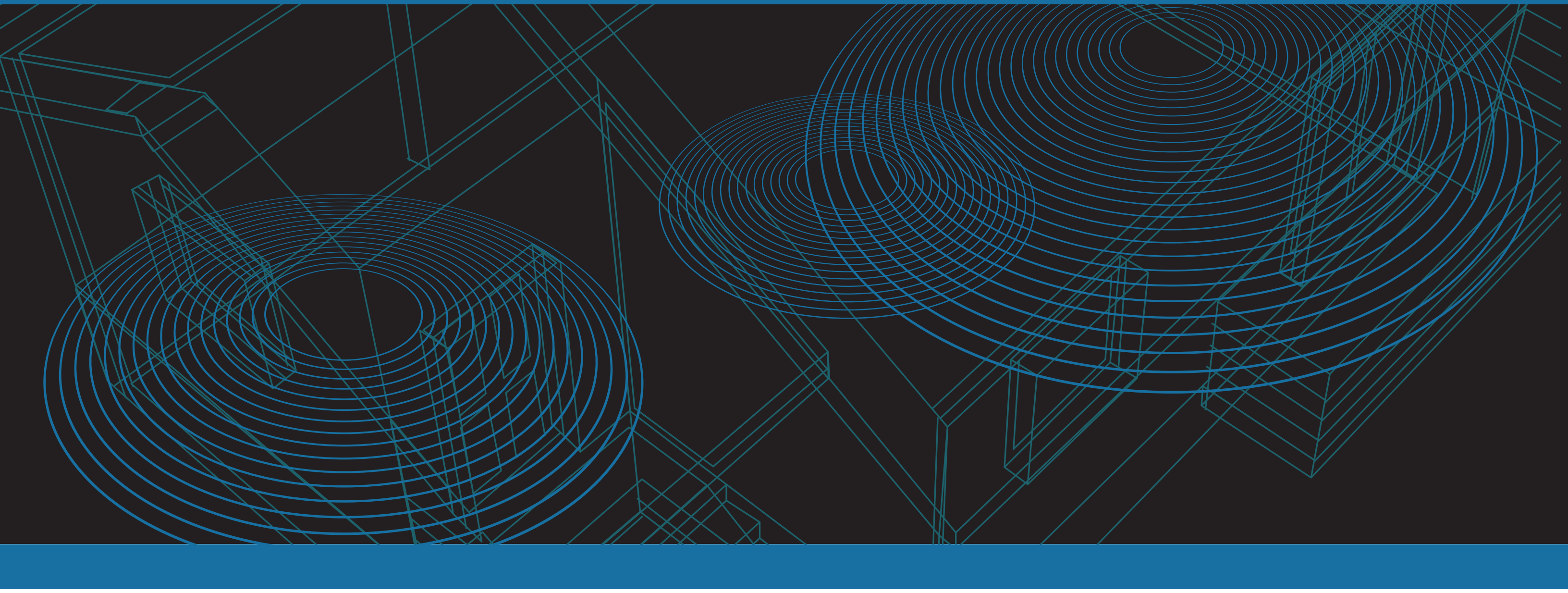
HAWKING® TECHNOLOGY

Wireless-1750AC Managed Access Point Pro

HW17ACM



website www.hawkingtech.com
e-mail techsupport@hawkingtech.com

USER'S MANUAL ▶▶

COPYRIGHT

Hawking Technologies 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 Hawking Technologies, its distributor, or its dealer) assumes the entire cost of all necessary servicing, repair, and any incidental or consequential damages resulting from any defect in the software. Further, this company reserves the right to revise this publication and to make changes from time to time in the contents thereof without obligation to notify any person of such revision or changes.

Federal Communication Commission
Interference Statement

FCC Part 15

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 equipment must be installed and operated in accordance with provided instructions and a minimum 20 cm spacing must be provided between computer mounted antenna and person’s body (excluding extremities of hands, wrist and feet) during wireless modes of operation.

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.

Federal Communication Commission (FCC) Radiation Exposure Statement

This equipment complies with FCC radiation exposure set forth for an uncontrolled environment. In order to avoid the possibility of exceeding the FCC radio frequency exposure limits, human proximity to the antenna shall not be less than 20cm (8 inches) during normal operation.

The antenna(s) used for this transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

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, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

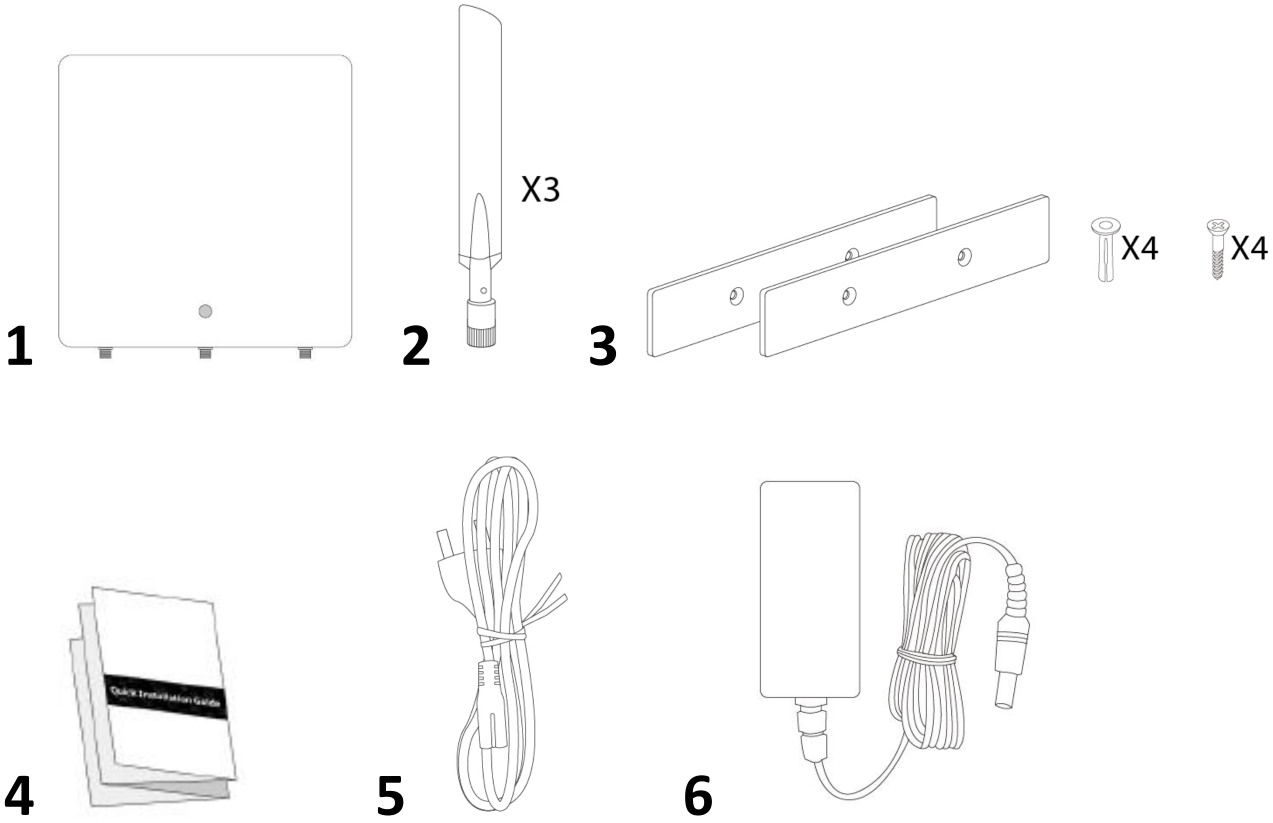
The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

CONTENTS

1-1. Package Contents

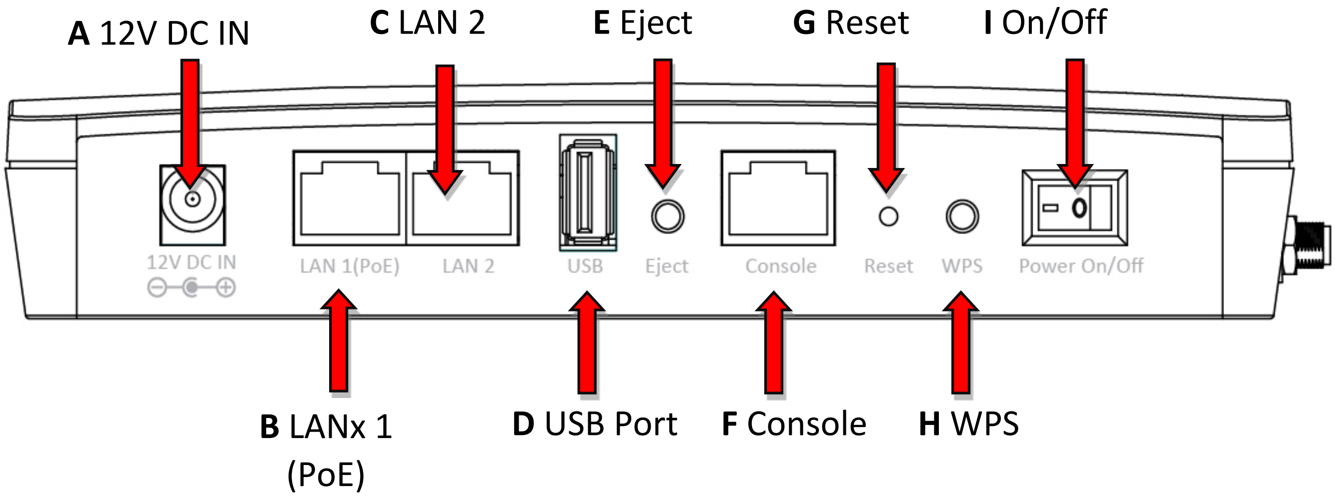


1. HW17ACM
2. 3x 2dBi Omnidirectional Dual Band Antennas
3. Magnetic Wall Mount x 2 screws
4. Quick Installation Guide
5. Power Cord
6. Power Adapter 12V/4A

1-2. System Requirements

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

1-3. Hardware Overview



A. 12V DC port to connect the power adapter

B. LAN port with Power over Ethernet (PoE PD, IN)

C. LAN port with Power over Ethernet (PoE PSE, OUT)

D. USB Port for system log

E. Eject an attached USB device

F. Connect a management console

G. Reset the access point to factory default settings

H. Wi-Fi Protected Setup (WPS) button

I. Switch the access point on/off

1-4. LED Status

LED Status	Description
Off	The access point is off.
Blue	The access point is on.
Amber	The access point is starting up.

1-5. 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 20 seconds then release the button.

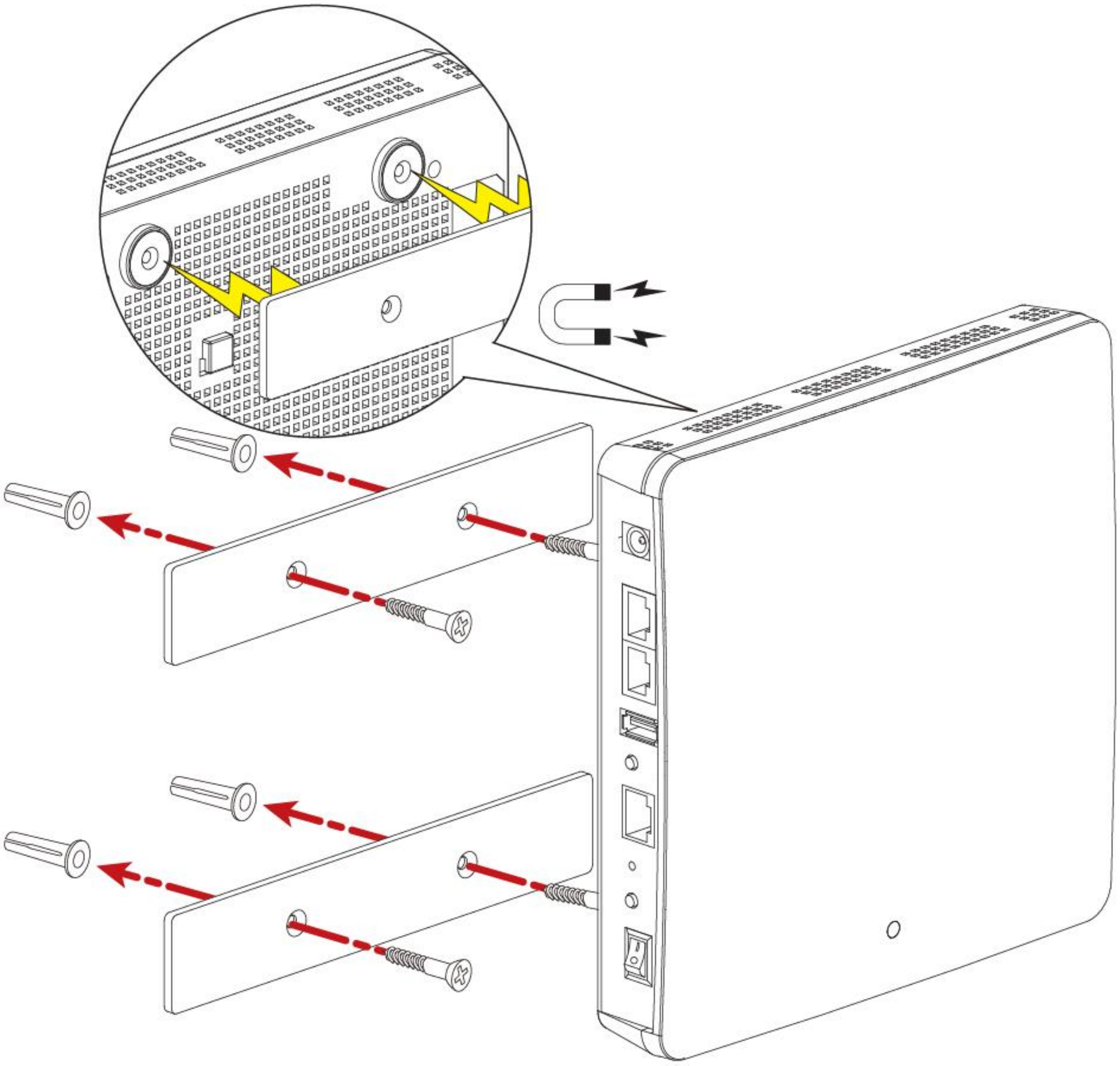
⚠ ***You may need to use a pin or similar sharp object to push the reset button.***

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

I-6. Magnetic Wall Mount

The access point includes a magnetic wall mount which requires some assembly.

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



2. Press the back of your access point firmly against the two wall mounted magnetic strips, with the access point in the correct position, upright orientation as displayed above.

Ensure your access point is securely attached to the magnetic strips.

I-7. Console

The access point can be configured via the “Console” port located on the access point’s side panel using a terminal-emulation program (e.g. HyperTerminal).

Use the following configuration settings for terminal-emulation programs:

Baud Rate	115200
Data	8 bit
Parity	None
Stop	1 bit
Flow Control	None

1-8. Safety Information

In order to ensure the safe operation of the device and its users, please 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. Please 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, please 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.

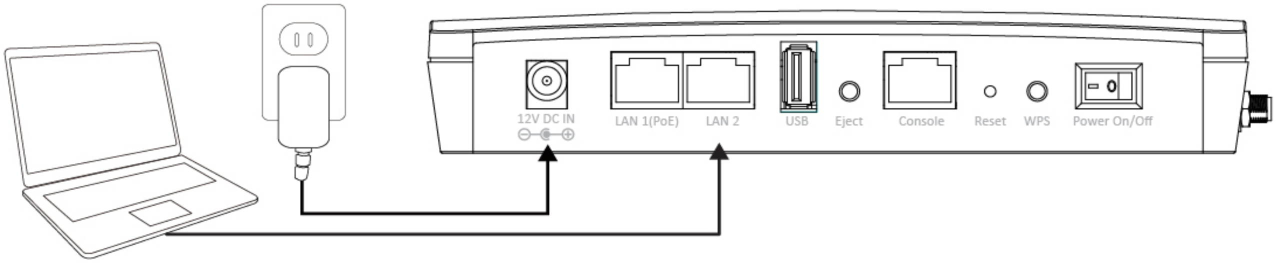
9. If you smell burning or see smoke coming from the access point or power adapter, then disconnect the access point and power adapter immediately, as far as it is safely possible to do so. Call your dealer of purchase for help.

Your access point can be up and running in just a few minutes. This quick installation guide will help to set up your access point and configure its basic settings. Please follow the instructions in the chapters below:

2-1. Initial Setup

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

2. Connect the power adapter to the access point's 12VDC port and plug the power adapter into a power supply using the included cable.

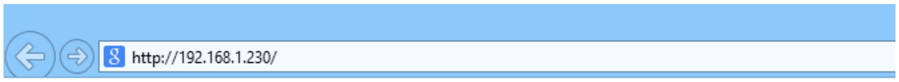


3. Please wait a moment for the access point to start up. The access point is ready when the LED is **blue**.

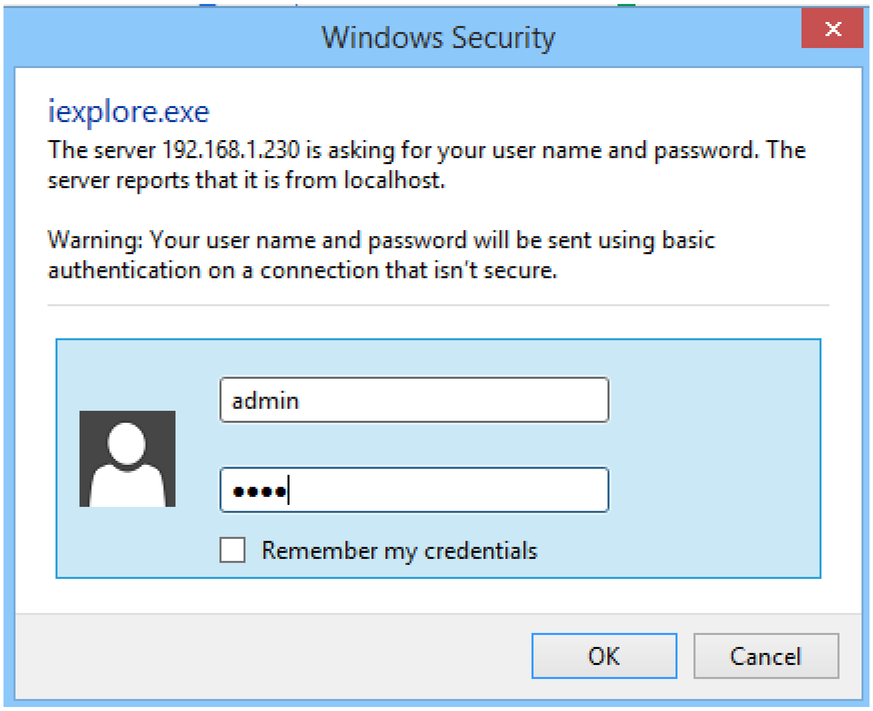
4. Set your computer's IP address to **192.168.1.x** where **x** is a number in the range **1 – 100**. If you are unsure how to do this, please refer to the Chapter 5-1.

Please 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 **192.168.1.230** into the URL bar of a web browser.


http://192.168.1.230/

6. You will be prompted for a username and password. Enter the default username "admin" and the default password "1234".



Windows Security

iexplore.exe

The server 192.168.1.230 is asking for your user name and password. The server reports that it is from localhost.

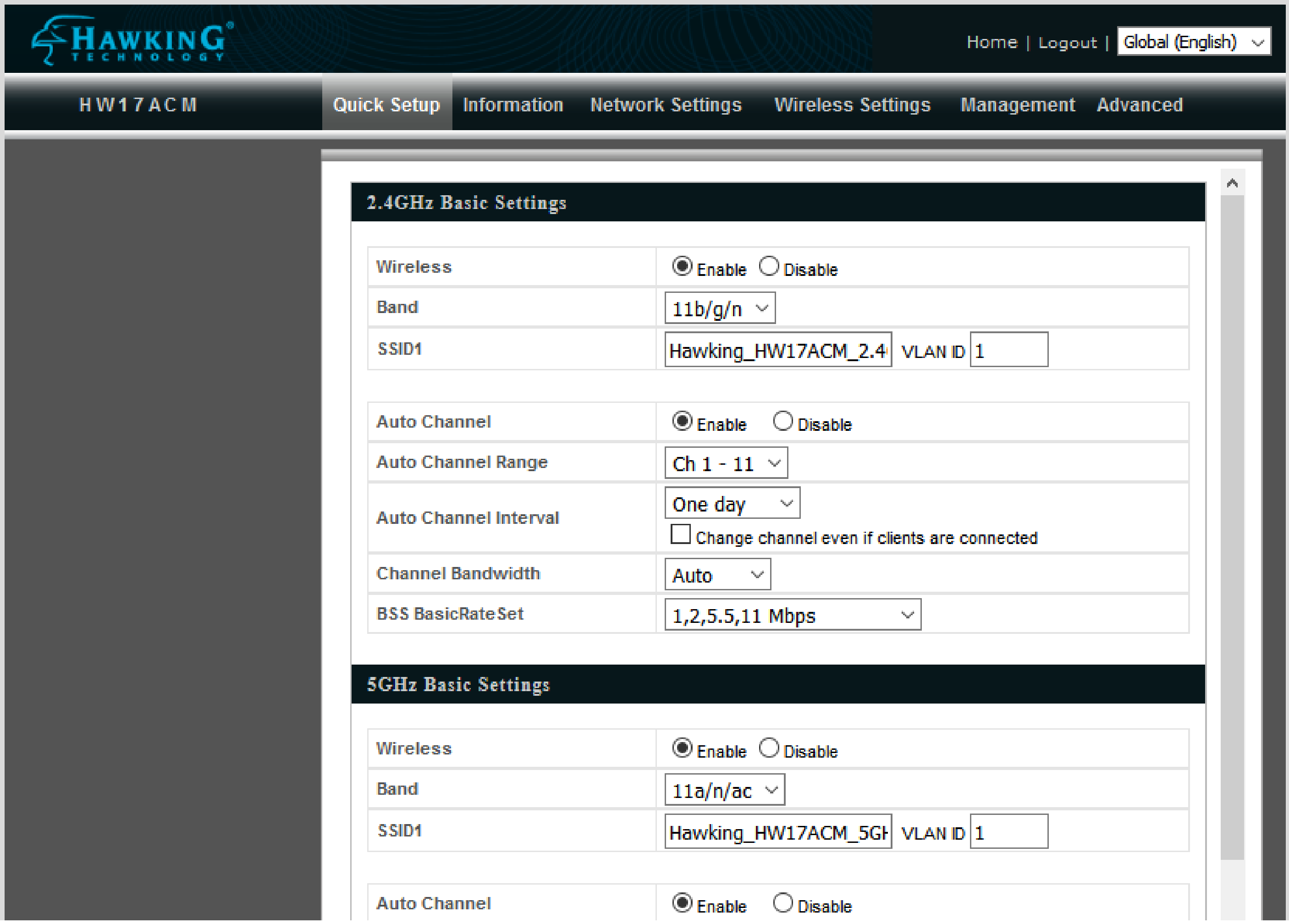
Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

admin

••••

□ Remember my credentials

7. You will arrive the "Quick Setup" screen shown below.



2.4GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11b/g/n
SSID1	Hawking_HW17ACM_2.4 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

5GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11a/n/ac
SSID1	Hawking_HW17ACM_5GH VLAN ID 1
Auto Channel	● Enable ○ Disable

8. Next, please follow the instructions below in **2-2. Quick Setup** to configure the access point’s basic settings.

For more advanced configurations, please refer to Chapter 4. Browser Based Configuration Interface.

2-2. Quick Setup Settings

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

1 ***2.4GHz & 5GHz SSID LAN IP Address***

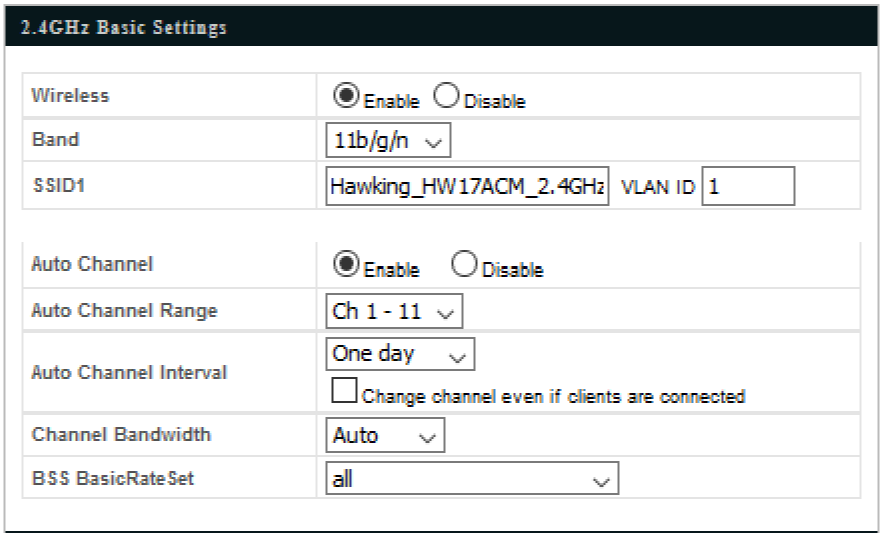
2 ***LAN IP Address***

3 ***2.4GHz & 5GHz SSID Security***

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

1. To change the SSID of your access point's 2.4GHz wireless network(s), go to "2.4GHz Basic Settings". Enter the new SSID for your 2.4GHz wireless network in the "SSID1" field". The default 2.4GHz SSID is "Hawking_HW17ACM_5GHz"

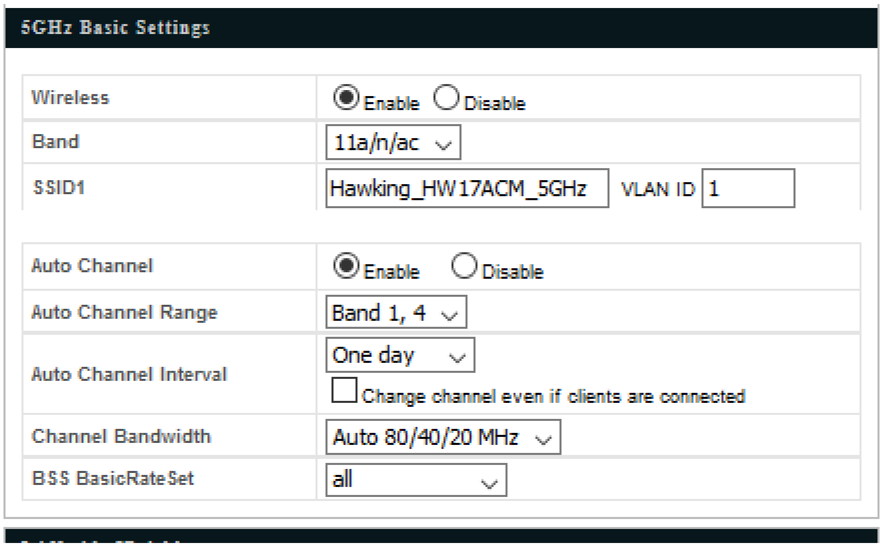
To utilize multiple 2.4GHz SSIDs, open the drop down menu labelled *"Enable SSID number"* ***and select how many SSIDs you require. Then enter a new SSID in the corresponding numbered fields below, before clicking "Apply".***



2.4GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11b/g/n
SSID1	Hawking_HW17ACM_2.4GHz 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	all

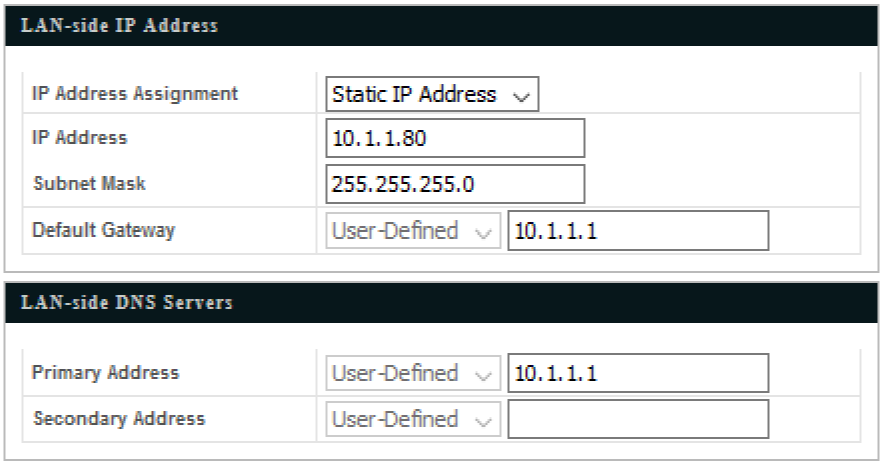
2. Go to **"5GHz Basic Settings"** and repeat step 1 for the access point's 5GHz AC wireless network. The default 5GHz SSID is "Hawking_HW17ACM_5GHz"



5GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11a/n/ac
SSID1	Hawking_HW17ACM_5GHz VLAN ID 1
Auto Channel	● Enable ○ Disable
Auto Channel Range	Band 1, 4
Auto Channel Interval	One day □ Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz
BSS BasicRateSet	all

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



LAN-side IP Address

IP Address Assignment	Static IP Address	
IP Address	10.1.1.80	
Subnet Mask	255.255.255.0	
Default Gateway	User-Defined	10.1.1.1

LAN-side DNS Servers

Primary Address	User-Defined	10.1.1.1
Secondary Address	User-Defined	

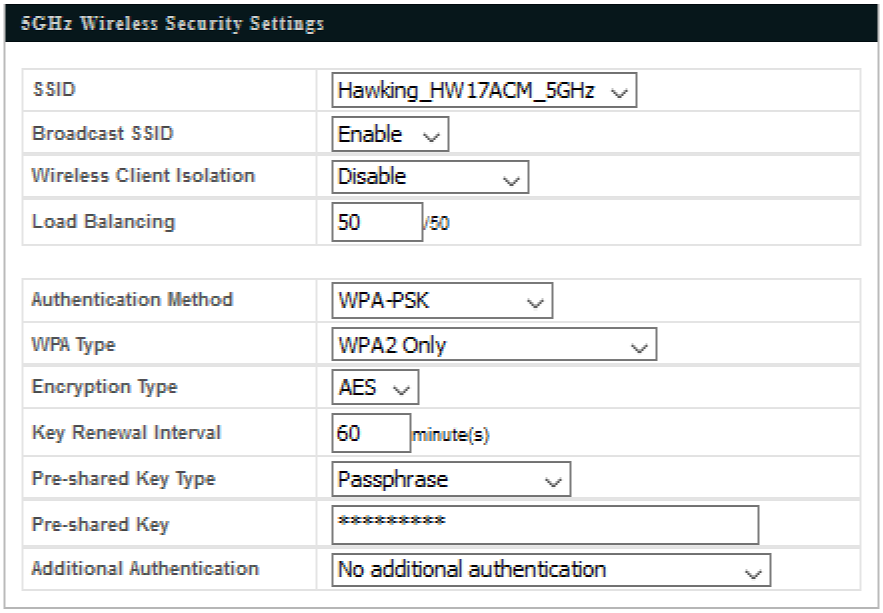
4. Enter the IP address settings you wish to use for your access point. You can use a dynamic (DHCP) or static IP address, depending on your network environment. Click "Next" to save the changes and to go to the security settings.

When you change your access point's IP address, you need to use the new IP address to access the browser based configuration interface instead of the default IP *192.168.1.230.*

5. To configure the security of your access point's 2.4GHz wireless network(s), go to **"2.4GHz Wireless Security Settings"**. Select an "Authentication Method" and enter a "Pre-shared Key" or "Encryption

Key” depending on your choice, then click “Apply”. Hawking recommends at least WPA/WPA2 security.

If using multiple SSIDs, specify which SSID to configure using the “SSID” drop down menu.



5GHz Wireless Security Settings

SSID	Hawking_HW17ACM_5GHz
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	**********
Additional Authentication	No additional authentication

6. Go to **“Wireless Setting” > “5GHz 11ac 11an”** and repeat steps **5** for the access point’s 5GHz wireless network. Click “Apply” and the device will now reset and save your settings.

7. The basic settings of your access point are now configured. Please refer to **Chapter 3 - Hardware Installation** for guidance on connecting your access point to a router or PoE switch.

2-3 Wi-Fi Protected Setup (WPS)

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. You can use the WPS button to establish a connection between the access point and a WPS-compatible wireless device/client.

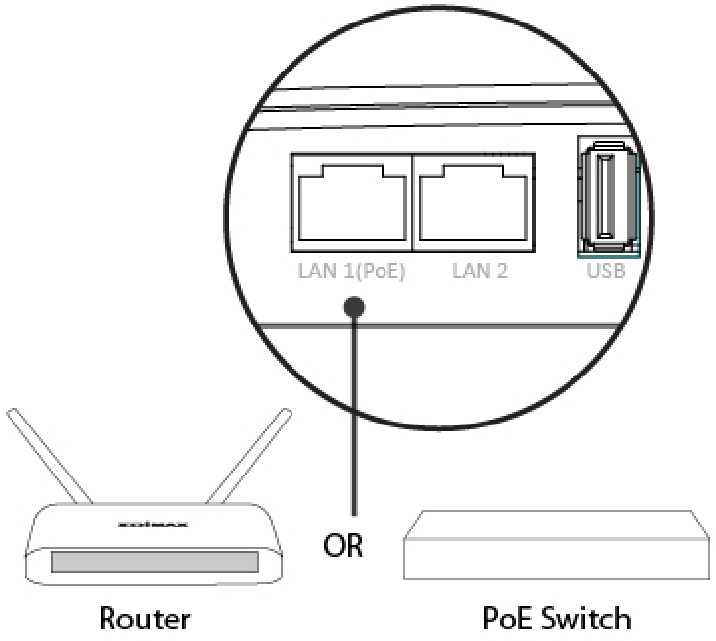
1. Press and hold the WPS/Reset button on the back of the access point for 2 seconds.

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

3. The devices will establish a connection.

3-1. Connecting the access point to a router or PoE switch

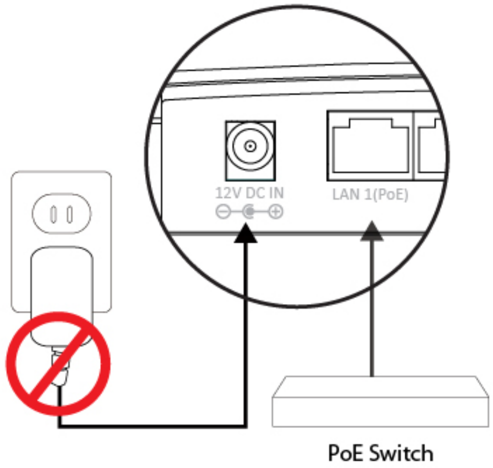
1. Connect a router or PoE switch to the access point's LAN 1 port using an Ethernet cable. PoE switches must be connected to the access point's LAN 1 port.



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

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.

Do not use the power adapter if you are using a PoE switch.



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

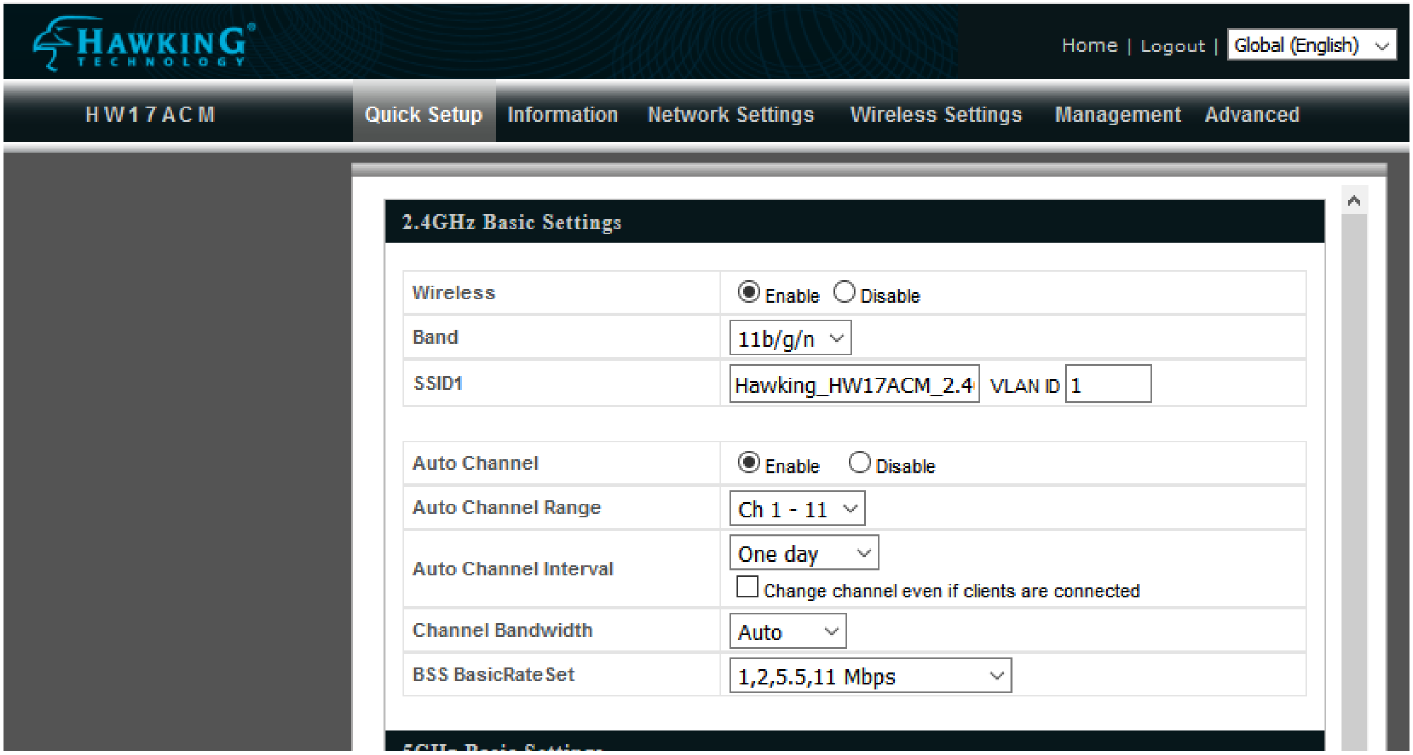
1. Connect a computer to your access point using an Ethernet cable.

2. Enter your access point's IP address in the URL bar of a web browser (as configured in Chapter 2-2. The access point's default IP address is **192.168.1.230.**

3. You will be prompted for a username and password. The default username is "admin" and the default password is "1234", though it was recommended that you change the password during setup (see **Chapter 2-2 Basic Settings**).

If you cannot remember your password, reset the access point back to its factory default settings. Refer to *Chapter 1-5 Reset*

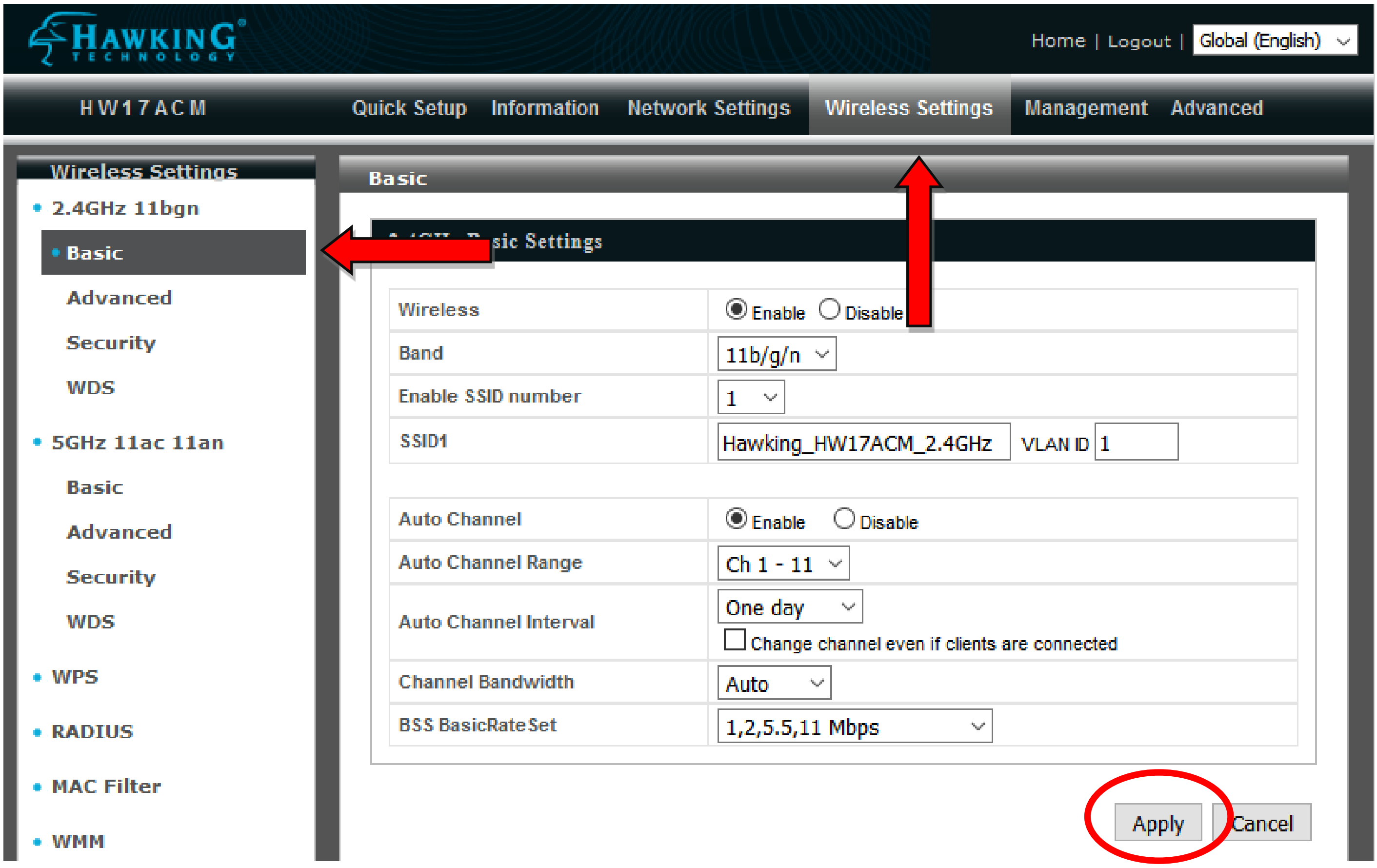
4. You will arrive at the "Settings" screen shown below.



2.4GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11b/g/n
SSID1	Hawking_HW17ACM_2.4 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

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

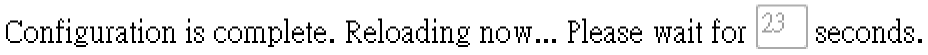


sic Settings

Wireless	● Enable ○ Disable
Band	11b/g/n
Enable SSID number	1
SSID1	Hawking_HW17ACM_2.4GHz 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.

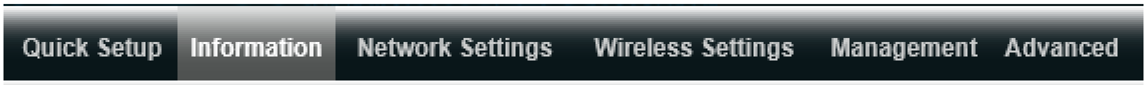
Please wait a few seconds for the access point to reload after you "Apply" changes, as shown below.



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

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

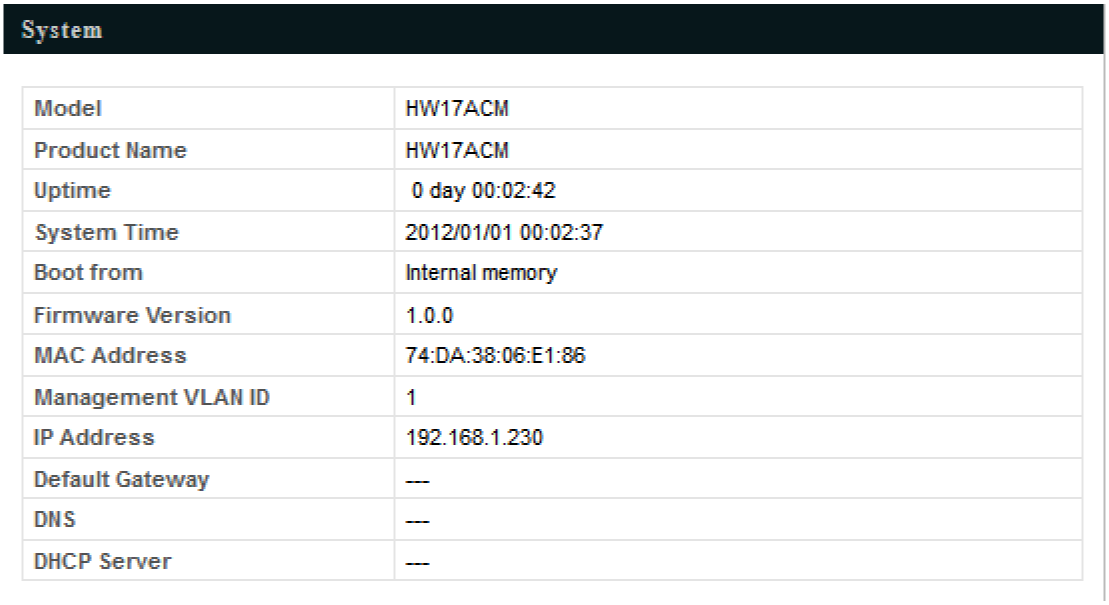
4-1. Information



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

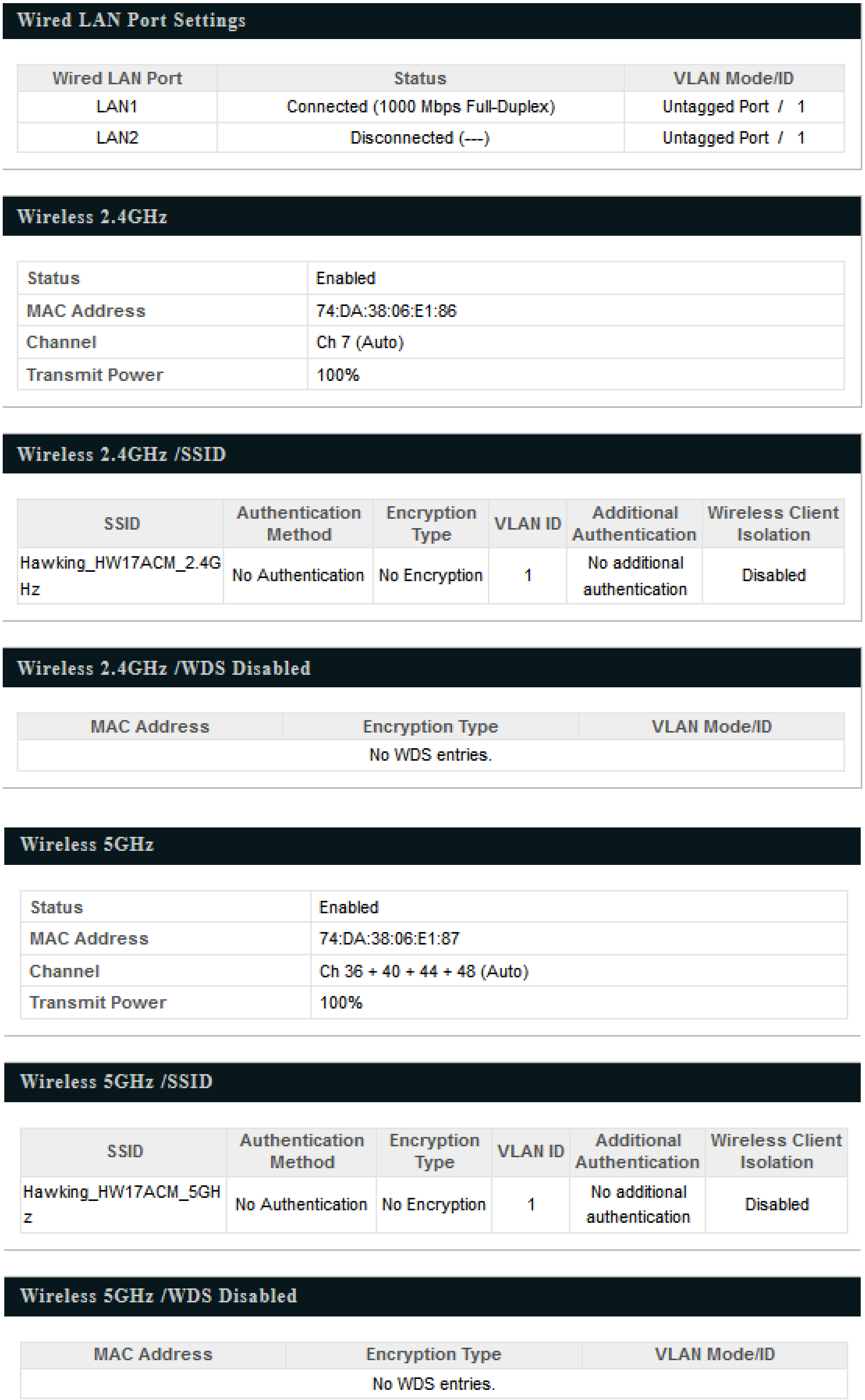
4-1-1. System Information

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



System

Model	HW17ACM
Product Name	HW17ACM
Uptime	0 day 00:02:42
System Time	2012/01/01 00:02:37
Boot from	Internal memory
Firmware Version	1.0.0
MAC Address	74:DA:38:06:E1:86
Management VLAN ID	1
IP Address	192.168.1.230
Default Gateway	---
DNS	---
DHCP Server	---



Wired LAN Port Settings

Wired LAN Port	Status	VLAN Mode/ID
LAN1	Connected (1000 Mbps Full-Duplex)	Untagged Port / 1
LAN2	Disconnected (---)	Untagged Port / 1

Wireless 2.4GHz

Status	Enabled
MAC Address	74:DA:38:06:E1:86
Channel	Ch 7 (Auto)
Transmit Power	100%

Wireless 2.4GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
Hawking_HW17ACM_2.4GHz	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 2.4GHz /WDS Disabled

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

Wireless 5GHz

Status	Enabled
MAC Address	74:DA:38:06:E1:87
Channel	Ch 36 + 40 + 44 + 48 (Auto)
Transmit Power	100%

Wireless 5GHz /SSID

SSID	Authentication Method	Encryption Type	VLAN ID	Additional Authentication	Wireless Client Isolation
Hawking_HW17ACM_5GHz	No Authentication	No Encryption	1	No additional authentication	Disabled

Wireless 5GHz /WDS Disabled

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

System	
Model	Displays the model number of the access point.
Product Name	Displays the product name for reference, which consists of “AP” plus the MAC address.
Uptime	Displays the total time since the device was turned on.
Boot From	Displays information for the booted hardware, booted from either USB or internal memory
Version	Displays the firmware version.
MAC Address	Displays the access point’s MAC address.
Management VLAN ID	Displays the management VLAN ID.
IP Address	Displays the IP address of this device. Click “Refresh” to update this value.
Default Gateway	Displays the IP address of the default gateway.
DNS	IP address of DNS (Domain Name Server).
DHCP Server	IP address of DHCP Server.

Wired LAN Port Settings	
Wired LAN Port	Specifies which LAN port.
Status	Displays the status of the LAN port (connected or disconnected).
VLAN Mode/ID	Displays the VLAN mode (tagged or untagged) and VLAN ID for the LAN port. See **4-2-3. VLAN**

Wireless 2.4GHz (5GHz)	
Status	Displays the status of the 2.4GHz or 5GHz wireless (enabled or disabled).
MAC Address	Displays the access point’s MAC address.
Channel	Displays the channel number the specified wireless frequency is using for broadcast.
Transmit Power	Displays the wireless radio transmit power level as a percentage.

Wireless 2.4GHz (5GHz) / SSID	
SSID	Displays the SSID name(s) for the specified frequency.

Authentication Method	Displays the authentication method for the specified SSID. See **4-3. Wireless Settings**
Encryption Type	Displays the encryption type for the specified SSID. See **4-3. Wireless Settings**
VLAN ID	Displays the VLAN ID for the specified SSID. See **4-2-3. VLAN**
Additional Authentication	Displays the additional authentication type for the specified SSID. See **4-3. Wireless Settings**
Wireless Client Isolation	Displays whether wireless client isolation is in use for the specified SSID. See **4-2-3. VLAN**

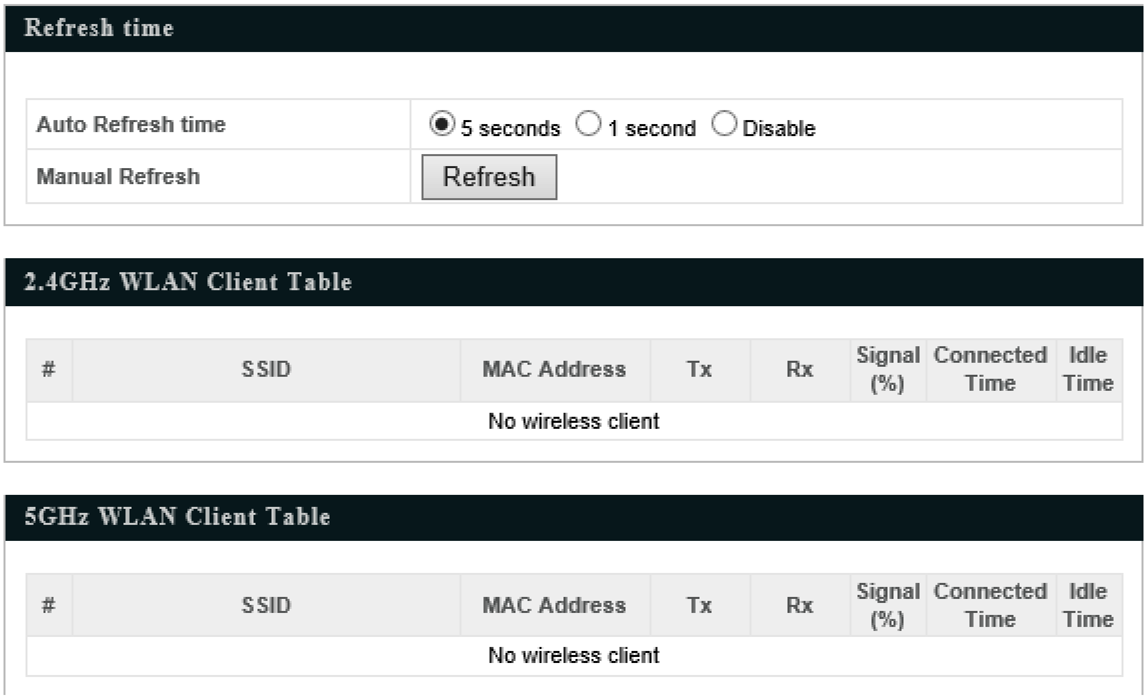
Wireless 2.4GHz (5GHz) / WDS Status	
MAC Address	Displays the peer access point's MAC address.
Encryption Type	Displays the encryption type for the specified WDS. See **4-3-1-4. WDS**
VLAN Mode/ID	Displays the VLAN ID for the specified WDS. See **4-3-1-4. WDS**

Refresh	Click to refresh all information.

4-1-2. Wireless Clients

• Wireless Clients

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



Refresh time

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

2.4GHz WLAN Client Table

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

5GHz WLAN Client Table

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

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

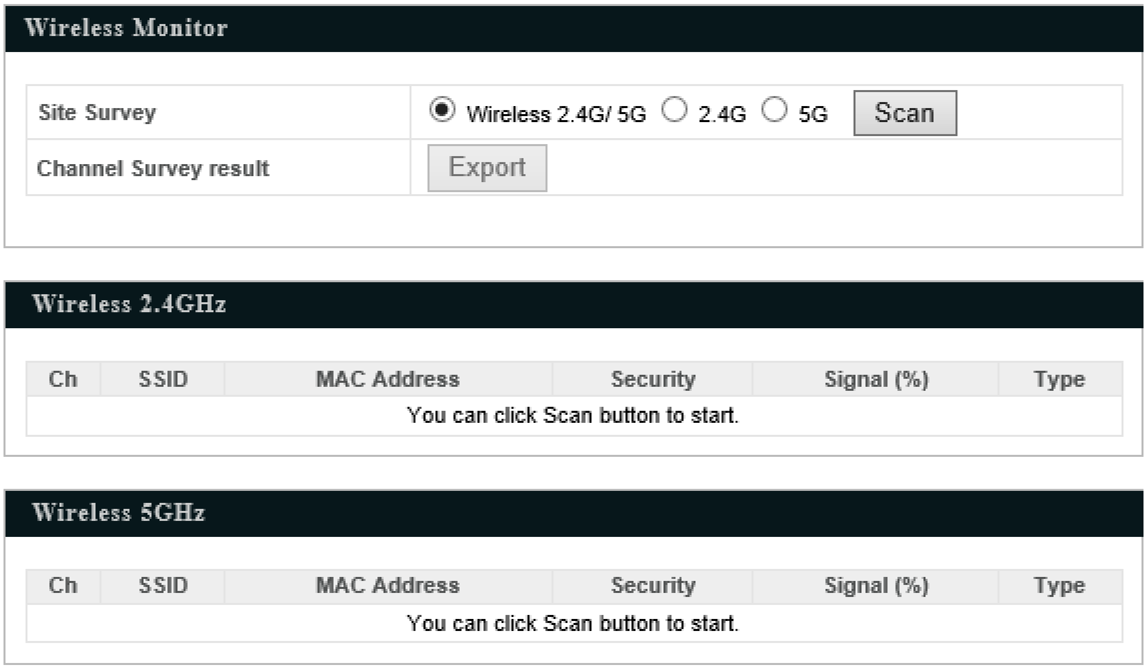
2.4GHz (5GHz) WLAN Client Table	
SSID	Displays the SSID which the client is connected to.
MAC Address	Displays the MAC address of the client.
Tx	Displays the total data packets transmitted by the specified client.
Rx	Displays the total data packets received by the specified client.
Signal (%)	Displays 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.

4-1-3. Wireless Monitor

• Wireless Monitor

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



Wireless Monitor

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

Wireless 2.4GHz

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

Wireless 5GHz

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

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

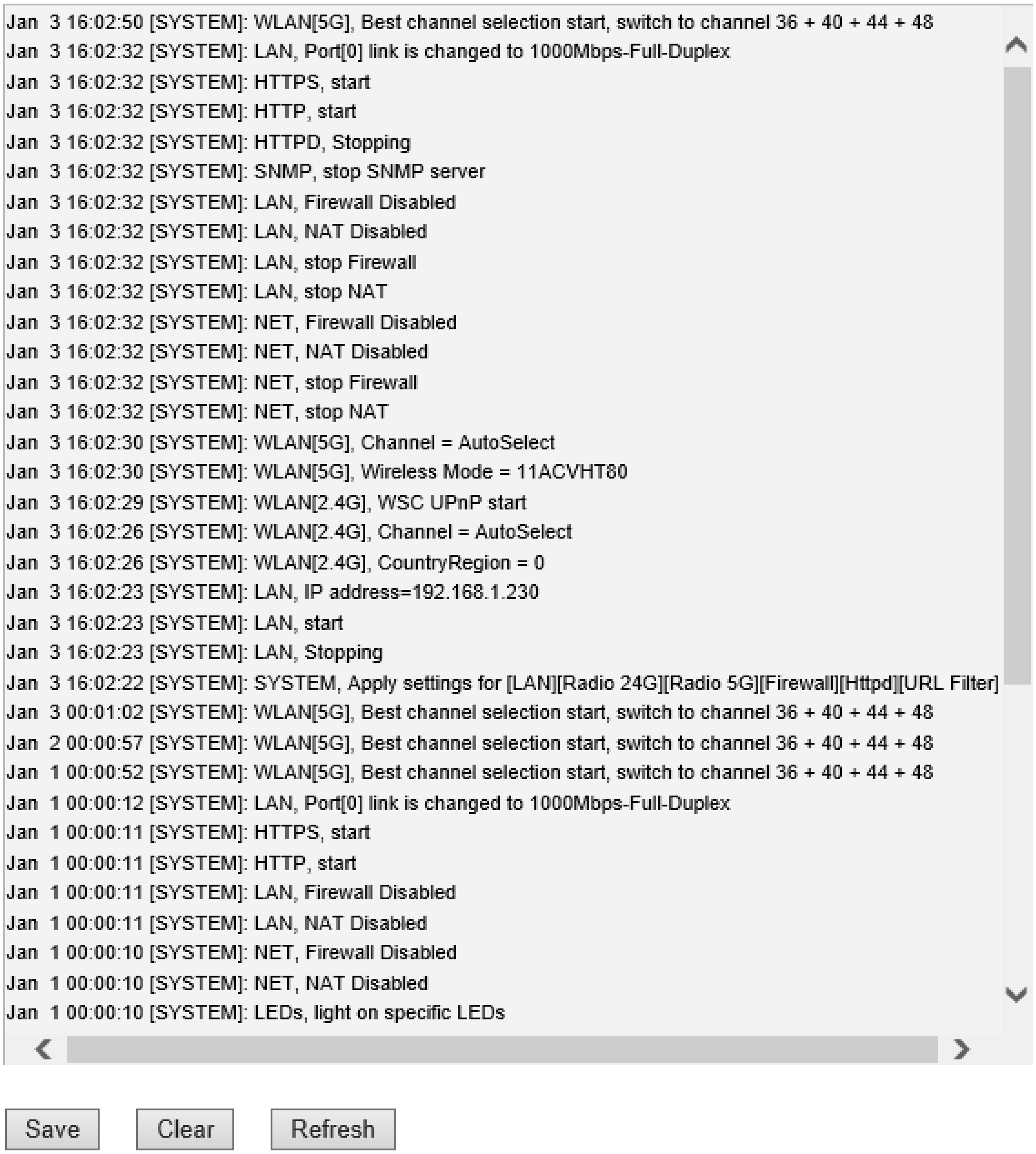
Site Survey Results	
Ch	Displays the channel number used by the specified SSID.
SSID	Displays the SSID identified by the scan.
MAC Address	Displays the MAC address of the wireless router/access point for the specified SSID.
Security	Displays the authentication/encryption type of the specified SSID.
Signal (%)	Displays the current signal strength of the SSID.

Type	Displays the 802.11 wireless networking standard(s) of the specified SSID.
Vendor	Displays the vendor of the wireless router/access point for the specified SSID.

4-1-4. Log

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

When the log is full, old entries are overwritten.



```
Jan  3 16:02:50 [SYSTEM]: WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48
Jan  3 16:02:32 [SYSTEM]: LAN, Port[0] link is changed to 1000Mbps-Full-Duplex
Jan  3 16:02:32 [SYSTEM]: HTTPS, start
Jan  3 16:02:32 [SYSTEM]: HTTP, start
Jan  3 16:02:32 [SYSTEM]: HTTPD, Stopping
Jan  3 16:02:32 [SYSTEM]: SNMP, stop SNMP server
Jan  3 16:02:32 [SYSTEM]: LAN, Firewall Disabled
Jan  3 16:02:32 [SYSTEM]: LAN, NAT Disabled
Jan  3 16:02:32 [SYSTEM]: LAN, stop Firewall
Jan  3 16:02:32 [SYSTEM]: LAN, stop NAT
Jan  3 16:02:32 [SYSTEM]: NET, Firewall Disabled
Jan  3 16:02:32 [SYSTEM]: NET, NAT Disabled
Jan  3 16:02:32 [SYSTEM]: NET, stop Firewall
Jan  3 16:02:32 [SYSTEM]: NET, stop NAT
Jan  3 16:02:30 [SYSTEM]: WLAN[5G], Channel = AutoSelect
Jan  3 16:02:30 [SYSTEM]: WLAN[5G], Wireless Mode = 11ACVHT80
Jan  3 16:02:29 [SYSTEM]: WLAN[2.4G], WSC UPnP start
Jan  3 16:02:26 [SYSTEM]: WLAN[2.4G], Channel = AutoSelect
Jan  3 16:02:26 [SYSTEM]: WLAN[2.4G], CountryRegion = 0
Jan  3 16:02:23 [SYSTEM]: LAN, IP address=192.168.1.230
Jan  3 16:02:23 [SYSTEM]: LAN, start
Jan  3 16:02:23 [SYSTEM]: LAN, Stopping
Jan  3 16:02:22 [SYSTEM]: SYSTEM, Apply settings for [LAN][Radio 24G][Radio 5G][Firewall][Httpd][URL Filter]
Jan  3 00:01:02 [SYSTEM]: WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48
Jan  2 00:00:57 [SYSTEM]: WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48
Jan  1 00:00:52 [SYSTEM]: WLAN[5G], Best channel selection start, switch to channel 36 + 40 + 44 + 48
Jan  1 00:00:12 [SYSTEM]: LAN, Port[0] link is changed to 1000Mbps-Full-Duplex
Jan  1 00:00:11 [SYSTEM]: HTTPS, start
Jan  1 00:00:11 [SYSTEM]: HTTP, start
Jan  1 00:00:11 [SYSTEM]: LAN, Firewall Disabled
Jan  1 00:00:11 [SYSTEM]: LAN, NAT Disabled
Jan  1 00:00:10 [SYSTEM]: NET, Firewall Disabled
Jan  1 00:00:10 [SYSTEM]: NET, NAT Disabled
Jan  1 00:00:10 [SYSTEM]: LEDs, light on specific LEDs
```

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

The following information/events are recorded by the log:

- **USB**

  Mount & unmount
- **Wireless Client**

  Connected & disconnected

  Key exchange success & fail
- **Authentication**

  Authentication fail or successful.
- **Association**

  Success or fail
- **WPS**

  M1 - M8 messages

  WPS success
- **Change Settings**
- **System Boot**

  Displays current model name
- **NTP Client**
- **Wired Link**

  LAN Port link status and speed status
- **Proxy ARP**

  Proxy ARP module start & stop
- **Bridge**

  Bridge start & stop.
- **SNMP**

  SNMP server start & stop.
- **HTTP**

  HTTP start & stop.
- **HTTPS**

  HTTPS start & stop.
- **SSH**

  SSH-client server start & stop.
- **Telnet**

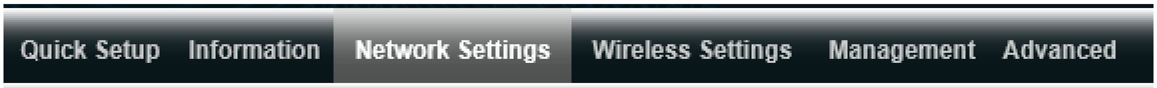
  Telnet-client server start or stop.
- **WLAN (2.4G)**

  WLAN (2.4G] channel status and country/region status
- **WLAN (5G)**

  WLAN (5G) channel status and country/region status

- **ADT**

4-2. Network Settings

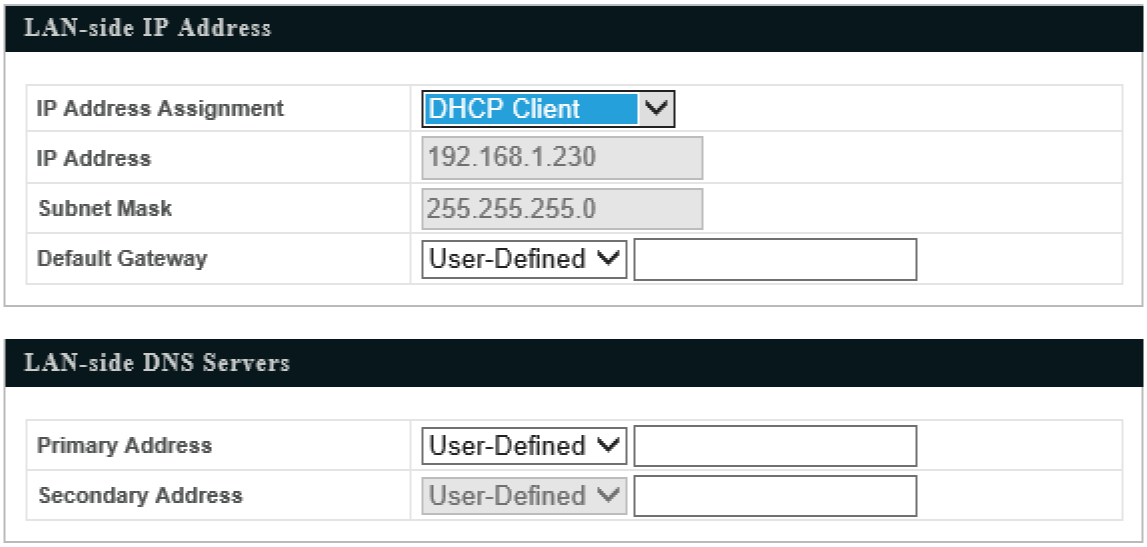


Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

4-2-1. LAN-Side IP Address

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

The access point's default IP address is 192.168.1.230.



LAN-side IP Address

IP Address Assignment	DHCP Client
IP Address	192.168.1.230
Subnet Mask	255.255.255.0
Default Gateway	User-Defined

LAN-side DNS Servers

Primary Address	User-Defined
Secondary Address	User-Defined

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.

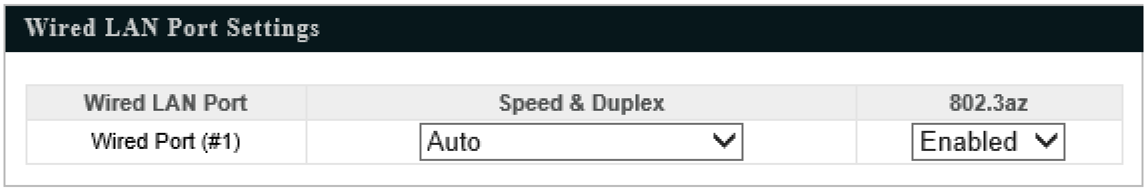
Subnet Mask	Specify a subnet mask. The default value is 255.255.255.0
Default Gateway	For DHCP users, select “From DHCP” to get default gateway from your DHCP server or “User-Defined” to enter a gateway manually. For static IP users, the default value is blank.

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”.

4-2-2. LAN Port

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



Wired LAN Port Settings

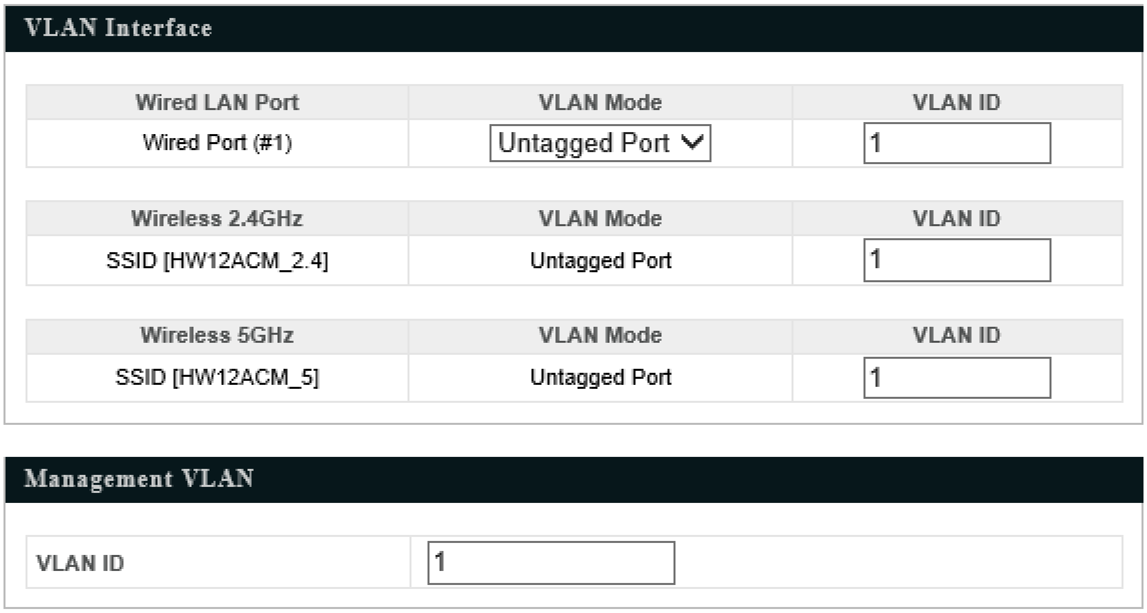
Wired LAN Port	Speed & Duplex	802.3az
Wired Port (#1)	Auto	Enabled

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

4-2-3. VLAN

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

VLAN IDs in the range 1 – 4094 are supported.



VLAN Interface

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

Wireless 2.4GHz	VLAN Mode	VLAN ID
SSID [HW12ACM_2.4]	Untagged Port	1

Wireless 5GHz	VLAN Mode	VLAN ID
SSID [HW12ACM_5]	Untagged Port	1

Management VLAN

VLAN ID	1

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

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

4-3. Wireless Settings

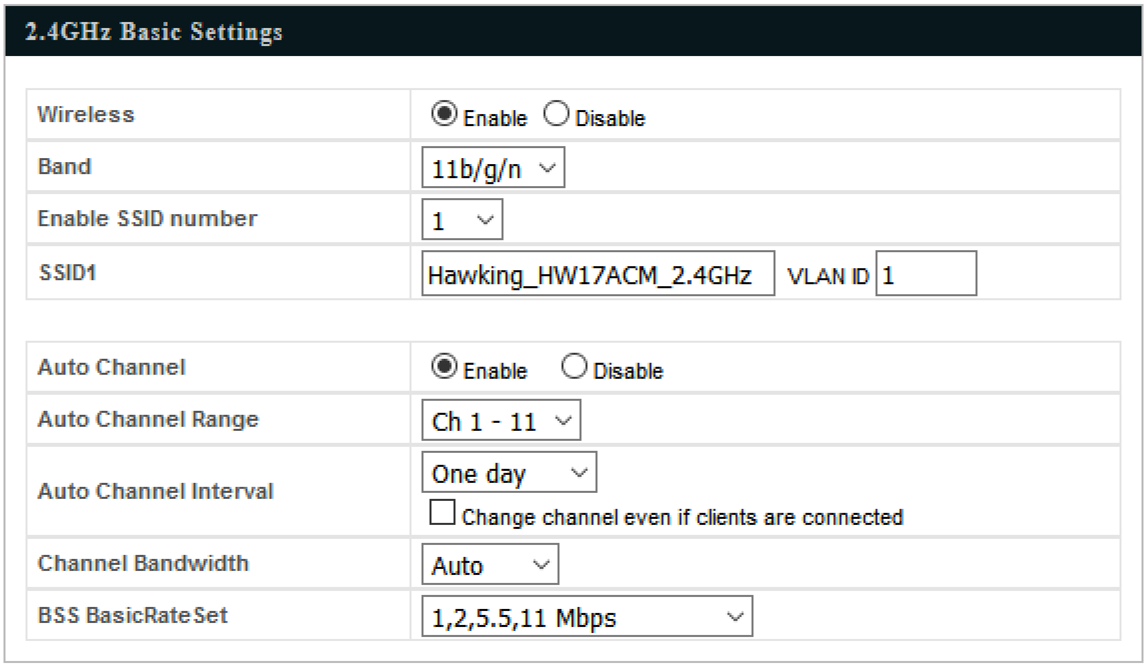
Screenshots displayed are examples. The information shown on your screen will vary depending on your configuration.

4-3-1. 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.

4-3-1-1. Basic

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



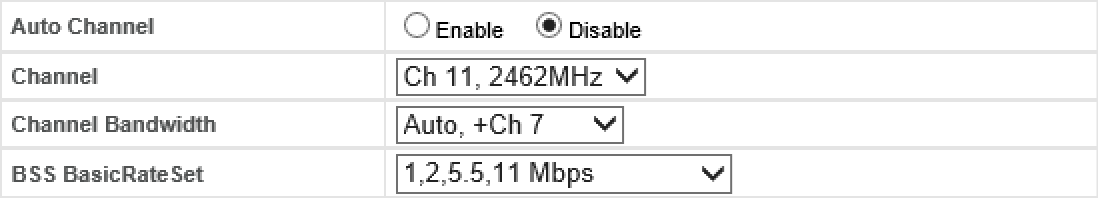
2.4GHz Basic Settings

Wireless	● Enable ○ Disable
Band	11b/g/n
Enable SSID number	1
SSID1	Hawking_HW17ACM_2.4GHz 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 2.4GHz wireless radio. When disabled, no 2.4GHz SSIDs will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11b, 802.11g & 802.11n can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 2.4GHz frequency from the drop down menu. A maximum of 16 can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.
VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point’s 2.4GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the “Change channel even if clients are connected” box according to your preference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (higher performance but potentially higher interference) or Auto (automatically select based on interference level).
BSS BasicRateSet	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:



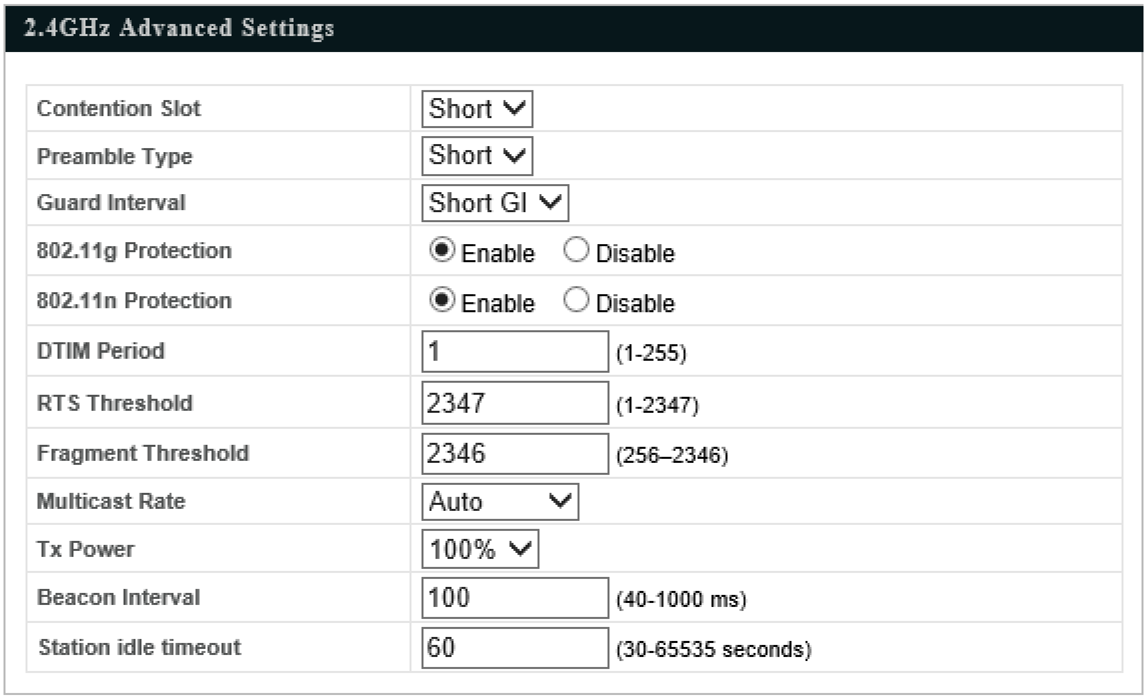
Auto Channel	○ Enable ● Disable
Channel	Ch 11, 2462MHz
Channel Bandwidth	Auto, +Ch 7
BSS BasicRateSet	1,2,5.5,11 Mbps

Channel	Select a wireless channel from 1 – 11.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), 40MHz (higher performance but potentially higher interference) or Auto (automatically select based on interference level).
BSS BasicRate Set	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

4-3-1-2. Advanced

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

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



2.4GHz Advanced Settings

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

Contention Slot	Select "Short" or "Long" – this value is used for contention windows in WMM (see **4-3-6. 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.

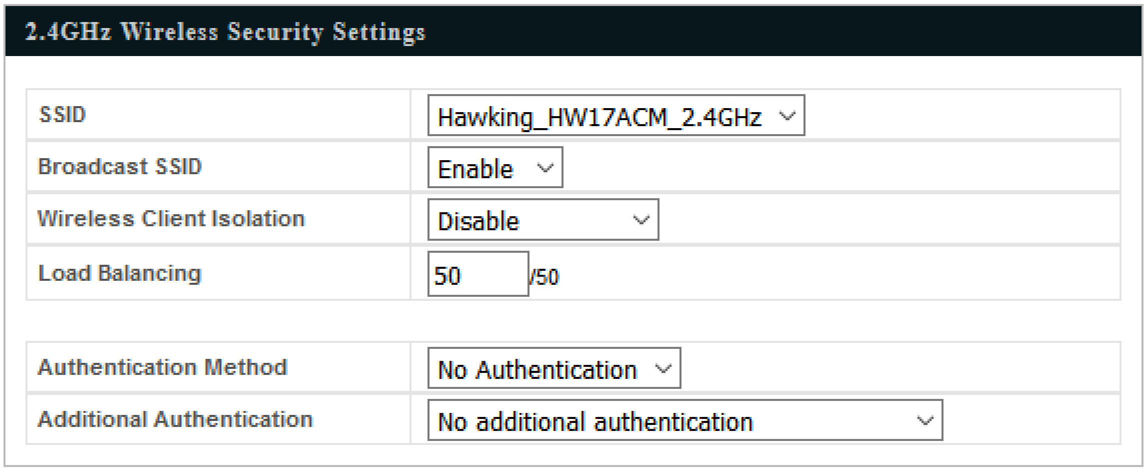
4-3-1-3. Security

• 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	Hawking_HW17ACM_2.4GHz
Broadcast SSID	Enable
Wireless Client Isolation	Disable
Load Balancing	50 /50
Authentication Method	No Authentication
Additional Authentication	No additional authentication

SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.
Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method.
Additional Authentication	Select an additional authentication method from the drop down menu and refer to the information below (**4-3-1-3-6.**) appropriate for your method.

4-3-1-3-1. No Authentication

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

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

4-3-1-3-2. WEP

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

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

4-3-1-3-3. IEEE802.1x/EAP

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

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

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

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

4-3-1-3-5. WPA-EAP

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

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

4-3-1-3-6. Additional Authentication

Additional wireless authentication methods can also be used:

MAC Address Filter

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

See** *4-3-5.MAC Filter* **to configure MAC filtering.

MAC Filter & MAC-RADIUS Authentication

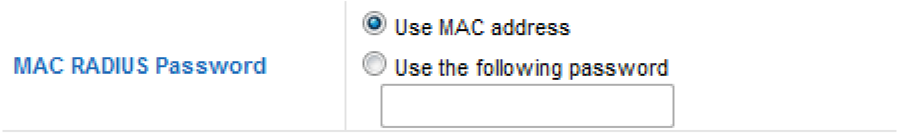
Restrict wireless clients access using both of the above MAC filtering & RADIUS authentication methods.

MAC-RADIUS Authentication

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

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

WPS must be disabled to use MAC-RADIUS authentication. See** *4-3-3.* **for WPS settings.



MAC RADIUS Password

● Use MAC address

○ Use the following password

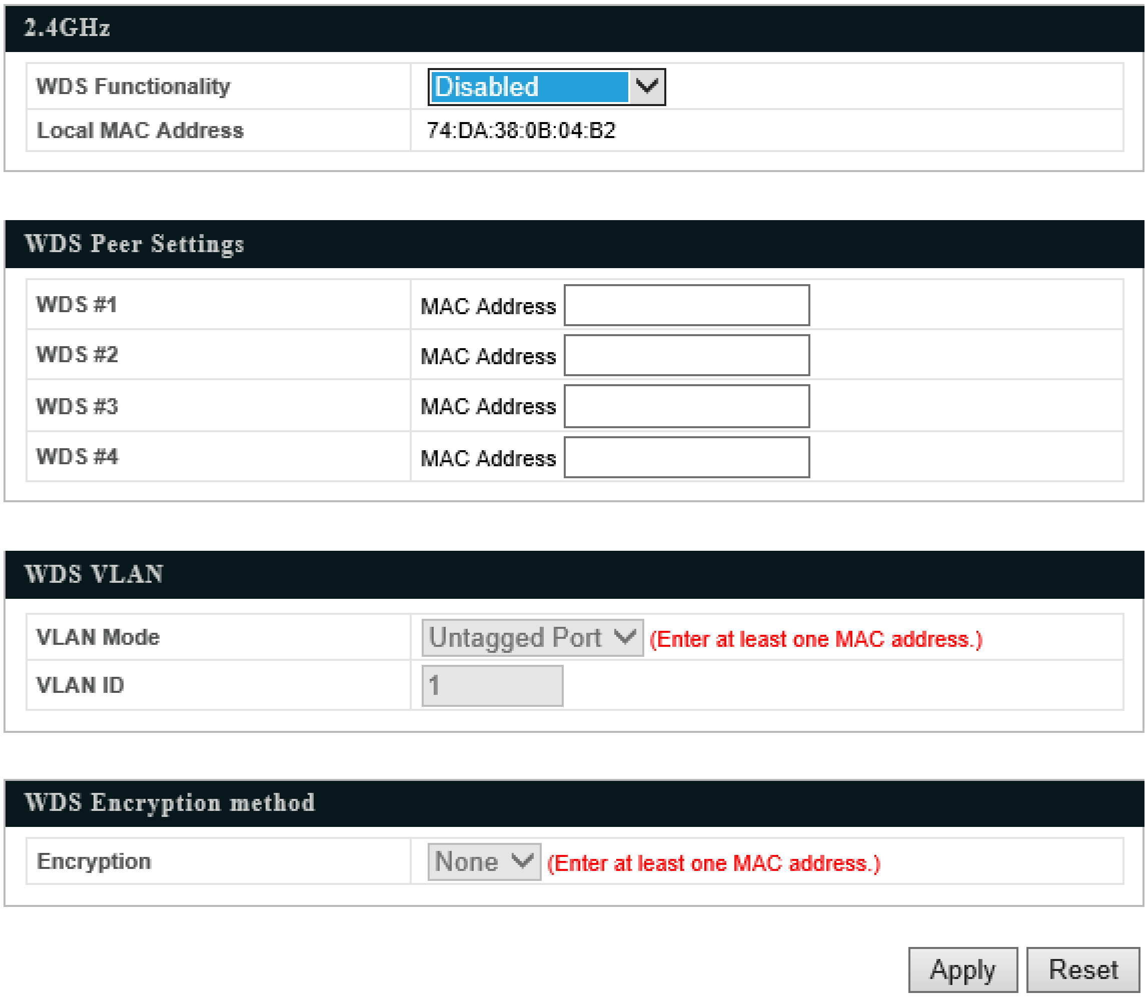
MAC RADIUS Password	Select whether to use MAC address or password authentication via RADIUS server. If you select "Use the following password", enter the password in the field below. The password should match the "Shared Secret" used in **IV-3-4. RADIUS**.

4-3-1-4. WDS

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

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

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



2.4GHz

WDS Functionality	Disabled
Local MAC Address	74:DA:38:0B:04:B2

WDS Peer Settings

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

WDS VLAN

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

WDS Encryption method

Encryption	None (Enter at least one MAC address.)

2.4GHz	
WDS Functionality	Select “WDS with AP” to use WDS with access point or “Dedicated WDS” to use WDS and also block communication with regular wireless clients. When WDS is used, each access point should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your access point.

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

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

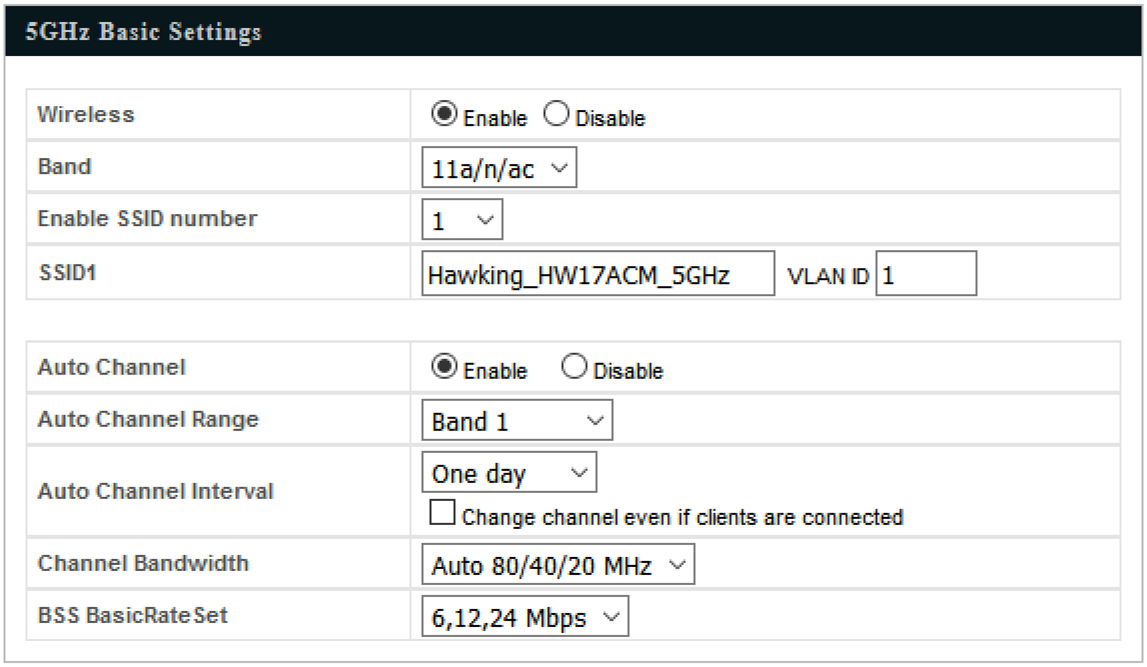
WDS Encryption method	
Encryption	Select whether to use “None” or “AES” encryption and enter a pre-shared key for AES consisting of 8-63 alphanumeric characters.

4-3-2. 5GHz 11ac 11an

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

4-3-2-1. Basic

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



5GHz Basic Settings

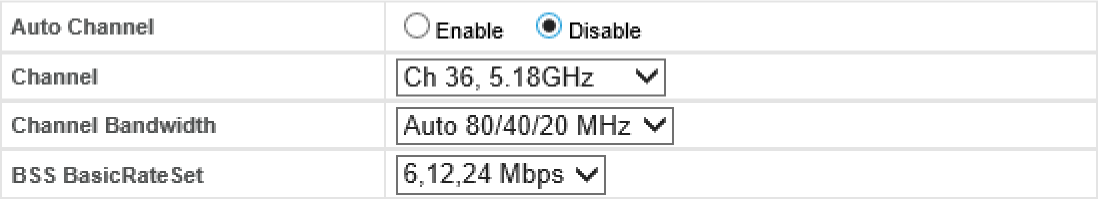
Wireless	● Enable ○ Disable
Band	11a/n/ac
Enable SSID number	1
SSID1	Hawking_HW17ACM_5GHz VLAN ID 1

Auto Channel	● Enable ○ Disable
Auto Channel Range	Band 1
Auto Channel Interval	One day □ Change channel even if clients are connected
Channel Bandwidth	Auto 80/40/20 MHz
BSS BasicRateSet	6,12,24 Mbps

Wireless	Enable or disable the access point's 5GHz wireless radio. When disabled, no 5GHz SSIDs will be active.
Band	Select the wireless standard used for the access point. Combinations of 802.11a, 802.11n & 802.11ac can be selected.
Enable SSID Number	Select how many SSIDs to enable for the 5GHz frequency from the drop down menu. A maximum of 16 can be enabled.
SSID#	Enter the SSID name for the specified SSID (up to 16). The SSID can consist of any combination of up to 32 alphanumeric characters.

VLAN ID	Specify a VLAN ID for each SSID.
Auto Channel	Enable/disable auto channel selection. Auto channel selection will automatically set the wireless channel for the access point's 5GHz frequency based on availability and potential interference. When disabled, select a channel manually as shown in the next table.
Auto Channel Range	Select a range from which the auto channel setting (above) will choose a channel.
Auto Channel Interval	Specify a frequency for how often the auto channel setting will check/reassign the wireless channel. Check/uncheck the "Change channel even if clients are connected" box according to your preference.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (automatically select based on interference level).
BSS BasicRate 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:



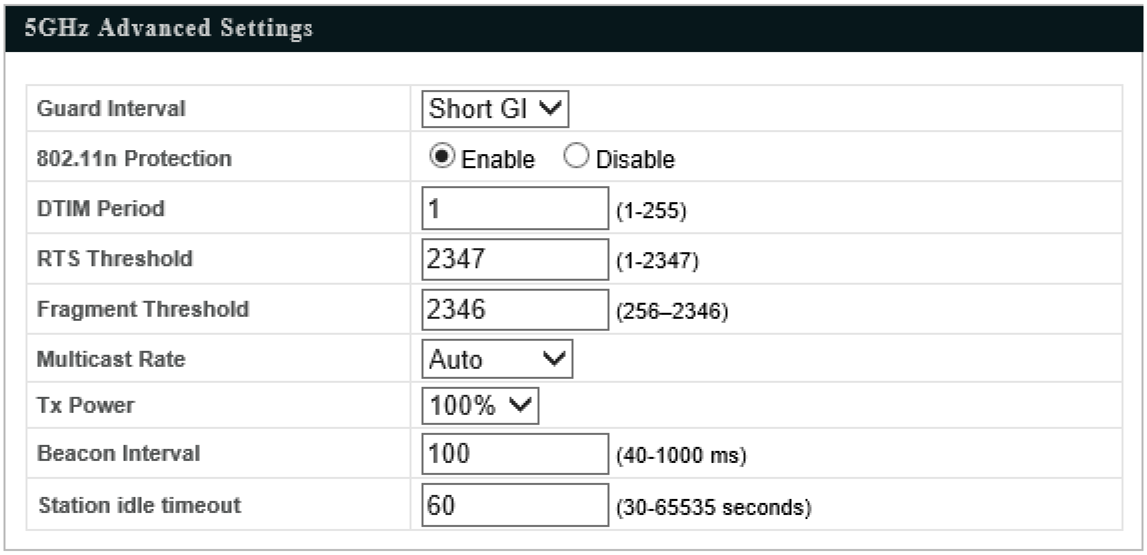
Auto Channel	○ Enable ● Disable
Channel	Ch 36, 5.18GHz
Channel Bandwidth	Auto 80/40/20 MHz
BSS BasicRate Set	6,12,24 Mbps

Channel	Select a wireless channel.
Channel Bandwidth	Set the channel bandwidth: 20MHz (lower performance but less interference), Auto 40/20MHz or Auto 80/40/20MHz (automatically select based on interference level).
BSS BasicRate Set	Set a Basic Service Set (BSS) rate: this is a series of rates to control communication frames for wireless clients.

4-3-2-2. Advanced

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

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



5GHz Advanced Settings

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

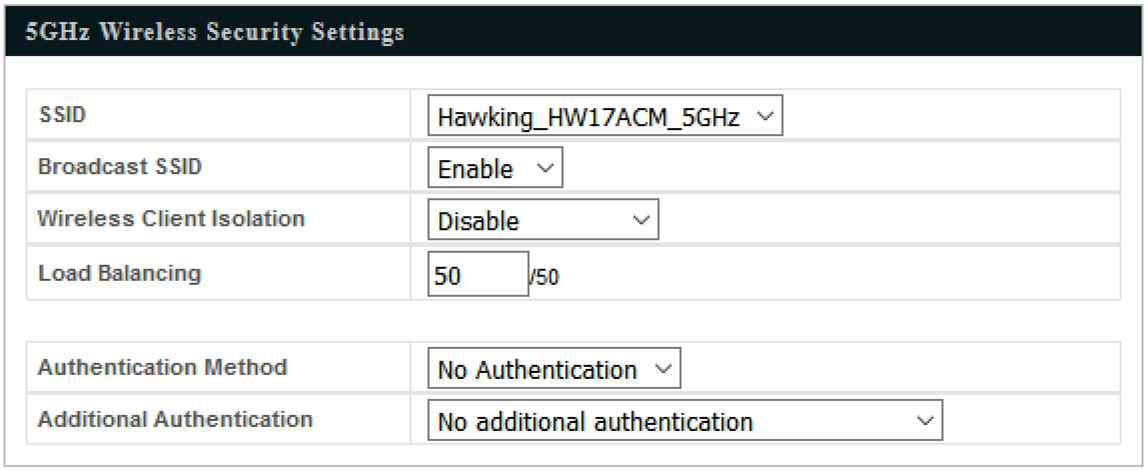
Guard Interval	Set the guard interval. A shorter interval can improve performance.
802.11n Protection	Enable/disable 802.11n protection, which increases reliability but reduces bandwidth (clients will send Request to Send (RTS) to access point, and access point will broadcast Clear to Send (CTS), before a packet is sent from client.)
DTIM Period	Set the DTIM (delivery traffic indication message) period value of the wireless radio. The default value is 1.
RTS Threshold	Set the RTS threshold of the wireless radio. The default value is 2347.
Fragment Threshold	Set the fragment threshold of the wireless radio. The default value is 2346.
Multicast Rate	Set the transfer rate for multicast packets or use the “Auto” setting.
Tx Power	Set the power output of the wireless radio. You may not require 100% output power. Setting a lower power output can enhance security since potentially malicious/unknown users in distant areas will not be able to access your signal.
Beacon Interval	Set the beacon interval of the wireless radio. The default value is 100.
Station idle timeout	Set the interval for keep alive messages from the access point to a wireless client to verify if the station is still alive/active.

4-3-2-3. Security

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

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

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



5GHz Wireless Security Settings

SSID	Hawking_HW17ACM_5GHz
Broadcast SSID	Enable
Wireless Client Isolation	Disable
Load Balancing	50 /50

Authentication Method	No Authentication
Additional Authentication	No additional authentication

SSID Selection	Select which SSID to configure security settings for.
Broadcast SSID	Enable or disable SSID broadcast. When enabled, the SSID will be visible to clients as an available Wi-Fi network. When disabled, the SSID will not be visible as an available Wi-Fi network to clients – clients must manually enter the SSID in order to connect. A hidden (disabled) SSID is typically more secure than a visible (enabled) SSID.
Wireless Client Isolation	Enable or disable wireless client isolation. Wireless client isolation prevents clients connected to the access point from communicating with each other and improves security. Typically, this function is useful for corporate environments or public hot spots and can prevent brute force attacks on clients' usernames and passwords.

Load Balancing	Load balancing limits the number of wireless clients connected to an SSID. Set a load balancing value (maximum 50).
Authentication Method	Select an authentication method from the drop down menu and refer to the information below appropriate for your method.
Additional Authentication	Select an additional authentication method from the drop down menu and refer to the information below appropriate for your method.

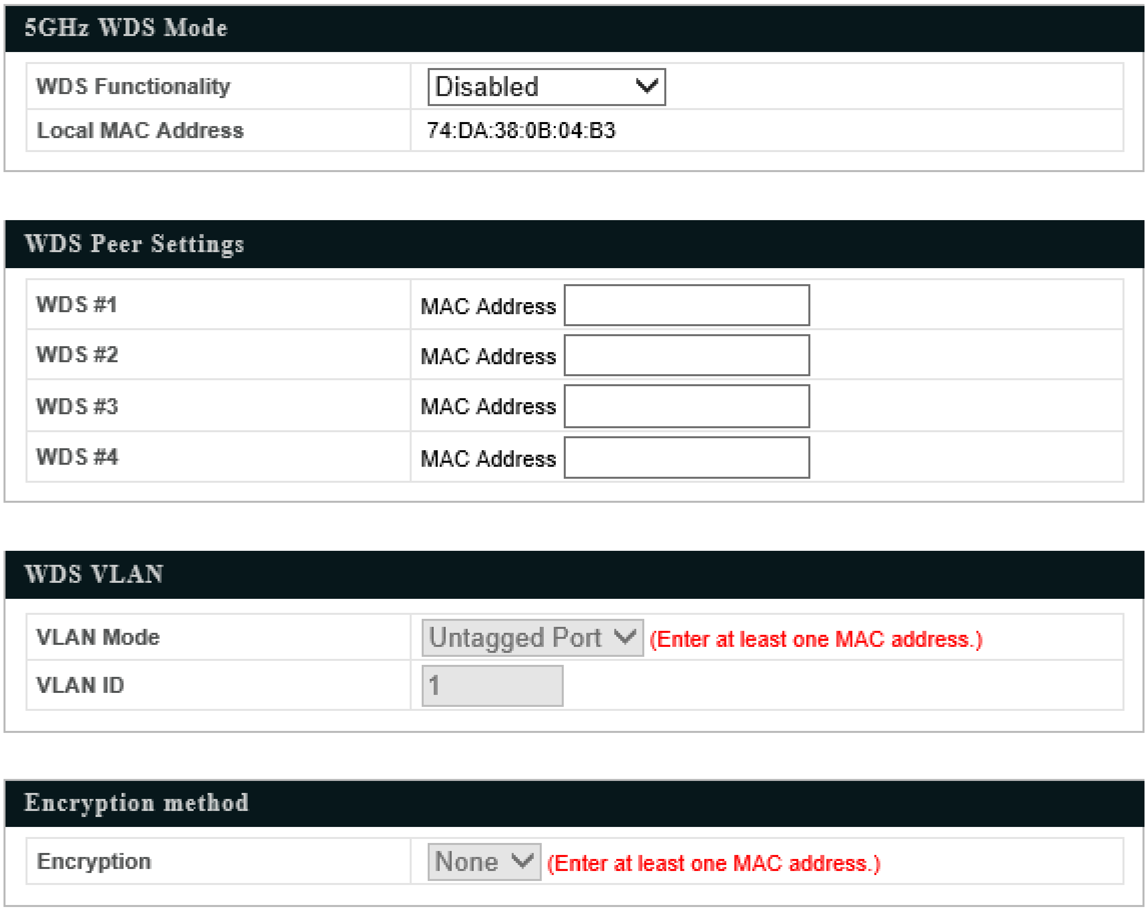
Please refer back to **4-3-1-3. Security** for more information on authentication and additional authentication types.

4-3-2-4. WDS

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

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

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



5GHz WDS Mode

WDS Functionality	Disabled
Local MAC Address	74:DA:38:0B:04:B3

WDS Peer Settings

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

WDS VLAN

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

Encryption method

Encryption	None (Enter at least one MAC address.)

5GHz WDS Mode

WDS Functionality	Select “WDS with AP” to use WDS with access point or “Dedicated WDS” to use WDS and also block communication with regular wireless clients. When WDS is used, each access point should be configured with corresponding MAC addresses, wireless channel and wireless encryption method.
Local MAC Address	Displays the MAC address of your access point.

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

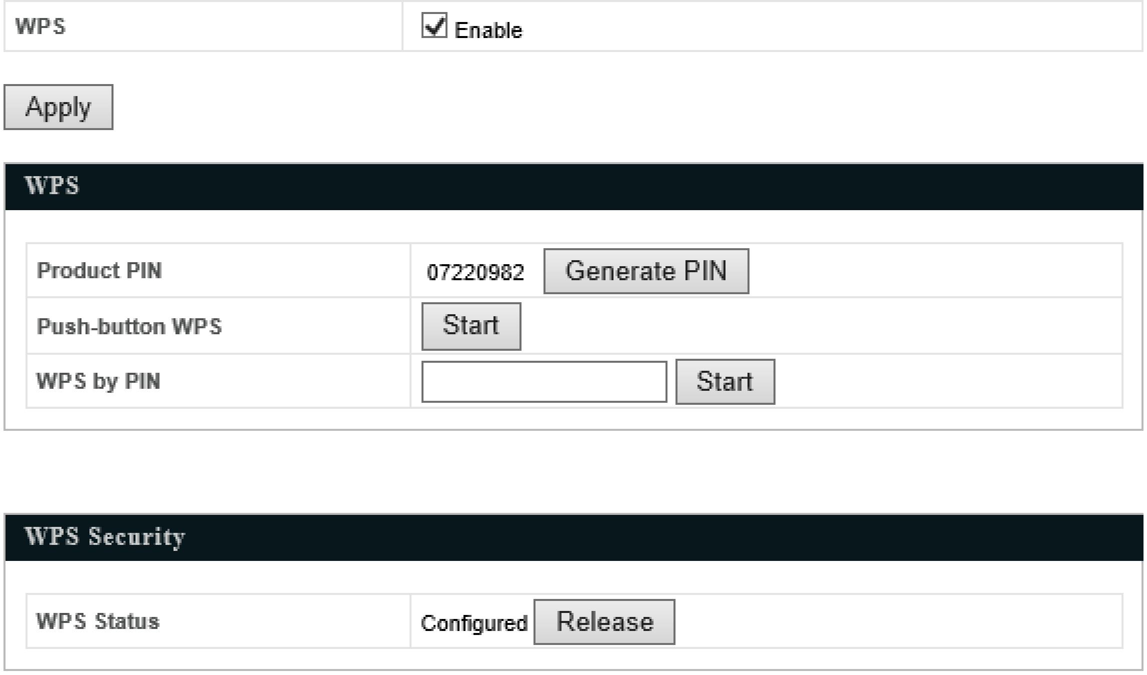
WDS VLAN	
VLAN Mode	Specify the WDS VLAN mode to “Untagged Port” or “Tagged Port”.
VLAN ID	Specify the WDS VLAN ID when “Untagged Port” is selected above.

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

4-3-3. WPS

Wi-Fi Protected Setup is a simple way to establish connections between WPS compatible devices. WPS can be activated on compatible devices by pushing a WPS button on the device or from within the device's firmware/configuration interface (known as PBC or "Push Button Configuration"). When WPS is activated in the correct manner and at the correct time for two compatible devices, they will automatically connect. "PIN code WPS" is a variation of PBC which includes the additional use of a PIN code between the two devices for verification.

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



WPS	☑ Enable

WPS

Product PIN	07220982 Generate PIN
Push-button WPS	Start
WPS by PIN	▭ Start

WPS Security

WPS Status	Configured Release

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

Product PIN	Displays the WPS PIN code of the device, used for PIN code WPS. You will be required to enter this PIN code into another WPS device for PIN code WPS. Click "Generate PIN" to generate a new WPS PIN code.
Push-Button WPS	Click "Start" to activate WPS on the access point for approximately 2 minutes. This has the same effect as physically pushing the access point's WPS button.

WPS by PIN	Enter the PIN code of another WPS device and click “Start” to attempt to establish a WPS connection for approximately 2 minutes.

WPS Status	WPS security status is displayed here. Click “Release” to clear the existing status.

4-3-4. RADIUS

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

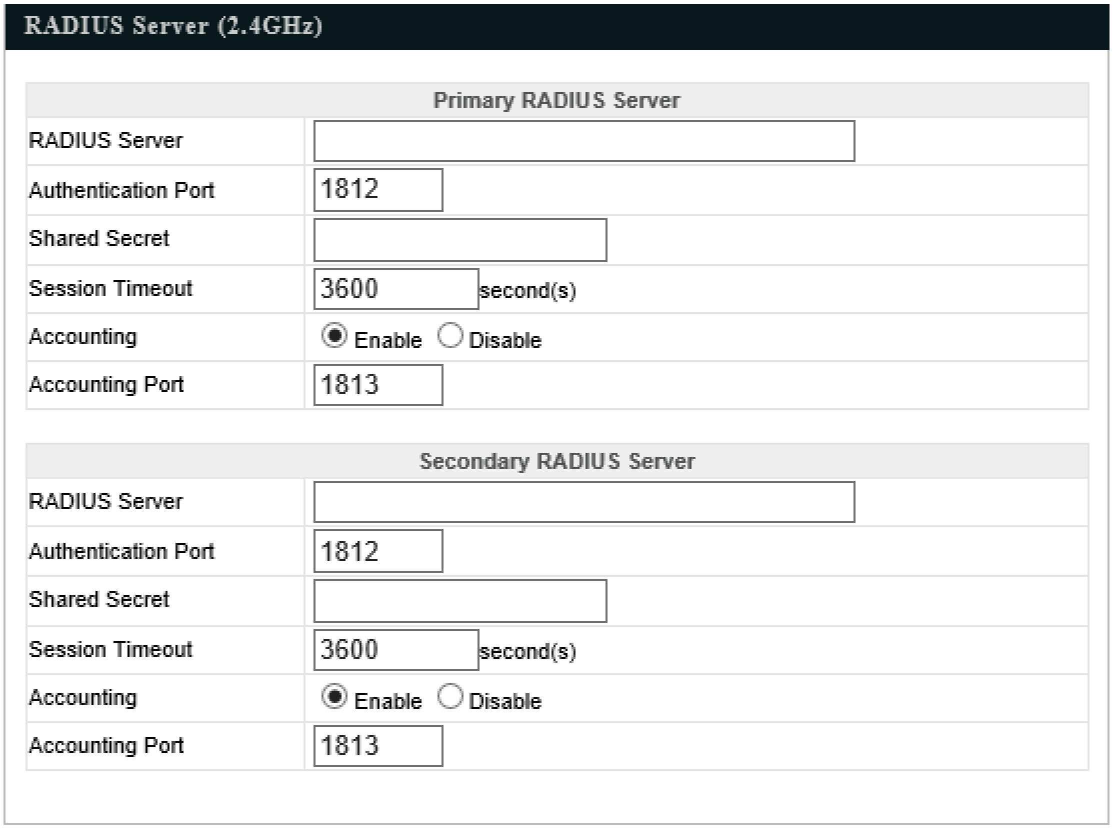
A RADIUS server provides user-based authentication to improve security and offer wireless client control – users can be authenticated before gaining access to a network.

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

To use RADIUS servers, go to *“Wireless Settings” → “Security”* ***and select*** *“MAC RADIUS Authentication” → “Additional Authentication”* ***and select*** *“MAC RADIUS Authentication”* ***(see 4****-3-1-3.* ***& 4****-3-2-3****).***

RADIUS Settings

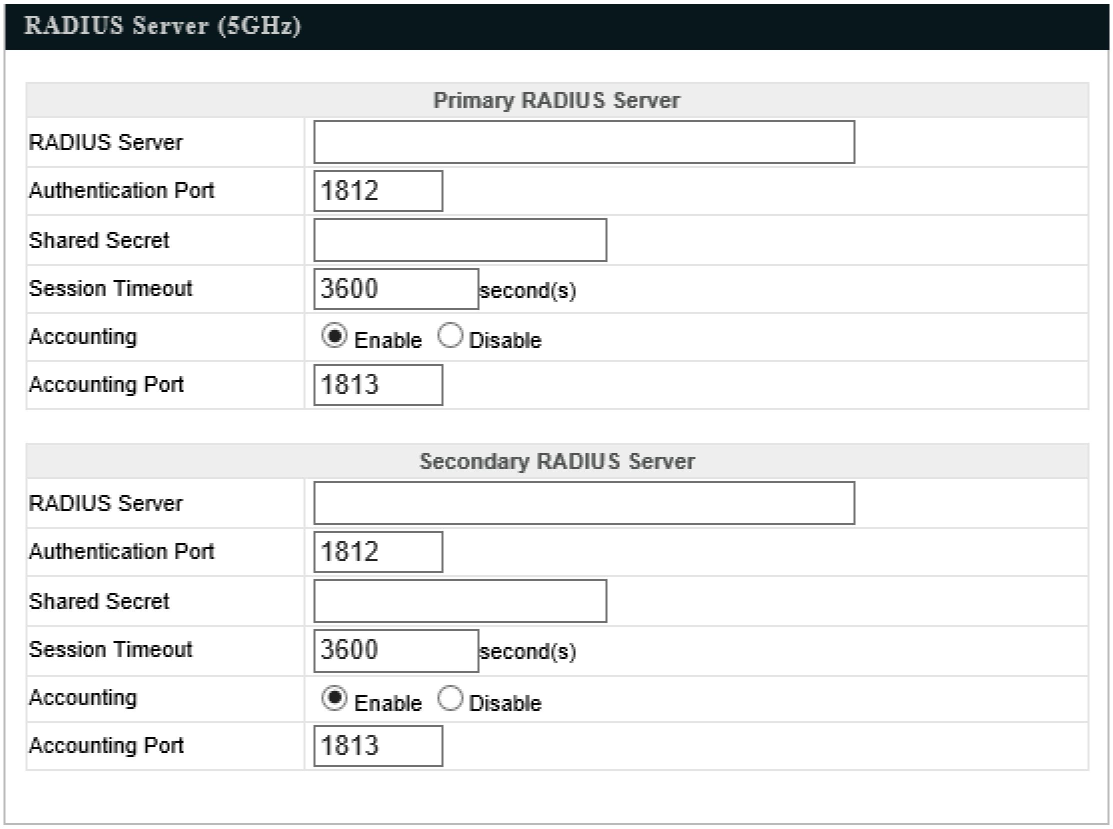
Configure the RADIUS server settings for 2.4GHz & 5GHz. Each frequency can use an internal or external RADIUS server.



RADIUS Server (2.4GHz)

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

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



RADIUS Server (5GHz)

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

Secondary RADIUS Server	
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 **4-3-1-3-6** or **4-3-2-3**.
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.

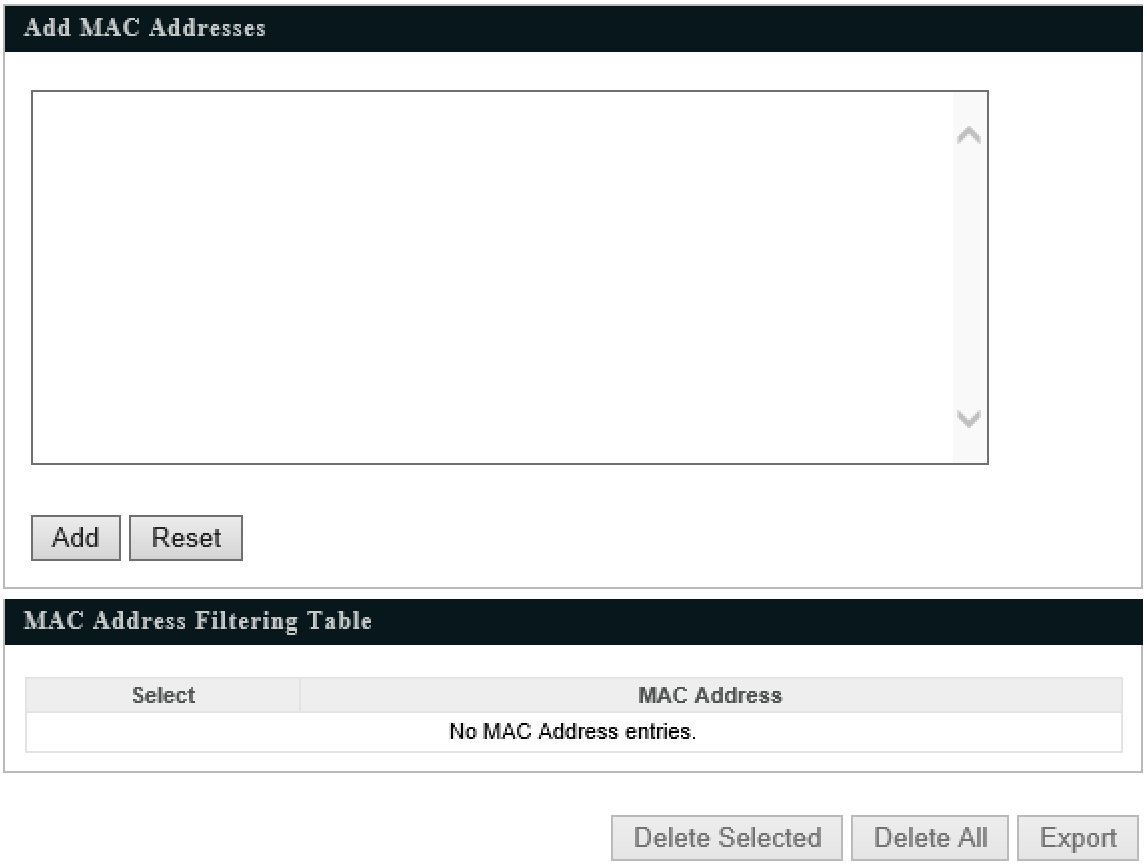
4-3-5. MAC Filter

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

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

To enable MAC filtering, go to *"Wireless Settings"* **→** *"2.4GHz 11bgn/5GHz 11ac 11an"* **→** *"Security"* **→** *"Additional Authentication"* ***and select*** *"MAC Filter"* ***(see*** *4-3-1-3.* ***&*** *4-3-2-3****).***

The MAC address filtering table is displayed below:



Add MAC Addresses

MAC Address Filtering Table

Select	MAC Address
No MAC Address entries.	

Add MAC Address	Enter a MAC address of computer or network device manually e.g. 'aa-bb-cc-dd-ee-ff' or enter multiple MAC addresses

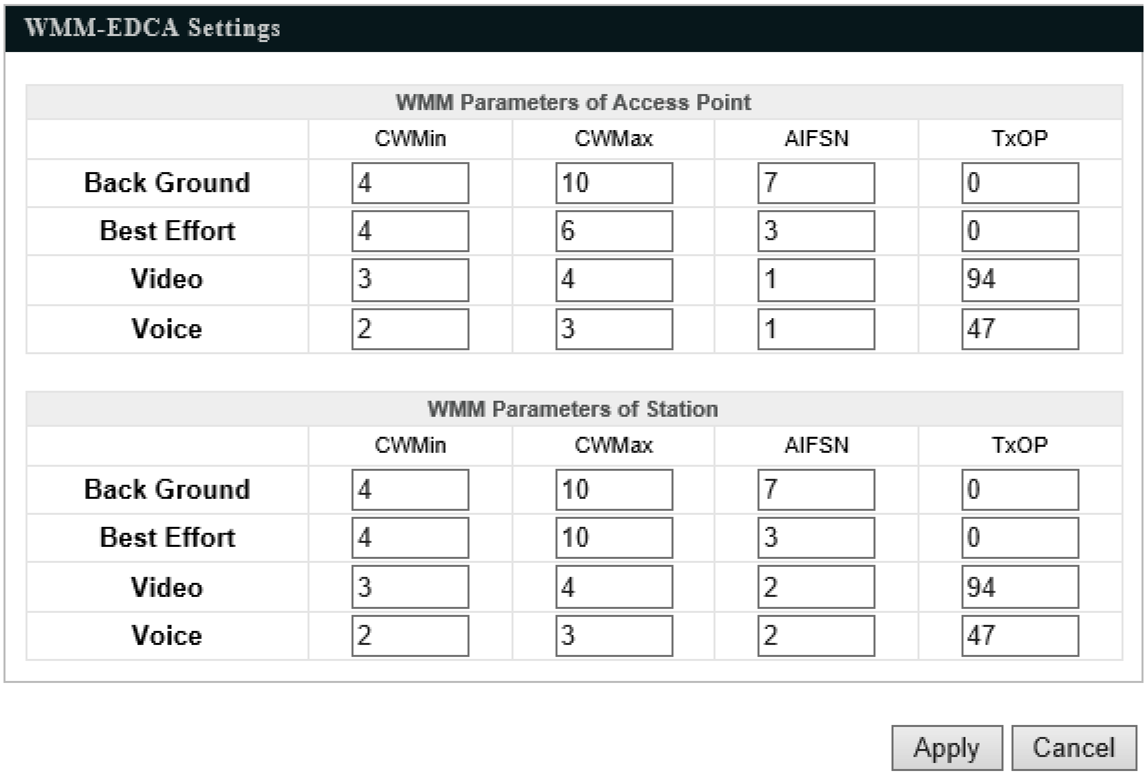
	separated with commas, e.g. ‘aa-bb-cc-dd-ee-ff,aa-bb-cc-dd-ee-gg’
Add	Click “Add” to add the MAC address to the MAC address filtering table.
Reset	Clear all fields.

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

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

4-3-6. WMM

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



WMM-EDCA Settings

WMM Parameters of Access Point

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

WMM Parameters of Station

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

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

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

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

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

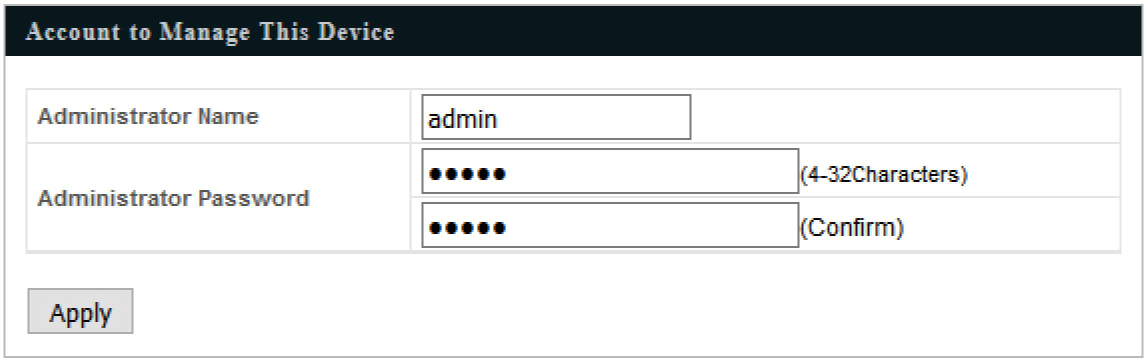
4-4. Management

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

4-4-1. Admin

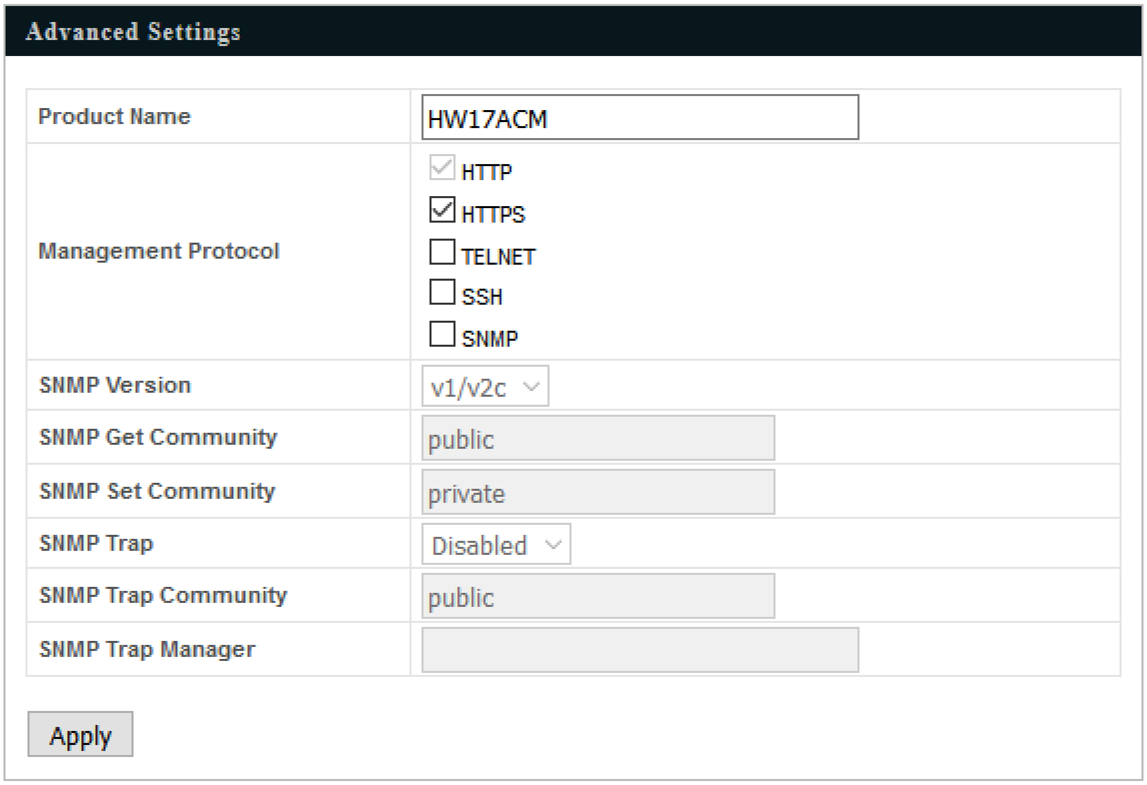
You can change the password used to login to the browser-based configuration interface here. It is advised to do so for security purposes.

If you change the administrator password, please make a note of the new password. In the event that you forget this password and are unable to login to the browser based configuration interface, see Chapter 1-5 for how to reset the access point.



Account to Manage This Device

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



Advanced Settings

Product Name	HW17ACM
Management Protocol	☑ HTTP ☑ HTTPS □ TELNET □ SSH □ SNMP
SNMP Version	v1/v2c
SNMP Get Community	public
SNMP Set Community	private
SNMP Trap	Disabled
SNMP Trap Community	public
SNMP Trap Manager	

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

Advanced Settings	
Product Name	Edit the product name according to your preference consisting of 1-32 alphanumeric characters. This name is used for reference purposes.

Management Protocol	Check/uncheck the boxes to enable/disable specified management interfaces (see below). When SNMP is enabled, complete the SNMP fields below.
SNMP Version	Select SNMP version appropriate for your SNMP manager.
SNMP Get Community	Enter an SNMP Get Community name for verification with the SNMP manager for SNMP-GET requests.
SNMP Set Community	Enter an SNMP Set Community name for verification with the SNMP manager for SNMP-SET requests.
SNMP Trap	Enable or disable SNMP Trap to notify SNMP manager of network errors.
SNMP Trap Community	Enter an SNMP Trap Community name for verification with the SNMP manager for SNMP-TRAP requests.
SNMP Trap Manager	Specify the IP address or sever name (2-128 alphanumeric characters) of the SNMP manager.

HTTP

Internet browser HTTP protocol management interface

HTTPS

Internet browser HTTPS protocol management interface

TELNET

Client terminal with telnet protocol management interface

SSH

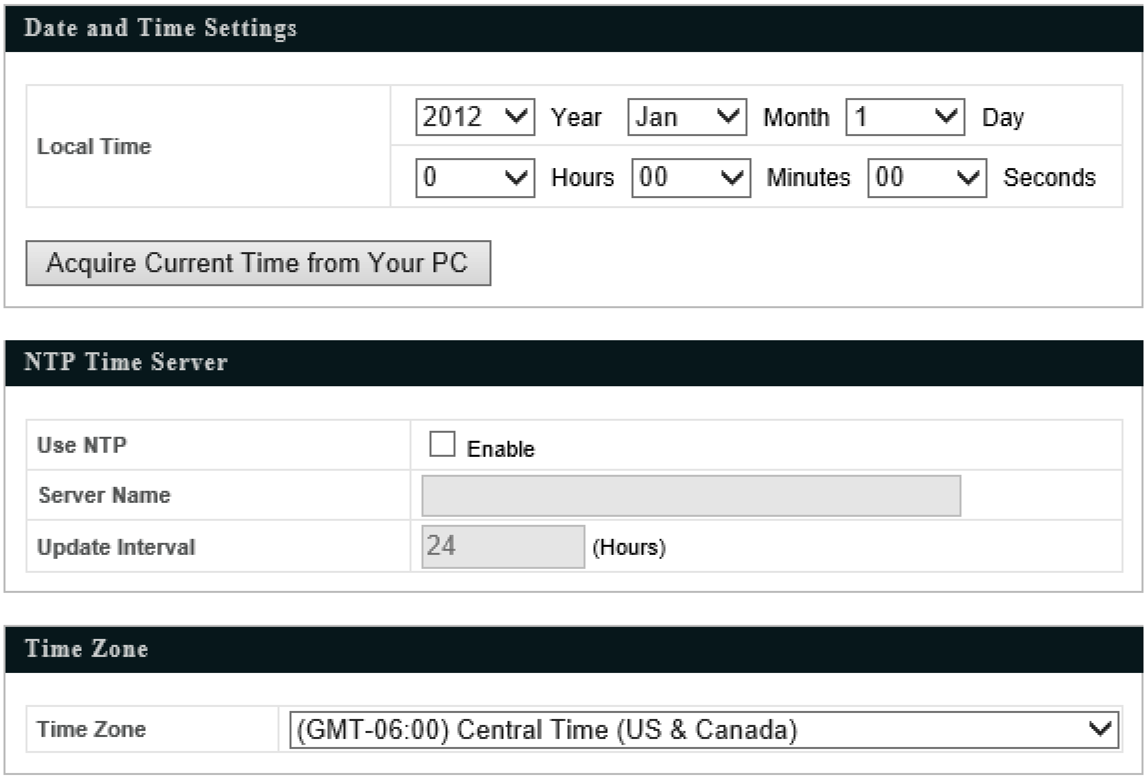
Client terminal with SSH protocol version 1 or 2 management interface

SNMP

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

4-4-2. Date and Time

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



Date and Time Settings

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

Acquire Current Time from Your PC

NTP Time Server

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

Time Zone

Time Zone	(GMT-06:00) Central Time (US & Canada)

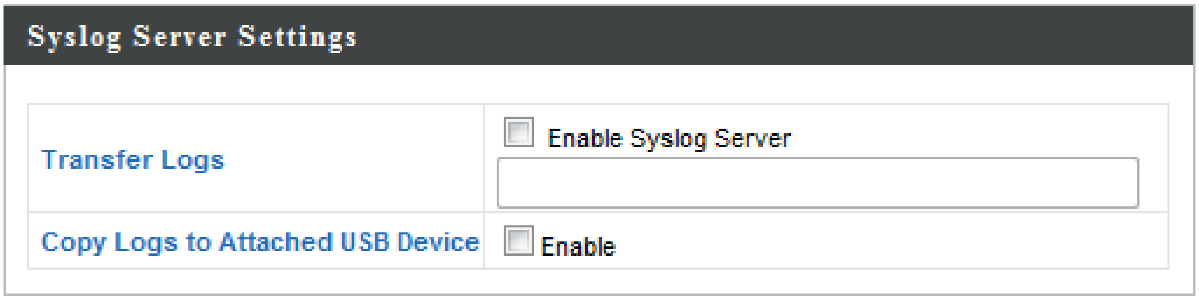
Date and Time Settings	
Local Time	Set the access point's date and time manually using the drop down menus.
Acquire Current Time from your PC	Click "Acquire Current Time from Your PC" to enter the required values automatically according to your computer's current time and date.

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

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

4-4-3. Syslog Server

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



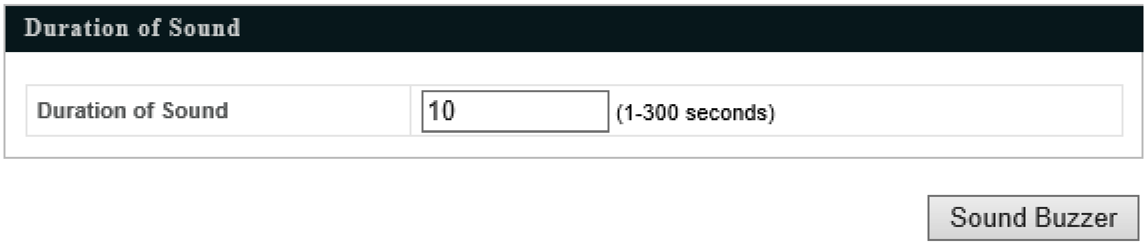
Syslog Server Settings

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

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

4-4-4. I’m Here

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



Duration of Sound

Duration of Sound: 10 (1-300 seconds)

The buzzer is loud!

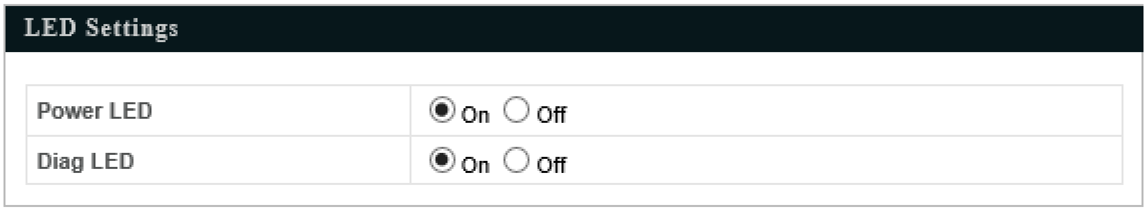
Duration of Sound	Set the duration for which the buzzer will sound when the “Sound Buzzer” button is clicked.
Sound Buzzer	Activate the buzzer sound for the above specified duration of time.

4-5. Advanced

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

4-5-1. LED Settings

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



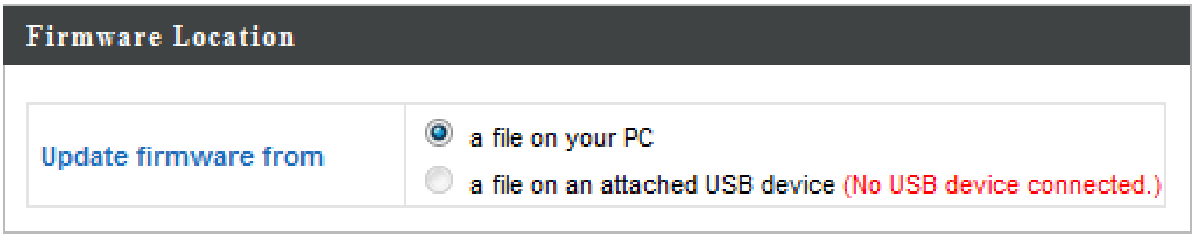
LED Settings

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

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

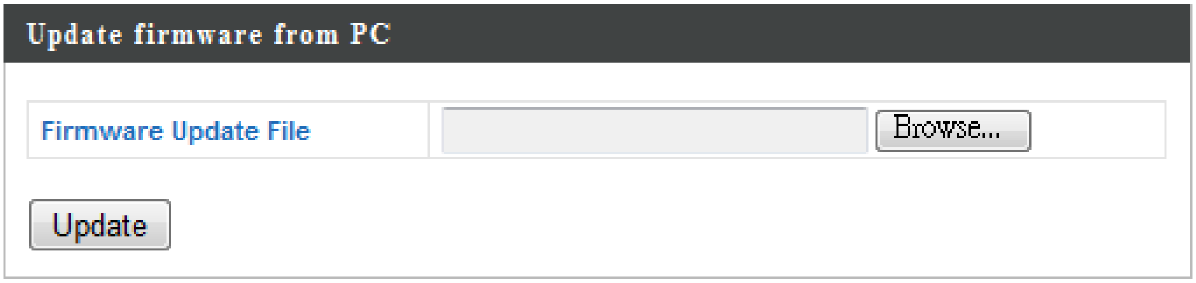
4-5-2. Update Firmware

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 website.



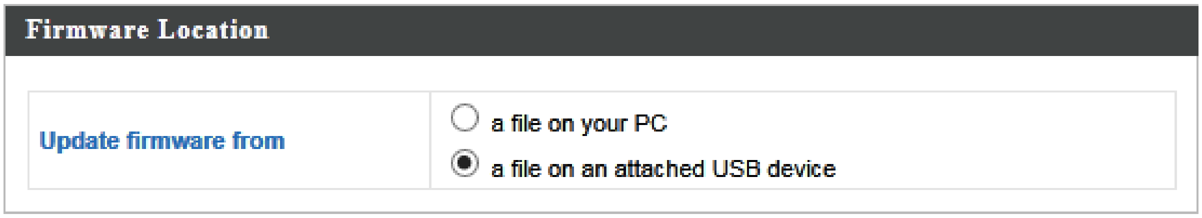
Firmware Location

Update firmware from: ● a file on your PC ○ a file on an attached USB device (No USB device connected.)



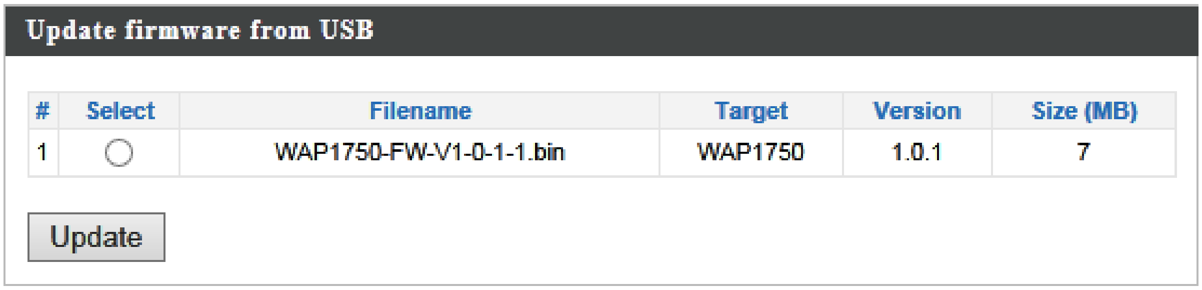
Update firmware from PC

Firmware Update File



Firmware Location

Update firmware from: ○ a file on your PC ● a file on an attached USB device



Update firmware from USB

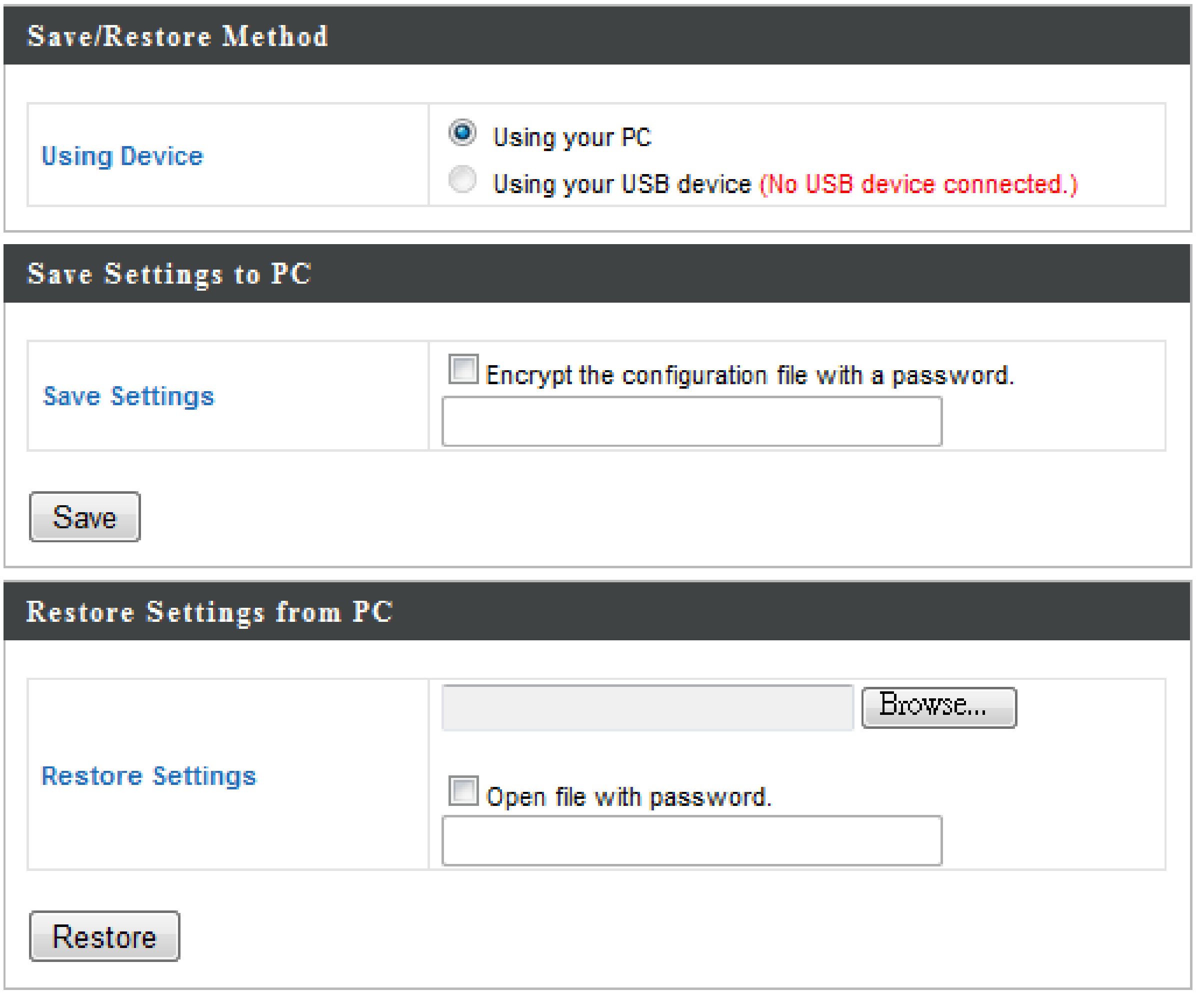
#	Select	Filename	Target	Version	Size (MB)
1	○	WAP1750-FW-V1-0-1-1.bin	WAP1750	1.0.1	7

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 or from an attached USB device. (You must transfer a firmware file to the USB device first).
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.

4-5-3. Save/Restore Settings

• 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

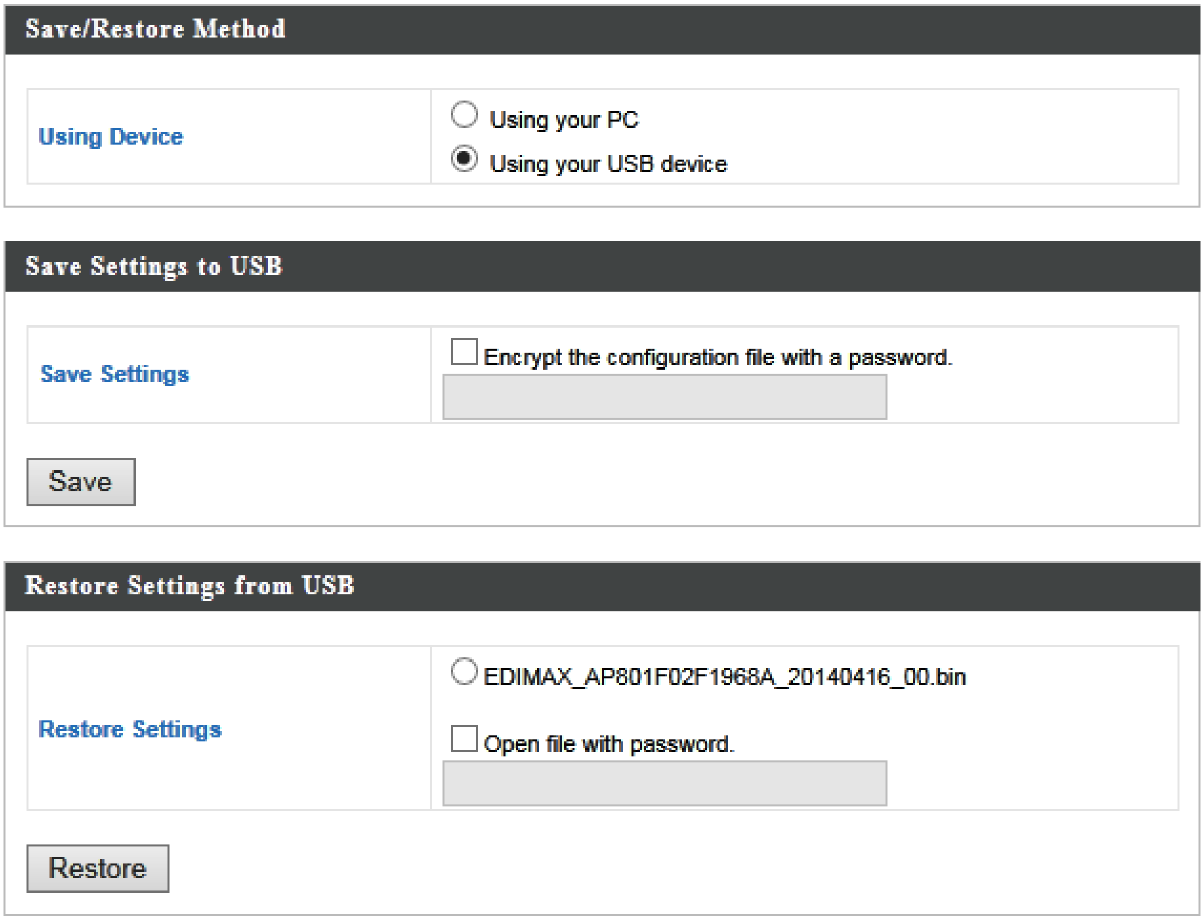
Using Device	● Using your PC ○ Using your USB device (No USB device connected.)

Save Settings to PC

Save Settings	□ Encrypt the configuration file with a password.

Restore Settings from PC

Restore Settings	□ Open file with password.



Save/Restore Method

Using Device: ○ Using your PC ● Using your USB device

Save Settings to USB

Save Settings: □ Encrypt the configuration file with a password.

Restore Settings from USB

Restore Settings: ○ EDIMAX_AP801F02F1968A_20140416_00.bin

□ Open file with password.

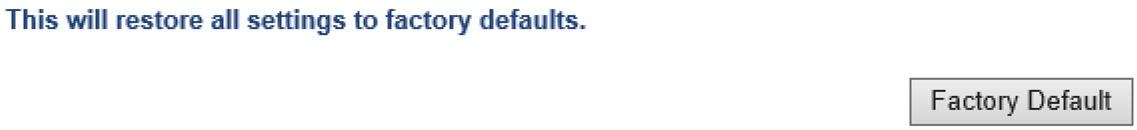
Save / Restore Settings	
Using Device	Select "Using your PC" to save the access point's settings to your local computer or to an attached USB device.

Save Settings to PC/USB	
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/USB	
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.

4-5-4. Factory Default

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

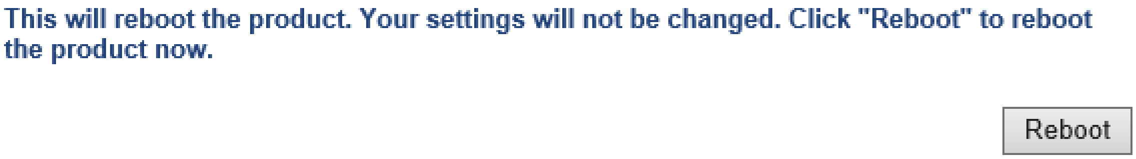

This will restore all settings to factory defaults.

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

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

4-5-5. 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 **4-5-4**). 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.

5-1. Configuring your IP address

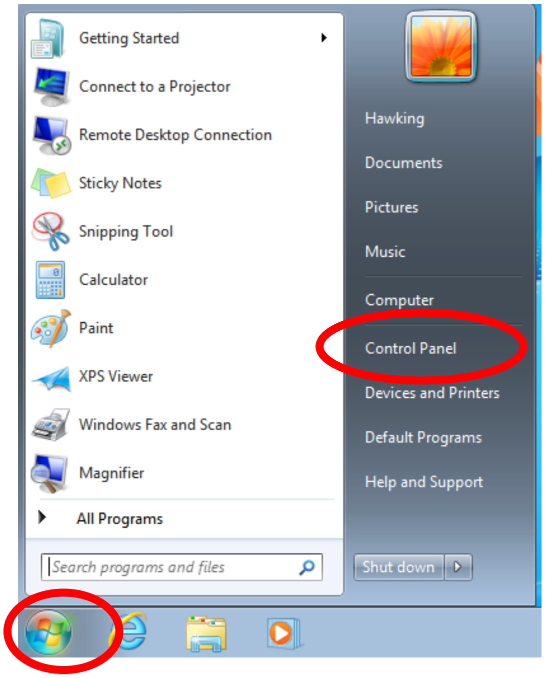
The access point uses the default IP address **192.168.1.230**. In order to access the browser based configuration interface, you need to modify the IP address of your computer to be in the same IP address subnet e.g. **192.168.1.x (x = 1-200).**

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

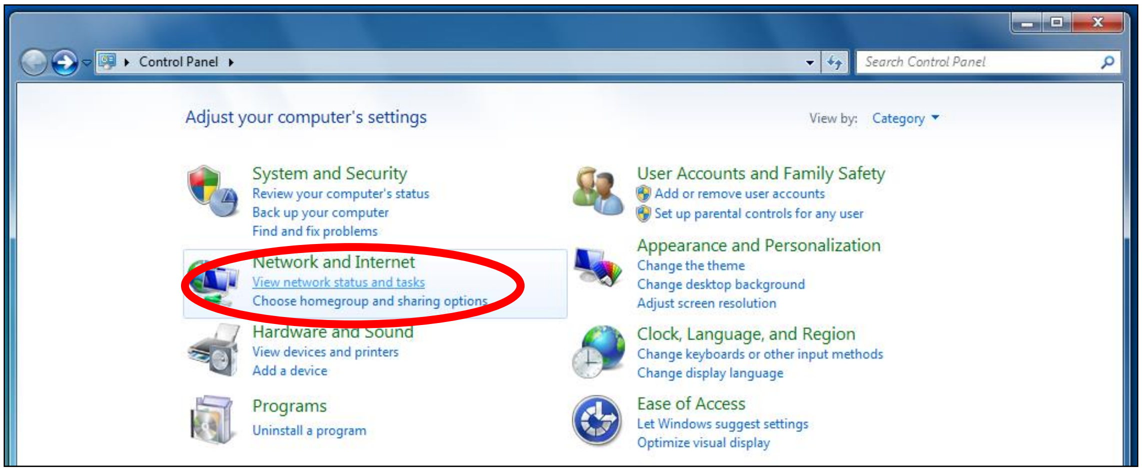
In the following examples, we use the IP address **192.168.1.10** though you can use any IP address in the range **192.168.1.x (x = 1 – 100).**

5-1-1. Windows 7

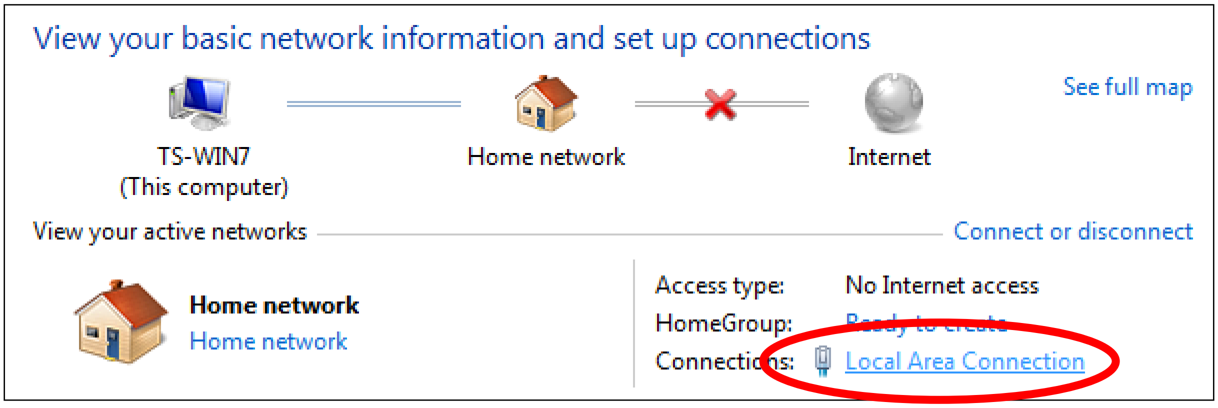
1. Click the “Start” button (it should be located in the lower-left corner of your computer), then click “Control Panel”.



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”.



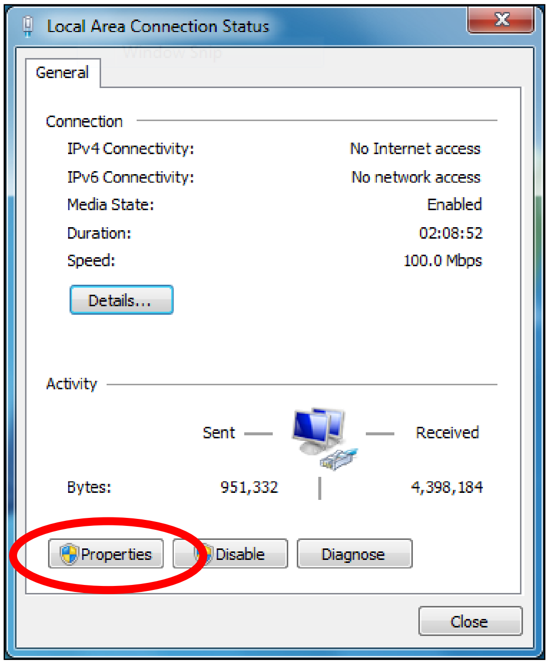
View your basic network information and set up connections

View your active networks

Home network
Home network

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

4. Click “Properties”.



Local Area Connection Status

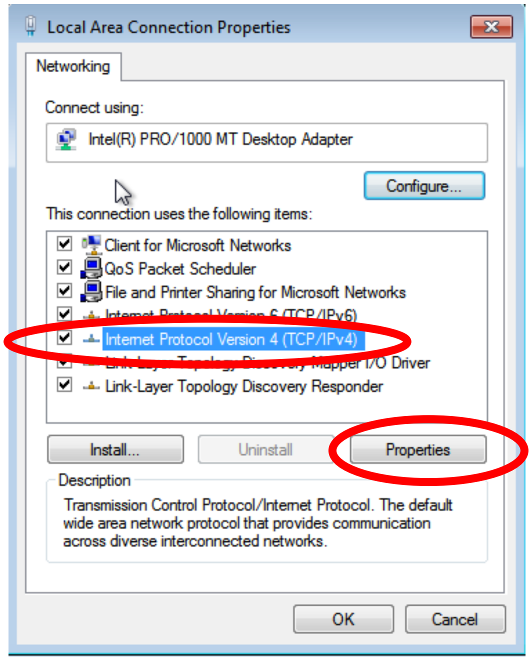
Connection

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”.



Connect using:

Intel(R) PRO/1000 MT Desktop Adapter

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

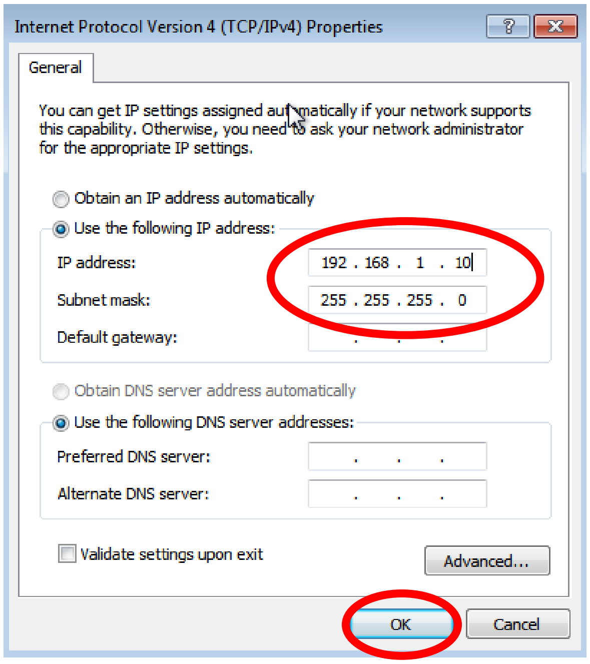
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

IP address: 192.168.1.10

Subnet Mask: 255.255.255.0

Click ‘OK’ when finished.



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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

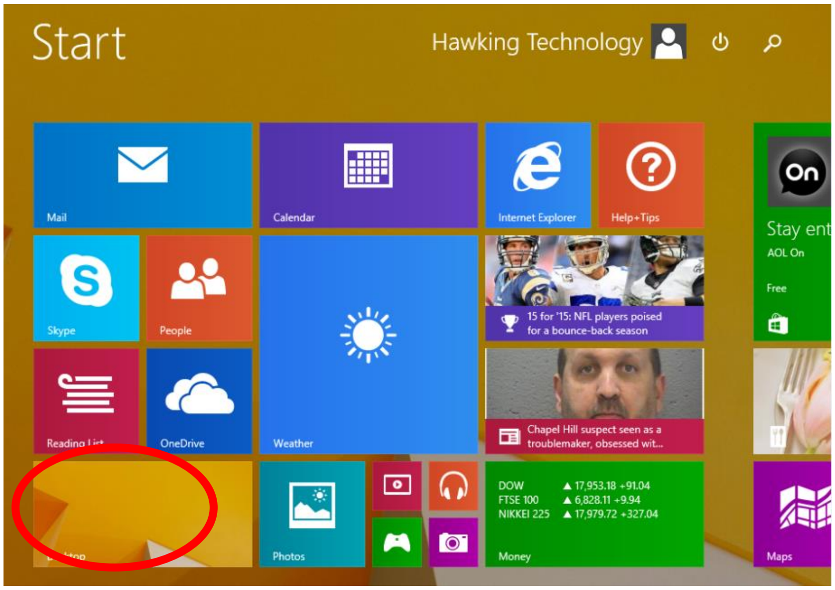
Preferred DNS server: . . .

Alternate DNS server: . . .

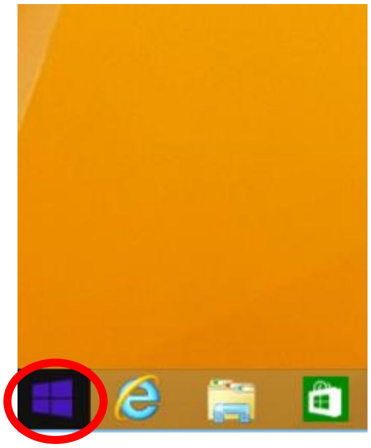
□ Validate settings upon exit

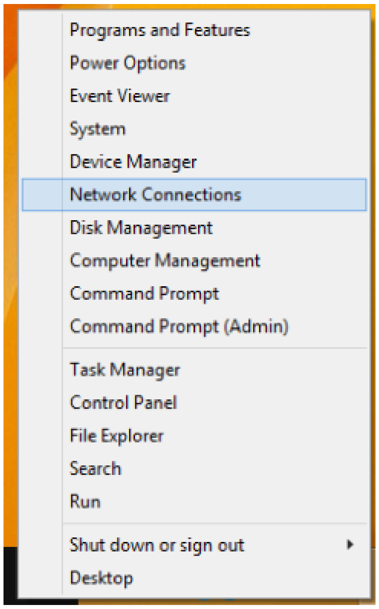
5-1-2. Windows 8.1

1. From the Windows 8.1 Start screen, you need to switch to desktop mode. Click on the Desktop icon.

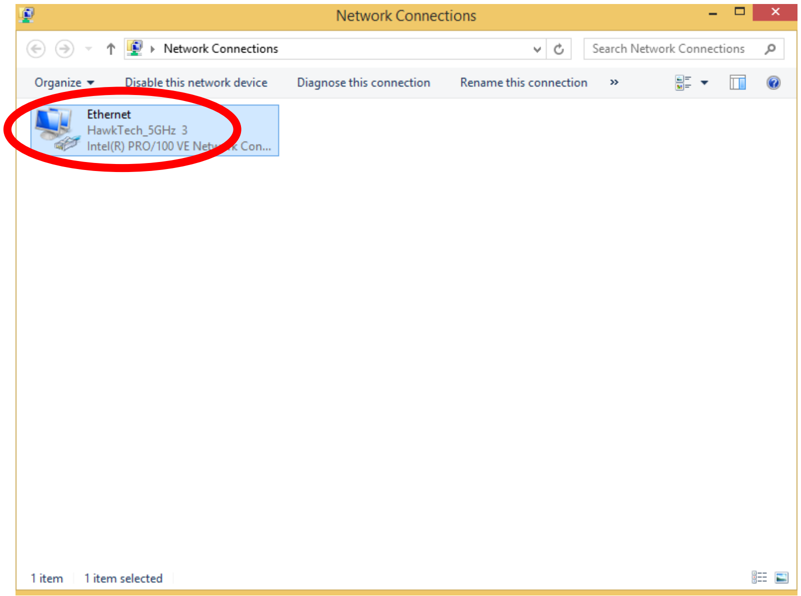

Start
Hawking Technology
Mail
Calendar
Internet Explorer
Help+Tips
Stay ent
AOL On
Free
Skype
People
15 for '15: NFL players poised for a bounce-back season
Reading List
OneDrive
Weather
Chapel Hill suspect seen as a troublemaker, obsessed wit...
Photos
DOW ▲ 17,953.18 +91.04
FTSE 100 ▲ 6,828.11 +9.94
NIKKEI 225 ▲ 17,979.72 +327.04
Money
Maps

2. In desktop mode, right click on the Start Menu and choose Network Connections



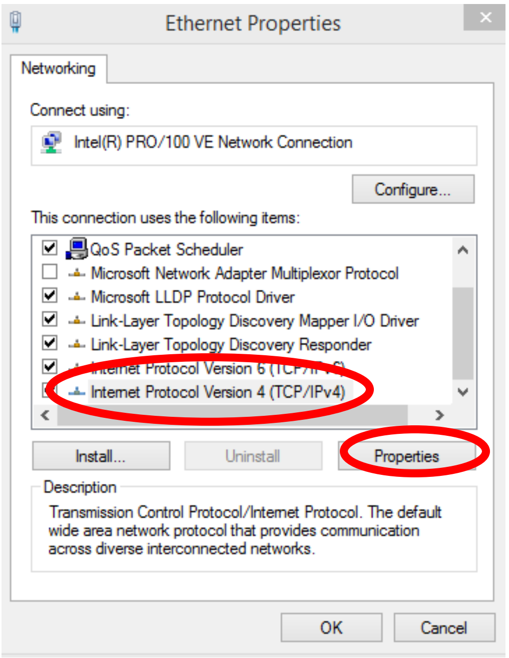


3. Right click “Ethernet” and then select “Properties”.



Ethernet
HawkTech_5GHz 3
Intel(R) PRO/100 VE Network Con...

4. In the window that opens, select “Internet Protocol Version 4 (TCP/IPv4)”, then click on properties.



Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☐ 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

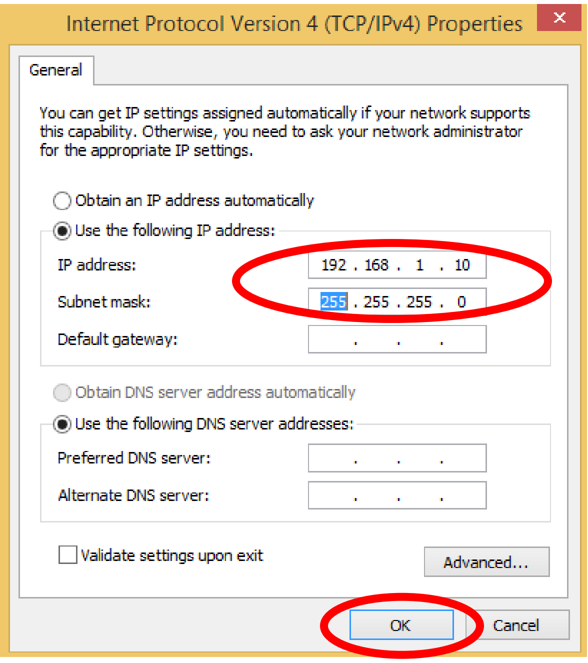
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

IP address: 192.168.1.10

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 . 1 . 10

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

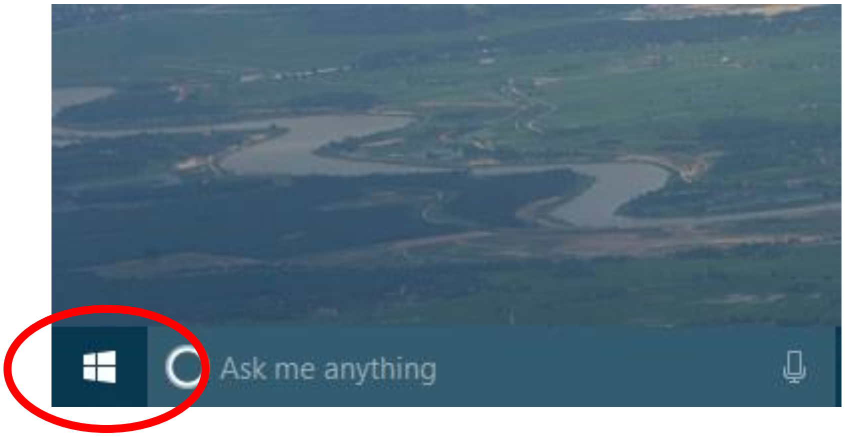
Preferred DNS server: . . .

Alternate DNS server: . . .

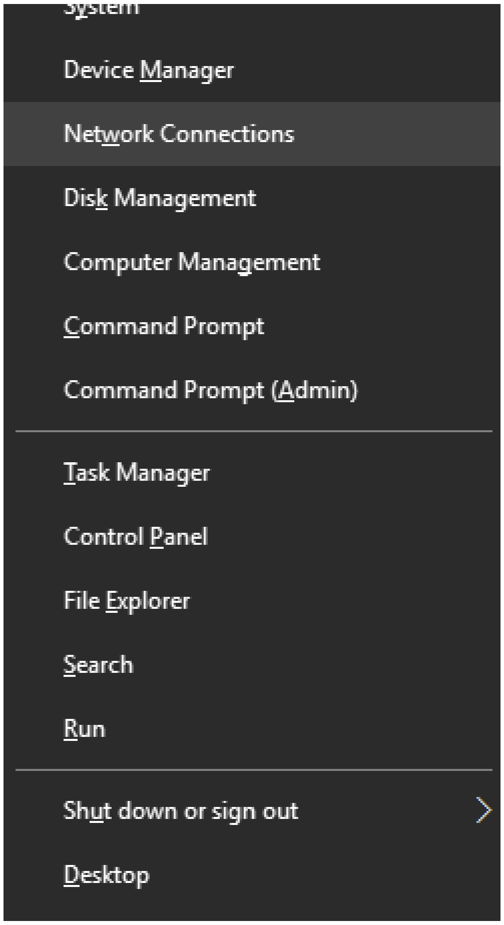
□ Validate settings upon exit

5-1-3. Windows 10

6. From the Windows 10 Start screen, right click on the Start button.



7. Select Network Connections



System

Device Manager

Network Connections

Disk Management

Computer Management

Command Prompt

Command Prompt (Admin)

Task Manager

Control Panel

File Explorer

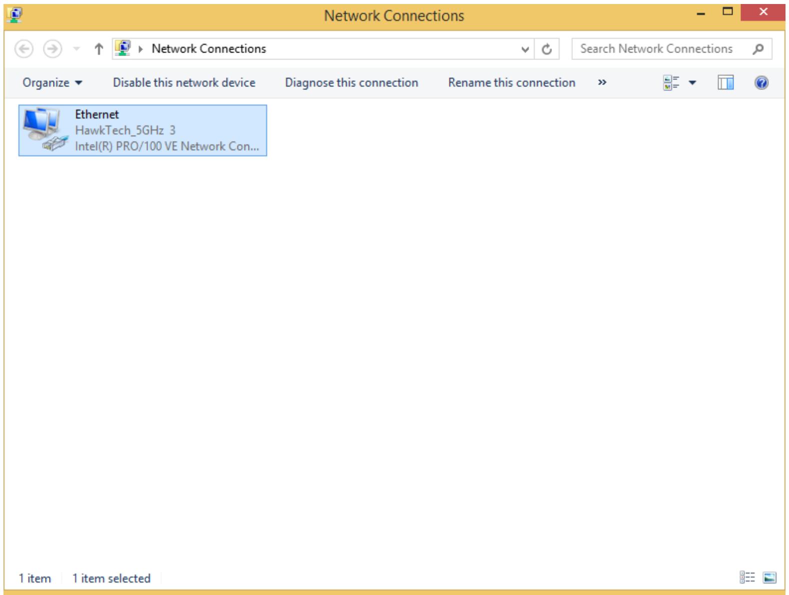
Search

Run

Shut down or sign out

Desktop

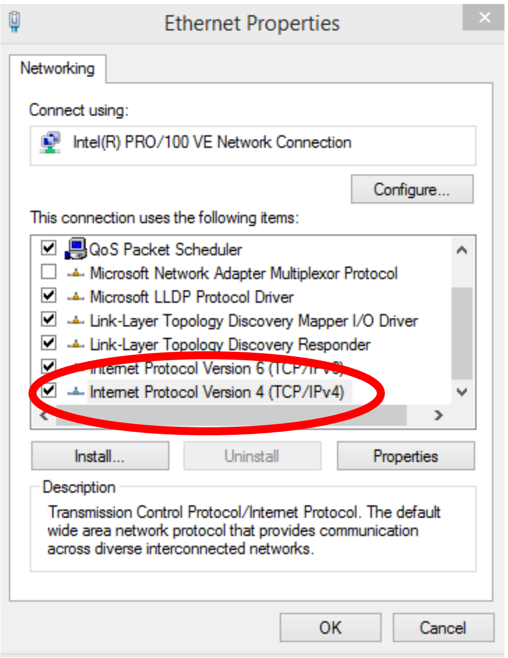
8. Right click “Ethernet” and then select “Properties”.



Ethernet
HawkTech_5GHz 3
Intel(R) PRO/100 VE Network Con...

1 item 1 item selected

9. In the window that opens, select “Internet Protocol Version 4 (TCP/IPv4)”, then click on properties.



Connect using:

Intel(R) PRO/100 VE Network Connection

This connection uses the following items:

- ☑ QoS Packet Scheduler
- ☐ 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

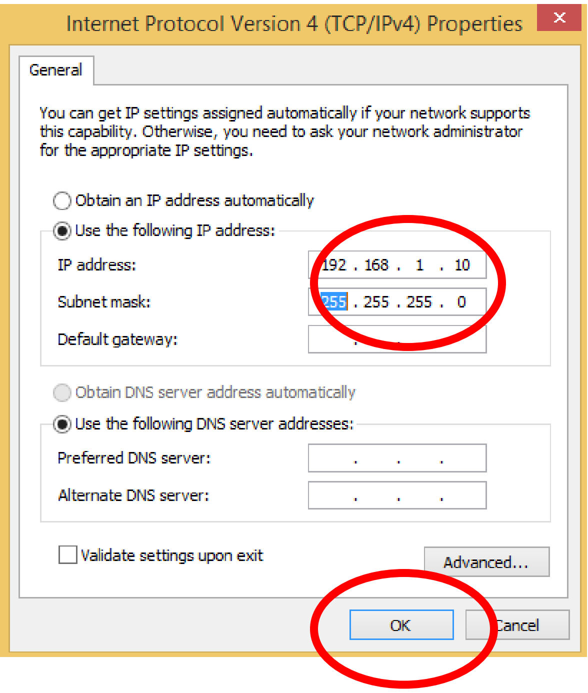
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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

IP address: 192.168.1.10

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 . 1 . 10
Subnet mask:	255 . 255 . 255 . 0
Default gateway:	. . .

○ Obtain DNS server address automatically

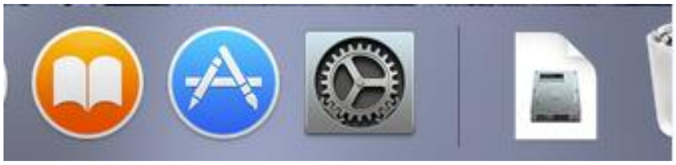
● Use the following DNS server addresses:

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

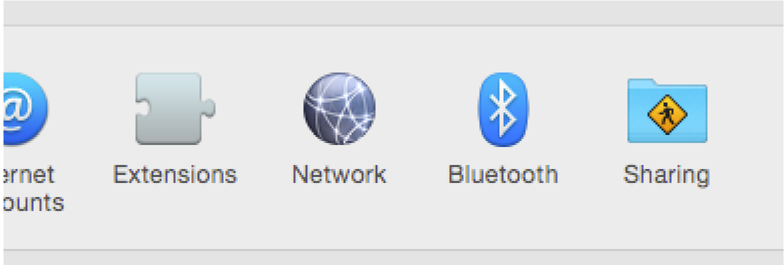
□ Validate settings upon exit

5-1-4. Mac

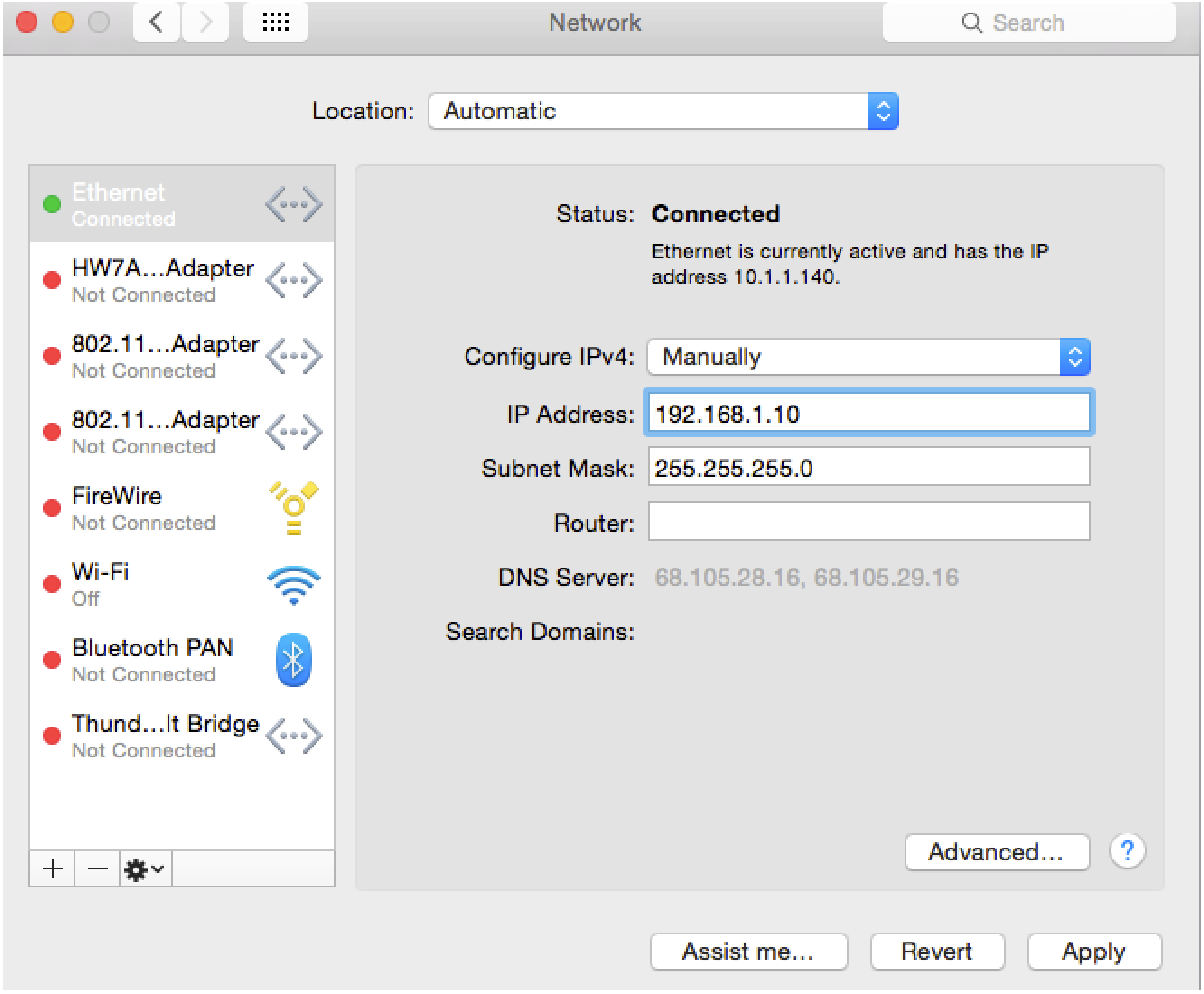
1. Have your Mac computer operate as usual, and click on “System Preferences”



2. In System Preferences, click on “Network”.



3. Click on “Ethernet” in the left panel. Under configure IPv4, change it to manually. Enter the IP address 192.168.1.10 and subnet mask 255.255.255.0. Click on “Apply” to save the changes.



Location: Automatic

Ethernet	Connected
HW7A...Adapter	Not Connected
802.11...Adapter	Not Connected
802.11...Adapter	Not Connected
FireWire	Not Connected
Wi-Fi	Off
Bluetooth PAN	Not Connected
Thund...lt Bridge	Not Connected

Status: **Connected**

Ethernet is currently active and has the IP address 10.1.1.140.

Configure IPv4: Manually

IP Address: 192.168.1.10

Subnet Mask: 255.255.255.0

Router:

DNS Server: 68.105.28.16, 68.105.29.16

Search Domains:

5-2. Hardware Specification

MCU/RF	Qualcomm Atheros QCA9558 (2.4GHz) + QCA9880 (5GHz)
PHY/Switch	Qualcomm Atheros AR8033 and AR8035
Memory	DDR2 128MB
Flash	16MB
Physical Interface	- DC Power Jack - LAN: 2x 10/100/1000 Gigabit Ethernet with PoE support 802.3at (LAN 1) + 802.3af PSE Out (LAN 2) - USB2.0 Interface - Eject Button (USB Eject) - RJ45 Console Port - Reset / WPS button – Power On/Off Switch
Power Requirement	Power over Ethernet, IEEE 802.3at DC : 12V / 4A
Antenna	3 x External Dipole Detachable 2dBi Dual Band Antennas
Others	Internal Buzzer (Find me)

5-3. Environmental and Physical

Temperature Range	Operation : Using PoE : 0 to 50℃ (32°F to 122°F) Using Power Adapter: 0 to 40℃ (32°F to 104°F) Storage : -20 to 60℃ (-4°F to 140°F)
Humidity	90% or less – Operating, 90% or less - Storage
Certifications	FCC, CE
Dimensions	183.3(L) x 183.3(W) x 36(H)mm
Weight	560g (with Antennas)

5-4. 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.