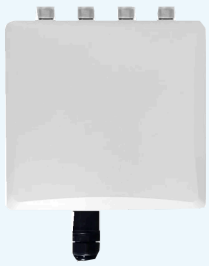
NWA3000 & NWAO3000 Access Point User Manual

Select your model before installing or configuring the access point.



NWA3000

Indoor ceiling access point. See the appendix for the indoor mounting, port and LED diagrams, connection steps, and web interface screenshots.



NWAO3000

Outdoor IP67 access point. The series datasheet lists one 2.5 GbE RJ45 WAN port with PoE input. Connect using that port.

NWAO3000 port layout



Ethernet: One 2.5 GbE RJ45 WAN port with PoE input. The Ethernet cable enters through the gland on the bottom edge.

Reset: The datasheet lists a reset button. Its position is unmarked in this view.

Choose a management method

Both models support stand-alone operation or central management with the NWAC128 as listed in the Wireless & Router datasheet v1.5. Check the firmware in use before adopting a unit into a controller.

Model-specific instructions. The supplied hardware diagrams, factory defaults, and screenshots in the appendix are for the NWA3000. For the NWAO3000, use the device label and its supplied installation instructions for mounting, seals, and power details. Ask Niveo support to confirm the setup details if those instructions are missing.

Set up the access point

1. **Identify and mount the unit.** Check the model on the label. Use the ceiling installation diagrams in the appendix for the NWA3000. For the NWAO3000, follow the installation instructions supplied with the outdoor unit.
2. **Connect power and network.** Use the PoE input specified for your model and confirm Ethernet link. The NWAO3000 uses its single WAN/PoE port for this connection.
3. **Locate the unit.** For a controller-managed installation, use the NWAC128 to discover the unit and check its model and firmware. For a stand-alone installation, use the unit's documented management address or, if the unit was assigned an address by DHCP, locate its lease by MAC address.
4. **Configure wireless service.** Select the installation country and set the SSIDs, security, and VLANs required by the site. Apply centrally managed settings on the controller. For stand-alone configuration, use the menus available in the unit's firmware.
5. **Verify operation.** Confirm that a client can join the SSID and receive an address on the intended network. Record the installed model and firmware version. Change any factory credentials during commissioning and save a configuration backup.

> **NWA3000 first connection.** The source manual identifies **192.168.100.1** as the management address for the illustrated firmware, but gives a different subnet in its wired example. Put the commissioning computer on the same subnet as the unit's confirmed management address. If the confirmed address is 192.168.100.1/24, use an unused address in 192.168.100.0/24 for the computer.

NWA3000 appendix

The appendix preserves the v1.2 reference diagrams and web interface walkthrough. It covers status, operating modes, wireless settings, controller management, diagnostics, configuration backup, firmware and restart. Use the firmware package approved for the exact model and hardware revision.

For model-specific assistance, contact ___ .

1. Product Introduction

1.1: LED indicator definition



Front

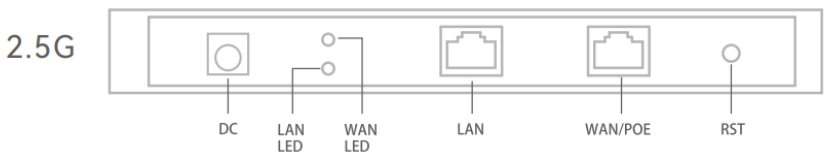


Back

Three LED Indicator	Designation	Normal Status	Explanation
	SYSTEM LED	Bright	System boots up successfully
		Flashing	System reset default
	2.4G LED	Flashing	2.4G Wireless boots up successfully
	5.8G LED	Flashing	5.8G Wireless boots up successfully

*The number of LEDs for different models of ceiling mount AP will be different, please refer to the actual product.

1.2: Ports Definition



Ports & Buttons	Explanation
DC Socket	Power input port
LED Indicator	LED indicator will bright up when Ethernet cable is connected to WAN/LAN ports
Reset Button	Reset device to factory default settings ,press it for 10 seconds when powered on, device will reboot
WAN PoE	Connect to internet through modem or broadband; Under AP and mesh mode, WAN port will be changed to LAN port; It it PoE port also.
LAN Port	LAN port can connect LAN device

* The interface for different models of products may be different, the above diagram is only for reference , pls refer to the actual product !

- **Operation environment**

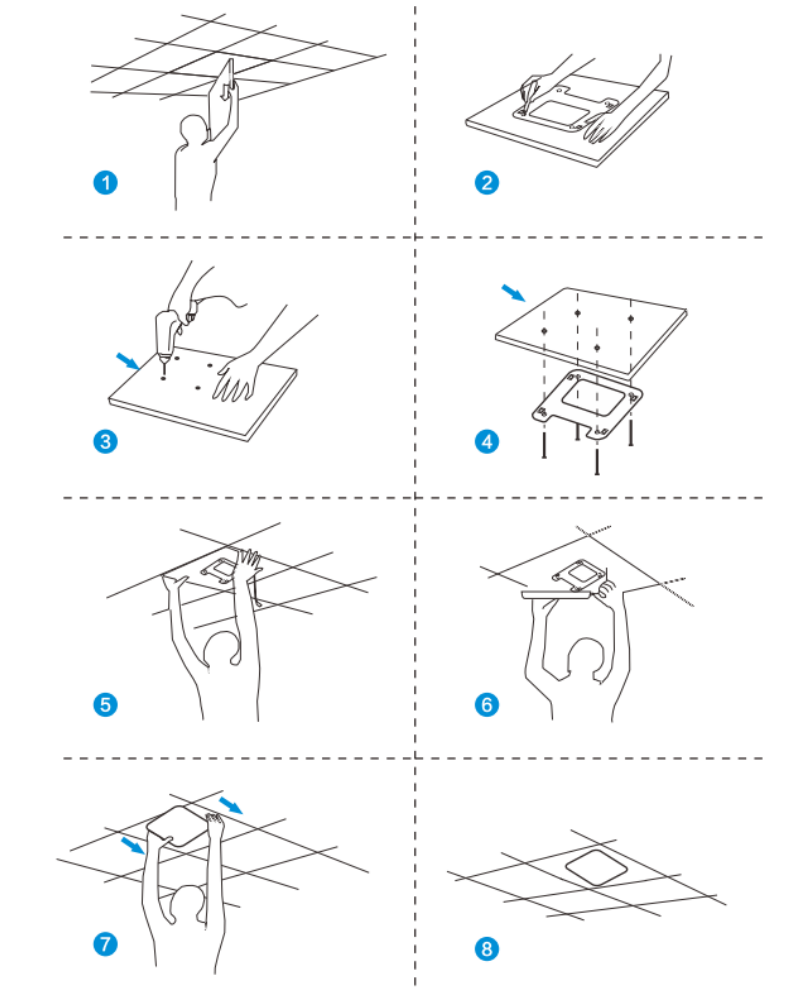


Suitable for safe use in areas below 2000 meters above sea level

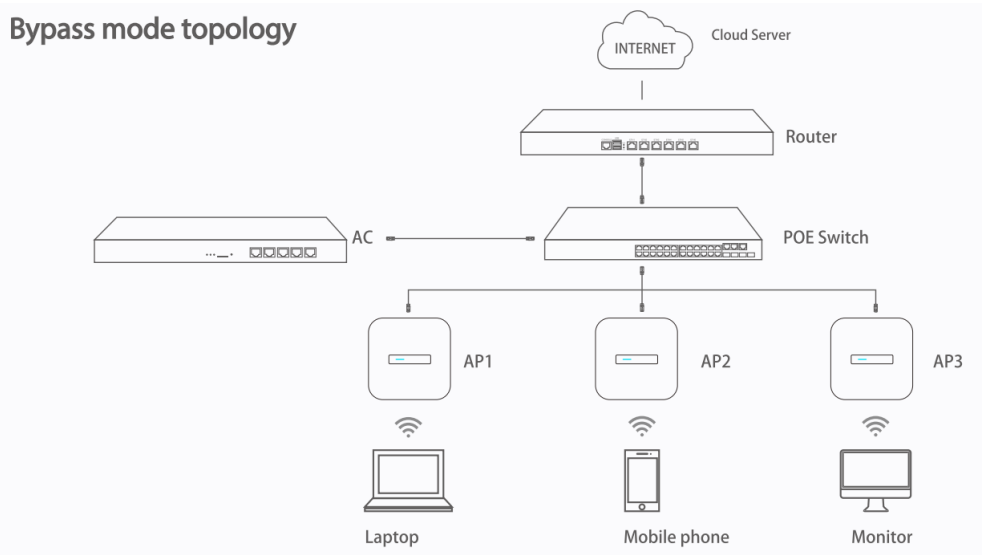


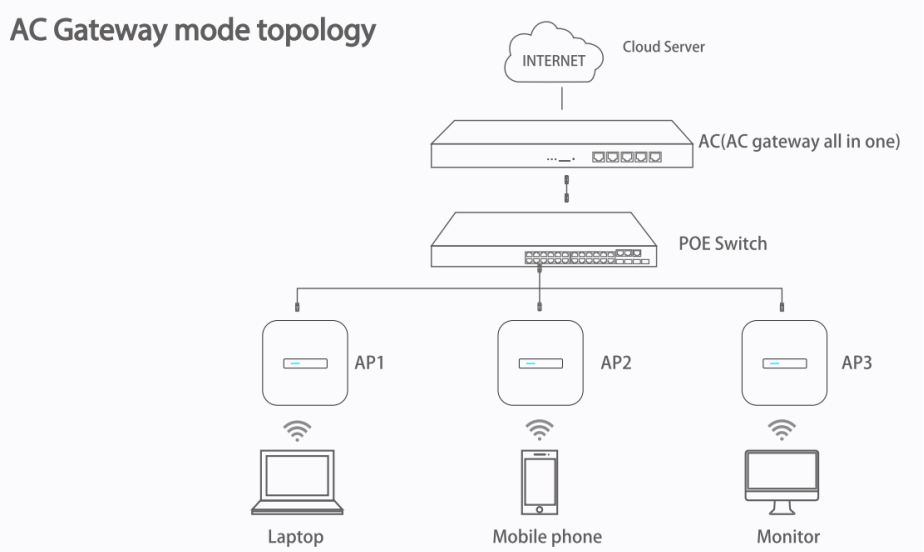
Only Suitable for safe use in non-tropical climatic conditions.

1.3 Device Installation



1.4: Device Network Topology





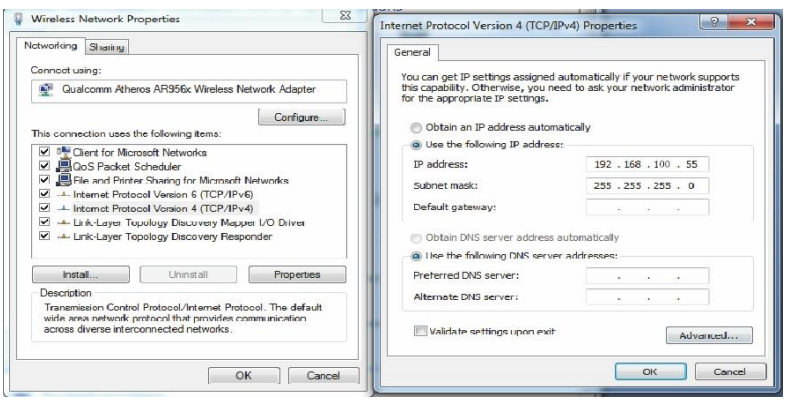
Tips:

1. The wireless AP is a standard 48V PoE device, pls use a standard IEEE 802.3af/at PoE switch or PoE adapter, or wireless AP will be damaged;
2. When deploy a large wireless network, there are many APs and there is a router in the network, it is recommended to use a wireless AC controller to centralized manage all wireless APs in the network;
3. When there is no router in the network, it is recommended to use our AC controller & gateway to do the router and AP management, support VPN, VLAN... Or if our AC controller access into cloud, it support SD-WAN;

2. Device Connection

2.1 Connect device to PC by wireless

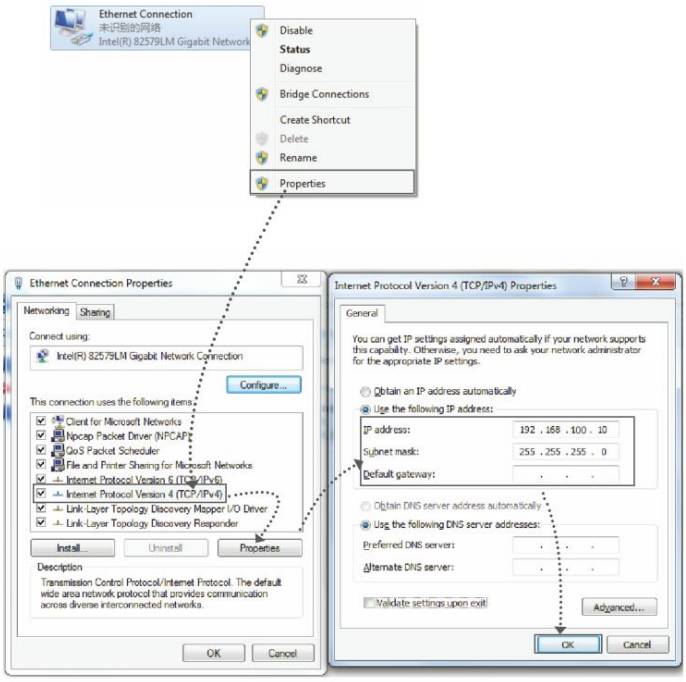
(1) To connect an AP wirelessly, please set the IP address of the TCP/IP properties of the wireless network card to 192.168.100.X (X is number range of 3-252) first, so that the AP and PC in the same IP segment, and set the subnet mask to 255.255.255.0, as shown in the following picture:



After setting the IP address of PC, connect PC with AP in wireless, double-click "Wireless network connection", in the pop-up wireless SSID list, select "Wireless 2.4G", click "Connect", then enter the password in the pop-up password dialogue box, the default password is"12345678", click "OK" to connect

2.2 Connect device to PC by wired

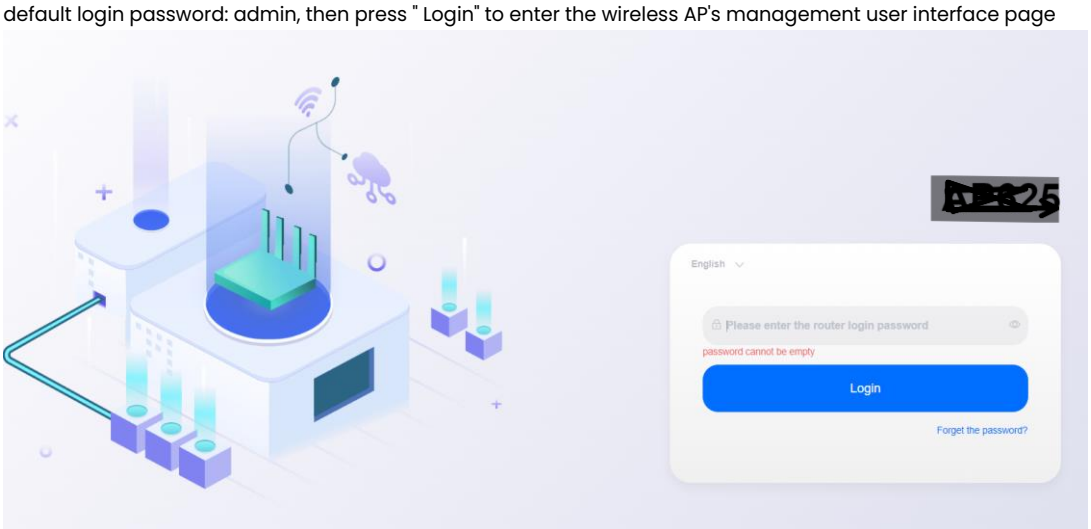
Connect the wireless AP's LAN port by LAN cable, set the IP address of the TCP/IP properties of the wired network card to 192.168.1.X (X is number range of 3-252), and the PC will be the same IP segment as AP



3 Device Web Interface Login and settings

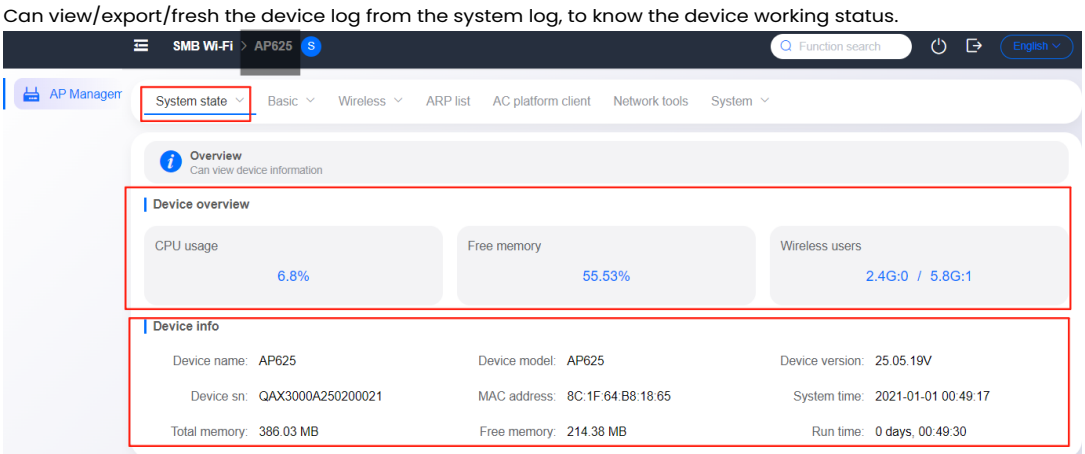
3.1 Device login and System state

3.1.1 Open Internet Explorer to visit http://192.168.100.1, pop up the login page shown in the following picture, input the default login password: admin, then press " Login" to enter the wireless AP's management user interface page



3.1.2. In the AP manager page, it will show the AP's information, such as CPU usage, memory, MAC address, wireless users, device model, Serial number, firmware version, system time and running time;

Can view/export/fresh the device log from the system log, to know the device working status.

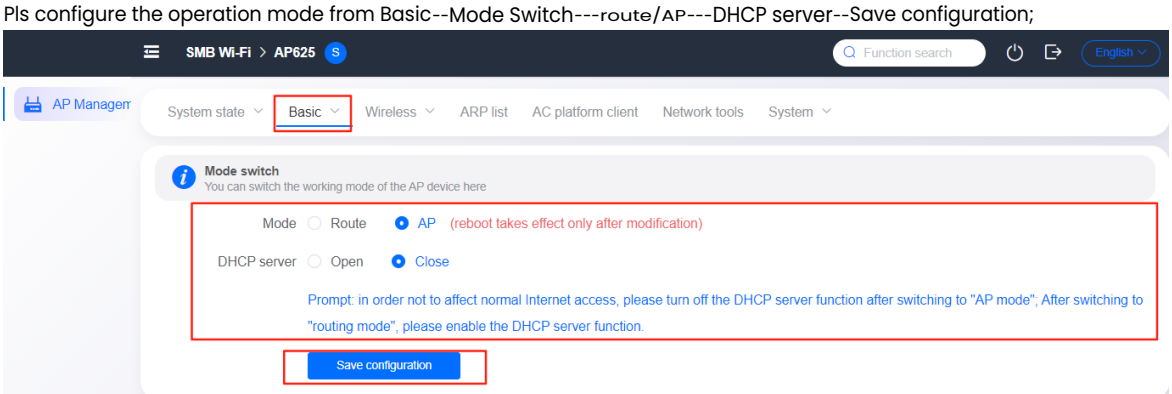


"S" mean it is AP operation mode, "M" mean it is in router mode; can switch to router mode in Basic settings,
Run time: the time is calculated from system running; Device info: show the CPU and memory usage;
Wireless users: show the users connection status in this wireless AP;
System log: can view/export/fresh the device log, to know the device working status.

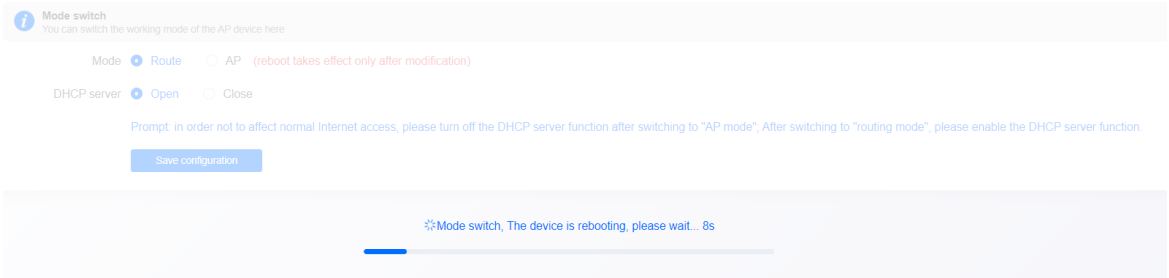
3.2 Basic Function settings

3.2.1: Operation mode settings:

It support wireless access point and wireless router operation mode;
Pls configure the operation mode from Basic--Mode Switch---route/AP---DHCP server--Save configuration;



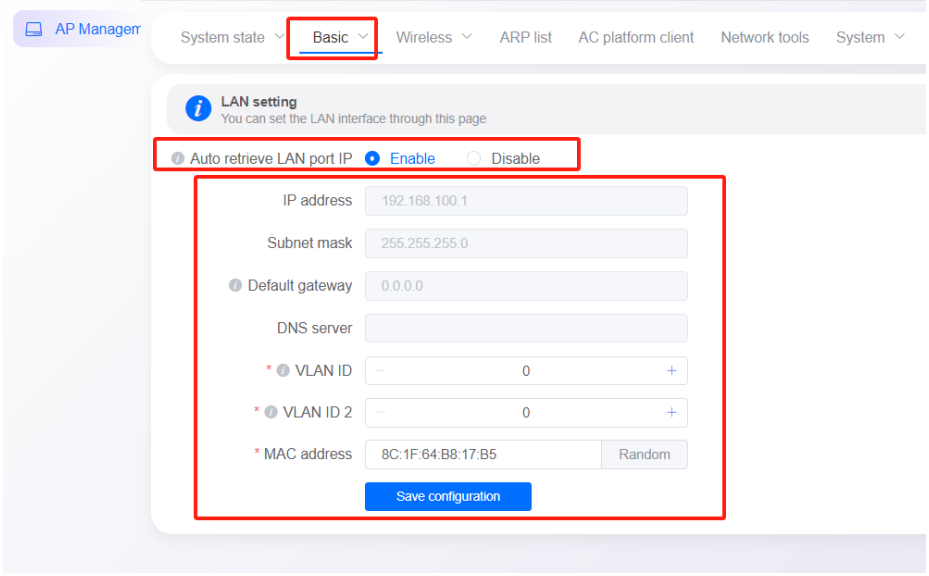
AP mode: it is AP mode in default, it is for wireless coverage for large area, which will connect to router/firewall on the top side by cable. In this mode,the NAT, DHCP, firewall and all WAN related functions will be turned, all wireless and wired interface will be bridged together, all RJ45 ports are LAN ports
Router mode: Connect Ethernet to the WAN port, static IP, DHCP, or PPPOE to convert Ethernet into wireless network and local area network through static IP, DHCP or PPPoE. Users obtain the WAN IP from this router. In this mode, NAT, DHCP servers, etc. are enabled by default, one RJ45 port is WAN port, one RJ45 is LAN port
DHCP server: mean assign the IP address for users. Normally it is close in AP mode, Open in route mode.



Pls note that the device will be rebooted if change the operation mode.

3.2.2: LAN settings

LAN setting mean the Internal network connection method, the IP acquisition method of AP devices
In the LAN settings, including the IP address, subnet mask for the device, DNS server and VLAN ID;

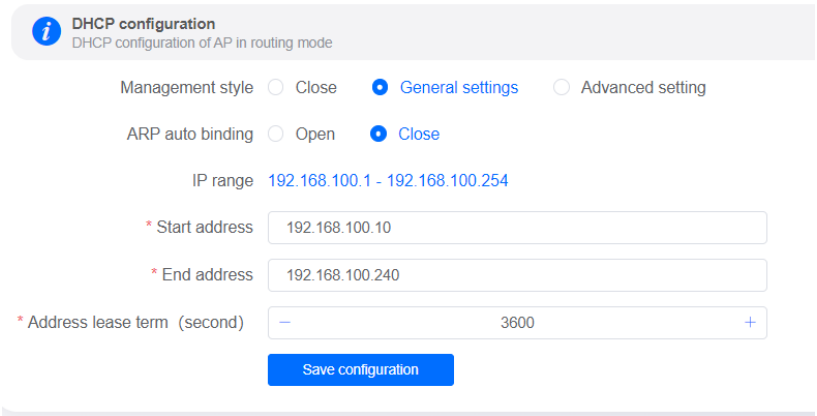


Auto retrieve LAN port IP: Enable mean the IP is allocated and managed by AP controller; Disable this AP is not managed by AP controller, can modify the device’ s login IP address, Subnet mask, default gateway and DNS server.

VLAN ID: there are 2 VLAN ID for this device, mean can set special VLAN ID for this LAN port; If work with AP controller, copy the LAN VLAN ID from AP controller to AP.
MAC address: Modify the MAC address based on the internal network. Generally, the default MAC address is available, no need to be adjusted;

3.2.3: DHCP Configuration

DHCP configure: Set the IP address range of the connected device, it is the function under router mode;
In AP mode, it is closed in default to avoid IP address conflict, because the users will obtain the IP address from gateway, not from this AP;
Here introduce the DHCP function under router mode.



In general settings, it will set the DHCP IP address range for end users.
Start address：The start address of the IP automatically assigned by the DHCP server. The range of the starting address is within the network segment calculated by the IP address and subnet mask;
End address：The end address of the IP automatically assigned by the DHCP server. The end address range is within the network segment calculated by the IP address and subnet mask.
Address lease time (seconds) ： The validity period of the automatically assigned IP. After this period, the devices in the LAN will re-acquire the IP address.

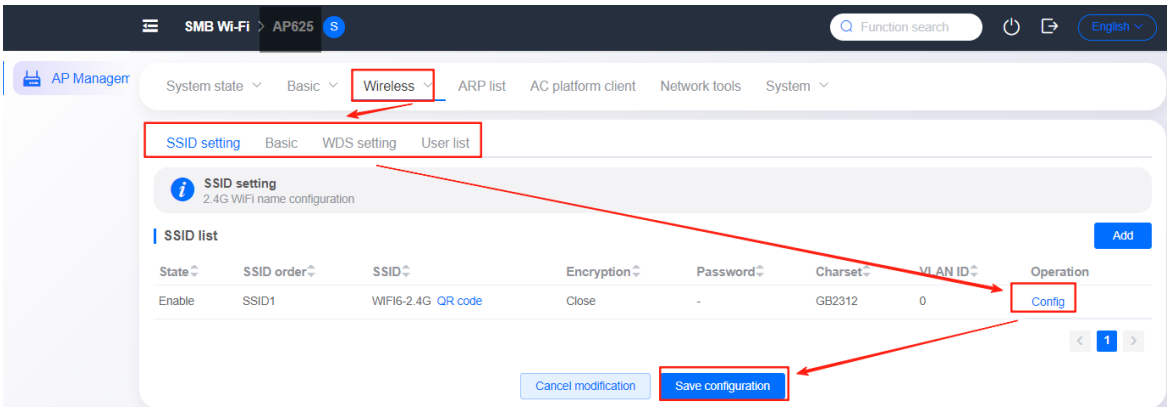
In advanced setting, it will set the DHCP gateway, Subnet mask, DNS server...
DHCP gateway：The default gateway address assigned by the DHCP server. This address is automatically changed according to the above “Start Address”. For example, if the start address is filled in as 192.168.100.10, the DHCP gateway address here is automatically updated to 192.168.100.1
Subnet mask：The default is usually 255.255.255.0. Change the mask range as needed；
Preferred DNS server: Fill in the DNS server. The preferred server will be used as the first DNS server
Alternate DNS server: Fill in the alternate DNS server. When the preferred server cannot be used normally, the alternate server will continue to work
Custom Option: Select and configure Option as needed. When any LAN port configuration or modification is submitted, the device will automatically restart to save and read the latest configuration data.

3.3 Wireless Function settings

In this part, mainly to set WiFi 2.4G and 5G wireless parameters, specify MAC address for terminal failure to connect, turn off WiFi during scheduled time, and configure advanced WiFi parameters

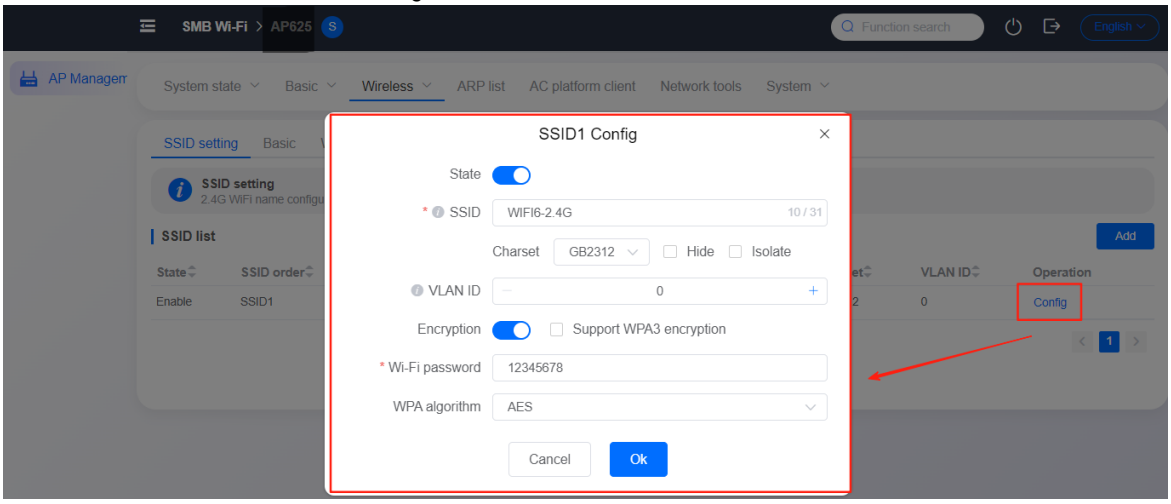
3.3.1 SSID setting

Click Wireless, select 2.4G or 5G wireless, click add to create more SSIDs; Click Config to modify the data of main or slave SSID.



SSID setting: there is one SSID in the SSID list, this is the main SSID,

Add: mean can create multiple SSIDs for this wireless AP, max 8 SSIDs can be added in 2.4G or 5G; Multiple SSIDs are used to create WiFi for different VLANs or guest WiFi.



State: enable or disable wireless SSID.

Hide: enable, mean SSID is not viewable;

Isolate: enable, mean the users can't communicate each other even they access into same AP.

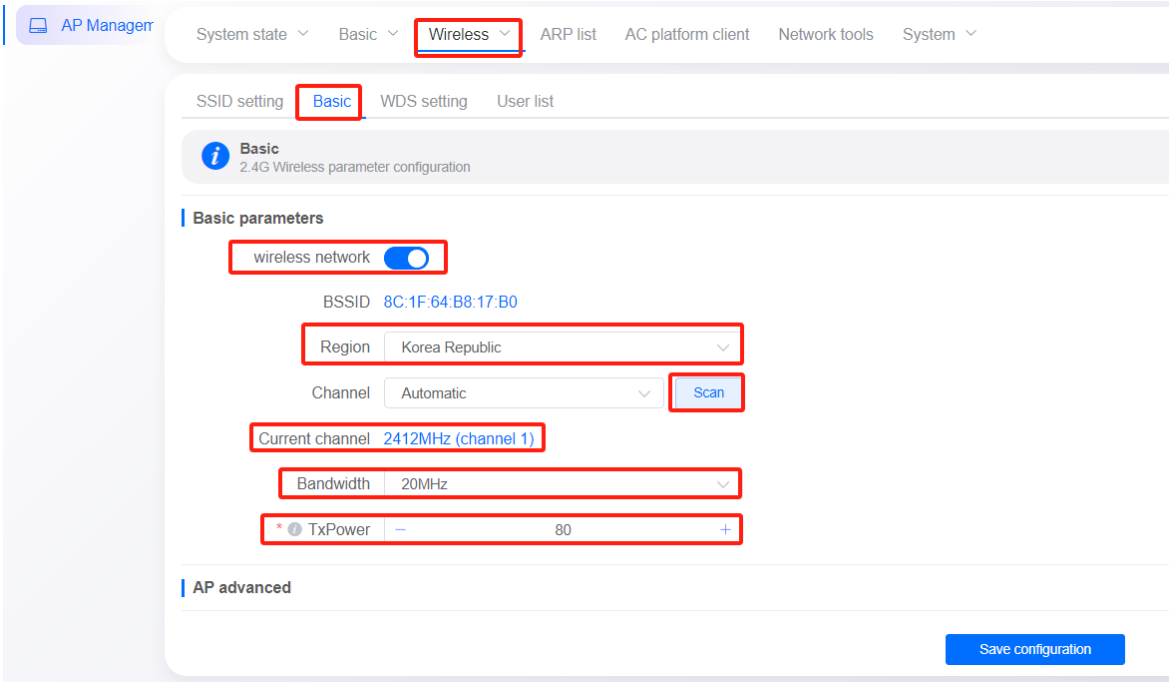
VLAN: Input VLAN ID to banding VLAN ID with SSID, to complete data isolation

Encryption: WPA/WPA2PSK hybrid encryption, if WPA3PSK is selected, the non WPA3 supported users will be unable to connect to WiFi.

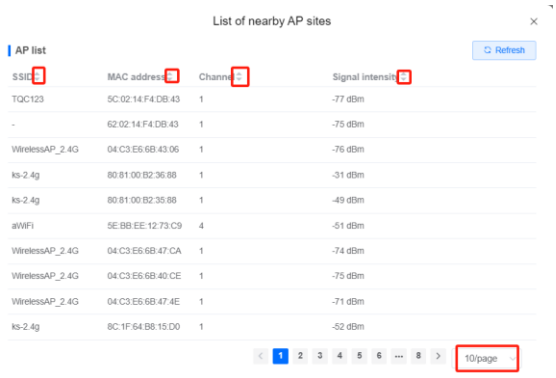
WiFi password: The length requirement is at least 8 characters or more.

3.3.2 Basic setting of SSID

In Basic setting on SSID, mainly to select the correctly country code, set channel, bandwidth and TxPower.

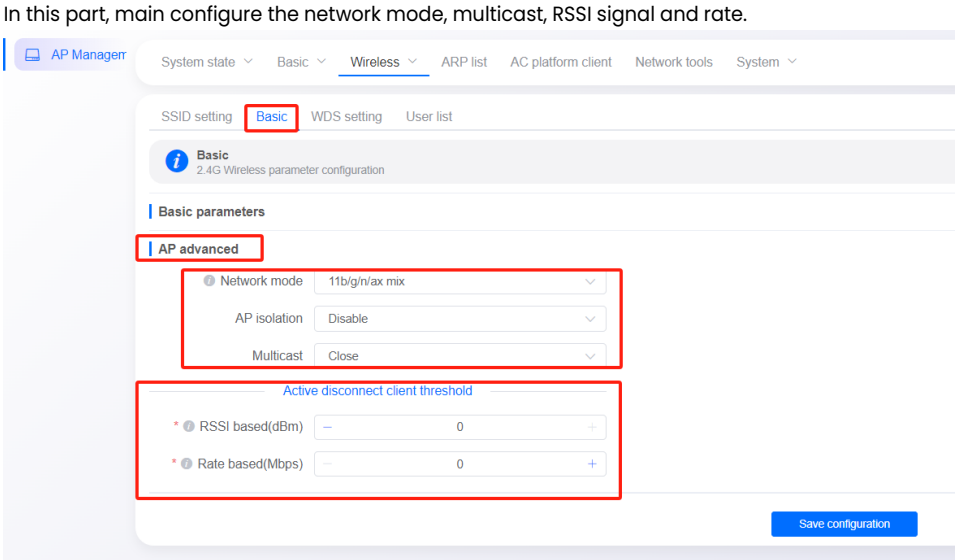


Bandwidth: the higher the bandwidth, the faster speed, but wifi range will be shorter;
TX Power: Mean the RF power, 100 mean more RF power, more range;
Channel: support auto channel or fix channel, if select the fix channel, better to scan the wifi channels of nearby wireless AP, to decrease the wifi interface, click Scan to view the nearby SSID, signal strength and channel.



3.3.3 Advanced setting of SSID

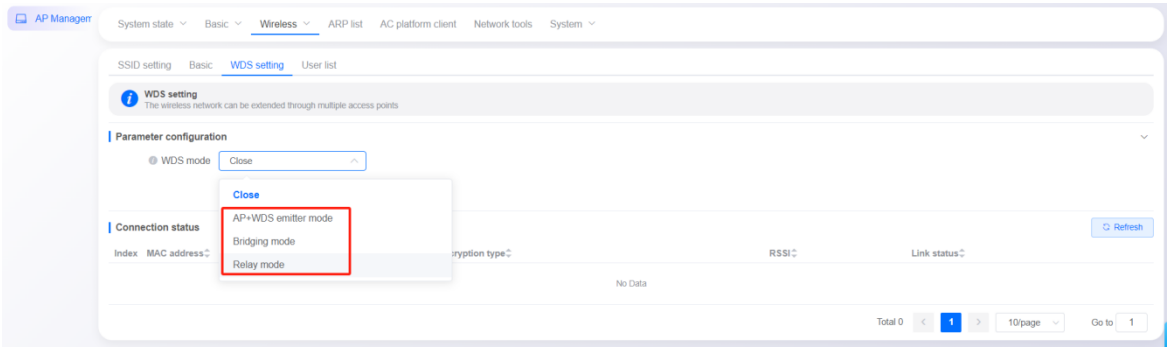
In this part, main configure the network mode, multicast, RSSI signal and rate.



Network mode: refers to the highest supported bandwidth. Generally, please use the default 11b/g/n/ax mixed for 2.4G, 11ax/ac/an in 5G;
AP Isolation: Enable or disable AP isolation, mean APs will be isolated in same network.
Multicast: Enable or close multicast;
Close, the multicast function is closed and does not take effect;
Multicast-to-multicast can achieve the purpose of transmitting data to all target nodes at once or only transmitting data to specific objects;
Multicast to unicast is generally used in multicast videos to make the video smoother;
RSSI based: Switch the wireless roaming based on the signal strength of the wireless terminal. If the trigger roaming RSSI threshold is set to -70 and the terminal signal strength is -80, the system will automatically disconnect the wireless network and switch the terminal wireless network to a wireless network with better signal strength. The signal strength range is -95 to -50, and a value of 0 means that signal strength detection switching is not enabled;
Rate based: The principle is the same as RSSI based, but the standard is different. The setting range of rate detection is 0-99. Generally, please take the default value.

3.3.4 WDS setting

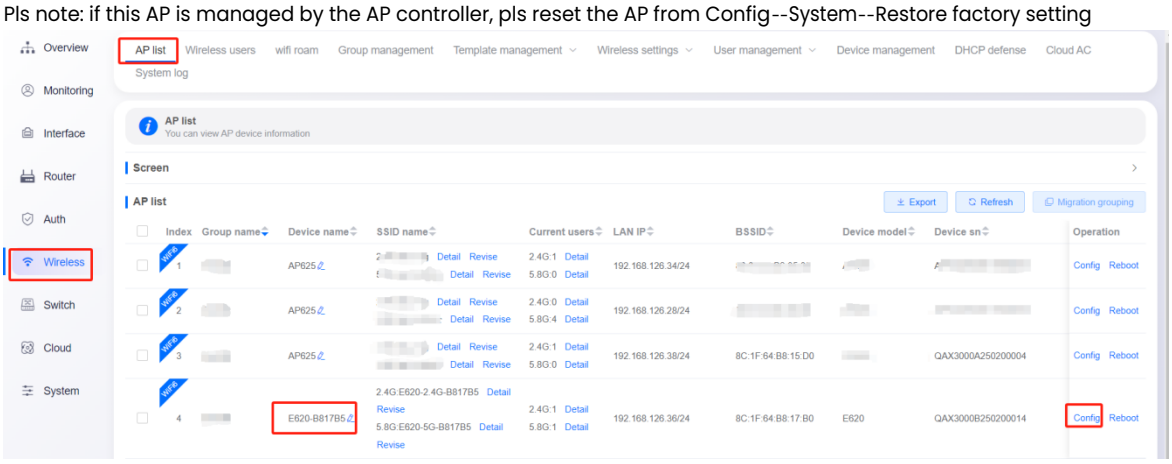
In WDS setting, it mean this AP can work as Wi-Fi bridge or Wi-Fi repeater.
Close in default mean this device is work as router or AP mode;
Enable mean there are two devices, one is AP+WDS emitter mode, one is bridge or relay mode;
Or one device that 2.4G is in bridge mode, 5.8G is AP mode.



AP+WDS emitter mode: under this mode, the two WDS device should be with same frequency.

Bridge mode: If there is an AP/wireless router, if 2.4G is used to receive the wifi signal from AP/wireless router, then 5G signal is used for wifi coverage for users. Under this mode, this device' s LAN IP address will be obtained from the bridged gateway. Should configure this device from gateway as showed in below;

Pls note: if this AP is managed by the AP controller, pls reset the AP from Config--System--Restore factory setting

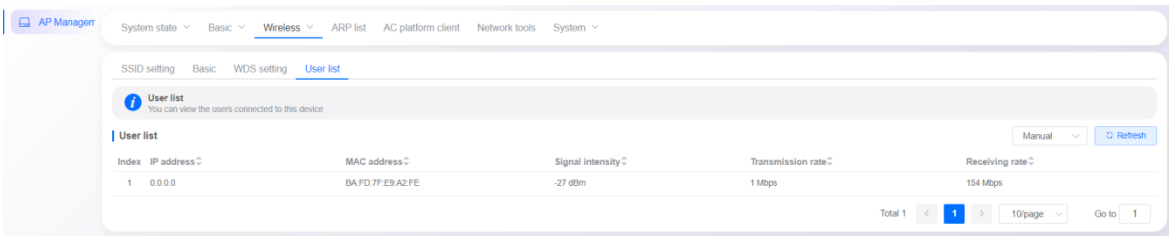


Relay mode: it is repeater operation mode, regeneration and amplification of signals from the AP, while bridging focuses on transmitting and connecting data from the AP. These functions are used in situations where physical lines are difficult to traverse.

3.3.5 User list

Under user list, it will show IP address, MAC address, signal strength, data rate of all the accessed wireless users

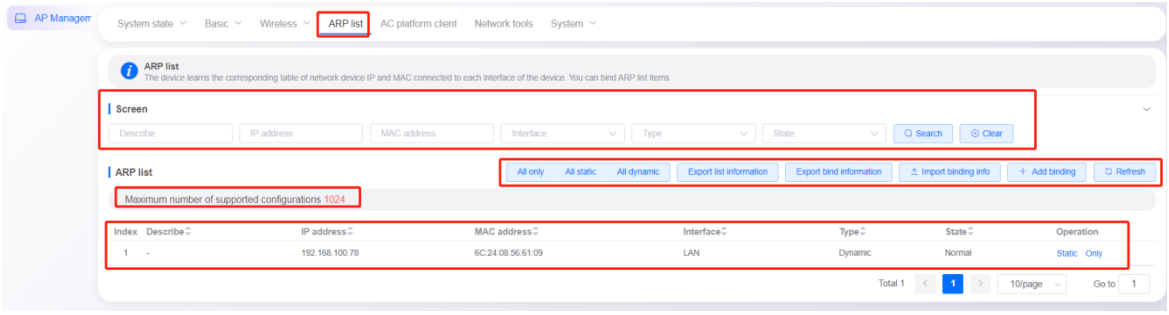
If IP address show 0.0.0.0, mean no Ethernet for this user.



3.4 ARP list

The device learns the IP and MAC correspondence table of the network devices connected to each interface of the device, and can bind the ARP list items

In general, all users within the intranet and the current WAN port will be displayed in the ARP list.



Screen

If a certain IP will be binding statically, uniquely(only), or dynamically, can set it here. If want to confirm or view the binding status of a certain IP, can expand the "screen" function and filter by the terminal's IP address or MAC address, or LAN port.

All only: One-click quick binding of all intranet terminal IP and MAC addresses to be unique. For a terminal bound as unique, the device will automatically learn the terminal's current physical MAC address and assigned IP address in the LAN. When the terminal connects to the network again, the device will automatically detect whether the IP obtained by the terminal and the bound MAC are the bound addresses. If any of the IP or MAC does not match the learned address, the terminal cannot use the network normally.

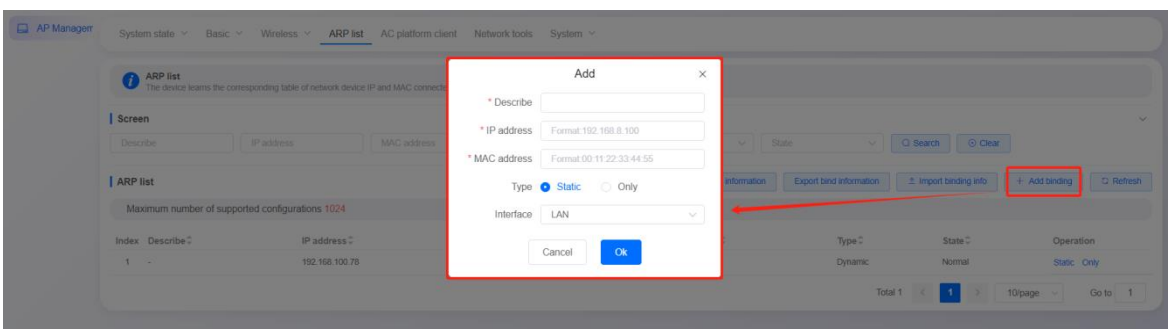
All static: One-click quick binding of all intranet terminal IP and MAC addresses to static. The difference from binding to unique is that when binding to unique, both the terminal's IP and MAC address must be matched successfully. The static mechanism is that the IP learned by the device can only be used on the MAC terminal bound to it. Even if the terminal's MAC is not assigned to the specified original bound IP, it can still use the network normally, but the bound IP address will not be assigned to other terminals and can only be used on the specified terminal;

All dynamic: All intranet terminals are dynamic, not affected by MAC and IP addresses, and are based on the addresses assigned by the routing device;

Export list information: All ARP information in the list will be exported, including the ARP information of the WAN port;

Export bind information: Only the ARP binding information in the list is exported separately, generally used for backup;

Import binding information: re-import the backed-up ARP binding information, generally used for recovery;



Add Binding: Manually add an ARP binding address.

Describe: Customize the description content to facilitate differentiation among many rules;

IP address: Fill in the IP address of the terminal to be bound. The address format must follow the IP format, otherwise the input will fail. Please make sure to fill in the address correctly to avoid terminal network failure due to incorrect address filling;

MAC address: Fill in the MAC address of the terminal to be bound. The MAC address must be real and correct;

Type: Select the binding type as only or static. The difference between the two can be found above;

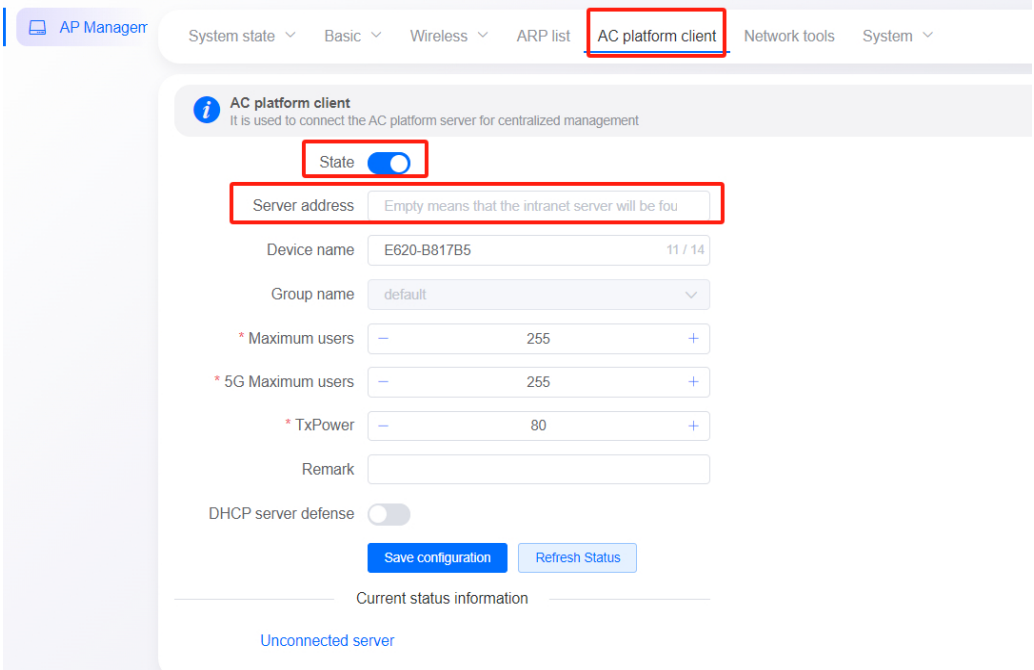
Interface: the bound address interface, LAN or external network, 4G.

ARP List

List of bound or unbound users. The list shows the current or detected terminal information, and you can perform "static", "only" or "dynamic" ARP binding on a terminal. Among them, the detection type terminal refers to a terminal that has been connected to the local area network wireless, disconnected and not connected to other wireless devices.

3.5 AC Controller Management

In the case of multiple wireless APs are installed in same network, an AC controller is generally used to manage the wireless APs, in this case, the AC controller is needed to configure the wireless APs centrally, the wireless SSID configured and other settings on this GUI page will not take effect, AC controller management is enabled in default.

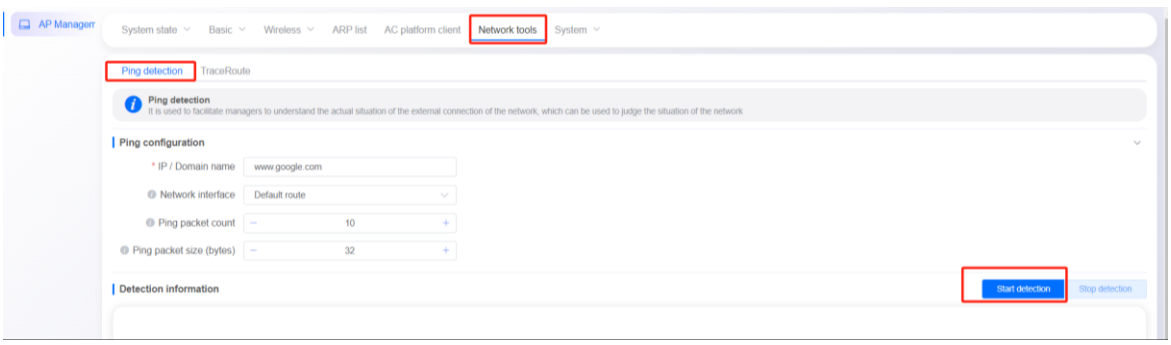


In the server address, Empty means AC controller's management address will be founded automatically;
Device name: mean the name of this wireless AP
Group name: this is configured from the AC controller;
Maximum users: mean the maximum users can access into this wireless AP. 0 mean no limited users; Normally this data is obtained from the connected AC controller under enable state;
TX power: mean the RF power of this AP, this data is obtained from AC controller under enable state;
DHCP server defense: this is the function under router, to prevent IP errors caused by multiple DHCP servers.

3.6 Network tools

3.6.1 Ping detection

It is used to help administrators understand the actual status of the network's external connections. The Ping detection function can be used to determine the network status.

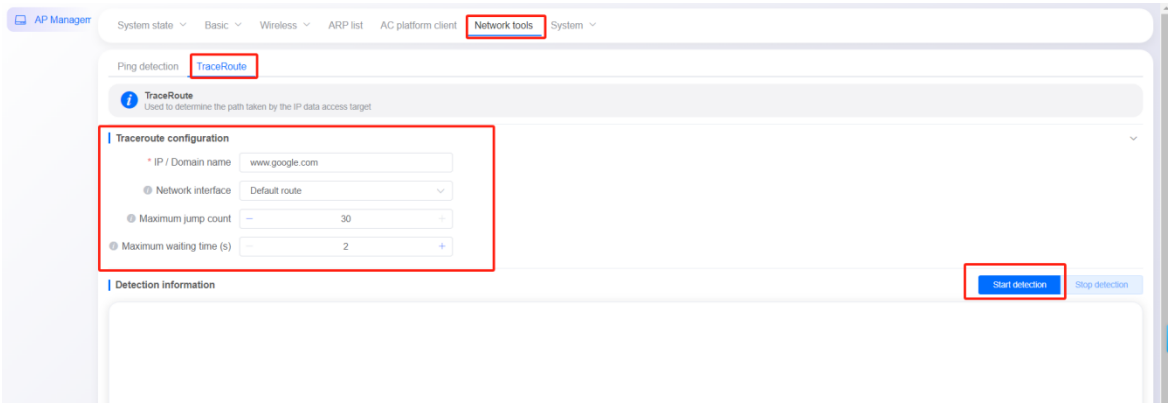


Ping Configuration

IP/Domain Name: Fill in the IP or domain name that needs to be pinged;
Network interface: Select the port from which the ping test is to be conducted;
Ping Packet Count: Set the number of packets for each Ping detection, the default is10, and the range is 1-1000;
Ping Packet Size (Bytes): Set the size of the packet for each Ping check. The default is 32 and the setting range is 1-10240.
After configuring the rules, can click " Start Detection " and the detection results will be displayed below. If want to stop the detection, click " Stop Detection " .

3.6.2 TraceRoute

Used to determine the path taken by IP data to reach a target.



TraceRoute Configuration

IP/Domain Name: Fill in the IP or domain name whose path needs to be determined;

Network interface: select the port from which the data path will go out;

Maximum jump count: Set the maximum jump count between data, the default is 30, the range is 2-30;

Maximum waiting time (seconds): Maximum waiting time setting, the default is 2 seconds, the range is 2-10.

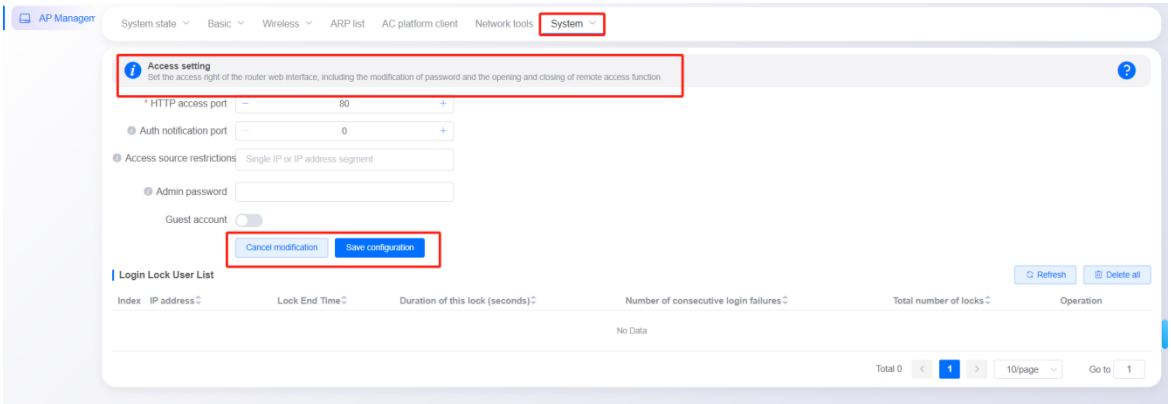
After configuring the rules, can click " Start Detection " and the detection results will be displayed below. If want to stop the detection, click " Stop Detection ".

3.7 System Management

From system, can configure the remote access page, backup and import the configure file of wireless AP, restore the factory settings, upgrade the firmware and restart.

3.7.1 Access setting

Set the access right of this AP' s web interface, including the modification of password and the opening and closing of remote access function.



HTTP access port: The port used by the local area network to access the wireless AP. The default value is 80;

Auth notification port: 0 means the same as the management port;

Access source restriction: The filled address will not be able to access the remote address of the system;

Admin Password:

A custom administrator password , which has the highest management privileges for the router ;

By default, there is no need to set or modify the account in this system, and the account is always "admin" by default ;

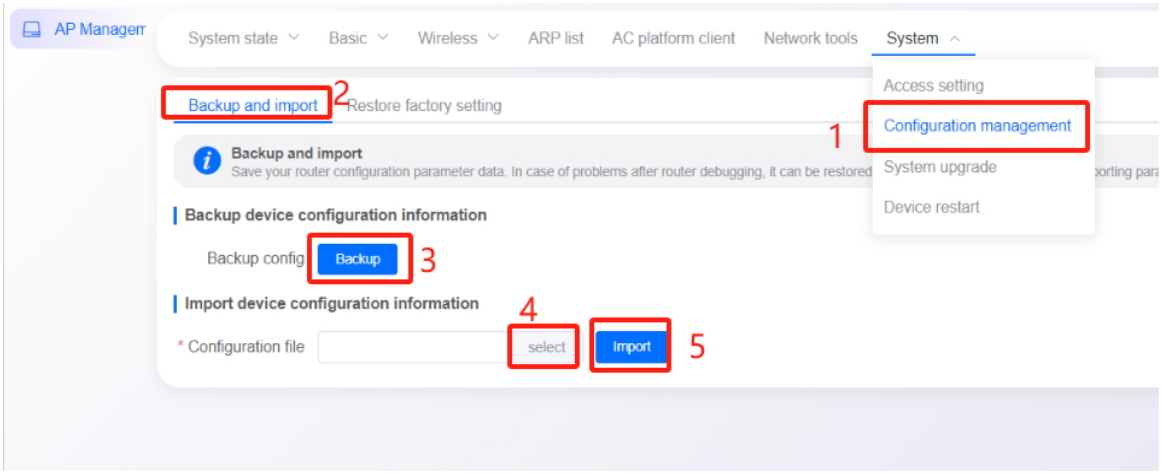
To change the password, directly enter the new password in "Admin Password", then enter "Admin Password Confirmation" and "Original Admin Password", and submit to complete the change.

3.7.2 Configuration management

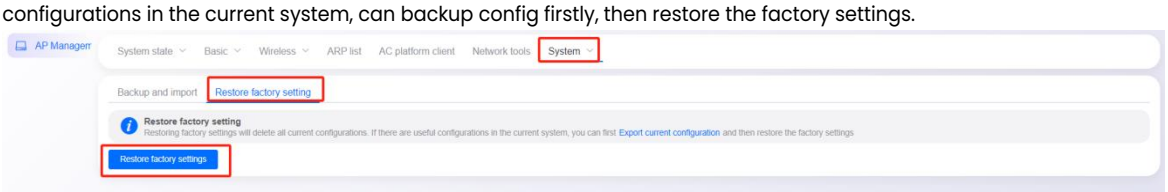
Including backup all parameter settings of the AP configuration, import this backup file and restore factory settings;

Backup steps: click 1,2, 3 in below picture;

Import the backup file: click 1,2,4,5 in below picture



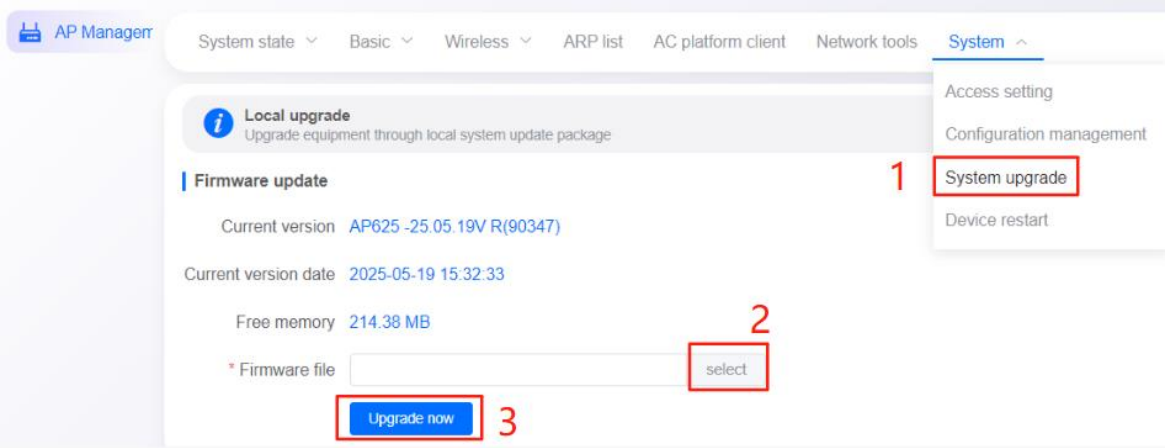
Restore factory setting: mean reset this wireless AP, will delete all current configurations. If there are useful configurations in the current system, can backup config firstly, then restore the factory settings.



3.7.3 Local firmware upgrade

Can upload new firmware file and upgrade the device locally;

Please obtatin the latest firmware, then click steps 1, 2 to select the firmware, click 3 to upgrade firmware.



3.7.4 Restart the wireless AP

In this part, including device restart immediately and timed reboot at special time or days

