B:7D:A8	0 Bytes	1.8 KBytes	100	25 secs	3

5GHz WLAN Client Table

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

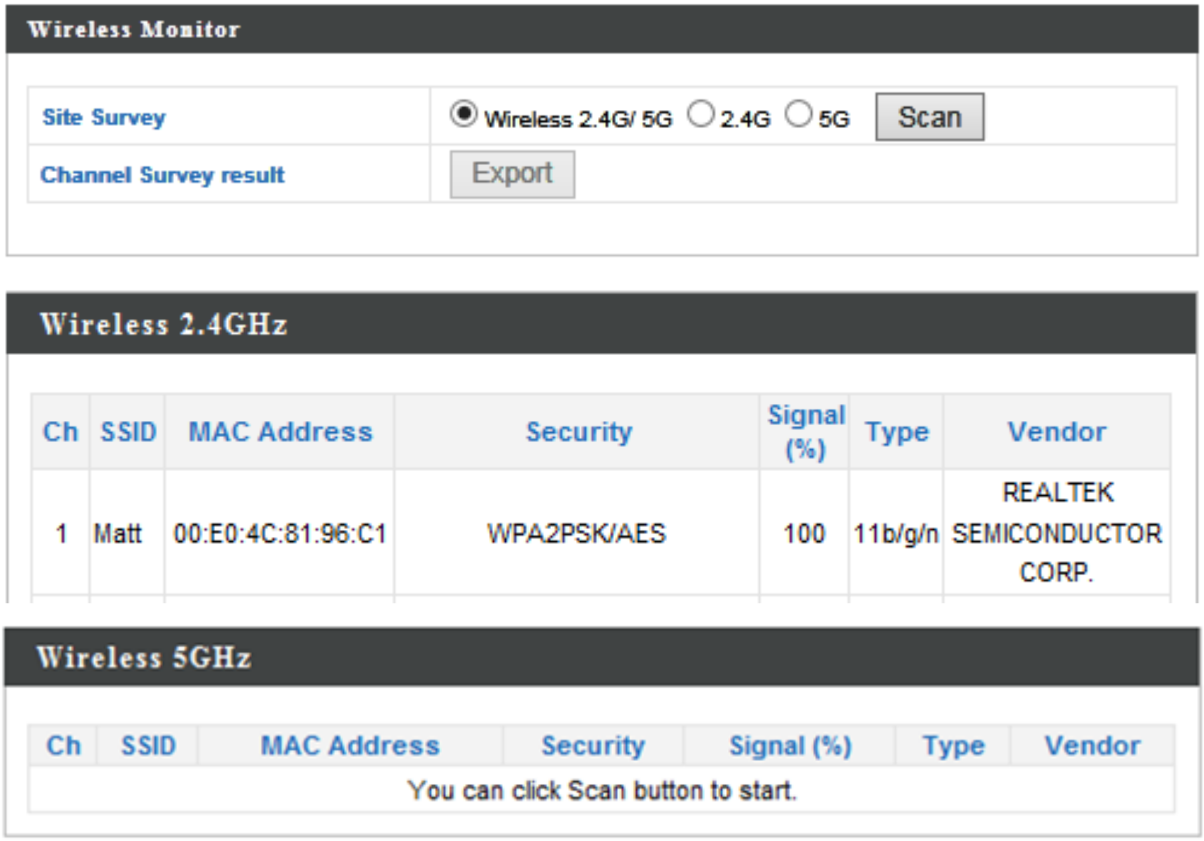
Refresh time	
Auto Refresh Time	Select a time interval for the client table list to automatically refresh
Manual Refresh	Click refresh to manually refresh the client table

2.4GHz (5GHz) WLAN Client Table	
SSID	Displays the SSID that 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

I-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.



Wireless Monitor

Site Survey	● Wireless 2.4G/ 5G ○ 2.4G ○ 5G Scan
Channel Survey result	Export

Wireless 2.4GHz

Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
1	Matt	00:E0:4C:81:96:C1	WPA2PSK/AES	100	11b/g/n	REALTEK SEMICONDUCTOR CORP.

Wireless 5GHz

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

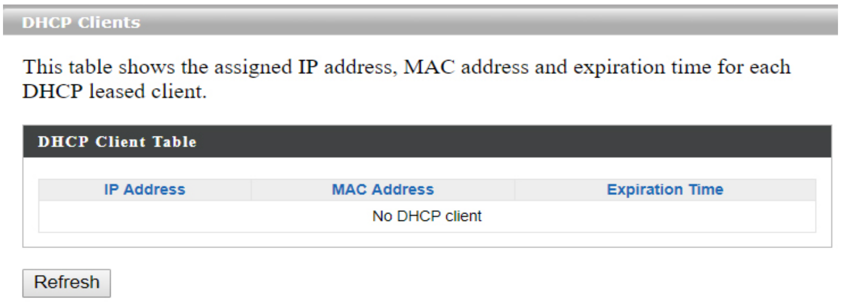
Wireless Monitor	
Site Survey	Select which frequency (or both) to scan, and click “Scan” to begin
Channel Survey Result	After a scan is complete, click “Export” to save the results to local storage

Site Survey Results	
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

I-1-4. DHCP Clients

Displays the assigned IP Address, MAC address and DHCP Lease expiration time for each DHCP leased client.



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

DHCP Client Table

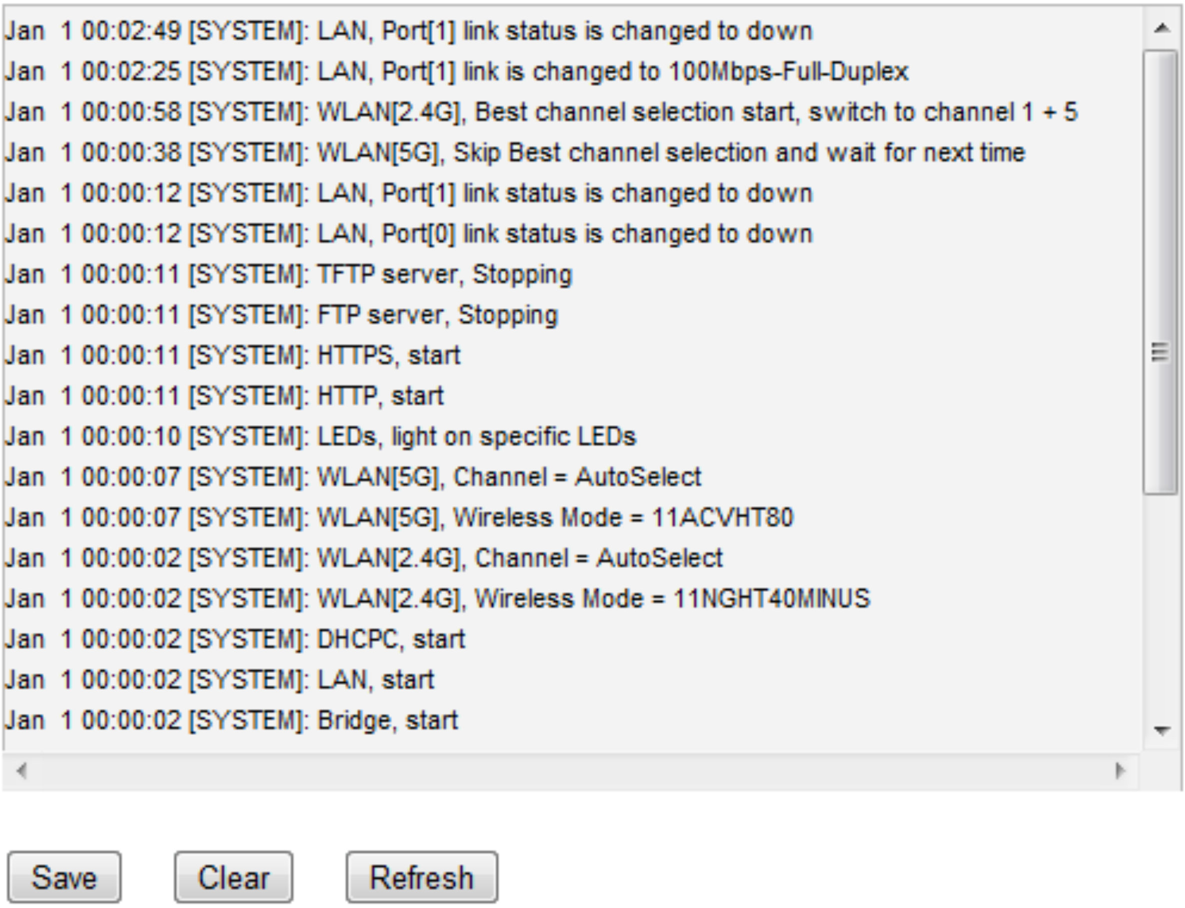
IP Address	MAC Address	Expiration Time
No DHCP client		

DHCP Client Table	
IP Address	IP Address assigned to the connected client device.
MAC Address	MAC Address of the connected client device
Expiration Time	Lease expiration time of the connected client device

I-1-5. Log

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

When the log is full, old entries are overwritten.



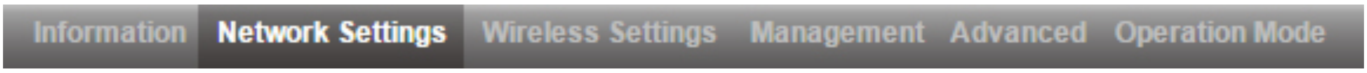
```
Jan  1 00:02:49 [SYSTEM]: LAN, Port[1] link status is changed to down
Jan  1 00:02:25 [SYSTEM]: LAN, Port[1] link is changed to 100Mbps-Full-Duplex
Jan  1 00:00:58 [SYSTEM]: WLAN[2.4G], Best channel selection start, switch to channel 1 + 5
Jan  1 00:00:38 [SYSTEM]: WLAN[5G], Skip Best channel selection and wait for next time
Jan  1 00:00:12 [SYSTEM]: LAN, Port[1] link status is changed to down
Jan  1 00:00:12 [SYSTEM]: LAN, Port[0] link status is changed to down
Jan  1 00:00:11 [SYSTEM]: TFTP server, Stopping
Jan  1 00:00:11 [SYSTEM]: FTP server, Stopping
Jan  1 00:00:11 [SYSTEM]: HTTPS, start
Jan  1 00:00:11 [SYSTEM]: HTTP, start
Jan  1 00:00:10 [SYSTEM]: LEDs, light on specific LEDs
Jan  1 00:00:07 [SYSTEM]: WLAN[5G], Channel = AutoSelect
Jan  1 00:00:07 [SYSTEM]: WLAN[5G], Wireless Mode = 11ACVHT80
Jan  1 00:00:02 [SYSTEM]: WLAN[2.4G], Channel = AutoSelect
Jan  1 00:00:02 [SYSTEM]: WLAN[2.4G], Wireless Mode = 11NGHT40MINUS
Jan  1 00:00:02 [SYSTEM]: DHCPC, start
Jan  1 00:00:02 [SYSTEM]: LAN, start
Jan  1 00:00:02 [SYSTEM]: Bridge, start
```

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

The following information/events are recorded by the log:

- **Wireless Client**
  Connected & disconnected
  Key exchange success & fail
- **Authentication**
  Authentication fail or successful
- **Association**
  Success or fail
- **WPS**
  M1 - M8 messages
  WPS success
- **Change Settings**
- **System Boot**
  Displays current model name
- **NTP Client**
- **Wired Link**
  LAN Port link status and speed status
- **Proxy ARP**
  Proxy ARP module start & stop
- **Bridge**
  Bridge start & stop.
- **SNMP**
  SNMP server start & stop
- **HTTP**
  HTTP start & stop
- **HTTPS**
  HTTPS start & stop.
- **SSH**
  SSH-client server start & stop
- **Telnet**
  Telnet-client server start or stop
- **WLAN (2.4G)**
  WLAN (2.4G] channel status and country/region status
- **WLAN (5G)**
  WLAN (5G) channel status and country/region status
- **ADT**

I-2. Network Settings

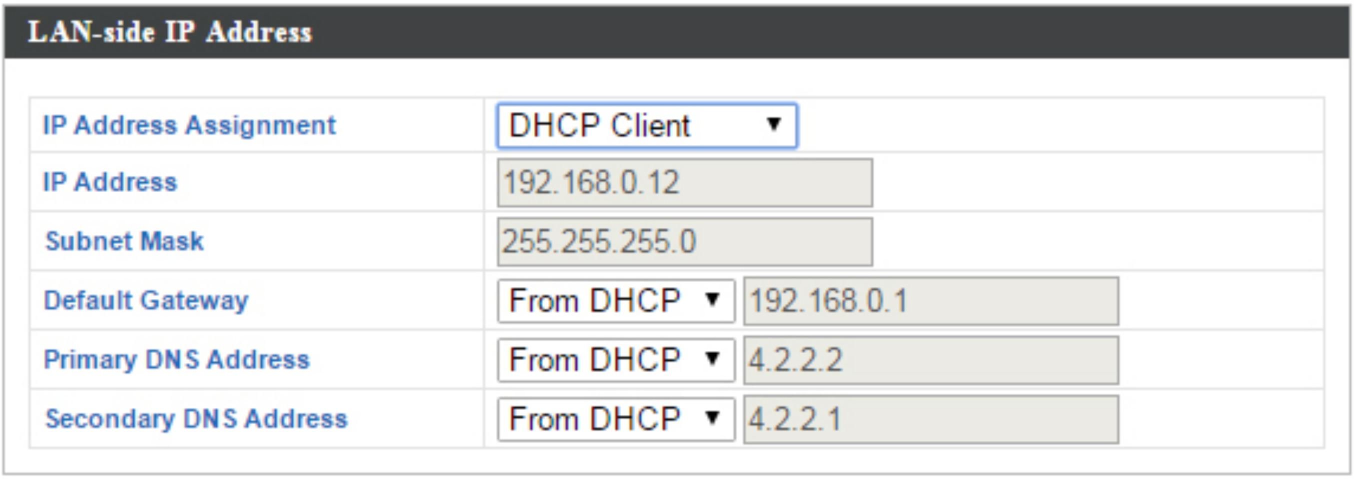


Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

I-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.

The access point's default IP address is 192.168.2.2 or 192.168.2.1.



LAN-side IP Address

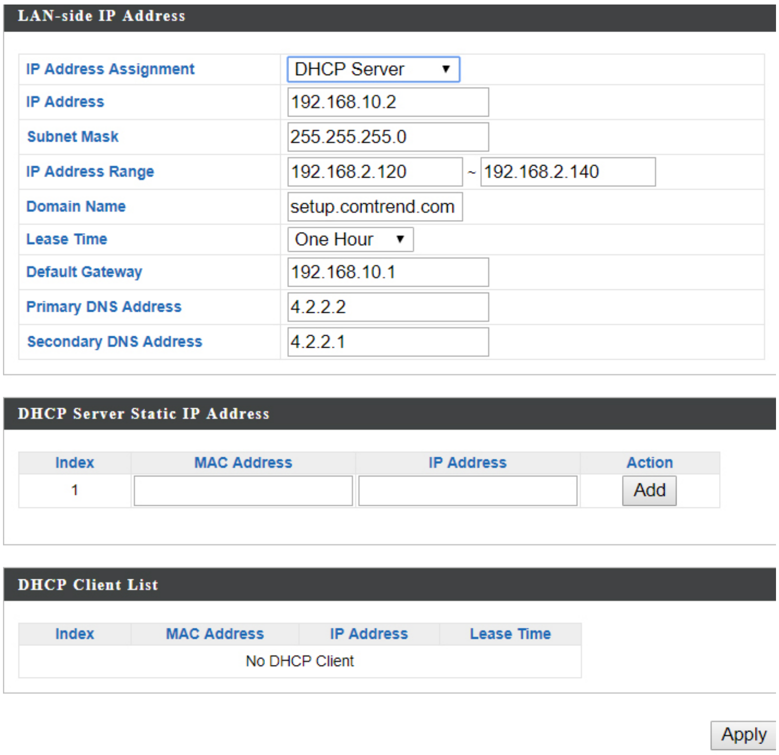
IP Address Assignment	DHCP Client ▾	
IP Address	192.168.0.12	
Subnet Mask	255.255.255.0	
Default Gateway	From DHCP ▾	192.168.0.1
Primary DNS Address	From DHCP ▾	4.2.2.2
Secondary DNS Address	From DHCP ▾	4.2.2.1

LAN-side IP Address (DHCP Client)	
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 "Static IP" to manually specify a static/fixed IP address for your access point (below)
IP Address	Specify the IP address here. This IP address will be assigned to your access point and will

	replace the default IP address
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank

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

Primary Address	DHCP users can select “From DHCP” to get primary DNS server’s IP address from DHCP or “User-Defined” to manually enter a value. For static IP users, the default value is blank
Secondary Address	Users can manually enter a value when DNS server’s primary address is set to “User-Defined”



LAN-side IP Address

IP Address Assignment	DHCP Server ▾
IP Address	192.168.10.2
Subnet Mask	255.255.255.0
IP Address Range	192.168.2.120 ~ 192.168.2.140
Domain Name	setup.comtrend.com
Lease Time	One Hour ▾
Default Gateway	192.168.10.1
Primary DNS Address	4.2.2.2
Secondary DNS Address	4.2.2.1

DHCP Server Static IP Address

Index	MAC Address	IP Address	Action
1			Add

DHCP Client List

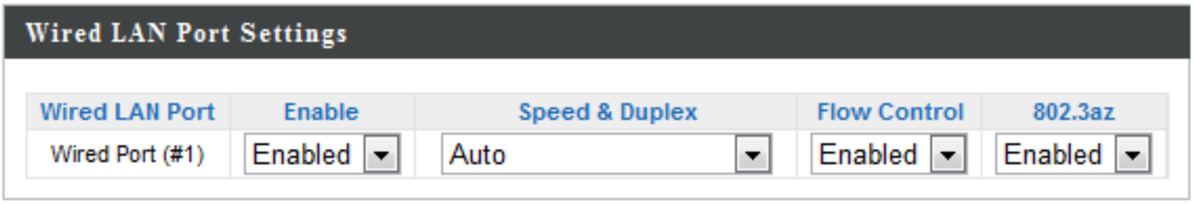
Index	MAC Address	IP Address	Lease Time
No DHCP Client			

LAN-side IP Address (DHCP Server)	
IP Address Assignment	Select “DHCP Server” for your access point to function as a DHCP Server.
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
IP Address Range	Specify the starting and ending IP Address for the DHCP Address Pool.
Domain Name	Provide a domain name for the DHCP Server here.
Lease Time	Value indicates how long the DHCP Server will lease the IP Address to the connected device.
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 Address	Indicates the Primary DNS Server IP Address that will be provided by the DHCP Server to connected client devices.
Secondary DNS Address	Indicates the Secondary DNS Server IP Address that will be provided by the DHCP Server to connected client devices.
DHCP Server Static IP Address	
Index	DHCP Reservation Index Number
MAC Address	MAC Address of client device for reservation
IP Address	IP Address reserved for client device
DHCP Client List	
Index	Client List Index Number
MAC Address	MAC Address of the client device
IP Address	IP Address assigned to the client device
Lease Time	Lease Time for the client device

I-2-2. LAN Port

The “LAN Port” page allows you to configure the settings for your access point’s wired LAN (Ethernet) port.



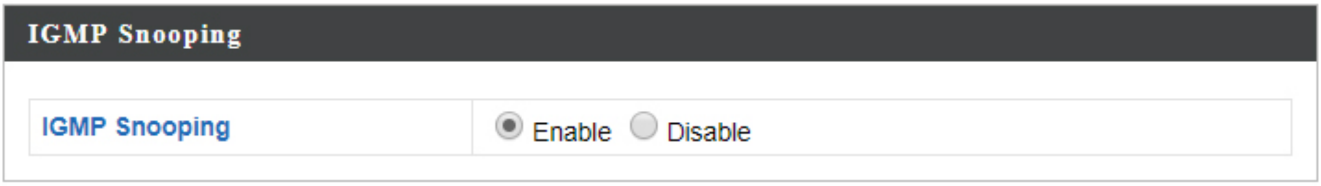
Wired LAN Port Settings

Wired LAN Port	Enable	Speed & Duplex	Flow Control	802.3az
Wired Port (#1)	Enabled	Auto	Enabled	Enabled

Wired LAN Port	Identifies LAN port 1
Enable	Enable/disable LAN port
Speed & Duplex	Select a speed & duplex type for 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 that disables unused interfaces to reduce power usage

I-2-3. IGMP Snooping

Enables/Disables IGMP Snooping.

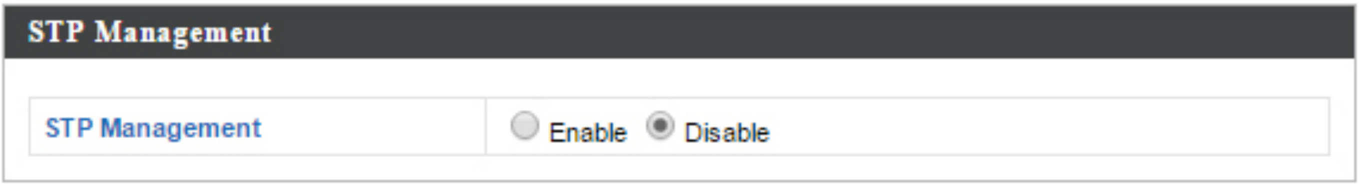


IGMP Snooping

IGMP Snooping ● Enable ○ Disable

I-2-4. STP Management

Spanning Tree Protocol is used to prevent network loops, thus allowing redundant network paths.



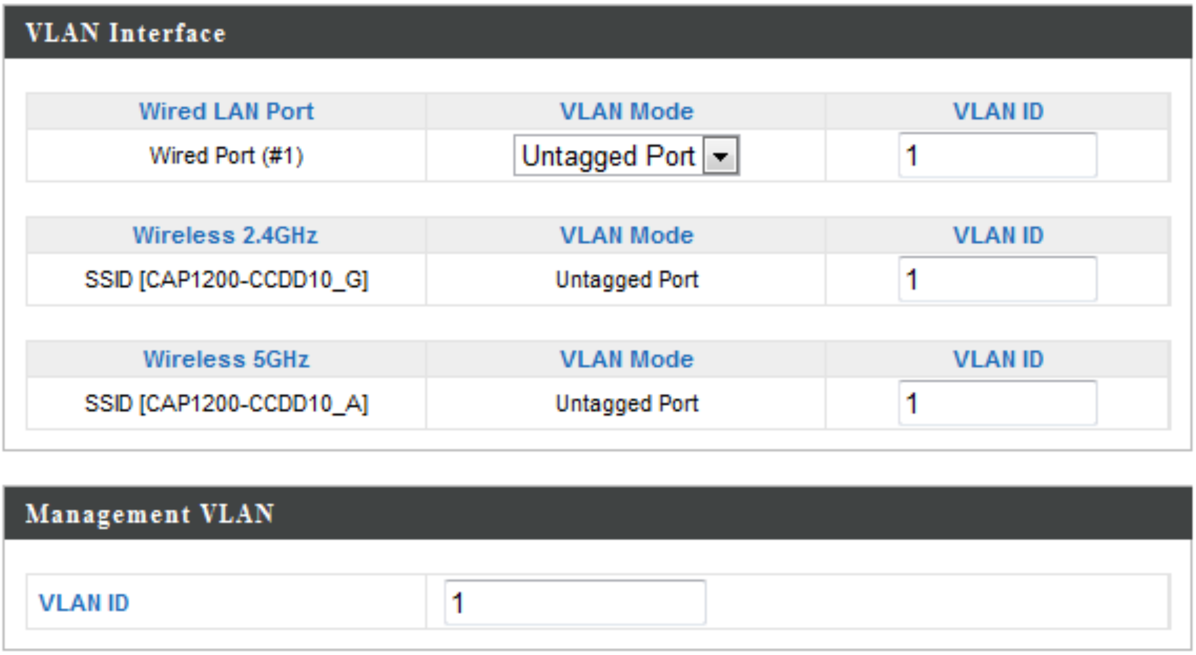
STP Management

STP Management	○ Enable ● Disable

I-2-5. 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 – 4094 are supported.

⚠ ***VLAN IDs in the range 1 – 4094 are supported.***



VLAN Interface

Wired LAN Port	VLAN Mode	VLAN ID
Wired Port (#1)	Untagged Port ▾	1

Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [CAP1200-CCDD10_G]	Untagged Port	1

Wireless 5GHz	VLAN Mode	VLAN ID
SSID [CAP1200-CCDD10_A]	Untagged Port	1

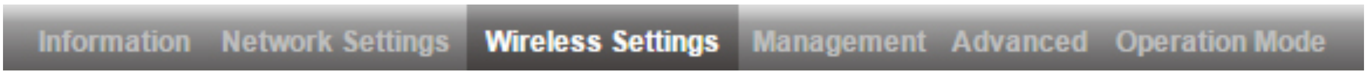
Management VLAN

VLAN ID	1

VLAN Interface	
Wired LAN Port/Wireless	Identifies LAN port 1 and wireless SSIDs (2.4GHz or 5GHz)
VLAN Mode	Select “Tagged Port” or “Untagged Port” for LAN interface
VLAN ID	Set a VLAN ID for specified interface, if “Untagged Port” is selected

Management VLAN	
VLAN ID	Specify the VLAN ID of the management VLAN. Only the hosts belonging to the same VLAN can manage the device

I-3. Wireless Settings



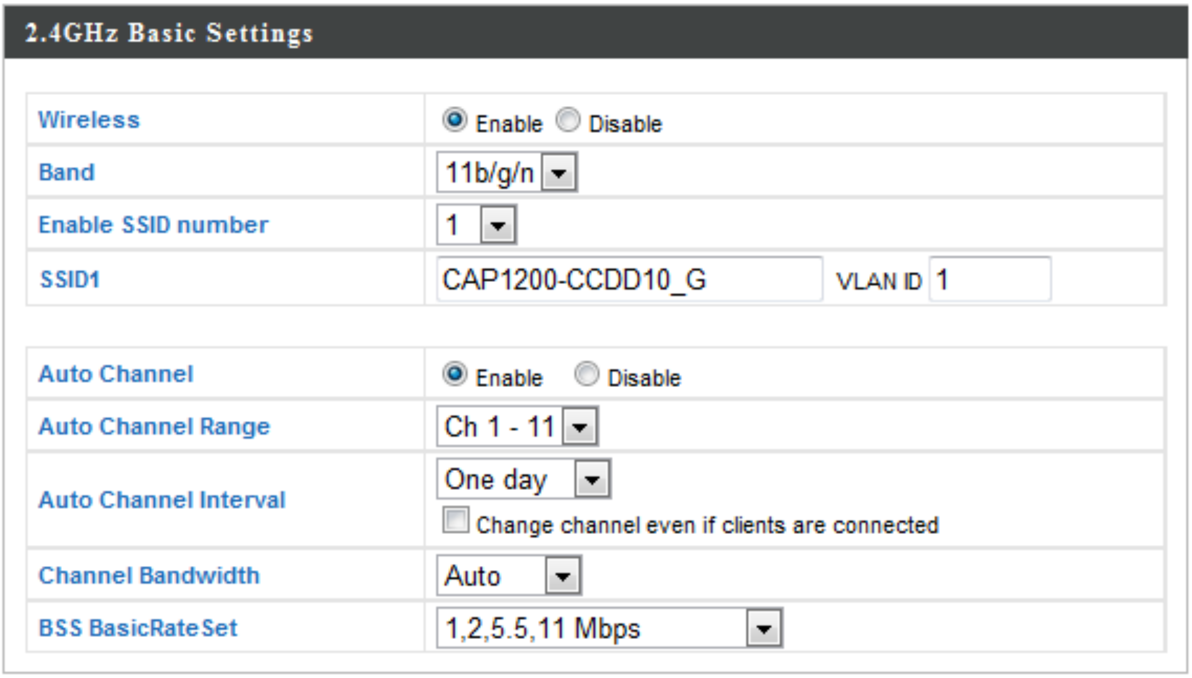
Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

I-3-1. 2.4GHz 11bgn

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.

I-3-1-1.Basic

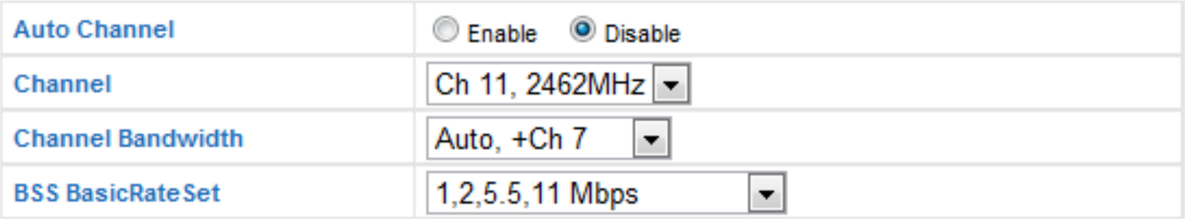
The “Basic” screen displays basic settings for your access point’s 2.4GHz Wi-Fi network (s).



2.4GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11b/g/n
Enable SSID number	1
SSID1	CAP1200-CCDD10_G VLAN ID 1

Auto Channel	● Enable ○ Disable
Auto Channel Range	Ch 1 - 11
Auto Channel Interval	One day □ Change channel even if clients are connected
Channel Bandwidth	Auto
BSS BasicRateSet	1,2,5.5,11 Mbps



Auto Channel	○ Enable ● Disable
Channel	Ch 11, 2462MHz
Channel Bandwidth	Auto, +Ch 7
BSS BasicRateSet	1,2,5.5,11 Mbps

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 & 802.11n can be selected
Enable SSID Number	Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. A maximum of 16 can be enabled
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters
VLAN ID	Specify a VLAN ID for each SSID
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point’s 2.4GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the “Change channel even if clients are connected” box according to your preference
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (higher performance but potentially higher interference) or 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

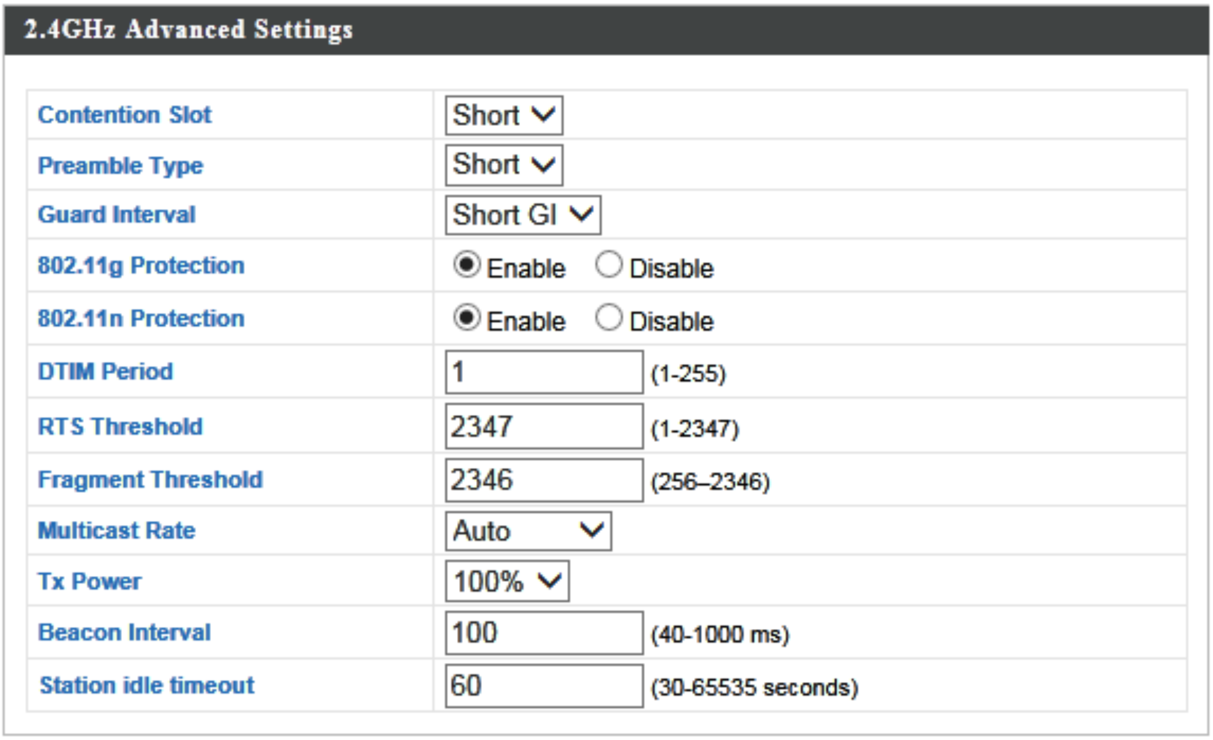
When auto channel is disabled, select a wireless channel manually:

Channel	Select a wireless channel from 1 – 11 (1-13).
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (higher performance but potentially higher interference) or 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

I-3-1-2.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.

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



2.4GHz Advanced Settings

Contention Slot	Short
Preamble Type	Short
Guard Interval	Short GI
802.11g Protection	● Enable ○ Disable
802.11n Protection	● Enable ○ Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256–2346)
Multicast Rate	Auto
Tx Power	100%
Beacon Interval	100 (40-1000 ms)
Station idle timeout	60 (30-65535 seconds)

Contention Slot	Select "Short" or "Long" – this value is used for contention windows in WMM (see **I-3-6. WMM**)
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication 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 Preamble"
Guard Interval	Set the guard interval. A shorter interval can improve performance

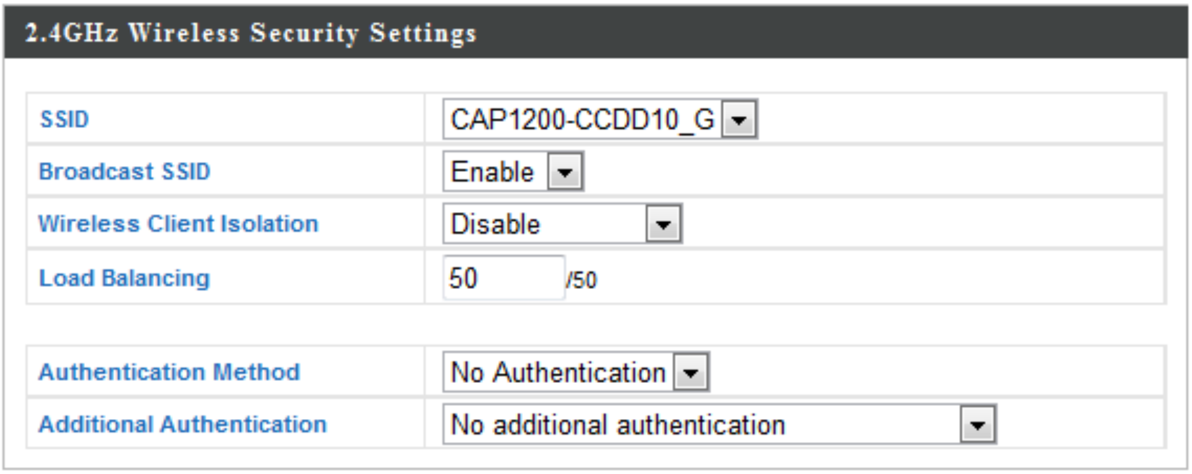
802.11g Protection	Enable/disable 802.11g protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
802.11n Protection	Enable/disable 802.11n protection, 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 interval for keep alive messages from the access point to a wireless client to verify if the station is still alive/active

I-3-1-3. 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.

⚠ ***It's essential to configure wireless security in order to prevent unauthorised access to your network.***

⚠ ***Select hard-to-guess passwords which include combinations of numbers, letters and symbols, and change your password regularly.***



2.4GHz Wireless Security Settings

SSID	CAP1200-CCDD10_G ▾
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
Load Balancing	50 /50

Authentication Method	No Authentication ▾
Additional Authentication	No additional authentication ▾

SSID Selection	Select which SSID to configure security settings for
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50)
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method
Additional Authentication	Select an additional authentication method from the drop down menu and refer to the information below (**I-3-1-3-6.**) appropriate for your method

I-3-1-3-1. 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.

I-3-1-3-2. WEP

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

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 that is the default key
Encryption Key 1 – 4	Enter your encryption key/password according to the format you selected above

I-3-1-3-3. IEEE802.1x/EAP

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

I-3-1-3-4. WPA-PSK

WPA-PSK is a secure wireless encryption type with strong data protection and user authentication, utilizing 128-bit encryption keys.

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	Choose from "Passphrase" (8 – 63

Type	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

I-3-1-3-5. WPA-EAP

WPA Type	Select from WPA/WPA2 Mixed Mode-EAP, WPA2-EAP or WPA-EAP
Encryption	Select “TKIP/AES Mixed Mode” or “AES” encryption type
Key Renewal Interval	Specify a frequency for key renewal in minutes

WPA-EAP must be disabled to use MAC-RADIUS authentication.

I-3-1-3-6. Additional Authentication

Additional wireless authentication methods can also be used:

MAC Address Filter
Restrict wireless clients access based on MAC address specified in the MAC filter table.

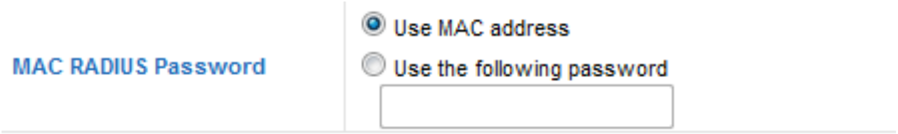
See *I-3-5.MAC Filter* ***to configure MAC filtering.***

MAC Filter & MAC-RADIUS Authentication
Restrict wireless clients access using both of the above MAC filtering & RADIUS authentication methods.

MAC-RADIUS Authentication
Restrict wireless clients access based on MAC address via a RADIUS server, or password authentication via a RADIUS server.

See *I-3-4.RADIUS* ***to configure RADIUS servers.***

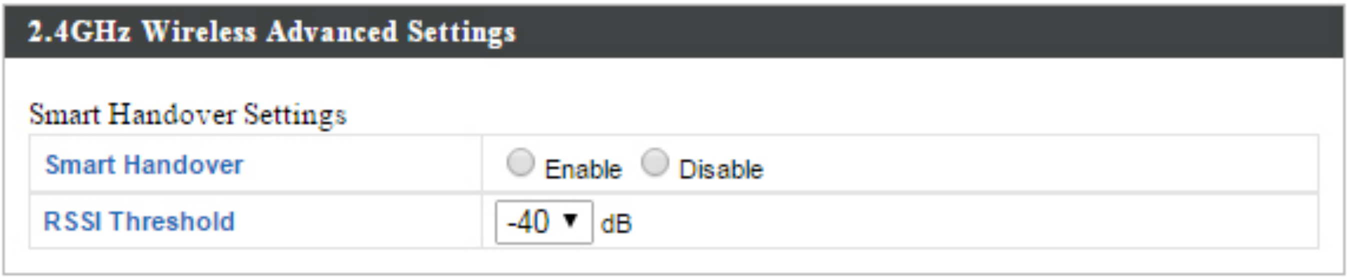
WPS must be disabled to use MAC-RADIUS authentication. See *I-3-3*. ***for WPS settings.***



MAC RADIUS Password	● Use MAC address ○ Use the following password

MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If you select "Use the following password", enter the password in the field below. The password should match the "Shared Secret" used in **I-3-4. RADIUS**.

Smart Handover
Enable Smart Handover to configure an RSSI Threshold. The RSSI Threshold is the signal strength in which a wireless client handoff will occur. The higher the number, the stronger the signal.



2.4GHz Wireless Advanced Settings

Smart Handover Settings

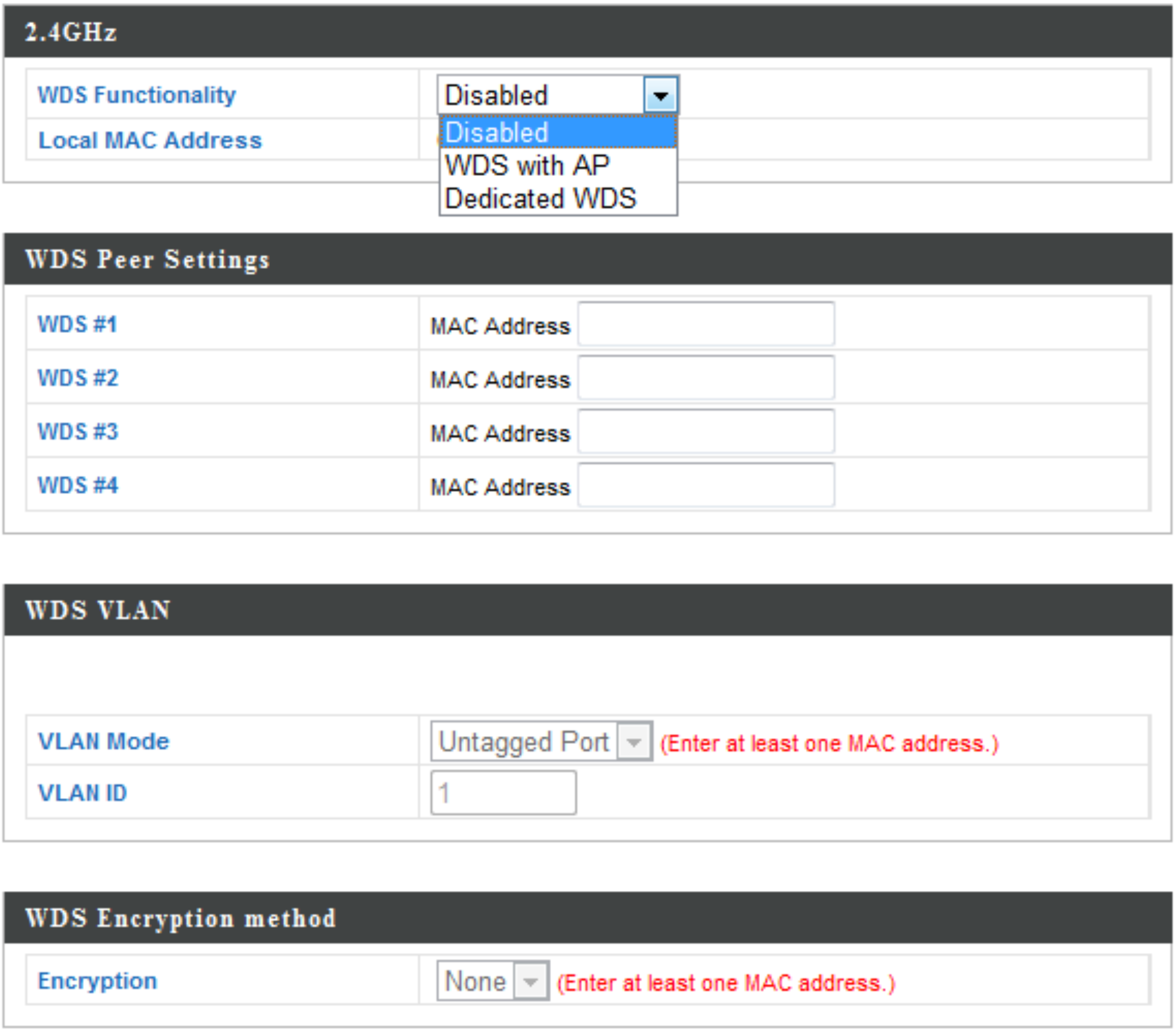
Smart Handover	○ Enable ○ Disable
RSSI Threshold	-40 ▼ dB

I-3-1-4.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.

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



2.4GHz

WDS Functionality	Disabled Disabled WDS with AP Dedicated WDS
Local MAC Address	

WDS Peer Settings

WDS #1	MAC Address
WDS #2	MAC Address
WDS #3	MAC Address
WDS #4	MAC Address

WDS VLAN

VLAN Mode	Untagged Port (Enter at least one MAC address.)
VLAN ID	1

WDS Encryption method

Encryption	None (Enter at least one MAC address.)

2.4GHz	
WDS Functionality	Select "WDS with AP" to use WDS with access point 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 wireless encryption method
Local MAC Address	Displays the MAC address of your access point

WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDS devices you wish to connect

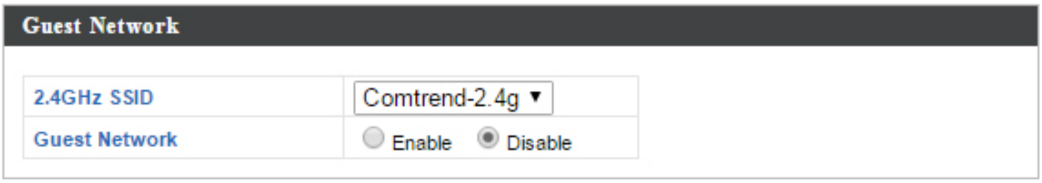
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to "Untagged Port" or "Tagged Port"
VLAN ID	Specify the WDS VLAN ID when "Untagged Port" is selected above

WDS Encryption method	
Encryption	Select whether to use "None" or "AES" encryption and enter a pre-shared key for AES consisting of 8-63 alphanumeric characters

I-3-1-5.Guest Network

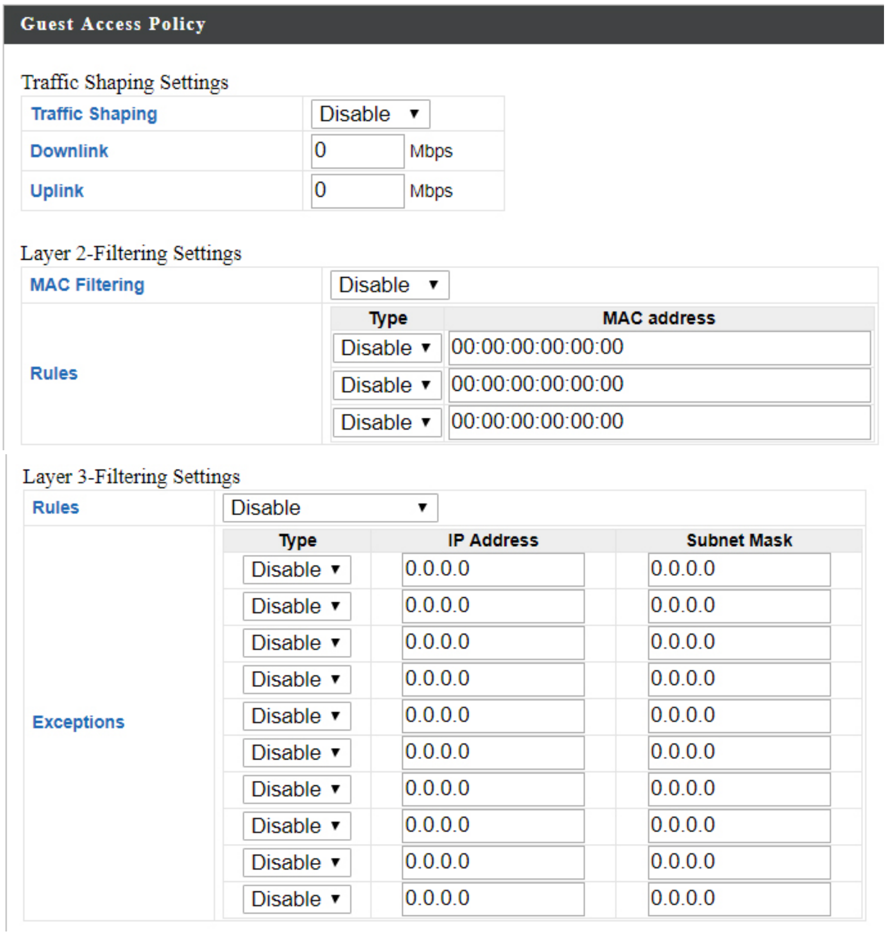
The "Guest Network" page allows you to configure a guest network that will have a Layer-3 IP Filter applied to all traffic passing through the specific SSID.

When using a Guest Network, Traffic Shaping and IP Filter settings will be applied to all traffic passing through the Guest Network SSID.



Guest Network

2.4GHz SSID	Comtrend-2.4g ▼
Guest Network	○ Enable ● Disable



Guest Access Policy

Traffic Shaping Settings

Traffic Shaping	Disable ▾
Downlink	0 Mbps
Uplink	0 Mbps

Layer 2-Filtering Settings

MAC Filtering	Disable ▾	
Rules	Type	MAC address
	Disable ▾	00:00:00:00:00:00
	Disable ▾	00:00:00:00:00:00
	Disable ▾	00:00:00:00:00:00

Layer 3-Filtering Settings

Rules	Disable ▾		
Exceptions	Type	IP Address	Subnet Mask
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0

Guest Network	
2.4GHz SSID	Select the SSID that you want to apply the Guest Network settings to
Guest Network	Enable or Disable Guest Network settings
Guest Access Policy	
Traffic Shaping	Select “Enable” to apply bandwidth limitations on the “Downlink” and “Uplink” performance on the Guest Network
Layer 2-Filtering Settings	
MAC Filtering	Select “Disable”, “Whitelist” or “Blacklist”. Up to 3 MAC Filters are supported
Rules	Select “Disable” or “Enable” to toggle the application of the rule to the MAC Address.
Layer 3-Filtering Settings	
Rules	Select “Disable”, “Deny all by default” or “Allow all by default”. Up to 10 Exceptions are supported

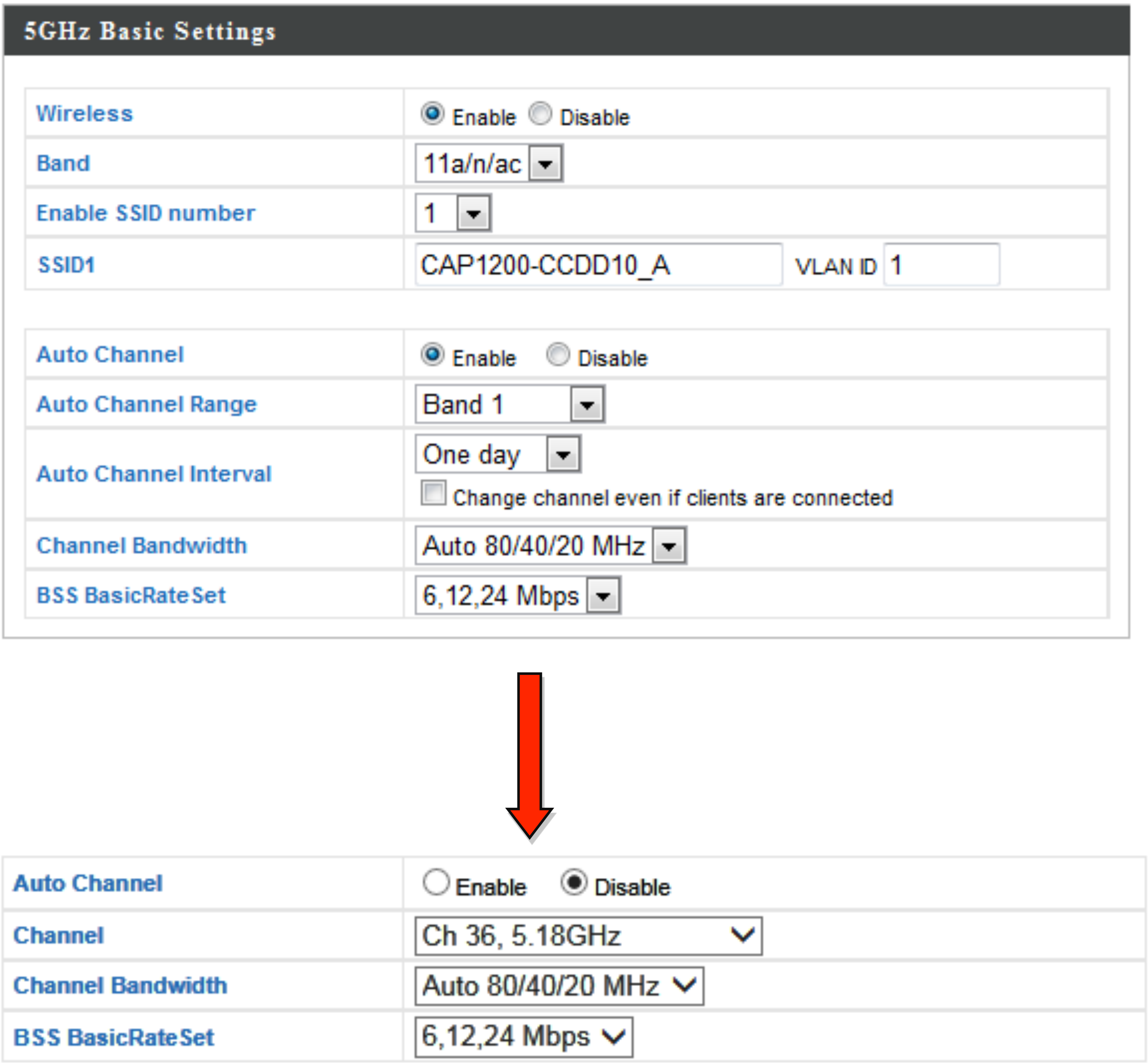
Exceptions	Select “Disable”, “Deny” or “Allow”. Provide a starting IP Address and Subnet Mask to apply to the exception.

I-3-2. 5GHz 11ac 11an

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

I-3-2-1. Basic

The “Basic” screen displays basic settings for your access point’s 5GHz Wi-Fi network (s).



5GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11a/n/ac
Enable SSID number	1
SSID1	CAP1200-CCDD10_A VLAN ID 1
Auto Channel	● Enable ○ Disable
Auto Channel Range	Band 1
Auto Channel Interval	One day □ Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz
BSS BasicRateSet	6,12,24 Mbps

Auto Channel	○ Enable ● Disable
Channel	Ch 36, 5.18GHz
Channel Bandwidth	Auto 80/40/20 MHz
BSS BasicRateSet	6,12,24 Mbps

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 & 802.11ac can be selected
Enable SSID Number	Select how many SSIDs to enable for the 5GHz frequency from the drop down menu. A maximum of 16 can be enabled
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters
VLAN ID	Specify a VLAN ID for each SSID
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 5GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (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

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

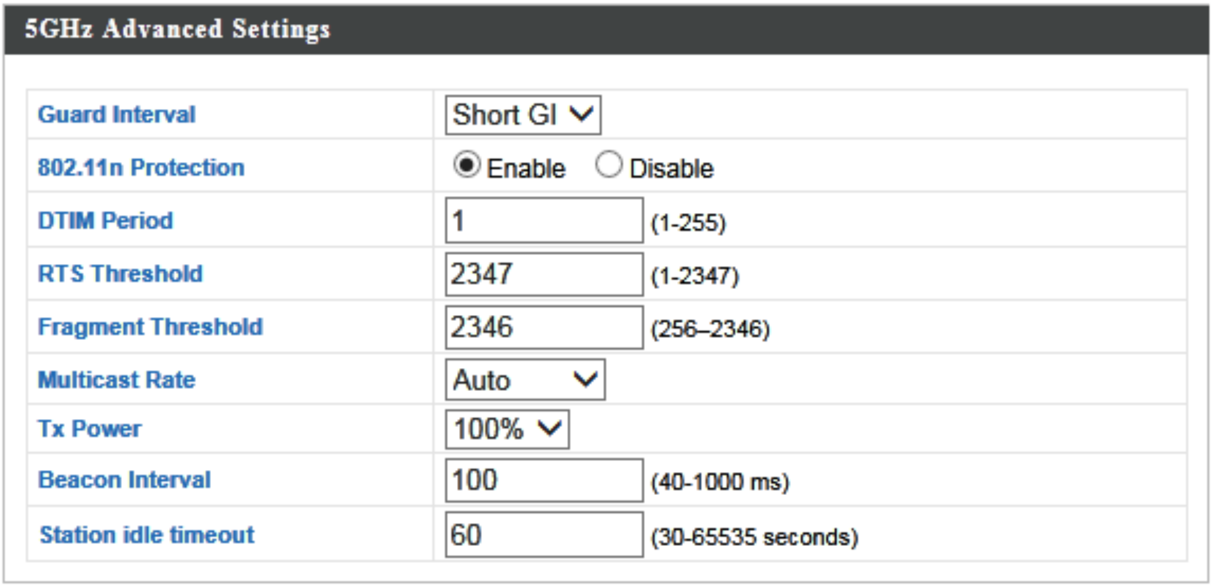
Channel	Select a wireless channel.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (automatically select based on interference level)

BSS Basic Rate Set	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients

I-3-2-2.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.

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



5GHz Advanced Settings

Guard Interval	Short GI
802.11n Protection	● Enable ○ Disable
DTIM Period	1 (1-255)
RTS Threshold	2347 (1-2347)
Fragment Threshold	2346 (256–2346)
Multicast Rate	Auto
Tx Power	100%
Beacon Interval	100 (40-1000 ms)
Station idle timeout	60 (30-65535 seconds)

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

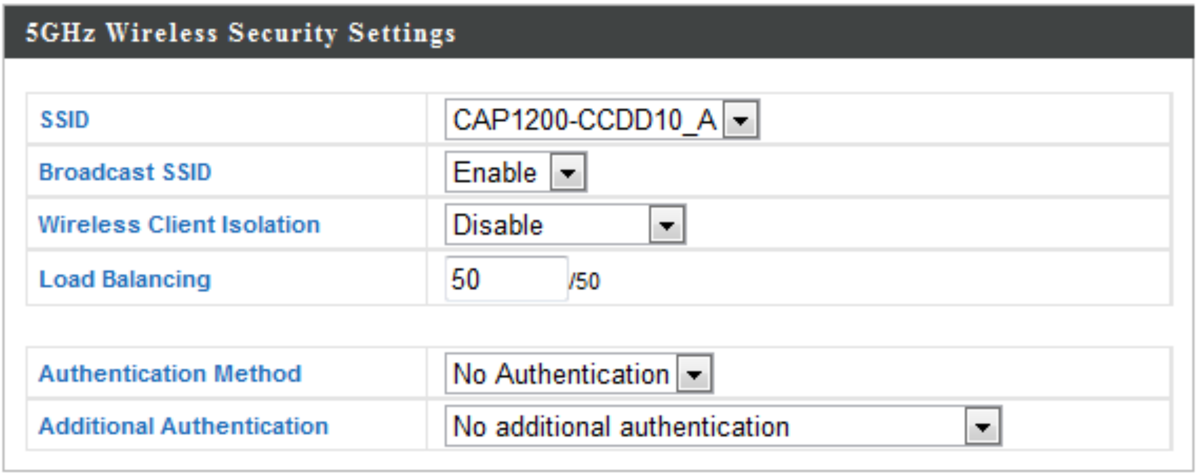
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal
Beacon Interval	Set the beacon interval of the wireless radio. 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

I-3-2-3.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.

It's essential to configure wireless security in order to prevent unauthorised access to your network.

Select hard-to-guess passwords which include combinations of numbers, letters and symbols, and change your password regularly.



5GHz Wireless Security Settings

SSID	CAP1200-CCDD10_A
Broadcast SSID	Enable
Wireless Client Isolation	Disable
Load Balancing	50 /50
Authentication Method	No Authentication
Additional Authentication	No additional authentication

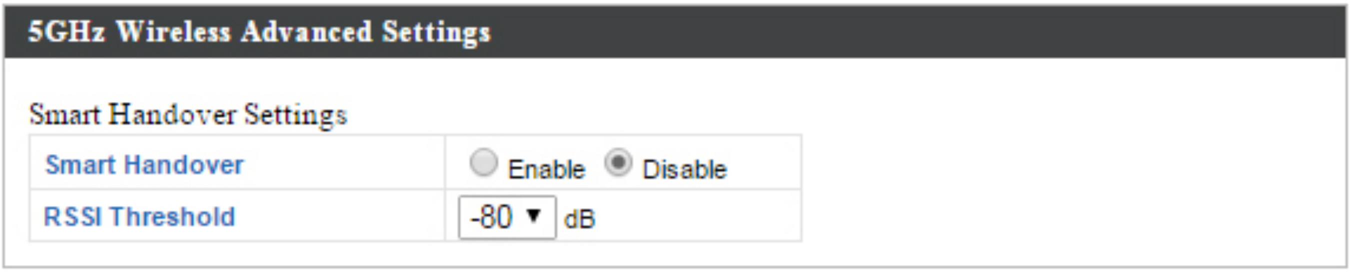
SSID Selection	Select which SSID to configure security settings for
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID

Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50)
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method
Additional Authentication	Select an additional authentication method from the drop down menu and refer to the information below appropriate for your method

Please refer back to **I-3-1-3. Security** for more information on authentication and additional authentication types.

Smart Handover

Enable Smart Handover to configure an RSSI Threshold. The RSSI Threshold is the signal strength in which a wireless client handoff will occur. The higher the number, the stronger the signal.



5GHz Wireless Advanced Settings

Smart Handover Settings

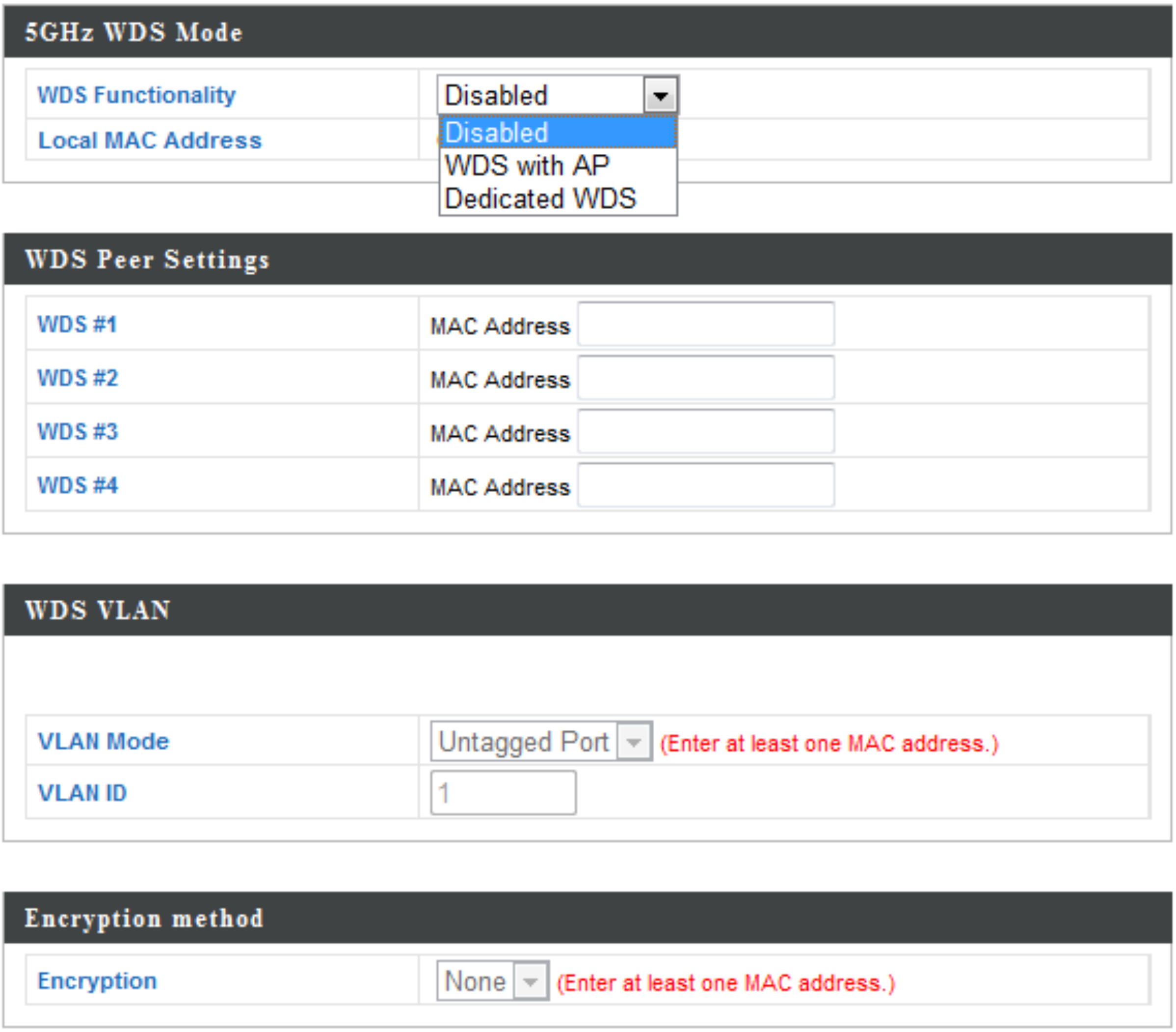
Smart Handover	○ Enable ● Disable
RSSI Threshold	-80 ▼ dB

I-3-2-4.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.***

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



5GHz WDS Mode

WDS Functionality	Disabled
Local MAC Address	

WDS Peer Settings

WDS #1	MAC Address	
WDS #2	MAC Address	
WDS #3	MAC Address	
WDS #4	MAC Address	

WDS VLAN

VLAN Mode	Untagged Port (Enter at least one MAC address.)
VLAN ID	1

Encryption method

Encryption	None (Enter at least one MAC address.)

5GHz WDS Mode

WDS Functionality	Select “WDS with AP” to use WDS with access point 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 wireless encryption method
Local MAC Address	Displays the MAC address of your access point

WDS Peer Settings	
WDS #	Enter the MAC address for up to four other WDA devices you wish to connect

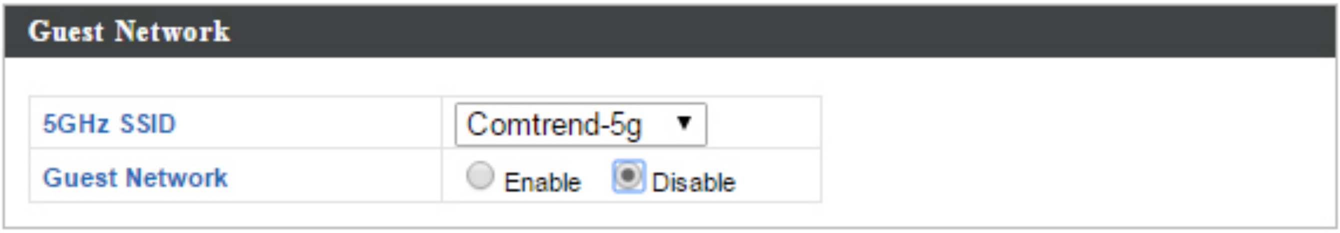
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above

WDS Encryption	
Encryption	Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES with 8-63 alphanumeric characters

I-3-2-5.Guest Network

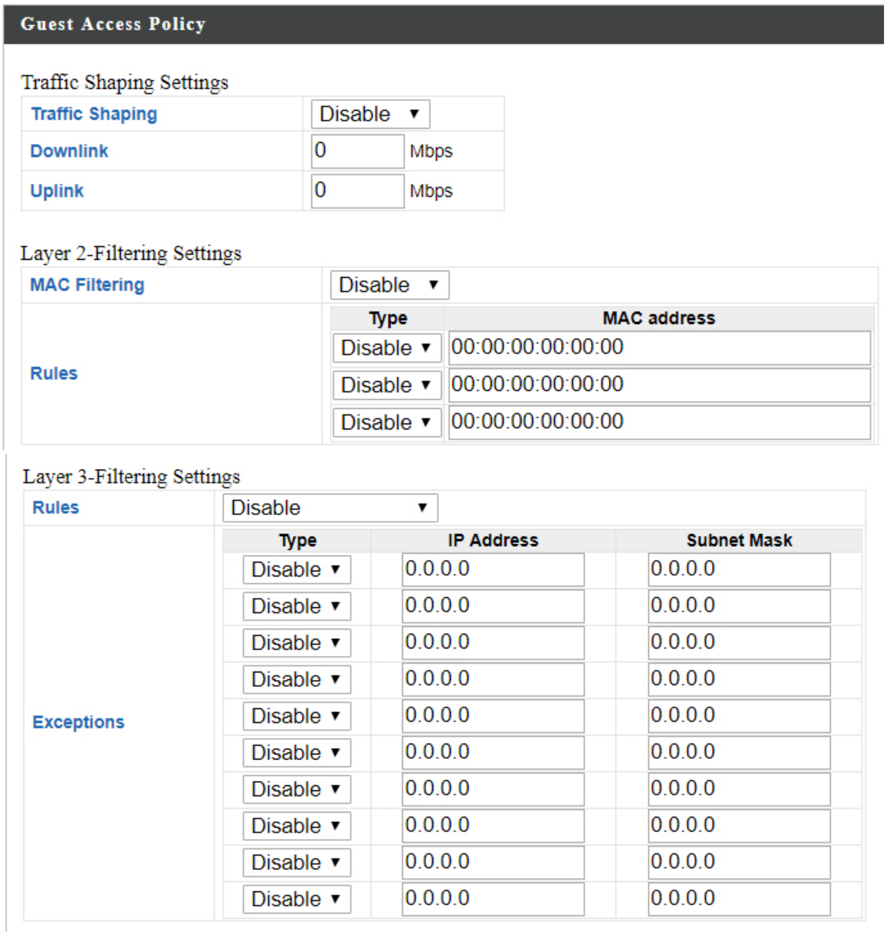
The “Guest Network” page allows you to configure a guest network that will have a Layer-3 IP Filter applied to all traffic passing through the specific SSID.

When using a Guest Network, Traffic Shaping and IP Filter settings will be applied to all traffic passing through the Guest Network SSID.



Guest Network

5GHz SSID	Comtrend-5g ▼
Guest Network	○ Enable ● Disable



Guest Access Policy

Traffic Shaping Settings

Traffic Shaping	Disable ▾	
Downlink	0	Mbps
Uplink	0	Mbps

Layer 2-Filtering Settings

MAC Filtering	Disable ▾	
Rules	Type	MAC address
	Disable ▾	00:00:00:00:00:00
	Disable ▾	00:00:00:00:00:00
	Disable ▾	00:00:00:00:00:00

Layer 3-Filtering Settings

Rules	Disable ▾		
Exceptions	Type	IP Address	Subnet Mask
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0
	Disable ▾	0.0.0.0	0.0.0.0

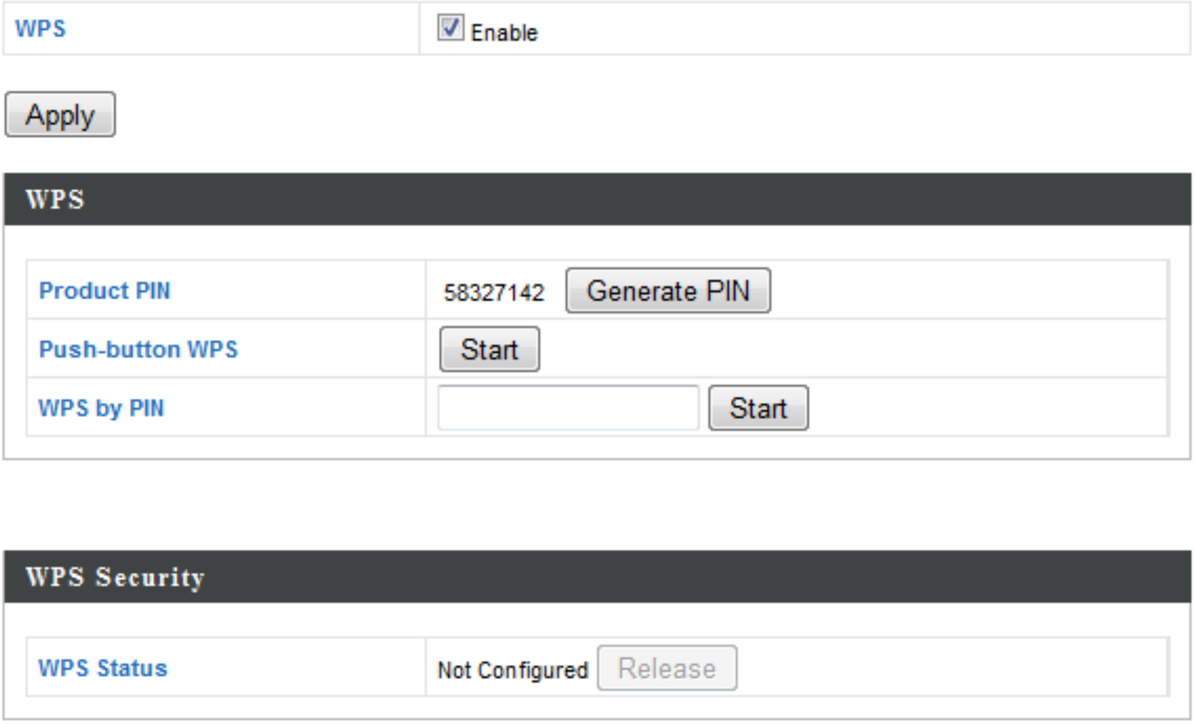
Guest Network	
5GHz SSID	Select the SSID that you want to apply the Guest Network settings to
Guest Network	Enable or Disable Guest Network settings
Guest Access Policy	
Traffic Shaping	Select “Enable” to apply bandwidth limitations on the “Downlink” and “Uplink” performance on the Guest Network
Layer 2-Filtering Settings	
MAC Filtering	Select “Disable”, “Whitelist” or “Blacklist”. Up to 3 MAC Filters are supported
Rules	Select “Disable” or “Enable” to toggle the application of the rule to the MAC Address.
Layer 3-Filtering Settings	
Rules	Select “Disable”, “Deny all by default” or “Allow all by default”. Up to 10 Exceptions are supported

Exceptions	Select “Disable”, “Deny” or “Allow”. Provide a starting IP Address and Subnet Mask to apply to the exception.

I-3-3. WPS

Wi-Fi Protected Setup 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.

Please refer to manufacturer’s instructions for your other WPS device.



WPS	☑ Enable

WPS

Product PIN	58327142 Generate PIN
Push-button WPS	Start
WPS by PIN	Start

WPS Security

WPS Status	Not Configured Release

WPS	Check/uncheck this box to enable/disable WPS functionality. WPS must be disabled when using MAC-RADIUS authentication (see **I-3-1-3-6 & I-3-4**)

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

I-3-4. RADIUS

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.

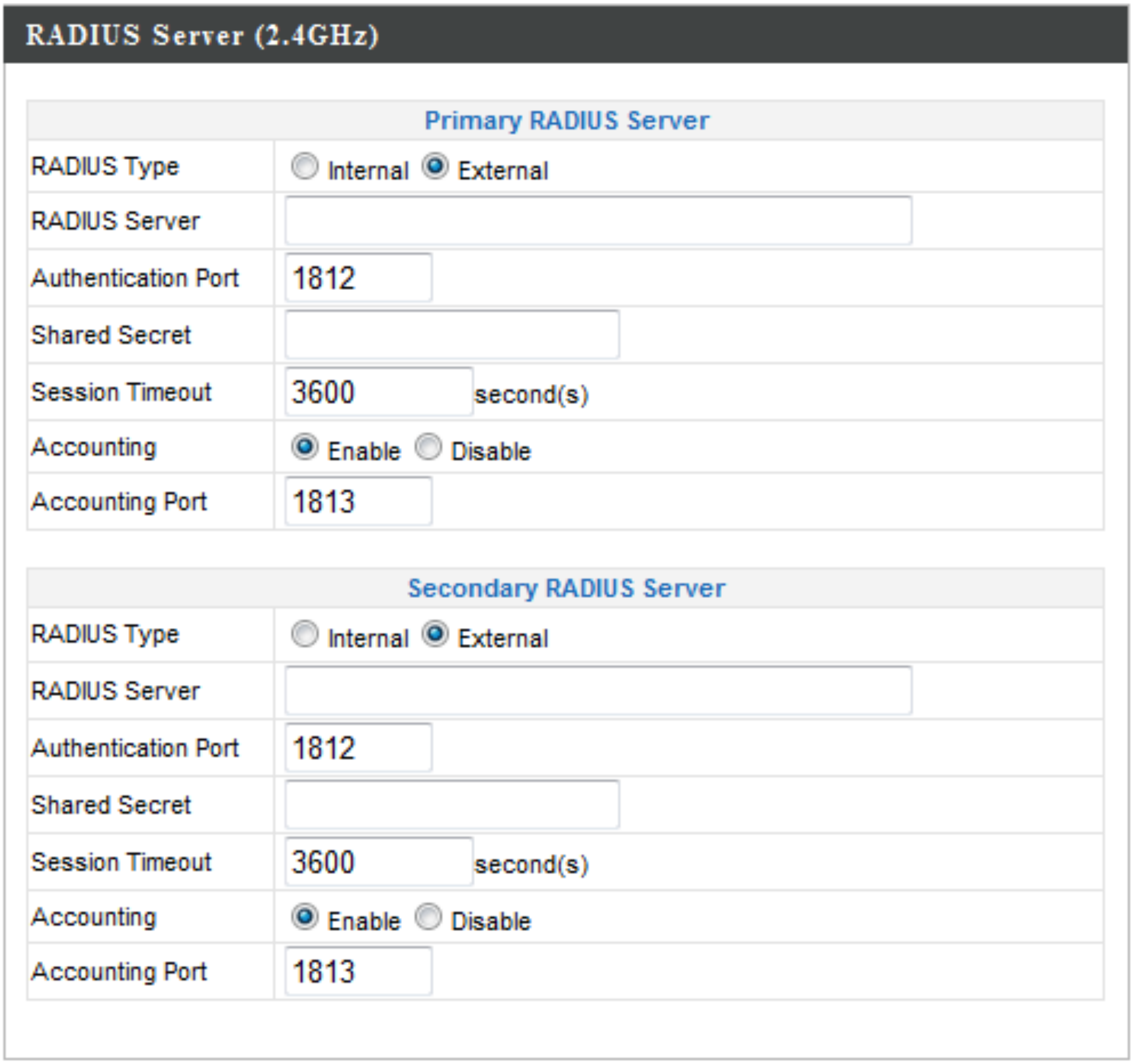
The access point can utilize both a primary and secondary (backup) RADIUS server for each of its wireless frequencies (2.4GHz & 5GHz). External RADIUS servers can be used or the access point’s internal RADIUS server can be used.

To use RADIUS servers, go to *“Wireless Settings”* **→** *“Security”* ***and select*** *the desired Authentication Method* **→** *“Additional Authentication”* ***and select*** *“MAC RADIUS Authentication”* ***(see*** *I-3-1-3.* ***&*** *I-3-2-3****).***

*The “****MAC RADIUS Authentication****” feature works with an external RADIUS Server Only.*

I-3-4-1.RADIUS Settings

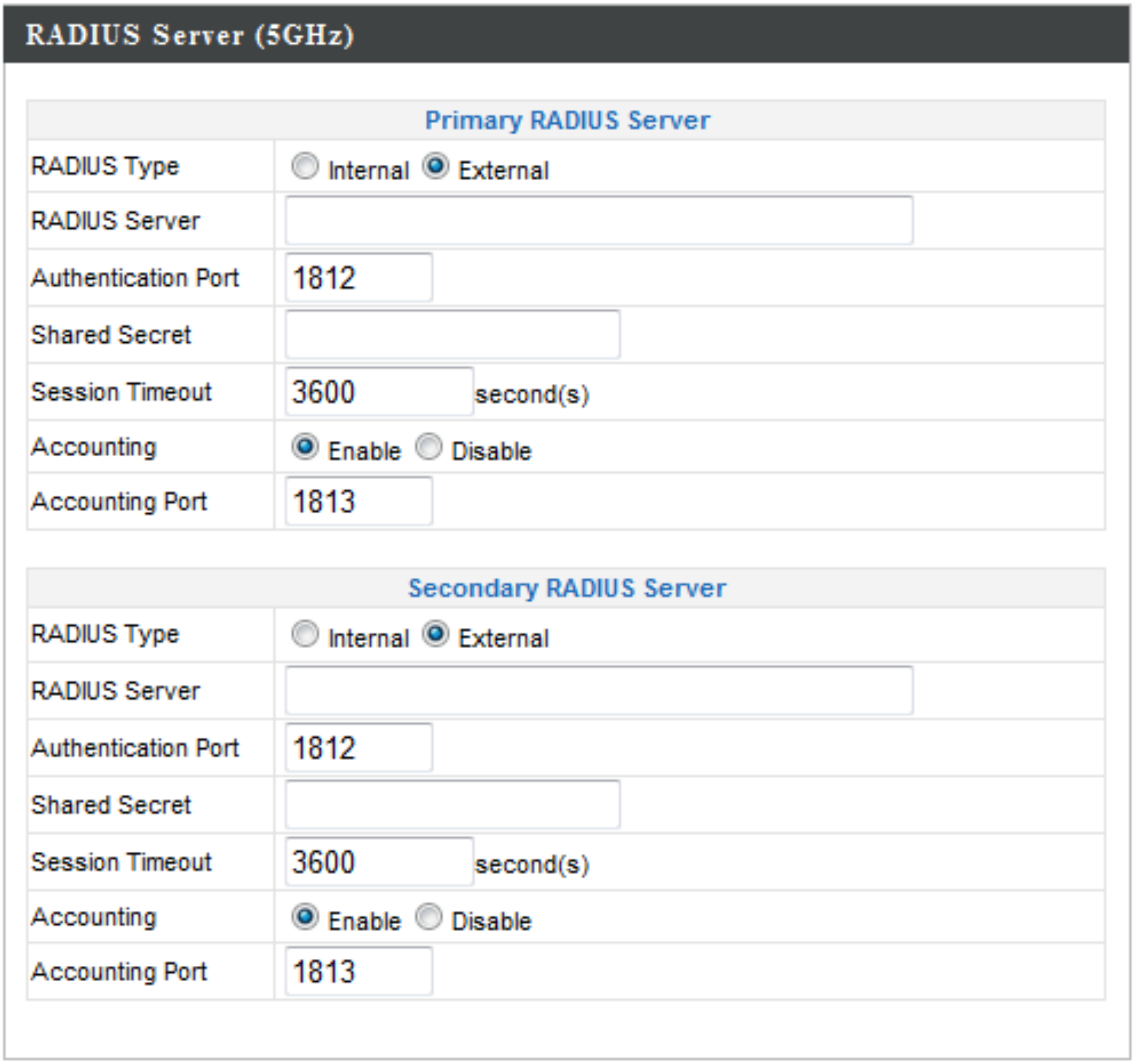
Configure the RADIUS server settings for 2.4GHz & 5GHz. Each frequency can use a primary and secondary (backup) RADIUS server.



RADIUS Server (2.4GHz)

Primary RADIUS Server	
RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

Secondary RADIUS Server	
RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813



RADIUS Server (5GHz)

Primary RADIUS Server	
RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

Secondary RADIUS Server	
RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

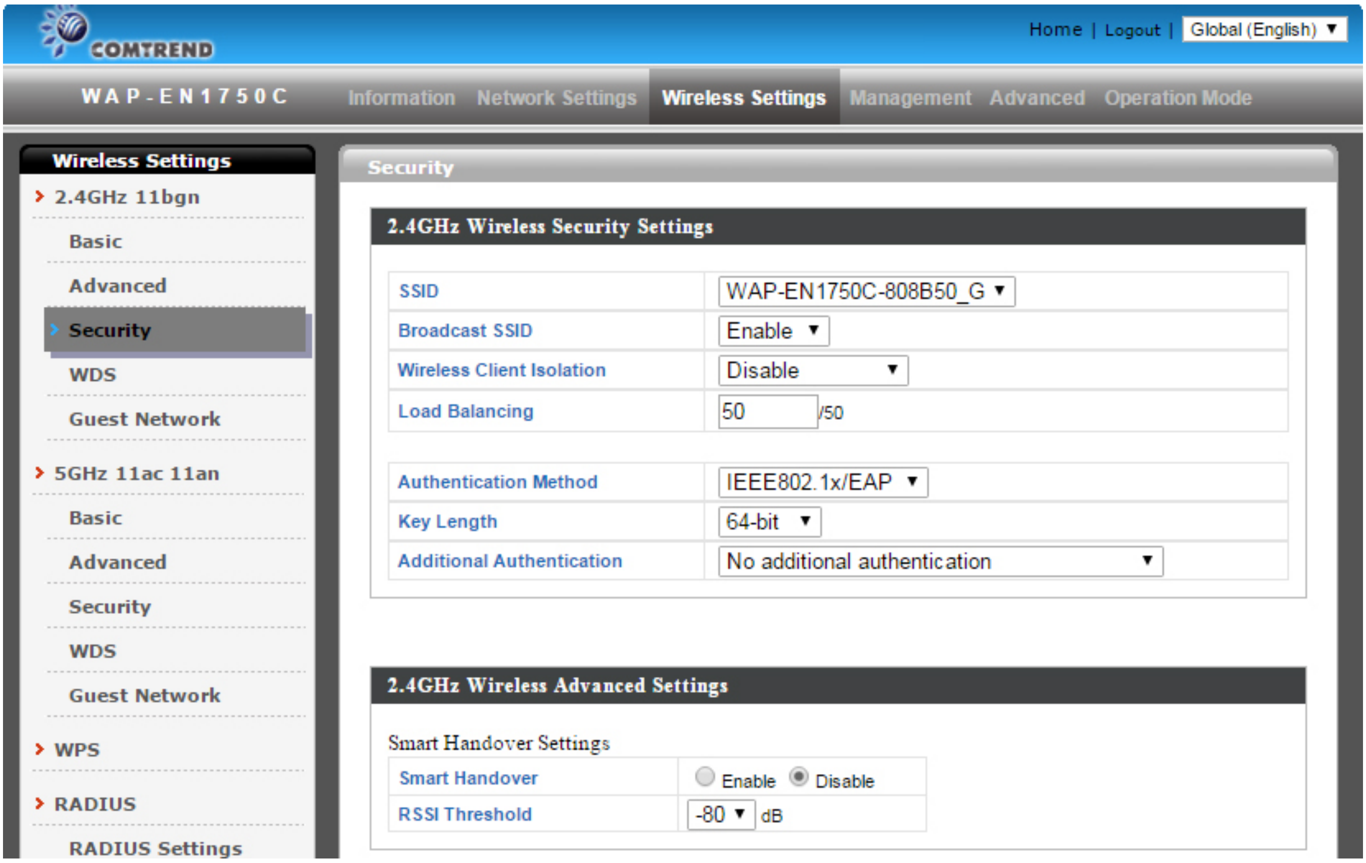
RADIUS Type	Select “Internal” to use the access point’s built-in RADIUS server or “external” to use an external RADIUS server
RADIUS Server	Enter the RADIUS server host IP address
Authentication Port	Set the UDP port used in the authentication protocol of the RADIUS server. Value must be between 1 – 65535
Shared Secret	Enter a shared secret/password between 1 – 99 characters in length. This should match the “MAC-RADIUS” password used in **I-3-1-3-6** or **I-3-2-3**
Session Timeout	Set a duration of session timeout in seconds between 0 – 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 – 65535

I-3-4-2.Internal Server

Internal Server

To use the Internal Radius Server as an additional authentication, configure the "Authentication Method" in "Wireless Settings/Security" to "IEEE802.1x/EAP". Leave "Additional Authentication" set to "No additional authentication". Click "Apply" to save settings. (Example image below)



2.4GHz Wireless Security Settings

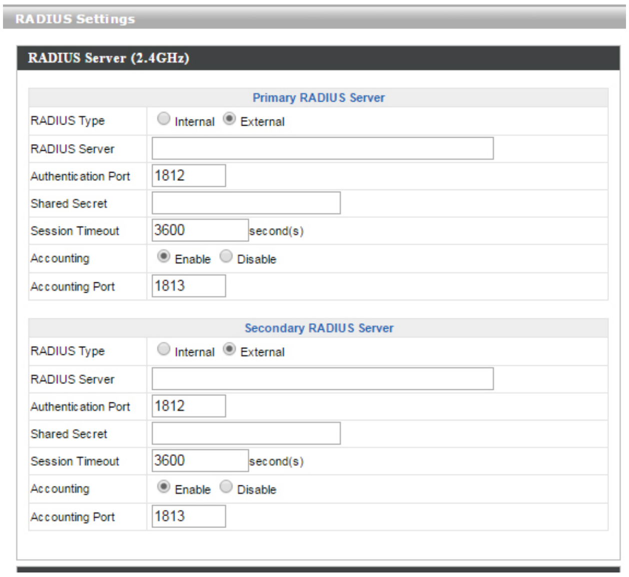
SSID	WAP-EN1750C-808B50_G ▾
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
Load Balancing	50 /50
Authentication Method	IEEE802.1x/EAP ▾
Key Length	64-bit ▾
Additional Authentication	No additional authentication ▾

2.4GHz Wireless Advanced Settings

Smart Handover Settings

Smart Handover	○ Enable ● Disable
RSSI Threshold	-80 ▾ dB

Next, Under "Radius/Radius Settings", Select "Internal" for Radius Type. Click "Apply" to save settings. (Example image below)



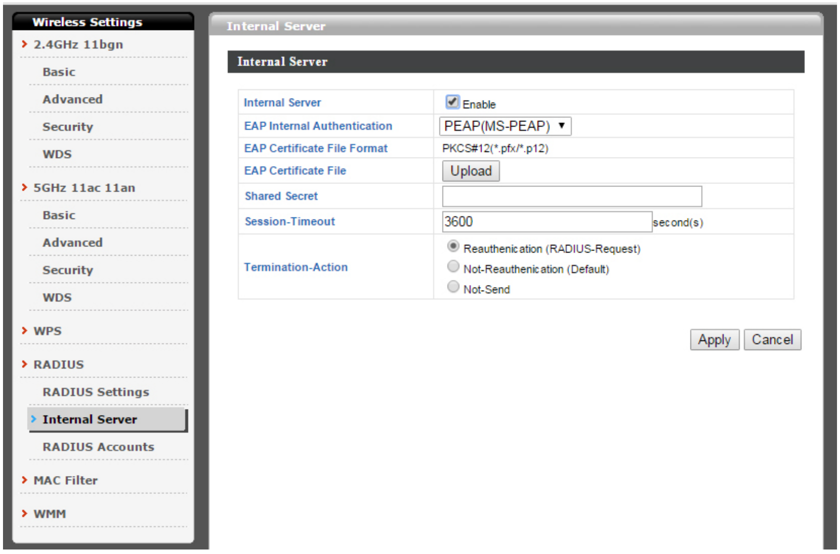
RADIUS Settings

RADIUS Server (2.4GHz)

Primary RADIUS Server	
RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

Secondary RADIUS Server	
RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

Under “Radius/Internal Server”, check the “Enable” box next to “Internal Server”. Select “PEAP (MS-PEAP)” for “EAP Internal Authentication”. Enter numbers or characters in the field “Shared Secret”. Set “Termination-Action” option to “Re-authentication (Radius-Request).” Click “Apply” to save changes. (Example image below)

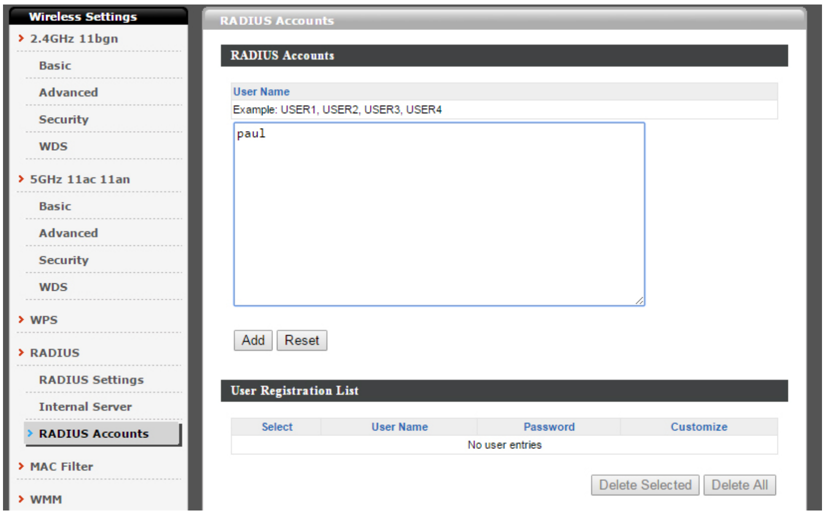


Internal Server

Internal Server	
Internal Server	☑ Enable
EAP Internal Authentication	PEAP(MS-PEAP) ▾
EAP Certificate File Format	PKCS#12(*.pfx/*.p12)
EAP Certificate File	Upload
Shared Secret	
Session-Timeout	3600 second(s)
Termination-Action	● Reauthenication (RADIUS-Request) ○ Not-Reauthenication (Default) ○ Not-Send

I-3-4-3.RADIUS Accounts

Do the following to add Radius User Names and configure passwords. Under “Radius/Radius Accounts”, enter a “User Name” in the window and click “Add”. (Example image below)



RADIUS Accounts

User Name

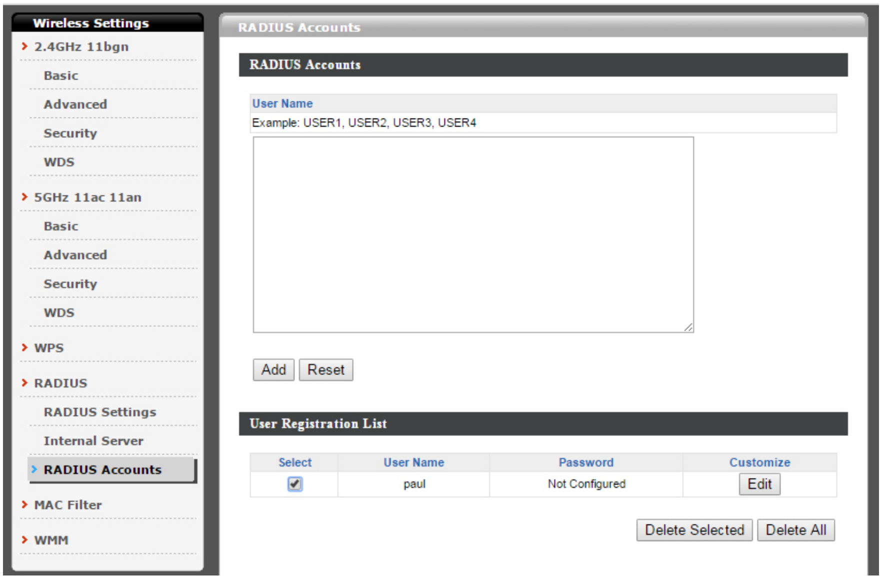
Example: USER1, USER2, USER3, USER4

paul

User Registration List

Select	User Name	Password	Customize
No user entries			

Select the “User Name” from the “User Registration List” and select “Edit”. (Example image below)



RADIUS Accounts

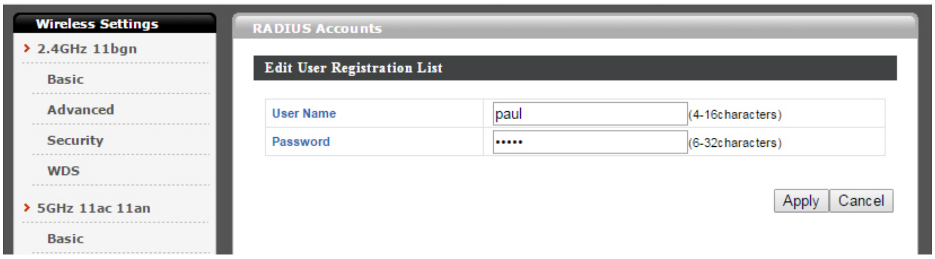
RADIUS Accounts

User Name
Example: USER1, USER2, USER3, USER4

User Registration List

Select	User Name	Password	Customize
☑	paul	Not Configured	Edit

Enter a password for the selected “User”. Click “Apply” to save changes. (Example image below)



RADIUS Accounts

Edit User Registration List

User Name	paul (4-16characters)
Password	••••• (6-32characters)

Your access point is now setup to authenticate Users with the Internal Radius Server.

Wireless Client Configuration for Radius Connection on Windows 7 (Example)

1. Go to “Control Panel/Network and Sharing Center/Manage Wireless Network”.
2. Click “Add” on the “Manage wireless networks thse use (Wireless Connection)” screen.
3. Click “Manually create a network profile”.
4. Enter the “Network Name” which you want to connect to. The Network Name is the SSID for the Radius connection. In the examples above, the network name used is “Internal-Radius”.
5. Adjust the “Security Type” to “802.1x”. Click “Next”.
6. Click “Change Connection Settings”.
7. Click the “Security” tab and then “Settings”.
8. Uncheck “Validate server certificate”.
9. Click “Configure” next to “Secured password (EAP-MSCHAP v2)”.
10. Uncheck “Automatically use my Windows Logon name and password”.
11. Click “OK” to close all windows.
12. Select the Radius Network and Click “Connect”.
13. You will receive a pop up message stating “Additional information is needed to conenct“.
14. Click on the message to continue.
15. Enter the Username and password you created in the “Windows Security” window.
16. Click “OK”.
17. Your connection to the SSID with Radius Authentication is now “Connected”.

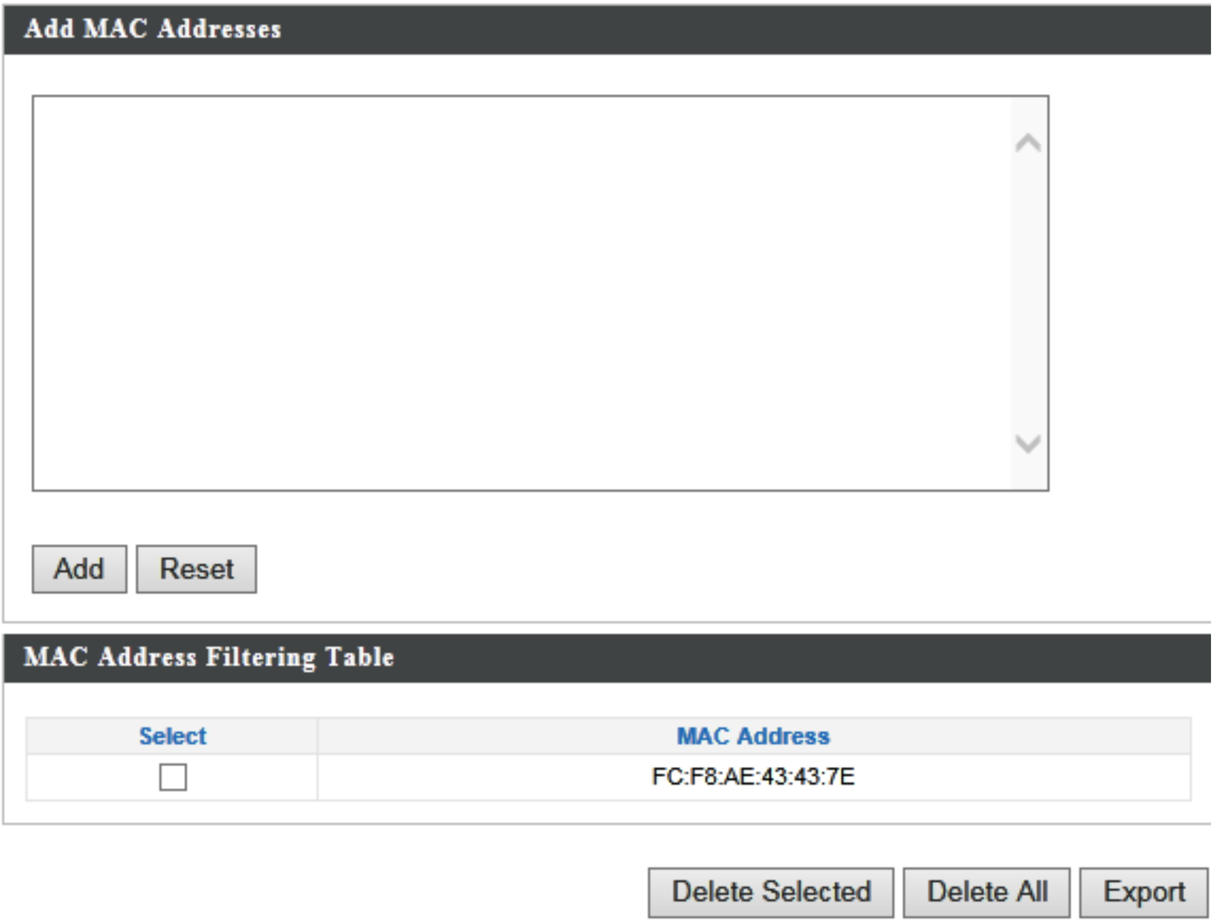
I-3-5. MAC Filter

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

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

To enable MAC filtering, go to *"Wireless Settings"* **→** *"2.4GHz 11bgn/5GHz 11ac 11an"* **→** *"Security"* **→** *"Additional Authentication"* ***and select*** *"MAC Filter"* ***(see*** *I-3-1-3.* ***&*** *I-3-2-3****).***

The MAC address filtering table is displayed below:



Select	MAC Address
□	FC:F8:AE:43:43:7E

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,

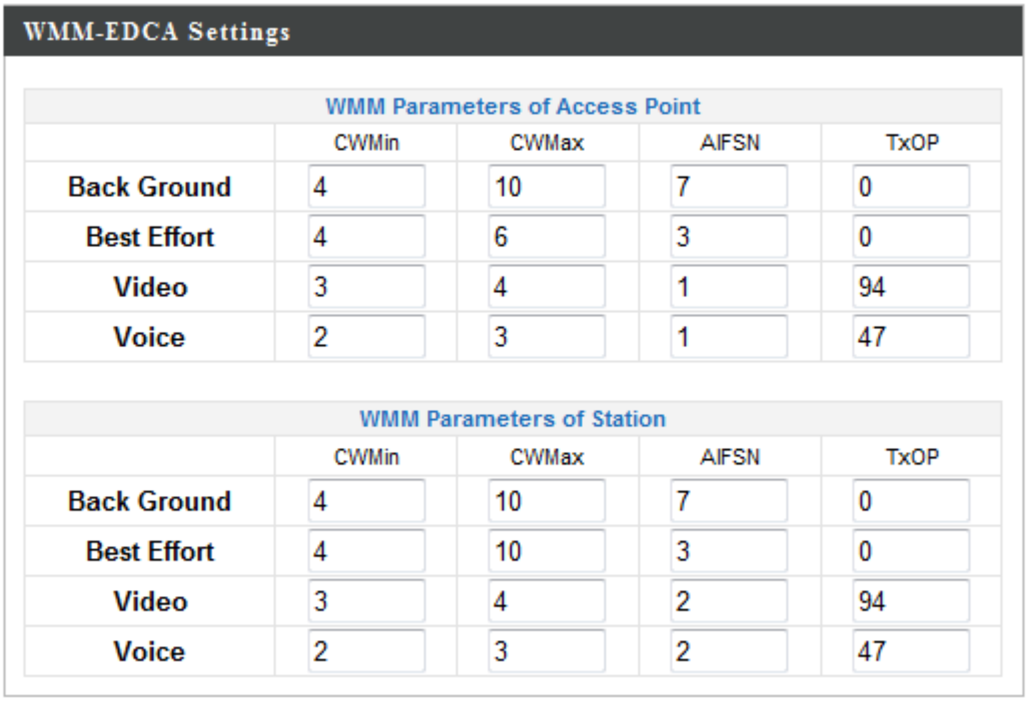
	aa-bb-cc-dd-ee-gg’
Add	Click “Add” to add the MAC address to the MAC address filtering table
Reset	Clear all fields

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

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
Export	Click “Export” 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

I-3-6. 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

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

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

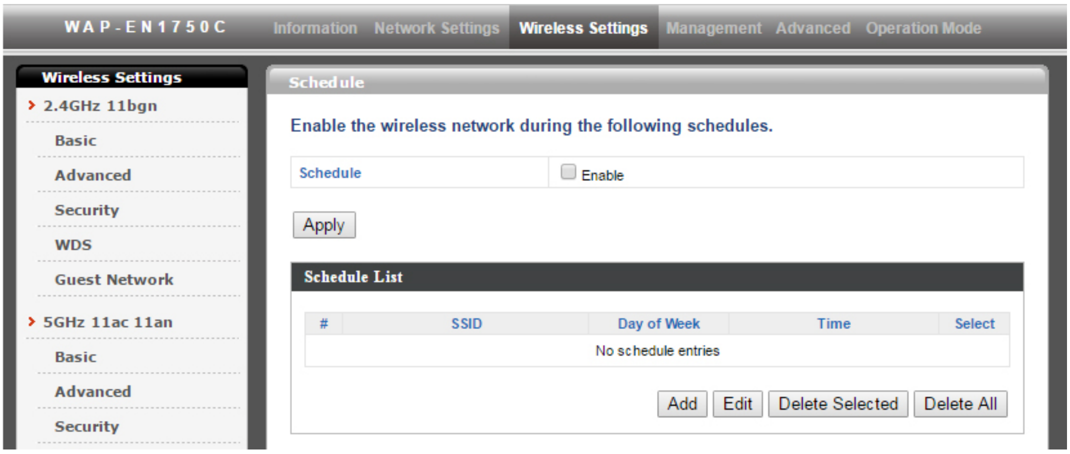
Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can further be adjusted manually:

CWMin	Minimum Contention Window (milliseconds):

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

I-3-7. Schedule

Schedule allows an administrator to create a schedule for the Wireless Access Point. This feature is commonly used to disable the wireless during non-business hours or any other time sensitive application.



Enable the wireless network during the following schedules.

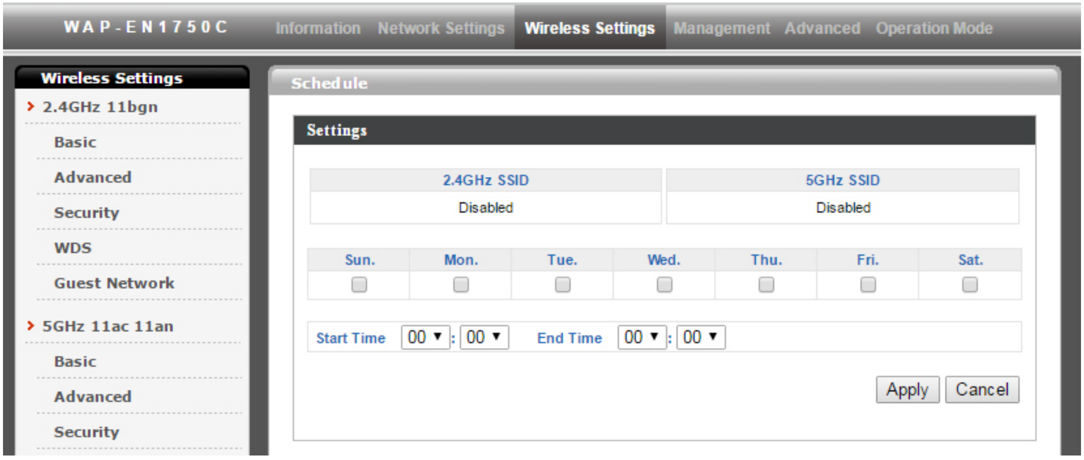
Schedule	□ Enable

Apply

Schedule List

#	SSID	Day of Week	Time	Select
No schedule entries				

Once enabled, an independent schedule for both the 2.4GHz and 5GHz band can be created.



Settings

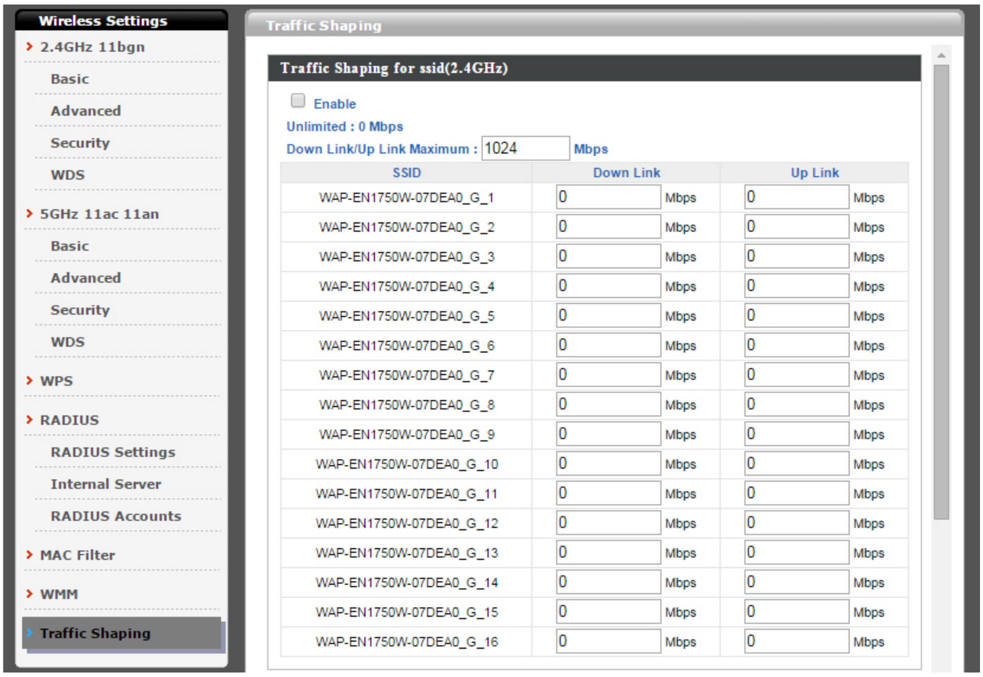
2.4GHz SSID	5GHz SSID
Disabled	Disabled

Sun.	Mon.	Tue.	Wed.	Thu.	Fri.	Sat.
□	□	□	□	□	□	□

Start Time 00 : 00 End Time 00 : 00

I-3-8. Traffic Shaping

Traffic Shaping allows an administrator to limit the bandwidth available to each SSID. Providing a value between 0-1024Mbps. A value of “0” indicates unlimited bandwidth.



Traffic Shaping for ssid(2.4GHz)

□ Enable

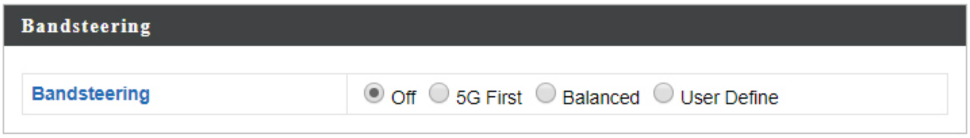
Unlimited : 0 Mbps

Down Link/Up Link Maximum : 1024 Mbps

SSID	Down Link		Up Link	
WAP-EN1750W-07DEA0_G_1	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_2	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_3	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_4	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_5	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_6	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_7	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_8	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_9	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_10	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_11	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_12	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_13	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_14	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_15	0	Mbps	0	Mbps
WAP-EN1750W-07DEA0_G_16	0	Mbps	0	Mbps

I-3-9. Band Steering

Bandsteering allows the wireless access point to select the wireless band for client devices.

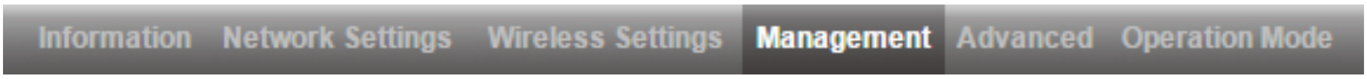


Bandsteering

Bandsteering ● Off ○ 5G First ○ Balanced ○ User Define

Band Steering	
Off	Disables Band Steering
5G First	Client devices will be connected to the 5Ghz Band First
Balanced	Client devices will be managed across both bands
User Defined	
2.4Ghz Overload Threshold	Value determines when client device connections should be limited or restricted
5Ghz Overload Threshold	Value determines when client device connections should be limited or restricted
Min RSSI	Value determines minimum connection strength for client devices

I-4. Management



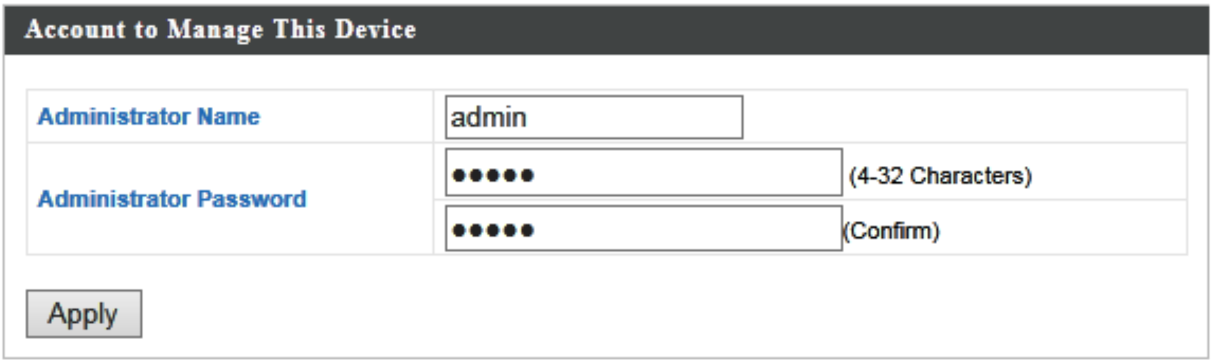
Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

I-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.

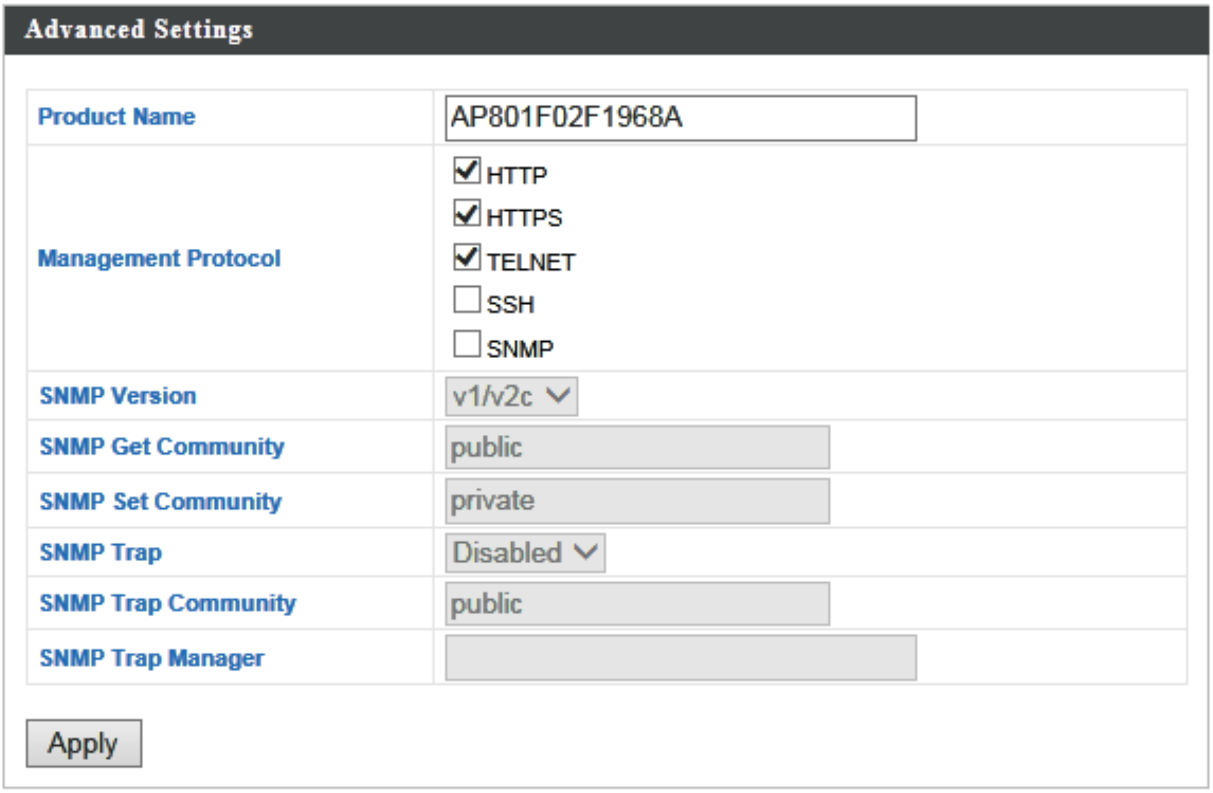
If you change the administrator password, please make a note of the new password. In the event that you forget this

password and are unable to login to the browser based configuration interface, see** I-5. Reset **for how to reset the access point.



Account to Manage This Device

Administrator Name	admin	
Administrator Password	●●●●●	(4-32 Characters)
	●●●●●	(Confirm)



Advanced Settings

Product Name	AP801F02F1968A
Management Protocol	☑ HTTP ☑ HTTPS ☑ TELNET ☐ SSH ☐ SNMP
SNMP Version	v1/v2c
SNMP Get Community	public
SNMP Set Community	private
SNMP Trap	Disabled
SNMP Trap Community	public
SNMP Trap Manager	

Account to Manage This Device	
Administrator Name	Set the access point’s administrator name. This is used to log in to the browser based configuration interface and must be between 4-16 alphanumeric characters (case sensitive)
Administrator Password	Set the access point’s administrator password. This is used to log in to the browser based configuration interface and must be between 4-32 alphanumeric characters (case sensitive)

Advanced Settings	
Product Name	Edit the product name according to your preference consisting of 1-32 alphanumeric characters. 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 (2-128 alphanumeric 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

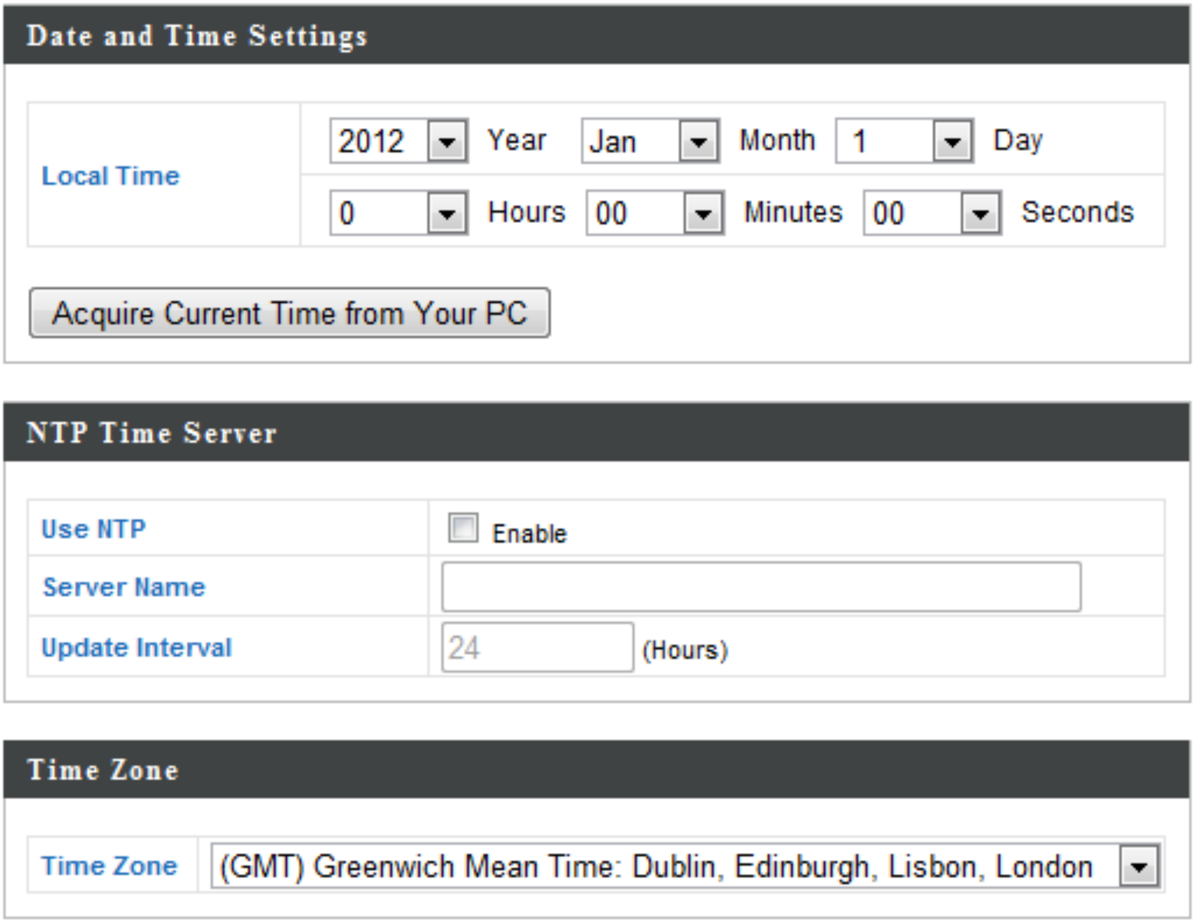
Client terminal with SSH protocol version 1 or 2 management interface

SNMP

Simple Network Management Protocol. SNMPv1, v2 & v3 protocol supported. SNMPv2 can be used with community based authentication. SNMPv3 uses user-based security model (USM) architecture.

I-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.



Date and Time Settings

Local Time	2012 Year, Jan Month, 1 Day 0 Hours, 00 Minutes, 00 Seconds

NTP Time Server

Use NTP	□ Enable
Server Name	
Update Interval	24 (Hours)

Time Zone

Time Zone	(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London

Date and Time Settings	
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

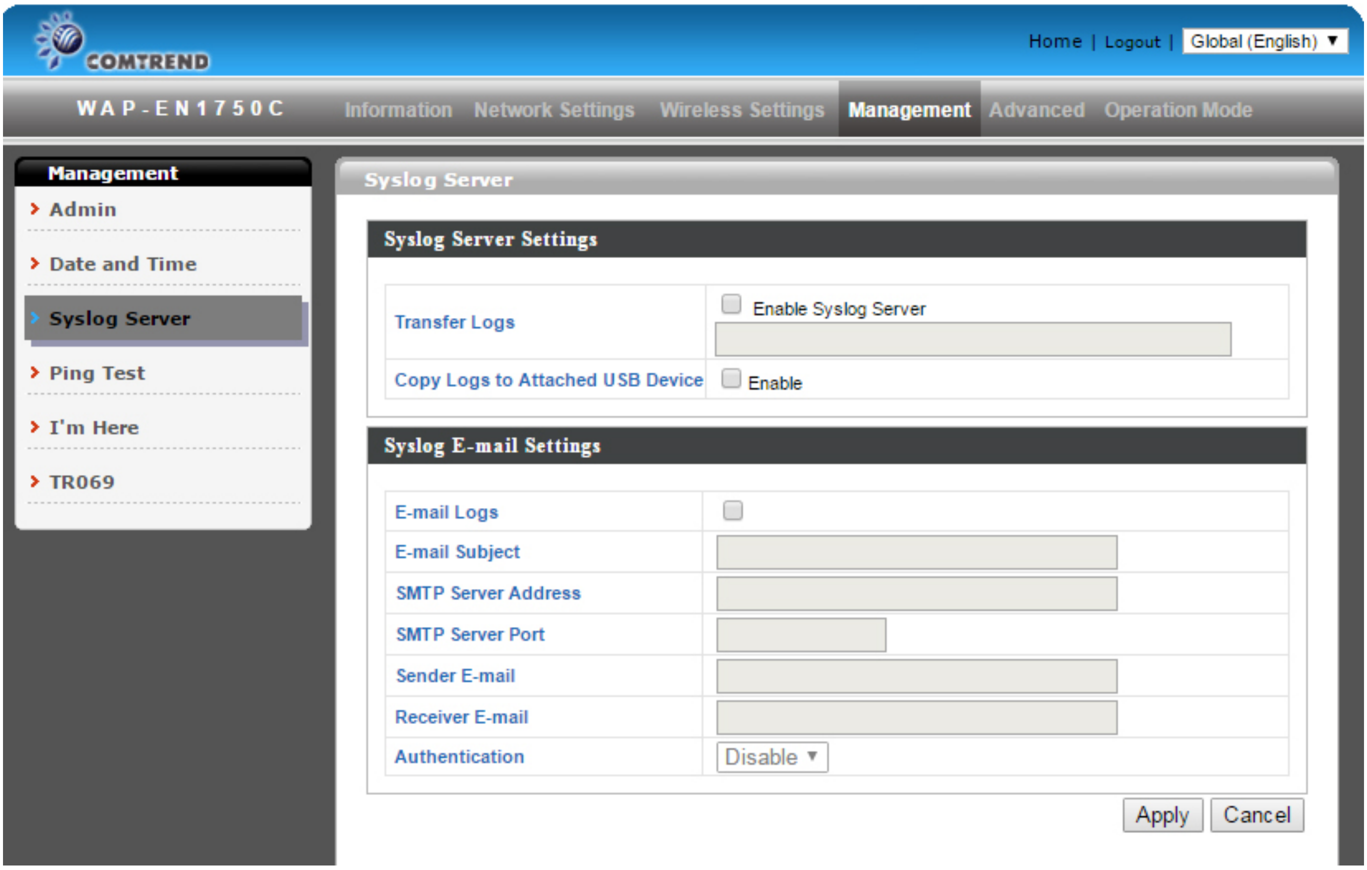
NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup
Server Name	Enter the host name or IP address of the time

	server if you wish
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP server

Time Zone	
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

I-4-3. Syslog Server

The system log can be sent to a server, stored on an attached USB device or emailed.



Syslog Server Settings

Transfer Logs	□ Enable Syslog Server
Copy Logs to Attached USB Device	□ Enable

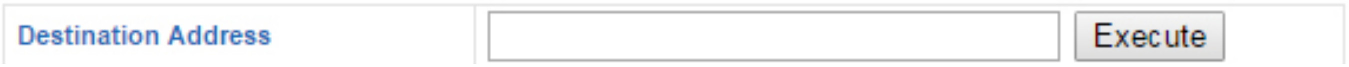
Syslog E-mail Settings

E-mail Logs	□
E-mail Subject	
SMTP Server Address	
SMTP Server Port	
Sender E-mail	
Receiver E-mail	
Authentication	Disable

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

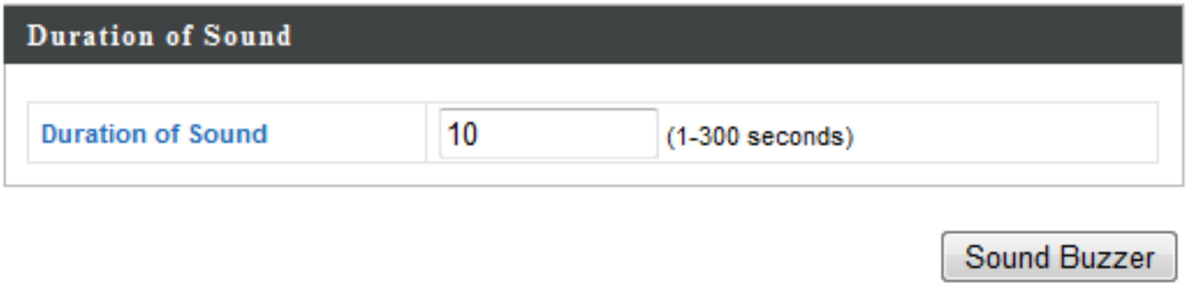
I-4-4. Ping Test

The “Ping Test” will send a continuous Ping to the IP Address specified. Results are posted in the dialog box below the Destination Address Execution window.



I-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.


Duration of Sound

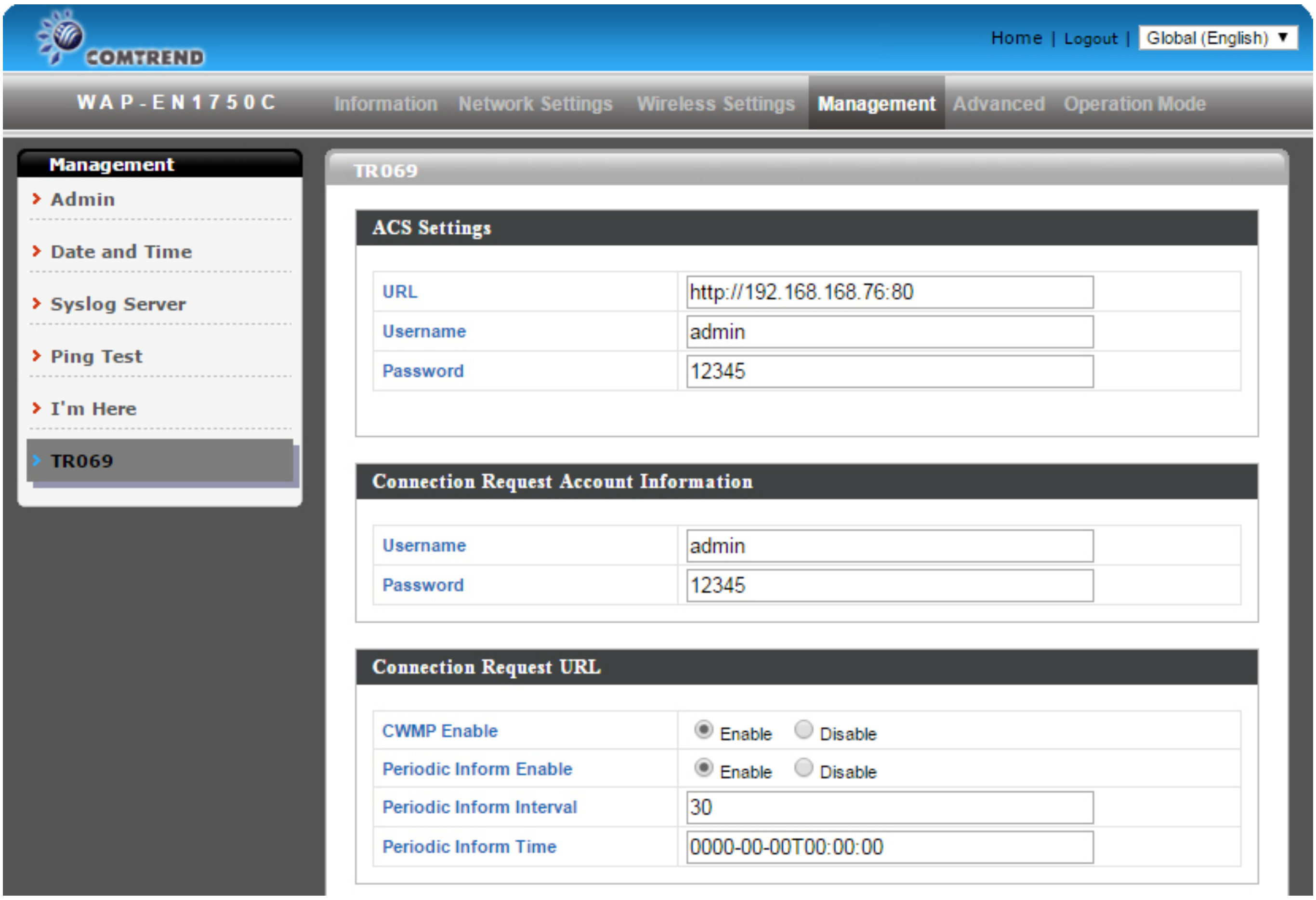
Duration of Sound: 10 (1-300 seconds)

⚠ ***The buzzer is loud!***

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.

I-4-6. TR-069

TR-069 allows an administrator to connect the wireless access point to a remote ACS system. Provide the destination and login credentials to the ACS system.



TR069

ACS Settings

URL	http://192.168.168.76:80
Username	admin
Password	12345

Connection Request Account Information

Username	admin
Password	12345

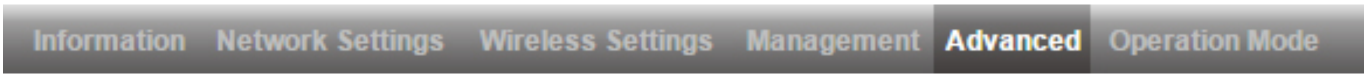
Connection Request URL

CWMP Enable	● Enable ○ Disable
Periodic Inform Enable	● Enable ○ Disable
Periodic Inform Interval	30
Periodic Inform Time	0000-00-00T00:00:00

I-4-7. wifiXtend

Enable and Disable WifiXtend here. WifiXtend is a feature that allows a Comtrend Gateway to share the primary wireless SSID and Password with a remote wireless access point.

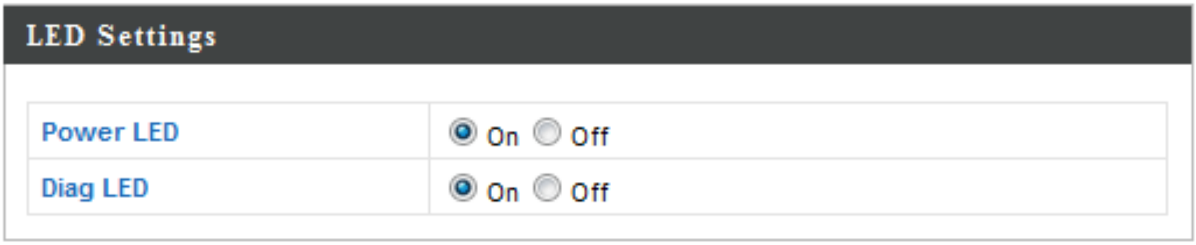
I-5 Advanced



Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

I-5-1. LED Settings

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



LED Settings

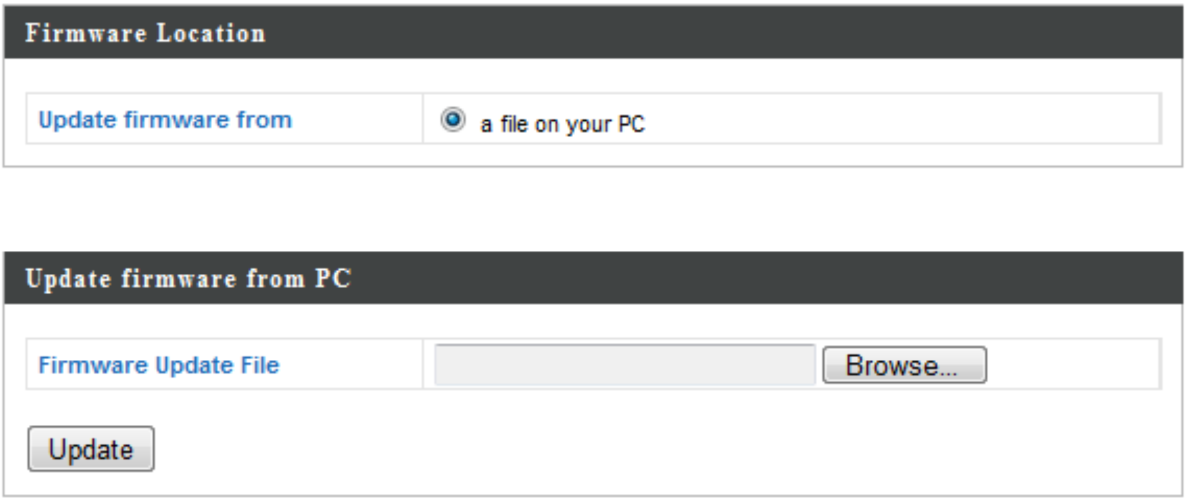
Power LED	● On ○ Off
Diag LED	● On ○ Off

Power LED	Select on or off.
Diagnostic LED	Select on or off.

I-5-2. Update Firmware

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 Comtrend website.



Firmware Location

Update firmware from ● a file on your PC

Update firmware from PC

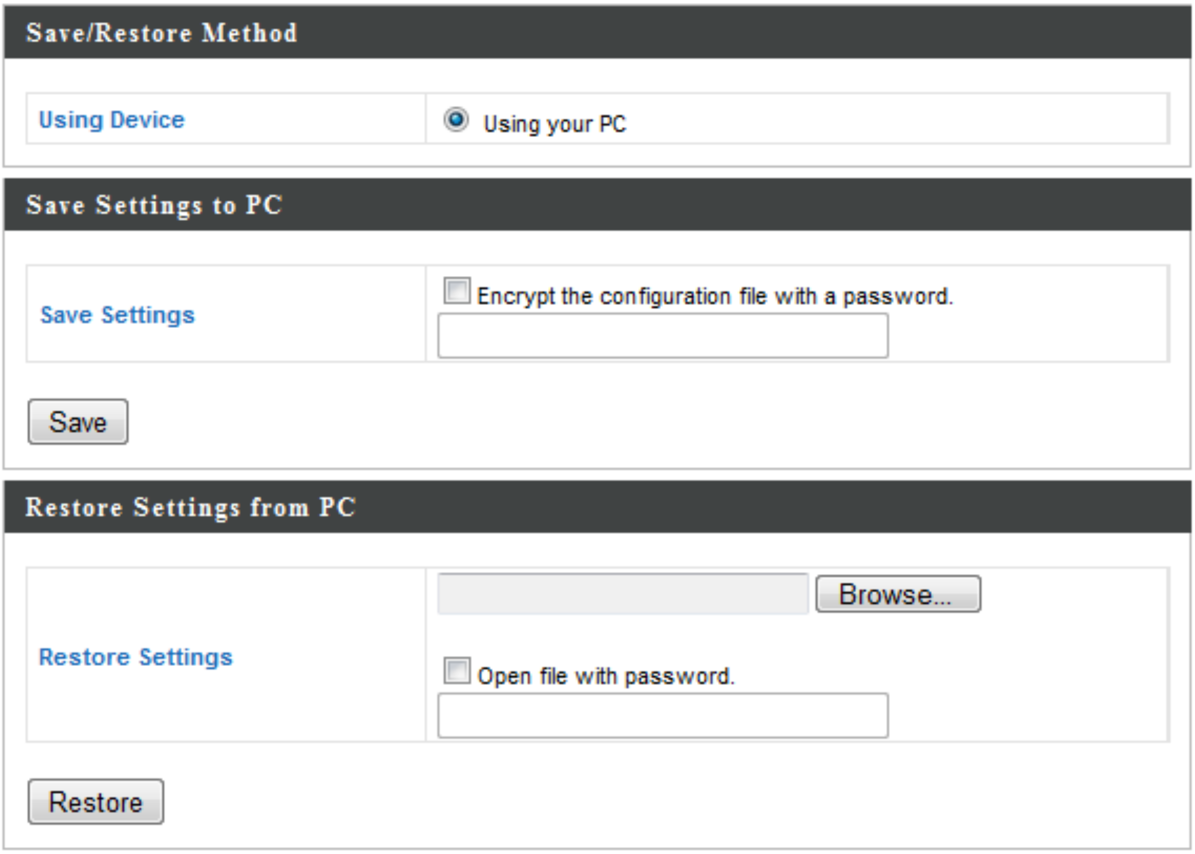
Firmware Update File

Do not switch off or disconnect the access point during a firmware upgrade, as this could damage the device.

Update Firmware From	Select “a file on your PC” to upload firmware from your local computer
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

I-5-3. Save/Restore Settings

The access point's "Save/Restore Settings" page enables you to save/backup the access point's current settings as a file to your local computer, and restore the access point to previously saved settings.



Save/Restore Method

Using Device	● Using your PC

Save Settings to PC

Save Settings	□ Encrypt the configuration file with a password.

Restore Settings from PC

Restore Settings	Browse... □ Open file with password.

Save / Restore Settings	
Using Device	Select "Using your PC" to save the access point's settings to your local computer

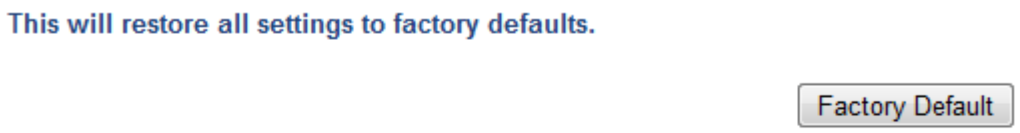
Save Settings to PC	
Save Settings	Click "Save" to save settings and a new window will open to specify a location to save the settings file. You can also check the "Encrypt the configuration file with a password" box and enter a password to protect the file in the field underneath, if you wish

Restore Settings from PC

Restore Settings	Click the browse button to find a previously saved settings file on your computer, 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

I-5-4. Factory Default

If the access point malfunctions or is not responding, then it is recommended that you reboot the device (see **I-5.5**) 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.



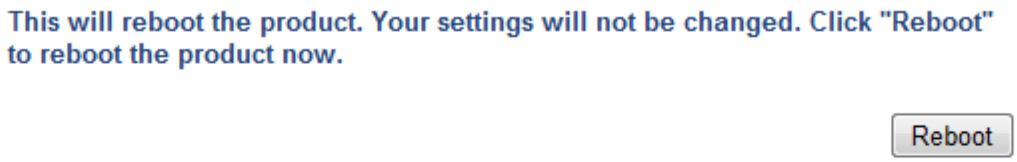
This will restore all settings to factory defaults.

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.

I-5-5. Reboot

If the access point malfunctions or is not responding, then it is recommended that you reboot the device or reset the access point back to its factory default settings (see **I-5-4**). You can reboot the access point remotely using this feature.



This will reboot the product. Your settings will not be changed. Click "Reboot" to reboot the product now.

Reboot	Click “Reboot” to reboot the device. A countdown will indicate the progress of the reboot

I-6. Operation Mode

This Menu Section will determine the operational characteristic of the wireless access point. Options include AP Mode, Repeater Mode, AP Controller Mode, Managed AP Mode and Client Bridge Mode.

II. Appendix

II-1. Configuring your IP address

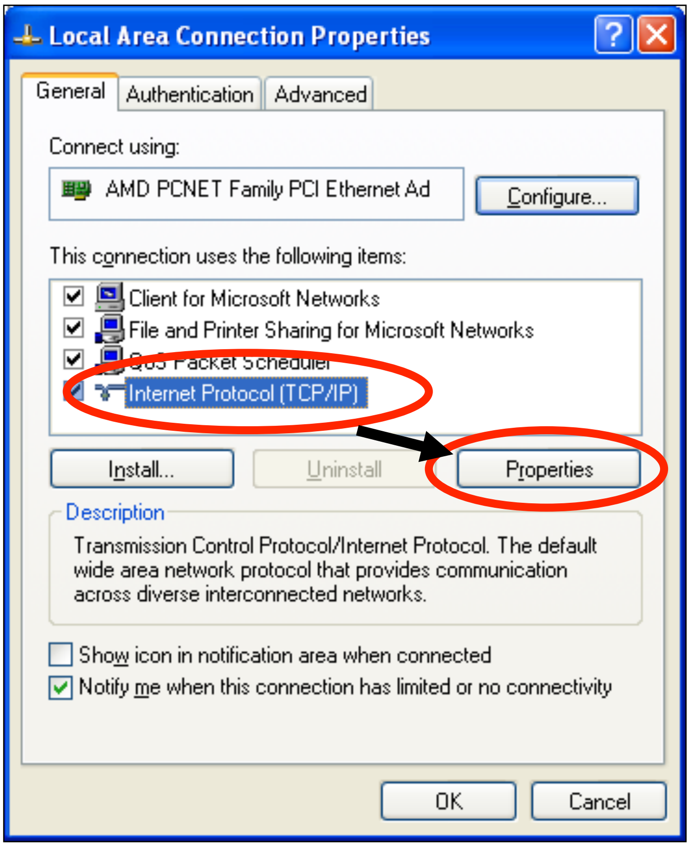
If no DHCP Service is detected, the access point uses the default IP address **192.168.2.2 or 192.168.2.1**. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. **192.168.2.x (x = 3 – 254).**

The procedure for modifying your IP address varies across different operating systems; please follow the guide appropriate for your operating system.

In the following examples we use the IP address **192.168.2.10** though you can use any IP address in the range **192.168.2.x (x = 3 – 254).**

II-1-1. Windows XP

1. Click the "Start" button (it should be located in the lower-left corner of your computer), then click "Control Panel". Double-click the "Network and Internet Connections" icon, click "Network Connections", and then double-click "Local Area Connection". The "Local Area Connection Status" window will then appear, click "Properties".



Connect using:

AMD PCNET Family PCI Ethernet Ad

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol (TCP/IP)

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

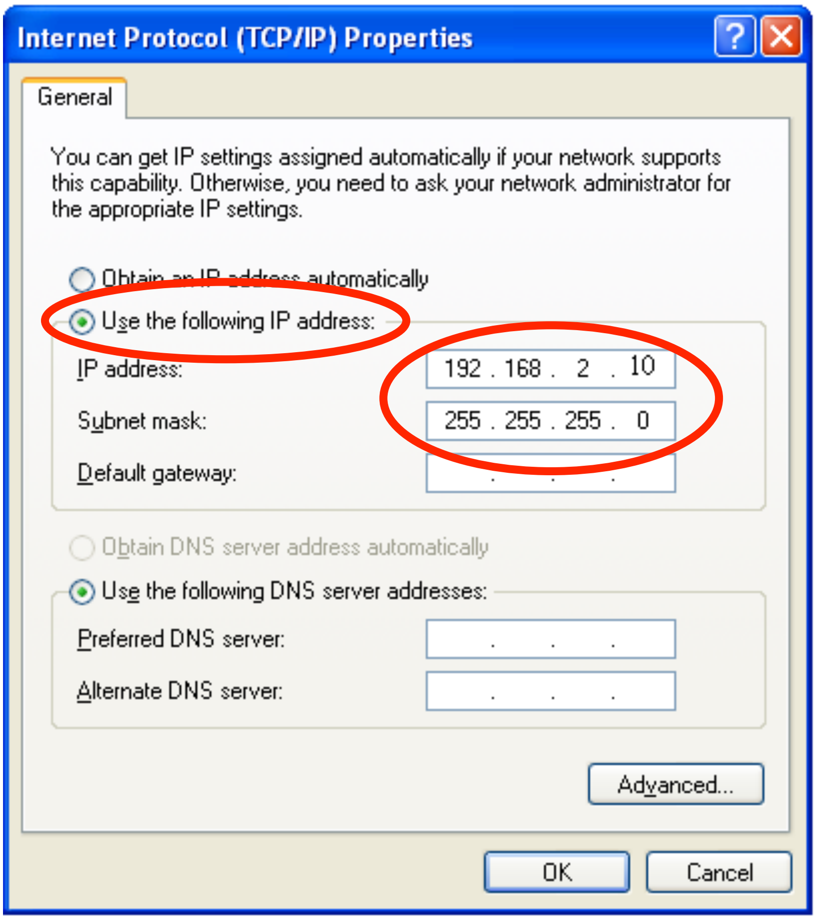
□ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

2. Select "Use the following IP address", then input the following values:

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click 'OK' when finished.



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

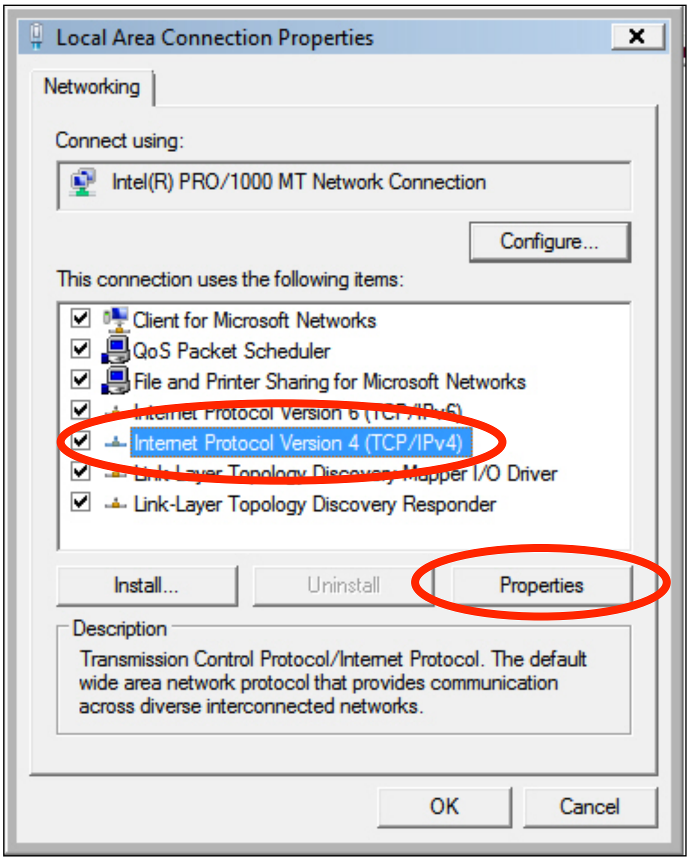
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

II-1-2. Windows Vista

1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”. Click “View Network Status and Tasks”, then click “Manage Network Connections”. Right-click “Local Area Network”, then select “Properties”. The “Local Area Connection Properties” window will then appear, select “Internet Protocol Version 4 (TCP / IPv4)”, and then click “Properties”.



Local Area Connection Properties

Networking

Connect using:

Intel(R) PRO/1000 MT Network Connection

Configure...

This connection uses the following items:

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

Install... Uninstall Properties

Description

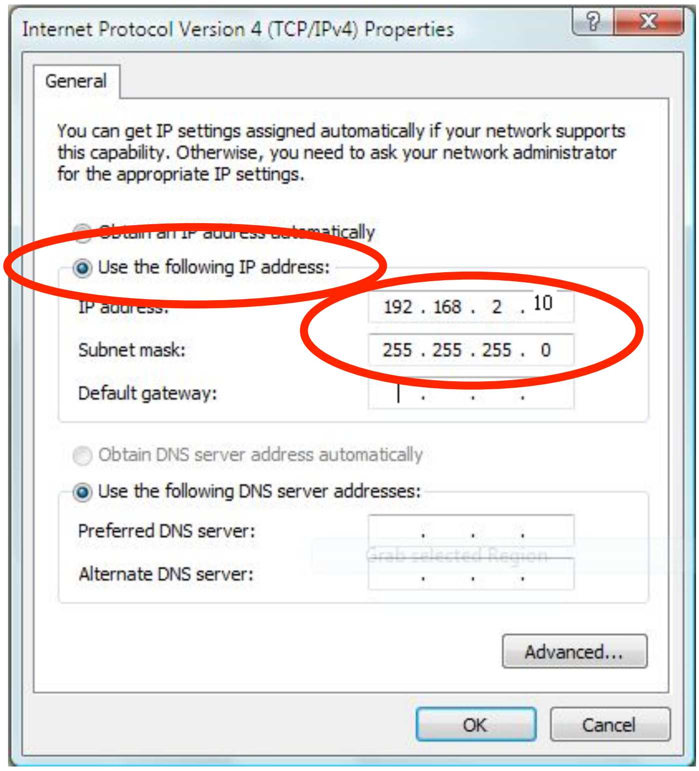
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK Cancel

2. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

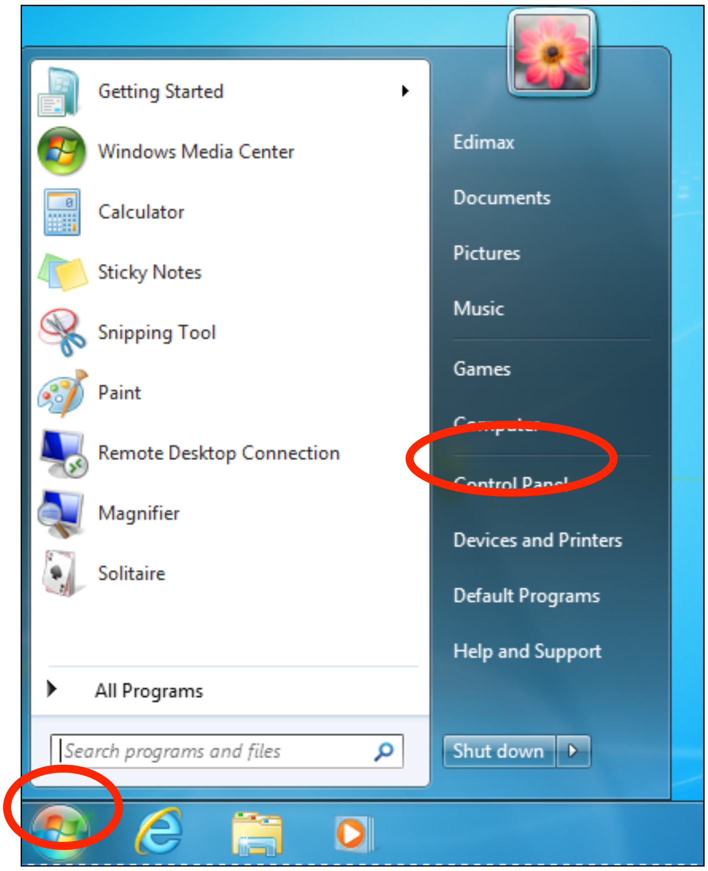
● Use the following DNS server addresses:

Preferred DNS server: . . .

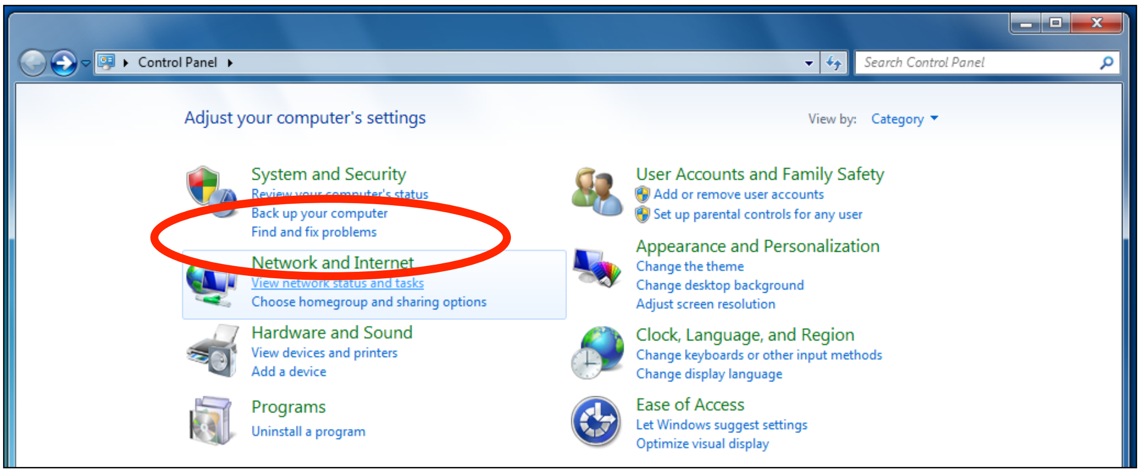
Alternate DNS server: . . .

II-1-3. Windows 7

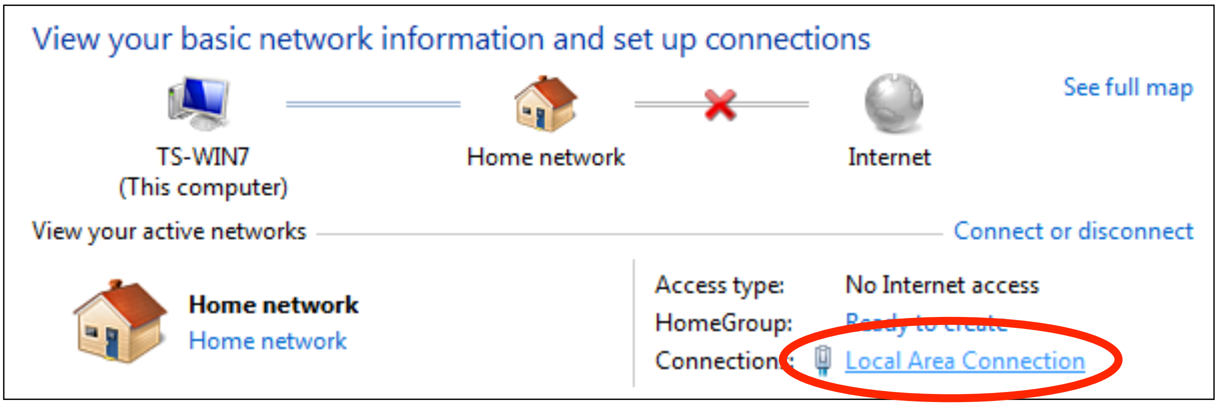
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



2. Under “Network and Internet” click “View network status and tasks”.


Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Change display language
Ease of Access
Let Windows suggest settings
Optimize visual display

3. Click “Local Area Connection”.



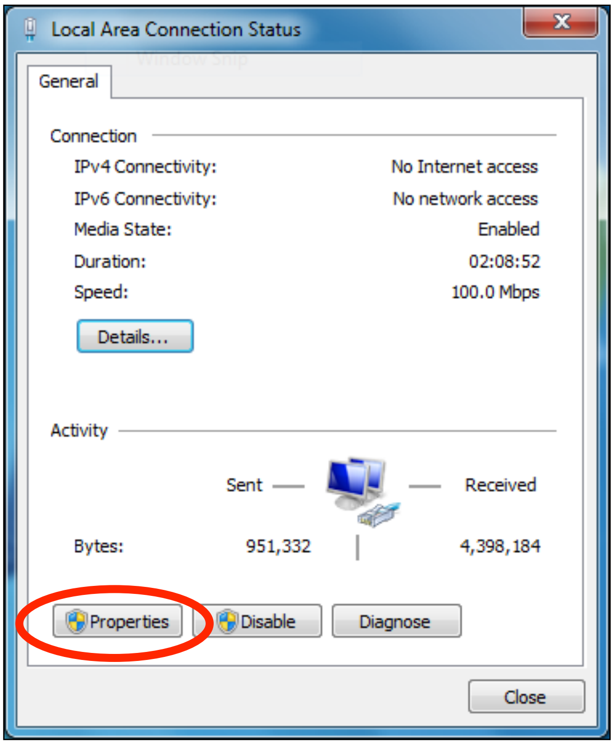
View your basic network information and set up connections

Access type: No Internet access

HomeGroup: Ready to create

Connections: Local Area Connection

4. Click “Properties”.



Local Area Connection Status

IPv4 Connectivity: No Internet access

IPv6 Connectivity: No network access

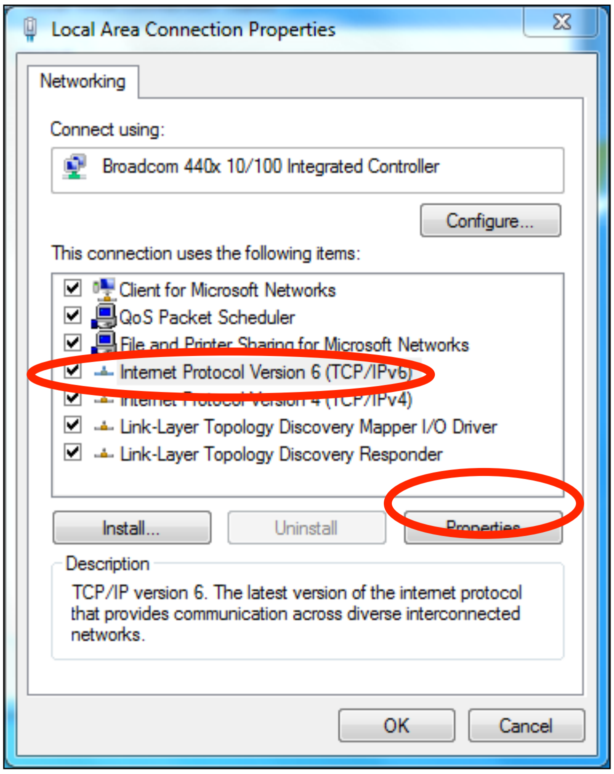
Media State: Enabled

Duration: 02:08:52

Speed: 100.0 Mbps

Bytes: 951,332 | 4,398,184

5. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.

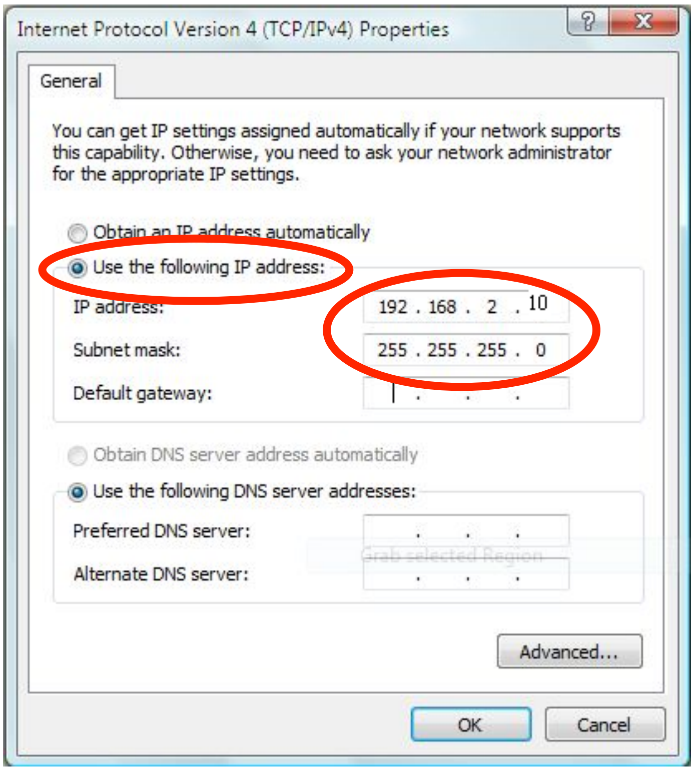


Local Area Connection Properties
Networking
Connect using:
Broadcom 440x 10/100 Integrated Controller
Configure...
This connection uses the following items:
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
Install...
Uninstall
Properties
Description
TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.
OK
Cancel

6. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

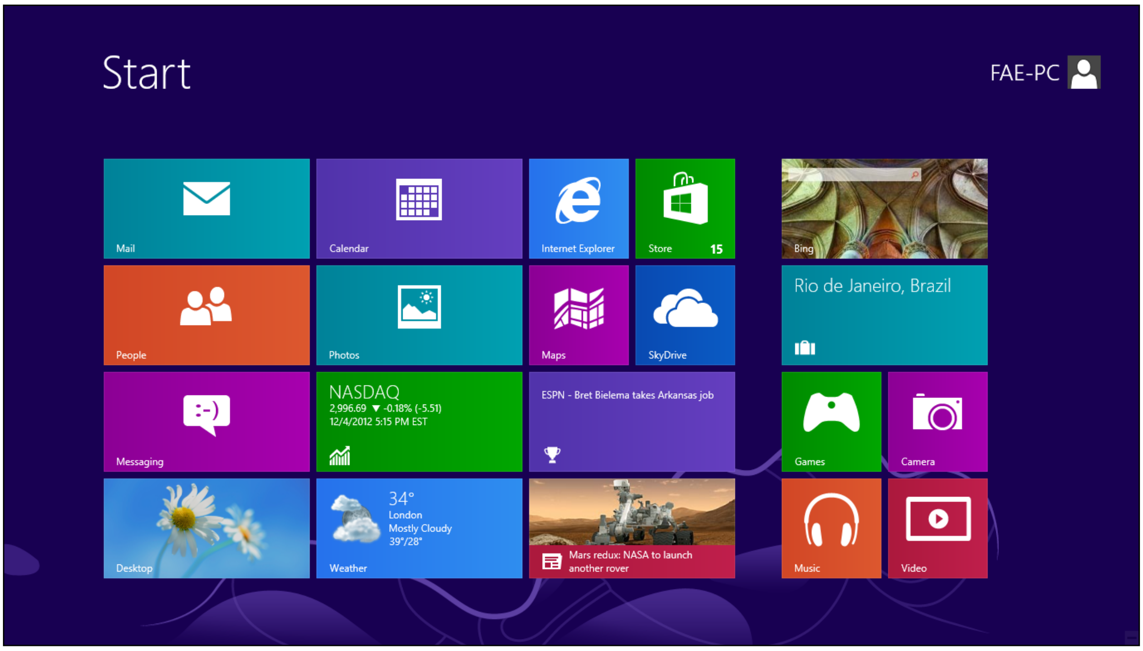
● Use the following DNS server addresses:

Preferred DNS server: . . .

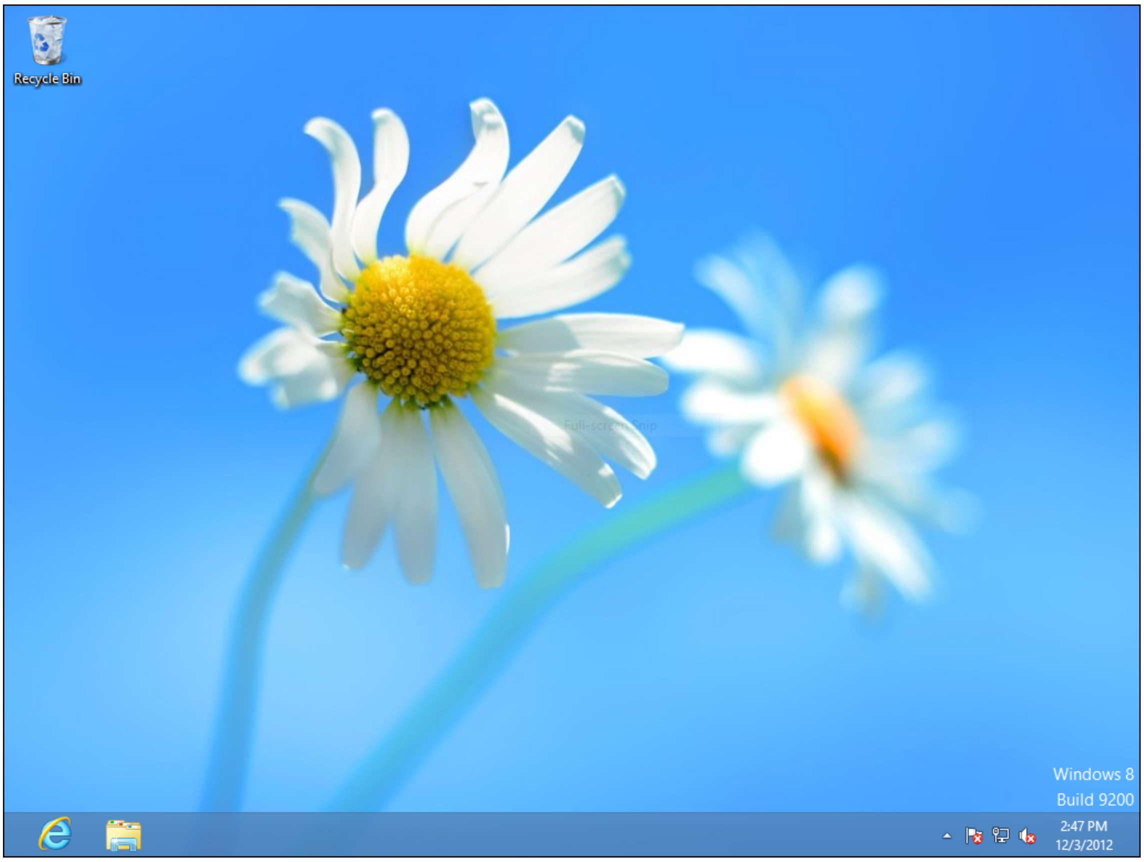
Alternate DNS server: . . .

II-1-4. Windows 8

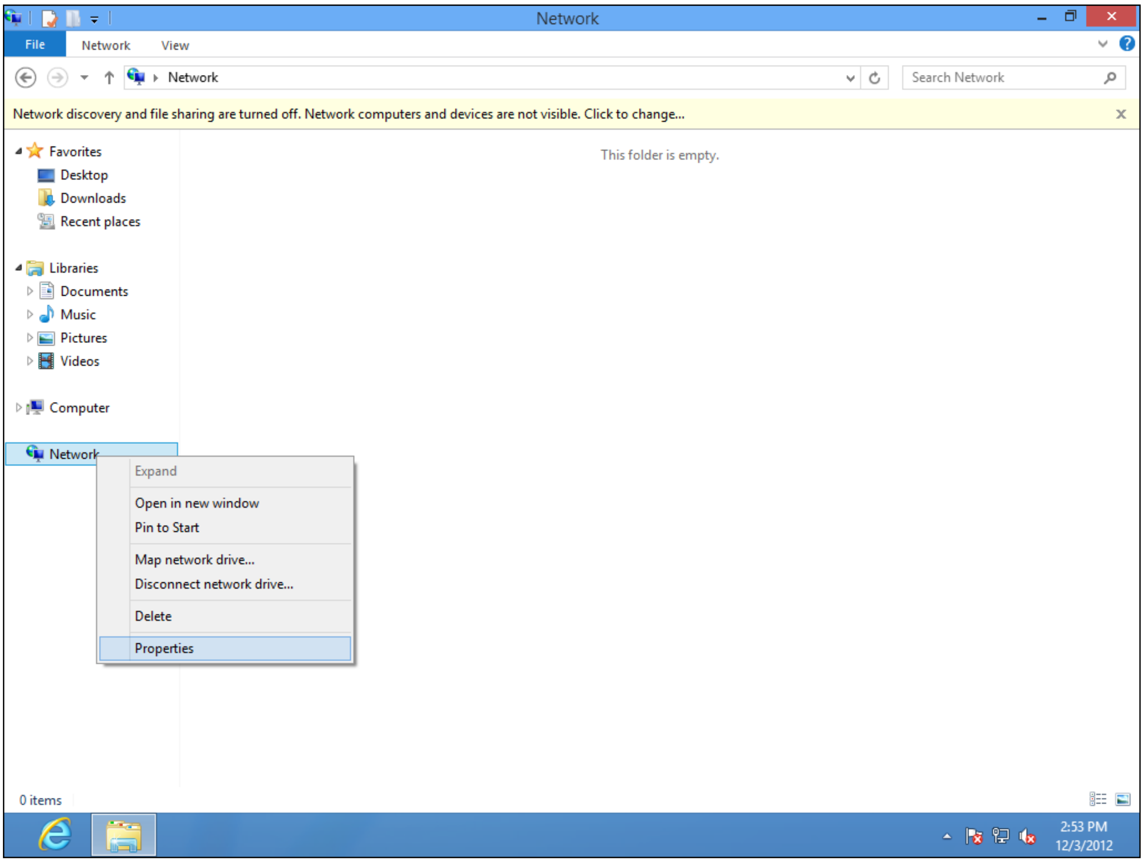
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your curser to the bottom left of the screen and click.



2. In desktop mode, click the File Explorer icon in the bottom left of the screen, as shown below.



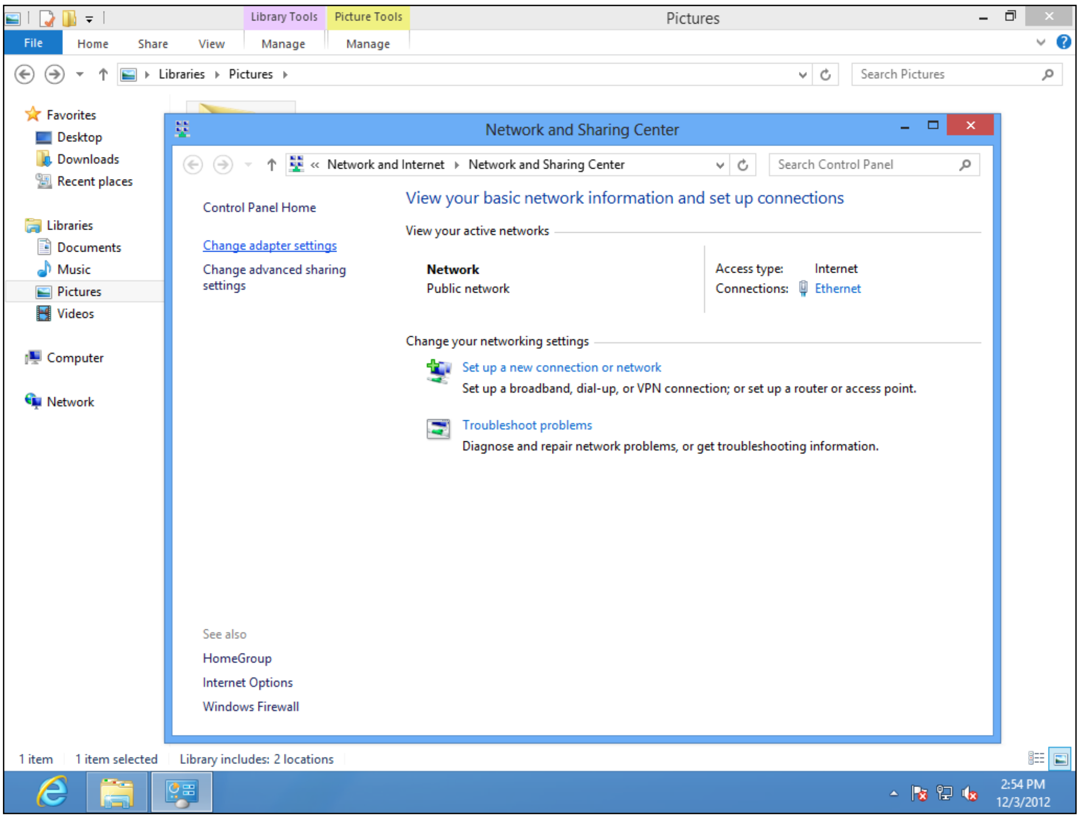
3. Right click “Network” and then select “Properties”.



Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...

This folder is empty.

4. In the window that opens, select “Change adapter settings” from the left side.



View your basic network information and set up connections

View your active networks

Network
Public network

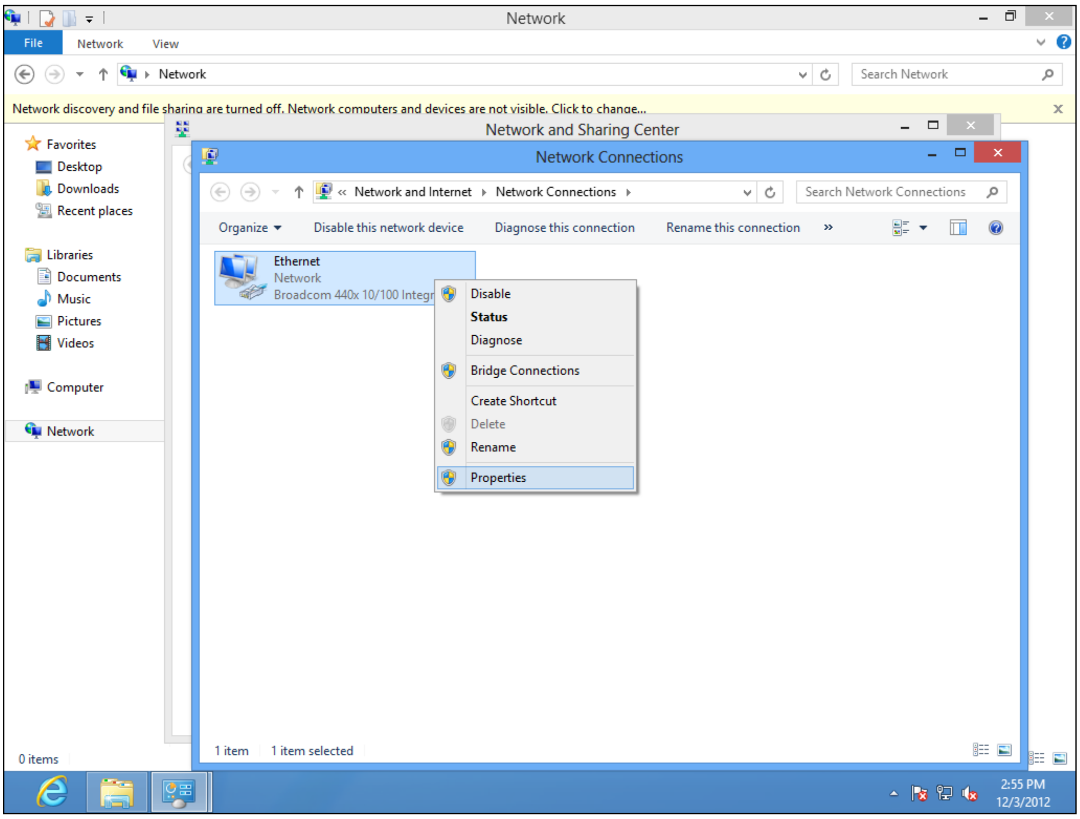
Access type: Internet
Connections: Ethernet

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

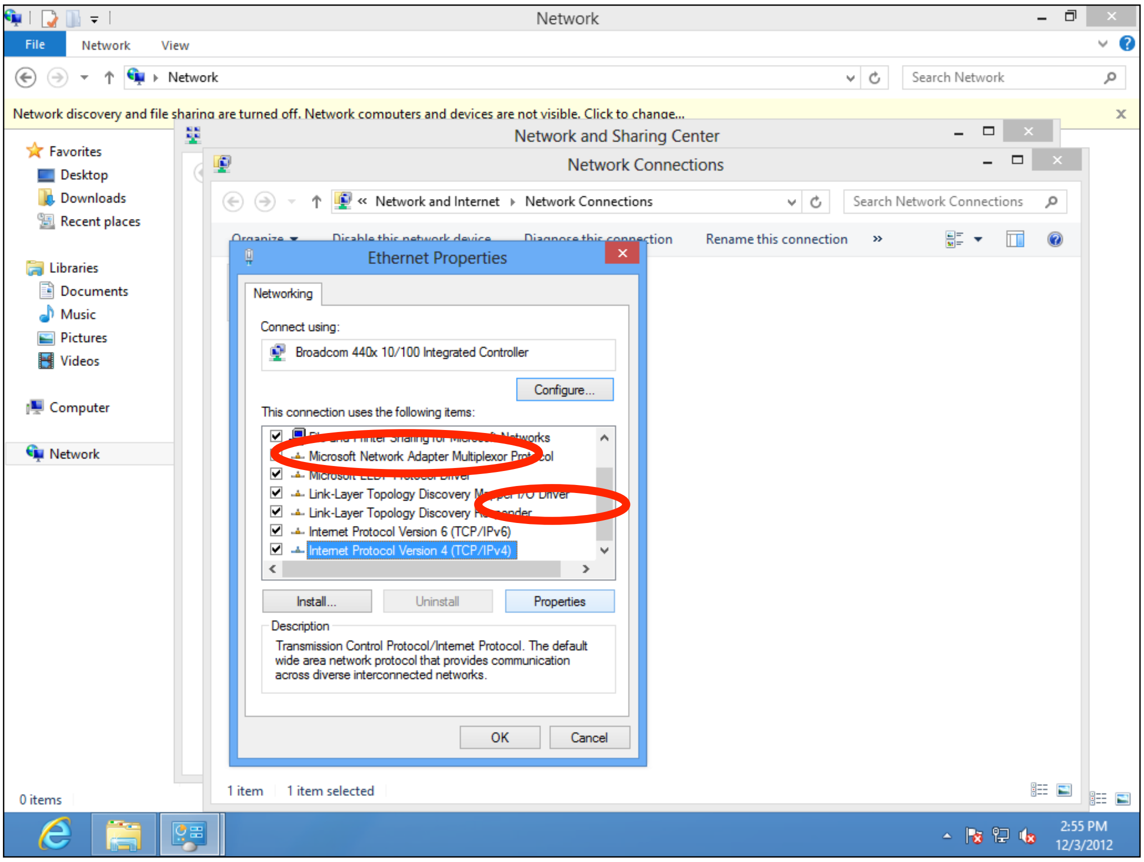
5. Choose your connection and right click, then select “Properties”.



Network discovery and file sharing are turned off. Network computers and devices are not visible. Click to change...

Ethernet
Network
Broadcom 440x 10/100 Integr

6. Select “Internet Protocol Version 4 (TCP/IPv4) and then click “Properties”.



Connect using:

Broadcom 440x 10/100 Integrated Controller

This connection uses the following items:

☑ File and Printer Sharing for Microsoft Networks
☐ Microsoft Network Adapter Multiplexor Protocol
☑ Microsoft LLDP Protocol Driver
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)

Description

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

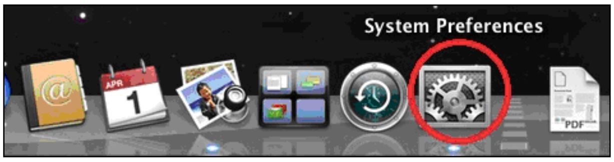
7. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

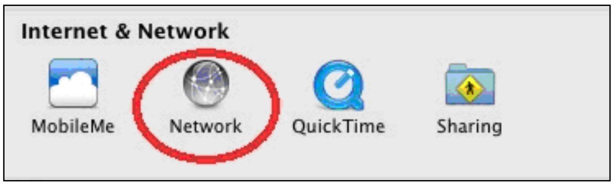
Click ‘OK’ when finished.

II-1-5. Mac

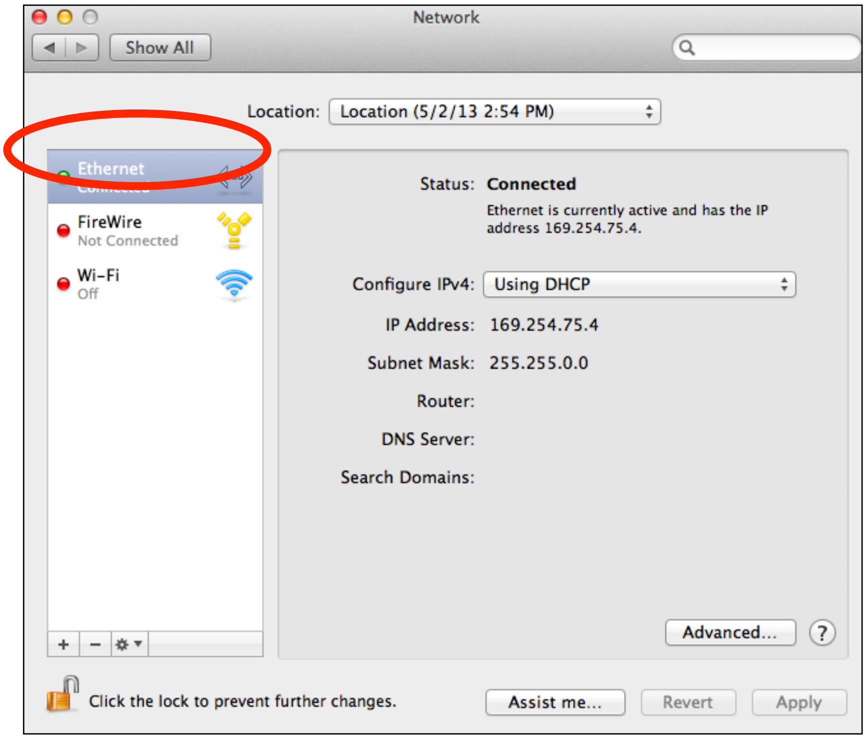
1. Have your Macintosh computer operate as usual, and click on "System Preferences"



2. In System Preferences, click on "Network".



3. Click on "Ethernet" in the left panel.



Location: Location (5/2/13 2:54 PM)

Ethernet
Connected

FireWire
Not Connected

Wi-Fi
Off

Status: **Connected**

Ethernet is currently active and has the IP address 169.254.75.4.

Configure IPv4: Using DHCP

IP Address: 169.254.75.4

Subnet Mask: 255.255.0.0

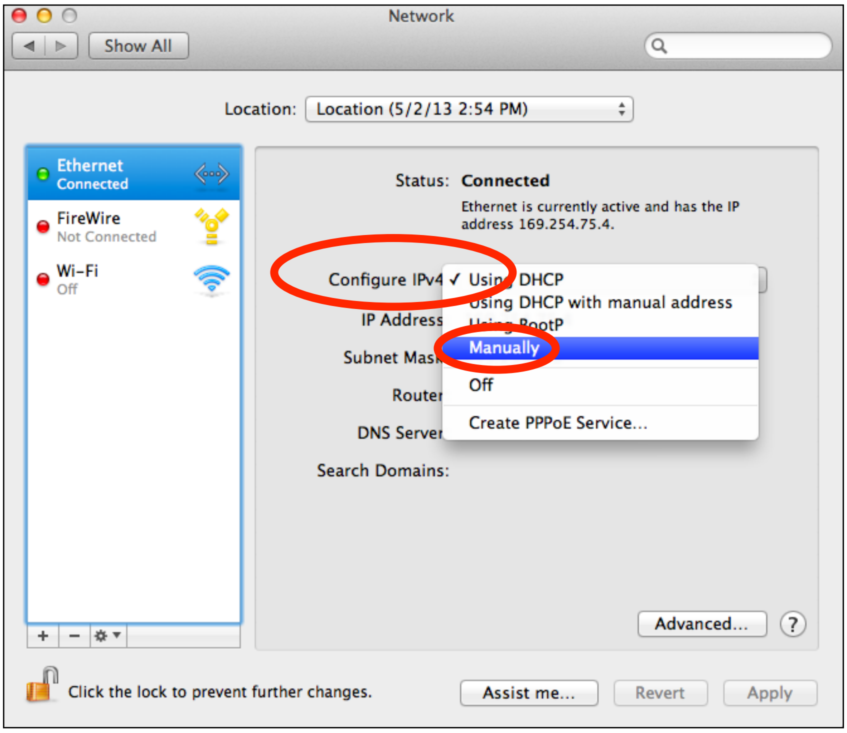
Router:

DNS Server:

Search Domains:

Click the lock to prevent further changes.

4. Open the drop-down menu labeled "Configure IPv4" and select "Manually".



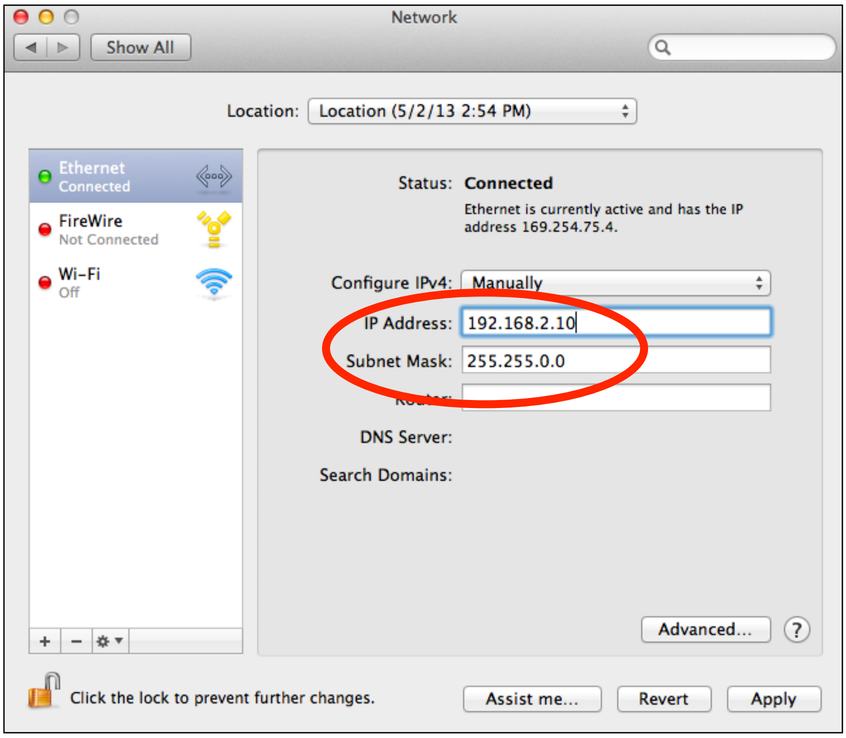
Location: Location (5/2/13 2:54 PM)

Status: Connected

Ethernet is currently active and has the IP address 169.254.75.4.

Configure IPv4: ✓ Using DHCP

5. Enter the IP address 192.168.2.10 and subnet mask 255.255.255.0. Click on "Apply" to save the changes.



Location: Location (5/2/13 2:54 PM)

Status: Connected

Ethernet is currently active and has the IP address 169.254.75.4.

Configure IPv4: Manually

IP Address: 192.168.2.10

Subnet Mask: 255.255.0.0

Router:

DNS Server:

Search Domains:

II-1-6. Glossary

Default Gateway (Access point): Every non-access point IP device needs to configure a default gateway’s IP address. When the device sends out an IP packet, if the destination is not on the same network, the device has to send the packet to its default gateway, which will then send it out towards the destination.

DHCP: Dynamic Host Configuration Protocol. This protocol automatically gives every computer on your home network an IP address.

DNS Server IP Address: DNS stands for Domain Name System, which allows Internet servers to have a domain name (such as www.Broadbandaccess point.com) and one or more IP addresses (such as 192.34.45.8). A DNS server keeps a database of Internet servers and their respective domain names and IP addresses, so that when a domain name is requested (as in typing "Broadbandaccess point.com" into your Internet browser), the user is sent to the proper IP address. The DNS server IP address used by the computers on your home network is the location of the DNS server your ISP has assigned to you.

DSL Modem: DSL stands for Digital Subscriber Line. A DSL modem uses your existing phone lines to transmit data at high speeds.

Ethernet: A standard for computer networks. Ethernet networks are connected by special cables and hubs, and move data around at up to 10/100 million bits per second (Mbps).

IP Address and Network (Subnet) Mask: IP stands for Internet Protocol. An IP address consists of a series of four numbers separated by periods, that identifies a single, unique Internet computer host in an IP network. Example: 192.168.2.2. It consists of 2 portions: the IP network address, and the host identifier.

The IP address is a 32-bit binary pattern, which can be represented as four cascaded decimal numbers separated by “.”: aaa.aaa.aaa.aaa, where each “aaa” can be anything from 000 to 255, or as four cascaded binary numbers separated by “.”: bbbbbbbb.bbbbbbbb.bbbbbbbb.bbbbbbbb, where each “b” can either be 0 or 1.

A network mask is also a 32-bit binary pattern, and consists of consecutive leading 1’s followed by consecutive trailing 0’s, such as 11111111.11111111.11111111.00000000. Therefore sometimes a network mask can also be described simply as “x” number of leading 1’s.
When both are represented side by side in their binary forms, all bits in the IP address that correspond to 1’s in the network mask become part of the IP network address, and the remaining bits correspond to the host ID.

For example, if the IP address for a device is, in its binary form, 11011001.10110000.10010000.00000111, and if its network mask is, 11111111.11111111.11110000.00000000
It means the device’s network address is 11011001.10110000.10010000.00000000, and its host ID is, 00000000.00000000.00000000.00000111. This is a convenient and efficient method for access points to route IP packets to their destination.

ISP Gateway Address: (see ISP for definition). The ISP Gateway Address is an IP address for the Internet access point located at the ISP's office.

ISP: Internet Service Provider. An ISP is a business that provides connectivity to the Internet for individuals and other businesses or organizations.

LAN: Local Area Network. A LAN is a group of computers and devices connected together in a relatively small area (such as a house or an office). Your home network is considered a LAN.

MAC Address: MAC stands for Media Access Control. A MAC address is the hardware address of a device connected to a network. The MAC address is a unique identifier for a device with an Ethernet interface. It is comprised of two parts: 3 bytes of data that corresponds to the Manufacturer ID (unique for each manufacturer), plus 3 bytes that are often used as the product’s serial number.

NAT: Network Address Translation. This process allows all of the computers on your home network to use one IP address. Using the broadband access point’s NAT capability, you can access the Internet from any computer on your home network without having to purchase more IP addresses from your ISP.
Port: Network Clients (LAN PC) uses port numbers to distinguish one network application/protocol over another. Below is a list of common applications and protocol/port numbers:

Application	Protocol	Port Number
Telnet	TCP	23
FTP	TCP	21
SMTP	TCP	25
POP3	TCP	110
H.323	TCP	1720
SNMP	UCP	161
SNMP Trap	UDP	162
HTTP	TCP	80
PPTP	TCP	1723
PC Anywhere	TCP	5631
PC Anywhere	UDP	5632

Access point: A access point is an intelligent network device that forwards packets between different networks based on network layer address information such as IP addresses.

Subnet Mask: A subnet mask, which may be a part of the TCP/IP information provided by your ISP, is a set of four numbers (e.g. 255.255.255.0) configured like an IP address. It is used to create IP address numbers used only within a particular network (as opposed to valid IP address numbers recognized by the Internet, which must be assigned by InterNIC).

TCP/IP, UDP: Transmission Control Protocol/Internet Protocol (TCP/IP) and Unreliable Datagram Protocol (UDP). TCP/IP is the standard protocol for data transmission over the Internet. Both TCP and UDP are transport layer protocol. TCP performs proper error detection and error recovery, and thus is reliable. UDP on the other hand is not reliable. They both run on top of the IP (Internet Protocol), a network layer protocol.

WAN: Wide Area Network. A network that connects computers located in geographically separate areas (e.g. different buildings, cities, countries). The Internet is a wide area network.

Web-based management Graphical User Interface (GUI): Many devices support a graphical user interface that is based on the web browser. This means the user can use the familiar Netscape or Microsoft Internet Explorer to Control/configure or monitor the device being managed.

II-2. ENVIRONMENT & PHYSICAL

Temperature Range	Operation : 0 to 40℃ (32℉ to 104℉) Storage : -20 to 60℃ (-4℉ to 140℉)
Humidity	90% or less – Operating, 90% or less - Storage
Certifications	FCC, CE
Dimensions	6.9(D) x 1.2(H) inches
Weight	10.8 oz.

COPYRIGHT

This company 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 this company, 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, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

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

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter. 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, and (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 authority to operate equipment.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 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.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Bulgaria, Cyprus, Czech, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Turkey, and United Kingdom. The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not Intended for Use

None