MACC User Guide

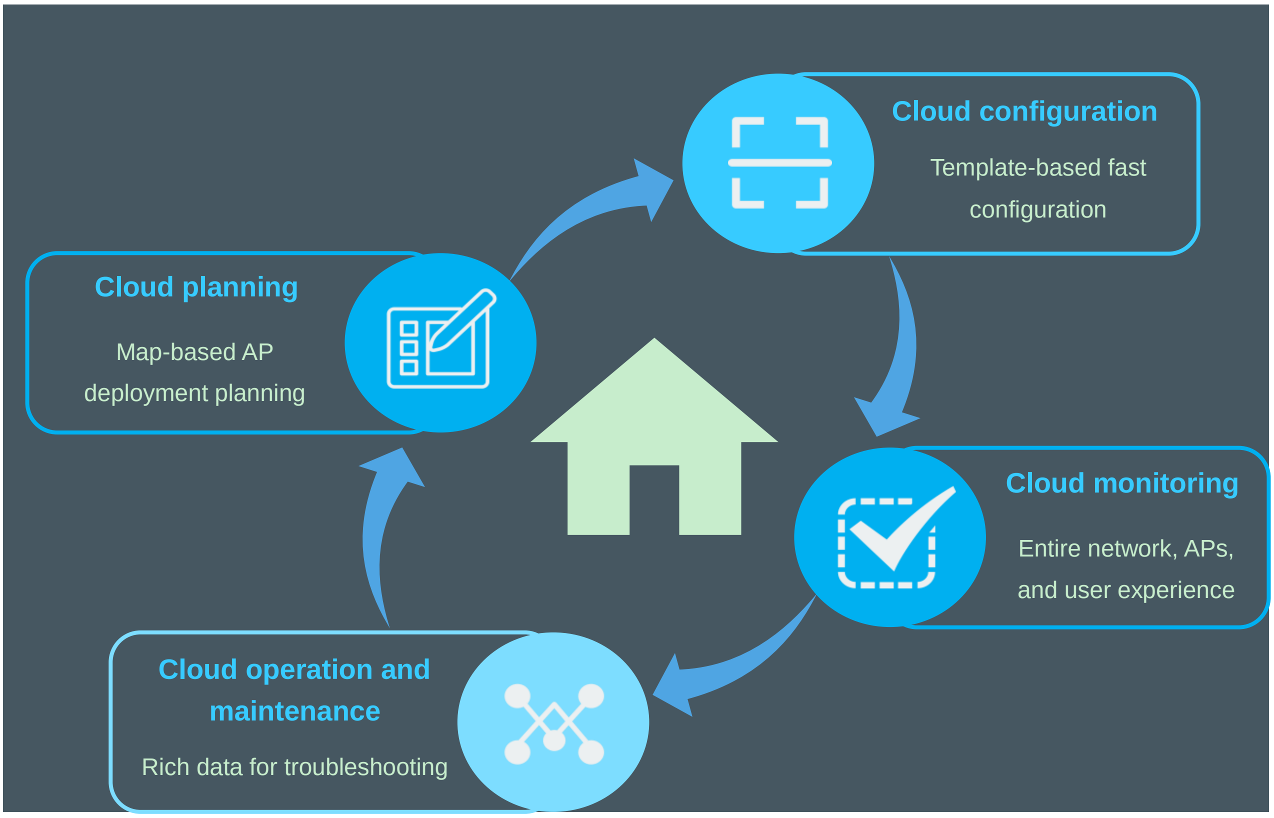
Contents

1 Summary

MACC (Mobile Access Cloud Center, MACC for short) is a cloud WiFi management and control platform for chain stores, small and medium enterprises, enterprises with a headquarters-branch structure, operator networks, and lightweight scenarios.

MACC solves a problem that access points (APs) are scattered in different cities and stores and are difficult to manage or monitor in a centralized way. The conventional tight coupling manner is more suitable for management on a large quantity of APs by hardware access controller (AC) in a local area network (LAN). By contrast, weak coupling between MACC and APs and separation of management from data better suit a cross-Internet wireless network.

MACC not only implements AP management, but also realizes wireless control functions the same as those of the conventional hardware AC, such as automatic channel and power adjustment, optimized radio frequency (RF) management, and L2/L3 roaming, providing an actually available wireless network.


Cloud configuration
Template-based fast configuration
Cloud planning
Map-based AP deployment planning
Cloud monitoring
Entire network, APs, and user experience
Cloud operation and maintenance
Rich data for troubleshooting

Cloud management in the entire life cycle

Protocol specifications

- CPE WAN Management Protocol (CWMP) is a technical standard initiated by the DSL (Digital Subscriber's Line) forum. CWMP specifies a general framework, message specifications, management methods, and data models for customer-premises equipment (CPE) wide area network (WAN) management. CWMP is numbered as TR-069, and therefore, is also known as the TR-069 protocol.

- Simple Traversal of UDP over NAT (STUN) is a protocol that realizes NAT traversal and allows clients to find out their own public network addresses and ports after network address translation (NAT) or multi-NAT. STUN enables hosts respectively connected to two routers that are experiencing NAT to set up User Datagram Protocol (UDP) communication, providing the traversal NAT function. For description about STUN, refer to RFC 3489.

2 Dashboard

The **Dashboard** page is the MACC homepage, and summarizes most commonly used information for intuitive display to you.

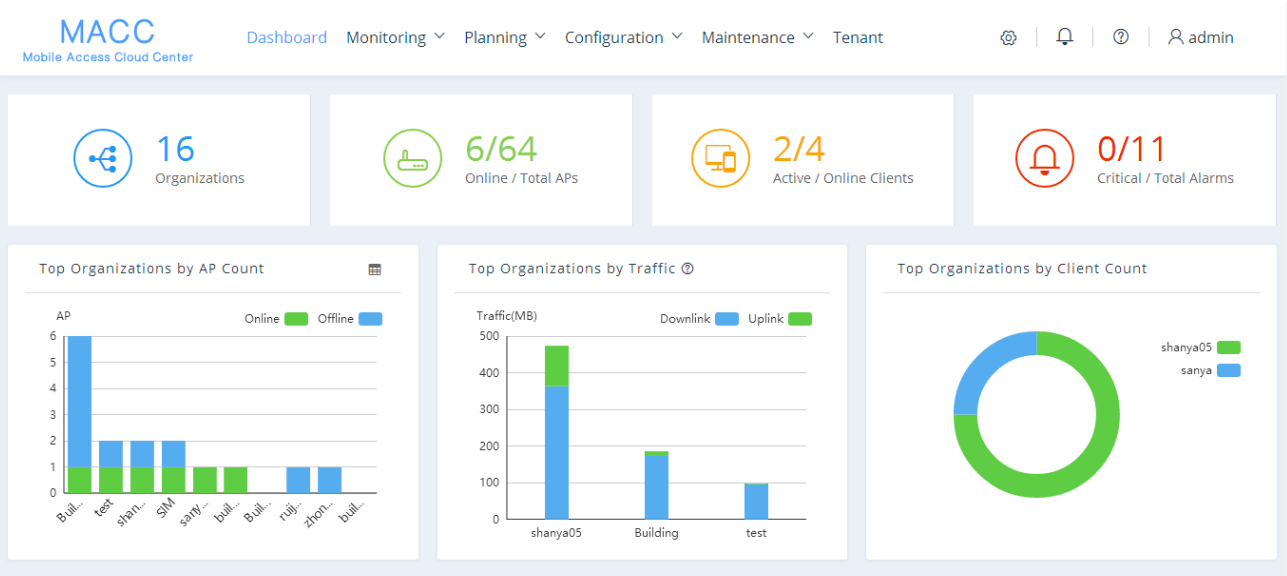


Figure 2-1 MACC Homepage

The **Dashboard** page provides the following information:

- Total AP count and online AP count
- Online and active client count, and top organizations by client count
- Alarm statistics
- Top organizations by traffic
- Top organizations by AP count

3 Planning

The Planning module allows you to group APs.

You can import or delete APs, bind APs to different groups, and configure RF and roaming information for APs.

The Planning module includes three parts: **Locations**, **Radios**, and **Roaming**.

3.1 Locations

3.1.1 Adding Groups

Choose **Planning** > **Locations** to open the location planning page, as shown in the following figure.

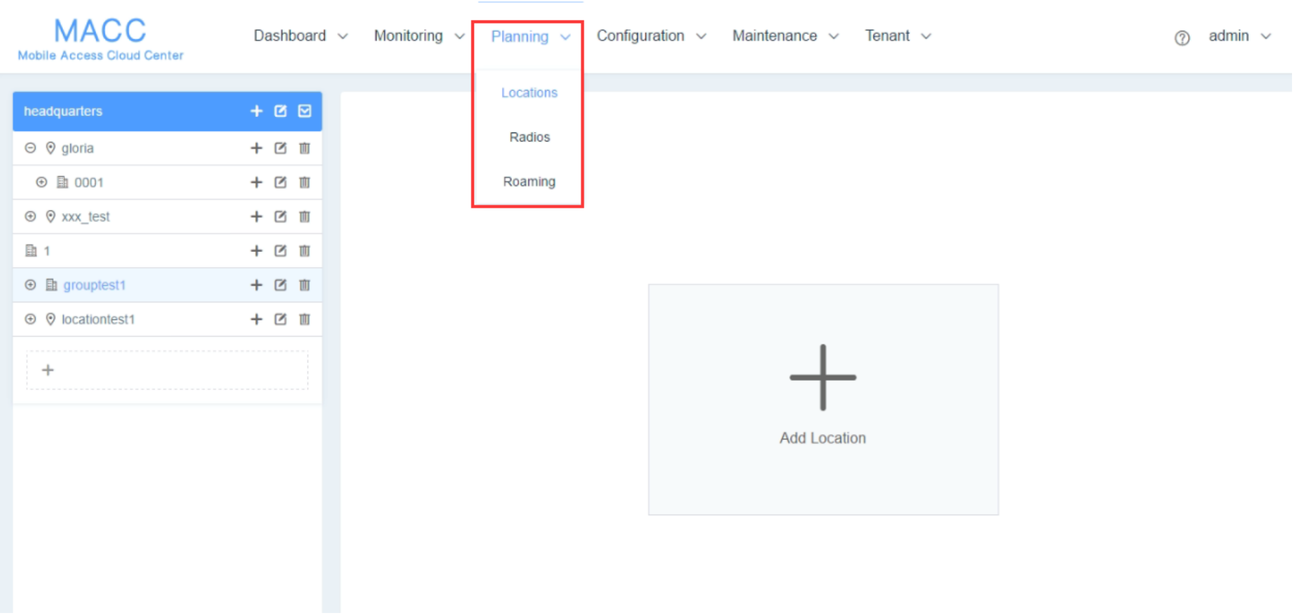


Figure 3-1 Planning

Click **+** to add a group.

Three types of groups can be added: Location, Organization, and Floor.

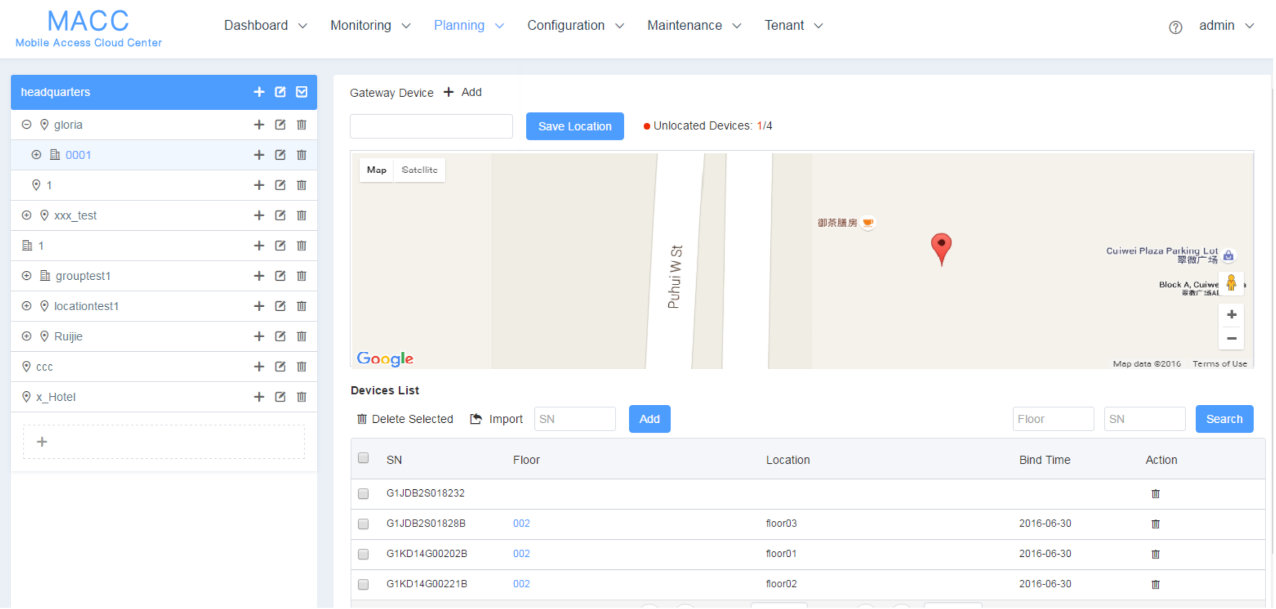
Network planning must be compliant with the following rules:

- A root group must be a Location or Organization group.
- A Location group includes only Location and Organization groups.
- An organization group includes only Floor groups.

Specify a group location

Select a Location or Organization group, and click **Add Location** to bind this group to a location.

You can locate a Location or Organization group by using the AutoNavi map.



Devices List

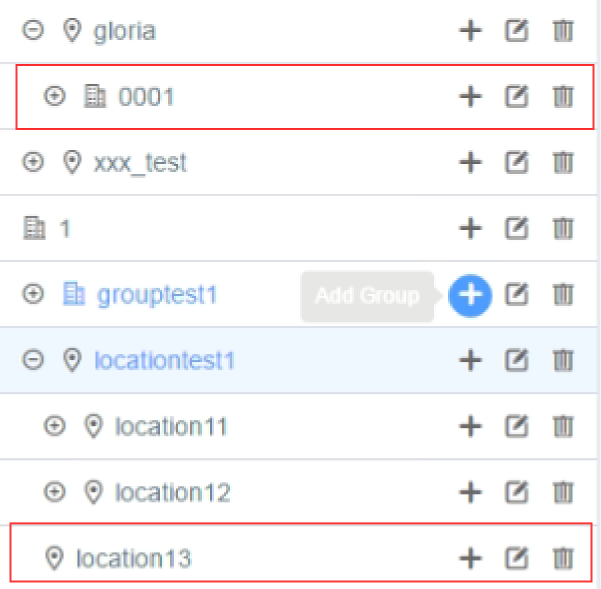
Delete Selected | Import | SN | Add | Floor | SN | Search

□	SN	Floor	Location	Bind Time	Action
□	G1JDB2S018232				🗑
□	G1JDB2S01828B	002	floor03	2016-06-30	🗑
□	G1KD14G00202B	002	floor01	2016-06-30	🗑
□	G1KD14G00221B	002	floor02	2016-06-30	🗑

Figure 3-2 Location Selection

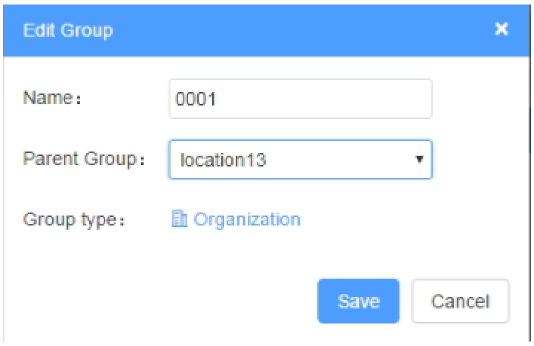
3.1.2 Changing Groups

To move a group into another parent group, click ✎ in the red frame



For example, to move **0001** into parent group **location13**, click ✎ corresponding to **0001**, and set **Parent Group** to **location13** in the displayed dialog box.

ⓘ A group that contains configurations cannot be moved.


Edit Group ×

Name: 0001

Parent Group: location13

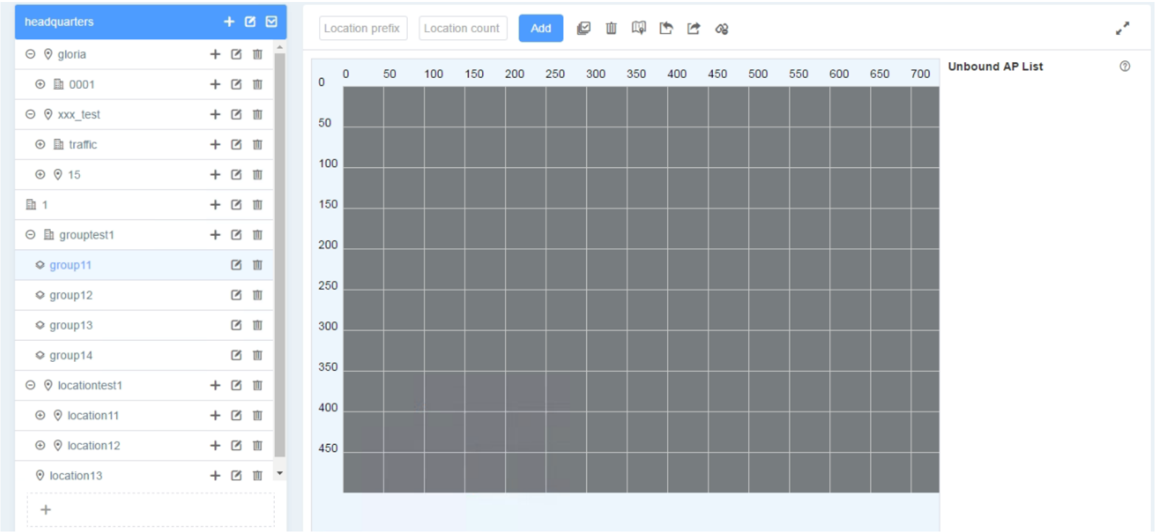
Group type: Organization

3.1.3 Uploading Floor Plans

On the **Floor** page, you can upload the floor plan.

- Click a Floor group to open the page shown in the following figure.

The currently selected floor is **group11**.



- Click 🗺 to import a floor plan in local upload mode or image library mode.

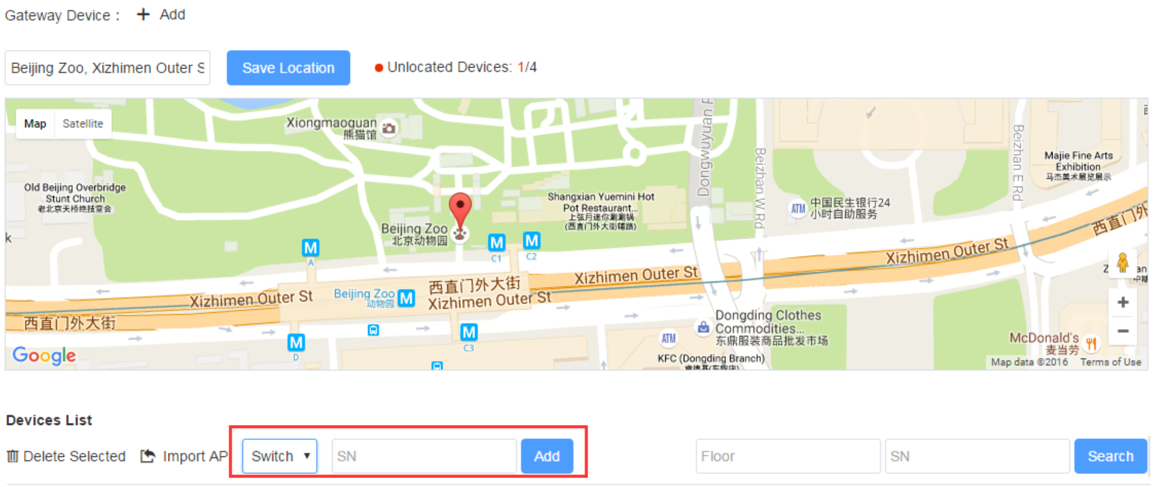
You can import an uploaded image in image library mode. Fuzzy search by image name is supported.

3.1.4 Importing Devices

Switches and APs need to be imported.

3.1.4.1 Importing Switches

1. Select an organization for which switches need to be imported.
2. As shown in the following figure, select **Switch** from the drop-down list, enter the device serial number in the **SN** text box, and click **Add** to import the switch.



In this way, a switch is imported to the organization but is not allocated to a specific location.

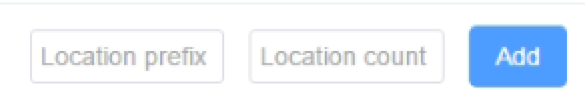
3.1.4.2 Importing APs

APs can be imported in two modes based on different scenarios.

Scenario 1: The deployment location of an AP is known. It is recommended that an AP be imported by floor. The import method is as follows:

- Select a floor.

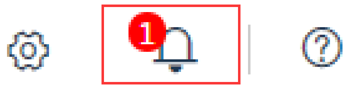
Enter the **Location prefix** and **Location count**, and click **Add** to add a location, as shown in the following figure.



Click to download an EXCEL file, enter serial numbers of to-be-imported APs in the EXCEL file, and click to import the APs as prompted.

You can specify a location name and serial number in the EXCEL file to add a location and bind the location with an AP. An initial location is in the upper left corner.

After APs are imported in batches, a message is displayed in the upper right corner, as shown by the red frame in the following figure. (No message will be displayed if only one AP is imported.)



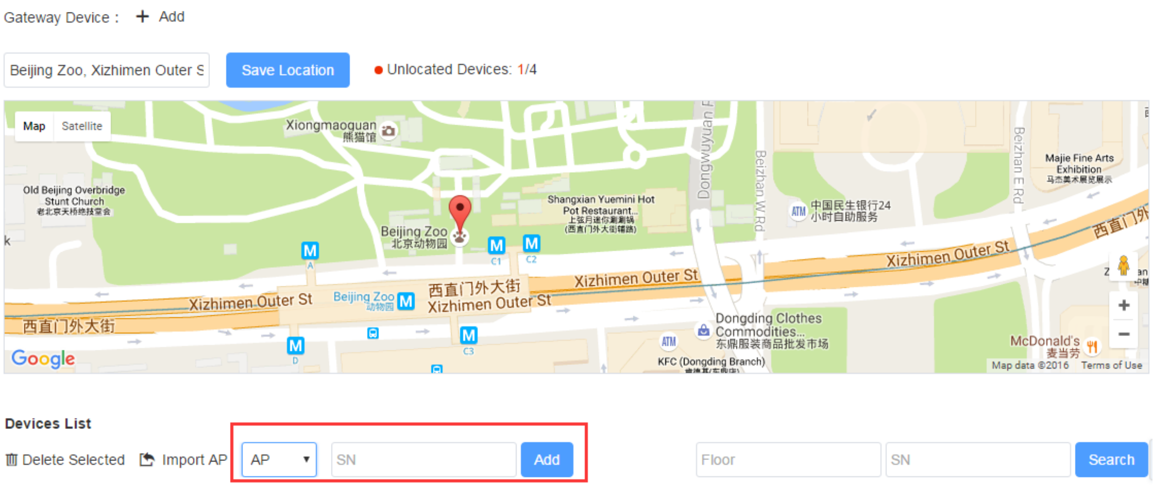
You can click the icon in the red frame to query information about imported APs.

By using this method, you can bind an AP to a specific location of a floor.

Scenario 2: The deployment location of an AP is unknown, but an organization to which the AP belongs is known. It is recommended that an AP be imported by organization. The import method is as follows:

- Select an organization.

To import a single AP, enter the AP serial number in the **SN** text box, and click **Add**, as shown in the following figure.



Gateway Device : + Add

Beijing Zoo, Xizhimen Outer S | Save Location | ● Unlocated Devices: 1/4

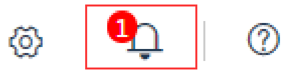
Map
Satellite
Xiongmaoguan
熊猫馆
Old Beijing Overbridge Stunt Church
Beijing Zoo
北京动物园
Shangxian Yuemini Hot Pot Restaurant
Xizhimen Outer St
西直门外大街
Beijing Zoo
Dongding Clothes Commodities
东鼎服装商品批发市场
KFC (Dongding Branch)
中国民生银行24小时自助服务
Majie Fine Arts Exhibition
McDonald's
麦当劳
Google
Map data ©2016 Terms of Use

Devices List

Delete Selected | Import AP | AP ▾ | SN | Add | Floor | SN | Search

To import multiple APs, click Import to import APs as prompted.

After APs are imported in batches, a message is displayed in the upper right corner, as shown by the red frame in the following figure. (No message will be displayed if only one AP is imported.)



You can click the icon in the red frame to query information about imported APs.

By using this method, you can bind an AP to an organization but cannot specify its location.

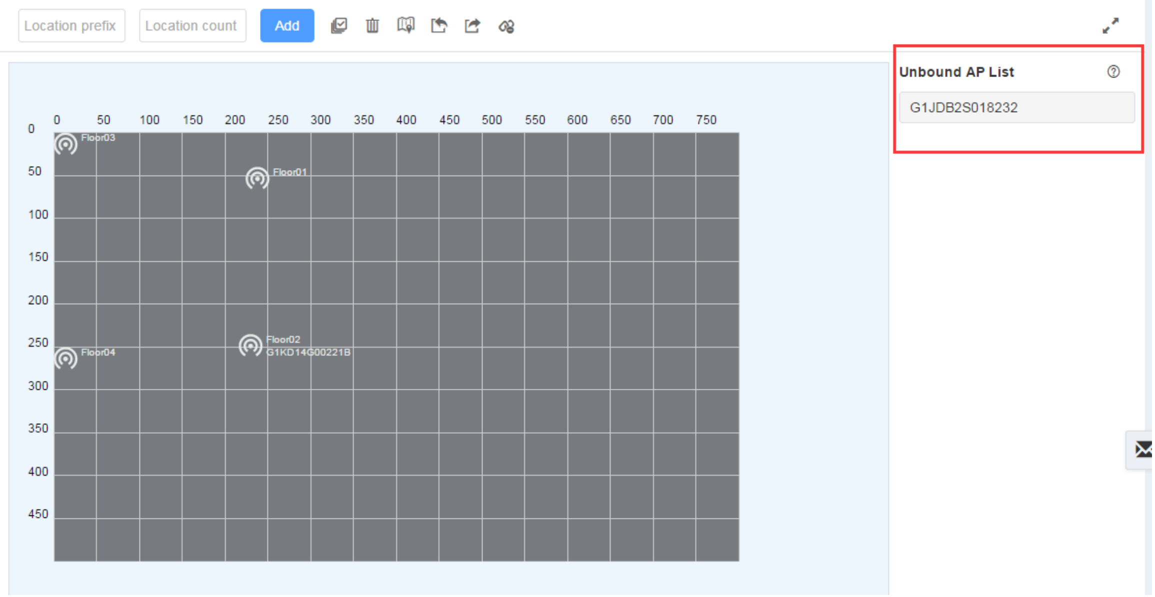
Scenario 3: After an AP is imported to an organization, you want to bind the AP to a specific location. The import methods are as follows:

Method 1:

- Select a floor.

The unbound AP list on the right shows APs that have been imported to an organization but are not bound to a location.

- Add a location.
- Select an AP from in the unbound AP list and drag it to the target location.



Location prefix | Location count | Add

Unbound AP List

G1JDB2S018232

Method 2: Import APs according to the import method in scenario 1.

If a location is already bound to an AP, the AP will be unbound, and the location will be bound to the new AP.

3.1.5 Deleting APs

An AP can be deleted only from an organization. If an AP is deleted or unbound from a floor, the AP still exists in the organization.

The deletion methods are as follows:

Method 1: Select an AP from the AP list, and click 🗑 to delete a single AP.

Method 2: Select multiple APs, and click **Delete Selected** to delete APs in batches.

3.1.6 Unbinding APs

AP unbinding is different from AP deletion. AP unbinding is to remove the binding relation between an AP and a location, but the AP still exists in the organization and can be controlled by the MACC. AP deletion is to delete an AP from an organization, and the AP cannot be controlled by the MACC after being deleted.

The unbinding methods are as follows:

Method 1: Select an AP, and click 🔗 to unbind the AP from a location. An unbound AP will be moved from a floor group to its parent organization group.

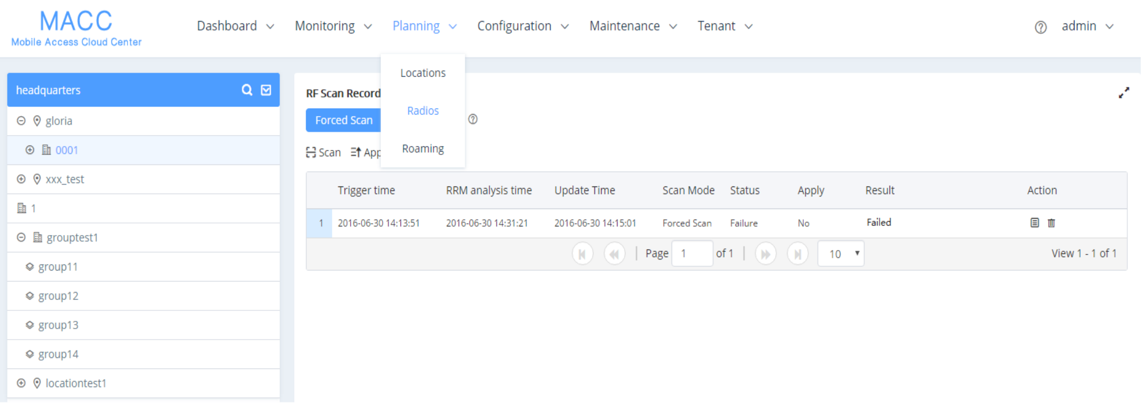
Method 2: If a location is already bound to an AP, you can drag another AP to the location to replace the old AP.

3.2 Radios

RF planning refers to adjusting channels and power of APs in a same area network, so as to optimize channel allocation and power of the APs. Proper RF configuration planning can reduce channel interference and increase channel utilization, thereby improving the overall wireless network performance and capacity.

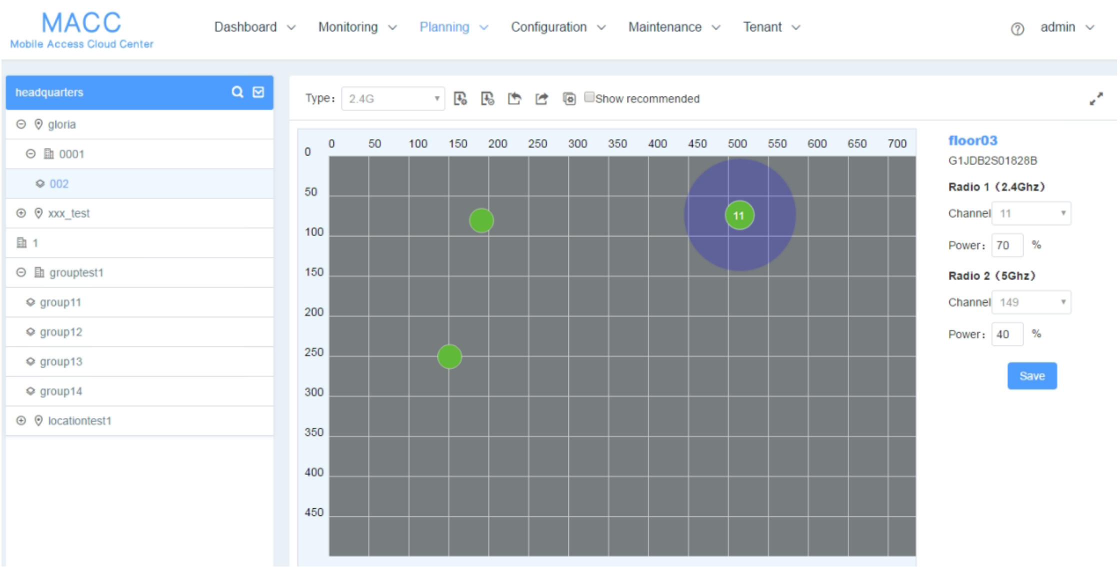
- Choose **Planning** > **Radios** to open the RF planning page. Currently, the MACC supports manual RF planning and automatic RF planning.

Click an organization group on the left to open the automatic RF planning page.



	Trigger time	RRM analysis time	Update Time	Scan Mode	Status	Apply	Result	Action
1	2016-06-30 14:13:51	2016-06-30 14:31:21	2016-06-30 14:15:01	Forced Scan	Failure	No	Failed	

Click a floor group on the left to open the manual RF planning page. This function supports location-based RF adjustment.



Type: 2.4G

□Show recommended

floor03
G1JDB2S01828B

Radio 1（2.4Ghz）
Channel 11
Power: 70 %

Radio 2（5Ghz）
Channel 149
Power: 40 %

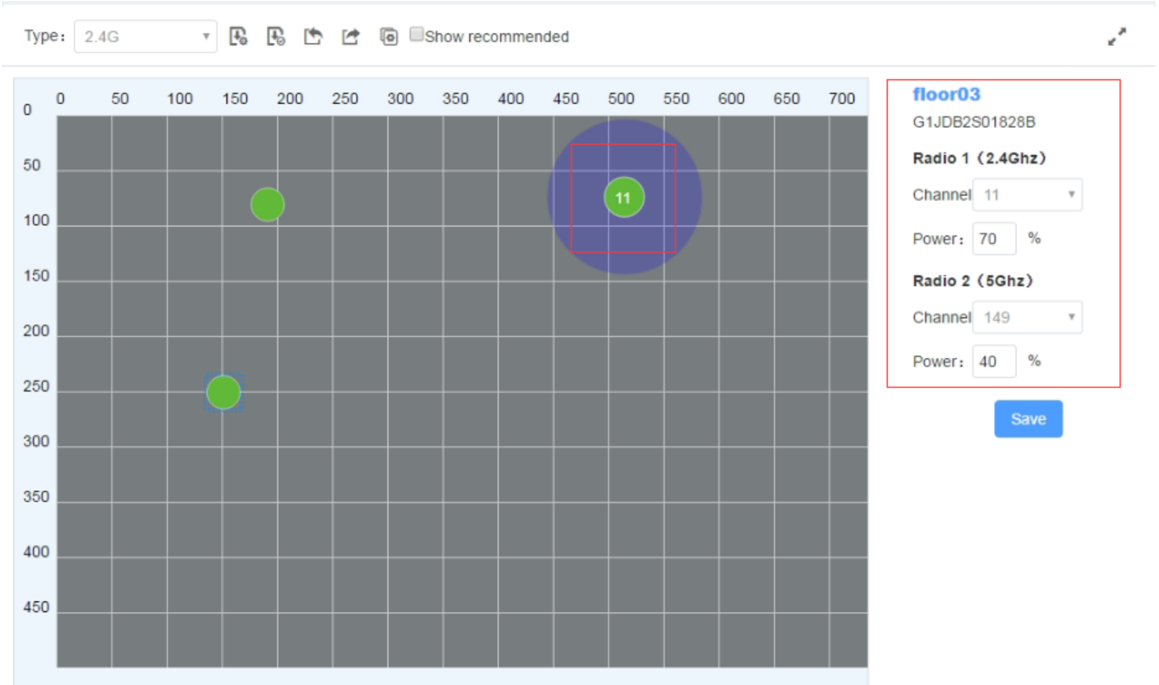
For details about the two types of RF planning, see chapters 3.2.1 and 3.2.2.

3.2.1 Manual RF Planning

Click a floor group on the left to open the manual RF planning page. The **Type** drop-down list above the diagram enables you to select an RF type (2.4 GHz/5 GHz) to display. The number inside the location icon indicates the current channel, and a range displayed when the cursor stays on the location icon indicates a power percentage.

The RF channel or power data is not displayed during configuration.

You can click a location icon to display the RF channel and power configurations on the right. If the location is bound to an AP, the SN of the bound AP is also displayed.



Type: 2.4G

□Show recommended

floor03
G1JDB2S01828B

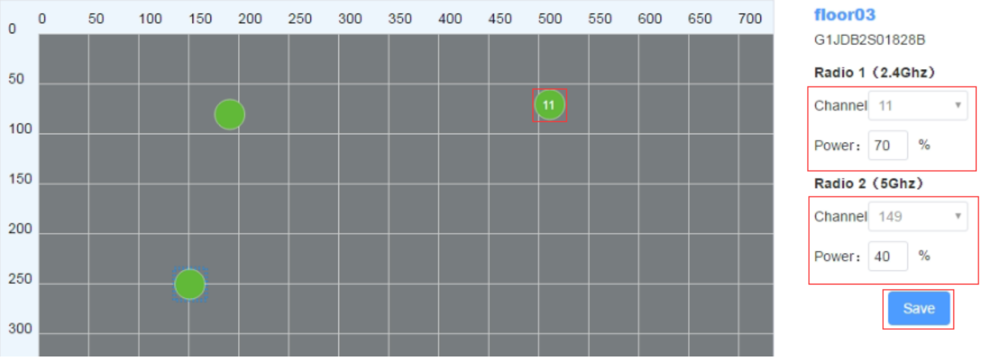
Radio 1（2.4Ghz）
Channel 11
Power: 70 %

Radio 2（5Ghz）
Channel 149
Power: 40 %

To perform manual RF planning:

- Set the RF configurations of a location in one of the following three ways:
  - Configure one location

Click a location icon and enter configurations on the right, and click **Save**.

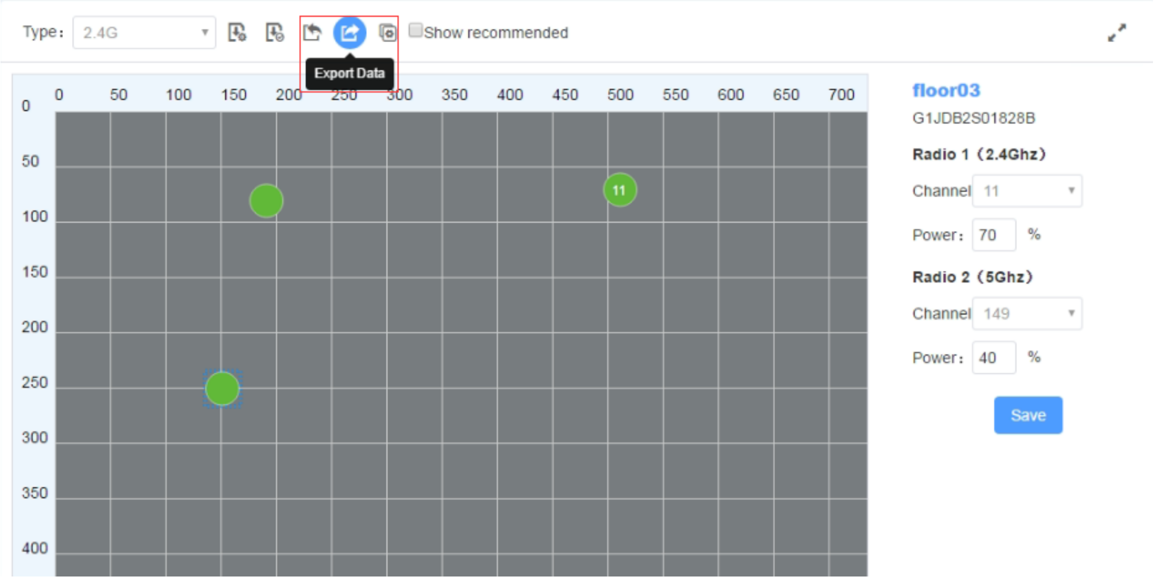


floor03
G1JDB2S01828B
Radio 1（2.4Ghz）
Channel: 11
Power：70 %
Radio 2（5Ghz）
Channel: 149
Power：40 %

- Import configurations

This function is used to configure the RF channel and power for a large batch of locations, and is suitable for a scenario with many locations on a floor.

(1) Click above the location diagram to export location data of the current floor in an EXCEL file.

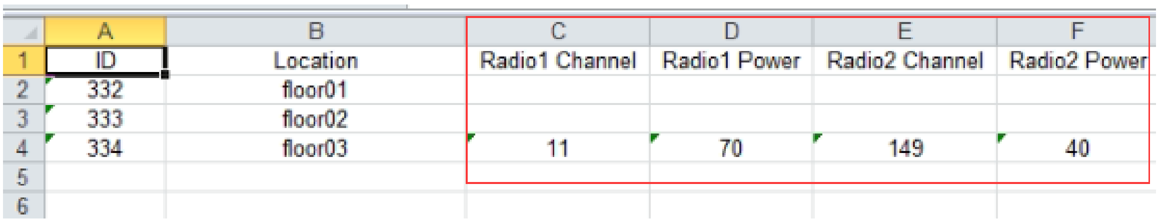


Type：2.4G
□ Show recommended

floor03
G1JDB2S01828B
Radio 1（2.4Ghz）
Channel: 11
Power：70 %
Radio 2（5Ghz）
Channel: 149
Power：40 %

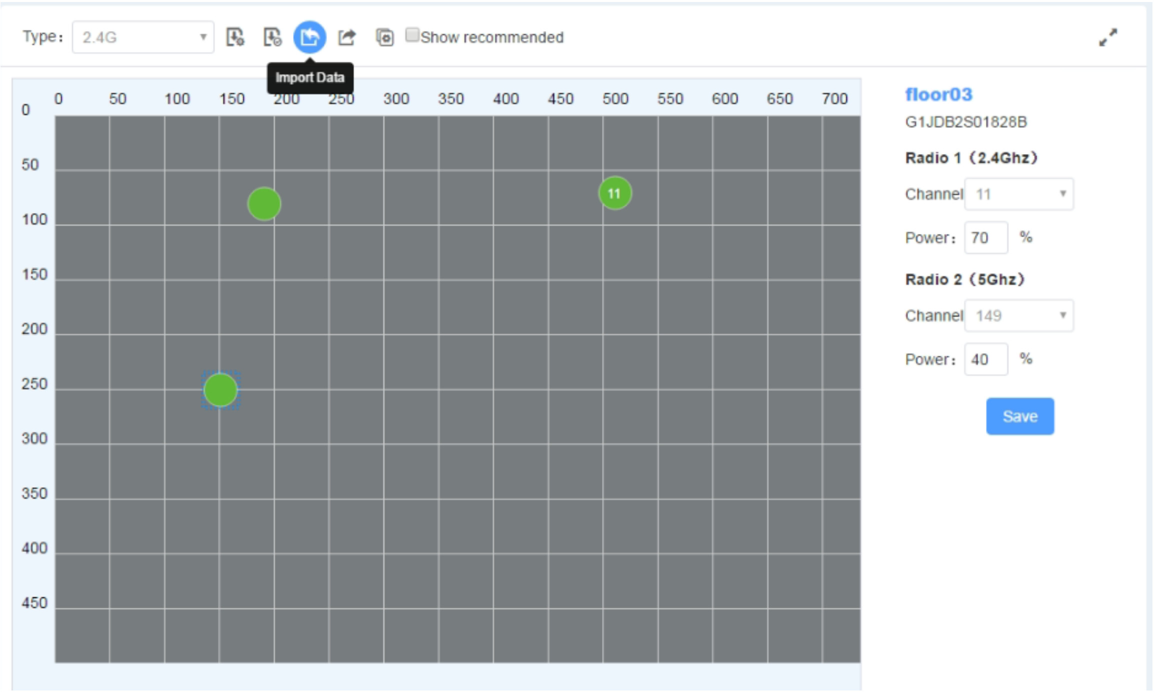
(2) Enter RF channel and power information, and save the EXCEL file.

Radio 1 represents the 2.4 GHz frequency band, and Radio 2 represents the 5 GHz frequency band. The field can be left empty.



	A	B	C	D	E	F
1	ID	Location	Radio1 Channel	Radio1 Power	Radio2 Channel	Radio2 Power
2	332	floor01				
3	333	floor02				
4	334	floor03	11	70	149	40
5						
6						

(3) Click above the location diagram to upload the saved EXCEL file as prompted.



Type: 2.4G

□Show recommended

floor03

G1JDB2S01828B

Radio 1（2.4Ghz）

Channel 11

Power: 70 %

Radio 2（5Ghz）

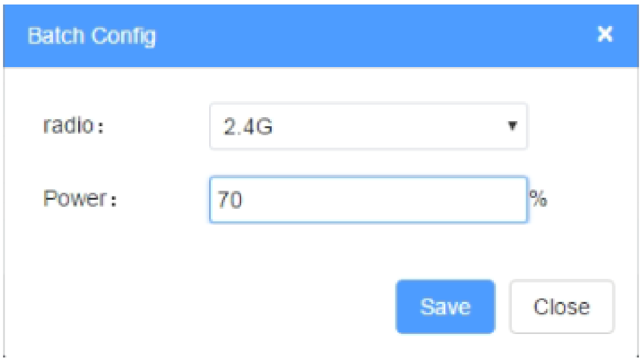
Channel 149

Power: 40 %

Save

- Configure locations in batches

Click above the location diagram to configure the power percentage for all locations on a floor uniformly.



Batch Config ×

radio: 2.4G

Power: 70 %

Save Close

Synchronize the RF configurations of the location to a bound AP.

Click or above the location diagram to synchronize the RF configurations of the corresponding location to the bound AP.

You can select multiple locations for batch operations before clicking .

After the synchronization is successful, is displayed in the lower right corner. At this point, the configurations of the location are synchronized to the bound AP.

If you perform an unbind or bind operation, RF configurations are removed from or synchronized to the AP.

3.2.2 Automatic RF Planning

The MACC automatic RF planning function allows the cloud to calculate the optimal channel configurations and power values for APs by using the radio resource management (RRM) algorithm according to RF information collected by each AP. Optimal recommended configurations can be applied to the APs or locations.

The entire process of the automatic RF planning includes three parts:

1. The cloud triggers APs to scan and upload RF information.

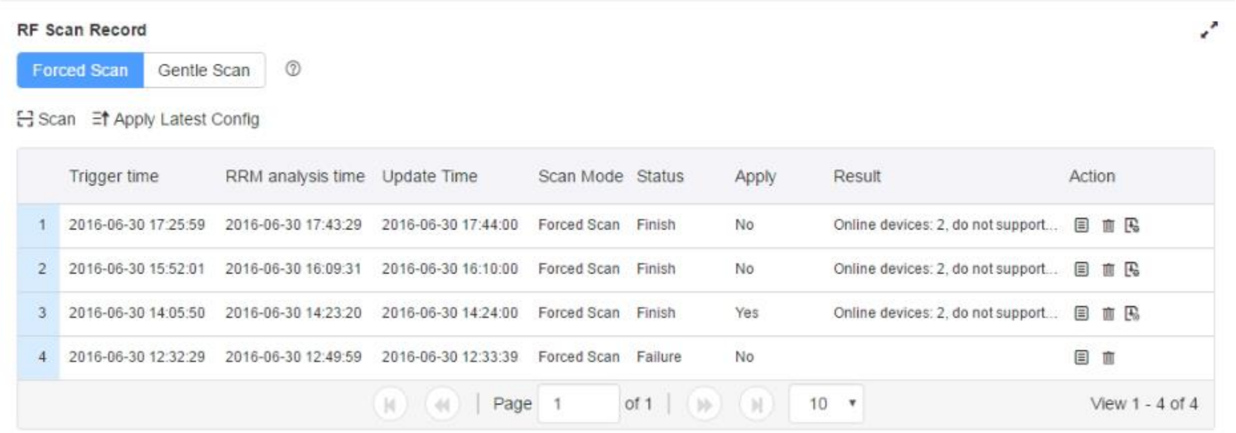
2. The cloud calculates the optimal recommended configurations.

3. The optimal recommended configurations are applied to the APs or locations

The MACC automatic RF planning supports organization-based planning only.

The AP RF channel optimization algorithm staggers RF channels of neighboring APs respectively based on the 2.4 GHz frequency band and the 5 GHz frequency band while ensuring as much as possible that original configurations are unchanged. The AP power optimization algorithm automatically increases or decreases RF power of an AP according to co-channel interference of the AP to reach optimal power.

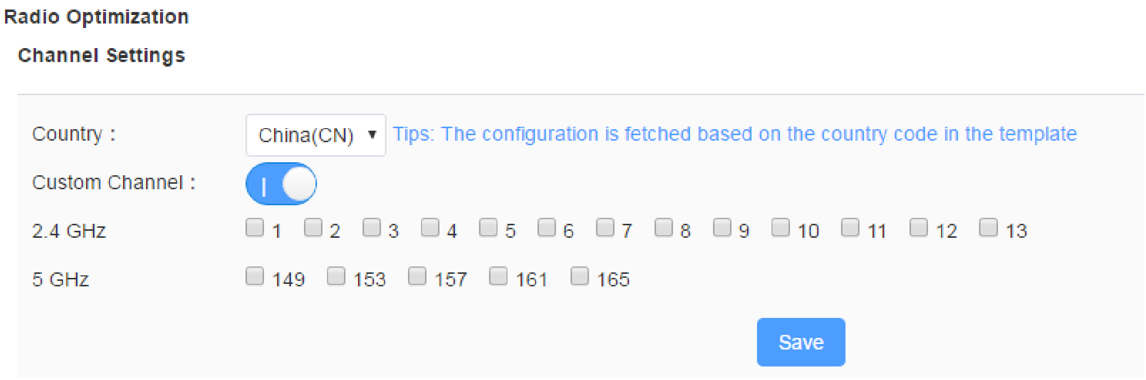
After an organization group is selected on the RF planning page, a page for automatic RF scanning and planning of organizations is displayed. On this page, APs of an organization can be triggered to scan the RF, display recommended RF configurations calculated after the scanning, and save the recommended RF configurations to APs or locations.



	Trigger time	RRM analysis time	Update Time	Scan Mode	Status	Apply	Result	Action
1	2016-06-30 17:25:59	2016-06-30 17:43:29	2016-06-30 17:44:00	Forced Scan	Finish	No	Online devices: 2, do not support...	
2	2016-06-30 15:52:01	2016-06-30 16:09:31	2016-06-30 16:10:00	Forced Scan	Finish	No	Online devices: 2, do not support...	
3	2016-06-30 14:05:50	2016-06-30 14:23:20	2016-06-30 14:24:00	Forced Scan	Finish	Yes	Online devices: 2, do not support...	
4	2016-06-30 12:32:29	2016-06-30 12:49:59	2016-06-30 12:33:39	Forced Scan	Failure	No		

The **RF Scan Record** page displays historical records of the automatic RF scanning and planning. Each record shows triggering information of each time, including the automatic RF planning status, the start time, the end time, the status (Initializing/Scanning/RRM analysis/Finish/Failure), whether to apply to APs, and the running logs.

1. On the **Channel Settings** page, select the country and channel.



Country : China(CN) Tips: The configuration is fetched based on the country code in the template

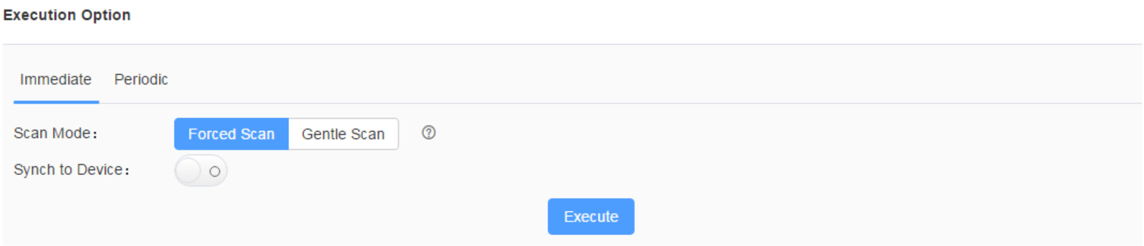
Custom Channel : ●

2.4 GHz □ 1 □ 2 □ 3 □ 4 □ 5 □ 6 □ 7 □ 8 □ 9 □ 10 □ 11 □ 12 □ 13

5 GHz □ 149 □ 153 □ 157 □ 161 □ 165

On the **Channel Settings** page, you can select the country and customize channels. When **Custom Channel** is enabled, the RF channel is selected from custom channels and optimized. If **Custom Channel** is disabled, the default channel on the MACC is selected for RF channel optimization.

2. Select an execution mode to trigger RF scanning and optimization.



Execution Option

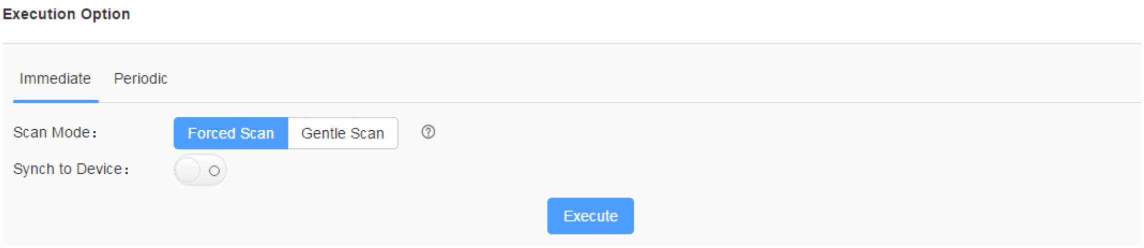
Immediate | Periodic

Scan Mode: Forced Scan | Gentle Scan

Synch to Device: ○

There are two execution modes: immediate and periodic.

- Immediate execution



Execution Option

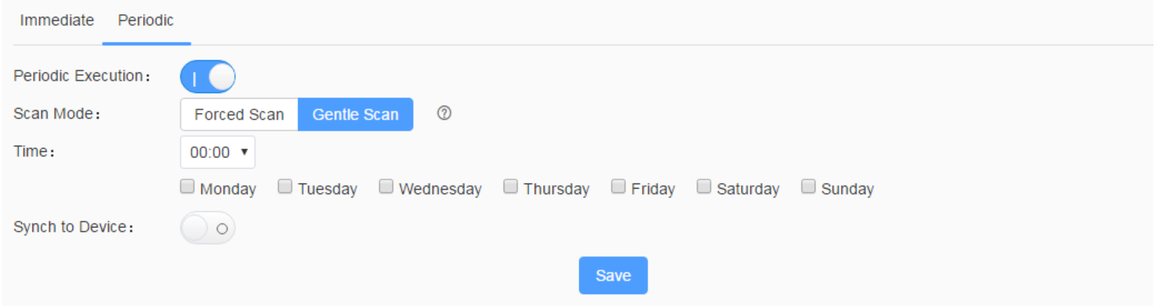
Immediate | Periodic

Scan Mode: Forced Scan | Gentle Scan

Synch to Device: ○

Click **Execute**, and the cloud triggers RF scanning. Data will be uploaded after scanning.

- Periodic execution



Immediate | Periodic

Periodic Execution: I

Scan Mode: Forced Scan | Gentle Scan

Time: 00:00 ▾

□ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

Synch to Device: ○

On the **Periodic** page, you can choose whether to enable **Periodic Execution**. When a periodic task is triggered, this periodic task is automatically canceled if the organization is already in a scanning triggered state (for example, immediate execution is being triggered).

- Related parameters

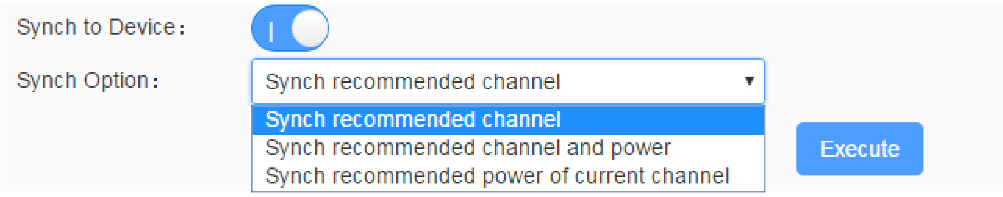
(1) Scan Mode

Scan Mode: Forced Scan | Gentle Scan

Gentle Scan: This mode enables APs to provide the WiFi service properly during scanning. However, data acquired in this mode is not so accurate as that in the **Forced Scan** mode. Therefore, the calculation result based on the data in this mode is less accurate than that in the **Forced Scan** mode. This mode is applied when it is expected that the current network is not affected.

Forced Scan: This mode is also referred to as the enhanced mode, and causes wireless clients to go offline at the beginning and ending of the scanning. Data acquired in this mode is more accurate than that in the **Gentle Scan** mode, and the automatic RF planning based on the data is more accurate. This mode shall be applied at the initial stage of the overall network planning or when disadvantages of this mode are tolerable.

(2) Synch to Device



Synch to Device:

Synch Option: Synch recommended channel ▾

- Synch recommended channel
- Synch recommended channel and power
- Synch recommended power of current channel

Execute

If this function is enabled, the RF scanning result will be automatically pushed to the AP. In this case, skip step 3.

3. Manually push the RF optimization results (synchronize the RF configurations to the locations or APs).

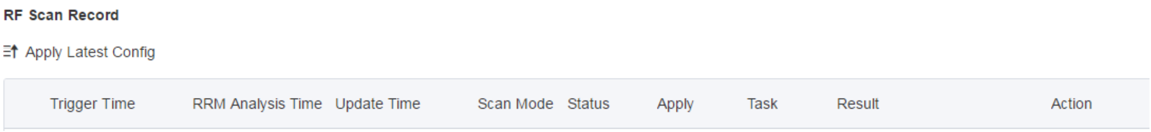
Skip this step if **Synch to Device** is enabled.

After the status in the record of the triggered RF planning becomes **Finish**, check the planning result, and synchronize the recommended RF configurations of the automatic planning to the APs or the locations of the APs. This step can be performed in two modes: location-based and AP-based.

- AP-based

This mode allows you to directly view the RF optimization results, and directly push the optimized configurations to APs of an organization, without relying on the location planning of the APs. Therefore, this mode is convenient and suitable for fast deployment, and can be used when the APs have no location planning or are not bound.

1. Click ▤ in the list to display the automatic RF planning result list of the APs.



RF Scan Record

Apply Latest Config

Trigger Time	RRM Analysis Time	Update Time	Scan Mode	Status	Apply	Task	Result	Action

In the RF optimization result list of the APs, **Recommended Power of Current Channel** indicates a recommended power value for the current channel. **Recommended Power of Recommended Channel** indicates a recommended power value for the recommended channel. It is calculated based on the recommended channel, and is configured together with the recommended channel.

2. Click 🖹 in the trigger record, and select a mode to push the recommended optimization configurations to the corresponding APs.

Three modes are available: pushing the recommended channel configurations, pushing the recommended power configurations of the current channel, and pushing the recommended power configurations of the recommended channel. You can select any of the three modes as required.

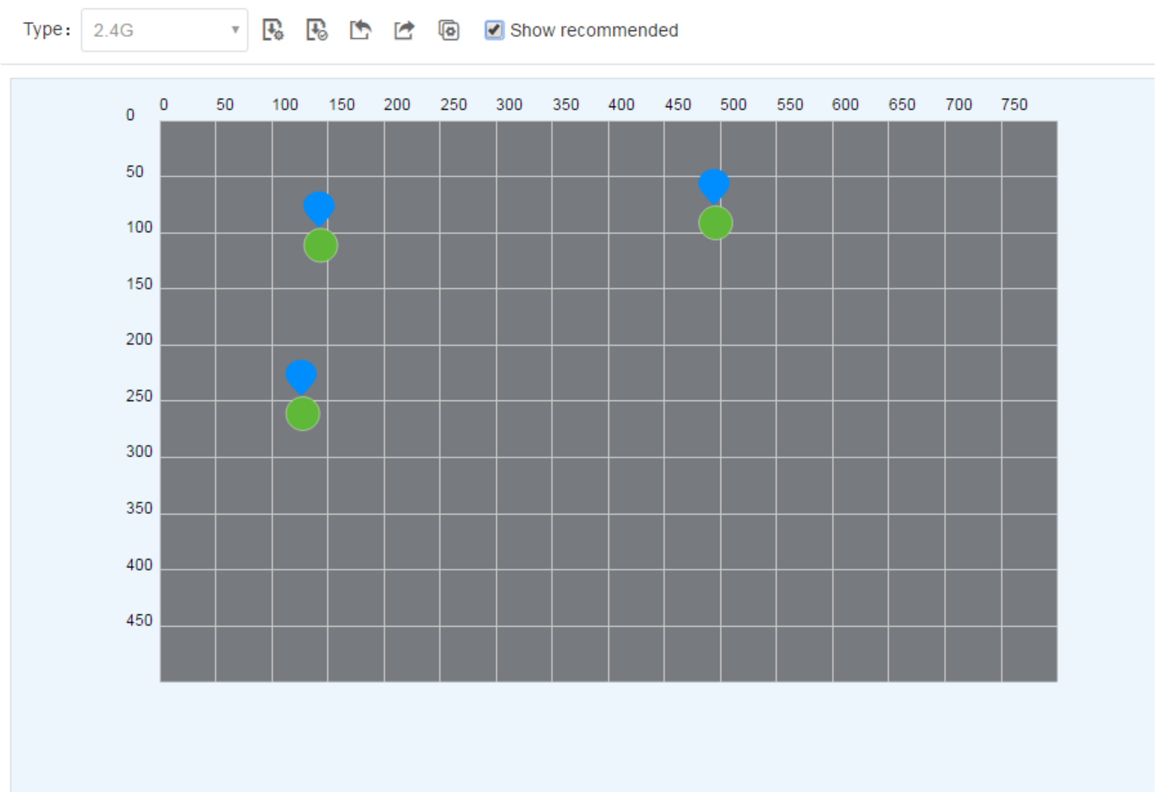
ℹ If an AP has been bound to a location and has been synchronized with RF configurations of the location. This operation will remove the RF synchronization between the location and the AP, and push the selected recommended optimization configurations to the AP.

- Location-based

Please make sure that the location planning of the network deployment has been completed, and an AP has been bound to a location. The advantages of this mode lie in clear display of the automatic RF planning results and location-based application of the recommended optimization configurations.

1. On a floor page for RF planning, select **Show recommended** to display the latest recommended values for automatic channel planning.

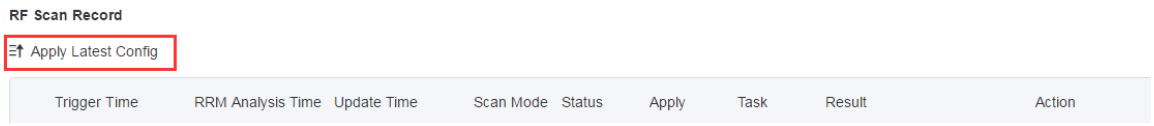
The values will be updated when an organization triggers automatic RF planning each time.



Type: 2.4G

☑ Show recommended

2. On the **RF Scan Record** page, click **Apply Latest Config** to save the planning results to the location.



RF Scan Record

Apply Latest Config

Trigger Time	RRM Analysis Time	Update Time	Scan Mode	Status	Apply	Task	Result	Action

After this step, the operation for synchronizing the RF configurations is the same as that in the manual RF planning mode. For details, refer to step 2 in chapter 3.2.1.

3.3 Roaming

Roaming planning refers to enabling the organization-based roaming.

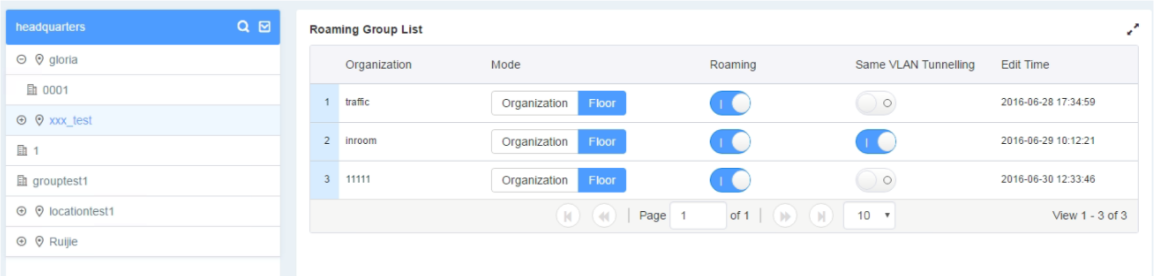
The MACC supports the organization-based roaming in two modes: Organization and Floor.

In Organization mode, all APs of a same organization serve as a roaming group.

In Floor mode, all APs on a same floor serve as a roaming group. Roaming across floors is not supported.

Roaming: Specify whether to enable roaming. By default, it is disabled.

Same VLAN Tunneling: Specify whether to enable same VLAN (L2) tunneling. By default, it is disabled.



Roaming Group List

	Organization	Mode	Roaming	Same VLAN Tunnelling	Edit Time
1	traffic	Organization [✓ Floor]	●	○	2016-06-28 17:34:59
2	inroom	Organization [✓ Floor]	●	●	2016-06-29 10:12:21
3	11111	Organization [✓ Floor]	●	○	2016-06-30 12:33:46

Page 1 of 1 10 View 1 - 3 of 3

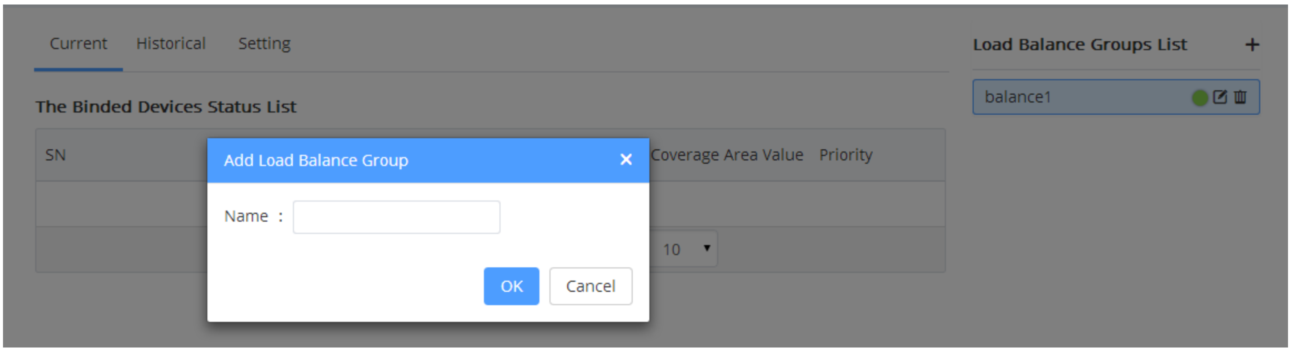
For wireless roaming, SSID signals must be consistent; otherwise, roaming may fail.

3.4 Load Balancing

The MACC load balancing function manages APs in a load balancing group, identifies APs on which the number of clients exceeds the limit, and leads new clients to associate with APs with less load.

Use of the load balancing function:

(1) Choose **Planning** > **Load Balance** and click + beside **Load Balance Groups List** to add a load balancing group.



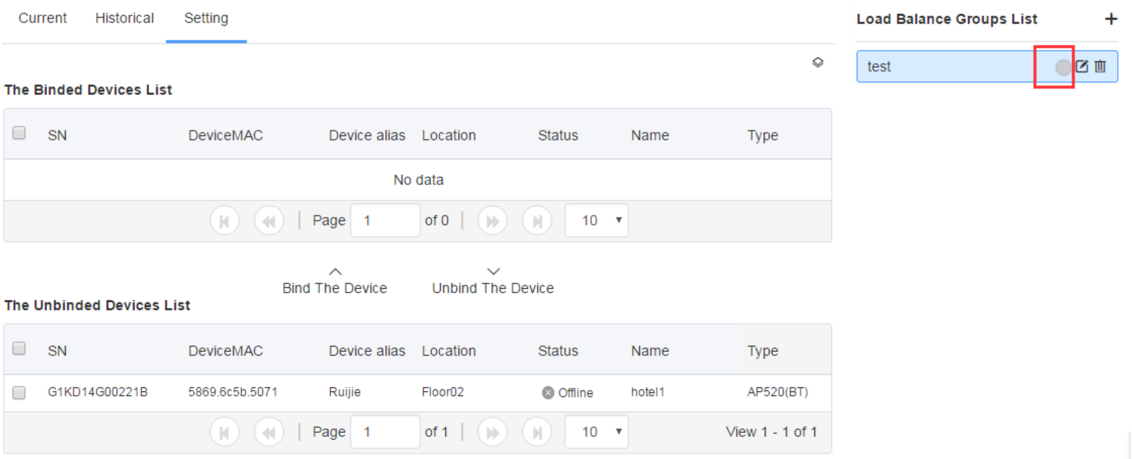
The Binded Devices Status List

SN	Coverage Area Value	Priority

Add Load Balance Group ✕

Name :

(2) On the **Setting** tab page, add APs to the required load balancing group. Click the ○ icon marked by the red frame in the following figure to enable the automatic load balancing function for this group.



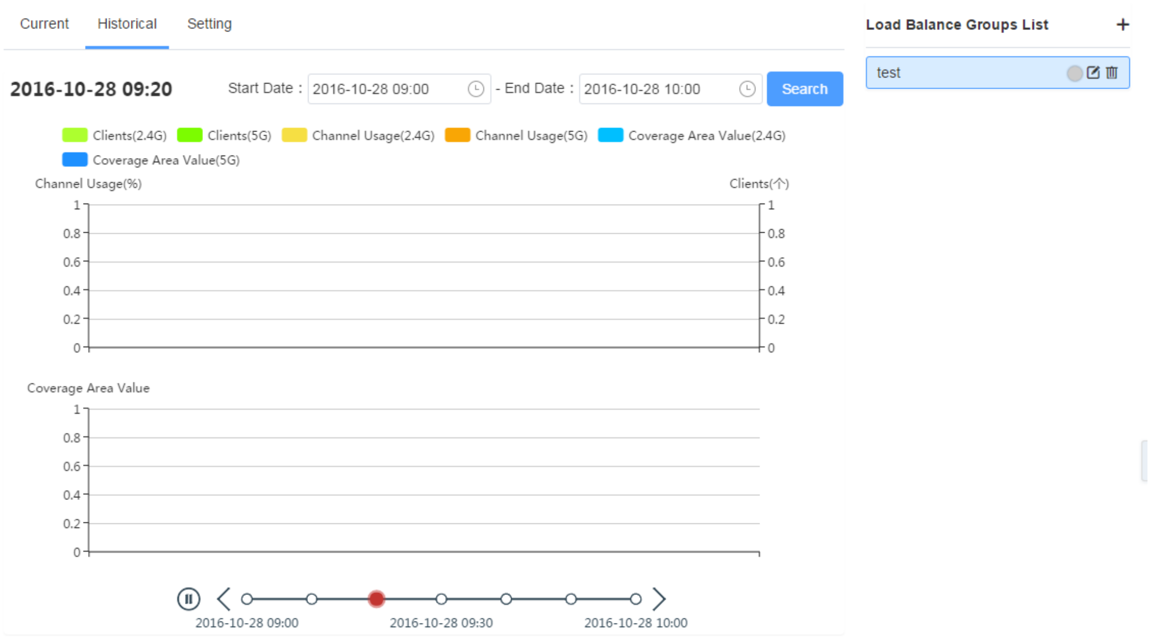
The Binded Devices List

□	SN	DeviceMAC	Device alias	Location	Status	Name	Type
No data							

The Unbinded Devices List

□	SN	DeviceMAC	Device alias	Location	Status	Name	Type
□	G1KD14G00221B	5869.6c5b.5071	Ruijie	Floor02	Offline	hotel1	AP520(BT)

(3) On the **Historical** tab page, you can query historical load balancing records.



2016-10-28 09:20

Start Date : 2016-10-28 09:00 - End Date : 2016-10-28 10:00

4 Configuration

The MACC configuration management module enables centralized configuration management on the entire wireless network, including the wireless AP configuration and the gateway configuration. The **Configuration** module provides two types of secondary menus, which respectively correspond to the wireless AP configuration and the gateway configuration.

Several wireless coverage areas usually co-exist in the same organization or on the same floor, and are formed by wireless APs in the organization or on the floor. Each wireless AP has the same function and plays the same role. Generally speaking, the configuration is also the same; therefore, the MACC configures wireless APs by floor or organization.

The **Configuration** module provides four submenus: **Settings**, **Gateway**, **Templates**, and **Logs**. **Gateway** enables the gateway configuration; **Settings**, **Templates**, and **Logs** correspond to the wireless AP configuration. The following two sections respectively describe **Settings** and **Gateway**.

4.1 Settings

The MACC configures wireless APs by floor or organization. The configuration by floor or organization is implemented via templates with configuration details. The wireless AP configuration mainly includes configuration template management, configuration validation, and configuration logs display.

4.1.1 Templates

Choose **Configuration** > **Templates**.

The **Templates** page provides the add, edit, copy, and share functions.

4.1.2 Adding Templates

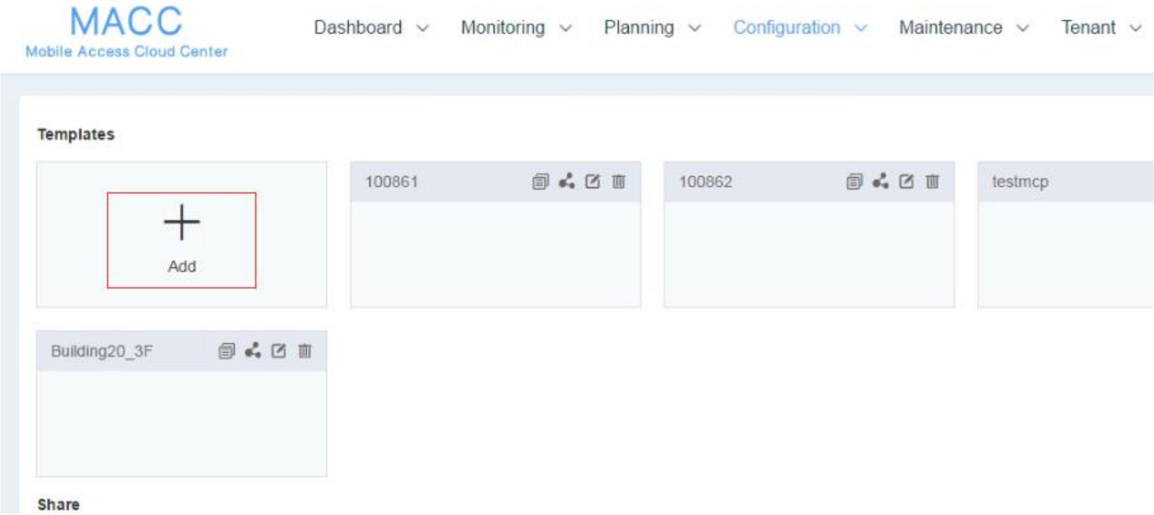
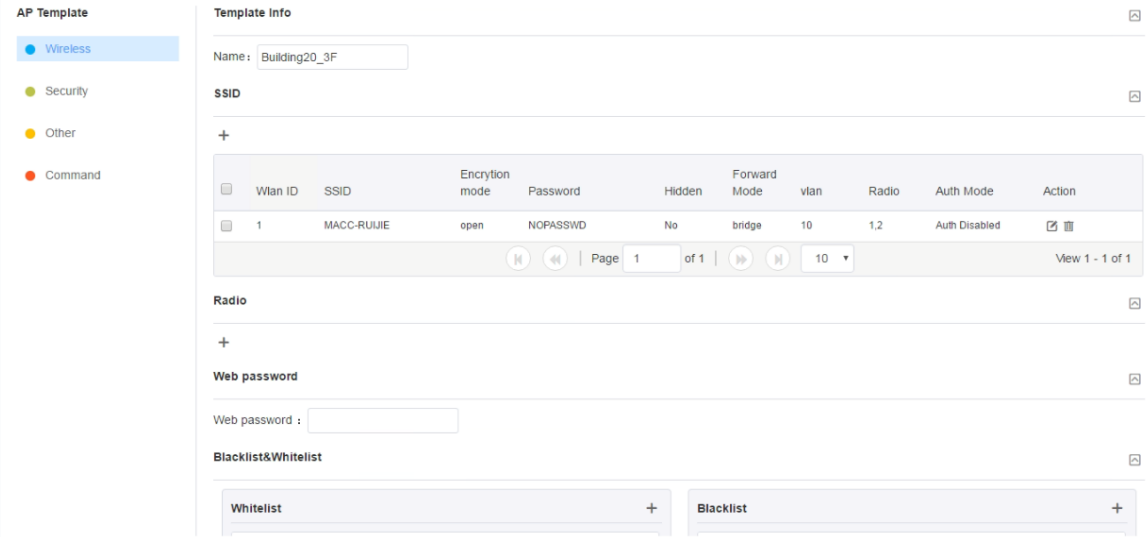


Figure 4-1 Adding Templates

On the **Templates** interface, click **Add**, enter a template name. The **AP Templates** page appears.

4.1.3 Editing Templates



Name： Building20_3F

☐	Wlan ID	SSID	Encrytion mode	Password	Hidden	Forward Mode	vlan	Radio	Auth Mode	Action
☐	1	MACC-RUIJIE	open	NOPASSWD	No	bridge	10	1,2	Auth Disabled	

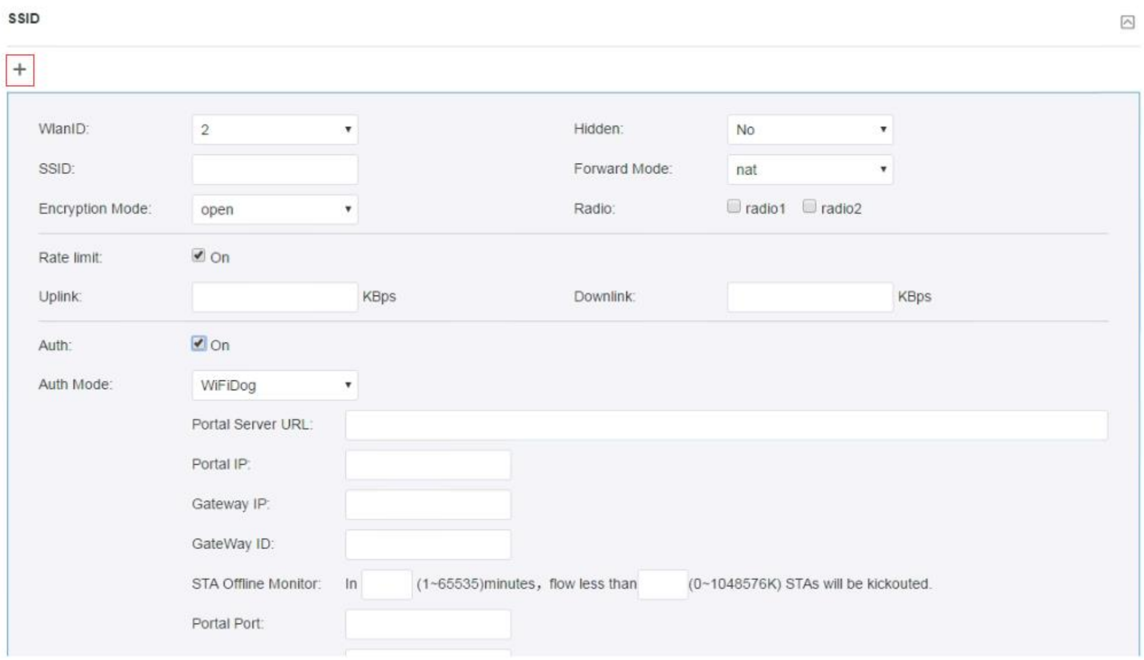
Page 1 of 1 10 View 1 - 1 of 1

Web password：

Figure 4-2 Editing Templates

On the **AP Template** page, the menu bar on the left displays **Wireless**, **Security**, **Others**, and **Command**, and the area on the right displays **SSID**, **Radio**, **Web password**, and **Blacklist/Whitelist**, **CWMP**, and **CLI** correspondingly. The following describes several configuration items.

- SSID


SSID

+

WlanID: 2 Hidden: No

SSID: Forward Mode: nat

Encryption Mode: open Radio: □ radio1 □ radio2

Rate limit: ☑ On

Uplink: KBps Downlink: KBps

Auth: ☑ On

Auth Mode: WiFiDog

Portal Server URL:

Portal IP:

Gateway IP:

GateWay ID:

STA Offline Monitor: In (1~65535)minutes，flow less than (0~1048576K) STAs will be kickouted.

Portal Port:

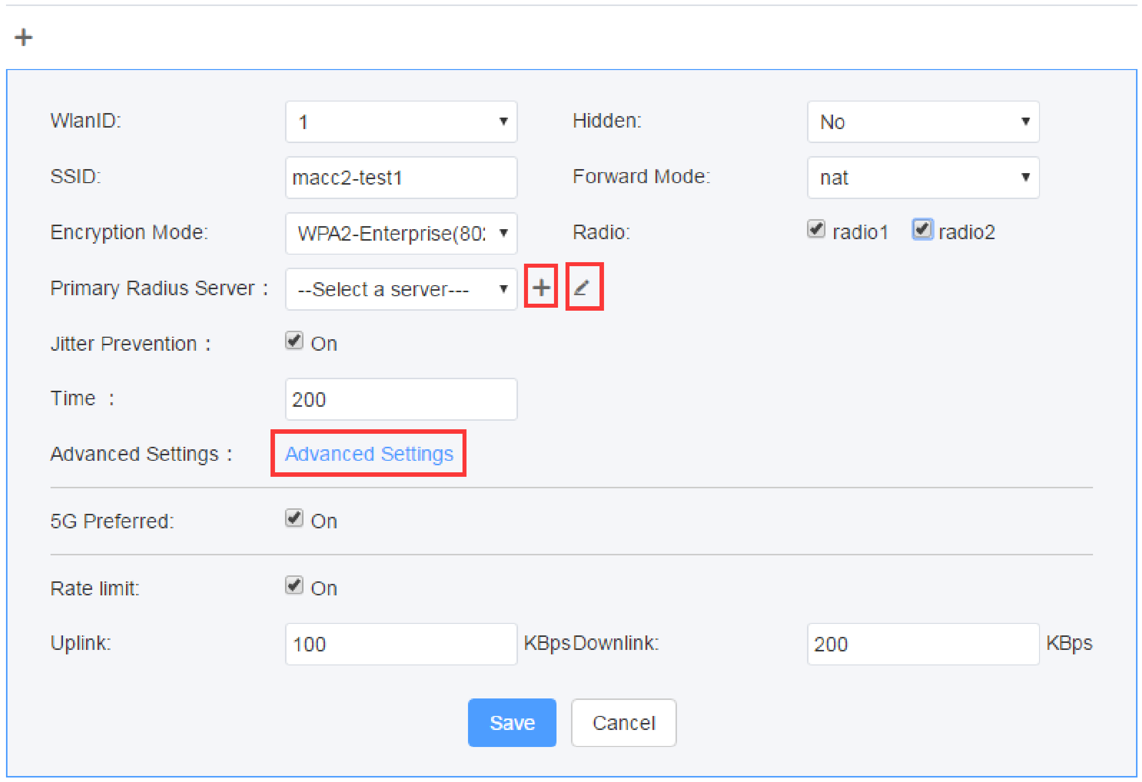
Figure 4-3 SSID

Click **+** in the upper left corner to add an SSID. In addition, the **SSID** page further enables you to configure the rate limit and the authentication function. Parameters on the **SSID** page are defined as follows.

WlanID: Select a WLAN ID. An SSID matches a WLAN ID one to one. The WLAN ID can be specified only when an SSID is added and cannot be changed subsequently. The maximum value of **WlanID** is 32.

SSID: Enter an SSID name.

Encryption Mode: Four modes are available: **open**, **wpa-psk**, **wpa2-psk** and **wpa2-Enterprise(802.1x)**. **open** indicates that no password needs to be configured; **wpa-psk** or **wpa2-psk** indicates that a password needs to be configured. **WPA2-Enterprise(802.1x)** indicates that the 802.1x authentication mode is adopted for the SSID. After the 802.1x authentication mode is selected, the following page is displayed.


+

WlanID: 1 Hidden: No

SSID: macc2-test1 Forward Mode: nat

Encryption Mode: WPA2-Enterprise(80: Radio: ☑ radio1 ☑ radio2

Primary Radius Server： --Select a server---

Jitter Prevention： ☑ On

Time ： 200

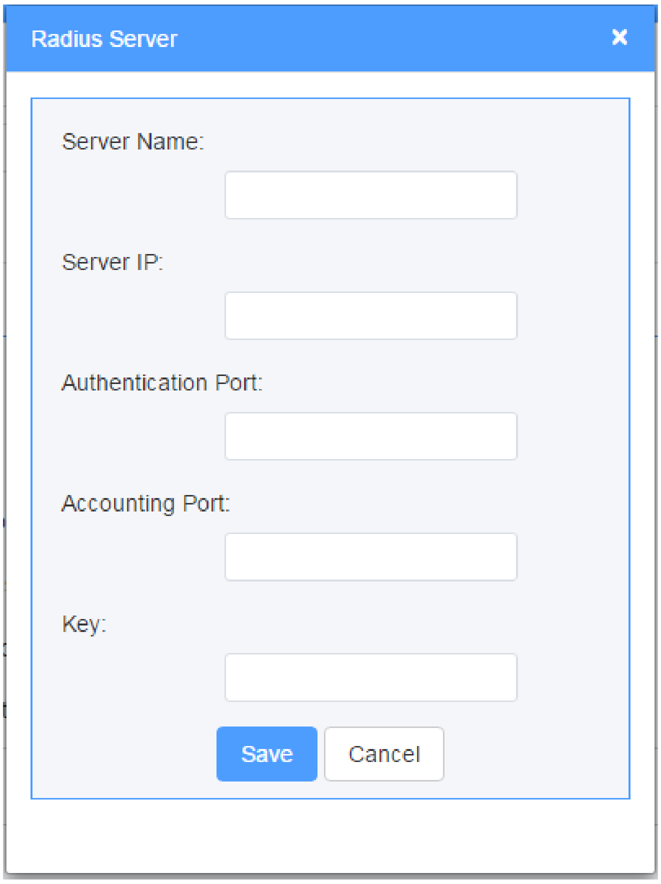
Advanced Settings： Advanced Settings

5G Preferred: ☑ On

Rate limit: ☑ On

Uplink: 100 KBps Downlink: 200 KBps

Click + to add an authentication server. A dialog box for Radius server configuration is displayed, as shown in the following figure.



Radius Server

Server Name:

Server IP:

Authentication Port:

Accounting Port:

Key:

Server IP, **Authentication Port**, **Accounting Port**, and **Key** can be configured for a RADIUS server. **Authentication Port** and **Accounting Port** are optional, and are set to the default values **1812** and **1813** respectively if no values are entered. The jitter prevention function can be configured in 802.1x authentication mode, as shown in the SSID configuration page with **Encryption Mode** set to **WPA2-Enterprise(802.1x)**. After the jitter prevention function is enabled (the jitter prevention duration range is 0–600), clients will not go offline within the jitter prevention duration in case of jitters. The default jitter prevention duration of an AP is 2 seconds. Note that the jitter prevention function may not be supported in earlier AP versions. In addition, the **Advanced Settings** function is provided for 802.1x authentication. In **Advanced Settings**, the NAS IP address (available in the NAT environment) and accounting update period can be configured and the added authentication server can be managed.

Hidden: Specify whether to hide the SSID, which can be set to **Yes** or **No**.

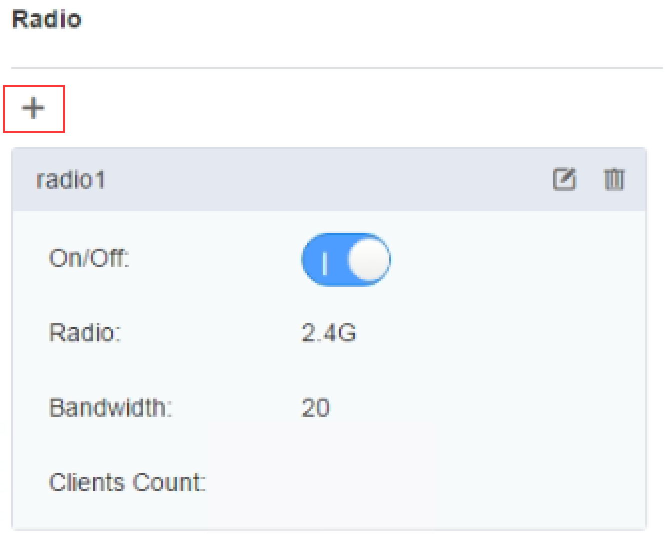
Forward Mode: Select a forward mode of a wireless AP. **nat** indicates that an IP address is allocated to a client by an AP; **bridge** indicates that an IP address is allocated to a client by an upstream device of an AP. A VLAN ID must be configured when the **bridge** mode selected.

5G Preferred: It is enabled when the SSID is associated with Radio 1 and Radio 2 for dual-band APs (2.4 GHz and 5 GHz), so as to ensure that clients supporting dual bands access the 5 GHz frequency band preferentially, thereby reducing the load in the 2.4 GHz frequency band and improving user experience.

Rate limit: Specify whether to enable the rate limit function for a client. When this function is enabled, uplink and downlink rates must be configured.

Auth Mode: Select **WiFiDog** or **WiFi via WeChat**.

- Radio



Radio

+

radio1

On/Off: ●

Radio: 2.4G

Bandwidth: 20

Clients Count:

Figure 4-4 Radio

The Radio page enables you to configure the radio ports of APs. As shown in Figure 4-4, the **Radio** page provides the **On/Off**, **Radio**, **Bandwidth**, and **Client Count** items; and you can choose **Planning** > **RF** to configure the radio channel power. Parameters on the **Radio** page are defined as follows:

On/Off: Specify whether to enable the radio function. When it is set to **Off**, the SSID is invalid; the corresponding SSID can be used properly only when this function is set to **On**.

Radio: Select the radio type, which can be configured as 2.4 GHz or 5 GHz, and is only valid to part of APs. Some AP hardware does not support radio switching.

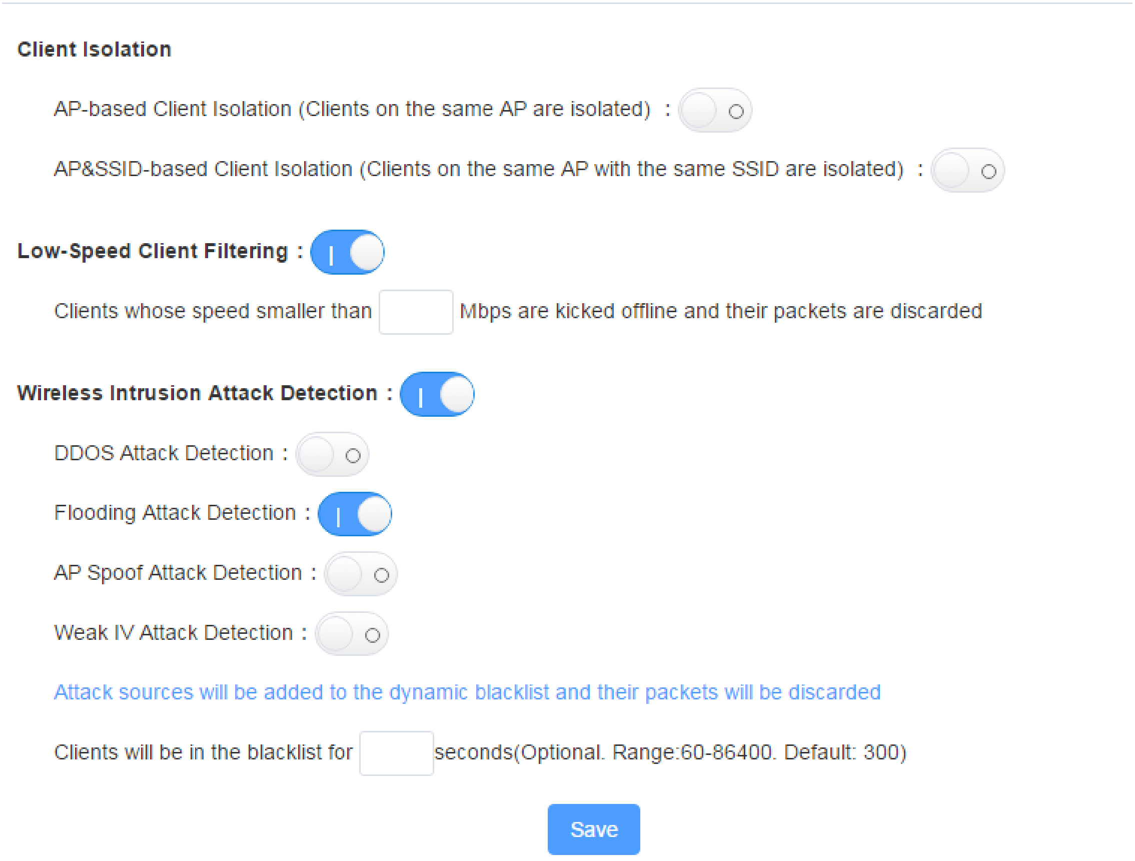
Bandwidth: Enter the radio bandwidth. A smaller bandwidth indicates a farther wireless signal transmission distance and better penetrability, which, however, is more vulnerable to interference. **Bandwidth** can be set to **20**, **40**, or **80**. Note that **Bandwidth** cannot be set to **80** for partial APs.

Clients Count: Enter the upper limit of associated clients in a frequency band.

Deletion of the radio configurations indicates that the MACC preserves the current configurations.

Web password: Enter the web login password of an AP. When the password is empty, the MACC does not push the password.

- Radio security configuration



Client Isolation

AP-based Client Isolation (Clients on the same AP are isolated) : ○

AP&SSID-based Client Isolation (Clients on the same AP with the same SSID are isolated) : ○

Low-Speed Client Filtering : I

Clients whose speed smaller than ____ Mbps are kicked offline and their packets are discarded

Wireless Intrusion Attack Detection : I

DDOS Attack Detection : ○

Flooding Attack Detection : I

AP Spoof Attack Detection : ○

Weak IV Attack Detection : ○

Attack sources will be added to the dynamic blacklist and their packets will be discarded

Clients will be in the blacklist for ____ seconds(Optional. Range:60-86400. Default: 300)

Save

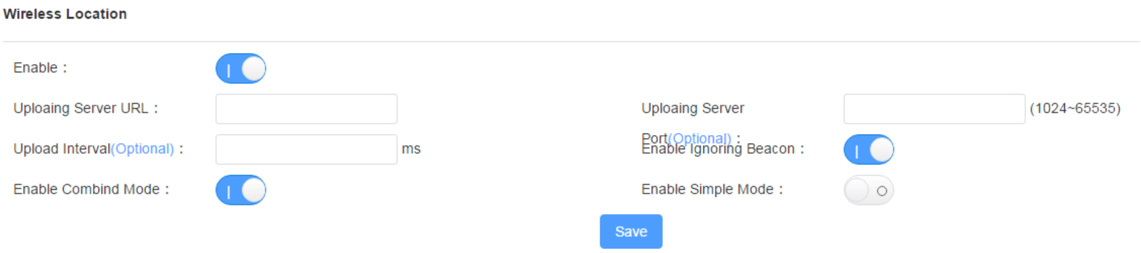
As shown in the preceding figure, **Client Isolation**, **Low-Speed Client Filtering**, and **Wireless Intrusion Attack Detection** can be configured.

Client Isolation: Clients are isolated without affecting their network access to ensure that they cannot communicate with each other, thereby ensuring client service security. AP-based client isolation or AP&SSID-based client isolation can be selected. If AP-based client isolation is enabled, all layer-2 clients associated with the same AP cannot communicate with each other. If AP&SSID-based client isolation is enabled, clients in the same WLAN on the same AP cannot communicate with each other.

Low-Speed Client Filtering: Clients whose speed is lower that the preset threshold will be forced to go offline.

Wireless Intrusion Attack Detection: Include DDOS attack detection, flooding attack detection, spoof attack detection, and weak IV attack detection. If this function is enabled, at least one of the preceding four detection functions needs to be enabled. In addition, the dynamic blacklist function will be enabled, and the dynamic blacklist duration can be configured.

- Wireless Location



Wireless Location

Enable : I

Uploaing Server URL : ____

Uploaing Server Port(Optional) : ____ (1024~65535)

Upload Interval(Optional) : ____ ms

Enable Ignoring Beacon : I

Enable Combind Mode : I

Enable Simple Mode : ○

Save

To configure the wireless location function, the wireless location switch needs to be enabled, as shown in the preceding figure. The wireless location function of an AP can be used in combination with a location server. Therefore, the IP address and port number of the location server need to be configured to ensure normal communication between the AP and location server. In addition, the uploading interval can be configured and is set to 300 ms by default. **Enable ignoring**

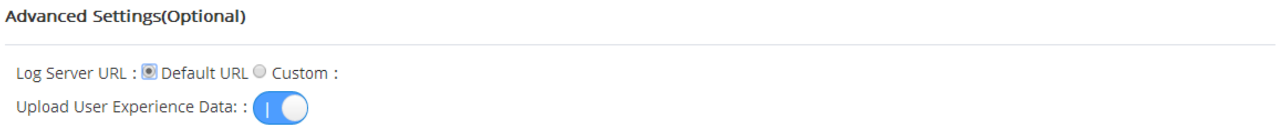
Beacon can filter beacon packets sent by the AP to reduce bandwidth consumption. **Enable Simple Mode** is available only when a location server developed by Ruijie is used, and can reduce bandwidth consumption.

Blacklist&Whitelist: Enter blacklisted websites, and websites that can be accessed directly without authentication. Generally, the blacklist and whitelist take effect only after **Auth** is set to **On**. The MACC clears the AP blacklist/whitelist when this parameter is empty.

CWMP Keepalive Interval: Enter the AP CWMP keepalive interval. The MACC does not push the CWMP keepalive interval when this parameter is empty.

CLI Command: Enter commands to be pushed to APs. This function allows you to perform some configurations unsupported by MACC via CLI commands.

- Advanced Settings



Advanced Settings(Optional)

Log Server URL : ● Default URL ○ Custom :

Upload User Experience Data: :

Log Server URL: Set the log server URL for AP log uploading. The default URL or a customized URL can be used.

Upload User Experience Data: Enable **Upload User Experience Data** to enable the AP to upload user experience logs.

4.1.3.1 Copying and Sharing Templates

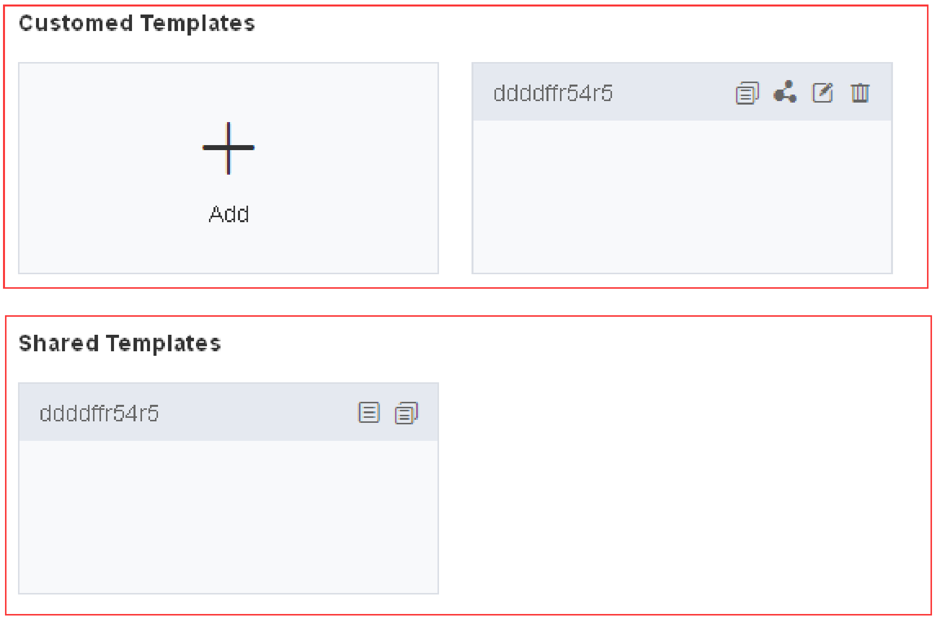


Figure 4-5 Templates and Share Modules

As shown in Figure 4-5, the configuration template interface provides the **Customed Templates** and **Share Templates** modules.

The **Customed Templates** module displays templates of the current client, and enables the client to add, copy, share, edit, delete, and apply these templates. Only a template in the **Customed Templates** module can be applied.

The **Shared Templates** module displays templates shared by other clients of the same tenant with the current client, and enables the clients to view and copy these templates.

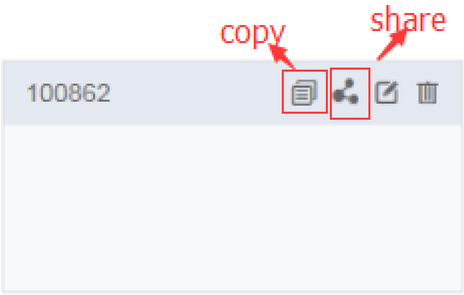


Figure 4-6 Copying and Sharing Templates

The MACC provides the copy and share functions to quickly add templates.

On the **Templates** module, as shown in figure 4-6, each template provides four buttons in the upper right corner, which respectively indicate the copy, share, edit, and delete functions.

After a template is copied, the client can edit the added template.

After a template is shared, other clients of the same tenant can view and copy the template in the **Shared Templates** module.

Only unbound templates can be shared.

4.1.3.2 Deleting Templates

As shown in Figure 4-6, click 🗑 to delete templates.

Only unbound templates can be deleted.

4.1.4 Applying Configurations

After a template is configured, the MACC applies the template to a floor or organization for the template to take effect

Choose **Configure** > **Setting**. The **Wireless** page provides **Apply**, **Switch**, and **Delete** functions for a floor or organization to implement the wireless AP configuration management.

The MACC only applies templates to organizations and floors. Each organization or floor can only apply one template; however, one template can be applied to multiple organizations or floors.

4.1.4.1 Applying Templates

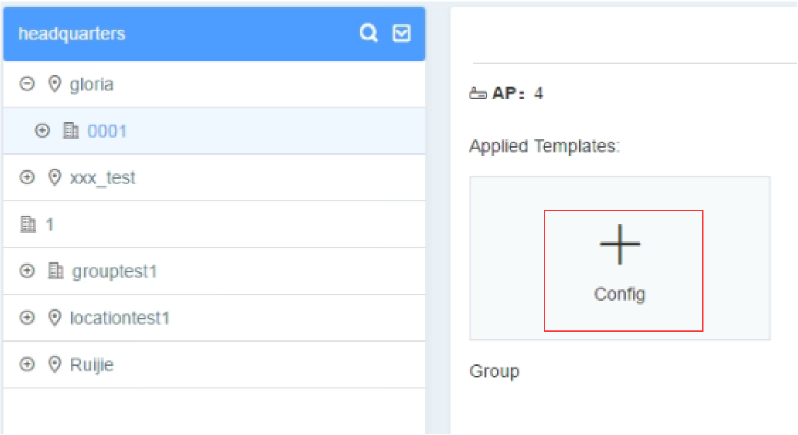


Figure 4-7 Binding Templates

- As shown in Figure 4-7, click the organization or floor that requires template application, and click **+** on the right to open the **Select Template** page.

As shown in Figure 4-8, select a corresponding template, and click **Save** in the lower right corner.

If the organization or the floor has online APs, the MACC immediately push configurations to the APs.

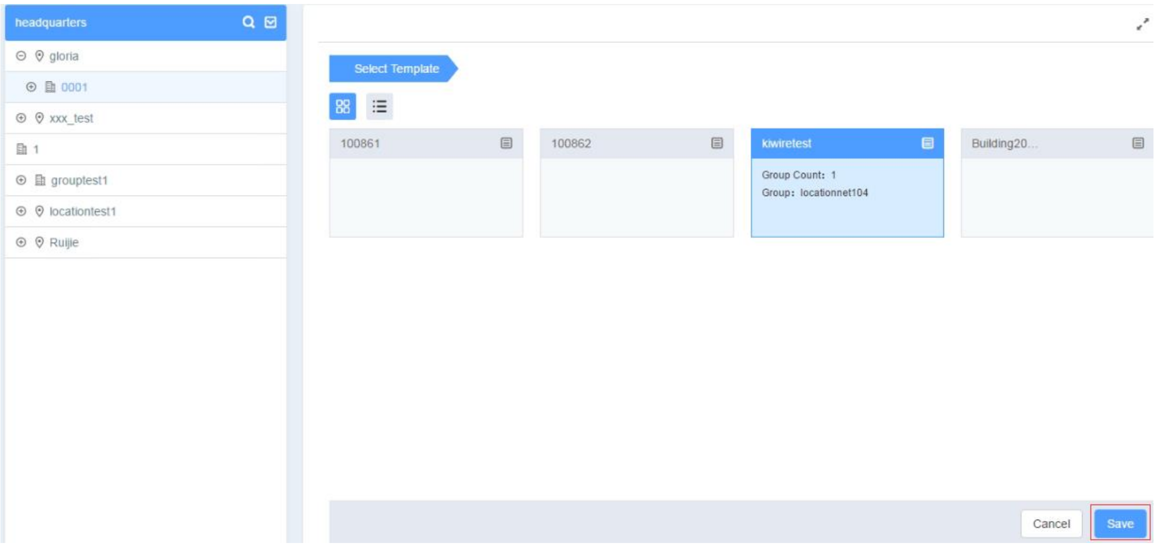


Figure 4-8 Selecting Templates

4.1.4.2 Templates Effectiveness Scope

After templates are applied, the configuration scope is compliant with certain rules. When an organization applies a template, it does not mean that organizations or floors under the organization all apply the configurations in the template. Likewise, when a floor or an organization does not apply a template, it also does not mean that the MACC does not push configurations to the floor or organization.

There is hierarchy between an organization and a floor, which are considered as groups. The MACC configuration follows such a principle: The MACC searches for groups having a template from the current group to upper-level groups, and push configurations corresponding to the template to found groups. In this way, if a floor does not apply a template but the parent organization of this floor applies a template, the MACC pushes configurations based on the template of the organization to the floor. If a floor and its parent organization apply different templates, the MACC configures the floor based on its own template and does not push configurations of the template applied by the parent organization.

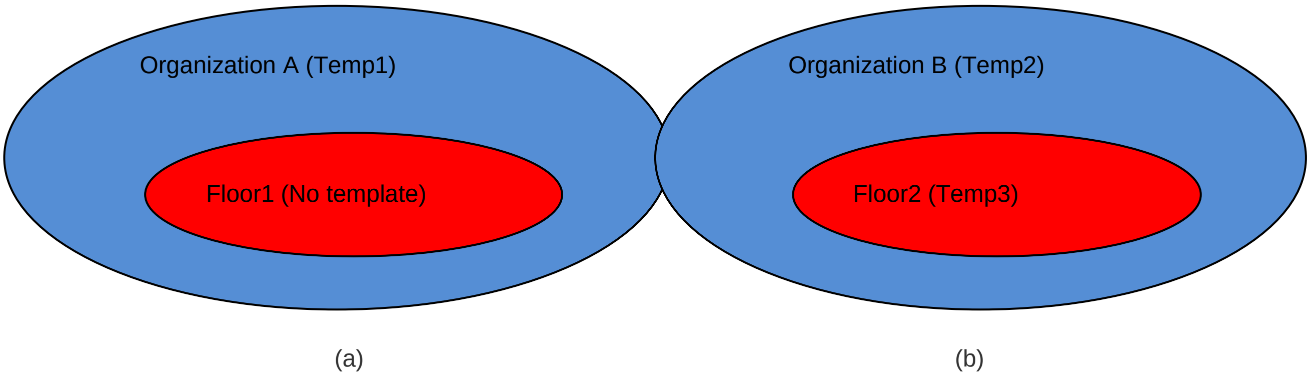


Figure 4-9 Example of the Template Effectiveness Scope

Figure 4-9 shows an example of the template effectiveness scope.

In (a), Organization A includes Floor 1. Organization A applies Temp 1 but Floor 1 does not. In this case, APs in Organization A and APs on Floor 1 both apply configurations of Temp 1.

In (b), Organization B applies Temp 2 but Floor 2 applies Temp 3. In this case, APs in Organization B apply configurations of Template 2, and APs on Floor 2 apply configurations of Temp 3.

4.1.4.3 Pushing Configurations

To simplify operation procedures, after organizations or floors apply templates, the MACC automatically push configurations to APs of the organizations or floors. The MACC pushes configurations mainly in the following situations:

- Template application or switching

After a floor or an organization applies or switches a template, the APs in the corresponding group synchronize with the configurations of the template. For online APs, the MACC immediately pushes the configurations to the APs. For offline APs, the MACC also automatically pushes the configurations after the APs go online, to ensure the AP configurations are synchronous with those of the MACC. In addition, after removing a template from a group, if an upper-level group of this group applies a template, the MACC pushes configurations of this new template to APs in this group.

- Template update

After configurations in a template are updated, if the template has been applied to some organizations or floors, the MACC automatically pushes the updated configurations to corresponding APs.

- AP first online

When an AP goes online for the first time, the MACC pushes configurations of a template of a corresponding group (or a template of an upper-level group) to the AP.

- AP version change

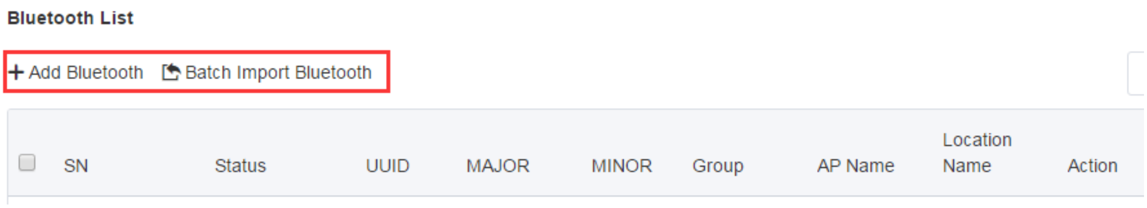
After the version of an AP changes, the MACC pushes configurations of a template corresponding to the AP's group (or a template of an upper-level group) to the AP.

- AP group change

After the group of an AP changes, the MACC pushes configurations of a template corresponding to the new group (or a template of an upper-level group) to the AP.

4.1.5 Configuring Bluetooth

Bluetooth configuration functions include Bluetooth configuration batch import, Bluetooth configuration adding for a single AP, Bluetooth configuration modification, and Bluetooth configuration deletion, as shown in the following figure:



Bluetooth List

☐	SN	Status	UUID	MAJOR	MINOR	Group	AP Name	Location Name	Action

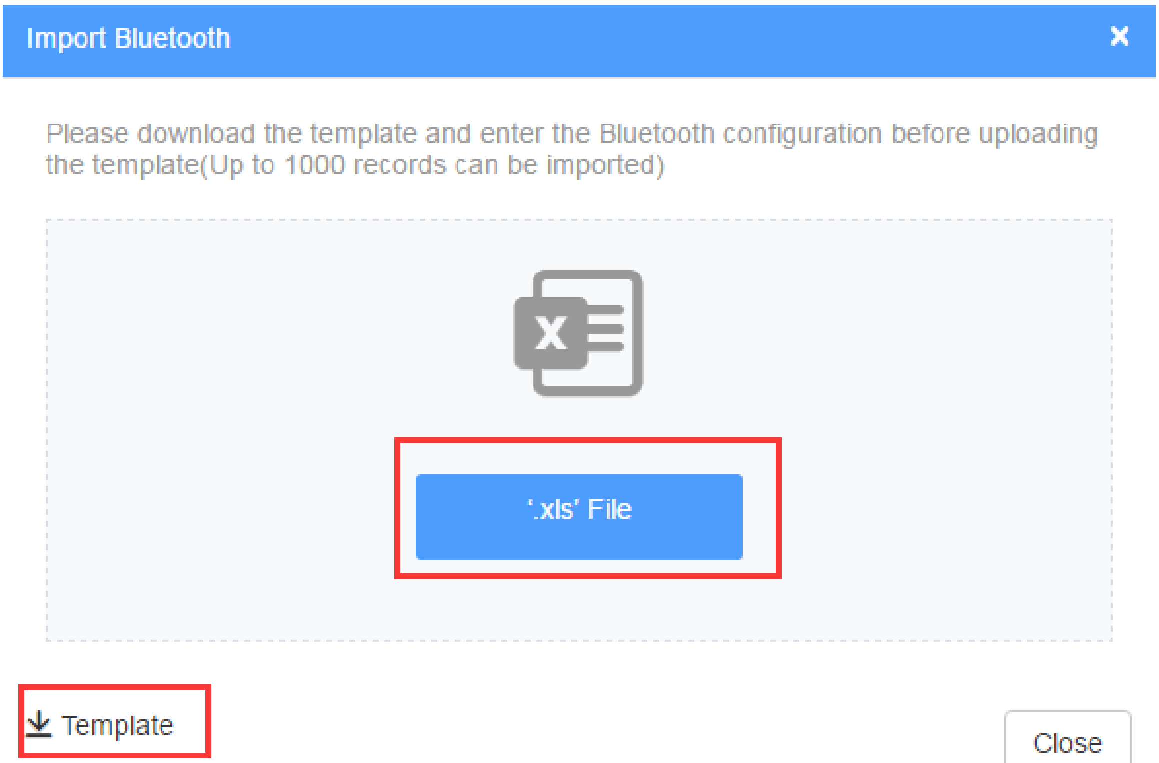
- Bluetooth configuration batch import

Click **Batch import Bluetooth**. The **Import Bluetooth** dialog box is displayed. For initial use, you can click **Template** in the lower left corner to export an EXCEL file corresponding to APs in the current group and set corresponding parameters in the file. Requirements for the **UUID**, **MAJOR**, and **MINOR** parameters are as follows:

UUID: Enter a string of 32 characters in hexadecimal format.

MAJOR: Enter a string of 4 characters in hexadecimal format.

MINOR: Enter a string of 4 characters in hexadecimal format.

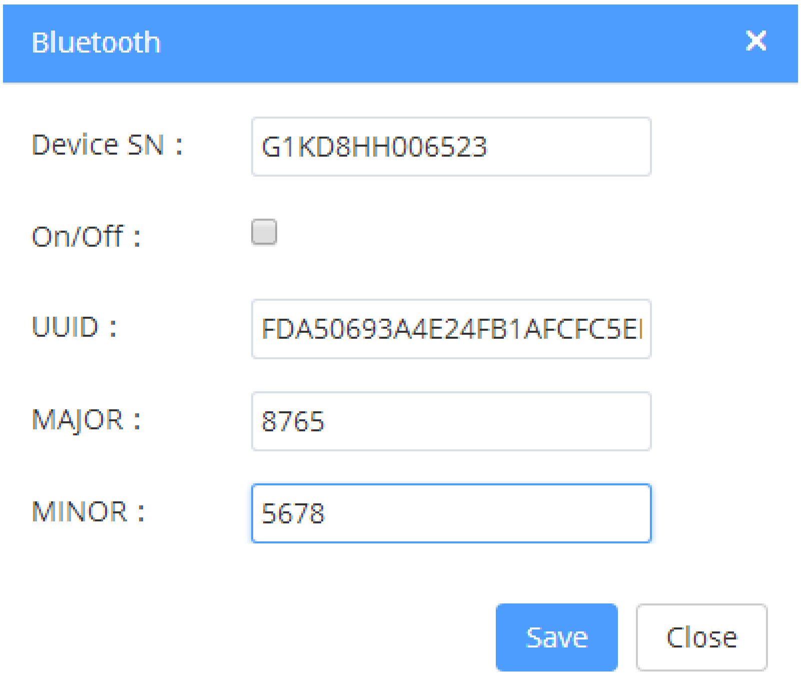


Import Bluetooth ×

Please download the template and enter the Bluetooth configuration before uploading the template(Up to 1000 records can be imported)

After the parameters in the EXCEL file are configured, click **'.xls' File** to import the file. A prompt will be displayed if an exception occurs during the import.

- Bluetooth configuration adding for a single AP



Bluetooth ×

Device SN : G1KD8HH006523

On/Off : □

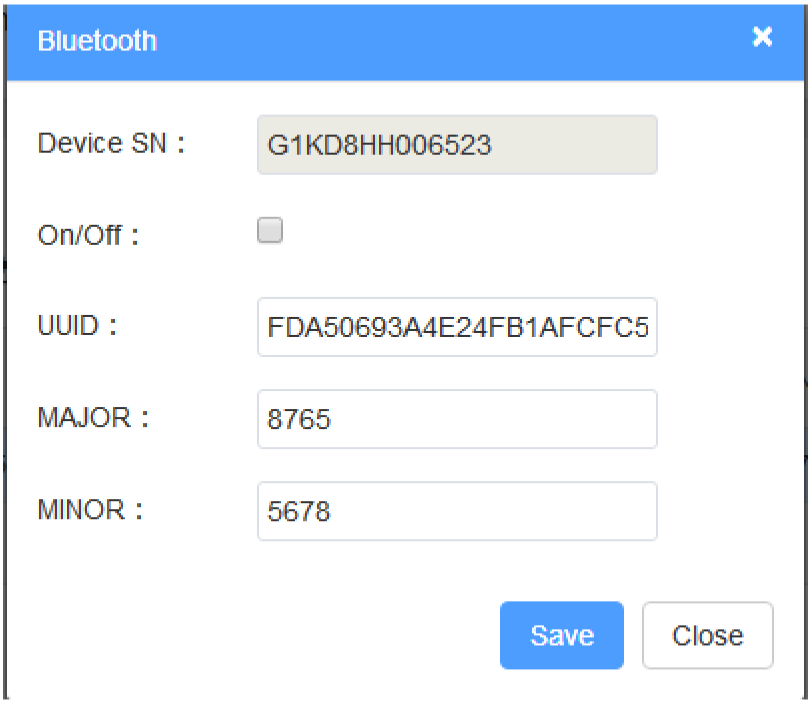
UUID : FDA50693A4E24FB1AFCFC5EI

MAJOR : 8765

MINOR : 5678

Click **Add Bluetooth**. The **Bluetooth** dialog box is displayed, as shown in the preceding figure. Specify the parameters as required to add Bluetooth configuration for one AP and click **Save**. If Bluetooth configuration is already configured for the AP, the existing Bluetooth configuration will be updated.

- Bluetooth configuration modification for a single AP



Bluetooth

Device SN : G1KD8HH006523

On/Off : □

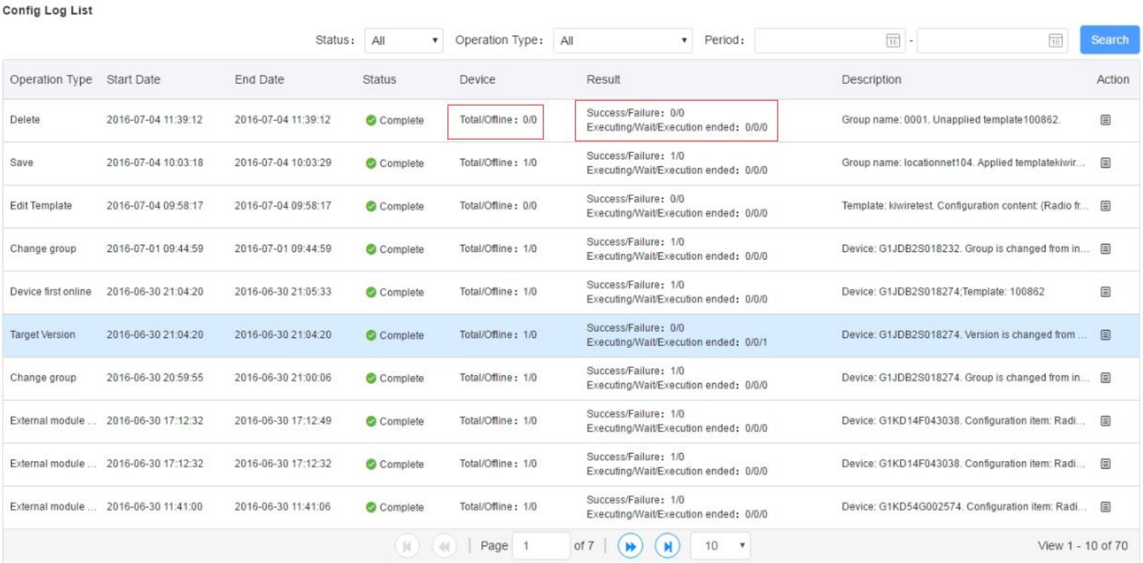
UUID : FDA50693A4E24FB1AFCFC5

MAJOR : 8765

MINOR : 5678

Click **Add Bluetooth**. The **Bluetooth** dialog box is displayed, as shown in the preceding figure. Modify the required parameters and click **Save**.

4.1.6 Checking Configuration Logs



Config Log List

Status: All Operation Type: All Period:

Operation Type	Start Date	End Date	Status	Device	Result	Description	Action
Delete	2016-07-04 11:39:12	2016-07-04 11:39:12	✓ Complete	Total/Offline：0/0	Success/Failure：0/0 Executing/Wait/Execution ended：0/0/0	Group name: 0001. Unapplied template100862.	☰
Save	2016-07-04 10:03:18	2016-07-04 10:03:29	✓ Complete	Total/Offline：1/0	Success/Failure：1/0 Executing/Wait/Execution ended：0/0/0	Group name: locationnet104. Applied templatekiwir...	☰
Edit Template	2016-07-04 09:58:17	2016-07-04 09:58:17	✓ Complete	Total/Offline：0/0	Success/Failure：0/0 Executing/Wait/Execution ended：0/0/0	Template: kiwiretest. Configuration content: {Radio fr...	☰
Change group	2016-07-01 09:44:59	2016-07-01 09:44:59	✓ Complete	Total/Offline：1/0	Success/Failure：1/0 Executing/Wait/Execution ended：0/0/0	Device: G1JDB2S018232. Group is changed from in...	☰
Device first online	2016-06-30 21:04:20	2016-06-30 21:05:33	✓ Complete	Total/Offline：1/0	Success/Failure：1/0 Executing/Wait/Execution ended：0/0/0	Device: G1JDB2S018274;Template: 100862	☰
Target Version	2016-06-30 21:04:20	2016-06-30 21:04:20	✓ Complete	Total/Offline：1/0	Success/Failure：0/0 Executing/Wait/Execution ended：0/0/1	Device: G1JDB2S018274. Version is changed from ...	☰
Change group	2016-06-30 20:59:55	2016-06-30 21:00:06	✓ Complete	Total/Offline：1/0	Success/Failure：1/0 Executing/Wait/Execution ended：0/0/0	Device: G1JDB2S018274. Group is changed from in...	☰
External module ...	2016-06-30 17:12:32	2016-06-30 17:12:49	✓ Complete	Total/Offline：1/0	Success/Failure：1/0 Executing/Wait/Execution ended：0/0/0	Device: G1KD14F043038. Configuration item: Radi...	☰
External module ...	2016-06-30 17:12:32	2016-06-30 17:12:32	✓ Complete	Total/Offline：1/0	Success/Failure：1/0 Executing/Wait/Execution ended：0/0/0	Device: G1KD14F043038. Configuration item: Radi...	☰
External module ...	2016-06-30 11:41:00	2016-06-30 11:41:06	✓ Complete	Total/Offline：1/0	Success/Failure：1/0 Executing/Wait/Execution ended：0/0/0	Device: G1KD54G002574. Configuration item: Radi...	☰

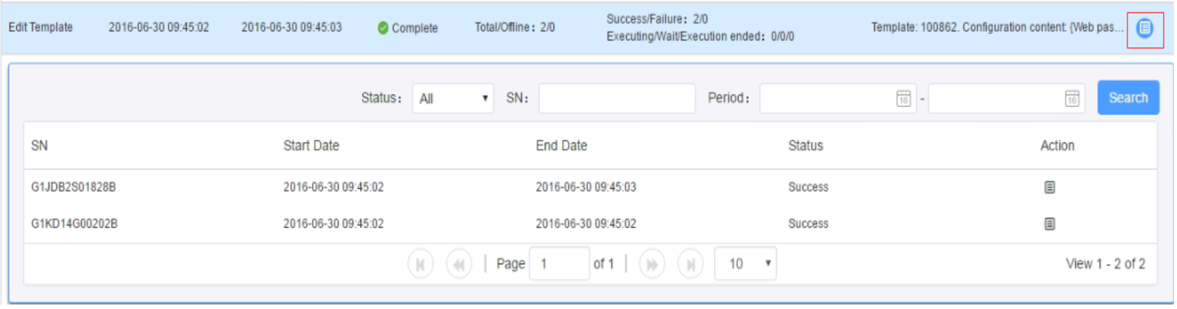
Page 1 of 7 10 View 1 - 10 of 70

Figure 4-10 Configuration Log List (First Level)

The configuration logs record the information about MACC configuration changes and pushing in three levels. As shown in Figure 4-10, the first level records operation types that cause the configuration change or configuration pushing. The operation types include: apply templates, update templates, switch templates, and version upgrade. In addition, the first-level logs also record the running status statistics and some parameters.

1. Click ☰ to check APs involved by the operation type.

Figure 4-11 shows the configuration application statuses: **Success**, **Failure**, or **Offline**.



Edit Template 2016-06-30 09:45:02 2016-06-30 09:45:03 Complete Total/Offline：2/0 Success/Failure：2/0 Executing/Wait/Execution ended：0/0/0 Template: 100862. Configuration content: {Web pas...

Status： All SN： Period： - Search

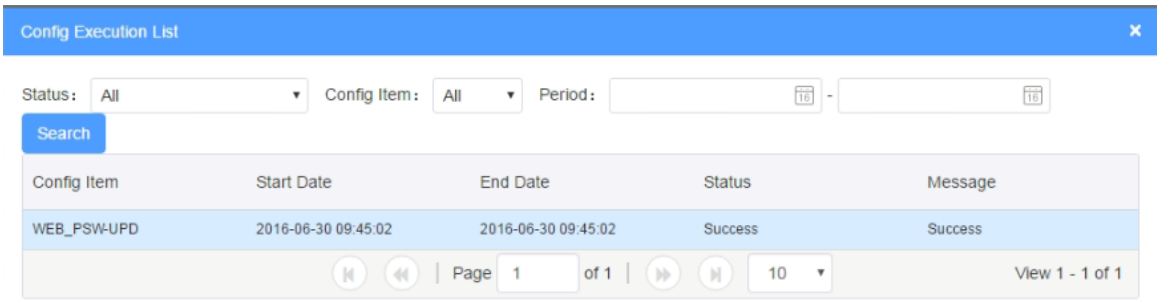
SN	Start Date	End Date	Status	Action
G1JDB2S01828B	2016-06-30 09:45:02	2016-06-30 09:45:03	Success	▤
G1KD14G00202B	2016-06-30 09:45:02	2016-06-30 09:45:02	Success	▤

Page 1 of 1 10 View 1 - 2 of 2

Figure 4-11 Configuration Log List (Second Level)

2. Click the rightmost action column of the second-level logs to check the push status of each configuration item.

Figure 4-12 shows an example of full configurations, including the configuration execution status of **SSID**, **Auth**, **Radio**, **CWMP Keepalive Interval**, and **Blacklist&Whitelist**.



Config Execution List

Status： All Config Item： All Period： -

Search

Config Item	Start Date	End Date	Status	Message
WEB_PSW-UPD	2016-06-30 09:45:02	2016-06-30 09:45:02	Success	Success

Page 1 of 1 10 View 1 - 1 of 1

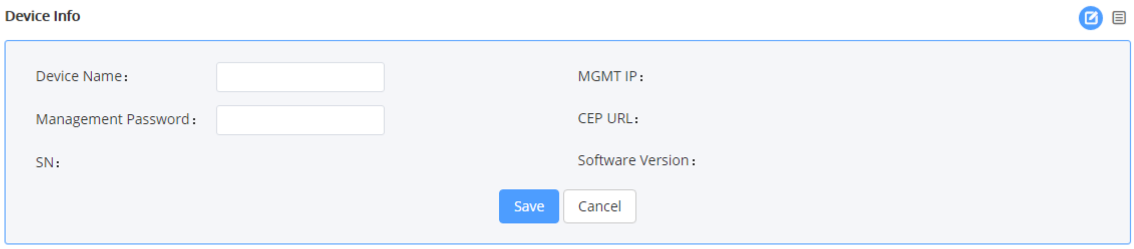
Figure 4-12 Configuration Log List (Third Level)

4.2 Gateway

A gateway is the egress device of wireless APs. Gateway configuration mainly include basic information configuration, configuration backup, and configuration reverting.

Choose **Configuration** > **Gateway**. The **Gateway** page appears.

4.2.1 Basic Gateway Information Configuration



Device Info

Device Name：

Management Password：

SN：

MGMT IP：

CEP URL：

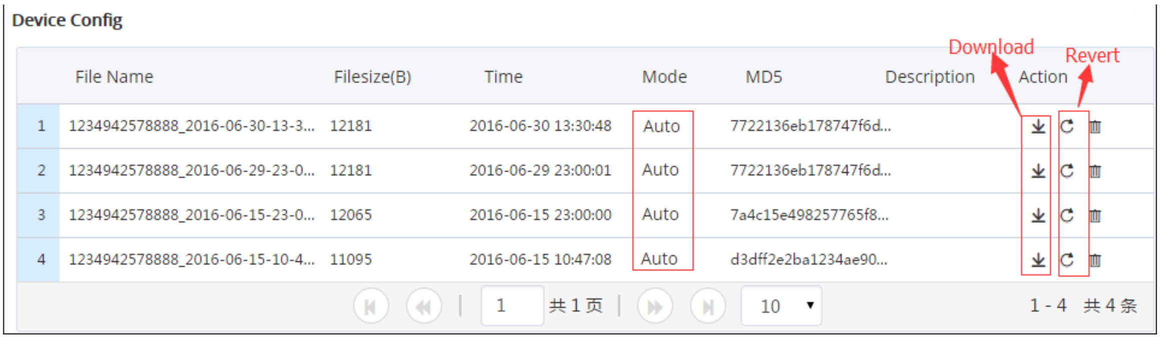
Software Version：

Save Cancel

Figure 4-13 Basic Information Configuration

As shown in Figure 4-13, the basic gateway information includes the device name and management password. The management password is the login password of the gateway.

4.2.2 Automatic Backup



Device Config

	File Name	Filesize(B)	Time	Mode	MD5	Description	Action
1	1234942578888_2016-06-30-13-3...	12181	2016-06-30 13:30:48	Auto	7722136eb178747f6d...		⤓ ↻ 🗑
2	1234942578888_2016-06-29-23-0...	12181	2016-06-29 23:00:01	Auto	7722136eb178747f6d...		⤓ ↻ 🗑
3	1234942578888_2016-06-15-23-0...	12065	2016-06-15 23:00:00	Auto	7a4c15e498257765f8...		⤓ ↻ 🗑
4	1234942578888_2016-06-15-10-4...	11095	2016-06-15 10:47:08	Auto	d3dff2e2ba1234ae90...		⤓ ↻ 🗑

Figure 4-14 Backup List Configuration

The MACC periodically (once in a day) obtains and saves the gateway configuration status. As shown in Figure 4-14, the backup files are recorded in a list (backup files in **Auto** mode are saved automatically). A device can save 30 backup files at most (including manually and automatically backed up files), and the earliest backup file will be deleted when the backup file number exceeds 30.

4.2.3 Manual Configuration

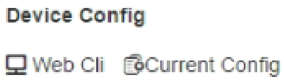
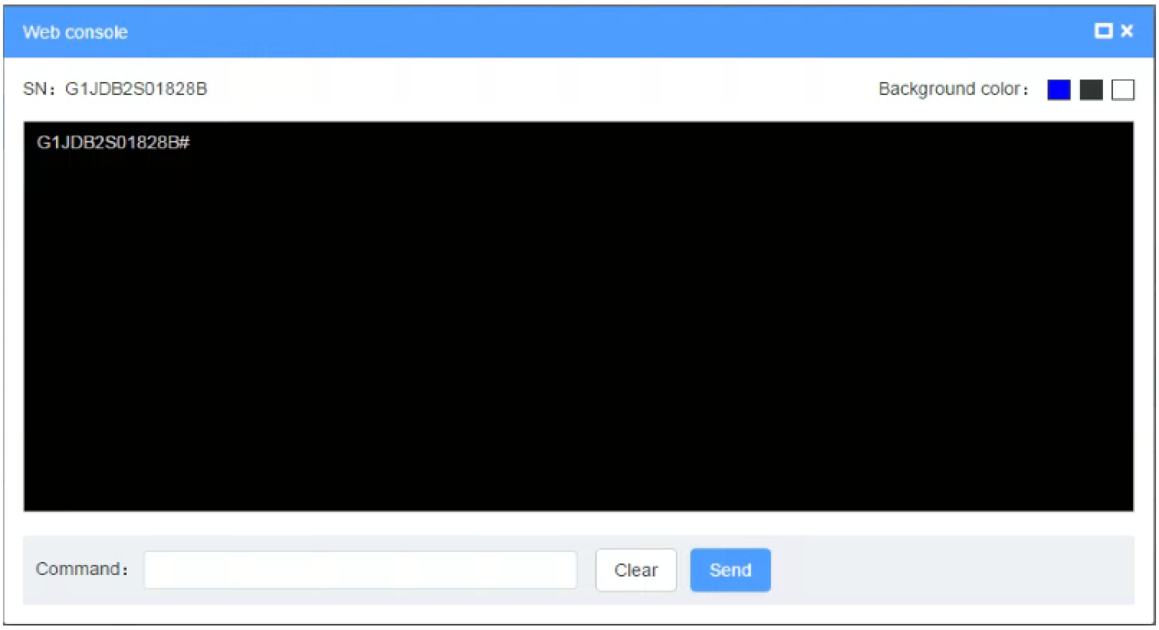


Figure 4-15 Device Configuration

The gateway interface further provides the **Web Cli** and **Current Config** functions.

Click **Web Cli** to enter the **Web console** interface, as shown in figure 4-16; the MACC can immediately push some commands to the gateway to implement the configuration.



SN：G1JDB2S01828B

```
G1JDB2S01828B#
```

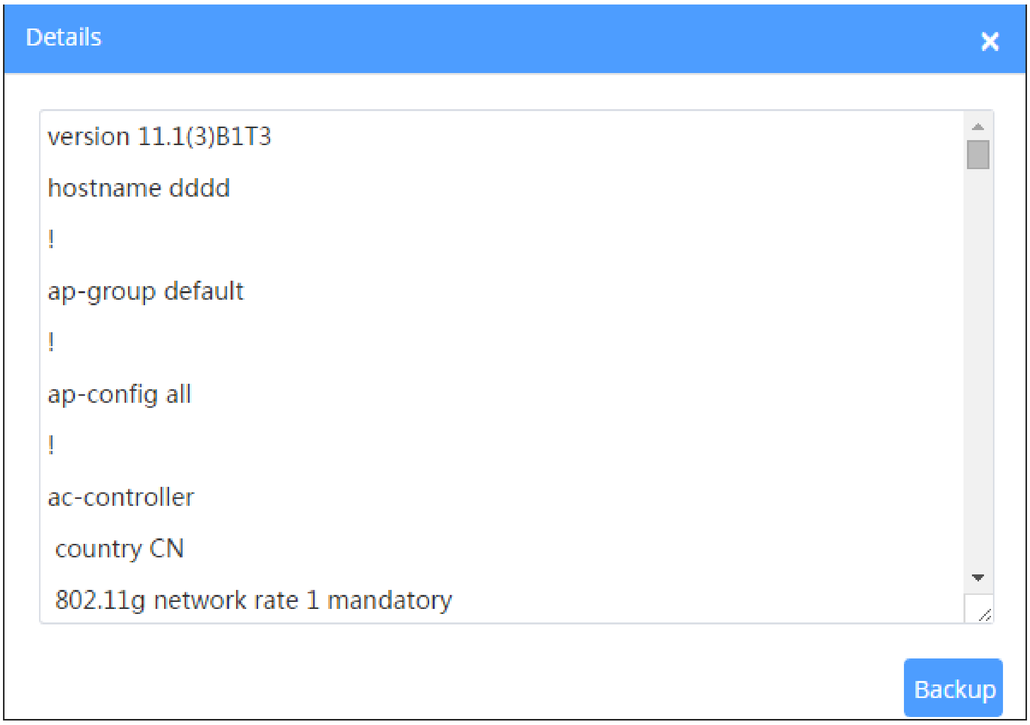
Figure 4-16 Web Console Interface

4.2.4 Checking and Manually Backing Up Configurations

1. Click **Current Config** to open the **Details** page, as shown in figure 4-17, and check the current configuration status.

2. Click **Backup** in the lower right corner to backup configurations.

A new backup record with the **Manual** mode will be generated in the backup list shown in the following figure.



```
version 11.1(3)B1T3
hostname dddd
!
ap-group default
!
ap-config all
!
ac-controller
 country CN
 802.11g network rate 1 mandatory
```

Figure 4-17 Current Gateway Configuration Details

4.2.5 Downloading Configurations

Click **Download** on the right of the backup list to download the corresponding files locally.

4.2.6 Reverting Configurations

Click **Revert** on the right of the backup list to push corresponding configurations to the gateway and revert the configurations. The gateway restarts after the configurations are reverted.

5 Monitoring

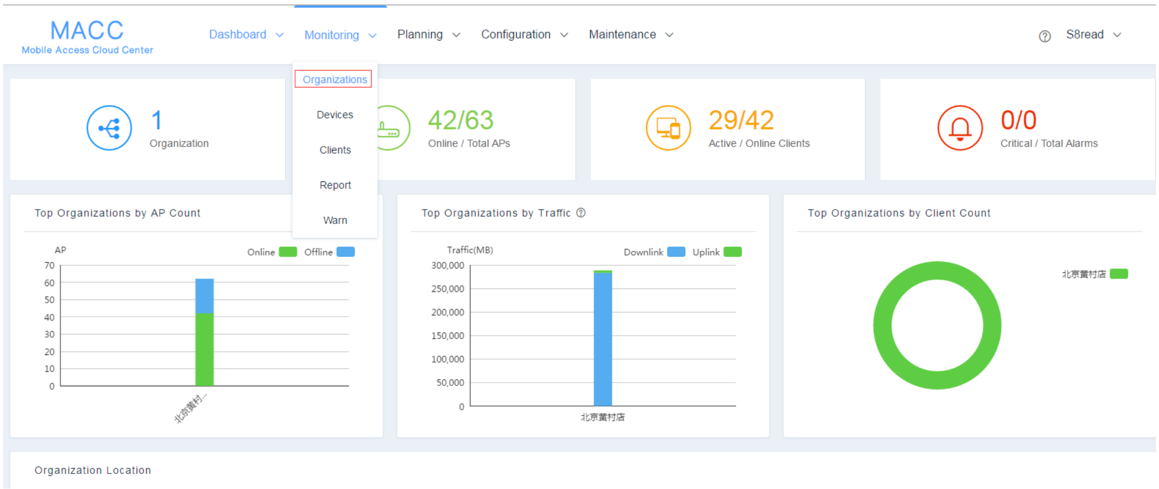
The MACC enables you to monitor the following items:

- Organizations
- APs
- Clients
- SIM cards (for vehicle-mounted APs only)

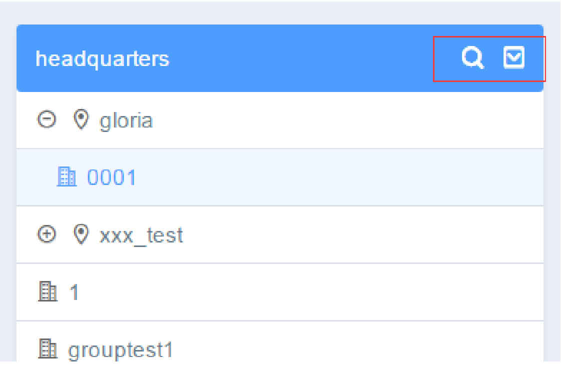
5.1 Organizations

The **Organizations** page displays the statistics information of network statuses of each organization, including:

- Overview
- Client statistics
- AP network status
- Gateway monitoring information



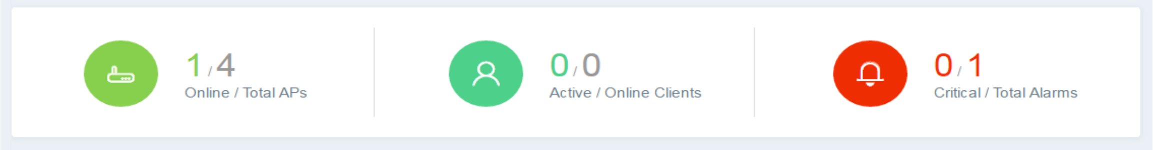
Choose **Monitoring** > **Organizations** to open the **Organizations** page, and select an organization on the left to check the monitoring information.



The organization selection area on the left supports the functions of searching and expanding all organizations.

5.1.1 Overview

Click **Overview** to open the **Overview** page. This page displays the numbers of APs, clients, and alarms.



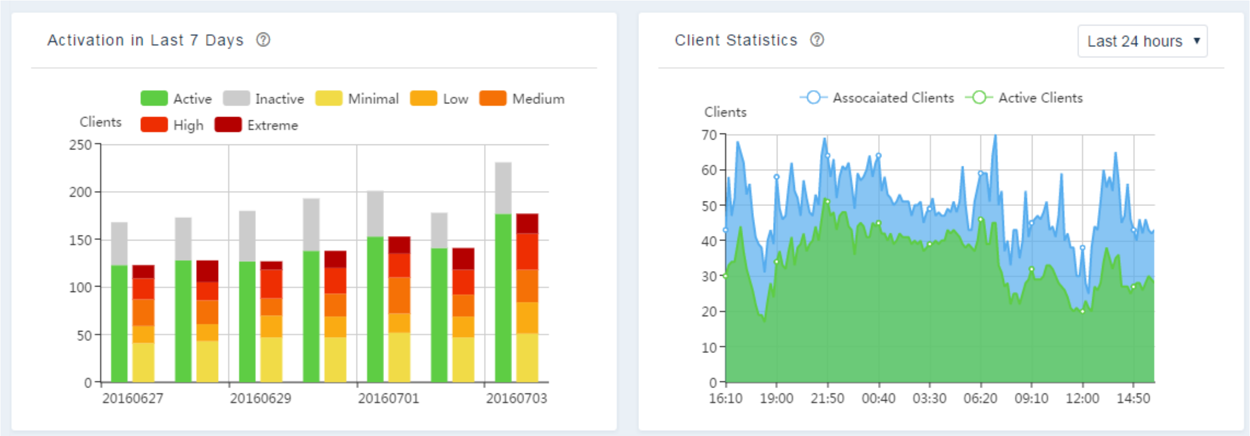
1 / 4 Online / Total APs

0 / 0 Active / Online Clients

0 / 1 Critical / Total Alarms

- The figure above displays the numbers of online APs and total APs, the numbers of active clients and online clients, and the quantities of critical alarms and total alarms.

An active client refers a client with the total traffic over 100 KB when it goes online.



- The left figure above displays a bar chart of activation in last 7 days. The client activation is classified into different levels according to the go-online duration and traffic as follows:

Extreme: 8 h/d * accumulated traffic 10 MB/2

High: 4 h/d * accumulated traffic 5 MB/3

Medium: 2 h/d * accumulated traffic 2 MB/4

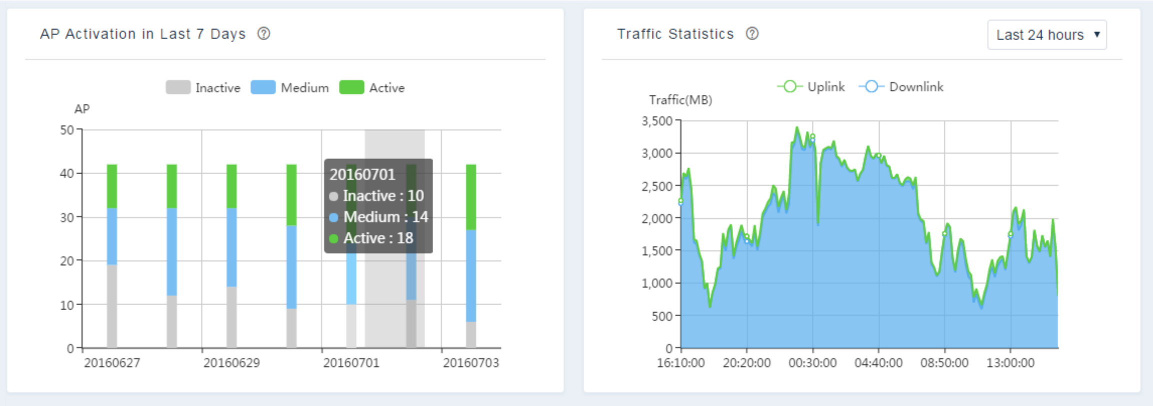
Low: 1 h/d * accumulated traffic 500 kb/5

Minimum: any duration * traffic > 100 kb/6

Inactive: traffic < 100 kb

Move the cursor to the bar chart to display detailed values.

- The right figure above displays a graph of clients. You can choose to display the client statistics in the last 24 hours or the last 7 days using the drop-down list in the upper right corner. The graph displays statistics about associated clients and active clients.



- The left figure above displays the AP activation in the last 7 days. The AP activation is graded according to the number of accumulated clients on a single AP in one day as follows:

Inactive: client count < 5

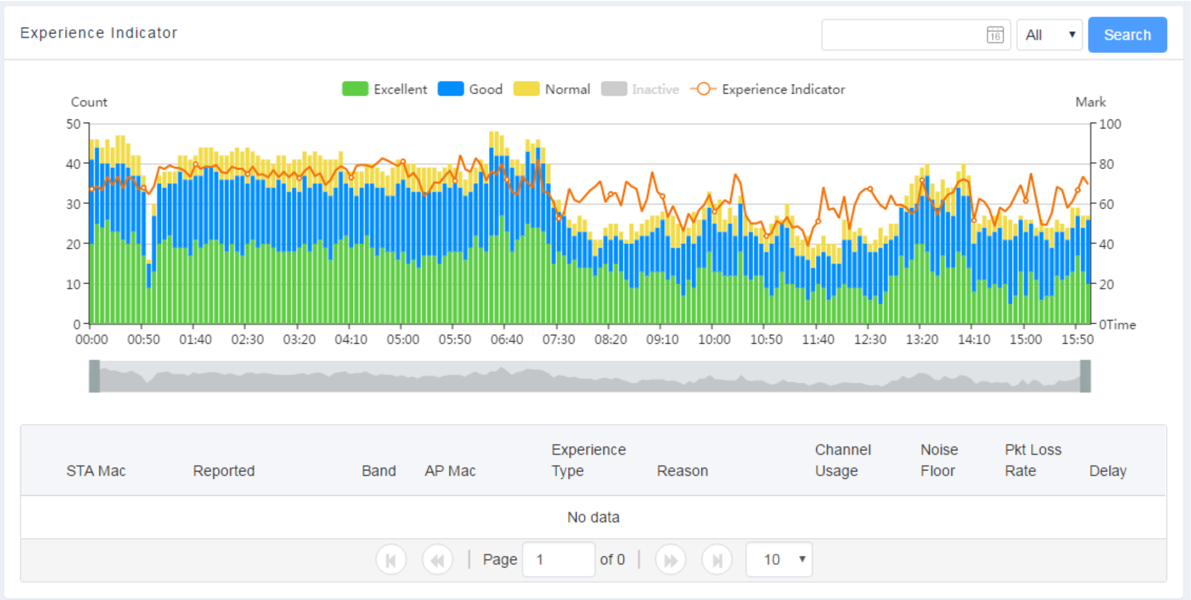
Medium: 5 ≤ client count < 10

Active: client count ≥ 10

- The right figure above displays statistics about total AP traffic. You can choose to display the client statistics in the last 24 hours or the last 7 days using the drop-down list in the upper right corner. The graph displays statistics about uplink traffic and downlink traffic.

5.1.2 Client Statistics

The client page displays the following information:

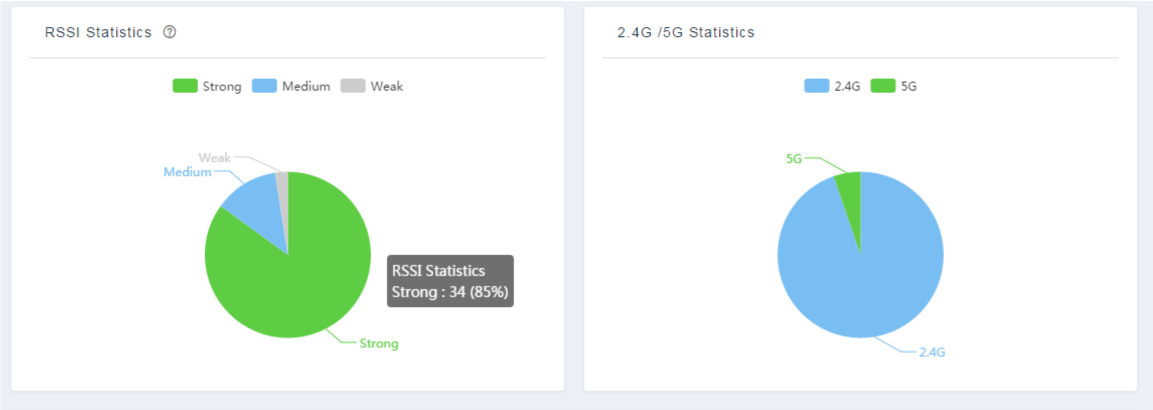


Experience Indicator

STA Mac	Reported	Band	AP Mac	Experience Type	Reason	Channel Usage	Noise Floor	Pkt Loss Rate	Delay
No data									

- Experience indicator bar graph
  - ➢ Displays the status of each client from 00:00:00 to 23:59:59 of past days, and from 00:00:00 to current local time of the current day.
  - ➢ Collects statistics every 5 minutes.
  - ➢ Displays the experience indicator of different dates by selecting time.
  - ➢ Supports selection between the 2.4 GHz and 5 GHz frequency bands.
- Client information

You can click the experience indicator bar graph to display the client information.



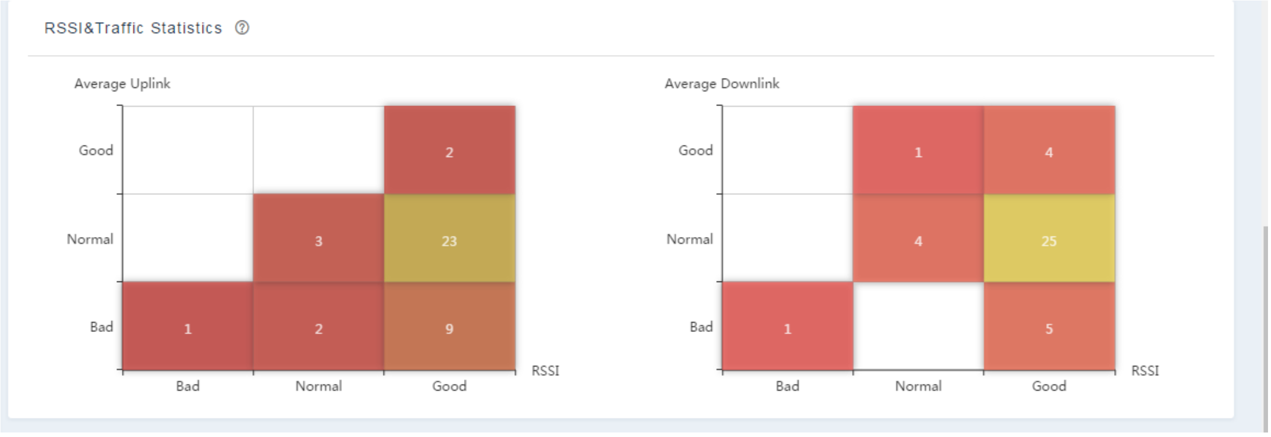
Signal strength distribution (left figure): The signal strength is defined as follow:

Weak: RSSI ≤ -80

Medium: -80 < RSSI ≤ -70.

Strong: RSSI > -70

- Client distribution at 2.4 GHz/5 GHz (right figure)



- Uplink and downlink rate distribution of online clients (figure above): An area in which a client is located is described according to signal strength and average uplink and downlink rates.

The signal strength and average uplink and downlink rates are defined as follows:

Signal strength:

Bad: RSSI ≤ -80

Normal: -80 < RSSI ≤ -70

Good: RSSI > -70

Average rate:

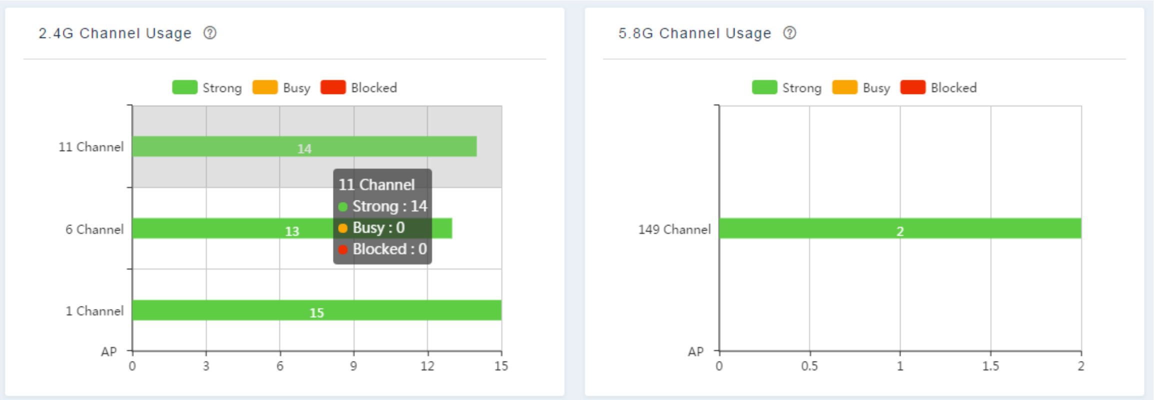
Bad: average rate ≤ 10 Mbps

Normal: 10 Mbps < average rate ≤ 80 Mbps.

Good: average rate > 80 Mbps

5.1.3 AP Statistics

The AP page displays the following information:

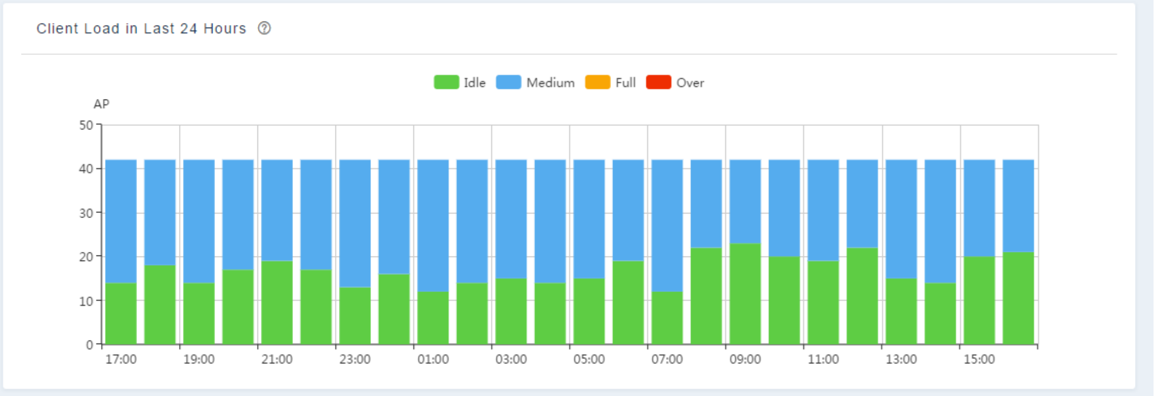


- Current 2.4G/5.8G channel usage (figure above): The channel usage is graded as follows:

Strong: 0% to 59%.

Busy: 60% to 79%

Blocked: 80% to 100%



Client load of APs in the last 24 hours (figure above): APs are graded according to load as follows:

Idle: client count = 0

Medium: 1 ≤ client count ≤ 20

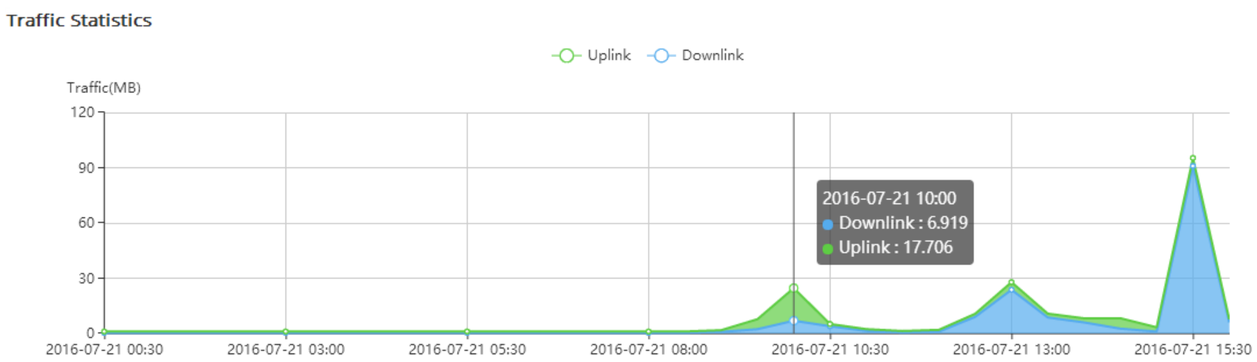
Full: 21 ≤ client count ≤ 32

Over: client count ≥ 33

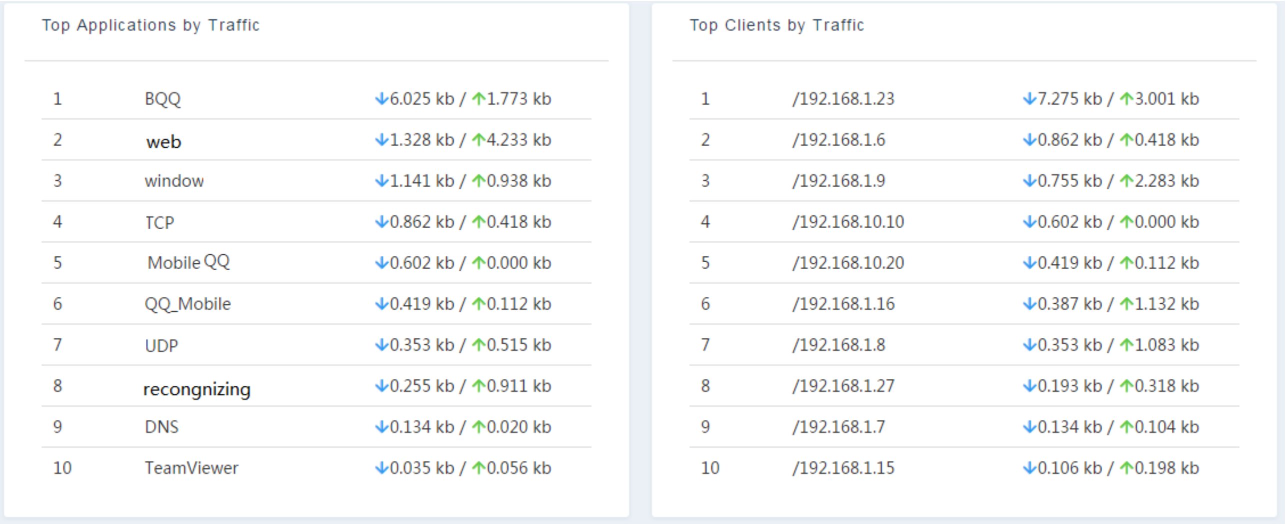
5.1.4 Gateway Monitoring Information

The gateway monitoring page displays the following information:

- Gateway traffic graph: Displays the gateway traffic statistics on the current day.



- Top 10 applications by traffic and top 10 clients by traffic



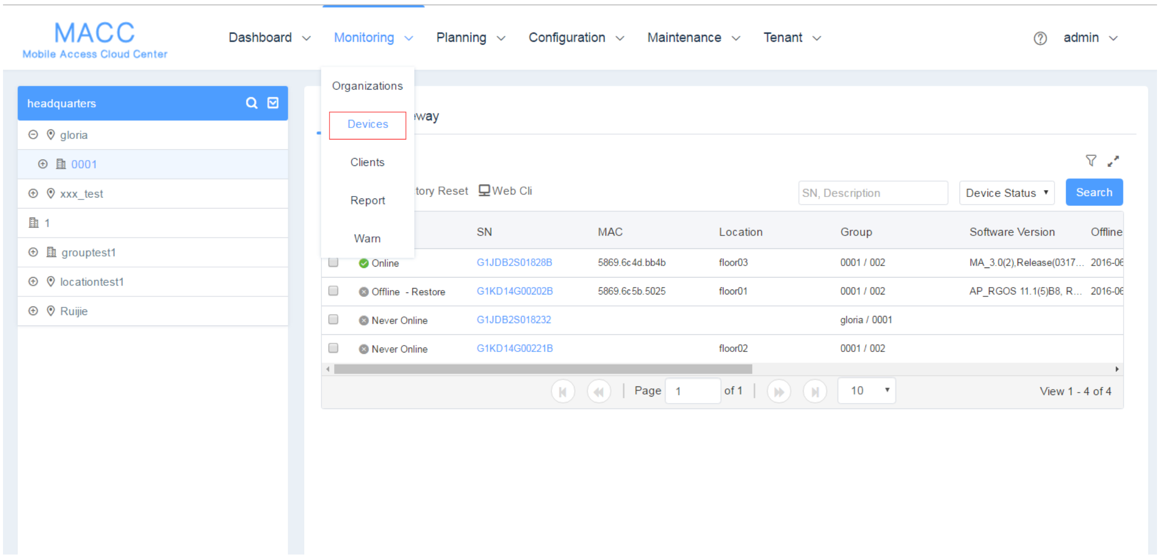
Top Applications by Traffic

1	BQQ	↓6.025 kb / ↑1.773 kb
2	web	↓1.328 kb / ↑4.233 kb
3	window	↓1.141 kb / ↑0.938 kb
4	TCP	↓0.862 kb / ↑0.418 kb
5	Mobile QQ	↓0.602 kb / ↑0.000 kb
6	QQ_Mobile	↓0.419 kb / ↑0.112 kb
7	UDP	↓0.353 kb / ↑0.515 kb
8	recongnizing	↓0.255 kb / ↑0.911 kb
9	DNS	↓0.134 kb / ↑0.020 kb
10	TeamViewer	↓0.035 kb / ↑0.056 kb

Top Clients by Traffic

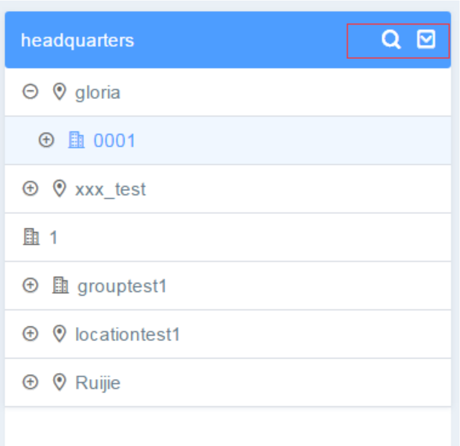
1	/192.168.1.23	↓7.275 kb / ↑3.001 kb
2	/192.168.1.6	↓0.862 kb / ↑0.418 kb
3	/192.168.1.9	↓0.755 kb / ↑2.283 kb
4	/192.168.10.10	↓0.602 kb / ↑0.000 kb
5	/192.168.10.20	↓0.419 kb / ↑0.112 kb
6	/192.168.1.16	↓0.387 kb / ↑1.132 kb
7	/192.168.1.8	↓0.353 kb / ↑1.083 kb
8	/192.168.1.27	↓0.193 kb / ↑0.318 kb
9	/192.168.1.7	↓0.134 kb / ↑0.104 kb
10	/192.168.1.15	↓0.106 kb / ↑0.198 kb

5.2 Devices



		SN	MAC	Location	Group	Software Version	Offline
□	Online	G1JDB2S01828B	5869.6c4d.bb4b	floor03	0001 / 002	MA_3.0(2),Release(0317...	2016-06
□	Offline - Restore	G1KD14G00202B	5869.6c5b.5025	floor01	0001 / 002	AP_RGOS 11.1(5)B8, R...	2016-06
□	Never Online	G1JDB2S018232			gloria / 0001		
□	Never Online	G1KD14G00221B		floor02	0001 / 002		

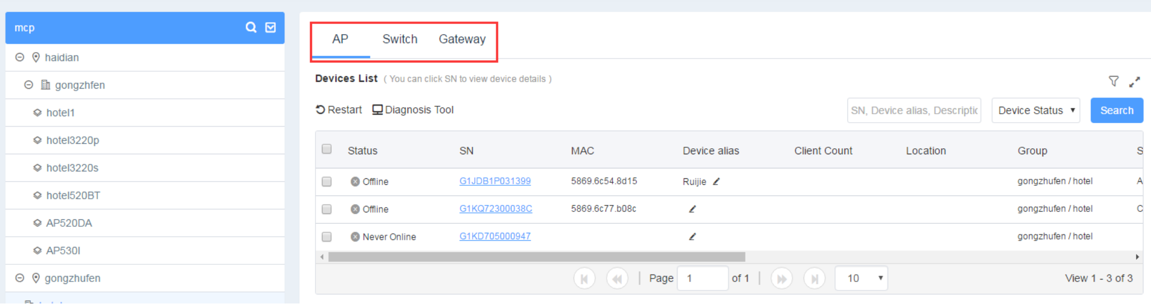
Choose **Monitoring** > **Devices** to display the **Devices** page, and select a group on the left to filter devices.



The group selection area on the left supports functions of searching and expanding all groups.

5.2.1 Devices List

The devices list includes the AP list, switch and the gateway list. Click **AP** , **Switch** or **Gateway** to display the corresponding devices list.



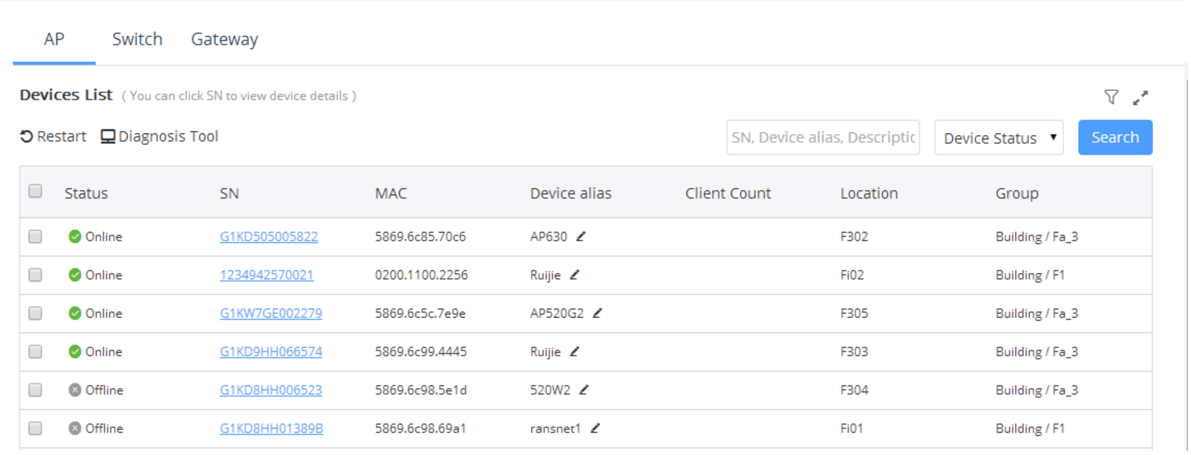
Devices List (You can click SN to view device details)

☐	Status	SN	MAC	Device alias	Client Count	Location	Group	S
☐	Offline	G1JDB1P031399	5869.6c54.8d15	Ruijie			gongzhufen / hotel	A
☐	Offline	G1KQ72300038C	5869.6c77.b08c				gongzhufen / hotel	C
☐	Never Online	G1KD705000947					gongzhufen / hotel	

Page 1 of 1 10 View 1 - 3 of 3

The AP devices describes basic device information, including the online/offline status, serial number, MAC address, location, group, software version, offline time, device model, management IP address, egress IP address, configuration status, and description.

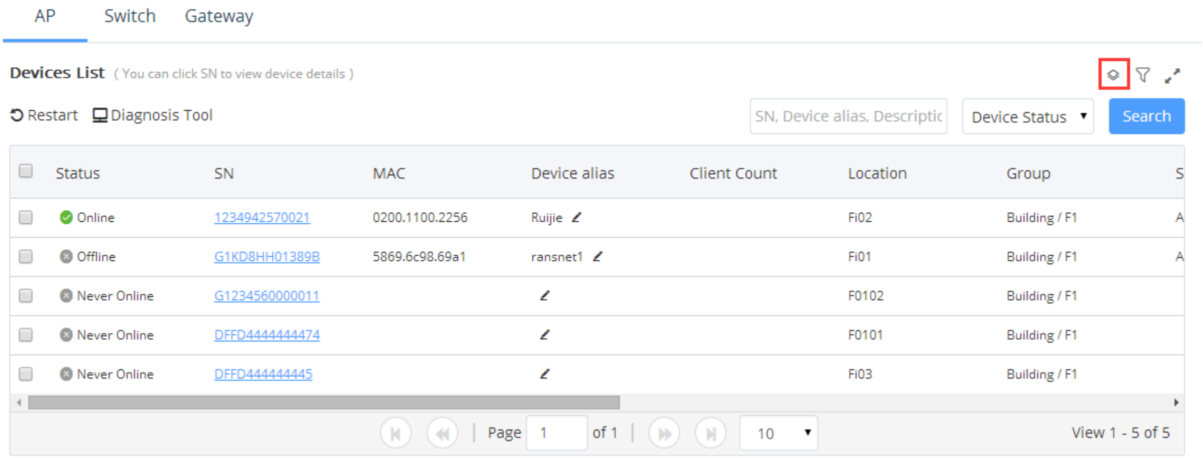
The **Search** function supports fuzzy queries based on the serial number and description, and also supports queries based on device status.



Devices List (You can click SN to view device details)

☐	Status	SN	MAC	Device alias	Client Count	Location	Group
☐	Online	G1KD505005822	5869.6c85.70c6	AP630		F302	Building / Fa_3
☐	Online	1234942570021	0200.1100.2256	Ruijie		Fi02	Building / F1
☐	Online	G1KW7GE002279	5869.6c5c.7e9e	AP520G2		F305	Building / Fa_3
☐	Online	G1KD9HH066574	5869.6c99.4445	Ruijie		F303	Building / Fa_3
☐	Offline	G1KD8HH006523	5869.6c98.5e1d	520W2		F304	Building / Fa_3
☐	Offline	G1KD8HH01389B	5869.6c98.69a1	ransnet1		Fi01	Building / F1

In a floor group, click ◈ to enter the map mode and check the device location.



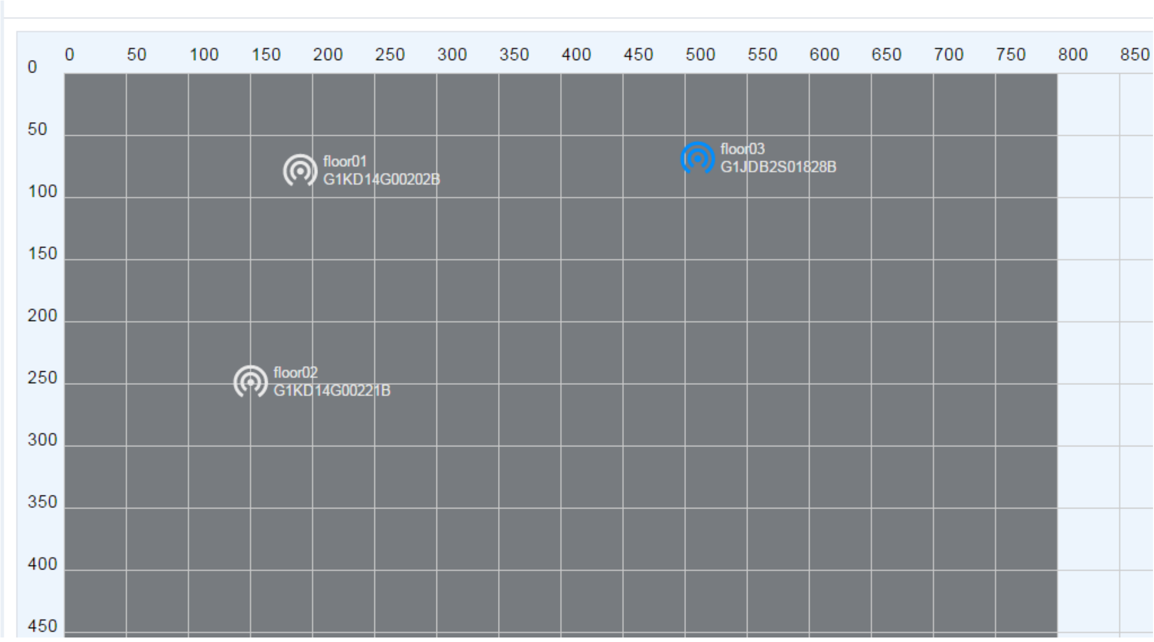
Devices List (You can click SN to view device details)

Restart Diagnosis Tool

SN, Device alias, Descriptic | Device Status ▾ | Search

□	Status	SN	MAC	Device alias	Client Count	Location	Group	S
□	Online	1234942570021	0200.1100.2256	Ruijie		Fi02	Building / F1	A
□	Offline	G1KD8HH01389B	5869.6c98.69a1	ransnet1		Fi01	Building / F1	A
□	Never Online	G1234560000011				F0102	Building / F1	
□	Never Online	DFFD4444444474				F0101	Building / F1	
□	Never Online	DFFD444444445				Fi03	Building / F1	

Page 1 of 1 | 10 ▾ | View 1 - 5 of 5

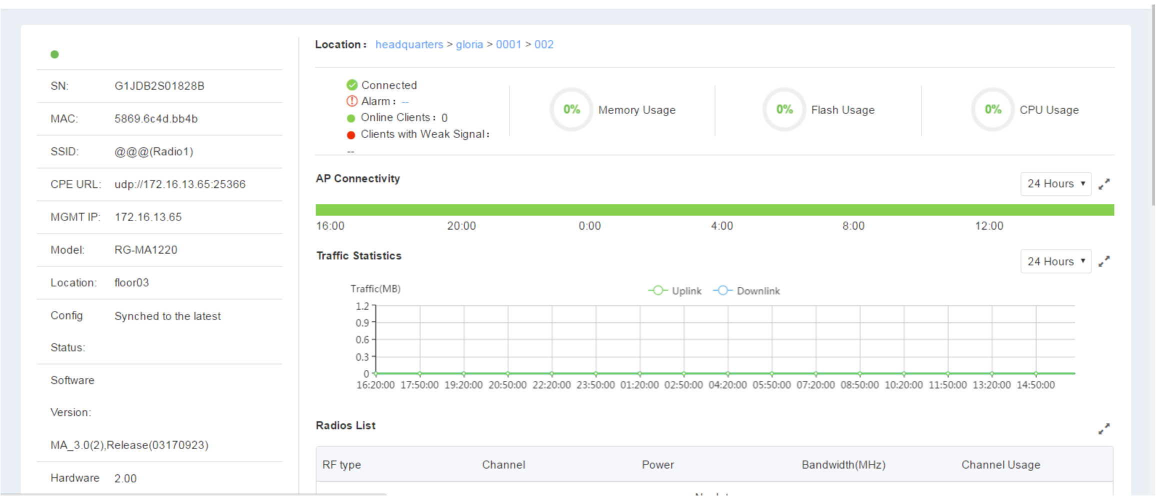


Above the list are the **Restart**, **Factory Reset**, and **Web Cli** functions. For use details, see 5.2.3 Basic AP Operations.

Click the device serial number in the devices list for details of a single device. For use details, see 5.2.2 Device Details.

5.2.2 Device Details

Click the serial number in the devices list to jump to the details page of a single device. The page displays detailed device information, including basic information, performance data, traffic data, client data, online/offline status, RF information, and device logs.



●

SN:	G1JDB2S01828B
MAC:	5869.6c4d.bb4b
SSID:	@@@(Radio1)
CPE URL:	udp://172.16.13.65:25366
MGMT IP:	172.16.13.65
Model:	RG-MA1220
Location:	floor03
Config Status:	Synched to the latest
Software Version:	MA_3.0(2),Release(03170923)
Hardware	2.00

Location： headquarters > gloria > 0001 > 002

Connected
Alarm： --
Online Clients： 0
Clients with Weak Signal：
--

0% Memory Usage
0% Flash Usage
0% CPU Usage

AP Connectivity 24 Hours

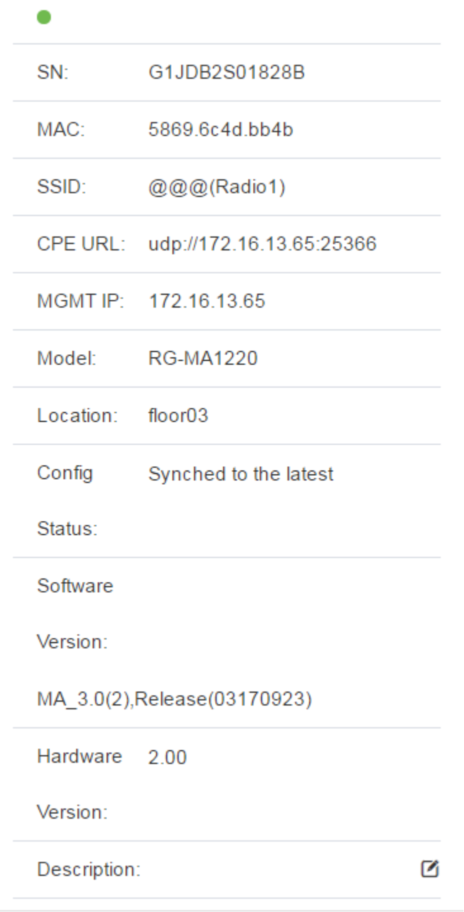
Traffic Statistics 24 Hours

Radios List

RF type	Channel	Power	Bandwidth(MHz)	Channel Usage

The AP information is described as follows:

- Basic information



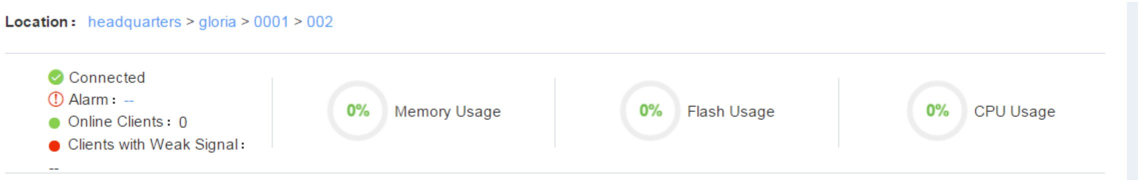
●

SN:	G1JDB2S01828B
MAC:	5869.6c4d.bb4b
SSID:	@@@(Radio1)
CPE URL:	udp://172.16.13.65:25366
MGMT IP:	172.16.13.65
Model:	RG-MA1220
Location:	floor03
Config Status:	Synched to the latest
Software Version: MA_3.0(2),Release(03170923)	
Hardware Version:	2.00
Description:	

The basic information includes the online/offline status, serial number, MAC address, SSID, CPE URL, management IP address, device model, location, configuration status, software version, hardware version, and description.

A red spot indicates the offline status, and a green spot indicates the online status. The configuration status indicates whether the corresponding configuration items have been synchronized to devices.

- Performance data

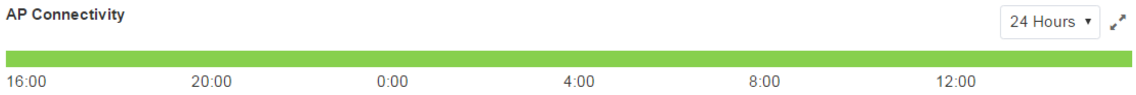


Location： headquarters > gloria > 0001 > 002

✓ Connected
ⓘ Alarm： --
● Online Clients： 0
● Clients with Weak Signal： --

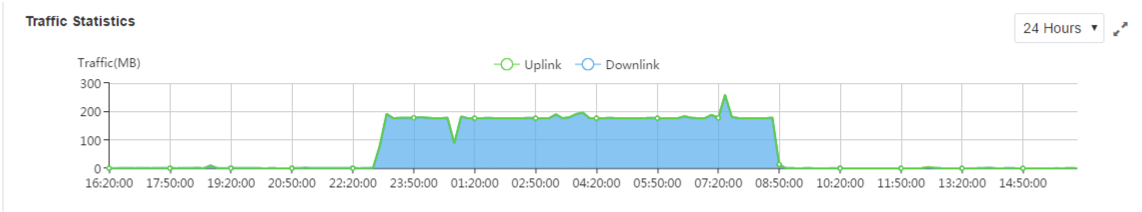
The performance data includes the AP connection status, online client count, CPU usage, memory usage, and flash usage.

- AP connectivity



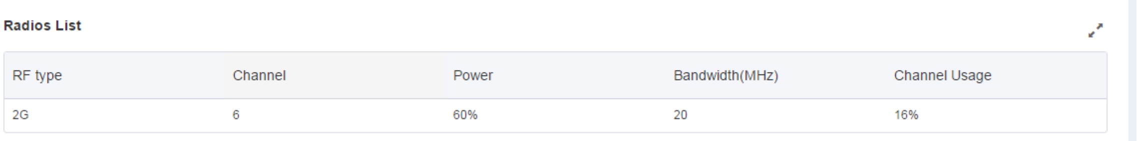
The AP connectivity refers to the connectivity (online status) between AP and the MACC within a period (24 hours or 7 days).

- Traffic statistics



You can choose to view the AP traffic statistics in the last 24 hours or the last 7 days.

- Radio list

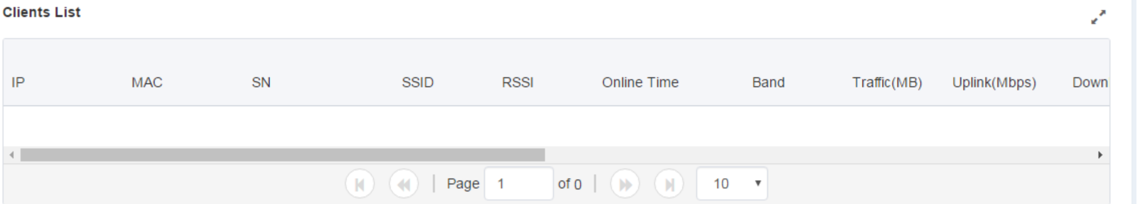


Radios List

RF type	Channel	Power	Bandwidth(MHz)	Channel Usage
2G	6	60%	20	16%

The **Radio List** page displays the RF information, including the RF type, current channel, power (percentage), frequency bandwidth, and channel usage.

- Clients list

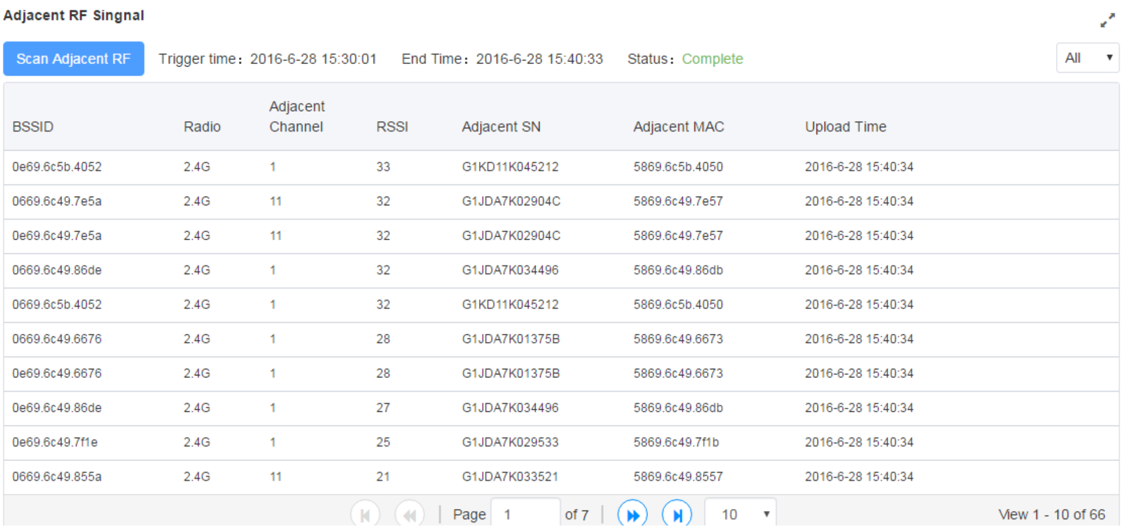


Clients List

IP	MAC	SN	SSID	RSSI	Online Time	Band	Traffic(MB)	Uplink(Mbps)	Down

The client list displays information about clients currently associated with the APs, including the AP IP address, MAC address, SSID, RSSI, traffic, online/offline status, and terminal type.

- Adjacent RF signal



Adjacent RF Singnal

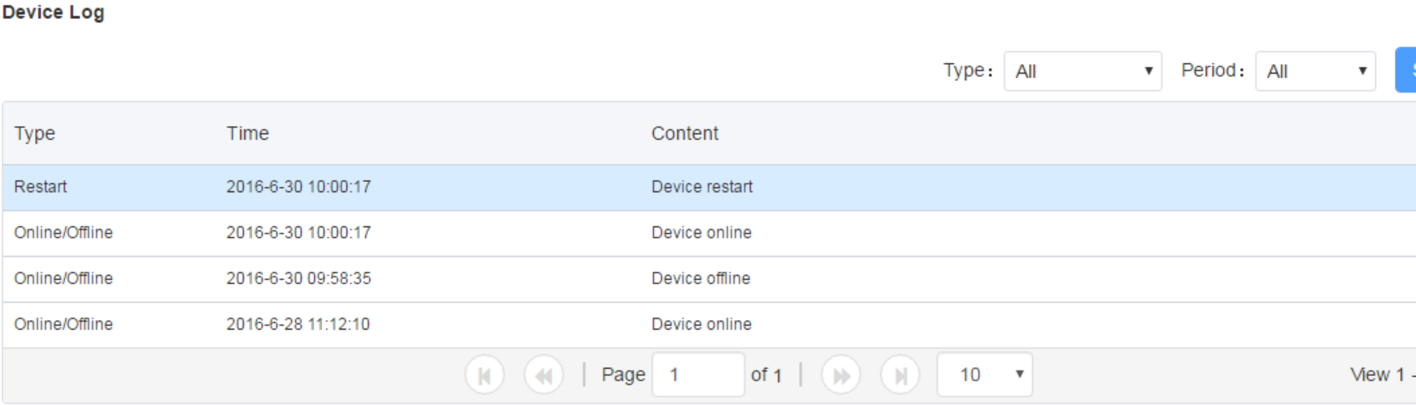
Trigger time：2016-6-28 15:30:01 End Time：2016-6-28 15:40:33 Status：Complete

BSSID	Radio	Adjacent Channel	RSSI	Adjacent SN	Adjacent MAC	Upload Time
0e69.6c5b.4052	2.4G	1	33	G1KD11K045212	5869.6c5b.4050	2016-6-28 15:40:34
0669.6c49.7e5a	2.4G	11	32	G1JDA7K02904C	5869.6c49.7e57	2016-6-28 15:40:34
0e69.6c49.7e5a	2.4G	11	32	G1JDA7K02904C	5869.6c49.7e57	2016-6-28 15:40:34
0669.6c49.86de	2.4G	1	32	G1JDA7K034496	5869.6c49.86db	2016-6-28 15:40:34
0669.6c5b.4052	2.4G	1	32	G1KD11K045212	5869.6c5b.4050	2016-6-28 15:40:34
0669.6c49.6676	2.4G	1	28	G1JDA7K01375B	5869.6c49.6673	2016-6-28 15:40:34
0e69.6c49.6676	2.4G	1	28	G1JDA7K01375B	5869.6c49.6673	2016-6-28 15:40:34
0e69.6c49.86de	2.4G	1	27	G1JDA7K034496	5869.6c49.86db	2016-6-28 15:40:34
0e69.6c49.7f1e	2.4G	1	25	G1JDA7K029533	5869.6c49.7f1b	2016-6-28 15:40:34
0669.6c49.855a	2.4G	11	21	G1JDA7K033521	5869.6c49.8557	2016-6-28 15:40:34

The **Adjacent RF Signal** page displays the RF signals (scanned BSSID) emitted by adjacent APs. The **Radio**, **Adjacent Channel**, and **RSSI** in the list are scanned information. If a signal comes from the AP managed by the cloud controller, the adjacent AP SN and adjacent MAC address will be identified and displayed; otherwise, these two items are in a unidentified state.

For more information about the functions and application scenarios of the adjacent RF signals scanning function, see 5.2.4 Adjacent RF Scanning.

- Device log



Device Log

Type： All Period： All

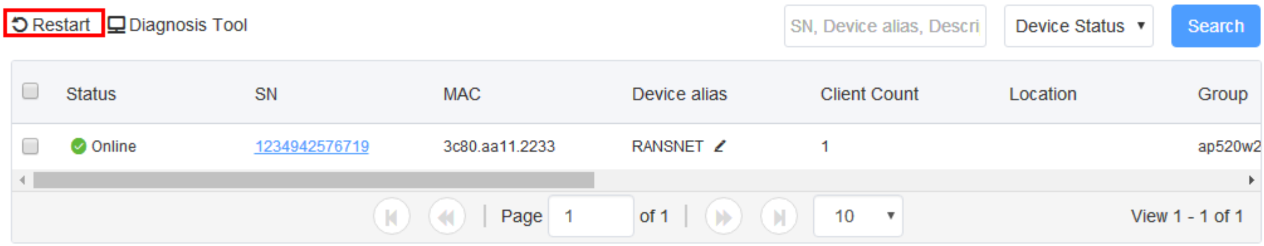
Type	Time	Content
Restart	2016-6-30 10:00:17	Device restart
Online/Offline	2016-6-30 10:00:17	Device online
Online/Offline	2016-6-30 09:58:35	Device offline
Online/Offline	2016-6-28 11:12:10	Device online

The device log records the historical operations, and currently supports the online/offline records, restart records, and upgrade records, and supports queries based on the log type and period.

5.2.3 Basic AP Operations

- **Restart**

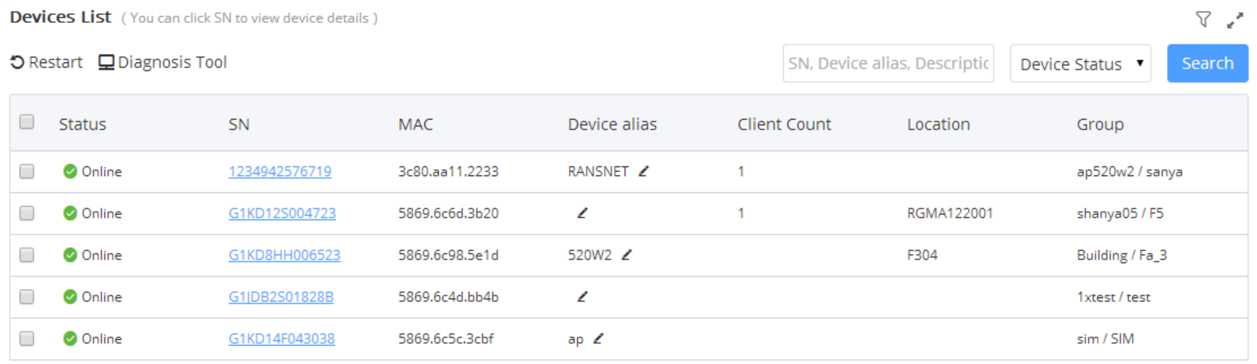
In the devices list, select the target AP (one or multiple), and click **Restart**.



□	Status	SN	MAC	Device alias	Client Count	Location	Group
□	Online	1234942576719	3c80.aa11.2233	RANSNET	1		ap520w2

- **Diagnosis Tool**

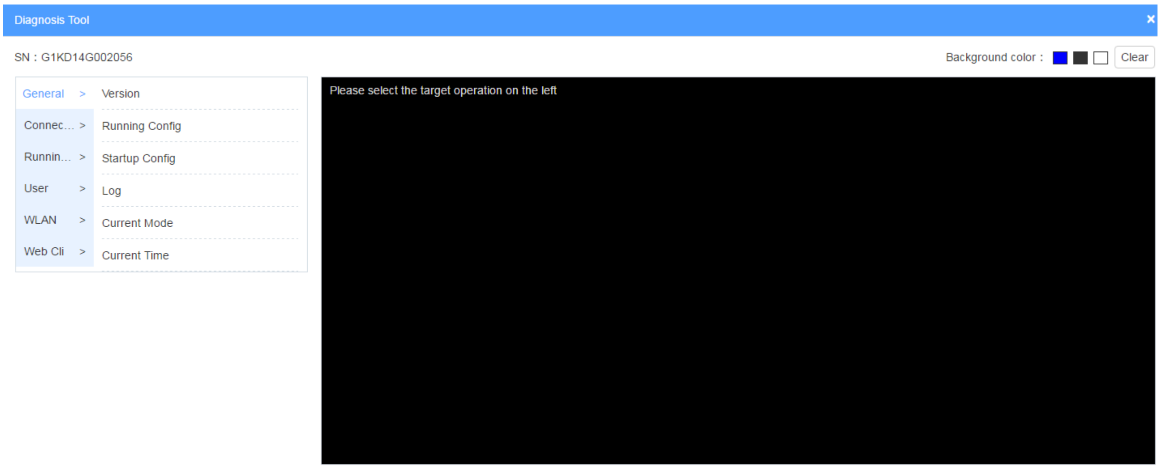
In the device list, select one required AP, and click **Diagnosis Tool**. The **Diagnosis Tool** dialog box is displayed, and you can query device information via the menus in this dialog box.



Devices List (You can click SN to view device details)

□	Status	SN	MAC	Device alias	Client Count	Location	Group
□	Online	1234942576719	3c80.aa11.2233	RANSNET	1		ap520w2 / sanya
□	Online	G1KD12S004723	5869.6c6d.3b20		1	RGMA122001	shanya05 / F5
□	Online	G1KD8HH006523	5869.6c98.5e1d	520W2		F304	Building / Fa_3
□	Online	G1JDB2S01828B	5869.6c4d.bb4b				1xtest / test
□	Online	G1KD14F043038	5869.6c5c.3cbf	ap			sim / SIM

The menus displayed vary with the product.



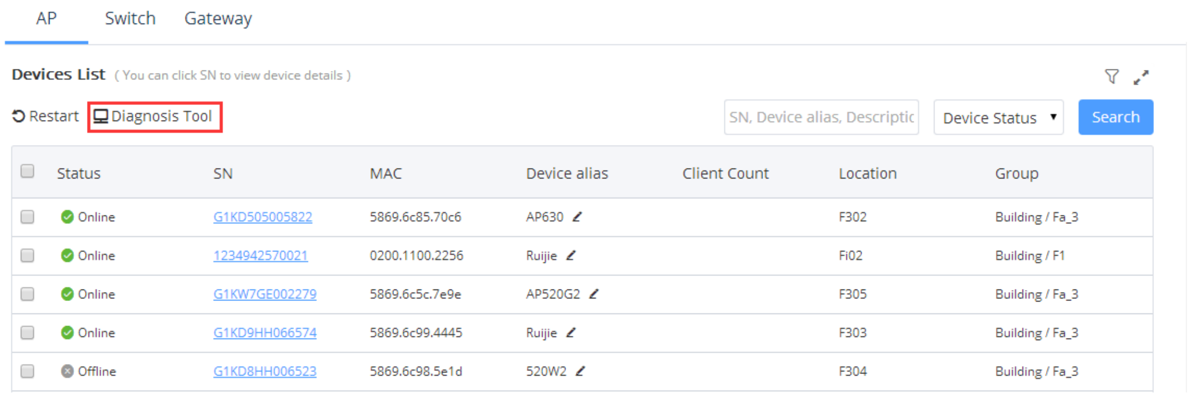
Diagnosis Tool

SN : G1KD14G002056

Please select the target operation on the left

- **Diagnosis Tool**

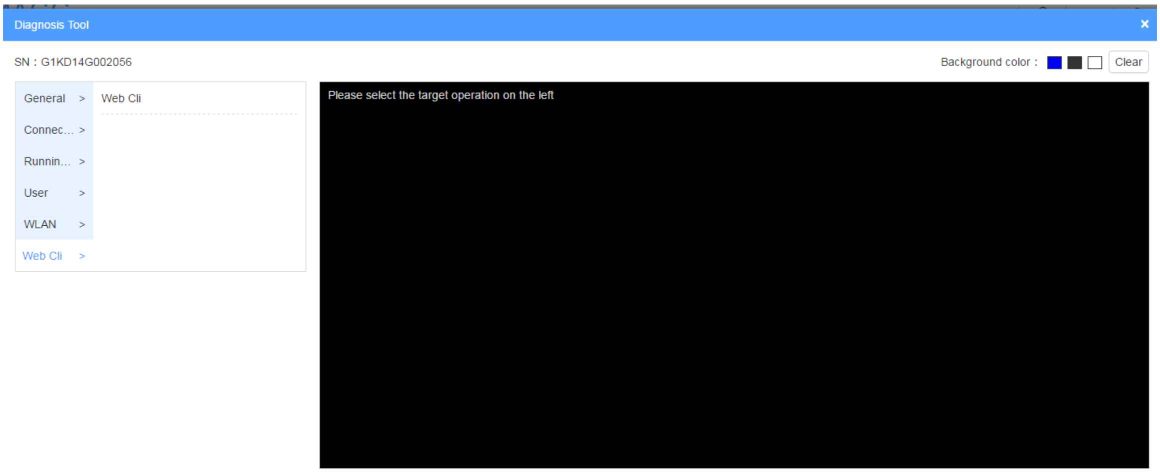
In the devices list, select the target device, click **Diagnosis Tool** to open the CLI entry box and enter commands.



Devices List (You can click SN to view device details)

□	Status	SN	MAC	Device alias	Client Count	Location	Group
□	Online	G1KD505005822	5869.6c85.70c6	AP630		F302	Building / Fa_3
□	Online	1234942570021	0200.1100.2256	Ruijie		Fi02	Building / F1
□	Online	G1KW7GE002279	5869.6c5c.7e9e	AP520G2		F305	Building / Fa_3
□	Online	G1KD9HH066574	5869.6c99.4445	Ruijie		F303	Building / Fa_3
□	Offline	G1KD8HH006523	5869.6c98.5e1d	520W2		F304	Building / Fa_3

In addition, in the command entry box, the **TAB** key and **?** both can complete a command.



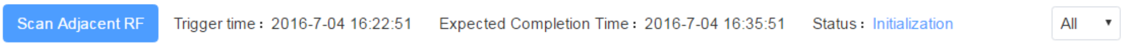
5.2.4 Adjacent RF Scanning

The MACC provides the function of triggering APs to scan adjacent RF signals. With this function, identified and unidentified RF signals can be observed. There are two known scenarios:

- Testing the number and strength of RF signals emitted by neighboring APs that are not managed by the MACC, so as to predict a degree of RF interference.
- Identifying RF signals emitted by neighboring APs managed by the MACC, so as to diagnose the RF functions and powered-on status of the neighboring APs.

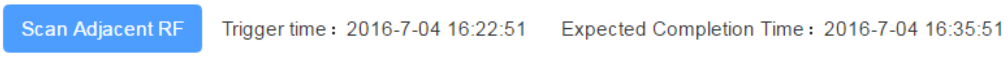
On the device details page, an AP may be triggered to perform scanning and display the scanning result. The following steps describe the method for scanning the adjacent RF signals:

- Click **Scan Adjacent RF** to trigger an AP to scan adjacent RF signals.



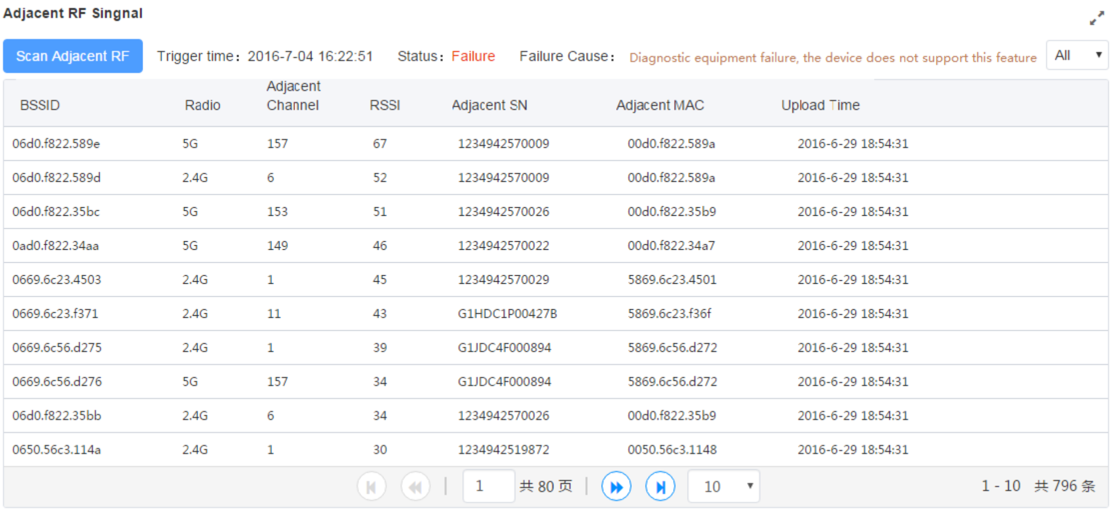
Trigger time：2016-7-04 16:22:51 Expected Completion Time：2016-7-04 16:35:51 Status：Initialization

After the AP is triggered, the trigger time, expected completion time, and status are displayed in the status bar. Then wait for the AP to finish scanning and send the results to the cloud controller.



Trigger time：2016-7-04 16:22:51 Expected Completion Time：2016-7-04 16:35:51

A list of RF signals scanned by the AP is displayed after the scanning. The list supports filtering function based on the RF type (2.4 GHz/5 GHz).



Adjacent RF Singnal

Scan Adjacent RF Trigger time：2016-7-04 16:22:51 Status：Failure Failure Cause：Diagnostic equipment failure, the device does not support this feature All

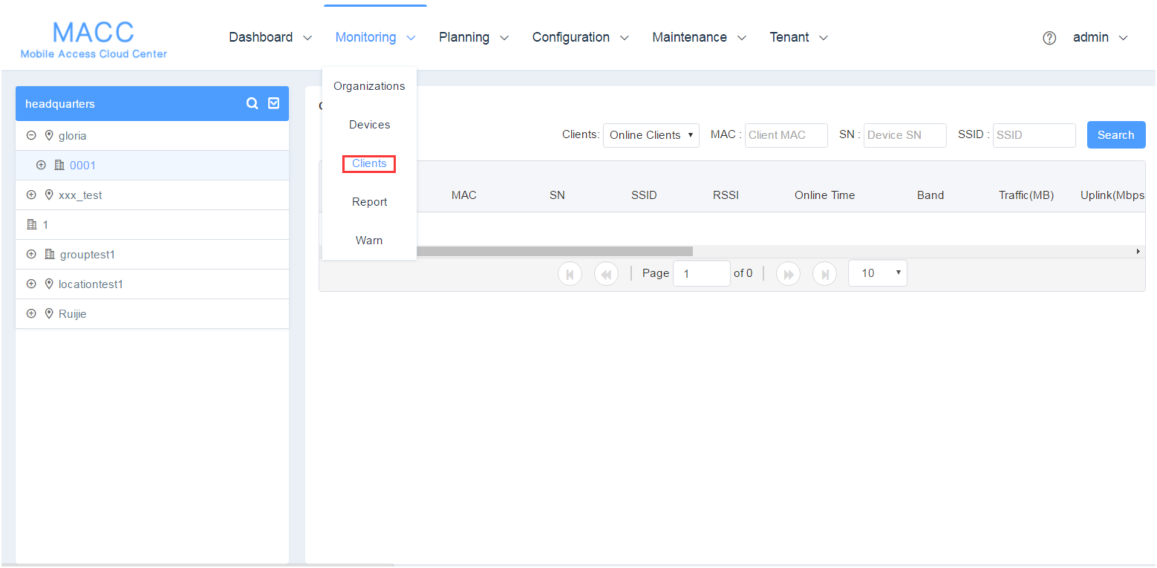
BSSID	Radio	Adjacent Channel	RSSI	Adjacent SN	Adjacent MAC	Upload Time
06d0.f822.589e	5G	157	67	1234942570009	00d0.f822.589a	2016-6-29 18:54:31
06d0.f822.589d	2.4G	6	52	1234942570009	00d0.f822.589a	2016-6-29 18:54:31
06d0.f822.35bc	5G	153	51	1234942570026	00d0.f822.35b9	2016-6-29 18:54:31
0ad0.f822.34aa	5G	149	46	1234942570022	00d0.f822.34a7	2016-6-29 18:54:31
0669.6c23.4503	2.4G	1	45	1234942570029	5869.6c23.4501	2016-6-29 18:54:31
0669.6c23.f371	2.4G	11	43	G1HDC1P00427B	5869.6c23.f36f	2016-6-29 18:54:31
0669.6c56.d275	2.4G	1	39	G1JDC4F000894	5869.6c56.d272	2016-6-29 18:54:31
0669.6c56.d276	5G	157	34	G1JDC4F000894	5869.6c56.d272	2016-6-29 18:54:31
06d0.f822.35bb	2.4G	6	34	1234942570026	00d0.f822.35b9	2016-6-29 18:54:31
0650.56c3.114a	2.4G	1	30	1234942519872	0050.56c3.1148	2016-6-29 18:54:31

1 共 80 页 10 1 - 10 共 796 条

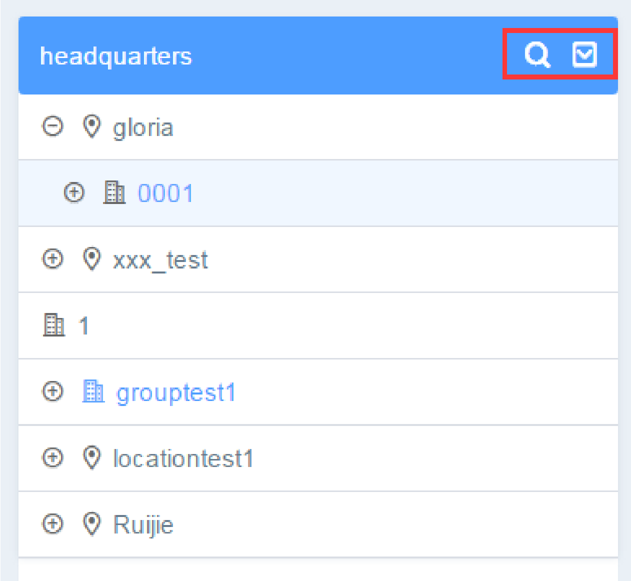
The MACC stores the latest scanning result, which overwrites earlier data.

If the adjacent AP SN and MAC address are unidentified, it indicates that the RF source is not managed by the MACC; otherwise, the RF signal is emitted by the AP managed by the MACC.

5.3 Clients



Choose **Monitoring** > **Clients** to open the **Clients List** page, and select a group on the left to filter clients.



headquarters

gloria

0001

xxx_test

1

grouptest1

locationtest1

Ruijie

The group selection area on the left supports functions of searching and expanding all groups.

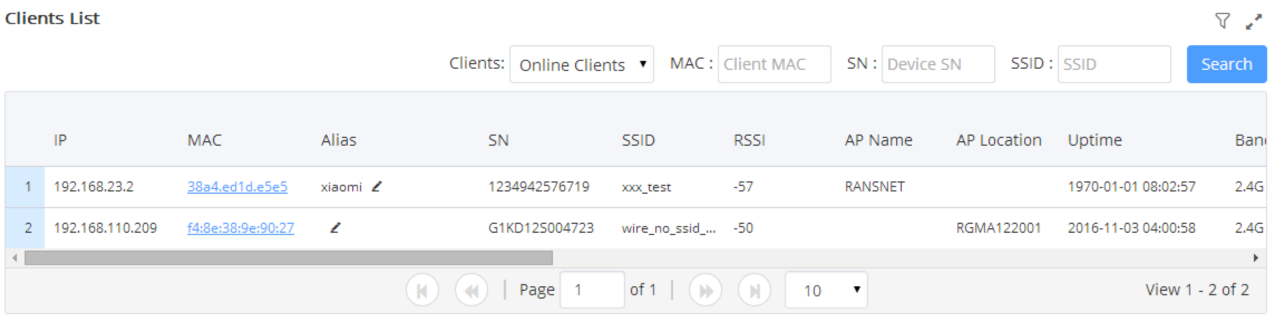
5.3.1 Clients List

1. Choose **Monitoring** > **Clients** to open the **Clients List** page. This page displays the information about online clients and historical clients of the current group.
2. Click the **Clients** drop-down list to switch between online clients and historical clients.

The client information includes the basic information, organization, band, and online time.

Select online clients in **Clients** to modify the clients' aliases.

Click the hyperlink in the **MAC** column. The **Clients Details** page will be displayed.



Clients List

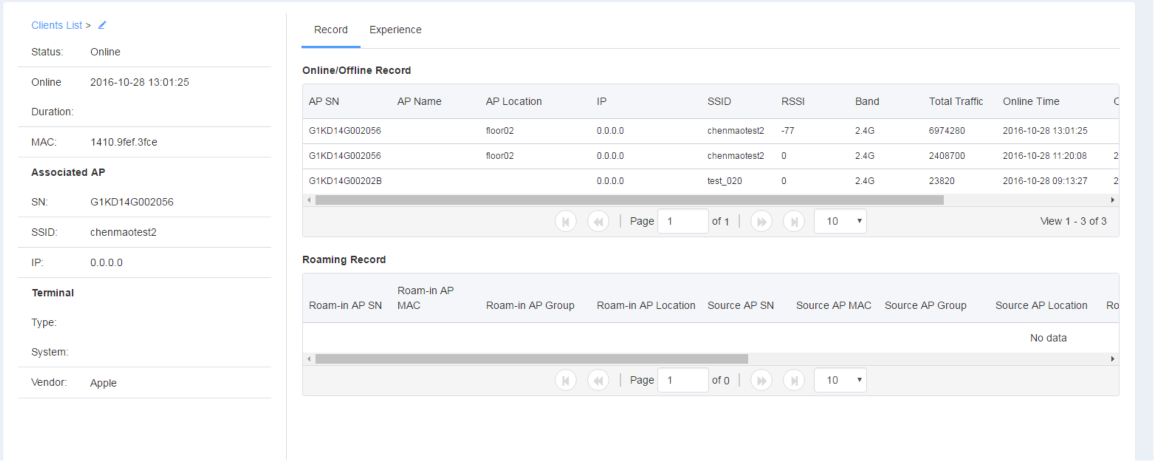
Clients: Online Clients MAC : Client MAC SN : Device SN SSID : SSID Search

	IP	MAC	Alias	SN	SSID	RSSI	AP Name	AP Location	Uptime	Ban
1	192.168.23.2	38a4.ed1d.e5e5	xiaomi	1234942576719	xxx_test	-57	RANSNET		1970-01-01 08:02:57	2.4G
2	192.168.110.209	f4:8e:38:9e:90:27		G1KD12S004723	wire_no_ssid_...	-50		RGMA122001	2016-11-03 04:00:58	2.4G

Page 1 of 1 10 View 1 - 2 of 2

5.3.2 Clients Details

On the **Clients Details** page, basic client information is displayed on the left area, including the status, offline time, associated AP, and vendor; and two labels are displayed on the right area: **Record** and **Experience**.



Clients List >

Status: Online

Online Duration: 2016-10-28 13:01:25

MAC: 1410.9fef.3fce

Associated AP

SN: G1KD14G002056

SSID: chenmaotest2

IP: 0.0.0.0

Terminal

Type:

System:

Vendor: Apple

Record Experience

Online/Offline Record

AP SN	AP Name	AP Location	IP	SSID	RSSI	Band	Total Traffic	Online Time	C
G1KD14G002056		floor02	0.0.0.0	chenmaotest2	-77	2.4G	6974280	2016-10-28 13:01:25	
G1KD14G002056		floor02	0.0.0.0	chenmaotest2	0	2.4G	2408700	2016-10-28 11:20:08	2
G1KD14G00202B			0.0.0.0	test_020	0	2.4G	23820	2016-10-28 09:13:27	2

Page 1 of 1 10 View 1 - 3 of 3

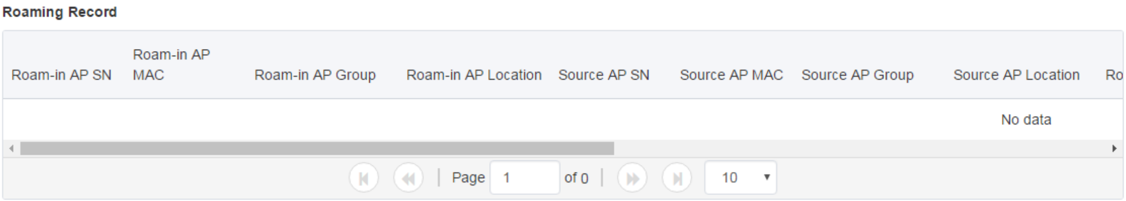
Roaming Record

Roam-in AP SN	Roam-in AP MAC	Roam-in AP Group	Roam-in AP Location	Source AP SN	Source AP MAC	Source AP Group	Source AP Location	Ro
							No data	

Page 1 of 0 10

5.3.2.1 Record

The **Record** page displays the client online/offline records and roaming records. The online/offline records are displayed in the right area of the preceding figure; and the roaming records are displayed in the following figure.



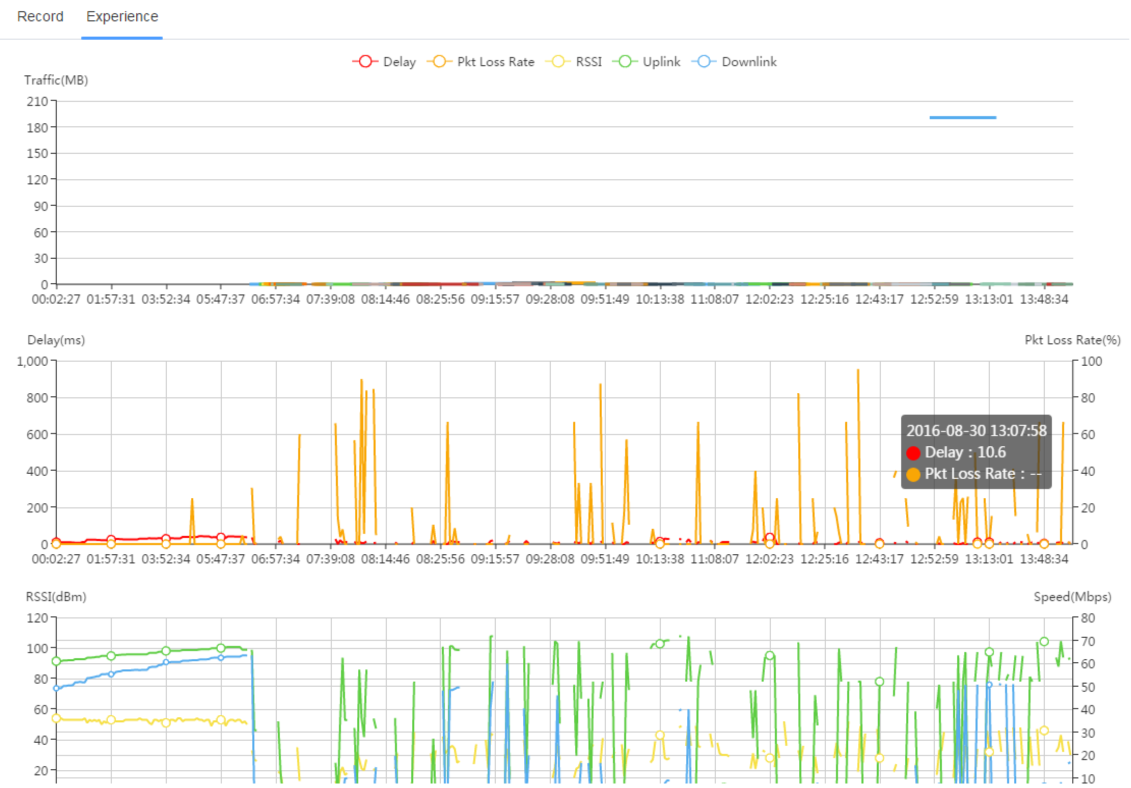
Roaming Record

Roam-in AP SN	Roam-in AP MAC	Roam-in AP Group	Roam-in AP Location	Source AP SN	Source AP MAC	Source AP Group	Source AP Location	Ro
							No data	

Page 1 of 0 10

5.3.2.2 Experience

The following figure shows the client traffic/time diagram in the lower part, the delay/packet loss rate/time diagram in the middle (indicating the relationship between the delay and packet loss rate), and the signal strength/rate/time diagram in the lower part. The time axes in the three diagrams are the same and all start from 00:00 to the current time of the current day.



5.4 Report

5.4.1 Searching Reports

Choose **Monitoring** > **Report** > **Search** to open the **Search** page.

- Filter condition

Type: Selecta report type, such as client, device, and CWMP log.

Data source: Select a data source, such as online clients and client statistics by day/hour.

- Search criteria

Select a field in the drop-down list for settings, and click **Add** to create a search criteria.

> Search criteria cannot be added repeatedly.

- Search result

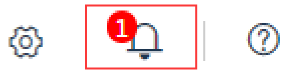
After a search criteria is added, and click **Search** to display the search results in the lower area on the page.

You can click ▽ on the right to select a field to be displayed or exported.

- Report export

Click **Export Report** to export a report.

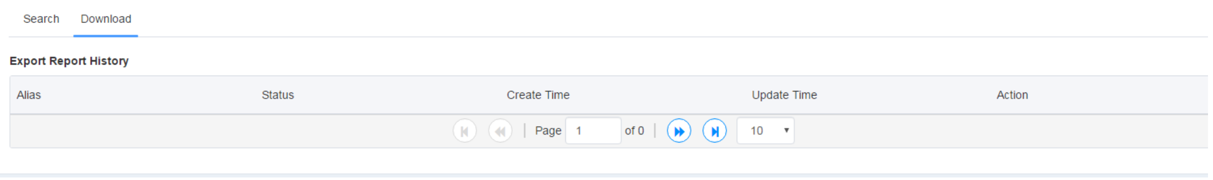
A prompt will be displayed after a report is successfully generated or fails to be generated, as shown in the red frame in the following figure:



You can click the icon to query the report export information.

5.4.2 Downloading Reports

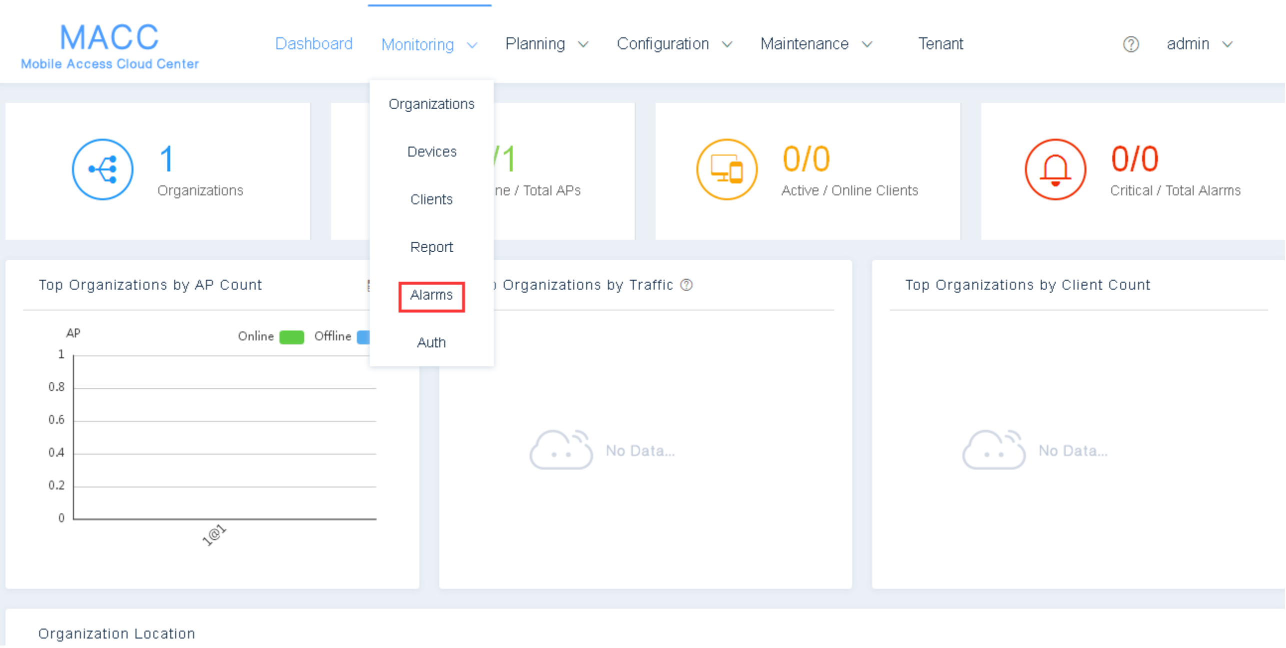
Click **Monitoring** > **Report** > **Download** to open the **Download** page, and learn about the download history.



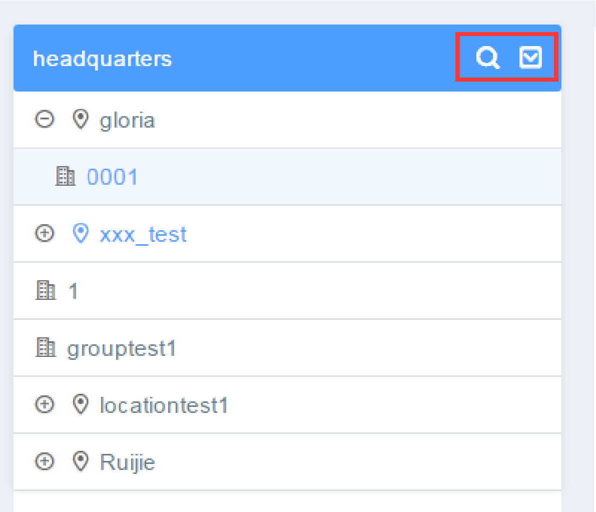
Export Report History

Alias	Status	Create Time	Update Time	Action

5.5 Alarms

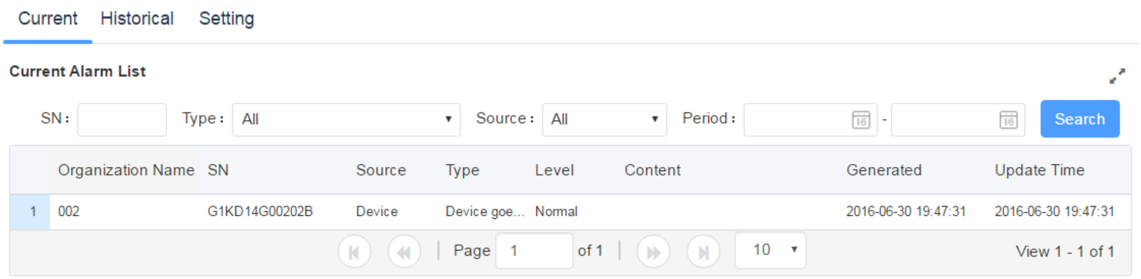


Click **Monitoring** > **Alarms** to open the alarm page, and select an organization on the left to display the alarm information.



The organization selection area on the left supports functions of searching and expanding all organizations.

5.5.1 Current Alarms



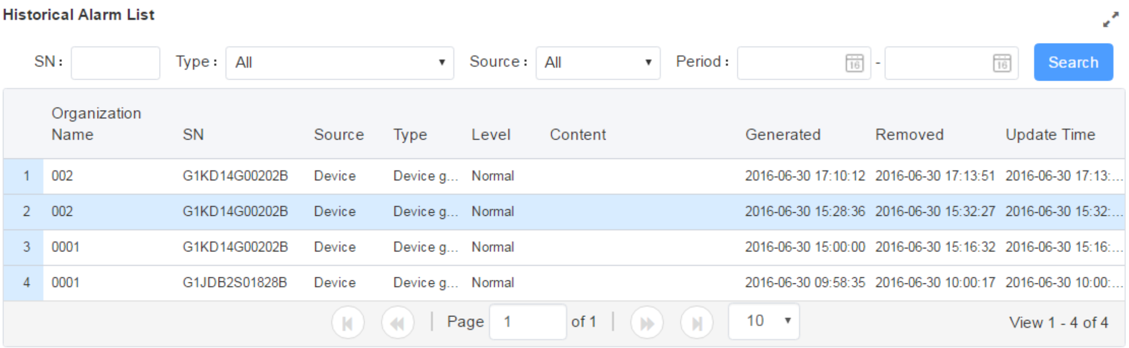
	Organization Name	SN	Source	Type	Level	Content	Generated	Update Time
1	002	G1KD14G00202B	Device	Device goe...	Normal		2016-06-30 19:47:31	2016-06-30 19:47:31

- The current alarm list page displays the generated alarms that have not been cleared. Currently supported alarm types include: **Device goes offline**, **Device goes online and offline continually**, **STUN changes continually**, and **Channel utilization**.
- The alarm list supports searches based on the device serial number, alarm type, alarm source (organization/AP), and alarm generation time. Only one current alarm record is displayed for alarms of the same source and the same type.
- Once the current AP alarm is cleared, the corresponding record will be moved to the historical alarm list.

The following describes the conditions for generating alarms.

Type	**Condition**	**Description**
Device goes offline	An AP goes offline on the MACC.	The AP is disconnected from the MACC, or the AP is powered off.
Device goes online and offline continually	Online/offline change times of an AP within two hours exceeds a default threshold.	The connection between the AP and the MACC is unstable or the AP has a software or hardware fault.
STUN changes continually	Change times of STUN addresses within two hours exceeds a default threshold.	Indicates that the NAT mapping at upstream export is unstable. The upstream egress NAT mapping of the AP is unstable.
Channel utilization	The RF channel utilization exceeds 80%.	RF channel utilization is high and interference is strong. It is recommended to change the channel.

5.5.2 Historical Alarms



Historical Alarm List

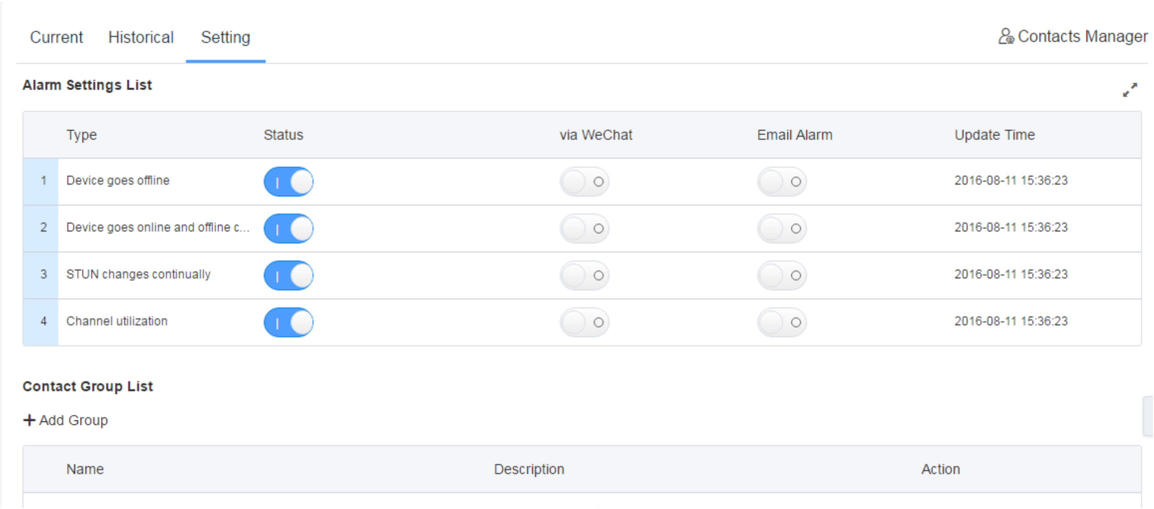
SN: Type: All Source: All Period: -

	Organization Name	SN	Source	Type	Level	Content	Generated	Removed	Update Time
1	002	G1KD14G00202B	Device	Device g...	Normal		2016-06-30 17:10:12	2016-06-30 17:13:51	2016-06-30 17:13:...
2	002	G1KD14G00202B	Device	Device g...	Normal		2016-06-30 15:28:36	2016-06-30 15:32:27	2016-06-30 15:32:...
3	0001	G1KD14G00202B	Device	Device g...	Normal		2016-06-30 15:00:00	2016-06-30 15:16:32	2016-06-30 15:16:...
4	0001	G1JDB2S01828B	Device	Device g...	Normal		2016-06-30 09:58:35	2016-06-30 10:00:17	2016-06-30 10:00:...

Page 1 of 1 | 10 | View 1 - 4 of 4

- The historical alarm list page displays the cleared alarms. Currently supported alarm types include: **Device goes offline**, **Device goes online and offline continually**, **STUN changes continually**, and **Channel utilization**.
- The historical alarm list supports the searches based on the AP serial number, alarm type, alarm source (organization/device), and alarm generation time.

5.5.3 Alarm Settings



Alarm Settings List

	Type	Status	via WeChat	Email Alarm	Update Time
1	Device goes offline	●	○	○	2016-08-11 15:36:23
2	Device goes online and offline c...	●	○	○	2016-08-11 15:36:23
3	STUN changes continually	●	○	○	2016-08-11 15:36:23
4	Channel utilization	●	○	○	2016-08-11 15:36:23

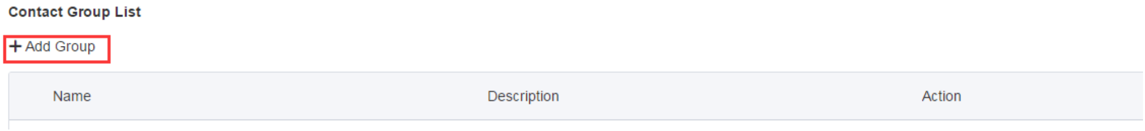
Contact Group List

+ Add Group

Name	Description	Action

Alarm settings are configured by organization. If no alarm settings are configured, the MACC global settings are adopted.

On the Alarm Settings List page, switches are provided to detect alarms of various types and push alarms via WeChat and/or via emails. Alarms can be pushed via WeChat and/or emails only when the alarm detection switch is enabled. When the alarm detection switch is enabled, alarm information of the corresponding type is displayed on the **Current** and **Historical** pages. When the **via WeChat** switch is enabled, the MACC can push messages about alarm generation and clearing to the client of a bound WeChat account. When the **Email Alarm** switch is enabled, alarms of the corresponding type concerning an organization will be pushed via emails to the contacts configured in the contact list of the organization.



Contact Group List

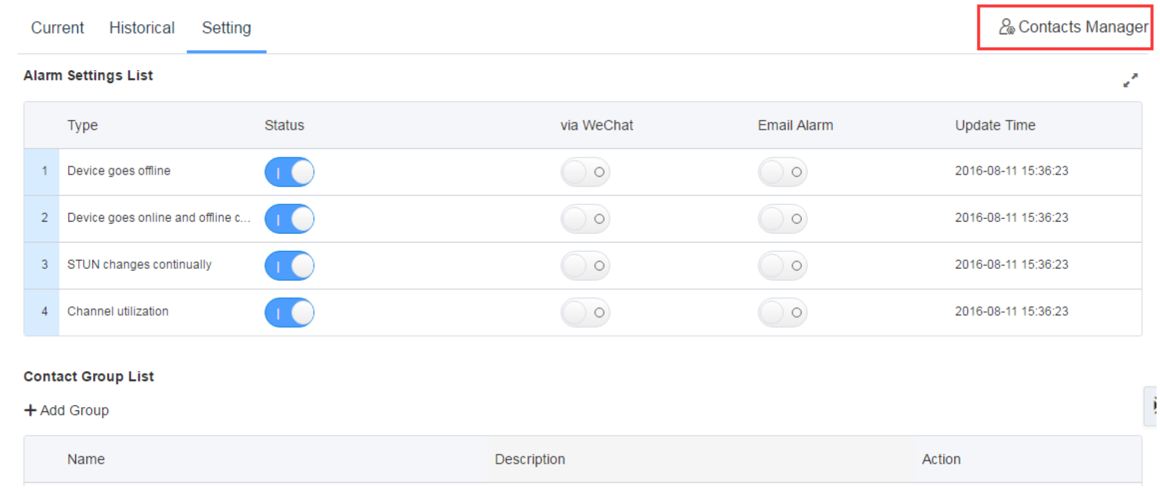
+ Add Group

Name	Description	Action

Note: To use the Email Alarm function, click ⚙ and select System Settings to preset the account and password of the SMTP server for sending emails on the Advanced page via the administrator account. For details about the configuration page, see section 7.1.2.

5.5.4 Alarm Contact Settings

Alarm contacts are configured by account. Alarm contacts configured for different accounts are invisible to each other. You can click **Contacts Manager** in the following figure to display the **Contacts Manager** page.



Alarm Settings List

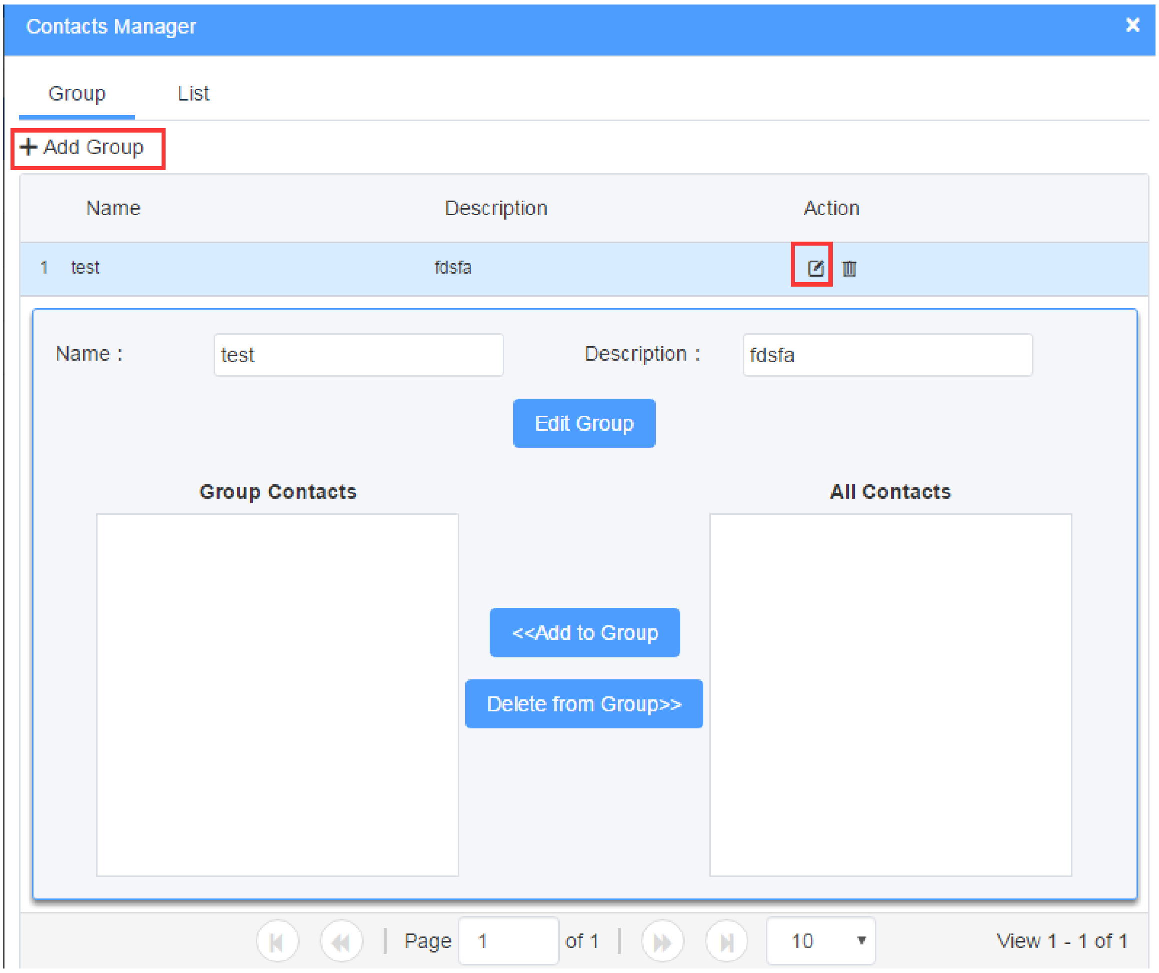
	Type	Status	via WeChat	Email Alarm	Update Time
1	Device goes offline	●	○	○	2016-08-11 15:36:23
2	Device goes online and offline c...	●	○	○	2016-08-11 15:36:23
3	STUN changes continually	●	○	○	2016-08-11 15:36:23
4	Channel utilization	●	○	○	2016-08-11 15:36:23

Contact Group List

+ Add Group

Name	Description	Action

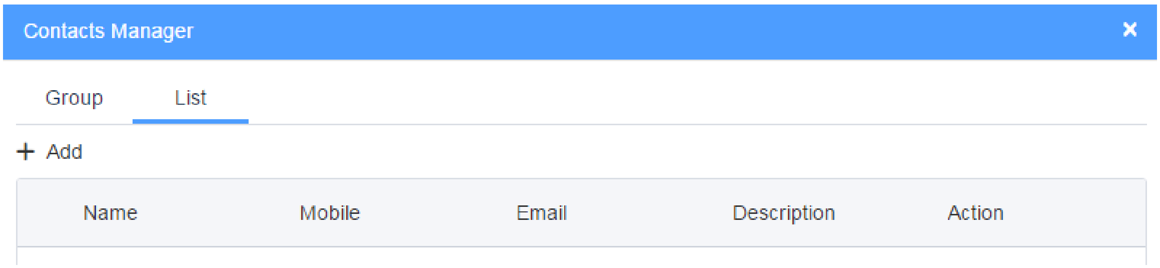
On the **Contacts Manager** page, you can create contact groups, and add contacts to contact groups.



	Name	Description	Action
1	test	fdsfa	

Name : test

Description : fdsfa



Name	Mobile	Email	Description	Action

6 Maintenance

The **Maintenance** module mainly provides the following functional services:

- Device upgrade
- Fault diagnosis
- Account management
- Disk cleanup

6.1 Device Upgrade

The following three tab pages are provided for device firmware management:

- Upgrade
- Upgrade Logs
- Firmware

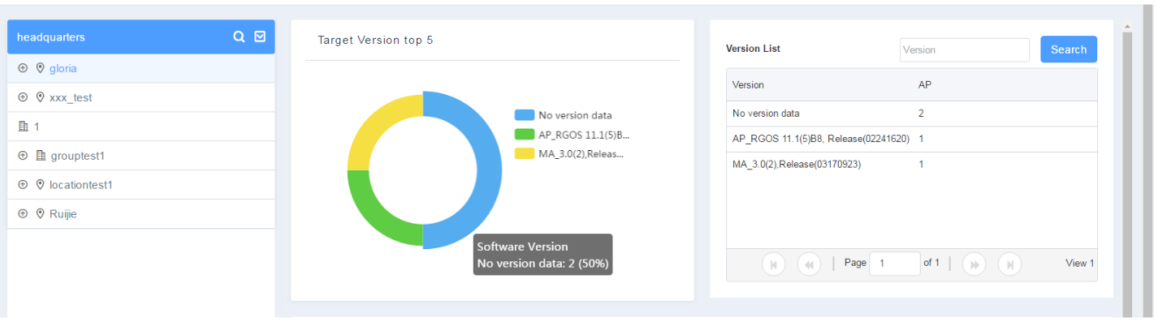
6.1.1 Upgrade

The **Upgrade** page consists of the following two modules:

- Version statistics
- Software upgrade

6.1.1.1 Checking Version Information

Choose **Maintenance** > **Upgrade** to display the top 5 versions in the form of a pie chart and a list for each group.



Version	AP
No version data	2
AP_RGOS 11.1(5)B8, Release(02241620)	1
MA_3.0(2),Release(03170923)	1

6.1.1.2 Upgrading Devices

For convenience, two upgrade modes are provided:

- **Upgrade Selected**

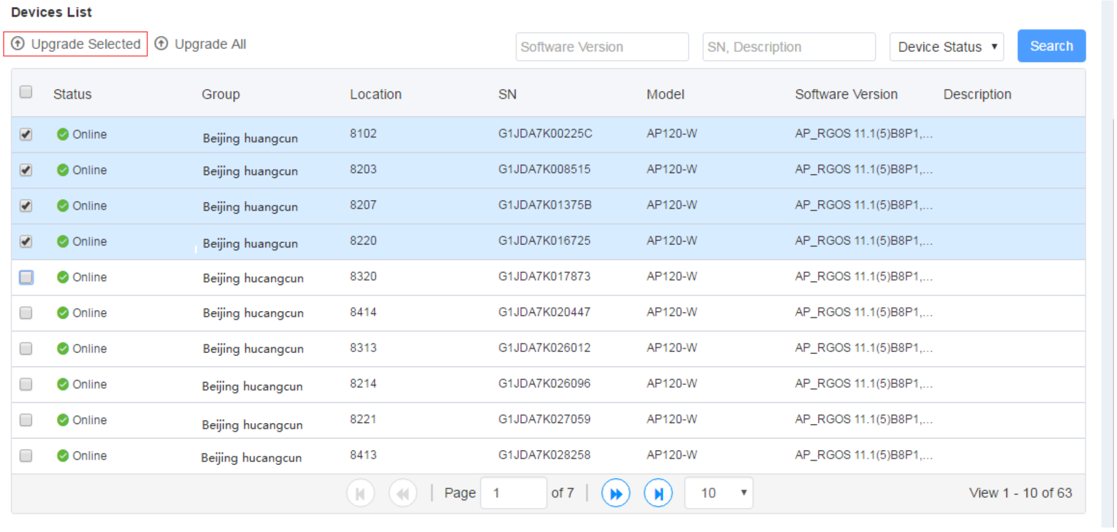
This mode enables you to upgrade a selected AP, and is suitable for a scenario with a few APs to be upgraded.

- **Upgrade All**

Selects all the devices in the list, and applies to the status when multiple devices require upgrade; implements a quick upgrade with selected groups and version numbers. This mode enables you to upgrade all APs in the list, and is suitable for a scenario with a large number of APs. A group or a software version number can be specified to perform fast upgrades.

- **Upgrade Selected**

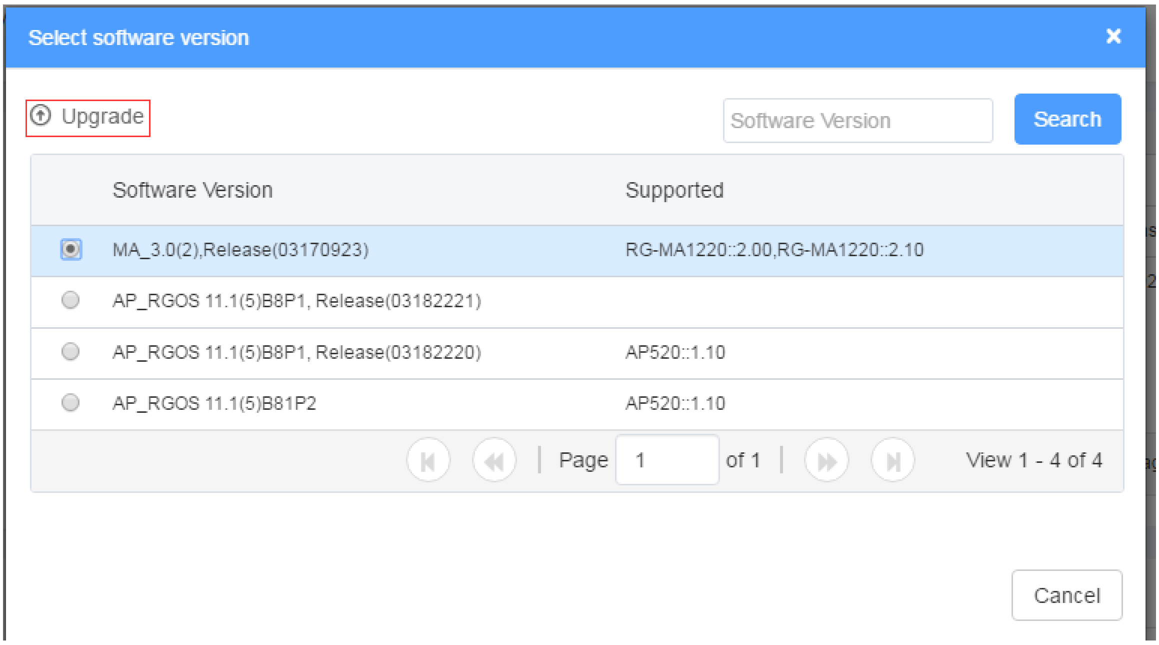
1. Select a group on the left, select a target AP, and click **Upgrade Selected**.



Devices List

☐	Status	Group	Location	SN	Model	Software Version	Description
☑	Online	Beijing huangcun	8102	G1JDA7K00225C	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☑	Online	Beijing huangcun	8203	G1JDA7K008515	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☑	Online	Beijing huangcun	8207	G1JDA7K01375B	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☑	Online	Beijing huangcun	8220	G1JDA7K016725	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☐	Online	Beijing hucangcun	8320	G1JDA7K017873	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☐	Online	Beijing hucangcun	8414	G1JDA7K020447	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☐	Online	Beijing hucangcun	8313	G1JDA7K026012	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☐	Online	Beijing hucangcun	8214	G1JDA7K026096	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☐	Online	Beijing hucangcun	8221	G1JDA7K027059	AP120-W	AP_RGOS 11.1(5)B8P1,...	
☐	Online	Beijing hucangcun	8413	G1JDA7K028258	AP120-W	AP_RGOS 11.1(5)B8P1,...	

2. Select a software version.



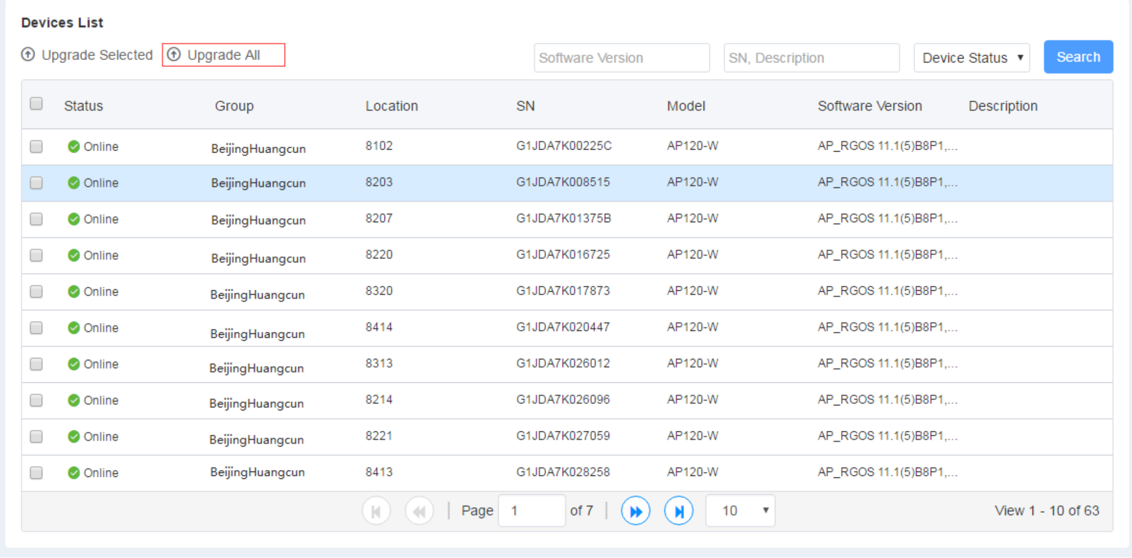
Select software version

	Software Version	Supported
●	MA_3.0(2),Release(03170923)	RG-MA1220::2.00,RG-MA1220::2.10
○	AP_RGOS 11.1(5)B8P1, Release(03182221)	
○	AP_RGOS 11.1(5)B8P1, Release(03182220)	AP520::1.10
○	AP_RGOS 11.1(5)B81P2	AP520::1.10

Upgrading APs

- **Upgrade All:**

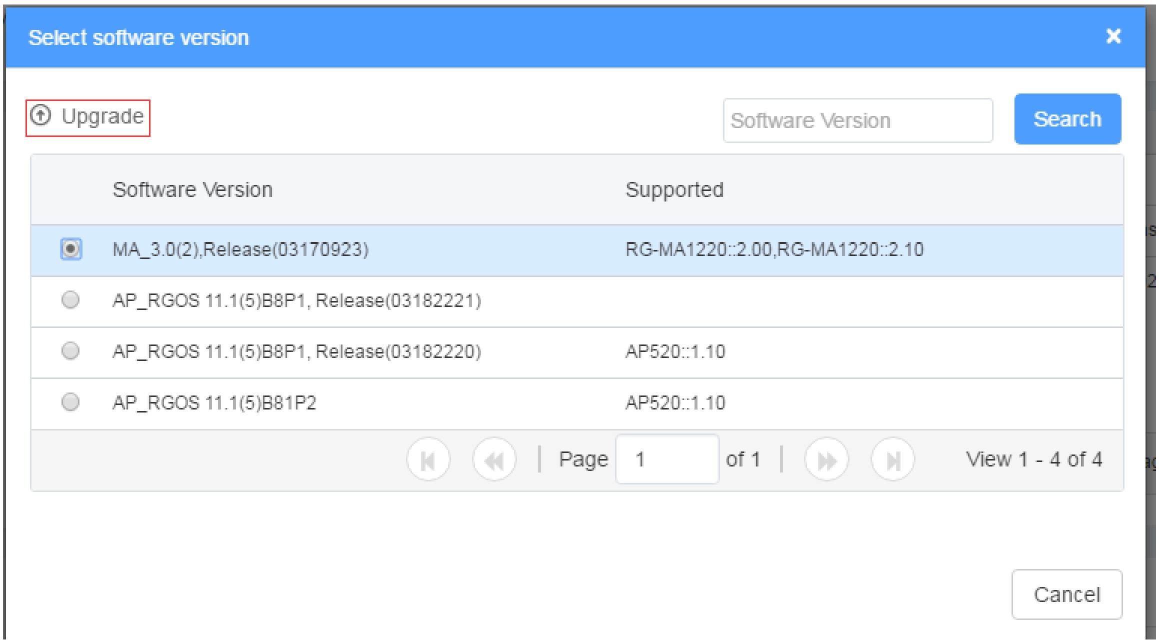
1. Check the devices list based on a condition, and click **Upgrade All**.



Devices List

□	Status	Group	Location	SN	Model	Software Version	Description
□	Online	BeijingHuangcun	8102	G1JDA7K00225C	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8203	G1JDA7K008515	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8207	G1JDA7K01375B	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8220	G1JDA7K016725	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8320	G1JDA7K017873	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8414	G1JDA7K020447	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8313	G1JDA7K026012	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8214	G1JDA7K026096	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8221	G1JDA7K027059	AP120-W	AP_RGOS 11.1(5)B8P1,...	
□	Online	BeijingHuangcun	8413	G1JDA7K028258	AP120-W	AP_RGOS 11.1(5)B8P1,...	

2. Select a software version.

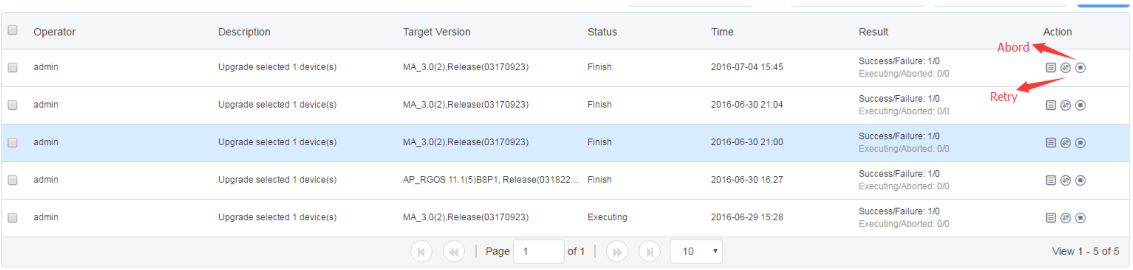


Select software version

	Software Version	Supported
●	MA_3.0(2),Release(03170923)	RG-MA1220::2.00,RG-MA1220::2.10
○	AP_RGOS 11.1(5)B8P1, Release(03182221)	
○	AP_RGOS 11.1(5)B8P1, Release(03182220)	AP520::1.10
○	AP_RGOS 11.1(5)B81P2	AP520::1.10

6.1.2 Upgrade Logs

The MACC provides the upgrade tracing function, and enables you to check the upgrade status, abort the upgrade, and retry.

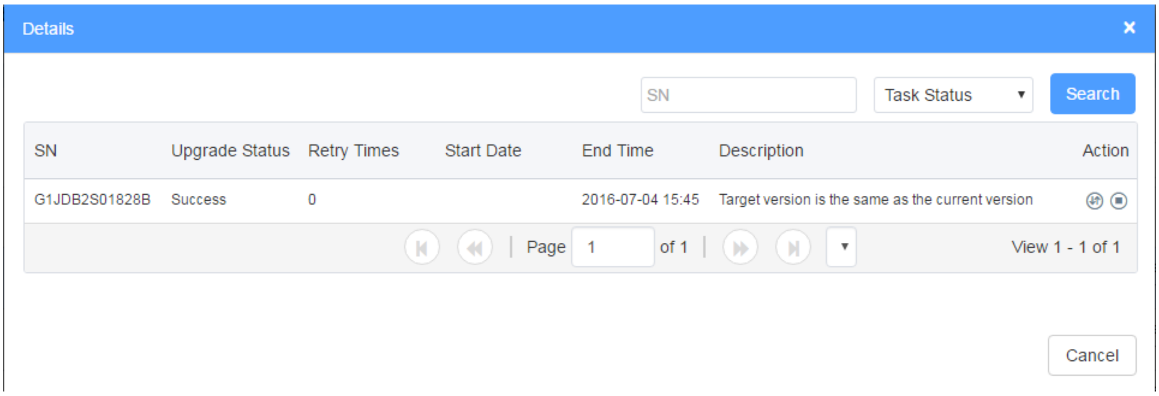


□	Operator	Description	Target Version	Status	Time	Result	Action
□	admin	Upgrade selected 1 device(s)	MA_3.0(2),Release(03170923)	Finish	2016-07-04 15:45	Success/Failure: 1/0 Executing/Aborted: 0/0	
□	admin	Upgrade selected 1 device(s)	MA_3.0(2),Release(03170923)	Finish	2016-06-30 21:04	Success/Failure: 1/0 Executing/Aborted: 0/0	
□	admin	Upgrade selected 1 device(s)	MA_3.0(2),Release(03170923)	Finish	2016-06-30 21:00	Success/Failure: 1/0 Executing/Aborted: 0/0	
□	admin	Upgrade selected 1 device(s)	AP_RGOS 11.1(5)B8P1, Release(031822...	Finish	2016-06-30 16:27	Success/Failure: 1/0 Executing/Aborted: 0/0	
□	admin	Upgrade selected 1 device(s)	MA_3.0(2),Release(03170923)	Executing	2016-06-29 15:28	Success/Failure: 1/0 Executing/Aborted: 0/0	

Retry: Restart the upgrade task that failed or is aborted.

Abort: Stops the upgrade task if the upgrade command has not been pushed.

Click ☰ to check log details.



Details ×

SN | Task Status ▾ | Search

SN	Upgrade Status	Retry Times	Start Date	End Time	Description	Action
G1JDB2S01828B	Success	0		2016-07-04 15:45	Target version is the same as the current version	

Page 1 of 1 ▾ View 1 - 1 of 1

Cancel

Retry: Restart the upgrade task.

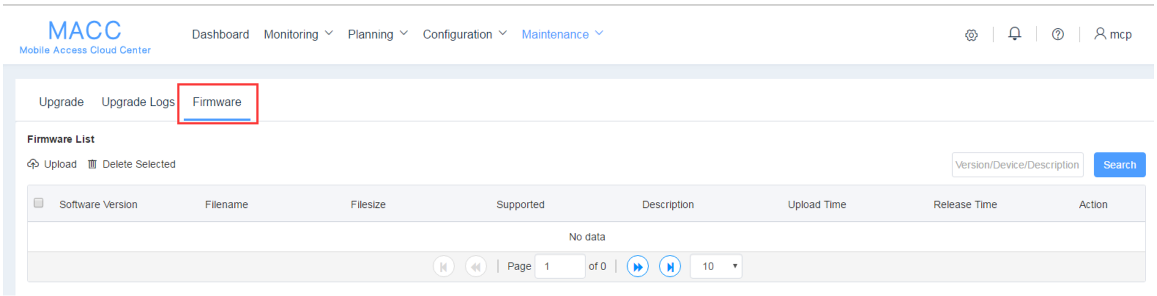
Abort: Stop the upgrade task.

Abort: You cannot stop the upgrade task if the upgrade command has been pushed to the AP.

Retry: You can only restart the failed or aborted upgrade task.

6.1.3 Managing Firmware

Choose **Maintenance** > **Upgrade** and switch to **Firmware**. The **Firmware** tab page enables you to upload firmware and query, modify, and delete firmware information.



Firmware List

Upload | Delete Selected | Version/Device/Description | Search

□	Software Version	Filename	Filesize	Supported	Description	Upload Time	Release Time	Action
No data								

Page 1 of 0 | 10 ▾

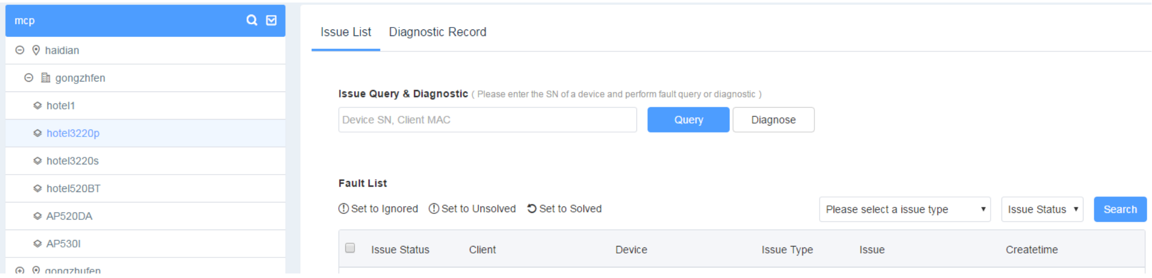
6.2 Fault Diagnosis

Choose **Maintenance** > **Fault Diagnosis** to display the **Fault Diagnosis** page. On the left side of the page, the organization to which an AP belongs can be selected.

The **Fault Diagnosis** page provides the following functions:

- Device diagnosis
- Issue list
- Diagnostic records

6.2.1 Issue List



Issue Query & Diagnostic (Please enter the SN of a device and perform fault query or diagnostic)

Device SN, Client MAC

Fault List

□	Issue Status	Client	Device	Issue Type	Issue	Createtime

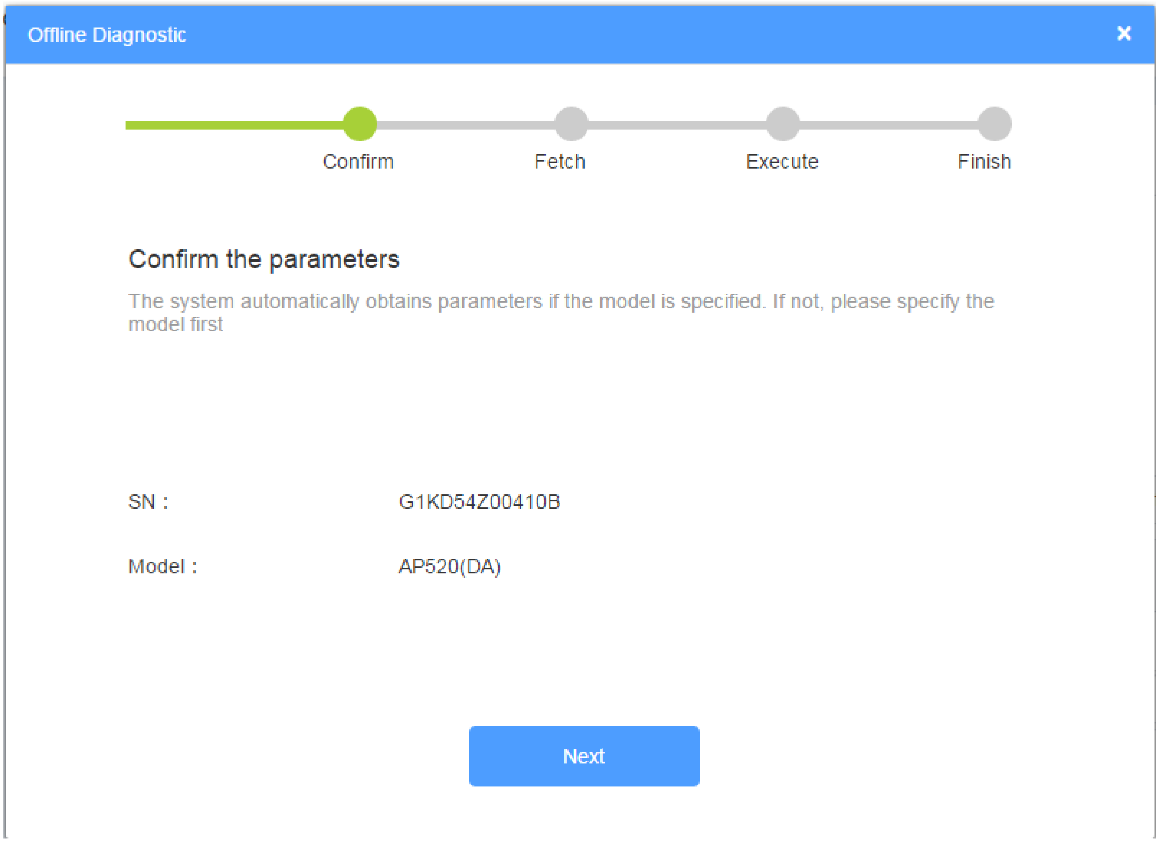
- ➢ In the **Issue Query & Diagnostic** area, enter the serial number or MAC address of an AP in the text box and click **Query** to display the issue list. The issue type and the issue status can be specified to query the issues. The status of a selected issue can be set to **Set to Ignored**, **Set to Unsolved**, and **Set to Solved** above the list. In the **Fault List** area, basic information about MACC issues is displayed. You can click an issue to query the details. The following describes the details pages for different issue types.

  1. Number of clients associated with an AP exceeding the limit

  The list on the left displays serial numbers of APs in the same organization with the same issue. After you click a serial number, the issue details (including the organization information, AP information, issue description, and suggestion) are displayed in the right area. In the lower part, records about this issue in different time periods are displayed. After you click a corresponding record, the AP overload data is displayed in a bar chart.

- ➢ In the **Issue Query & Diagnostic** area, enter the complete serial number of an AP in the text box and click **Diagnose** to perform diagnosis as promoted. The following describes the offline diagnosis process.

  (1) To perform offline diagnosis on an offline AP, confirm the AP information obtained automatically by the system. If no AP information exists, manually select an AP and click **Next**.



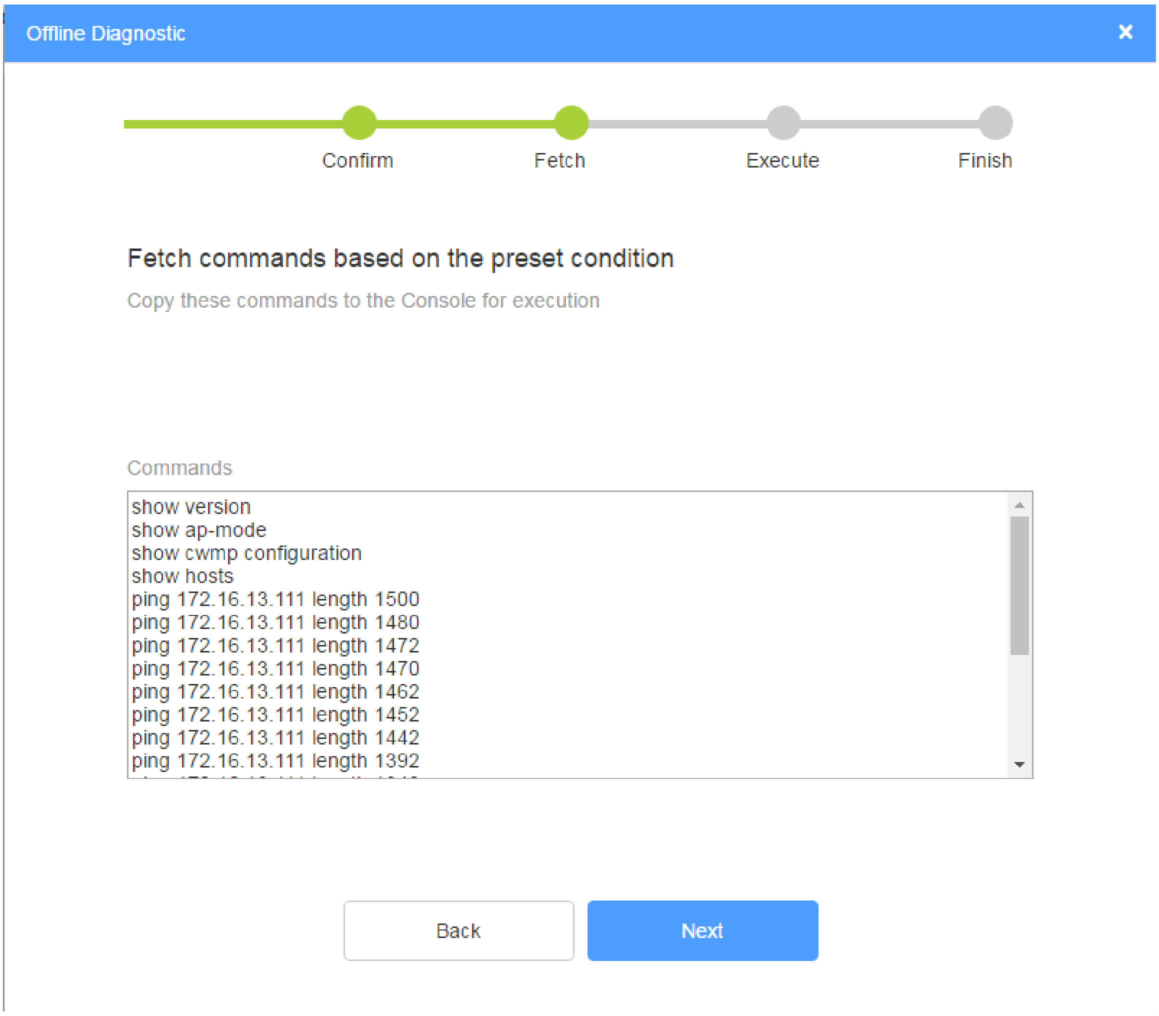
Confirm the parameters

The system automatically obtains parameters if the model is specified. If not, please specify the model first

SN : G1KD54Z00410B

Model : AP520(DA)

  (2) Obtain the commands of the AP. Copy the commands to the AP CLI for execution and click **Next**.



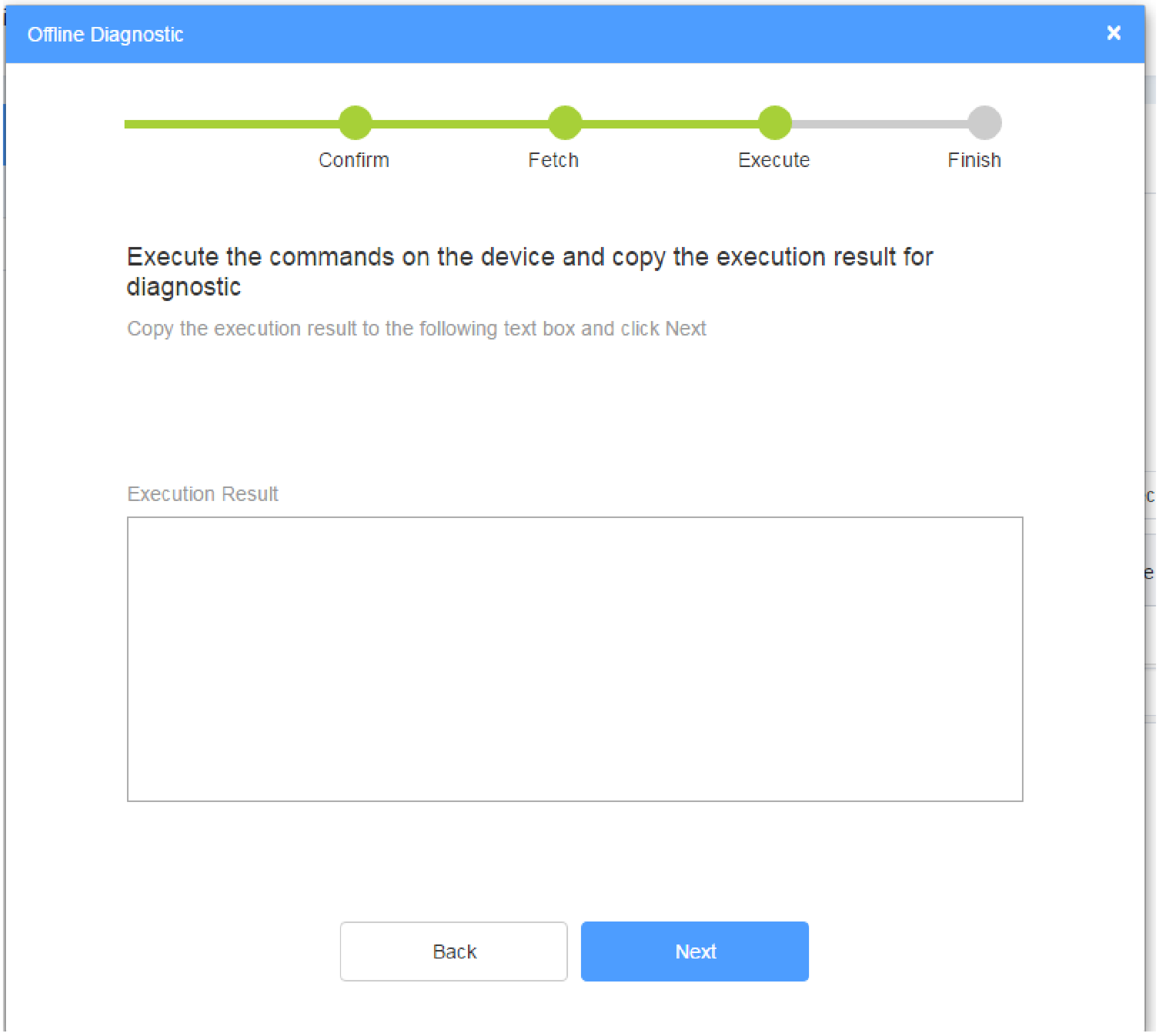
Fetch commands based on the preset condition

Copy these commands to the Console for execution

Commands

```
show version
show ap-mode
show cwmp configuration
show hosts
ping 172.16.13.111 length 1500
ping 172.16.13.111 length 1480
ping 172.16.13.111 length 1472
ping 172.16.13.111 length 1470
ping 172.16.13.111 length 1462
ping 172.16.13.111 length 1452
ping 172.16.13.111 length 1442
ping 172.16.13.111 length 1392
```

(3) Copy the command execution results to the **Execution Result** text box and click **Next**.



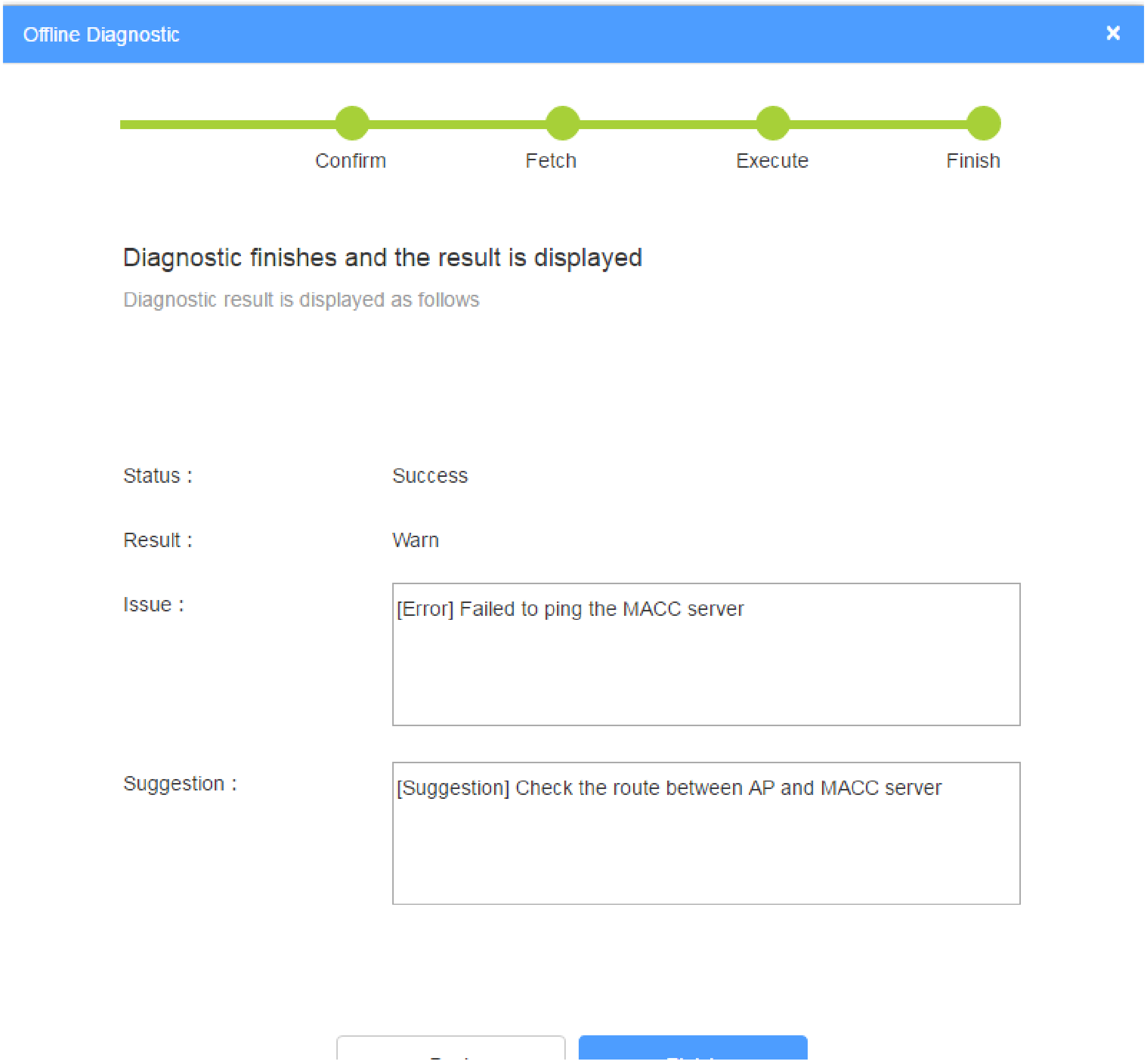
Offline Diagnostic

Execute the commands on the device and copy the execution result for diagnostic

Copy the execution result to the following text box and click Next

Execution Result

(4) The offline diagnosis results, including the diagnosis status, diagnosis result, detected issues, and corresponding suggestions are displayed.



Diagnostic finishes and the result is displayed

Diagnostic result is displayed as follows

Status : Success

Result : Warn

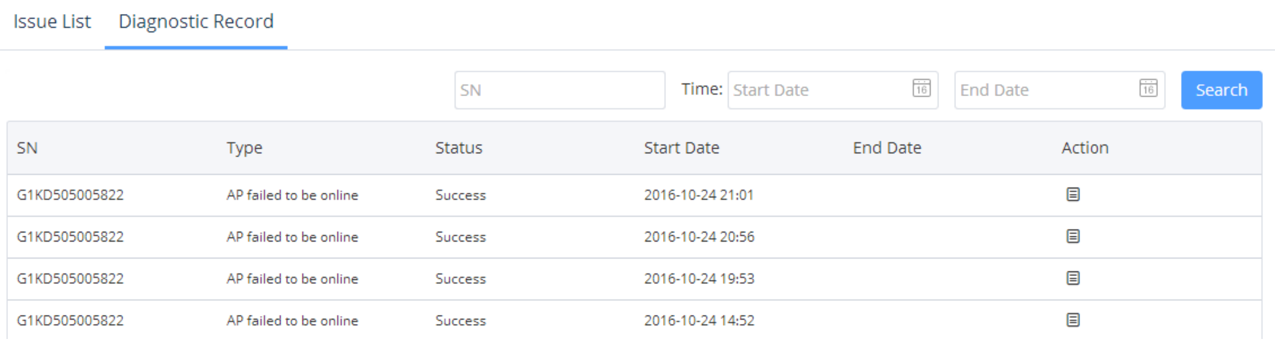
Issue : [Error] Failed to ping the MACC server

Suggestion : [Suggestion] Check the route between AP and MACC server

（5） Click **Finish**. Each diagnosis result is recorded and can be queried on the **Diagnostic Record** page.

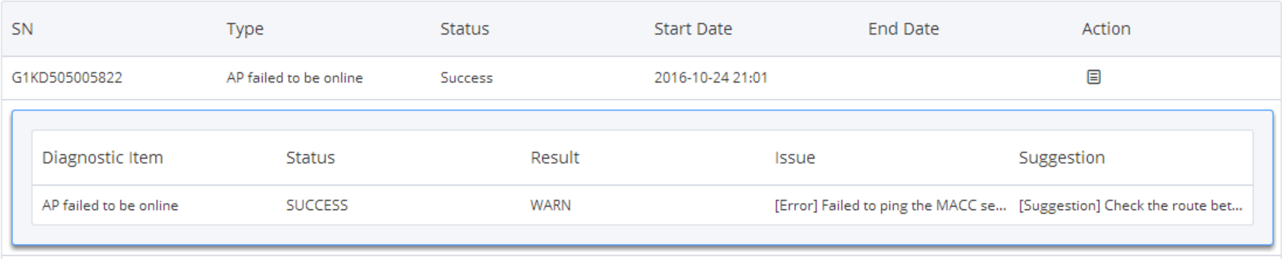
6.2.2 Diagnostic Record

On the **Diagnostic Record** page, diagnostic records of APs can be queried. You can select an organization on the left and query the diagnostic records based on criteria such as the serial number and diagnosis time range.



SN	Type	Status	Start Date	End Date	Action
G1KD505005822	AP failed to be online	Success	2016-10-24 21:01		▤
G1KD505005822	AP failed to be online	Success	2016-10-24 20:56		▤
G1KD505005822	AP failed to be online	Success	2016-10-24 19:53		▤
G1KD505005822	AP failed to be online	Success	2016-10-24 14:52		▤

In the diagnostic record list, **SN**, **Type**, **Status**, **Start Date**, and **End Date** about diagnostic records are displayed. You can click the operation button in the **Action** column of a record to query the diagnosis details. The issues detected during the diagnosis and the corresponding suggestions will be displayed.



SN	Type	Status	Start Date	End Date	Action
G1KD505005822	AP failed to be online	Success	2016-10-24 21:01		▤

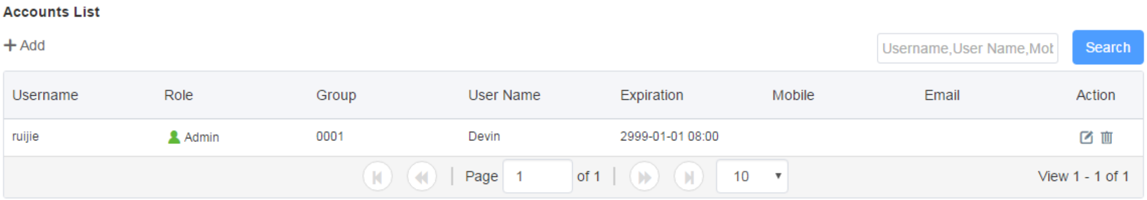
Diagnostic Item	Status	Result	Issue	Suggestion
AP failed to be online	SUCCESS	WARN	[Error] Failed to ping the MACC se...	[Suggestion] Check the route bet...

6.3 Account Management

Account management includes the following functions:

- Basic operations
- Permission management

Basic operations include add, delete, edit, and search.



Accounts List

+ Add

Username,User Name,Mot

Search

Username	Role	Group	User Name	Expiration	Mobile	Email	Action
ruijie	Admin	0001	Devin	2999-01-01 08:00			✎ 🗑

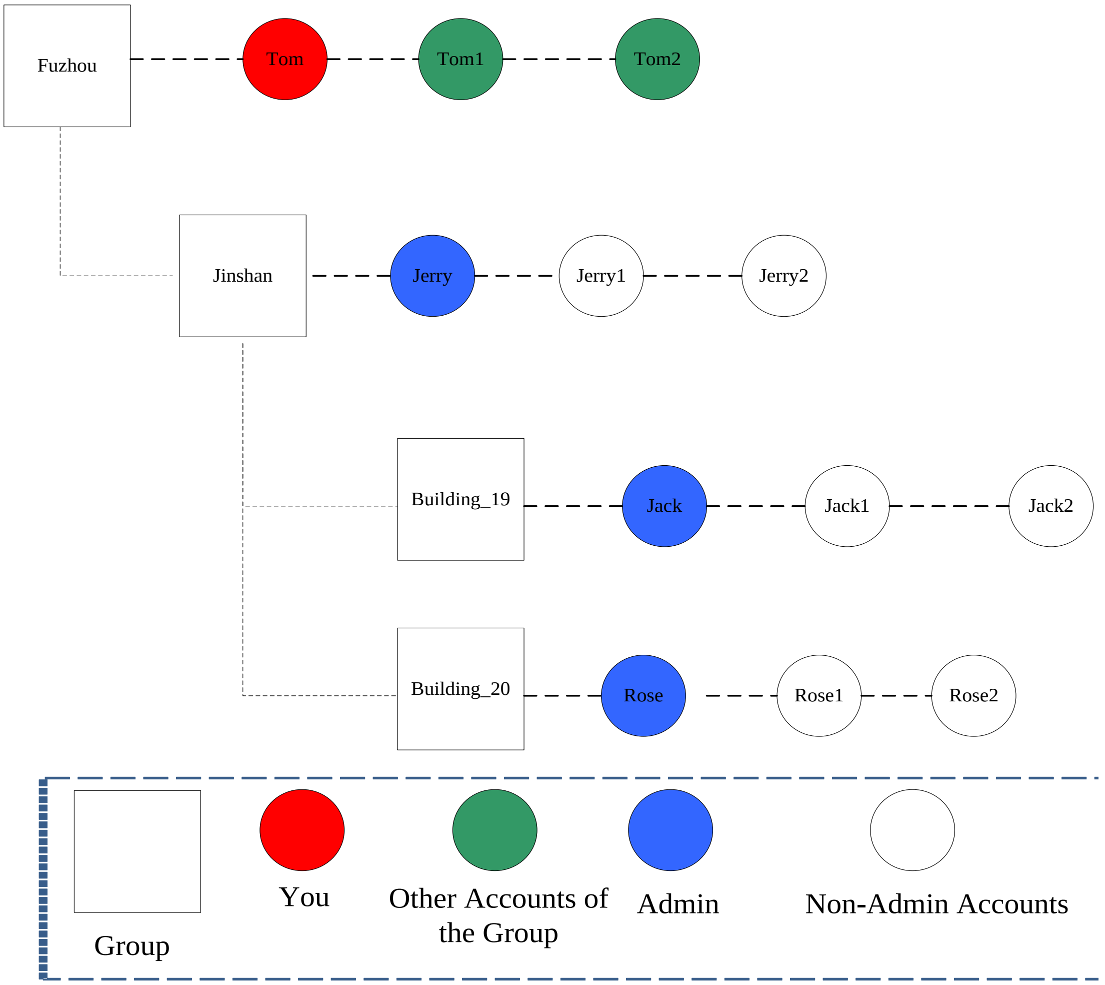
6.3.1 Permission Overview

6.3.1.1 Network Resource Permissions

The MACC controls the network resource permissions by group. Each AP must be associated with a group. The groups are hierarchical, and each account can be associated with one group. After an account is associated with a group, the account can only control the group tree but cannot manage groups that are not in the tree.

For ease of management, the administrator role is introduced to allocate accounts. One group can have one administrator at most, and the administrator has the right to manage accounts of lower-level groups and groups of the same level.

For ease of understanding, the relationship between accounts and groups from the perspective of **Tom** is displayed as follows:



In this section, Tom, Jack, and Rose and their group permissions are used as an example herein for description.

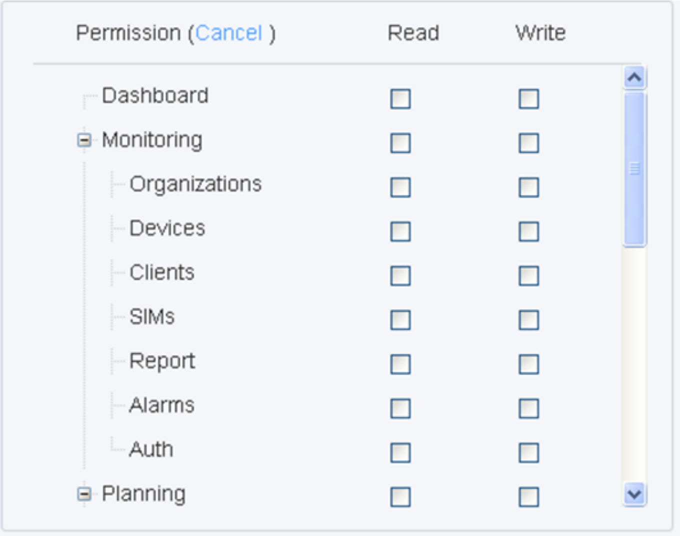
Account	AP Permission	Account Permission
Tom	Checks and manages all APs in the **Fuzhou** group and its sub groups.	Owns permissions on all accounts in the **Fuzhou** group.
Jack	Checks and manages all APs in the **Building_19** group and its sub groups.	Owns permissions on all accounts under the **Building_19** group.
Rose	Checks and manages all APs in the **Building_20** group and its sub groups.	Owns no permissions

Accounts cannot be allocated to a floor group.

6.3.1.2 Menu Permissions

The MACC supports resource control based on menu permissions. Each menu page has read and write permissions.

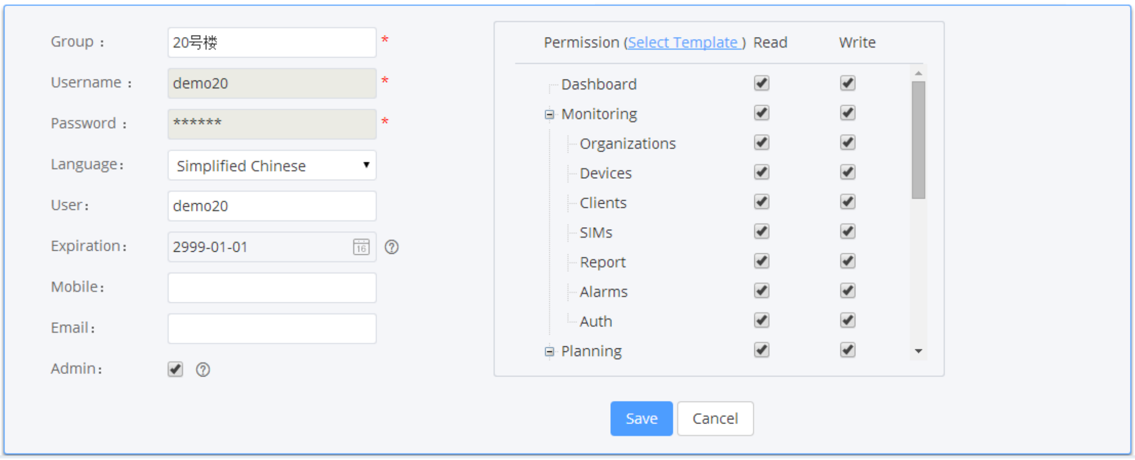
Menus with the read permission provide the display function; menus with the write permission provide the add, delete, and edit functions.



Permission (Cancel)	Read	Write
Dashboard	□	□
⊟ Monitoring	□	□
Organizations	□	□
Devices	□	□
Clients	□	□
SIMs	□	□
Report	□	□
Alarms	□	□
Auth	□	□
⊟ Planning	□	□

6.3.2 Adding Accounts

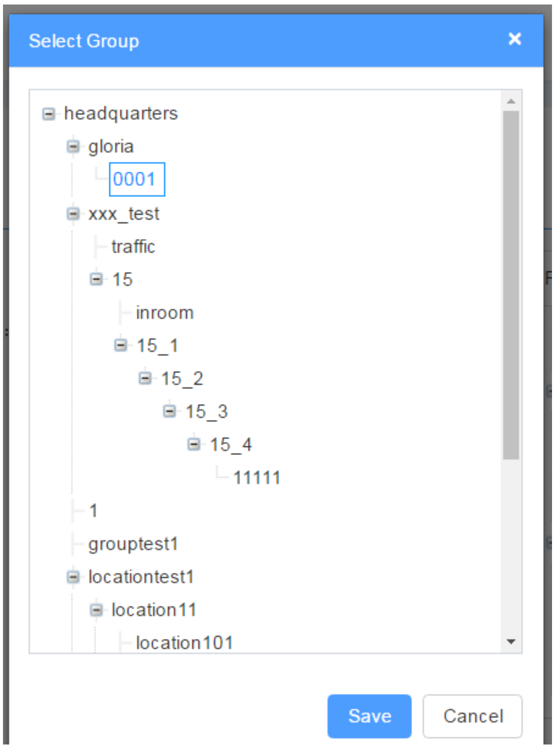
(1) Click +Add to add an account.

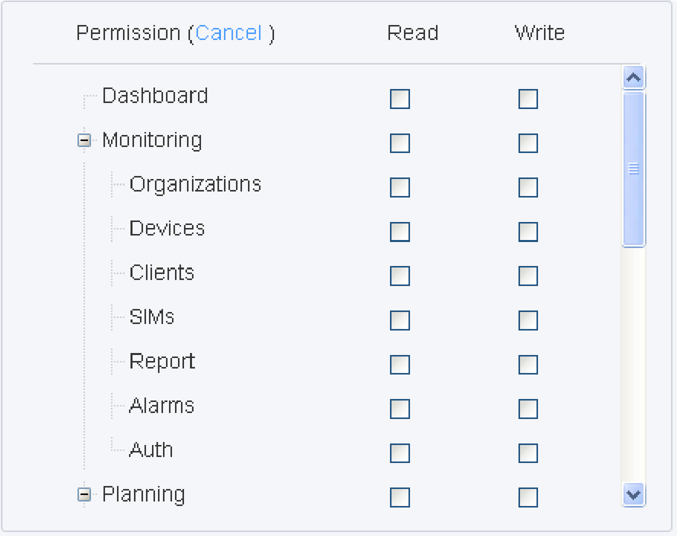


Group :	20号楼 *
Username :	demo20 *
Password :	****** *
Language:	Simplified Chinese ▾
User:	demo20
Expiration:	2999-01-01
Mobile:	
Email:	
Admin:	☑

Permission (Select Template)	Read	Write
Dashboard	☑	☑
⊟ Monitoring	☑	☑
Organizations	☑	☑
Devices	☑	☑
Clients	☑	☑
SIMs	☑	☑
Report	☑	☑
Alarms	☑	☑
Auth	☑	☑
⊟ Planning	☑	☑

(2) Click the **Group** text box to select a group for an account.

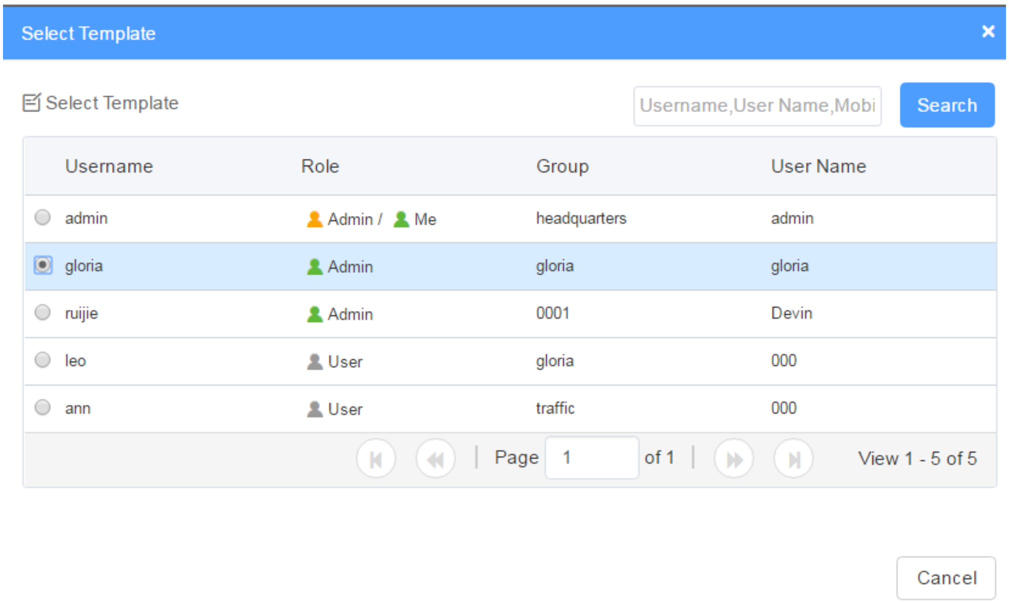




Permission (Cancel)	Read	Write
Dashboard	□	□
Monitoring	□	□
Organizations	□	□
Devices	□	□
Clients	□	□
SIMs	□	□
Report	□	□
Alarms	□	□
Auth	□	□
Planning	□	□

(3) Use this menu to configure permissions of an account on the Web: Accounts with the read permission can view the page, and accounts with the write permission can perform the add, delete, and edit operations.

(4) Click **Cancel** to open the **Select Template** page. Select a template to copy its permissions to the current account.



Select Template ×

Select Template   Username,User Name,Mobi   Search

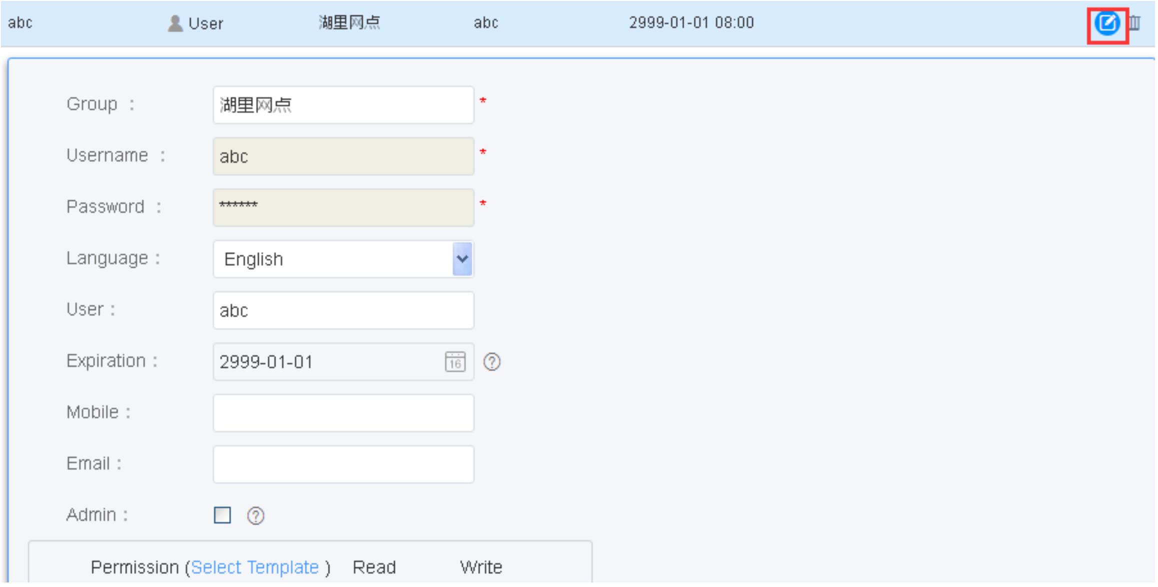
	Username	Role	Group	User Name
○	admin	Admin / Me	headquarters	admin
●	gloria	Admin	gloria	gloria
○	ruijie	Admin	0001	Devin
○	leo	User	gloria	000
○	ann	User	traffic	000

Page 1 of 1   View 1 - 5 of 5

Cancel

6.3.3 Editing Accounts

Click ✎ in the upper right corner of the account list to edit an account.



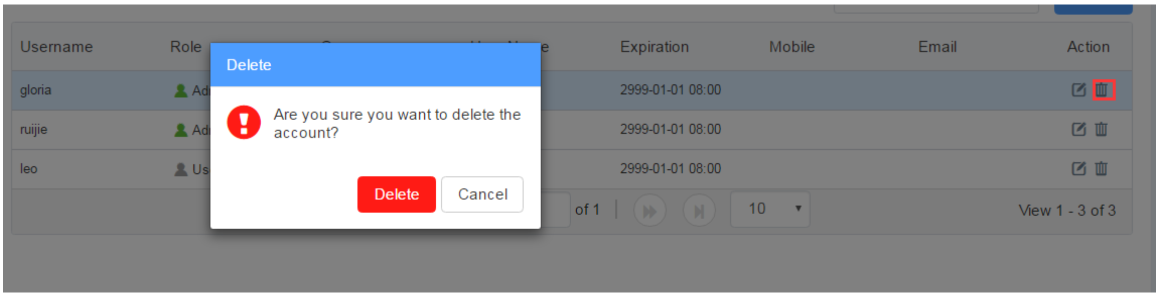
abc   User   湖里网点   abc   2999-01-01 08:00

Group :	湖里网点 *
Username :	abc *
Password :	****** *
Language :	English
User :	abc
Expiration :	2999-01-01
Mobile :	
Email :	
Admin :	□

Permission (Select Template)   Read   Write

6.3.4 Deleting Accounts

Click 🗑 in the upper right corner of the account list to delete an account.



Username	Role	Expiration	Mobile	Email	Action
gloria	Ad	2999-01-01 08:00			
ruijie	Ad	2999-01-01 08:00			
leo	Us	2999-01-01 08:00			

of 1 | 10 View 1 - 3 of 3

Delete

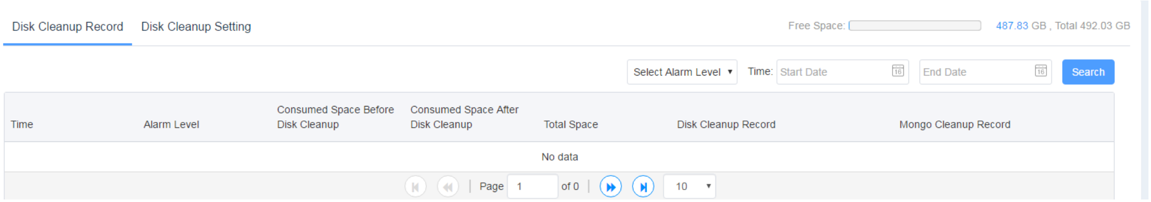
Are you sure you want to delete the account?

Delete Cancel

6.4 Disk Cleanup

Choose **Maintenance** > **Disk Cleanup** to display the **Disk Cleanup** page.

6.4.1 Disk Cleanup Record



Free Space: 487.83 GB , Total 492.03 GB

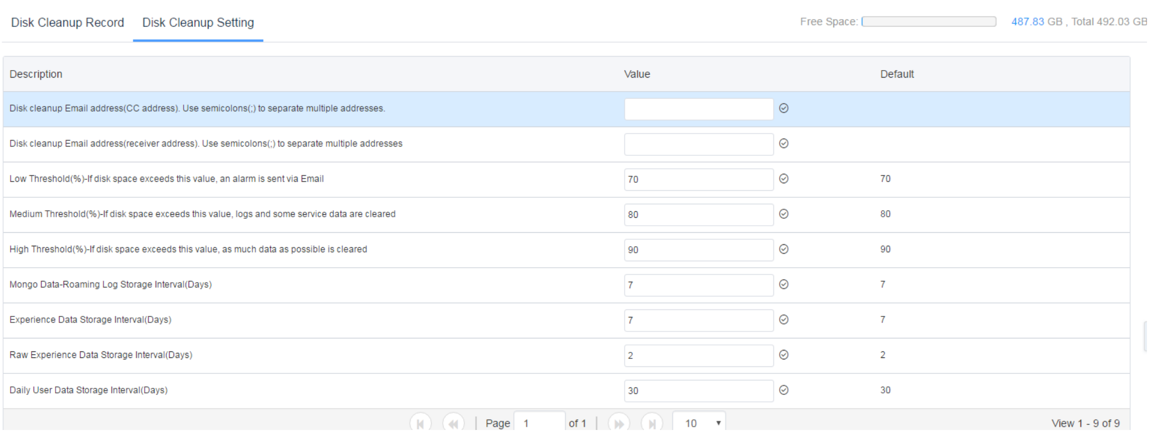
Select Alarm Level Time: Start Date End Date Search

Time	Alarm Level	Consumed Space Before Disk Cleanup	Consumed Space After Disk Cleanup	Total Space	Disk Cleanup Record	Mongo Cleanup Record
No data						

Page 1 of 0 | 10

The current disk usage is displayed in the upper right corner on the **Disk Cleanup Record** page. The disk cleanup records can be queried by alarm level and processing time. In the disk cleanup record list, **Time**, **Alarm Level**, **Consumed Space Before Disk Cleanup**, **Consumed Space After Disk Cleanup**, **Total Space**, **Disk Cleanup Record**, and **Mongo Cleanup Record** are displayed.

6.4.2 Disk Cleanup Setting



Free Space: 487.83 GB , Total 492.03 GB

Description	Value	Default
Disk cleanup Email address(CC address). Use semicolons(;) to separate multiple addresses.		
Disk cleanup Email address(receiver address). Use semicolons(;) to separate multiple addresses		
Low Threshold(%)-If disk space exceeds this value, an alarm is sent via Email	70	70
Medium Threshold(%)-If disk space exceeds this value, logs and some service data are cleared	80	80
High Threshold(%)-If disk space exceeds this value, as much data as possible is cleared	90	90
Mongo Data-Roaming Log Storage Interval(Days)	7	7
Experience Data Storage Interval(Days)	7	7
Raw Experience Data Storage Interval(Days)	2	2
Daily User Data Storage Interval(Days)	30	30

Page 1 of 1 | 10 View 1 - 9 of 9

The **Disk Cleanup Setting** page provide the following automatic MACC disk cleanup configuration options:

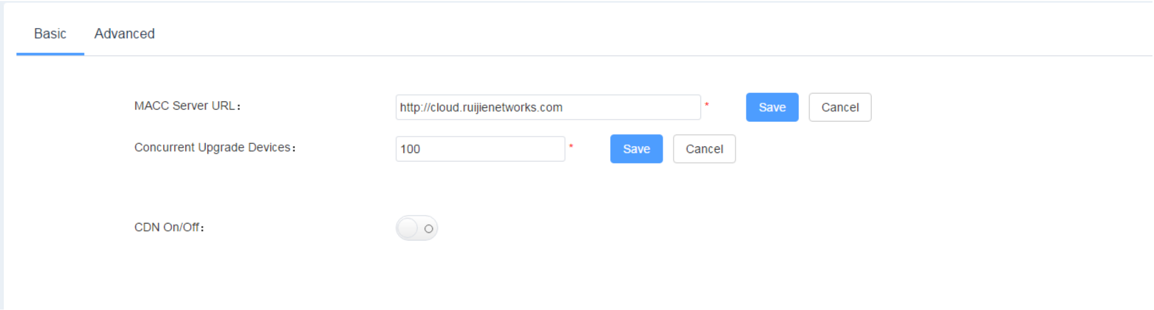
- Disk cleanup Email address(CC address)
- Disk cleanup Email address(receiver address)
- Roaming Log Storage Interval (Days)
- Experience Data Storage Interval(Days)
- Raw Experience Data Storage Interval(Days)
- Daily Use Data Storage Interval (Days)

7 System

7.1 System Settings

Click ⚙ in the upper right corner and select **System Settings**. The **System Settings** page is displayed, and allows you to configure system parameters on the **Basic** and **Advanced** pages.

7.1.1 Basic Settings



MACC Server URL: http://cloud.ruijienetworks.com *

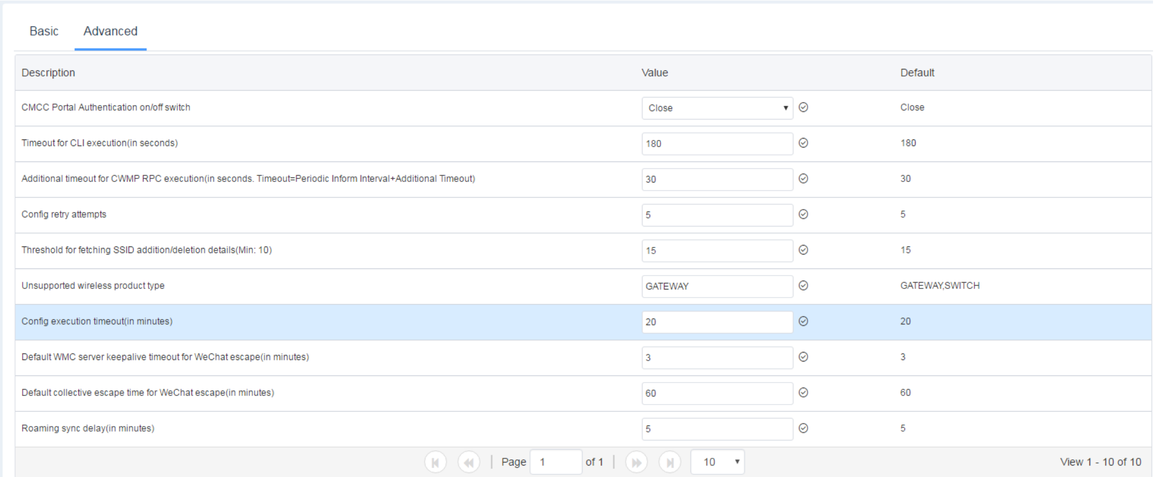
Concurrent Upgrade Devices: 100 *

CDN On/Off: ○

Three configuration items are displayed on the **Basic** page, as listed in the following figure.

Parameter	**Description**	**Default Value**
MACC Server URL	Specifies the MACC server address, which must be specified again during initial deployment or after the server IP address is changed.	http://127.0.0.1:80 This parameter must be changed to the actual server address during initial deployment.
Concurrent Upgrade Devices	Specifies the maximum number of devices that can be simultaneously upgraded.	20
CDN On/Off	Specifies the CDN switch.	Off
CDN Download URL	Specifies the address of the upgrade download server, which can be set to the CDN server address.	http://127.0.0.1:80 If **CDN On/Off** is enabled, this parameter must be correctly specified.

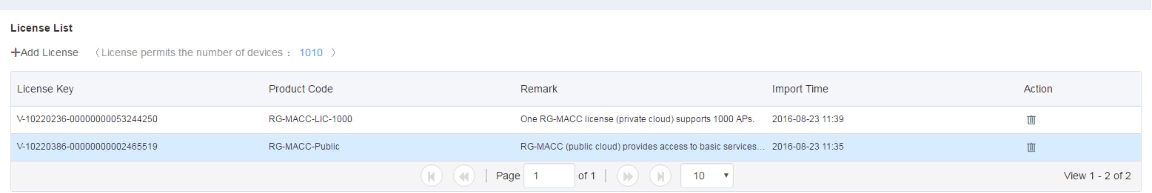
7.1.2 Advanced Settings



Description	Value	Default
CMCC Portal Authentication on/off switch	Close	Close
Timeout for CLI execution(in seconds)	180	180
Additional timeout for CWMP RPC execution(in seconds. Timeout=Periodic Inform Interval+Additional Timeout)	30	30
Config retry attempts	5	5
Threshold for fetching SSID addition/deletion details(Min: 10)	15	15
Unsupported wireless product type	GATEWAY	GATEWAY,SWITCH
Config execution timeout(in minutes)	20	20
Default WMC server keepalive timeout for WeChat escape(in minutes)	3	3
Default collective escape time for WeChat escape(in minutes)	60	60
Roaming sync delay(in minutes)	5	5

7.2 License Configuration

Click ⚙ in the upper right corner, and select **License**. This **License List** page is displayed, and allows you to add a license.



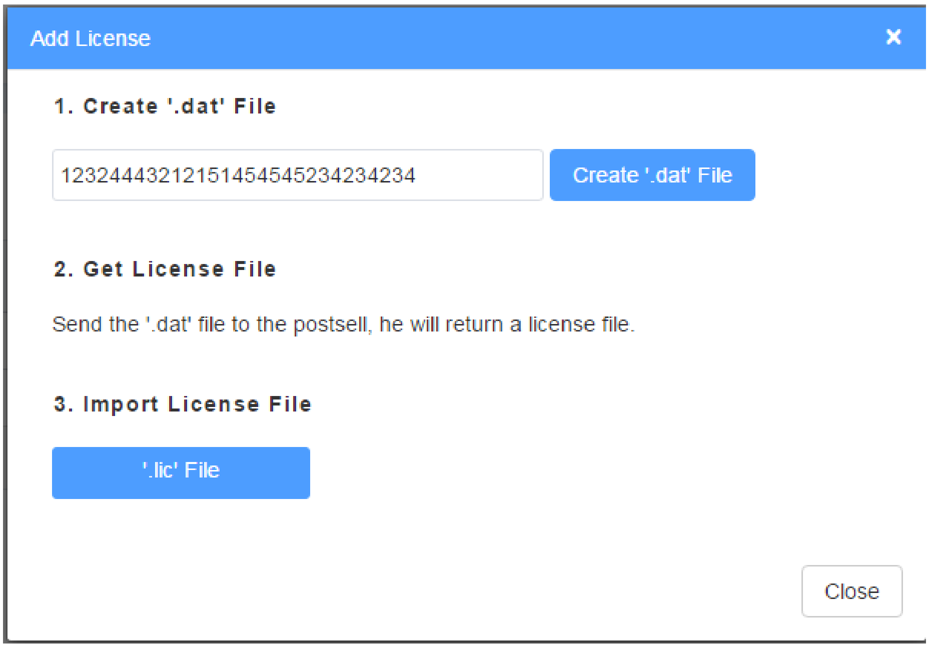
License List

License Key	Product Code	Remark	Import Time	Action
V-10220236-00000000053244250	RG-MACC-LIC-1000	One RG-MACC license (private cloud) supports 1000 APs.	2016-08-23 11:39	🗑
V-10220386-00000000002465519	RG-MACC-Public	RG-MACC (public cloud) provides access to basic services...	2016-08-23 11:35	🗑

7.2.1 Adding Licenses

By default, the system allows you to manage ten devices, and you can add a license as follows:

1. Click **+Add License**.
2. Enter the authorization code, and click **Create '.dat' File** to download the .dat file.
3. Send the .dat file to the after-sales service personnel to generate a license file.
4. Import the license file.



1. Create '.dat' File

12324443212151454545234234234

2. Get License File

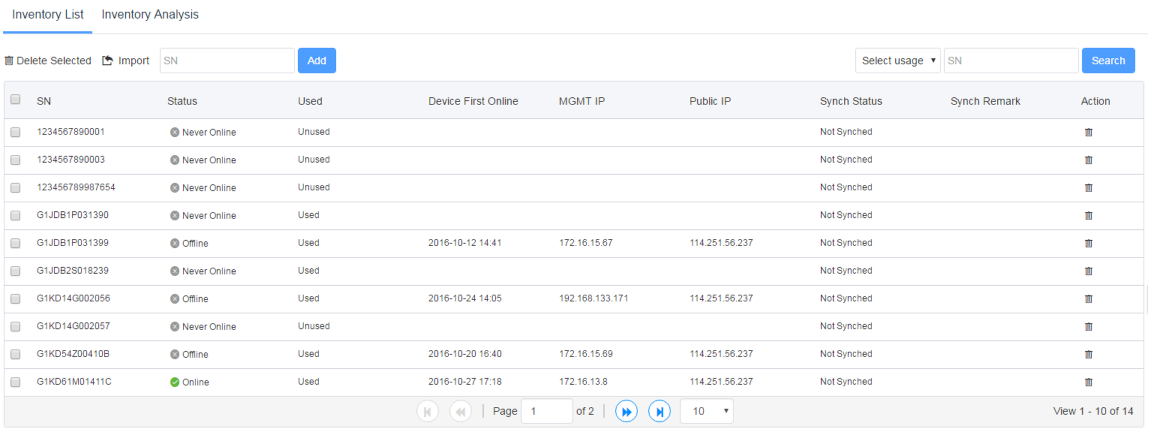
Send the '.dat' file to the postsell, he will return a license file.

3. Import License File

7.3 Inventory Management

Move the cursor to ⚙ in the upper right corner and select **Inventory** to display the inventory management page. On the inventory management page, inventory management and undeployed inventory analysis can be performed.

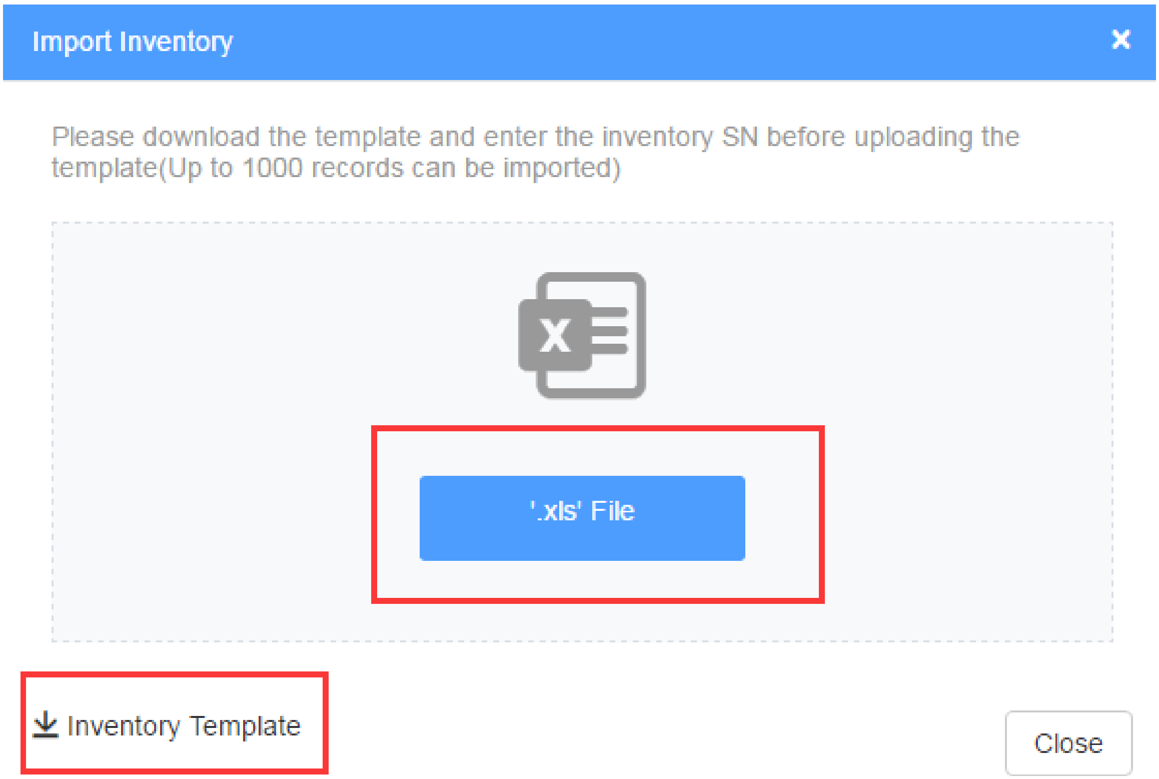
7.3.1 Inventory List



□	SN	Status	Used	Device First Online	MGMT IP	Public IP	Synch Status	Synch Remark	Action
□	1234567890001	Never Online	Unused				Not Synched		🗑
□	1234567890003	Never Online	Unused				Not Synched		🗑
□	123456789987654	Never Online	Unused				Not Synched		🗑
□	G1JDB1P031390	Never Online	Used				Not Synched		🗑
□	G1JDB1P031399	Offline	Used	2016-10-12 14:41	172.16.15.67	114.251.56.237	Not Synched		🗑
□	G1JDB2S018239	Never Online	Used				Not Synched		🗑
□	G1KD14G002056	Offline	Used	2016-10-24 14:05	192.168.133.171	114.251.56.237	Not Synched		🗑
□	G1KD14G002057	Never Online	Unused				Not Synched		🗑
□	G1KD54Z00410B	Offline	Used	2016-10-20 16:40	172.16.15.69	114.251.56.237	Not Synched		🗑
□	G1KD61M01411C	Online	Used	2016-10-27 17:18	172.16.13.8	114.251.56.237	Not Synched		🗑

On the **Inventory List** page, **SN**, **Status**, **Used**, **Device First Online**, **MGMT IP**, **Public IP**, **Synch Status**, and **Synch Remark** about inventories are provided. In the upper part, **Deleted Selected**, **Import**, **Add**, and search criteria are provided.

Click Import . The **Import Inventory** dialog box is displayed, as shown in the following figure. Click **Inventory Template** in the lower left corner to download an inventory template and fill inventory information to be imported in batches based on the template. Click **'.xls' File** and select the inventory template with the inventory information filled for import.



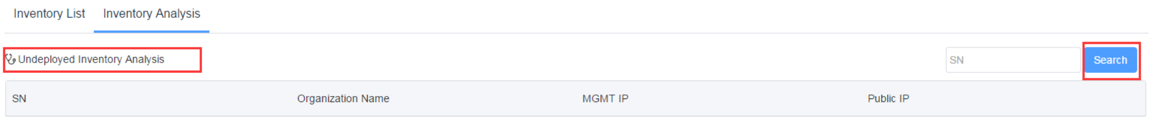
Import Inventory

Please download the template and enter the inventory SN before uploading the template(Up to 1000 records can be imported)

7.3.2 Inventory Analysis

The **Inventory Analysis** page is used to analyze information about deployed and undeployed inventories in the inventory list and provide the possible organization to which undeployed inventories belong.

Click **Inventory Analysis** to display the **Inventory Analysis** page, as shown in the following figure.

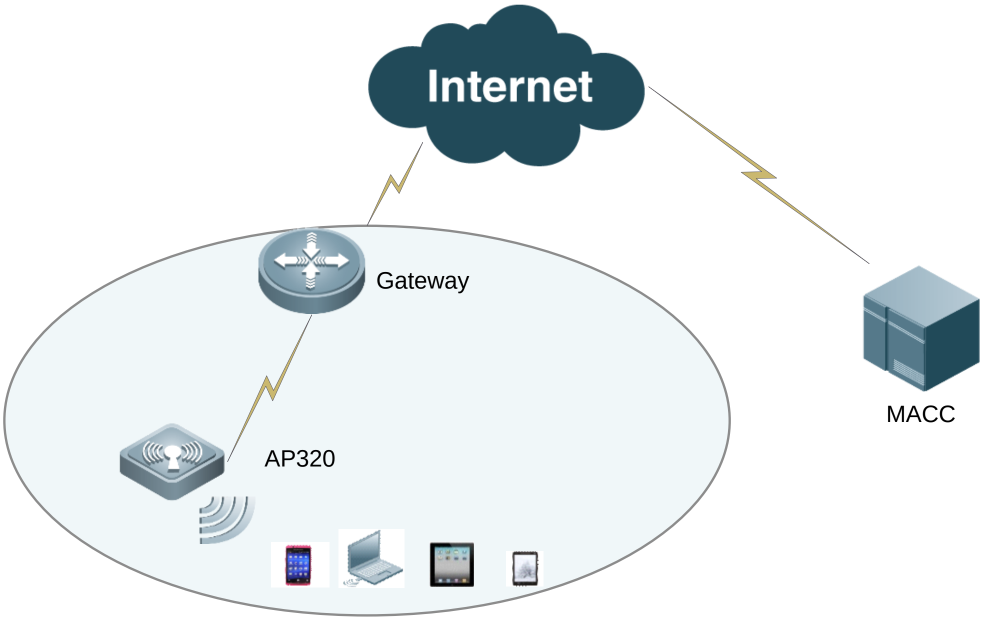


SN	Organization Name	MGMT IP	Public IP

Click **Undeployed Inventory Analysis** to obtain the inventory analysis result. Click **Search** in the upper right corner to obtain the inventory analysis list. **SN**, **Organization Name**, **MGMT IP**, and **Public IP** are displayed for undeployed inventories by organization.

8 Application Examples

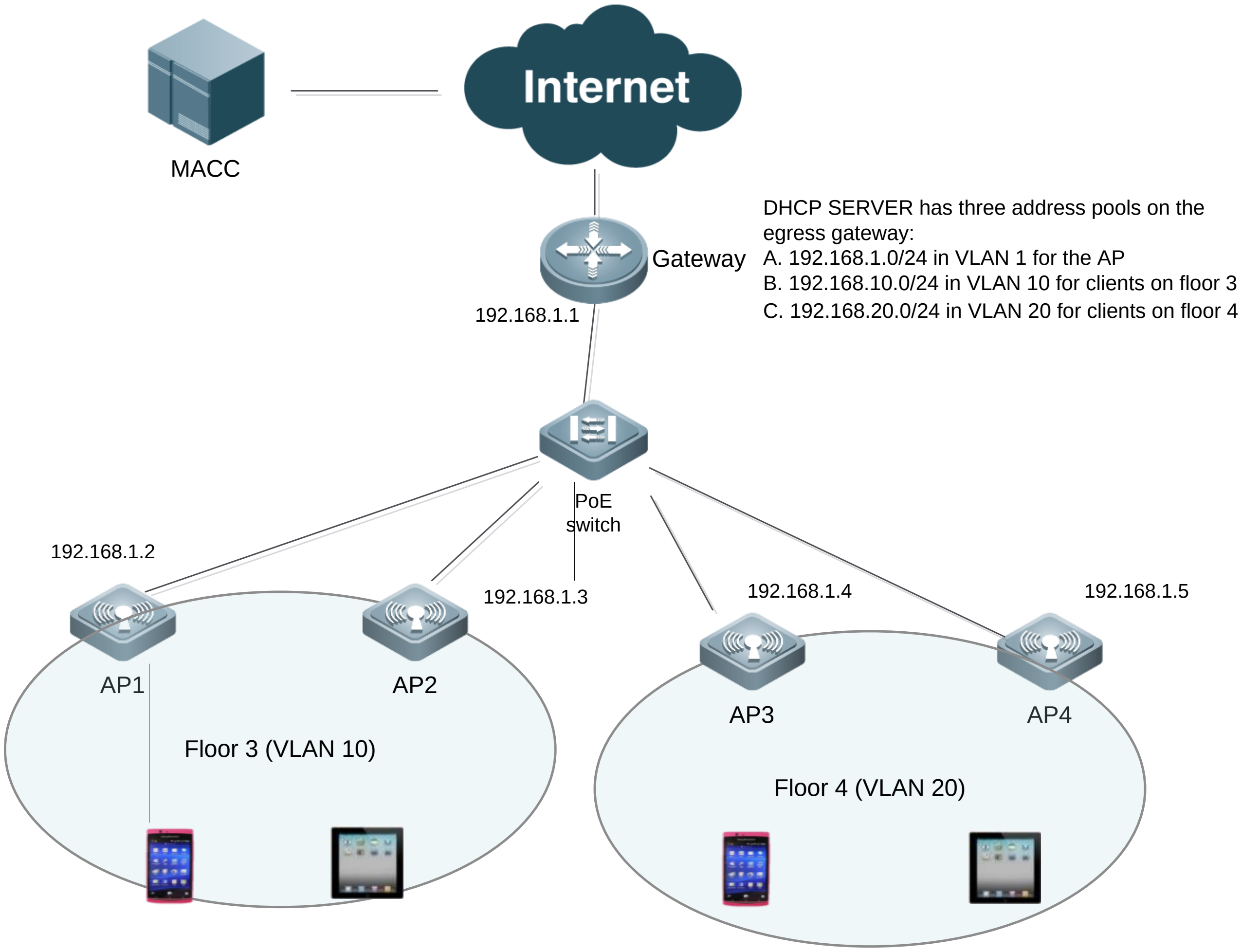
This chapter introduces how to quickly connect AP320 to the MACC, and use the MACC to manage AP320 to emit WiFi signals. For example, to deploy an organization for a new branch, a WiFi network with the SSID of "MACC-RUIJIE" is provided for staffs. The WiFi network is encrypted in wpa2-psk mode, with a password 12345678 and a rate limit 100 Kbps for a connected client.



8.1 Wireless Roaming

Organization implementation refers to the implementation process of a single organization after the cloud controller is deployed.

For example, to deploy an organization for a new branch, a WiFi network with the SSID "MACC-RUIJIE" is provided for external personnel for free. The WLAN for clients on floor 3 is divided into VLAN 10, and the WLAN for clients on floor 4 is divided into VLAN 20. The roaming function is supported, and the uplink and downlink rates of all clients are limited to 100 Kbps.


MACC
Internet
Gateway
192.168.1.1
DHCP SERVER has three address pools on the egress gateway:
A. 192.168.1.0/24 in VLAN 1 for the AP
B. 192.168.10.0/24 in VLAN 10 for clients on floor 3
C. 192.168.20.0/24 in VLAN 20 for clients on floor 4
PoE switch
192.168.1.2
192.168.1.3
192.168.1.4
192.168.1.5
AP1
AP2
AP3
AP4
Floor 3 (VLAN 10)
Floor 4 (VLAN 20)

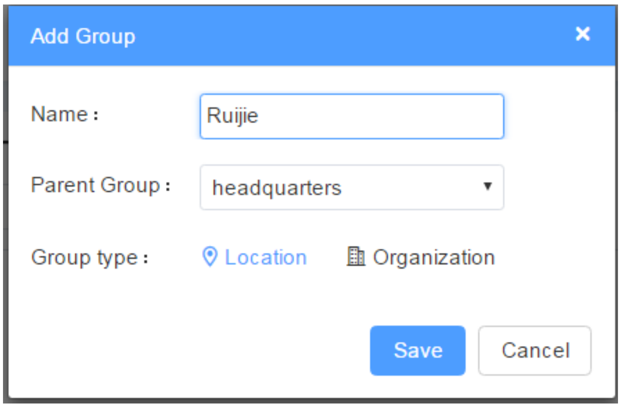
The procedure includes six steps.

8.1.1 Adding Organizations

Organization planning is realized using **Location, Organization**, and **Floor**.

- Location

1. Choose **Planning** > **Locations**.
2. On the navigation tree on the left, click **+** in the first row to add a group.
3. Enter a group name in **Name**, and select **Location** in **Group type**, as shown in the following figure.


Add Group ×

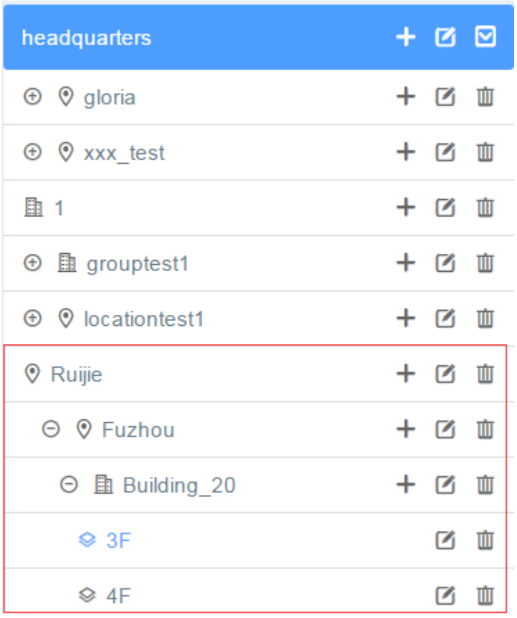
Name : Ruijie

Parent Group : headquarters ▾

Group type : Location Organization

4. Click **Save**.

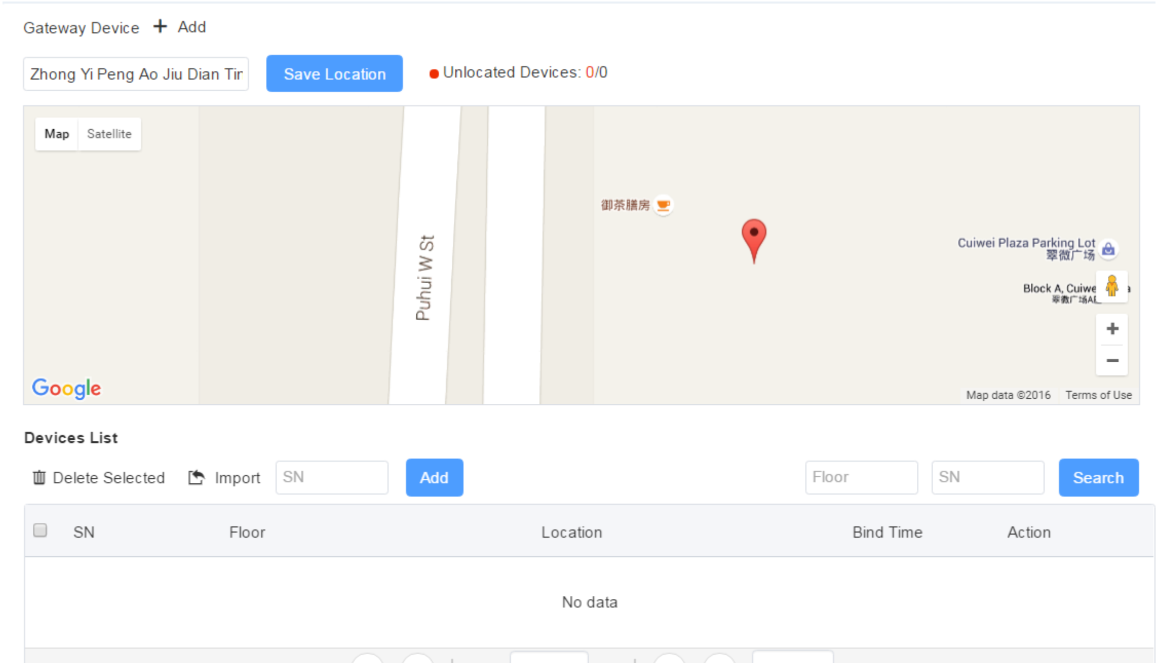
You can add more groups according to this method, as shown in the following figure.



headquarters
gloria
xxx_test
1
grouptest1
locationtest1
Ruijie
Fuzhou
Building_20
3F
4F

5. Select **Building_20**, and click **Add Location** on the right area to display a map.

6. Enter a location name in the search box, select the location marked by 📍 on the map, and then click **Save Location**.



Gateway Device + Add

Zhong Yi Peng Ao Jiu Dian Tir | Save Location | ● Unlocated Devices: 0/0

Devices List

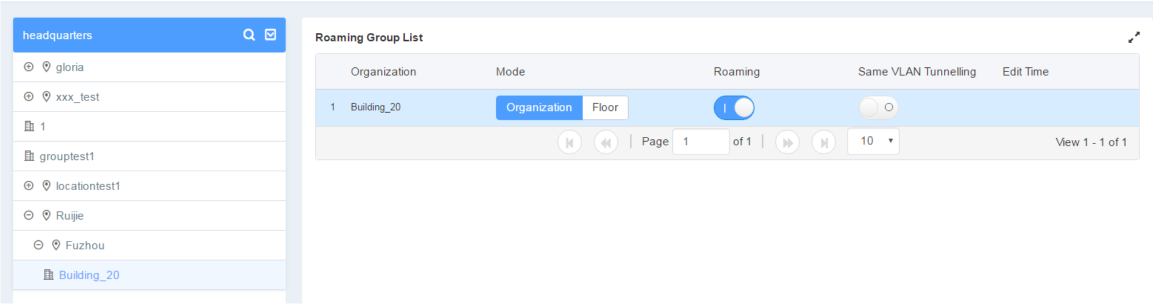
Delete Selected | Import | SN | Add | Floor | SN | Search

□	SN	Floor	Location	Bind Time	Action
			No data		

8.1.2 Enabling Organization Roaming Function

1. Choose **Planning** > **Roaming**.

2. Select **Building_20**.



headquarters

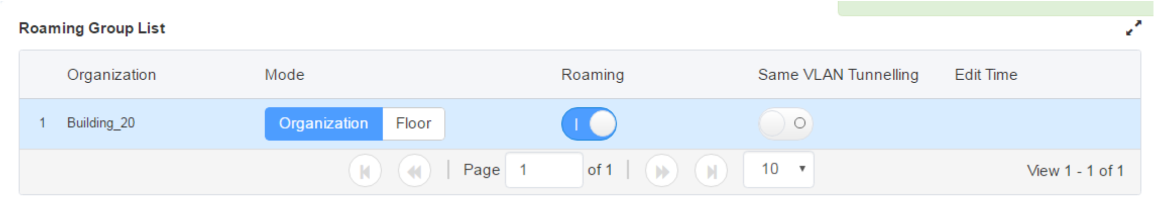
- gloria
- xxx_test
- 1
- grouptest1
- locationtest1
- Ruijie
  - Fuzhou
    - Building_20

Roaming Group List

	Organization	Mode	Roaming	Same VLAN Tunnelling	Edit Time
1	Building_20	Organization / Floor	I	○	

Page 1 of 1 10 View 1 - 1 of 1

3. Enable the roaming function for this organization.



Roaming Group List

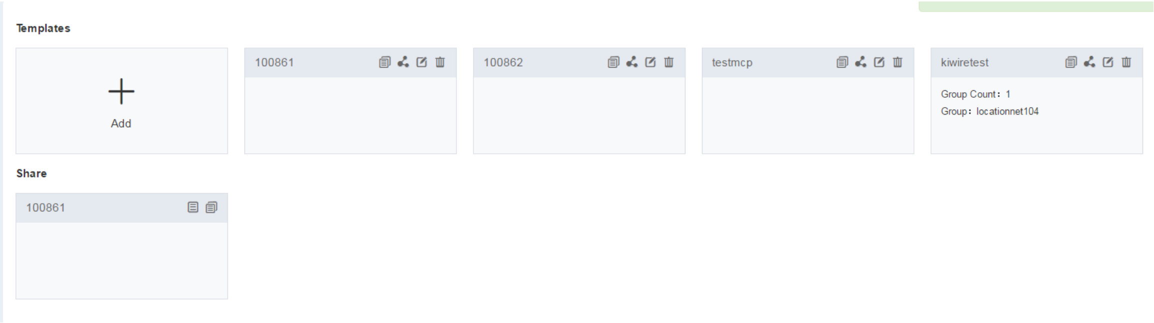
	Organization	Mode	Roaming	Same VLAN Tunnelling	Edit Time
1	Building_20	Organization / Floor	I	○	

Page 1 of 1 10 View 1 - 1 of 1

8.1.3 Organization Configurations

8.1.3.1 Adding Templates

1. Choose **Configuration** > **Templates**.



Templates

+ Add

100861

100862

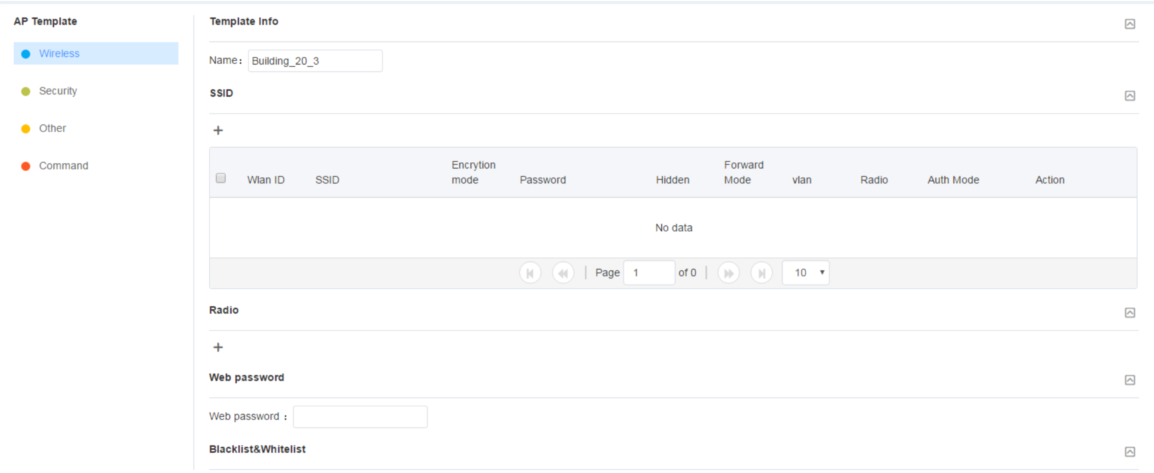
testmcp

kiwiretest
Group Count: 1
Group: locationnet104

Share

100861

2. Click **Add** to add the **Building_20_3** template.



AP Template

- Wireless
- Security
- Other
- Command

Template Info

Name: Building_20_3

SSID

+

□	Wlan ID	SSID	Encrytion mode	Password	Hidden	Forward Mode	vlan	Radio	Auth Mode	Action

No data

Page 1 of 0 10

Radio

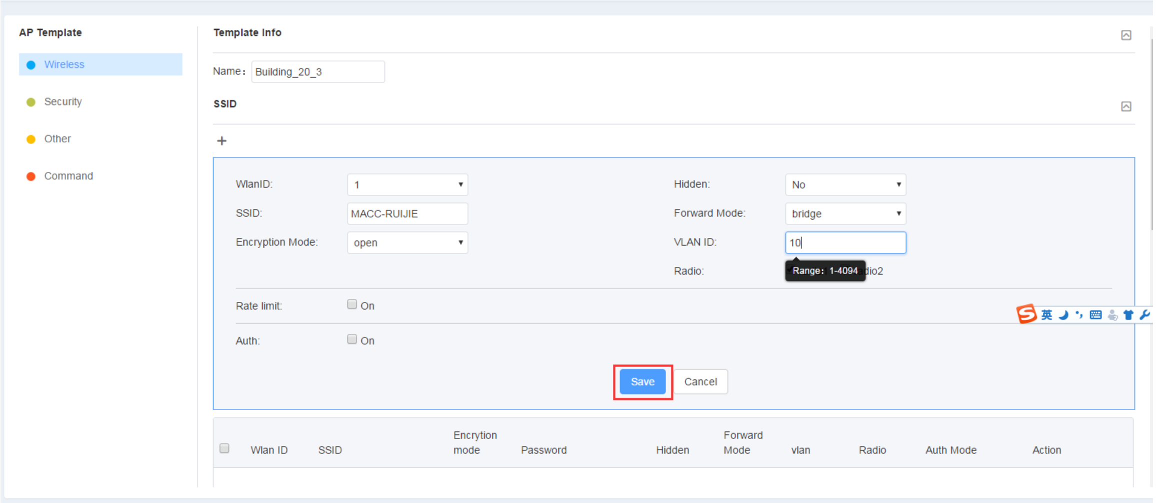
+

Web password

Web password :

Blacklist&Whitelist

3. Click **+** under **SSID**, enter **MACC-RUIJIE** in the **SSID** text box, set **Forward Mode** to **bridge**, set **VLAN ID** to **10**, set **Rate limit** to 100 Kbps, and click **Save**.



Name：Building_20_3

WlanID: 1

SSID: MACC-RUIJIE

Encryption Mode: open

Hidden: No

Forward Mode: bridge

VLAN ID: 10

Range：1-4094

Radio:

Rate limit: □ On

Auth: □ On

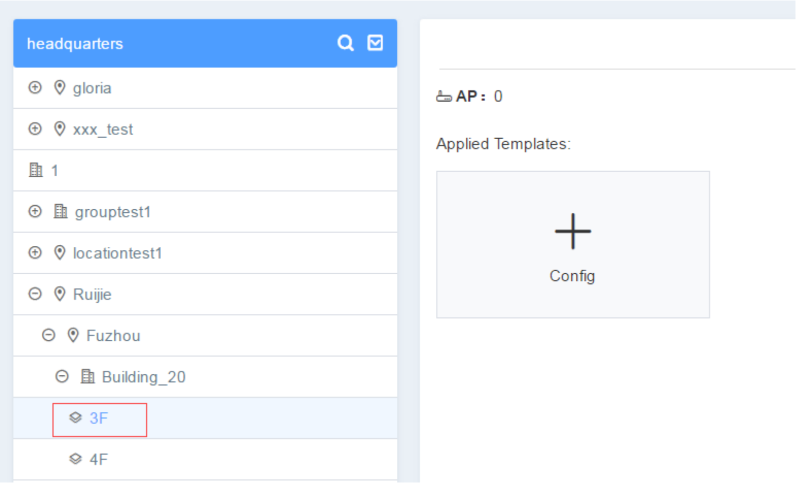
□	Wlan ID	SSID	Encrytion mode	Password	Hidden	Forward Mode	vlan	Radio	Auth Mode	Action

4. Add the **Building_20_4** template with VLAN ID 20 according to the same method.

8.1.3.2 Applying Configurations

1. Choose **Configuration** > **Settings**.

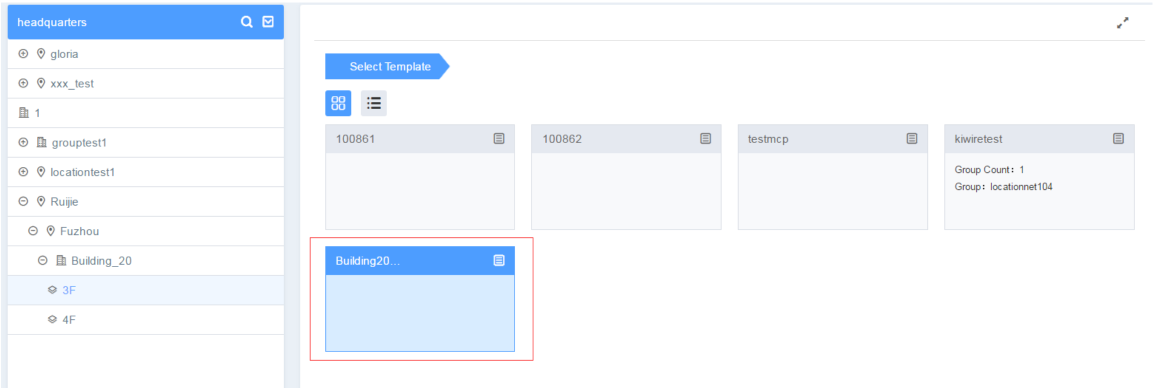
2. Select the **3F** group on the left.



AP： 0

Applied Templates:

3. Click **Config**, select the **Building_20_3** template and click **Save**.



Group Count：1

Group：locationnet104

4. Bind the **4F** group to the **Building_20_4** template.

8.1.4 Importing APs

Bind AP1 and AP2 to the **3F** group, and bind AP3 and AP4 to the **4F** group.

8.1.5 APs Online

Gateway configuration

Add the AP address pool 192.168.1.0/24.

Floor 3 client address pool: 192.168.10.0/24; gateway: 192.168.10.1; VLAN: 10

Floor 4 client address pool: 192.168.20.0/24; gateway: 192.168.20.1; VLAN: 20

PoE switch configuration

On the port through which the PoE switch is connected to the AP, configure a trunk port with the native ID set to 1 by default, and add VLAN 10 and VLAN 20.

8.1.6 Verification

8.1.6.1 Connecting to WiFi Signals

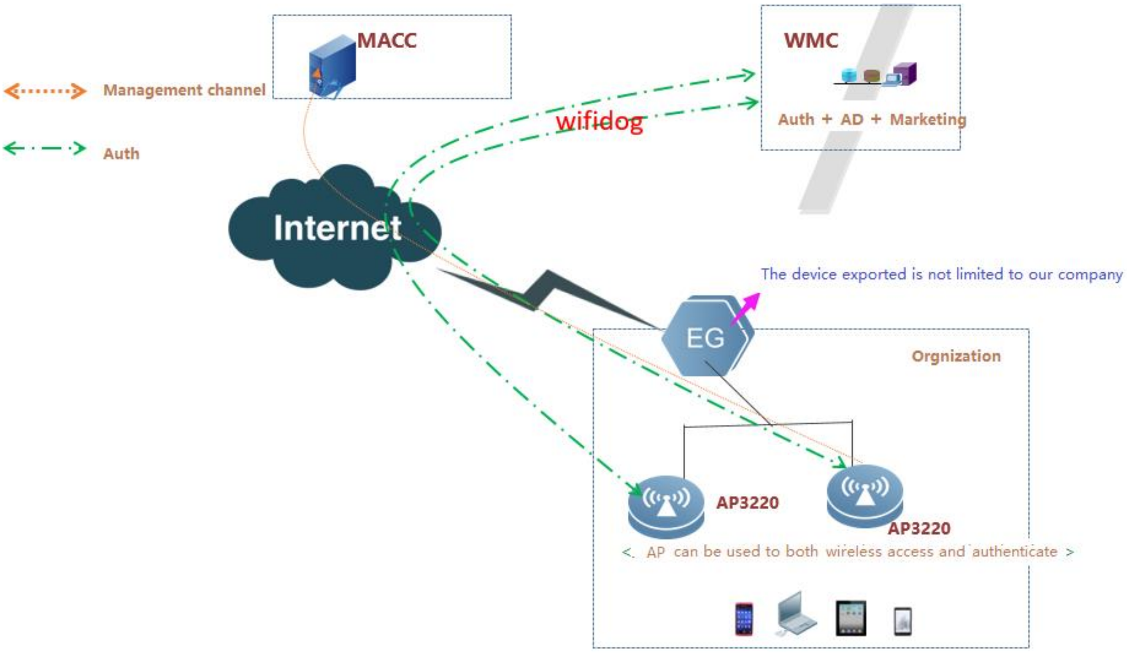
Connect a mobile phone to the WiFi network properly for Internet access.

8.1.6.2 Testing Wireless Roaming

Connect a mobile phone to with the WiFi network “MACC-RUIJIE”, and go upstairs from floor 3 to floor 4. Reconnection and Internet access failure do not occur.

8.2 Authentication Scheme

8.2.1 WiFiDog


MACC
WMC
Management channel
Auth
wifidog
Auth + AD + Marketing
Internet
The device exported is not limited to our company
EG
Orgnization
AP3220
AP3220
<. AP can be used to both wireless access and authenticate >

Third-party authentication servers adopt the WiFiDog protocol for authentication. Ruijie industrial APs interconnect with the third-party authentication servers based on the WiFiDog protocol.

You must learn about the interconnection protocol adopted by third-party authentication server for evaluation and confirmation by the R&D personnel before interconnecting with the third-party authentication servers.

9 Appendix

9.1 Acronyms and Abbreviations

Acronyms and Abbreviations	Full Name
MACC	Mobile Access Cloud Center
AP	Access Point
STA	Station
AC	Access Controller
BOSS	Business & Operation Support System
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
EAP	Extensible Authentication Protocol
EAPOL	EAP Over Lan
EAP AKA	Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement
ESSID	Extended Service Set Identification
FTP	File Transfer Protocol
HLR/AuC	Home Location Register
HTTP	Hypertext Transfer Protocol
IMSI	International Mobile Subscriber Identification
MSISDN	Mobile Subscriber ISDN
NAT	Network Address Translation
PAT	Port Address Translation
Radius	Remote Authentication Dial In User Service
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
UDP	User Datagram Protocol
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WAPI	Wireless LAN Authentication and Privacy Infrastructure
WLAN	Wireless Local Access Network

9.2 Glossary

Term	Explanation
Cloud	Specifies the cloud center management end, supports private clouds and public clouds, allows separate deployment of a system of a private cloud version, and also provides cloud services of the public cloud version.
Group	Enables devices grouping for ease of management on a large quantity of devices. It is recommended that groups be added by geographical location or device use.

9.3 Relevant Documents

Document	Main Content
MACC Datasheet	Introduces functional features, parameters, and operating environment of the MACC.
MACC Release Notes	Describes information about the released version and functional limitations.
MACC Quick Setup Guide	Describes how to associate an AP with the MACC and set up wireless networks.
MACC Installation Guide	Describes the MACC installation process.

9.4 FAQ

- N/A