CERIO Corporation
CenOS 5.0

User Manual

CW-500 R3

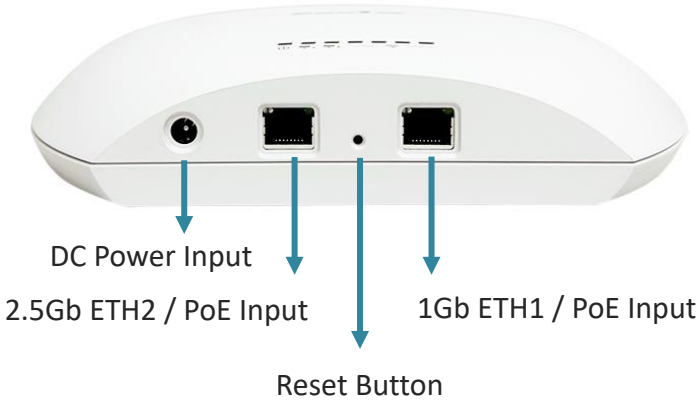
eXtreme High Power WiFi6 Tri-Radio AX4200

Ceiling/Wall PoE Access Point (500mW)

Content

1. Device and Software Configuration

1-1. Device appearance

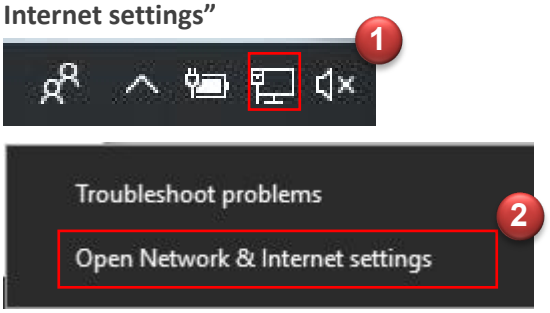


1-2. Setup Preparation of AP

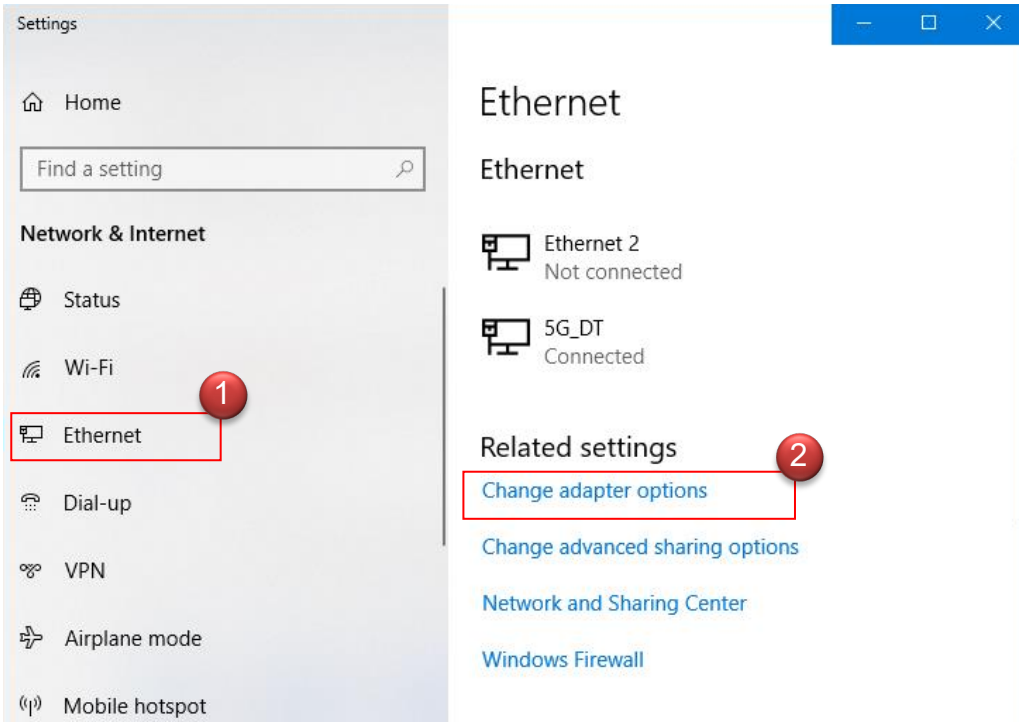
Please PC link to Device used cat5/6 Ethernet cable.

The following setup uses a Windows PC, user OS may vary.

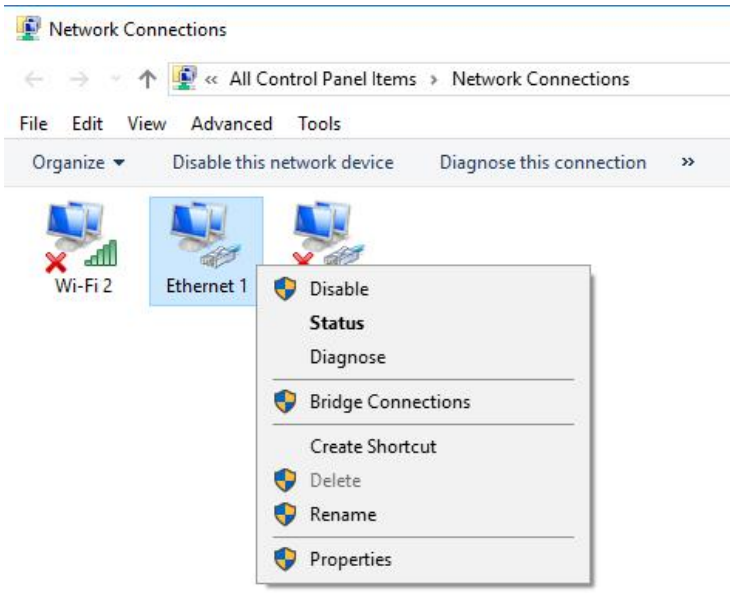
Step 1: Please click on the computer icon in the bottom right window, and click **"Open Network and Internet settings"**



Step 2: After click left side "**Ethernet**" function, click on the right side "**Change adapter options**" again.



Step 3: In **"Change adapter options"** Page. Please find Ethernet (Local LAN) and Click the right button on the mouse and Click **"Properties"**

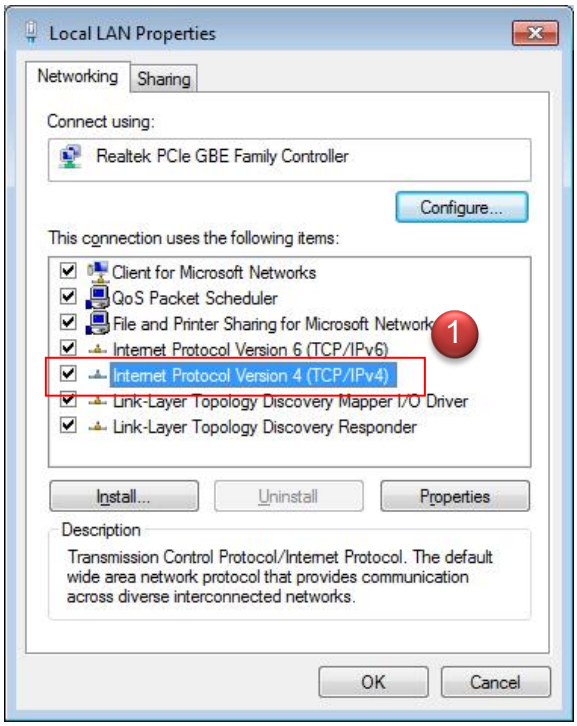


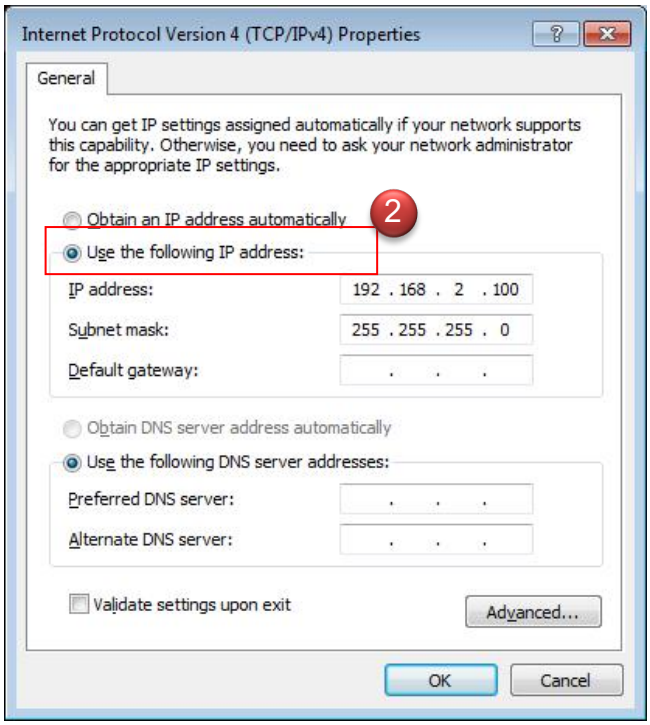
Step 4: In Properties page to setting IP address, please find **"Internet Protocol Version 4 (TCP/IPv4)"** and double click or click **"OK"** button.

Step 5 : Select **"Use the following IP address"**, and fix in IP Address : 192.168.2.#

ex. The # is any number by 1 to 253

Subnet mask : 255.255.255.0

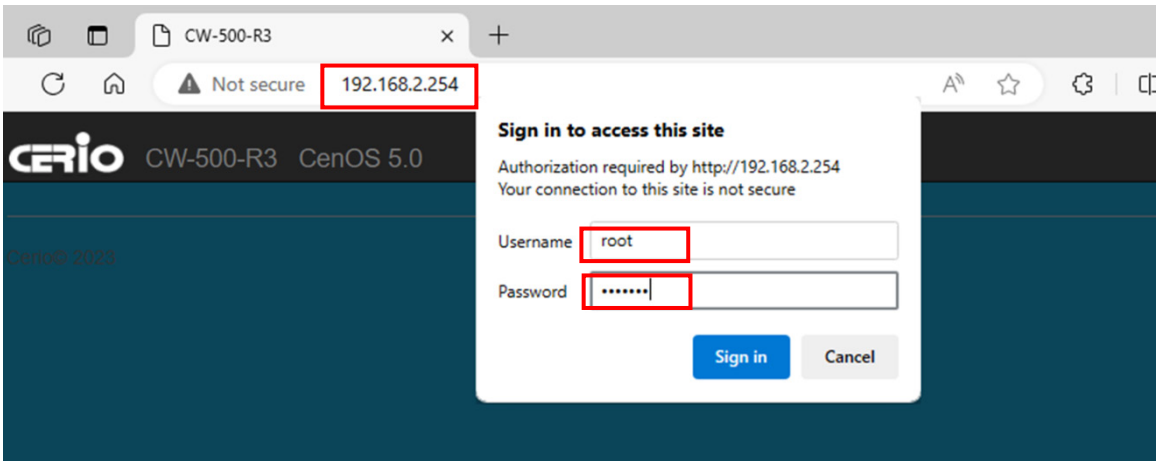




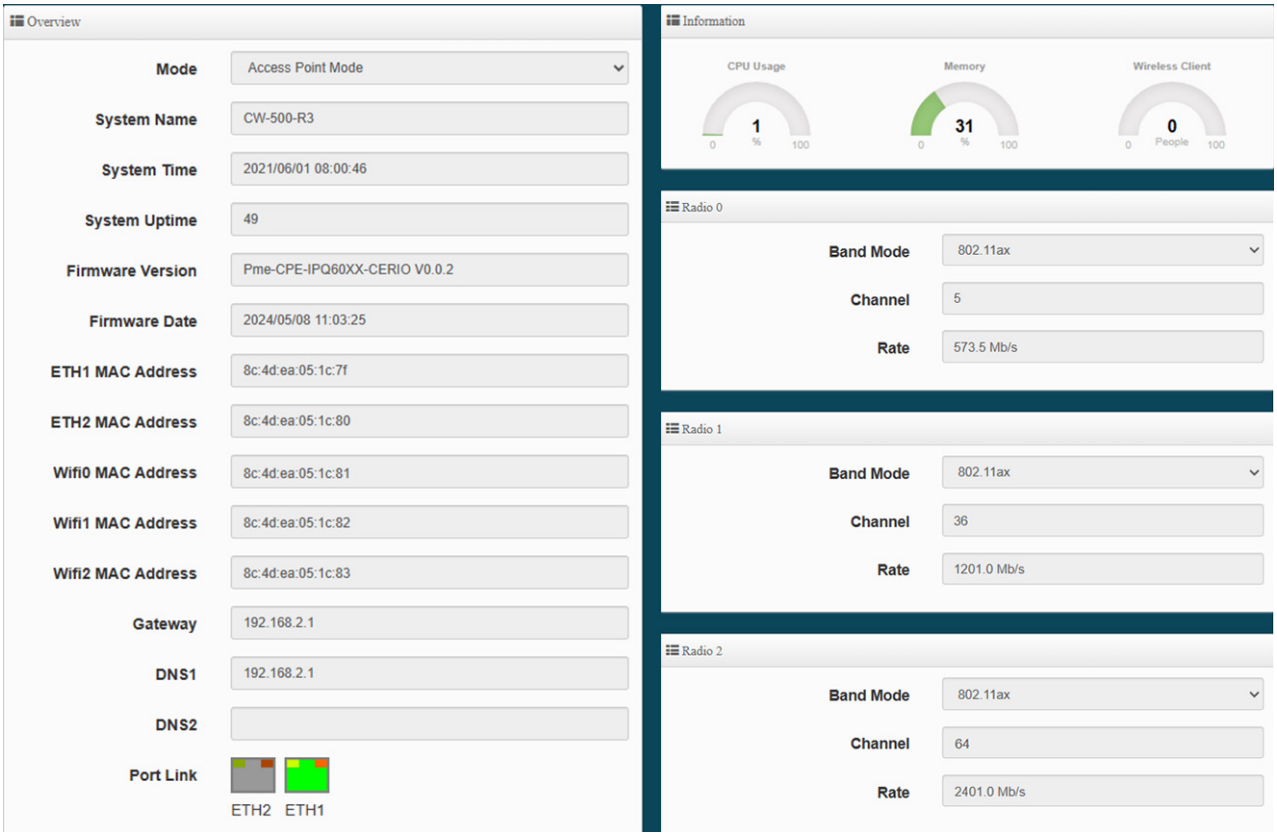
And Click **"OK"** to complete the fixed computer IP setting

1-3. Login Web Page

Launch as web browser to access the web management interface of system by entering the default IP Address, **http://192.168.2.254**, in the URL field, and then press Enter.



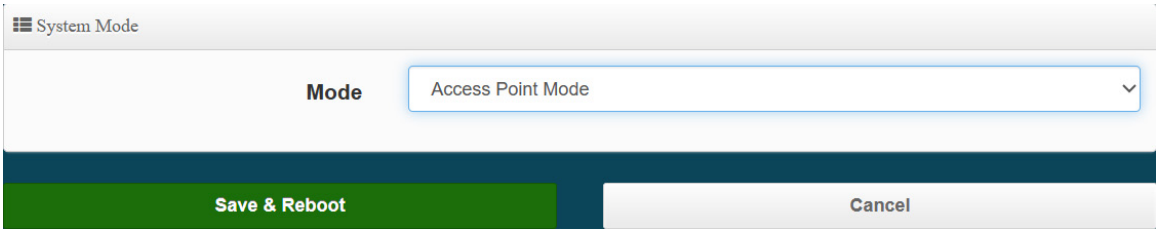
➢ Default login Usermane is 〝**root**〞 and Password is 〝**default**〞 .



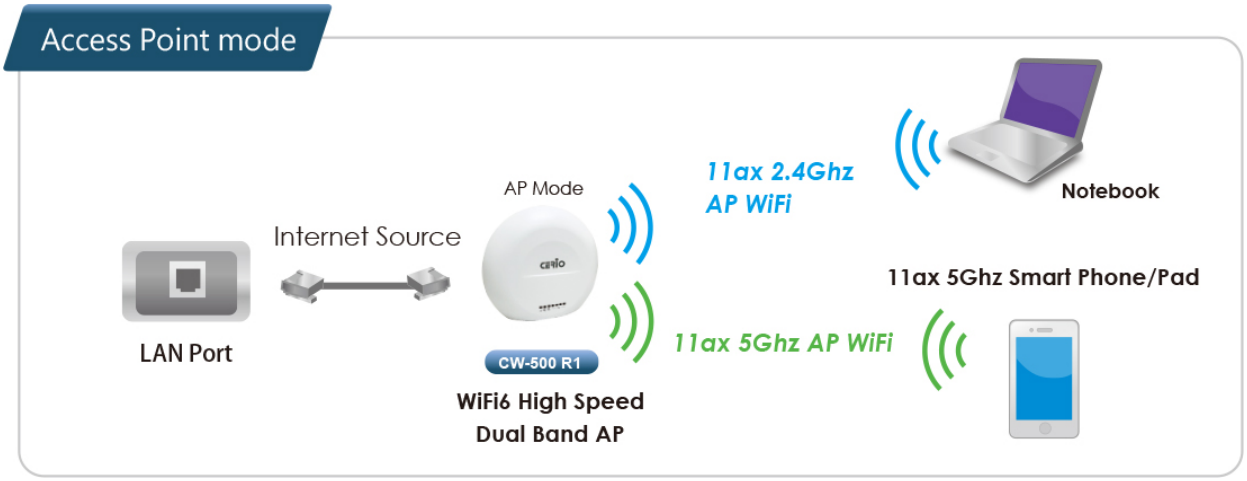
2. Operating Mode Introduction

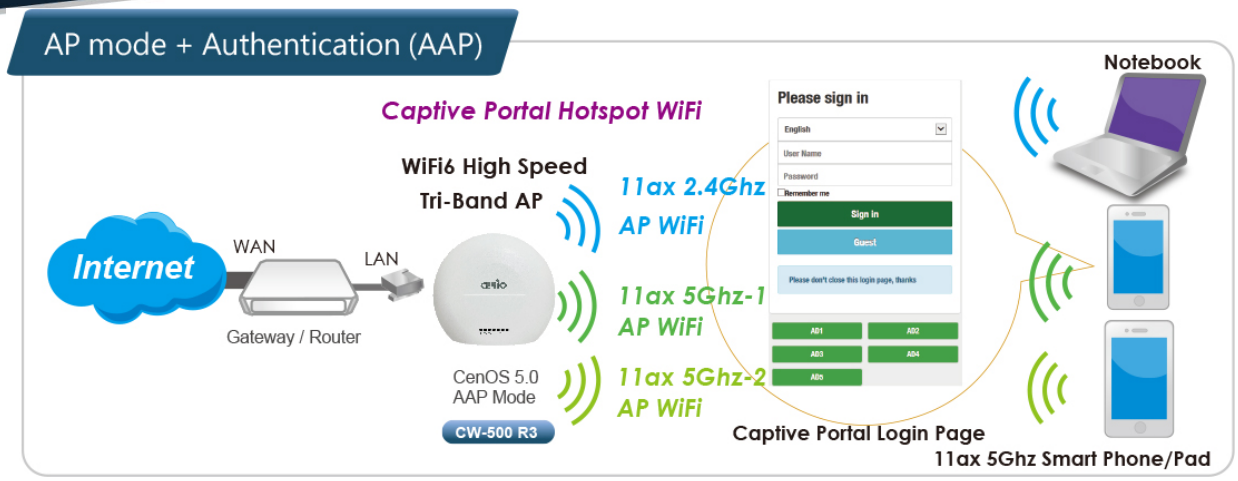
2-1. Access Point Mode (Default Mode)

Please click on System ->Mode Setup and choose Access Point Mode



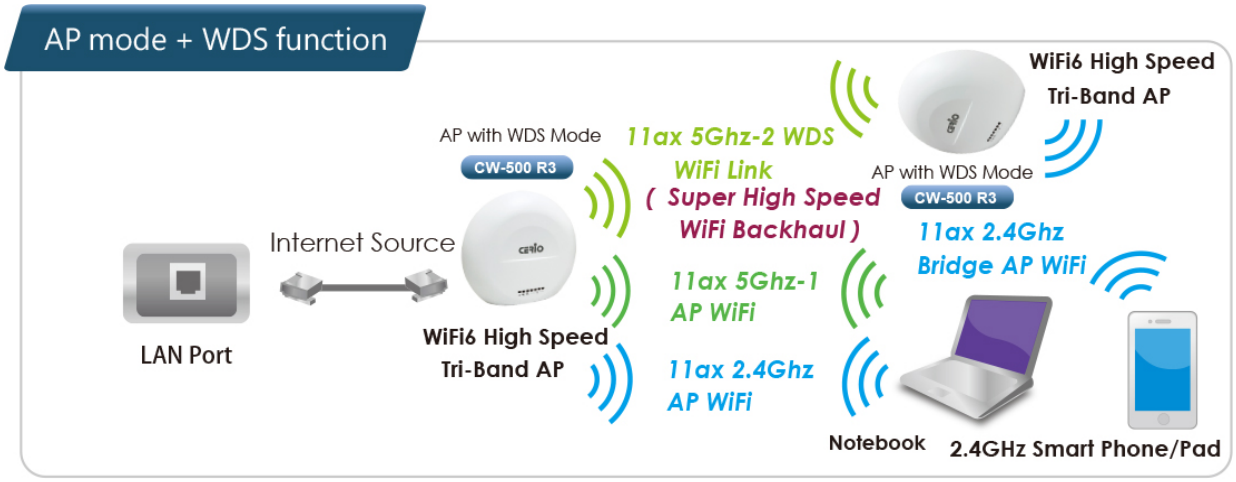
- It can be deployed as a traditional fixed wireless Access Point
- It allow wireless clients or Stations (STA) to access
- Supports DHCP Service, allowing for automated assigning of IP addresses to clients connecting to the network
- WDS Setup includes AES (Advanced Encryption Standard) Authentication
- This enables the wireless interconnection of Access Point in a IEEE802.11 network and accepts wireless
- Support Captive Portal authentication.





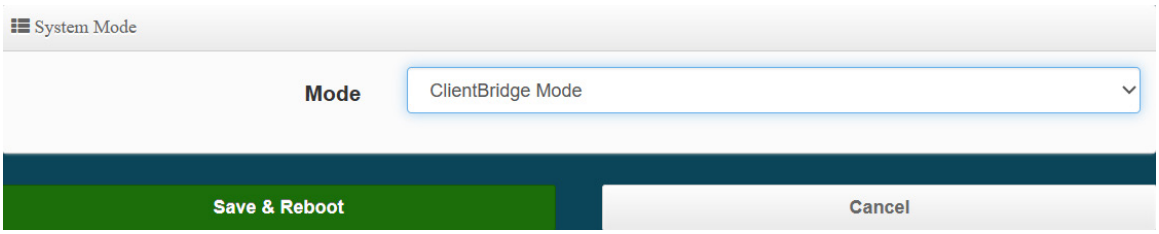
Application of WDS function in Access Point mode

WDS can be used for long-distance point-to-point wireless connections, as well as applications for long-distance point-to-multipoint wireless connections. You can enable the WDS function under the Access Point (AP Mode), which is an application of AP + WDS, which means that the device can also use the services of the Access Ponit (AP station), it can be used for long distance with another AP through WDS.



2-2. Client Bridge + Repeater Mode

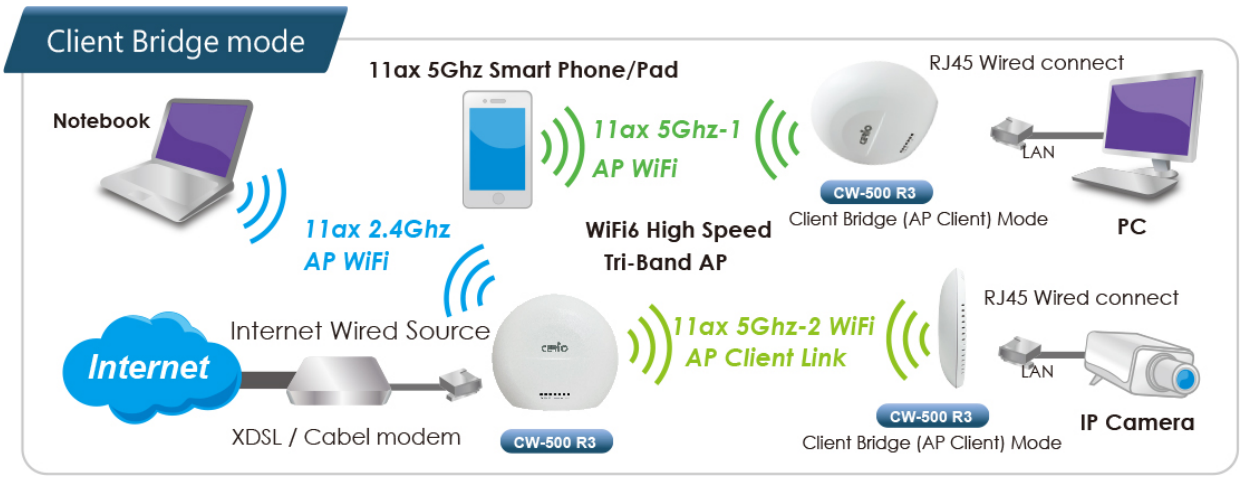
Please click on System ->Mode Setup and choose Client Bridge Mode



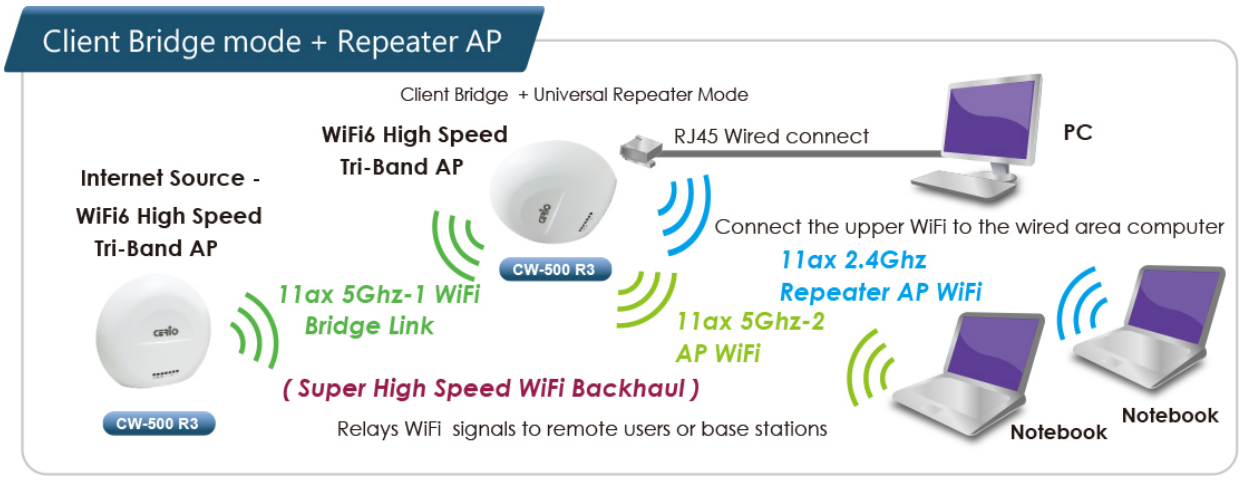
- It can be used as a Client Bridge + Repeater AP to receive wireless signals over last mile applications,

helping WISPs deliver wireless broadband Internet service to new residential and business customers.

- In this mode, the AP is enabled with DHCP Server functions. The wired clients of the AP are in the same subnet from Main Base Station and it accepts wireless connections from client devices. You can disabled the repeater extending AP function, which will enable the “AP Client ” function

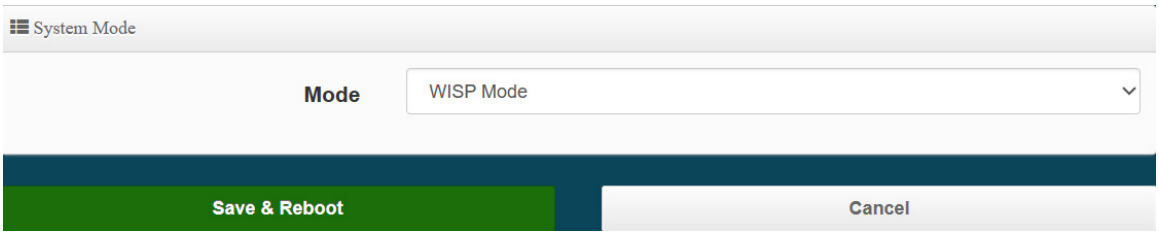


Note: If Client Bridge used 5GHz connection to AP station then Repeater AP only use 2.4GHz.



2-3. WISP + Repeater AP Mode

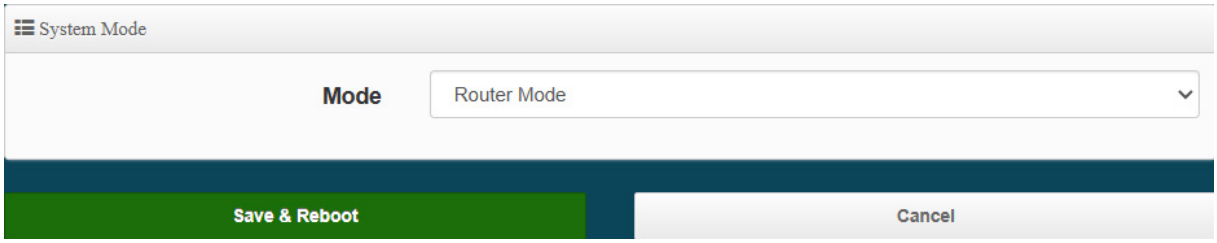
Please click on System ->Mode Setup and choose WISP Mode



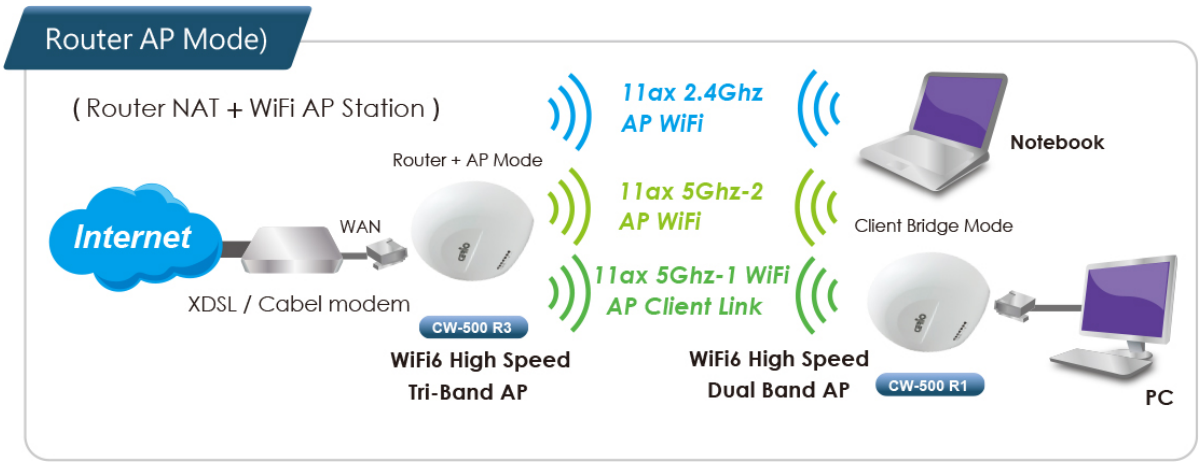
- It can be used as an WISP (Wireless Internet Service Provide) to receive wireless signals over last mile application, helping WISPs deliver wireless broadband Internet service to residents and business customers.
- In the WISP (CPE) mode, the CenOS 5.0 AP is a gateway enabled with NAT and DHCP Server functions. The wired clients connected to APs are in different subnet from those connected to Main Base Station, and, in WISP (CPE) mode, it does not accept wireless association from wireless clients.

2-4. Router mode

Please click on System -> Mode Setup and choose Router Mode

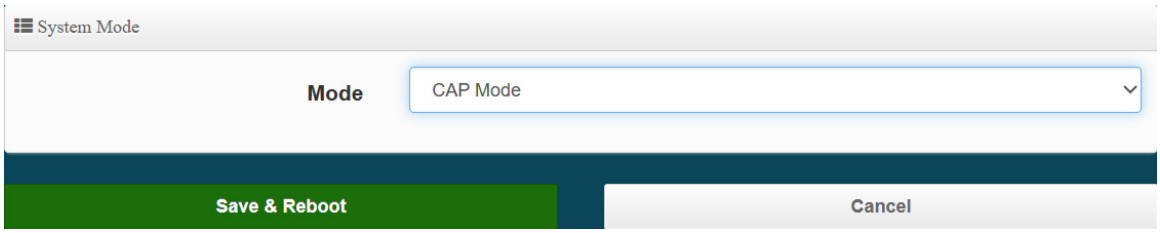


- Router AP with 802.1Q tag VLAN, can use multi-ESSID with VLAN Tag
- Router AP mode support Bandwidth management / virtual server / DMZ / Firewall / Basic DoS
- defense.

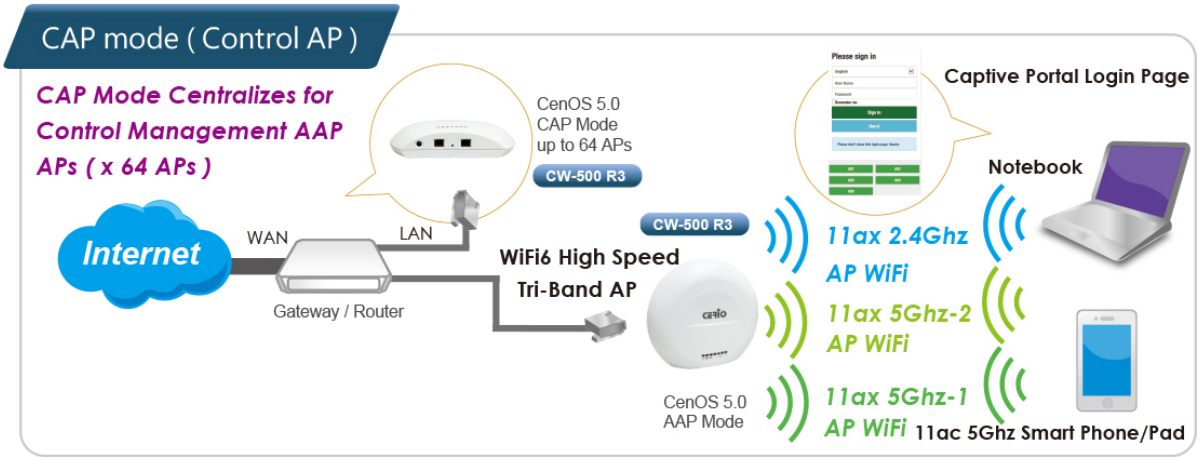


2-5. CAP mode (Centralizes Access Point)

Please click on System ->Mode Setup and choose CAP Mode



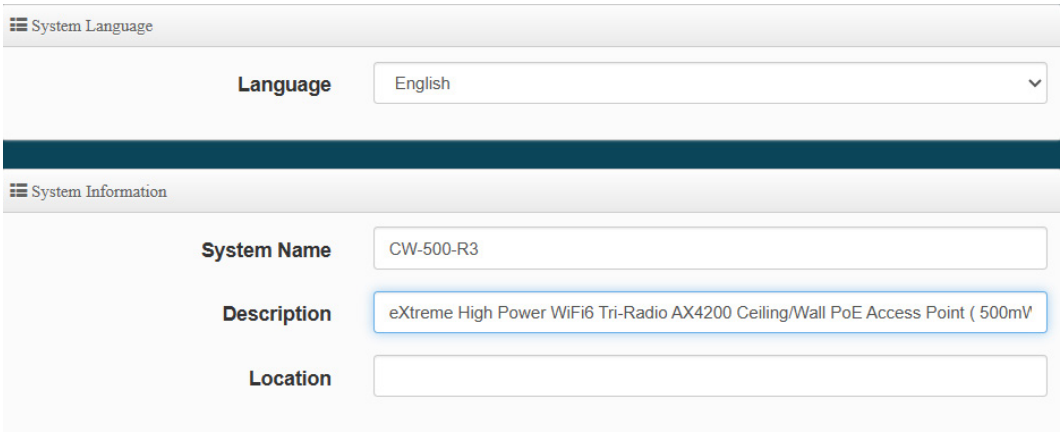
- Control Management of CenOS5.0 APs
- AP Management support 802.1Q VLAN infrastructure
- Centralized setting Access Point function and firmware upgrade.
- APs Group management for concept.



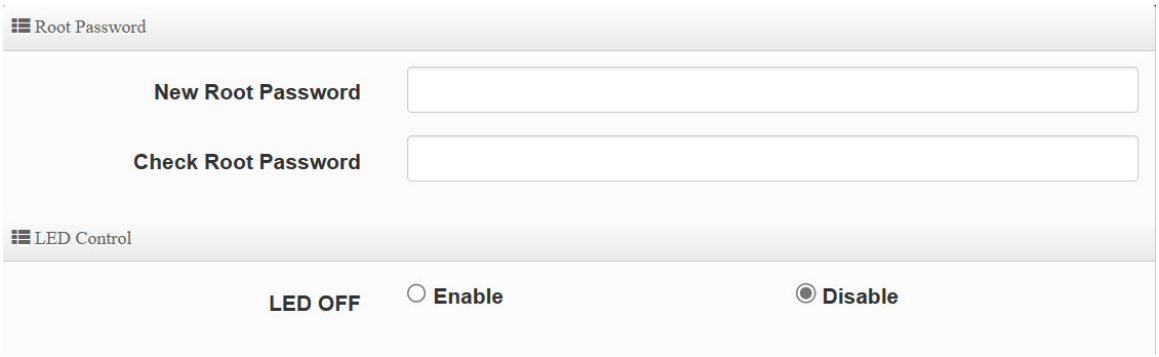
3. System Configuration

3-1. Management

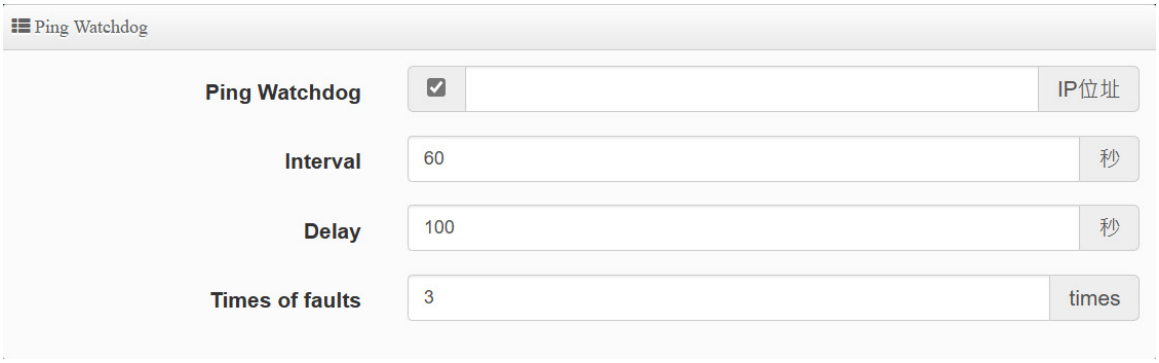
Please click on System ->Management and choose System Language.



- **System Language**：Administrator can select system language for English and Traditional Chinese
- **System Information**：Administrator can set the system name / Description and Location.

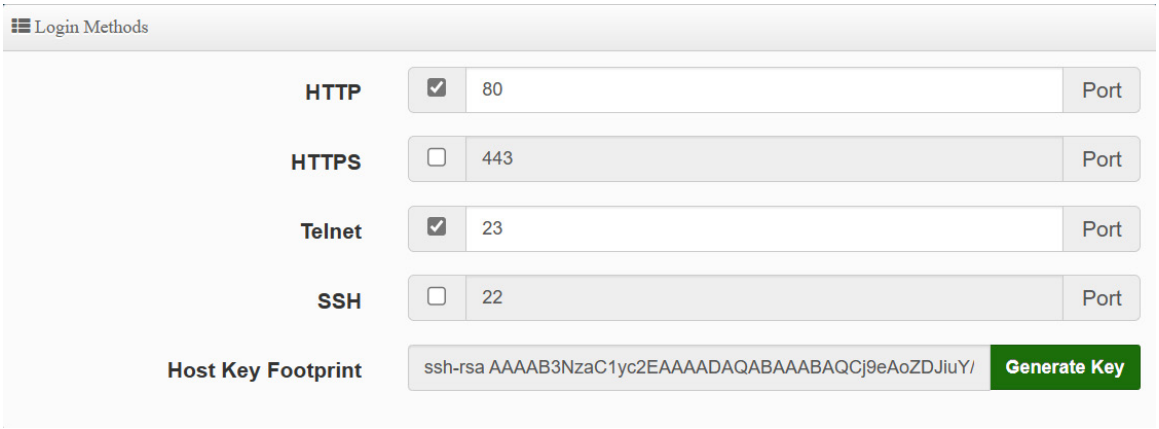


- **Root Password**：Administrator can change system login password.
- **LED Control**：Administrator can select enable or disable of the LED flashes.



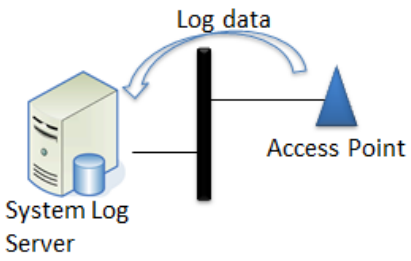
- **Ping Watchdog**：Ping Watchdog helps administrator to automatically reboot the system when its not working properly.

- **Interval**：Ping interval of time.
- **Delay**：After system start, the set time value starts execution Ping watchdog.
- **Times of faults**：After the error exceeds the set value, system will auto reboot.



➢ **Login Methods**：Administrator can set system login protocol of the http/https/telnet and SSH.

➢ **Access WAN**：Administrator can enable and disable login access from WAN Public IP address **(This feature only works when the mode is switched to Router mode or WISP mode with NAT attributes) .**

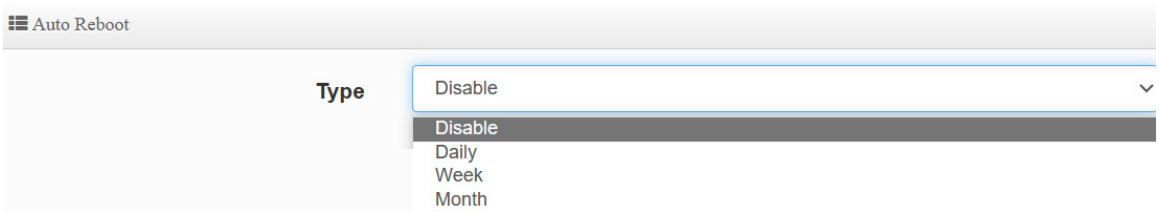


➢ **System Log Setup**：Administrator can be backup system log or authentication log to remote server. Please enter IP address and port of remote syslog server.

- **Remote Server:** Set the IP address of the remote system Log server。

- **Port:** Set the port number of the remote system Log server. **By the default , the built-in log center of the "Cerio AP Controller" corresponds to port 514.**

Notice	If you use the built-in log server function of Cerio's AP Controller product, please use the default 514 remote server port for the designated connection. The built-in log server of the AP management controller provided by Cerio Company provides a complete log format and all complete format information for its wireless AP devices of Cerio Company. It is recommended to use it in conjunction with it to fully understand all aspects of AP usage in the environment. Status information is left behind.



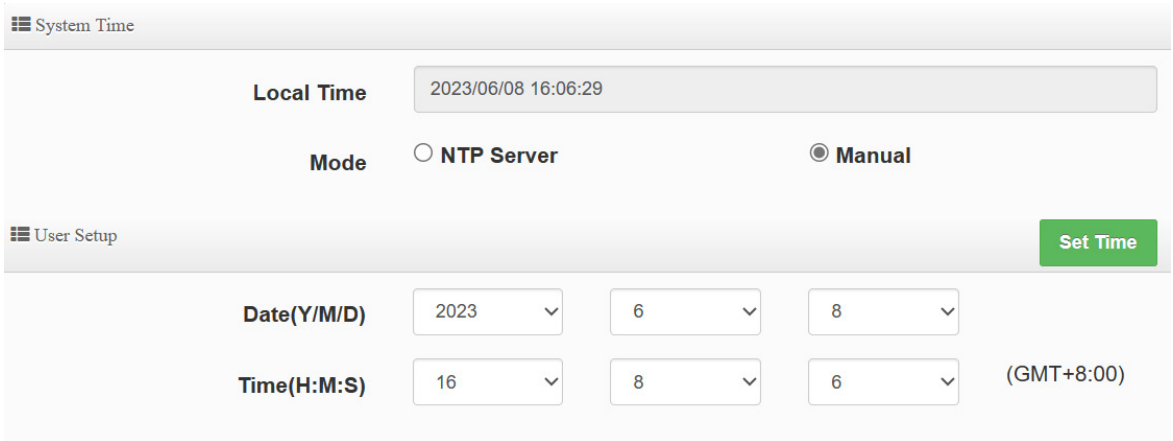
➢ **Auto Reboot**：The functions can Auto-reboot the system by Date/time management.

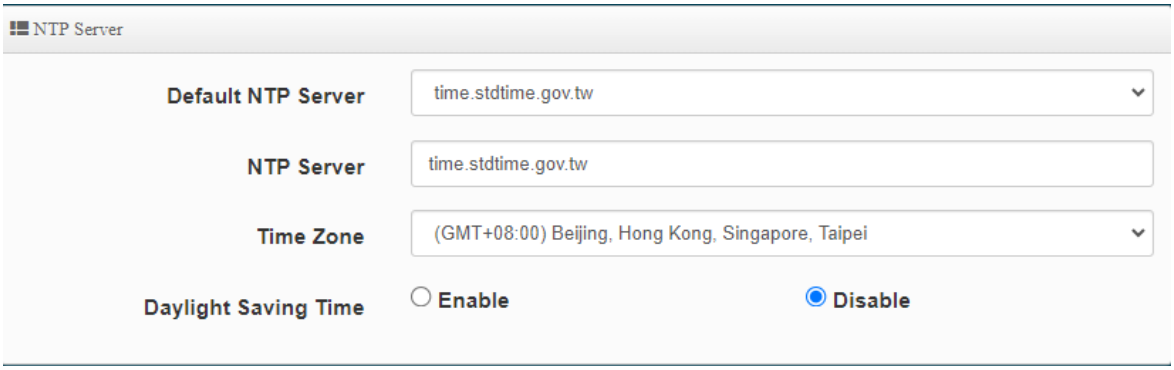
- **Daily :** Setting time to system reboot.
- **Weekly :** Setting frequency (ex. Weekly) and time of system reboot.
- **Monthly :** Setting Every month, fixed date and time to system reboot.

Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

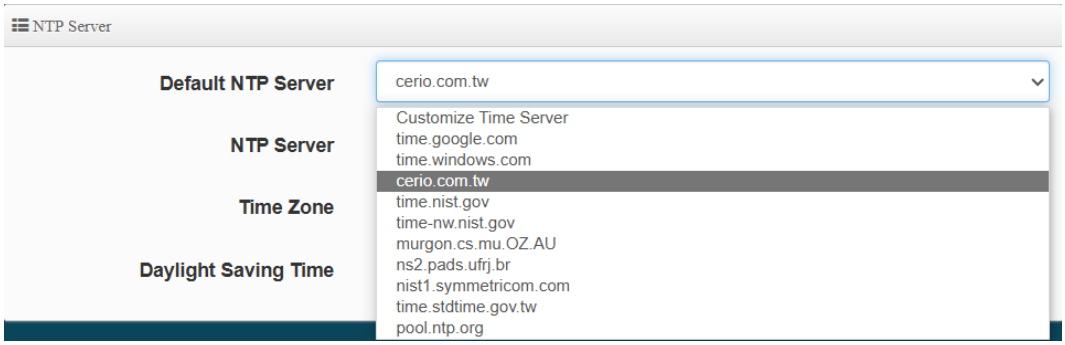
3-2. Configure Time Server

Please click on System ->Time Server and choose System Time.





- **System time**
  - **Mode**：Administrator can select NTP Server or Manual.
- **NTP Server:** System can auto update the system time. Administrator needs setting as NTP Server.
  - **Default NTP Server**：Administrator can select NTP Server.
  - **NTP Server**：Administrator can setting as NTP Server. **For example, select the time server of**



"cerio.com.tw" on the Internet as the basis for NTP time calibration as follows.

  - **Time Zone**：Administrator can select a desired time zone from the drop-down list.
  - **Daylight Saving Time**：Enable or disable Daylight saving.
- **Manual**：Administrator must to set the system time.

Notice	Administrator can select manual or via a NTP server to modify system time for the right local time. 1. This product supports hardware battery memory time keep design, When "Manual Update" time is selected and the time can be stored in the hardware memory, if the time cannot be stored and always becomes invalid and returns to the default time, the hardware battery must be replaced. 2. Administrator can select manual or via a NTP server to modify system time for the right local time. If select update the system time for the NTP Server, system must set gateway and DNS server, the system can be connected internet.

Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

3-3. SNMP

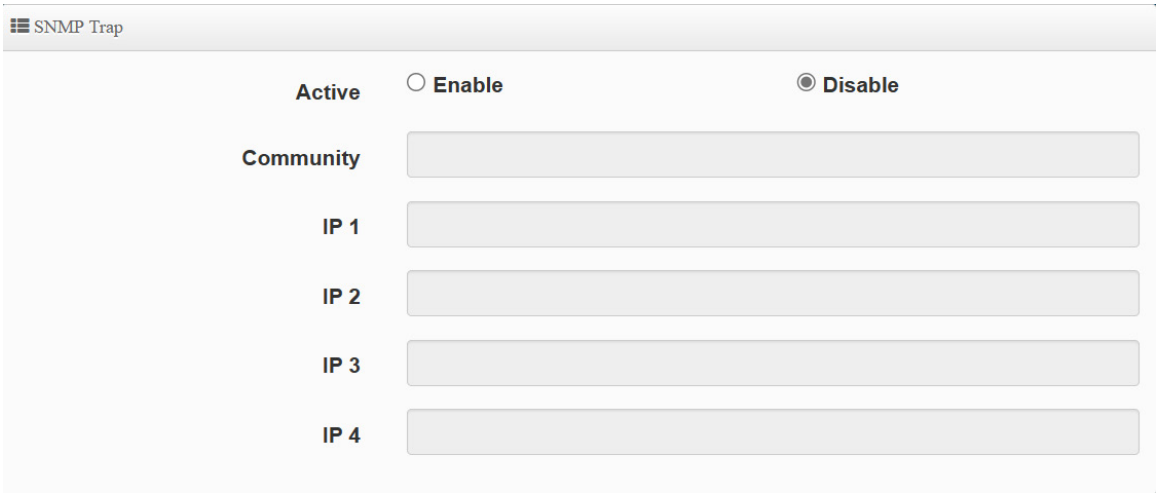
SNMP is an application-layer protocol that provides a message format for communication between SNMP managers and agents. By enabling SNMP function, the administrator can obtain the system information remotely.

Please click on **System -> SNMP** and follow the below setting.

- **SNMP V2c Function**
  - ✓ **Active**：Administrator can select Enable or Disable the service.
  - ✓ **RO Community**：Set a community string to authorize read-only access.
  - ✓ **RW Community**：Set a community string to authorize read/write access.

➢ **SNMP V3 Function**

- ✓ **Active**：Administrator can select Enable or Disable the service.
- ✓ **RO Username**：Set a community string to authorize read-only access.
- ✓ **RO Password**：Set a password to authorize read-only access.
- ✓ **RW Username**：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.

- ✓ **Active**：Administrator can select Enable or Disable the service.
- ✓ **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.

3-4. Configure Time Policy

Policy List

#	Comment	Mode	Edit
1	Policy 1	On Schedule	Edit
2	Policy 2	On Schedule	Edit
3	Policy 3	On Schedule	Edit
4	Policy 4	On Schedule	Edit
5	Policy 5	On Schedule	Edit

- Please click **Edit** button to setting Time Policy rules

Time Policy Rules

Comment: Policy 1

Mode: (●) On Schedule ( ) Out Of Schedule

- **Comment:** Enter the description of Time Policy rule.
- **Mode:** Administrator can select On schedule or Out of schedule to execution the rules.

Policy List — Create New Policy

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

Time Policy Rules

Day of Week: [x] Sun [x] Mon [x] Tue [x] Wed [x] Thu [x] Fri [x] Sat

Start Time: 00 : 00

End Time: 23 : 59

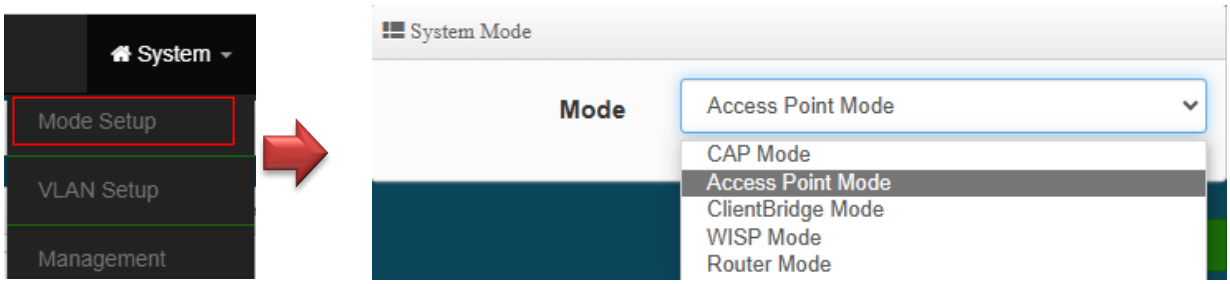
- **Administrator can set time for week / start time and end time.**

Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

4. Access Point mode

When AP mode is chosen, the system can be configured as an Access Point. This section provides detailed explanation for users to configure in the AP mode with help of illustrations. In the AP mode, functions listed in the table below are also available from the Web-based GUI interface.

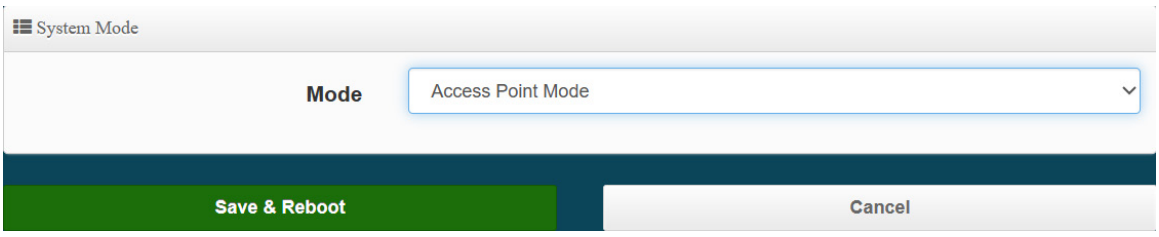
4-1. Change Setup mode



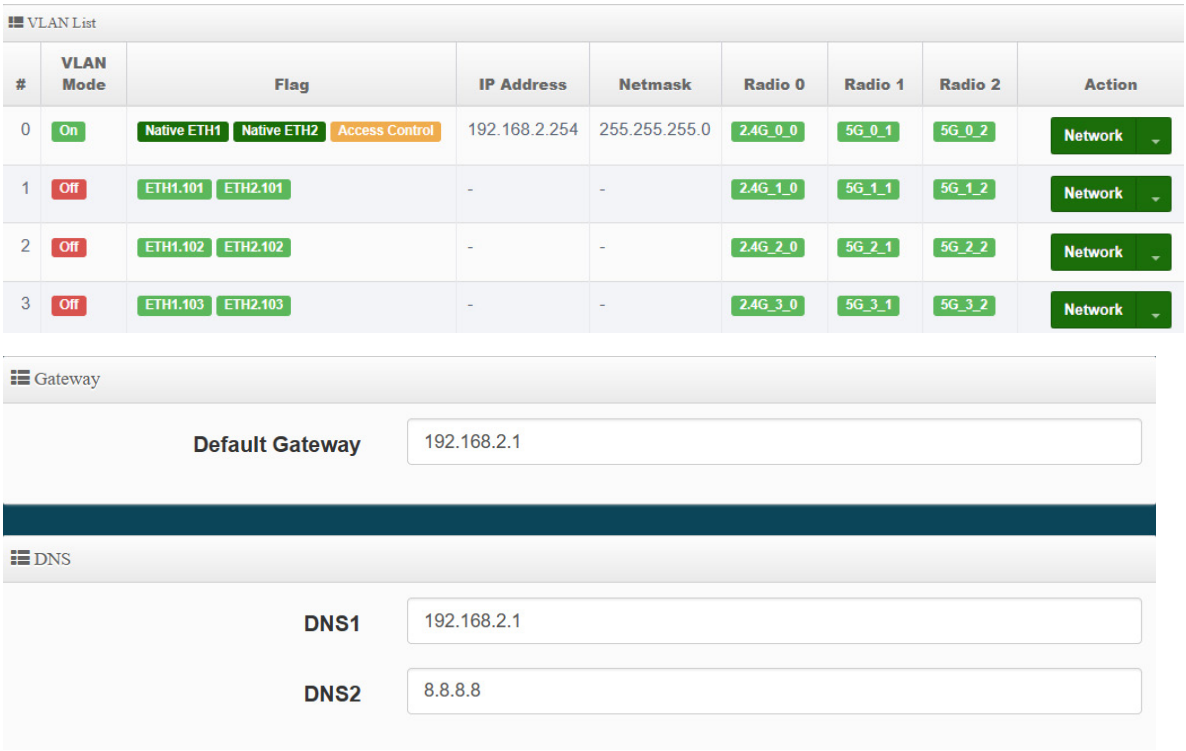
Notice

1. Please note that the LAN IP addresses in each mode are different from each other and will not continue. For the first time after switching modes, always perform access management on the LAN default IP address of 192.168.2.254
2. Cerio's dual-band wireless base station supports 16 VLANs and 48 SSIDs (Each VLAN supports 2.4Ghz SSID x1 and 5Ghz-1 band SSID x1 and 5Ghz-2 band SSID x1)

4-2. VLAN Setup



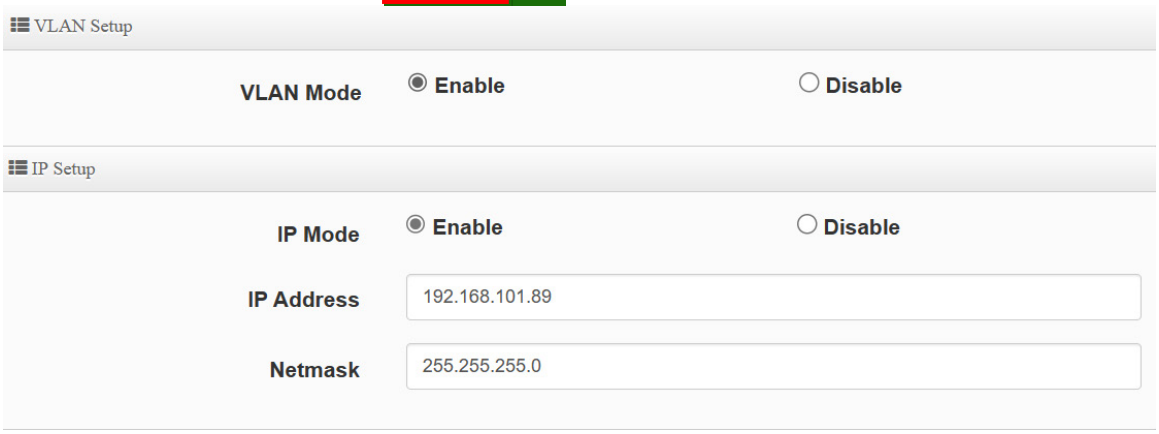
Here are the instructions to setup the local IP Address / Netmask / Gateway / DNS and management Access Point 2.4G or 5G-1 Radio or 5G-2 Radio on/off. Administrators can change settings such as LAN Spanning Tree and Tag VLAN functions.



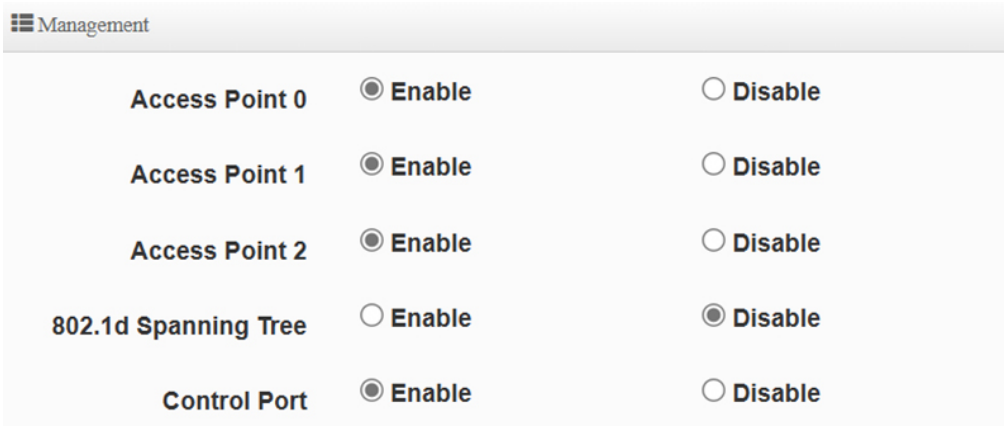
- **VLAN Mode**：Display on/off for the VLAN network.
- **Flag**：Display master VLAN and VLAN Tag No. information. When displayed Native ETH1 Native ETH2 it means that the current main wired connection is this virtual network as the main login system.
- **IP Address**：Display IP Address for VLAN Network
- **NetMask**：Display IP netmask.
- **Radio 0**：Display radio 2.4G SSID name.
  - Action : Click the Network button to enter the LAN setting page. Click the Network drop-down arrow to display the wireless setting function list.
- **Radio 1**：Display radio 5G-1 SSID name.
  - Action : Click the Network button to enter the LAN setting page. Click the Network drop-down arrow to display the wireless setting function list.
- **Radio 2**：Display radio 5G-2 SSID name.
  - Action : Click the Network button to enter the LAN setting page. Click the Network drop-down arrow to display the wireless setting function list.
- **Default Gateway**：Set the gateway IP address.
- **DNS**：Set the IP address for DNS resolution.

Network Setup

Administrator can click " Network " button to set VLAN network functions.

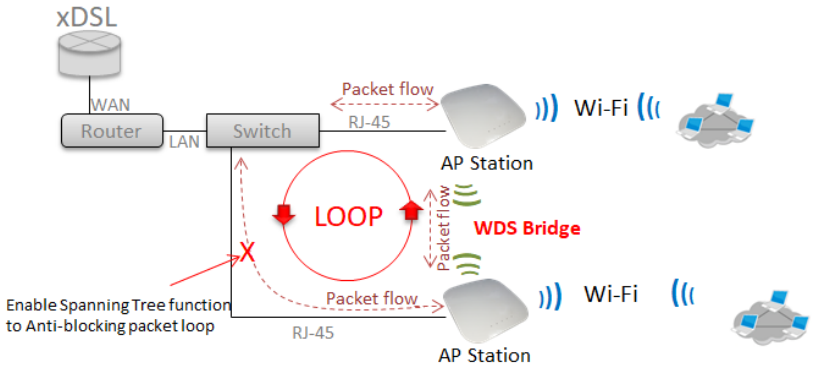


- **VLAN Mode**：Administrator can select Enable or disable for the VLAN Network.
- **IP Mode**：Administrator can select enable or disable function for VLAN IP.
- **IP Address/ NetMask**：Administrator can set IP address and netmask for the VLAN.



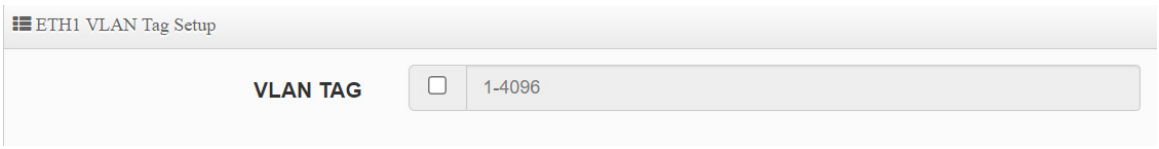
Management

- **Access Point 0**：Administrator can Enable or Disable 2.4G Radio.
- **Access Point 1**：Administrator can Enable or Disable 5G-1 Radio.
- **Access Point 2**：Administrator can Enable or Disable 5G-2 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, which is also referred to as STP, is defined in the IEEE Standard 802.1d



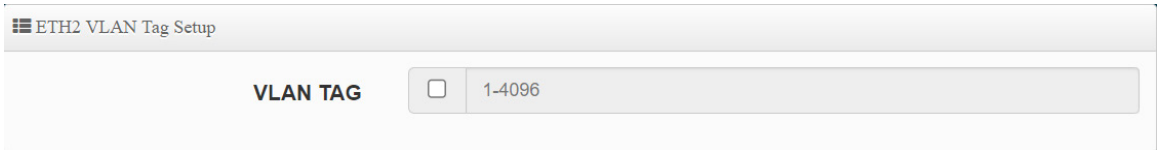
- **Control Port**：Administrator can select one of the VLAN as managed AP.
- **VLAN Tag Setup:** Set the VLAN used tags.

ETH1 VLAN Tag Setup



- **Network port VLAN Tag Setup:** Follow standard 802.1Q specification, the function can be turned off or enabled. You can define the tag to the ETH1 physical network port , which can be set from 1 to 4096.

ETH2 VLAN Tag Setup



- **Network port VLAN Tag Setup:** Follow standard 802.1Q specification, the function can be turned off or enabled. You can define the tag to the ETH2 physical network port , which can be set from 1 to 4096

Notice

If ETH0 is configured to use VLAN Tag, then entering the management interface requires a VLAN with the same tag to enter the management settings. Domains other than this VLAN will be completely blocked.

Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

Network Pull-down menu

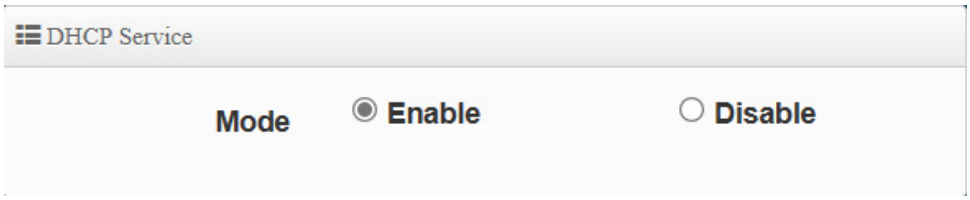
Administrator can set DHCP Server and 2.4/5G security for the access point and set 802.11r fast roaming.

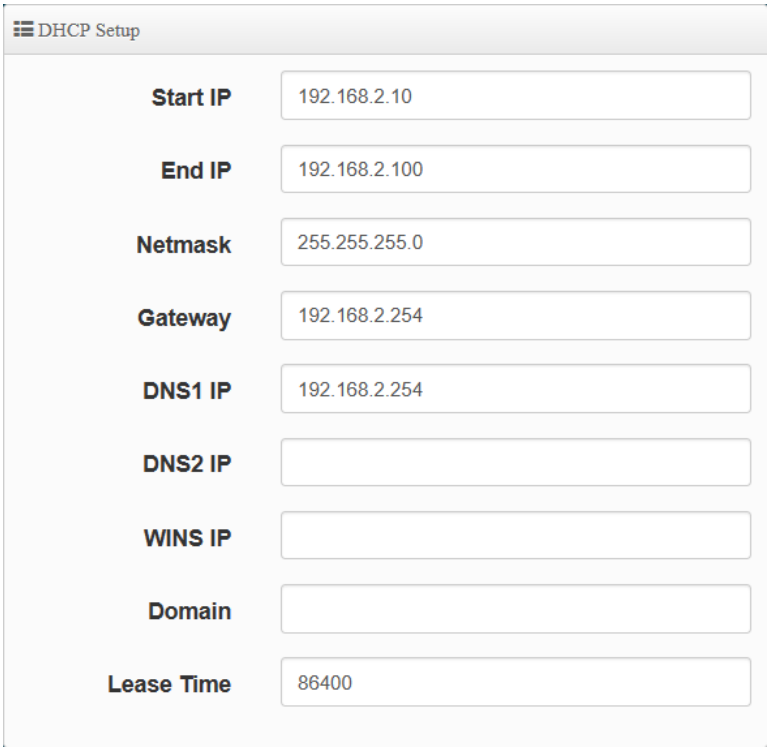
Please click 

pull-down button.

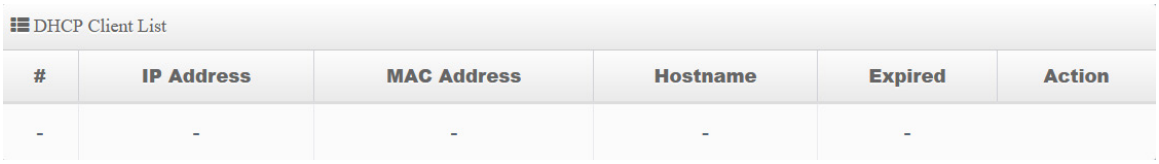
4-2-1 DHCP Server

Administrator can select enable / disable the function





- **Start IP:** Set Start IP address for DHCP Service.
- **End IP:** Set End IP address for DHCP Service.
- **Netmask:** Set IP Netmask, the default is 255.255.255.0
- **Gateway:** Set Gateway IP address for DHCP Service.
- **DNS(1-2) IP :** Set DNS IP address for DHCP Service.
- **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



➢ **DHCP Client List**

Administrator can view IP address used status of client users on each DHCP Server.

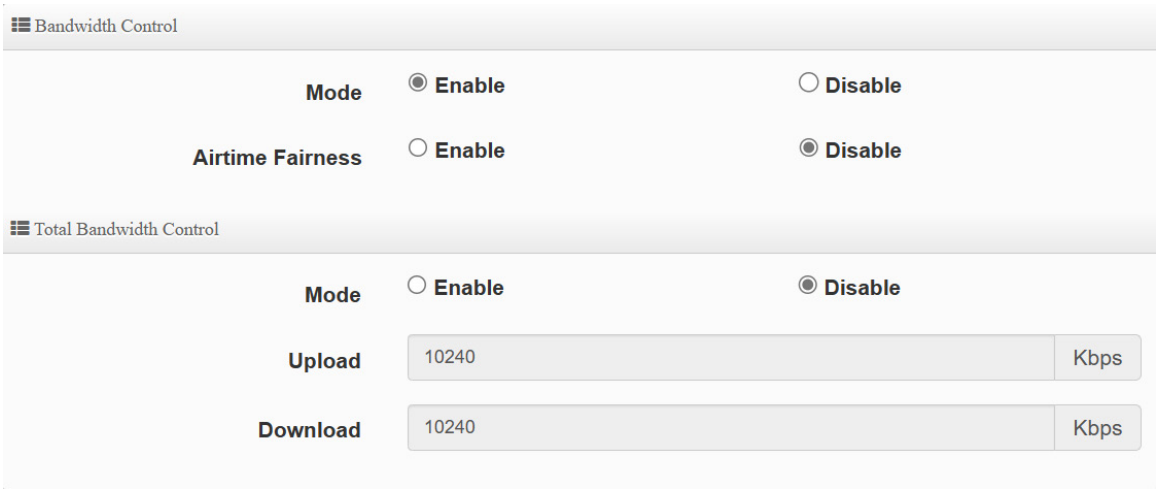
➢ **Static Lease IP Setup**：Administrator can set be delivered fixed IP address to the users.

- **Comment:** Enter rule description.
- **IP Address:** Enter access point IP.
- **MAC Address:** Enter Client MAC Address of PC network.

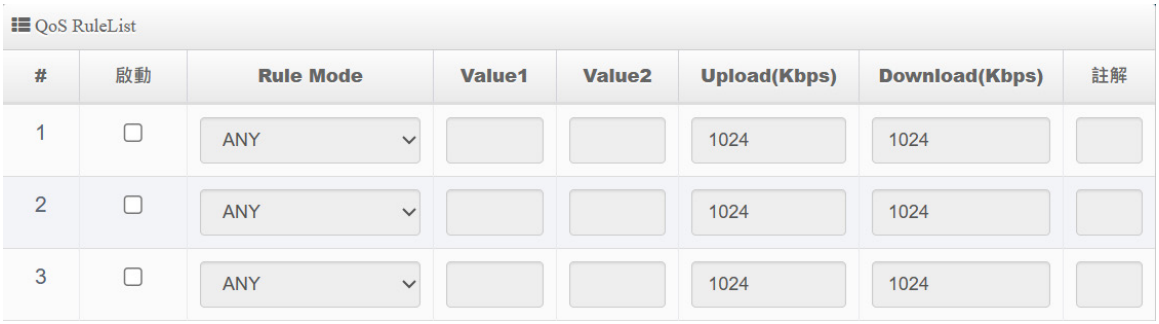
Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

4-2-2 Bandwidth Control

Administrators can set bandwidth limit the max/min bandwidth of the Wi-Fi users, Bandwidth control can set IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP and WEB.



- Bandwidth Control / Total Bandwidth Control
  - **Mode:** Administratior can Enable or Disable the function.
  - **Airtime Fairness:** TX/RX traffic balancing, if device use point-to-point (WDS or AP mode + Client Bridge) then recommended to enable it.
  - **Total Bandwidth Control:** Administrator can set total bandwidth used limit in VLAN

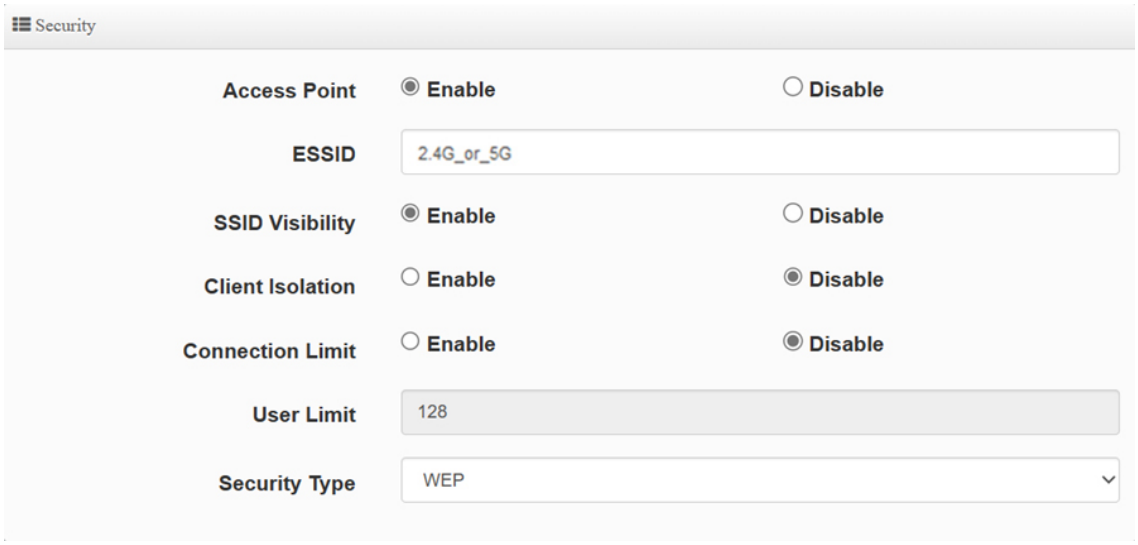


- **QoS Rule List:** Administrator can set bandwidth limit by IP/MASK, IP Range, Port(Service), SIP, RTP/RTSP, WEB protocol , each VLAN can set 10 bandwidth management rule.

Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

4-2-3 Radio 0(2.4G)/Radio1(5G)/Radio2(5G) Access Point Setup

Administrator can Enable or Disable radio 0/1/2 (2.4/5G/5G) Wi-Fi. If radio 0/1/2 (2.4/5G/5G) are enabled, administrators can set the SSID and security for the 2.4/5G access point.

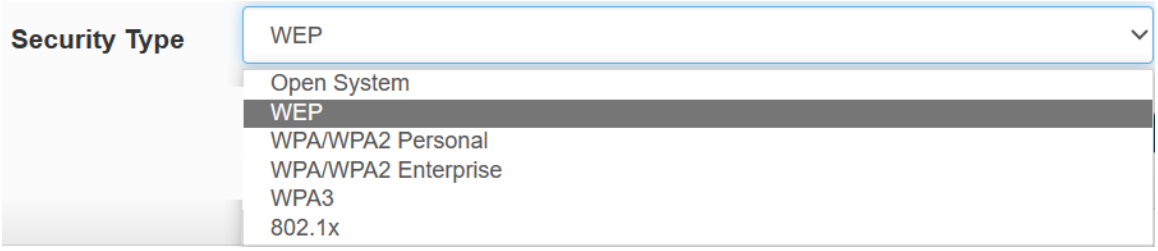


- **Access Point:** Administrator can Enable or Disable the radio 0/1/2 (2.4G/5G/5G).

- **ESSID:** Administrator can set Wi-Fi SSID name
- **SSID Visibility:** Administrator can select Enable or Disable the Visibility.
- **Client Isolation:** Enable or Disable the client isolation function.
- **Connection Limit:** Administrator can select Enable or Disable WiFi connection Limit.

【Supports 128 users to access at the same time.】

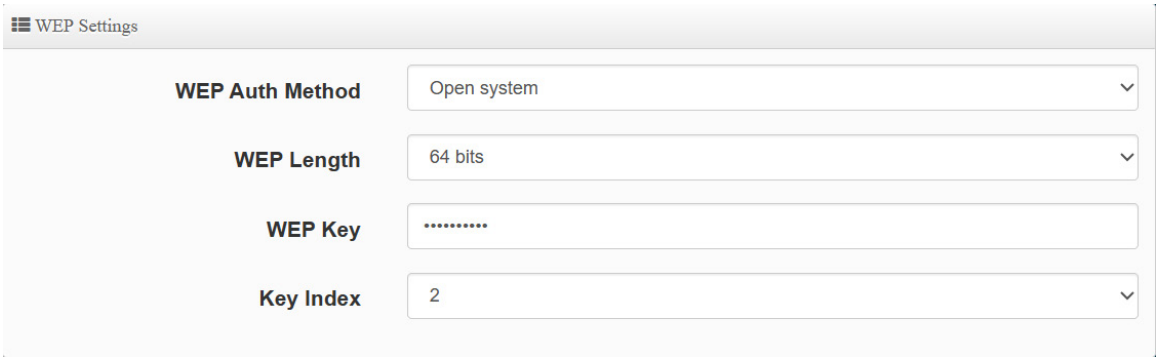
- **Security Type:** Select the desired security type from the drop-down list; the options are Open System, WPA-PSK/WPA2-Personal, WPA/WPA2-Enterprise, WPA3 and 802.1x



Notice

Notes: The WEP encryption mode is currently known to be not the most secure wireless encryption method, and will not be able to support 802.11ac/ax. It is not recommended that you continue to use this WEP encryption mode. It is recommended that you use a rate that meets 802.11ac/ax Correspondingly supported encryption modes above WPA / WPA2 to increase your wireless network security.

- **Open System**：Data is not unencrypted during transmission when this option is selected.**(be not recommended for use)**

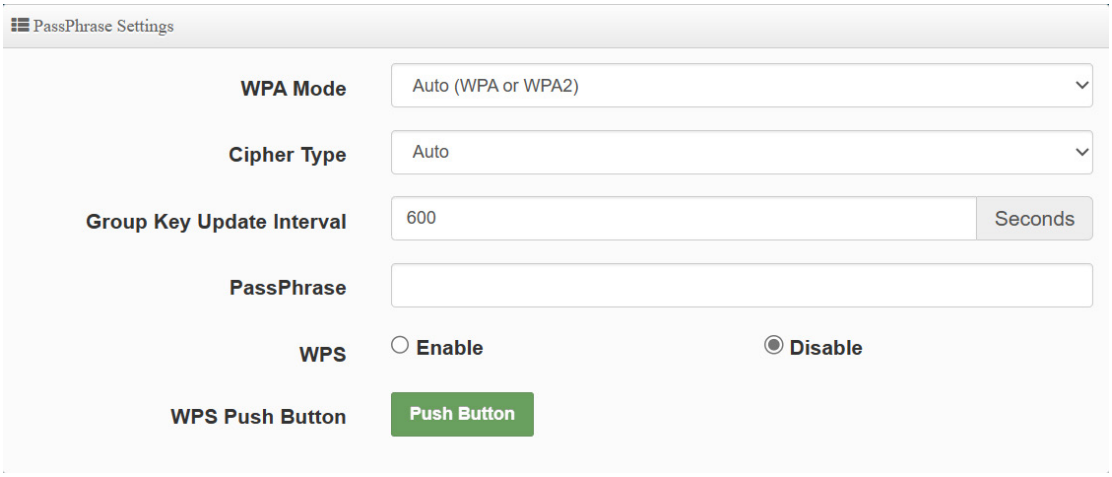


- **WEP**：
  - ✓ **WEP Auth Method**：Administrator can choose the WEP Open system open authentication method or the WEP Shared password authentication method.
  - ✓ **WEP Length**：Administrator can choose to use 64bits, 128bits, and 152bits encryption key lengths, but must make sure that the wireless network card used by your wireless client also

supports the corresponding wireless key length.

- ✓ **WEP Key**：There are four groups of optional settings the 16-bit (HEX) key value.
- ✓ **Key Index**：Administrator can pre-set 4 WEP Key for your WEP and "save".when the future wireless client wants to connect, can be choose which group of wireless keys and establish a connection through WEP encryption.

Notice	Note: If you choose to use WEP encryption mode, please enter the corresponding WEP key value according to the following requirements. 64bits: 10 groups of Hexadecimal characters (0~9, A~F and a~f can be used) 5 groups of ASCII characters (0~9, A~Z and a~z can be used) 128bits: 26 groups of Hexadecimal characters (0~9, A~F and a~f can be used) 13 groups of ASCII characters (0~9, A~Z and a~z can be used) 152bits: 32 groups of Hexadecimal characters (0~9, A~F and a~f can be used) 16 groups of ASCII characters (0~9, A~Z and a~z can be used)



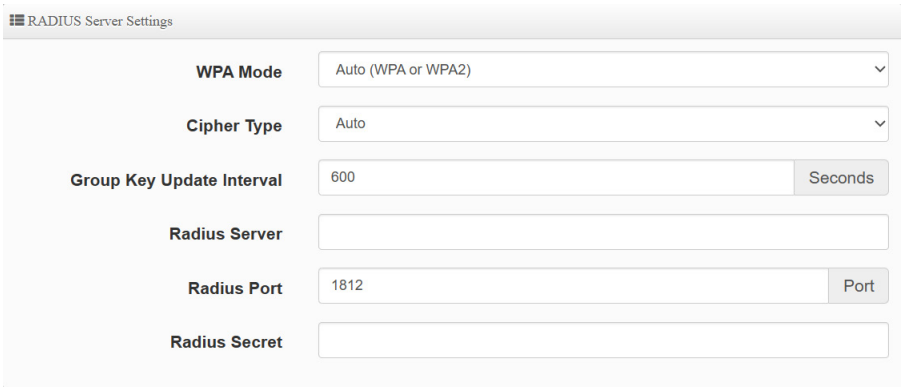
- ● **WPA / WPA2-Personal**：
  - ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
  - ✓ **Cipher Type:** Administrator can select use AES or TKIP with WPA / WPA2 encryption method.
    - ◆ **AES** is short for "**Advanced Encryption Standard**", The AES cipher is specified 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.

Notice	Note: When setting WEP or TKIP encryption, the data rate will not exceed 54 Mbps. The IEEE 802.11n protocol prohibits the use of high throughput with WEP or TKIP as unicast keys. If you use these encryption methods (such as WEP, WPA-TKIP, WPA2-TKIP), your data rate will be reduced to 54 Mbps, or if it is used for commercial purposes, such as applications where the end user cannot connect to the wireless at a higher speed than 54 Mbps.

- ✓ **Group Key Update Interval**: The time interval is for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Pass Phrase:** Enter the ESSID pass phrase.
- ✓ **WPS Push Button:** Administrator can used WPS function to link WiFi client. If enabled, administrator can click the WPS Push Button.

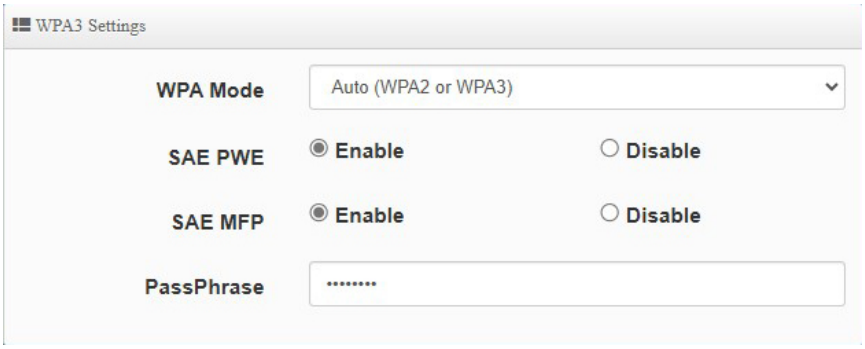


- **WPA / WPA2-Enterprise**：
  - ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
  - ✓ **Cipher Type:** Administrator can select use AES or TKIP with WPA / WPA2 encryption method.
    - **AES** is short for "**Advanced Encryption Standard**", The AES cipher is specified 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.

Notice

Note: When setting WEP or TKIP encryption, the data rate will not exceed 54 Mbps. The IEEE 802.11n protocol prohibits the use of high throughput with WEP or TKIP as unicast keys. If you use these encryption methods (such as WEP, WPA-TKIP, WPA2-TKIP), your data rate will be reduced to 54 Mbps, or if it is used for commercial purposes, such as applications where the end user cannot connect to the wireless at a higher speed than 54 Mbps.

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



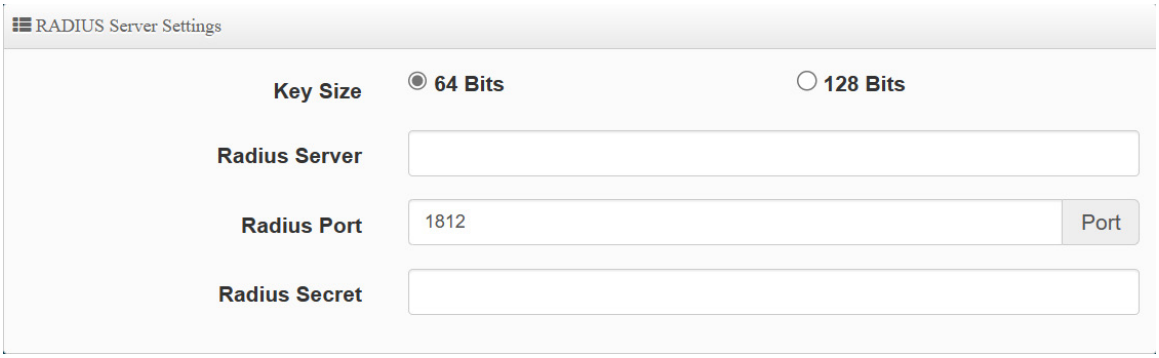
- ● **WPA3 :**

The 802.11ax peer-to-peer entity authentication mode is different from the Pre-Shared Key .

- ✓ **SAE Password**：When the administrator sets this virtual wireless network SSID to use WPA3 calculation, the SAE connection password must be at least 8 characters.
- ✓ **SAE PWE**：Optionally enable the SAE PWE (Password Element) function, before exchanging SAE authentication messages, both parties will generate a private element PWE (Password Element) and two private values (rand and mask) for advanced authentication exchange.
- ✓ **SAE MFP**：The SAE password authentication mechanism adds a more secure anti-theft, anti-spy, and anti-skimming password Management Frame Protection (MFP).
  If the AP enabled this mode, please ensure that both the AP and the client running in this mode need Management Frame Protection (MFP) support.

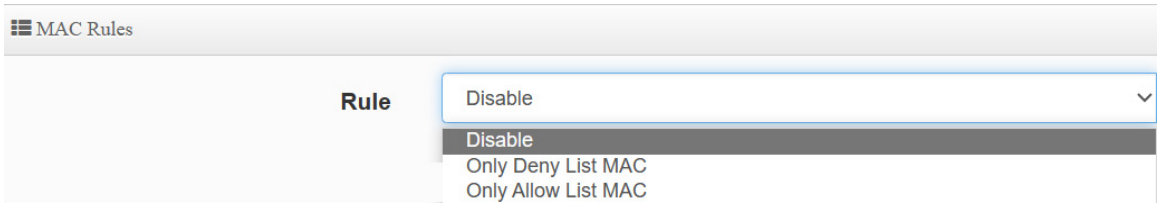
Notice

The WPA3 is latest and most secure protocol currently available for Wi-Fi devices. It is applicable to all access devices that support Wi-Fi 6 (802.11ax). If the wireless access card does not support WPA3 calculation mode, that you adjust the use to WPA2 / AES calculus mode recommended.



- **802.1x**
  - ✓ **Key Size**：Enter the IP address of the Authentication RADIUS server.
  - ✓ **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.

4-2-4 MAC Filter

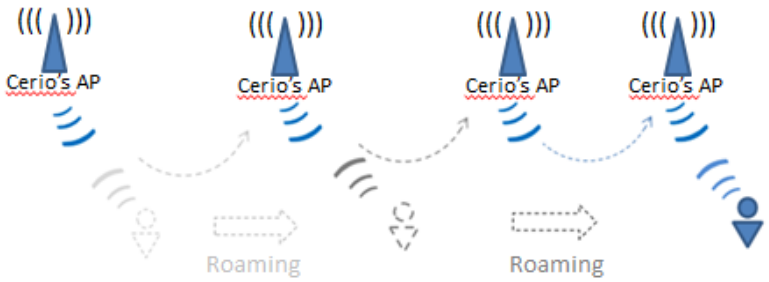


- **Only Deny List MAC**：Administrator can add wireless users MAC address in MAC list. The access point will deny connection in MAC address list.
- **Only Allow List MAC**：Administrator can add wireless users MAC address in MAC list. The access point will allow connection in MAC address list.

- **MAC Address:** Set managed MAC address of the client.
- **MAC Address List:** Display managed MAC address list.

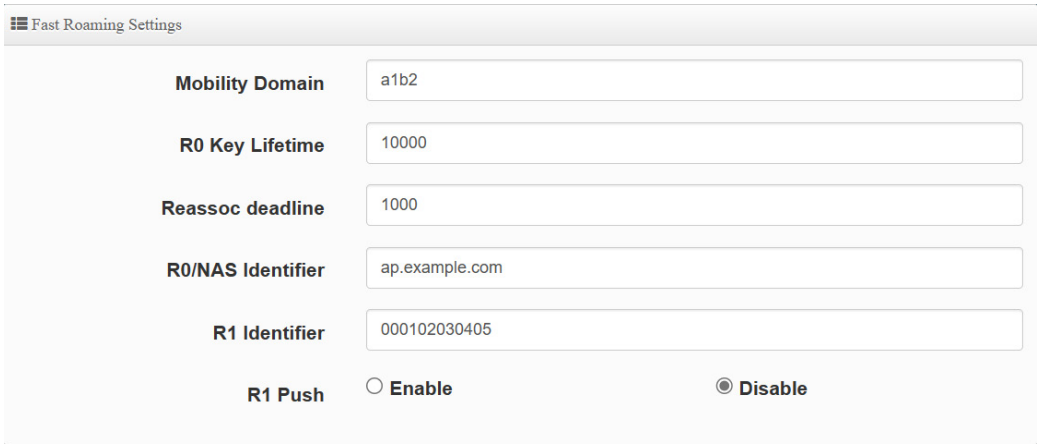
Click **"Save"** button to save your changes. Then click Reboot button to activate your changes.

4-2-5 802.11r Fast Roaming Setup



The Tri band Access Point supports 802.11r/802.11k function for 2.4G (Rado 0)and 5G (Rado 1)and (Rado 2). 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.

Notice	If this feature is enabled when using 802.11r fast roaming, the wireless user equipment must support 802.11k functionality to work properly

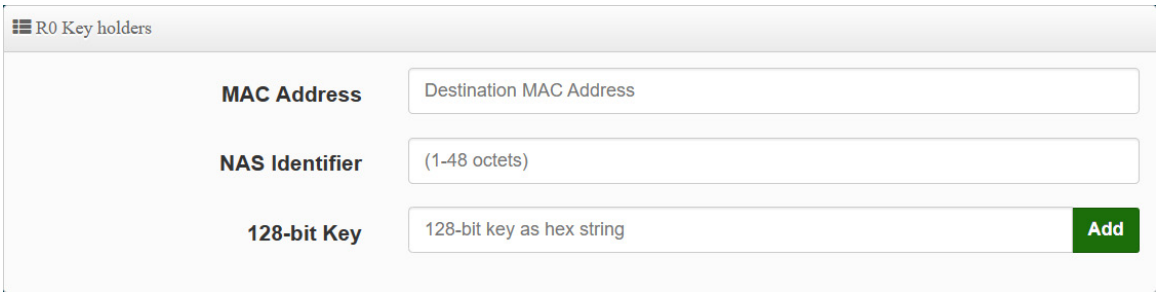


- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition.

Notice

This setting must be 2-octet of hex string codes. For example, enter 8c4d

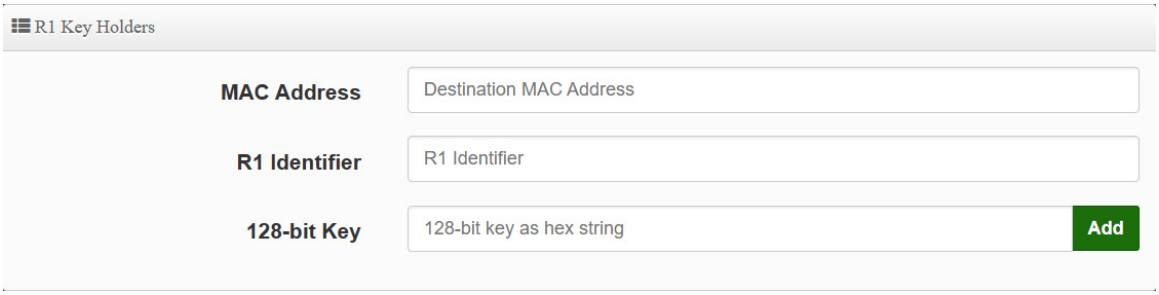
- **R0 Key Lifetime:** Default lifetime of the PMK-RO in minutes, the default is 10000, administrator can setting 1~65535.
- **Reassoc deadline:** Reassociation deadline in time units (TUs / 1.024 ms; range 1000~65535). The default is 1000.
- **R0/NAS Identifier:** PMK-R0 Key Holder identifier. When 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 or disable. If enable the function will automatically sent the R1 Key.



- **R0 Key holders :** To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access

Points.

- **MAC Address:** Administrators must enter the MAC Address of another side AP.
- **NAS Identifier:** Enter 1~48 octets of network domain name.
- **128-bit Key:** Enter Shared Key of 128 bit.



➢ **R1 Key holders :** Enter a unified set of R1 Key Holder identification certification.

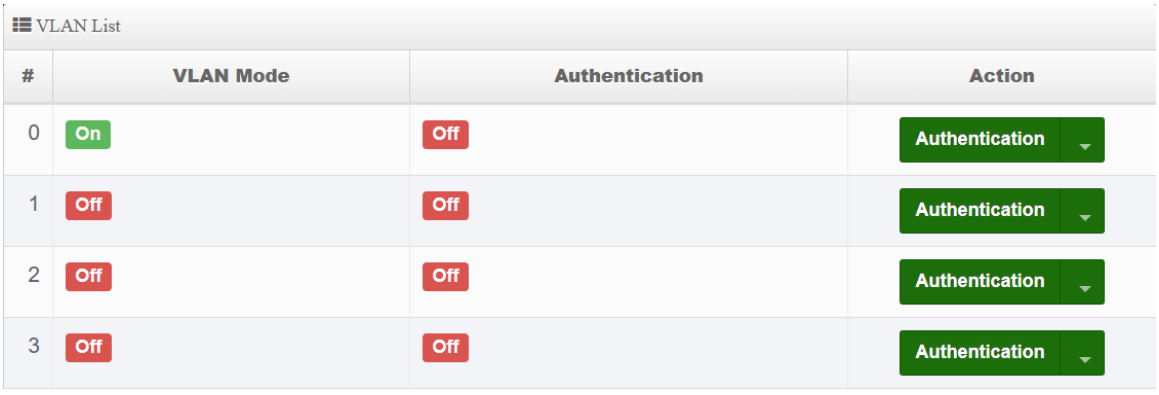
- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

Click **"Save"** button to save your changes. Then click Reboot button to activate your changes.

4-3. Authentication

This function is for Web Authentication in **Access Point** mode**,** the function is for Web Authentication. It supports authentication for local users / RADIUS Server / OAuth2.0 and Guest. The system supports in N VLANs with web authentication.

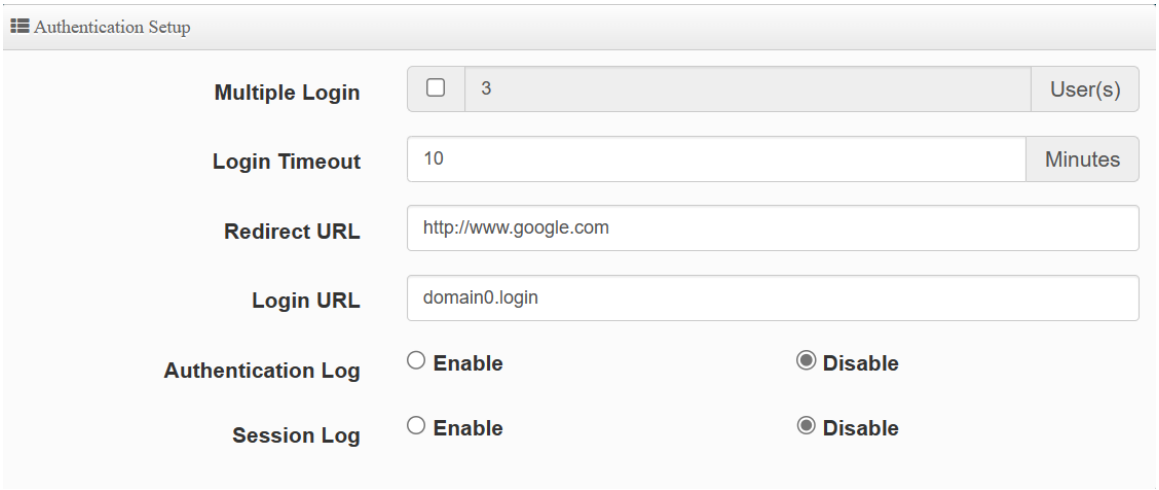
Please click on System -> Authentication



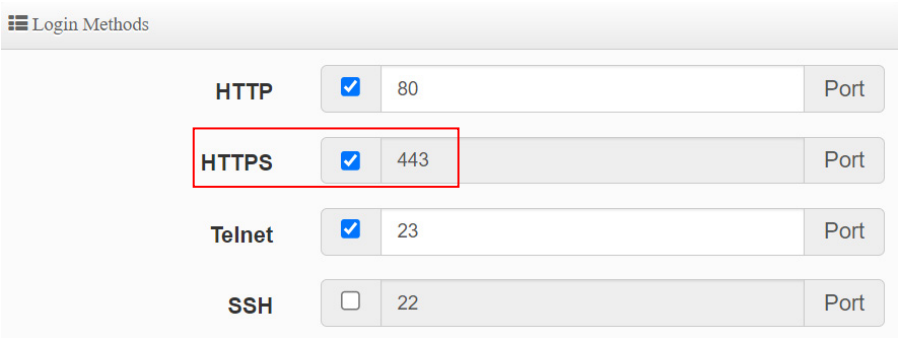
Notice

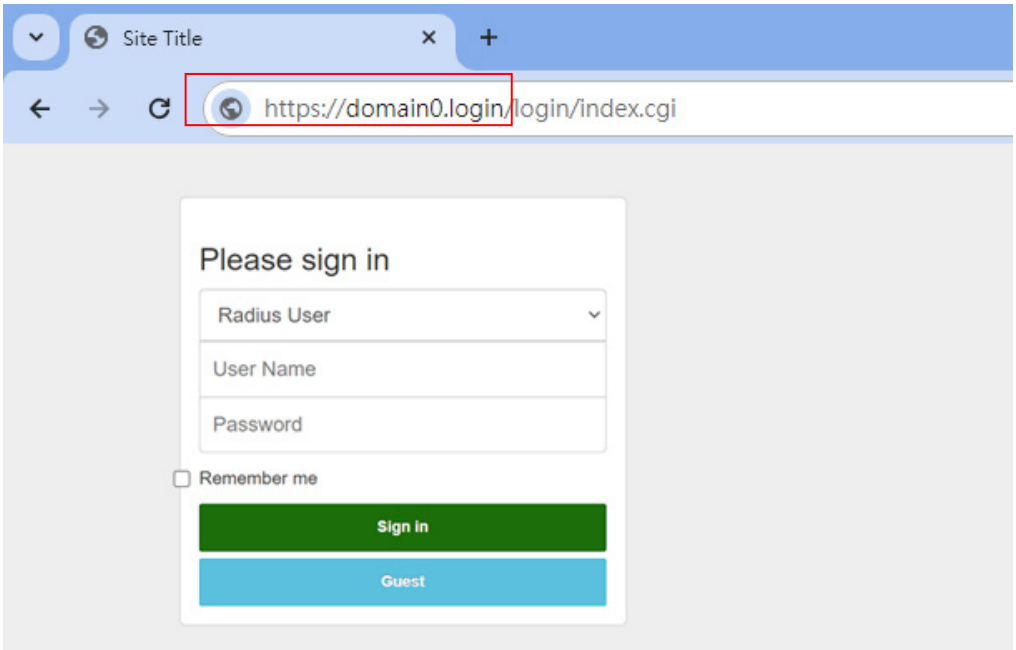
When enable web authentication function, please does make the Access Point can be connected to gateway. Please refer to VLAN Setup. If the gateway IP address is set error address then web login page can't display

- **#**：Display VLANs number.
- **VLAN Mode**：Displays VLAN on/off status. (Please refer to 4.2 VLAN Setup)
- **Authentication**：Displays VLAN# whether enable or disable web authentication.



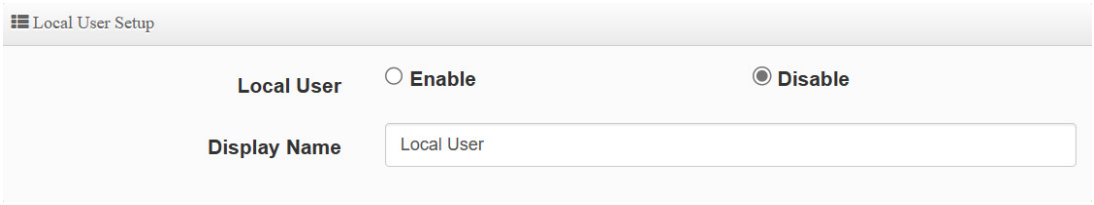
- **Multiple Login**：Administrator can set one account to multiple users simultaneously login and the users can set limit.(0 = not limited)
- **Login Timeout**：After account login for some time no traffic, system will automatic timeout for account. Administrator can enter a time (Minutes).
- **Redirect URL**：After the success of the login, system will redirect to URL. Administrator can enter web site URL.
- **Login URL**：Administrator can set URL for login page. Set the URL that automatically triggers the login page. When you start the web page and want to log in, directly enter the default login page URL **http://domain0.login**, and you can quickly jump to the complete login authentication login page **http://domain0.login/login/index.cgi**. , if you want to use **https://domain0.login**, please be sure to confirm whether HTTPS login is enabled and open for use in the "Management Interface Login Settings". Please refer to 3.1 Management → "Login Methods" Settings, or as shown below.





- **Authentication Log:** Account authentication log will copy to the Cerio Controller device ‘s syslog server. **(For this part of the “AP controller’s log server function, please refer to the detailed description of "Authentication Log" in the relevant " AP controller " series product manual of Cerio Company).**
- **Session Log**：If network have Syslog server. Administrator can to system➔management setting IP address for syslog server and enable the function. Account session log will copy to the Cerio Controller device ‘s syslog server. **(For this part of the “AP controller’s log server function, please refer to the detailed description of "Session Log" in the relevant " AP controller " series product manual of Cerio Company).**

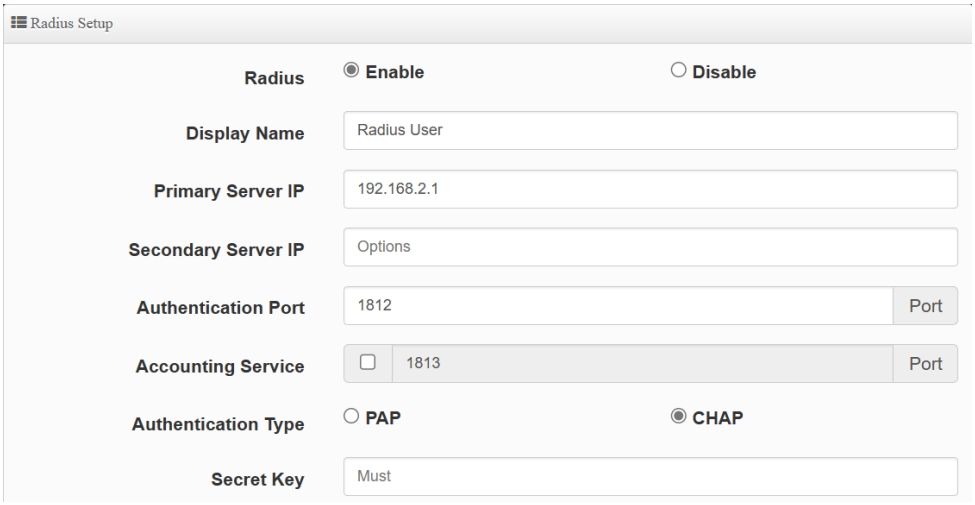
Notice	After enabling it, you must go to System Settings > System Management to set "System Logging Settings" to specify the IP address and port number of the SysLog server in the environment, so that session log messages can be sent to the Server.



- **Local User**：Administrator can enable authentication for local user. Create user account can to reference **" Local User"** setup**.**

Notice	After activating the local account, be sure to go to the "Local Account" function menu to create an authenticated user account..

※ **RADIUS**：Authentication support remote RADIUS Server. Administrator can enter security information for remote RADIUS Server.

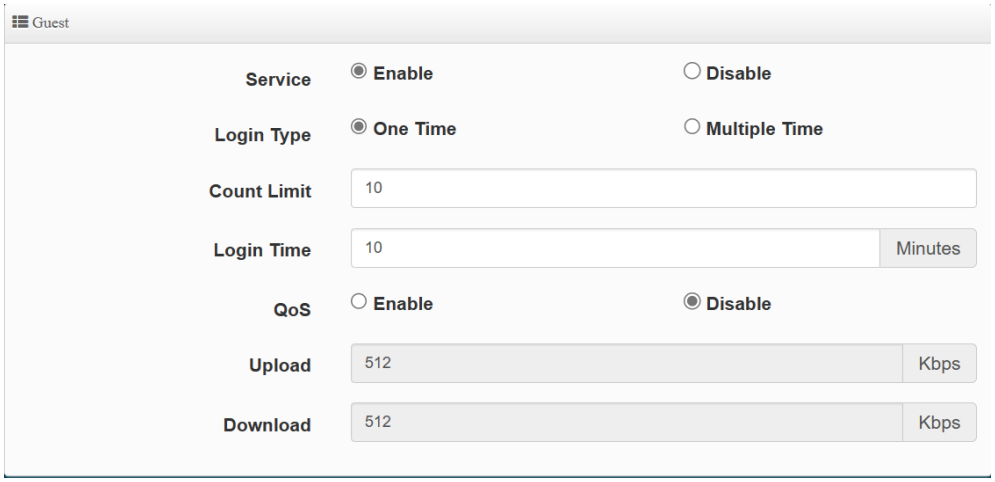


- **Radius**：This authentication service can be set to "enable" or "disable"
- **Disaplay Name**：Dsiaplay the Radius name
- **Primary Server IP**：Set the IP address of the remote RADIUS server.
- **Secondary Server IP**：Set the secondary RADIUS server IP address. (Set according to environmental requirements).
- **Authentication port**：Set the communication port number used by the RADIUS server.
- **Accounting service**：If the remote RADIUS server has the function of enabling accounting services (such as statistics traffic, etc.), you can set the accounting service port of the remote RADIUS server here.
- **Authentication type**：You can choose the authentication type of PAP or CHAP.
- **Secret Key:**：Enter the key to connect to the remote RADIUS server.

Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

4-3-1. Guest

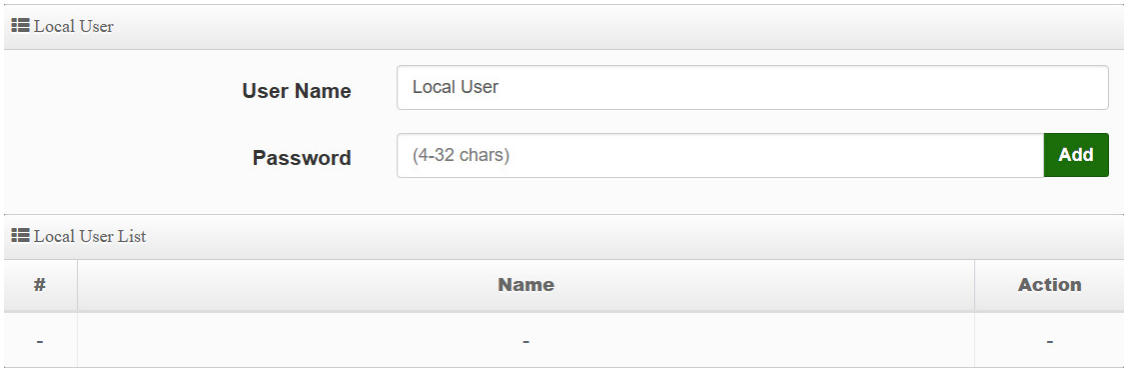
Administrator can enable or disable guest authentication. If enabled, the administrator can set guest Count Limit / login time and type and flow control.



- **Service**：Administrator can select enable or disable this function.
- **Login Type :**
  - ✓ **One Time:** Login to start counting until the end of time.
  - ✓ **Multiple Times:** logout time will stop counting until the next re-login to time start counting.
- **Count Limit:** Administrator can set guest limit.
- **Login Time:** Within a certain timeframe with no traffic, the system will auto logout.
- **QoS:** Administrator can restrict the traffic of guest. Traffic management can set users upload and download traffic.

4-3-2. Local User

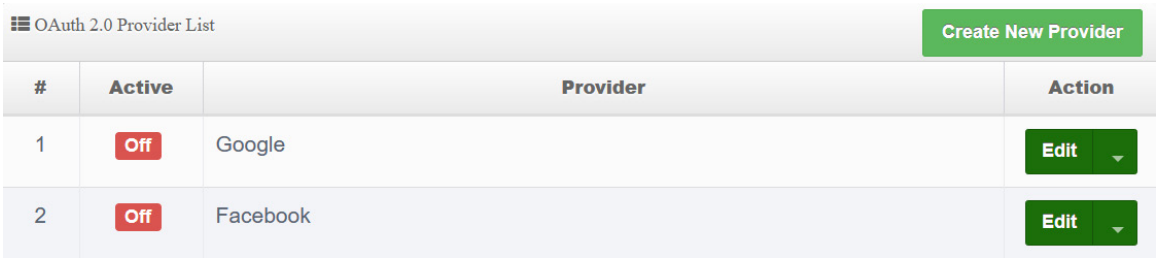
Administrator can create local user account for web login and up to 10 users.



- **User Name**： Administrator can create users account.
- **Password**：Set account password.

4-3-3. OAuth 2.0

- The OAuth2.0 function supports Facebook and Google by default. Users can add additional OAuth2.0 servers through UI settings.

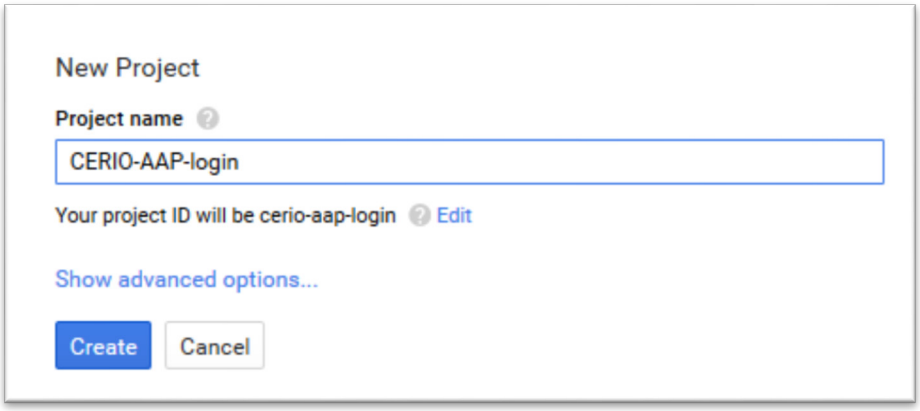


- **#**：Display items.
- **Active**：Display on/off status for the authentication.
- **Provider**：Display authentication server. The system default use authentication server for Google and Facebook.

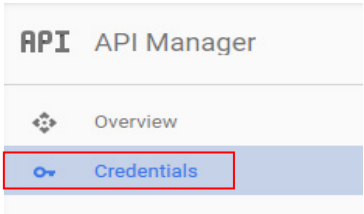
#Sample for Google OAuth2.0 setup

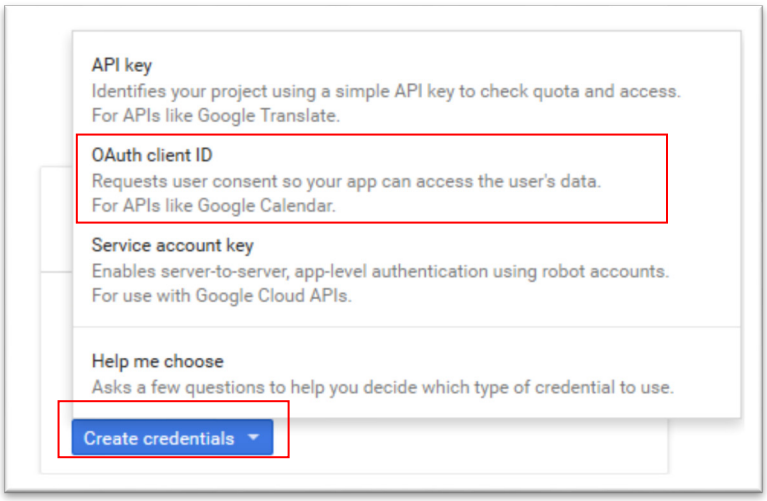
Please complete the application on the Google website to receive an account ID and password, follow the steps below.

Step.1 Please go to the **Google Developers Console page** and **create a project** (Reference https://developers.google.com/identity/protocols/OAuth2)

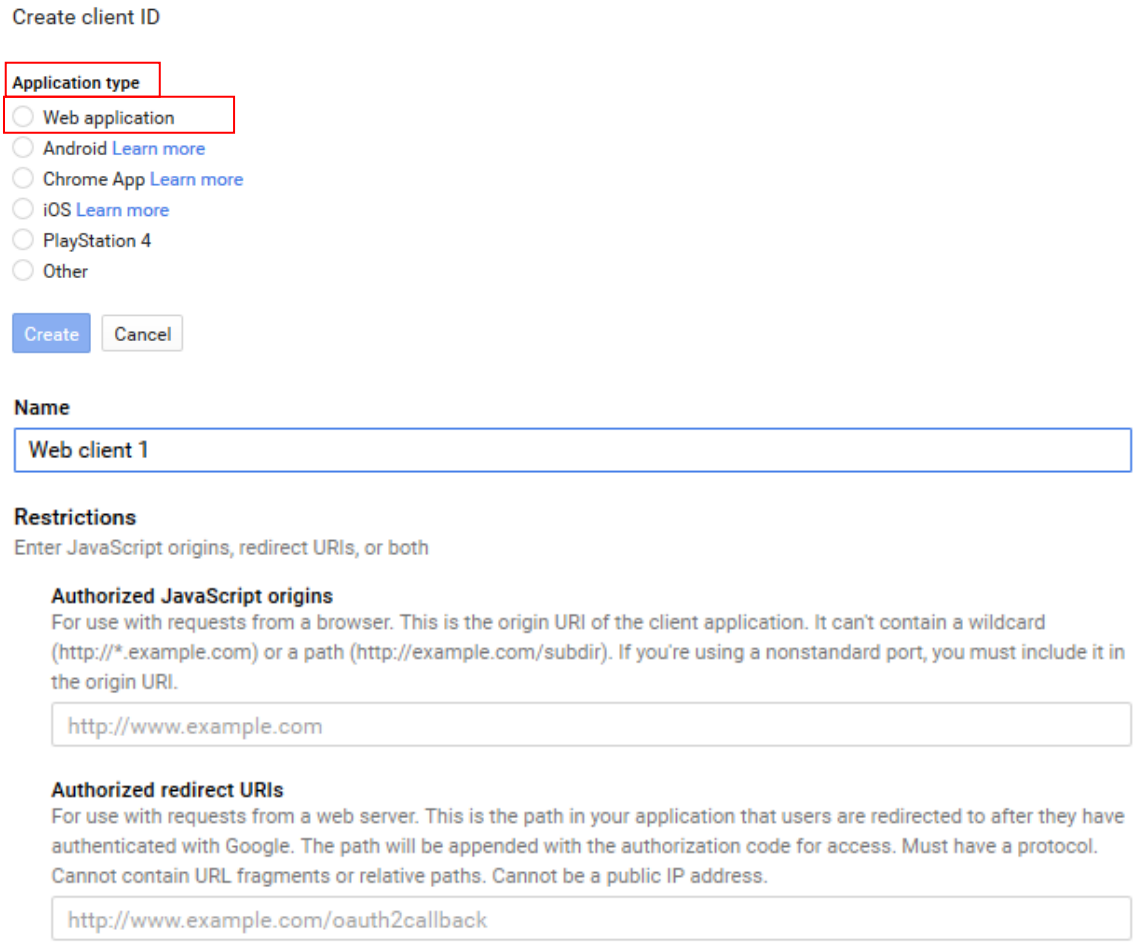


Step.2 Click Credentials to create OAuth client ID in the API manager page.





Step.3 Select web application in the "Application Type" section and set **"Restrictions"** URL.



Step.4 Set Authorized JavaScript origins and Authorized redirect URLs (important)

Administrator must set login URL in the device function. After complete set of login URL go to the

"Restrictions" function in web page. Follow the steps below to set login URLs

- Setup login URL in the device. Please Click **system➔Authentication** and enable the function.
- The "Authentication Setup" page to set Login URL

After complete set of login URL go to the **"Restrictions"** function in web page. Copy and paste the login URL from the system display into the "Restriction" page on the Google Developer website.

- Google Authorized JavaScript origins URL is **http://domain0.login.com** (same as Login URL)
- Google Authorized redirect URLs is **http://domain0.login.com/login/callback.cgi**

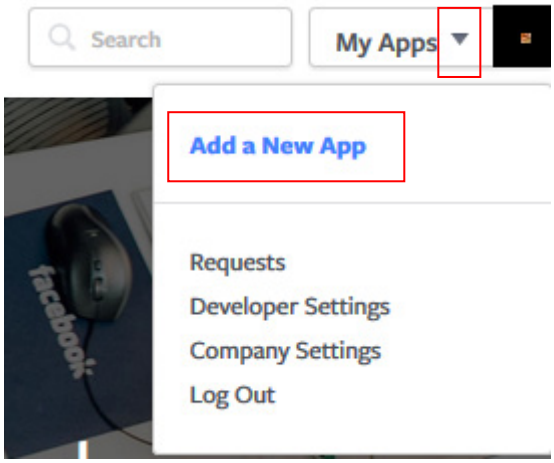
Step.5 After completing the "Restrictions" setup, click the create button. An OAuth Client page will pop-up with your **"client ID"** and "client secret". Administrators must copy and paste their client ID and secret into the OAuth 2.0 Setup page in our software UI.

Save and reboot the AP system, complete the setup.

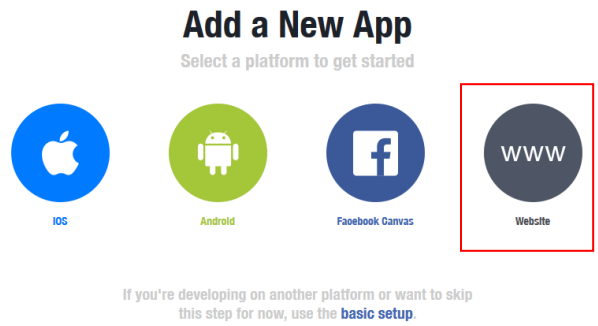
#Sample for Facebook OAuth2.0 setup

Please complete the application on the Facebook website to receive an account ID and password, follow the steps below.

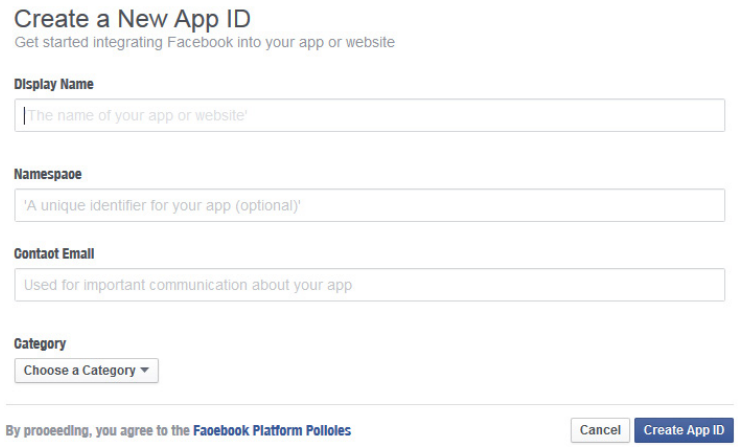
Step.1 Please to Facebook developer's page and add a New App



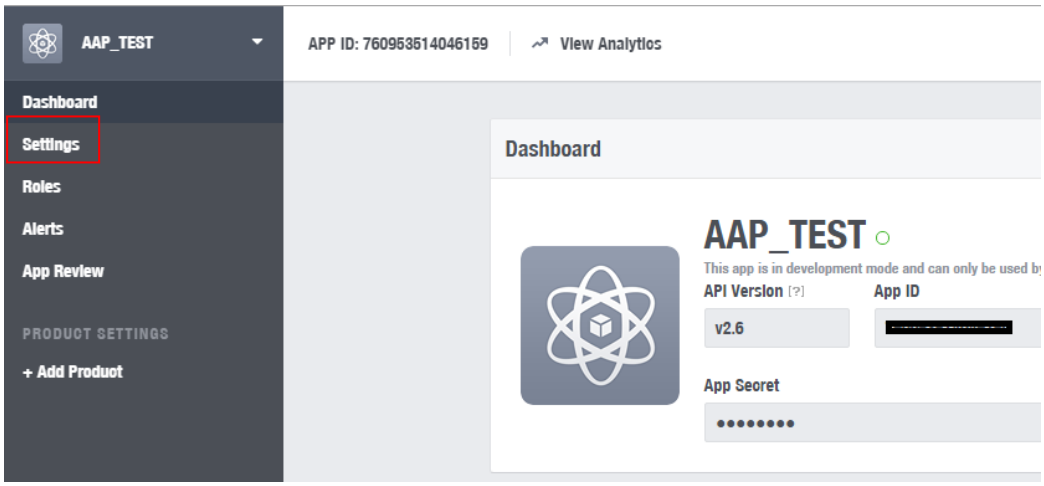
Step.2 Select WWW function



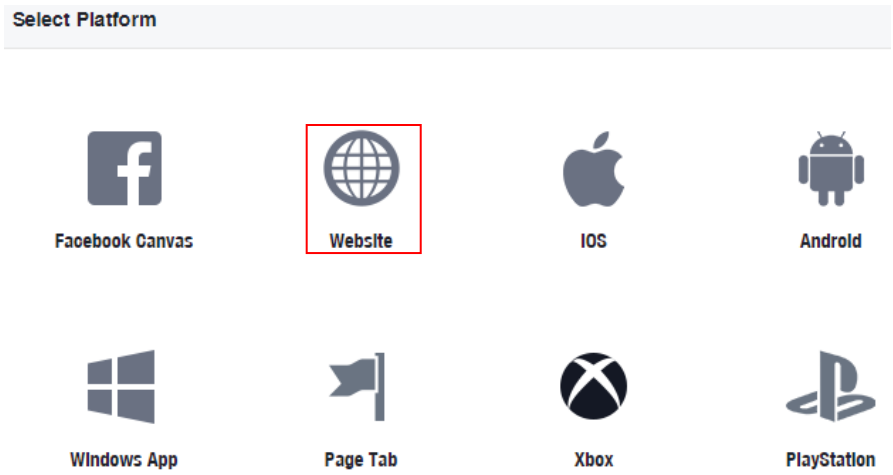
Step.3 Administrator must set www for your information.



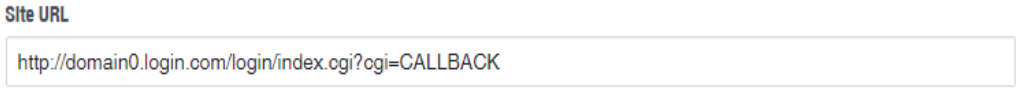
Step.4 Please click **"Setting"** and add Platform



Step.5 Select Platform for "**Website**"

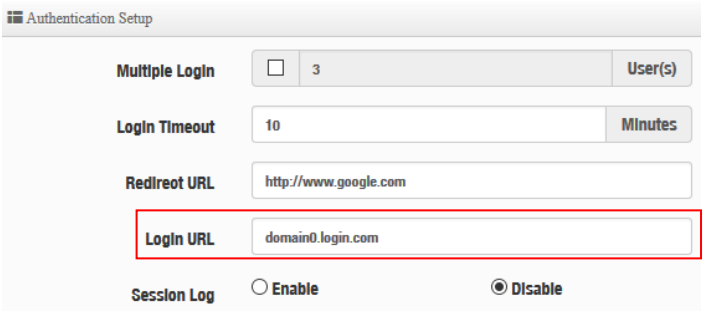


Step.6 Enter URL is **http://domain0.login.com/login/callback.cgi**



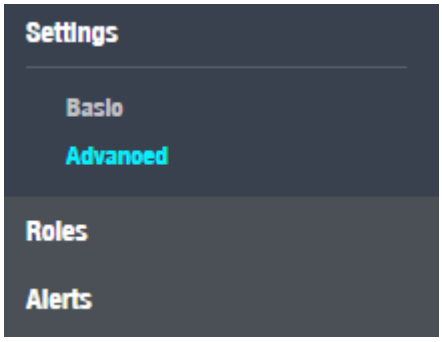
Administrator must set login URL in the device function. After complete set of login URL go to the "**Facebook** Site URL" function in web page. Follow the steps below to set login URLs

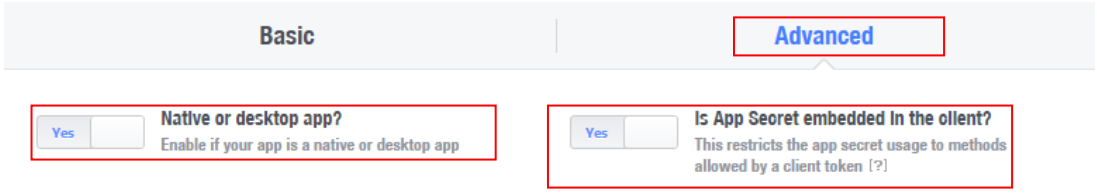
- Setup login URL in the device. Please Click **system➔Authentication** and enable the function.
- The **"Authentication Setup"** page to set Login URL



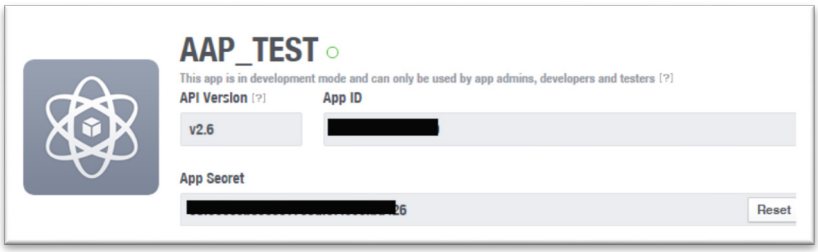
After complete set of login URL go to the "**Facebook** Site URL" function in web page. Copy and paste the login URL from the system display into the "Site URL" page on the Facebook website.

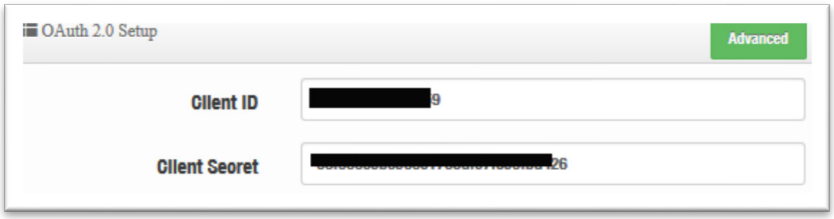
Step.7 Click Advanced function to enable the **"Native or desktop app?"** and **"Is App Secret embedded in the client? "**





Step.8 After completing the "**Facebook** Site URL" setup. Administrators must copy and paste their App ID and App secret into the OAuth 2.0 Setup page in our software UI.



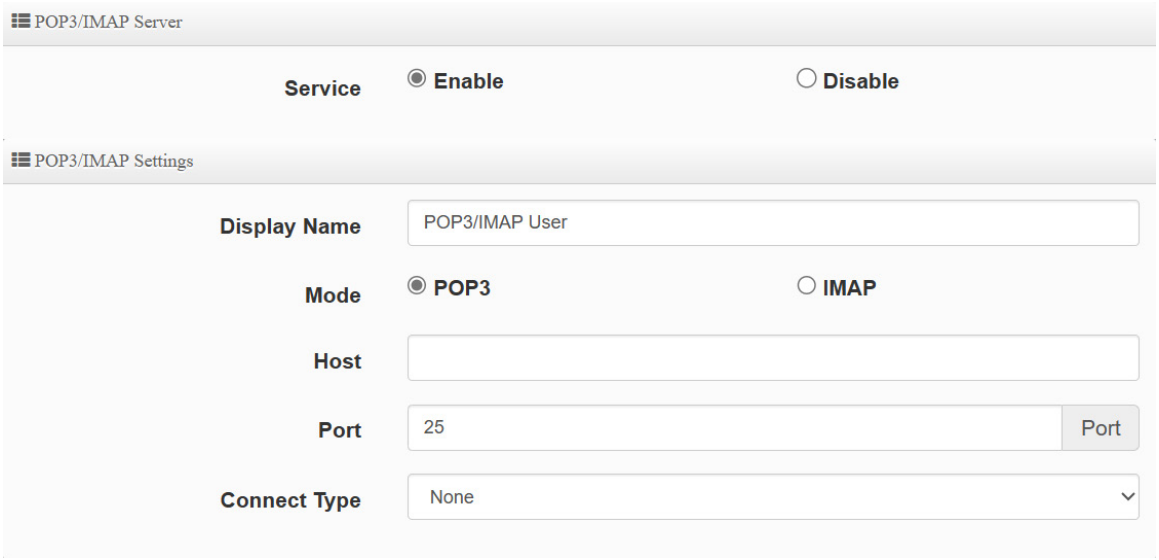


Notice

Client ID and Client Secret setup by third parties such as Facebook and Google are subject to change. The instructions above follow the 2016 setup procedure. Any future changes to the Facebook/Google process may lead to our instructions becoming invalid.

4-3-4. POP3/IMAP Server

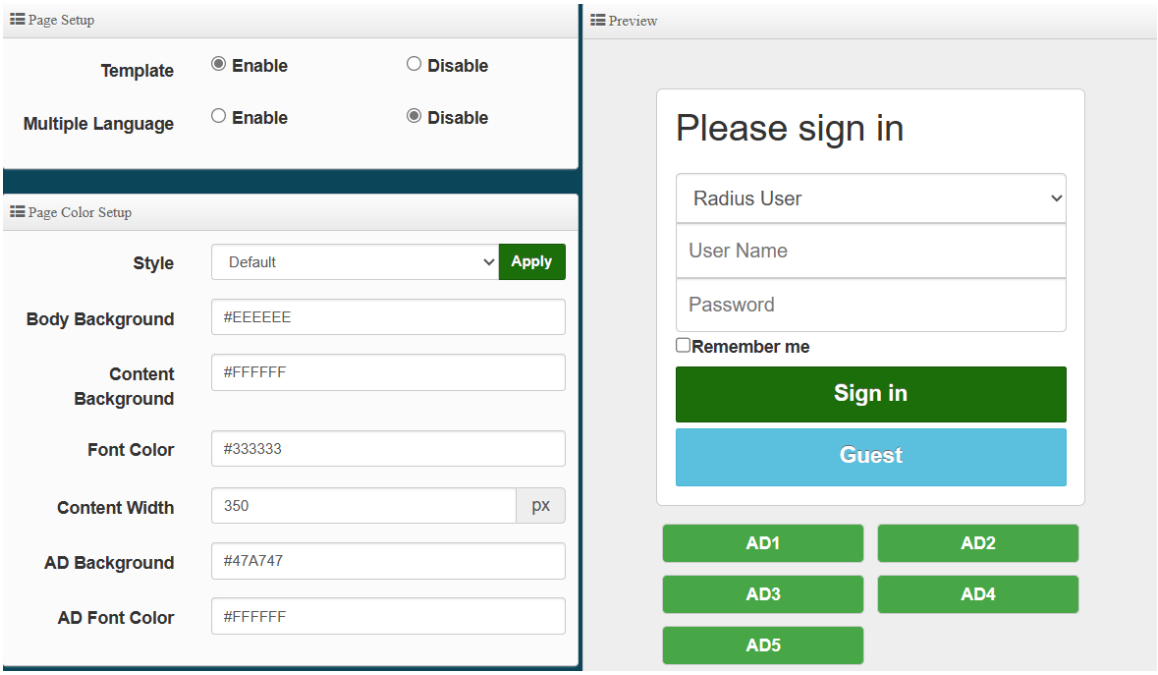
The purpose of this integrated function is to allow clients to link a POP3 server for receiving emails from a remote server.



- **Service:** Administrator can choose Enable or Disable the PoP3 authentication.
- **Display Name**：Set the “Display Name” based on the appropriate POP3 user or client.
- **Host :** Define the desired Host server name.
- **Port :** Input the proper port number for the corresponding server.
- **Connect Type :** Select the Connect type with options of “STARTTLS”, “SSL/TTL”, or “None”.
- **POP3 Server Test :** Use this tool to test if the POP3 server is operating correctly with your selected email

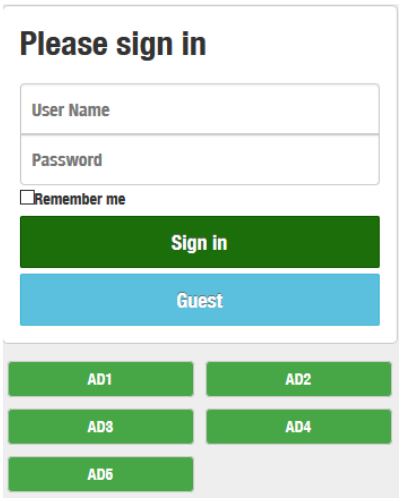
4-3-5. Customize

This function is to customize the user Login Page. This supports Multiple Language and allows comprehensive customization through HTML editing.

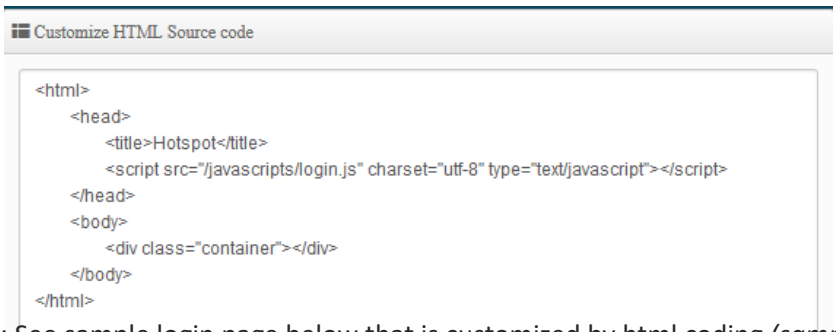


Page Setup

- **Template**：Administrator can select Enable or disable.
  - Select enable to active default Login Page



- Select disable to active HTML Source code window for customization



Sample: See sample login page below that is customized by html coding *(sample login page html code templates are available on Cerio website)*

The following function uses the enabled Template

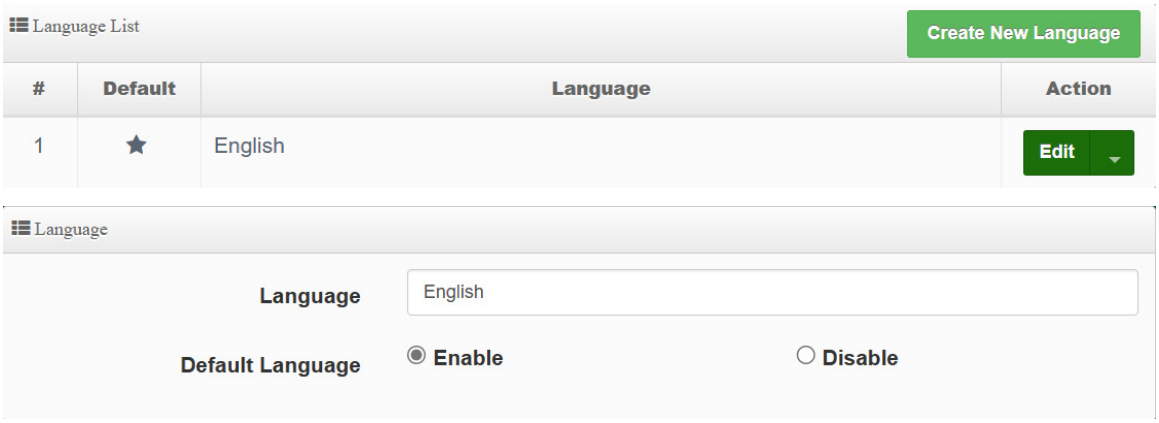
- **Multiple Language**：Administrator can select enable or disable multiple language for login page.

Administrator must to Language function create new language.

Page Color Setup：Administrator can change the login page color

4-3-6. Language

Administrator can create other language for login page.



Click “Create New Language” button go to add or edit language for login page.

- Language: Set description of language.
- Default Language: Display default language.

4-3-7. 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.

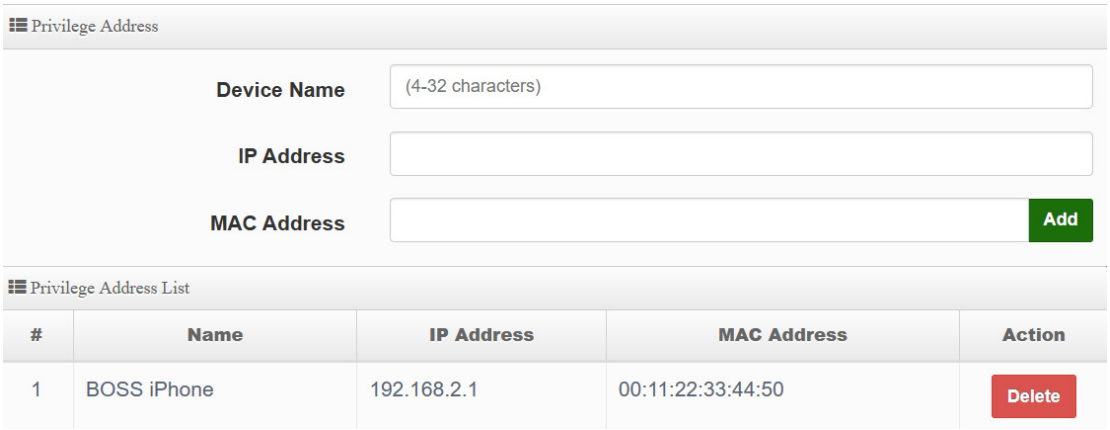
- **Display Name:** Set name of Website.
- **IP Address/Domain:** Set IP or Domain of the Open the website.

- **Full URL:** Set full website name.

Click **"Save"** button to save your changes. Then click Reboot button to activate your changes..

4-3-8. 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.



- **Device Name:** Enter Device or Users Name.
- **IP Address:** Enter used IP Address of Device or Users PC.
- **MAC Address:** Enter MAC Address of Device or Users PC.

Click **"Save"** button to save your changes. Then click Reboot button to activate your changes..

4-3-9. Bulk MAC Address

This function is similar to the privileged list, the difference is that this function only verifies the MAC address, and the MAC list can only be built in batches by uploading

When this function is turned on, as long as the devices on the MAC list will not need to do web page verification and can directly use Internet services.

- **Rules: Administrators can enable or disable this function.**
- **Upload MAC Address:** Select the location of MAC data file and upload to import into this function for system judgment.

Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

4-3-10. Profile

Administrator can backup current authentication configuration and login page for HTML Source code. But also can recover.

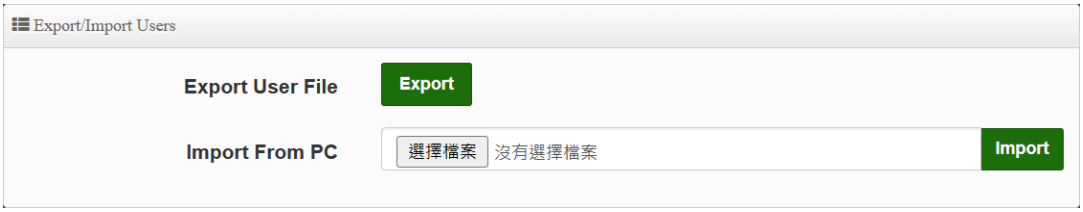
Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

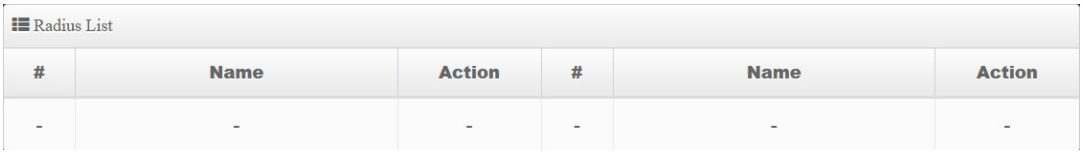
4-4. RADIUS Server

- **Service**：Administrator can select Enable or disable the function.
- **Radius**：Administrator must to set remote RADIUS Server use Port.。
- **Radius Secret**：Administrator must to set remote RADIUS Server use Key.

Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

4-5. RADIUS Account Setup

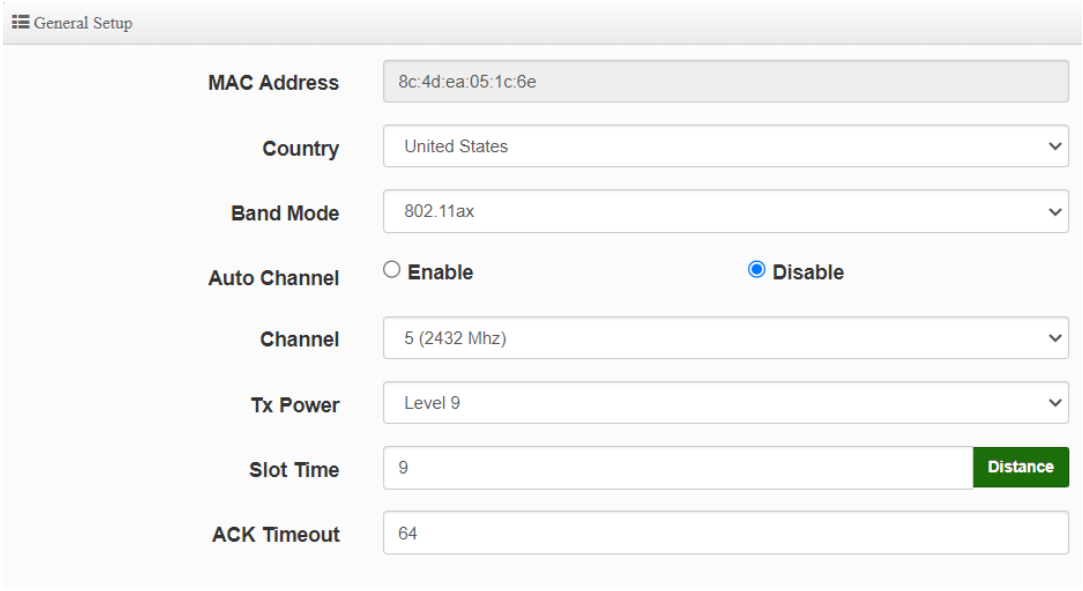




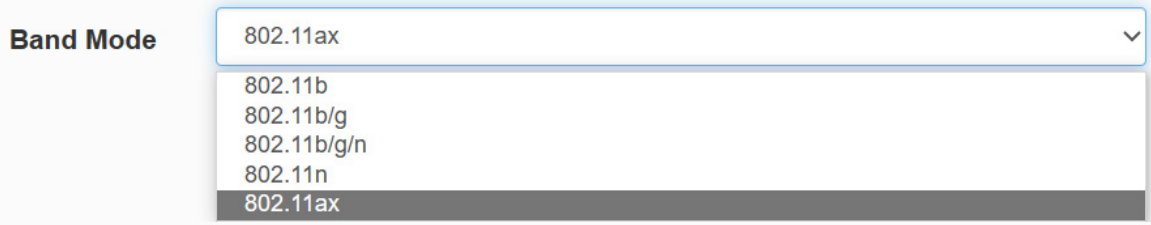
- **User Name**：Create users name for RADIUS account.
- **Password**：Enter password for user name.
- **Export User File**：Administrator can export account list in RADIUS Server.
- **Import From PC**：Administrator can import account list to the RADIUS Server.

4-6. Wireless Configuration

4-6-1. Radio 0 (2.4G) Basic Setup



- **General Setup**
  - **MAC Address**：Display 2.4G WiFi MAC address.
  - **Country**：Administrator can select country: US or EU or Japan or Taiwan.
  - **Band Mode**：Administrator can select 2.4G Band for 802.11b、802.11b/g、802.11b/g/n、802.11n. or 802.11ax, The default is 802.11ax

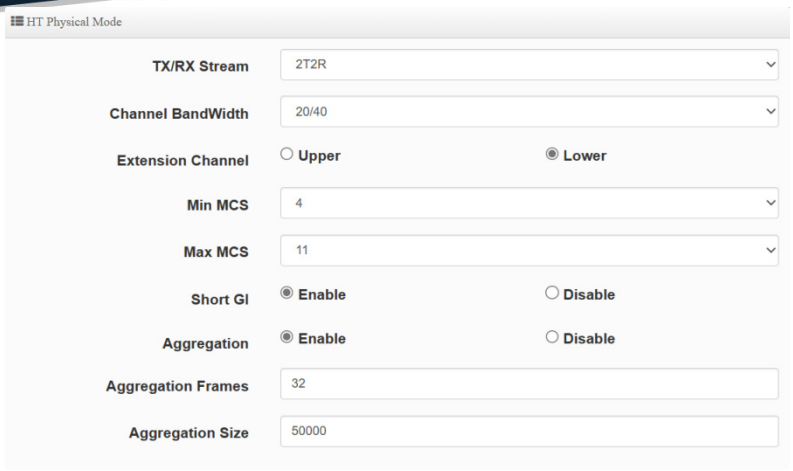


- **Auto Channel**：Administrator can Enable or Disable the function. If disabled, the WiFi channel will be fixed to the manually selected channel.
- **Channel**：There are different options for wireless operation modes in regions, which can be used for Upper or Lower extension.
- **Tx Power**：Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow

  Distance : When the Distance button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
- **ACK timeout**：When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice	Setting ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

- **HP Physical Mode**



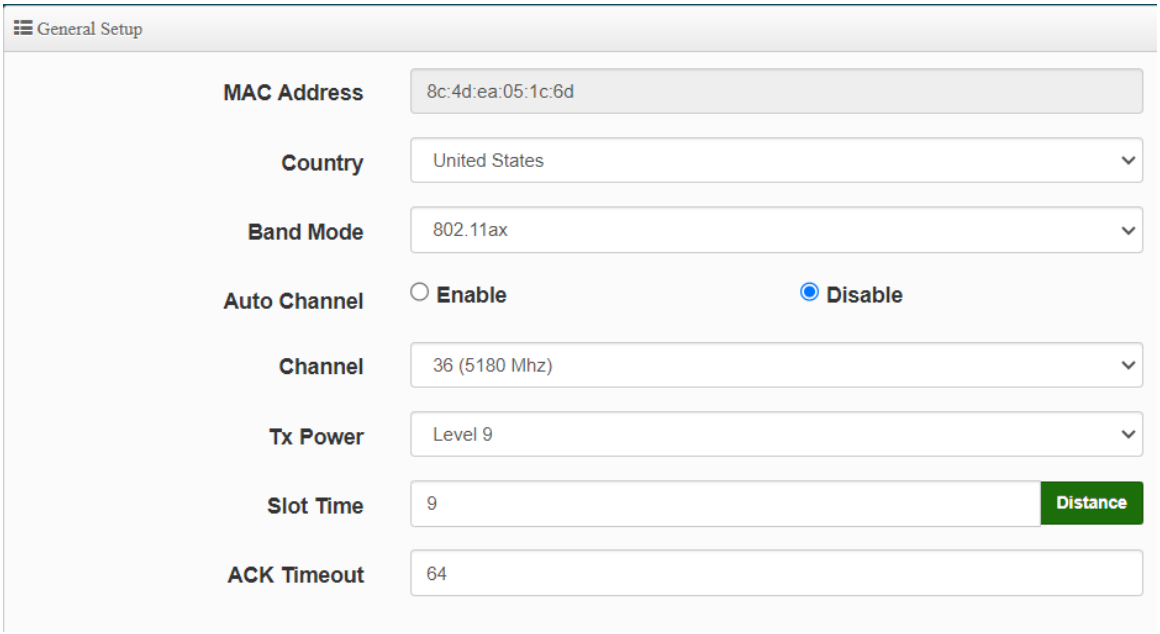
- **TX/RX Stream**：The CenOS 5.0 AP support 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

Notice

The 2.4Ghz antenna of this product thinks that it has a built-in 2x2. The default is already set to 2T2R. If there is no special requirement, please keep the setting.

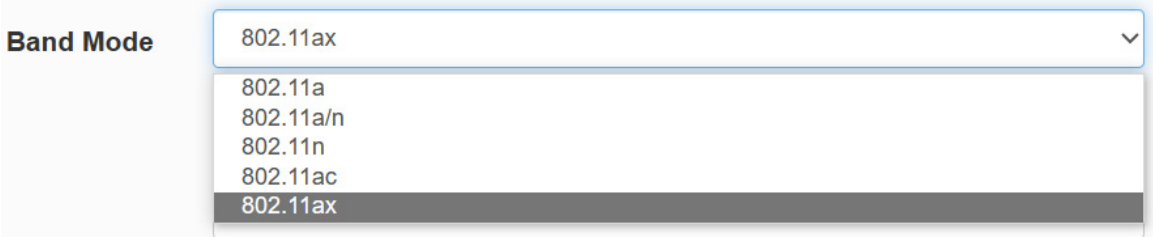
- **Channel Bandwidth**：The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel**：Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.
- **MIN MCS:** MCS compilation is a representation proposed by 802.11ax on the communication rate of WLAN.The MCS coding value will affect the main factor of the communication rate and corresponds to the channel bandwidth.
- **MAX MCS:** Maximum MCS compile set value. The Max MCS value must be greater than the Min MCS value.
- **Short GI**：Short Guard Interval is "Enabled" by default to increase throughput. 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 "**Enabled**". Select "Disable" to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard), 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:** Set frames size of Aggregation.
- **Aggregation Size:** Set aggregation size.

4-6-2. Radio 1 (5G-1) / Radio 2 (5G-2)Basic Setup



- **General Setup**

  - **MAC Address:** Display 5G-1(Radio 1) / 5G-2(Radio 2) WiFi MAC address.
  - **Country:** Administrator can select country: US or EU or Japan or Taiwan.
  - **Band Mode:** Administrator can select 5G Band for 802.11a、802.11a/n、802.11n、802.11ac. or 802.11ax, The default is 802.11ax



  - **Auto Channel:** Administrator can Enable or Disable the function. If select disabled function the WiFi channel can be manually fixed.
  - **Channel**：There are different options for wireless operation modes in regions.
  - **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
  - **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow

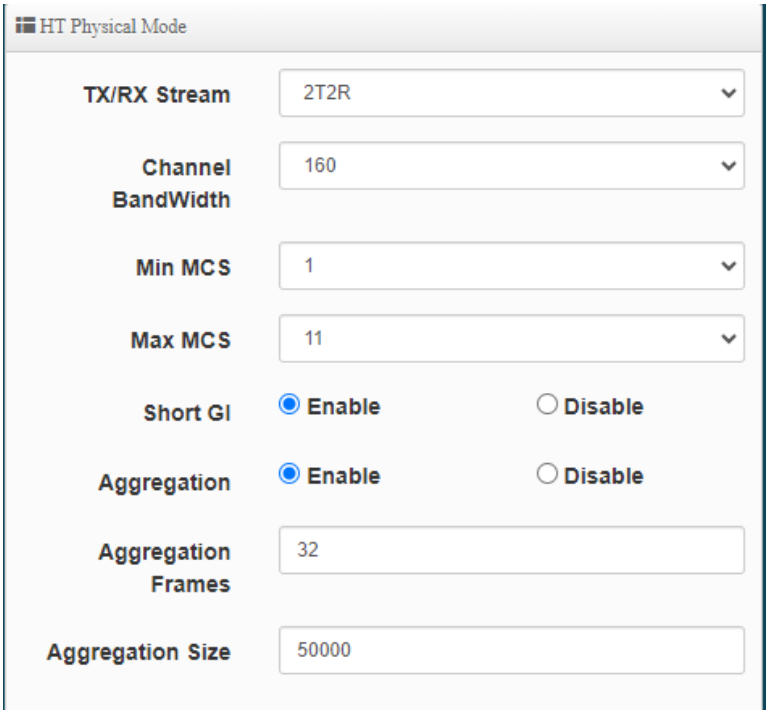
    Distance : When the Distance button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
  - **ACK timeout**：When waiting for the "ACKnowledgment frame" interval is too long to be received,

the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice

Setting ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

- **HP Physical Mode**



- **TX/RX Stream:** Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

Notice

The 5Ghz antenna of this product thinks that it has a built-in 2x2. The default is already set to 2T2R. If there is no special requirement, please keep the setting.

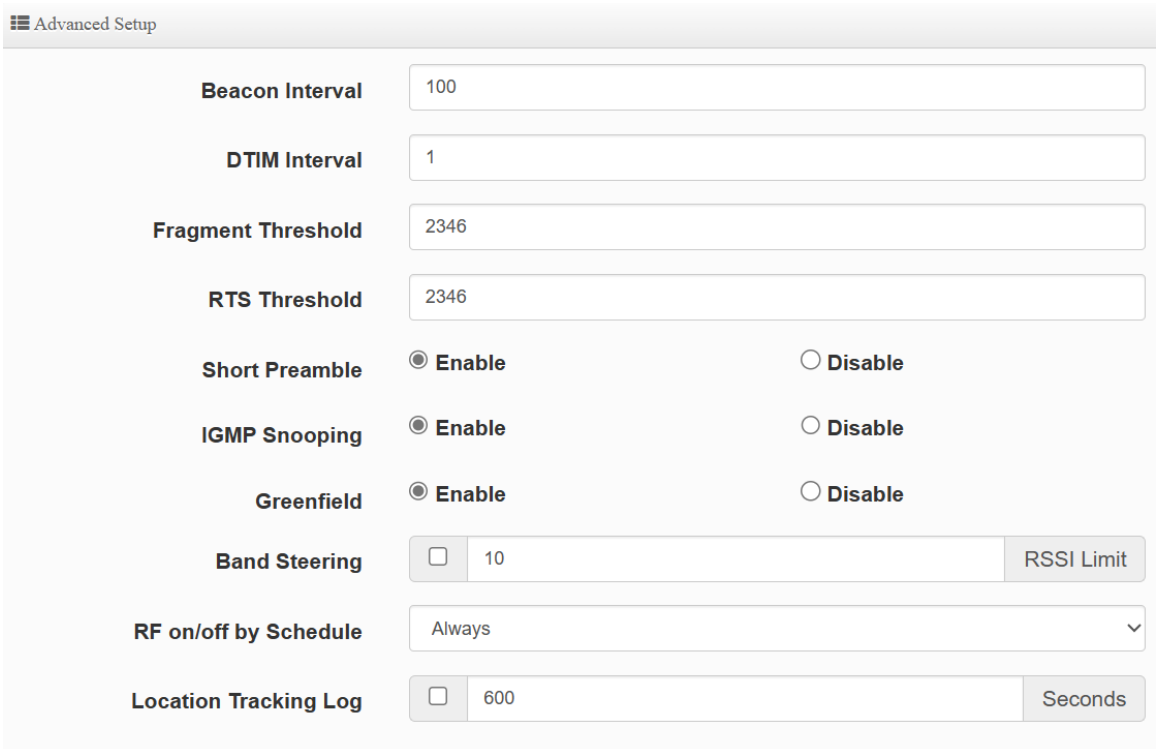
- **Channel BandWith:** The Wireless 5G can choose 20 or 20/40 Mhz or 11ac/ax 80Mhz at 5G-1 (Radio-1) or 11ax 160Mhz at 5G-2 (Radio) as the data transmission speed between the base station and wireless users.
- **MIN MCS:** MCS compilation is a representation proposed by 802.11ax on the communication rate of WLAN.The MCS coding value will affect the main factor of the communication rate and

corresponds to the channel bandwidth.

- **MAX MCS:** Maximum MCS compile set value. The Max MCS value must be greater than the Min MCS value.
- **Shout GI:** Short Guard Interval is “Enabled” by default to increase throughput. 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 “**Enabled**”. Select “Disable” to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard), 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:** Set frames size of Aggregation, the size recommend use default value is 32.
- **Aggregation Size:** Set aggregation size, the size recommends use default value is 500000.

Click **“Save”** button to save your set function. Then click “Reboot” button to activate your changes.

4-6-3. Advanced Setup



- **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 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.

- **Fragmentation Threshold:** Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same, it fragments the data packets.

  Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. Let's say from Ethernet we have to send 1400 byte packet but the fragmentation threshold is set as 400. In this case when the packet is to be transmitted on air it will fragment the packet in to 4 small packet 400+400+400+200 and send on air. This includes MAC header+ frame body and CRC so 400 byte will be in total including headers. This helps in increasing the throughput. The default is 2346.

- **RTS Threshold:** TRTS 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, this function is "***Enabled***". ***Disabling*** will automatically use the 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.
- **Band Steering(5G Priority)**：When 2.4GHz and 5GHz networks exist at the same time, the 5GHz client connection is automatically connected to the 5GHz network as the main connection to improve performance.
- **RF on/off by schedule:** Administrator can apply Time Policy to on or off wireless signal.
- **Location Tracking Log: T**he system can detect the signal strength of the wireless client to determine the location of the Access Point and send to database.

4-6-4. WMM Setup

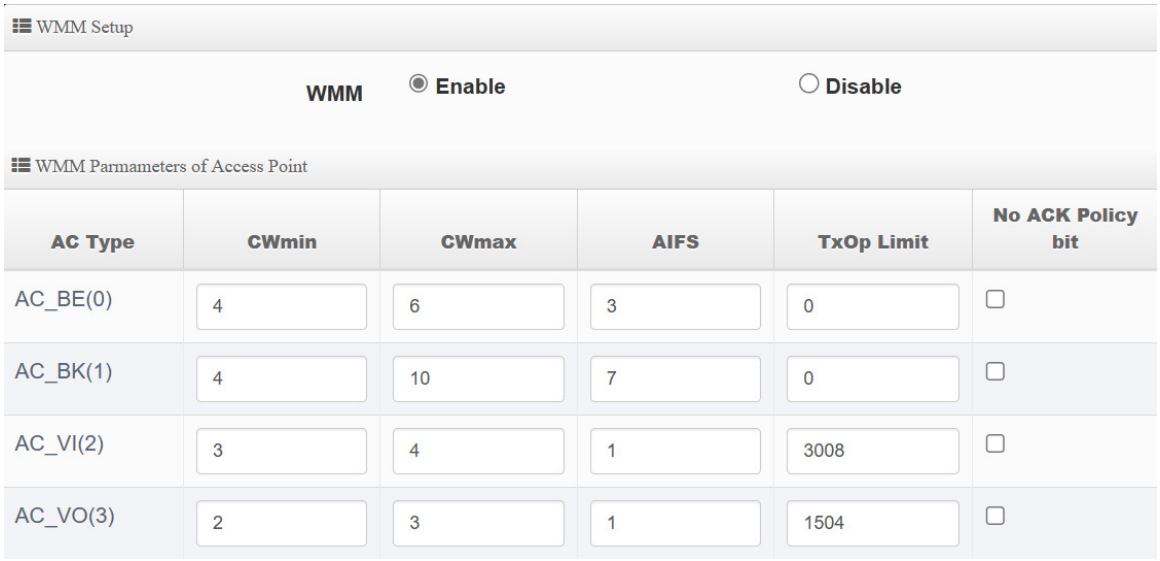
This affects traffic flowing from the access point to the client station.

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.

Please click on **Wireless -> WMM Setup**



- **AC Type**：

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

- **CWmin**: Minimum Contention Window. This parameter is input to the algorithm that 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**"

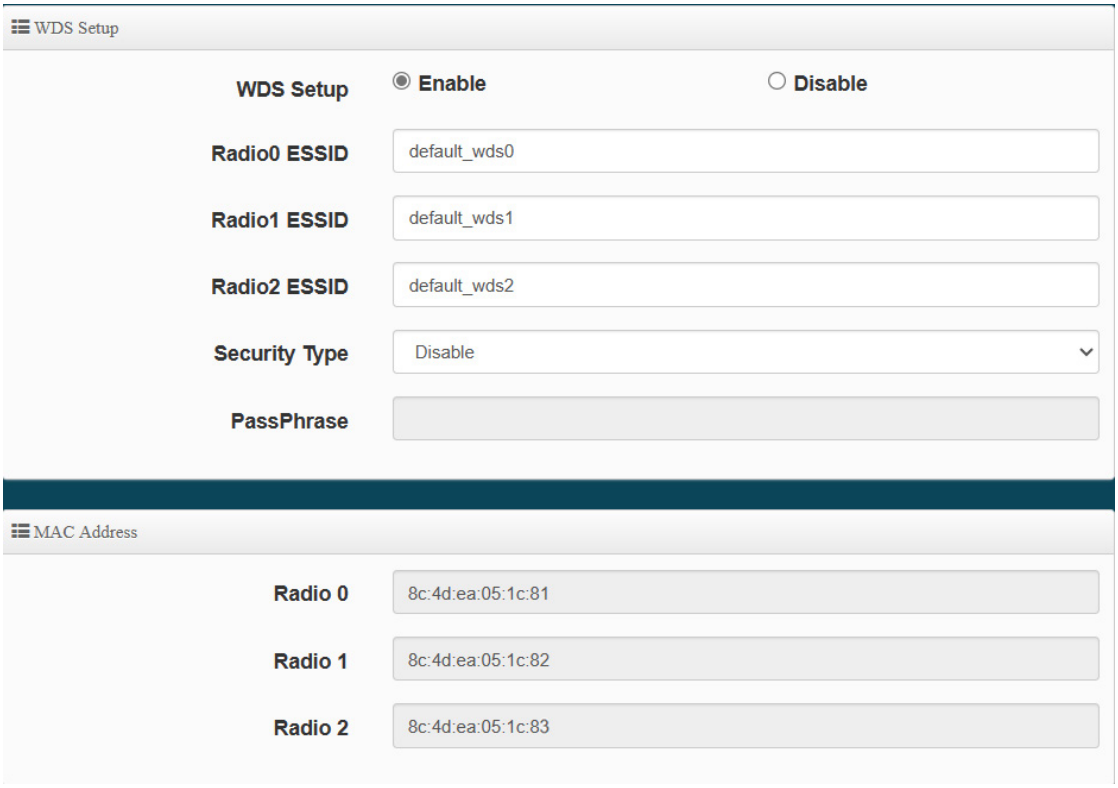
  When the no acknowledgement (No ACK) policy is used, the recipient does not acknowledge received packets during wireless packet exchange. This policy is suitable in the environment where communication quality is fine and interference is weak.
  While the No ACK policy helps improve transmission efficiency, 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.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

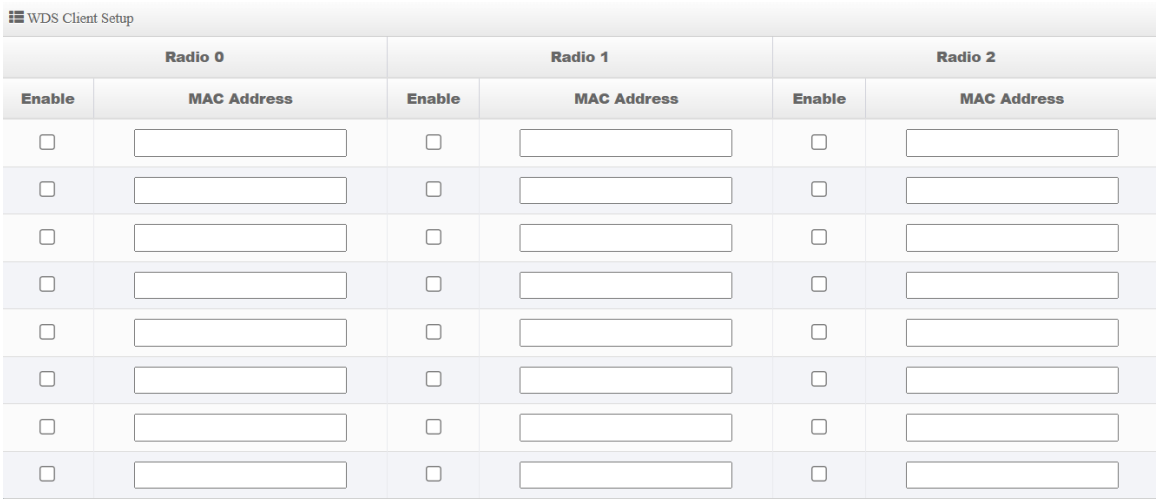
4-6-5. WDS Setup

When using the AP+WDS function, the wireless base stations at both ends must support the WDS function at the same time, and the wireless base stations at both ends must set the MAC address of the other party's wireless interface. In other words, each base station must contain the required MAC address of each base station to which WDS is connected. At the same time, you must confirm that each WDS base station must use the same wireless network name, channel and wireless encryption method. You can choose to enable or disable it.

Please click on Wireless -> WDS Setup



When the WDS function is enabled, it can be set to use Radio 0 (2.4G) for WDS or Radio 1 (5G-1) for WDS or Radio 2 (5G-2) for WDS, etc., and a maximum of 24 groups can be set up to bridge to 2.4G + 5G+ 5G. In WDS The function supports VLAN tag transmission. If there is a tag set in the network domain, WDS can bring multiple groups of tags to another bridge endpoint.



VLAN Setup

VLAN#	Radio 0			Radio 1			Radio 2		
	Native	TAG	TAG ID	Native	TAG	TAG ID	Native	TAG	TAG ID
VLAN 0	◉	☐		◉	☐		◉	☐	
VLAN 1	○	☐	101	○	☐	101	○	☐	101
VLAN 2	○	☐	102	○	☐	102	○	☐	102
VLAN 3	○	☐	103	○	☐	103	○	☐	103
VLAN 4	○	☐	104	○	☐	104	○	☐	104

- **WDS Setup:** Administrator can select Enable or Disable.
- **Radio ESSID:** For connected Radio, please enter the same SSID name for each radio.
- **Security Type:** Enable or Disable AES encryption function.
- **PassPhrase:** AES encryption custom key can input 0 ~ 9 numbers or A ~ Z uppercase and lowercase English format, it can support 8 ~ 32 characters key encryption algorithm in each WDS connecting each other with secure encrypted transmission.

Notice

WDS considerations
1. When two wireless APs want to use WDS connection, the channels of the two must be the same.
2. If the two base AP stations are A and B, the WDS Client Setup of station A needs to set the wireless MAC address of station B, and the WDS Client Setup of station B needs to set the wireless MAC address of station A.
3. If tags must be used in the architecture, the APs on both sides can select multiple sets of tags in the virtual network settings.
4. WDS encryption setting is by optional use.

- **MAC Address :** Enter the MAC address of the other party's host to agree to accept the connection.
- **WDS Client Setup:** Administrator can used Radio 0(2.4G) or Radio 1(5G-1) or Radio 2(5G-2)for WDS Links. A Single Radio supports up to 8 WDS links
- **VLAN Setup:** The WDS aisle support Multi-tag VALN

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

4-6-6. WDS Status

Displays 2.4G (Radio 0) and 5G-1(Radio-1)and 5G-2(Radio-2) radios WDS link status through MAC and Date (TX/RX)

Please click on **Wireless -> WDS status**

Radio0 Client

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

Radio1 Client

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

Radio2 Client

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

- **MAC Address**：Display connected MAC Address.
- **Rate(TX/RX)**：Display Tx/Rx rate of the point to point.
- **RSSI:** Display signal connection value of RSSI.

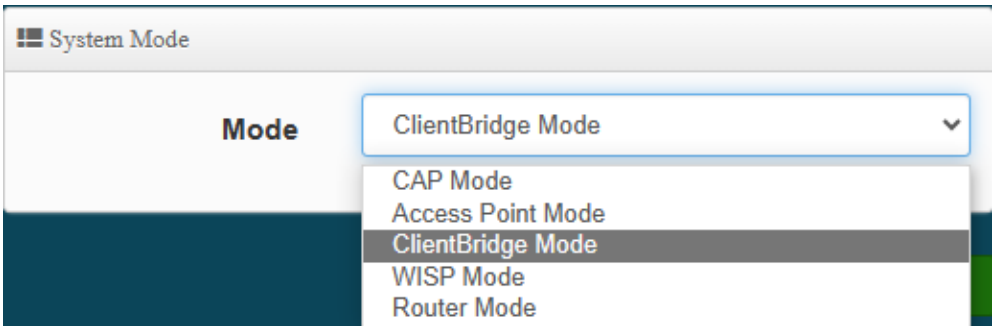
Notice

The RSSI signal quality display of this product is expressed through the signal strength measurement method. Therefore, for RSSI, the larger the "positive value", the better the connection quality.

5. Client Bridge Mode

If the administrator needs to switch to Client Bridge mode, Please click "System"-> " Mode Setup " to change Client Bridge mode.

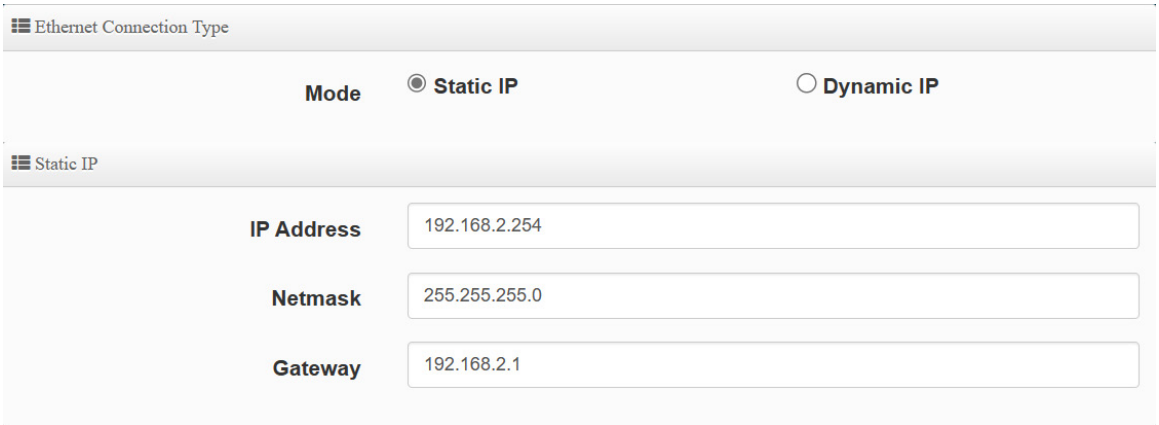
5-1. Change Setup Mode



This section provides detailed explanation for users to configure in the Client Bridge Mode and Repeater AP function with help of illustrations.

5-2. Configure LAN Setup

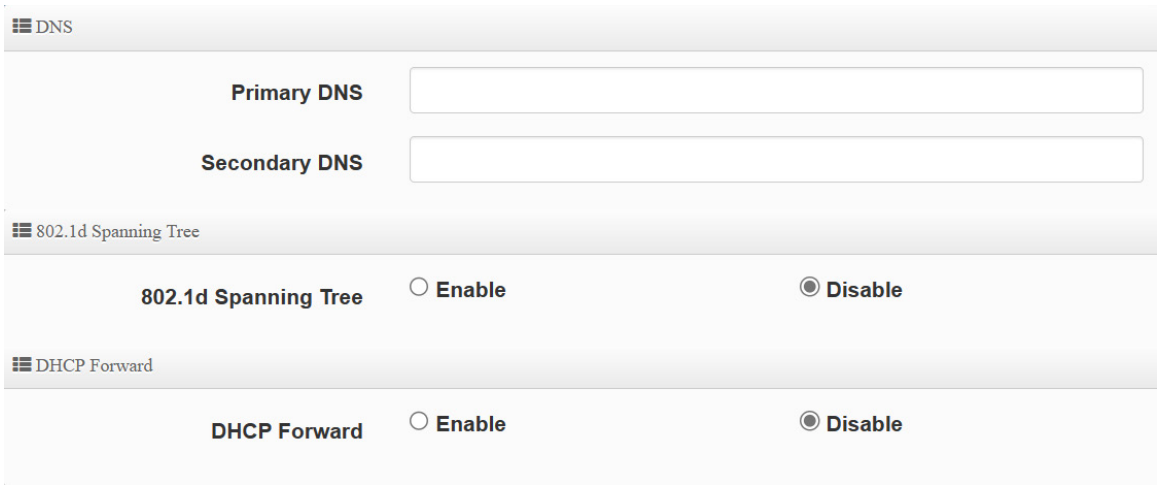
Here are the instructions for how to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting.



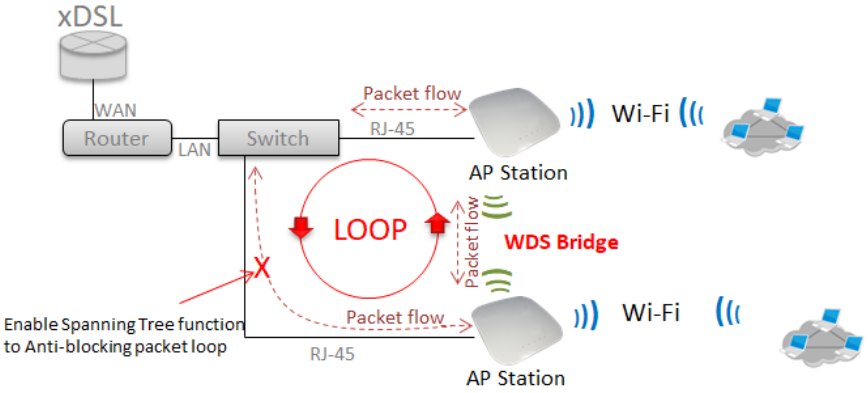
- **Mode:** Administrator can select the IP used Static or Dynamic IP address.
  - Static IP : A set of fixed IP addresses can be manually set for the system to use.
  - Dynamic IP : If there is a DHCP server on the top, you can use the dynamic IP address to let the system obtain a set of IP automatically.

Notice	*That when using a dynamic IP, the system will automatically obtain the IP address sent by DHCP, and the obtained IP address will be obtained after the operation is confirmed by the upper DHCP server. Obtaining the IP address is not fixed. For system management, the upper DHCP server must query the IP address obtained by the current system.*

- **Static IP:**
  - **IP address:** The IP address is 192.168.2.254
  - **Netmask:** The default Netmask is 255.255.255.0
  - **Gateway:** The default Gateway IP Address is 192.168.2.1, Please check your Gateway IP and change.



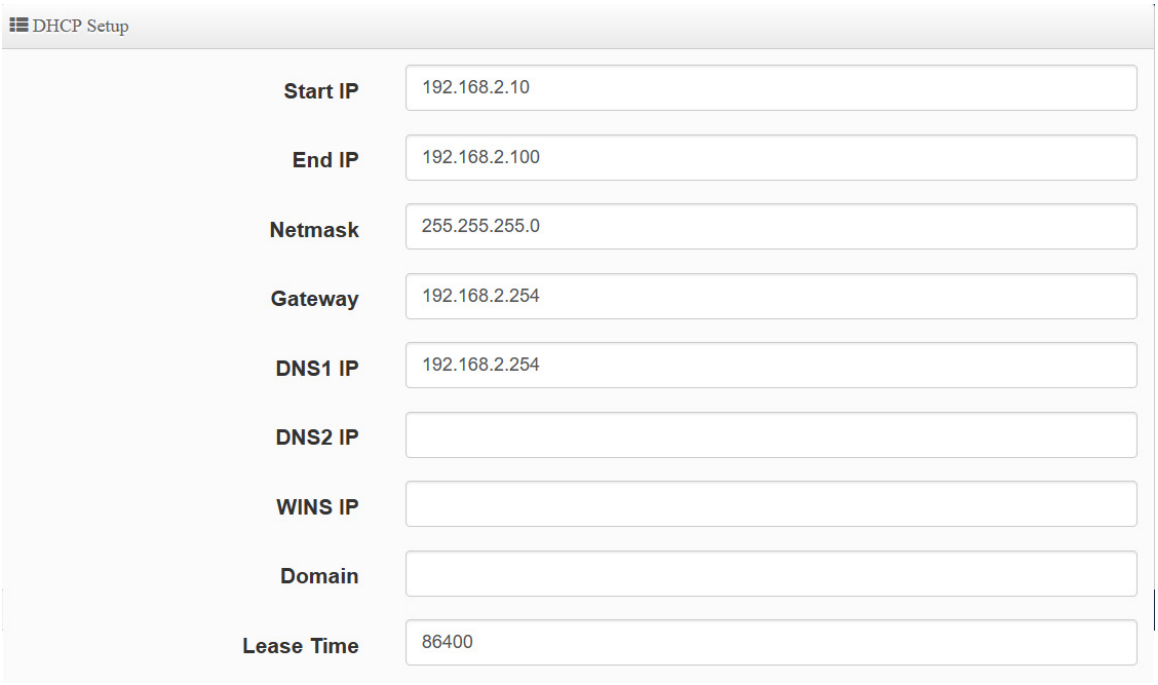
- **DNS**: Enter IP address of domain name service.
  - **Primary DNS**: The IP address of the primary DNS server.
  - **Secondary**: The IP address of the secondary DNS server.
- **802.1d Spanning Tree :** The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.
- **DHCP Forward:** When the AP Mode device and Client Bridge AP are linked, and DHCP Service is "Enabled", the Client Bridge AP must also enable DHCP Forward to allow connecting clients to receive the IP Address from the source AP (AP Mode Device). By default, DHCP Forward is disabled in Client Bridge devices. This function must be enabled to allow clients connecting to the Client Bridge device to receive IP Addresses from the source AP.



Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

5-3. Configure DHCP Setup

The DHCP Service function in the Client Bridge device can select a separate IP Address range within the same network segment of the source AP, and allocate those IP Addresses to connecting clients.

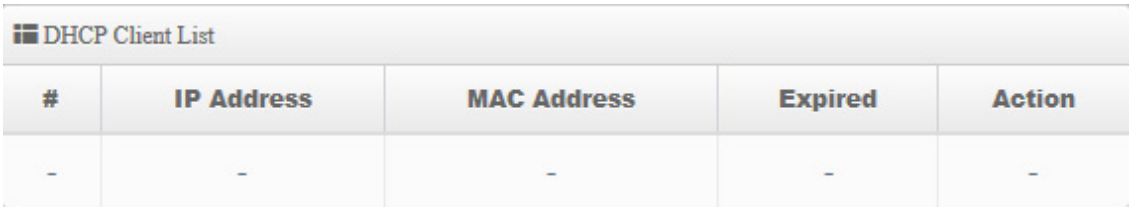


- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when

assigning IP address to clients.

- **Netmask:** The netmask default is 255.255.255.0.
- **Gateway:** Enter source gateway IP address.
- **DNS1:** Enter IP address of the first DNS server; this field is required.
- **DNS2:** 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.

DHCP Clients List: When users link to CenOS 5.0 AP and use IP address of the DHCP service, the DHCP Client List will display users the information and used IP address.

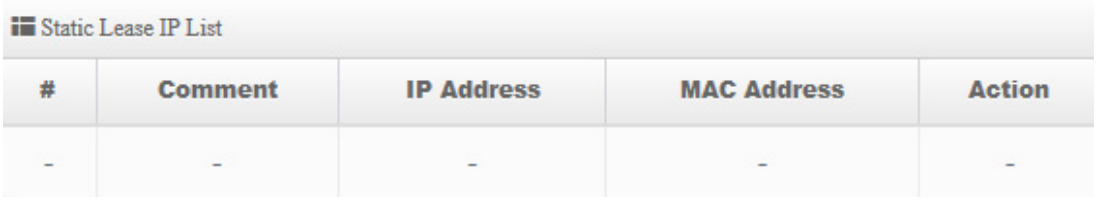


- **IP Address:** Display users used IP address.
- **MAC Address:** Display MAC Address of users used device.
- **Expired:** Display Lease expiration time of IP address.
- **Action:** Kicked user button.

Static Lease IP Setup: Administrator can set as static IP address for users.

- **Comment:** Enter description for the information.
- **IP Address:** Set static IP address for users.
- **MAC Address:** Set MAC address of user device.

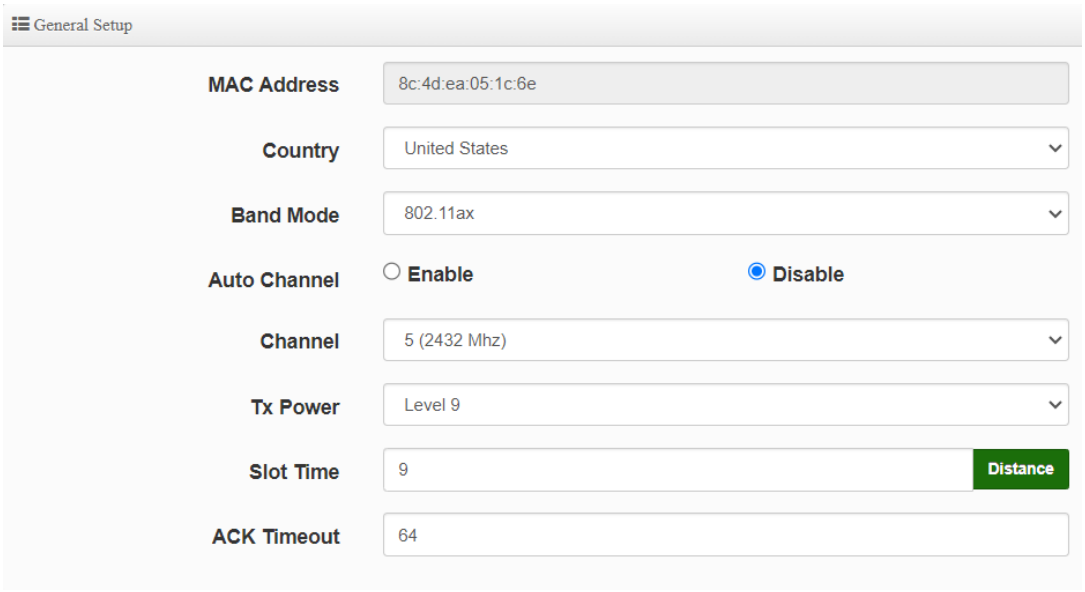
Static Lease IP List: Display users list of static IP address.



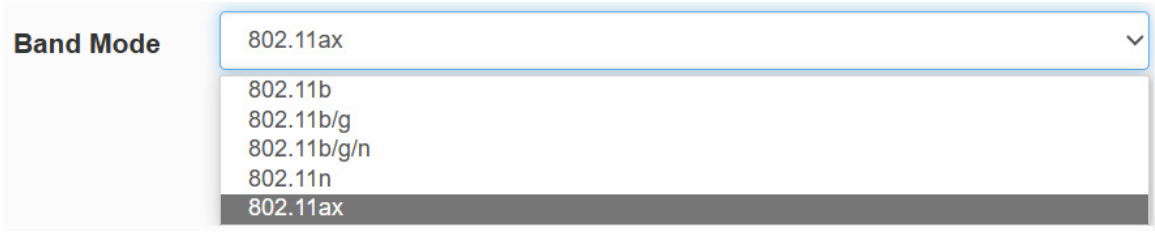
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

5-4. Wireless General Setup

5-4-1. Radio 0 (2.4G) Basic Setup



- **General Setup**
  - **MAC Address**：Display 2.4G WiFi MAC address.
  - **Country**：Administrator can select country: US or EU or Japan or Taiwan.
  - **Band Mode**：Administrator can select 2.4G Band for 802.11b、802.11b/g、802.11b/g/n、802.11n. or 802.11ax, The default is 802.11ax



  - **Auto Channel**：Administrator can Enable or Disable the function. If disabled, the WiFi channel will

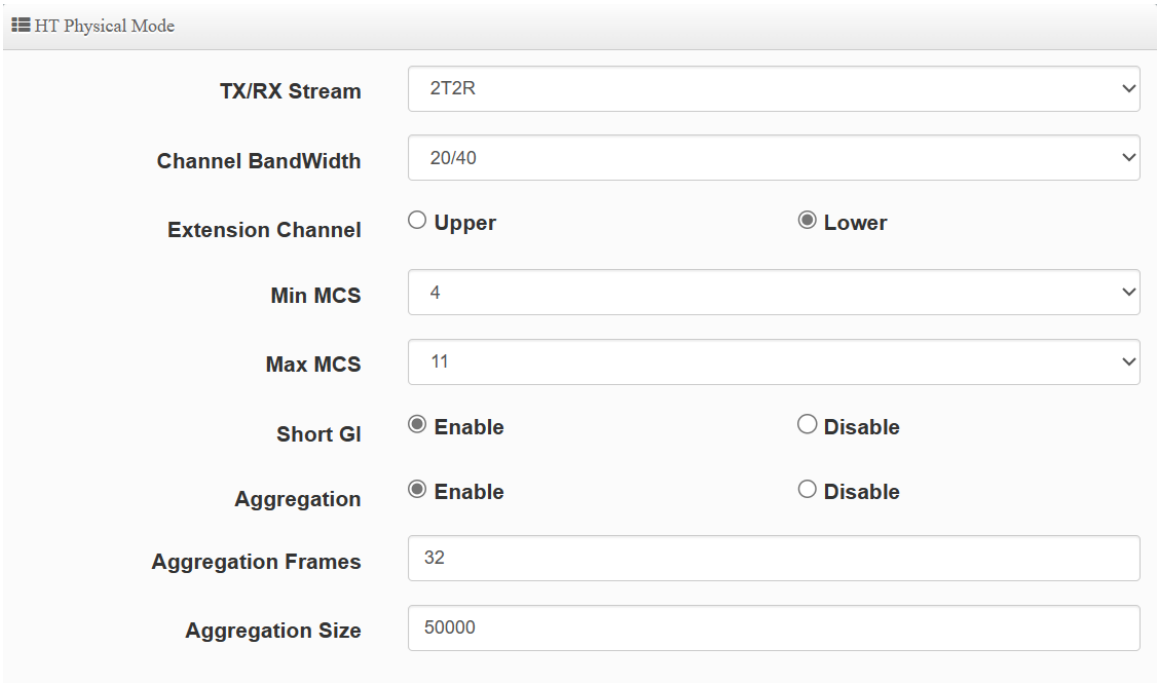
be fixed to the manually selected channel.

- **Channel**：There are different options for wireless operation modes in regions, which can be used for Upper or Lower extension.
- **Tx Power**：Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow

  Distance : When the Distance button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
- **ACK timeout**：When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice	Setting ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

HP Physical Mode



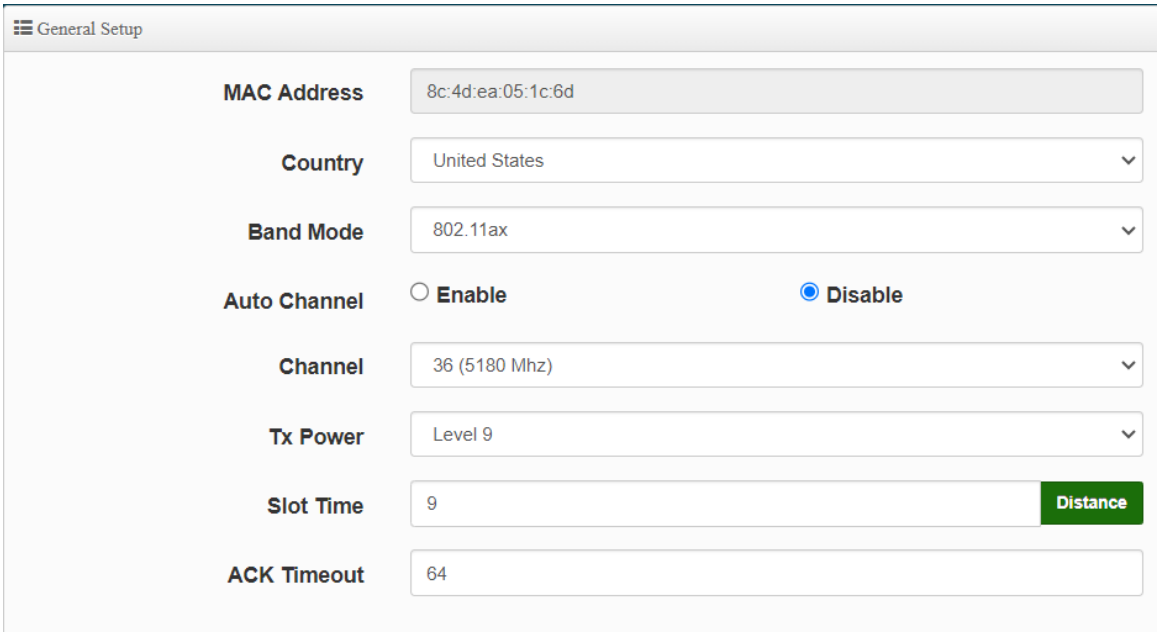
- **TX/RX Stream**：The CenOS 5.0 AP support 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

Notice

The 2.4Ghz antenna of this product thinks that it has a built-in 2x2. The default is already set to 2T2R. If there is no special requirement, please keep the setting.

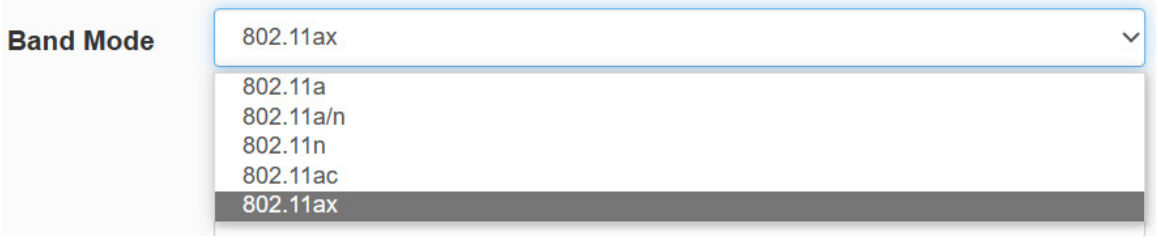
- **Channel Bandwidth**：The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel**：Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.
- **MIN MCS:** MCS compilation is a representation proposed by 802.11ax on the communication rate of WLAN.The MCS coding value will affect the main factor of the communication rate and corresponds to the channel bandwidth.
- **MAX MCS:** Maximum MCS compile set value. The Max MCS value must be greater than the Min MCS value.
- **Short GI**：Short Guard Interval is "Enabled" by default to increase throughput. 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 "**Enabled**". Select "Disable" to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard), 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:** Set frames size of Aggregation.
- **Aggregation Size:** Set aggregation size.

5-4-2. Radio 1 (5G-1) / Radio 2 (5G-2) Basic Setup

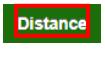


- **General Setup**

  - **MAC Address:** Display 5G-1(Radio 1) / 5G-2(Radio 2) WiFi MAC address.
  - **Country:** Administrator can select country: US or EU or Japan or Taiwan.
  - **Band Mode:** Administrator can select 5G Band for 802.11a、802.11a/n、802.11n、802.11ac. or 802.11ax, The default is 802.11ax



  - **Auto Channel:** Administrator can Enable or Disable the function. If select disabled function the WiFi channel can be manually fixed.
  - **Channel**：There are different options for wireless operation modes in regions.
  - **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
  - **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow

    Distance : When the 

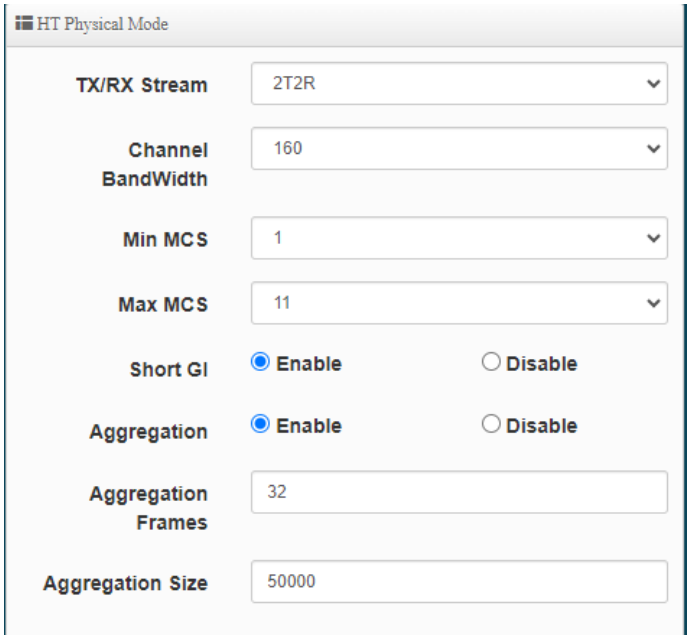
button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
  - **ACK timeout**：When waiting for the "ACKnowledgment frame" interval is too long to be received,

the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice

Setting ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

- **HP Physical Mode**



- **TX/RX Stream:** Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

Notice

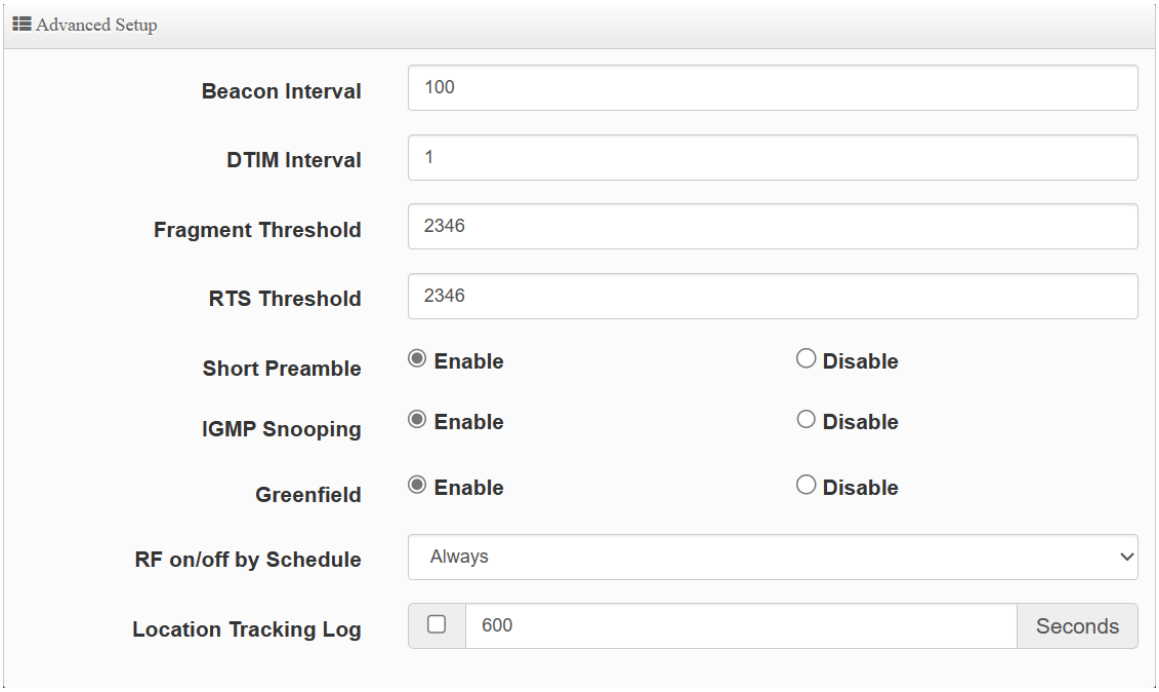
The 5Ghz antenna of this product thinks that it has a built-in 2x2. The default is already set to 2T2R. If there is no special requirement, please keep the setting.

- **Channel BandWith:** The Wireless 5G can choose 20 or 20/40 Mhz or 11ac/ax 80Mhz at 5G-1 (Radio-1) or 11ax 160Mhz at 5G-2 (Radio) as the data transmission speed between the base station and wireless users.
- **MIN MCS:** MCS compilation is a representation proposed by 802.11ax on the communication rate of WLAN.The MCS coding value will affect the main factor of the communication rate and corresponds to the channel bandwidth.
- **MAX MCS:** Maximum MCS compile set value. The Max MCS value must be greater than the Min MCS value.

- **Shout GI:** Short Guard Interval is “Enabled” by default to increase throughput. 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 “**Enabled**”. Select “Disable” to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard), 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:** Set frames size of Aggregation, the size recommend use default value is 32.
- **Aggregation Size:** Set aggregation size, the size recommends use default value is 500000.

Click **“Save”** button to save your set function. Then click “Reboot” button to activate your changes.

5-4-3. Advanced Setup



- **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 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.
- **Fragmentation Threshold:** Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same, it fragments the data packets.
  Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. Let's say from Ethernet we have to send 1400 byte packet but the fragmentation threshold is set as 400. In this case when the packet is to be transmitted on air it will fragment the packet in to 4 small packet 400+400+400+200 and send on air. This includes MAC header+ frame body and CRC so 400 byte will be in total including headers. This helps in increasing the throughput. The default is 2346.
- **RTS Threshold:** TRTS 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, this function is "***Enabled***". ***Disabling*** will automatically use the 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.
- **RF on/off by schedule:** Administrator can apply Time Policy to on or off wireless signal.
- **Location Tracking Log: T**he system can detect the signal strength of the wireless client to determine the location of the Access Point and send to database.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

5-4-4. WMM Setup

His 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.

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	☐

WMM Parmameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
AC_BE(0)	4	10	3	0	☐
AC_BK(1)	4	10	7	0	☐
AC_VI(2)	3	4	2	3008	☐
AC_VO(3)	2	3	2	1504	☐

- **AC Type**：

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

- **CWmin**：
  Minimum Contention Window. This parameter is input to the algorithm that 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

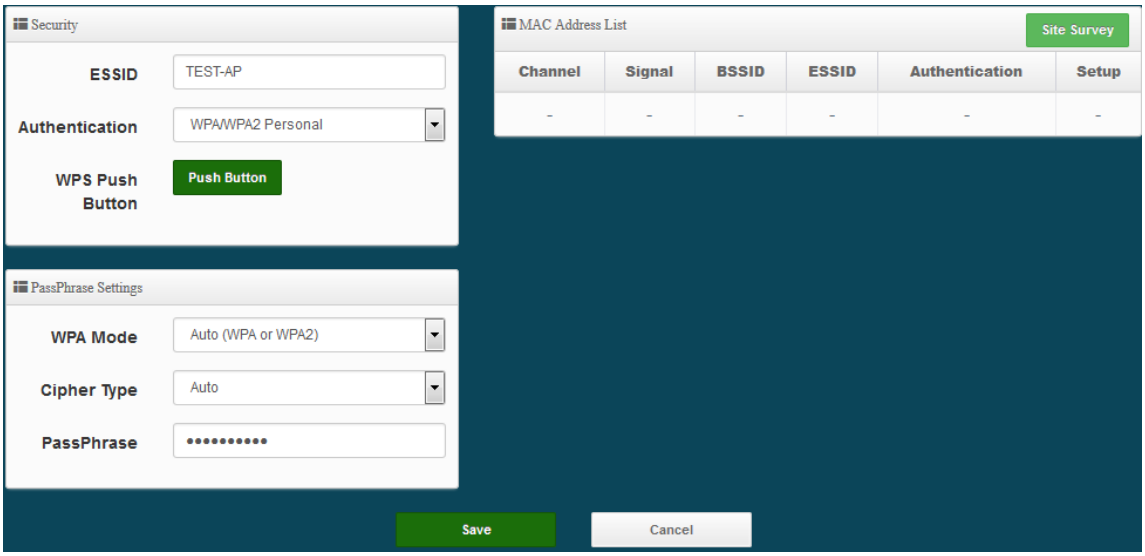
doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, 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. ◦

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

5-4-5. Station Setup

The functions setting functions include Client Bridge link to AP station. Administrator can used "site survey" function to Search for AP stations.



- **MAC Address List:** The function can discovery AP Station and select want to link the AP station, please click site survey button.
-

Notice

If want to discovery 2.4G station then administrator need to enable station mode in Radio 0 (2.4G) function page (reference manual 5.4.1 "Radio 0 Basic Setup"). Same practice if want to discovery 5G-1 or 5G-2 station will need to enable station mode in Radio 1(5G-1) or Radio 2(5G-2) function page (reference manual 5.4.2 "Radio 1(5G-1) / Radio 2(5G-2) Basic Setup").

- **Security:** After site survey AP station complete will list all AP station, when click AP station setup button then AP station information (ESSID/Security type) will display on page.
- **PassPhrase Settings:** Administrator need manual set correct ESSID security/Cipher type and pass phrase.

Notice

If Security/Cipher selected or set PassPhrase is wrong, it will not be able to bridge normally.

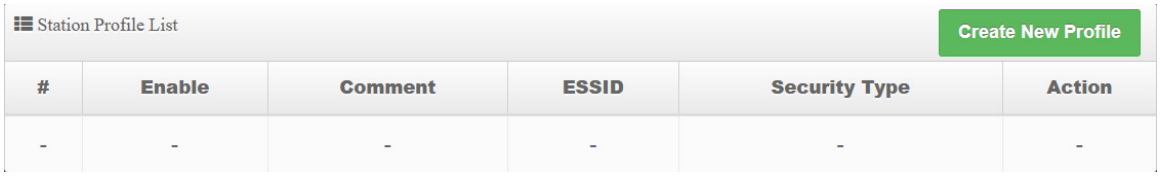
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

5-4-6. Station Porfile Setup

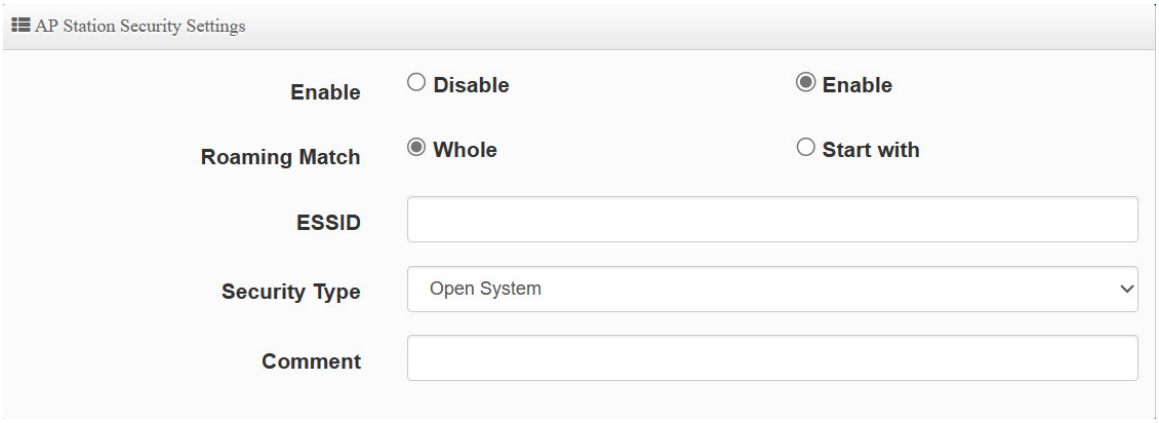
You can create setting multiple configuration files for your working Client Bridge AP connection settings and choose whether to enable single or multiple transactions at the same time.

It will automatically connect wirelessly to the bridging base stations (stations) when you move with sufficient RSSI quality.

The system will automatically connect to the bridging base stations (stations) that are enabled in the list.



- **Create New Profile：Administrator can select new ststion setup.**

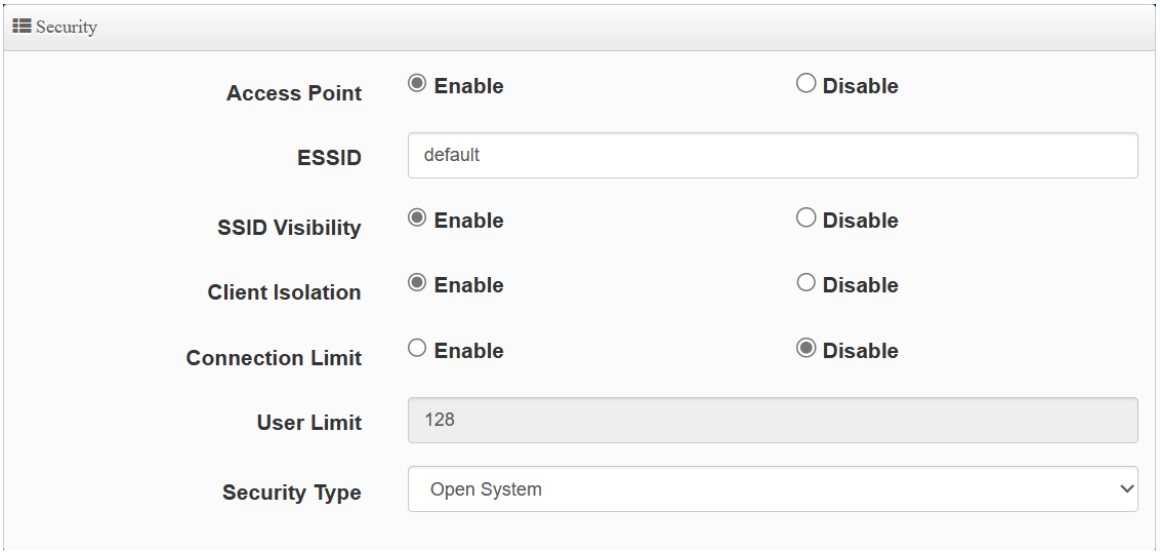


- **AP Station Security Settings**
  - **Enable**：Administrator can choose this profile enable or disable.
  - **Roaming Match**：The roaming SSID acceptance format setting requirements for all bridge AP.
    - **Whole**：Only accept same bridge AP SSID name for wireless automatic connection.
    - **Start with**：The SSID name format with different SSID but the same prefix of the wireless automatic connection bridge AP can be accepted.

      For example, the SSID names of all bridging base stations along the line may be station 1, station 2 or station3 and other SSID format names for different station divisions.
  - **SSID**：Administrator can set Wi-Fi SSID name
  - **Security Type**：Administrator can select the encryption information corresponding to the bridge AP connection.
  - **Comment**：Administrator can be marked for each of profiles individual notes.

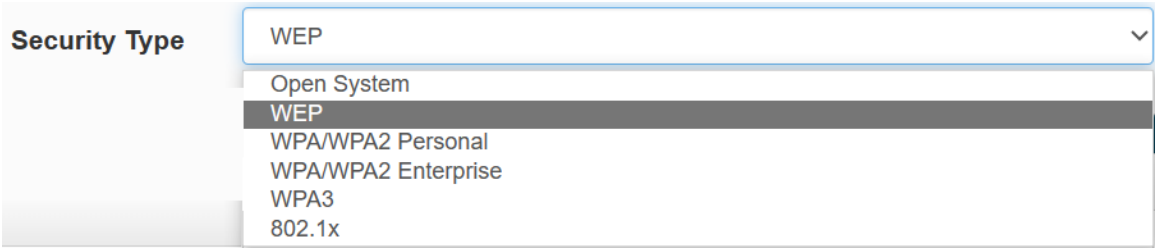
5-4-7. Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations.



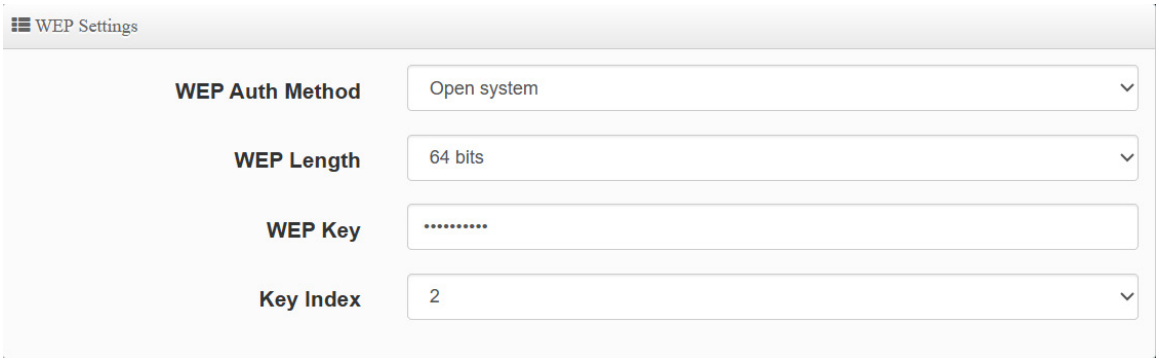
- **Access Point:** Administrator can Enable or Disable the Repeater AP function.
- **ESSID:** Enter the Repeater AP of ESSID name.
- **SSID Visibility:** The default it's Enable**.** When select Disable the SSID will not is discovered.
- **Client Isolation:** This function is Disabled by default. All clients will be isolated from each other, which mean they can't reach each other.
- **Connection Limit:** Administrator can select Enable or Disable WiFi connection Limit

  【Supports 128 users to access at the same time.】
- **Security Type:** Select the desired security type from the drop-down list; the options are Open System, WPA-PSK/WPA2-Personal, WPA/WPA2-Enterprise, WPA3 and 802.1x



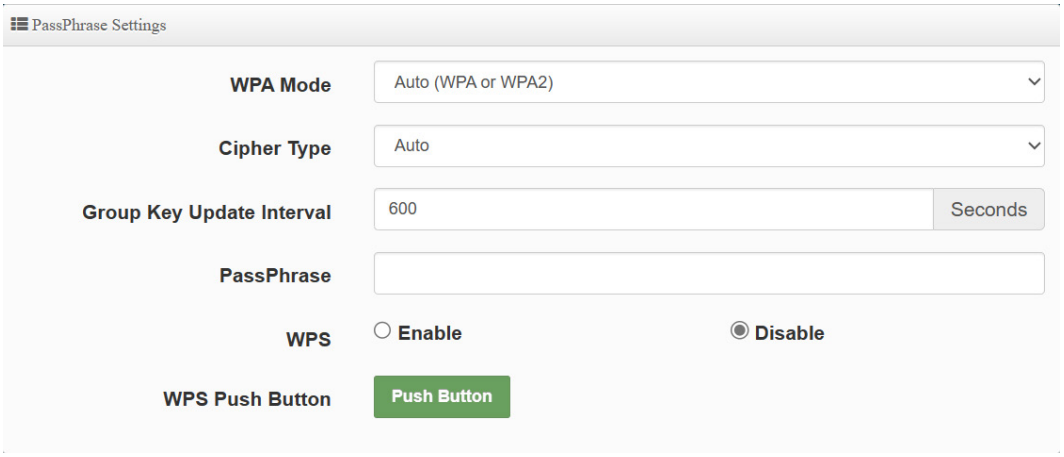
Notice	*Notes: The WEP encryption mode is currently known to be not the most secure wireless encryption method, and will not be able to support 802.11ac/ax. It is not recommended that you continue to use this WEP encryption mode. It is recommended that you use a rate that meets 802.11ac/ax Correspondingly supported encryption modes above WPA / WPA2 to increase your wireless network security.*

- **Open System**：Data is not unencrypted during transmission when this option is selected.**(be not recommended for use)**



- **WEP**：
  - ✓ **WEP Auth Method**：Administrator can choose the WEP Open system open authentication method or the WEP Shared password authentication method.
  - ✓ **WEP Length**：Administrator can choose to use 64bits, 128bits, and 152bits encryption key lengths, but must make sure that the wireless network card used by your wireless client also supports the corresponding wireless key length.
  - ✓ **WEP Key**：There are four groups of optional settings the 16-bit (HEX) key value.
  - ✓ **Key Index**：Administrator can pre-set 4 WEP Key for your WEP and "save".when the future wireless client wants to connect, can be choose which group of wireless keys and establish a connection through WEP encryption.

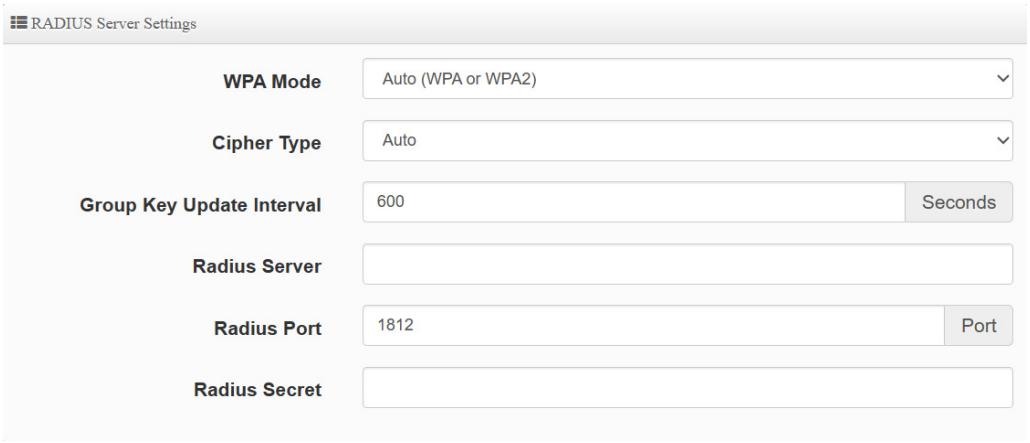
Notice	*Note: If you choose to use WEP encryption mode, please enter the corresponding WEP key value according to the following requirements.* *64bits:* *10 groups of Hexadecimal characters (0~9, A~F and a~f can be used)* *5 groups of ASCII characters (0~9, A~Z and a~z can be used)* *128bits:* *26 groups of Hexadecimal characters (0~9, A~F and a~f can be used)* *13 groups of ASCII characters (0~9, A~Z and a~z can be used)* *152bits:* *32 groups of Hexadecimal characters (0~9, A~F and a~f can be used)* *16 groups of ASCII characters (0~9, A~Z and a~z can be used)*



- **WPA / WPA2-Personal**：
  - ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
  - ✓ **Cipher Type:** Administrator can select use AES or TKIP with 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.

Notice	Note: When setting WEP or TKIP encryption, the data rate will not exceed 54 Mbps. The IEEE 802.11n protocol prohibits the use of high throughput with WEP or TKIP as unicast keys. If you use these encryption methods (such as WEP, WPA-TKIP, WPA2-TKIP), your data rate will be reduced to 54 Mbps, or if it is used for commercial purposes, such as applications where the end user cannot connect to the wireless at a higher speed than 54 Mbps.

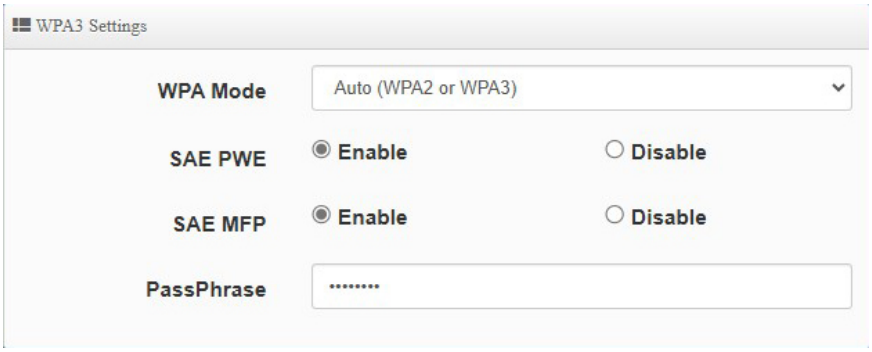
- ✓ **Group Key Update Interval**: The time interval is for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Pass Phrase:** Enter the ESSID pass phrase.
- ✓ **WPS Push Button:** Administrator can used WPS function to link WiFi client. If enabled, administrator can click the WPS Push Button.



- **WPA / WPA2-Enterprise：**
  - ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
  - ✓ **Cipher Type:** Administrator can select use AES or TKIP with 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.

Notice	Note: When setting WEP or TKIP encryption, the data rate will not exceed 54 Mbps. The IEEE 802.11n protocol prohibits the use of high throughput with WEP or TKIP as unicast keys. If you use these encryption methods (such as WEP, WPA-TKIP, WPA2-TKIP), your data rate will be reduced to 54 Mbps, or if it is used for commercial purposes, such as applications where the end user cannot connect to the wireless at a higher speed than 54 Mbps.

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



- **WPA3 :**

  The 802.11ax peer-to-peer entity authentication mode is different from the Pre-Shared Key .

  ✓ **SAE Password**：When the administrator sets this virtual wireless network SSID to use WPA3 calculation, the SAE connection password must be at least 8 characters.

  ✓ **SAE PWE**：Optionally enable the SAE PWE (Password Element) function, before exchanging SAE authentication messages, both parties will generate a private element PWE (Password Element) and two private values (rand and mask) for advanced authentication exchange.

  ✓ **SAE MFP**：The SAE password authentication mechanism adds a more secure anti-theft, anti-spy, and anti-skimming password Management Frame Protection (MFP).
  If the AP enabled this mode, please ensure that both the AP and the client running in this mode need Management Frame Protection (MFP) support.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

5-4-8. MAC Filter Setup

Administrator can setup allow or reject WiFi clients(MAC address) to access Repeater AP.

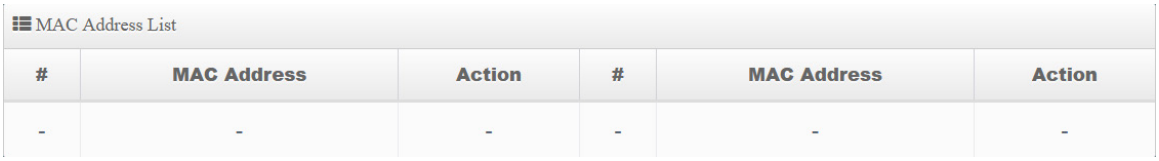
➢ **Rule:** Select the desired access control type from the drop-down list; the options are Disable, Allow or Reject.

- **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**".

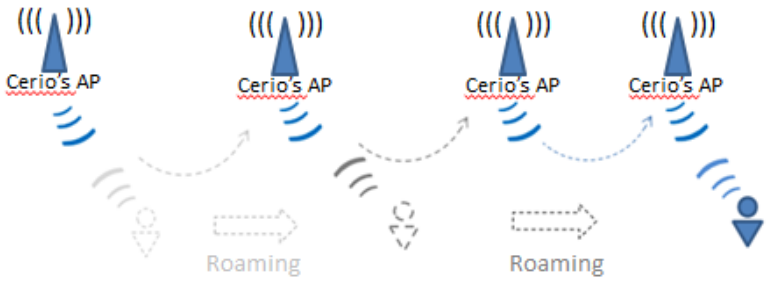
➢ **MAC Address:** Enter MAC Address for WiFi Clients.

➢ **MAC Address List:** Display the MAC address of WiFi Clients.

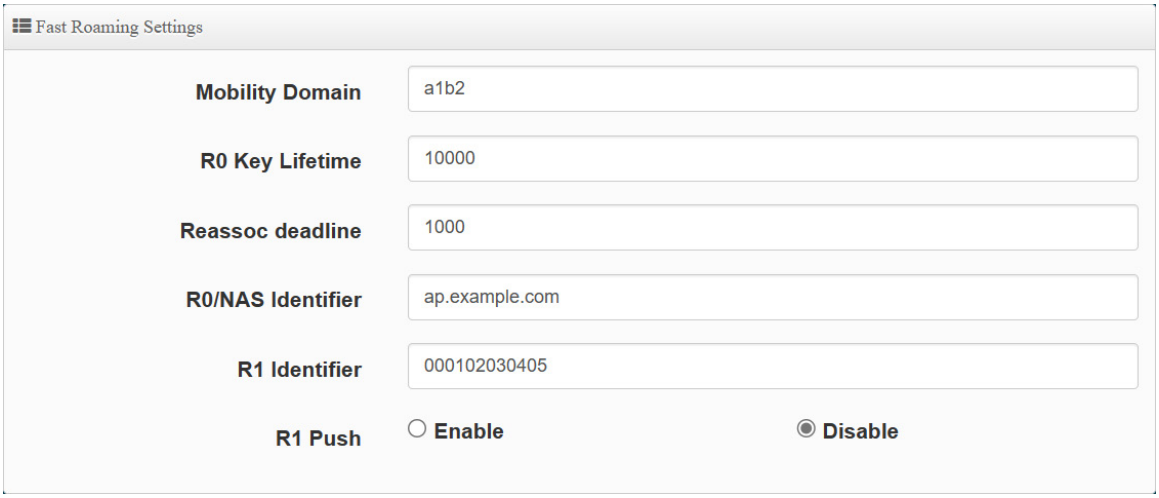


Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

5-4-9. 802.11r Fast Roaming



The Tri band Access Point supports 802.11r/802.11k function for 2.4G (Rado 0)and 5G (Rado 1)and (Rado 2). 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.



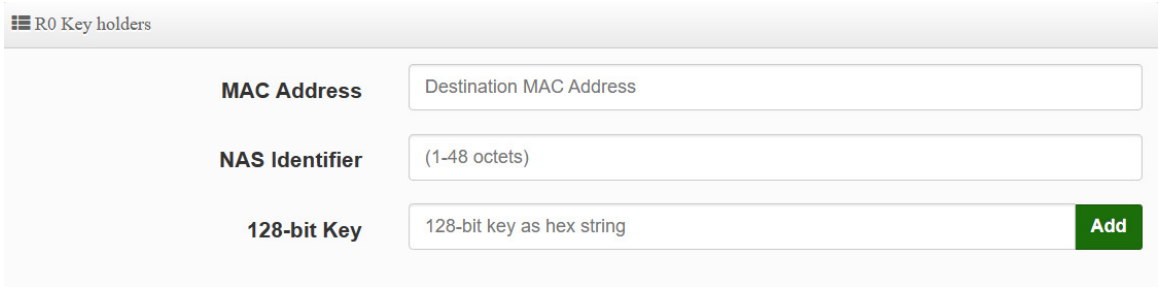
- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition.

Notice *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 setting 1~65535.
- **Reassoc deadline:** Reassociation deadline in time units (TUs / 1.024 ms; range 1000~65535). The default is 1000.
- **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 or disable. If enable the function will automatically sent the R1 Key.

R0 Key Address:

To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.

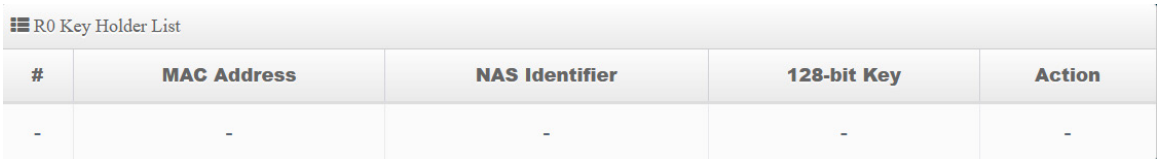


- **MAC Address:** Enter must key in the MAC Address of other AP
- **NAS Identifier:** Enter 1~48 octets of network domain name.

- **128-bit Key:** Enter Shared Key of 128 bit.

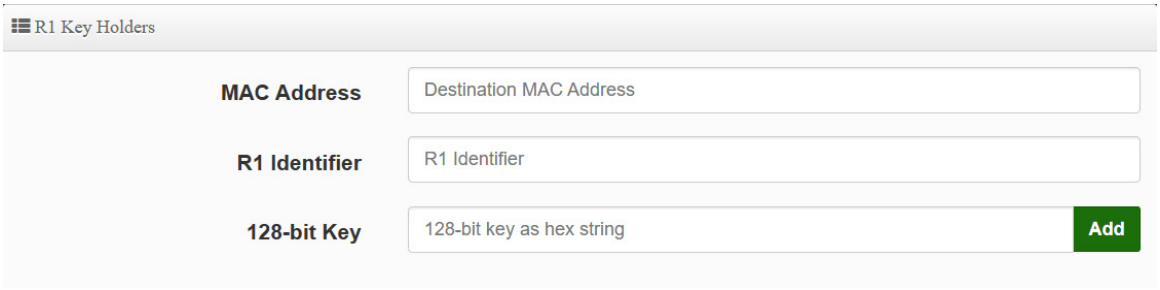
R0 Key Holder List:

After setting "R0 Key holders" function the information will appear in list.



R1 Key Holder List:

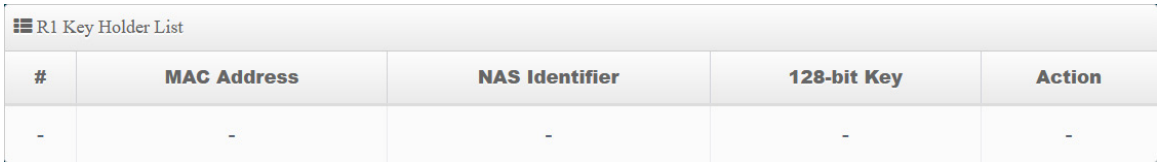
Enter a unified set of R1 Key Holder identification certification.



- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

R1 Key Holder List:

After setting "R1 Key holders" function the information will appear in list.



Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes

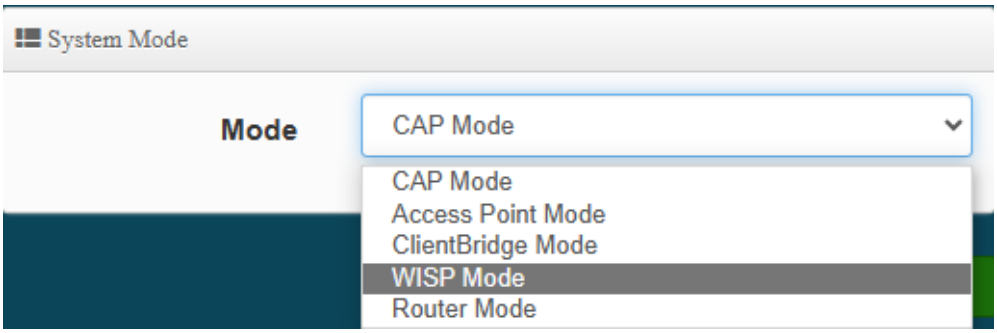
6. WISP Mode

WISP Mode is a router function, if the Telecom company permits wireless connection to their WAN, administrators can change the CenOS 5.0 AP to WISP Mode to connect to the wifi network.
The WISP Mode support PPPoE / Static IP / Dynamic IP and PPTP for WAN, and support Repeater AP function.

6-1. Change Setup mode

If the administrator needs to switch to WISP mode, Please click "System"-> " Mode Setup " to change WISP mode.

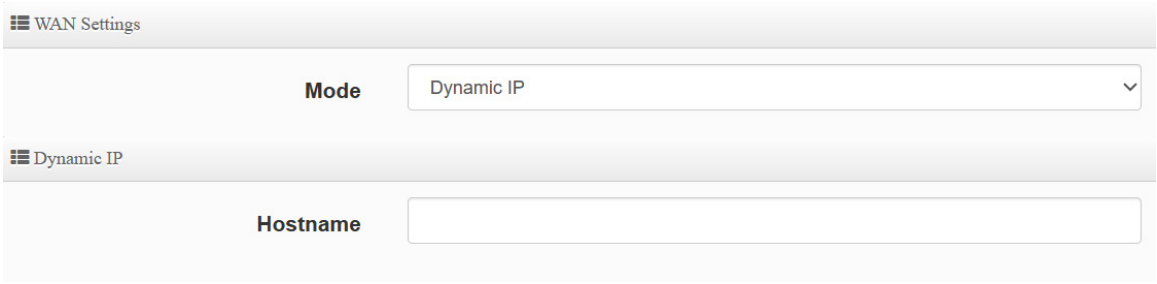
Notice	*When the upper limit of the 2.4G frequency is used, the repeater AP will only be able to use the other two 5G extension Repeater AP APs. If the upper end AP with a Radio 1 (5G) frequency is used, the repeater AP will only Use 2.4G and another Radio 2 (5G) as the extension Repeater AP base.*



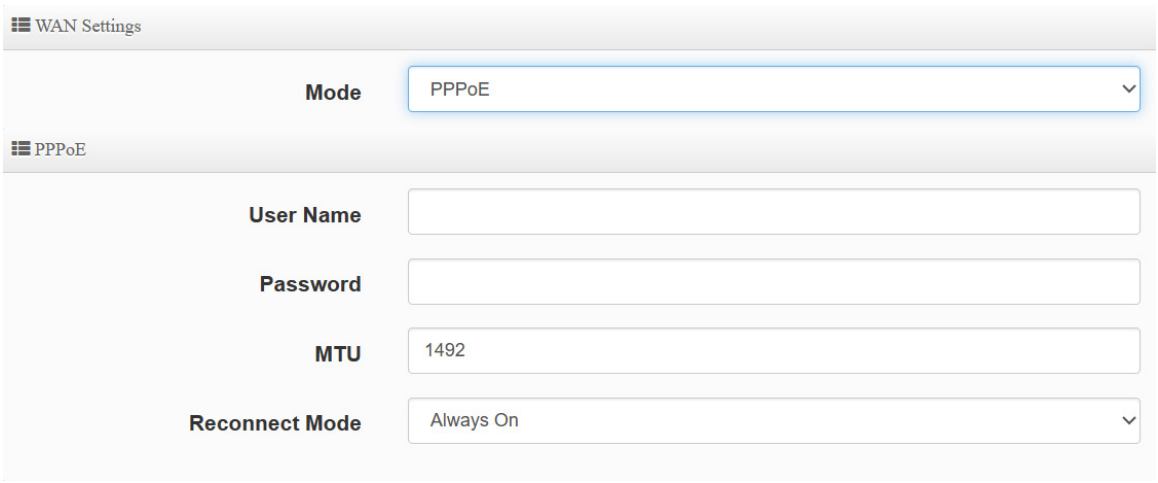
6-2. Configure WAN Setup

There are four connection types for the WAN port: **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**. Please click on **System -> WAN** and follow the below setting.

- **Static IP:** Users can manually setup the WAN IP address with a static IP provided by WISP.
  - **IP Address:** The IP address of the WAN port.
  - **IP Netmask:** The Subnet mask of the WAN port.
  - **IP Gateway:** The default gateway of the WAN port.

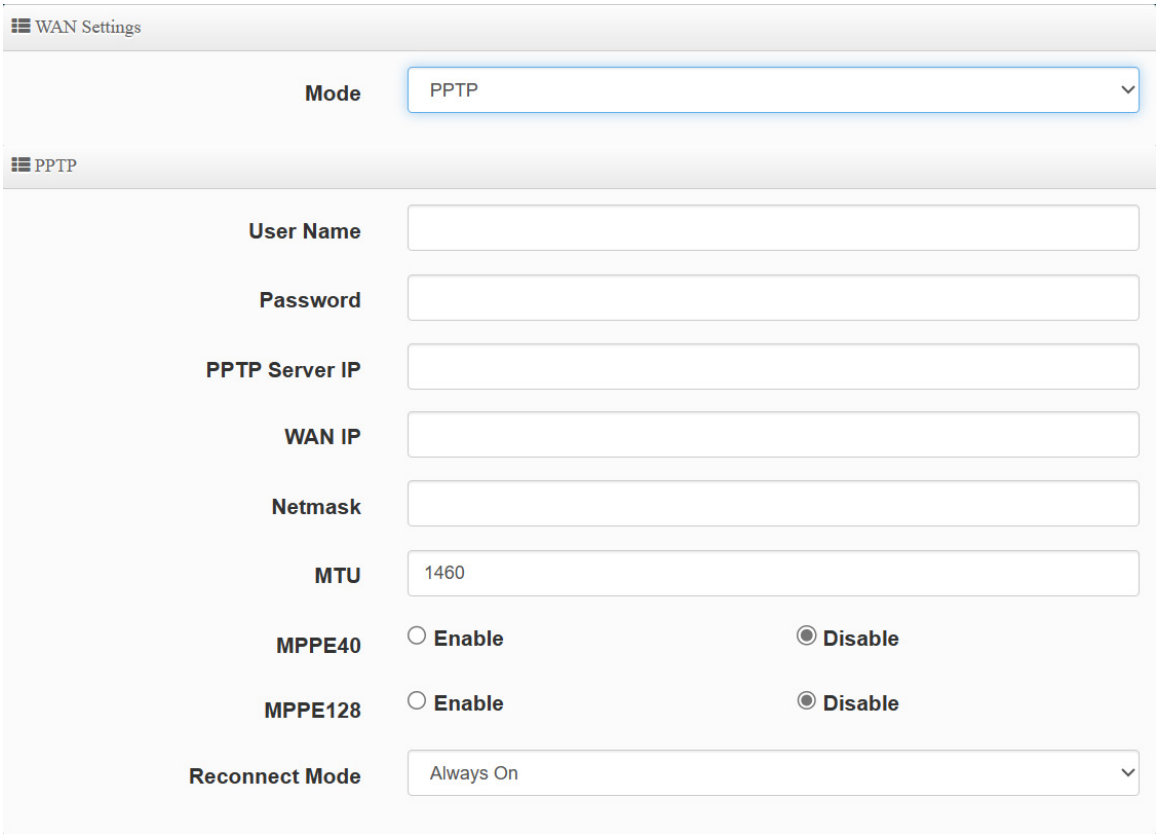


- **Dynamic IP:** Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click ***Release*** button to release IP address and click ***Renew*** button to renew IP address again.
  - **Hostname :** The Hostname of the WAN port



- **PPPoE :** To create wireless PPPoE WAN connection to a PPPoE server in network.
  - **User Name :** Enter User Name for PPPoE connection
  - **Password :** Enter Password for PPPoE connection
  - **MTU:** By default, MTU is set to **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
  - **Reconnect Mode:** Administrator can select three function for Always On / On Demand / Manual.
    - ✓ **Always on** – A connection to Internet is always maintained.

- ✓ **On Demand** – A connection to Internet is made as needed.
- ✓ **Manual** – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.

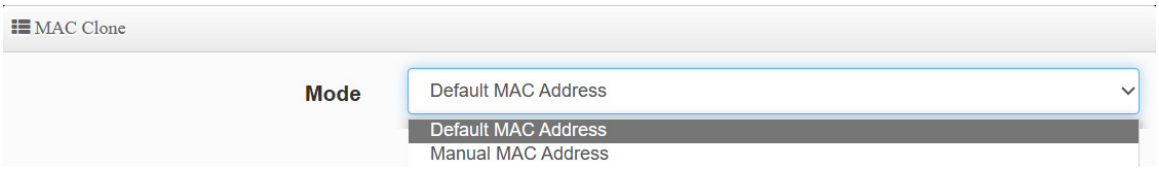


➢ **PPTP:** The Point-to-Point Tunneling Protocol (PPTP) mode enables the implementation of secure multi-protocol Virtual Private Networks (VPNs) through public networks.

- **User Name:** Enter account for PPTP.
- **Password:** Enter user name account used password for PPTP.
- **PPTP Server IP:** Enter remote IP address of PPTP Server.
- **WAN IP:** The IP address of the WAN port.
- **Netmask:** The Subnet mask of the WAN port.
- **MTU:** By default, it's **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **MPPE40/128:** 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:** Administrator can select three function for Always On / On Demand / Manual.
  - ✓ **Always on** – A connection to Internet is always maintained.
  - ✓ **On Demand** – A connection to Internet is made as needed.
  - ✓ **Manual** – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.



➢ **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.

- **Default MAC Address:** Keep the default MAC address of WAN port on the system.
- **Manual MAN Address:** Enter the MAC address registered with your ISP.

➢ **DNS :** Check "No Default DNS Server" or "Specify DNS Server IP" radial button as desired to set up system DNS.

- **Primary DNS:** The IP address of the primary DNS server.
- **Secondary DNS:** The IP address of the secondary DNS server.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

6-3. Configure LAN Setup

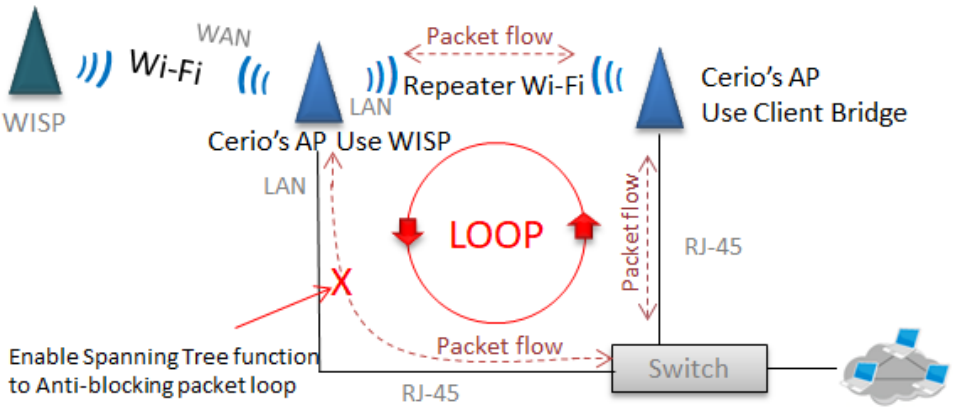
Here are the instructions for how to setup the local IP Address and Netmask. Please click on **System -> LAN** and follow the below setting.

IP Settings: Administrator can select the IP used Static or Dynamic IP address.

- Static IP : A set of fixed IP addresses can be manually set for the system to use.
- Dynamic IP : If there is a DHCP server on the top, you can use the dynamic IP address to let the system obtain a set of IP automatically.

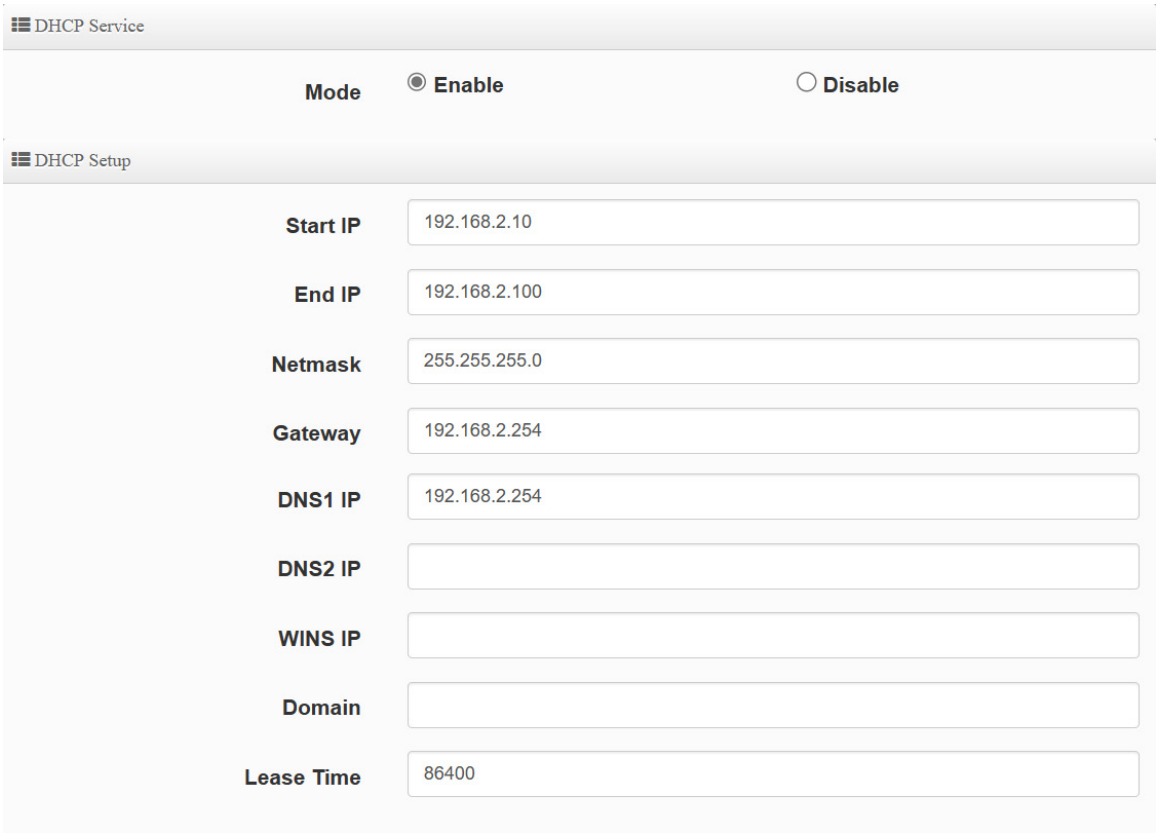
802.1d Spanning Tree：

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, which is also referred to as STP, is defined in the IEEE Standard 802.1d.



6-4. Configure DHCP Setup

The DHCP Service function in the WISP device can select a separate IP Address range within the same network segment of the source AP, and allocate those IP Addresses to connecting clients.



DHCP Setup

- **Start IP / End IP:** Specify the range of IP addresses to be used by the DHCP server when assigning IP address to clients.
- **Netmask:** The netmask default is 255.255.255.0.
- **Gateway:** Enter source gateway IP address.
- **DNS1:** Enter IP address of the first DNS server; this field is required.
- **DNS2:** 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

DHCP Clients List:

When users link to CenOS 5.0 AP and use IP address of the DHCP service, the DHCP Client List will display users the information and used IP address.

DHCP Client List

#	IP Address	MAC Address	Hostname	Expired	Action
-	-	-	-	-	

- **IP Address:** Display users used IP address.
- **MAC Address:** Display MAC Address of users used device.
- **Expired:** Display Lease expiration time of IP address.
- **Action:** Kicked user button.

Static Lease IP Setup

Comment

IP Address

MAC Address

Add

- **Static Lease IP Setup:** Administrator can set as static IP address for users.
  - **Comment:** Enter description for the information.
  - **IP Address:** Set static IP address for users.
  - **MAC Address:** Set MAC address of user device.

Static Lease IP List

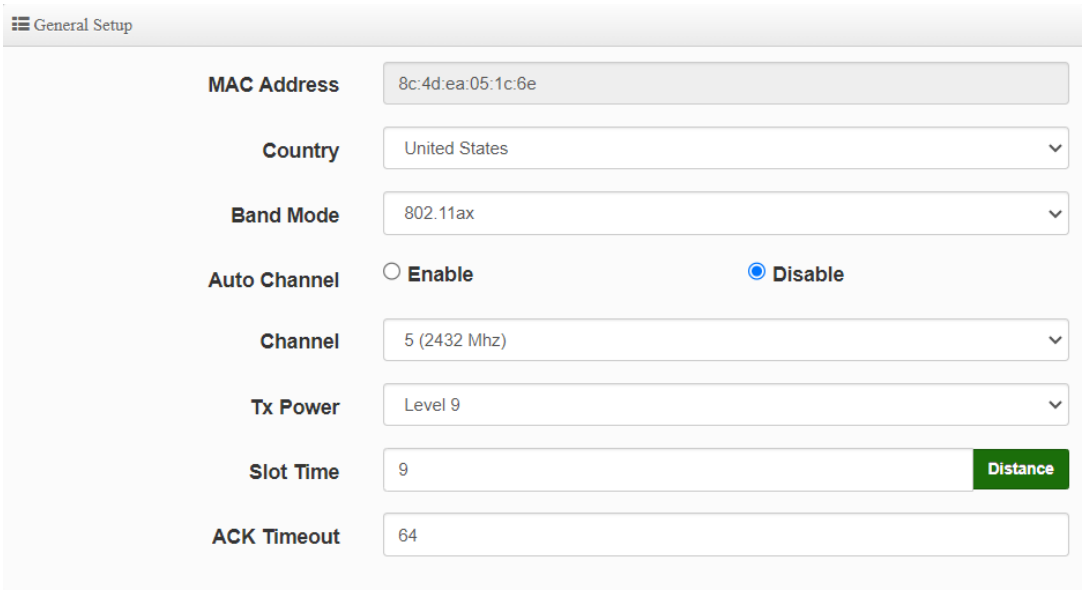
#	Comment	IP Address	MAC Address	Action
-	-	-	-	-

- **Static Lease IP List:** Display users list of static IP address.

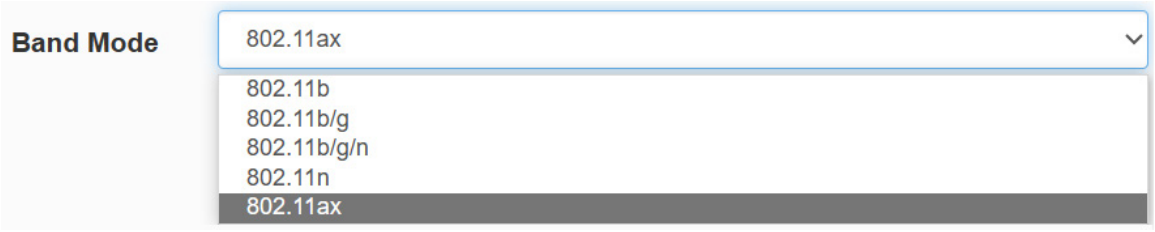
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

6-5. Wireless General Setup

6-5-1. Radio 0 (2.4G) Basic Setup



- **General Setup**
  - **MAC Address**：Display 2.4G WiFi MAC address.
  - **Country**：Administrator can select country: US or EU or Japan or Taiwan.
  - **Band Mode**：Administrator can select 2.4G Band for 802.11b、802.11b/g、802.11b/g/n、802.11n. or 802.11ax, The default is 802.11ax



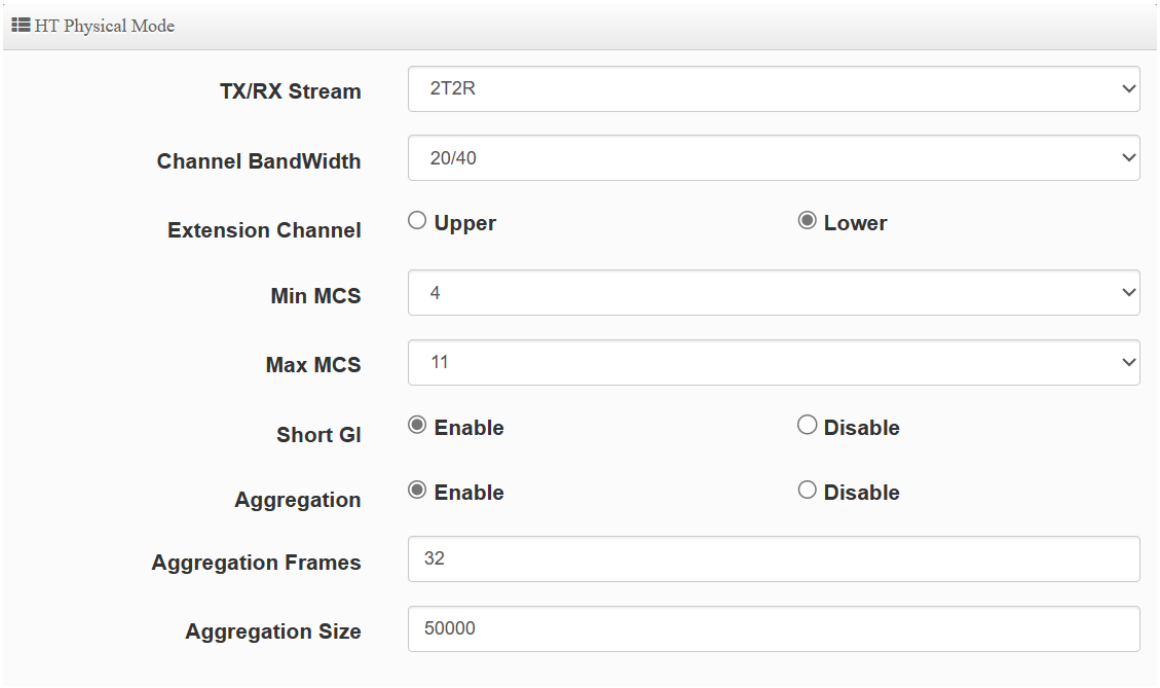
- **Auto Channel**：Administrator can Enable or Disable the function. If disabled, the WiFi channel will be fixed to the manually selected channel.
- **Channel**：There are different options for wireless operation modes in regions, which can be used for Upper or Lower extension.
- **Tx Power**：Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow

  Distance : When the Distance button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).

- **ACK timeout**：When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice	Setting ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

HP Physical Mode



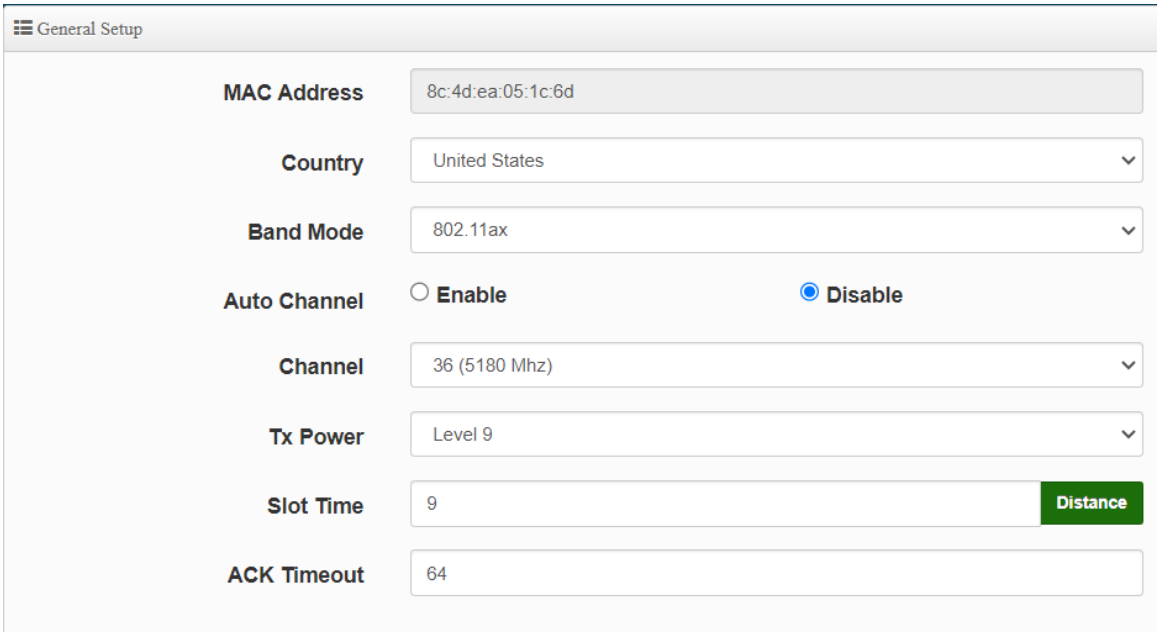
- **TX/RX Stream**：The CenOS 5.0 AP support 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

Notice	The 2.4Ghz antenna of this product thinks that it has a built-in 2x2. The default is already set to 2T2R. If there is no special requirement, please keep the setting.

- **Channel Bandwidth**：The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel**：Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.

- **MIN MCS:** MCS compilation is a representation proposed by 802.11ax on the communication rate of WLAN.The MCS coding value will affect the main factor of the communication rate and corresponds to the channel bandwidth.
- **MAX MCS:** Maximum MCS compile set value. The Max MCS value must be greater than the Min MCS value.
- **Short GI**：Short Guard Interval is “Enabled” by default to increase throughput. 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 “**Enabled**”. Select “Disable” to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard), 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:** Set frames size of Aggregation.
- **Aggregation Size:** Set aggregation size.

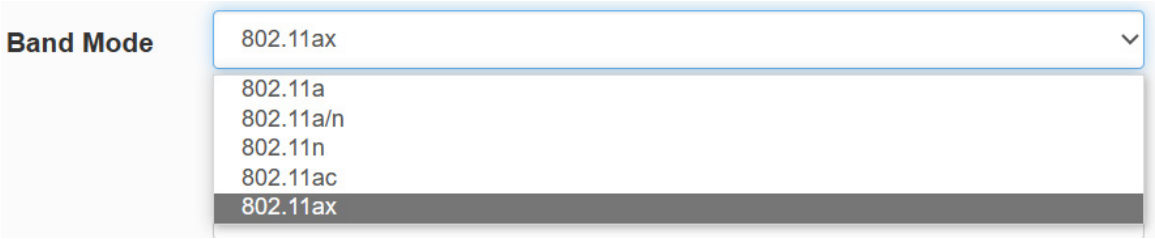
6-5-2. Radio 1 (5G-1) / Radio 2 (5G-2) Basic Setup



- **General Setup**

- **MAC Address:** Display 5G-1(Radio 1) / 5G-2(Radio 2) WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Japan or Taiwan.

- **Band Mode:** Administrator can select 5G Band for 802.11a、802.11a/n、802.11n、802.11ac. or 802.11ax, The default is 802.11ax

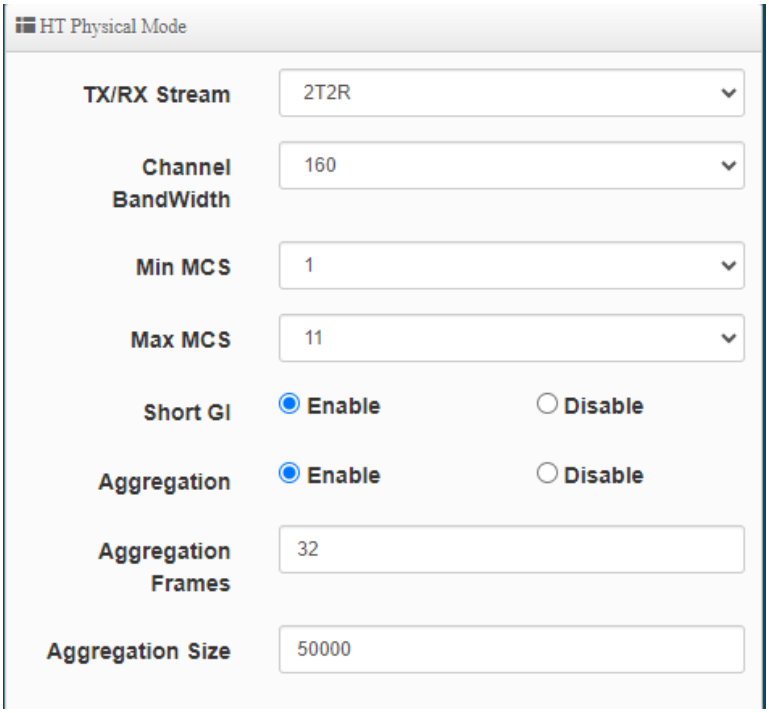


- **Auto Channel:** Administrator can Enable or Disable the function. If select disabled function the WiFi channel can be manually fixed.
- **Channel**：There are different options for wireless operation modes in regions.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow

  Distance : When the Distance button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
- **ACK timeout**：When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice	Setting ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

- **HP Physical Mode**



- **TX/RX Stream:** Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

Notice	The 5Ghz antenna of this product thinks that it has a built-in 2x2. The default is already set to 2T2R. If there is no special requirement, please keep the setting.

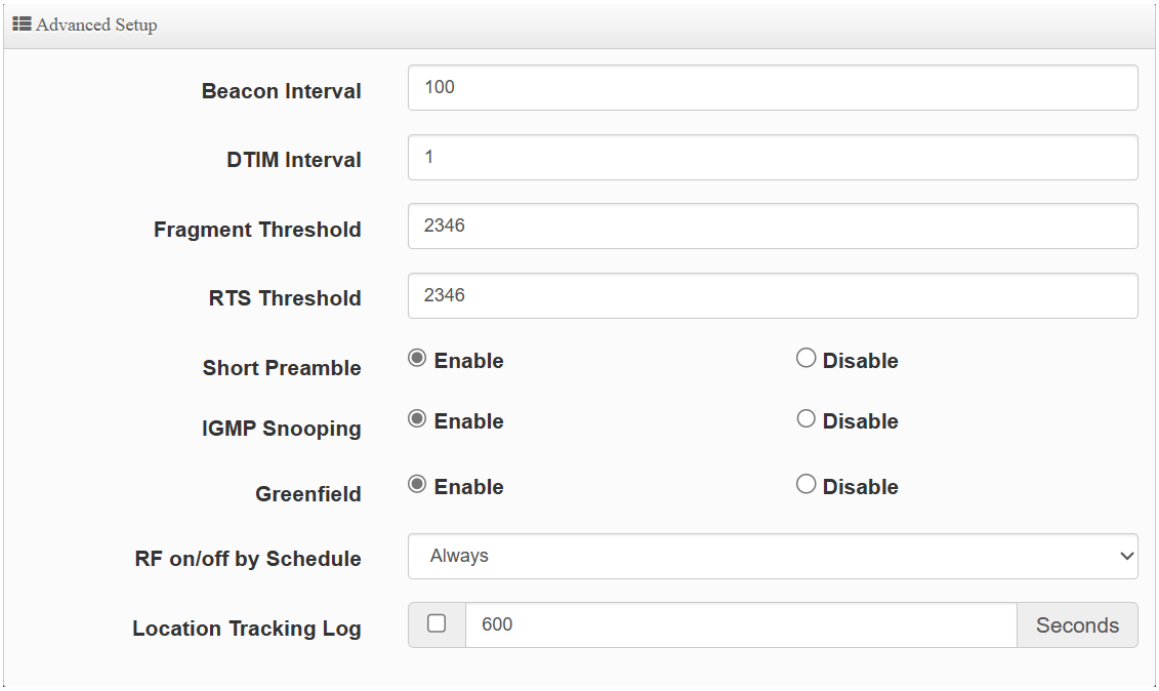
- **Channel BandWith:** The Wireless 5G can choose 20 or 20/40 Mhz or 11ac/ax 80Mhz at 5G-1 (Radio-1) or 11ax 160Mhz at 5G-2 (Radio) as the data transmission speed between the base station and wireless users.
- **MIN MCS:** MCS compilation is a representation proposed by 802.11ax on the communication rate of WLAN.The MCS coding value will affect the main factor of the communication rate and corresponds to the channel bandwidth.
- **MAX MCS:** Maximum MCS compile set value. The Max MCS value must be greater than the Min MCS value.
- **Shout GI:** Short Guard Interval is “Enabled” by default to increase throughput. 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 “**Enabled**”. Select “Disable” to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard), 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:** Set frames size of Aggregation, the size recommend use default value is 32.
- **Aggregation Size:** Set aggregation size, the size recommends use default value is 500000.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

6-5-3. Advanced Setup



- **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 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.
- **Fragmentation Threshold:** Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same, it fragments the data packets.
  Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. Let's say from Ethernet we have to send 1400 byte packet but the fragmentation threshold is set as 400. In this case when the packet is to be transmitted on air it will fragment the packet in to 4 small packet 400+400+400+200 and send on air. This includes MAC header+ frame body and CRC so 400 byte will be in total including headers. This helps in increasing the throughput. The default is 2346.
- **RTS Threshold:** TRTS 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, this function is "***Enabled***". ***Disabling*** will automatically use the 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.

- **RF on/off by schedule:** Administrator can apply Time Policy to on or off wireless signal.
- **Location Tracking Log: T**he system can detect the signal strength of the wireless client to determine the location of the Access Point and send to database.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

6-5-4. WMM Setup

His 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.

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	☐

WMM Parmameters of Station

AC Type	CWmin	CWmax	AIFS	TxOp Limit	ACM bit
AC_BE(0)	4	10	3	0	☐
AC_BK(1)	4	10	7	0	☐
AC_VI(2)	3	4	2	3008	☐
AC_VO(3)	2	3	2	1504	☐

- **AC Type**：

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

- **CWmin**：

  Minimum Contention Window. This parameter is input to the algorithm that 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

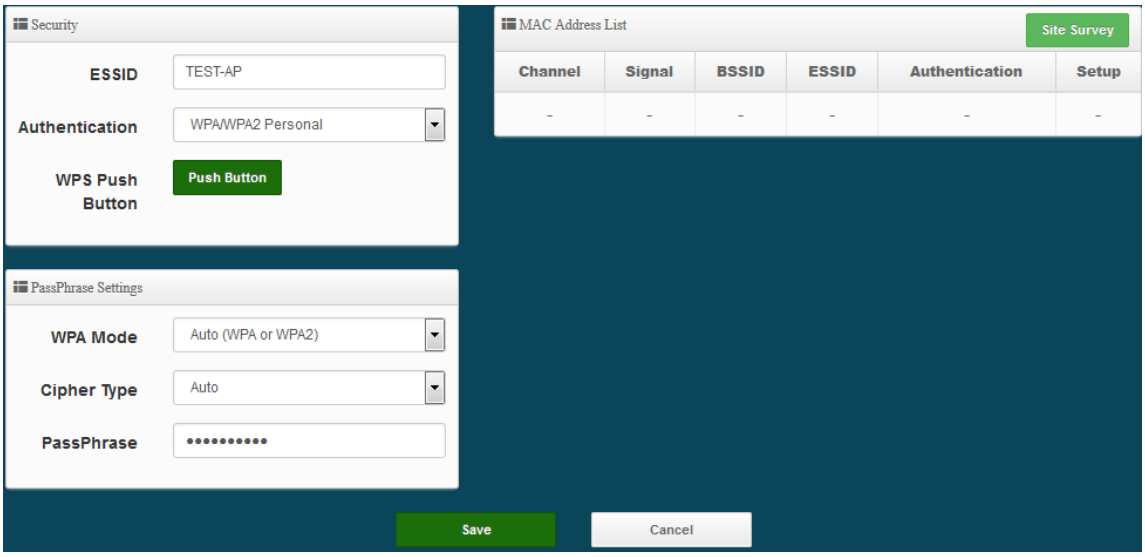
doubling continues until either the data frame is sent or the Maximum Contention Window size is reached. Once the Maximum Contention Window size is reached, retries will continue until a maximum number of retries allowed is reached. Valid values for the "cwmax" are 1, 3, 7, 15, 31, 63, 127, 255, 511, 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. ◦

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

6-5-5. Station Setup

The functions setting functions include WISP link to AP station. Administrator can used "site survey" function to Search for AP stations.



- **MAC Address List:** The function can discovery AP Station and select want to link the AP station, please click site survey button.

Notice

If want to discovery 2.4G station then administrator need to enable station mode in Radio 0 (2.4G) function page (reference manual 6.5.1 "Radio 0 Basic Setup"). Same practice if want to discovery 5G-1 or 5G-2 station will need to enable station mode in Radio 1(5G-1) or Radio (5G-2) function page (reference manual 6.5.2 "Radio 1(5G-1) / Radio 1(5G-2) Basic Setup").

- **Security:** After site survey AP station complete will list all AP station, when click AP station setup button then AP station information (ESSID/Security type) will display on page.
- **PassPhrase Settings:** Administrator need manual set correct ESSID security/Cipher type and pass phrase.

Notice

If Security/Cipher selected or set PassPhrase is wrong, it will not be able to bridge normally.

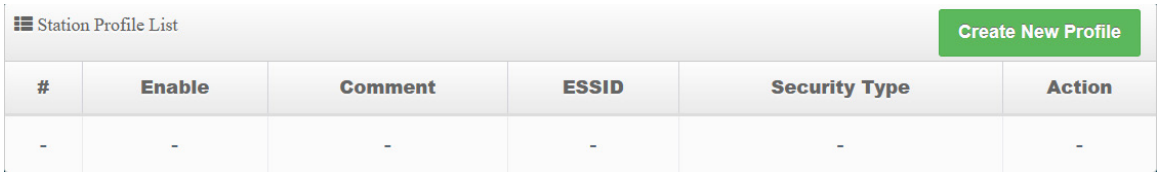
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

6-5-6. Station Porfile Setup

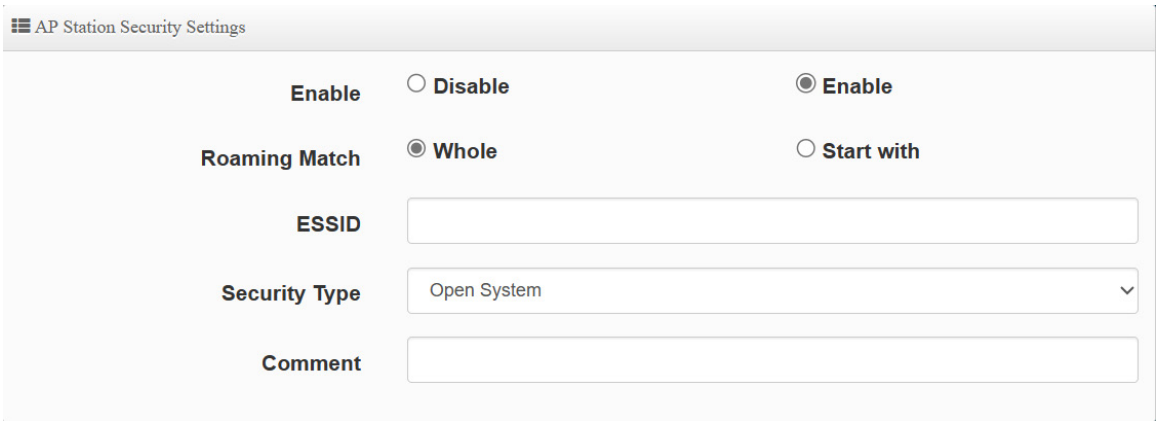
You can create setting multiple configuration files for your working WISP AP connection settings and choose whether to enable single or multiple transactions at the same time.

It will automatically connect wirelessly to the bridging base stations (stations) when you move with sufficient RSSI quality.

The system will automatically connect to the bridging base stations (stations) that are enabled in the list.



- **Create New Profile：Administrator can select new ststion setup.**

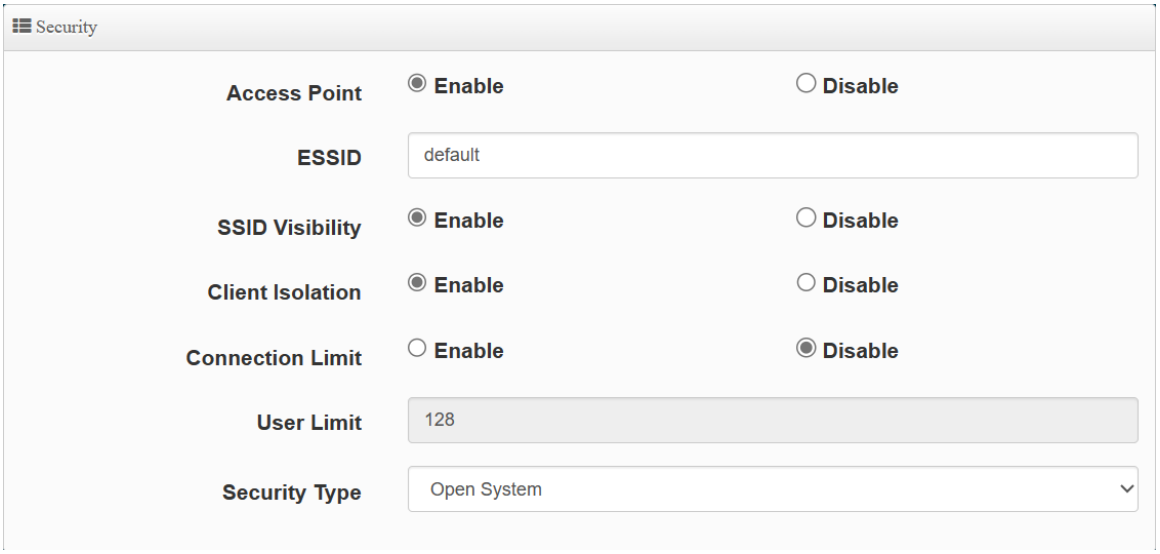


- **AP Station Security Settings**
  - **Enable**：Administrator can choose this profile enable or disable.
  - **Roaming Match**：The roaming SSID acceptance format setting requirements for all bridge AP.
    - **Whole**：Only accept same bridge AP SSID name for wireless automatic connection.
    - **Start with**：The SSID name format with different SSID but the same prefix of the wireless automatic connection bridge AP can be accepted.

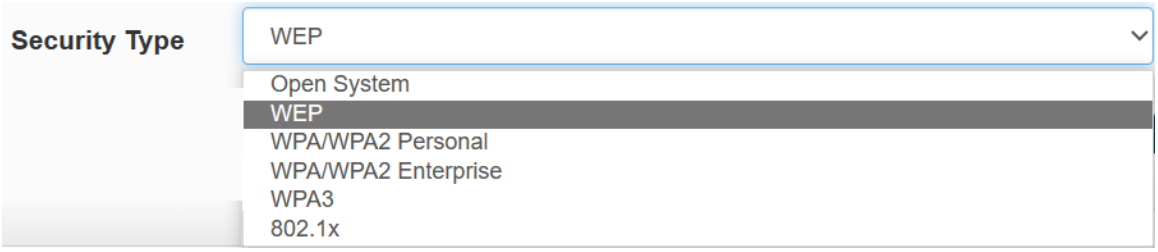
      For example, the SSID names of all bridging base stations along the line may be station 1, station 2 or station3 and other SSID format names for different station divisions.
  - **SSID**：Administrator can set Wi-Fi SSID name
  - **Security Type**：Administrator can select the encryption information corresponding to the bridge AP connection.
  - **Comment**：Administrator can be marked for each of profiles individual notes.

6-5-7. Repeater AP Setup

Administrators can configure ESSID, SSID broadcasting, Maximum number of client associations.

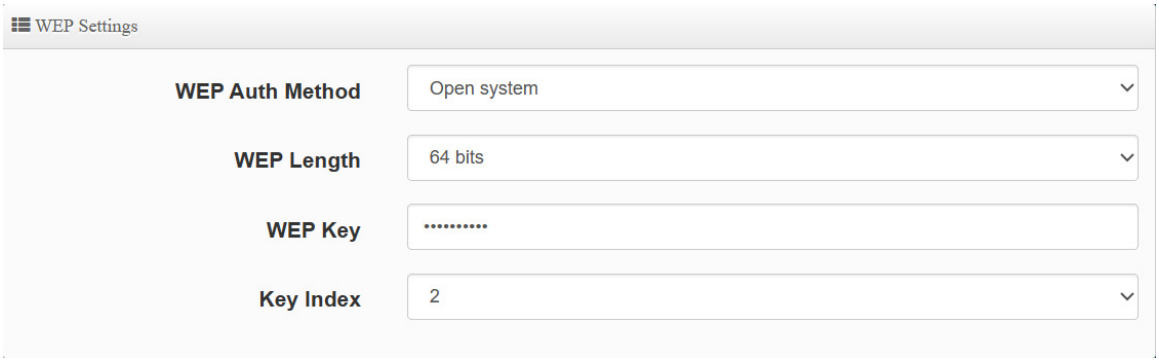


- **Access Point:** Administrator can Enable or Disable the Repeater AP function.
- **ESSID:** Enter the Repeater AP of ESSID name.
- **SSID Visibility:** The default it's Enable**.** When select Disable the SSID will not is discovered.
- **Client Isolation:** This function is Disabled by default. All clients will be isolated from each other, which mean they can't reach each other.
- **Connection Limit:** Administrator can select Enable or Disable WiFi connection Limit
  【Supports 128 users to access at the same time.】
- **Security Type:** Select the desired security type from the drop-down list; the options are Open System, WPA-PSK/WPA2-Personal, WPA/WPA2-Enterprise, WPA3 and 802.1x



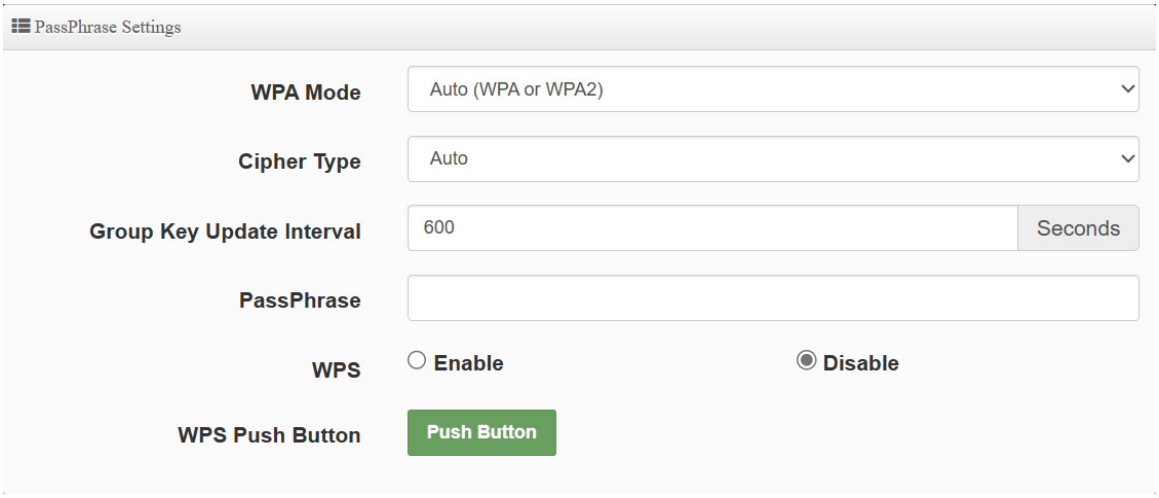
Notice	*Notes: The WEP encryption mode is currently known to be not the most secure wireless encryption method, and will not be able to support 802.11ac/ax. It is not recommended that you continue to use this WEP encryption mode. It is recommended that you use a rate that meets 802.11ac/ax Correspondingly supported encryption modes above WPA / WPA2 to increase your wireless network security.*

- **Open System**：Data is not unencrypted during transmission when this option is selected.**(be not recommended for use)**



- **WEP**：
  - ✓ **WEP Auth Method**：Administrator can choose the WEP Open system open authentication method or the WEP Shared password authentication method.
  - ✓ **WEP Length**：Administrator can choose to use 64bits, 128bits, and 152bits encryption key lengths, but must make sure that the wireless network card used by your wireless client also supports the corresponding wireless key length.
  - ✓ **WEP Key**：There are four groups of optional settings the 16-bit (HEX) key value.
  - ✓ **Key Index**：Administrator can pre-set 4 WEP Key for your WEP and "save".when the future wireless client wants to connect, can be choose which group of wireless keys and establish a connection through WEP encryption.

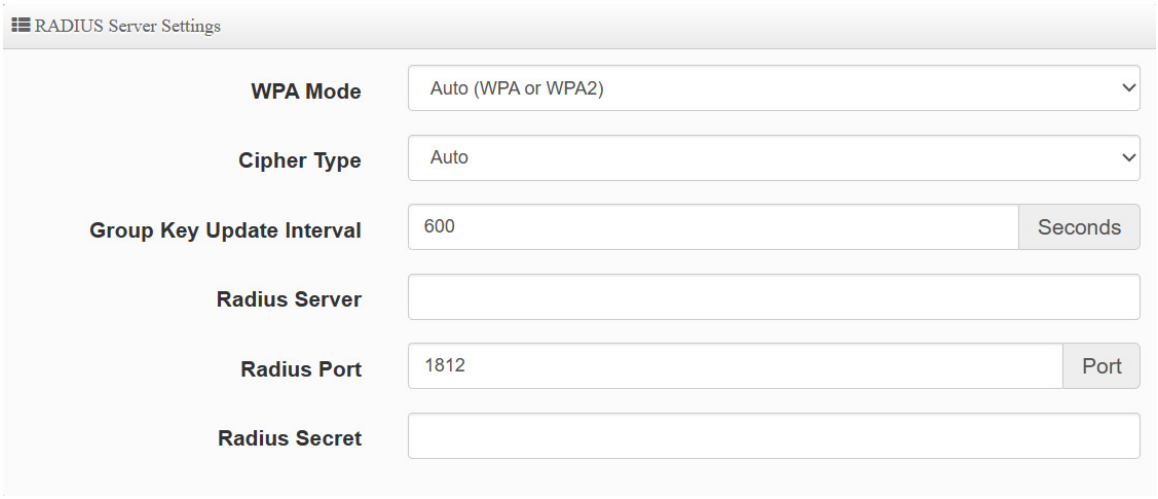
Notice	*Note: If you choose to use WEP encryption mode, please enter the corresponding WEP key value according to the following requirements.* *64bits:* *10 groups of Hexadecimal characters (0~9, A~F and a~f can be used)* *5 groups of ASCII characters (0~9, A~Z and a~z can be used)* *128bits:* *26 groups of Hexadecimal characters (0~9, A~F and a~f can be used)* *13 groups of ASCII characters (0~9, A~Z and a~z can be used)* *152bits:* *32 groups of Hexadecimal characters (0~9, A~F and a~f can be used)* *16 groups of ASCII characters (0~9, A~Z and a~z can be used)*



- **WPA / WPA2-Personal**：
  - ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
  - ✓ **Cipher Type:** Administrator can select use AES or TKIP with 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.

Notice	Note: When setting WEP or TKIP encryption, the data rate will not exceed 54 Mbps. The IEEE 802.11n protocol prohibits the use of high throughput with WEP or TKIP as unicast keys. If you use these encryption methods (such as WEP, WPA-TKIP, WPA2-TKIP), your data rate will be reduced to 54 Mbps, or if it is used for commercial purposes, such as applications where the end user cannot connect to the wireless at a higher speed than 54 Mbps.

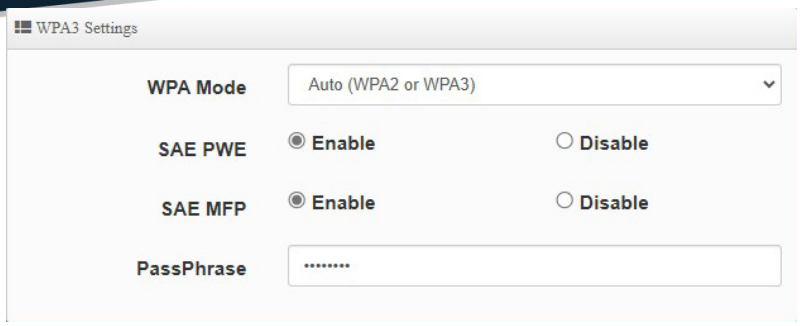
  - ✓ **Group Key Update Interval**: The time interval is for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
  - ✓ **Pass Phrase:** Enter the ESSID pass phrase.
  - ✓ **WPS Push Button:** Administrator can used WPS function to link WiFi client. If enabled, administrator can click the WPS Push Button.



- **WPA / WPA2-Enterprise：**
  - ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
  - ✓ **Cipher Type:** Administrator can select use AES or TKIP with 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.

Notice	Note: When setting WEP or TKIP encryption, the data rate will not exceed 54 Mbps. The IEEE 802.11n protocol prohibits the use of high throughput with WEP or TKIP as unicast keys. If you use these encryption methods (such as WEP, WPA-TKIP, WPA2-TKIP), your data rate will be reduced to 54 Mbps, or if it is used for commercial purposes, such as applications where the end user cannot connect to the wireless at a higher speed than 54 Mbps.

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



- **WPA3 :**

  The 802.11ax peer-to-peer entity authentication mode is different from the Pre-Shared Key .

  ✓ **SAE Password**：When the administrator sets this virtual wireless network SSID to use WPA3 calculation, the SAE connection password must be at least 8 characters.

  ✓ **SAE PWE**：Optionally enable the SAE PWE (Password Element) function, before exchanging SAE authentication messages, both parties will generate a private element PWE (Password Element) and two private values (rand and mask) for advanced authentication exchange.

  ✓ **SAE MFP**：The SAE password authentication mechanism adds a more secure anti-theft, anti-spy, and anti-skimming password Management Frame Protection (MFP).
  If the AP enabled this mode, please ensure that both the AP and the client running in this mode need Management Frame Protection (MFP) support.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

6-5-8. MAC Filter Setup

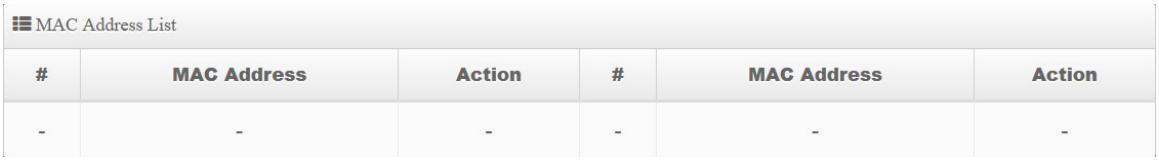
Administrator can setup allow or reject WiFi clients(MAC address) to access Repeater AP.

➢ **Rule:** 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**".

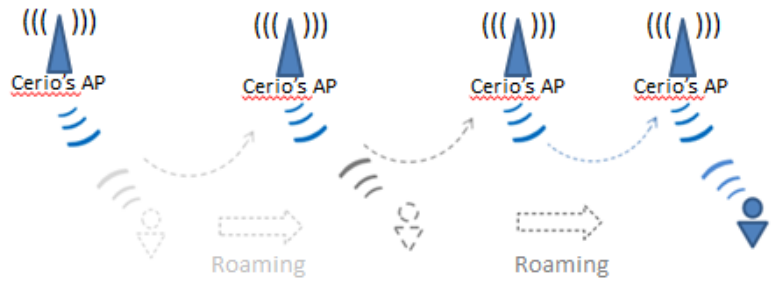
- **MAC Address:** Enter MAC Address for WiFi Clients.

- **MAC Address List:** Display the MAC address of WiFi Clients.

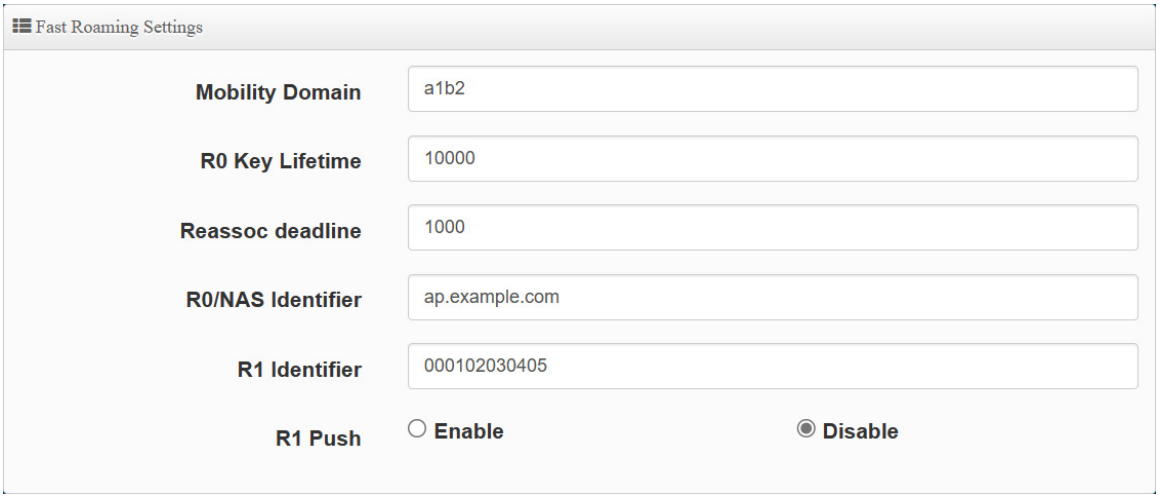


Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

6-5-9. 802.11r Fast Roaming



The Tri band Access Point supports 802.11r/802.11k function for 2.4G (Rado 0)and 5G (Rado 1)and (Rado 2). 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.



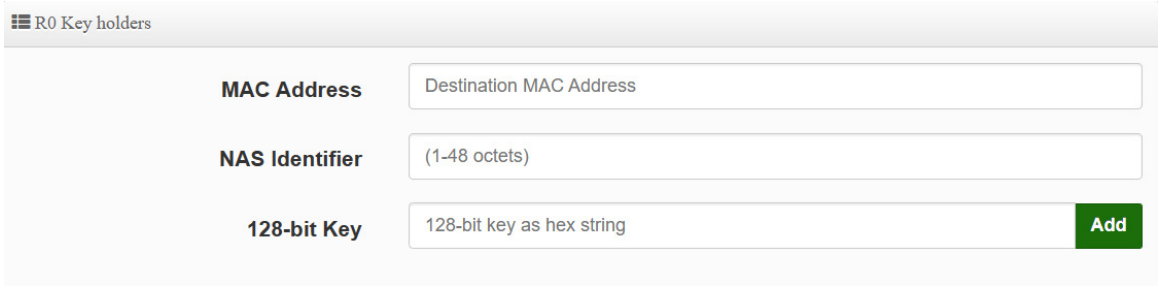
- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition.

Notice	*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 setting 1~65535.
- **Reassoc deadline:** Reassociation deadline in time units (TUs / 1.024 ms; range 1000~65535). The default is 1000.
- **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 or disable. If enable the function will automatically sent the R1 Key.

R0 Key Address:

To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access Points.

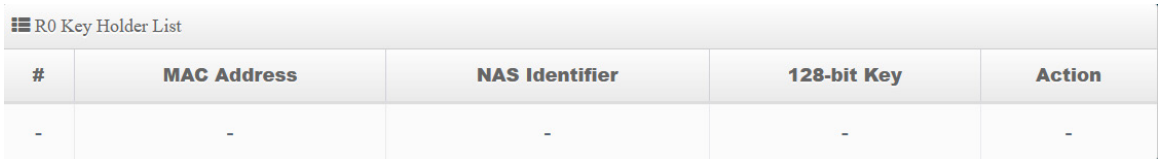


- **MAC Address:** Enter must key in the MAC Address of other AP

- **NAS Identifier:** Enter 1~48 octets of network domain name.
- **128-bit Key:** Enter Shared Key of 128 bit.

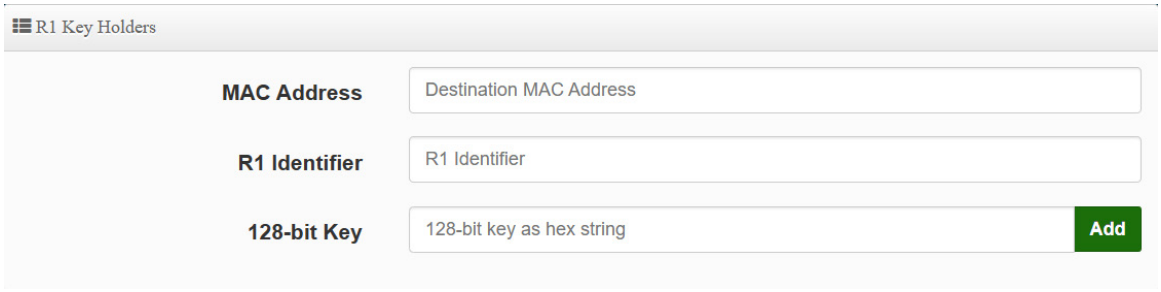
R0 Key Holder List:

After setting "R0 Key holders" function the information will appear in list.



R1 Key Holder List:

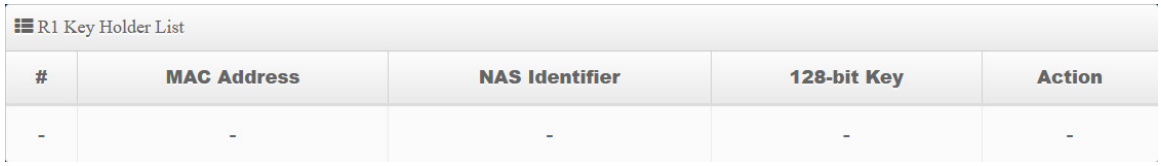
Enter a unified set of R1 Key Holder identification certification.



- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

R1 Key Holder List:

After setting "R1 Key holders" function the information will appear in list.



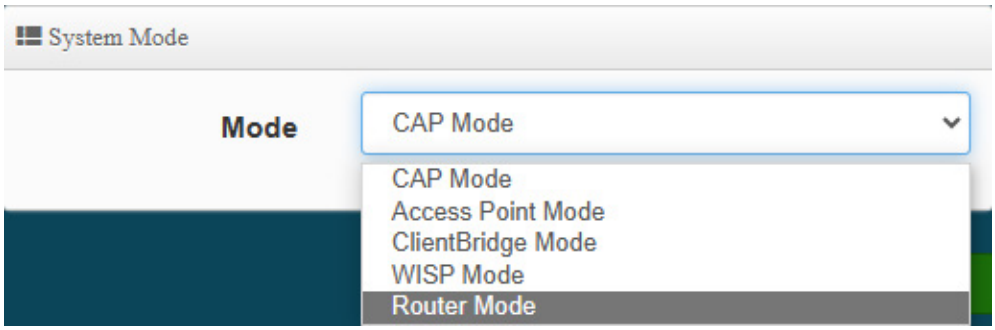
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes

7. Router Mode

7-1. Change Setup Mode

When Router AP mode is chosen, the system can be configured as an Router AP mode. This section provides detailed explanation for users to configure in the Router AP mode with help of illustrations. In the Router AP mode, functions listed in the table below are also available from the Web-based GUI interface.

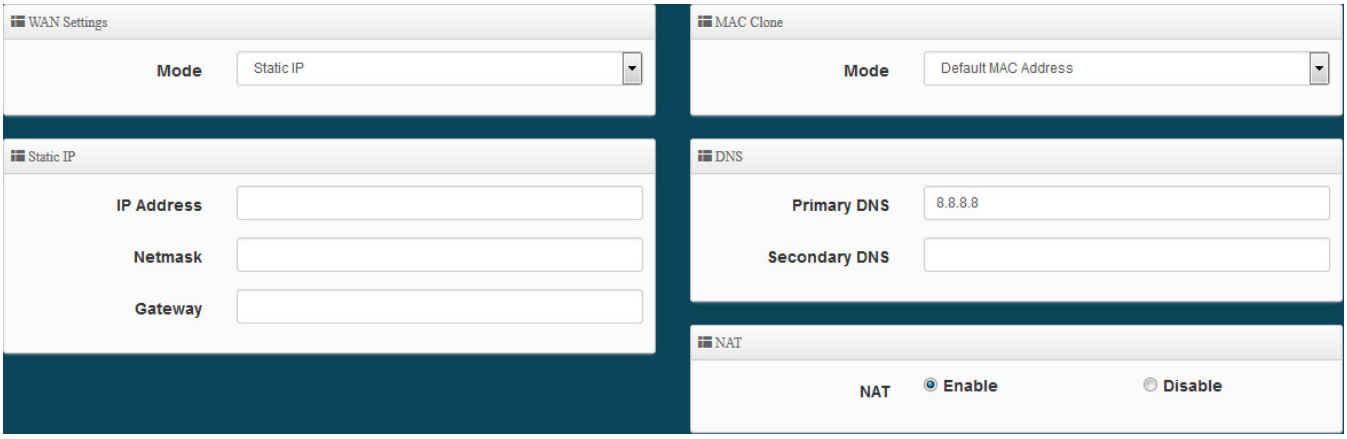
If the administrator needs to switch to Router mode, Please click "System"-> " Mode Setup " to change Router mode.



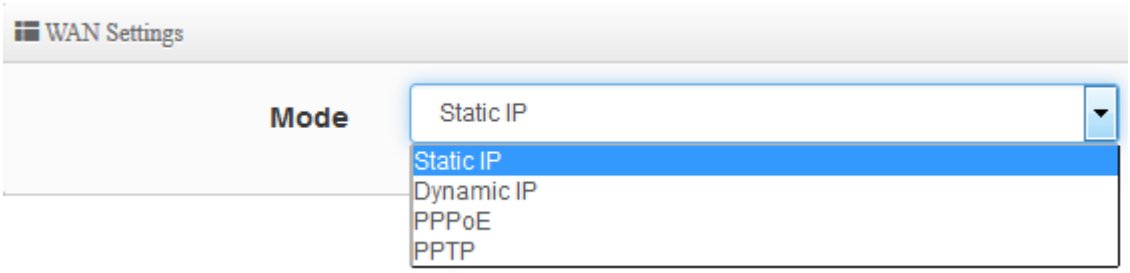
Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

7-2. Configure WAN Setup

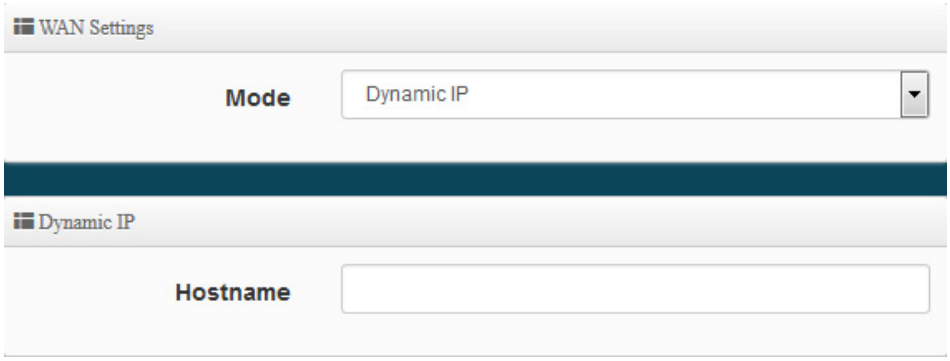
There are four connection types for the WAN port: **Static IP**, **Dynamic IP**, **PPPoE** and **PPTP**. Please click on **System -> WAN** and follow the below setting.



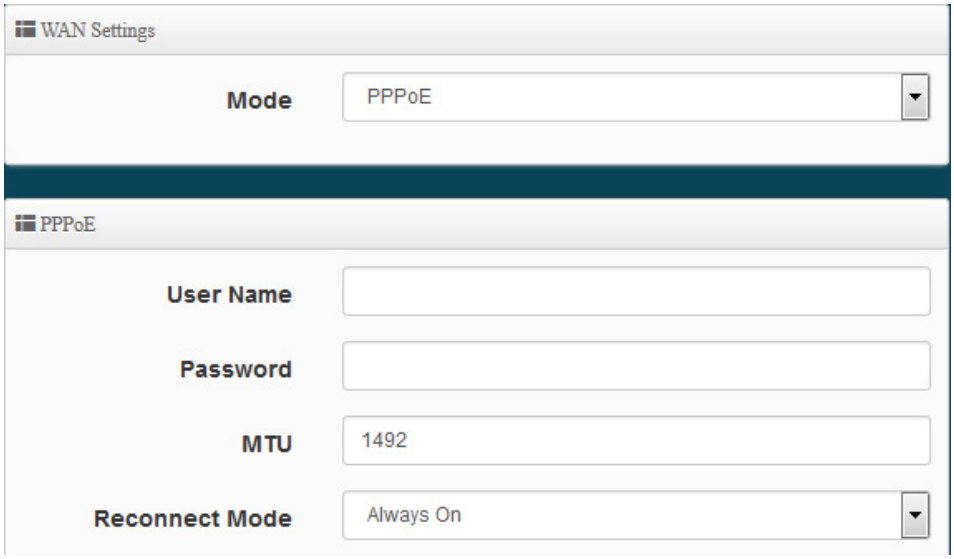
WAN Setting



- **Static IP:** Users can manually setup the WAN IP address with a static IP provided by WISP.
  - **IP Address:** The IP address of the WAN port.
  - **IP Netmask:** The Subnet mask of the WAN port.
  - **IP Gateway:** The default gateway of the WAN port.
- **Dynamic IP:** Please consult with WISP for correct wireless settings to associate with WISP AP before a dynamic IP, along with related IP settings. If IP Address is not assigned, please double check with your wireless settings and ensure successful association. Also, you may go to "**WAN Information**" in the Overview page to click ***Release*** button to release IP address and click ***Renew*** button to renew IP address again.



  - **Hostname :** The Hostname of the WAN port
- **PPPoE:** To create wireless PPPoE WAN connection to a PPPoE server in network.

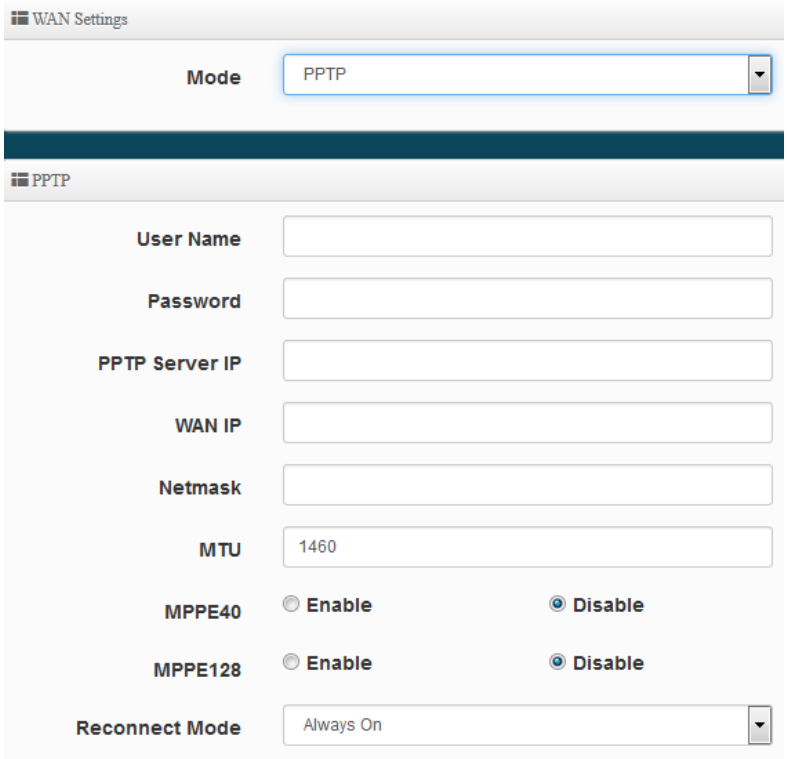


- **User Name :** Enter User Name for PPPoE connection
- **Password :** Enter Password for PPPoE connection
- **MTU:** By default, MTU is set to **1492** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **Reconnect Mode:** Administrator can select three function for Always On / On Demand / Manual.
  - ✓ **Always on** – A connection to Internet is always maintained.
  - ✓ **On Demand** – A connection to Internet is made as needed.

Notice	*When **Time Server** is enabled at the "On Demand" mode, the "Reconnect Mode" will turn out "Always on".*

  - ✓ **Manual** – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.

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



- **User Name:** Enter account for PPTP.
- **Password:** Enter user name account used password for PPTP.
- **PPTP Server IP:** Enter remote IP address of PPTP Server.
- **WAN IP:** The IP address of the WAN port.

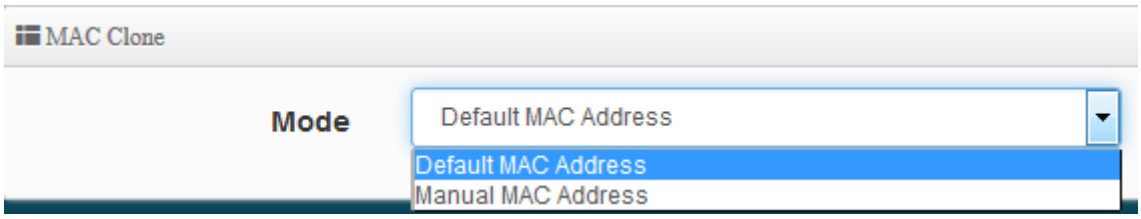
- **Netmask:** The Subnet mask of the WAN port.
- **MTU:** By default, it's **1460** bytes. MTU stands for Maximum Transmission Unit. Consult with WISP for a correct MTU setting.
- **MPPE40/128:** Microsoft Point-to-Point Encryption (MPPE) encrypts data in Point-to-Point Protocol (PPP)-based dial-up 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:** Administrator can select three function for Always On / On Demand / Manual.
  - ✓ **Always on** – A connection to Internet is always maintained.
  - ✓ **On Demand** – A connection to Internet is made as needed.

Notice	*When **Time Server** is enabled at the "On Demand" mode, the "Reconnect Mode" will turn out "Always on".*

  - ✓ **Manual** – Click the "**Connect**" button on "**WAN Information**" in the Overview page to connect to the Internet.

➢ **MAC Clone**

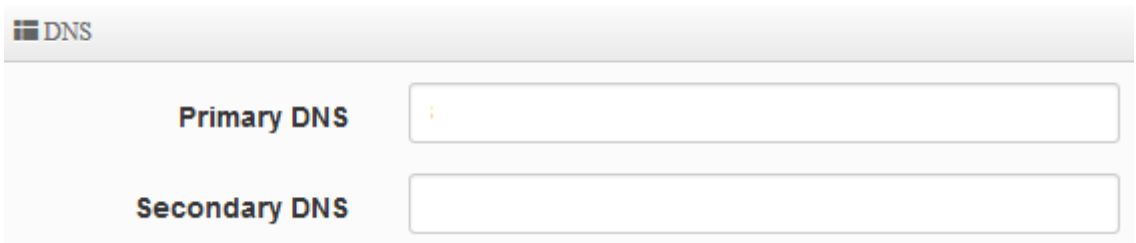
The MAC address is a 12-digit HEX code uniquely assigned to hardware as identification. Some ISPs require you to register a MAC address in order to access to Internet. If not, you could use default MAC or clone MAC from a PC.



- **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.

➢ **DNS**

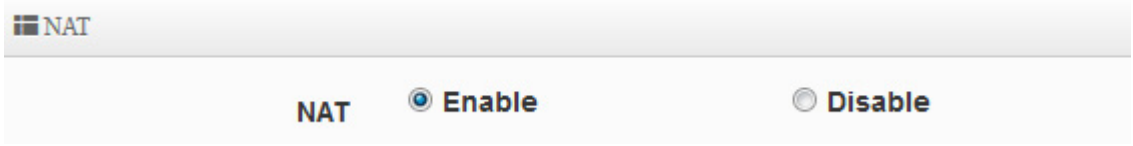
Check "No Default DNS Server" or "Specify DNS Server IP" radial button as desired to set up system DNS.



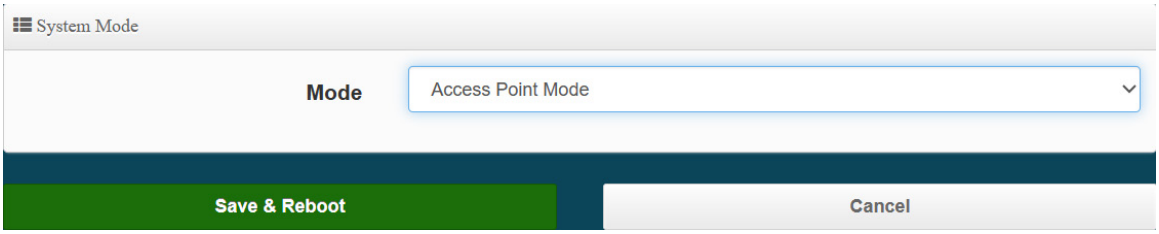
- **Primary DNS:** The IP address of the primary DNS server.
- **Secondary DNS:** The IP address of the secondary DNS server.

➢ **NAT**

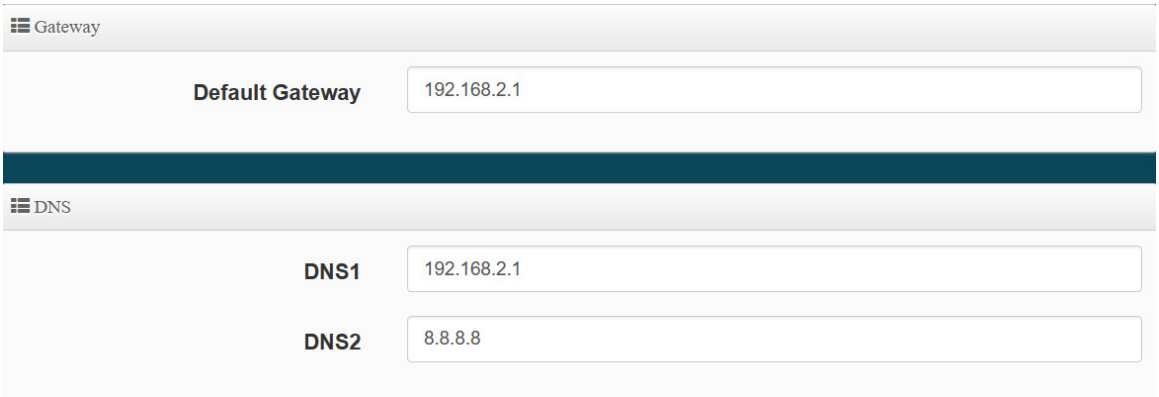
The NAT support Enable and Disable Service



7-3. VLAN Setup



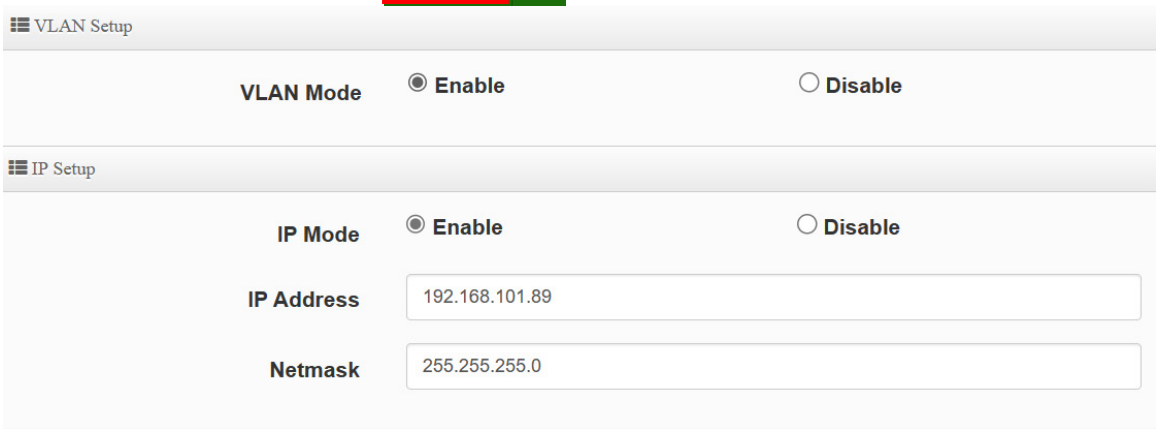
Here are the instructions to setup the local IP Address / Netmask / Gateway / DNS and management Access Point 2.4G or 5G-1 Radio or 5G-2 Radio on/off. Administrators can change settings such as LAN Spanning Tree and Tag VLAN functions.



- **VLAN Mode**：Display on/off for the VLAN network.
- **Flag**：Display master VLAN and VLAN Tag No. information. When displayed Native ETH1 Native ETH2 it means that the current main wired connection is this virtual network as the main login system.
- **IP Address**：Display IP Address for VLAN Network
- **NetMask**：Display IP netmask.
- **Radio 0**：Display radio 2.4G SSID name.
  - Action : Click the Network button to enter the LAN setting page. Click the Network drop-down arrow to display the wireless setting function list.
- **Radio 1**：Display radio 5G-1 SSID name.
  - Action : Click the Network button to enter the LAN setting page. Click the Network drop-down arrow to display the wireless setting function list.
- **Radio 2**：Display radio 5G-2 SSID name.
  - Action : Click the Network button to enter the LAN setting page. Click the Network drop-down arrow to display the wireless setting function list.
- **Default Gateway**：Set the gateway IP address.
- **DNS**：Set the IP address for DNS resolution.

Network Setup

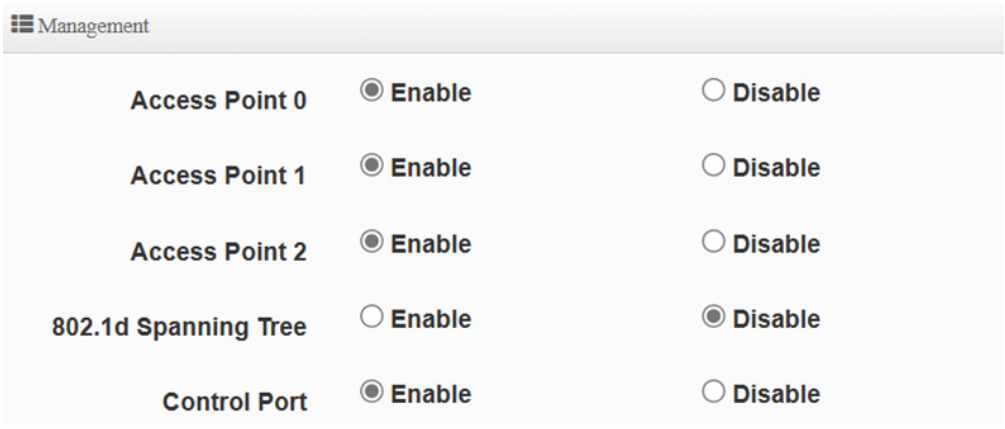
Administrator can click " Network " button to set VLAN network functions.



- **VLAN Mode**：Administrator can select Enable or disable for the VLAN Network.
- **IP Mode**：Administrator can select enable or disable function for VLAN IP.
- **IP Address/ NetMask**：Administrator can set IP address and netmask for the VLAN.

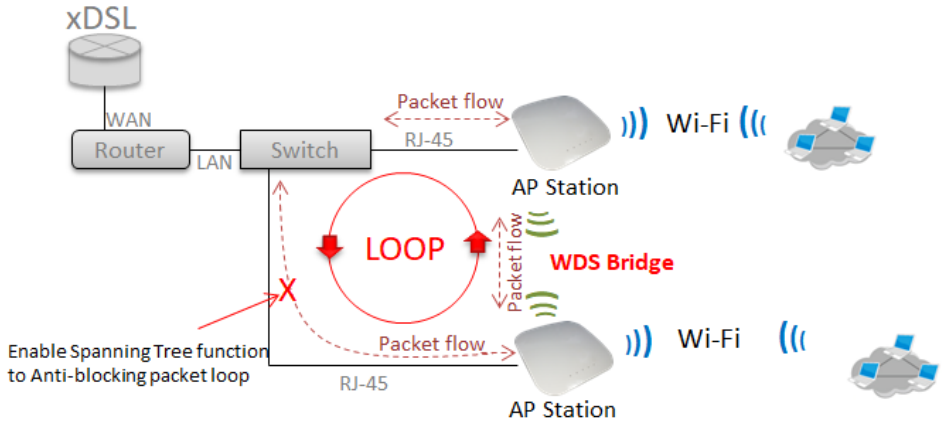
Notice

At least one VLAN will always be enabled by default



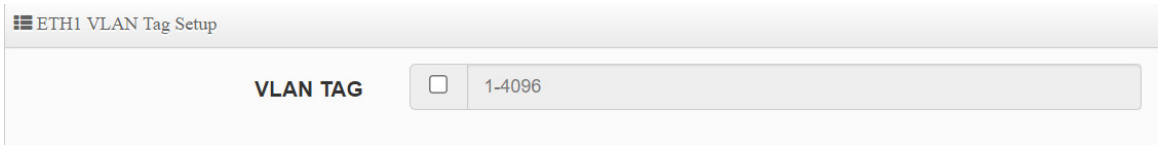
Management

- **Access Point 0**：Administrator can Enable or Disable 2.4G Radio.
- **Access Point 1**：Administrator can Enable or Disable 5G-1 Radio.
- **Access Point 2**：Administrator can Enable or Disable 5G-2 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, which is also referred to as STP, is defined in the IEEE Standard 802.1d



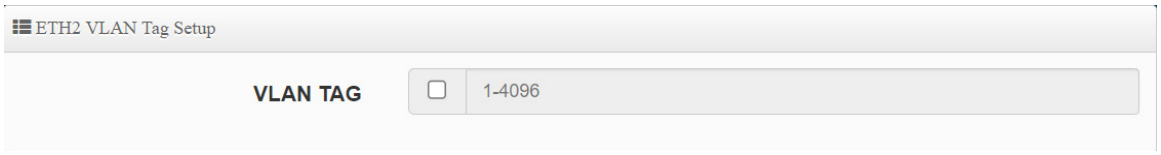
- **Control Port**：Administrator can select one of the VLAN as managed AP.
- **VLAN Tag Setup:** Set the VLAN used tags.

ETH1 VLAN Tag Setup



- **Network port VLAN Tag Setup:** Follow standard 802.1Q specification, the function can be turned off or enabled. You can define the tag to the ETH1 physical network port , which can be set from 1 to 4096.

ETH2 VLAN Tag Setup



- **Network port VLAN Tag Setup:** Follow standard 802.1Q specification, the function can be turned off or enabled. You can define the tag to the ETH2 physical network port , which can be set from 1 to 4096

Notice	Note: If ETH1 is configured to use a VLAN Tag, then entering the management interface requires a VLAN with the same tag to enter the management settings. Domains other than this VLAN will be completely blocked.

Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

Network Pull-down menu

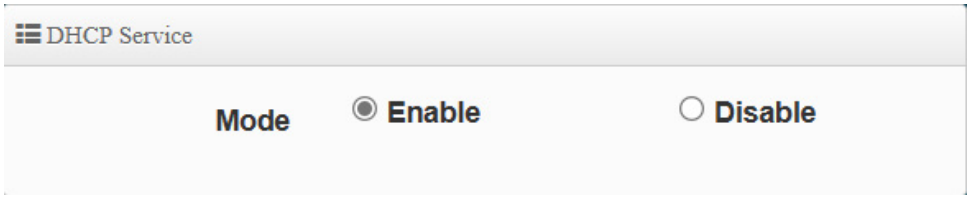
Administrator can set DHCP Server and 2.4/5G security for the access point and set 802.11r fast roaming.

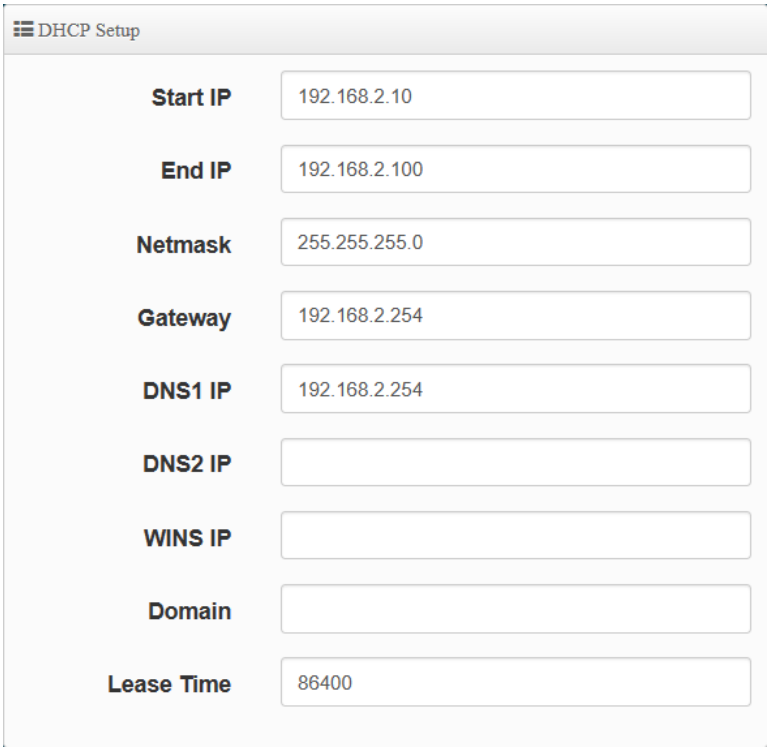
Please click 

pull-down button.

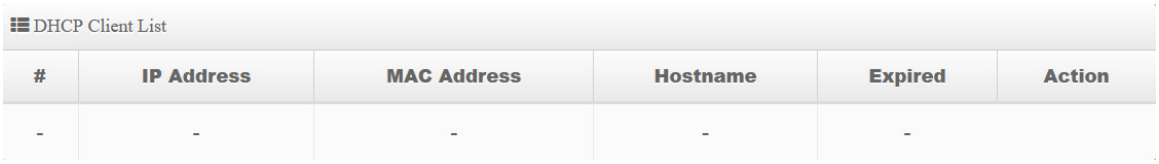
7-3-1 DHCP Server

Administrator can select enable / disable the function



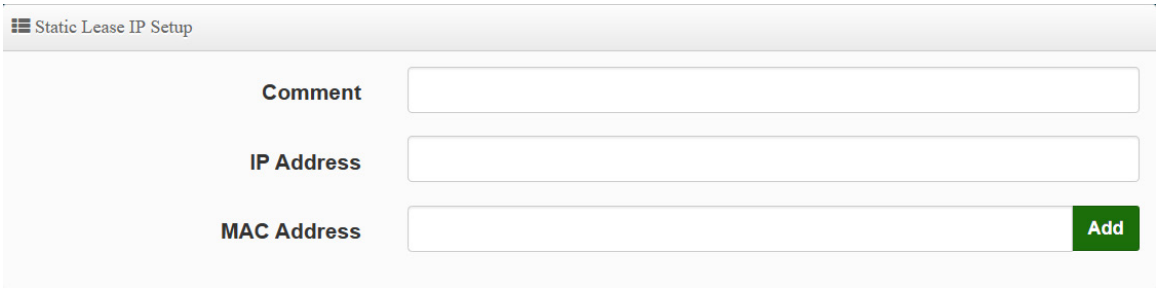


- **Start IP:** Set Start IP address for DHCP Service.
- **End IP:** Set End IP address for DHCP Service.
- **Netmask:** Set IP Netmask, the default is 255.255.255.0
- **Gateway:** Set Gateway IP address for DHCP Service.
- **DNS(1-2) IP :** Set DNS IP address for DHCP Service.
- **WINS IP:** Enter IP 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



➢ **DHCP Client List**

Administrator can view IP address used status of client users on each DHCP Server.

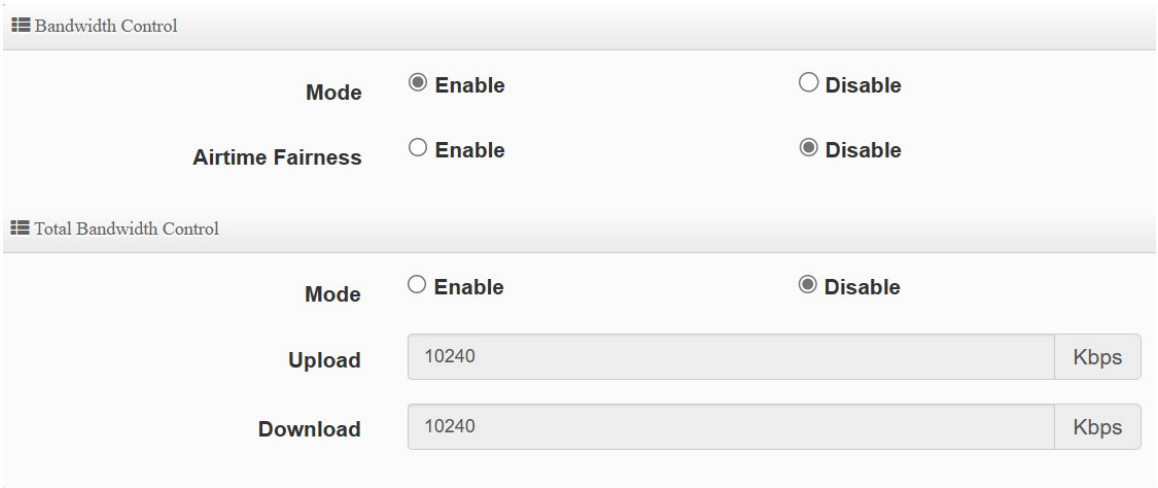


- **Static Lease IP Setup**：Administrator can set be delivered fixed IP address to the users.
  - **Comment:** Enter rule description.
  - **IP Address:** Enter access point IP.
  - **MAC Address:** Enter Client MAC Address of PC network.

Click "**Save"** button to save your changes. Then click **Reboot** button to activate your changes.

7-3-2 Bandwidth Control

Administrators can set bandwidth limit the max/min bandwidth of the Wi-Fi users, Bandwidth control can set IP/MASK , IP Range, Port(Service), SIP, RTP/RTSP and WEB.



- Bandwidth Control / Total Bandwidth Control
  - **Mode:** Administratior can Enable or Disable the function.
  - **Airtime Fairness:** TX/RX traffic balancing, if device use point-to-point (WDS or AP mode + Client Bridge) then recommended to enable it.
  - **Total Bandwidth Control:** Administrator can set total bandwidth used limit in VLAN

QoS RuleList

#	啟動	Rule Mode	Value1	Value2	Upload(Kbps)	Download(Kbps)	註解
1	☐	ANY			1024	1024	
2	☐	ANY			1024	1024	
3	☐	ANY			1024	1024	

- **QoS Rule List:** Administrator can set bandwidth limit by IP/MASK, IP Range, Port(Service), SIP, RTP/RTSP, WEB protocol , each VLAN can set 10 bandwidth management rule.

Click "**Save**" button to save your changes. Then click **Reboot** button to activate your changes.

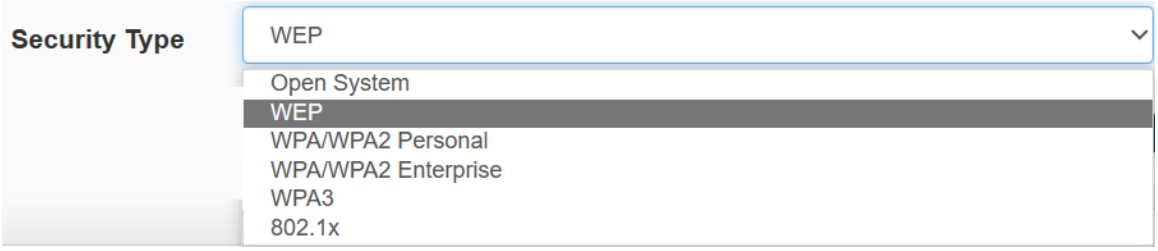
7-3-3 Radio 0(2.4G)/Radio1(5G)/Radio2(5G) Access Point Setup

Administrator can Enable or Disable radio 0/1/2 (2.4/5G/5G) Wi-Fi. If radio 0/1/2 (2.4/5G/5G) are enabled, administrators can set the SSID and security for the 2.4/5G access point.

Security

Access Point	◉ Enable	○ Disable
ESSID	2.4G_or_5G	
SSID Visibility	◉ Enable	○ Disable
Client Isolation	○ Enable	◉ Disable
Connection Limit	○ Enable	◉ Disable
User Limit	128	
Security Type	WEP	

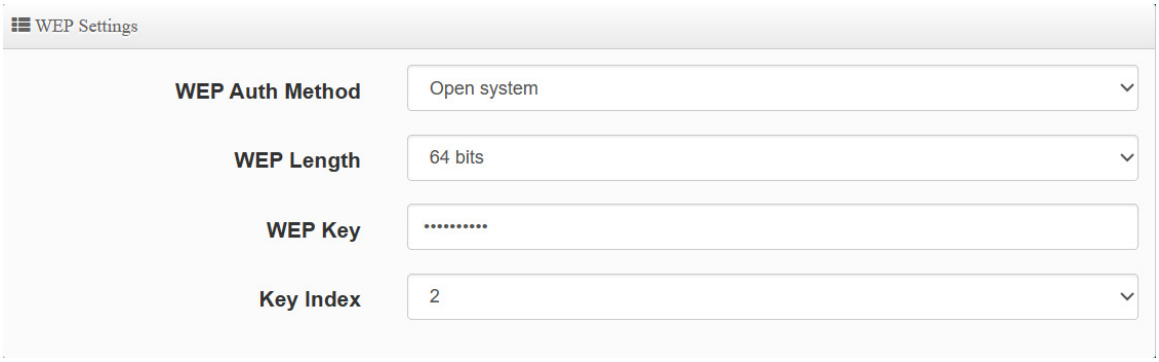
- **Access Point:** Administrator can Enable or Disable the radio 0/1/2 (2.4G/5G/5G).
- **ESSID:** Administrator can set Wi-Fi SSID name
- **SSID Visibility:** Administrator can select Enable or Disable the Visibility.
- **Client Isolation:** Enable or Disable the client isolation function.
- **Connection Limit:** Administrator can select Enable or Disable WiFi connection Limit.
  【Supports 128 users to access at the same time.】
- **Security Type:** Select the desired security type from the drop-down list; the options are Open System, WPA-PSK/WPA2-Personal, WPA/WPA2-Enterprise, WPA3 and 802.1x



Notice

Notes: The WEP encryption mode is currently known to be not the most secure wireless encryption method, and will not be able to support 802.11ac/ax. It is not recommended that you continue to use this WEP encryption mode. It is recommended that you use a rate that meets 802.11ac/ax Correspondingly supported encryption modes above WPA / WPA2 to increase your wireless network security.

- **Open System**：Data is not unencrypted during transmission when this option is selected.**(be not recommended for use)**



- **WEP**：
  - ✓ **WEP Auth Method**：Administrator can choose the WEP Open system open authentication method or the WEP Shared password authentication method.
  - ✓ **WEP Length**：Administrator can choose to use 64bits, 128bits, and 152bits encryption key lengths, but must make sure that the wireless network card used by your wireless client also supports the corresponding wireless key length.
  - ✓ **WEP Key**：There are four groups of optional settings the 16-bit (HEX) key value.
  - ✓ **Key Index**：Administrator can pre-set 4 WEP Key for your WEP and "save".when the future wireless client wants to connect, can be choose which group of wireless keys and establish a connection through WEP encryption.

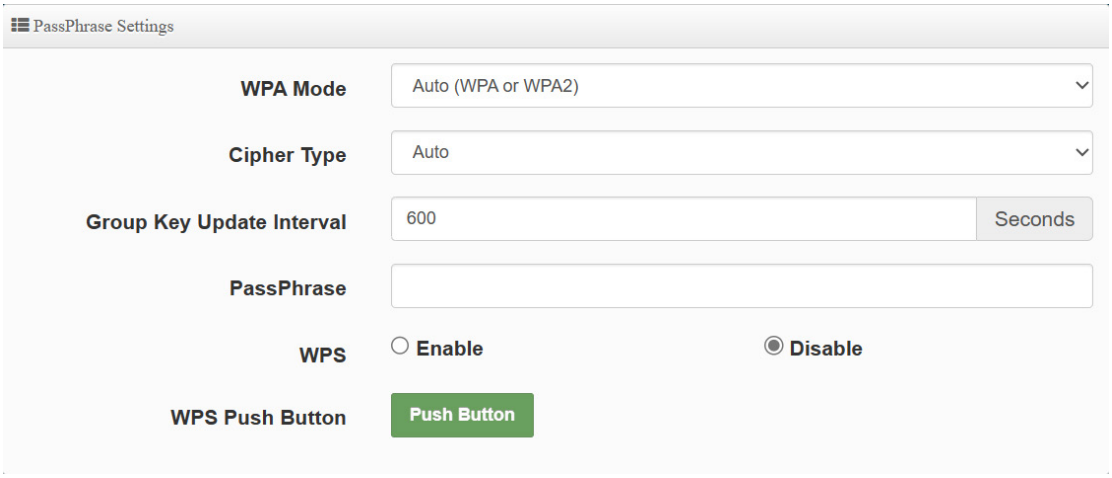
Notice

Note: If you choose to use WEP encryption mode, please enter the corresponding WEP key value according to the following requirements.

64bits:
10 groups of Hexadecimal characters (0~9, A~F and a~f can be used)
5 groups of ASCII characters (0~9, A~Z and a~z can be used)

128bits:
26 groups of Hexadecimal characters (0~9, A~F and a~f can be used)
13 groups of ASCII characters (0~9, A~Z and a~z can be used)

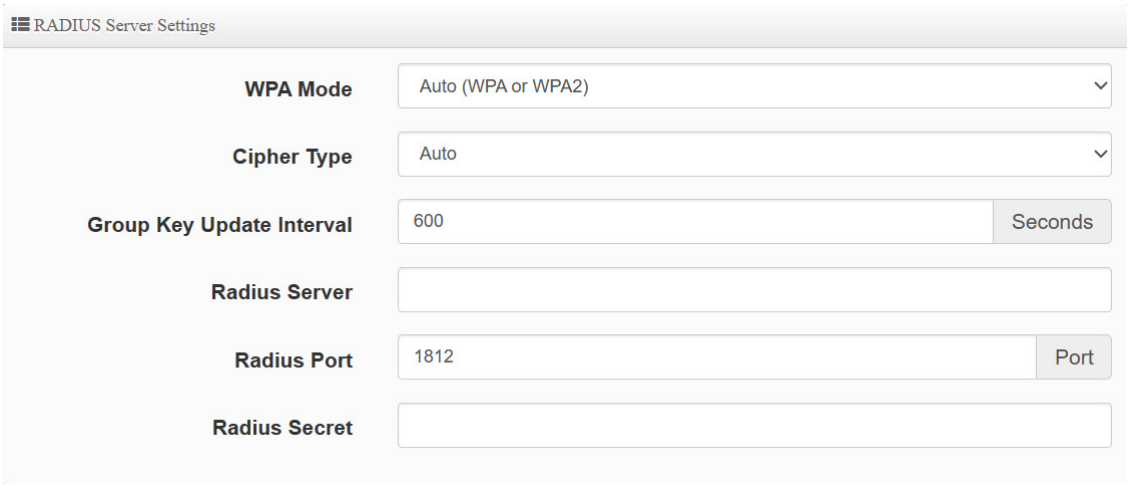
152bits:
32 groups of Hexadecimal characters (0~9, A~F and a~f can be used)
16 groups of ASCII characters (0~9, A~Z and a~z can be used)



- **WPA / WPA2-Personal**：
  - ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
  - ✓ **Cipher Type:** Administrator can select use AES or TKIP with 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.

Notice	Note: When setting WEP or TKIP encryption, the data rate will not exceed 54 Mbps. The IEEE 802.11n protocol prohibits the use of high throughput with WEP or TKIP as unicast keys. If you use these encryption methods (such as WEP, WPA-TKIP, WPA2-TKIP), your data rate will be reduced to 54 Mbps, or if it is used for commercial purposes, such as applications where the end user cannot connect to the wireless at a higher speed than 54 Mbps.

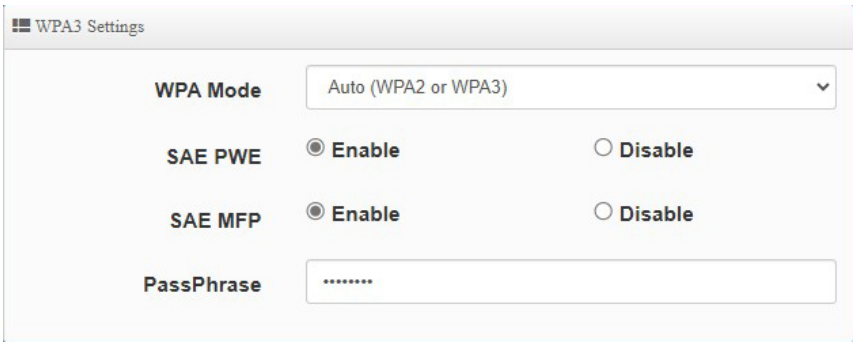
- ✓ **Group Key Update Interval**: The time interval is for re-keying GTK (broadcast/multicast encryption keys) in seconds. Enter the time-length required; the default time is 600 seconds.
- ✓ **Pass Phrase:** Enter the ESSID pass phrase.
- ✓ **WPS Push Button:** Administrator can used WPS function to link WiFi client. If enabled, administrator can click the WPS Push Button.



- **WPA / WPA2-Enterprise**：
  - ✓ **WPA Mode:** Administrator can select security for Auto or only WPA or only WPA2.
  - ✓ **Cipher Type:** Administrator can select use AES or TKIP with 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.

Notice	Note: When setting WEP or TKIP encryption, the data rate will not exceed 54 Mbps. The IEEE 802.11n protocol prohibits the use of high throughput with WEP or TKIP as unicast keys. If you use these encryption methods (such as WEP, WPA-TKIP, WPA2-TKIP), your data rate will be reduced to 54 Mbps, or if it is used for commercial purposes, such as applications where the end user cannot connect to the wireless at a higher speed than 54 Mbps.

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



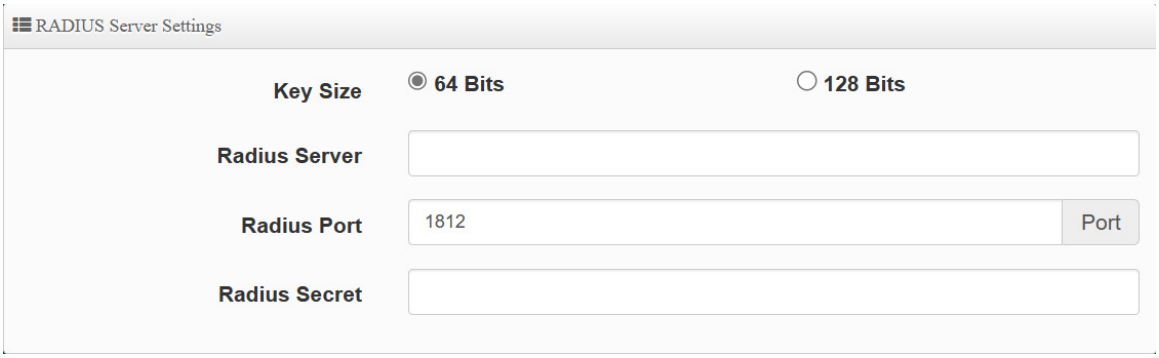
- **WPA3 :**

The 802.11ax peer-to-peer entity authentication mode is different from the Pre-Shared Key .

- ✓ **SAE Password**：When the administrator sets this virtual wireless network SSID to use WPA3 calculation, the SAE connection password must be at least 8 characters.
- ✓ **SAE PWE**：Optionally enable the SAE PWE (Password Element) function, before exchanging SAE authentication messages, both parties will generate a private element PWE (Password Element) and two private values (rand and mask) for advanced authentication exchange.
- ✓ **SAE MFP**：The SAE password authentication mechanism adds a more secure anti-theft, anti-spy, and anti-skimming password Management Frame Protection (MFP).
  If the AP enabled this mode, please ensure that both the AP and the client running in this mode need Management Frame Protection (MFP) support.

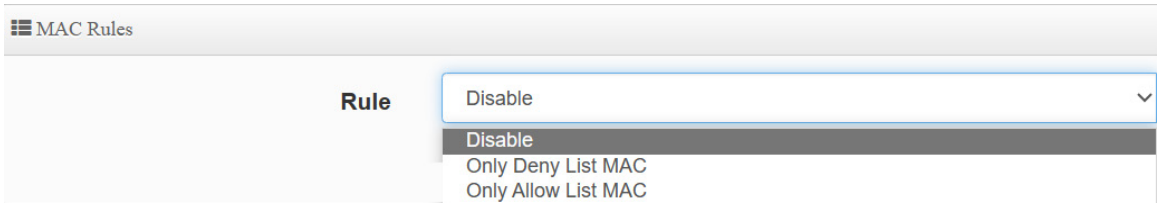
Notice

The WPA3 is latest and most secure protocol currently available for Wi-Fi devices. It is applicable to all access devices that support Wi-Fi 6 (802.11ax). If the wireless access card does not support WPA3 calculation mode, that you adjust the use to WPA2 / AES calculus mode recommended.



- **802.1x**
  - ✓ **Key Size**：Enter the IP address of the Authentication RADIUS server.
  - ✓ **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.

7-3-4 MAC Filter

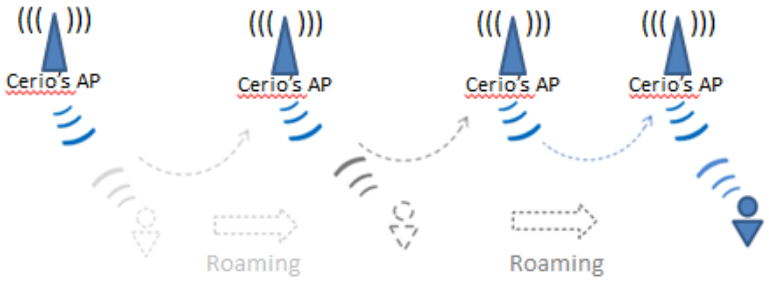


- **Only Deny List MAC**：Administrator can add wireless users MAC address in MAC list. The access point will deny connection in MAC address list.
- **Only Allow List MAC**：Administrator can add wireless users MAC address in MAC list. The access point will allow connection in MAC address list.

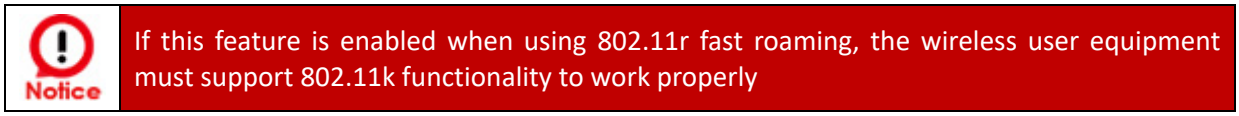
- **MAC Address:** Set managed MAC address of the client.
- **MAC Address List:** Display managed MAC address list.

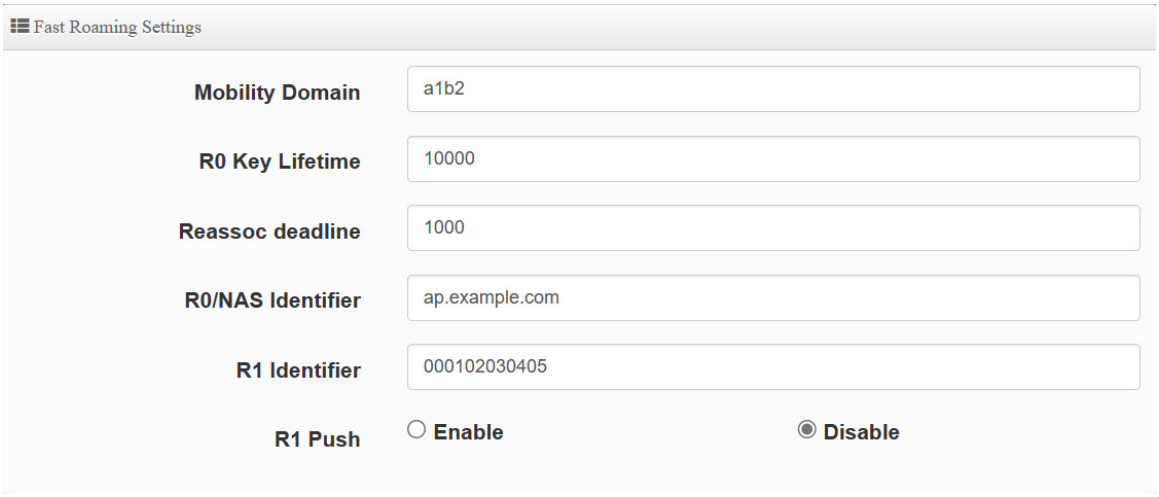
Click **"Save"** button to save your changes. Then click Reboot button to activate your changes.

7-3-5 802.11r Fast Roaming Setup



The Tri band Access Point supports 802.11r/802.11k function for 2.4G (Rado 0)and 5G (Rado 1)and (Rado 2). 802.11r, which is the IEEE standard for fast roaming, introduces a new concept of roaming where the initial handshake with the new AP is done even before the client roams to the target AP.



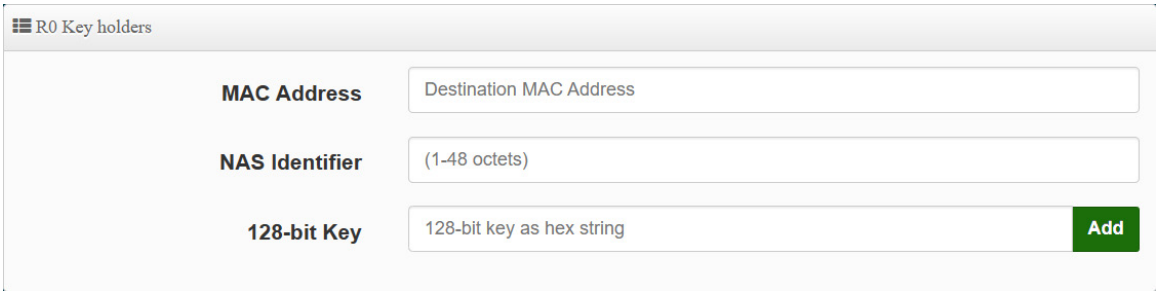


- **Mobility Domain:** MDID is used to indicate a group of APs (within an ESS, i.e., sharing the same SSID) between which a STA can use Fast BSS Transition.

Notice

This setting must be 2-octet of hex string codes. For example, enter 8c4d

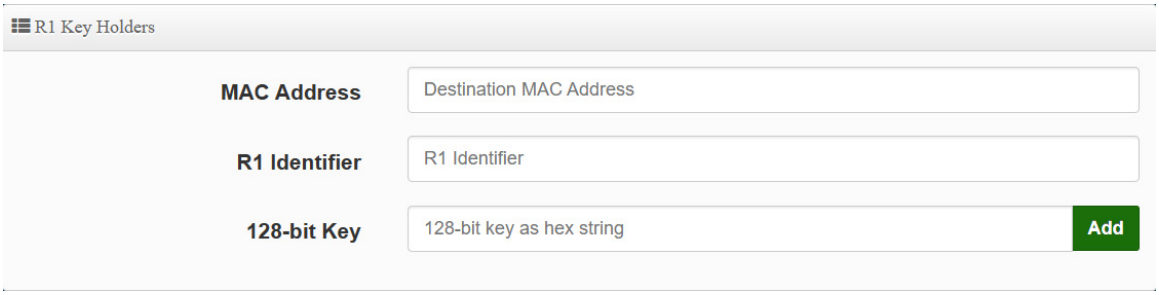
- **R0 Key Lifetime:** Default lifetime of the PMK-RO in minutes, the default is 10000, administrator can setting 1~65535.
- **Reassoc deadline:** Reassociation deadline in time units (TUs / 1.024 ms; range 1000~65535). The default is 1000.
- **R0/NAS Identifier:** PMK-R0 Key Holder identifier. When 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 or disable. If enable the function will automatically sent the R1 Key.



- **R0 Key holders :** To enable roaming between multiple AP devices, AP1 must key in the MAC Address of AP2, and AP2 must key in the MAC Address of AP1. The NAS Identifier and 128-bit Key should be identical in both AP settings. This will enable device roaming between the two Access

Points.

- **MAC Address:** Administrators must enter the MAC Address of another side AP.
- **NAS Identifier:** Enter 1~48 octets of network domain name.
- **128-bit Key:** Enter Shared Key of 128 bit.



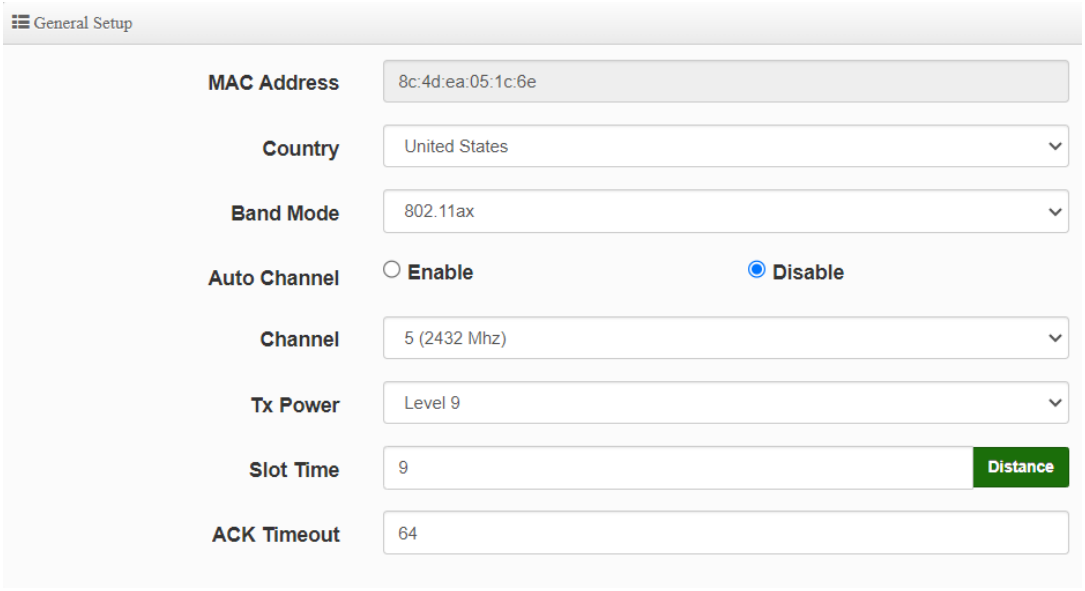
➢ **R1 Key holders :** Enter a unified set of R1 Key Holder identification certification.

- **MAC Address:** Enter the main roaming device MAC address
- **R1 Identifier:** Enter Shared identifier.
- **128-bit Key:** Enter Shared Key of 128 bit.

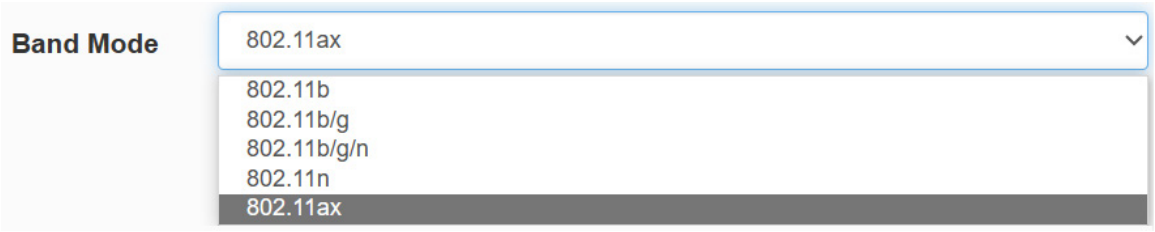
Click **"Save"** button to save your changes. Then click Reboot button to activate your changes.

7-4. Wireless Configuration

7-4-1. Radio 0 (2.4G) Basic Setup



- **General Setup**
  - **MAC Address**：Display 2.4G WiFi MAC address.
  - **Country**：Administrator can select country: US or EU or Japan or Taiwan.
  - **Band Mode**：Administrator can select 2.4G Band for 802.11b、802.11b/g、802.11b/g/n、802.11n. or 802.11ax, The default is 802.11ax



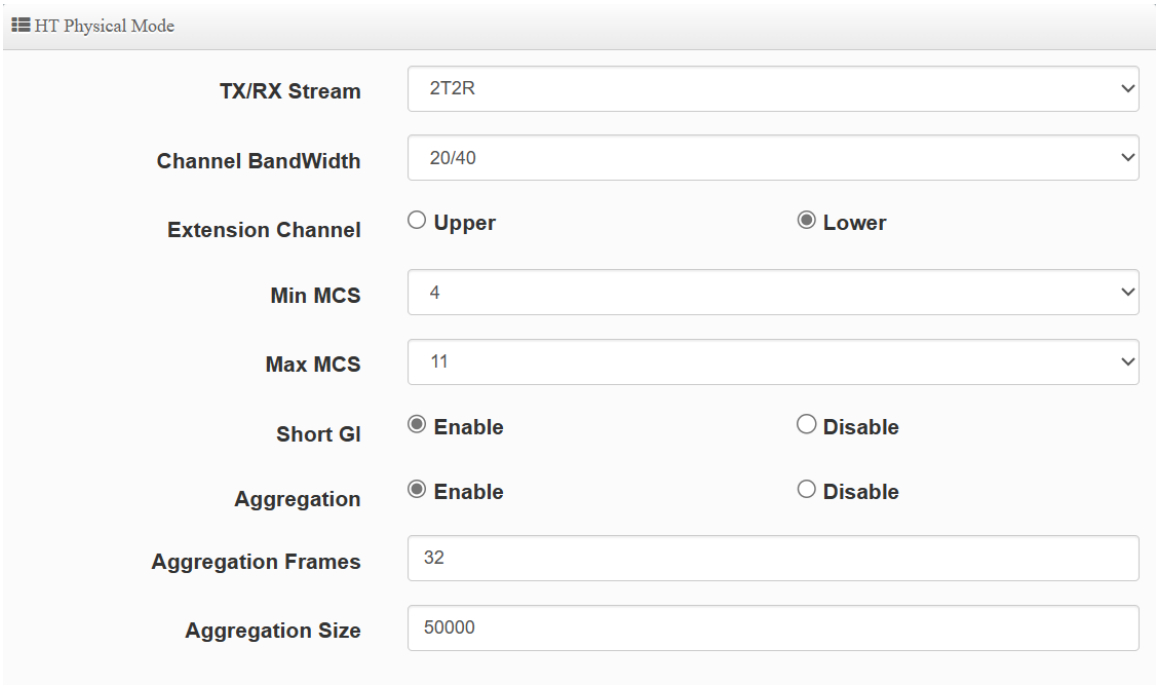
- **Auto Channel**：Administrator can Enable or Disable the function. If disabled, the WiFi channel will be fixed to the manually selected channel.
- **Channel**：There are different options for wireless operation modes in regions, which can be used for Upper or Lower extension.
- **Tx Power**：Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow

  Distance : When the Distance button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).

- **ACK timeout**：When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice	Setting ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

HP Physical Mode



- **TX/RX Stream**：The CenOS 5.0 AP support 2TX/2RX streams. Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

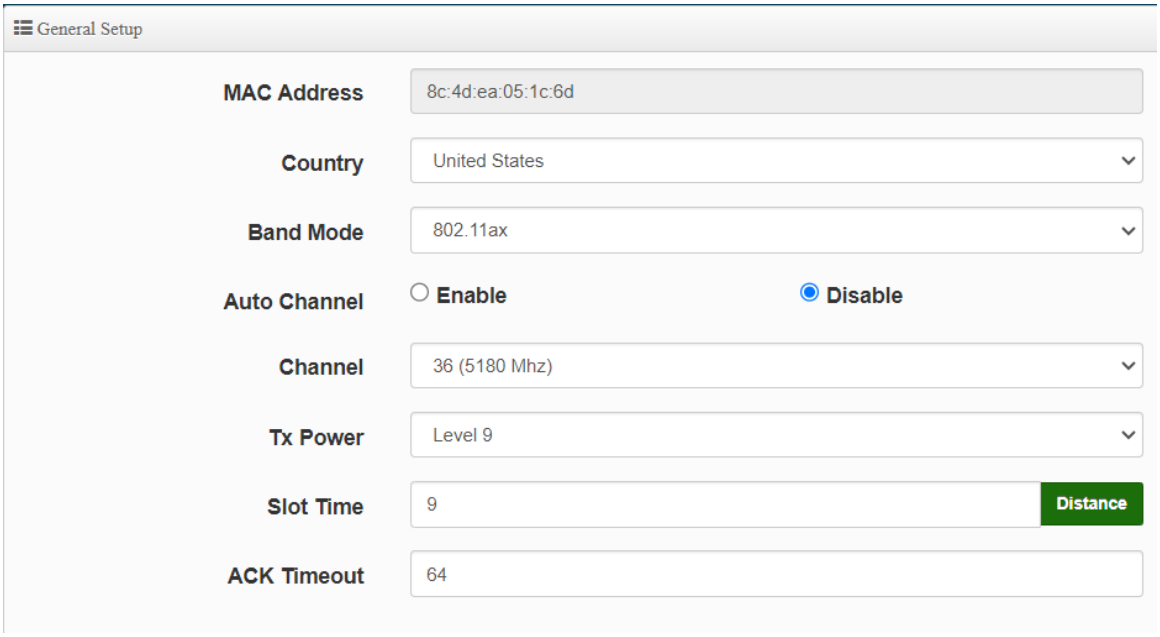
Notice	The 2.4Ghz antenna of this product thinks that it has a built-in 2x2. The default is already set to 2T2R. If there is no special requirement, please keep the setting.

- **Channel Bandwidth**：The "**20/40**" MHz option is usually best. The other option is available for special circumstances.
- **Extension Channel**：Sets channel select to Upper or Lower. The Upper supports 1 to 7 range CH and Lower supports 5 to 11 range CH.
- **MIN MCS:** MCS compilation is a representation proposed by 802.11ax on the communication rate of WLAN.The MCS coding value will affect the main factor of the communication rate and

corresponds to the channel bandwidth.

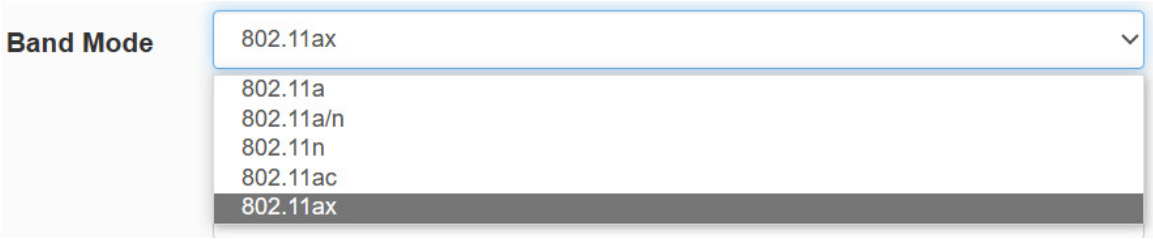
- **MAX MCS:** Maximum MCS compile set value. The Max MCS value must be greater than the Min MCS value.
- **Short GI**：Short Guard Interval is “Enabled” by default to increase throughput. However, it can also increase error rate in some installations, due to increased sensitivity to radio-frequency reflections. Select the option that works best for your installation.
- **Aggregation:** By default, it's “**Enabled**”. Select “Disable” to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard), 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:** Set frames size of Aggregation.
- **Aggregation Size:** Set aggregation size.

7-4-2. Radio 1 (5G-1) / Radio 2 (5G-2)Basic Setup



- **General Setup**

- **MAC Address:** Display 5G-1(Radio 1) / 5G-2(Radio 2) WiFi MAC address.
- **Country:** Administrator can select country: US or EU or Japan or Taiwan.
- **Band Mode:** Administrator can select 5G Band for 802.11a、802.11a/n、802.11n、802.11ac. or 802.11ax, The default is 802.11ax

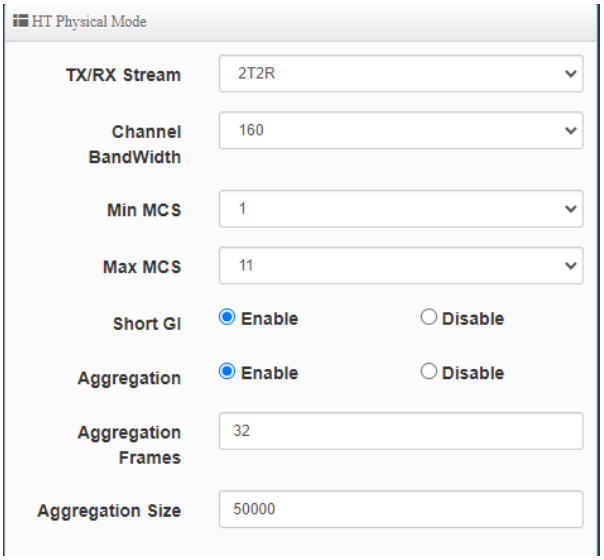


- **Auto Channel:** Administrator can Enable or Disable the function. If select disabled function the WiFi channel can be manually fixed.
- **Channel**：There are different options for wireless operation modes in regions.
- **Tx Power:** Administrator can control the WiFi Tx output power. The power Max. Level 9.
- **Slot Timout :** You can enter the slot time value here. When the distance is long or short, the waiting time for packet transmission will be adjusted fast and slow

  Distance : When the Distance button is clicked, the point-to-point bridge distance can be entered. The system will automatically calculate the ideal reference value for the Slot Time and ACK Timeout. The input distance is calculated in units (meters).
- **ACK timeout**：When waiting for the "ACKnowledgment frame" interval is too long to be received, the ACK will be retransmitted. A higher ACK Timeout will reduce packet loss, but the transmission efficiency will be poor.

Notice	Setting ACK Timeout can strengthen the long-distance connection. Changing the value can optimize the setting. If the value is too low, the length transmission will be reduced. If the value is too high, there may be disconnection.

- **HP Physical Mode**



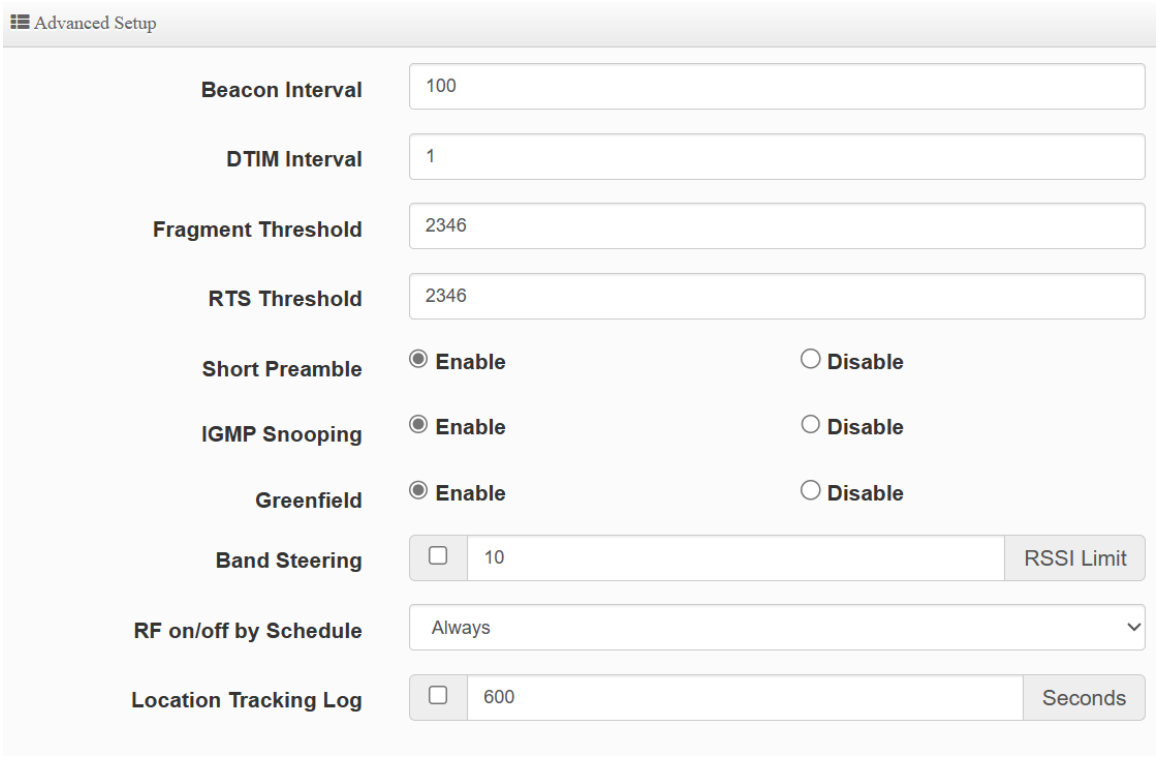
- **TX/RX Stream:** Administrator can select 1 or 2 TX/RX. The default is 2TX/2RX.

Notice	The 5Ghz antenna of this product thinks that it has a built-in 2x2. The default is already set to 2T2R. If there is no special requirement, please keep the setting.

- **Channel BandWith:** The Wireless 5G can choose 20 or 20/40 Mhz or 11ac/ax 80Mhz at 5G-1 (Radio-1) or 11ax 160Mhz at 5G-2 (Radio) as the data transmission speed between the base station and wireless users.
- **MIN MCS:** MCS compilation is a representation proposed by 802.11ax on the communication rate of WLAN.The MCS coding value will affect the main factor of the communication rate and corresponds to the channel bandwidth.
- **MAX MCS:** Maximum MCS compile set value. The Max MCS value must be greater than the Min MCS value.
- **Shout GI:** Short Guard Interval is “Enabled” by default to increase throughput. 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 “**Enabled**”. Select “Disable” to deactivate Aggregation.
  A part of the 802.11n standard (or draft-standard), 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:** Set frames size of Aggregation, the size recommend use default value is 32.
- **Aggregation Size:** Set aggregation size, the size recommends use default value is 500000.

Click **“Save”** button to save your set function. Then click “Reboot” button to activate your changes.

7-4-3. Advanced Setup



- **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 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.

- **Fragmentation Threshold:** Fragmentation Threshold is one more parameter which is given in all stations and Access points. Fine tuning Fragmentation Threshold parameter can result in good throughput but not using it properly can results in low throughput. In simple words it does the same thing which MTU do in Ethernet. Both are different parameters but the work done is same, it fragments the data packets.

  Fragmentation threshold will be used when we have more data packet size to be transmitted and we have less fragment threshold value. Let's say from Ethernet we have to send 1400 byte packet but the fragmentation threshold is set as 400. In this case when the packet is to be transmitted on air it will fragment the packet in to 4 small packet 400+400+400+200 and send on air. This includes MAC header+ frame body and CRC so 400 byte will be in total including headers. This helps in increasing the throughput. The default is 2346.
- **RTS Threshold:** TRTS 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, this function is "***Enabled***". ***Disabling*** will automatically use the 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.
- **Band Steering(5G Priority)**：When 2.4GHz and 5GHz networks exist at the same time, the 5GHz

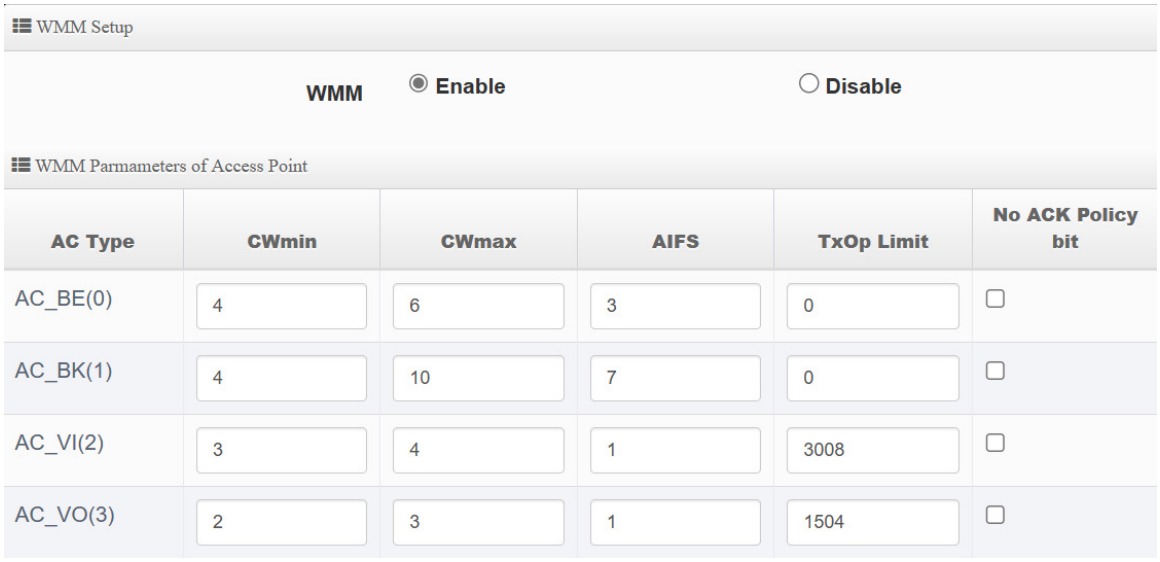
client connection is automatically connected to the 5GHz network as the main connection to improve performance.

- **RF on/off by schedule:** Administrator can apply Time Policy to on or off wireless signal.
- **Location Tracking Log: T**he system can detect the signal strength of the wireless client to determine the location of the Access Point and send to database.

7-4-4. WMM Setup

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.
Please click on **Wireless -> WMM Setup**



- **AC Type**：

Queue	Data Transmitted AP to Clients	Priority	Description
AC_BK	Background	Low	High throughput. Bulk data that requires maximum throughput and is not time-sensitive is sent to this queue (FTP data, for example).
AC_BE	Best Effort	Medium	Medium throughput and delay. Most traditional IP data is sent to this queue.
AC_VI	Video	High	Minimum delay. Time-sensitive video data is automatically sent to this queue.
AC_VO	Voice	High	Time-sensitive data like VoIP and streaming media are automatically sent to this queue.

- **CWmin**: Minimum Contention Window. This parameter is input to the algorithm that 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.

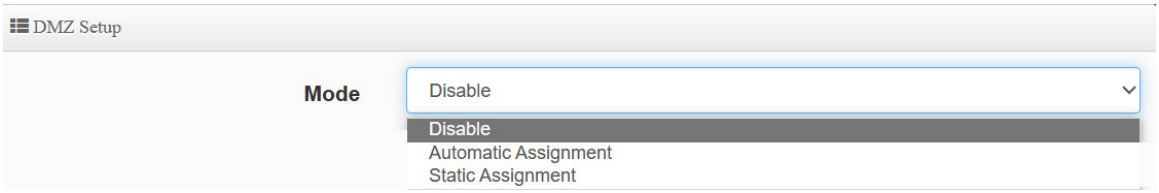
When the Normal ACK policy is used, the recipient acknowledges each received uncast packet.

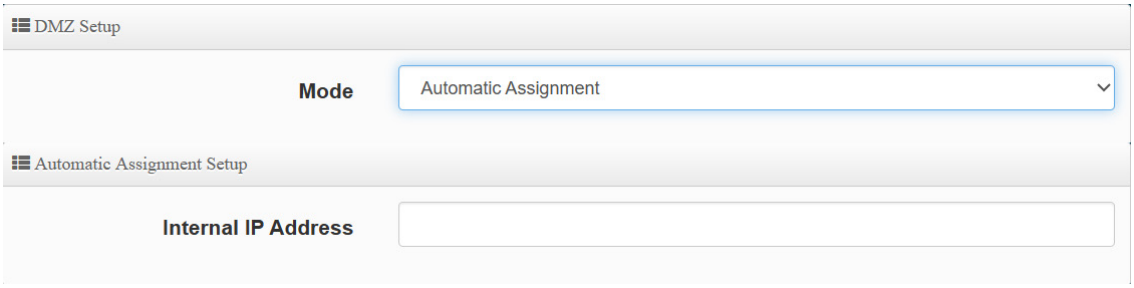
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

8. Advanced Setup (Available in WISP mode and Router Mode)

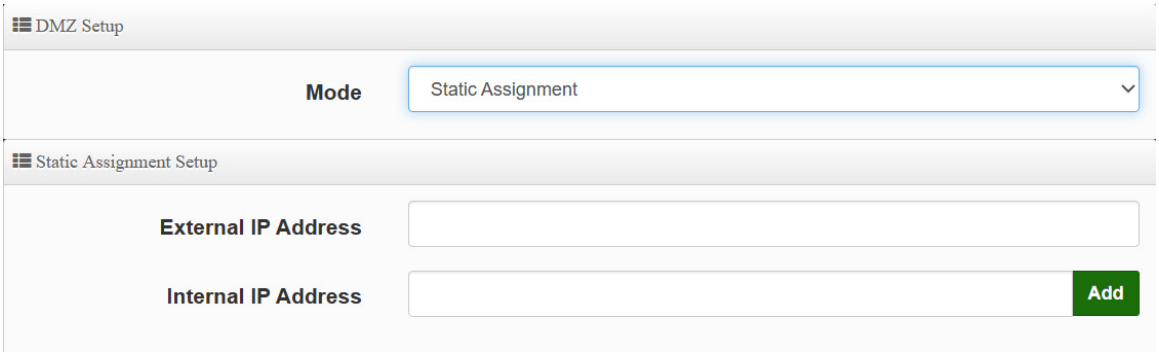
8-1. DMZ

DMZ is commonly work with the NAT functionality as an alternative of Virtual Server(Port Forwarding) while wanting all ports of DMZ host visible to Internet users. Virtual Server rules have precedence over the DMZ rule. In order to use a range of ports available to access to different internal hosts Virtual Server rules are needed.





- **Automatic Assignment:** Enter Internal IP address of DMZ host and only one DMZ host is supported.
  - **Internal IP Address:** Enter Virtual IP for service device.



- **Static Assignment:** Enter external and internal IP address of DMZ host. The function only external IP to Internal IP address
  - **External IP Address:** Enter external IP address
  - **Internal IP Address:** Enter Virtual IP for service device.

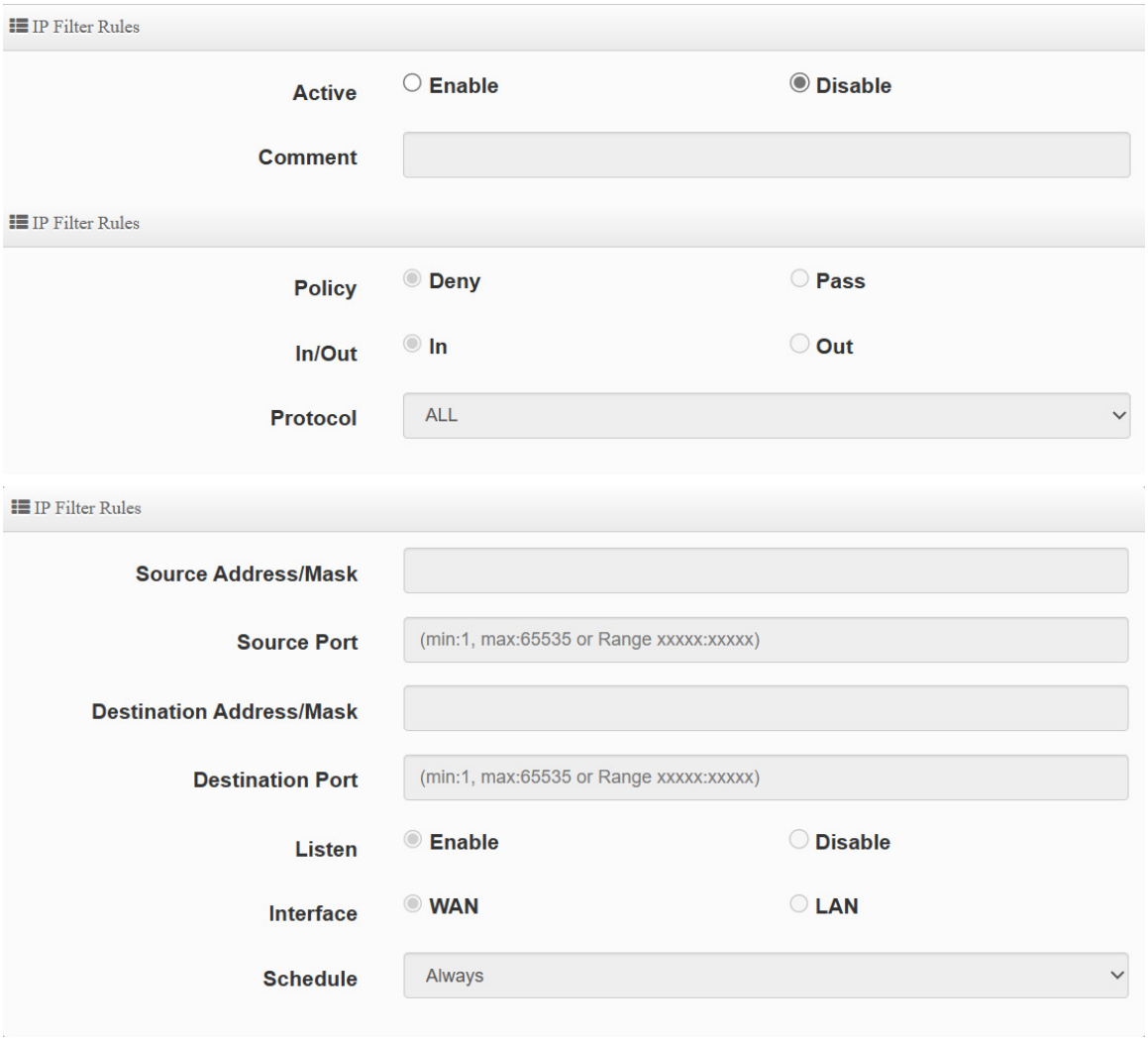
8-2. IP Filter

Can allow or deny 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. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List.

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

Please click **Edit** button to setting IP filter.



- **Active:** Administrator can select Enable or Disable the service.
- **Comment:** Enter the description of IP filter rule.
- **Policy:** Administrator can select the IP flow rule of Deny or Pass.
- **In/ Out:** Administrator can select the IP flow rule of In/out bound.
- **Protocol:** Set used service Port of **TCP**, **UDP** or **ICMP**.
- **Source Address/Mask:** Enter desired source IP address and netmask. i.e. 192.168.2.10/32 or 192.168.2.10/255.255.255.0
- **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 or 192.168.2.10/255.255.255.0
- **Destination Port:** Enter a port or a range of ports as **start:end.** i.e. port 20:80
- **Listen:** Select Enable 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.

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. So, if you just want one IP address to access the system via telnet from your subnet, not others, the Example 1 demonstrates it, not rules in the Example 2.

Example 1:

Create a higher priority rule to allow IP address 192.168.2.2 Telnet access from LAN port first, and deny Telnet access from remaining IP addresses in the same subnet.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Deny	LAN

Example 2:

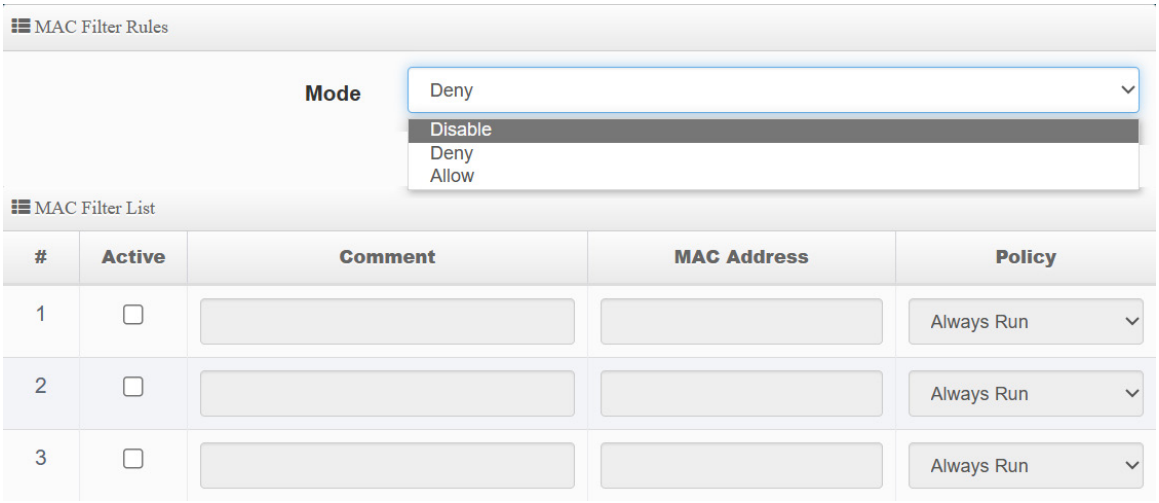
All Telnet access to the system from the IP addresses of subnet 192.168.2.x works with the rule 1 of Example 2. The rule 2 won't make any difference.

Rule	Source		Destination		In/Out	Protocol	Listen	Action	Side
	IP/Mask	Port	IP/Mask	Port					
1	192.168.2.0/24		192.168.2.254/32	22	In	TCP	n	Pass	LAN
2	192.168.2.2/32		192.168.2.254/32	22	In	TCP	n	Deny	LAN

Click "**Save**" button to add IP filter rule. Total of **20** rules maximum allowed in the IP Filter List. All rules can be edited or removed from the List. Click ***Reboot*** button to activate your changes.

8-3. MAC Filter

Allows creating MAC filter rules to allow or deny unicast or multicast packets from limited number of MAC addresses. Important and must note. That MAC filter rules have precedence over IP Filter rules.



- **Mode:** Administrator can select Deny or Allow.
  - **Deny:** The MAC Filter List will be **denied** to access (LAN to WAN). Others will be allowed.
  - **Allow:** The MAC Filter List will be **allowed** to access (LAN to WAN). Others will be denied.
- **Comment:** Enter the description of MAC filter rule.
- **MAC Address:** Enter MAC address (e.g. aa:bb:cc:00:00:0a) and click "**Add**" button, then the MAC address should display in the MAC Filter List.
- **Policy:** Administrator can select to use rule by **"Time Policy".**

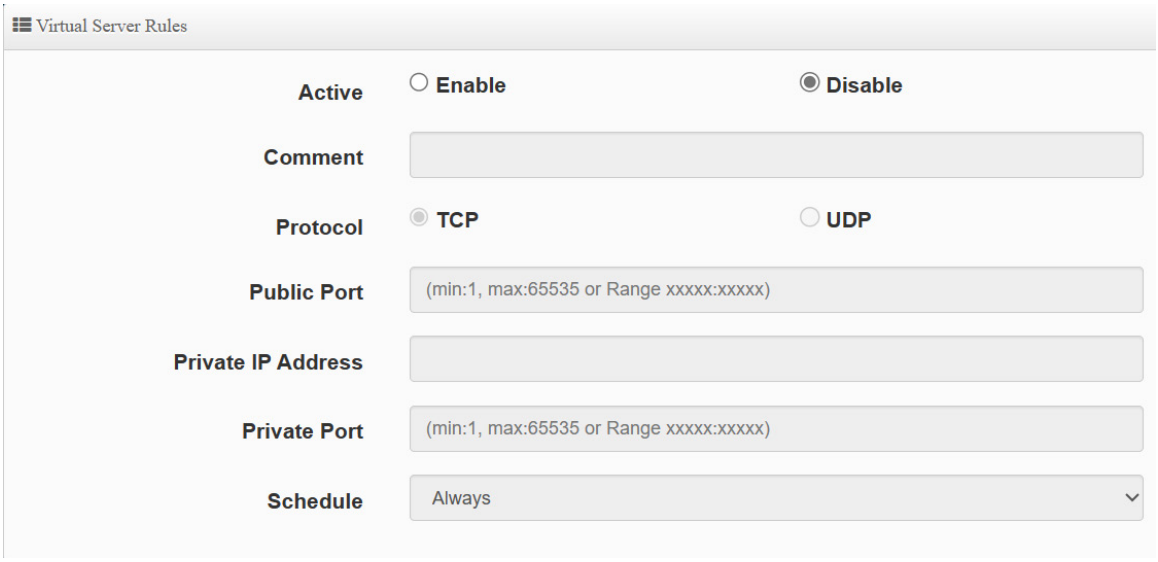
Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

8-4. Virtual Server

The **"Virtual Server"** can also referred to as "Port Forward" as well and used interchangeably. Resources in the network can be exposed to the Internet users in a controlled manner including on-line gaming, video conferencing or others via Virtual Server setup. Don't repeat ports' usage to avoid confusion.

Suppose you want to assign ports 21-25 to one FTP, Telnet and SMTP server (A in the example), and port 80 to another (B in the example). You assign the LAN IP addresses and the ISP assigns the WAN IP address. The NAT network appears as a single host on the Internet.

Please click **Edit** button to setting Virtual Server rules.



- **Active:** Administrator can select Virtual server rule to Enable or disable.
- **Comment:** Enter the description of virtual server rule.
- **Protocol:** Administrator can select service protocol of TCP or UDP.
- **Public Port:** Enter service port No. for public.
- **Private IP Address:** Enter corresponding IP address for internal.
- **Private Port:** Enter internal service port No. for private.
- **Schedule :** Administrator can select to used rule of **"Time Policy"**

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

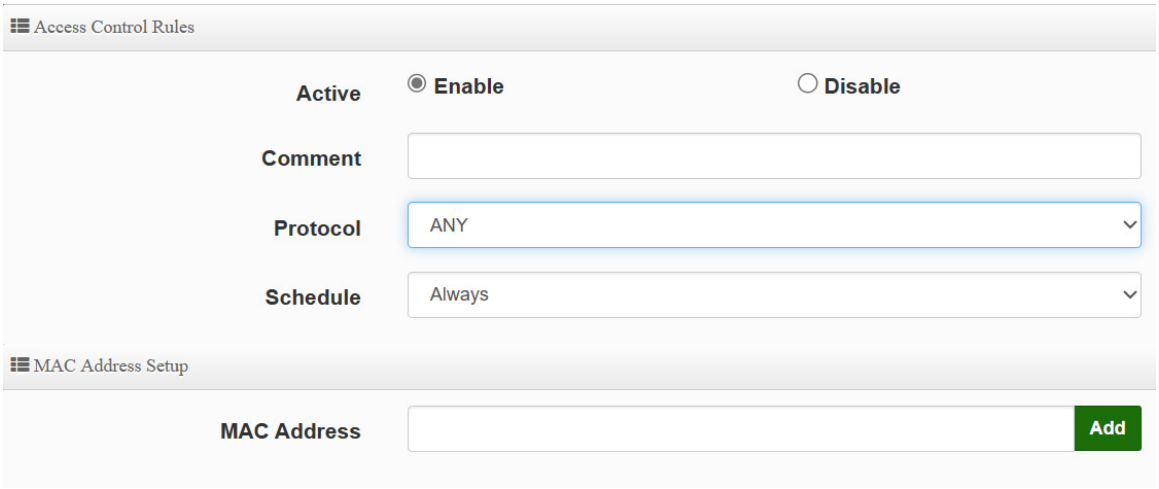
8-5. Access Control

The Access Control function administrator can to block or allow specific kinds of TCP/UDP/ICMP protocol, such as Internet access, designated services, and websites. The Access Control function can set 20 profiles.

Please click on **Advance -> Access Control** and follow the below setting.

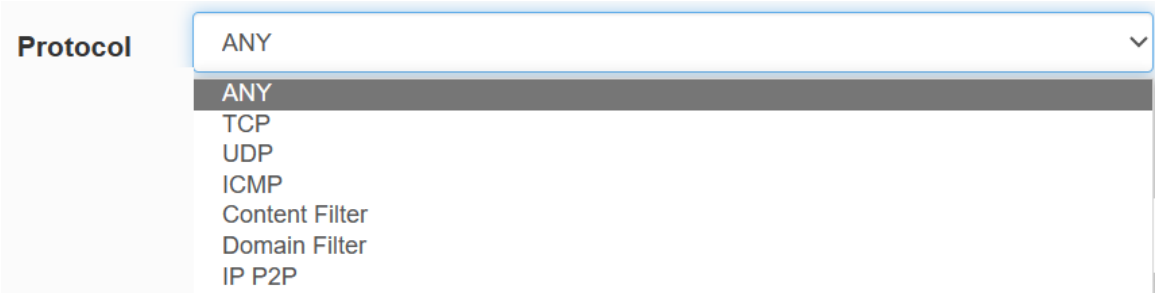
- **#**：Display access control list.
- **Active**：Display Active or InActive for the access control rule.
- **Comment:** Display information for the rule.

- **Protocol**：Display information for the protocol.
- **Edit**：Administrator can click the button to set Access Control rule.



 # Access control rules：

- **Active**：Administrator can select Enable or Disable for the Access control rule.
- **Comment**：Administrator can enter comment for the role.
- **Protocol**：Administrator can to select management protocol by TCP/UDP/ICMP/Content Filter/Domain Filter and IP P2P.



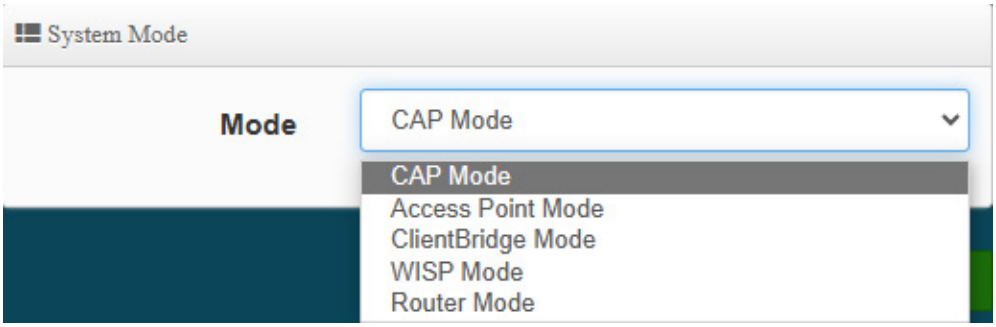
  - ✓ **ANY:** Select **"Any"** is all deny Protocol, administrator can filter local IP / IP range go to destination IP / IP range and use protocol.
  - ✓ **TCP:** Deny TCP Protocol, Administrator can set TCP protocol and assign IP / IP range.
  - ✓ **UDP:** Deny UDP Protocol, Administrator can set UDP protocol and assign IP / IP range.
  - ✓ **ICMP:** Deny ICMP Protocol, Administrator can assign IP / IP range.
  - ✓ **Content Filter:** Administrator can set web Keyword to filter.
  - ✓ **Domain Filter:** Administrator can set domain name to filter.
  - ✓ **IP P2P:**
- **Schedule**：The rule can apply Time Policy.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.

9. CAP Mode

9-1. Change Setup Mode

If the administrator needs to switch to CAP mode, Please click "System"-> " Mode Setup " to change CAP mode.



Click ***"Save"*** button to save your changes. And click ***"Reboot"*** button to activate your changes

Notice	Please note that the LAN IP addresses in each mode are different from each other and will not continue. For the first time after switching modes, always perform access management on the LAN default IP address of 192.168.2.254

9-2. VLAN Setup

VLAN List

#	Status	Flag	IP Address	Netmask	Action
0	On	Native ETH1 Native ETH2	192.168.2.254	255.255.255.0	Network
1	Off	ETH1.101 ETH2.101	192.168.101.254	255.255.255.0	Network
2	Off	ETH1.102 ETH2.102	192.168.102.254	255.255.255.0	Network
3	Off	ETH1.103 ETH2.103	192.168.103.254	255.255.255.0	Network

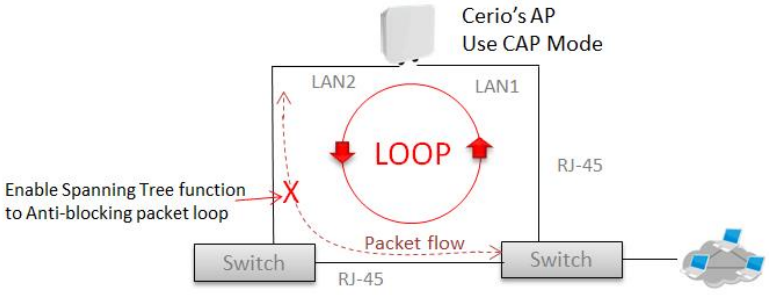
- **#**：Display VLAN No.
- **Status**：Display on /off line status for the VLAN mode
- **Flag**：Displays the tag ID information used by the virtual network. When Native ETH1 Native ETH2 is displayed, it means that the current main wired connection is the virtual network as the main login system.

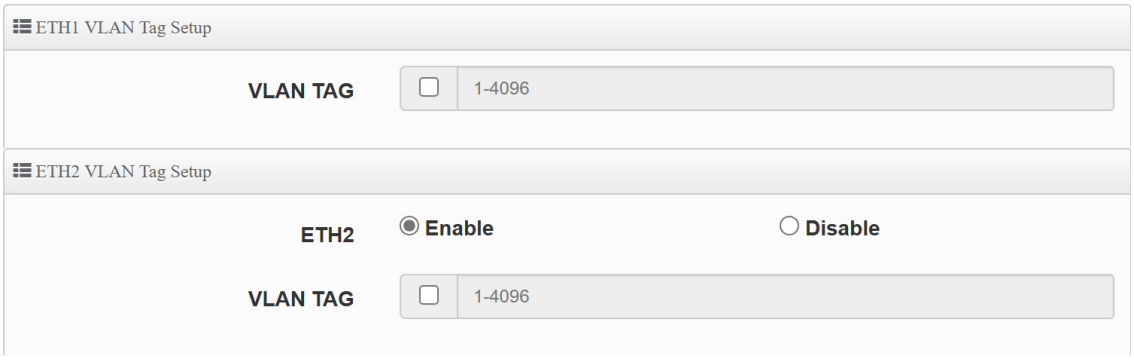
- **IP Address**：Display IP address for the VLAN mode.
- **NetMask**：Display netmask for the VLAN mode.
- **Action**：Administrator can set VLAN IP、Radio 2.4 or 5G-1 or 5G-2 on/off、Spanning tree and VLAN tag

- **VLAN Mode**：Administrator can Enable or disable the VLAN function.
- **IP Setup**：Administrator can set the VLAN IP address and NetMask or disable IP.
- **NetMask**：Display netmask for the VLAN mode.

Notice	There must always be at least one VLAN enabled. If the administrator disables all the VLANs, he/she will not be able to login to the manager page. The administrator must then reset to default.

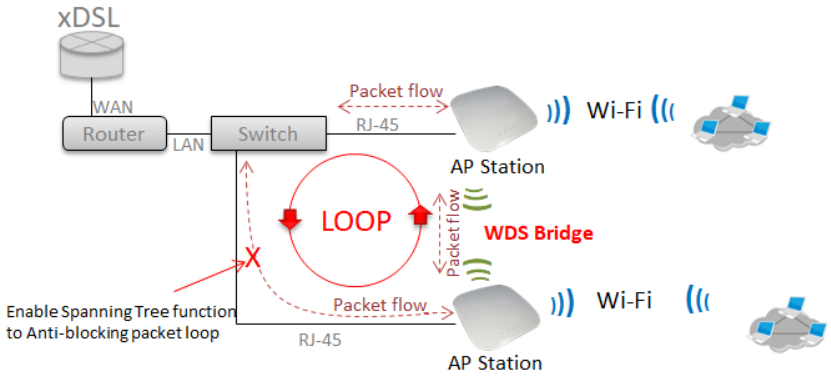
- **802.1d Spanning Tree**：The spanning tree network protocol provides a loop free topology for a bridged LAN between LAN interface and 8 WDS interfaces from wds0 to wds7. The Spanning Tree Protocol, which is also referred to as STP, is defined in the IEEE Standard 802.1d.





- **ETH1 VLAN Tag Setup**： Administrator can set Tag ID for the Ethernet port.
- **ETH2 VLAN Tag Setup**：Administrator select Enable/disable the Ethernet port and set the Tag ID for the Ethernet port.

Click **"Save"** button to save your set function. Then click "Reboot" button to activate your changes.



9-3. AP Control

When CenOS5.0 AP changes to CAP mode, Administrator can use AP Control functions to centralize management of APs in the network architecture. AP control Setting functions have "Scan Device", "Batch Setup", "AP Setup", "Group / Map setup" and Authentication Profile setup etc..

Please click **"AP Control"** to enter AP Management settings

9-3-1. Scan Device

Centralized Management APs operating Instructions.

1. **Filter Device**：
   - **VLAN#**：Administrator can select VLAN network to discovery managed Aps
   - **Default Password**：Set login system password by managed Aps.
   - **Sort**：Administrator can select discovery managed Aps Type. (IP or MAC)

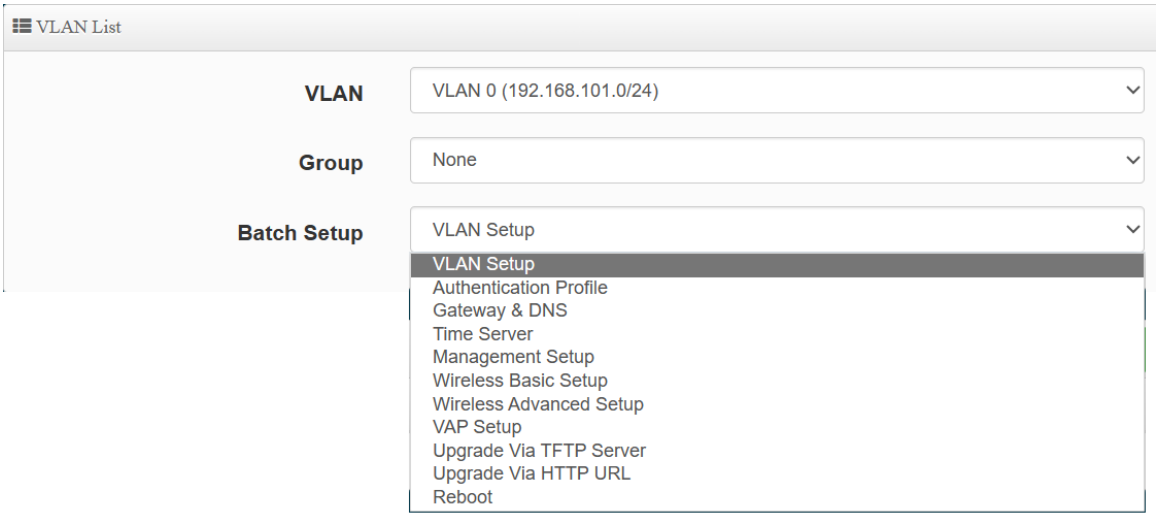
2. **Scan Result**
   - **#**： Display managed APs items
   - **Device**：Administrator can select all or single for managed Aps**.**
   - **MAC Address**：Display MAC address for managed AP.
   - **IP Address**：Display IP address for managed AP.
   - **Netmask**：Administrator can set single Netmask for Managed AP.
   - **Default**：Administrator click the button will can reset to default for select managed APs.

3. **Update IP Address & Netmask**
   - **Control Port**：Administrator can change VLAN network for managed APs.
   - **VLAN TAG**：Administrator can set VLAN TAG ID for managed APs.
   - **IP Address**：Administrator can set IP address for managed APs, the IP address is auto-incrementally.
   - **NetMask**：Administrator can set NetMask for managed APs.

When the setting managed APs is completed, please click Apply & Reboot button to complete the setup process.

9-3-2. Batch Setup

The AP control function supports centralized configuration of managed APs. Administrator can change VLAN network / Group and batch setup for managed APs.



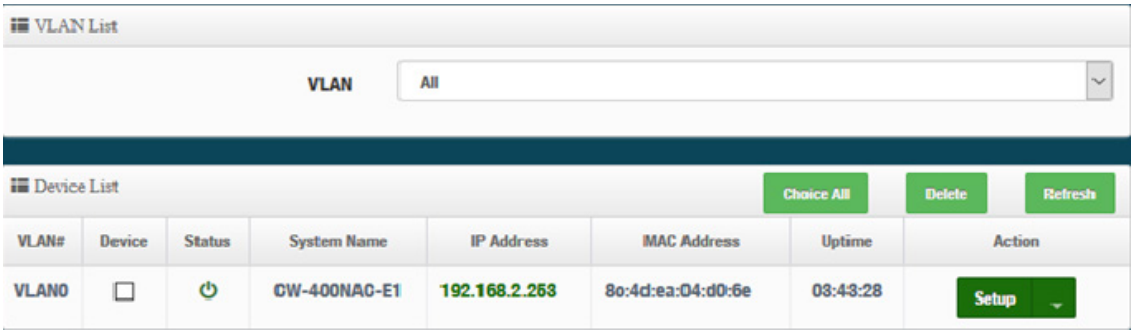
- **VLAN**：When VLAN Tag function is enabled (please refer for “System VLAN Setup”), administrator can change VLAN tag for managed APs
- **Group**：When AP Groups are created (please refer” Group setup”), Administrators can select and change group settings of managed APs.
- **Batch Setup**：Administrator can centralize setting changes for managed APs.
  - **VLAN Setup**：Administrator can set VLAN Tag, IP address and Wi-Fi on/off for the managed APs。
  - **Authentication Profile**：After creating Profiles, See: “Authentication Profile” users can conveniently apply Authentication profiles
  - **Gateway & DNS:** Setting Gateway and DNS for managed APs
  - **Time Server:** Setting System Time for managed APs. (Please refer to Configure Time Server)
  - **Management Setup:** Setting system name/ system login port and system log server service for managed APs. (Please refer to “system management”)
  - **Wireless Batch Setup:** Setting Wi-Fi configurations for managed APs. (Please refer to “Wireless Basic Setup”)
  - **Wireless Advanced Setup:** Setting Wi-Fi Advanced settings for managed APs. (Please refer to “Wireless Advanced Setup”)
  - **VAP Setup**：Wi-Fi SSID / channel or security settings for managed APs. (Please refer to “ Configure Radio 0/1”)
  - **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.

9-3-3. AP Setup

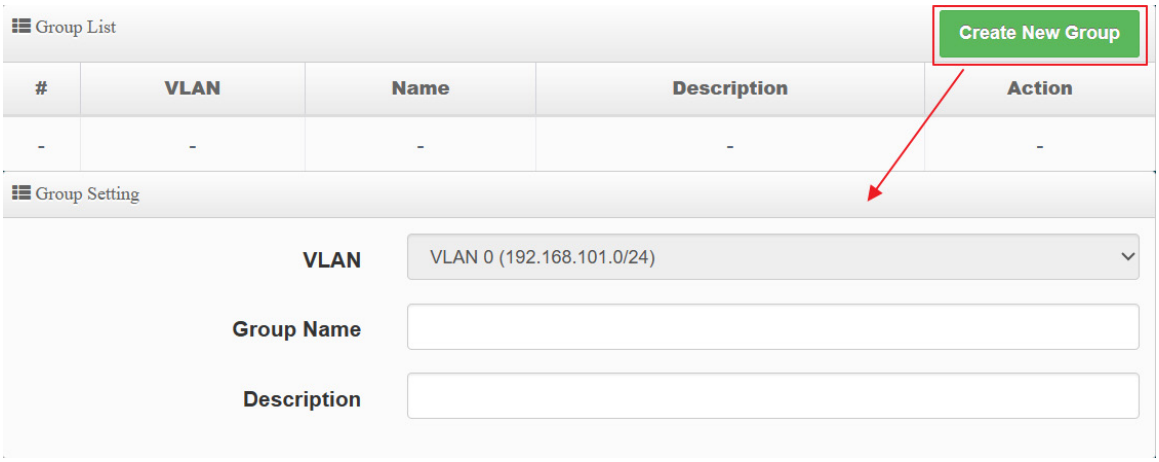
Administrator can monitor statuses and modify managed APs information.



- **VLAN**：Select desired VLAN for AP setup
- **Setup**：Administrator can modify IP addresses, system login passwords, and web login port for managed APs. If administrator has change AP devices, administrator can modify MAC address of the new managed AP.

9-3-4. Group Setup

Administrator can create Groups within the same VLAN.

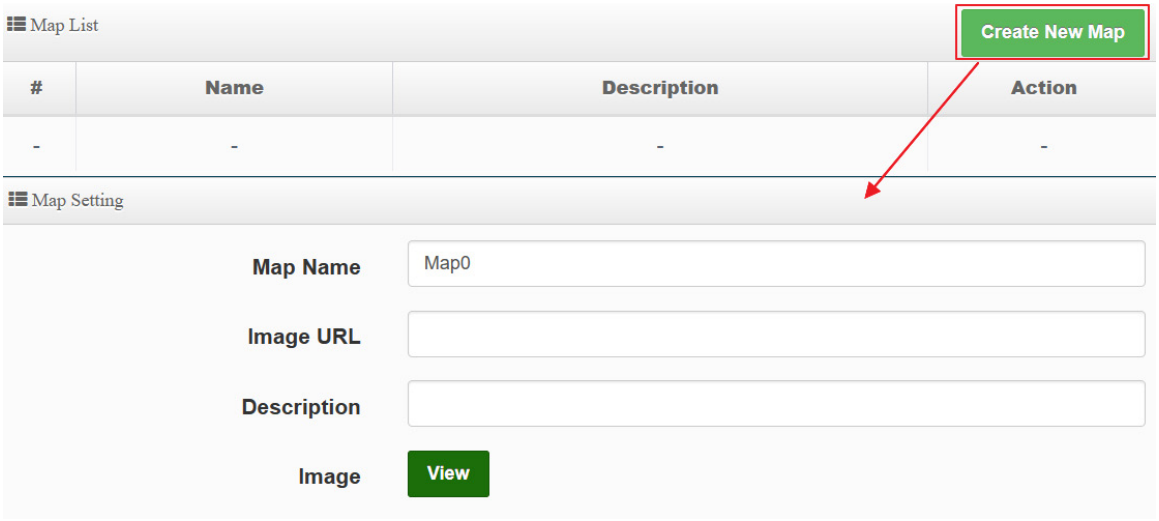


- **VLAN**：Select VLAN.
- **Create New Group**：Click the button to create a new AP Group

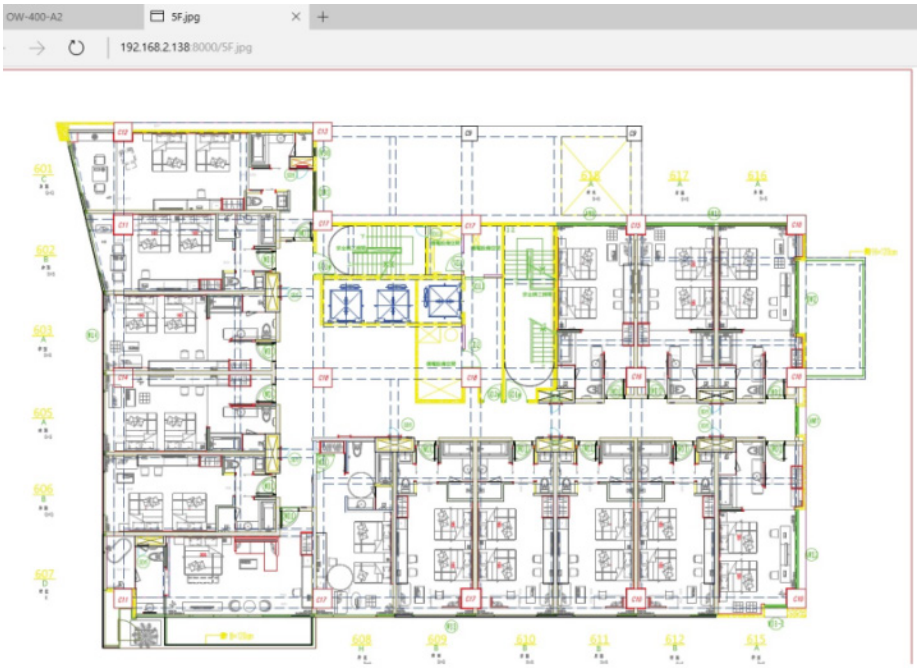
- **Device**：Administrator can select managed APs and import them into the Group.

9-3-5. 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 the AP network

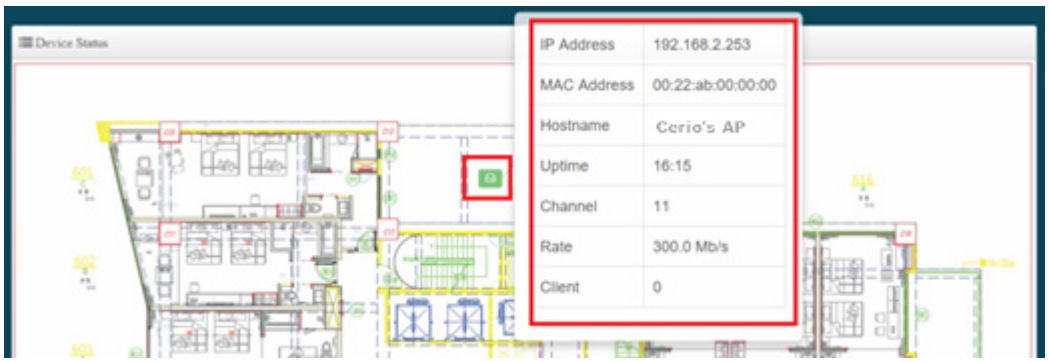


- **Create New Map**：Click the button to create map
- **Map Name**：Enter map name.
- **Image URL**：Paste Map image url
- **Description**：Enter the description for the map.
- **Image-View Button**：Once the Map is created and properly in the Map List, administrators can click the “Layout” button in the action tab to map out the AP network. Managed APs will appear in the “Device List” section of the layout page. Administrators can simply drag the AP (IP Address) to the correct installation location.



After the Map URL setup confirmation, please reboot the system.

View：Once complete, administrators can click the “View” button to monitor AP statuses and locations.。



9-3-6. Authentication Profile (Profile)

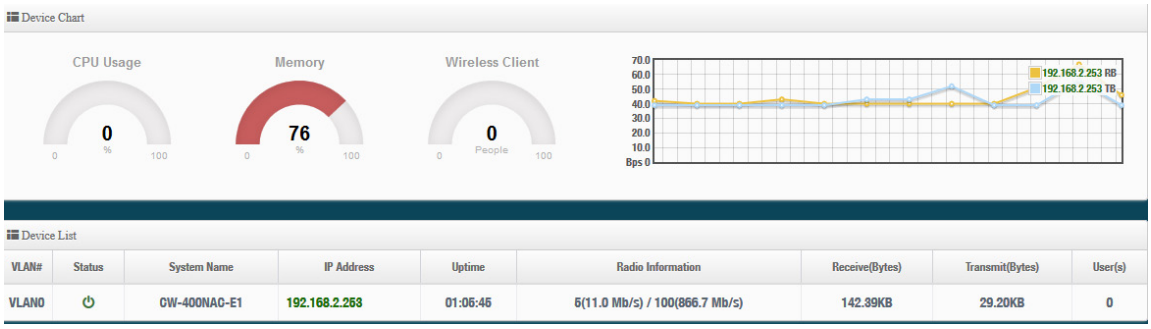
Administrator can pre-set authentication conditions in the profile, the authentication set can refer “Authentication”.

- **Create New Profile**：Administrator can create authentication profile.
- **Edit**： Authentication Click the Authentication button to Enable or Disable authentication function. For more details, refer to **"Authentication".**

  Authentication Click Dropdown to set authentication functions. Refer to **"Authentication"** dropdown functions.
- **Action:** Setup The button can modify or delete for the authentication profile.

9-3-7. Status

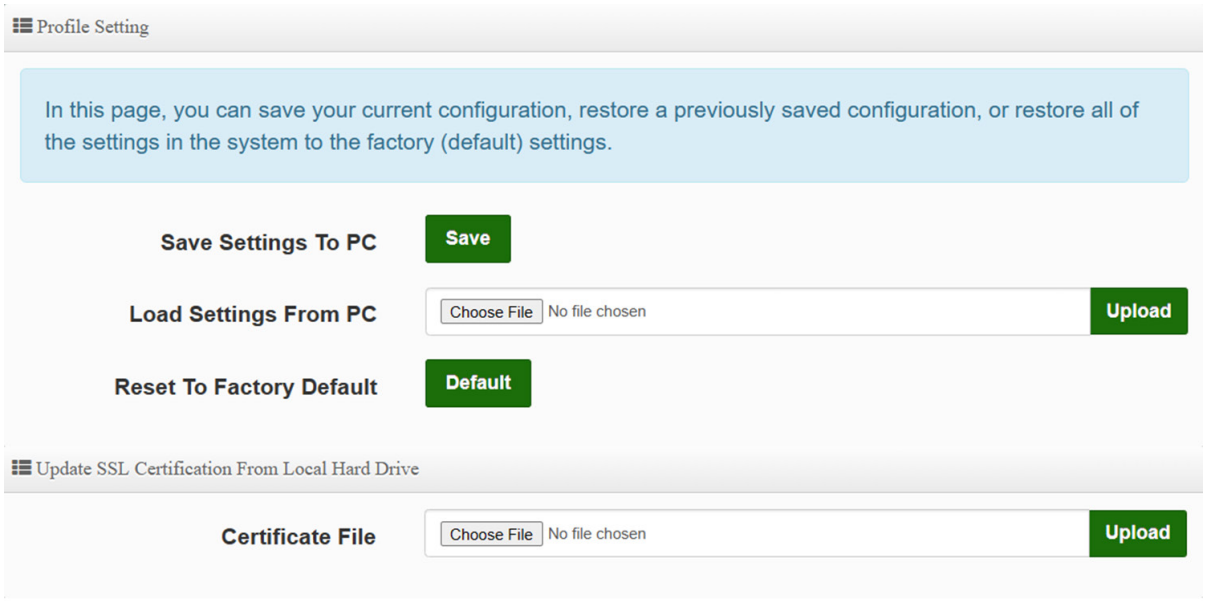
Administrator can monitor Tx/Rx flow information, show online users and check system CPU / Memory information and on/off line for the managed APs. The information data display support graphical interface.



10. Utility

10-1. Profile Setting

This Functions purpose is to backup current configuration, restore prior configuration or reset back to factory default configurations.



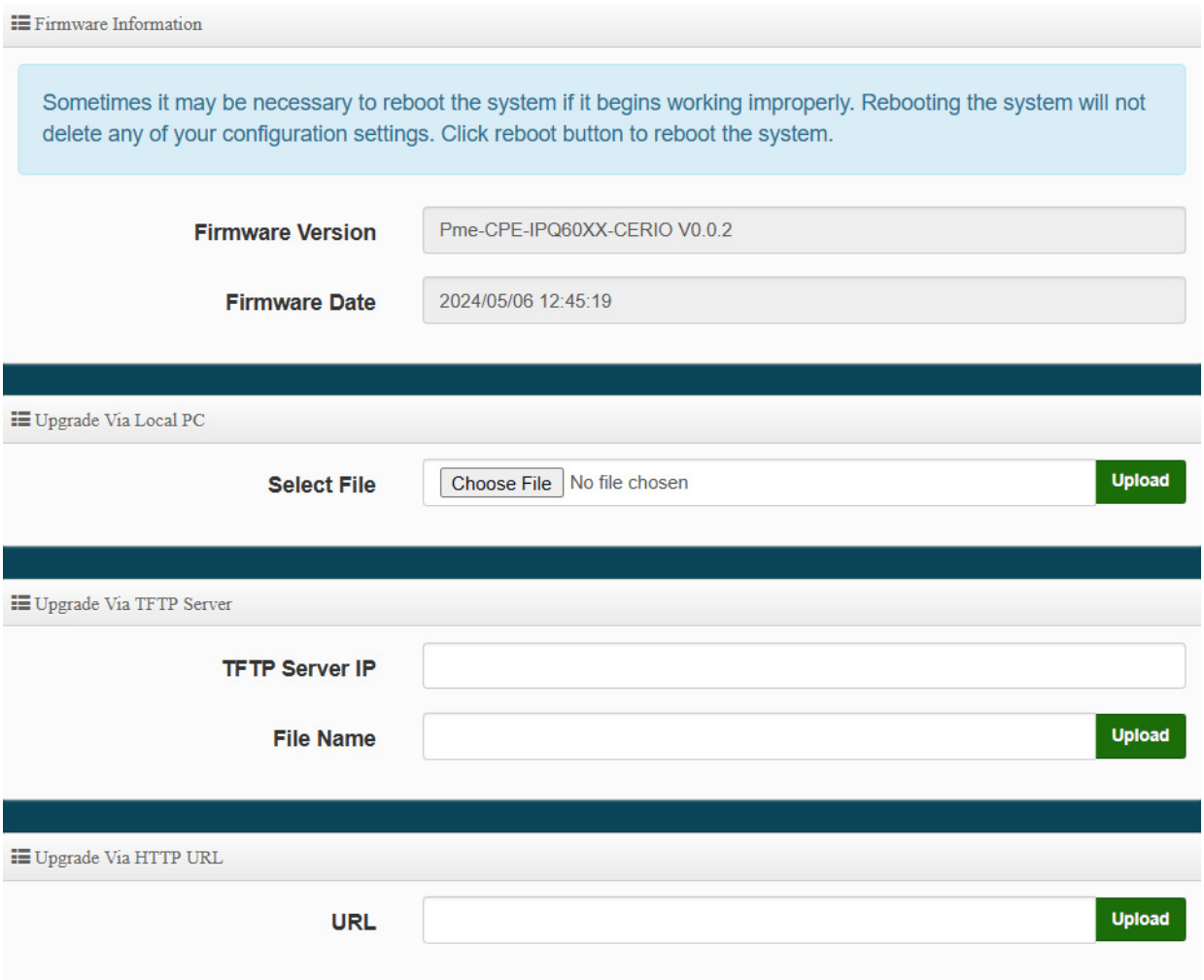
- **Save Settings to PC:** Click ***Save*** button to save the current configuration to a local disk.
- **Load Settings from PC:** Click ***Browse*** button to locate a configuration file to restore, and then click ***Upload*** button to upload.
- **Reset To Factory Default:** Click ***Default*** button to reset back to the factory default settings and expect **Successful** loading message**.** Then, click ***Reboot*** button to activate.

10-2. 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 bugs 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 Information:

Display the system firmware information.



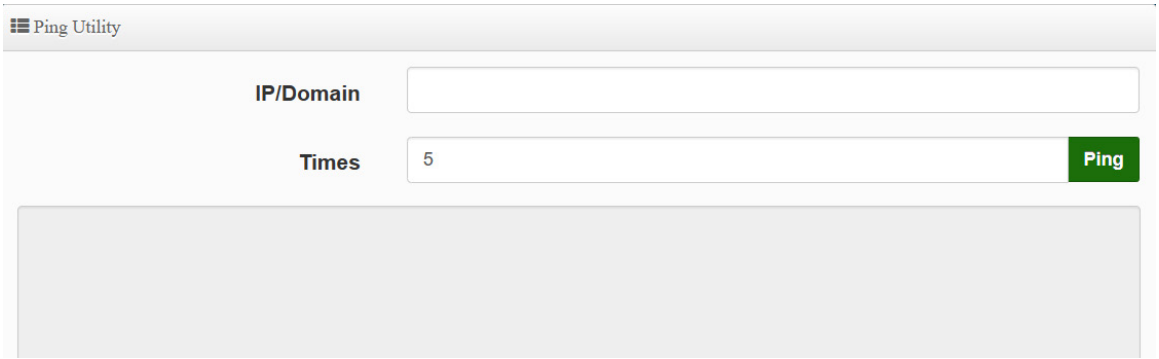
- **Select File:** Administrator can select Firmware file in Local PC.

Upgrade Via Local PC and TFTP Server:

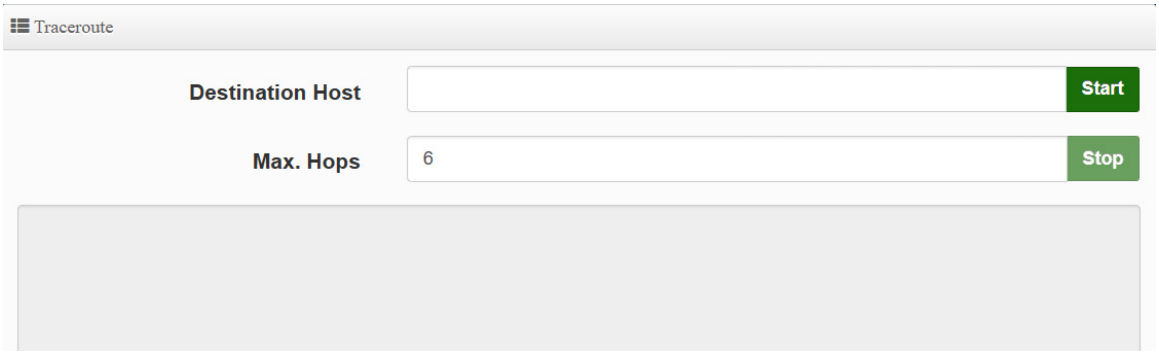
The upgrade firmware will support via local PC and TFTP Server and HTTP URL to upgrade system.

Notice	*We strongly recommend that you perform the firmware update by following these steps:* *1.Please use a RJ-45 network cable to connect the computer and the wireless base AP mode to perform the update operation. Do not use a wireless connection for firmware update operations.* *2. During the update process, please do not turn off or power off the system.* *3. Make sure to update using a compatible web browser to avoid update failures.* *4. After the update is complete, make sure to perform a factory default reset operation and restart the wireless AP mode.* *5. If the update operation is not performed according to the above steps, if the update fails and the system cannot provide services or cannot operate normally, please forgive us for treating this situation as a human error and you will lose the product warranty. Service and you will be charged for related maintenance.*

10-3. Network Utility

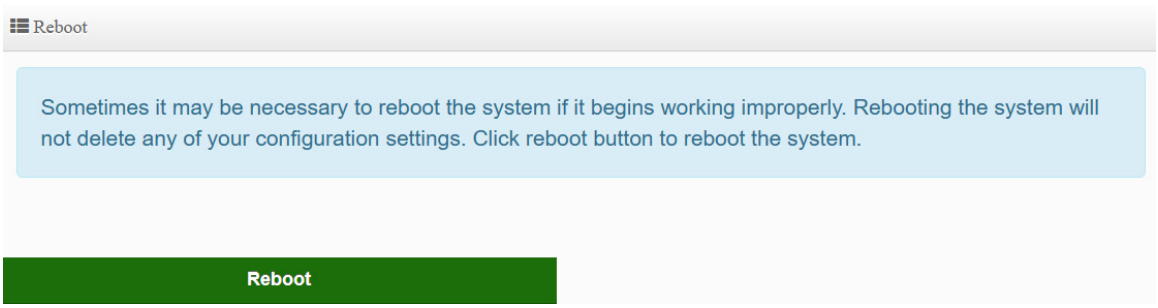


- **Ping**：This utility will help ping other devices on the network to verify connectivity. Ping utility, using ICMP packets, detects connectivity and latency between two network nodes. As result of that, packet loss and latency time are available in the **Result** field while running the PING test.
  - **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:** By default, its 5 and the range is from 1 to 50. It indicates number of connectivity test.



- **Traceroute**：Allows tracing the hops from the CenOS 5.0 AP 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 Hops**: Specifies the maximum number of hops (max time-to-live value) trace route will probe.

10-4. Reboot

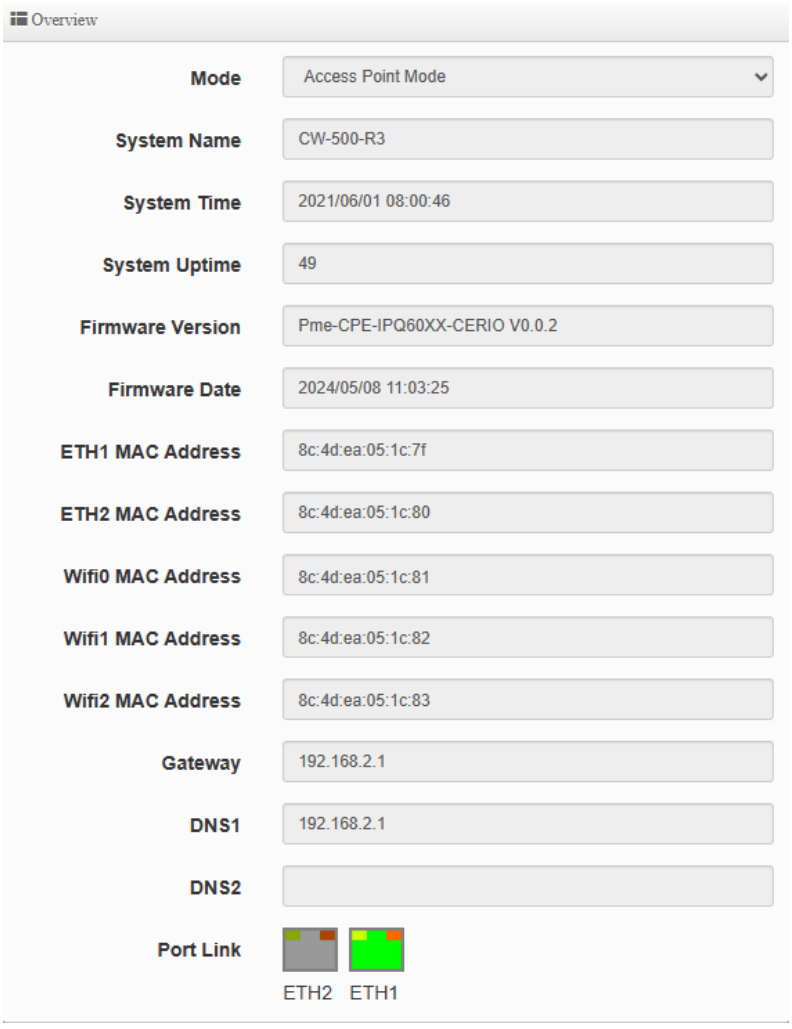


This function allows user to restart system with existing or most current settings when changes are made. Click **Reboot** button to proceed and take around three minutes to complete.

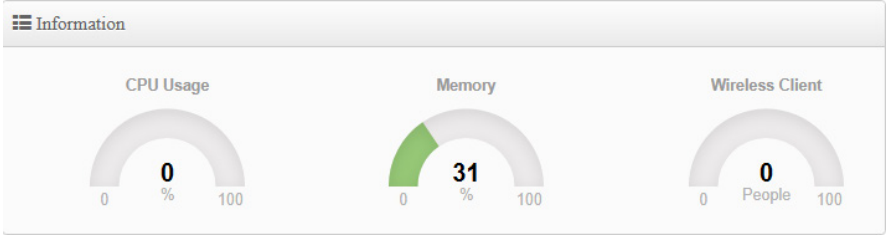
11. Status

The status mainly displays system related information, including system network information, wireless base station information, and wireless user connection information.

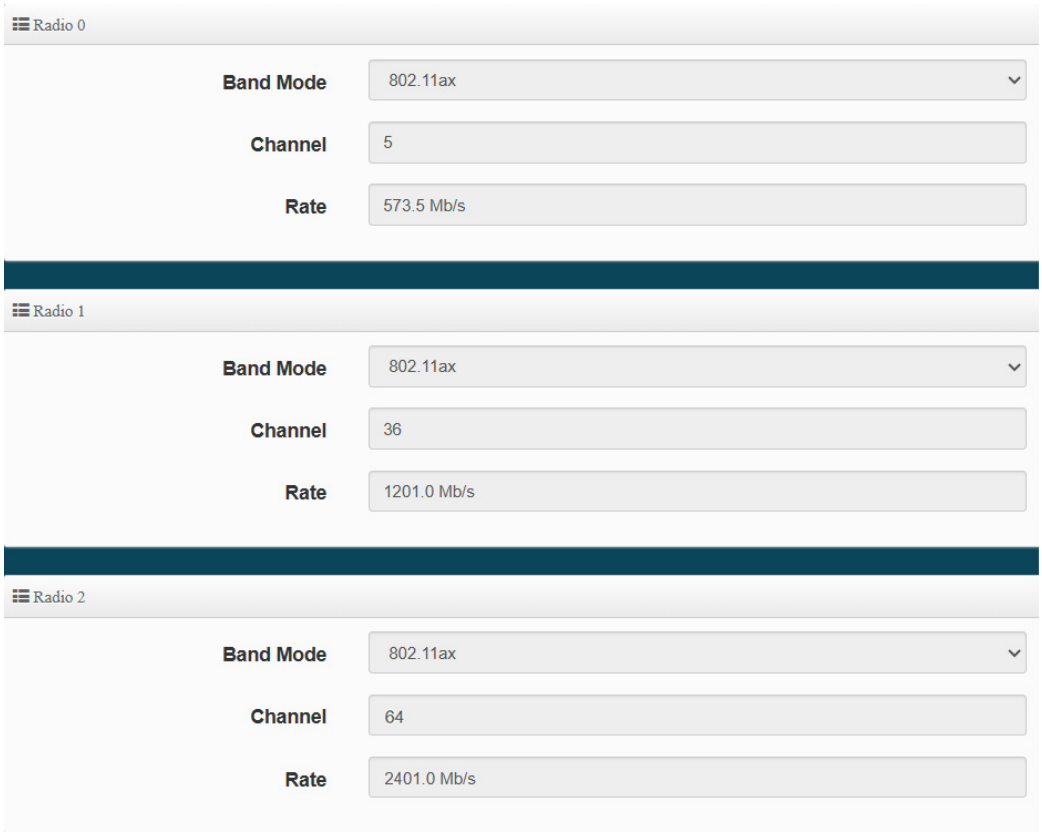
11-1. Overview



- **Overview**：It mainly displays the current mode, name, time, firmware version, network card address and related network settings.
- **Information**：Shows the performance / memory usage of the total CPU space used by the current system and the current number of connected wireless users.



- **Radio 0/Radio 1/Radio2**：Displays the basic operating mode information of the current Radio 0 (2.4GHz) / Radio 1 (5GHz-1) / Radio 2 (5GHz-2) wireless AP.



11-2. Wireless Client

LAN

Radio	MAC Address	RSSI	Rate(RX/TX)	Bytes(RX/TX)	Packet(RX/TX)	SEQ(RX/TX)
-	-	-	-	-	-	-

※ The page can be display Wireless user information link to access point. Administrator can monitor MAC address / rate and RSSI for the wireless users. (In addition to CAP mode)

- **Radio**：Display information for wireless client connection Radio 0 or 1
- **MAC Address**：Display information of clients Wi-Fi MAC address
- **RSSI**：Display information of clients Wi-Fi connection signal strong and weak.
- **Rate(RX/TX)**：Display information of clients Wi-Fi connection data rete.
- **Byte(RX/TX)**：Display information of clients Wi-Fi byte
- **Packet(RX/TX)**：Display information of clients Wi-Fi packet
- **SEQ(RX/TX)**：Display information of clients Wi-Fi sequence.

11-3. Online Users

The status can display online users by Captive Portal. Administrator can monitor user's login / logout time and account type for the authentication account. (This page only used AP mode)

Authentication Zone Online Users

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

Notice

This function works in the wireless AP mode. When the web authentication function is activated, the current connection status and related information of online users who have passed the authentication will be displayed.

- **VLAN#**：Display VLAN number.
- **Authentication**：Display Captive Portal authentication function is on/off in the VLANs.
- **User Count**：Display the VLAN network connected user's amount.
- **Download/Upload Packets**：Display total download or Upload packets amount information of the VLAN.。
- **Download/Upload Bytes**：Display total download or Upload flow information of the VLAN.

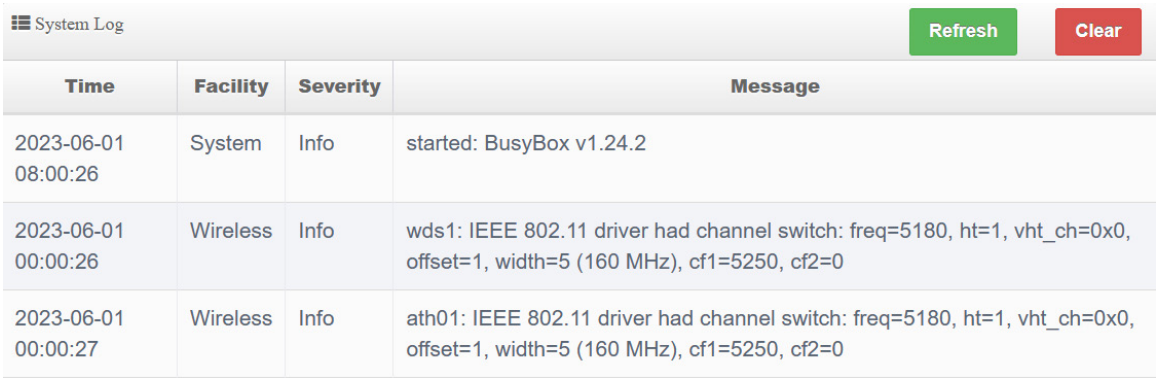
11-4. Authentication Log

Authentication Zone Log

Date	VLAN#	Detail
-	-	-

- **Date**：Administrator can select dates.
- **VLAN#**：Administrator can select VLANs.
- **Detall**：Administrator can clicl button to open detall information.

11-5. System Log



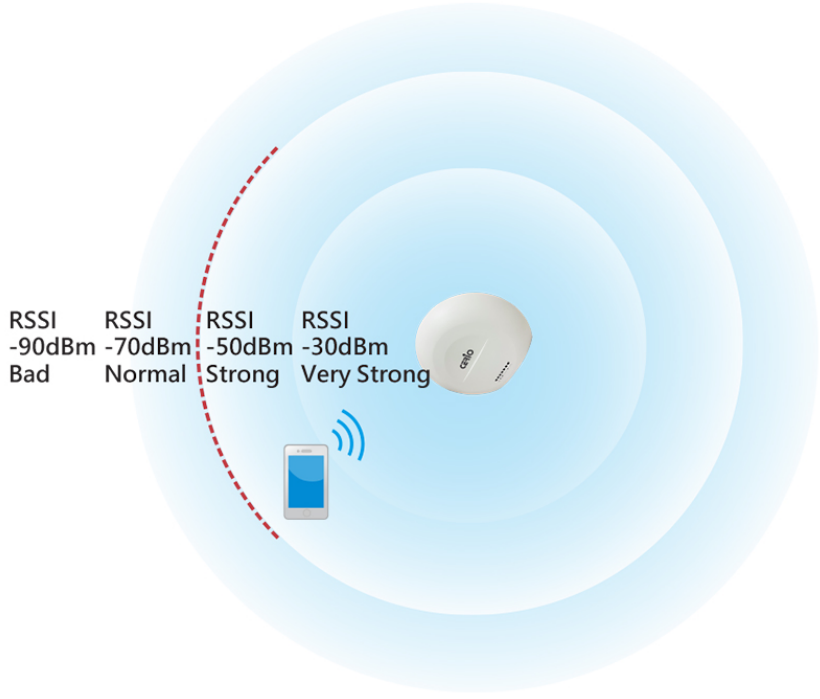
- **Time**：The date and time when the event occurred.
- **Facility**：It helps users to identify source of events such “System” or “User”
- **Severity**：Severity level that a specific event is associated such as “info”, “error”, “warning”, etc.
- **Message**：Description of the event.
- Click **“Refresh”** button to renew the log
- Click “**Clear”** button to clear all the record.

12. [Other technical documents]

12-1. Fast Roaming 802.11r Fast Roaming Settings

The roaming mechanism of 802.11r depends entirely on the user's device. WiFi roaming refers to accessing from one BSS (BSSID = MAC address of WiFi AP) to another BSS (BSSID = MAC address of WiFi AP) within an ESS (ESSID = the name of the wireless network), while fast roaming allows client network card devices (such as handheld WiFi client devices or WiFi laptops that require seamless connection when moving) to connect from a Cerio When the AP access point switches to another Cerio WiFi AP access point, it maintains a continuous wireless connection and can continue to transmit without reconnecting. The support of 802.11r fast roaming solves the problem that the WiFi client device will not trigger an early disconnection from the old AP (the original connected AP), that is, it will not proactively send a disassociation or deauthentication report to the old AP (the original connected AP). Since there is no mechanism or roaming neighbor list to rely on, it may be connected until the transmission is unable to jump to the available WiFi AP. point phenomenon, the process is a state of seamless roaming.

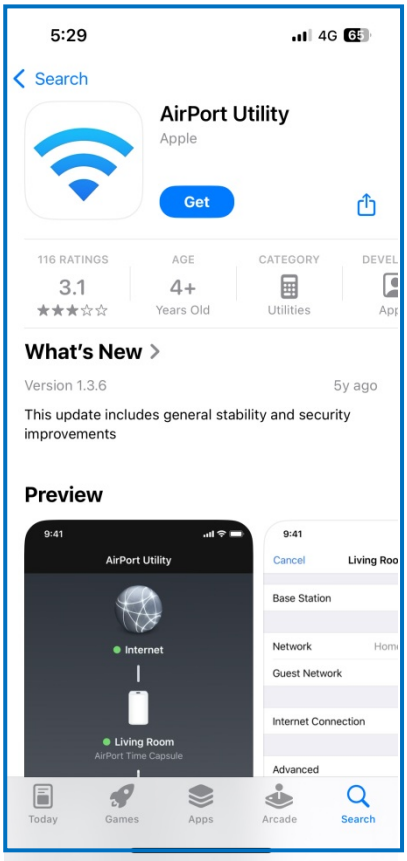
Utilize the 802.11r/802.11k fast roaming enablement of each AP. Configure the list of R0/R1Key Holders and other related neighbor APs required for the "WiFi client network card device". Once the "WiFi client network card device" is connected, the set "R0/R1Key Holders and other related neighbor lists" are obtained. When the "WiFi client network card device" moves to the signal (RSSI) with the Cerio WiFi AP access point When the "critical value" is reached, you can seamlessly switch to the next WiFi AP access point (the AP is regarded as a handover procedure).

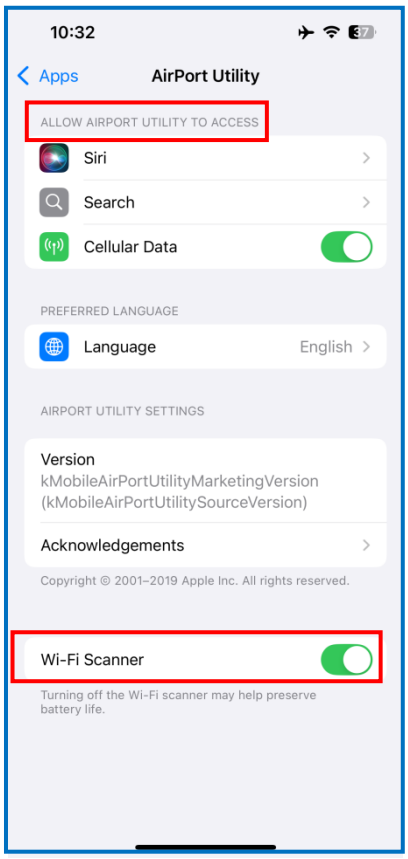


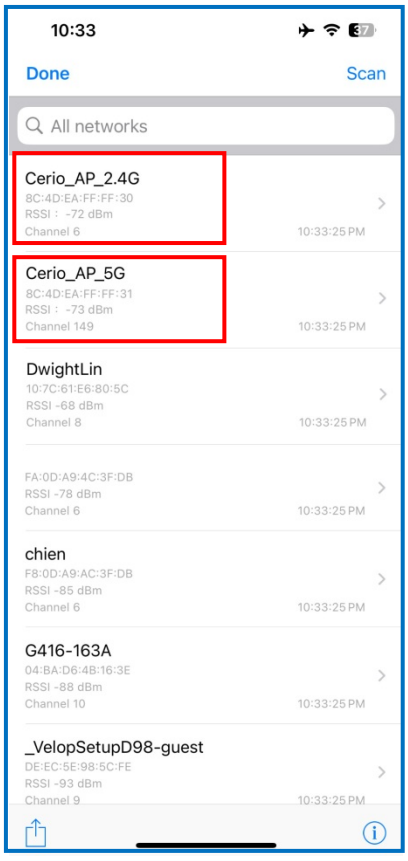
Step-1 : Complete AP location planning before setting up WiFi AP

The signal RSSI value (Received Signal Strength Indicator Unit) of the WiFi client network card device connected to the WiFi AP access point will have different signal results depending on the environmental obstacle pattern. The closer the RSSI value (Received Signal Strength Indicator Unit) is to 0, the better. And the "critical value" of the WiFi client network card device's own design driver to start roaming handover is generally defined between RSSI -70 and -80, and

Different WiFi client network card devices (such as mobile phones with low WiFi power) and WiFi AP access points with different power capabilities will produce different possible RSSI quality results. Before setting up the Cerio WiFi AP, please ensure that the relative signal transmission power (Power Level) of each Cerio WiFi AP in your environment is appropriately arranged. Know the relative distance between your WiFi client network card device and the WiFi AP and the reachable RSSI status. You can use, for example, the iPhone Apple Store to download and use AirPort to turn on the "WiFi Scanner" in the APP settings. Functions are arranged in advance.







The mutual signals of multiple Cerio WiFi AP access points must generate overlapping "roaming end signals". This signal usually refers to the RSSI between -70 and -80 after the WiFi client network card is connected to the Cerio WiFi AP access point. When the driver automatic mechanism of the WiFi client network card detects that the RSSI between itself and the WiFi AP access point has reached the "critical value" (RSSI between -70 and -80), it will be based on the "R0" previously obtained by the WiFi AP access point. /R1Key Holders and other related AP neighbor lists" to perform roaming and replace other better WiFi AP neighbors. Before roaming settings, it is relatively necessary to properly conduct the necessary "overlapping signals at the roaming end" layout point planning for each WiFi AP access point.

The placement of WiFi APs that are inappropriately close or too far from each other may result in poor "seamless roaming" results or even unsuccessful roaming. This reminder "the prerequisite for seamless roaming is:

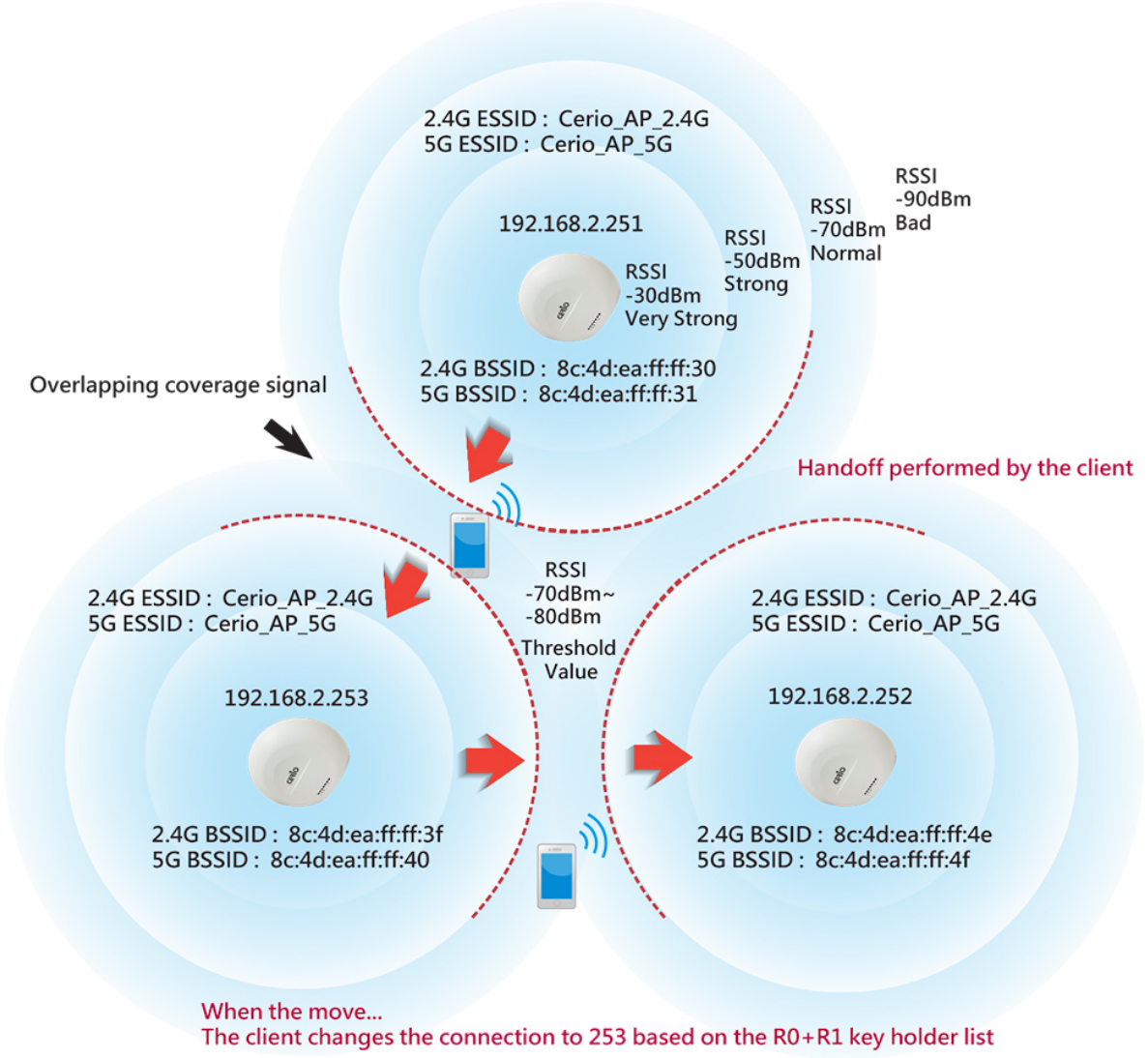
1. Environment: Each Cerio WiFi AP has "overlapping signals at the roaming end" deployed with each other.
2. Each Cerio WiFi AP uses the same channel, the same SSID name (ESSID) and the same WiFi encryption.
3. For each Cerio WiFi AP, set its own relative "R0/R1Key Holders and other related AP neighbor lists".
4. The WiFi client network card (Client) connected to the Cerio WiFi AP must also support the same 802.11r/k roaming protocol.

Step-2 : Confirm the BSSID of each WiFi AP to be set in the roaming environment

The following figure shows that three IP addresses are 251. 252 and 253 are neighbors, and their respective BSSIDs (MAC address IDs) are as follows:

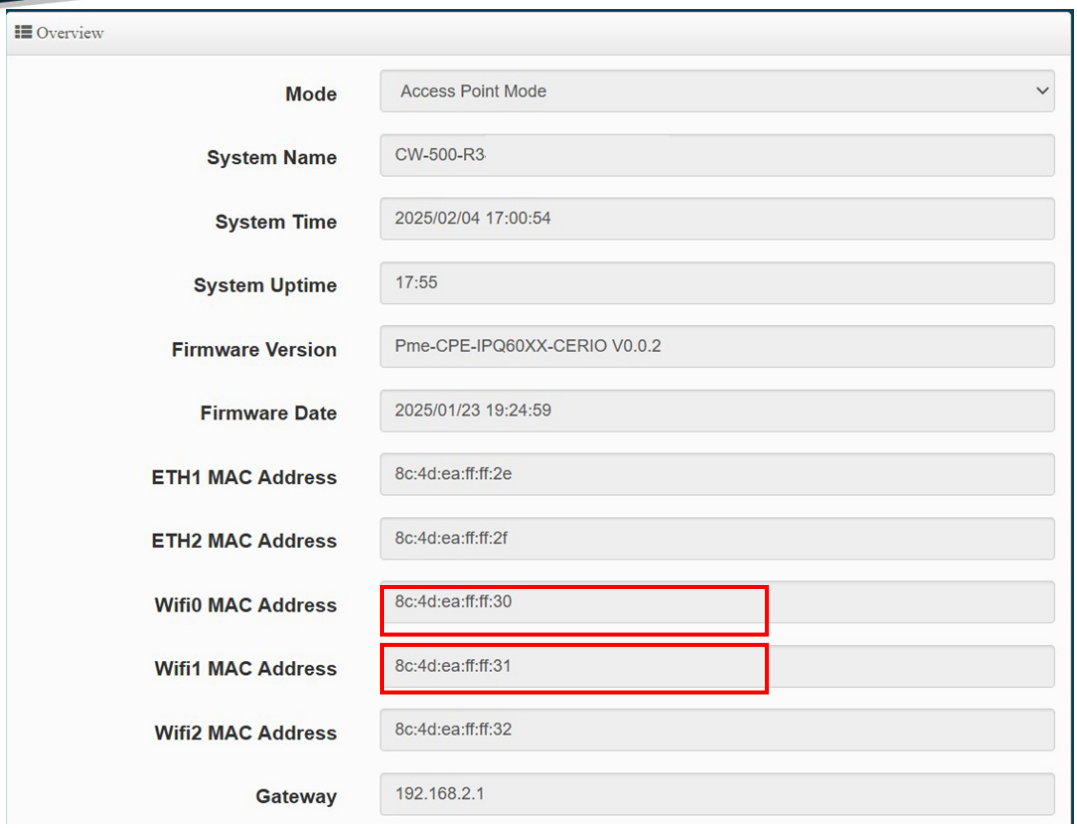
	AP unit 1	**AP unit 2**	**AP unit 3**
LAN IP	192.168.2.251	192.168.2.252	192.168.2.253
Radio-0(2.4G) BSSID	8c:4d:ea:ff:ff:30	8c:4d:ea:ff:ff:3f	8c:4d:ea:ff:ff:4e
Radio-1(5G-1) BSSID	8c:4d:ea:ff:ff:31	8c:4d:ea:ff:ff:40	8c:4d:ea:ff:ff:4f

AP distance/power level is based on client connection RSSI threshold.



The mutual signals of multiple Cerio WiFi AP access points must generate overlapping "roaming end signals". This signal usually refers to the RSSI between -70 and -80 after the WiFi client network card is connected to the Cerio WiFi AP access point. When the driver automatic mechanism of the WiFi client

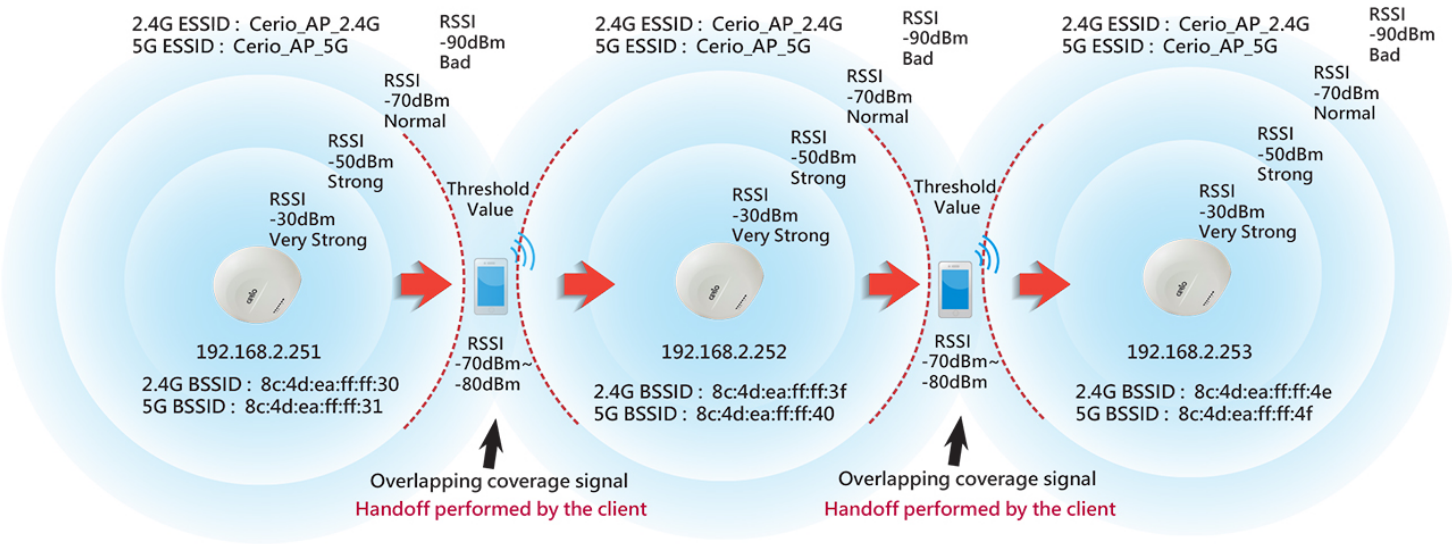
*Tip : In addition to the above-mentioned query methods through the software UI, you can also quickly obtain the MAC address ID of each relative radio through the off-machine label of the Cerio product body.



Step-3 : First understand the neighbor status of each AP where it is located

Through the overall planning of the "overlapping signals at the roaming end", you can clearly understand the neighbors of each WiFi AP's "overlapping signals at the roaming end". The 802.11r roaming mechanism is responsible for the WiFi AP. It must set which APs are its neighbors, and enter and add them to the list, so that the WiFi client network card device can connect to any WiFi AP at any time and also get the pre-determined "neighbor list" of the 802.11r roaming agreement. Therefore, Wi The Fi client network card can smoothly accelerate the completion of fast roaming and connection change in advance.

AP distance/power level is based on client connection RSSI threshold.



subsequent related settings.

Through the overall planning of the "overlapping signals at the roaming end", you can clearly understand the neighbors of each WiFi AP's "overlapping signals at the roaming end". The 802.11r roaming mechanism is responsible for the WiFi AP. It must set which APs are its neighbors, and enter and add them to the list, so that the WiFi client network card device can connect to any WiFi AP at any time and also get the pre-determined "neighbor list" of the 802.11r roaming agreement. Therefore, Wi The Fi client

1.) The neighbor of IP 251 WiFi AP is IP 252 WiFi AP, which means that IP251 WiFi AP must :

In the roaming 11r setting of Radio-0 (2.4G), you need to add neighbor 8c:4d:ea:ff:ff:3f in the roaming list (R0KH or R1KH list).

In the roaming 11r setting of Radio-1 (5G-1), you need to add neighbor 8c:4d:ea:ff:ff:40 in the roaming list (R0KH or R1KH list).

2.) The adjacent neighbors of IP 252 WiFi AP are IP 251 WiFi AP and IP 253 WiFi AP, which means that IP252 WiFi AP must :

In the roaming 11r setting of Radio-0 (2.4G), you need to add neighbors 8c:4d:ea:ff:ff:30 and 8c:4d:ea:ff:ff:4e to the roaming list (R0KH or R1KH list).

In the roaming 11r setting of Radio-1 (5G-1), you need to add neighbors 8c:4d:ea:ff:ff:41 and 8c:4d:ea:ff:ff:4f to the roaming list (R0KH or R1KH list).

3.) The neighbor of IP 253 WiFi AP is IP 252 WiFi AP, which means that IP253 WiFi AP must :

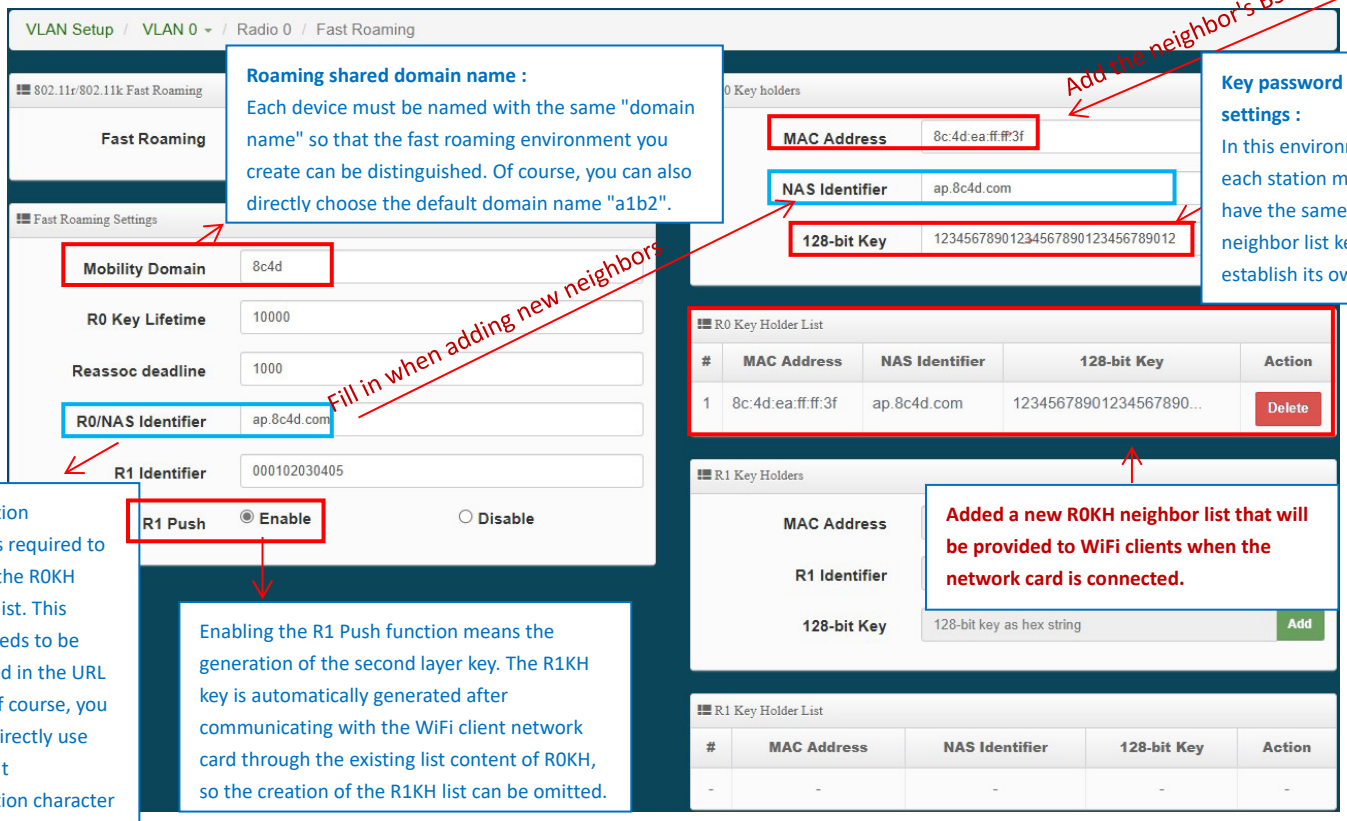
In the roaming 11r setting of Radio-0 (2.4G), you need to add neighbor 8c:4d:ea:ff:ff:3f in the roaming list (R0KH or R1KH list).

In the roaming 11r setting of Radio-1 (5G-1), you need to add neighbor 8c:4d:ea:ff:ff:40 in the roaming list (R0KH or R1KH list).

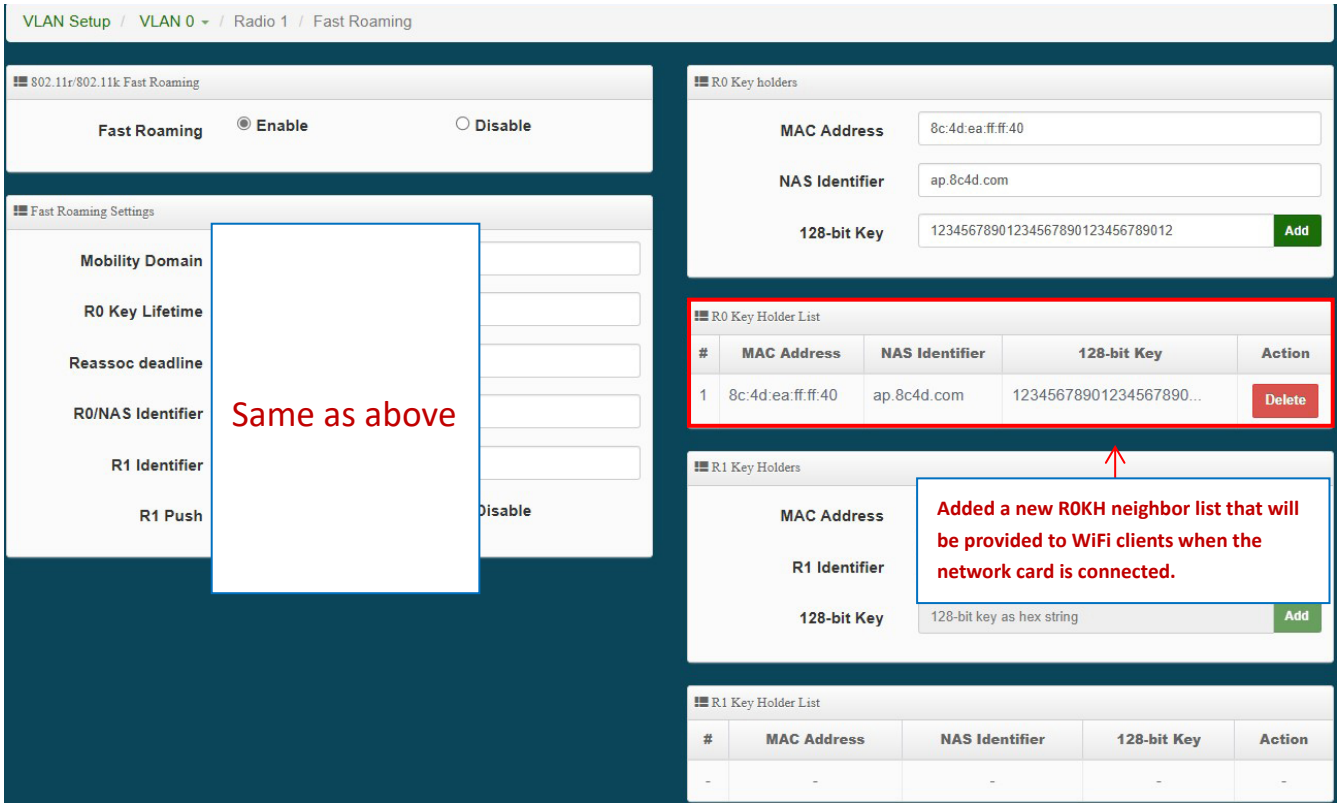
From the above to steps 1 to 3, the guide explains that after the WiFi client network card device is connected to the WiFi AP access point Understanding the basic operational relationship of 802.11r fast roaming formulated by the IEEE802.11 Association will quickly help you follow up on how to establish the R0/R1Key Holders (R0KH or R1KH) neighbor list settings for each device. The following continues to start with the setting page to guide the new roaming list:

1.) The neighbor of IP 251 WiFi AP is IP 252 WiFi AP, which means that IP251 WiFi AP must :

In the roaming 11r setting of Radio-0 (2.4G), you need to add neighbor 8c:4d:ea:ff:ff:3f in the roaming list (R0KH or R1KH list).

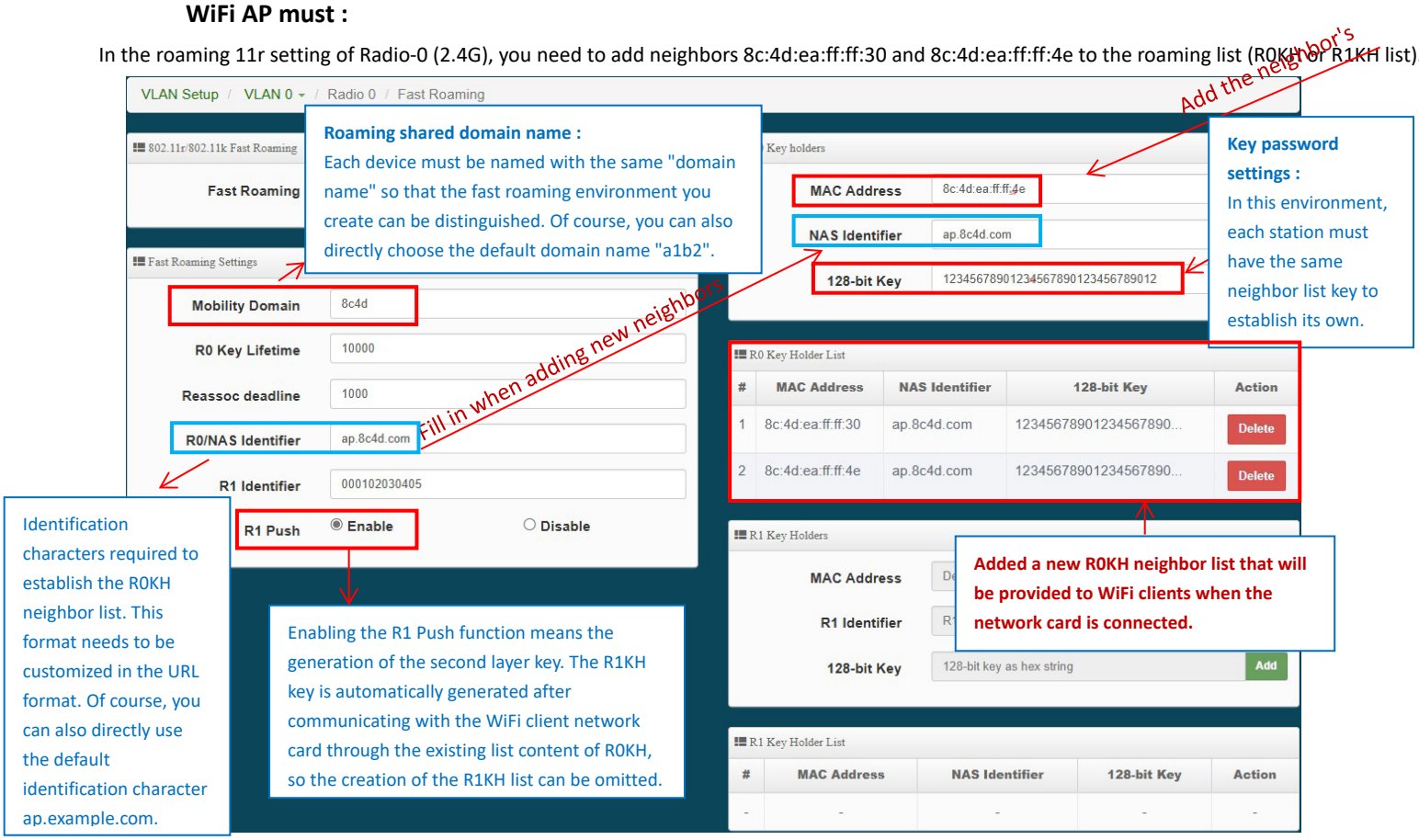


In the roaming 11r setting of Radio-1 (5G-1), you need to add neighbor 8c:4d:ea:ff:ff:40 in the roaming list (R0KH or R1KH list).

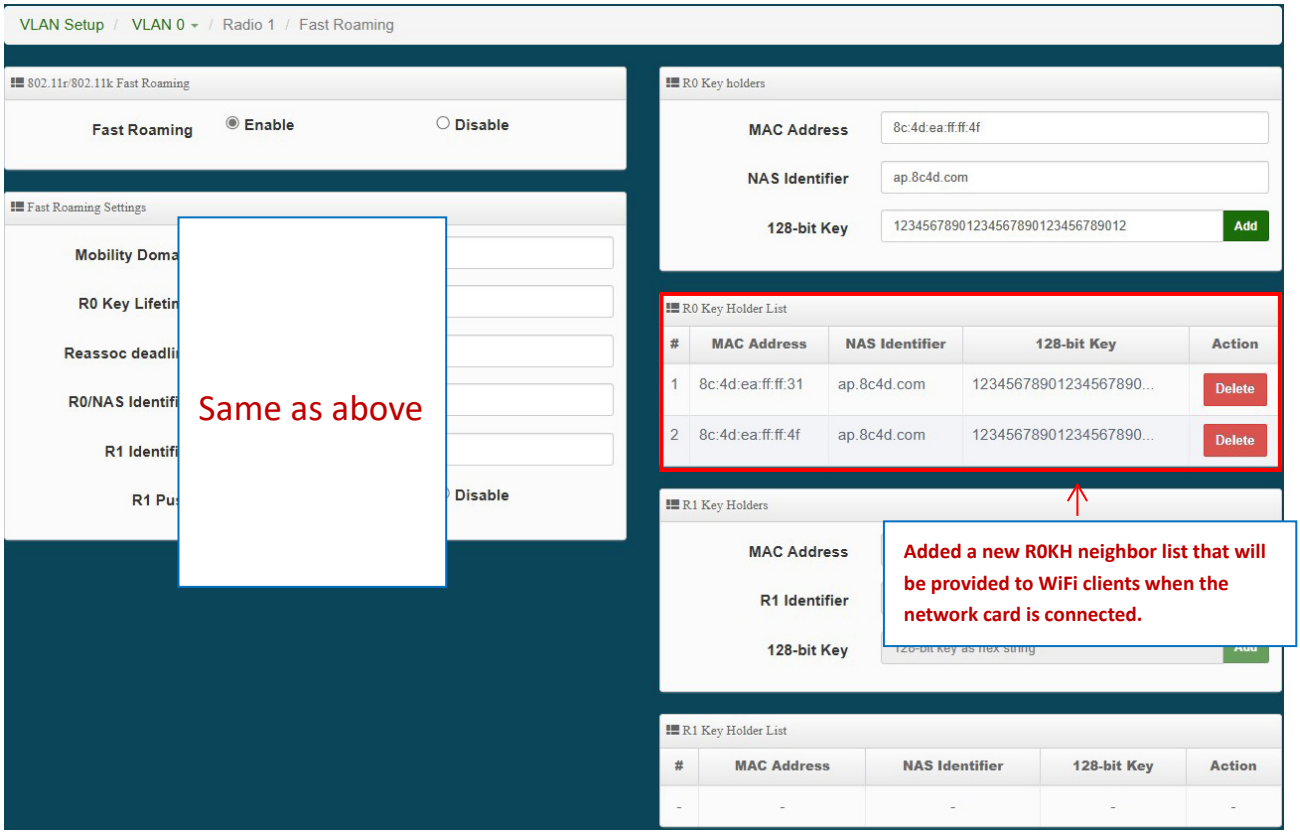


2.) The adjacent neighbors of IP 252 WiFi AP are IP 251 WiFi AP and IP 253 WiFi AP, which means that IP252 WiFi AP must :

In the roaming 11r setting of Radio-0 (2.4G), you need to add neighbors 8c:4d:ea:ff:ff:30 and 8c:4d:ea:ff:ff:4e to the roaming list (R0KH or R1KH list).



In the roaming 11r setting of Radio-1 (5G-1), you need to add neighbors 8c:4d:ea:ff:ff:41 and 8c:4d:ea:ff:ff:4f to the roaming list (R0KH or R1KH list).



3.) The neighbor of IP 253 WiFi AP is IP 252 WiFi AP, which means that IP253 WiFi AP must :

In the roaming 11r setting of Radio-0 (2.4G), you need to add neighbor 8c:4d:ea:ff:ff:3f in the roaming list (R0KH or R1KH list).

According to the diagram, the R0KH neighbor list that needs to be added is the same as IP251. Please refer to 1.) I will not repeat it here.

In the roaming 11r setting of Radio-1 (5G-1), you need to add neighbor 8c:4d:ea:ff:ff:40 in the roaming list (R0KH or R1KH list).

According to the diagram, the R0KH neighbor list that needs to be added is the same as IP251. Please refer to 1.) I will not repeat it here.

The necessary prerequisites for successful 802.11r seamless roaming setting are once again reminded as follows:

1. Environment Each Cerio WiFi AP "has been deployed with each other" with "overlapping signals at the roaming end".
2. Each Cerio WiFi AP uses the same channel, the same SSID name (ESSID) and the same WiFi encryption
3. For each Cerio WiFi AP" set its own relative "R0/R1Key Holders and other related AP neighbor lists"
4. The WiFi client network card (Client) connected to the Cerio WiFi AP must also support the same 802.11r/k roaming protocol

For more detailed settings, please refer to the relevant chapters such as "Wireless Base Station SSID", "Channel Settings" and 802.11r Fast Roaming in the manual.

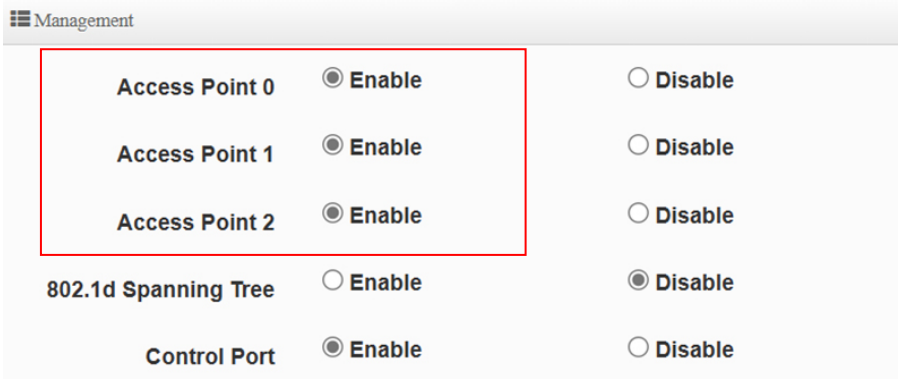
12-2. Point to Point / Multi-Point for WDS settings

The WDS function is applied in the wireless AP mode. This function is mainly used for point-to-point wireless AP bridging. For the setting method,You can **refer to the manual "WDS Setting"**. This document mainly guides the key WDS procedures. Can easily structure WDS point-to-point or point to multi point applications

1) If point-to-point bridging is used for WDS function, it is recommended to use our products to avoid compatibility issues.
2) If point-to-point bridging is used for WDS function, it is recommended to use our products to avoid compatibility issues.
3) According to the requirements to be applied to 2.4G or 5G, please make sure that each wireless AP sets a set of same channels **(please refer to the manual "Wireless Configuration" (Radio 0 or Radio 1 or Radio 2 Setup)**
4) Restart after confirmation will complete WDS point-to-point bridging, **please refer to the manual "WDS Status**" to confirm the RSSI value.The value If show to "-1" indicates that the connection is not successful, please re-confirm whether the configuration file follows the above instructions, or between APs. Signals are blocked by interference.
5) Please refer to WDS setting page, please set the MAC address information of other wireless for the wireless AP correctly. If two bridges, Radio A and Radio B, are used as examples, the MAC address information of Radio B must be entered in the MAC address list of Radio A of the site, and, the MAC address information of Radio A must be entered in the MAC address list of Radio B of the site.

Ps, The RSSI value is recommended to fall between 30 ~ 50. If over the RSSI value means the AP is too close to the AP. If below the RSSI value means the signal is not right or the distance is too far.

Remark: Because the WDS application is in the wireless AP mode, if the WDS function is enabled, it will be an AP + WDS application. If the wireless AP is not required to use the WDS function purely, **you can refer to the manual "VLAN Setup" instructions,** turn off the wireless AP, as shown below.

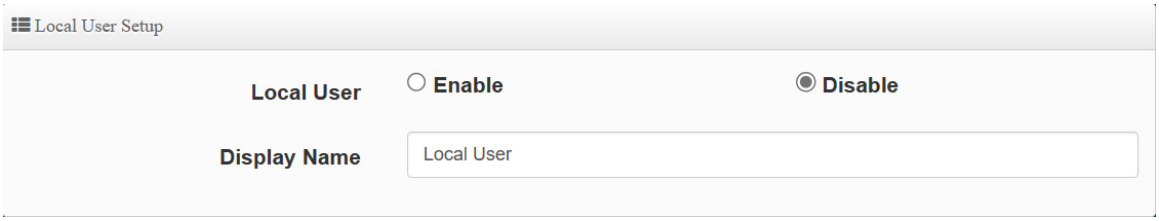


12-3. Apply CERIO web authentication login page sample

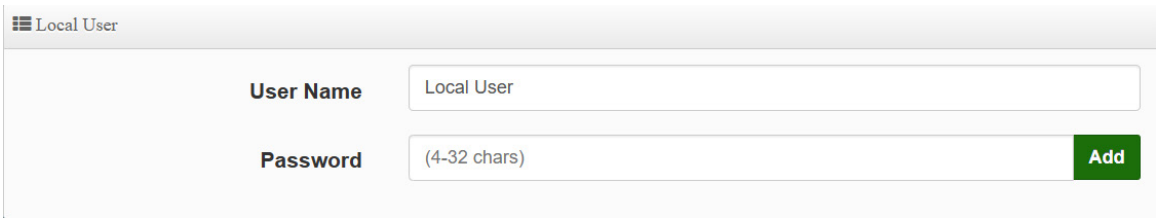
If the device uses our company's wireless AP CenOS5.0, and the web authentication function is enabled, you will be able to customize the web authentication page. You can follow the steps below to easily complete the sample login page.

Step 1 : Start the web page authentication function first, and in the “System” settings => “Authentication” function **(refer to Manual "Authentication” function)**

Step 2 : After confirming the activation, you can choose what type of login account to use. This step uses “Local User” as an example, and will “enable to create a Local User”. After confirming the activation, and “Save it”, See as follows.



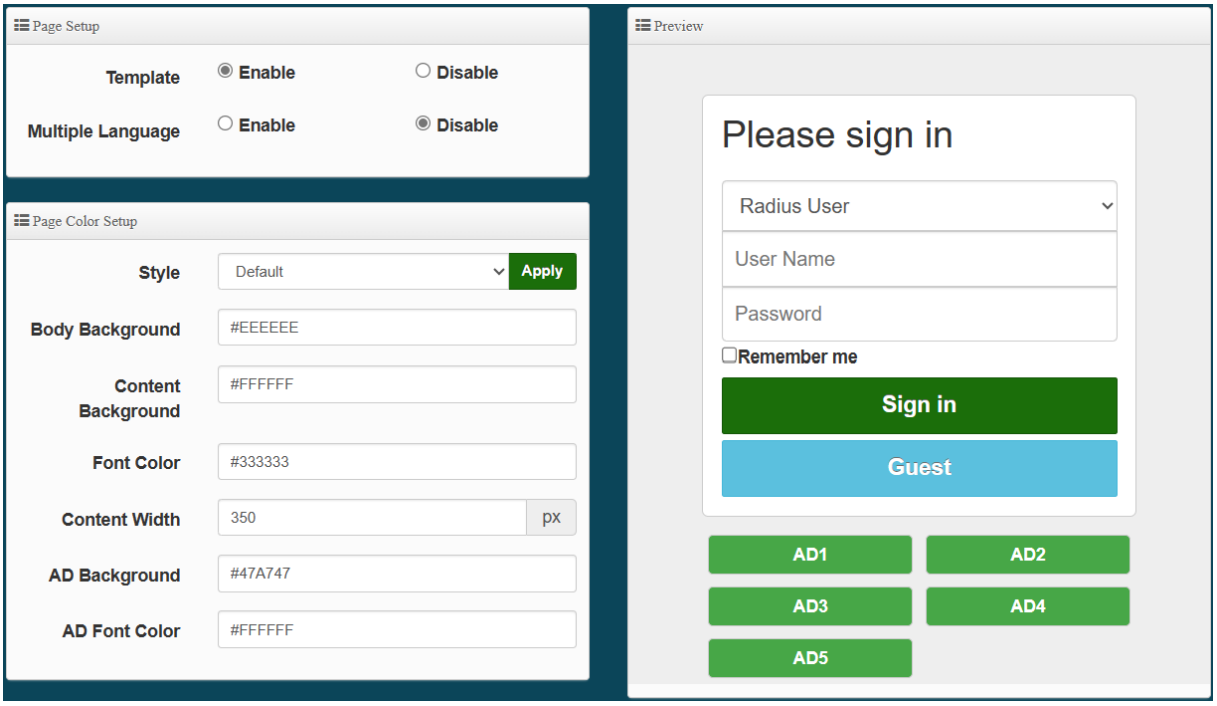
Step 3 : Please go to the pull-down function button of the authentication function, and enter the “User Name” and “password” , See as follows.



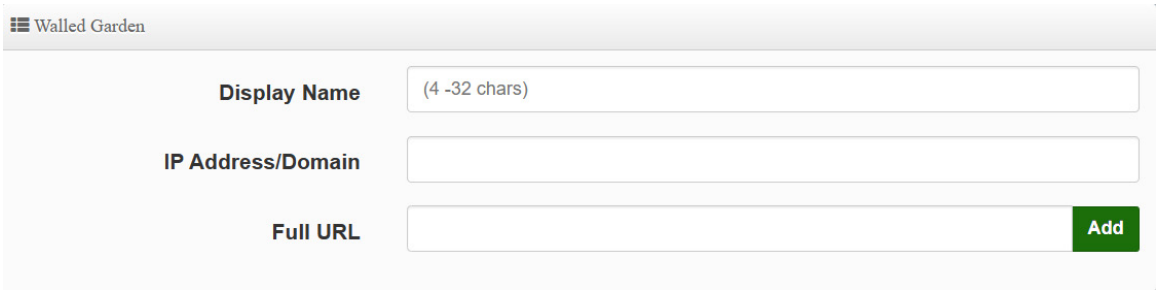
* If want to use the system preset page, please refer to **step 4,**
* If want to apply our template, please refer to below for **step 5,**
* If want to edit the webpage by yourself, please refer to **step 7**.

Remark ： If you want to edit the webpage by yourself, it is recommended that the administrator must have the basic ability to make webpages in HTML / CSS.) This department has no responsibility for webpage syntax guidance.

Step 4 : If you want to use the preset authentication page, you can refer to the instruction **manual “Customized Page”**, you will be able to set the preset. Format for color editing and revision, if you need to customize the page and apply our template, **please refer to step 5**

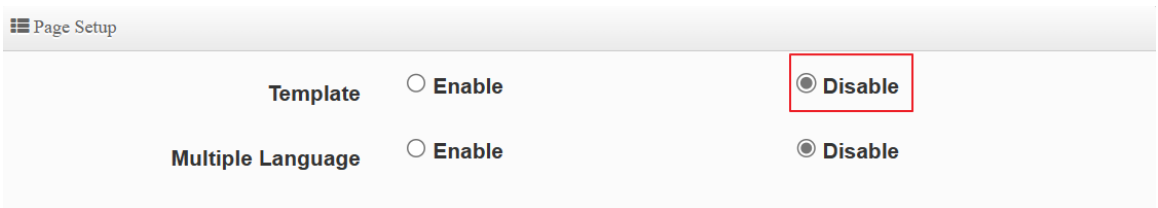


Step 5 : The image file of the login page must be placed on the website server, the website address must be whitelisted. The background image of this example is stored on below second server (URL: www.serio.com.tw), so please make sure Enter into Walled Garden.



Step 6 : Go to the company's Cerio website to download the sample file first. And open your download sample, select all the HTML syntax and copy it, then paste it on the custom edit page of the system and save it.

Download example address: https://www.cerio.com.tw/extreme-indoor/customized-page/



After clearing the HTML source code content, then paste all the downloaded source code into the field, save and restart the device, and you can finish editing the login page.

Customize HTML Source code

```
<html>
<head>
<title>Authentication Login Page ( On-line Web Demo Version )</title>
<link rel="stylesheet" type="text/css" href="http://www.serio.com.tw/login_page_demo
/sample3_en/format.css" />
<script src="/javascripts/login.js" charset="utf-8" type="text/javascript"></script>
<style type="text/css">
.t1 { color: #FFF;  background-color: #421f19;     text-align: center;}
.t1_a {font-size: 18px;  font-family: Century Gothic;}
.backg {background-image: url(http://www.serio.com.tw/login_page_demo/sample3_en
/newshop_background.jpg);}
.reme_font {
      font-size: 12px;
      height: 30px;
      line-height: 30px;
      text-align: center;
      color: #333;
      border-radius: 10px 10px 0px 0px;
      font-weight: bold;
}
.backg2 {background-image: url(http://www.serio.com.tw/login_page_demo/sample3_en
```

Login page for template below :

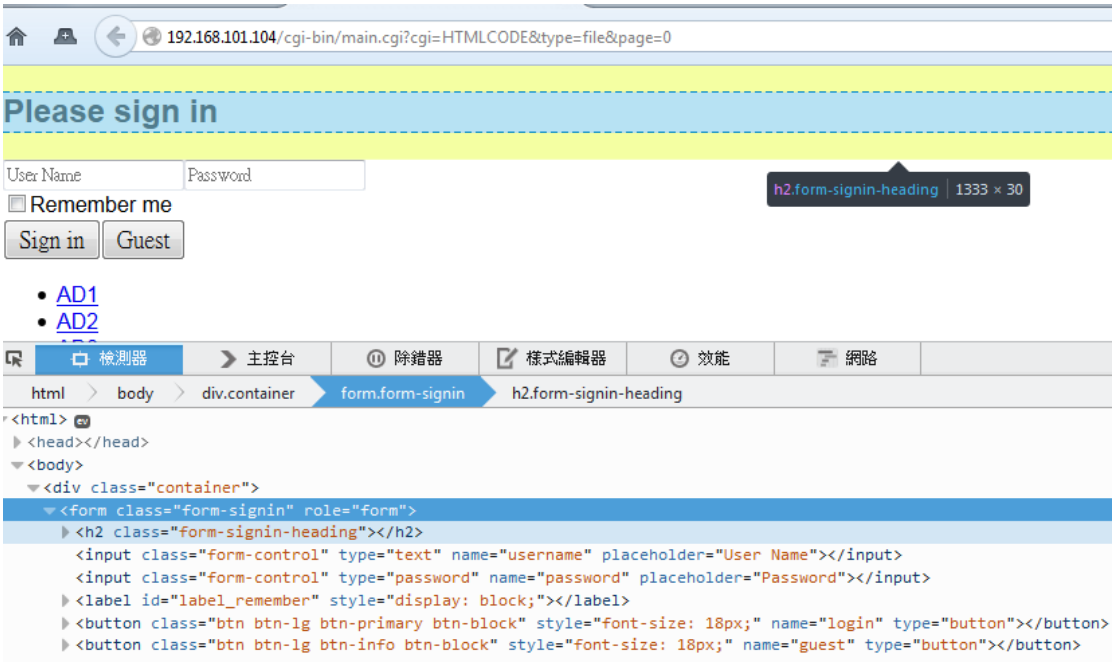
1. *This part must be within 190 lines. If the written HTML / CSS and other source code exceeds a certain line, it is recommended to save the CSS source code to the remote Web server, and then enter the IP address of the remote web server. Within Walled Garden. (Please refer to the manual "Walled Garden" setting instructions)*
2. *This device does not support the storage spaWce of picture files. If necessary, store the picture files on a remote web server and call the address recently, See as above.*

Step 7 : If the custom page is to be make by yourself, the original code of the following scarlet letters must not be removed, others will be able to make by themselves

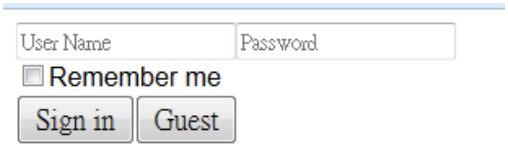
```
<html>
  <head>
        <title>Hotspot</title>
        <script src="/javascripts/login.js" charset="utf-8" type="text/javascript"></script>
  </head>
  <body>
        <div class="container"></div>
  </body>
</html>
```

Step 8 : The login function of this system is displayed by default. If there are unnecessary fields, specific fields can be hidden by CSS syntax, as explained below:

Add the **<style> class** tag in the syntax and then add **{display: none;} </ style>** as the following example, find the ID code of the field to be hidden by the browser, for example, to hide the **"Please "Sign in"** description, then find out its Class ID as shown below.



Add **<style> .form-signin-heading {display: none;} </ style>** in the head to hide the description **"Please Sign in"** as shown in the figure below, and find the Please Sign in word disappeared, and so on.



12-4. Regional 5Ghz WiFi channel related, country/region DFS (Dynamic Frequency

Frequency band/U-NII	Frequency/ (MHz)	Frequency / Bandwidth mode / Channel				Regional standards			
		20MHz	40Mhz	80Mhz	160Mhz	(US)	(Europe)	Japan	Taiwan
Band1 (U-NII-1)	5180	36	36~40 (38)	36~48 (42)	36~64 (50)	YES	Indoors	Indoors	Indoors
	5200	40				YES	Indoors	Indoors	Indoors
	5220	44	44~48 (46)			YES	Indoors	Indoors	Indoors
	5240	48				YES	Indoors	Indoors	Indoors
Band2 (U-NII-2A)	5260	52	52~56 (54)	52~64 (58)		DFS	Indoors/DFS	Indoors/DFS	Indoors
	5280	56				DFS	Indoors/DFS	Indoors/DFS	Indoors
	5300	60	60~64 (62)			DFS	Indoors/DFS	Indoors/DFS	Indoors
	5320	64				DFS	Indoors/DFS	Indoors/DFS	Indoors
Band3 (U-NII-2C)	5500	100	100~104 (102)	100~112 (106)	100~128 (114)	DFS	DFS	DFS	DFS
	5520	104				DFS	DFS	DFS	DFS
	5540	108	108~112 (110)			DFS	DFS	DFS	DFS
	5560	112				DFS	DFS	DFS	DFS
	5580	116	116~120 (118)	116~128 (122)		DFS	DFS	DFS	DFS
	5600	120				DFS	DFS	DFS	DFS
	5620	124	124~128 (126)			DFS	DFS	DFS	DFS
	5640	128				DFS	DFS	DFS	DFS
Band4 (U-NII-3)	5660	132	132~136 (134)	132~144 (138)	N/A	DFS	DFS	DFS	DFS
	5680	136				DFS	DFS	DFS	DFS
	5700	140	140~144 (142)			DFS	DFS	DFS	DFS
	5720	144				DFS	NO	NO	NO
	5745	149	149~153 (151)	149~161 (155)		YES	NO	NO	NO
	5765	153				YES	NO	NO	NO
	5785	157	157~161 (159)			YES	NO	NO	NO
	5805	161				YES	NO	NO	NO
	5825	165				YES	NO	NO	NO

*** DFS channels increase the number of channels users can choose. These additional channels are shared for specific military radars, satellite communications, and weather radars. The channel sharing process will undergo a pre-use availability check process (CAC) and follow the automatic avoidance and channel hopping mechanism. For point-to-point or point-to-multi "WDS and other modes" that need to be bound to fixed channels, when one of the sites avoids frequency hopping, it will cause multi-point or multi-point wireless interruption and will need to be reset again. If it is not a simple "Access Point station mode", etc., it is for wireless network card storage. For channel-specific settings such as Internet access or "Client Bridg mode", it is recommended that you try not to use DFS shared channels.**

Appendix. WEB GUI Valid Characters

Table A WEB GUI Valid Characters

Block	Field	Valid Characters
LAN	IP Address	IP Format; 1-254
	IP Netmask	128.0.0.0 ~ 255.255.255.252
	IP Gateway	IP Format; 1-254
	Primary DNS	IP Format; 1-254
	Secondary DNS	IP Format; 1-254
	Hostname	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
DHCP Server	Start IP	IP Format; 1-254
	End IP	IP Format; 1-254
	DNS1 IP	IP Format; 1-254
	DNS2 IP	IP Format; 1-254
	WINS IP	IP Format; 1-254
	Domain	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	Lease Time	600 ~ 99999999

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
Management	System Name/ Location	Length : 32 0-9, A-Z, a-z Space ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	Description	32 chars
	Password	Length : 4 ~ 30 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	HTTP/ HTTPS Port	1 ~ 65535
	Telnet/ SSH Port	1 ~ 65535
SNMP	RO/RW community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; `, . =
	RO/RW user	Length : 31 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; `, . =
	RO/RW password	Length : 8 ~ 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; `, . =
	Community	Length : 32 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] ; `, . =
	IP	IP Format; 1-254
General Setup	Tx Power	1-100 %
Wireless Profile	Profile Name	32 chars
	ESSID	Length : 31 Space 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Pre-shared Key	8 ~ 63 ASCII chars; 64 HEX chars
Advanced Setup	Beacon Interval	20 ~ 1024
	Date Beacon Rate	1 ~ 255
	Fragment Threshold	256 ~ 2346
	RTS Threshold	1 ~ 2347

Table B WEB GUI Valid Characters (continued)

Block	Field	Valid Characters
Virtual AP Setup	ESSID	Length : 31 Space 0-9, A-Z, a-z ~ ! @ # $ % ^ * ( ) _ + - { } | : < > ? [ ] / ; `, . =
	Maximum Clients	1 ~ 32
	VLAN ID	1 ~ 4094
	WEP Key	10, 26 HEX chars or 5, 13 ASCII chars
	Group Key Update Period	>=60 seconds
	PMK Cache Period	> 0 minute
	Pre-Shared Key	8 ~ 63 ASCII chars; 64 HEX chars
	Radius Server IP	IP Format; 1-254
	Radius Port	1 ~ 65535
	Shared Secret	8 ~ 64 characters
	Session Timeout	>= 60 seconds; 0 is disable
WDS Setup	AES Key	8 ~ 63 ASCII chars; 64 HEX chars
	Peer's MAC Address	12 HEX chars
	Description	32 chars
IP Filter	Source Address	IP Format; 1-254
	Source Mask	0 ~ 32
	Source Port	1 ~ 65535
	Destination Address	IP Format; 1-254
	Destination Mask	0 ~ 32
	Destination Port	1 ~ 65535
MAC Filter	MAC address	MAC Format; 12 HEX chars
Virtual Server	Description	32 chars
	Private IP	IP Formate; 1-254
	Private/ Public Port	1 ~ 65535