Ruijie Japan Cloud Service User Guide

Copyright statement

Exemption statement

Audience

This manual is intended for:

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

Obtaining Technical Assistance

- Ruijie Networks Website: https://www.ruijienetworks.com/
- Technical Support Website: https://ruijienetworks.com/support
- Case Portal: https://caseportal.ruijienetworks.com
- Community: https://community.ruijienetworks.com
- Technical Support Email: service_rj@ruijienetworks.com
- Skype: service_rj@ruijienetworks.com

Symbols

Important information. Contains helpful suggestions or references.

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

Contents

1   Summary

Ruijie Cloud Service is Ruijie's easy and efficient cloud solutions for chain stores, small and medium-sized businesses and boutique hotels. The solutions include equipment deployment, monitoring, network optimization and operational lifecycle management; enabling customers with simple plug and play deployment and operation and maintenance. Meeting the needs for automatic cloud RF planning and user experience monitoring. At the same time it provides flexible wireless user access control features.

2 Supported Browser

For browser, it is recommended to use the following versions or above.

| Supported Browser	Version
Chrome	57.0.2987.133
Safari	10.1
Firefox	52.0.2

3   Addresses & Ports to be Permitted

Source IP	Destination	Src. port	Dst. port	Protocol	Description	Device using this rule
Your network	devicereg.ruijienetworks.com devreg.ruijienetworks.com	Any	80, 443	TCP	Ruijie Cloud login server	Ap/AC/Switch/Gateway
Your network	cwmpsvr-japan.ruijienetworks.com	Any	80, 443	TCP	Ruijie Cloud server	Ap/AC/Switch/Gateway
Your network	35.194.101.74 34.84.13.46	Any	10000-12 000	TCP	Ruijie Cloud server establishes the tunnel connection with the gateway	Gateway
Your network	cwmpsvr-japan.ruijienetworks.com devicereg.ruijienetworks.com devreg.ruijienetworks.com	Any	3478, 3479,	UDP	Ruijie Cloud server delivers the CLI commands to the device	Ap/AC/Switch/Gateway
Your network	cdn-japan.ruijienetworks.com	Any	80, 443	TCP	Ruijie Cloud authentication server	STA
Your network	rylog-japan.ruijienetworks.com	Any	80, 443	TCP	Device log upload	AP,AC, Switch, Gateway
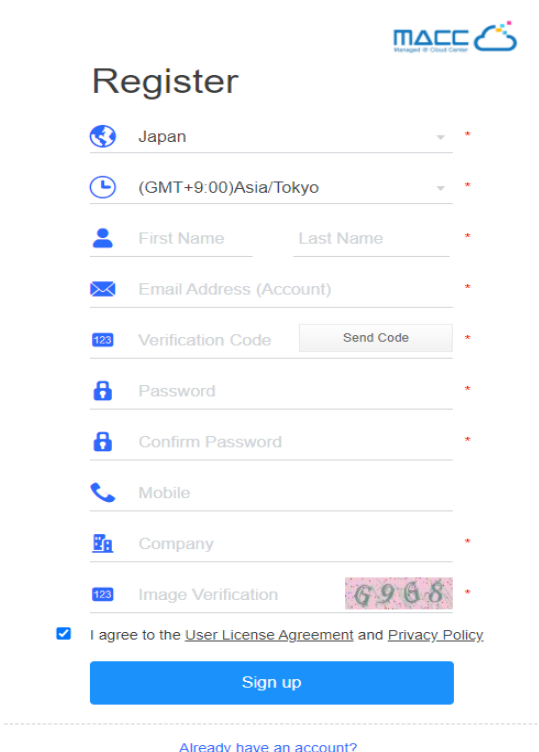
4   Register and Login

4.1 Register

1.   Visit https://cloud-japan.ruijienetworks.com.
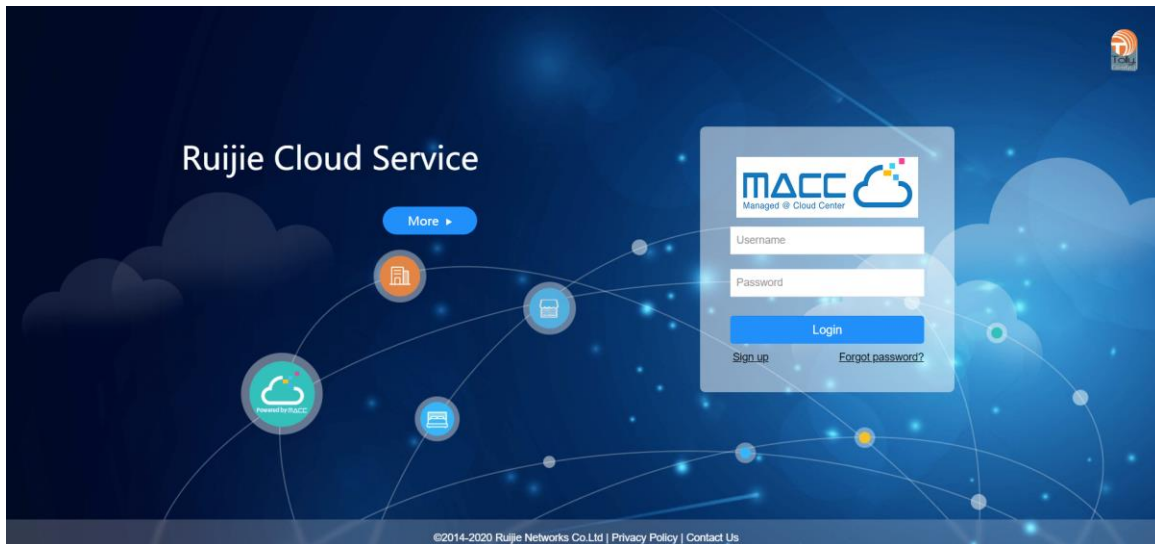
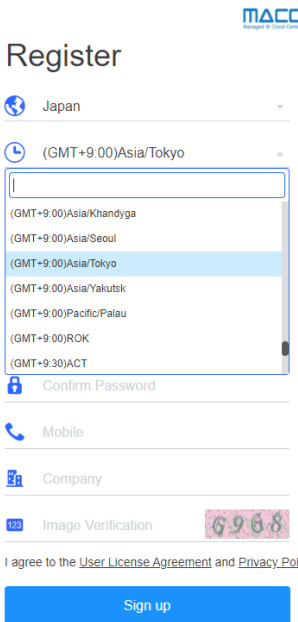2.   Click **Sign up** to open the **Register** page.
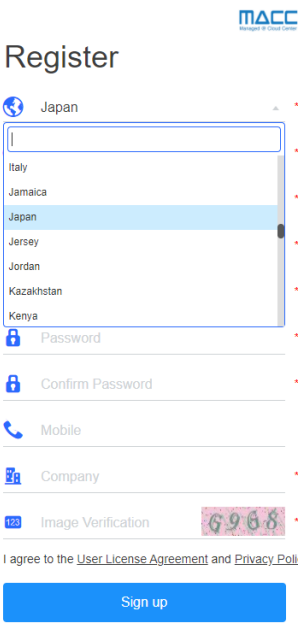
3.   Select your country or region.

Note: The Server Hosting is determined by country. Please choose your country correctly, or the device may fail to go online. When the selected country or region does not match the current server, the page will automatically refresh without affecting the registration.

4.   Select your time zone.

5.   Enter your Email address, click **Get Code**, and enter the security code contained in the Email into the **Verification Code** box.

Note: One email address can be registered once only.

6.   Enter and confirm the password.

Note: The password should be a combination of two or more items among numbers, letters and special characters in the length of 5 to 12 characters. Space is not supported.

7.   Fill in the rest required information and click **Sign up**. If your information is verified and saved, the registration succeeds.

4.2 Login

1.   Visit https://cloud-japan.ruijienetworks.com.
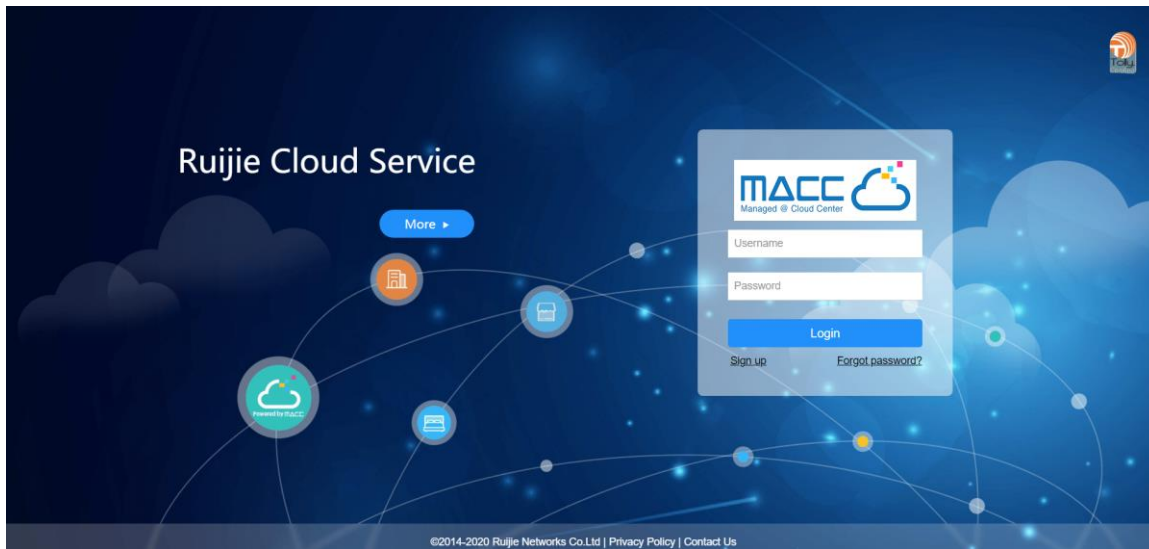
2.   Enter your username and password, and click **Login**. After the information is verified, you can access the system.

4.3 Forgot Password

1.   Visit https://cloud-japan.ruijienetworks.com.
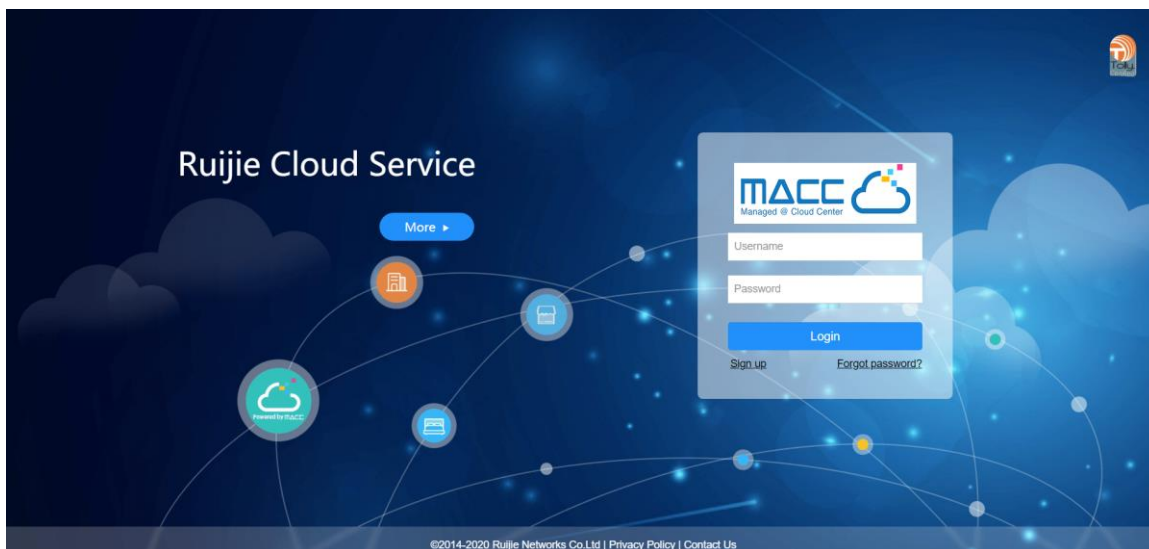
2.   Click **Forgot password?** to open the **Forgot password** page.
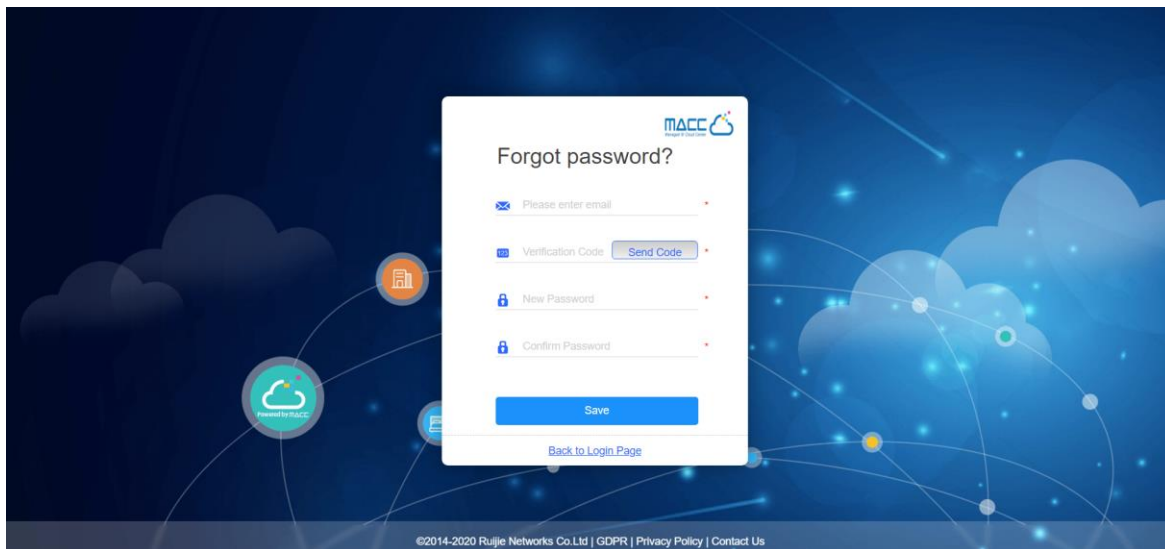
3.   Enter the Email address for retrieving the password. Click **Get Security Code**, and enter the security code contained in the Email into the **Security Code** box.

Note: The Email address is generally the same as the account.

4.   Enter and confirm the new password.

Note: The password should be a combination of two or more items among numbers, letters and special characters in the length of 5 to 12 characters. Space is not supported.

5.   Click **Save**. If your information is verified and saved, you can use the new password to log into the system.

5 Monitoring

This part enables you to monitor the following items:

- DASHBOARD

- TOPOLOGY

- ALARM

- REPORT

- DEVICE

- CLIENT

5.1 Dashboard

After logging in, the **Dashboard** appears, or you can click **Dashboard** in the menu to open the page.
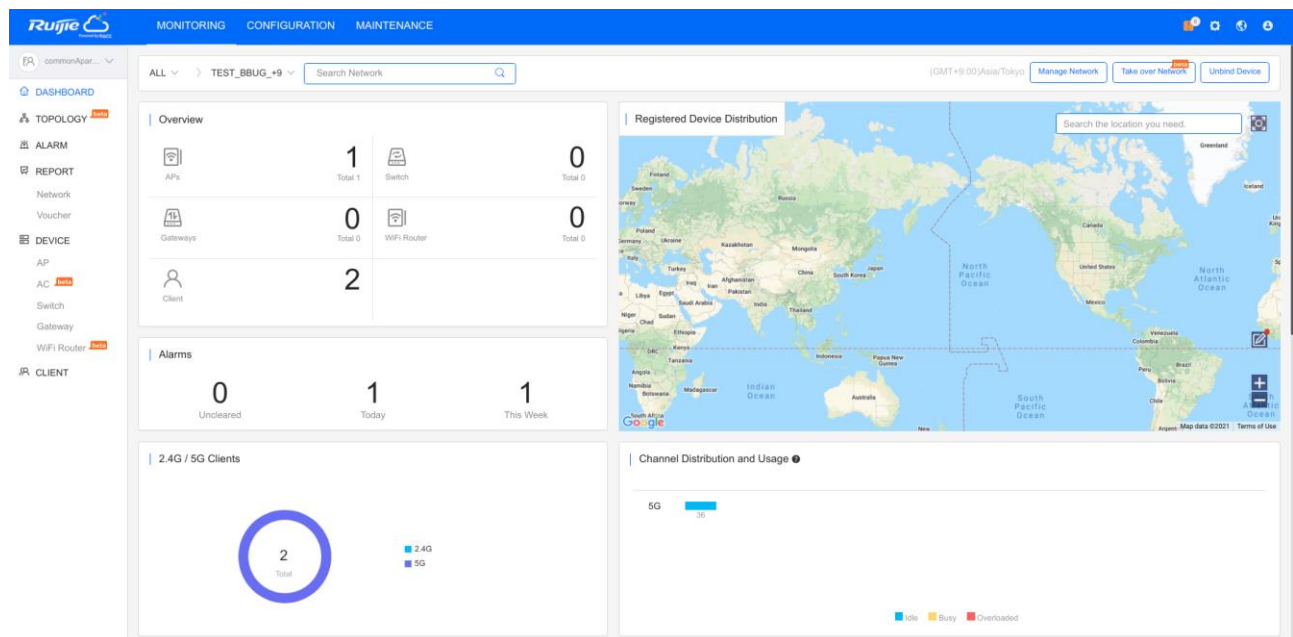
5.1.1 Overview
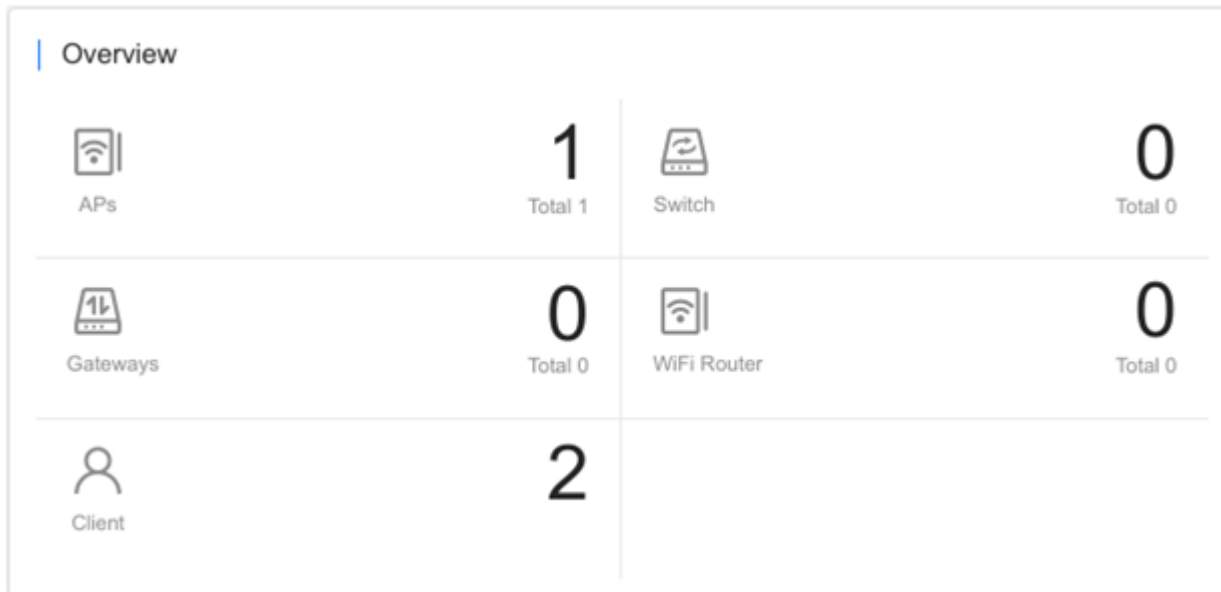
Overview displays the statistics of APs, switches, gateways and clients. The upper number indicates the number of online devices, and the lower number indicates the total number of devices.

5.1.2 Alarms
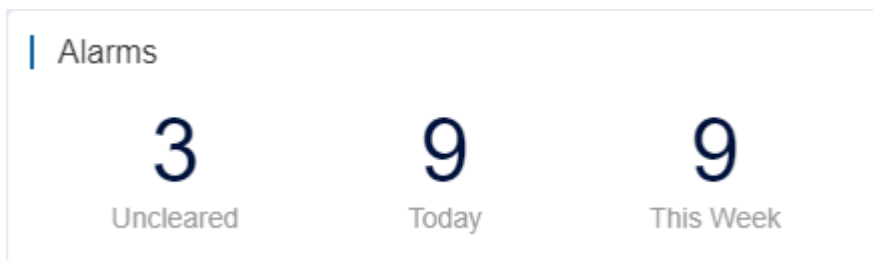
Alarms displays the number of uncleared alarms, new alarms today and total alarms generated this week.

5.1.3   Registered Device Distribution
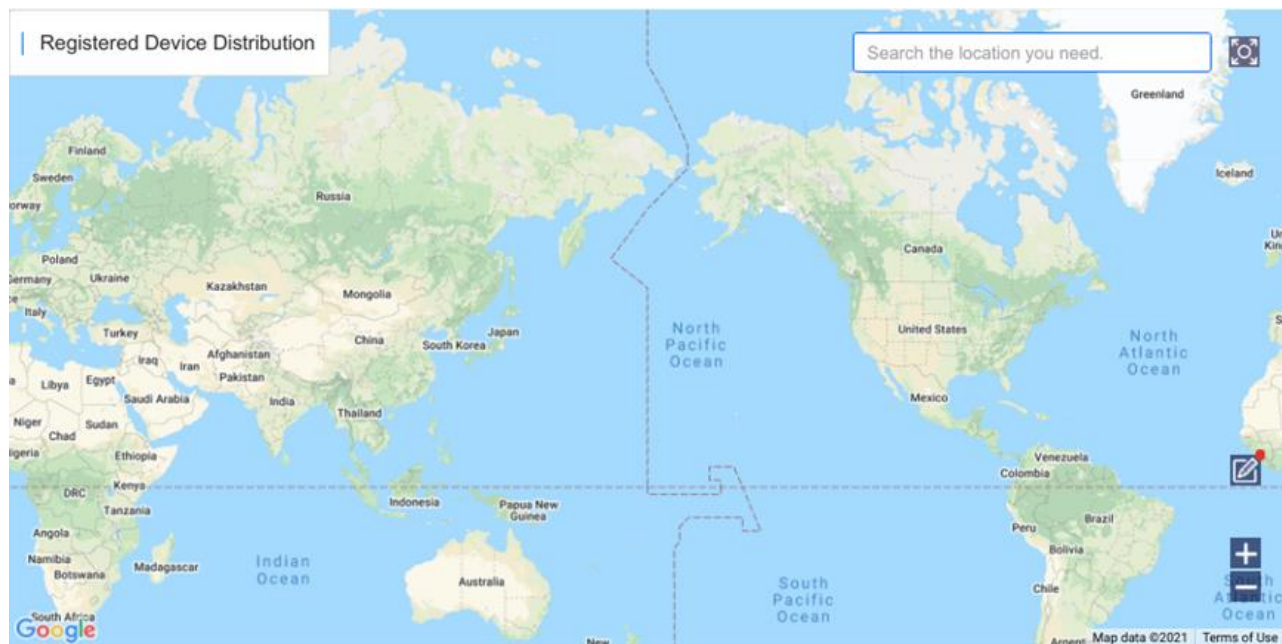
The map displays the device distribution by default. Devices are displayed in network, and the number on icon indicates the device number. Point to the icon, and the device and alarm number are displayed.
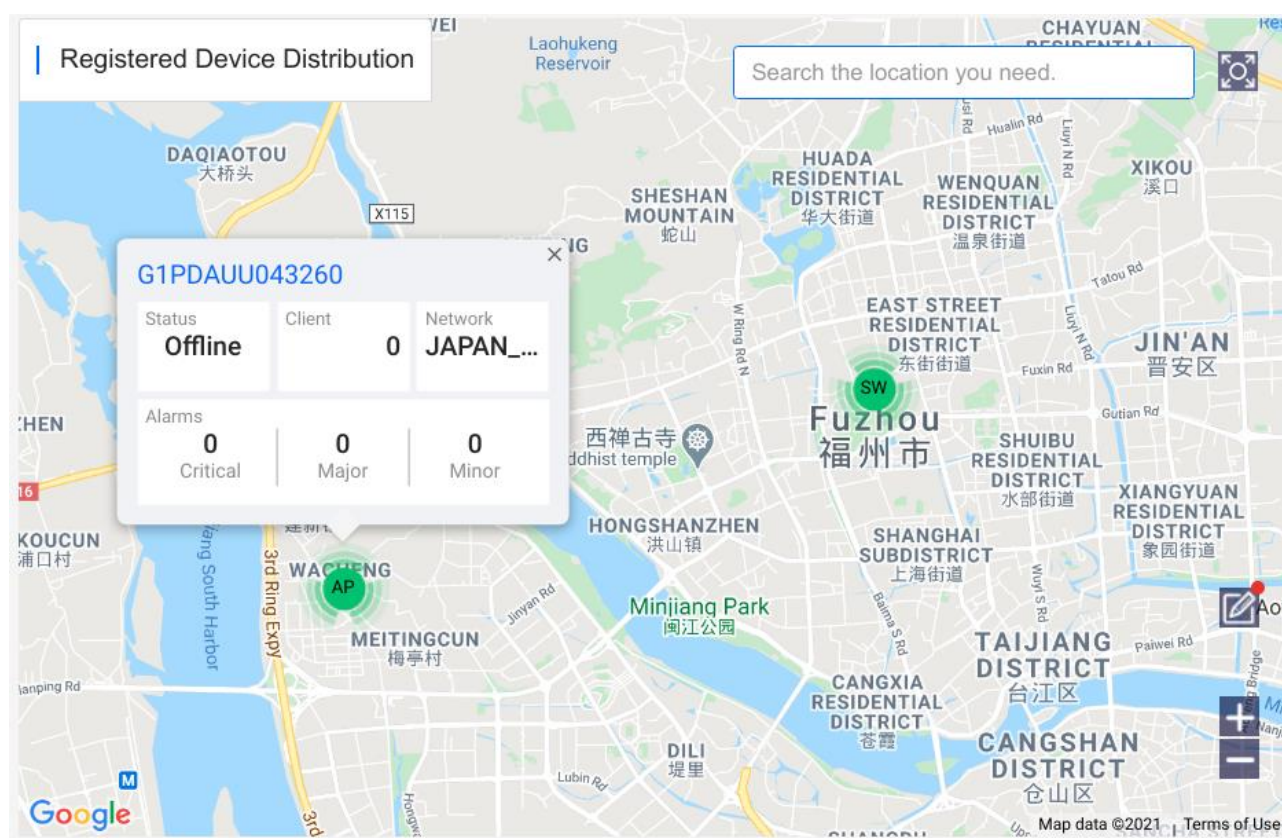
Click ![icon] to bind networks. In the **Unbound Network List**, you can drag a device to the map to bind the location; on map, you can drag a network to change its location, or click **Unbind** to unbind the location.

5.1.4 2.4G / 5G Clients
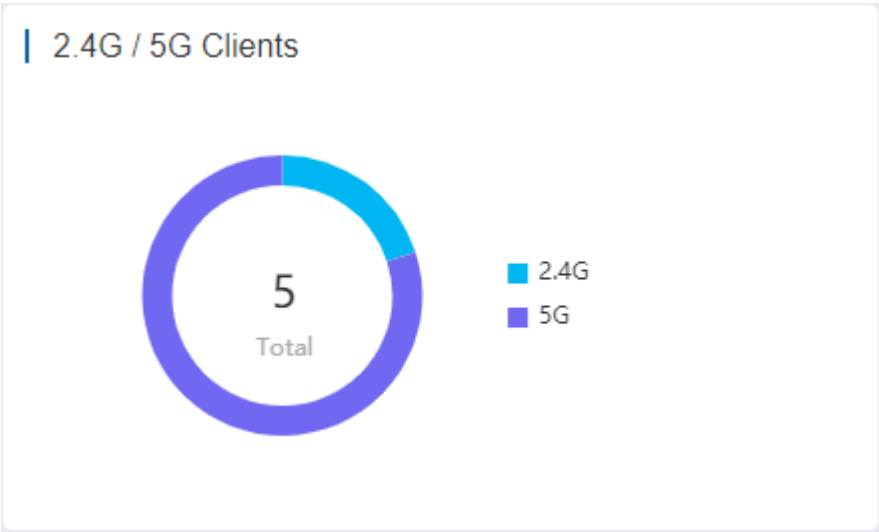
The chart displays the statistics of clients using 2.4G and 5G.

5.1.5 Channel Distribution and Usage
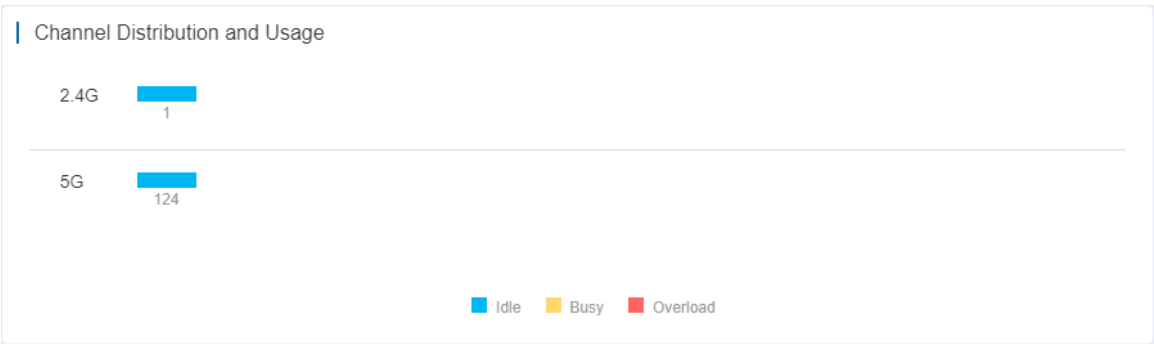
The chart displays the channel statistics.
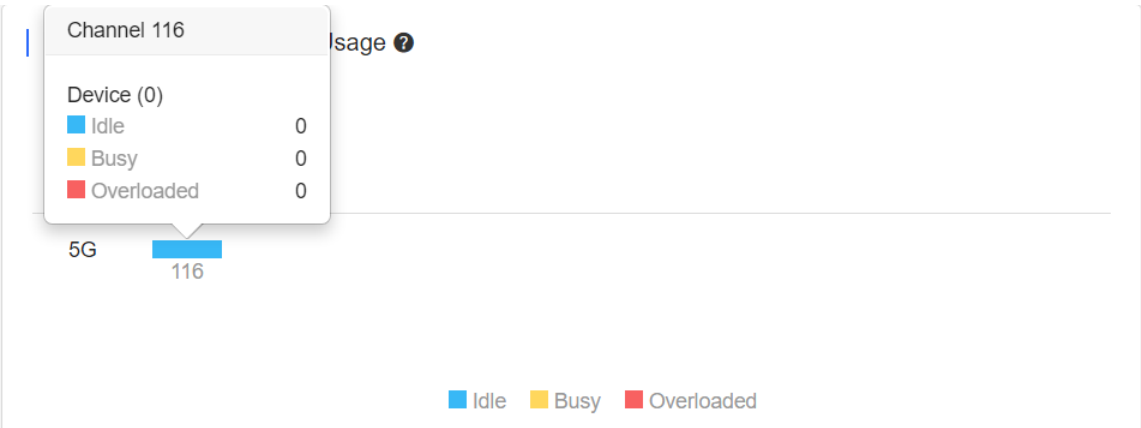
Point to a channel, and more details appear. The channel usage is graded as:

Idle: 0% to 59%

Busy: 60% to 79%

Overload: 80% to 100%

5.1.6 Client Summary
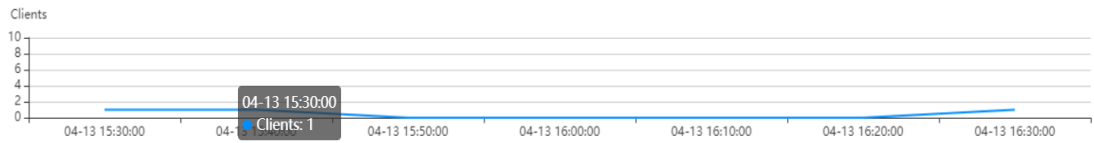
The chart displays the trend of recent clients.

5.1.7 Top 10 Networks by Traffic

The table displays the top 10 networks ranked by traffic.

5.1.8 Top 10 Clients by Traffic

The chart displays the top 10 clients ranked by traffic.

5.1.9 Top 10 APs by Traffic

Top 10 APs by Traffic			
Ranking	AP	Traffic	Clients
1	G1KD9HH02861B	161.92M	11
2	G1KQB7F01872A	8.67K	1

The table displays the top 10 APs based on traffic.

5.1.10 Top 10 SSIDs by Traffic

Top 10 SSIDs by Traffic

939.78G
Total

- SSID_testData9
- Nature_Cloudtest
- Nature2_Cloudtest
- Guoqiang
- 015_New_Portal_SSID_015
- SSID_testData5

1/2
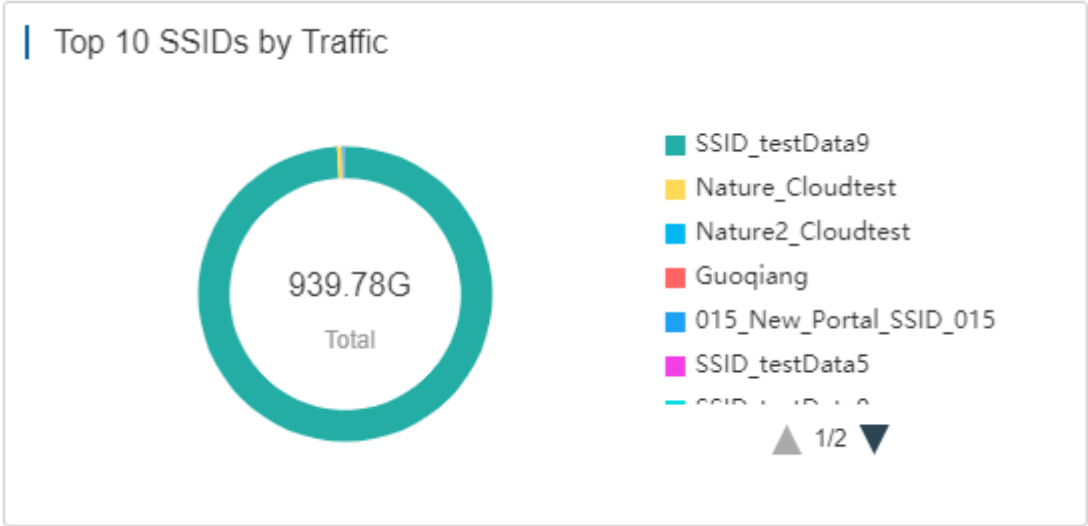
The chart displays the top 10 SSIDs based on traffic.

5.2 Topology (beta)

Topology displays the network topology and status, and offers the project report.
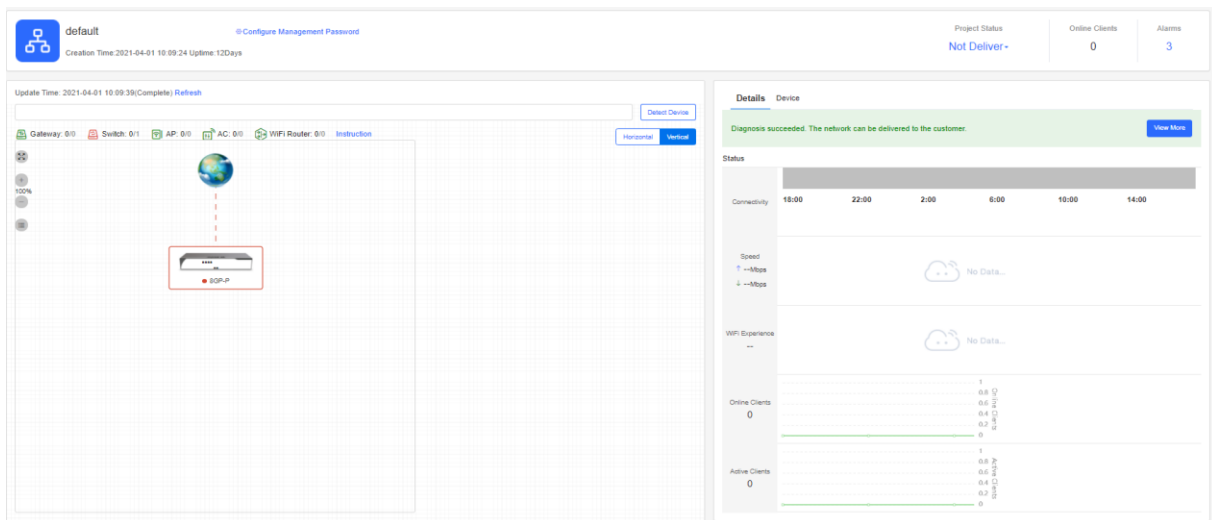
5.2.1 Data Monitoring

● Basic Information

Including the creation time, uptime, quantity of online clients and alarms.
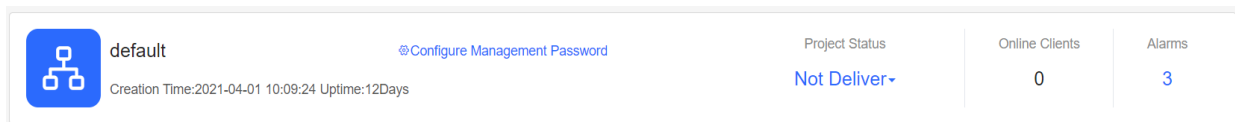
● Network Topology

The topology displays the device connection and status. Click a device, and its detailed information will be displayed on the right.

● Details and Device

Details displays connectivity, network speed, WiFi experience, and online/active client quantity.

Device displays the data of different kinds of devices.
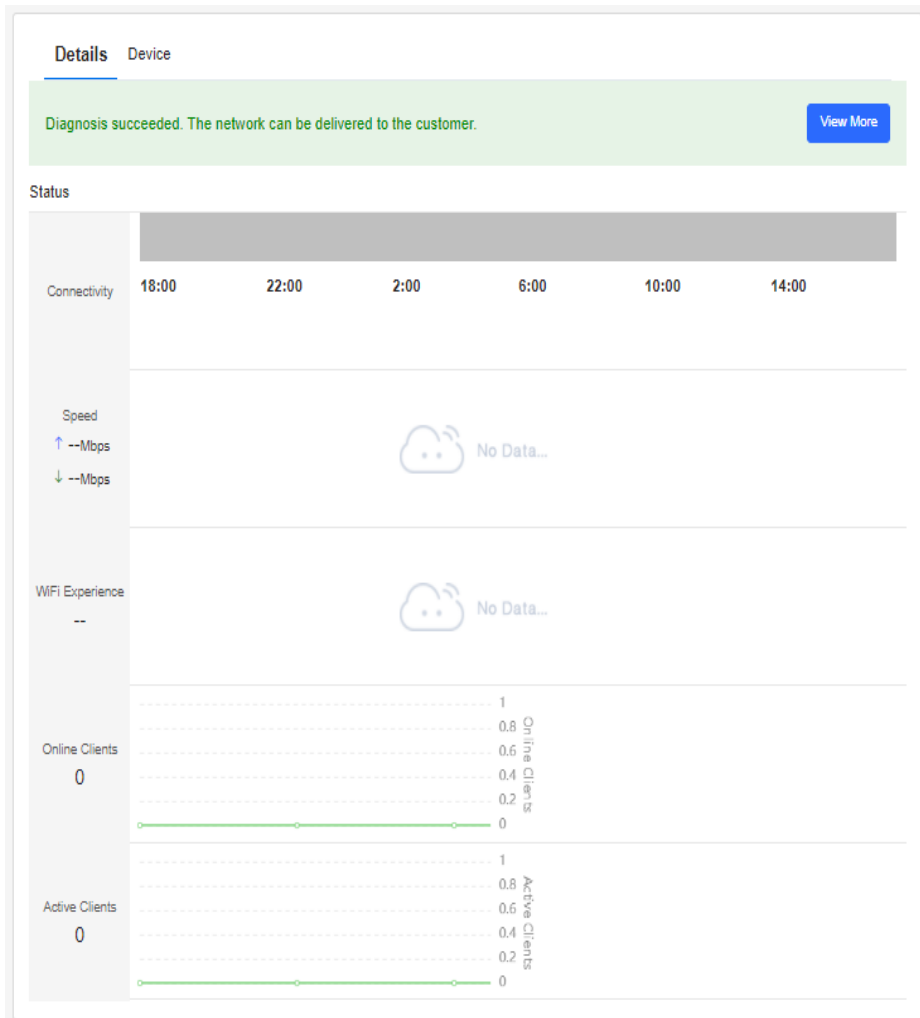
5.2.2 Report

Point to **Project Status**, and click **View Report**.

5.2.2.1   Edit

You can download or edit the report. Click **Edit** on the upper right corner to customize the report.

You can edit

- Title

- Cover

- Basic information

- Configuration

- Diagnosis data

- Device list

- Topology

5.2.3   New Device

5.2.3.1   Device Information

Click a device in the topology to check its configuration.

5.2.4   Diagnosis

The function diagnoses the network connectivity and link status. Click **Start Diagnosis** or **Diagnose again** on the right to start diagnosis.

Click **View More** to check the previous diagnosis results.

5.3 Alarm

5.3.1 Alarm List

- **Alarm List** displays the cleared alarms. **Alarm List** supports the search based on AP serial number, alarm type, alarm source (network/device), and alarm generation time.

- You can configure thresholds in **Alarm Settings**.

The following describes the conditions for generating alarms.

Type	Condition	Description
Device goes offline	An AP goes offline.	The AP is disconnected from the Cloud Service, or the AP is powered off.
Device goes online and offline continually	The online/offline change times of an AP exceeds the default threshold within two hours.	The connection between the AP and the system is unstable or the AP has a firmware or hardware fault.
All devices are offline	All APs in a network go offline.	
High channel usage on AP	The RF channel utilization exceeds 80%.	RF channel utilization is high and interference is strong. It is recommended to change the channel.
System usage(CPU/memory usage) above threshold	The CPU or memory usage of AP/switch/gateway exceeds the threshold.	For AP, the default threshold for CUP usage is 85% and for memory usage is 85%. For switch, the default threshold for CUP usage is 50% and for memory usage is 65%. For gateway, the default threshold for CUP usage is 50% and for memory usage is 65%. Custom values are not supported.
Switch loopback detected (RLDP)	A loop occurs on the switch.	
Abnormal network access on gateway	The gateway port fails to ping the specified domain or IP for several times.	When the Ping test failed for the specified times, the alarm is sent. The times and domain/IP address can be configured manually.
High packet loss rate on gateway	The packet loss rate of gateway exceeds the threshold.	When the packet loss rate exceeds the specified percentage of threshold for several times in 5 minutes, the alarm is sent. The times and threshold can be configured

		manually.
Uplink rate above threshold on gateway	The uplink rate exceeds the specified percentage of threshold for several times.	When the uplink rate exceeds the specified percentage of threshold for several times, the alarm is sent. The threshold, times and percentage can be configured manually.
Downlink rate above threshold on gateway	The downlink rate exceeds the specified percentage of threshold for several times.	When the downlink rate exceeds the specified percentage of threshold for several times, the alarm is sent. The threshold, times and percentage can be configured manually.
SIM card traffic exceeds limit	SIM card traffic exceeds a default threshold.	Only MTFi devices support this alarm.
GPS signal is not found	GPS signal is not found.	Only MTFi devices support this alarm.
CPU usage is high	CPU usage exceeds a default threshold.	Only MTFi devices support this alarm.
Memory usage is high	Memory usage exceeds a default threshold.	Only MTFi devices support this alarm.
Disk space usage is high	Disk space usage exceeds a default threshold.	Only MTFi devices support this alarm.
Flash usage is high	Flash usage exceeds a default threshold.	Only MTFi devices support this alarm.
CPU temperature is high	CPU temperature exceeds a default threshold.	Only MTFi devices support this alarm.

5.3.2 Ignore Alarm

Select the alarm you want to ignore in **Alarm List**, and click the **Ignore Alarm** button. A popup window will be displayed. After click **OK**, the alarm will be ignored.

5.4 Report

5.4.1 Network

Network is divided into 3 parts: **Summary**, **Device** and **Client**. Except the statistical charts with Real-time that display real-time data and **Client** > **Experience** chart that only displays data in the last 7 days, all other charts support searching data in the last 94 days with the same query conditions. All charts automatically refresh every minute. Reports can be exported into CSV or PDF files, or sent by Email.

● Export to CSV

Point to [icon], and click **Export to CSV**.
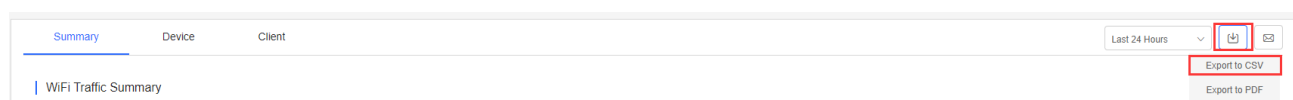
● Export to PDF
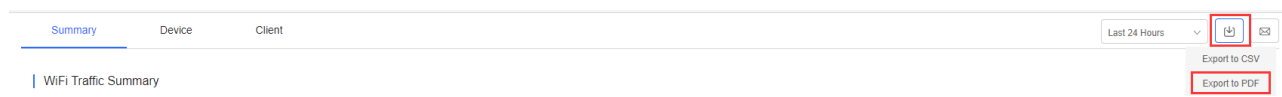
Point to ⌃, and click **Export to PDF**.

● Mail

Click ✉, and select **Send Email**. Choose a file type for the report, then enter Email addresses. After click **OK**, the report will be sent immediately.

Click ✉, and select **Delivery Plan**. Click **Enable** to send the report on the specified time.

Report includes the data of Summary, Device and Client, and supports CSV and PDF file formats.

Up to three Email addresses are supported.

Reports can be sent every month, week or day.

● Summary > WiFi Traffic Summary
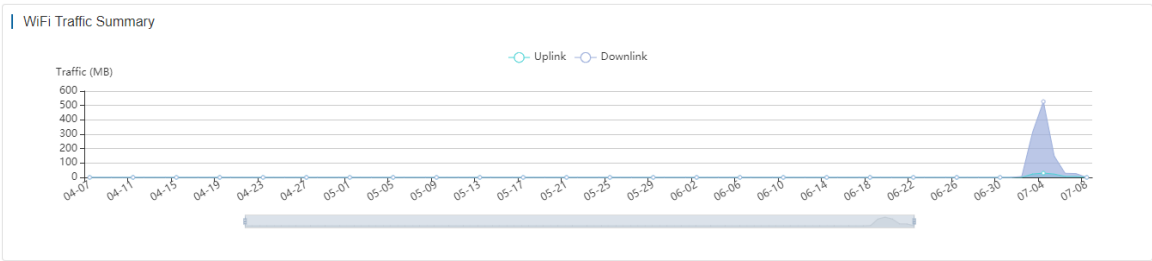
The uplink/downlink traffic summaries of the selected network during the specific period.

Uplink: Traffic directed from internal network to external network.

Downlink: Traffic directed from external network to internal network.

● Summary > Channel Distribution and Usage
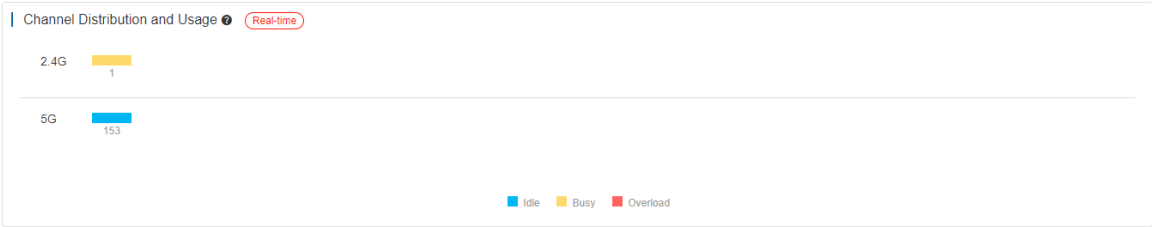
The channel distribution and usage of the selected network.
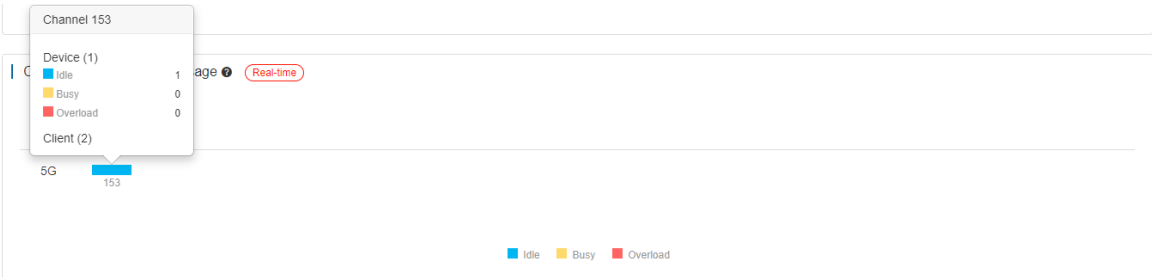
Point to a channel to view more details. The channel usage is graded as:

Idle: 0% to 59%

Busy: 60% to 79%

Overload: 80% to 100%

● Summary > SSIDs by Client

SSIDs by Client

Ranking	SSID	Clients		Traffic
1	Nature_Cloudtest	10	▰	770.35M
2	A_oneclick	9	▰	21.48M
3	nature1	7	▰	18.69K
4	A_voucher	7	▰	2.55M
5	wang1	7	▰	49.51K
6	A_oneclick123	6	▰	23.38K
7	nateure2	4	▰	20.68K

The SSIDs ranked by client number of the selected network during the specific period.

● Summary > SSIDs by Traffic

SSIDs by Traffic

Ranking	SSID	Traffic		Clients
1	Nature_Cloudtest	770.35M	▰▰▰▰	10
2	Venus_Cloudtest	181.04M	▰	1
3	A_oneclick	21.48M	▏	9
4	A_voucher	2.55M	▏	7
5	wang1	49.51K	▏	7
6	A_oneclick123	23.38K	▏	6
7	nateure2	20.68K	▏	4

The SSIDs ranked by traffic of the selected network during the specific period.

● Summary > RSSI Statistics

RSSI Statistics ❓ (Real-time)
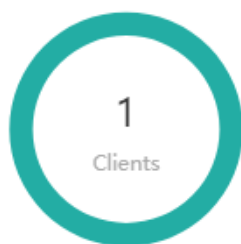
	Strength	Clients	Proportion
■	Strong	1	100%
■	Medium	0	0%
■	Weak	0	0%

1 Clients

The wireless signal strength of the selected network during the specific period. The signal intensity is defined below:

Weak: RSSI ≤ -80dB

Medium: -80dB < RSSI ≤ -70dB.

Strong: RSSI > -70dB

- Device > Device Summary

The online status of devices of the selected network during the specific period.

- Device > AP Activity
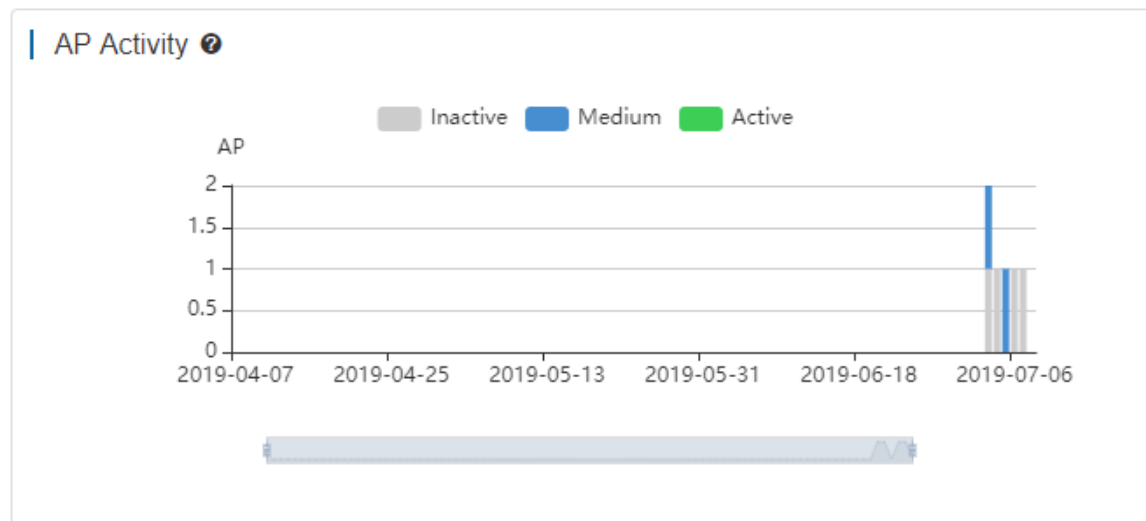
The AP activity of the selected network during the specific period. The chart does not support searching data in the last 24 hours.

AP activity is evaluated based on the number of active clients accessing the AP in a day. APs not associated with any clients are not calculated.

Inactive: <5 active clients

Medium: 5-9 active clients

Active: ≥10 active clients.

● Device > Top 10 APs by Client

The top 10 APs ranked by client number of the selected network during the specific period.

● Device > Top 10 APs by Traffic

The top 10 APs ranked by traffic of the selected network during the specific period.

● Device > Firmware Version

The proportion of firmware versions of the selected network during the specific period.

● Device > Hardware Version
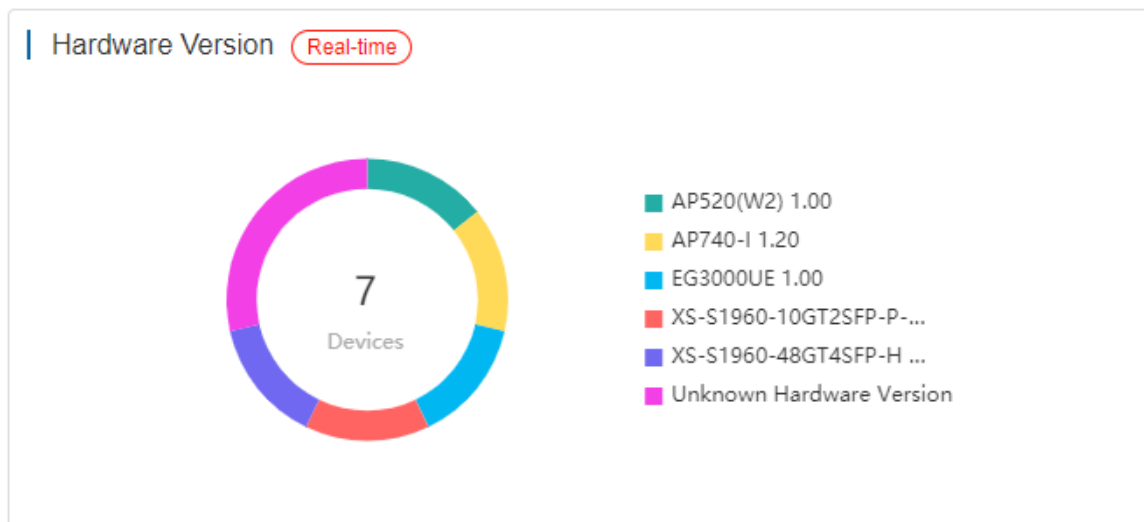
The proportion of hardware versions of the selected network during the specific period.

● Device > PoE Utilization
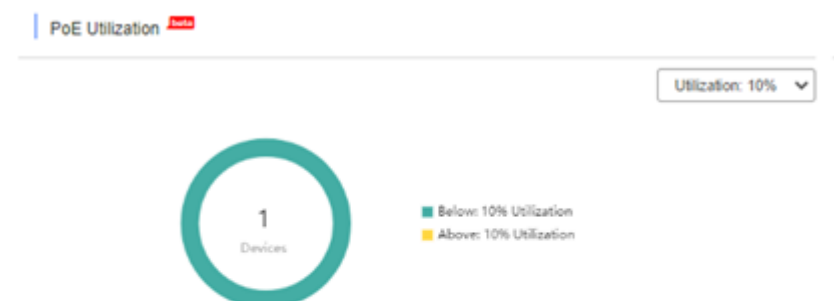
The numbers of PoE switches above and below the selected utilization percentage.

● Device > PoE Power Summary
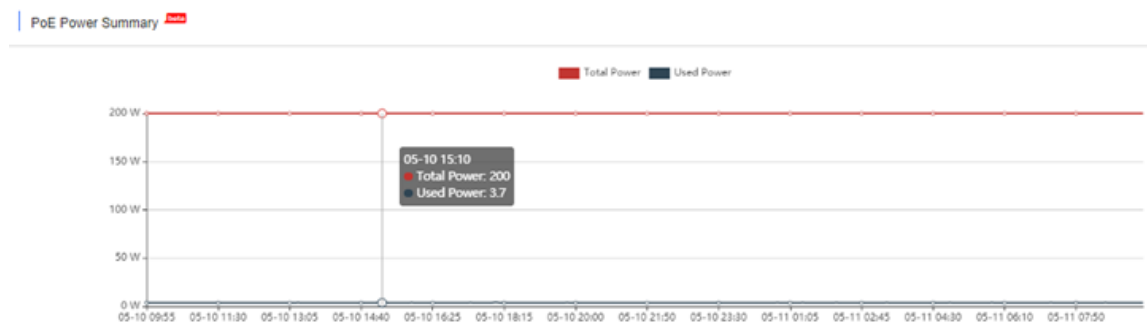
The power summary of the entire PoE device, including the total power and used power.

● Client > WiFi Client Summary
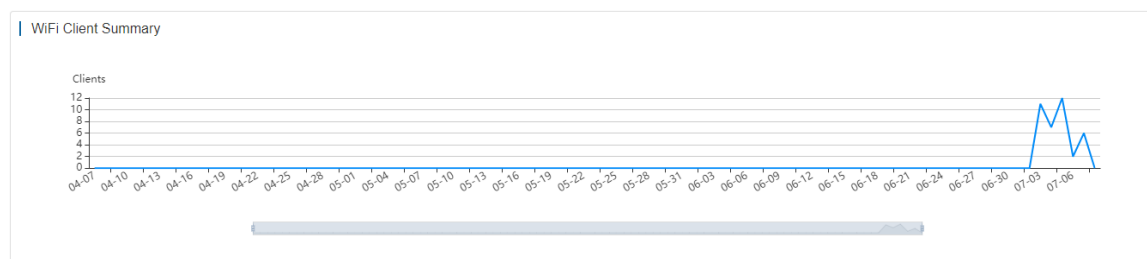
The client summary of the selected network during the specific period.

● Client > WiFi Client Activity
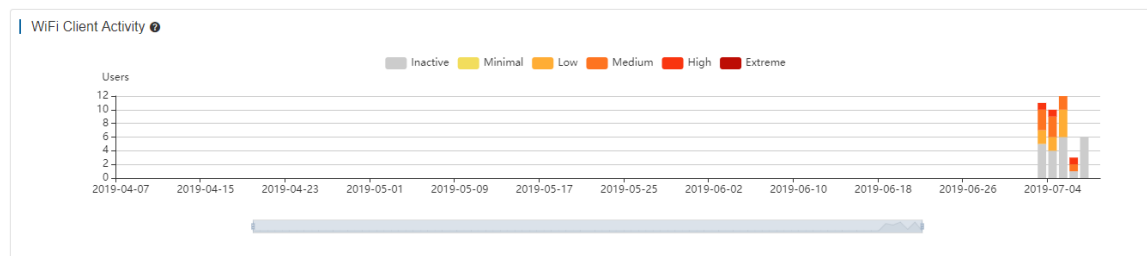
The client activity of the selected network during the specific period. The chart does not support searching data in the last 24 hours.

Client activity is evaluated based on online duration and traffic volume (from highest to lowest):

Inactive: ≤100KB traffic

Minimal: Any time and 100KB traffic

Low: 1h/d and 500K traffic

Medium: 2h/d time and 2M traffic

High: 4h/d time and 5MB traffic

Extreme: 8h/d time and 10MB traffic

● Client > 2.4G / 5G Clients
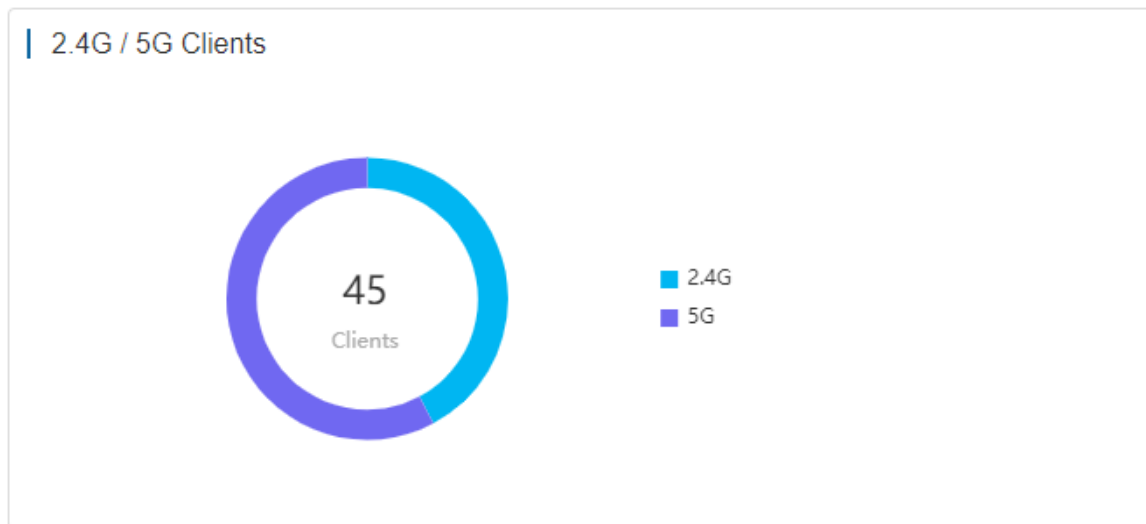
The proportion of STAs using 2.4G/5G of the selected network during the specific period.

● Client > Top 10 WiFi Clients by Traffic

The top 10 clients ranked by traffic of the selected network during the specific period.

● Client > Experience

Client MAC	Reported at	Band	AP MAC	Experience Type	Reason	Channel Usage	Noise Floor	Pkt Loss Rate	Delay
64b0.a695.1ee4	2019-07-08 16:57	5G	5869.6c99.08f5	Good	-	87%	-103	0	58.9
a057.e32a.9203	2019-07-08 16:57	5G	5869.6c99.08f5	Good	-	87%	-103	5.3	11
18f0.e4eb.6cbb	2019-07-08 16:57	5G	5869.6c99.08f5	Excellent	-	87%	-103	0	0.8
8c0d.7677.f87d	2019-07-08 16:57	5G	5869.6c99.08f5	Excellent	-	87%	-103	0	0.5
dccf.963f.79c3	2019-07-08 16:57	5G	5869.6c99.08f5	Excellent	-	87%	-103	0	6

The experience status during the specified time and collects data every 5 minutes. You can switch between 2.4GHz and 5 GHz.

Client information: Click an indicator bar to display more information.

Excellent: HDV and online game are available.

Good: communication application, Web page and VoIP are available.

Poor: go offline frequently or hard to go online.

Inactive: check whether a client is inactive according to the traffic and power usage.

Score: Take the parameters of client delay, client packet loss, signal strength and so on as the reference, and then use the SVM algorithm to get the score.

5.4.2   Voucher

The **Voucher Report** records the sales of voucher during the specified period.

No.	Package Name	Description	Price	Qty	Activated Accounts	Total Price
Total				0	0	0.00

Click to export the **Voucher Report** in PDF format.

Qty: Number of vouchers generated by each package in the specified period.

Activated Accounts: Number of vouchers activated by each package in the specified period.

Total Price: Total price of vouchers activated by each package in the specified period.

Total: Number of vouchers generated by all packages, number of vouchers activated by all packages and total amount of vouchers activated by all packages.

5.5 Device

Choose **MONITORING > DEVICE** to display the **Devices** page, and select a network on the top to filter devices.

5.5.1   AP

5.5.1.1   AP List

Non-apartment Scenario

The **AP List** displays basic device information, including online/offline status, SN, configuration status, MAC, alias, management IP, public IP, client quantity, network, firmware version, offline time, model and description.

Apartment Scenario

The **AP List** displays basic device information, including the online/offline status, SN, configuration status, MAC, alias, management IP, public IP, client number, network, firmware version, offline time, model, building name, room, remark and description.

The **AP List** automatically refreshes every minute. Click to enable/disable the auto refresh function.

Above the list is the **Add AP**, **Web CLI and eWeb** functions. Click to display the **Move to**, **Delete**, and **Reboot** functions. For more information, refer to **Basic AP Operations**.

The **Search** function supports fuzzy queries based on the serial number, alias and description, and also supports queries based on online/offline status.

Click the record in the **Config Status** column to open the **Config Status** page. On this page, you can deliver one or all configurations.

The number of devices which have available firmware for upgrade is displayed on the upper-left corner of the **AP List** page. Click **New Firmware** to display the **New Firmware List**. Then click **Go To Upgrade** to enter the **MAINTENANCE** > **UPGRADE** > **Upgrade** page.

Model	Current Version	Hardware Version	Devices	Recommended Version	Action
AP630(IDA2)	AP_RGOS 11.1(5)B40P2, Release(05161916)	1.01	1	AP_RGOS 11.1(5)B40P6, Release(06150512)	Go To Upgrade
AP740-I	AP_RGOS 11.1(5)B40P9	1.00	1	AP_RGOS 11.1(5)B40P6, Release(06150512)	Go To Upgrade
AP130(W2)	AP_RGOS 11.1(5)B40P2, Release(05170916)	1.00	1	AP_RGOS 11.1(5)B40P6, Release(06150511)	Go To Upgrade
AP720-L	AP_RGOS 11.1(5)B40P2	1.00	1	AP_RGOS 11.1(5)B40P6, Release(06150511)	Go To Upgrade
AP720-L	AP_RGOS 11.1(5)B40P9	1.00	1	AP_RGOS 11.1(5)B40P6, Release(06150511)	Go To Upgrade
AP710	AP_RGOS 11.1(5)B40P9	1.21	1	AP_RGOS 11.1(5)B40P6, Release(06150511)	Go To Upgrade
AP130(L)	AP_RGOS 11.1(5)B9P2, Release(04162719)	1.02	1	AP_RGOS 11.1(5)B9P11, Release(05151200)	Go To Upgrade
AP740-I	AP_RGOS 11.1(5)B40P2, Release(05161917)	1.00	1	AP_RGOS 11.1(5)B40P6, Release(06150512)	Go To Upgrade
AP720-I	AP_RGOS 11.1(5)B40P9	1.01	1	AP_RGOS 11.1(5)B40P6, Release(06150512)	Go To Upgrade
AP720-I	AP_RGOS 11.1(5)B40P9	1.02	1	AP_RGOS 11.1(5)B40P6, Release(06150512)	Go To Upgrade

First   Previous   Page 1 of 2   Next   Last   10 ▲   11 in total

For more information, refer to **Device Details**.

5.5.1.2 Device Details

Click the serial number in the device list to open the details page for a single device. The page displays detailed device information, including basic information, connectivity, traffic summary, client data, online/offline status, RF information, and device log.

The AP information is described as:

● AP Info

| AP Info

SN : G1PH646015472   MAC : 300d.9ede.6d81   MGMT IP : 192.168.21.75

Model : AP180(JA)   Config Status : Synchronized

Hardware Version: 1.01

Firmware Version : AP_RGOS 11.9(4)B1P3, Release(08170714)

Alias : test ✏

Description : ✏

SSID : ↻   JP_HL_RCP_AP_001,   JP_HL_RCP_AP_003,   JP_HL_RCP_AP_002,   eg_portal1

The basic information includes serial number, MAC address, management IP address, device model, configuration status, firmware version, hardware version, alias, and description.

● Static

| Status

⊘ Online	Memory Usage
● Online Clients: 0	75.0%
● Clients with Weak Signal : 0	

CPU Usage   7.0%   Alarms : 0   🔔
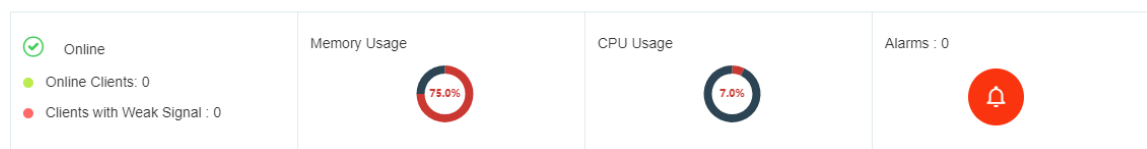
The performance data includes the AP connection status, online client count, CPU usage, and memory usage.

● Connectivity

| Connectivity   Last 24 Hours   Last 7 Days

22:00   2:00   6:00   10:00   14:00   18:00

AP connectivity refers to the connectivity (online status) between AP and Cloud Service within a period (1 day or 7 days).

● Traffic Summary
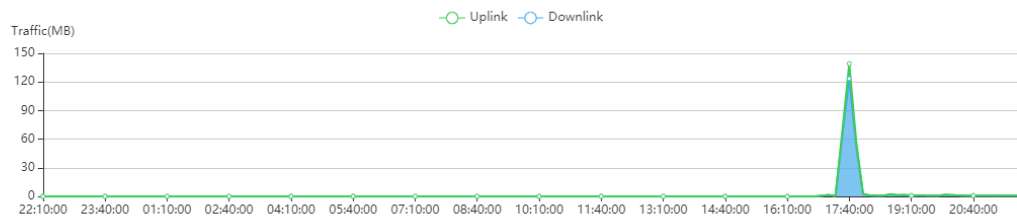
You can select to view the AP traffic statistics in the last 24 hours or the last 1 week.

● Radio List

RF Type	Channel	Power	Channel Width (MHz)	Channel Usage
5G	36	100%	40	42%
2.4G	1	100%	20	71%

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

● Client List

IP	MAC	SSID	RSSI	AP Alias	Band	Traffic (MB)	Manufacturer	Online Time	Offline Time
192.168.23.2	70EF.002B.0F13	Nature_Cloudtest	-55	Ruijie	2.4G	1.489	Apple	2019-04-08 06:24:16	-

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

● Adjacent RF Signal

Scan Adjacent RF

Start Time: 2020-10-26 15:59:35   End Time: 2020-10-26 16:14:46   Status: Complete

| BSSID	Radio	Adjacent SSID	Adjacent Channel	RSSI	Adjacent SN	Adjacent MAC	Uploaded at
92d0.f019.990a	Radio2(5G)	999999999	36	64	G1PC5PK010012	00d0.f019.9904	2020-10-26 16:14:48
82d0.f019.9909	Radio1(2.4G)	999999999	7	56	G1PC5PK010012	00d0.f019.9904	2020-10-26 16:14:48
06d0.f822.3347	Radio1(2.4G)	testfor180	2	28	1234942570014	00d0.f822.3344	2020-10-26 16:14:48
06d0.f822.3348	Radio2(5G)	testfor180	149	23	1234942570014	00d0.f822.3344	2020-10-26 16:14:48
e20d.9ee8.71ef	Radio1(2.4G)	SSID-E871EA	2	21	G1PD7PW00080B	300d.9ee8.71ea	2020-10-26 16:14:48
3e05.8863.45d2	Radio2(5G)		44	60	Unidentified	Unidentified	2020-10-26 16:14:48
82d0.f811.2239	Radio2(5G)	WWWQQQQQ	52	49	Unidentified	Unidentified	2020-10-26 16:14:48
3205.885a.da54	Radio1(2.4G)	�\x8F�\x8B��\x9E\x9C	1	48	Unidentified	Unidentified	2020-10-26 16:14:48
b053.6556.cede	Radio1(2.4G)	CMCC-Nic	9	48	Unidentified	Unidentified	2020-10-26 16:14:48
b253.6556.cede	Radio1(2.4G)	CMCC-NIC	9	48	Unidentified	Unidentified	2020-10-26 16:14:48

First   Previous   Page 1 of 29   Next   Last   10 ▲   286 in total

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 an unidentified state.

You can trigger APs to scan adjacent RF signals, and identified and unidentified RF signals can be observed. There are two known scenarios:

1) Testing the number and strength of RF signals emitted by neighboring APs that are not managed by the system to predict a degree of RF interference.

2) Identifying RF signals emitted by neighboring APs managed by the system to diagnose the RF functions and powered-on status of neighboring APs.

On the device details page, you can perform adjacent RF scanning and check the scanning result. The following steps describe the method for scanning the adjacent RF signals:

Step 1. Click **Scan Adjacent RF** to trigger an AP to scan adjacent RF signals.

Step 2. 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.

Step 3. A list of RF signals scanned by the AP is displayed after the scanning. The list supports a filtering function based on the RF type (2.4 GHz/5 GHz).

| Adjacent RF Signal

Scan Adjacent RF

Start Time: 2020-10-26 15:59:35   **End Time:** 2020-10-26 16:14:46   **Status:** Complete

BSSID	Radio	Adjacent SSID	Adjacent Channel	RSSI	Adjacent SN	Adjacent MAC	Uploaded at
92d0.f019.990a	Radio2(5G)	999999999	36	64	G1PC5PK010012	00d0.f019.9904	2020-10-26 16:14:48
82d0.f019.9909	Radio1(2.4G)	999999999	7	56	G1PC5PK010012	00d0.f019.9904	2020-10-26 16:14:48
06d0.f822.3347	Radio1(2.4G)	testfor180	2	28	1234942570014	00d0.f822.3344	2020-10-26 16:14:48
06d0.f822.3348	Radio2(5G)	testfor180	149	23	1234942570014	00d0.f822.3344	2020-10-26 16:14:48
e20d.9ee8.71ef	Radio1(2.4G)	SSID-E871EA	2	21	G1PD7PW00080B	300d.9ee8.71ea	2020-10-26 16:14:48
3e05.8863.45d2	Radio2(5G)		44	60	Unidentified	Unidentified	2020-10-26 16:14:48
82d0.f811.2239	Radio2(5G)	WWWQQQQQ	52	49	Unidentified	Unidentified	2020-10-26 16:14:48
3205.885a.da54	Radio1(2.4G)	�\x8F�\x8B��\x9E\x9C	1	48	Unidentified	Unidentified	2020-10-26 16:14:48
b053.6556.cede	Radio1(2.4G)	CMCC-Nic	9	48	Unidentified	Unidentified	2020-10-26 16:14:48
b253.6556.cede	Radio1(2.4G)	CMCC-NIC	9	48	Unidentified	Unidentified	2020-10-26 16:14:48

First   Previous   Page 1 of 29   Next   Last   10 ▲   286 in total

The system stores the latest scanning results, 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 system; otherwise, the RF signal is emitted by an AP.

● Configuration Backup List

The function is supported only in the apartment scenario.

| Configuration Backup List

Current   Back up   Download   Restore   Delete   Compare

	File Name	File Size	Time	Mode	MD5	Description	Action
☐	1234942570359_1620723768054	2.37K	2021-05-11 18:02:52	Manual	52723cb9a156973ed90d89109a60ea9a	Manual backup	Details
☐	1234942570359_1620717429553	2.35K	2021-05-11 16:17:13	Manual	db02bd0f2121ba5115b2b476aff8027e	Manual backup	Details
☐	1234942570359_1620659718284	2.01K	2021-05-11 00:15:22	Manual	f0d336ccab39b51d1c3617c67e8ae990	一丨丿丶乛乚丿丿乚丁ㄒ一丄丿乀ㄋ〇十ㄨㄧㄧㄒㄣㄨ…	Details
☐	1234942570359_1620639081388	2.01K	2021-05-10 18:31:25	Manual	f0d336ccab39b51d1c3617c67e8ae990	?一丨丿丶乛乚丿丿乚丁ㄒ一丄丿乀ㄋ〇十ㄨㄧㄧㄒㄣㄨ…	Details
☐	1234942570359_1620296672980	2.01K	2021-05-06 19:24:38	Manual	f0d336ccab39b51d1c3617c67e8ae990	Manual backup	Details
☐	1234942570359_1620139216901	2.01K	2021-05-04 23:40:20	Manual	f0d336ccab39b51d1c3617c67e8ae990	Manual backup	Details
☐	1234942570359_1620139179731	2.01K	2021-05-04 23:39:43	Manual	f0d336ccab39b51d1c3617c67e8ae990	Manual backup	Details
☐	1234942570359_1619581523244	2.01K	2021-04-29 13:34:52	Auto	6d7d3783c73c32320456e774a927c1ae	Auto backup	Details
☐	1234942570359_1619275199494	2.01K	2021-04-27 07:29:36	Auto	f0d336ccab39b51d1c3617c67e8ae990	12345678912345678912345678912345678912345…	Details
☐	1234942570359_1619190971301	2.00K	2021-04-24 00:16:15	Auto	fe69ef30380df37c7fd727c024d18f01	Auto backup	Details

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

The backup records include configuration file name, size, time, mode and MD5.

Click **Current** to display the current configuration. Click **Backup** in the **Config Details** page to back up the current configuration.

Click **Back up** and then click **OK** in the message box to back up the current configuration.
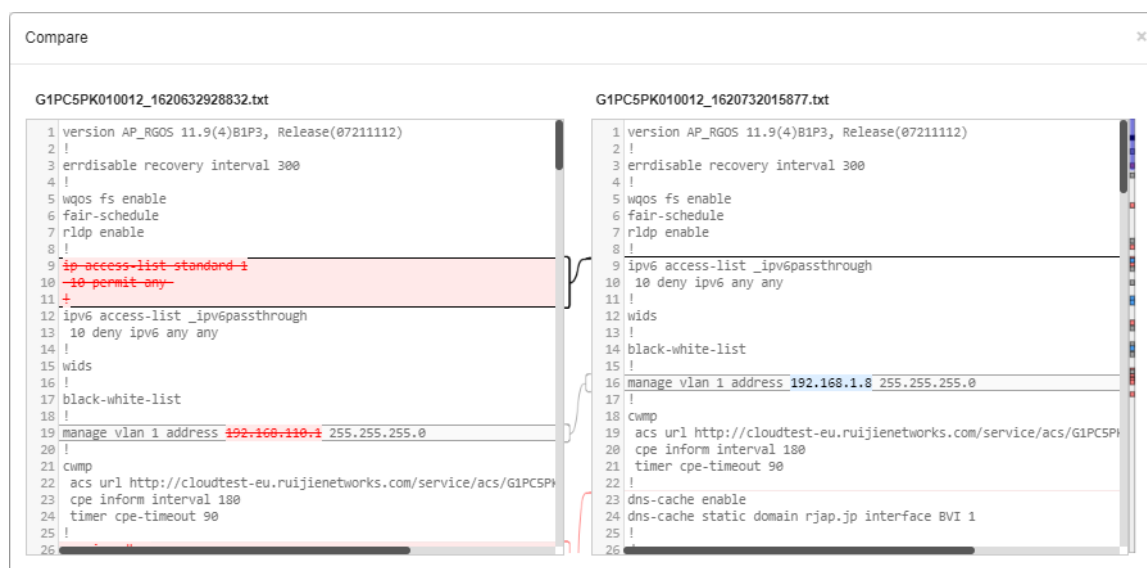

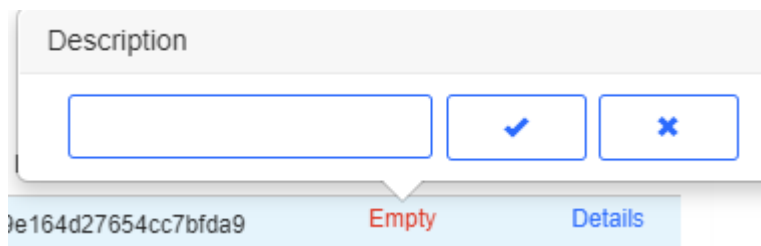Select one record, and click **Download** to download the configuration file.

Select one record, and click **Restore** to restore the current configuration.

Select one or multiple records, and click **Delete** to delete the backup record.

Select two records, and click **Compare** to compare the differences.

Description can be edited. Click **Details** in the **Action** column to check the backup configuration.

- Device Log

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.

5.5.1.3 Basic AP Operations

- Add AP
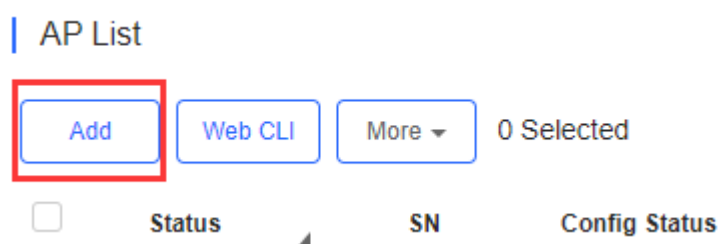
Select the network, and click **Add**. Both batch import and manual add are supported.

Non-apartment Scenario

To batch import APs, click **Download Template** to download the template, enter AP information, and click '**.xls' File** to import the template.

Add   ×

Download and fill in the template. Up to 200 records can be imported

".xls" File   Download Template

Click to select devices parsing rule **(Deafult Template)**

Add a Device   Close

To manually add APs, click **Add a Device**, enter SN and alias of the AP, and click **OK**. Click ✛ to add multiple APs.

Add   ×

1 SN [   ]   Alias [   ] 🗑 +

Batch Import   OK   Close

Apartment Scenario

To batch import APs, click **Download Template** to download the template, enter AP information, and click **'.xls' File** to import the template.

Add   ×

Download and fill in the template.Up to 500 records can be imported

".xls" File   Download Template

Click to select devices parsing rule **(Deafult Template)**

Add a Device   Close

Model	SN	MAC	PN	SSID	SSID Password	Alias	Room	Building Name	Remark

Model: device model, **optional**

SN: device serial number, **mandatory**

MAC: device MAC address, **optional**

PN: device part number, **optional**

SSID/SSID Password: support up to 4 SSIDs/SSID passwords, and each SSID and password need to be separated by ",", **optional**

Alias: device alias, **optional**

Room : the room that installs the device, **optional**

Building Name: the building that installs the device, **optional**

Remark: device remark**, optional**

You can also customize the template in EXCEL file to import devices. In order to parse the EXCEL file correctly, you should first create and specify the parse role.

Click **Click to select devices parsing rule**, and a new window pops up.

There will be one default rule.

1. **Add** button: Add a new rule

2. Menu bar: Display rule content

   - **Name**: User defined name

   - **snPosition**: Specify the starting position of SN in template

   - **ssidPosition**: Specify the starting position of SSID in template

   - **ssidPasswordPosition**: Specify the starting position of SSID's password in template

   - **roomPosition**: Specify the starting position of room number in template

   - **buildingNamePosition**: Specify the starting position of building name in template

   - **RemarkPosition**: Specify the starting position of remark in template

   If an entry is left empty, it will not be imported when importing the template. For example, ssidPosition will not be imported if it is empty.

※*User can customize the EXCEL parsing rule from columns A to Z and rows 1 to 15.*

3. Check box: Only one rule can be selected at a time

4. Rule control button:

- : Edit the rule

- : Delete the rule

- : Set the rule as default rule

5. Page up and down button

Import device by custom EXCEL file.

- Move to

Select one or multiple devices in the **AP List**, click **More** > **Move to**, select the new network and click **OK**.

- Delete

Select one or multiple devices in the **AP List**, click **More** > **Delete** and click **OK**.

- Reboot

Select one or multiple devices in the **AP List**, and click **Reboot.**

5.5.2   AC (beta)

5.5.2.1   AC List

The **AC List** displays basic device information, including online/offline status, SN, alias, management IP, MAC, public IP, network, firmware version, offline time, model and description.

The **AC List** automatically refreshes every minute. Click   to enable/disable the auto refresh function.

Above the list are the **Add, Web CLI, eWeb** and **Upgrade** functions. Click   to display **Reboot, Export** and **Delete** functions. For more information, refer to **Basic AC Operations**.

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

5.5.2.2   Device Details

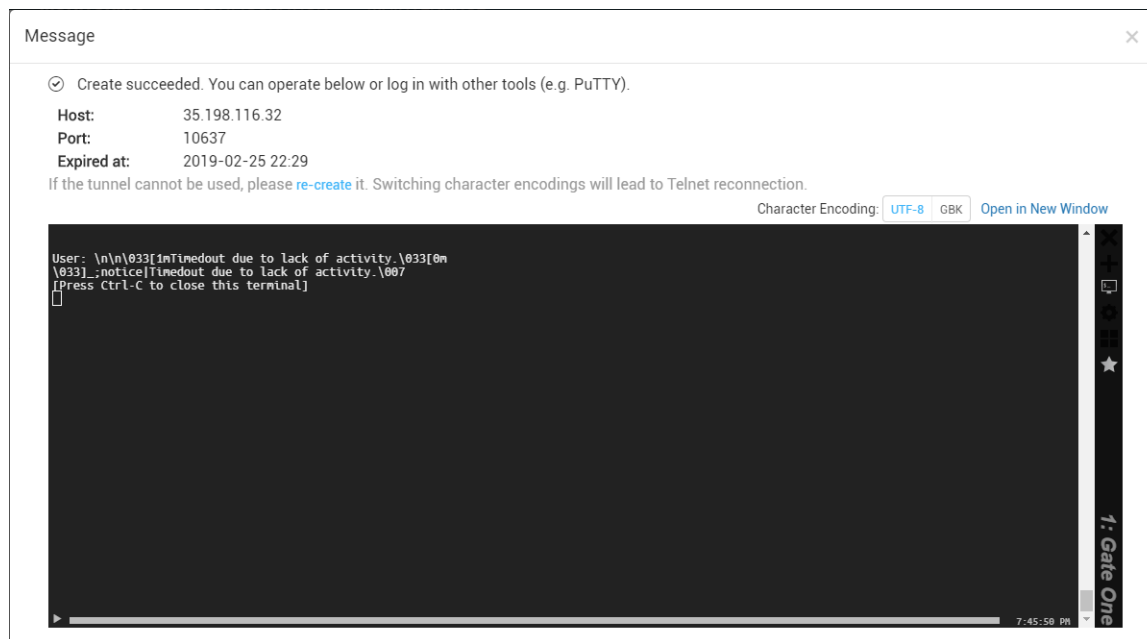Click the serial number in the device list to open the details page for a single device.

●   eWeb
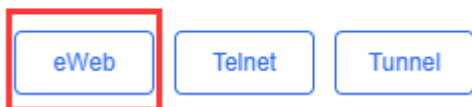
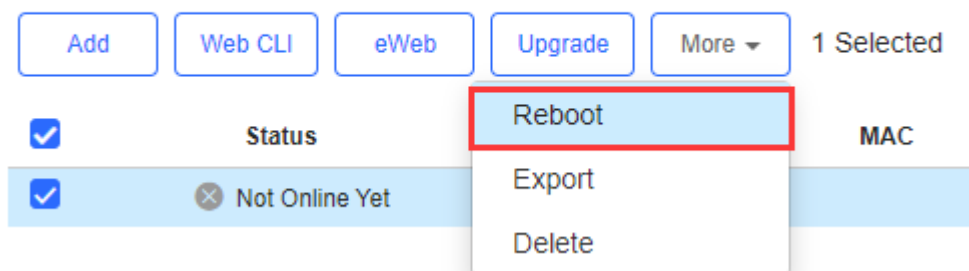Click **eWeb** to open the eWeb system in a new window.

●   Telnet

Click **Telnet** to connect to AC by Telnet protocol. Enter CLI commands to configure the AC.

- More > Reboot

Click **More** > **Reboot** to restart the AC.

- Refresh

Click to refresh all data in the page.

- Port Panel

The port panel imitates the actual AC panel, displaying the port type and status.

- Basic

Basic information includes the alias, model, SN and other information. Alias, MGMT Password and Description can be edited.

● Overview > CPU & Memory Usage

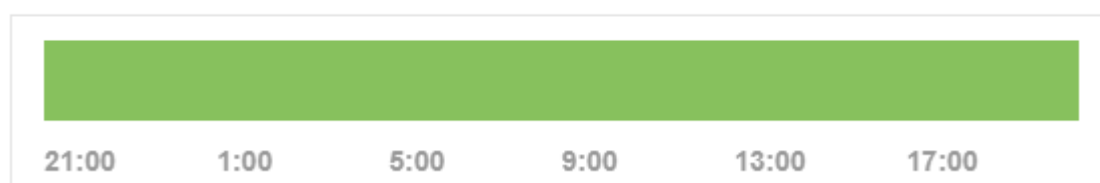CPU & memory usage are displayed here.

● Overview > Device Status

Device status includes online status, online clients and active clients.

● Overview > Connectivity

Connectivity refers to the connectivity (online status) between AC and Cloud Service within a period (1 day or 7 days).

● Overview > CPU/Memory Summary

CPU/memory summary over the 24 hours are displayed.

● Overview > Device Log

The device log records the historical operations, including online/offline, restart, upgrade and VLAN change, and supports queries based on log type and time.
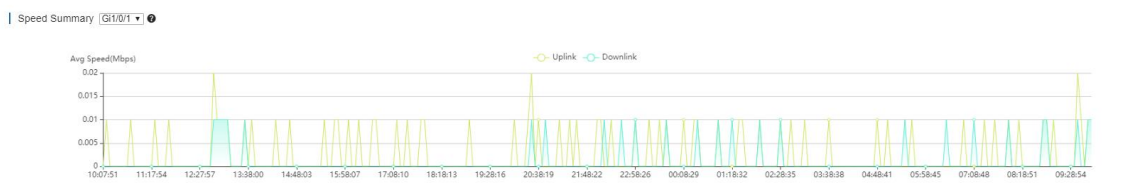
● Overview > Config Log

The Config log records the historical configuration delivery, and supports queries based on status and time.

● Port > Speed Summary

Uplink & downlink speed of port are displayed. This page supports queries based on day, week and month. Click to refresh the summary.

● Port > Port Status

Port						
Port Name	Admin Status	Status	Duplex Mode	Port Type	VLAN	PoE Status
Gi1/0/1	Enabled	Connected(1000M)	Full-duplex	Access	1	Unsupported
Te1/0/1	Enabled	Disconnected	Disconnected	Access	1	Unsupported
Gi1/0/2	Enabled	Disconnected	Disconnected	Access	1	Unsupported
Te1/0/2	Enabled	Disconnected	Disconnected	Access	1	Unsupported
Gi1/0/3	Enabled	Disconnected	Disconnected	Access	1	Unsupported
Gi1/0/4	Enabled	Disconnected	Disconnected	Access	1	Unsupported
Gi1/0/5	Enabled	Disconnected	Disconnected	Access	1	Unsupported
Gi1/0/6	Enabled	Disconnected	Disconnected	Access	1	Unsupported
Gi1/0/7	Enabled	Disconnected	Disconnected	-	-	Unsupported
Gi1/0/8	Enabled	Disconnected	Disconnected	-	-	Unsupported

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

Port information includes port name, VLAN etc.

● Config > AC Configuration Backup List

Backup List						
File Name	File Size	Time	Mode	MD5	Description	Action
G1ML11L000045_1586012511307.txt	5378		Auto	145f227d7f5c3b1aff24202fac8f1128		Details
G1ML11L000045_1585753262845.txt	5359		Auto	dd9f2a99891f3cbf70b94c7bb037a8af		Details
G1ML11L000045_1574694003928.txt	8758		Auto	a1af0dcf4fb86cd4e9cf7847b82e27aa		Details
G1ML11L000045_1574175664555.txt	8758		Auto	3cc0ac1b27e6c98bdde9d6d1eaa08587		Details
G1ML11L000045_1573830003576.txt	8745		Auto	71a75cec91d536e1f3db6b7c5be436b5		Details

First   Previous   Page ___ of 1   Next   Last   10 ▲   5 in total

The backup records include configuration file name, size, time, mode and MD5.

Click **Current** to display the current configuration. Click **Back up** in the **Config Details** page to back up the current configuration.

Config Details   ✕

```
Building configuration...
Current configuration: 5378 bytes

version AC_RGOS 11.9(5)B1, Release(06240613)
hostname ac177
!
wlan-config 1 ACtest1
 ssid-code utf-8
 wlan-based per-user-limit up-streams average-data-rate 200 burst-data-rate 200
 wlan-based per-user-limit down-streams average-data-rate 200 burst-data-rate 200
```

Backup

● Config > AP Configuration Backup List

The backup records include configuration file name, size, time, mode and MD5.

Click **Back up** and then click **OK** in the message box to back up the current configuration.

Select one record, and click **Download** to download the configuration file.

Select one record, and click **Restore** to restore the current configuration.

Select one or multiple records, and click **Delete** to delete the backup record.

Select two records, and click **Compare** to compare the differences

●   Tunnel > Create Tunnel

Create Tunnel

Select the tunnel type and click **Create Tunnel**. The tunnel types include Telnet, eWeb and SSH.

●   Tunnel > Tunnel List

Tunnel information includes tunnel type, host, port, destination device, expiration time and status. Click **Re-create** in the **Action** column to re-create a tunnel. Click **Telnet/eWeb** in the **Action** column to open the corresponding page.

5.5.2.3 Basic AC Operations

●   Add AC Network

●   Add AC

Click **Add**, enter the SN and Alias, and click **OK** to add an AC to the network. Only one AC can be added to a network.

●   eWeb

Select the device and click **eWeb**. The system will connect to AC and automatically open the eWeb page in a new window.

If a tunnel is created successfully but the eWeb page does not automatically open, a message is displayed as below. The user can manually click the link to open the page.
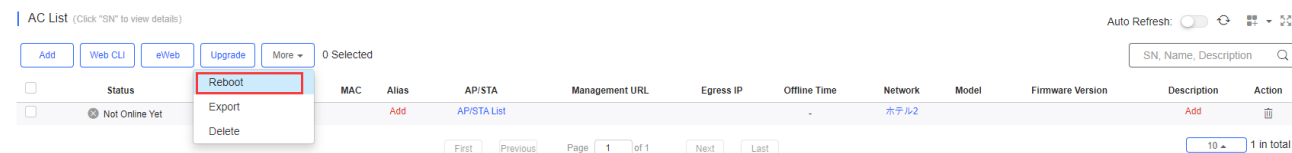
● Reboot

Select the device in the **AC List**, click **More** > **Reboot** and click **OK**.

● Web CLI

Select the device to be managed by CLI command, click **Web CLI.** The **Web CLI** page provides commonly-used CLI commands on the left. Click the command, or manually enter the command and click **Send**. Only one AC can be configured at a time.

● Tunnel Config
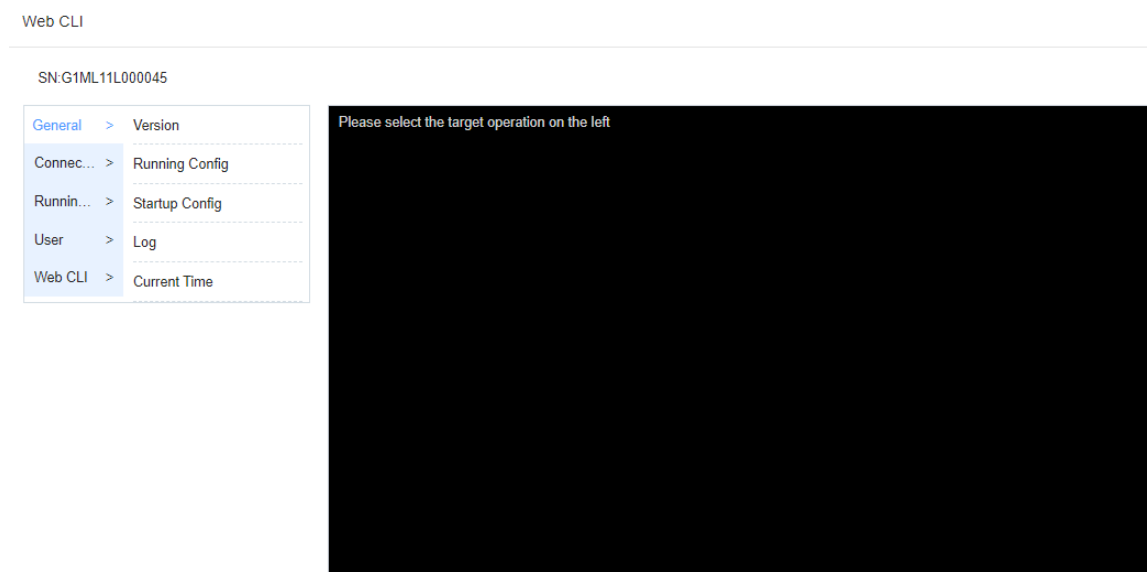
The user can create a Web-based tunnel to enter the eWeb system of an AC for more monitoring and management functions.

Note: If any security system exists in the network, such as a firewall, the traffic of destination TCP port 10000-10300 should be permitted.

Select the device for tunnel management, and click **More** > **Tunnel Config**. In the **Tunnel Management** page, only the **Web** type can be selected now, and the **Tunnel List** displays the tunnels already created.

Overview   Port   Config   **Tunnel**   Description: ✏️

| Create Tunnel

Type: [Telnet ▾]   [Create Tunnel]

| Tunnel List

[Local] [Global]

Click Refresh to update the tunnel status.   If the tunnel is unavailable, please close the tunnel and re-create it. If the re-created tunnel is still unavailable, please contact us for support.

🔄

Type	Host	Port	Destination Device	Destination Port	Expired at	Status	Action
			No Data				

First   Previ...   Page [0] of 0   Next   Last   [10 ▴] 0 in total

● **Delete**

| AC List (Click "SN" to view details)   Auto Refresh: ⬭ 🔄 ▦ ▾ ⛶

[Add] [Web CLI] [eWeb] [Upgrade ▾] [More ▾] 0 Selected   [SN, Name, Description 🔍]

Reboot
Export

☐	Status		MAC	Alias	AP/STA	Management URL	Egress IP	Offline Time	Network	Model	Firmware Version	Description	Action
☐	⊗ Not Online Yet			Add	AP/STA List			-	ホテル2			Add	🗑️

First   Previous   Page [1] of 1   Next   Last   [10 ▴] 1 in total

Select the device in the **AC List**, click **More** > **Delete** and click **OK**.

5.5.2.4   AP / STA List

| AC List (Click "SN" to view details)   Auto Refresh: 🔵 🔄 ▦ ▾ ⛶

[Add] [Web CLI] [eWeb] [Upgrade ▾] [More ▾] 0 Selected   [SN, Name, Description]

☐	Status	SN	MAC	Alias	AP/STA	Management URL	Egress IP	Offline Time	Network	Model	Firmware Version	Description	Action
☐	⊗ Not Online Yet	20210630		20210630	AP/STA List			-	となりまアップデバイスdhbfsdg56df4g515g4...			Add	🗑️

First   Previ...   Page [1] of 1   Next   Last   [10 ▴] 1 in total

Click **AP/STA List** to display AP and STA list.

| Fit AP List   ▦ ▾ ⛶

[MAC]   [Name]   [🔍 Search]

Status	MAC	SN	IP	Alias	Firmware Version	Model	Network	Description
					No Data			

First   Previ...   Page [0] of 0   Next   Last   [10 ▴] 0 in total

[Return]   0 Selected

| STA List   ▦ ▾ ⛶

[MAC]   [SSID]   [🔍 Search]

☐	IP	Client MAC	SSID	Online Time	Uplink Speed	Downlink Speed	Speed	Uplink Traffic	Downlink Traffic	Traffic	Band	RSSI	Auth Mode	Access Type	Channel	Uptime
								No Data								

First   Previ...   Page [0] of 0   Next   Last   [10 ▴] 0 in total

[Return]   0 Selected

5.5.3   Switch

5.5.3.1   Switch List

Status	SN	MAC	Alias	MGMT IP	Egress IP	Offline Time	Network	Model	Firmware Version	Description	Action
✓ Online	1234942570071	00d0.f822.335e	1930-50	172.18.20.207	120.35.11.140	2021-04-12 11:03:07	test	XS-S1930J-48GT4SFP	S1930J_RGOS 11.4(1)B70P10, Release(07233016)	Empty	🗑
⊘ Offline	1234942570088	00d0.f822.3366	1930-18GT2SFP	172.18.23.204	218.106.154.153	2021-02-01 16:34:07	test	XS-S1930J-18GT2SFP	S1930J_RGOS 11.4(1)B70P15, Release(08140110)	Empty	🗑
⊘ Offline	1234942570089	00d0.f822.3390	19-8GT	192.168.21.104	218.106.154.153	2021-02-03 16:05:07	default	XS-S1930J-8GT2SFP	S1930J_RGOS 11.4(1)B70P15, Release(08132618)	Empty	🗑
⊘ Offline	1234942570090	00d0.f822.336a	1930-18GT-P	192.168.21.103	120.35.11.140	2021-04-06 21:36:07	test	XS-S1930J-18GT2SFP-P	XS1930J_RGOS 11.4(1)B70P15, Release(08160218)	Empty	🗑
⊗ Not Online Yet	040800001		0408#00001			-	test_poeStatus_1 / test_poeStatus_1_1			Empty	🗑
⊗ Not Online Yet	040800002		0408#00002			-	test_poeStatus_1 / test_poeStatus_1_1			Empty	🗑
⊗ Not Online Yet	040800003		0408#00003			-	test_poeStatus_1 / test_poeStatus_1_1			Empty	🗑
⊗ Not Online Yet	040800004		0408#00004			-	test_poeStatus_1 / test_poeStatus_1_1			Empty	🗑
⊗ Not Online Yet	040800005		0408#00005			-	test_poeStatus_1 / test_poeStatus_1_1			Empty	🗑
⊗ Not Online Yet	040800006		0408#00006			-	test_poeStatus_1 / test_poeStatus_1_1			Empty	🗑

First Previous Page 1 of 321 Next Last   10 3206 in total

The **Switch List** displays basic device information, including the online/offline status, SN, MAC, alias, management IP & public IP, offline time, network, model, firmware version and description.

The **Switch List** automatically refreshes every minute. Click   to enable/disable the auto refresh function.

Above the list is the **Add Switch** and **Web CLI** function. Click   to display the **Move to**, **Delete**, and **Reboot** functions. For more information, refer to **Basic Switch Operations**.

The **Search** function supports fuzzy queries based on the serial number, alias and description, and also supports queries based on online/offline status.
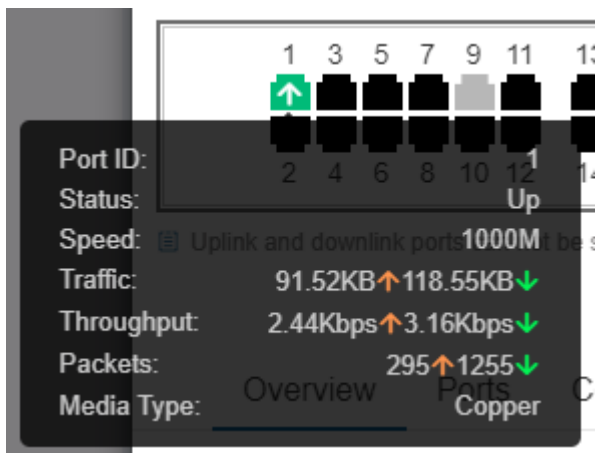
5.5.3.2   Device Details

Click the serial number in the device list to open the details page of a single device. The page displays detailed device information, including the port panel, basic information, overview, ports, config, PoE and diagnosis.

● Port Panel
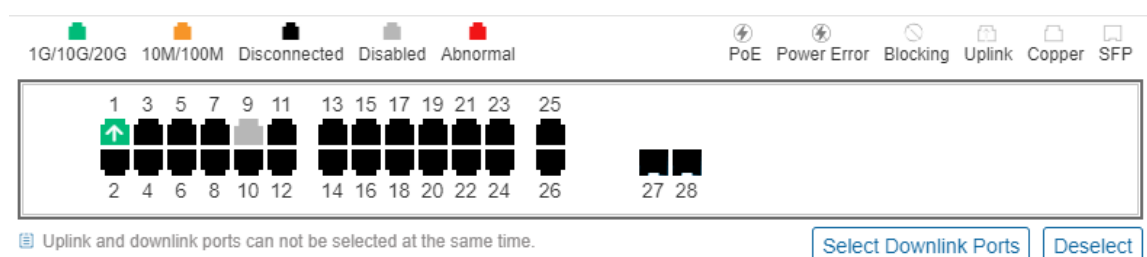
The port panel imitates the actual switch panel, displaying the port type, status and speed.

When you point the mouse to a port, the traffic, speed and other information of the port will be displayed.
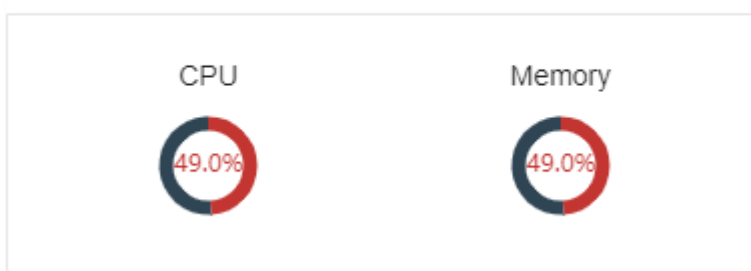
● Switch Info

Switch information includes the alias, model, SN and other information. **Alias** and **Description** can be edited.
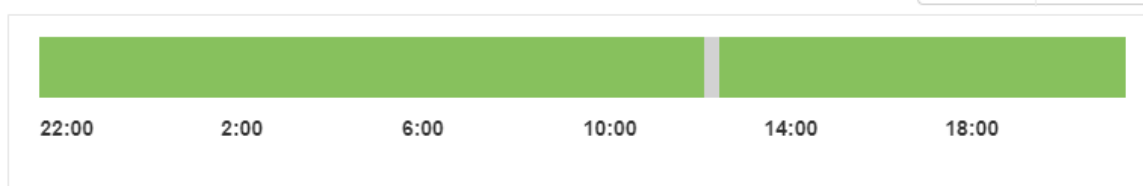
● Overview > CPU & Memory Usage

● Overview > Connectivity

Connectivity refers to the connectivity (online status) between Switch and Cloud Service within a period (1 day or 7 days).
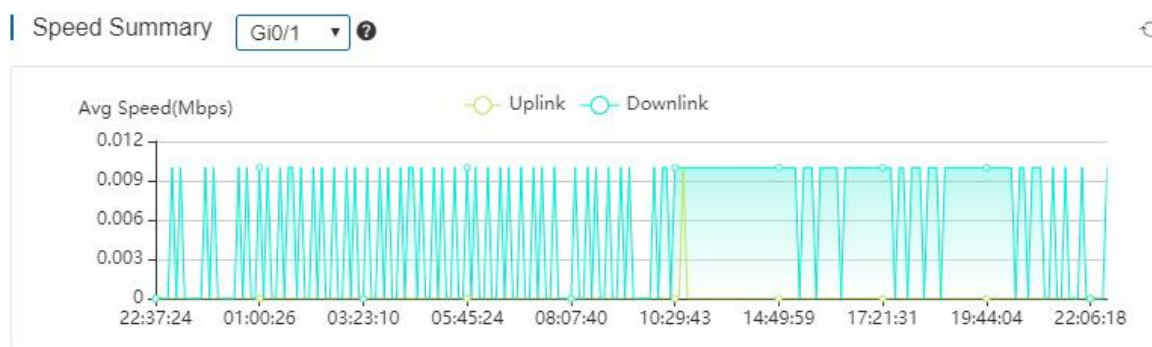
● Overview > Uplink

Uplink information includes the port, speed, duplex, uplink/downlink speed and uplink/downlink traffic.

● Overview > Speed Summary

Speed summary includes the uplink/downlink speed summary over the past 24 hours.

● Overview > Device Log

The device log records the historical operations, including online/offline, restart, upgrade, and VLAN change, and supports queries based on log type and time.

● Overview > Config Log

Log Record					Device Log	Config Log	Port Log

Operation Type	Started at	Ended at	Status	Description	Details
+ Device first online	2021-03-09 11:54	2021-03-09 11:54	Succeeded	Device: 1234942570071	
+ Switch device group	2020-12-10 17:43	2020-12-10 17:43	Succeeded	Device: 1234942570071. Group is changed fr...	
+ Initial online of the device	2020-12-10 17:33	2020-12-10 17:33	Succeeded	Device: 1234942570071	
+ Device first online	2020-12-09 17:12	2020-12-10 17:33	Aborted	Device: 1234942570071	

First   Previous   Page 1 of 1   Next   Last   10 ▲   4 in total

The config log records the historical configuration delivery, and supports queries based on status and time.

● Overview > Port Log

Log Record			Device Log	Config Log	Port Log

Port [   ]   2021-04-14 [   ]   Q Search   ↻

Port	Updated at	Content
	No Data	

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

The port log records the changes of port configuration, and supports queries based on port ID and time.

● Ports > Port Settings

| Port Settings

Admin Status	Enabled ⌄		Type	Access ⌄
Duplex Mode	Auto-negotiation ⌄		VLAN ID	1
Speed	⌄			
Description	Custom ⌄ [ ]			
PoE-Capable	On ⌄			
Media Type	Copper ⌄ Unsupported			

Save

Select one or multiple ports in the port panel to display and edit the port configuration, including admin status, duplex mode and speed.

● Ports > Port List

| Port List

Port	Admin Status	Status	Duplex Mode	Port Type	VLAN ID	PoE Status	Action
Gi0/1	Enabled	Connected(1000M)	Full-duplex	Access	1	Unsupported	
Gi0/2	Enabled	Disconnected	Disconnected	Access	1	Unsupported	
Gi0/3	Enabled	Disconnected	Disconnected	Access	1	Unsupported	
Gi0/4	Enabled	Disconnected	Disconnected	Access	1	Unsupported	
Gi0/5	Enabled	Disconnected	Disconnected	Access	1	Unsupported	
Gi0/6	Enabled	Disconnected	Disconnected	Access	1	Unsupported	
Gi0/7	Enabled	Disconnected	Disconnected	Access	1	Unsupported	
Gi0/8	Enabled	Disconnected	Disconnected	Access	1	Unsupported	
Gi0/9	Enabled	Disconnected	Disconnected	Access	1	Unsupported	
Gi0/10	Enabled	Disconnected	Disconnected	Access	1	Unsupported	

First   Previous   Page 1 of 6   Next   Last   10 ▲   52 in total

Port list includes the information of all ports, including port ID, admin status, port status, duplex mode, port type, VLAN ID and PoE status, and support queries based on admin status, port type and PoE status.

● Config > VLAN List

VLAN list includes the VLAN ID and the correspondingly ports.

● Config > SVI & DHCP

SVI & DHCP information includes VLAN ID, SVI and DHCP pool name. You can add, edit or delete the SVI or DHCP configuration.

Click **Add** to configure the IP and subnet mask of a VLAN, and configure the name, IP segment, subnet mask and gateway of DHCP service.

● Config > DHCP Snooping

Enable **DHCP Snooping Status**, select ports and click **Save**. The uplink port is selected by default if it is not routed port. If the port connecting to the DHCP server is not an uplink port, please select it manually.

- Config > RLDP

Enable **RLDP Status**, select one or multiple ports, choose the troubleshooting method for a loop, and click **Save**. The troubleshooting methods include **Warning, Warning and Block, Warning and Shutdown,** and **Shutdown SVI**. If **Warning** is chosen, the **Switch loopback detected (RLDP)** alarm should be enabled in the **Alarm Settings** page.

Click **Auto Config** to enable the default configuration.

Message   ✕

Uplink port of the switch: Gi0/1

Recommended Config: Detect the loop on all ports
except uplink and unavailable ports. Loop
Detection The solution is Warning and Block (For
Aggregate: Warning and Shutdown).

You can click Cancel to manually select ports and
customize the policy.

OK   Cancel

● Config > Service List

| Service List

Service	Admin Status	Value
eWeb	●	Login Password

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

Configure the admin status and login password of the eWeb service.

● Config > Configuration Backup List

| Configuration Backup List

Current   Back up   Download   Restore   Delete   Compare   0 Selected   ⟳ ⬛ ▾

	File Name	File Size	Time	Mode	MD5	Description	Action
☐	1234942570071_1615434805681	2.51K	2021-03-11 12:52:28	Auto	764c62a8a5767d03023cb89080c116d0	Empty	Details
☐	1234942570071_1610982066463	2.51K	2021-01-18 23:01:02	Auto	f8e9d47a45d450a4d0ada05ab94c7c2f	Empty	Details
☐	1234942570071_1607501546391	2.86K	2020-12-09 17:12:17	Auto	77576e33edfc31c4d6b132b7b4025ca8	Empty	Details

First   Previous   Page 1 of 1   Next   Last   10 ▲   3 in total

The backup records include configuration file name, size, time, mode and MD5.

Click **Current** to display the current configuration. Click **Backup** in the **Config Details** page to back up the current configuration.

Select one record, and click **Download** to download the configuration file.

Select one record, and click **Restore** to restore the current configuration.

Select one or multiple records, and click **Delete** to delete the backup record.

Select two records, and click **Compare** to compare the differences.

Description can be edited. Click **Details** in the **Action** column to check the backup configuration.
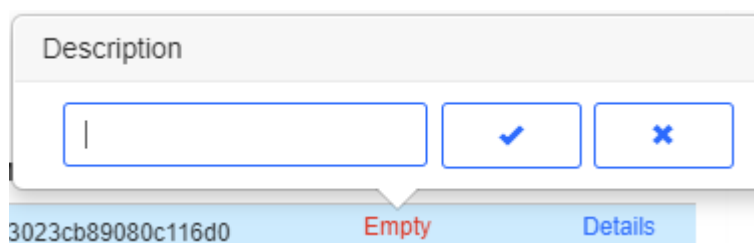
● PoE > PoE Port List

PoE Port List

Total Power:185.0 W, Current Power:0.0 W, Time:2019-04-09 18:50:47

Port	PoE-capable	PoE Status	Power	PD class	Description
Gi0/1	Enable	Off	0.0 W	NA	-
Gi0/2	Enable	Off	0.0 W	NA	-
Gi0/3	Enable	Off	0.0 W	NA	-
Gi0/4	Enable	Off	0.0 W	NA	-
Gi0/5	Enable	Off	0.0 W	NA	-
Gi0/6	Enable	Off	0.0 W	NA	-
Gi0/7	Enable	Off	0.0 W	NA	-
Gi0/8	Enable	Off	0.0 W	NA	-
Gi0/9	Enable	Off	0.0 W	NA	-
Gi0/10	Enable	Off	0.0 W	NA	-

First | Previous | Page 1 of 3 | Next | Last   10 ▲   24 in total

PoE statistics are displayed above **PoE Port List**, including the total power, current power and time.

PoE configuration includes the port, PoE-capable, PoE status, power, PD class and description.

5.5.4 PoE > Schedule Policy

Schedule Policy ^beta

Add

Policy Name	Time Period	Status	Action
jok	Weekdays(01:02~04:04)	Inactive	✎ 🗑

First | Previous | Page 1 of 1 | Next | Last   10 ▲   1 in total

The **Schedule Policy** displays the time period policy for powering off PoE ports, including the policy name, time period, and status indicating whether the policy has been used on ports.

5.5.5 PoE > Auto Checking Policy

Auto Checking Policy ^beta

Add

Policy Name	Ping Interval Time(s)	Retry Times	Check Failure Action	Action
uuuiuui	10	3	Reboot	✎ 🗑
jjk	10	3	Reboot	✎ 🗑

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

The **Auto Checking Policy** displays the auto-checking policy for checking the working status of a PD connected to a PoE port, including the policy name, ping interval, number of retry times, and action used upon check failure.

5.5.6   PoE > Poe Control Policy Setting

Poe Control Policy Setting ᵇᵉᵗᵃ

Port	Priority	Maximum Power	Offline Time Policy	Auto Checking Policy	Ping IP Address	Action
Gi0/1	Low		Never	Never		☑
Gi0/2	Low		Never	Never		☑
Gi0/3	Low		Never	Never		☑
Gi0/4	Low		Never	Never		☑
Gi0/5	Low		Never	Never		☑
Gi0/6	Low		Never	Never		☑
Gi0/7	Low		Never	Never		☑
Gi0/8	Low		Never	Never		☑

First   Previous   Page [1] of 1   Next   Last   [10 ▲] 10 in total

The **Poe Control Policy Setting** displays effective PoE port settings, including the power supply priority, maximum power, power supply stop policy, port auto-checking policy, and IP address for checking PDs.

● Diagnose > Fault Diagnosis

Fault Diagnosis

Type	PoE Power Supply ▼ ↻

Port   Please select a port for detection

No Power   Power   Abnormal   Undetectable   Uplink   Copper   SFP

```
      1  3  5  7  9 11   13 15 17 19 21 23   25
    ┌──────────────────────────────────────────────
    │ �◼ ◼ ◼ ◼ ◼ ◼   ◼ ◼ ◼ ◼ ◼ ◼   ◻
    │ ◼ ◼ ◼ ◼ ◼ ◼   ◼ ◼ ◼ ◼ ◼ ◼   ◻      ◻ ◻
      2  4  6  8 10 12   14 16 18 20 22 24   26      27 28
```

[Diagnose]   [Deep Diagnosis]

There are two types of fault diagnosis: **PoE Power Supply** and **SFP Port**. Select a port in the panel, click **Diagnose**, and the diagnosis procedure is displayed as below.

Procedure	History>>

19:48:15 Complete
Result: No exception detected

Advice: Please contact our after-sales personnel
19:48:15 Complete
Result: No exception detected

Advice: Please contact our after-sales personnel
📄 19:48:08 Port Gi0/3 Starting...

Click **History**, and the diagnosis history is displayed.

Status	Result	Advice	PoE-capable	PoE Status	PD Class	Voltage	Remaining Power	Start at
Complete	No exception detected	Please contact our after-sales personnel	Enable	off	N/A	0.0V	185.0 W	2019-04-09 20:01:59

History   Procedure>>

First   Previous   Page [1] of 1   Next   Last   [10 ▲] 1 in total

Select a port in the panel, click **Deep Diagnose**, and click **Diagnose** in the **PoE Diagnosis** page.

Normal diagnosis: The Cloud server delivers CLI commands to collect the switch information, and the diagnosis occurs on the Cloud server.

Deep diagnosis: The diagnosis occurs on the switch, and the results are reported to the Cloud server.

5.5.6.1 Basic Switch Operations

● Add Switch

Select the network, and click **Add**. Both batch import and manual add are supported.

Click **Download Template** to download the template, enter switch information, and click **'.xls' File** to import the template.

Click **Add a Device**, enter SN and alias of the switch, and click **OK**. Click ╋ to add multiple switches.

● Move to

Select one or multiple devices in the **Switch List**, click **More** > **Move to**, select the new network and click **OK**.

● Delete

Select one or multiple devices in the **Switch List**, click **More** > **Delete** and click **OK**.

- **Reboot**

Select one or multiple devices in the **Switch List**, and click **Reboot.**

Select one or multiple devices in the **Switch List**, and click **Web CLI**. The **Web CLI** dialog box is displayed, and device information can be queried via the menus in this dialog box. The menus vary with the products.
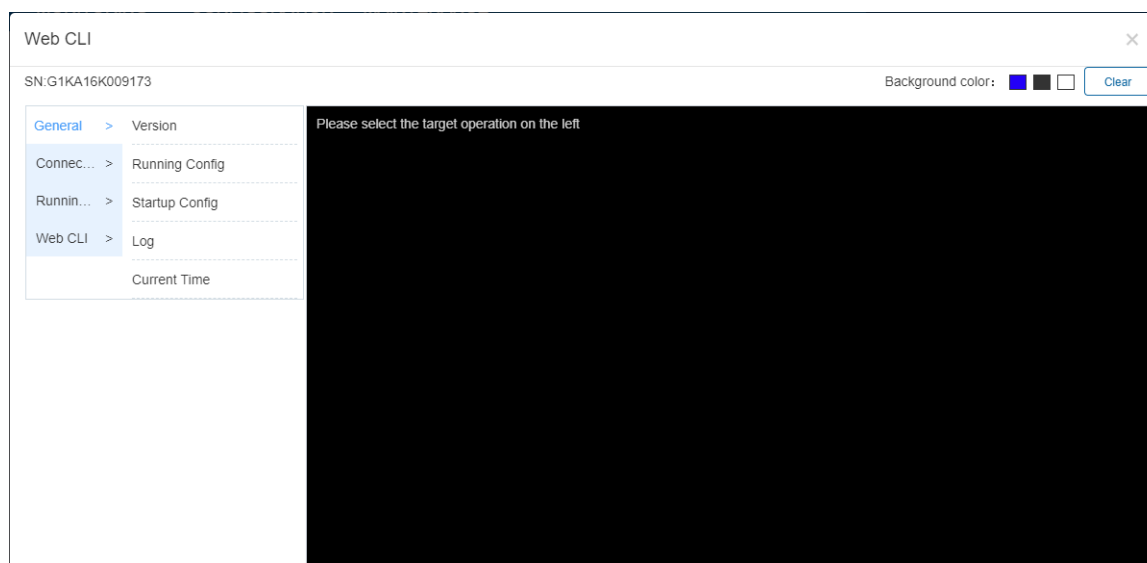
In addition, in the command entry box, the **TAB** key and question mark (?) both can complete a command.
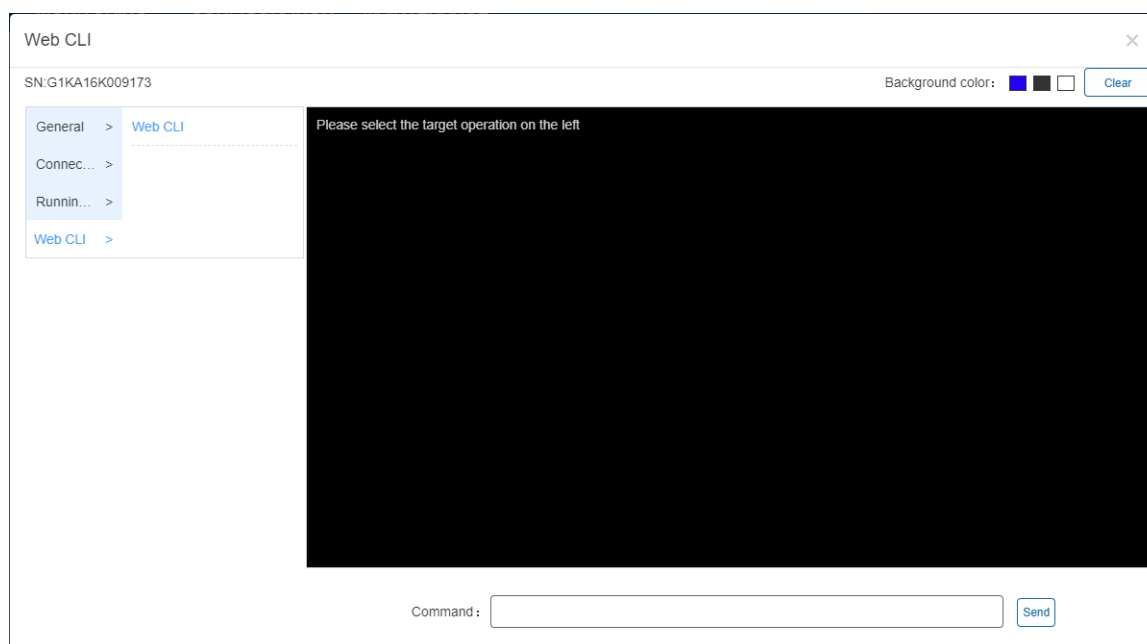
5.5.7   Gateway

5.5.7.1   Gateway List

The **Gateway List** displays basic device information, including the online/offline status, SN, alias, management IP, MAC, public IP, network, firmware version, offline time, model and description.

The **Gateway List** automatically refreshes every minute. Click ⟨Auto Refresh: ⬤⟩ to enable/disable the auto refresh function.

Above the list are the **Add Gateway**, **Web CLI** and **eWeb** functions. Click ⟨More ▾⟩ to display the **Move to**, **Reboot**, **Tunnel** and **Delete** functions. For more information, refer to **Basic Gateway Operations**.

The **Search** function supports fuzzy queries based on the serial number, alias and description, and also supports queries based on online/offline status.

5.5.7.2   Device Details

● Web CLI

Click **Web CLI**, and the **Web CLI** page is displayed. The **Web CLI** page provides commonly-used CLI commands on the left. Click the command, or manually enter the command and click **Send**.
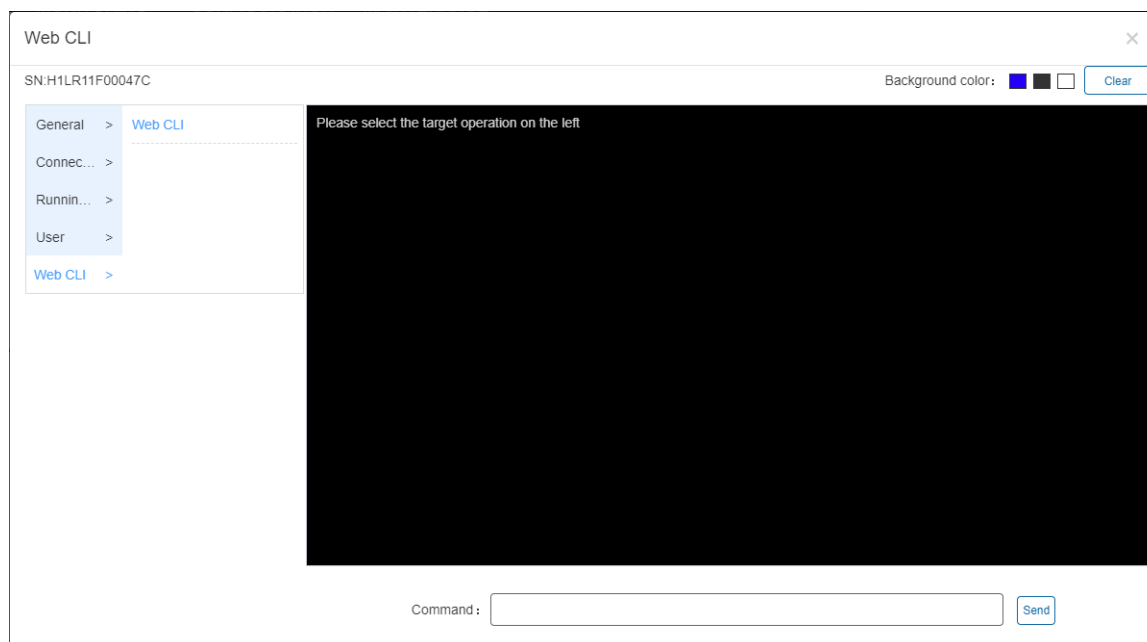
- eWeb

Click **eWeb** to open the eWeb system in a new window.

- Telnet

Click **Telnet**, and a window is opened to connect to the gateway by Telnet protocol. Enter CLI commands to configure the gateway.
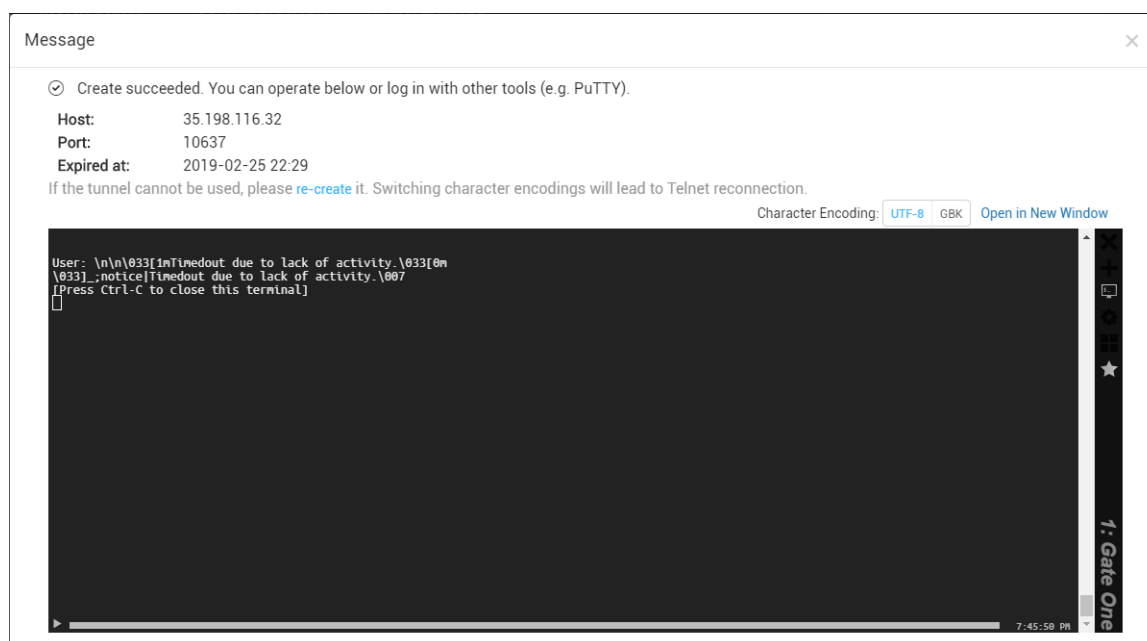
- More > SSH
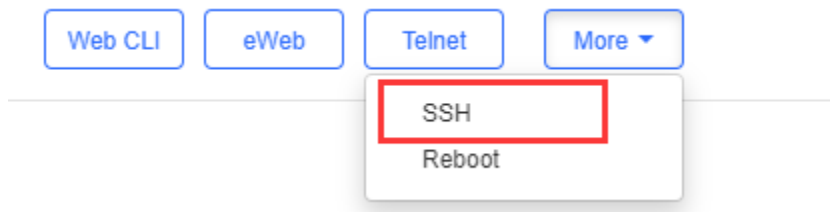
Click **More** > **SSH**, and a window is opened to connect to the gateway by SSH protocol. Use other SSH tools to connect to the gateway.
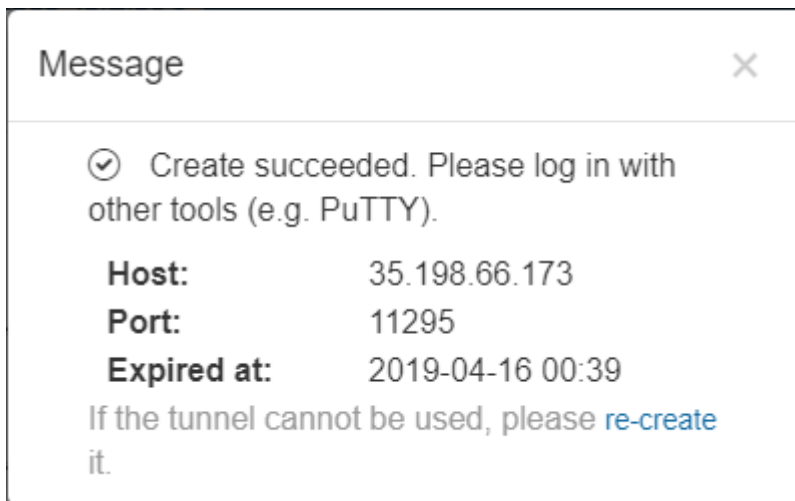
● More > Reboot
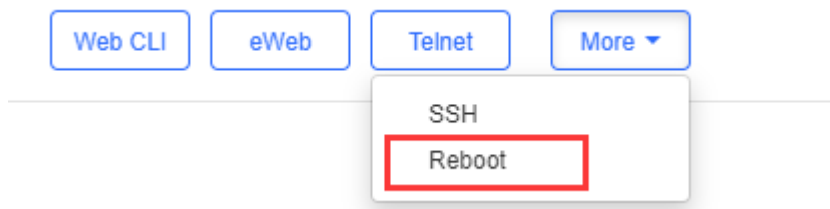
Click **More** > **Reboot** to restart the gateway.

● Refresh

Click to refresh all data in the page.
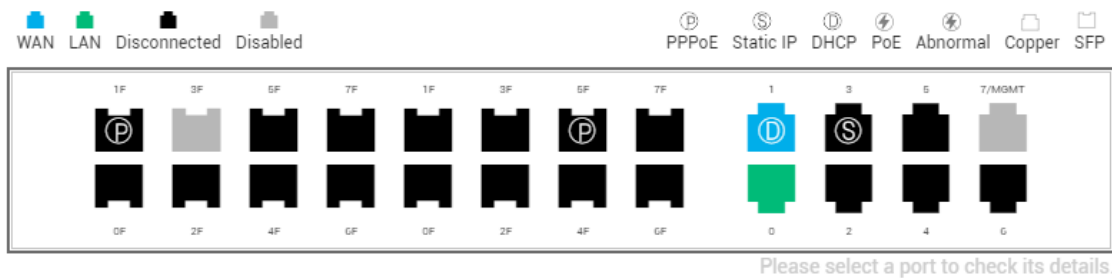
● Port Panel

The port panel imitates the actual gateway panel, displaying the port type and status.

● Basic

Basic information includes the alias, model, SN and other information. **Alias, MGMT Password** and **Description** can be edited.

● Overview > CPU & Memory Usage

CPU & memory usage are displayed here.

● Overview > Device Status

Device status includes online status, online clients and sessions.

● Overview > Connectivity
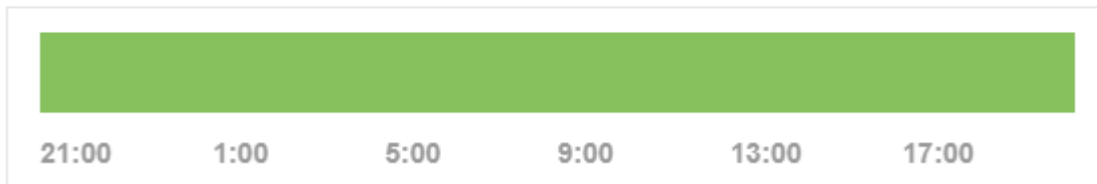
Connectivity refers to the connectivity (online status) between Gateway and Cloud Service within a period (1 day or 7 days).

● Overview > Speed Summary
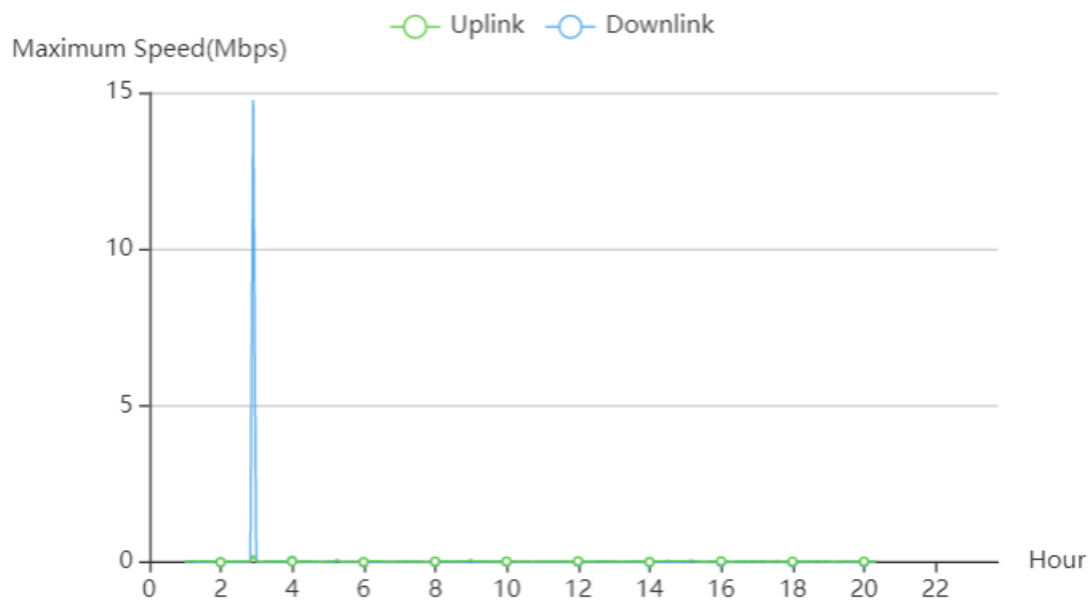
The uplink/downlink speed summary over the 24 hours is displayed.

● Overview > Client Summary

2021-06-28 Client Summary
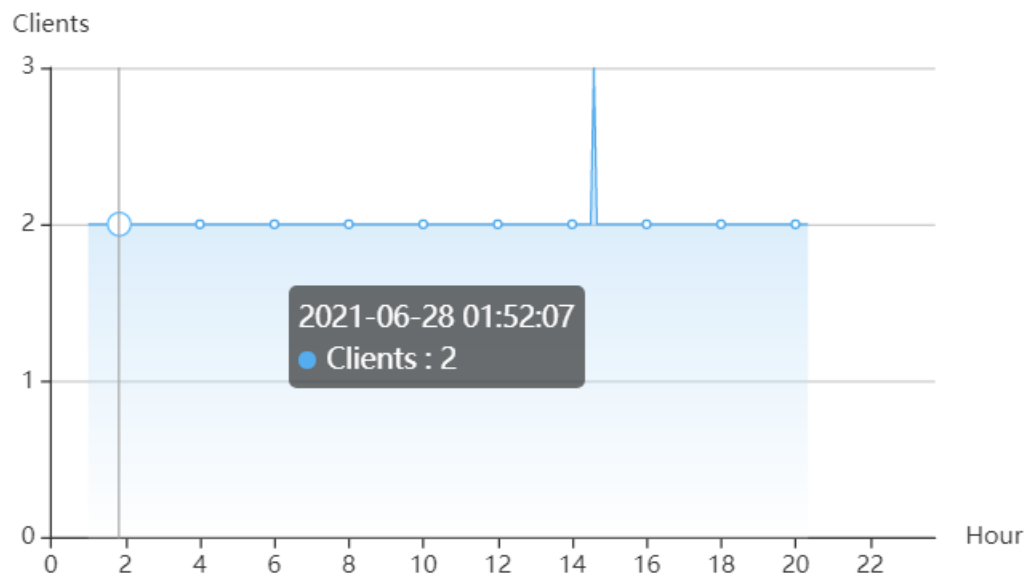
The client statistics over the 24 hours are displayed.

● Overview > CPU/Memory Summary

2019-02-23~2019-02-24 CPU/Memory Summary
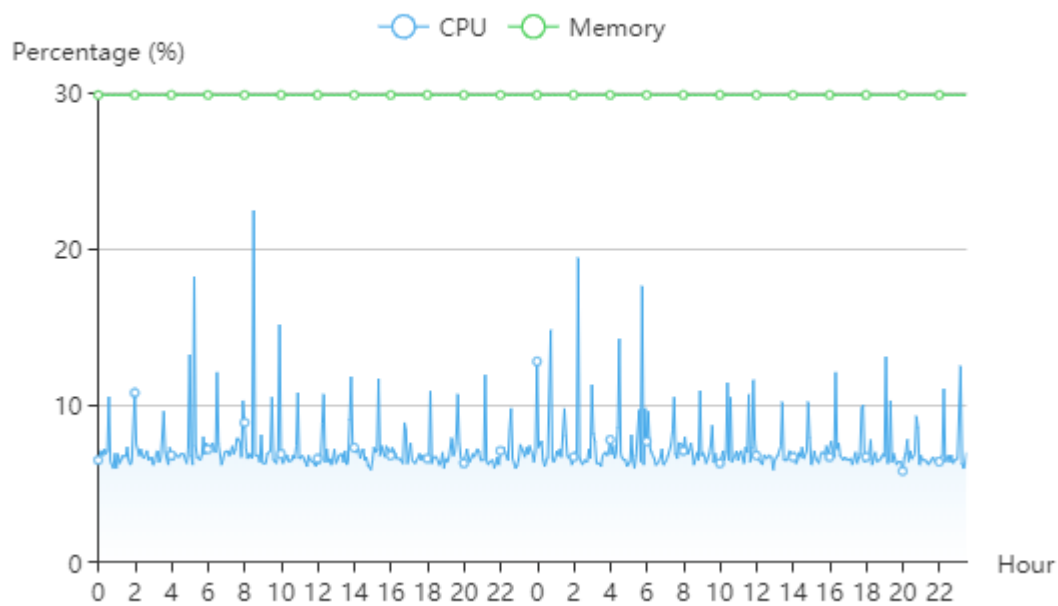
CPU/memory summary over the 24 hours are displayed.

● Overview > Session Summary

2019-02-23~2019-02-24 Session Summary
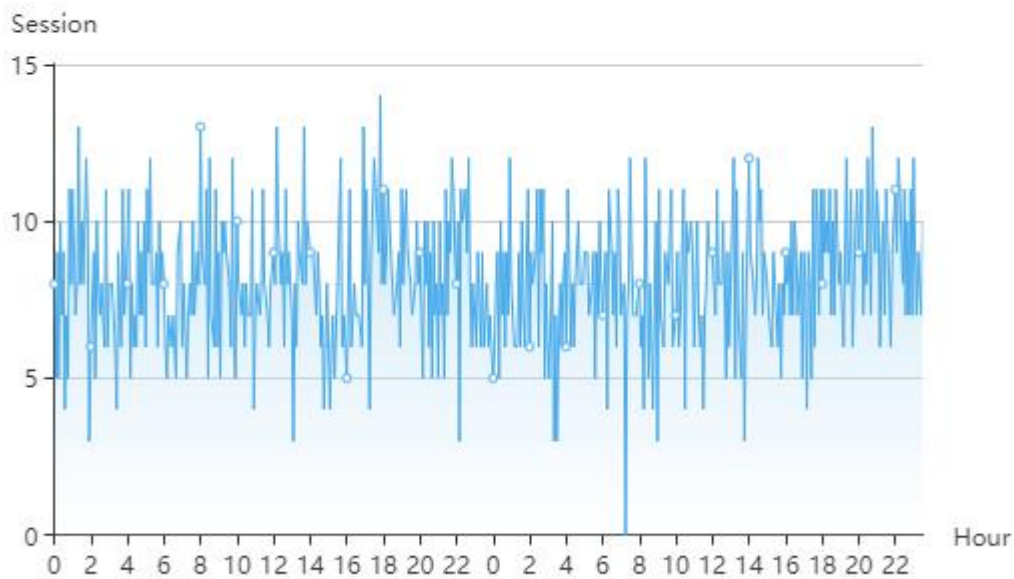
Session summary over the 24 hours is displayed.

● Overview > Top 10 Applications by Traffic

| Top 10 Applications by Traffic

No.	Application	Traffic
1	HTTP-BROWSE	2.17 KB ↓ /2.81 KB ↑
2	SYN_ACK	240.00 B ↓ /456.00 B ↑
3	UDP-COMMUTE	81.00 B ↓ /75.00 B ↑
4	LOOKMYPC	25.00 B ↓ /75.00 B ↑
5	DNS	0.00 B ↓ /0.00 B ↑

Top 10 applications by downlink traffic are displayed.

● Overview > Top 10 Users by Traffic

| Top 10 Users by Traffic

No.	Username	Traffic
1	10.10.12.2	1.88 KB ↓ /1.76 KB ↑
2	10.10.12.1	639.00 B ↓ /1.65 KB ↑

Top 10 users by downlink traffic are displayed.

● Overview > Device Log

| Log Record | | | Device Log | Config Log |

All ▾   🔍 Search   ↻ ▦ ▾

Type	Updated at	Content
Online/Offline	2021-04-13 11:38:07	Device offline. The final time when it sends packets to MACC is: 2021-04-13 11:38:07(It is an estimated value. The deviation is 1 minute.)
Online/Offline	2021-04-12 11:33:22	Device online
Reboot	2021-04-12 11:33:22	Device restart
Online/Offline	2021-04-12 11:12:07	Device offline. The final time when it sends packets to MACC is: 2021-04-12 11:12:07(It is an estimated value. The deviation is 1 minute.)
Online/Offline	2021-04-11 13:48:03	Device goes online for the first time
Online/Offline	2021-04-05 16:35:16	Device online
Reboot	2021-04-05 16:35:16	Device restart
Online/Offline	2021-04-05 11:02:07	Device offline. The final time when it sends packets to MACC is: 2021-04-05 11:02:07(It is an estimated value. The deviation is 1 minute.)
Online/Offline	2021-04-01 11:29:17	Device online
Online/Offline	2021-04-01 11:27:07	Device offline. The final time when it sends packets to MACC is: 2021-04-01 11:27:07(It is an estimated value. The deviation is 1 minute.)

First   Previous   Page 1 of 9   Next   Last   10 ▲   89 in total

The device log records the historical operations, including online/offline, restart, upgrade and VLAN change, and supports queries based on log type and time.

● Overview > Config Log

| Log Record | | | Device Log | Config Log |

🔍 Search   ↻ ▦ ▾

	Operation Type	Started at	Ended at	Status	Description	Details
+	Switch device group	2021-04-12 15:26	2021-04-12 15:27	Succeeded	Device: H1MSC0M000147. Group is changed ...	
+	Device first online	2021-04-11 13:48	2021-04-11 13:49	Succeeded	Device: H1MSC0M000147	
+	Switch device group	2021-04-09 17:02	2021-04-09 17:02	Succeeded	Device: H1MSC0M000147. Group is changed ...	
+	Switch device group	2021-04-09 15:32	2021-04-09 15:32	Succeeded	Device: H1MSC0M000147. Group is changed ...	
+	Switch device group	2021-04-01 17:16	2021-04-01 17:17	Succeeded	Device: H1MSC0M000147. Group is changed ...	
+	Switch device group	2021-04-01 17:13	2021-04-01 17:14	Succeeded	Device: H1MSC0M000147. Group is changed ...	
+	Switch device group	2021-03-25 14:46	2021-03-25 14:49	Succeeded	Device: H1MSC0M000147. Group is changed ...	
+	Switch device group	2021-03-25 12:39	2021-03-25 12:40	Succeeded	Device: H1MSC0M000147. Group is changed ...	
+	Switch device group	2021-03-25 12:15	2021-03-25 12:16	Succeeded	Device: H1MSC0M000147. Group is changed ...	
+	Switch device group	2021-03-25 11:38	2021-03-25 11:39	Succeeded	Device: H1MSC0M000147. Group is changed ...	

First   Previous   Page 1 of 6   Next   Last   10 ▲   59 in total

The Config log records the historical configuration delivery, and supports queries based on status and time.

● WAN > Port

| Port   Gi0/6 ▾

Select one WAN port to display the corresponding port information and rate summary.

● WAN > Basic

Basic

IP :   172.17.126.2

Subnet Mask: 255.255.255.128

Description: GigabitEtherne0/6

Basic information includes the IP, subnet mask and description. If PPPoE is enabled and dialing port is configured, the PPPoE information is displayed.

PPPoE

Port: di2

IP Type: adsl

Uplink Bandwidth: --

Downlink Bandwidth: --

● WAN > Speed Summary

Speed Summary

2021-4 Speed Summary
─○─ Uplink   ─○─ Downlink
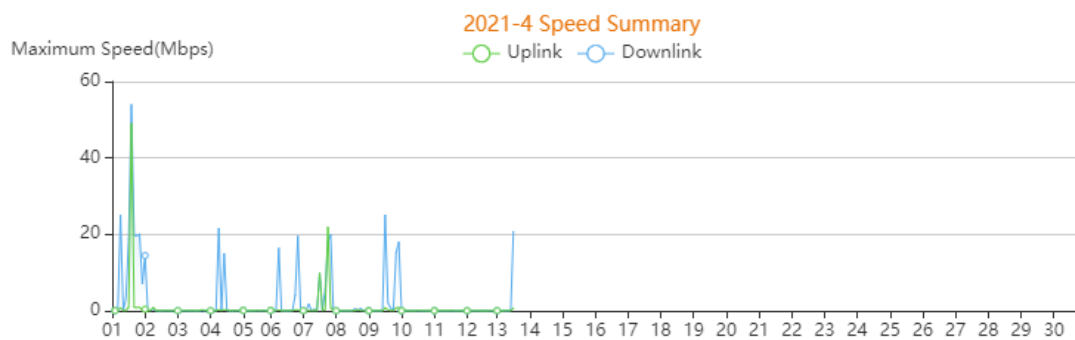
Uplink & downlink rate of WAN port are displayed. This page supports queries based on day, week and month. Click to refresh the summary.

● WAN > Port Status

Port Status(Only daily summary is supported)

2019-04-07~2019-04-08 Packet Loss Rate

2019-04-07~2019-04-08 Latency
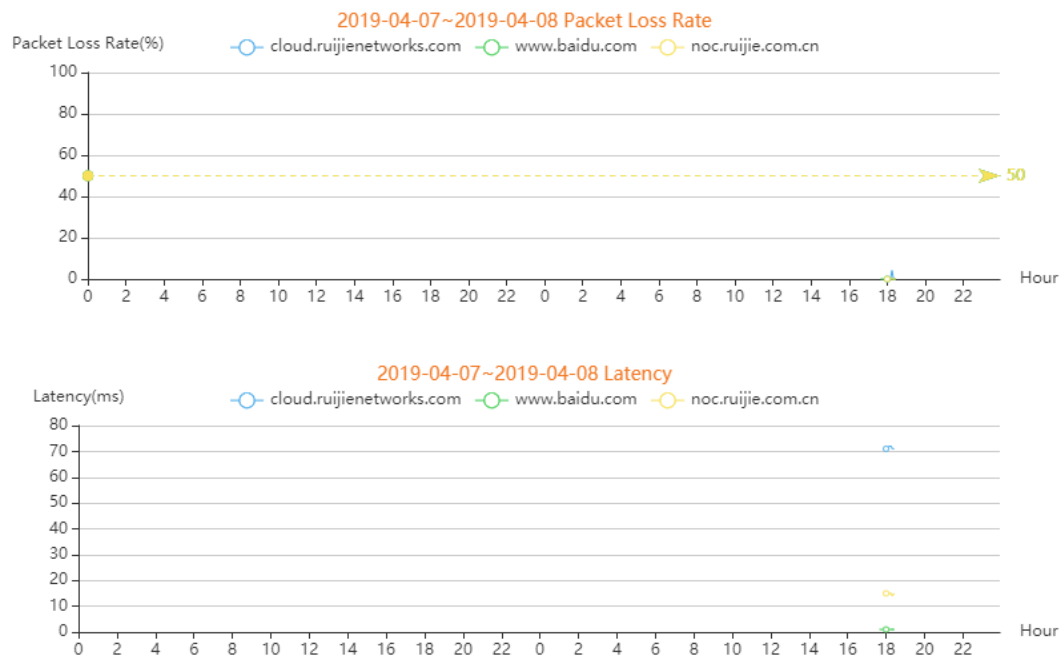
Packet loss rate and latency summary are displayed. This page supports queries based on day, week and month. Click

to refresh the summary.

- LAN > Port

Select a LAN port to display the corresponding information of its switch port, routed port and subinterface.

- LAN > Switch Port

Switch port information includes the switch port, including duplex and rate.

- LAN > Routed Port

Routed Port (Gi0/2)

IP :   192.168.1.1

Subnet Mask: 255.255.255.0

LAN: LAN 1,LAN 2,LAN
                 3,LAN 4,LAN 5,LAN
                 6,LAN 7

Description: --

Routed port information includes the IP address, subnet mask, LAN and description.

● LAN > Subinterface

Subinterface (Gi0/2)

Name	IP	VLAN
Gi0/2.1	192.168.2.1	2
Gi0/2.2	192.168.3.1	3

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

Subinterface information includes the name, IP address, and VLAN.

● Config > Configuration Backup List

Configuration Backup List

Current   Back up   Download   Restore   Delete   Compare

	File Name	File Size	Time	Mode	MD5	Description	Action
☐	H1MSC0M000147_1618208997448	30.04K	2021-04-12 15:29:30	Auto	d3fcb3d5a8db89e164d27654cc7bfda9	Empty	Details
☐	H1MSC0M000147_1618195178807	108.35K	2021-04-12 11:39:28	Auto	0219f5b7edb89853074fdecdd2b836e2	Empty	Details
☐	H1MSC0M000147_1618122070639	108.03K	2021-04-11 15:20:51	Auto	3d71a80b58661abdb424ca438d8c4948	Empty	Details
☐	H1MSC0M000147_1618116679633	107.89K	2021-04-11 13:51:04	Auto	5328fb08052081b499a066da689886c5	Empty	Details
☐	H1MSC0M000147_1617955686114	29.72K	2021-04-09 17:08:00	Auto	feea84fc058b8d9f879784d361524da8	Empty	Details
☐	H1MSC0M000147_1617953636882	107.83K	2021-04-09 16:33:37	Auto	f2df3218a0b2ccd4a5d13c8d2a5389e2	Empty	Details
☐	H1MSC0M000147_1617951834771	101.10K	2021-04-09 16:03:29	Auto	d1ca38a3303a326f4d88e94c3e5b8b30	Empty	Details
☐	H1MSC0M000147_1617950041310	100.66K	2021-04-09 15:33:23	Auto	e9a6409bb30296b1182ab532b3658fa9	Empty	Details
☐	H1MSC0M000147_1617938046093	29.59K	2021-04-09 12:14:00	Auto	6c471fef9ffbf1c13ca8e0b197bff298	Empty	Details
☐	H1MSC0M000147_1617884371738	29.85K	2021-04-08 21:19:24	Auto	8fa8698f8ff3f2d50eecb6ba2d287da9	Empty	Details

First   Previous   Page 1 of 3   Next   Last   10 ▴   30 in total

The backup records include configuration file name, size, time, mode and MD5.

Click **Current** to display the current configuration. Click **Backup** in the **Config Details** page to back up the current configuration.

Click **Back up** and then click **OK** in the message box to back up the current configuration.

Select one record, and click **Download** to download the configuration file.

Select one record, and click **Restore** to restore the current configuration.

Select one or multiple records, and click **Delete** to delete the backup record.

Select two records, and click **Compare** to compare the differences

Description can be edited. Click **Details** in the **Action** column to check the backup configuration.

- PoE > PoE List

Port	Physical Port	PoE-capable	PoE Status	Power	PD class
port0	Gi0/0	Disable	Off	0.0W	Unknown
port1	LAN 1	Enable	Off	0.0W	Unknown
port2	LAN 2	Enable	Off	0.0W	Unknown
port3	LAN 3	Enable	On	6.0W	4
port4	LAN 4	Enable	Off	0.0W	Unknown
port5	LAN 5	Enable	Off	0.0W	Unknown
port6	LAN 6	Enable	Off	0.0W	Unknown
port7	LAN 7	Enable	Off	0.0W	Unknown

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

PoE configuration includes the port, physical port, PoE-capable, PoE status, power and PD class.

● **Alarm**

Alarm	To configure alarm settings, click here. To apply the configuration to other devices, click here.
Type	Rule
Threshold ❓	Egress Channel Width (The values are automatically retrieved. If incorrect, please modify the value manually, and the system will not automatically fetch values any more)
	REMOTE_CONF_1 Uplink Channel Width 1000 M Downlink Channel Width 1000 M
	REMOTE_CONF_7 Uplink Channel Width 1000 M Downlink Channel Width 1000 M
	If the bandwidth exceeds 80 % of threshold for 5 times, the alarm is sent.
Port Status/Packet Loss Speed	Test: ⬤

Insufficient bandwidth: When the bandwidth exceeds the specified percentage of threshold for several times, the alarm is sent. The threshold, times and percentage can be configured manually.

Ping failure: When the Ping test failed for the specified times, the alarm is sent. The times and domain/IP address can be configured manually.

High packet loss rate: When the packet loss rate exceeds the specified percentage of threshold for several times in 5 minutes, the alarm is sent. The times and threshold can be configured manually.

Besides, the corresponding alarm should be enabled in the **Alarm Settings** page. For insufficient bandwidth, the alarm types are **Uplink rate above threshold on gateway** and **Downlink rate above threshold on gateway**; for Ping failure, the alarm type is **Abnormal network access on gateway**; and for high packet loss rate, the alarm type is **High packet loss rate on gateway.**

Alarm Settings				↻ 〰
Type	Status	Alarm Threshold	Email Alarm
Device goes offline	⬤	-	◯
Device goes online and offline continually	⬤	>20 % ⊘	◯
All devices are offline	⬤	-	⬤
High channel usage on AP	⬤	-	◯
System usage(CPU/memory usage) above threshold	⬤	-	⬤
Switch loopback detected (RLDP)	⬤	-	◯
interface updown rate above threshold.	◯	-	◯
Abnormal network access on gateway	⬤	-	◯
High packet loss rate on gateway	⬤	-	◯
Uplink rate above threshold on gateway	⬤	-	⬤
Downlink rate above threshold on gateway	⬤	-	⬤

After changing the configuration, click **Save** below.

When the modified bandwidth and the actual bandwidth do not match, click **Fetch Bandwidth** to check the actual bandwidth which will then be set as the threshold.

●   Tunnel > Create Tunnel

Select the tunnel type and click **Create Tunnel**. The tunnel types include **Telnet**, **eWeb** and **SSH**.

●   Tunnel > Tunnel List

| Tunnel List

If the tunnel is unavailable, please re-create it or contact us for support.

Type	Host	Port	Destination Device	Destination Port	Expired at	Status	Action
eWeb	35.221.107.197	10000	Local	80	2021-04-07 23:37	Disabled	Re-create
eWeb	35.221.107.197	10000	Local	80	2021-03-16 15:10	Disabled	Re-create
Telnet	35.221.107.197	10000	Local	--	2021-03-11 14:38	Abnormal	Re-create
SSH	35.221.107.197	10004	Local	--	2021-03-10 19:12	Abnormal	Re-create
Telnet	35.221.107.197	10003	Local	--	2021-03-10 19:11	Abnormal	Re-create
Telnet	35.221.107.197	10002	Local	--	2021-03-10 19:07	Disabled	Re-create
eWeb	35.221.107.197	10001	Local	80	2021-03-10 19:03	Abnormal	Re-create
Telnet	35.221.107.197	10000	Local	--	2021-03-10 16:36	Abnormal	Re-create
eWeb	35.221.107.197	10021	Local	80	2021-02-27 14:33	Disabled	Re-create
Telnet	35.221.107.197	10020	Local	--	2021-02-25 20:27	Disabled	Re-create

First   Previous   Page 1 of 3   Next   Last   10 ▲   28 in total

Tunnel information includes tunnel type, host, port, destination device, expiration time and status. Click **Re-create** in the **Action** column to re-create a tunnel. Click **Telnet/SSH** in the **Action** column to open the corresponding page.

5.5.7.3 Basic Gateway Operations

● Add Gateway

| Gateway List

[Add]   [Web CLI]   [eWeb]   [More ▼]   0 Selected

Click **Add**, enter the SN, Alias and Web Password, and click **OK** to add a gateway to the network. Only one gateway can be added to a network.

Add   ✕

SN [   ]   Alias [   ]

Tip: Please enter the password of admin account of the eWeb system to authorize Cloud to manage this device. You can skip this step now, and authorize the password and check the results in MONITORING > Device > Gateway.

Password [   ]

[OK]   [Close]

Unauthorized Gateway List						
SN	Alias	Status	Network	Added at	Action	
eeeeeeeeeee30		No password	vvvvvvvvvv00011111111_____...	2020-12-18 10:35:06	Re-authorize Delete	

First   Previous   Page 1 of 1   Next   Last   5 ▲ 1 in total

Before a gateway is authorized, it is displayed in the **Unauthorized Gateway List**. If authorization fails, you can click **Re-authorize** in the **Action** column to re-enter the Web password to re-authorize the device.

Message ✕

Note: Password verification needs to interact with the device. If the device is offline, the system needs to wait for it to go online. If the password of admin account is the default password, please change the password first.

Password : [＿＿＿＿＿]

OK   Cancel

● eWeb

Gateway List

Add	Web CLI	eWeb	More ▾	0 Selected

☐	Status	SN	Alias	MGMT IP
☐	⊗ Offline	H1MSC0M000147	Empty	192.168.21.

Select the device to be managed by eWeb, and click **eWeb**. The system will try to connect the gateway and automatically open the eWeb page in a new window.
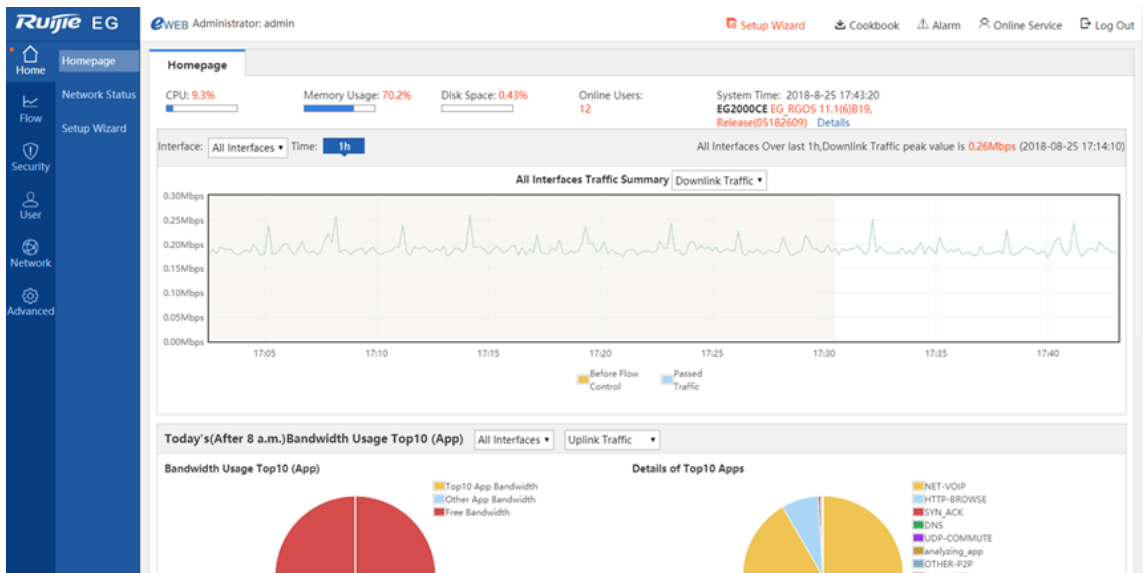
If a tunnel is created successfully but the eWeb page does not automatically open, the system will pop up a message. The user can manually click the link to open the page.
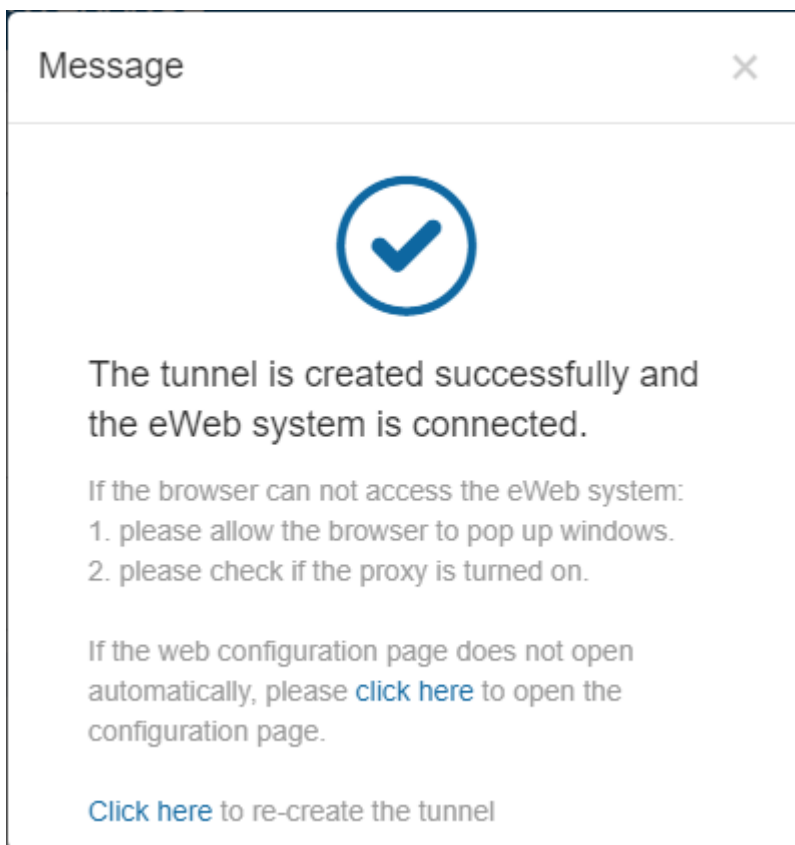
● Move to
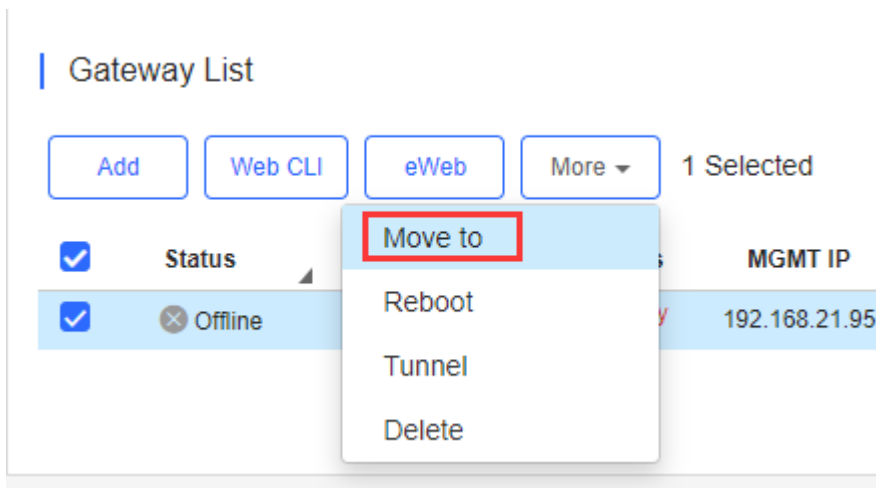
Select the device in the **Gateway List**, click **More** > **Move to**, select the new network and click **OK**. Only one gateway can be moved at a time.
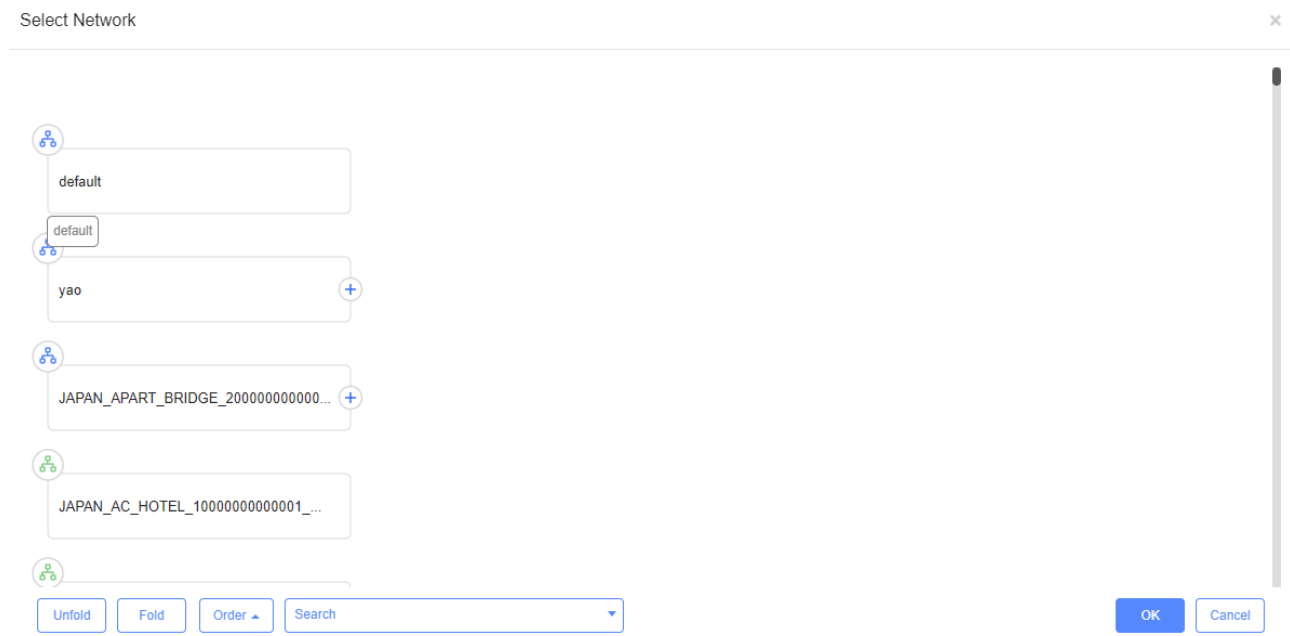
- Reboot
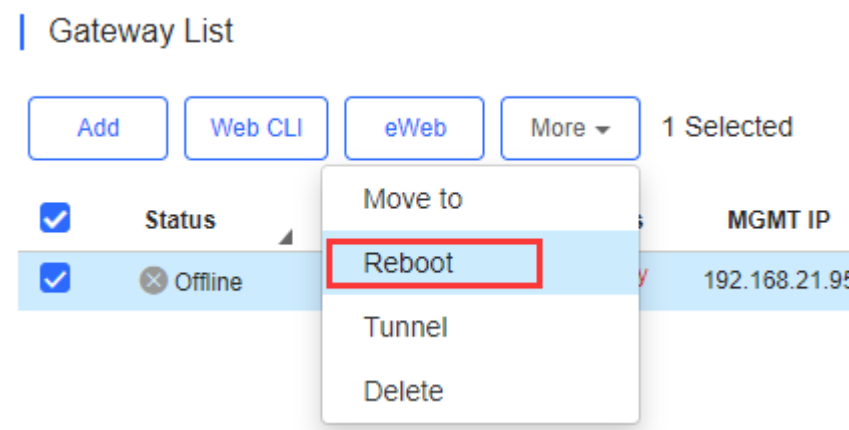
Select the device in the **Gateway List**, click **More** > **Reboot** and click **OK**.

- Tunnel
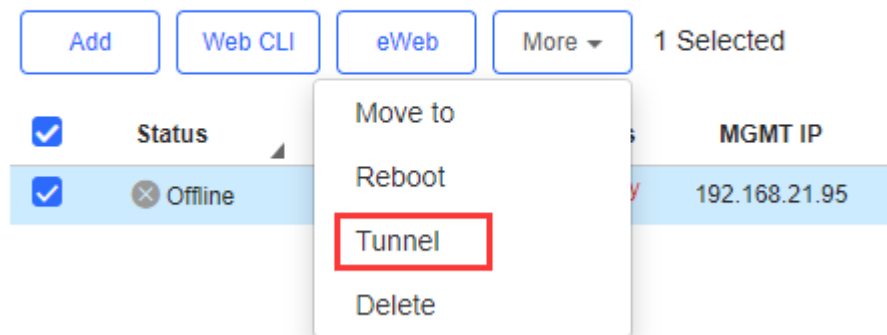
The user can create a Web-based tunnel to enter the eWeb system of a gateway for more monitoring and management functions.

Note: If any security system exists in the network, such as a firewall, the traffic of destination TCP port 10000-12000 should be permitted.

Select the device for tunnel management, and click **More** > **Tunnel Config**. On the **Tunnel Management** page, **WEB**, **Telnet** and **SSH** types can be selected or you can customize the tunnel configuration. The **Tunnel List** displays the tunnels already created.
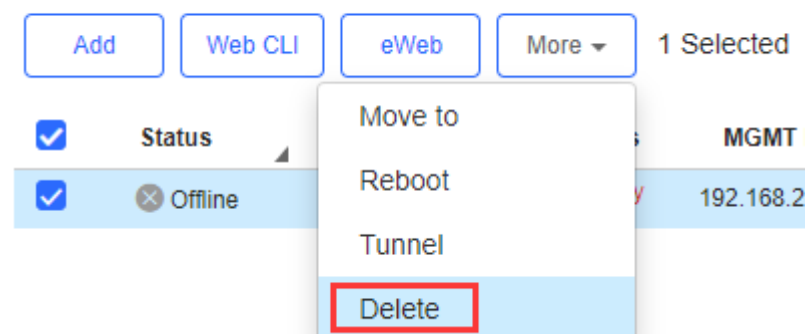
● Delete

Select the device in the **Gateway List**, click **More** > **Delete** and click **OK**.

5.5.8   WiFi Router (beta)

5.5.8.1   WiFi Router List

The **WiFi Router List** displays basic device information, including the online/offline status, SN, MAC, alias, management IP & public IP, offline time, network, model, firmware version and description.

The **WiFi Router List** automatically refreshes every minute. Click **Auto Refresh:** ⬤ to enable/disable the auto refresh function.

Above the list is the **Add** function. Click **More ▾** to display the **Move to**, **Delete**, **Export**, and **Reboot** functions. For more information, refer to **Basic Router Operations**.

The **Search** function supports fuzzy queries based on the serial number, alias and description, and also supports queries based on online/offline status.

Click the record in the **Config Status** column to open the **Config Status** page. On this page, you can deliver one or all configurations.

The number of devices which have available firmware for upgrade is displayed on the upper-left corner of the **AP List** page. Click **New Firmware** to display the **New Firmware List**. Then click **Go To Upgrade** to enter the **MAINTENANCE** > **UPGRADE** > **Upgrade** page.

For more information, refer to **Device Details**.

5.5.8.2 Device Details

Click the serial number in the device list to open the details page for a single device. The page displays detailed device information, including basic information, performance data, speed data, client data, online/offline status, and device logs.

Router information is described as:

● Router Info

The basic information includes serial number, MAC address, management IP address, device model, configuration status, firmware version, hardware version, alias, and description.

● Status

| Status

The performance data includes the router connection status, online client count, CPU usage, and memory usage.
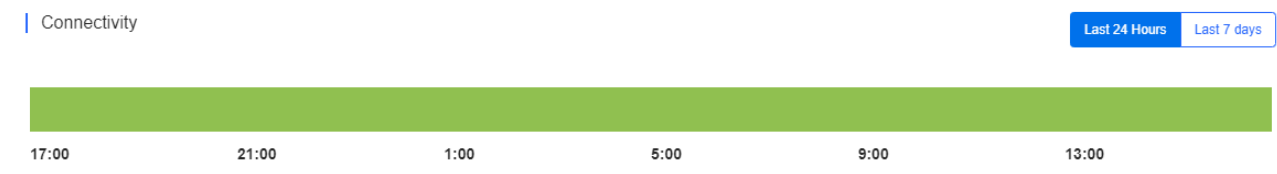
- Connectivity

Router connectivity refers to the connectivity (online status) between router and Cloud Service within a period (1 day or 7 days).

- Speed Summary
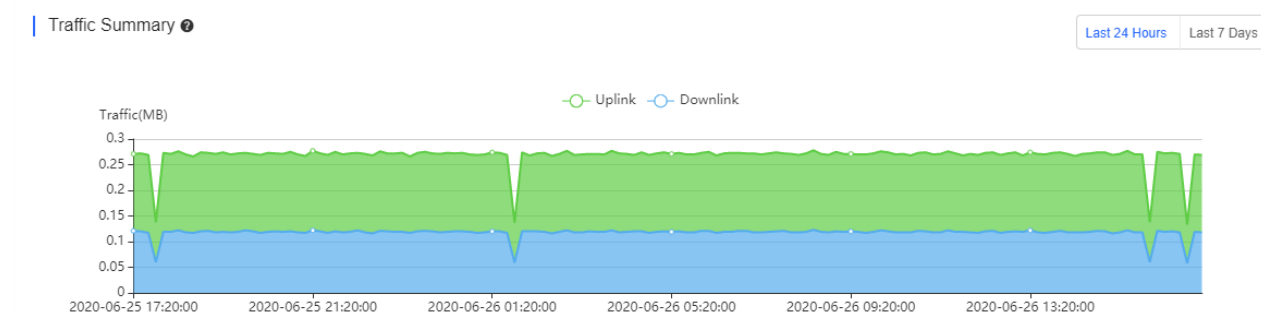
You can choose to view the router speed statistics in the last 24 hours or the last 1 week.

- Device Log

The Device Log records the device type, update time and content.

- Config Log

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

5.5.8.3 Basic Router Operations

● Add Router

Select the network, and click **Add**. Both batch import and manual add are supported.

Click **download template** to download the template, enter router information, and click **'.xls' File** to import the template.

Click **Add a Device**, enter SN and alias of the AP, and click **OK**. Click + to add multiple APs.

● Move to

Select one or multiple devices in the **WiFi Router List**, click **More** > **Move to**, select the new network and click **OK**.

● Delete

Select one or multiple devices in the **WiFi Router List**, click **More** > **Delete** and click **OK**.

● Reboot

Select one or multiple devices in the **WiFi Router List**, and click **Reboot.**

5.5.8.4 Web CLI

Select one or multiple devices in the **WiFi Router List**, and click **Web CLI**. The **Web CLI** dialog box is displayed, and device information can be queried via the menus in this dialog box. The menus vary with the products.

In the command entry box, the **TAB** key and question mark (?) both can complete a command.

5.6 Client

Select **MONITORING > CLIENT** to open the **Client** page.

5.6.1   Client List

1.   This page displays the information about online clients and historical clients of the current network.

2.   Click the drop-down list next to **Advanced Search** to switch between **Online Clients** and **History Clients**.

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

3.   Search for user data by online status, MAC, AP, SN or SSID.

4.   Click the device **MAC**, and the **Client Details** page is displayed.

5.6.2   Client Details

●   Client Info

Client Info includes alias, online status, MAC etc.

●   Performance

Performance ❂

Traffic(MB)

Delay(ms)
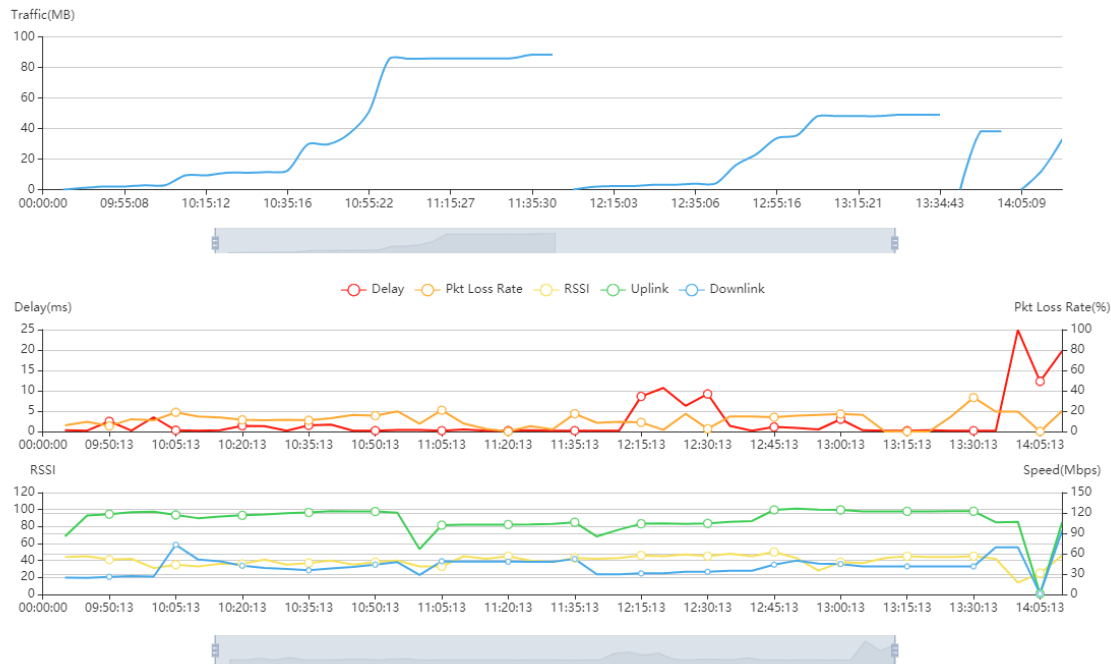
RSSI

Performance displays the traffic summary etc.

● Online/Offline Record

Online/Offline Record

AP SN	AP Alias	IP	SSID	RSSI	Band	Traffic(MB)	Online Time	Offline Time	Updated at
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-53	2.4G	32.762	2019-04-16 14:05:09	-	2019-04-16 14:13:46
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	38.179	2019-04-16 13:46:16	2019-04-16 13:57:23	2019-04-16 13:57:43
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	49.051	2019-04-16 12:04:10	2019-04-16 13:34:43	2019-04-16 13:35:23
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	88.296	2019-04-16 09:36:35	2019-04-16 11:36:13	2019-04-16 11:36:31
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	4.442	2019-04-15 15:24:59	2019-04-15 15:58:43	2019-04-15 15:59:26
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	1.520	2019-04-15 12:39:38	2019-04-15 12:47:05	2019-04-15 12:47:59
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	66.523	2019-04-15 10:15:38	2019-04-15 11:56:59	2019-04-15 11:57:46
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	12.954	2019-04-12 17:46:01	2019-04-12 18:28:59	2019-04-12 18:29:52
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	326.045	2019-04-12 14:01:03	2019-04-12 17:26:35	2019-04-12 17:26:40
G1KD9HH02861B	520w2	172.17.125.140	Nature_cloud_as	-	2.4G	2.815	2019-04-12 13:40:13	2019-04-12 13:51:20	2019-04-12 13:51:52

First   Previous   Page 1 of 2   Next   Last   10 ▴   12 in total

Online/Offline Record displays AP SN, AP alias, IP, SSID etc.

● Roaming Record

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	Roam
G1KD84Y017646	5869.6c7a.5dd0	San_Jose	Outdoor RG-AP630(CD)	G1KD83S04970C	5869.6c79.44f7	San_Jose	Indoor AP520-I	G1KD
G1KD83S04970C	5869.6c79.44f7	San_Jose	Indoor AP520-I	G1KD14G00221B	5869.6c5b.5071	San_Jose	Indoor AP520(BT)	G1KD
G1KD14G00221B	5869.6c5b.5071	San_Jose	Indoor AP520(BT)	G1KD83S04970C	5869.6c79.44f7	San_Jose	Indoor AP520-I	G1KD
G1KD90N003414	5869.6caa.72e2	San_Jose	AP630(IODA)	G1KDA0T003926	5869.6cb9.7926	San_Jose	Indoor AP740-I	G1KD
G1KD90N003414	5869.6caa.72e2	San_Jose	AP630(IODA)	G1KDA0T003926	5869.6cb9.7926	San_Jose	Indoor AP740-I	G1KD
G1KDA0T003926	5869.6cb9.7926	San_Jose	Indoor AP740-I	G1KD84Y017646	5869.6c7a.5dd0	San_Jose	Outdoor RG-AP630(CD)	G1KD
G1KD83S04970C	5869.6c79.44f7	San_Jose	Indoor AP520-I	G1KDAHJ052008	5869.6cc1.96d0	San_Jose	indoor AP130(W2)	G1KD

First   Previous   Page 1 of 1   Next   Last   10 ▴   7 in total

Roaming Record displays roam-in AP, source AP, SSID etc.

6   Configuration

The Configuration module includes two parts: **NETWORKS** and **WIRELESS**.

6.1 Networks

6.1.1   Networks

Select **CONFIGURATION** > **NETWORKS** to open the **NETWORKS** page.
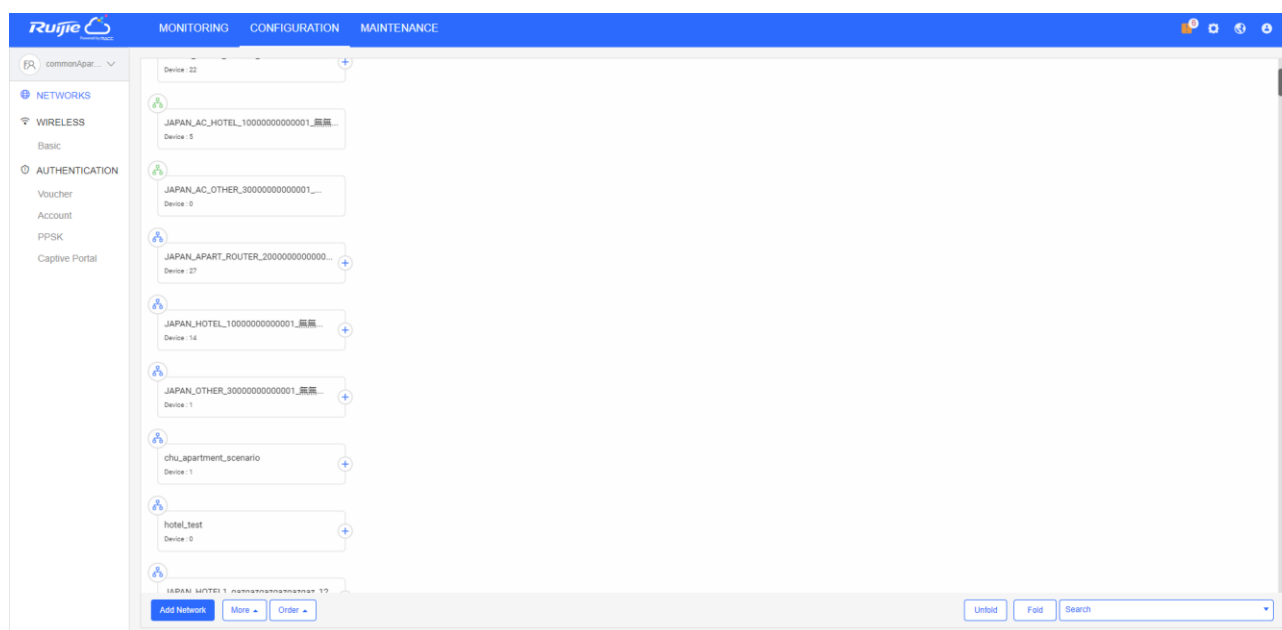
Click a network, and four operation icons are displayed around the network for adding a sub network, sharing the network, handing over the network, and deleting a network. You can click these icons or the buttons in the lower right corner to perform operations on the network.
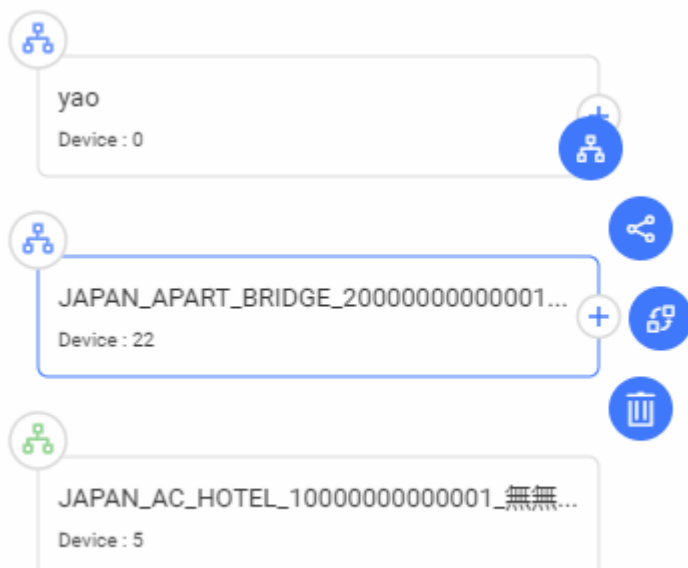
6.1.1.1   Add Sub Networks for AP Networks

Select the network and click **Add Sub Network**.
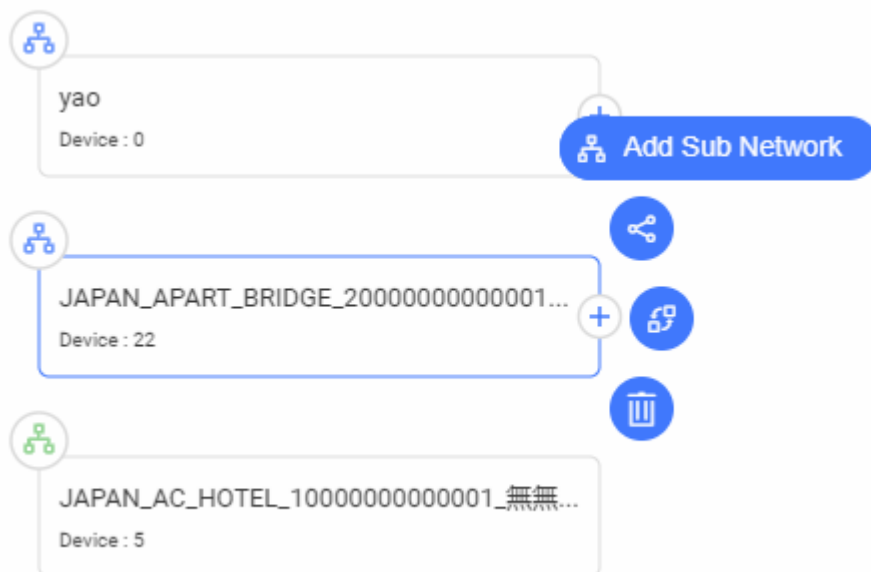
6.1.1.2   Share with

A network can be shared to other users for check and management. You can set the validity so that the network sharing will be canceled after the specified time.

Select a network and click **Share with**.
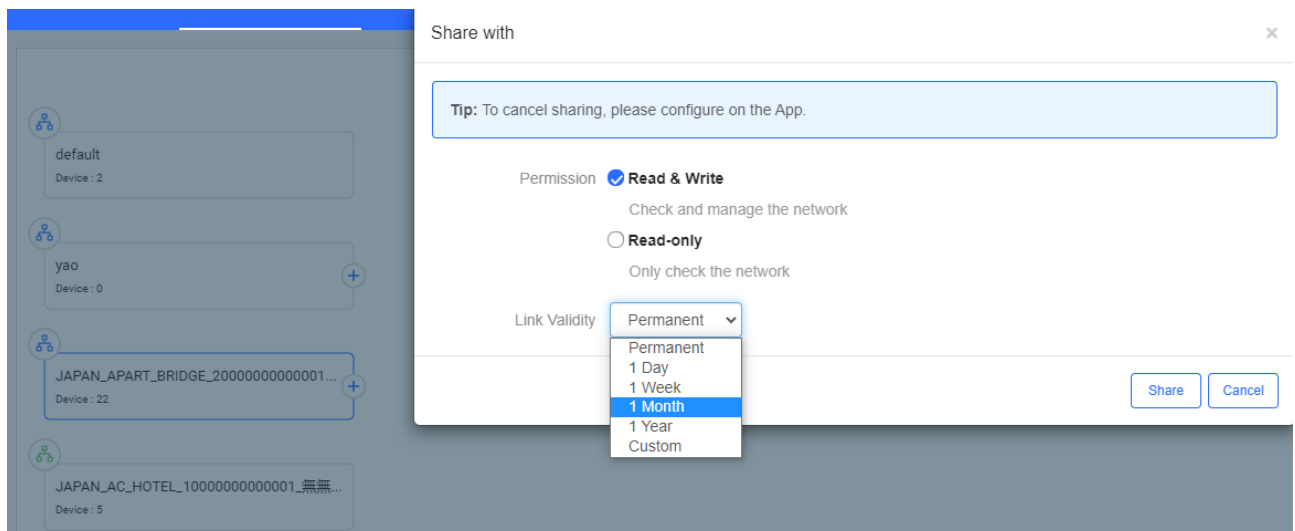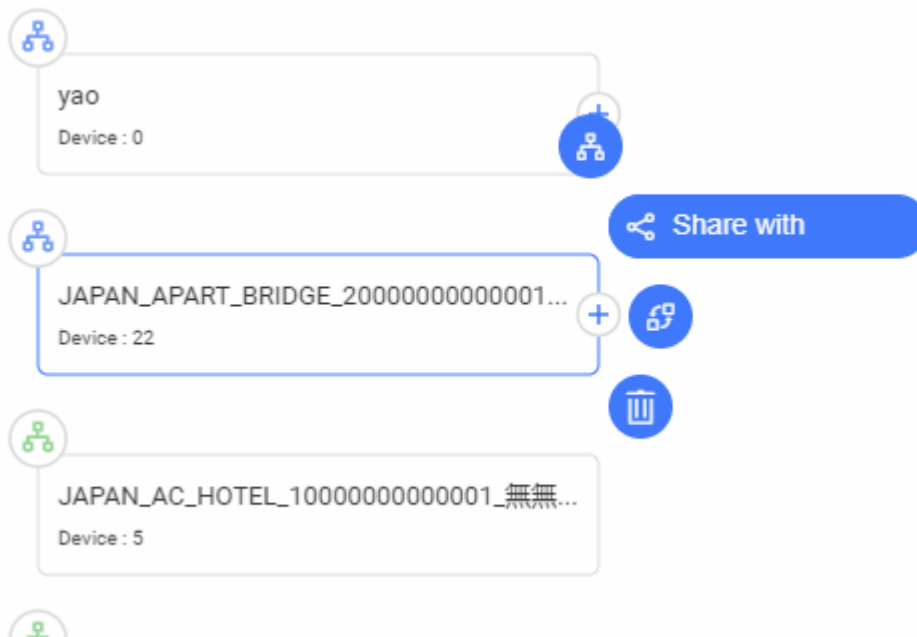
Copy the link and send to the receiver. The receiver can visit the URL and log in to receive the network.
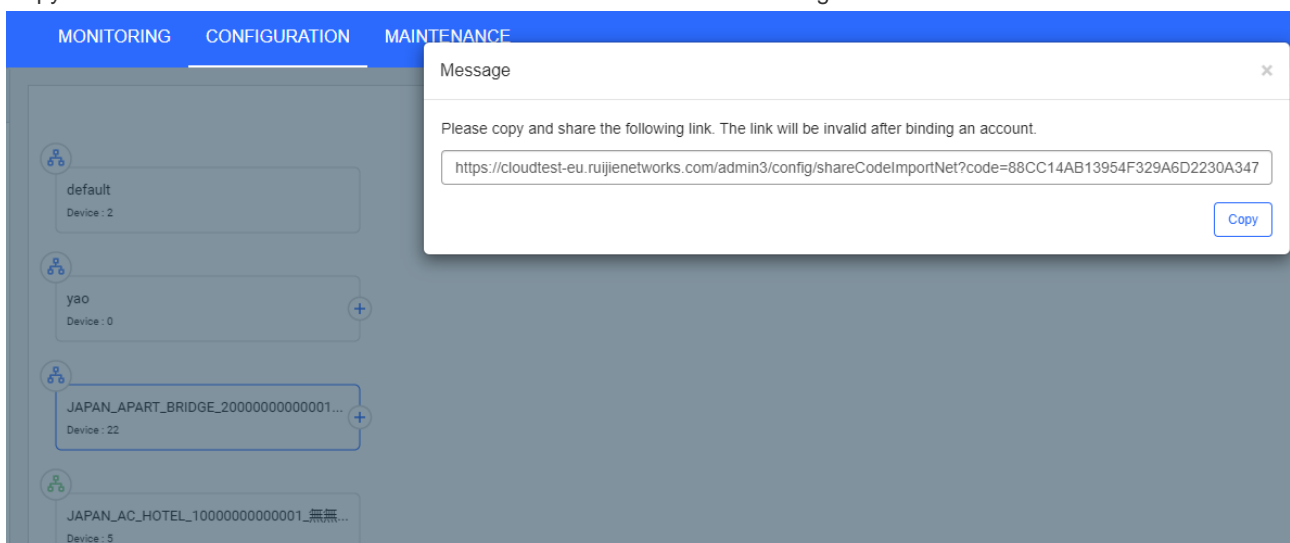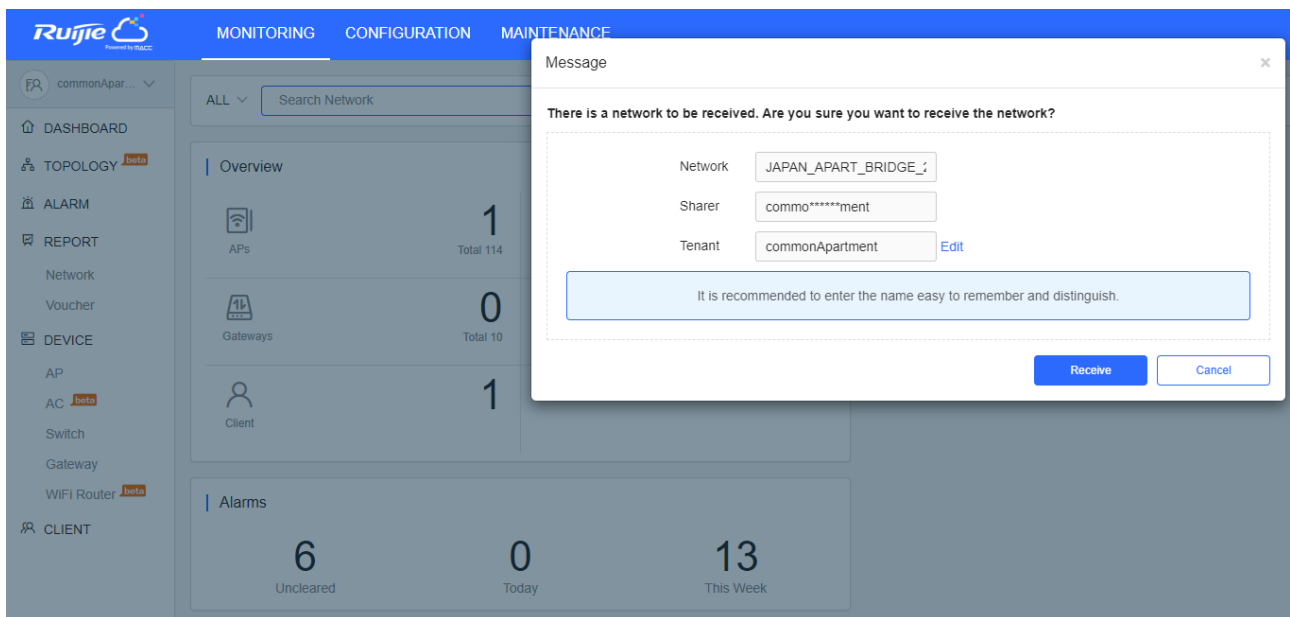
Click the ⌄ on the upper left corner to switch tenant and check the shared network.
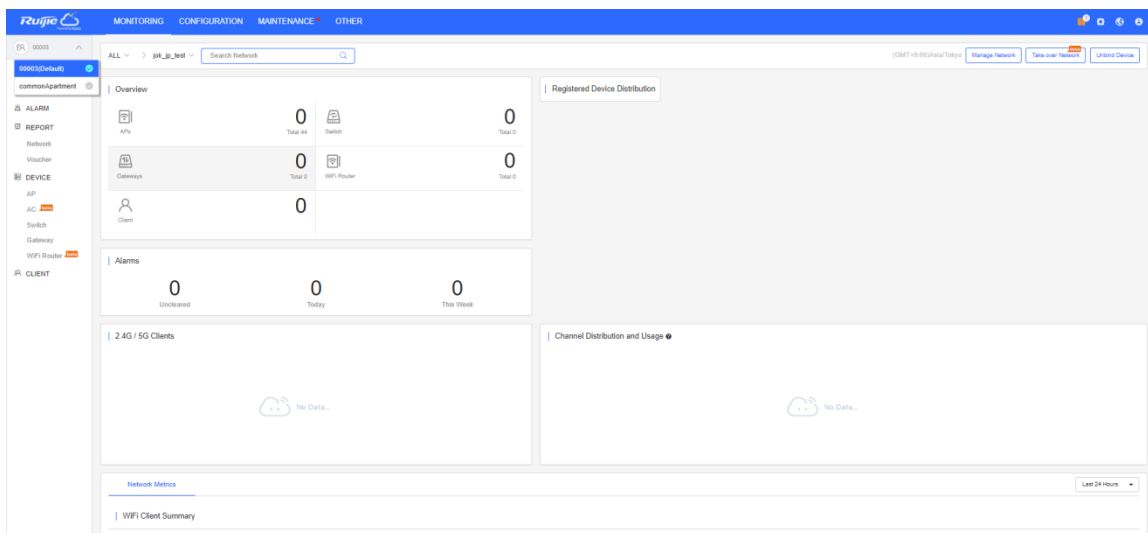
6.1.1.3 Hand over

The network can be handed over to another tenant.

Select a network and click **Hand over**.

Enter the Email address of tenant, and click **OK**. After the receiver takes over the network, you can not manage the network anymore.
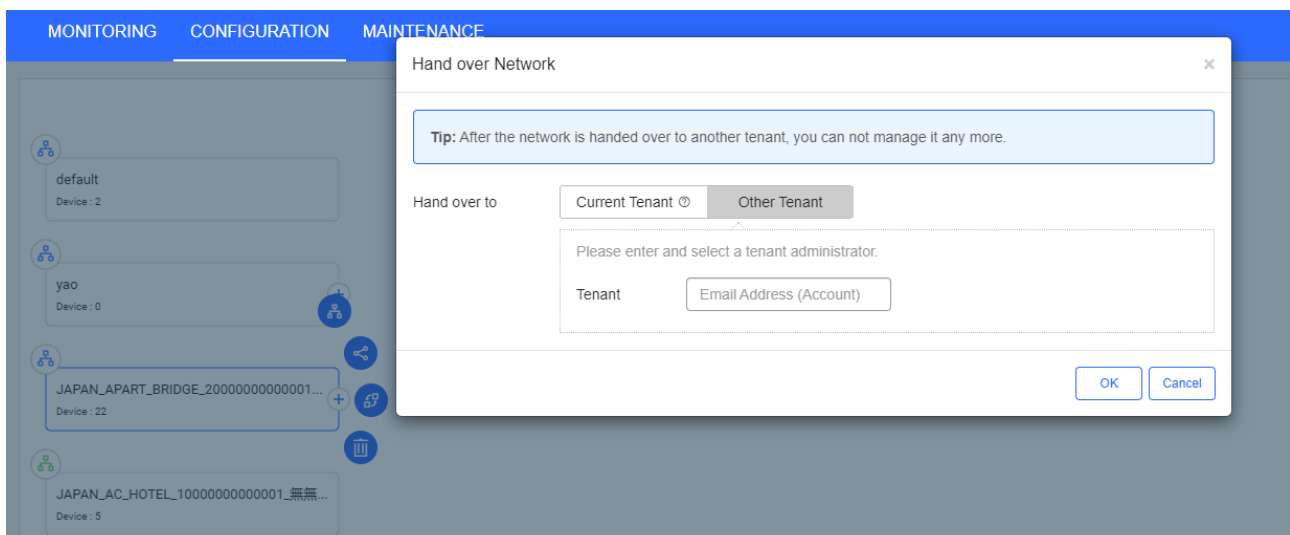
As the receiver logs in to Ruijie Cloud, an icon is displayed on the upper right corner.
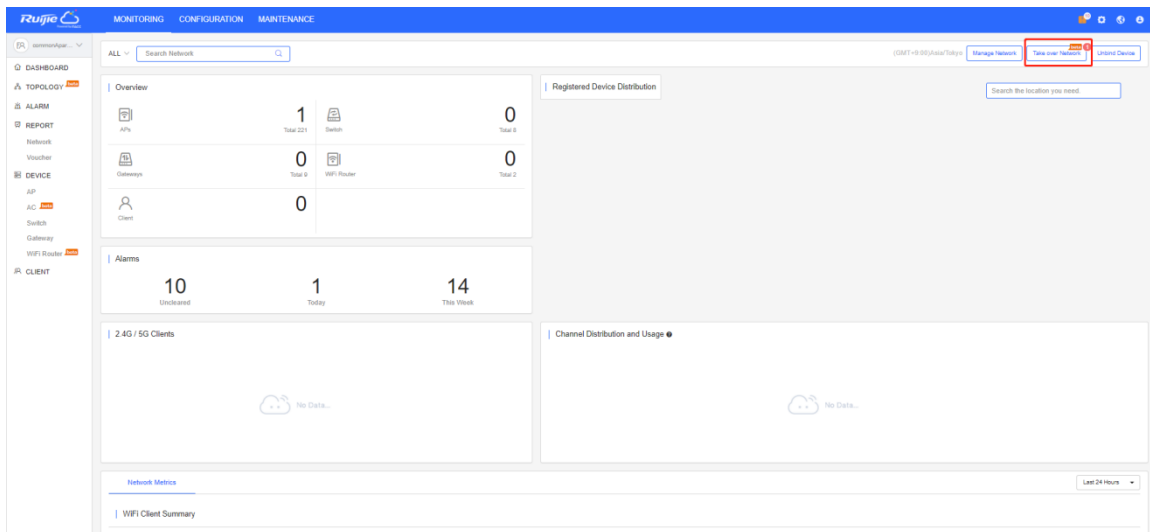
Click **Take over Network** to take over or refuse the network.
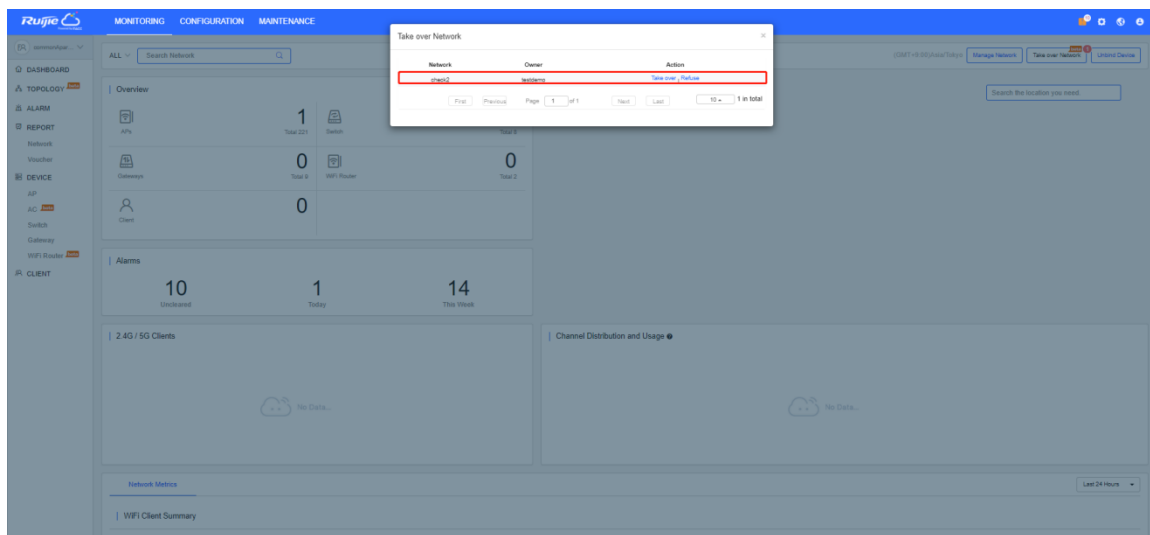
6.1.1.4 Config

Select the network and click **Config**.
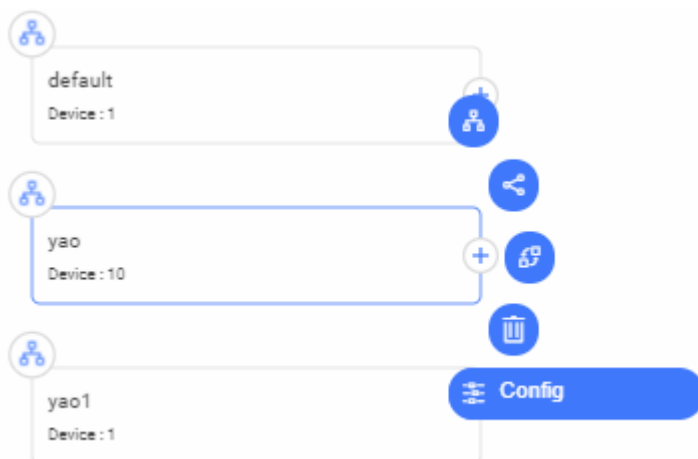
6.1.1.5 Delete

Select the network and click **Delete**. When the delete confirmation window is displayed, click **OK**.
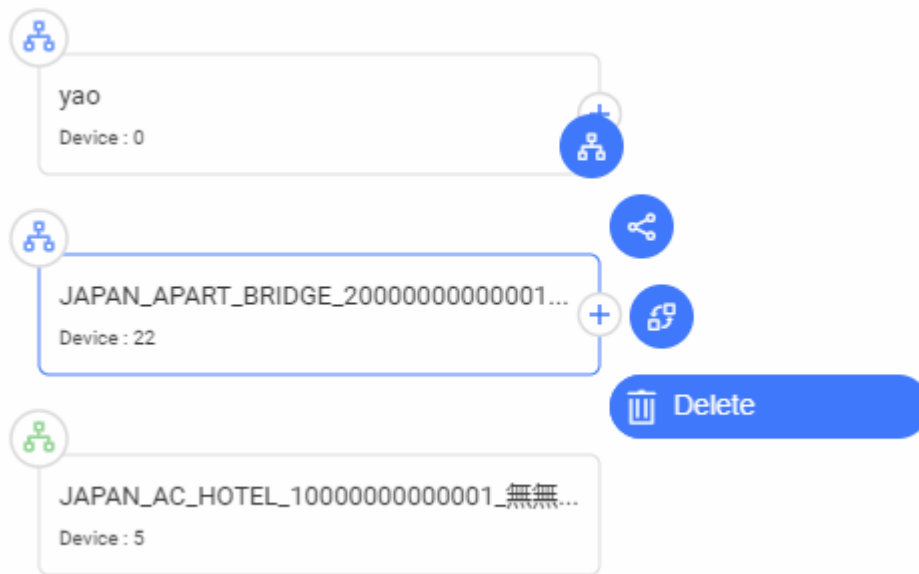
6.1.1.6 Order Networks

Networks can be unordered or sorted by name in the ascending/descending order.
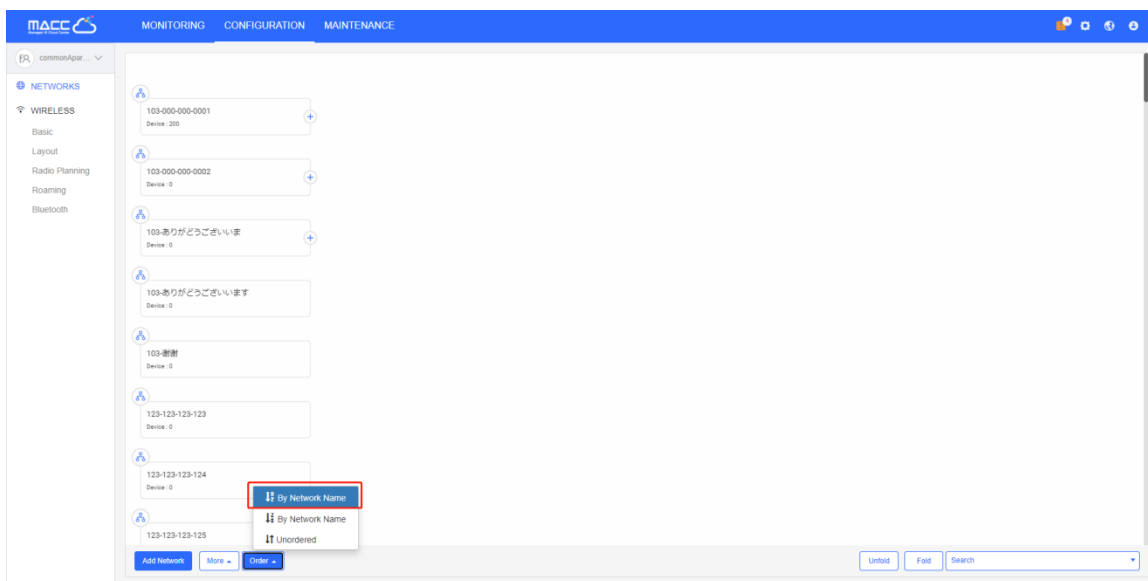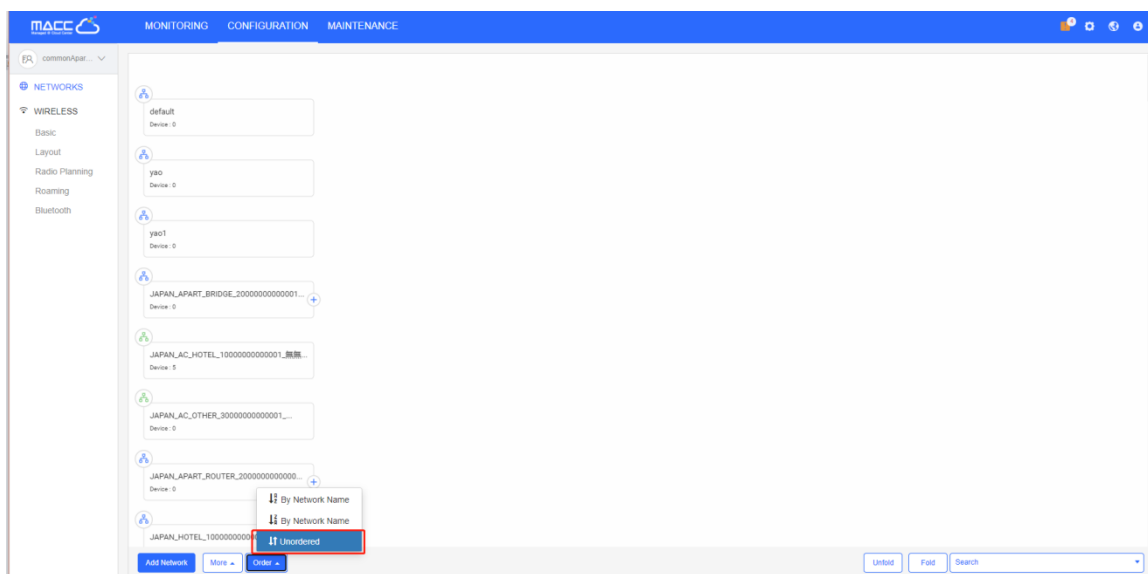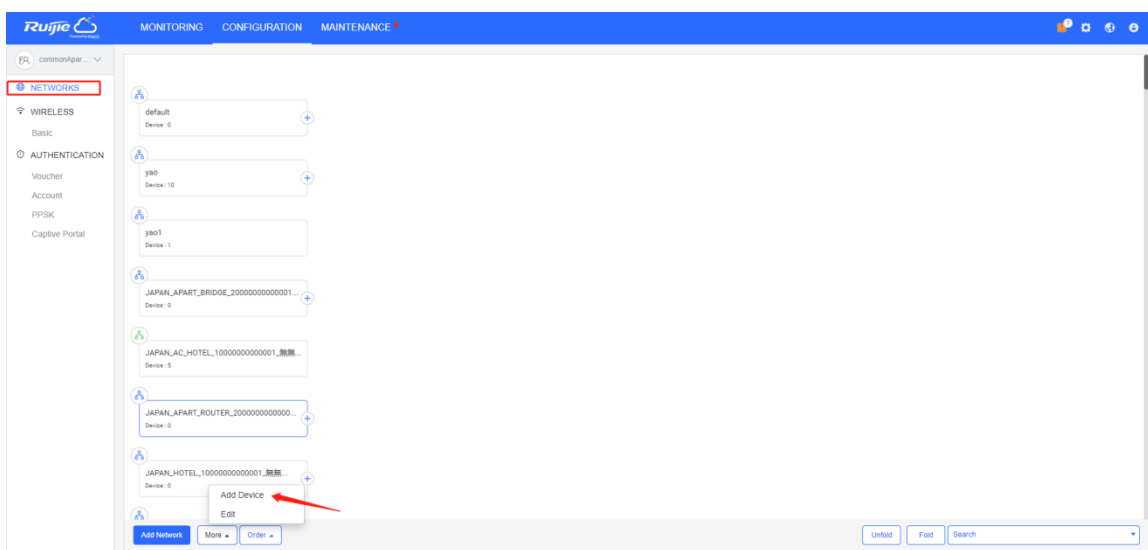
6.1.1.7   Add Device

Non-apartment Mode

Choose **NETWORKS**, select a network in non-apartment mode, and click **More** > **Add Device** to add APs, switches, gateways, and WiFi routers.

Apartment Mode

Choose **NETWORKS**, select a network in apartment mode, and click **More** > **Add Device** to add APs.

6.1.2   Add Network

Select **CONFIGURATION**>**NETWORKS**, and click **Add Network**.
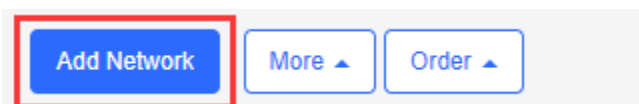
Non-apartment Scenario

Enter the network name.

Specify the network location.
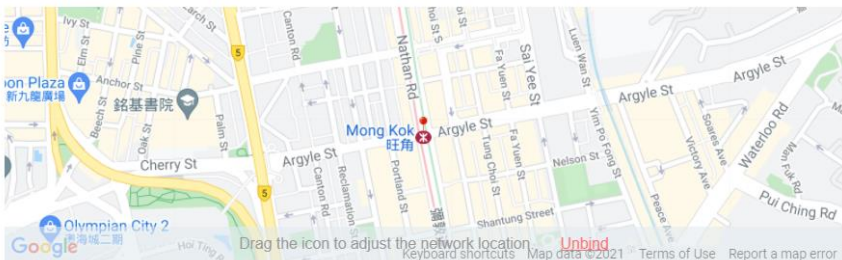
Enter the WiFi information as required.

Enter the information of APs, switches and gateways, and click **Save & Next**. Or click **Batch Import** to download the template, enter the device information in the table, and then batch import devices into the system.

Apartment Scenario

Enter the network name, select the scenario and bind the location.

6.1.3 Edit Network

Select the network and click **Edit**.

Non-apartment Scenario

You can edit network name and time zone, and bind location here.

Apartment Scenario

You can edit network name and time zone, and bind location here.

6.2 Wireless

6.2.1 Basic (Apartment Scenario)

Select **CONFIGURATION > WIRELESS > Basic** to configure SSID and password of AP.
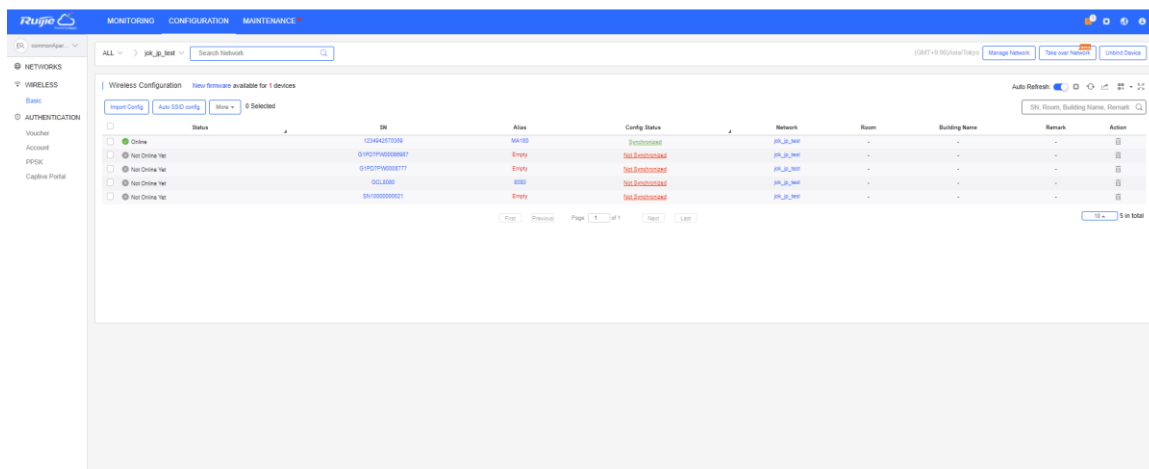
In the apartment scenario, SSID and password can be configured in 2 ways.

Click **Import Config** to manually import SSIDs and passwords in an EXCEL file.

Or you can select **Auto SSID Config**. In this way, you don't need to manually configure the SSID and password.

6.2.1.1 Customize Template Rules

To batch import devices or change SSIDs/passwords, you can customize the importing template.

Download and fill in the template.Up to 500 records can be imported

"xls" File   Download Template

Click to select devices parsing rule (**Deafult Template**)

Click **Click to select devices parsing rule**, the rule customizing page appears.

There will be one default rule.

1. **Add** button: Add a new rule

2. Menu bar: Display rule content

    ●   **Name**: User defined name

    ●   **snPosition**: Specify the starting position of SN in template

    ●   **ssidPosition**: Specify the starting position of SSID in template

    ●   **ssidPasswordPosition**: Specify the starting position of SSID's password in template

    ●   **roomPosition**: Specify the starting position of room number in template

    ●   **buildingNamePosition**: Specify the starting position of building name in template

    ●   **RemarkPosition**: Specify the starting position of remark in template

If an entry is left empty, it will not be imported when importing the template. For example, ssidPosition will not be imported if it is empty.

※User can customize the EXCEL parsing rule from columns A to Z and rows 1 to 15.

3. Check box: Only one rule can be selected at a time

4. Rule control button:

    ●   : Edit the rule

    ●   : Delete the rule

- : Set the rule as default rule

5. Page up and down button

6.2.1.2 Auto SSID Config

Click **Auto SSID Config** to configure the SSID and password automatically.

To configure the password only, select **Only regenerate passwords**.

To configure both the SSID and password, select **Regenerate SSIDs and passwords**. At most 4 SSIDs can be configured.

You can use either custom template or the default template.

● Use Customized Template to Configure SSID/Password

The customized template need to include SN, Building Name, Room Number, SSID, SSID Password, and Remark.

The following is an example to change the SSID and password only:

The custom rule may be set as below:

- ● Name: ModifySSID
- ● snPosition:
- ● ssidPosition:

- ● ssidPasswordPosition:

- ● roomPosition: B2

- ● buildingNamePosition: A2

- ● RemarkPosition:

※If Remark is filled in EXCEL file, the former remark saved in the Cloud will be overwritten.

- ● Use Cloud's Default Template to Configure SSID/Password
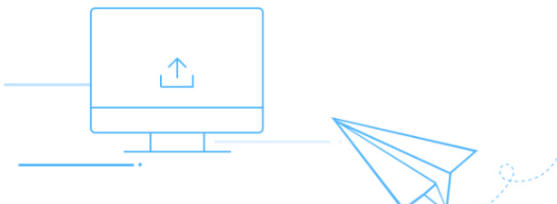
Download the template and fill the information as below:

SN	Remark	Room	Building Name
SN100001	10111	203	building1
SN10002	10112	204	building2

Import the template.

After the template is successfully imported, a prompt will be displayed. Click the prompt to open the Config Log page, and export the SSID configuration result.

To view the configuration result of the specified device, you can also point to the device SN to check the SSID/password.

.

6.2.1.3 Import Config

● Use Default Template to Import SSID and Password

Click **Download Template**.

Enter SSID and password. Each AP supports at most 4 SSIDs, and SSIDs and passwords need to be separated by ','.

	A	B	C	D	E	F	G	H	I	J
	Model	SN	MAC	PN	SSID	SSID Password	Alias	Room	Building Name	Remark
		G1PD7PW00080B			10001,10002	66666666,88888888				

Click **"xls" File** to import the template.

After the template is successfully imported, a prompt will be displayed. Click the prompt to open the Config Log page, and export the SSID configuration result.
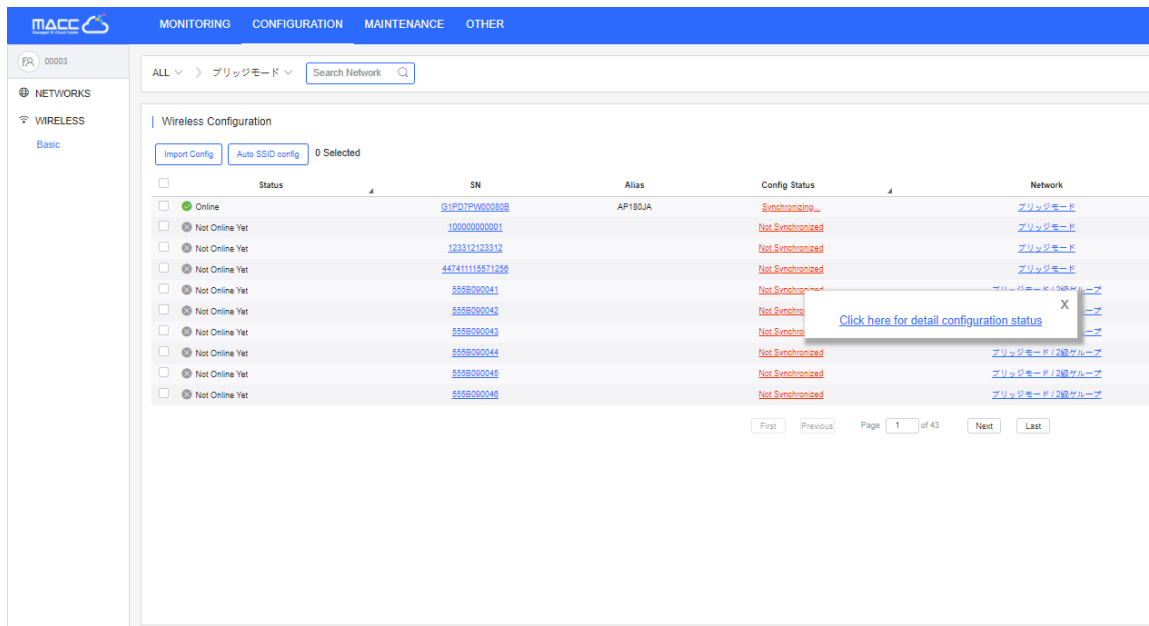
To view the configuration result of the specified device, you can also point to the device SN to check the SSID/password.
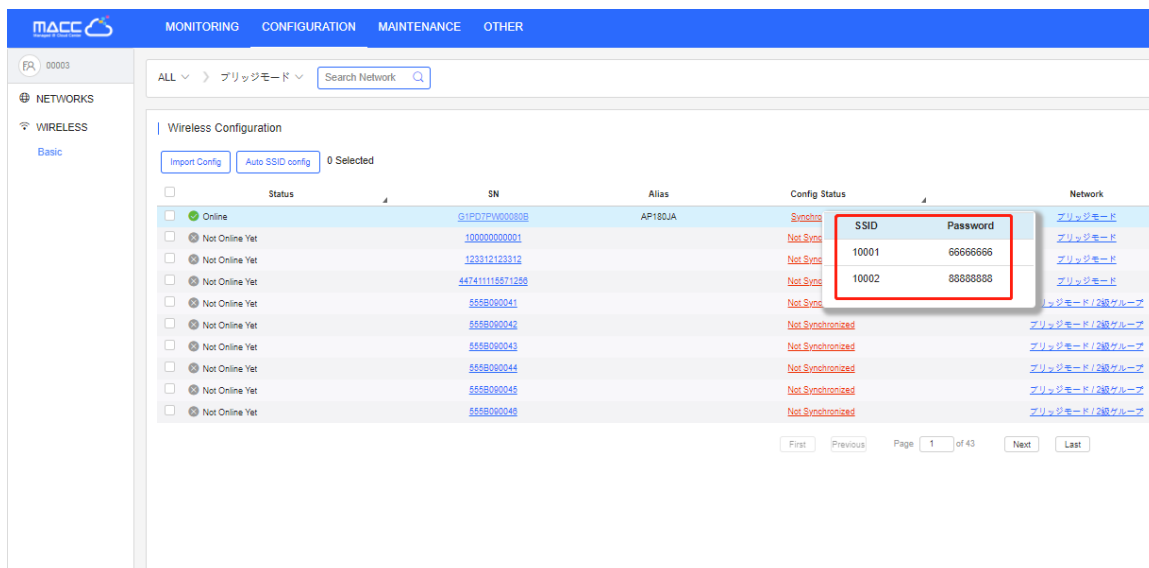
● Use Customized Template to Import SSID and Password

The operation is almost the same with that in **Auto SSID Config**. The only difference is that you need to fill in the SSID and password to be changed in the template.

The custom rule may be set as below:

- ● Name: ModifySSID

- ● snPosition:

- ● ssidPosition: G3

- ● ssidPasswordPosition: H3

- ● roomPosition: C3

- ● buildingNamePosition: B3

- ● remarkPosition: D3

※If Remark is filled in EXCEL file, the former remark saved in the Cloud will be overwritten.

6.2.1.4 Sync SSID
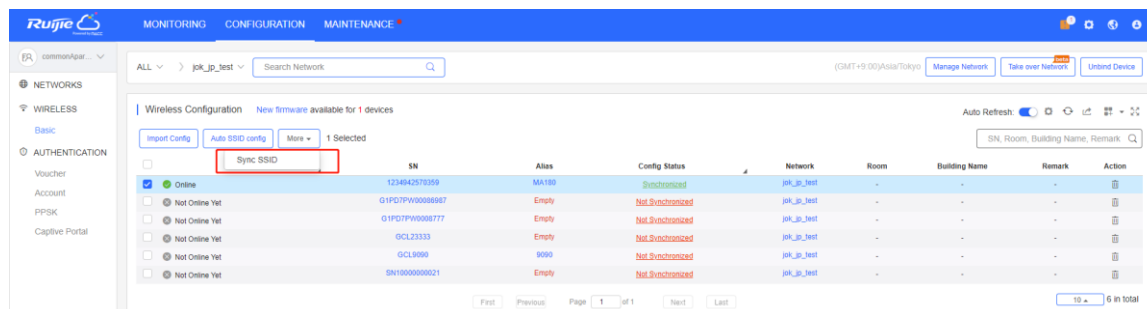
Select devices to be synchronized, and click **More** > **Sync SSID** to synchronize the SSIDs and passwords of the devices. A maximum of 100 devices can be selected. After the synchronization, synchronized SSIDs and passwords are displayed.

6.2.1.5 Auto Sync Config File From Device
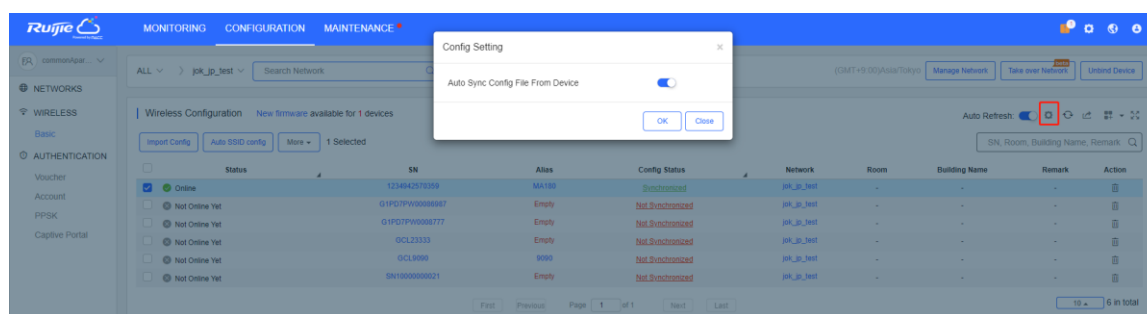
Enable the **Auto Sync Config File From Device** function. Configuration files will be automatically synchronized from the devices in the network at an interval of 20 to 28 hours.

6.2.2 Basic (Non-apartment Scenario)

If a network is not configured, it will inherit configuration from its parent network by default. You can create or import a configuration file from other networks. Note that if there is any captive portal template unavailable for the network, the configuration file can not be imported.

Click **Save** to configure the network.

On the **Basic** page, **Wireless**, **Security**, and **Advanced Settings** can be configured.

6.2.2.1 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.

WLAN ID: 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 can not be changed subsequently. The maximum value of **WLAN ID** is 32.

SSID: Enter an SSID name.

Encryption Mode: Open, **WPA-PSK**, **WPA2-PSK, WPA/WPA2-PSK**, **WPA2-ENTERPRISE (802.1X)** and **PPSK**. **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. **PPSK** indicates that each terminal device is bound with a unique WiFi account and key. After the PPSK mode is selected, you need to configure your account in **CONFIGURATION>AUTHENTICATION>PPSK**.

If you select the **WPA2-Enterprise(802.1x)** mode, the following page is displayed.

| SSID   ✕

WLAN ID	2		Hidden	No
SSID			Forward Mode ❷	Bridge
Encryption Mode	WPA2-Enterprise(802.1X)		VLAN ID	1

Radio ☑ Radio1(2.4GHz) ☑ Radio2(5GHz)
☐ Radio3 ❷ (2.4GHz or 5GHz)

Primary Server	--Select a server--	⊕ ☑
Jitter Prevention	⬤
Advanced Settings	Advanced Settings
5G-Prior Access ❷	⬤
Speed Limit per Client	⬤
Speed Limit by SSID	⬤

OK   Cancel

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

| Radius Server   ✕

Server Name :
Server IP :
Authentication Port :
Accounting Port :
Key :

Save   Cancel

Server IP, **Authentication Port**, **Accounting Port**, and **Key** can be configured for a RADIUS server. **Authentication Port** and **Accounting Port** are optional, and respectively set to the default values **1812** and **1813** 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)**. In case of jitters: after the jitter prevention function is enabled (the jitter prevention duration range is 0–600), clients will not go offline within the duration of jitter prevention. 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 AP's upstream device. A VLAN ID must be configured when the **Bridge** mode selected.

NAT Address Pool Configuration: Click the **NAT Address Pool Configuration** link to display the window.

NAT Address Pool Configuration   ✕

Note: 1. Only after the SSID has been configured with NAT forwarding mode, the NAT address pool configuration will be delivered to the AP.
        2. If the address pool has changed, the original client must re-associate the SSID to get the new address of the address pool.

🔵 Common Address Pool Configuration (Recommended)
    Use the current address pool or the default address pool (192.168.23.0/24), Click here to configure the address pool. ⌄

◯ NAT Roaming Address Pool Configuration (Cloud will allocate different address pools for different APs. The AP must support L3 roaming. Please select this option when all APs in the network are dual-radio APs.)
    By default, it is auto allocated by server. (Range: 10.233.0.0/24-10.254.254.0/24), Click here to customize the address pool. ⌄

                                                                                    Save   Cancel

5G-Prior Access: It is enabled when the SSID is associated with Radio 1 and Radio 2 for dual-band APs (2.4 GHz and 5 GHz) to ensure that clients supporting dual bands access the 5 GHz frequency band preferentially. This reduces the load in the 2.4 GHz frequency band and improves user experience.

Speed 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: Common APs support **External Portal** and **Captive Portal** authentication.

6.2.2.2 External Portal

To edit **SSID**, enable **Auth** and select **External Portal**. Enter the required information and click **OK**.

Auth 🔵

Mode   External Portal   ⌄

Portal Server URL ❷ [   ]

Portal IP ❷   [   ]

Portal Port(Optional) [   ]

Gateway ID(Optional) [   ]

Seamless Online   ☐ Enable(Available only when supported by Auth server)

Idle Client Timeout ☑ ⌄ Inactive Client Auto Offline (Optional)

6.2.2.3 Captive Portal

1.   On the **SSID** page, enable **Auth** and select **Captive Portal**.

| SSID   ×

WLAN ID	3	Hidden	No
SSID	FXC	Forward Mode ❓	NAT
			"NAT Address Pool Configuration"
Encryption Mode	Open	Radio	☑ Radio1(2.4GHz) ☑ Radio2(5GHz)
			☐ Radio3 ❓ (2.4GHz or 5GHz)
5G-Prior Access ❓	⚪		
Speed Limit per Client	🔵		
Uplink		KB/s	Downlink		KB/s
Speed Limit by SSID	⚪		
Auth	🔵		
Mode	Captive Portal		

OK   Cancel

2.   Enable **Seamless Online** and select the portal.

Mode	Captive Portal
Seamless Online ❓ 🔵	1 Day

Please select a portal or add a new portal.

jok-portal2   jok-portal

‹   ›

6.2.2.4 Radio

Radio

Radio1(2.4GHz)		Radio2(5GHz)		Radio3 ❓ (2.4GHz or 5GHz)		☑ Scan ☐ Access
ON/OFF	🔵	ON/OFF	🔵	ON/OFF	⚪	
Max Clients	32	Max Clients	32	Max Clients	32	

The Radio page enables you to configure the AP radio ports. As shown in Figure 4-4, the **Radio** page provides the **On/Off** and **Max Clients** items. 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**.

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

ℹ️   Deletion of radio configurations indicates that the system preserves the current configurations.

6.2.2.5 Security Configuration

As shown in the preceding figure, **eWeb Settings**, **Telnet Settings**, **Client Isolation**, and **Wireless Intrusion Detection** can be configured.

eWeb Settings: Enter the Web login password of an AP. When the password is empty, the system does not push the password to AP.

Telnet Settings: Enable the Telnet service of AP. When the Telnet service is enabled, the password is required.

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.

Wireless Intrusion Attack Detection: Include DDOS attack detection, flooding attack detection, AP 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.

6.2.2.6 Advanced Settings

● AP RF Scheduling

If **AP RF Scheduling** is disabled, AP will broadcast the SSID.

AP RF Scheduling

RF Shutdown Scheduling ⬜

To specify the time of turning on/off WiFi, enable **RF Shutdown Scheduling** and configure the period.

AP RF Scheduling

RF Shutdown Scheduling 🔵

Period				
Start Time	This day ⌄	23 ⌄	:	00 ⌄
End Time	Next day ⌄	8 ⌄	:	00 ⌄

● Whitelist

Enter whitelisted websites, and websites that can be accessed directly without authentication. For Facebook social login, you need check on Facebook Whitelist so that clients can access Facebook API before authentication.

● CLI Command

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

6.2.3 Layout (Non-apartment Scenario)

On the Layout page, you can bind an AP to a specific location after importing it to a network.

1. Select a network.

The **Unbound Device List** on the right displays APs that have been imported to the network, but are not bound to a location. Click **Config Layout** to display the list.

Config Layout   ×

Name	Action
ssdsd	☑ 🗑
re334	☑ 🗑

Add Layout

Click **Add Layout** to add the local layout or map layout. The local layout can be used to bind the location of indoor APs and the map layout can be used to bind the location of outdoor APs.

2.   Select an AP from in the unbound AP list and drag it to the target location.

6.2.3.1   Unbind APs

AP unbinding is different from AP deletion. AP unbinding removes the binding relation between an AP and a location, but the AP still exists in the network and can be controlled. AP deletion deletes an AP from a network and the AP cannot be controlled after being deleted.

The unbinding methods are:
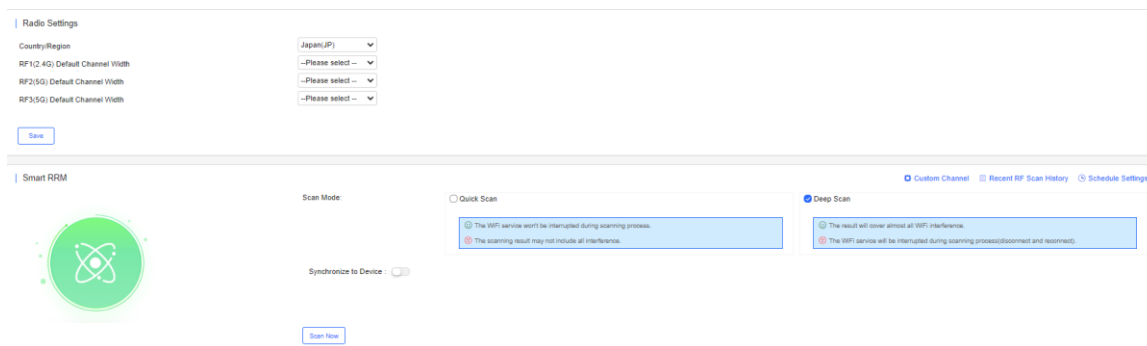
Method 1: Select an AP, and click 🗑 Remove Device to unbind the AP from a location. An unbound AP will then be moved from a network to its parent network.

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

6.2.4   Radio Planning (Non-apartment Scenario)

Radio planning can adjust channels and power of APs in a same area network to optimize the channel allocation and power of the APs. Proper RF configuration planning can reduce channel interference, increase channel utilization and improve overall wireless network performance and capacity.
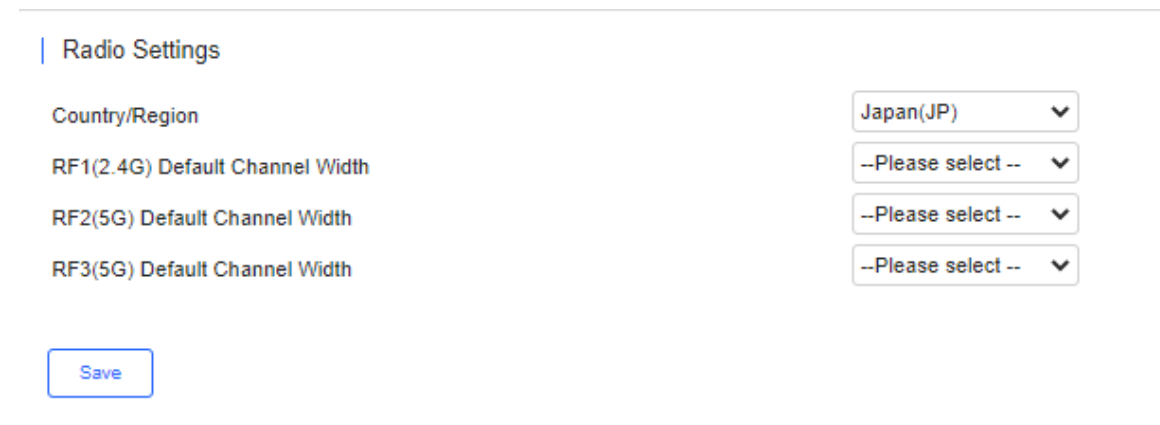
Choose **CONFIGURATION** > **WIRELESS** > **Radio Planning** to open the **Radio planning** page. Both manual and automatic planning are currently supported.

6.2.4.1   Radio Settings

On the **Radio Settings** page, select the country and bandwidth.

For 2.4G channels, the bandwidth can be 20 or 40 MHz. For 5G channels, the bandwidth can be 20, 40, 80, or 160 MHz.

6.2.4.2   Smart RRM

The 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.

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.

The automatic RF planning supports network-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. To reach optimal power, The AP power optimization algorithm automatically increases or decreases the RF power for an AP according to the co-channel interference.

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

The **Recent RF Scan History** page displays historical records of automatic RF scanning and planning. Each record shows triggering information got 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 the APs, and the running logs.

● Smart RRM

There are two execution modes: immediate and periodic. Click **Scan Now**, and the cloud triggers RF scanning. Data will be uploaded after scanning.

● Schedule Settings

On the **Schedule Settings** page, **Periodic Execution** can be enabled.

> When a periodic task is triggered, this periodic task is automatically canceled if the network is already in a scanning triggered state (for example, immediate execution is being triggered).

● Related parameters

(1) Scan Mode

Quick Scan: This mode enables APs to provide the WiFi service properly during scanning. However, data acquired in this mode is not as accurate as that in the **Deep Scan** mode. The calculation result based on the data in this mode is less

accurate than that in the **Deep Scan** mode. This mode is applied when it is expected that the current network is not affected.

Deep 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 **Quick 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) Synchronize to Device
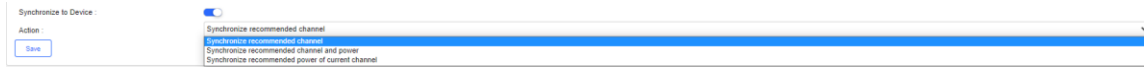
If this function is enabled, the RF scanning result will be automatically pushed to the AP. In this case, skip step 3.

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

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

After the status in the record of the triggered RF planning displays **Finish**, check the planning results, and synchronize the recommended automatic planning RF configurations to the APs.

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

(1)   Click ▤ **Recent RF Scan History** in the list to display the automatic RF planning result list of the APs.
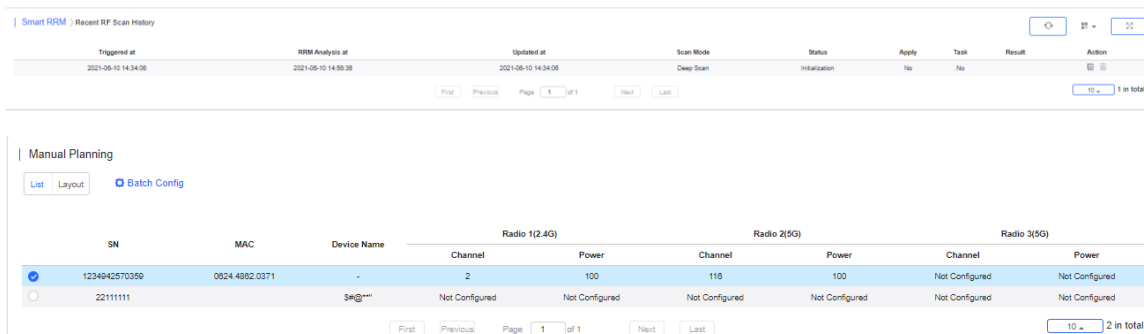
In the RF optimization result list of the APs, **Recommended Power of Current Channel** indicates a recommended power value for the current channel. **Recommended Power of Recommended Channel** indicates a recommended power value for the recommended channel. It is calculated based on the recommended channel, and is configured together with the recommended channel.

(2)   Click Sync Latest Config To AP 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. Any of the three modes can be selected 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.

6.2.4.3 Manual Planning

Click a network on the left to open the manual RF planning page. The **Radio Select** drop-down list above the diagram lets you 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.

ℹ️   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.

To perform manual RF planning:

1.   Set the RF configurations of a location in one of the following ways:

●   Configure one location

Click a location icon, enter configurations on the right, and click **Apply**.
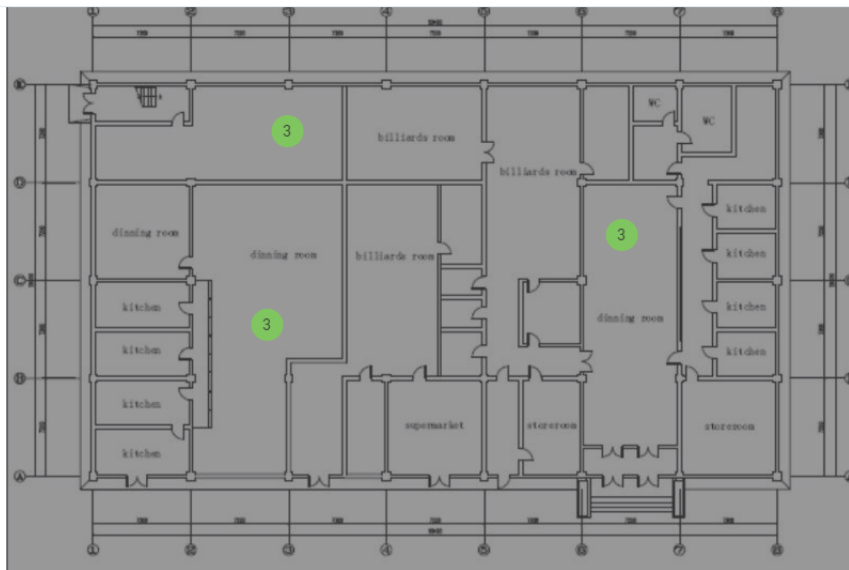
●   Configure locations in batches

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 network.

Click **Batch Config** above the location diagram to uniformly configure the power percentage for all locations on a network.

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

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

Batch operations for multiple locations can be select before clicking **Apply** .

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 an unbind or bind operation is performed, RF configurations are removed from or synchronized to the AP.

6.2.4.4 AC Smart RRM

In the AC network, click **Radio Planning** to open the **Smart RRM** page.
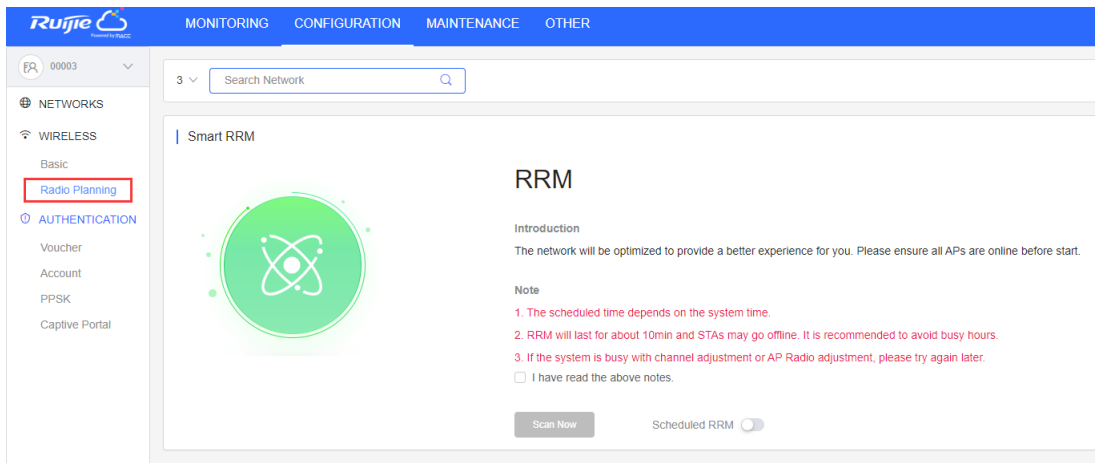
Check the note, click to start RRM. The whole process takes about 10 to 15 minutes.

Enable **Scheduled RRM** to configure the time, and RRM will start at the set time.

6.2.5 Roaming (Non-apartment Scenario)

Roaming planning refers to enabling network-based roaming.

L3 Roaming: Specify whether to enable Layer3 Roaming. It is enabled by default.

L2 InVLAN Tunnel Forwarding: Specify whether to enable Layer2 Roaming. It is enabled by default.
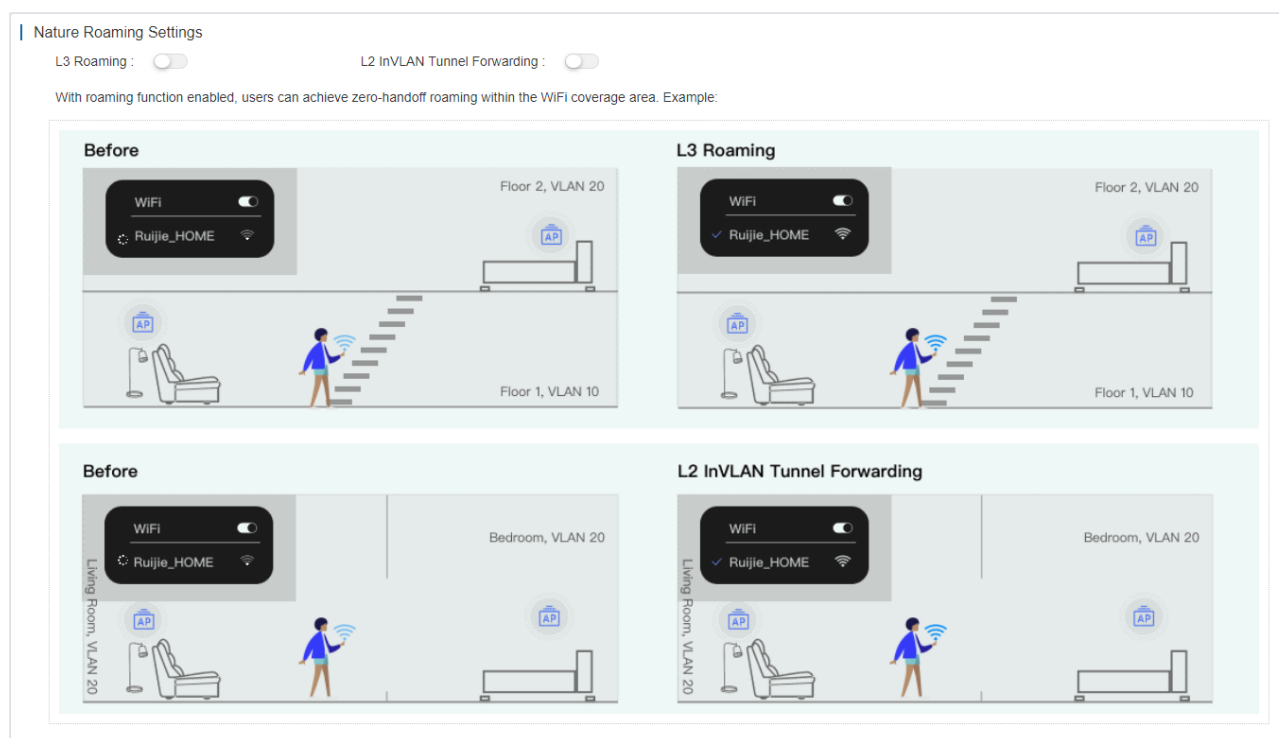
ℹ️ For wireless roaming, SSID signals must be consistent; otherwise, roaming may fail.

6.2.6   Bluetooth (Non-apartment Scenario)

You can batch import, add, change and delete the Bluetooth configuration.

● Bluetooth configuration import

Click **Import**. The **Import** dialog box is displayed. For initial use, you can click **Download Template** in the lower right corner to download an EXCEL file corresponding to APs in the current network and set corresponding parameters in the file. Requirements for the **UUID**, **Major**, and **Minor** parameters are:

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   ×

Please download the template and enter the Bluetooth configuration before uploading the template. Up to 200 records can be imported

[".xls" File]   [Download Template]

[Cancel]

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 :   [   ] *
Status :   ( )
UUID :   [   ] *
Major :   [   ] *
Minor :   [   ] *

                                                    [Save] [Close]

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

● Bluetooth configuration modification for a single AP

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

6.3 Authentication

6.3.1 Voucher

6.3.1.1 Voucher Authentication

Voucher authentication on Ruijie Cloud allows you to charge users for wireless network access using access codes. Concurrent users, time period and data quota limit can be customized and offered to your guests.

6.3.1.2 Configuration Steps

1. Enable **Voucher** function in the **Captive Portal** mode of **SSID** under the corresponding network.

2. Select **CONFIGURATION > AUTHENTICATION > Voucher**.

3. Select **Manage Package > Add Package** to define a voucher type for your guests.

4. Click **OK** to go back to the **Voucher** page and click **Print Voucher**.

5. Select the way you want to print voucher codes and enter the quantity if you select **Multiple Vouchers**.

6.   Click the **Print** button.

6.3.1.3 Bind/Unbind MAC

If **Bind MAC** is enabled for the package, the voucher code used by a device will be bound with its MAC address. The number of bound MAC can be set in **Max Concurrent Devices**. When the **Status** is **Activated** or **Depleted**, you can click

 in the **Bind MAC** column to unbind MAC addresses.

6.3.2 Account

6.3.2.1 Account Authentication

Account authentication requires the valid account and password. Concurrent users, time period and data quota limit can be customized and offered to your guests.

6.3.2.2 Configuration Steps

1.   Enable **Captive Portal** in the **SSID** page, and select a template with Account Authentication.

2.   Select **CONFIGURATION > AUTHENTICATION > Account**.

3.   Select **Manage Package > Add Profile** to define an account type for your guests.

Add Profile   ✕

Profile Name [   ]   *

Description [   ]

Concurrent Devices [3   ˅] ❓

Period [30 Minutes   ˅]

Data Quota [100 MB   ˅] ❓

Download Speed [Unlimited   ˅]

Upload Speed [Unlimited   ˅]

[OK]   [Cancel]

4.   Click **OK** to go back to the **Account** page and click **Add Account**.

5.   Enter the account and password, select the package, and click **Save**.

Add Account   ✕

Account ⓘ [   ] *   Description: 1
                                          Max Concurrent Devices: 3
Password ⓘ [   ] *   Period: 30 Minutes
                                          Data Quota: 100 MB
Profile [1   ˅]   Download Speed: Unlimited
                                          Upload Speed: Unlimited
Alias [   ]

[Batch Import]   [Save]   [Cancel]

6.   Connect to the SSID, select **Account Login** in the pop-up page, enter the account and password created in the last step, and click **Login**.
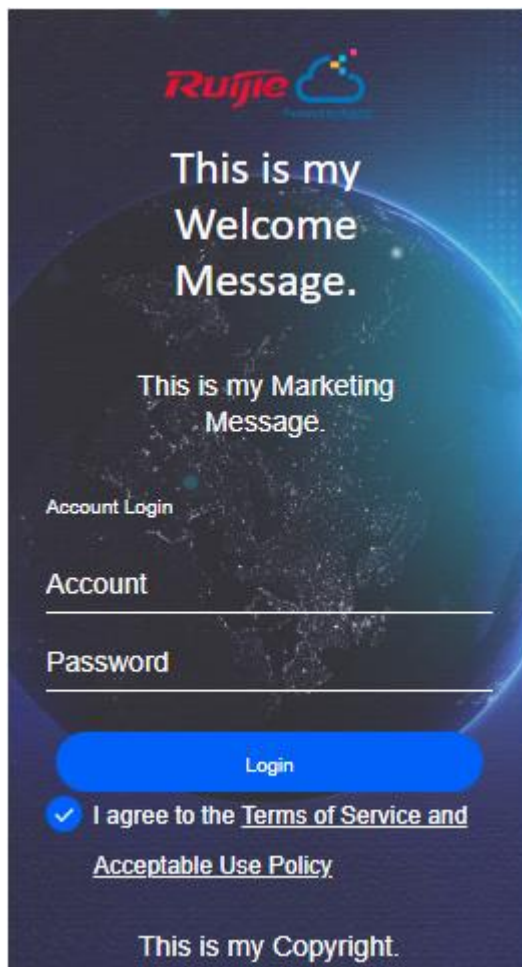
6.3.3 PPSK

6.3.3.1 PPSK Authentication

PPSK combines the advantages of PSK and 802.1x. It prevents the network from being stolen. Each terminal device is bound with a unique WiFi account and key so that the key will not be shared. This can also be called "One Client, One Password".

1. The main tasks of the PPSK administrator:

    ● Log in to Ruijie Cloud and deploy the network, so that APs can access the Ruijie Cloud.

    ● Set the authentication mode of SSID to PPSK (the administrator can configure it directly).

    ● On the **PPSK Configuration** page, an enterprise can enable the PPSK function and choose the network.

    ● Open account for staffs in batch.

2. Staffs can connect to the SSID with a unique WiFi key allocated by the administrator and access the Internet.

6.3.3.2 Configuration Steps

1. Choose **CONFIGURATION** > **WIRELESS** > **Basic**, click ⊕ beside **SSID**, and set the **Encryption Mode** as **PPSK**.

2.   Choose **CONFIGURATION** > **AUTHENTICATION** > **PPSK**.

3.   Click **Add Account** to batch import or manually add new accounts.

4.   Click the view button on the **Action** column of the PPSK list to check **PPSK Sync Log**.

5.   Bind MAC address for accounts in the PPSK list.
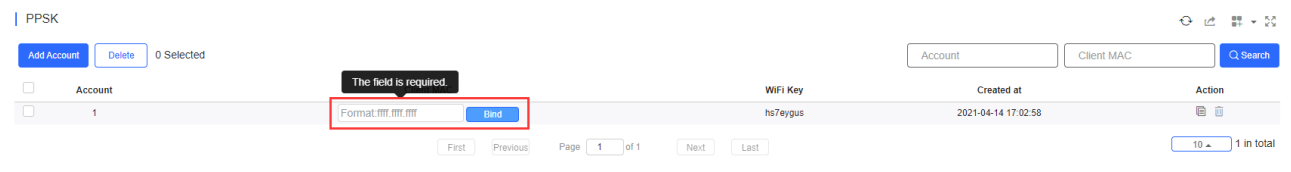
6.3.4   Captive Portal

Select **CONFIGURATION > AUTHENTICATION > Captive Portal** to display the **Captive Portal** page, and select a network on the top to filter captive portals.

When **Captive Portal** is enabled, SSID can associate with the templates. You can manage templates under a network, but only use or associate templates under a sub-network.

6.3.4.1   Captive Portal List

The list displays all captive portal templates, including thumbnails, name, association status, creation time and description.

●   Add Captive Portal
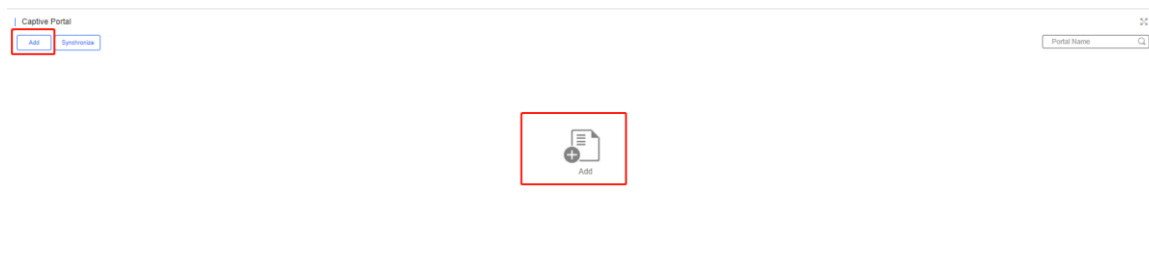
Click ![icon] or [Add] to open the **Add Captive Portal** page. Enter name, description and post login URL, and select login options. After **Status Balance Page** is enabled, you can check your balance information after login.

There are four login options: **One-click Login, Voucher,** and **Account**.

One-Click Login: You can set **Access Duration** and **Access Times Per Day**.

The page for One-click Login:
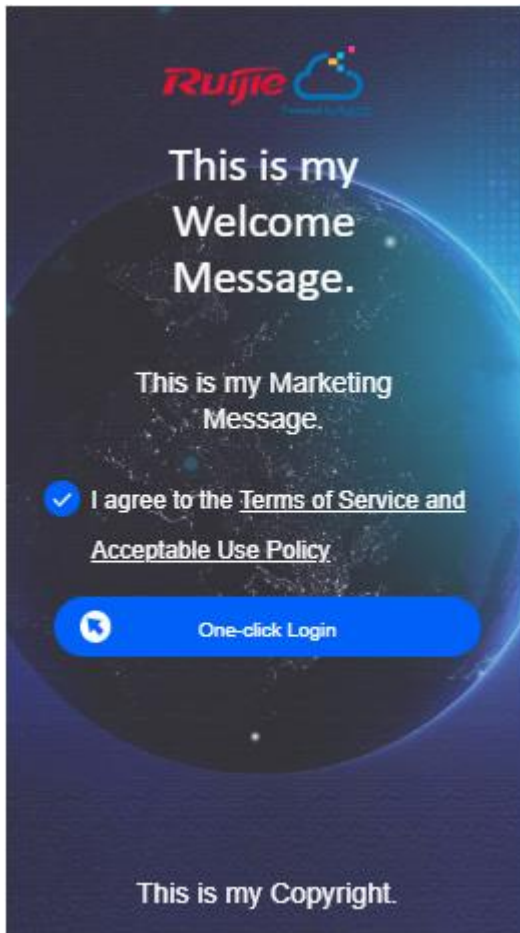
Voucher: You can log in with the voucher code.

The page for Voucher:
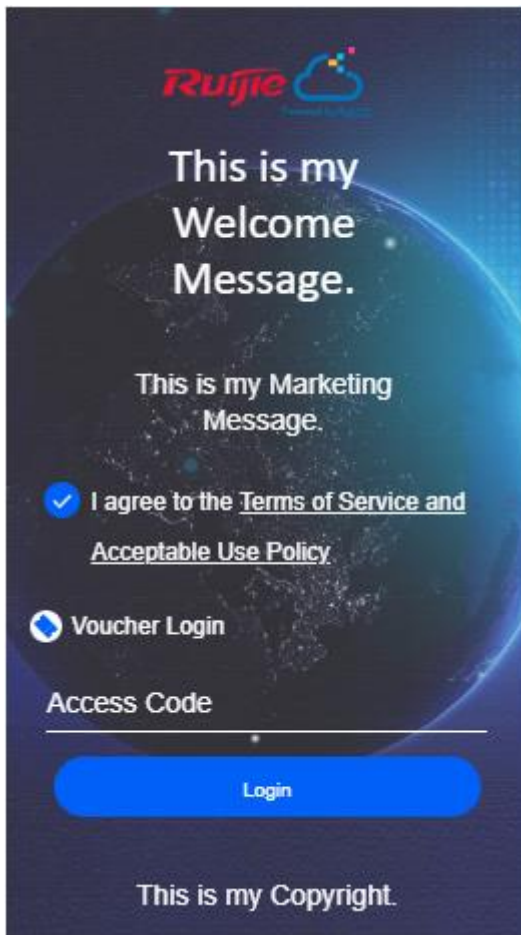
Account: You can log in with the account and password.

The page for Account:

You can also select multiple login options. The page for One-click Login, Voucher, and Account Login:

● Portal Page

You can customize the content and style of the login page. The previews on the mobile phone and PC are displayed on the right.

Note: Each type of authentication supports a maximum of three languages. During authentication, users can select a language switching icon in the upper right corner of the authentication page to switch the language.

In the **Basic** tab, set the logo picture, background color or image, welcome massage, marketing message, terms & conditions and copyright.

In the **Advanced** tab, set the Logo position, background mask color/opacity, text color/size. Click **Reset Style** to restore the default style.

Click [OK] on the bottom to save.

6.3.4.2 Edit Captive Portal
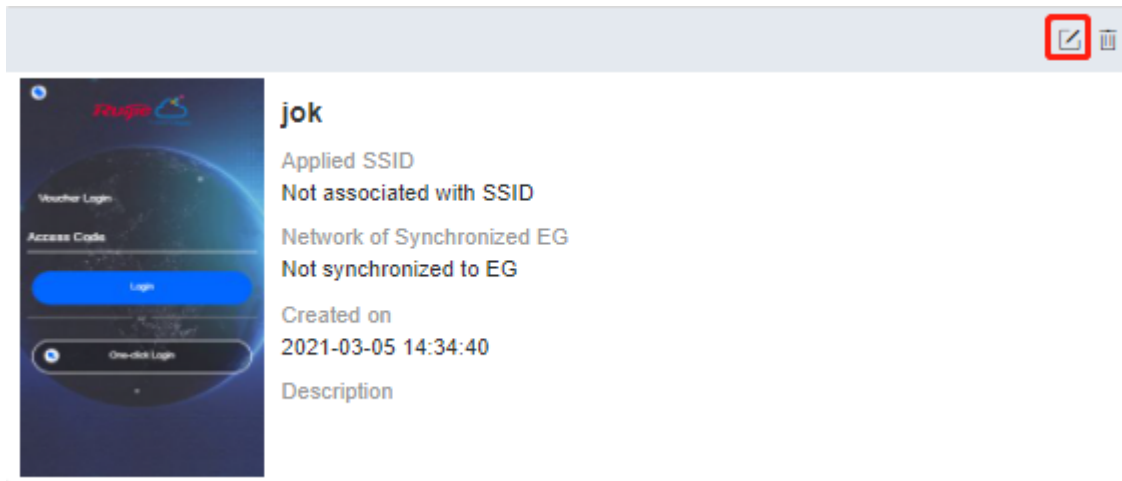
Click [edit icon] to edit a template, and click [OK] to save.

6.3.4.3 Delete Captive Portal
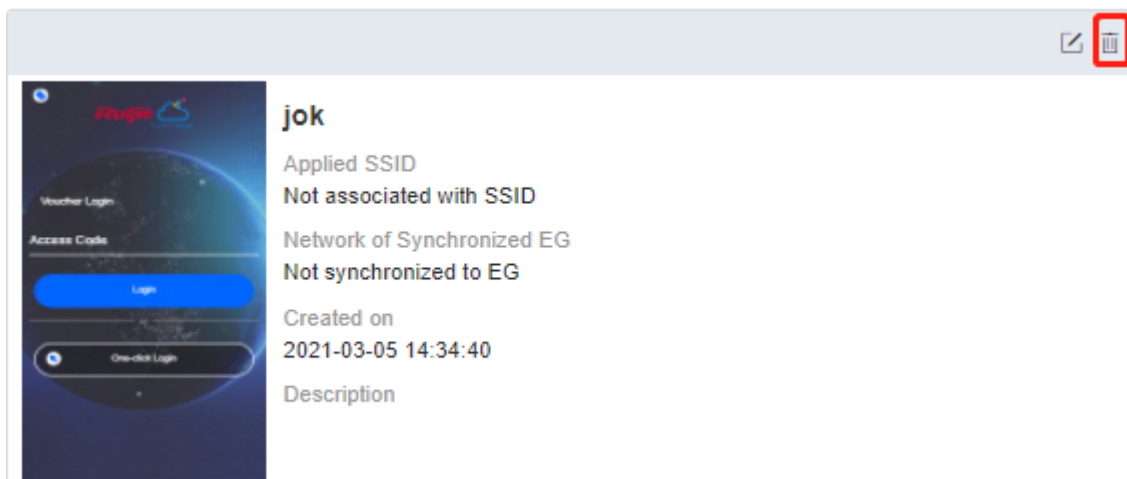
Click [delete icon] and then click [OK] in the confirmation window to delete a template.
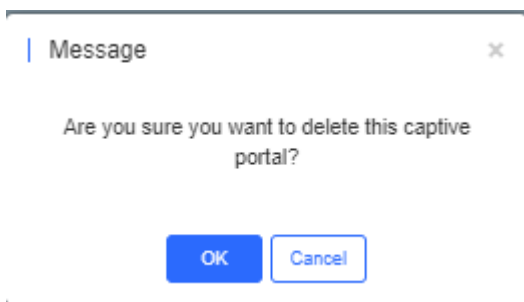
If the template is associated to an SSID or applied to the EG, then you need to dissociate it before delete.

Message   ✕

The portal is in use. Please dissociate first.
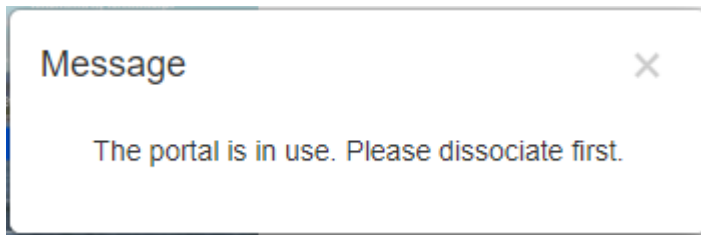
6.3.4.4 Apply to EG

Click [Synchronize] to synchronize the captive portal template to the EG.

If no EG exists in the current network, you can click [icon] to jump to the **MONITORING** > **DEVICE** > **Gateway** page.

| Captive Portal ⟩ Synchronize

Please add a gateway first.
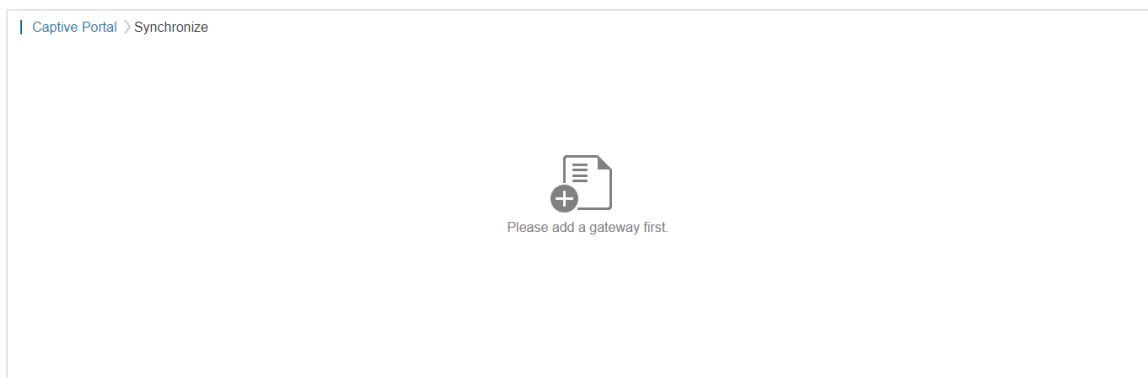
If there is an EG in the current network, the page is displayed as below:
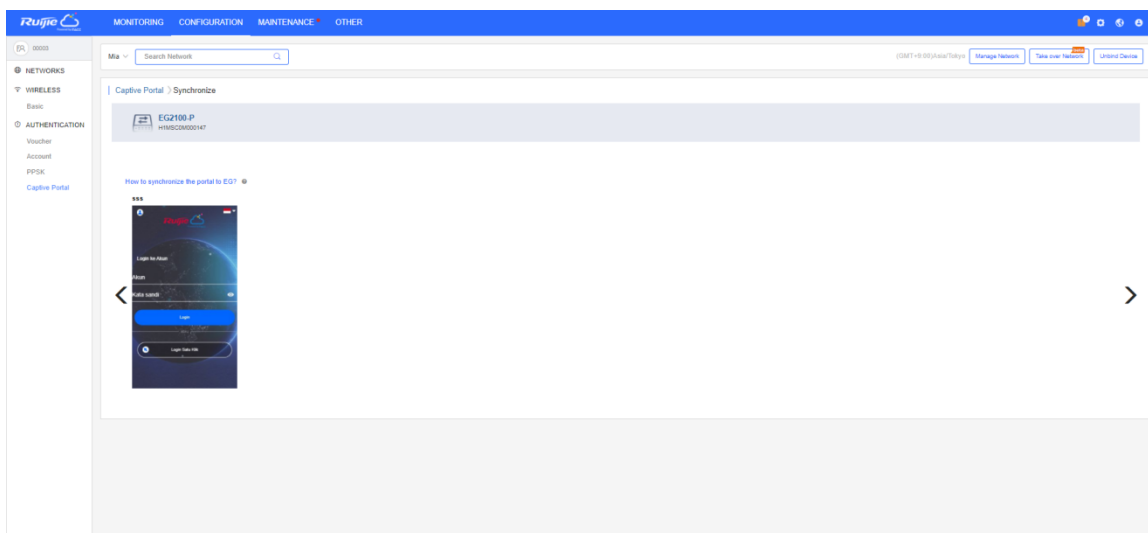
Only one template can be synchronized to an EG. Select a template and click [OK].
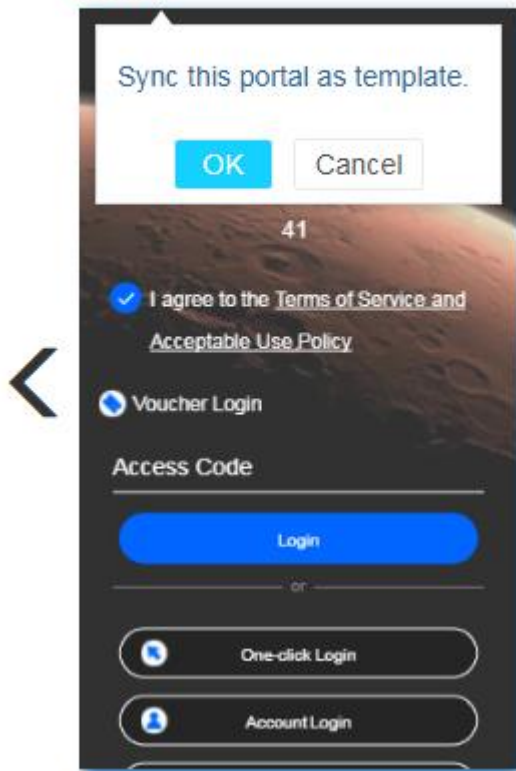
After the template is applied, the date of last synchronization will be displayed above.
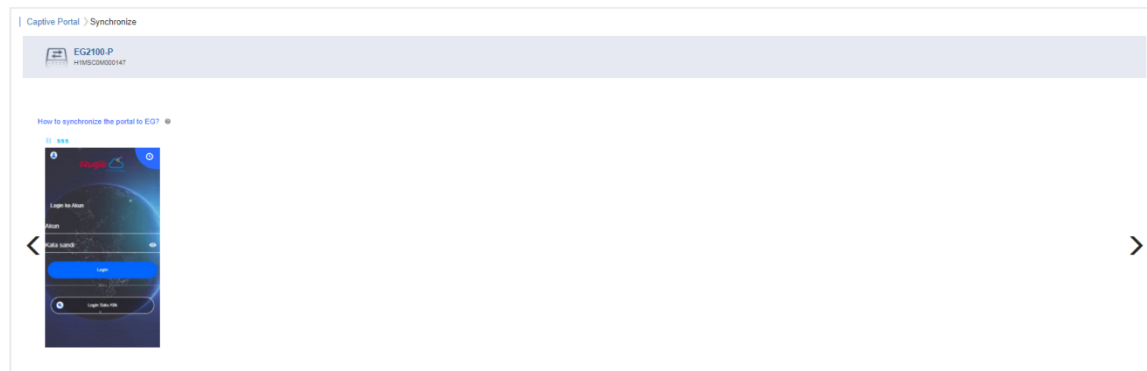
7   Maintenance

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

● LOGS

● UPGRADE

7.1 Logs

7.1.1   Operation Log

This page shows operation logs.

Click to check log details.

General operation log details are shown as follows:

7.1.2   Config Log

7.1.2.1   Action View

When the device configuration is imported, a prompt will pop up. Click the prompt to open the log page and export the SSID result.

On the log page, the latest record will be displayed by default

- Status: View the status of the configuration

  Complete: Configuration completes

  Incomplete: Configuration is in progress

- Result: View configuration results

  Success: Number of devices configured successfully

  Failure: Number of devices whose configuration fails

- Devices

  Total: Total devices in the network

  Offline: Number of offline devices

  Not Online Yet: Number of devices that never go online

Cloud will give priority to the online devices, and will actively apply the configuration after the offline devices go online.

- Description: View configuration command

- Refresh: As it takes a while to complete the configuration, you can click this button to refresh the configuration progress.

Click to display more configuration information.

Click [icon] to export the configuration result.

The exported file is shown as the figure below.

You can check the result in the column **Result** which may be "Succeeded" or "Failed".

7.1.2.2 End SSID and Password Configuration of Offline Device Immediately (Apartment Scenario)

Suppose the operator changes the SSIDs and passwords of two rooms and exports the result.

Although there are offline devices waiting for SSID and password configuration, the overall configuration is completed. The operator can export result and send new SSIDs/passwords to the tenant. When the offline devices go online, the new SSIDs and passwords will be synchronized to the devices automatically.

7.1.2.3 Device View

Click ▤ in the action column to check the push status of each configuration item.

The following figure shows an example of full configuration, including the configuration execution status of SSID, Radio and so on.

7.1.3 Upgrade Log

This part provides the upgrade tracing function. You can check the upgrade status, and abort or retry the upgrade.

Retry: Restarts the upgrade task that failed or was aborted.

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

Click ▤ to check log details.

Retry: Restart the upgrade task.

Abort: Stop the upgrade task.

> ℹ **Abort**: You can not stop the upgrade task if the upgrade command has been pushed to the AP.
>
> ℹ **Retry**: You can only restart the failed or aborted upgrade task.

7.2 Upgrade

The following tab pages are provided for device firmware management:

● Upgrade

● Firmware

7.2.1 Upgrade

Ruijie Cloud supports the online upgrade of device firmware, and it allows network administrators to utilize the latest features and security enhancement for their Ruijie devices. Online upgrade allows administrators to easily arrange the firmware upgrade on their networks and view firmware releases.

The **Upgrade** page includes two modules:

● Version statistics

● Firmware upgrade

Three ways are available to check whether there is a new version for the device:

1)   **MAINTENANCE** Menu (for all devices)
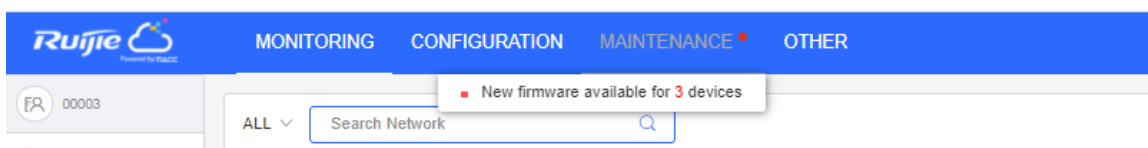
2)   **Upgrade** in the Navigation Bar (for all devices)

3) **AP List**, **Switch List** and **Gateway List** (for devices in the network)

7.2.1.1   Check Version Information

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

7.2.1.2   Upgrade

You can enter the **Upgrade** page in either of the following ways.

1.   Hover the mouse over **MAINTENANCE**, a link will appear. Click the link to enter the **Upgrade** page. The default network information is **All**.

2.   On the **AP List, Switch List** or **Gateway List**, click **New firmware** to open **New Firmware List** window. Then click **Go to Upgrade** to enter the **Upgrade** page, and select and upgrade devices via **Search**.

3. Click **Go to Upgrade** in **Firmware List** to enter the **Upgrade** page, and select and upgrade devices via **Search**.

7.2.1.3 Upgrade 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 upgrading, and implements a quick upgrade with selected networks and version numbers. This mode enables upgrading of all APs in the list, and is suitable for a scenario with a large number of APs. A network or a firmware version number can be specified to perform fast upgrades.

● **Upgrade Selected**

1.   Select a network on the left, select a target AP, and click **Upgrade.**
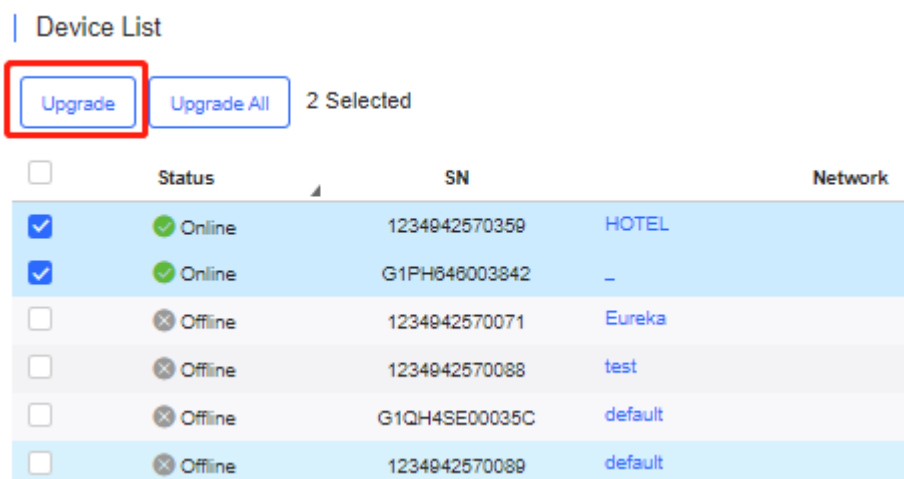
2.   Select a firmware version.

On the **Equipment Upgrade** page, you can check the device information and the details of versions, choose a version (the recommended version is the latest one), enable scheduled upgrade and set retry times if the upgrade fails.

3. Upgrade the selected APs

● **Upgrade All**

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

2. Select the version and click **Start Upgrade**

Upgrade   ✕

Check in Maintenance > Log >Upgrade Log

Model: XS-S1930J-18GT2SFP   Hardware Version: 1.00   Current Version: S1930J_RGOS 11.4(1)B70P15, Release(08140110)   ✕

Upgrade Version: Please select a firmware version.   [Select Firmware]

Upgrade Device: 1

Model: XS-S1930J-18GT2SFP-P   Hardware Version: 1.00   Current Version: XS1930J_RGOS 11.4(1)B70P15, Release(08160218)   ✕

Upgrade Version: Please select a firmware version.   [Select Firmware]

Upgrade Device: 1

Model: XS-S1930J-48GT4SFP   Hardware Version: 1.00   Current Version: S1930J_RGOS 11.4(1)B70P10, Release(07233016)   ✕

Upgrade Version: Please select a firmware version.   [Select Firmware]

Upgrade Device: 1

Model: XS-S1930J-8GT2SFP   Hardware Version: 1.00   Current Version: S1930J_RGOS 11.4(1)B70P15, Release(08132618)   ✕

Upgrade Version: Please select a firmware version.   [Select Firmware]

Upgrade Device: 1

Model: AP180(JA)   Hardware Version: 1.01   Current Version: AP_RGOS 11.9(4)B1P3, Release(07211112)   ✕

Upgrade Version: Please select a firmware version.   [Select Firmware]

Upgrade Device: 1

☐ Scheduled Upgrade

Advanced Settings ∨

[Start Upgrade]   [Cancel]

Set the update criteria and click **Start Upgrade**, and a message box will pop up. Users can check details in **LOGS > Upgrade Log**.

Message   ✕

The upgrade task has been created. Please check

Upgrade Log for details.

| Upgrade Log

Operator	Description	Target Version	Process	Time	Result (Success/Failure/Aborted)	Action
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15, Release(08140223)	0/ 1	2021-04-14 16:44:06	0/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15, Release(08140223)	1/ 1	2021-02-03 14:52:08	1/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15, Release(08131911)	1/ 1	2021-01-20 16:21:32	1/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15, Release(08132009)	1/ 1	2021-01-20 16:01:13	1/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15, Release(08131911)	1/ 1	2021-01-20 15:50:44	1/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15, Release(08132009)	1/ 1	2021-01-20 15:31:29	1/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15, Release(08131911)	1/ 1	2021-01-20 15:21:19	1/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15	1/ 1	2021-01-20 15:19:20	1/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15, Release(08132009)	1/ 1	2021-01-20 15:11:18	1/0/0	
testdemo	Upgrade selected1 device(s)	XS19_RGOS 11.4(1)B70P15	1/ 1	2021-01-20 14:02:32	1/0/0	

First   Previous   Page 1 of 2   Next   Last   10 ▲   12 in total

Details   ×

SN	Upgrade Status	Retry Times	Started at	Ended at	Description	Action
1234942570071	Executing	0	2021-04-14 16:44:06	-	Downloading files…Please wait	

First Previous Page 1 of 1 Next Last   10 1 in total
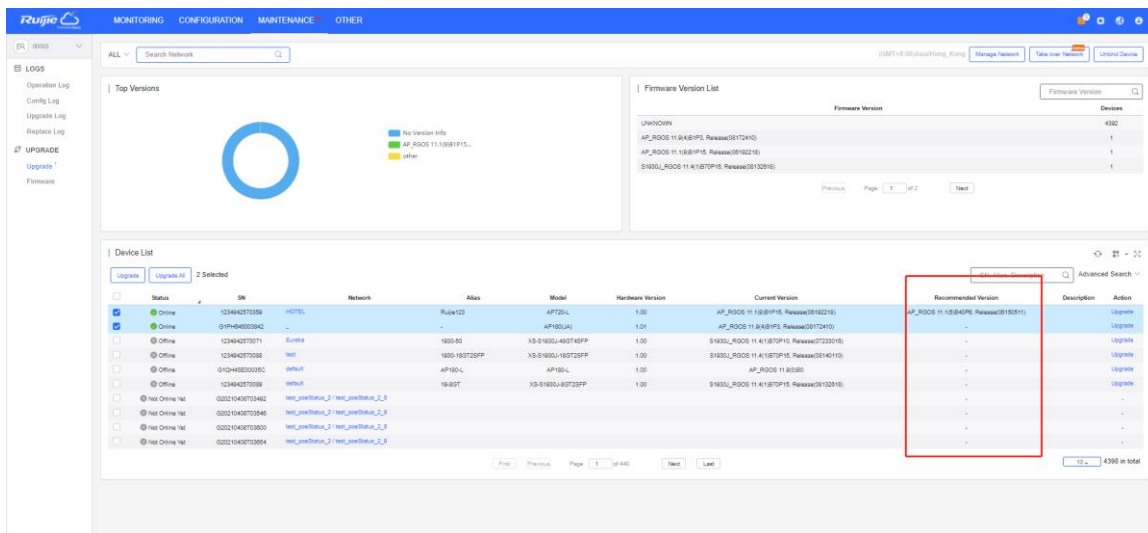
3. If the upgrade is successful, log will show **Upgrade succeeded**.

Details   ×

SN	Upgrade Status	Retry Times	Started at	Ended at	Description	Action
1234942570089	Succeeded	0	-	2021-02-03 14:52:09	Your version is the latest version	

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

Check the results in the **Recommend Version** of **Device List**.

The numbers of devices which have available firmware for upgrade in **MAINTENANCE** Menu and **Upgrade** in Navigation Bar will change accordingly.

7.2.2   Firmware

7.2.2.1   Version Details

The **Version Details** list displays the versions of firmware installed on all devices. Click **Go To Upgrade** in the **Action** column to open the **MAINTENANCE** > **UPGRADE** > **Upgrade** page.

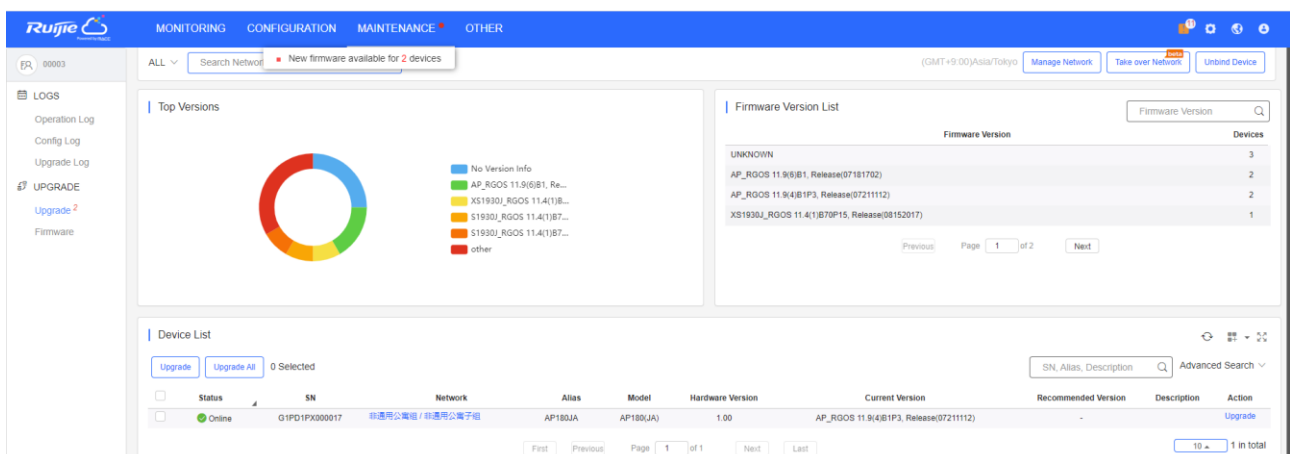| Model	Current Version	Hardware Version	Devices	Recommended Version	Action
UNKNOWN	UNKNOWN	UNKNOWN	3449	-	Go To Upgrade
XS-S1930J-18GT2SFP	S1930J_RGOS 11.4(1)B70P15, Release(08140110)	1.00	1	-	Go To Upgrade
XS-S1930J-48GT4SFP	S1930J_RGOS 11.4(1)B70P10, Release(07233016)	1.00	1	-	Go To Upgrade
AP180(JA)	AP_RGOS 11.9(4)B1P3, Release(07211112)	1.01	1	-	Go To Upgrade
XS-S1930J-8GT2SFP	S1930J_RGOS 11.4(1)B70P15, Release(08132618)	1.00	1	-	Go To Upgrade
XS-S1930J-18GT2SFP-P	XS1930J_RGOS 11.4(1)B70P15, Release(08160218)	1.00	1	-	Go To Upgrade

First   Previous   Page 1 of 1   Next   Last   10 ▲ 6 in total

7.2.2.2   Private Firmware

The **Private Firmware** list displays the private firmware uploaded by all accounts under a tenant.

	Firmware Version	File	File Size (MB)	Applicable Model	Uploaded at	Released at	Description	Action
☐	XS19_RGOS 11.4(1)B70P15, Release(08140223)	XS19_RGOS11.4_1_B70P15_08140223_install.bin	20.15	NBS2028G-E-LP::1.20,NBS228F-E-LP::1.10,...	2021-02-03 14:47:38	2021-02-03 14:47:38	8GT	✎ 🗑
☐	XS19_RGOS 11.4(1)B70P15, Release(08132009)	XS19_RGOS11.4_1_B70P15_08132009_install.bin	19.71	NBS2028G-E-LP::1.20,NBS228F-E-LP::1.10,...	2021-01-20 14:10:57	2021-01-20 15:10:56		✎ 🗑
☐	XS19_RGOS 11.4(1)B70P15	XS19_RGOS11.4_1_B70P15_install-0120.bin	19.71	NBS2028G-E-LP::1.20,NBS228F-E-LP::1.10,...	2021-01-20 13:02:08	2021-01-20 14:02:07		✎ 🗑
☐	XS19_RGOS 11.4(1)B70P15	XS19_RGOS11.4_1_B70P15_install-0119.bin	19.71	NBS2028G-E-LP::1.20,NBS228F-E-LP::1.10,...	2021-01-19 14:22:37	2021-01-19 15:22:37	1930-18GT-0119	✎ 🗑
☐	XS19_RGOS 11.4(1)B70P15, Release(08131911)	XS19_RGOS11.4_1_B70P15_08131911_install.bin	19.71	NBS2028G-E-LP::1.20,NBS228F-E-LP::1.10,...	2021-01-19 13:45:37	2021-01-19 14:45:37	S1930J-18GT-0119	✎ 🗑

First   Previous   Page 1 of 1   Next   Last   10 ▲ 5 in total

Click **Upload Firmware** to upload private firmware.

Upload Firmware   ✕

'tar.gz' or '.bin' File

Close

Upload Firmware   ✕

        File   RG-MACC_JP_RC_1.2.1D_Build_48.tar.gz

  Description [   ]

               [Import]

                                                                    [Close]

Click [✎] in the **Action** column to edit the **Description** of firmware.

Edit Description   ✕

        File   AP_RGOS11.9_4_B1P2_S2X2-08-FULL_07200421_install.bin

  Description [   ]

                                                      [OK] [Cancel]

Click **Delete** or [🗑] in the **Action** column to delete private firmware.

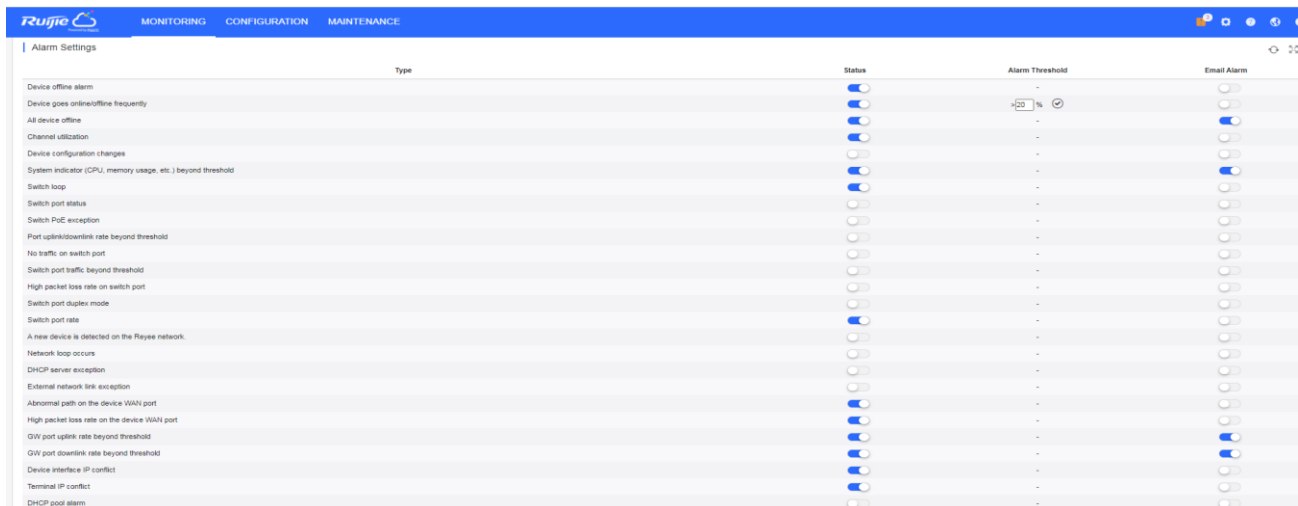Message   ✕

   Are you sure you want to delete the firmware?

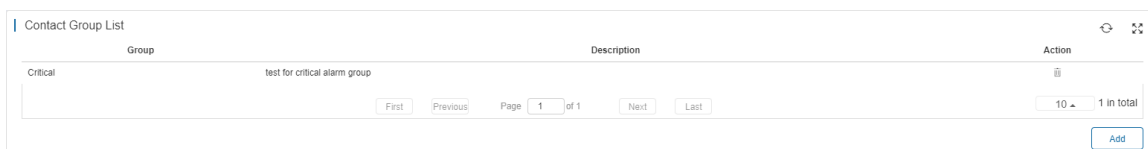   [OK] [Cancel]

8 System Settings

8.1 Alarm Settings

Click in the upper right corner and select **Alarm Settings**. The **Alarm Settings** page is displayed for alarm parameter configuration.

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

On the **Alarm Settings** page, you can configure to receive alarms or not and in which way. When the **Status** is enabled, alarm information is displayed on the **Alarm** page. Alarms can be pushed via Email only when the **Status** is enabled. When the **Email Alarm** is enabled, alarms will be pushed via Email to the contacts in the **Contact List** of the network.

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 6.2.2.

8.2 Contact

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

8.2.1 Contact List

Add a contact as the Email recipient.

Contact List				
Name	Mobile	Email	Description	Action
TestContact	18800001111	test@test.com	test contact	☑ 🗑

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

Add

Add/Edit Contact   ✕

Name :   [   ] *

Email :   [   ] *

Mobile :   [   ] *

Description : [   ]
              [   ]
              [   ] *

                                                    Save   Cancel

---

8.2.2   Contact Group

Add a group and move the contacts to the group.

Contact Group			
Group		Description	Action
lkisle		wwww	☑ 🗑
e_e_eport		===	☑ 🗑
test		www	☑ 🗑

First   Previous   Page 1 of 1   Next   Last   10 ▲   3 in total

Add

Edit Contact Group   ✕

Name   [lklskle   ]

Description   [wwww   ]
                [   ]

Contact Group   All Contacts
[jok   ]   [jok1   ]
                            << Add to Group
                            Delete from Group >>

                                                    Save   Cancel

9 Account

Point to on the upper right corner, the **Account** menu is displayed, which includes **Account**, **Sub Account** and **Logout**.
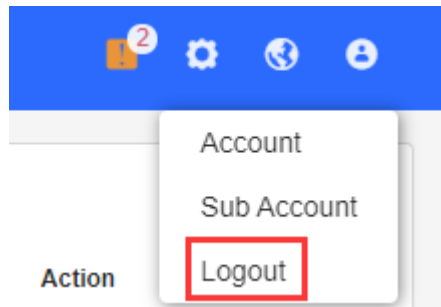

9.1 Account

The **Account** page is divided into the **User Info** area and **Modify Password** area. In the **User Info** area, you can edit the basic information of user (**Username** and **Email** is not allowed to be changed); In the **Modify Password** area, you can change the login password.

9.2 Sub Account

The **Sub Account List** displays the information of sub accounts. Click in the **Action** column to edit the sub account. Click in the **Action** column to delete the sub account.

Click **Add Sub Account** to add a new sub account. Select the network, enter the Email in the **Username** box and click **Send Code**. Enter the security code contained in the Email, set the password, language, full name, expiration date, mobile and role, and click **Save**.

Role: **Admin** owns the permissions to create an account. **Employee** owns the permissions to edit data. **Operator** owns the permissions to print voucher and view account data. **Guest** owns the permissions to view data.

The existing sub account can be added to the network so that a sub account can manage multiple networks.

Add Sub Account   ✕

Note: If you have a Cloud account, you can share the network and do not need to add a sub account. 🖝 Details

Type   ○ New Account   ● Existing Account

Network   default   *

Username (Email)   Please enter email   *

Role   Admin   ❓

Save   Cancel

9.3 Logout

Click **Logout** to exit the system and return to the login page.

10 Unbind Device

Click **Unbind Device**, enter the device SN to get URL. Configure the URL as the ACS URL on device, and the device will automatically unbind on Cloud.

11 Appendix

11.1 Acronyms and Abbreviations

Acronyms and Abbreviations	Full Name
AP	Access Point
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

11.2 Glossary

Term	Definition
Cloud	Specify the cloud center management end, supports private and public clouds, allows separate deployment of a system of a private cloud version, and provides cloud services of the public cloud version.
Network	Enable the device grouping for easy management of a large quantity of devices. It is recommended that networks be added by geographical location or device use.

11.3 Limitations

No.	Module	Description
1	Device	Up to 200 devices can be imported each time. To import more than 200 devices, users need to do it in batches.
2	Configuration	Configurations of up to 200 devices can be imported each time. To import configurations of over 200 devices, users need to do it in batches.
3	EXCEL template	For the Excel template, only the XLS format is supported.
4	SSID	SSIDs can be made up of numbers, English letters, and "-".
5	Custom excel template	In an Excel template for customization, A to Z columns and 1 to 15 rows are supported.
6	AP	Account-based policies may fail on some models, such as AP680(CD), where they are disabled by default. In this case, users need to batch apply from the Cloud the **web-auth acct-update-interval 1** command to enable those policies.
7	SSID reverse sync	The Cloud does not support SSIDs containing special characters. If such SSIDs are set on end devices, the Cloud would fail to deliver them after they are synchronized to the Cloud.