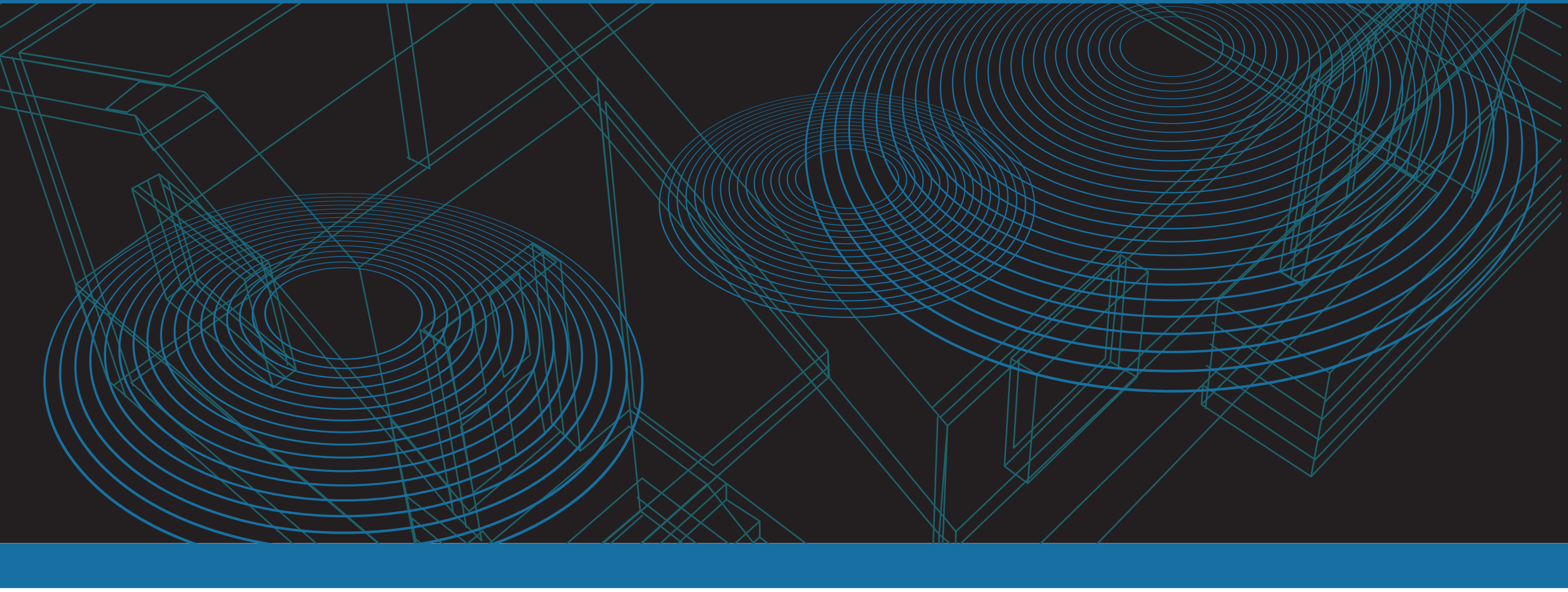
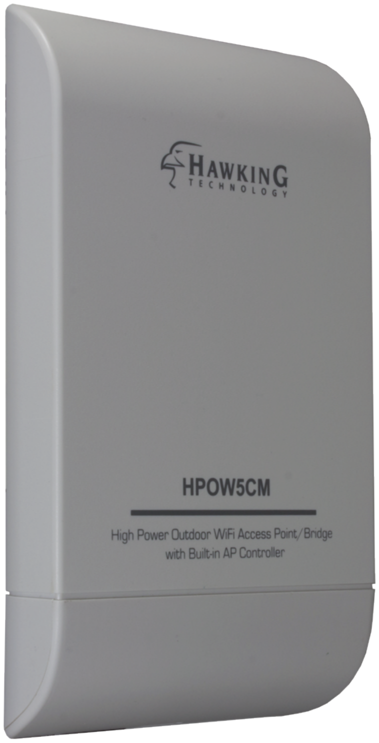
HAWKING® TECHNOLOGY

High Power Outdoor Wireless Access Point with Built-in AP Controller

HPOW5CM




HAWKING TECHNOLOGY
HPOW5CM
High Power Outdoor WiFi Access Point/Bridge
with Built-in AP Controller

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

USER'S MANUAL ▶▶

COPYRIGHT

LIMITED WARRANTY

Hawking Technology guarantees that every HPOW5CM High Power Outdoor Wireless Access Point with Built-in AP Controller is free from physical defects in material and workmanship under normal use for one (1) year from the date of purchase. If the product proves defective during this one-year warranty period, call Hawking Customer Service in order to obtain a Return Authorization number. Warranty is for repair or replacement only. Hawking Technology does not issue any refunds. BE SURE TO HAVE YOUR PROOF OF PURCHASE. RETURN REQUESTS CAN NOT BE PROCESSED WITHOUT PROOF OF PURCHASE. When returning a product, mark the Return Authorization number clearly on the outside of the package and include your original proof of purchase.

IN NO EVENT SHALL HAWKING TECHNOLOGY'S LIABILTY EXCEED THE PRICE PAID FOR THE PRODUCT FROM DIRECT, INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OF THE PRODUCT, ITS ACCOMPANYING SOFTWARE OR ITS DOCUMENTATION. Hawking Technology makes no warranty or representation, expressed, implied or statutory, with respect to its products or the contents or use of this documentation and all accompanying software, and specifically disclaims its quality, performance, merchantability, or fitness for any particular purpose. Hawking Technology reserves the right to revise or updates its products, software, or documentation without obligation to notify any individual or entity. Please direct all inquiries to: techsupport@hawkingtech.com

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.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Table of Contents

Chapter I: Product Information

1-1 Introduction

Thank you for purchasing the HPOW5CM Hawking High Power Outdoor Wireless Access Point with Built-in AP Controller. This highly efficient access point is the best choice for ***Small office / Home office*** users. With the AP controller mode, it allows one unit to control all your HPOW5CMs Access Points on the network. It also allows computers and network devices to gain wireless access in several modes throughout their network. Easy install procedures allow any computer user to setup a network environment in a very short time.

This access point supports IEEE 802.11b/g/n. Using its internal 5dBi Omnidirectional Antennas, all computers and wireless-enabled network devices (including PDA, cellular phone, game console, etc.) can connect to this outdoor wireless access point without additional cabling. 802.11N wireless capability also gives you the highest wireless speeds and compatibility and the 800mW high power gives you the greatest range and flexibility.

Other features of the HPOW5CM include:

- Supports 2.4GHz wireless standard
- Provides IEEE 802.11b/g/n wireless
- 800mW max 2.4GHz wireless transmission power
- 2x 5dBi Omnidirectional Antennas (HPOW5CM)
- 6 different Wireless Modes: AP Controller, Access Point, Router, Wireless Client, Repeater, WISP Client Router
- IEEE 802.11N 2T/2R, Bandwidth up to 300Mbps (Tx and Rx)
- Supports 802.1X, 64/128-bit WEP, WPA, and WPA2 wireless data encryption.
- QoS & WMM
- Integrated Dual Ethernet – 2x 10/100Mbps Ethernet Ports - Power over Ethernet (PoE) & PoE Passthrough
- Multiple Virtual AP
- Business Class WLAN Security and Client Authentication
- Web Management and SNMP MIB II
- Client Isolation through Layer 2 VLAN
- Bandwidth traffic Shaping
- 802.11r Fast Roaming

Networking

- Support Static IP, Dynamic IP(DHCP Client) and PPPoE on WiFi WAN Connection
- Support MPPE-64 and MPPE-128 Encryption on PPTP Connection
- PPPoE and PPTP Reconnect – Always On , On demand, Manual
- Support PPTP/L2TP Pass Through
- MAC Cloning
- DHCP Server
- 802.3 Bridging

- NAT
- Proxy DNS
- Dynamic DNS
- NTP Client
- DMZ
- Virtual Server (Port Forwarding)
- Support MAC Filter
- Support IP Filter
- Support Layer-7 Protocol Filter and Content Filter
- Support Static Routing
- Support RIP and OSPF Dynamic Routing
- Bandwidth traffic Shaping

Wireless Feature

- Transmission power control : 3%, 6%, 12.5%, 25%, 50%, 100%
- Channel selection : Manual or Auto
- Associated clients limitation : 64
- No. of ESSID (Virtual AP): 8
- No. of Max. WDS setting: 8
- Preamble setting: Short/ Long
- Setting for 802.11b only, 802.11b/g mix, 802.11b/g/n mix or 802.11n only
- Setting for transmission speed
- Dynamic Wireless re-transmission
- IEEE802.11f IAPP (Inter Access Point Protocol), hand over users to another AP
- IEEE 802.11i Preauth (PMKSA Cache)
- IEEE 802.11d -Multi country roaming
- Wireless Site Survey
- Channel Bandwidth setting : 20MHz or 20/40MHz
- HT Tx/Rx Stream selection : 1 or 2
- A-MSDU and A-MPDU support
- Maximal MPDU density for TX aggregation setting
- Short Slot support
- RTS Threshold and Fragment Threshold support
- IGMP Snooping v1, v2 and v3
- 802.11r Fast Roaming

Authentication/ Encryption (Wireless Security)

- Layer2 User Isolation
- Blocks client to client discovery within a specified VLAN
- WEP 64/ 128 /152 Bits
- EAP-TLS + Dynamic WEP
- EAP-TTLS + Dynamic WEP
- PEAP/ MS-PEAP+Dynamic WEP
- WPA (PSK +TKIP)
- WPA (802.1x certification + TKIP)

- 802.11i WPA2 (PSK + CCMP/ AES)
- 802.11i WPA2 (802.1x certification + CCMP/ AES)
- Setting for TKIP/ CCMP/ AES key's refreshing period
- Hidden ESSID support
- Setting for "Deny ANY " connection request
- MAC ACL
- No. of registered RADIUS servers : 2
- VLAN assignment on ESSID
- VLAN tag over WDS
- Support WEP and AES data encryption over WDS link

Quality of Service

- Download and Upload traffic control
- IEEE802.11e WMM

System Administration

- Intuitive Web Management Interface
- Password Protected Access
- Firmware upgrade via Web
- Reset to Factory Defaults
- Profiles Configuration Backup and Restore
- One-button-click to reset factory default
- Two administrator accounts
- Remote Link Test – Display connect statistics
- Full Statistics and Status Reporting
- NTP Time Synchronization
- Even Log
- Support SNMP v1, v2c, v3
- SNMP Traps to a list of IP Address
- Support MIB II
- Ping Watchdog
- CLI access via Telnet and SSH
- Administrative Access : HTTP and HTTPS
- UPnP (Universal Plug and Play)

1-2 Safety Information

In order to keep the safety of users and property, please follow these safety instructions:

1. This access point is designed for outdoor use and is weather resistant.

2. DO NOT put this access point at or near hot or humid places, like kitchens or bathrooms. Also, do not leave this access point in the car in summer.

3. DO NOT pull any connected cable with force; disconnect them from the access point first.

4. If you want to place this access point in a high place or hang on the wall, please make sure the access point is firmly secured. Falling can damage the access point and its accessories and the warranty will be void.

5. Accessories of this access point, like antennas and power supply, are a danger to small children under 3 years old. KEEP THIS ACCESS POINT OUT OF THE REACH OF CHILDREN!

6. The access point will become warm when used for a long period of time (***This is normal and is not a malfunction).*** DO NOT put this access point on paper, cloth, or other flammable materials.

7. There are no user-serviceable parts inside the access point. If you have found that the access point is not working properly, please contact technical support or your place of purchase and ask for help. DO NOT disassemble the access point, or warranty will be void.

8. If the access point falls into water when it's powered on, DO NOT use your hands to pick it up. Switch the electrical power off before you do anything, or contact an experienced technician for help.

9. If you smell something strange, or see smoke coming out from the access point or power supply, remove the power supply or switch the electrical power off immediately, and call techsupport or your place of purchase for help.

1-3 System Requirements

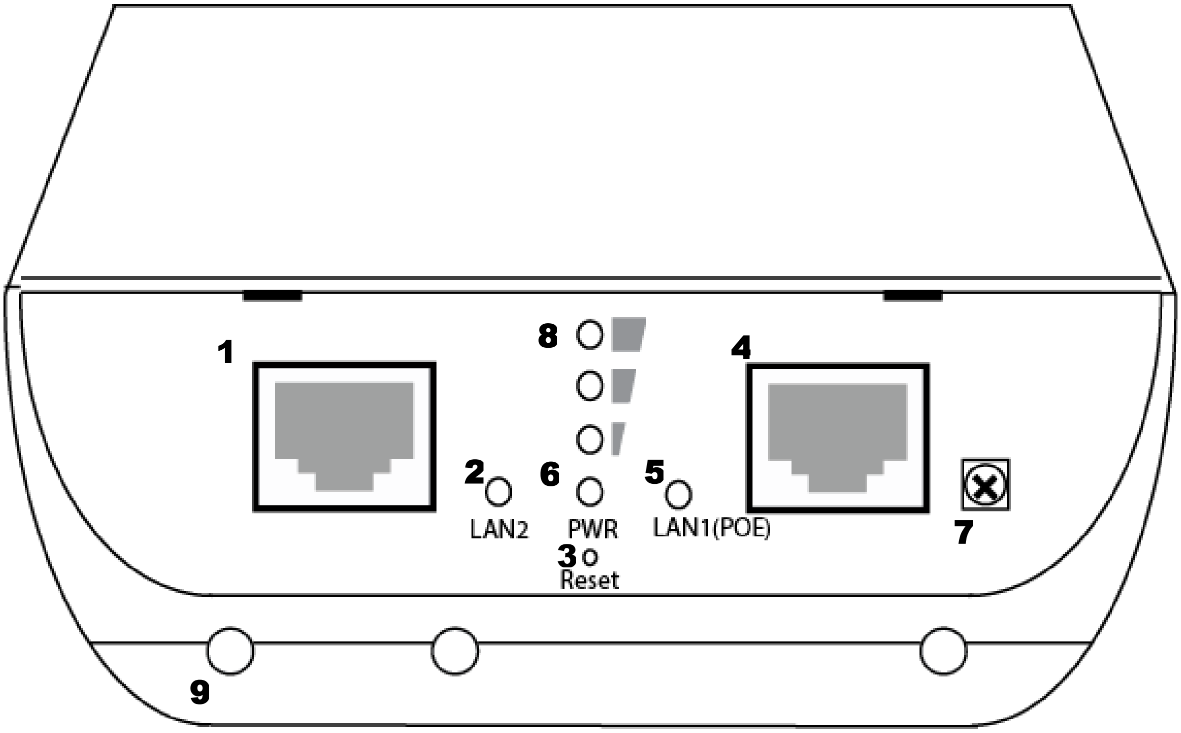
- One computer (Mac or PC).
- Internet Web Browser (Internet Explorer, Safari, etc.)
- A Wired or Wireless network adapter (e.g. Airport card, built-in Ethernet adapter, etc.)

1-4 Package Contents

Before you start to use this access point, please check if there's anything missing in the package, and contact your place of purchase or contact Hawking Technologies.

- 1x HPOW5CM
- 1x RJ45 Cable
- 1x Power Adapter (Power Supply)
- 1x Power Over Ethernet (PoE) Adapter
- 1x Wall Mounting Kit
- 2x Cable Ties for Stand/Pole mounting
- 1x Setup CD (includes Manual/QIG)
- 1x Quick Installation Guide (QIG)

1-5 Product Overview



(1) LAN2's Ethernet port
(2) LED Indicator for LAN2
(3) Reset Button. Press and hold the reset button for at least 15 seconds to factory reset the device.

(4) LAN1 (PoE) Ethernet port

(5) LED indicator for LAN1

(6) Power LED

(7) Grounding Connection: Grounding cable can protect this device from lightning strikes and buildup of static electricity. Grounding cable not included in the package. We suggest 16-18 AWG grounding cable.

(8) LED for strong/weak WiFi Signal Indicator for Client Bridge, Repeater, WISP

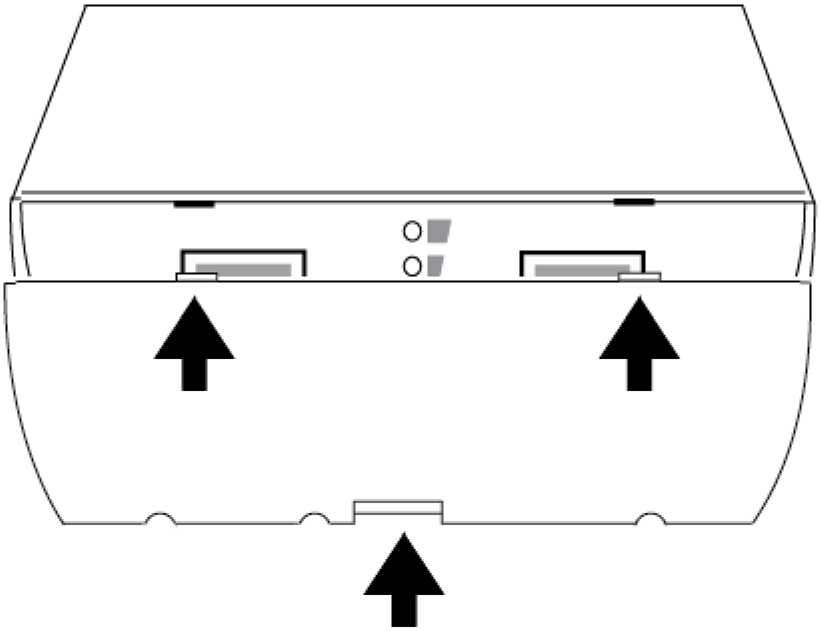
(9) Ethernet cable guide ports. These can be popped out to guide your Ethernet cables out of the device. Guide your Ethernet cables through here so you can close the outside latch.

Chapter II: System and Network Setup

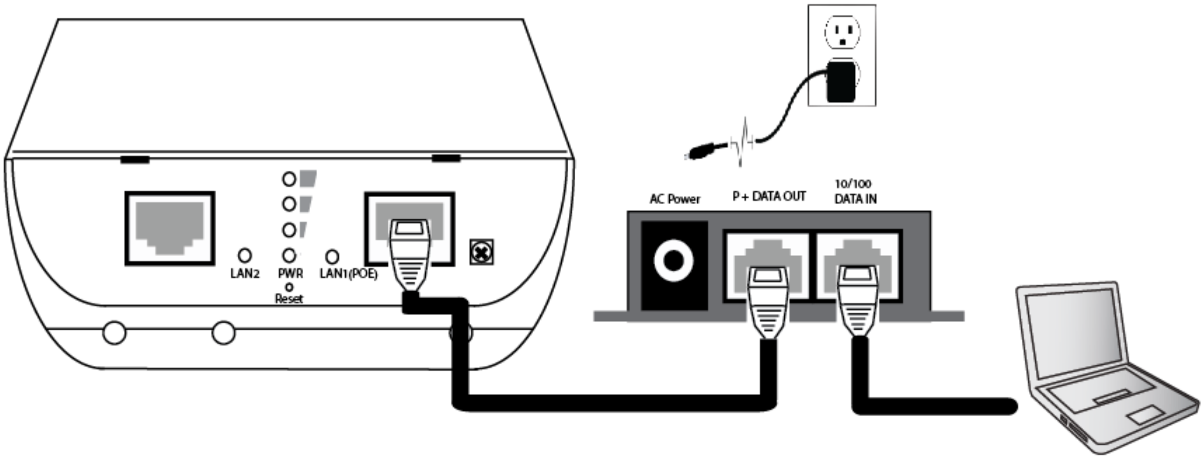
2-1 Build Network Connection

Please follow the following instructions to build the network connection between your new HPOW5CM access point and your computers and other network devices:

1. Remove cover from device. Press the center tab (you may need a flathead screwdriver) and the cover should be able to be removed with a small amount of force.



2. Connect the A/C power adapter to the wall socket, and then connect it to the 'Power' socket of the PoE injector. Connect a Ethernet cable from the "P + Data Out" port on the PoE injector into the HPOW5CM LAN1(POE) Port.
3. Connect a Ethernet cable from the "10/100 Data in" on the PoE injector to your computer/network.

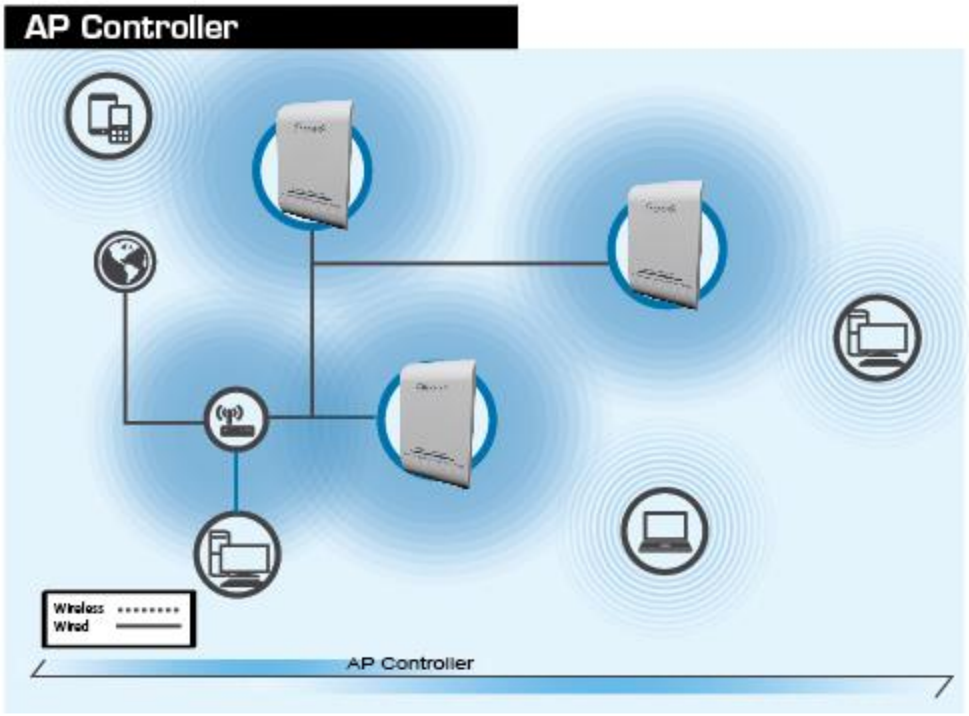


4. Configure the IP Address of your computer to be in the same range as the HPOW5CM (see section 2-3)

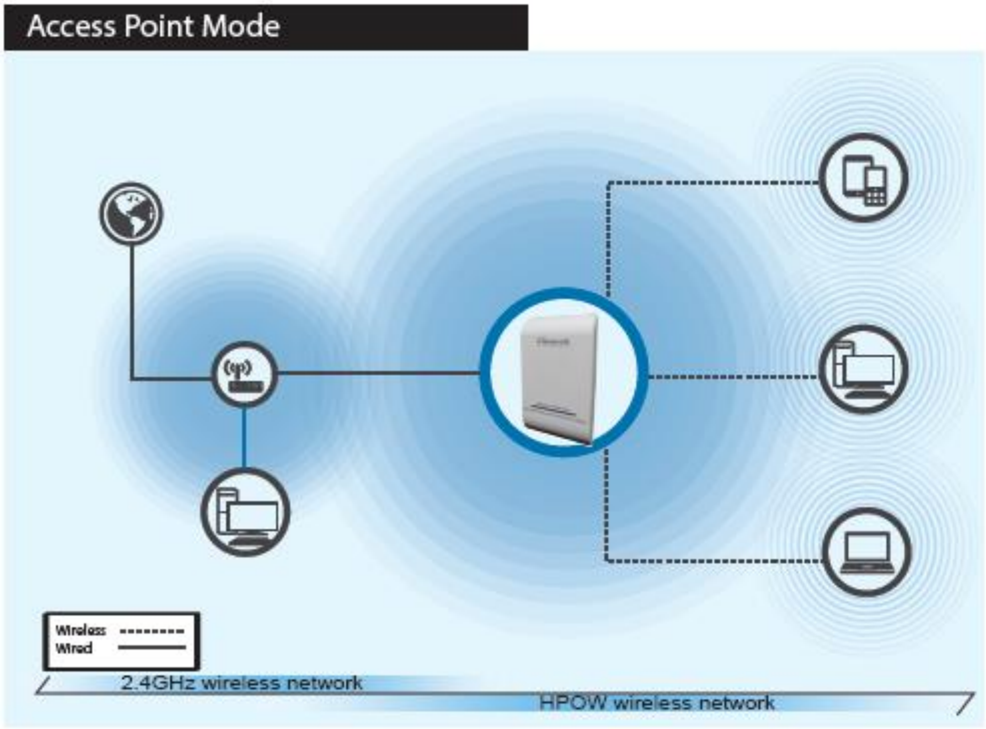
Log into the setup page to configure the HPOW5CM

2-2 Definitions of HPOW5CM Supported Modes

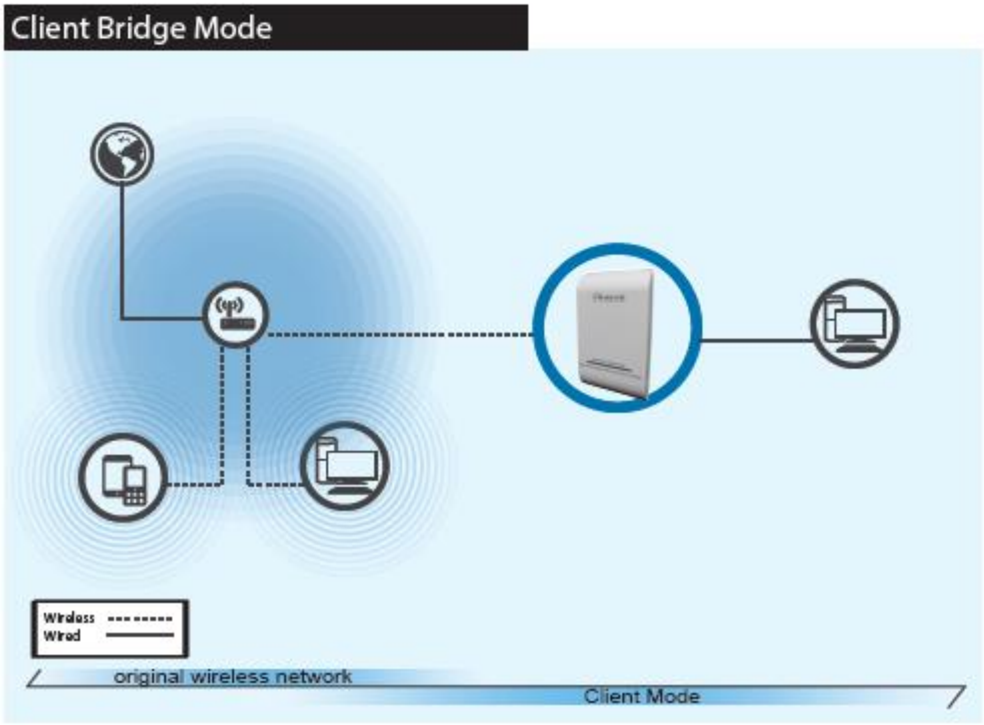
The HPOW5CM supports 6 different modes.



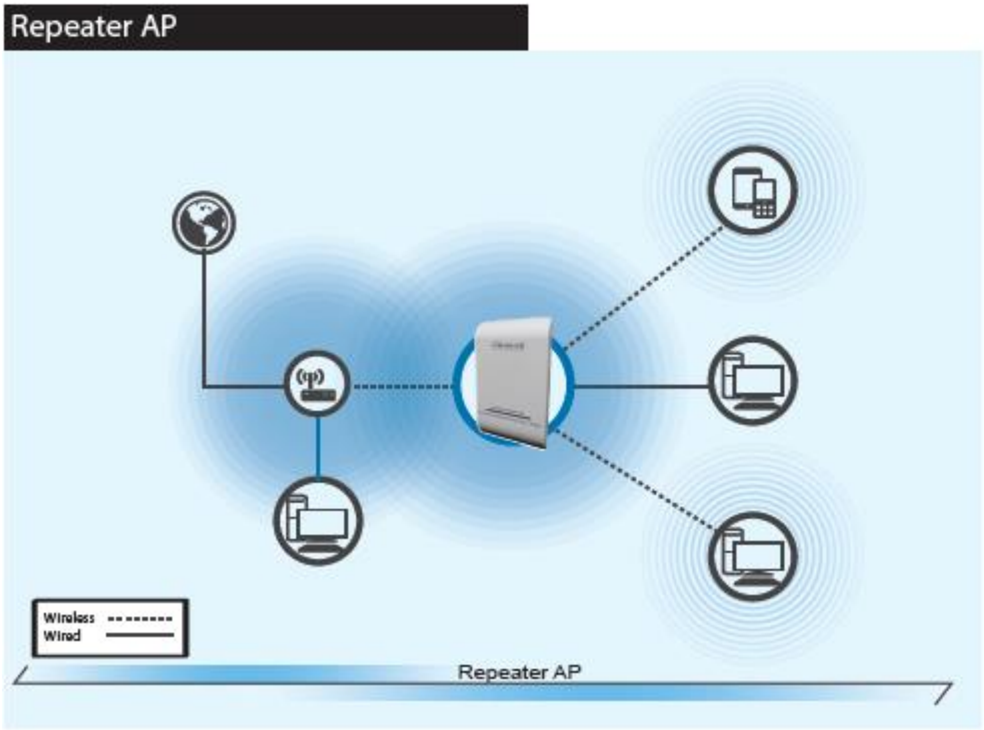
When AP Controller mode is setup, one HPOW5CM is setup to control multiple HPOW5CM's on the network. The HPOW5CM in AP controller mode can set IPs, configure wireless settings, monitor wireless status, upgrade firmware and remotely controll multiple HPOW5CMs. The other HPOW5CMs must be in AP mode. Go to section 3-1



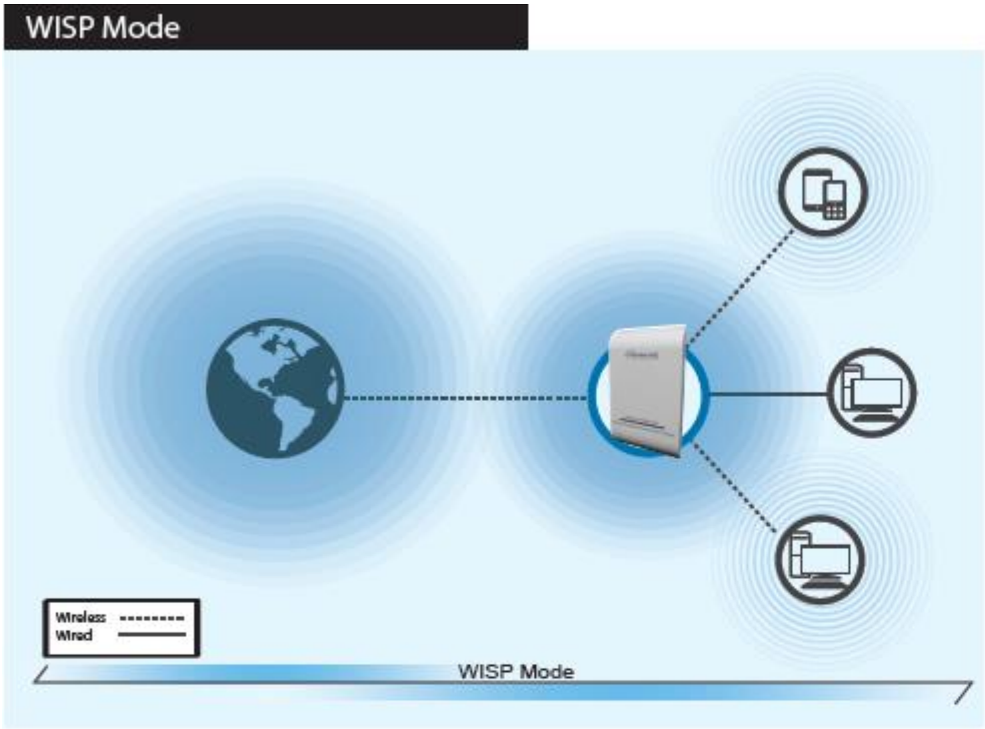
When AP mode is chosen, the system can be configured as a standard wireless access point. In this mode, the device can be used as an Access Point for wireless client connection. All Ethernet ports wand wireless interfaces are bridged together. Go to section 3-2



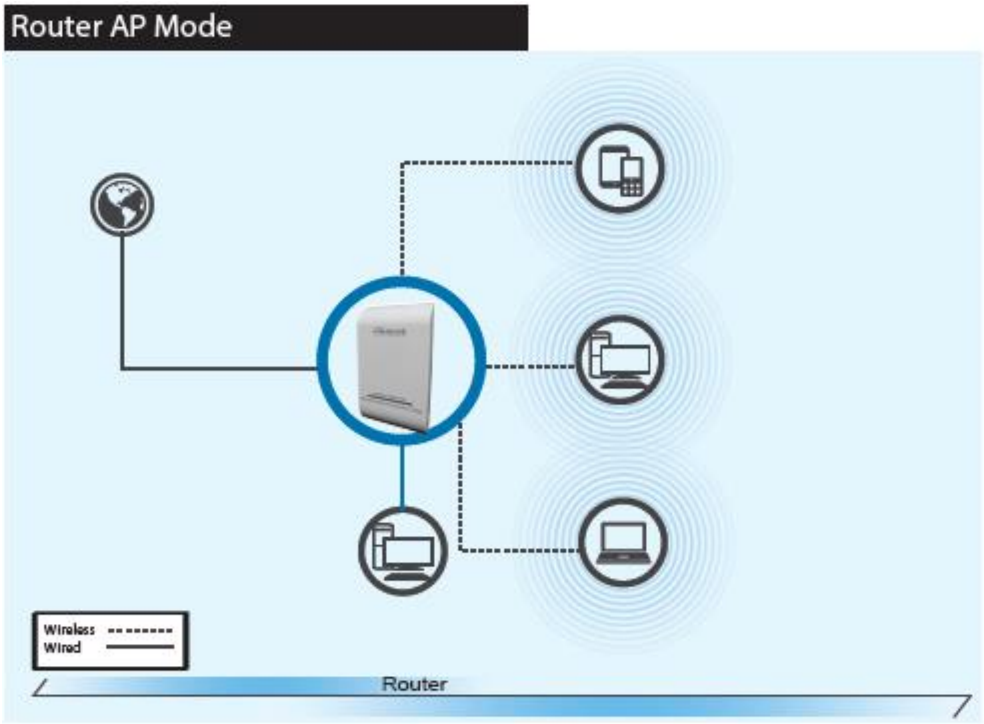
When Client Bridge + Repeater AP Mode is chosen, the system can be configured in bridged mode. In this mode, the device can connect to other Access Points via a wireless link and be used to bridge wired clients to the network. Go to section 3-3



In this mode, the device can connect to other Access Points via a wireless link and be used to bridge wired clients to the network and work as a wireless repeater for wireless devices. All Ethernet ports and repeater access points are bridged together. Go to section 3-3



When WISP mode is chosen, the system can be configured in Wireless repeater mode. In this mode, the device can wirelessly connect to a WISP (wireless internet service provider), ie. Another wireless AP, HotSpot, etc. It can then wirelessly repeat the signal and can even act as a router for these signals. NAT is enabled and wired and wireless computers can share the same IP range. Go to section 3-4



When Router AP mode is chosen, the system can be configured as a Wireless Router. In this mode, the device is supposed to be connected to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN/WLAN port share the same IP to ISP through the WAN port. The connection type can be setup in WAN page by using static IP, Dynamic IP, PPPoE or PPTP client. Go to section 3-5

2-3 Connecting to the HPOW5CM via Web Browser

After the network connection is built, the next step you should do is setup the access point with proper network parameters, so it can work properly in your network environment.

Before you can connect to the access point and start configuration procedures, your computer must be set to static IP. Please follow the following instructions to configure your computer to use a static IP address:

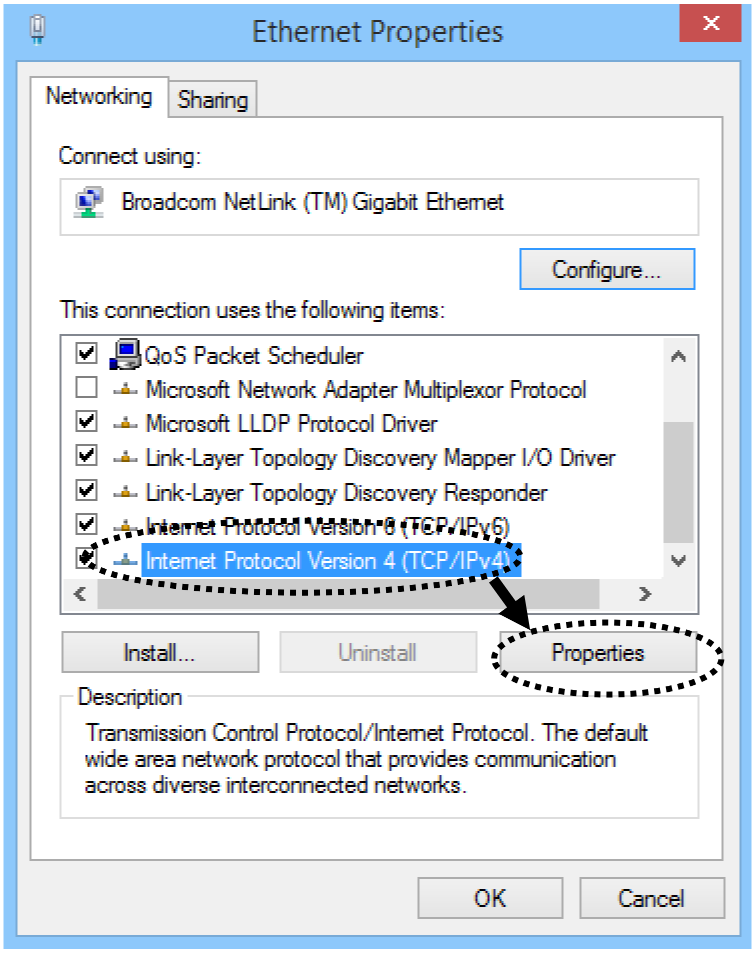
If the operating system of your computer is….

Windows 7/8/10	**- please go to section 2-3-1**
Mac OS	**- please go to section 2-3-2**

2-3-1 Windows 7/8/10 IP address setup

1. You will have to assign your computer an IP address temporarily. Note, once this is done, please remember to change it back to ‘obtain an IP address automatically’.

First, right click on 'Start' button (or left click if this is Windows 7 or below), then choose **Control Panel**. Under ***Network and Internet,*** choose ***View Network Status and Tasks***, then choose ***Change Adapter Settings*** on the left hand column. Right-click ***Ethernet (or Local Area Connection), then select 'Properties'. Ethernet (Local Area Connection) Properties*** window will appear, select 'Internet Protocol Version 4 (TCP / IPv4), and then click 'Properties'



Ethernet Properties

Networking | Sharing

Connect using:

Broadcom NetLink (TM) Gigabit Ethernet

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

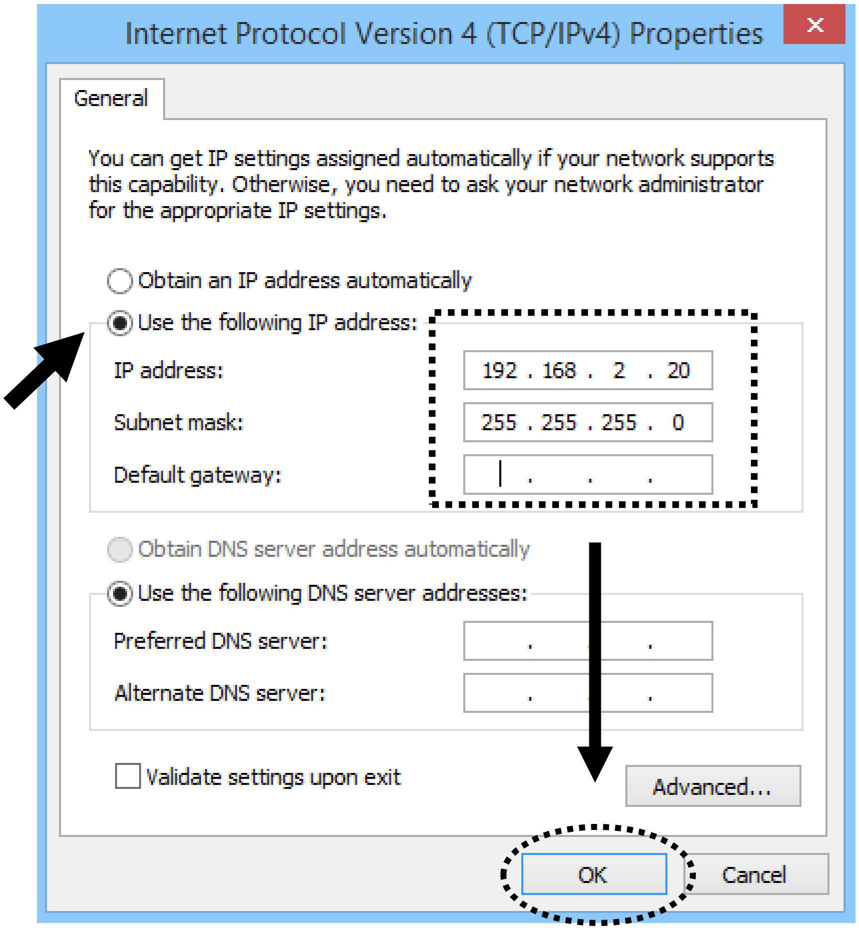
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

2. Select 'Use the following IP address', then input the following settings in respective field:

IP address: 192.168.2.20

Subnet Mask: 255.255.255.0

click 'OK' when finish.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

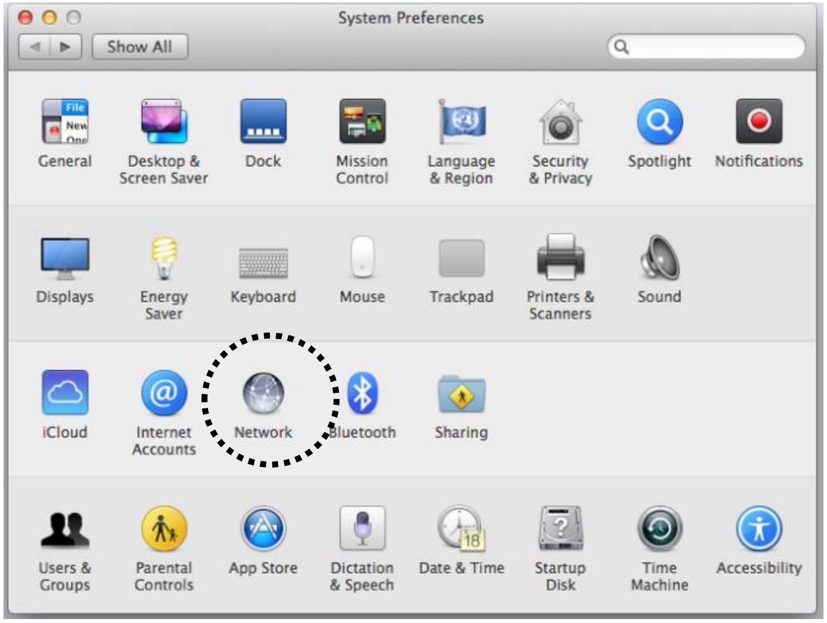
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

2-3-2 Mac OS X IP Address Setup

Go to your System Preferences, go to Network.

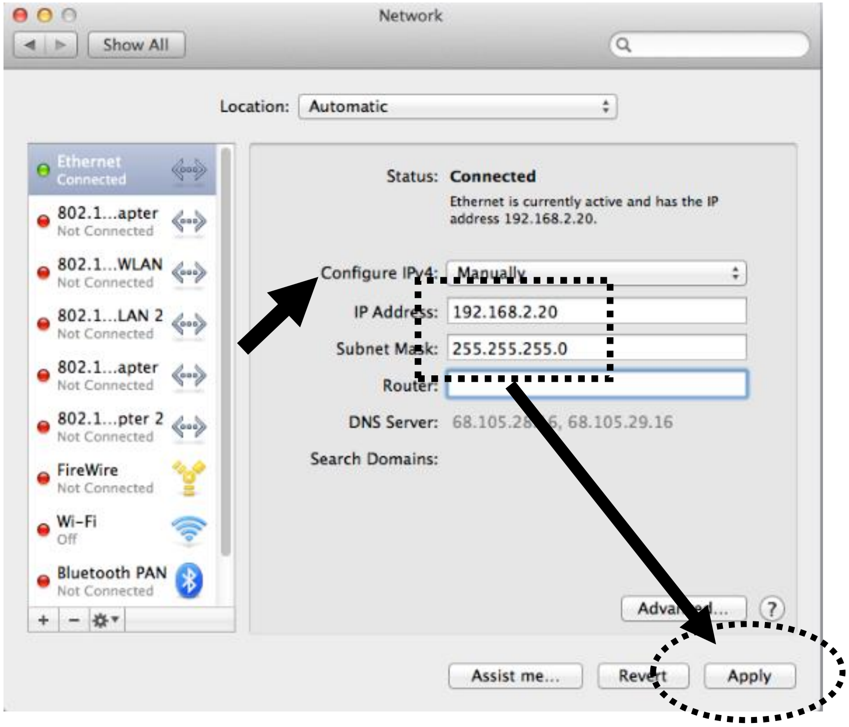


Select your Ethernet adapter. Make sure next to “Configure IPv4”, you have it set under “Manually”

IP Address 192.168.2.20

Subnet Mask: 255.255.255.0

Click ‘Apply’ when finished



Location: Automatic

Status: **Connected**

Ethernet is currently active and has the IP address 192.168.2.20.

Configure IPv4: Manually

IP Address: 192.168.2.20

Subnet Mask: 255.255.255.0

Router:

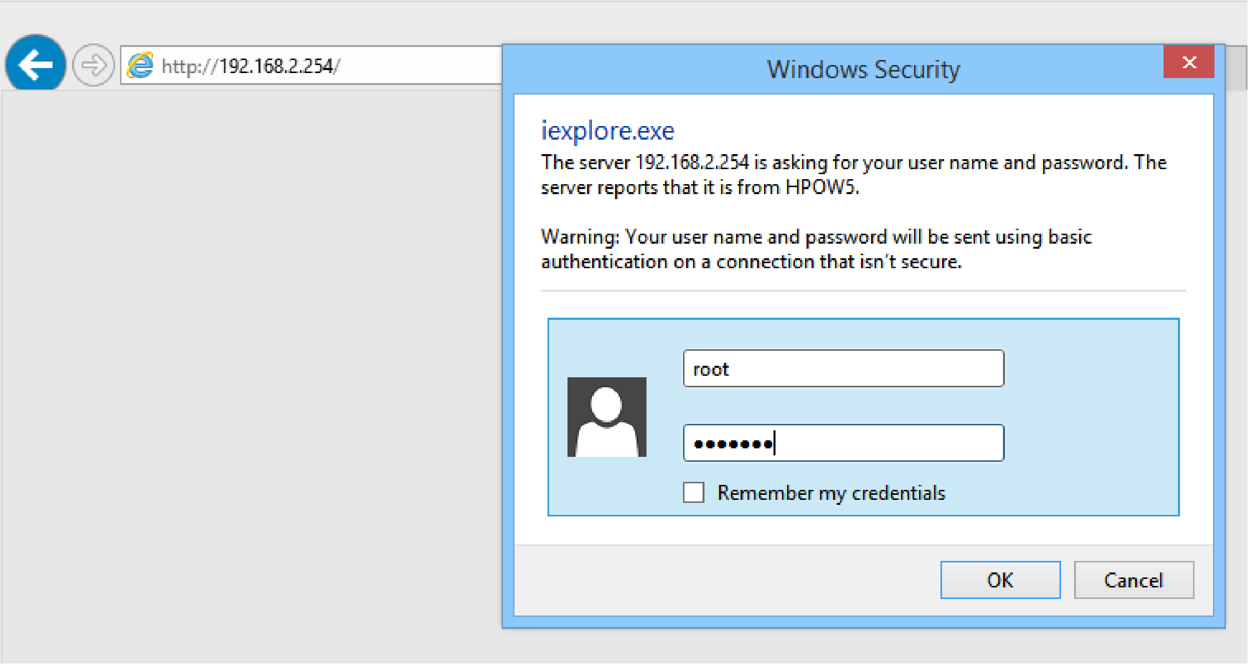
DNS Server: 68.105.28.16, 68.105.29.16

Search Domains:

2-3-3 Accessing the Web Page User Interface

After the IP address setup is complete, please open your web browser.
In the address field, please type: ‘192.168.2.254’ and press enter.

The following message should be shown:



iexplore.exe

The server 192.168.2.254 is asking for your user name and password. The server reports that it is from HPOW5.

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

root

•••••••

□ Remember my credentials

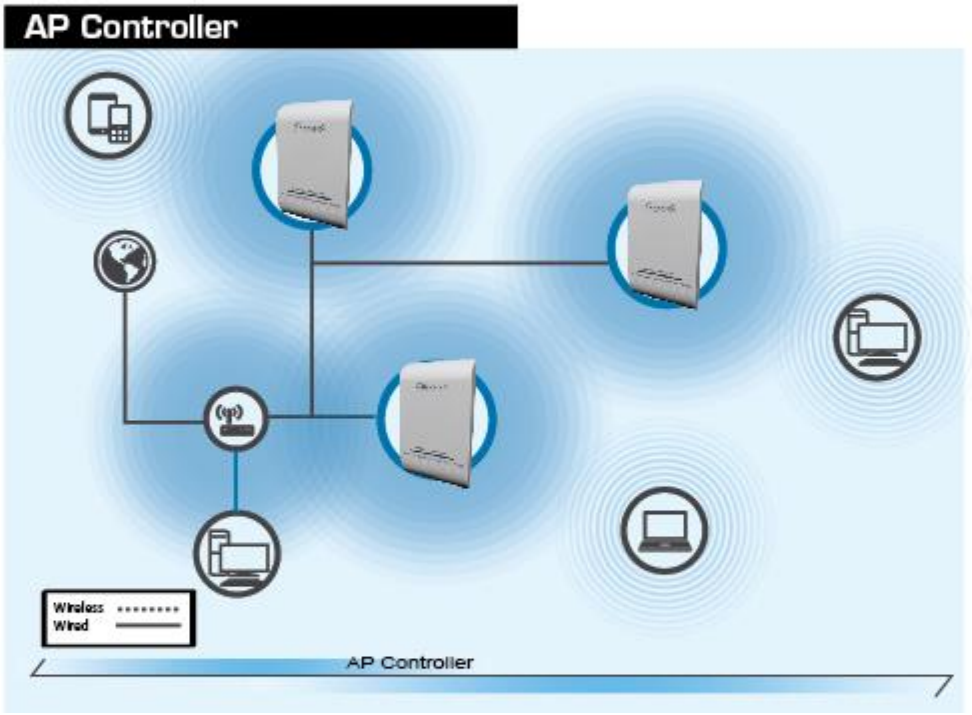
For username and passwords, see the table below:

	Root Account
Username:	root
Password:	default

Chapter III: Setup Wizard

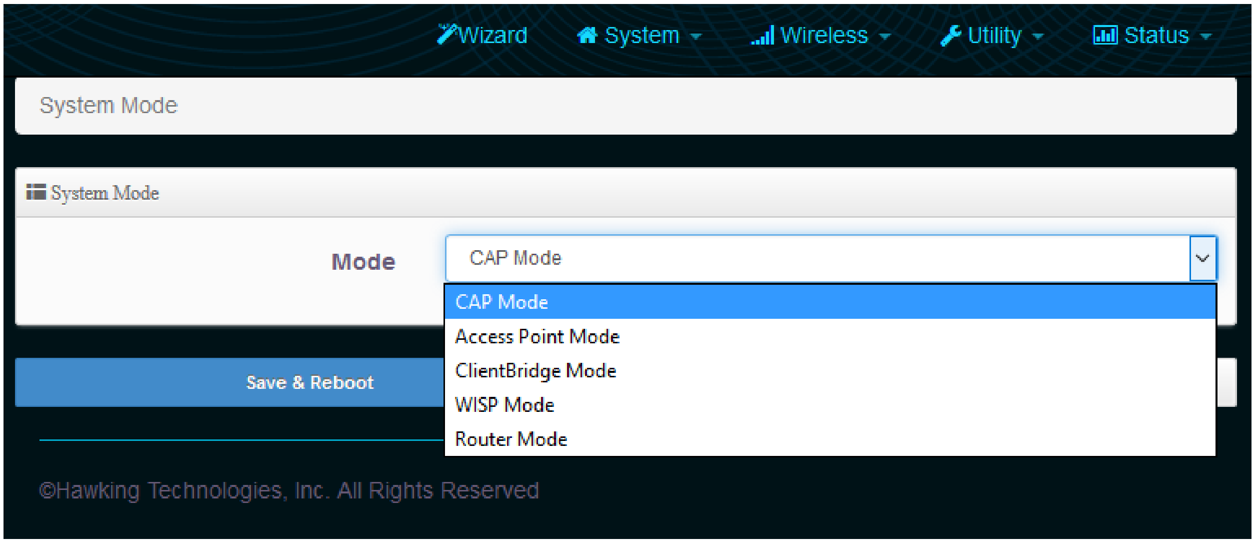
This section will outline how to access the setup wizard and configure each of the modes in the HPOW5CM

3-1 Controller AP Mode



When AP Controller mode is selected, one HPOW5CM is setup to control multiple HPOW5CM's in AP mode on the network. The HPOW5CM in AP controller mode can set IPs, configure wireless settings, monitor wireless status, upgrade firmware and remotely controll multiple HPOW5CMs. Note: the other HPOW5CMs can only be in AP Mode.

Log into the settings page, go to system and select "Mode Setup". Choose CAP Mode. Click Save & Reboot.

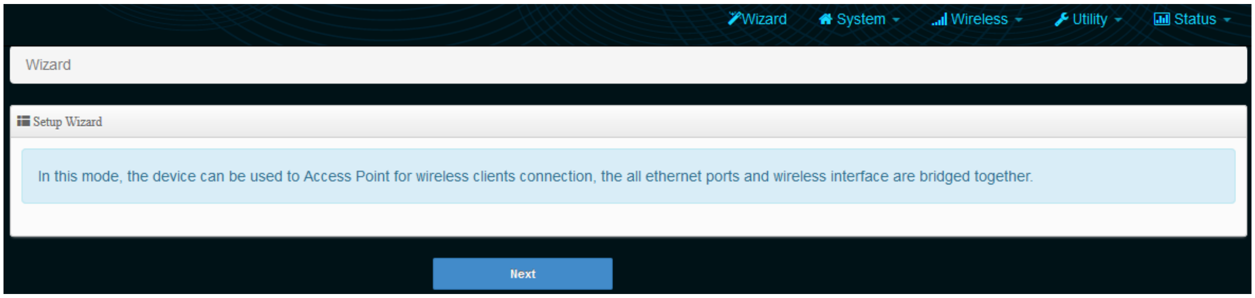


Mode: CAP Mode

©Hawking Technologies, Inc. All Rights Reserved

The device will now reboot.

Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Click on “Wizard”. Click “Next”



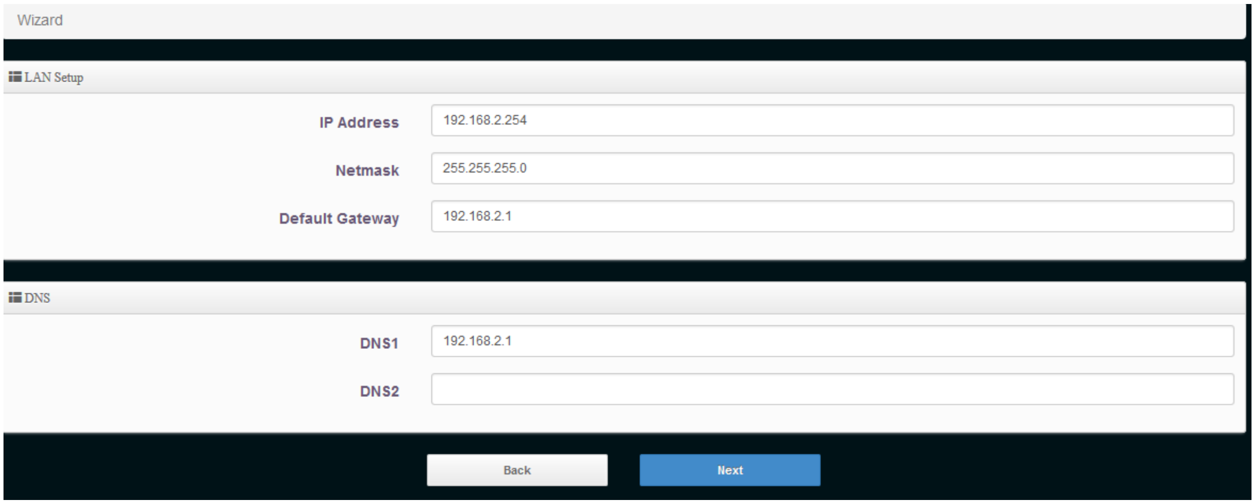
In this mode, the device can be used to Access Point for wireless clients connection, the all ethernet ports and wireless interface are bridged together.

3-1-1 Setup Wizard

This section is optional and will only setup the IP settings and the AP settings in CAP mode.

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose “specify” and enter in your values.



Wizard

LAN Setup

IP Address	192.168.2.254
Netmask	255.255.255.0
Default Gateway	192.168.2.1

DNS

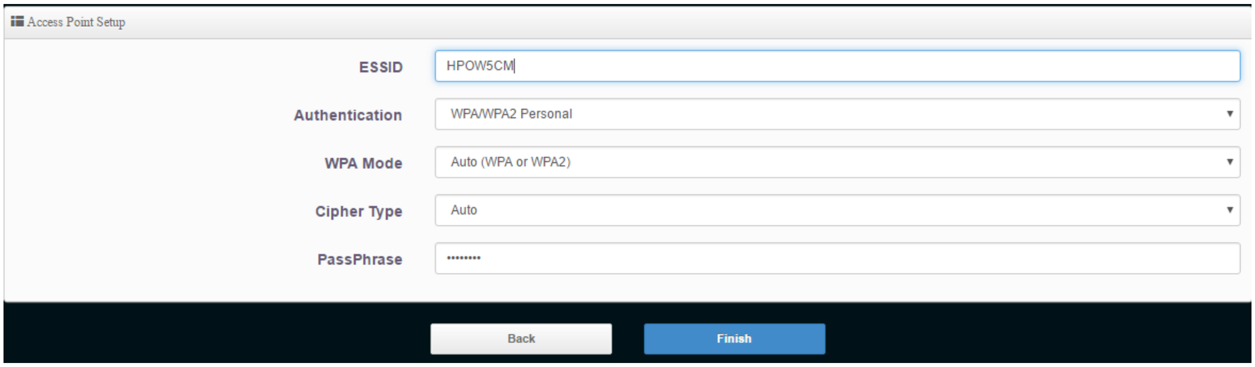
DNS1	192.168.2.1
DNS2	

3-1-1-1 Wireless Setup

This page is used to define the parameters for the wireless for the CAP Mode. In CAP Mode, the HPOW5CM can also act as an access point.

ESSID: *This is the wireless broadcast name. By default, it is 'Hawking_HPOW5CM' but you can change it to whatever you want.*

Authentication: *Choose your type of security (Hawking recommends AUTO (WPA or WPA-2PSK))*



Access Point Setup

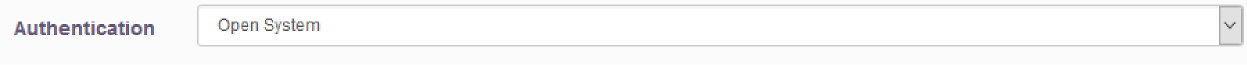
ESSID	HPOW5CM
Authentication	WPA/WPA2 Personal
WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
PassPhrase	••••••••

3-1-1-2 Authentication (Wireless Security)

This section allows you to set up wireless security to prevent any unauthorized access to your wireless network.

- Open System (security disabled)

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled

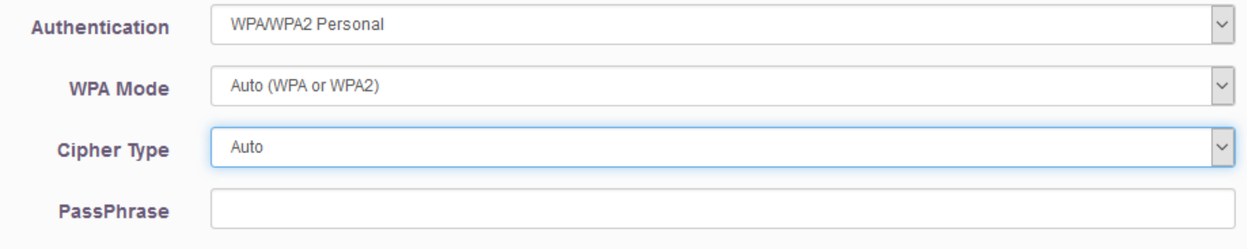


Authentication: Open System

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

- Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:



Authentication	WPA/WPA2 Personal
WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
PassPhrase	

Cipher Type: ***AES*** *is short for* ***Advanced Encryption Standard****, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.* ***TKIP*** *is short for* ***Temporal Key Integrity Protocol****, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

Pre-shared: *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

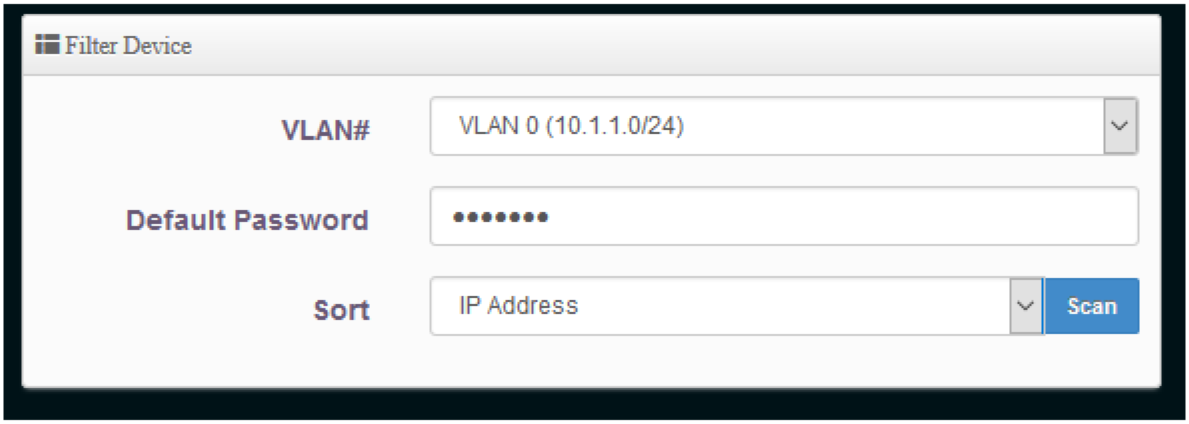
Hawking recommends using WPA2-PSK w/ AES cipher type as your default level of security.

Click Finish and the device will automatically restart and save your settings. After you have finished, a network device must be connected to your network via the 10/100 Data In port on the PoE adapter or the LAN2 port to add this device to your network. Please change your computer IP address back to "Obtain an IP automatically".

3-1-2 Scan AP Device

In this section, you will add other HPOW5CM's to the Controller list.

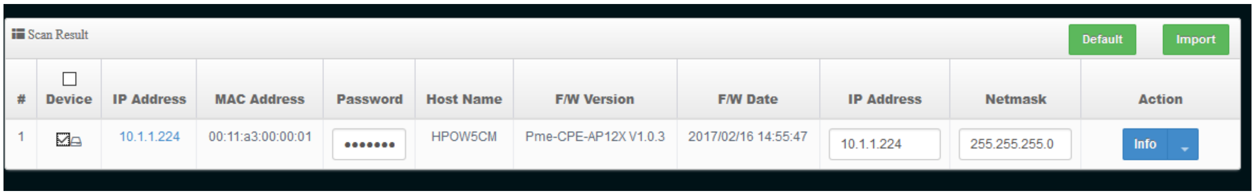
Go to AP Control and click Scan Device. Any HPOW5CMs in AP mode will be detected.



Filter Device

VLAN#	VLAN 0 (10.1.1.0/24)
Default Password	●●●●●●●
Sort	IP Address

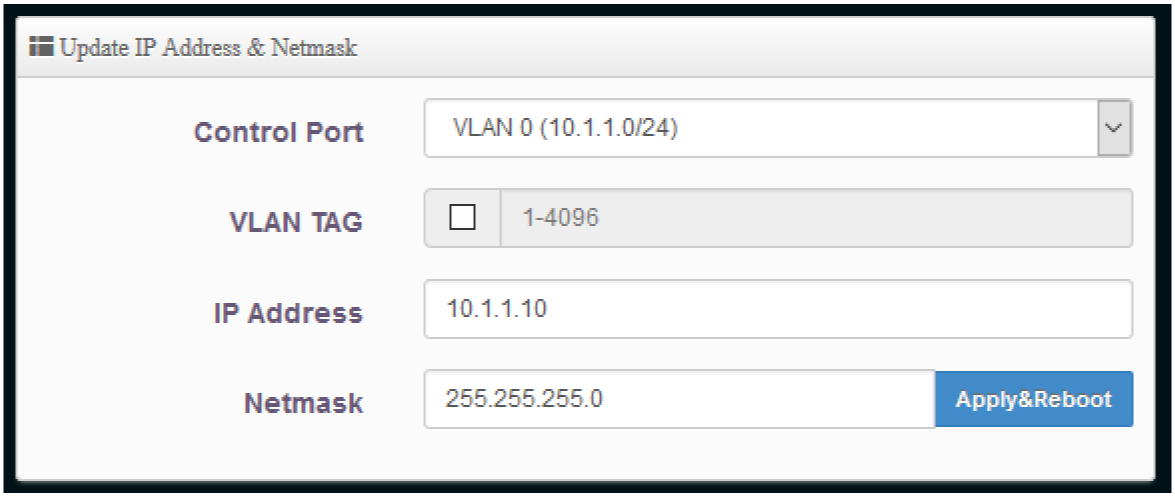
Check the device you want to import and click “Import”. This will add the AP you selected to your Controller. You can also change the IP address settings of the devices



Scan Result

#	□ Device	IP Address	MAC Address	Password	Host Name	F/W Version	F/W Date	IP Address	Netmask	Action
1	☑	10.1.1.224	00:11:a3:00:00:01	●●●●●●●	HPOW5CM	Pme-CPE-AP12X V1.0.3	2017/02/16 14:55:47	10.1.1.224	255.255.255.0	Info

Check the device and then go to the Update IP address and Netmask and make your changes. Click ‘Apply and Reboot’

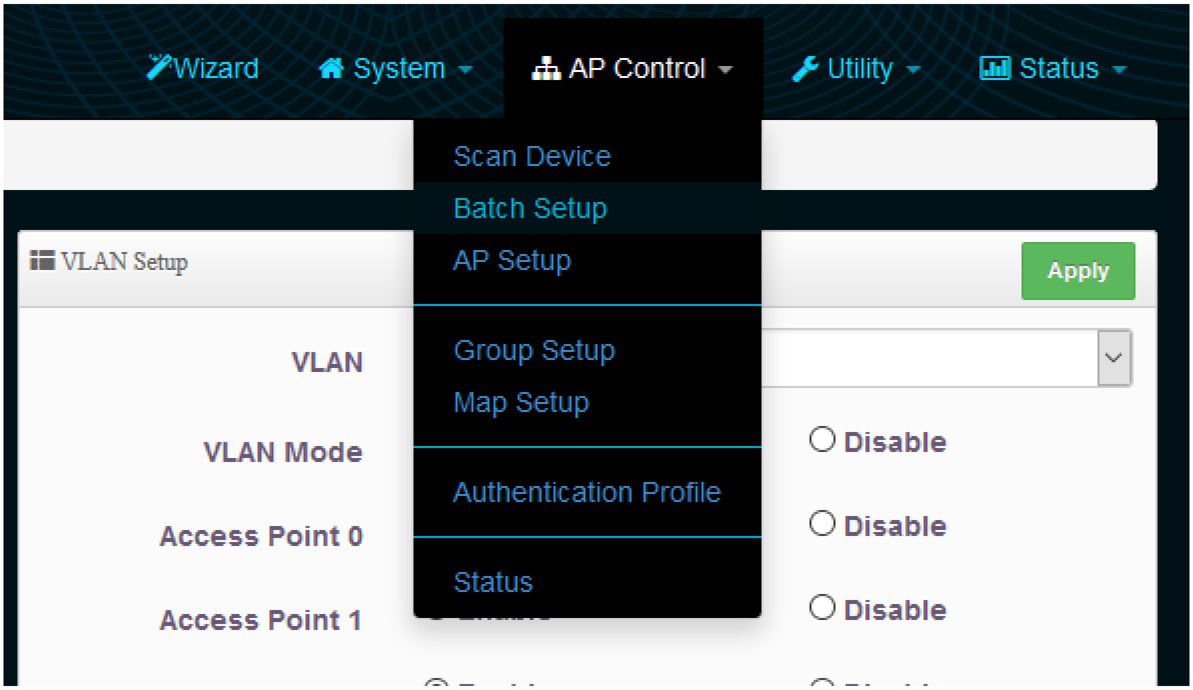


Update IP Address & Netmask

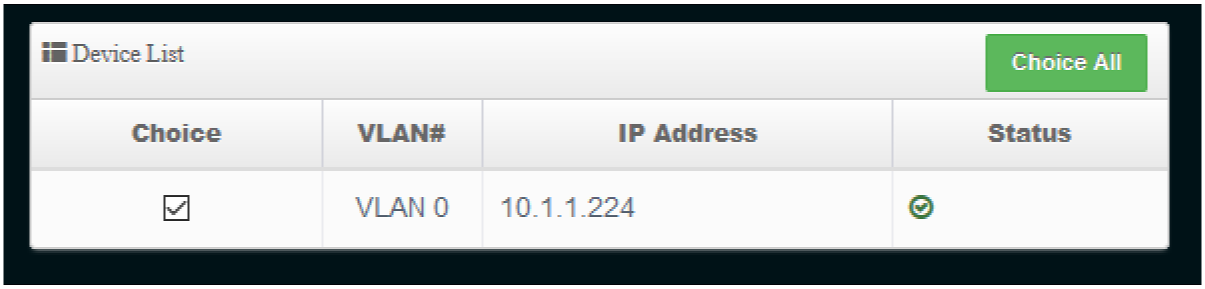
Control Port	VLAN 0 (10.1.1.0/24)
VLAN TAG	□ 1-4096
IP Address	10.1.1.10
Netmask	255.255.255.0

3-1-2-1 Batch setup

Go to AP Control-Batch Setup.



Check the devices you want to Batch Setup under "Device List"



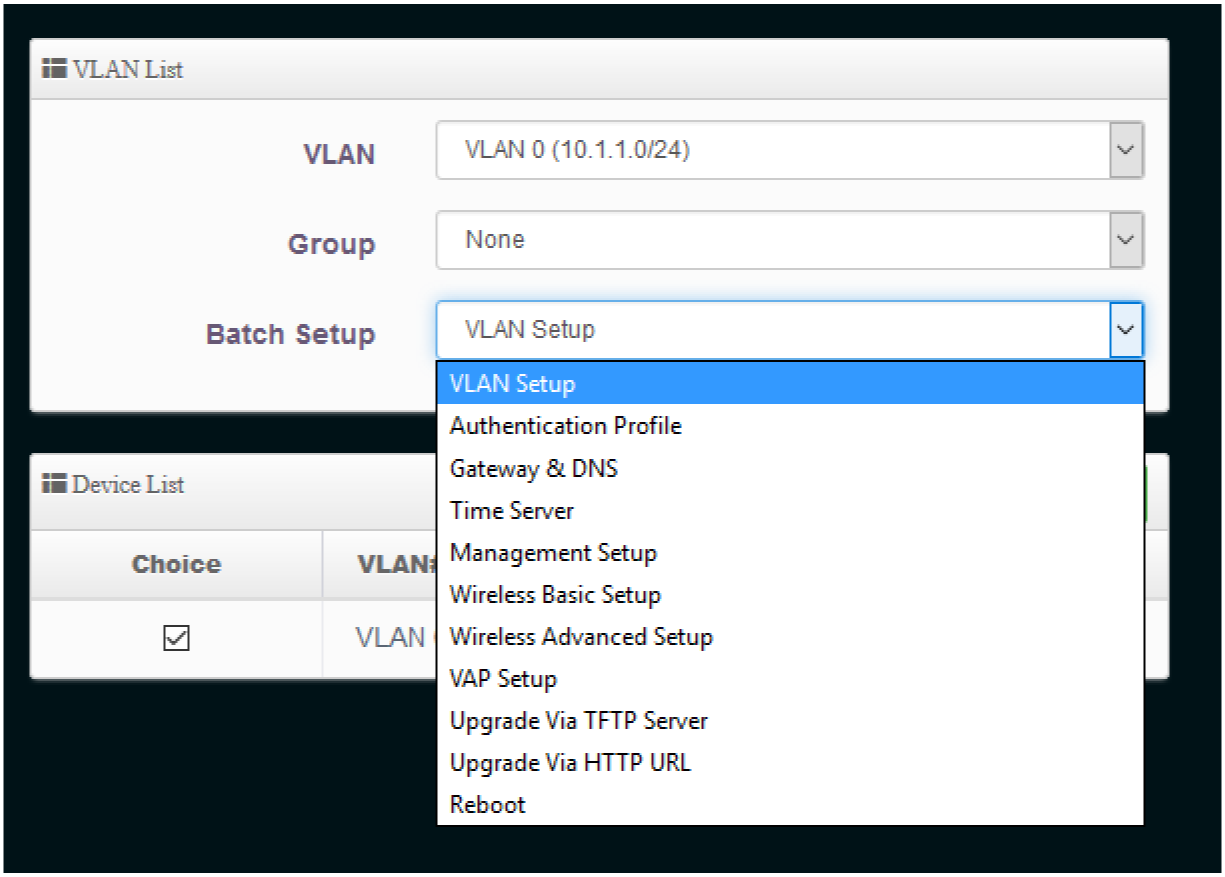
Device List

Choice All

Choice	VLAN#	IP Address	Status
☑	VLAN 0	10.1.1.224	✓

Under VLAN List, you should see options to configure VLAN, Authentication Profile, Gateway & DNS, time Server, Management, Wireless Basic Setup, Wireless Advanced Setup, VAP setup, Upgrade and

Reboot. For more information go to section 7-2



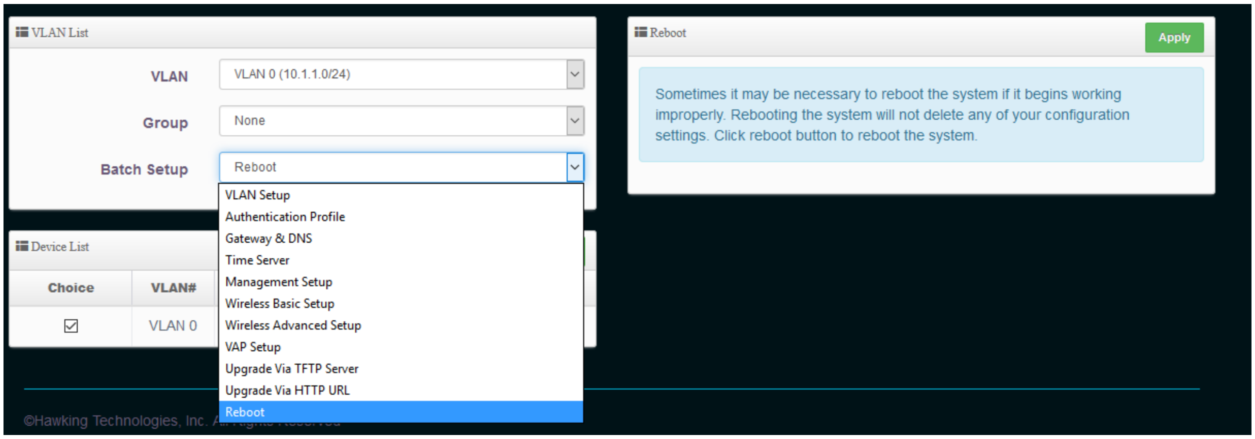
VLAN List

VLAN: VLAN 0 (10.1.1.0/24)

Group: None

Batch Setup: VLAN Setup

After you make your changes, be sure to choose “Reboot” and Apply so the changes take effect.



VLAN List

VLAN: VLAN 0 (10.1.1.0/24)

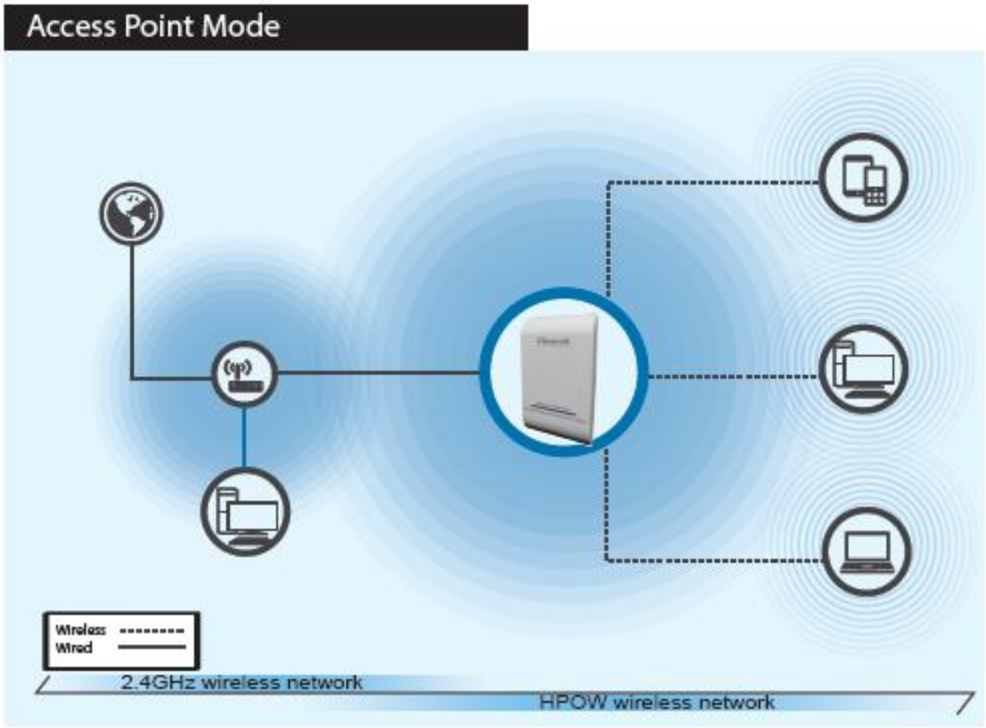
Group: None

Batch Setup: Reboot

Reboot

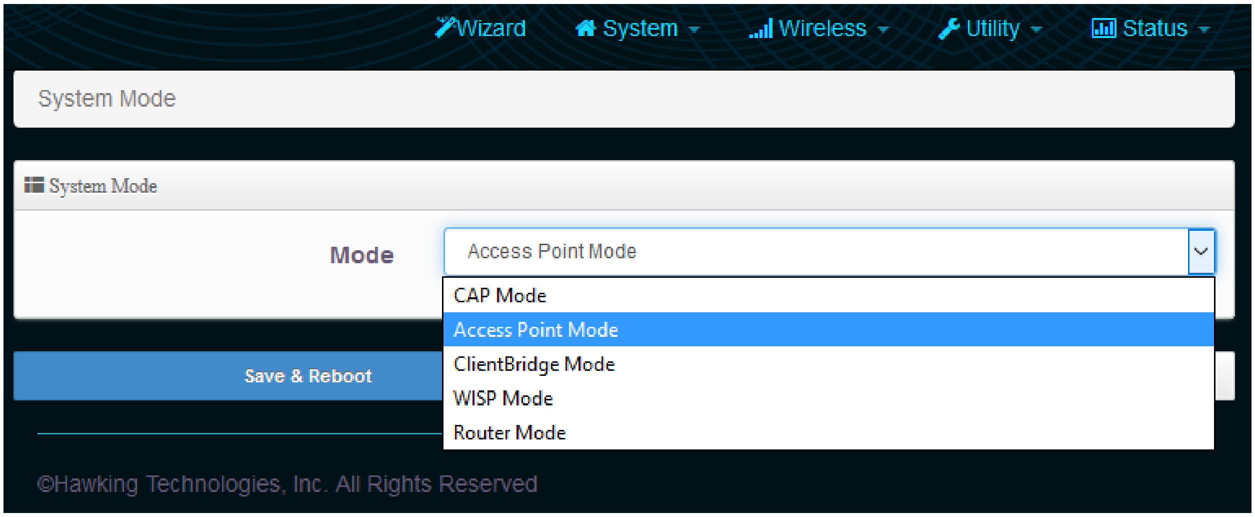
Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

3-2 AP Mode



When AP mode is chosen, the system can be configured as a standard wireless access point. In this mode, the device can be used as an Access Point for wireless client connection. All Ethernet ports wand wireless interfaces are bridged together. This section provides a detailed explanation for users on how to configure AP mode.

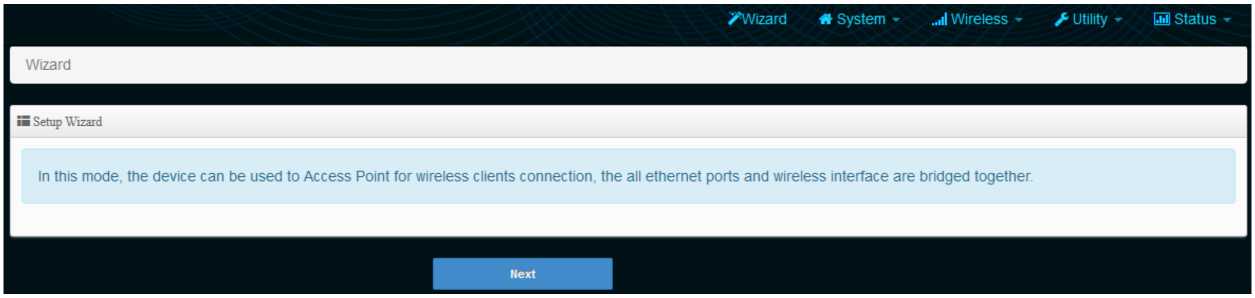
Log into the settings page, go to system and select "Operating Mode"



Mode: Access Point Mode

Choose AP Mode and click save & reboot. The device will now reboot.

Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Click on "Wizard". Click "Next"



Wizard

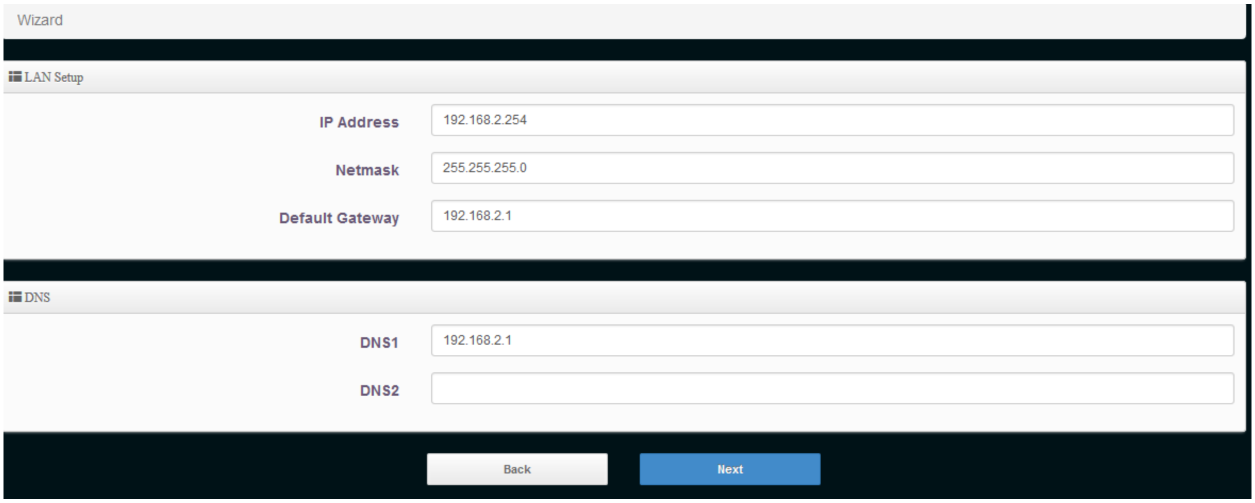
Setup Wizard

In this mode, the device can be used to Access Point for wireless clients connection, the all ethernet ports and wireless interface are bridged together.

3-2-1 LAN setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose "specify" and enter in your values.



Wizard

LAN Setup

IP Address	192.168.2.254
Netmask	255.255.255.0
Default Gateway	192.168.2.1

DNS

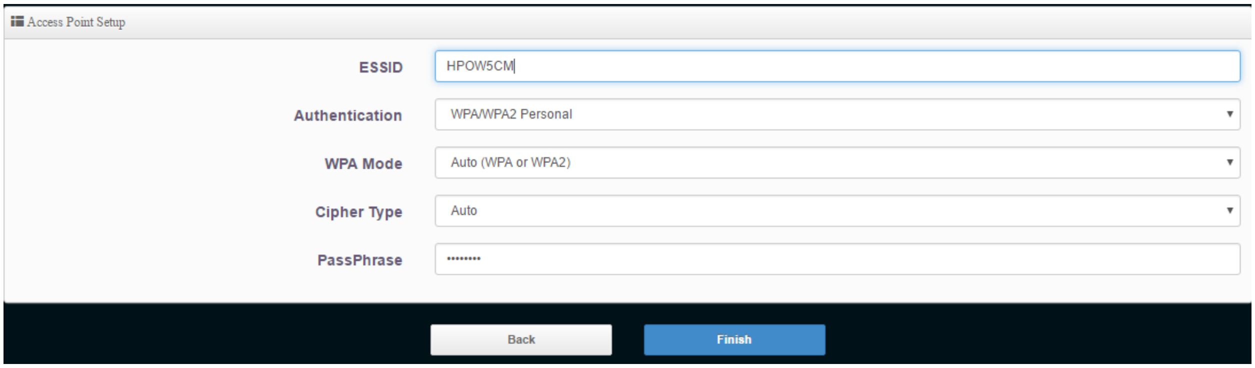
DNS1	192.168.2.1
DNS2	

3-2-2 Wireless Setup

This page is used to define the parameters for the wireless LAN clients

ESSID: *This is the wireless broadcast name. By default, it is 'Hawking_HPOW5CM' but you can change it to whatever you want.*

Authentication: *Choose your type of security (Hawking recommends AUTO (WPA or WPA-2PSK))*



Access Point Setup

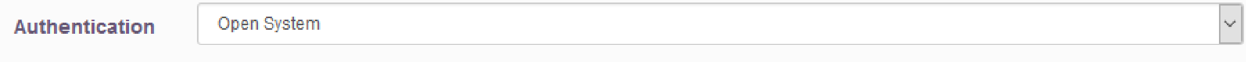
ESSID	HPOW5CM
Authentication	WPA/WPA2 Personal
WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
PassPhrase	••••••••

3-2-2-1 Authentication (Wireless Security)

This section allows you to set up wireless security to prevent any unauthorized access to your wireless network

- Open System (security disabled)

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled

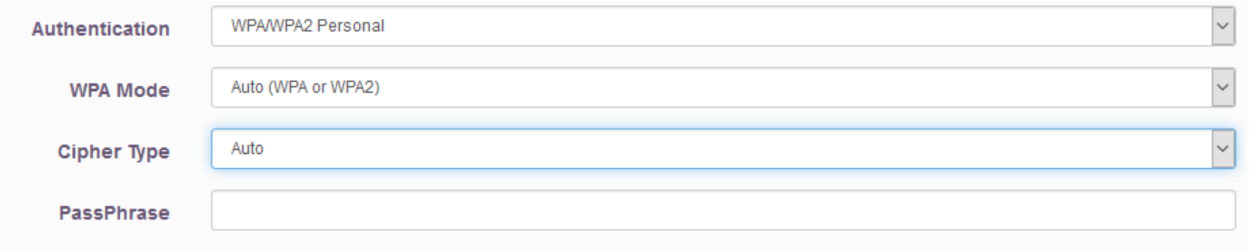


Authentication	Open System

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

- Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:



Authentication	WPA/WPA2 Personal
WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
PassPhrase	

Cipher Type: ***AES*** *is short for* ***Advanced Encryption Standard****, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.* ***TKIP*** *is short for* ***Temporal Key Integrity Protocol****, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

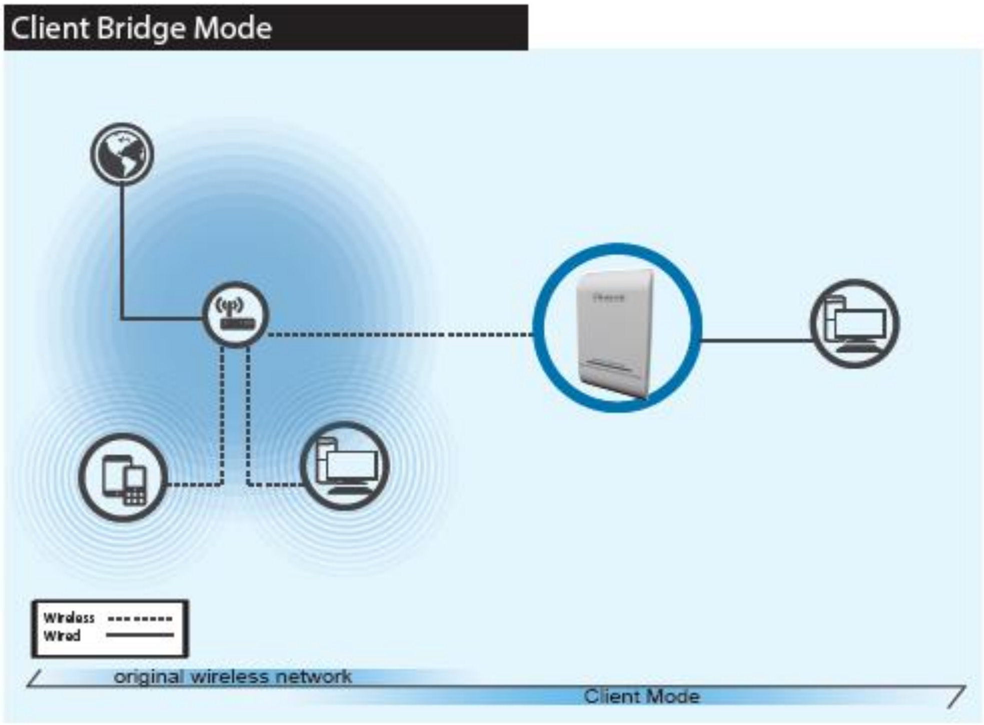
Pre-shared *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

Hawking recommends using WPA2-PSK w/ AES cipher type as your default level of security.

Click Finish and the device will automatically restart and save your settings. After you have finished, you can connect the device to your network via the 10/100 Data IN port on the PoE adapter or the LAN2 port to add this access point to your network. Please change your computer IP address back to "Obtain an IP automatically".

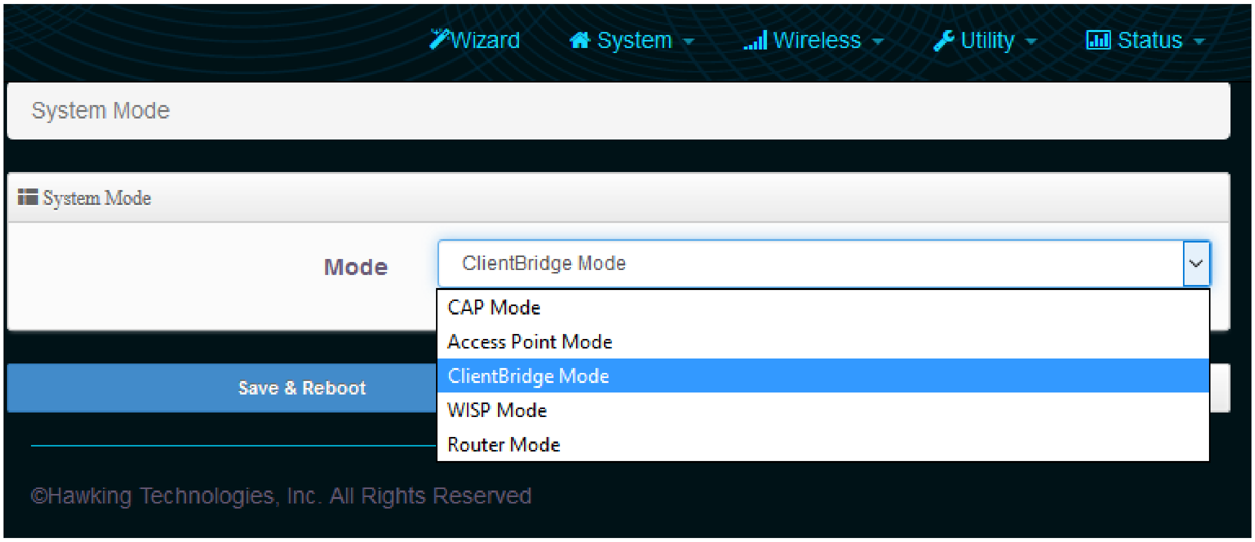
You can manually configure these settings by going to section 4-3-3

3-3 Client Bridge – Repeater Mode



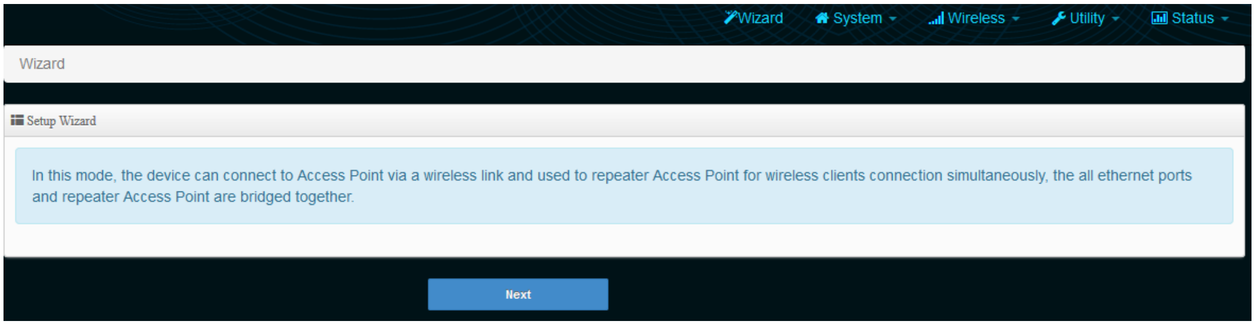
When Client Bridge + Repeater Mode is chosen, the system can be configured in bridged mode. In this mode, the device can connect to other Access Points via a wireless link and be used to bridge wired clients to the network. It can also act as a wireless repeater. All Ethernet ports and repeater access points are bridged together. This section provides a detailed explanation for users on how to configure this mode.

Log into the settings page, go to system and select "Mode Setup"



Choose ClientBridge Mode and click save & reboot. The device will now reboot.

Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Go to “Wizard”. Click “Next”

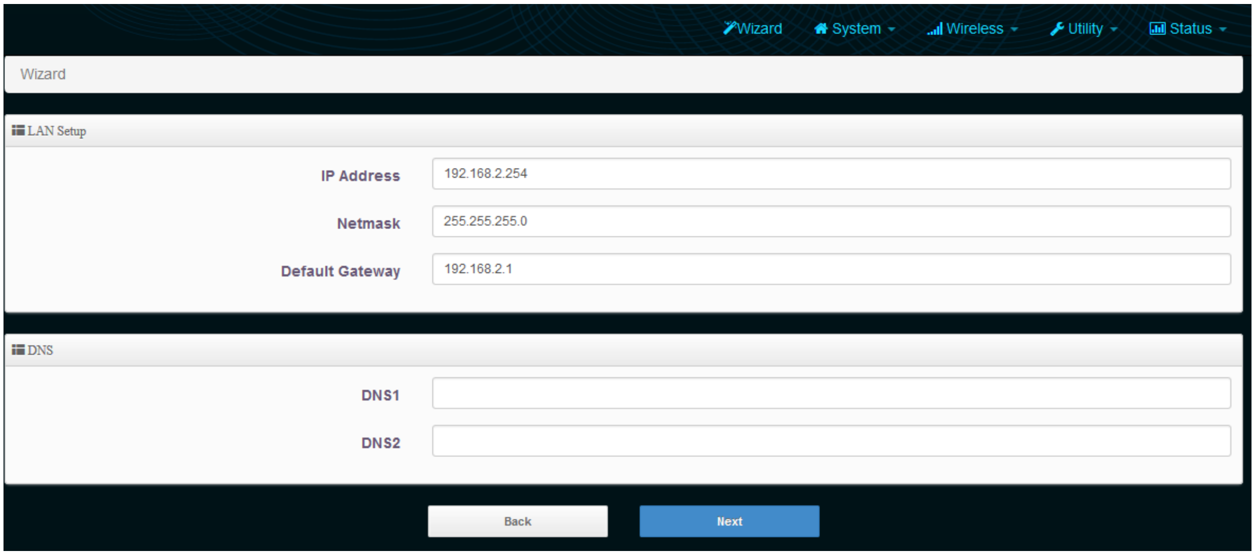


In this mode, the device can connect to Access Point via a wireless link and used to repeater Access Point for wireless clients connection simultaneously, the all ethernet ports and repeater Access Point are bridged together.

3-3-1 LAN setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose “specify” and enter in your values.



LAN Setup

IP Address: 192.168.2.254

Netmask: 255.255.255.0

Default Gateway: 192.168.2.1

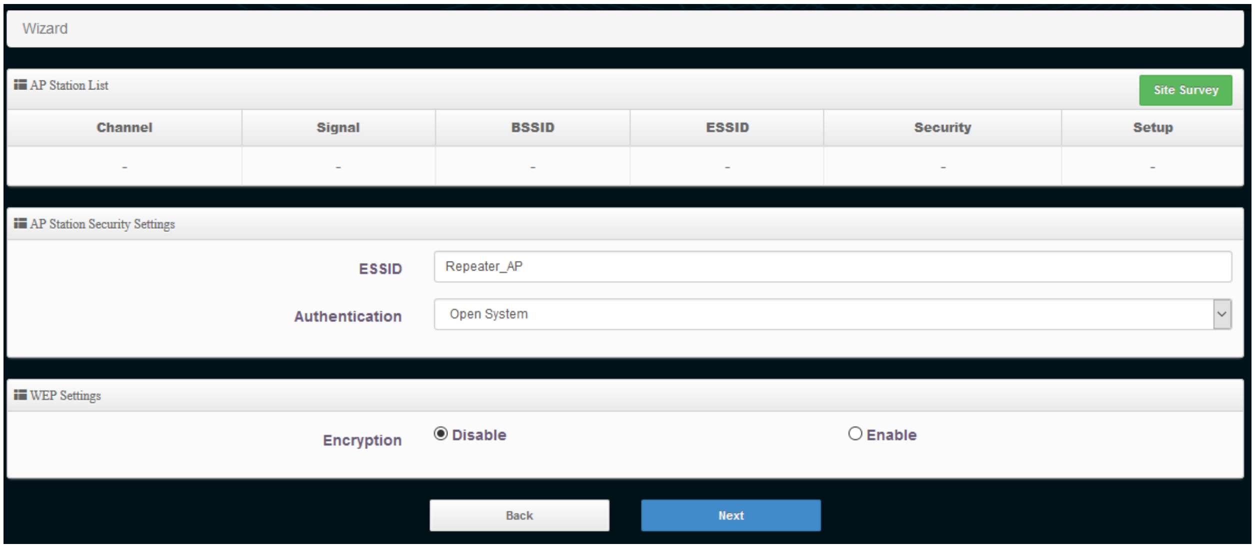
DNS

DNS1:

DNS2:

3-3-2 AP Station List Setup

This page allows you to search for an available Access Point to Connect. Click "Site Survey" for it to automatically scan for a network to connect to.



AP Station List

Channel	Signal	BSSID	ESSID	Security	Setup
-	-	-	-	-	-

AP Station Security Settings

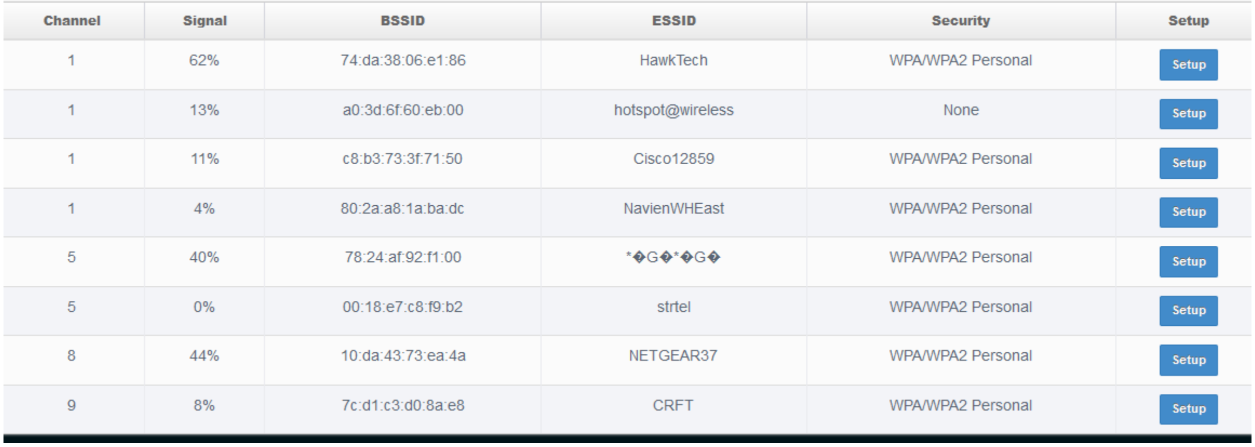
ESSID: Repeater_AP

Authentication: Open System

WEP Settings

Encryption: ● Disable ○ Enable

Site Survey: *Press this button for the device to automatically scan for wireless networks. After it scans, a list of wireless networks in the area will appear. Click "Setup" to connect to this network.*



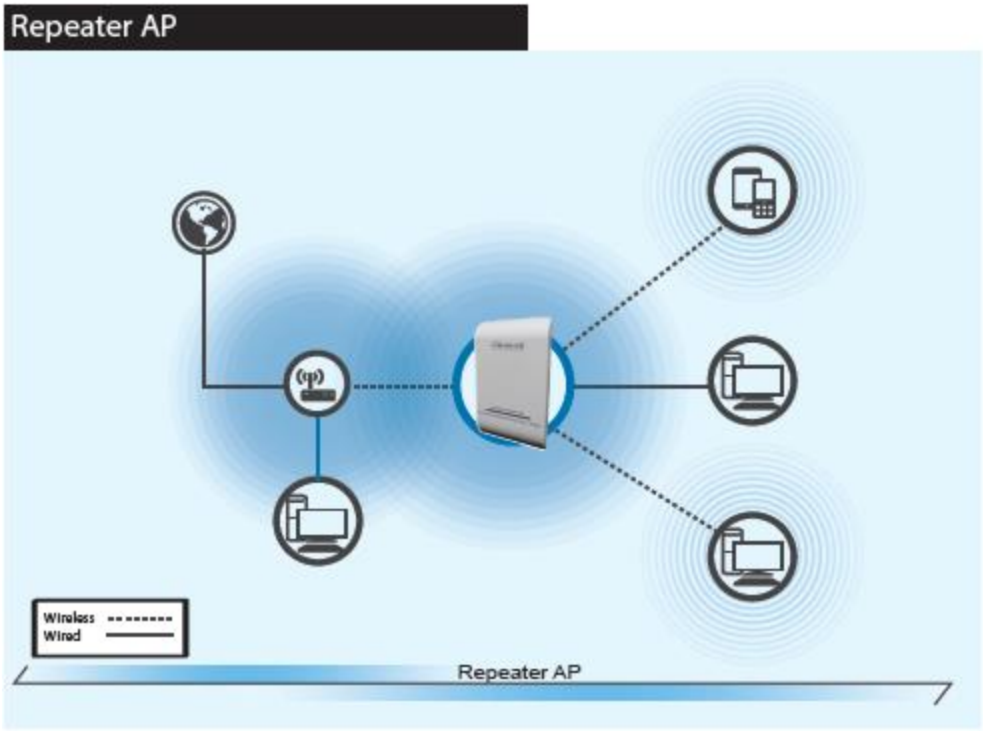
Channel	Signal	BSSID	ESSID	Security	Setup
1	62%	74:da:38:06:e1:86	HawkTech	WPA/WPA2 Personal	Setup
1	13%	a0:3d:6f:60:eb:00	hotspot@wireless	None	Setup
1	11%	c8:b3:73:3f:71:50	Cisco12859	WPA/WPA2 Personal	Setup
1	4%	80:2a:a8:1a:ba:dc	NavienWHEast	WPA/WPA2 Personal	Setup
5	40%	78:24:af:92:f1:00	*�G�*�G�	WPA/WPA2 Personal	Setup
5	0%	00:18:e7:c8:f9:b2	strtel	WPA/WPA2 Personal	Setup
8	44%	10:da:43:73:ea:4a	NETGEAR37	WPA/WPA2 Personal	Setup
9	8%	7c:d1:c3:d0:8a:e8	CRFT	WPA/WPA2 Personal	Setup

ESSID: *After you click setup, the name of the wireless network you wish to connect to will appear here. You can also manually enter the name or click on "Site Survey" for the device to scan for wireless networks.*

Authentication *After you click setup, the security type of the wireless network you wish to connect to will appear here. Type in your key to connect.*

Click Next

3-3-3 Repeater AP Setup

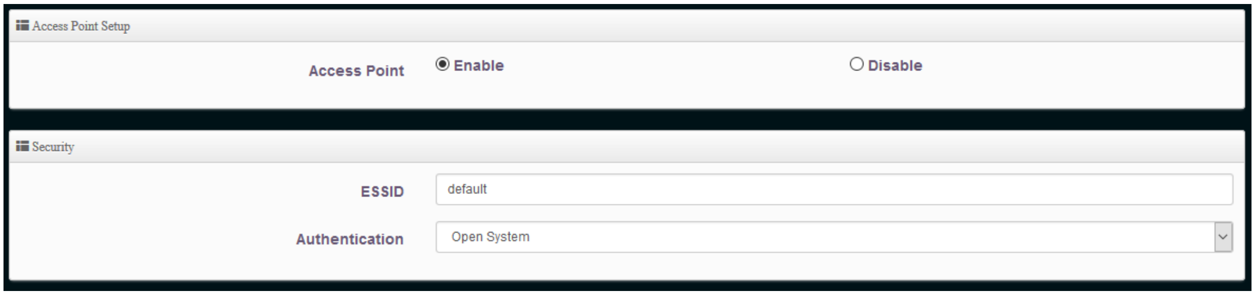


This allows you to create a repeater AP and set SSID to your wireless network. Enable this if you want the device to act as a wireless repeater. If your choose disable, the device will be configured ONLY as a client bridge. If you click enable, you can set the settings for the repeater.

This page is used to define the parameters for the wireless LAN clients

ESSID: *This is the wireless broadcast name in repeater mode. By default, it is 'Default' but you can change it to whatever you want.*

Authentication: *Choose your type of security (Hawking recommends AUTO (WPA or WPA-2PSK))*



Access Point Setup

Access Point ● Enable ○ Disable

Security

ESSID: default

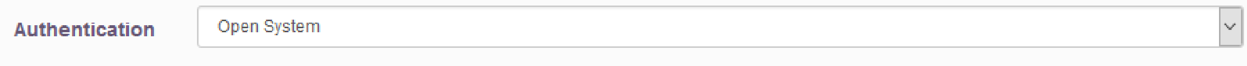
Authentication: Open System

3-3-3-1 Authentication (Wireless Security)

This section allows you to set up wireless security to prevent any unauthorized access to your wireless network

- Open System (security disabled)

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled

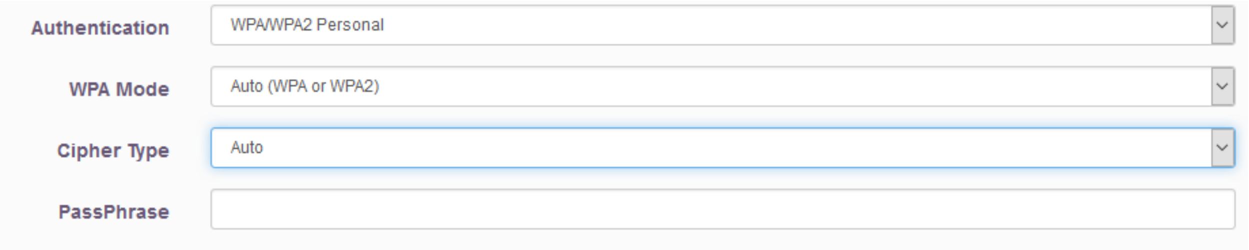


Authentication: Open System

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

- Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:



Authentication: WPA/WPA2 Personal

WPA Mode: Auto (WPA or WPA2)

Cipher Type: Auto

PassPhrase:

Cipher Type: ***AES*** *is short for* ***Advanced Encryption Standard****, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.* ***TKIP*** *is short for* ***Temporal Key Integrity Protocol****, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

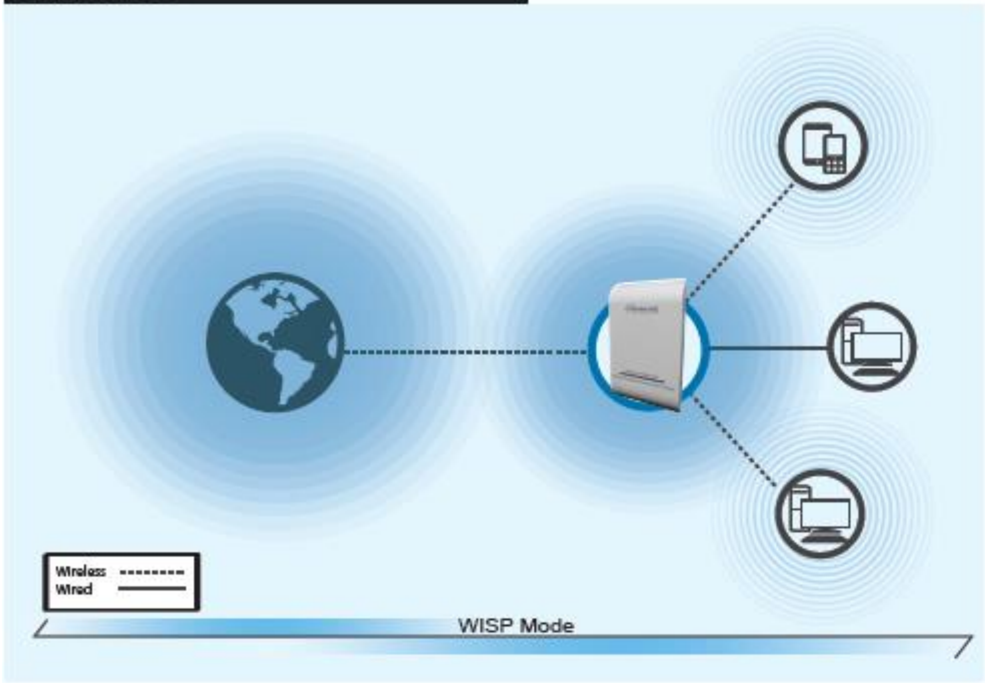
Pre-shared *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

Hawking recommends using WPA2-PSK w/ AES cipher type as your default level of security.

Click Finish and the device will automatically restart and save your settings. After you have finished, a network device must be connected to your network via the 10/100 Data In port on the PoE adapter or the LAN2 port to add this client device to your network. It should not be plugged back into the main network (should be remote). If using as a Repeater, the device just needs to be powered on via the P-Data Out port on the PoE adapter and can be standalone (you can also connect any wired client computers to the 10/100 Data In Port or LAN2). Please change your computer IP address back to "Obtain an IP automatically".

3-4 WISP Mode

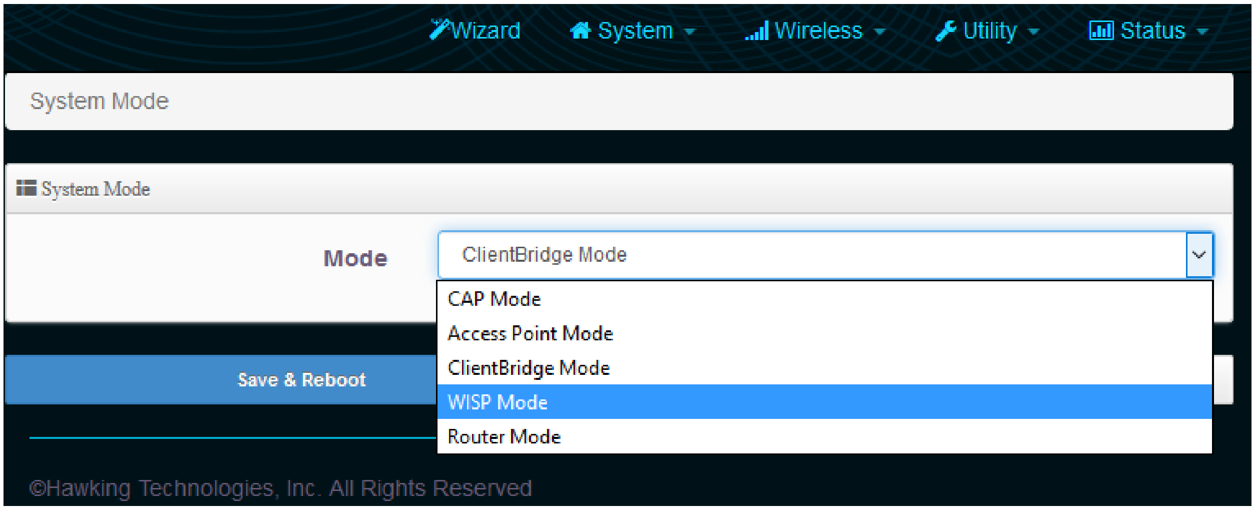
WISP Mode



When WISP Mode is chosen, the system can be configured in Wireless Internet repeater mode. In this mode, the device can wirelessly connect to a WISP (wireless internet service provider), ie. Another wireless AP, HotSpot, etc. It can then wirelessly repeat the signal and can even act as a router for these signals. NAT is enabled and wired and wireless computers can share the same IP range. This section provides a detailed explanation for users on how to configure this mode.

Choose WISP Mode

Log into the settings page, go to system and select "Mode Setup"



System Mode

System Mode

Mode: ClientBridge Mode

- CAP Mode
- Access Point Mode
- ClientBridge Mode
- WISP Mode
- Router Mode

©Hawking Technologies, Inc. All Rights Reserved

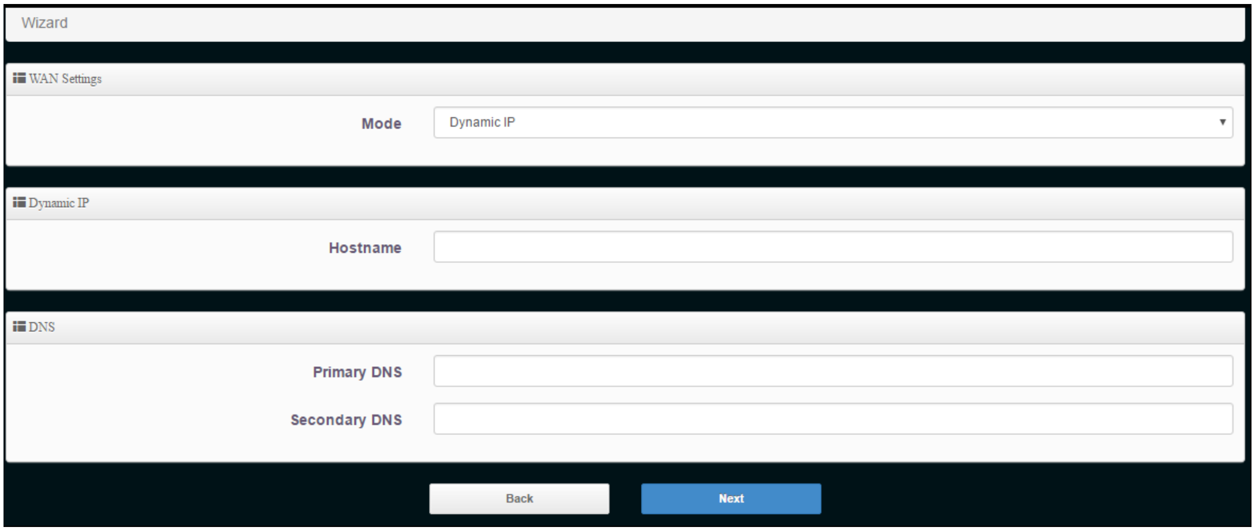
Choose WISP Mode and click save & reboot.

Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Go to "Wizard". Click "Next"

3-4-1 WAN Settings and DNS Setings

Choose your mode. Most ISPs use “Dynamic IP”. If you are unsure, please contact your ISP. Refer to Section 4-1 for a more in-depth explanation of these settings. Enter your hostname settings if you have one. You may leave it blank if it is not required.

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose “specify” and enter in your values.



Wizard

WAN Settings

Mode: Dynamic IP

Dynamic IP

Hostname:

DNS

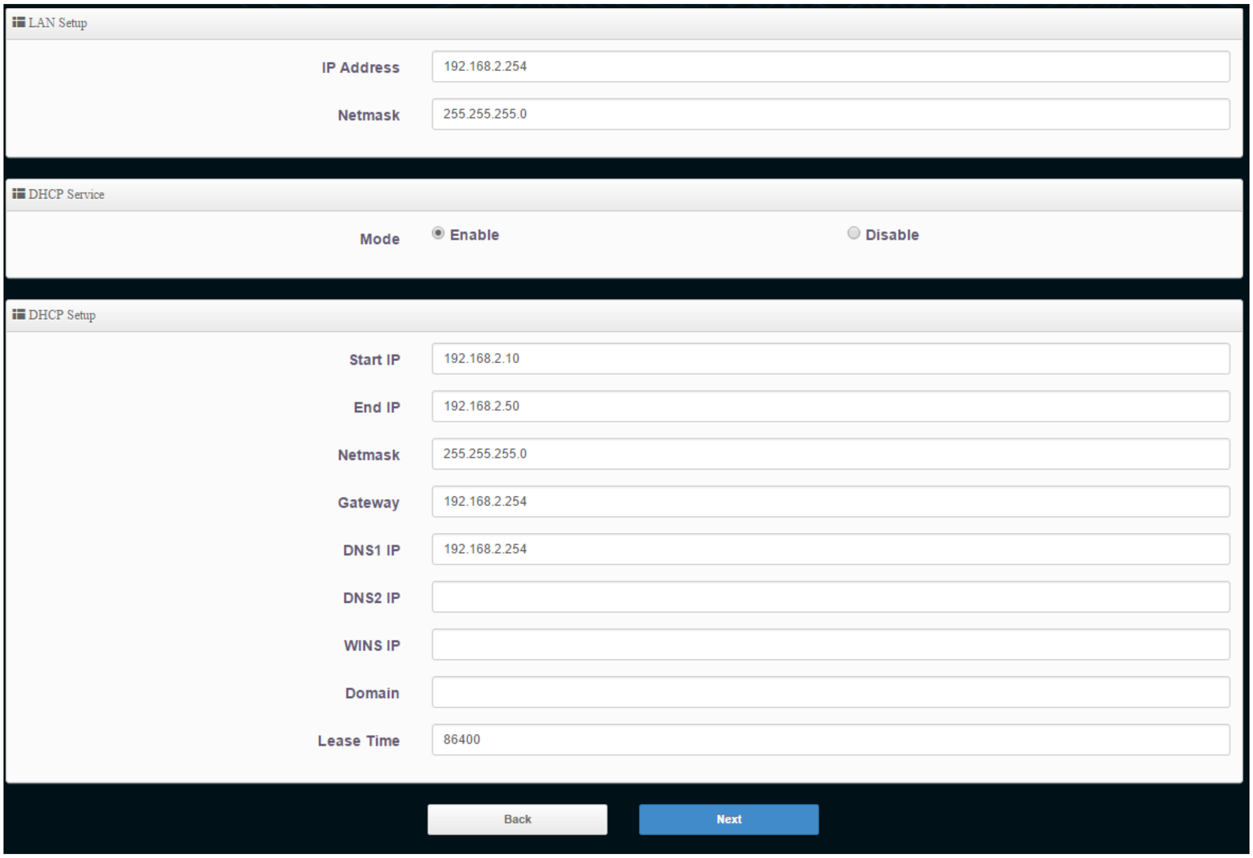
Primary DNS:

Secondary DNS:

3-4-2 LAN setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254

In router mode, by default, IP addresses will be assigned to any LAN/WLAN clients that are connected to the device. You can disable this feature. By default, DHCP is enabled and the IP range is 192.168.2.10 – 192.168.2.70



LAN Setup

IP Address	192.168.2.254
Netmask	255.255.255.0

DHCP Service

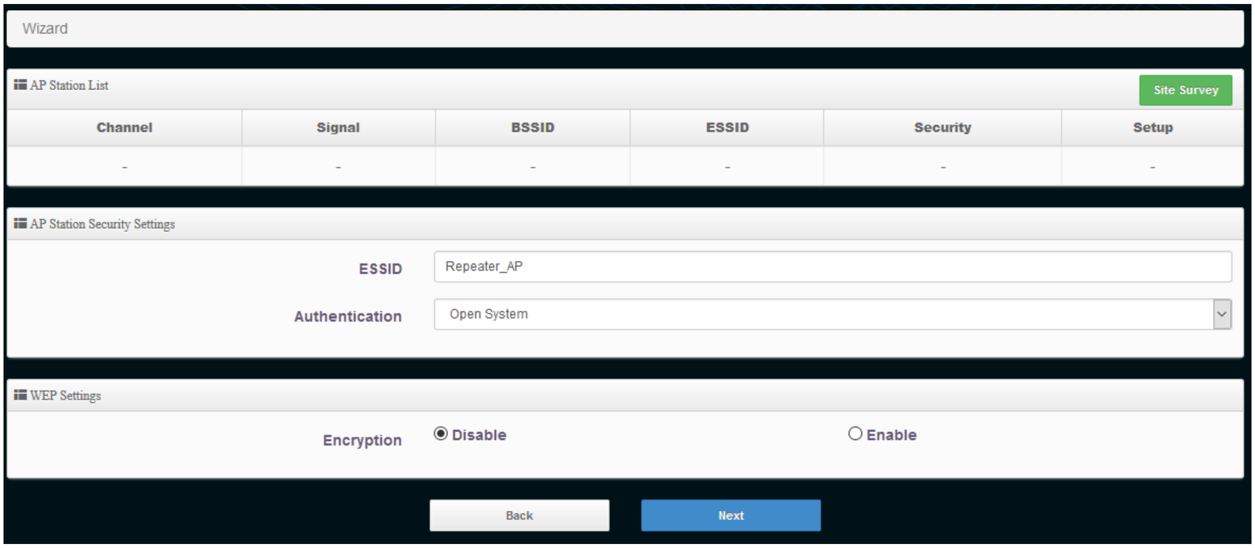
Mode ● Enable ○ Disable

DHCP Setup

Start IP	192.168.2.10
End IP	192.168.2.50
Netmask	255.255.255.0
Gateway	192.168.2.254
DNS1 IP	192.168.2.254
DNS2 IP	
WINS IP	
Domain	
Lease Time	86400

3-4-3 AP Station List Setup

This page allows you to search for an available Access Point to Connect. Click “Site Survey” for it to automatically scan for a network to connect to.



Wizard

AP Station List

Channel	Signal	BSSID	ESSID	Security	Setup
-	-	-	-	-	-

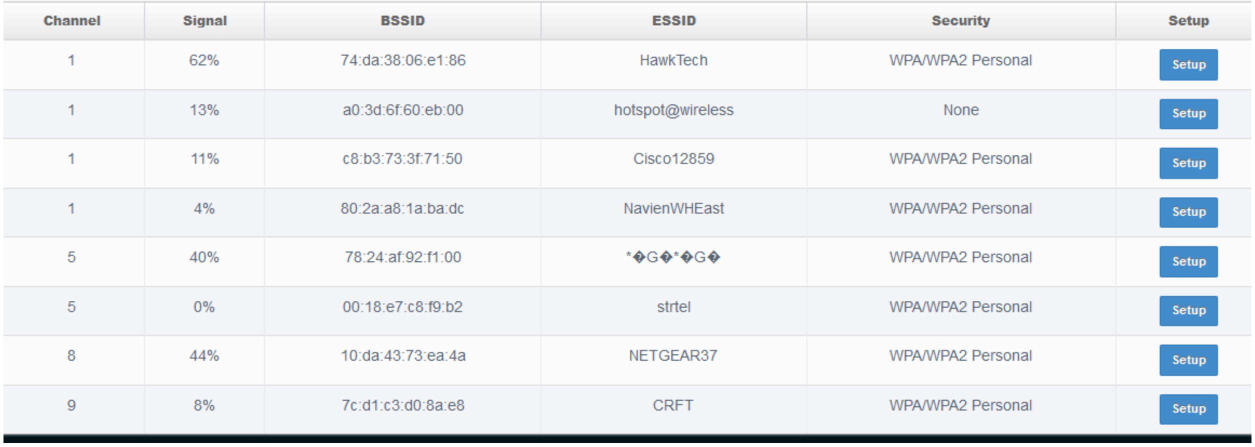
AP Station Security Settings

ESSID	Repeater_AP
Authentication	Open System

WEP Settings

Encryption ● Disable ○ Enable

Site Survey: *Press this button for the device to automatically scan for wireless networks. After it scans, a list of wireless networks in the area will appear. Click "Setup" to connect to this network.*



Channel	Signal	BSSID	ESSID	Security	Setup
1	62%	74:da:38:06:e1:86	HawkTech	WPA/WPA2 Personal	Setup
1	13%	a0:3d:6f:60:eb:00	hotspot@wireless	None	Setup
1	11%	c8:b3:73:3f:71:50	Cisco12859	WPA/WPA2 Personal	Setup
1	4%	80:2a:a8:1a:ba:dc	NavienWHEast	WPA/WPA2 Personal	Setup
5	40%	78:24:af:92:f1:00	*�G�*�G�	WPA/WPA2 Personal	Setup
5	0%	00:18:e7:c8:f9:b2	strtel	WPA/WPA2 Personal	Setup
8	44%	10:da:43:73:ea:4a	NETGEAR37	WPA/WPA2 Personal	Setup
9	8%	7c:d1:c3:d0:8a:e8	CRFT	WPA/WPA2 Personal	Setup

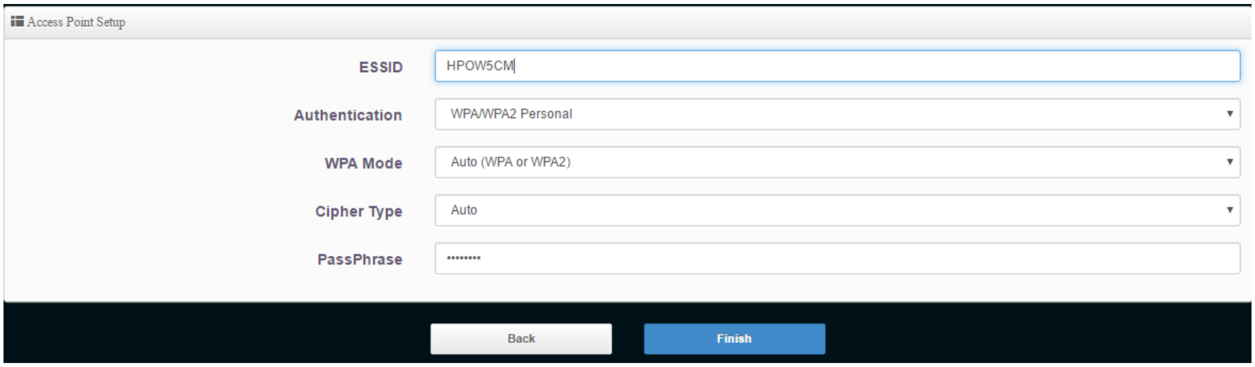
ESSID: *After you click setup, the name of the wireless network you wish to connect to will appear here. You can also manually enter the name or click on "Site Survey" for the device to scan for wireless networks.*

Authentication *After you click setup, the security type of the wireless network you wish to connect to will appear here. Type in your key to connect.*

Click Next

3-4-4 Repeater AP Setup

This allows you to create a repeater AP and set SSID to your wireless network.



Access Point Setup

ESSID: HPOW5CM

Authentication: WPA/WPA2 Personal

WPA Mode: Auto (WPA or WPA2)

Cipher Type: Auto

PassPhrase: ••••••••

This page is used to define the parameters for the wireless LAN clients

ESSID: *This is the wireless broadcast name. By default, it is 'Hawking_HPOW5CM' but you can change it to whatever you want.*

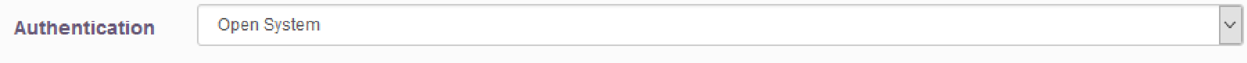
Authentication: *Choose your type of security (Hawking recommends AUTO (WPA or WPA-2PSK))*

3-4-4-1 Authentication (Wireless Security)

This section allows you to set up wireless security to prevent any unauthorized access to your wireless network

- Open System (security disabled)

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled

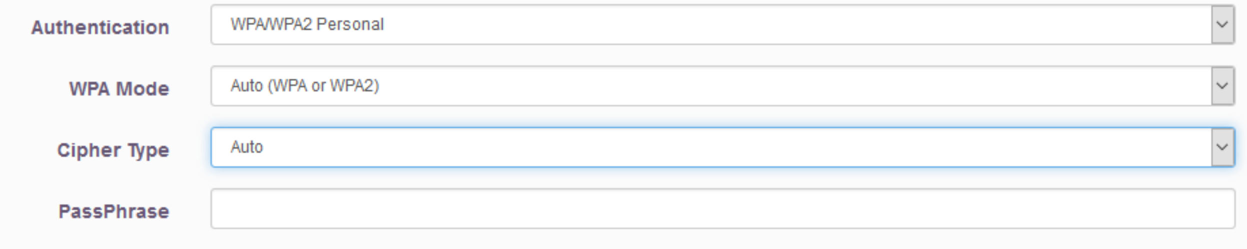


Authentication: Open System

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

- Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:



Authentication: WPA/WPA2 Personal

WPA Mode: Auto (WPA or WPA2)

Cipher Type: Auto

PassPhrase:

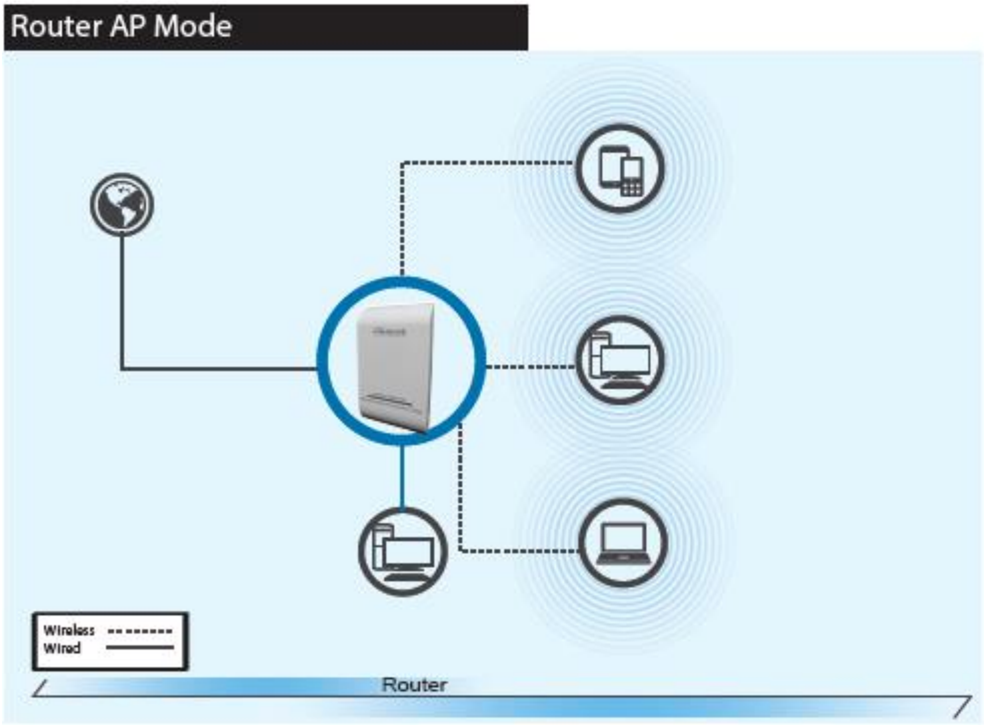
Cipher Type: *__AES__ is short for __Advanced Encryption Standard__, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key. __TKIP__ is short for __Temporal Key Integrity Protocol__, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

Pre-shared *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

Hawking recommends using WPA2-PSK w/ AES cipher type as your default level of security.

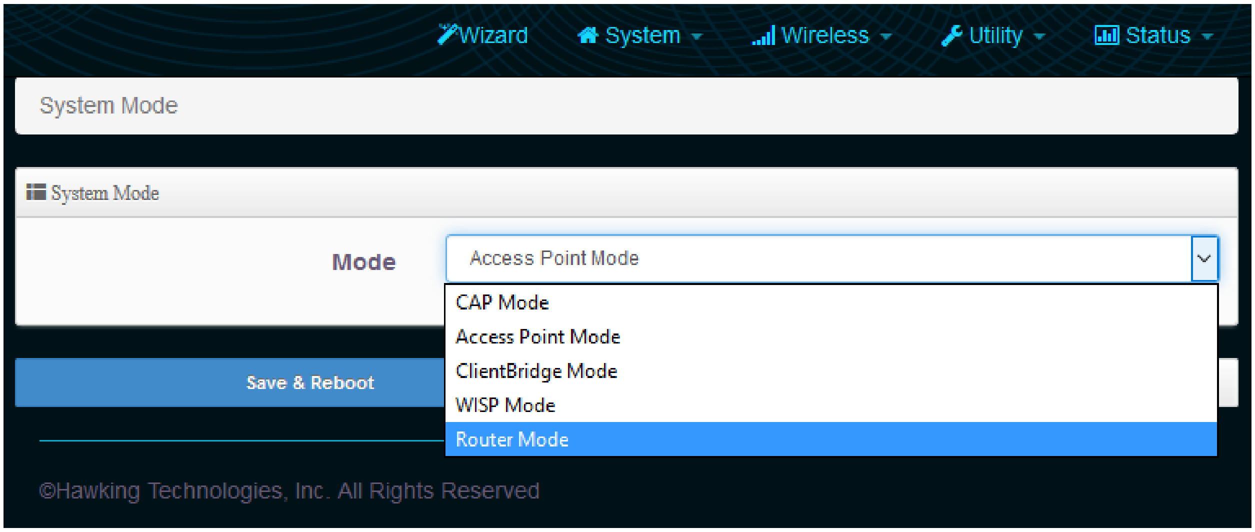
Click Finish and the device will automatically restart and save your settings. After you have finished, this device will act as a Wireless Internet Service Provider. The device just needs be powered on via the P-Data Out port on the PoE adapter and can be standalone (you can also connect any wired clients to the 10/100 Data in Port on LAN2). Please change your computer IP address back to "Obtain an IP automatically.

3-5 Router Mode



When Router mode is chosen, the system can be configured as a Wireless Router. In this mode, the device is supposed to be connected to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN/WLAN port share the same IP to ISP through the WAN port. The connection type can be setup in WAN page by using static IP, Dynamic IP, PPPoE or PPTP client. This section provides a detailed explanation for users on how to configure Router AP mode.

Log into the settings page, go to system and select "Mode Setup"



System Mode

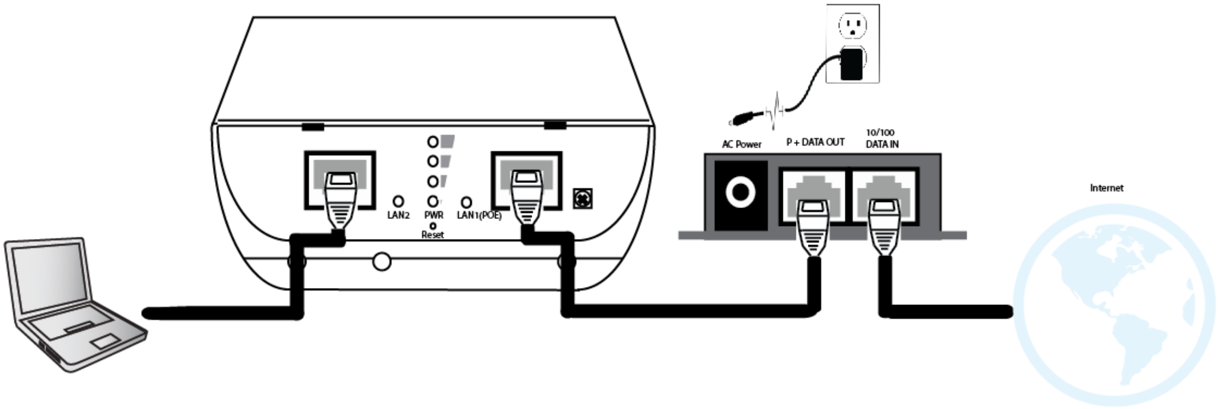
System Mode

Mode: Access Point Mode

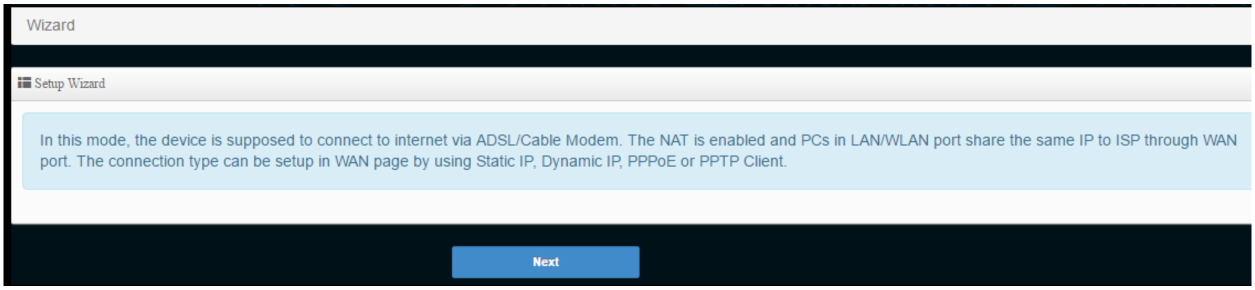
©Hawking Technologies, Inc. All Rights Reserved

Choose Router Mode and click save & reboot. The device will now reboot. After the device has finished rebooting, you will have to make changes to your computer's physical connection. See below.

The physical setup is slightly different than the standard setup. Plug your computer into LAN2 on the access point. Plug your ISP's modem into the PoE '10/100 data in' port.



Now, open your browser and go to 192.168.2.254. It should take you back into the settings page. Go to system and select "Setup Wizard". Click "Next"



Wizard

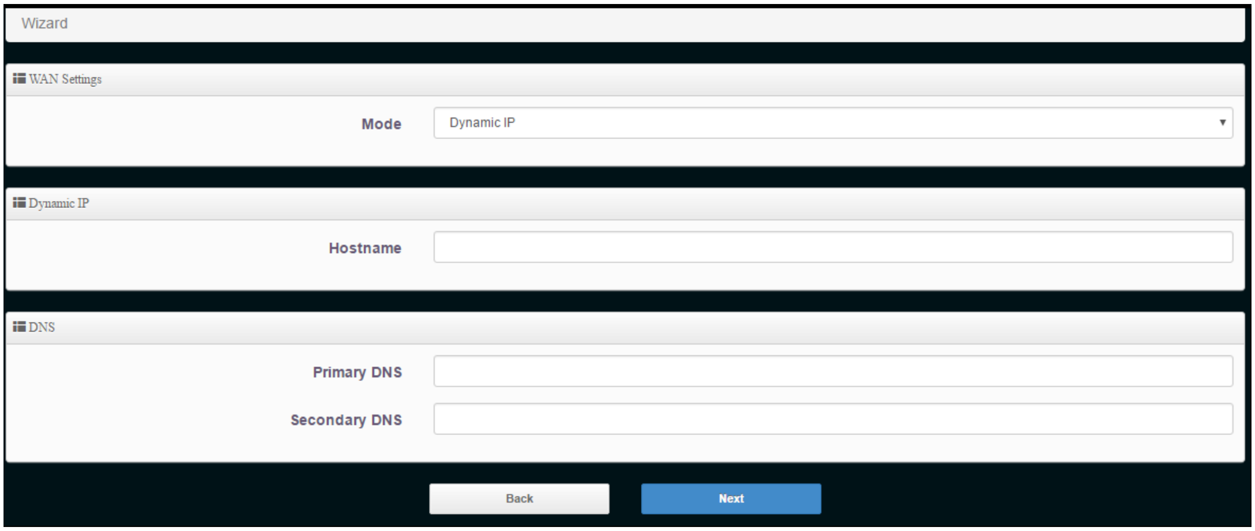
Setup Wizard

In this mode, the device is supposed to connect to internet via ADSL/Cable Modem. The NAT is enabled and PCs in LAN/WLAN port share the same IP to ISP through WAN port. The connection type can be setup in WAN page by using Static IP, Dynamic IP, PPPoE or PPTP Client.

3-5-1 WAN Settings and DNS Settings

Choose your mode. Most ISPs use "Dynamic IP". If you are unsure, please contact your ISP. Refer to Section 4-1 for a more in-depth explanation of these settings. Enter your hostname settings if you have one. You may leave it blank if it is not required.

Choose your DNS type. By default, it will be received automatically but if you have a preferred DNS or you have to specify one, please choose "specify" and enter in your values.



Wizard

WAN Settings

Mode: Dynamic IP

Dynamic IP

Hostname

DNS

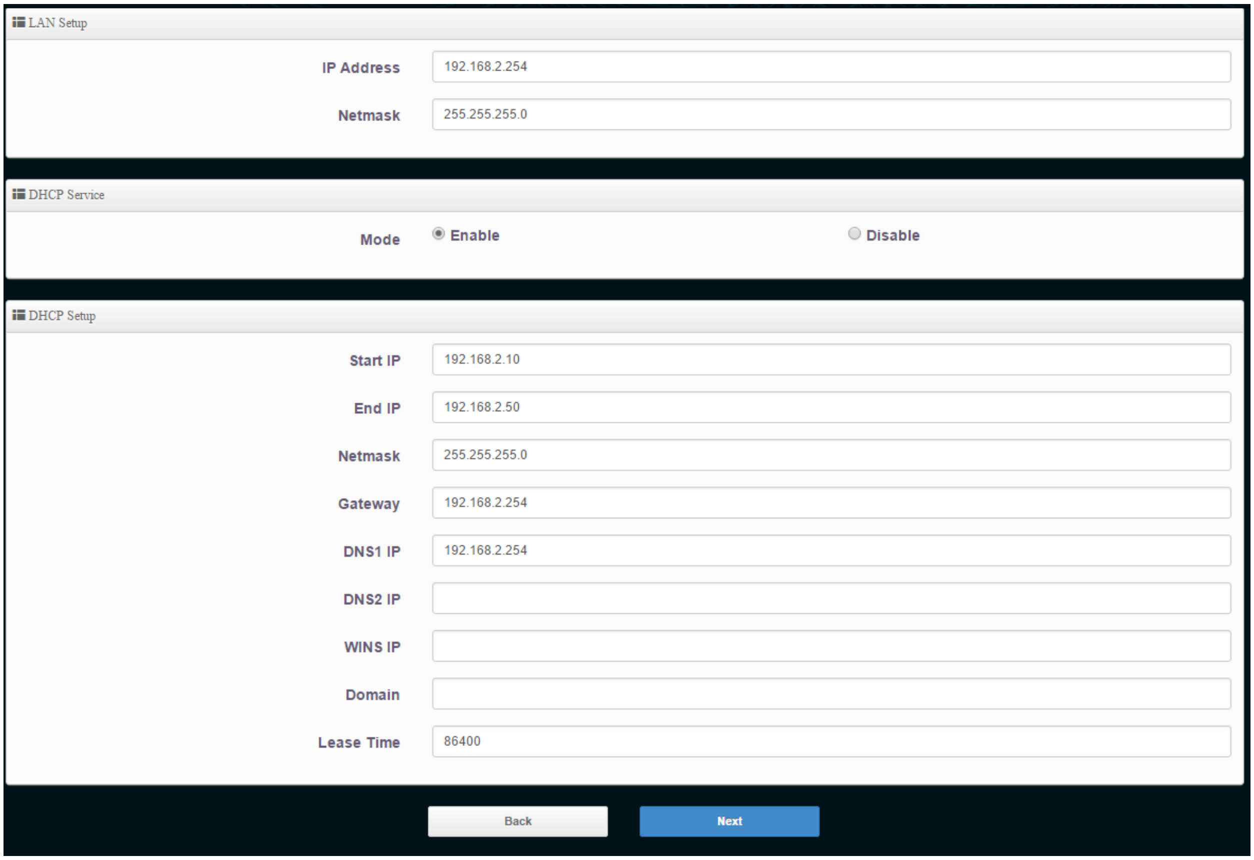
Primary DNS

Secondary DNS

3-5-2 LAN setup

You can change the default IP of the device here if required. By default, the IP is 192.168.2.254

In router mode, by default, IP addresses will be assigned to any LAN/WLAN clients that are connected to the device. You can disable this feature. By default, DHCP is enabled and the IP range is 192.168.2.10 – 192.168.2.70



LAN Setup

IP Address	192.168.2.254
Netmask	255.255.255.0

DHCP Service

Mode	● Enable	○ Disable

DHCP Setup

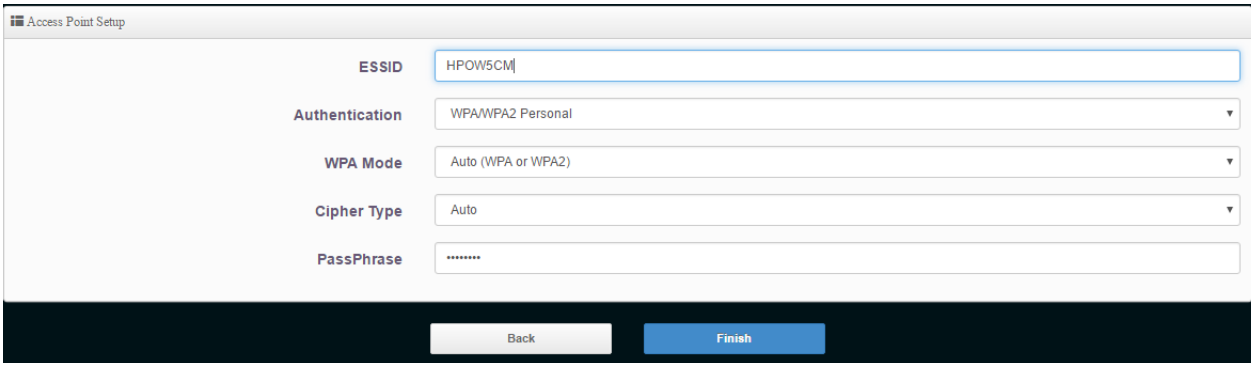
Start IP	192.168.2.10
End IP	192.168.2.50
Netmask	255.255.255.0
Gateway	192.168.2.254
DNS1 IP	192.168.2.254
DNS2 IP	
WINS IP	
Domain	
Lease Time	86400

3-5-3 Wireless Setup

This page is used to define the parameters for the wireless LAN clients

ESSID: *This is the wireless broadcast name. By default, it is 'Hawking_HPOW5CM' but you can change it to whatever you want.*

Authentication *Choose your type of security (Hawking recommends AUTO (WPA or WPA-2PSK))*



Access Point Setup

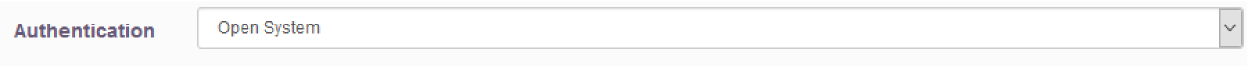
ESSID	HPOW5CM
Authentication	WPA/WPA2 Personal
WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
PassPhrase	••••••••

3-5-3-1 Authentication (Wireless Security)

This section allows you to set up wireless security to prevent any unauthorized access to your wireless network

- Open System (security disabled)

When you select this mode, data encryption is disabled, and every wireless device in proximity will be able to connect your wireless access point if no other security measure is enabled

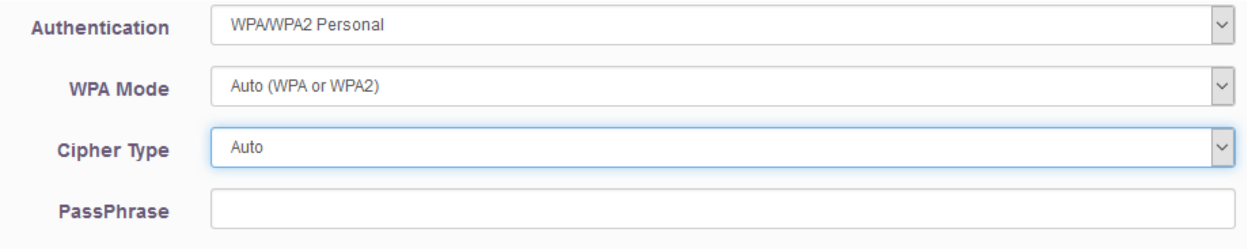


Authentication: Open System

Use this option only when you want to allow any user to use your wireless access point, and you are not concerned about unauthorized access to your files and/or transfers over your network.

- Wi-Fi Protected Access (WPA-PSK or WPA2-PSK):

When you select this mode, the wireless access point will use WPA encryption, and the following setup menu will be shown on your web browser:



Authentication: WPA/WPA2 Personal

WPA Mode: Auto (WPA or WPA2)

Cipher Type: Auto

PassPhrase:

Cipher Type: ***AES*** *is short for* ***Advanced Encryption Standard****, The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plain text into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.* ***TKIP*** *is short for* ***Temporal Key Integrity Protocol****, TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.*

Pre-shared *Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters*

Hawking recommends using WPA2-PSK w/ AES cipher type as your default level of security.

Click Finish and the device will automatically restart and save your settings. After you have finished, you can connect the device to your network via LAN2 to use this as a Router AP. You can add a network switch to LAN2 if you need more Ethernet ports. Please change your computer IP address back to "Obtain an IP automatically".

Settings can be modified via the VLAN setup after configuration is complete. See section 4-3.

Chapter IV: System Settings

Under this heading, several settings can be changed to configure this device

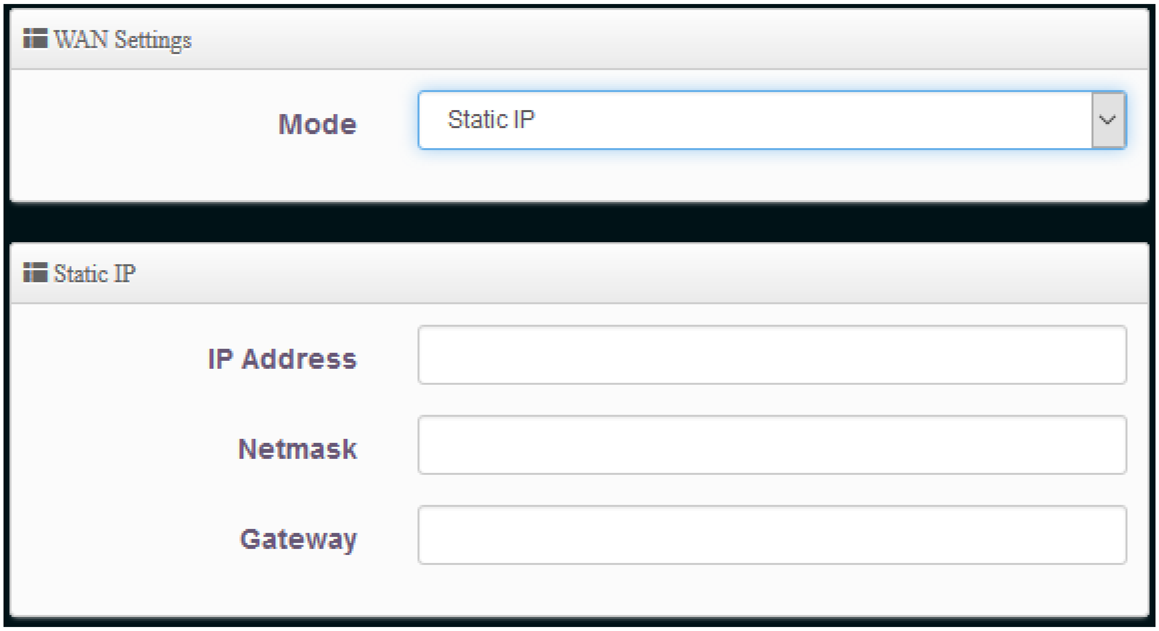
4-1 WAN Setup

Click under system, WAN setup. (This feature is only available under Router and WISP mode)

4-1-1 Internet Connection Type: Static IP

Static IP users can manually setup the WAN IP w/ a static IP provided by the Internet Service Provider (ISP).

IP Address, IP Netmask (subnet mask), IP Gateway are all provided by the ISP. Contact them if you are not sure.



WAN Settings

Mode: Static IP

Static IP

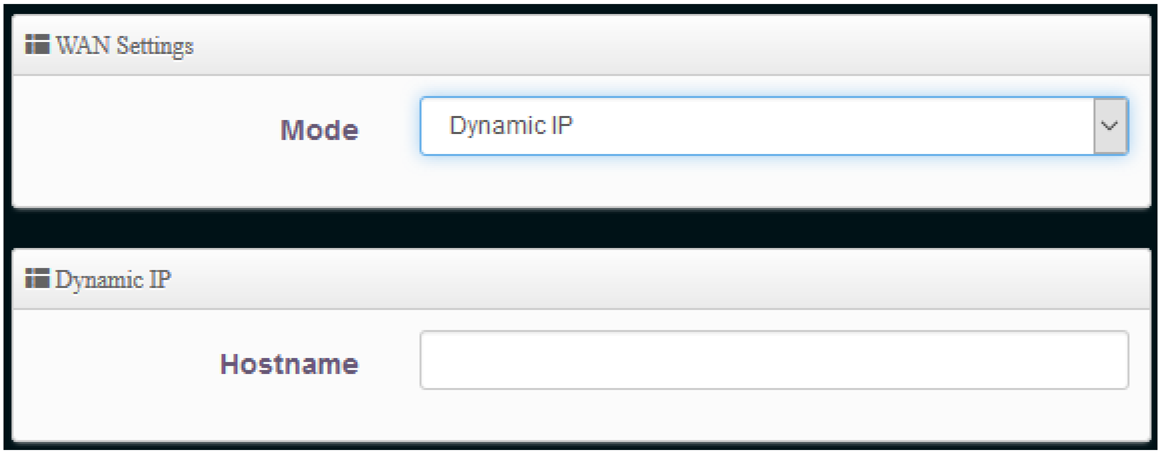
IP Address:

Netmask:

Gateway:

4-1-2 Internet Connection Type: Dynamic IP (Default)

Dynamic IP users receive all their IP, Subnet, Gateway and DNS settings from their ISP. This is the most common setting used.



WAN Settings

Mode: Dynamic IP

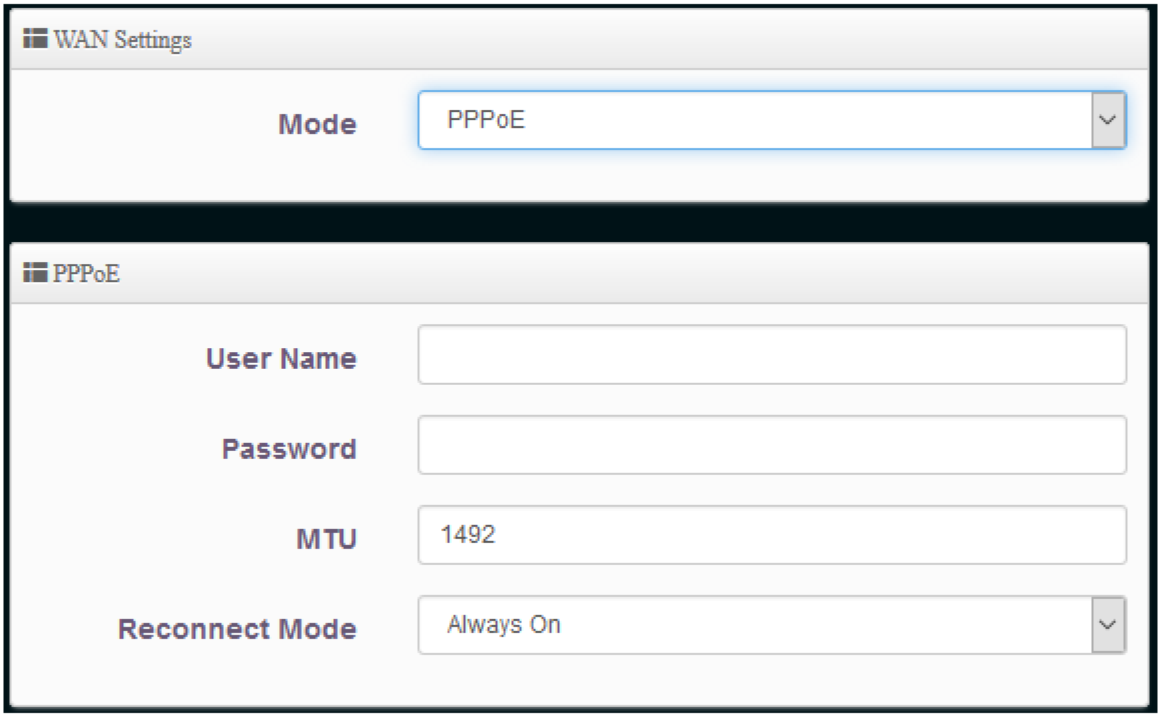
Dynamic IP

Hostname:

Hostname: *(optional). If your ISP uses dynamic IP addresses, you may need to enter a hostname provided by the ISP.*

4-1-3 Internet Connection Type: PPPoE

PPPoE users need to manually enter their ISP provided username/password. Please contact them if you are not sure.



WAN Settings

Mode: PPPoE

PPPoE

User Name:

Password:

MTU: 1492

Reconnect Mode: Always On

Username: *Enter user name for PPPoE connection*

Password: *Enter user name for PPPoE connection.*

MTU: *By default, it is 1492 bytes. Consult with your ISP for correct MTU setting.*

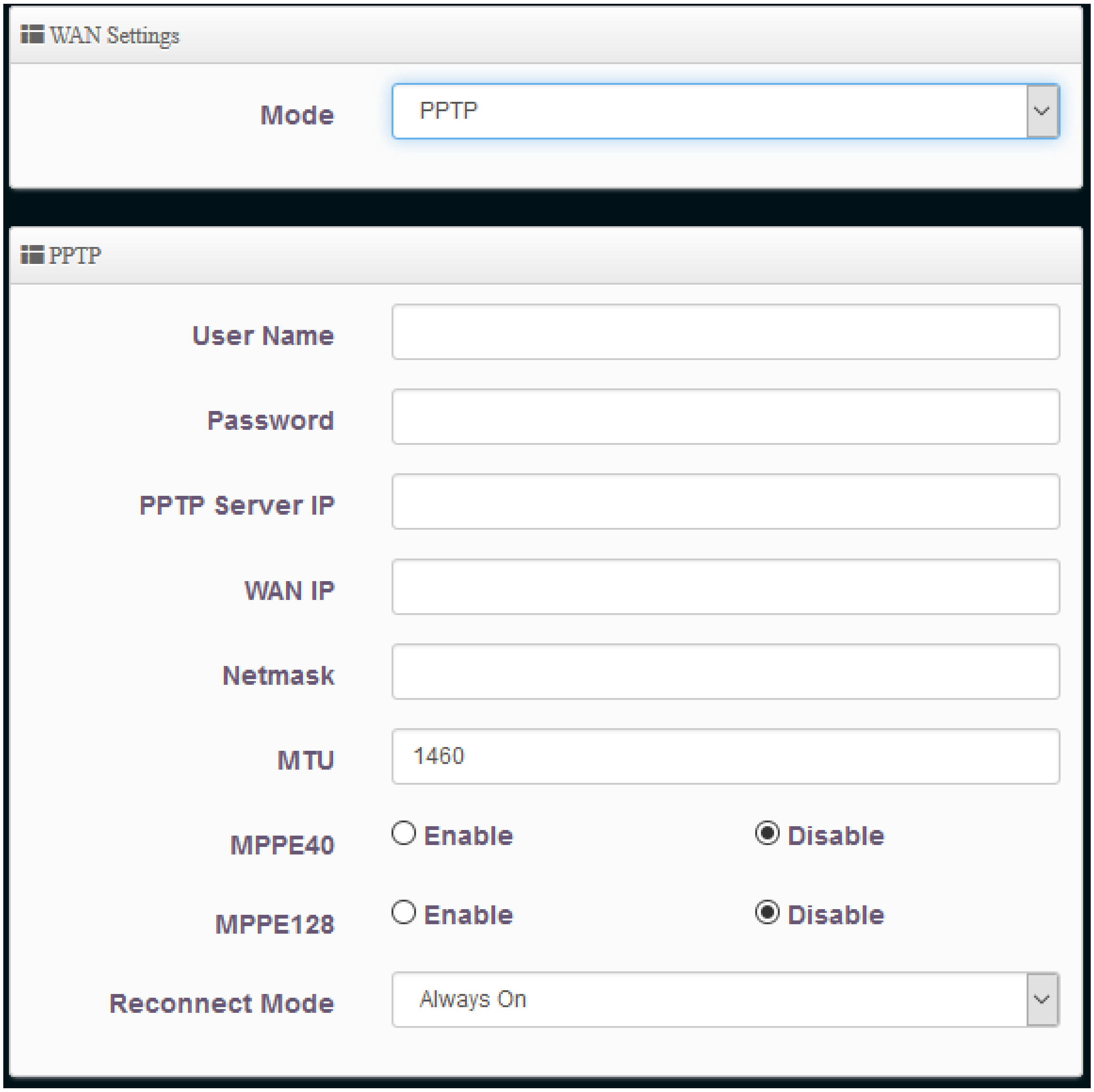
Reconnect Mode: *Always on – A connection to internet is always maintained*

On Demand – A connection to internet is made as needed

Manual – Click on the "Connect" button on "WAN information" in the overview page to connect to the internet.

4-1-4 Internet Connection Type: PPTP

The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPN) through public networks.



WAN Settings

Mode	PPTP

PPTP

User Name		
Password		
PPTP Server IP		
WAN IP		
Netmask		
MTU	1460	
MPPE40	○ Enable	● Disable
MPPE128	○ Enable	● Disable
Reconnect Mode	Always On	

Username: *Username of the PPTP connection*

Password: *Password of the PPTP connection*

PPTP Server IP Address: *The IP address of the PPTP Server*

WAN IP: *IP Address of the WAN port*

IP Netmask (Subnet): *The subnet mask of the WAN port*

PPTP Server IP address: *The IP address of the PPTP server*

MTU: *By default, it is 1492 bytes. Consult with your ISP for correct MTU setting.*

MPPE Encryption: *Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up connections or Point-to-Point Tunneling Protocol (PPTP) virtual private network (VPN) connections.* ***128-bit*** *key (strong) and* ***40-bit*** *key (standard) MPPE encryption schemes are supported. MPPE provides data security for the PPTP connection that is between the VPN client and the VPN server.*

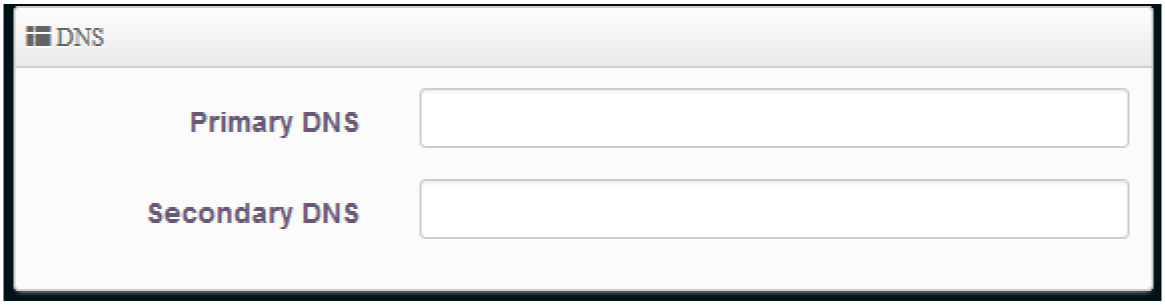
Reconnect Mode: *Always on – A connection to internet is always maintained*

On Demand – A connection to internet is made as needed

Manual – Click on the "Connect" button on "WAN information" in the overview page to connect to the internet.

4-1-5 DNS

"No default DNS server" (default) or "Specify a DNS server IP" to setup a system DNS.

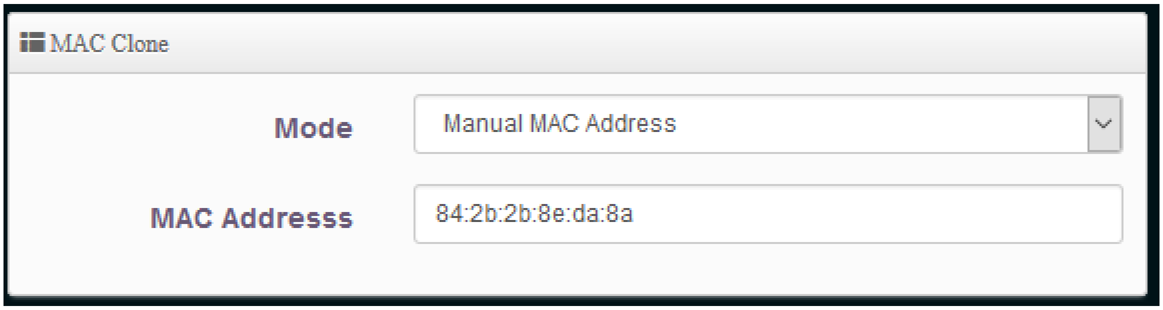


Primary: *The IP Address of the Primary DNS server*

Secondary: *The IP address of the secondary DNS server*

4-1-6 MAC Clone

The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



MAC Clone

Mode: Manual MAC Address

MAC Addresss: 84:2b:2b:8e:da:8a

Default MAC Address: *Keep the default MAC address of WAN port on the system.*

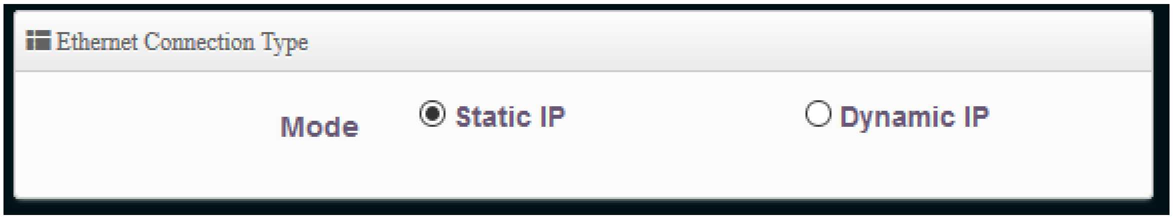
Manual MAC Address: *Enter the MAC address registered with your ISP.*

4-2 LAN Setup

Setup local IP Address/Netmask/Gateway/DNS and management. (This feature is only available under Router and WISP mode)

4-2-1 LAN IP Setup

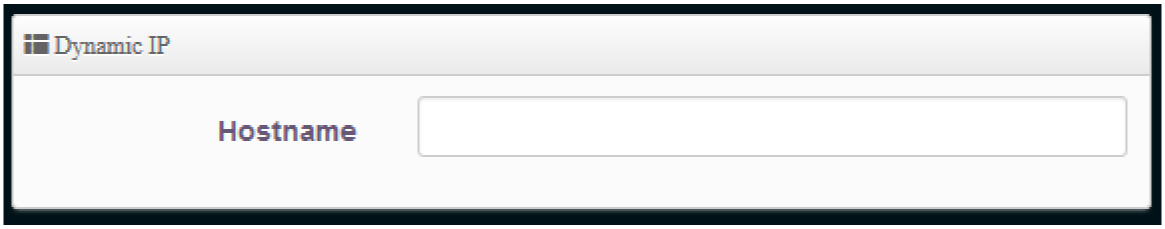
The administrator can set it to obtain (Dynamic IP) an IP automatically or manually setup (Static IP) the LAN IP address of the device.



Ethernet Connection Type

Mode ● Static IP ○ Dynamic IP

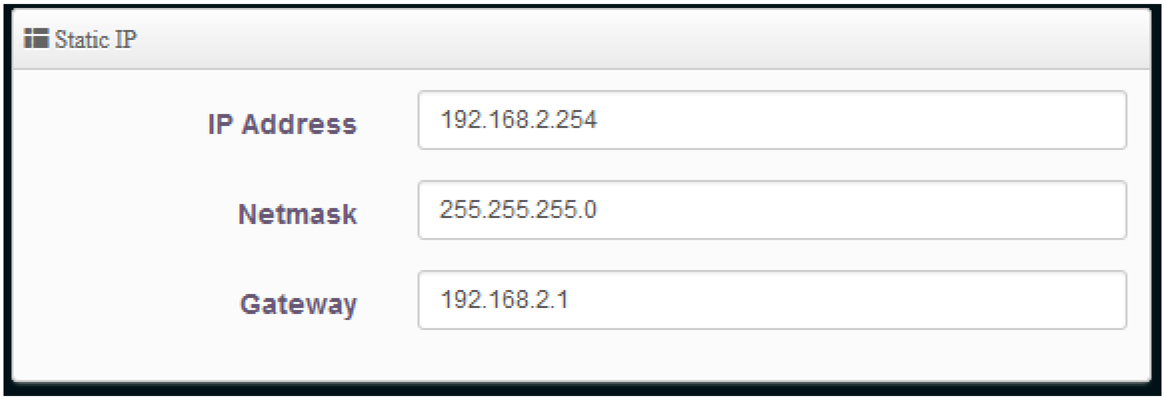
If you select Dynamic IP, you can input your host name (if required)



Dynamic IP

Hostname

If you Static IP, you can enter in your settings here:



Static IP

IP Address: 192.168.2.254

Netmask: 255.255.255.0

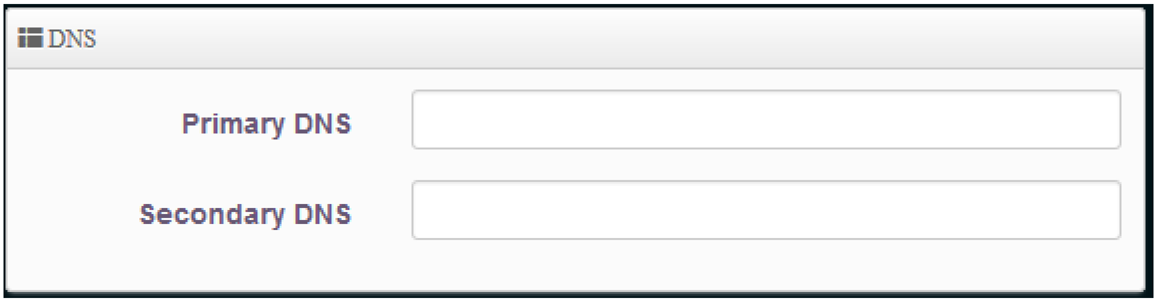
Gateway: 192.168.2.1

IP Address: *The IP address of the LAN port; default IP address is 192.168.2.254*

Netmask: *The Subnet mask of the LAN port; default Netmask is 255.255.255.0*

4-2-2 DNS

Check “No default DNS server” (default) or “Specify a DNS server IP” to setup a system DNS.



DNS

Primary DNS:

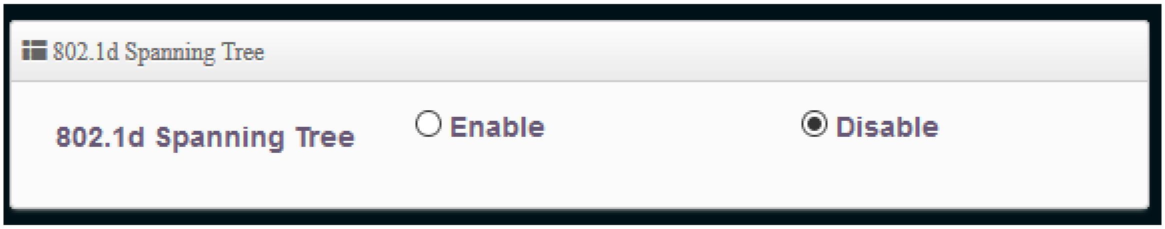
Secondary DNS:

Primary: *The IP Address of the Primary DNS server*

Secondary: *The IP address of the secondary DNS server*

4-2-3 802.1d Spinning Tree

The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.

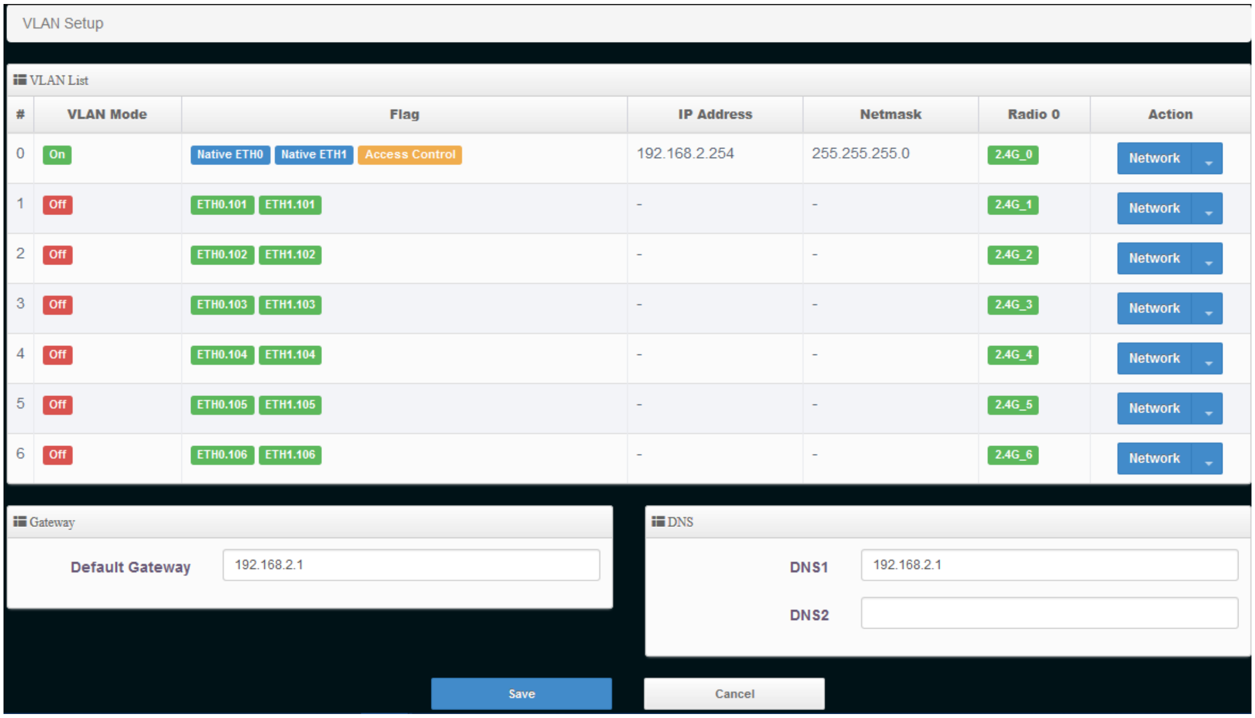


802.1d Spanning Tree

802.1d Spanning Tree ○ Enable ● Disable

4-3 VLAN Setup

The VLAN setup is used to configure VLANs. Click under System, VLAN Setup.



VLAN Setup

VLAN List

#	VLAN Mode	Flag	IP Address	Netmask	Radio 0	Action
0	On	Native ETH0 Native ETH1 Access Control	192.168.2.254	255.255.255.0	2.4G_0	Network
1	Off	ETH0.101 ETH1.101	-	-	2.4G_1	Network
2	Off	ETH0.102 ETH1.102	-	-	2.4G_2	Network
3	Off	ETH0.103 ETH1.103	-	-	2.4G_3	Network
4	Off	ETH0.104 ETH1.104	-	-	2.4G_4	Network
5	Off	ETH0.105 ETH1.105	-	-	2.4G_5	Network
6	Off	ETH0.106 ETH1.106	-	-	2.4G_6	Network

Gateway

Default Gateway: 192.168.2.1

DNS

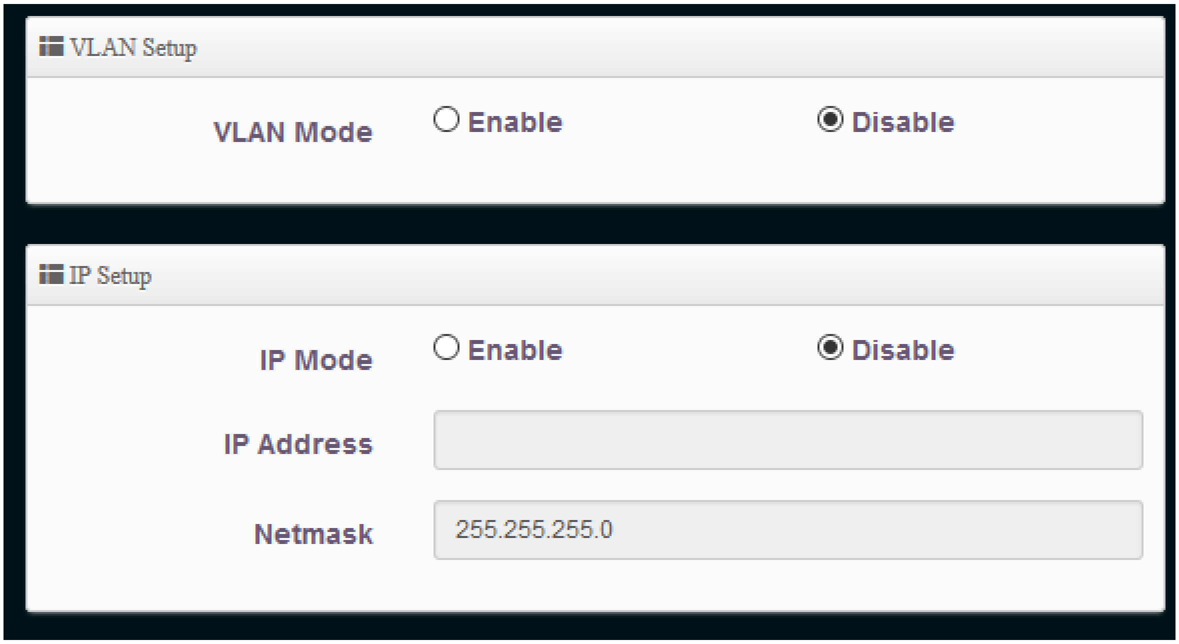
DNS1: 192.168.2.1

DNS2:

VLAN Mode:	*Number of VLANs (6 supported)*
VLAN Flag:	*Modes that are supported*
IP Address:	*IP address assigned to VLAN*
Netmask:	*Subnet Mask assigned to VLAN*
RADIO:	*WiFi frequency supported*
Action:	Click “Network” button for configuring VLAN settings

4-3-1 VLAN Network Settings

Click the Network button next to the VLAN you want to configure.



VLAN Setup

VLAN Mode ○ Enable ● Disable

IP Setup

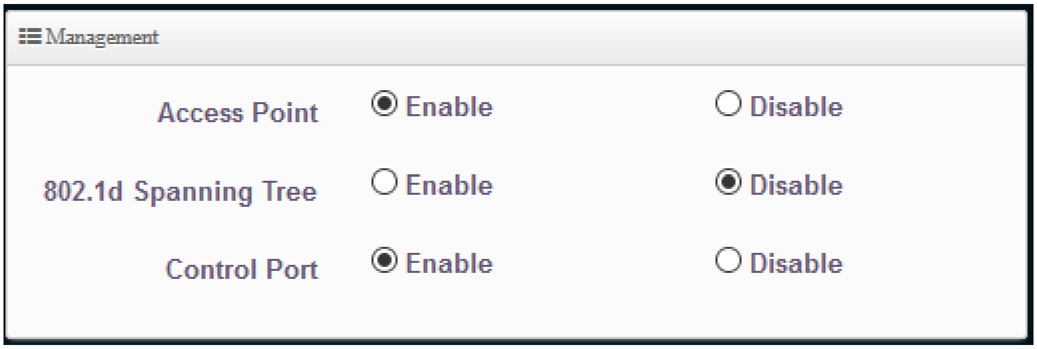
IP Mode ○ Enable ● Disable

IP Address

Netmask 255.255.255.0

VLAN Mode: *Enable/Disable to enable VLAN*

IP/Netmask Setup: *Assign an IP address for specific VLAN*



Management

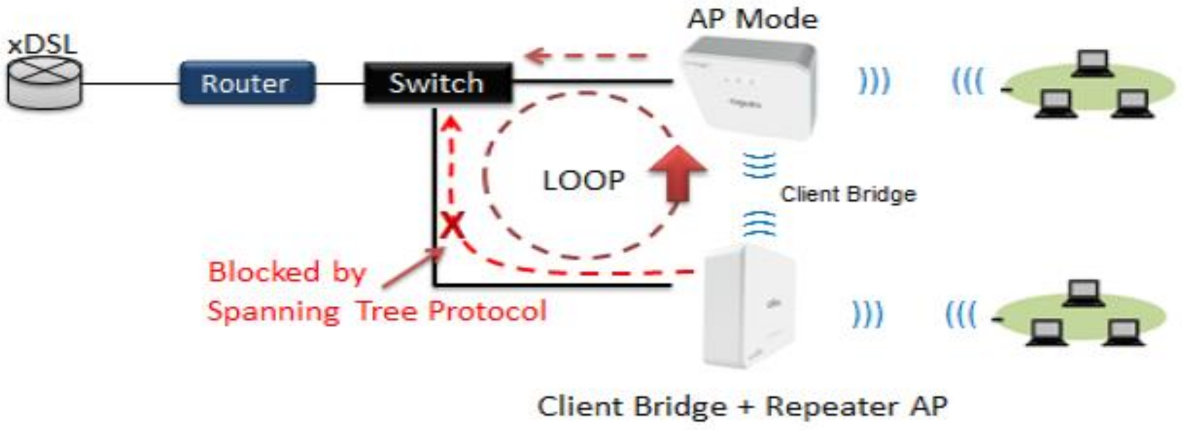
Access Point ● Enable ○ Disable

802.1d Spanning Tree ○ Enable ● Disable

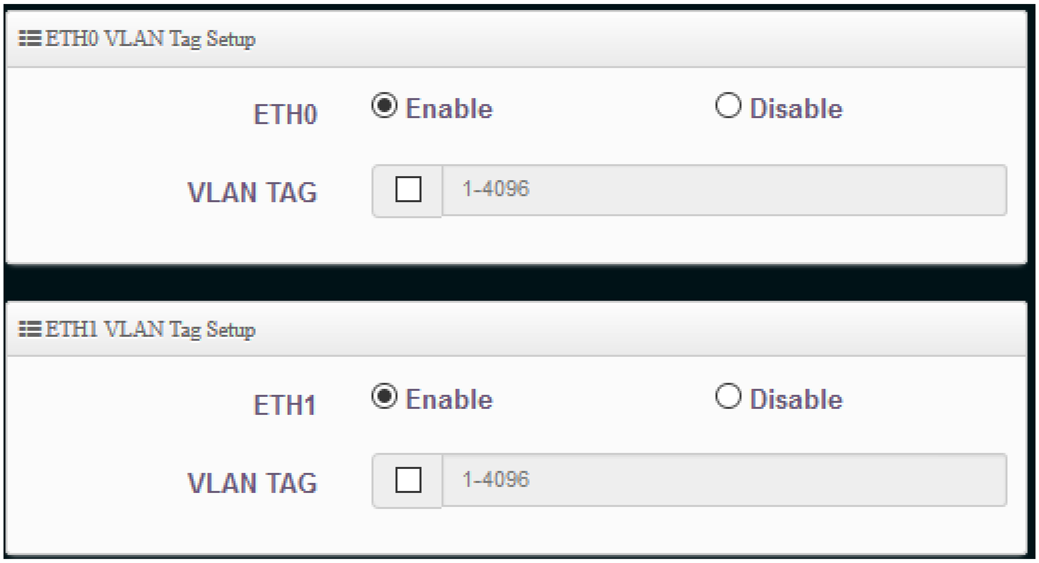
Control Port ● Enable ○ Disable

Access Point: *Enable/Disable the Wireless Radio*

802.1d Spanning Tree: *The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, also referred to as STP, is defined in the IEEE 802.1d standard.*



Control Port: *Select one of the VLANs to be managed AP.*



ETH0 VLAN Tag Setup

ETH0	● Enable	○ Disable
VLAN TAG	□ 1-4096	

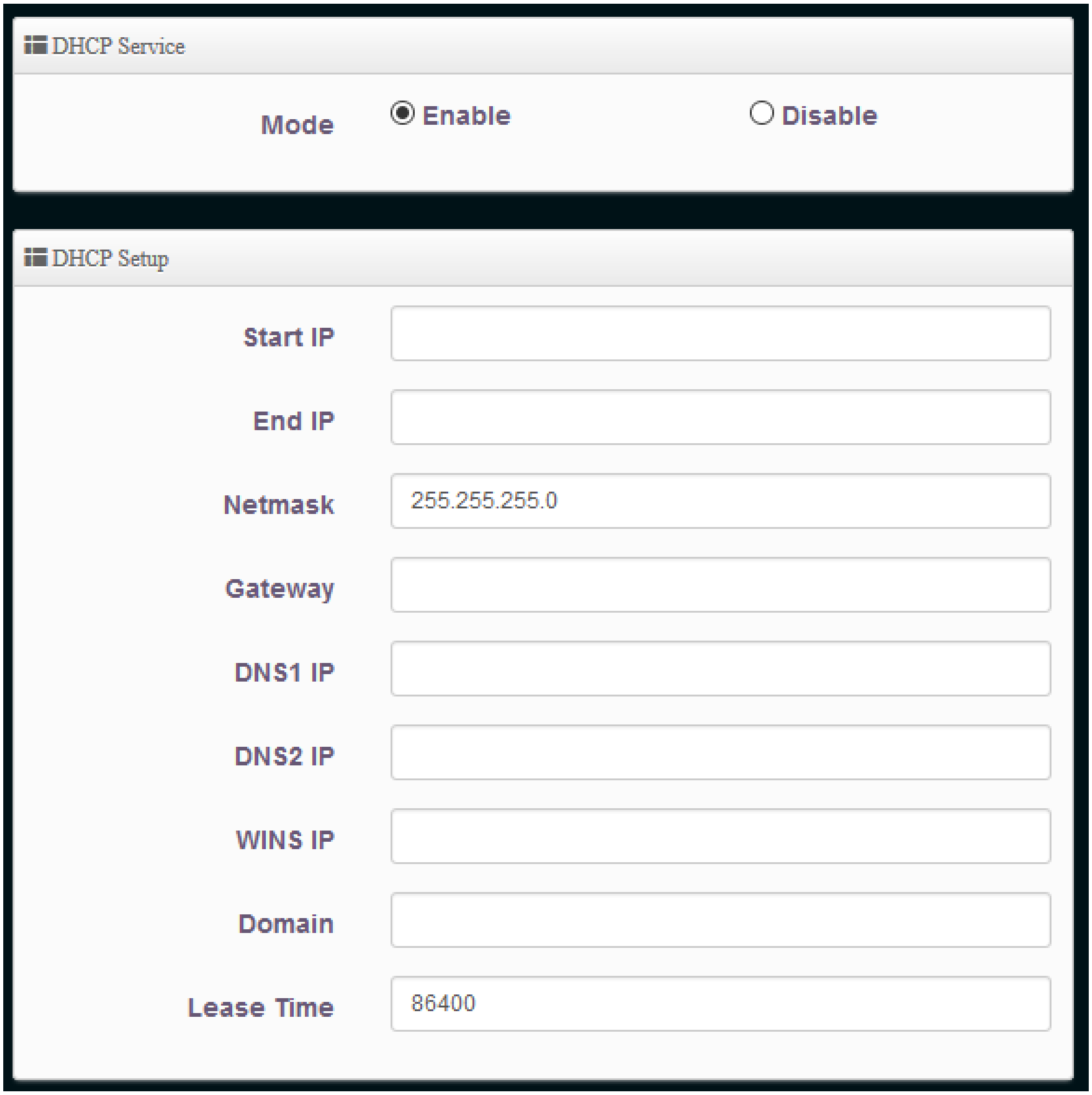
ETH1 VLAN Tag Setup

ETH1	● Enable	○ Disable
VLAN TAG	□ 1-4096	

ETH VLAN Tag Setup: *Enable/Disable and create your tags*

4-3-2 VLAN DHCP Service

Devices connected to the system can obtain an IP address automatically when this service is enabled. (This feature is only available in Router, ClientBridge + Repeater and WISP Modes)



DHCP Service

Mode	● Enable ○ Disable

DHCP Setup

Start IP	
End IP	
Netmask	255.255.255.0
Gateway	
DNS1 IP	
DNS2 IP	
WINS IP	
Domain	
Lease Time	86400

DHCP: *Check Enable button to activate this function or Disable to deactivate this service.*

Start IP / End IP: *Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70.*

Netmask: *Set IP Netmask, Default 255.255.255.0*

DNS1 IP: *Enter IP address of the first DNS server; this field is required.*

DNS2 IP: *Enter IP address of the second DNS server; this is optional.*

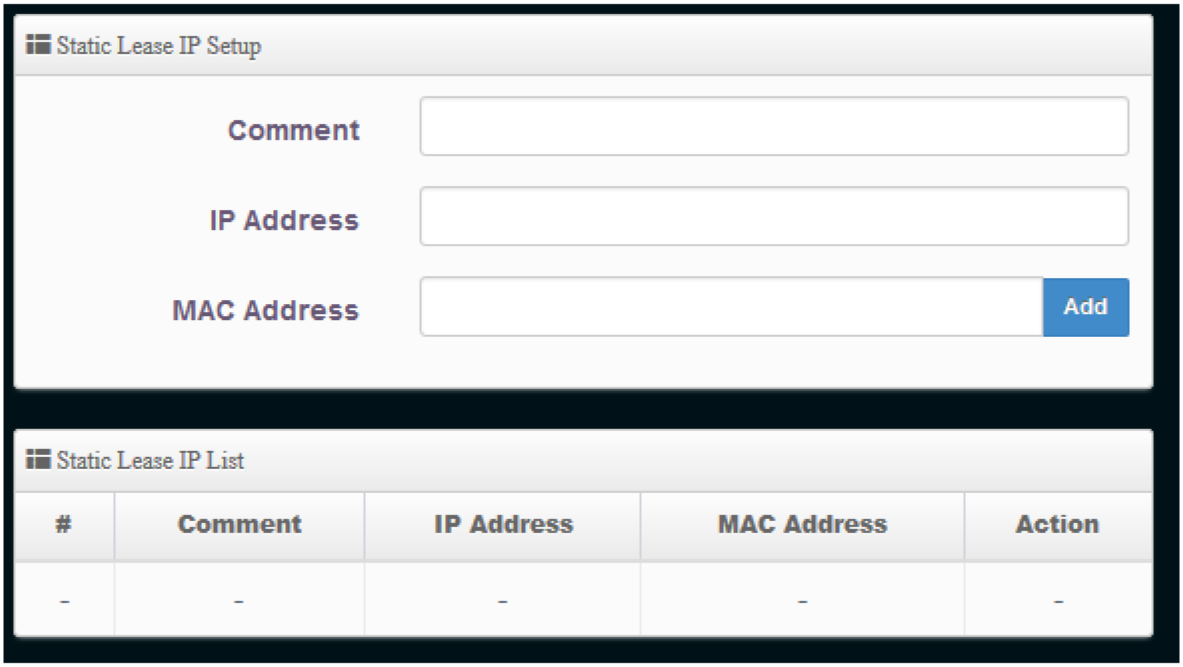
WINS IP: *Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.*

Domain: *Enter the domain name for this network.*

Lease Time: *The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is 86400 seconds*

Static Lease IP List

This function allows you to assign a static IP address to a specific computer forever, so you don't have to set the IP address for a computer, and still enjoy the benefit of using DHCP server. (This feature is only available in Router AP and WISP AP Modes)



Static Lease IP Setup

Comment

IP Address

MAC Address

Static Lease IP List

#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

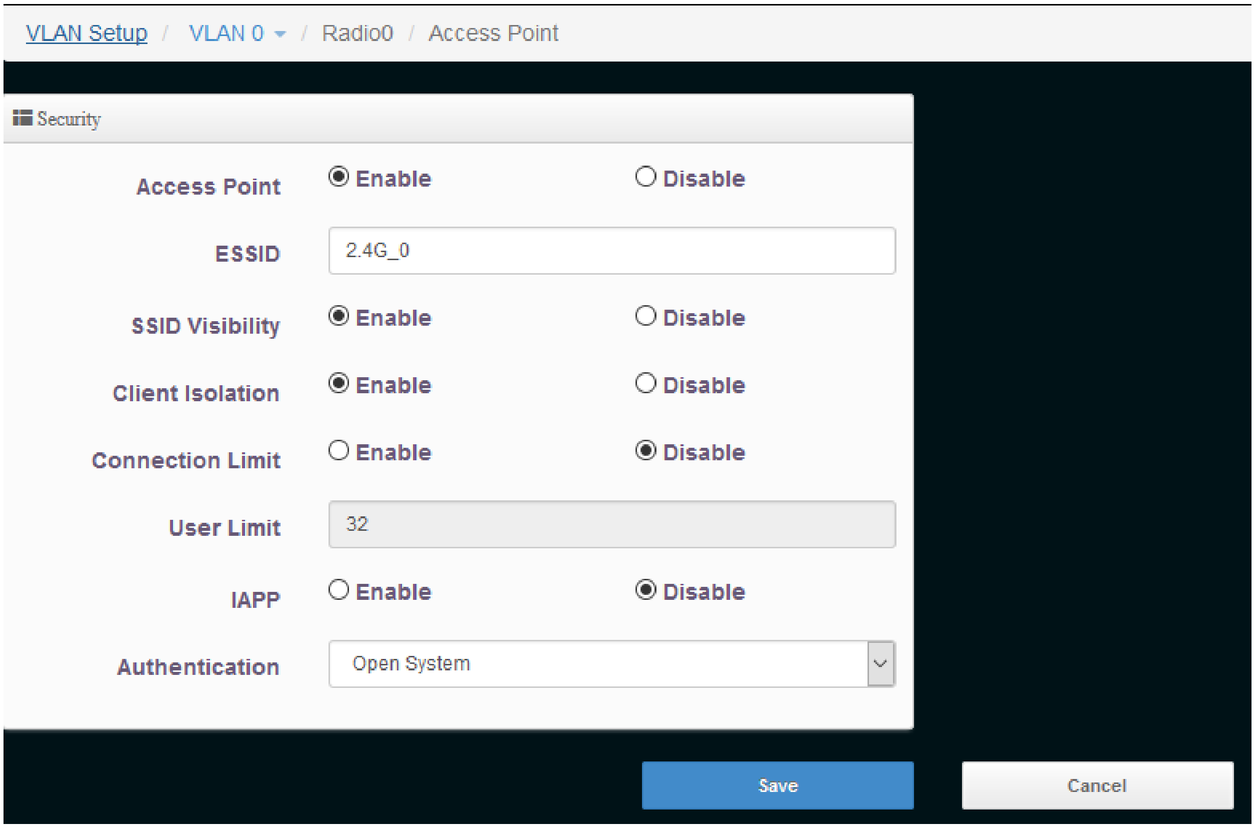
Comment: *You can enter a comment, for reference to the IP address you assigned. Ie "work computer, Living Room, etc.*

IP Address: *Input the IP address you want to assign to this computer or network device*

Mac Address: *Input the MAC address of the computer or network device (total 12 characters, with character from 0 to 9, and from a to f, like '001122aabbcc') Click "Add" to add the IP list to the table below.*

4-3-3 VLAN Access Point

For each Virtual AP, users can configure general settings and security. Click "edit" on the Virtual AP you wish to edit.



VLAN Setup / VLAN 0 / Radio0 / Access Point

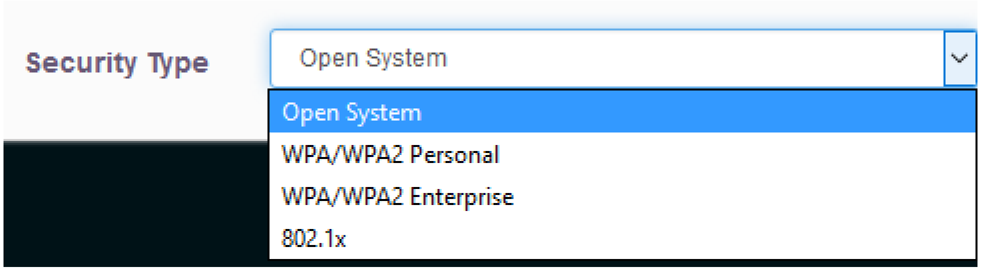
Security

Access Point	● Enable	○ Disable
ESSID	2.4G_0	
SSID Visibility	● Enable	○ Disable
Client Isolation	● Enable	○ Disable
Connection Limit	○ Enable	● Disable
User Limit	32	
IAPP	○ Enable	● Disable
Authentication	Open System	

ESSID:	*Extended Service Set ID indicates the SSID which the clients used to connect to the VAP. ESSID will determine the service type of a client which is assigned to the specified VAP.*
SSID Visibility:	*Select this option to enable the SSID to broadcast in your network. When configuring the network, it is suggested to enable this function but disable it when the configuration is complete. With this enabled, someone could easily obtain the SSID information with the site survey software and get unauthorized access to a private network. With this disabled, network security is enhanced and can prevent the SSID from begin seen on networked.*
Client Isolation:	*Select Enable, all clients will be isolated from each other. That means all clients cannot reach to other clients.*
Connection/User Limit:	*Enable if you want to have a user limit. Enter maximum number of clients to a desired number. For example, while the number of client is set to 32, only 32 clients are allowed to connect with this VAP.*
IAPP:	*Inter Access-Point Protocol is designed for the enforcement of unique association throughout a ESS(Extended Service Set) and for secure exchange of station's security context between current access point (AP) and new AP during hand off*

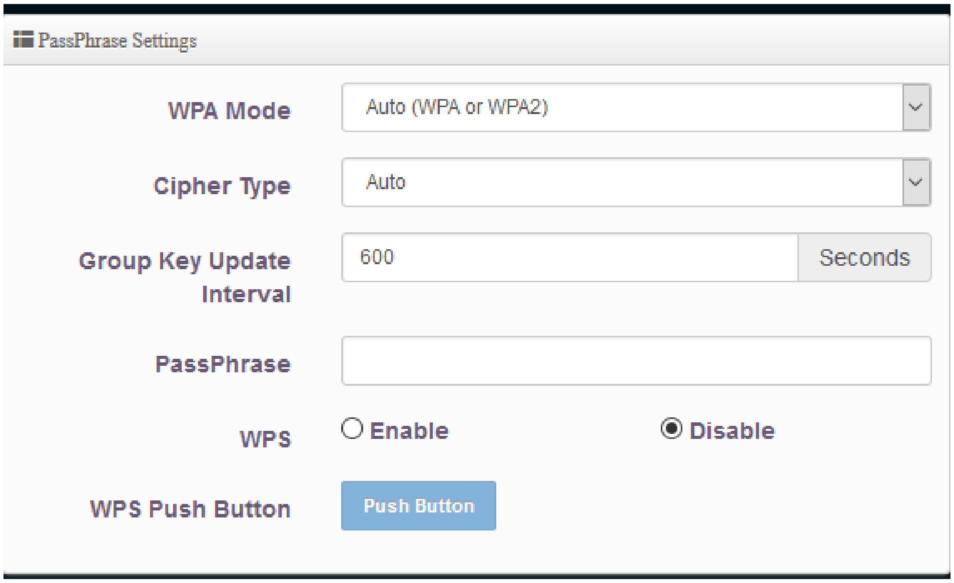
period. Notice: IAPP only used on WPA-PSK and WPA2-PSK security type. Only one of VAPs can be enabled.

Authentication: Choose your type of security you want to use for this Access Point



Security Type: Open System

Open System: Data are unencrypted during transmission when this option is selected.



PassPhrase Settings

WPA Mode: Auto (WPA or WPA2)

Cipher Type: Auto

Group Key Update Interval: 600 Seconds

PassPhrase:

WPS: ○ Enable ● Disable

WPS Push Button

WPA-PSK (or WPA2-PSK): WPA-PSK is short for W-Fi Protected Access-Pre-Shared Key. WPA-SPK uses the same encryption way with WPA, and the only difference between them is that WPA-PSK recreates a simple shared key, instead of using the user's certification.

Cipher Type: You can chose use AES or TKIP with your WPA / WPA2 encryption method,

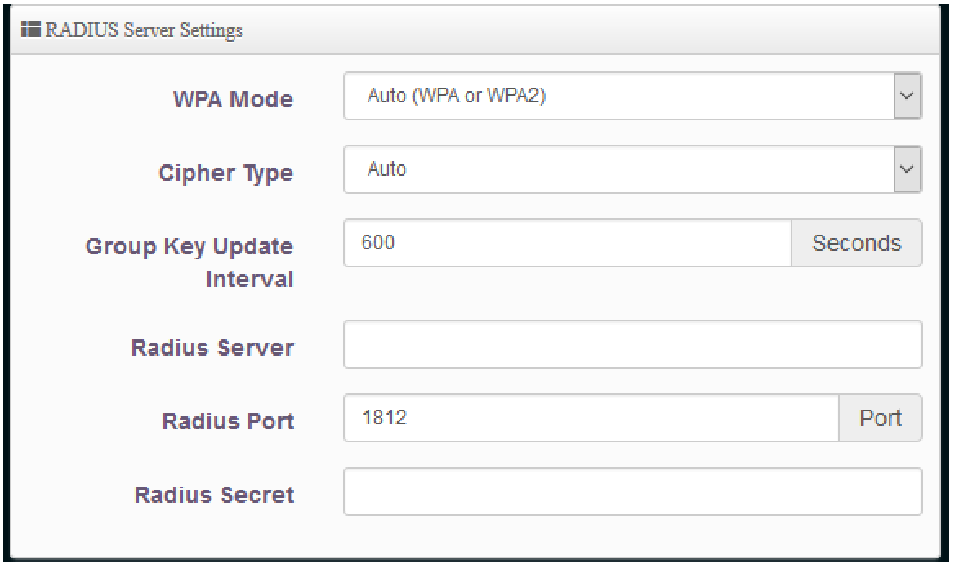
AES is short for Advanced Encryption Standard. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for "Temporal Key Integrity Protocol. TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

Group Key Update Period: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

Passphrase: Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

WPA-Enterprise (or WPA2-Enterprise) General Setting The RADIUS authentication and encryption will be both enabled if this selected.



RADIUS Server Settings

WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
Group Key Update Interval	600 Seconds
Radius Server	
Radius Port	1812 Port
Radius Secret	

Cipher Type: You can chose use AES or TKIP with your WPA / WPA2 encryption method,

AES is short for "Advanced Encryption Standard", The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for "Temporal Key Integrity Protocol", TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

Group Key Update Interval: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

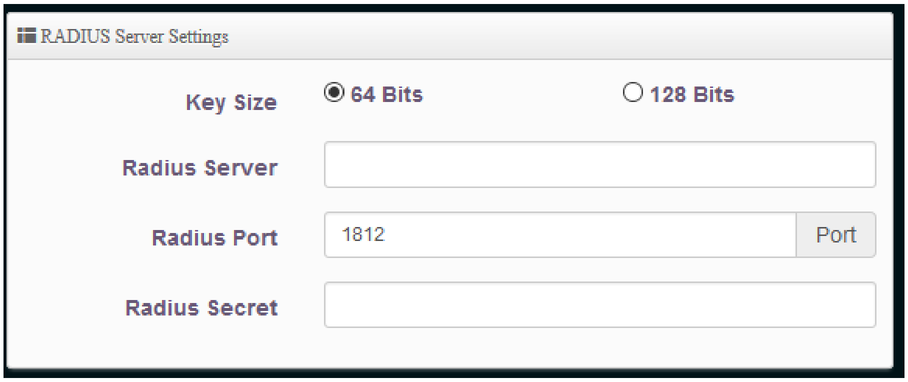
Authentication RADIUS Server Settings

Radius Server: Enter the IP address of the Authentication RADIUS server.

Radius Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Radius Secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

WEP 802.1x: When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.



RADIUS Server Settings

Key Size ● 64 Bits ○ 128 Bits

Radius Server

Radius Port 1812 Port

Radius Secret

Key Size: Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.

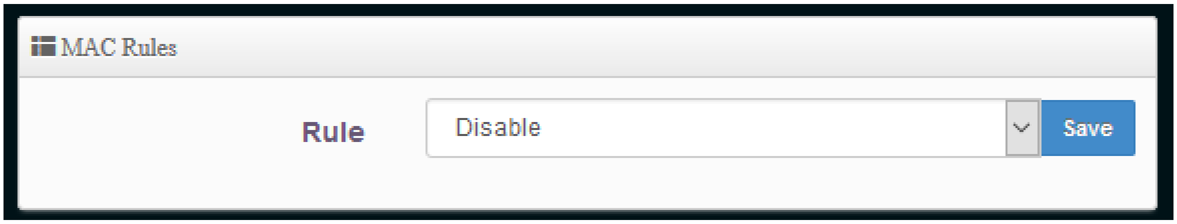
Radius Server: Enter the IP address of the Authentication RADIUS server.

Radius Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Radius Secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

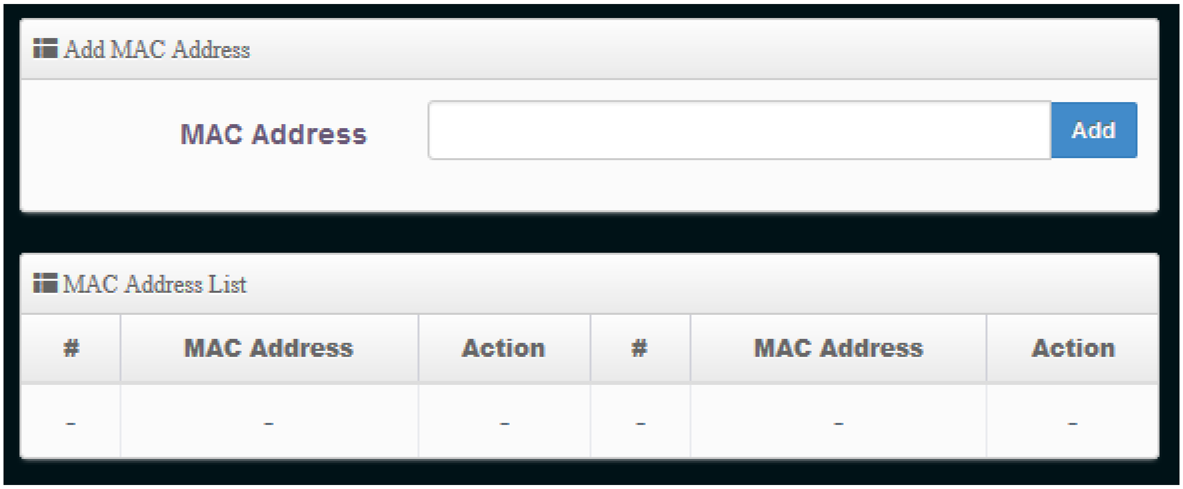
4-3-4 VLAN Mac Filter

For each VLAN AP, users can allow or reject clients based on their MAC address.



MAC Rules

Rule: Disable



Add MAC Address

MAC Address:

MAC Address List

#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

Action: *Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.*

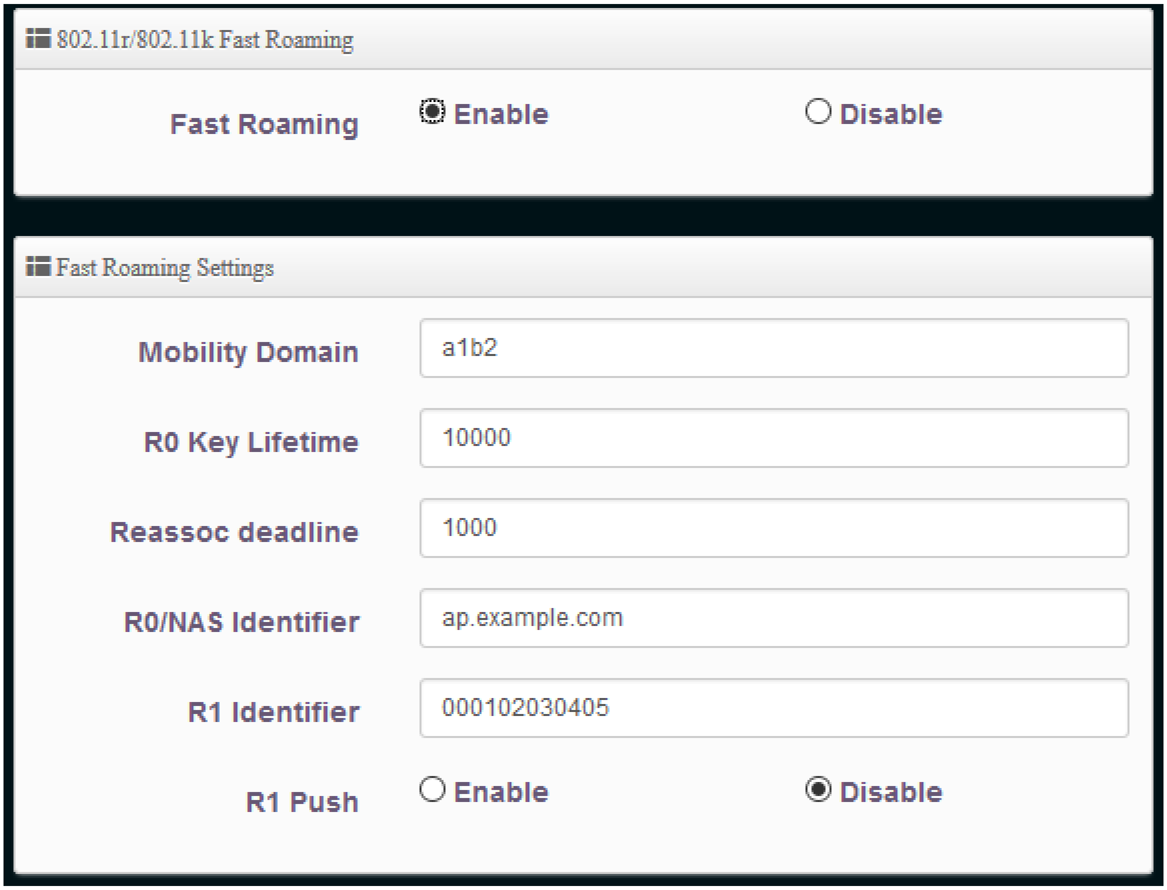
Only Allow List MAC: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "Only Allow List MAC".

Only Deny List MAC: Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to "Only Deny List MAC". MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

Mac Address: *Type in the Mac address of the client you wish to add under the Mac filter.*

4-3-5 VLAN 802.11r Fast Roaming

The HPOW5CM supports 802.11r function for 2.4GHz. This allows the client to make the initial handshake with the AP is done even before the client gets in range of the AP.



802.11r/802.11k Fast Roaming

Fast Roaming	● Enable	○ Disable

Fast Roaming Settings

Mobility Domain	a1b2
R0 Key Lifetime	10000
Reassoc deadline	1000
R0/NAS Identifier	ap.example.com
R1 Identifier	000102030405
R1 Push	○ Enable ● Disable

Fast Roaming: *Enable or Disable the feature here. Default is disabled.*

Mobility Domain: *MDID is used to indicate a group of Aps (within an ESS, ie. Sharing the same SSID) between which a STA can use Fast BSS Transition. Please enter 2-octet identifier as a hex string.*

R0 Key Lifetime: *Default lifetime of the PMK-RO in minutes, the default is 10000, administrator can set 1-65535*

Reassoc deadline:
Default: 1000 *Reassociation deadline in time units (Tus / 1.024 ms; range 1000-65535).*

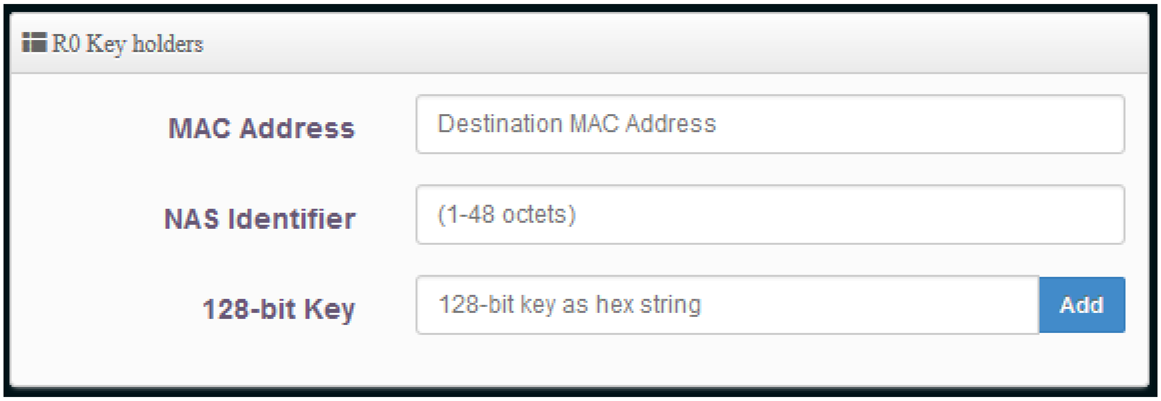
R0/NAS Identifier: *PMK-R0 Key Holder identifier. When using IEEE 802.11r, nas_identifier must be set and must be between 1 and 48 octets long.*

R1 Identifier: *PMK-R1 Key Holder identifier 6-octet identifier as a hex string*

R1 Push: *Administrator can select enable/disable. If enable, the function will automatically send the R1 Key*

R0 Key Address:

To enable roaming between multiple AP devices, the first AP must key in the MAC address of the second AP and vice versa. The NAS Identifier and 128-bit key should be identical on both Aps. This will enable device roaming between both APs.



R0 Key holders

MAC Address	Destination MAC Address
NAS Identifier	(1-48 octets)
128-bit Key	128-bit key as hex string

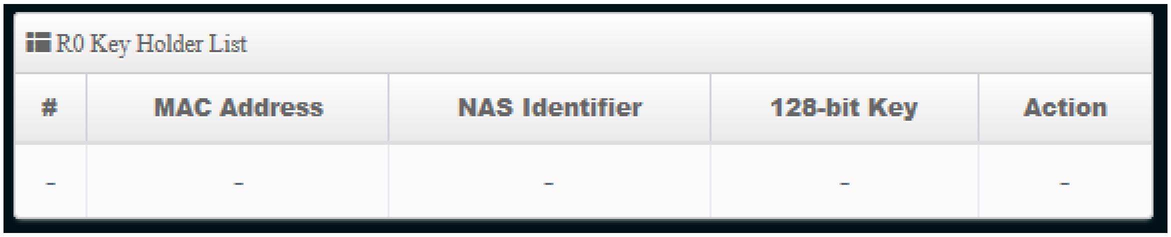
Mac Address: *Administrators must enter the MAC address of the other AP*

NAS Identifier: *Enter 1-48 octets of network domain name*

128-bit Key: *Enter shared key*

R0 Key Holder List

After setting up R0 Key Holder, the information will appear on this list.

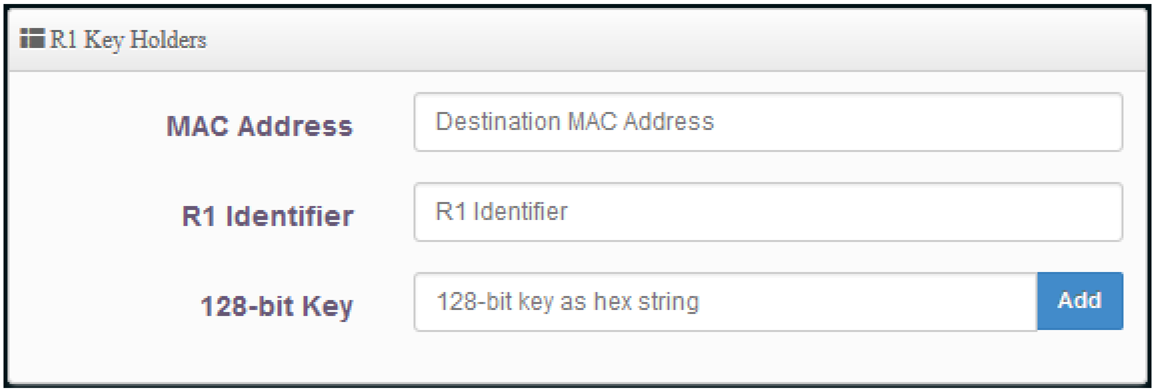


R0 Key Holder List

#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

R1 Key Holder List:

Enter a unified set of R1 Key Holder Identification certification.



R1 Key Holders

MAC Address: Destination MAC Address

R1 Identifier: R1 Identifier

128-bit Key: 128-bit key as hex string

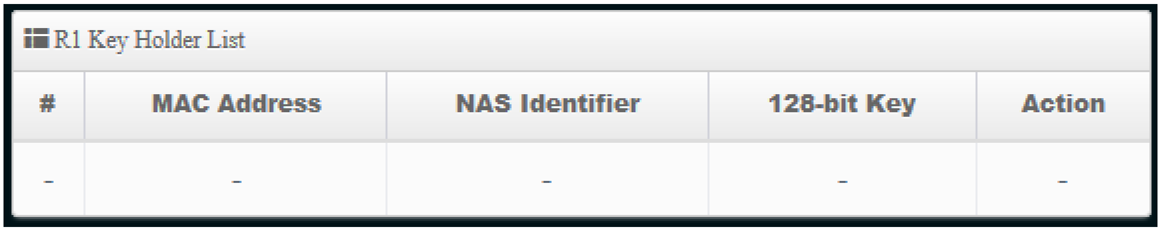
Mac Address: *Administrators must enter the MAC address of the other AP*

NAS Identifier: *Enter 1-48 octets of network domain name*

128-bit Key: *Enter shared key*

R1 Key Holder List

After setting up R1 Key Holder, the information will appear on this list.

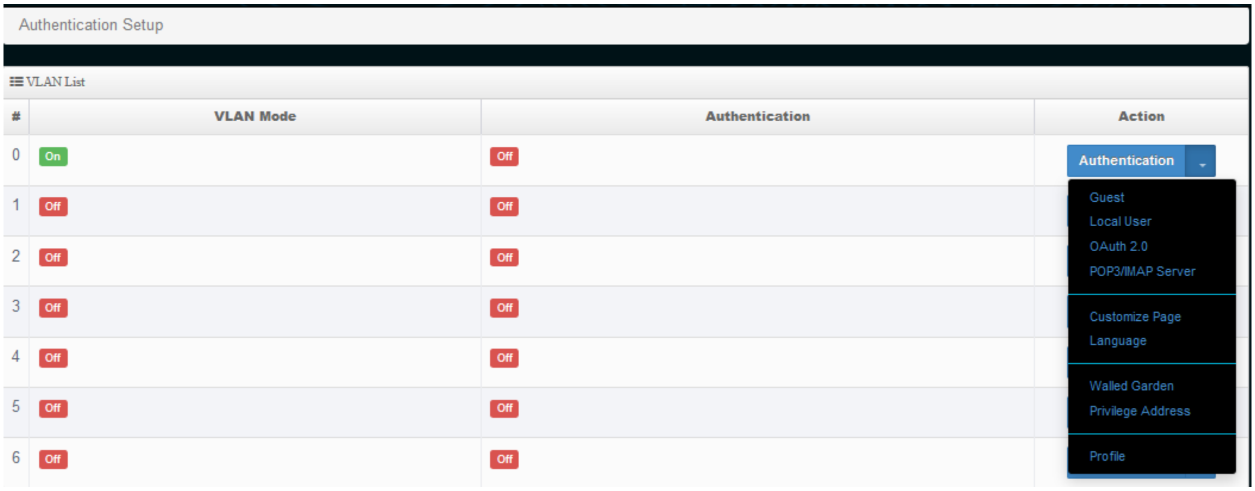


R1 Key Holder List

#	MAC Address	NAS Identifier	128-bit Key	Action
-	-	-	-	-

4-4 Authentication

This function is for web authentication. It supports authentication for local users / Radius Servers / 0Auth2.0 and Guest. The system supports 7 VLANs with web authentication.



Authentication Setup

VLAN List

#	VLAN Mode	Authentication	Action
0	On	Off	Authentication
1	Off	Off	
2	Off	Off	
3	Off	Off	
4	Off	Off	
5	Off	Off	
6	Off	Off	

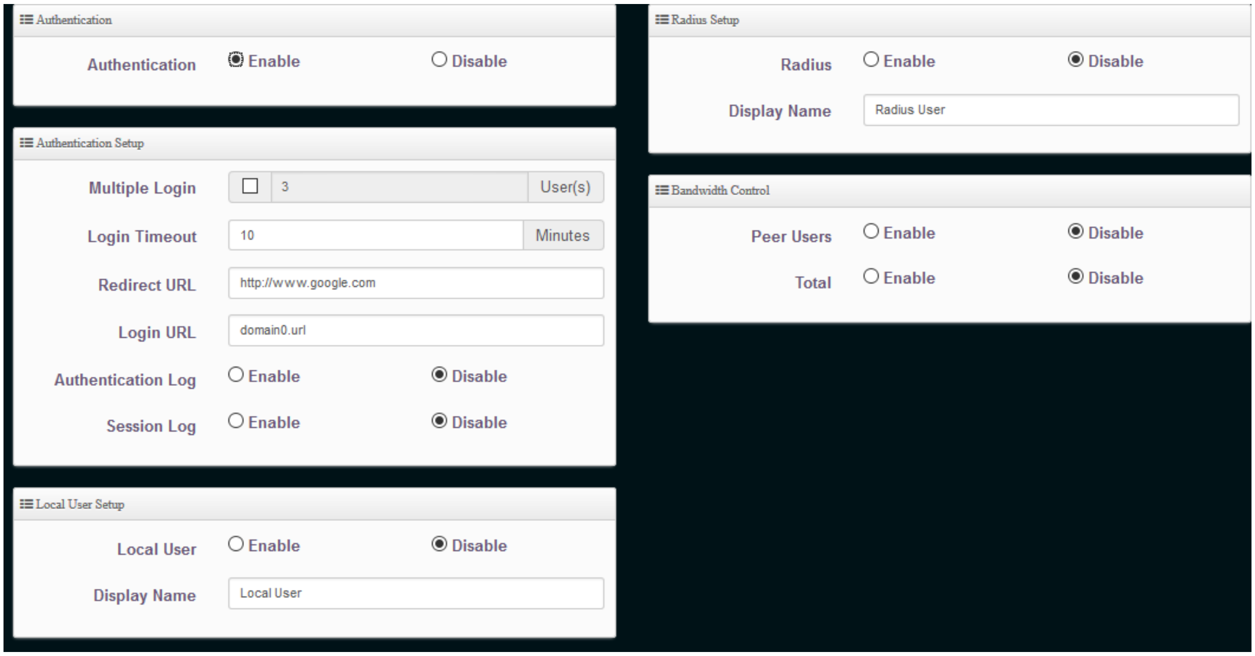
#: *Displays 7 VLANs*

Authentication: *Displays VLAN # and whether enable/disable web authentication*

Action: *Choose authentication or select drop down.*

4-4-1 Authentication

Click on the authentication button to get into the basic settings



Authentication

Authentication ● Enable ○ Disable

Authentication Setup

Multiple Login □ 3 User(s)

Login Timeout 10 Minutes

Redirect URL http://www.google.com

Login URL domain0.url

Authentication Log ○ Enable ● Disable

Session Log ○ Enable ● Disable

Local User Setup

Local User ○ Enable ● Disable

Display Name Local User

Radius Setup

Radius ○ Enable ● Disable

Display Name Radius User

Bandwidth Control

Peer Users ○ Enable ● Disable

Total ○ Enable ● Disable

Authentication: *Enable/disable*

Multiple Login: *Set one account or multiple users to simultaneously login (0 = not limited)*

Login Timeout: *After account login with no traffic, system with automatically timeout. Enter time in minutes.*

Redirect URL: *After successful login, system will redirect to URL.*

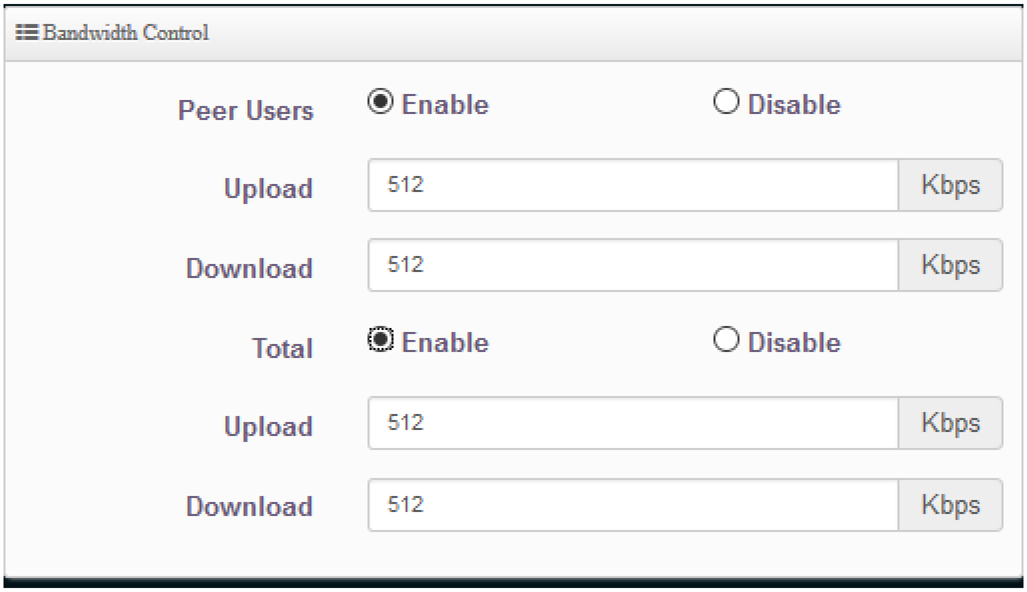
Login URL: *Set URL for login page*

Session Log: *If network has Syslog server, account session log will copy to syslog server*

Local User: *Can create a local user account.*

RADIUS: *Enter security information for remote RADIUS Server*

Bandwidth Control: *Can control traffic by users or total*



Bandwidth Control

Peer Users ● Enable ○ Disable

Upload 512 Kbps

Download 512 Kbps

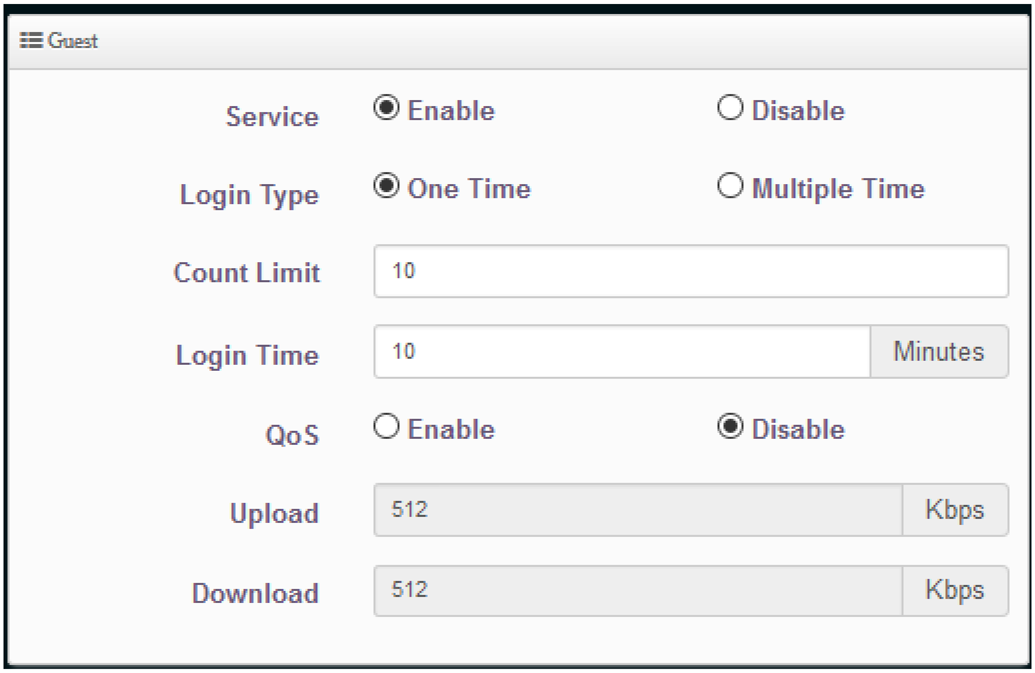
Total ● Enable ○ Disable

Upload 512 Kbps

Download 512 Kbps

4-4-2 Guest

If enabled, the administrator can set guest count limit / login time, type and flow control



Guest

Service ● Enable ○ Disable

Login Type ● One Time ○ Multiple Time

Count Limit 10

Login Time 10 Minutes

QoS ○ Enable ● Disable

Upload 512 Kbps

Download 512 Kbps

Service: *Enable/Disable*

Login Type: *One Time: login to start counting until end of time*

Multiple Times: logout time will stop counting until the next relogin to start counting

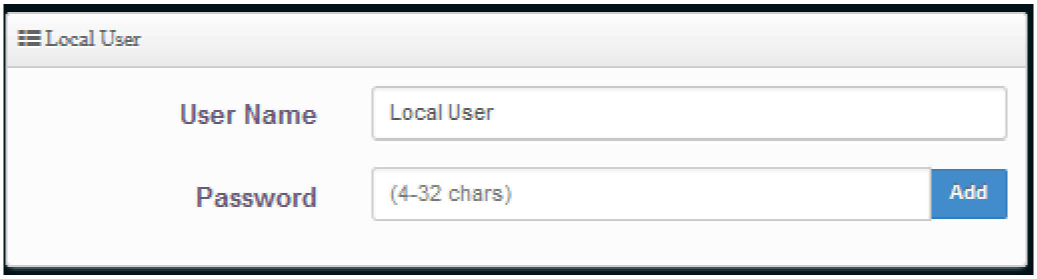
Count Limit: *Set guest limit*

Login Time: *With a certain timefame with no traffic, system will auto logout*

QoS: *Restrict traffic of guest. Set user upload/download traffic*

4-4-3 Local User

Create a local user account for web login



Local User

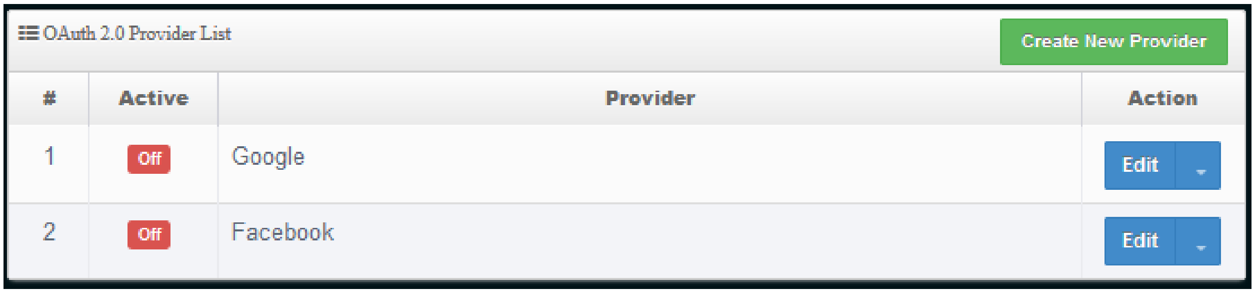
User Name	Local User
Password	(4-32 chars)

Username: *User account*

Password: *Account password*

4-4-4 OAuth2.0

Supports Facebook and Google by default. Users can add additional OAuth2.0 servers through UI settings.



OAuth 2.0 Provider List

#	Active	Provider	Action
1	Off	Google	Edit
2	Off	Facebook	Edit

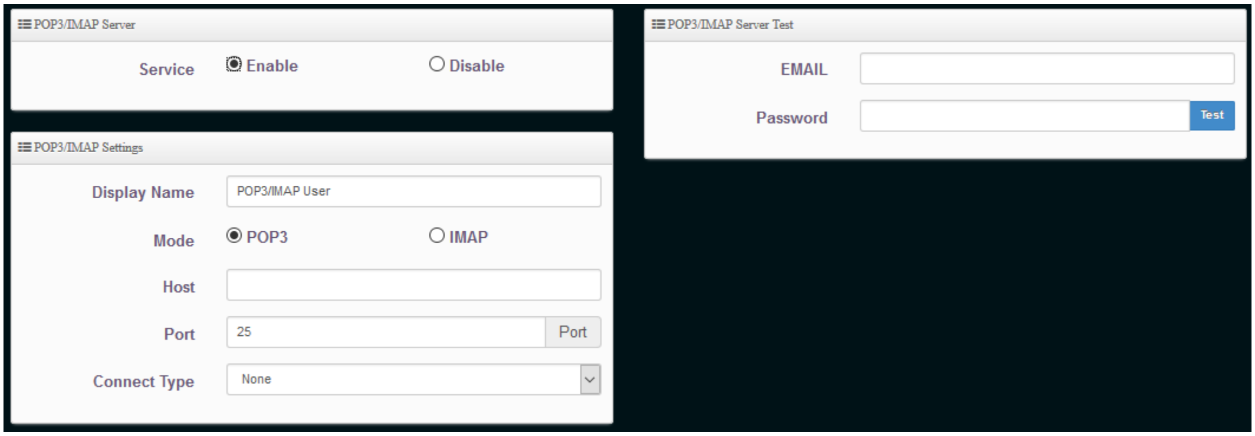
#: *Display items.*

Active: *Display on/off status for the authentication.*

Provider: *Display authentication server. The system default use authentication server for Google and Facebook*

4-4-5 POP3 Server

Allows clients to link a POP3 server for receiving emails from a remote server



POP3/IMAP Server

Service ● Enable ○ Disable

POP3/IMAP Settings

Display Name: POP3/IMAP User

Mode ● POP3 ○ IMAP

Host:

Port: 25 Port

Connect Type: None

POP3/IMAP Server Test

EMAIL:

Password:

POP3 Server: *Enable/Disable*

Display Name: *Set the display name based on POP3 user/client*

Host: *Host Server Name*

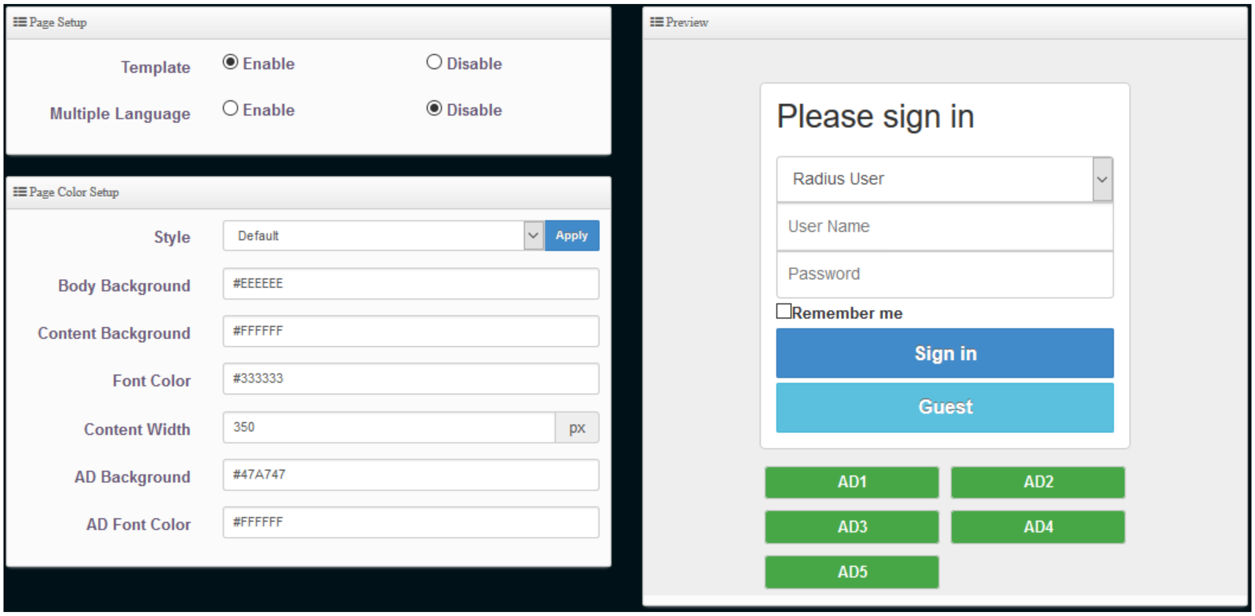
Port: *Port number for Host Server*

Connect Type: *STARTTLS, SSL/TTL or none.*

POP3 Server Test: *Test to see if the settings are operating correctly.*

4-4-6 Customize Page

This function allows the user to customize the user login page. This supports multiple languages and HTML editing.



Page Setup

Template ● Enable ○ Disable

Multiple Language ○ Enable ● Disable

Page Color Setup

Style: Default

Body Background: #EEEEEE

Content Background: #FFFFFF

Font Color: #333333

Content Width: 350 px

AD Background: #47A747

AD Font Color: #FFFFFF

Preview

Please sign in

Radius User

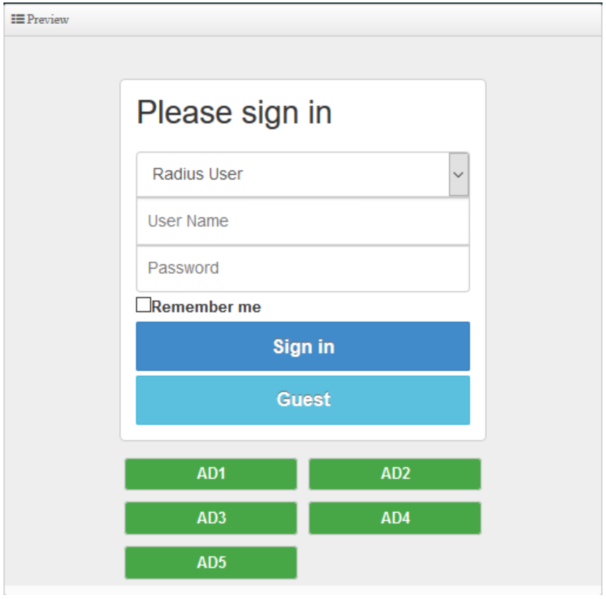
User Name

Password

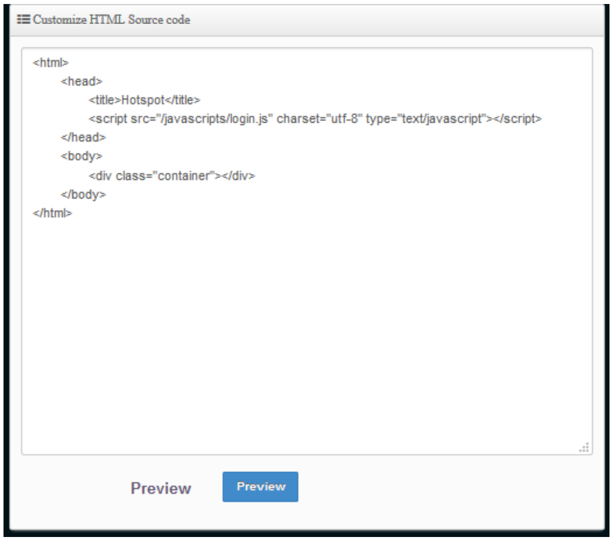
□ Remember me

Page Setup
Template: *Administrator can select Enable or disable.*

Select enable to active default Login Page



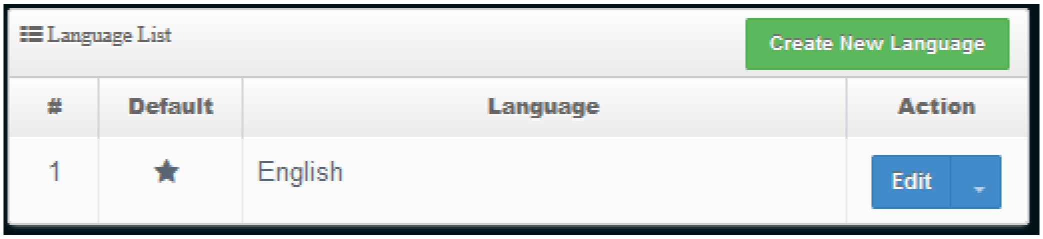
Select disable to activate HTML Source Code Window for Customization



```
<html>
        <head>
                <title>Hotspot</title>
                <script src="/javascripts/login.js" charset="utf-8" type="text/javascript"></script>
        </head>
        <body>
                <div class="container"></div>
        </body>
</html>
```

4-4-7 Customize Language

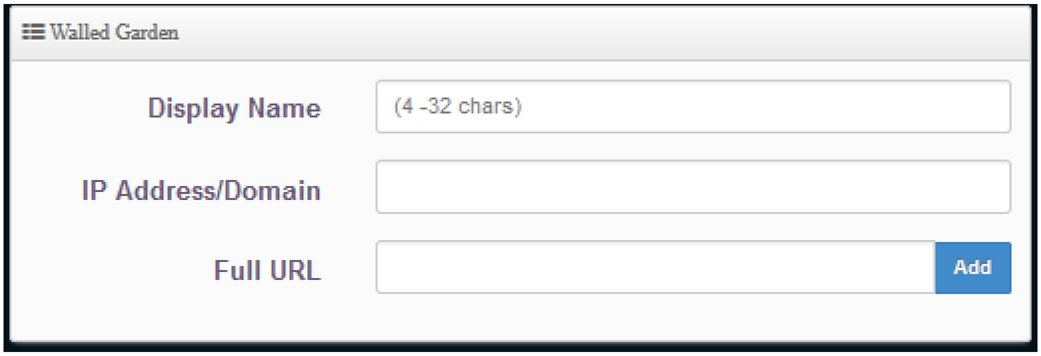
User can create other languages for login page.



#	Default	Language	Action
1	★	English	Edit

4-4-8 Walled Garden

This function provides certain free services or advertisement web pages for users to access the websites listed before login and authentication. User without the network access right can still have a chance to experience the actual network service free of charge in Walled Garden URL list.



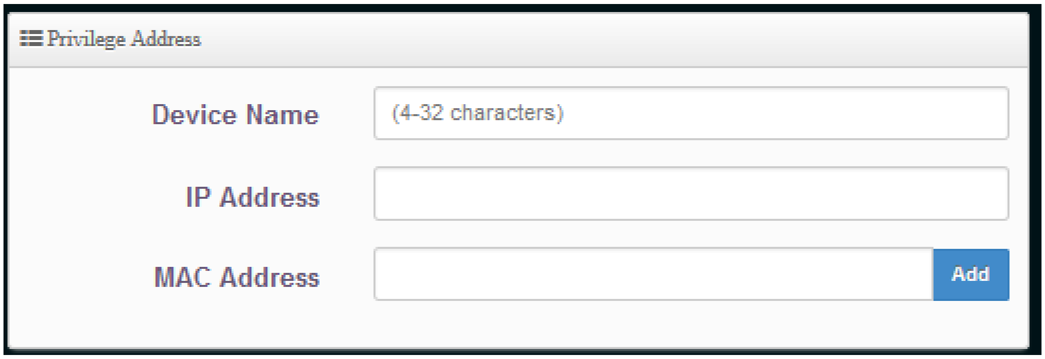
Display Name: *Set name of Website.*

IP Address/Domain: *Set IP or Domain of the Open the website.*

Full URL: *Set full website name.*

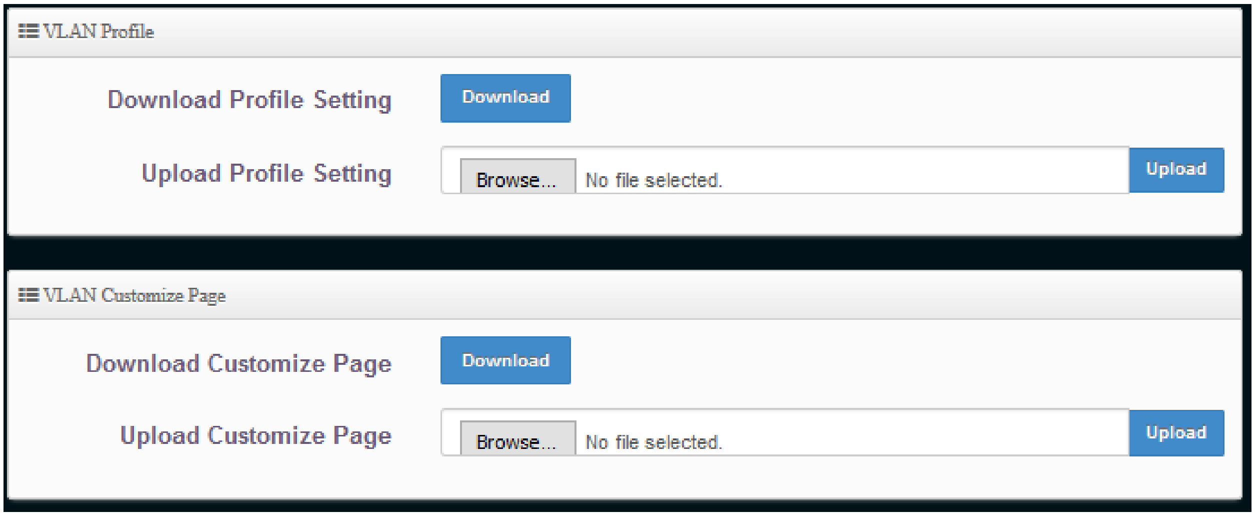
4-4-9 Privilege Address

This function provides local device can access Internet without authentication. If there are some workstations belonging NGS Access Point that need to access to network without authentication, enter the IP or MAC address of these workstations in this list.



4-4-10 Profile

Administrator can backup/upload current authentication configuration and login page for HTML Source



☰ VLAN Profile

Download Profile Setting [Download]

Upload Profile Setting [Browse...] No file selected. [Upload]

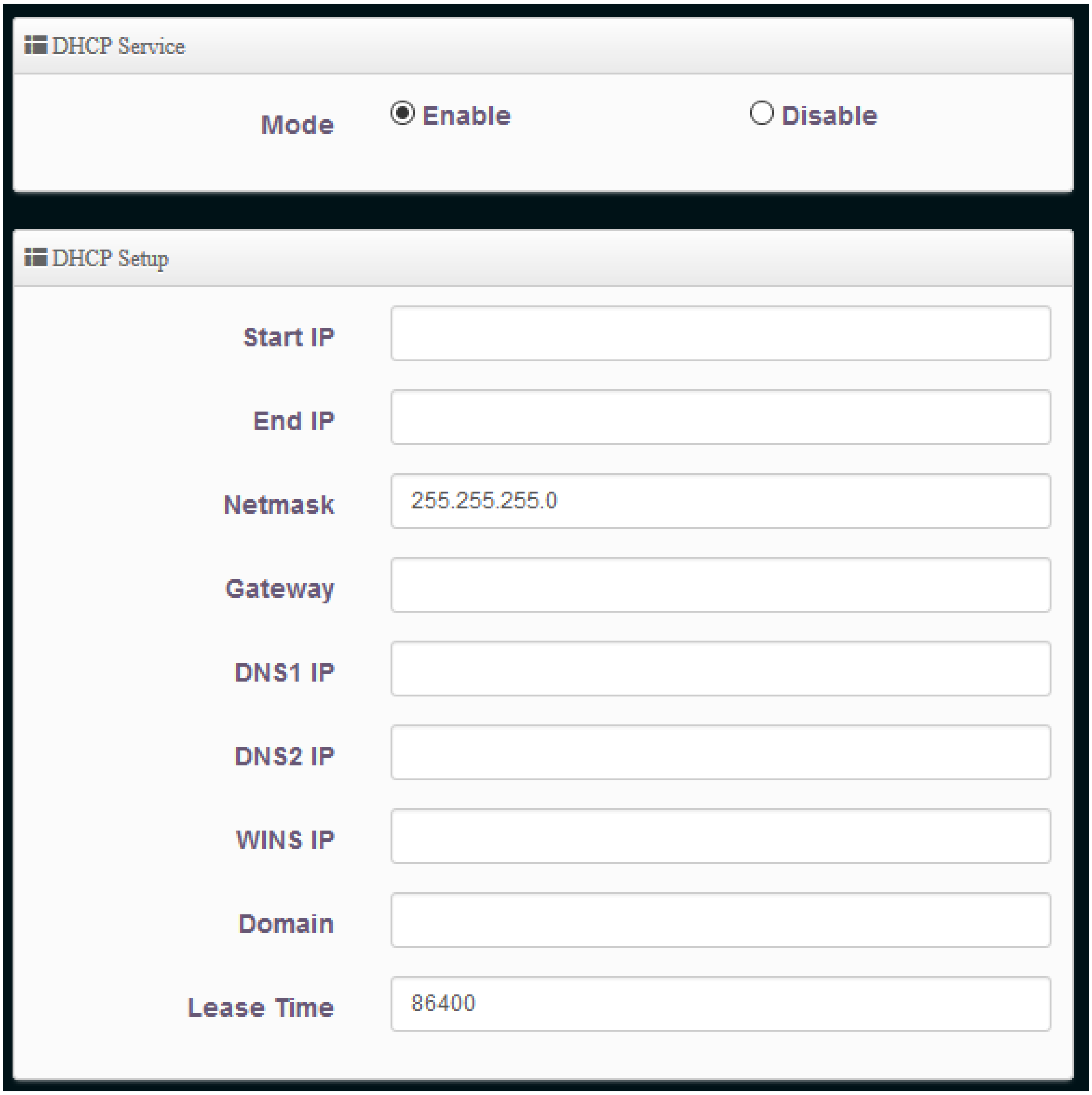
☰ VLAN Customize Page

Download Customize Page [Download]

Upload Customize Page [Browse...] No file selected. [Upload]

4-5 DHCP Setup

Devices connected to the system can obtain an IP address automatically when this service is enabled. (This feature is only available in Router and WISP Modes)



DHCP Service

Mode ● Enable ○ Disable

DHCP Setup

Start IP	
End IP	
Netmask	255.255.255.0
Gateway	
DNS1 IP	
DNS2 IP	
WINS IP	
Domain	
Lease Time	86400

DHCP: *Check Enable button to activate this function or Disable to deactivate this service.*

Start IP / End IP: *Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients. The default range IP address is 192.168.2.10 to 192.168.2.70, the netmask is 255.255.255.0*

DNS1 IP: *Enter IP address of the first DNS server; this field is required.*

DNS2 IP: *Enter IP address of the second DNS server; this is optional.*

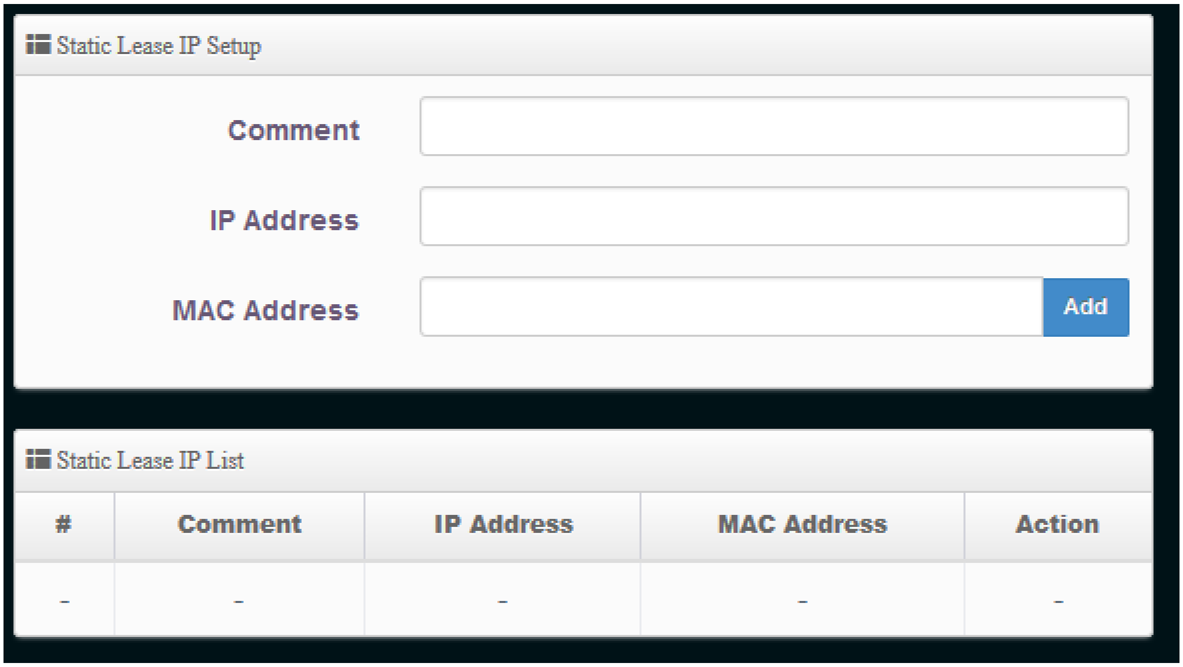
WINS IP: *Enter IP address of the Windows Internet Name Service (WINS) server; this is optional.*

Domain: *Enter the domain name for this network.*

Lease Time: *The IP addresses given out by the DHCP server will only be valid for the duration specified by the lease time. Increasing the time ensure client operation without interruptions, but could introduce potential conflicts. Lowering the lease time will avoid potential address conflicts, but might cause more interruptions to the client while it will acquire new IP addresses from the DHCP server. Default is 86400 seconds*

Static Lease IP List

This function allows you to assign a static IP address to a specific computer forever, so you don't have to set the IP address for a computer, and still enjoy the benefit of using DHCP server. (This feature is only available in Router AP and WISP AP Modes)



Static Lease IP Setup

Comment	
IP Address	
MAC Address	

Static Lease IP List

#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

Comment: *You can enter a comment, for reference to the IP address you assigned. Ie "work computer, Living Room, etc.*

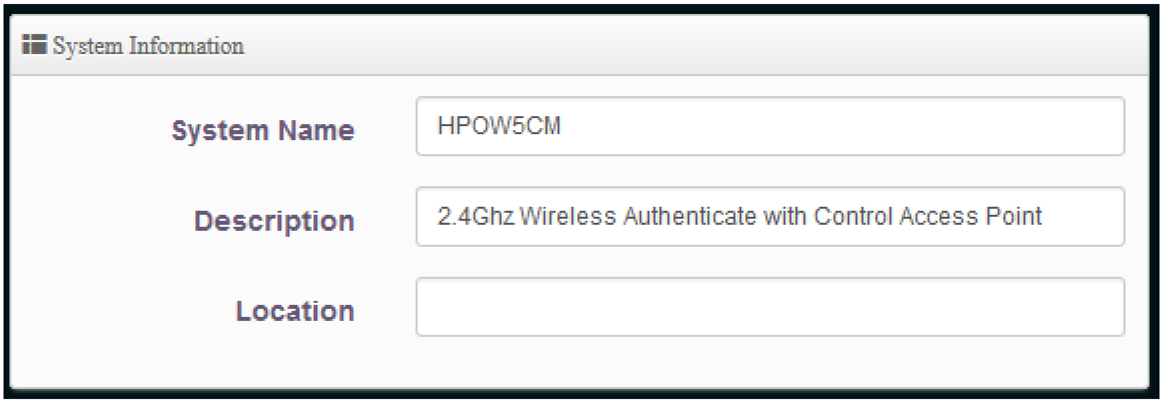
IP Address: *Input the IP address you want to assign to this computer or network device*

Mac Address: *Input the MAC address of the computer or network device (total 12 characters, with character from 0 to 9, and from a to f, like '001122aabbcc') Click "Add" to add the IP list to the table below.*

4-6 Management Setup

Administrators can setup system info, passwords and login methods. Click under System, Management

4-6-1 System Information System



System Information

System Name: HPOW5CM

Description: 2.4Ghz Wireless Authenticate with Control Access Point

Location:

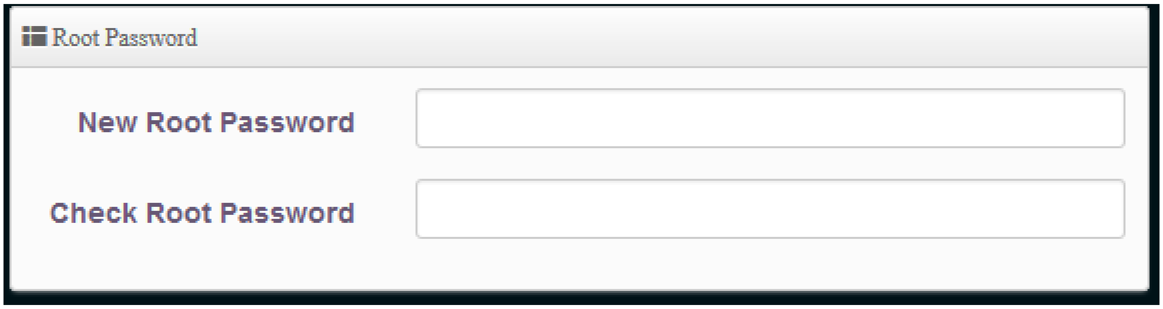
Name: *Enter a desired name or use the default one.*

Description: *Provide description of the system.*

Location: *Enter geographical location information of the system.*

4-6-2 Root Password

Full administrative rights and access to all aspects of the configuration



Root Password

New Root Password:

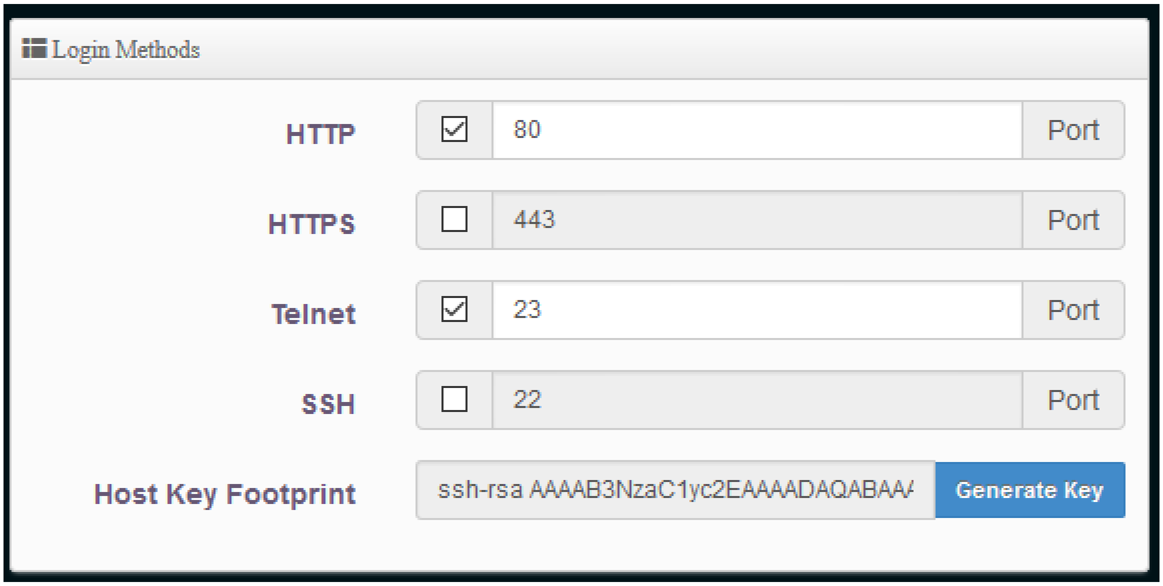
Check Root Password:

New Password: *Enter a new password if desired*

Check New Password: *Enter the same new password again*

4-6-3 Admin Login Methods:

Only root user can enable or disable system login methods and change services port.



Login Methods

HTTP ☑ 80 Port

HTTPS □ 443 Port

Telnet ☑ 23 Port

SSH □ 22 Port

Host Key Footprint ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAA/

Enable HTTP: *Check to select HTTP Service.*

Enable HTTPS: *Check to select HTTPS Service*

HTTPS Port: *The default is 443 and the range is between 1 ~ 65535.*

Enable Telnet: *Check to select Telnet Service*

Telnet Port : *The default is 23 and the range is between 1 ~ 65535*

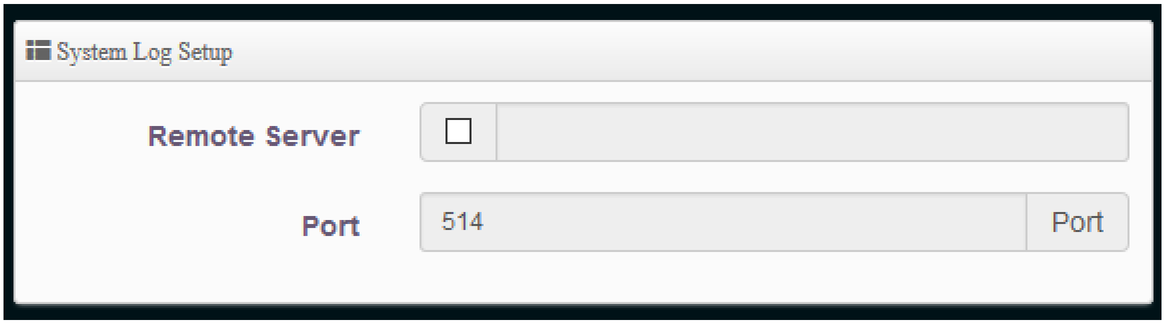
Enable SSH: *Check to select SSH Service*

SSH Port : *Please The default is 22 and the range is between 1 ~ 65535.*

Click "Generate Key" button to generate RSA private key. The "host key footprint" gray blank will display content of RSA key.

4-6-4 System Log Setup

Administrator can be the backup system log or authentication log to remote server. Please enter the IP address and port of the remote sys log server.

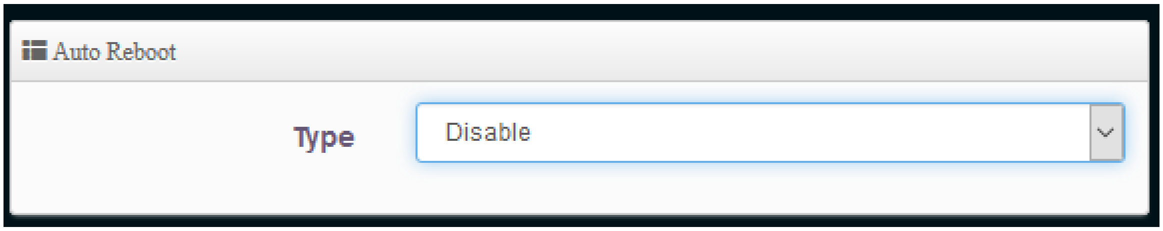

System Log Setup

Remote Server □

Port 514 Port

4-6-5 Auto Reboot

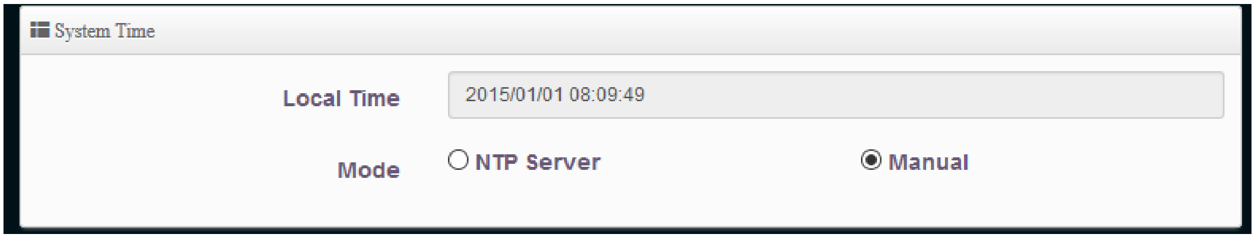
The device can be set to auto reboot in a daily, weekly, or monthly setting.


Auto Reboot

Type Disable

4-7 Time Server Setup

System time can be configured via this page, and manual setting or via a NTP server is supported. Please go to System, Time Server


System Time

Local Time 2015/01/01 08:09:49

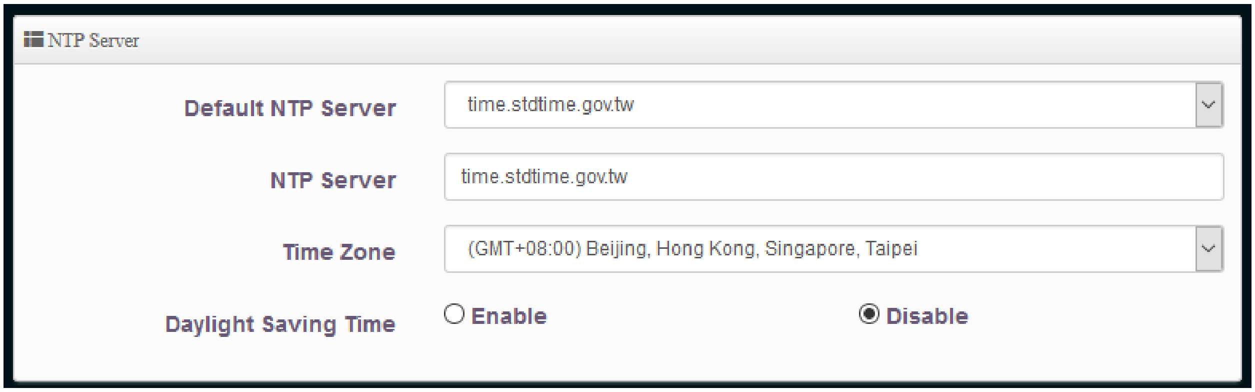
Mode ○ NTP Server ● Manual

Local Time: *Display the current system time.*

Mode: *Select NTP Server or Manual*

Setup Time Using NTP

Synchronize the system time with NTP server. System can autoupdate the system time.



NTP Server

Default NTP Server	time.stdtime.gov.tw
NTP Server	time.stdtime.gov.tw
Time Zone	(GMT+08:00) Beijing, Hong Kong, Singapore, Taipei
Daylight Saving Time	○ Enable ● Disable

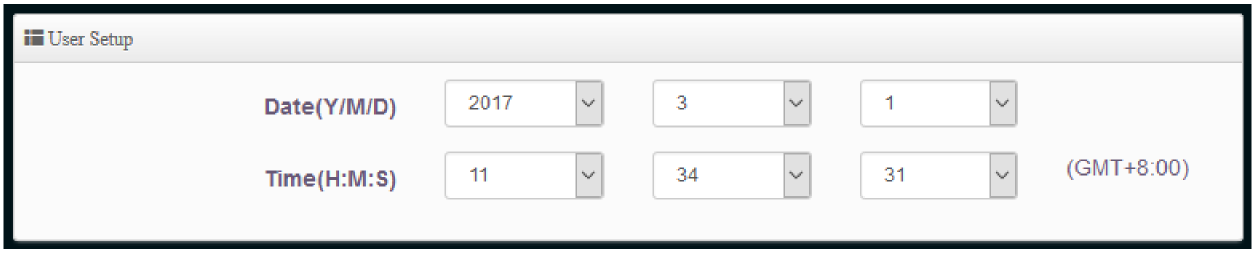
Default NTP Server: *Select the NTP Server from the drop-down list.*

Time Zone: *Select a desired time zone from the drop-down list.*

Daylight saving time: *Enable or disable Daylight saving.*

Setup Time Using Manual

The user can manually set time/date



User Setup

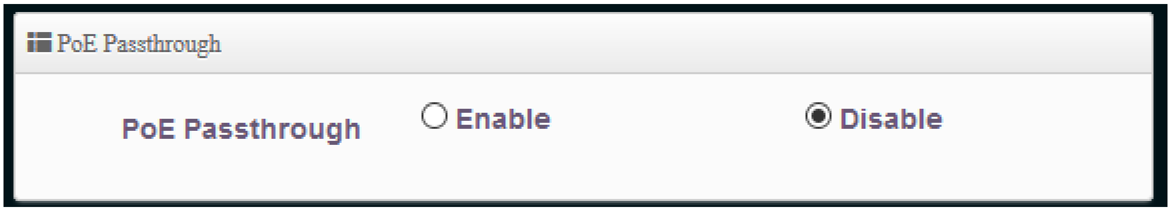
Date(Y/M/D)	2017	3	1	
Time(H:M:S)	11	34	31	(GMT+8:00)

Date: *Set the date for system.*

Time: *Set the time for system.*

4-8 PoE PassThrough

This device supports PoE Bridge function. If this is enabled, the Ethernet port LAN2 will allow other PoE devices to be powered through the secondary LAN port



PoE Passthrough

PoE Passthrough ○ Enable ● Disable

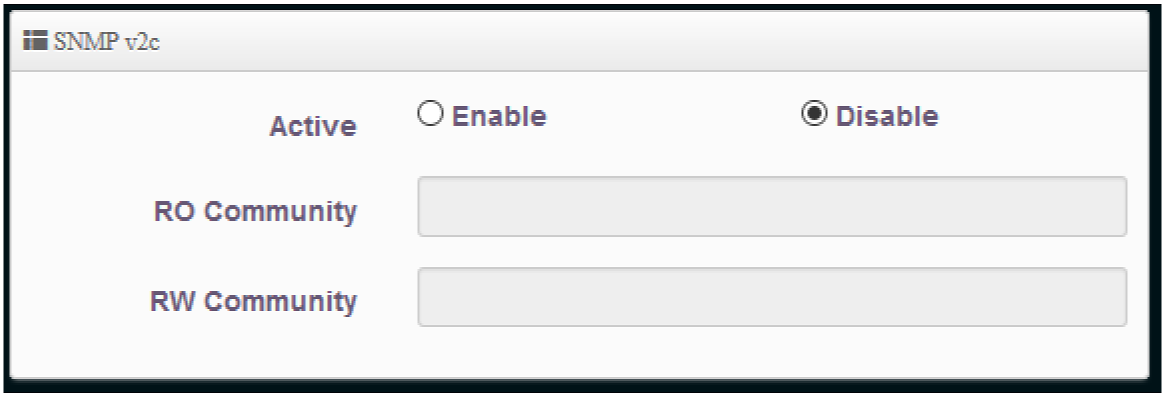
Service: the default is disabled but user can enable the feature here

4-9 SNMP Setup

SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely. You can access the settings by going to System, SNMP

SNMP v2c Enable

Check to enable SNMP v2c.



SNMP v2c

Active ○ Enable ● Disable

RO Community

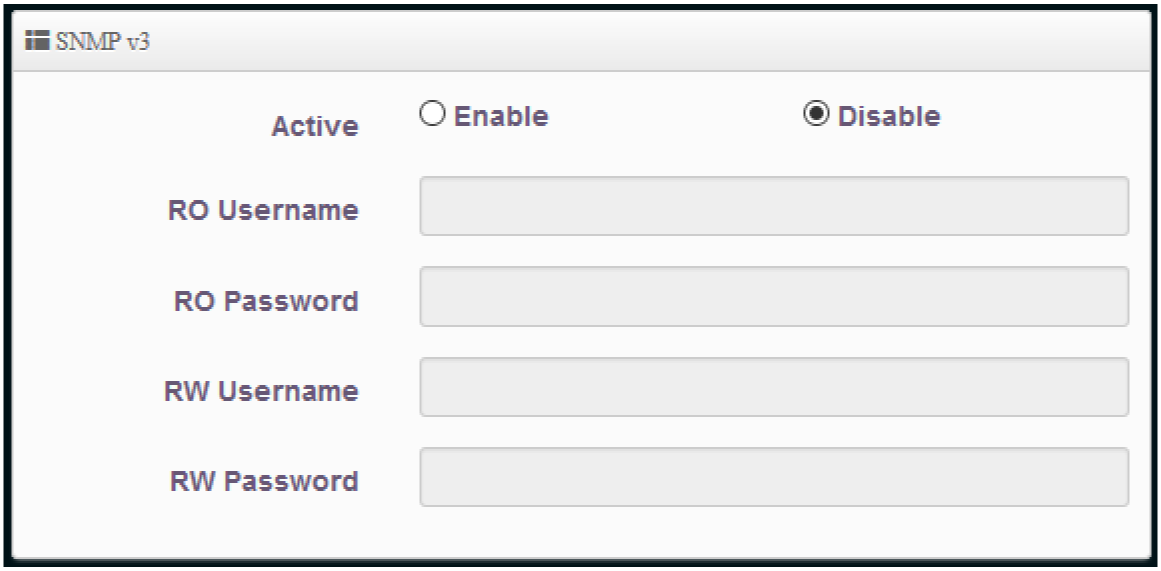
RW Community

RO Community: *Set a community string to authorize read-only access.*

RW Community: *Set a community string to authorize read/write access.*

SNMP v3 Enable

Check to enable SNMP v3. SNMP v3 supports the highest level SNMP security.



SNMP v3

Active ○ Enable ● Disable

RO Username

RO Password

RW Username

RW Password

RO Username: *Set a community string to authorize read-only access.*

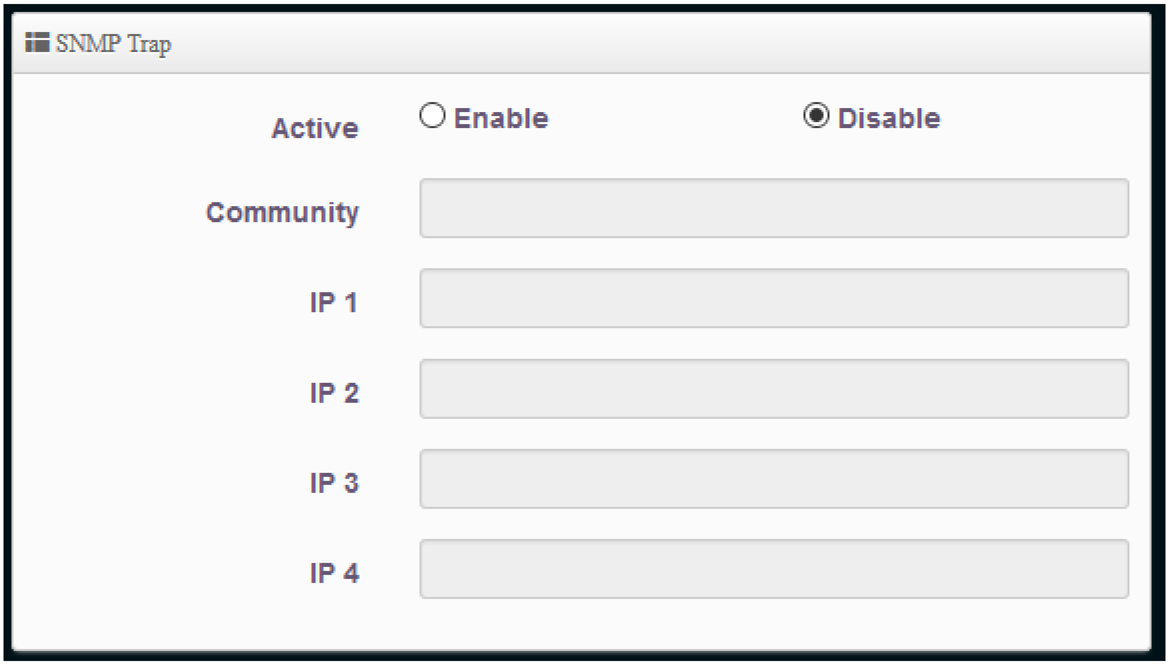
RO Password: *Set a password to authorize read-only access.*

RW User: *Set a community string to authorize read/write access.*

RW Password: *Set a password to authorize read/write access.*

SNMP Trap

Events such as cold start, interface up & down, and association & disassociation will report to an assigned server.



SNMP Trap

Active ○ Enable ● Disable

Community

IP 1

IP 2

IP 3

IP 4

Community: *Set a community string required by the remote host computer that will receive trap messages or notices send by the system.*

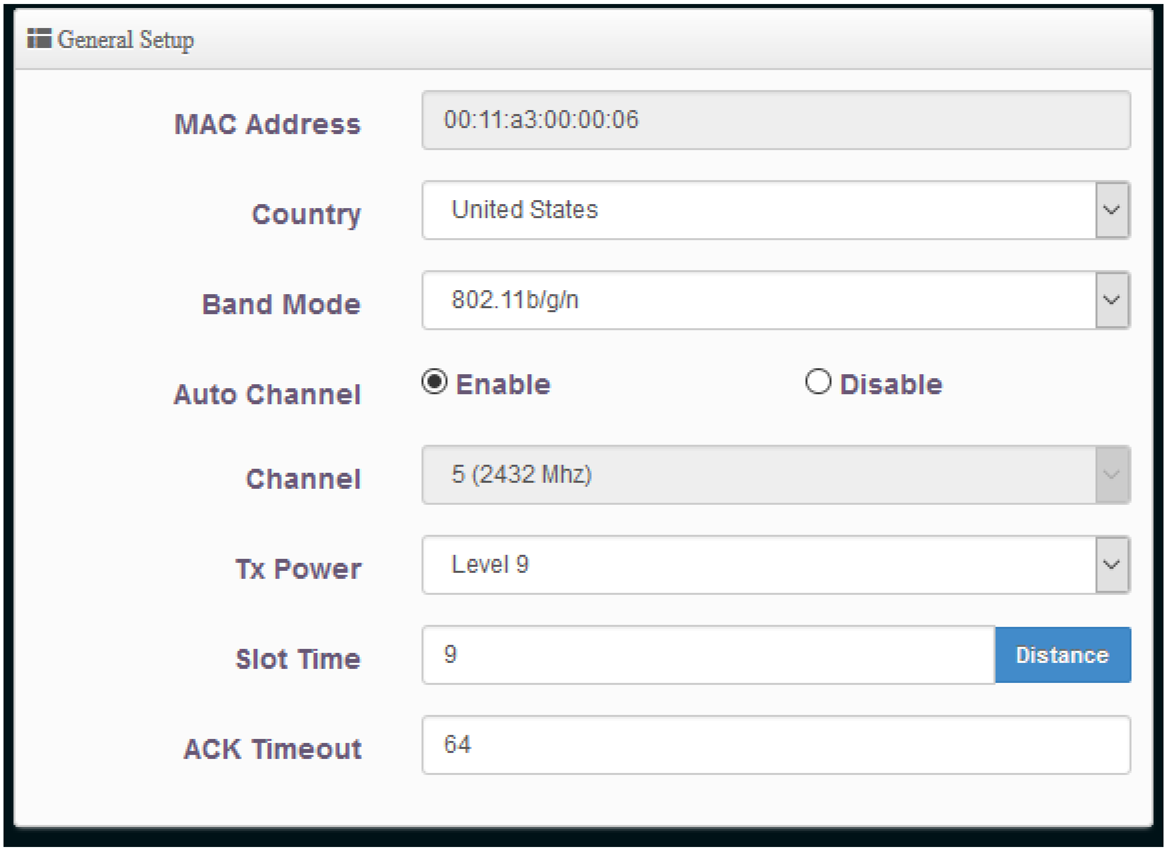
IP (1~4): *Enter the IP addresses of the remote hosts to receive trap messages.*

Chapter V: Wireless Setup

5-1 General Setup

This section allows you to set the data transmission, channel and output power for the system

5-1-1 Radio Basic Setup



General Setup

MAC Address: 00:11:a3:00:00:06

Country: United States

Band Mode: 802.11b/g/n

Auto Channel: ● Enable ○ Disable

Channel: 5 (2432 Mhz)

Tx Power: Level 9

Slot Time: 9

ACK Timeout: 64

MAC Address: *The MAC address of the Wireless interface is displayed here.*

Country: *This device only supports United States WiFi channels.*

Band Mode: *Please select the wireless band you wish to use. By selecting different band setting, you'll be able to allow or deny the wireless client of a certain band.*

*If you select 802.11b only wireless clients using the wireless band you select 802.11b will be able to connect to this access point. (*Maximum transfer rate 11Mbps)

*If you select 802.11b/g, then only wireless clients using 802.11b and 802.11g band will be able to connect to this access point. (*Maximum transfer rate 11Mbps for 802.11b clients, and maximum 54Mbps for 802.11g clients)

If you want to allow 802.11b, 802.11g, and 802.11n clients to connect to this access point, select 802.11b/g/n (Maximum transfer rate 11Mbps for 802.11b clients, maximum 54Mbps for 802.11g clients, and maximum 300Mbps for 802.11n clients*) (Default).*

*If you select 802.11n, the only wireless clients using 802.11n band will be able to connect to this access point. (M*aximum 300Mbps for 802.11n clients)

Auto Channel: *Enable/Disable the function. If disabled, the WiFi channel will be fixed to the manually selected channel.*

Channel: *Please select a channel from the dropdown list of 'Channel Number', You can choose any channel number you want to use, and almost all wireless clients can locate the channel you're using automatically without any problem. However, it's still useful to remember the channel number you use, as some wireless clients support manual channel number selecting, and this would help in certain scenarios when there are radio communication conflicts*

By default, it is on AUTO but if you have a specific channel you wish to use, you can select it here.

Tx Power: *You can adjust the output power of the access point to get the appropriate coverage for your wireless network. Specify power levels between level 1 and level 9. Level 9 is the maximum setting.*

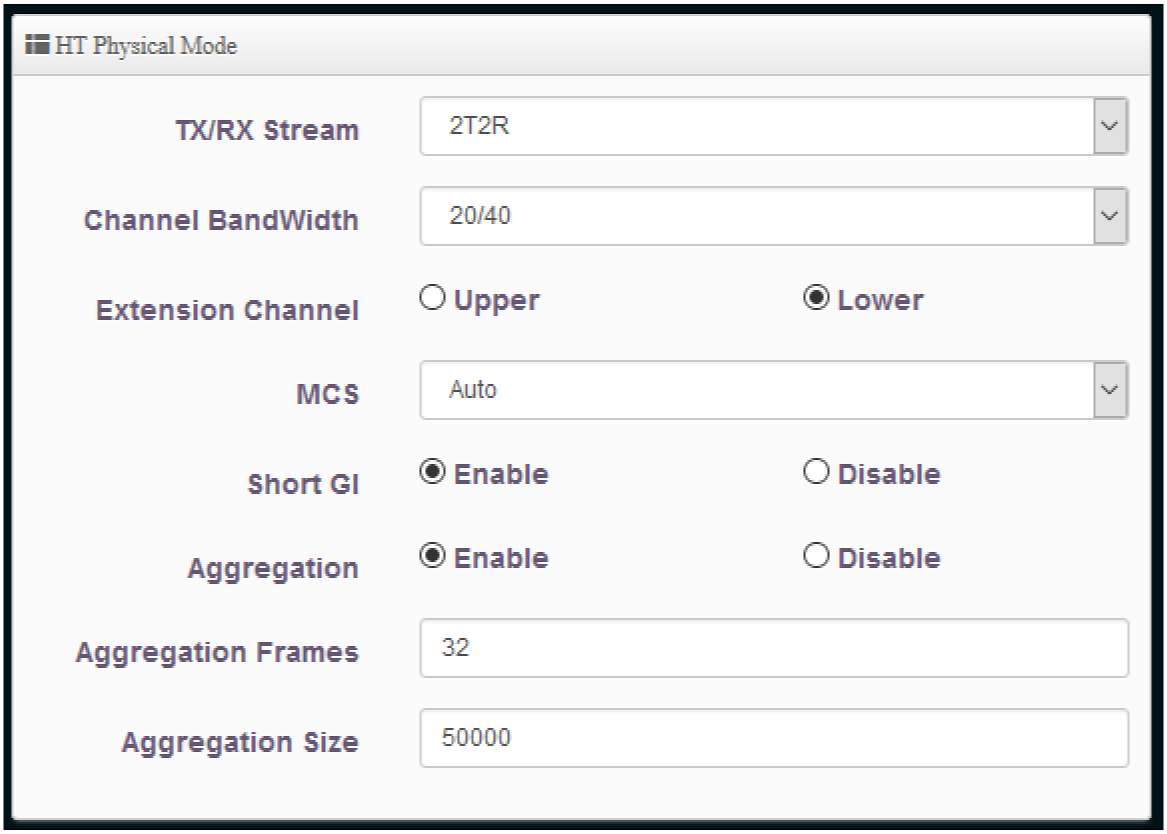
Slot Time: *Slot time is in the range of 9-1489ms. Default value is 9ms.*

Slot time is the amount of time a device waits after a collision before retransmitting a packet. Reducing the slot time decreases the overall back-off, which increases throughput. Back-off, which is a multiple of the slot time, is the random length of time a station waits before sending a packet on the LAN.

ACK Timeout: *ACK Timeout is in the range of 1-372ms. Default value is 64ms.*

All data transmissions in the 802.11b/g request an "Acknowledgement" (ACK) by the receiving radio. The transmitter will resend the original network packet if the ACK failed to arrive with the specified interval.

5-1-2 HT Physical Mode



HT Physical Mode

TX/RX Stream	2T2R	
Channel BandWidth	20/40	
Extension Channel	○ Upper	● Lower
MCS	Auto	
Short GI	● Enable	○ Disable
Aggregation	● Enable	○ Disable
Aggregation Frames	32	
Aggregation Size	50000	

Tx/Rx Stream: *2 is the default setting. Using 1 will halve your speed.*

Channel Bandwidth: *The "20/40" MHz option is usually best. The other option is available for special circumstances.*

Extension Channel: *Only for Channel Bandwidth "40" MHz. Select the desired channel bonding for control. Upper supports 1-7 and lower supports 5-11*

MCS: *This parameter represents transmission rate. By default (Auto) the fastest possible transmission rate will be selected. You have the option of selecting the speed if necessary.*

Shout GI: *Short Guard Interval, by default, it's "Enabled" so throughput can be increased. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.*

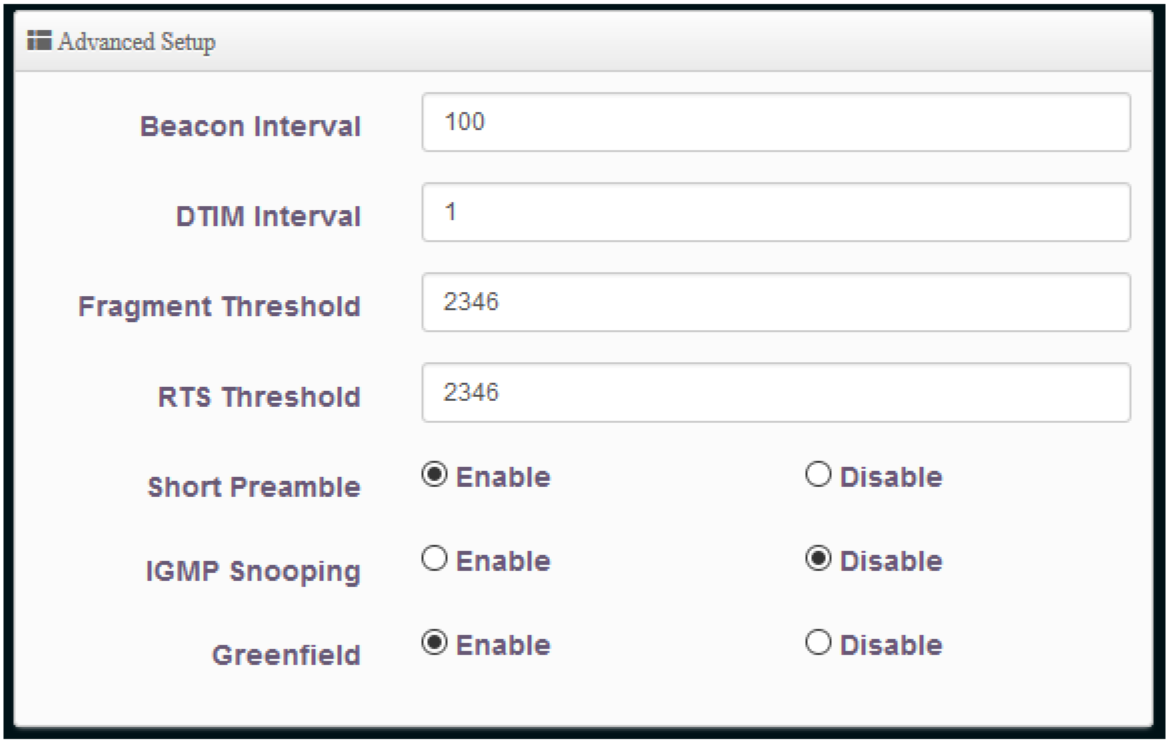
Aggregation: *By default, it's "Enable". It allows sending multiple frames per single access to the medium by combining frames together into one larger frame. It creates the larger frame by combining smaller frames with the same physical source and destination end points and traffic class (i.e. QoS) into one large frame with a common MAC header.*

Aggregation Frames: *The Aggregation Frames is in the range of 2~64, default is 32. It determines the number of frames combined on the new larger frame.*

Aggregation Size: *The Aggregation Size is in the range of 1024~65535, default is 50000. It determines the size (in Bytes) of the larger frame.*

5-2 Advanced Settings

The administrator can change the Slot Time, ACK Timeout, RTS threshold and fragmentation threshold settings for the system



Advanced Setup

Beacon Interval	100	
DTIM Interval	1	
Fragment Threshold	2346	
RTS Threshold	2346	
Short Preamble	● Enable	○ Disable
IGMP Snooping	○ Enable	● Disable
Greenfield	● Enable	○ Disable

Beacon Interval: *Beacon Interval is in the range of 40~3500 and set in unit of millisecond. The default value is 100 msec. Access Point (AP) in IEEE 802.11 will send out a special approximated 50-byte frame, called "Beacon". Beacon is broadcast to all the stations, provides the basic information of AP such as SSID, channel, encryption keys, signal strength, time stamp, support data rate. All the radio stations received beacon recognizes the existence of such AP, and may proceed to the next actions if the information from AP matches the requirement. Beacon is sent on a periodic basis. The time interval can be adjusted. By increasing the beacon interval, you can reduce the number of beacons and associated overhead, but that will likely delay the association and roaming process because stations scanning for available access points may miss the beacons. You can decrease the beacon interval, which increases the rate of beacons. This will make the association and roaming process very responsive; however, the network will incur additional overhead and throughput will go down.*

DTIM Interval: *The DTIM interval is in the range of 1~255. The default is 1. DTIM is defined as Delivery Traffic Indication Message. It is used to notify the wireless stations,* *which support power saving mode, when to wake up to receive multicast frame. DTIM is necessary and critical in wireless environment as a mechanism to fulfill power-saving synchronization.*

A DTIM interval is a count of the number of beacon frames that must occur before the access point sends the buffered multicast frames. For instance, if DTIM Interval is set to 3, then the Wi-Fi clients will expect to receive a multicast frame after receiving three Beacon frame. The higher DTIM interval will help power saving and possibly decrease wireless throughput in multicast applications.

Fragment Threshold: *Set the fragment threshold of the wireless radio. The default value is 2346.*

RTS Threshold: *RTS Threshold is in the range of 1~2347 byte. The default is 2347 byte. The main purpose of enabling RTS by changing RTS threshold is to reduce possible collisions due to hidden wireless clients. RTS in AP will be enabled automatically if the packet size is larger than the Threshold value. By default, RTS is disabled in a normal environment supports non-jumbo frames.*

Short Preamble: *By default, its set to “Enabled”. If Disabled, the device will use Long 128-bit Preamble Synchronization field. The preamble is used to signal "here is a train of data coming" to the receiver. The short preamble provides 72-bit Synchronization field to improve WLAN transmission efficiency with less overhead.*

IGMP Snooping: *The process of listening to Internet Group Management Protocol (IGMP) network traffic. The feature allows a network switch to listen in on the IGMP conversation between hosts and routers. By listening to these conversations the switch maintains a map of which links need which IP multicast streams. Multicasts may be filtered from the links which do not need them and thus controls which ports receive specific multicast traffic.*

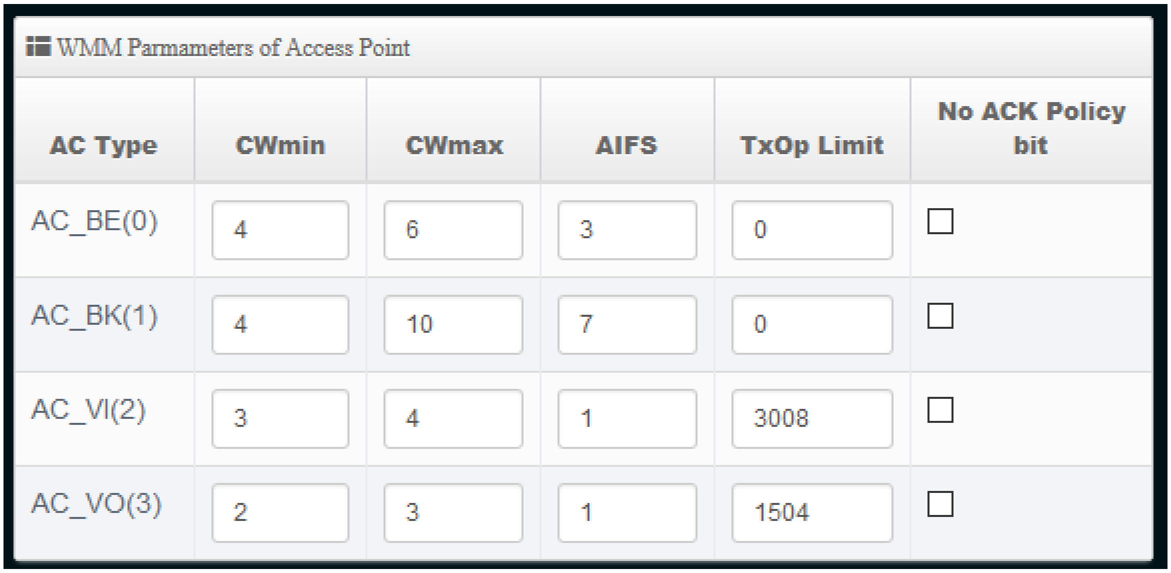
Greenfield: *In wireless WLAN technology, greenfield mode is a feature of major components of the 802.11n specification. The greenfield mode feature is designed to improve efficiency by eliminating support for 802.11b/g devices in an all draft-n network. In greenfield mode the network can be set to ignore all earlier standards.*

5-3 WMM QoS

This affects traffic flowing from the access point to the client station. Configuring QoS options consists of setting parameters on existing queues for different types of wireless traffic. You can configure different minimum and maximum wait times for the transmission of packets in each queue based on the requirements of the media being sent. Queues automatically provide minimum transmission delay for Voice, Video, multimedia, and mission critical applications, and rely on best-effort parameters for traditional IP data.

As an Example, time-sensitive Voice & Video, and multimedia are given effectively higher priority for transmission (lower wait times for channel access), while other applications and traditional IP data which are less time-sensitive but often more data-intensive are expected to tolerate longer wait times.

High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example). Medium throughput and delay. Most traditional IP data is sent to this queue. Minimum delay. Time-sensitive video data is automatically sent to this queue. Time-sensitive data like VoIP and streaming media are automatically sent to this queue.



WMM Parmameters of Access Point

AC Type	CWmin	CWmax	AIFS	TxOp Limit	No ACK Policy bit
AC_BE(0)	4	6	3	0	□
AC_BK(1)	4	10	7	0	□
AC_VI(2)	3	4	1	3008	□
AC_VO(3)	2	3	1	1504	□

CWmin: *Determines the initial random backoff wait time ("window") for retry of a transmission. The value specified here in the Minimum Contention Window is the upper limit (in milliseconds) of a range from which the initial random backoff wait time is determined.*

CWmax: *Maximum Contention Window. The value specified here in the Maximum Contention Window is the upper limit (in milliseconds) for the doubling of the random backoff value. This doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, or 1024. The value for "cwmax" must be higher than the value for "cwmin".*

AIFS *The Arbitration Inter-Frame Spacing Number specifies a wait time (in milliseconds) for data frames*

TxOP Limit *Transmission Opportunity is an interval of time when a WME AP has the right to initiate transmissions onto the wireless medium (WM). This value specifies (in milliseconds) the Transmission Opportunity (TXOP) for AP; that is, the interval of time when the WMM AP has the right to initiate transmissions on the wireless network.*

ACM bit: *Admission Control Mandatory, ACM only takes effect on AC_VI and AC_VO. When you do not click Checkbox, it means that the ACM is controlled by the connecting AP. If you click Checkbox, it means that the Client is in charge*

No ACK policy bit: *Acknowledgment Policy, WMM defines two ACK policies: Normal ACK and No ACK. Click "Checkbox" indicates "No ACK"*

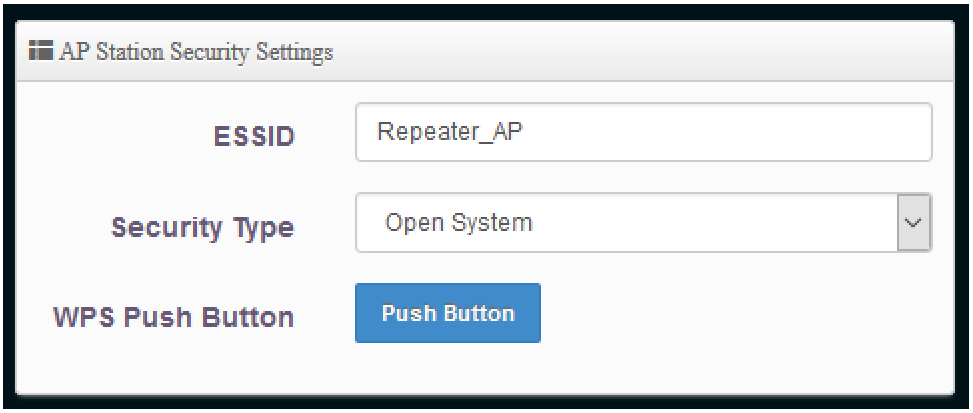
When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak. While the No ACK policy helps improve transmission efficiency, it can cause increased packet loss when communication quality deteriorates. This is because when this policy is used, a sender does not retransmit packets that have not been received by the recipient. When the Normal ACK policy is used, the recipient acknowledges each received uncast packet.

5-4 Station Setup

The network manager can configure related wireless settings, **AP Setup**, **Security Settings**, and **Access Control Settings**.

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations, security type settings and MAC Filter settings. (This feature is only available in Client Bridge + Repeater and WISP Modes)

5-4-1 AP Station Security Settings



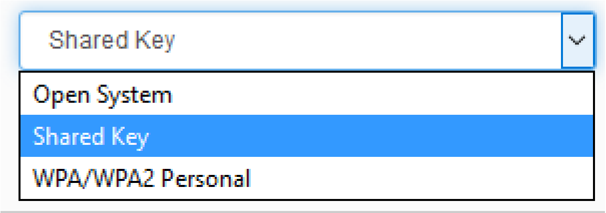
ESSID: Repeater_AP

Security Type: Open System

WPS Push Button

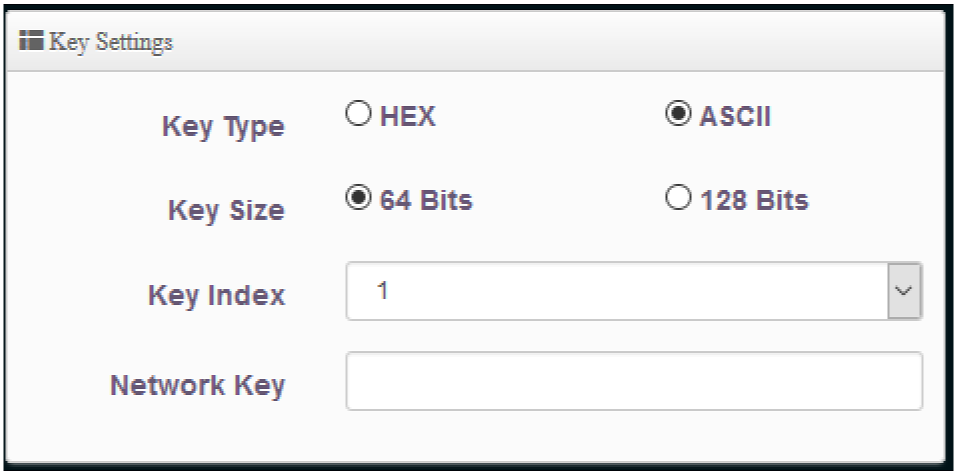
ESSID: *Extended Service Set ID. In station mode, this should be the network you are connecting to.*

Security Type: *Select the desired security type from the drop-down list; the options are Open System, Shared Key, WPA/WPA2 Personal. Setting should match the network being connected to.*



Open System: Data are unencrypted during transmission when this option is selected.

Shared Key: WEP, Wired Equivalent Privacy, is a data encryption mechanism based on a 64-bit, or 128-bit. Select Shared Key as the security type from the drop down list as desired.



Key Settings

Key Type ○ HEX ● ASCII

Key Size ● 64 Bits ○ 128 Bits

Key Index 1

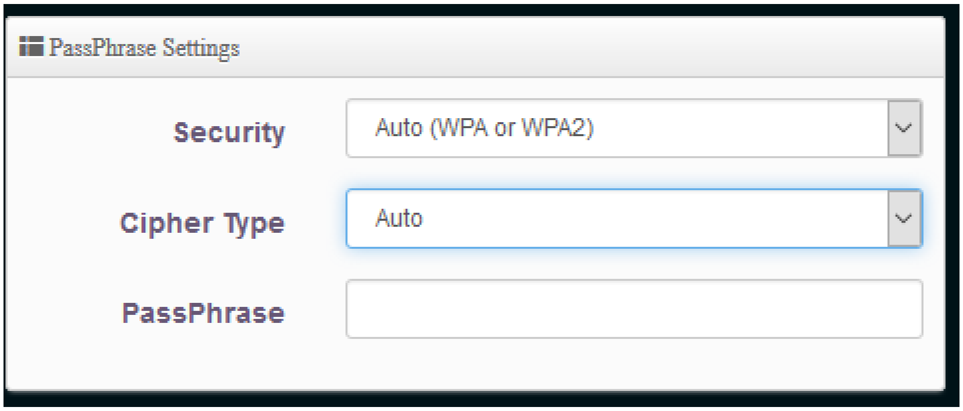
Network Key

Key Size: The key size of WEP encryption can be 64bit, 128bit.

Key Index: You can select the Key which you want to use. Other wireless station must have the same key value to connect with the device, 4 different WEP keys can be configured at the same time, but only one is used. Effective key is set with a choice of WEP Key 1, 2, 3 or 4.

Network Key #: You can chose either HEX or ASCII for your WEP key value, for 64bit encryption strength can use 10 digits for HEX (0~9, a~f and A-F) or 5 digits for ASCII (0~9, a~z and A~Z), for 128bit encryption strength can use 26 digits for HEX (0~9, a~f and A-F) or 13 digits for ASCII (0~9, a~z and A~Z), for 152bit encryption strength can use 32 digits for HEX (0~9, a~f and A-F) or 16 digits for ASCII (0~9, a~z and A~Z)

WPA-PSK (or WPA2-PSK): WPA-PSK is short for W-Fi Protected Access-Pre-Shared Key. WPA-SPK uses the same encryption way with WPA, and the only difference between them is that WPA-PSK recreates a simple shared key, instead of using the user's certification.



PassPhrase Settings

Security: Auto (WPA or WPA2)

Cipher Type: Auto

PassPhrase:

Cipher Type: You can chose use AES or TKIP with your WPA / WPA2 encryption method

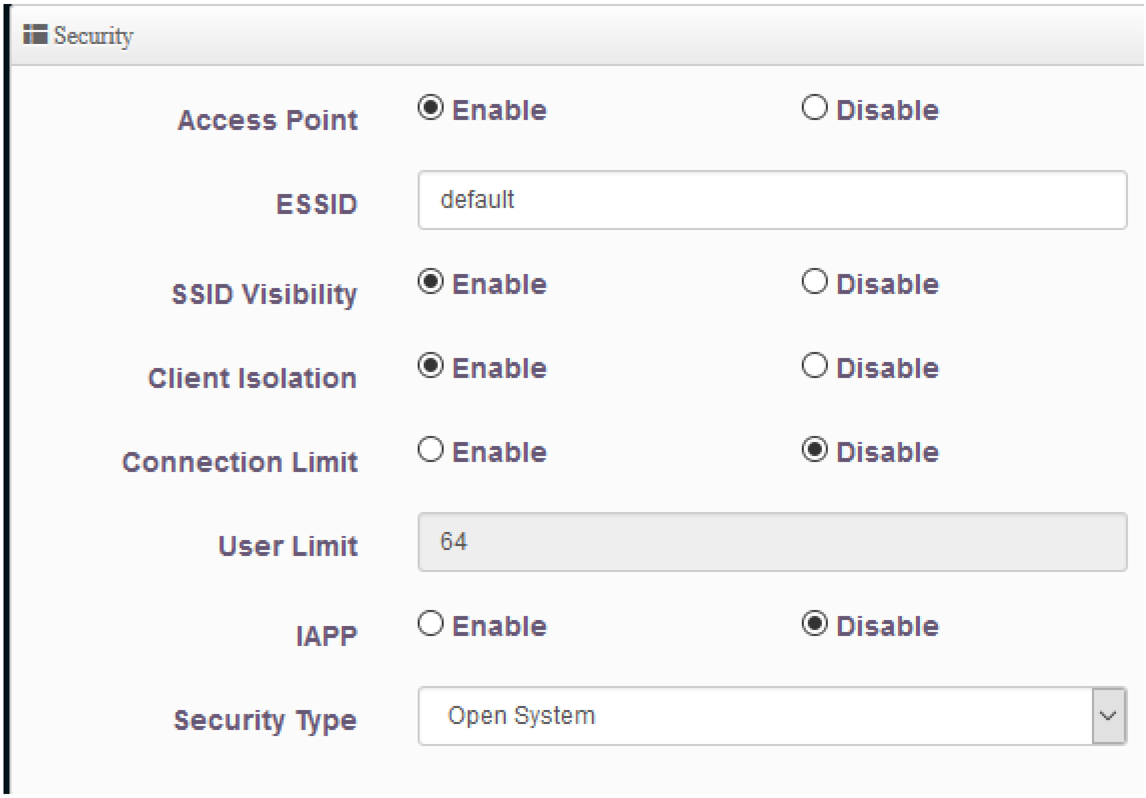
AES is short for Advanced Encryption Standard. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for "Temporal Key Integrity Protocol. TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

PassPhrase: Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

5-5 Repeater AP Setup

Settings for Repeater. (This feature is only available in Client Bridge + Repeater and WISP Modes)



Security

Access Point ● Enable ○ Disable

ESSID default

SSID Visibility ● Enable ○ Disable

Client Isolation ● Enable ○ Disable

Connection Limit ○ Enable ● Disable

User Limit 64

IAPP ○ Enable ● Disable

Security Type Open System

Access Point: *Choose Enable or Disable Repeater AP function, the default is Disable*

ESSID: *Extended Service Set ID. When users are browsing for available wireless networks, this is the SSID that will appear in the list..*

SSID Visibility: *By default, it is "Disable". Enable this option to stop the SSID broadcast in your network. When disabled, people could easily obtain the SSID information with the site survey software and get access to the network if security is not turned on. When enabled, network security is enhanced.*

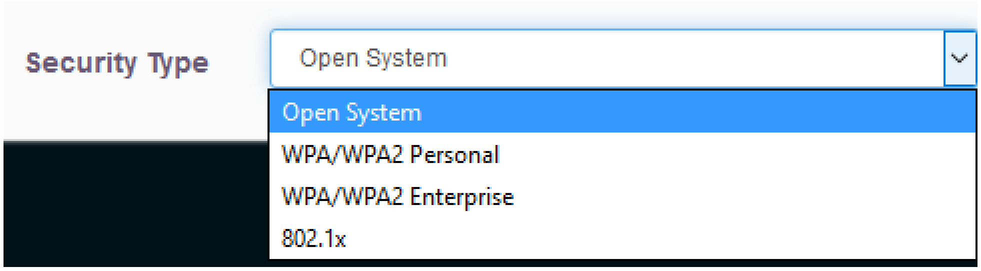
Client Isolation: *By default, it is "Disable". Select "Enable", all clients will be isolated from each other, which means they cannot reach each other.*

Connection Limit: *Enable/Disable user limits.*

User Limits: *The default value is 64. You can enter the number of wireless clients that can associate to a particular SSID. When the number of client is set to 5, only 5 clients at most are allowed to connect to this VAP.*

IAPP: *Enable/Disable for IAPP roaming. IAPP condition must use WPA-2PSK AES security*

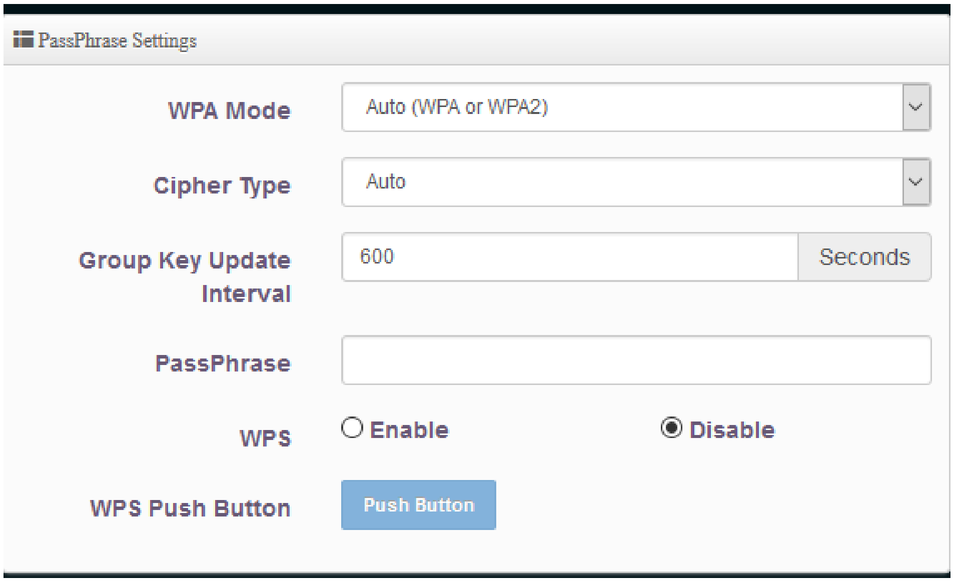
Authentication: *Select the desired security type from the drop-down list; the options are Open,, WPA-PSK/WPA2-PSK Personal, WPA/WPA2-Enterprise and WEP 802.1X.*



Security Type: Open System

Open System: Data are unencrypted during transmission when this option is selected.

WPA-PSK (or WPA2-PSK): WPA-PSK is short for W-Fi Protected Access-Pre-Shared Key. WPA-SPK uses the same encryption way with WPA, and the only difference between them is that WPA-PSK recreates a simple shared key, instead of using the user’s certification.



PassPhrase Settings

WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
Group Key Update Interval	600 Seconds
PassPhrase	
WPS	○ Enable ● Disable
WPS Push Button	Push Button

Cipher Type: You can chose use AES or TKIP with your WPA / WPA2 encryption method,

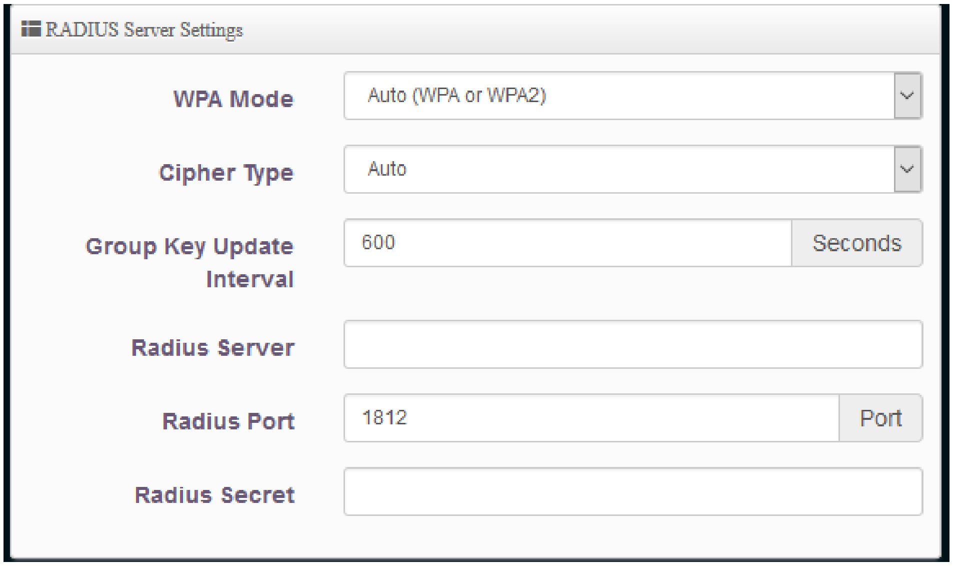
AES is short for Advanced Encryption Standard. The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for "Temporal Key Integrity Protocol. TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

Group Key Update Period: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

Passphrase: Enter the information for pre-shared key; the format of the information shall according to the key type selected. Pre-shared key can be either entered as a 256-bit secret in 64 HEX digits format, or 8 to 63 ASCII characters.

WPA-Enterprise (or WPA2-Enterprise) General Setting The RADIUS authentication and encryption will be both enabled if this selected.



RADIUS Server Settings

WPA Mode	Auto (WPA or WPA2)
Cipher Type	Auto
Group Key Update Interval	600 Seconds
Radius Server	
Radius Port	1812 Port
Radius Secret	

Cipher Type: You can chose use AES or TKIP with your WPA / WPA2 encryption method,

AES is short for "Advanced Encryption Standard", The AES cipher is specified as a number of repetitions of transformation rounds that convert the input plaintext into the final output of ciphertext. Each round consists of several processing steps, including one that depends on the encryption key. A set of reverse rounds are applied to transform ciphertext back into the original plaintext using the same encryption key.

TKIP is short for "Temporal Key Integrity Protocol", TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.

Group Key Update Interval: This time interval for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.

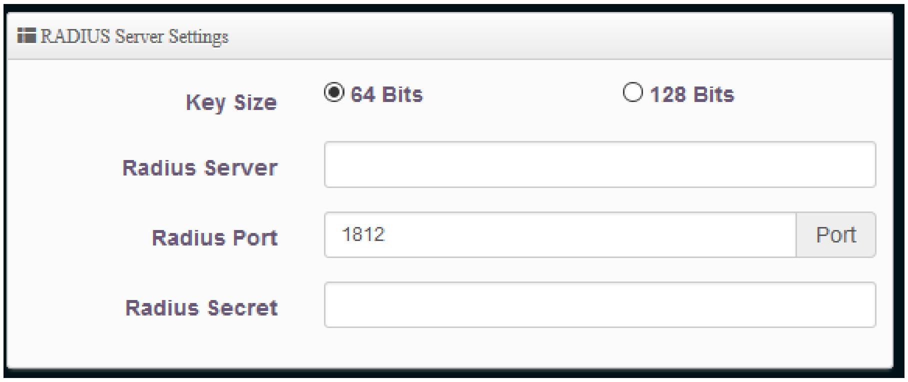
Authentication RADIUS Server Settings

Radius Server: Enter the IP address of the Authentication RADIUS server.

Radius Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Radius Secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

WEP 802.1x: When WEP 802.1x Authentication is enabled, please refer to the following Dynamic WEP and RADIUS settings to complete the configuration.



RADIUS Server Settings

Key Size ● 64 Bits ○ 128 Bits

Radius Server

Radius Port 1812 Port

Radius Secret

Key Size: Check on the respected button to enable either 64bits or 128bits key length. The system will automatically generate WEP keys for encryption.

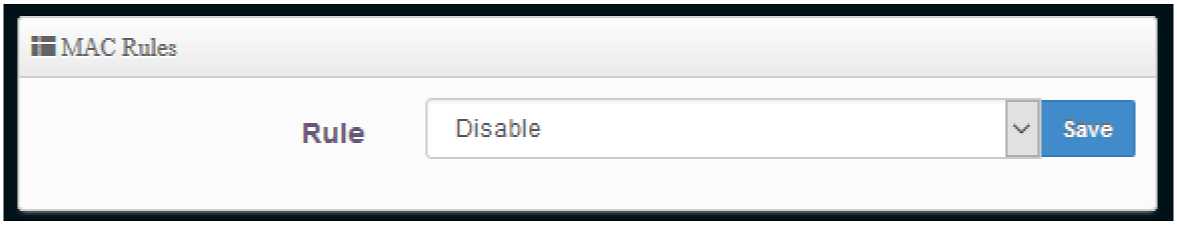
Radius Server: Enter the IP address of the Authentication RADIUS server.

Radius Port: The port number used by Authentication RADIUS server. Use the default 1812 or enter port number specified.

Radius Secret: The secret key for system to communicate with Authentication RADIUS server. Support 1 to 64 characters.

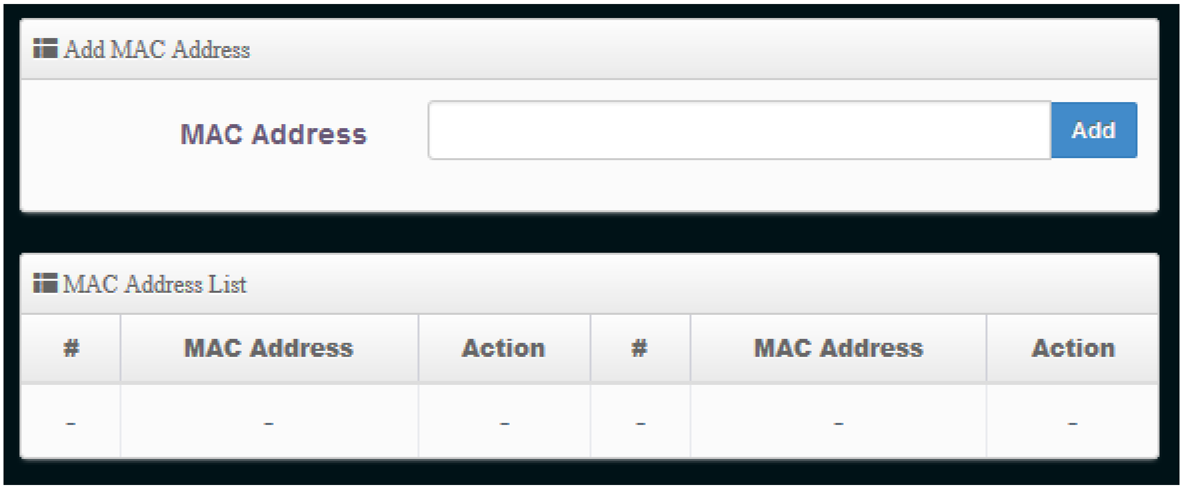
5-6 Repeater AP MAC Filter

For each Repeater AP, users can allow or reject clients based on their MAC address. Click on Wireless, Repeater AP MAC Filter Setup. (This feature is only available in Client Bridge + Repeater AP and WISP Modes)



MAC Rules

Rule: Disable



Add MAC Address

MAC Address:

MAC Address List

#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

Action: *Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.*

Only Allow List MAC: Define certain wireless clients in the list which will have granted access to the Access Point while the access will be denied for all the remaining clients – Action Type is set to "Only Allow List MAC".

Only Deny List MAC: Define certain wireless clients in the list which will have denied access to the Access Point while the access will be granted for all the remaining clients - Action Type is set to "Only Deny List MAC". MAC Access Control is the weakest security approach. WPA or WPA2 security methods should be used when possible.

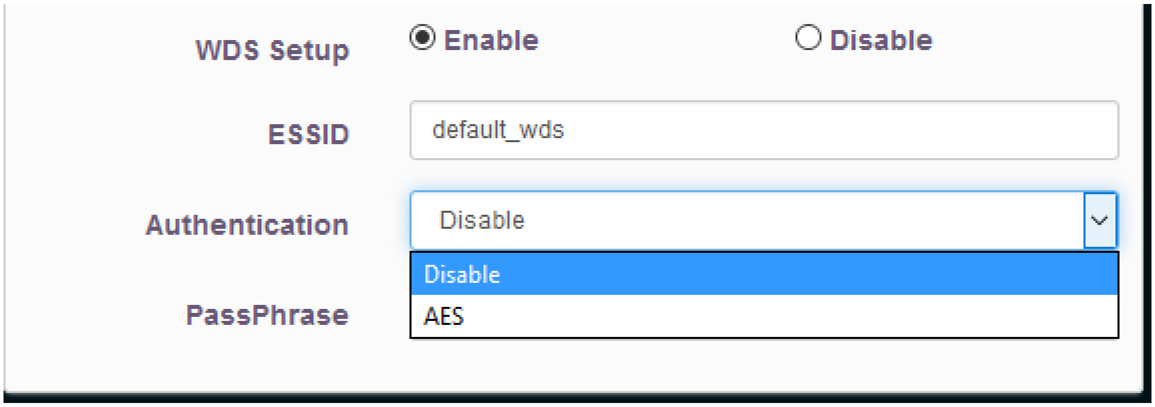
Mac Address: *Type in the Mac address of the client you wish to add under the Mac filter.*

5-7 WDS Setup

The administrator could create WDS Links to expand wireless network. When WDS is enabled, access point functions as a wireless bridge and is able to communicate with other access points via WDS links. **A**

WDS link is bidirectional and both side must support WDS. Access points know each other by MAC Address. In other words, each access point needs to include MAC address of its peer. Ensure all access points are configured with the same channel and own same security type settings. (This feature is only available in AP Mode)

Security Type: *Option is "Disable", "WEP", "TKIP" or "AES" from drop-down list.*



WDS Setup ● Enable ○ Disable

ESSID: default_wds

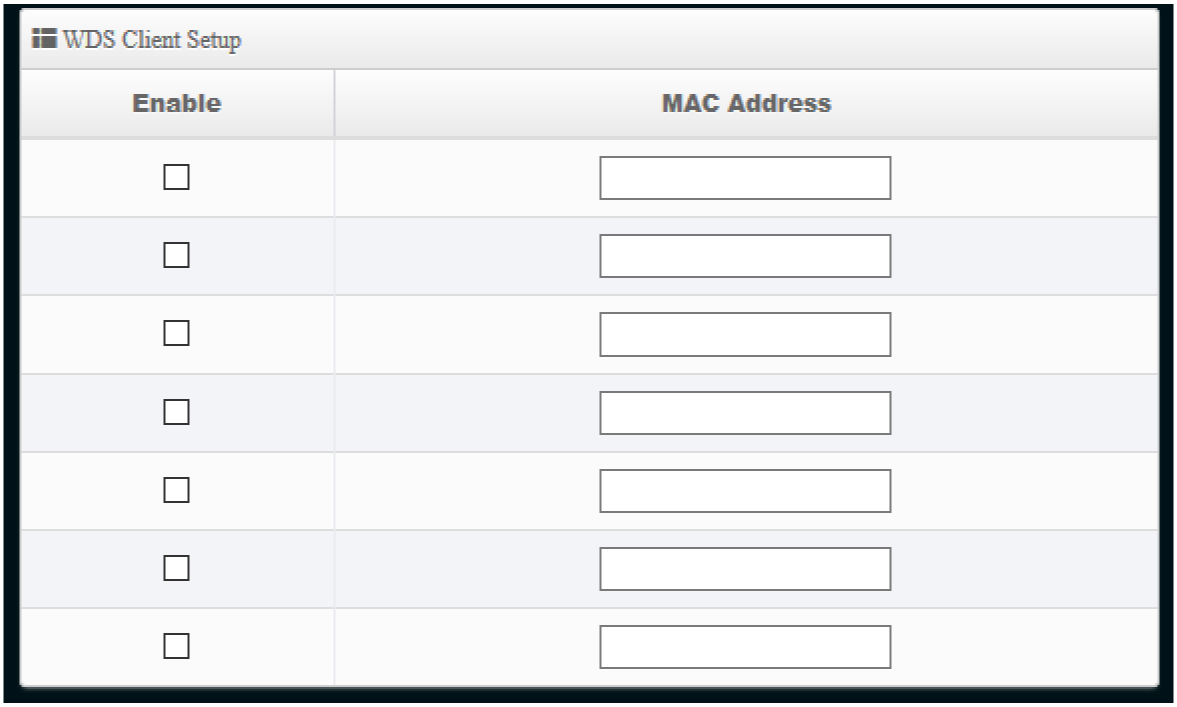
Authentication: Disable

- Disable
- AES

PassPhrase

AES Key: *Enter 8 to 63 ASCII or 64 HEX format AES key.*

Note that the security key must be the same on all WDS Peer Devices in order to build WDS links. Security type takes effect when WDS is enabled.



WDS Client Setup

Enable	MAC Address
□	
□	
□	
□	
□	
□	
□	

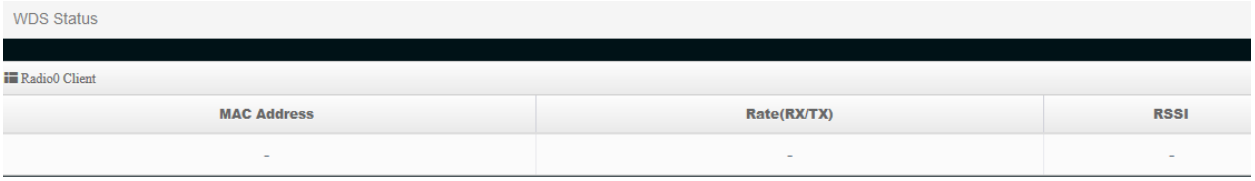
WDS MAC List Enable: *Check "Enable" to create WDS link.*

WDS Peer's MAC Address: *Enter the MAC address of WDS peer.*

Note: All WDS peers need to have same WiFi Channel and same Security Type.

5-8 WDS Status

This page shows the status of each WDS enabled device on the network. (This feature is only available in AP Mode)



WDS Status

Radio0 Client

MAC Address	Rate(RX/TX)	RSSI
-	-	-

MAC Address: *Display MAC address of WDS devices.*

RSSI: *Indicate the RSSI of the respective WDS's link.*

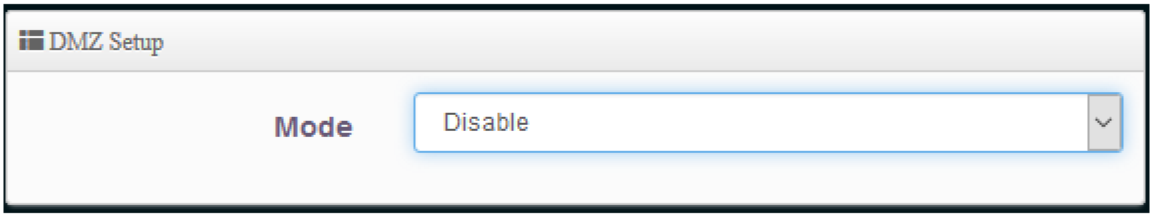
TX/RX Rate: *Indicate the TX/RX Rate of the respective WDS's link*

Disconnect: *Administrator can kick out a specific client, click “Delete” button to kick out specific WDS's link.*

Chapter VI: Advanced Settings

6-1 DMZ

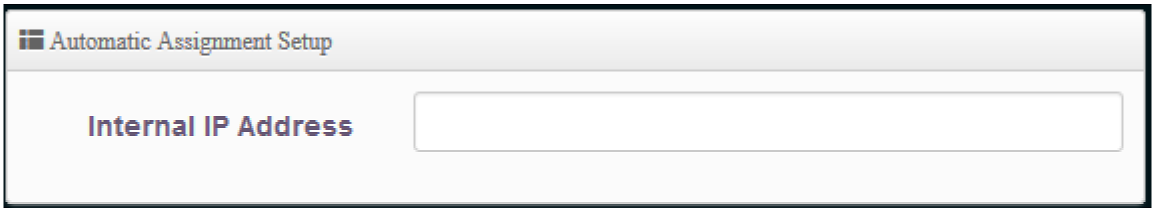
DMZ is a setting associated with NAT functionality and is an alternative to setting up a Virtual Server (Port Forwarding). This feature opens all ports of DMZ host to internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to different internal hosts, Virtual Server rules should be used. (This feature is only available in Router and WISP Modes)



DMZ Setup

Mode: Disable

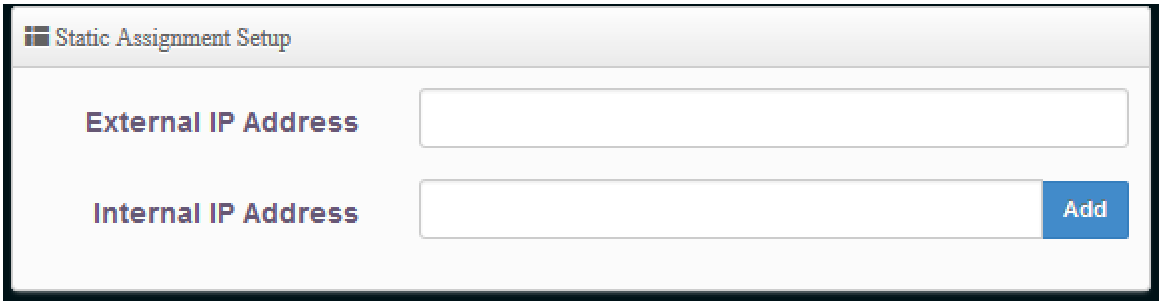
Service: *The DMZ is disabled by default. Chose an option to enable DMZ.*



Automatic Assignment Setup

Internal IP Address:

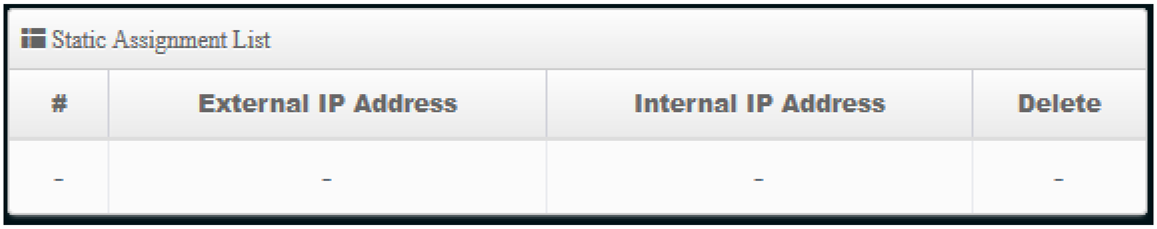
Automatic Assignment: *Enter Internal IP address of DMZ host. Only one DMZ host is supported.*



Static Assignment Setup

External IP Address:

Internal IP Address:



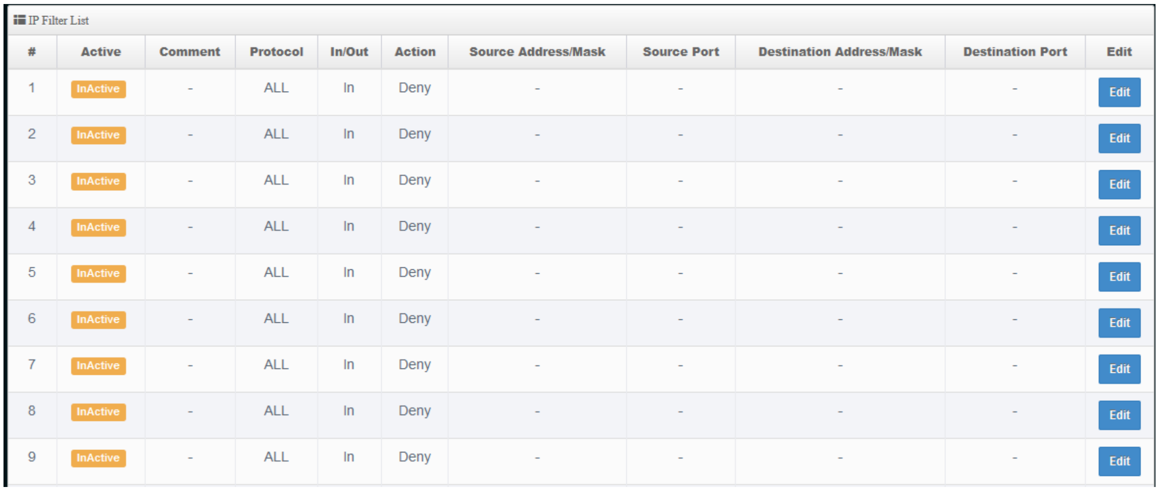
Static Assignment List

#	External IP Address	Internal IP Address	Delete
-	-	-	-

Static Assignment: *Enter external and internal IP address of DMZ host. This will map one external IP to one internal IP of the DMZ host.*

6-2 IP Filter

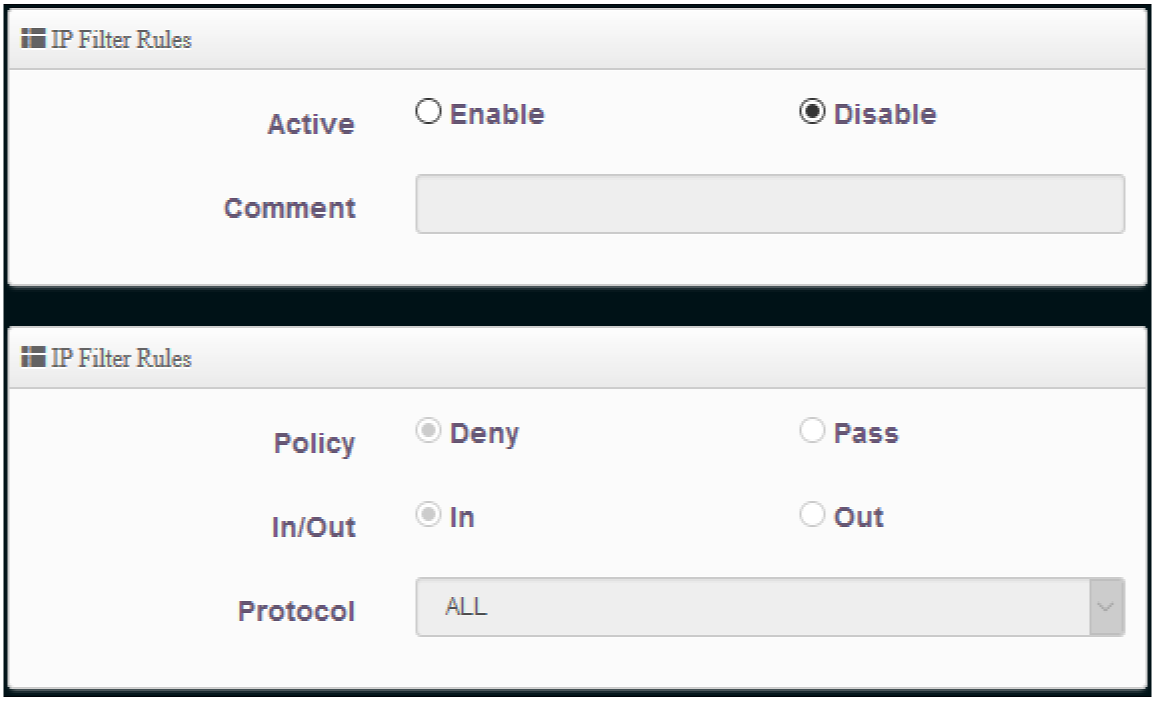
Allows users to create deny or allow rules to filter ingress or egress packets from specific source and/or to destination IP address on wired (LAN) or Wireless (WAN) ports. Filter rules could be used to filter unicast or multicast packets on different protocols as shown in the IP Filter Setup. Important to note that IP filter rules has precedence over Virtual server rules. (This feature is only available in Router and WISP Modes)



IP Filter List

#	Active	Comment	Protocol	In/Out	Action	Source Address/Mask	Source Port	Destination Address/Mask	Destination Port	Edit
1	InActive	-	ALL	In	Deny	-	-	-	-	Edit
2	InActive	-	ALL	In	Deny	-	-	-	-	Edit
3	InActive	-	ALL	In	Deny	-	-	-	-	Edit
4	InActive	-	ALL	In	Deny	-	-	-	-	Edit
5	InActive	-	ALL	In	Deny	-	-	-	-	Edit
6	InActive	-	ALL	In	Deny	-	-	-	-	Edit
7	InActive	-	ALL	In	Deny	-	-	-	-	Edit
8	InActive	-	ALL	In	Deny	-	-	-	-	Edit
9	InActive	-	ALL	In	Deny	-	-	-	-	Edit

Click Edit to configure/edit a rule.

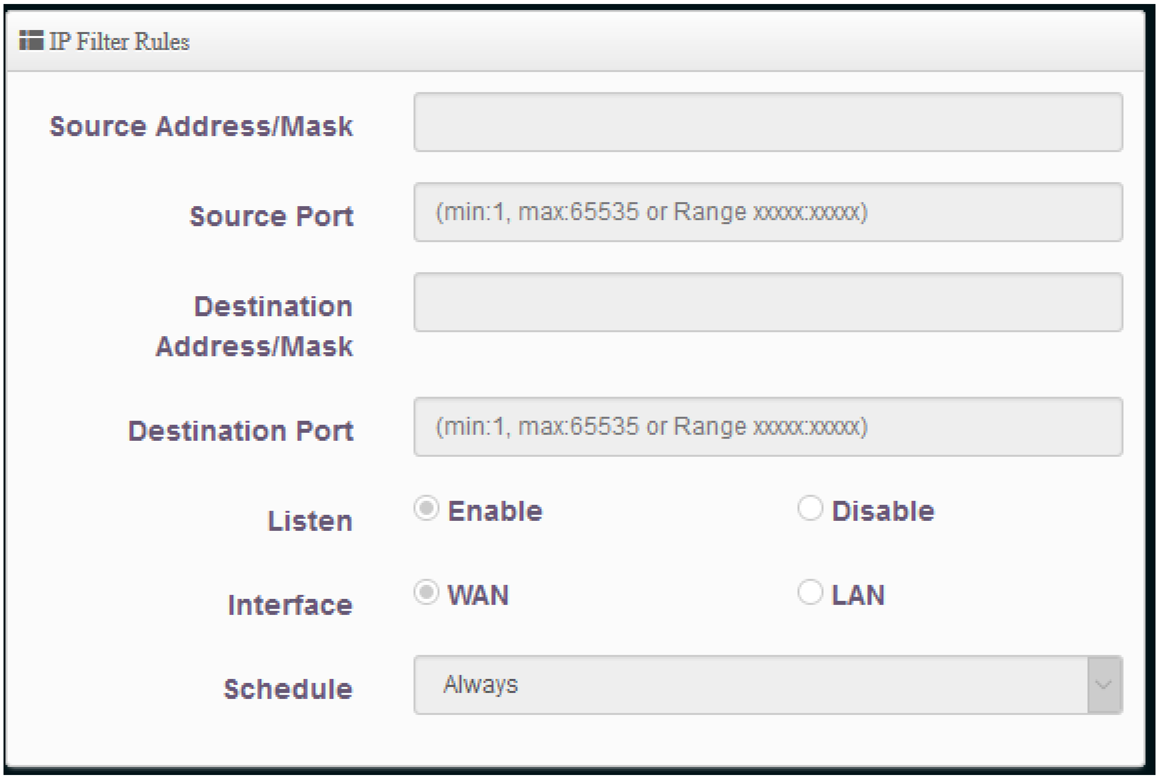


IP Filter Rules

Active	○ Enable	● Disable
Comment		

IP Filter Rules

Policy	● Deny	○ Pass
In/Out	● In	○ Out
Protocol	ALL	



IP Filter Rules

Source Address/Mask

Source Port (min:1, max:65535 or Range xxxxx:xxxxx)

Destination Address/Mask

Destination Port (min:1, max:65535 or Range xxxxx:xxxxx)

Listen ● Enable ○ Disable

Interface ● WAN ○ LAN

Schedule Always

Policy: *Deny to drop and Pass to allow per filter rules*

In/Out: *Applies to Ingress or egress packets.*

Protocol: *Supports TCP, UDP or ICMP.*

Source Address/Mask: *Enter desired source IP address and netmask. i.e. 192.168.2.10/32.*

Source Port: *Enter a port or a range of ports as start:end. i.e. port 20:80*

Destination Address/Mask: *Enter desired destination IP address and netmask. i.e. 192.168.1.10/32*

Destination Port: *Enter a port or a range of ports as start:end. i.e. port 20:80*

Listen: *Click Yes radial button to match TCP packets only with the SYN flag.*

Interface: *The interface that a filter rule applies*

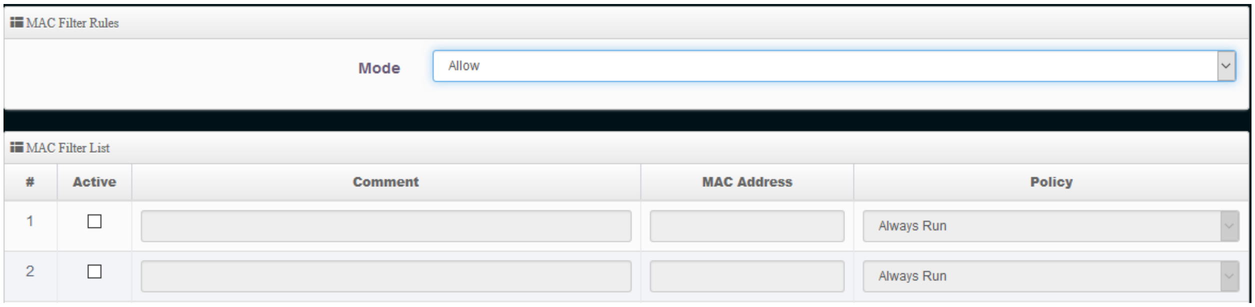
Schedule: *Can choose to use rule by “Time Policy”*

All packets are allowed by default. Deny rules could be added to the filter list to filter out unwanted packets and leave remaining allowed.

Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. When you create rules in the IP Filter List, the prior rules maintain higher priority. To allow limited access from a subnet to a destination network manager needs to create allow rules first and followed by deny rules.

6-3 MAC Filter

Allows users to create MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. That MAC filter rules have precedence over IP Filter rules. (This feature is only available in Router and WISP Modes)



MAC Filter Rules

Mode: Allow

MAC Filter List

#	Active	Comment	MAC Address	Policy
1	□			Always Run
2	□			Always Run

MAC Filter Mode: *Disable is the default setting. Options are Disabled, Only Deny List MAC or Only Allow List MAC.*

Only Allow List MAC: The wireless clients in the MAC Filter List will be allowed to access to Access Point; All others will be denied.

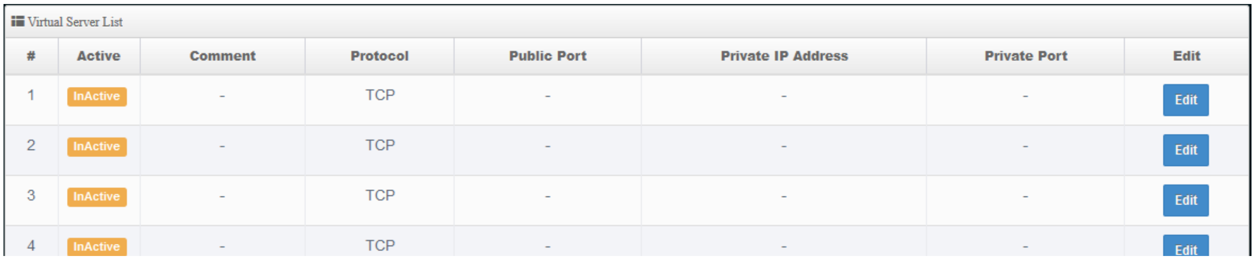
Only Deny List MAC The wireless clients in the MAC Filter List will be denied to access to Access Point; All others will be allowed.

MAC Address: *Enter MAC address (e.g. aa:bb:cc:dd:ee:ff) and click "Add". The MAC address should display in the MAC Filter List. There are a maximum of 20 clients allowed in this MAC Filter List. The MAC addresses of the wireless clients can be added and removed to the list using the Add and Delete buttons.*

Policy: *Can choose to use rule by "Time Policy"*

6-4 Virtual Server

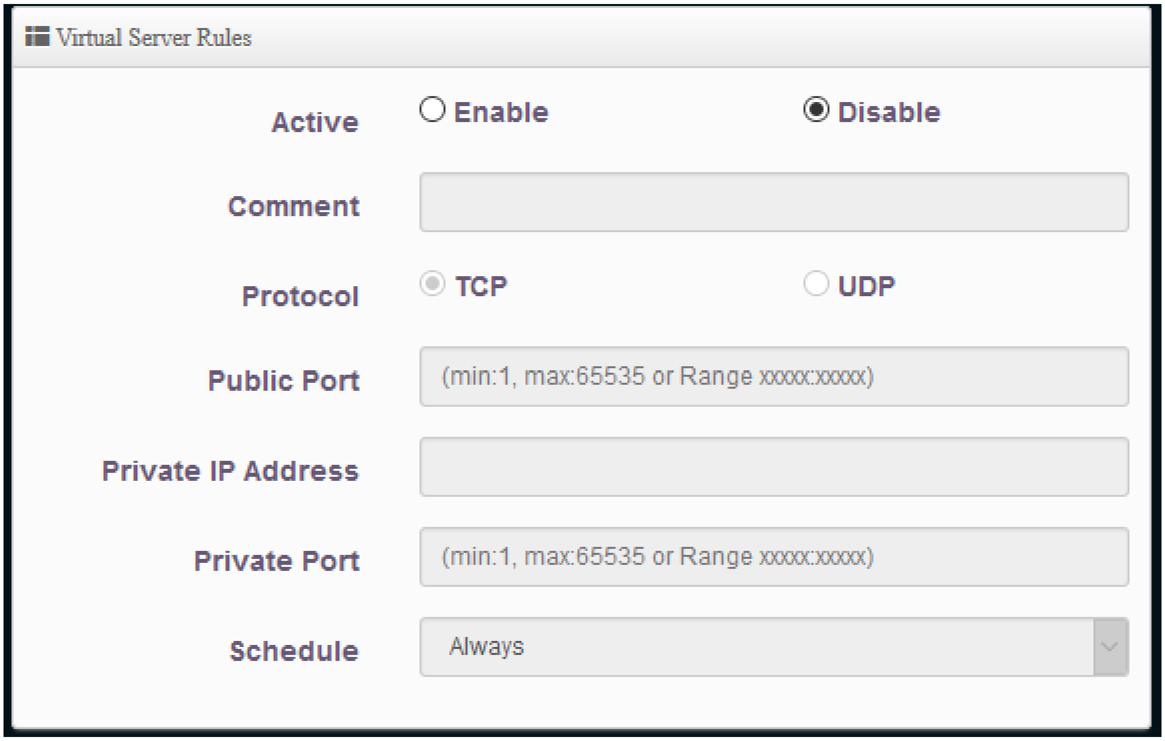
This function allows you to redirect a port on Internet IP address (on WAN port) to a specified port of an IP address on local network, so you can setup an Internet service on the computer on local network, without exposing it on Internet directly. It is also referred to as "Port Forwarding". You can also build many sets of port redirection, to provide many different Internet services on different local computers via a single Internet IP address. (This feature is only available in Router and WISP Modes)



Virtual Server List

#	Active	Comment	Protocol	Public Port	Private IP Address	Private Port	Edit
1	InActive	-	TCP	-	-	-	Edit
2	InActive	-	TCP	-	-	-	Edit
3	InActive	-	TCP	-	-	-	Edit
4	InActive	-	TCP	-	-	-	Edit

Click Edit to configure/edit a rule.



Virtual Server Rules

Active ○ Enable ● Disable

Comment

Protocol ● TCP ○ UDP

Public Port (min:1, max:65535 or Range xxxxx:xxxxx)

Private IP Address

Private Port (min:1, max:65535 or Range xxxxx:xxxxx)

Schedule Always

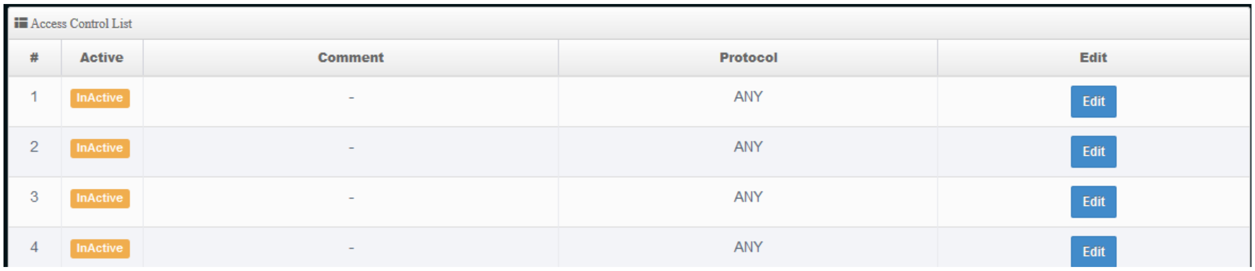
Active:	*By Default, the service is disabled. Check Enable radial button to enable Virtual Server.*
Comment:	*Enter appropriate message for resource sharing via Virtual Server.*
Protocol Type:	*Select appropriate sessions, TCP or UDP, from shared host via multiple private ports.*
Public Port:	*A port or a range of ports may be specified as start:end; i.e. port 20:80*
Private IP:	*Enter corresponding IP address of internal resource to share.*
Private Port:	*A port or a range of ports may be specified as start:end; i.e. port 20:80*
Schedule:	*Can choose to use rule by “Time Policy”*

Click “Save” button to add Virtual Server rule to List. Total of maximum **20** rules are allowed in this List. All rules can be edited or removed from the List.

When creating multiple Virtual Server rules, the prior rules have higher priority. The Virtual server rules have precedence over the DMZ rules when both rules exist.

6-5 Access Control

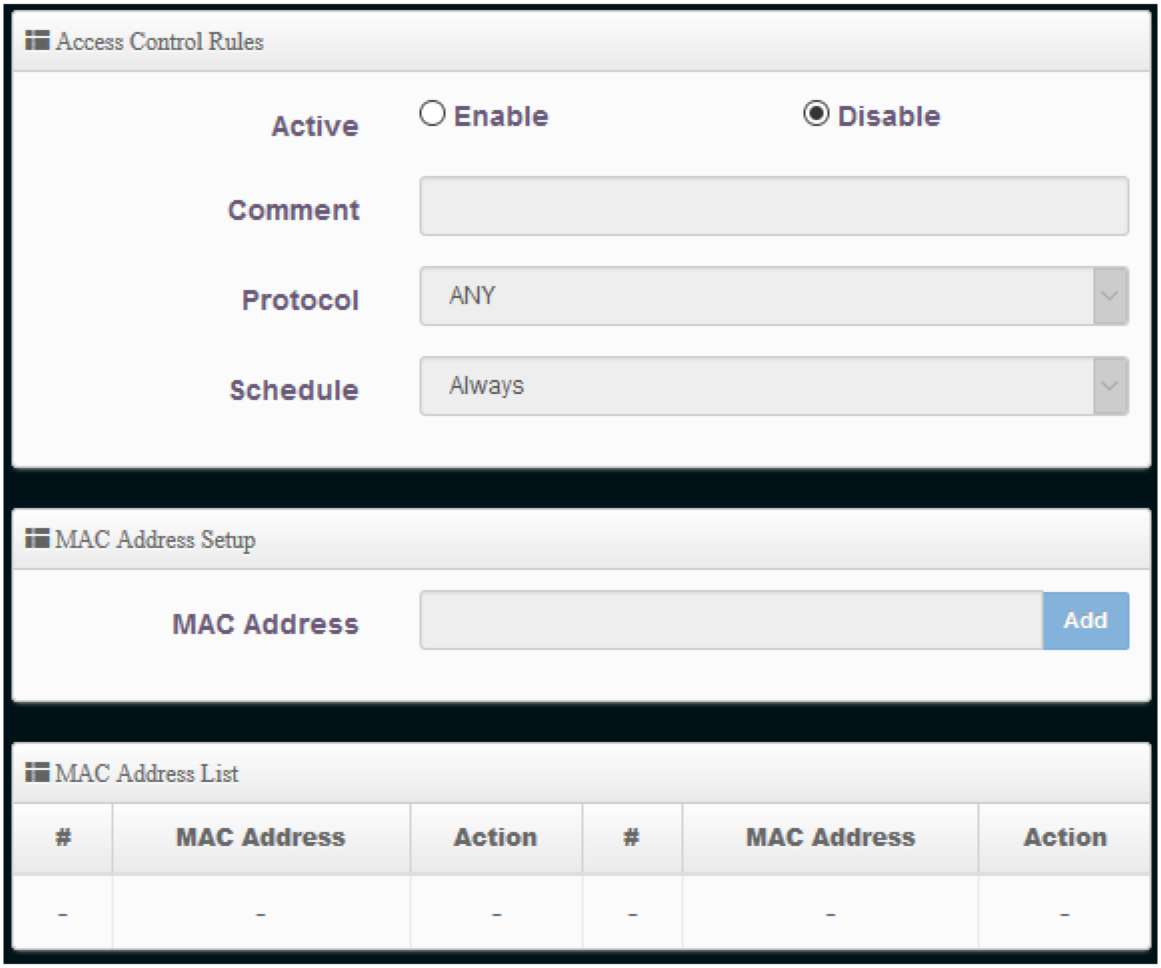
Access Control allows you to block or allow specific kinds of Internet usage and traffic, such as Internet access, designated services, and websites. (This feature is only available in Router and WISP Modes)



Access Control List

#	Active	Comment	Protocol	Edit
1	InActive	-	ANY	Edit
2	InActive	-	ANY	Edit
3	InActive	-	ANY	Edit
4	InActive	-	ANY	Edit

Click Edit to configure/edit a rule.



Access Control Rules

Active ○ Enable ● Disable

Comment

Protocol ANY

Schedule Always

MAC Address Setup

MAC Address

MAC Address List

#	MAC Address	Action	#	MAC Address	Action
-	-	-	-	-	-

Active: *Check Enable button to activate this rule, and Disable to deactivate.*

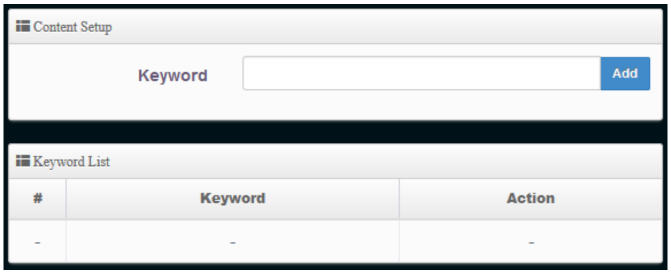
Comment: *Enter a descriptive name for this rule for identifying purposes.*

Protocol: *Select Any or specify a protocol (TCP, UDP, ICMP, Content Filter and Application) from drop-down list. When you select ICMP or Layer 7 Application, the Local(LAN)/ Destination Port cannot be used.*

TCP/UDP: Local Port: Specify local port(LAN port) range required for this rule
Destination Port : Specify destination port range required for this rule

ICMP: Specify the Local IP address for this rule

Content Filter: If you want to block websites with specific URL address or using specific keywords, enter each URL or keywords in the "Content Filter" field and click "Add" button to add in the Content Filter list of each rule. Click "Remove" button can remove URL or keywords.

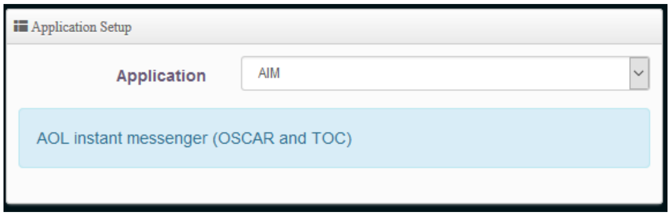

Content Setup

Keyword

Keyword List

#	Keyword	Action
-	-	-

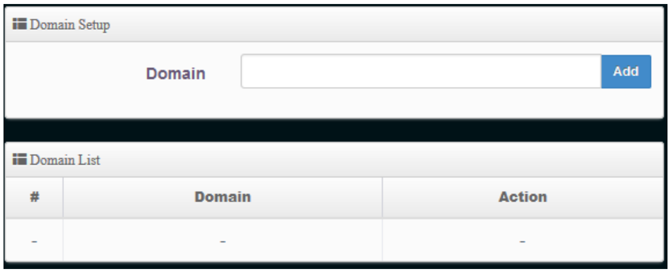
Application: Choose the application you wish to block. A small list of presets are available


Application Setup

Application: AIM

AOL instant messenger (OSCAR and TOC)

Domain Filter


Domain Setup

Domain

Domain List

#	Domain	Action
-	-	-

MAC Address: *Enter MAC address in valid MAC address format (aa.bb.cc.dd.ee.ff) and click "Add" button to add in the MAC group of each rule. Click "Remove" button can remove MAC address in the group of each rule. There are 10 MAC address maximum allowed in each rule.*

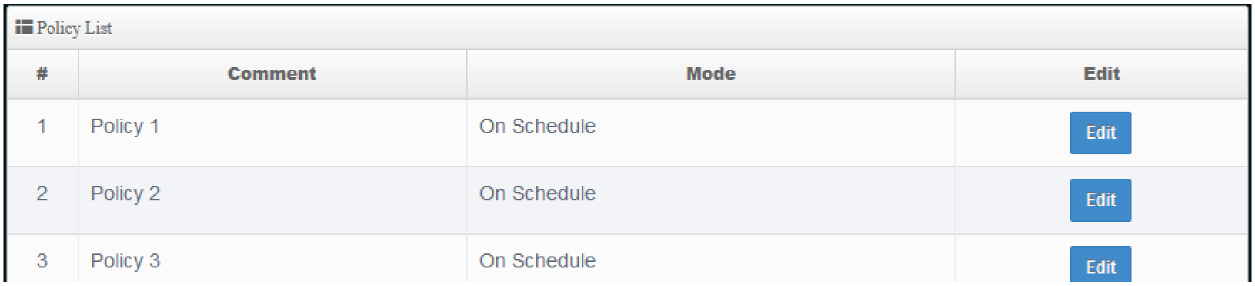
Local/Destination IP: *Specify local(LAN)/ destination IP addresses range required for this rule. If you specify local IP addresses range from 192.168.1.1 to 192.168.2.254. The matches a range of local IP addresses include every single IP address from the first to the last, so the example above includes everything from 192.168.1.1 to 192.168.2.254.*

Schedule: *Can choose to use rule by "Time Policy"*

Click "**Add"** button to add control rule to List. There are **10** rules maximum allowed in this Control List. All rules can be removed or edited on the list.

6-6 Time Policy

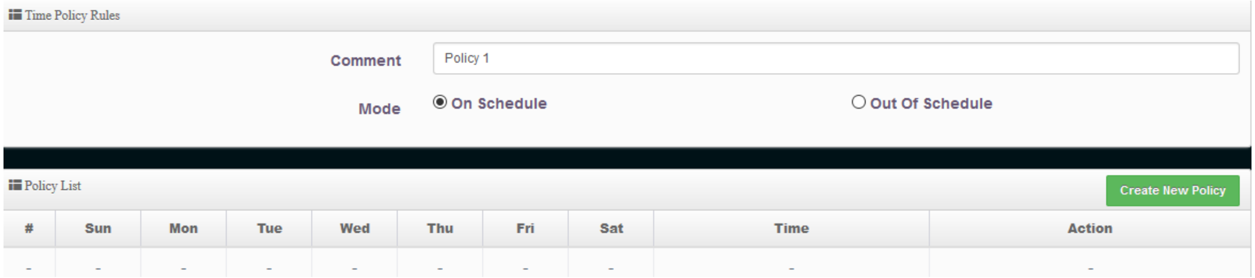
Users can define time policy for Service Domain, IP Filtering, MAC Filtering and Virtual Server. There are 10 policies that can be defined.



Policy List

#	Comment	Mode	Edit
1	Policy 1	On Schedule	Edit
2	Policy 2	On Schedule	Edit
3	Policy 3	On Schedule	Edit

Click Edit to configure/edit a policy



Time Policy Rules

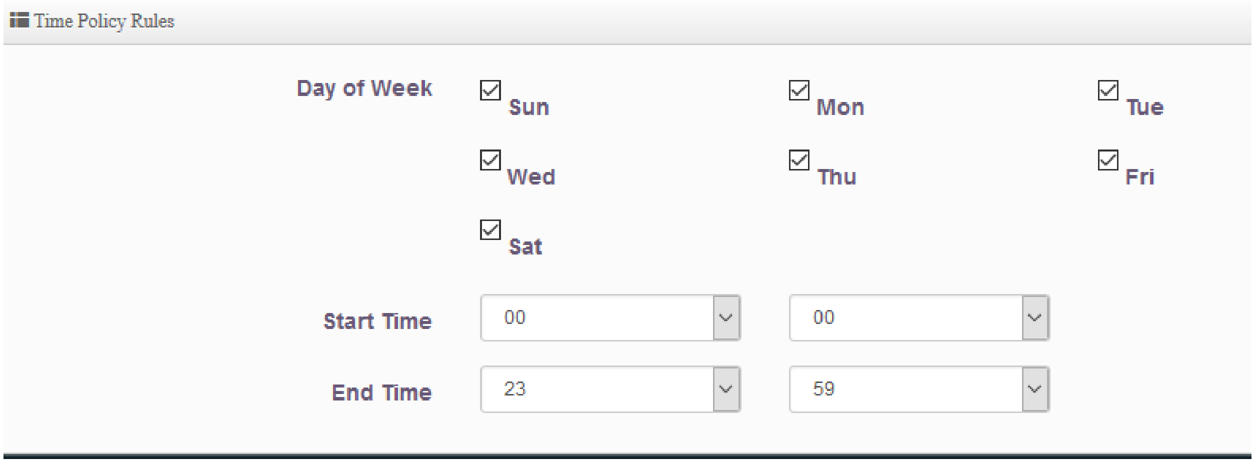
Comment: Policy 1

Mode: ● On Schedule ○ Out Of Schedule

Policy List

#	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time	Action
-	-	-	-	-	-	-	-	-	-

Create a Policy: *Select desired schedule for this policy.*



Time Policy Rules

Day of Week: ☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat

Start Time: 00 00

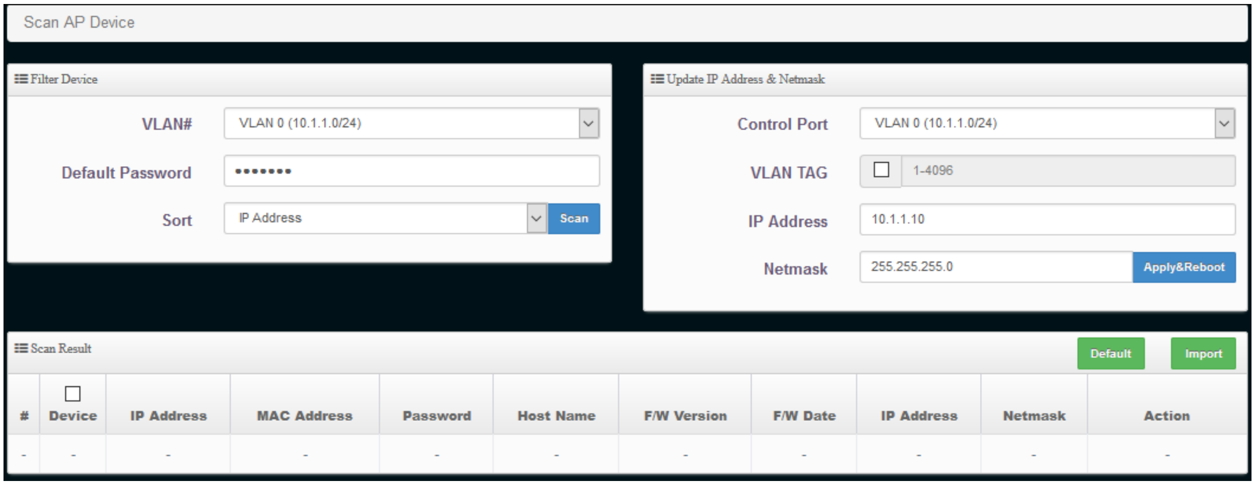
End Time: 23 59

Time Schedule: *Select desired day of week and time period for this policy.*

Chapter VII: AP Control

7-1 Scan Device

This page allows you to scan and add devices to the AP control list.



Scan AP Device

Filter Device

VLAN# VLAN 0 (10.1.1.0/24)

Default Password •••••••

Sort IP Address

Update IP Address & Netmask

Control Port VLAN 0 (10.1.1.0/24)

VLAN TAG □ 1-4096

IP Address 10.1.1.10

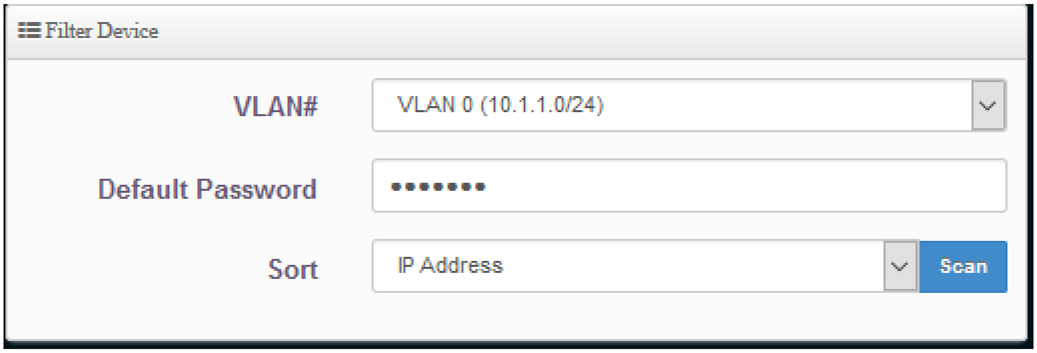
Netmask 255.255.255.0

Scan Result

#	□ Device	IP Address	MAC Address	Password	Host Name	F/W Version	F/W Date	IP Address	Netmask	Action
-	-	-	-	-	-	-	-	-	-	-

Click scan under filter device. It will scan for all managed APs on the network and list them under Scan Results. Select the APs you wish to manage and click “Import”

7-1-1 Filter Device



Filter Device

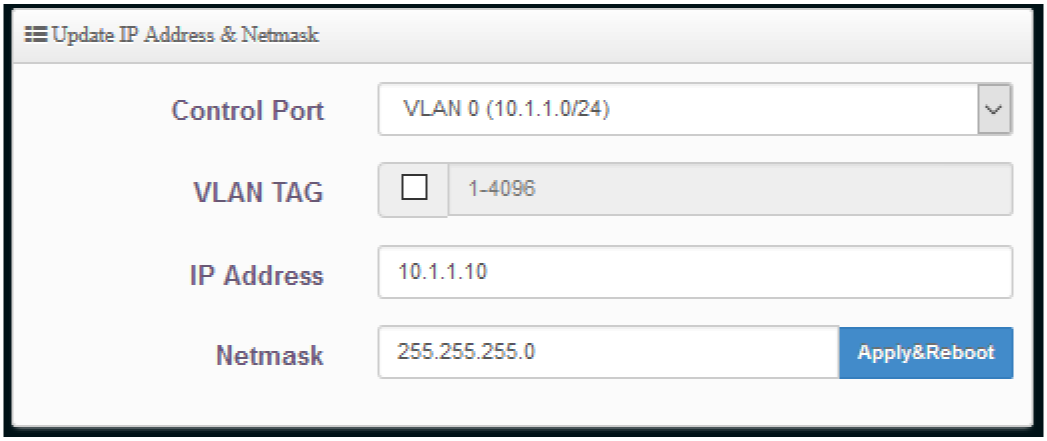
VLAN# VLAN 0 (10.1.1.0/24)

Default Password •••••••

Sort IP Address

VLAN #:	*Select VLAN network to discover managed APs*
Default Password:	*Set Login system password by managed APs*
Sort:	*Select discovered Aps by type (IP or MAC).*

7-1-2 Update IP Address & Netmask



Update IP Address & Netmask

Control Port: VLAN 0 (10.1.1.0/24)

VLAN TAG: □ 1-4096

IP Address: 10.1.1.10

Netmask: 255.255.255.0

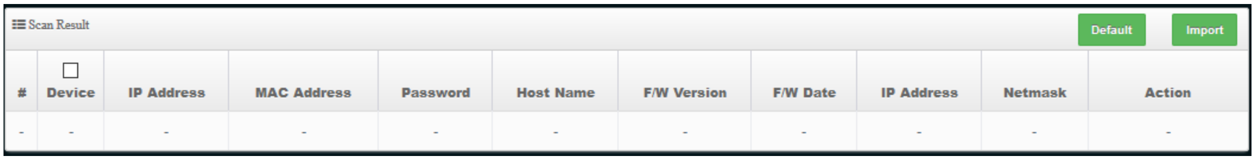
Control Port: *Change VLAN network for managed APs.*

VLAN TAG: *Set VLAN TAG ID for managed APs*

IP Address: *Set IP address for managed APs. The IP address will auto increment.*

Netmask: *Set NetMask for the managed APs*

7-1-3 Scan Result



Scan Result

#	□ Device	IP Address	MAC Address	Password	Host Name	F/W Version	F/W Date	IP Address	Netmask	Action
-	-	-	-	-	-	-	-	-	-	-

#: *Displays managed Aps*

IP Address: *Display IP address for managed APs*

MAC Address: *Display MAC Address for managed APs*

Host Name: *Display Host name for managed APs*

FW Version: *Displays the firmware version for managed APs*

FW Date: *Displays the firmware Release Date for managed APs.*

IP Address: *Displays the IP address of the unit. The administrator can set an IP for the managed AP here also.*

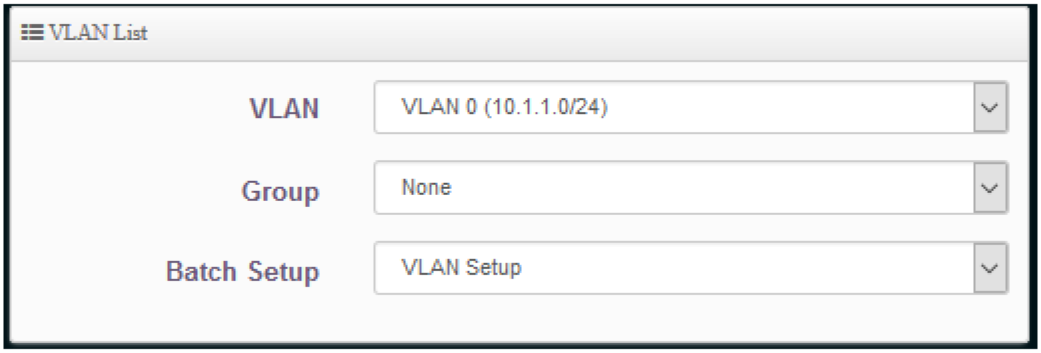
Netmask: *Displays the NetMask address of the unit. The administrator can set the netmask for the managed AP here also.*

Default: *Pressing this button will factory default the selected managed APs.*

7-2 Batch Setup

This section allows you to filter by VLAN/Group and choose which Batch setup functions you want to setup.

7-2-1 VLAN List



VLAN List

VLAN: VLAN 0 (10.1.1.0/24)

Group: None

Batch Setup: VLAN Setup

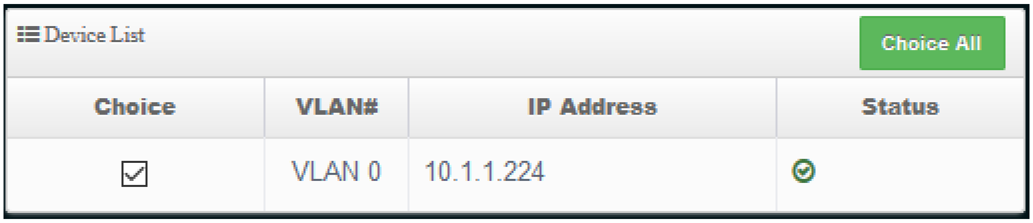
VLAN: *When VLAN Tag Function is enabled (Please refer to 4.3 system VLAN setup), administrator can change VLAN tag for managed APs.*

Group: *When AP groups are created (please refer to 7.4), administrators can select and change group settings for managed APs.*

Batch Setup: *Administrators can centralize setting changes for managed APs. (See section 7.2.3)*

7-2-2 Device List

This section shows you all the devices you have connected to the AP controller. You can connect devices by following section 7-1

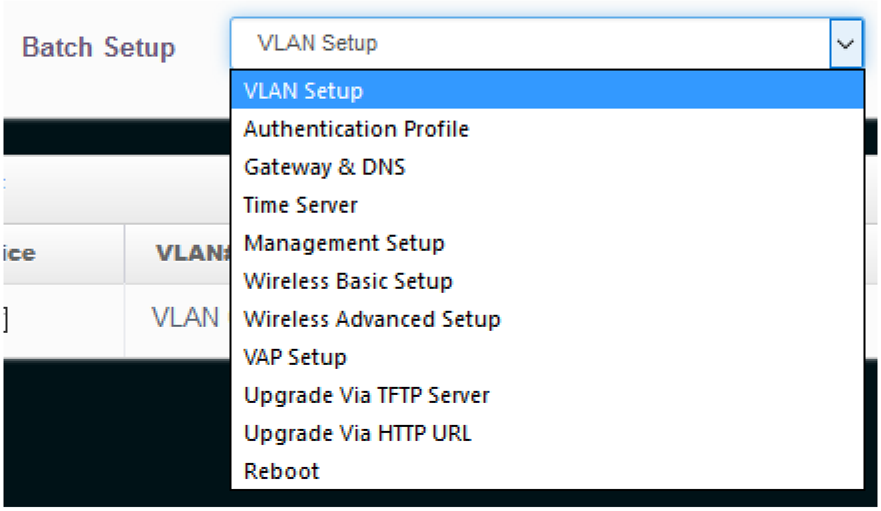


Device List

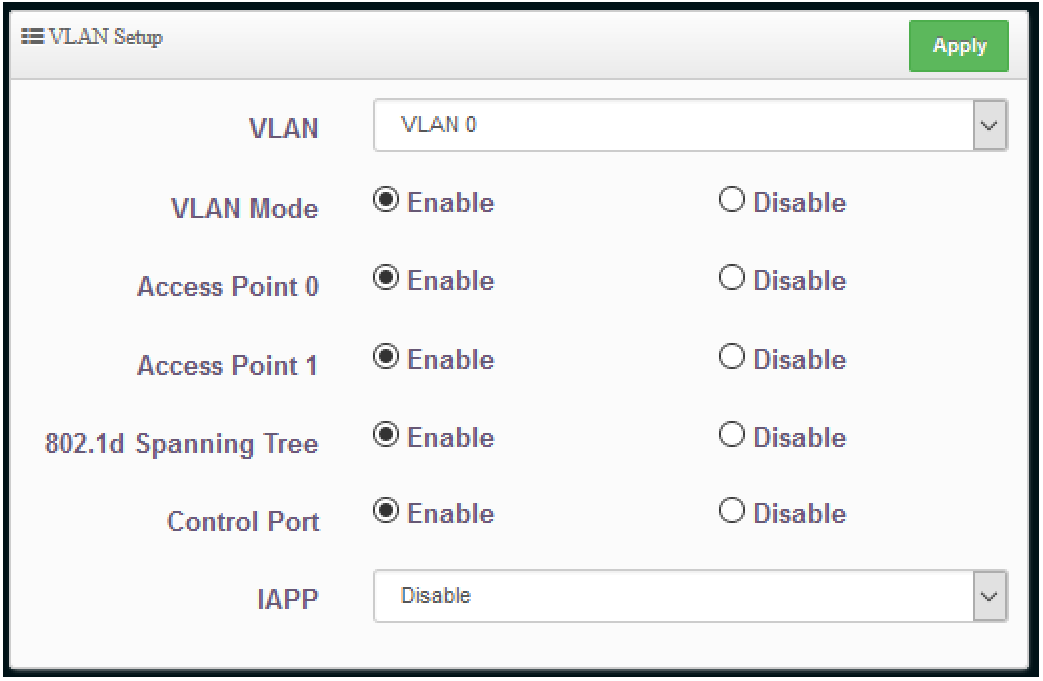
Choice	VLAN#	IP Address	Status
☑	VLAN 0	10.1.1.224	✓

7-2-3 Batch Setup

Under VLAN setup, choose Batch Setup and the drop down box. Make sure you select the devices you wish to configure under the Device List and then choose the settings you want to configure. You can configure VLANs, Authentication Profiles, Gateway & DNS, Time Servers, Management Setups, Wireless Basic and Advanced settings, Access Point Setups, Upgrades and Reboot.



- VLAN setup:



VLAN: VLAN 0

VLAN Mode: ● Enable ○ Disable

Access Point 0: ● Enable ○ Disable

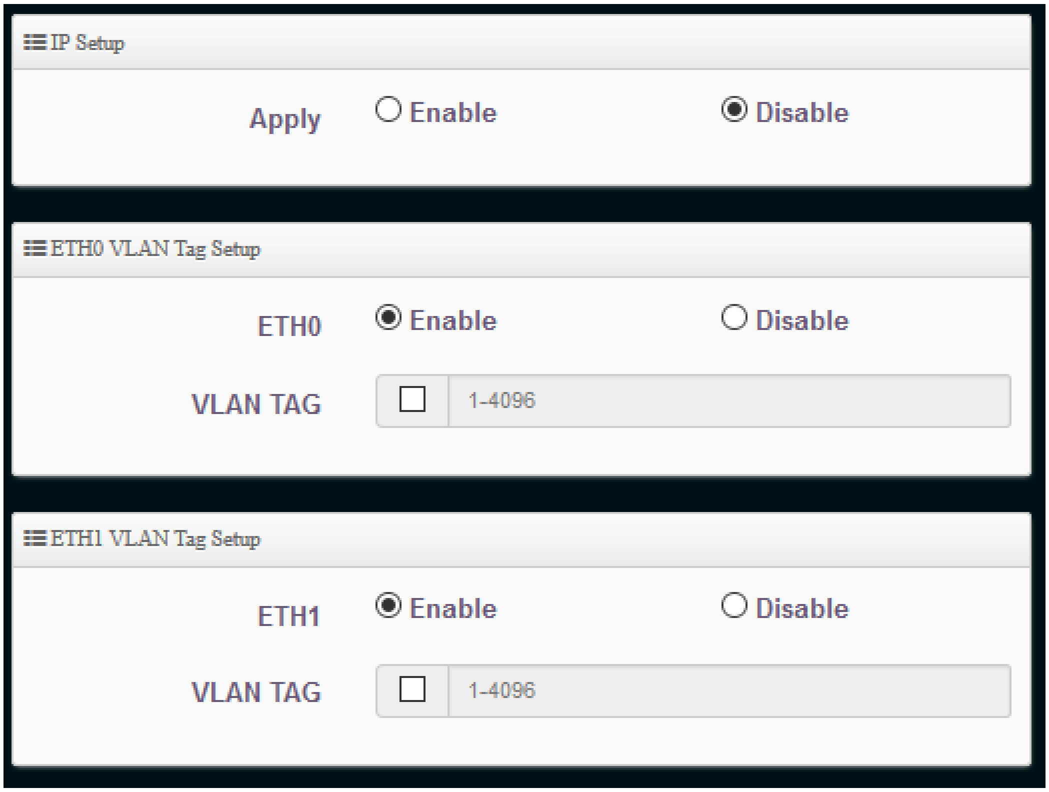
Access Point 1: ● Enable ○ Disable

802.1d Spanning Tree: ● Enable ○ Disable

Control Port: ● Enable ○ Disable

IAPP: Disable

VLAN: *The function can select VLAN (see section 4-3-1)*
VLAN Mode: *Administrator can enable or disable VLAN mode of the managed APs.*
Access Point0: *Administrator can enable or disable 2.4GHz of the managed APs.*
802.1d Spanning Tree: *Administrator can enable or disable the function. (See section 4-3-1)*
Control Port: *The function administrator can enable or disable of the managed APs (please refer to section 4.3.1)*
IAPP The function: *Administrator can enable or disable of the managed APs. (See section 4-3-3)*



IP Setup

Apply ○ Enable ● Disable

ETH0 VLAN Tag Setup

ETH0 ● Enable ○ Disable

VLAN TAG □ 1-4096

ETH1 VLAN Tag Setup

ETH1 ● Enable ○ Disable

VLAN TAG □ 1-4096

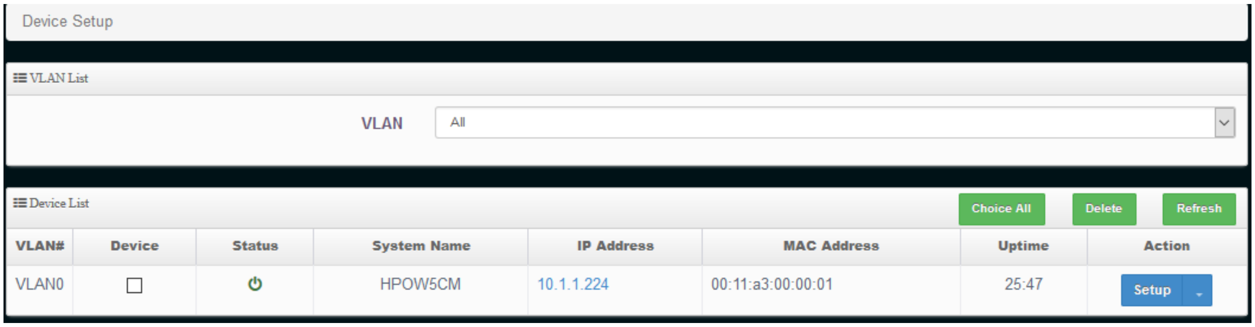
IP Setup: Administrator can set IP address and Netmask of the managed APs.

ETH0/1 VLAN Tag Setup: Administrator can set VLAN Tag or disable VLAN function of the managed APs.

- *Authentication Profile: After creating Profiles, See section 7-6 users can apply Authentication profiles*
- *Gateway & DNS: Setting Gateway and DNS for managed APs.*
- *Time Server: Setting System Time for managed APs. See section 4-7*
- *Management Setup: Setting system name/ system login port and system log server service for managed APs. See section 4-6*
- *Wireless Batch Setup: Setting Wi-Fi configurations for managed APs. See section 5.1*
- *Wireless Advanced Setup: Setting Wi-Fi Advanced settings for managed APs. See section 5.2*
- *VAP Setup: Wi-Fi SSID / channel or security settings for managed APs. See section 4.3.3*
- *Upgrade via TFTP Server: Administrator can centrally upgrade firmware via TFTP Server for the managed APs.*
- *Upgrade via HTTP Server: Administrator can centrally upgrade firmware via HTTP Server for the managed APs.*
- *Reboot: Administrator can reboot managed APs.*

7-3 AP Setup

AP setup allows you to configure each individual AP you added to the Controller. You can edit the network settings, remove the devices from the controller or reboot them.



VLAN: All

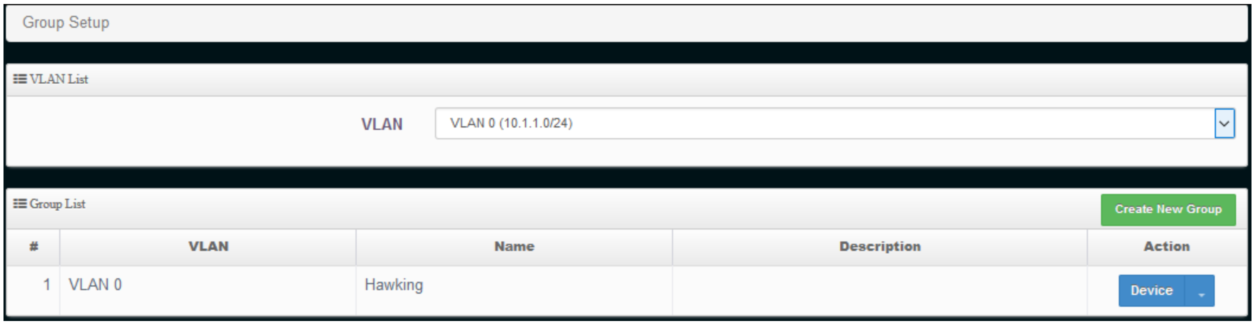
VLAN#	Device	Status	System Name	IP Address	MAC Address	Uptime	Action
VLAN0	□	⏻	HPOW5CM	10.1.1.224	00:11:a3:00:00:01	25:47	Setup

VLAN: selected Desired VLAN for AP setup

Setup: Administrators can modify IP address, system login passwords, web login port for managed APs. If administrator has to change AP devices, they can modify MAC address of new managed AP.

7-4 Group Setup

Group setup allows you to create groups within the same VLAN for your Access Points.



VLAN: VLAN 0 (10.1.1.0/24)

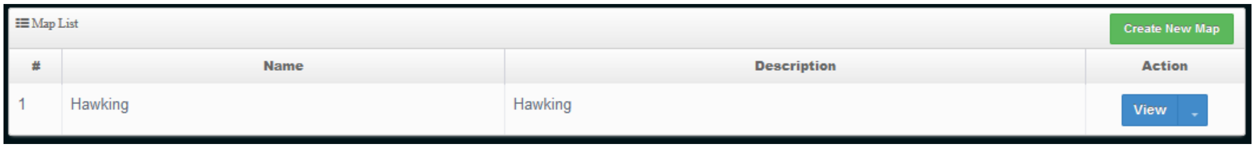
#	VLAN	Name	Description	Action
1	VLAN 0	Hawking		Device

VLAN: *Select VLAN*

Device Button: *Select the managed APs and import them into a group.*

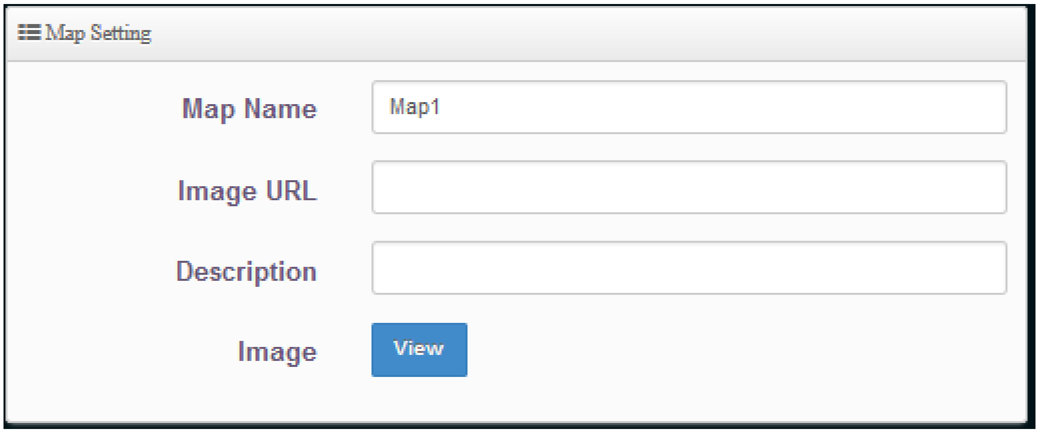
7-5 Map Setup

The Map Setup feature allows administrators to upload a floor plan image to a web server, then use the image URL to import the map into the AP user interface. Once the image is uploaded, administrators can use the Map Setup Function to map out the locations of an AP network.



#	Name	Description	Action
1	Hawking	Hawking	View

Create New Map: *Click the button to create map.*



☰ Map Setting

Map Name: Map1

Image URL:

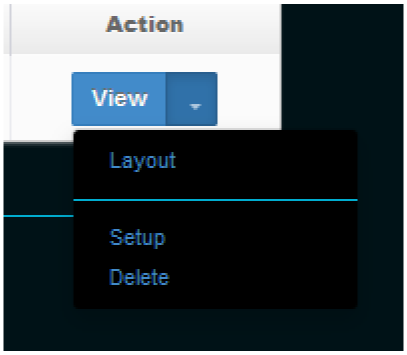
Description:

Image

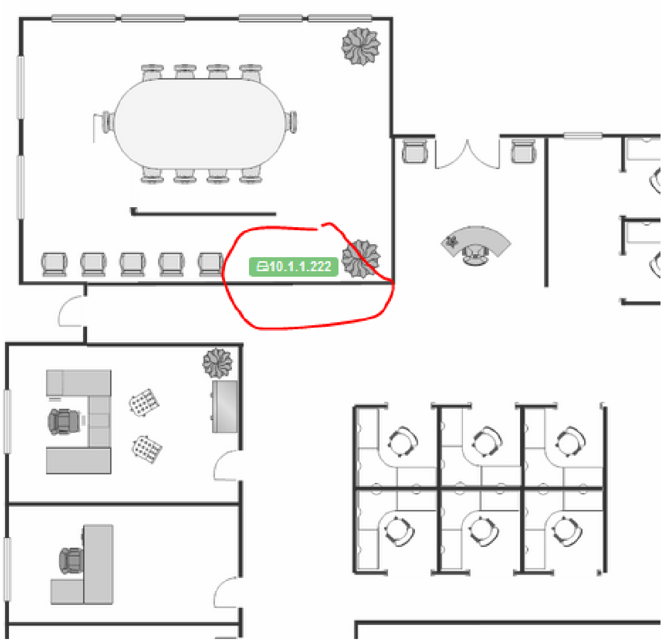
Map Name: *Enter a map name*

Image URL: *Enter the URL of the map image.*

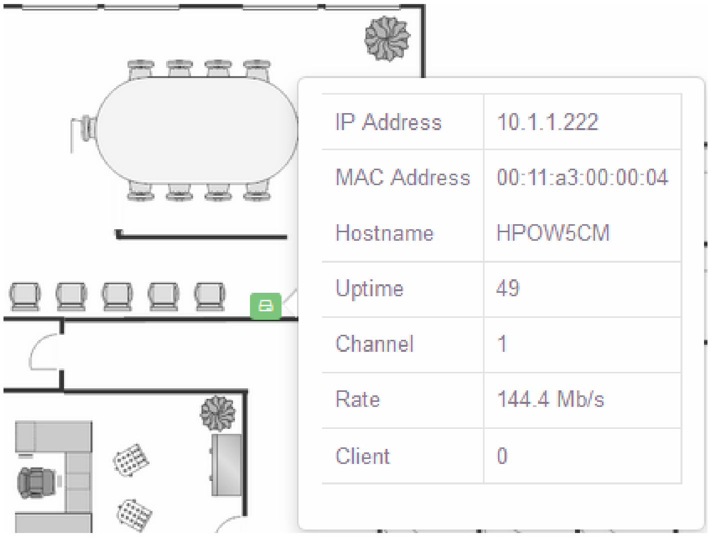
Description: *Enter a description of the map.*



Layout: *Once the map is on the Map List, administrators can click on the "Layout" button in the action tab to map out the AP network. Managed APs will appear on the device list section of the layout page. Administrators can simply drag the AP to the correct location.*



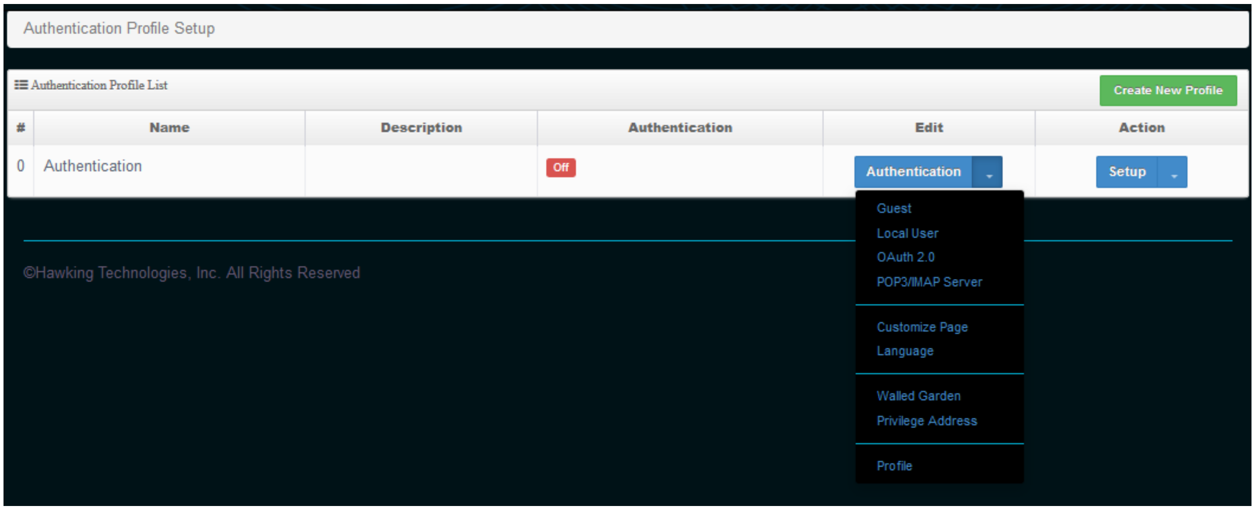
View: *Once a device is placed, you can click the "View" button to monitor AP status and locations.*



IP Address	10.1.1.222
MAC Address	00:11:a3:00:00:04
Hostname	HPOW5CM
Uptime	49
Channel	1
Rate	144.4 Mb/s
Client	0

7-6 Authentication Profile

Administrators can pre-set authentication conditions in the profile. For authentication, refer to 4.3.4 - Authentication



#	Name	Description	Authentication	Edit	Action
0	Authentication		Off	Authentication	Setup

Create New Profile: *Create a new authentication profile.*

Edit: *Click the Authentication button to Enable or Disable authentication function.*

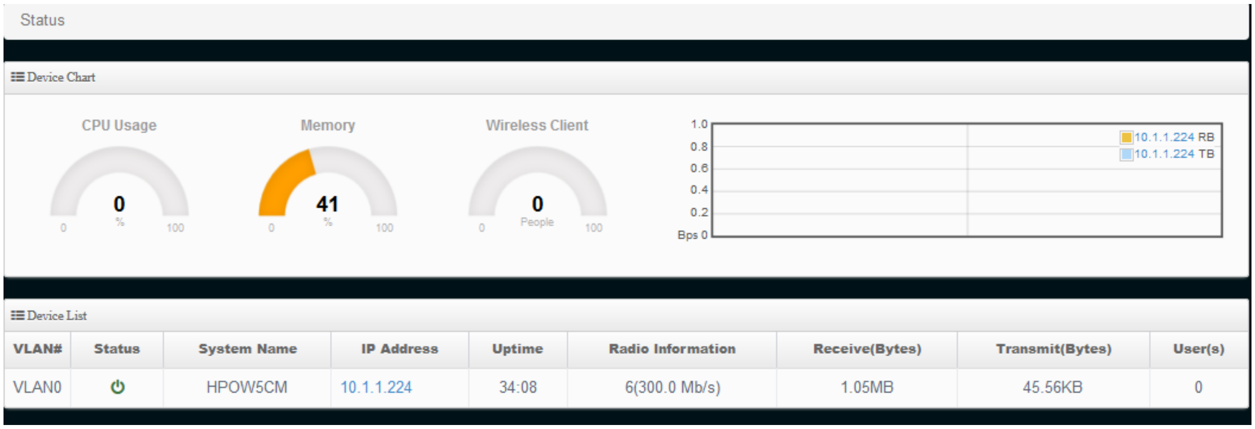
See section 4-4

Click Dropdown to set authentication functions. See section 4-4

Action: *Setup button can modify or delete for the authentication profile.*

7-7 Status

Check the status of each Access Point assigned to the Controller. Check their settings and network information.

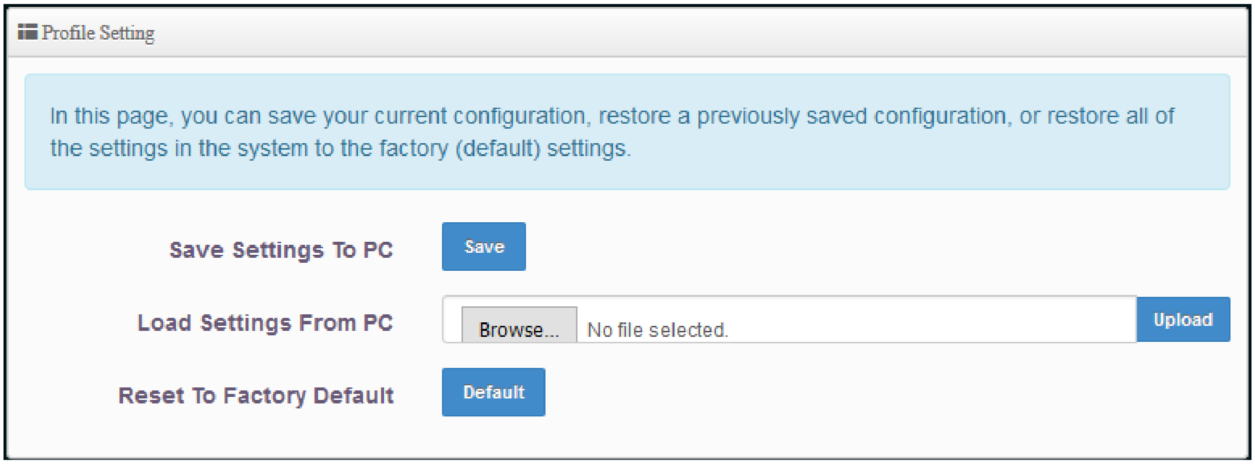


VLAN#	Status	System Name	IP Address	Uptime	Radio Information	Receive(Bytes)	Transmit(Bytes)	User(s)
VLAN0	⏻	HPOW5CM	10.1.1.224	34:08	6(300.0 Mb/s)	1.05MB	45.56KB	0

Chapter VIII: Utilities

8-1 Profile Setting

In this page you can save your current configuration, restore a previous saved configuration or restore all the settings in the system to the factory default settings.



Profile Setting

In this page, you can save your current configuration, restore a previously saved configuration, or restore all of the settings in the system to the factory (default) settings.

Save Settings To PC

Load Settings From PC — No file selected.

Reset To Factory Default

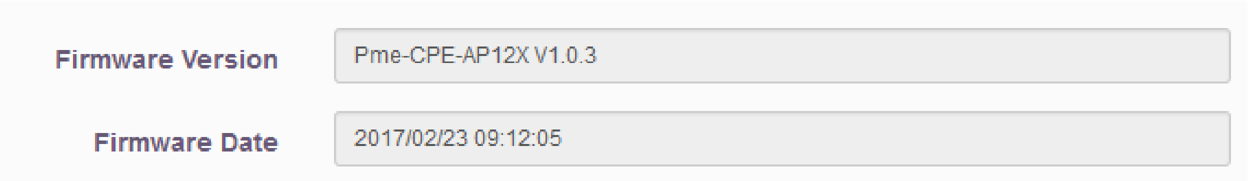
Save Settings to PC: *Click Save button to save the current configuration to a local disk.*

Load Settings from PC: *Click Browse button to locate a configuration file to restore, and then click Upload button to upload.*

Reset To Factory Default: *Click Default button to reset back to the factory default settings and expect Successful loading message. Then, click Reboot button to activate.*

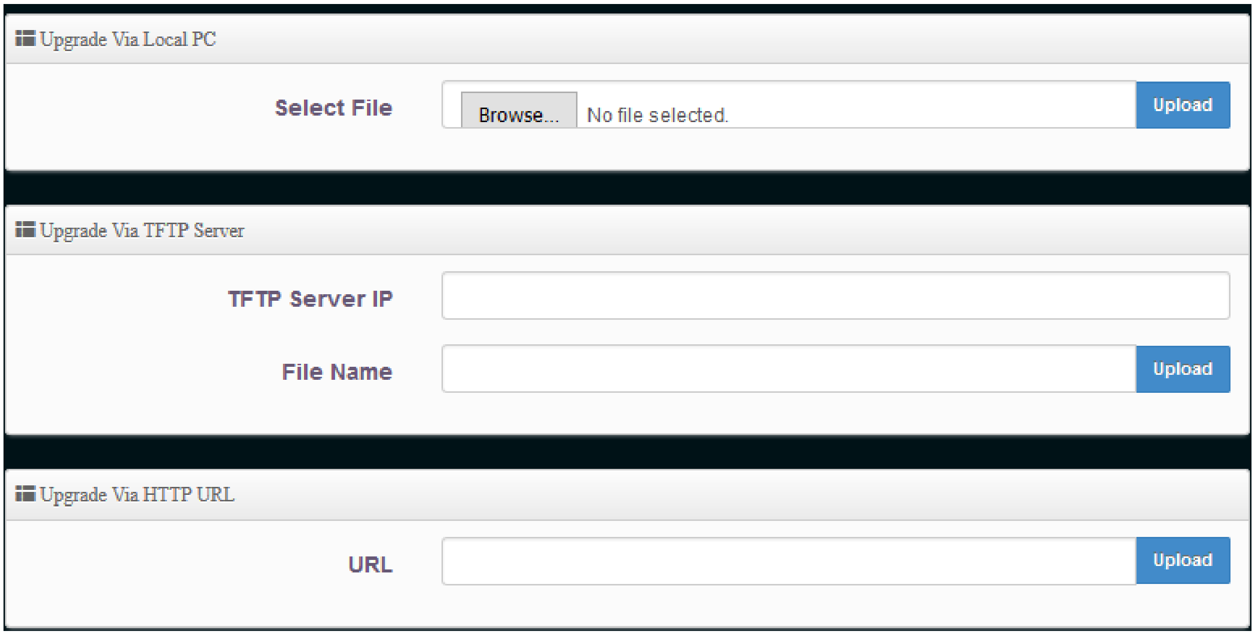
8-2 System Upgrade

Firmware is the main software image that system needs to respond to requests and to manage real time operations. Firmware upgrades are sometimes required to include new features or a bug fix. It takes around 2 minutes to upgrade due to complexity of firmware. To upgrade system firmware, click Browse button to locate the new firmware, and then click Upgrade button to upgrade.



Firmware Version	Pme-CPE-AP12X V1.0.3
Firmware Date	2017/02/23 09:12:05

Shows current system software version and software date



Upgrade Via Local PC

Select File: Browse... No file selected.

Upgrade Via TFTP Server

TFTP Server IP

File Name

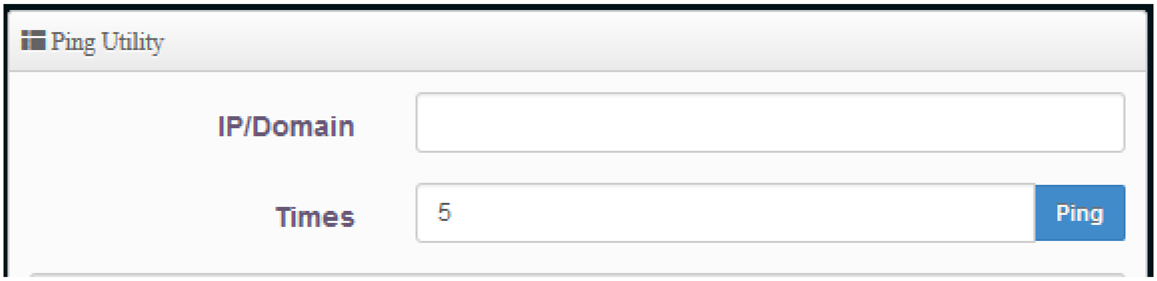
Upgrade Via HTTP URL

URL

Upgrade Firmware: *Upgrade firmware will support via Local PC, TFTP Server and HTTP URL upgrade*

8-3 Network Utility

The administrator can diagnose network connectivity via the PING or TRACEROUTE utility.



Ping Utility

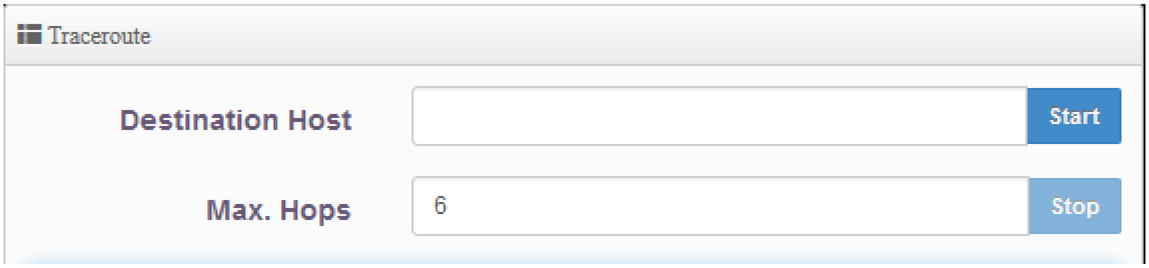
IP/Domain

Times: 5

Ping: *This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the Result field while running the PING test.*

IP/Domain: Enter desired domain name, i.e. www.google.com, or IP address of the destination, and click ping button to proceed. The ping result will be shown in the Result field.

Times: The default setting is 5 and the range is from 1 to 50. It indicates number of connectivity test.



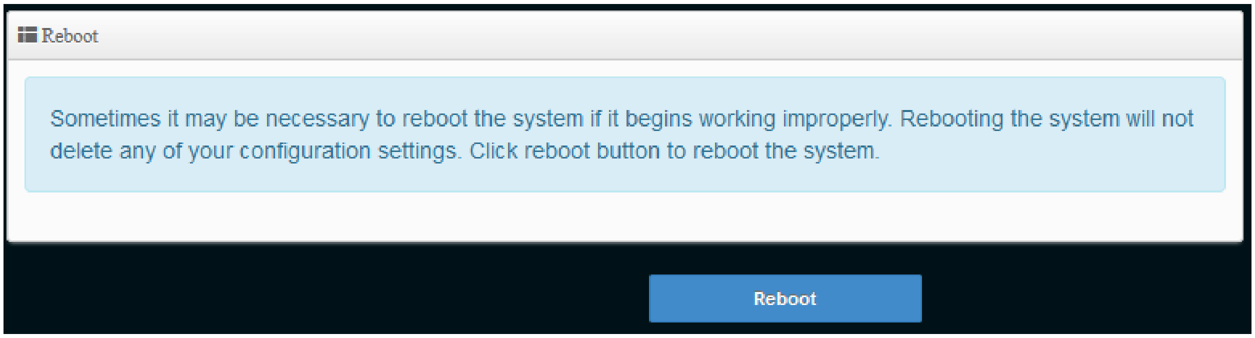
Traceroute: *Allows tracing the hops from the device to a selected outgoing IP address. It should be used for the finding the route taken by ICMP packets across the network to the destination host. The test is started using the Start button, click Stop button to stopped test.*

Destination Host: Specifies the Destination Host for the finding the route taken by ICMP packets across the network.

MAX Hop: Specifies the maximum number of hops (max time-to-live value) trace route will probe.

8-4 Reboot

This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

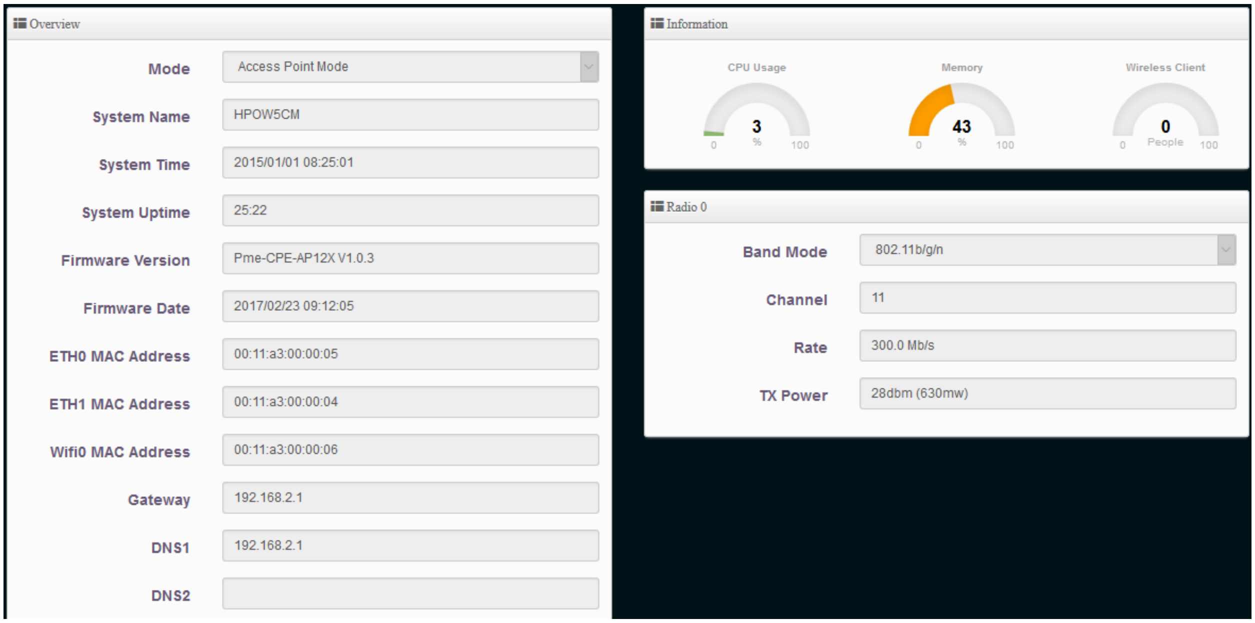


Sometimes it may be necessary to reboot the system if it begins working improperly. Rebooting the system will not delete any of your configuration settings. Click reboot button to reboot the system.

Chapter IX: Status

9-1 Overview

Detailed information on the Device and Network can be viewed on this page.



Overview

Mode	Access Point Mode
System Name	HPOW5CM
System Time	2015/01/01 08:25:01
System Uptime	25:22
Firmware Version	Pme-CPE-AP12X V1.0.3
Firmware Date	2017/02/23 09:12:05
ETH0 MAC Address	00:11:a3:00:00:05
ETH1 MAC Address	00:11:a3:00:00:04
Wifi0 MAC Address	00:11:a3:00:00:06
Gateway	192.168.2.1
DNS1	192.168.2.1
DNS2	

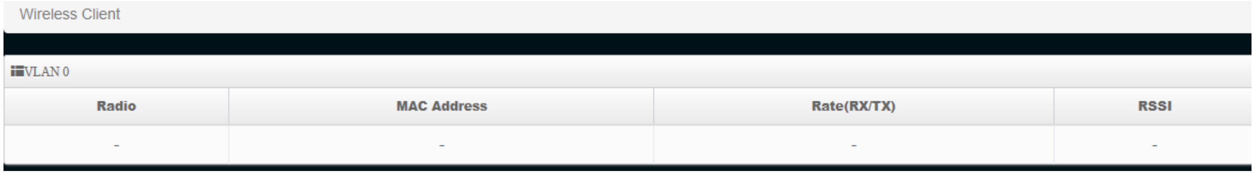
Information

Radio 0

Band Mode	802.11b/g/n
Channel	11
Rate	300.0 Mb/s
TX Power	28dbm (630mw)

9-2 Wireless Client

Administrators can view the status of all Wireless users.



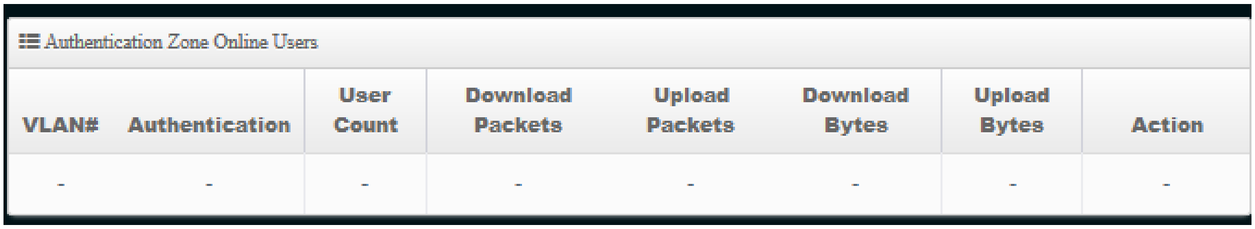
Wireless Client

VLAN 0

Radio	MAC Address	Rate(RX/TX)	RSSI
-	-	-	-

9-3 Online Users

The status can display online users by captive portal. Administrators can monitor user's login/logout time and account type for the authentication account



Authentication Zone Online Users

VLAN#	Authentication	User Count	Download Packets	Upload Packets	Download Bytes	Upload Bytes	Action
-	-	-	-	-	-	-	-

VLAN: *Display VLAN number*

Authentication: *Display captive Portal Authentication function is on/off on VLANs*

Download Packets: *Display total download packets amount information of the VLAN*

Upload Packets: *Display total upload packets amount information of the VLAN*

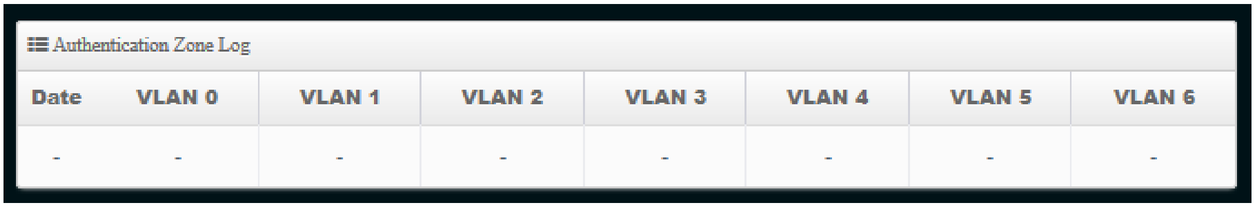
Download Bytes: *Display total download flow information of the VLAN*

Upload Bytes: *Display total upload flow information of the VLAN*

Action: *Click "Detail" to monitor all user's use of network*

9-4 Authentication Log by Captive Portal

The authentication log can monitor account login/logout type and account use time

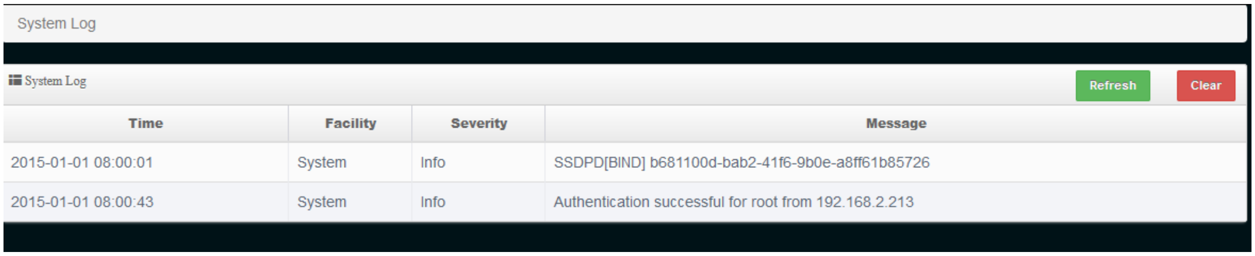


Authentication Zone Log

Date	VLAN 0	VLAN 1	VLAN 2	VLAN 3	VLAN 4	VLAN 5	VLAN 6
-	-	-	-	-	-	-	-

9-5 System Log

The Event log displays system events when system is up and running. Also, it becomes very useful as a troubleshooting tool when issues are experienced in system.



System Log

System Log

Time	Facility	Severity	Message
2015-01-01 08:00:01	System	Info	SSDPD[BIND] b681100d-bab2-41f6-9b0e-a8ff61b85726
2015-01-01 08:00:43	System	Info	Authentication successful for root from 192.168.2.213

Time: *The date and time when the event occurred.*

Facility: *Identify source of events such as "System" or "User"*

Severity: *Severity level that a specific event is associated such as "info", "error", "warning", etc.*

Message: *Description of the event.*

Click **"Refresh"** button to renew the log

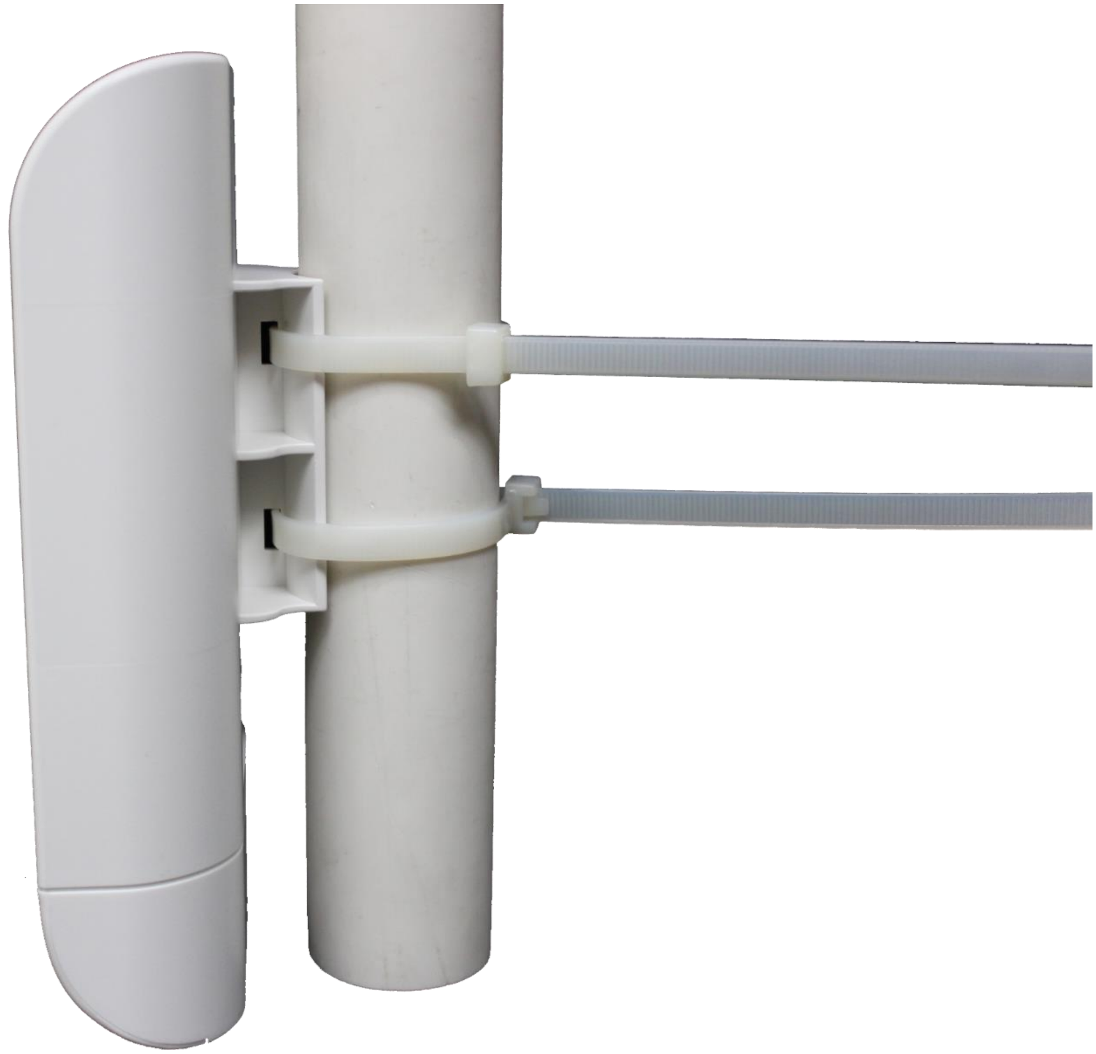
Click "**Clear"** button to clear all the records.

Chapter X: Hardware Install

The HPOW5CM are designed with wall mounts and pole mounts for exterior installations.

10-1 Pole Mount

Using the provided zip ties, secure the HPOW5CM through the holes on the back of the device. Make sure they are tight and secure. Make sure the pole itself is secure.

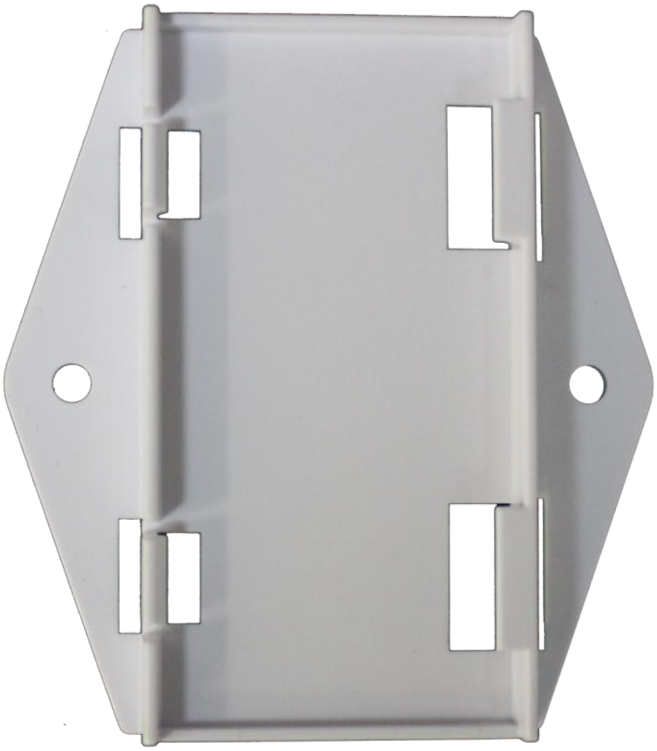


Note: you will need an Ethernet cable long enough to go from the device to the PoE injector. The PoE injector is not weather proofed. We do not recommend any cabling over 100 feet in length.

Note2: Make sure you also use a long enough grounding cable (not included) to mount to your grounding point. We recommend 16-18 AWG grounding cable

10-2 Wall Mount

Using the optional wall mount kit, first mount the wall mounting kit on a secure wall.



Screw it in using the provided screws. Once secure, simply snap the HPOW5CM into the wall mount kit.

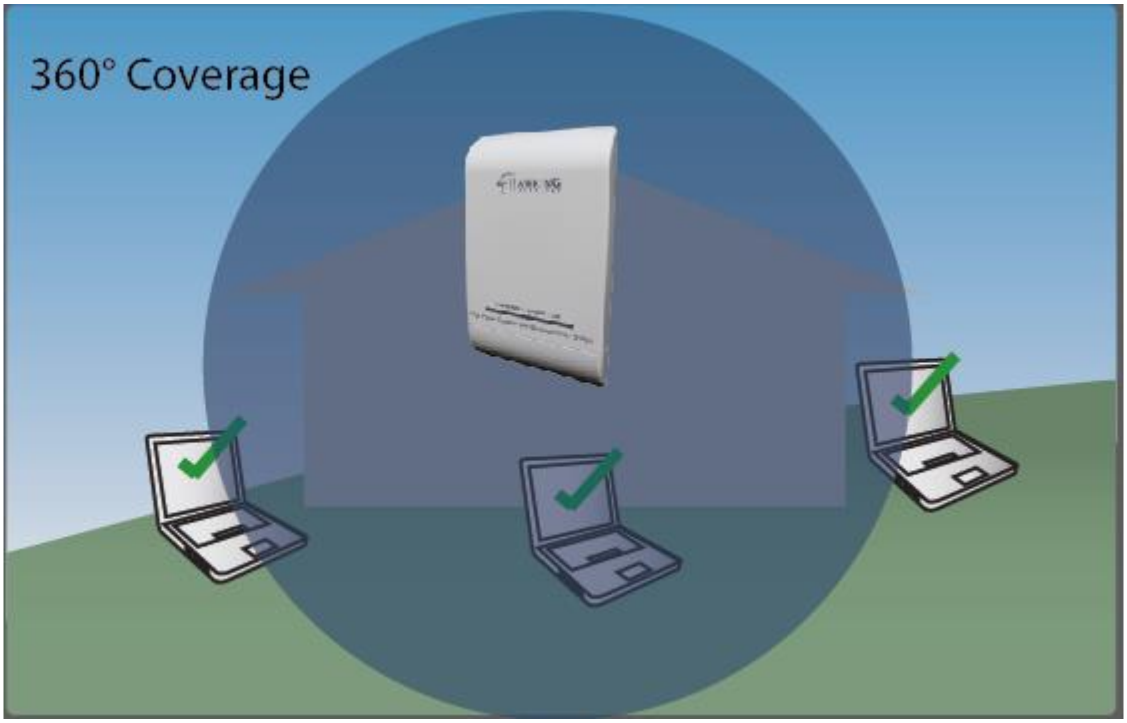
Note: you will need an Ethernet cable long enough to go from the device to the PoE injector. The PoE injector is not weather proofed. We do not recommend any cabling over 100 feet in length.

Note2: Make sure you also use a long enough grounding cable (not included) to mount to your grounding point. We recommend 16-18 AWG grounding cable

10-3 Antenna Orientation

Once you have mounted and connected HPOW5CM, be sure to note the signal pattern of the antenna. Only devices within the transmission cone are guaranteed to get a good signal. You will receive optimal wireless signal by placing your wi-fi enabled device within the designated area. Adjust the antenna as needed.

The HPOW5CM has a 360 degree coverage radius. As seen in the diagram below, the signal will be transmitted in a sphere around the HPOW5CM. All devices within the range of the device should get a signal.



Chapter XI: Appendix

11-1 Specifications

Hardware Specification	
Base Platform	AR9341 **(AR1321)**
CPU Clock Speed	535 MHz
Wireless Radio	IEEE 802.11b/g/n
Serial Port	1 * Console (Internal)
Reset Switch Built-in	Push-button momentary contact switch
Standards Conformance	IEEE 802.3 / IEEE 802.3u
Ethernet Ports	• 2 x 10/100Mbps Ethernet ports (PoE Pass Through) • IEEE 802.3, 802.3u compliant • CSMA/CD 10/100 auto sense • Power over Ethernet (PoE)
Flash	On board : 8MB
SDRAM	On board : 32MB
Built-In LED Indicators	1 x Power, 2 x LAN, 4 x WLAN (Signal LED Indicator)
Wireless Specification	
Network Standards Conformance	IEEE802.11 b/g/n compliant
Data Transfer Rate	IEEE802.11b : 1 / 2 / 5.5 / 11Mbps (auto sensing) IEEE802.11g : 6/ 9/ 12/ 18/ 24/ 36/ 48/ 54Mbps (auto sensing) IEEE801.11n : 300Mbps (Tx), 300Mbps (Rx)
Frequency Range	2.412 ~ 2.462GHz (USA)
Channel Spacing	IEEE802.11b/g : 20MHz IEEE802.11n : 20/40MHz
Media Access Protocol	CSMA/ CA with ACK
Modulation Method	IEEE 802.11b: DSSS (DBPK,DQPSK,CCK) IEEE 802.11g/n : OFDM(64-QAM,16-QAM,QPSK,BPSK)
RF Output Power	800mW (±2dB dBm)
Frequency Response Flatness	±1dB over operating range
Receive Sensitivity	-96dBm (±2dB dBm)

Environmental & Mechanical Characteristics	
Operating Temperature	-20 °C ~ 60 °C
Storage Temperature	-20 °C ~ 85 °C
Operating Humidity	100% Non-Condensing
Storage Humidity	100% Non-Condensing
Built-in Antenna	HPOW5CM: 5dBi, 2.4GHz Omni Antenna (H-Plane: 360, E-Plane: 60)
Input Power	48 VDC
Ethernet Connector	2 * Ethernet Connector
Power Supply	AC Input : 110 – 220V AV Power DC Output : 48 VDC, 0.5A input (PoE Power Injector, support up to 1A)
Unit Weight	0.289KG
Unit Dimensions	190.5 x 114 x 57 mm