COMTREND

WAP-EN300C N300 Ceiling Mount Access Point

User Manual

Version 1.0, June 1, 2016

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

Copyright© 2015 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without the prior written consent of Comtrend Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/

NOTE: This document is subject to change without notice.

Protect Our Environment

This symbol indicates that when the equipment has reached the end of
it’s 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

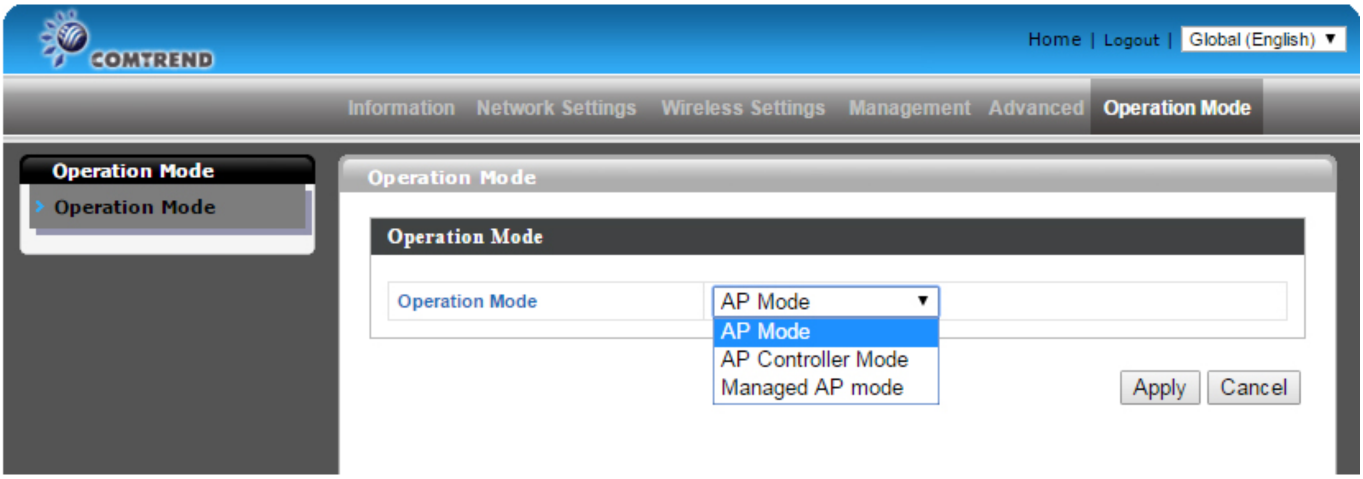
Your access point can function in three different modes.

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

AP Mode is a regular access point for your network.

AP Controller Mode acts as a designated “Master” for an array of “Slave” access points. (Group of linked access points)

Managed AP Mode acts like a “Slave” access point in an access point array. (Controlled by the AP Controller “Master”)



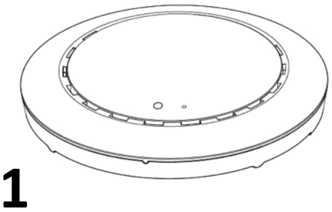
Operation Mode: AP Mode ▼ (AP Mode / AP Controller Mode / Managed AP mode)

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

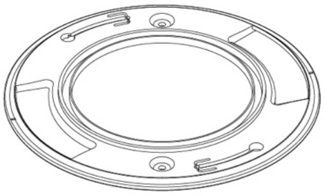
This manual covers **AP Mode. Controller Mode** is covered in the NMS manual.   Both manuals are available on the CD that came with your product and are available online.

I. Product Information

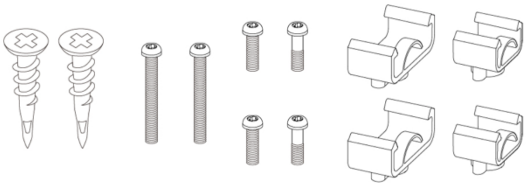
I-1. Package Contents



1

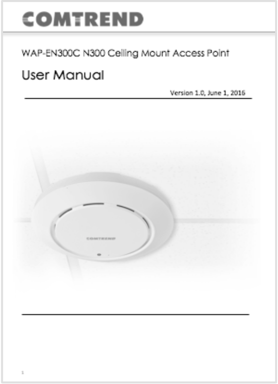


2



3

4



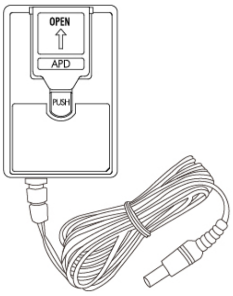
COMTREND

WAP-EN300C N300 Ceiling Mount Access Point

User Manual

Version 1.0, June 1, 2016

5

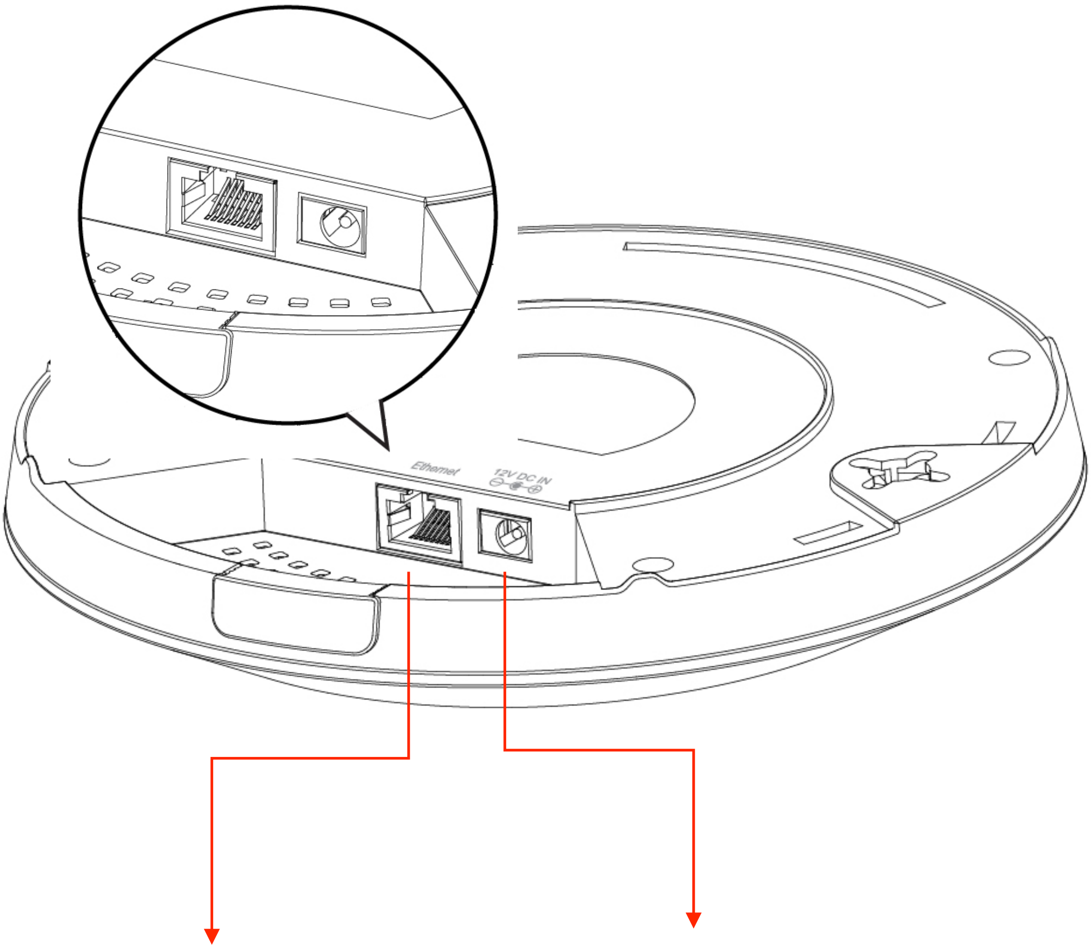


1. Access Point
2. Ceiling Mount Bracket
3. T-Rail Mounting Kit & Screws
4. Quick Installation Guide
5. Power Adapter

I-2. System Requirements

- Existing cable/DSL modem & router
- Computer with web browser for access point configuration

I-3. Hardware Overview



Ethernet Port

Power Port

I-4. LED Status

Blue	Amber	Status
Off	Off	AP is off
On	On	Booting up, Going to Reboot
On	Off	AP is up and every function working properly
Long Flashing	OFF	Firmware upgrading
Short Flashing	Off	Ready to reset to factory default
Off	Flashing	Error

I-5. Reset

If you experience problems with your access point, you can reset the device back to its factory settings. This resets **all** settings back to default.

1. Press and hold the reset button on the access point for at least 10 seconds then release the button.

You may need to use a pencil or similar sharp object to push the reset button.

2. Wait for the access point to restart. The access point is ready for setup when the LED is **blue**.

I-6. Safety Information

In order to ensure the safe operation of the device and its users, read and act in accordance with the following safety instructions.

1. The access point is designed for indoor use only; do not place the access point outdoors.

2. Do not place the access point in or near hot/humid places, such as a kitchen or bathroom.

3. Do not pull any connected cable with force; carefully disconnect it from the access point.

4. Handle the access point with care. Accidental damage will void the warranty of the access point.

5. The device contains small parts which are a danger to small children under 3 years old. Keep the access point out of reach of children.

6. Do not place the access point on paper, cloth, or other flammable materials. The access point may become hot during use.

7. There are no user-serviceable parts inside the access point. If you experience problems with the access point, contact your dealer of purchase and ask for help.

8. The access point is an electrical device and as such, if it becomes wet for any reason, do not attempt to touch it without switching the power supply off. Contact an experienced electrical technician for further help.

9. If you smell burning or see smoke coming from the access point or power adapter, then disconnect the access point and power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

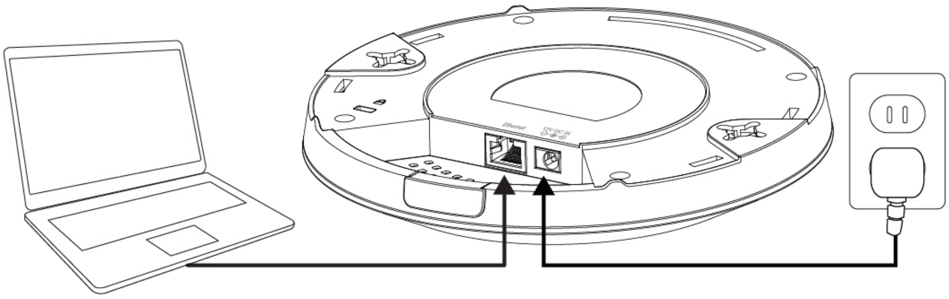
II. Quick Setup

Follow the instructions in the chapters below to setup your access point and then configure its basic settings.

II-1. Initial Setup

1. Connect the access point to a computer via Ethernet cable.

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



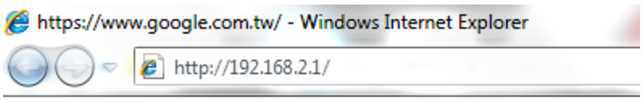
/

3. Wait a moment for the access point to start up. The access point is ready when the LED is **blue**.

4. Set your computer's IP address to **192.168.2.x** where **x** is a number in the range **3 – 100**. If you are unsure how to do this, refer to **V-1. Configuring your IP address** for more information.

> ***Ensure there are no other active network connections on your computer (disconnect Wi-Fi connections and Ethernet cables).***

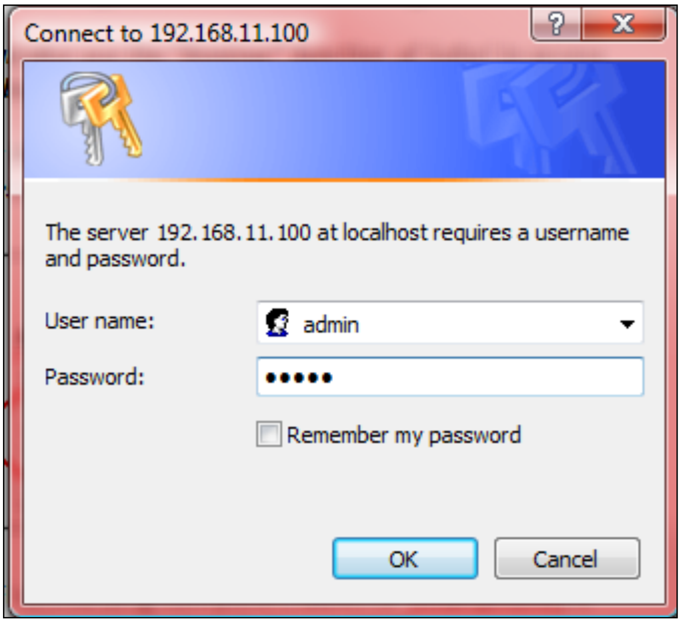
5. Enter the access point's default IP address **192.168.2.1** into the URL bar of a web browser.



https://www.google.com.tw/ - Windows Internet Explorer

http://192.168.2.1/

6. You will be prompted for a username and password. Enter the default username "admin" and the default password "admin".



Connect to 192.168.11.100

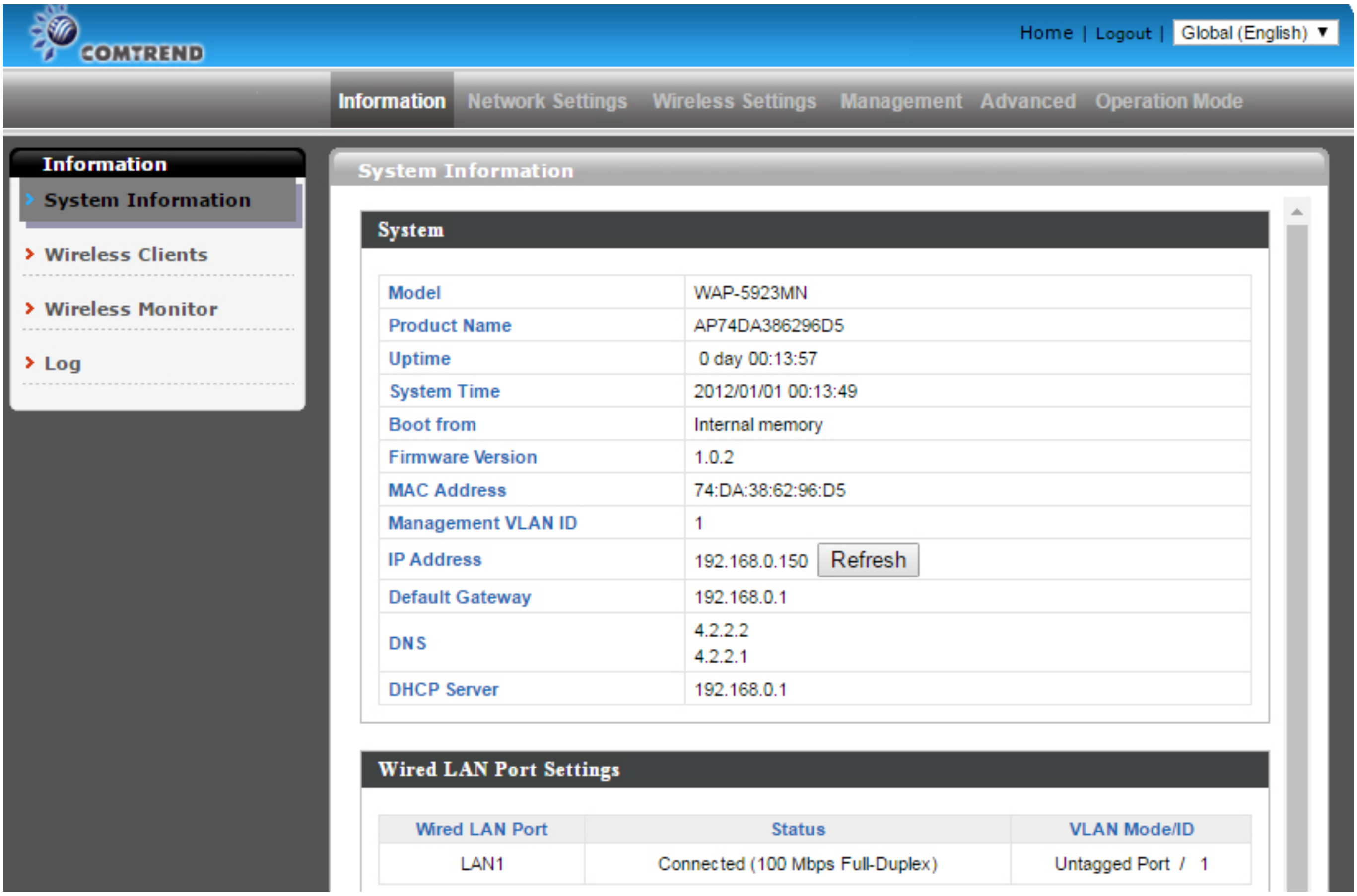
The server 192.168.11.100 at localhost requires a username and password.

User name: admin

Password: •••••

□ Remember my password

7. You will arrive the "System Information" screen shown below.



System Information

System

Model	WAP-5923MN
Product Name	AP74DA386296D5
Uptime	0 day 00:13:57
System Time	2012/01/01 00:13:49
Boot from	Internal memory
Firmware Version	1.0.2
MAC Address	74:DA:38:62:96:D5
Management VLAN ID	1
IP Address	192.168.0.150 Refresh
Default Gateway	192.168.0.1
DNS	4.2.2.2 4.2.2.1
DHCP Server	192.168.0.1

Wired LAN Port Settings

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

8. Next, follow the instructions below in **II-1. Basic Settings** to configure the access point's basic settings.

For more advanced configurations, refer to IV. Browser Based Configuration Interface.

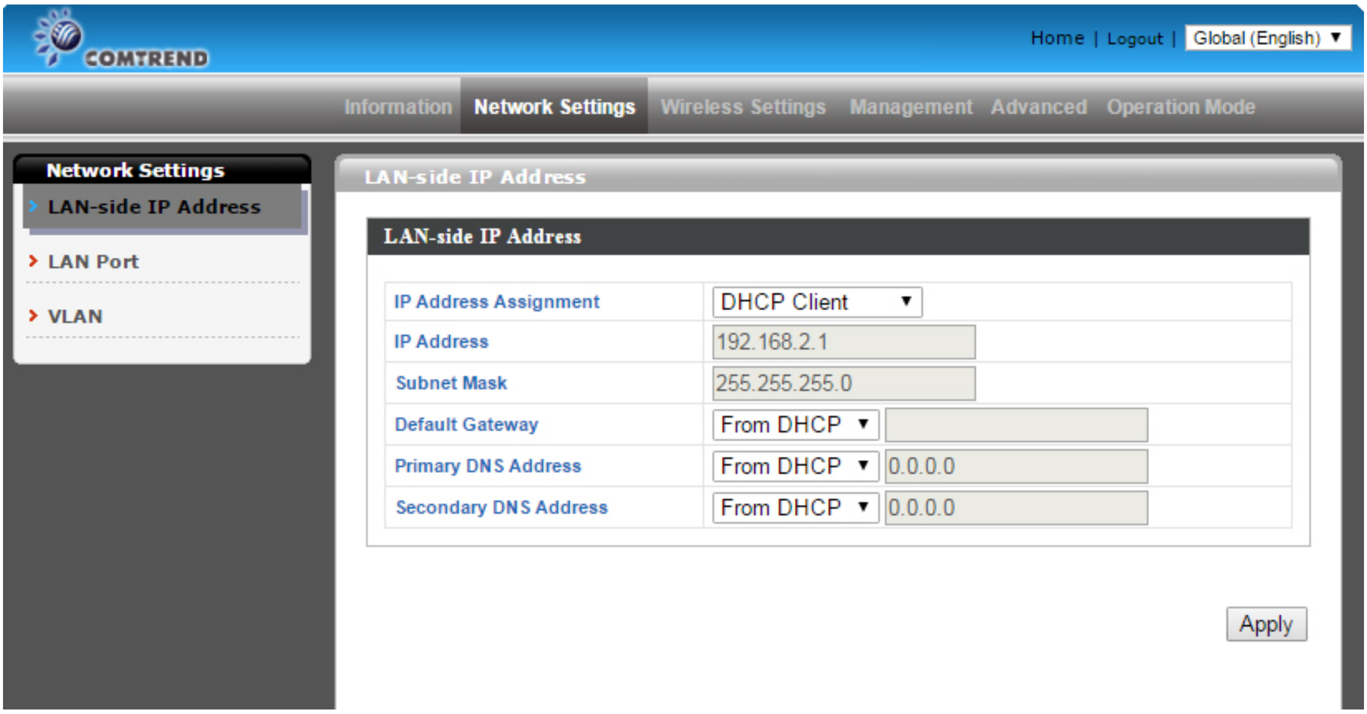
II-2. Basic Settings

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

It is recommended you configure these settings before using the access point.

- ***LAN IP Address***
- ***SSID & Security***
- ***Login Password***
- ***Time & Date***

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



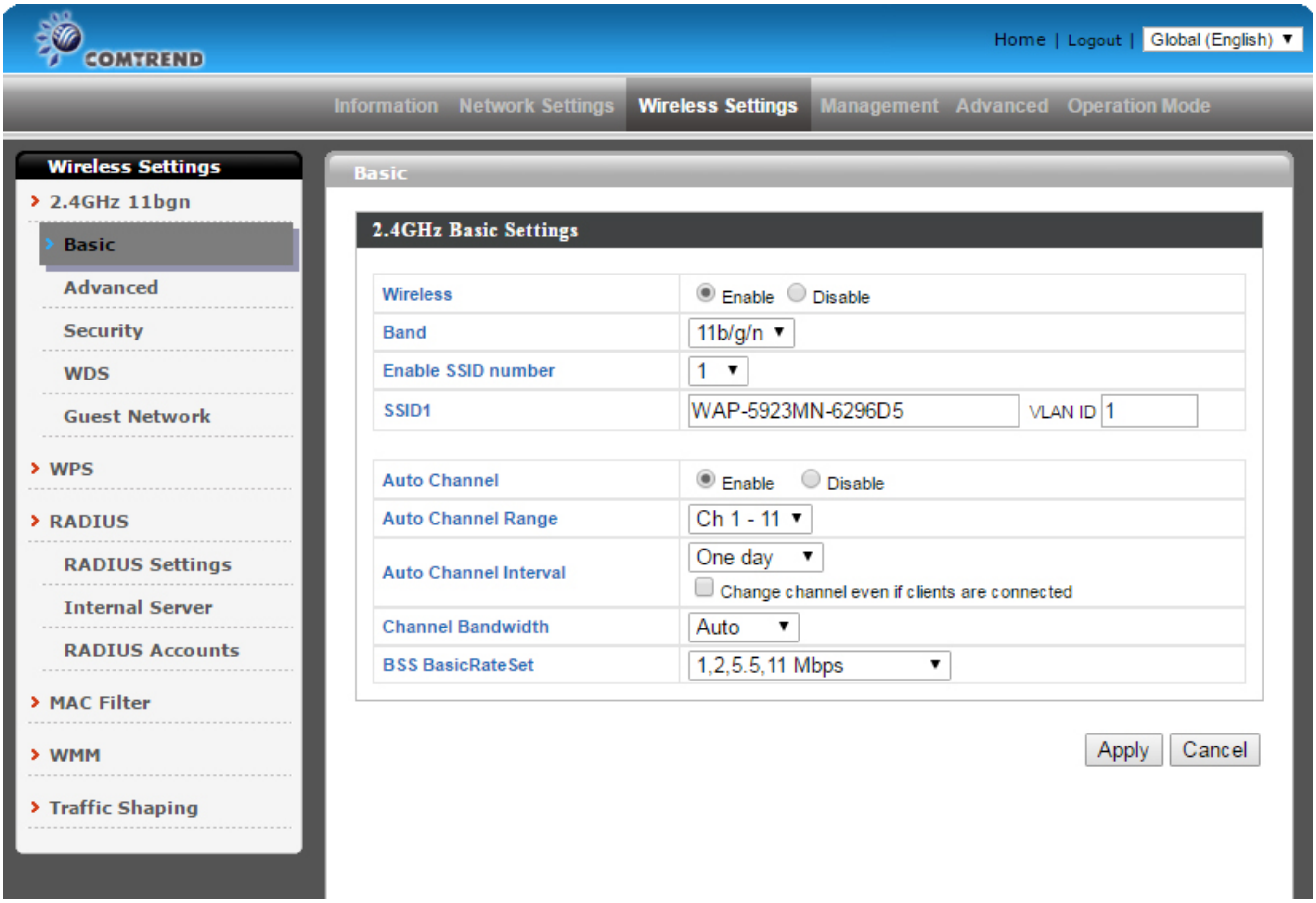
LAN-side IP Address

IP Address Assignment	DHCP Client ▼	
IP Address	192.168.2.1	
Subnet Mask	255.255.255.0	
Default Gateway	From DHCP ▼	
Primary DNS Address	From DHCP ▼	0.0.0.0
Secondary DNS Address	From DHCP ▼	0.0.0.0

2. Enter the IP address settings you wish to use for your access point. Click "Apply" to save the changes the wait a few moments for the access point to reload.

When you change your access point's IP address, you need to use the new IP address to access the browser based configuration interface instead of the default IP *192.168.2.1.*

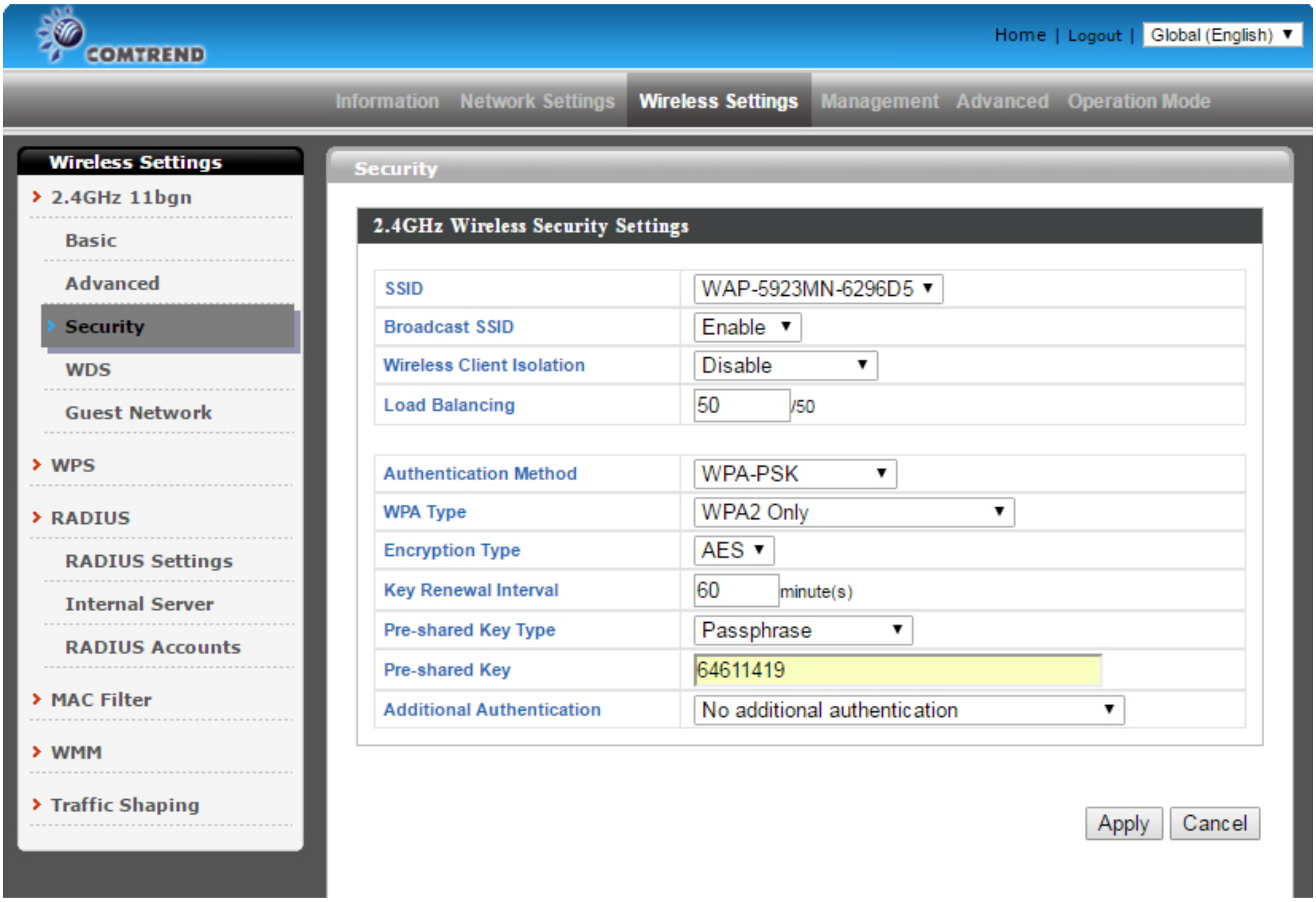
3. To change the SSID and password of your access point's wireless network(s), go to **"Wireless Setting" > "2.4GHz" > "Basic"**. Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field and click "Apply".



2.4GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11b/g/n ▼
Enable SSID number	1 ▼
SSID1	WAP-5923MN-6296D5 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 ▼

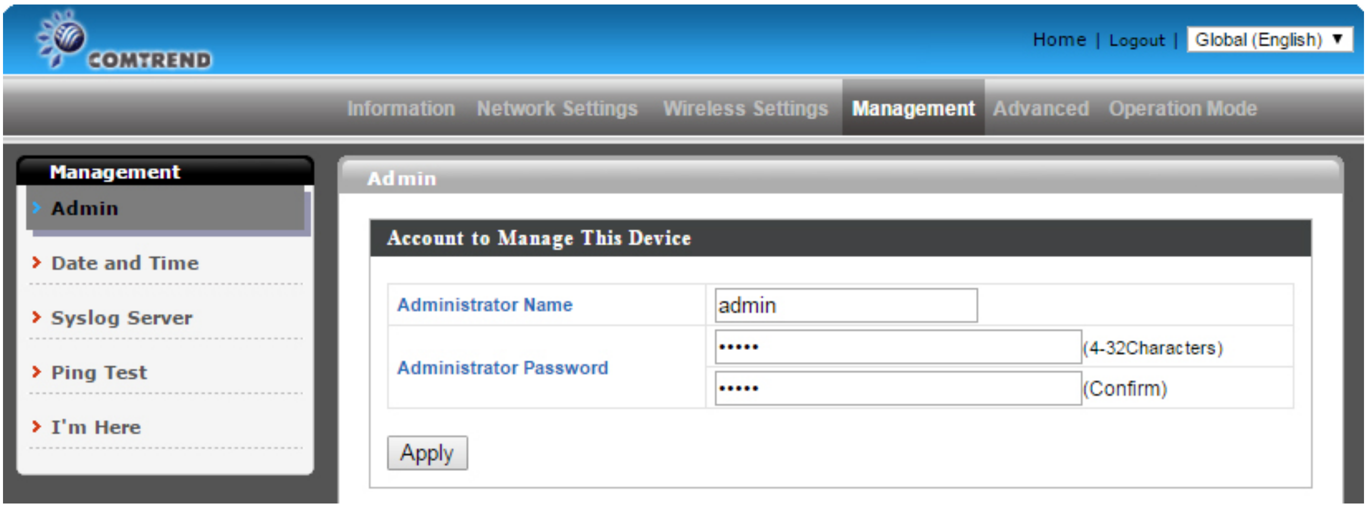
4. Go to **"Wireless Setting" > "2.4GHz" > "Security"**. Enter a new password for your 2.4GHz wireless network in the "Pre-shared Key" field and click "Apply".



2.4GHz Wireless Security Settings

SSID	WAP-5923MN-6296D5
Broadcast SSID	Enable
Wireless Client Isolation	Disable
Load Balancing	50 /50
Authentication Method	WPA-PSK
WPA Type	WPA2 Only
Encryption Type	AES
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase
Pre-shared Key	64611419
Additional Authentication	No additional authentication

5. To change the login password for the browser based configuration interface, go to **"Management" > "Admin"**.

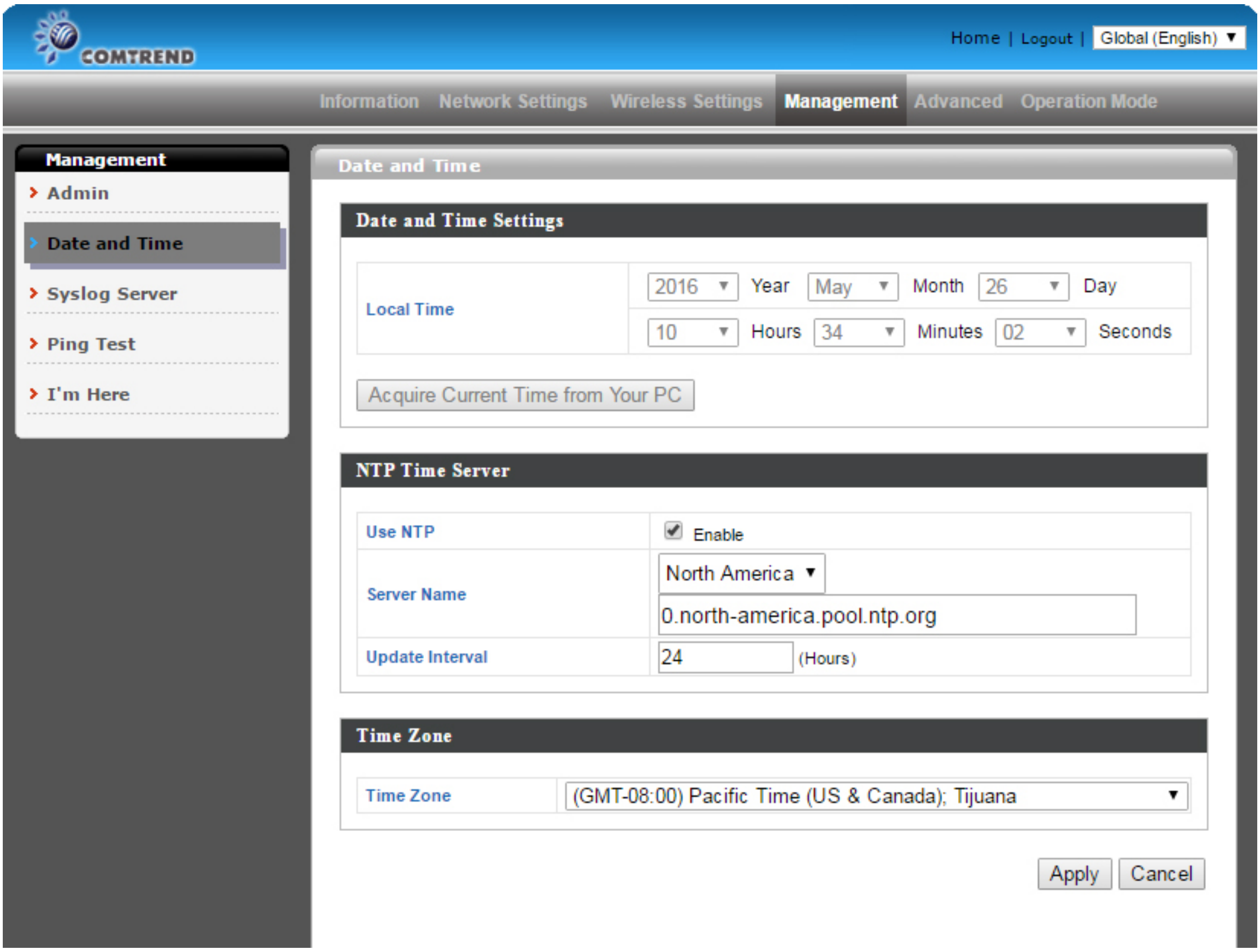


Account to Manage This Device

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

6. Complete the “Administrator Name”, “Administrator Password” and “Confirm” fields and click “Apply”.

7. To set the correct time for your access point, go to **“Management” > “Date and Time”**.



COMTREND
Home | Logout | Global (English) ▼
Information Network Settings Wireless Settings Management Advanced Operation Mode
Management
Admin
Date and Time
Syslog Server
Ping Test
I'm Here

Date and Time

Date and Time Settings

Local Time: 2016 Year, May Month, 26 Day; 10 Hours, 34 Minutes, 02 Seconds

Acquire Current Time from Your PC

NTP Time Server

Use NTP: ☑ Enable

Server Name: North America ▼ 0.north-america.pool.ntp.org

Update Interval: 24 (Hours)

Time Zone

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana ▼

Apply Cancel

8. Select the correct time zone for your access point from the drop down list. The access point also supports NTP (Network Time Protocol) so alternatively you can enter the host name or IP address of a time server. Click “Apply” when you are finished.

9. The basic settings of your access point are now configured. Refer to **III. Hardware Installation** for guidance on connecting your access point to a router or PoE switch and/or fixing your access point to a ceiling. Or refer to **IV. Browser Based Configuration Interface** for help with advanced configurations.

II-3. Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices.

After you have set up the access point as explained in **II. Quick Setup** you can use the WPS button to establish a connection between the access point and a WPS-compatible wireless device/client.

1. Press and hold the WPS/Reset button on the front of the access point for 2 seconds.

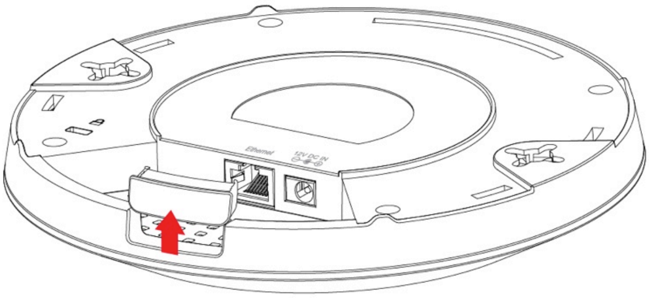
2. Within two minutes, activate WPS on your WPS-compatible wireless device. Check the documentation for your wireless device for information regarding its WPS function.

3. The devices will establish a connection.

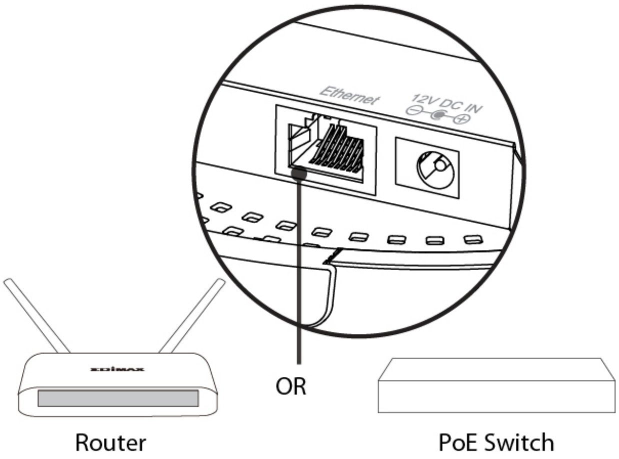
III. Hardware Installation

III-1. Connecting the access point to a router or PoE switch

1. If you need to, remove the cap from the underside of the access point. This creates extra space for your cables to pass through.

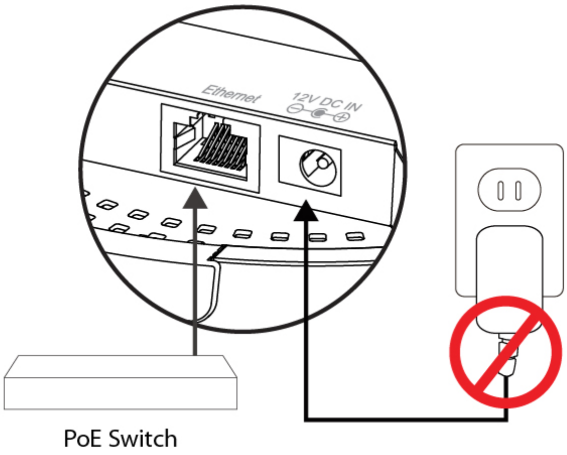


2. Connect a router or PoE switch to the access point's **LAN** port using an Ethernet cable.



3. If you are using a router, then connect the power adapter to the access point's 12V DC port and plug the power adapter into a power supply.

4. If you are using a PoE (Power over Ethernet) switch then it is not necessary to use the included power adapter, the access point will be powered by the PoE switch.



III-2. Mounting the access point to a ceiling

To mount the access point to a ceiling, follow the instructions below and refer to diagram **A** & **B**.

For Wooden Ceilings (refer to diagram A):

1. Place the ceiling mount bracket to a ceiling in your desired location and insert screw **iii** through hole **i** (x 2)and tighten to fix the bracket in place.

2. When the ceiling bracket is in place, inset screw **iv** into hole **v** (x 2) on the access point.

3. Fix the access point to the ceiling bracket by inserting the attached screws **iv** into hole **vi** and twisting the access point.

4. Lock the access point firmly into place when by twisting it to align screws **iv** with the grooves in the ceiling mount.

For Other Ceilings (refer to diagram B):

1. Place the ceiling mount bracket to a ceiling in your desired location and Insert screw **ii** through hole **i** (x 2) and tighten to fix the bracket in place, as shown in **A**.

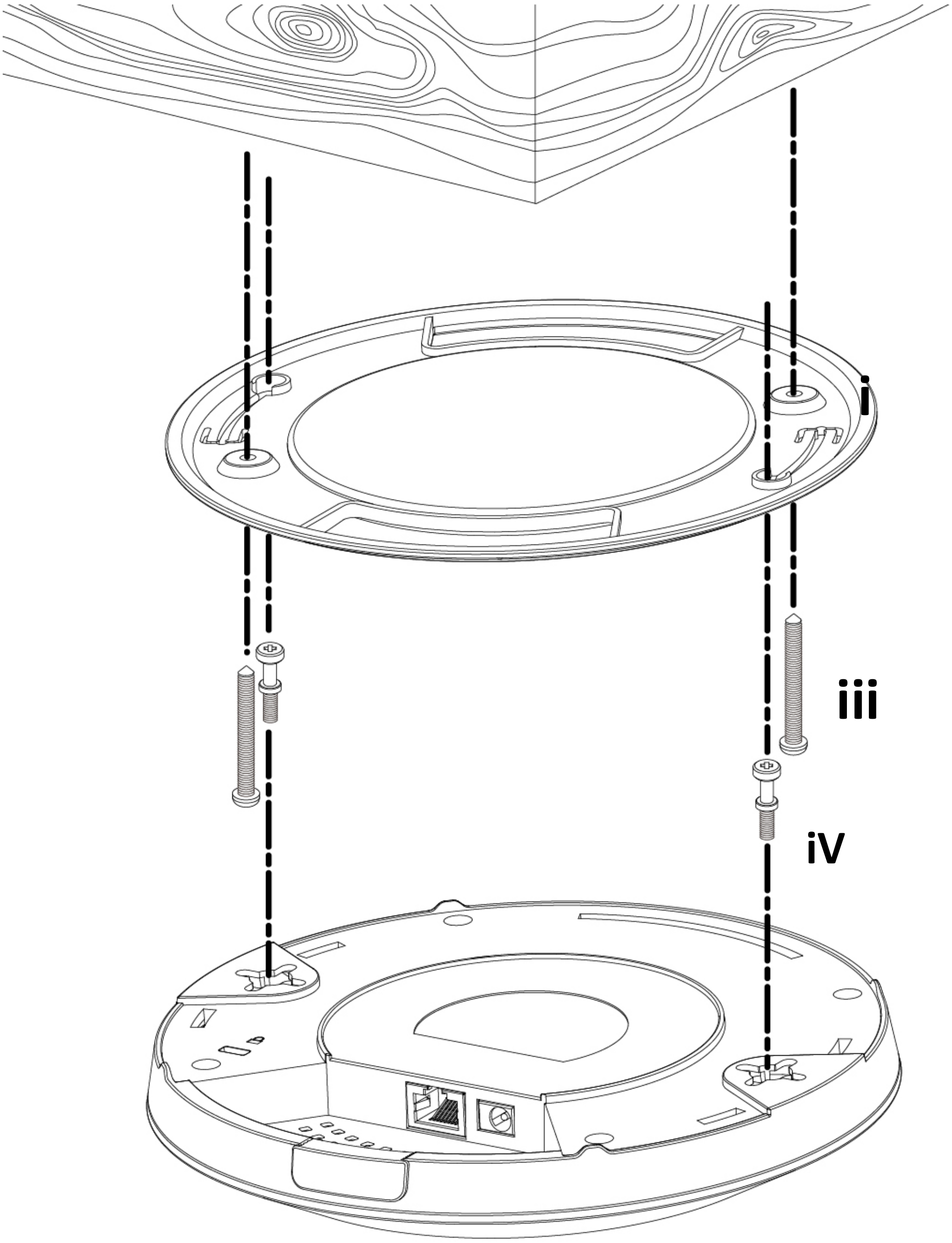
2. Insert screw **iii** through hole **i** and into the rear of screw ii and tighten to provide additional strength.

3. When the ceiling bracket is in place, insert screw **iv** into hole **v** (x 2) on the access point.

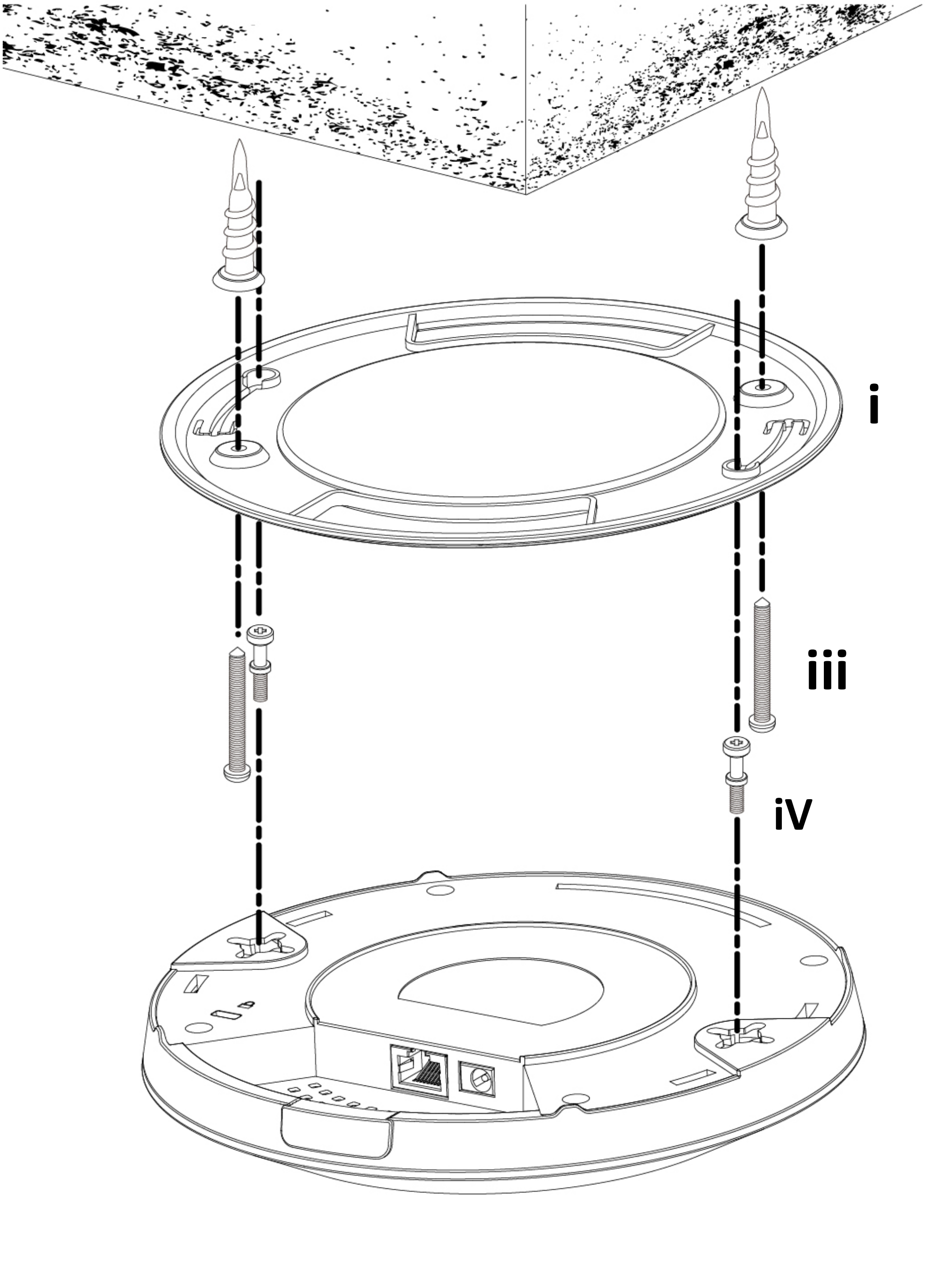
5. Fix the access point to the ceiling bracket by inserting the attached screws **iv** into hole **vi** and twisting the access point.

6. Lock the access point firmly into place by twisting it to align screws **iv** with the grooves in the ceiling mount.

A



B



III-3. T-Rail Mount

To mount the access point to a T-Rail, follow the instructions below and refer to diagram **C, D** & **E**.

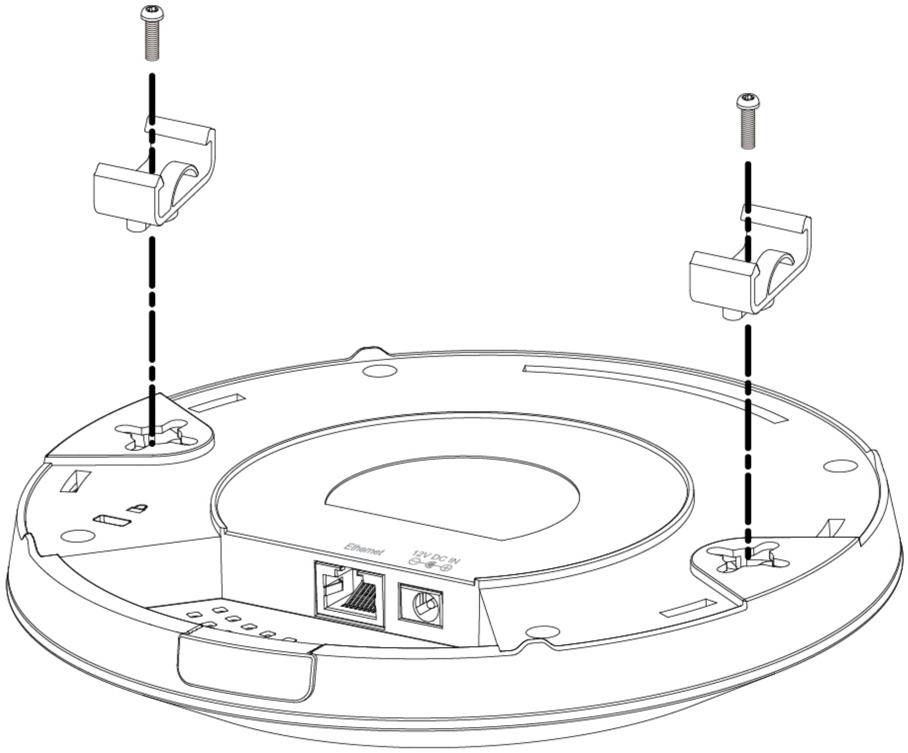
1. Select the correct size T-Rail bracket from the two sizes which are included in the package contents.

2. Attach the T-Rail bracket **i** to hole **ii** using screw **iii** (x 2) as shown in **C**.

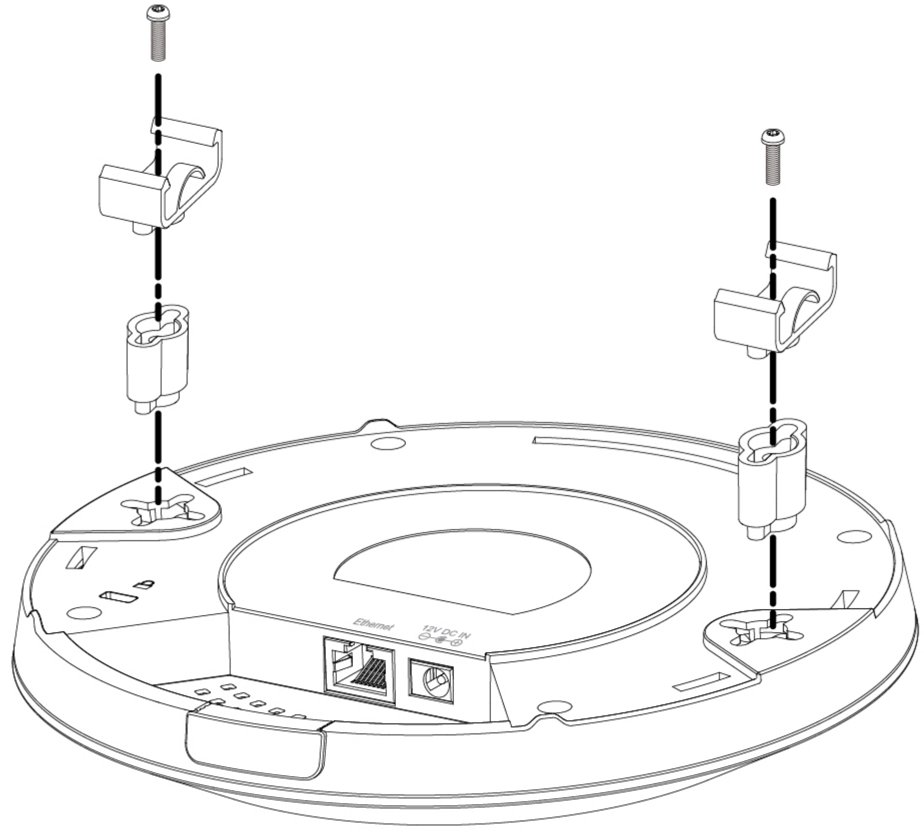
If you need more space between the access point and the T-Rail, then additionally use bracket *iv* ***between bracket*** *i* ***and hole*** *ii (x 2)**, and use the longer screws (x 2) included in the package contents.***

3. Clip the access point onto your T-Rail using the now attached T-Rail bracket.

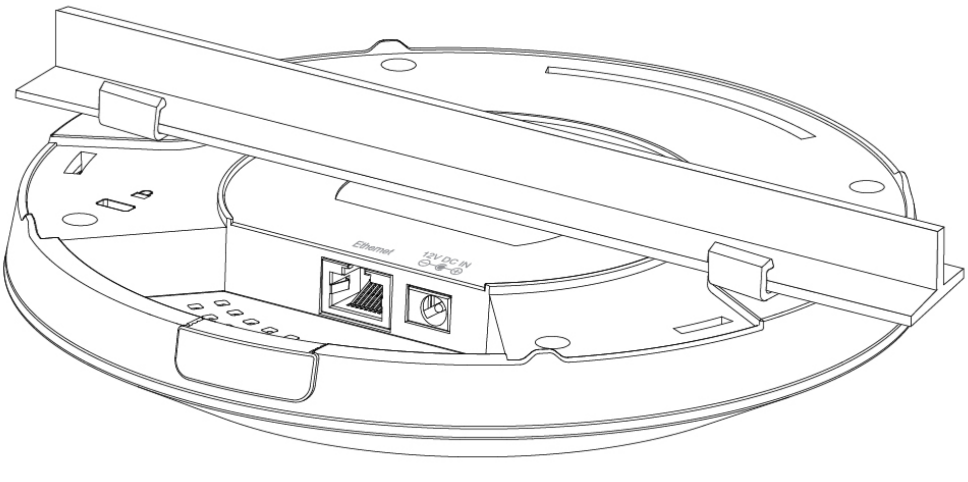
C



D



E



IV. Browser Based Configuration Interface

You can use the browser-based configuration interface to configure advanced settings.

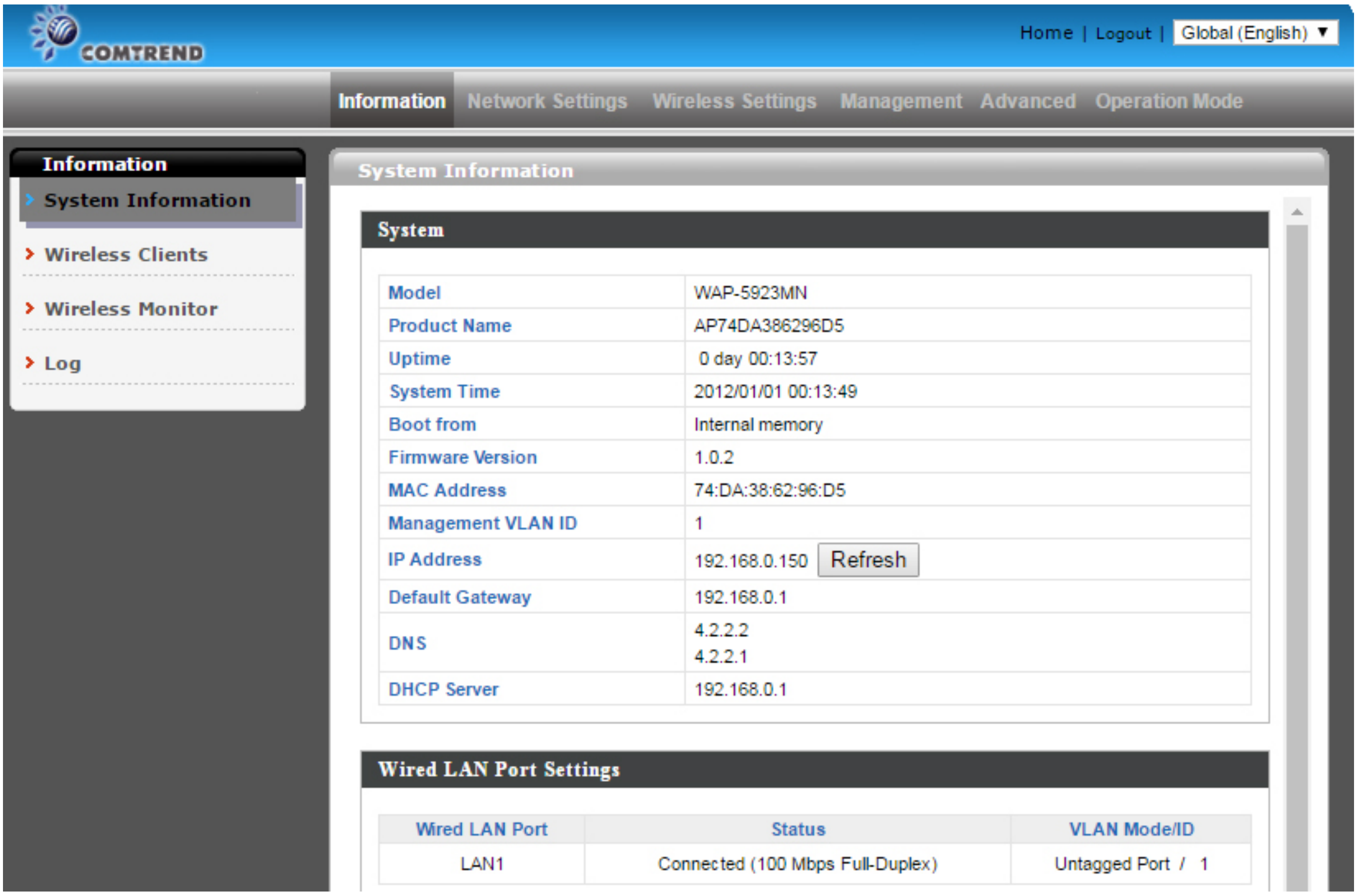
1. Connect a computer to your access point using an Ethernet cable.

2. Enter your access point's IP address in the URL bar of a web browser. The access point's default IP address is **192.169.2.2.**

3. You will be prompted for a username and password. The default username is "admin" and the default password is "admin", though it was recommended that you change the password during setup (see **II-2. Basic Settings**).

> ***If you cannot remember your password, reset the access point back to its factory default settings. Refer to*** *I-5. Reset*

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



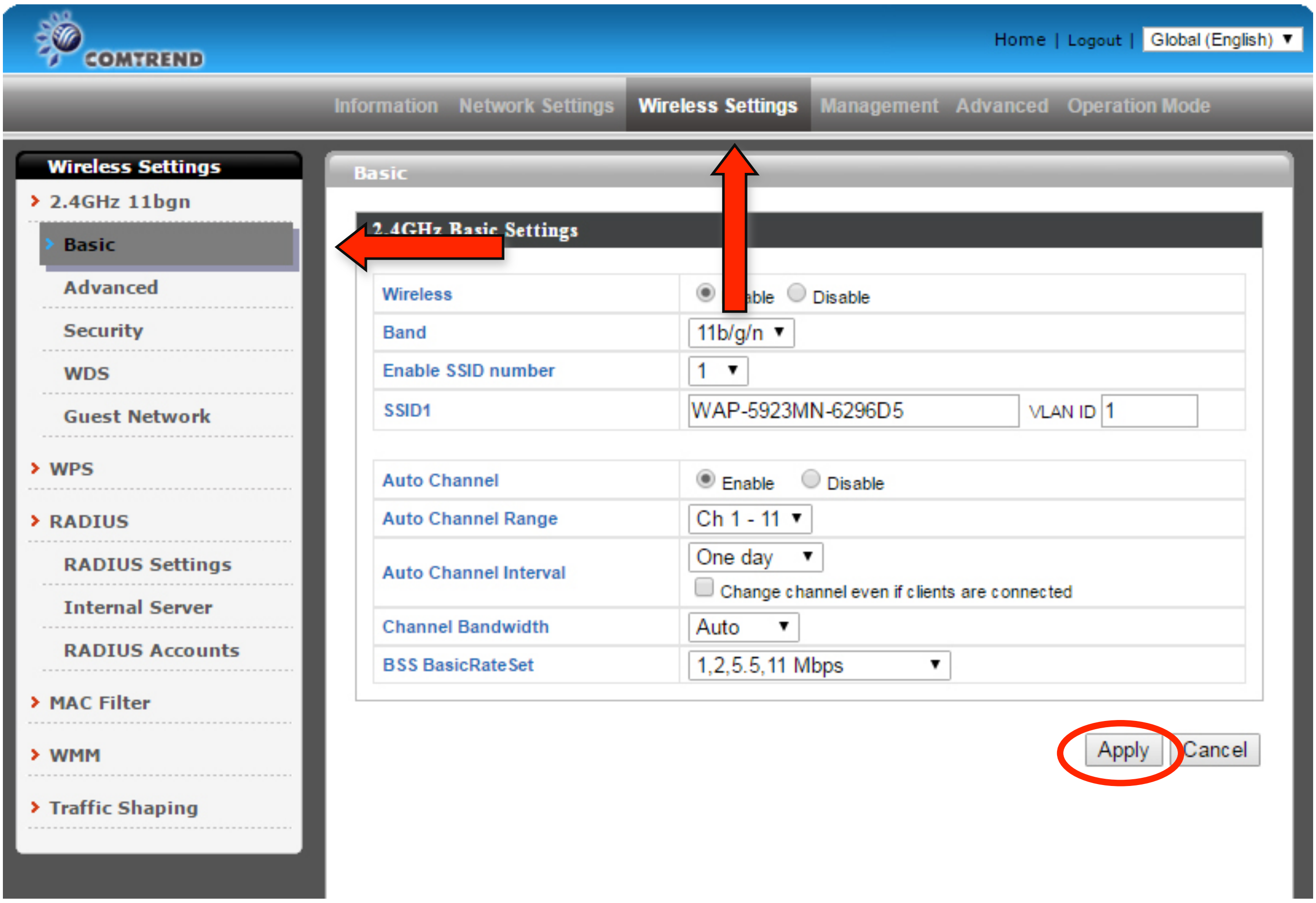
System

Model	WAP-5923MN
Product Name	AP74DA386296D5
Uptime	0 day 00:13:57
System Time	2012/01/01 00:13:49
Boot from	Internal memory
Firmware Version	1.0.2
MAC Address	74:DA:38:62:96:D5
Management VLAN ID	1
IP Address	192.168.0.150
Default Gateway	192.168.0.1
DNS	4.2.2.2 4.2.2.1
DHCP Server	192.168.0.1

Wired LAN Port Settings

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

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



2.4GHz Basic Settings

Wireless	● able ○ Disable
Band	11b/g/n
Enable SSID number	1
SSID1	WAP-5923MN-6296D5 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

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

⚠ ***Wait a few seconds for the access point to reload after you "Apply" changes, as shown below.***

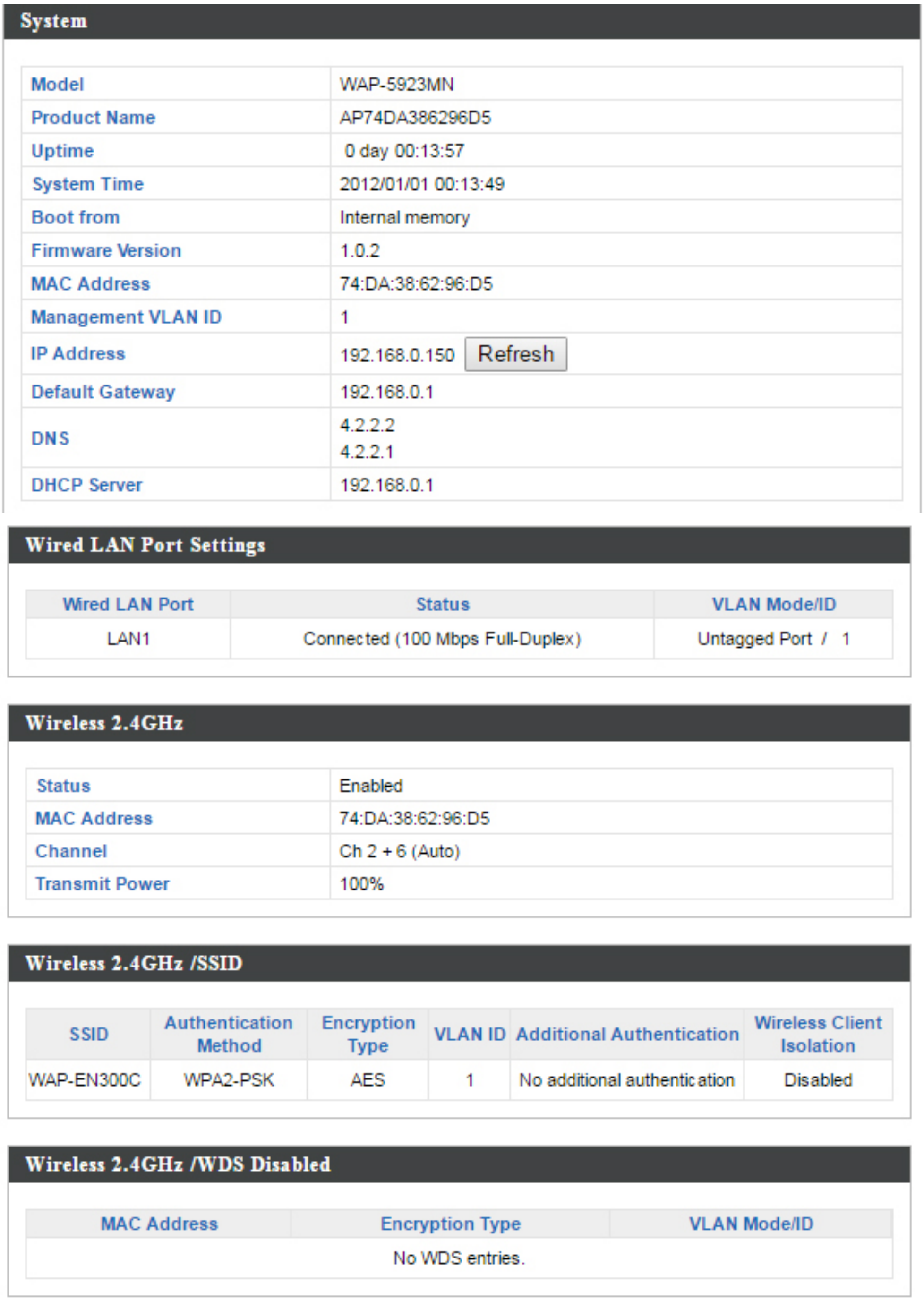
7. Refer to the following chapters for full descriptions of the browser based configuration interface features.

IV-1. Information

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

IV-1-1. System Information

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



System

Model	WAP-5923MN
Product Name	AP74DA386296D5
Uptime	0 day 00:13:57
System Time	2012/01/01 00:13:49
Boot from	Internal memory
Firmware Version	1.0.2
MAC Address	74:DA:38:62:96:D5
Management VLAN ID	1
IP Address	192.168.0.150 Refresh
Default Gateway	192.168.0.1
DNS	4.2.2.2 4.2.2.1
DHCP Server	192.168.0.1

Wired LAN Port Settings

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

Wireless 2.4GHz

Status	Enabled
MAC Address	74:DA:38:62:96:D5
Channel	Ch 2 + 6 (Auto)
Transmit Power	100%

Wireless 2.4GHz /SSID

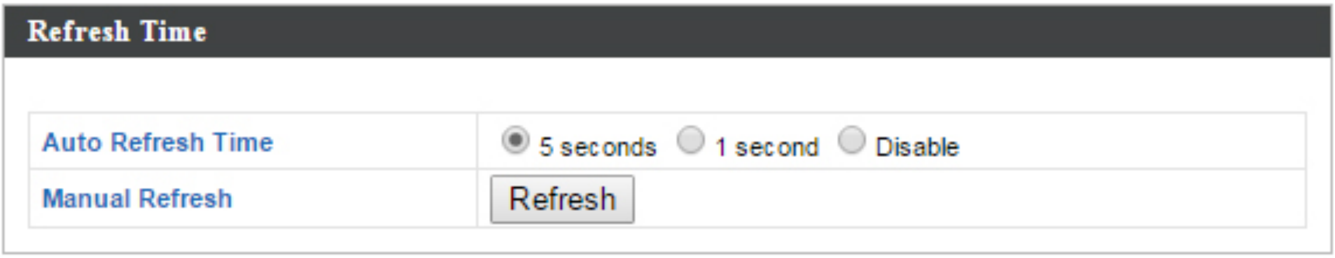
SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
WAP-EN300C	WPA2-PSK	AES	1	No additional authentication	Disabled

Wireless 2.4GHz /WDS Disabled

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

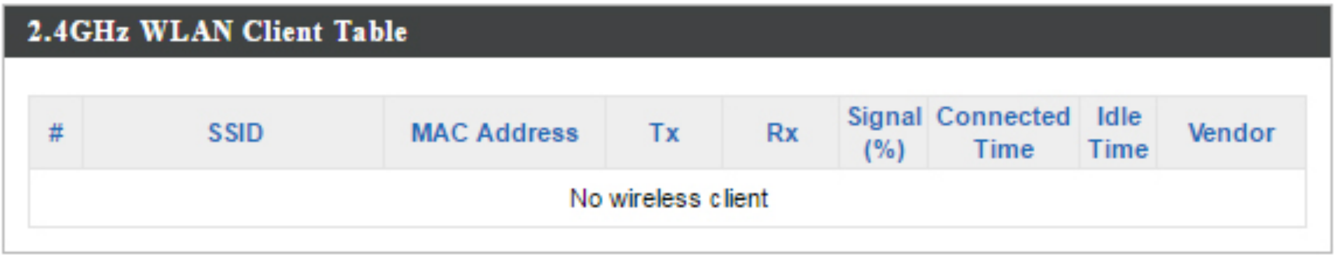
IV-1-2. Wireless Clients

The “Wireless Clients” page displays information about all wireless clients connected to the access point on the 2.4GHz frequency.



Refresh Time

Auto Refresh Time	● 5 seconds ○ 1 second ○ Disable
Manual Refresh	Refresh



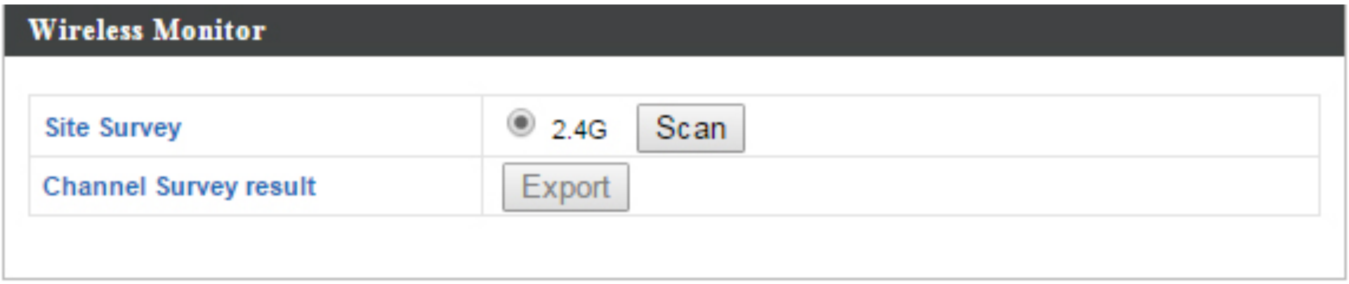
2.4GHz WLAN Client Table

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

2.4GHz WLAN Client Table	
SSID	Displays the SSID which the client is connected to.
MAC Address	Displays the MAC address of the client.
Tx	Displays the total data packets transmitted by the specified client.
Rx	Displays the total data packets received by the specified client.
Signal (%)	Displays the wireless signal strength for the specified client.
Connected Time	Displays the total time the wireless client has been connected to the access point.
Idle Time	Client idle time is the time for which the client has not transmitted any data packets i.e. is idle.
Vendor	The vendor of the client’s wireless adapter is displayed here.

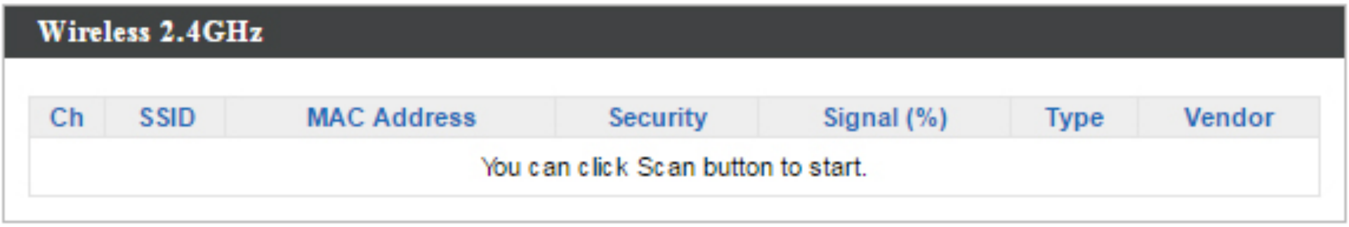
IV-1-3. Wireless Monitor

The “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	● 2.4G Scan
Channel Survey result	Export



Wireless 2.4GHz

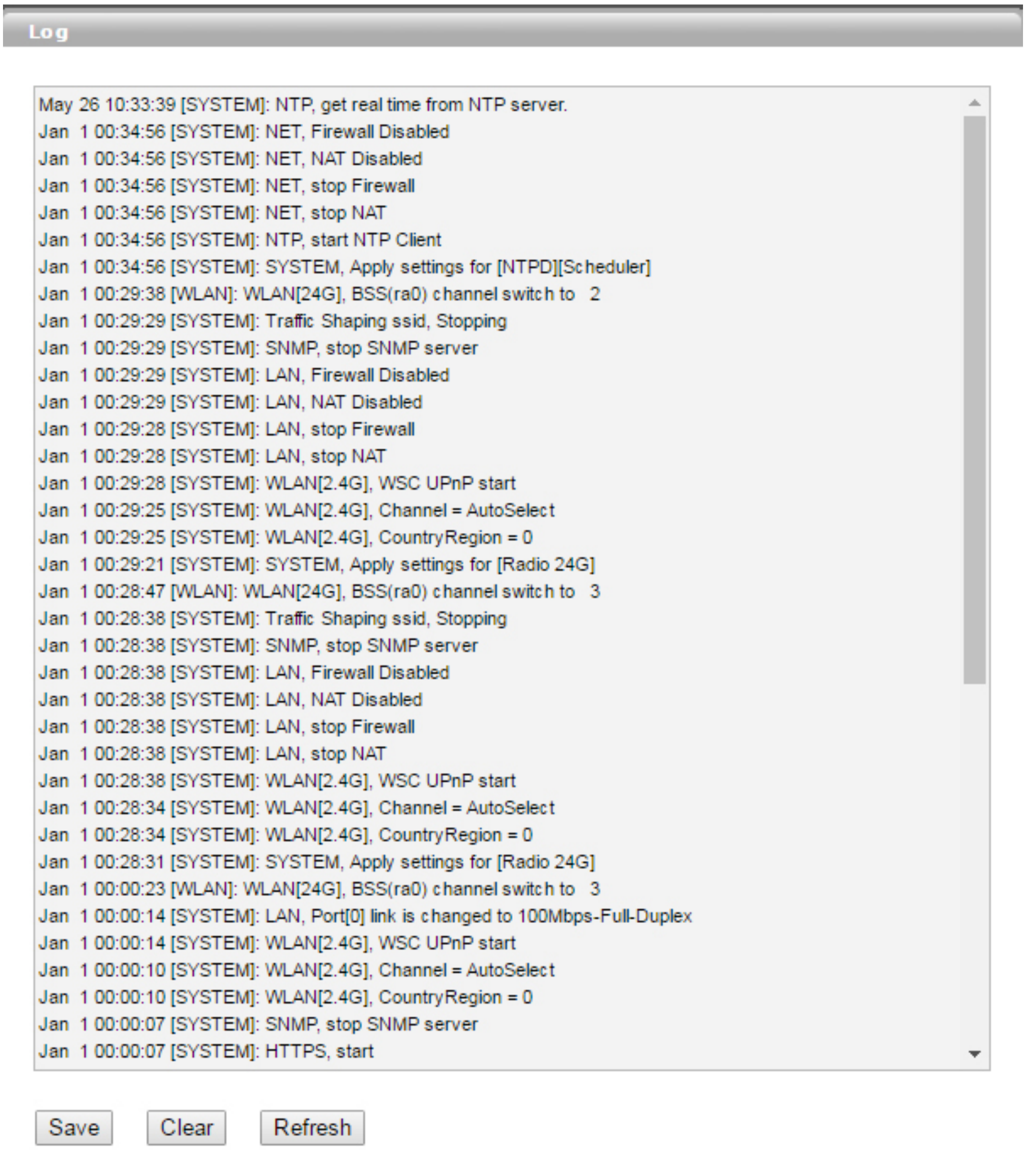
Ch	SSID	MAC Address	Security	Signal (%)	Type	Vendor
You can click Scan button to start.						

Wireless Monitor	
Site Survey	Click “Scan” to begin scanning.
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.

IV-1-4. Log

The “Log” Page displays system operation information such as up time and connection processes.



```
May 26 10:33:39 [SYSTEM]: NTP, get real time from NTP server.
Jan  1 00:34:56 [SYSTEM]: NET, Firewall Disabled
Jan  1 00:34:56 [SYSTEM]: NET, NAT Disabled
Jan  1 00:34:56 [SYSTEM]: NET, stop Firewall
Jan  1 00:34:56 [SYSTEM]: NET, stop NAT
Jan  1 00:34:56 [SYSTEM]: NTP, start NTP Client
Jan  1 00:34:56 [SYSTEM]: SYSTEM, Apply settings for [NTPD][Scheduler]
Jan  1 00:29:38 [WLAN]: WLAN[24G], BSS(ra0) channel switch to  2
Jan  1 00:29:29 [SYSTEM]: Traffic Shaping ssid, Stopping
Jan  1 00:29:29 [SYSTEM]: SNMP, stop SNMP server
Jan  1 00:29:29 [SYSTEM]: LAN, Firewall Disabled
Jan  1 00:29:29 [SYSTEM]: LAN, NAT Disabled
Jan  1 00:29:28 [SYSTEM]: LAN, stop Firewall
Jan  1 00:29:28 [SYSTEM]: LAN, stop NAT
Jan  1 00:29:28 [SYSTEM]: WLAN[2.4G], WSC UPnP start
Jan  1 00:29:25 [SYSTEM]: WLAN[2.4G], Channel = AutoSelect
Jan  1 00:29:25 [SYSTEM]: WLAN[2.4G], CountryRegion = 0
Jan  1 00:29:21 [SYSTEM]: SYSTEM, Apply settings for [Radio 24G]
Jan  1 00:28:47 [WLAN]: WLAN[24G], BSS(ra0) channel switch to  3
Jan  1 00:28:38 [SYSTEM]: Traffic Shaping ssid, Stopping
Jan  1 00:28:38 [SYSTEM]: SNMP, stop SNMP server
Jan  1 00:28:38 [SYSTEM]: LAN, Firewall Disabled
Jan  1 00:28:38 [SYSTEM]: LAN, NAT Disabled
Jan  1 00:28:38 [SYSTEM]: LAN, stop Firewall
Jan  1 00:28:38 [SYSTEM]: LAN, stop NAT
Jan  1 00:28:38 [SYSTEM]: WLAN[2.4G], WSC UPnP start
Jan  1 00:28:34 [SYSTEM]: WLAN[2.4G], Channel = AutoSelect
Jan  1 00:28:34 [SYSTEM]: WLAN[2.4G], CountryRegion = 0
Jan  1 00:28:31 [SYSTEM]: SYSTEM, Apply settings for [Radio 24G]
Jan  1 00:00:23 [WLAN]: WLAN[24G], BSS(ra0) channel switch to  3
Jan  1 00:00:14 [SYSTEM]: LAN, Port[0] link is changed to 100Mbps-Full-Duplex
Jan  1 00:00:14 [SYSTEM]: WLAN[2.4G], WSC UPnP start
Jan  1 00:00:10 [SYSTEM]: WLAN[2.4G], Channel = AutoSelect
Jan  1 00:00:10 [SYSTEM]: WLAN[2.4G], CountryRegion = 0
Jan  1 00:00:07 [SYSTEM]: SNMP, stop SNMP server
Jan  1 00:00:07 [SYSTEM]: HTTPS, start
```

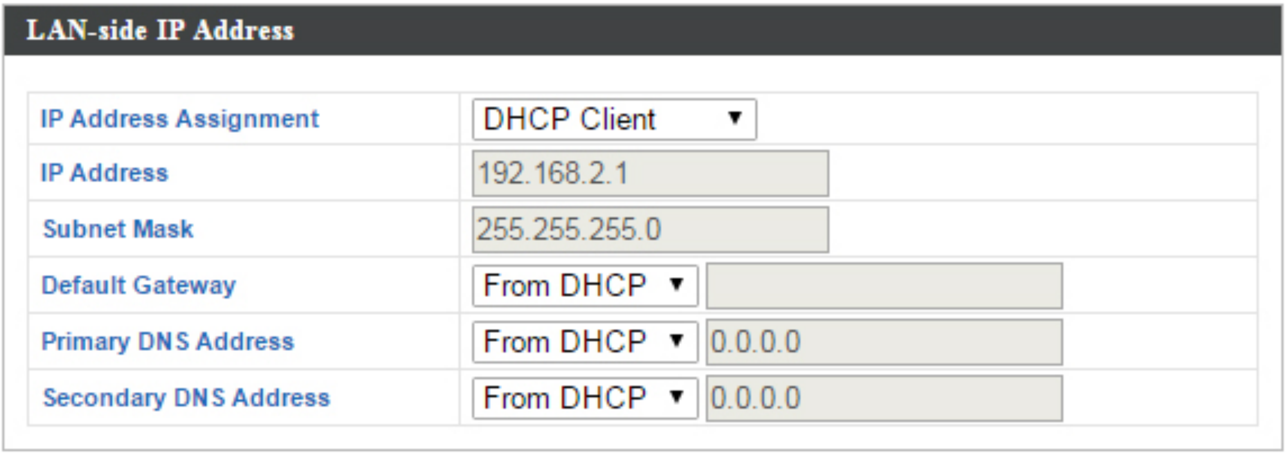
Save	Click “Save” and you will be prompted (example shown below) to save the log on your computer as .txt file.
Clear	Click “Clear” to clear/erase the existing log.
Refresh	Click “Refresh” to refresh the log and update any activity.

IV-2. Network Settings

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

IV-2-1. LAN-side IP Address

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



LAN-side IP Address

IP Address Assignment	DHCP Client ▼
IP Address	192.168.2.1
Subnet Mask	255.255.255.0
Default Gateway	From DHCP ▼
Primary DNS Address	From DHCP ▼ 0.0.0.0
Secondary DNS Address	From DHCP ▼ 0.0.0.0

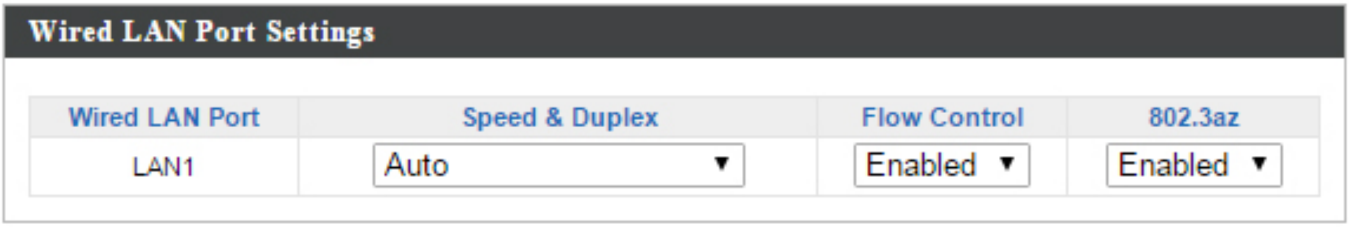
LAN-side IP Address	
IP Address Assignment	Select "DHCP Client" for your access point to be assigned a dynamic IP address from your router's DHCP server, or select "Static IP" to manually specify a static/fixed IP address for your access point (below).
IP Address	Specify the IP address here. This IP 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".

IV-2-2. LAN Port

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



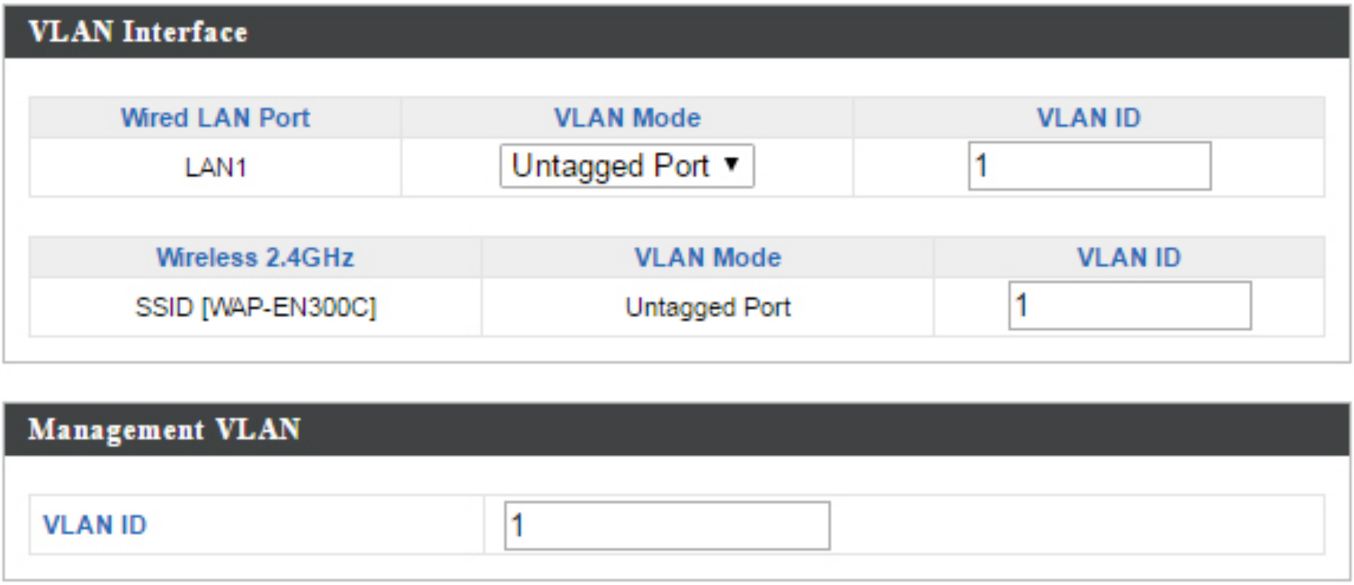
Wired LAN Port Settings

Wired LAN Port	Speed & Duplex	Flow Control	802.3az
LAN1	Auto ▼	Enabled ▼	Enabled ▼

Wired LAN Port	Identifies LAN port 1.
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 which disables unused interfaces to reduce power usage.

IV-2-3. VLAN

The "VLAN" (Virtual Local Area Network) enables you to configure VLAN settings. A VLAN is a local area network which maps workstations virtually instead of physically and allows you to group together or isolate users from each other. VLAN IDs 1 – 4094 are supported.



VLAN Interface

Wired LAN Port	VLAN Mode	VLAN ID
LAN1	Untagged Port ▼	1

Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [WAP-EN300C]	Untagged Port	1

Management VLAN

VLAN ID	1

VLAN Interface	
Wired LAN Port/Wireless	Identifies LAN port 1 and wireless SSIDs.
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.

IV-3. Wireless Settings

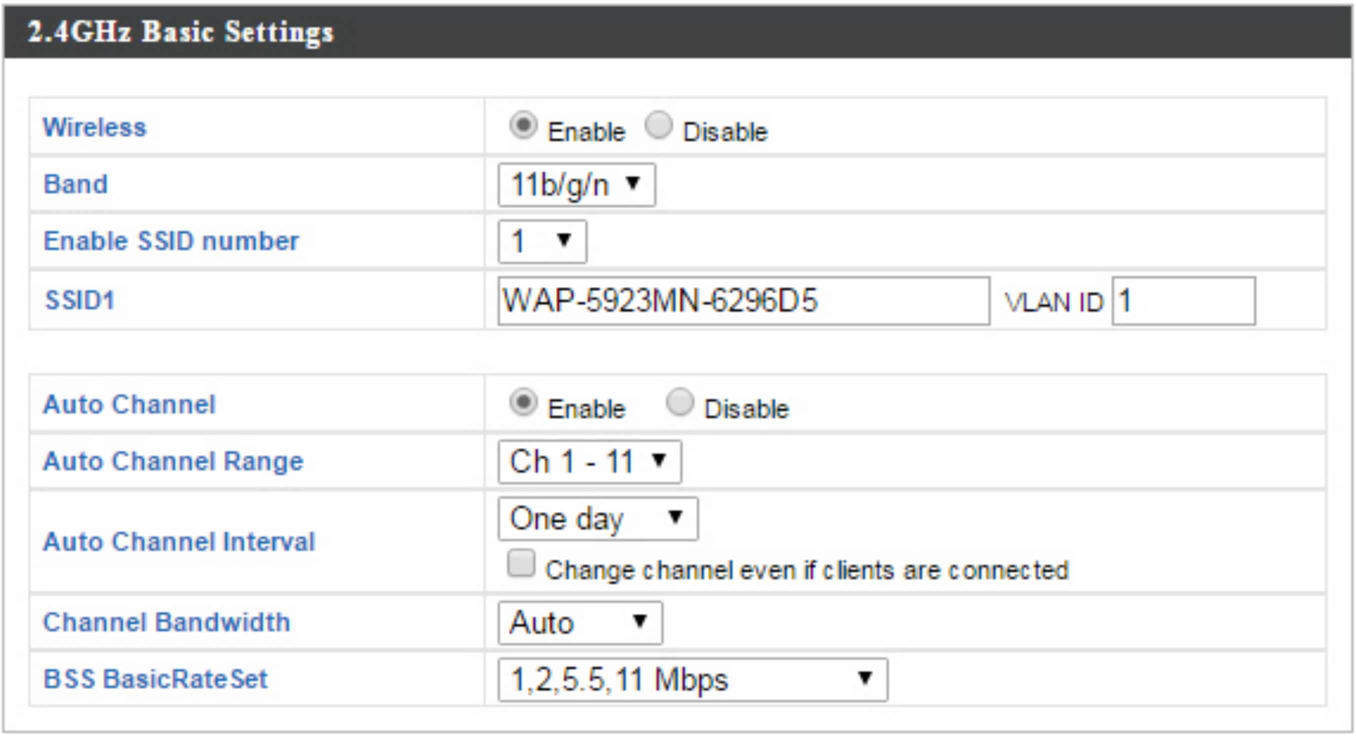
Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

IV-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.

IV-3-1-1 Basic

"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	WAP-5923MN-6296D5 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 ▼

Wireless	Enable or disable the access point’s wireless radio. When disabled, no 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.

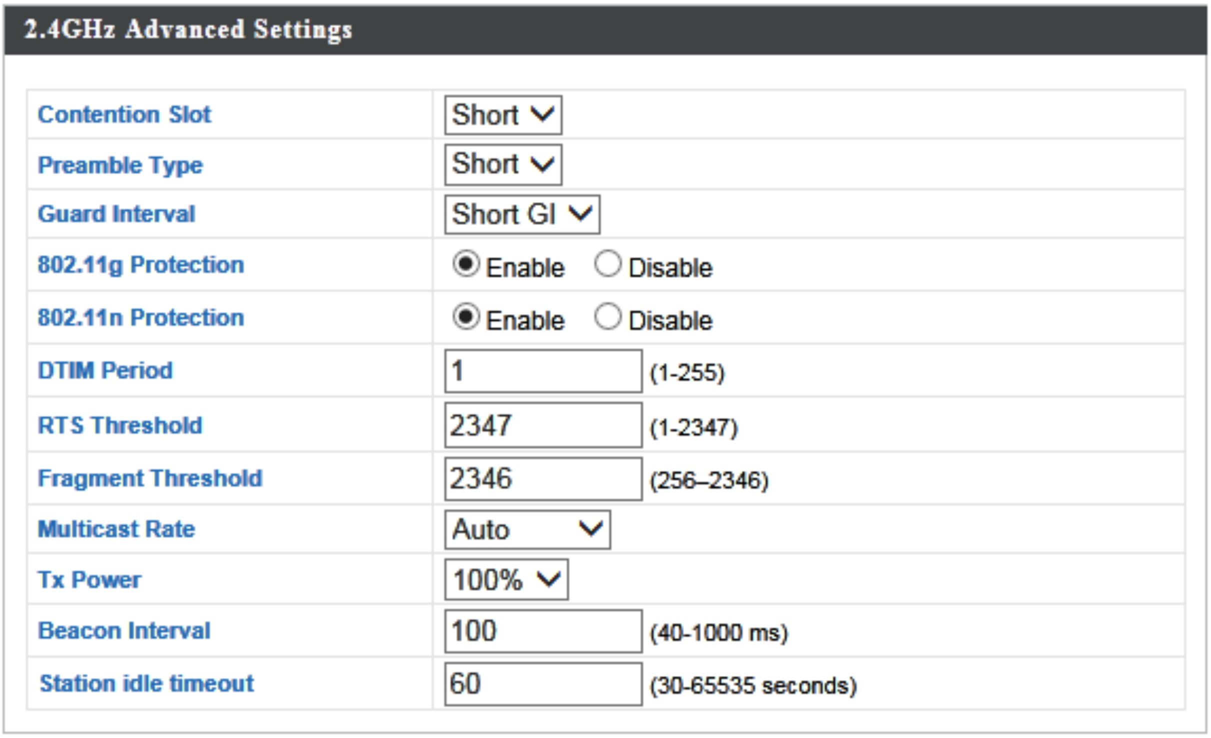
When auto channel is disabled, select a wireless channel manually:

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.

IV-3-1-2 Advanced

These settings are for experienced users only. 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 **IV-3-6. WMM**).

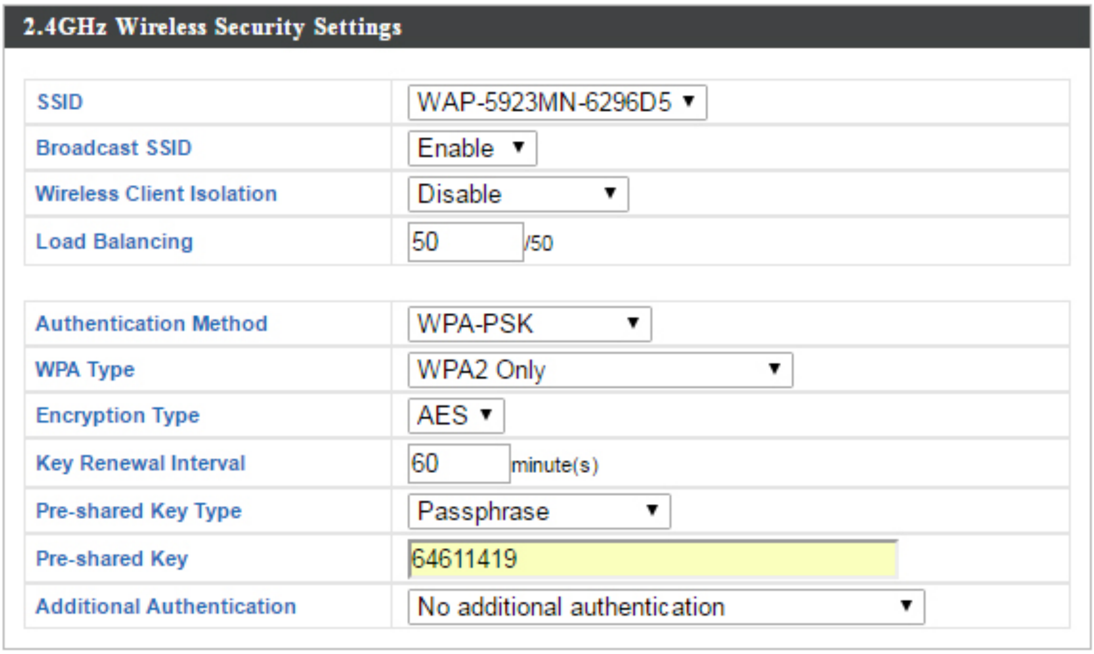
Preamble Type	Set the wireless radio preamble type. The preamble type in 802.11 based wireless communication defines the length of the CRC (Cyclic Redundancy Check) block for communication between the access point and roaming wireless adapters. The default value is “Short Preamble”.
Guard Interval	Set 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.

IV-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	WAP-5923MN-6296D5 ▾
Broadcast SSID	Enable ▾
Wireless Client Isolation	Disable ▾
Load Balancing	50 /50
Authentication Method	WPA-PSK ▾
WPA Type	WPA2 Only ▾
Encryption Type	AES ▾
Key Renewal Interval	60 minute(s)
Pre-shared Key Type	Passphrase ▾
Pre-shared Key	64611419
Additional Authentication	No additional authentication ▾

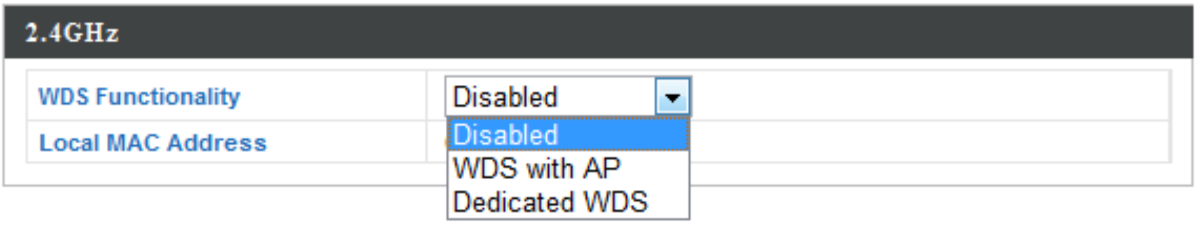
SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually 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 (**IV-3-1-3-6.**) appropriate for your method.

IV-3-1-4 WDS

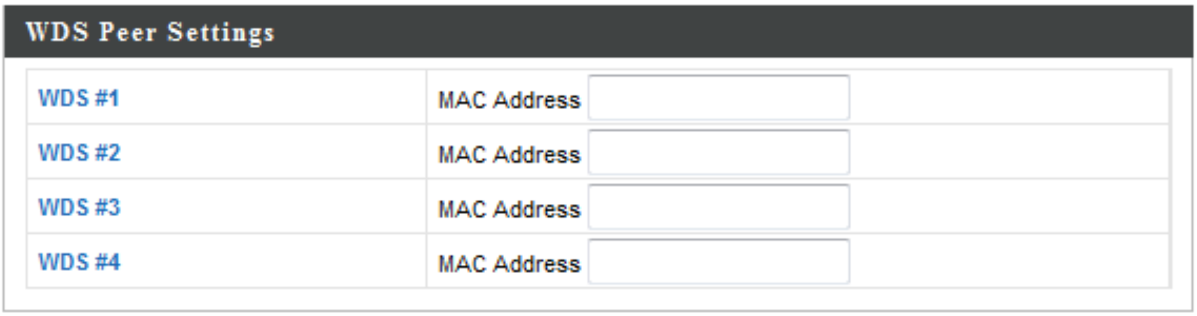
Wireless Distribution System (WDS) can bridge/repeat access points together in an extended network. WDS settings can be configured as shown below.

⚠ ***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.***



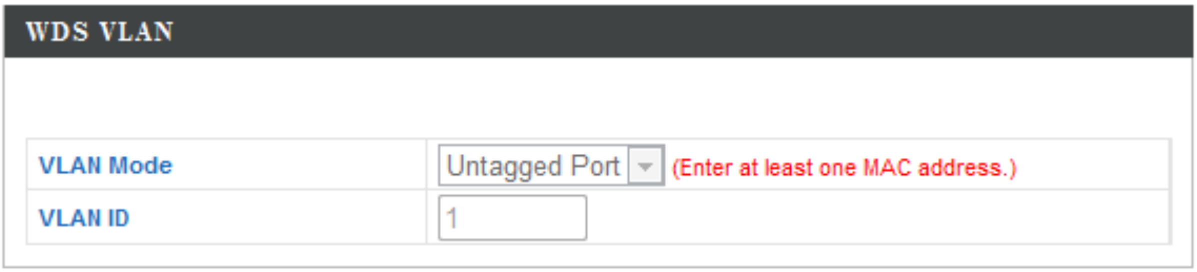
2.4GHz

WDS Functionality	Disabled
Local MAC Address	



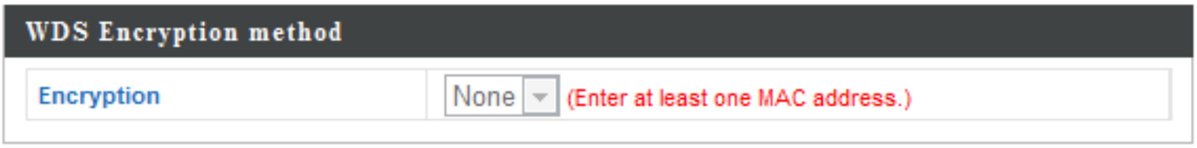
WDS Peer Settings

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



WDS Encryption method

Encryption	None (Enter at least one MAC address.)

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	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.

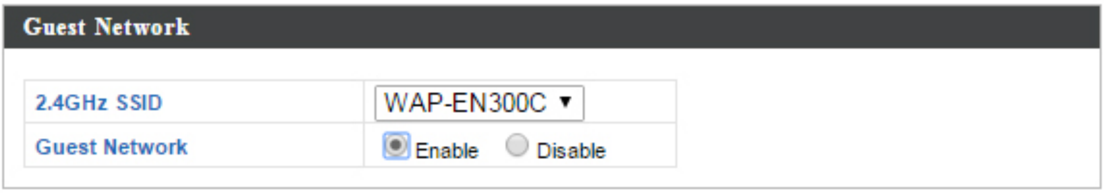
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

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.

IV-3-1-5 Guest Network

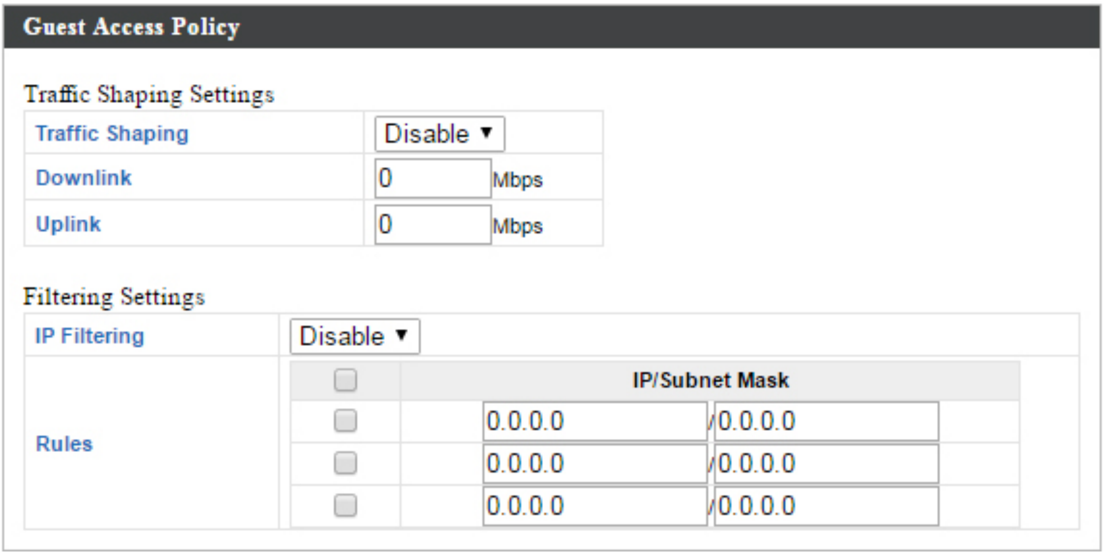
The “Guest Network” page allows you to configure a guest network that will have a Layer-3 IP Filter applied to all traffic passing through the specified SSID.

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	WAP-EN300C ▾
Guest Network	● Enable ○ Disable



Guest Access Policy

Traffic Shaping Settings

Traffic Shaping	Disable ▾
Downlink	0 Mbps
Uplink	0 Mbps

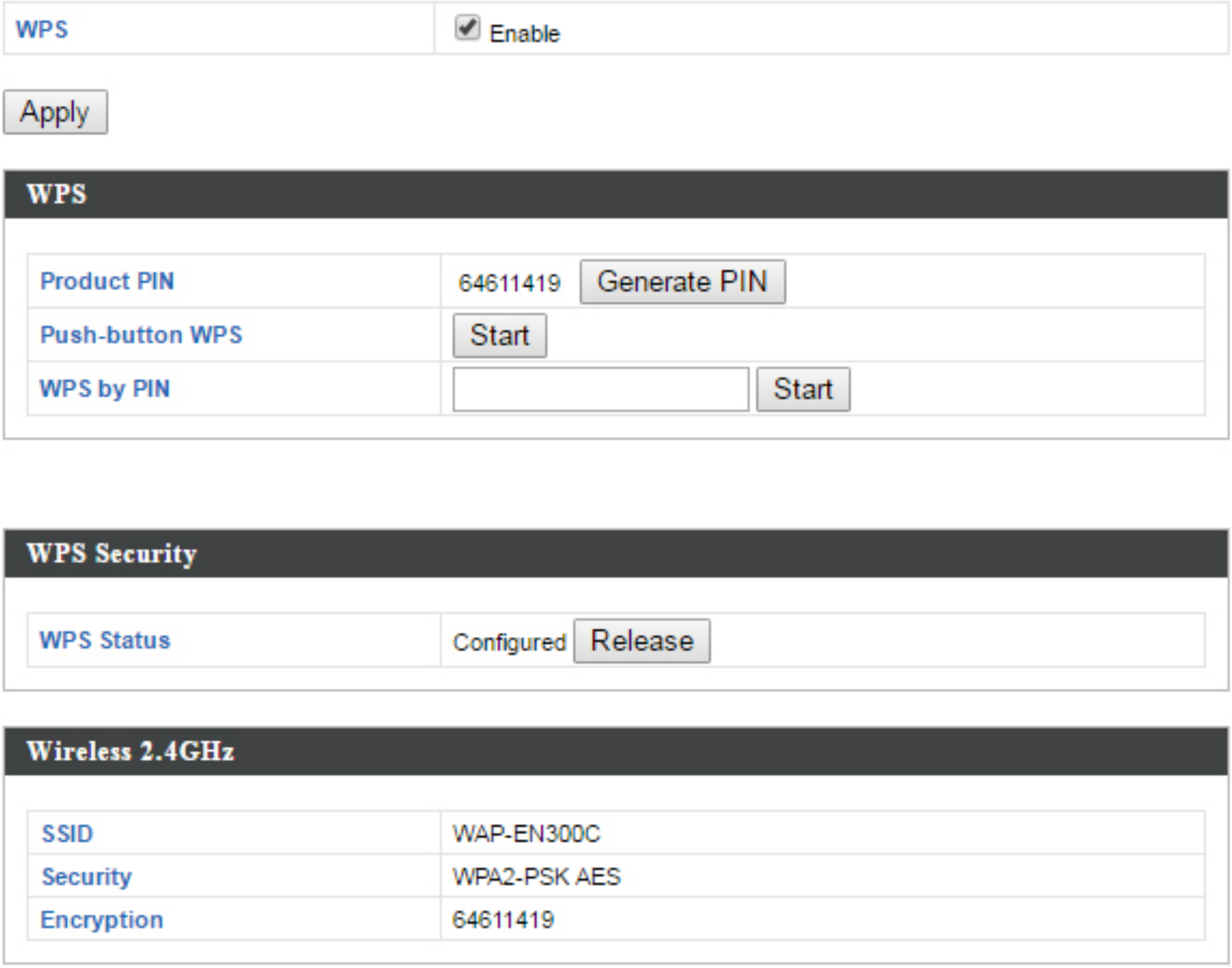
Filtering Settings

IP Filtering	Disable ▾	
Rules	□	IP/Subnet Mask
	□	0.0.0.0 / 0.0.0.0
	□	0.0.0.0 / 0.0.0.0
	□	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.
Filtering Settings	Select “Allow” or “Deny” to apply IP Filtering to the traffic on the Guest Network. Provide the IP and Subnet Mask you want to apply as a filter. Up to 3 IP Filters are supported.

IV-3-2 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. When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. PIN code WPS includes the use of a PIN code between the two devices for verification.



WPS	☑ Enable

WPS

Product PIN	64611419 Generate PIN
Push-button WPS	Start
WPS by PIN	Start

WPS Security

WPS Status	Configured Release

Wireless 2.4GHz

SSID	WAP-EN300C
Security	WPA2-PSK AES
Encryption	64611419

Enable WPS	Check/uncheck this box to enable/disable WPS.
WPS Current Status	Displays “Configured” or “unConfigured” depending on whether WPS and security/encryption settings for the device have been configured or not, either manually or using the WPS button.
Self PIN Code	Displays the WPS PIN code of the device.
2.4 GHz SSID	Displays the SSID (ESSID) of the device.
2.4GHz Authentication Mode	Displays the wireless security authentication mode of the device.
2.4GHz Passphrase Key	Displays the wireless security authentication key type.
Configure via Push Button	Click “Start to Process” to activate WPS on the access point. WPS will be active for 2 minutes.
WPS via PIN	Enter the wireless client’s PIN code here and click “Start to Process” to activate PIN code WPS. Refer to your wireless client’s documentation if you are unsure of its PIN code.

IV-3-3 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.

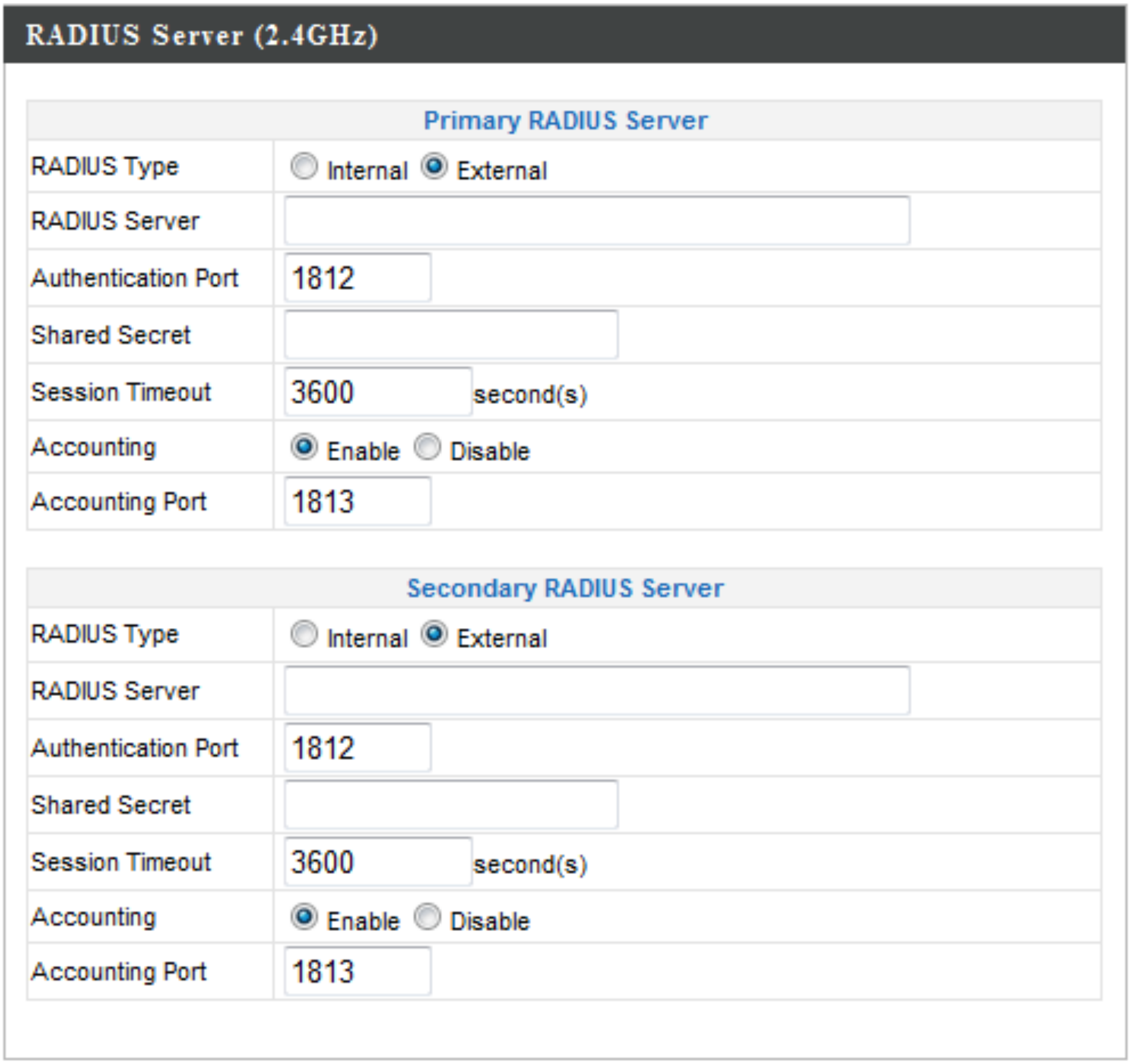
The access point can utilize both a primary and secondary (backup) RADIUS server. External RADIUS servers can be used or the access point’s internal RADIUS server can be used.

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

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

IV-3-3-1 Radius Settings

Configure the RADIUS server settings for 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

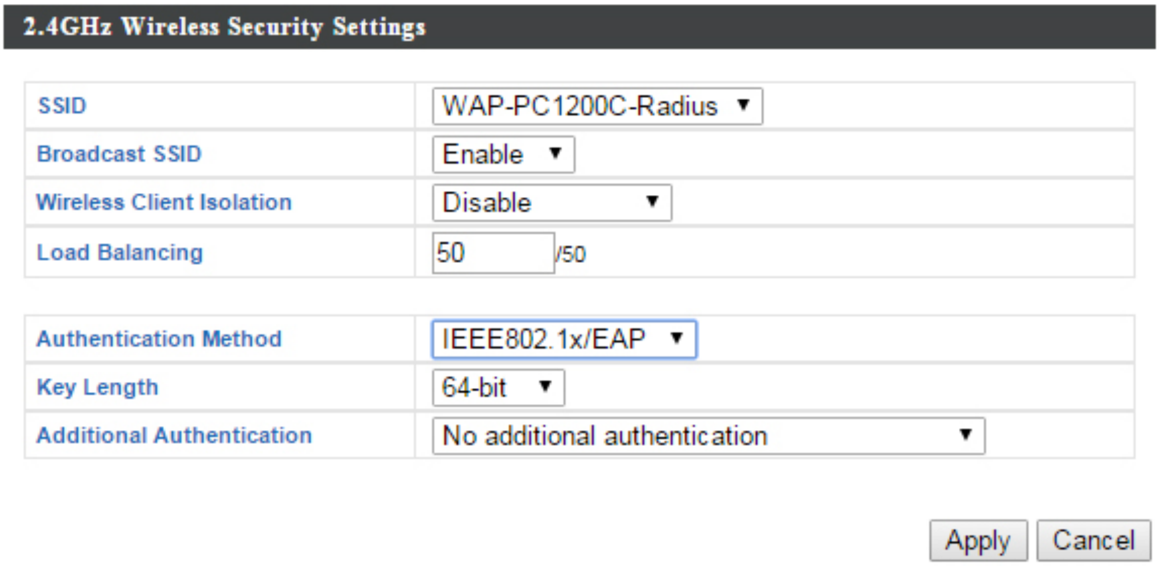
RADIUS Type	○ Internal ● External
RADIUS Server	
Authentication Port	1812
Shared Secret	
Session Timeout	3600 second(s)
Accounting	● Enable ○ Disable
Accounting Port	1813

RADIUS 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 **IV-3-1-3-6** or **IV-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.

IV-3-3-2 Internal Server

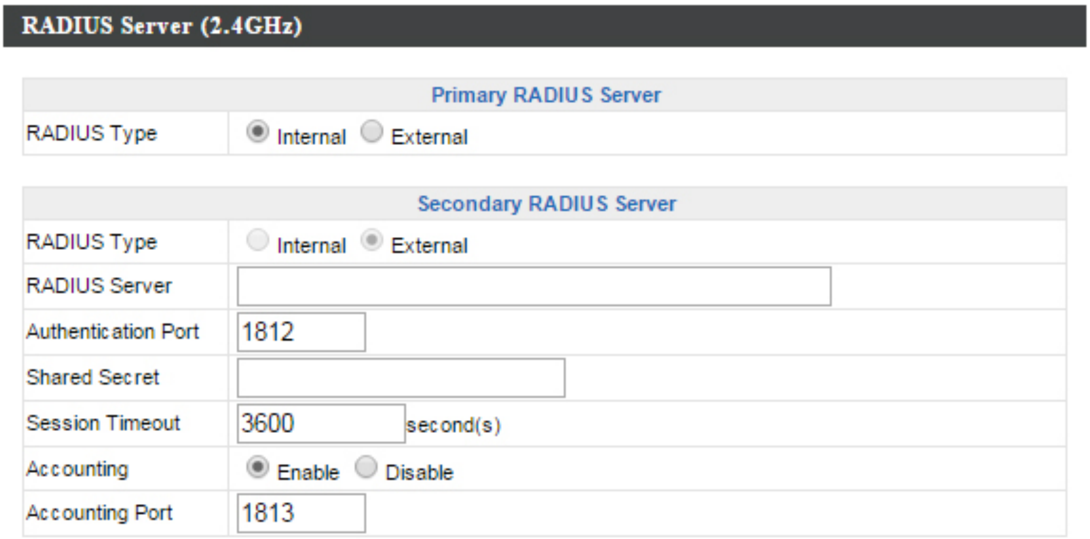
To use the Internal Radius Server as an additional authentication, configure the "Authentication Method" in "Wireless Settings/Security" to "IEEE802.1x/EAP". Leave "Additional Authentication" set to "No additional authentication". Click "Apply" to save settings. (Example image below)



2.4GHz Wireless Security Settings

SSID	WAP-PC1200C-Radius ▼
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 ▼

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

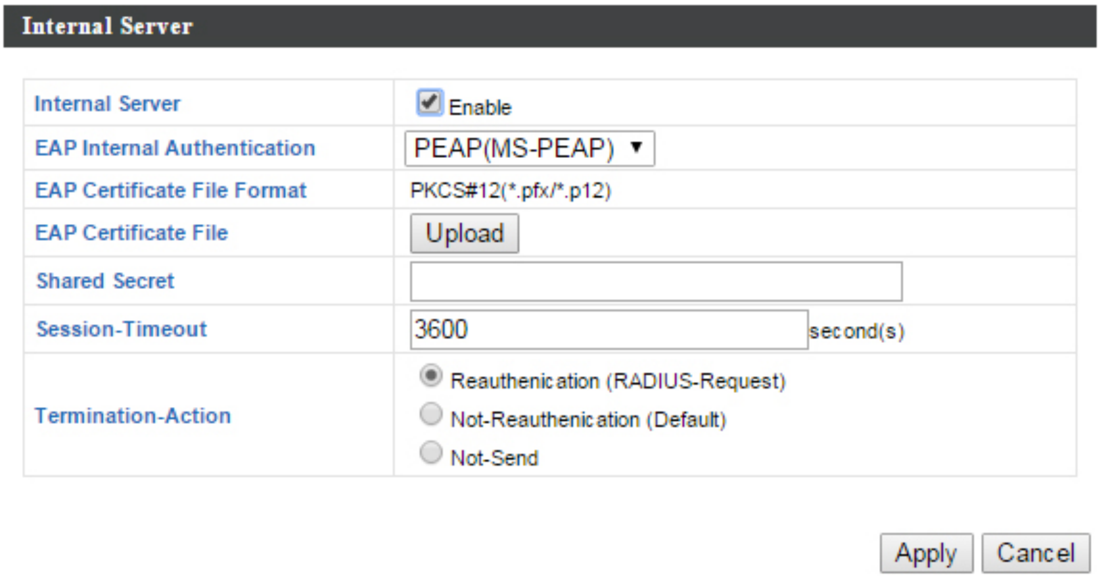


RADIUS Server (2.4GHz)

Primary RADIUS Server	
RADIUS Type	● Internal ○ External

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 "Reauthentication (Radius-Request)." Click "Apply" to save changes. (Example image below)

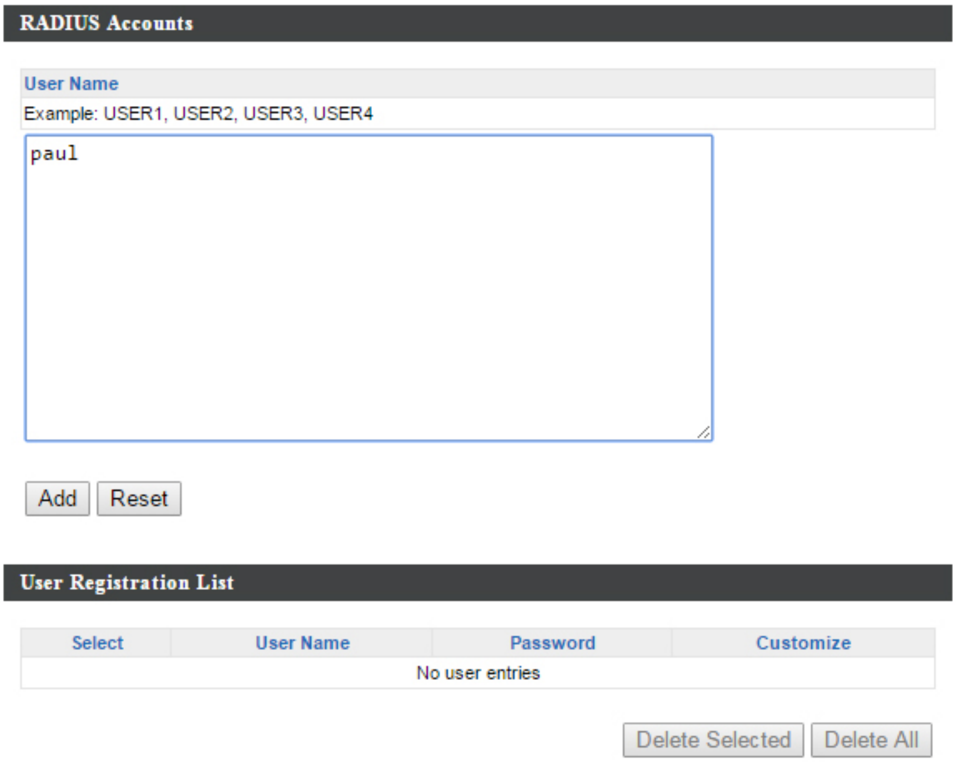


Internal Server

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

IV-3-3-3 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

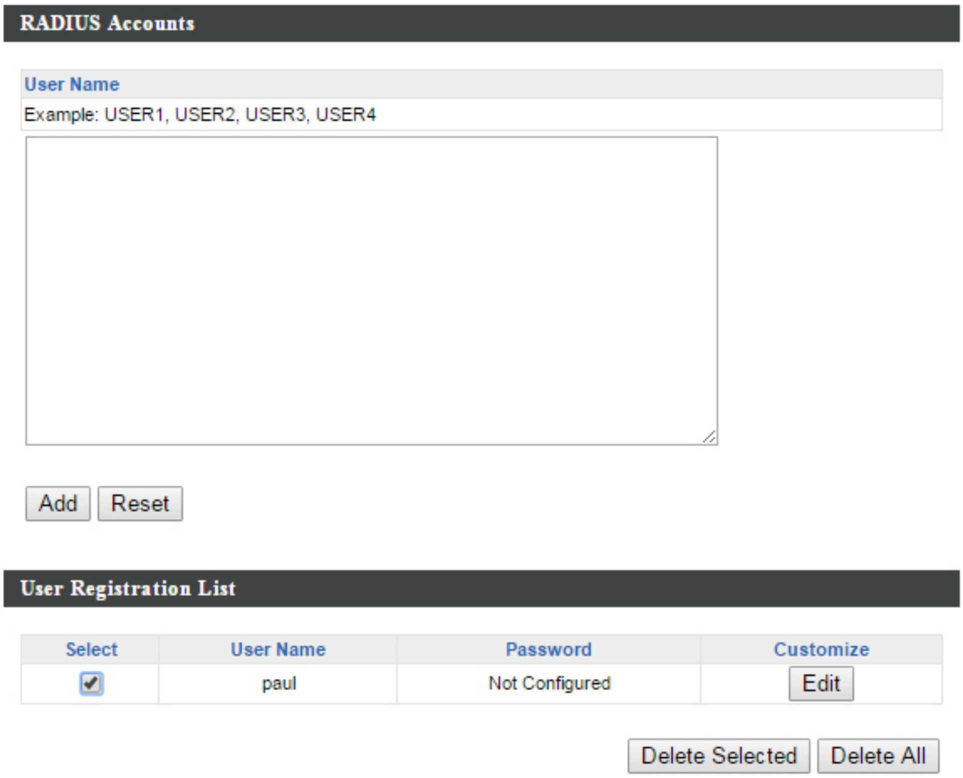
Example: USER1, USER2, USER3, USER4

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

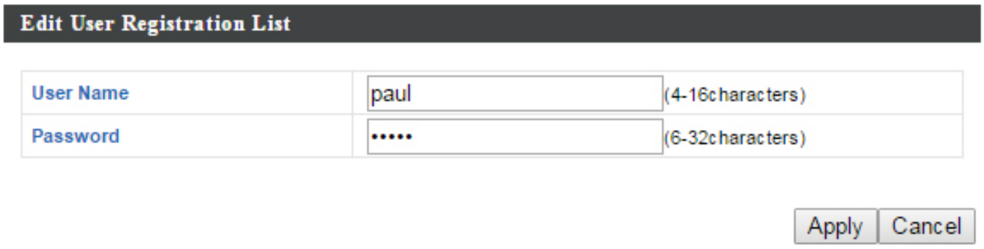
User Name

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)



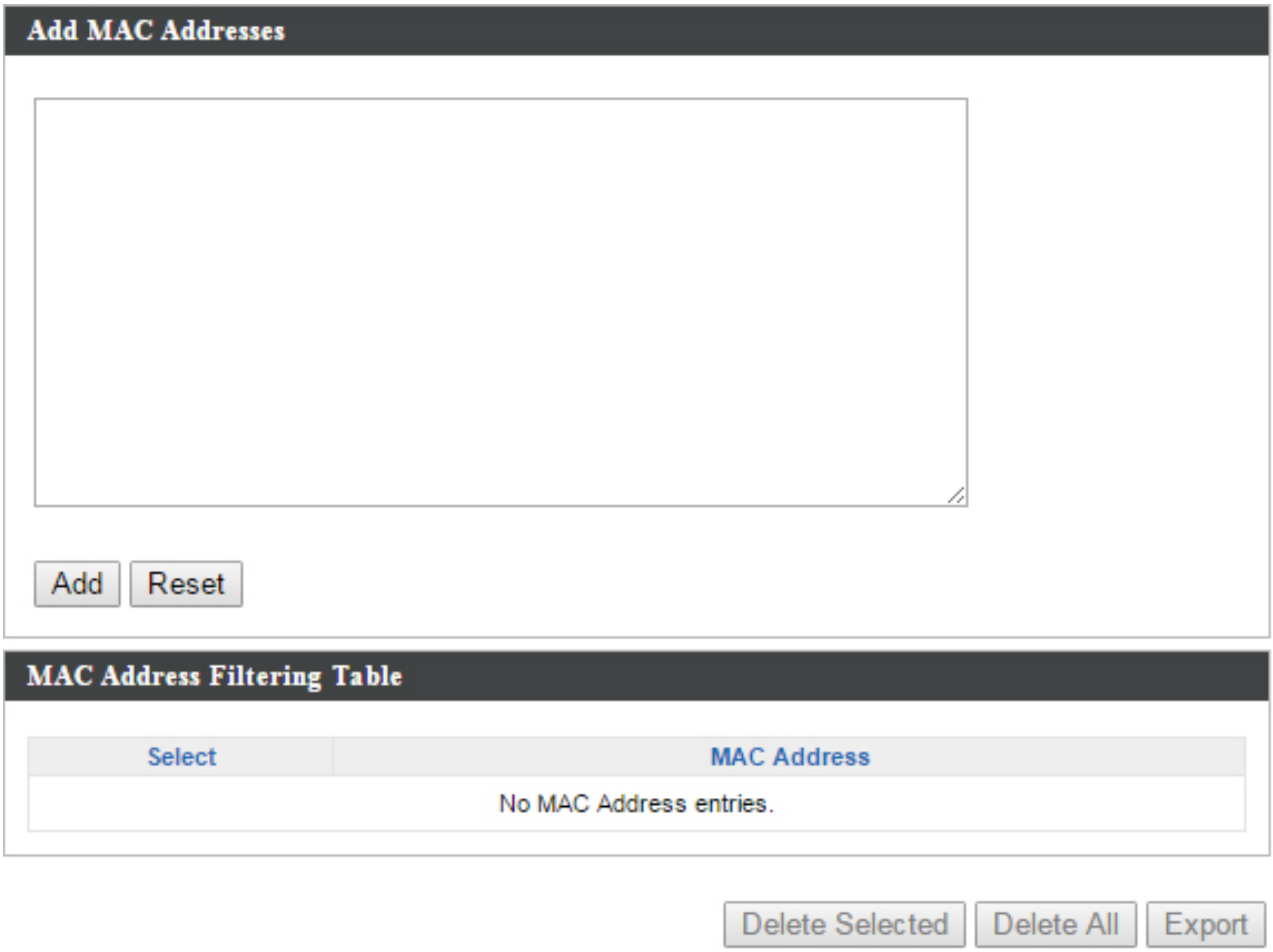
Edit User Registration List

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

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

IV-3-4 MAC Filter

The “MAC Filter” allows you add MAC address to filter access.



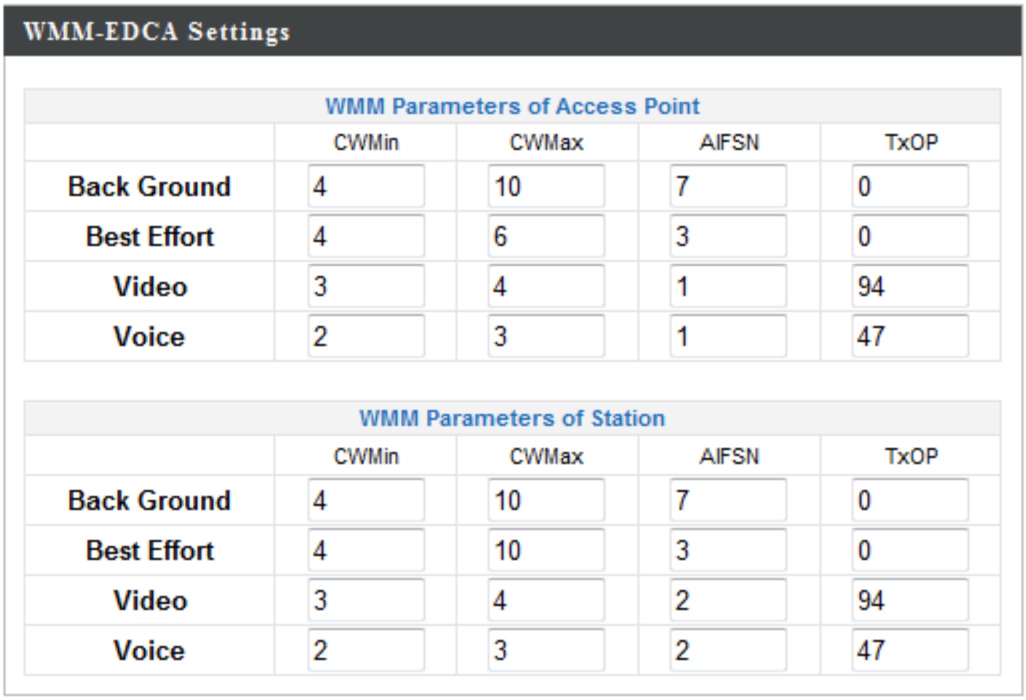
Add MAC Addresses

MAC Address Filtering Table

Select	MAC Address
No MAC Address entries.	

IV-3-5 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.

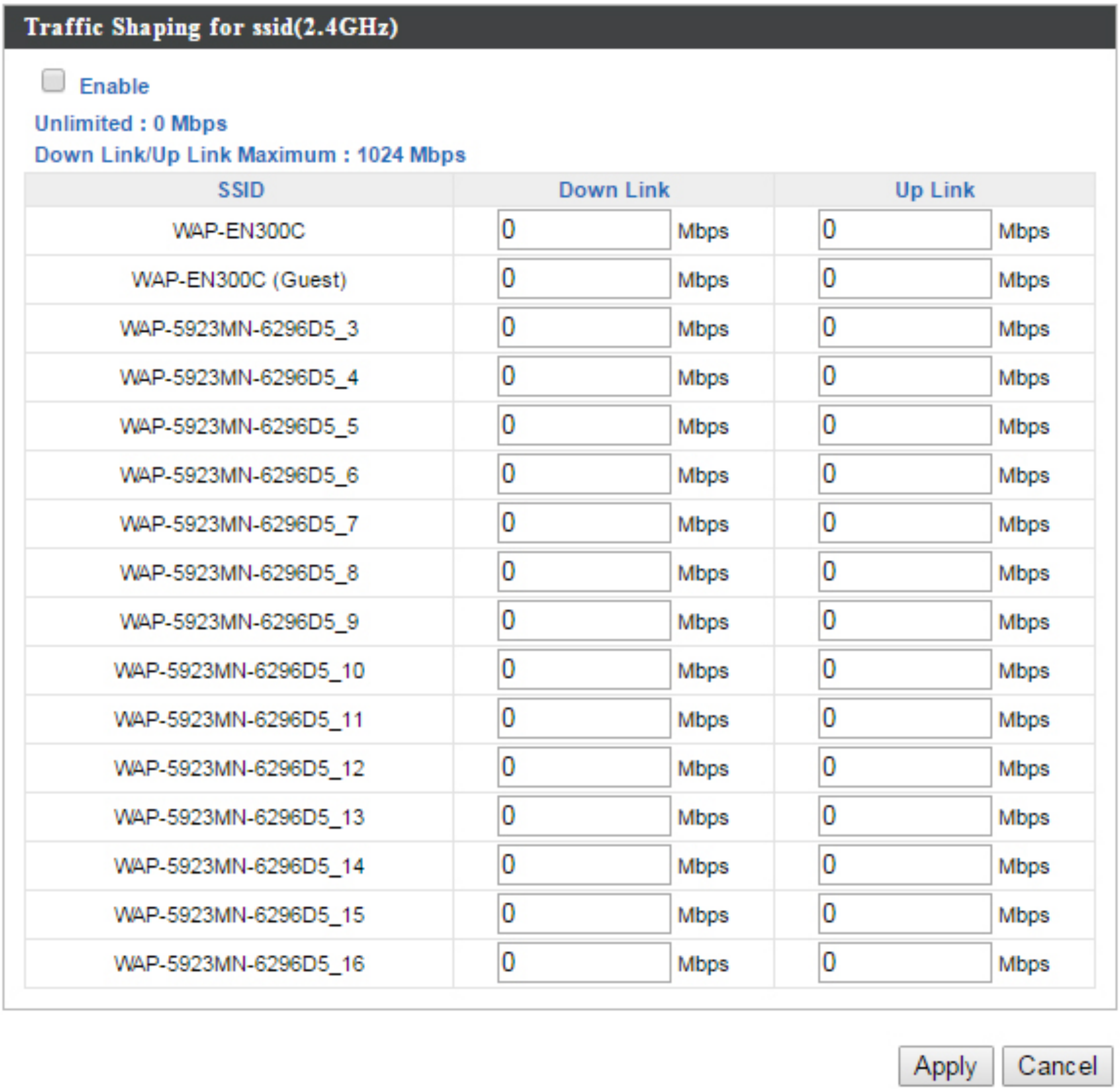
Queues automatically provide minimum transmission delays for video, voice, multimedia and critical applications. The values can further be adjusted manually:

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.

IV-3-6 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-EN300C	0 Mbps	0 Mbps
WAP-EN300C (Guest)	0 Mbps	0 Mbps
WAP-5923MN-6296D5_3	0 Mbps	0 Mbps
WAP-5923MN-6296D5_4	0 Mbps	0 Mbps
WAP-5923MN-6296D5_5	0 Mbps	0 Mbps
WAP-5923MN-6296D5_6	0 Mbps	0 Mbps
WAP-5923MN-6296D5_7	0 Mbps	0 Mbps
WAP-5923MN-6296D5_8	0 Mbps	0 Mbps
WAP-5923MN-6296D5_9	0 Mbps	0 Mbps
WAP-5923MN-6296D5_10	0 Mbps	0 Mbps
WAP-5923MN-6296D5_11	0 Mbps	0 Mbps
WAP-5923MN-6296D5_12	0 Mbps	0 Mbps
WAP-5923MN-6296D5_13	0 Mbps	0 Mbps
WAP-5923MN-6296D5_14	0 Mbps	0 Mbps
WAP-5923MN-6296D5_15	0 Mbps	0 Mbps
WAP-5923MN-6296D5_16	0 Mbps	0 Mbps

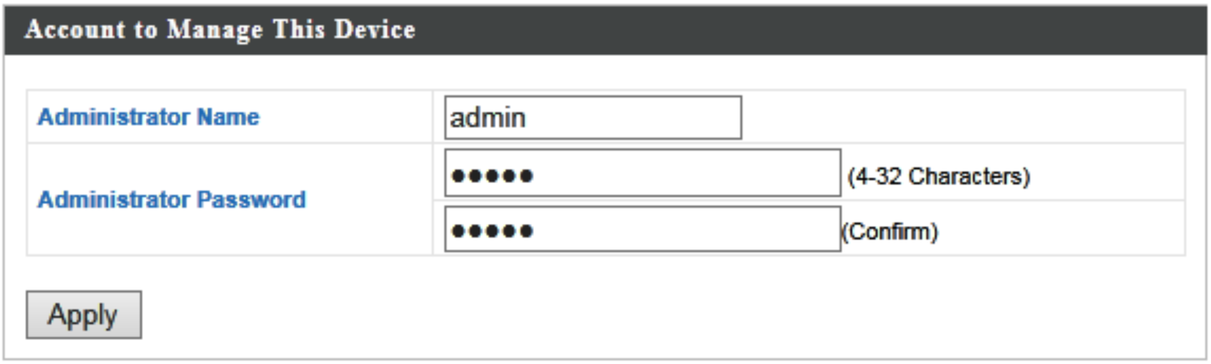
IV-4 Management

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

IV-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.

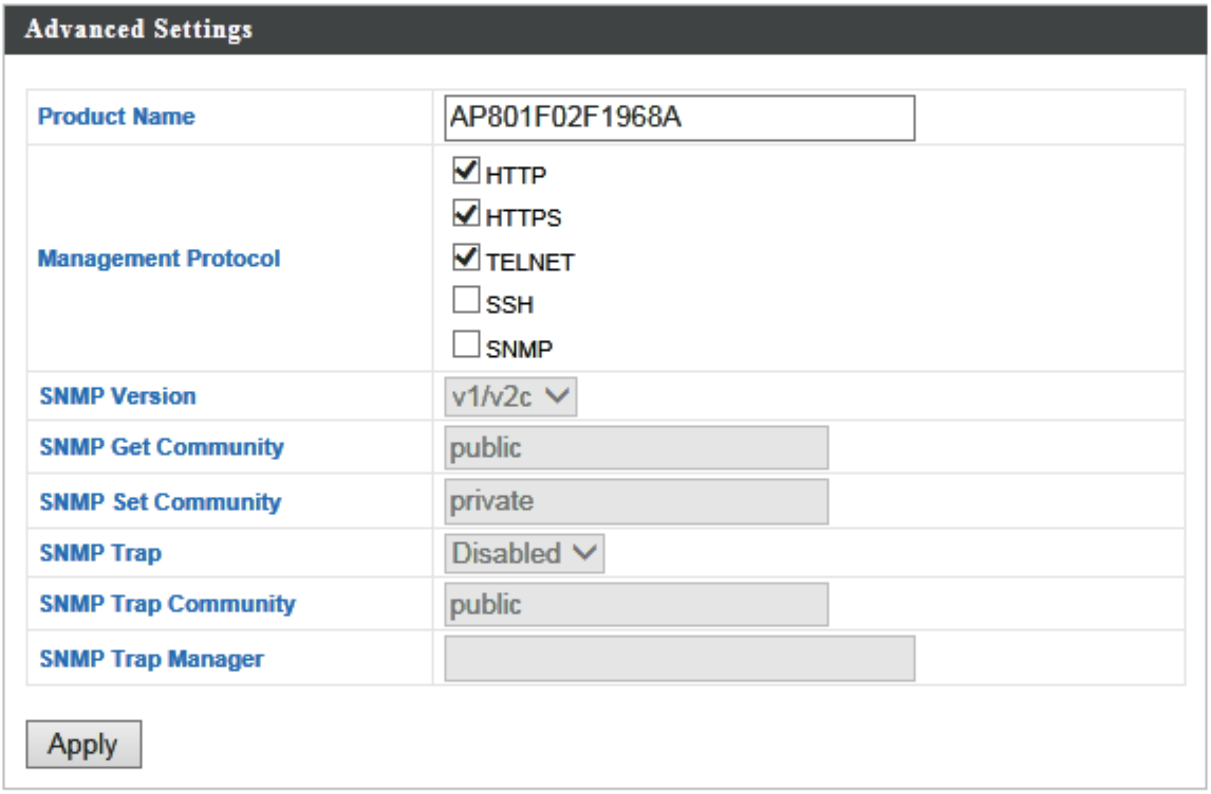
If you change the administrator password, make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface, see *I-5. Reset* ***for how to reset the access point.***



Account to Manage This Device

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

Apply



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	

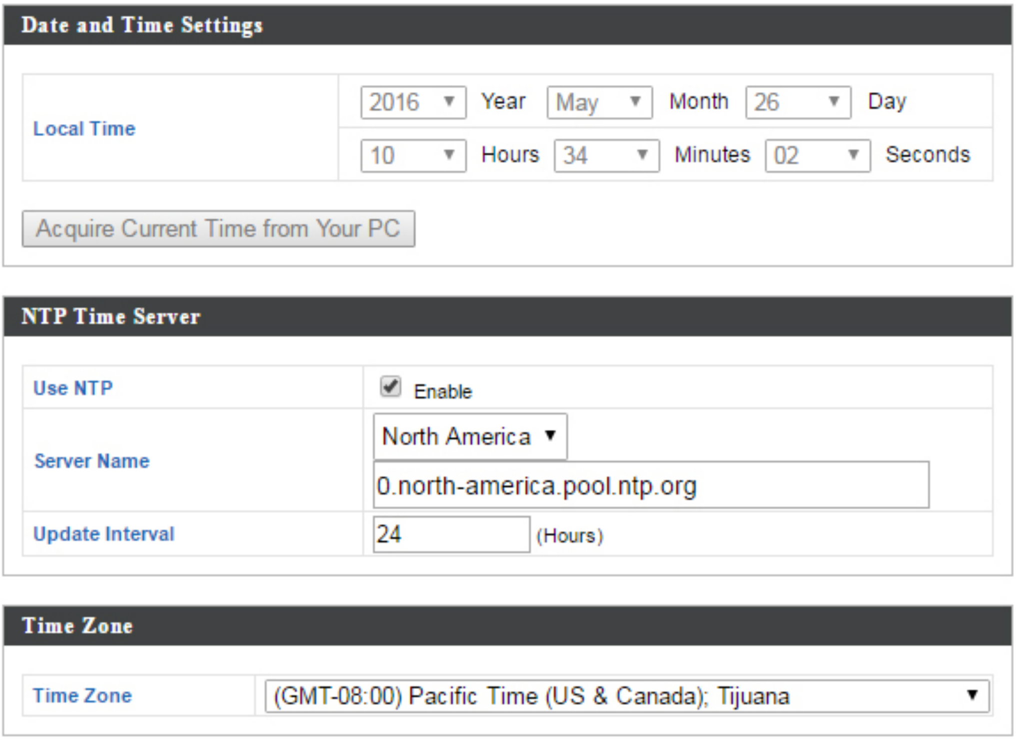
Apply

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.

IV-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: 2016 Year, May Month, 26 Day; 10 Hours, 34 Minutes, 02 Seconds

NTP Time Server

Use NTP: ☑ Enable

Server Name: North America ▾, 0.north-america.pool.ntp.org

Update Interval: 24 (Hours)

Time Zone

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana ▾

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.

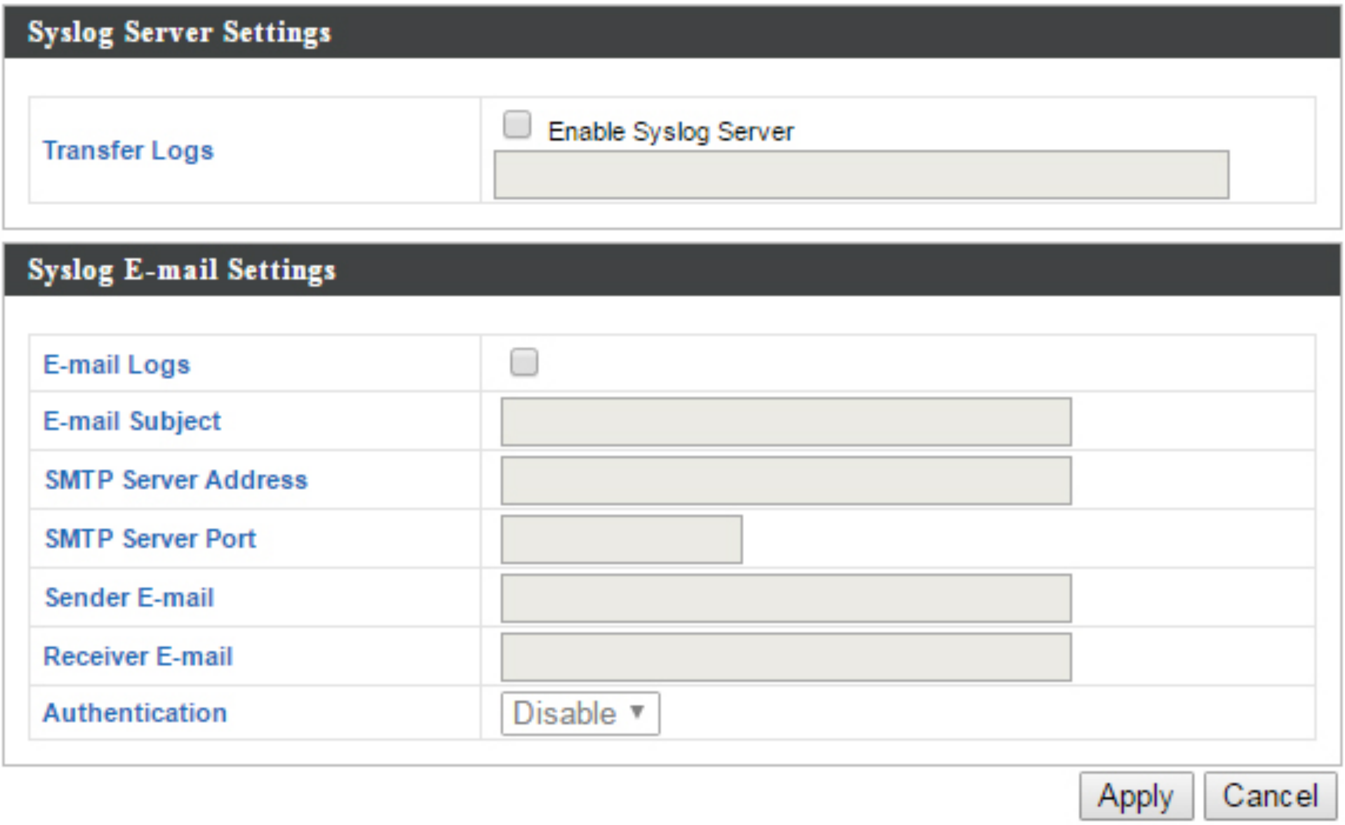
NTP Time Server	
Use NTP	The access point also supports NTP (Network Time Protocol) for automatic time and date setup.
Server Name	Enter the host name or IP address of the time server if you wish.
Update Interval	Specify a frequency (in hours) for the access point to update/synchronize with the NTP

	server.

Time Zone	
Time Zone	Select the time zone of your country/ region. If your country/region is not listed, select another country/region whose time zone is the same as yours.

IV-4-3 Syslog Server

The system log can be sent to a server or e-mailed.



Syslog Server Settings

Transfer Logs □ Enable Syslog Server

Syslog E-mail Settings

E-mail Logs □

E-mail Subject

SMTP Server Address

SMTP Server Port

Sender E-mail

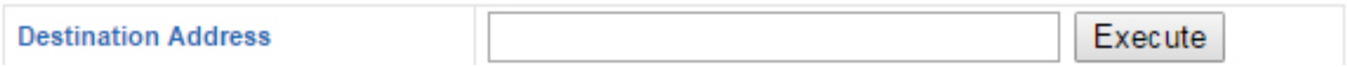
Receiver E-mail

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.

IV-4-4 Ping Test

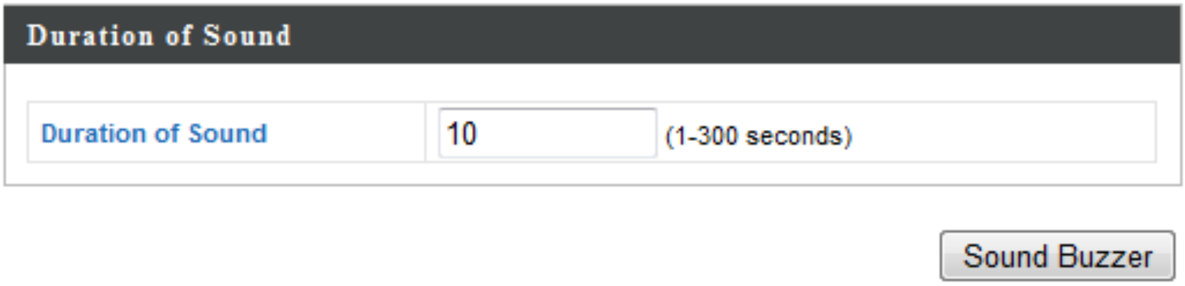
The "Ping Test" will send a continuous Ping to the IP Address specified. Results are posted in the dialog box below the Destination Address Execution window.



Destination Address

IV-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!

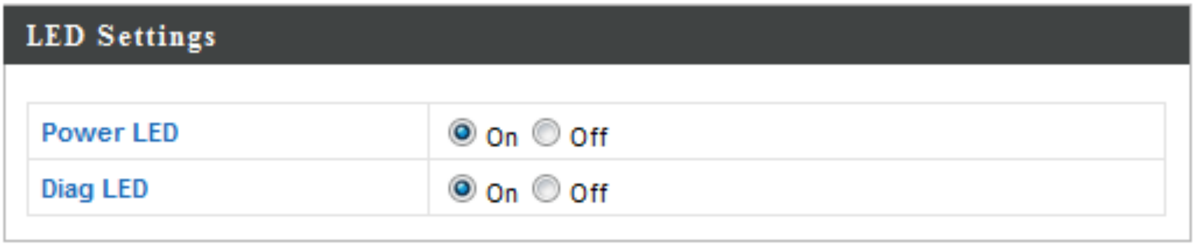
Duration of Sound	Set the duration for which the buzzer will sound when the "Sound Buzzer" button is clicked.
Sound Buzzer	Activate the buzzer sound for the above specified duration of time.

IV-5 Advanced

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

IV-5-1 LED Settings

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



LED Settings

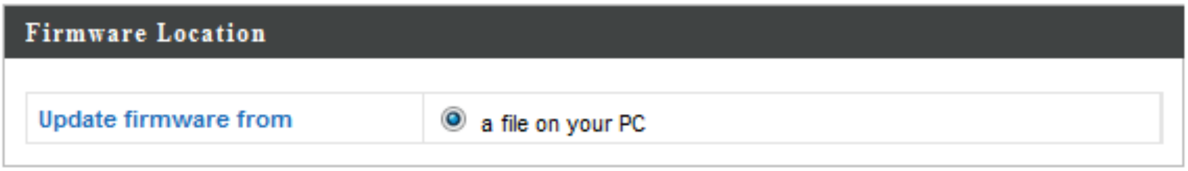
Power LED ● On ○ Off

Diag LED ● On ○ Off

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

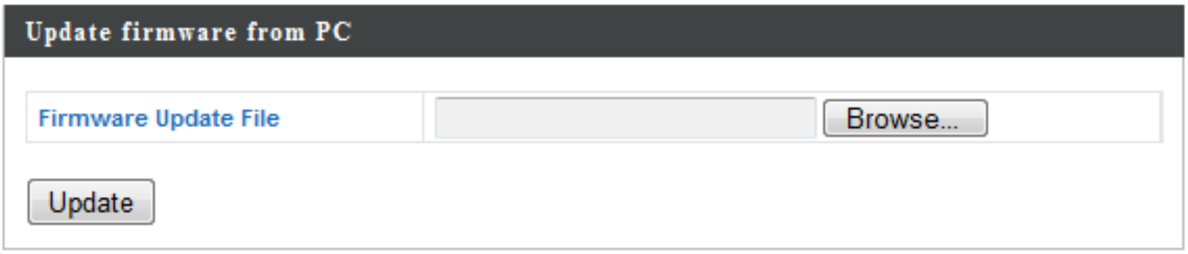
IV-5-2 Update Firmware

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



Firmware Location

Update firmware from ● a file on your PC



Update firmware from PC

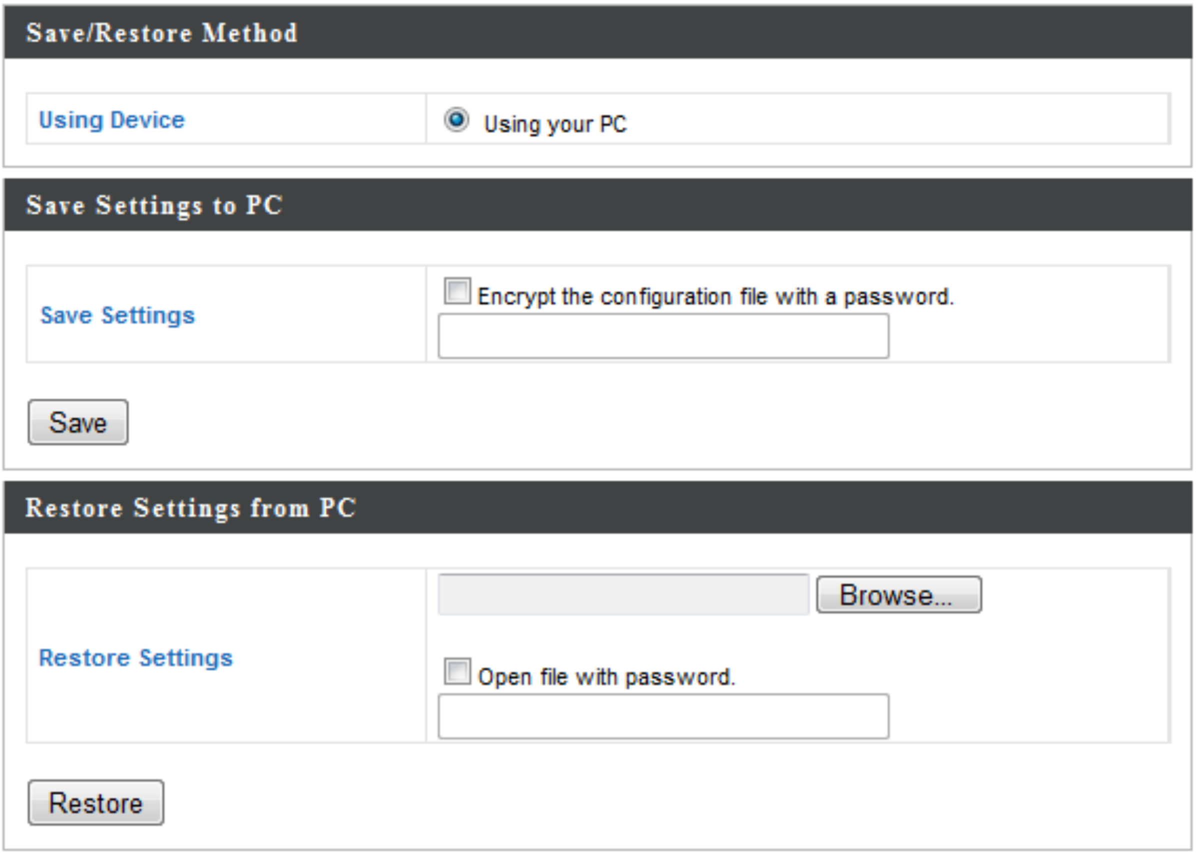
Firmware Update File

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.

IV-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: □ Open file with password.

Save / Restore Settings	
Using Device	Select “Using your PC” to save the access point’s settings to your local computer.

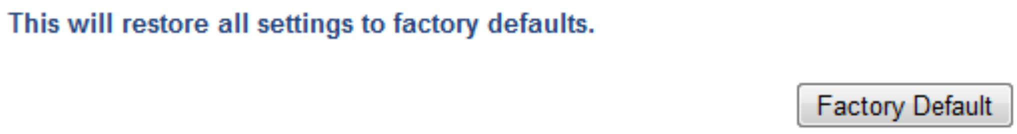
Save Settings to PC	
Save Settings	Click “Save” to save settings and a new

	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.

IV-5-4 Factory Default

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



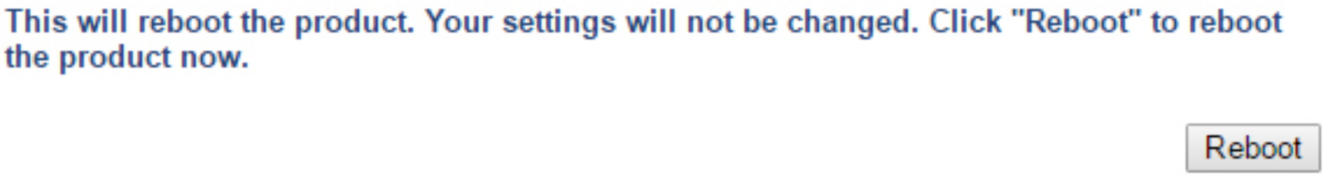
This will restore all settings to factory defaults.

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, wait for the access point to reset and restart.

IV-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 **IV-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.

IV-6 Operation Mode

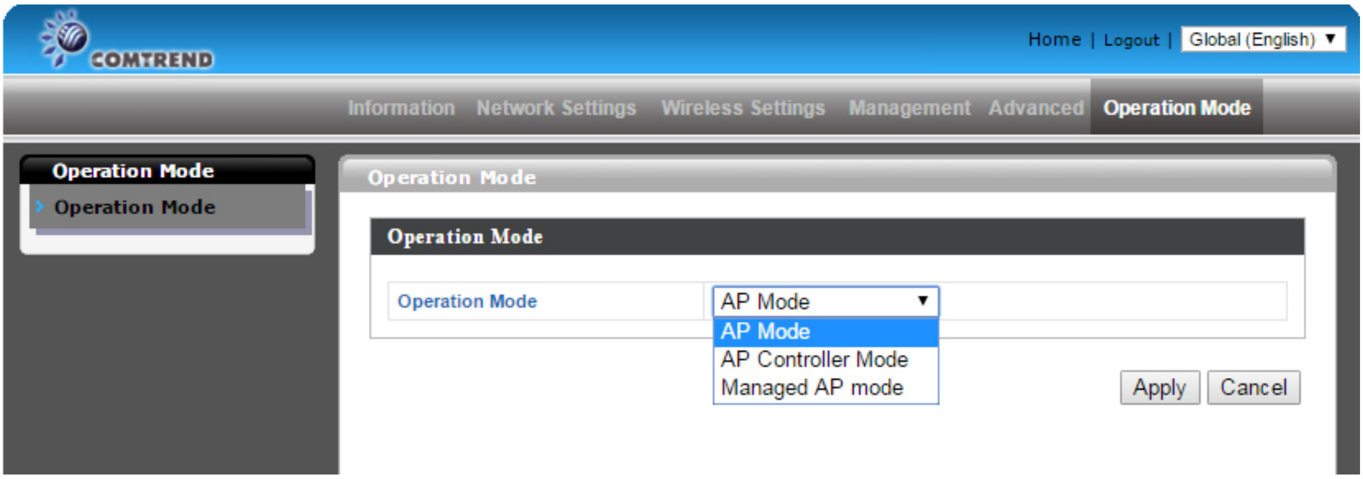
Your access point can function in three different modes.

The default mode for your access point is "AP Mode".

AP Mode is a regular access point for your network.

AP Controller Mode acts as a designated "Master" for an array of "Slave" access points. (Group of linked access points)

Managed AP Mode acts like a "Slave" access point in an access point array. (Controlled by the AP Controller "Master")



Operation Mode: AP Mode

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

This manual covers **AP Mode. Controller Mode** is covered in the NMS manual.   Both manuals are available on the CD that came with your product and are available online.

V. Appendix

V-1. Configuring your IP address

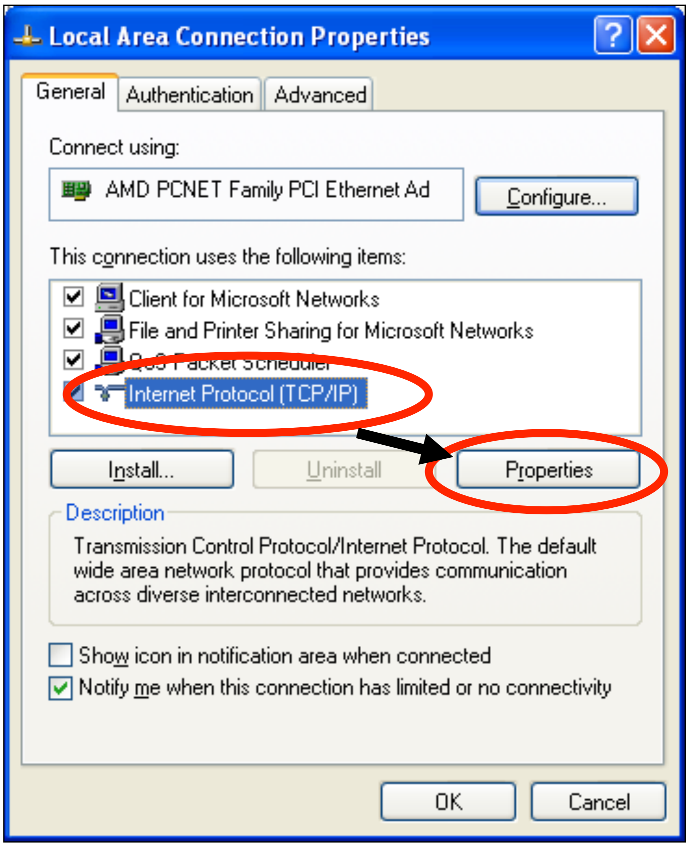
The access point uses the default IP address **192.168.2.2**. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. **192.168.2.x (x = 3 – 254).**

The procedure for modifying your IP address varies across different operating systems; 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).**

V-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”.



Local Area Connection Properties

General | Authentication | Advanced

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)

Description

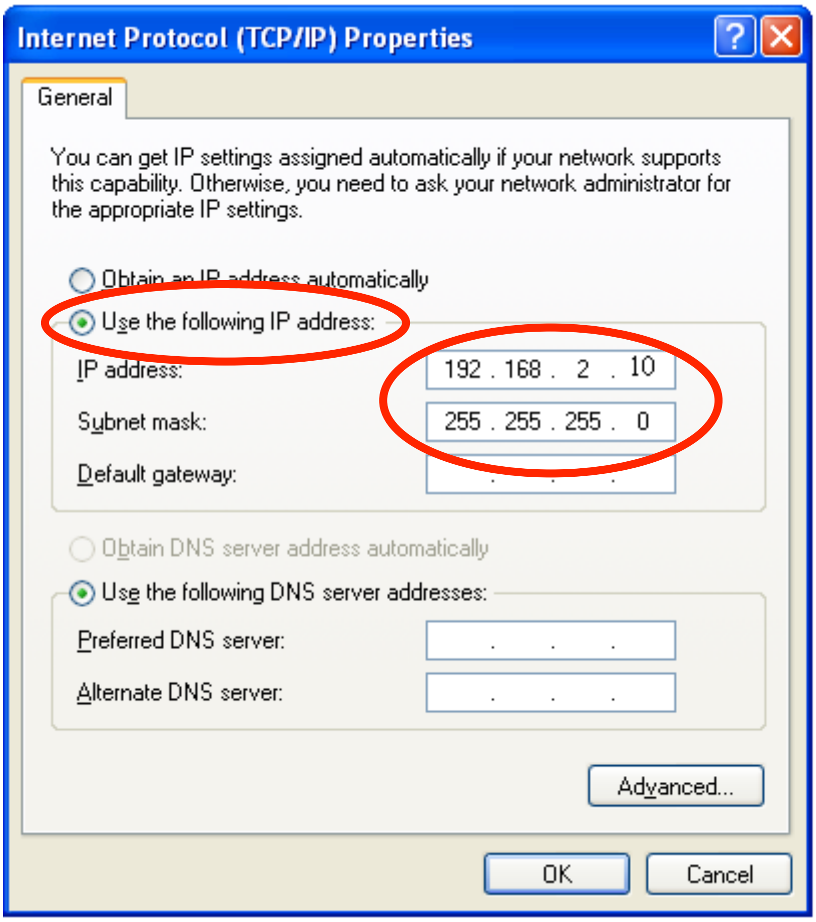
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ 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.



Internet Protocol (TCP/IP) 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

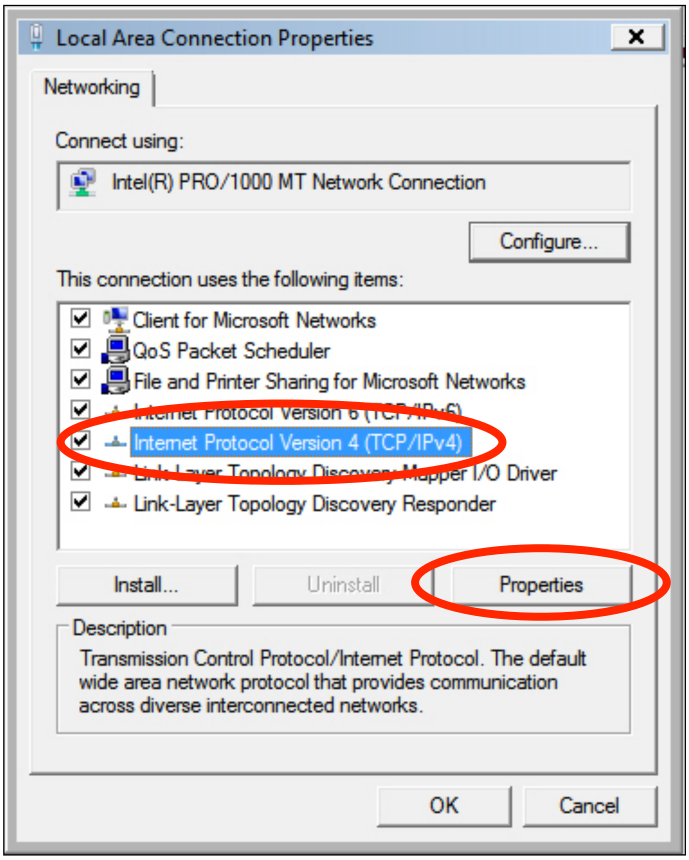
● Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

V-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

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

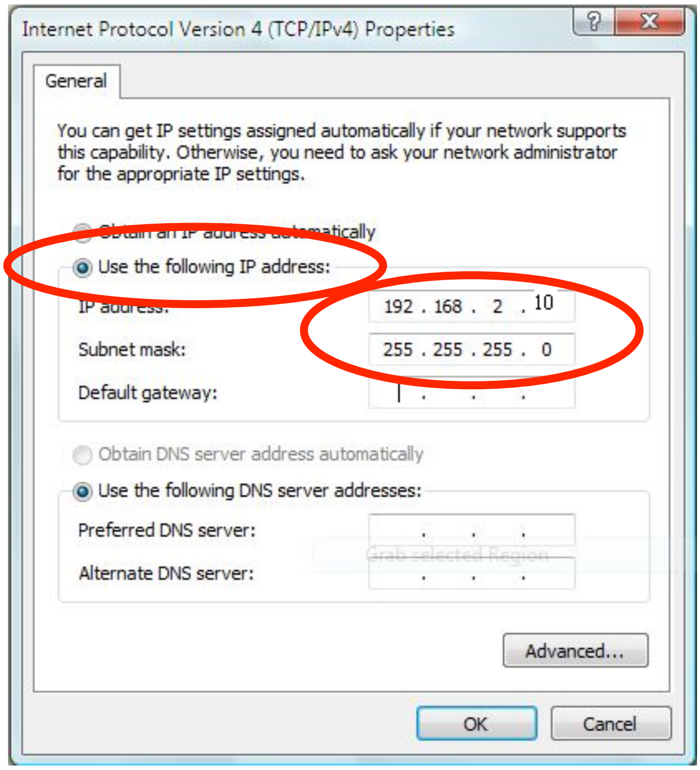
Description

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

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

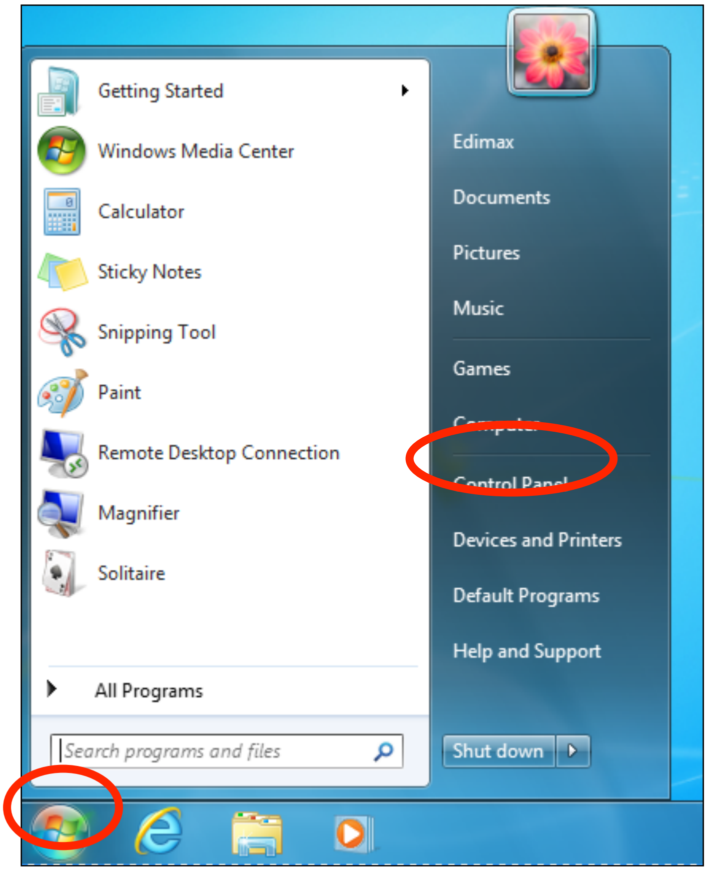
● Use the following DNS server addresses:

Preferred DNS server: . . .

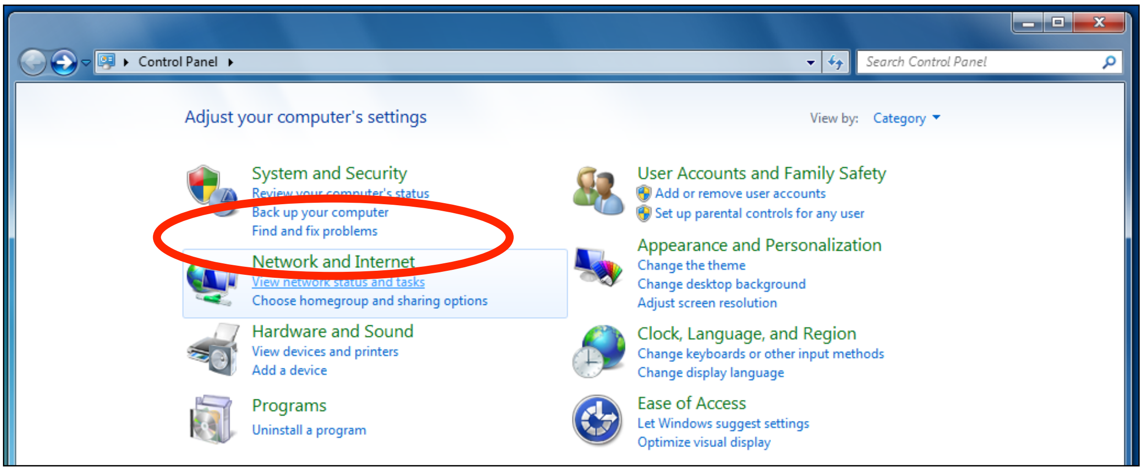
Alternate DNS server: . . .

V-1-3. Windows 7

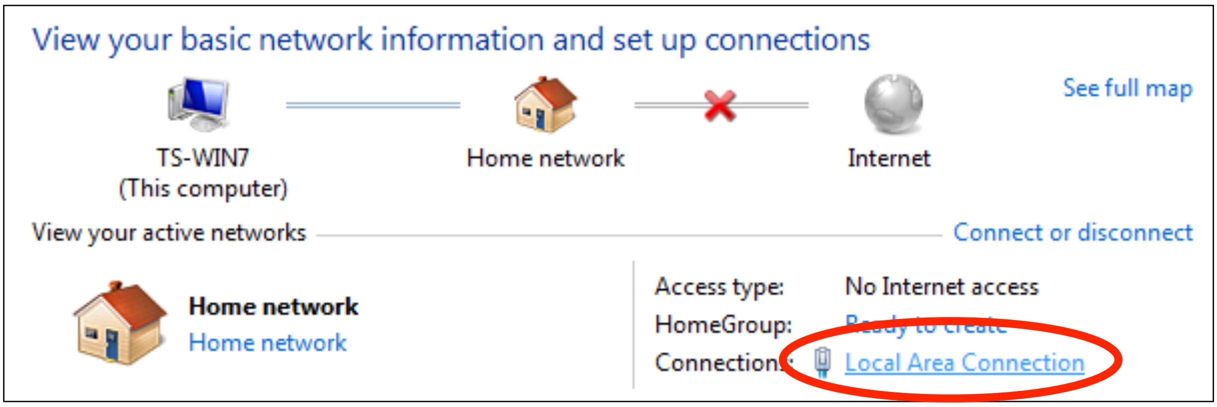
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



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”.



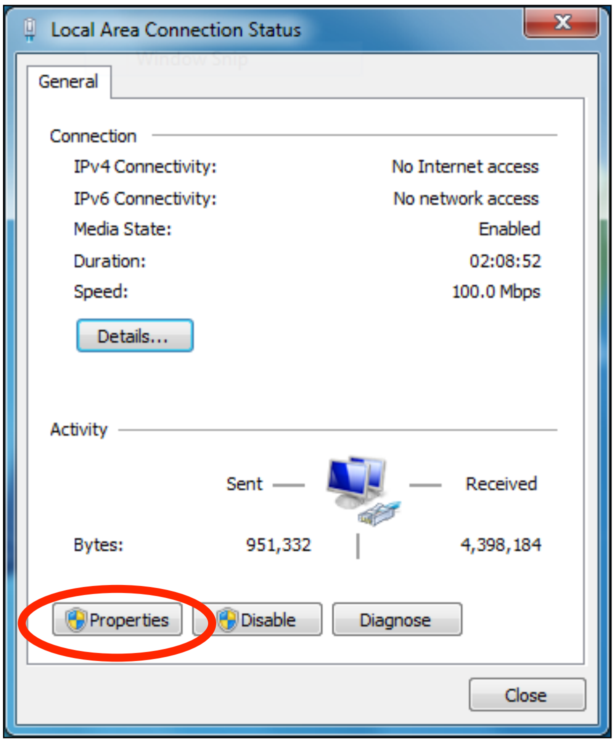
View your basic network information and set up connections

View your active networks — Connect or disconnect

Home network
Home network

Access type: No Internet access
HomeGroup: Ready to create
Connections: Local Area Connection

4. Click “Properties”.



Local Area Connection Status

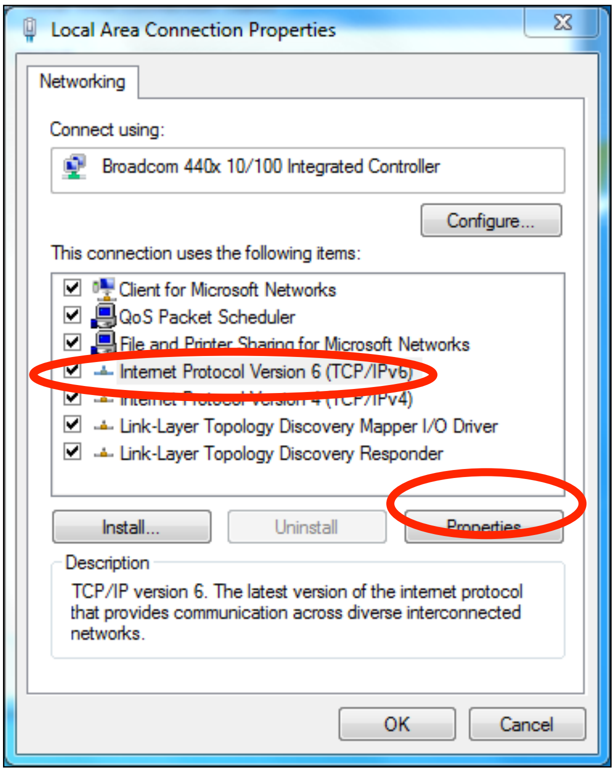
Connection

IPv4 Connectivity:	No Internet access
IPv6 Connectivity:	No network access
Media State:	Enabled
Duration:	02:08:52
Speed:	100.0 Mbps

Activity

	Sent	Received
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

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

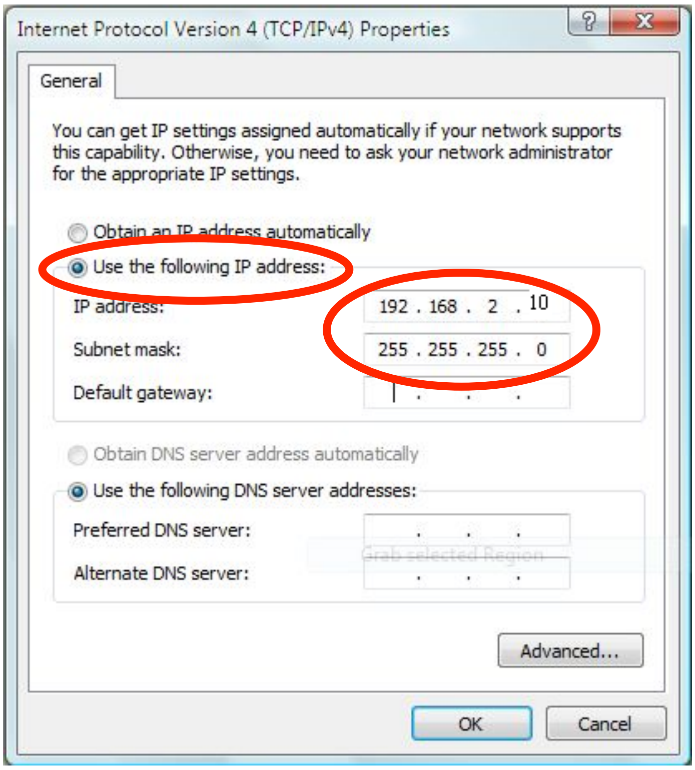
Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

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

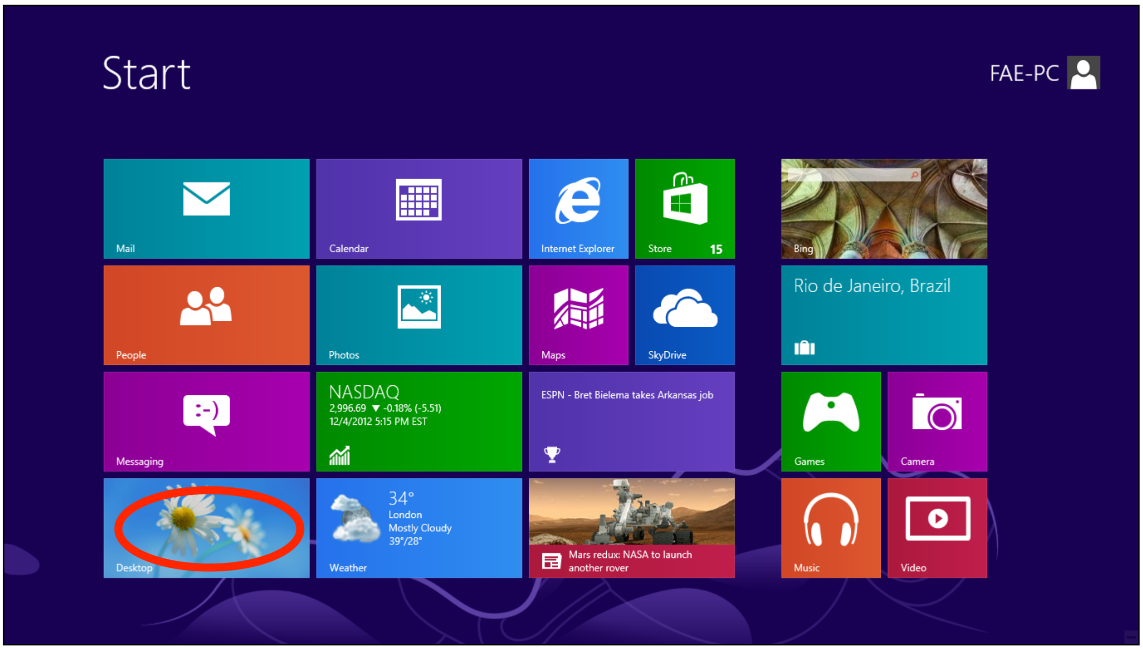
● Use the following DNS server addresses:

Preferred DNS server: . . .

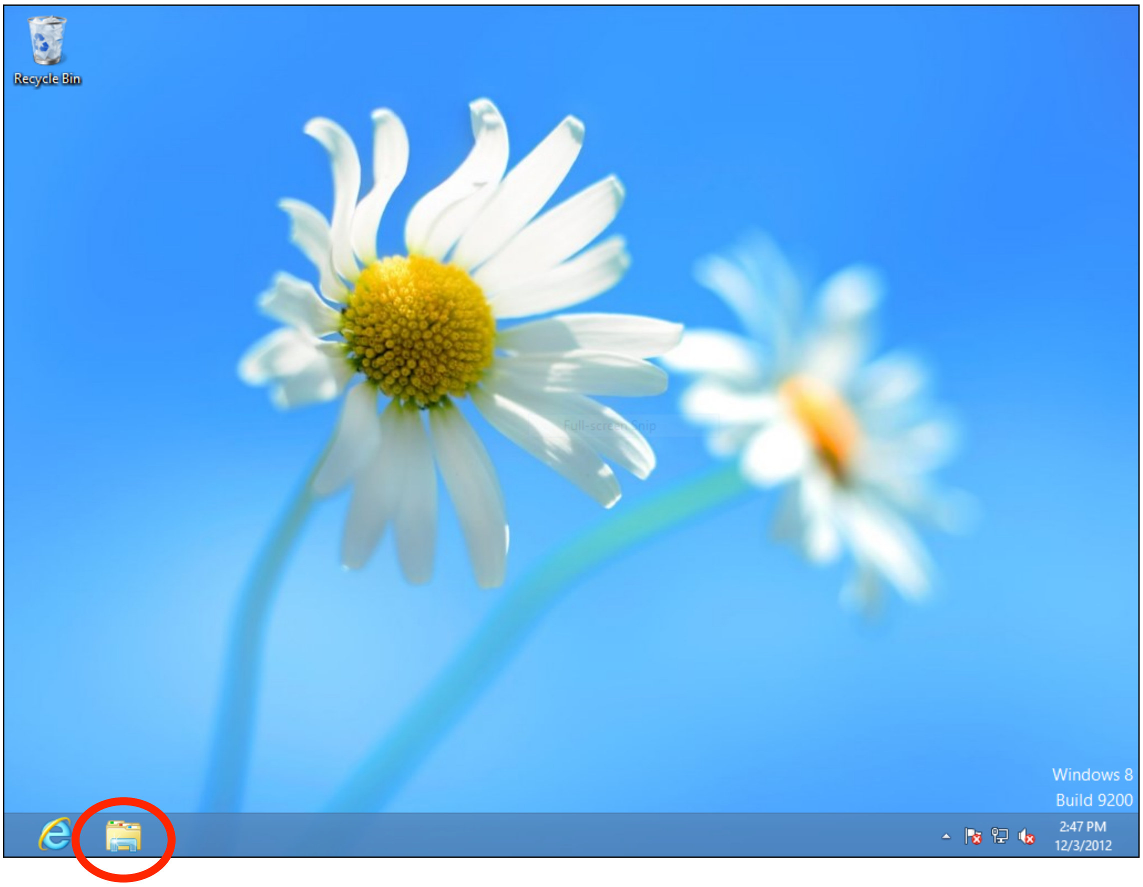
Alternate DNS server: . . .

V-1-4. Windows 8

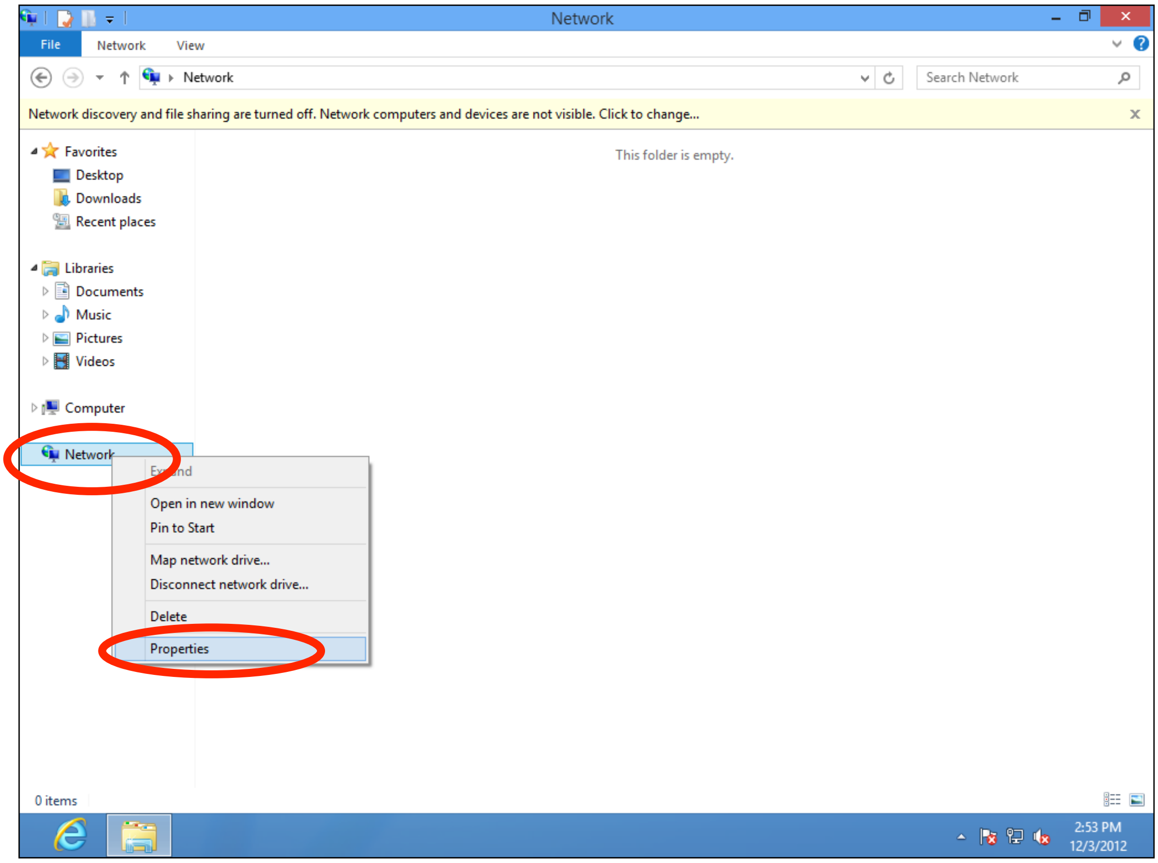
1. From the Windows 8 Start screen, you need to switch to desktop mode. Move your curser to the bottom left of the screen and click.



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



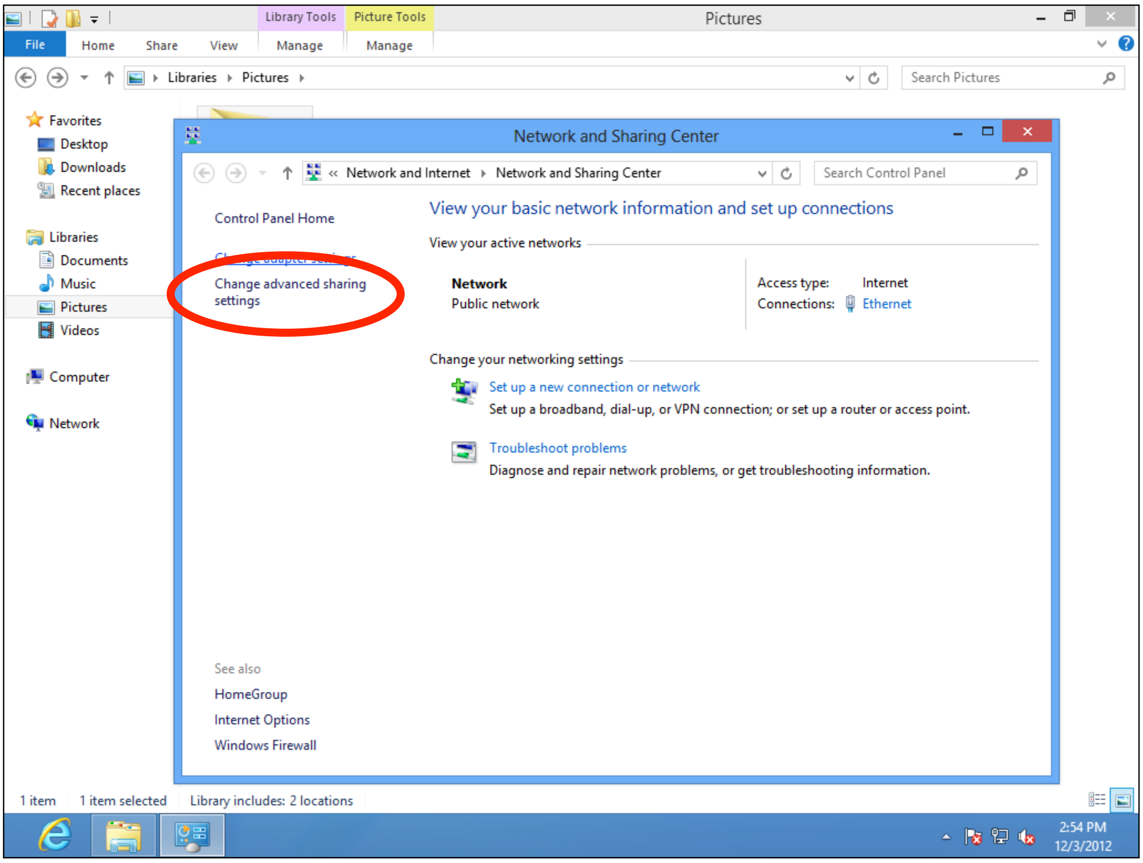
3. Right click “Network” and then select “Properties”.



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

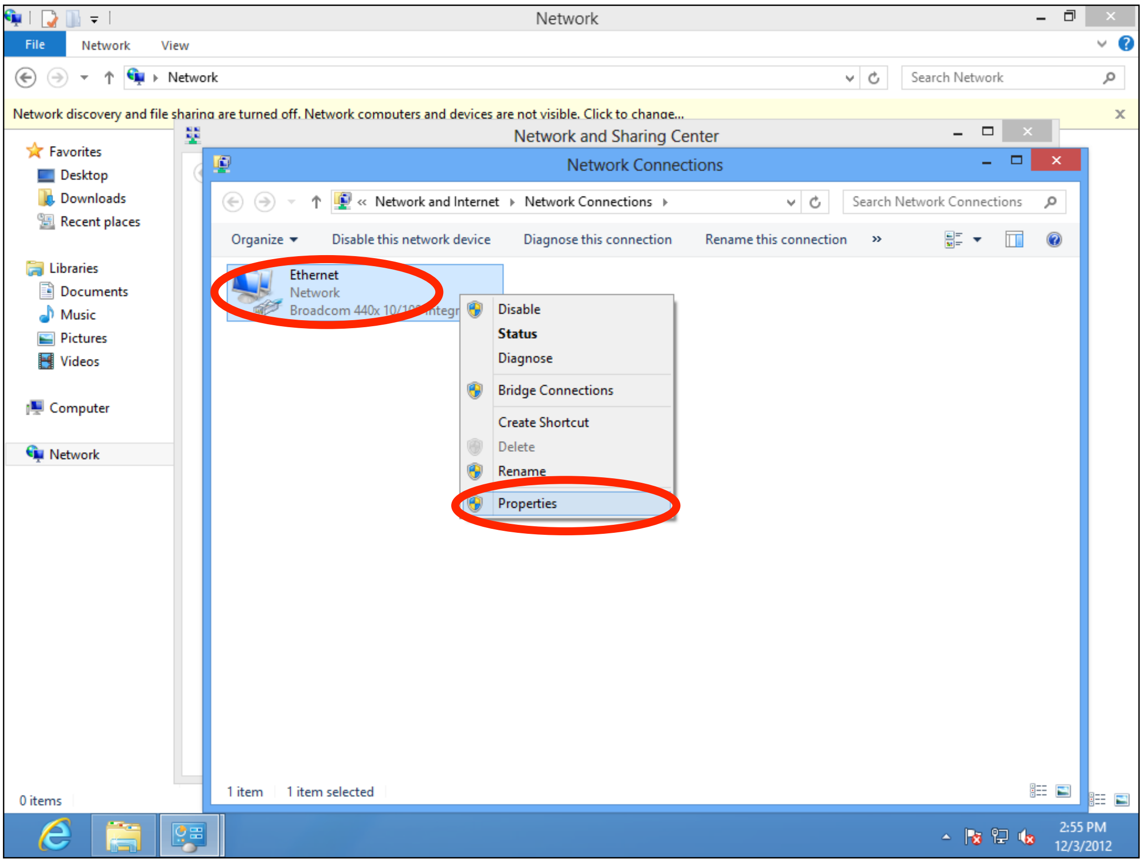
Access type: Internet
Connections: Ethernet

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.

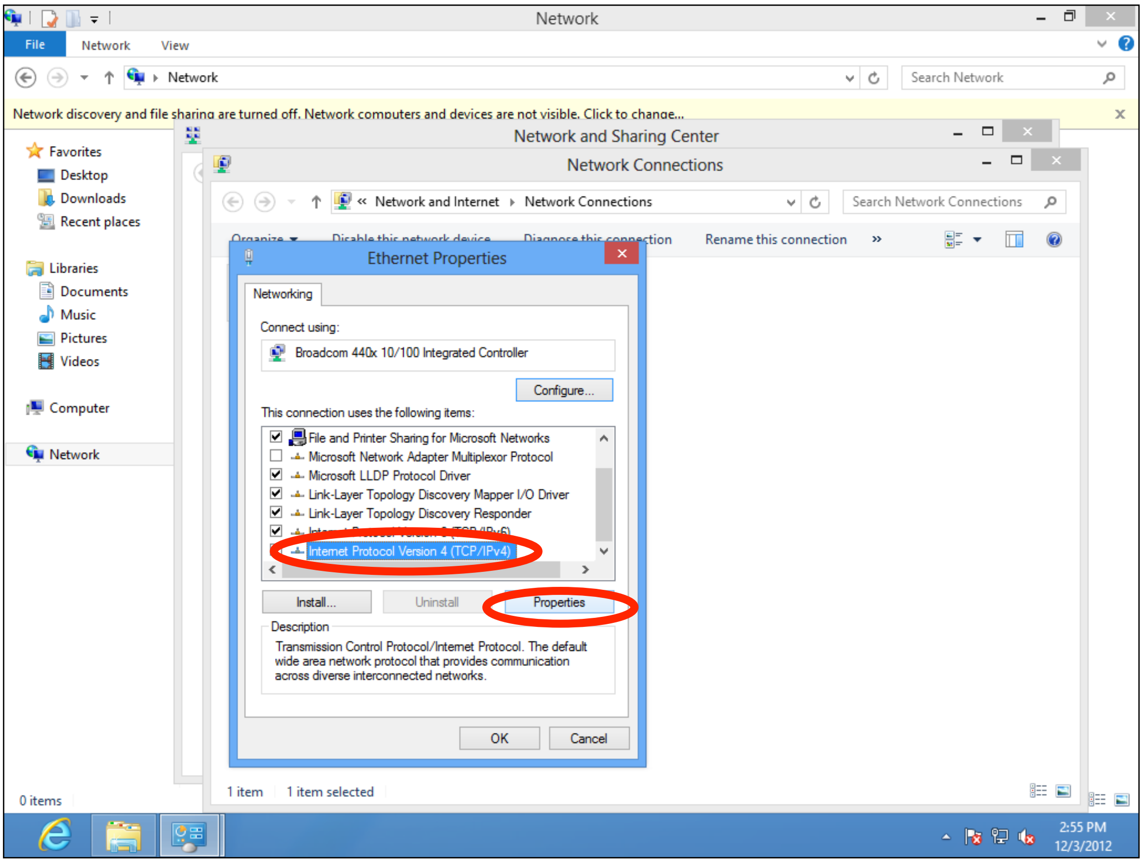
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

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...

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



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

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.

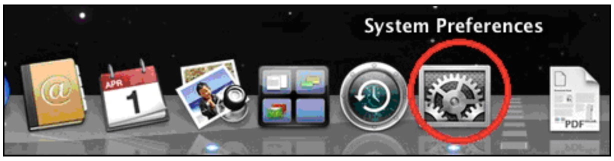
7. Select “Use the following IP address”, then input the following values:

IP address: 192.168.2.10
Subnet Mask: 255.255.255.0

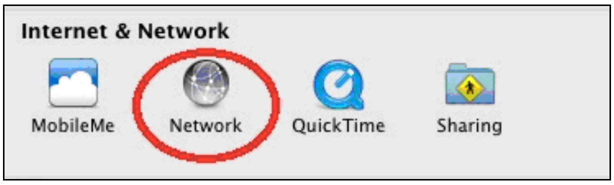
Click ‘OK’ when finished.

V-1-5. Mac

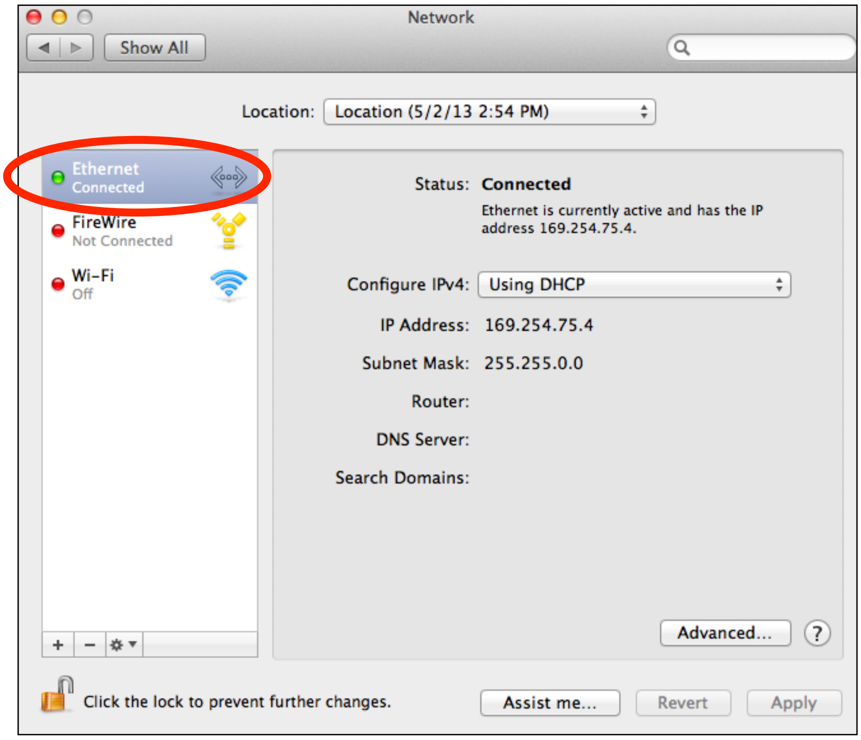
1. Have your Macintosh computer operate as usual, and click on "System Preferences"



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



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



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

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

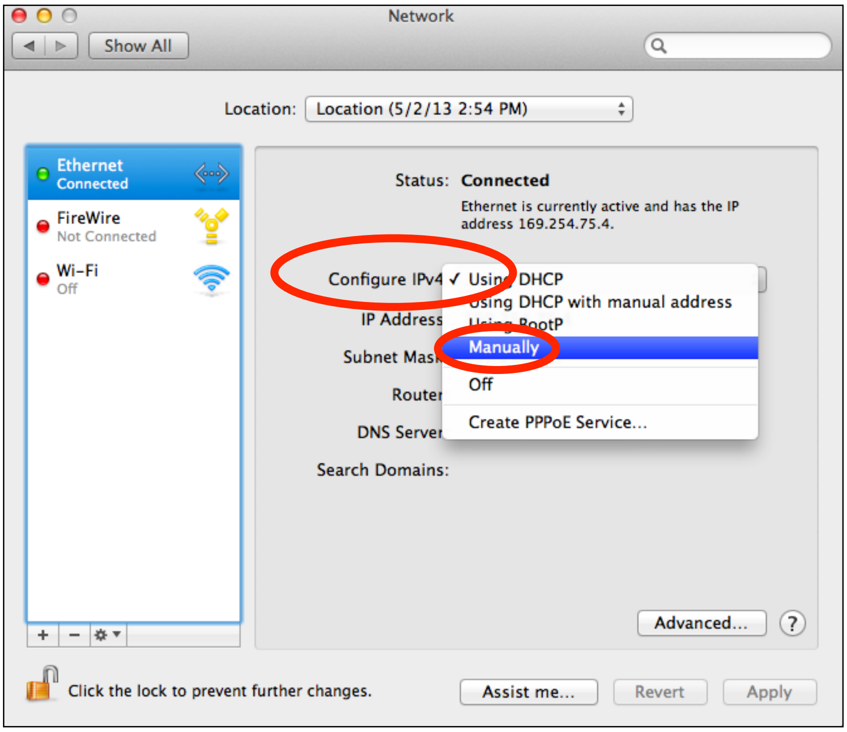
Router:

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: Manually

IP Address

Subnet Mask

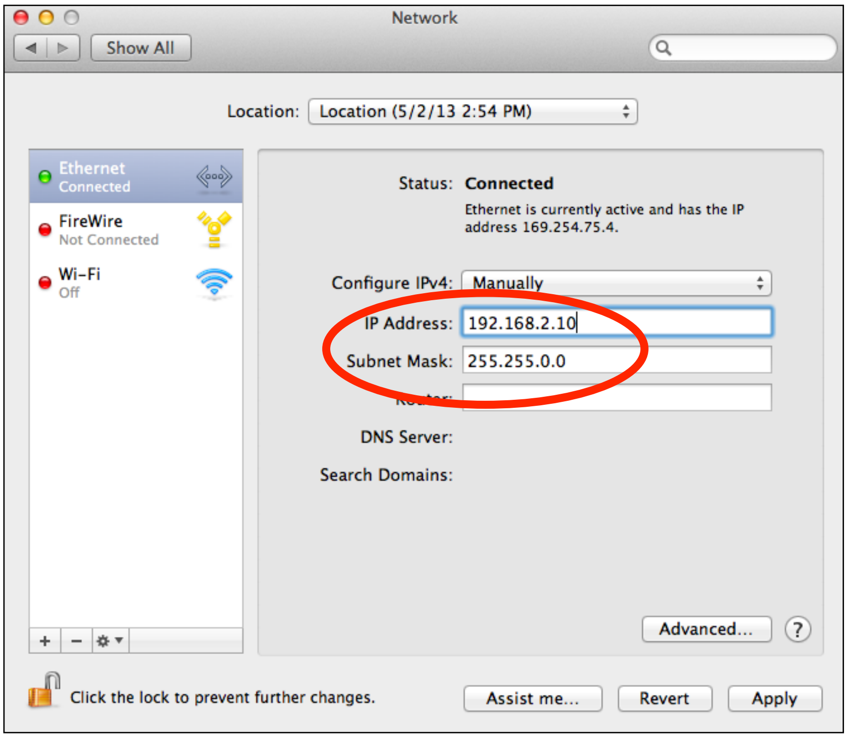
Router

DNS Server

Search Domains:

Click the lock to prevent further changes.

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:

Click the lock to prevent further changes.

V-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: 192.168.2.1. 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.

V-2. Hardware Specification

MCU/RF	MediaTek MT7620A(2.4GHz)
PHY/Switch	Qualcomm Atheros AR8035
Memory	DDR2 64MB
Flash	4MB
Physical Interface	-LAN: 10/100/1000 Gigabit Ethernet with PoE support 802.3af (PD In) -Reset Button -DC Power Jack
Power Requirement	Power over Ethernet, IEEE 802.3af DC : 12V / 1A
Antenna	Internal PIFA Antenna (3dBi 2.4GHz x 2)
Others	Internal Buzzer (Find me)

V-3. ENVIRONMENT & PHYSICAL

Temperature Range	Operation : 0 to 50□ (32□ to 122□) Storage : -20 to 60□ (-4□ to 140□)
Humidity	90% or less – Operating, 90% or less - Storage
Certifications	FCC, CE
Dimensions	176(D) x 30(H)mm
Weight	287g

COPYRIGHT

Copyright ©2015 by this company. All rights reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise, without the prior written permission of this company

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.

[redacted]

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