RG-MACC-BASE

Cookbook V1.0

Preface

Thank you for using our products.

Audience

This manual is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Symbols

Important information. Contains helpful suggestions or references.

Use caution. Could result in equipment damage or data loss.

1. Contents

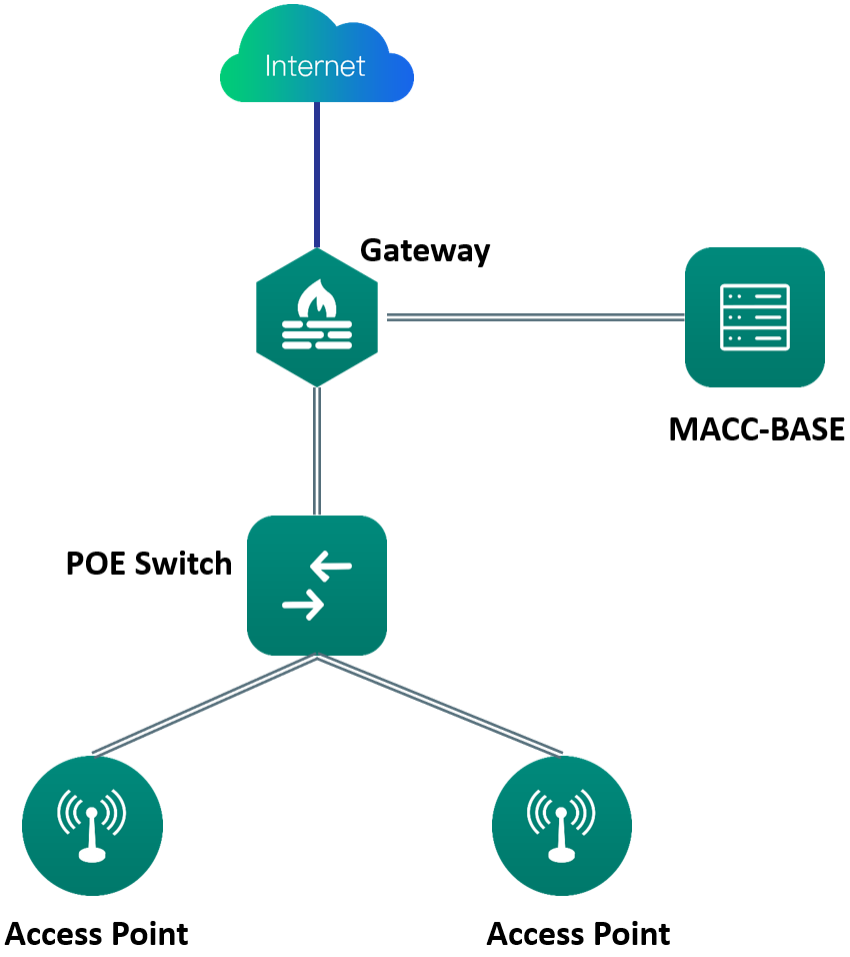
2. Software Introduction

2.1. Overview

The Ruijie RG-MACC (Managed @ Cloud Center) is a revolutionary cloud management platform which supports unified management and configuration of APs, switches and gateway devicess as well as value-added marketing features, site survey, etc.

The RG-MACC-BASE is a key component of the RG-MACC, supports device planning, configuration, control, operation and maintenance on cloud, which provides an easy solution to centrally manage all the Wi-Fi devices.

3. Network Topology Requirements



- MACC-BASE server with enough AP count license
- A DHCP-enabled network (so any device can obtain an IP address)
- Model of Access Point can support MACC-BASE since AP version B9P5
- Connectivity between the Access Point to MACC-BASE server

4. Hardware Supported

Product Type	Product Series	Hardware Model	Minimum Version Required
Access Point	AP130 Series	AP130(W2) , AP130(L)	AP_RGOS 11.1(5)B9P2 AP_RGOS 11.1(5)B9P5
	AP520 Series	AP520-I, AP520, AP520(BT), AP520(DA), AP520-I(G2), AP520(W2)	AP_RGOS 11.1(5)B9P2 AP_RGOS 11.1(5)B9P5
	AP630 Series	AP630(IDA) , AP630(IODA), AP630(CD)	AP_RGOS 11.1(5)B9P2 AP_RGOS 11.1(5)B9P5
	AP720 Series	AP720-I	AP_RGOS 11.1(5)B9P2 AP_RGOS 11.1(5)B9P5
	AP740 Series	AP740-I	AP_RGOS 11.1(5)B9P2 AP_RGOS 11.1(5)B9P5
MTFI	M520 Series	RG-MTFi-M520(IZEAA), RG-MTFi-M520(ILEAA)	MTFI_3.0(1)B3_MTFI-M520-RLIF
Switch	RG-S2910	RG-S2910-24GT4SFP-UP-H	S29_RGOS 11.4(1)B12
	RG-S2910C	RG-S2910C-24GT2XS-HP-E	S2910_RGOS 11.4(1)B1P3
	RG-S2928G	RG-S2928G-E V3.0	S29_RGOS 11.4(1)B12

5. Software Installation

RG-MACC-BASE_3.1 supports two installation methods: OVF and ISO.

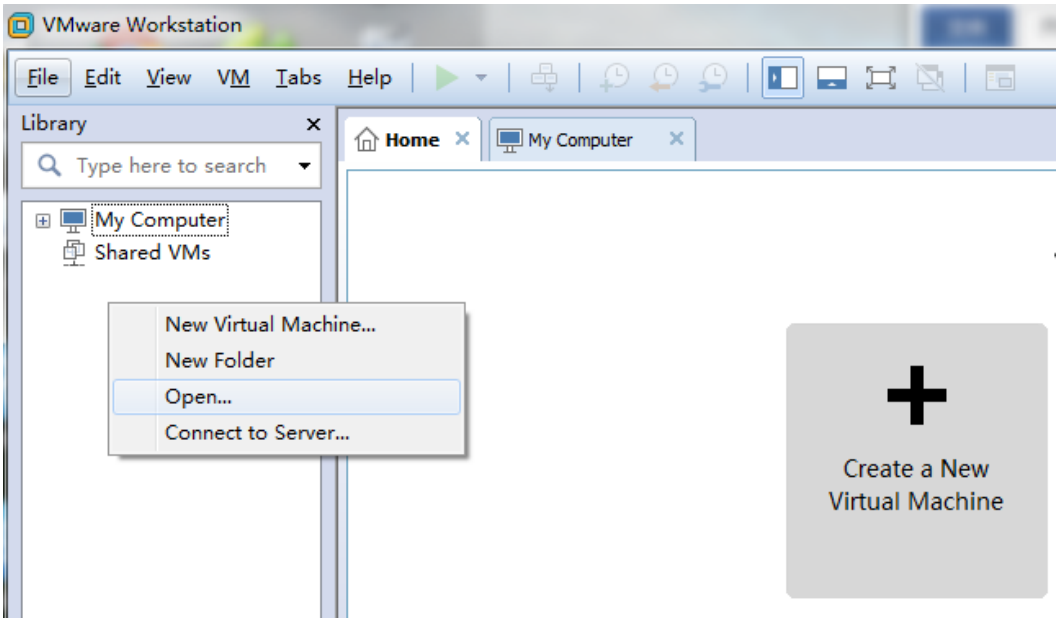
5.1. OVF Install

System Requirements

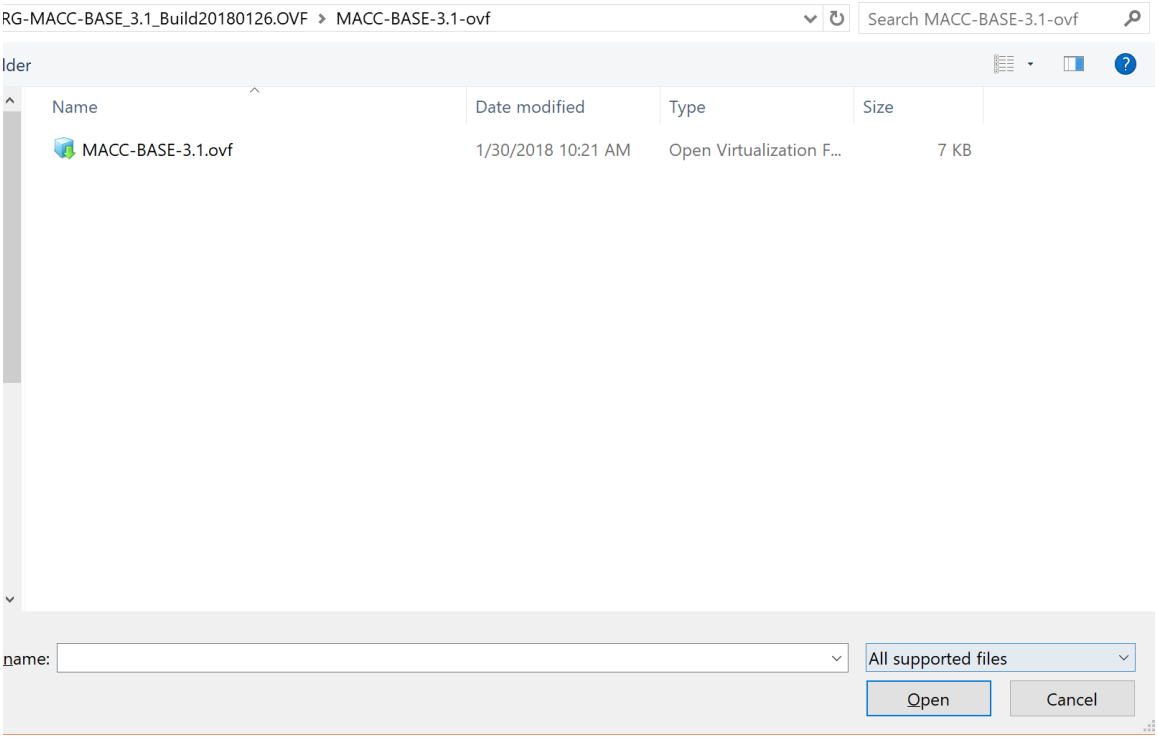
Application	VMware Workstation		
OS	Windows 7 / 8 / 10 (64-bit only) server		
Device Count	< 1000	1000 to 4000	Above 4000
CPU	4 cores 2.0 GHz	8 cores 2.0 GHz	…
RAM	8 GB	16 GB	…
HDD	768GB	1 TB	…
Remark	-	-	Contact Support

Installation Procedures

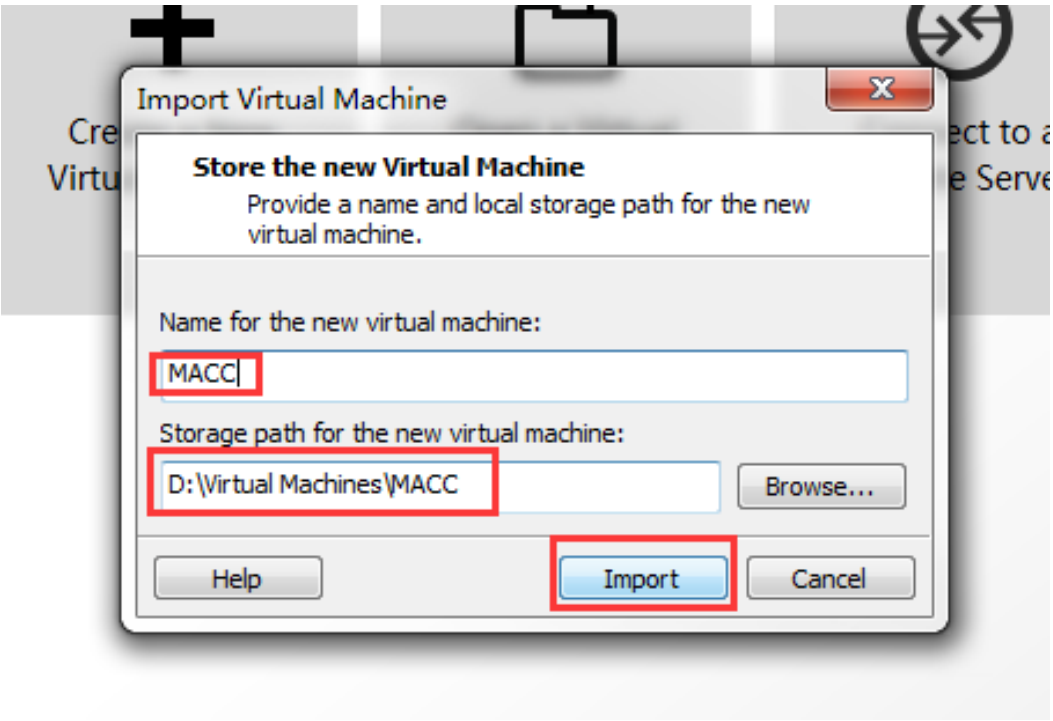
1) Click File > Open



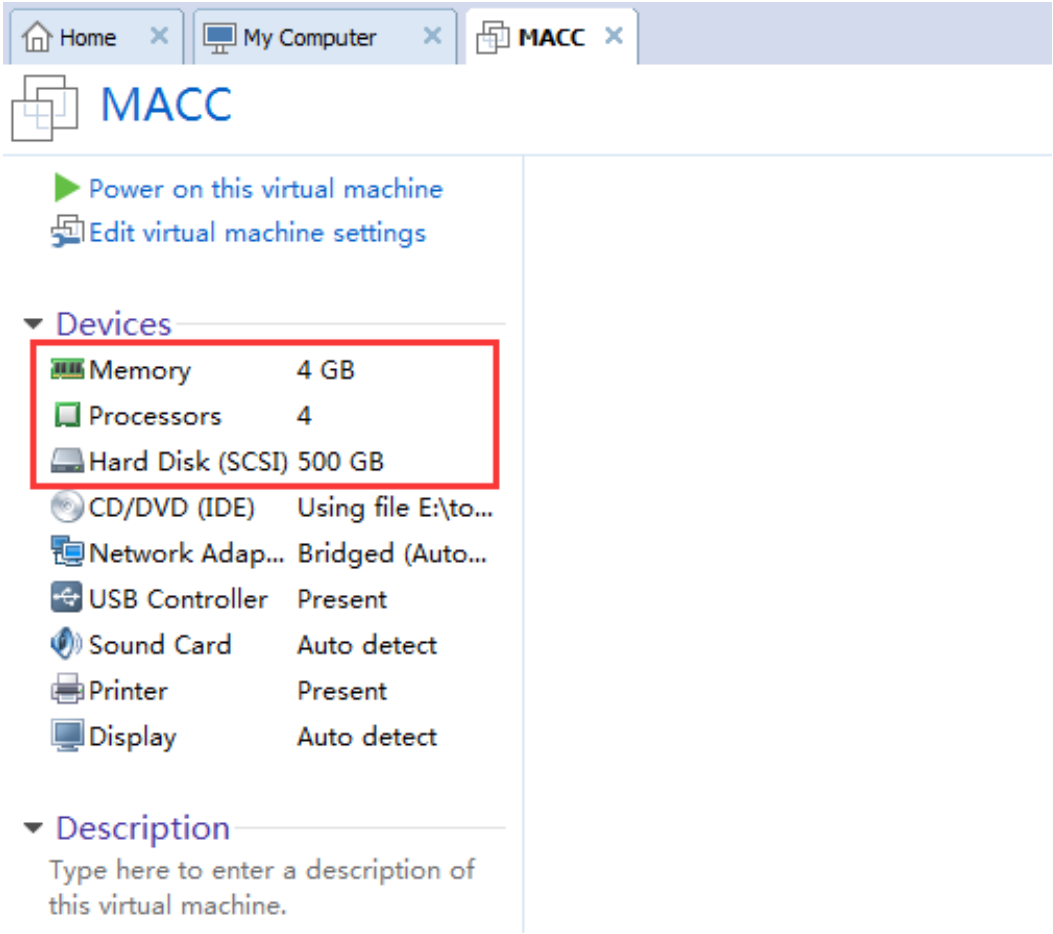
2) Download MACC-BASE image and unzip the OVF file, then Choose OVF format file on VMware.



3) Set a name and storage path for the virtual machine.



4) Set the hardware parameter according to your requirements.

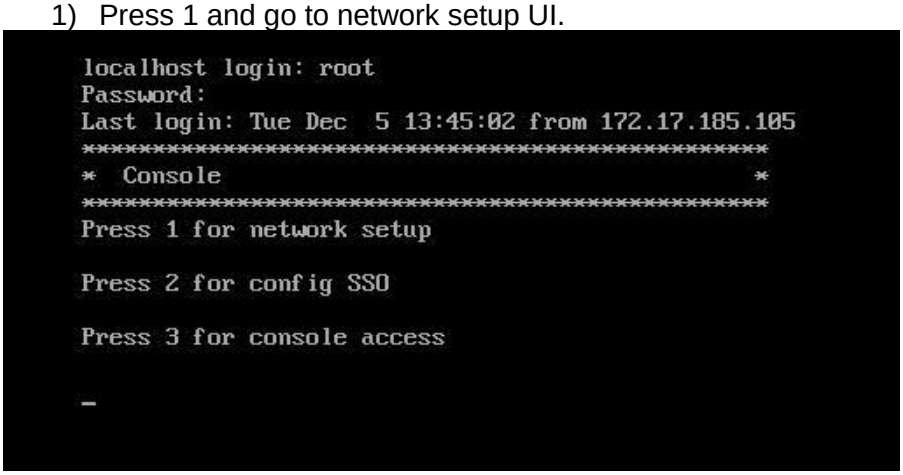


5) After installation, user can login system console by using account: root/ruijie.

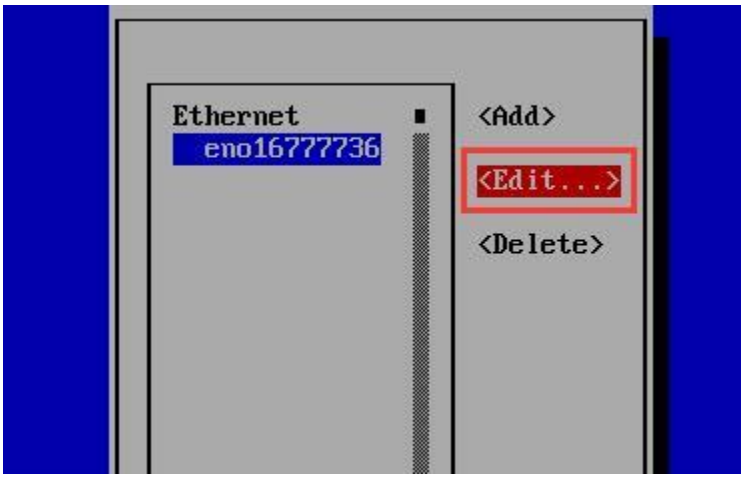
Advanced Setting-Network Setup

It provides a quick access to Network Manager UI for modifying the system IP address, DNS and so on.

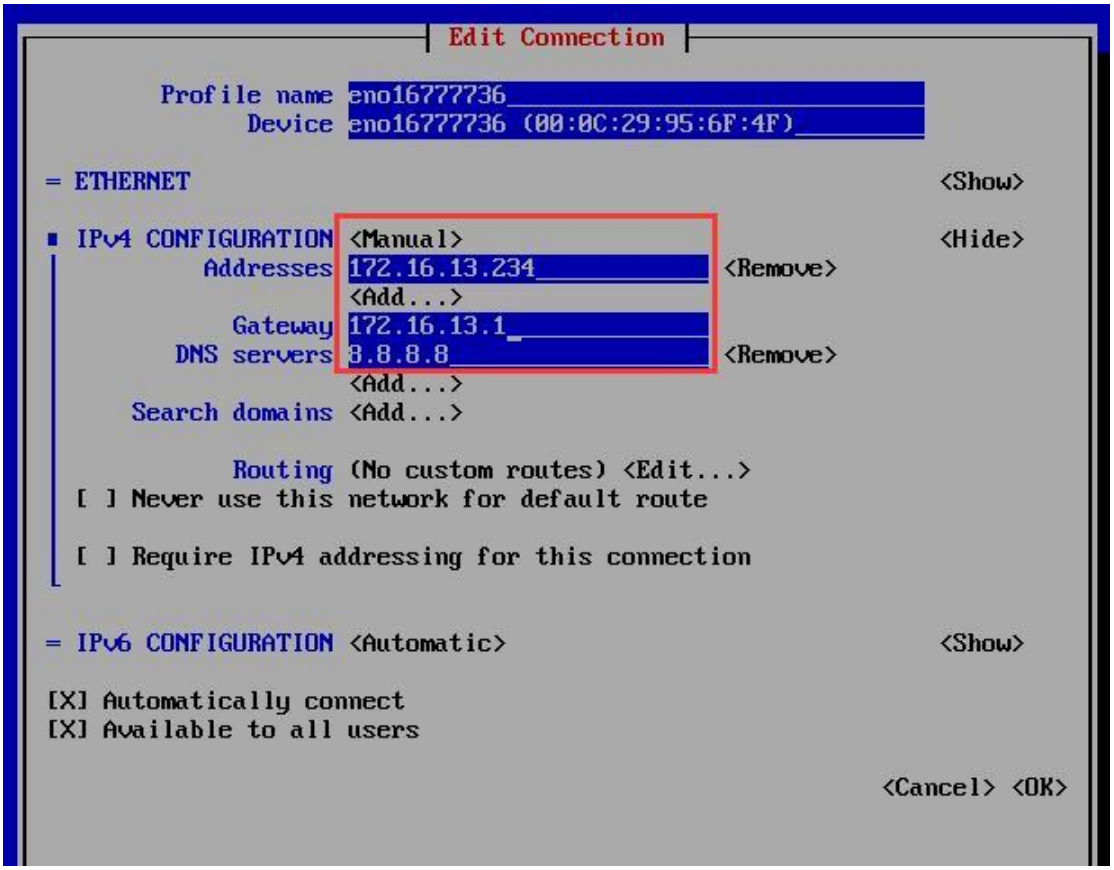
1) Press 1 and go to network setup UI.



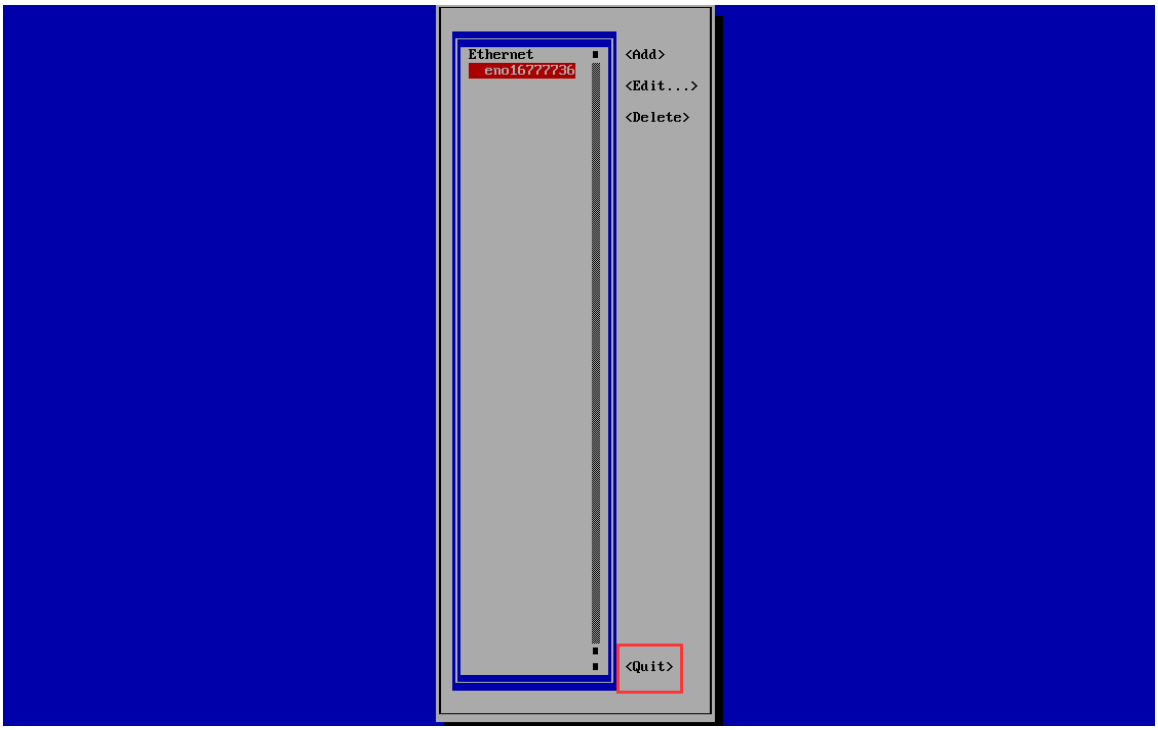
2) Select “Edit a connection” and Choose Edit.



3) Input the related Ethernet parameters base on network design.



4) Choose “OK” and “Quit” the Network Manager page.



Advanced Setting-SSO Setting

The MACC-BASE enabled SSO and only allow the user accesses the service from unique IP address, admin user can disable or change the SSO IP/URL by following setting.

1) Press 2 to modify the SSO setting

```
localhost login: root
Password:
Last login: Tue Dec  5 13:45:02 from 172.17.185.105
*************************************************
*  Console                                      *
*************************************************
Press 1 for network setup

Press 2 for config SSO

Press 3 for console access

-
```

2) Modify SSO setting by following the prompt.

```
config SSO...
If you want to open SSO, Please enter "y", else enter "n" not use SSO, Cancel enter other letter.
y
Please enter ip:
172.16.13.234
Please enter port (default 80):
80
config SSO success.
restart tomcat
Using CATALINA_BASE:   /macc/install/tomcat
Using CATALINA_HOME:   /macc/install/tomcat
Using CATALINA_TMPDIR: /macc/install/tomcat/temp
Using JRE_HOME:        /usr/lib/jvm/jdk8/jre
Using CLASSPATH:       /macc/install/tomcat/bin/bootstrap.jar:/macc/install/tomcat/bin/tomcat-juli.jar
Tomcat started.
[root@localhost ~]#
```

5.2. ISO Install

➢ System Requirements

⚠ The following table lists the minimum hardware and operating system configuration requirements:

Device Count	< 1000	1000 to 4000	Above 4000
CPU	4 cores 2.0 GHz	8 cores 2.0 GHz	…
RAM	8 GB	16 GB	…
HDD	256GB	512GB	…
Bandwidth (AP Connection)	10Mbps	10Mbps	…
Remark	-	-	Contact Support
Operation System	CentOS-7-x86_64-Minimal-1511.iso Download URL: http://vault.centos.org/7.2.1511/isos/x86_64/		

⚠ If the hardware cannot meet the requirements, the server may not work.

⚠ Port mapping (This requirement can be skipped if servers use public network IP addresses):

Ensure below port numbers are accessible and not be blocked by security equipment:

Internal Port	External Port	Protocol	Mandatory or Optional	Remarks
Port 80	Custom	TCP	Mandatory	HTTP access port
Port 443	Custom	TCP	Optional	HTTPS access port
Port 3478	Port 3478(Fixed)	UDP	Mandatory	For device interaction and Stun learning
Port 3479	Port 3479(Fixed)	UDP	Mandatory	For device interaction and STUN learning
Port 22	Custom	TCP	Optional	Secure shell (SSH) remote login port for the MACC-BASE server. Do not use Port 22 for mapping. The password for running the operating system must be highly complex to avoid attacks.
Port 8090	Custom	TCP	Optional	MACC-BASE Back-end Management

➢ Disk Partition and Directory Requirements

The **/macc** directory is used for saving both MACC-BASE installation and running data. This directory is required and assigned 200 GB or more space.

⚠ Single mass storage disk

If the operating system has been installed and cannot be partitioned, the **/macc** directory can be created by running the following command:

```
[root@localhost ~]# mkdir /macc
```

⚠ Multiple disks with no data disk mounted (Take the Alibaba Cloud Computing server as an example.)

Usually, the system has two disks: system and data.

To check the disk status, run the **fdisk –l** command:

```
[root@xxxxxxx ~]# fdisk -l

Disk /dev/xvda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00078f9c

      Device Boot      Start         End      Blocks   Id  System
/dev/xvda1     *           1        2611    20970496   83  Linux

Disk /dev/xvdb: 429.5 GB, 429496729600 bytes
255 heads, 63 sectors/track, 52216 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

To check the disk mounting status, run the **df** command:

```
[root@iZ28iclrr63Z ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       20G   2.4G   17G  13% /
/dev/xvdb       394G   275G  100G  74% /macc
```

If the data disk (**/dev/xvdb** in the example above) is not mounted, it needs to be formatted and mounted to **/macc**. The following process is recommended:

```
mkfs -t ext4 /dev/xvdb
mkdir /macc
mount /dev/xvdb /macc
##Modifying /etc/fstab   Automatically mounts the disk upon startup.
vi /etc/fstab           Adding a line at the end.
/dev/xvdb               /macc    ext4    defaults    0    0
/dev/xvdb is added as required. Run the df command for confirmation after restarting the server.
```

⚠ **Multiple disks with the data disk mounted**

It is necessary to create the data disk soft link in **/macc**.

To check the disk mounting status, run the **df** command:

```
[root@iZ28iclrr63Z ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/xvda1       20G   2.4G   17G  13% /
/dev/xvdb       394G   275G  100G  74% /data
```

If the data disk is mounted under the **/data** directory, you need to run the **mkdir/macc** command to create the **/macc** directory. Run the **vi/etc/fstab** command to mount the data disk to **/macc**, and then restart the server.

➢ Changing System Time

1) Run command **timedatectl** to display the current time.

```
[root@localhost ~]# timedatectl
      Local time: Fri 2017-11-24 01:10:24 EST
  Universal time: Fri 2017-11-24 06:10:24 UTC
        RTC time: Fri 2017-11-24 06:10:37
       Time zone: America/New_York (EST, -0500)
     NTP enabled: n/a
NTP synchronized: no
 RTC in local TZ: no
      DST active: no
 Last DST change: DST ended at
                  Sun 2017-11-05 01:59:59 EDT
                  Sun 2017-11-05 01:00:00 EST
 Next DST change: DST begins (the clock jumps one hour forward) at
                  Sun 2018-03-11 01:59:59 EST
                  Sun 2018-03-11 03:00:00 EDT
```

2) Run command **timedatectl set-timezone xxxxxxx** to edit the time zone.

```
[root@localhost ~]# timedatectl set-timezone Asia/Shanghai
[root@localhost ~]# timedatectl
      Local time: Fri 2017-11-24 14:10:55 CST
  Universal time: Fri 2017-11-24 06:10:55 UTC
        RTC time: Fri 2017-11-24 06:11:08
       Time zone: Asia/Shanghai (CST, +0800)
     NTP enabled: n/a
NTP synchronized: no
 RTC in local TZ: no
      DST active: n/a
```

3) Run command **timedatectl set-time "YYYY-MM-DD HH:MM:SS**" to set the time.

```
[root@localhost ~]# timedatectl set-time "2017-11-25 14:44:00"
[root@localhost ~]# timedatectl
      Local time: Sat 2017-11-25 14:44:04 CST
  Universal time: Sat 2017-11-25 06:44:04 UTC
        RTC time: Sat 2017-11-25 06:44:05
       Time zone: Asia/Shanghai (CST, +0800)
     NTP enabled: n/a
NTP synchronized: no
 RTC in local TZ: no
      DST active: n/a
```

⚠ The new time settings will take effect after the system is restarted.

➢ Configuring IP Addresses and DNS Servers

The IP address and DNS server need to be configured before deployment and installation.

Configuring the IP addresses

Run the **ifconfig** command to identify the external network interface:

[root@localhost ~]# ifconfig

```
eth0      Link encap:Ethernet  HWaddr 00:15:5D:5D:27:0B
          inet addr:172.18.33.67  Bcast:172.18.33.255  Mask:255.255.255.0
          inet6 addr: fe80::215:5dff:fe5d:270b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1212674 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1061523 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1133515990 (1.0 GiB)  TX bytes:1032504656 (984.6 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:3407442 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3407442 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:504690004 (481.3 MiB)  TX bytes:504690004 (481.3 MiB)
```

Take eth0 above as an example. Modify ***/etc/sysconfig/network-scripts/ifcfg-eth0***. Assume that the IP address of Port eth0 is 192.168.23.128 and the gateway IP address of Port eth0 is 192.168.23.1.

```
vi  /etc/sysconfig/network-scripts/ifcfg-eth0
```

```
DEVICE=eth0
HWADDR=00:0C:29:1E:A8:FE
TYPE=Ethernet
UUID=af14aac2-b6ab-413a-af07-a1c3f4328391
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=static
IPADDR=192.168.23.128
GATEWAY=192.168.23.1
NETMASK=255.255.255.0
```

Set **ONBOOT** to **yes**, and **BOOTPROTO** to **static**. Add IPADDR (IP address), GATEWAY (gateway), NETMASK (subnet mask), and then restart the server.

Configuring DNS servers

For example, run the following command to add the server with the IP address 8.8.8.8 as a DNS server:

```
echo “nameserver 8.8.8.8”  >> /etc/resolv.conf
```

➢ Uploading MACC-BASE Installation Package

The MACC-BASE installation package is in ISO format. This section describes how to upload the MACC-BASE installation package to the server, run the **mount** command to

mount the installation package to **/mnt/iso**, and to copy the ISO file to the **/mnt/install/** directory.

Using FTP/SFTP Tool

CentOS provides a simple tool that enables users to implement direct interaction between Windows and Linux systems. For details about using the tool, see “SecureFXPortable.exe (File Copy Tool)”.

Copy the ISO file to any directory of the server.

Run the **mount–o loop /directory for storing the upgrade file/file name/mnt/iso** command to mount the ISO file.

For example, to save a file in the **home** directory, run the following command:

```
mkdir /mnt/iso
mount -o loop /home/RG-MACC-BASE_3.1_Build20180126.iso /mnt/iso
```

Next, to copy the ISO file to the **/mnt/install/** directory, run the following command:

```
mkdir /mnt/install
cp -ar /mnt/iso/* /mnt/install/
```

Using a USB Flash Drive

Insert a USB flash drive into the USB port.

Run the **fdisk –l** command to check partitions:

```
Disk /dev/sdb: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x502626b1

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb2               1        6527    52428096   8e  Linux LVM
/dev/sda3            3/140       63271   223907104   8e  Linux LVM

Disk /dev/sdb: 53.7 GB, 53687091200 bytes
255 heads, 63 sectors/track, 6527 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x502626b1

   Device Boot      Start         End      Blocks   Id  System
/dev/sdb2               1        6527    52428096   8e  Linux LVM
```

Run the **mount -o loop /dev/sdb2 /mnt/** command to mount the USB flash drive to the **/mnt** directory.

```
mkdir /mnt/iso
mount –o loop /dev/sdb2 /mnt/iso
```

Copy the ISO file to the **/mnt/install** directory.

```
mkdir /mnt/install
cp -ar /mnt/iso/* /mnt/install/
```

➢ Deployment and Installation

Note: Enter commands manually to perform installation.

As described in “Uploading MACC-BASE Installation Package”, the MACC-BASE installation package has been uploaded to the server and mounted to the **/mnt/iso** directory. The ISO file has been copied to the **/mnt/install/** directory.

1) The following directories will be displayed in the deployment and upgrade directory:

```
[root@localhost pkg]# cd /mnt/install/
[root@localhost pkg]# ll
drwxr-xr-x. 4 root root    4096 Aug 29 16:43 installpkg
-rwx--x--x. 1 root root 35048 Aug 29 16:43 install.sh        <<-----Executed for initial installation
```

2) Run command **install.sh**.

```
[root@localhost install]#./install.sh -l en -i 172.18.33.200 <<----Herein, 172.18.33.200 is an external IP address.
System version : CentOS-7-x86_64-Minimal
Checking for system ...64-bit
Checking for macc directory...yes
Checking for ppl...no
Installing ppl...
```

Note 1: Run command **chmod** to obtain the execution permission of **install.sh**.

```
chmod 777 /mnt/install/install.sh
```

Note 2: The following RPM signature warning can be ignored.

```
warning:
/macc/install_pkg/ RG-MACC-BASE_3.1_Build20180126/installpkg/soft/rpm/kernel-headers-2.6.32-504.1.3.el6.x86_64.rpm: Header V3 RSA/SHA1 Signature, key ID c105b9de: NOKEY
```

Note 3: The following MySQL startup error can be ignored, and does not affect the installation.

```
Initializing mysql...
ERROR! MySQL server PID file could not be found!
Starting MySQL.. SUCCESS!
SUCCESS! MySQL running (2811)
Initialize mysql.....................[OK]
Checking for tomcat...no
spawn openssl genrsa -des3 -out ./ca/serverkey.pem 2048
```

Note 4: Run the following commands to restart mongoDB if it does not start normally.

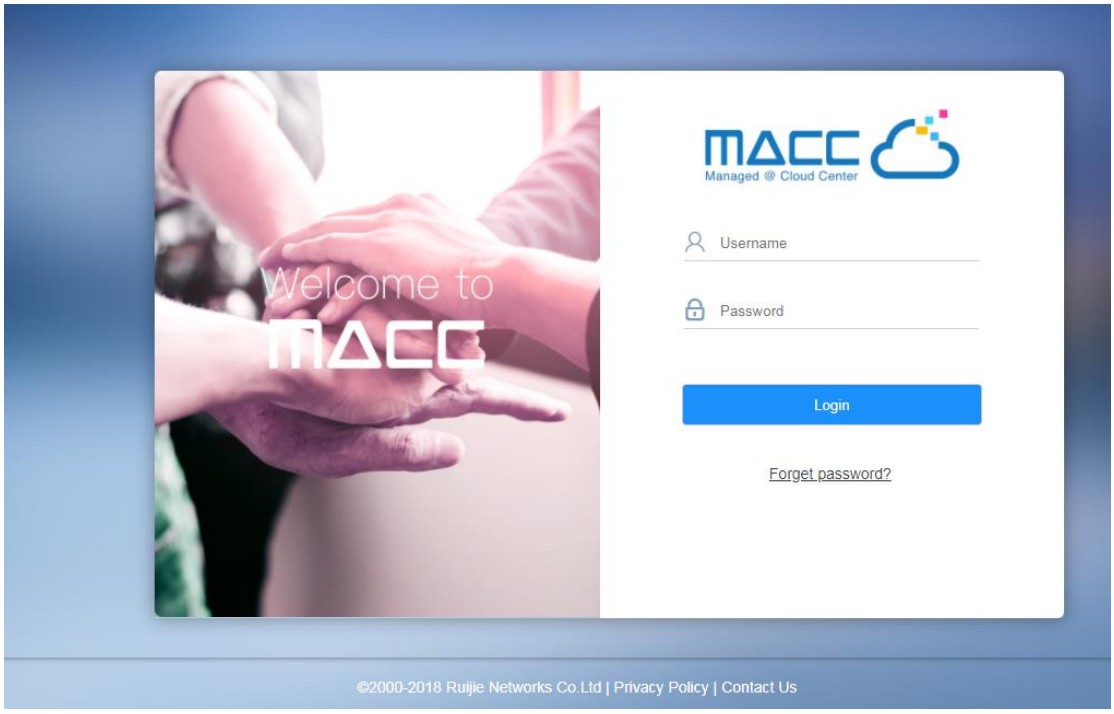
```
[root@localhost mongo]# ps -ef|grep mongod    <<------It starts normally if the mongod process exists.
mongod       3810         1    2 13:24 ?              00:00:00 /usr/bin/mongod -f /etc/mongod.conf
root          3838    2110    0 13:24 pts/0       00:00:00 grep mongodwarning:
```

```
<<-----If mongoDB is not started, execute the following operation to start mongoDB.
[root@localhost mongo]# rm -rf /var/lib/mongo/*     <<-----Deleting all the files under this directory.
[root@localhost mongo]# service mongod start     <<-----Starting mongoDB.
Starting mongod: [    OK    ]
```

5.3. Verifying Deployment and Installation

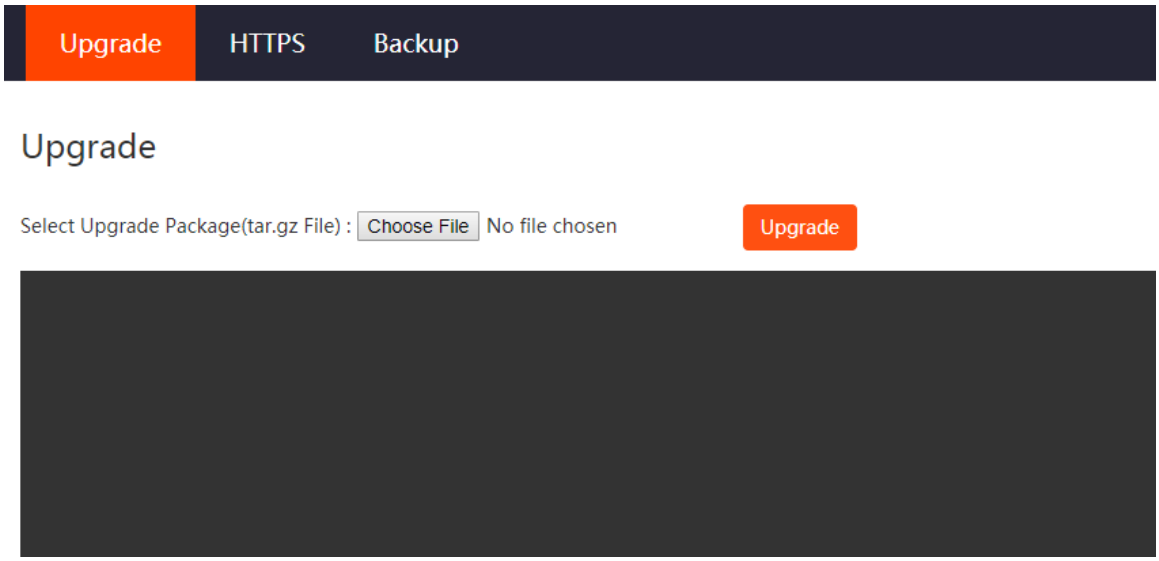
➢ **Verifying MACC-BASE Service**

Open the Google Chrome browser, and enter the URL *http://IP address or http://IP address:port* into the address bar to visit the website (the IP address is the actual IP address during installation and the default port is Port 80). Enter the account **admin** and password **admin** (default password) to log in to the MACC-BASE server. For details, see *RG-MACC-BASE_3.1 User Guide*.



➢ **Verifying Back-end Management System**

Use account **admin** and password **admin** to log in to the back-end management system (http://IP address:8090). It includes function of **Upgrade**, **HTTPs** and **Backup.**


Upgrade
HTTPS
Backup
Upgrade
Select Upgrade Package(tar.gz File) :
Choose File
No file chosen
Upgrade

6. Quick Start

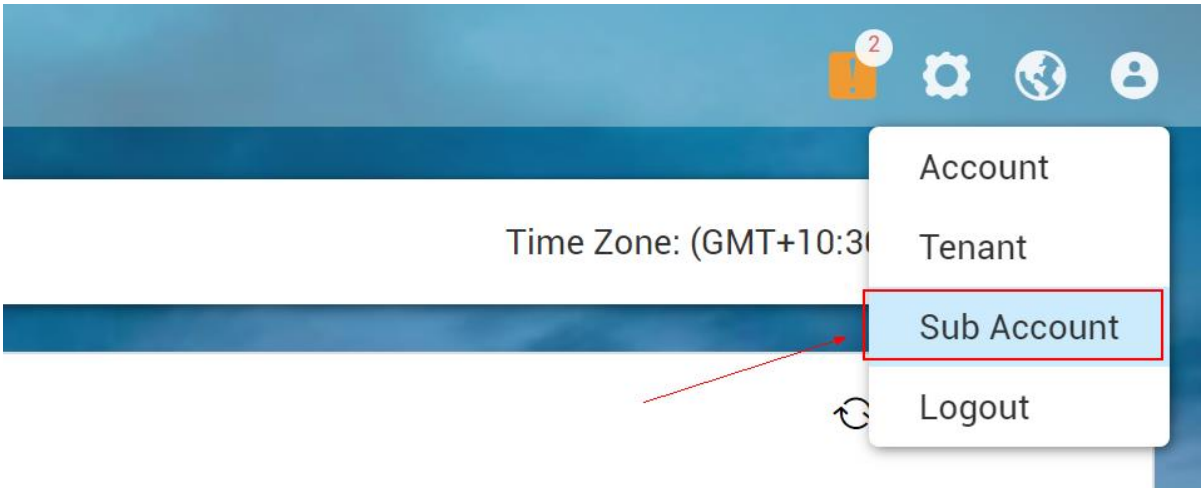
6.1. MACC-BASE Account Management

MACC provides 3 different roles for sub-account for admin user to manage system easily.

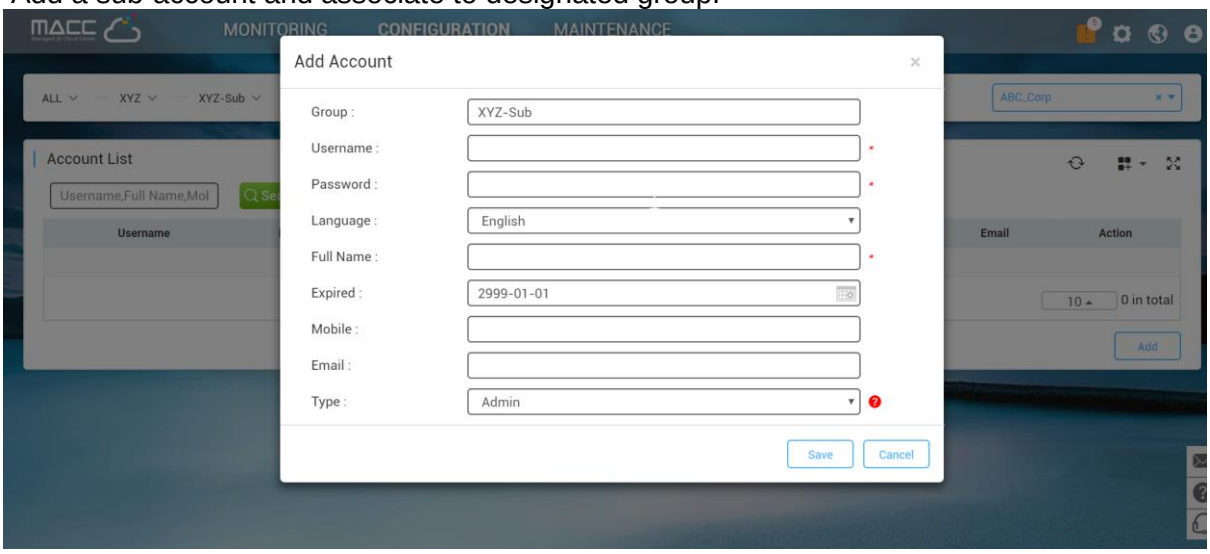
- **Admin**: Own the permissions to create sub-account, edit, read.
- **Employee**: Own the permissions to edit, read.
- **Guest**: Own the permissions to read.

Configure Steps:

1) Login MACC-BASE and click Account on top right corner



2) Add a sub-account and associate to designated group.



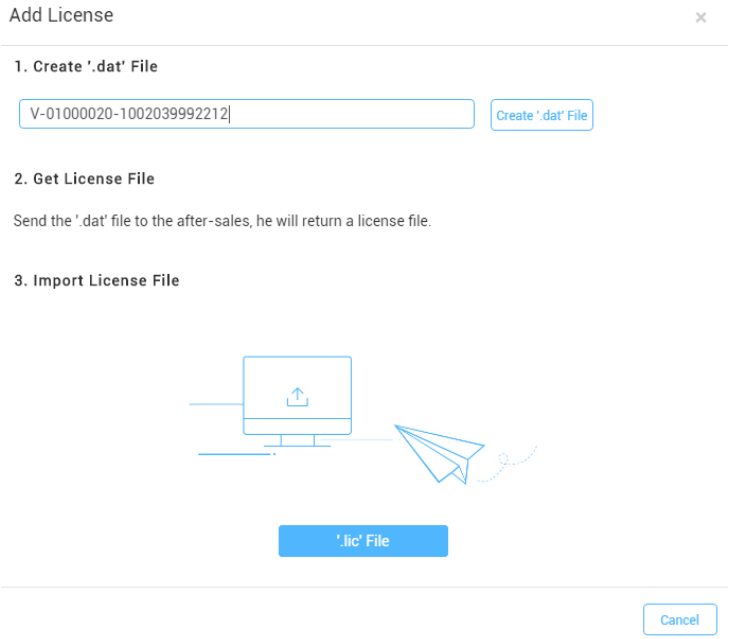
3) Login to MACC using this newly created account.

6.2. MACC-BASE License Key

Up to 10 devices are supported by default. You can add licenses as follows:

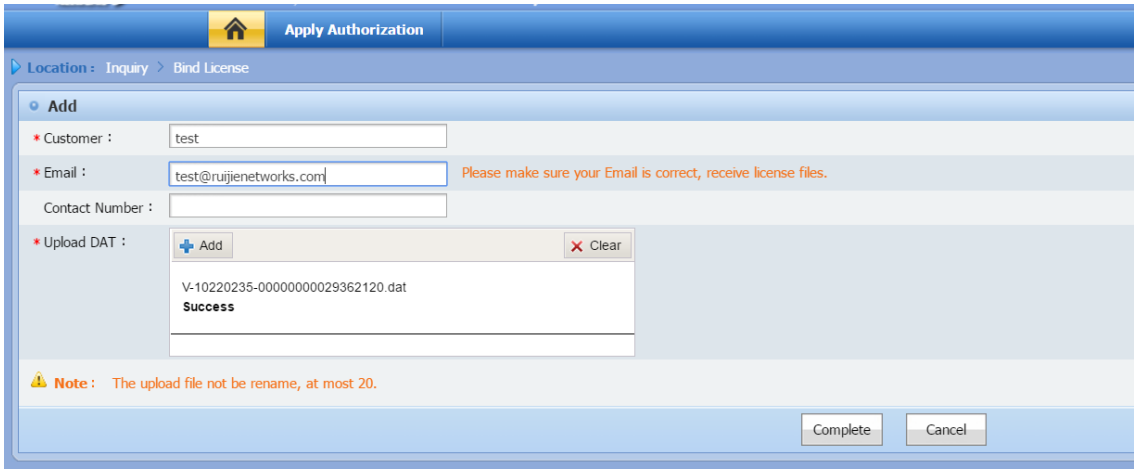
1) Click the Add button.

2) Enter the authorization code, and click Create '.dat' File to generate and download the ".dat" file.

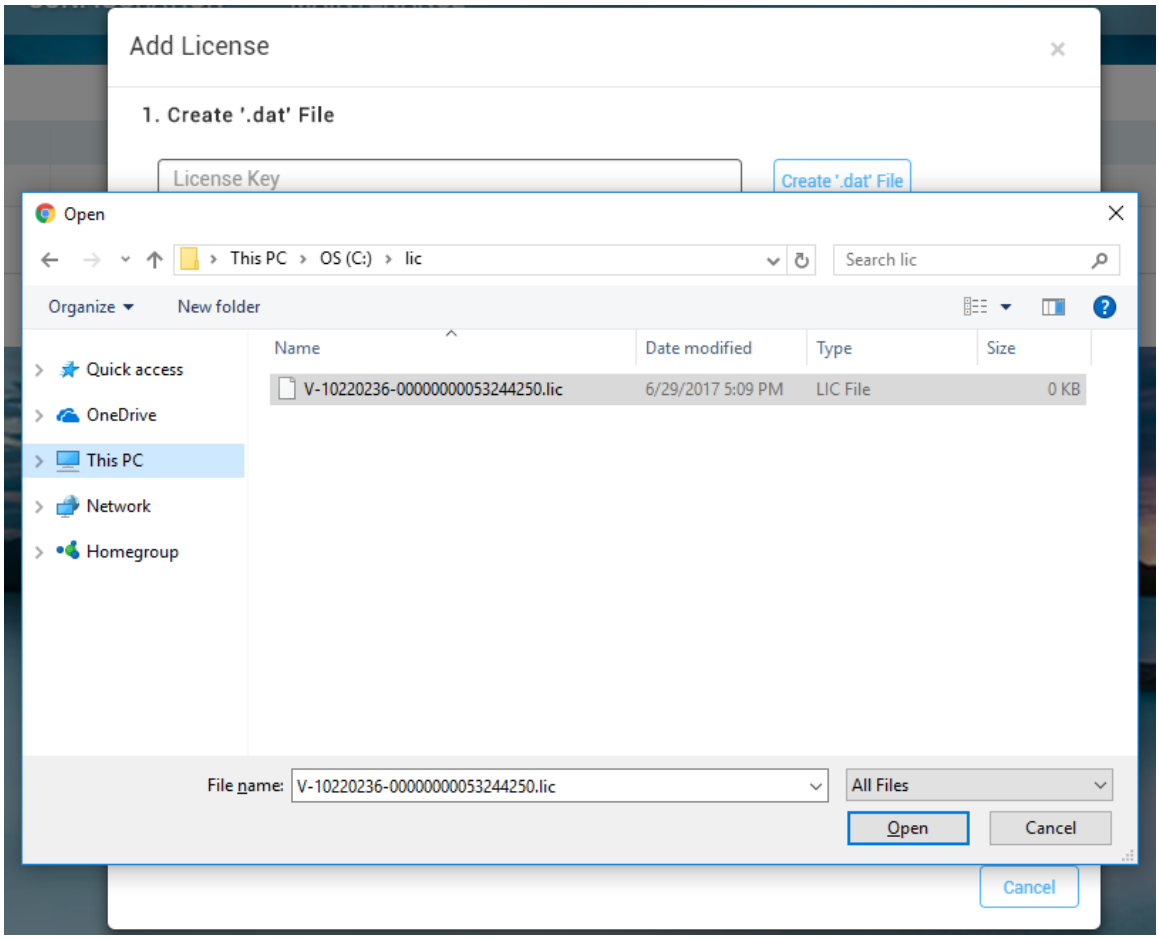


Note: After you have bought the authorized MACC-BASE, the authorization code will be automatically sent to your mailbox.

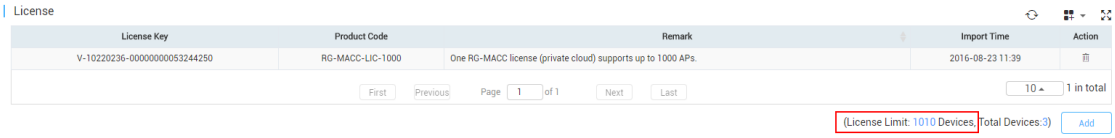
3) Import the ".dat" file to PA system to generate a ".lic" file, and download the".lic" file. (PA system address: http://pa.ruijie.com.cn:8001/main_software.jsf)



4) Import the “lic” file to MACC.



After the import operation is complete, please refresh the page. (The default AP license number in MACC-BASE is 10. After 100 licenses are imported, the total license number will be 110)

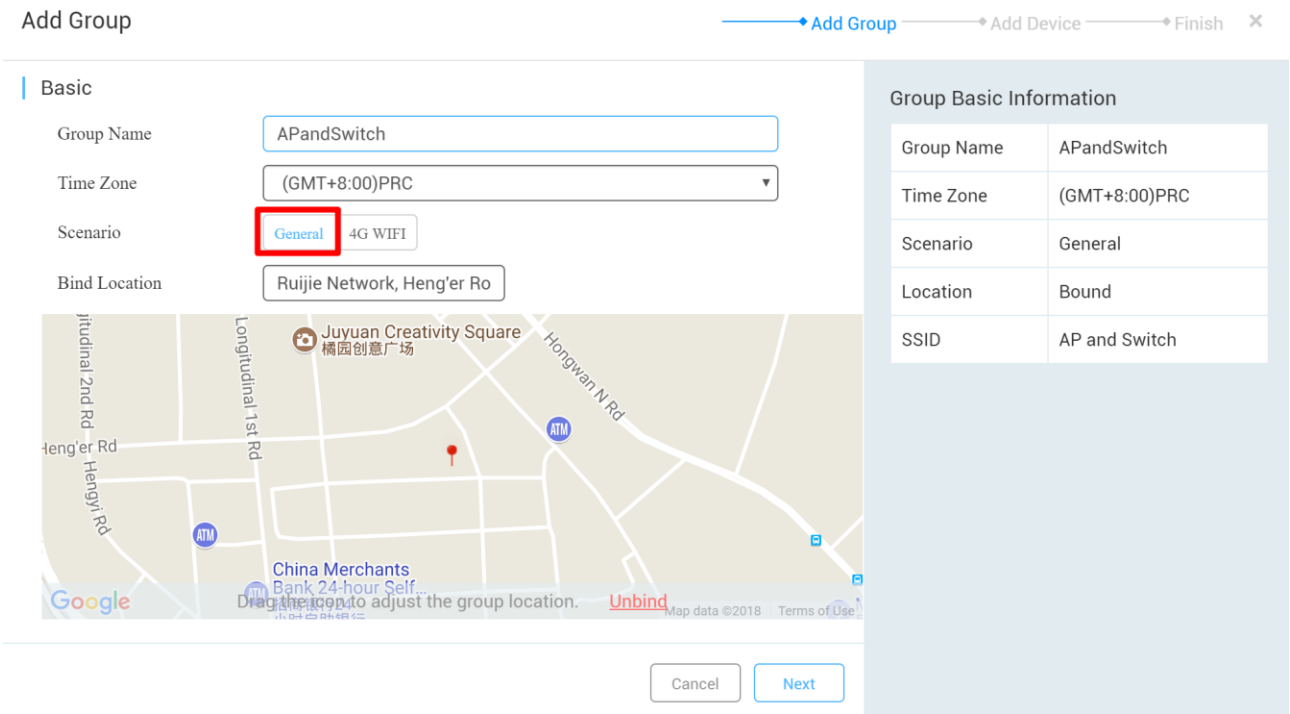


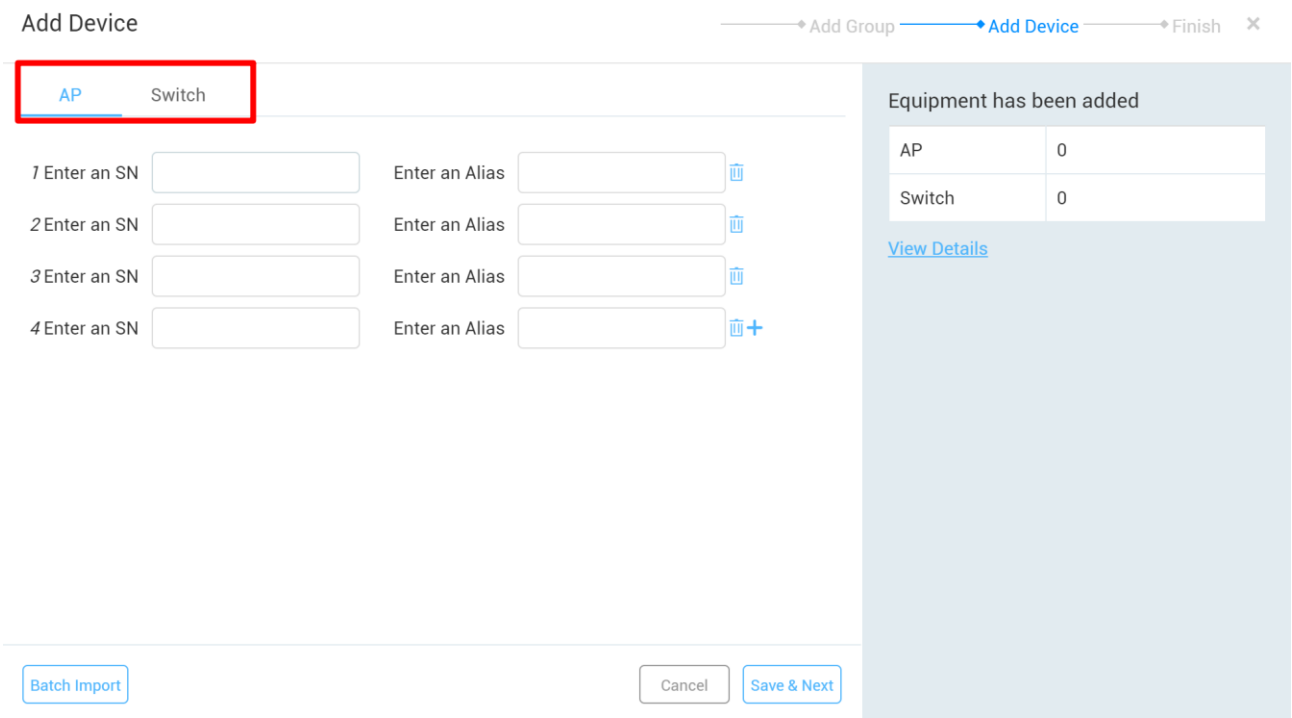
6.3. Getting Devices Online

6.3.1. Adding Devices

AP/Switch

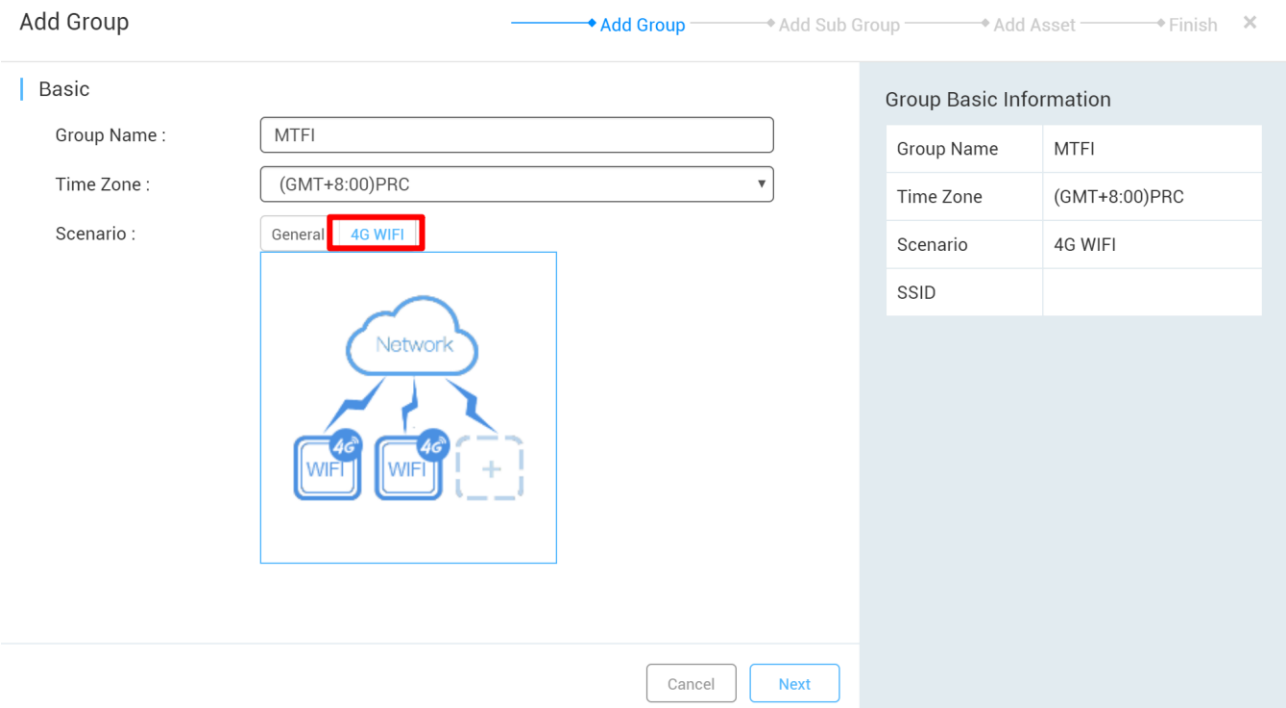
1) Go to **Configuration** > **Groups**
2) Click on **Add Group** on lower right corner
3) Select **General** Scenario and follow the Wizard to import **Serial Number (SN)** of APs and Switches.

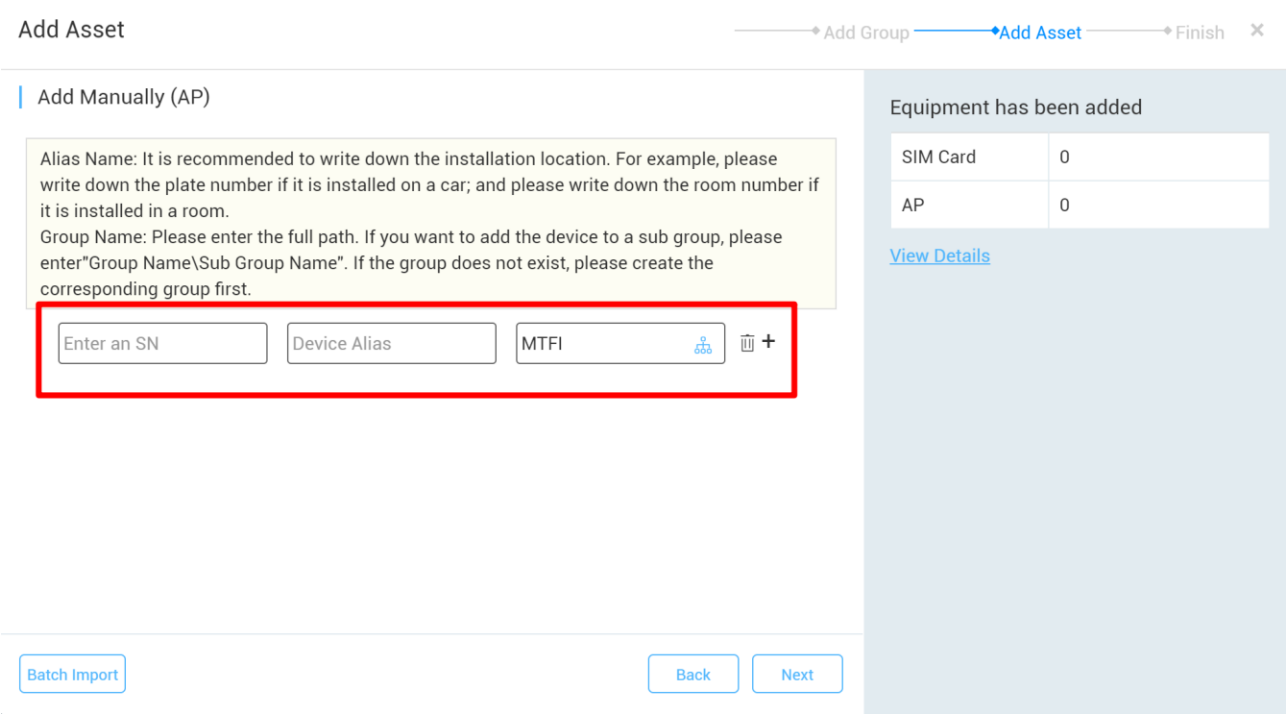




MTFI

1) Go to **Configuration** > **Groups**
2) Click on **Add Group** on lower right corner
3) Select **4G WIFI** Scenario and follow the Wizard to import **SIM Card** info and **MTFI's Serial Number (SN).**





6.3.2. Configuring Devices

Device can access MACC-BASE through three methods: DHCP server allocation, CLI configuration and Web configuration.

⚠ Please make sure that the device version can meet the requirements of MACC-BASE. For details, please refer to *MACC-BASE 3.1 Release Note*.

⚠ Please check the connectivity between device and MACC-BASE to make sure that the device can go online.

Allocating CWMP from DHCP Server (Apply to AP/ Switch)

1) Run the following commands to configure the DHCP server.

```
DHCP-Server#conf t
DHCP-Server(config)#service dhcp
DHCP-Server(config)#ip dhcp pool AP
DHCP-Server(config)#network 10.10.10.0 255.255.255.0                    //IP address of device
DHCP-Server(config)#network dns-server 8.8.8.8 8.8.4.4
DHCP-Server(config)#network default-router 10.10.10.254
DHCP-Server(config)#option 43 ascii http://A.B.C.D/service/tr069servlet       //A.B.C.D represents the URL
 or domain name of MACC-BASE
```

⚠ Switches cannot obtain IP address automatically by default. Please create an SVI and run the **ip add dhcp** command to obtain dynamic IP address.

2) After the dynamic IP address is obtained, the device will send a request to MACC-BASE for going online.

⚠ Please check the connectivity between device and MACC-BASE to make sure that the device can go online.

Configuring CWMP on CLI (Apply to AP/Switch)

⚠ Before configuration, please run command **ap-mode macc** to set the running mode of AP to MACC mode.

1) Run the following commands on CLI page to configure CWMP.

```
Ruijie#conf t
Ruijie(config)#cwmp
Ruijie(config-cwmp)#acs url http://A.B.C.D/service/tr069servlet        //A.B.C.D represents the IP address or
   domain name of MACC-BASE
```

2) Configure a static IP address, gateway and DNS server for the device.

```
Ruijie#conf t
Ruijie(config)#int bvi vlan-id                    //AP configuration
Ruijie(config)#int vlan vlan-id                   //switch configuration
Ruijie(config-if-VLAN-id)#ip add A.B.C.D   mask          //A.B.C.D represents the IP address of device
Ruijie(config)#ip domain-lookup                   //enable DNS lookup
Ruijie(config)#ip name-server 8.8.8.8 8.8.4.4
Ruijie(config)#ip route 0.0.0.0 0.0.0.0   X.X.X.X        //indicates the gateway address of device
```

3) After basic configuration, the device will send a request to MACC-BASE for going online.

Configuring CWMP on Web UI (Apply to AP/MTFi)

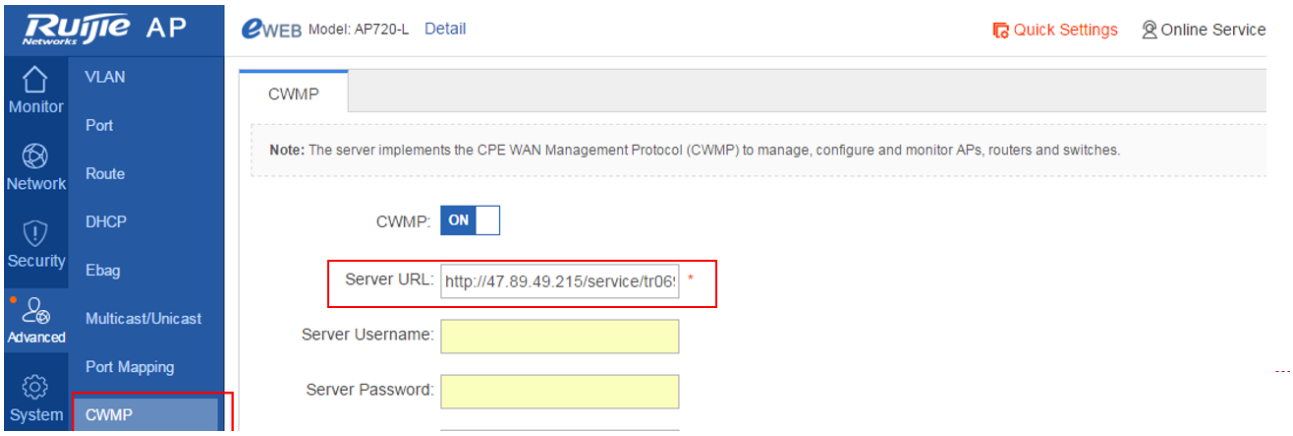
1) Log in to device Web UI with wired connection.

   MTFi:192.168.1.1:8888; Password: admin-mtfi

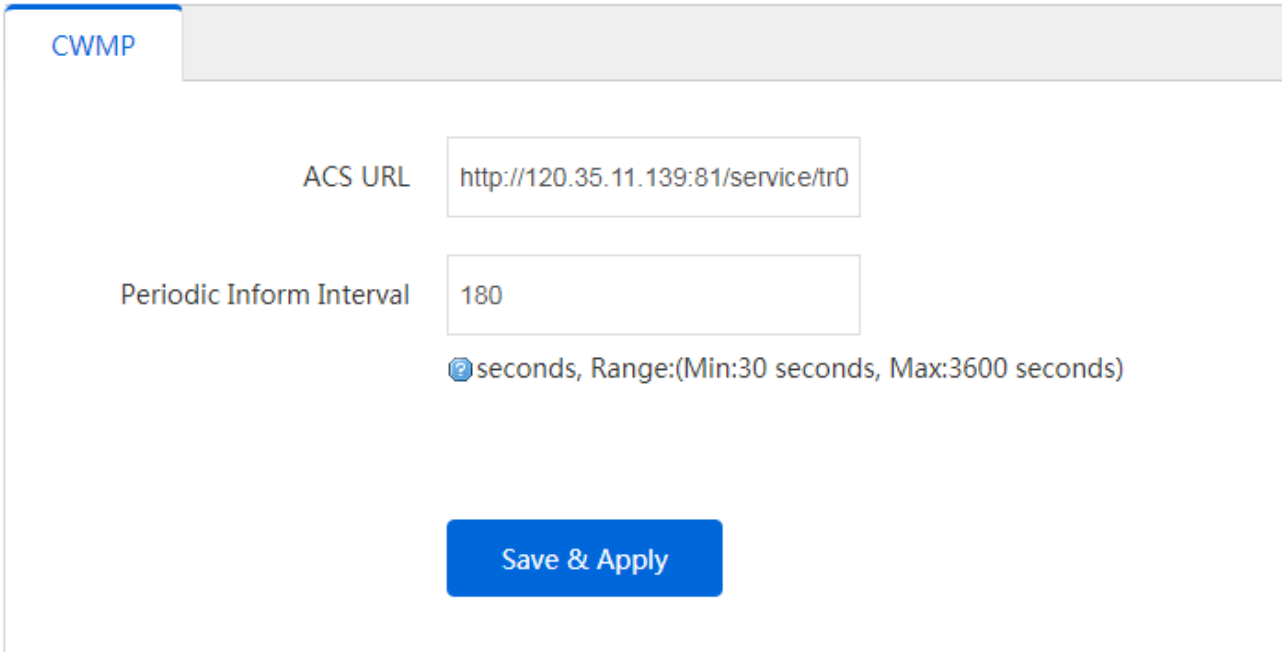
   AP:192.168.110.1:80; Username/Password: admin

2) Configure the CWMP URL (http://*A.B.C.D*/service/tr069servlet) on **Advanced > CWMP**.

AP:



MTFi:



6.3.3. Online Verification

Log in to MACC-BASE and click **Access Point** and **Switch** on **MONITOR** > **DEVICE** to check whether the device is online.

Status	SN	Config Status	MAC	Device Alias	MGMT IP	Public IP	Clients	Group	Firmware Version	Down	Model	Description	Action
Online	G1KDA0T003926	Not Synced	5869.6cb9.7926	Indoor AP740-I	172.16.15.79	172.16.15.79	1	Holiday_Hotel	AP_RGOS 11.1(5)B9P2, Release(04151613)		AP740-I		
Online	G1KD84P049831	Not Synced	5869.6c98.4341	Indoor AP130(L)	172.16.15.83	172.16.15.101	-	Holiday_Hotel	AP_RGOS 11.1(5)B9P2, Release(04162719)		AP130(L)		

First Previous Page 1 of 1 Next Last 10 2 in total

7. Configuration Guidance

MACC-BASE 3.1 can manage wireless and switch device as listed in release note. And this chapter will introduce configuration examples for each function.

7.1. Wireless Devices

7.1.1. WIFI Configuration

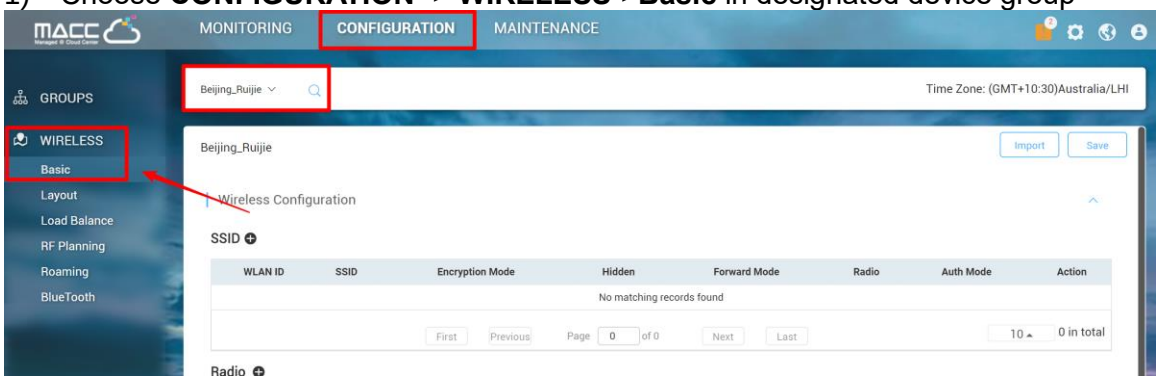
In this section will introduce how to create SSID for AP and MTFI device.

Access Point

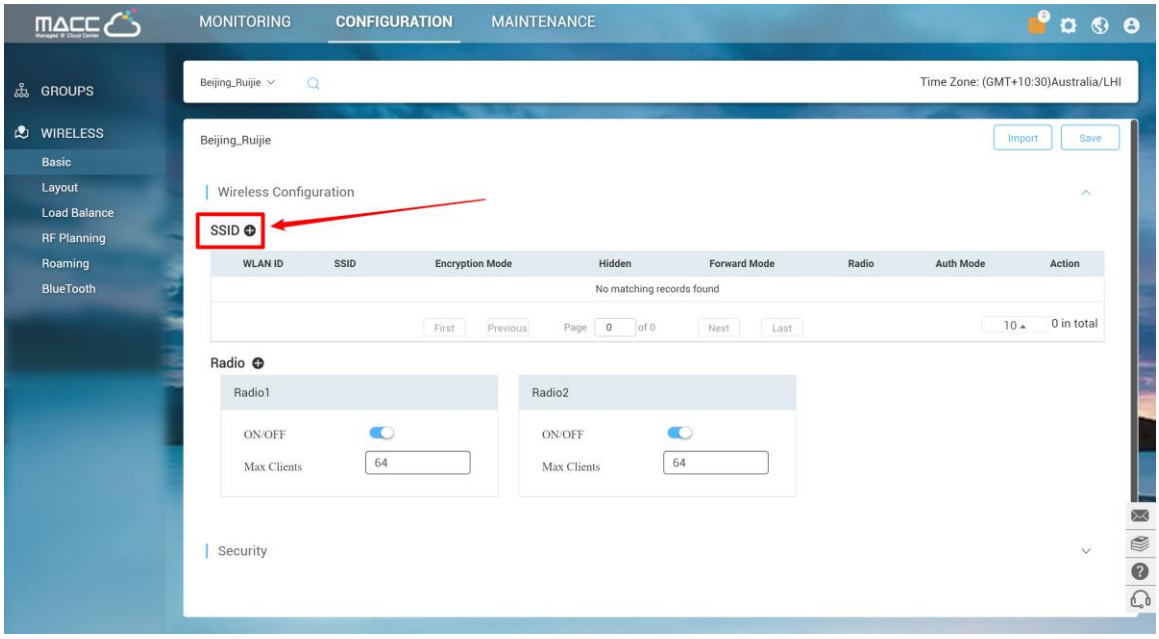
In WiFi Setting page, MACC-BASE support wireless basic functions as follow:

- **Authentication**: Open, PSK, Dot1x with 3rd party radius server, WiFidog authentication
- **SSID Advanced Setting**: SSID QOS, Bridge/NAT working mode, Band Steering, Seamless authentication
- **Radio Setting**: Maximum Connectors
- **Security**: Web Login Password, Wireless Attack Defence
- **Advanced Features**: Whitelist, CLI Command Batch Delivery

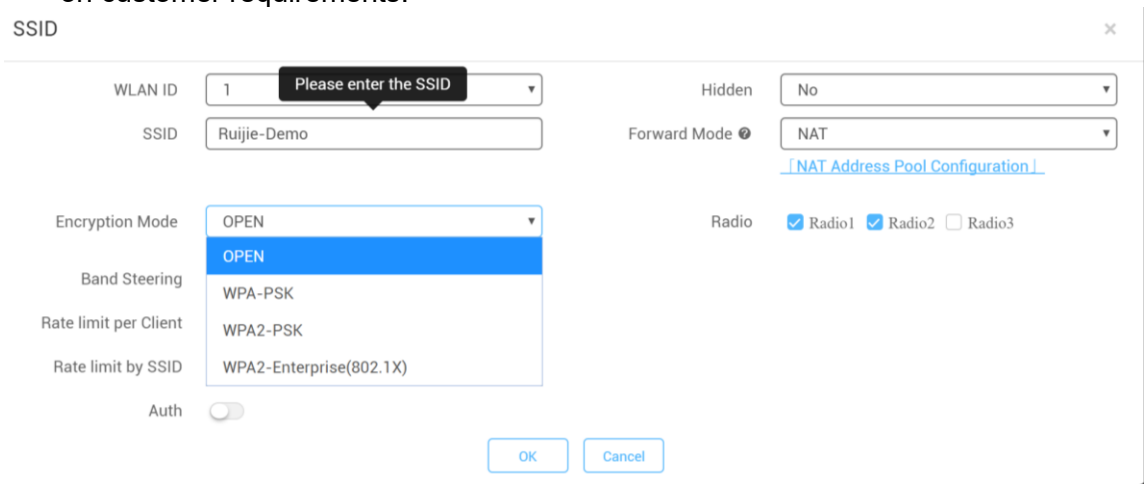
1) Choose **CONFIGURATION -> WIRELESS->Basic** in designated device group



2) Click "**+**" to create a SSID for the devices under this group



3) In SSID setting page, user can create an SSID and fill in related parameters based on customer requirements.



WLAN ID: Sequence number to represent SSID ID (Up to 32 SSID is supported, there may be differences between diverse models)

Hidden: Choose disable broadcasting SSID or not

SSID: WiFi Name

Forward Mode:

NAT mode or bridge mode. NAT mode: AP will work as a router and DHCP pool to provide IP address for terminal stations.

Bridge mode: AP will work as a switch and passthrough all traffic. It requires the user to fill in specific VLAN ID for STA.

(If not familiar with existed network design, NAT mode is recommended)

Encryption Mode:

OPEN: Open SSID and password is not required

WPA-PSK: Use WPA algorithm to encrypt SSID and password is required

WPA2-PSK: Use WPA2 algorithm to encrypt SSID and password is required

WPA2-Enterprise(802.1x): Dot1x authentication and external radius server is required

Radio: generally, Radio 1 represent 2.4Ghz and Radio 2 represent 5Ghz.

Band Steering: detect clients capable of 5 GHz operation and steers them to that frequency which leaves the more crowded 2.4 GHz band available for legacy clients. (Please ensure 5G Radio Interface is enabled)

Rate limit per Client: Upload and download speed limitation for each client on this SSID

Rate limit by SSID: Total throughput (upload & download) on this SSID

Auth:

Portal Server URL: external wifidog portal server URL for user login

Portal IP: Portal server IP address

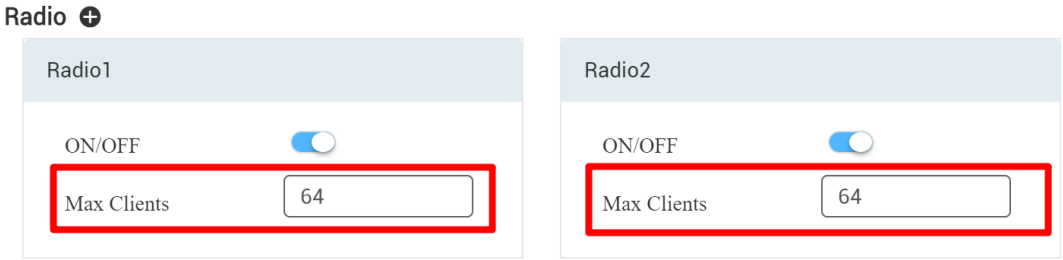
Portal Port: Port number for landing page redirection. Default is 80

Gateway ID: Gateway ID value for wifidog

Seamless Online: Seamless auth on STA connected to SSID second time. Authentication server supports seamless feature is required.

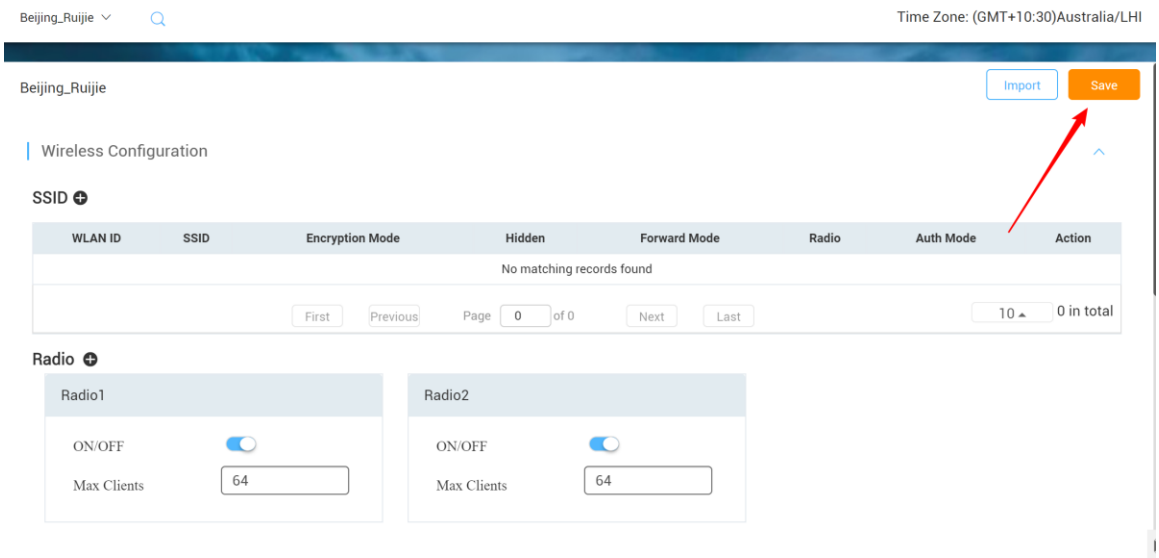
Idle Client Timeout: User will be kicked if low traffic or no traffic passthrough in specific period

4) Turn on the RF and fill in Max Clients value as required



⚠ The Max Clients of each Radio Interface is 32 by default.

5) Click Save on the top right corner to save all changes and take effect



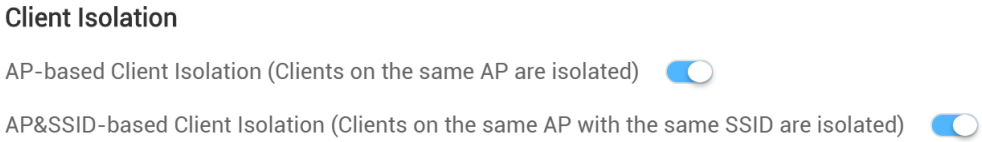
Advanced Setting

Web Password

This setting enables user to edit WEB UI and increase security level.

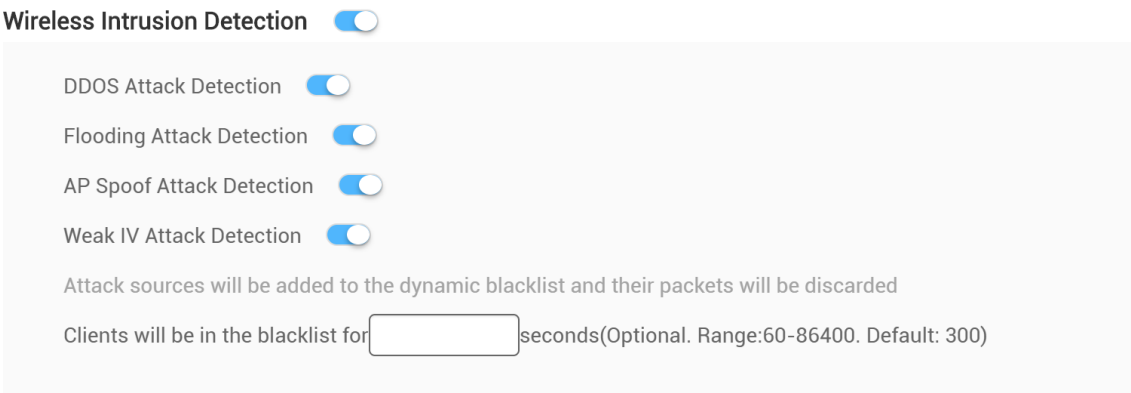
Isolation

Client Isolation is to isolate all traffic (unicast, multicast, broadcast) for each user.



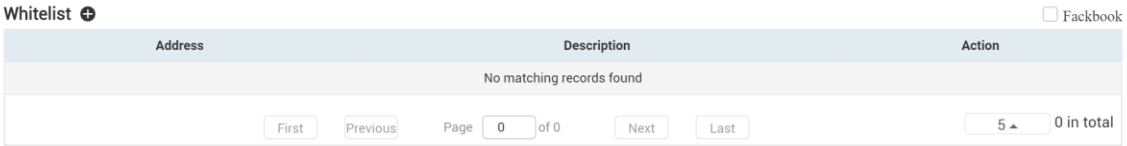
Wireless Intrusion Detection

Wireless Intrusion Detection can monitor STA behavior and prevent damage to network caused by anonymous hacker.



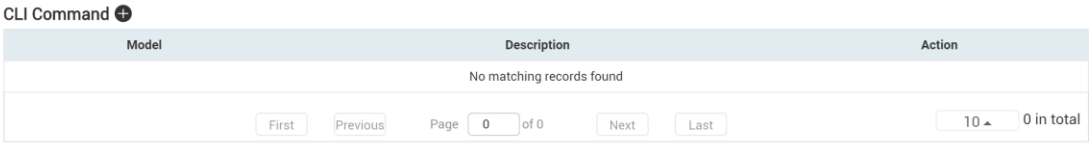
Whitelist

Whitelist feature can bypass those addresses or traffic on the list before STA completes authentication process.



CLI Command

CLI Command provides a window for user to exec cli setting which not be support in MACC-BASE UI.



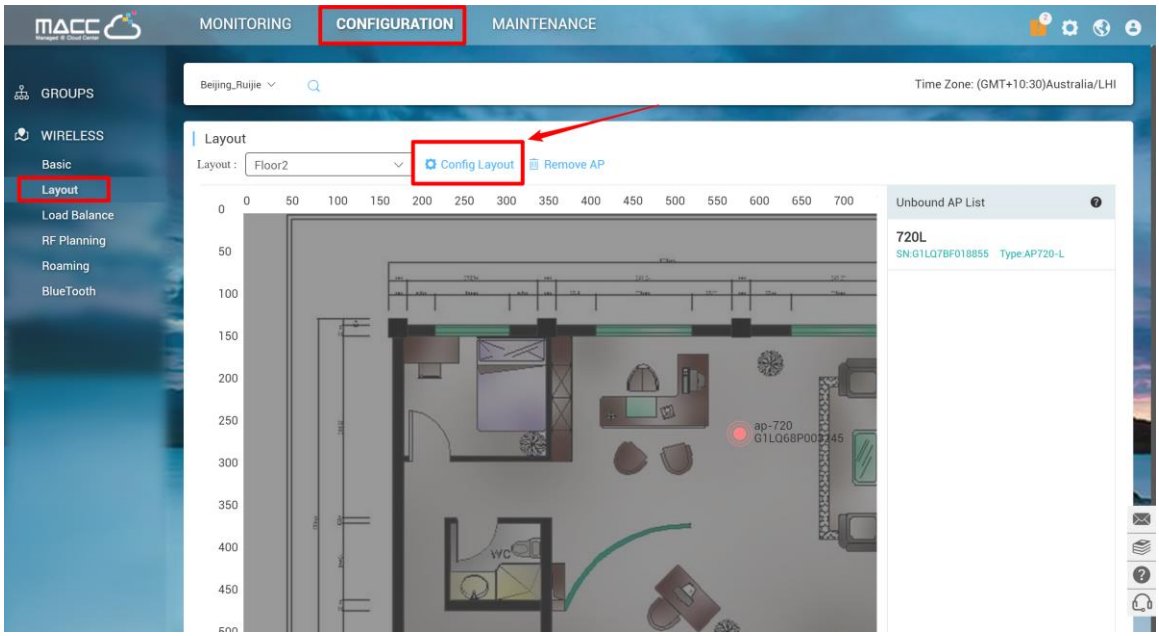
MTFI

Please refer "RG-MTFI Implementation Cookbook" on official website.

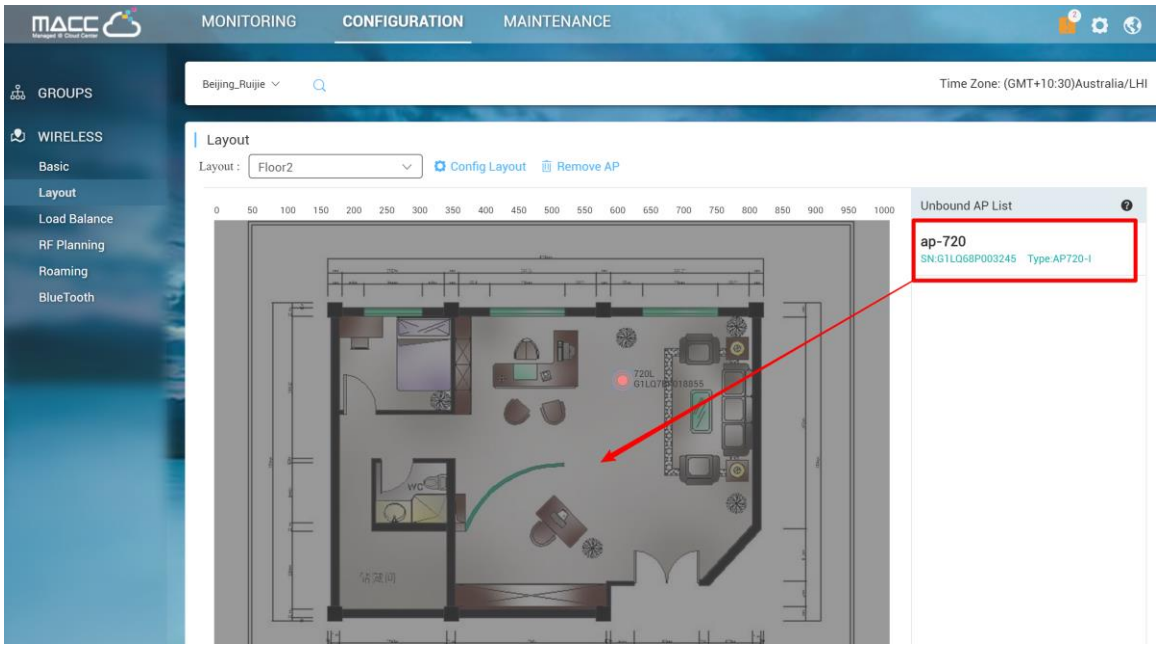
7.1.2. Layout Planning

Layout Planning allows user to import floor plan to MACC-BASE and binds AP to specific location as deployment.

Choose CONFIGUARTION->Layout and click Config Layout to add floor plan to MACC-BASE



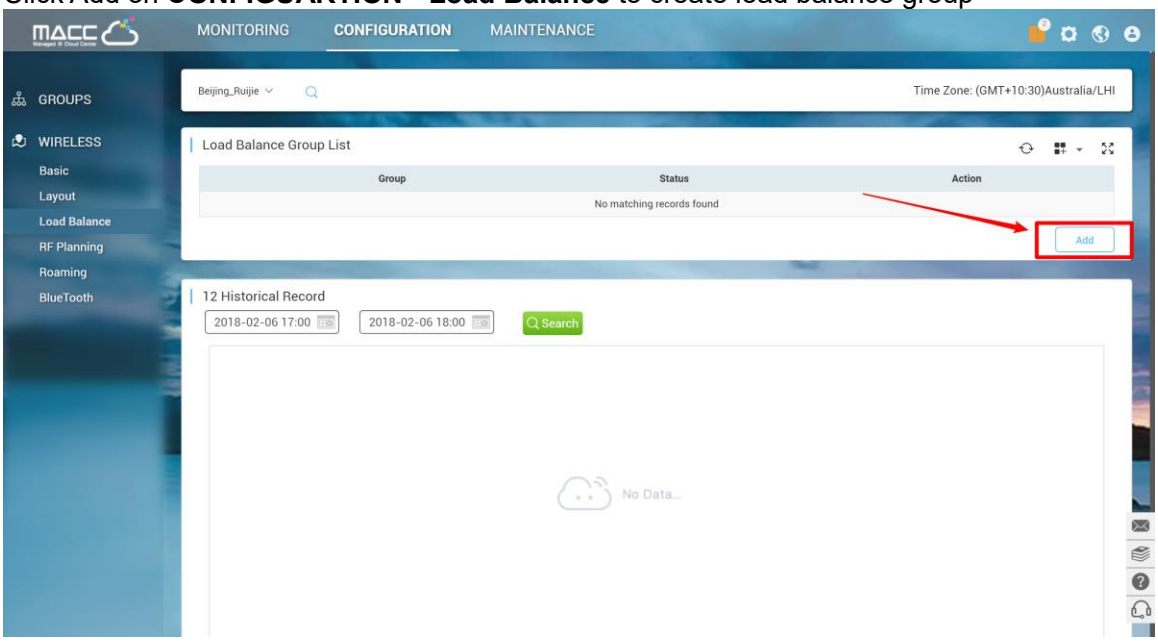
1) Drag the AP from un-bond AP list to floor plan to bind AP to specific location



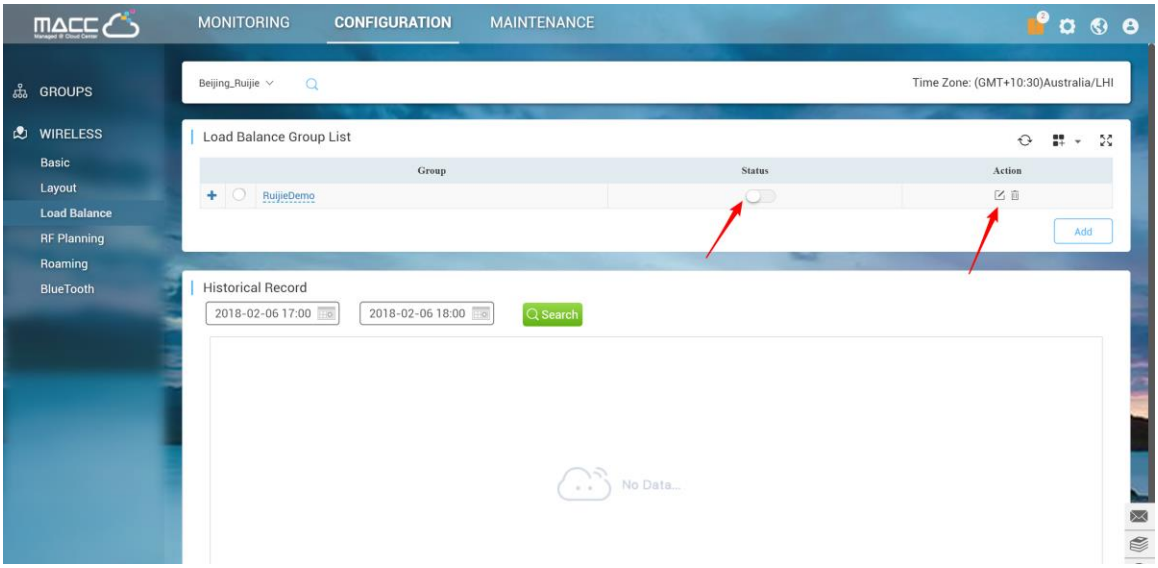
7.1.3. Load Balance

MACC-BASE load balance feature can dynamic allocate STA to each AP equally in high density scenario.

1) Click Add on **CONFIGUARTION->Load Balance** to create load balance group



2) Click **edit icon** to add access point into load balance group and **turn on** group status.



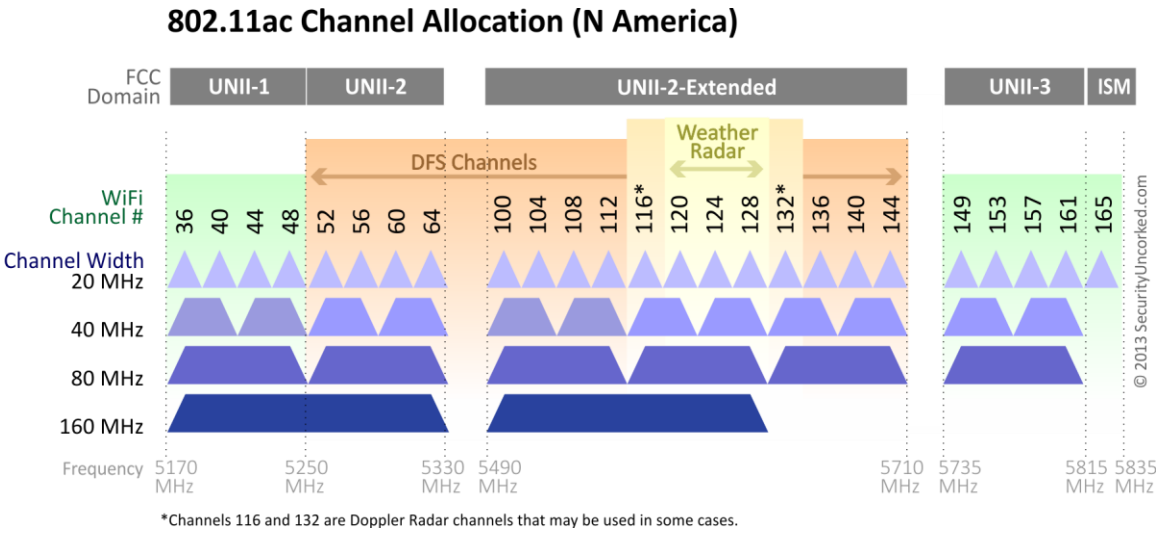
7.1.4. RF Setting

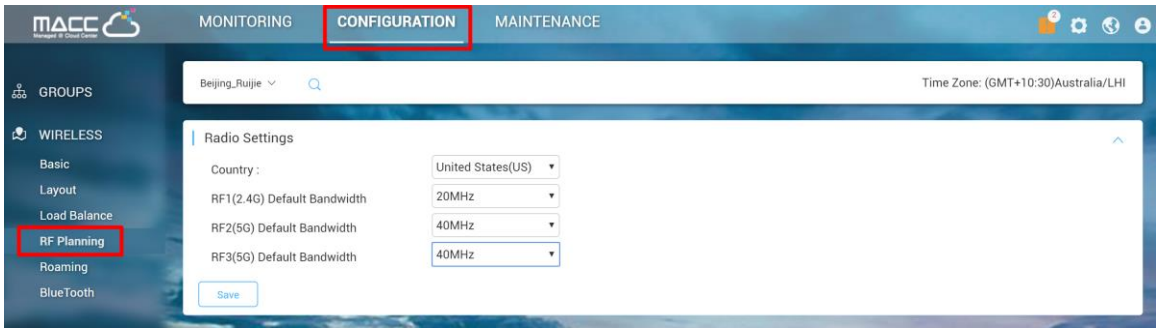
The RF Setting provides a global setting of wireless country code, bandwidth and intelligent channel/power planning.

Radio Setting

Country code enables you to specify a particular country of operation and it ensures each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulations. Frequency bandwidth determine how many non-overlap channels can be used for your AP to reduce RF interference.

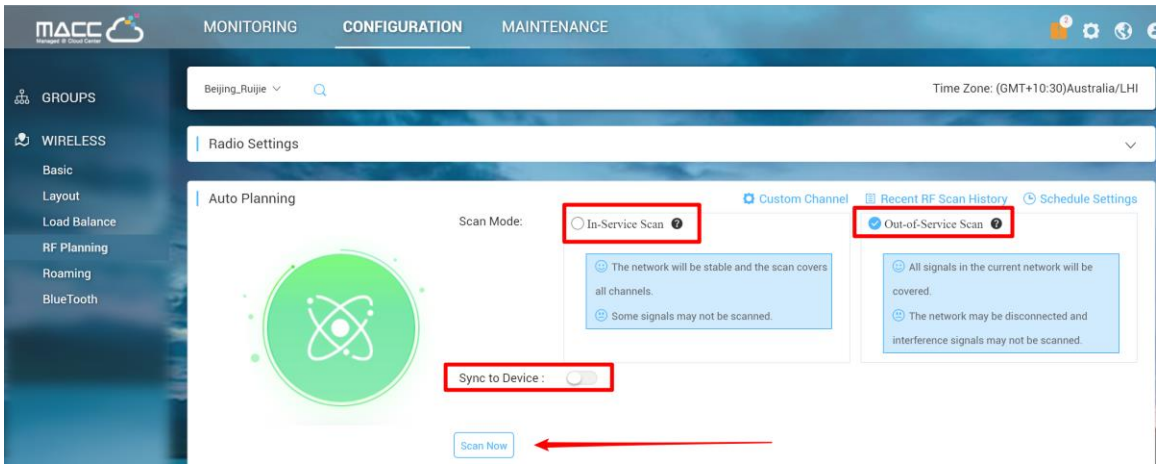
The best practice for user experience is 2.4GHz in 20MHz, 5GHz in 40MHz.





Auto Planning

Auto Planning works as a smart RRM function. It can help user to evaluate network channel and power status and provides recommended parameters by its intelligent algorithm.



Custom Channel: Allows user to select specific channel for channel planning

Recent RF Scan History: Records all scanning history and recommended value after scanning

Schedule Settings: Periodic scanning setting for access point

In-Service Scan (Quick Scan):

- The WiFi service won't be interrupted during scanning process.
- The scanning result may not include all interference.

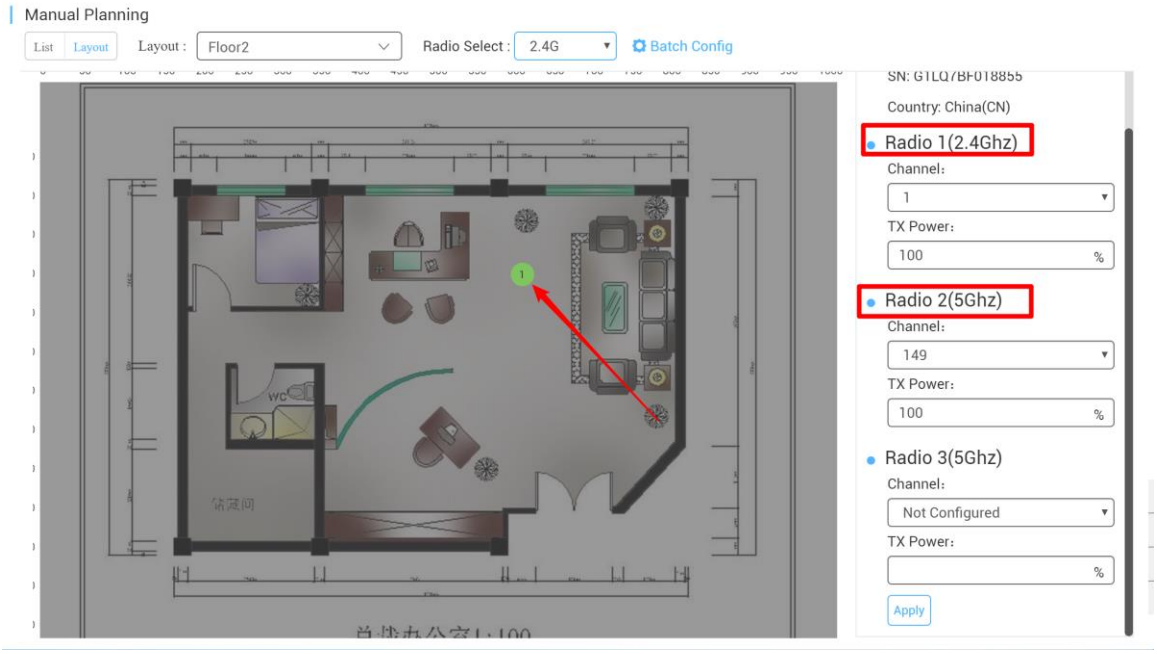
Out-of-Service Scan (Deep Scan):

- The result will cover almost all WiFi interference.
- The WiFi service will be interrupted during scanning process (disconnect and reconnect) and it will take around 30 minutes

Sync to Device: Whether sync the recommended setting to APs after scanning

Manual Planning

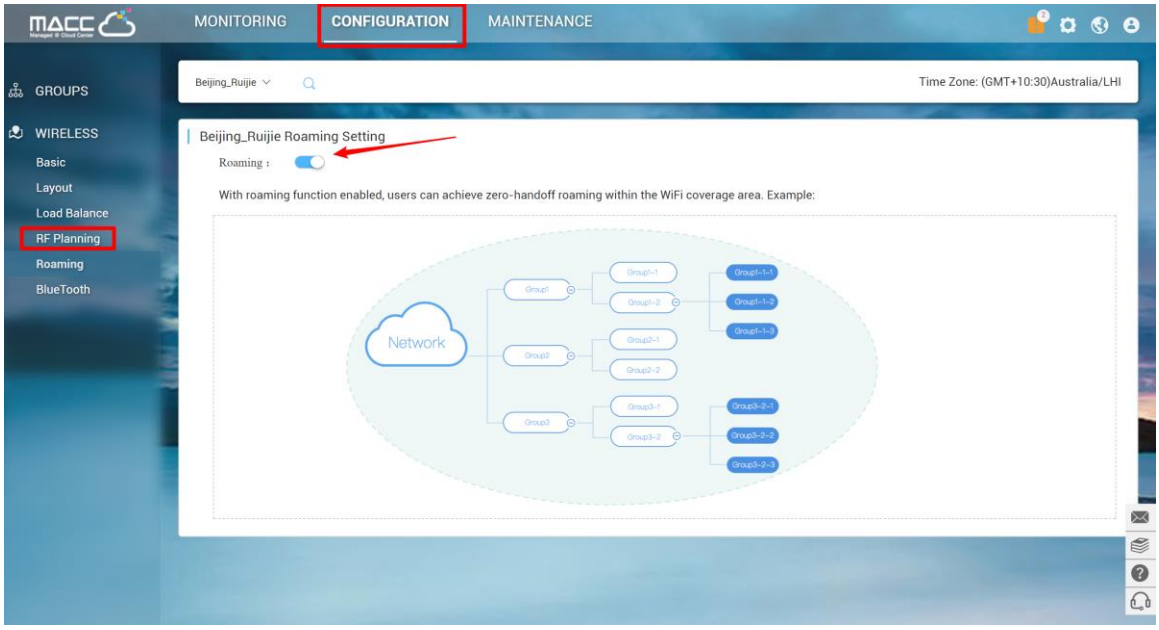
Manual Planning enables user to select designated AP and change the channel and power setting.



Only AP740-I can support Radio 3 setting

7.1.5. Roaming

MACC-BASE roaming function allows STA from AP-1 subnet A roaming to AP-2 subnet B (L3 roaming) seamlessly. Once user turns on the roaming button, L3 roaming ability will be enabled.

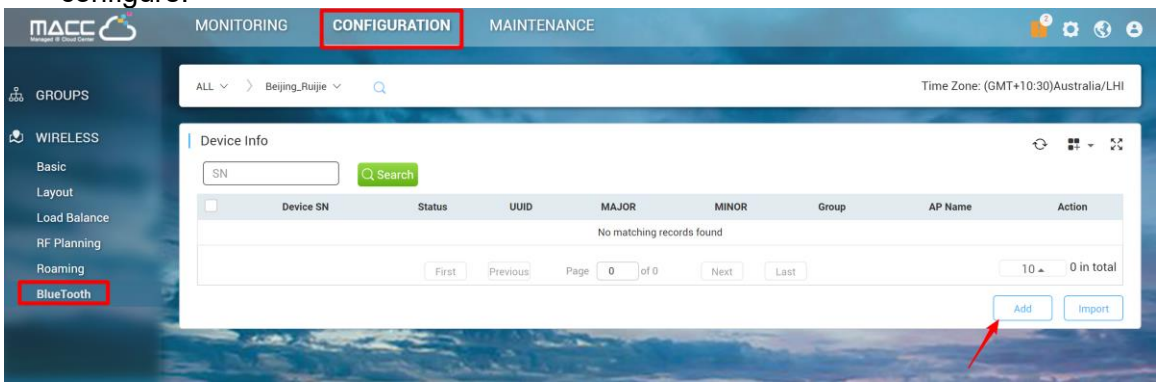


L2 roaming is enabled by default (OPEN, PPSK). For web authentication, seamless authentication function should be turned on to improving roaming user experience.

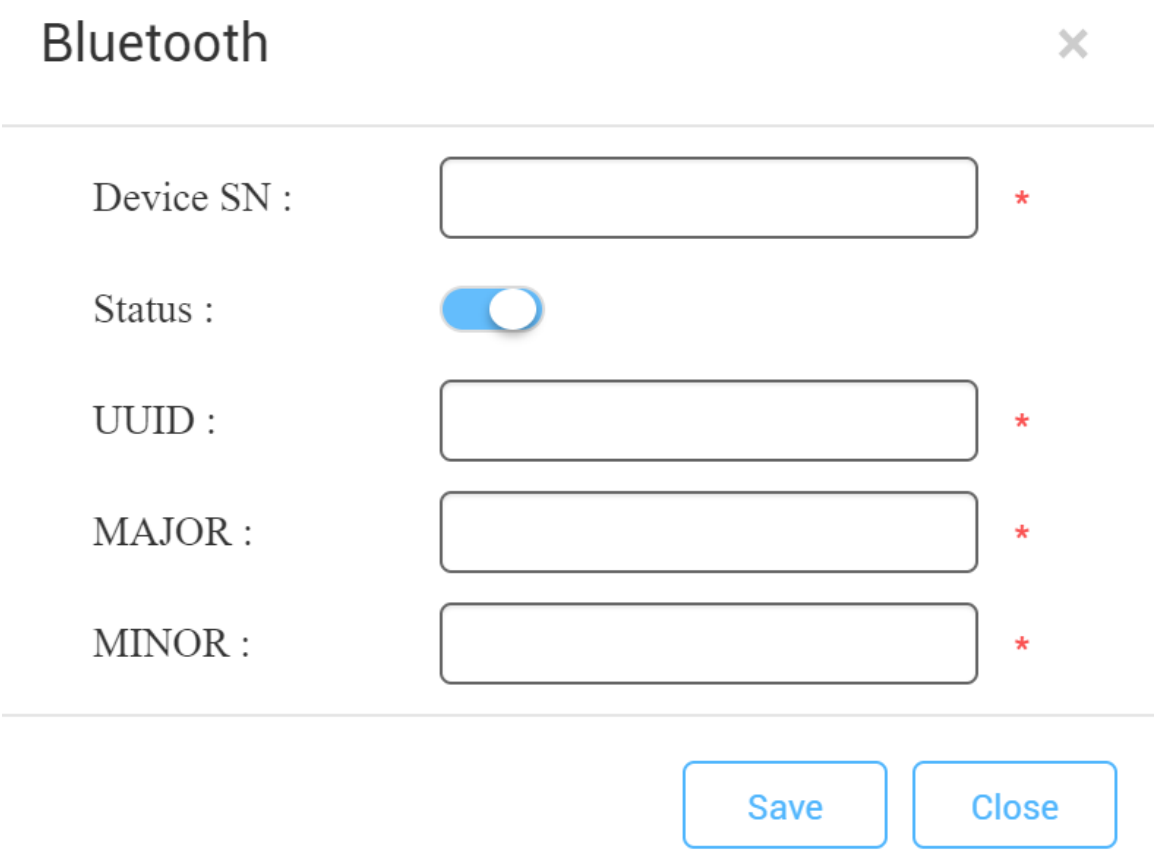
7.1.6. BlueTooth

BlueTooth is used for the AP which supports iBeacon feature to broadcast iBeacon signal.

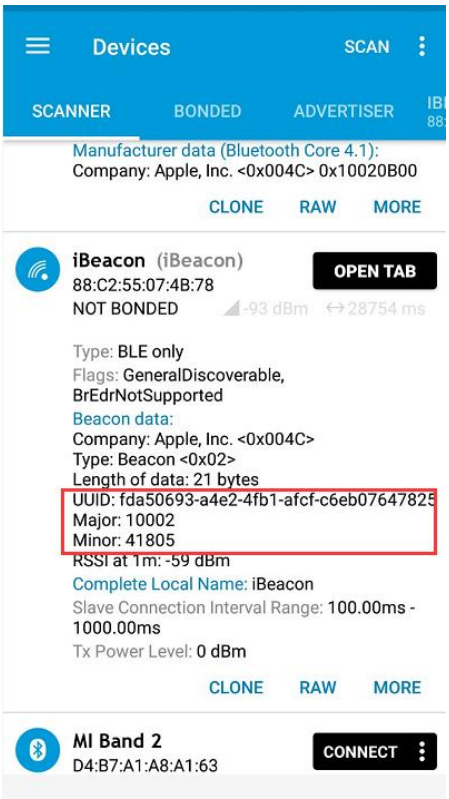
1) Click "**Add**" to iBeacon parameters to designated AP. Or click "**Import**" for batch configure.



2) Fill in AP serial number (needs to be online) and iBeacon parameters which are provided by iBeacon service provider.

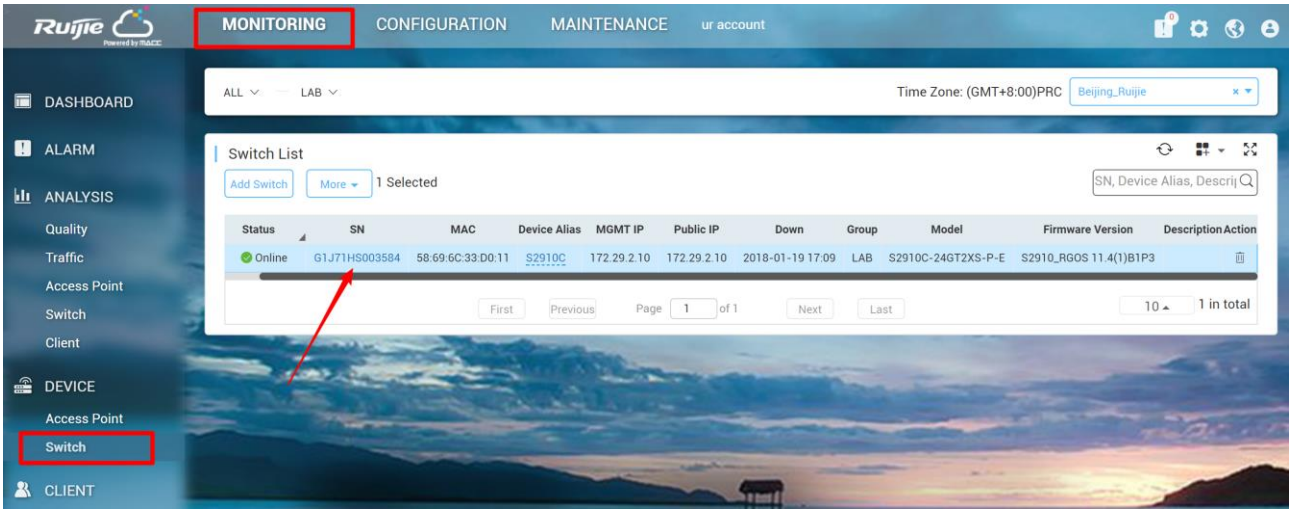


3) Verify by using “nRF Master Control Pannel” APP on Android phone.

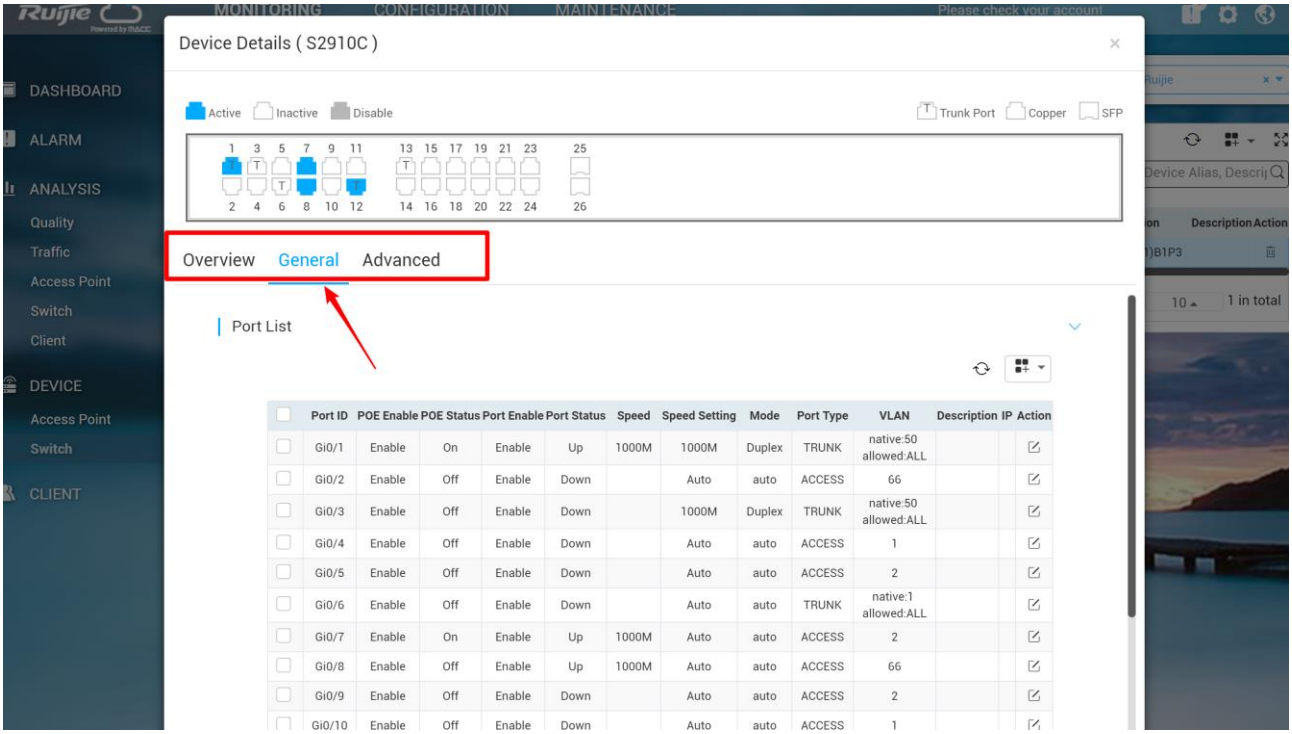

Devices
SCAN
SCANNER
BONDED
ADVERTISER
Manufacturer data (Bluetooth Core 4.1):
Company: Apple, Inc. <0x004C> 0x10020B00
CLONE
RAW
MORE
iBeacon (iBeacon)
88:C2:55:07:4B:78
NOT BONDED
-93 dBm
28754 ms
OPEN TAB
Type: BLE only
Flags: GeneralDiscoverable, BrEdrNotSupported
Beacon data:
Company: Apple, Inc. <0x004C>
Type: Beacon <0x02>
Length of data: 21 bytes
UUID: fda50693-a4e2-4fb1-afcf-c6eb07647825
Major: 10002
Minor: 41805
RSSI at 1m: -59 dBm
Complete Local Name: iBeacon
Slave Connection Interval Range: 100.00ms - 1000.00ms
Tx Power Level: 0 dBm
CLONE
RAW
MORE
MI Band 2
D4:B7:A1:A8:A1:63
CONNECT

7.2. Switch Device

1) Click designated switch on **MONITOR** > **Switch**.



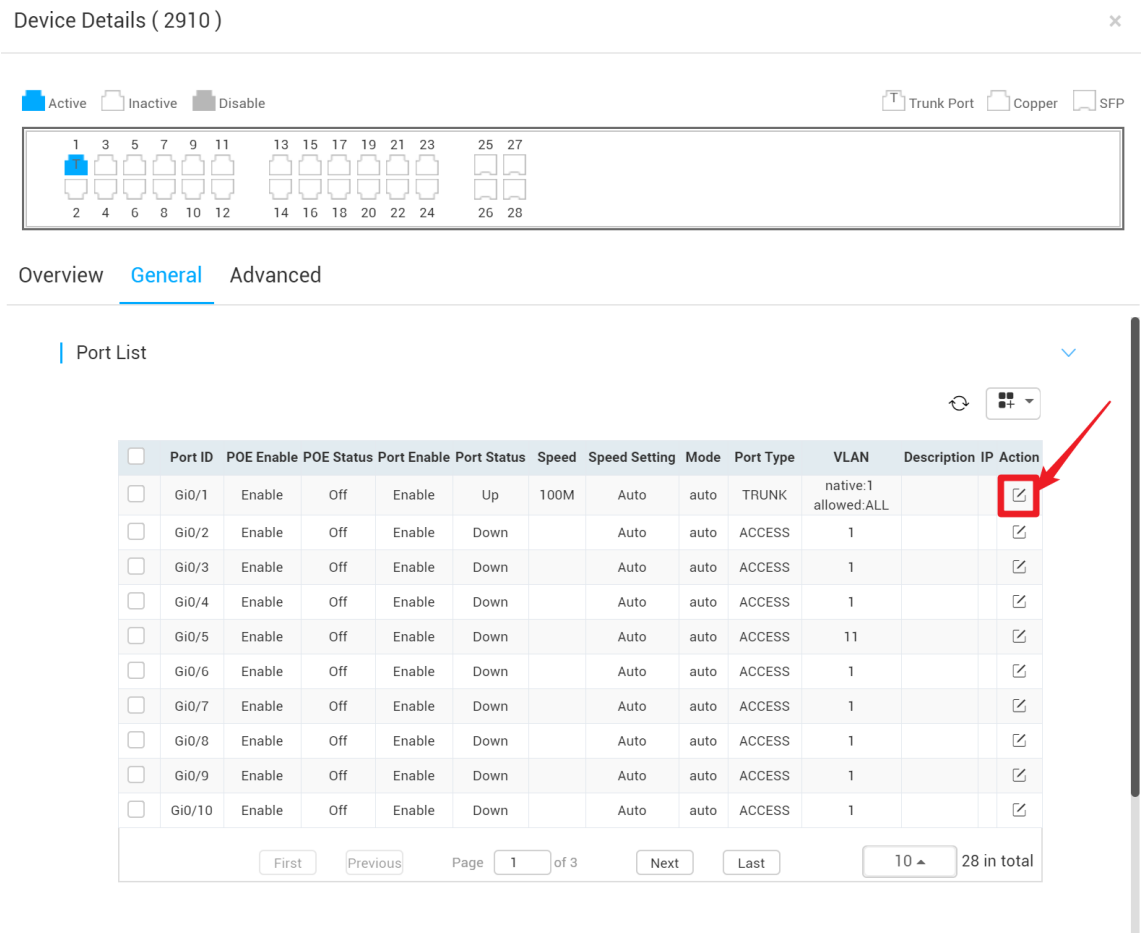
2) Click **General** or **Advanced** to configure the switch.



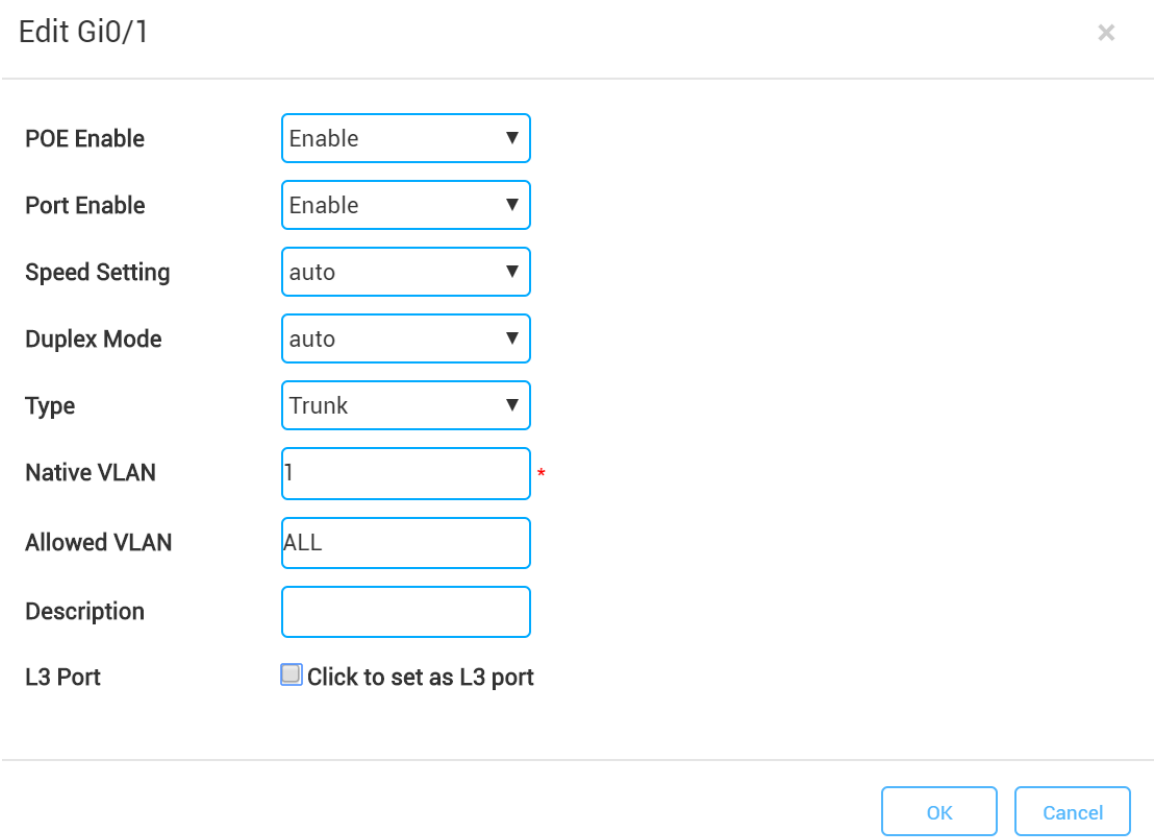
7.2.1. Port Setting

Port setting enables user to manage switch interface, including port status, speed, VLAN and SVI.

1) Click edit button on **General** page of device detail.

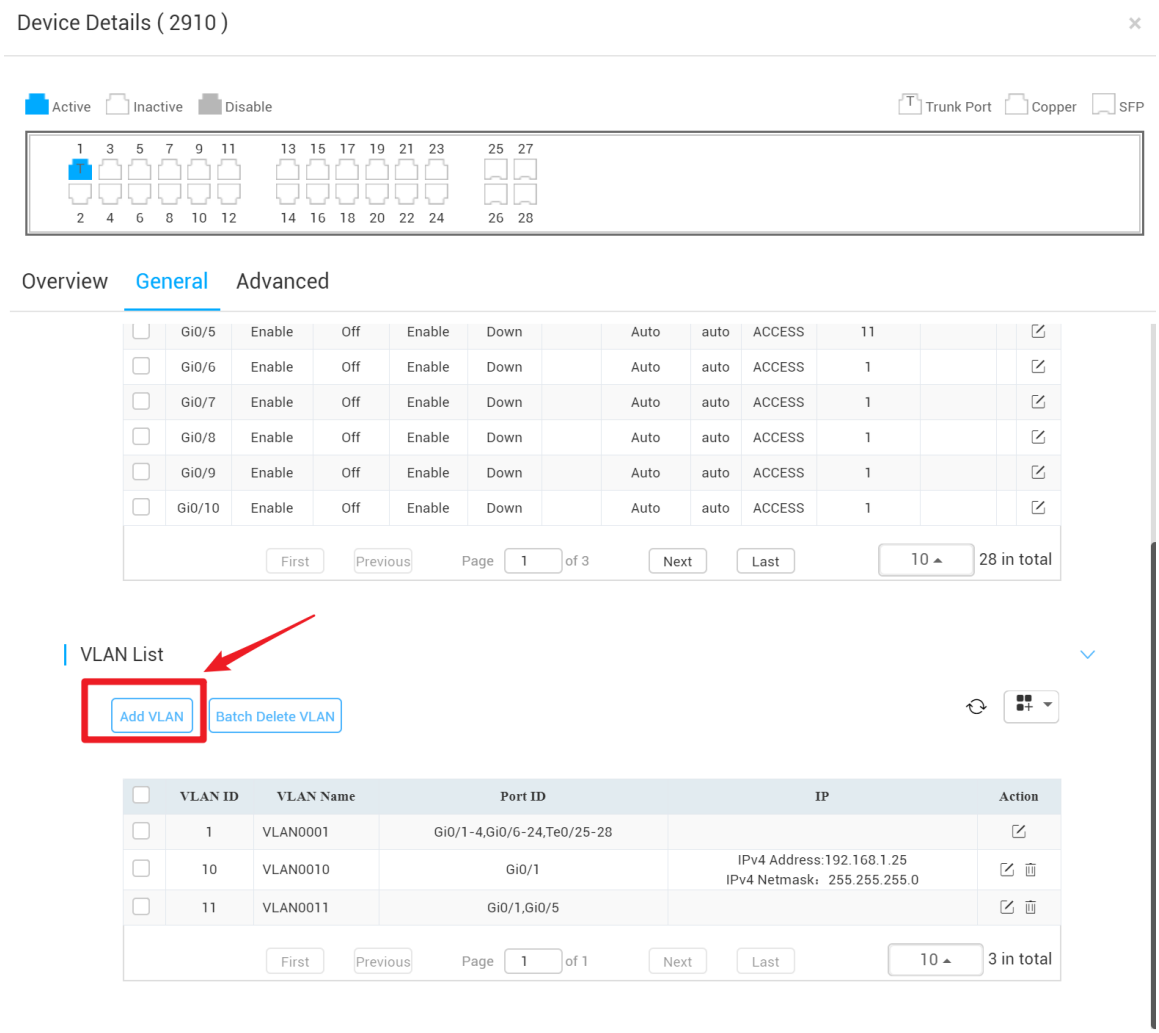


2) Modify interface setting as required.

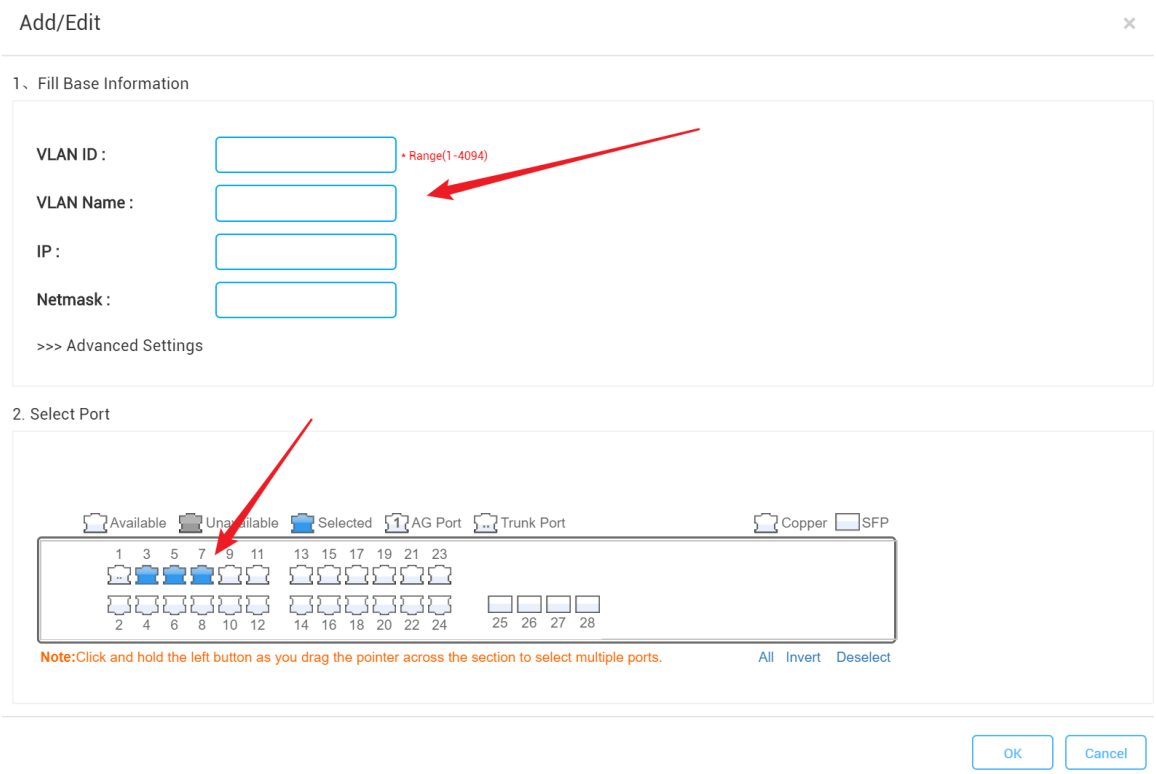


7.2.2. VLAN Setting

1) Click Add VLAN to create VLAN/SVI.

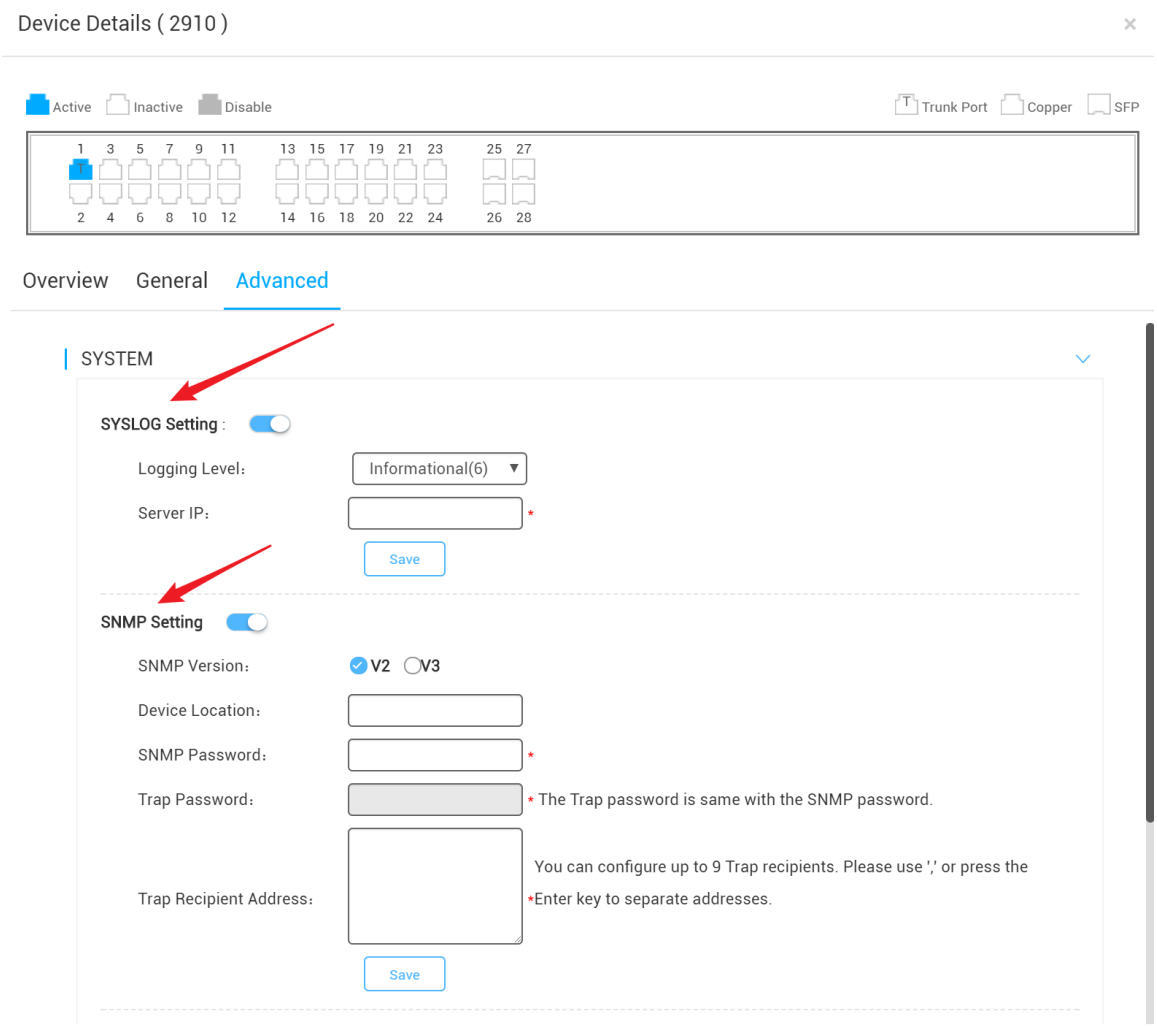


2) Fill in VLAN info and bind to corresponding interface.



7.2.3. Advanced Setting

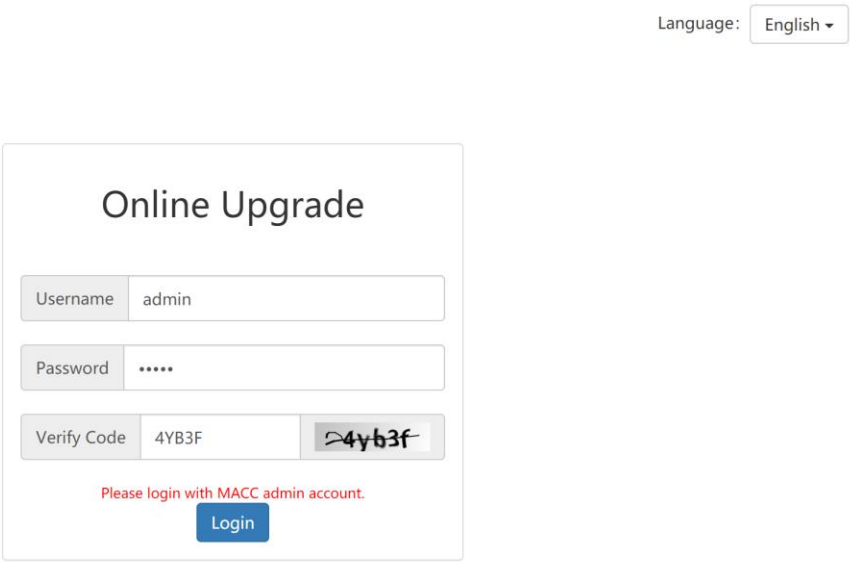
The advanced setting for switch includes system log, SNMP, NTP, DNS, NFPP and IGMP snooping.

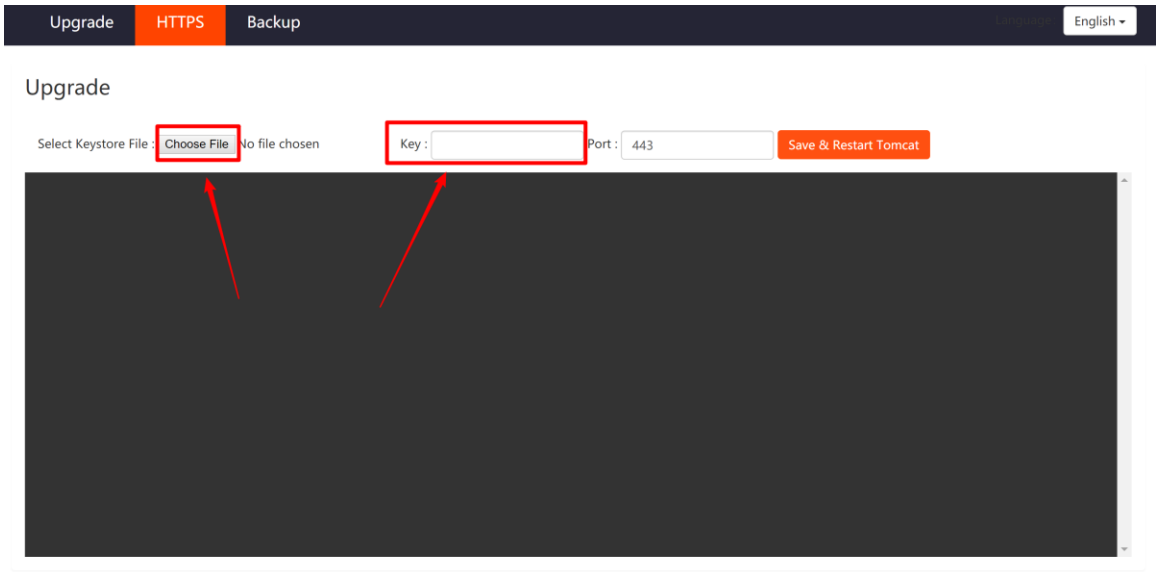


8. Maintenance & Upgrade

8.1. HTTPS Certification Import

Login MACC-BASE back-end system(*HTTP://MACC-IP:8090*) and click **HTTPS** to import custom HTTPS certification to HTTPS access.

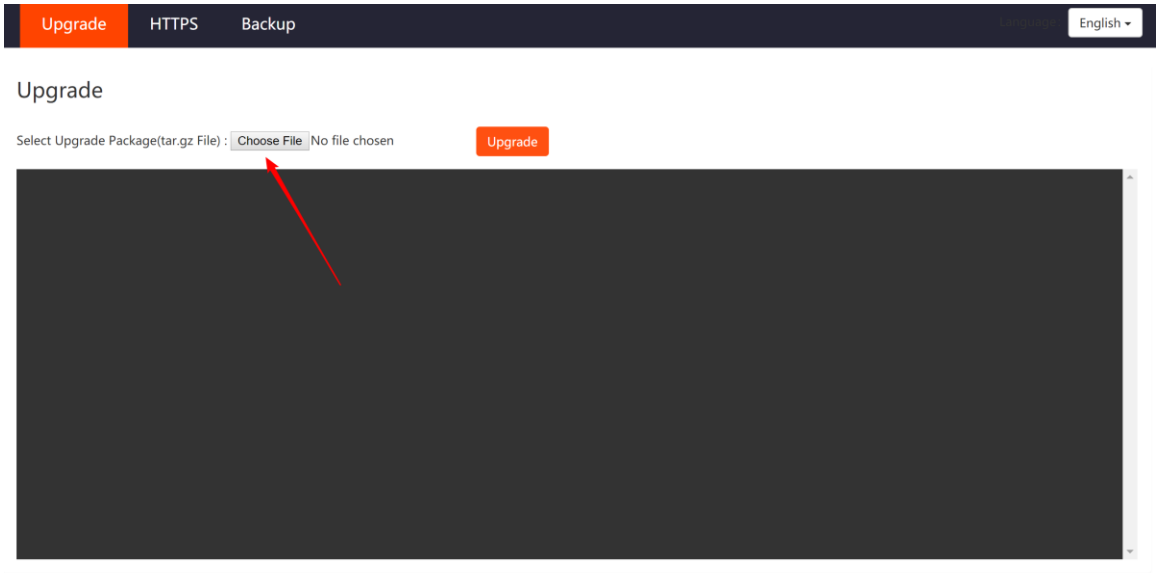




⚠ The key value is the private key of SSL certificate.

8.2. MACC-BASE Firmware Upgrade

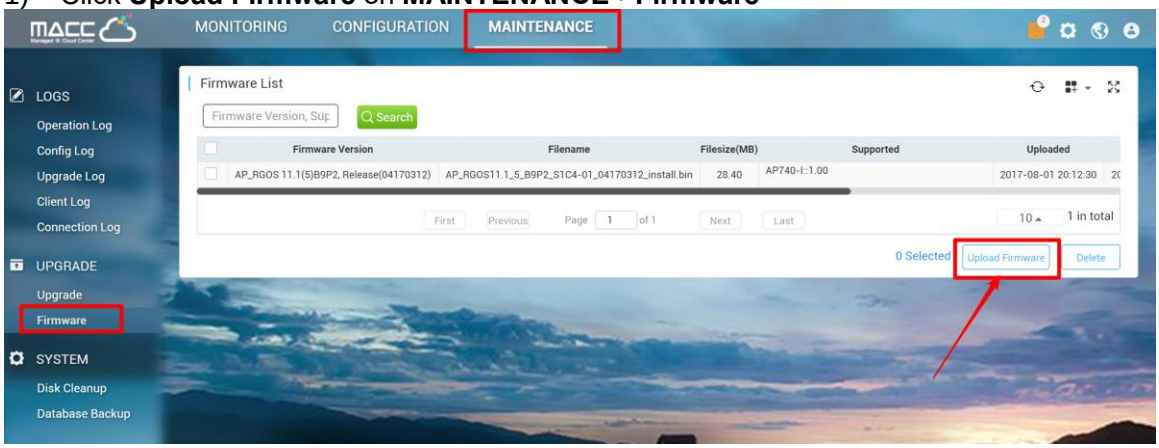
Login MACC-BASE back-end system(*HTTP://MACC-IP:8090*) and click **Upgrade** to import tag.gz format file to upgrade MACC-BASE. It will take around 30 minutes to finish upgrade process.



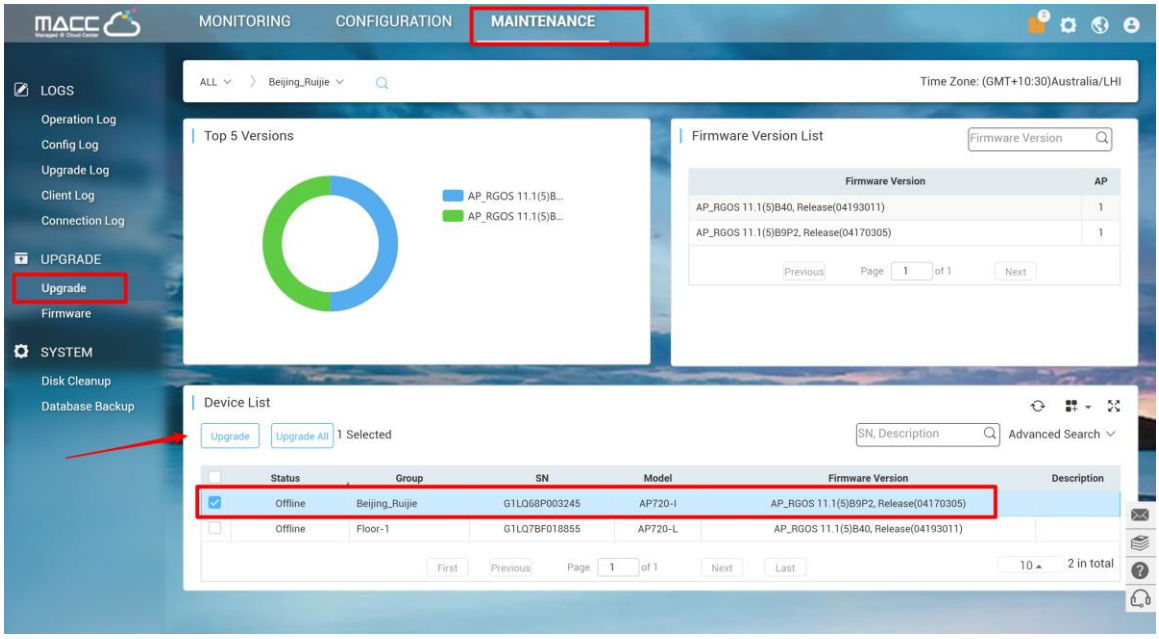
AP Firmware Upgrade

MACC-BASE can manage all devices firmware version (Access Point, Switch) through WEB UI and enables admin user maintain devices software easily.

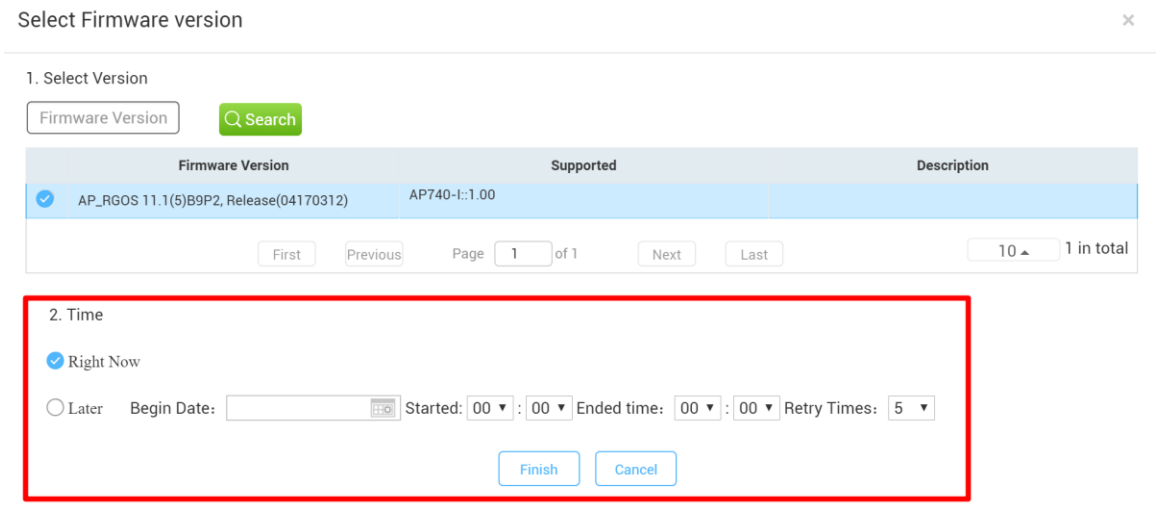
1) Click **Upload Firmware** on **MAINTENANCE->Firmware**



2) Select designated device to upgrade firmware version on Upgrade page and click **Upgrade**.



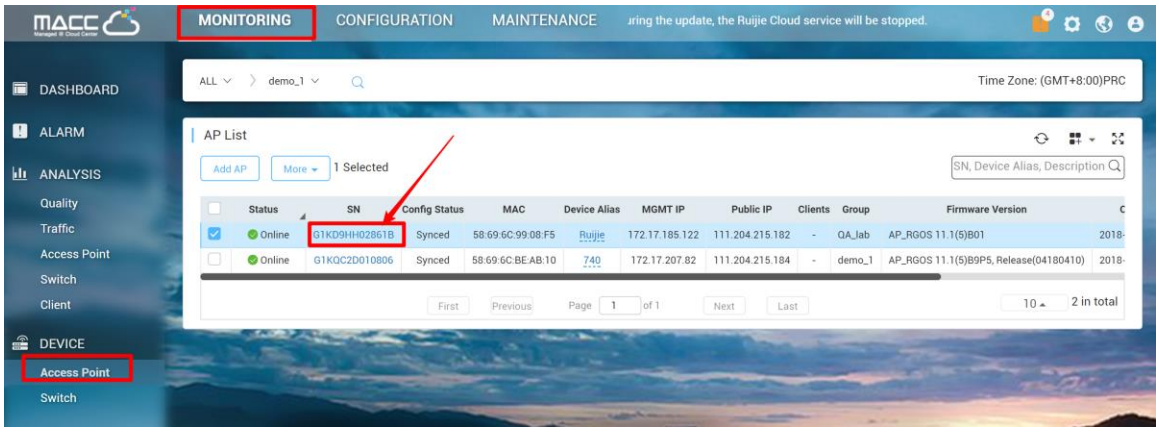
3) Choose schedule upgrade or execute the upgrade immediately.

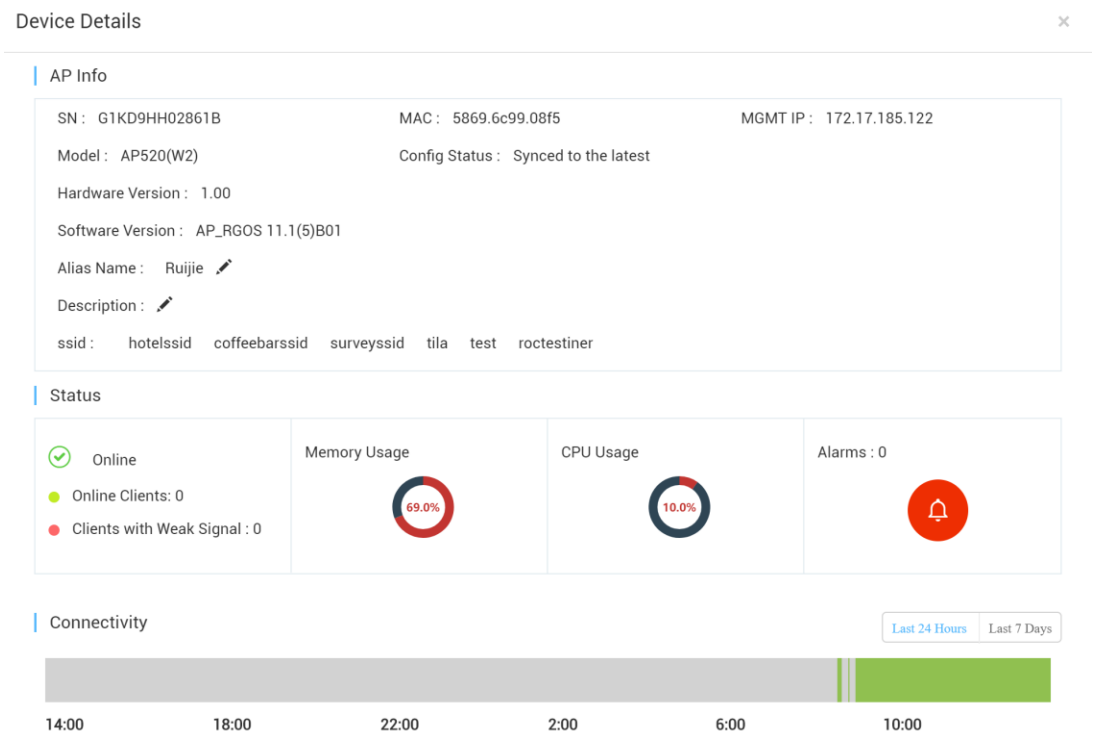


8.3. Monitoring

8.3.1. AP/MTFI Status

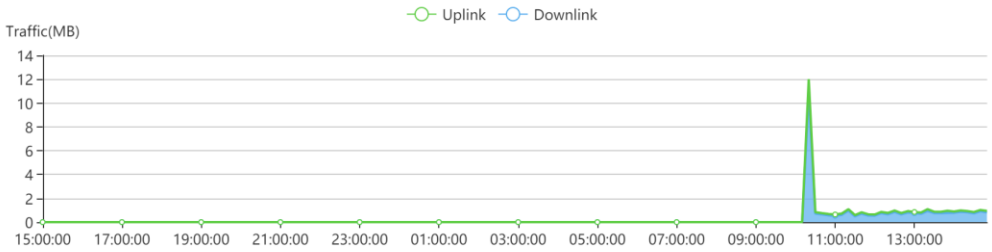
Click Access Point serial number to monitor AP running status, including AP info, CPU & Memory usage, connectivity record, traffic, RF setting and interference.


MONITORING
CONFIGURATION
MAINTENANCE
DASHBOARD
ALARM
ANALYSIS
Quality
Traffic
Access Point
Switch
Client
DEVICE
Access Point
Switch
Time Zone: (GMT+8:00)PRC
AP List
Add AP
More
1 Selected
SN, Device Alias, Description
Status
SN
Config Status
MAC
Device Alias
MGMT IP
Public IP
Clients
Group
Firmware Version
Online
G1KD9HH02861B
Synced
58:69:6C:99:08:F5
Ruijie
172.17.185.122
111.204.215.182
QA_lab
AP_RGOS 11.1(5)B01
Online
G1KQC2D010806
Synced
58:69:6C:BE:AB:10
740
172.17.207.82
111.204.215.184
demo_1
AP_RGOS 11.1(5)B9P5, Release(04180410)
First
Previous
Page 1 of 1
Next
Last
2 in total


Device Details
AP Info
SN : G1KD9HH02861B
MAC : 5869.6c99.08f5
MGMT IP : 172.17.185.122
Model : AP520(W2)
Config Status : Synced to the latest
Hardware Version : 1.00
Software Version : AP_RGOS 11.1(5)B01
Alias Name : Ruijie
Description :
ssid : hotelssid coffeebarssid surveyssid tila test roctestiner
Status
Online
Online Clients: 0
Clients with Weak Signal : 0
Memory Usage
69.0%
CPU Usage
10.0%
Alarms : 0
Connectivity
Last 24 Hours
Last 7 Days
14:00
18:00
22:00
2:00
6:00
10:00

Traffic Summary

Last 24 Hours | Last 7 Days



Radio List

RF Type	Channel	Power	Bandwidth（MHz）	Channel Usage(%)
2.4G	1	20%	20	59%
5G	149	20%	40	19%

Client List

IP	MAC	SSID	RSSI	Band	Traffic（MB）	OS	Manufacturer	Up	Down
No matching records found									

First Previous Page 0 of 0 Next Last 10 0 in total

Adjacent RF Signal

Triggered: 2016-11-21 16:00 **Ended:** 2016-11-21 16:11 **Status:** Complete

BSSID	Radio	Adjacent SSID	Adjacent Channel	RSSI	Adjacent SN	Adjacent MAC	Uploaded
0669.6c5b.5034	Radio2(5G)	zxkart	149	81	G1KD14G002056	5869.6c5b.5031	2016-11-21 16:11
0669.6c54.8d17	Radio1(2.4G)	Eweb_8D151	1	76	G1JDB1P031399	5869.6c54.8d15	2016-11-21 16:11
0669.6c5b.4fd7	Radio1(2.4G)	Ruijie_FREE.WiFi-Leon	1	75	G1KD14G001828	5869.6c5b.4fd5	2016-11-21 16:11
0a69.6c5b.4fd7	Radio1(2.4G)	Staff	1	75	G1KD14G001828	5869.6c5b.4fd5	2016-11-21 16:11
0669.6c7a.5dd2	Radio1(2.4G)	Eweb_5DD01	1	73	G1KD84Y017646	5869.6c7a.5dd0	2016-11-21 16:11
0669.6c99.2b67	Radio1(2.4G)	New-1	1	71	G1KD9HH050650	5869.6c99.2b65	2016-11-21 16:11
1669.6c99.2b67	Radio1(2.4G)	test-5	1	71	G1KD9HH050650	5869.6c99.2b65	2016-11-21 16:11
0669.6c85.82d5	Radio1(2.4G)	SanTest1	6	69	G1KD54Z00410B	5869.6c85.82d2	2016-11-21 16:11
0669.6c7a.5dd3	Radio2(5G)	Eweb_5DD01	149	68	G1KD84Y017646	5869.6c7a.5dd0	2016-11-21 16:11
0669.6c5b.4fd8	Radio2(5G)	Ruijie_FREE.WiFi-Leon	149	66	G1KD14G001828	5869.6c5b.4fd5	2016-11-21 16:11

First Previous Page 1 of 8 Next Last 10 77 in total

Scan Adjacent RF

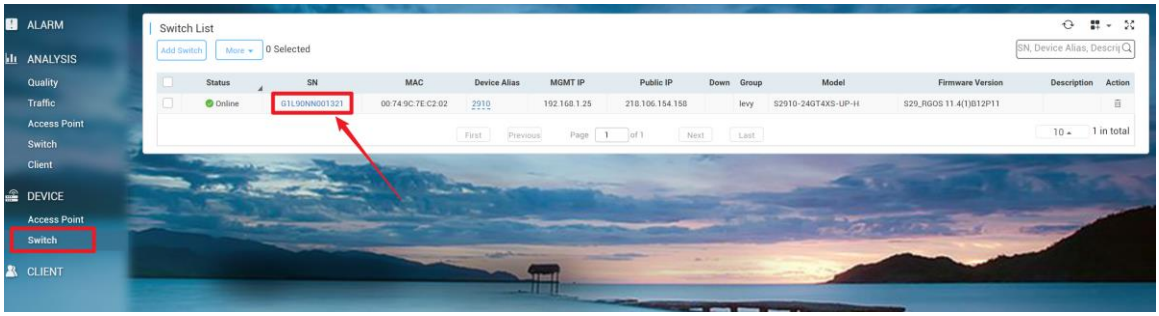
Device Log

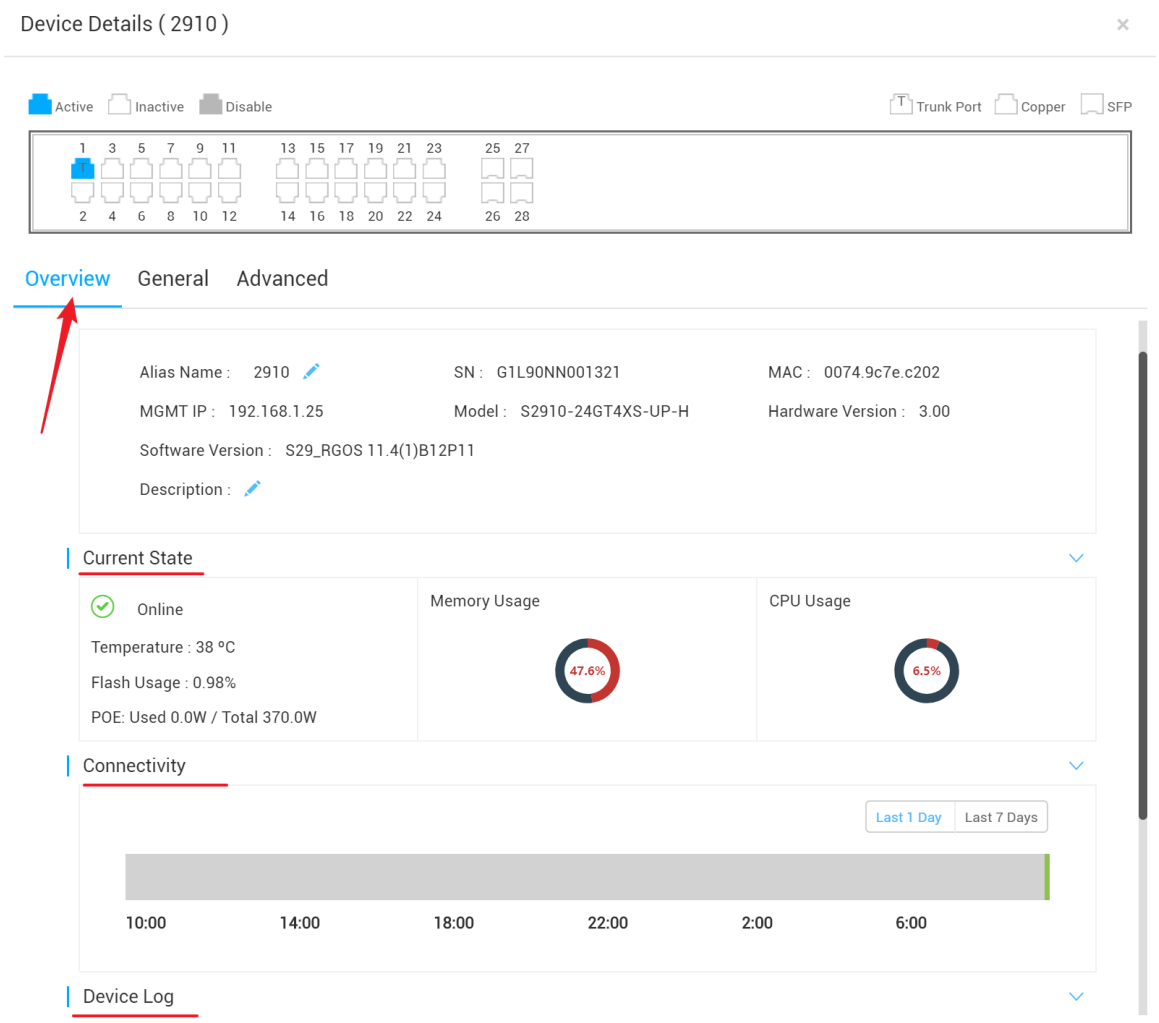
All Days | Search

Type	Updated On	Content
Online/Offline	2018-02-07 10:13:00	Device online
Online/Offline	2018-02-07 10:04:00	Device offline
Online/Offline	2018-02-07 10:02:23	Device online
Online/Offline	2018-02-07 09:53:00	Device offline

8.3.2. Switch Status

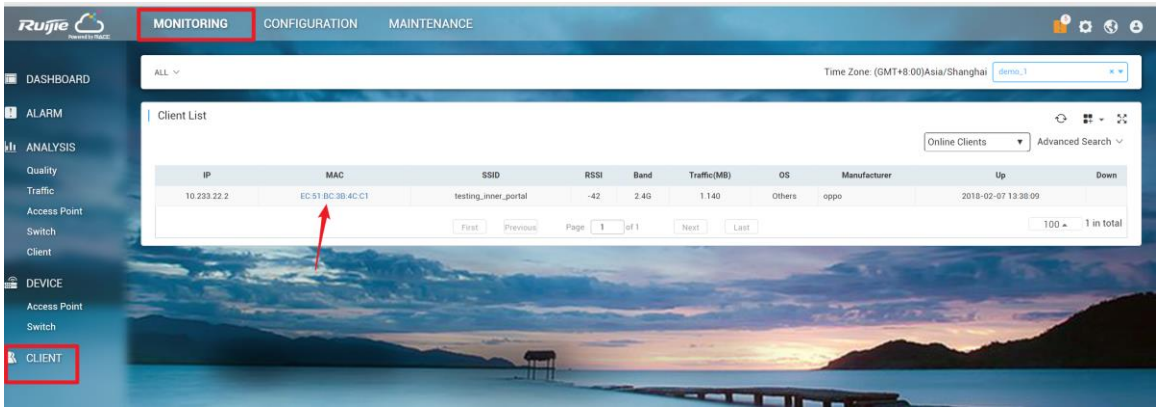
Click Switch serial number on switch list to monitor AP running status, including switch info, port status, CPU & Memory usage, connectivity record, traffic, device log.





8.3.3. STA Status

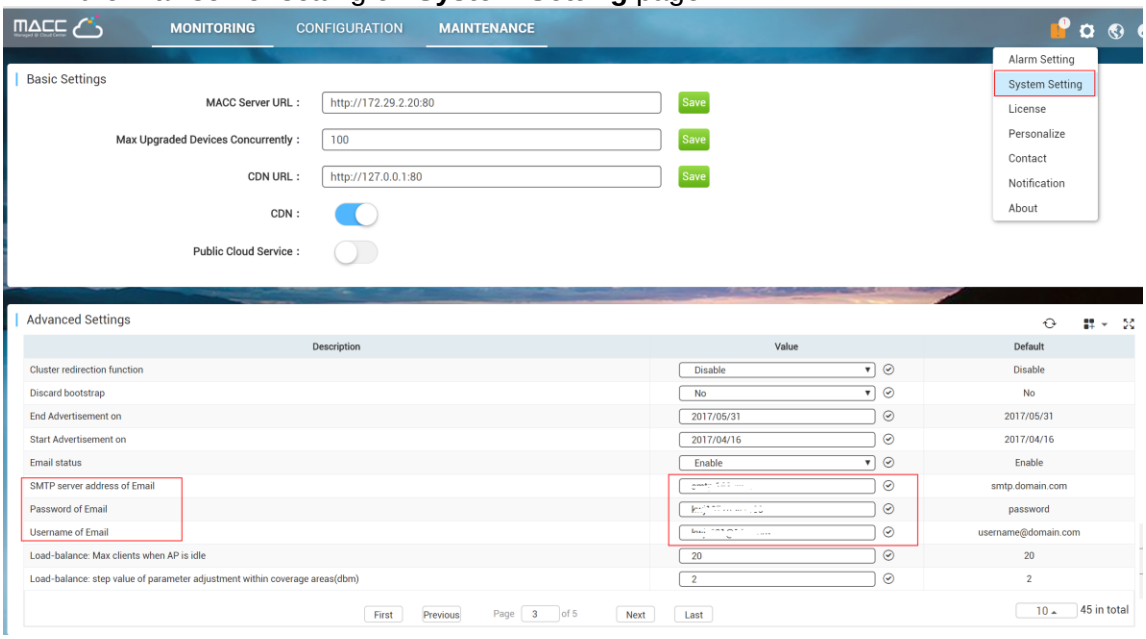
Click client mac address to view client details, including client info, traffic, delay, RSSI and connect record.



8.4. Alarm Setting

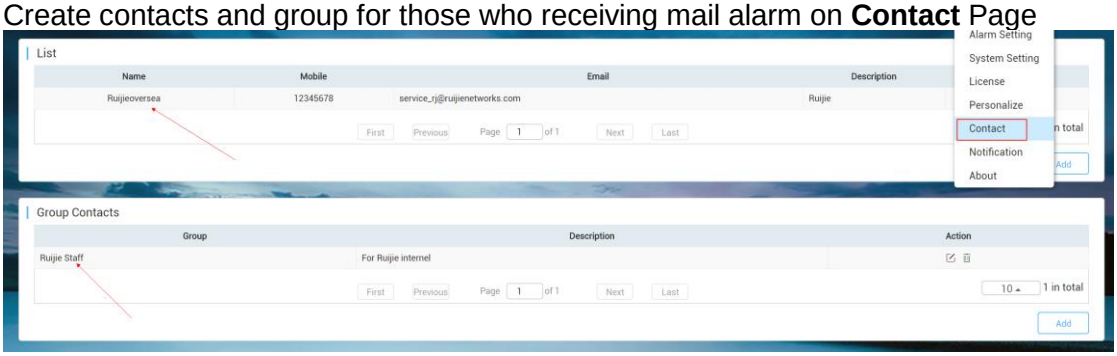
MACC supports AP exception alarm function, when AP offline, working on high channel utilization, AP state unstable, it will trigger the mail alarm function on MACC-BASE.

1) Fill in the mail server setting on **System Setting** page.

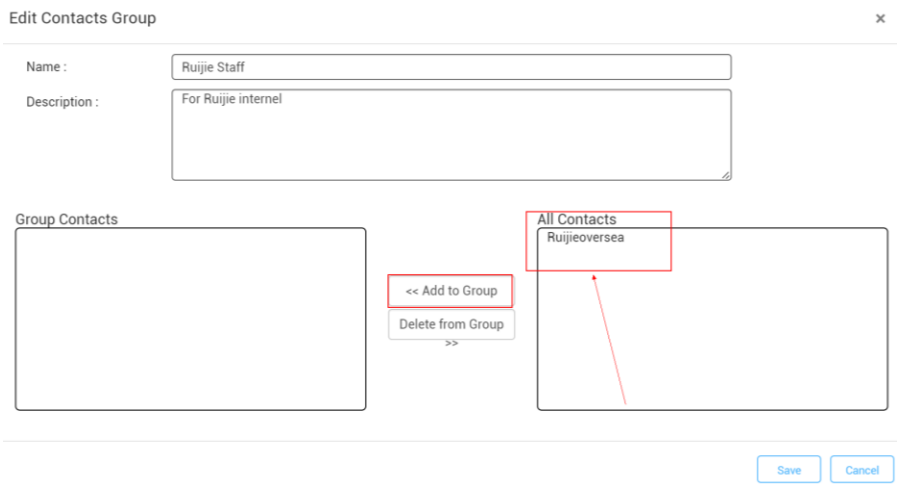


2) Enable the alarm function and turn on the mailing function on **Alarm Setting**.

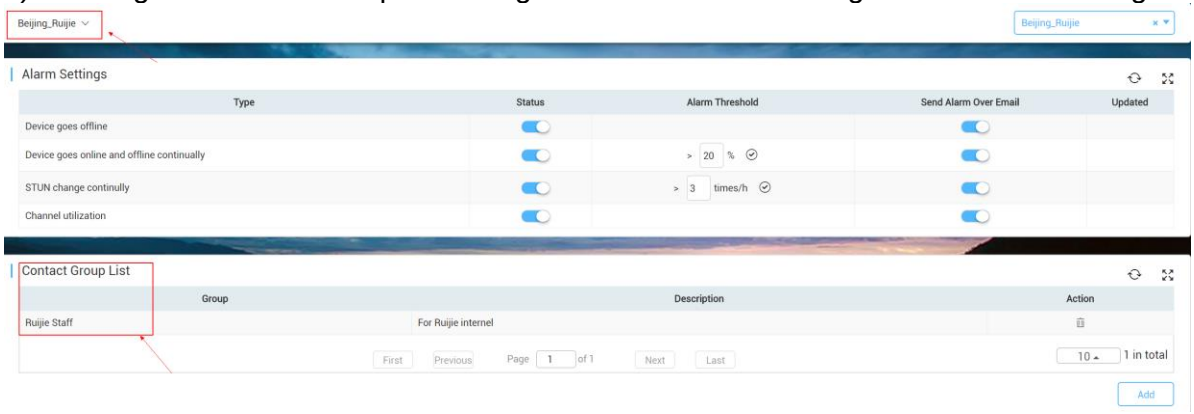
3) Create contacts and group for those who receiving mail alarm on **Contact** Page



4) Edit the **Group Contacts** and Add the contacts into this group.



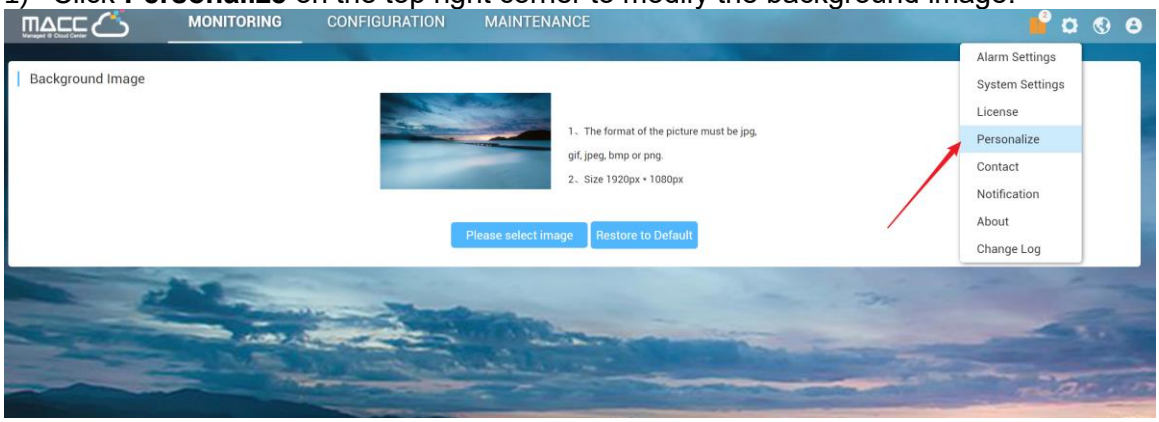
5) Binding the Contact Group to this organization on alarm settings and save the setting.



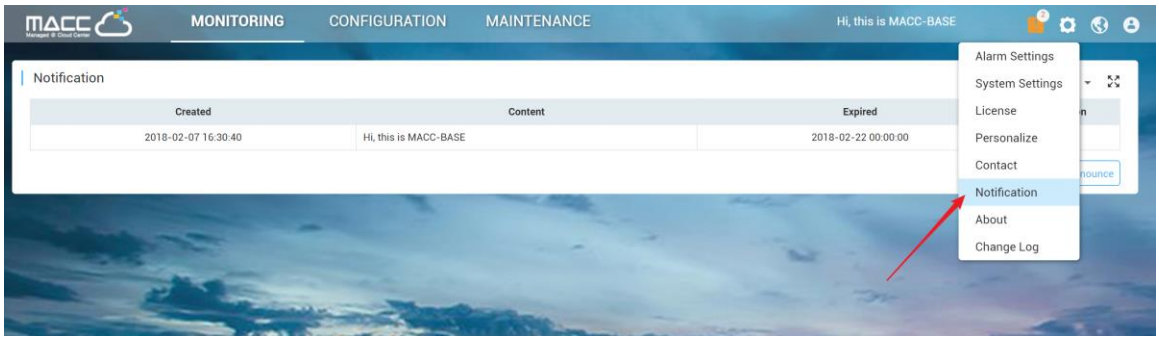
8.5. Customization

User can customize MACC-BASE background image and notification message on MACC-BASE.

1) Click **Personalize** on the top right corner to modify the background image.



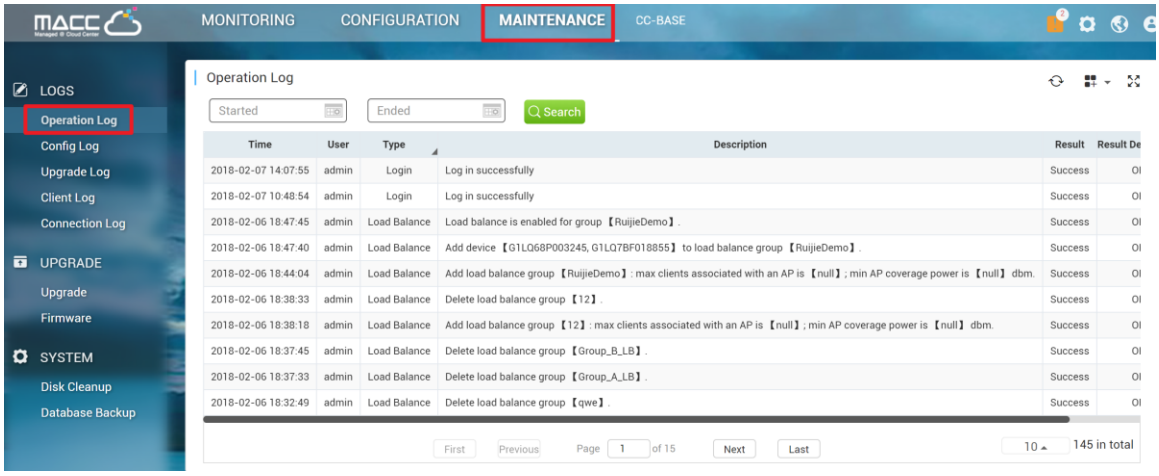
2) Add a prompt message on **Notification** page.



8.6. Log

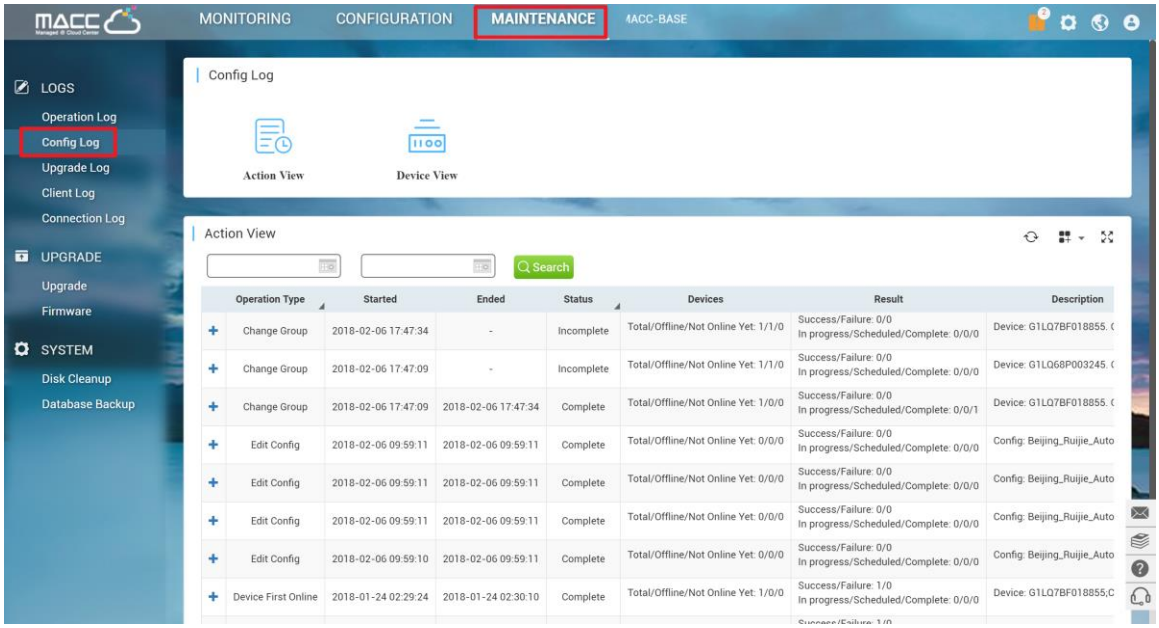
8.6.1. Operation Log

Operation Log records all operation info.



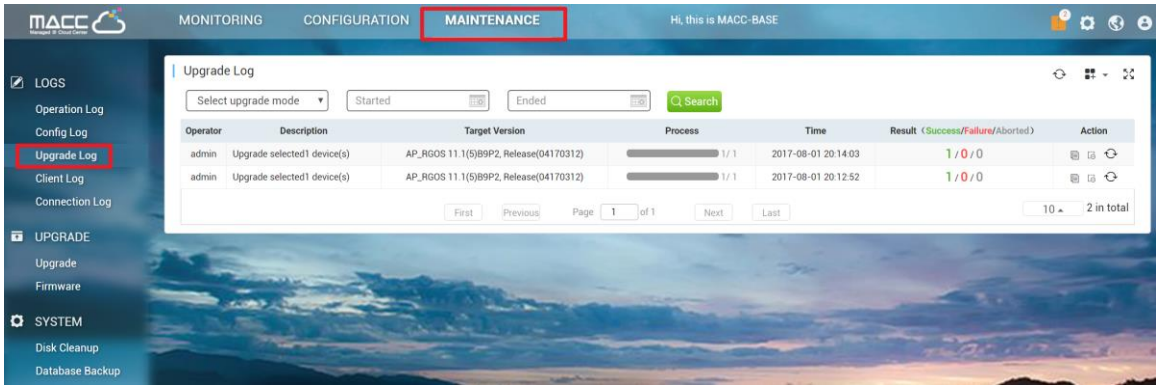
8.6.2. Config Log

Config Log lists down the status of device configuration. If the device stucks on not sync state, user can check the configuration delivery status by clicking the detail button.



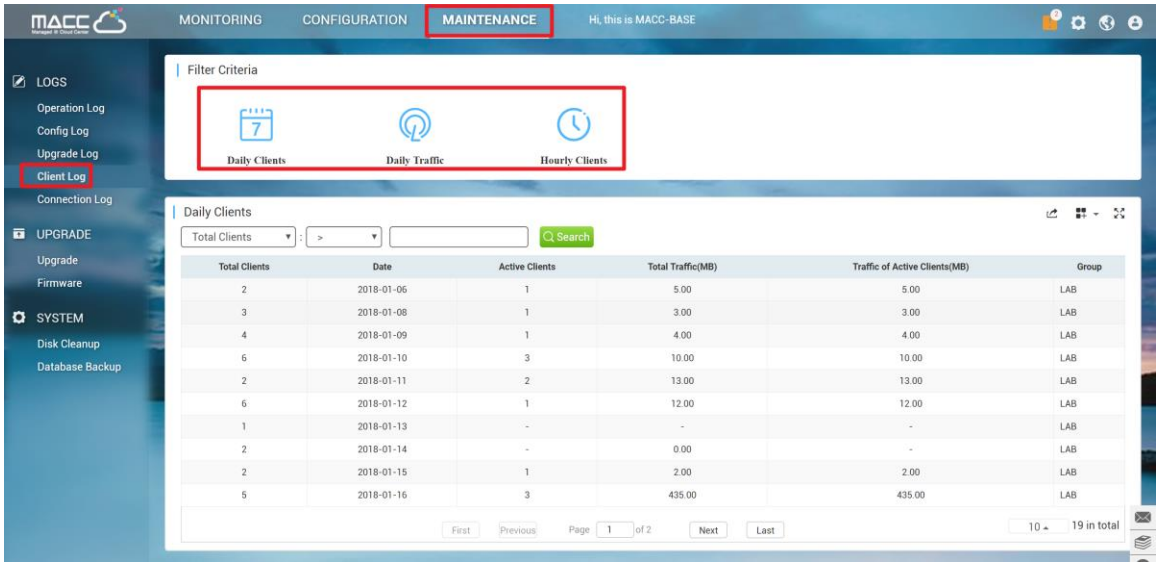
8.6.3. Upgrade Log

Devices firmware upgrade history will be listed on this page.



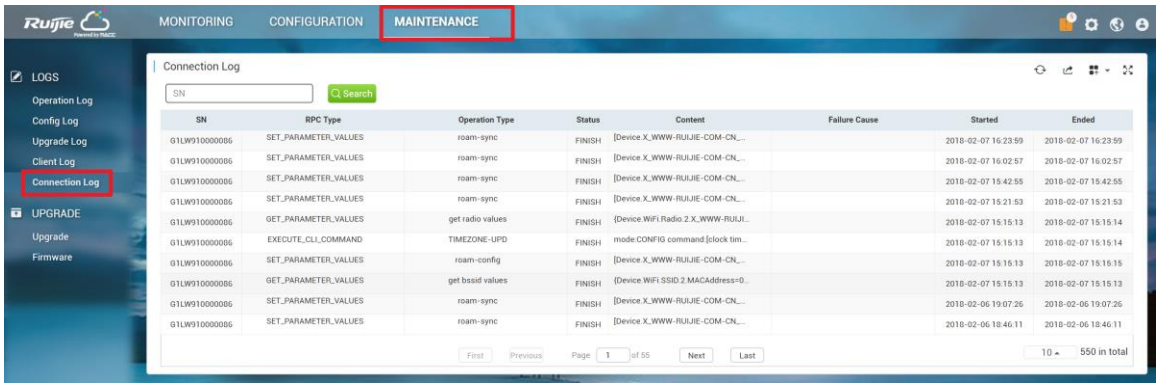
8.6.4. Client Log

Client History logs in client log page, and user can export client info base on days, traffic, hours.



8.6.5. Connection Log

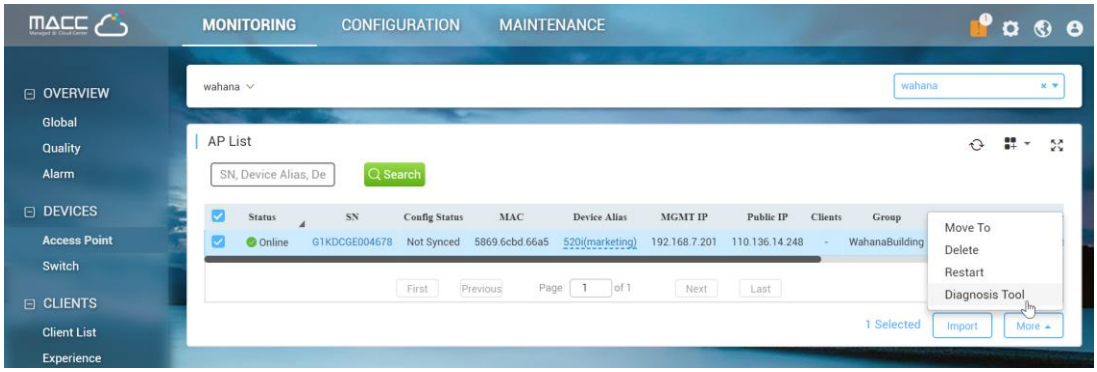
Connection Log is the connection record between MACC-BASE and managed devices. If the device is abnormal, it's recommended to check connection history on this page.



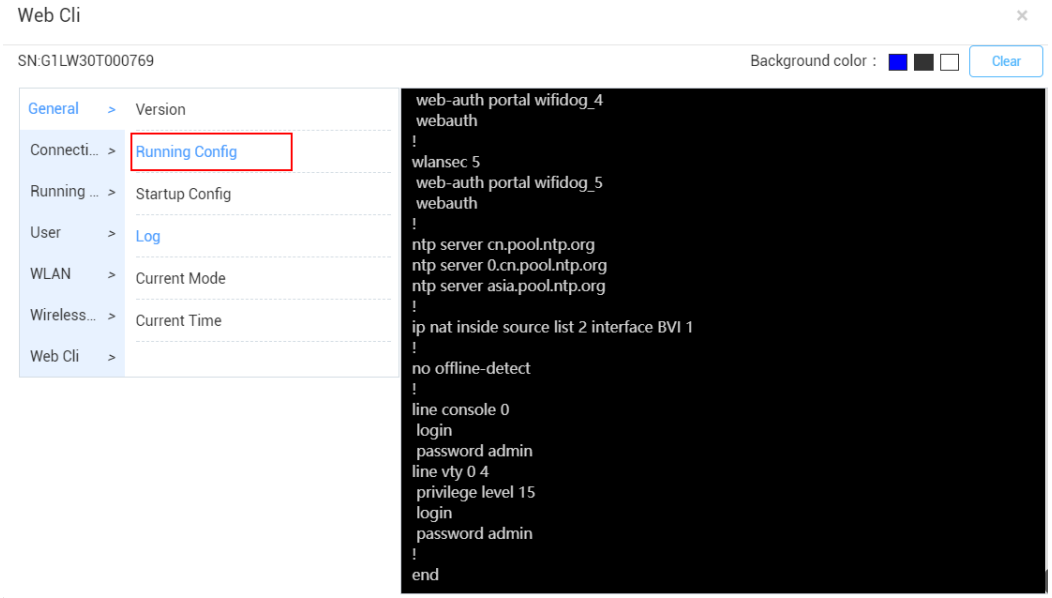
8.7. Diagnosis Tool

MACC supports Advanced troubleshooting, CLI access to devices to perform advanced debugging.

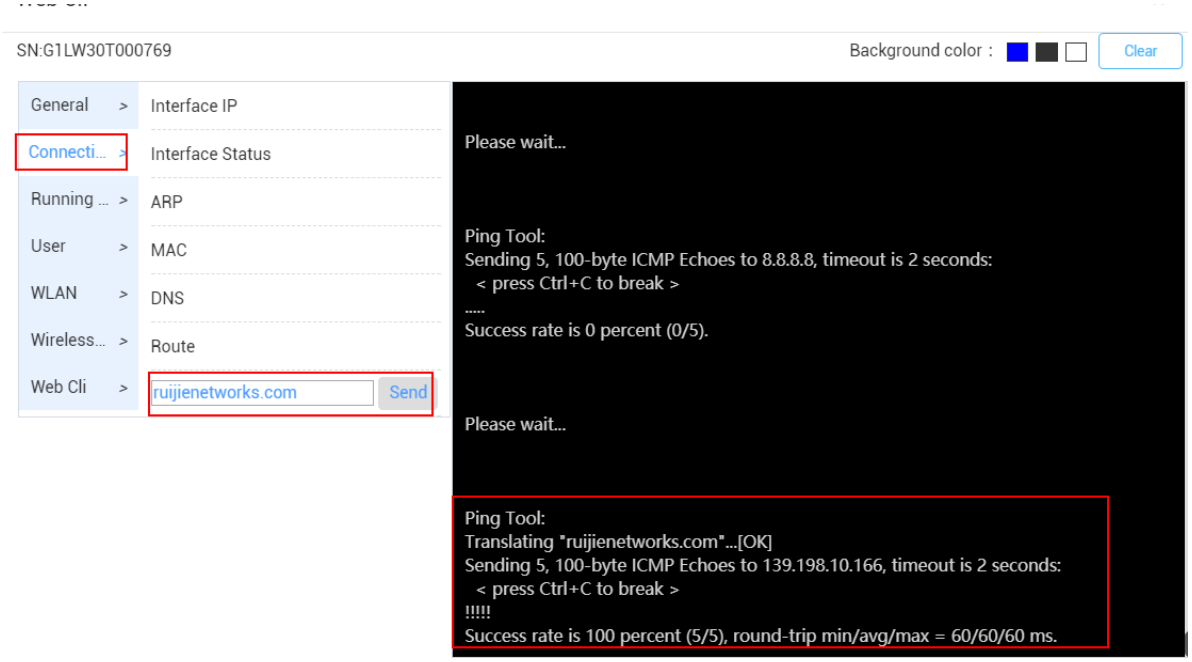
1) Go to **Monitoring Page** > Access Point /Switch. Click **More** and select **Diagnosis Tool**.



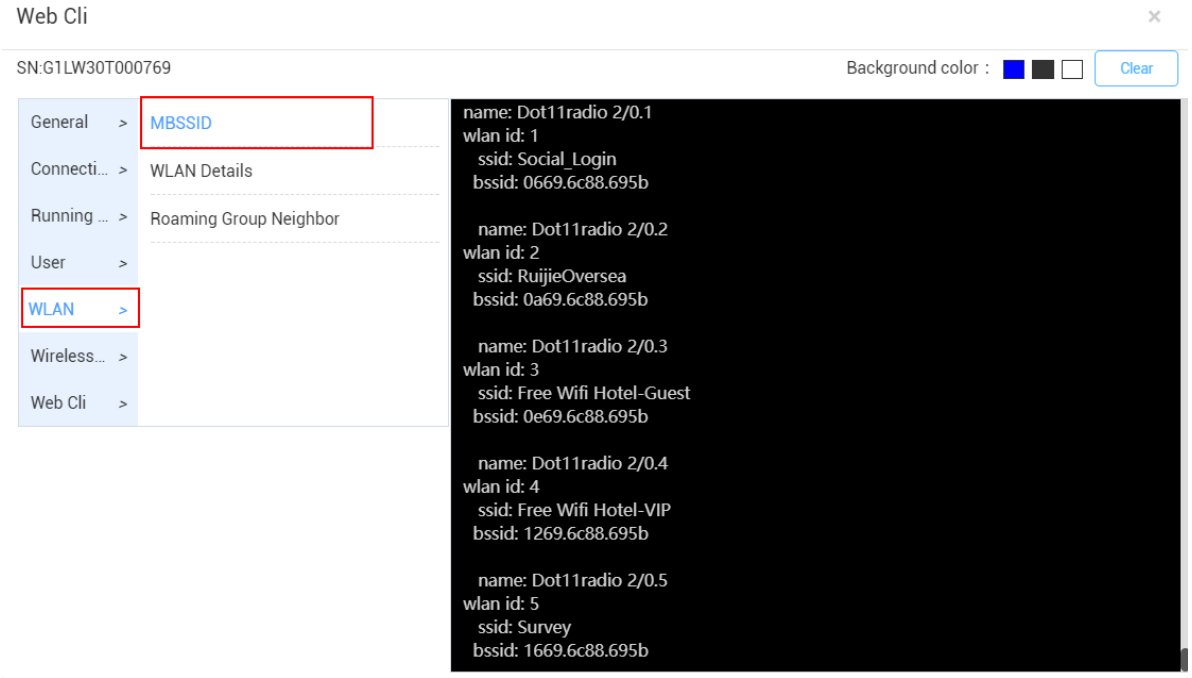
2) Use “General->Running Config” to verify the AP setting.



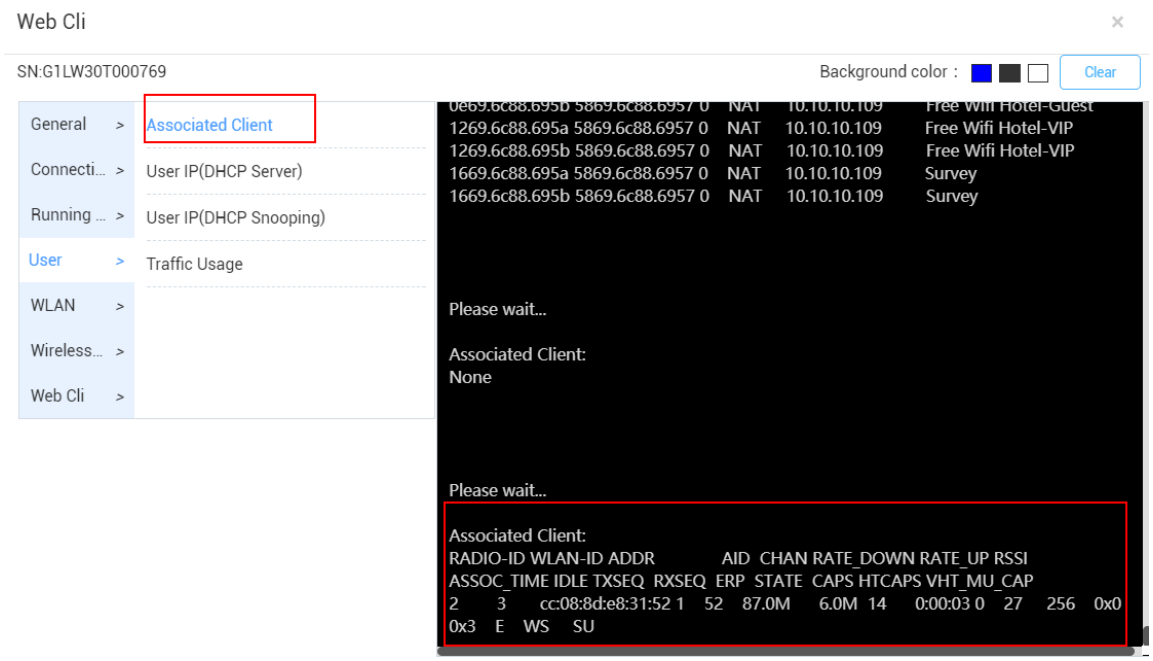
3) Use “Connection->Ping tool” to check the Internet connectivity.



4) Use “WLAN->MBSSID” to verify the broadcast SSID



5) Use “User->Associated Client” to check the online user.



9. FAQ-Frequency Asked Questions

Deployment

What should I check if MACC-BASE service is not running after installation?

Follow below checklist to ensure each item meet the requirement.

- Centos OS version: CentOS-7-x86_64-Minimal-1511.iso
- Physical/Virtual platform meet minimum hardware resource
- Port Mapping is required in NAT environment, refer *MACC-BASE installation guide*
- Disable built-in firewall on Cent OS: *systemctl disable firewalld.service*
- Restart follow services with Linux commands on console or restart the server
  - **tomcat:** *./macc/install/tomcat/bin/startup.sh*
  - **mysqld:** *service mysql start*
  - **mongod:** *mongod -f /etc/mongod.conf*
  - **redis:** *redis-server /etc/redis/redis.conf*
  - **zookeeper:** *./macc/install/zookeeper-3.4.9/bin/zkServer.sh start*
  - **activemq:** *./macc/install/apache-activemq-5.13.1/bin/activemq start*
- Collect services running log on server. Folder path is /tmp/ServiceMonitor.log

If above checklist cannot solve your problem, please contact Ruijie support.

How can I change the system time on MACC-BASE?

User can select designated time zone when creating device group, but the system time in MACC-BASE is relied on CentOS system. The following link will show you how to change the system time under CentOS.

http://www.putorius.net/2015/04/setting-time-and-date-in-red-hat-7.html

The URL of MACC-BASE will redirect to intranet IP with SSO when I access from Internet.

MACC-BASE is enabled SSO by default and which only allow user access the WEB service from unique entrance. We provide a script to change related settings If user needs to NAT WEB service to Internet or modify SSO URL/IP address.

1) Download the script from below link.
https://unifi.ruijiecloud.com/index.php/s/rQ2RVLFGrL4g1X3

2) Upload to CentOS server and authorize exec permission.

```
[root@localhost macc]# ls
cas.log  cdata  config_sso_final.sh  config_sso.sh  data  img  install  logback  logs  mysql  perfStats.log
[root@localhost macc]# chmod 777 config_sso.sh
[root@localhost macc]# _
```

Command: *chmod 777 config_sso.sh*

3) Execute the script and follow the prompts to complete SSO setting.

```
[root@localhost macc]#
[root@localhost macc]# ./config_sso.sh
config SSO...
If you want to open SSO, Please enter "y", else enter "n" not use SSO, Cancel enter other letter.
```

Command: *./config_sso.sh*

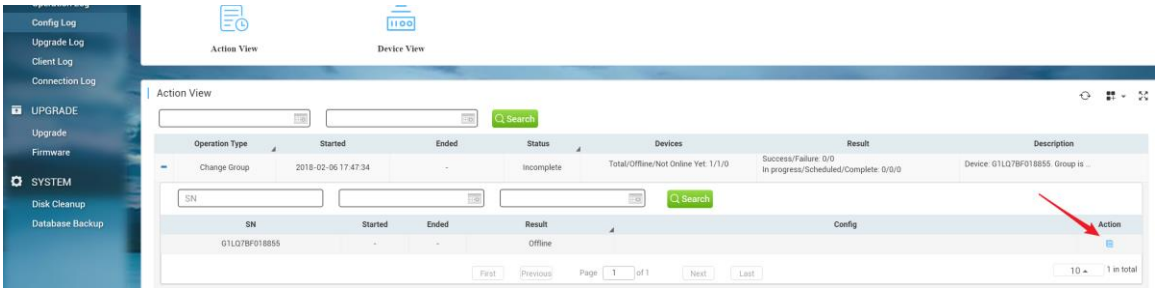
Why my AP cannot go online on MACC-BASE?

- Verify the MACC server URL on **System Setting**->**Basic Settings** with super admin account. The URL should point to MACC-BASE server IP address.
- Ensure devices (AP and Switch)'s versions are up to date.
- Connectivity between APs and MACC-BASE (Port:80/443), internet access and DNS setting are required.
- Verify whether the device's serial number was added to MACC-BASE or not.
- Use command "show cwmp config" on device's CLI and check whether the CWMP URL and CWMP Interval(180s) are correct.

Configuration

The AP is online but stuck on “Not Synced” status.

- Ensure devices (AP and Switch)’s versions are up to date.
- Use command “show cwmp config” on device’s CLI and check whether the CWMP URL and CWMP Interval(180s) are correct.
- Check the setting push status on **MAINTENANCE->Config Log**. And click detail for execution status.



If above steps cannot solve the problem, you can use command perform factory-reset for testing.

Command: *AP(config)#apm factory-reset*

Wireless STA shows IP address “0.0.0.0” on Client List

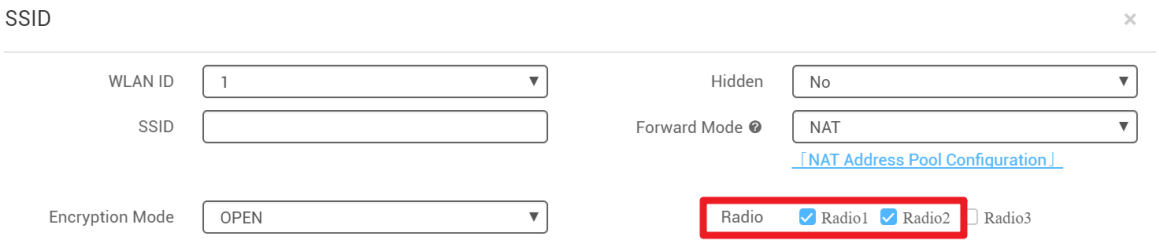
There are 2 possibilities may cause this problem:

- No traffic flow upload to AP after client connected
- It will take around 5 minutes to refresh the data on MACC-BASE

Could MACC-BASE support multi-tenant?

By default, the multi-tenant function on MACC-BASE is disabled, customer can contact Ruijie Support to enable this feature if needs. And MACC-BASE supports multi-account to manage organization.

How to choose 2.4GHz and 5GHz Radio interface for Access Point?



- Radio 1 represent 2.4GHz
- Radio 2 represent 5GHz

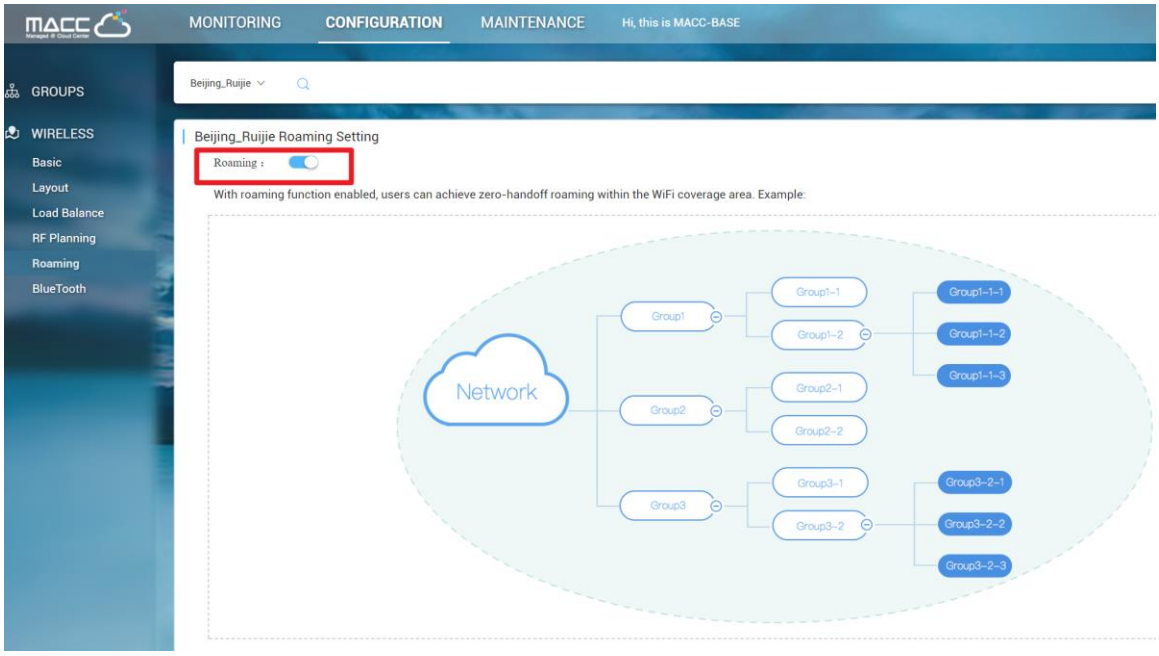
How to disable WEB portal page after user roaming to other APs?

In WEB authentication scenario, user can enable “Seamless Online” function on SSID page for seamless roaming.

Wireless STA cannot roam to other APs.

The MACC-BASE is enabled L2(same subnet) roaming by default.

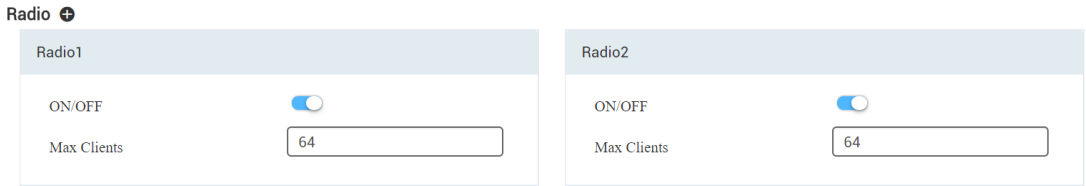
For SSID in NAT mode or L3 roaming, it’s required to select “**NAT Roaming Address Pool Configuration**” for roaming DHCP pool and enable Roaming feature on **Wireless-Roaming** page.



From AP's log, reaching the maximum online number of radio and STA cannot go online.

```
*Mar  1 11:33:34: %WLAN-6-OUTPUT: STA(b8bc.1b6a.fa5b) actives in BSSID(0a69.6cb9.7a43): Auth succeed.
*Mar  1 11:33:34: %WLAN-6-80211N: STA(b8bc.1b6a.fa5b) fails to active in BSSID(0a69.6cb9.7a43): STA is rejected by access control, status code(17).
*Mar  1 11:33:35: %WLAN-6-OUTPUT: STA(6476.bab5.9fb4) actives in BSSID(0a69.6cb9.7a43): Auth succeed 20 times in 45 seconds.
*Mar  1 11:33:35: %WLAN-6-80211N: STA(6476.bab5.9fb4) fails to active in BSSID(0a69.6cb9.7a43): STA is rejected by access control,and STA attamp to asso
 20 times in 45 seconds, status code(17).
*Mar  1 11:33:36: %WLAN-6-OUTPUT: STA(3cb6.b70d.14a6) actives in BSSID(0a69.6cb9.7a43): Auth succeed.
*Mar  1 11:33:36: %WLAN-6-OUTPUT: STA(3cb6.b70d.14a6) actives in BSSID(0a69.6cb9.7a43): Reasso succeed.
*Mar  1 11:33:37: %WLAN-6-OUTPUT: STA(a888.0867.4e56) actives in BSSID(0a69.6cb9.7a43): Auth succeed.
*Mar  1 11:33:37: %WLAN-6-80211N: STA(a888.0867.4e56) fails to active in BSSID(0a69.6cb9.7a43): STA is rejected by access control, status code(17).
*Mar  1 11:33:39: %WLAN-6-OUTPUT: STA(842e.270b.8a50) actives in BSSID(0a69.6cb9.7a43): Auth succeed.
*Mar  1 11:33:39: %WLAN-6-80211N: STA(842e.270b.8a50) fails to active in BSSID(0a69.6cb9.7a43): STA is rejected by access control, status code(17).
*Mar  1 11:33:43: %WLAN-6-OUTPUT: STA(b8bc.1b6a.fa5b) actives in BSSID(0a69.6cb9.7a43): Auth succeed.
*Mar  1 11:33:43: %WLAN-6-80211N: STA(b8bc.1b6a.fa5b) fails to active in BSSID(0a69.6cb9.7a43): STA is rejected by access control, status code(17).
*Mar  1 11:33:53: %WLAN-6-OUTPUT: STA(a888.0867.4e56) actives in BSSID(0a69.6cb9.7a43): Auth succeed.
*Mar  1 11:33:53: %WLAN-6-80211N: STA(a888.0867.4e56) fails to active in BSSID(0a69.6cb9.7a43): STA is rejected by access control, status code(17).
*Mar  1 11:33:53: %WLAN-6-OUTPUT: STA(b8bc.1b6a.fa5b) actives in BSSID(0a69.6cb9.7a43): Auth succeed.
*Mar  1 11:33:53: %WLAN-6-80211N: STA(b8bc.1b6a.fa5b) fails to active in BSSID(0a69.6cb9.7a43): STA is rejected by access control, status code(17).
*Mar  1 11:33:54: %WLAN-6-OUTPUT: STA(b8bc.1b6a.fa5b) actives in BSSID(0a69.6cb9.7a43): Auth succeed.
*Mar  1 11:33:54: %WLAN-6-80211N: STA(b8bc.1b6a.fa5b) fails to active in BSSID(0a69.6cb9.7a43): STA is rejected by access control, status code(17).
```

Adjust the **Max Client** value on MACC-BASE to support more users on radio interface.



Maintenance

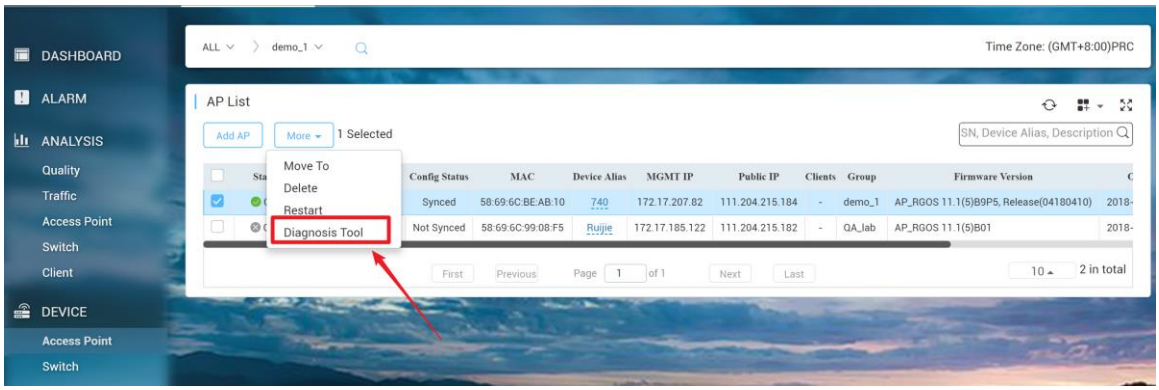
User cannot receive mail alarm from MACC-BASE

It needs to verify below setting:

- Configure SMTP server on **System Settings-Advanced Settings**
- Ensure the connectivity between MACC-BASE server and SMTP service
- Verify whether the mail address of user account is correct or not

How to use WEB CLI for device on MACC-BASE?

Choose designated device and click **More**->**Diagnosis Tool**



How to configure the function which MACC-BASE doesn't support?

Click **CLI Command** on **CONFIGUATION**–>**Basic** and add the command that needs to be configured.