Ruijie Japan Cloud Service User Guide

Copyright statement

Exemption statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Audience

This manual is intended for:

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

Obtaining Technical Assistance

- Ruijie Networks Website: https://ruijie.co.jp/
- Technical Support Website: https://www.ruijie.co.jp/service
- Inquiry&Repair: https://www.ruijie.co.jp/service/post-sales
- Technical Support Email: support_jp@ruijienetworks.com

Symbols

Important information. Contains helpful suggestions or references.

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

Contents

1 Summary

Ruijie Japan 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

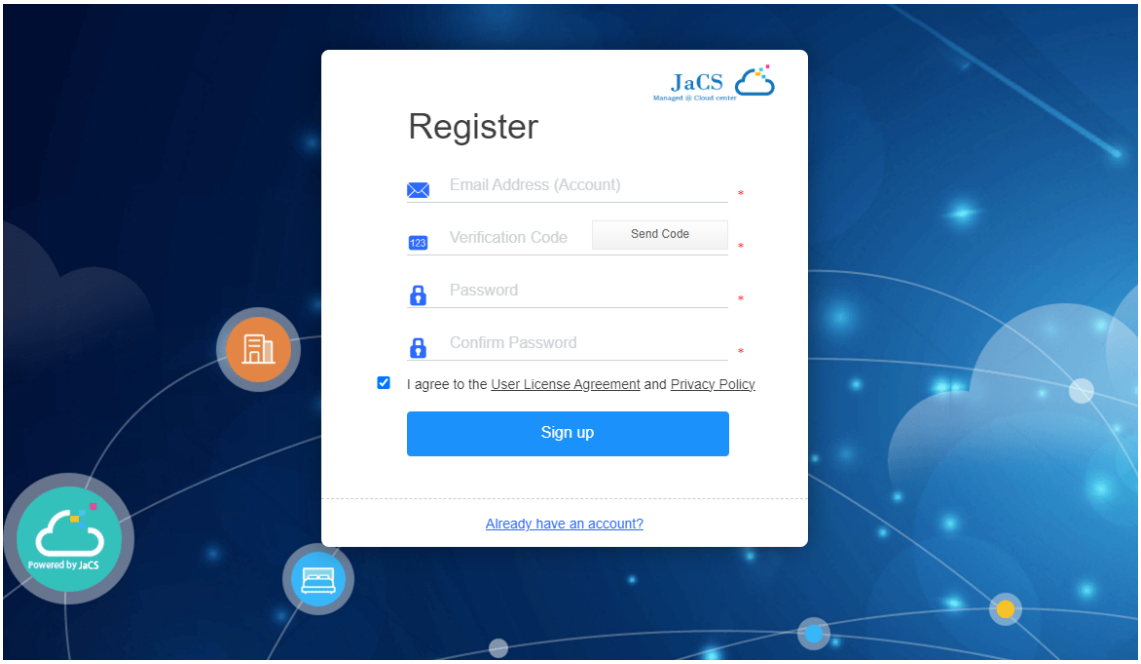
Source IP	Destination	Src. port	Dst. port	Protocol	Description	Device using this rule
Your network	devicereg.ruijienetworks.com devreg.ruijienetworks.com	Any	80, 443	TCP	Ruijie Cloud login server	Ap/AC/Switch/Gateway
Your network	cwmpsvr-japan.ruijienetworks.com	Any	80, 443	TCP	Ruijie Cloud server	Ap/AC/Switch/Gateway
Your network	35.194.101.74 34.84.13.46	Any	10000-12000	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

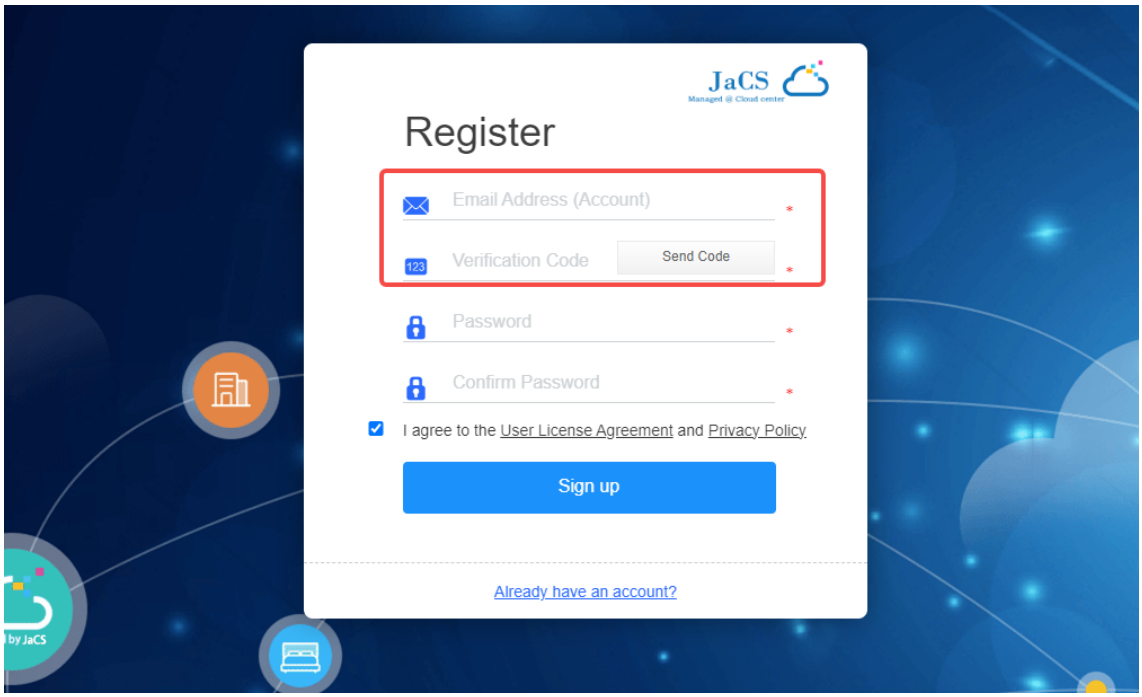
4.1 Register

1. Visit https://cloud-japan.ruijienetworks.com.

2. Click **Sign up** to open the **Register** page.

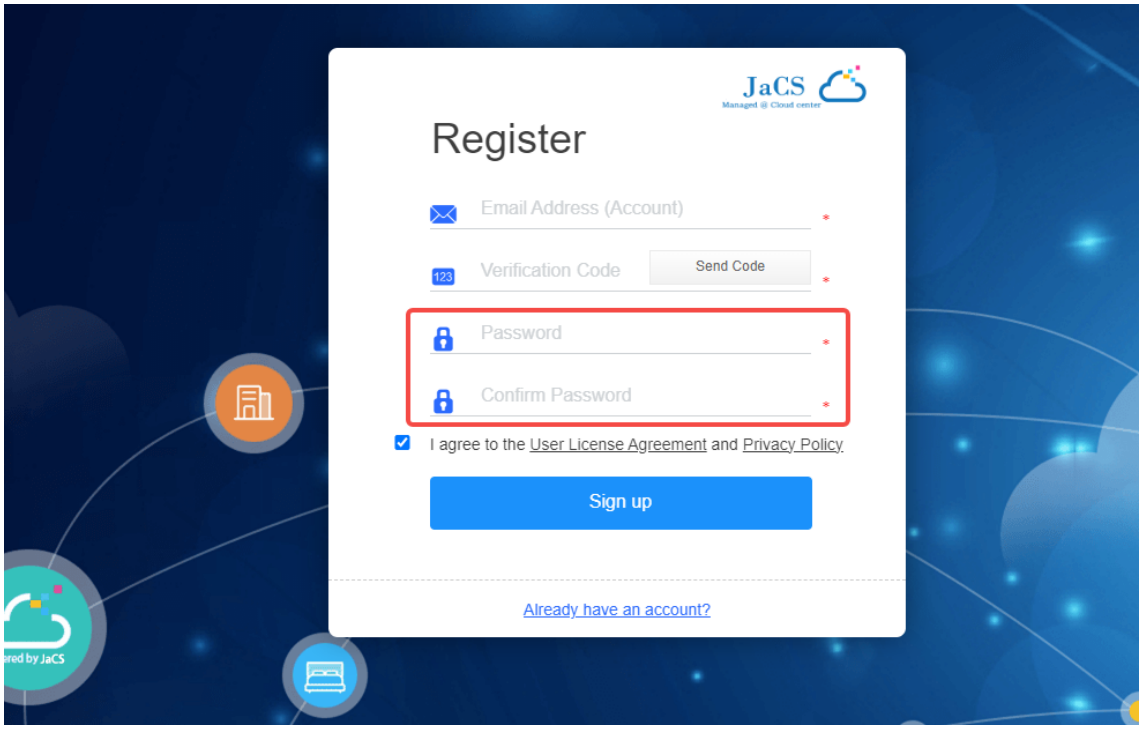


3. Enter your Email address, click **Send Code**, and enter the verification code contained in the Email into the **Verification Code** box.



One email address can be registered once only.

4. Enter and confirm the password.



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. 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.

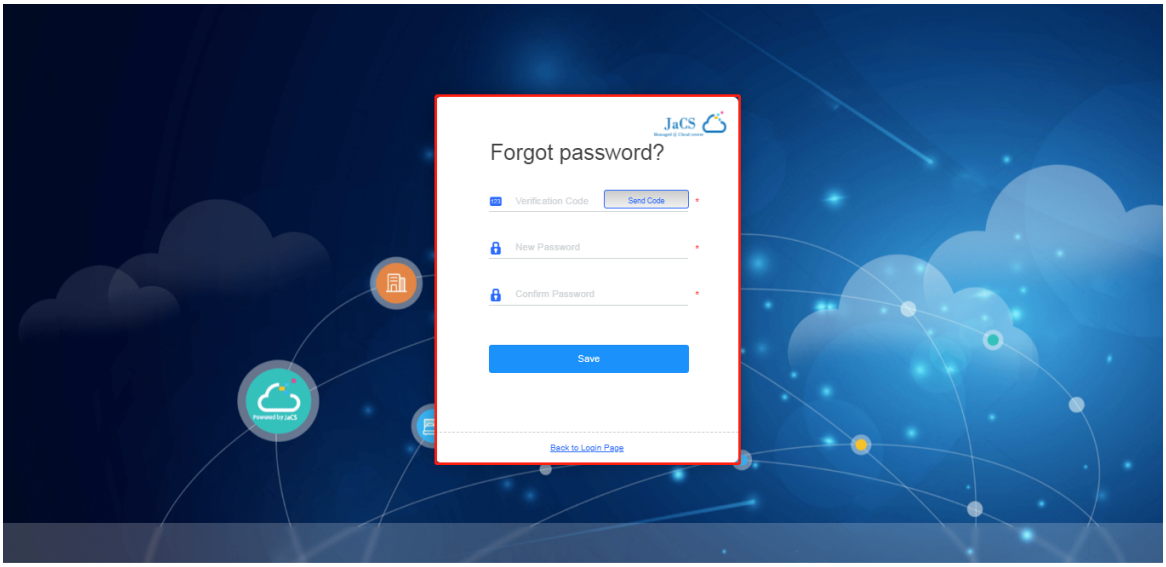
4.3 Trial Account

1. Click **Trial Account** to experience Ruijie JaCS under the guide without registering accounts.

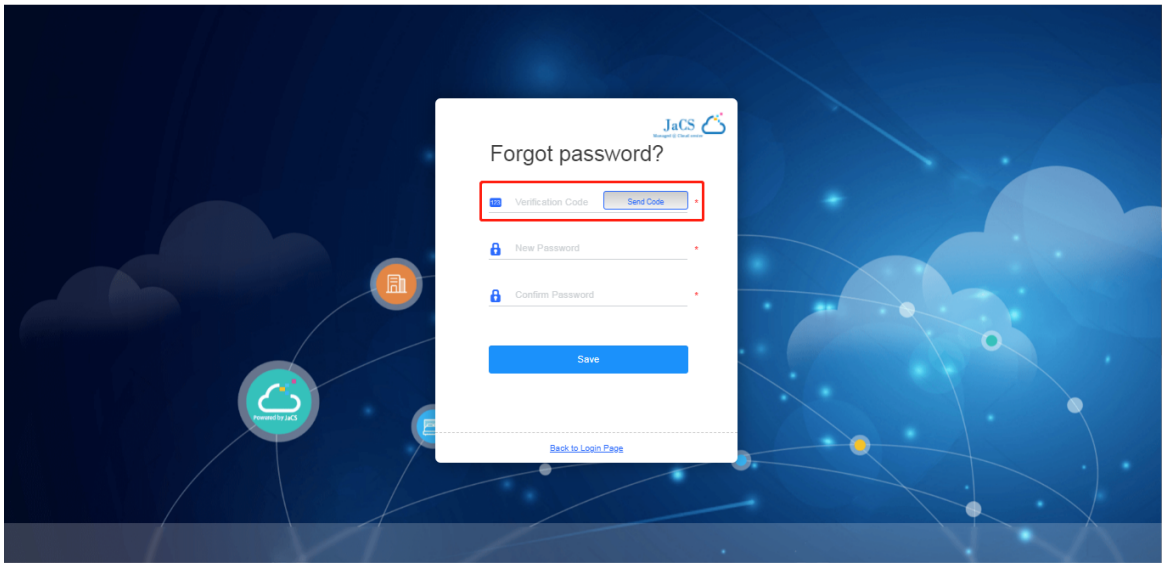
4.4 Forgot Password

1. Visit https://cloud-japan.ruijienetworks.com.

2. Click **Forgot password?** to open the **Forgot password** page.

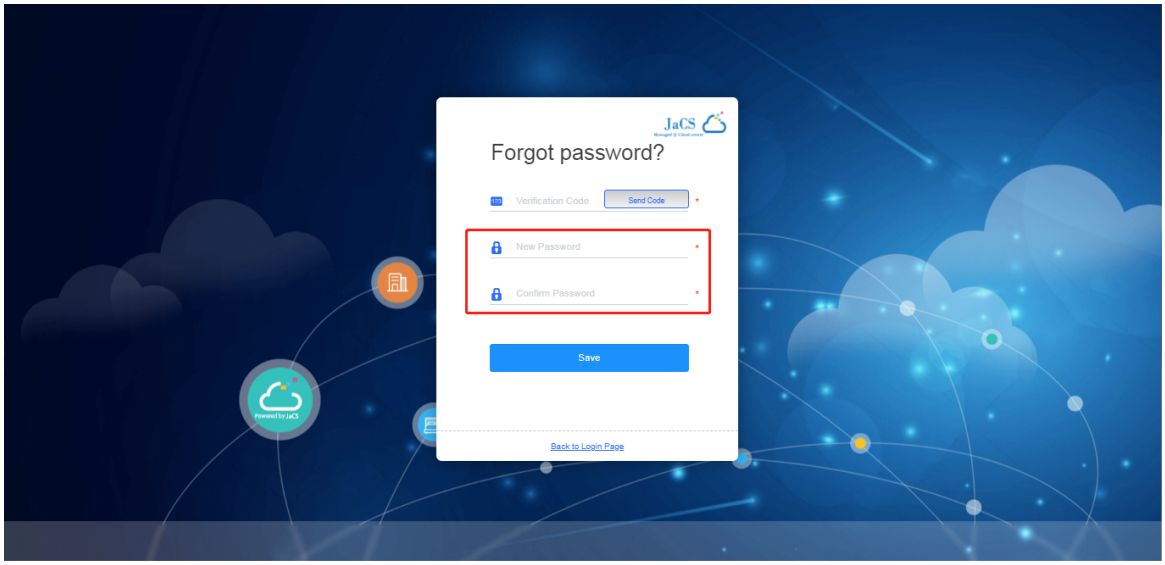


3. Enter the Email address for retrieving the password. Click **Send Code**, and enter the verification code contained in the Email into the **Verification Code** box.



The Email address is generally the same as the account.

4. Enter and confirm the new password.



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.

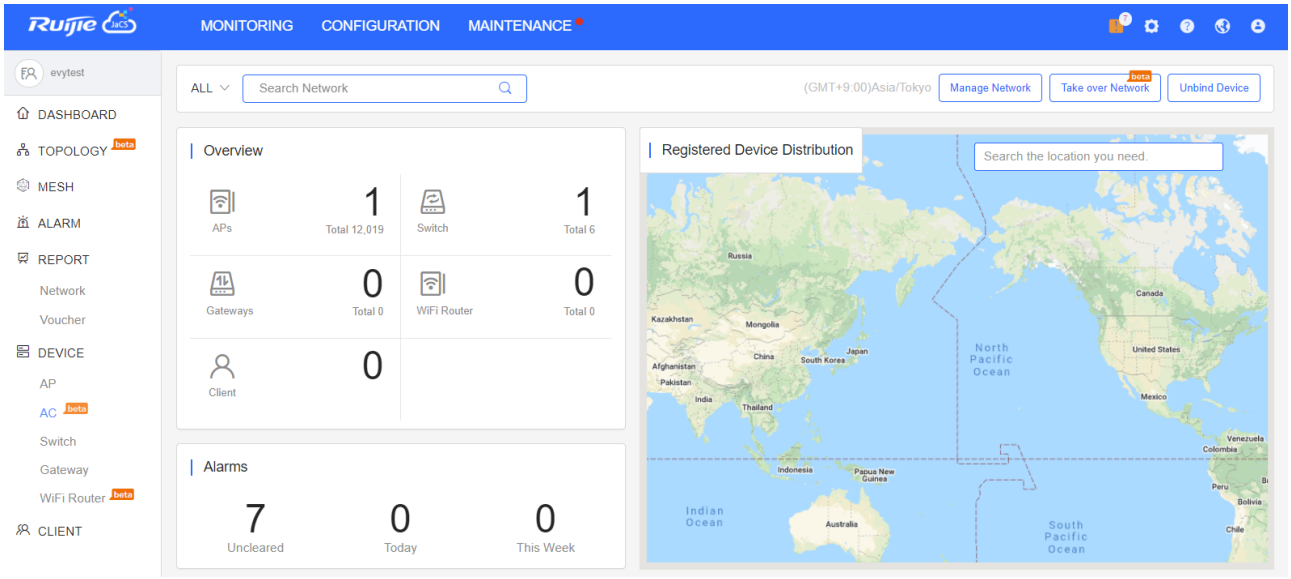
5 Monitoring

This part enables you to monitor the following items:

- DASHBOARD
- TOPOLOGY
- MESH
- ALARM
- REPORT
- DEVICE
- CLIENT

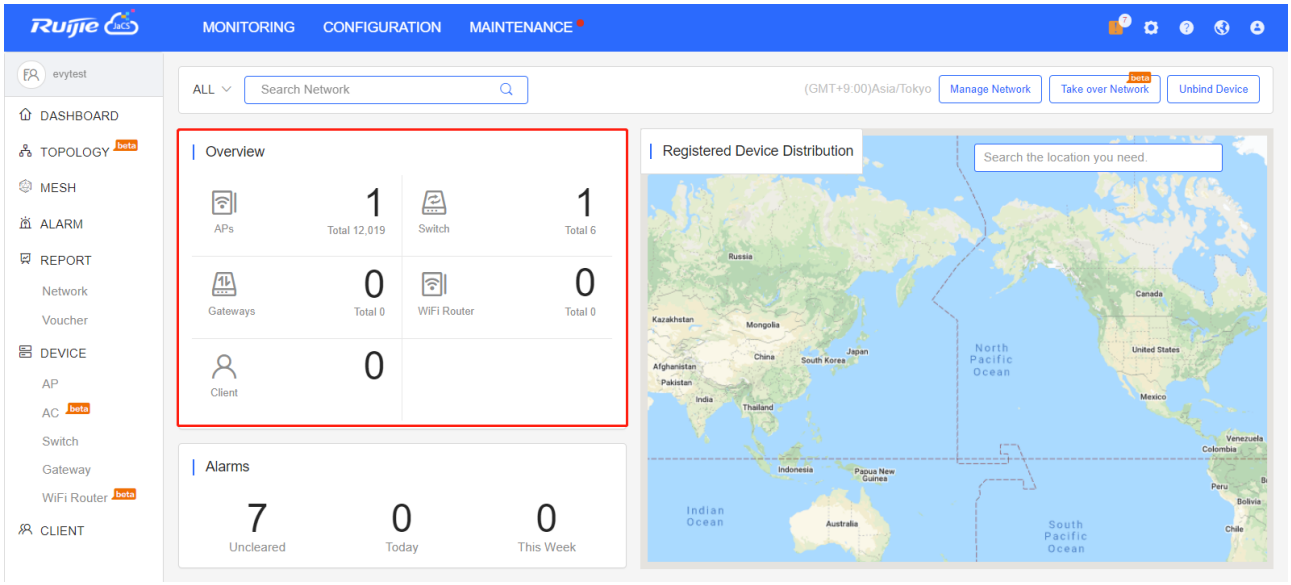
5.1 Dashboard

After logging in, the **Dashboard** appears, or you can click **Dashboard** in the menu to open the page.



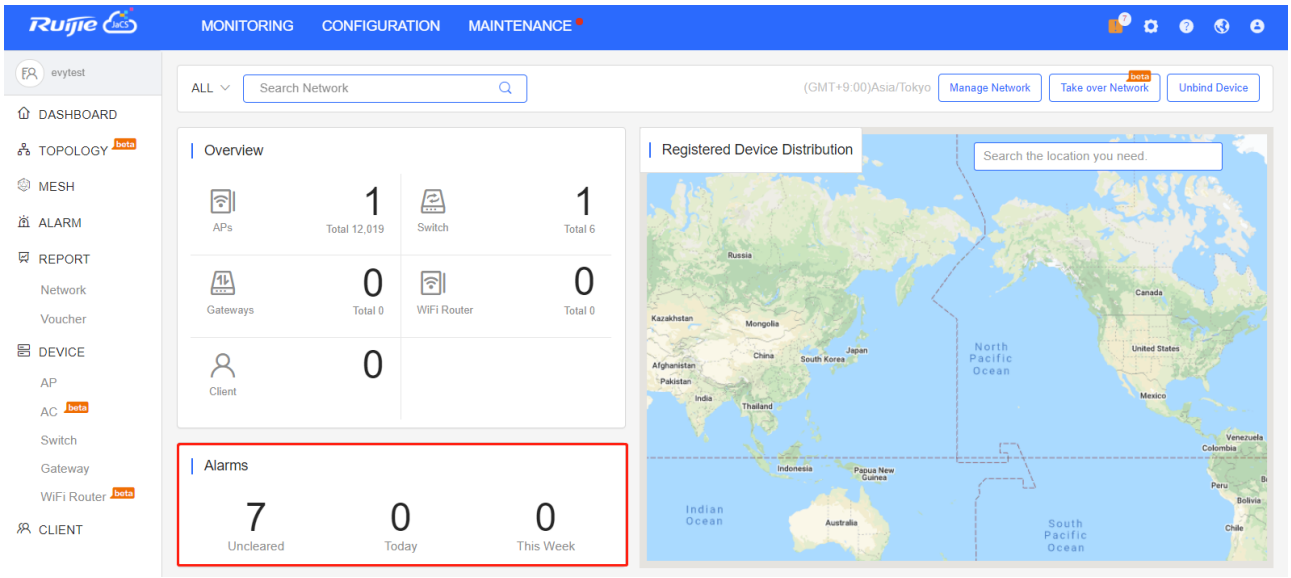
5.1.1 Overview

Overview displays the statistics of APs, switches, gateways and clients and WiFi Router. The upper number indicates the number of online devices, and the lower number indicates the total number of devices.

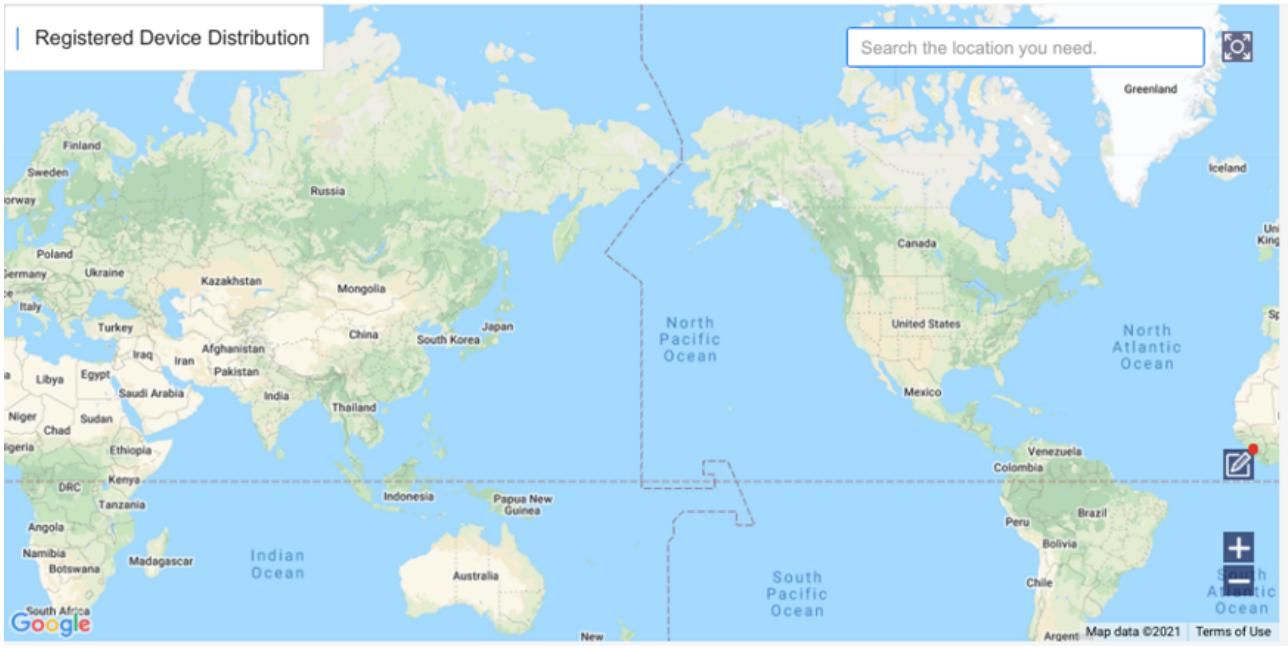


5.1.2 Alarms

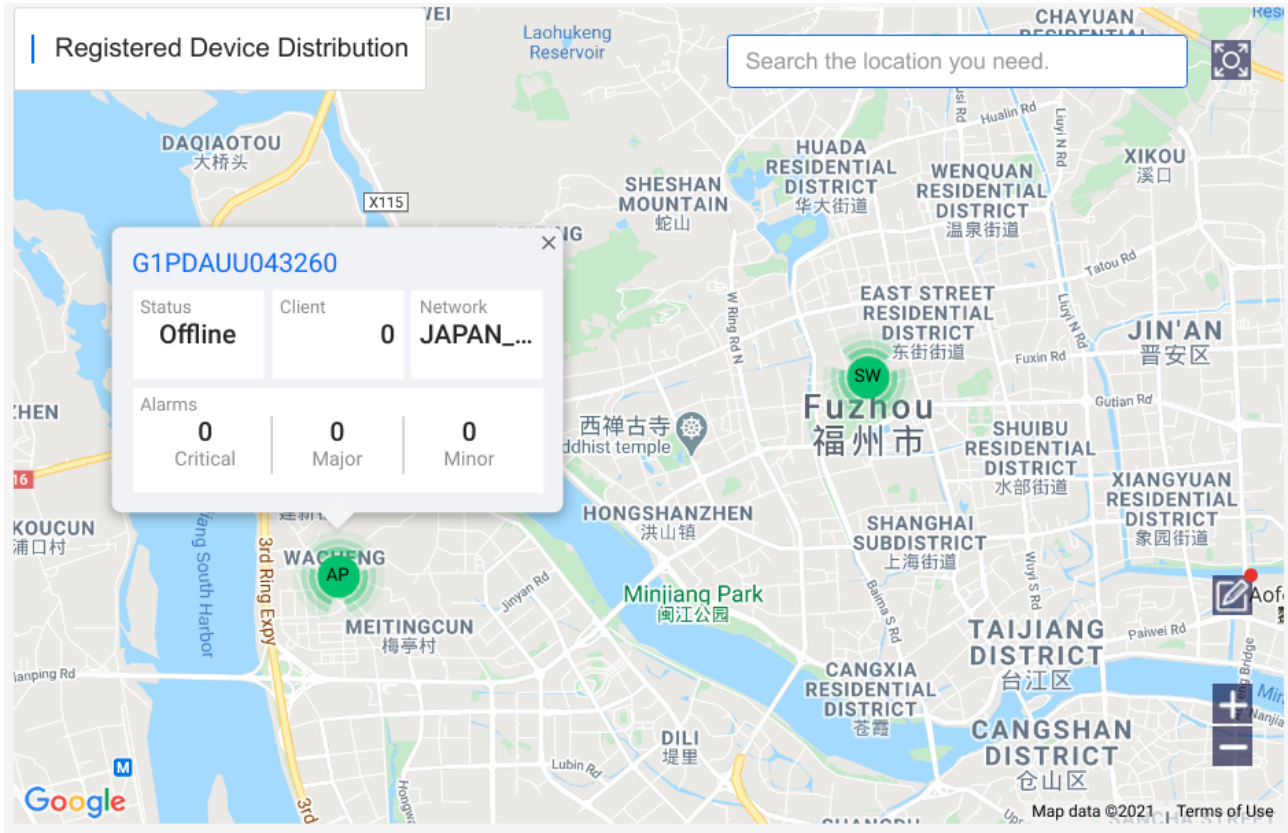
Alarms displays the number of uncleared alarms, new alarms today and total alarms generated this week.



5.1.3 Registered Device Distribution



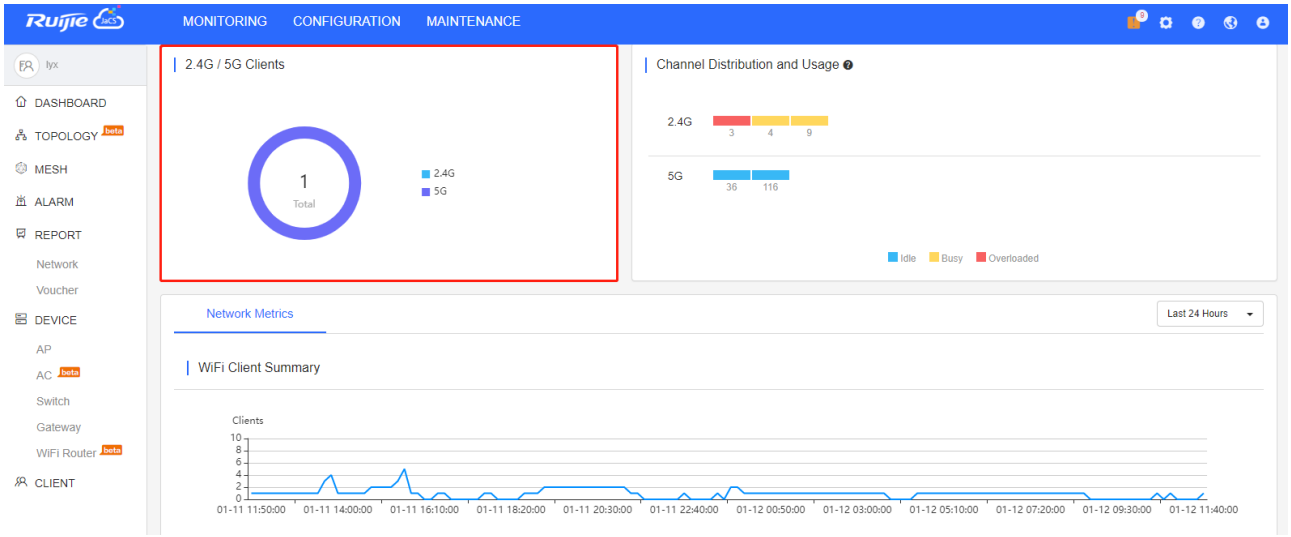
The map displays the device distribution by default. Devices are displayed in network, and the number on icon indicates the device number. Point to the icon, and the device and alarm number are displayed.



Click  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.

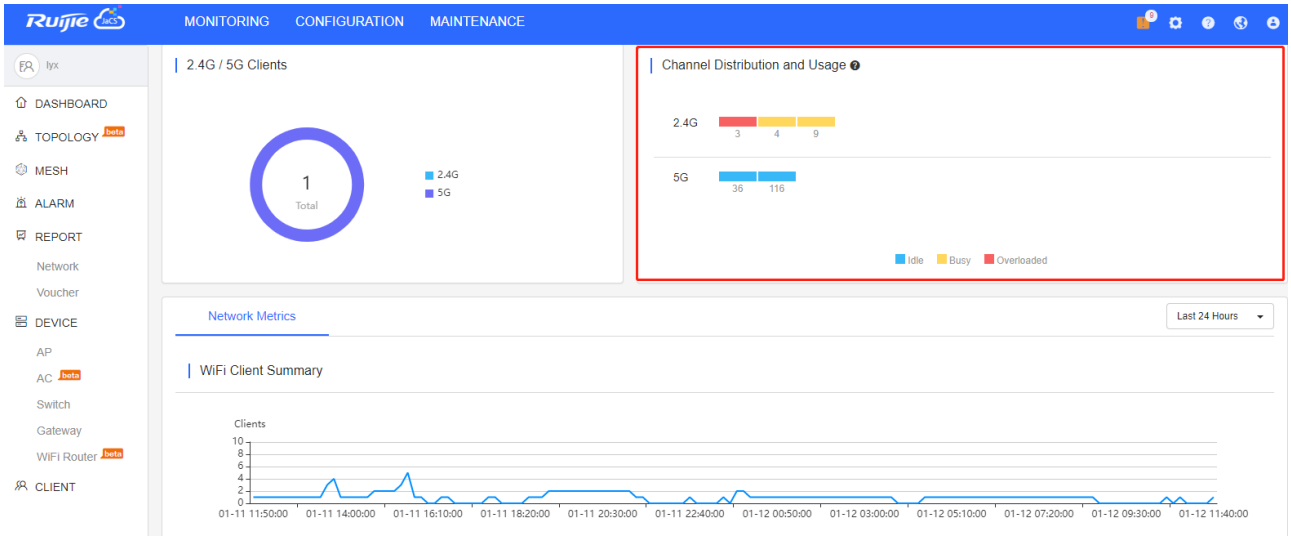
5.1.4 2.4G / 5G Clients

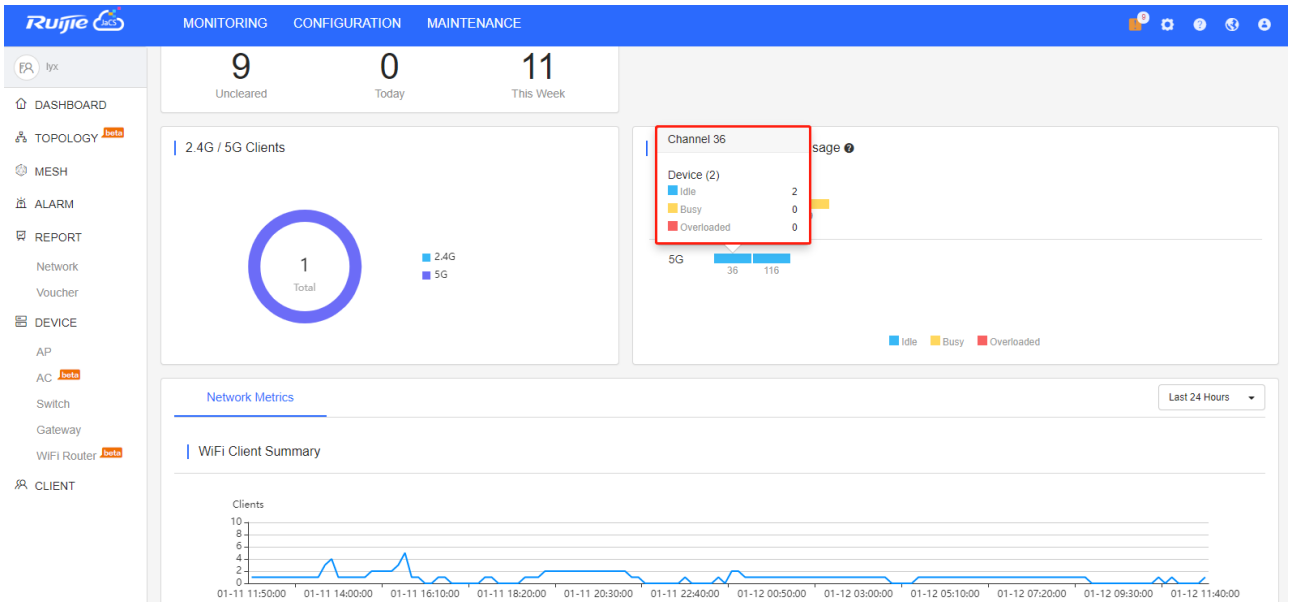
The chart displays the statistics of clients using 2.4G and 5G.



5.1.5 Channel Distribution and Usage

The chart displays the channel statistics.





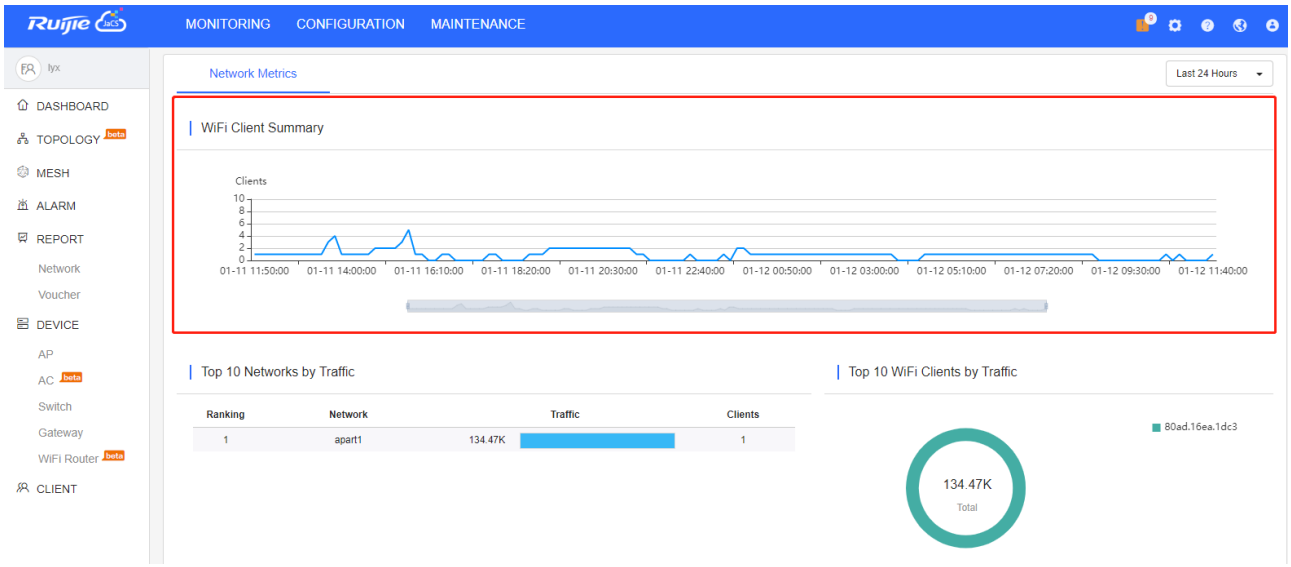
Point to a channel, and more details appear. The channel usage is graded as:

Idle: 0% to 59%

Busy: 60% to 79%

Overload: 80% to 100%

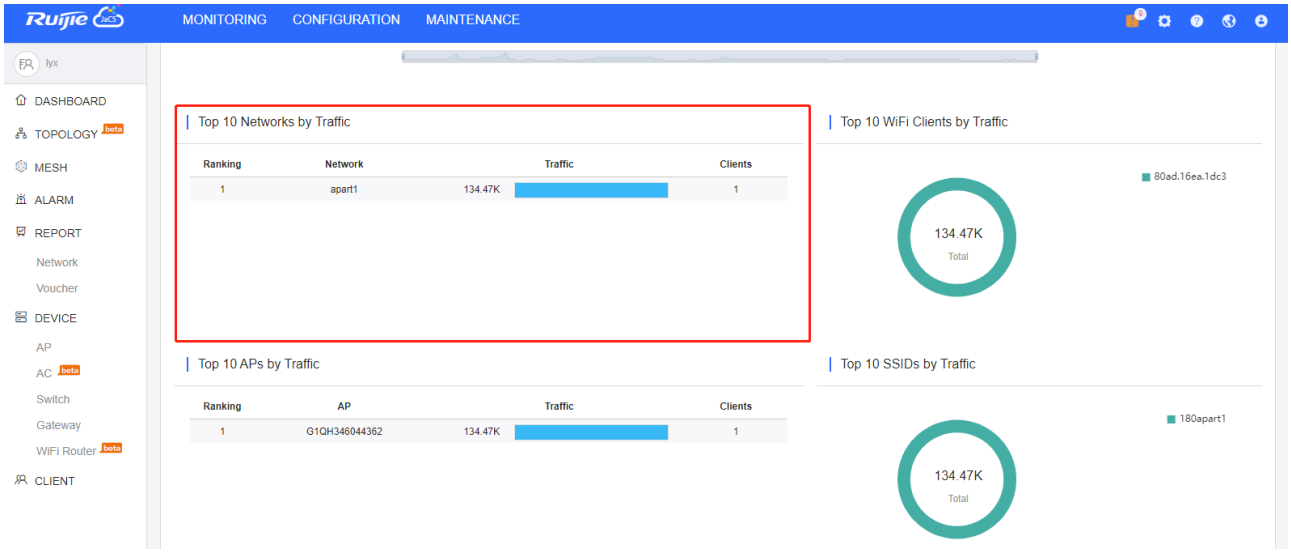
5.1.6 Client Summary



The chart displays the trend of recent clients.

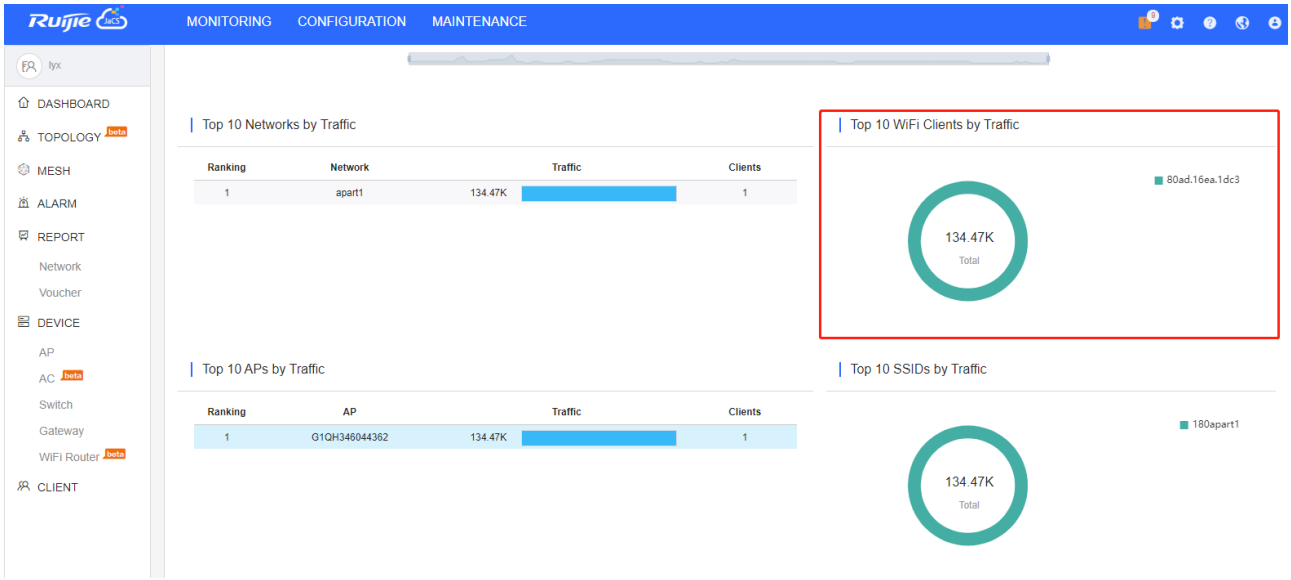
5.1.7 Top 10 Networks by Traffic

The table displays the top 10 networks ranked by traffic.



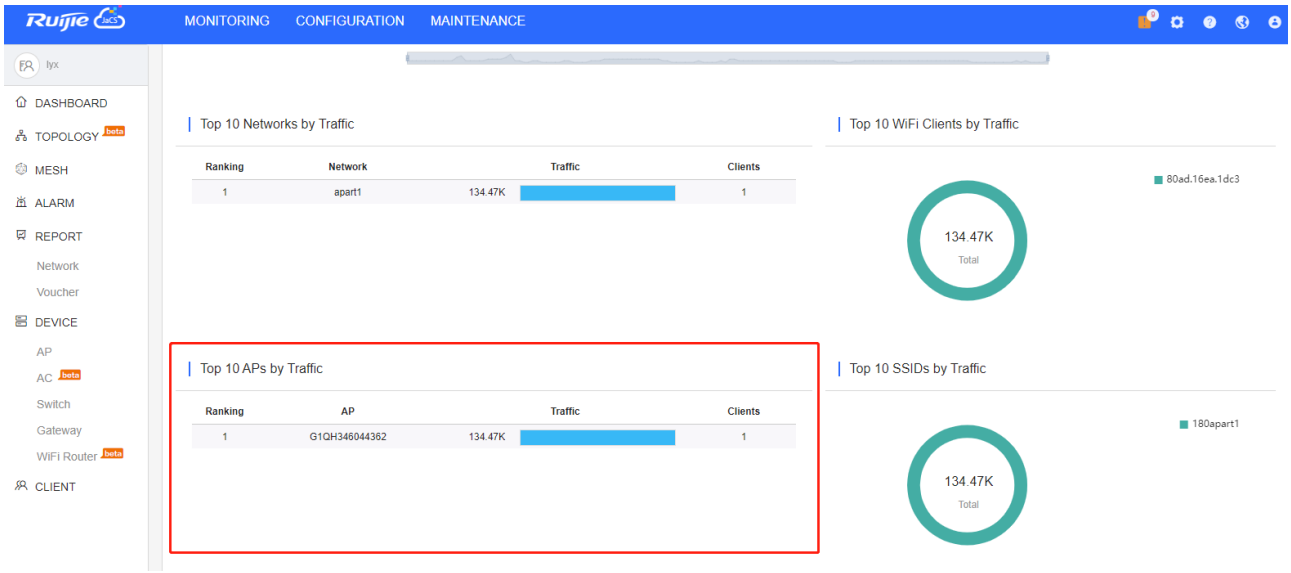
5.1.8 Top 10 Clients by Traffic

The chart displays the top 10 clients ranked by traffic.



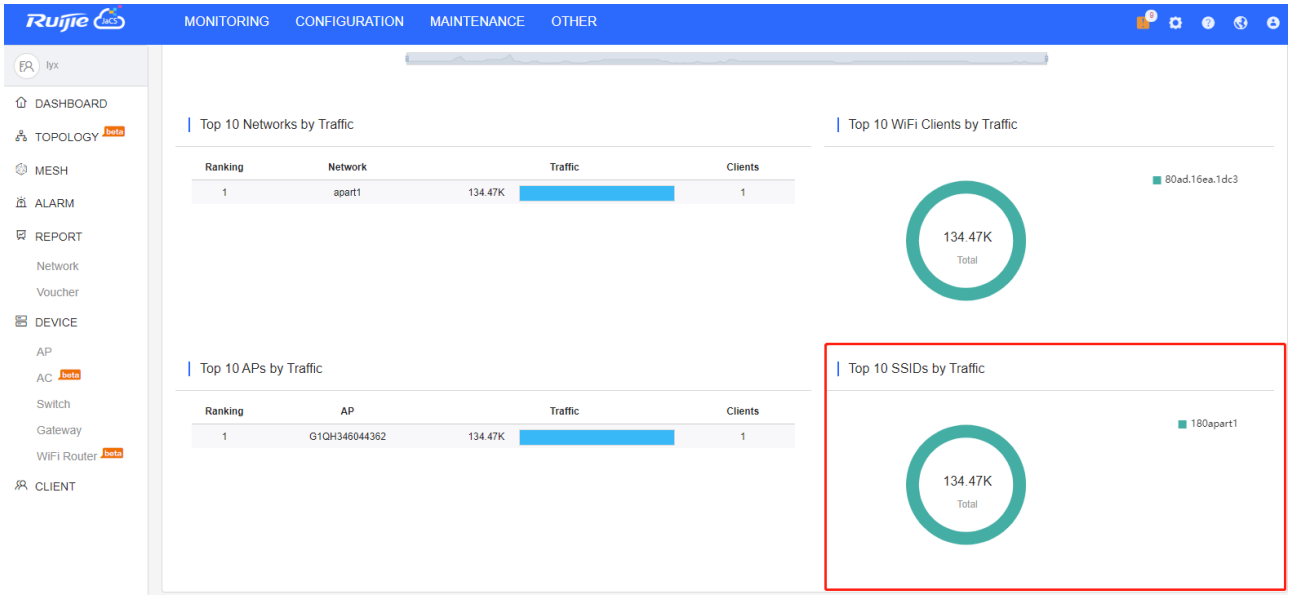
5.1.9 Top 10 APs by Traffic

The table displays the top 10 APs based on traffic.



5.1.10 Top 10 SSIDs by Traffic

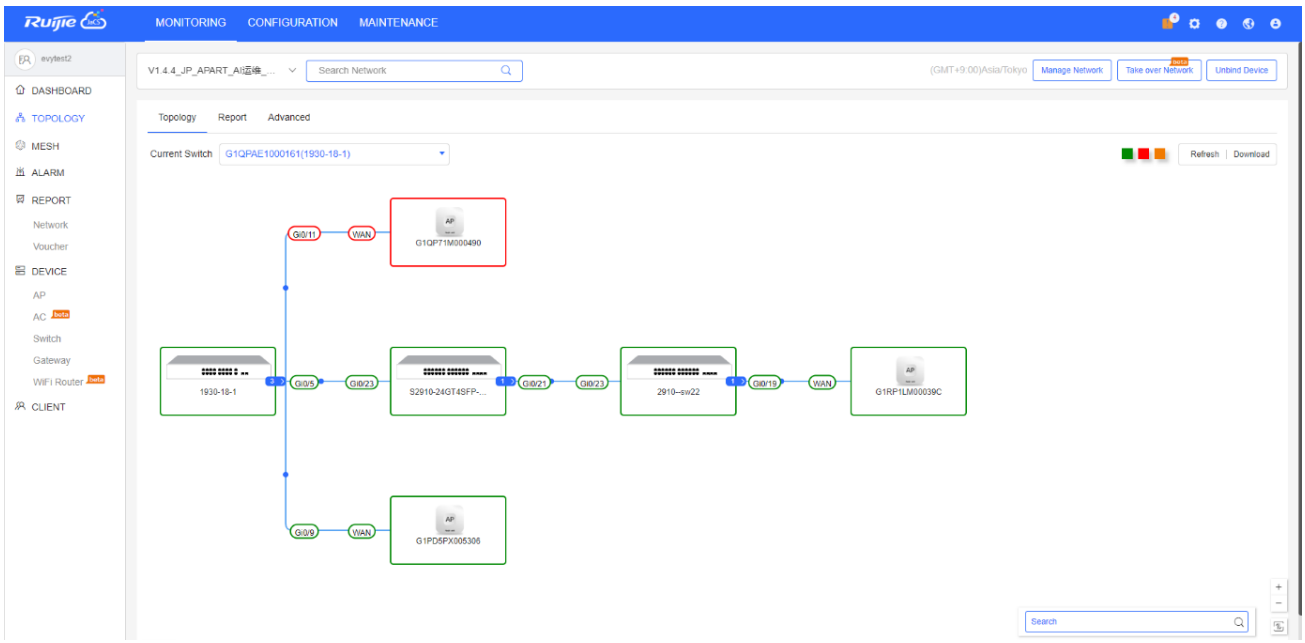
The chart displays the top 10 SSIDs based on traffic.



5.2 Topology

Topology page displays the topology of the downlink devices of an online switch in the current network. It supports to diagnose the running status of all online networks in a network, and generate diagnosis report.

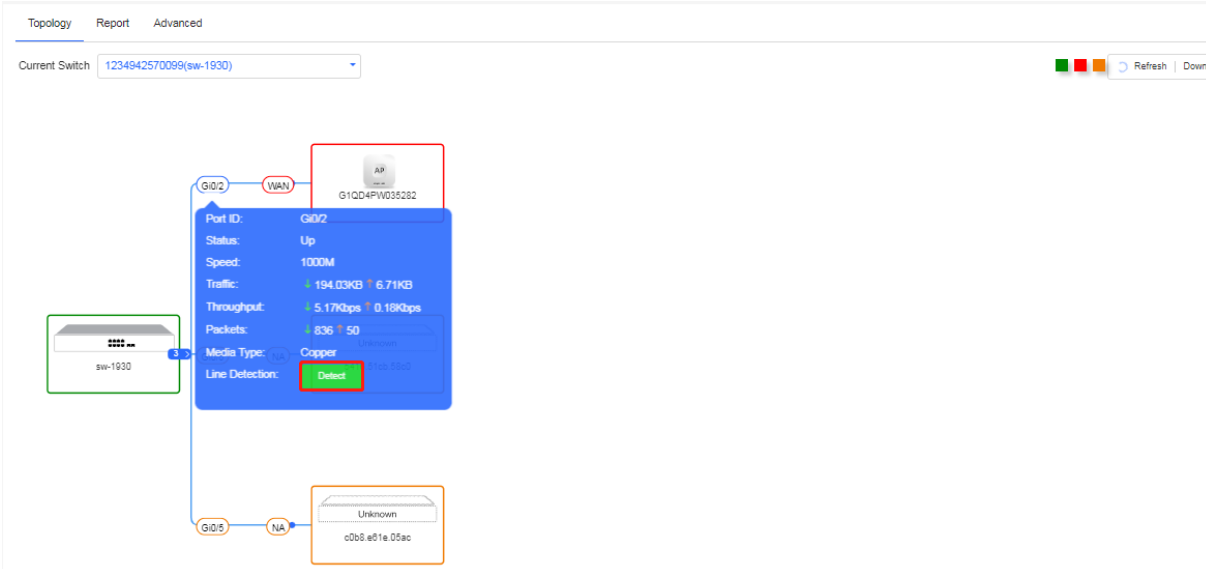
5.2.1 Topology



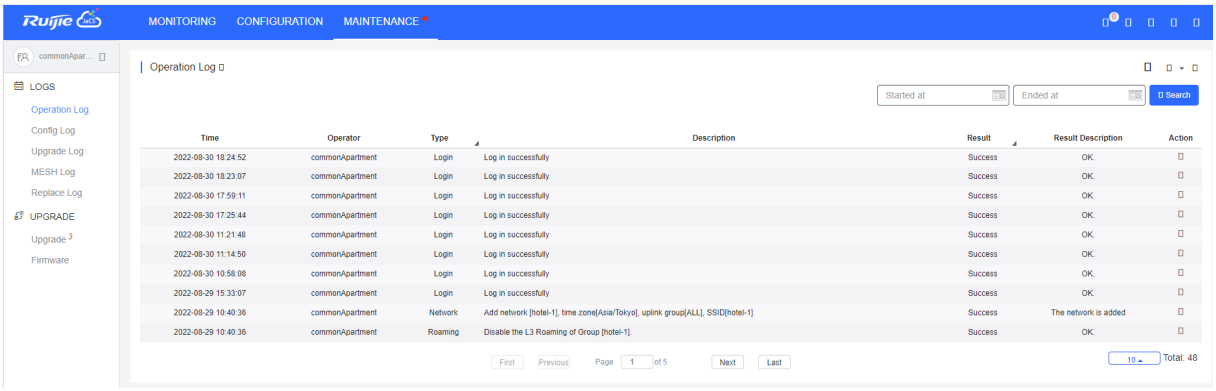
- **Current Switch:** You can select a switch in the current network group to display the topology of its downlink devices.
- **Search:** You can use a device SN or device name to search the device in the topology and check its information.
- Different colors indicate different connection status. Green indicates the device works normally. Red indicates the device goes offline or is disassociate from the switch. Orange indicates the device is not connected to the Cloud or it belongs to another account.
- **Refresh:** You can select a switch, and click **Refresh** to update the downlink topology of the switch. The fresh interval should be more than 10 minutes, otherwise a prompt message about frequent operations will appear. A topology update will be triggered when a switch is initially selected.

5.2.2 Physical Link Detection

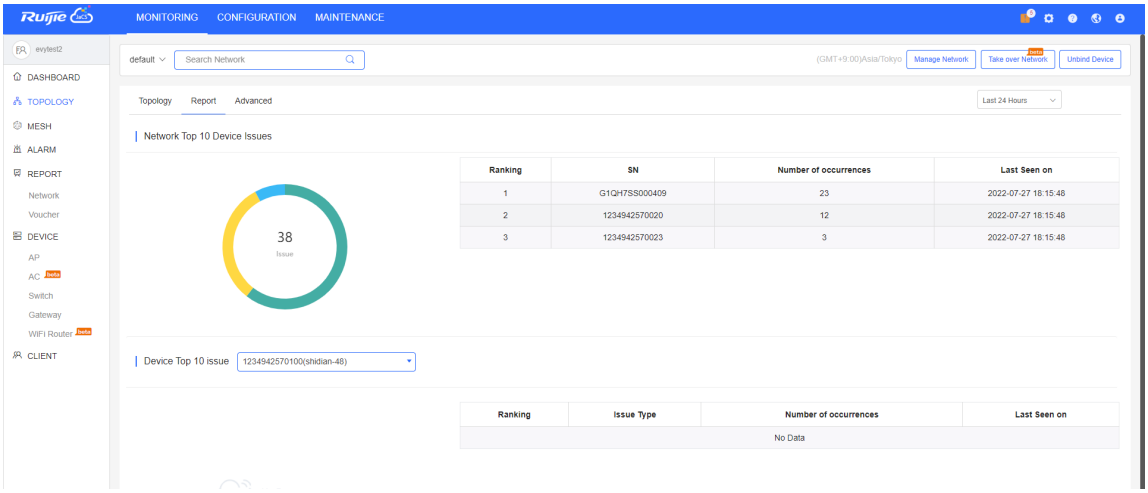
In a topology, when you hover the mouse over a switch, the detail information of the switch will be displayed in a pop-up window. In this pop-up window, you can click the **detect** button to detect the status of a link. When the link is under detection, please do not perform any operation. Three results may occur as shown follows, including normal link, link failure and no link.



After completing the operation, you can click **MAINTENANCE** > **LOGS** > **Operation Log** to check the log.



5.2.3 Report



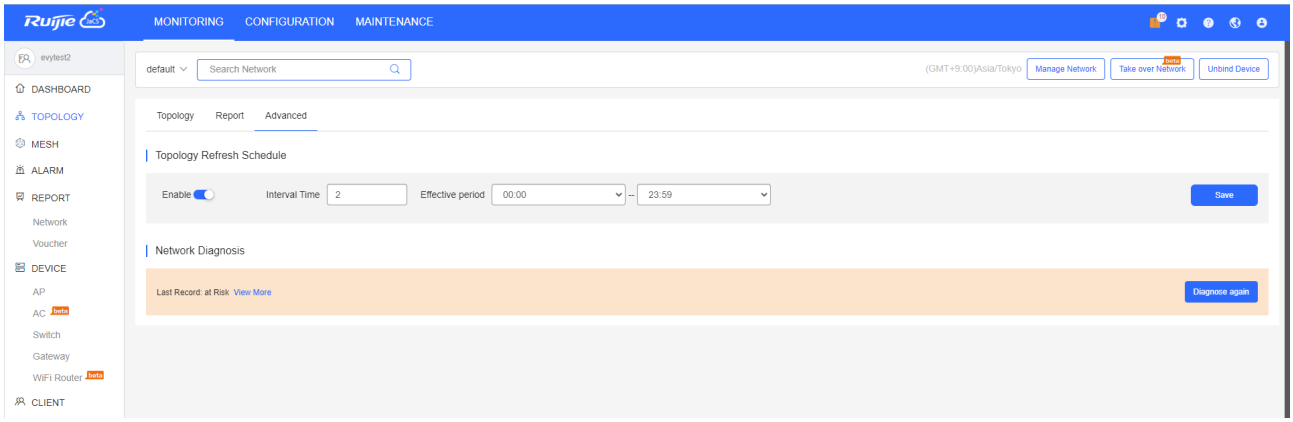
- Network Top 10 Device Issues

  This chart displays the top 10 faulty devices and the last time when the fault occurs in a network.

- Device Top 10 issue

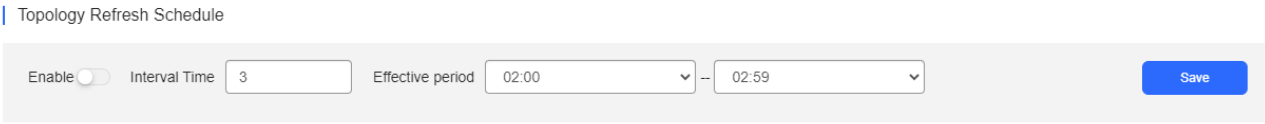
This chart displays the top 10 failure types occurring among devices and the last time when the fault occurs. You can hover the mouse over a failure to check the details.

5.2.4 Advanced

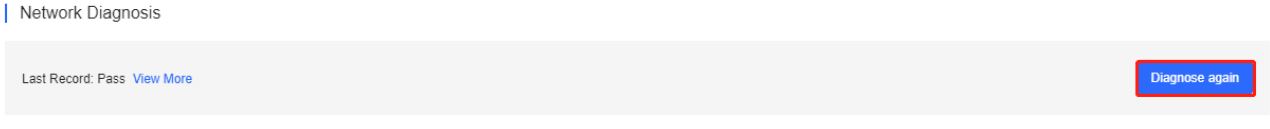


5.2.4.1 Topology Refresh Schedule

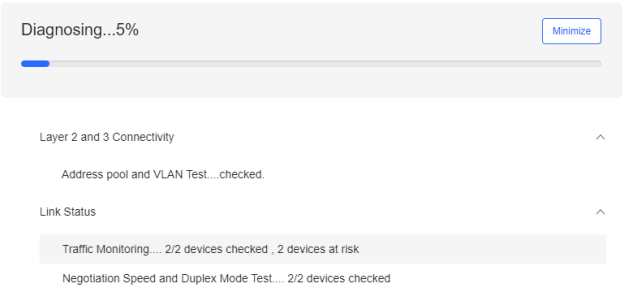
In this page, you can set the time to refresh the topology. The min interval is 2 hours. You also can set a period to refresh the topology. At the start time, the topology will be refreshed once only. If the interval between the start time and the end time is less than 2 hours, the topology will be refreshed only at the start time. If you disable this function, all the settings become invalid.

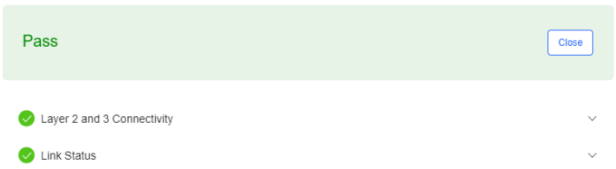


5.2.4.2 Network Diagnosis

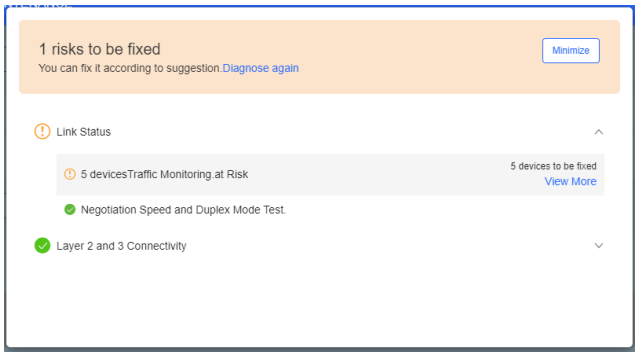


When you click Diagnose again, the following figures will be displayed.

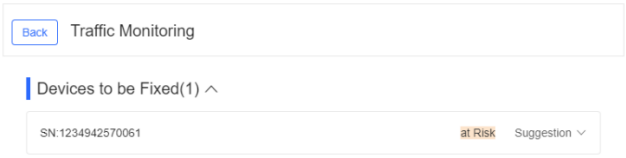




If a risk is detected, the following page will appear.



You can click **View More** to check the details of the risk.



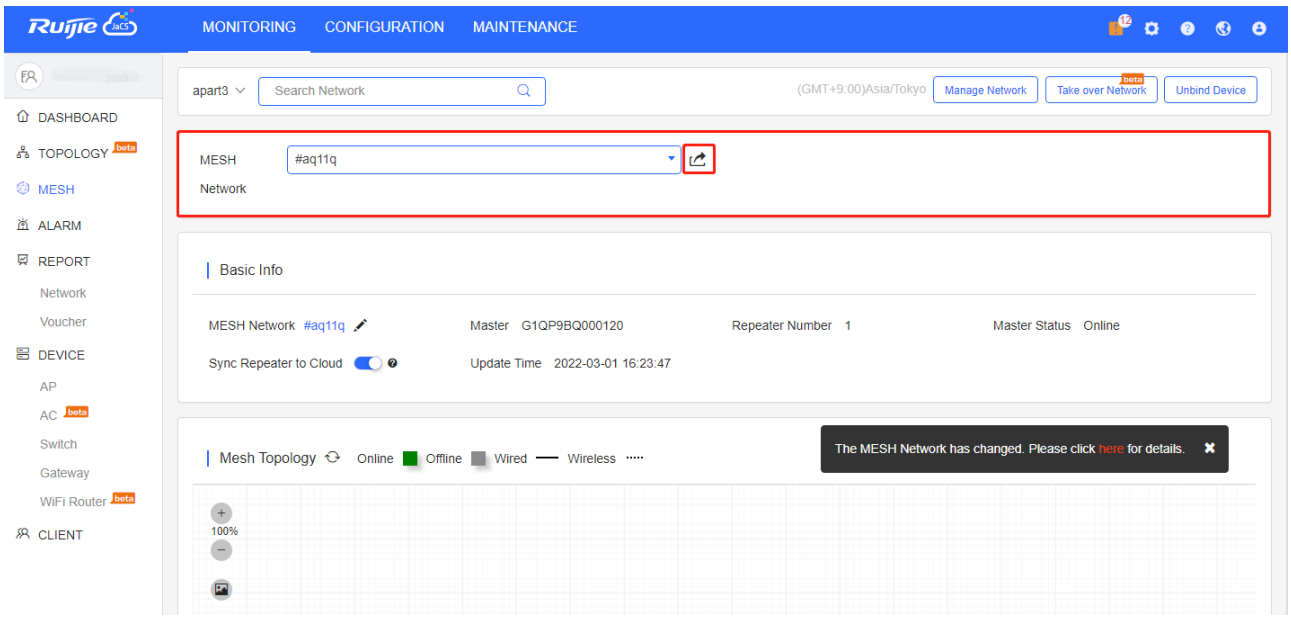
Click **Suggestion**, a suggestion will be offered to help you fix the issue.

5.3 Mesh

Mesh consists of three parts: **Mesh Network**, **Basic Info** and **Mesh Topology**.

5.3.1 Mesh Network

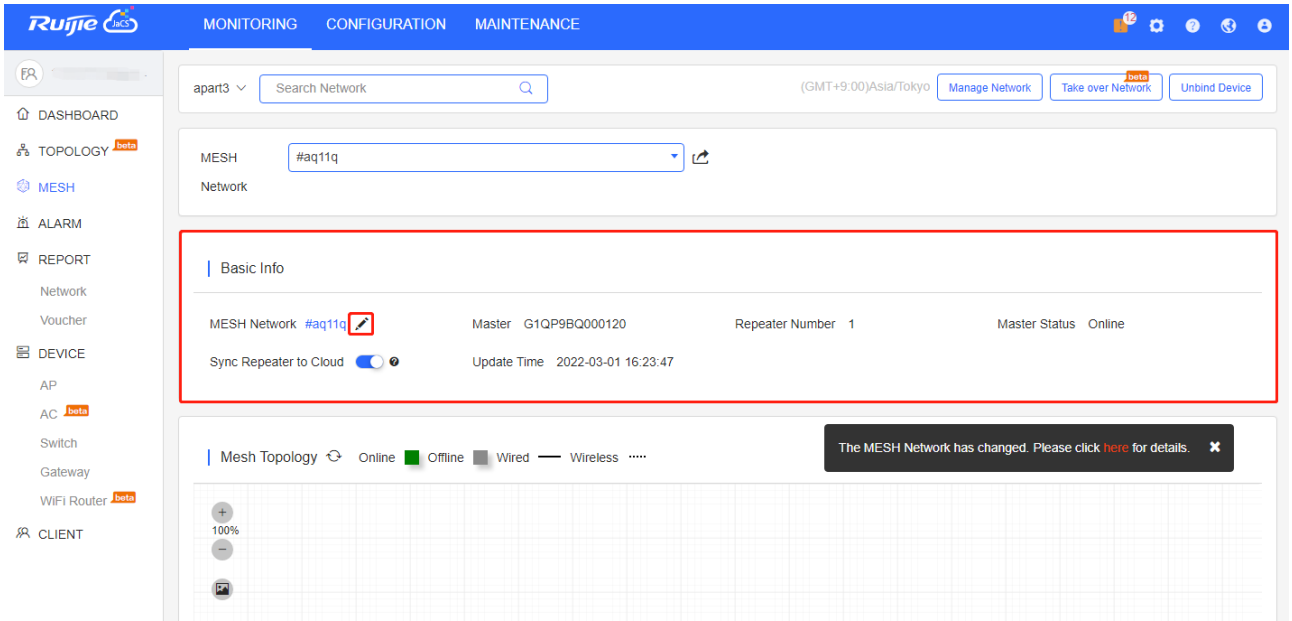
Select the specified Mesh network in the **Mesh Network** box, and click to export the network report.



5.3.2 Basic Information

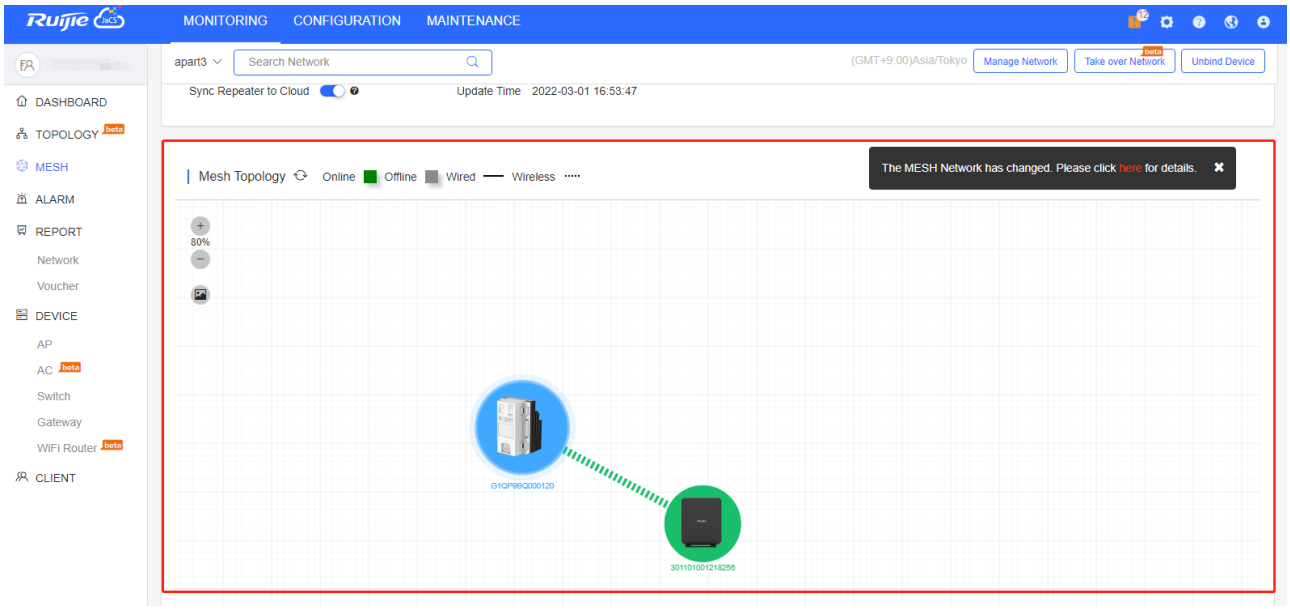
The basic information of Mesh network includes network name, SN of master device, quantity of repeaters, status of master device, and update time. You can enable/disable the function of automatically syncing repeaters to Ruijie JaCS.

To edit the network name, click .

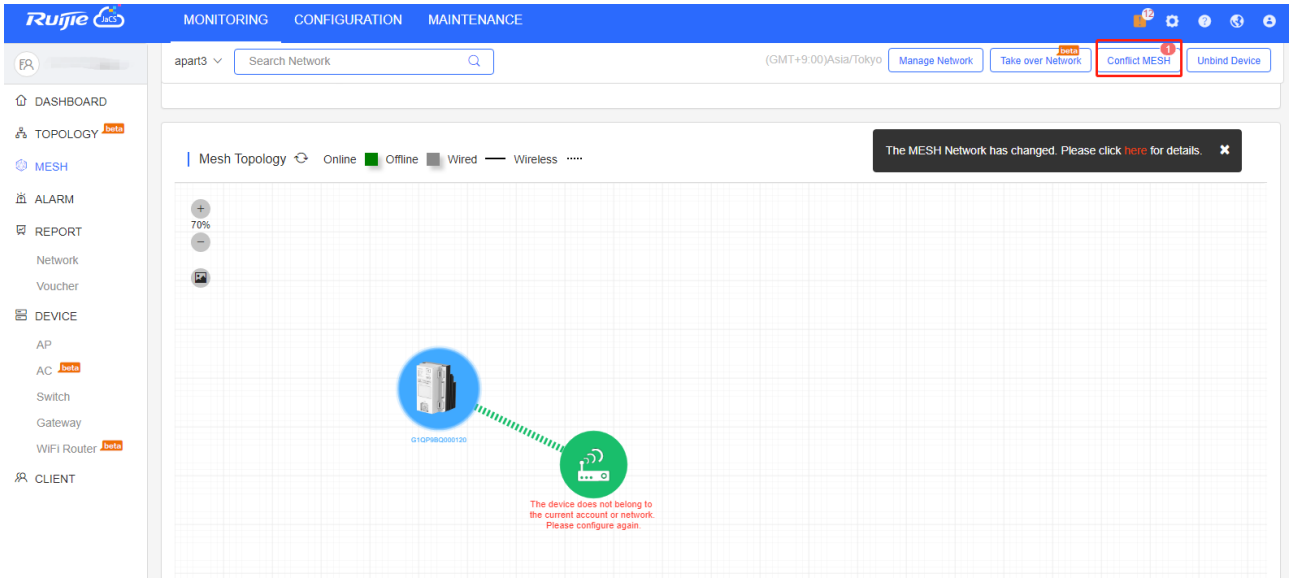


5.3.3 Mesh Topology

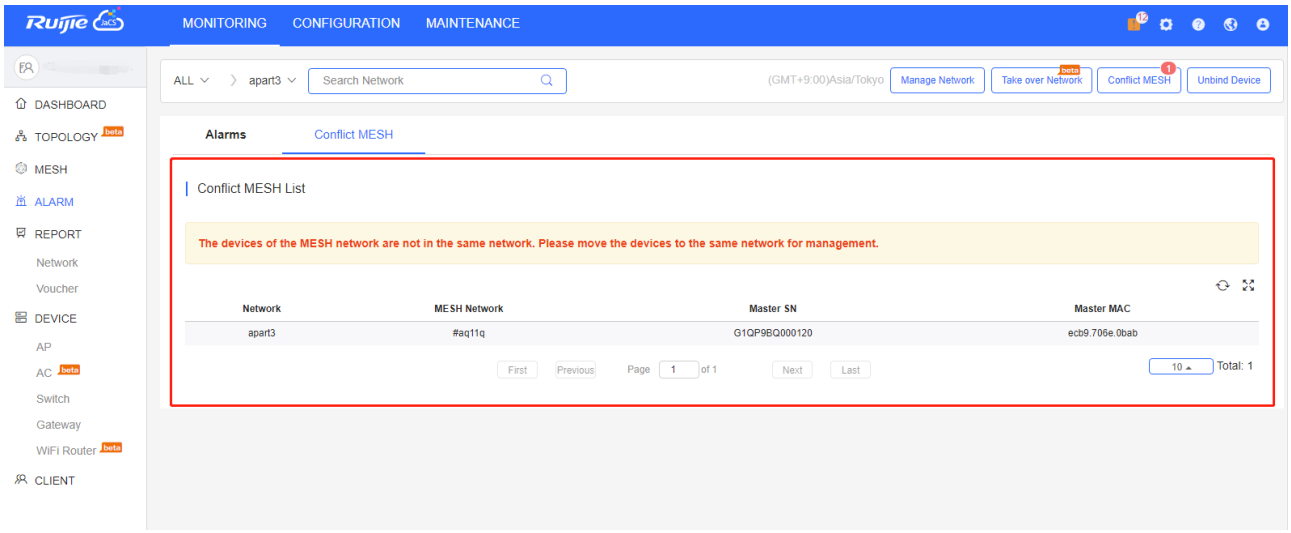
The **Mesh Topology** displays the current Mesh topology, including the information of devices and clients. If the topology changes, a prompt will be displayed and you can click the prompt to open the **Mesh Log** page.



If a device in the Mesh network does not belong to the current network or its sub-networks, the topology will be displayed as below:

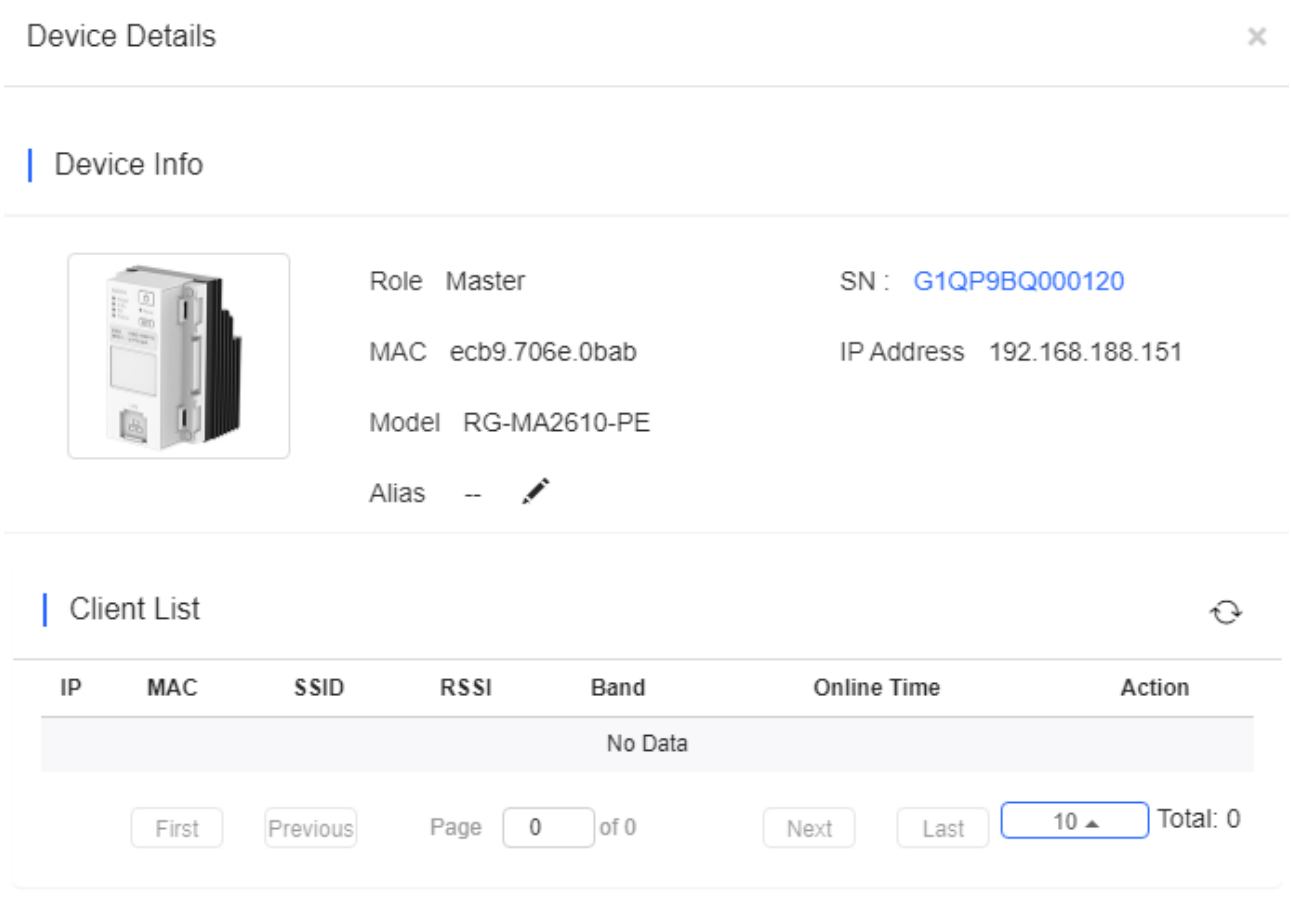


Click  to check the conflict Mesh network.

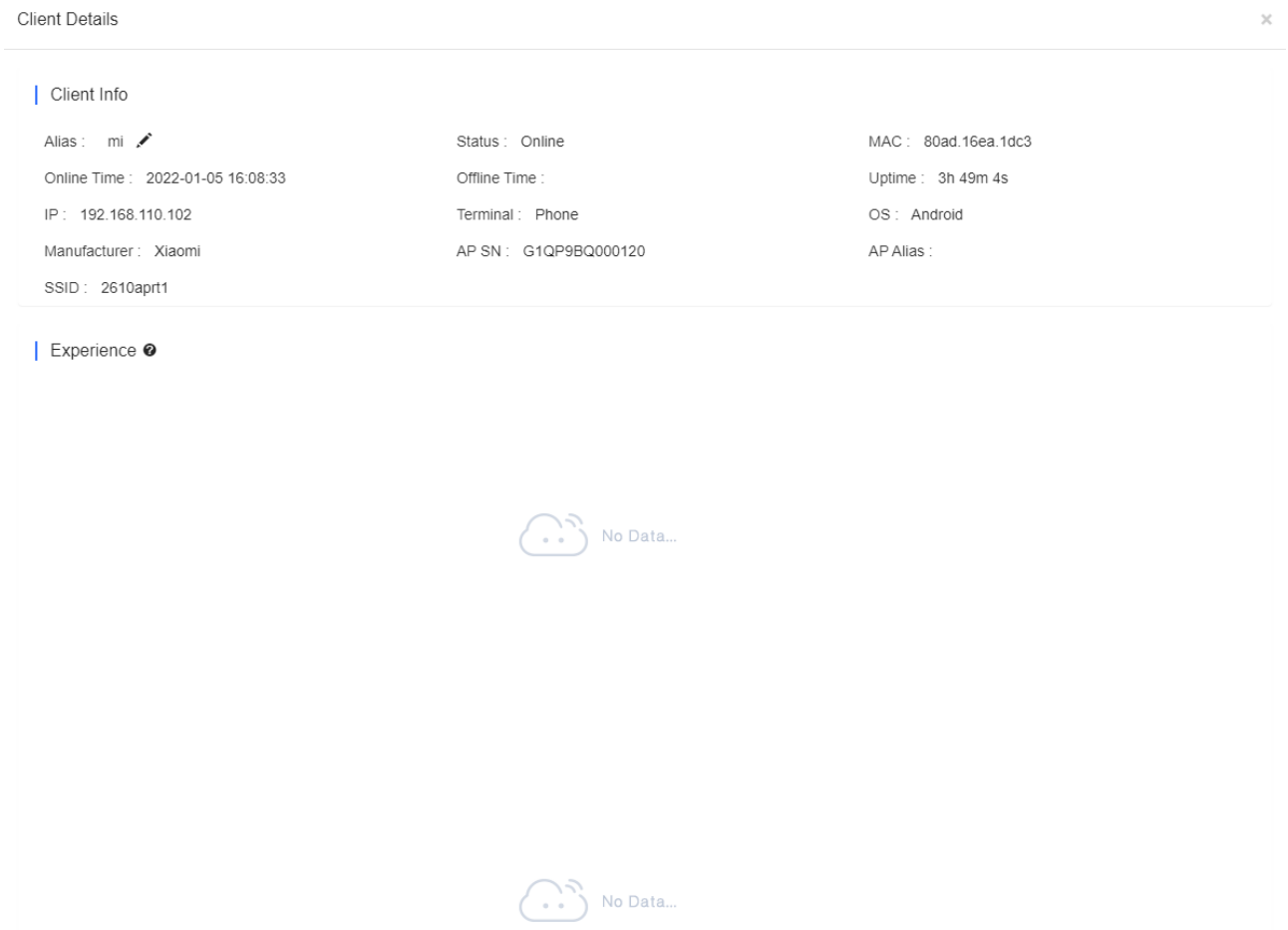


Only after the devices are added to the same network, the conflict prompt will disappear.

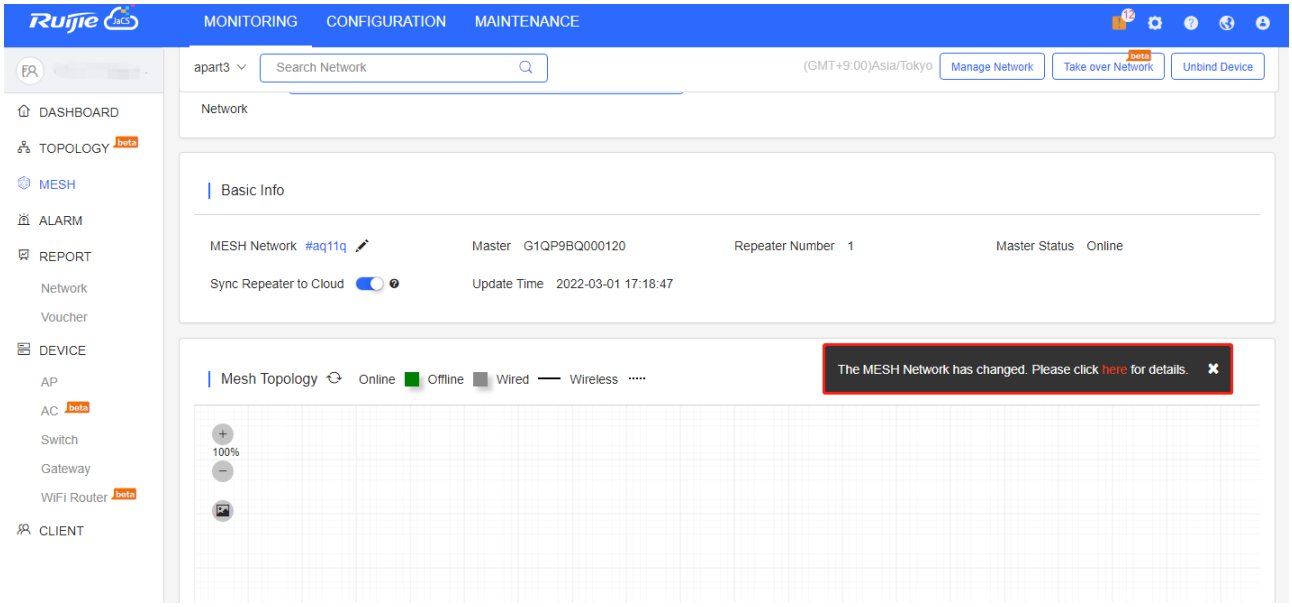
- Click a device, and the device details will be displayed.

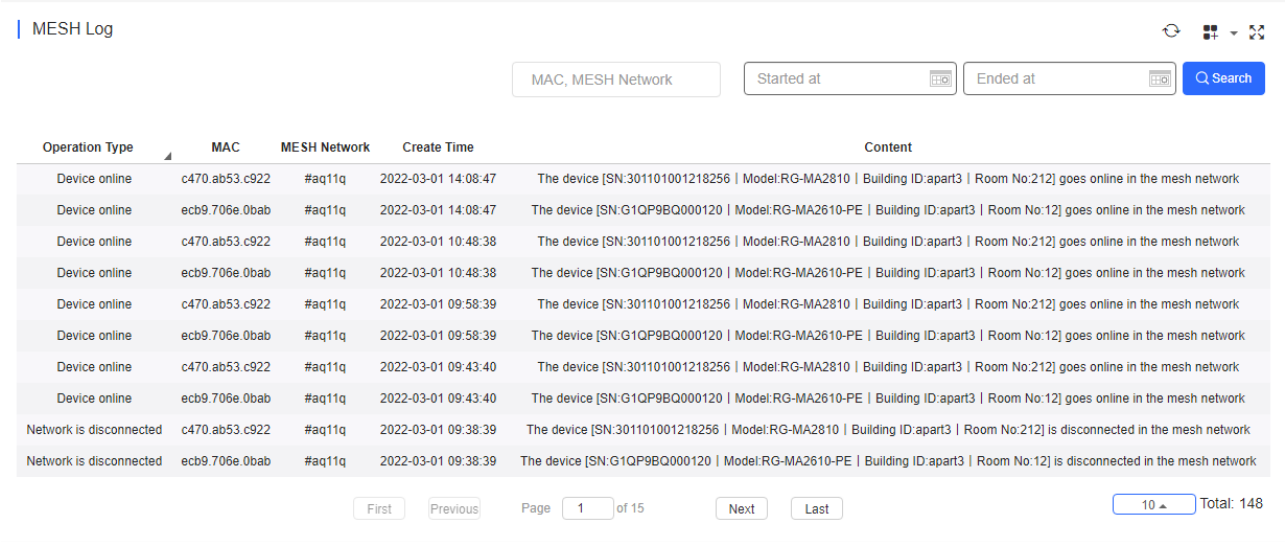


- Click a client, and the client details will be displayed.



- Click here to open the **Mesh Log**.



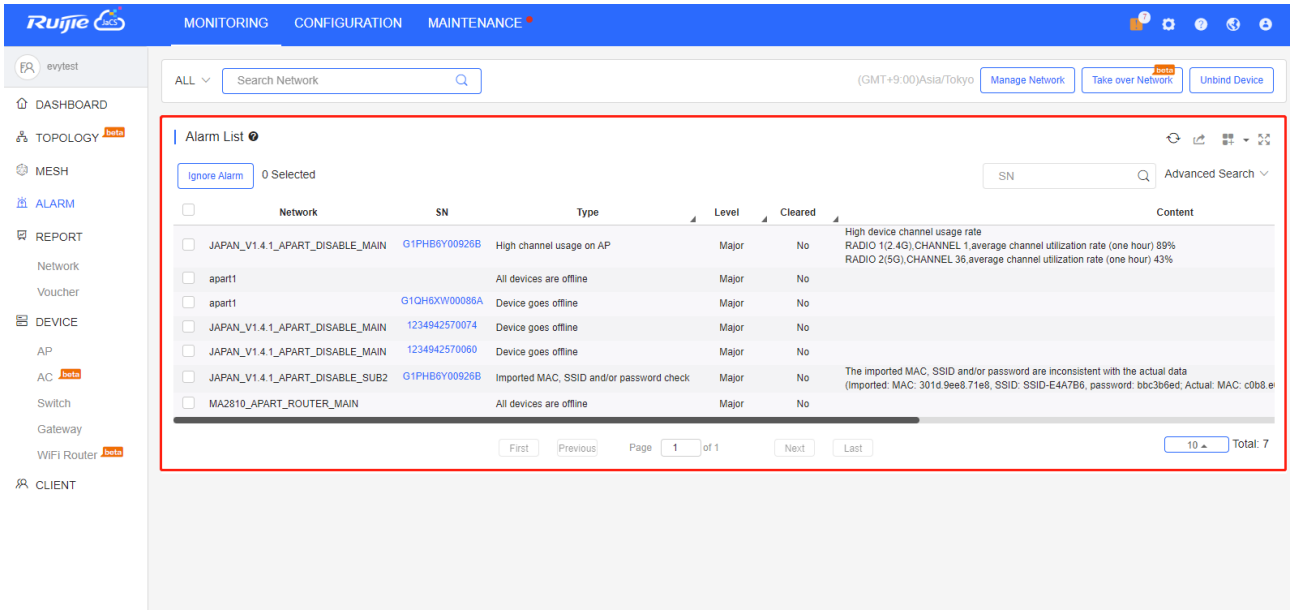


5.4 Alarm

5.4.1 Alarm List

Alarm List displays the cleared alarms. **Alarm List** supports the search based on AP serial number, alarm type, alarm level, alarm generation time and alarm updated time.

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



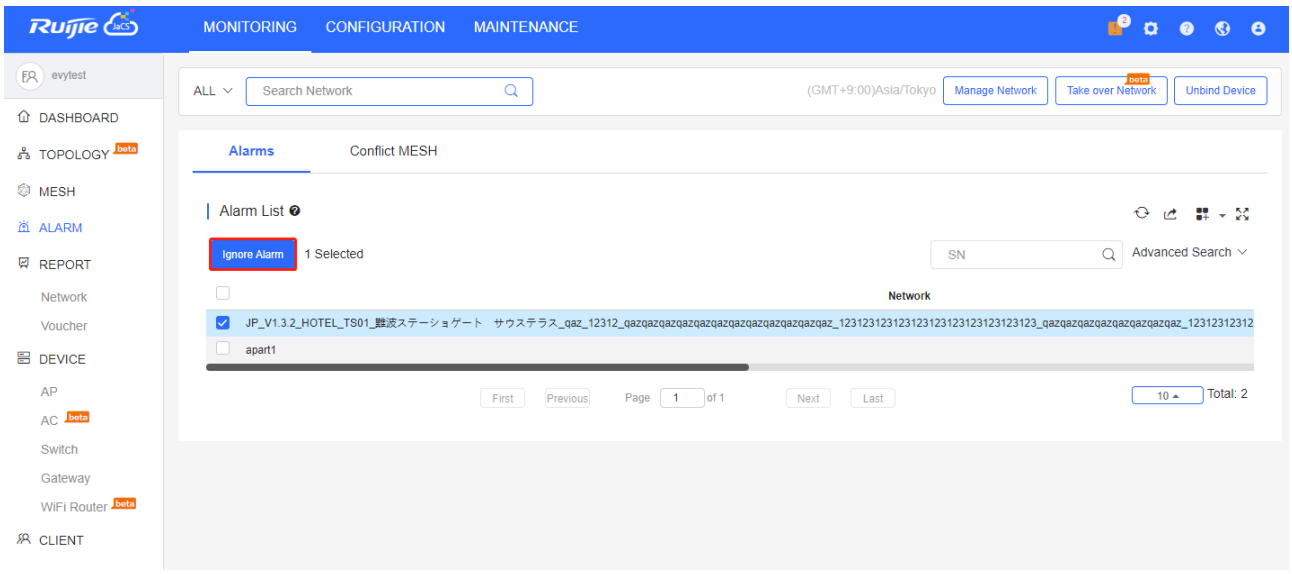
The following describes the conditions for generating alarms.

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 speed 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 speed 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 speed 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.
Imported MAC, SSID and/or password check	Device import	When the imported MAC and the actual MAC are inconsistent, or the SSID/password changes, the alarm is sent.

5.4.2 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.



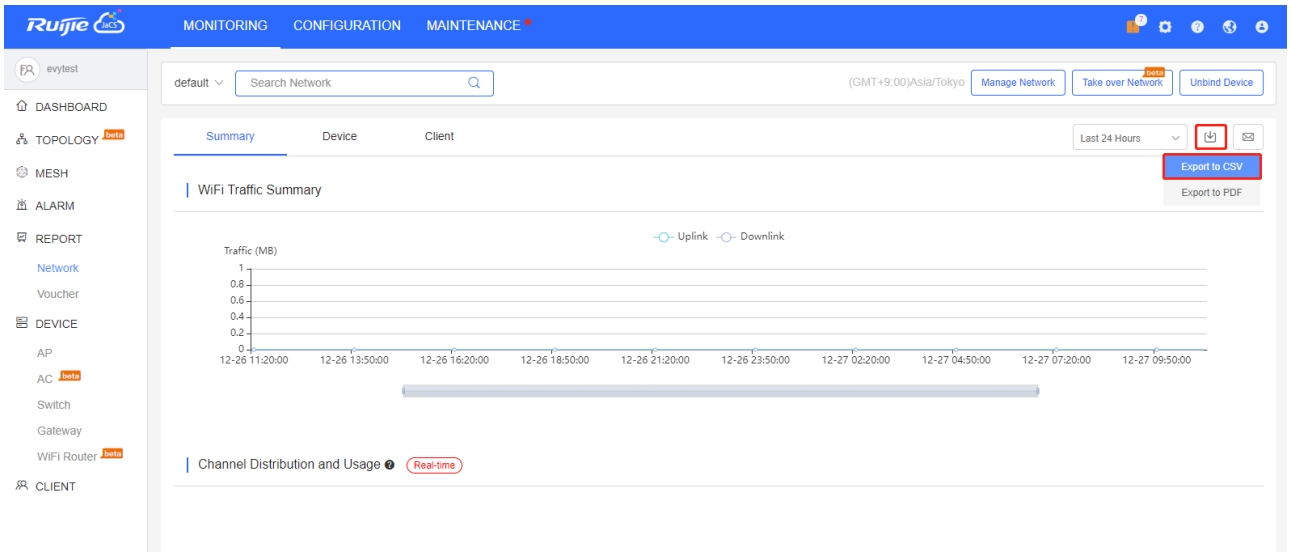
5.5 Report

5.5.1 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 30 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.

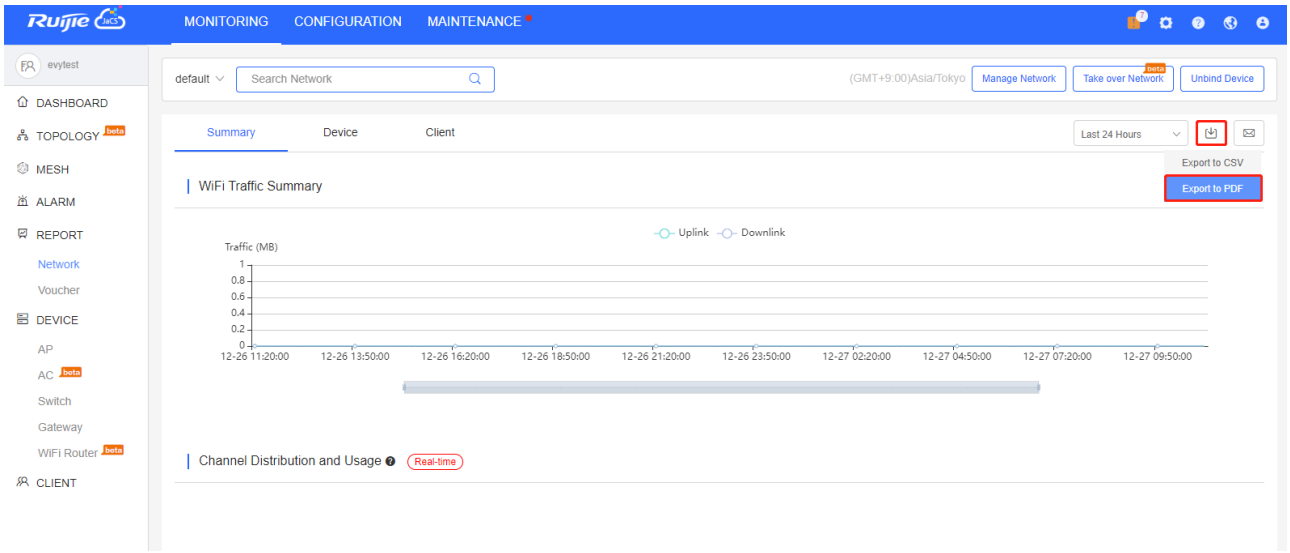
- Export to CSV

Point to , and click **Export to CSV**.



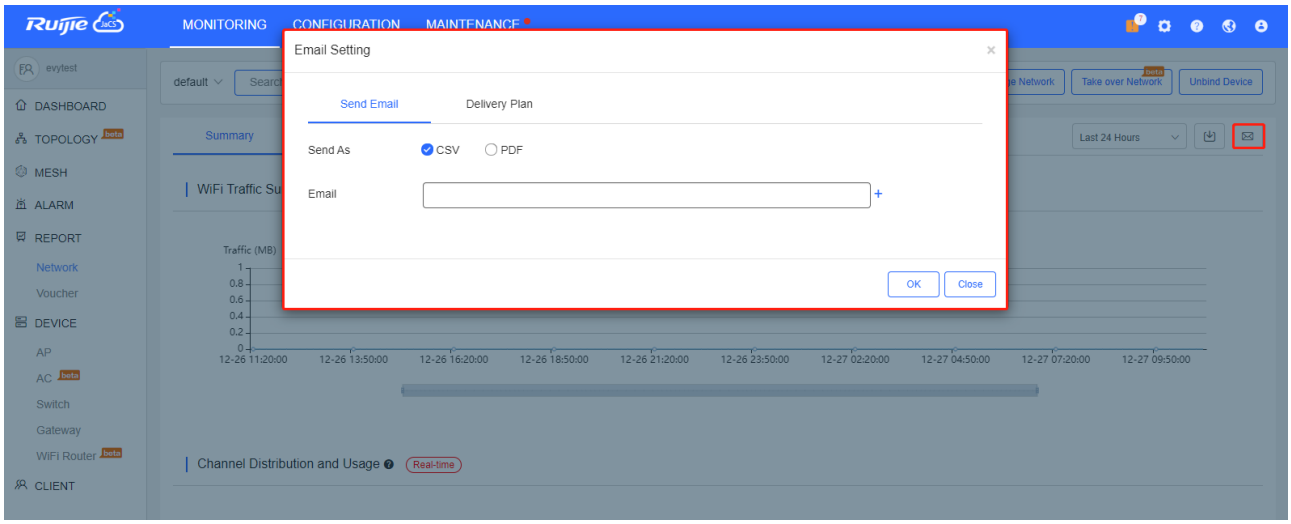
- Export to PDF

Point to , and click **Export to PDF**.



- Mail

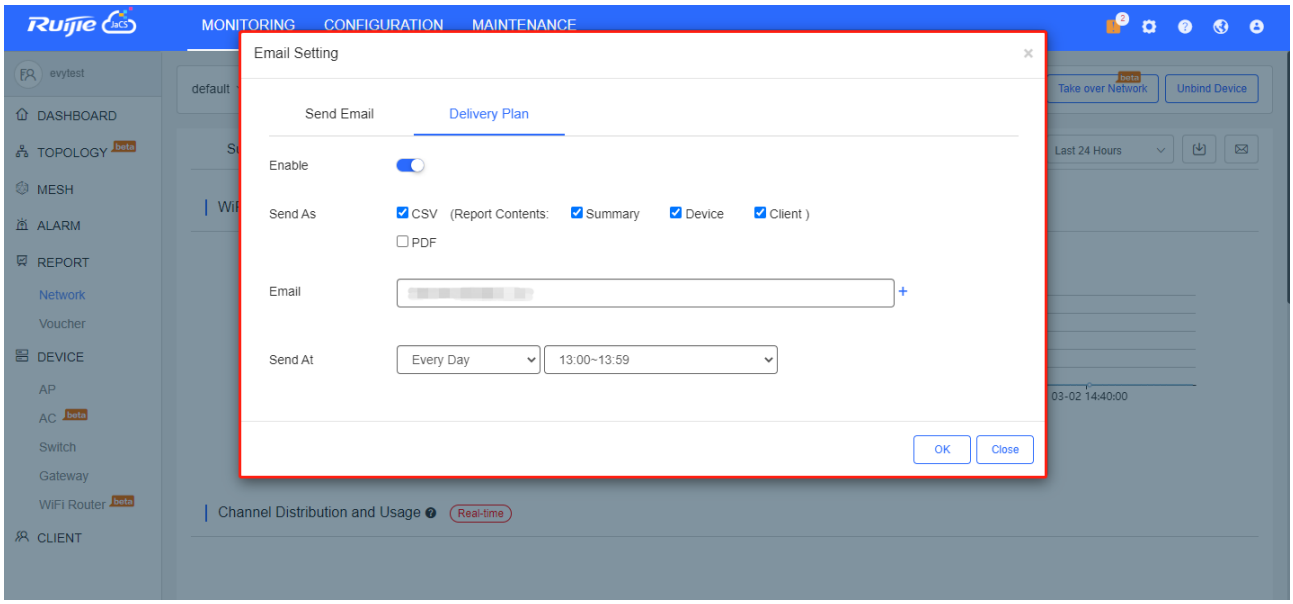
Click  , and select **Send Email**. Choose a file type for the report, then enter Email addresses. After click **OK**, the report will be sent immediately.



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

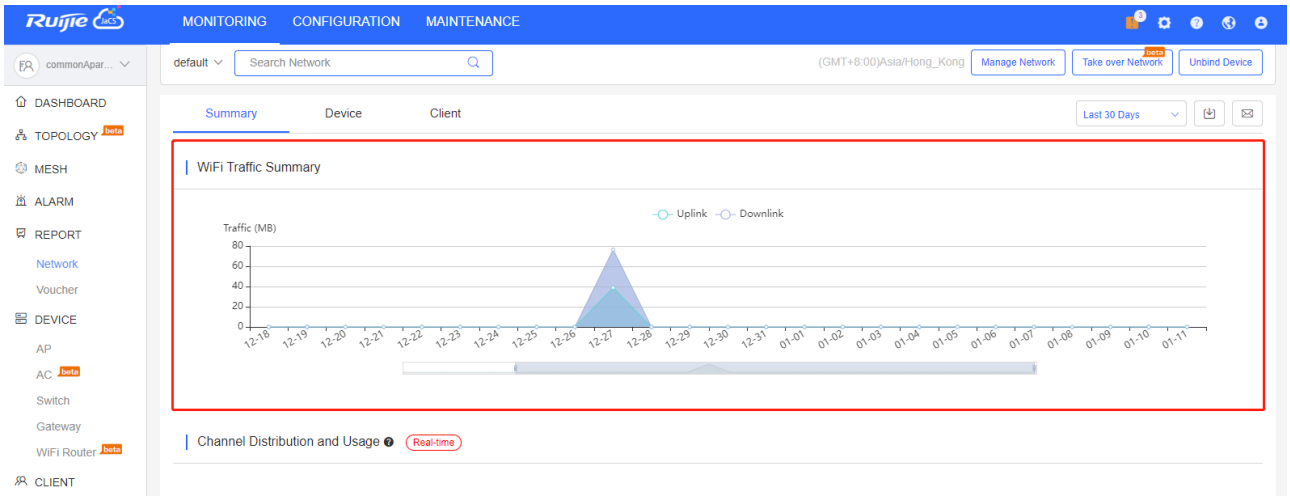
Report includes the data of Summary, Device and Client, and supports CSV and PDF file formats.

Reports can be sent every month, week or day.



Up to three Email addresses are supported.

- Summary > WiFi Traffic Summary

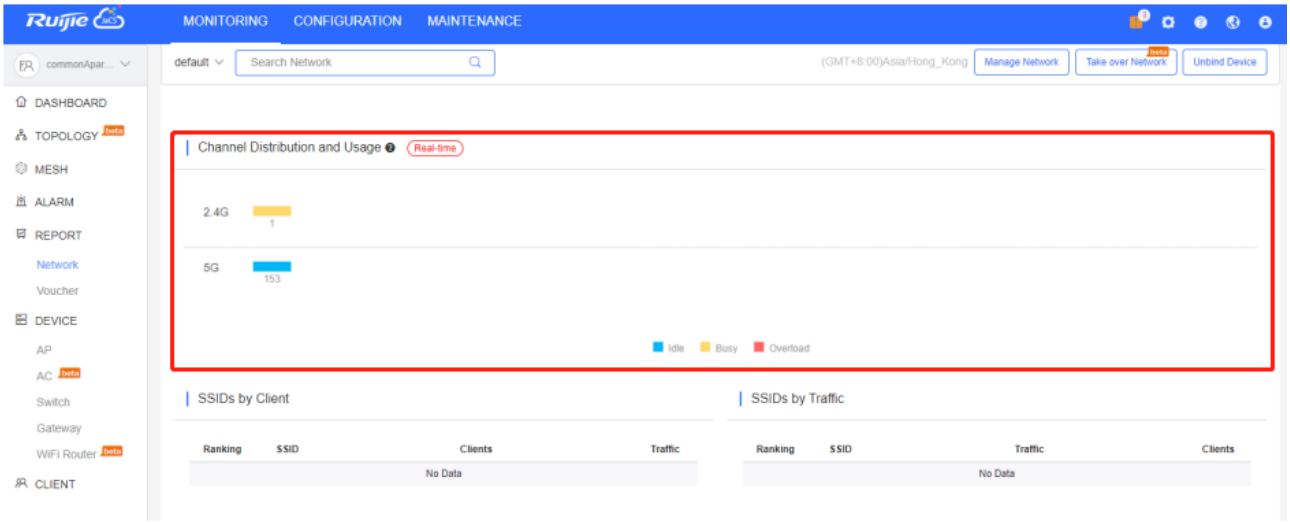


The uplink/downlink traffic summaries of the selected network during the specific period.

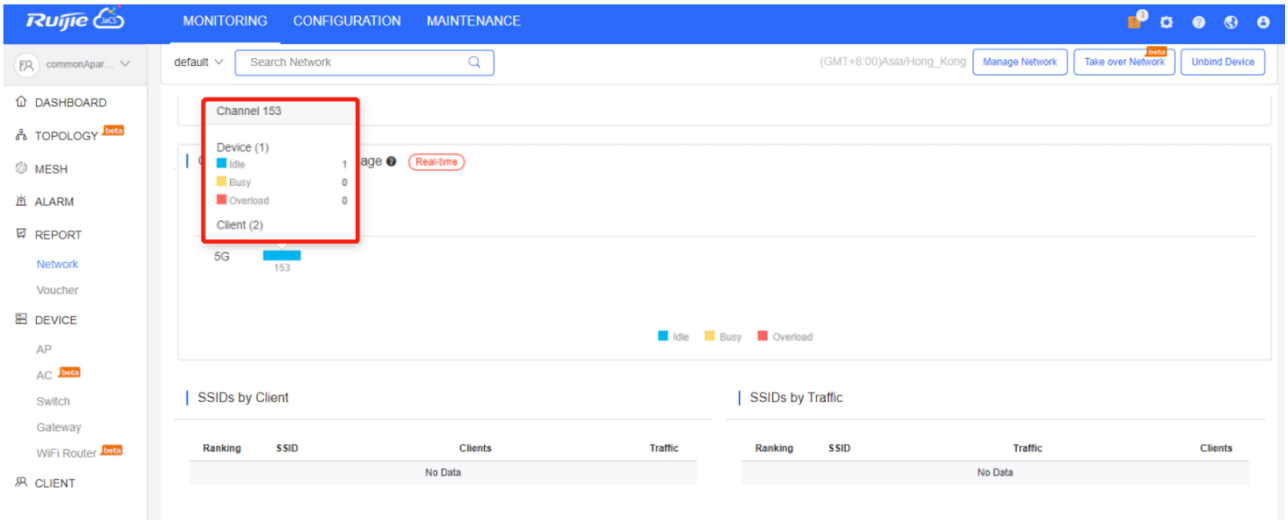
Uplink: Traffic directed from internal network to external network.

Downlink: Traffic directed from external network to internal network.

- Summary > Channel Distribution and Usage



The channel distribution and usage of the selected network.



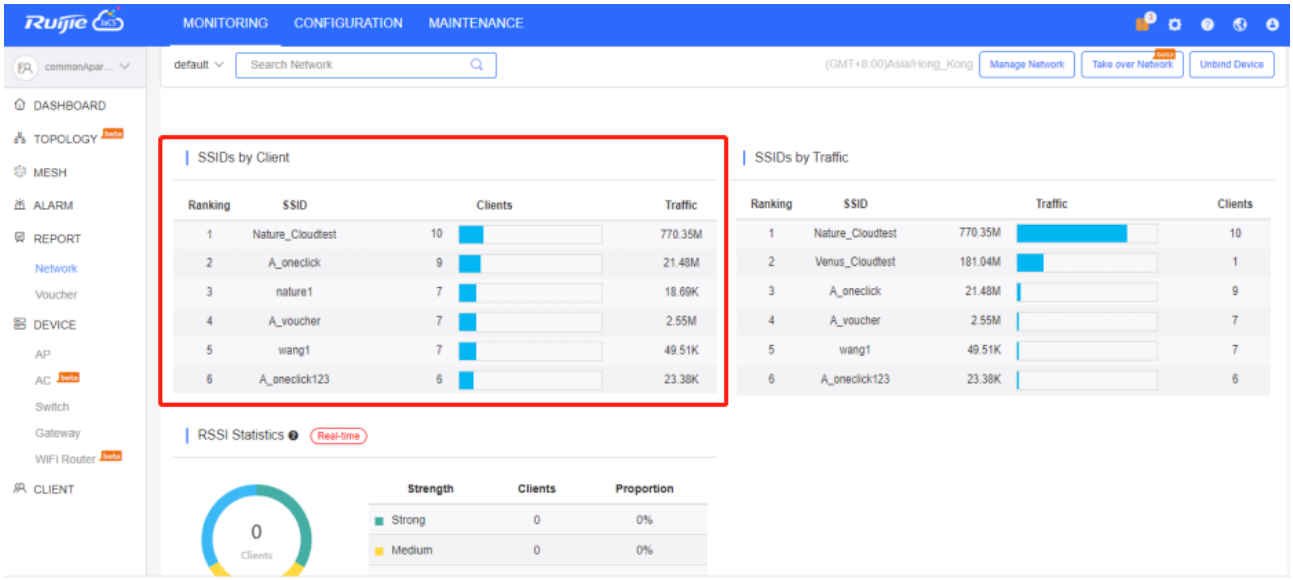
Point to a channel to view more details. The channel usage is graded as:

Idle: 0% to 59%

Busy: 60% to 79%

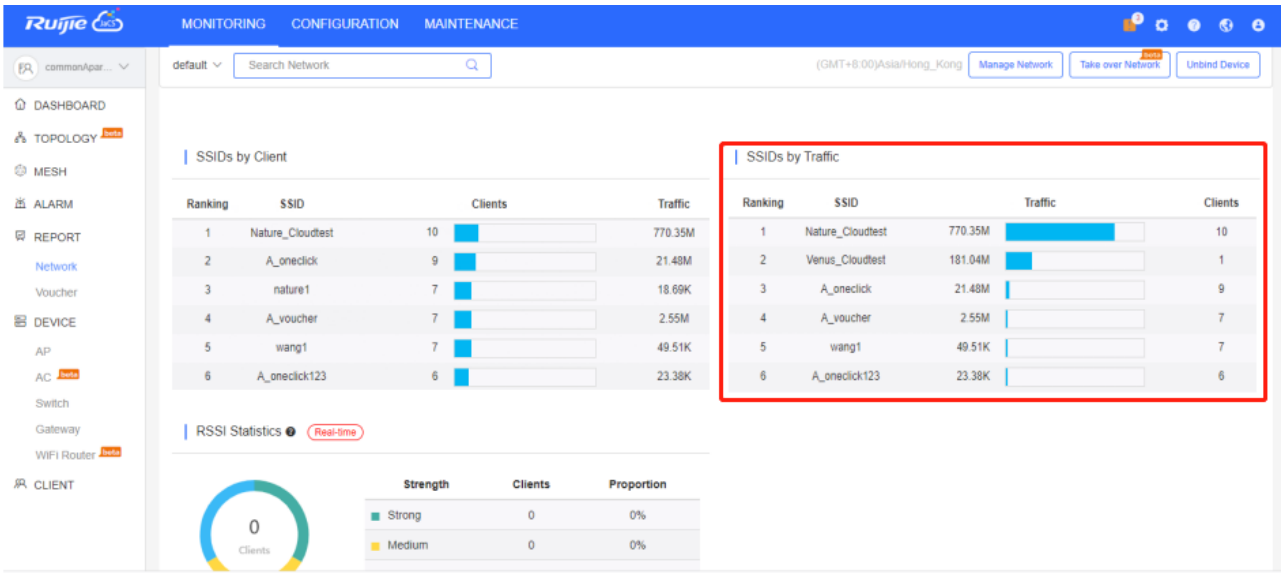
Overload: 80% to 100%

- Summary > SSIDs by Client



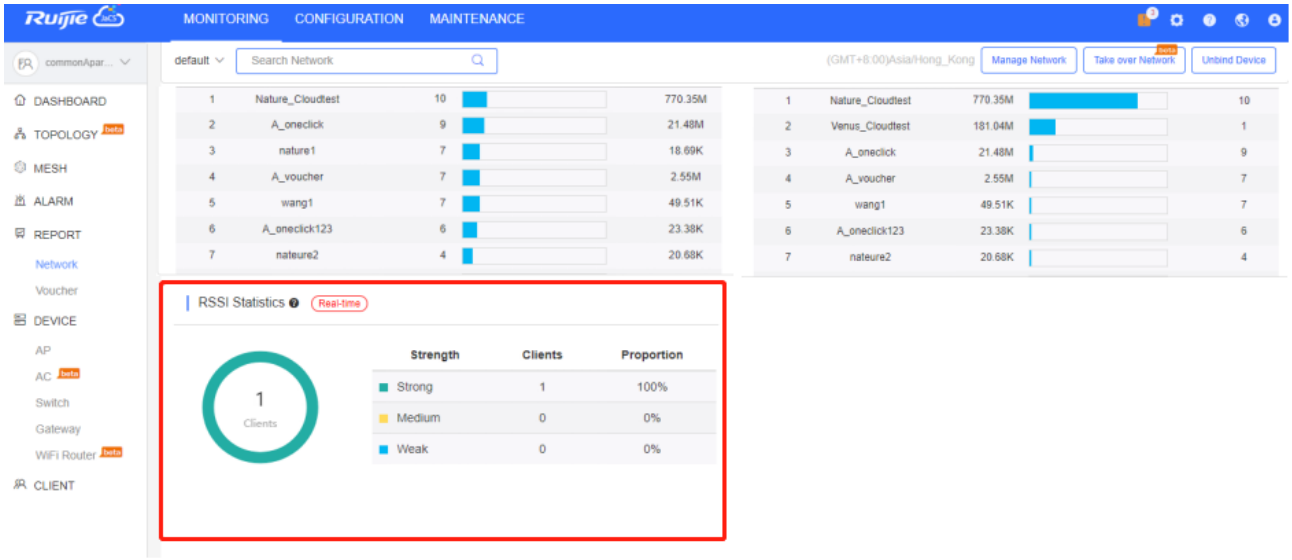
The SSIDs ranked by client number of the selected network during the specific period.

- Summary > SSIDs by Traffic



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

- Summary > RSSI Statistics



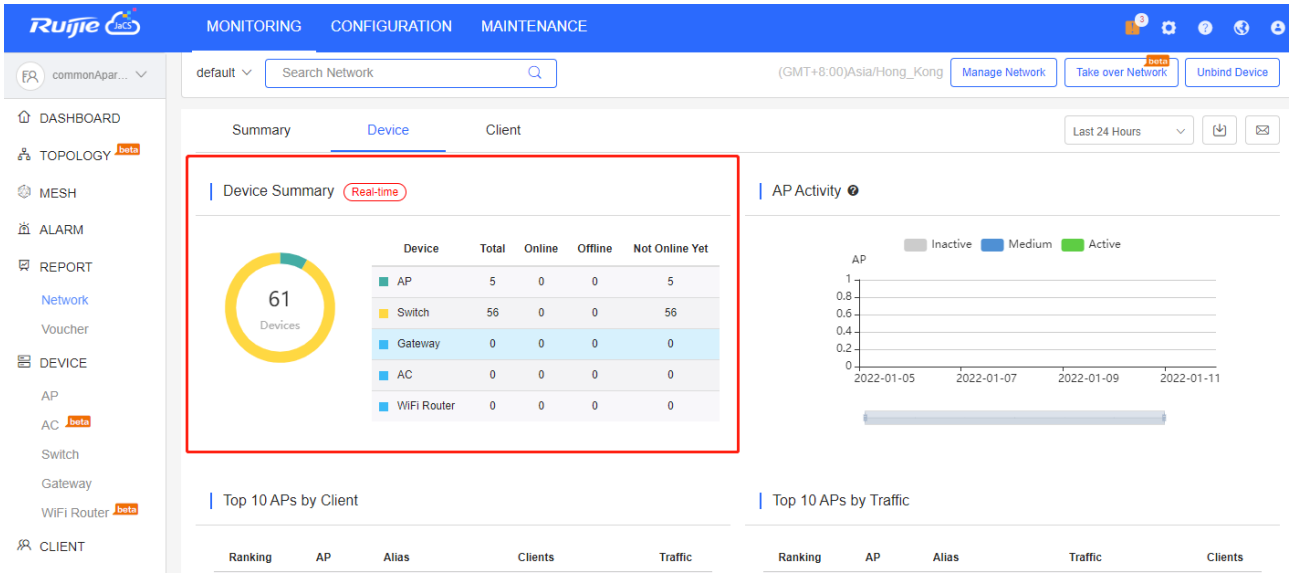
The wireless signal strength of the selected network during the specific period. The signal intensity is defined below:

Weak: RSSI ≤ -80dB

Medium: -80dB < RSSI ≤ -70dB.

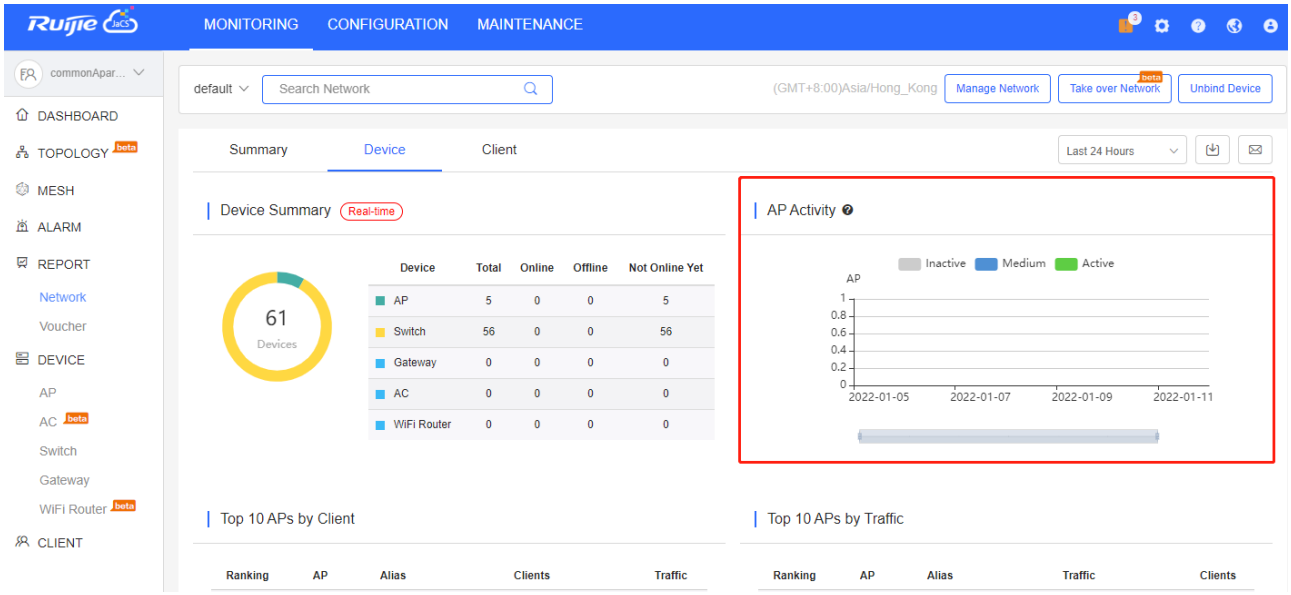
Strong: RSSI > -70dB

- 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.

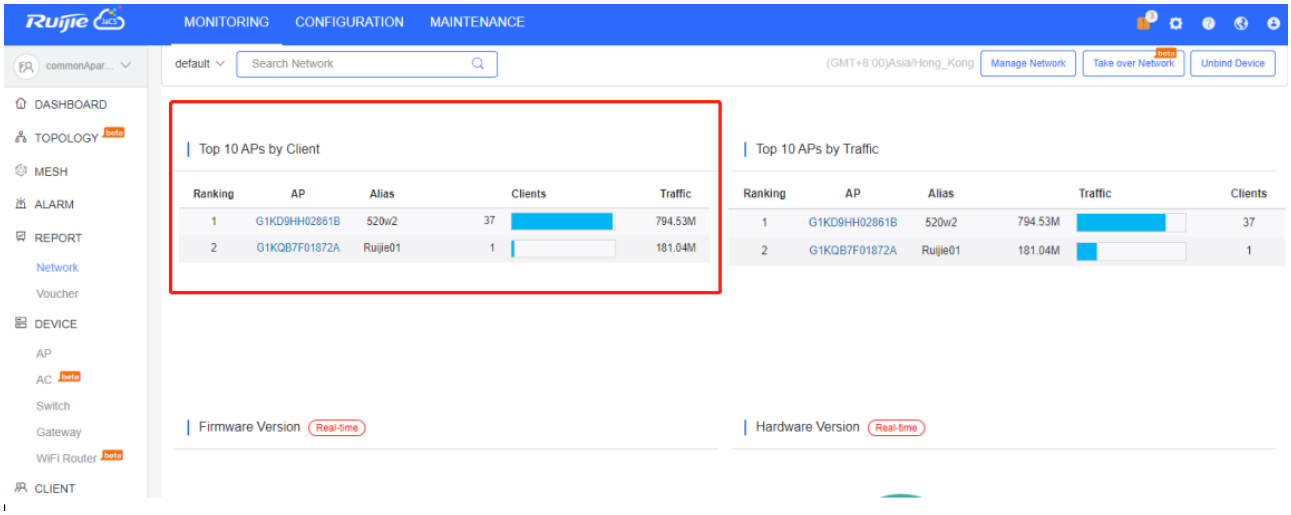
AP activity is evaluated based on the number of active clients accessing the AP in a day. APs not associated with any clients are not calculated.

Inactive: <5 active clients

Medium: 5-9 active clients

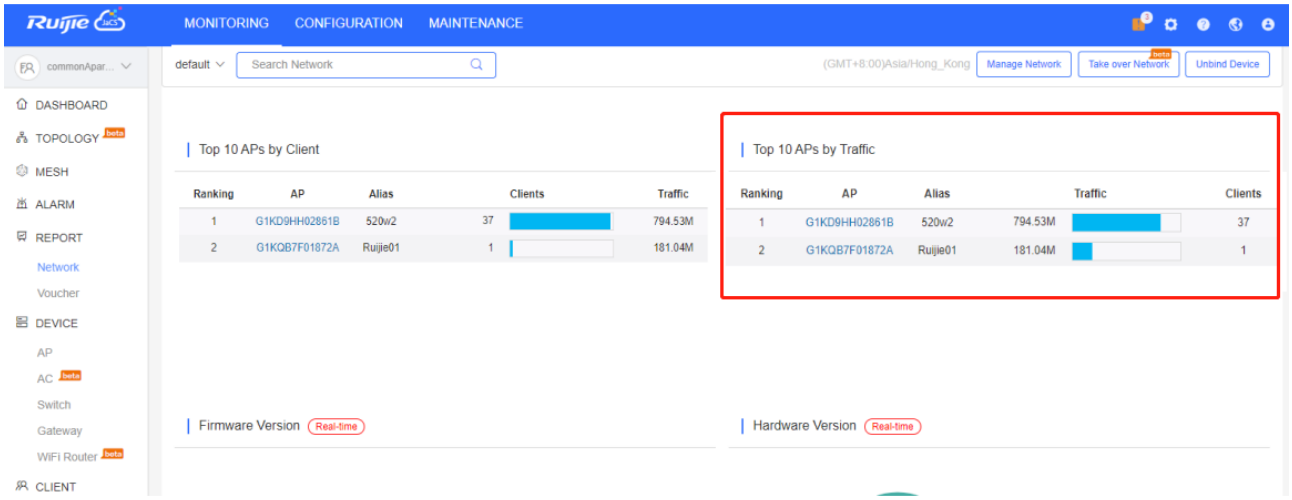
Active: ≥10 active clients.

- Device > Top 10 APs by Client



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

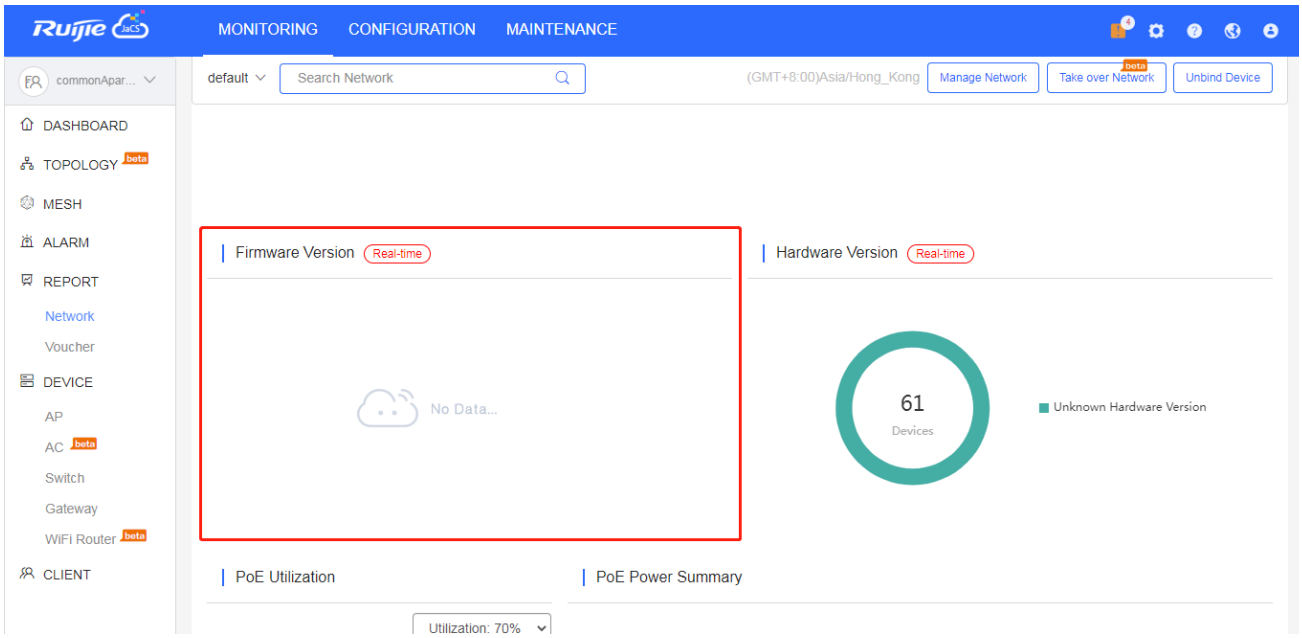
- Device > Top 10 APs by Traffic



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

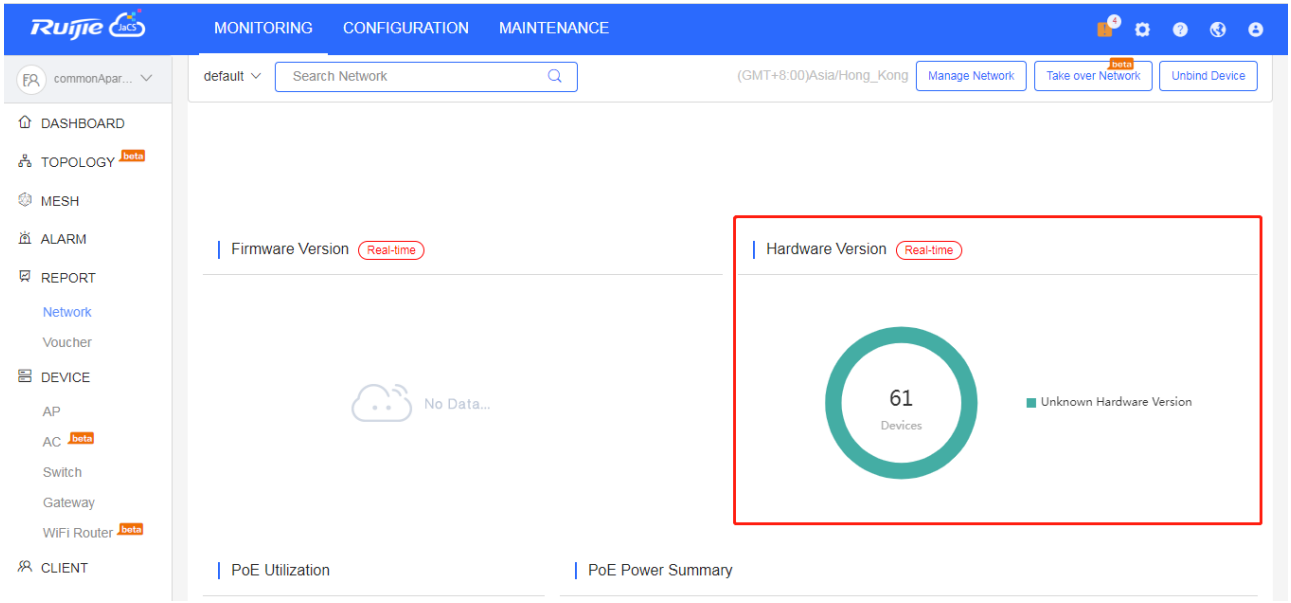
- Device > Firmware Version

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



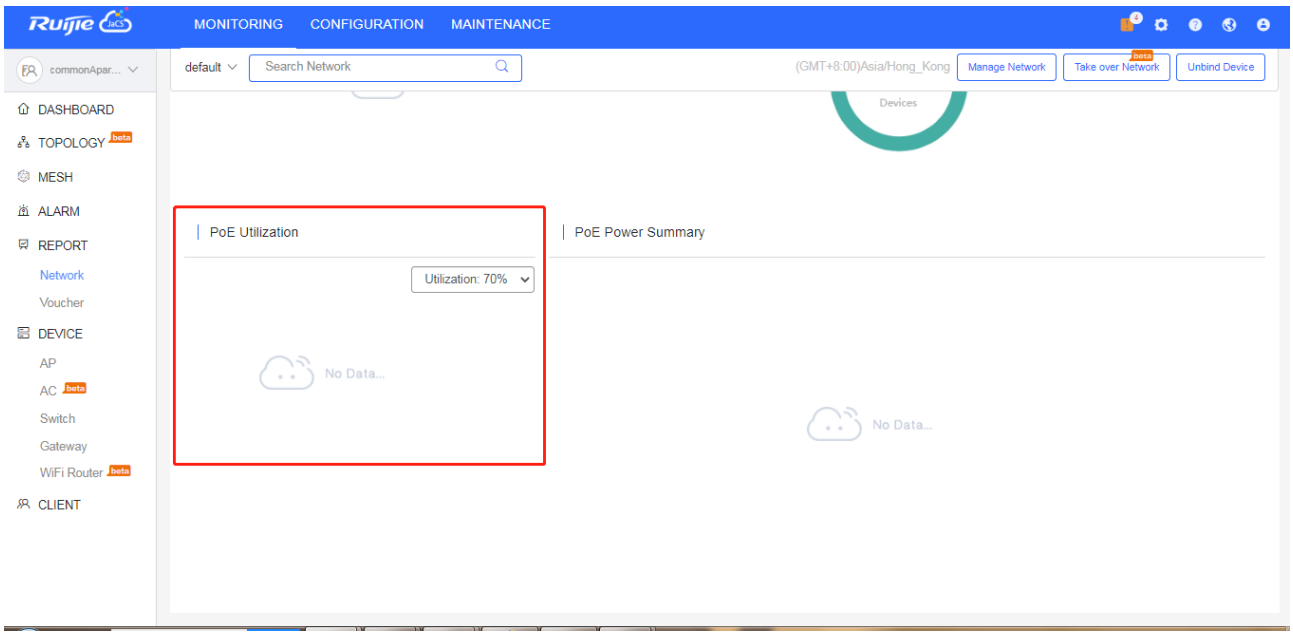
- Device > Hardware Version

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



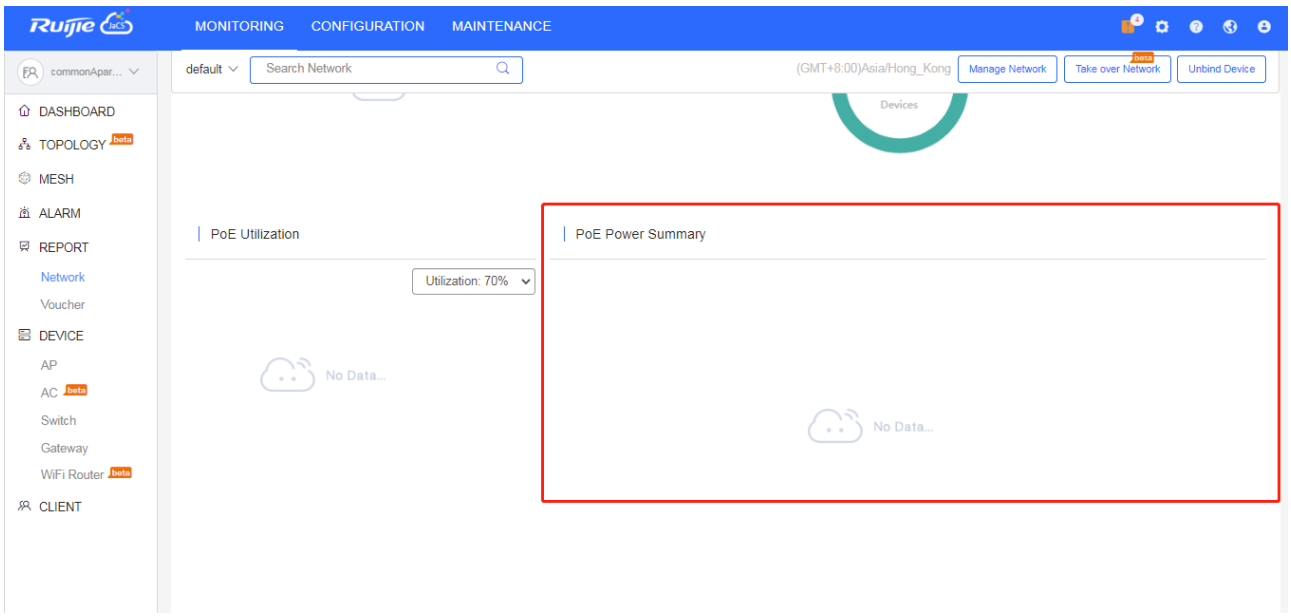
- Device > PoE Utilization

The numbers of PoE switches above and below the selected utilization percentage.

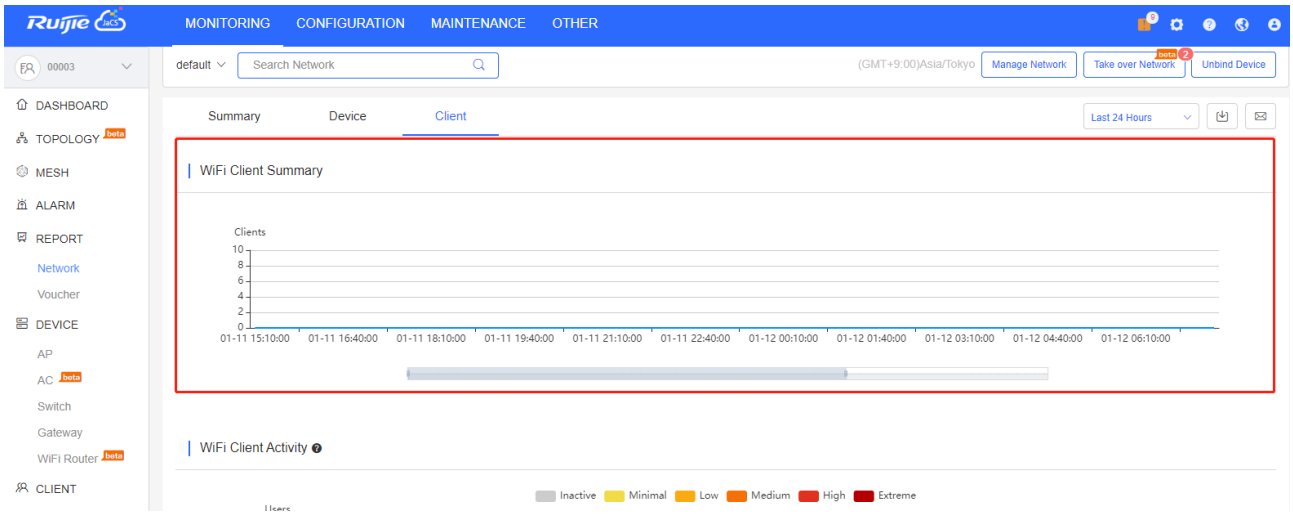


- Device > PoE Power Summary

The power summary of the entire PoE device, including the total power and used power.

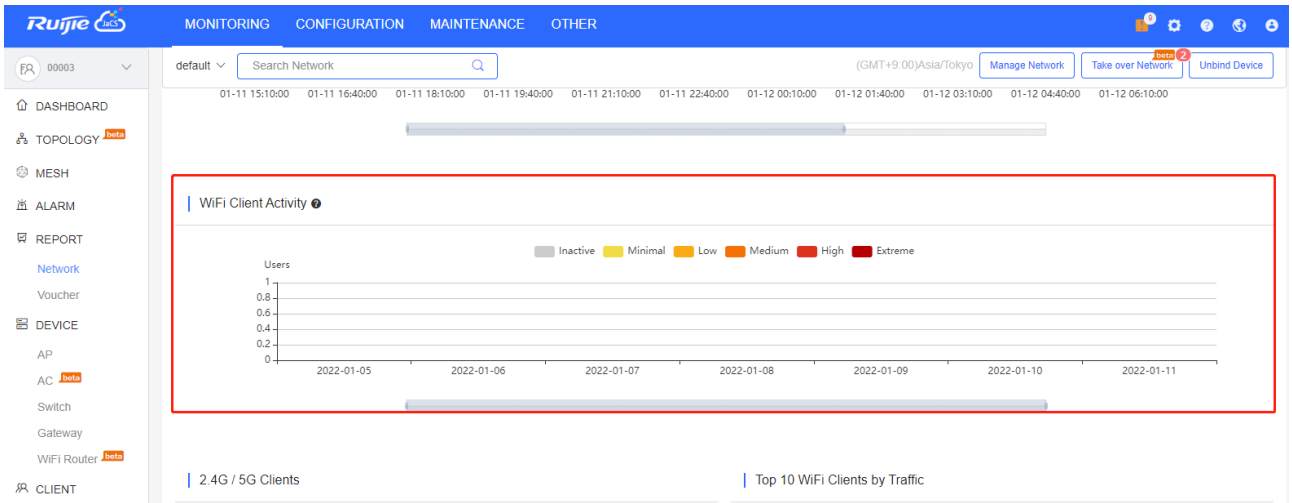


- Client > WiFi Client Summary



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

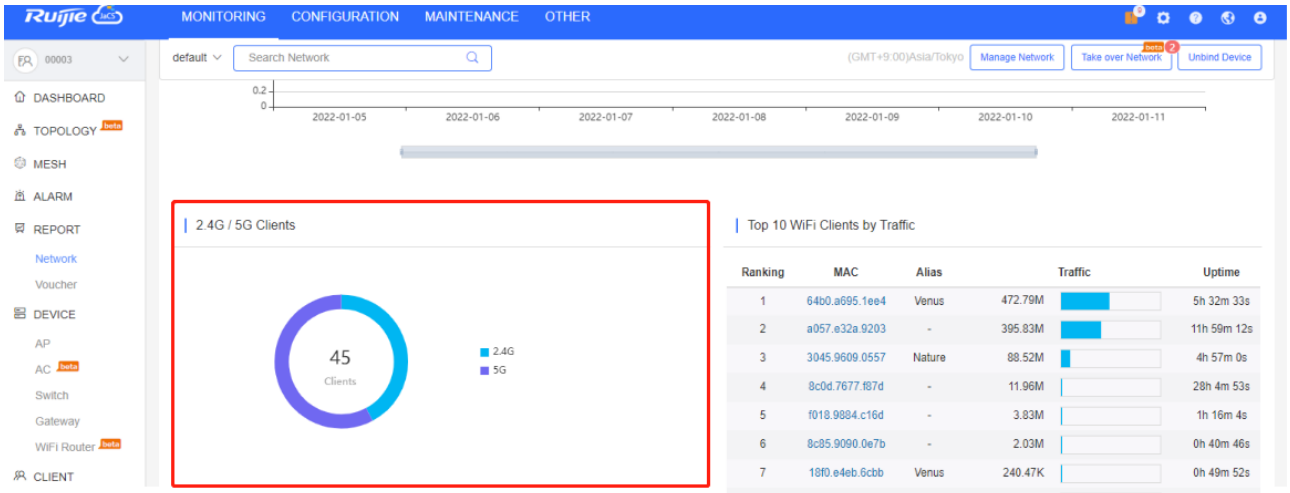
Low: 1h/d and 500K traffic

Medium: 2h/d time and 2M traffic

High: 4h/d time and 5MB traffic

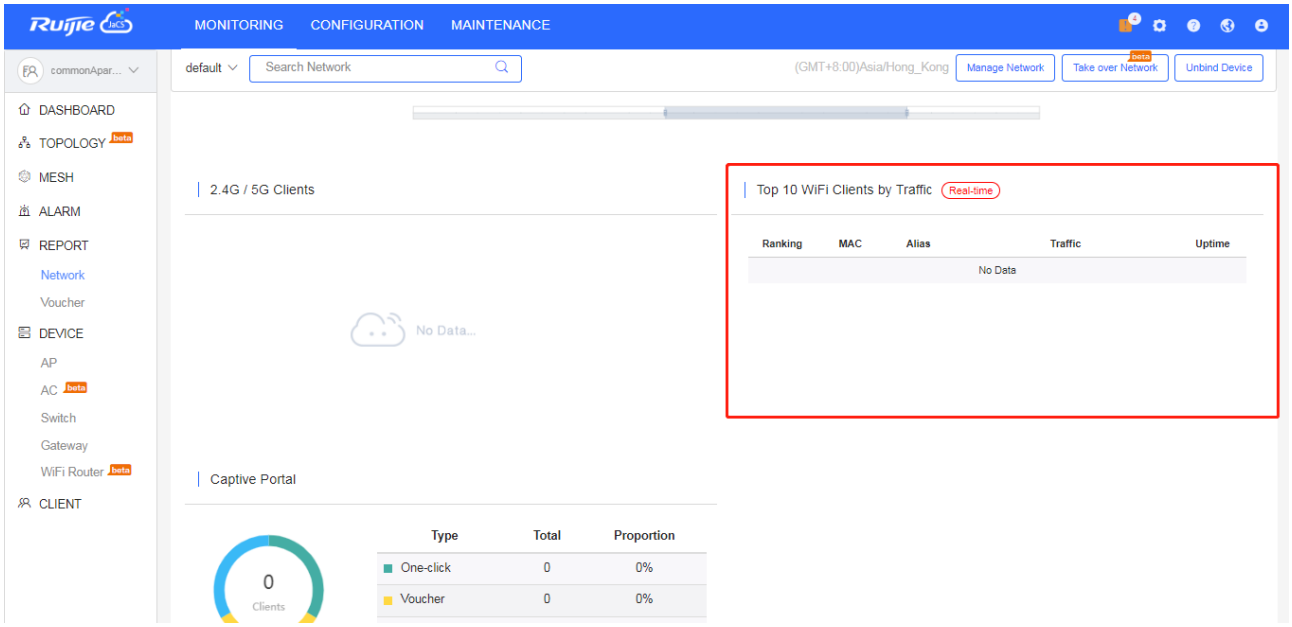
Extreme: 8h/d time and 10MB traffic

- Client > 2.4G / 5G Clients



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

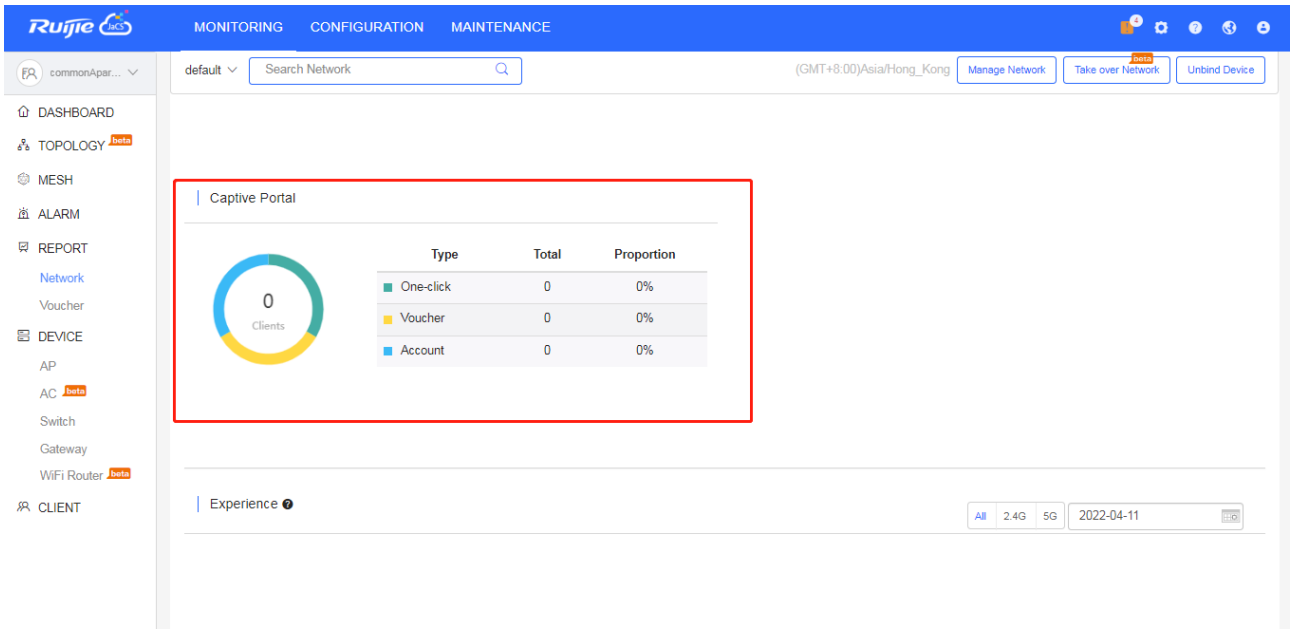
- Client > Top 10 WiFi Clients by Traffic



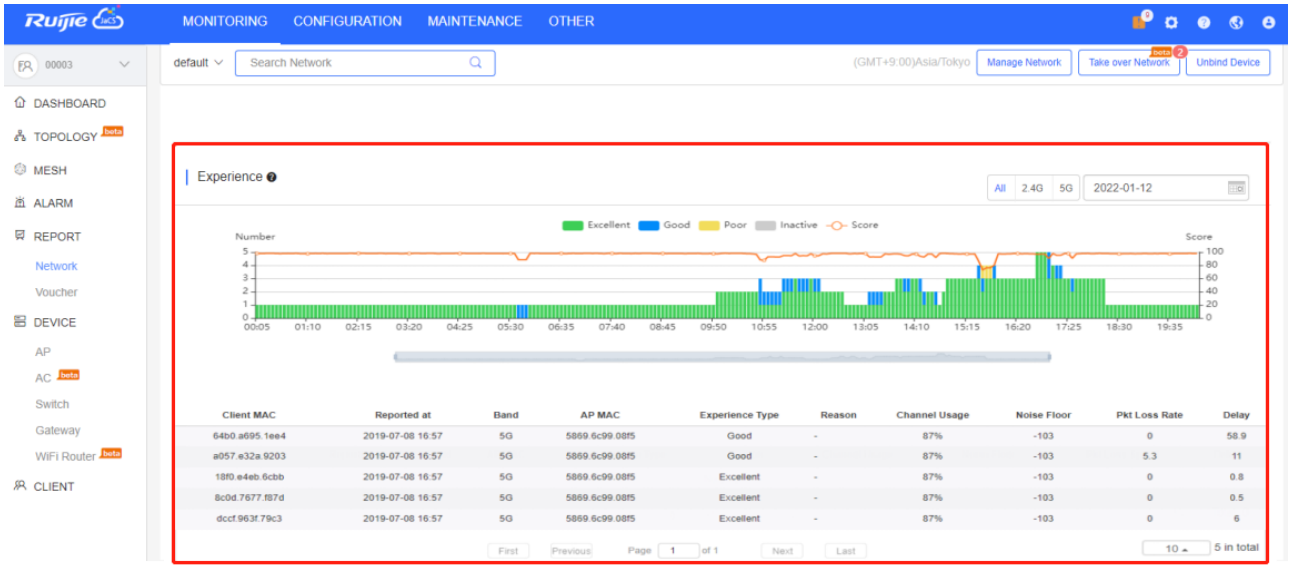
The top 10 clients ranked by traffic of the selected network during the specific period.

- Client >Captive Portal

The numbers and proportions of different portal authentication methods in the network. The statistics are refreshed every hour. Now 3 authentication methods (One-click, Voucher and Account) are supported.



- Client > Experience



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.

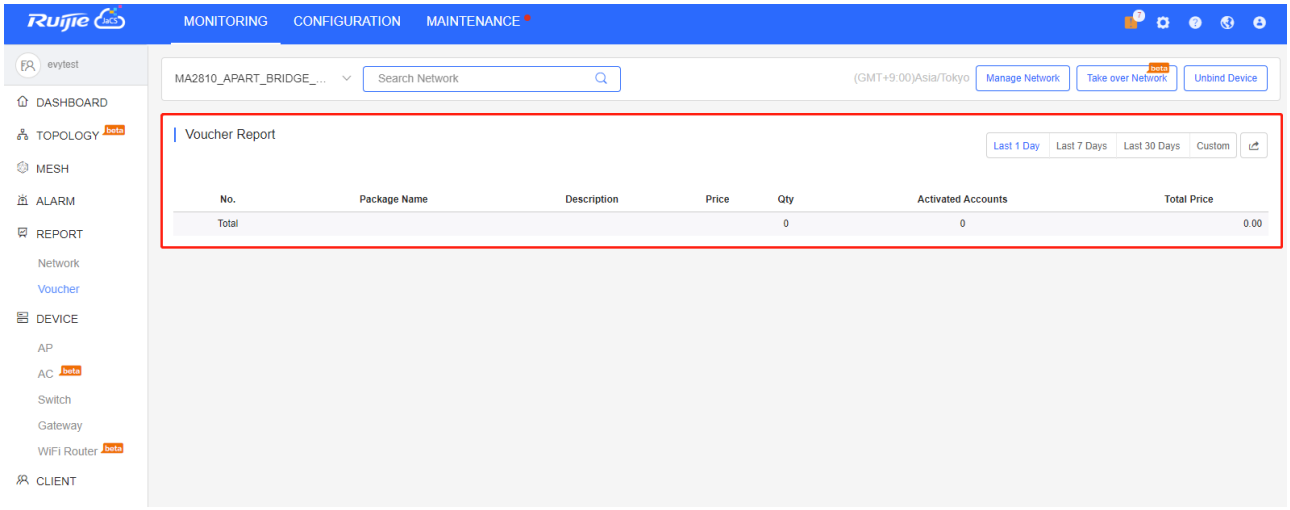
Inactive: check whether a client is inactive according to the traffic and power usage.

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.

5.5.2 Voucher

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

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



Item	Description
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.

5.6 Device

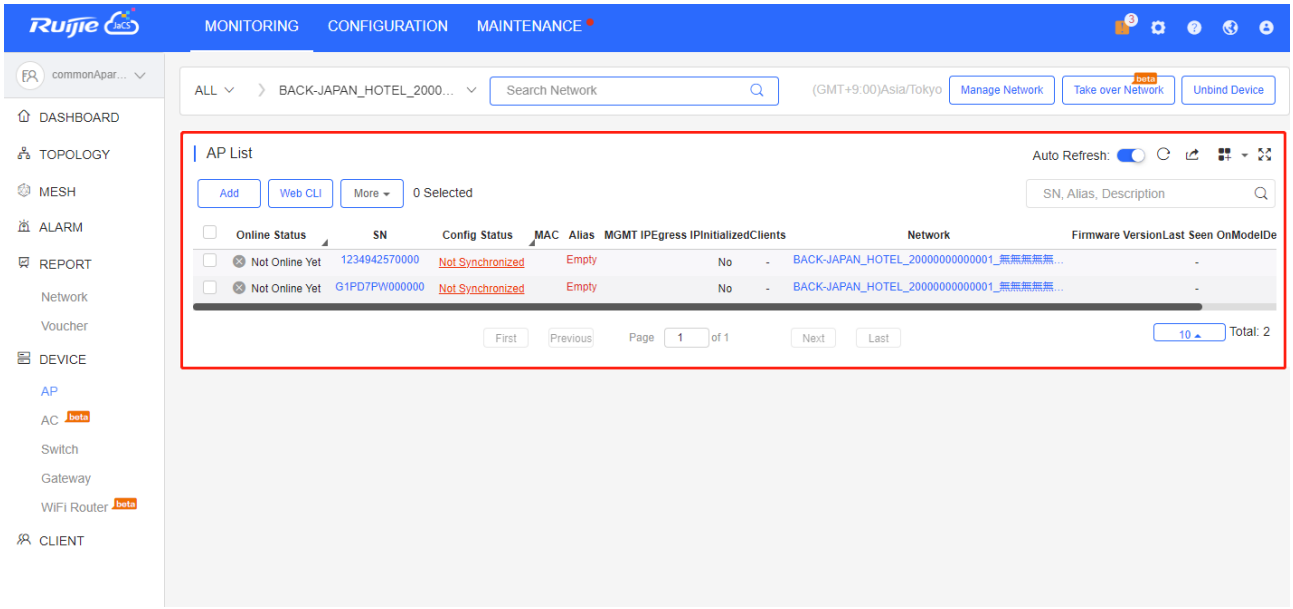
Choose **MONITORING > DEVICE** to display the **Devices** page, and select a network on the top to filter devices.

5.6.1 AP

5.6.1.1 AP List

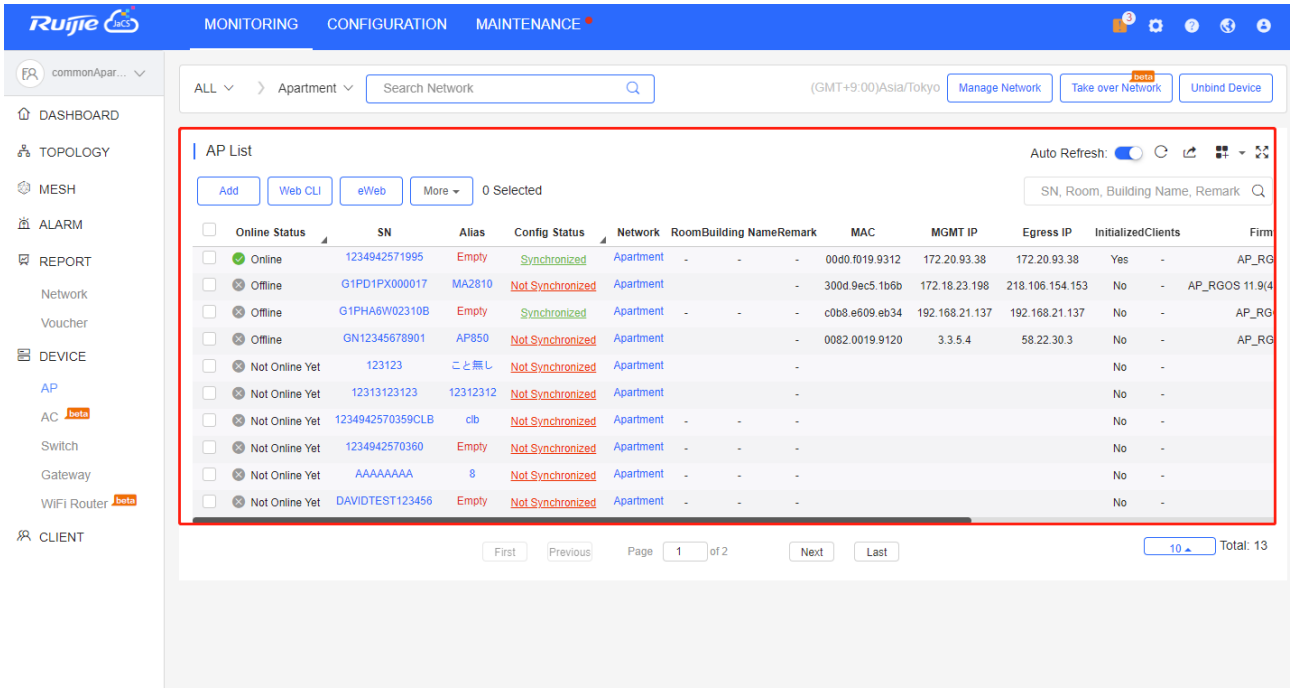
Non-apartment Scenario

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

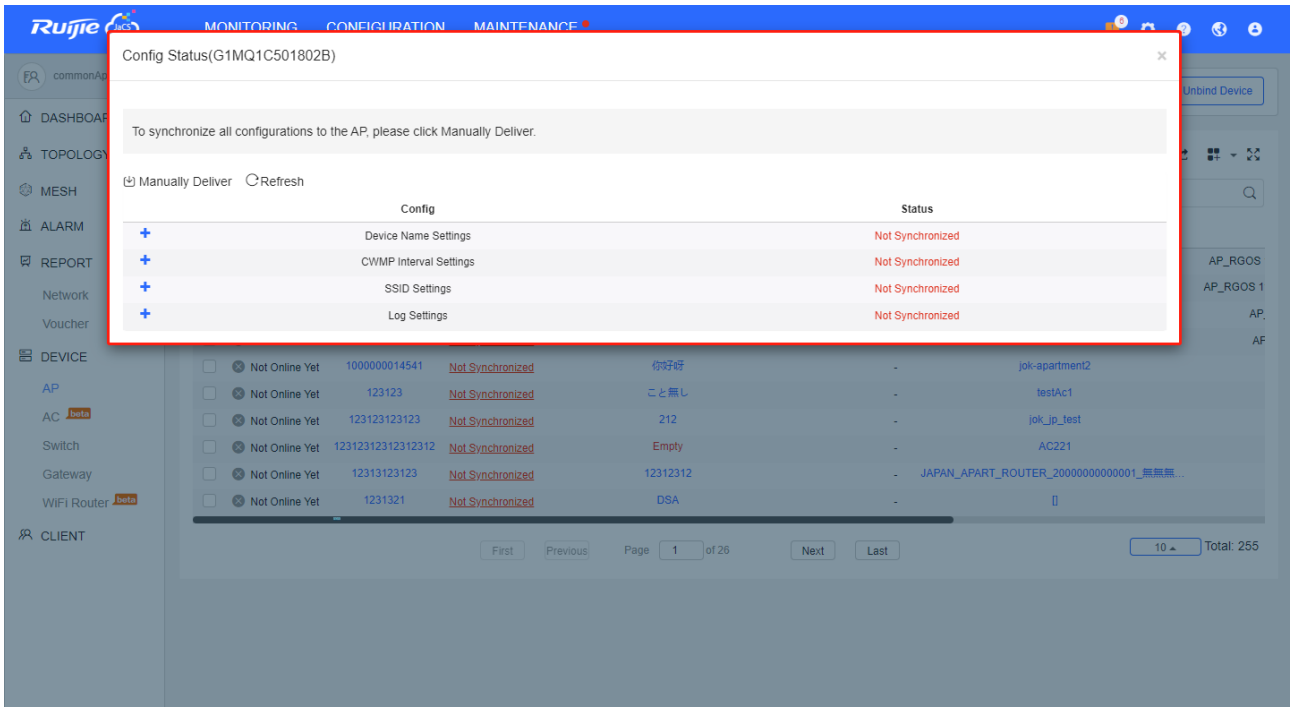


The **AP List** automatically refreshes every minute. Click Auto Refresh: to enable/disable the auto refresh function.

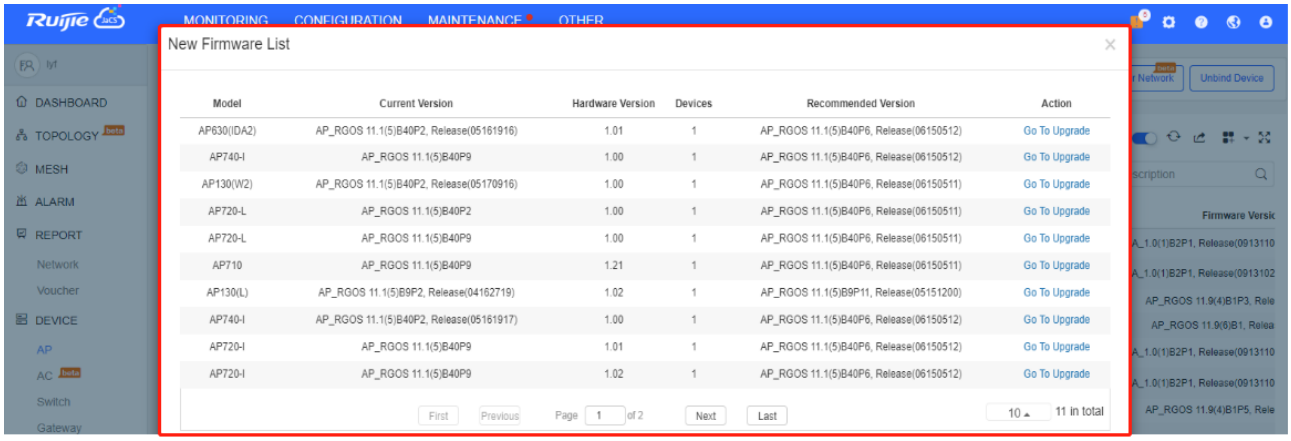
Above the list is the **Add AP**, **Web CLI and eWeb** functions. Click More to display the **Move to**, **Delete**, and **Reboot** functions. For more information, refer to **Basic AP Operations**.

In non-apartment scenario, the **Search** function supports fuzzy queries based on the serial number, alias and description, while in apartment scenario, it supports queries based on the serial number, room, building name and remark. It also supports queries based on online/offline status and configuration status in both scenarios.

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

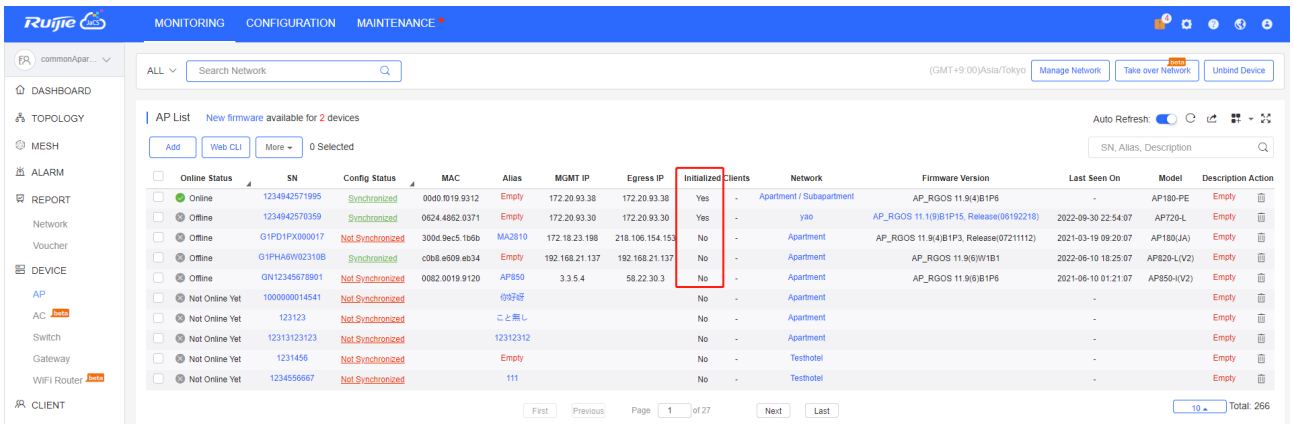


The number of devices which have available firmware for upgrade is displayed on the upper-left corner of the **AP List** page. Click **New Firmware** to display the **New Firmware List**. Then click **Go To Upgrade** to enter the **MAINTENANCE** > **UPGRADE** > **Upgrade** page.



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

If an initial configuration template has been applied to the device, **Yes** will be shown in the initialized column.

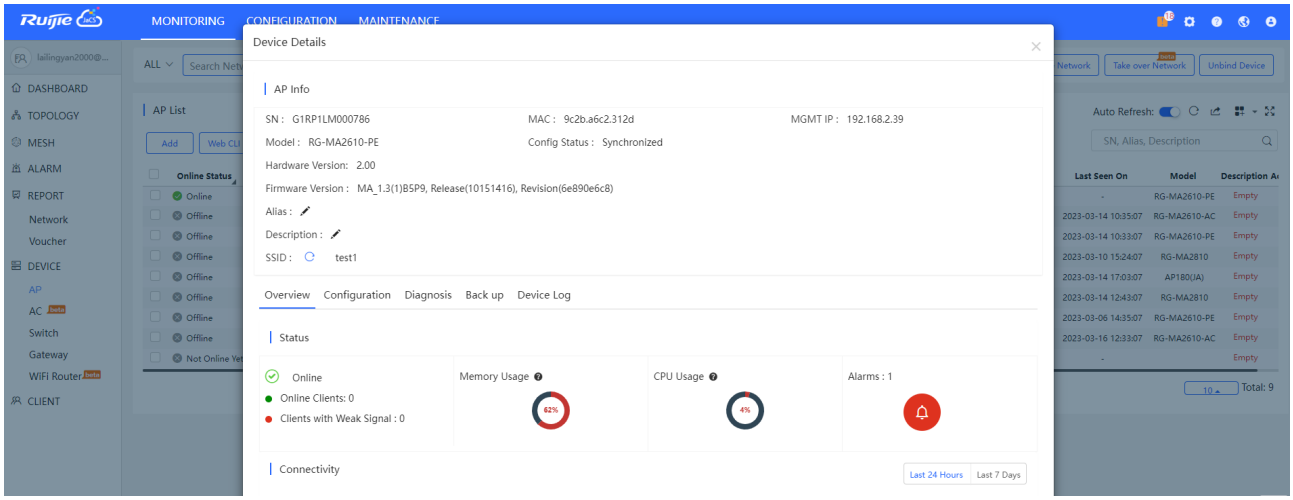


5.6.1.2 Device Details

Click the serial number in the AP list to open the details page for a single device. The page includes AP Info, Overview , Configuration, Diagnosis, Back up and Device Log.

- AP Info

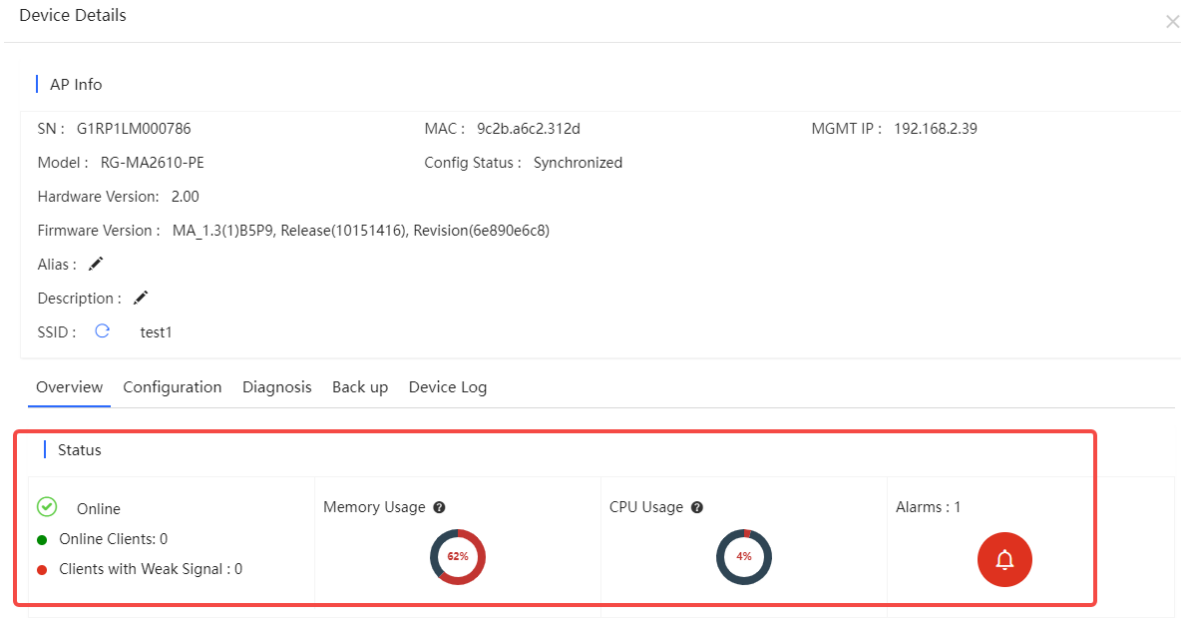
The basic information includes serial number, MAC address, management IP address, device model, configuration status, firmware version, hardware version, alias, and description.



- Overview

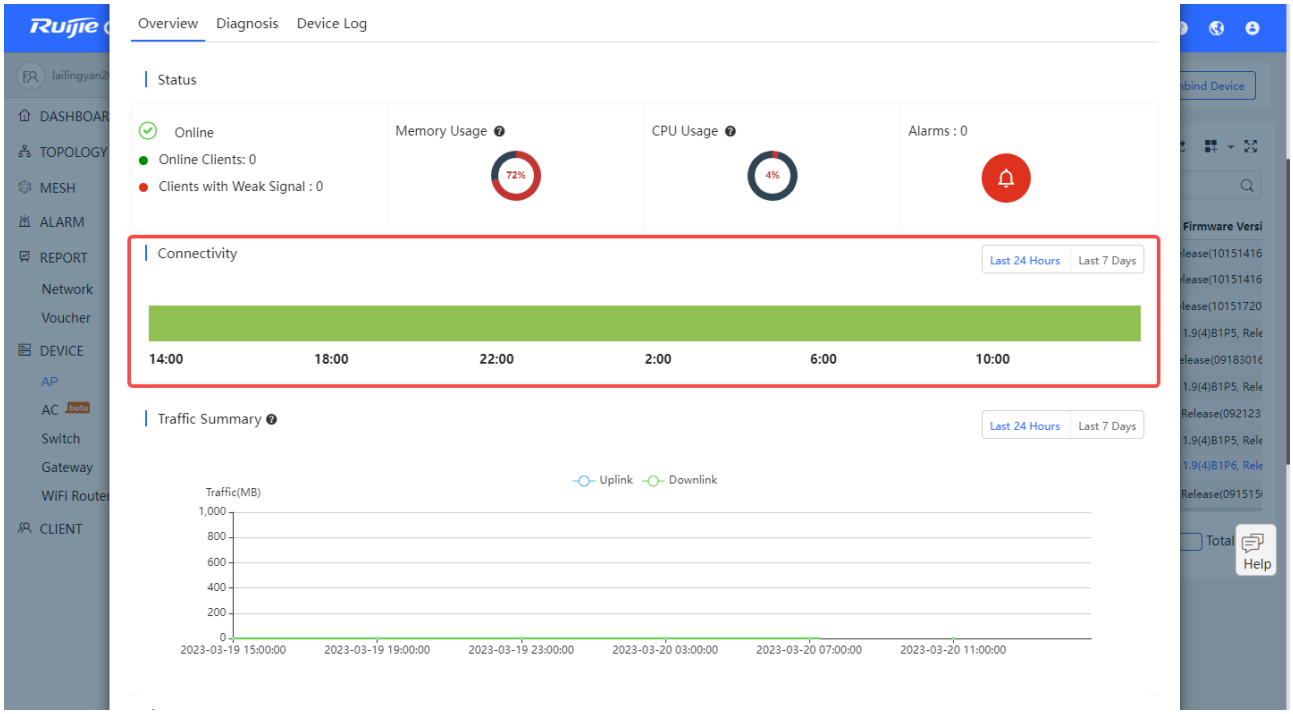
(1) Status

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



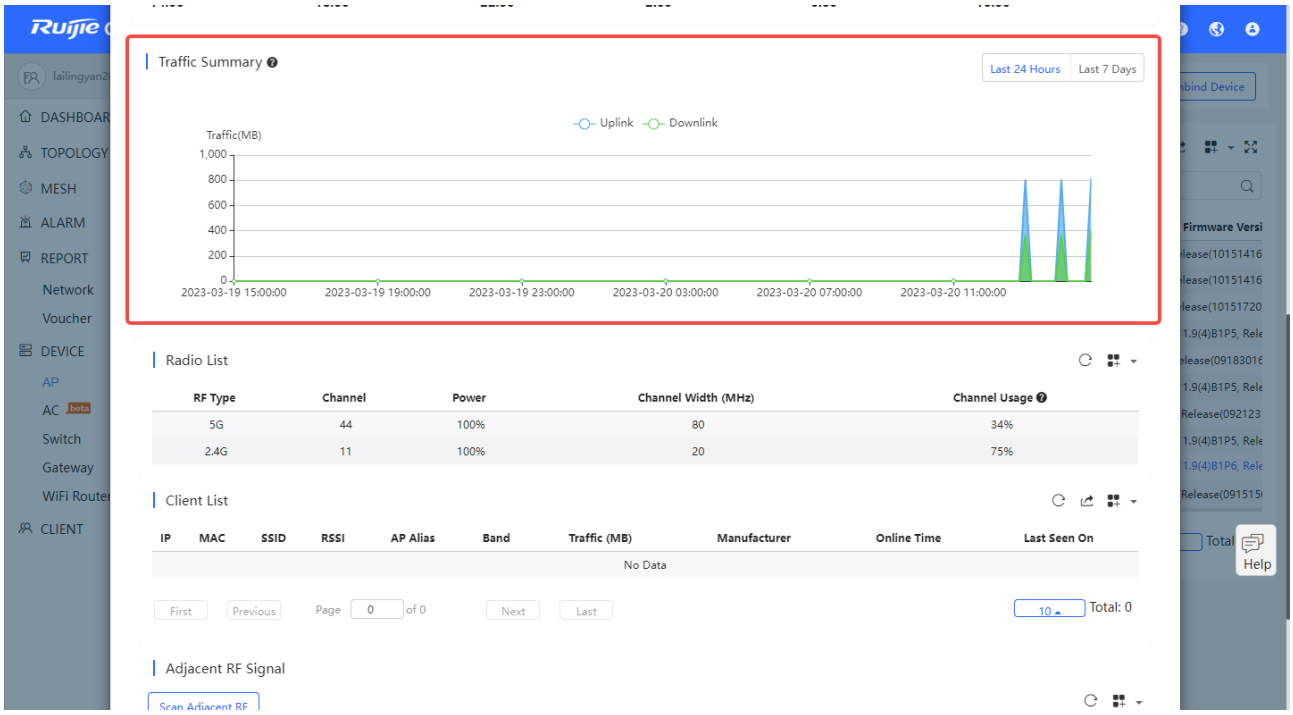
(2) Connectivity

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



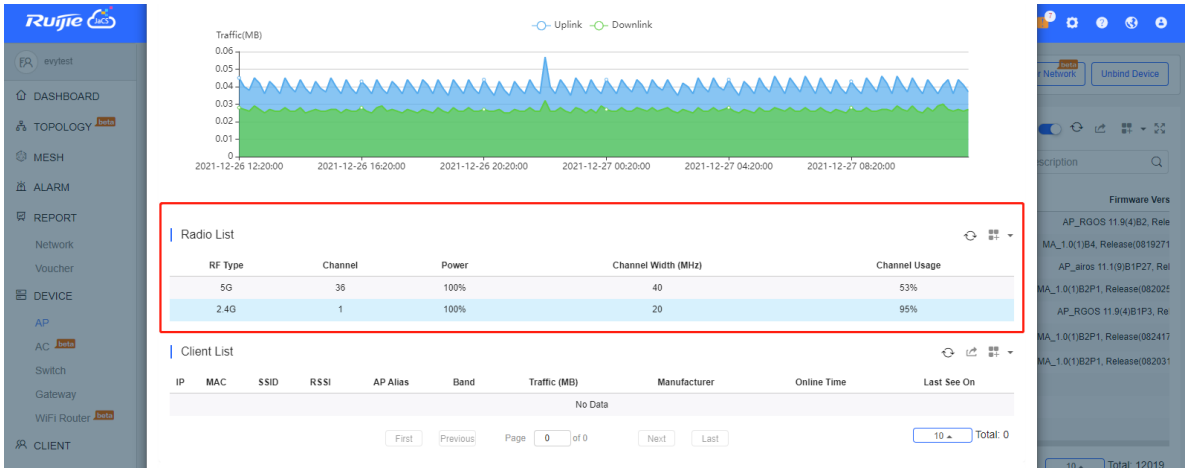
(3) Traffic Summary

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



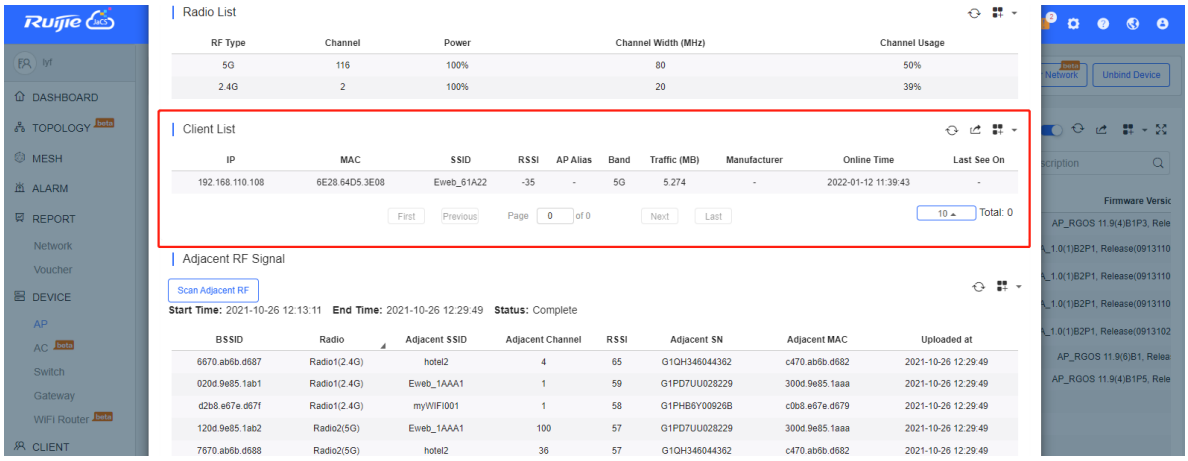
(4) Radio List

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



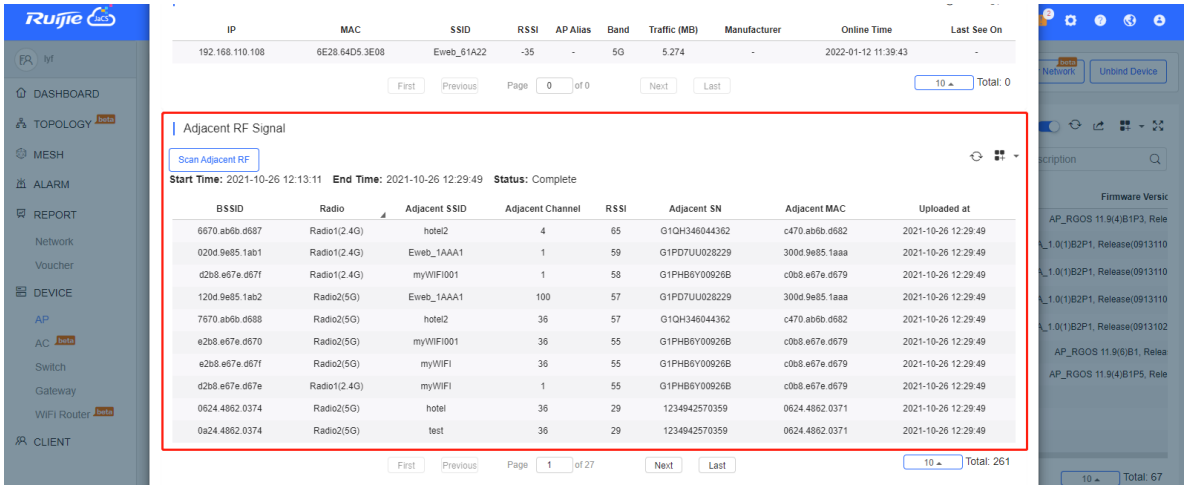
(5) Client List

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



(6) Adjacent RF Signal

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.

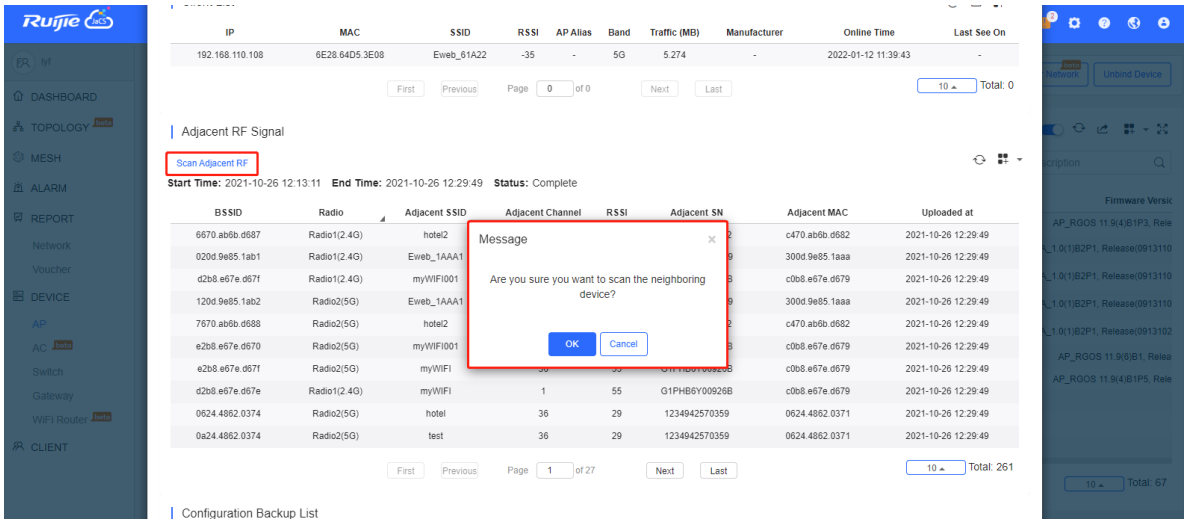


You can trigger APs to scan adjacent RF signals, and identified and unidentified RF signals can be observed. There are two known scenarios:

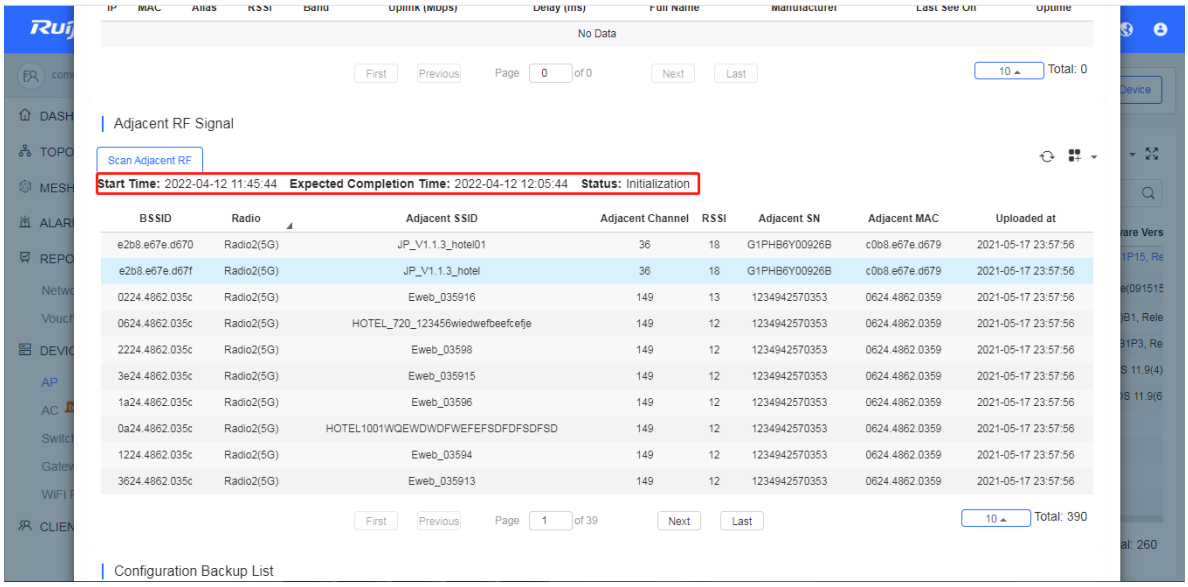
- Testing the number and strength of RF signals emitted by neighboring APs that are not managed by the system to predict a degree of RF interference.
- Identifying RF signals emitted by neighboring APs managed by the system to diagnose the RF functions and powered-on status of neighboring APs.

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:

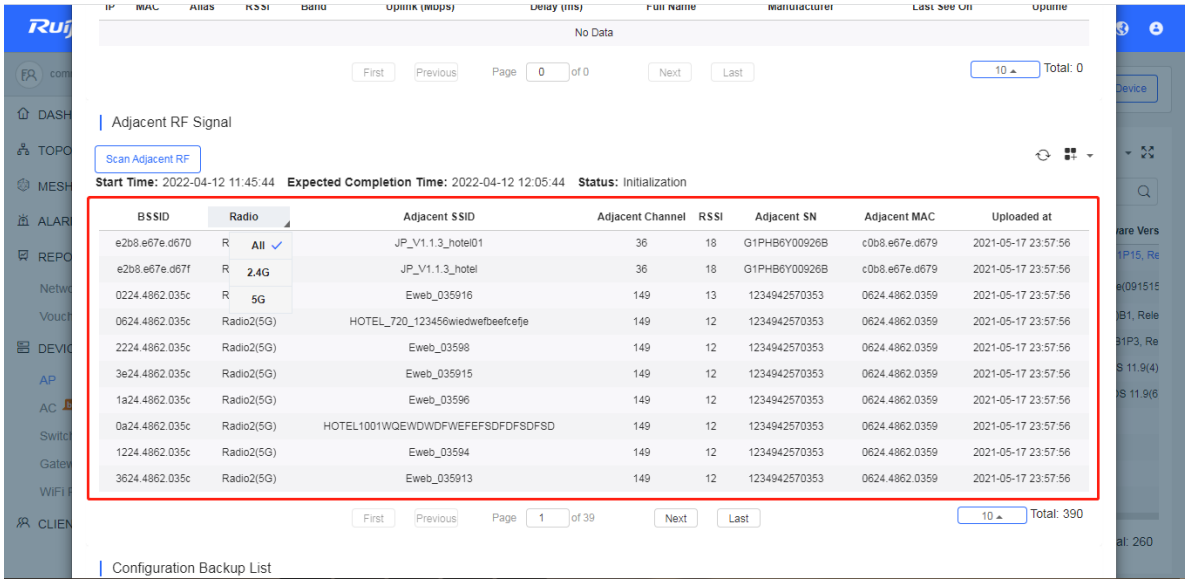
Step 1: Click **Scan Adjacent RF** to trigger an AP to scan adjacent RF signals.



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).



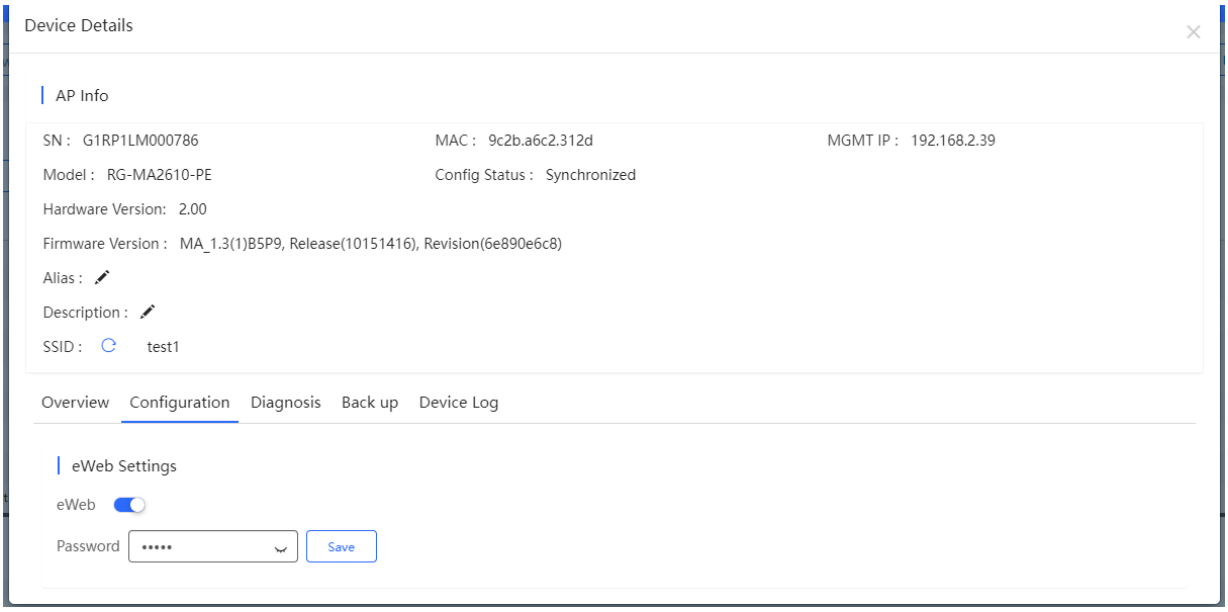
The system stores the latest scanning results, which overwrites earlier data.

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

(1) eWeb Settings

Support to enable and disable the entrance of a device's Web, and to configure the password of the Web admin account.

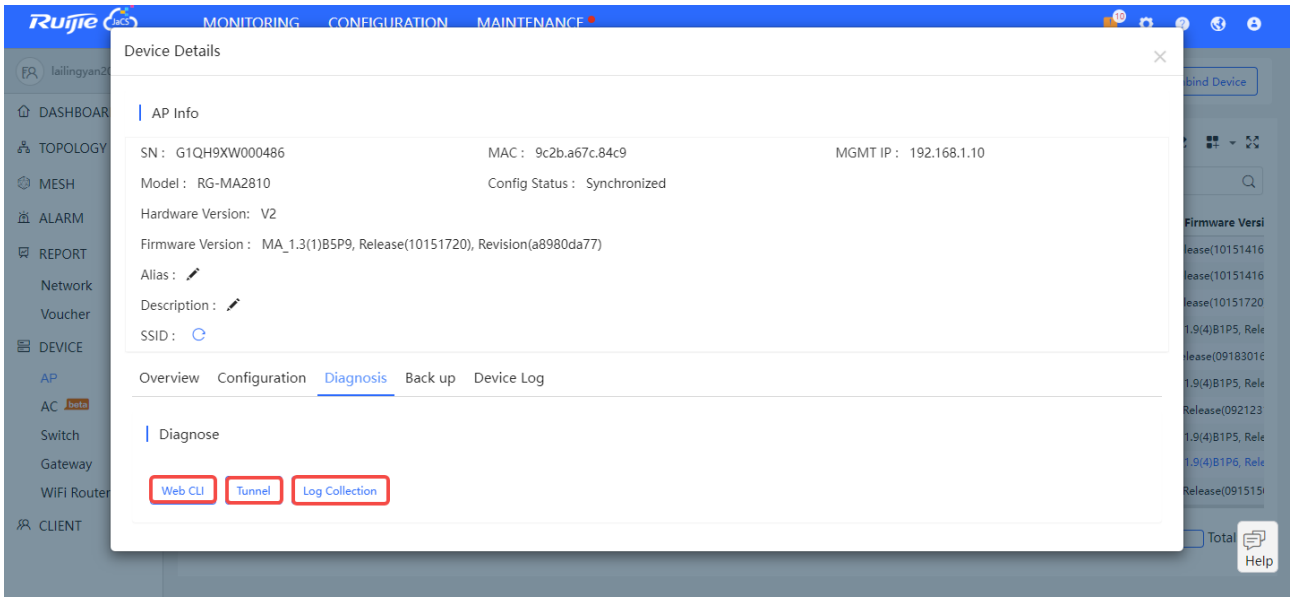


- Diagnose

Click **Web CLI** to open the CLI page of device.

Click **Tunnel** to create different types of tunnels, and check records and more information.

Click **Log collection** to export the logs of the devices. (Log collection is available only for MA series access points.)

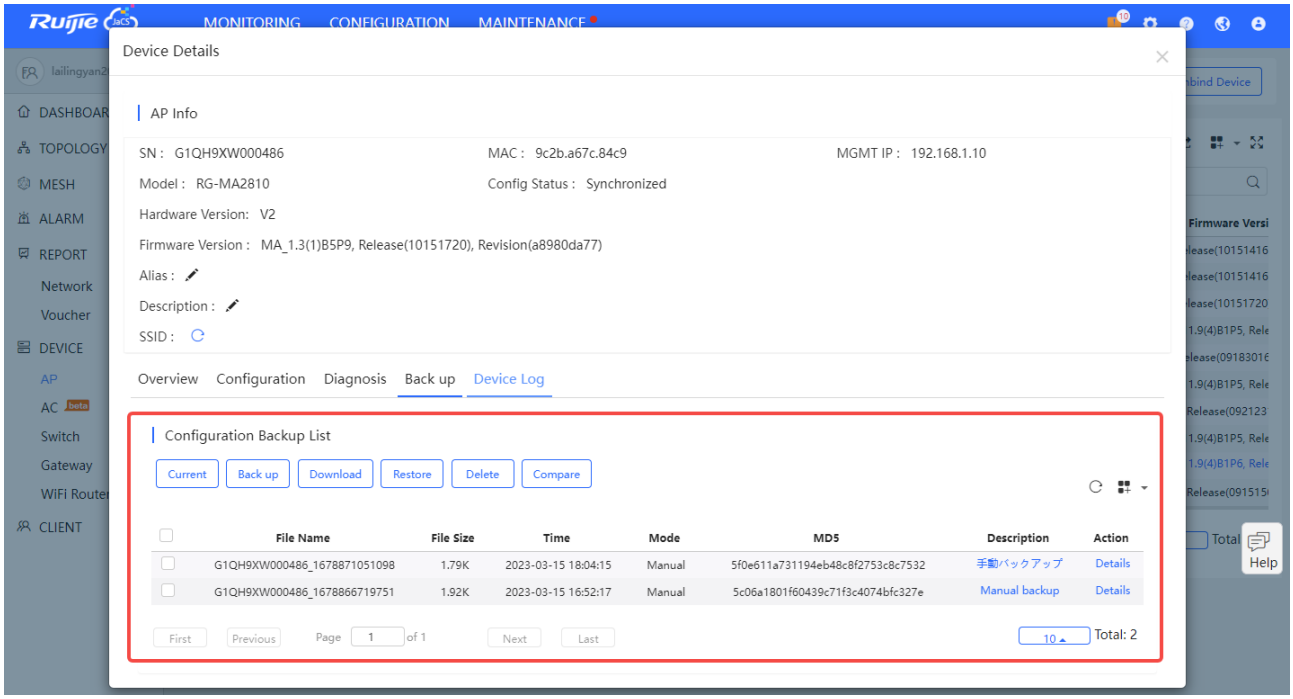


- Back up

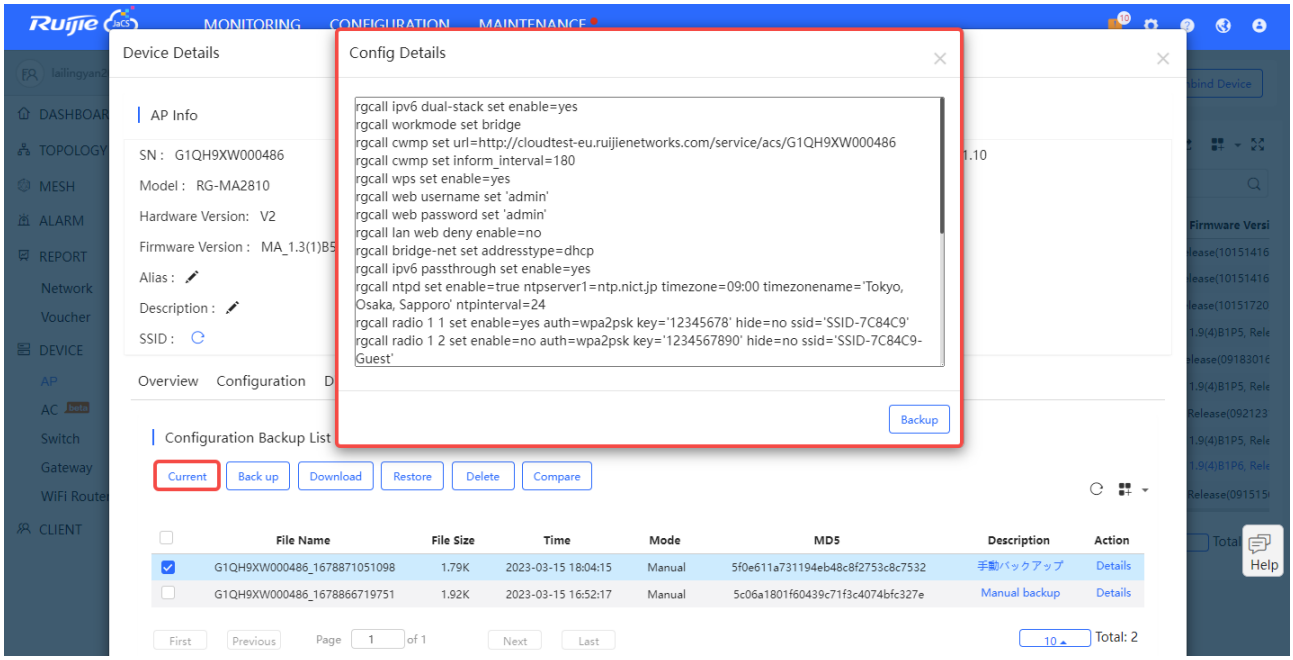
(1) Configuration Backup List

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

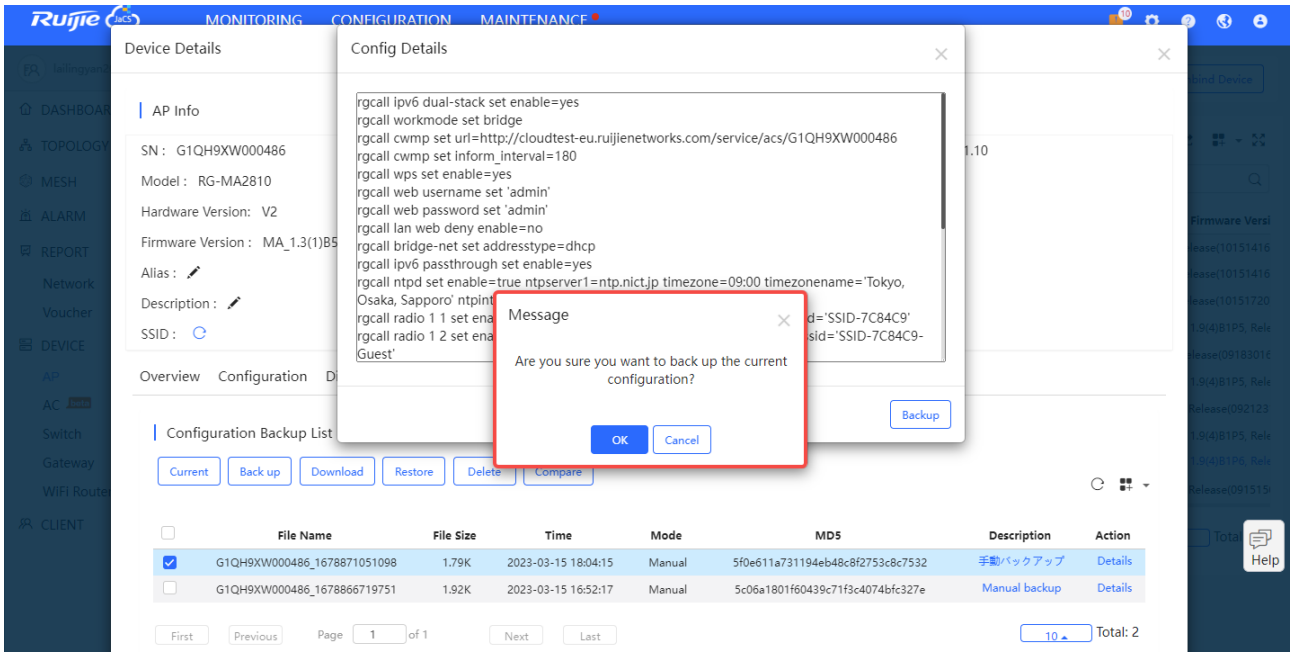
The function is supported only in the apartment scenario.



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.

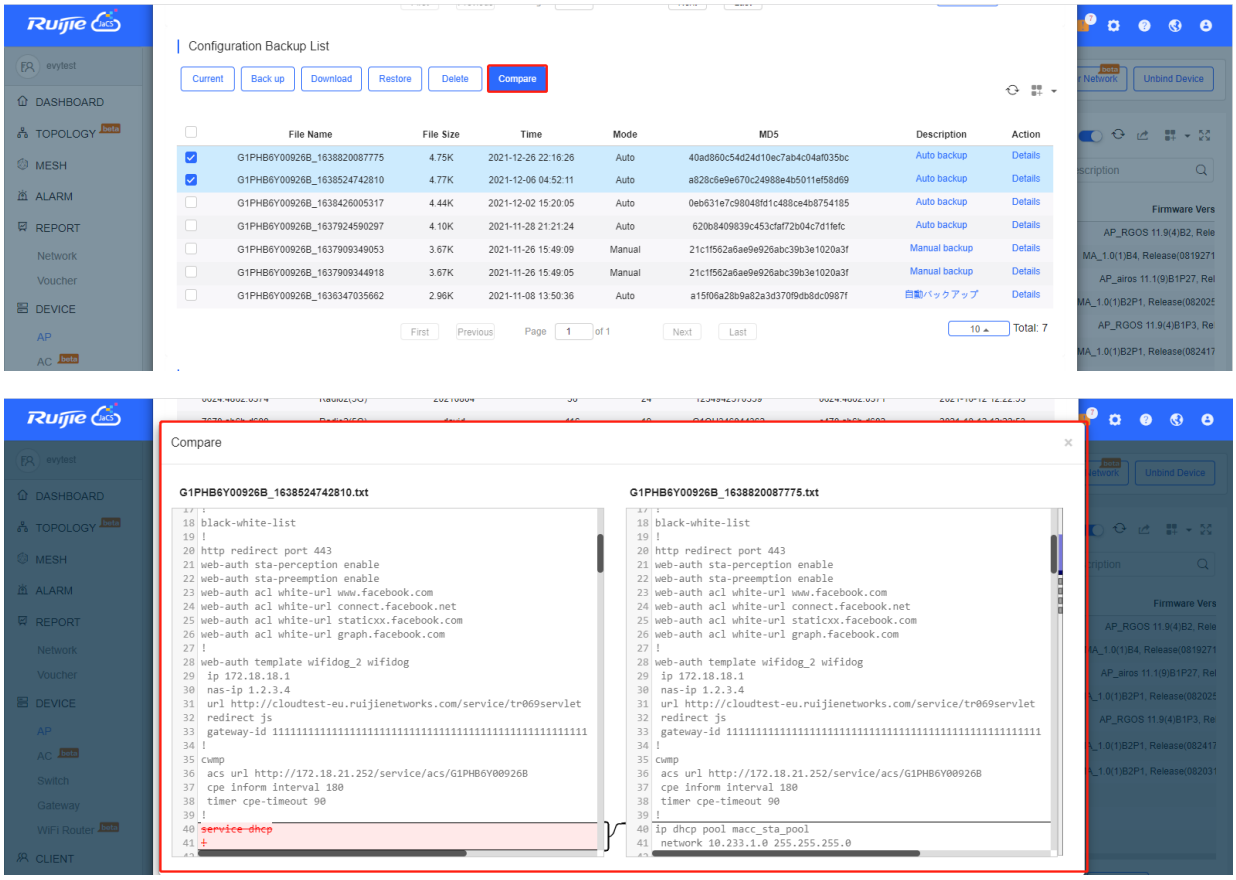


Select one record, and click **Download** to download the configuration file.

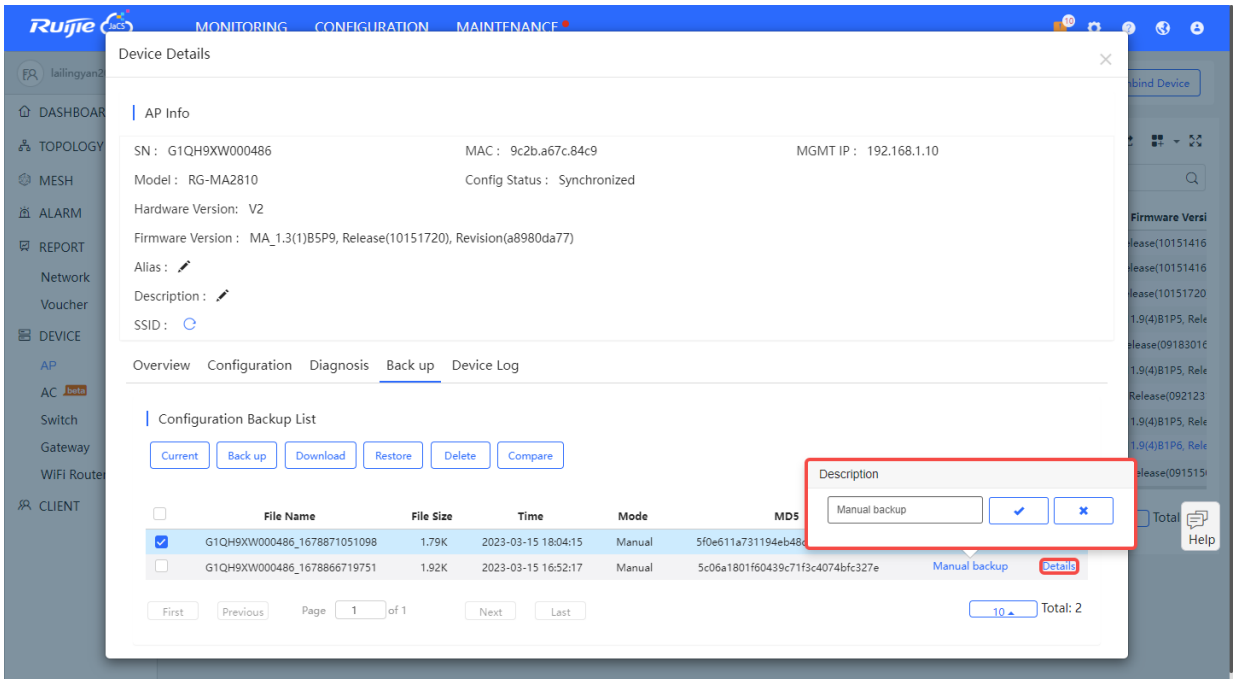
Select one record, and click **Restore** to restore the current configuration.

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

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

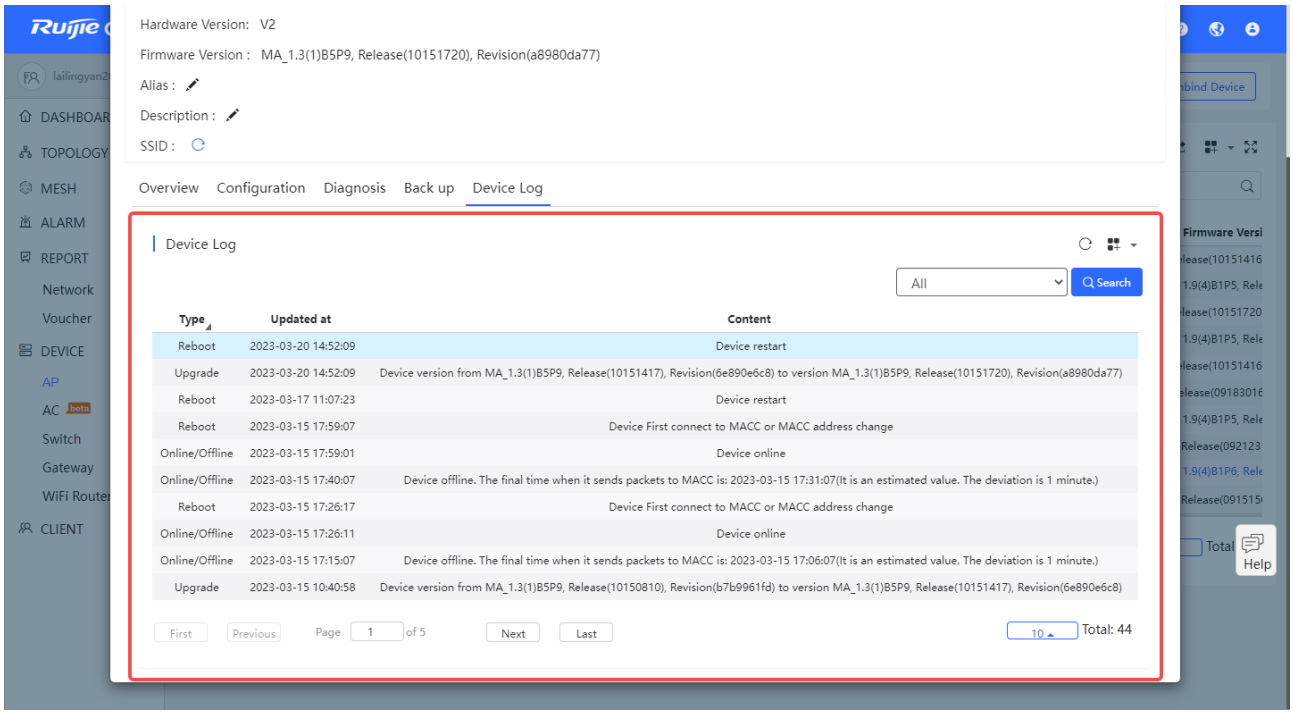


Description can be edited. Click **Details** in the **Action** column to check the backup configuration.



- Device Log

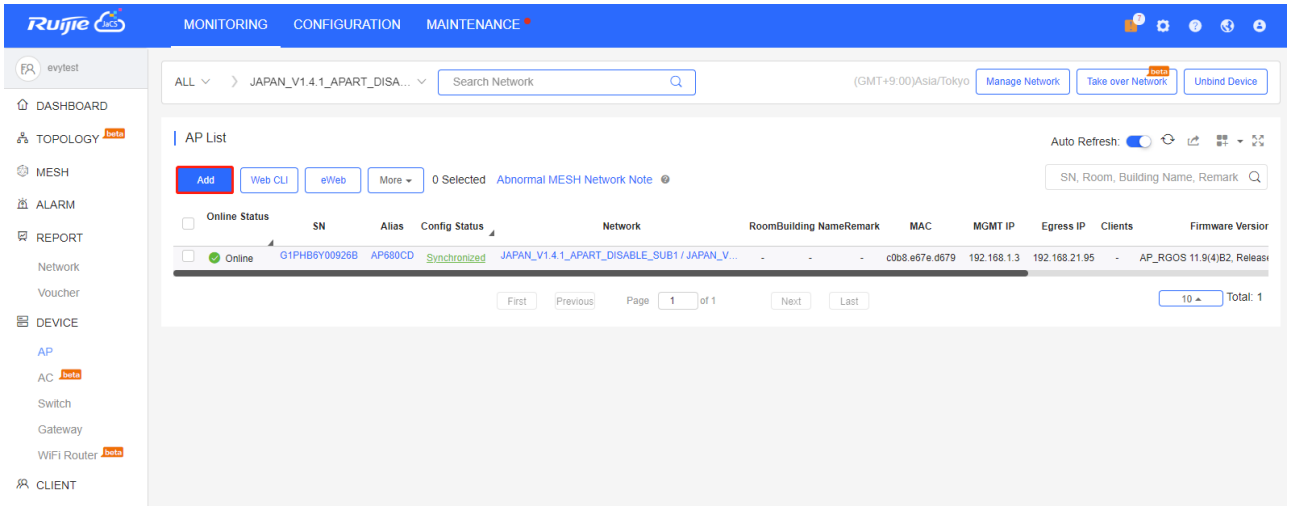
The device log records the historical operations, and currently supports the online/offline records, restart records, and upgrade records, and supports queries based on the log type and period.



5.6.1.3 Basic AP Operations

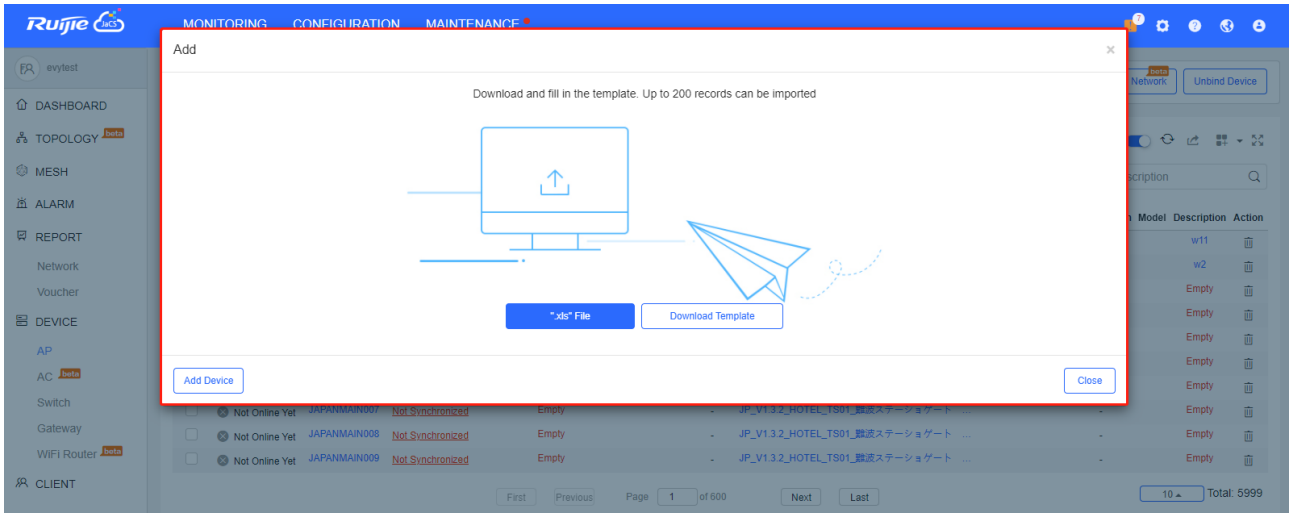
- Add AP

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

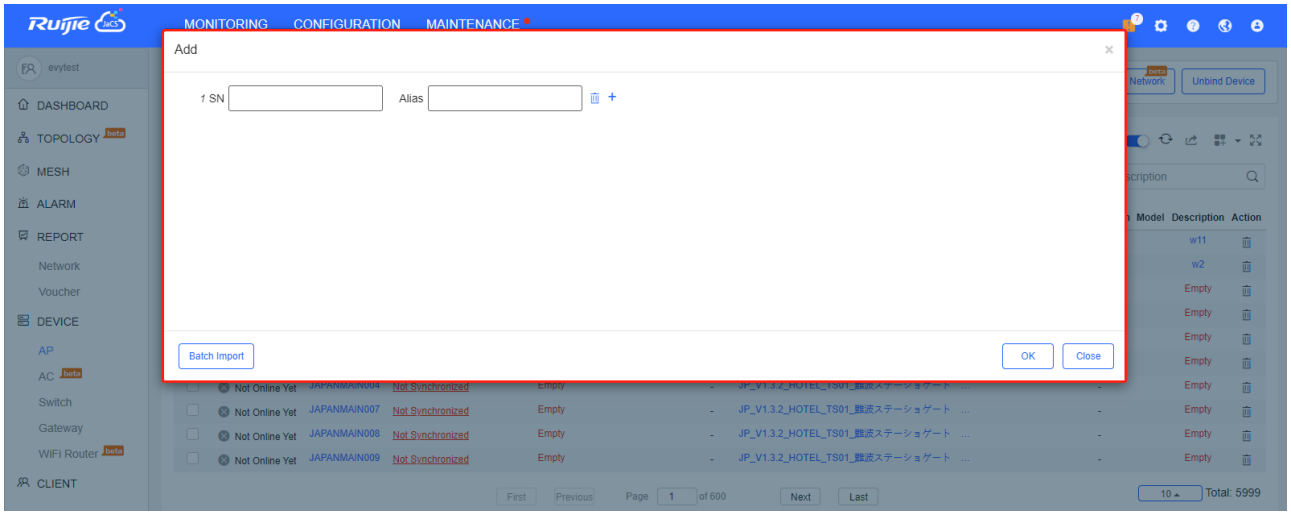


Non-apartment Scenario

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

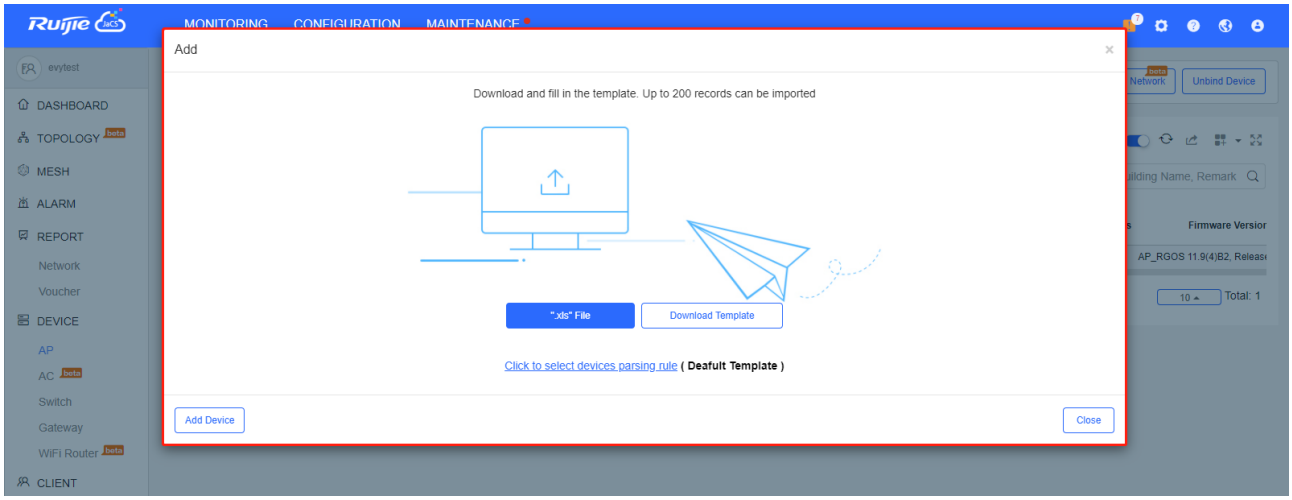


To manually add APs, click **Add a Device**, enter SN and alias of the AP, and click **OK**. Click + to add multiple APs.



Apartment Scenario

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



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**

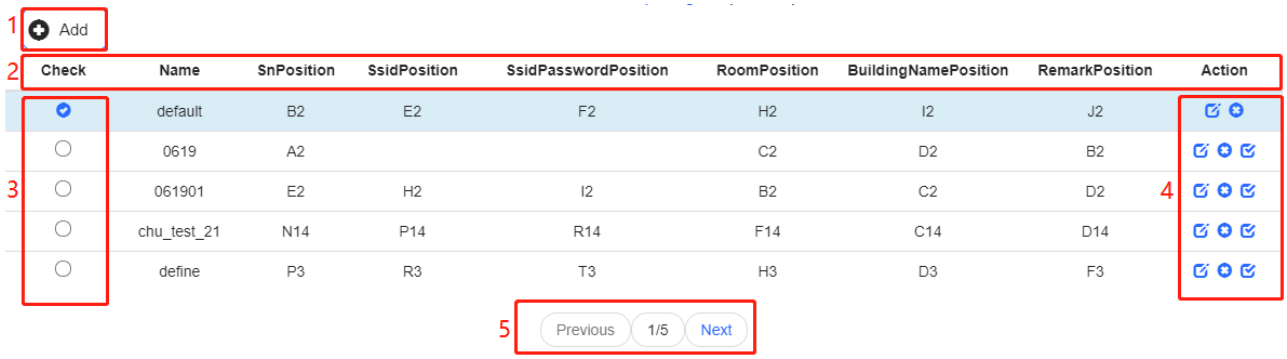
Building Name: the building that installs the device, **optional**

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.

Step 1: 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.

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

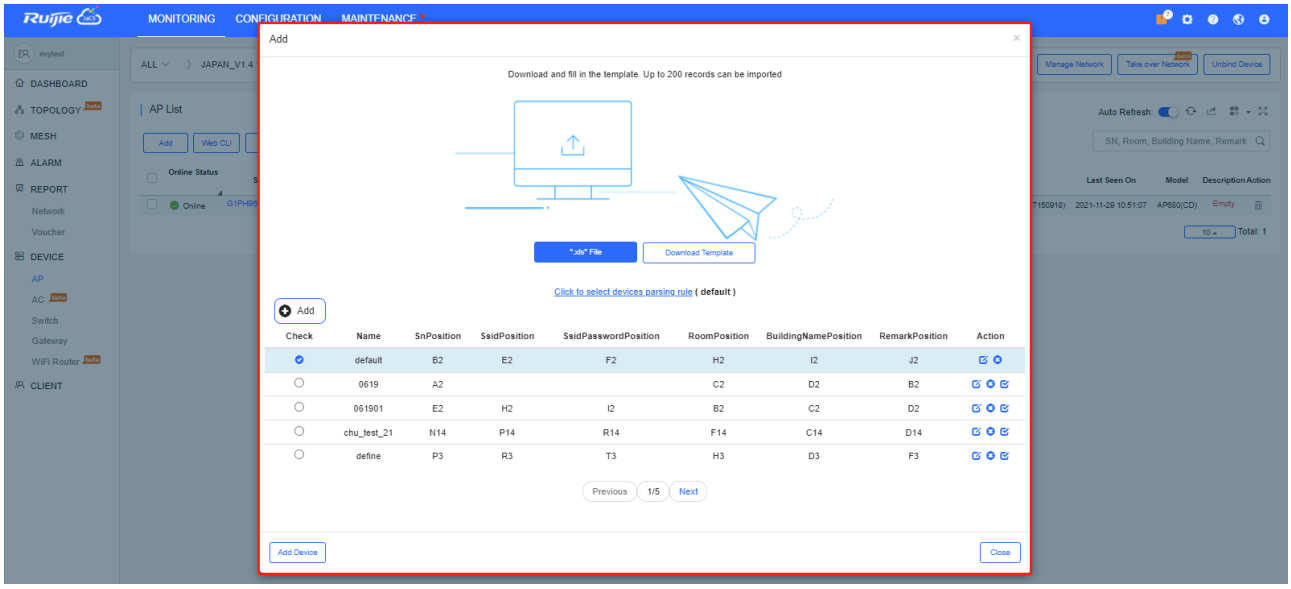
3. Check box: Only one rule can be selected at a time

4. Rule control button:

- : Edit the rule
- : Delete the rule
- : Set the rule as default rule

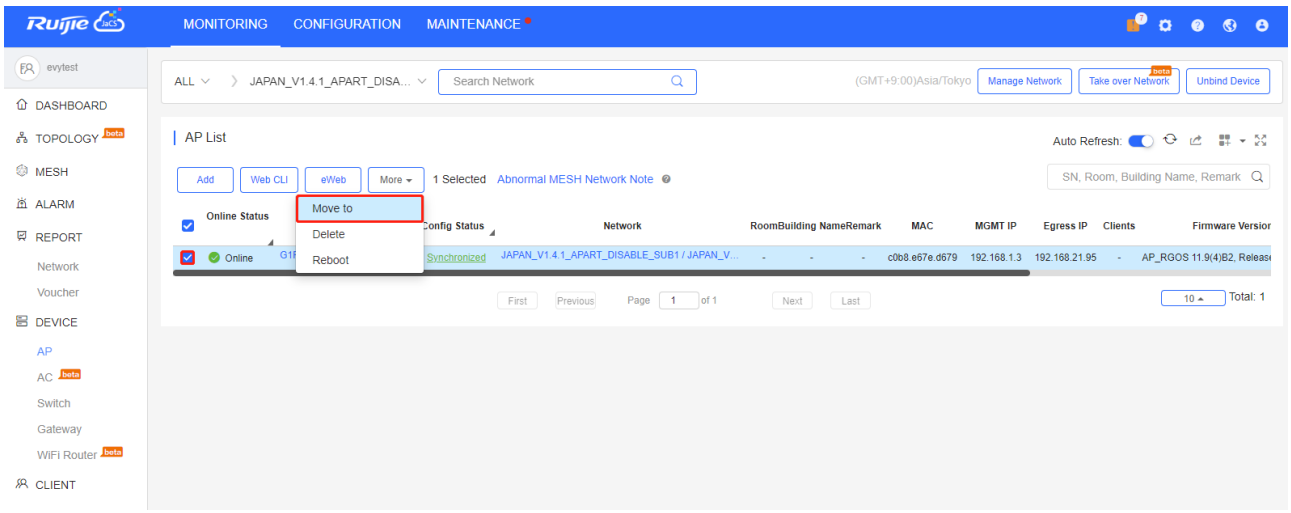
5. Page up and down button

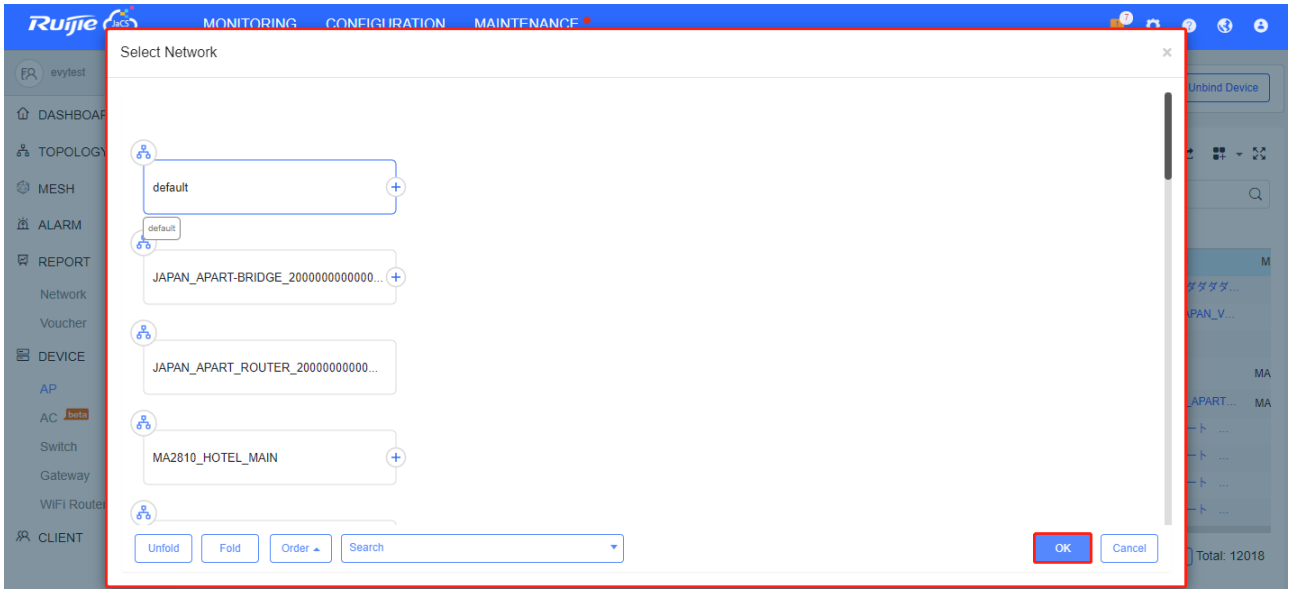
Step 2: Import device by custom EXCEL file.



- Move to

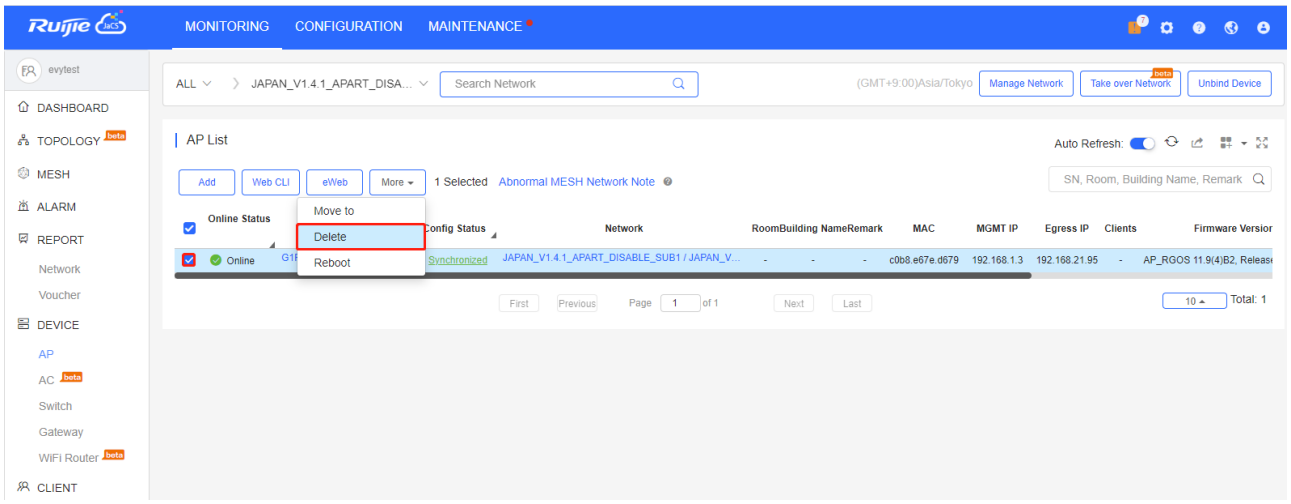
Select one or multiple devices in the **AP List**, click **More** > **Move to**, select the new network and click **OK**.





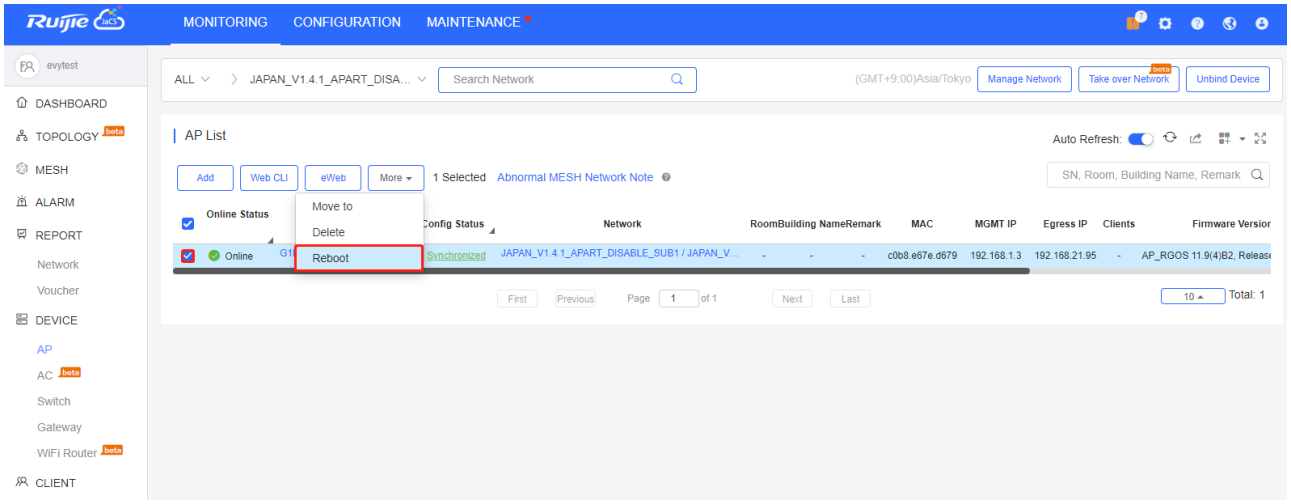
- Delete

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



- Reboot

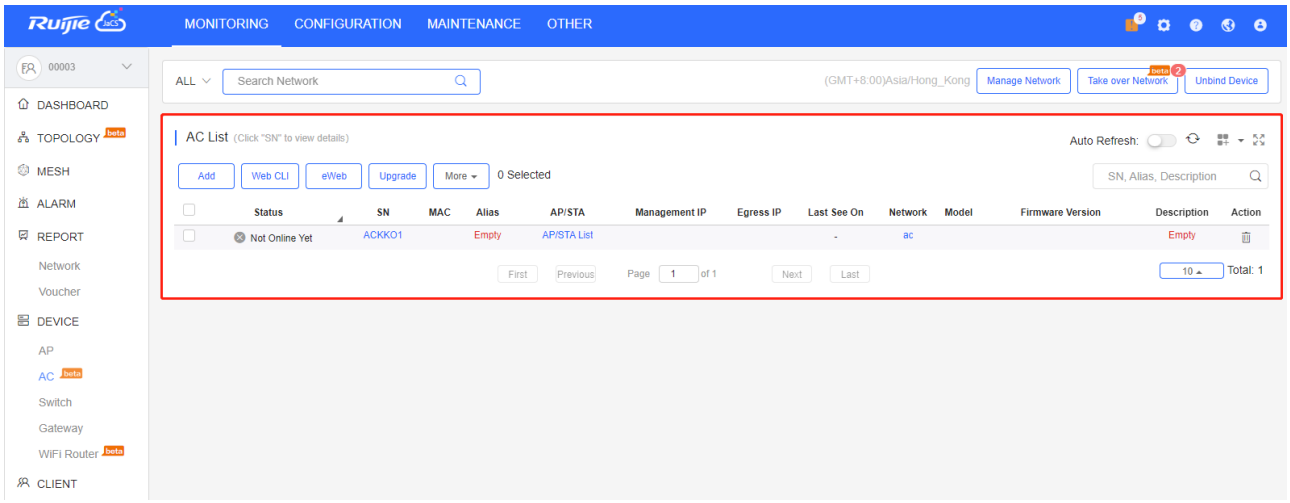
Select one or multiple devices in the **AP List**, and click **Reboot.**



5.6.2 AC (beta)

5.6.2.1 AC List

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



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

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

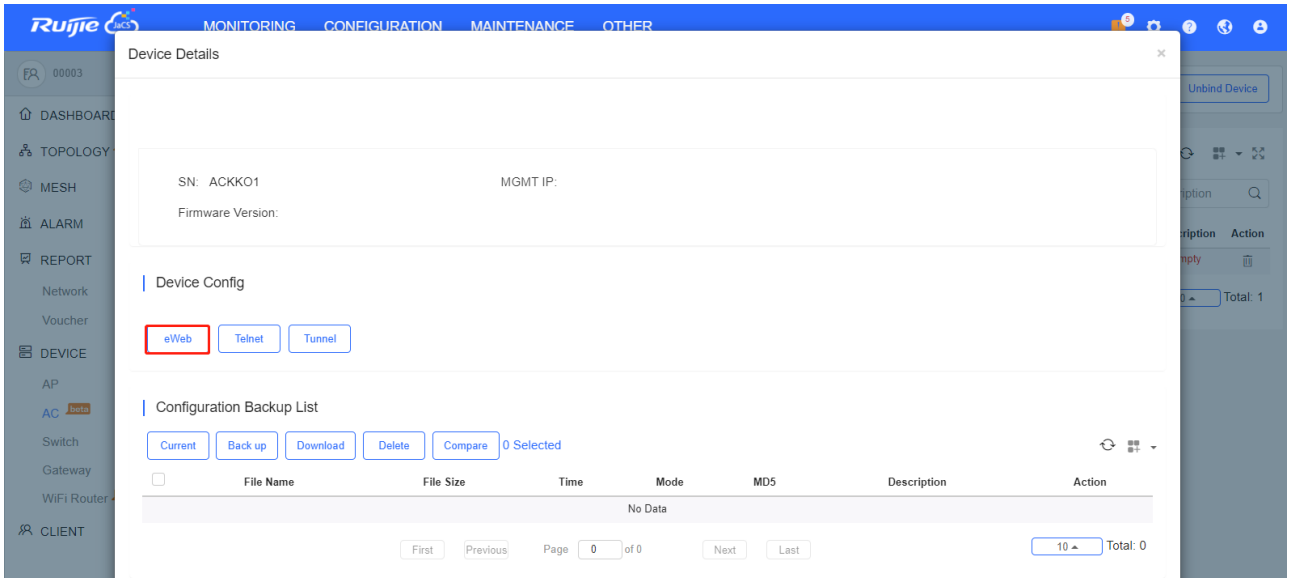
The **Search** function supports fuzzy queries based on the serial number, alias and description.

5.6.2.2 Device Details

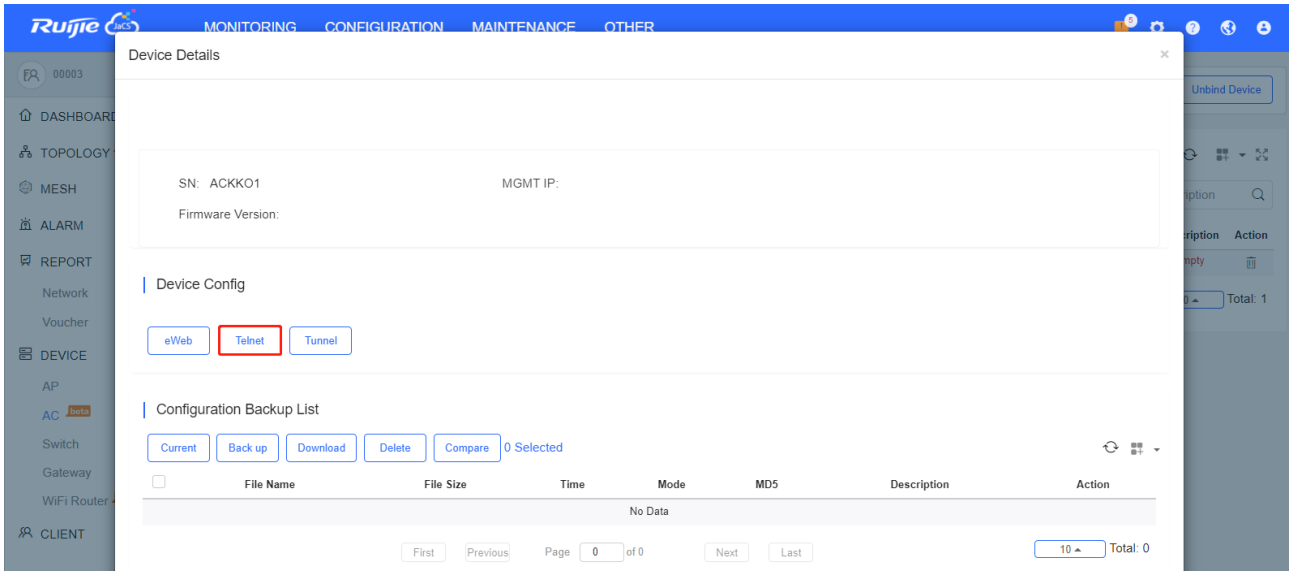
Click the serial number in the device list to open the details page for a single device.

- eWeb

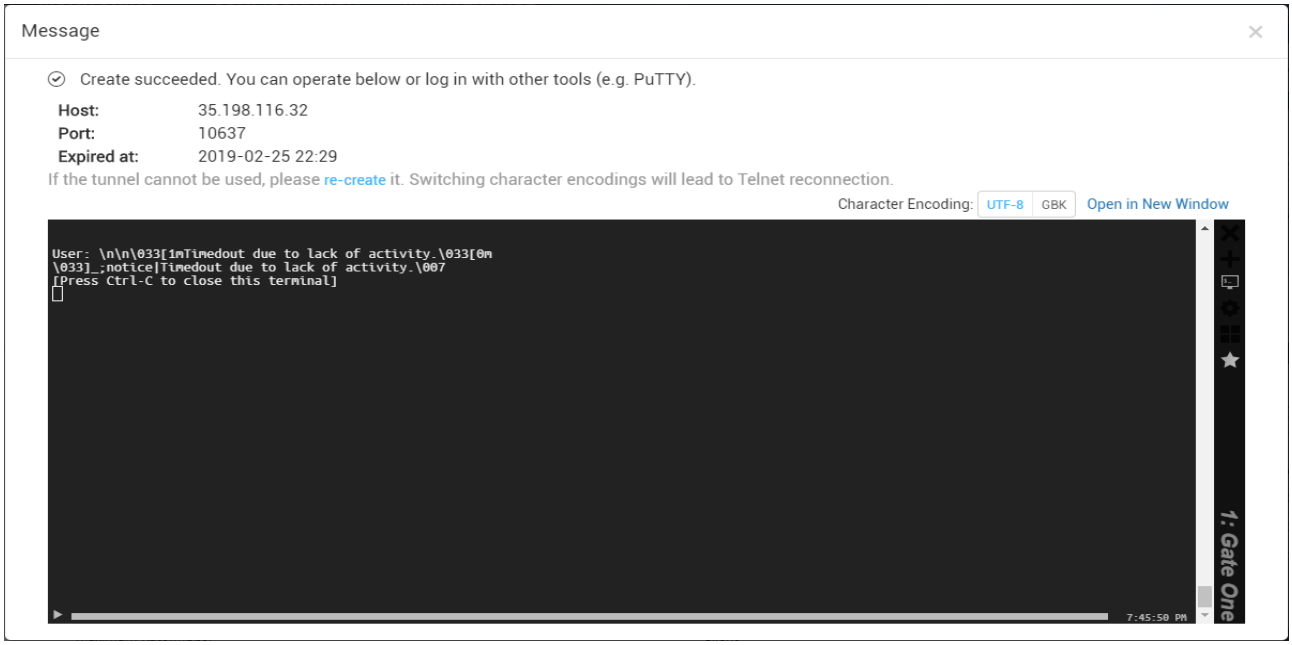
Click **eWeb** to open the eWeb system in a new window.



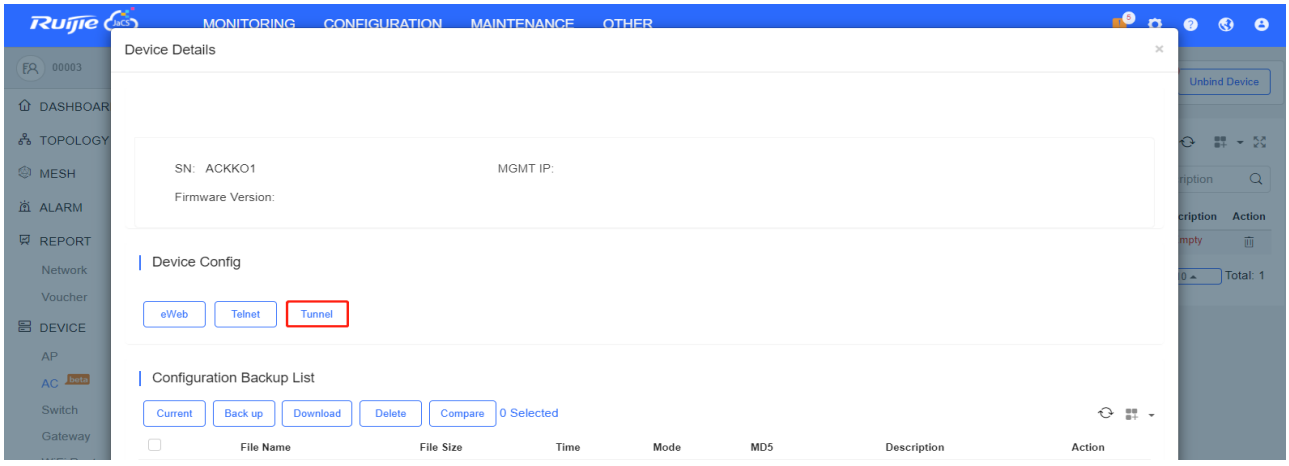
- Telnet



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

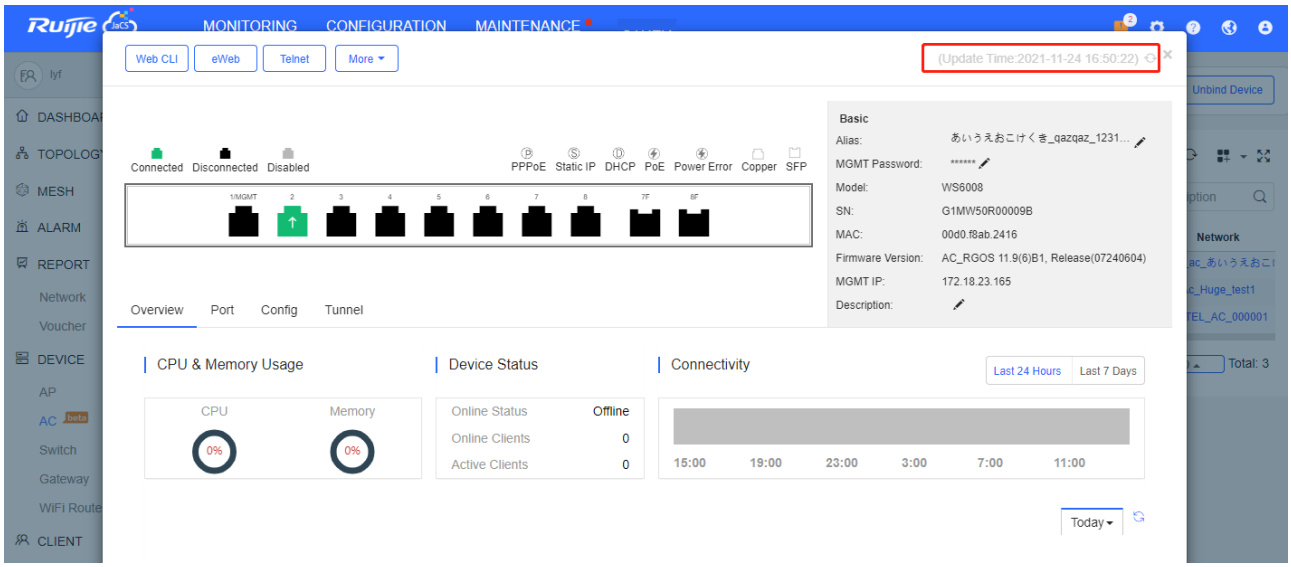


- Tunnel

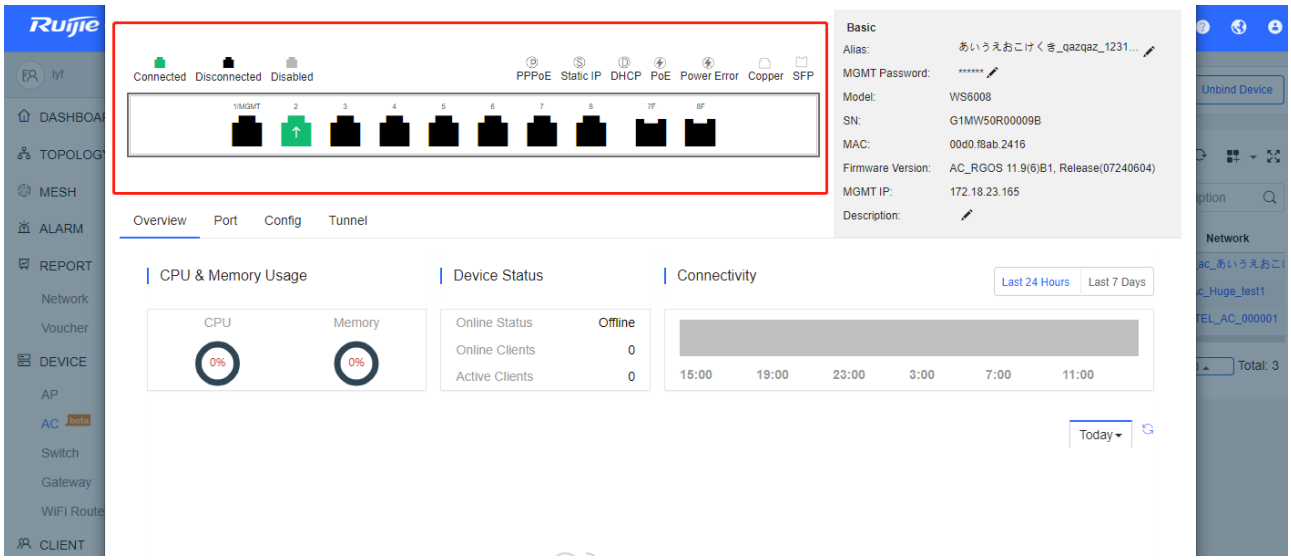


- Refresh

Click to refresh all data in the page.

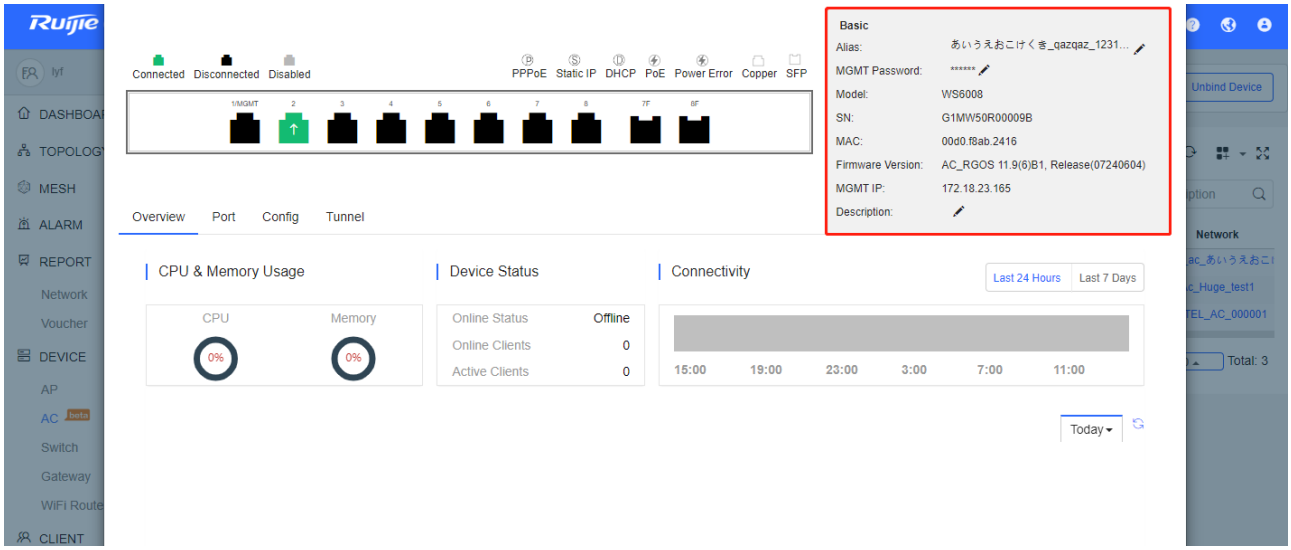


- Port Panel



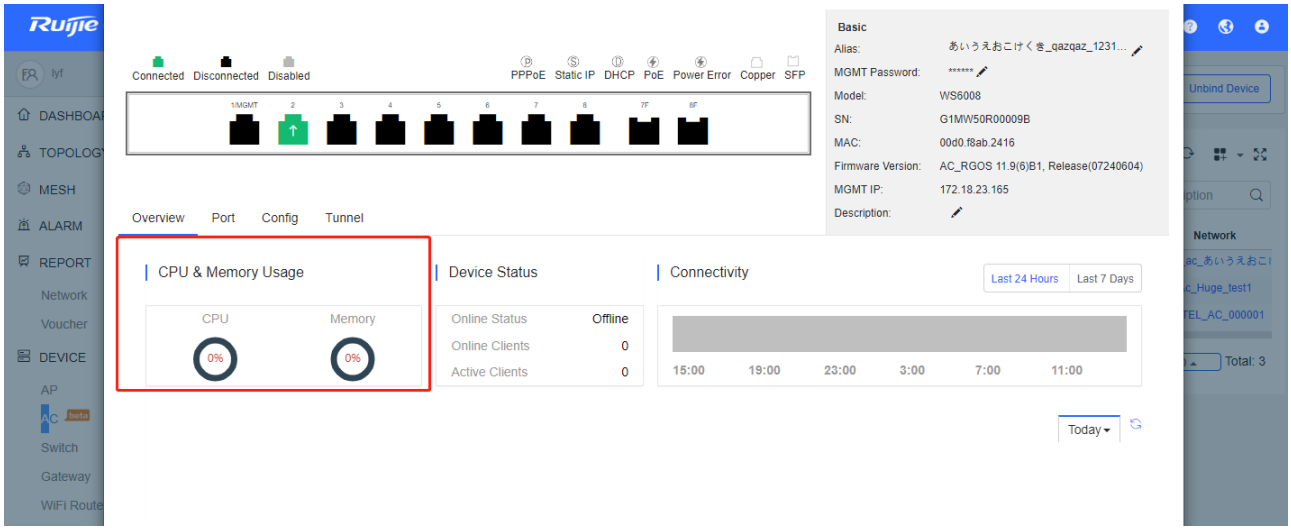
The port panel imitates the actual AC panel, displaying the port type and status.

- Basic



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

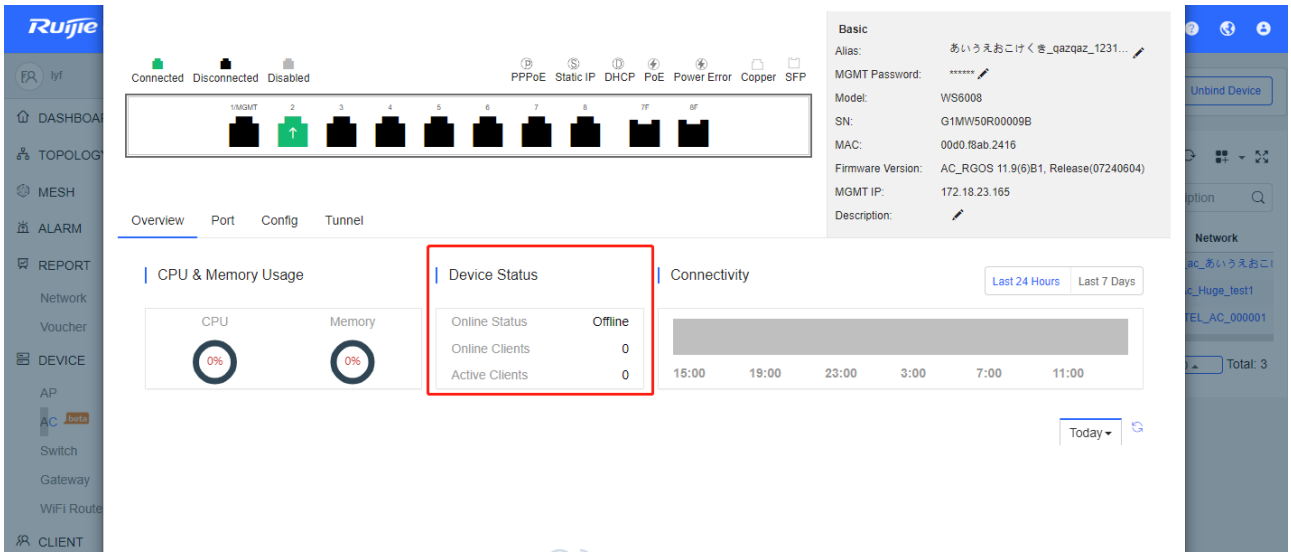
- Overview > CPU & Memory Usage



CPU & memory usage are displayed here.

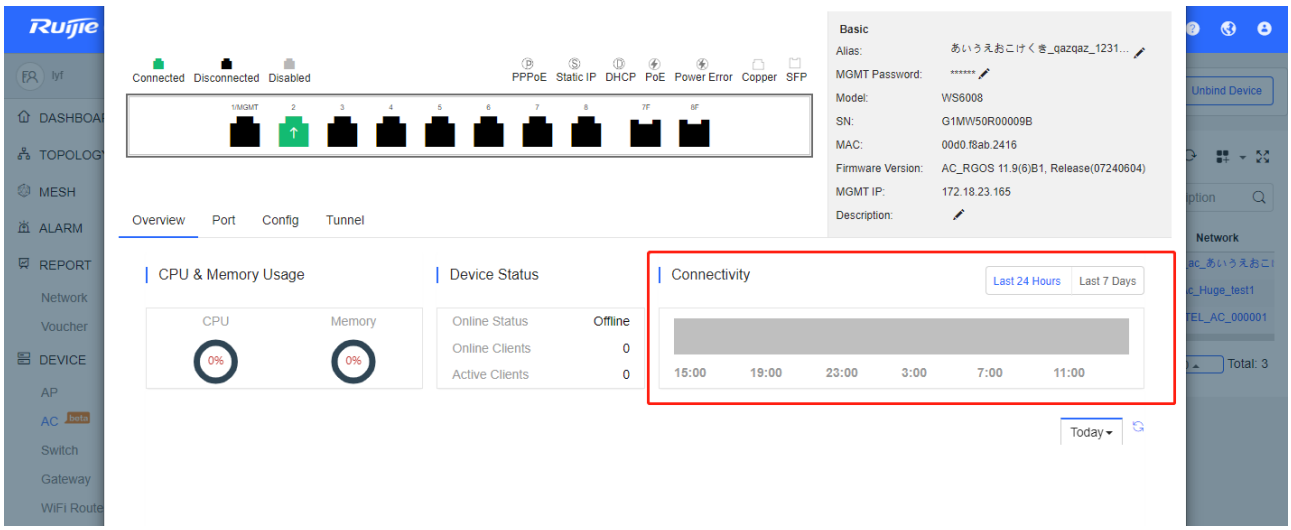
- Overview > Device Status

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



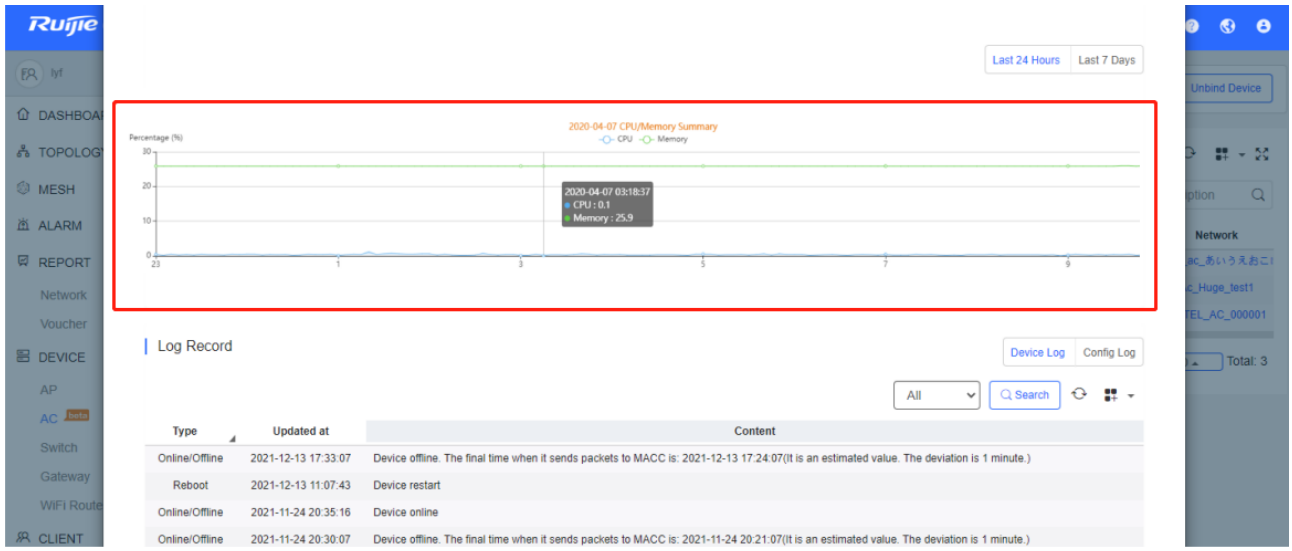
- Overview > Connectivity

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



- Overview > CPU/Memory Summary

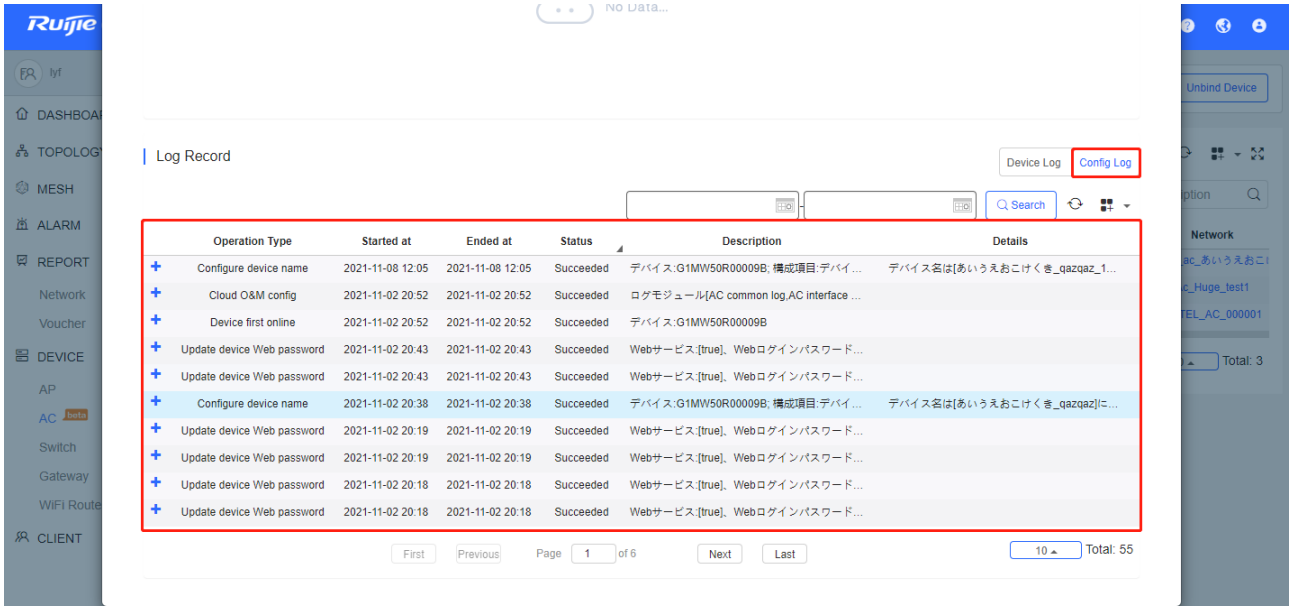
CPU/memory summary over the 24 hours are displayed.



- Overview > Device Log

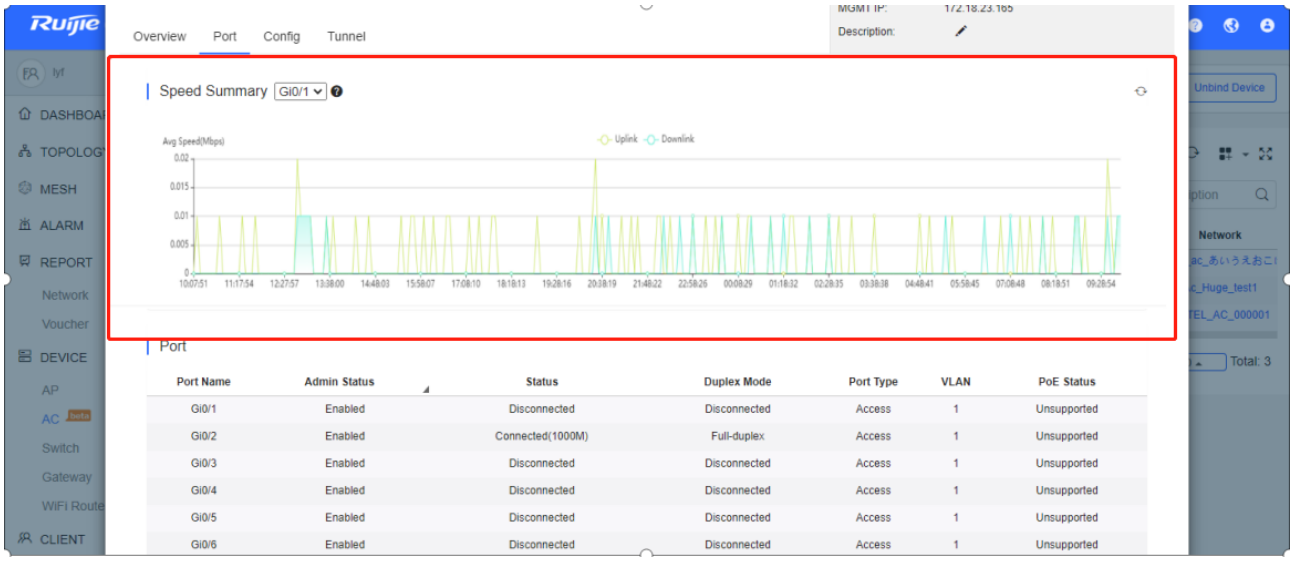
The device log records the historical operations, including online/offline, restart, upgrade and VLAN change, and supports queries based on log type and time.

- Overview > Config Log



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

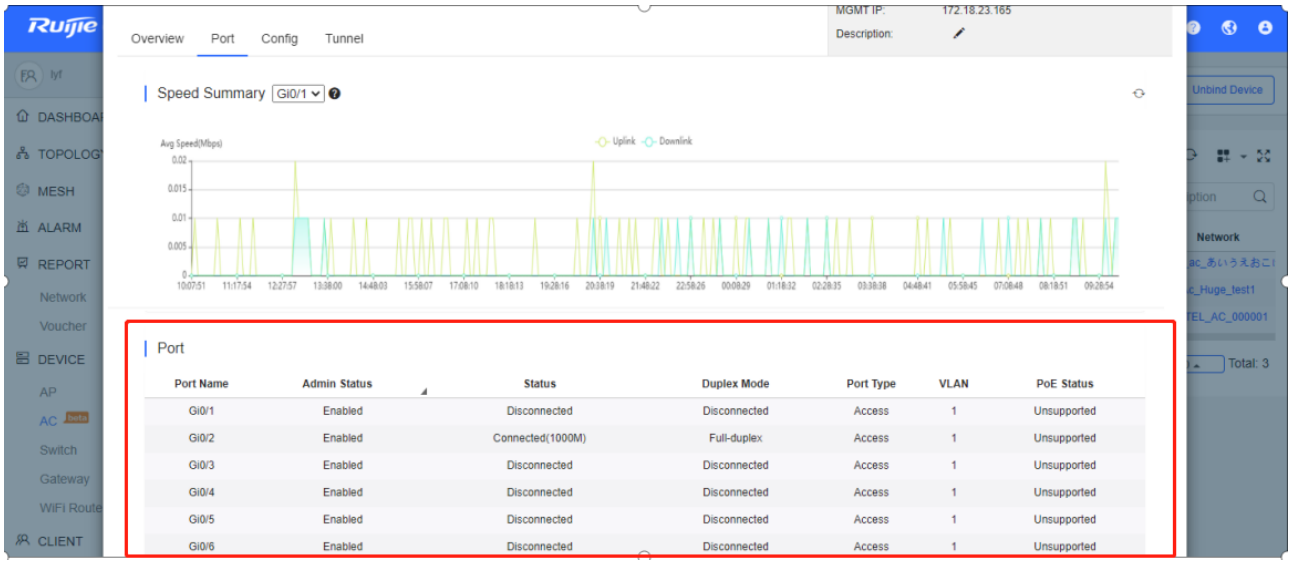
- Port > Speed Summary



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

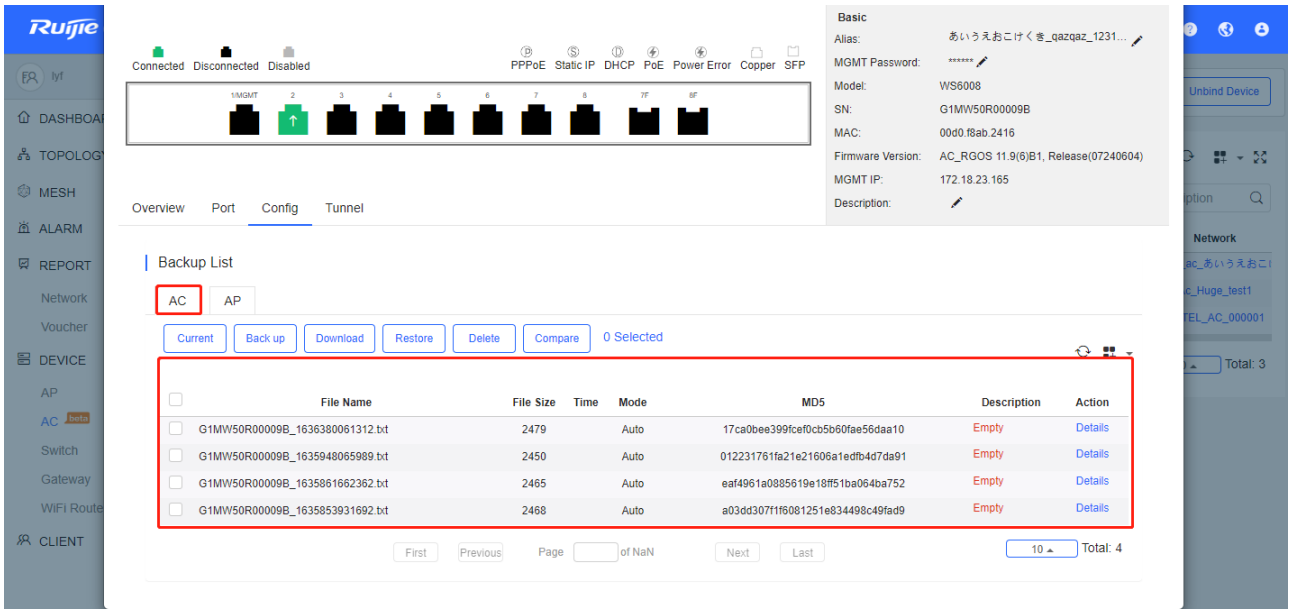
- Port > Port Status

Port information includes port name, VLAN etc.

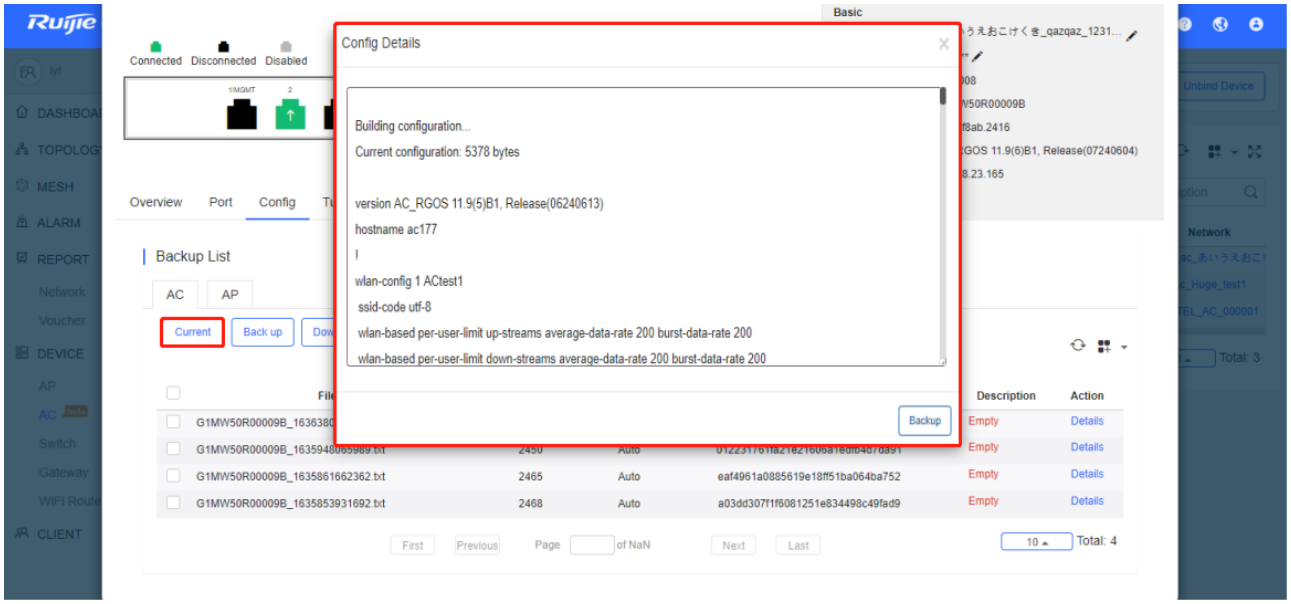


- Config > AC Configuration Backup List

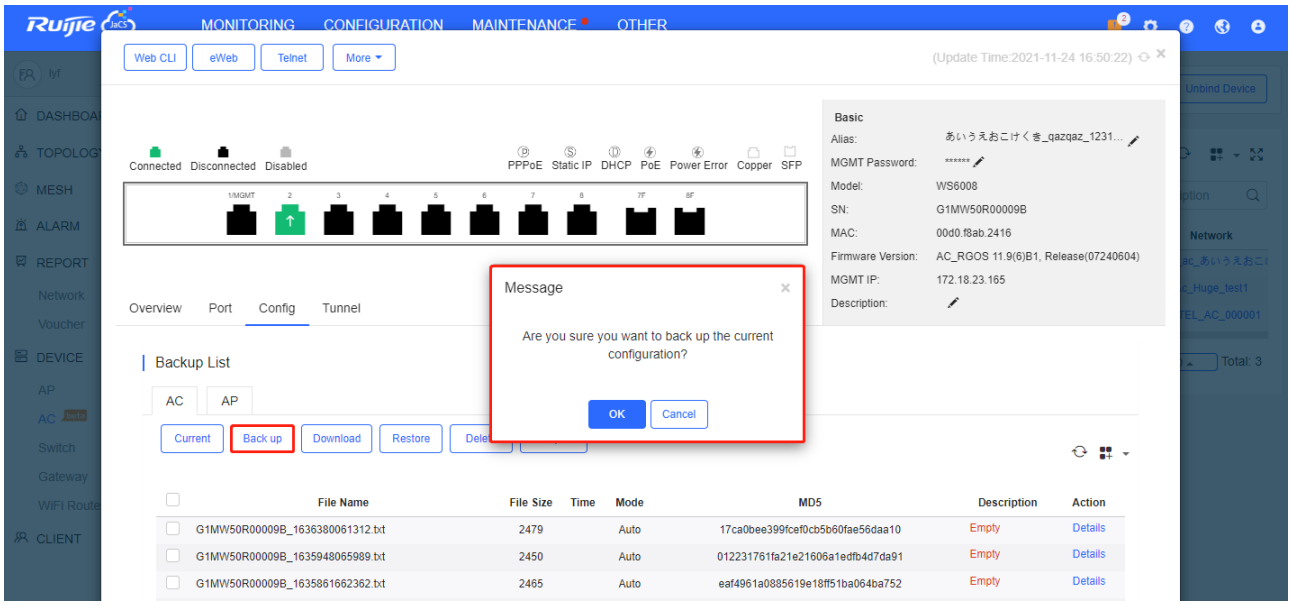
The backup records include configuration file name, size, time, mode and MD5.



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



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

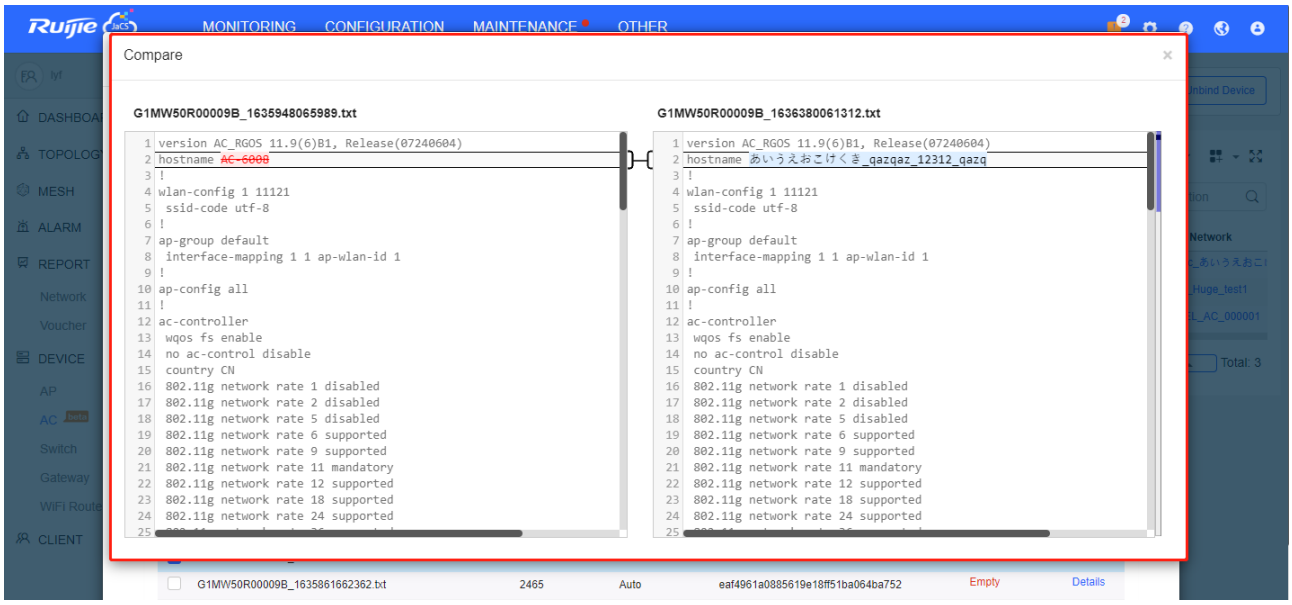


Select one record, and click **Download** to download the configuration file.

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

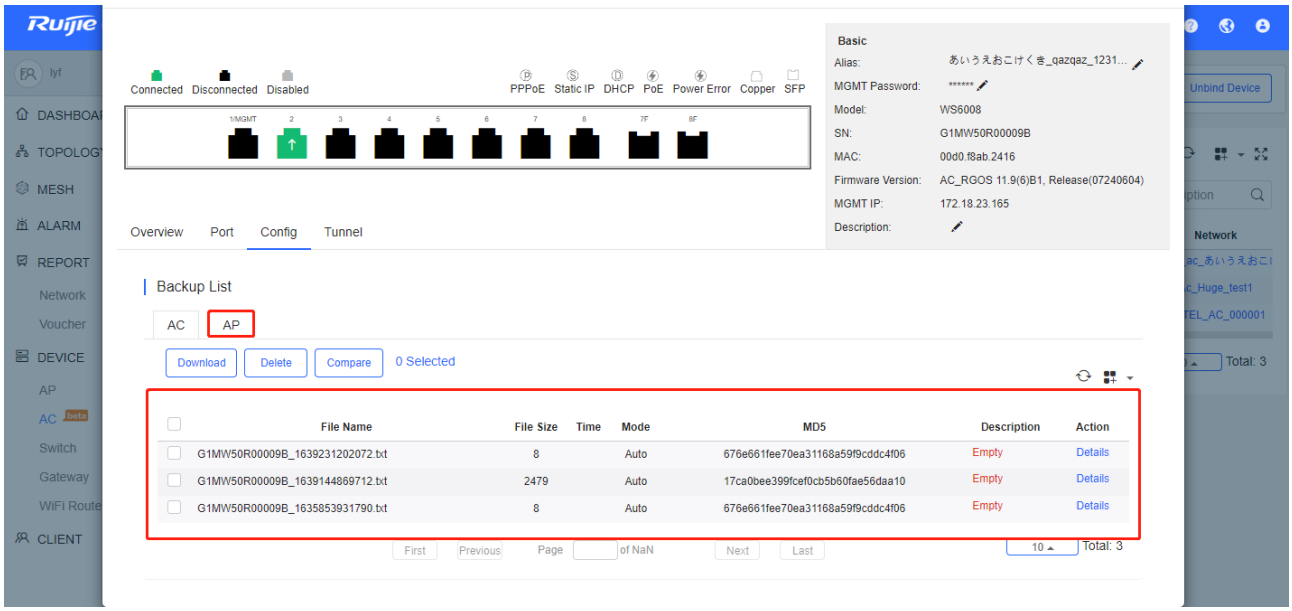
Select one or multiple records, and click **Delete** to delete the backup record.

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



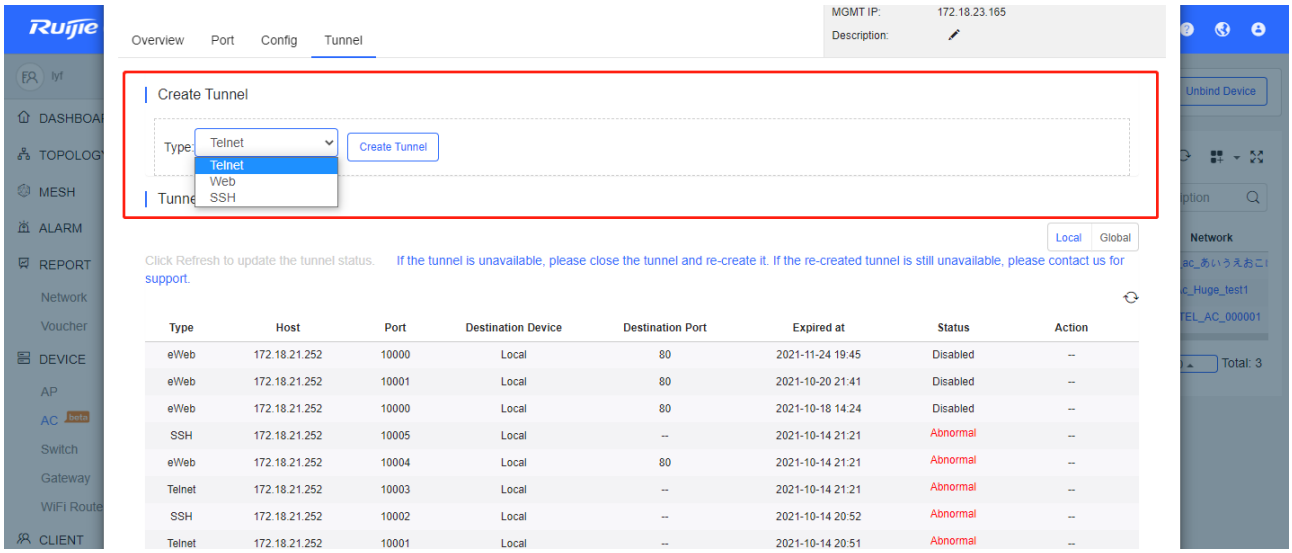
- Config > AP Configuration Backup List

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



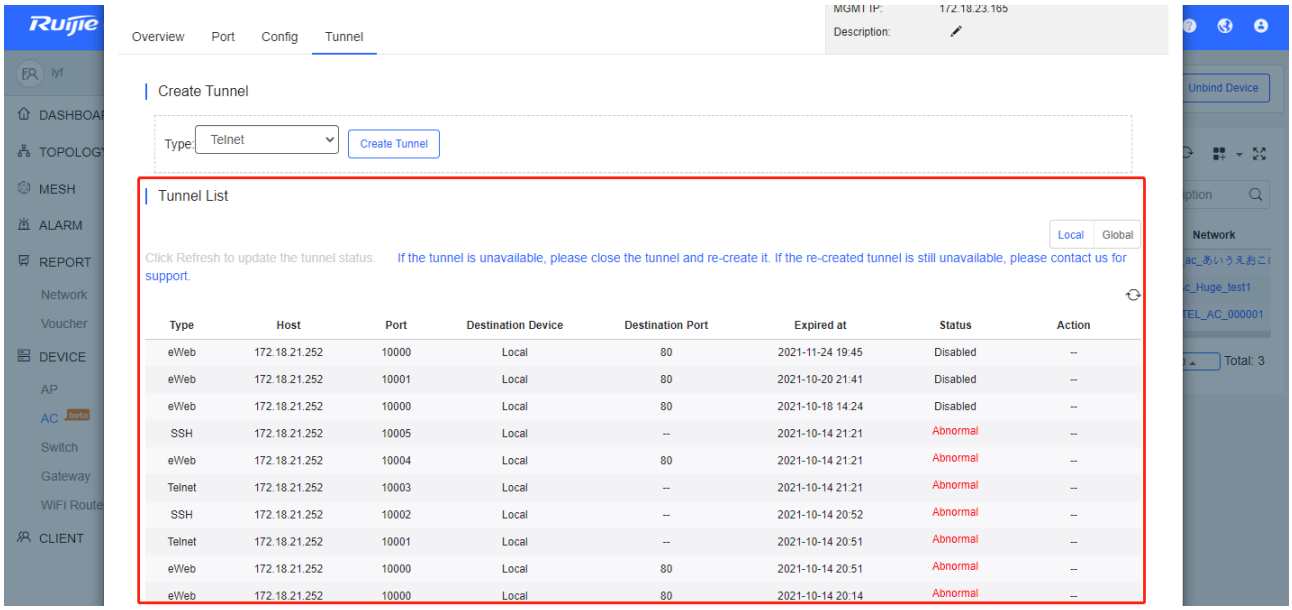
- Tunnel > Create Tunnel

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



- Tunnel > Tunnel List

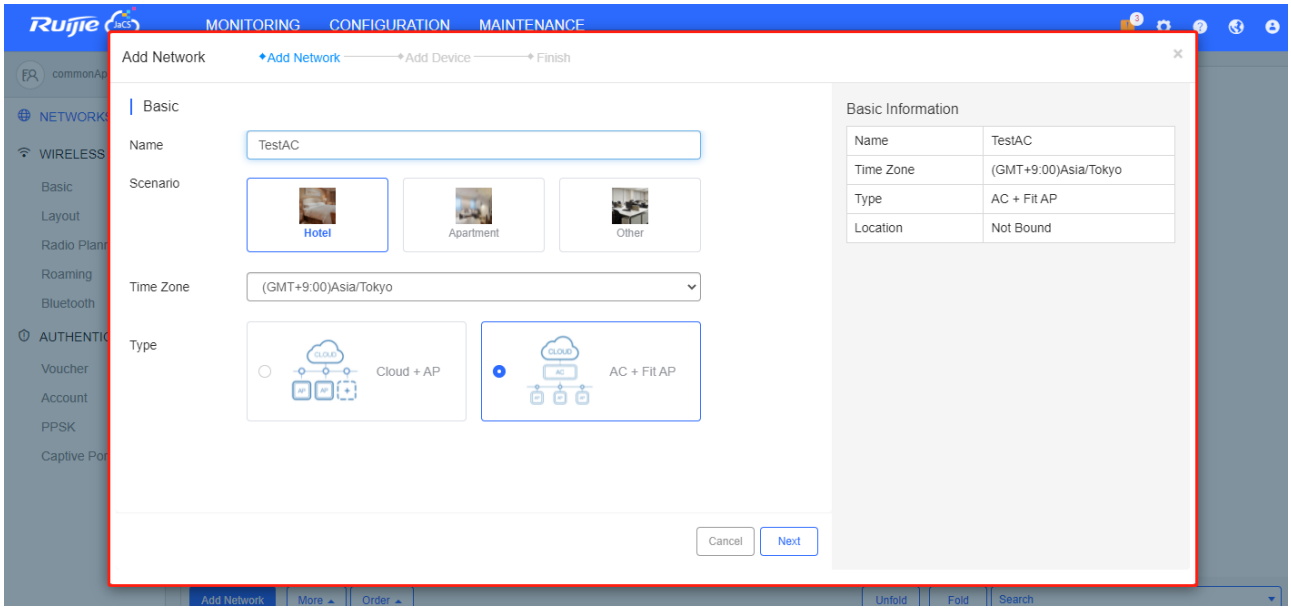
Tunnel information includes tunnel type, host, port, destination device, destination port, expiration time and status. Click **Re-create** in the **Action** column to re-create a tunnel.



5.6.2.3 Basic AC Operations

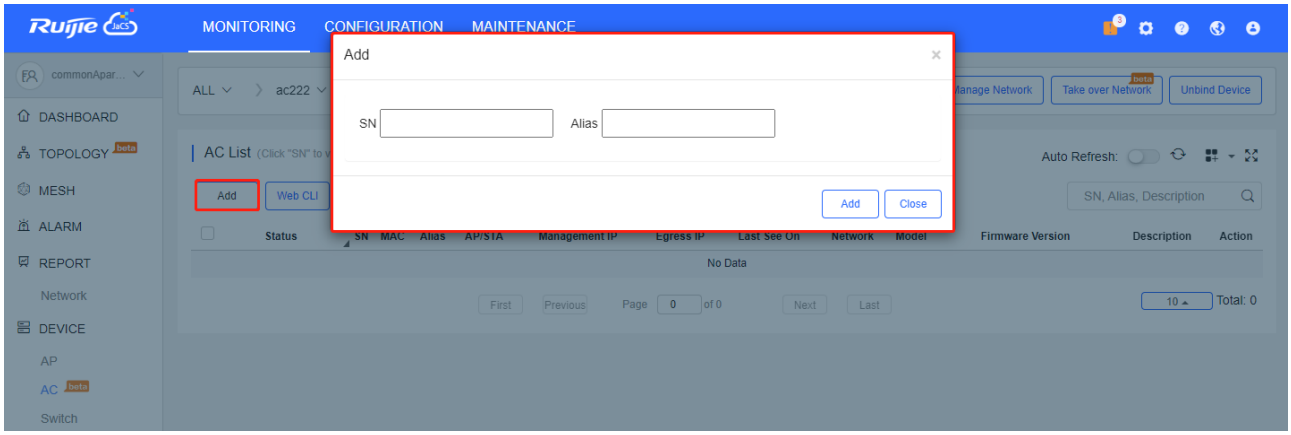
- Add AC Network

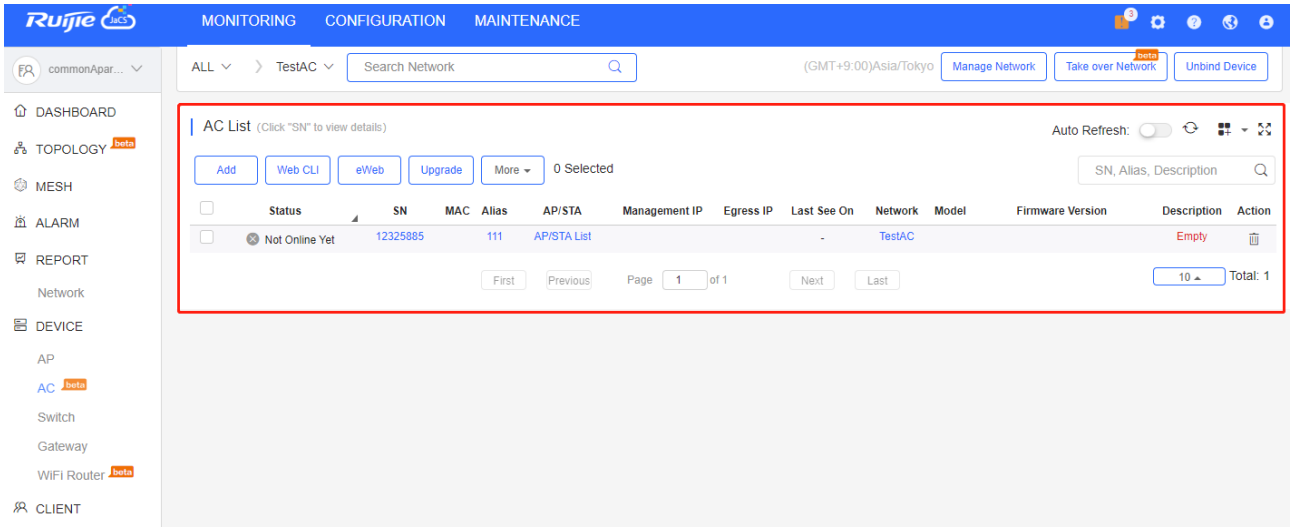
Click **CONFIGURATION** > **NETWORKS** > **Add Network** to add AC network.



- Add

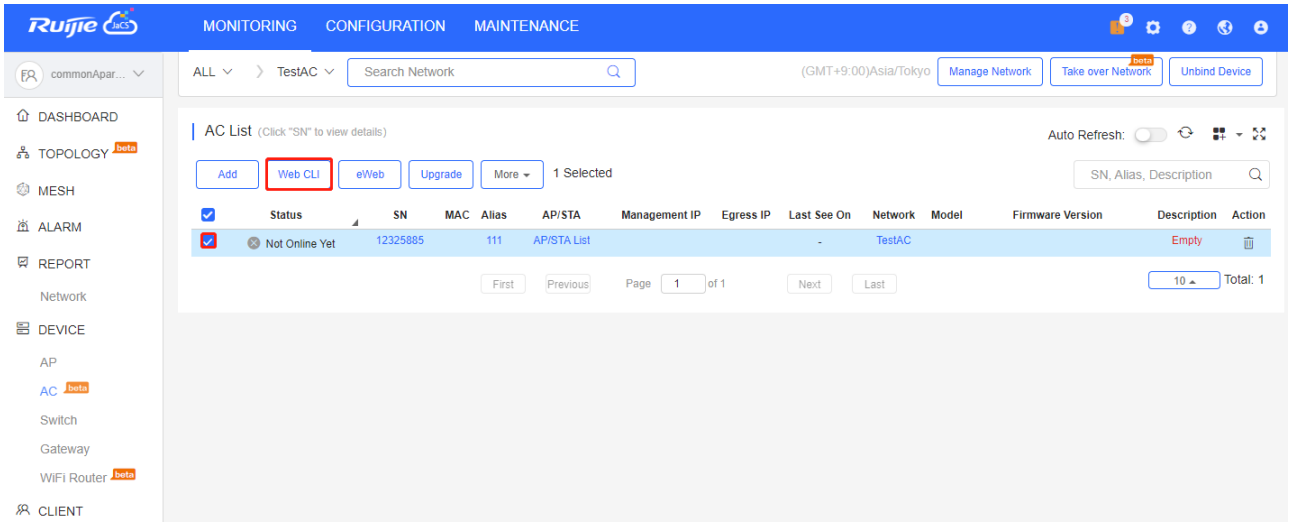
Click **Add**, enter the SN and Alias, and click **OK** to add an AC to the network. Only one AC can be added to a network.



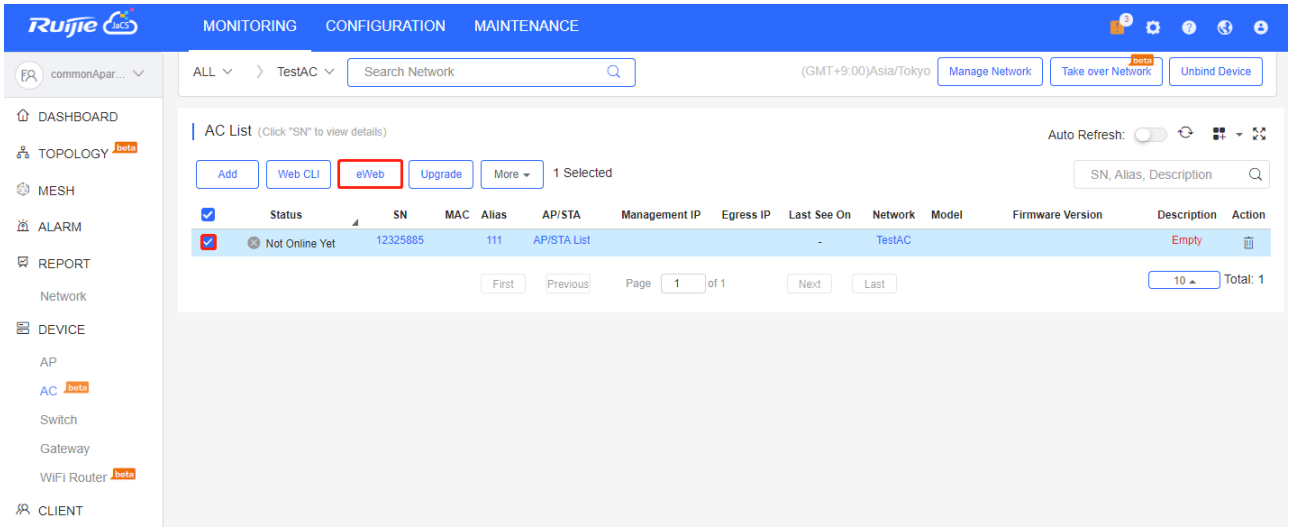


- Web CLI

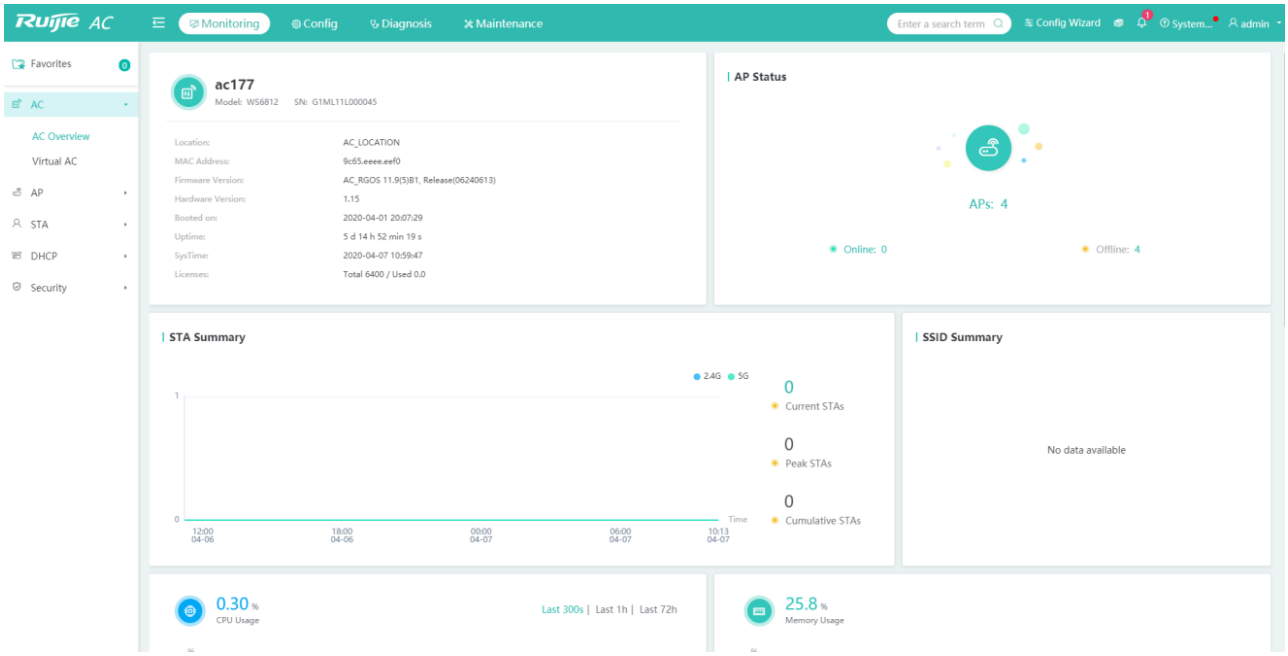
Select the device to be managed by CLI command, click **Web CLI.** The **Web CLI** page provides commonly-used CLI commands on the left. Click the command, or manually enter the command and click **Send**. Only one AC can be configured at a time.



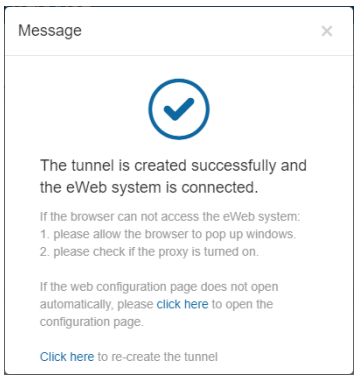
- eWeb



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

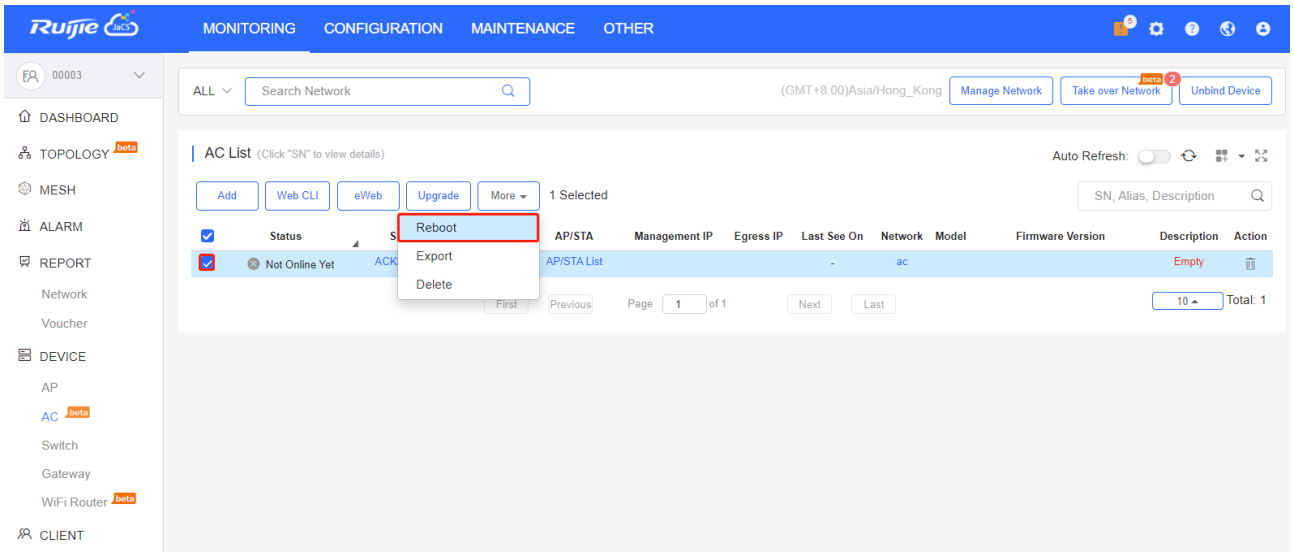


If a tunnel is created successfully but the eWeb page does not automatically open, a message is displayed as below. The user can manually click the link to open the page.



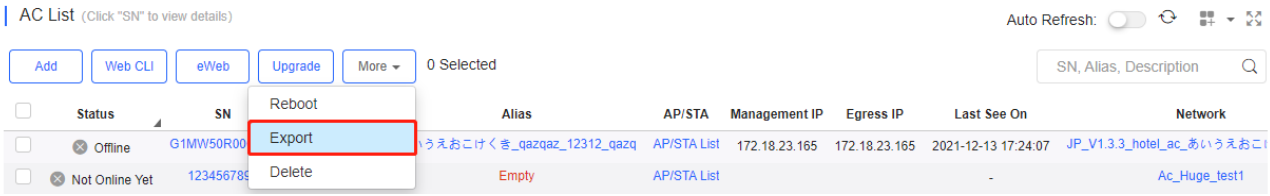
- More > Reboot

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



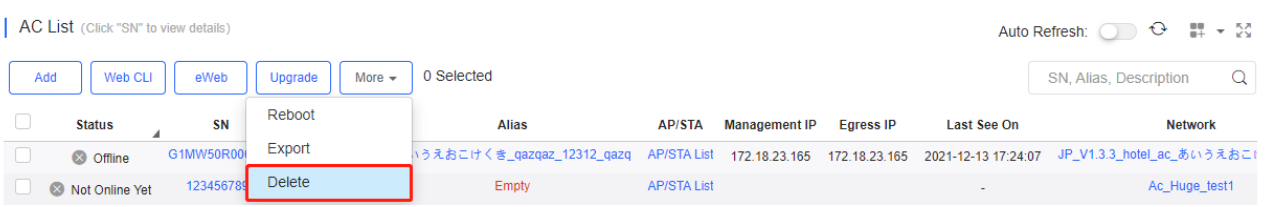
- More > Export

Select the device in the **AC List**, click **More** > **Export**.



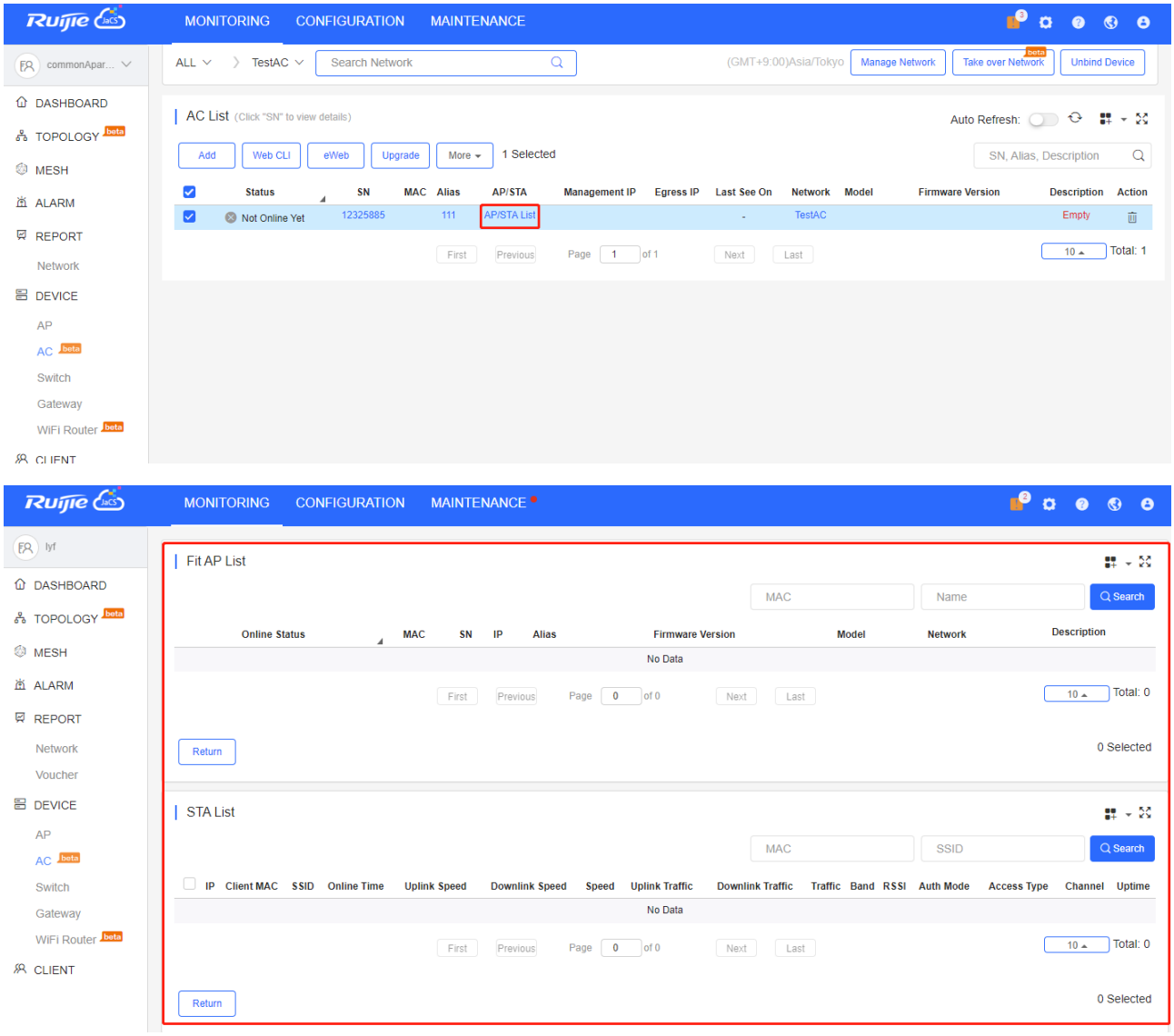
- More > Delete

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



5.6.2.4 AP / STA List

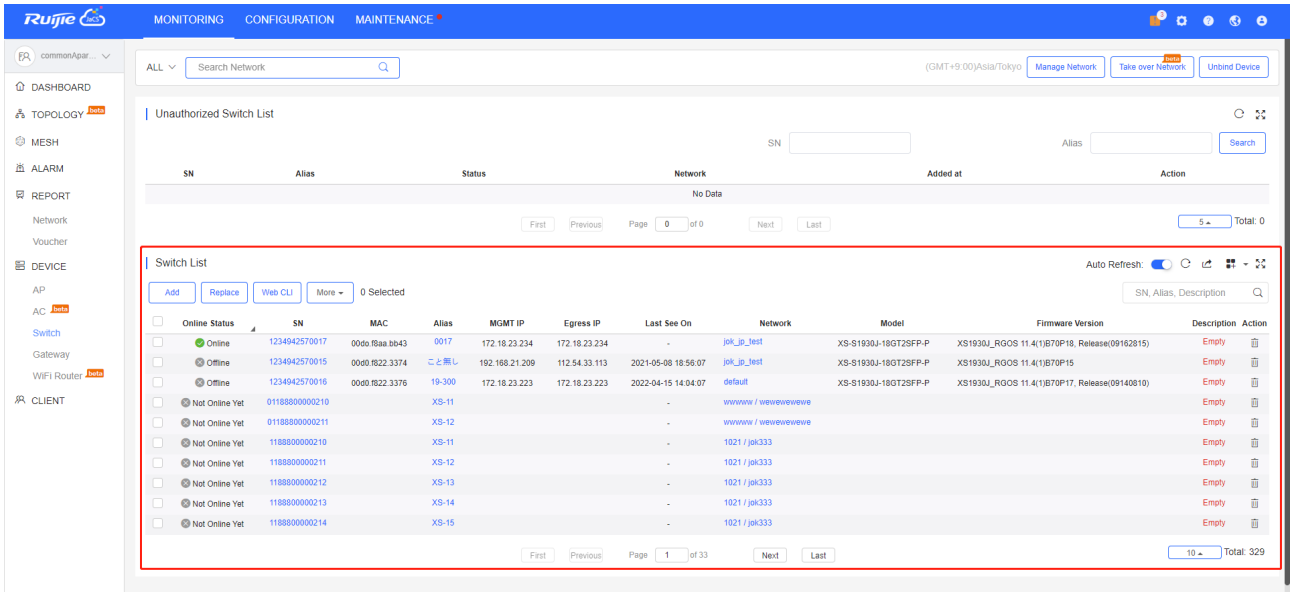
Click **AP/STA List** to display AP and STA list.



5.6.3 Switch

5.6.3.1 Switch List

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 Auto Refresh: to enable/disable the auto refresh function.

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

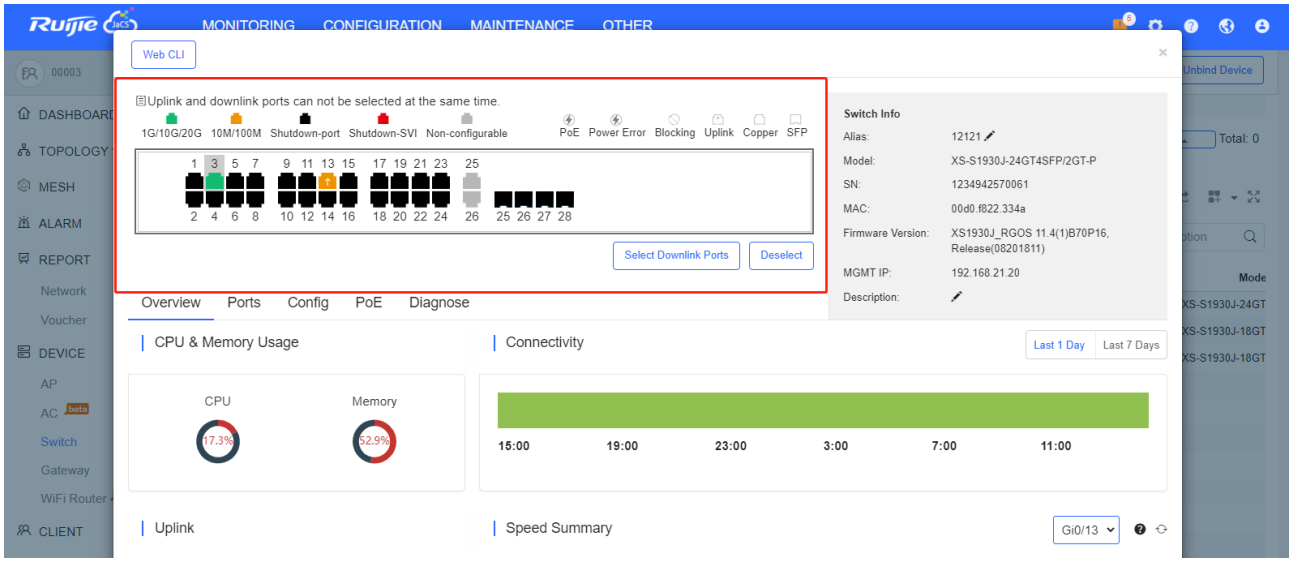
The **Search** function supports fuzzy queries based on the serial number, alias and description, and also supports queries based on online/offline status.

5.6.3.2 Device Details

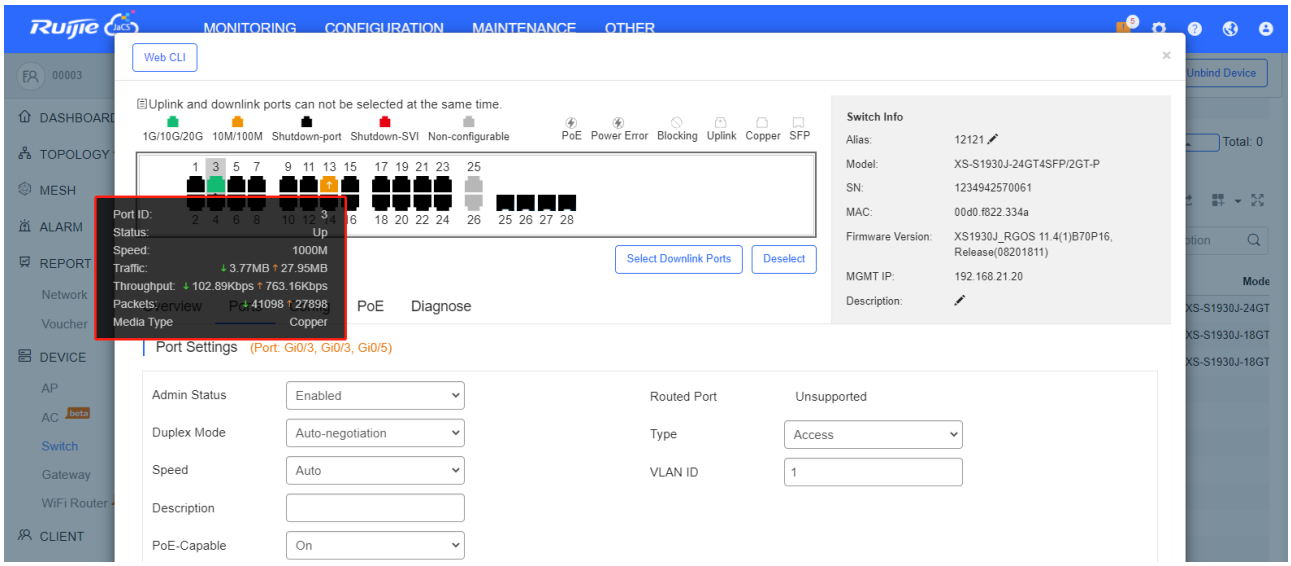
Click the serial number in the device list to open the details page of a single device. The page displays detailed device information, including the port panel, basic information, overview, ports, config, PoE and diagnosis.

- Port Panel

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

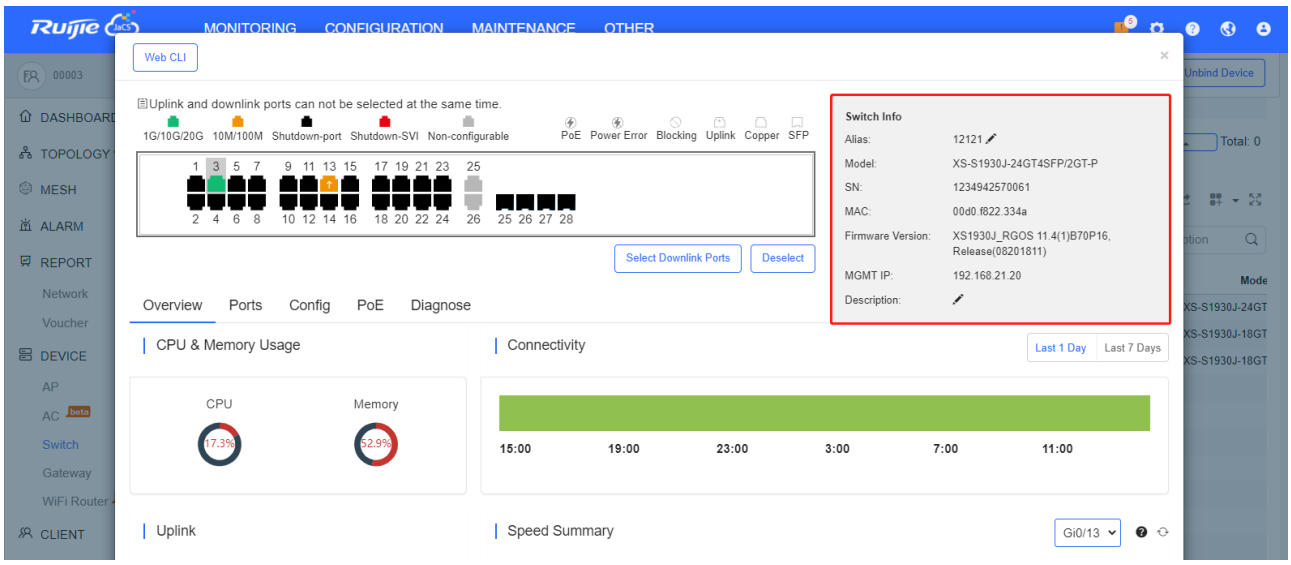


When you point the mouse to a port, the traffic, speed and other information of the port will be displayed.

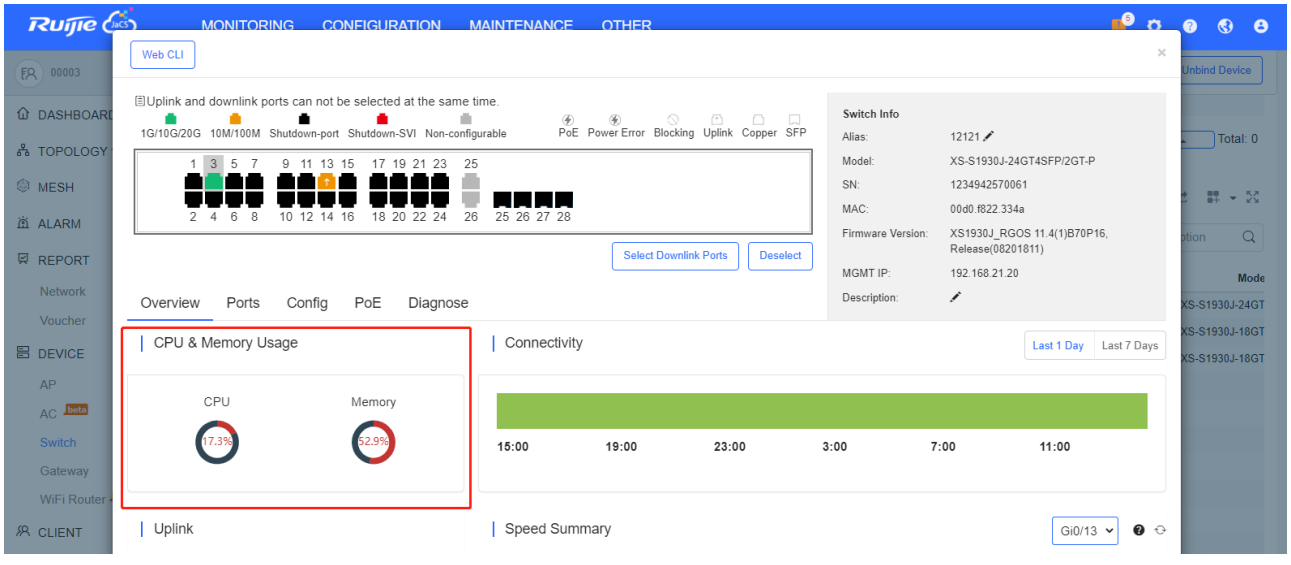


- Switch Info

Switch information includes the alias, model, SN, MAC address, firmware version, management IP and description. **Alias** and **Description** can be edited.

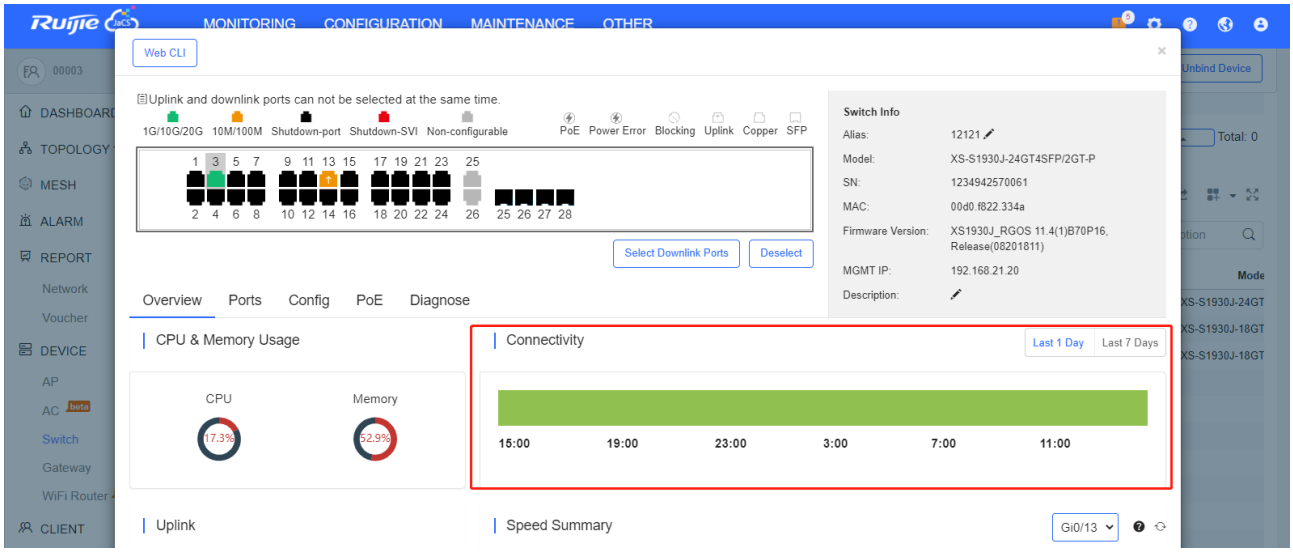


- Overview > CPU & Memory Usage

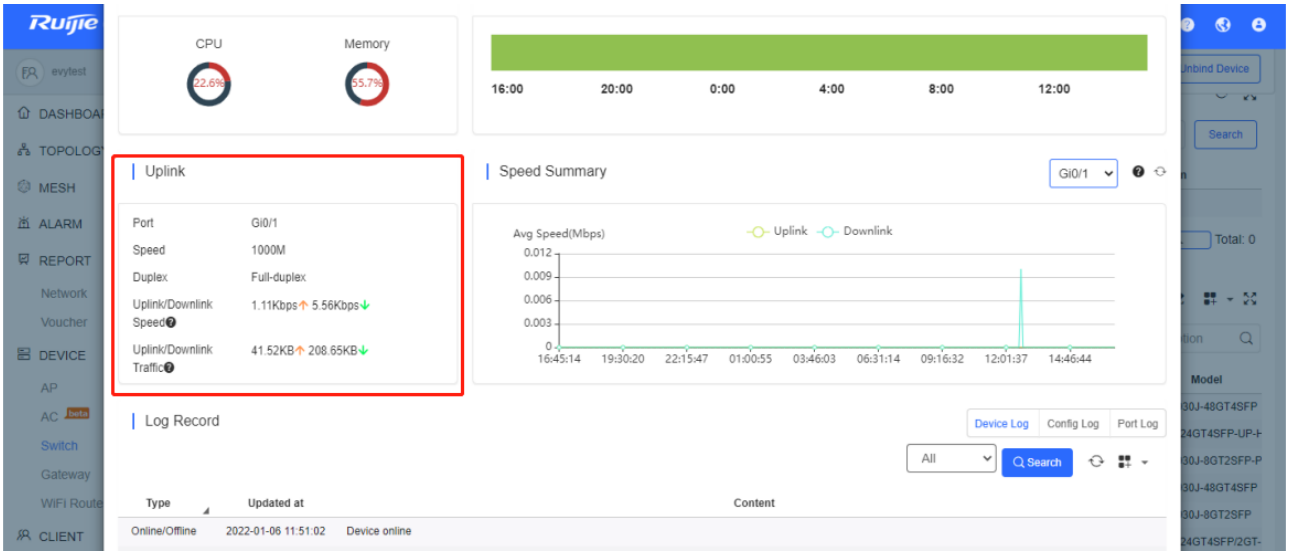


- Overview > Connectivity

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



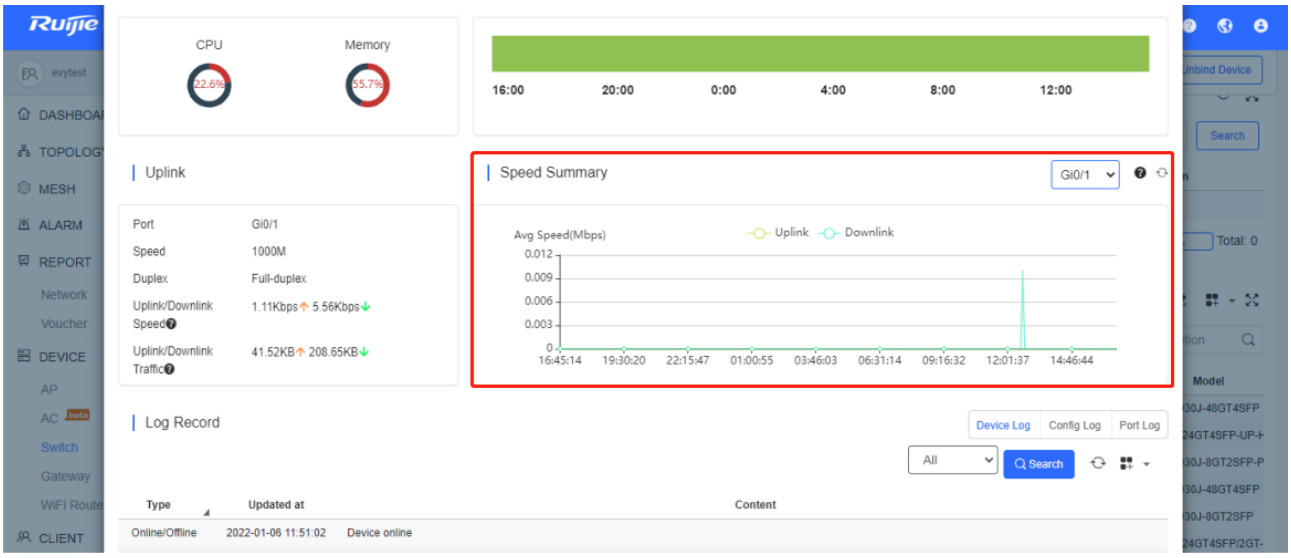
- Overview > Uplink



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

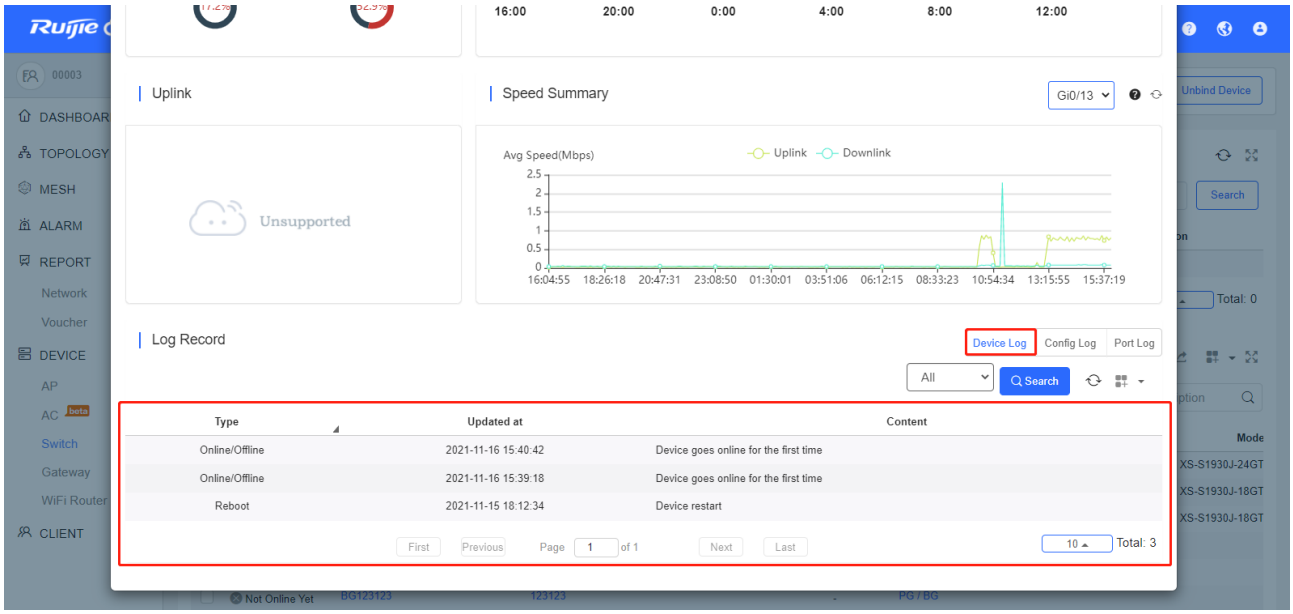
- Overview > Speed Summary

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



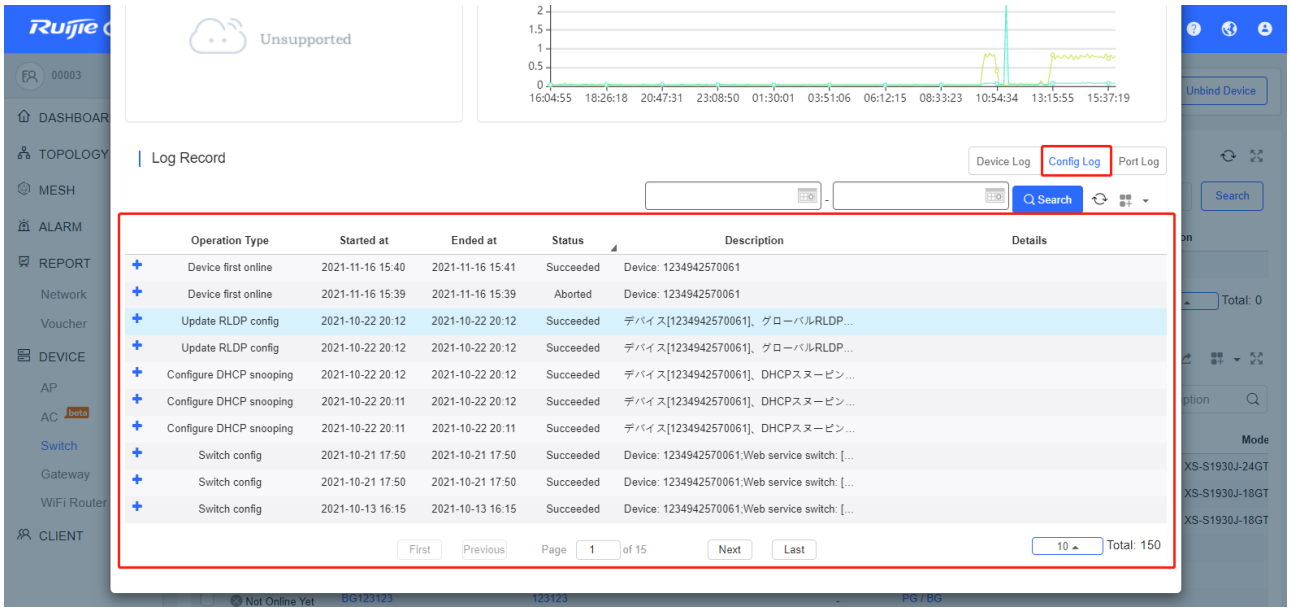
- Overview > Device Log

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



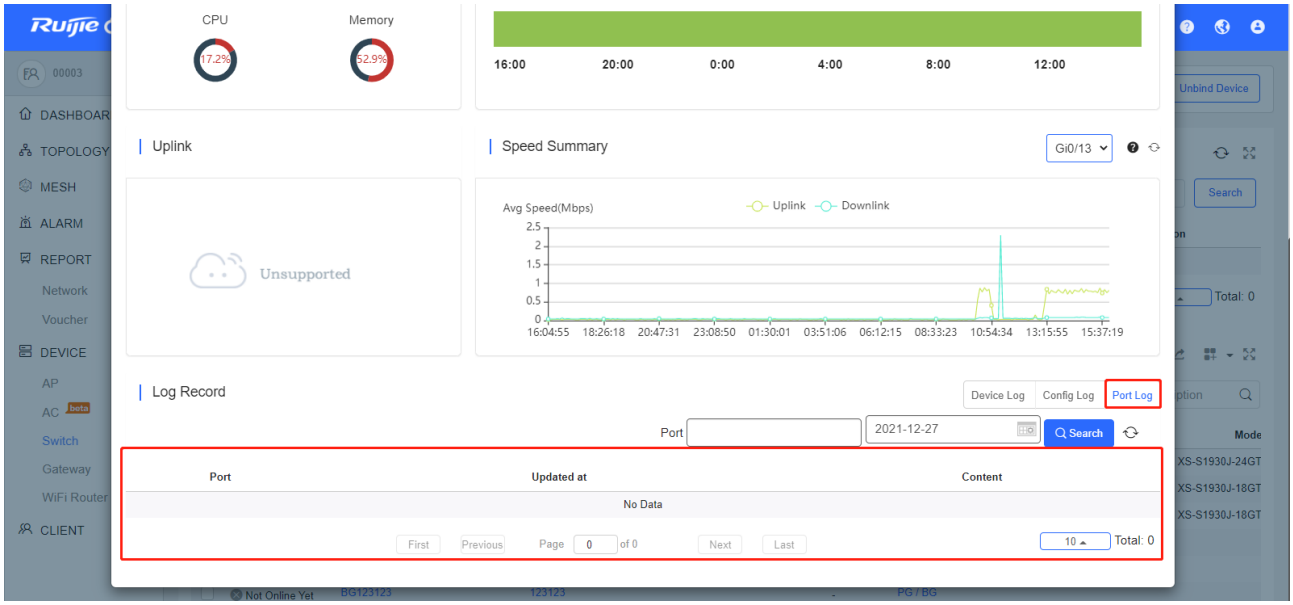
- Overview > Config Log

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



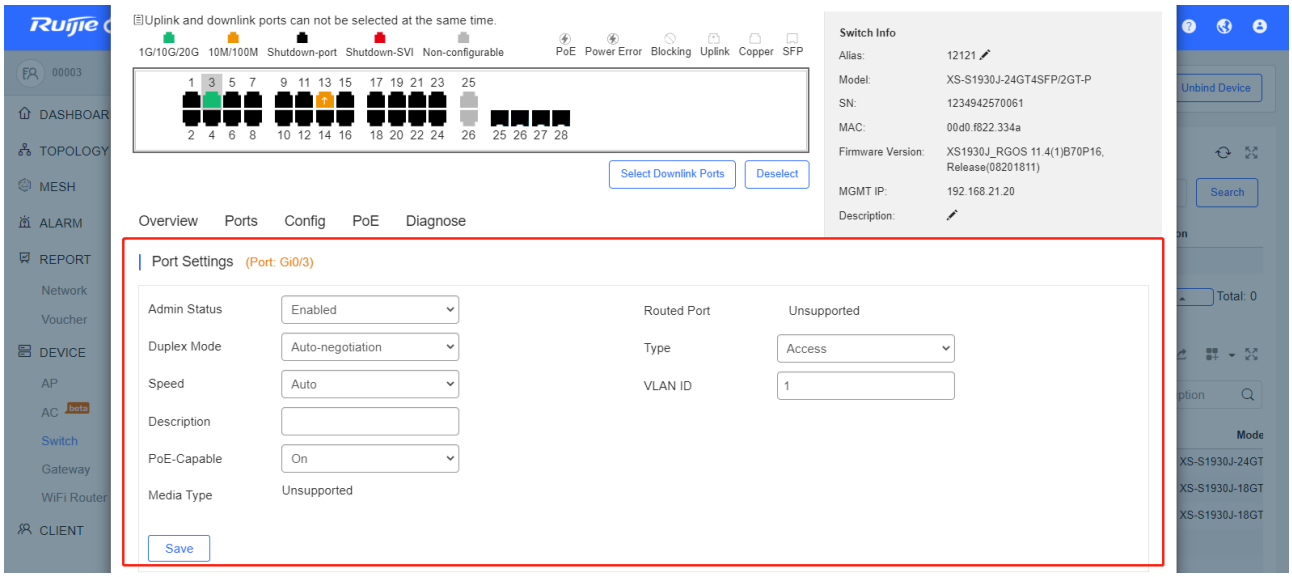
- Overview > Port Log

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



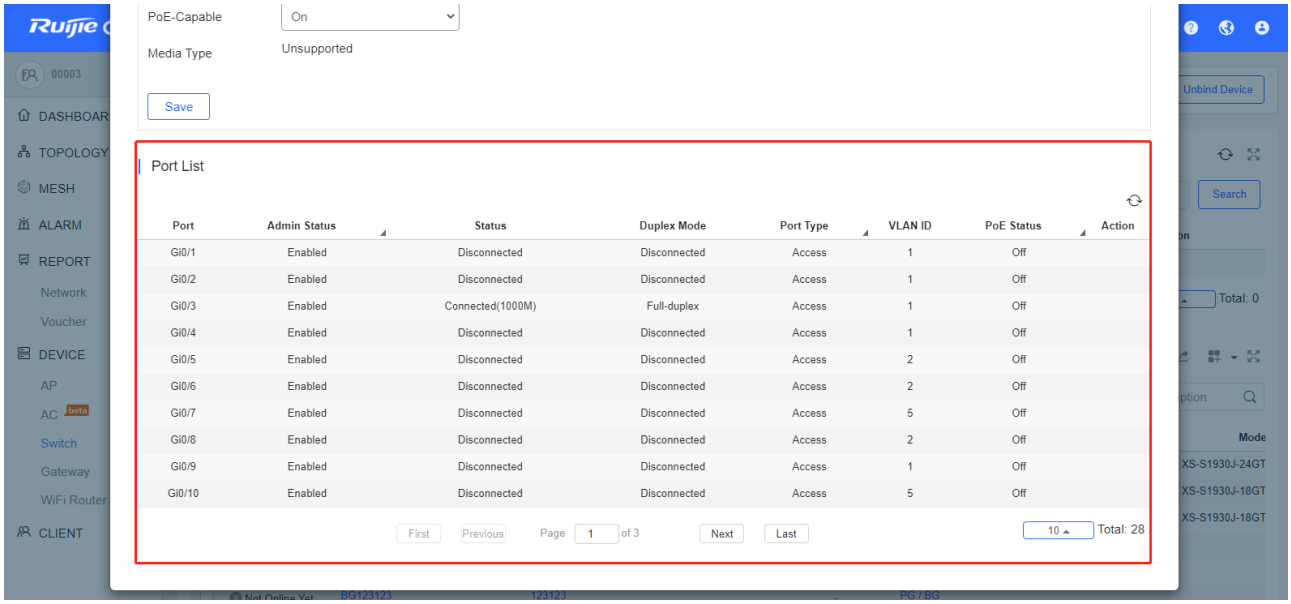
- Ports > Port Settings

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



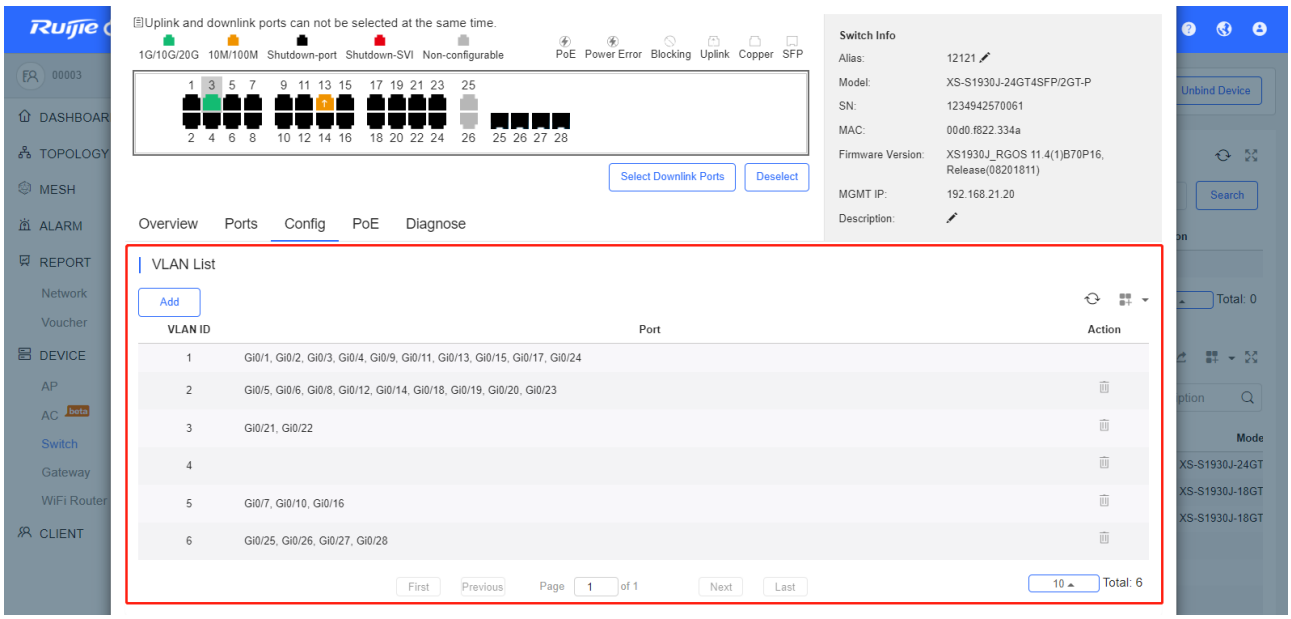
- Ports > Port List

Port list 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.

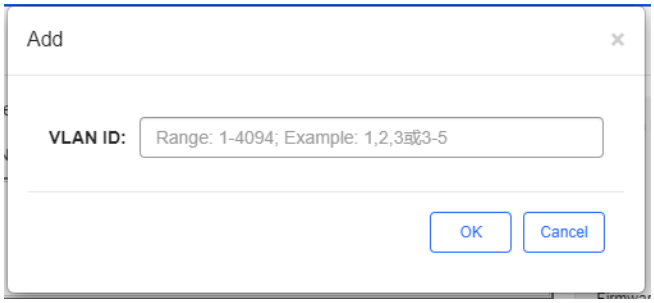


- Config > VLAN List

VLAN list includes the VLAN ID and the correspondingly ports.



Click **Add** to add VLAN IDs in batches.



If a VLAN ID you add exists, it will be ignored.

You can use the following two methods to add VLAN IDs in batches:

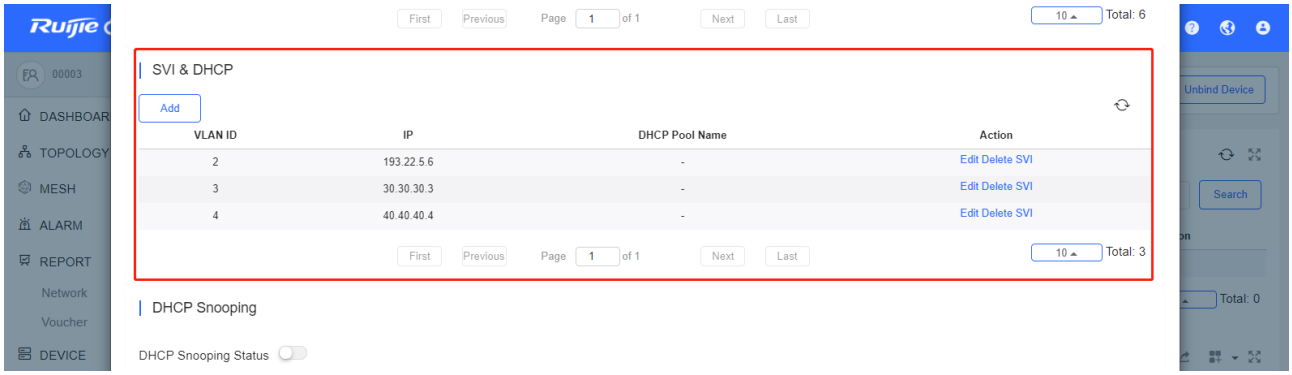
(1) Use commas (,) to separate multiple VLANs. Up to 10 VLANs are supported.

(2) Use an end dash (-) to indicate a VLAN range. No limit.

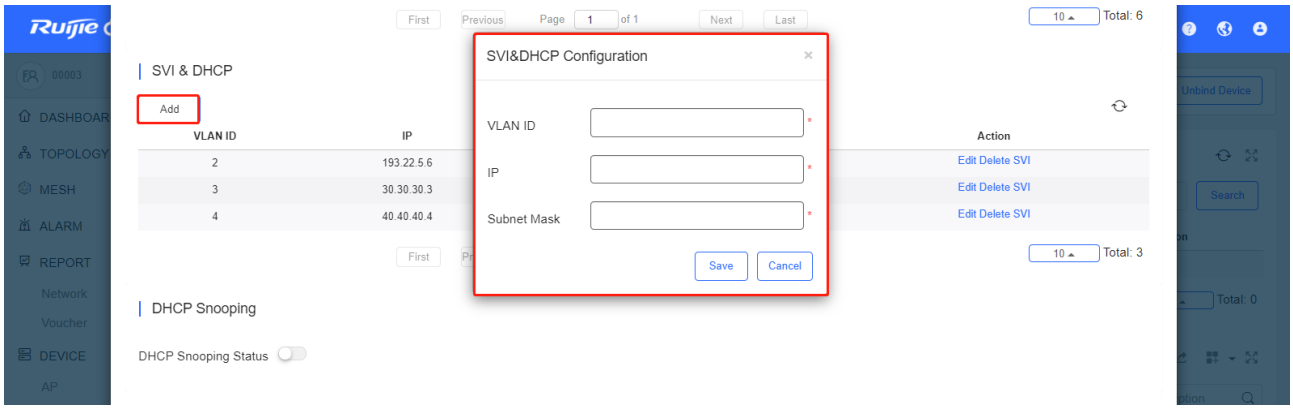
Note: Do not support to use commands and end dashes at the same time.

- 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.

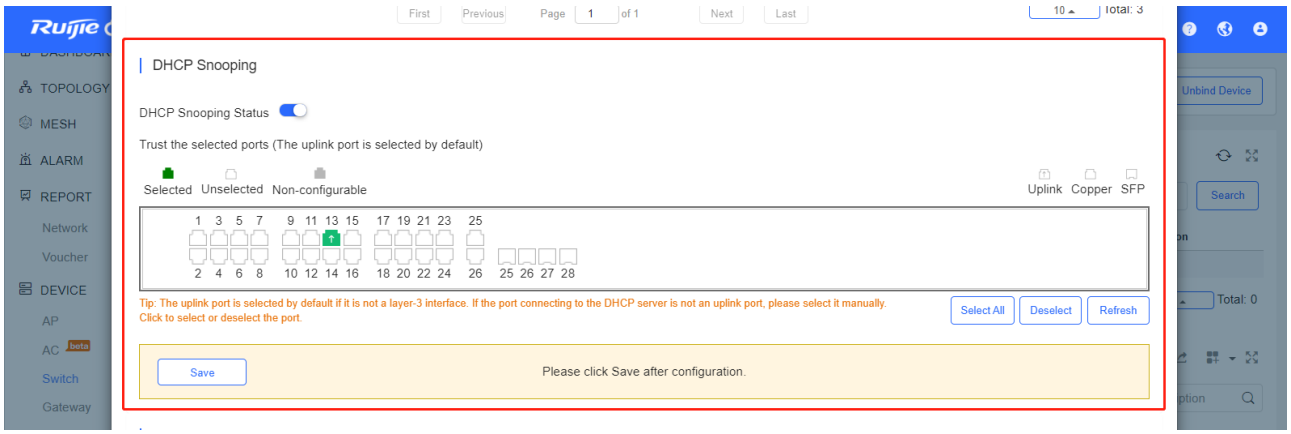


Click **Add** to configure the IP and subnet mask of a VLAN, and configure the name, IP segment, subnet mask and gateway of DHCP service.



- 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.

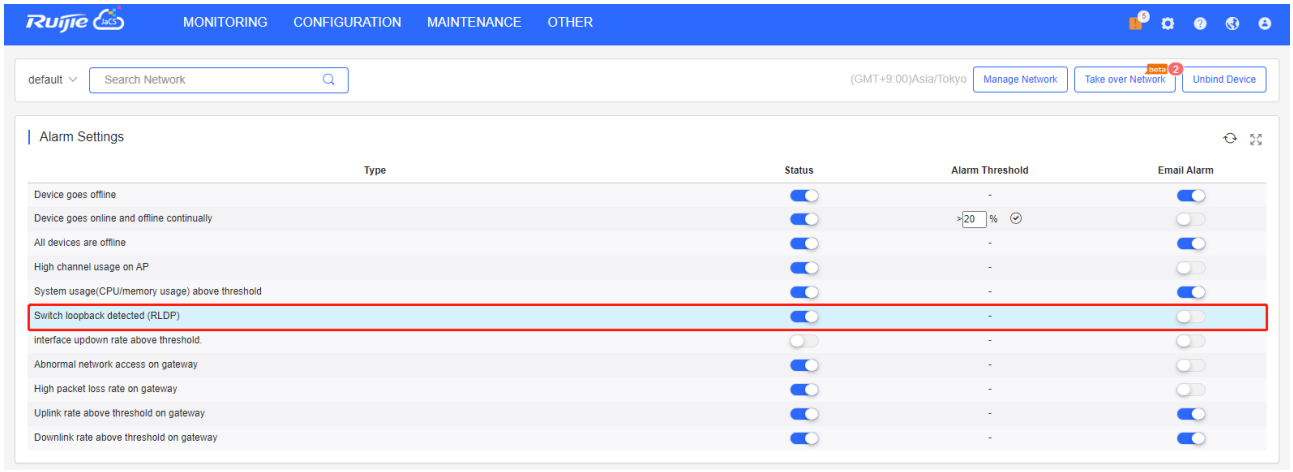


- Config > RLDP

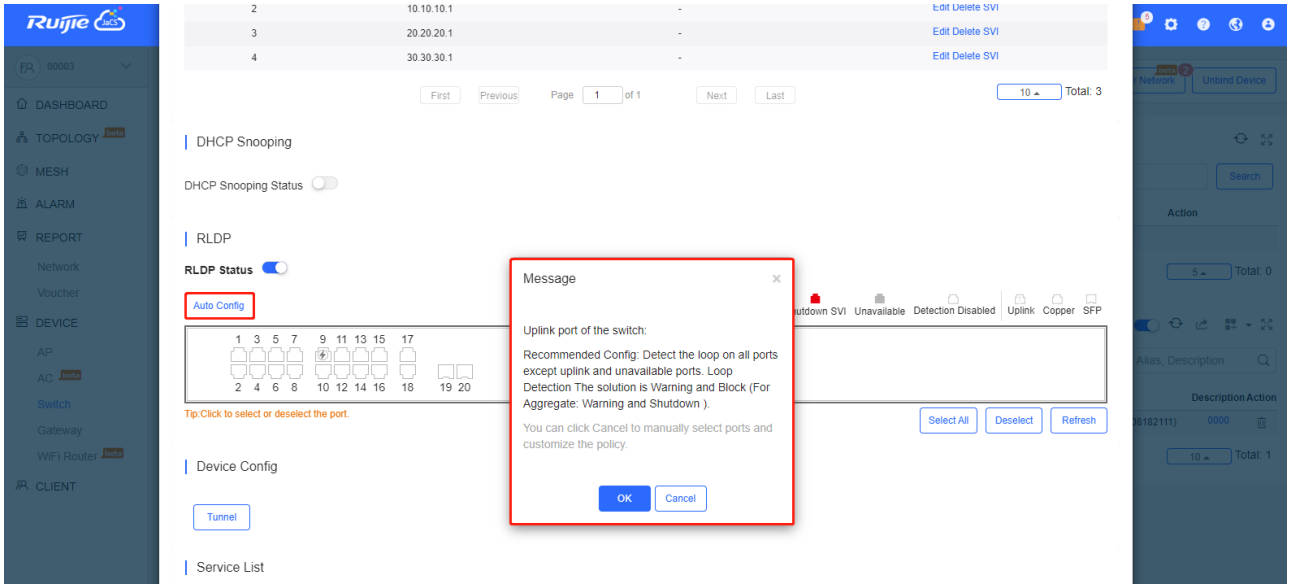
Enable **RLDP Status**, select one or multiple ports, choose the troubleshooting method for a loop, and click **Save**.

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.

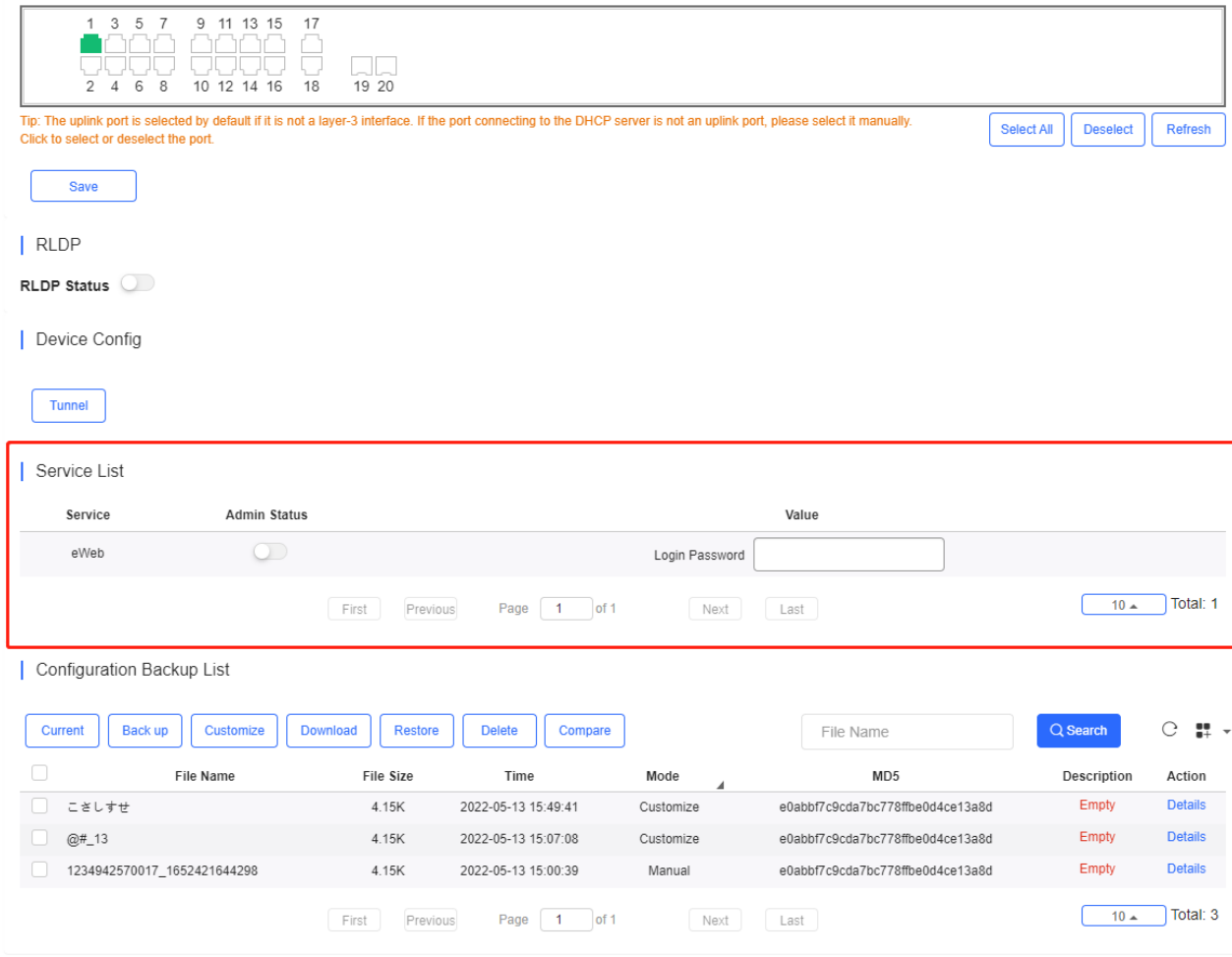


Click **Auto Config** to enable the default configuration.



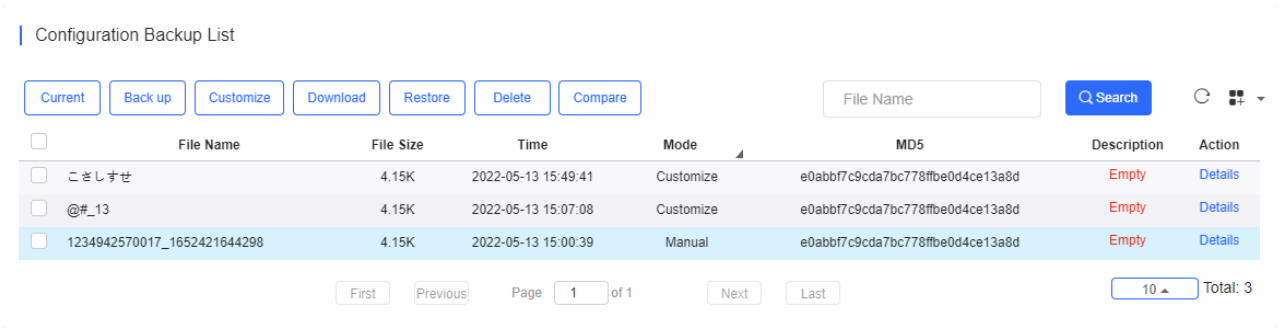
- Config > Service List

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



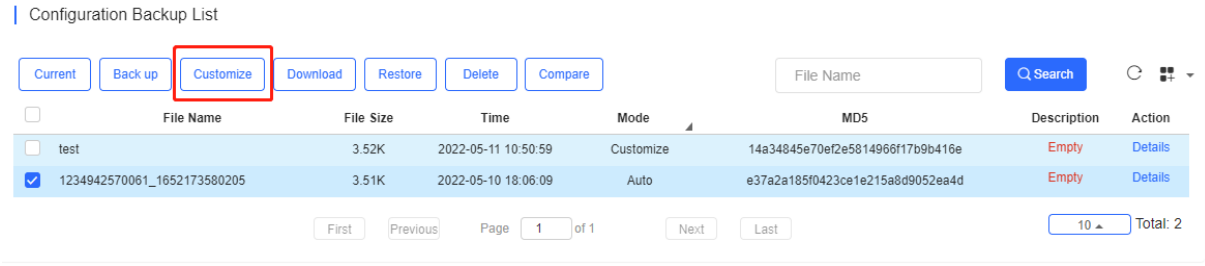
- Config > Configuration Backup List

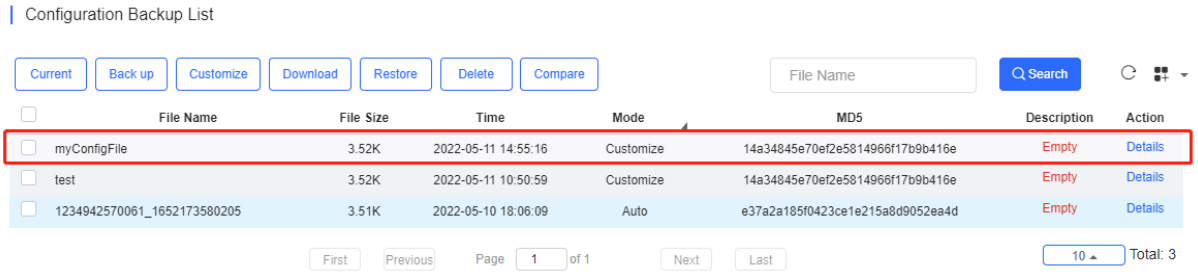
The backup records include configuration file name, size, time, mode and MD5.



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

To customize a configuration file, select an existing file and click **Customize**.



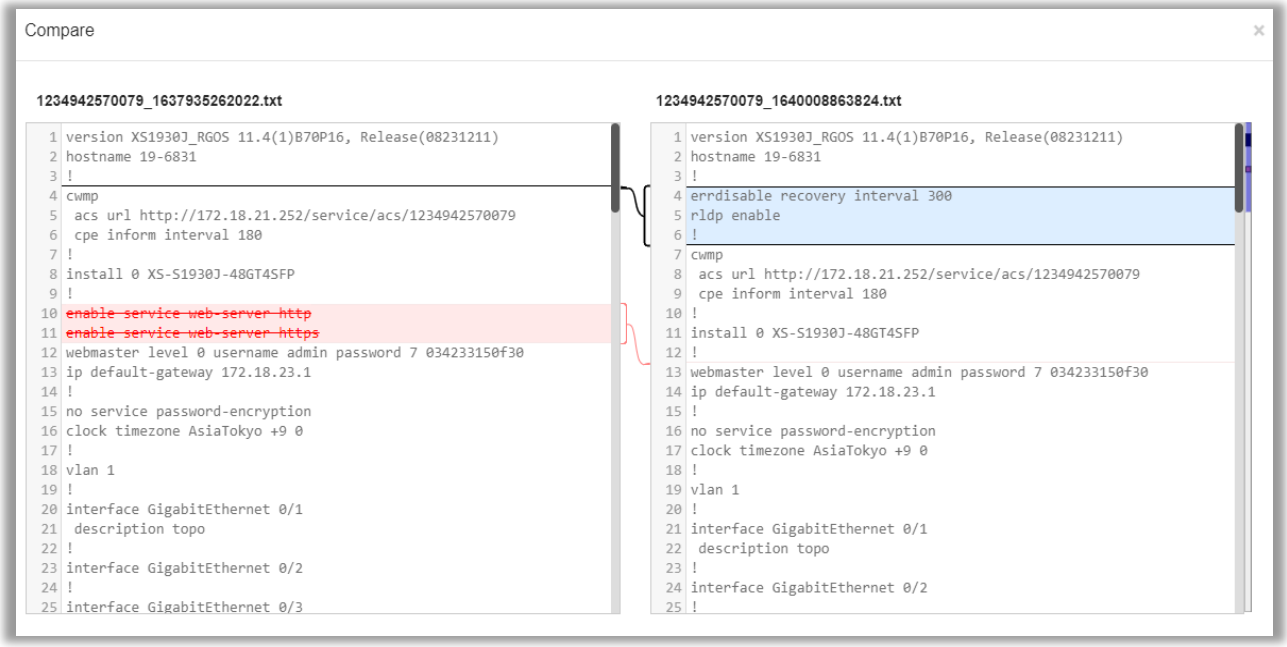


Select one record, and click **Download** to download the configuration file.

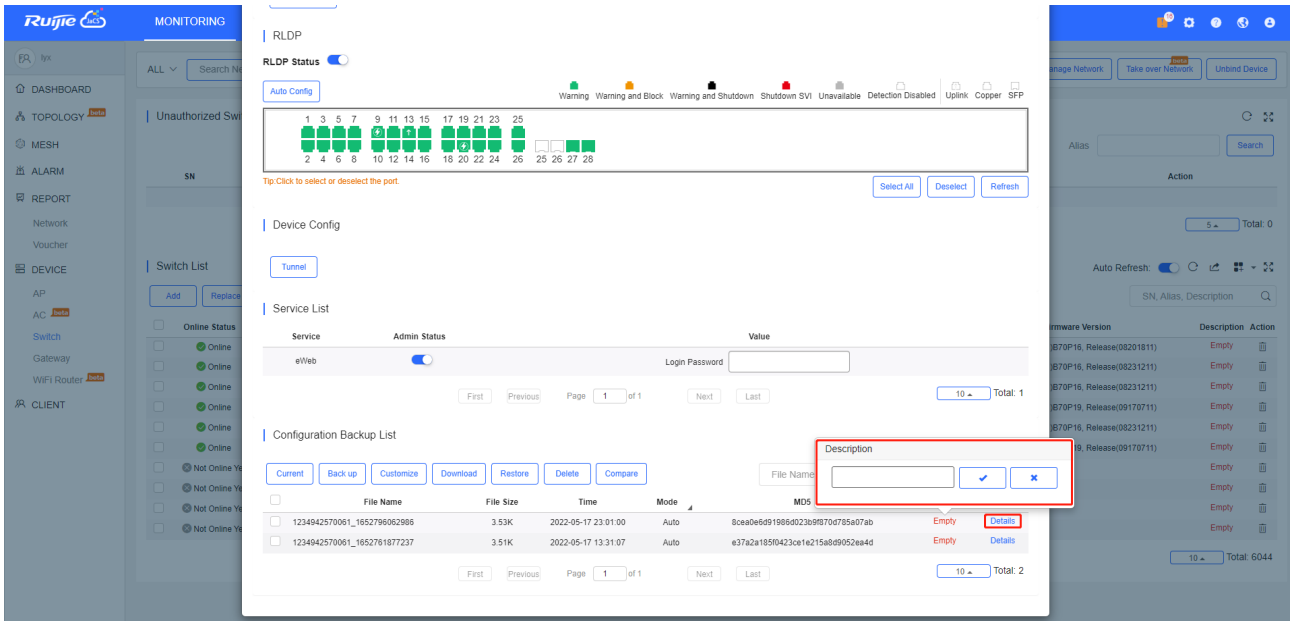
Select one record, and click **Restore** to restore the current configuration.

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

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



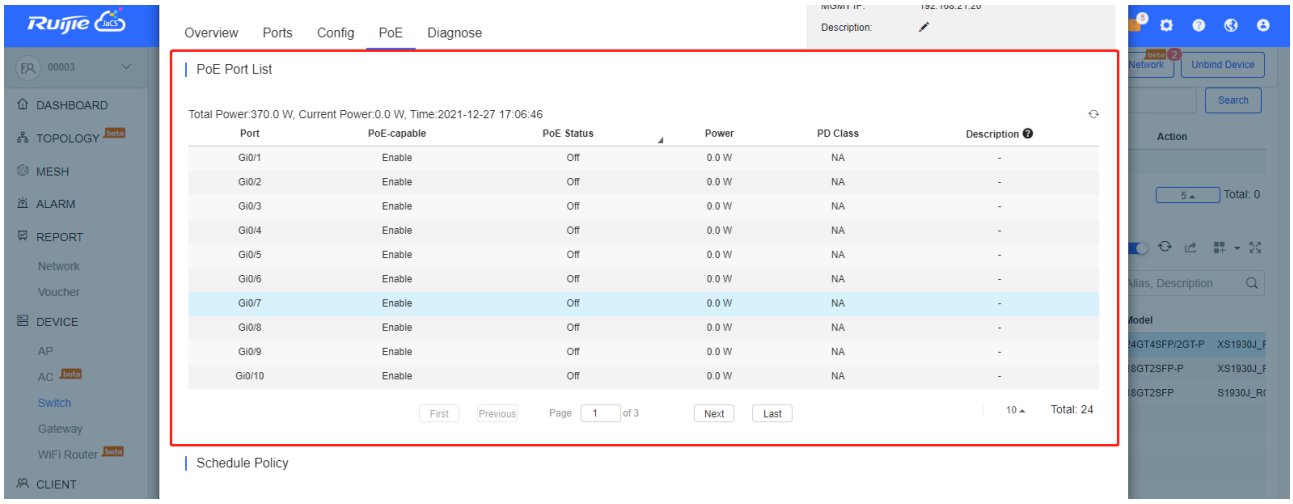
Description can be edited. Click **Details** in the **Action** column to check the backup configuration.



- PoE > PoE Port List

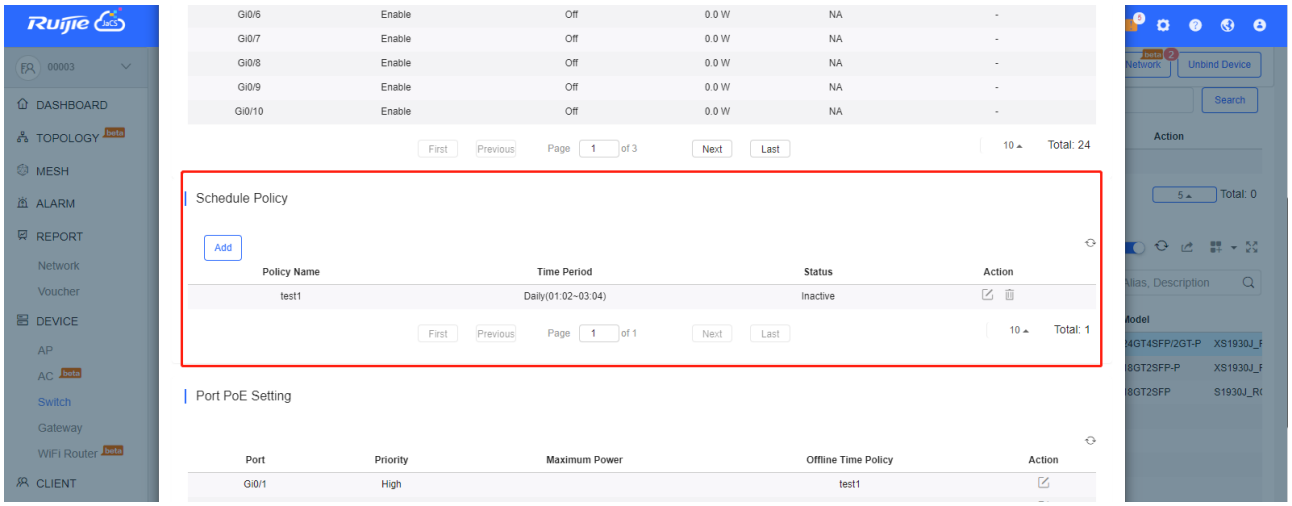
PoE statistics are displayed above **PoE Port List**, including the total power, current power and time.

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



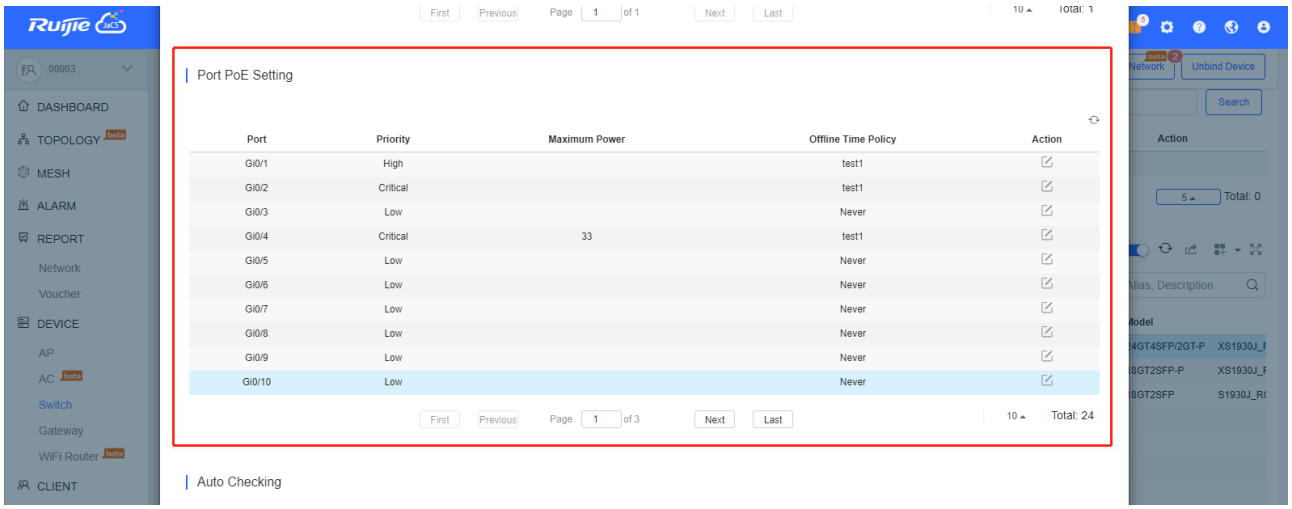
- PoE > Schedule Policy

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.



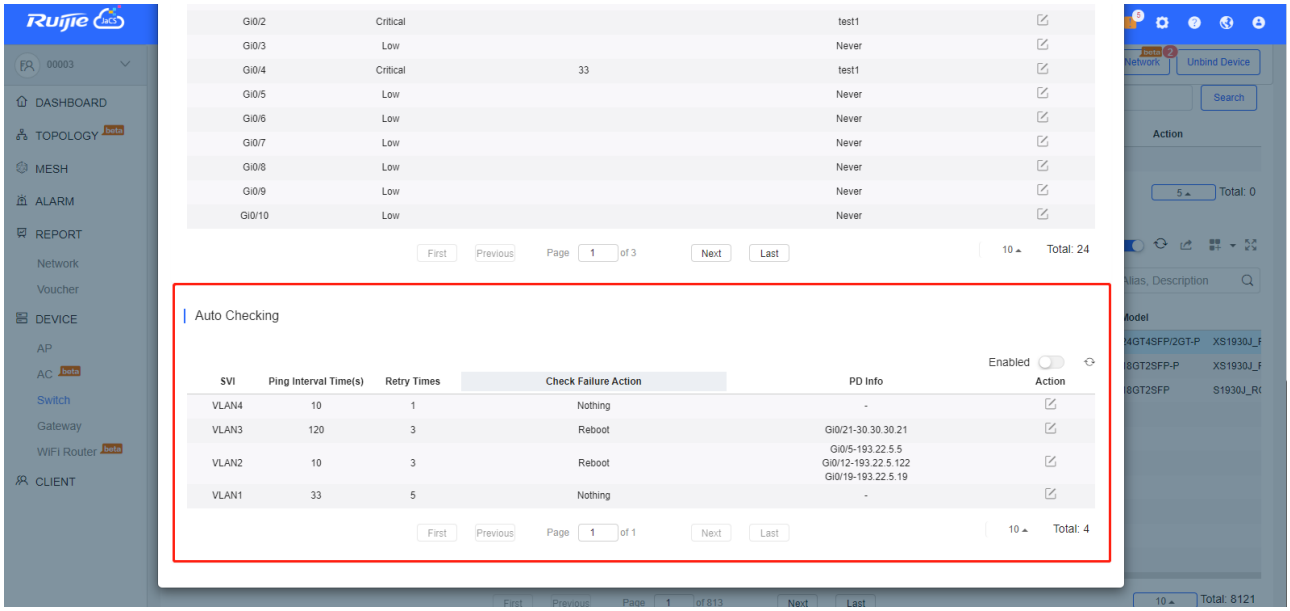
- PoE > Port PoE Setting

The **Port PoE Setting** displays effective port PoE settings, including port name, the power supply priority, maximum power and power supply stop policy.



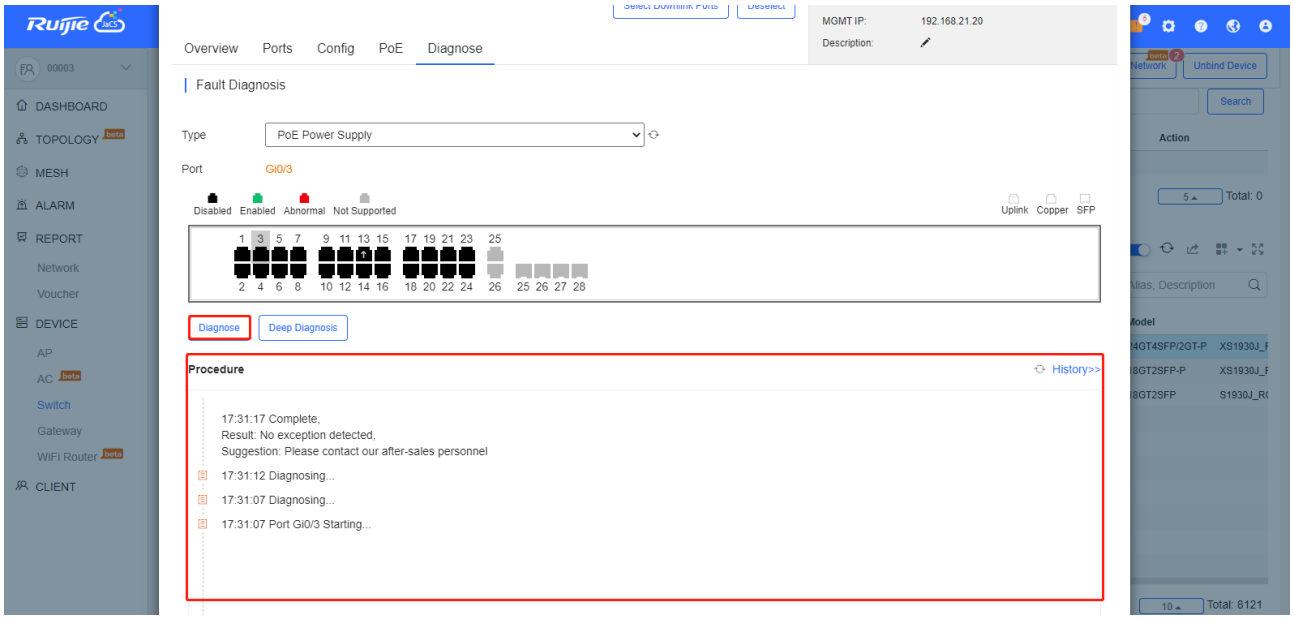
- PoE > Auto Checking

The **Auto Checking** displays the policy for checking the working status of a PD connected to a PoE port, including the Ping interval, number of retry times, action to be taken upon checking failure and IP address for checking PDs.

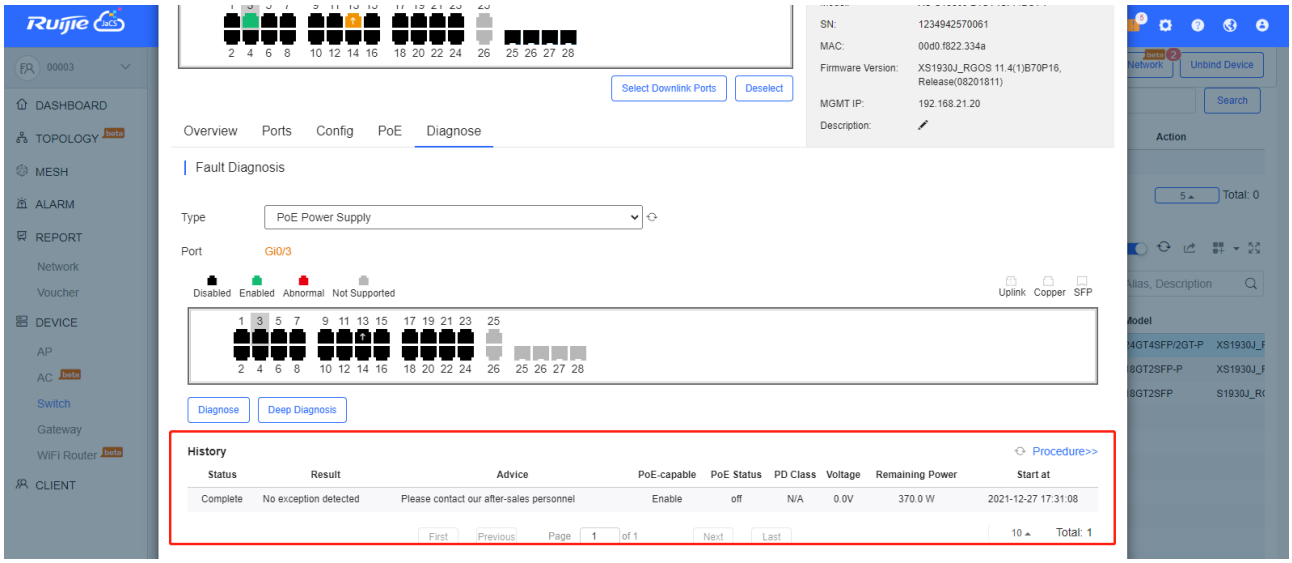


- Diagnose > Fault Diagnosis

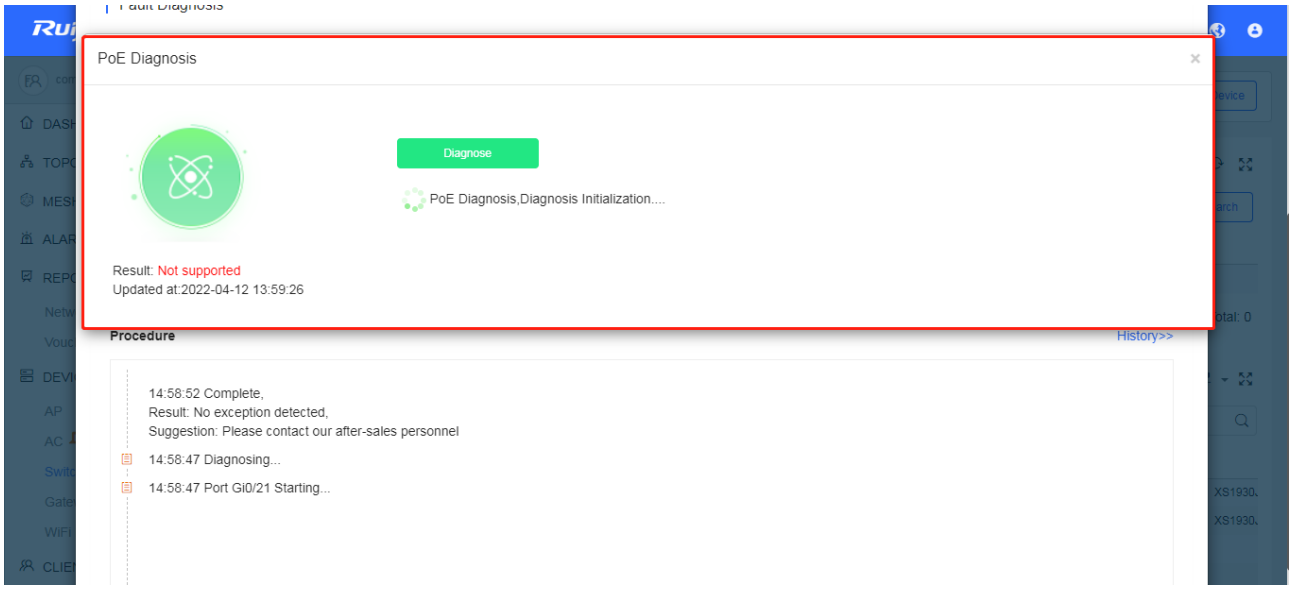
There are two types of fault diagnosis: **PoE Power Supply** and **SFP Port**. Select a port in the panel, click **Diagnose**, and the diagnosis procedure is displayed as below.



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



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



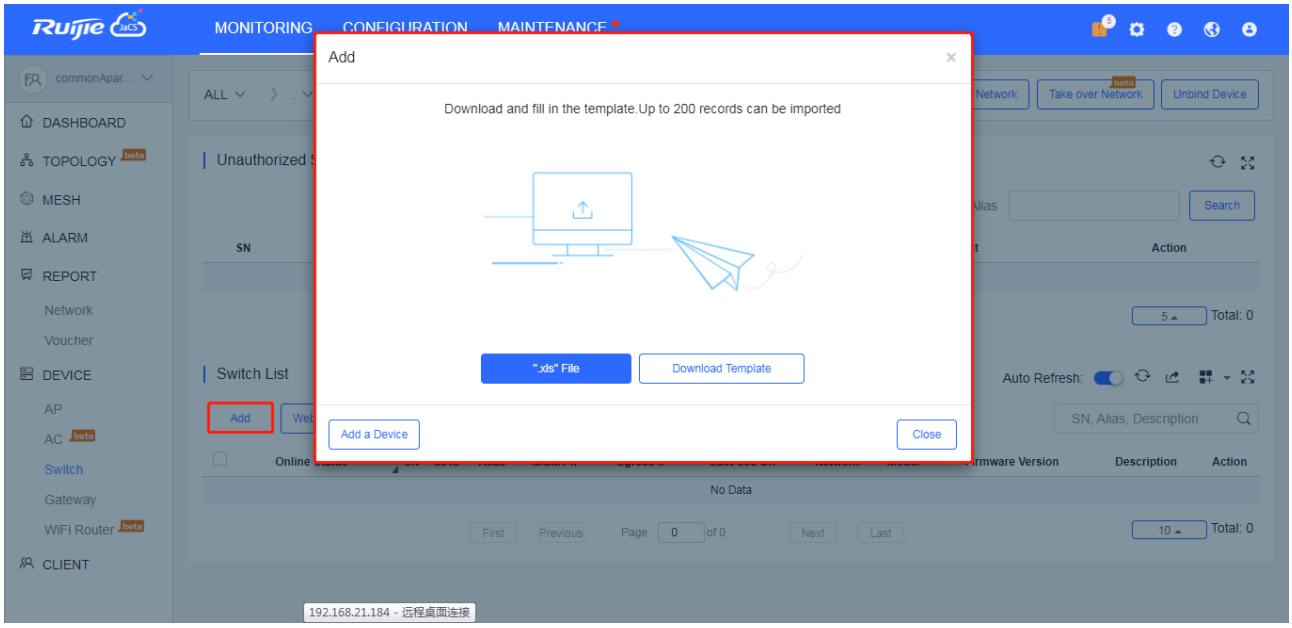
Normal diagnosis: The Cloud server delivers CLI commands to collect the switch information, and the diagnosis occurs on the Cloud server.

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

5.6.3.3 Basic Switch Operations

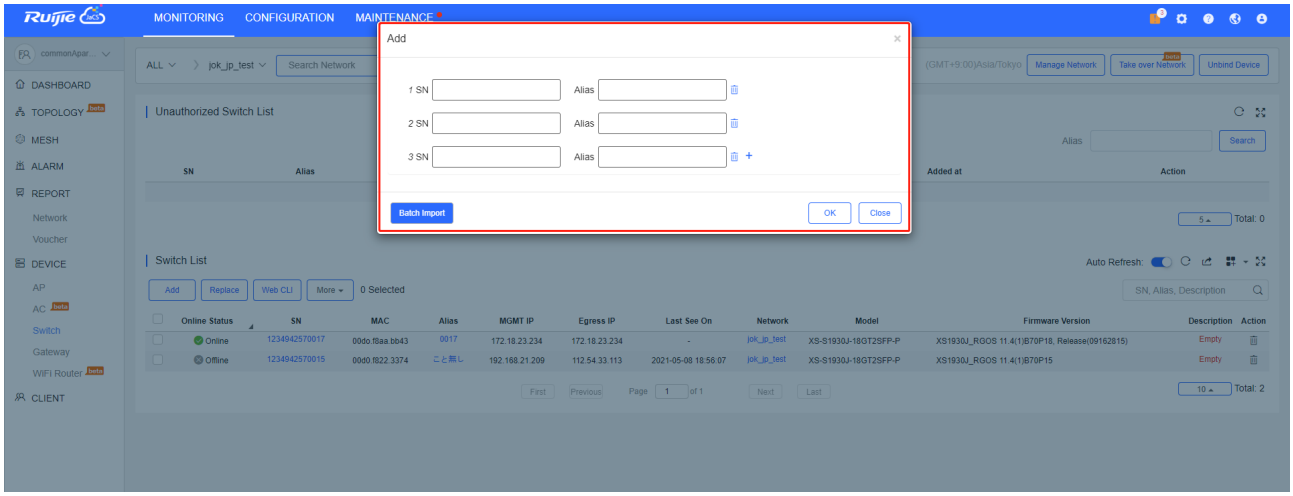
- Add Switch

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.

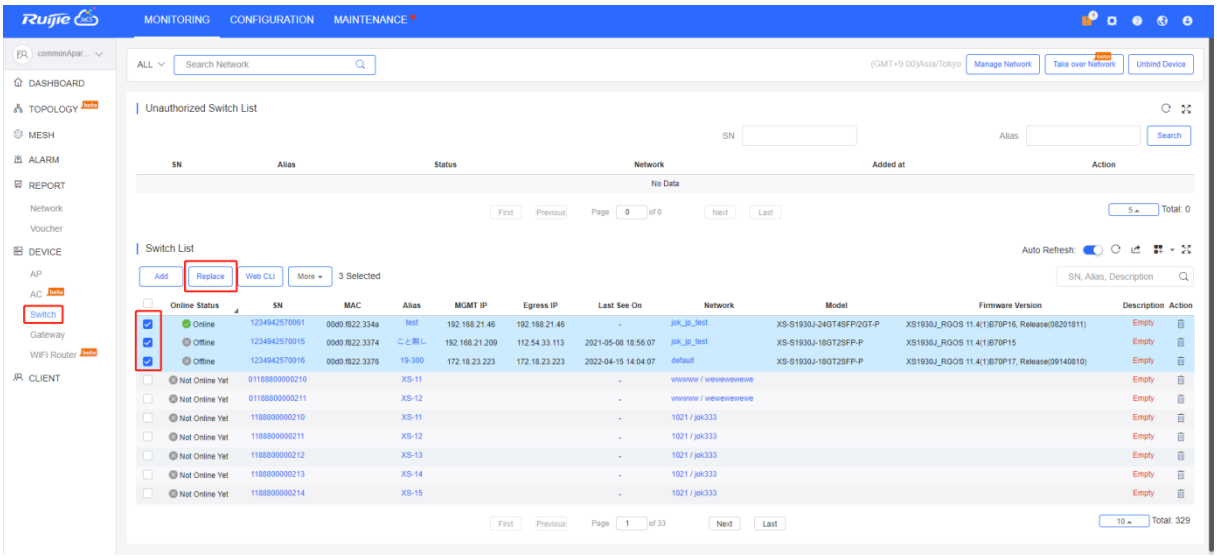
Click **Add a Device**, enter SN and alias of the switch, and click **OK**. Click + to add multiple switches.



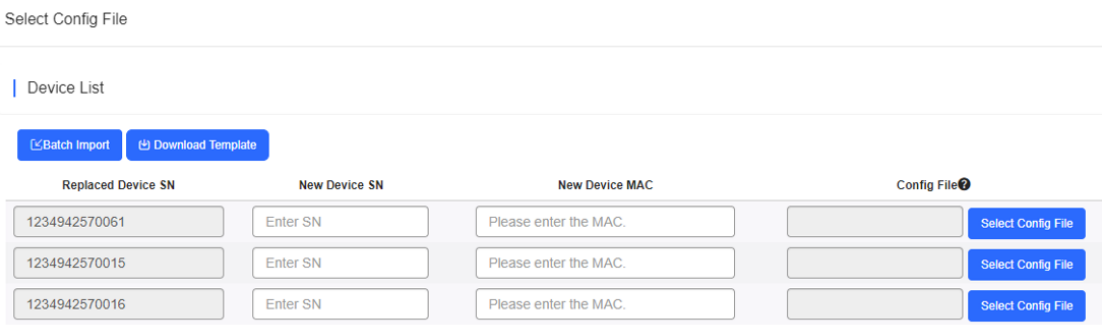
- Replace Switch

The configuration of old device can be synced to the new device. After the new device goes online, the configuration file of the old device will be delivered.

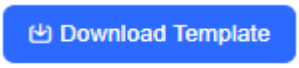
Select an existing device.

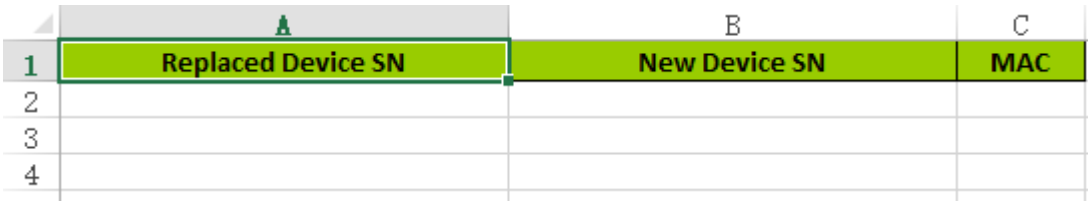


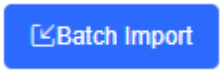
Click  .

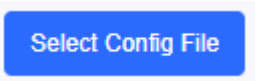


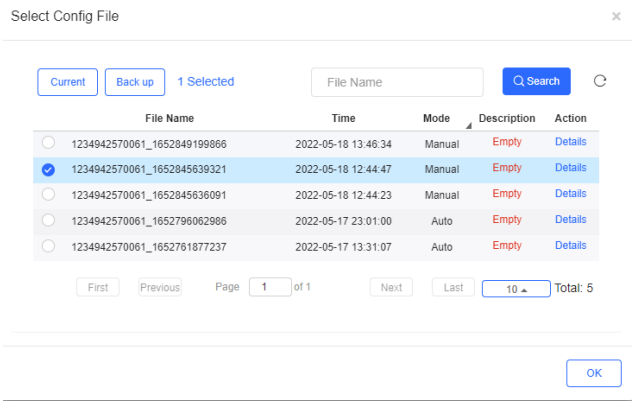
By default, the configuration file of the old device is the latest automatic configuration file, or you can select the history configuration file manually. The MAC of new device is required. The SN and the MAC of device should be consistent, and the models of old device and new device should be the same; otherwise, the replacement cannot be performed.

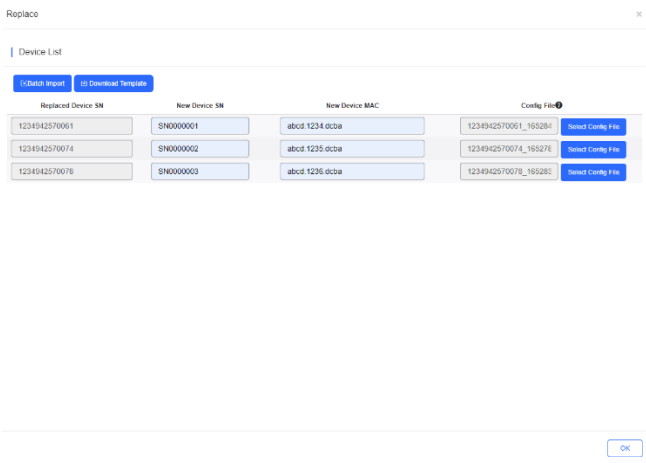
To batch replace switches, click  to download the template and enter the device information.



Click  to import the template.

To replace the configuration with the configuration of an existing device, click 

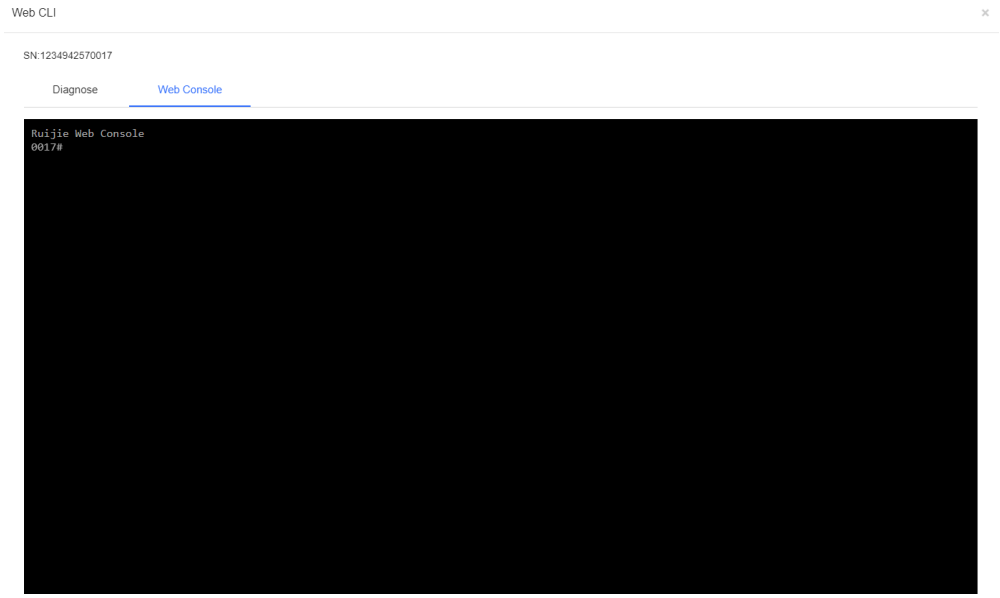




- Web CLI

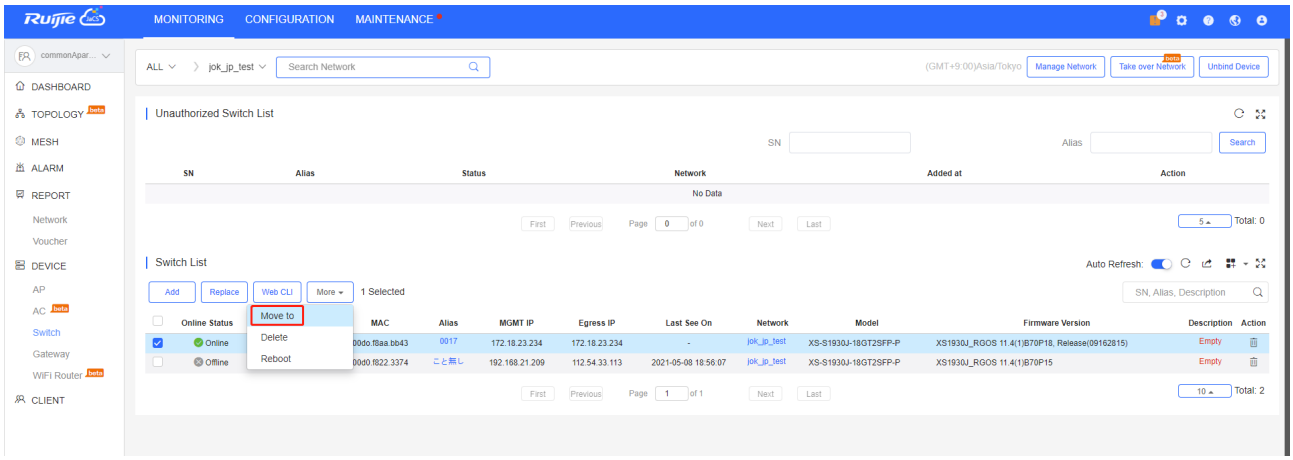
Select one or multiple devices in the **Switch List**, and click **Web CLI**. The **Web CLI** dialog box is displayed, and device information can be queried via the menus in this dialog box. The menus vary with the products.

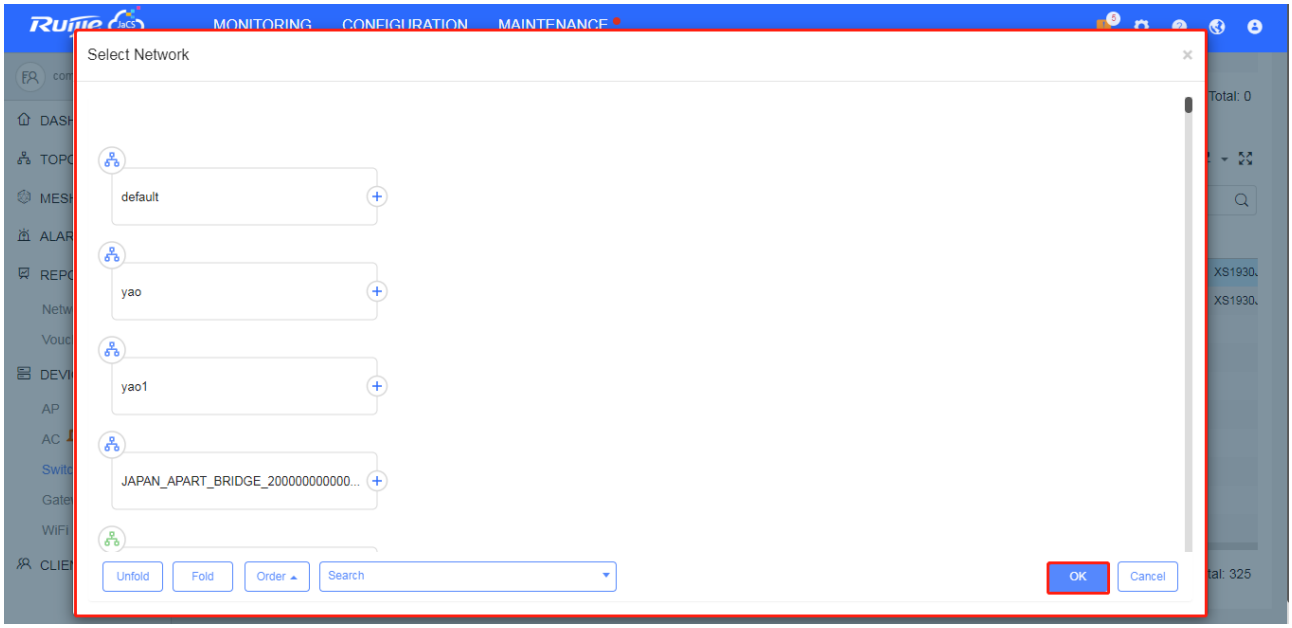
In addition, in the command entry box, the **TAB** key and question mark (?) both can complete a command.



- More > Move to

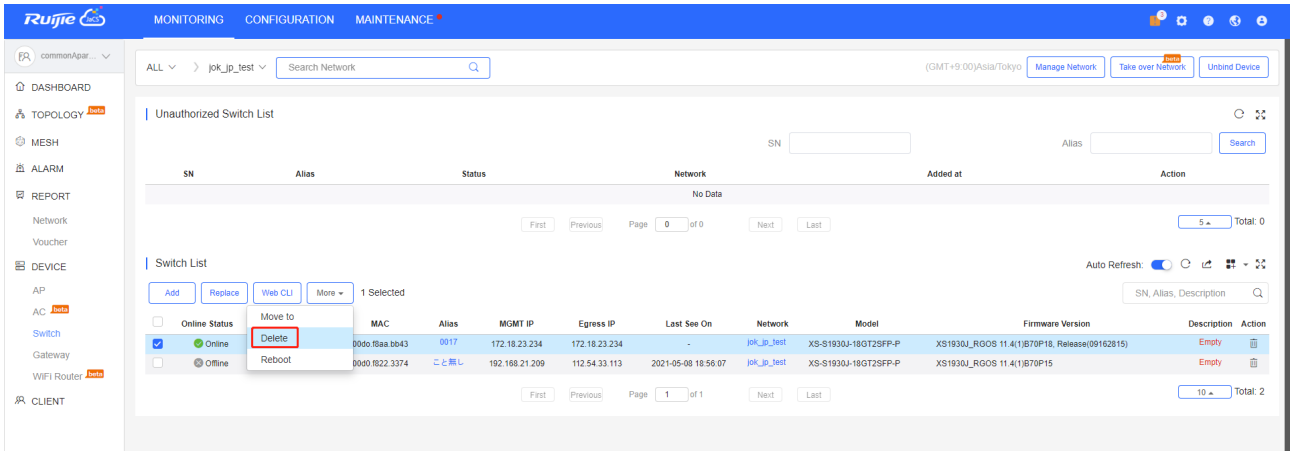
Select one or multiple devices in the **Switch List**, click **More** > **Move to**, select the new network and click **OK**.





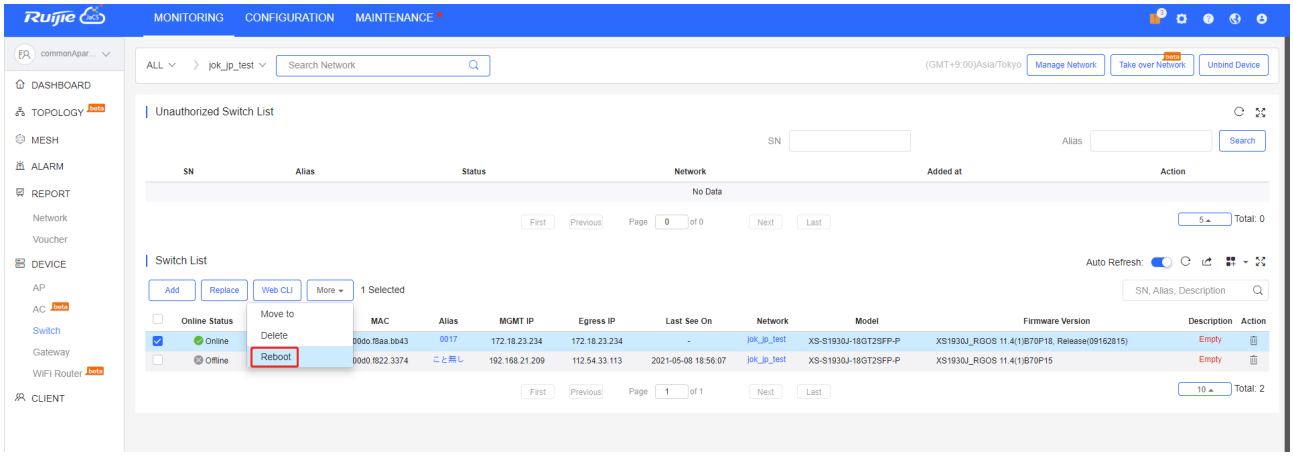
- More > Delete

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



- More > Reboot

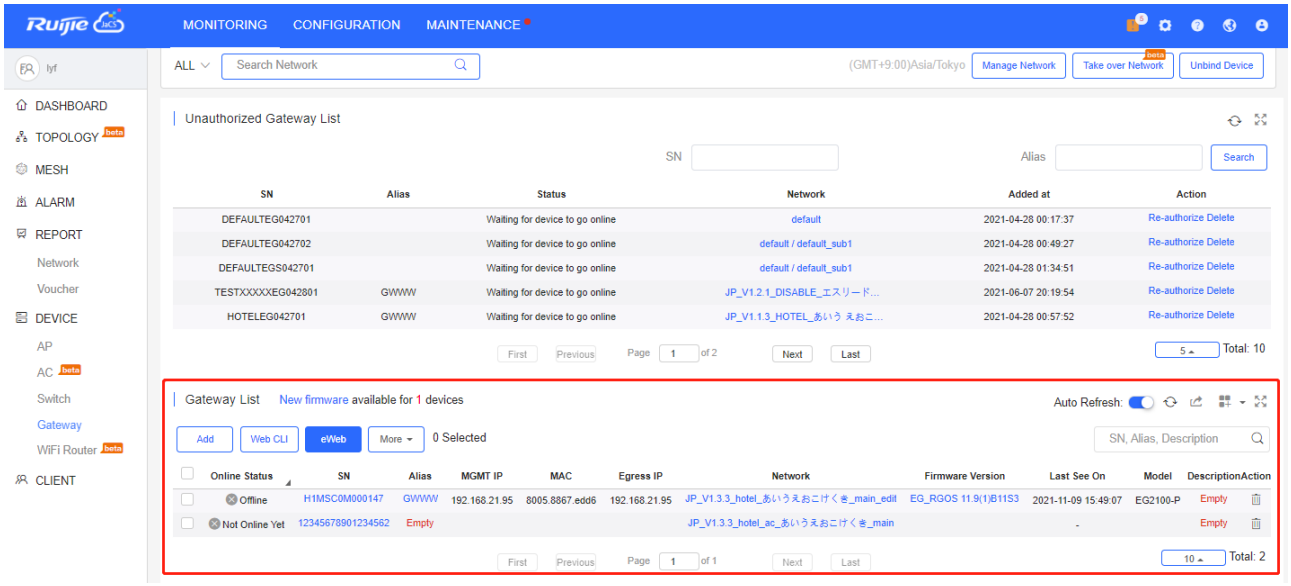
Select one or multiple devices in the **Switch List**, and click **Reboot.**



5.6.4 Gateway

5.6.4.1 Gateway List

The **Gateway List** displays basic device information, including the online/offline status, SN, alias, management IP, MAC, egress 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.

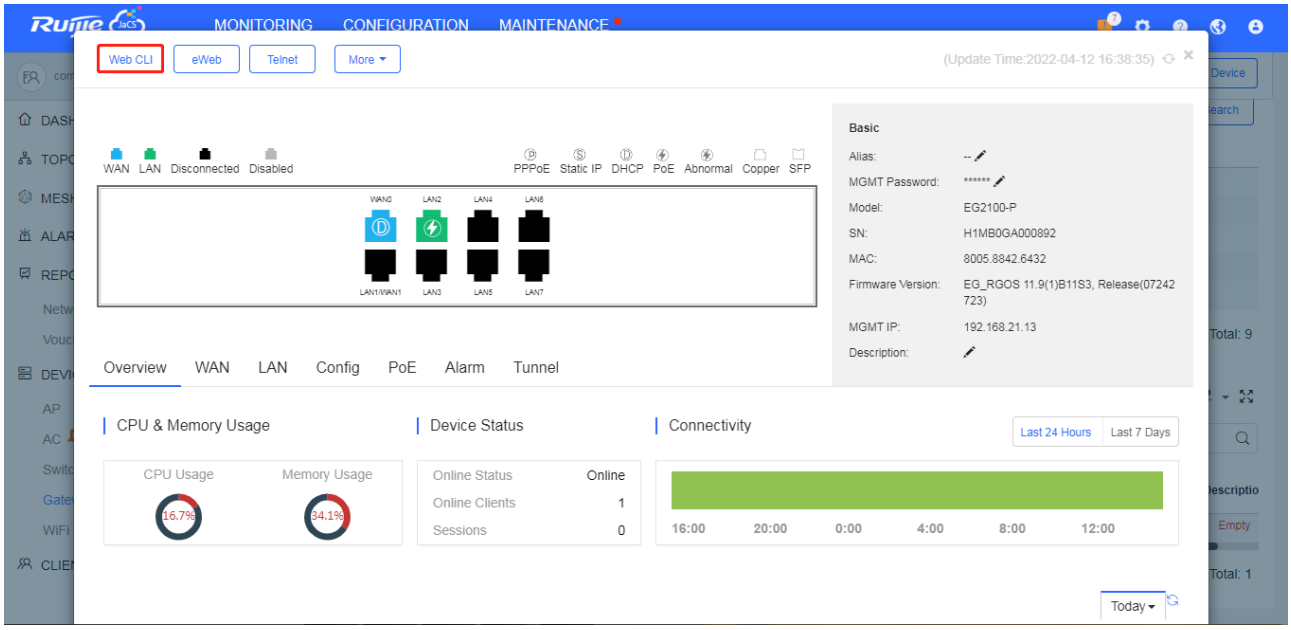
Above the list are the **Add Gateway**, **Web CLI** and **eWeb** functions. Click More to display the **Move to**, **Reboot**, **Tunnel** and **Delete** functions. For more information, refer to **Basic Gateway Operations**.

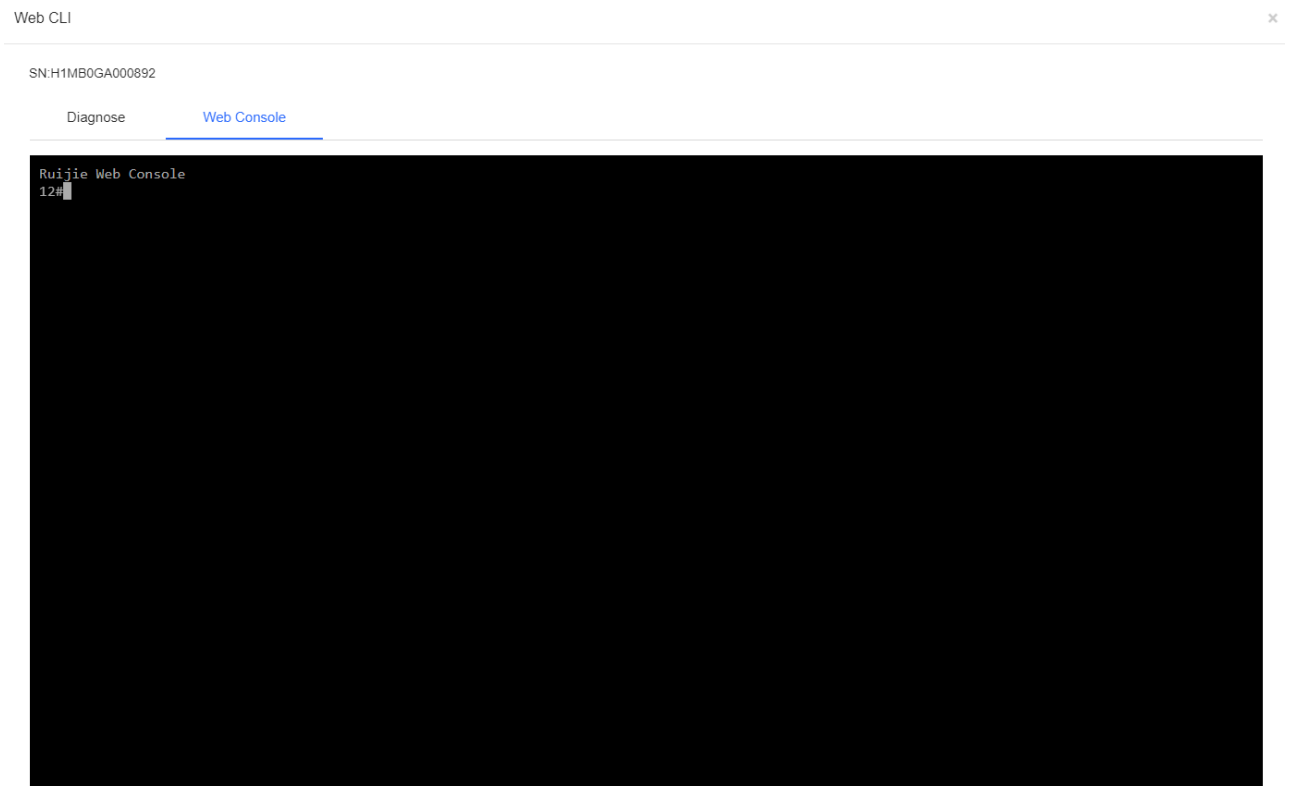
The **Search** function supports fuzzy queries based on the serial number, alias and description, and also supports queries based on online/offline status.

5.6.4.2 Device Details

- Web CLI

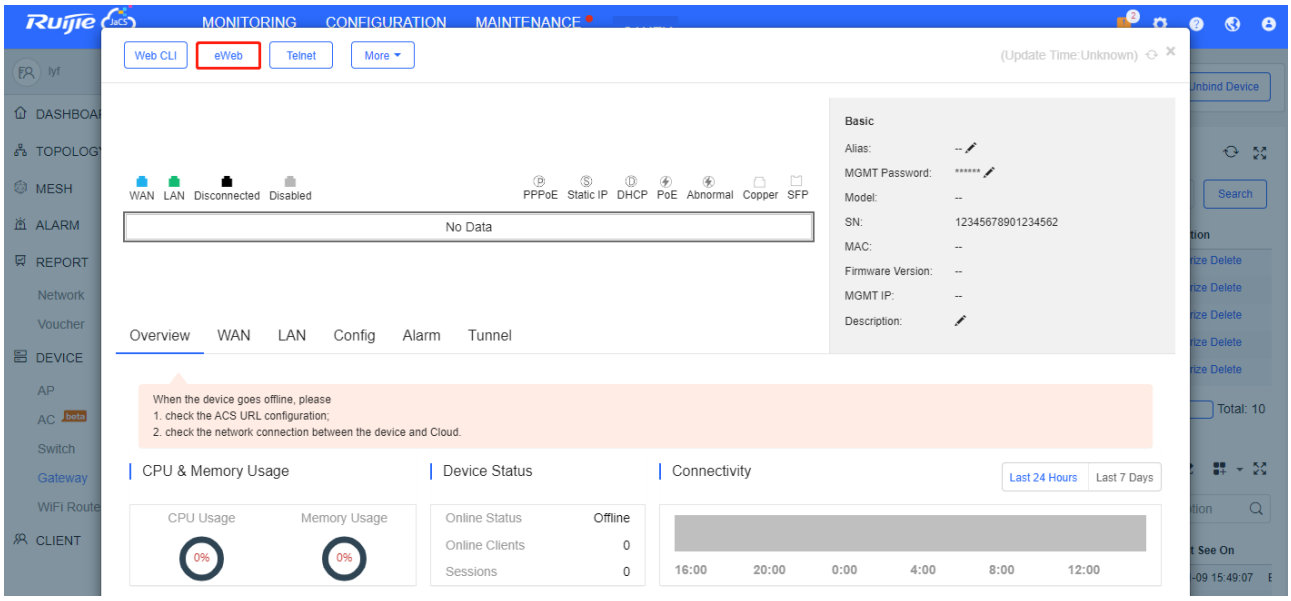
Click **Web CLI**, and the **Web CLI** page is displayed. The **Web CLI** page provides commonly-used CLI commands on the left. Click the command, or manually enter the command and click **Send**.

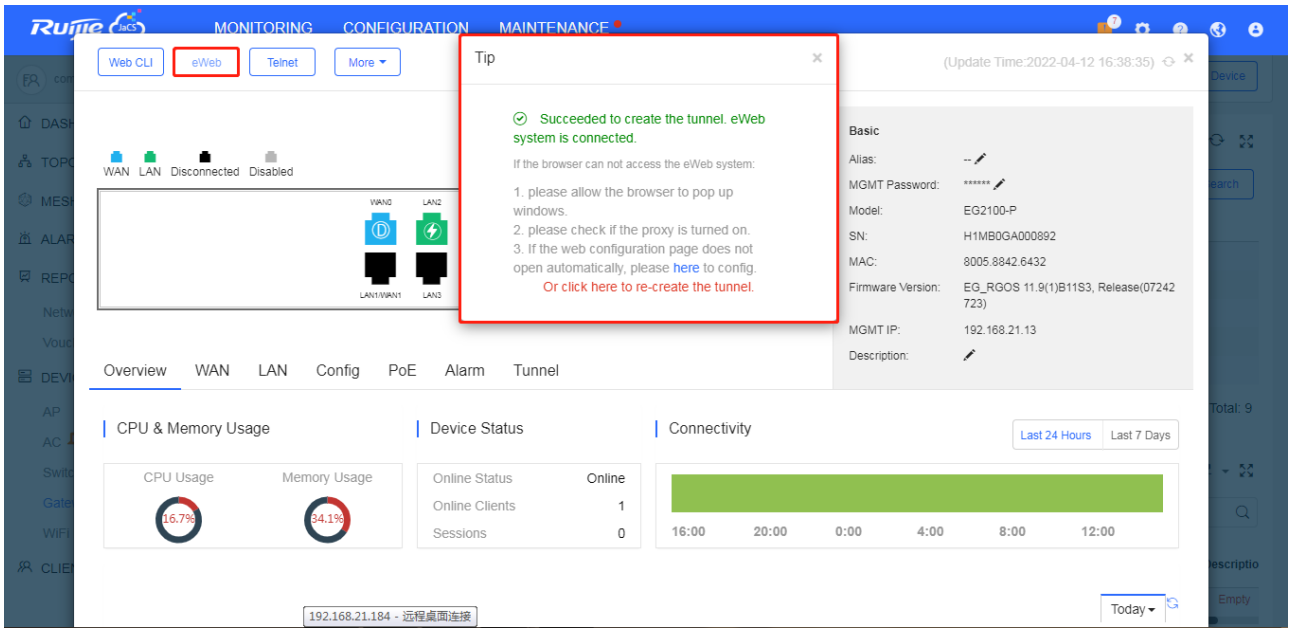




- eWeb

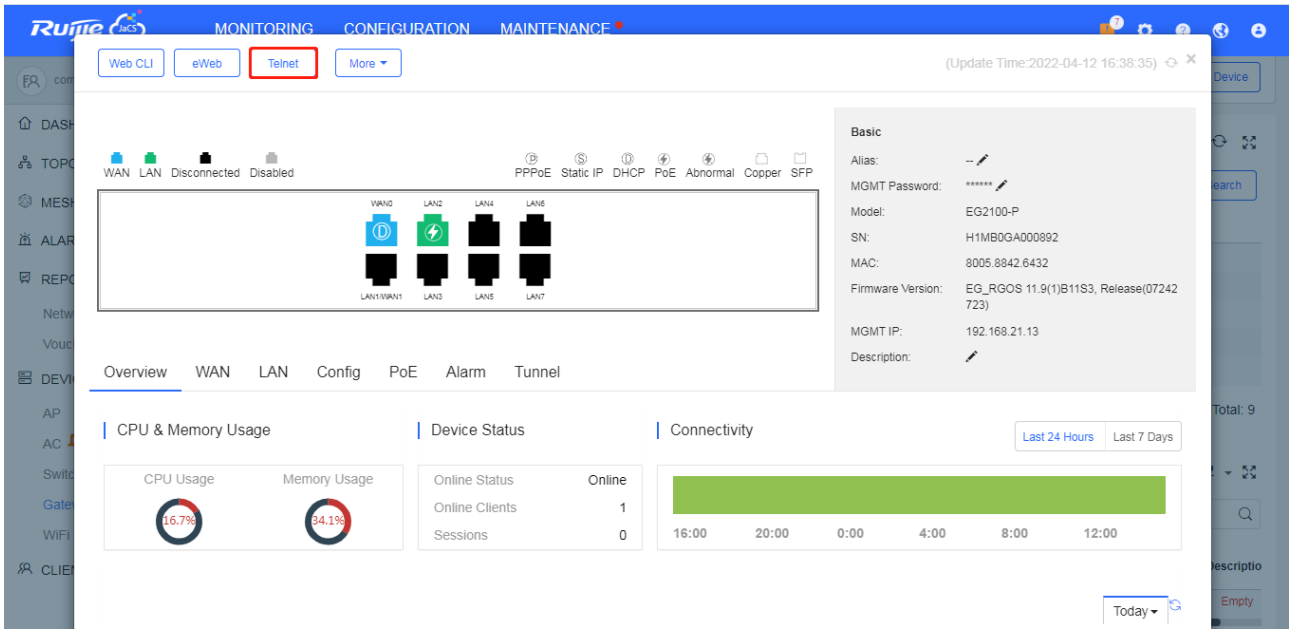
Click **eWeb** to open the eWeb system in a new window.

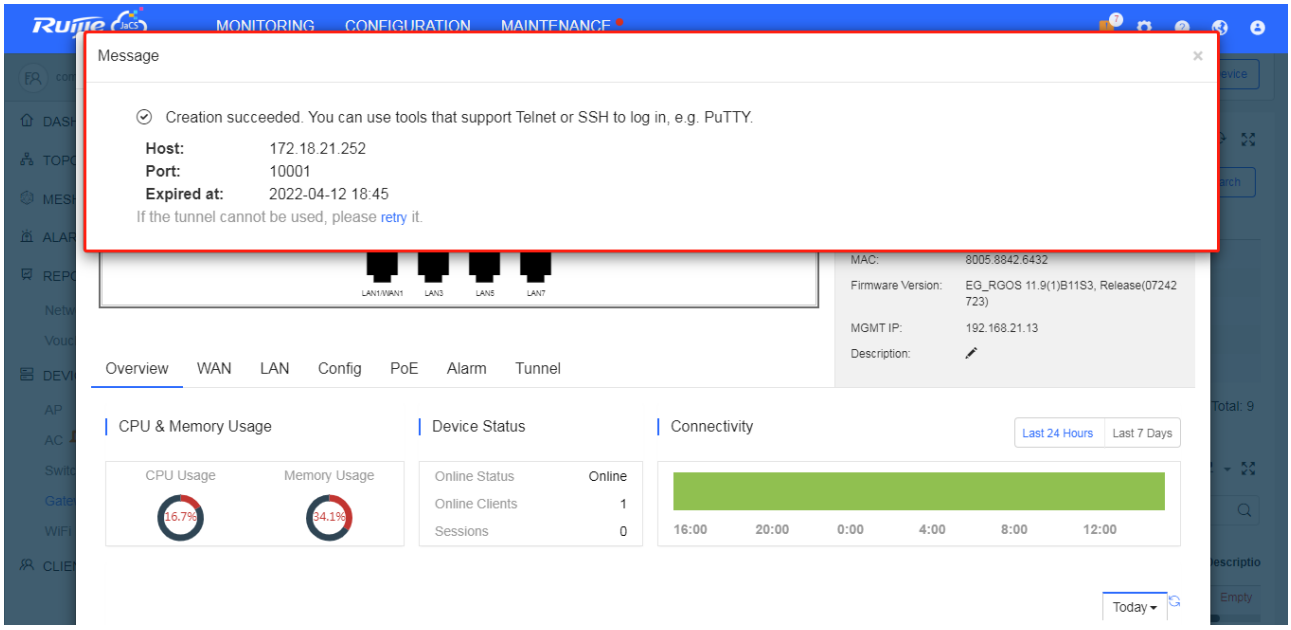




- Telnet

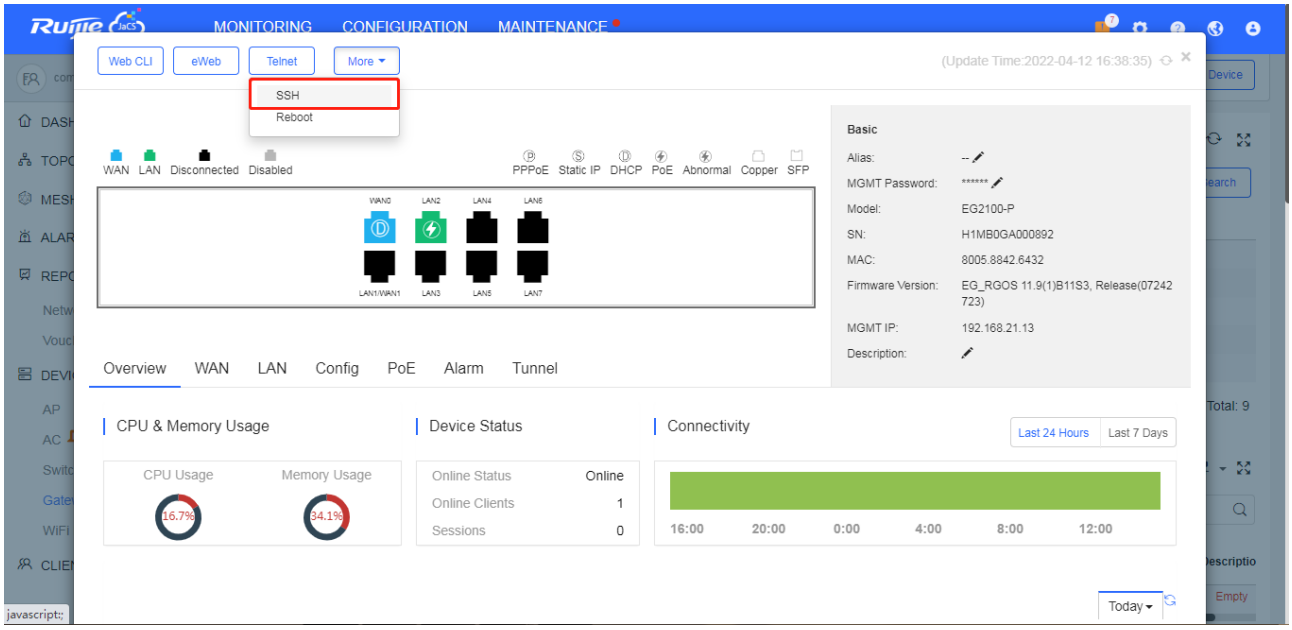
Click **Telnet**, and a window is opened to connect to the gateway by Telnet protocol. Enter CLI commands to configure the gateway.





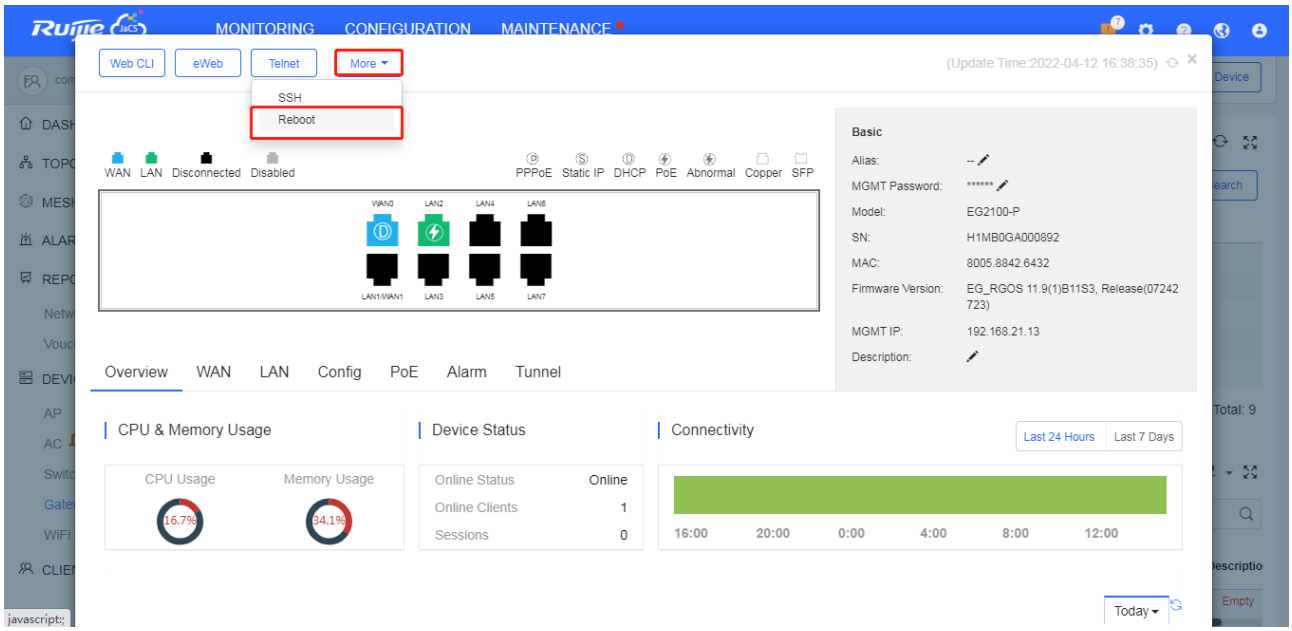
- More > SSH

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.



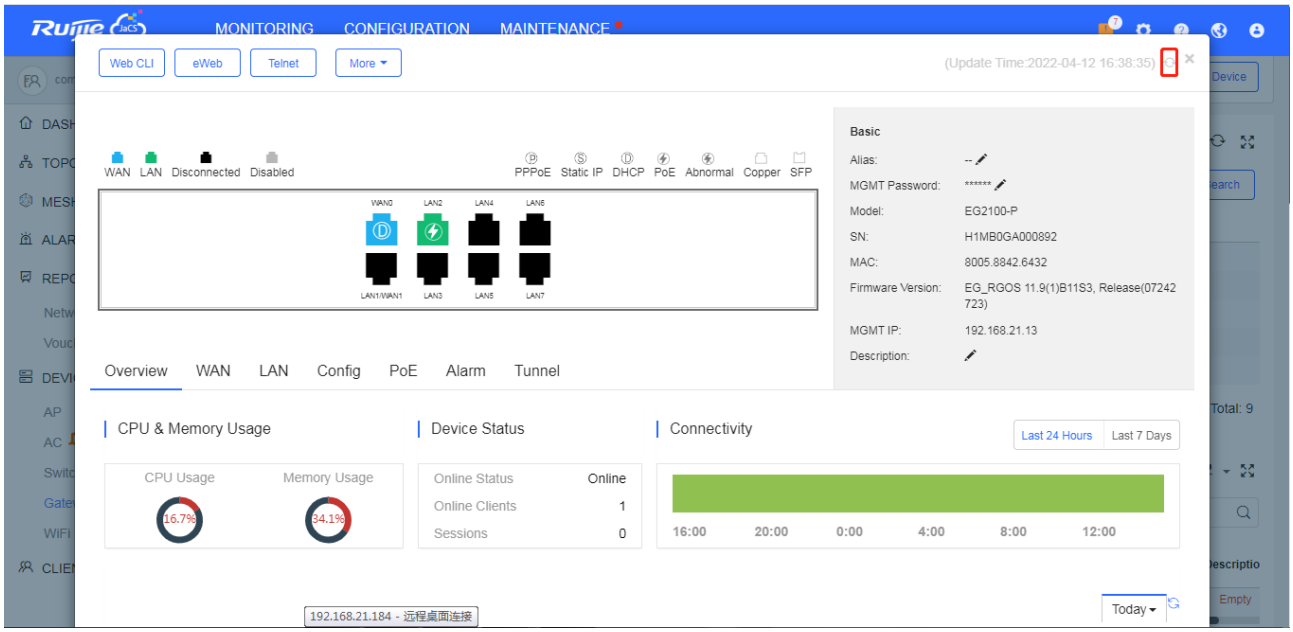
- More > Reboot

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



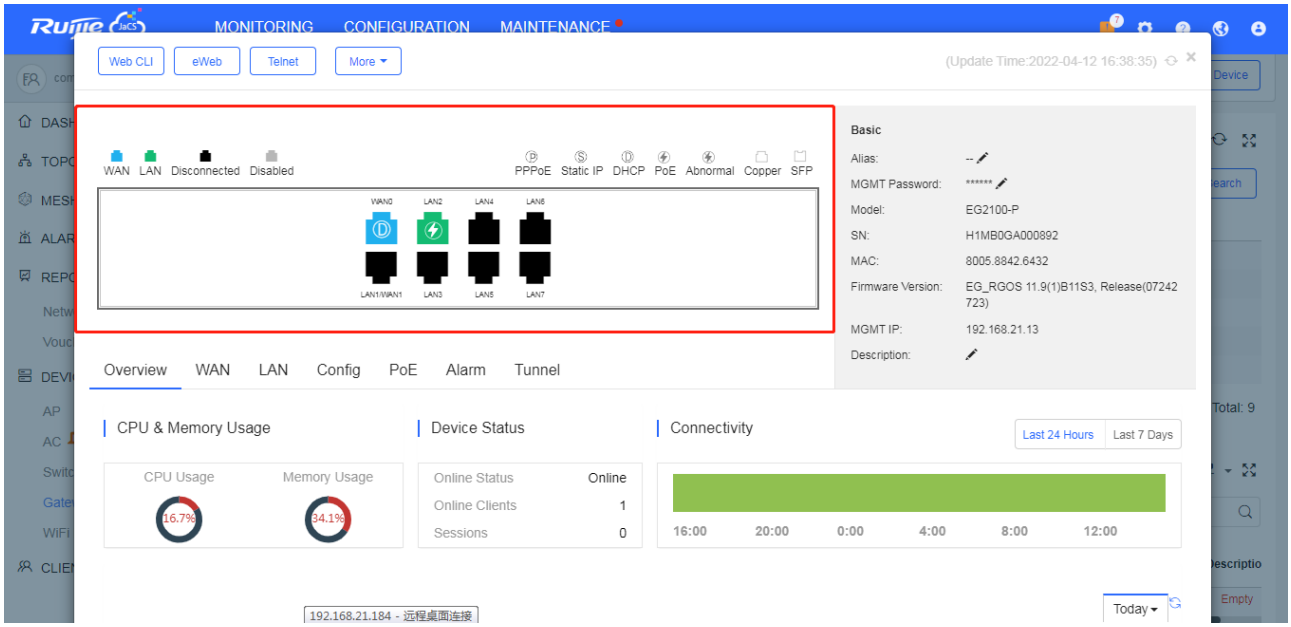
- Refresh

Click to refresh all data in the page.



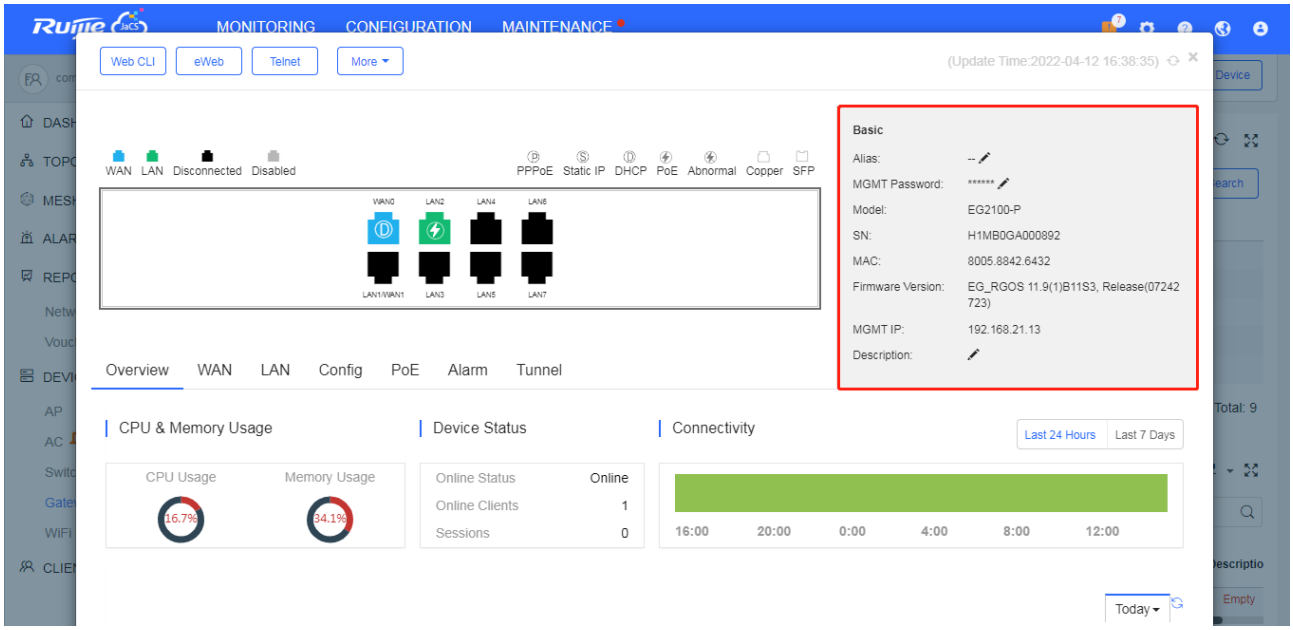
- Port Panel

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



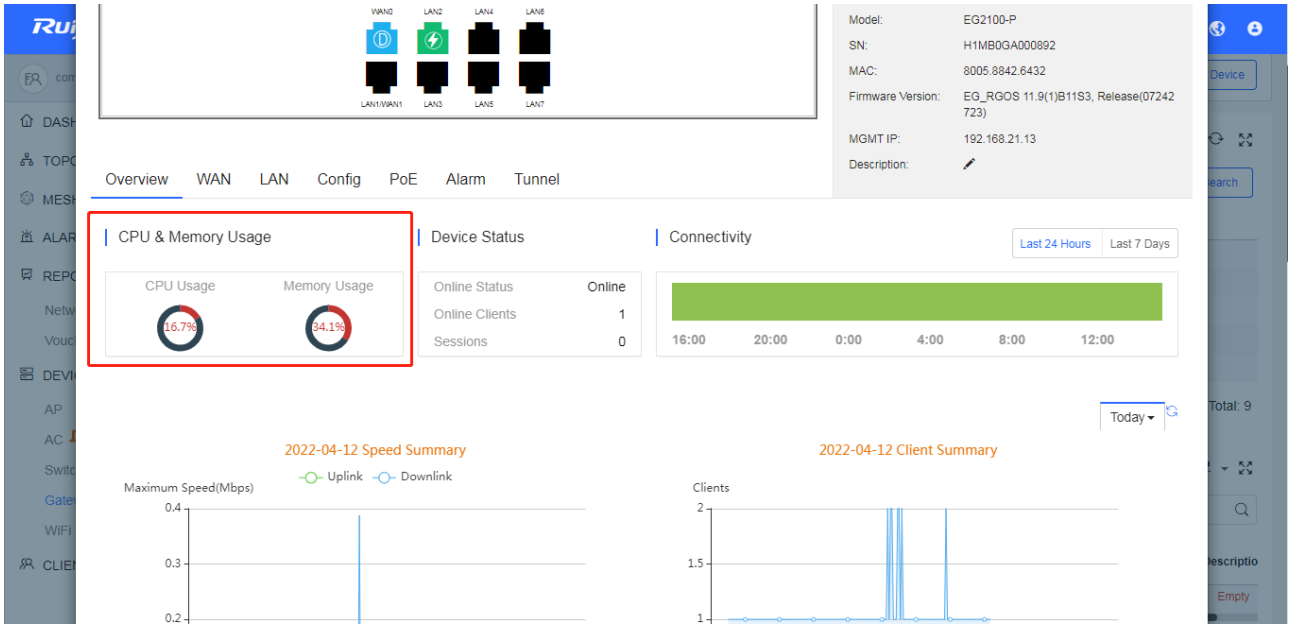
- Basic

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



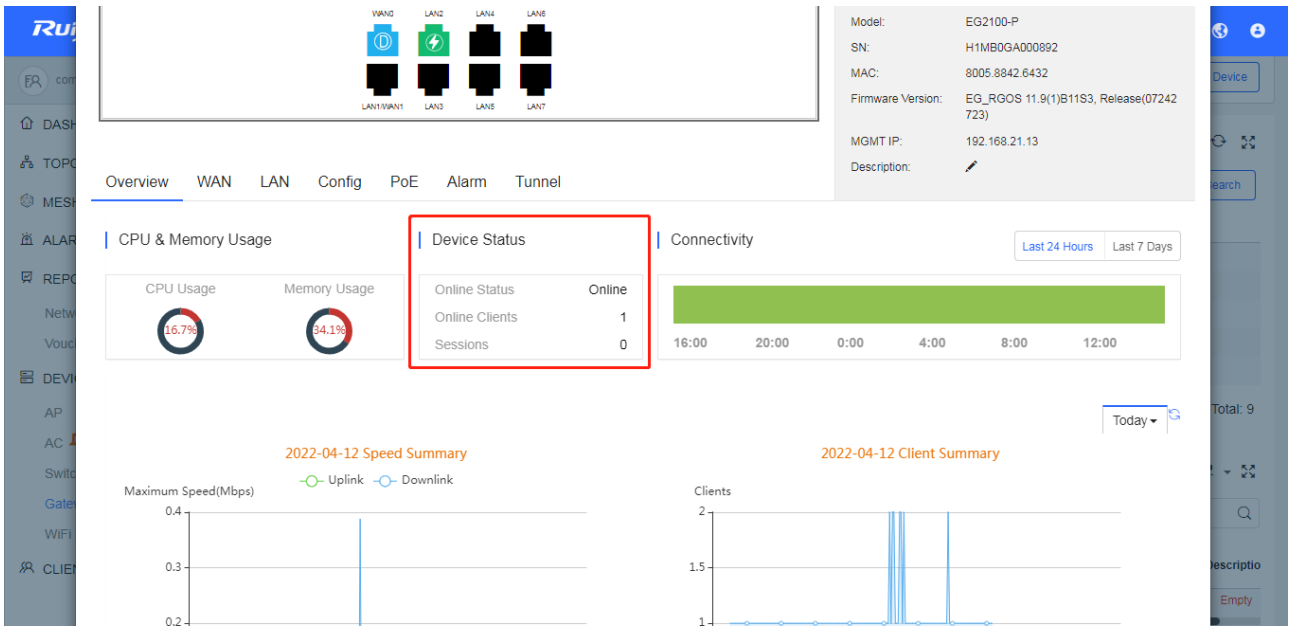
- Overview > CPU & Memory Usage

CPU & memory usage are displayed here.



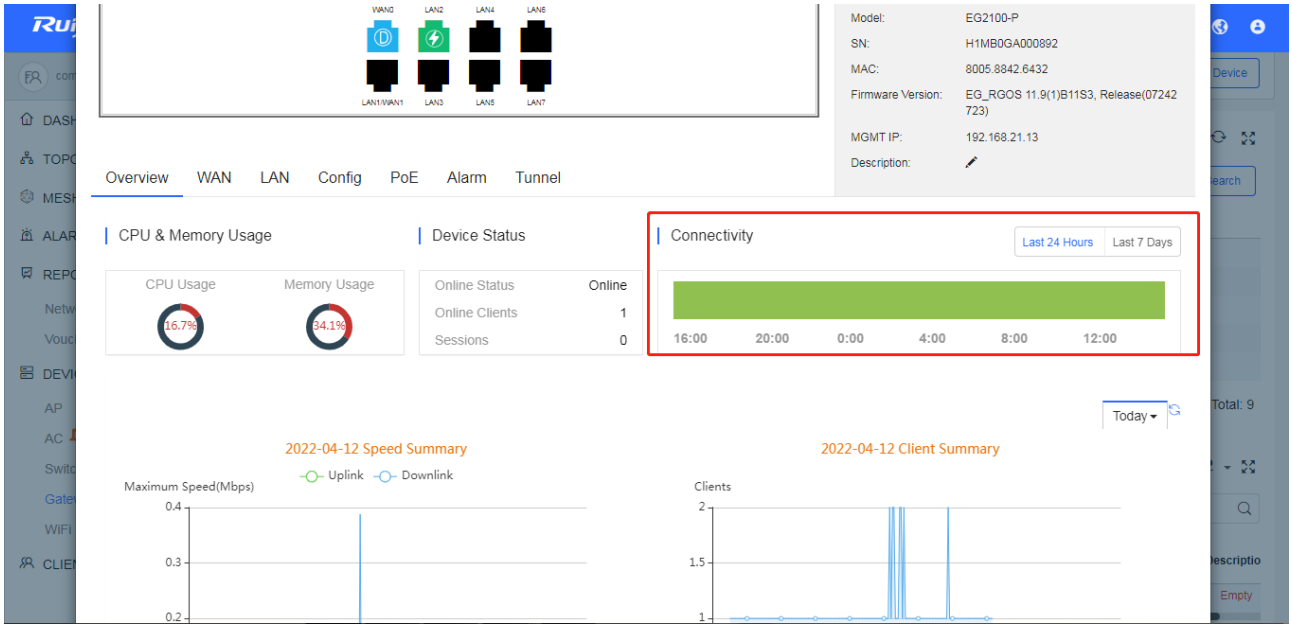
- Overview > Device Status

Device status includes online status, online clients and sessions.



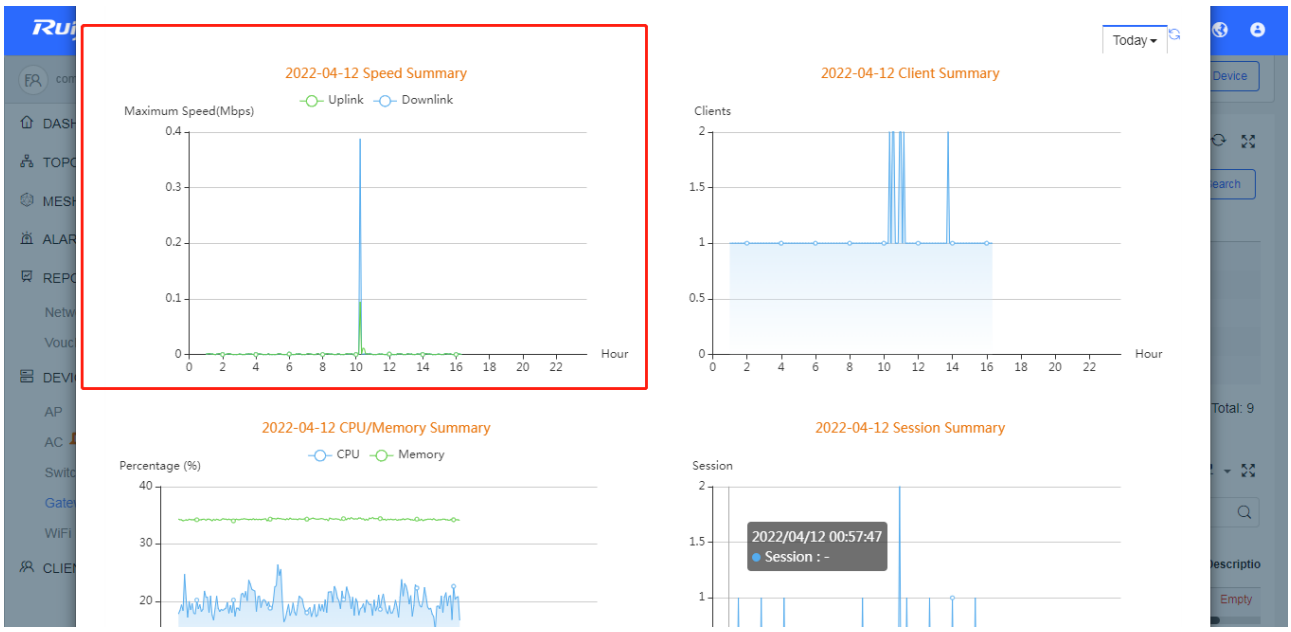
- Overview > Connectivity

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



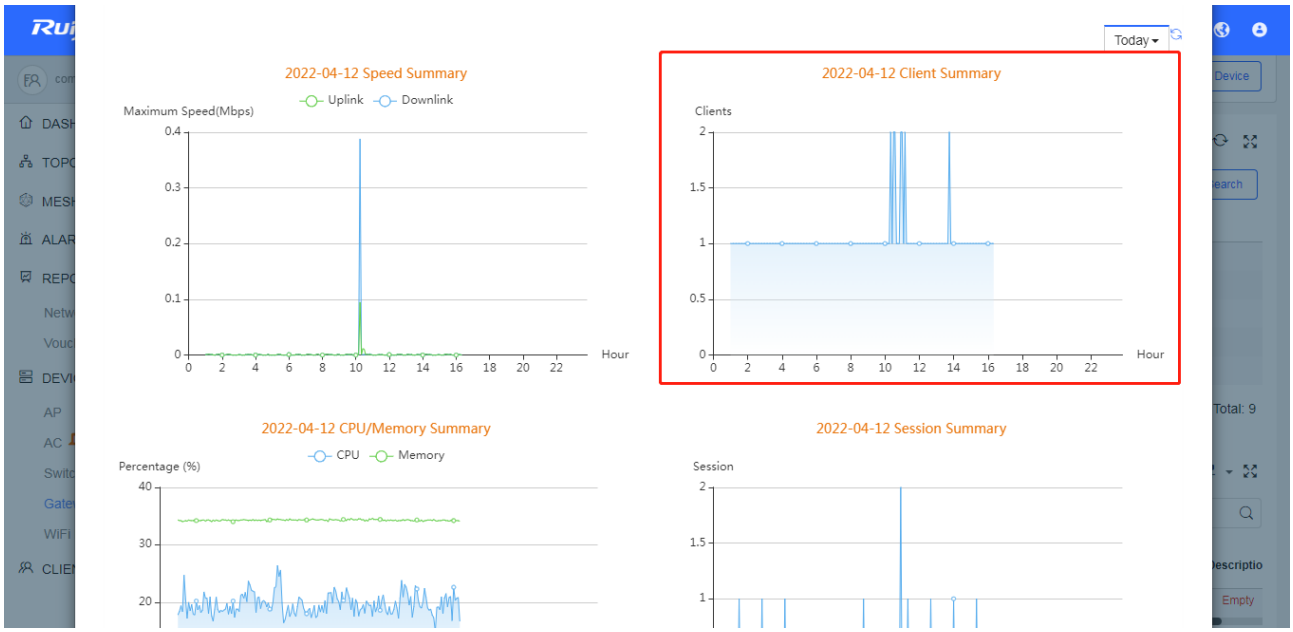
- Overview > Speed Summary

The uplink/downlink speed summary over the 24 hours is displayed.



- Overview > Client Summary

The client statistics over the 24 hours are displayed.

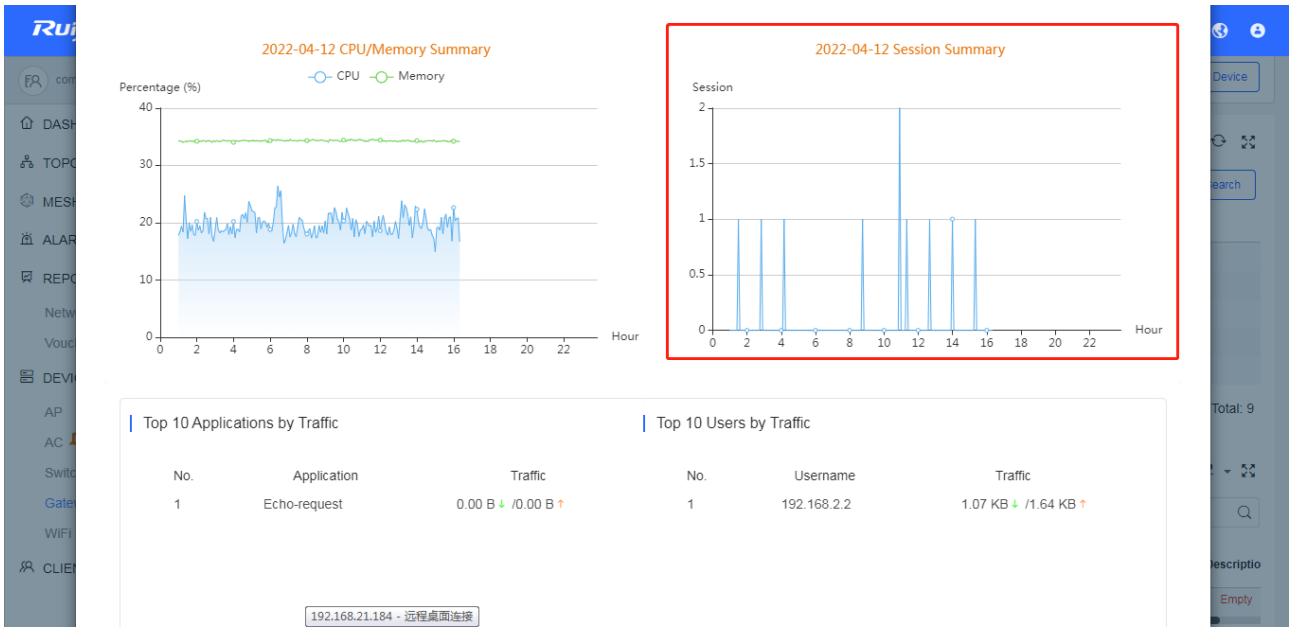


- Overview > CPU/Memory Summary

CPU/memory summary over the 24 hours are displayed.

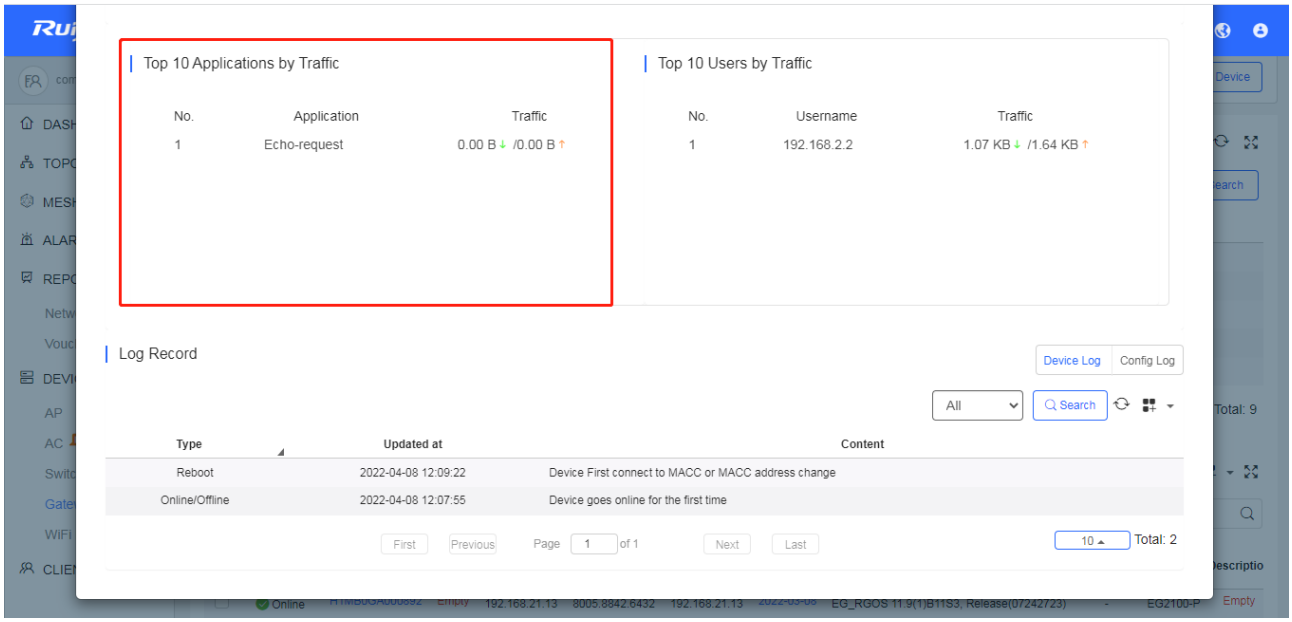
- Overview > Session Summary

Session summary over the 24 hours is displayed.



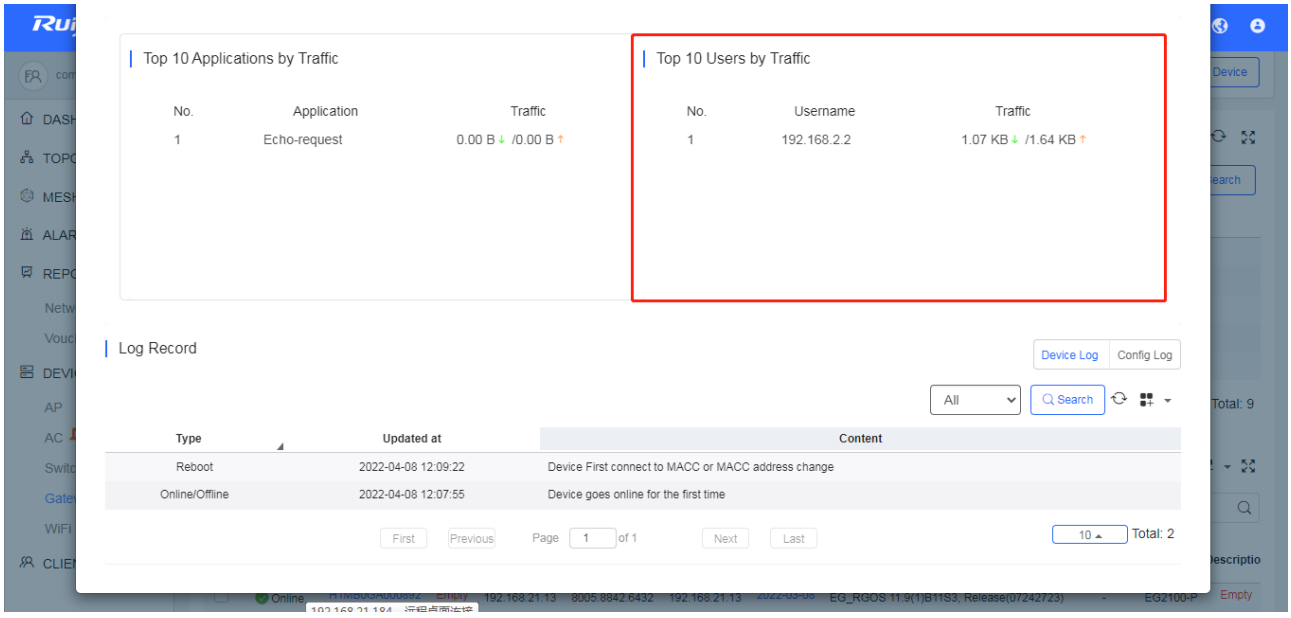
- Overview > Top 10 Applications by Traffic

Top 10 applications by downlink traffic are displayed.



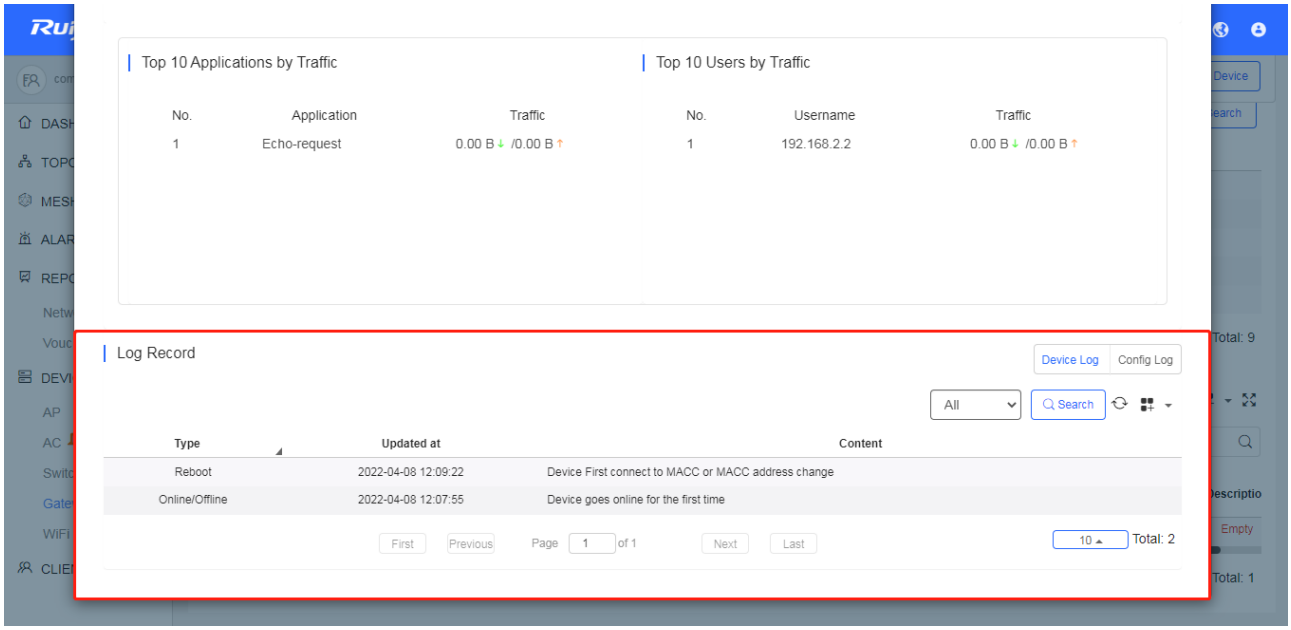
- Overview > Top 10 Users by Traffic

Top 10 users by downlink traffic are displayed.



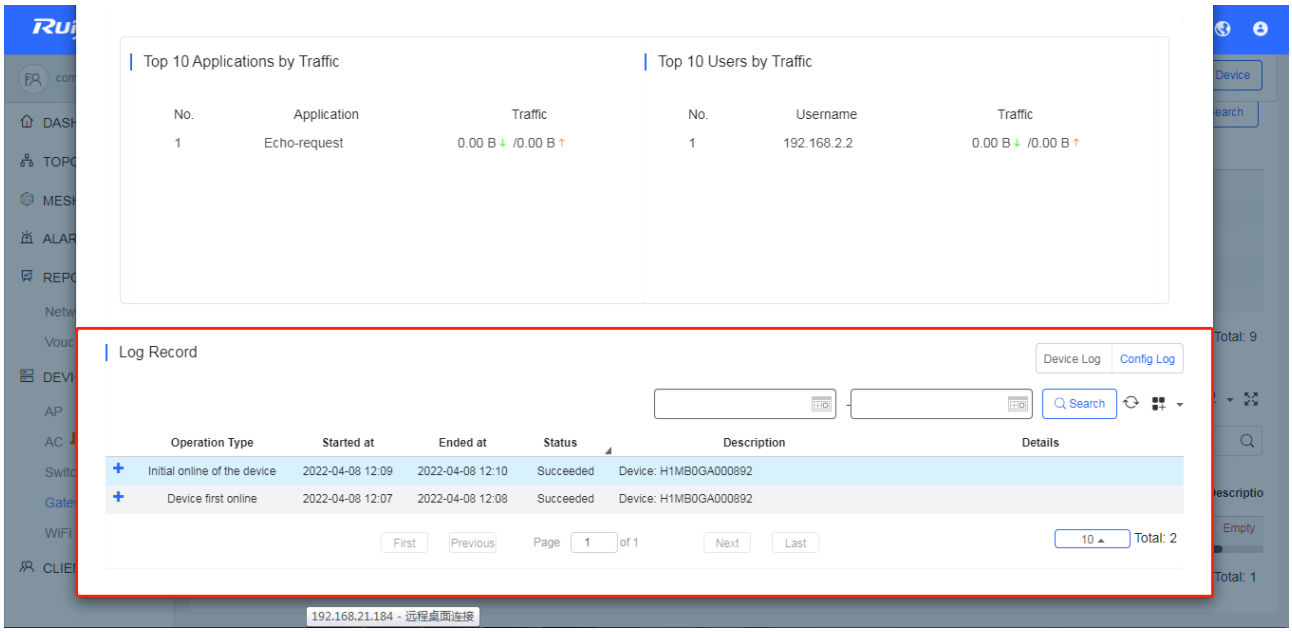
- Overview > Device Log

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



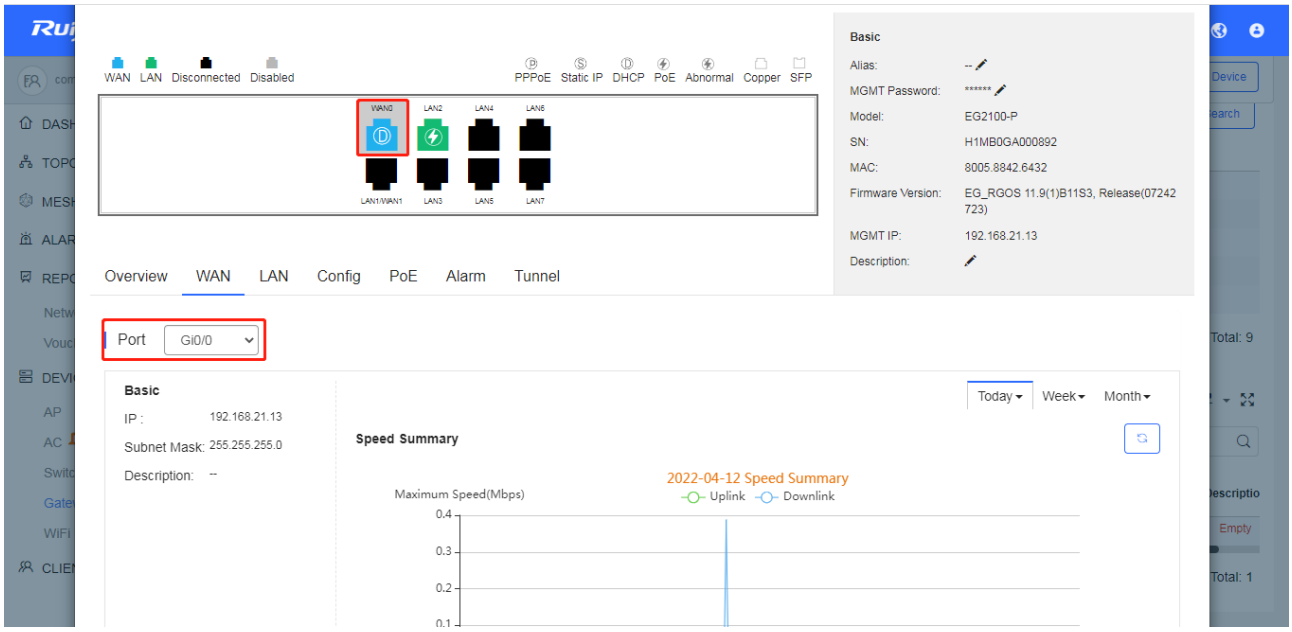
- Overview > Config Log

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



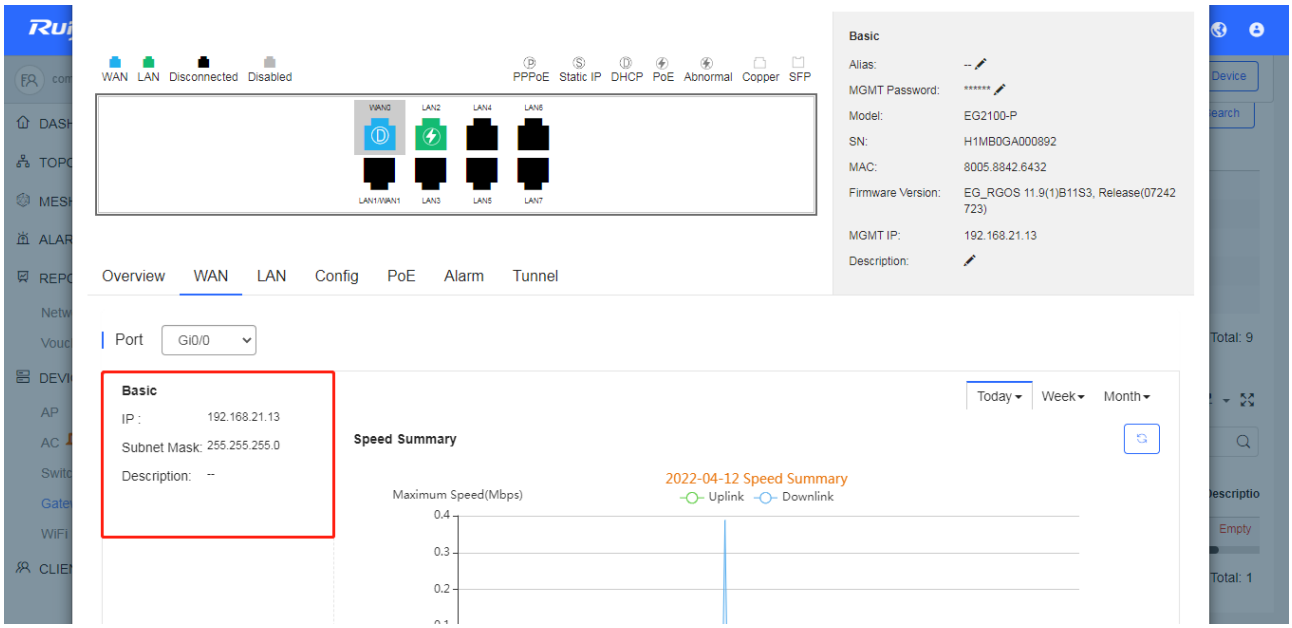
- WAN > Port

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



- WAN > Basic

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

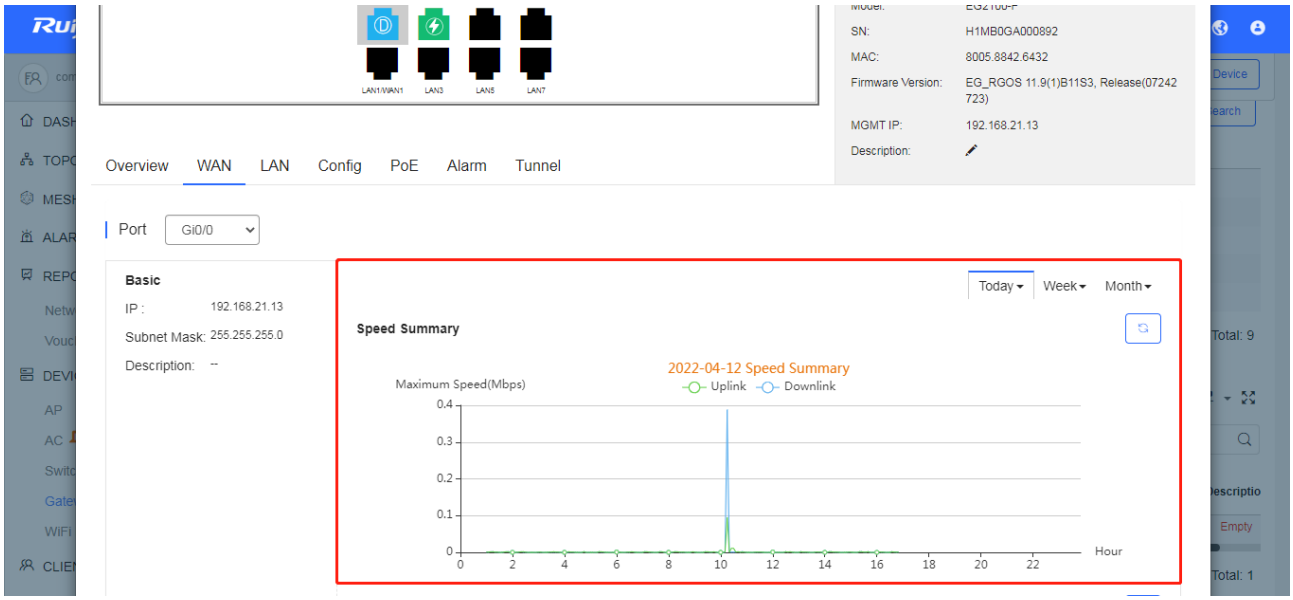
IP Type: adsl

Uplink Bandwidth: --

Downlink Bandwidth: --

- WAN > Speed Summary

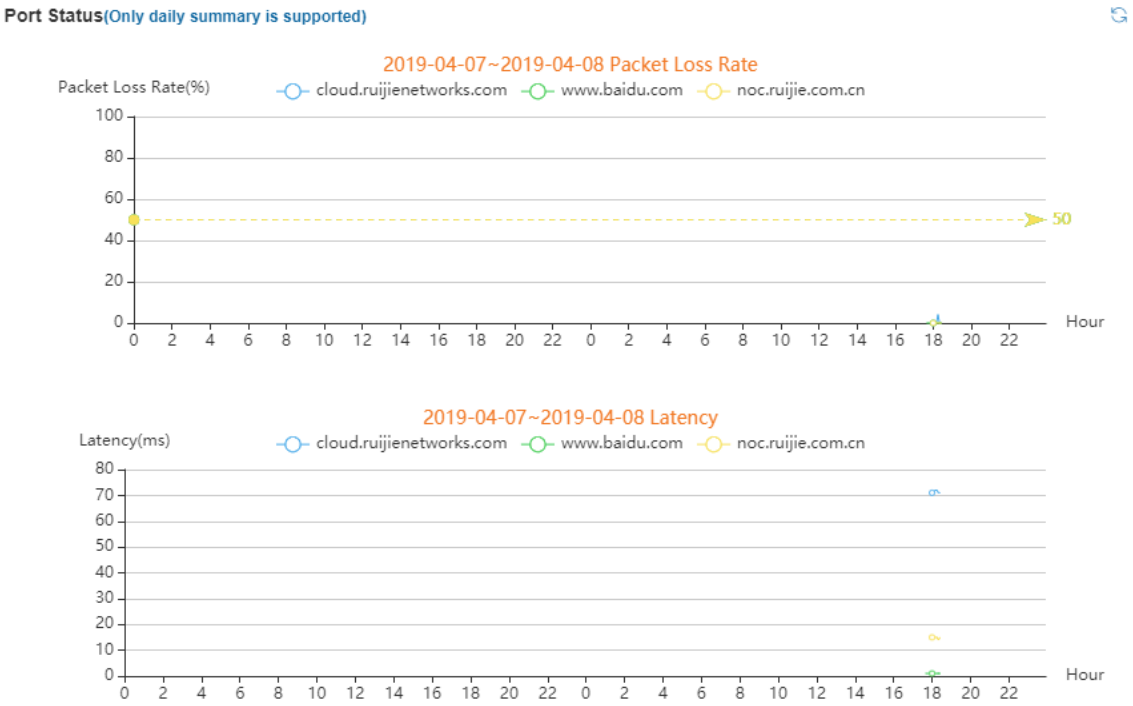
Uplink & downlink rate of WAN port are displayed. This page supports queries based on day, week and month. Click to refresh the summary.



- WAN > Port Status

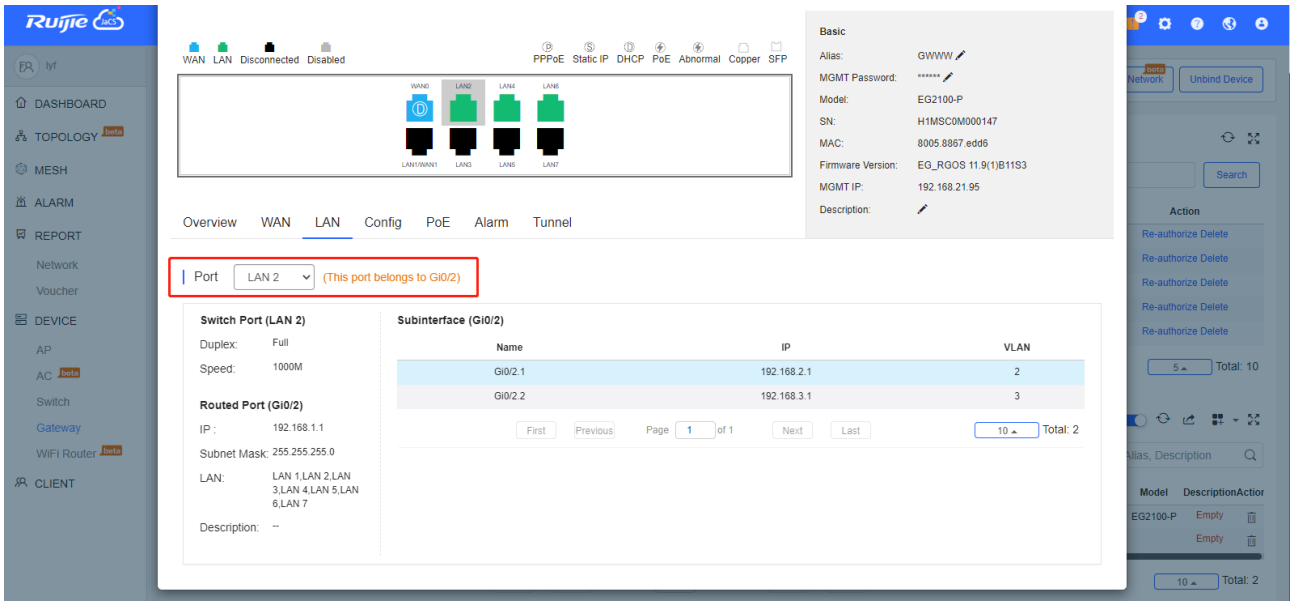
Packet loss rate and latency summary are displayed. This page supports queries based on day, week and month. Click

to refresh the summary.



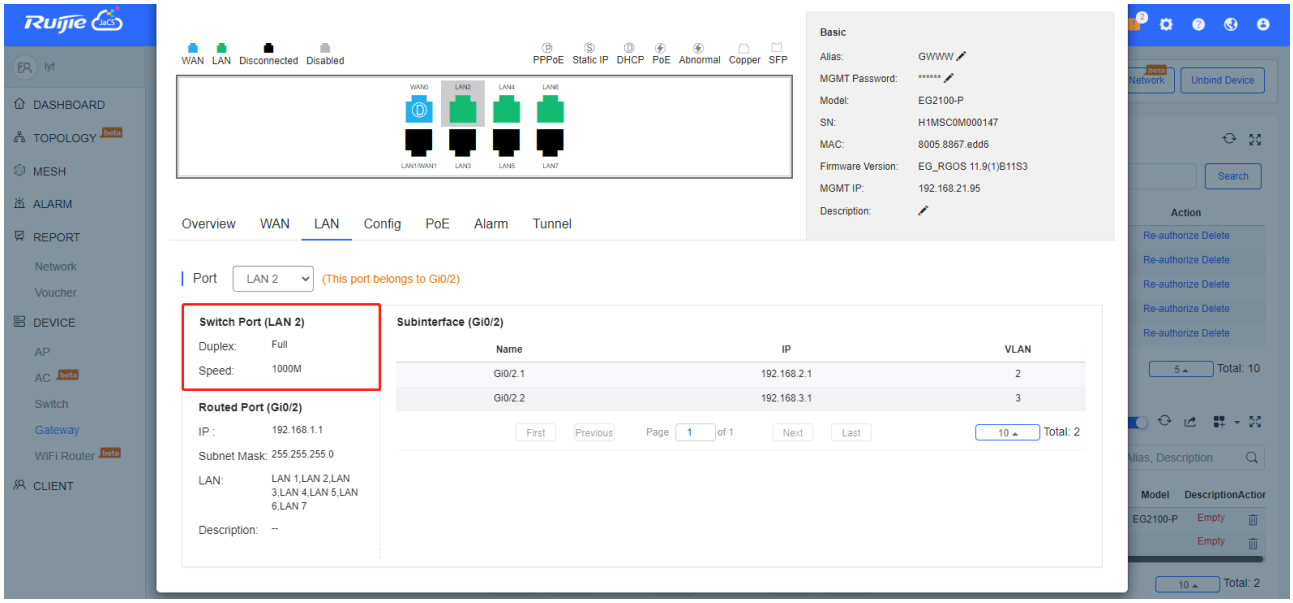
- LAN > Port

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



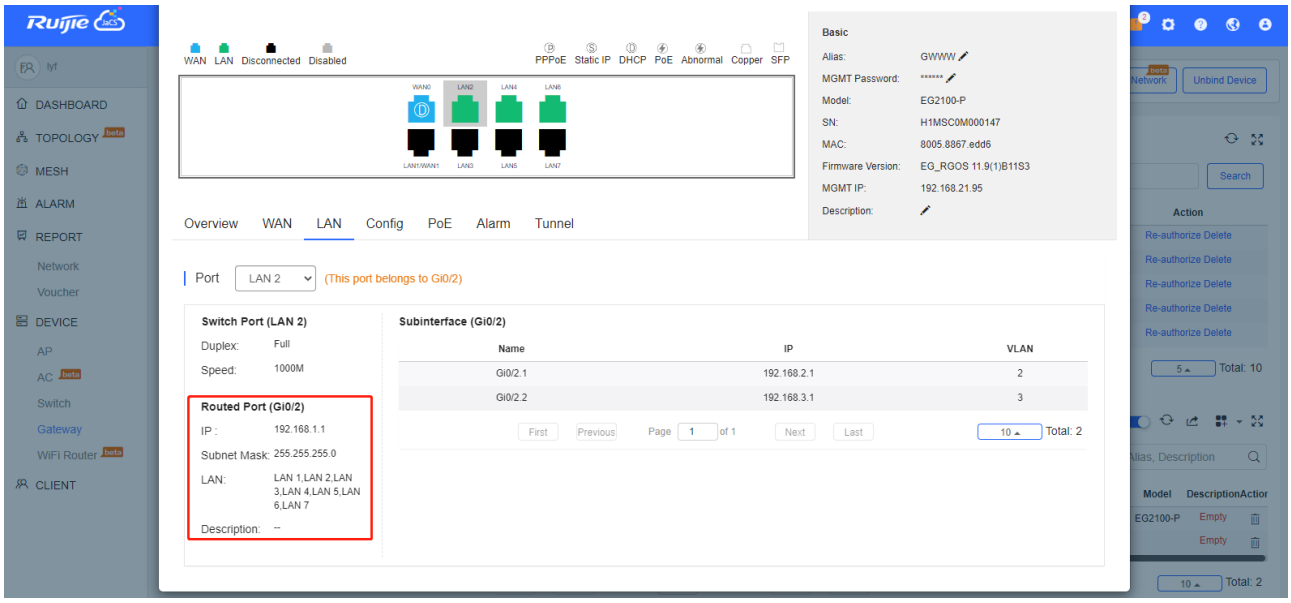
- LAN > Switch Port

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



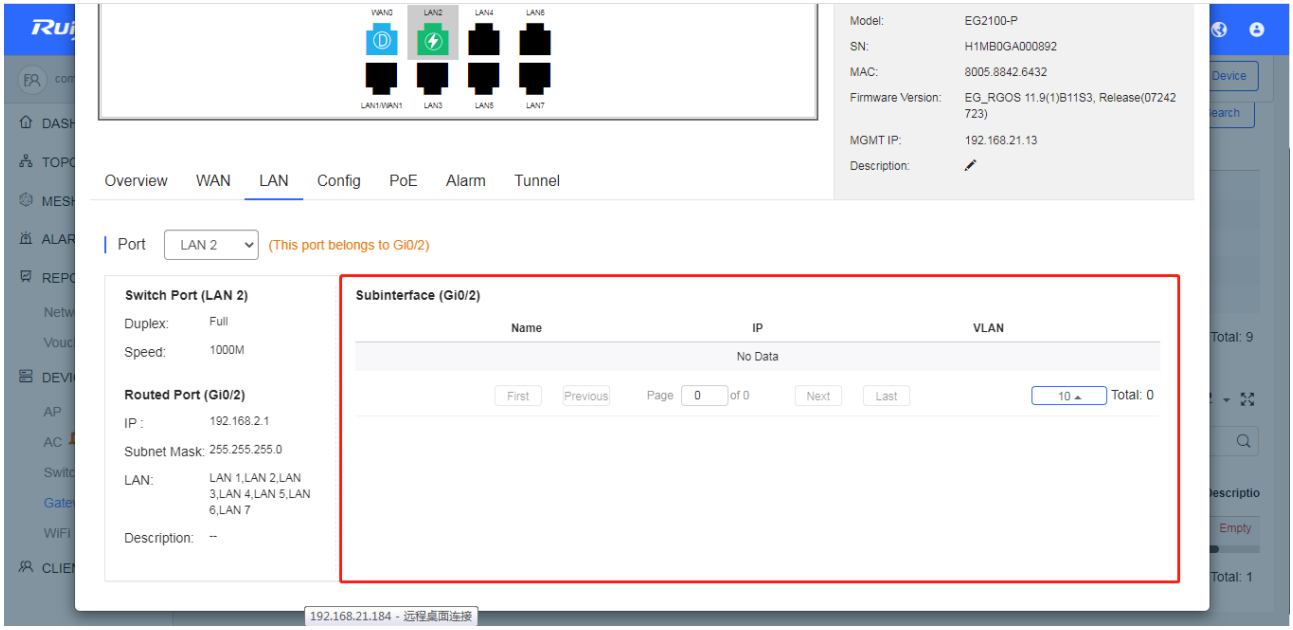
- LAN > Routed Port

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



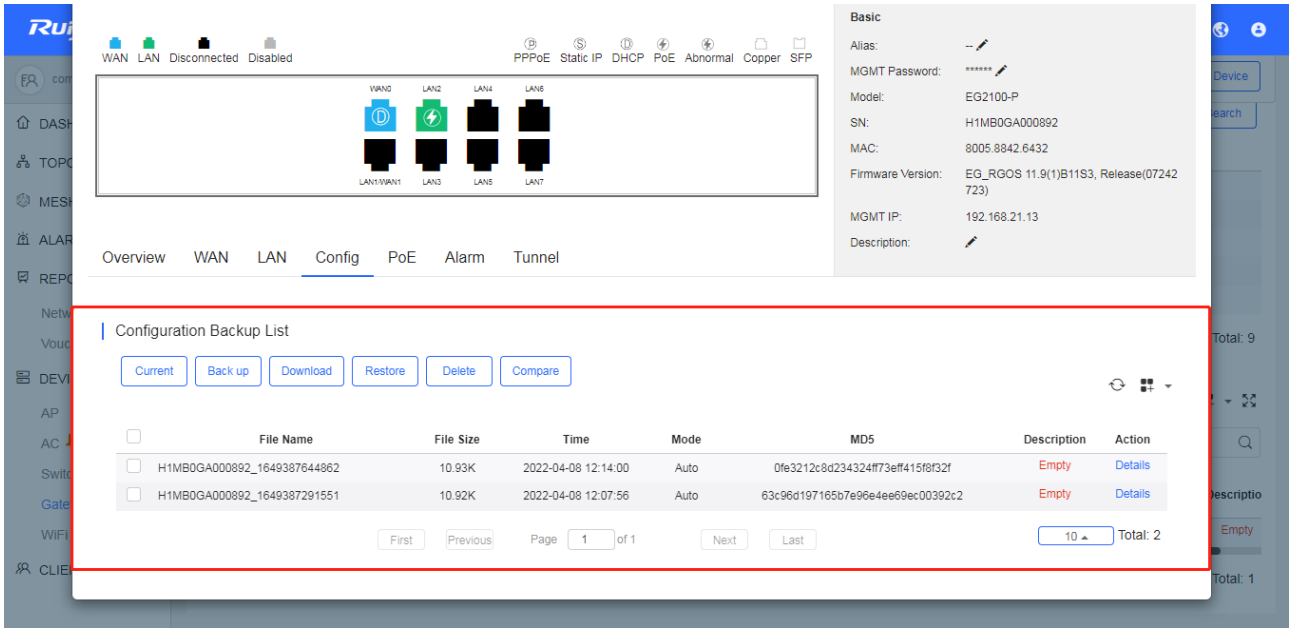
- LAN > Subinterface

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

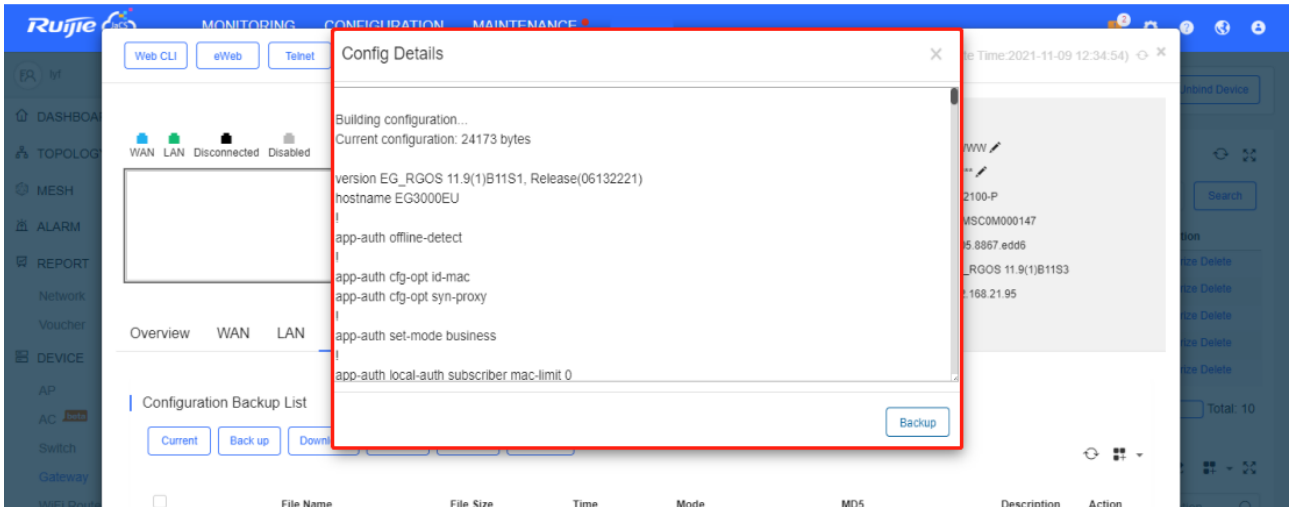


- Config > Configuration Backup List

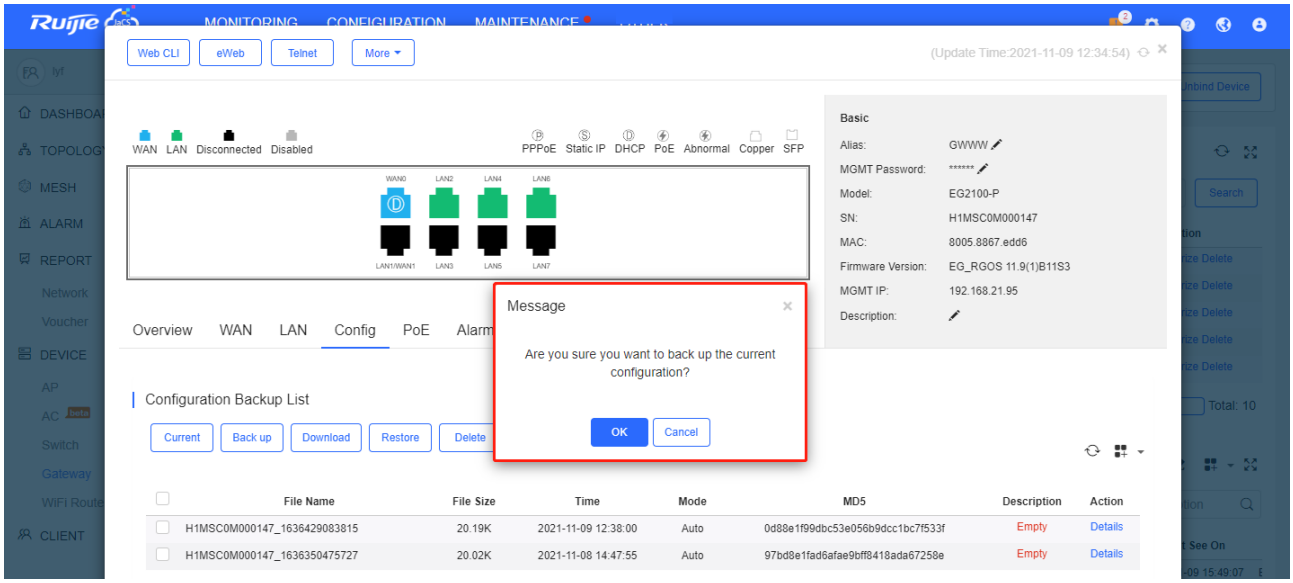
The backup records include configuration file name, size, time, mode and MD5.



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.

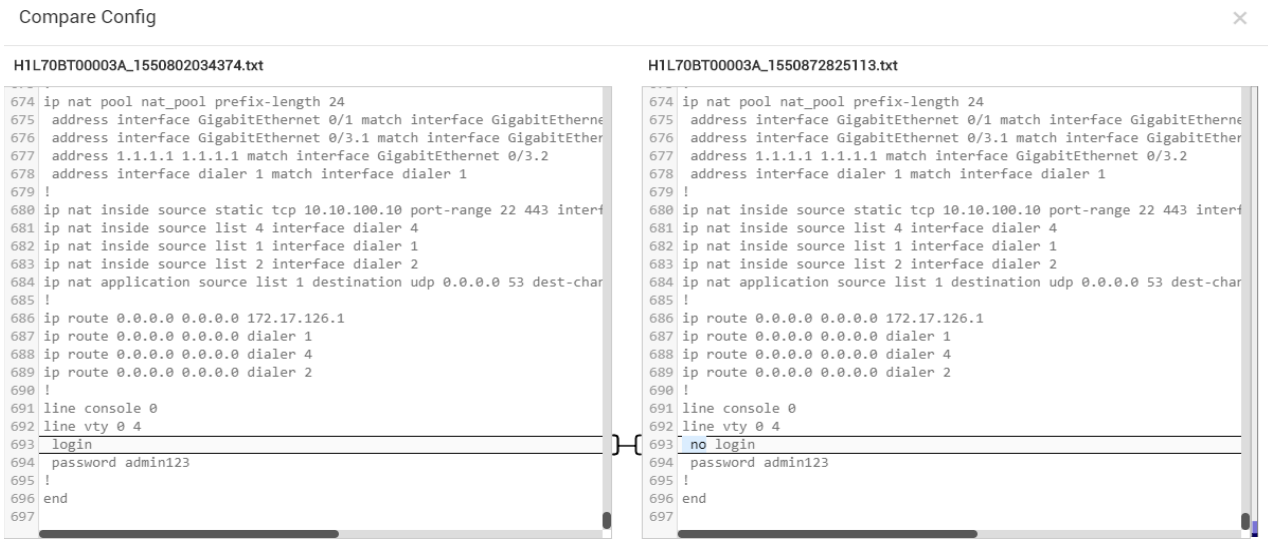


Select one record, and click **Download** to download the configuration file.

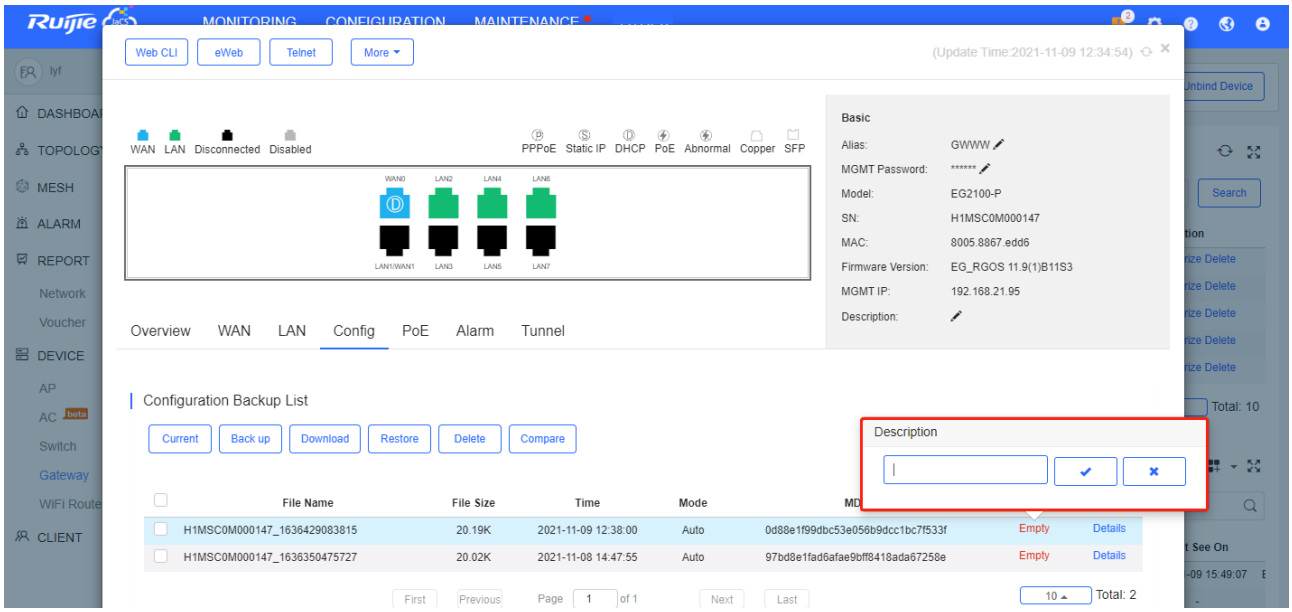
Select one record, and click **Restore** to restore the current configuration.

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

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

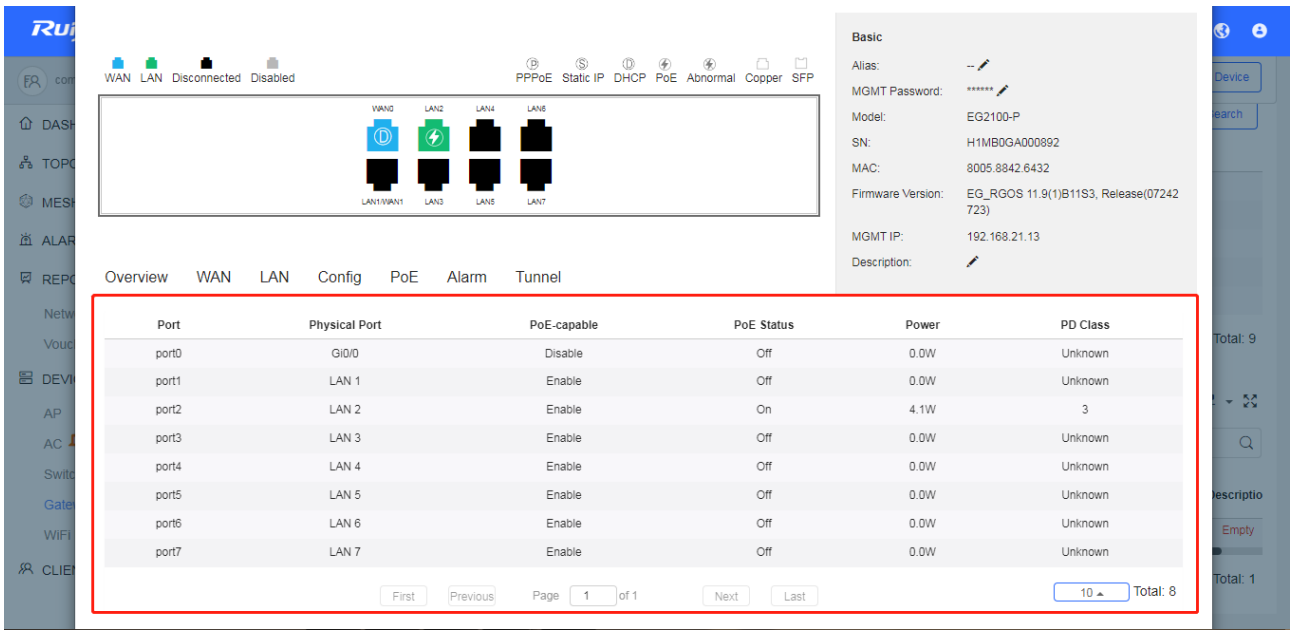


Description can be edited. Click **Details** in the **Action** column to check the backup configuration.

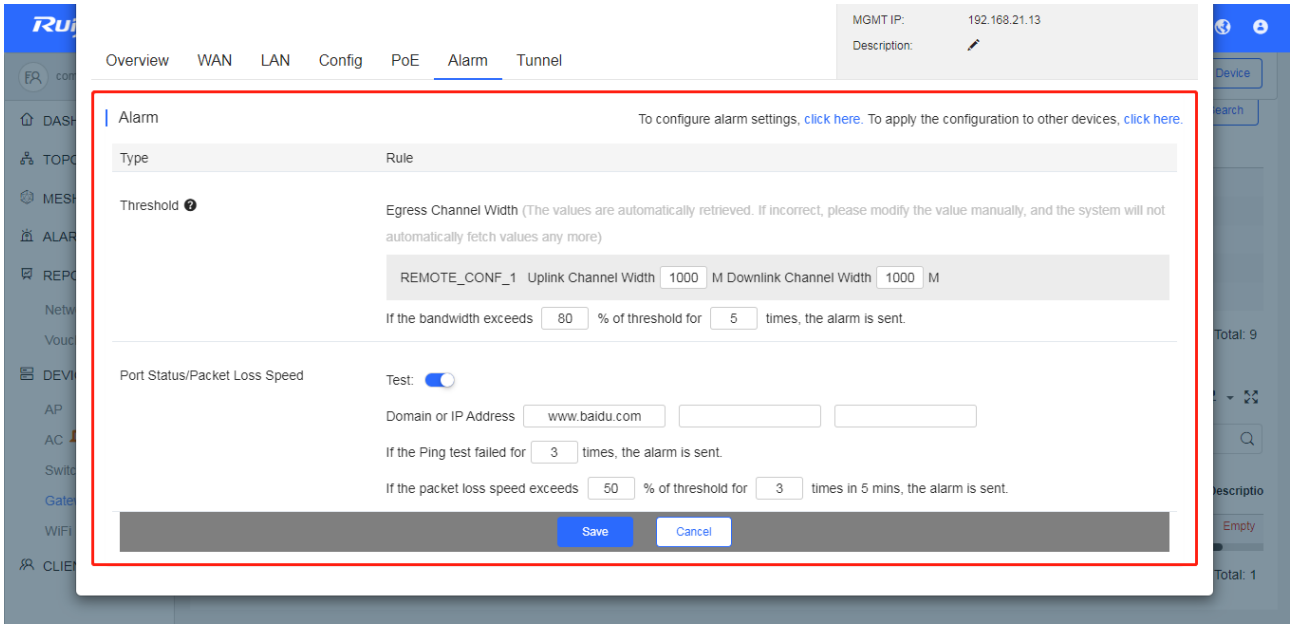


- PoE > PoE List

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



- Alarm

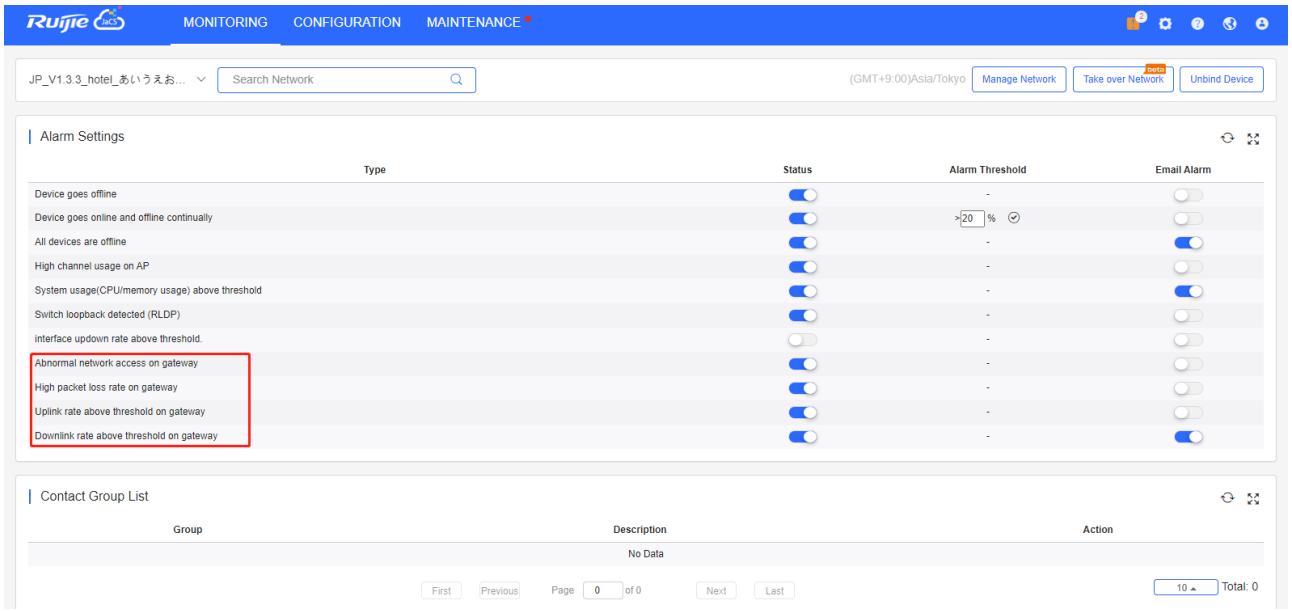


Insufficient bandwidth: When the bandwidth exceeds the specified percentage of threshold for several times, the alarm is sent. The threshold, times and percentage can be configured manually.

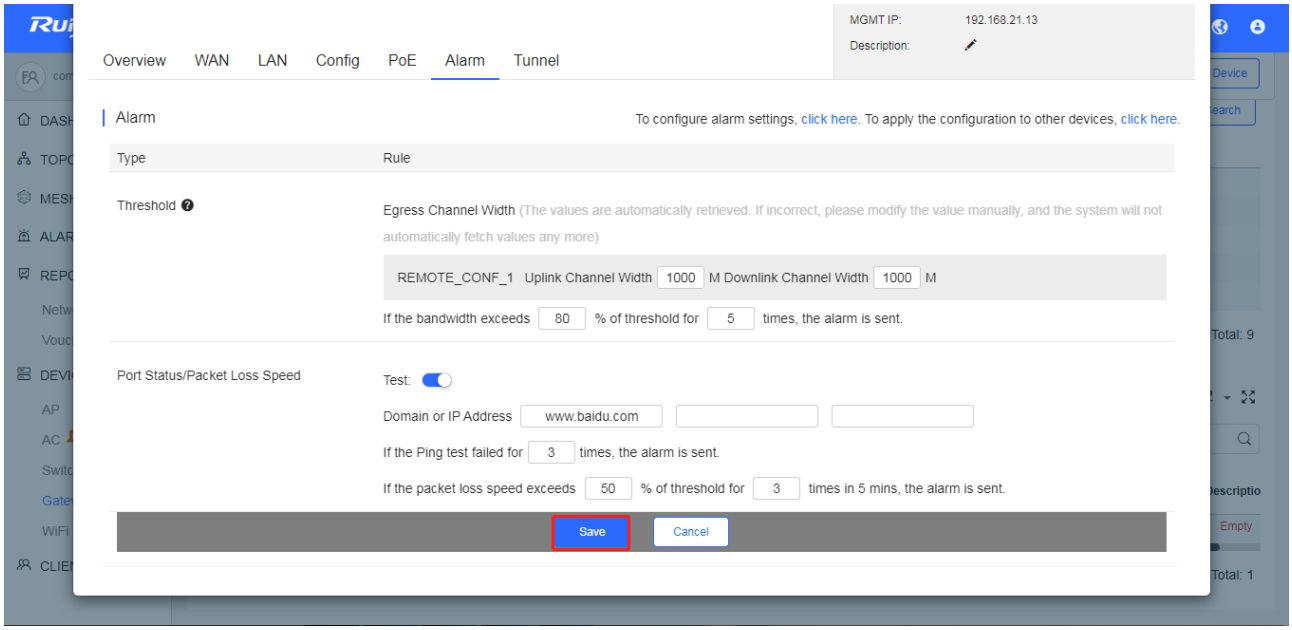
Ping failure: When the Ping test failed for the specified times, the alarm is sent. The times and domain/IP address can be configured manually.

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.

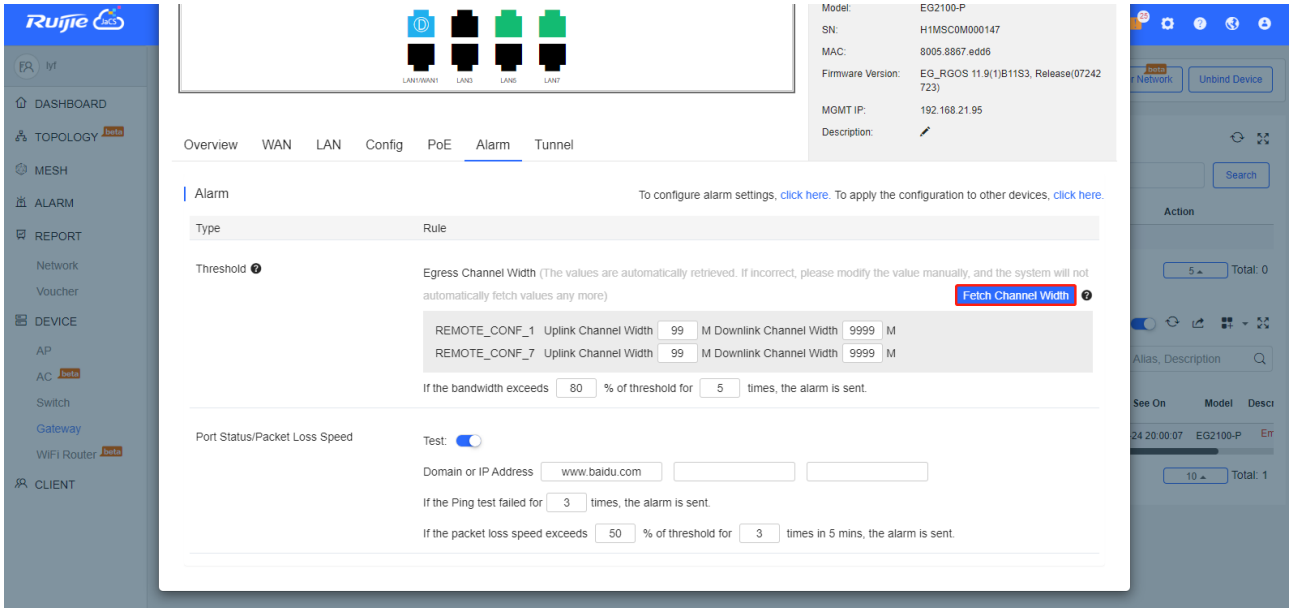
Besides, the corresponding alarm should be enabled in the **Alarm Settings** page. For insufficient bandwidth, the alarm types are **Uplink rate above threshold on gateway** and **Downlink rate above threshold on gateway**; for Ping failure, the alarm type is **Abnormal network access on gateway**; and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



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

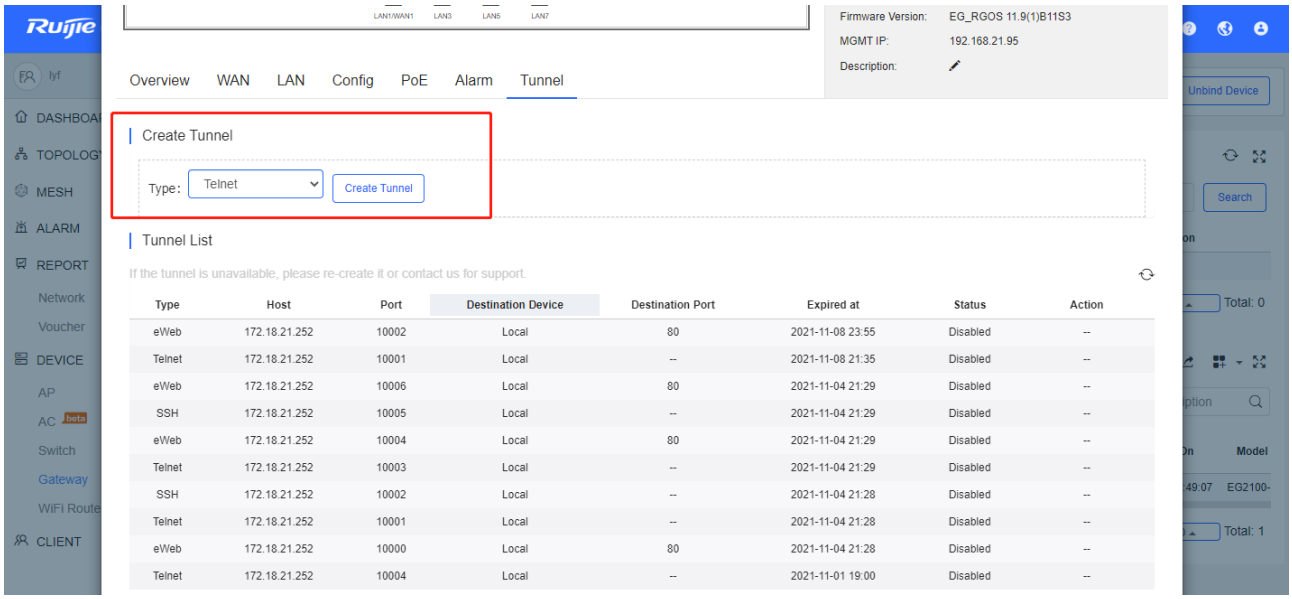


When the modified bandwidth and the actual bandwidth do not match, click **Fetch Bandwidth** to check the actual bandwidth which will then be set as the threshold.



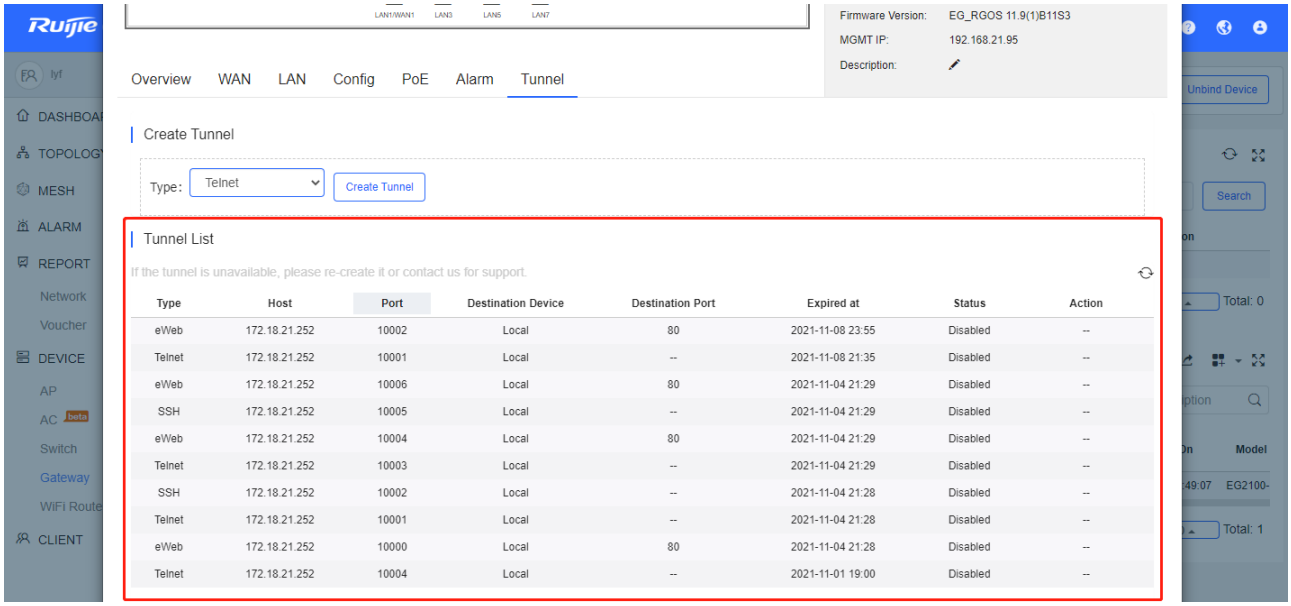
- Tunnel > Create Tunnel

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



- Tunnel > Tunnel List

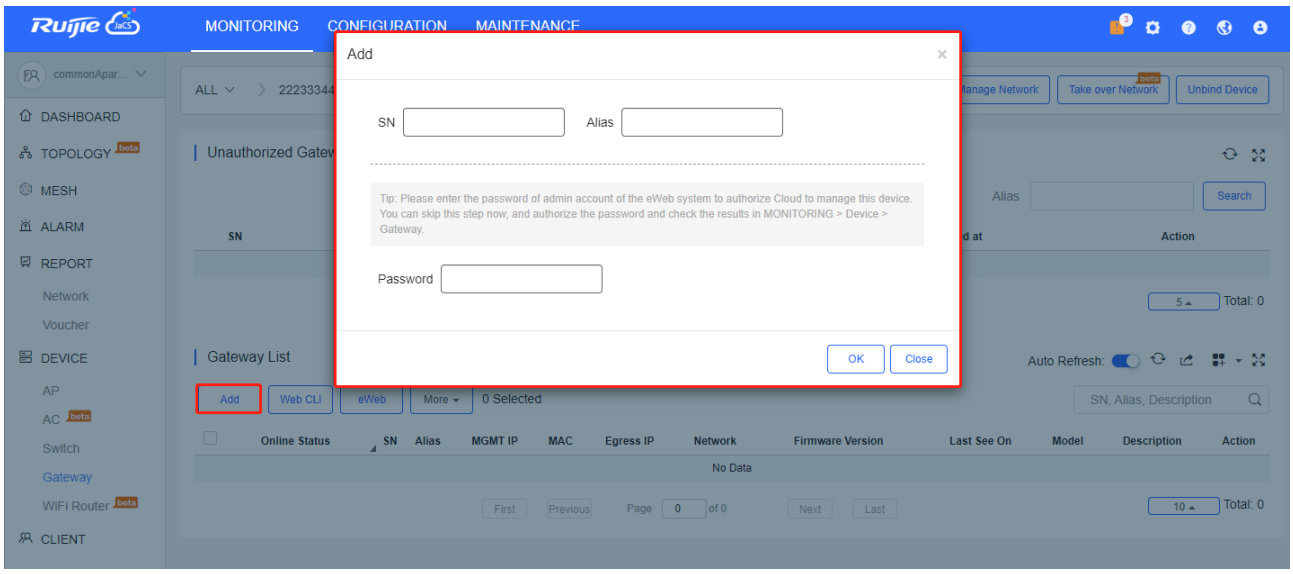
Tunnel information includes tunnel type, host, port, destination device, expiration time and status. Click **Re-create** in the **Action** column to re-create a tunnel.



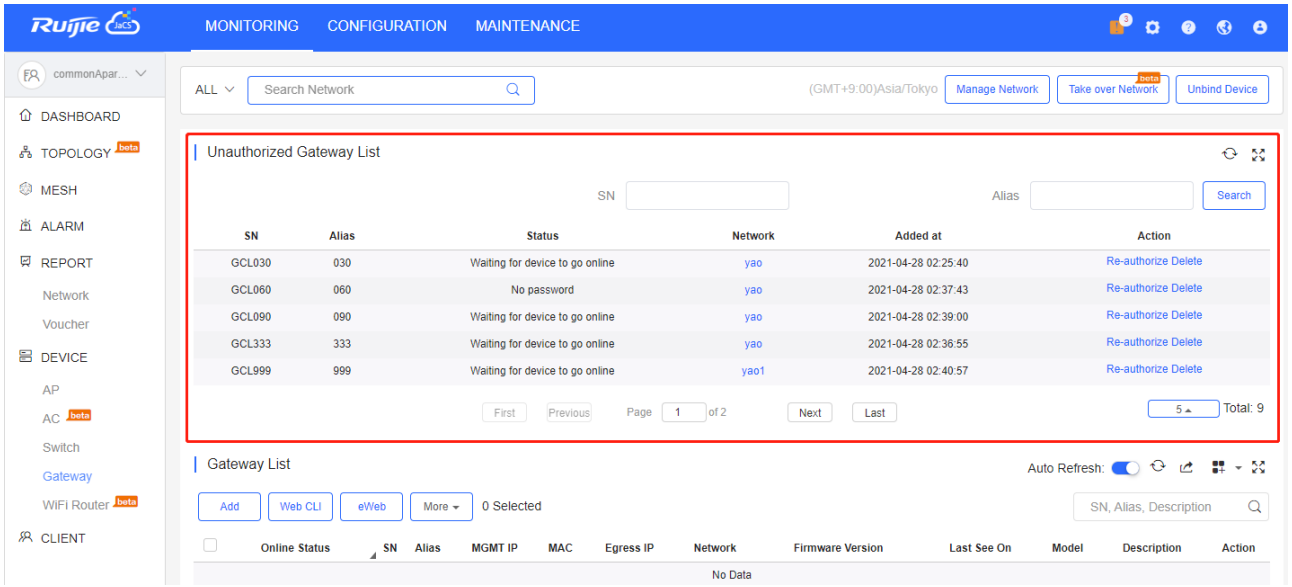
5.6.4.3 Basic Gateway Operations

- Add Gateway

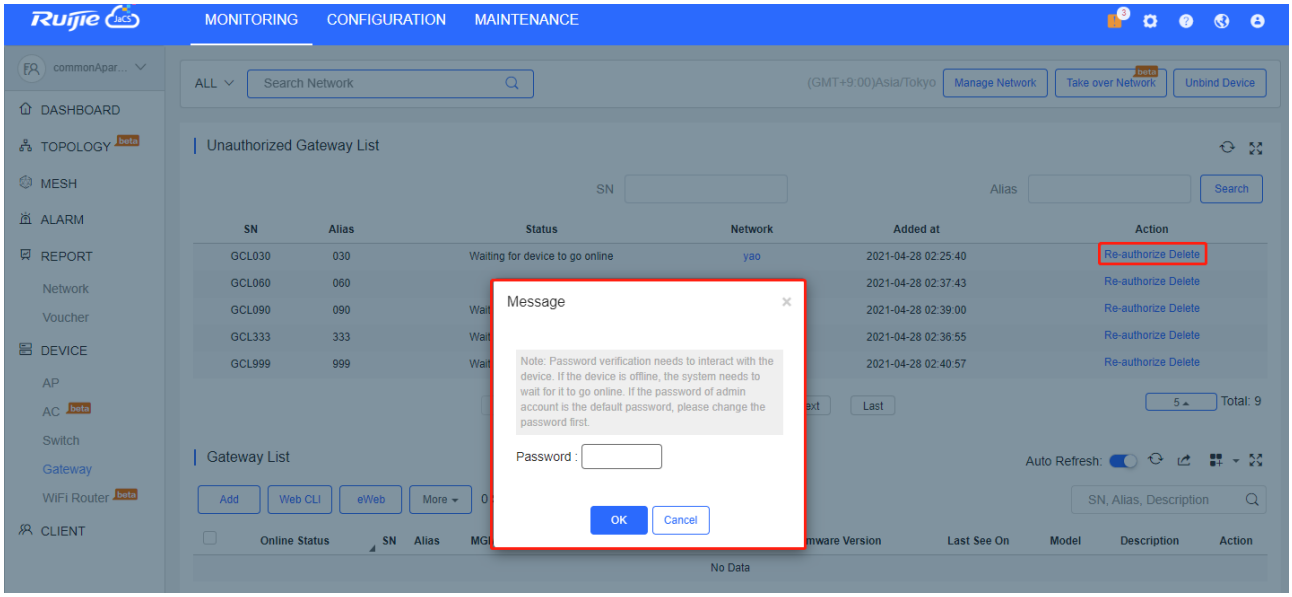
Click **Add**, enter the SN, Alias and eWeb Password, and click **OK** to add a gateway to the network. Only one gateway can be added to a network.



Before a gateway is authorized, it is displayed in the **Unauthorized Gateway List**.

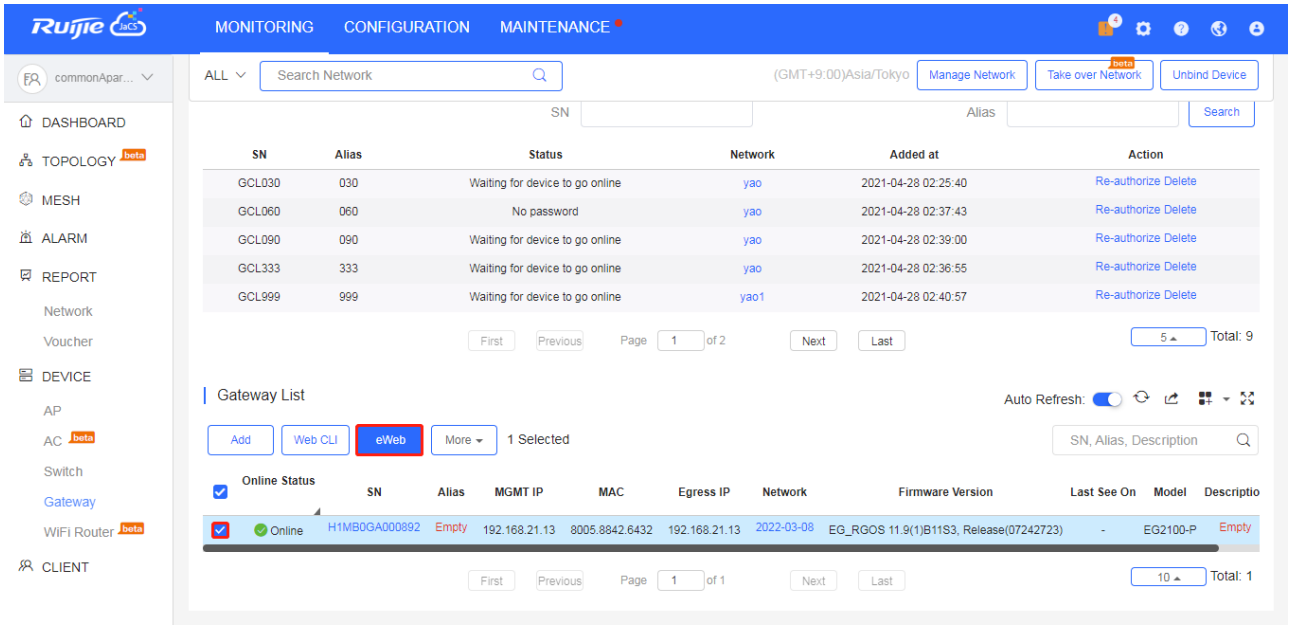


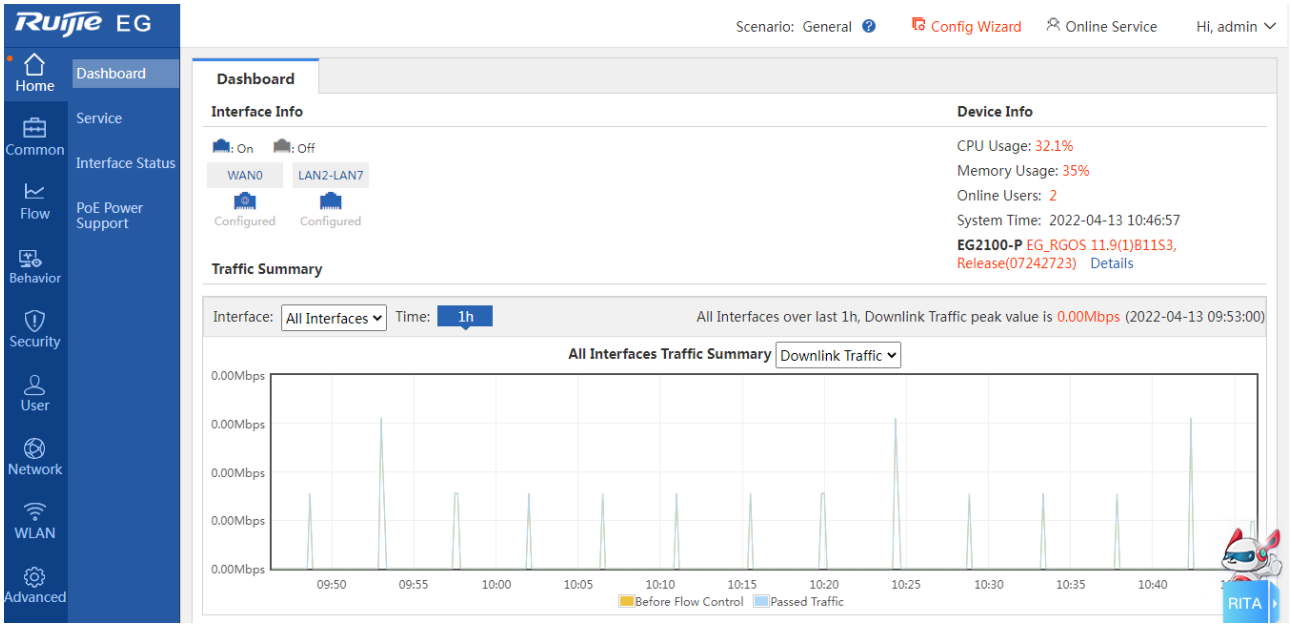
If authorization fails, you can click **Re-authorize** in the **Action** column to re-enter the Web password to re-authorize the device.



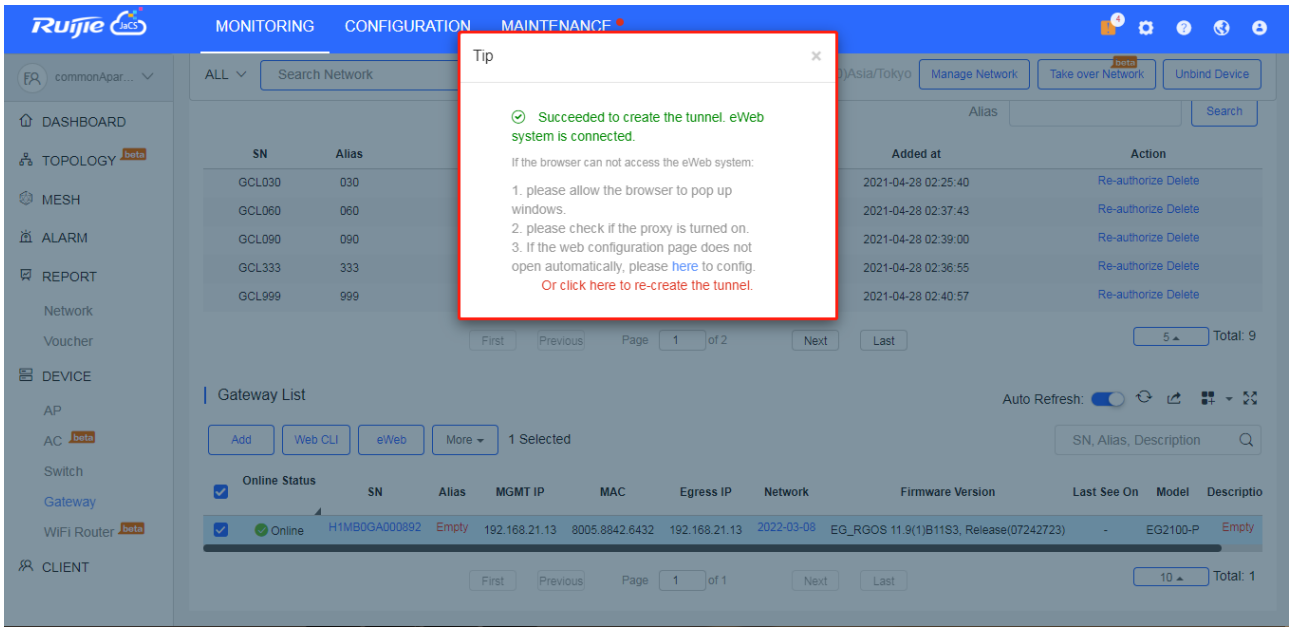
- eWeb

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.



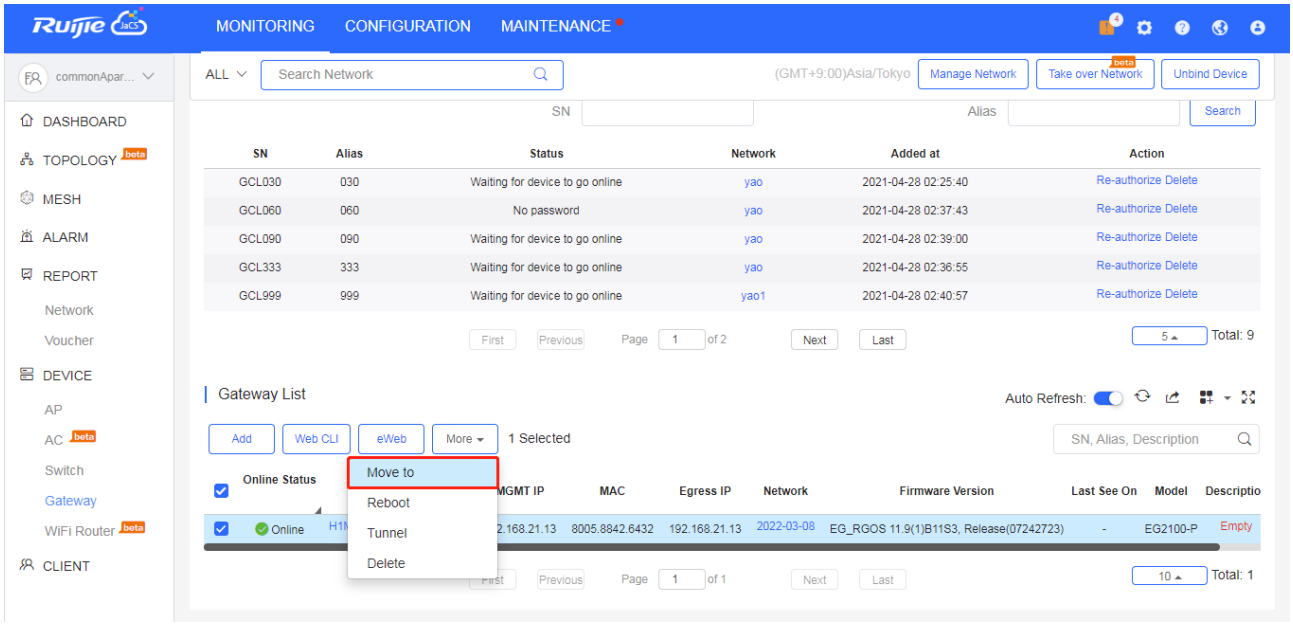


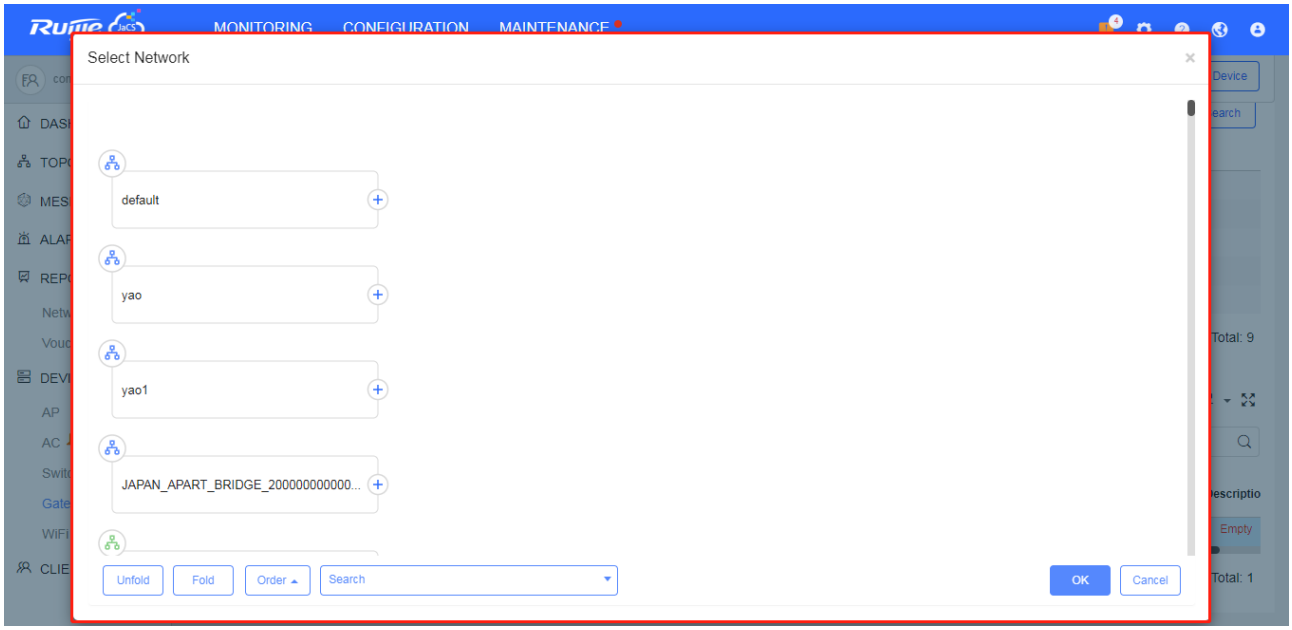
If a tunnel is created successfully but the eWeb page does not automatically open, the system will pop up a message. The user can manually click the link to open the page.



- More > Move to

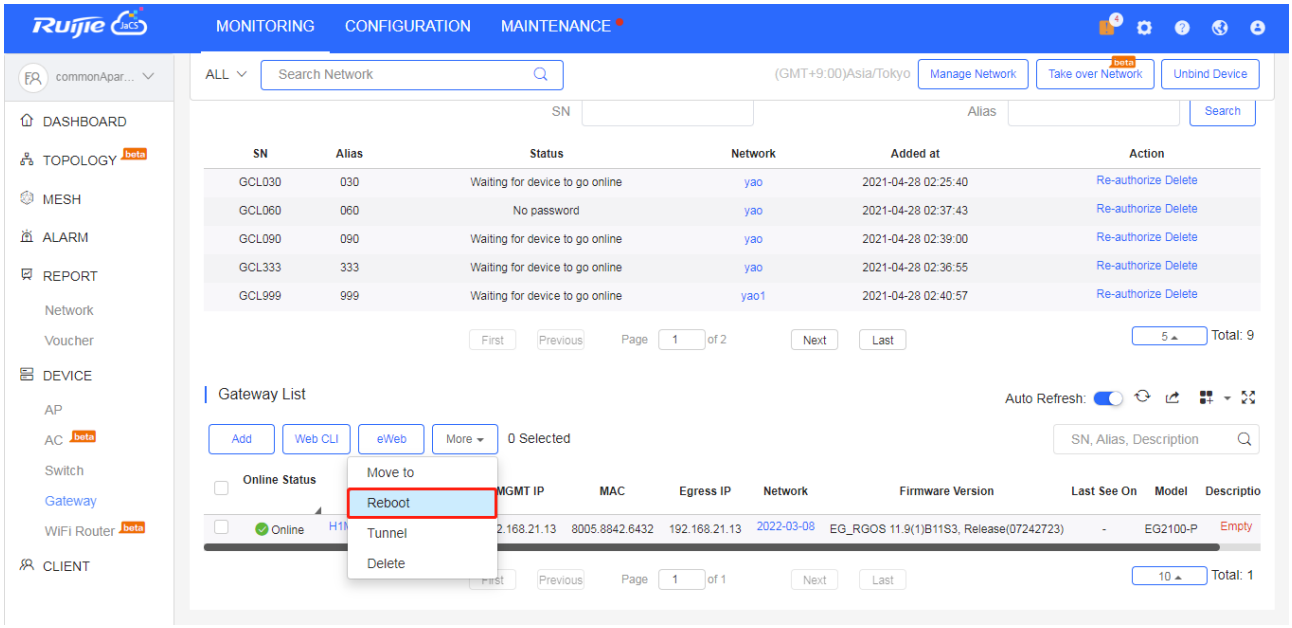
Select the device in the **Gateway List**, click **More** > **Move to**, select the new network and click **OK**. Only one gateway can be moved at a time.





- More > Reboot

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

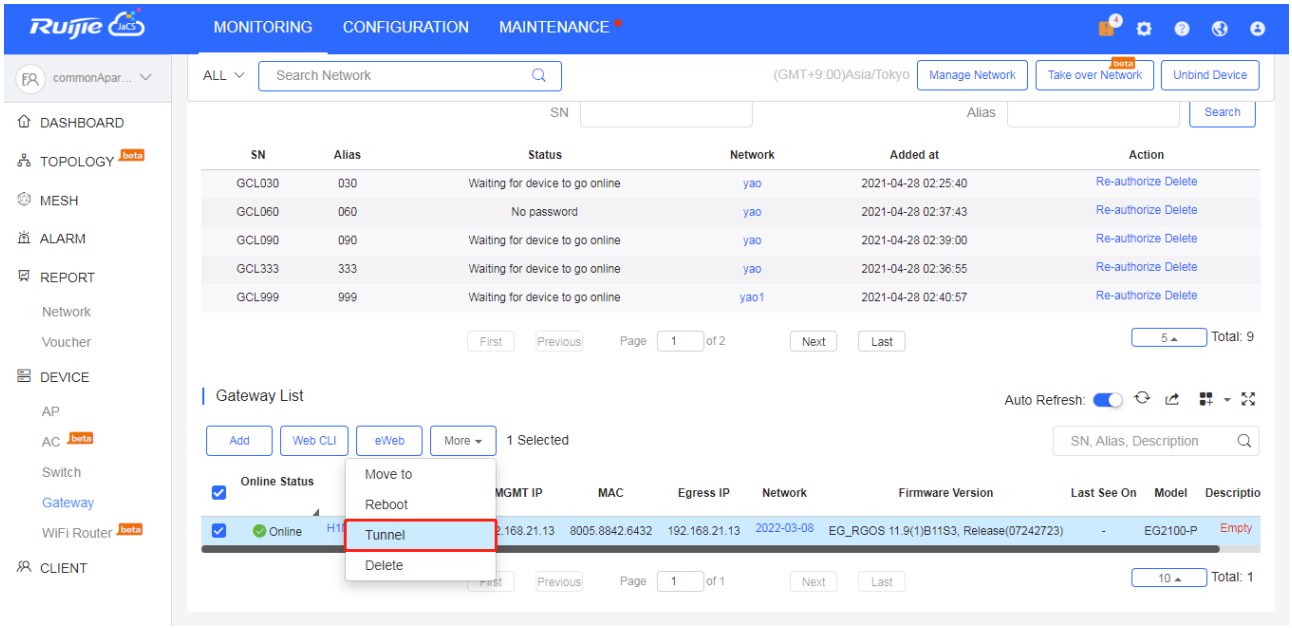


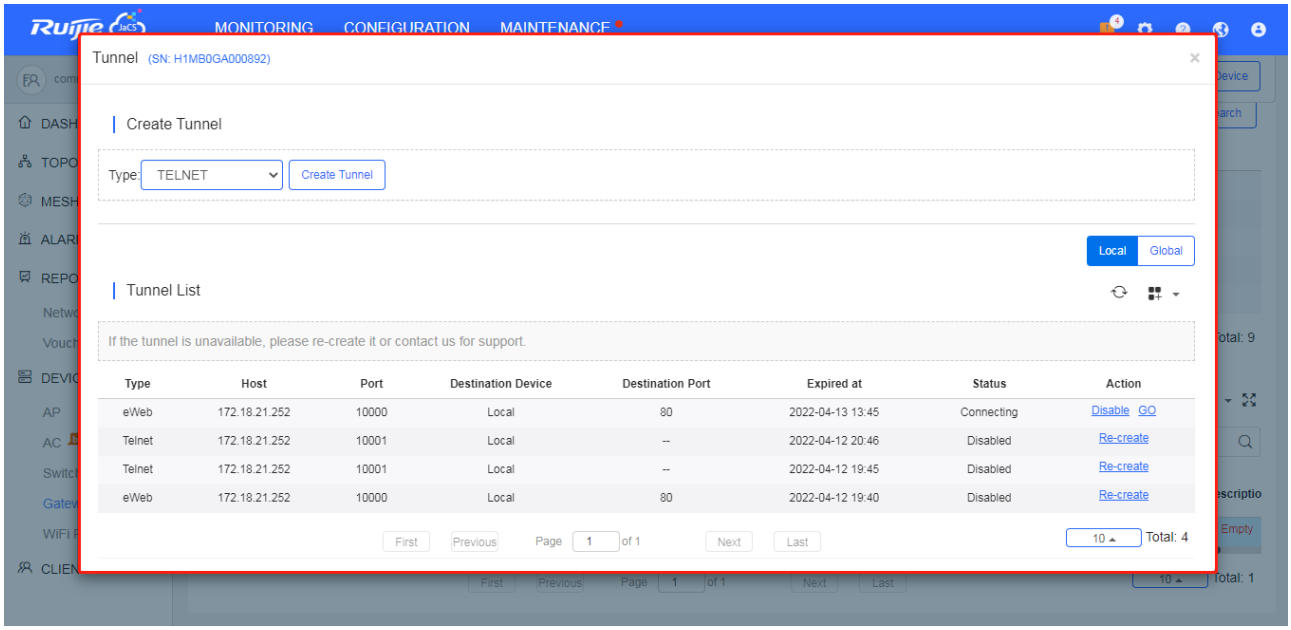
- More > Tunnel

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

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

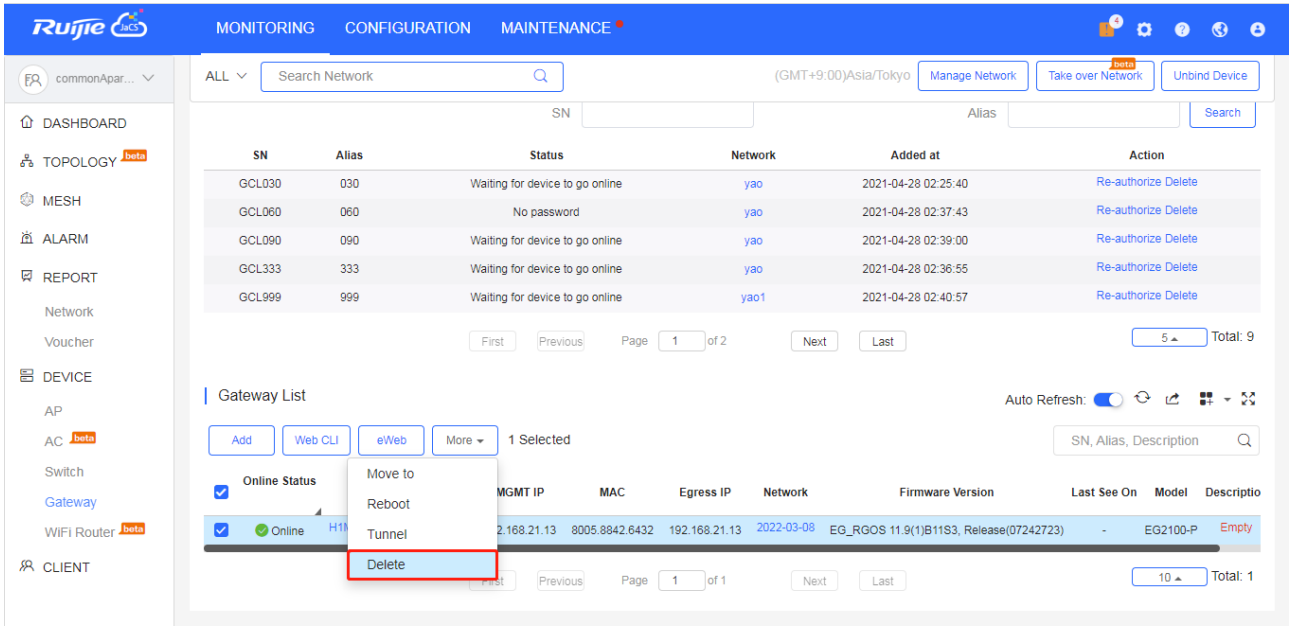
Select the device for tunnel management, and click **More** > **Tunnel**. On the **Tunnel Management** page, **WEB**, **Telnet** and **SSH** types (the tunnel types vary with products) can be selected or you can customize the tunnel configuration. The **Tunnel List** displays the tunnels already created.





- More > Delete

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



5.6.5 WiFi Router (beta)

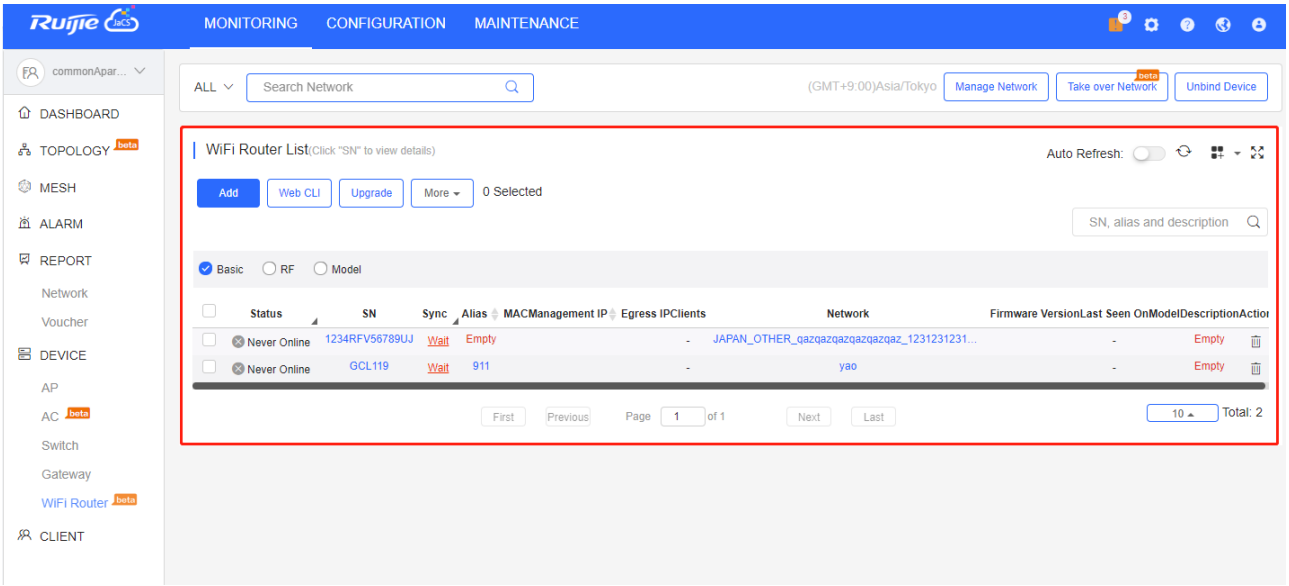
5.6.5.1 WiFi Router List

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

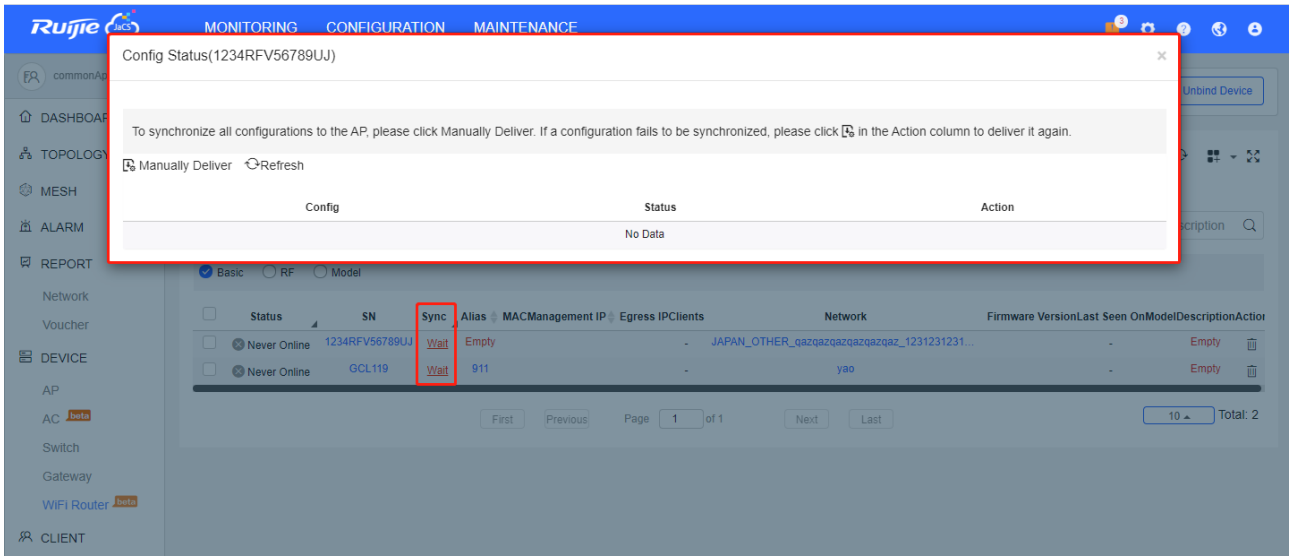
The **WiFi Router List** automatically refreshes every minute. Click Auto Refresh: to enable/disable the auto refresh function.

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

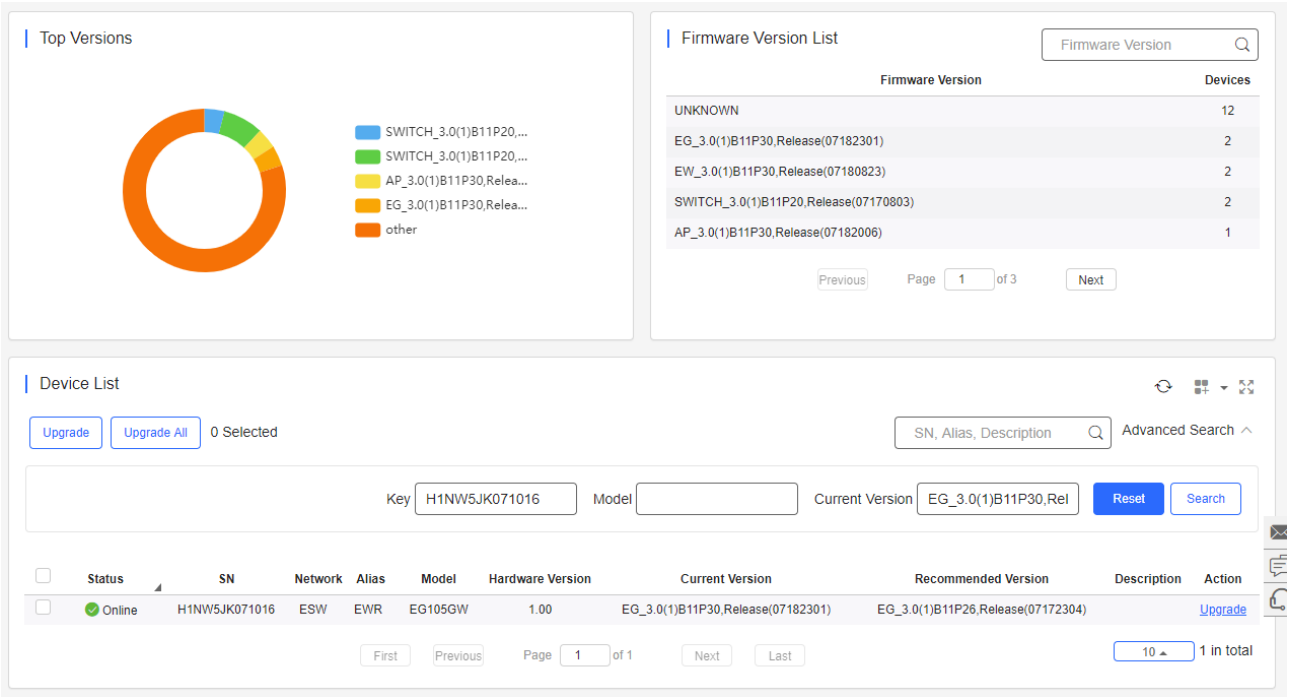
The **Search** function supports fuzzy queries based on the serial number, alias and description, and also supports queries based on sync status and online/offline status.



Click the record in the **Sync 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 **WiFi Router List** page. Click **New Firmware** to display the **New Firmware List**. Then click **Go To Upgrade** to enter the **MAINTENANCE** > **UPGRADE** > **Upgrade** page.



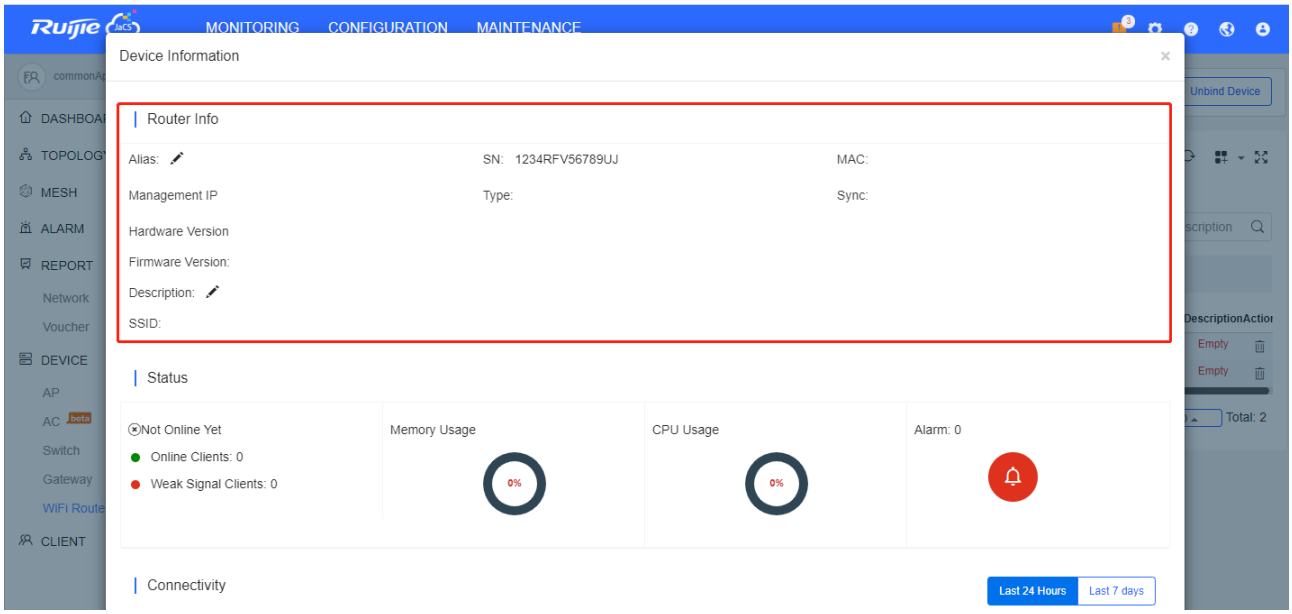
For more information, refer to **Device Details**.

5.6.5.2 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.

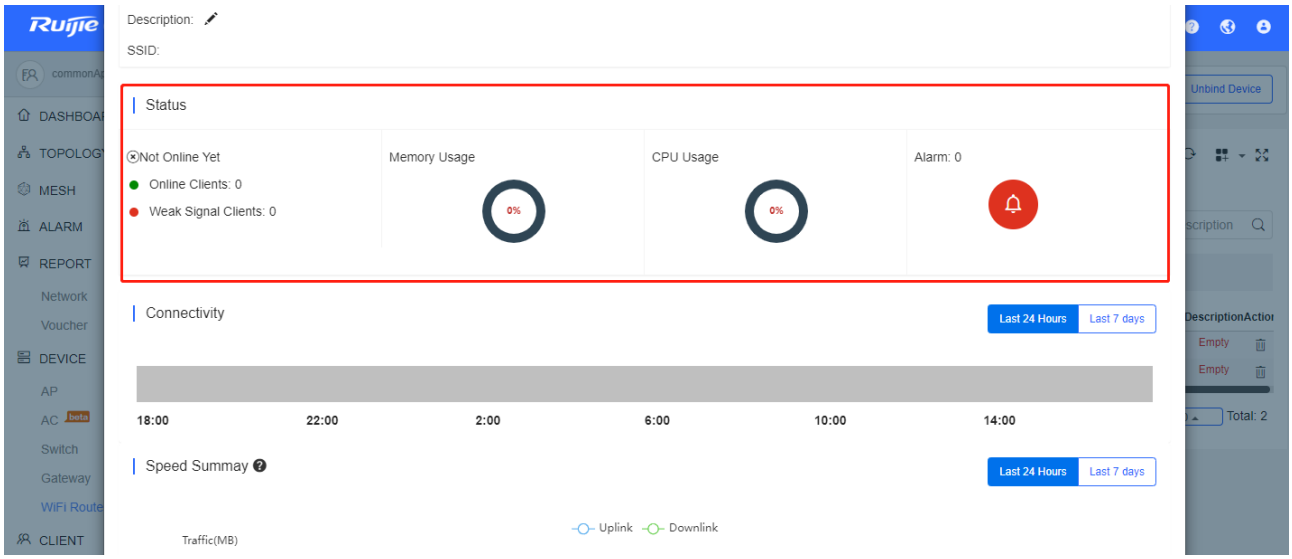
- Router Info

The basic information includes serial number, MAC address, management IP address, SSID, sync status, firmware version, hardware version, alias, and description.



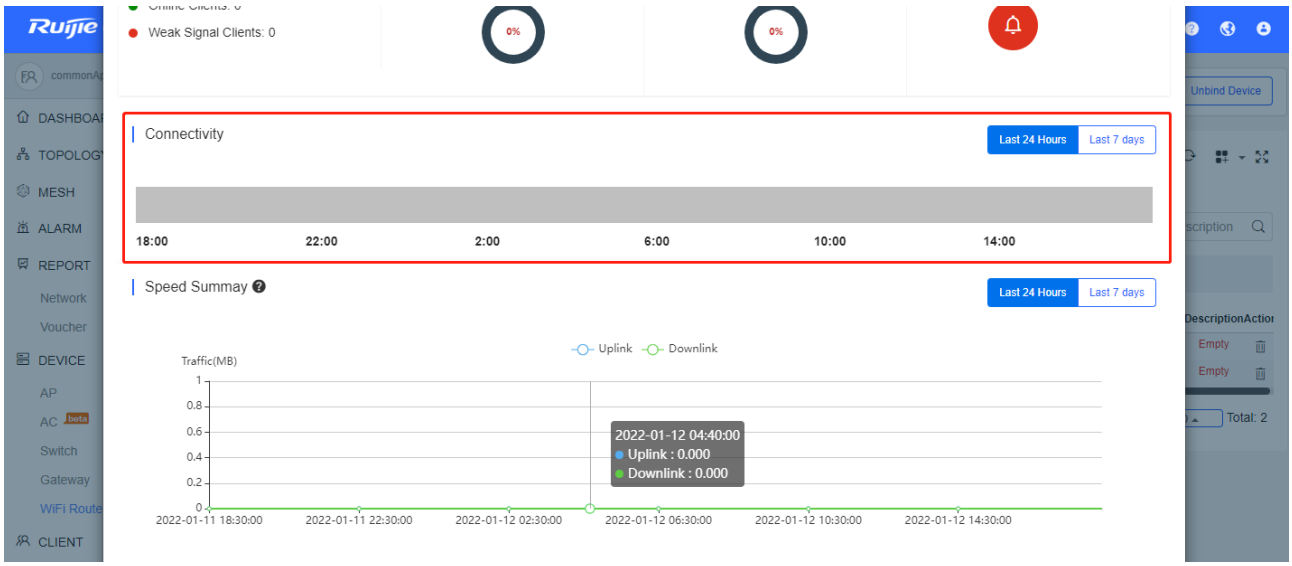
- Status

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



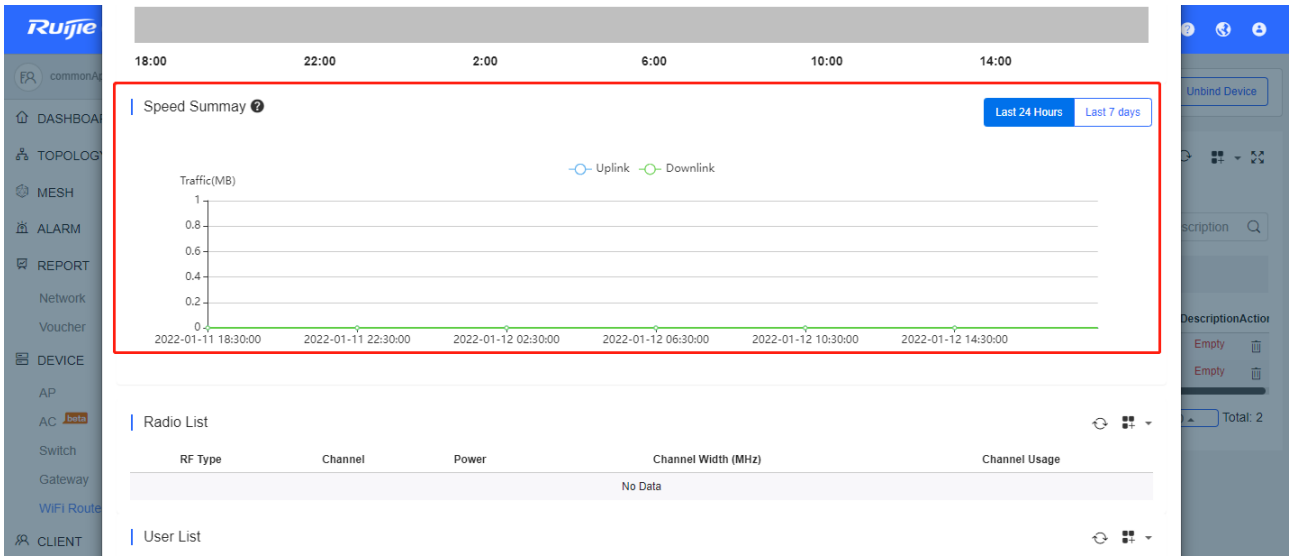
- Connectivity

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



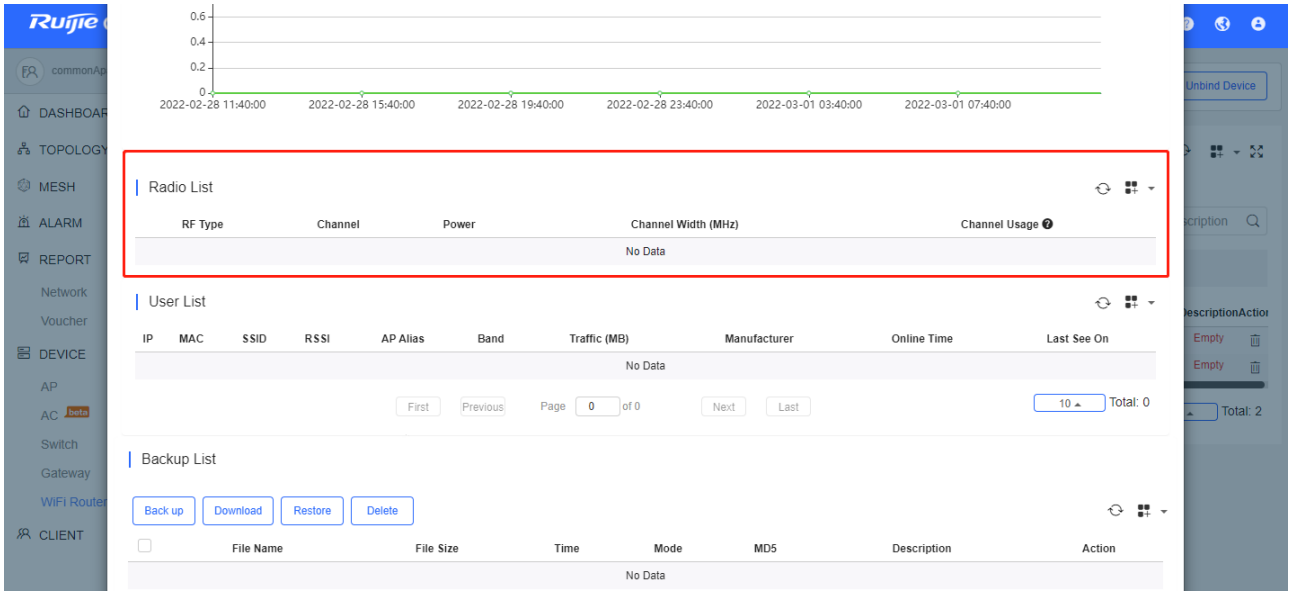
- Speed Summary

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



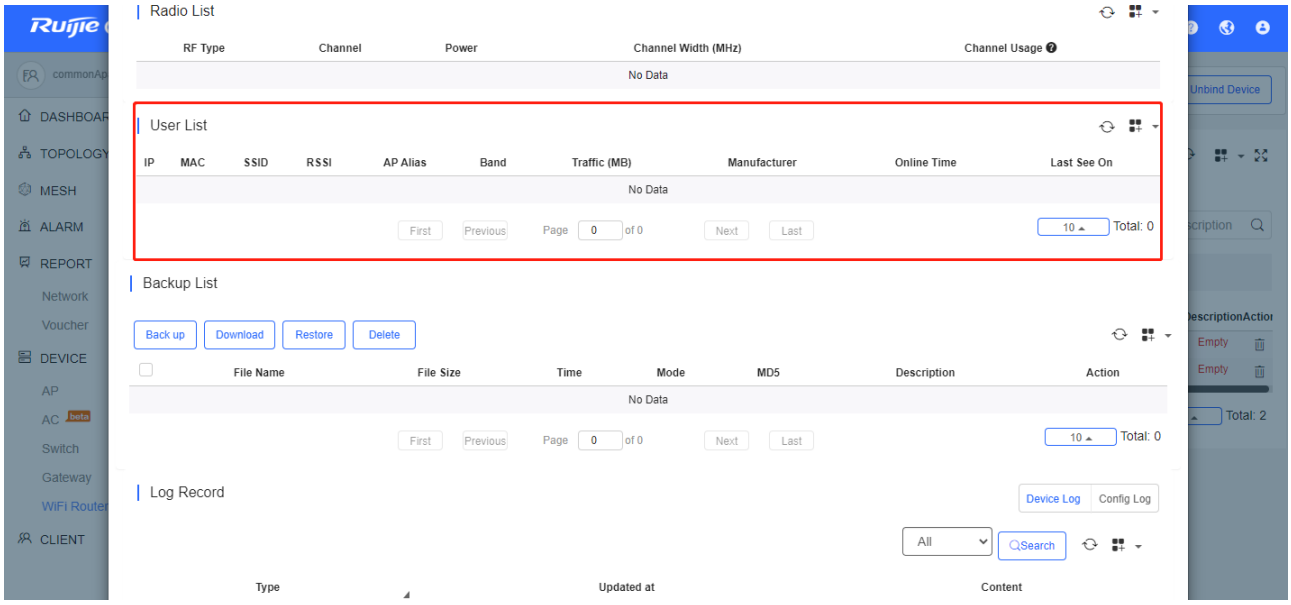
- Radio List

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



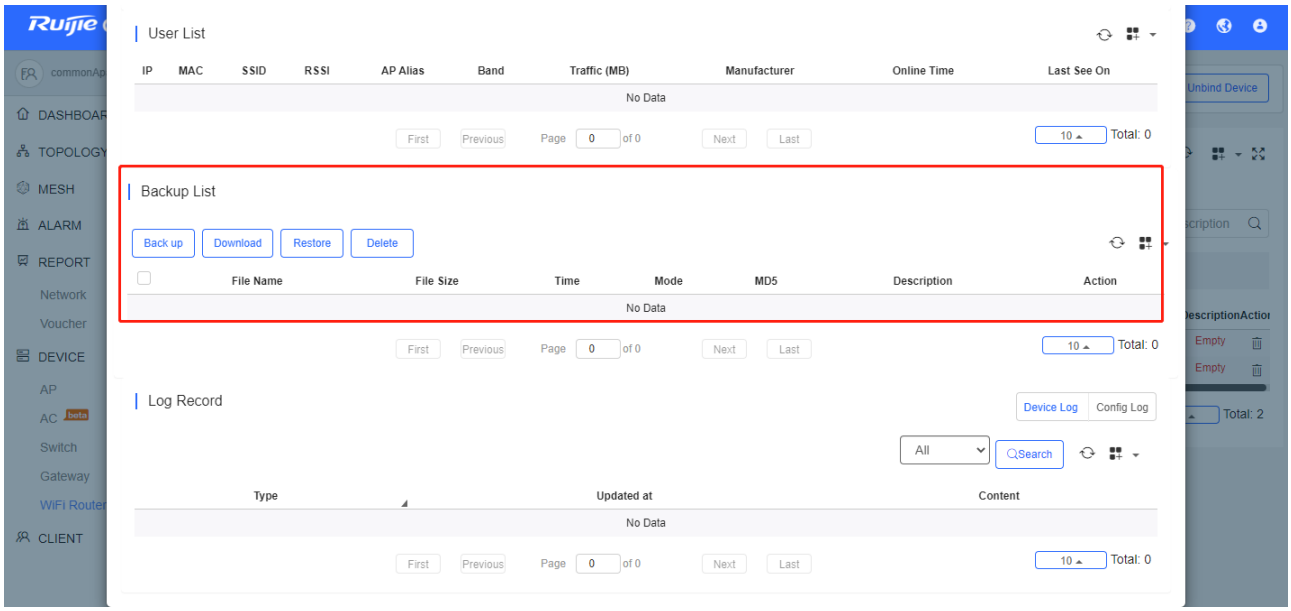
- User List

The **User list** displays information about clients currently associated with the routers, including the IP address, MAC address, SSID, RSSI, traffic, online/offline status, terminal type and so on.



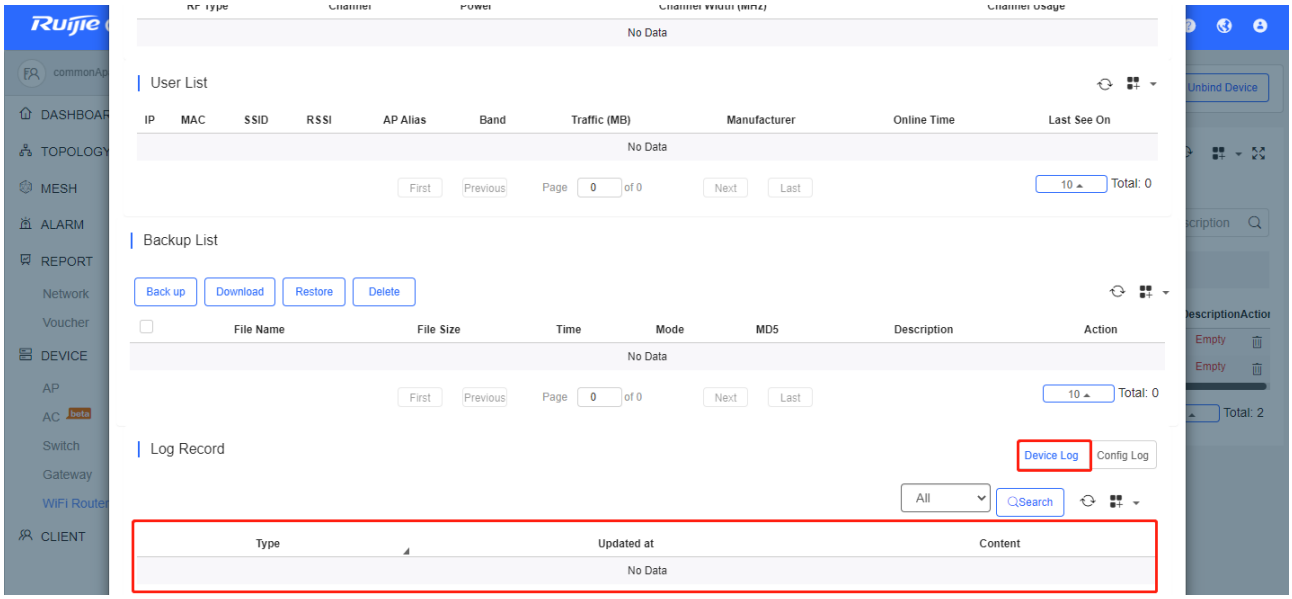
- Backup List

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



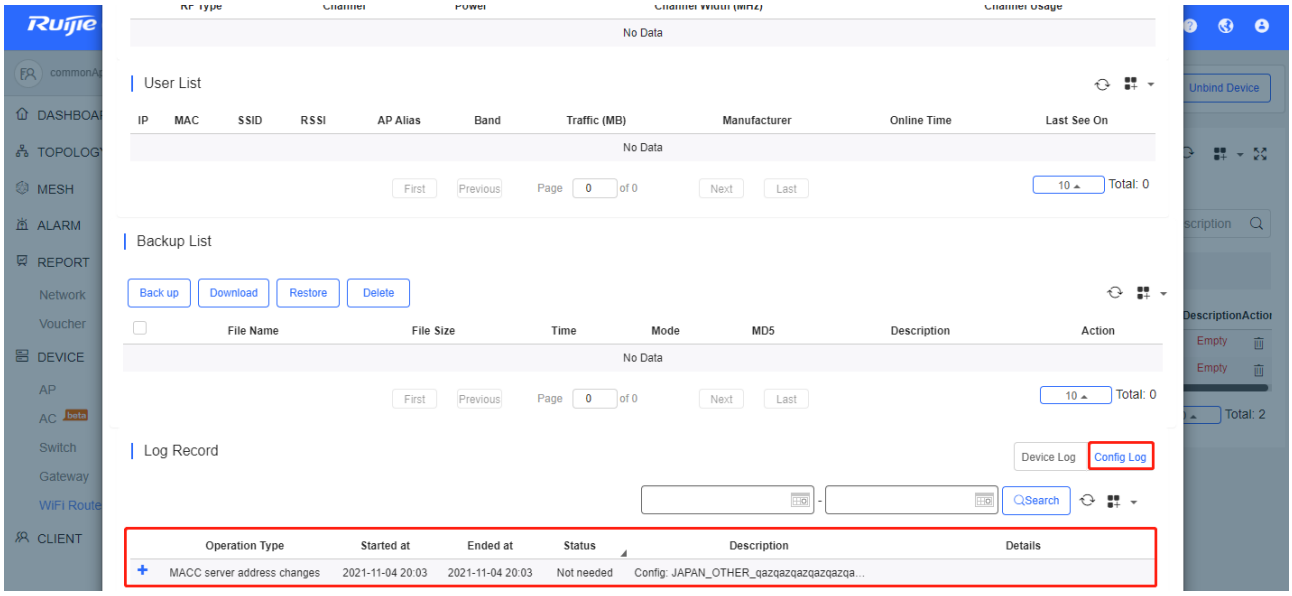
- Device Log

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



- Config Log

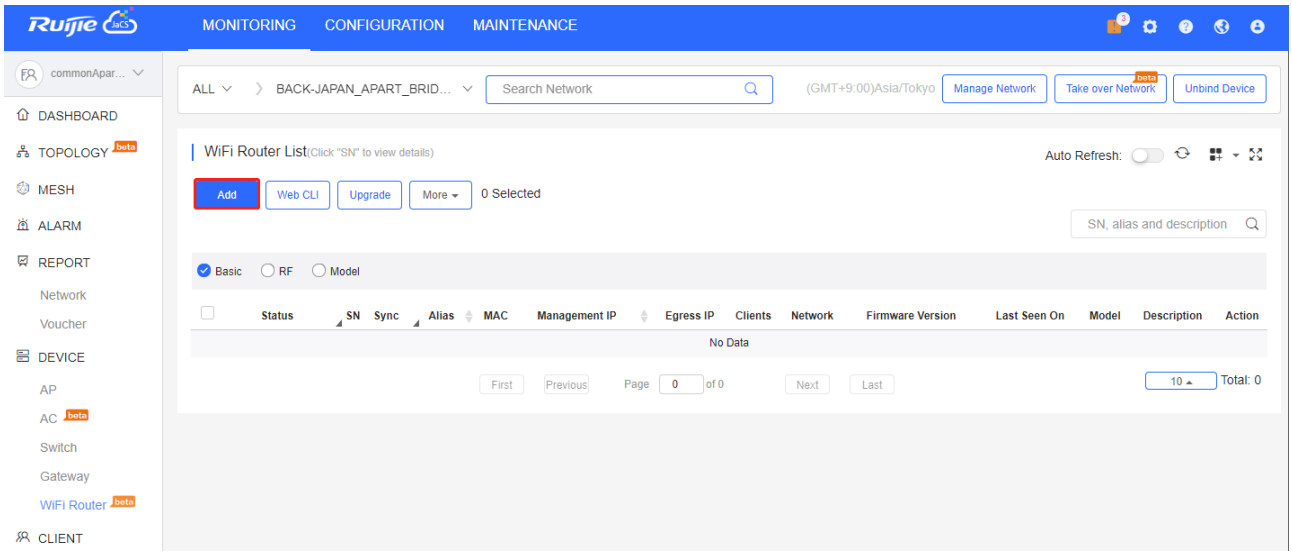
The Config Log records the historical operations, including online/offline, restart and upgrade records, and supports queries based on the status and period.



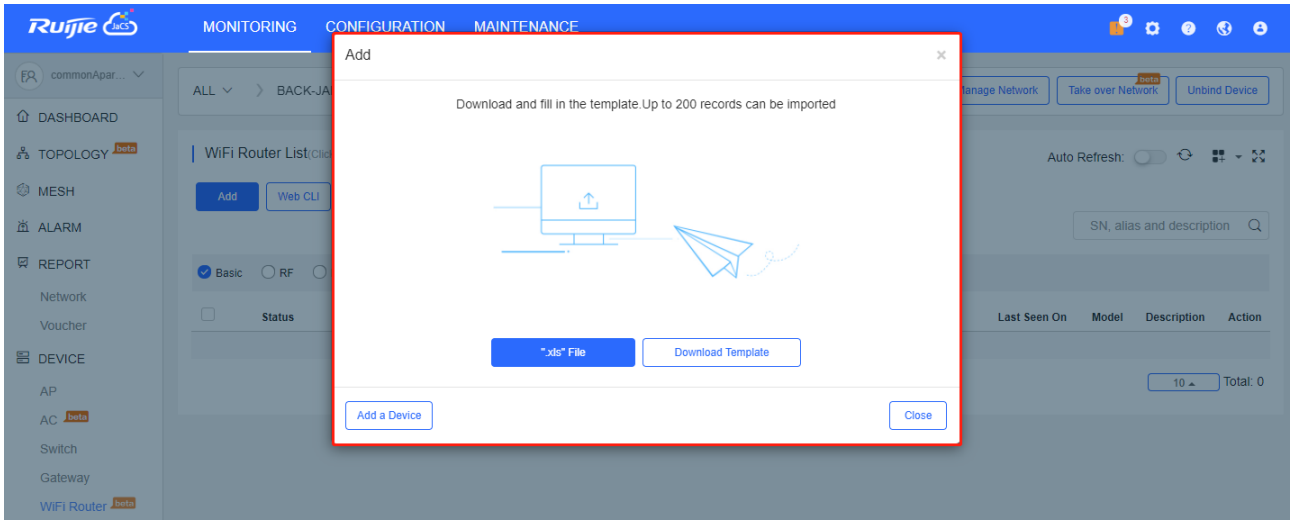
5.6.5.3 Basic Router Operations

- Add Router

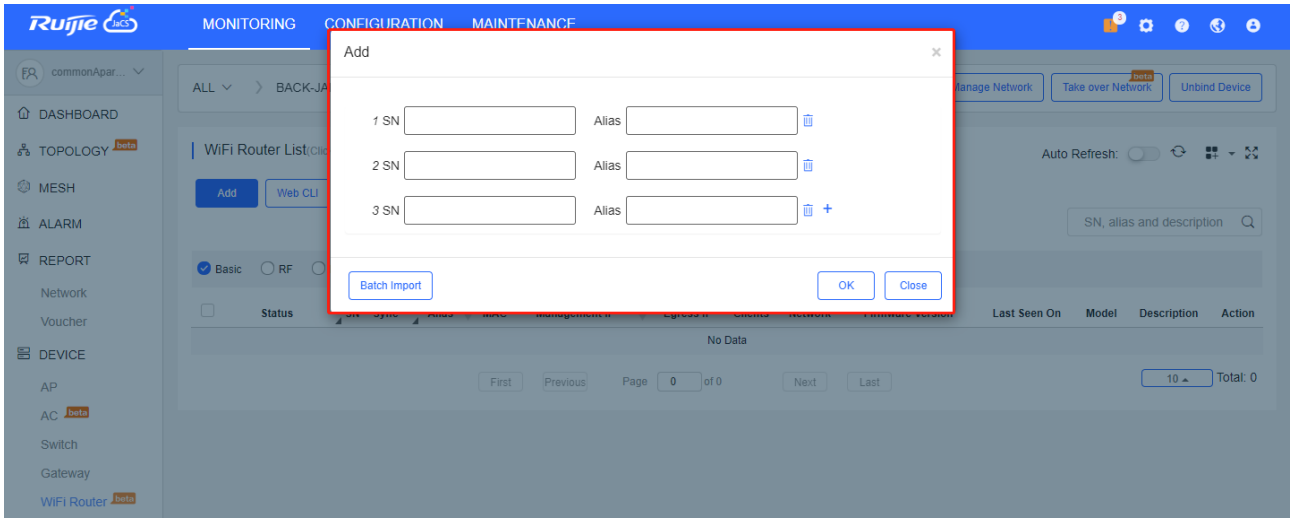
Step 1: Select the network, and click **Add**. Both batch import and manual add are supported.



Step 2: Click **download template** to download the template, enter router information, and click **'.xls' File** to import the template.

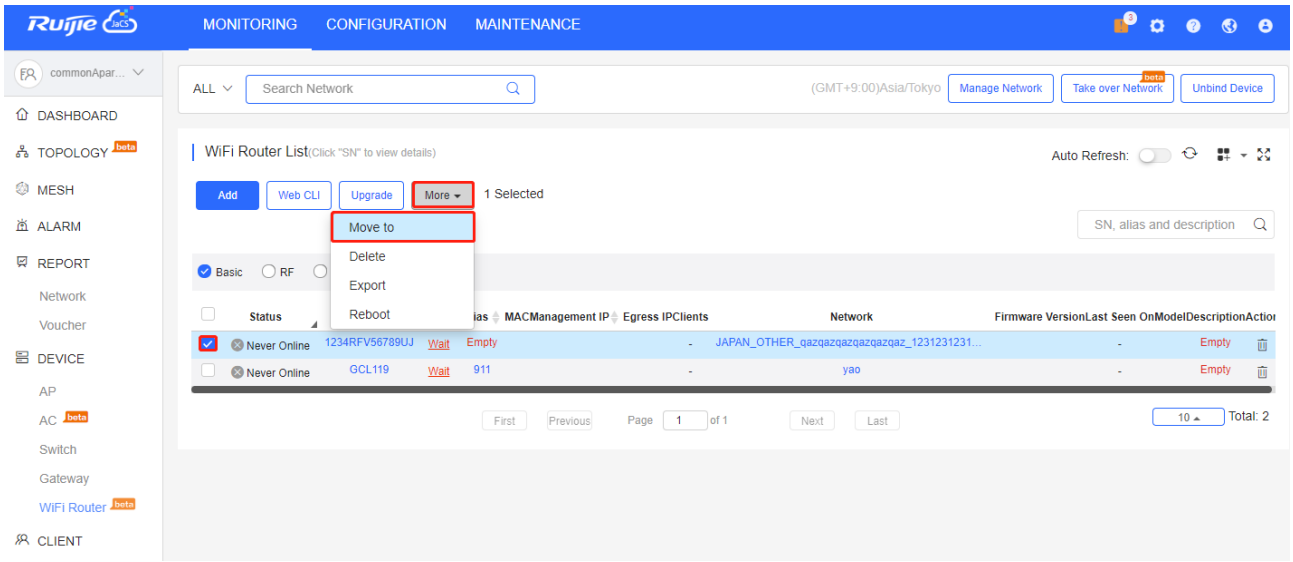


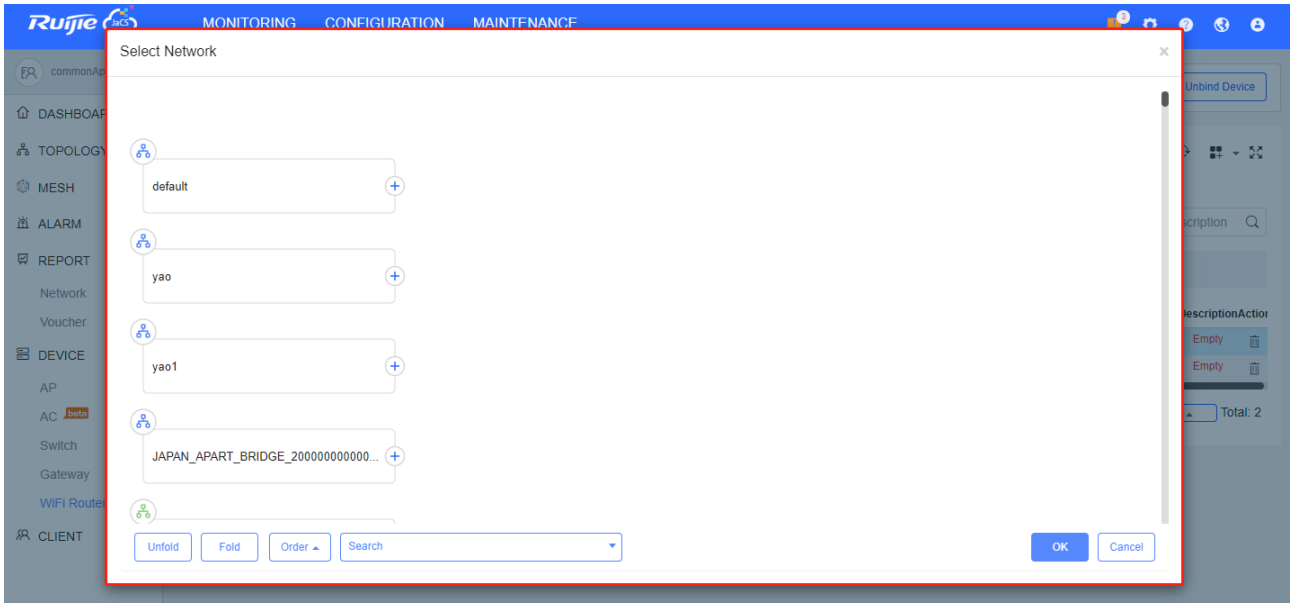
Or you can click **Add a Device**, enter SN and alias of the AP, and click **OK**. Click + to add multiple APs.



- More > Move to

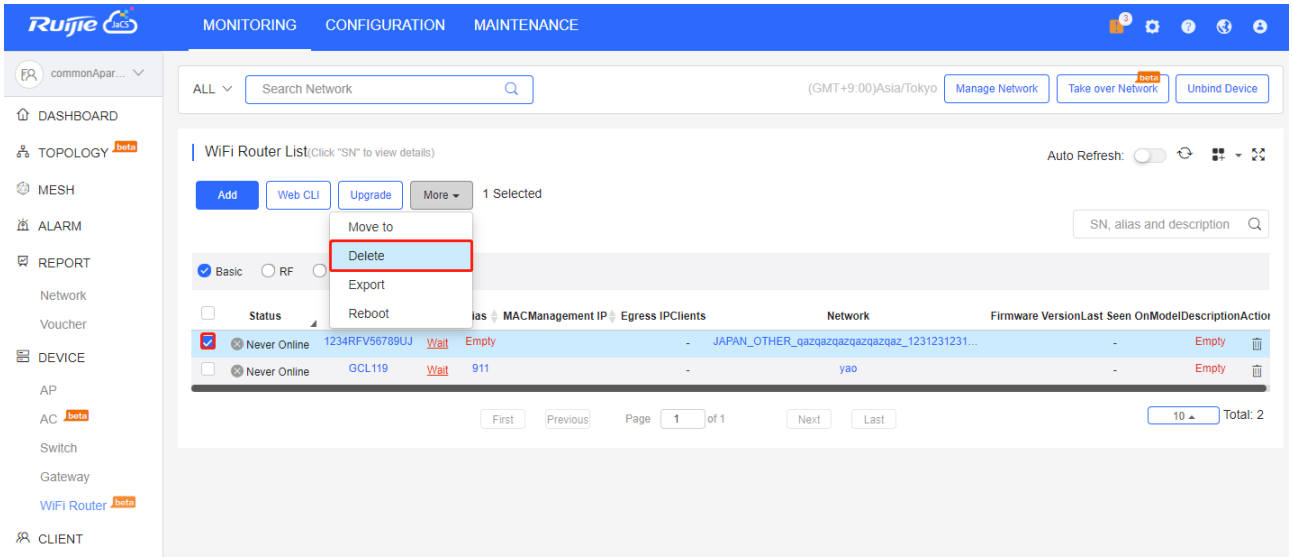
Select one or multiple devices in the **WiFi Router List**, click **More** > **Move to**, select the new network and click **OK**.





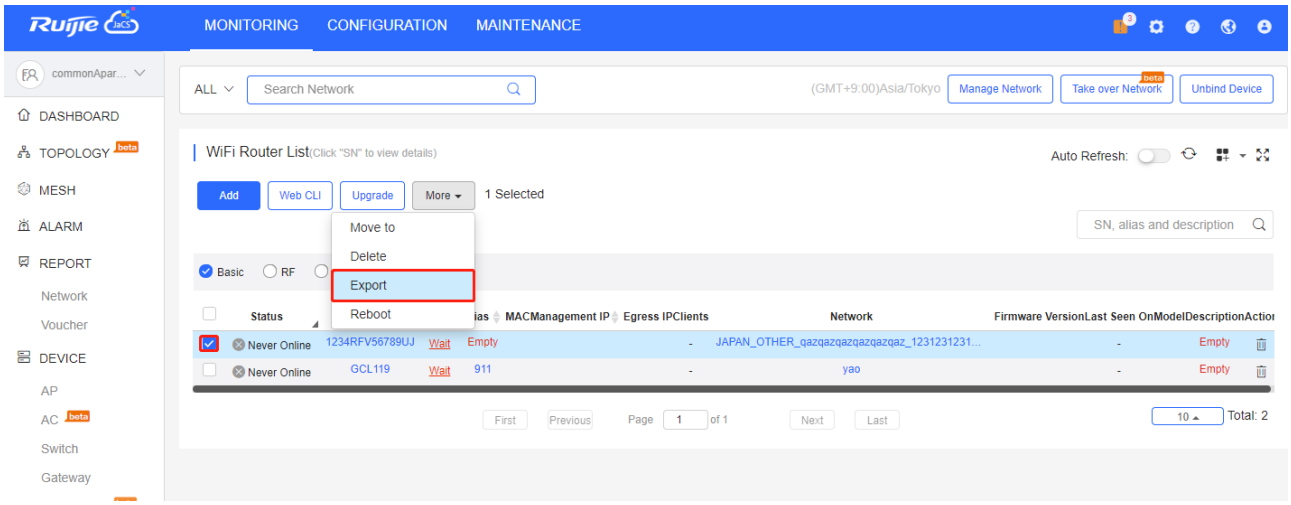
- More > Delete

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



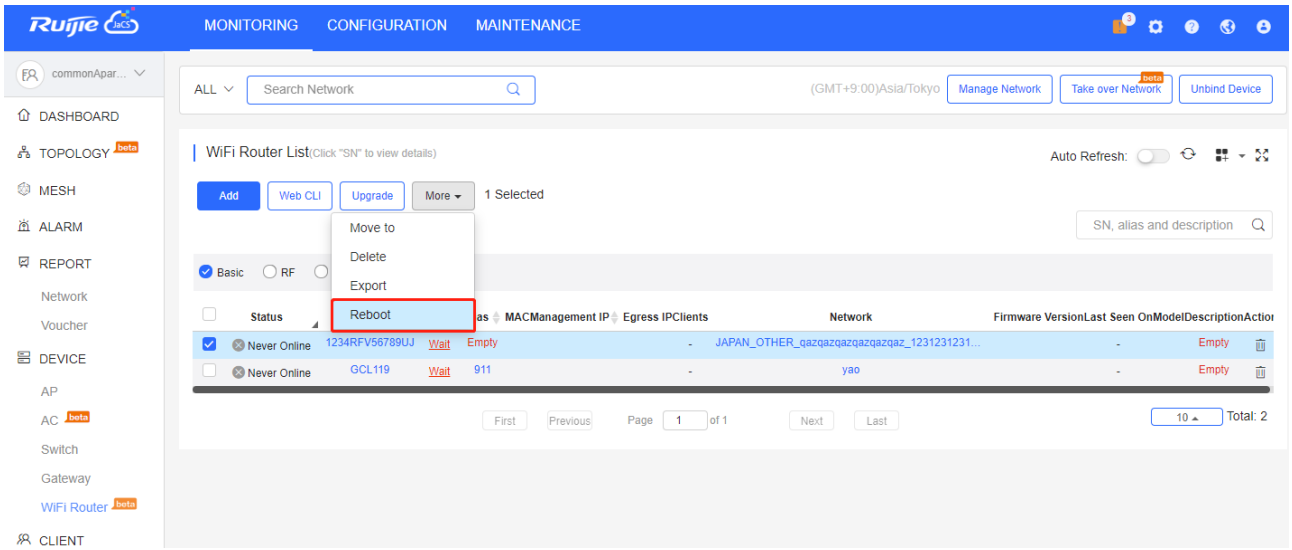
- More > Export

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



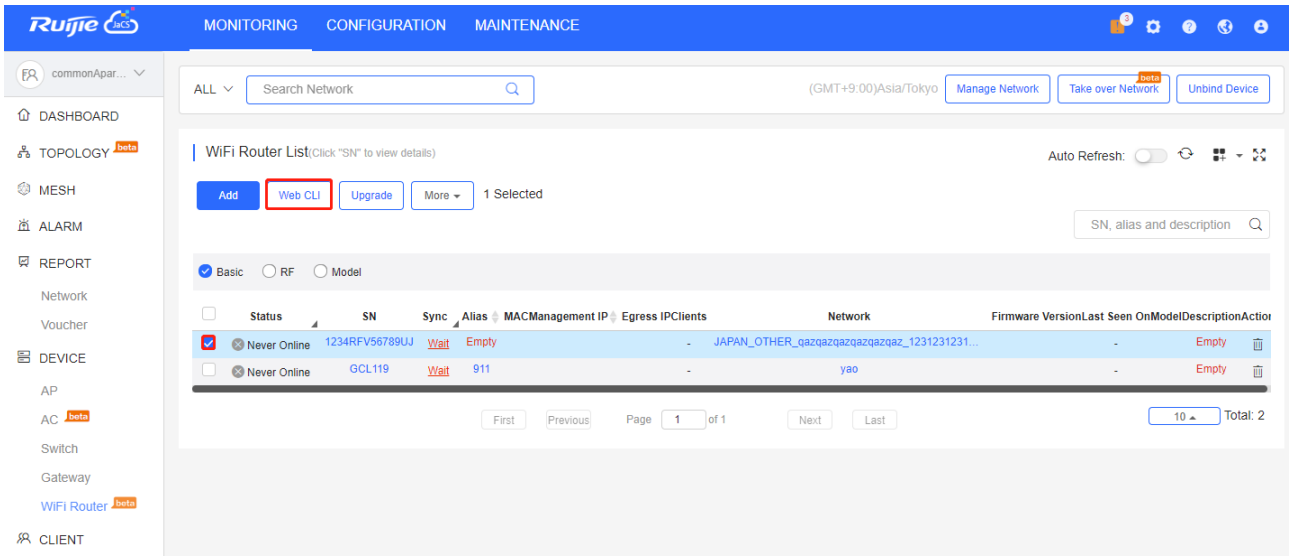
- More > Reboot

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



- 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.



5.7 Client

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

5.7.1 Client List

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

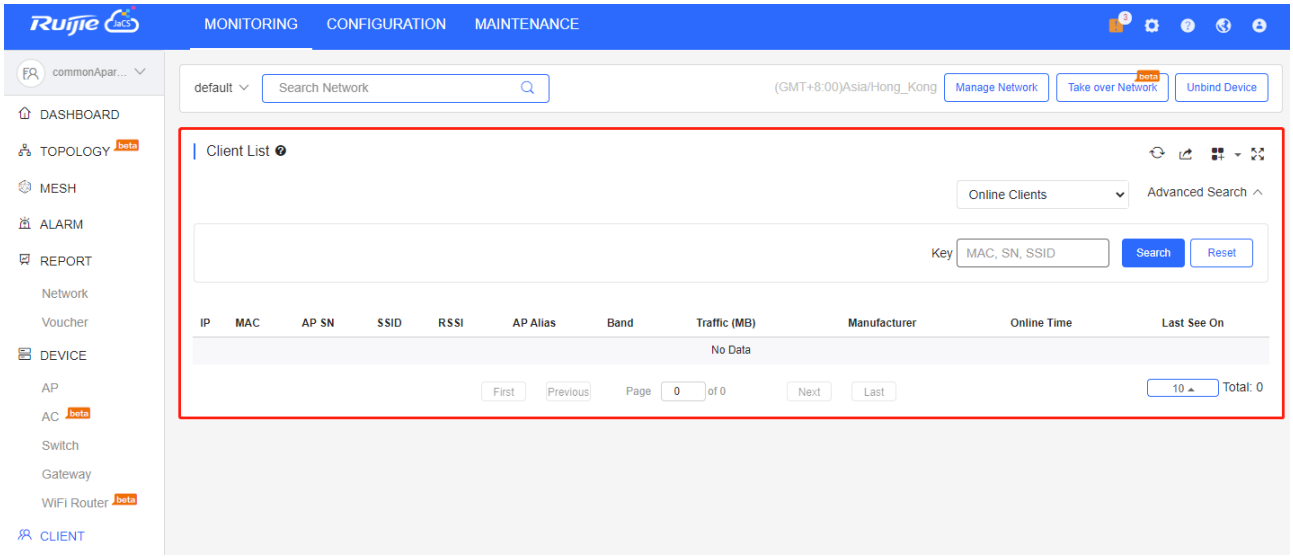
Click the drop-down list next to **Advanced Search** to switch between **Online Clients** and **History Clients**.

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

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

5.7.2 Client Details

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



- Client Info

Client Info includes alias, status, MAC address, online/offline time, uptime, IP address, terminal, operation system, manufacture, AP serial number, AP ailas and SSID.

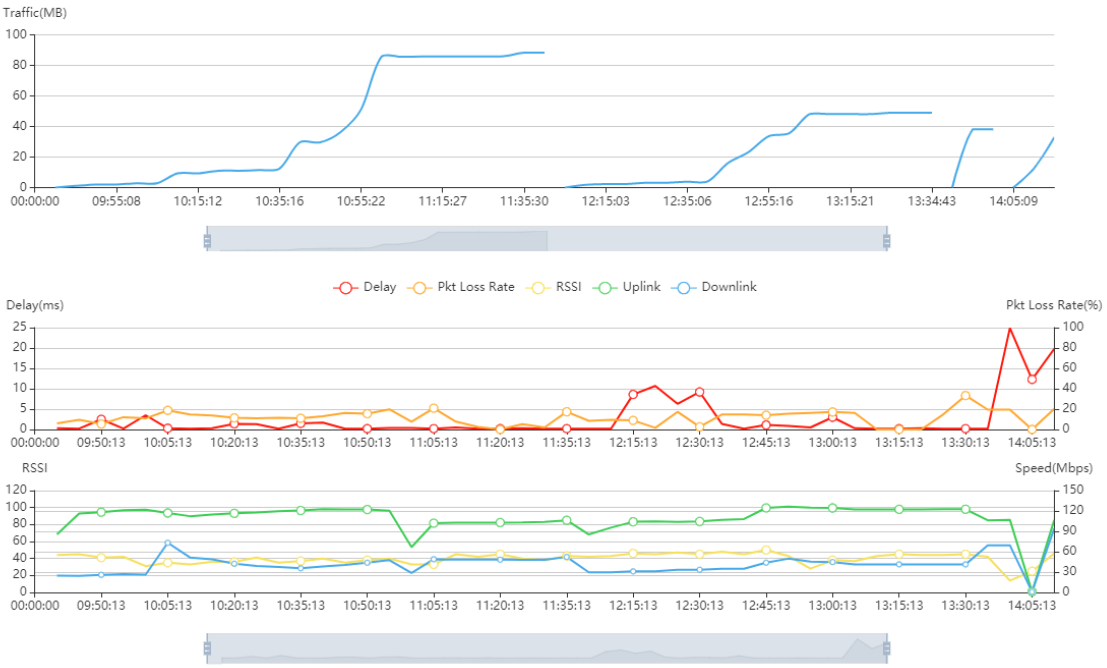
Client Info

Alias :	Status : Online	MAC : 3045.9609.0557
Online Time : 2019-04-16 14:05:09	Offline Time : -	Uptime : 0h 8m 26s
IP : 172.17.125.140	Terminal : Phone	OS : Android
Manufacturer : HUAWEI TECHNOLOGIES CO.,LTD	AP SN : G1KD9HH02861B	AP Alias : 520w2
SSID : Nature_cloud_as		

- Performance

Performance displays the traffic summary etc.

Performance



- 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

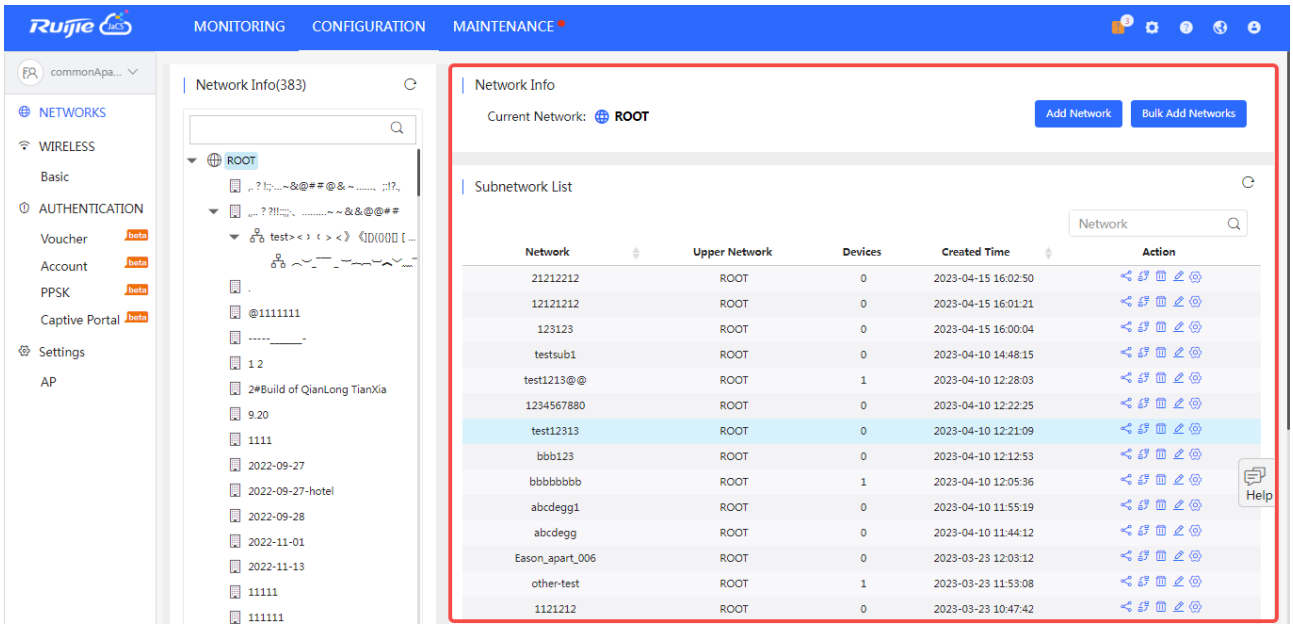
The Configuration module includes two parts: **NETWORKS** and **WIRELESS** and **AUTHENTIFICATION**.

6.1 Networks

6.1.1 Basic

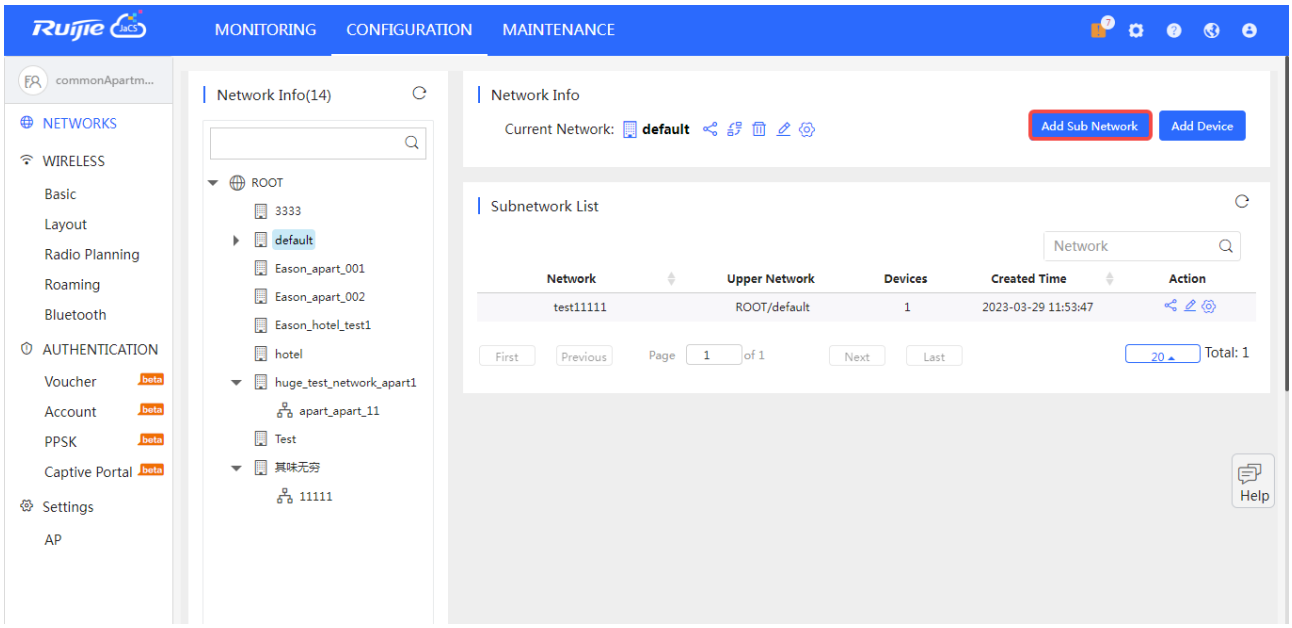
Select **CONFIGURATION** > **NETWORKS** to open the **NETWORKS** page. Then, all detailed information about the sub networks is displayed on the **Subnetwork List**, including the network name, its upper network, the number of connected devices and created time.

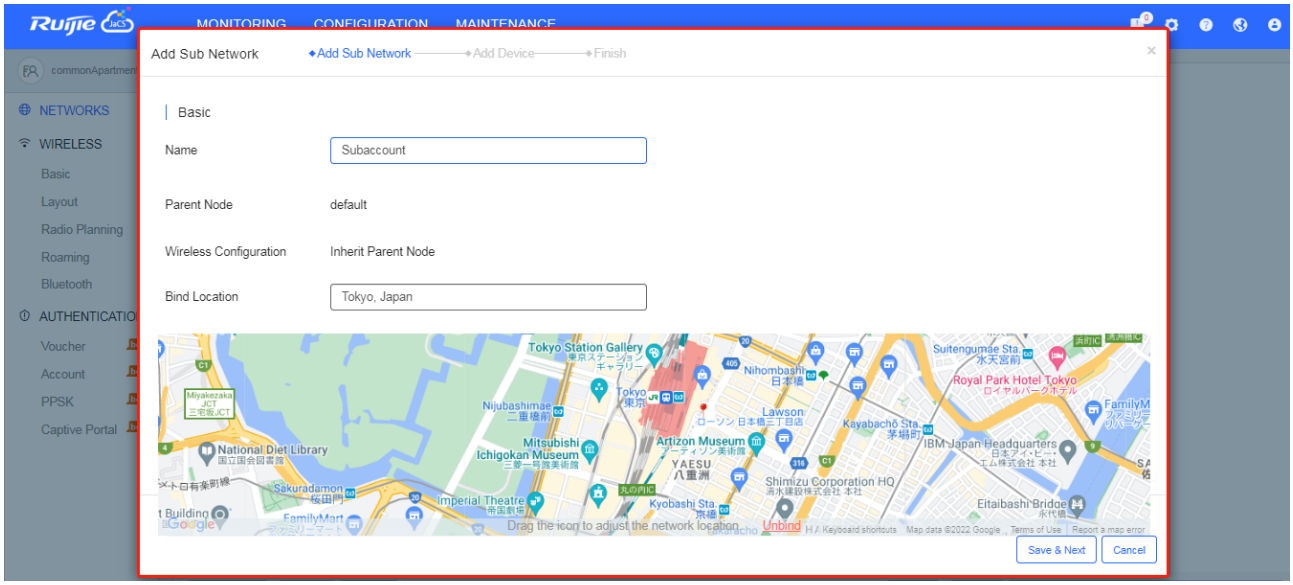
Additionally, five operation icons are provided in the **Action** column of a network for adding a sub network, sharing the network, handing over the network, deleting the network and configuring the network. You can click these icons to perform operations on the network.



6.1.1.1 Add Sub Networks

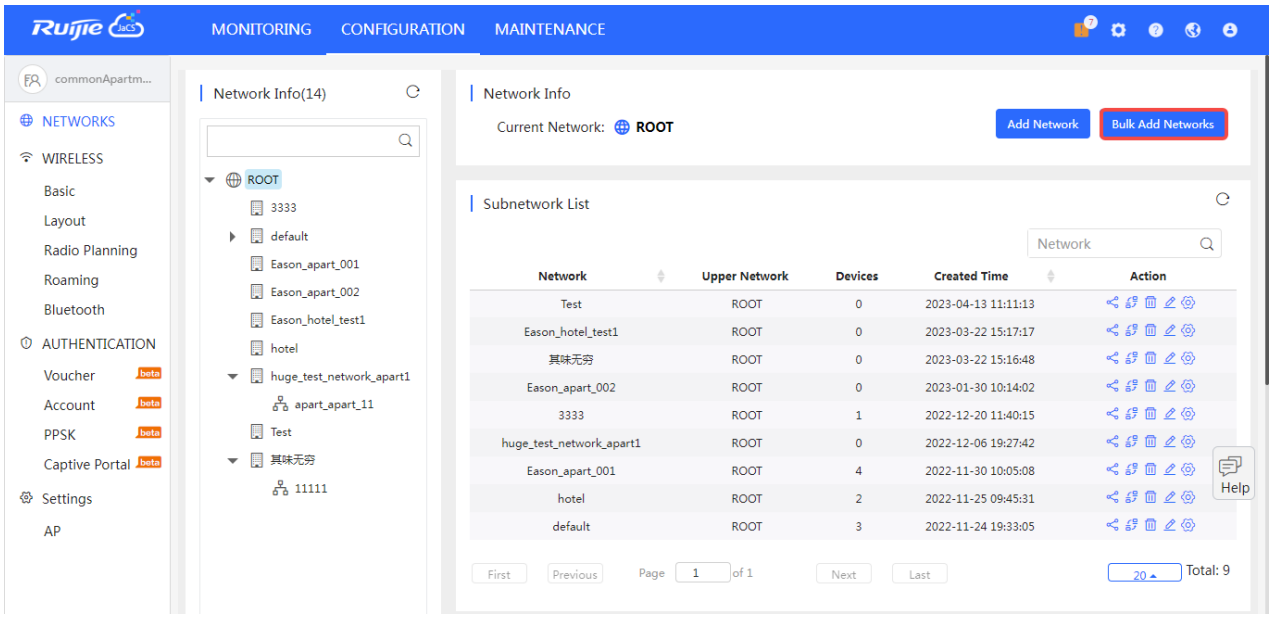
Select the network and click **Add Sub Network**.


MONITORING
CONFIGURATION
MAINTENANCE
NETWORKS
WIRELESS
Basic
Layout
Radio Planning
Roaming
Bluetooth
AUTHENTICATION
Voucher
Account
PPSK
Captive Portal
Settings
AP
Network Info(14)
ROOT
3333
default
Eason_apart_001
Eason_apart_002
Eason_hotel_test1
hotel
huge_test_network_apart1
apart_apart_11
Test
其味无穷
11111
Network Info
Current Network: default
Add Sub Network
Add Device
Subnetwork List
Network
Upper Network
Devices
Created Time
Action
test11111
ROOT/default
1
2023-03-29 11:53:47
First
Previous
Page 1 of 1
Next
Last
20
Total: 1
Help

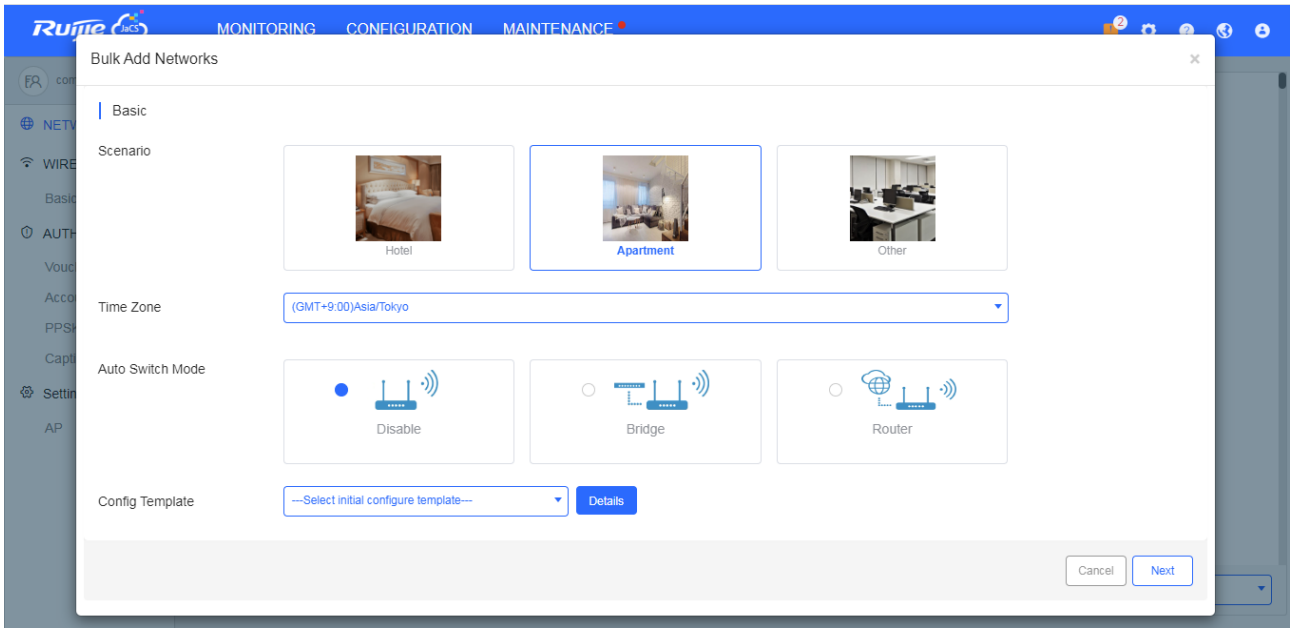

Add Sub Network
Add Sub Network
Add Device
Finish
Basic
Name
Subaccount
Parent Node
default
Wireless Configuration
Inherit Parent Node
Bind Location
Tokyo, Japan
Drag the icon to adjust the network location
Unbind
Save & Next
Cancel

6.1.1.2 Bulk Add Networks

Step 1 Click **Bulk Add Networks** to enter the setting page.

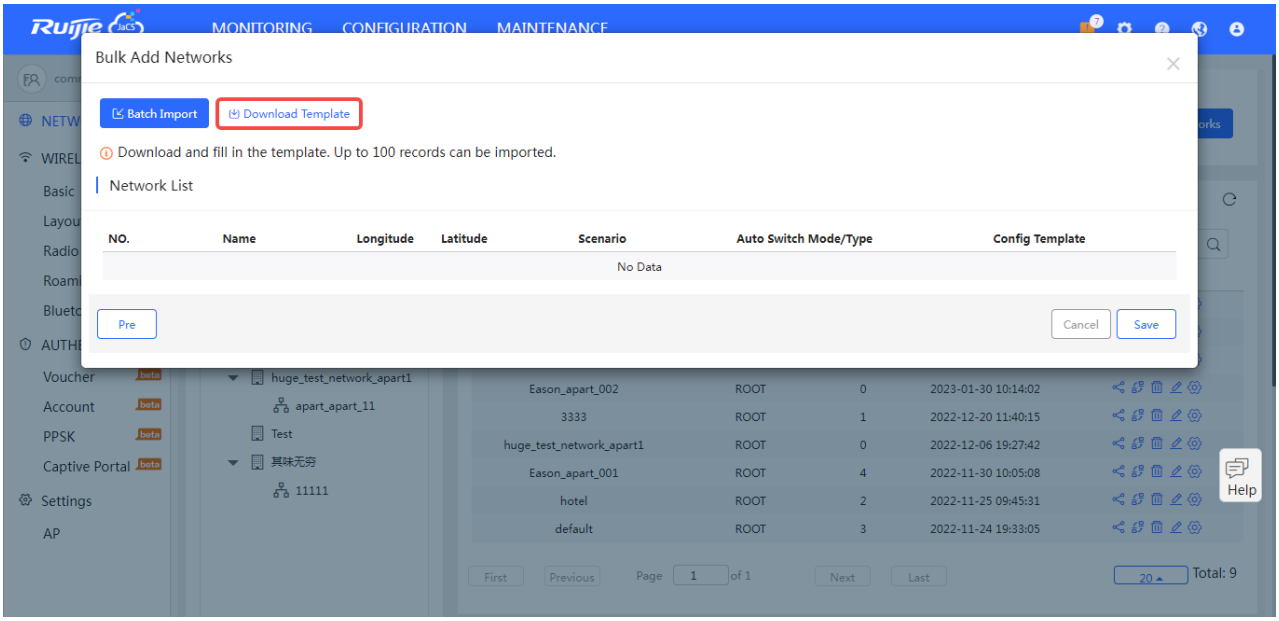


Step 2 Specify the **Scenario**, **Time Zone**, **Auto Switch Mode** and **Configuration Template** (optional).

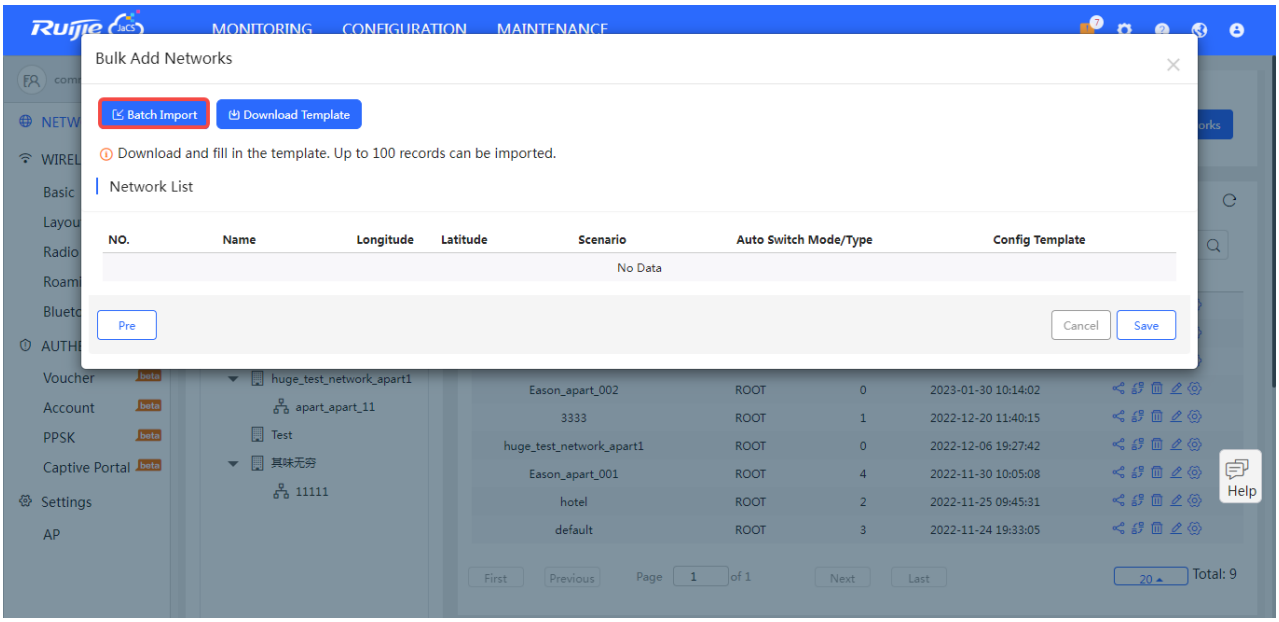


When an initial configuration template is selected, the **Enabled** button appears. By default, the function is disabled. When it is enabled, the configurations in the template will be delivered to all devices in the network when they go online for the first time.

Step 3 Click **Download Template** to download and fill in the template.



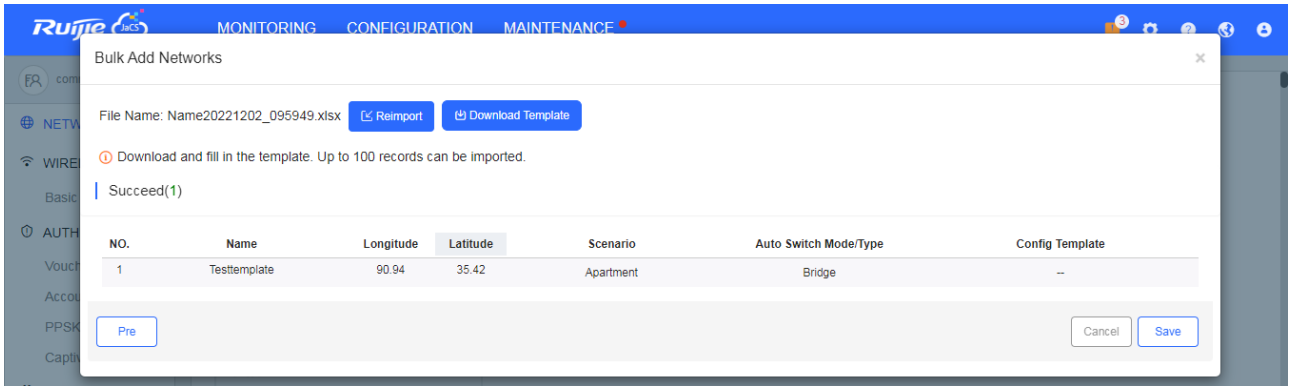
Step 4 Click **Batch Import** to import the filled template.



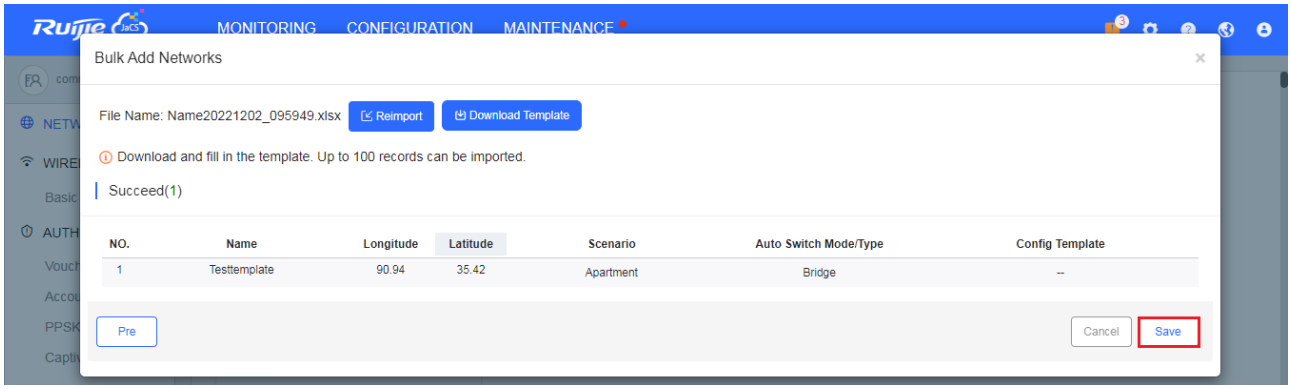
If a wrong file is imported, an error prompt appears for 3s.

If a correct file is imported, a confirmation box appears. Click **OK** in the confirmation box to import the file.

When the file is imported, the created networks will be displayed in the **Succeed** list. The networks of which parameters are consistent with other networks will be displayed in the **Failed** list.



Step 5 Click **Save** to complete the import. All the networks created will be displayed in the **CONFIGURATION** > **NETWORKS** page.

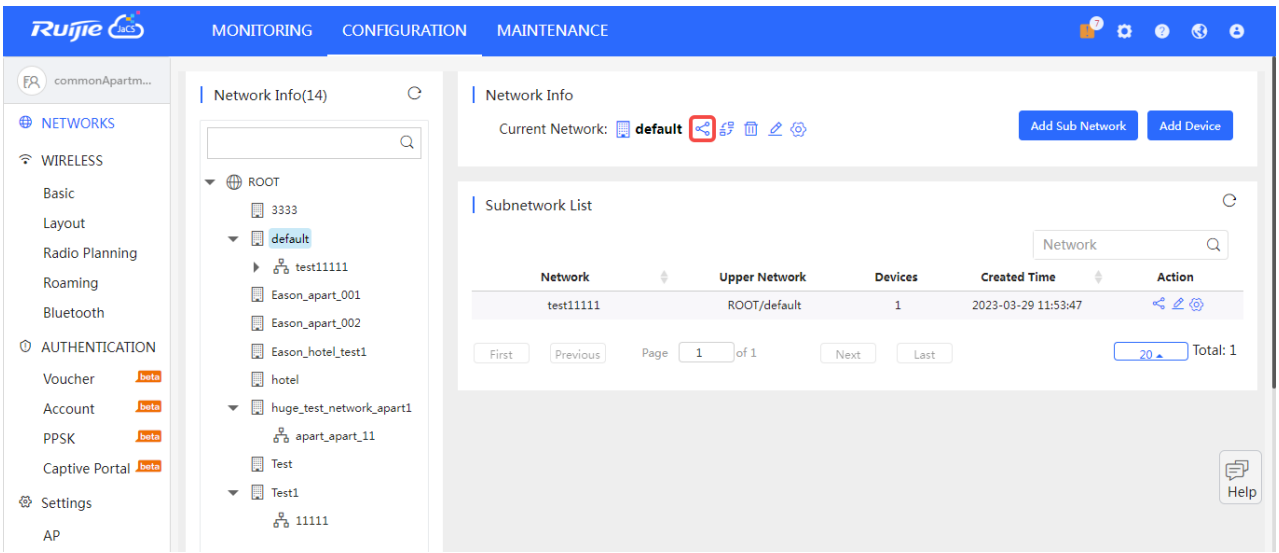


If several users import a same file at the same time, the file imported by the user who clicks **Save** first will be saved, and error prompt will be sent to the rest of the users.

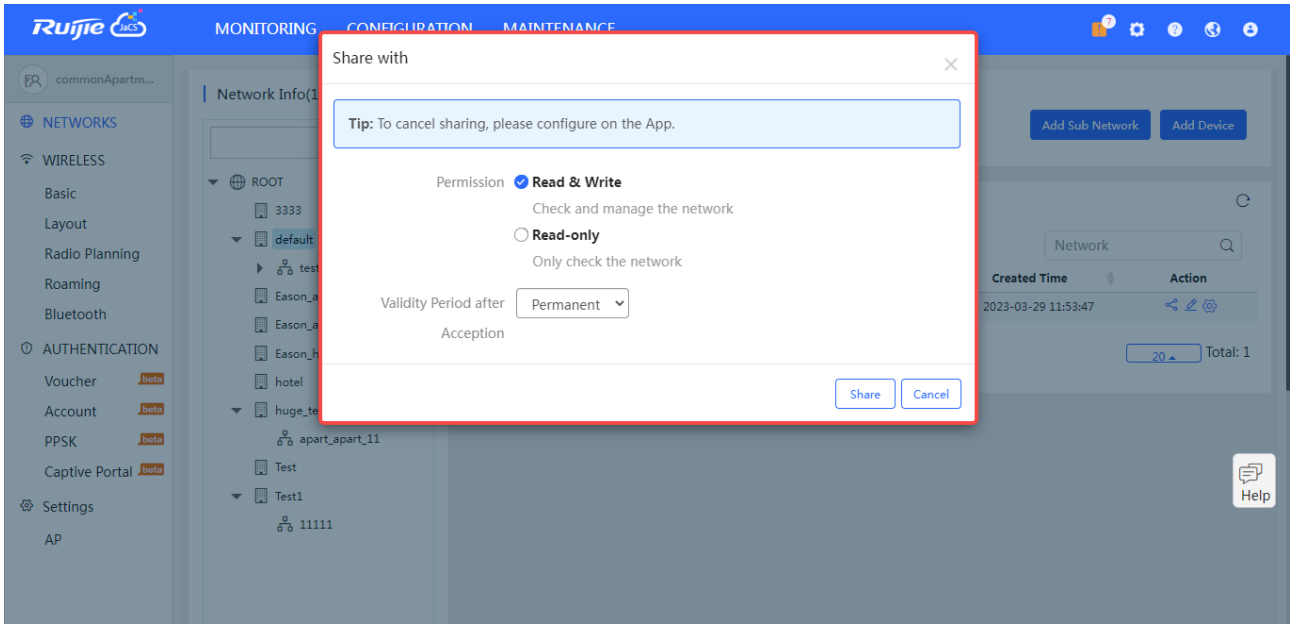
6.1.1.3 Share with

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.

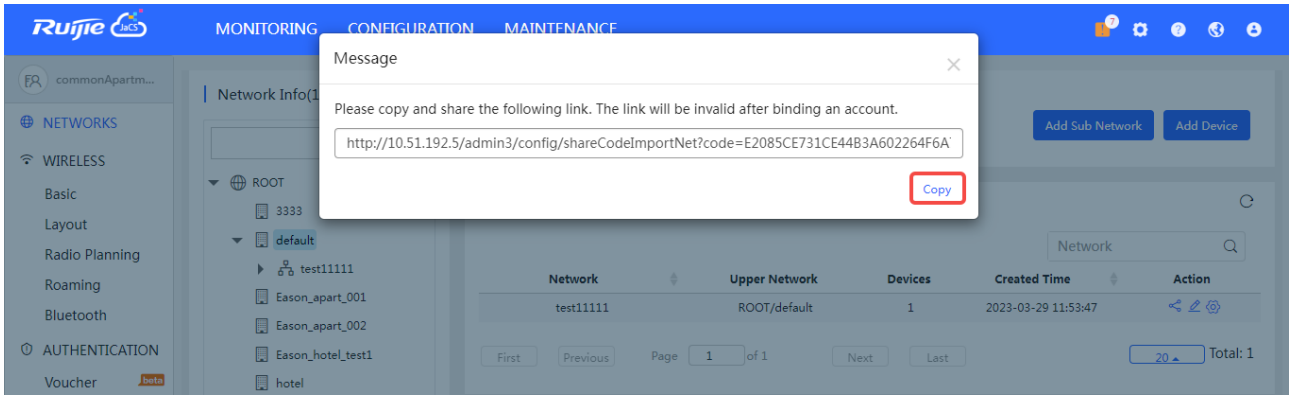
Step 1 Select a network and click the icon.

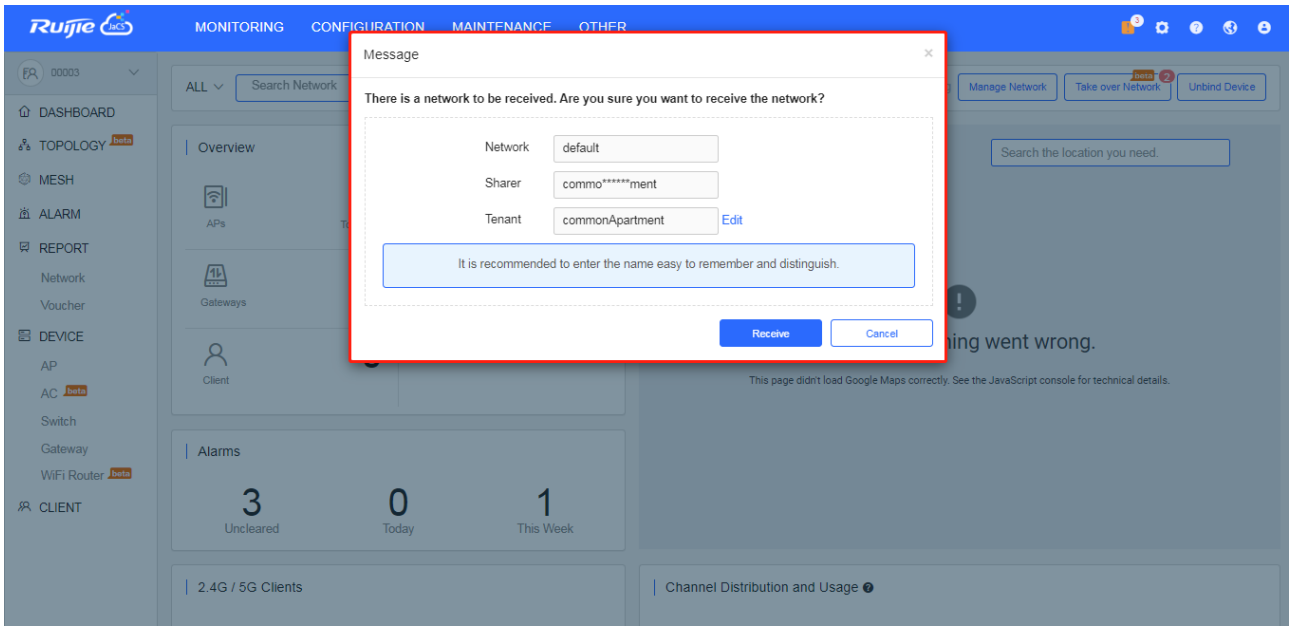


Step 2 Specify the permission and validity period.

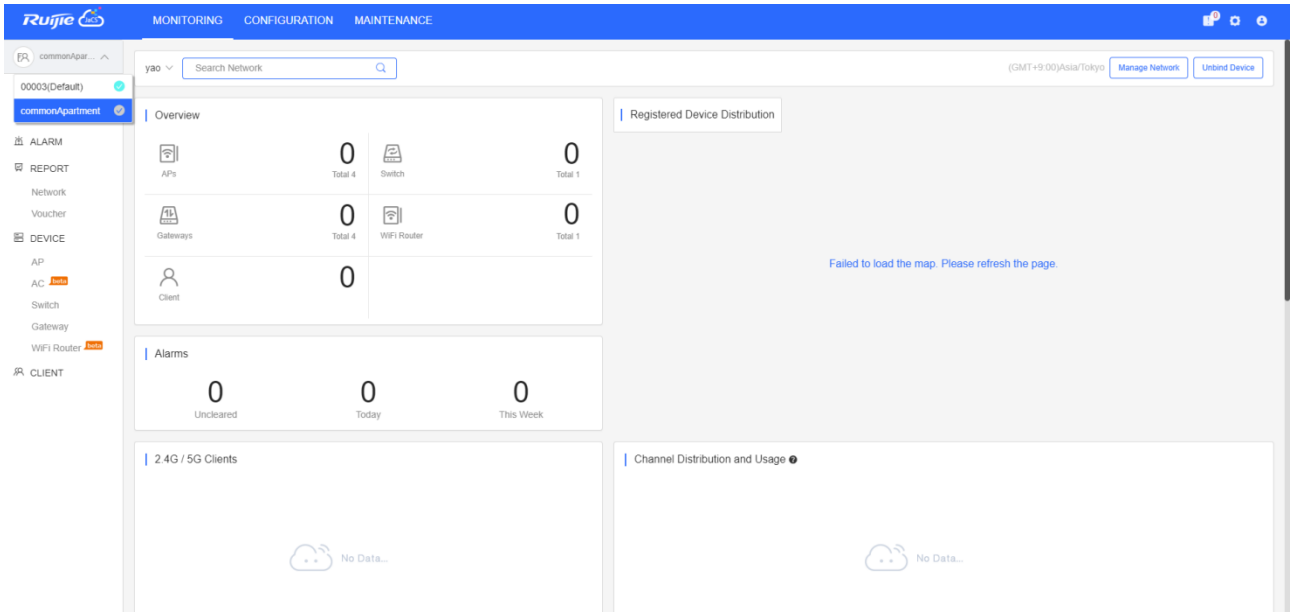


Step 3 Copy the link and send to the receiver. The receiver can visit the URL and log in to receive the network.





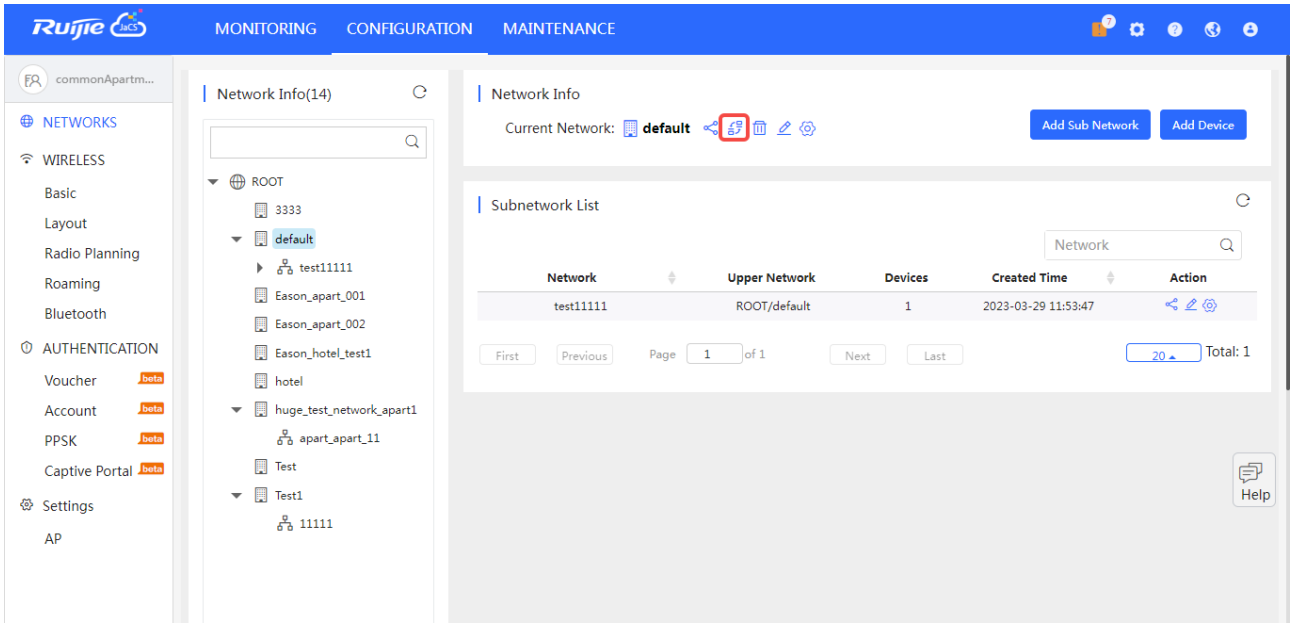
Step 4 Click the on the upper left corner to switch tenant and check the shared network.



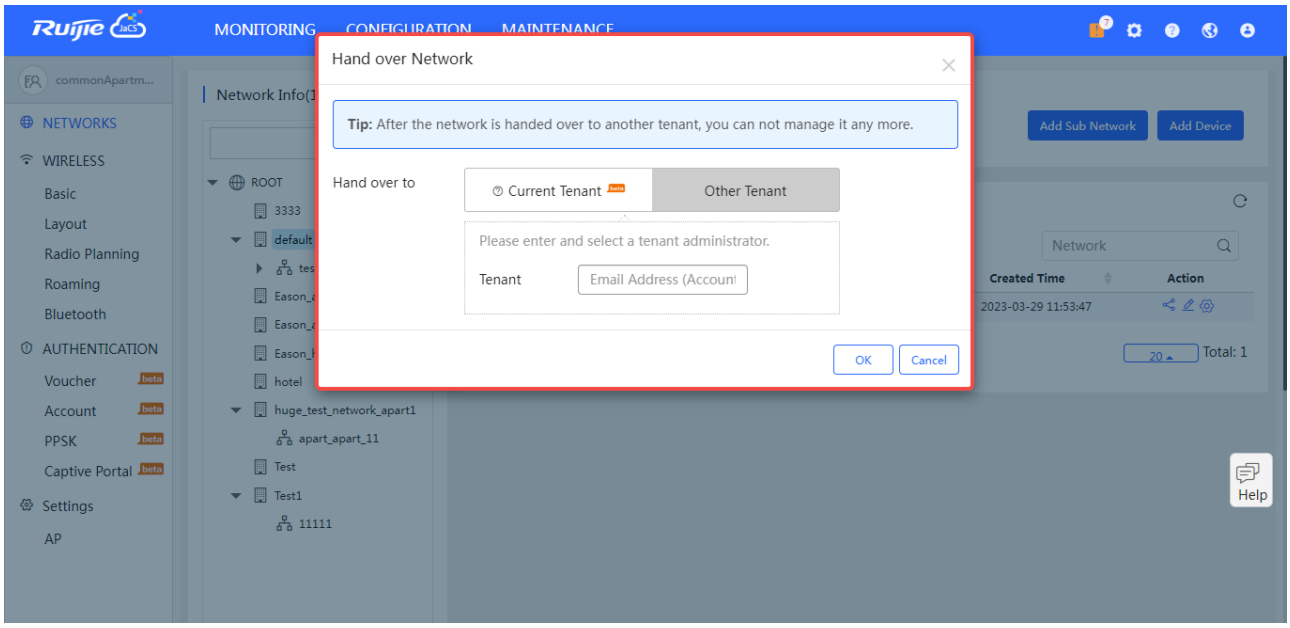
6.1.1.4 Hand over

The network can be handed over to another tenant.

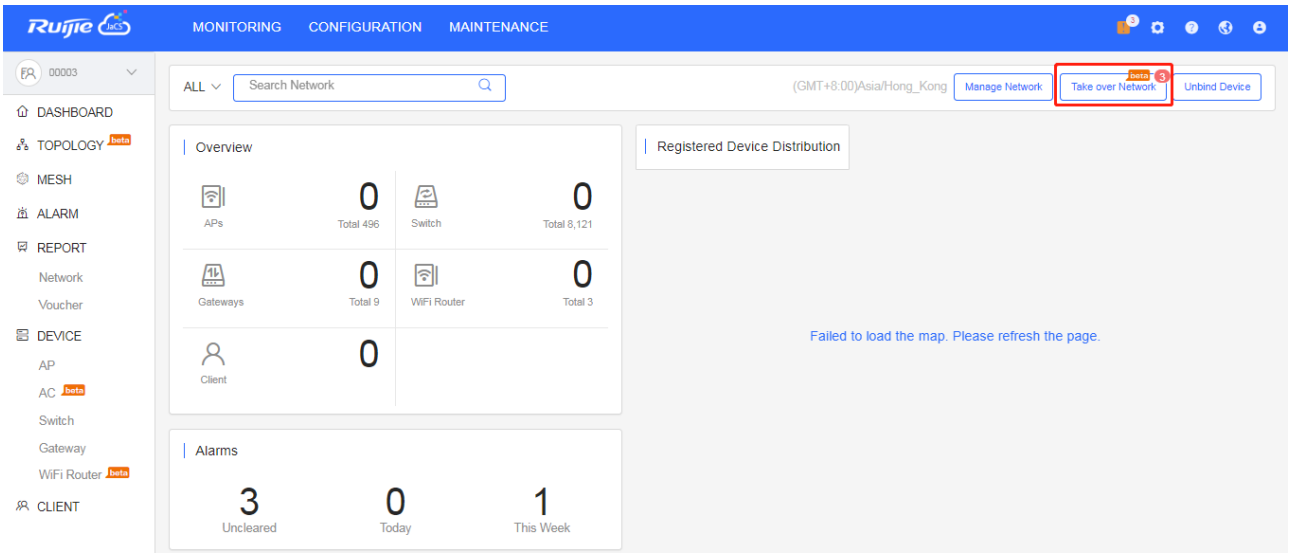
Step 1 Select a network and click the icon to hand over the network to another tenant.



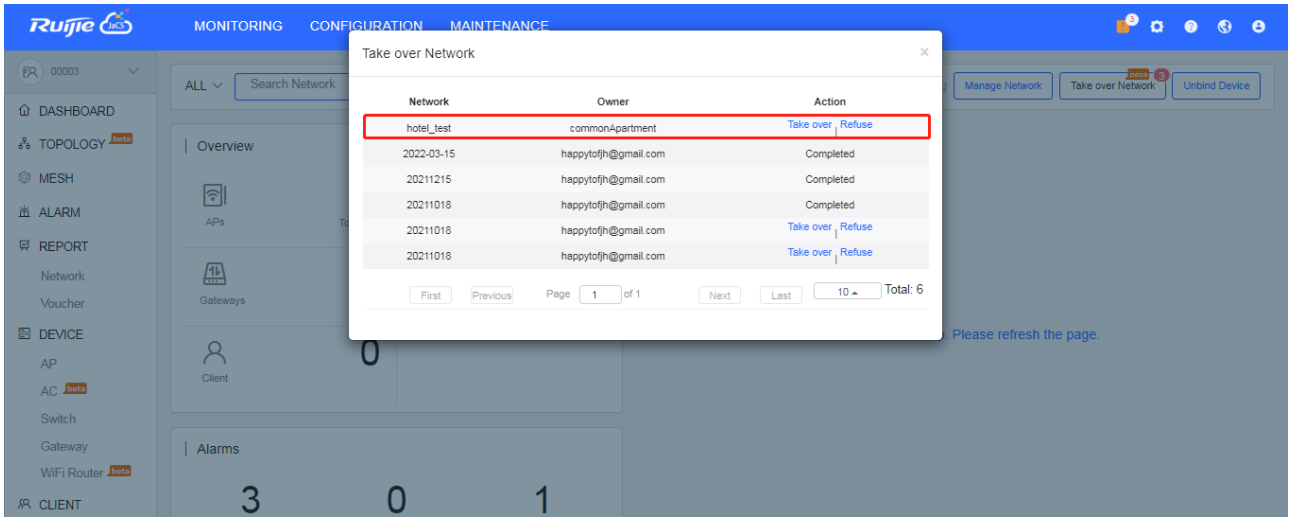
Step 2 Click **Other Tenant** and enter the Email address of tenant, and click **OK**. After the receiver takes over the network, you cannot manage the network anymore.



Step 3 As the receiver logs in to Ruijie JaCS, an icon is displayed on the upper right corner.



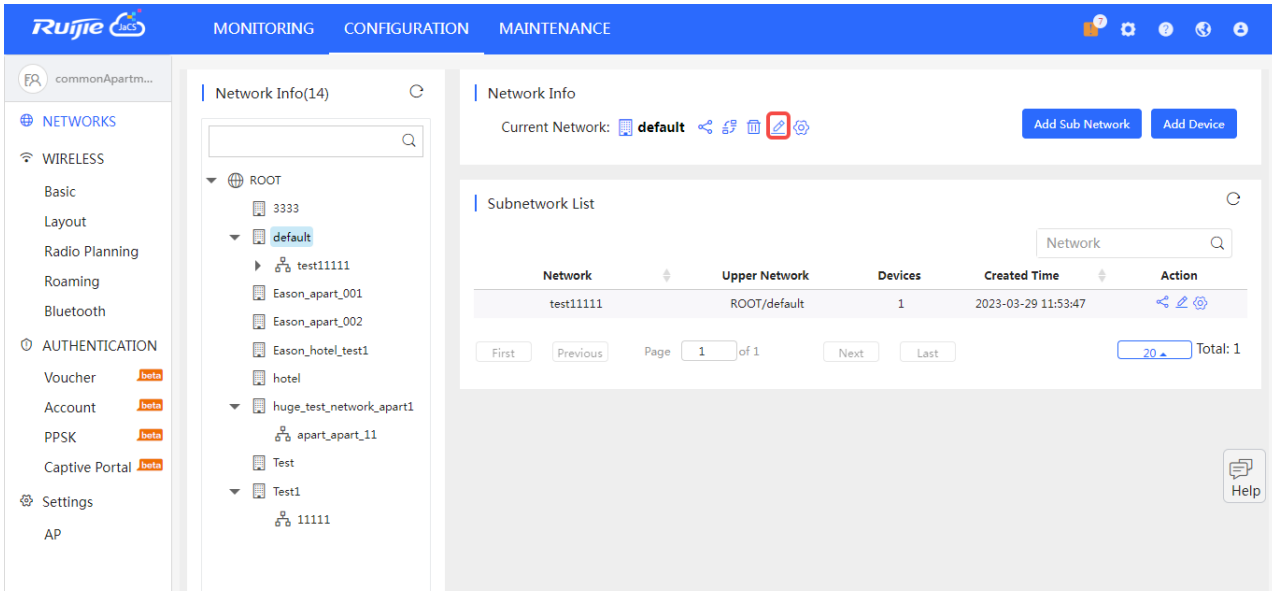
Step 4 Click **Take over Network** to take over or refuse the network.



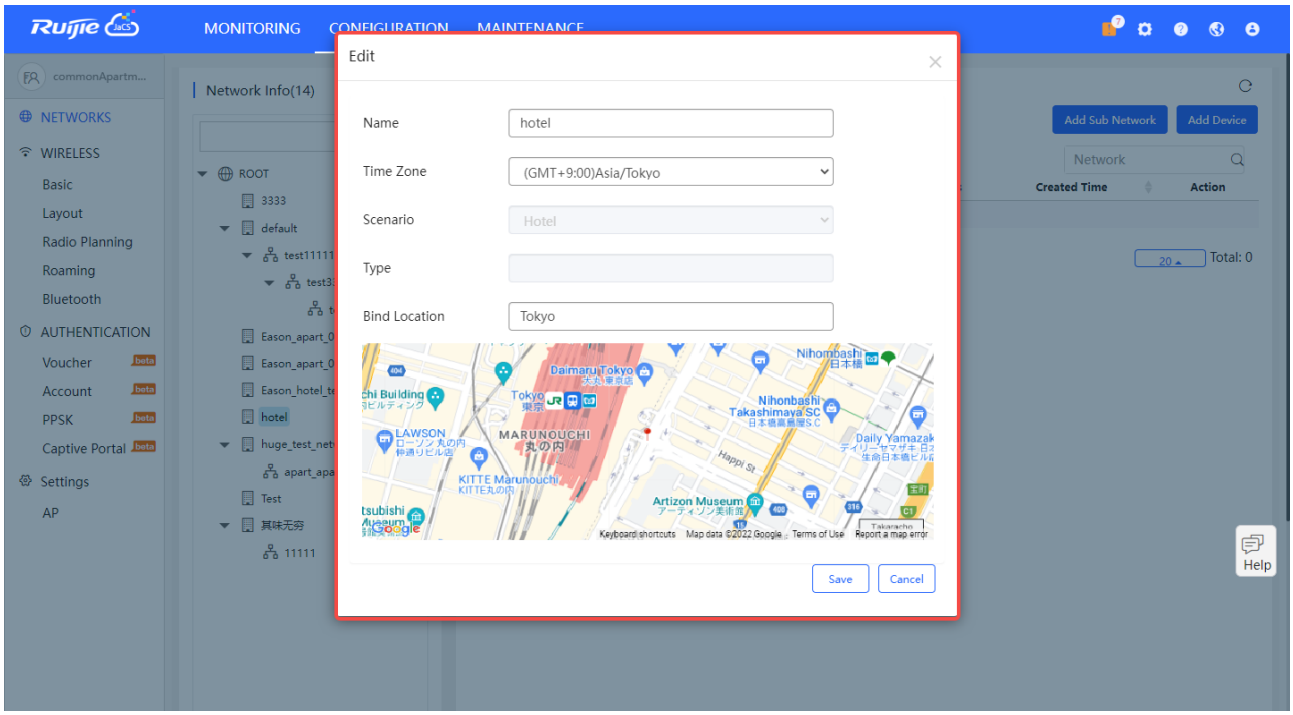
6.1.1.5 Edit

Select the network and click the icon to edit the network.

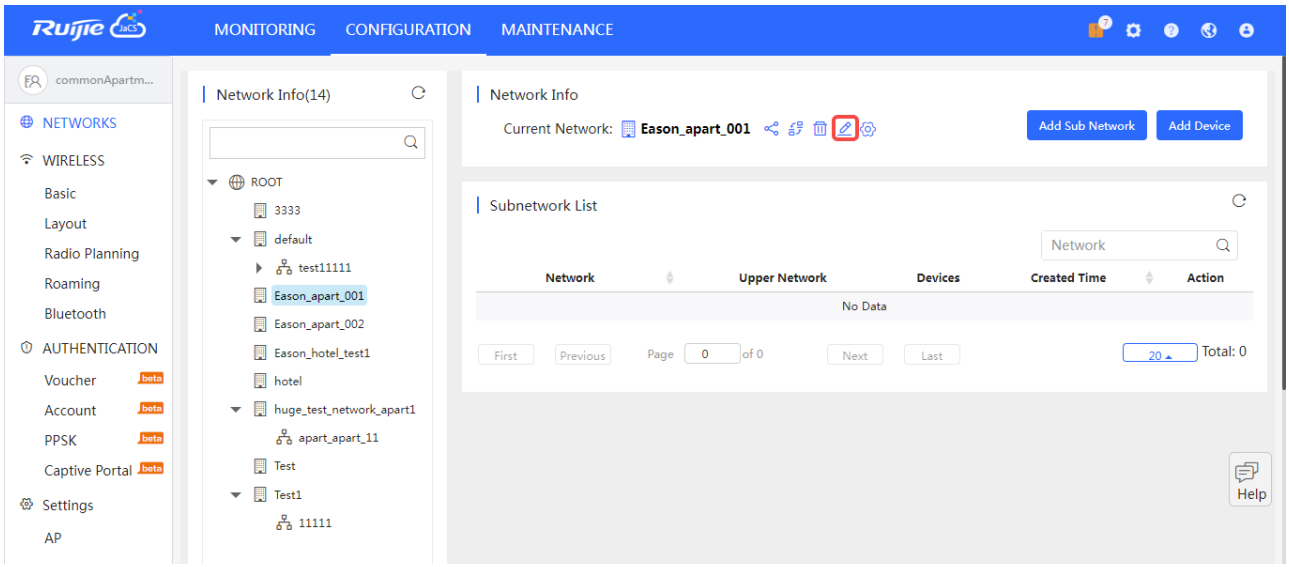
Non-apartment Scenario



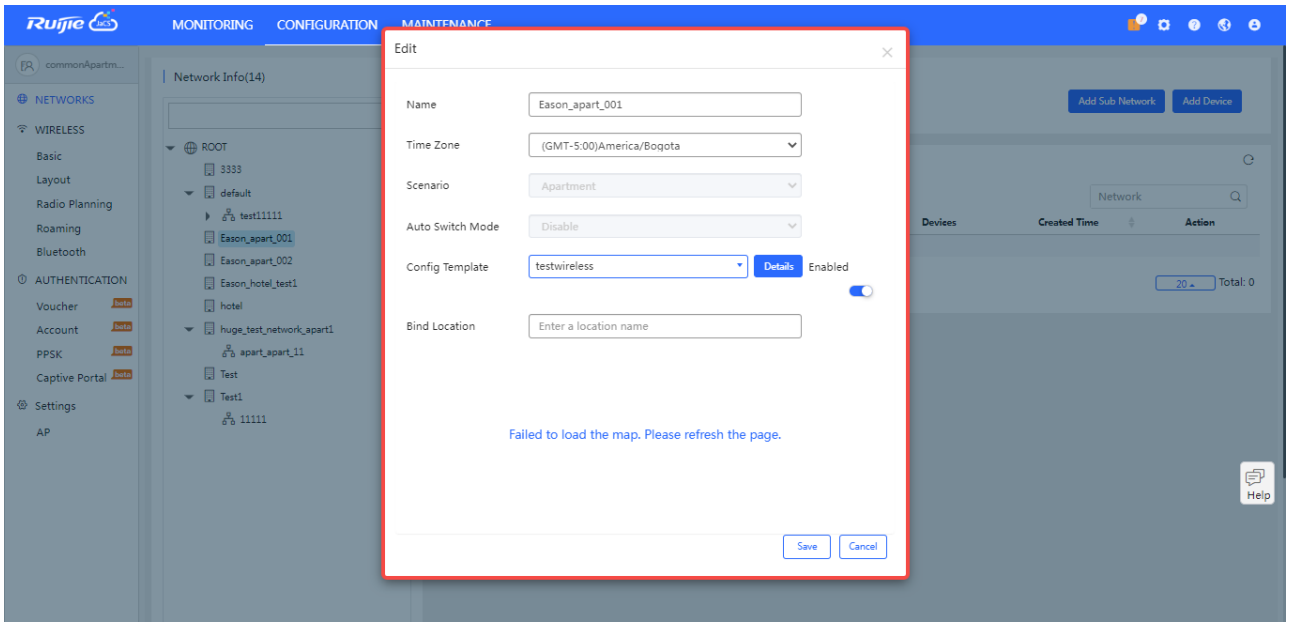
You can edit network name and time zone, and bind location here.



Apartment Scenario

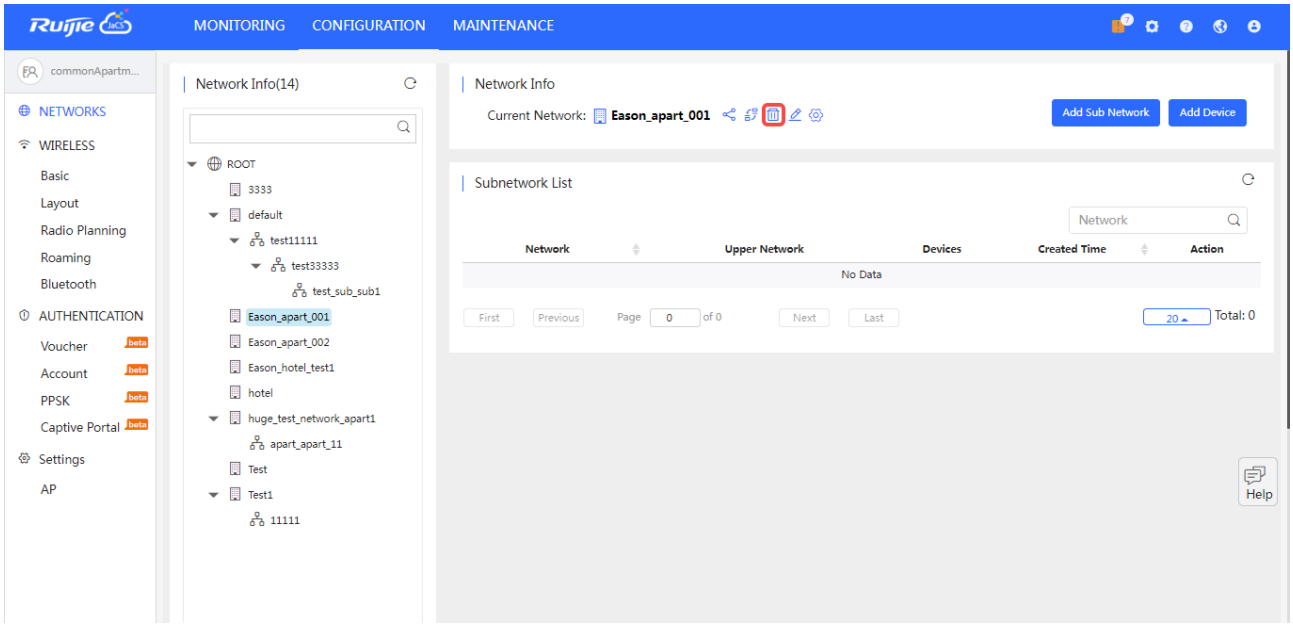


You can edit network name and time zone, bind location and select an initial configuration template here.



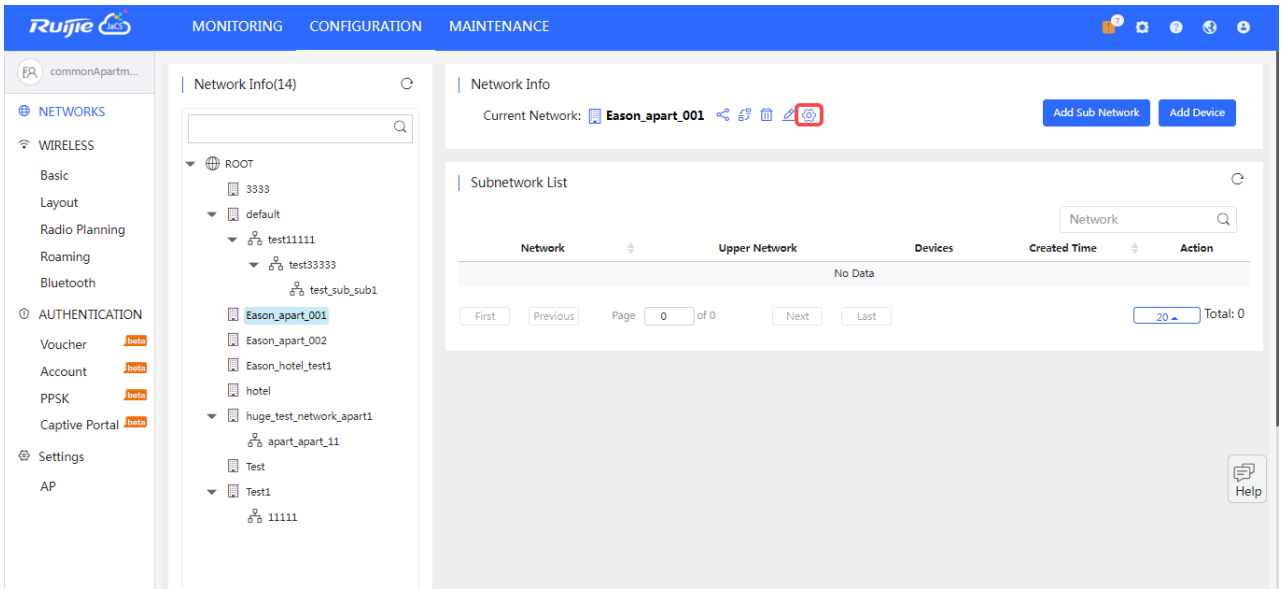
6.1.1.6 Delete

Select the network and click the icon to delete the network.



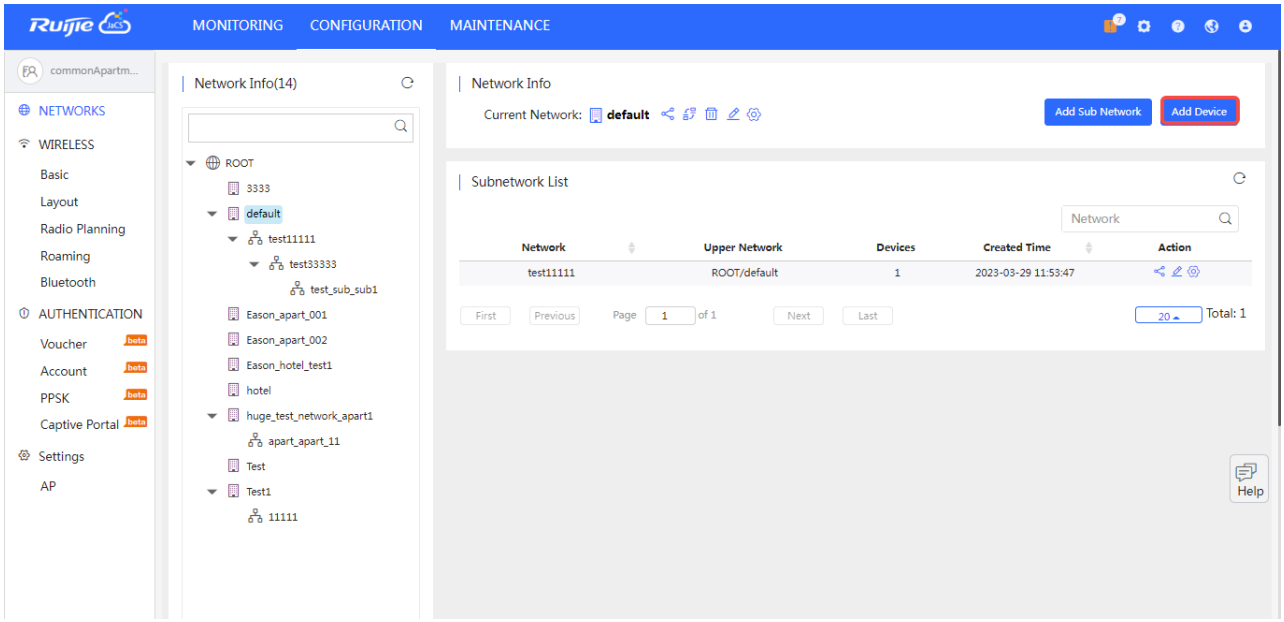
6.1.1.7 Configuration

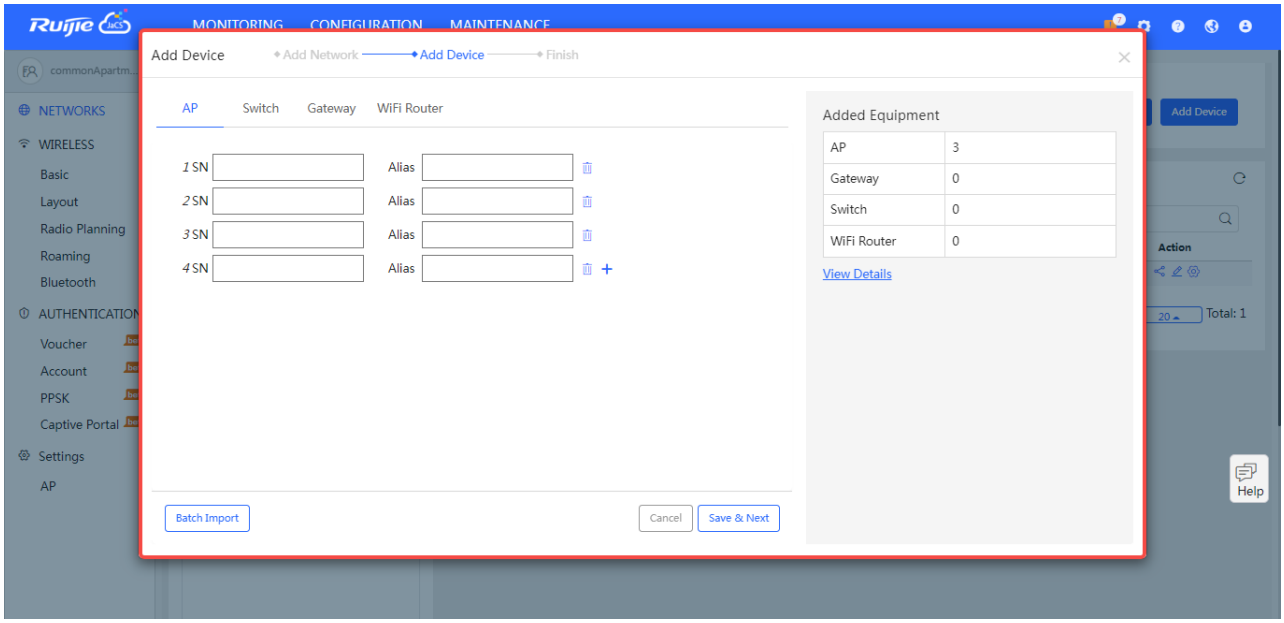
Select the network and click the icon on the **Action** column to configure it.



6.1.1.8 Add Device

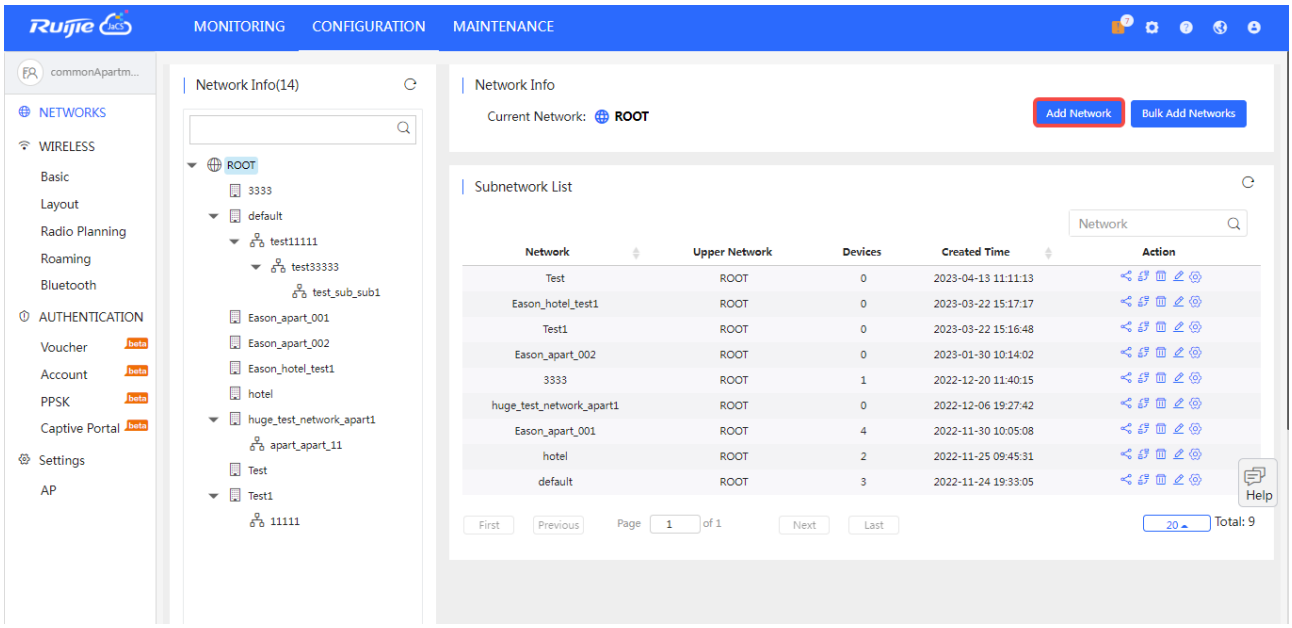
Click **CONFIGURATION** > **NETWORKS** to open the page. Choose a network, and click **Add Device** to add APs, switches, gateways, and WiFi routers.





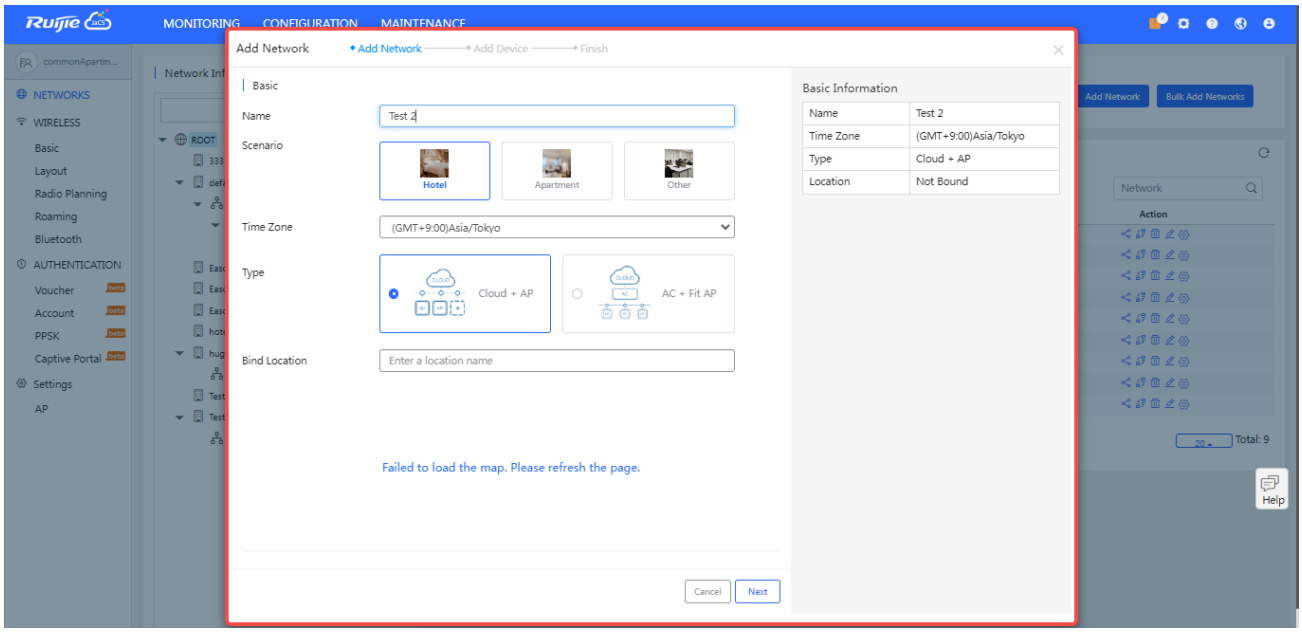
6.1.2 Add Network

Select **CONFIGURATION** > **NETWORKS**, and click **Add Network**.

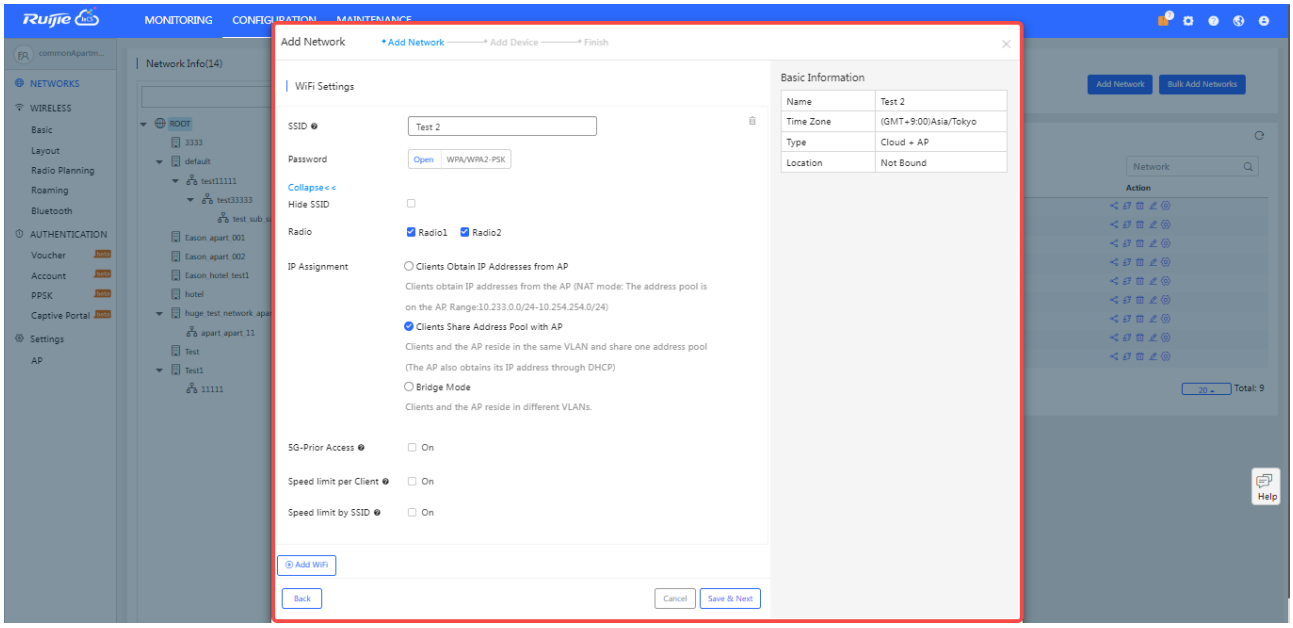


Non-apartment Scenario

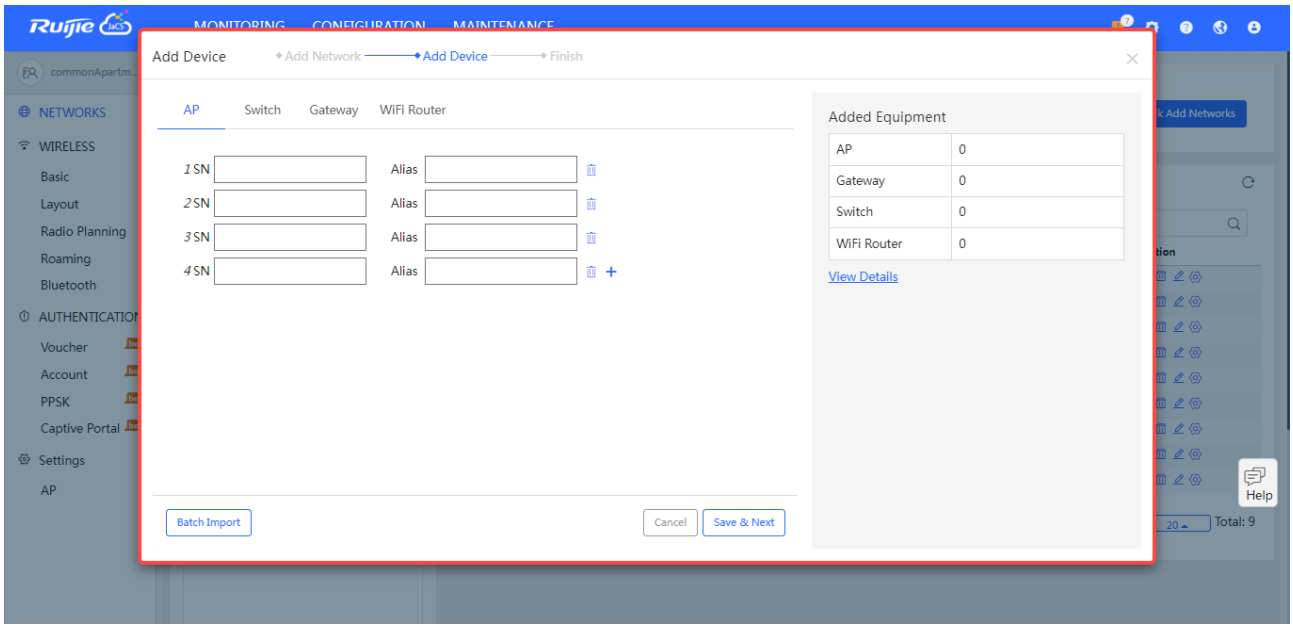
Enter the network name and specify the network location.



Enter the Wi-Fi information as required, and click **Save & Next**.

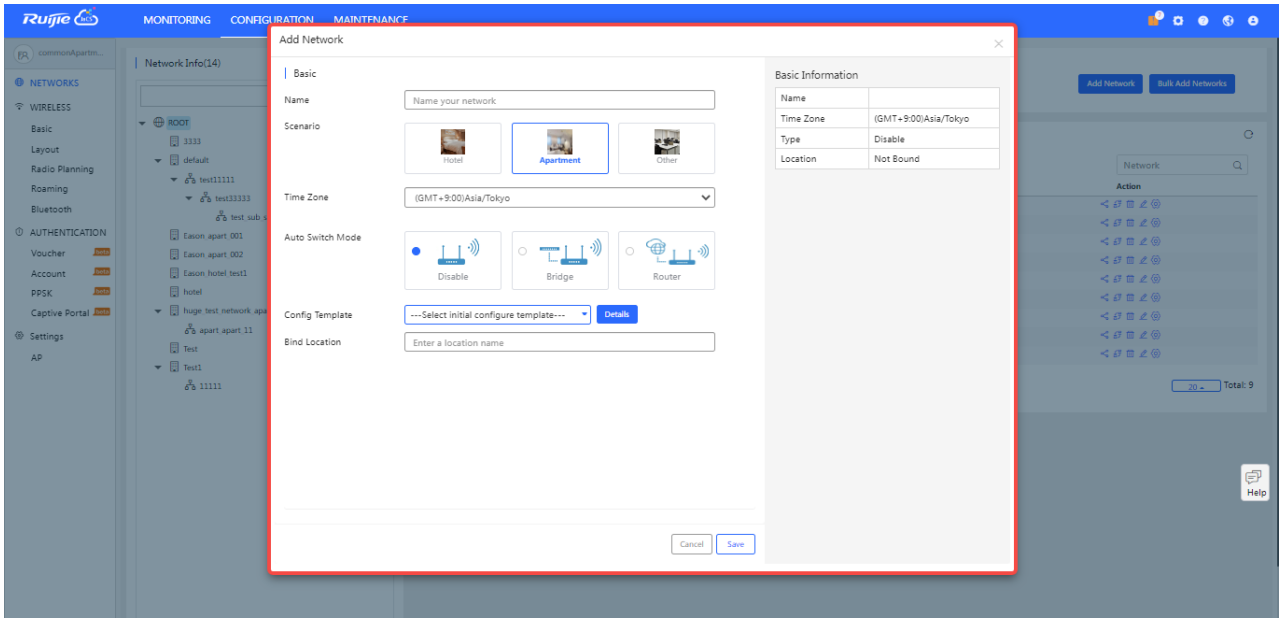


Enter the information of APs, switches and gateways, and click **Save & Next**. Or click **Batch Import** to download the template, enter the device information in the table, and then batch import devices into the system.



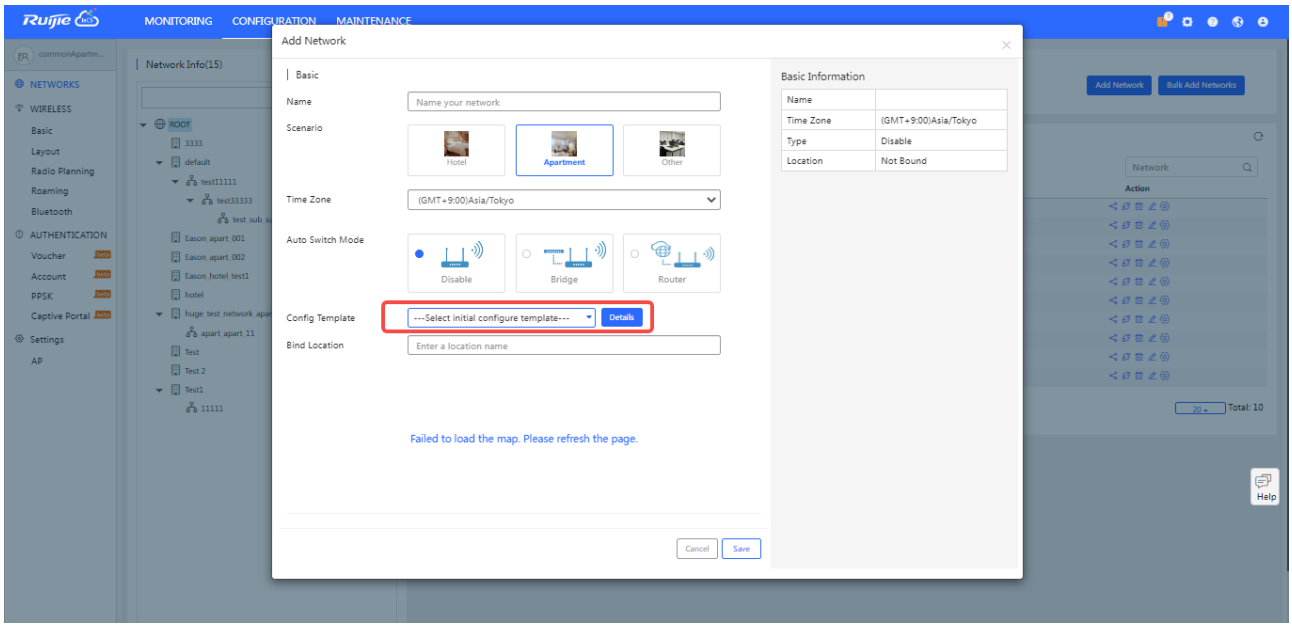
Apartment Scenario

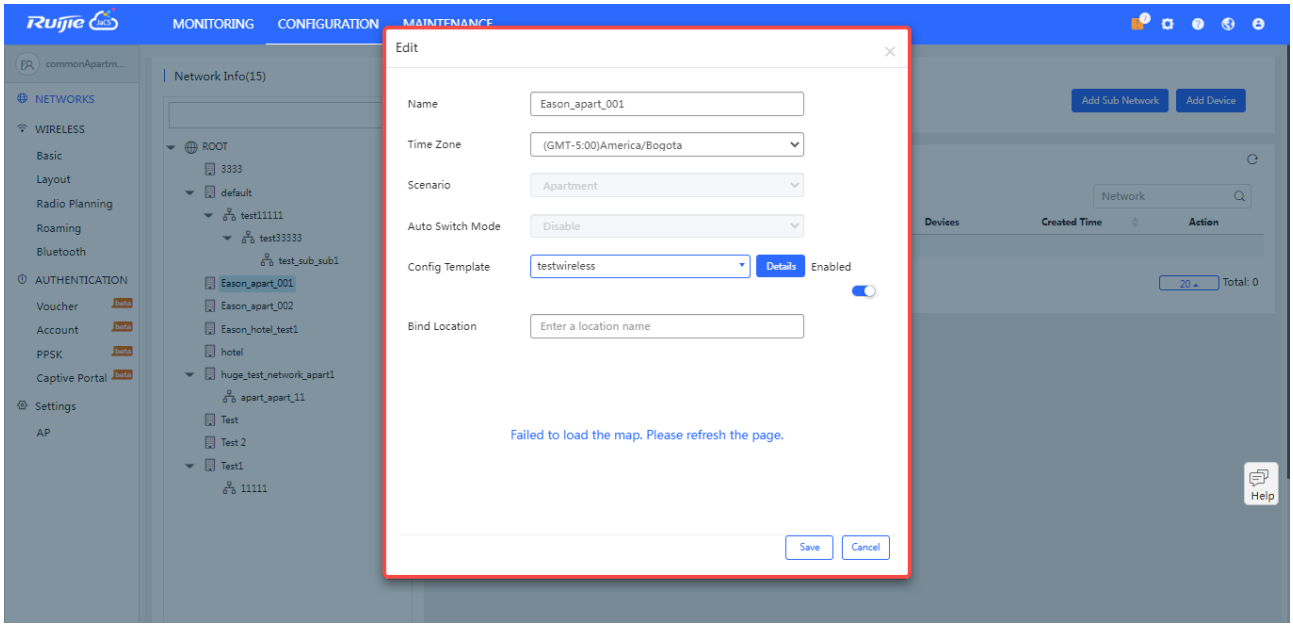
Enter the network name, select the scenario and bind the location.



6.1.3 Initial Configuration Template

When adding or editing an Apartment network, you can decide whether to apply an initial configuration template to the devices in the network. If you select a template and enable it, its configurations will be automatically applied to all AP180 series devices in the network when they are connected to the JaCS for the first time. It should be noticed that the configurations are automatically applied to the devices once only.



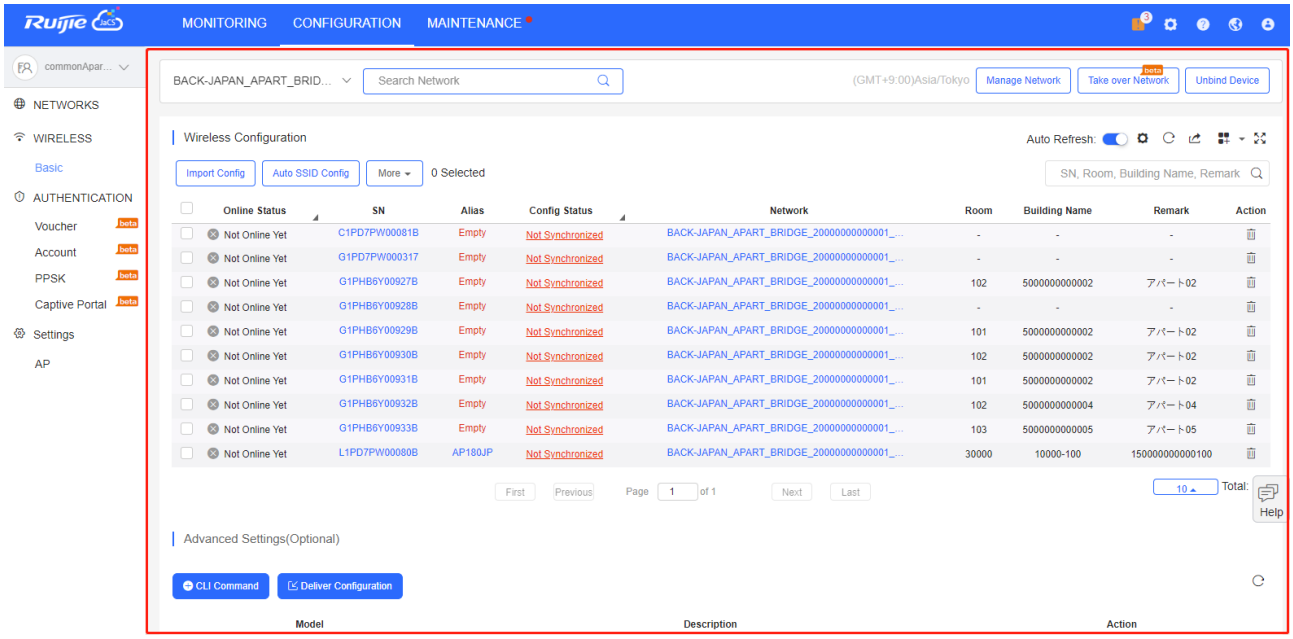


- When an Apartment network is edited, the last-applied initial configuration template is selected automatcially. In this case, you need to manually enbale or disable it.
- If a device is moved to an Apartment network to which an initial configuration template has been applied, the configurations of the template will automatically be applied to it.

6.2 Wireless

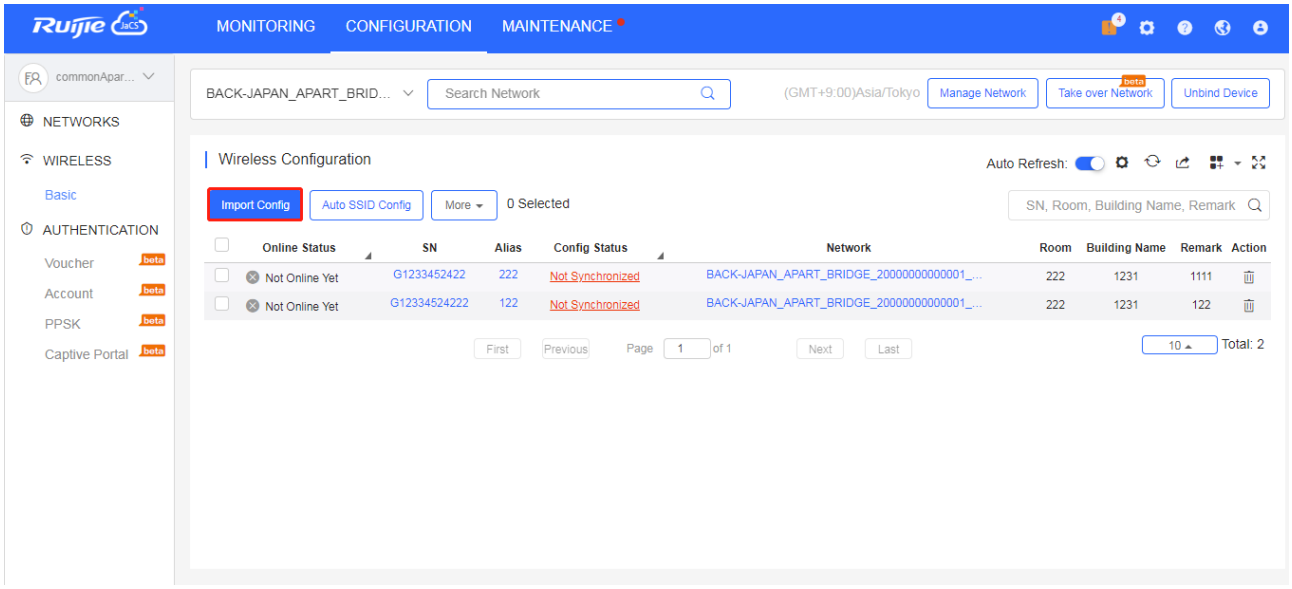
6.2.1 Basic (Apartment Scenario)

Select **CONFIGURATION > WIRELESS > Basic** to configure SSID and password of AP, and to run CLI commands to deliver configurations to the devices in the Apartment scenario.

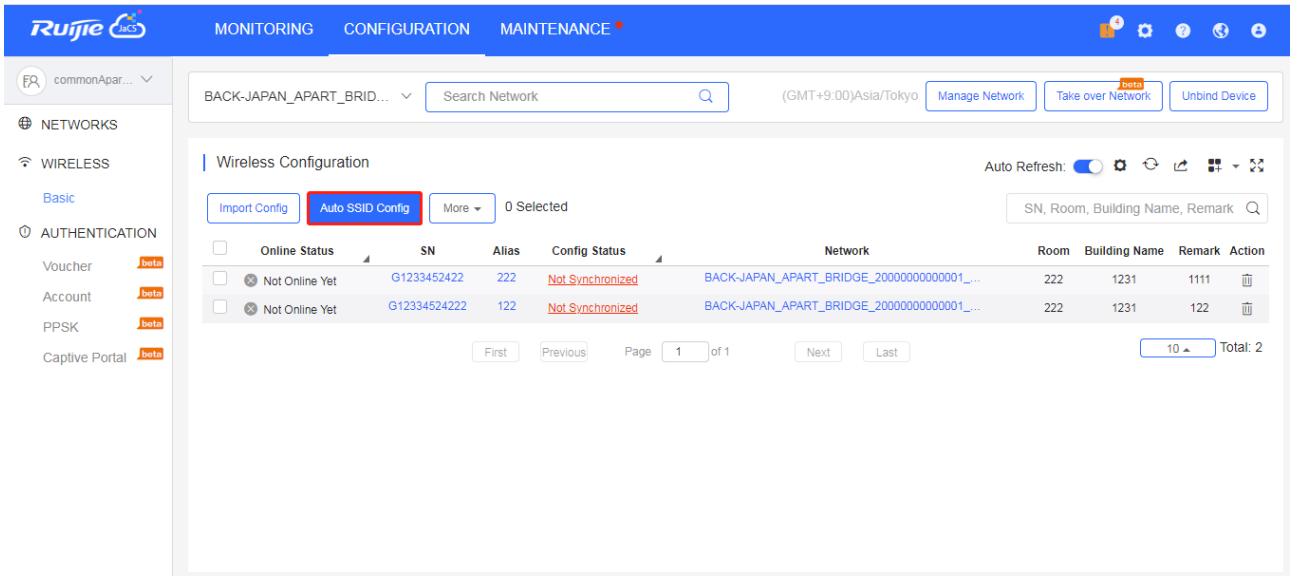


In the apartment scenario, SSID and password can be configured in 2 ways.

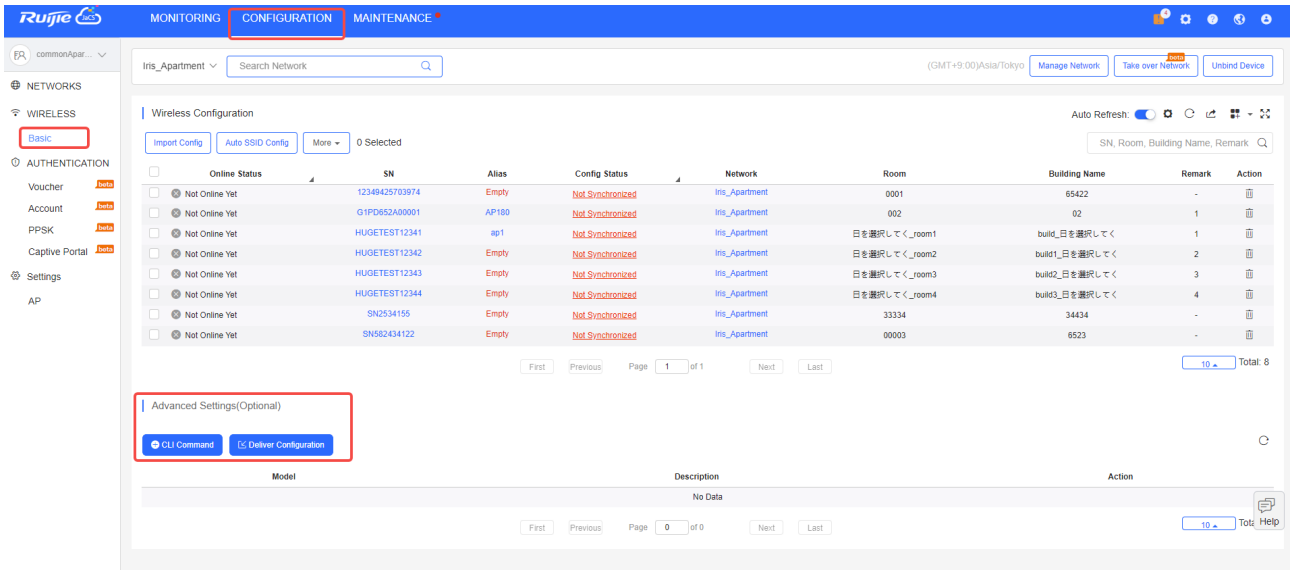
Option 1: Click **Import Config** to manually import SSIDs and passwords in an EXCEL file.



Option 2: Select **Auto SSID Config**. In this way, you don't need to manually configure the SSID and password.

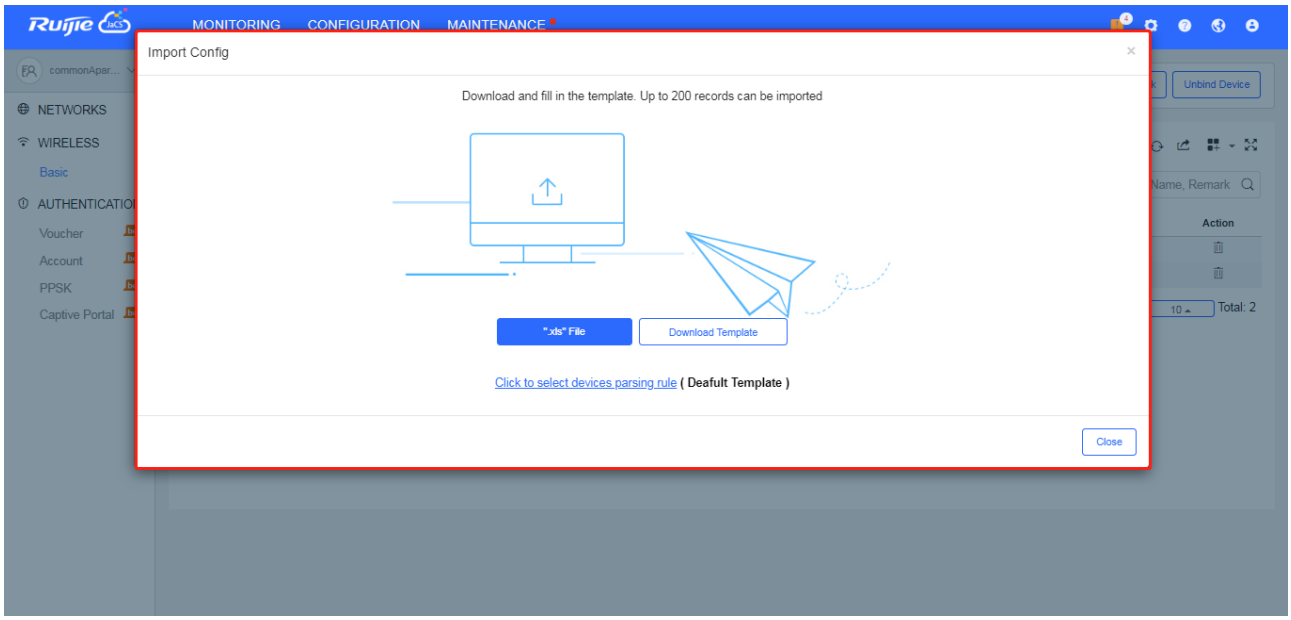


You also can run CLI commands in the **Advanced Settings** to deliver the configurations to the devices in the Apartment scenario.



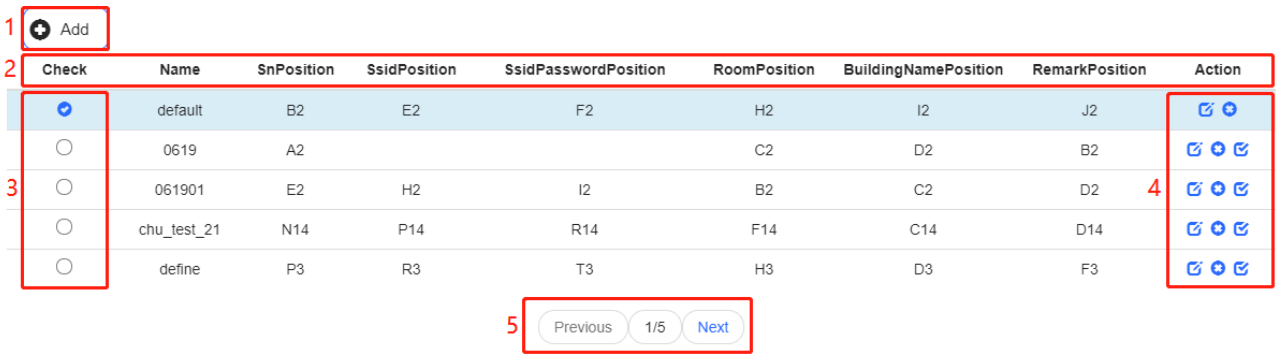
6.2.1.1 Customize Template Rules

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

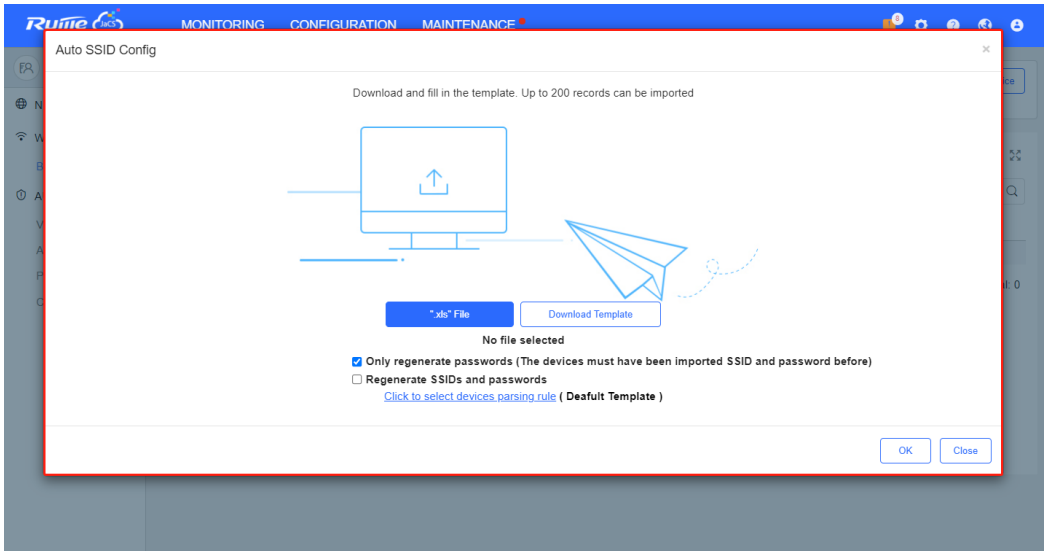
※User can customize the EXCEL parsing rule from columns A to Z and rows 1 to 15.

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

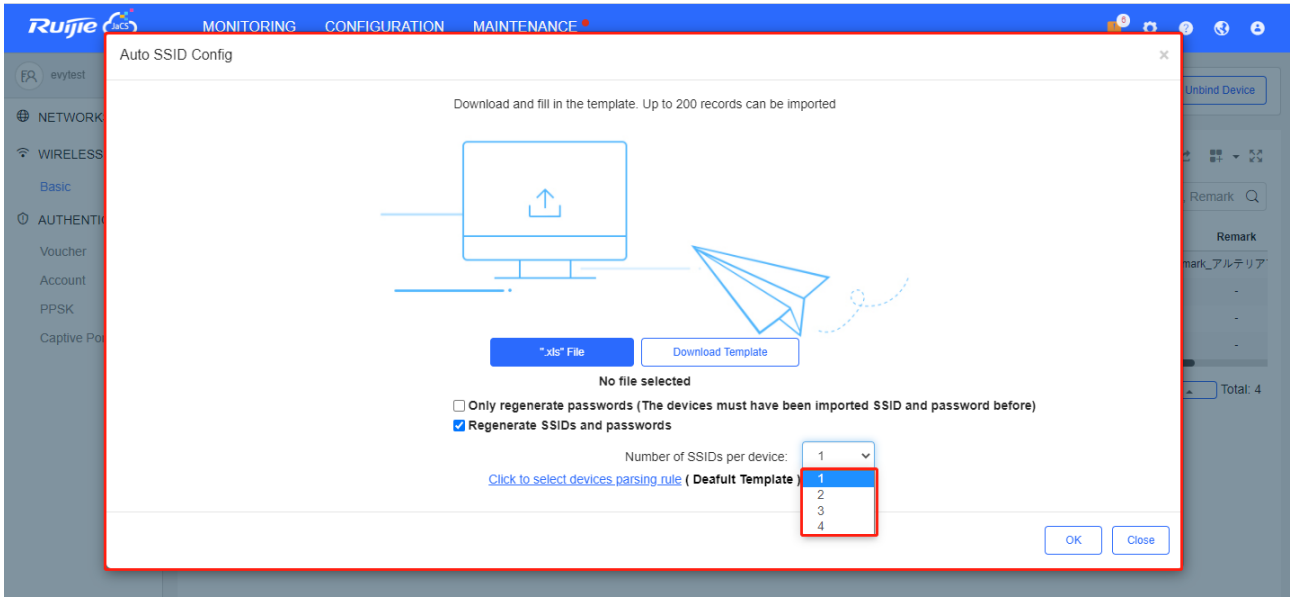
6.2.1.2 Auto SSID Config

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:

A	B	C	D	E	F	G
Building Name	Room					
100001	203					
100001	204					
100001	205					

The custom rule may be set as below:

- Name: ModifySSID
- snPosition:
- ssidPosition:
- ssidPasswordPosition:
- roomPosition: B2
- buildingNamePosition: A2
- RemarkPosition:

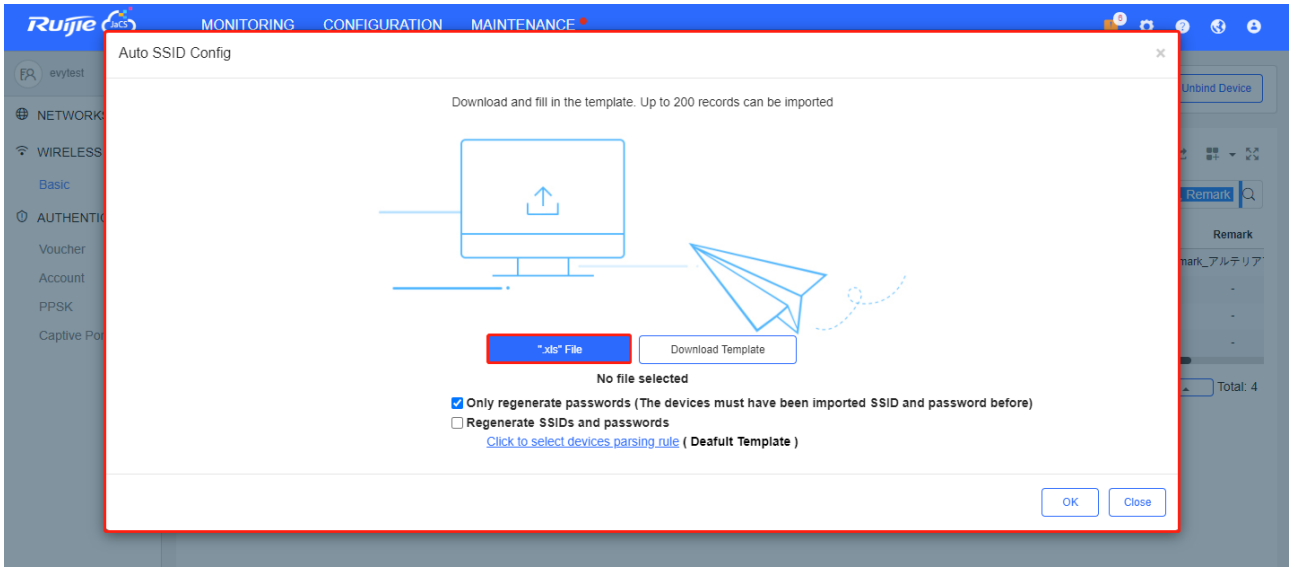
※If Remark is filled in EXCEL file, the former remark saved in the Cloud will be overwritten.

- Use Cloud's Default Template to Configure SSID/Password

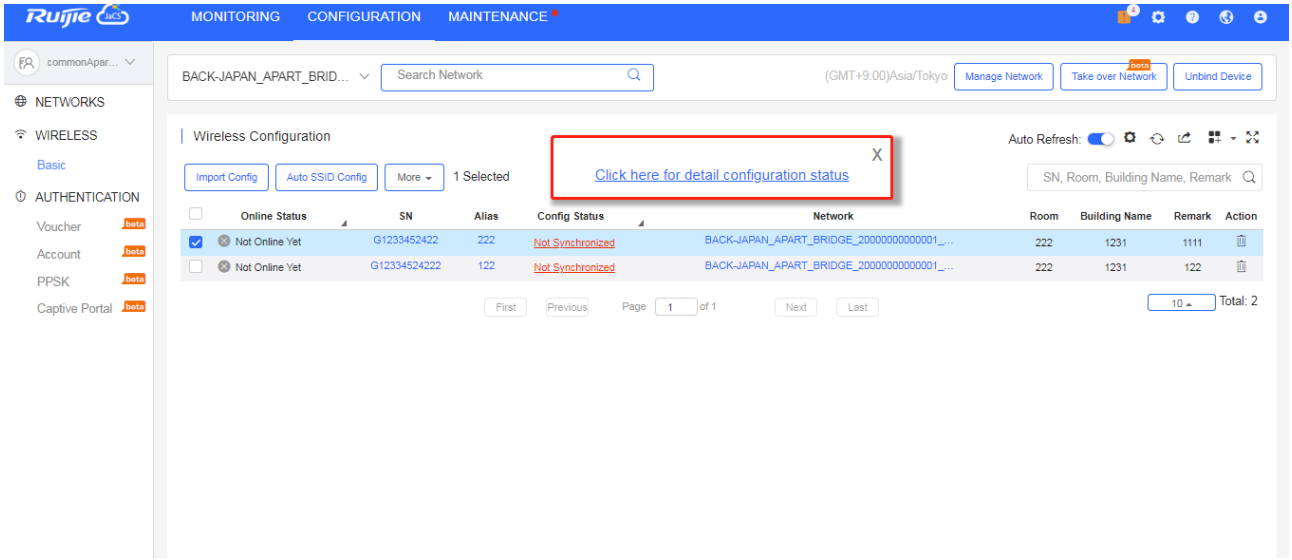
Download the template and fill the information as below:

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

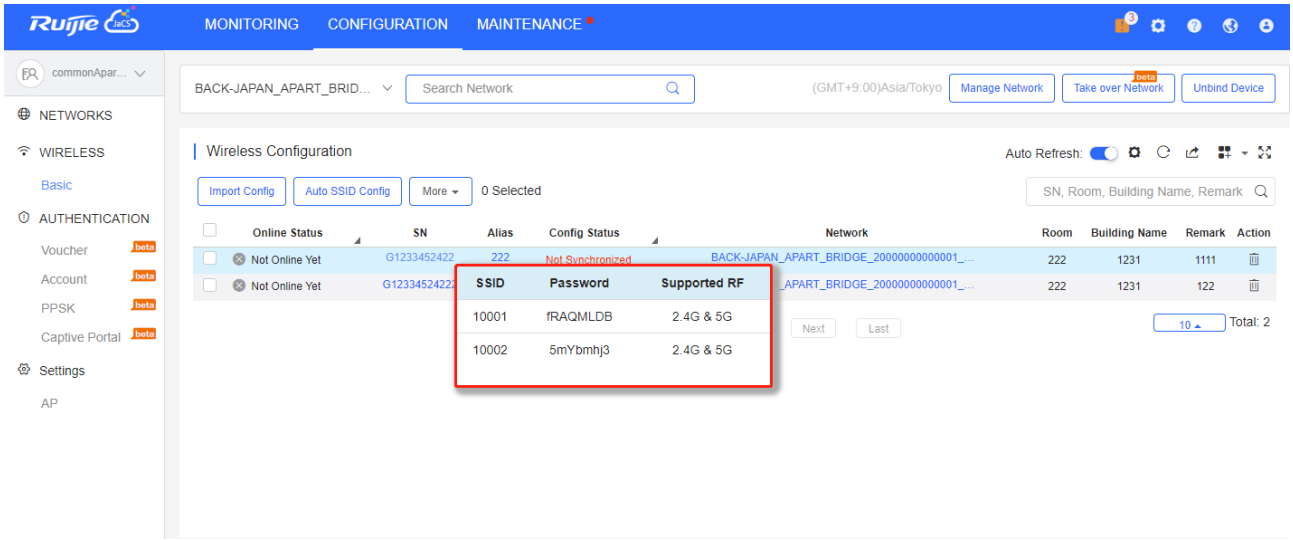
Import the template.



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.



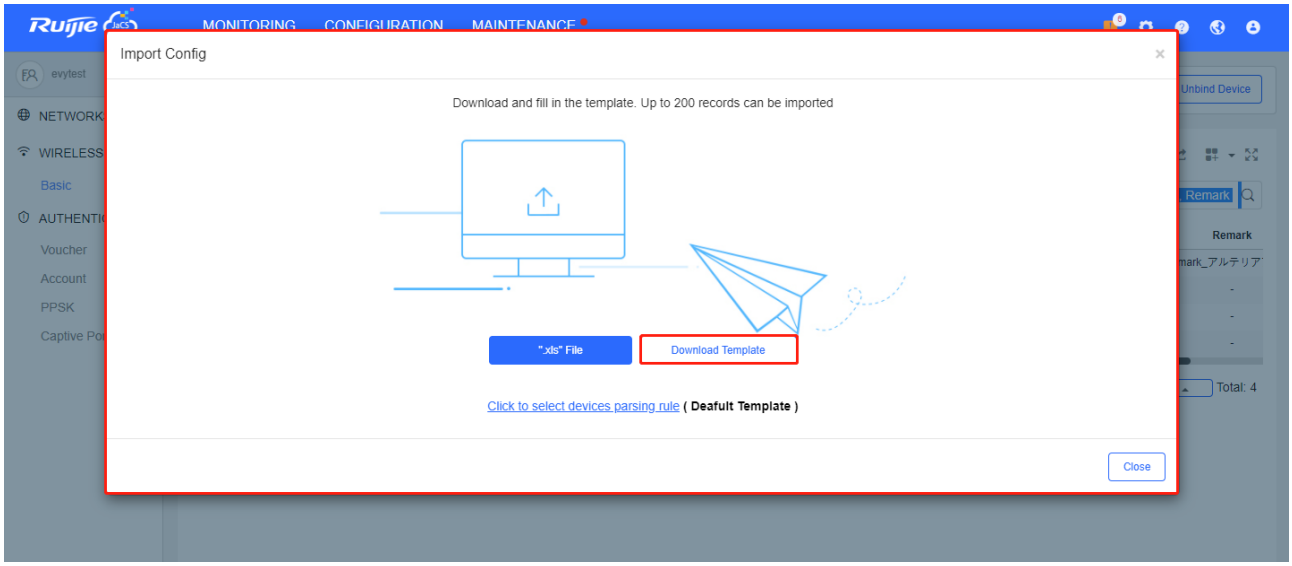
To view the configuration result of the specified device, you can also point to the device **SN** to check the SSID/password. You also can view the supported RF of the device.



6.2.1.3 Import Config

- Use Default Template to Import SSID and Password

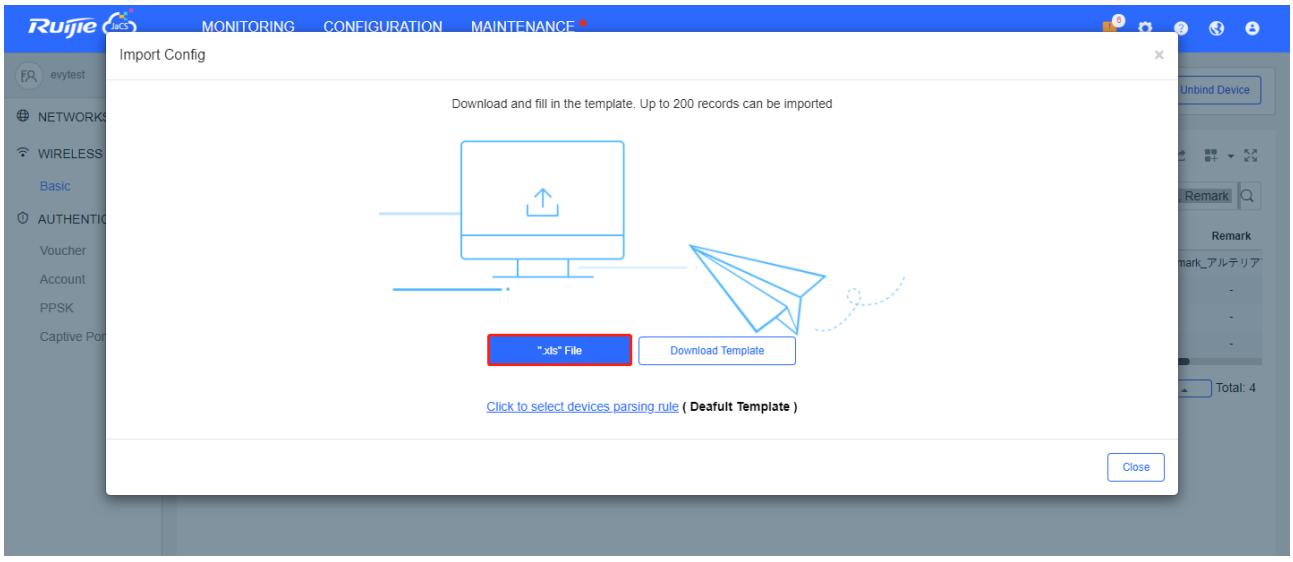
Click **Download Template**.



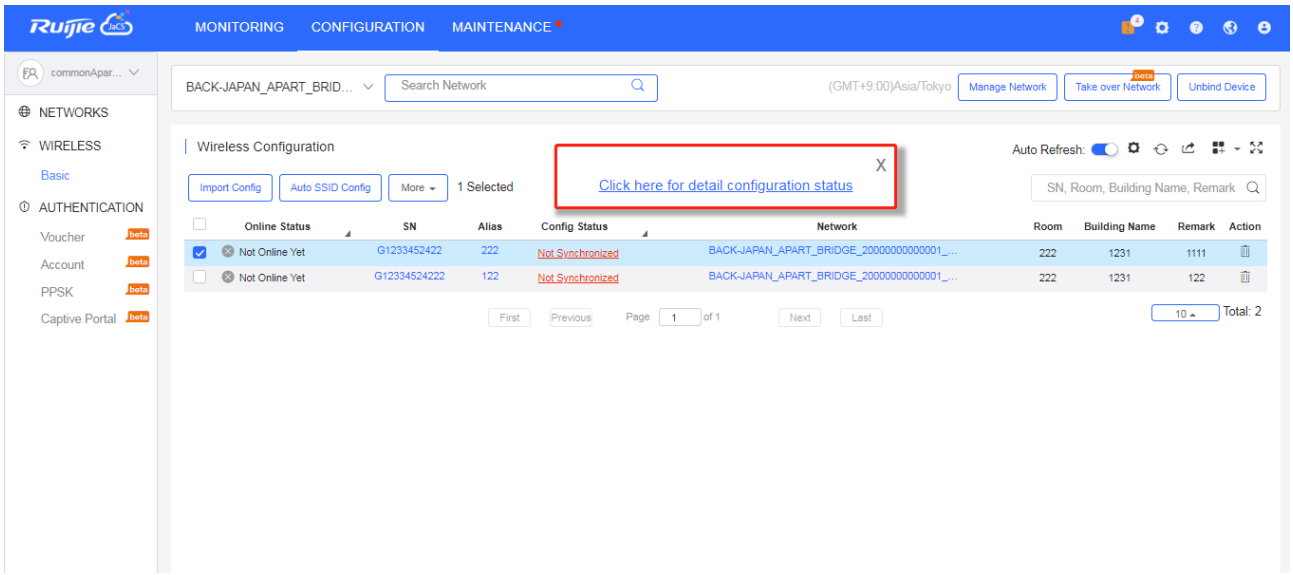
Enter SSID and password. Each AP supports at most 4 SSIDs, and SSIDs and passwords need to be separated by ‘,’.

	A	B	C	D	E	F	G	H	I	J
1	Model	SN	MAC	PN	SSID	SSID Password	Alias	Room	Building Name	Remark
2		G1233452422			10001,10002	66666666,88888888				
3										

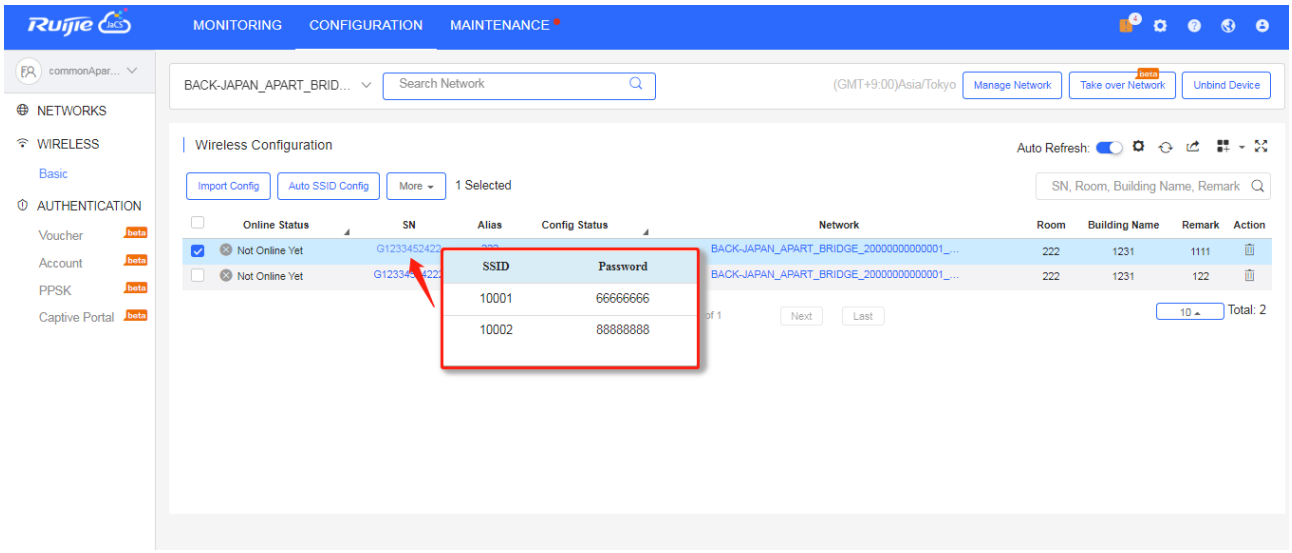
Click **“xls” File** to import the template.



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.

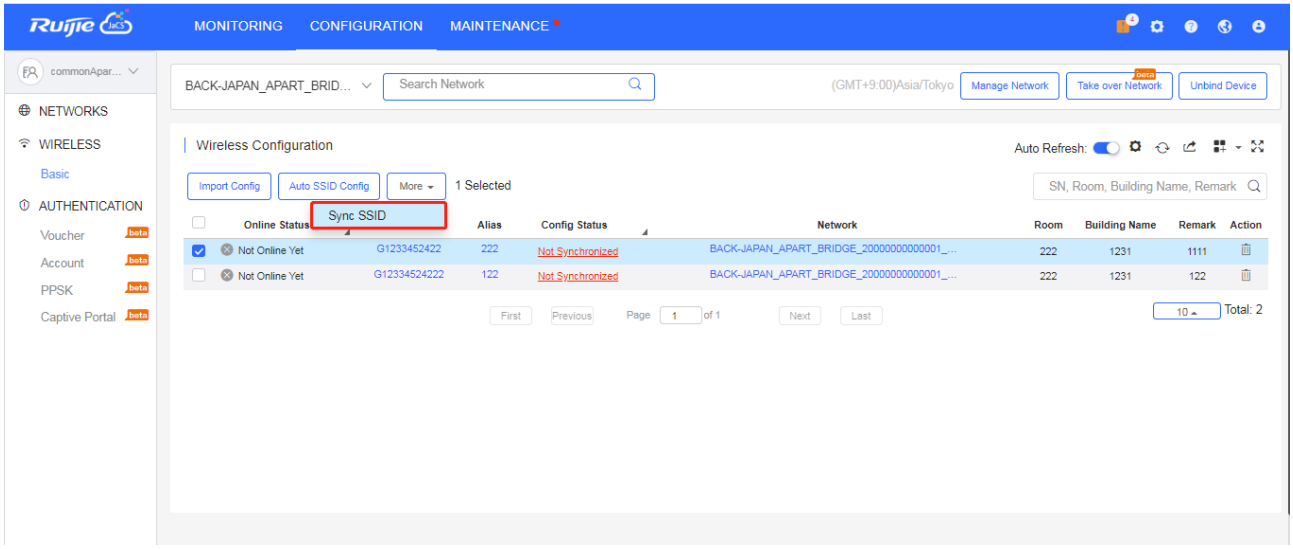
The custom rule may be set as below:

- 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 More > 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.

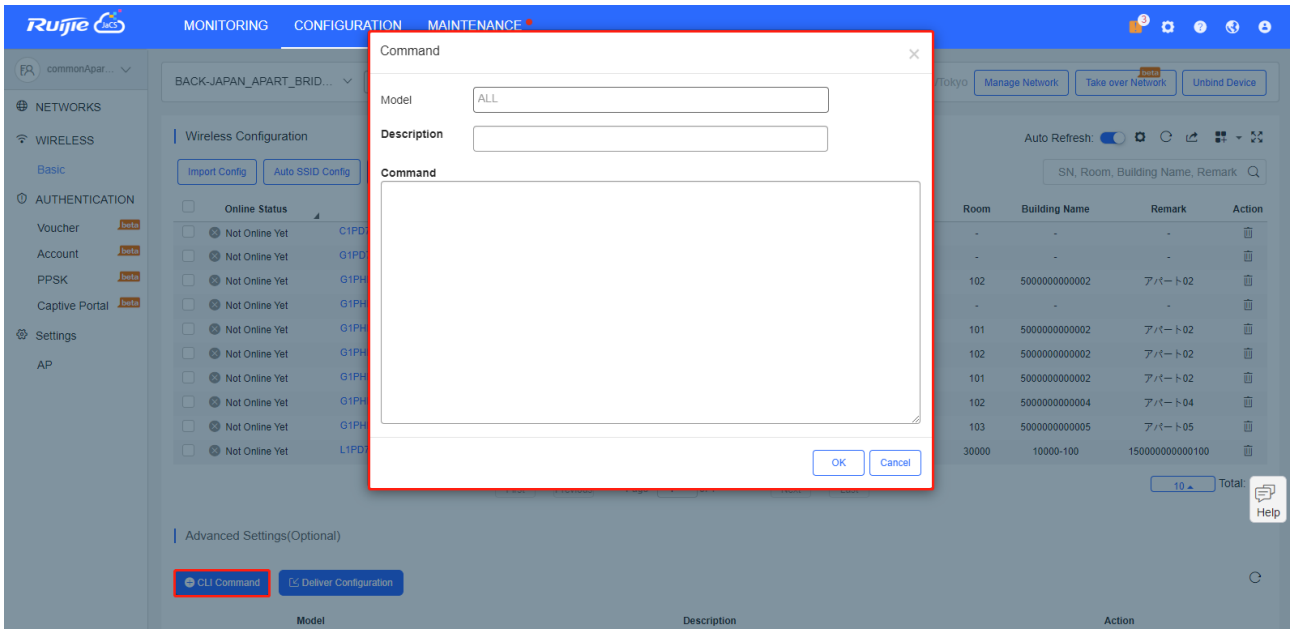


6.2.1.5 CLI Command

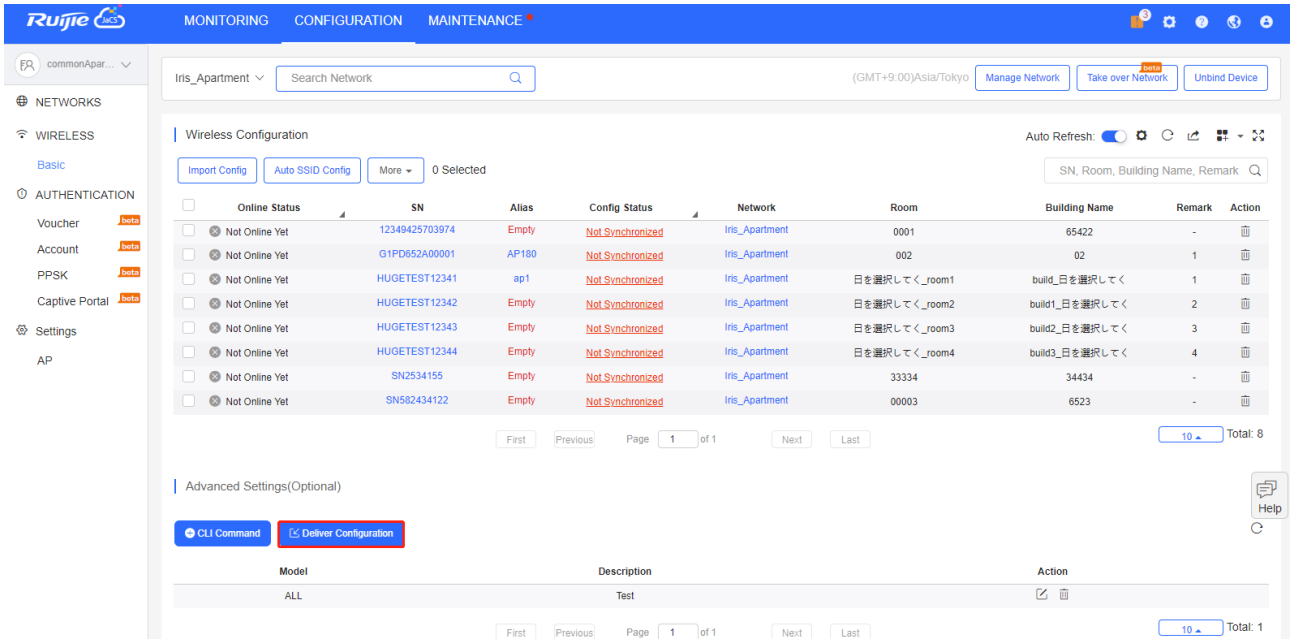
Step 1 Click **CLI Command** to open the setting page.

Step 2 Specify the device model. You can select **All** to deliver the configuration to all devices or select a specific device module.

Step 3 Edit CLI commands. Then, click **OK**.

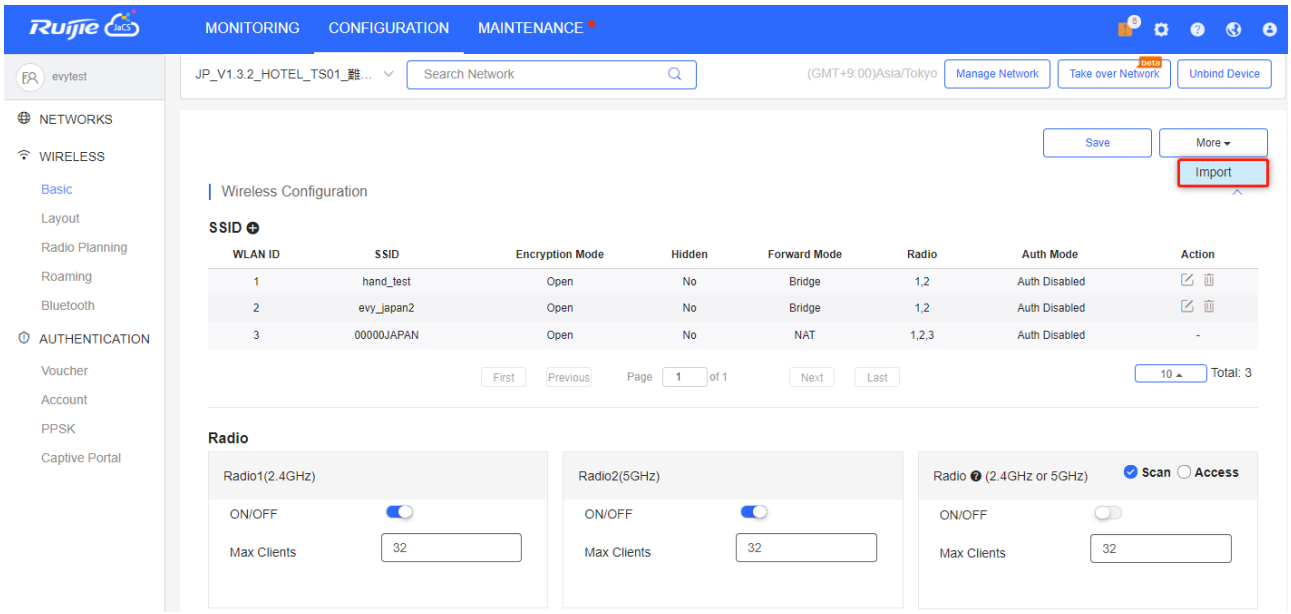


Step 4 Click **Deliver Configuration** to deliver the configuration to the device.

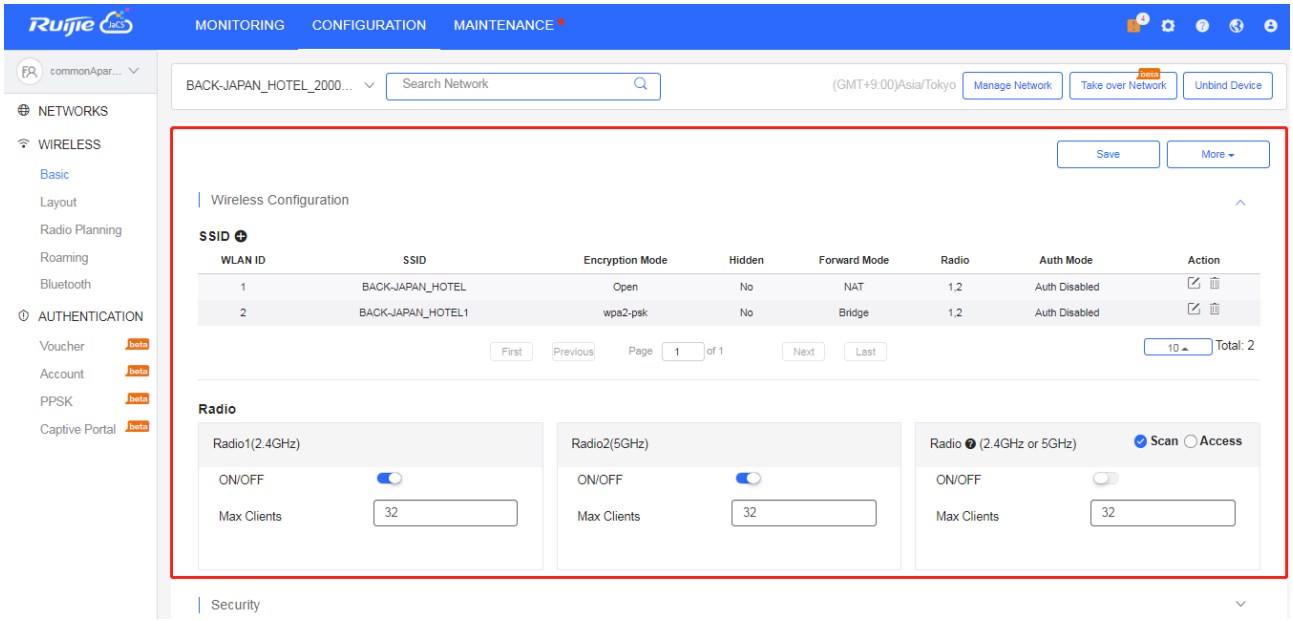


6.2.2 Basic (Non-apartment Scenario)

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 cannot be imported.



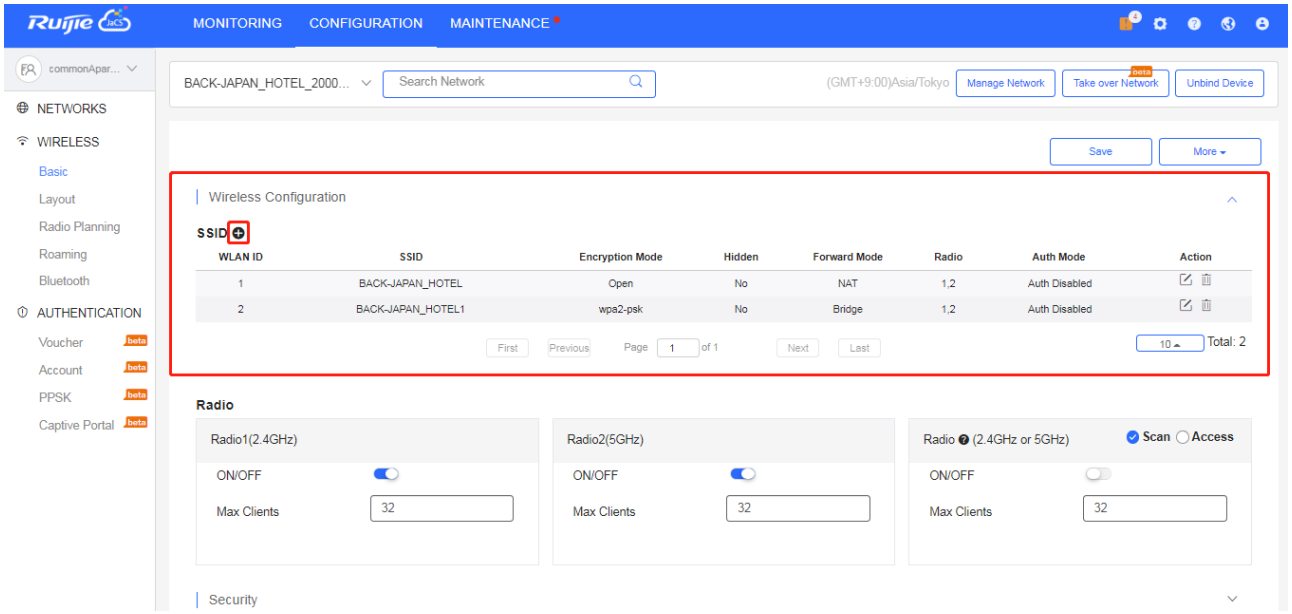
Click **Save** to configure the network.

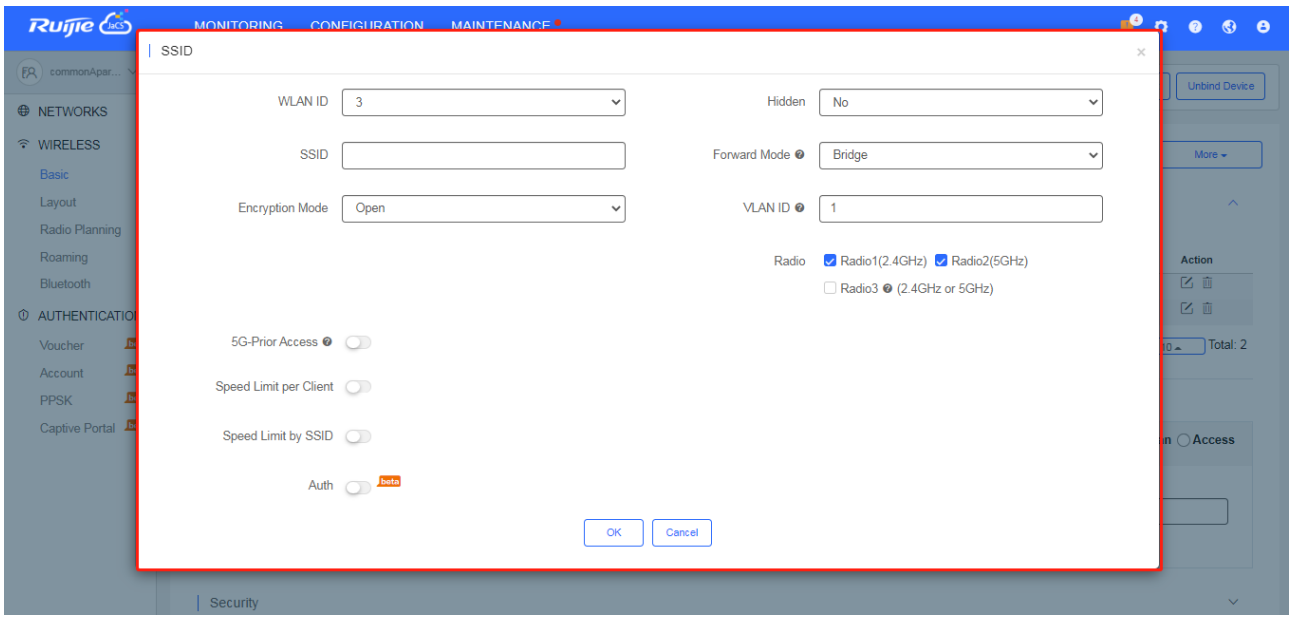


On the **Basic** page, **Wireless**, **Security**, and **Advanced Settings** can be configured.

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.





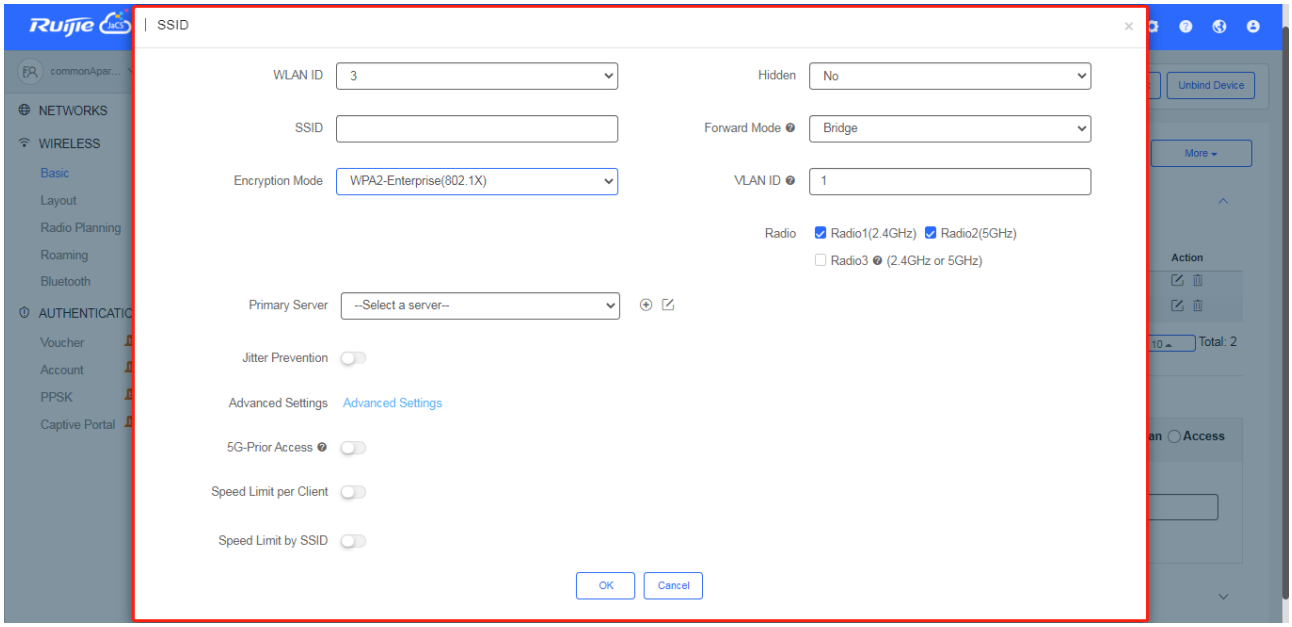
Parameters on the **SSID** page are defined as follows.

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 cannot be changed subsequently. The maximum value of **WLAN ID** is 16.

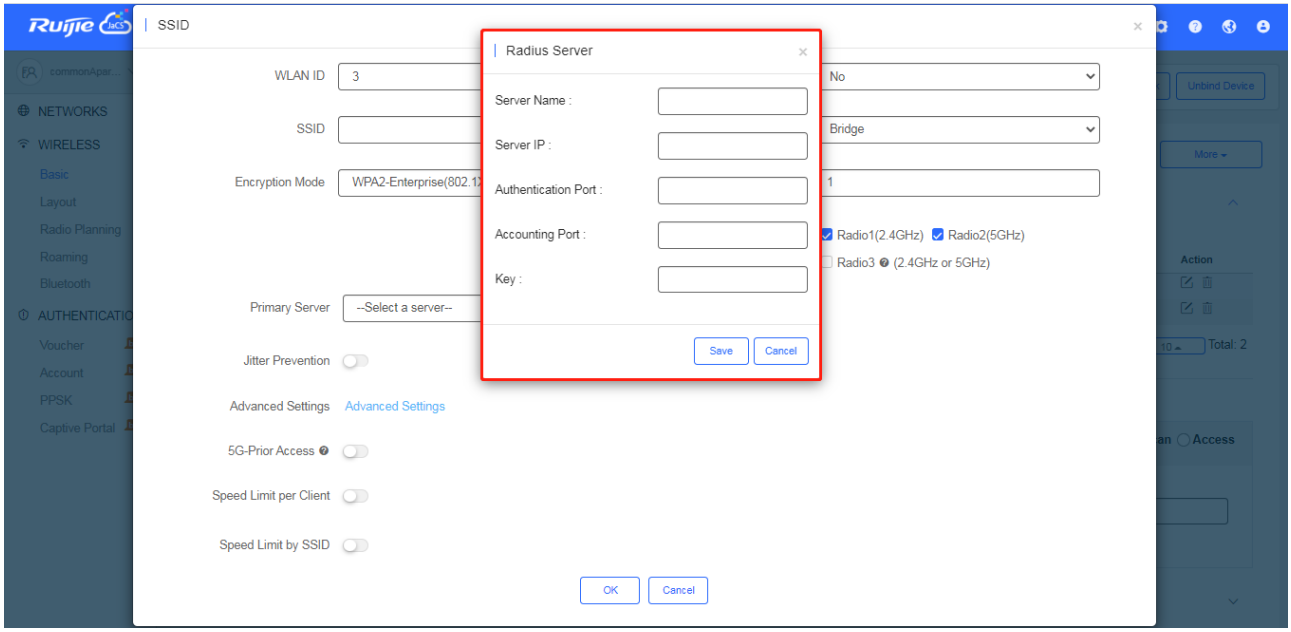
SSID: Enter an SSID name.

Encryption Mode: Open, **WPA-PSK**, **WPA2-PSK**, **WPA/WPA2-PSK**, **WPA2-ENTERPRISE (802.1X)**, **WPA3-PERSONAL, WPA2/WPA3-PERSONAL** 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.



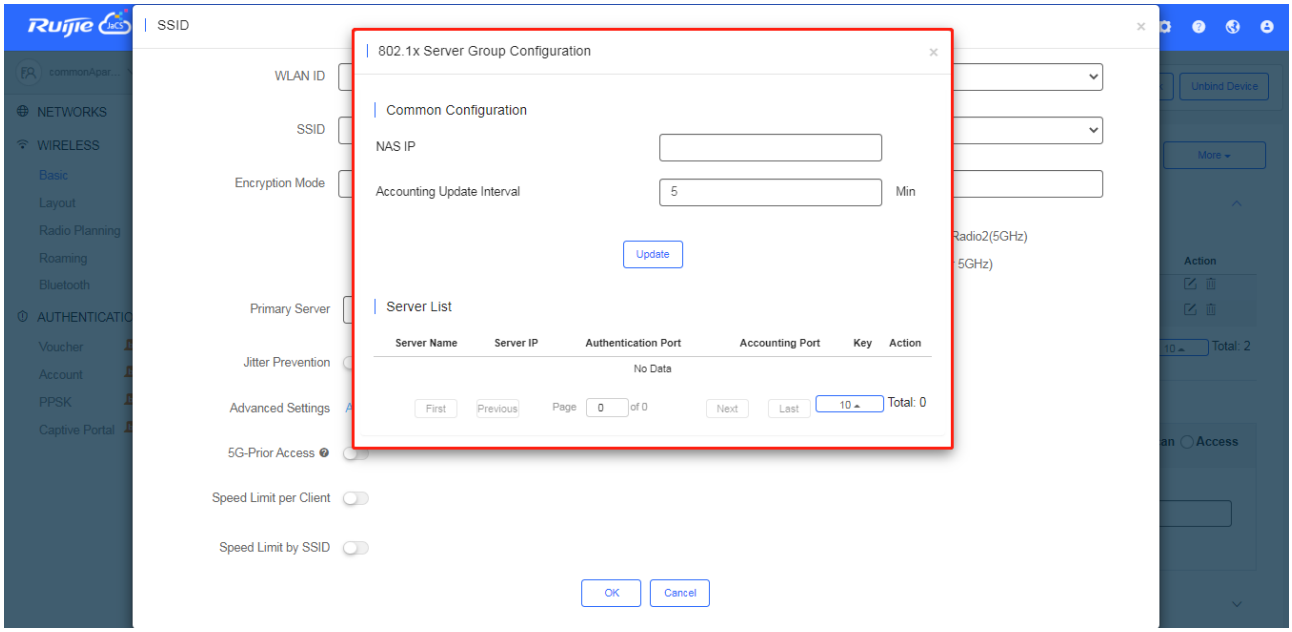
Click ⊕ to add an authentication server. A dialog box for a Radius server configuration is displayed, as shown in the following figure.



Server Name, **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.

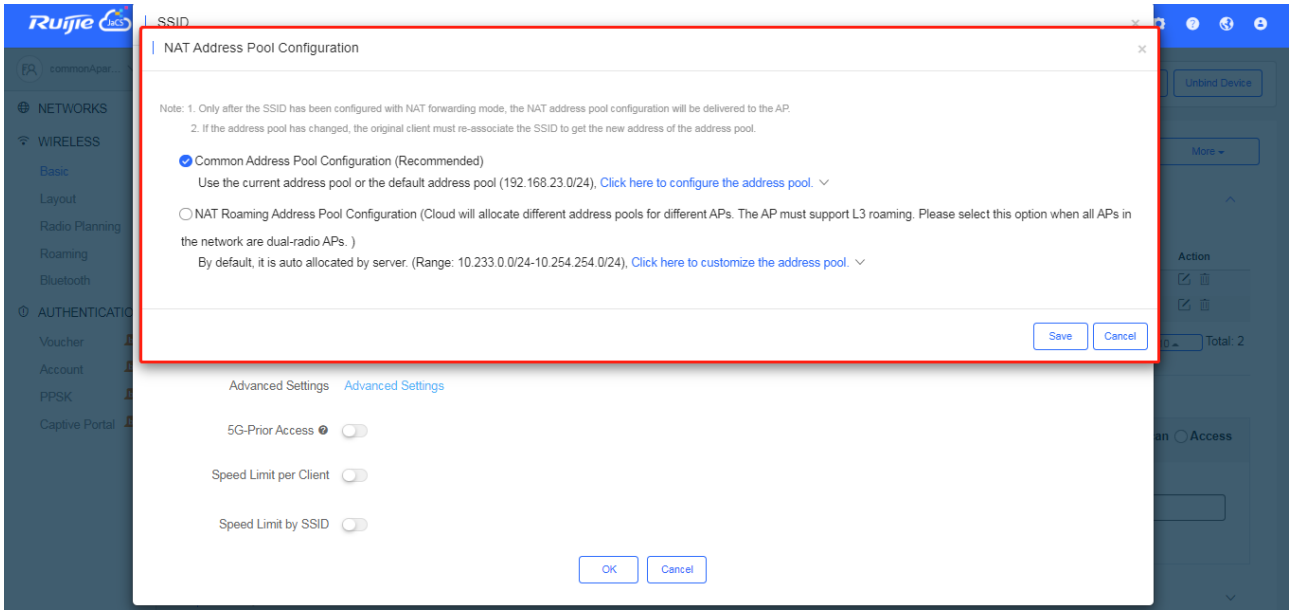
In addition, the **Advanced Settings** function is provided for 802.1x authentication. In **Advanced Settings**, the NAS IP address (available in the NAT environment) and accounting update period can be configured and the added authentication server can be managed.



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.



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.

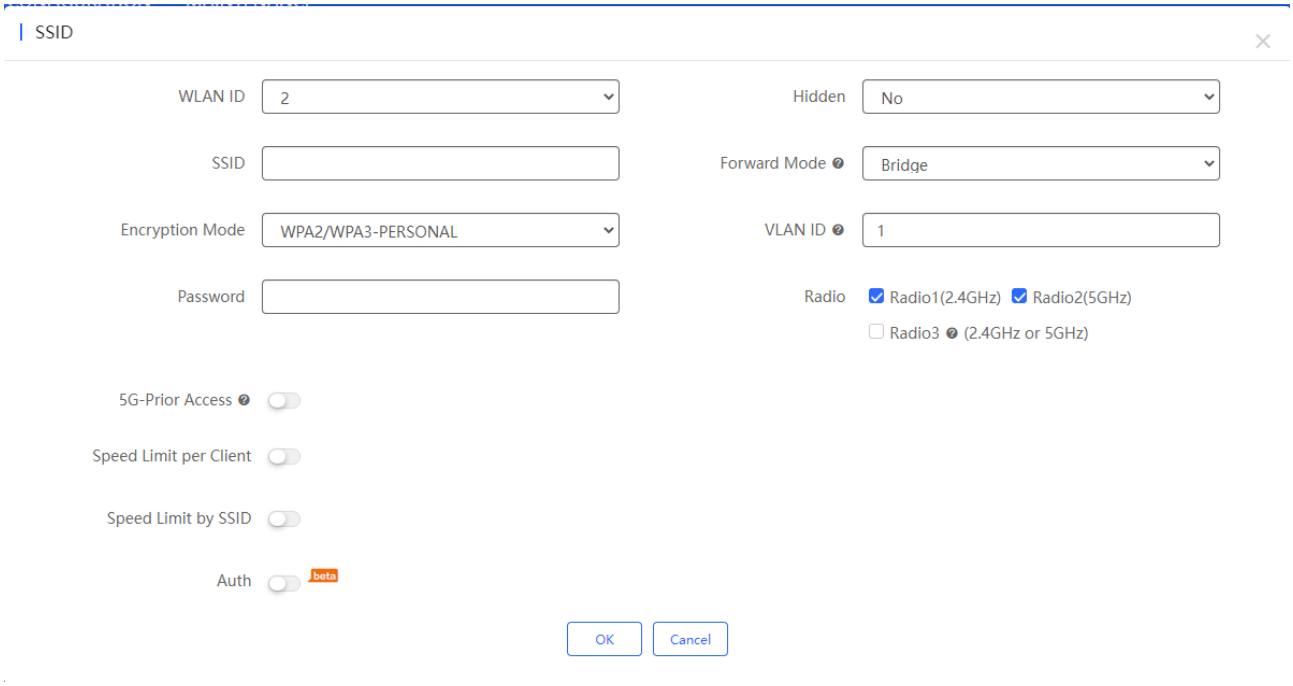
Speed Limit per Client: Specify whether to enable the speed limit function for a client. When this function is enabled, uplink and downlink speeds must be configured.

Speed Limited by SSID: Specify whether to enable the speed limit function for the SSID. When this function is enabled, uplink and downlink speeds must be configured.

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

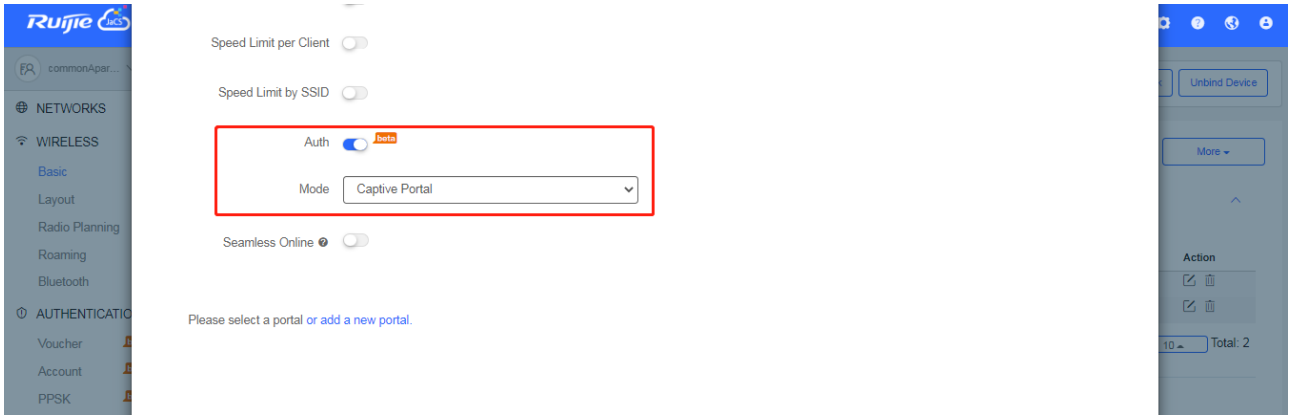
6.2.2.2 External Portal

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

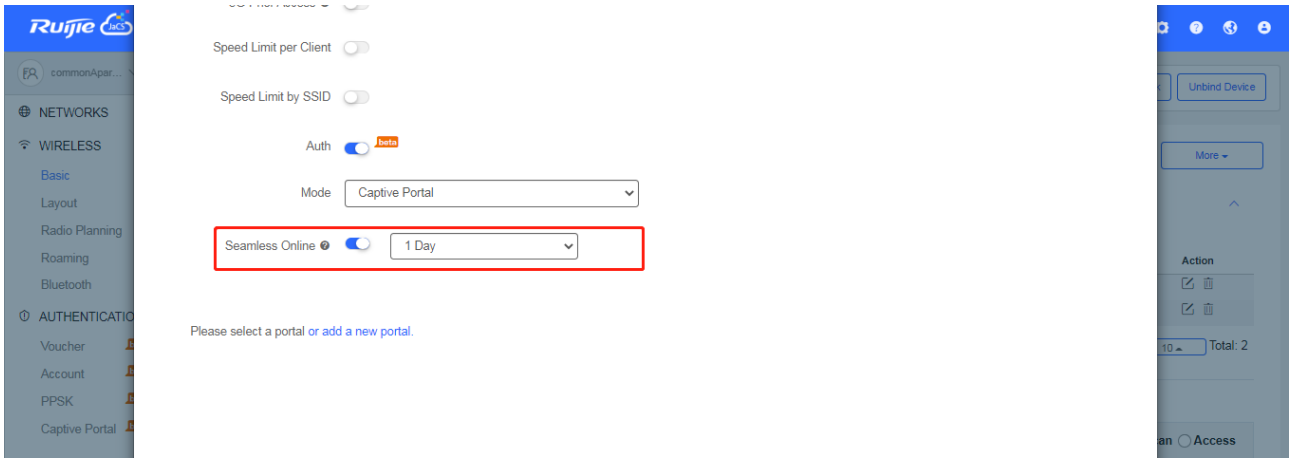


6.2.2.3 Captive Portal

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

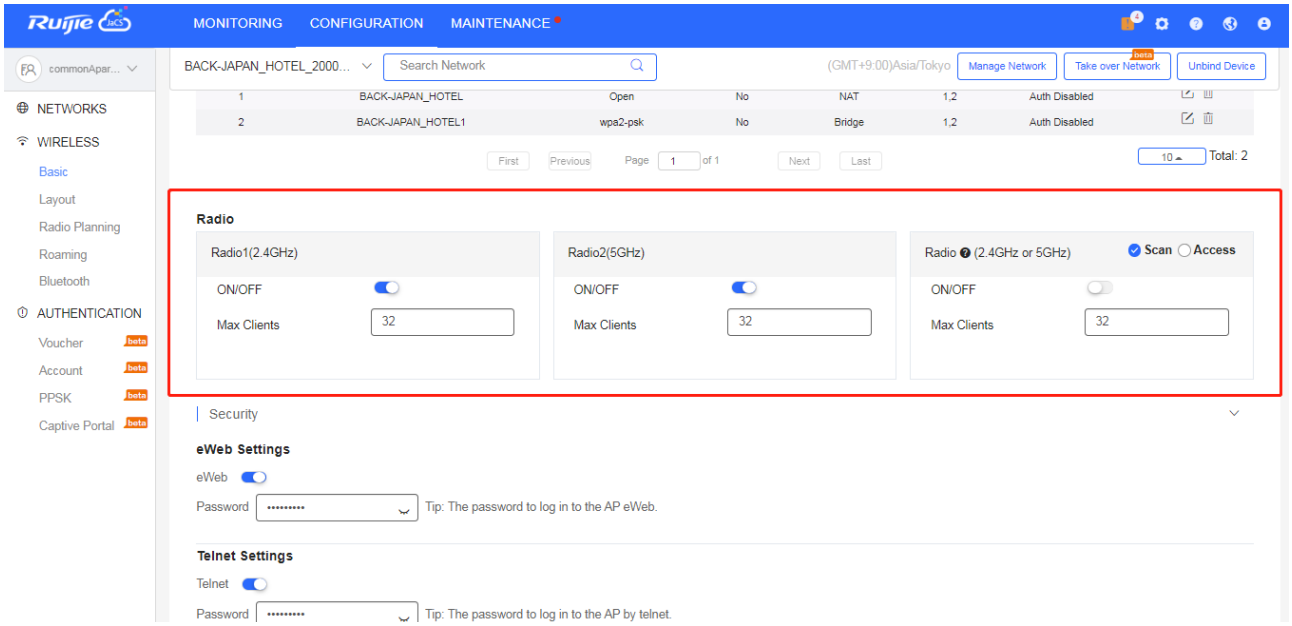


Step 2: Enable **Seamless Online** and select a portal or add new portal.



6.2.2.4 Radio

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:

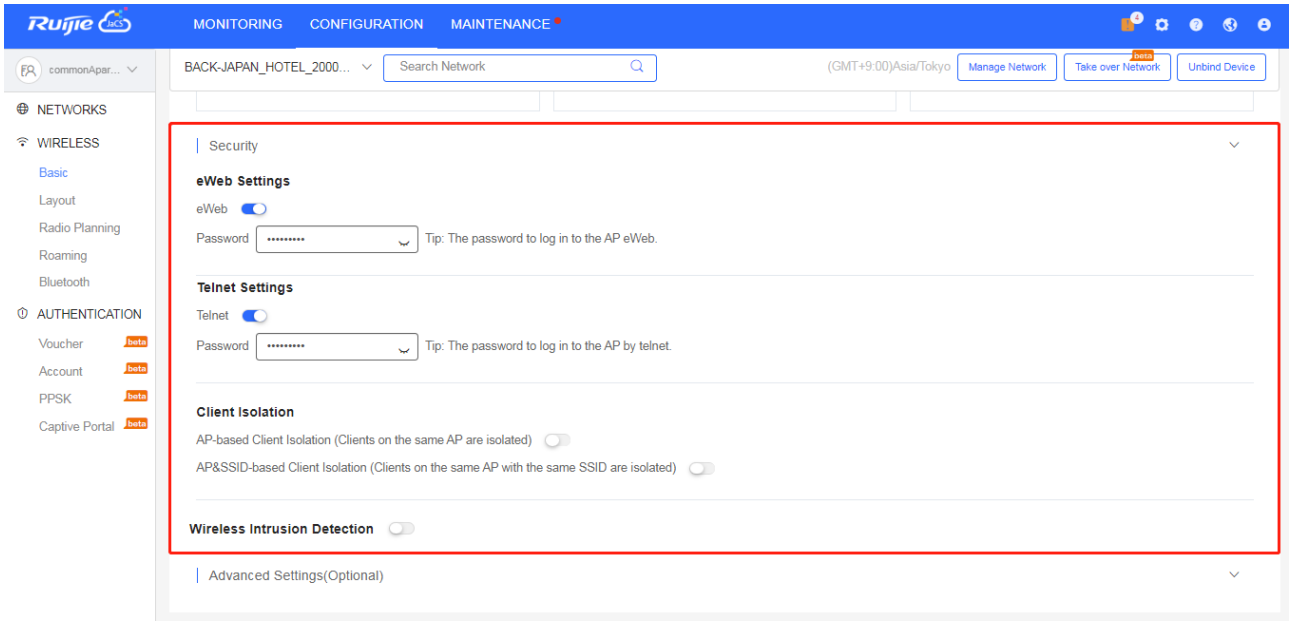
On/Off: Specify whether to enable the radio function. When it is set to **Off**, the SSID is invalid; the corresponding SSID can be used properly only when this function is set to **On**.

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

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.

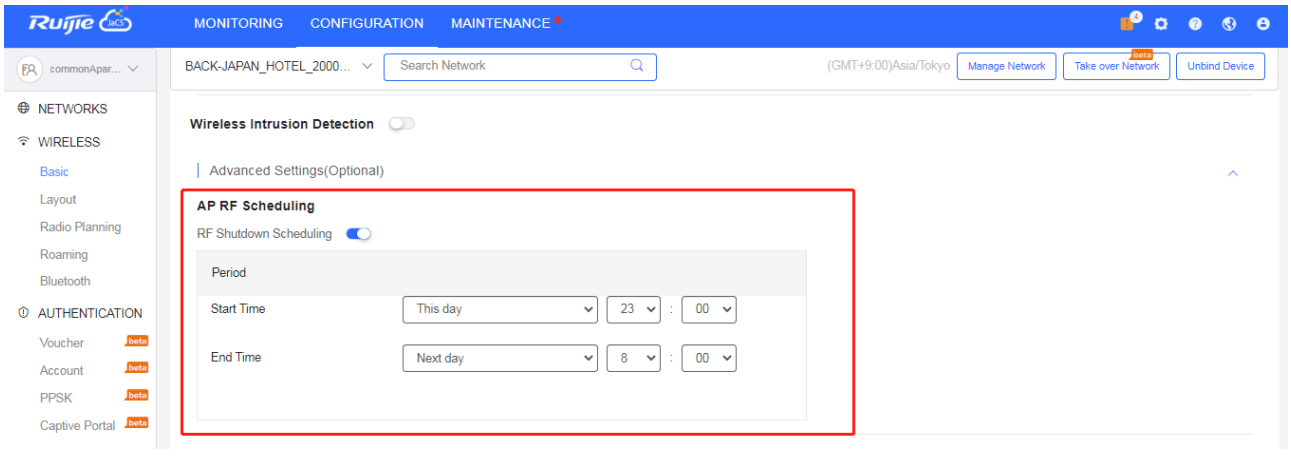
Wireless Intrusion Attack Detection: Include DDOS attack detection, flooding attack detection, AP spoof attack detection, and weak IV attack detection. If this function is enabled, at least one of the preceding four detection functions needs to be enabled.

6.2.2.6 Advanced Settings

- AP RF Scheduling

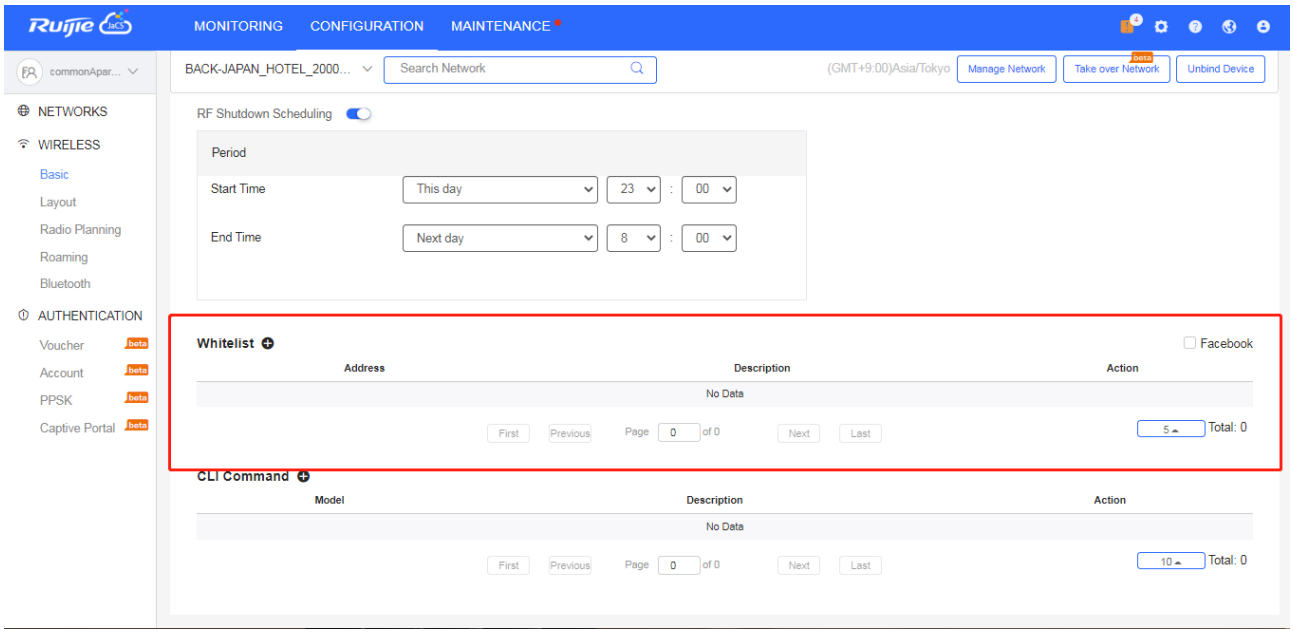
If **AP RF Scheduling** is disabled, AP will broadcast the SSID.

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



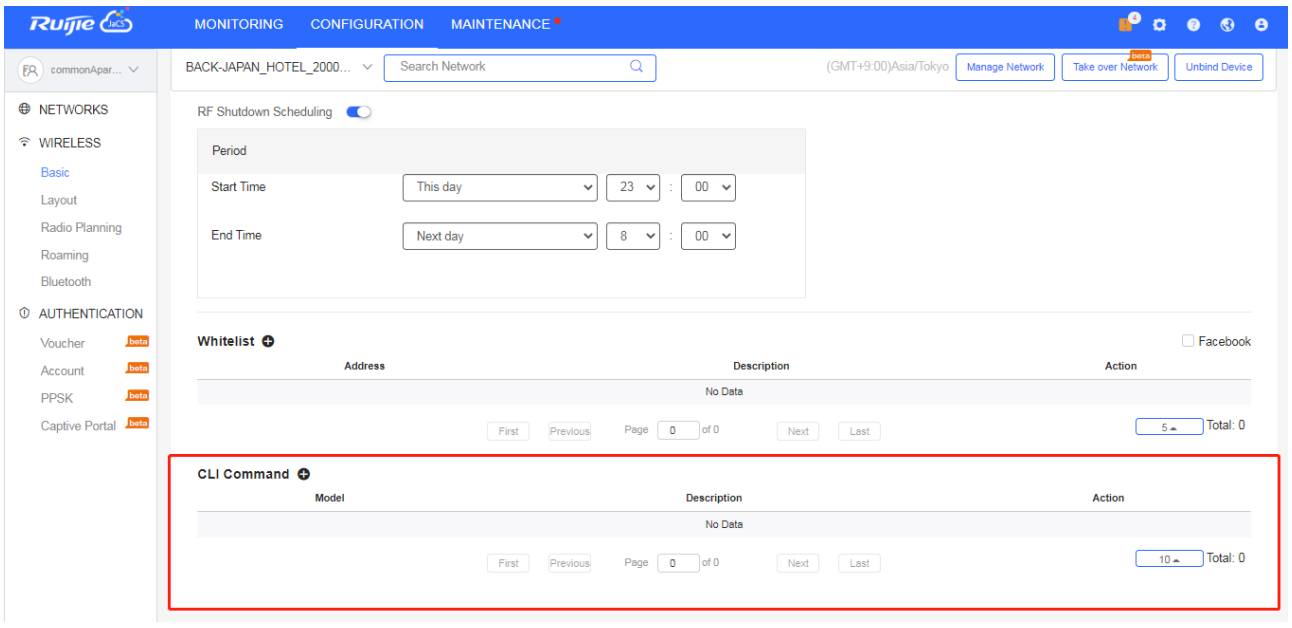
- Whitelist

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.

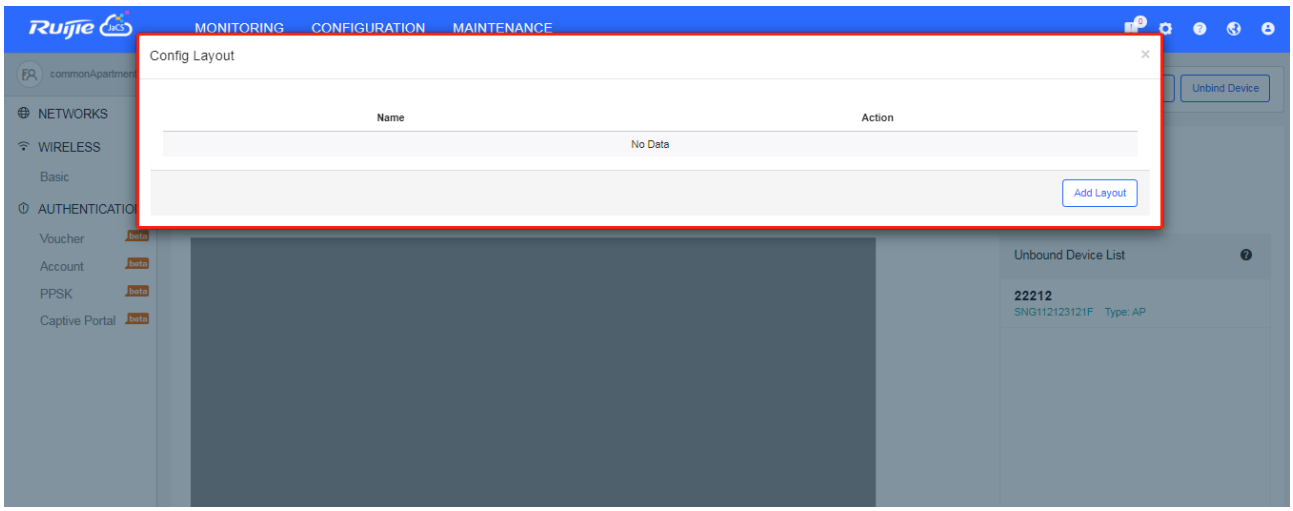


6.2.3 Layout (Non-apartment Scenario)

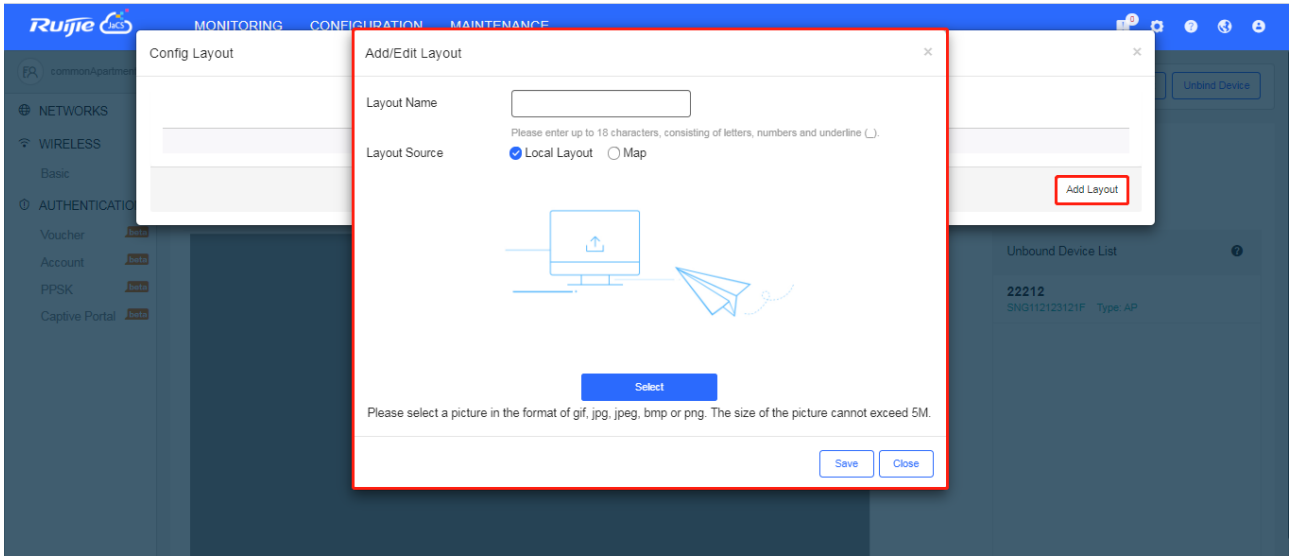
On the Layout page, you can bind an AP to a specific location after importing it to a network.

Step 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.



Step 2: 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.



Step 3: 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:

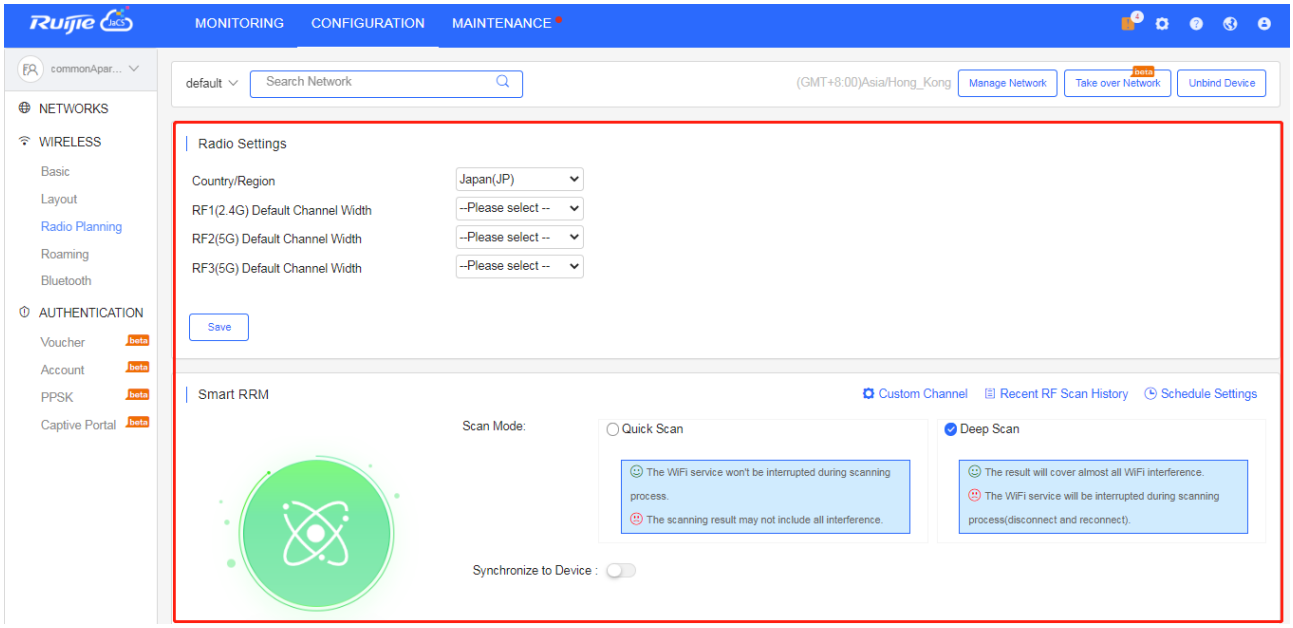
Method 1: Select an AP, and click Remove Device to unbind the AP from a location. An unbound AP will then be moved from a network to its parent network.

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)

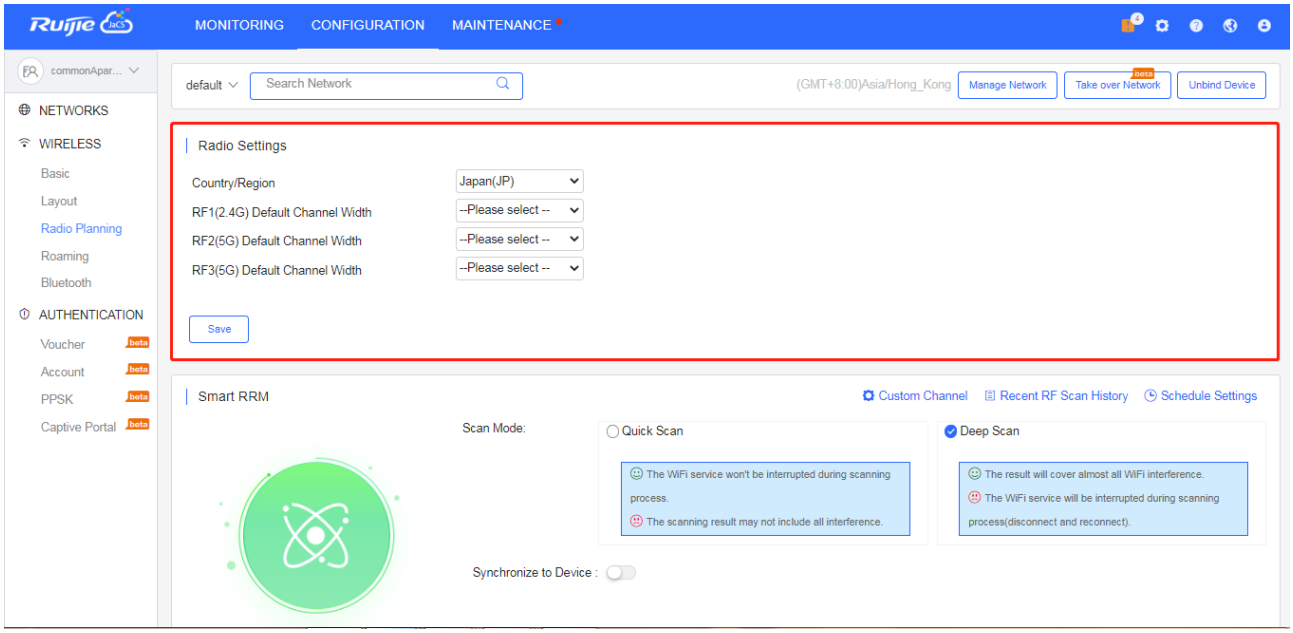
Radio planning can adjust channels and power of APs in a same area network to optimize the channel allocation and power of the APs. Proper RF configuration planning can reduce channel interference, increase channel utilization and improve overall wireless network performance and capacity.

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 Automatic RF Planning

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.

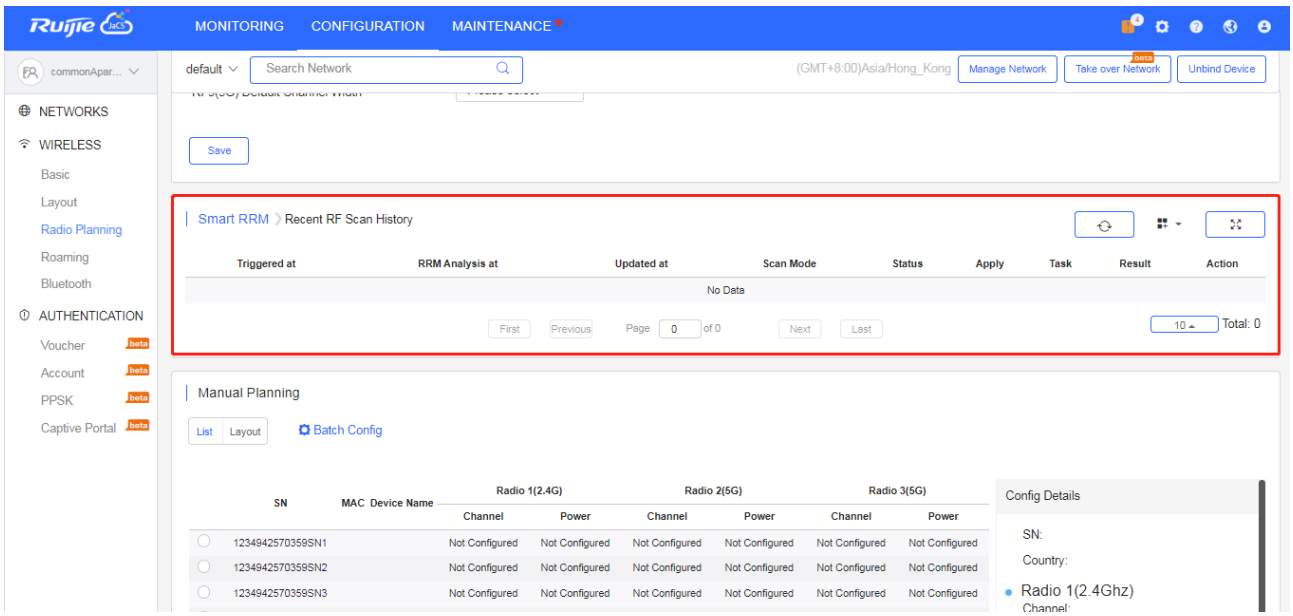
The entire process of the automatic RF planning includes three parts:

- The cloud triggers APs to scan and upload RF information.
- The cloud calculates the optimal recommended configurations.
- The optimal recommended configurations are applied to the APs.

The automatic RF planning supports network-based planning only.

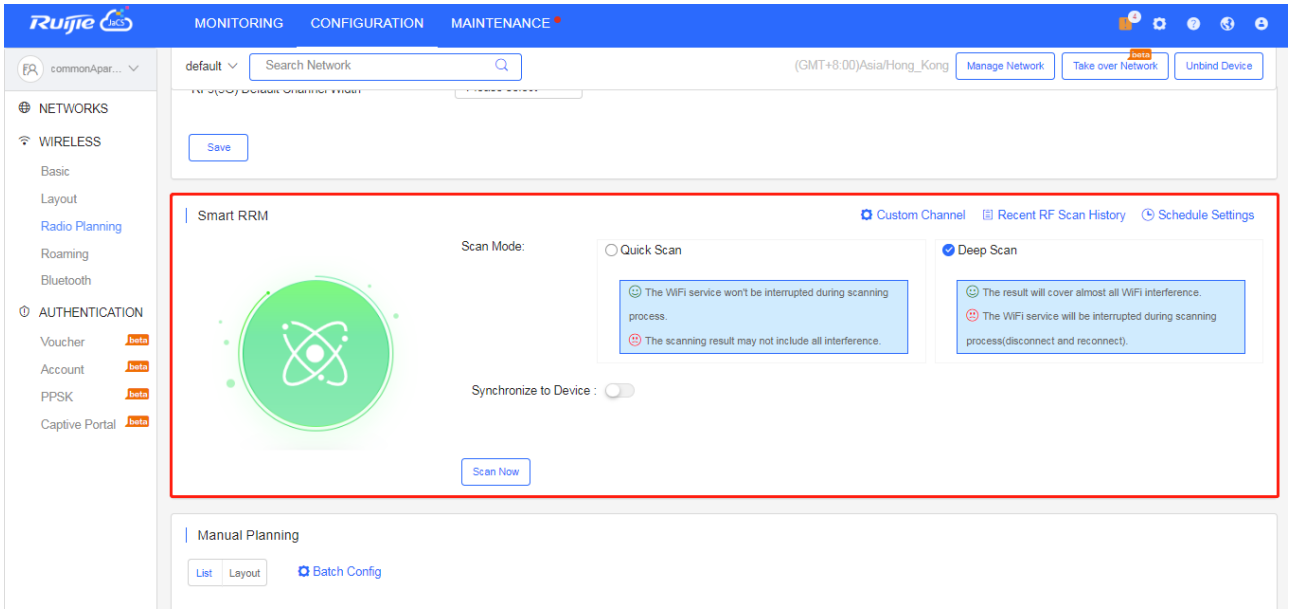
The AP RF channel optimization algorithm staggers RF channels of neighboring APs respectively based on the 2.4 GHz frequency band and the 5 GHz frequency band while ensuring as much as possible that original configurations are unchanged. To reach optimal power, The AP power optimization algorithm automatically 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.

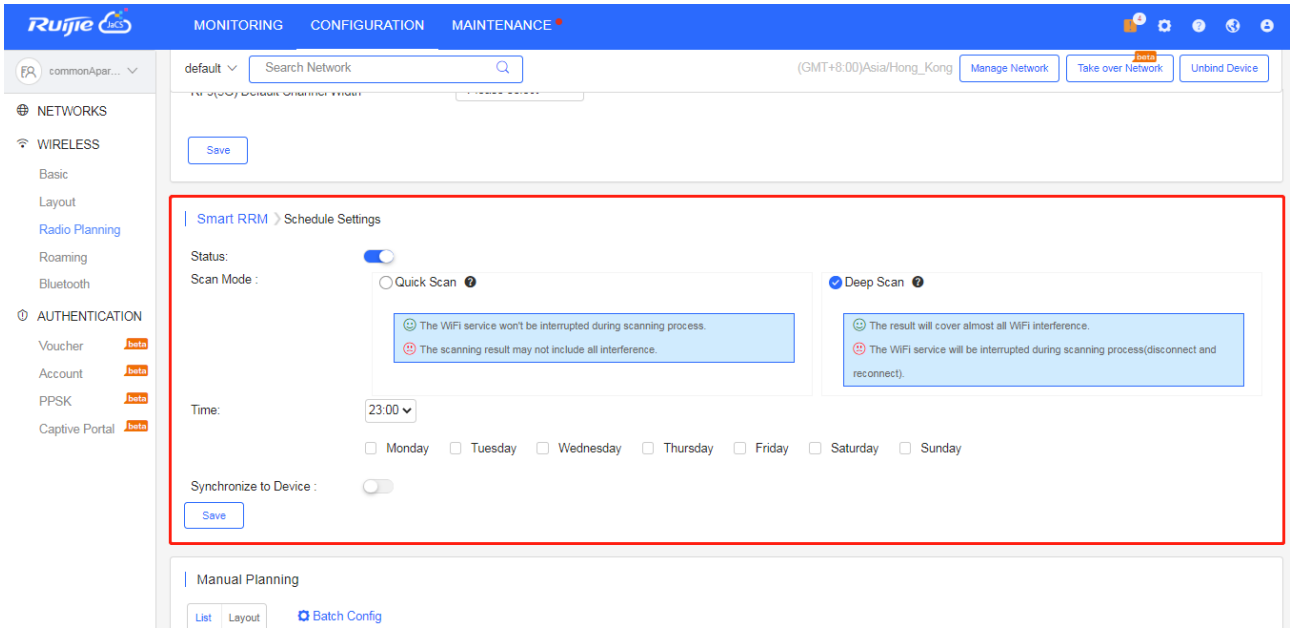
- Smart RRM



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

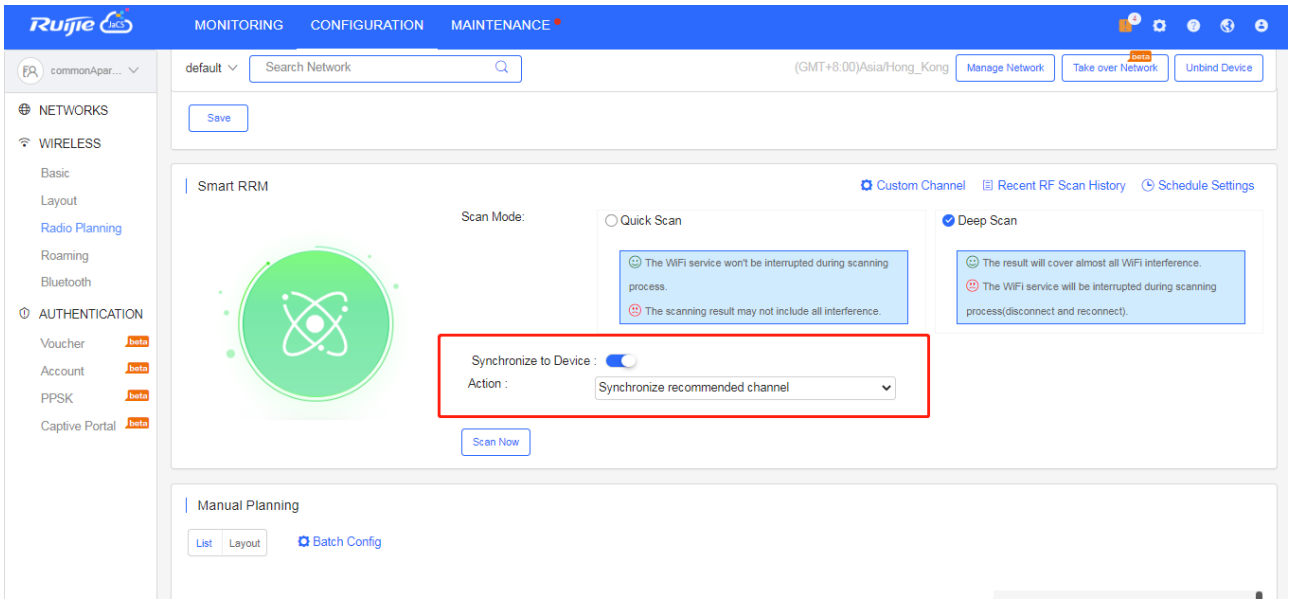
(1) Scan Mode

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

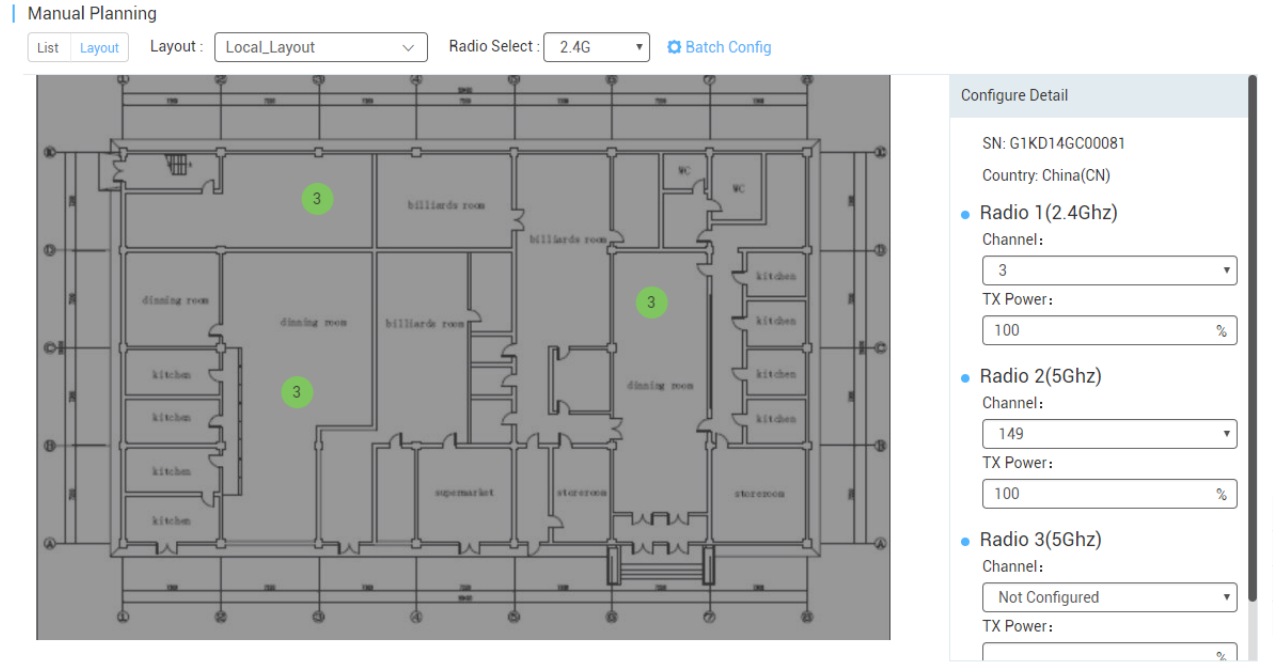
If this function is enabled, the RF scanning result will be automatically pushed to the AP. In this case, skip step 3.



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.



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

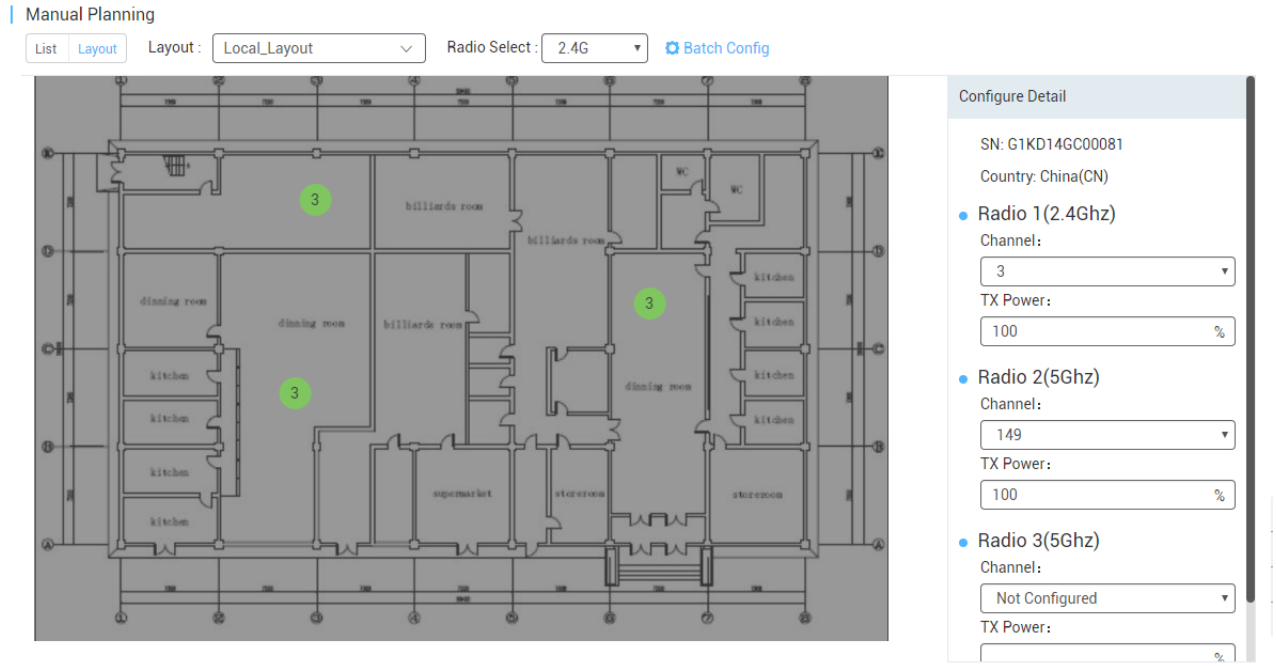
You can click a location icon to display the RF channel and power configurations on the right. If the location is bound to an AP, the SN of the bound AP is also displayed.

To perform manual RF planning:

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

- Configure one location

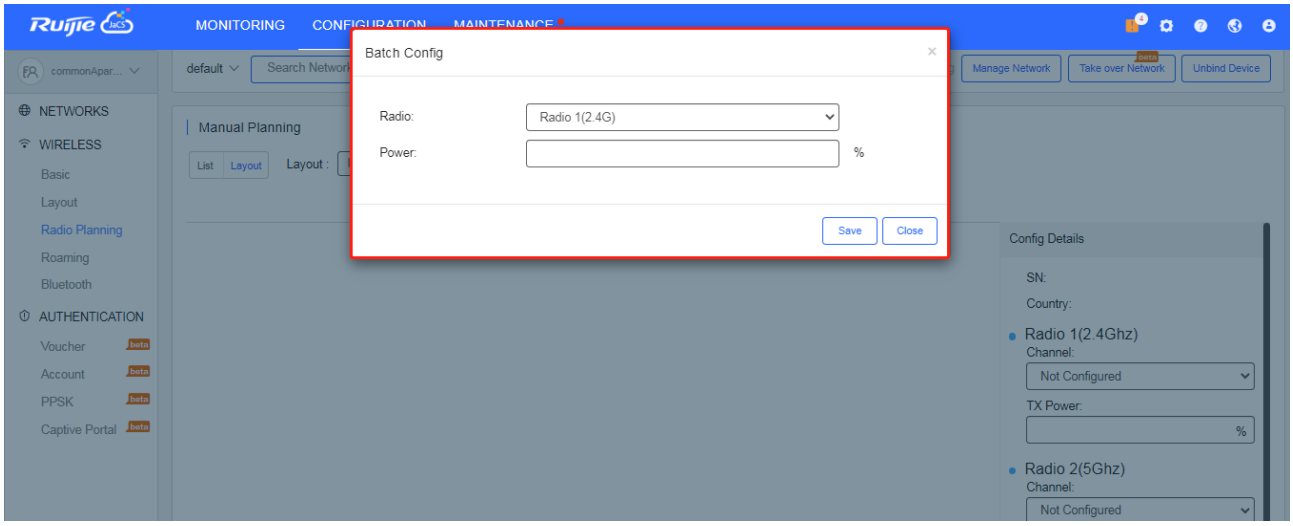
Click a location icon, enter configurations on the right, and click **Apply**.



- 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.

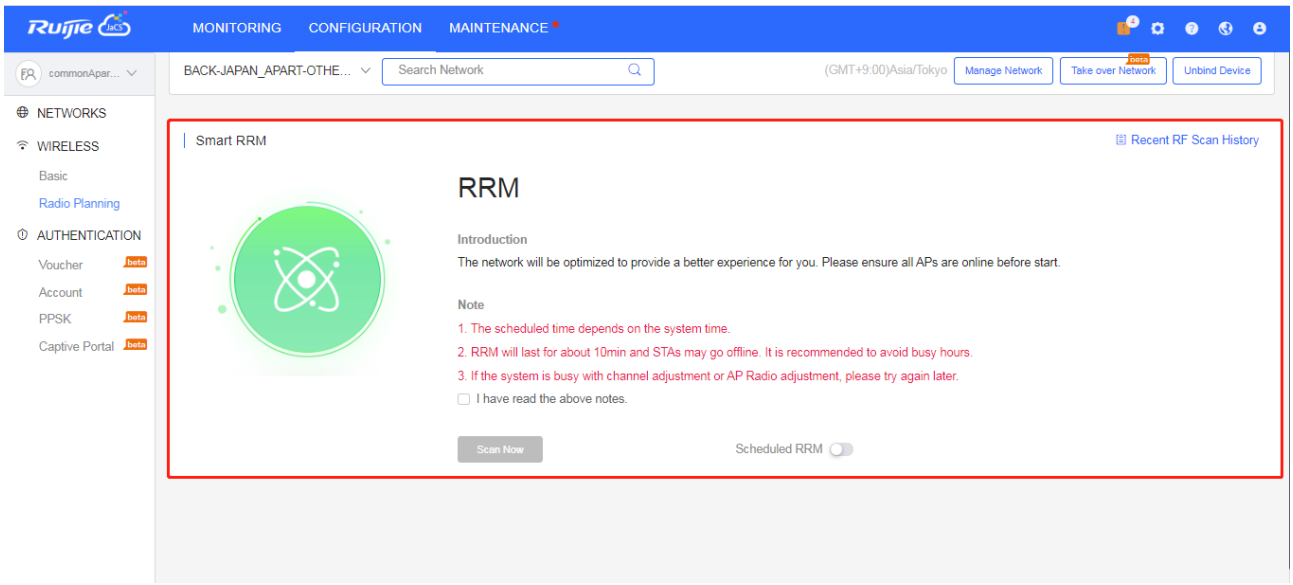
Batch operations for multiple locations can be select before clicking Apply .

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.

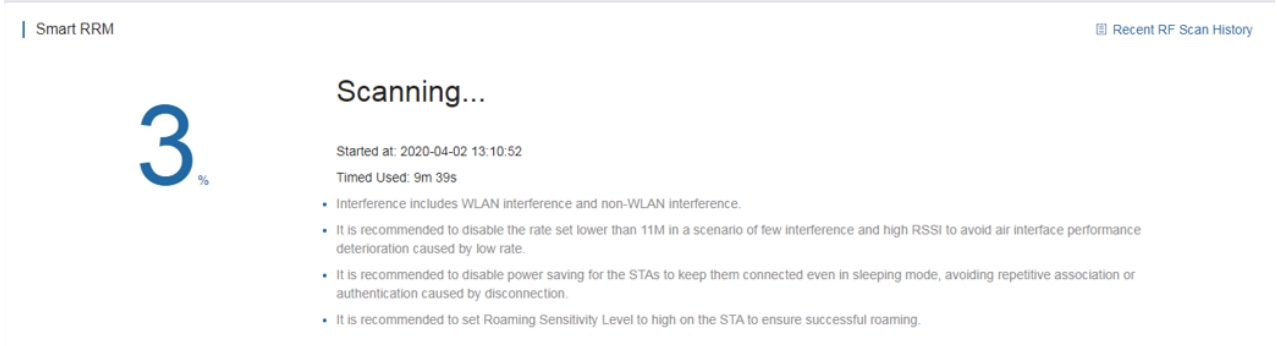
If an unbind or bind operation is performed, RF configurations are removed from or synchronized to the AP.

6.2.4.4 AC Smart RRM

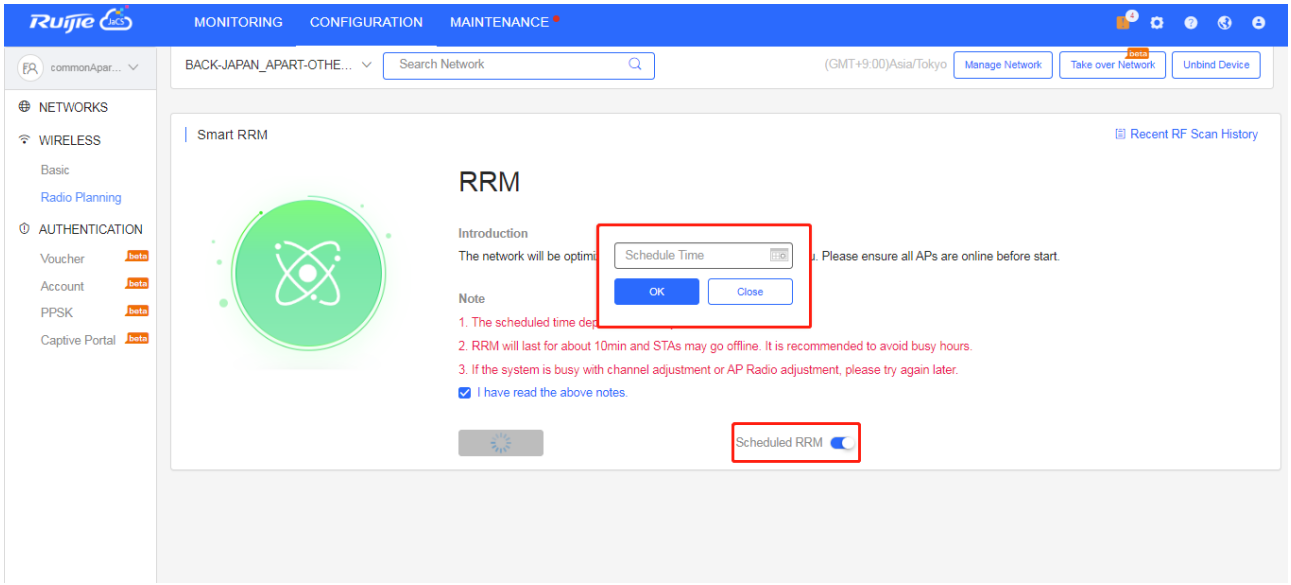
In the AC network, click **Radio Planning** to open the **Smart RRM** page.



Check the note, click Scan Now 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.

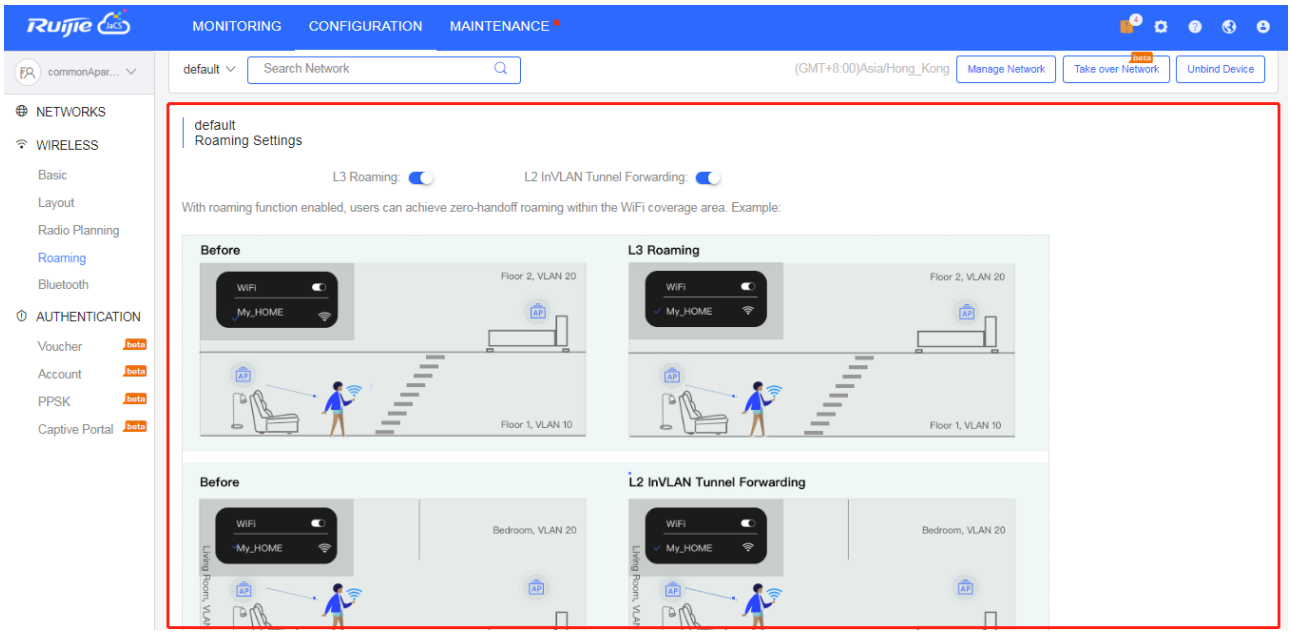


6.2.5 Roaming (Non-apartment Scenario)

Roaming planning refers to enabling network-based roaming.

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

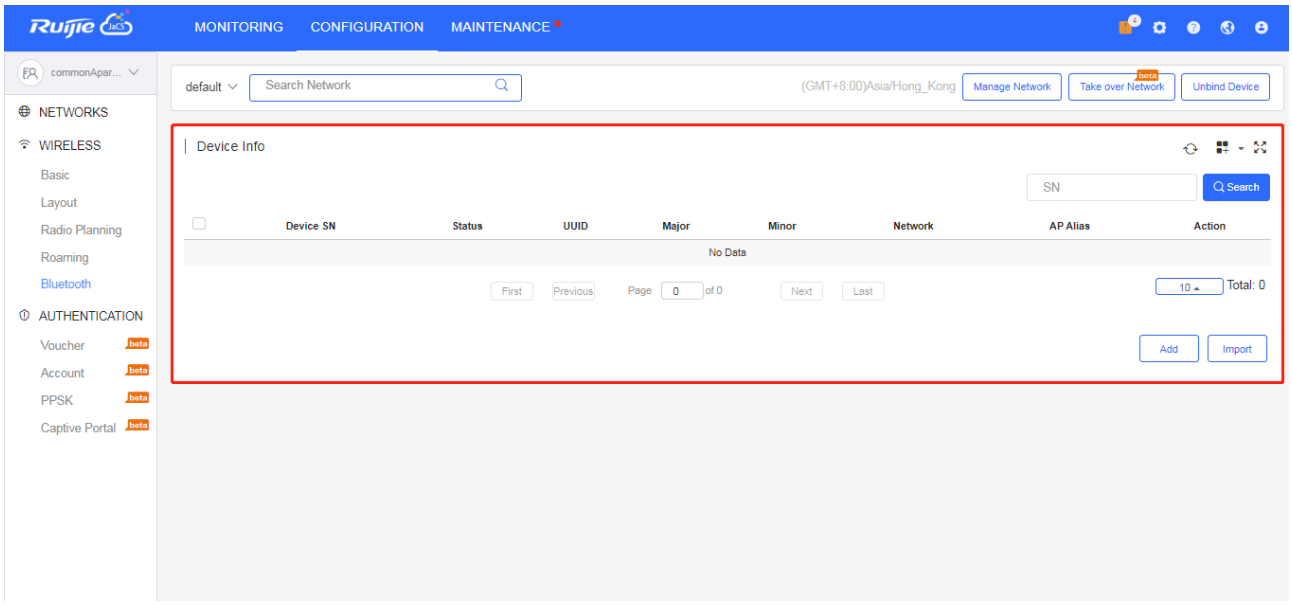
L2 InVLAN Tunnel Forwarding: Specify whether to enable Layer2 Roaming. It is enabled by default.



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

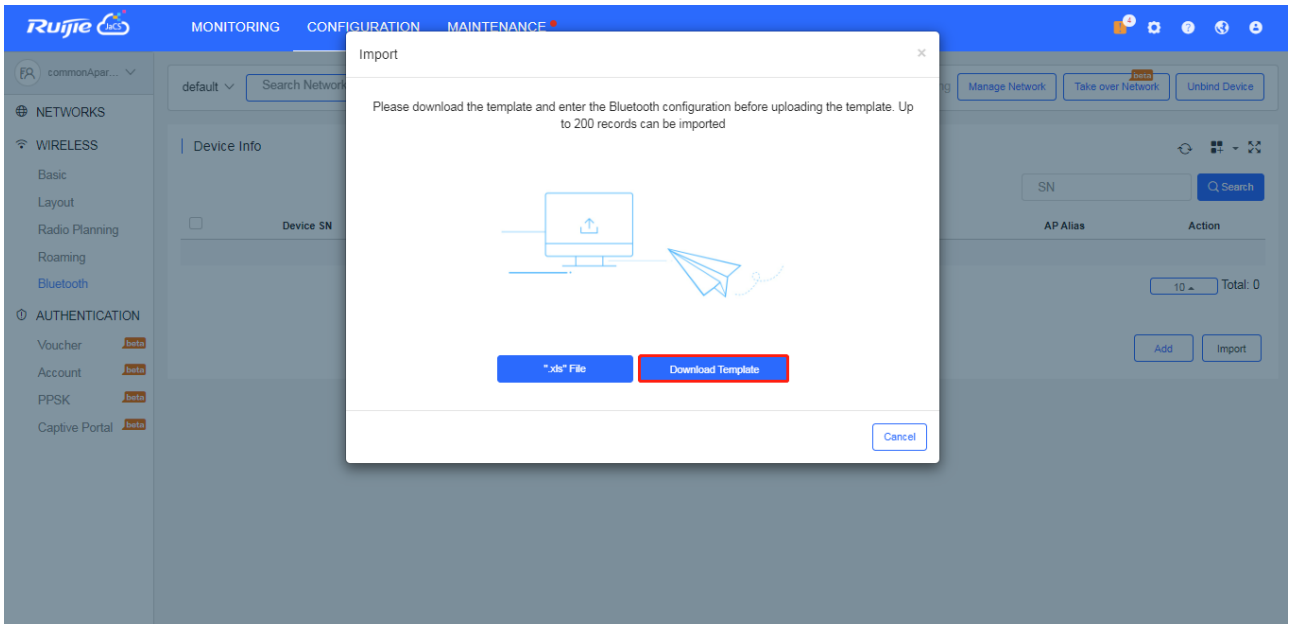
6.2.6 Bluetooth (Non-apartment Scenario)

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.

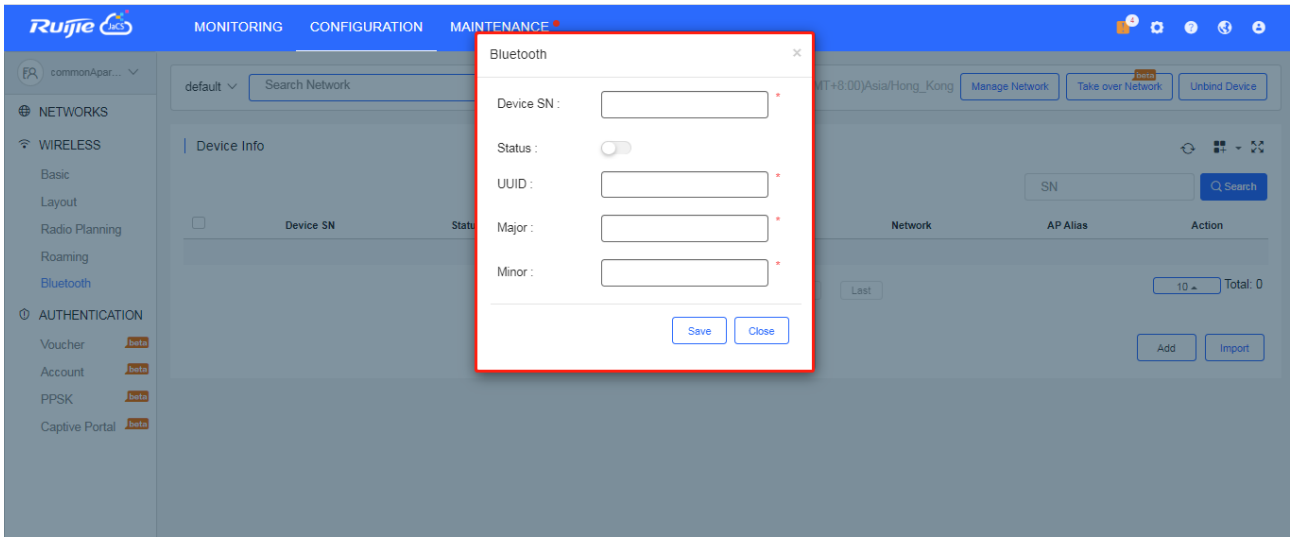
Major: Enter a string of 4 characters in hexadecimal format.

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

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

Click **Add**. The Bluetooth dialog box is displayed, as shown in the following 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 Authentication

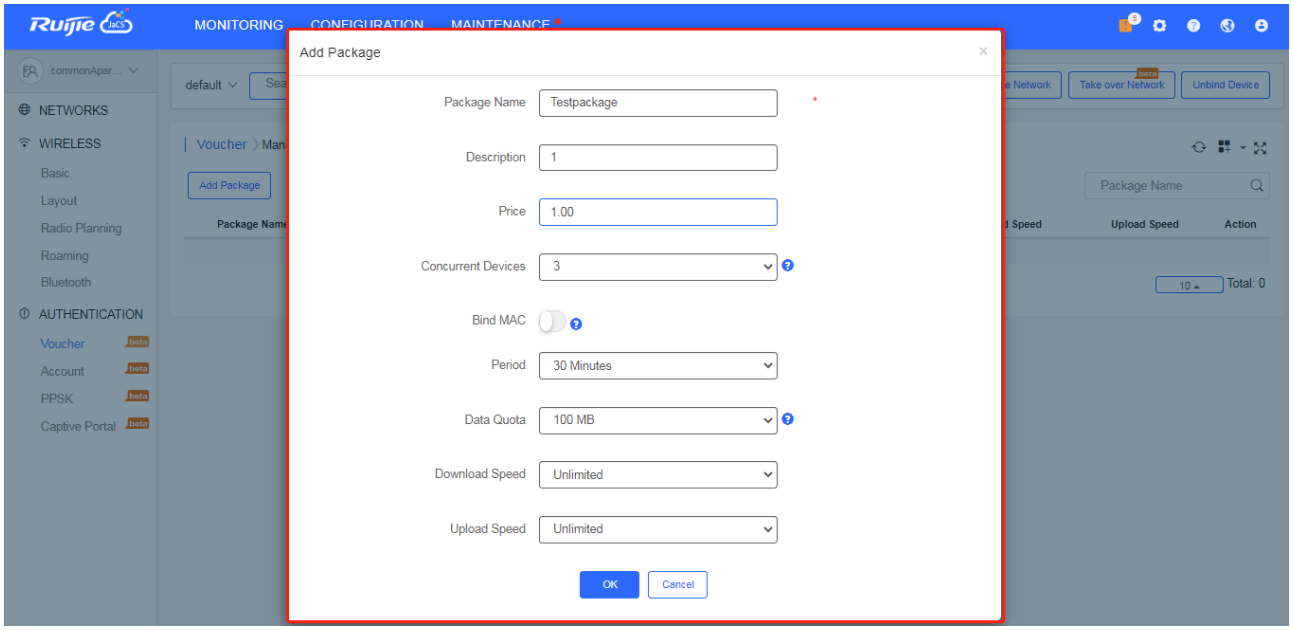
Voucher authentication on Ruijie JaCS allows you to charge users for wireless network access using access codes. Concurrent users, time period and data quota limit can be customized and offered to your guests.

6.3.1.1 Configuration Steps

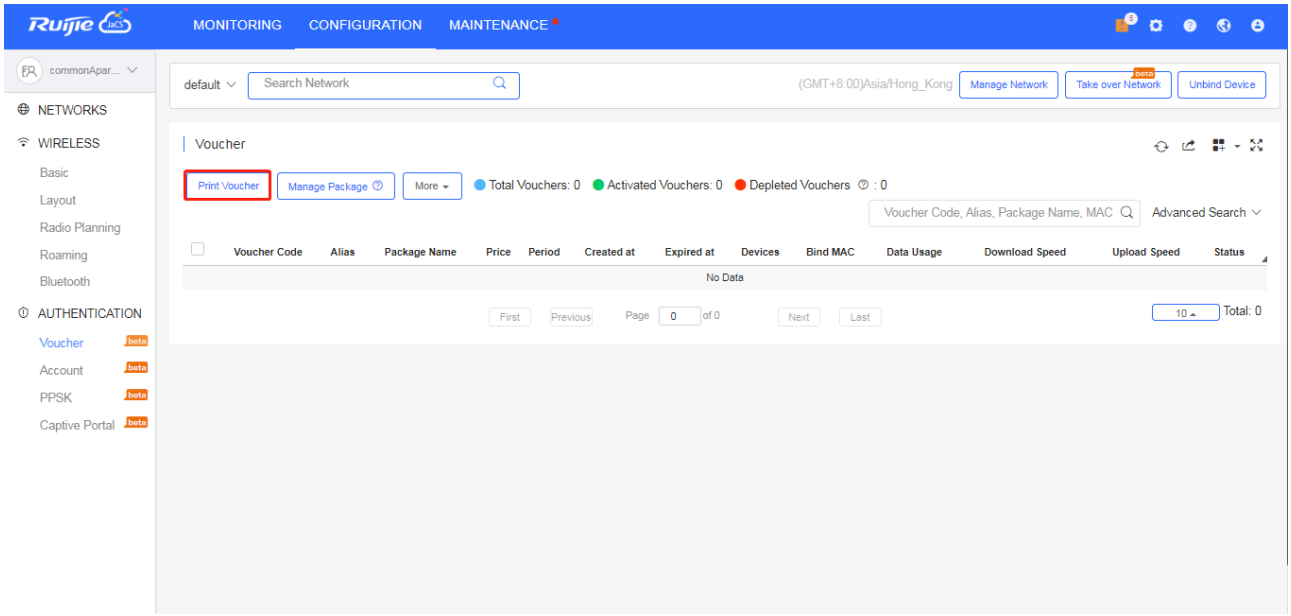
Step 1: Enable **Voucher** function in the **Captive Portal** mode of **SSID** under the corresponding network.

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

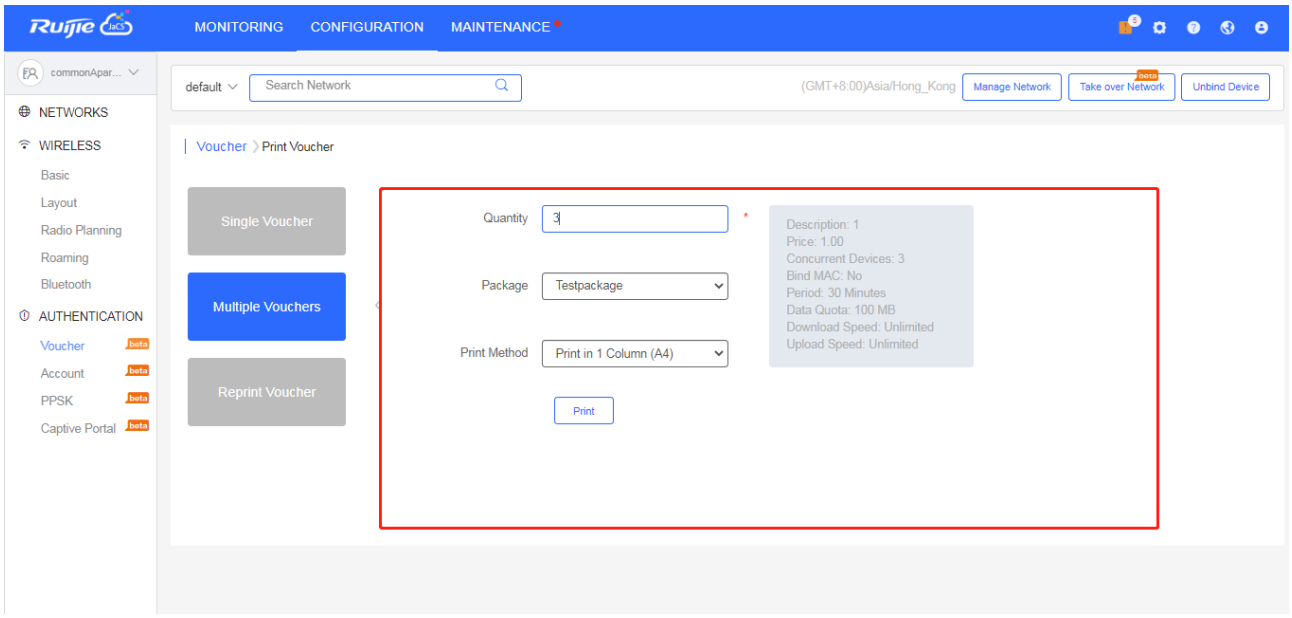
Step 3: Select **Manage Package > Add Package** to define a voucher type for your guests.



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



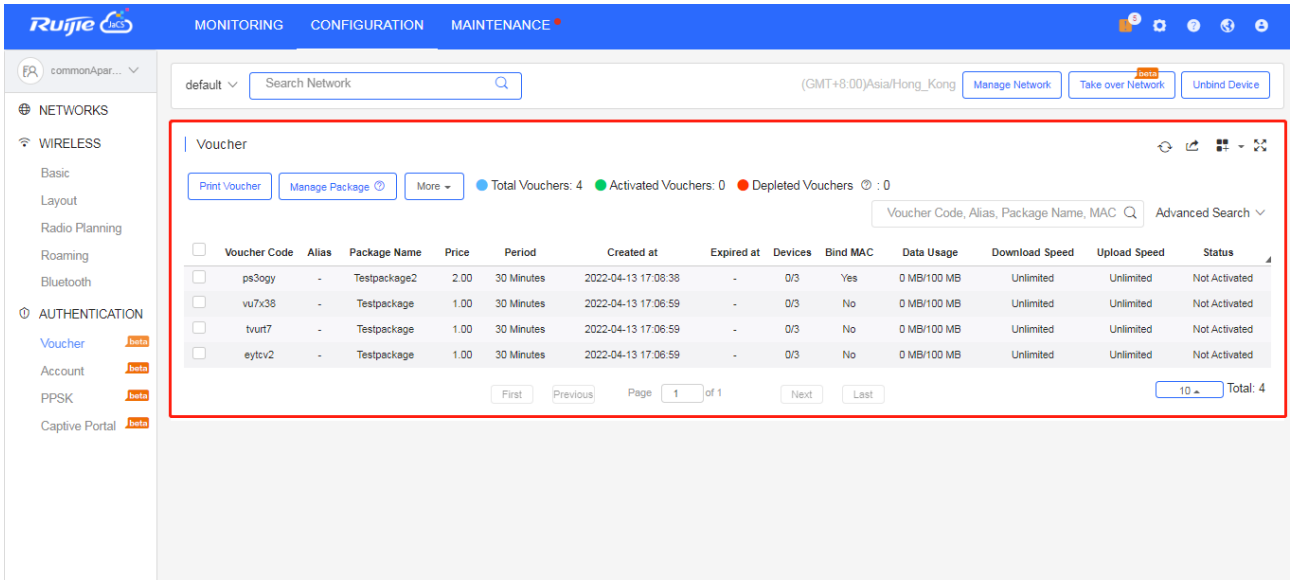
Step 5: Select the way you want to print voucher codes and enter the quantity if you select **Multiple Vouchers**.

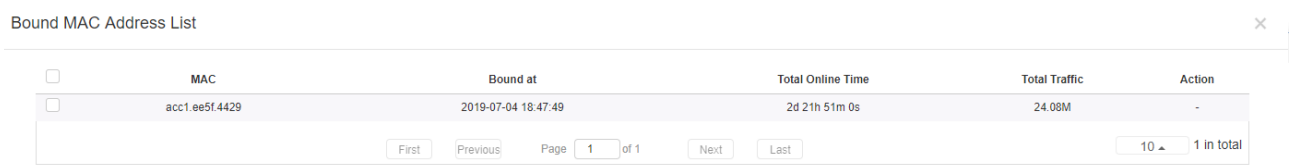


Step 6: Click the **Print** button.

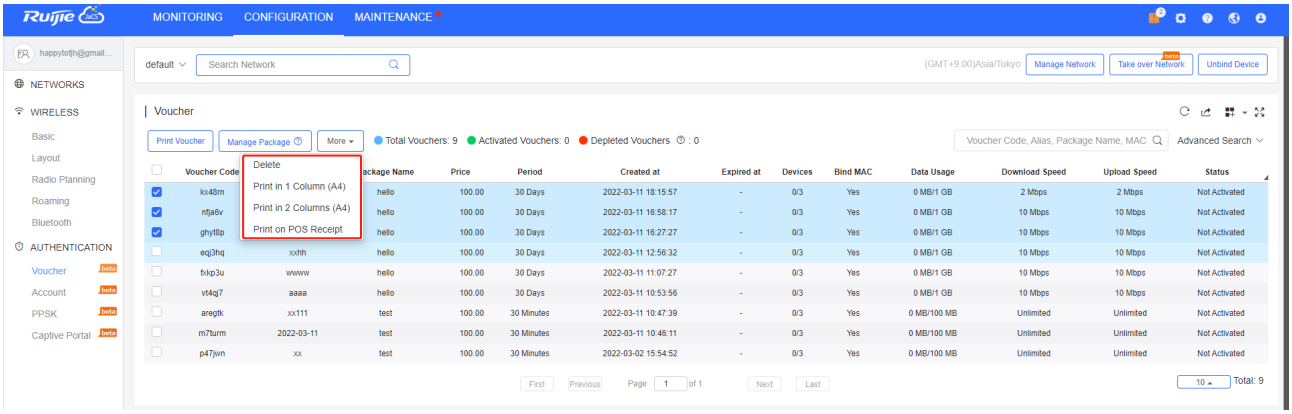
6.3.1.2 Bind/Unbind MAC

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.





6.3.1.3 More



Item	Description
Delete	● Delete the selected Vouchers
● Print in 1 Column(A4)	● Printed Vouchers will be displayed in the same column
● Print in 2 Columns(A4)	● Printed Vouchers will be displayed in two columns
● Print on POS Receipt	● Suitable for printing on POS receipts

6.3.2 Account Authentication

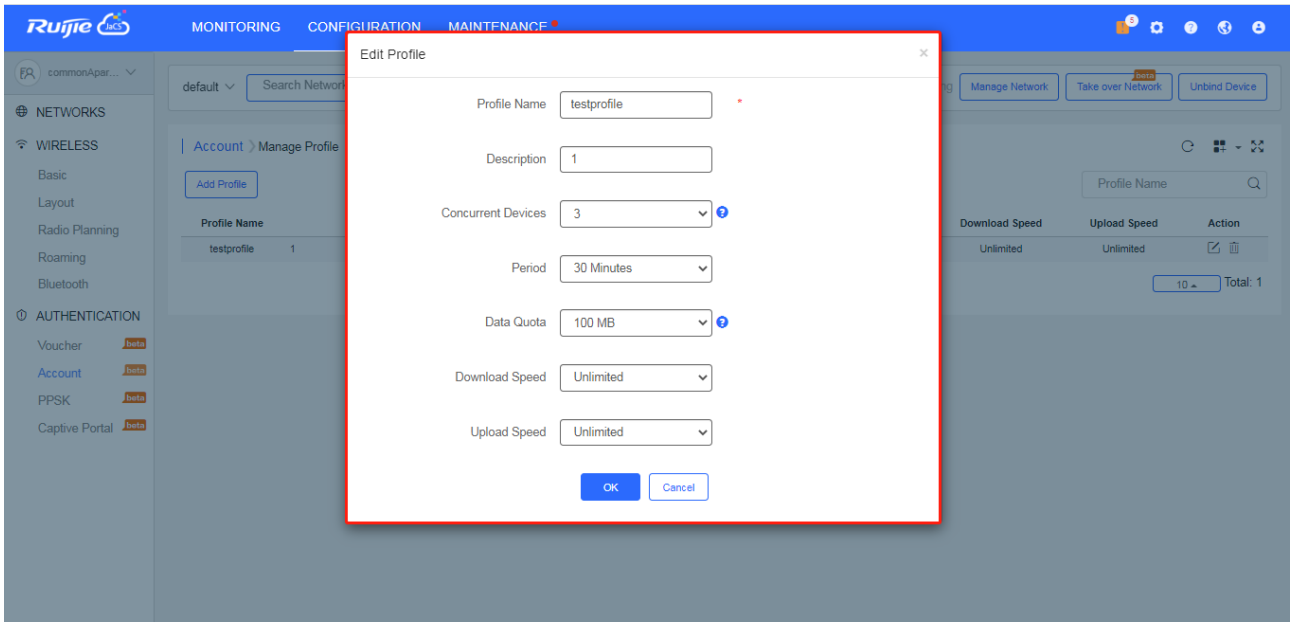
Account authentication requires the valid account and password. Concurrent users, time period and data quota limit can be customized and offered to your guests.

6.3.2.1 Configuration Steps

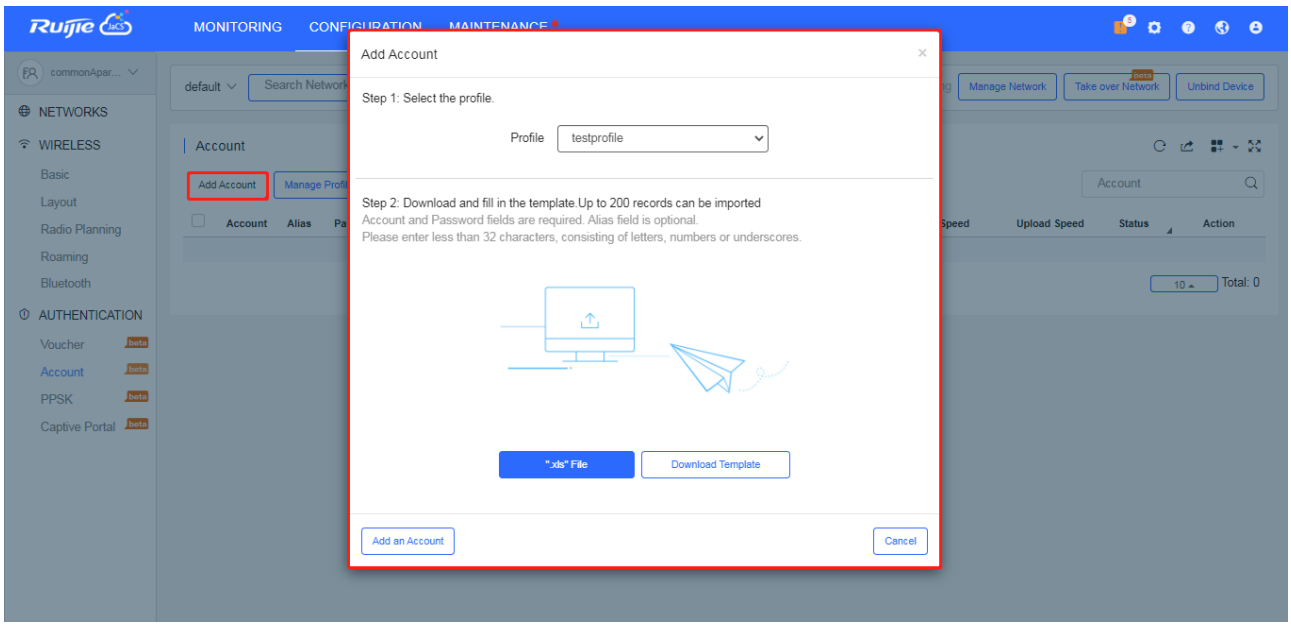
Step 1: Enable **Captive Portal** in the **SSID** page, and select a template with Account Authentication.

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

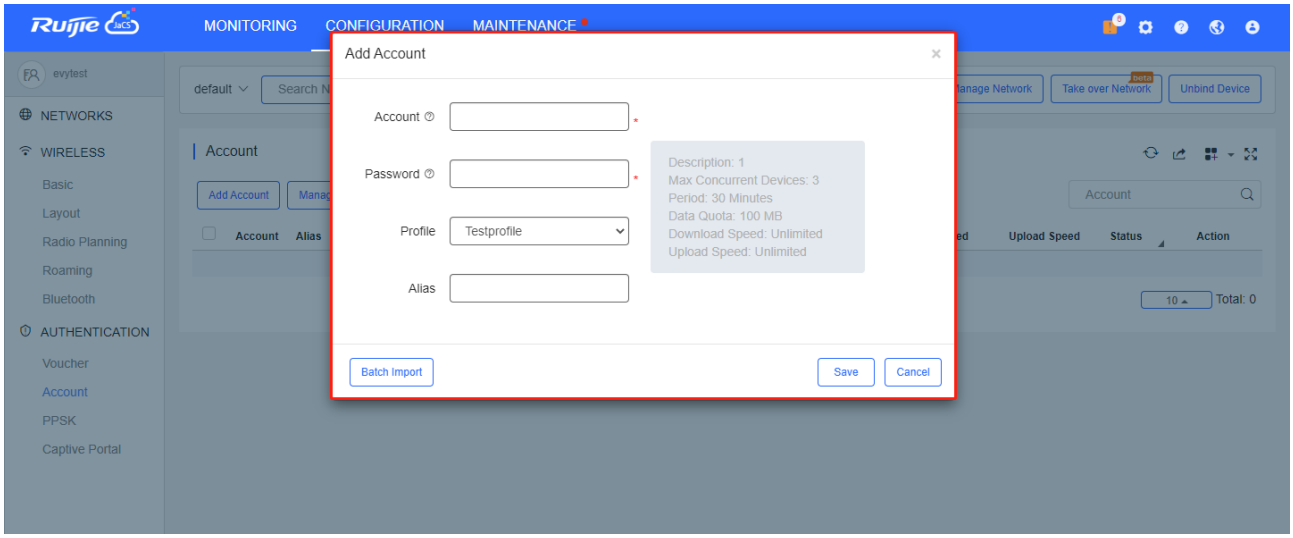
Step 3: Select **Manage Profile > Add Profile** to define an account type for your guests.



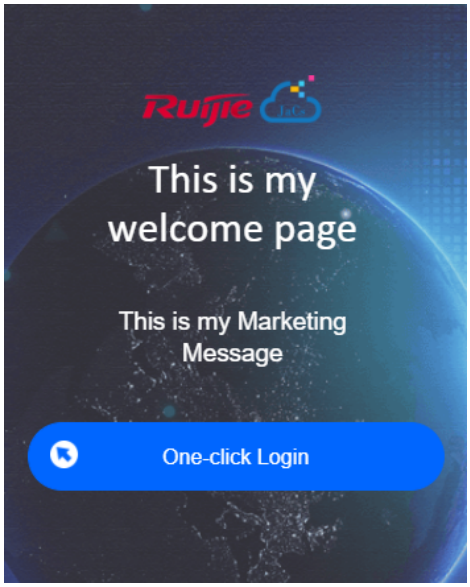
Step 4: Click **OK** and go back to the **Account** page and click **Add Account**.



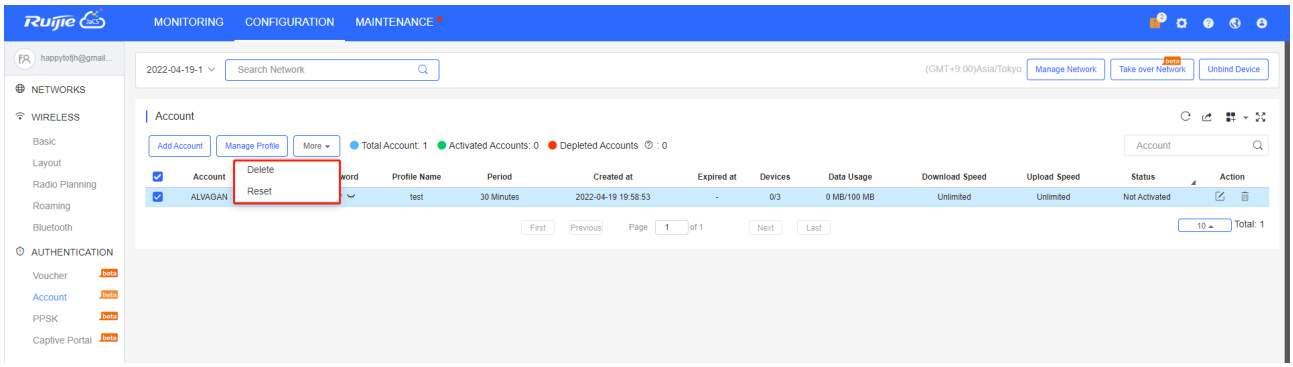
Step 5: Click **Add an Account** to enter the account, password and select the profile, and then click **Save**.



Step 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**.



6.3.2.2 More



Item	Description

Delete	• Delete the selected accounts
• Reset	• Reset the selected accounts

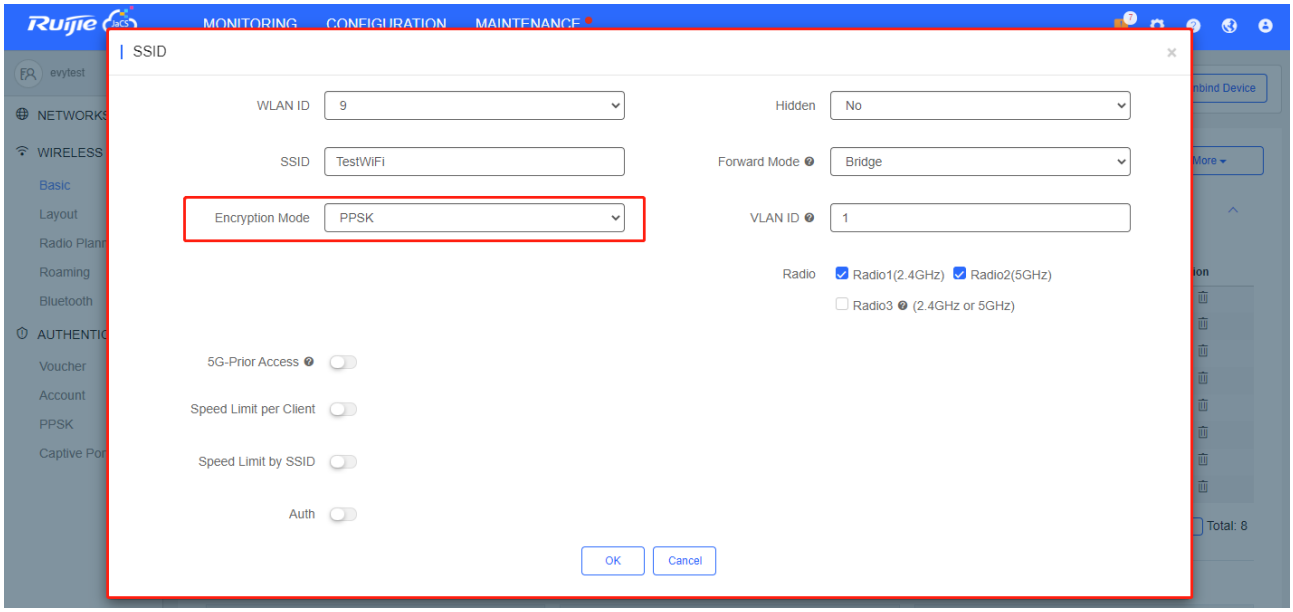
6.3.3 PPSK Authentication

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 JaCS and deploy the network, so that APs can access the Ruijie JaCS.
   - 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.

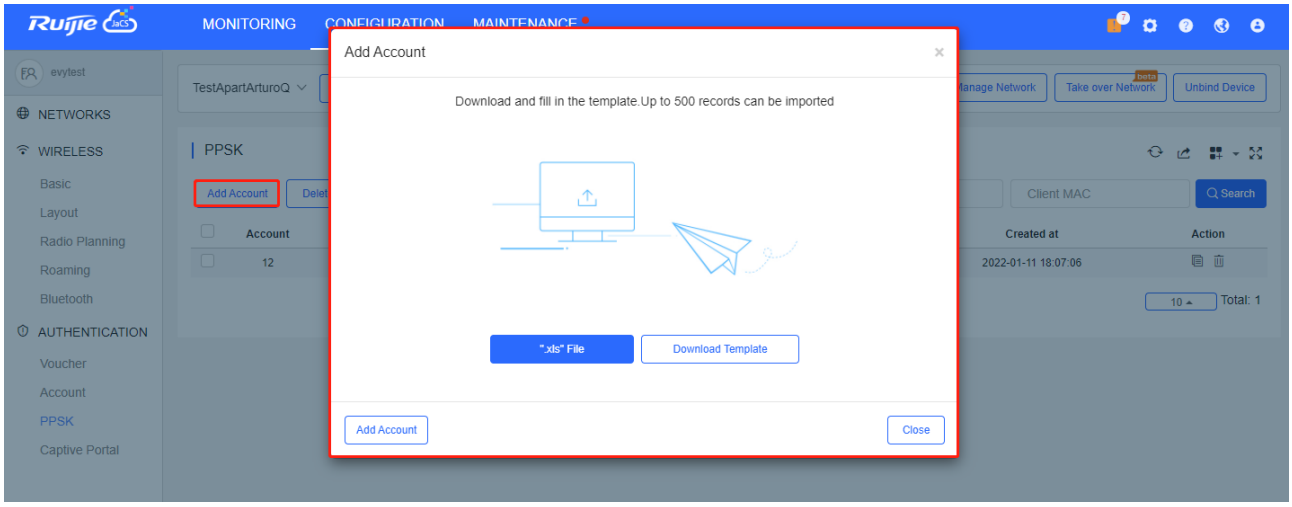
- **Configuration Steps**

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

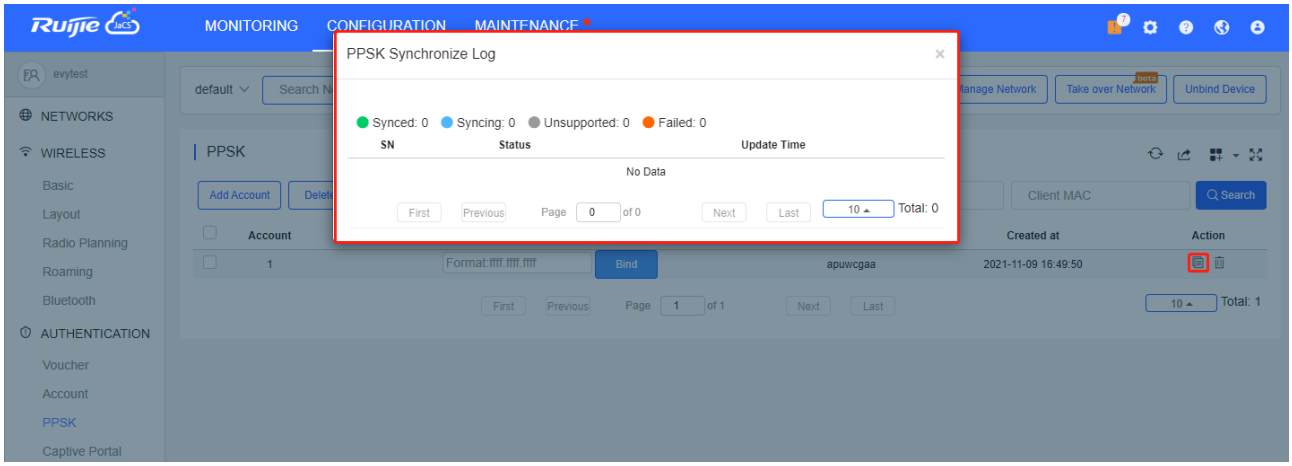


Step 2: Choose **CONFIGURATION** > **AUTHENTICATION** > **PPSK**.

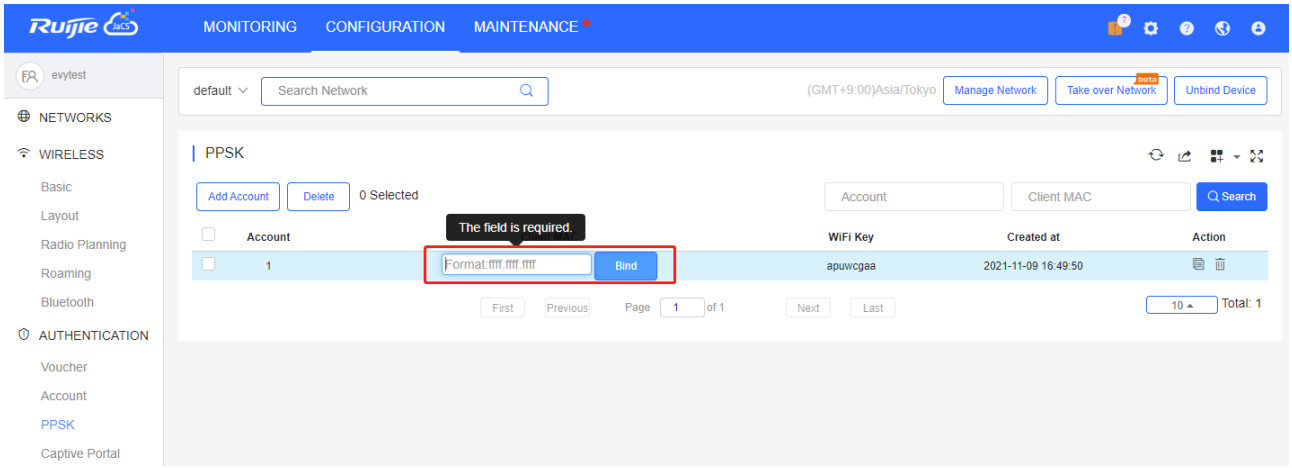
Step 3: Click **Add Account** to batch import or manually add new accounts.



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



Step 5: Bind MAC address for accounts in the PPSK list.



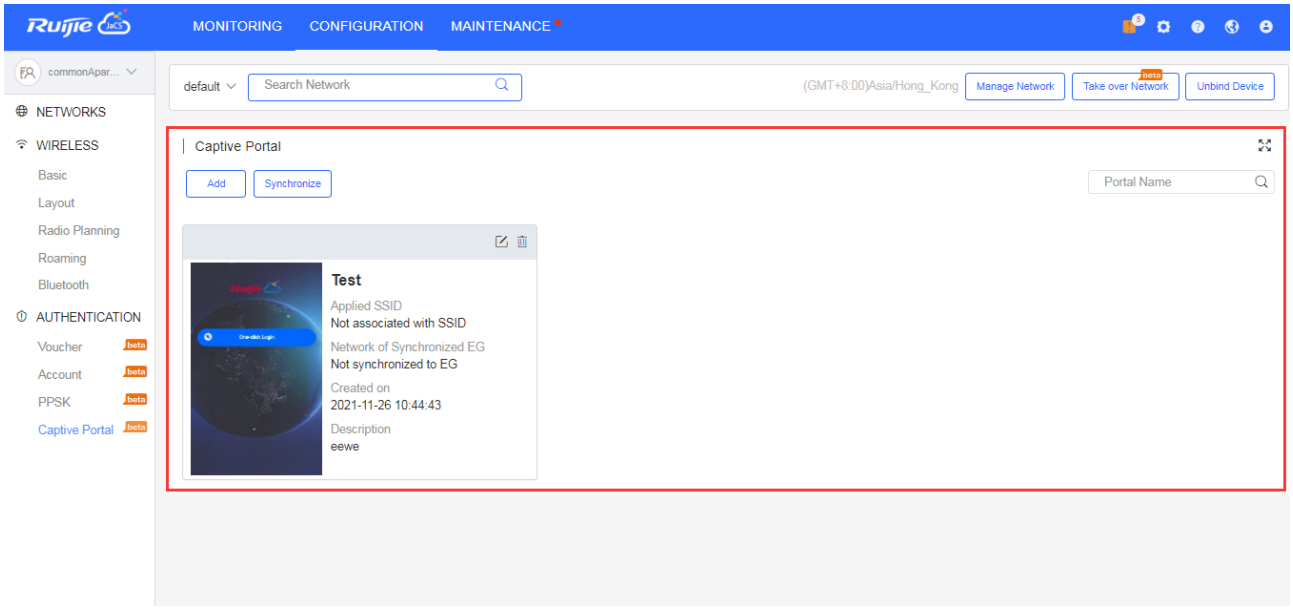
6.3.4 Captive Portal

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

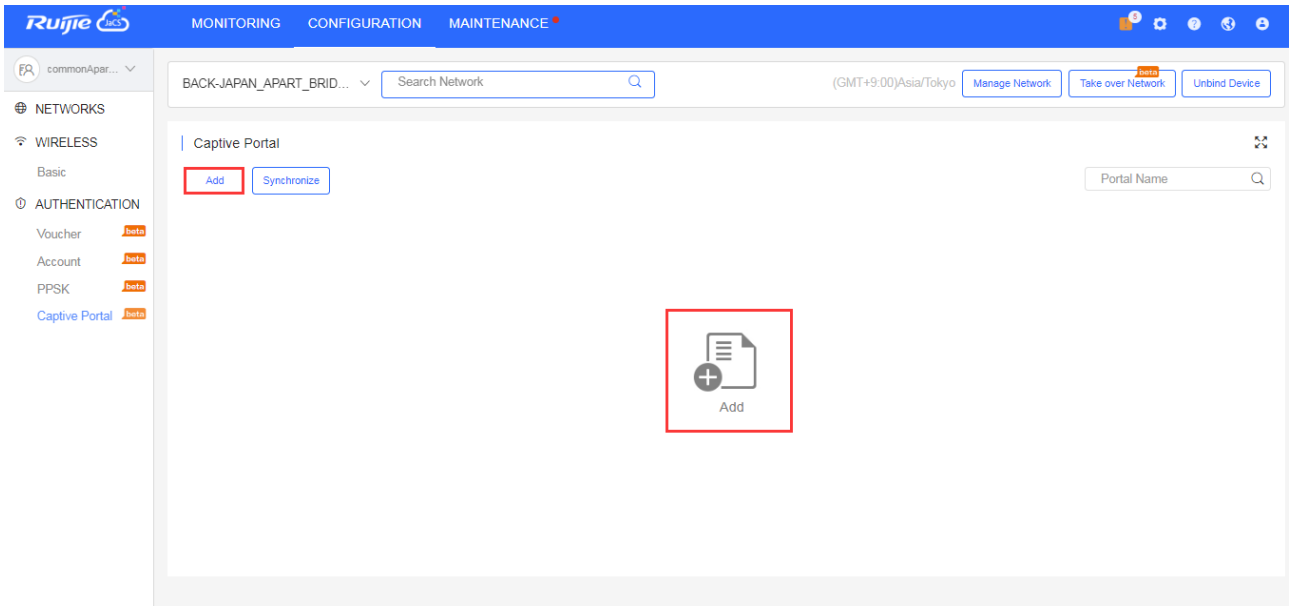
When **Captive Portal** is enabled, SSID can associate with the templates. You can manage templates under a network, but only use or associate templates under a sub-network.

6.3.4.1 Captive Portal List

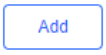
The list displays all captive portal templates, including thumbnails, name, association status, creation time and description.



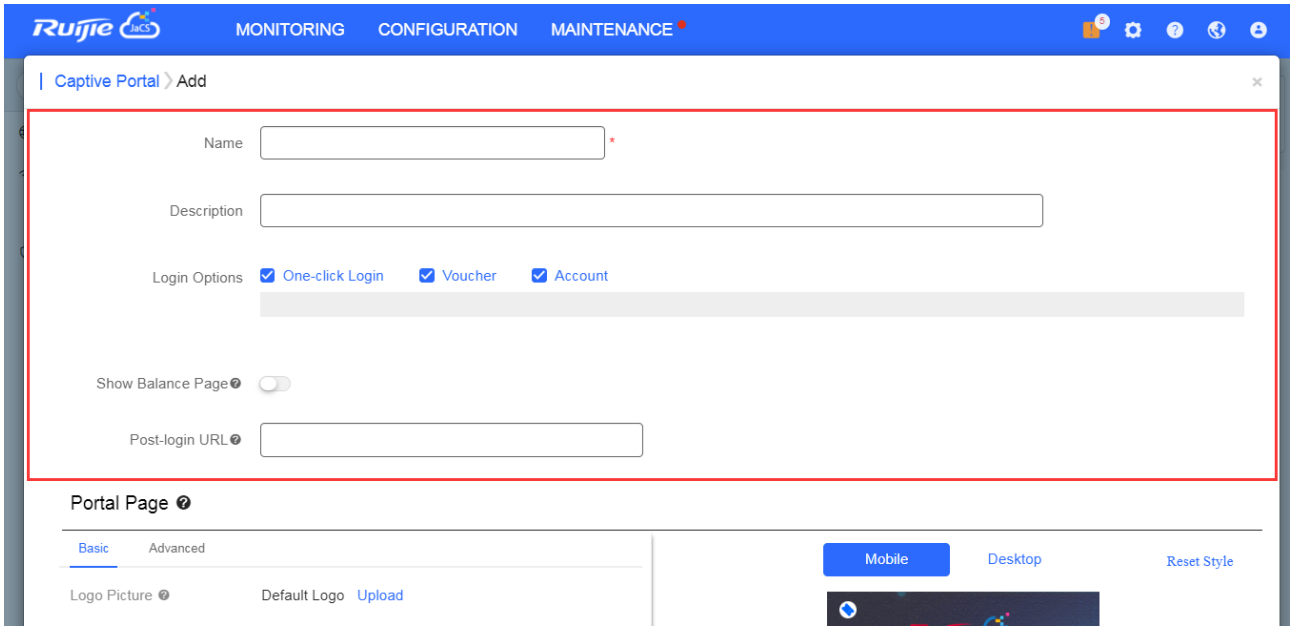
- Add Captive Portal



Click 

or 

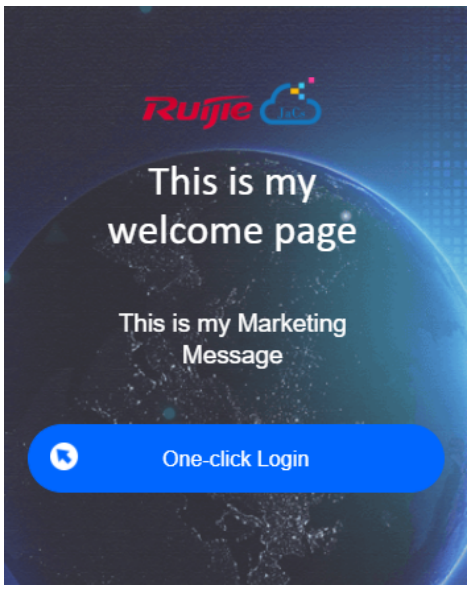
to open the **Add Captive Portal** page. Enter name, description and post login URL, and select login options. After **Status Balance Page** is enabled, you can check your balance information after login.



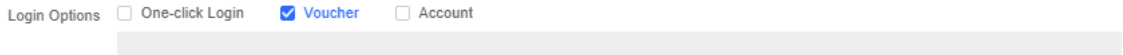
There are three login options: **One-click Login, Voucher,** and **Account**.

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

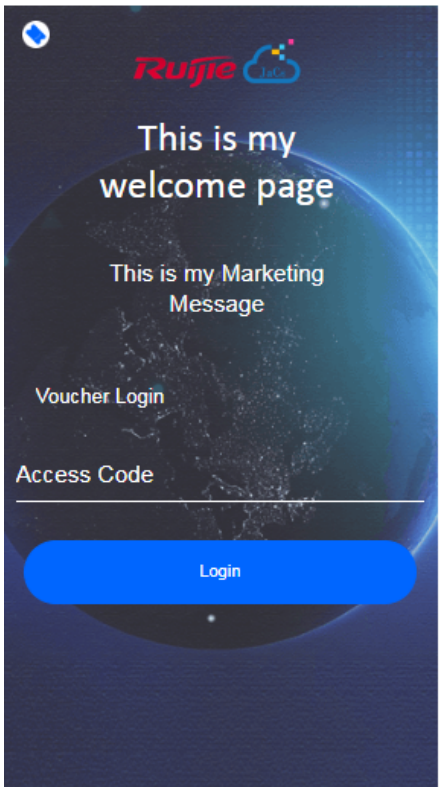
The page for One-click Login:



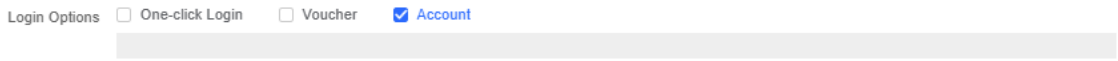
Voucher: You can log in with the voucher code.



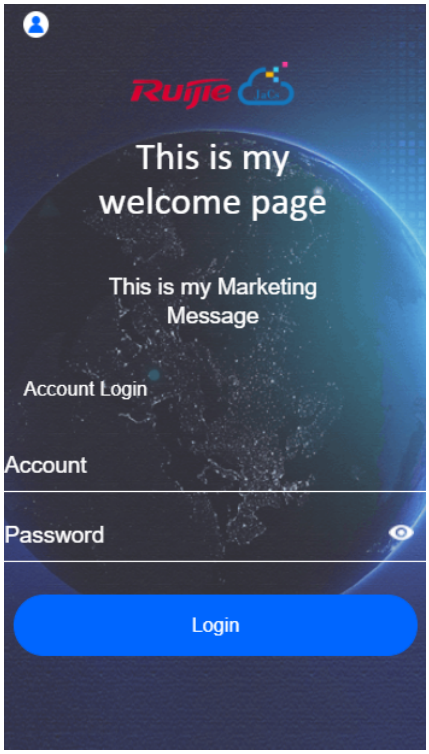
The page for Voucher:



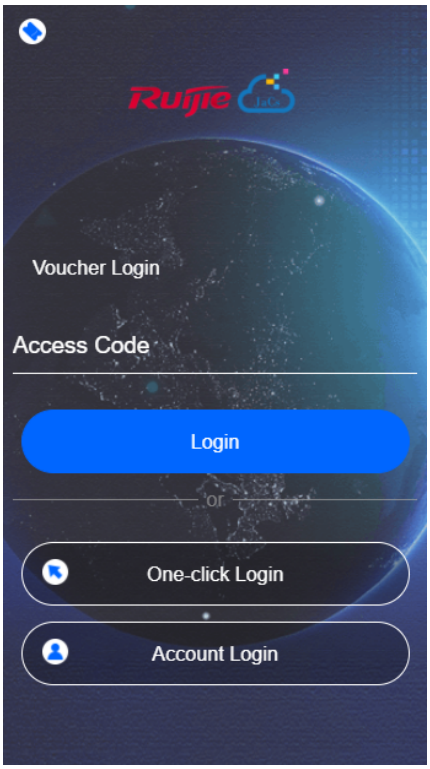
Account: You can log in with the account and password.



The page for Account:

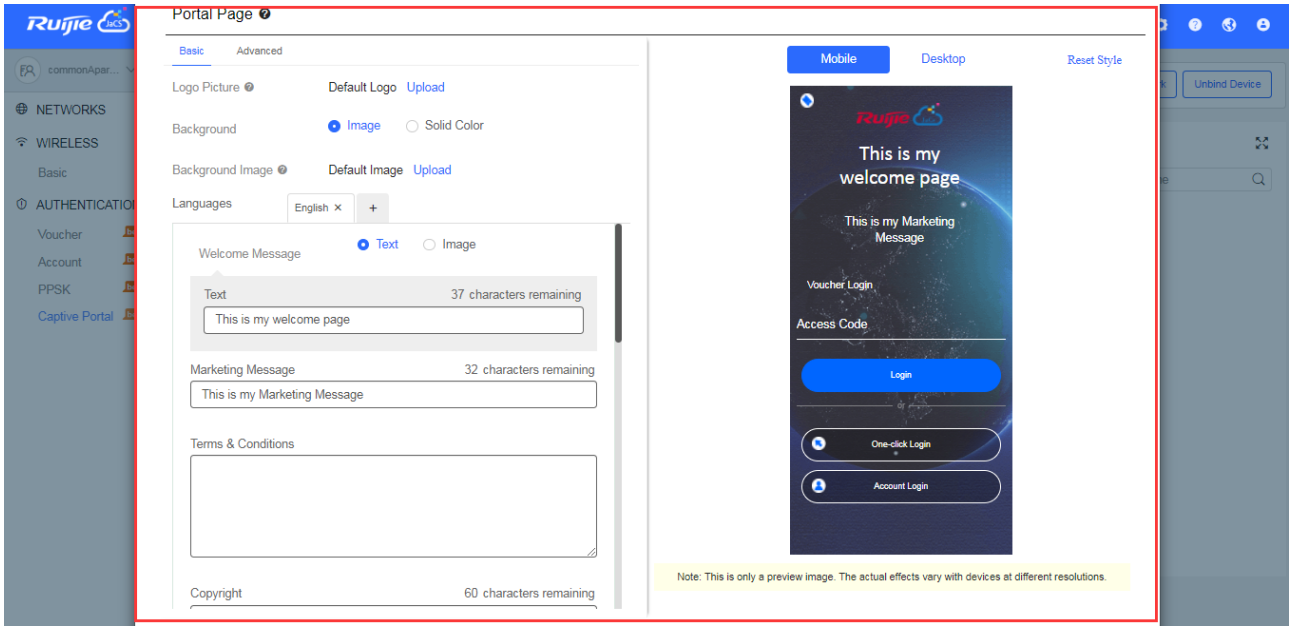


You can also select multiple login options. The page for One-click Login, Voucher, and Account Login:



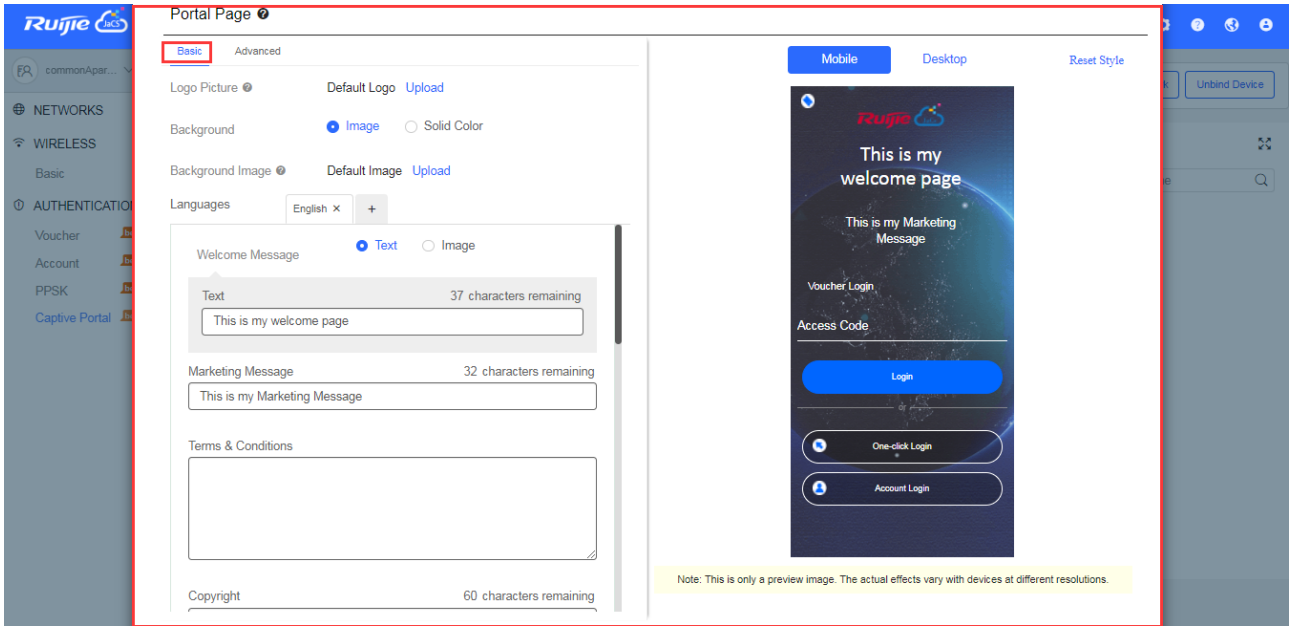
- Portal Page

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

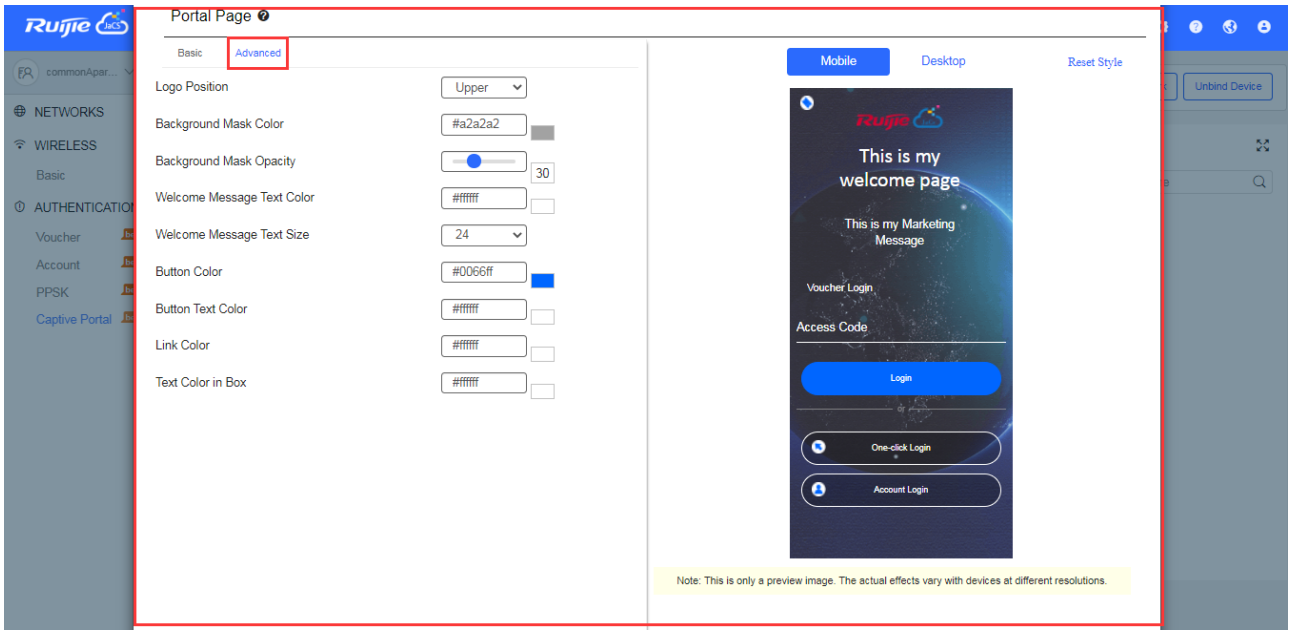


Each type of authentication supports a maximum of three languages. During authentication, users can select a language switching icon in the upper right corner of the authentication page to switch the language.

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



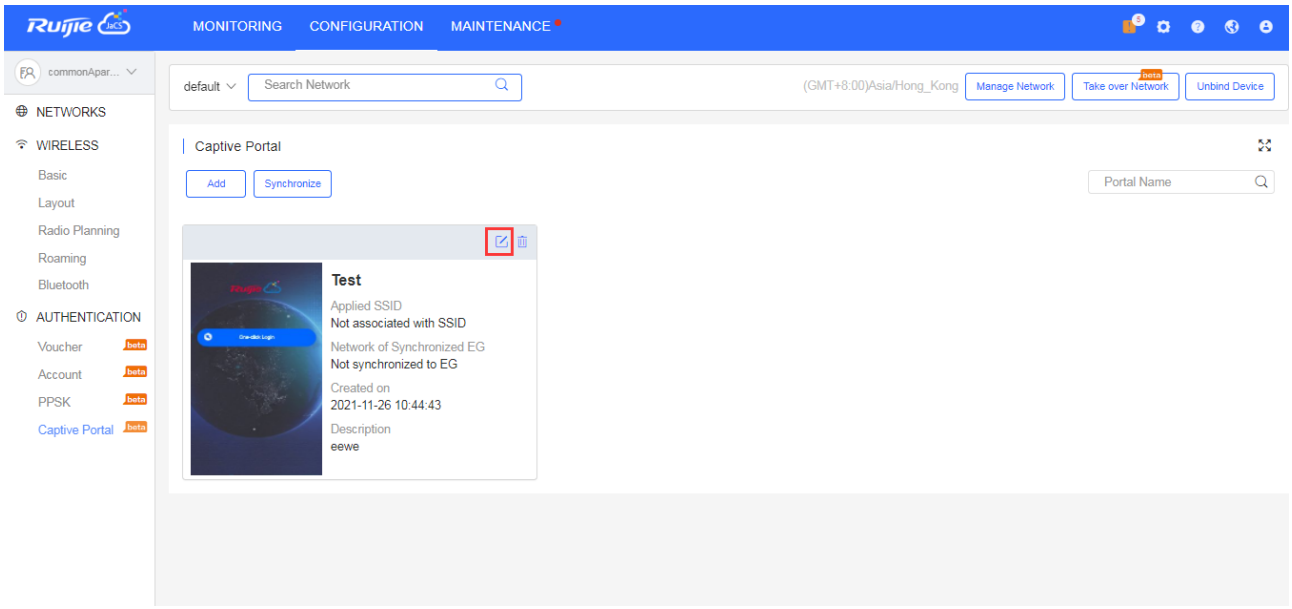
In the **Advanced** tab, set the Logo position, background mask color/opacity, text color/size. Click **Reset Style** to restore the default style.



Click OK on the bottom to save.

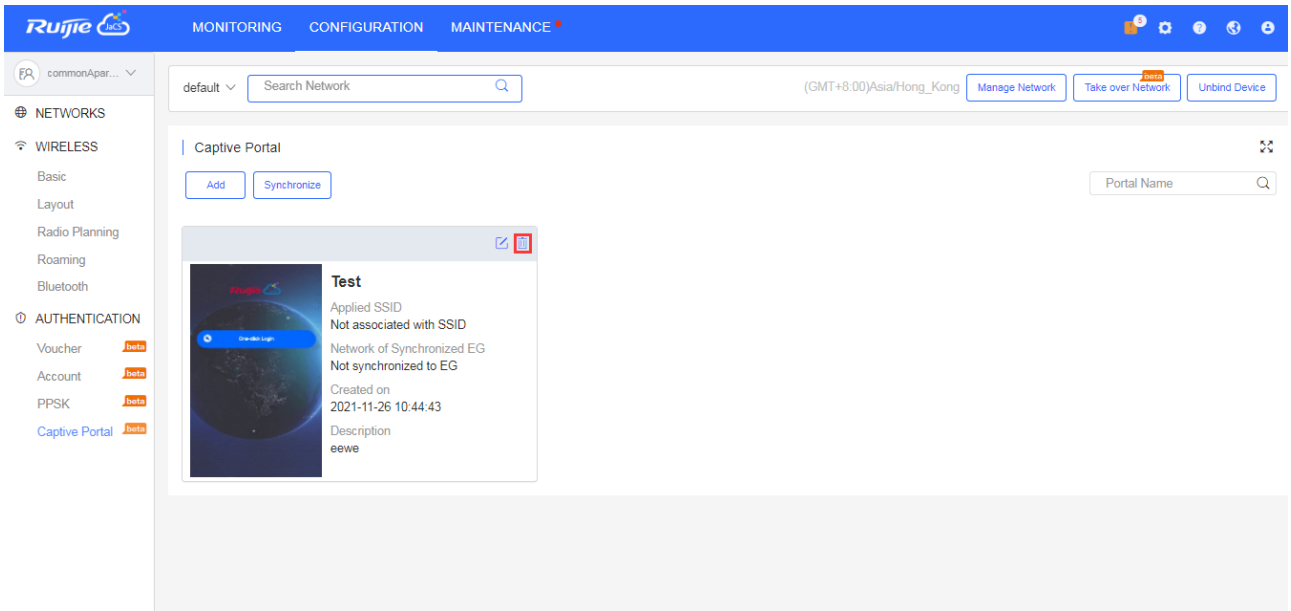
6.3.4.2 Edit Captive Portal

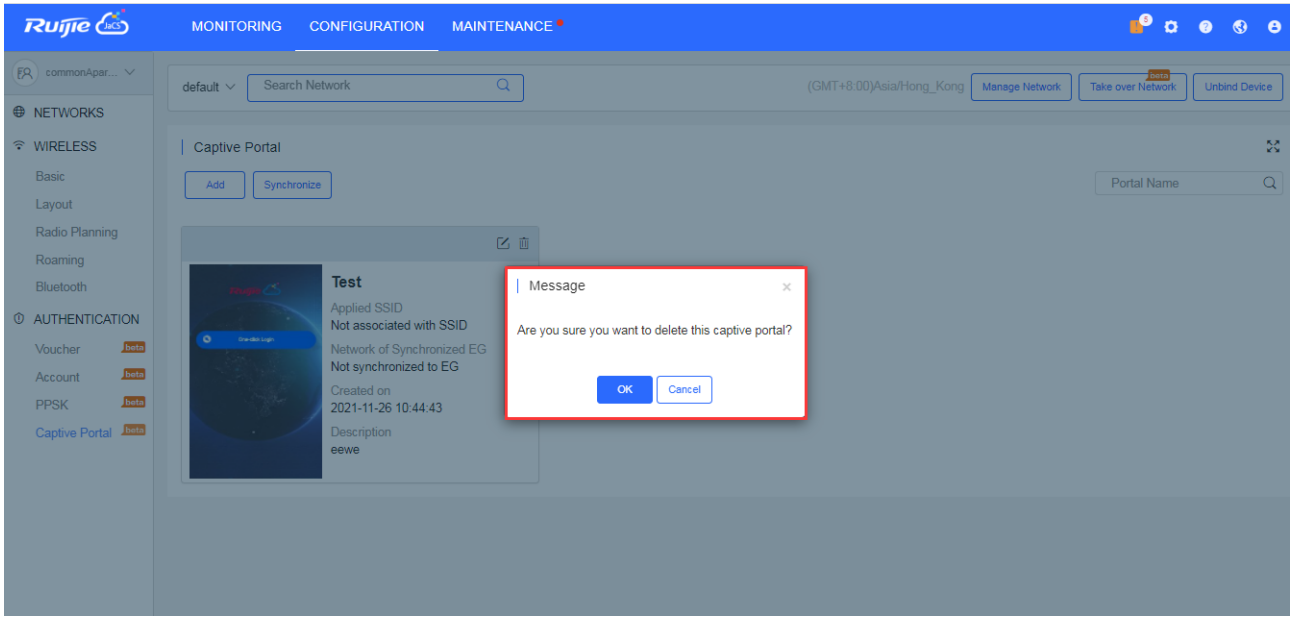
Click  to edit a template, and click OK to save.



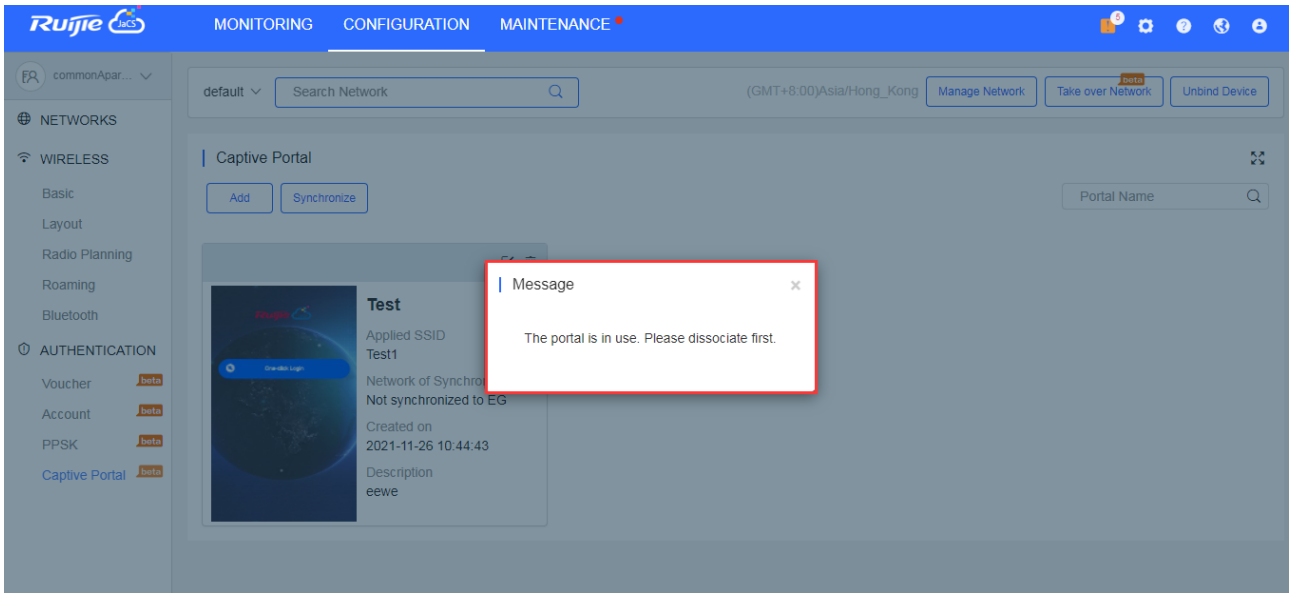
6.3.4.3 Delete Captive Portal

Click  and then click OK in the confirmation window to delete a template.





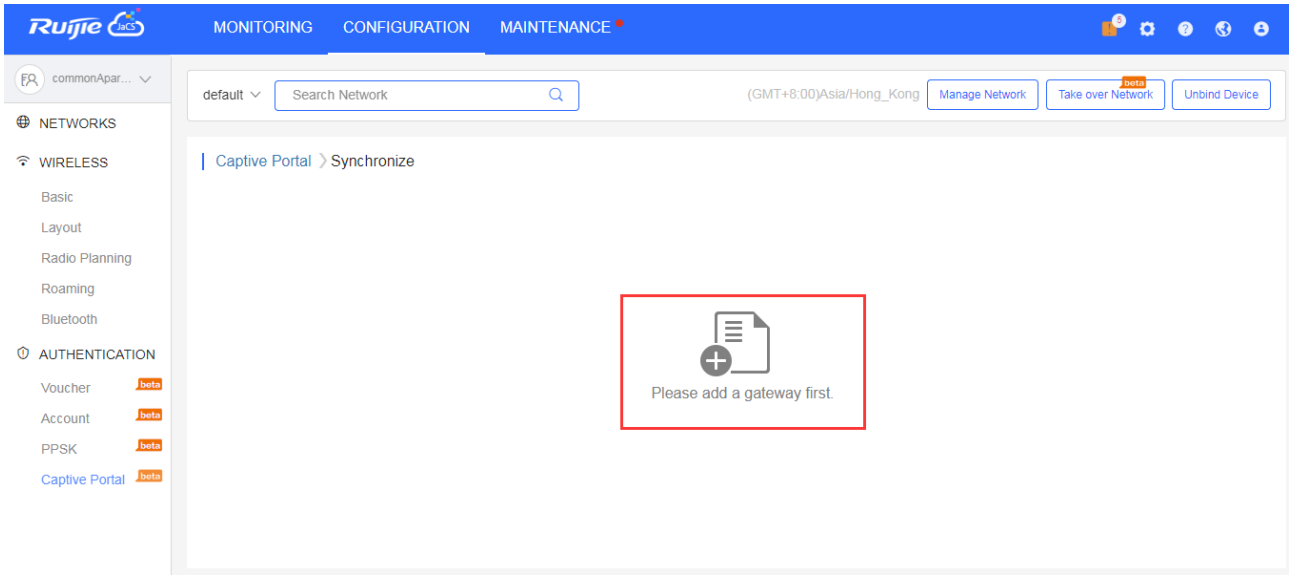
If the template is associated to an SSID or applied to the EG, then you need to dissociate it before delete.



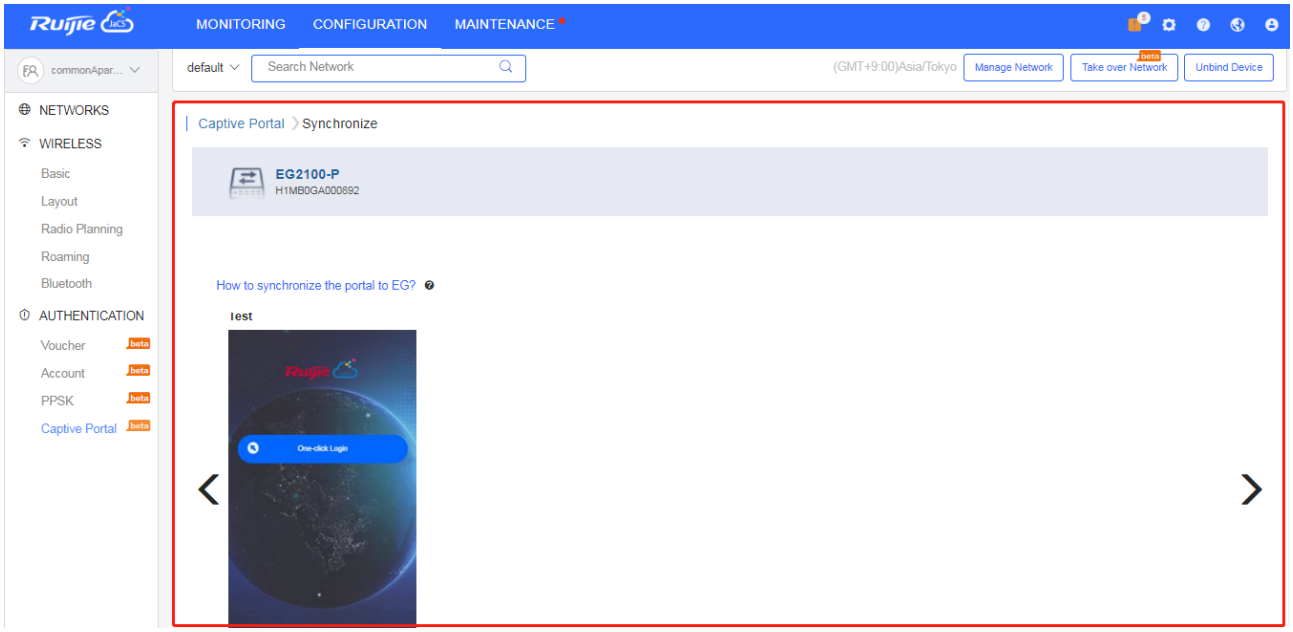
6.3.4.4 Apply to EG

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

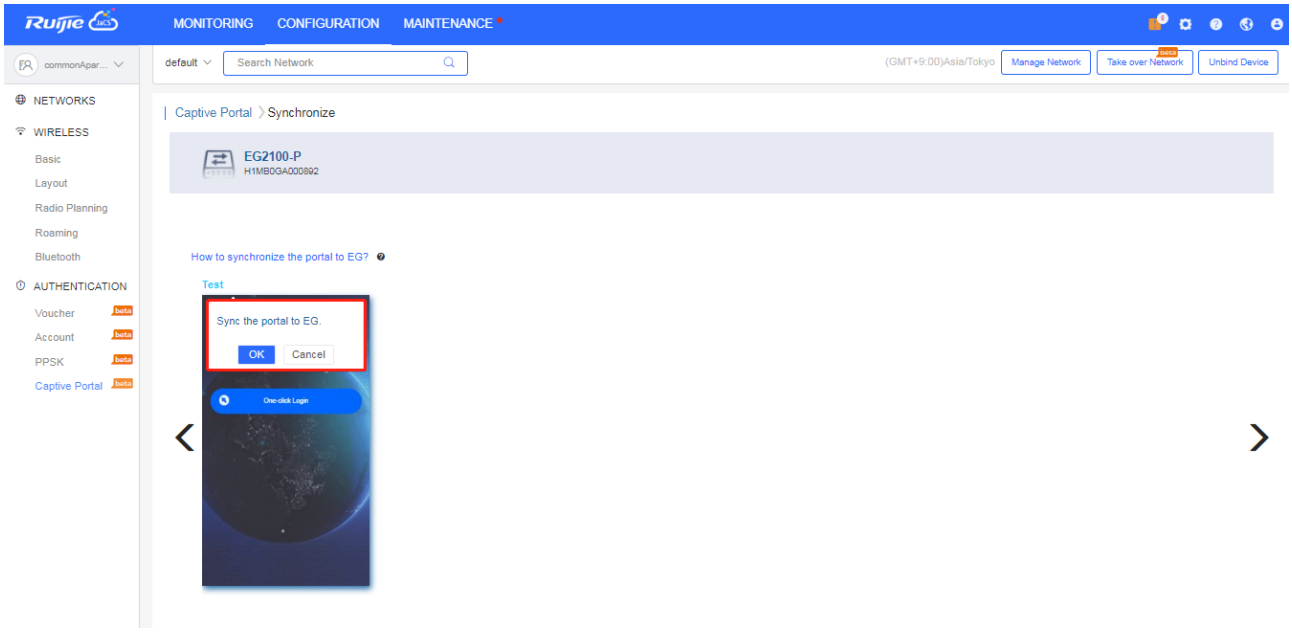
If no EG exists in the current network, you can click to jump to the **MONITORING** > **DEVICE** > **Gateway** page.



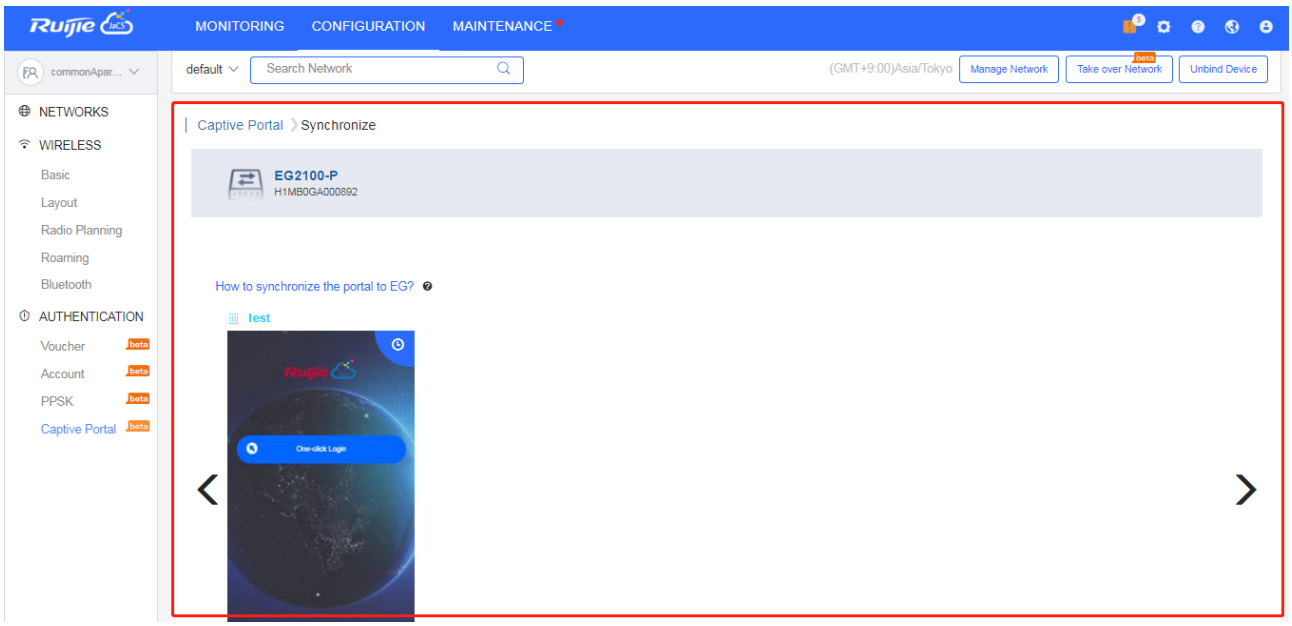
If there is an EG in the current network, the page is displayed as below:



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.



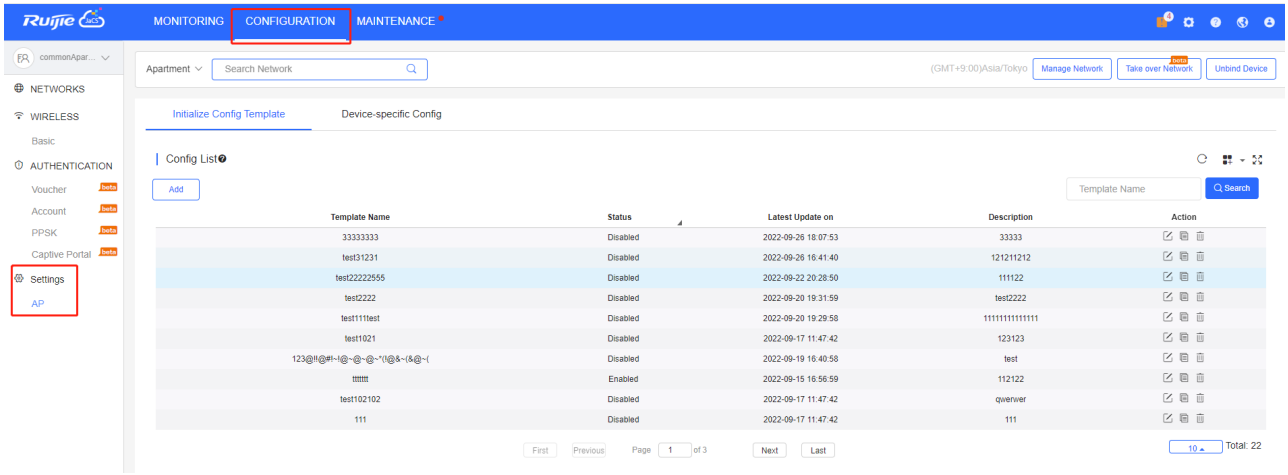
6.4 Settings

6.4.1 AP

6.4.1.1 Initial Configuration Template

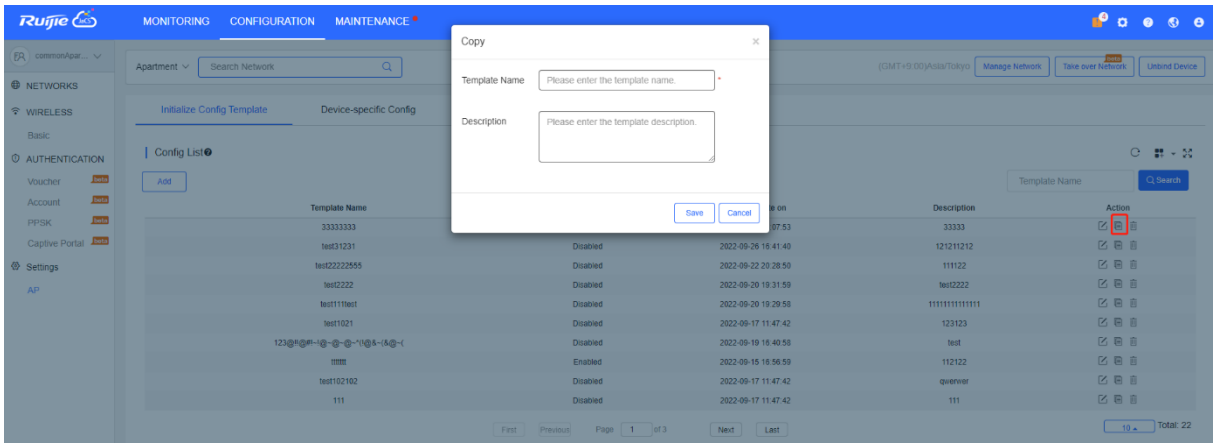
Click **Configuration** > **Settings** > **AP** to open the setting page. In this page, you can configure initial configuration template and device-specific config.

In the **Initial Config Template** page, a **Config List** is displayed, and all templates are shown in the order of update time. You can add, edit, copy and delete a template. You can also search a template by name.



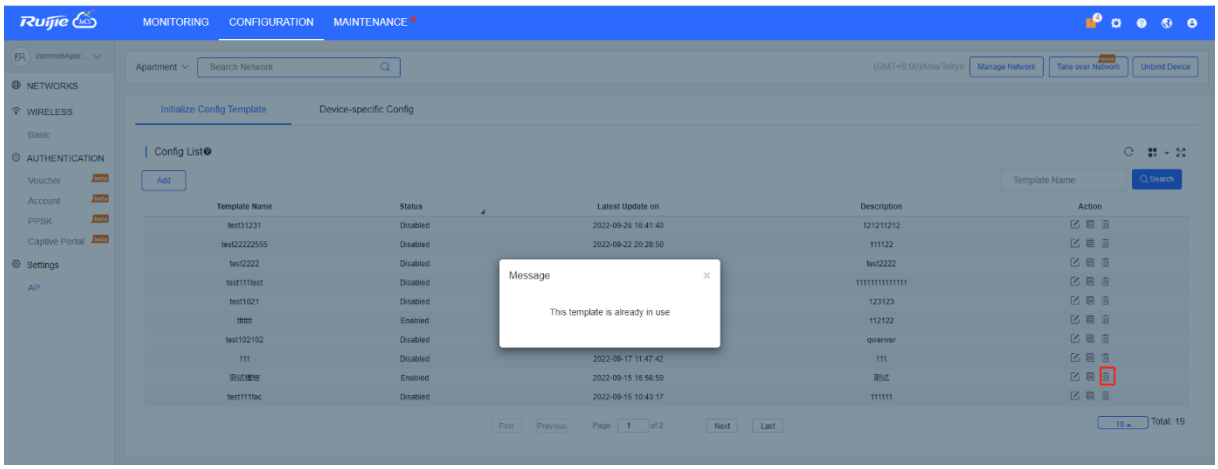
■ Copying a Template

After clicking in the **Action** column, a prompt will appear. Enter a new template name and description, then click **Save** to form a new template. Except the name and description, other configurations of the new template remain the same with the previous one.



■ Deleting a Template

Click in the **Action** column to delete a template. If the following prompt message appears, it means the template cannot be deleted as it is already in use.

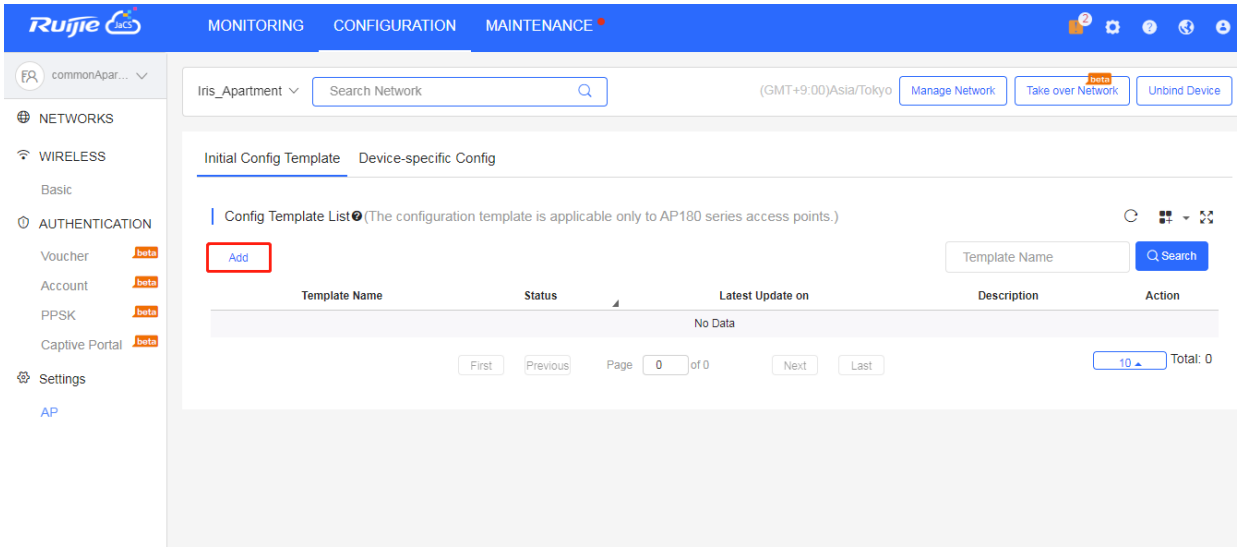


■ Editing a Template

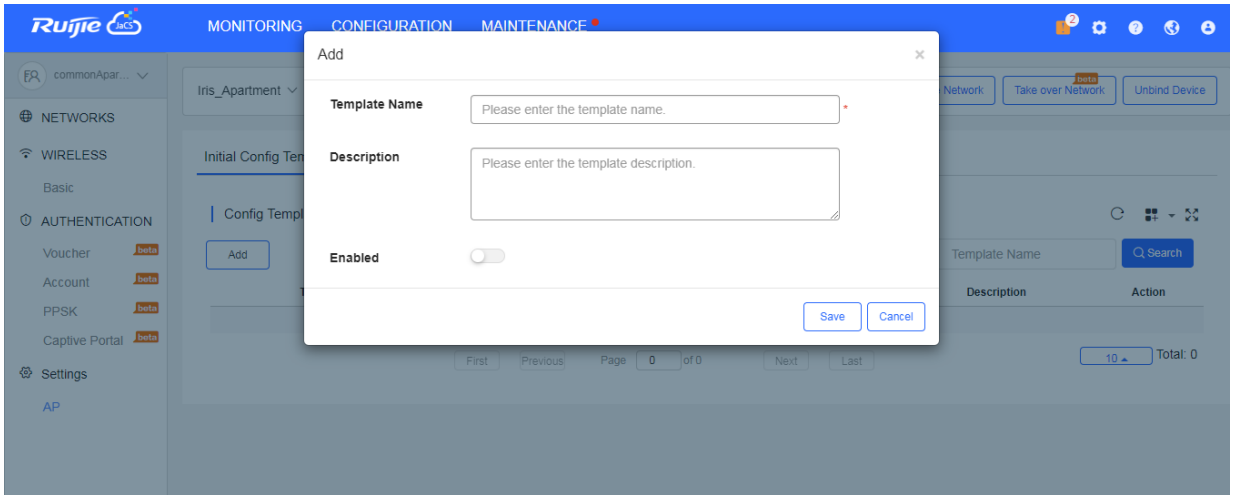
Click in the **Action** column to edit a template. You can edit all the configurations of the template, but if the template is in used, it cannot be edited.

Adding a Template

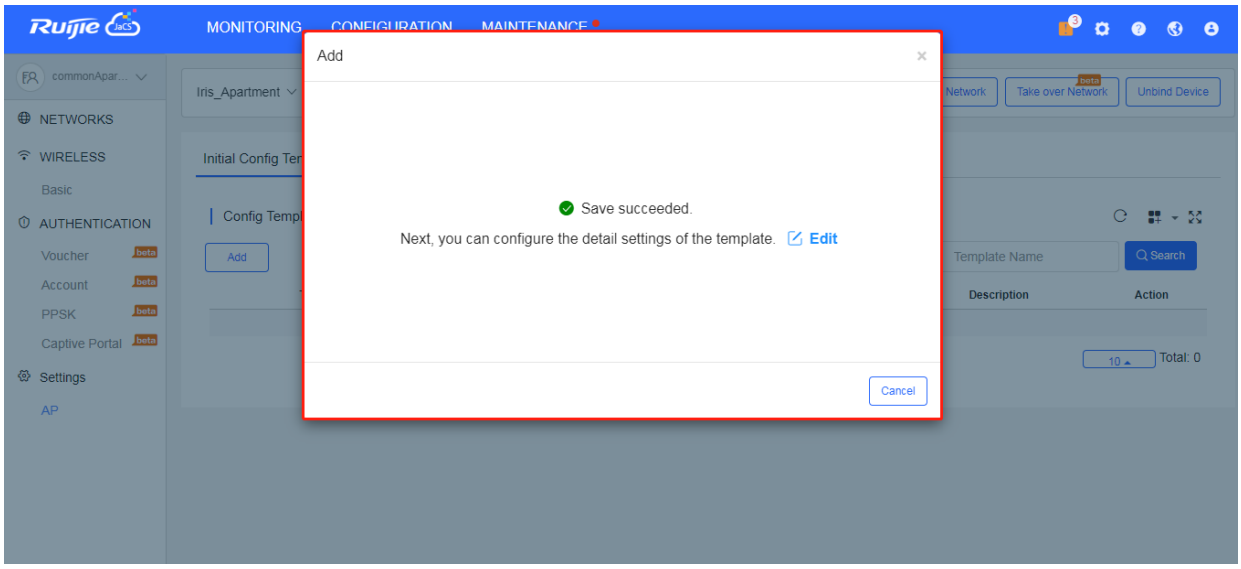
Click **Add** to open the setting page.



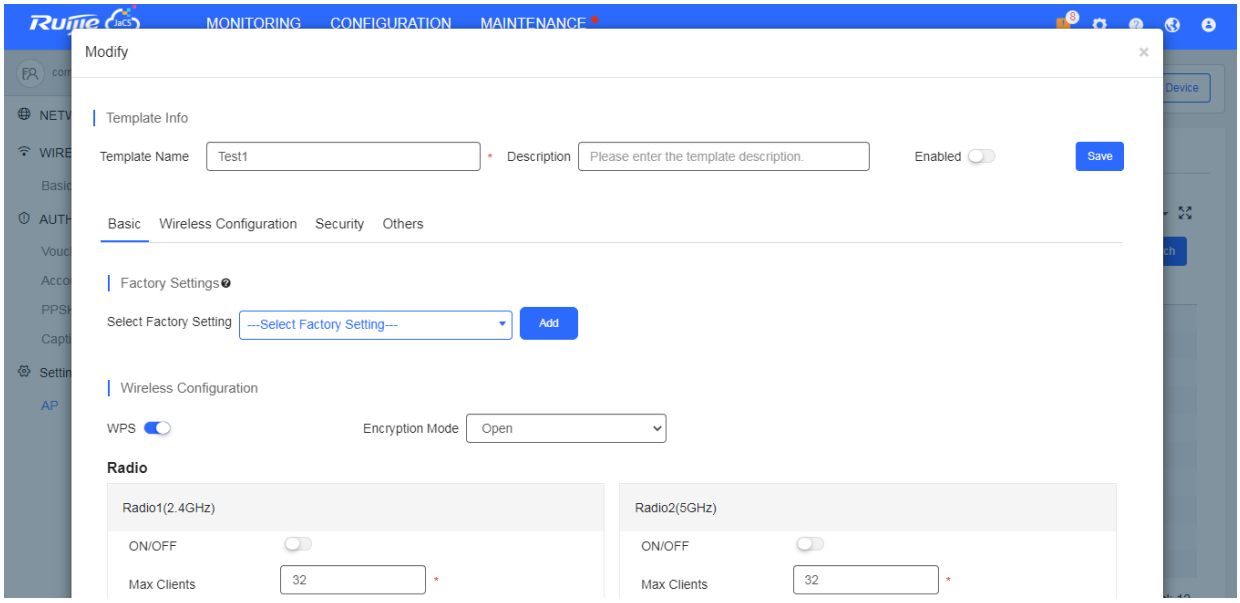
Specify the **Template Name** (required) and **Description** (optional), and then click **Save**.



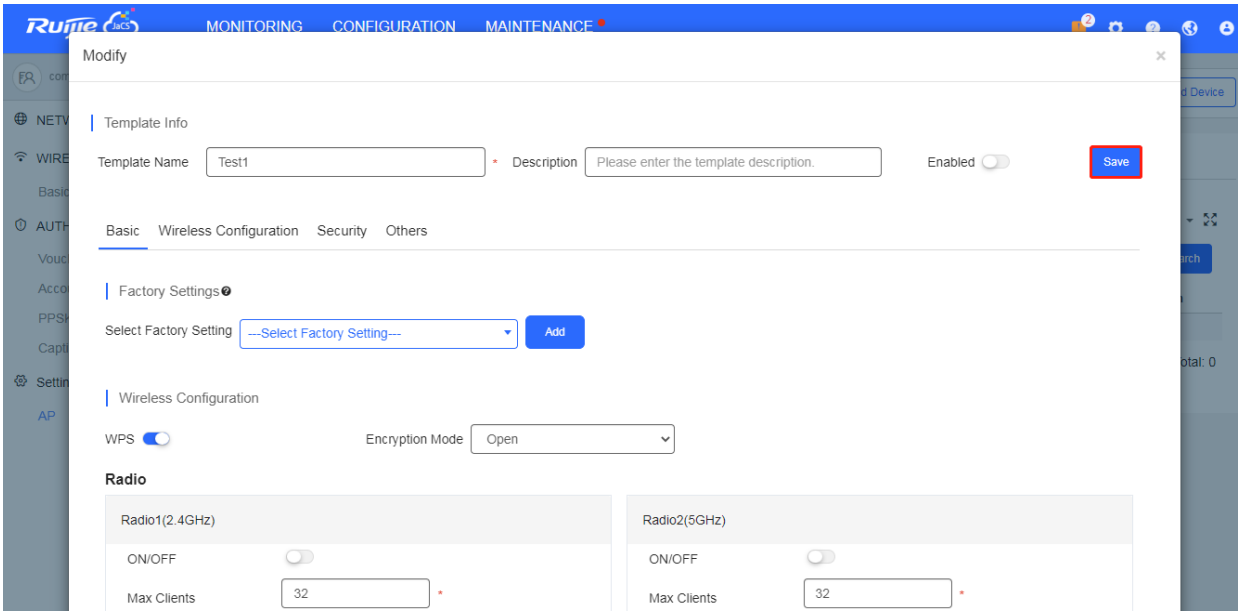
When the “**Save succeeded**” appears, the operation is complete.



Click Edit to modify the basic information of the template.



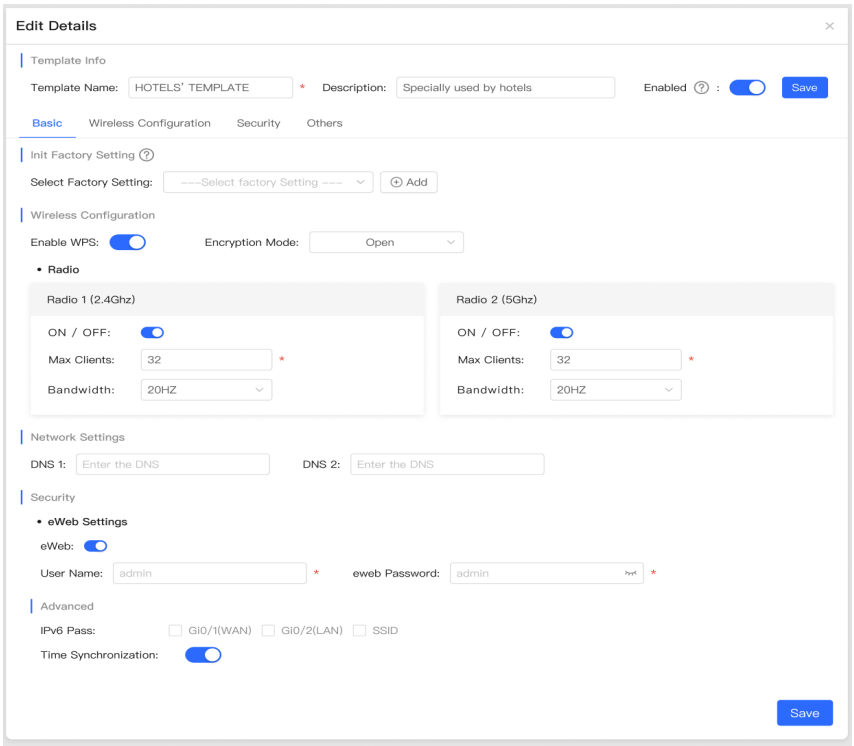
In the **Modify** page, you can change the settings of the template name, the description and the enabled status. When a change is made, click **Save** in the right side.



You also can specify the parameters in the four Tab pages: **Basic**, **Wireless Configuration**, **Security** and **Others**. After modifying the parameters, click **Save**.

- **Basic**

In this page, you can configure factory settings, radios, DNS, the password of eWeb and IPv6.

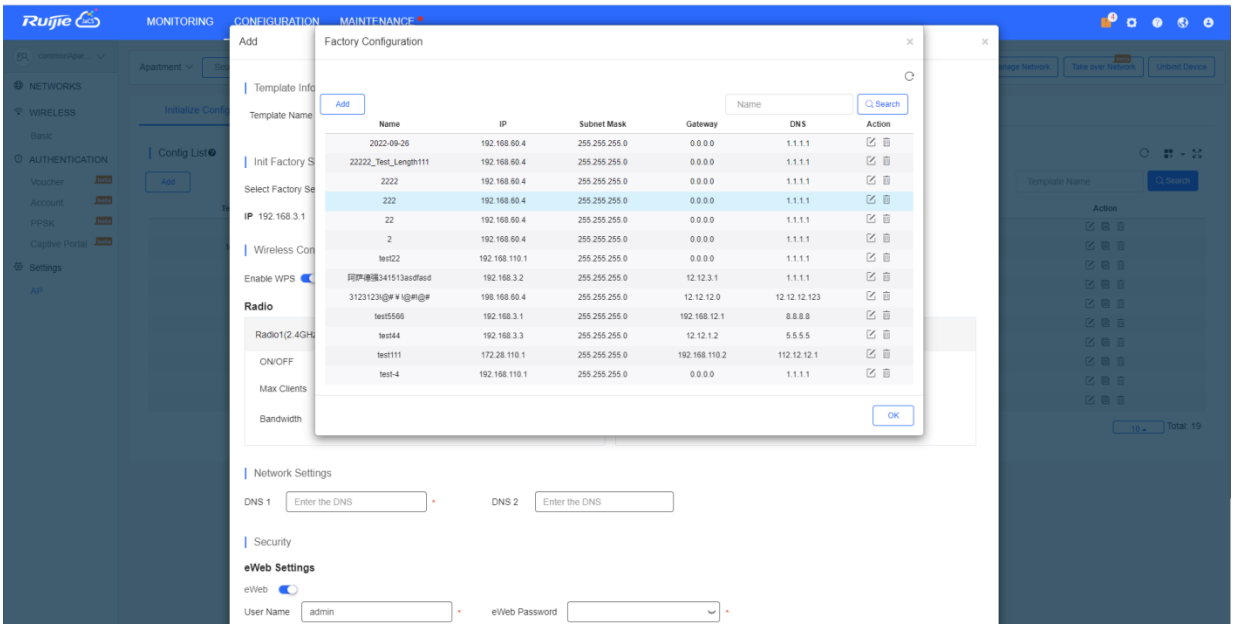


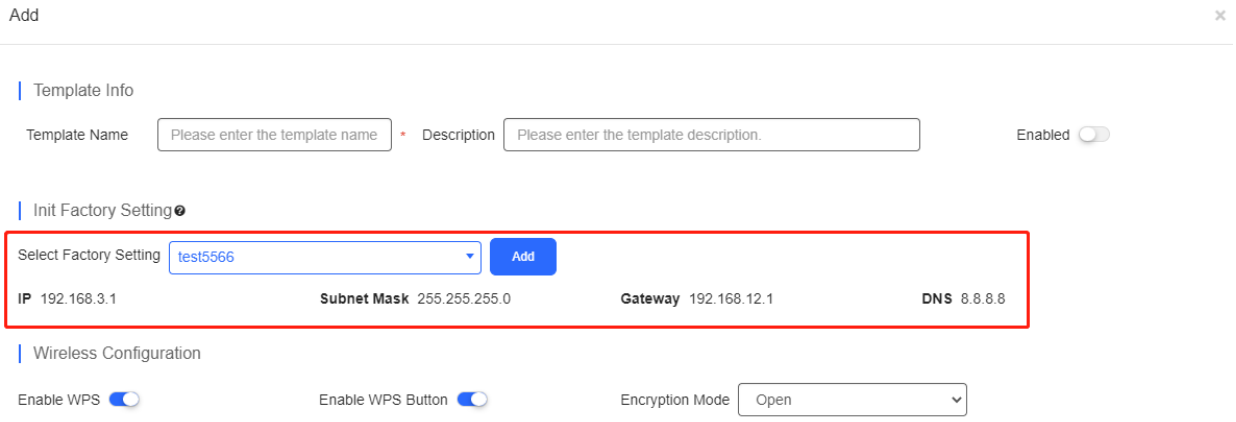
Initializing Factory Setting (Optional):

You can click the down arrow to select an existing template, or click **Add** to create a new one. If you select an existing template, the configurations of the template will be displayed below the selection box. If you need to add a new template, you can click **Add** to go to the **Factory Configuration** page.

When the factory settings are applied to a device, you need to press the reset button of the device to reset the device to make them take effect, and all global configurations and other configurations will be cleared.

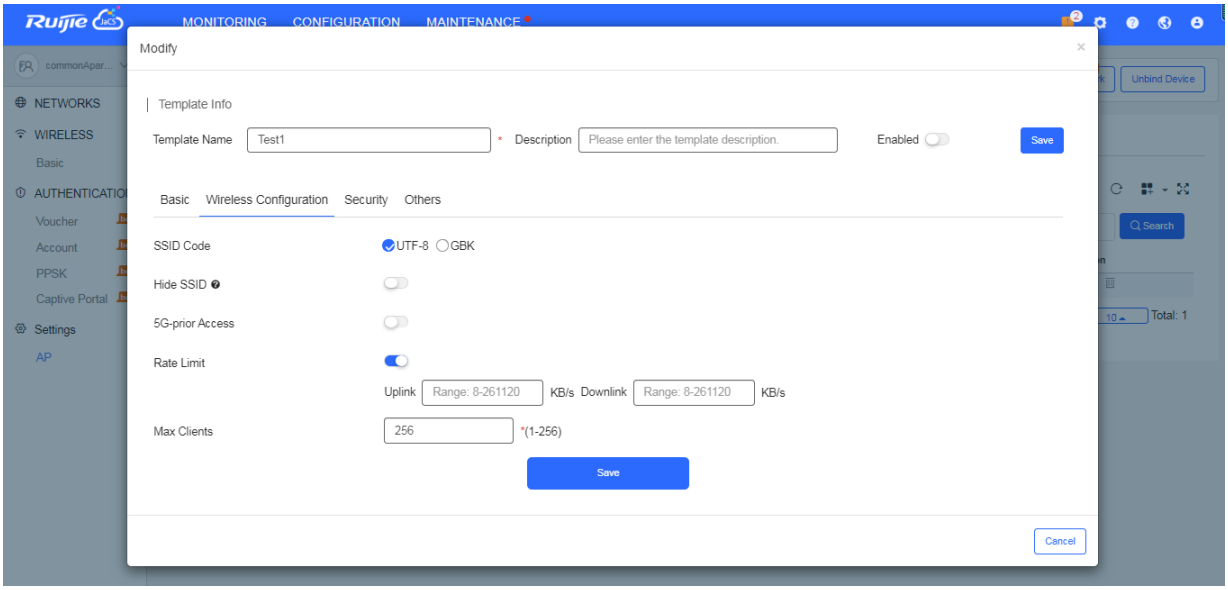
In the **Factory Configuration** page, you can add a new factory setting, and edit or delete an existing one. When a new factory setting is added, it will be displayed in the drop-down list box. If a factory setting is changed, it will take effect in all templates to which the factory settings are applied. Only an unused factory setting can be deleted.





- **Wireless Configuration**

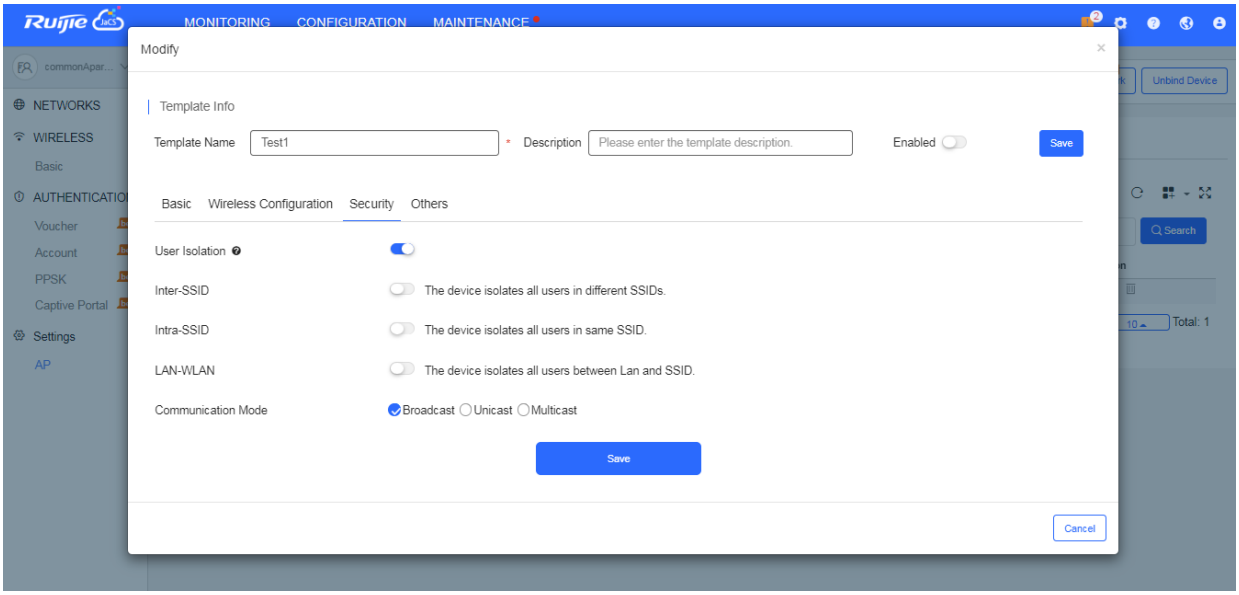
You can hover you mouse on to view the notes of **Hide SSID**.
When **Rate Limit** is enabled, you need to set the downlink and uplink rate.



- **Security**

In this page, you can configure user isolation and communication mode.

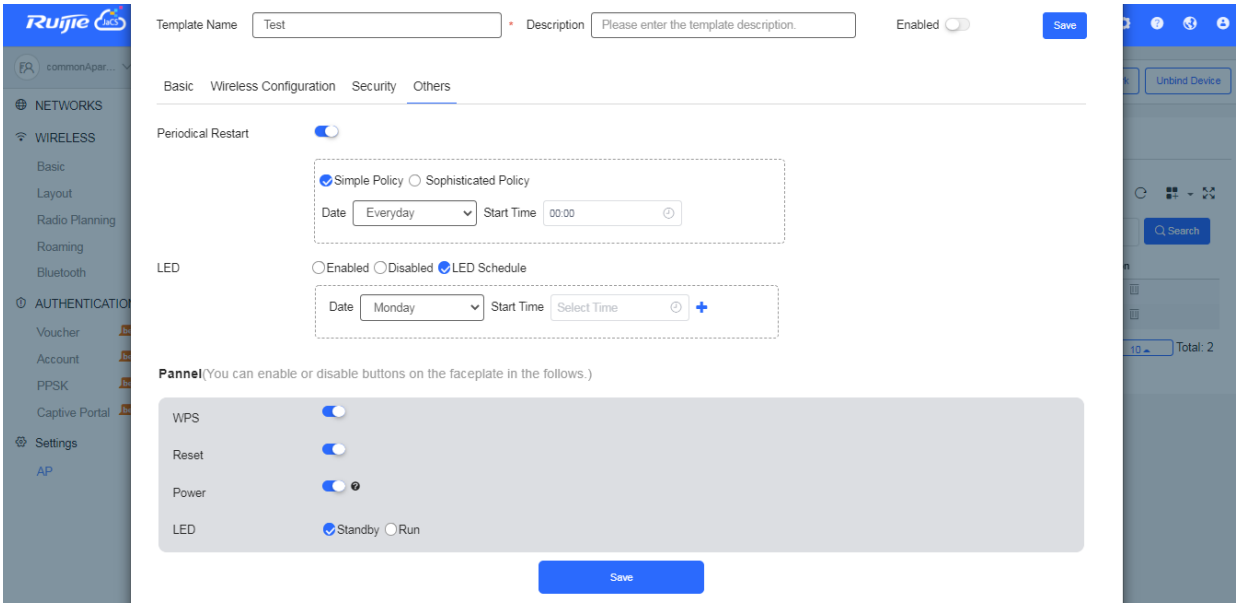
When the user isolation is enabled, inter-SSID, intra-SSID and LAN-WAN are enabled simultaneously. You can hover the mouse over to check more details about this function.



- **Others**

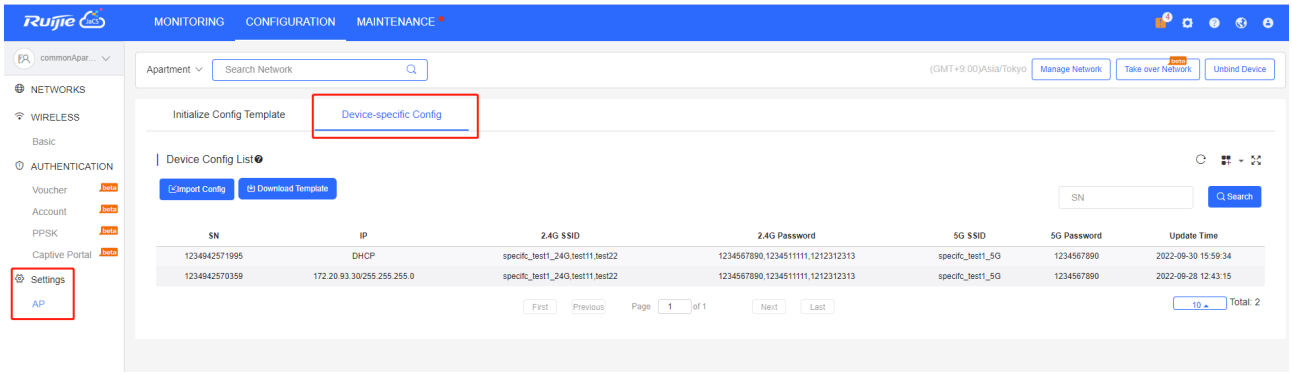
The **Periodical Restart** is disabled by default. When it is enable, you can choose **Simple Policy** and **Sophisticated Policy** to schedule the reboot of the device to take effect in a specific time.

When LED schedule is enabled, you should specify the start time and the end time.



6.4.1.2 Device-specific Configuration

In the **Device Config List**, the information of all devices with specific configuration is displayed, including SN, IP, 2.4G SSID, 2.4G PASSWORD, 5G SSID, 5G PASSWORD and Update Time. In the 2.4G/5G SSID and 2.4G/5G PASSWORD columns, commas (,) are used to separate multiple SSIDs and passwords. And the SSIDs and passwords are one-to-one correspondence. Up to 3 SSIDs or passwords are supported.



■ **Downloading the Template**

Click **Download Template** to download the template. The parameters and their description are shown as follows:

A	B	C	D	E	F	G
SN	IP Address	Subnet Mask	2.4G SSID	2.4G SSID Password	5G SSID	5G SSID Password

The SN is required. The IP address and subnet mask should be filled in or not filled in together (when they are left empty, the device will obtain IP address and subnet mask via DHCP). The other four fields are optional.

- Multiple SSIDs and passwords are supported. Use commas (,) to separate them.

■ **Importing Configuration**

Click **Import Config** to import the template. Up to 200 templates are supported. When a template is imported, the system will verify the parameters filled in the template. The import process will be stopped when one of the following situations occurs:

- The SN is not available in the current network.
- The format of IP address is incorrect.
- The number of SSIDs and passwords are different.

■ **Search**

You can enter the SN of a device in the search box in the upper right corner to search the device.

7 Maintenance

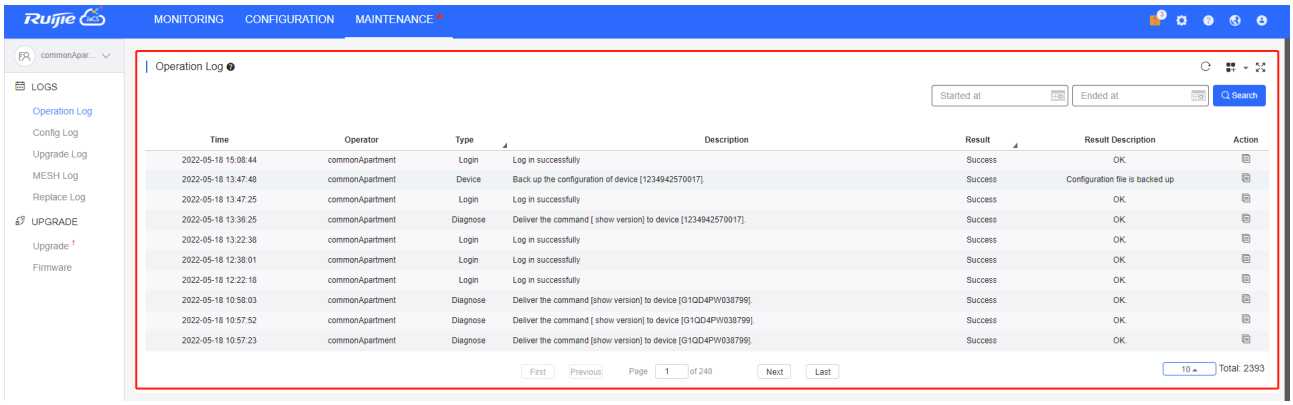
The **Maintenance** module mainly provides the following functional services:

- LOGS
- UPGRADE

7.1 Logs

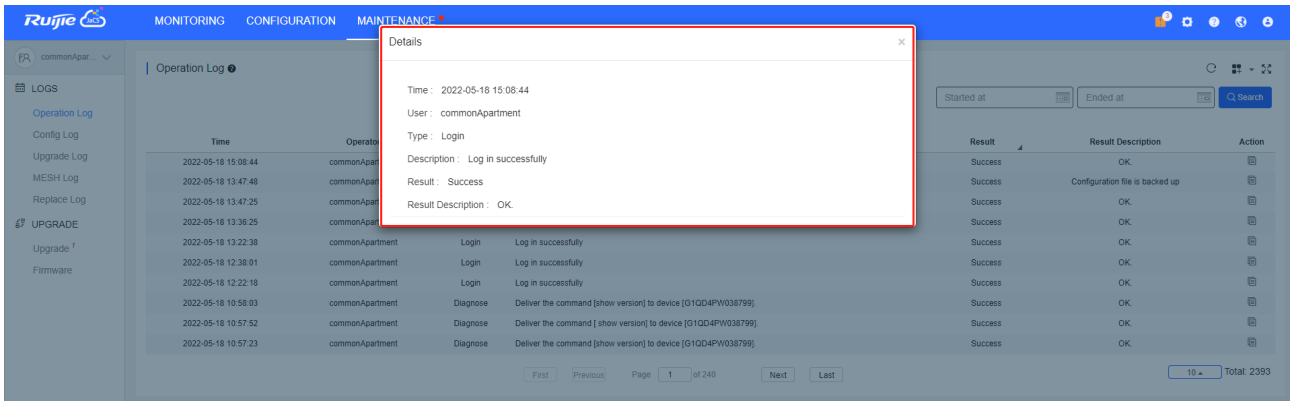
7.1.1 Operation Log

This page shows operation logs.



Click  in **Action** column to check log details.

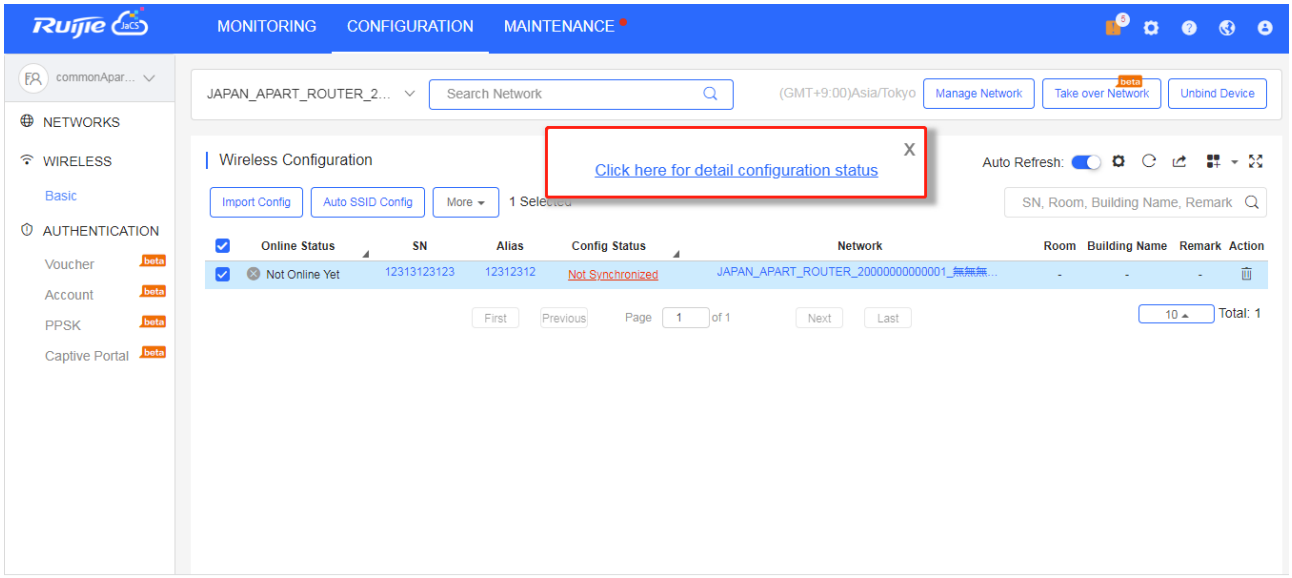
General operation log details are shown as follows:



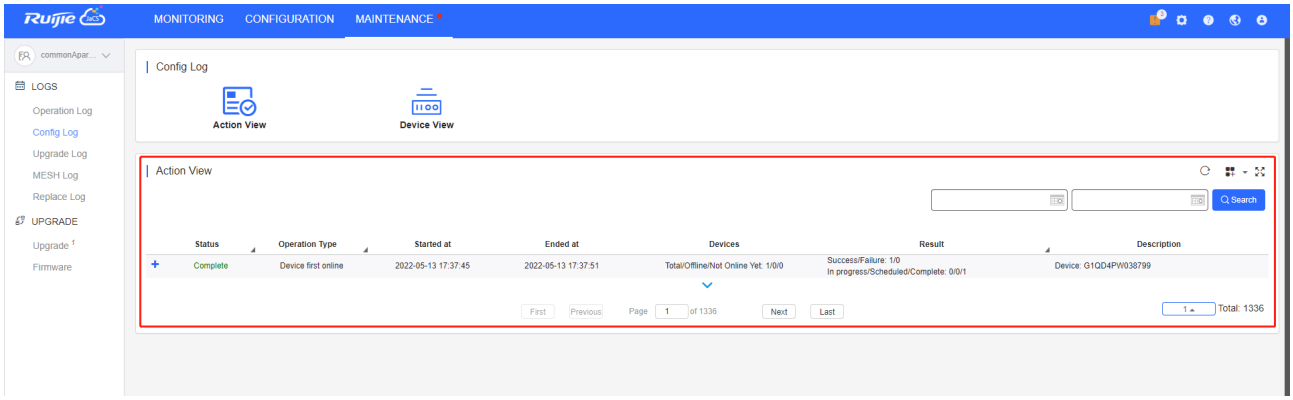
7.1.2 Config Log

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

  In progress: Configuration is in progress

  Scheduled: Configuration is scheduled

- Result: View configuration results

  Success: Number of devices configured successfully

  Failure: Number of devices whose configuration fails

- Devices

  Total: Total devices in the network

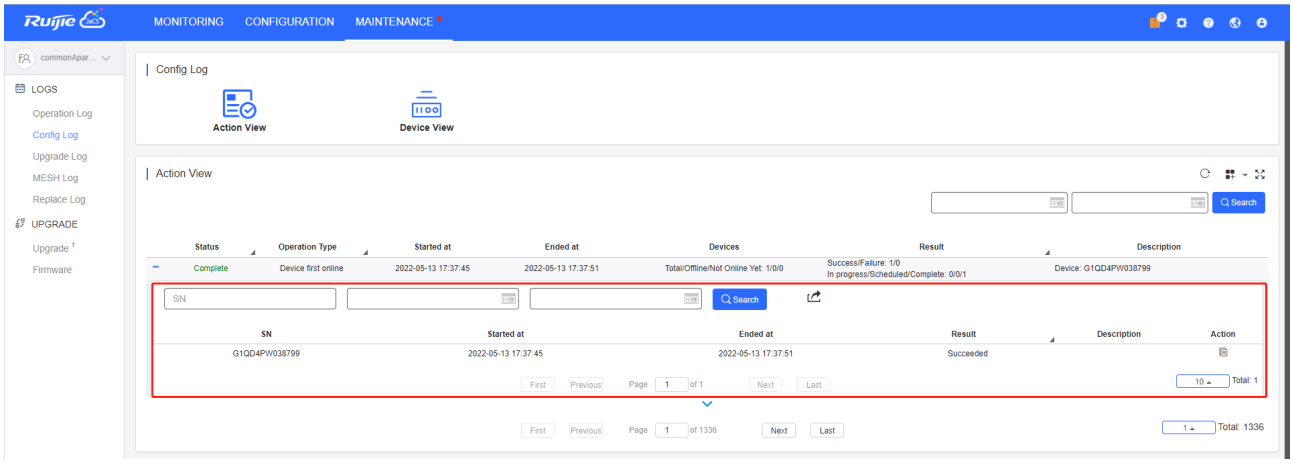
  Offline: Number of offline devices

  Not Online Yet: Number of devices that never go online

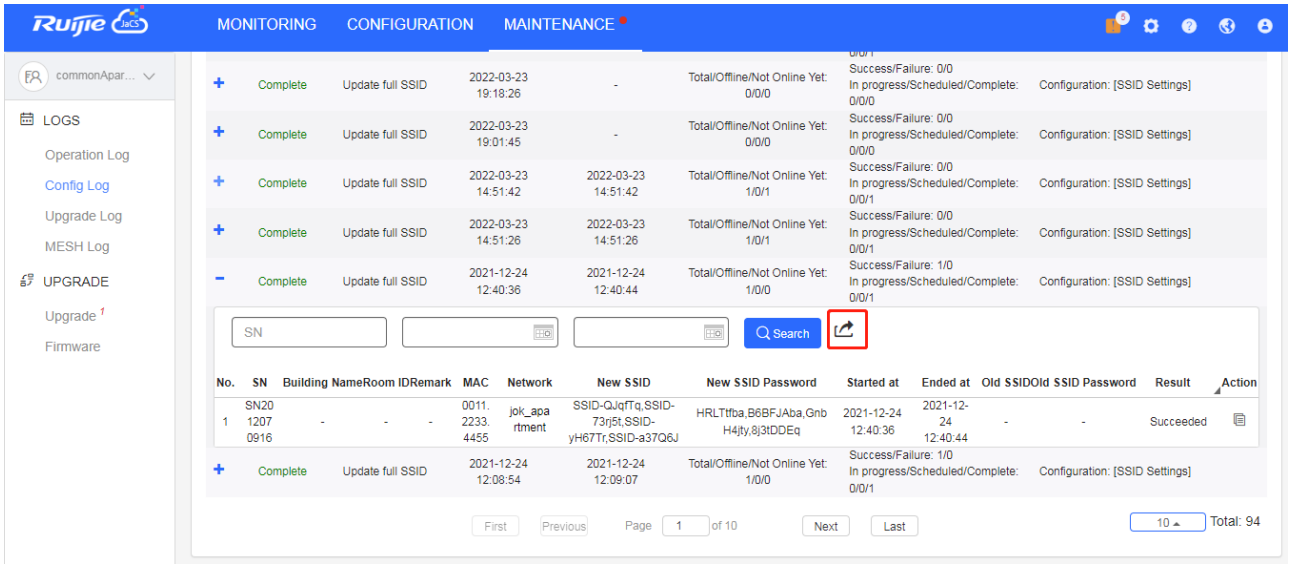
Cloud will give priority to the online devices, and will actively apply the configuration after the offline devices go online.

- 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  to export the configuration result.



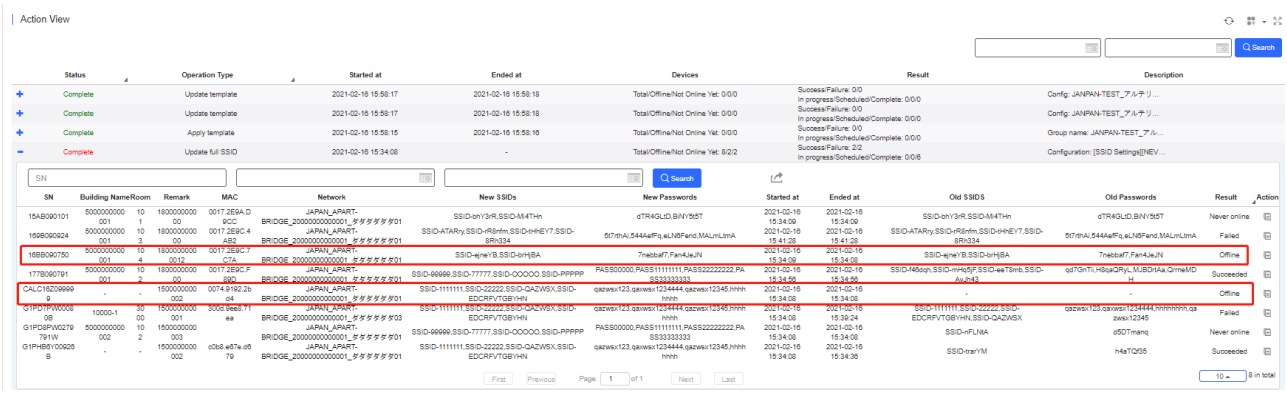
The exported file is shown as the figure below.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	SSID and Password Change Form (Output)												
2	NO.	Building Name	Room No	Remark	MAC	Network	New SSID	New SSID Password	Started	Ended	Old SSID	Old SSID Password	Result
3	1				0011.2233.445	jok_apartment	ID-73rj5t,SSID-yH67	B6BFJAba,GnbH4jty	2021 12/24 12:40	2021 12/24 12:40			Succeeded
4													

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

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

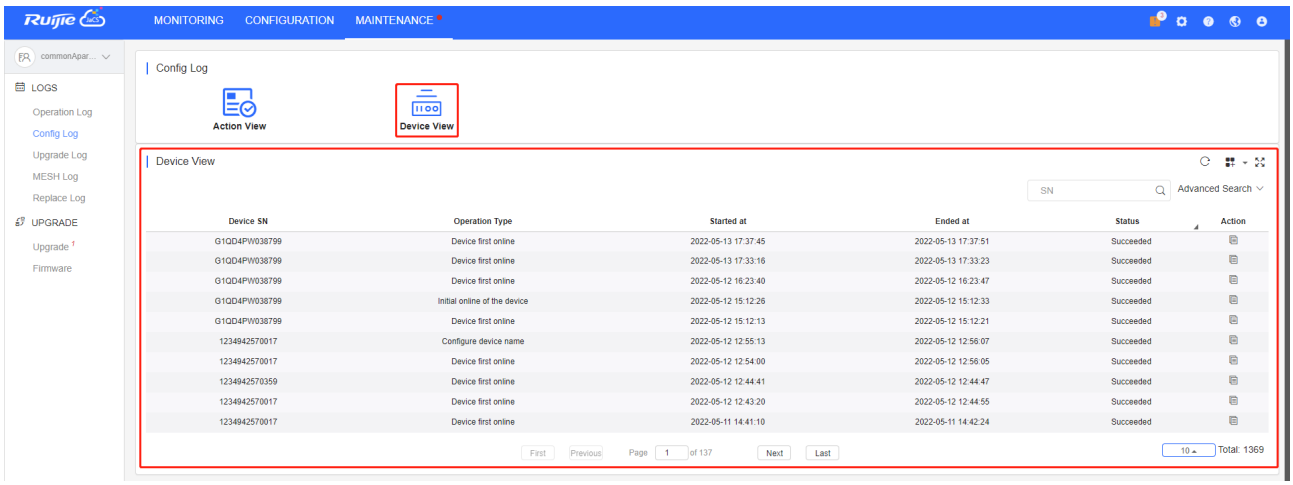
Suppose the operator changes the SSIDs and passwords of two rooms and exports the result.



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.

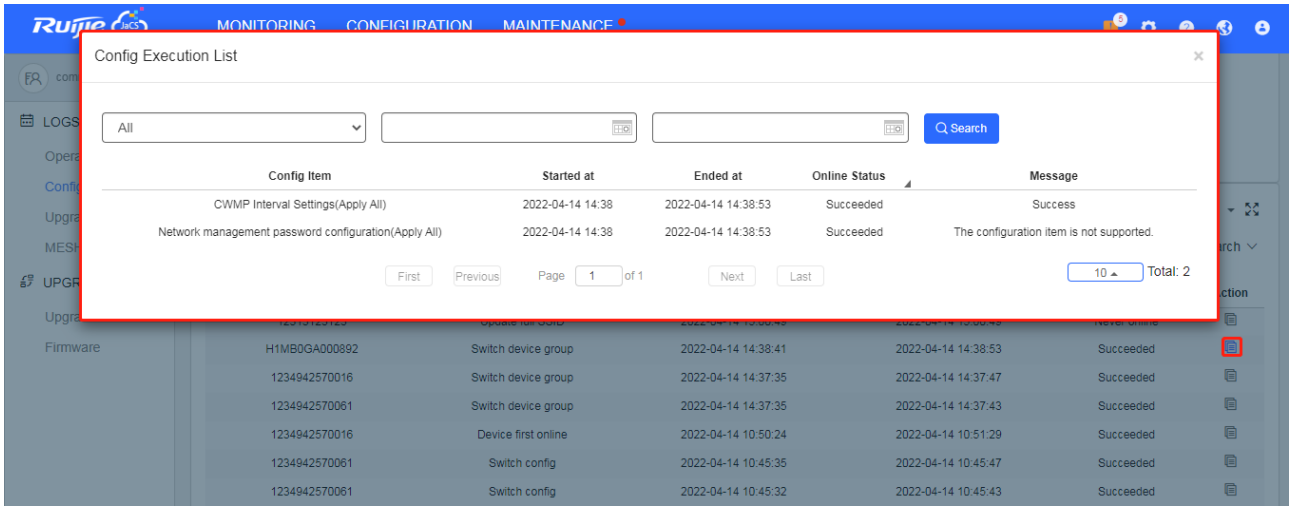
A	B	C	D	E	F	G	H	I	J	K	L	M
SSID and Password Change Form (Output)												
ID	Building Name	Room	Remark	MAC	Network	New SSIDs	New Passwords	Started	Ended	Old SSIDs	Old Passwords	Result
1	5000000000001	101	180000000000	0017.2E9A.D9CC	)GE_20000000000	-bhY3rR,SSID-Mi	TR4GLtD,BiNY5t5	2021 02/16 15:34	2021 02/16 15:34	)-bhY3rR,SSID-Mi	TR4GLtD,BiNY5t5	Never online
2	5000000000001	103	180000000000	0017.2E9C.4AB2	)GE_20000000000	-rR8nfm,SSID-tHI	AefFq,eLN6Fend,	2021 02/16 15:41	2021 02/16 15:41	)-rR8nfm,SSID-tHI	AefFq,eLN6Fend,	Failed
3	5000000000001	104	180000000000012	0017.2E9C.7C7A	)GE_20000000000	-ejneYB,SSID-brI	nebbaf7,Fan4JeJI	2021 02/16 15:34	2021 02/16 15:34	)-ejneYB,SSID-brI	nebbaf7,Fan4JeJI	Offline
4	5000000000001	102	180000000000	0017.2E9C.F89D	)GE_20000000000	(-77777,SSID-OOC	111111,PASS222	2021 02/16 15:34	2021 02/16 15:34	-mHq5jF,SSID-ee	TqaQRyL,MJBDrtA	Succeeded
5			1500000000002	0074.9192.2bd4	)GE_20000000000	22,SSID-QAZWSX	sx1234444,qazws	2021 02/16 15:34	2021 02/16 15:34			Offline
6	10000-1	3000	1500000000001	300d.9ee8.71ea	)GE_20000000000	22,SSID-QAZWSX	sx1234444,qazws	2021 02/16 15:34	2021 02/16 15:39	22,SSID-EDCRFV	sx1234444,hhhhhh	Failed
7	5000000000002	102	1500000000003		)GE_20000000000	(-77777,SSID-OOC	111111,PASS222	2021 02/16 15:34	2021 02/16 15:34	SSID-nFLNtA	d5DTmanq	Never online
8			1500000000002	c0b8.e67e.d679	)GE_20000000000	22,SSID-QAZWSX	sx1234444,qazws	2021 02/16 15:34	2021 02/16 15:34	SSID-trarYM	h4aTQf35	Succeeded

7.1.2.3 Device View



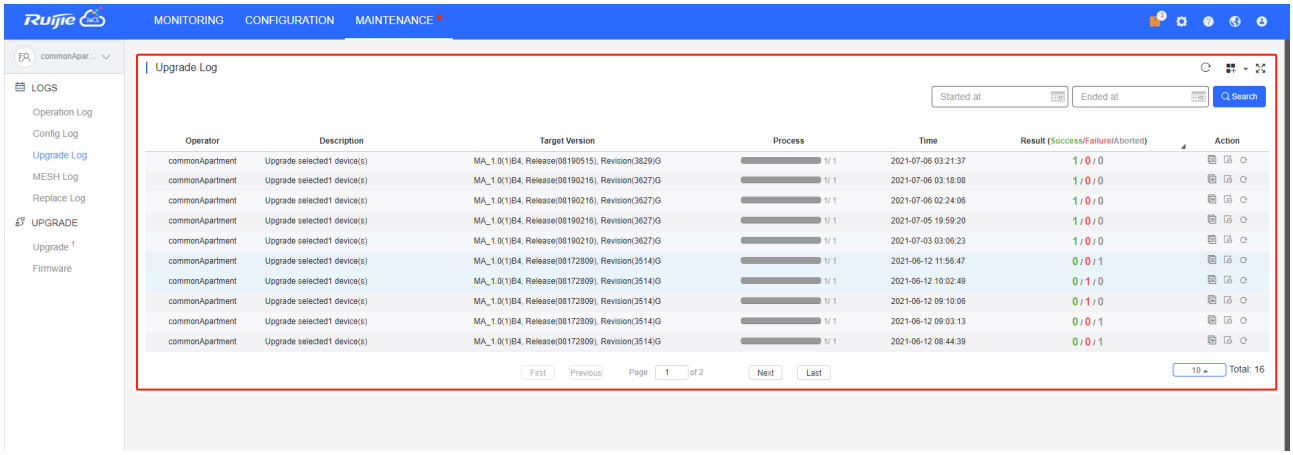
Click in the **Action** column to check the push status of each configuration item.

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

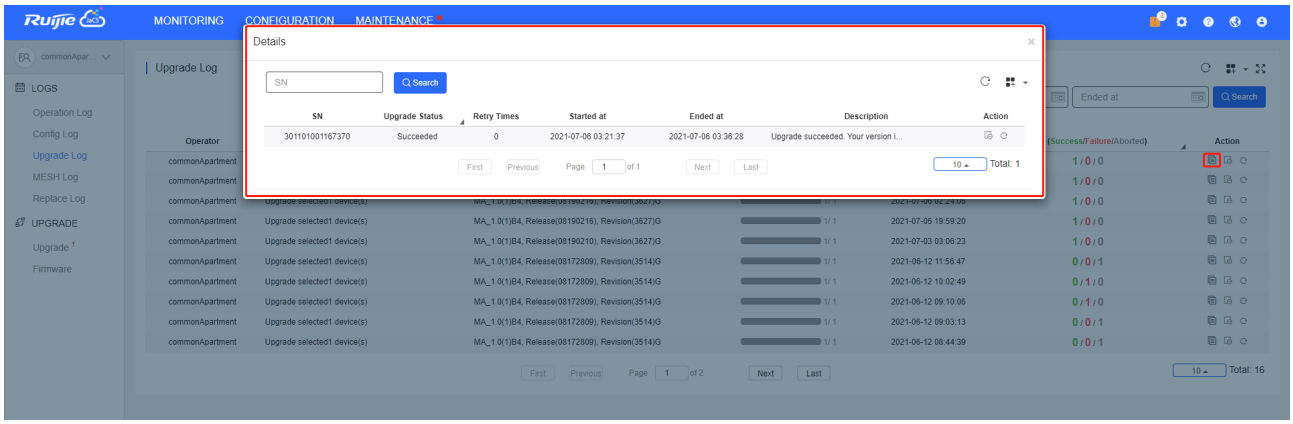
This part provides the upgrade tracing function. You can check the upgrade status, and abort or retry the upgrade.



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.

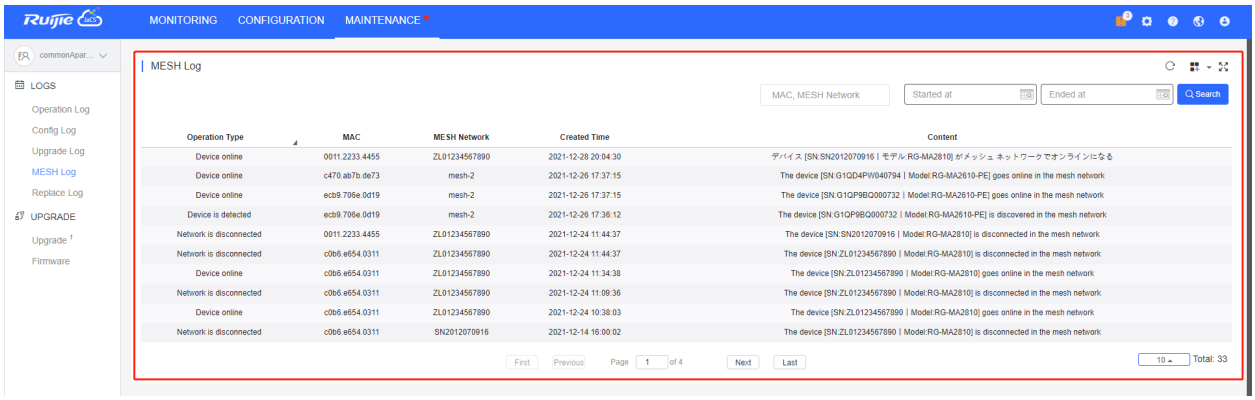
Abort: Stop the upgrade task.

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

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

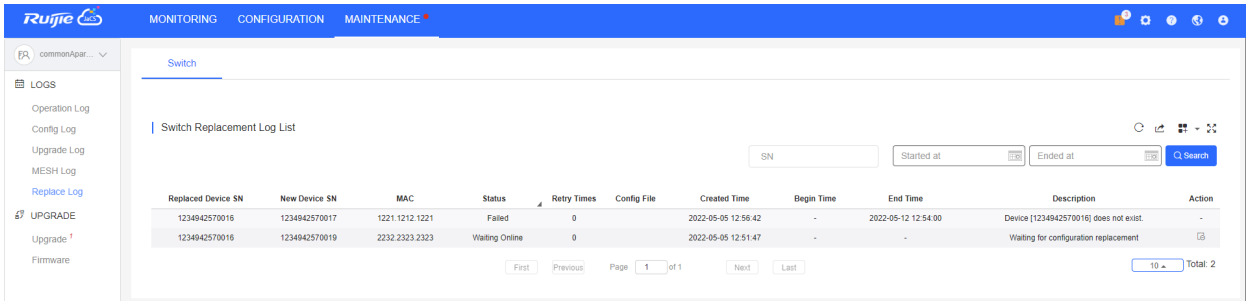
7.1.4 Mesh Log

The page displays the Mesh logs.



7.1.5 Replace Log

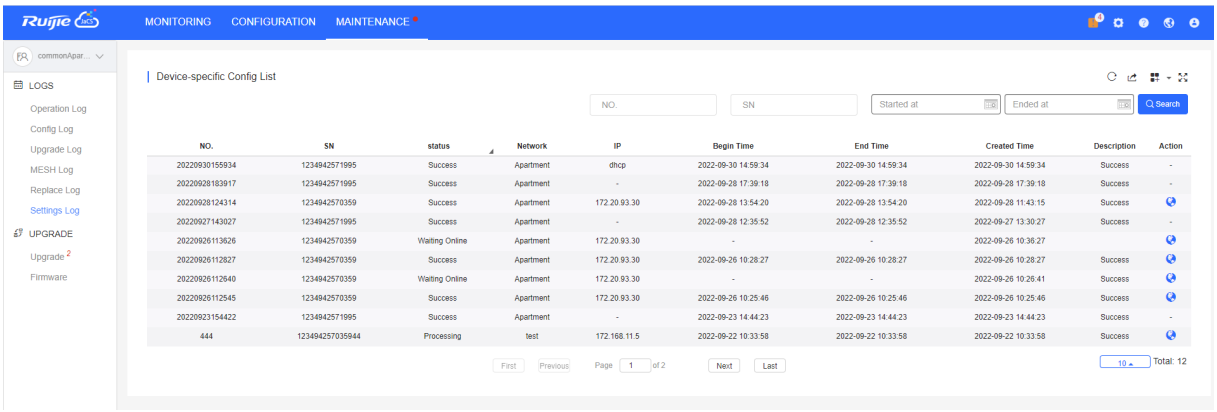
The page displays the replacement log of switches.



7.1.6 Settings Log

This page displays the information of device-specific configuration, including imported batch number, SN, Status, Network, IP address, Begin Time, End Time, Created Time, Description and Actions.

- Configuration status is displayed in the Status column：
- Processing: The configuration is in progress.
- Failed: The configuration failed to be applied to the device.
- Succeeded: The configuration has been applied to the device.
- Waiting online: The device is waiting to go online.
- The batch number and SN can be used for search.
- You can click in the **Action** column to jump to the Web of the device.



7.2 Upgrade

The following tab pages are provided for device firmware management:

- Upgrade
- Firmware

7.2.1 Upgrade

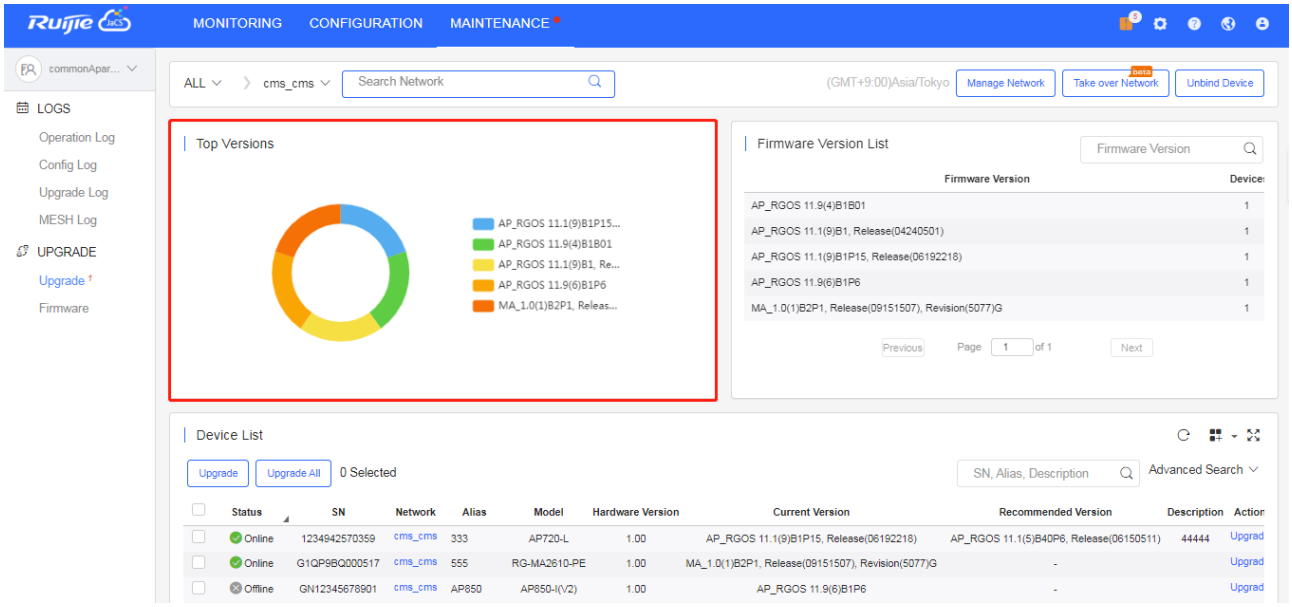
Ruijie JaCS supports the online upgrade of device firmware, and it allows network administrators to utilize the latest features and security enhancement for their Ruijie devices. Online upgrade allows administrators to easily arrange the firmware upgrade on their networks and view firmware releases.

The **Upgrade** page includes two modules:

- Version statistics
- Firmware upgrade
- Device List

7.2.1.1 Check Version Information

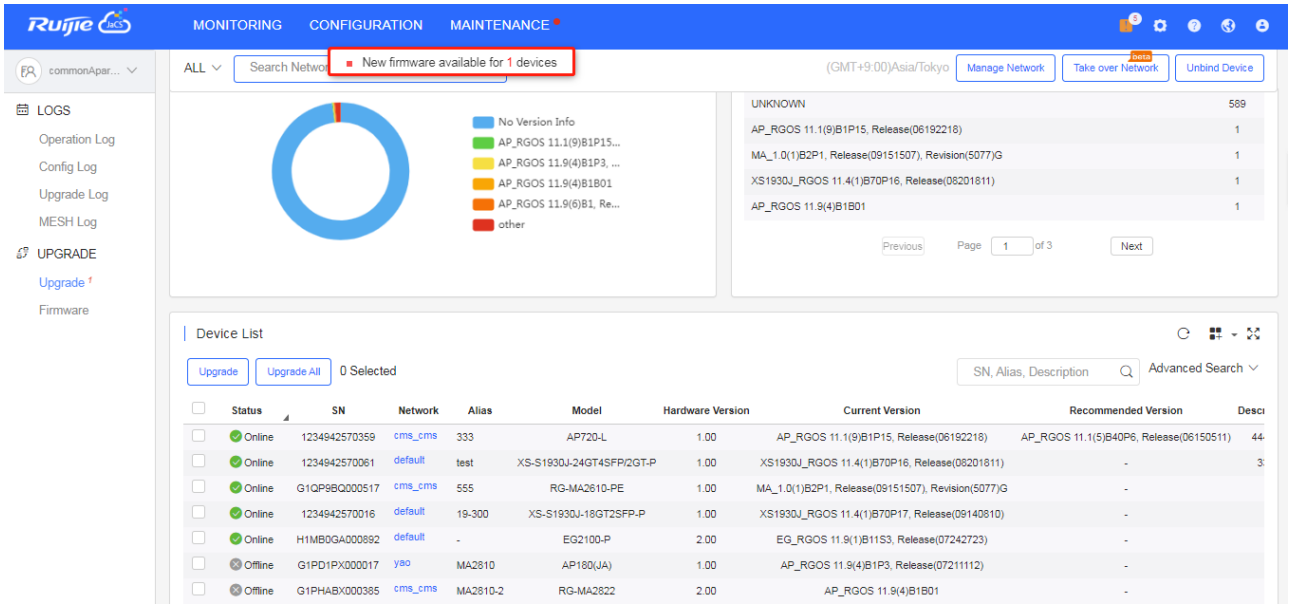
Select **Maintenance** > **Upgrade** to display the top 5 versions in pie chart form and a list for each network.



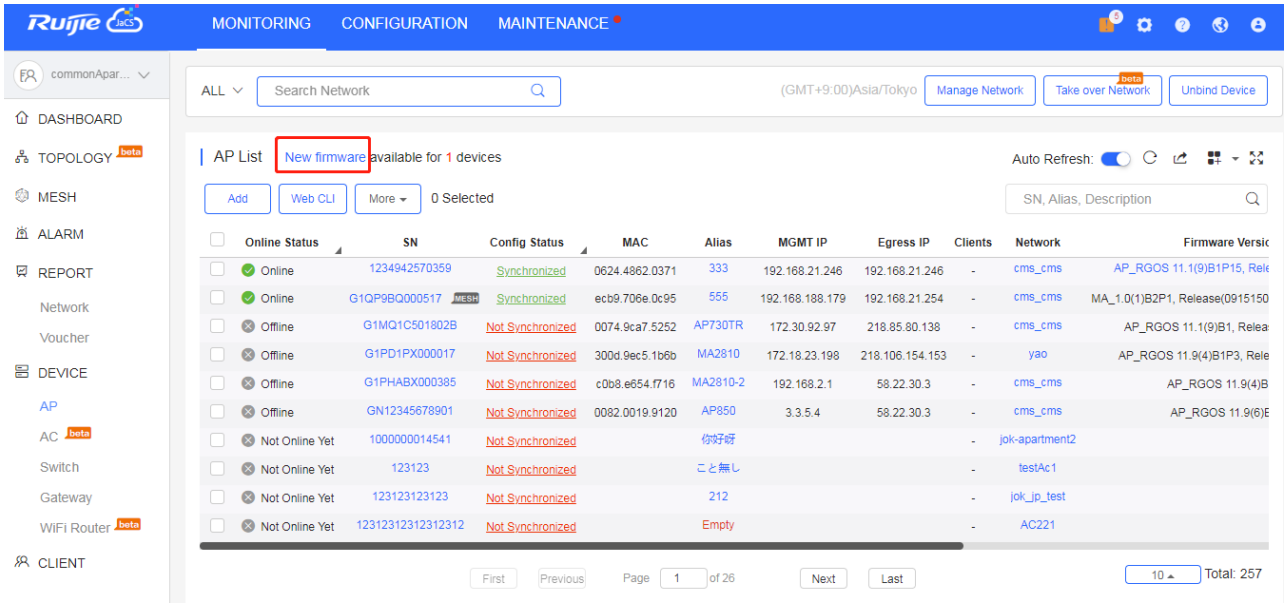
7.2.1.2 Upgrade

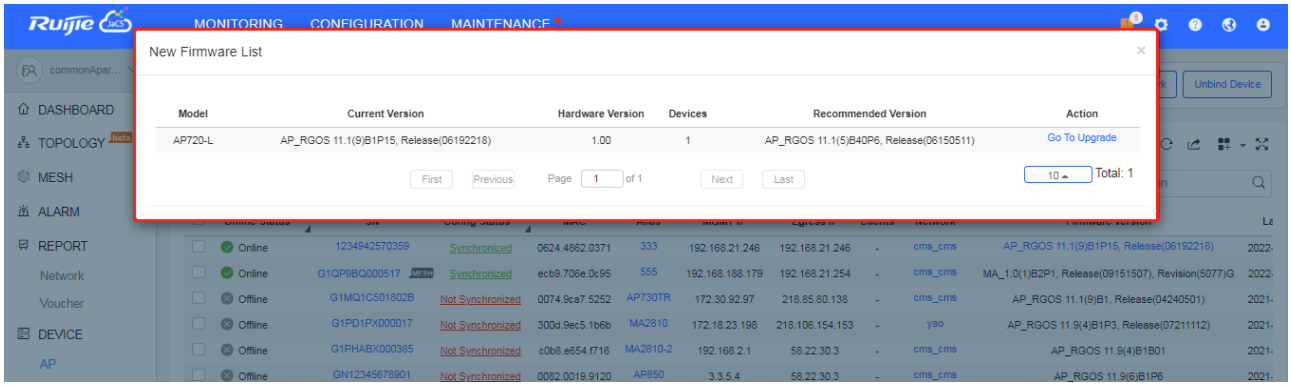
You can enter the **Upgrade** page in either of the following ways.

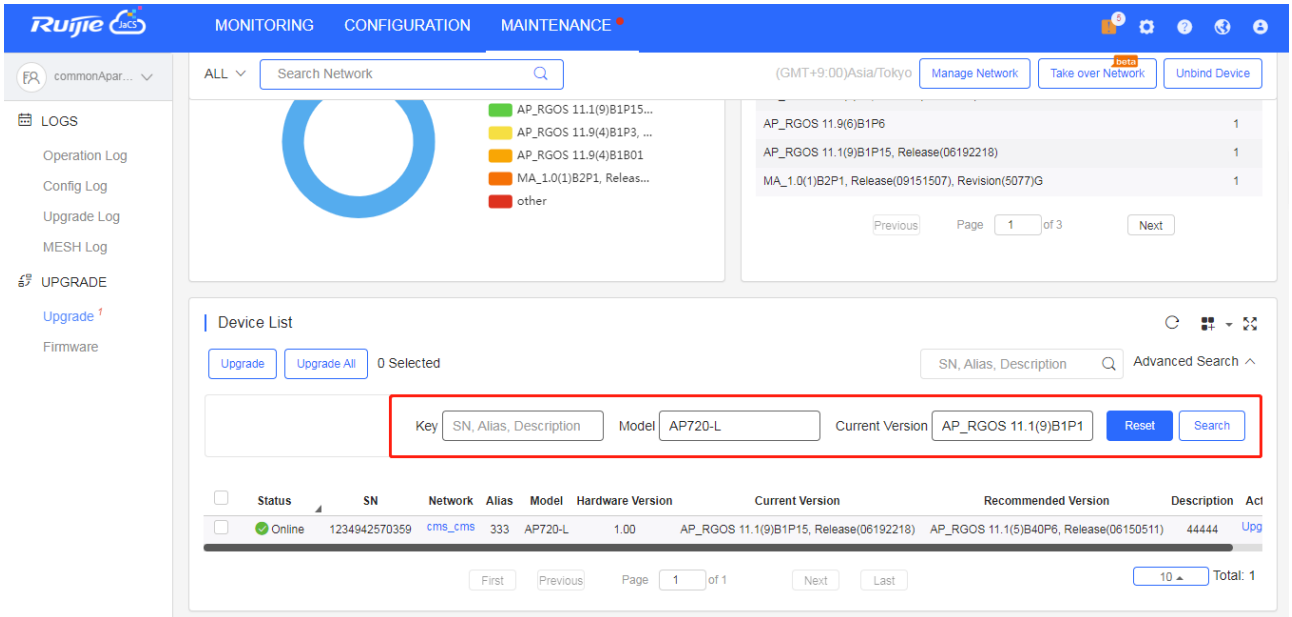
Method 1: Hover the mouse over **MAINTENANCE**, a link will appear. Click the link to enter the **Upgrade** page. The default network information is **All**.



Method 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**.







7.2.1.3 Upgrade Devices

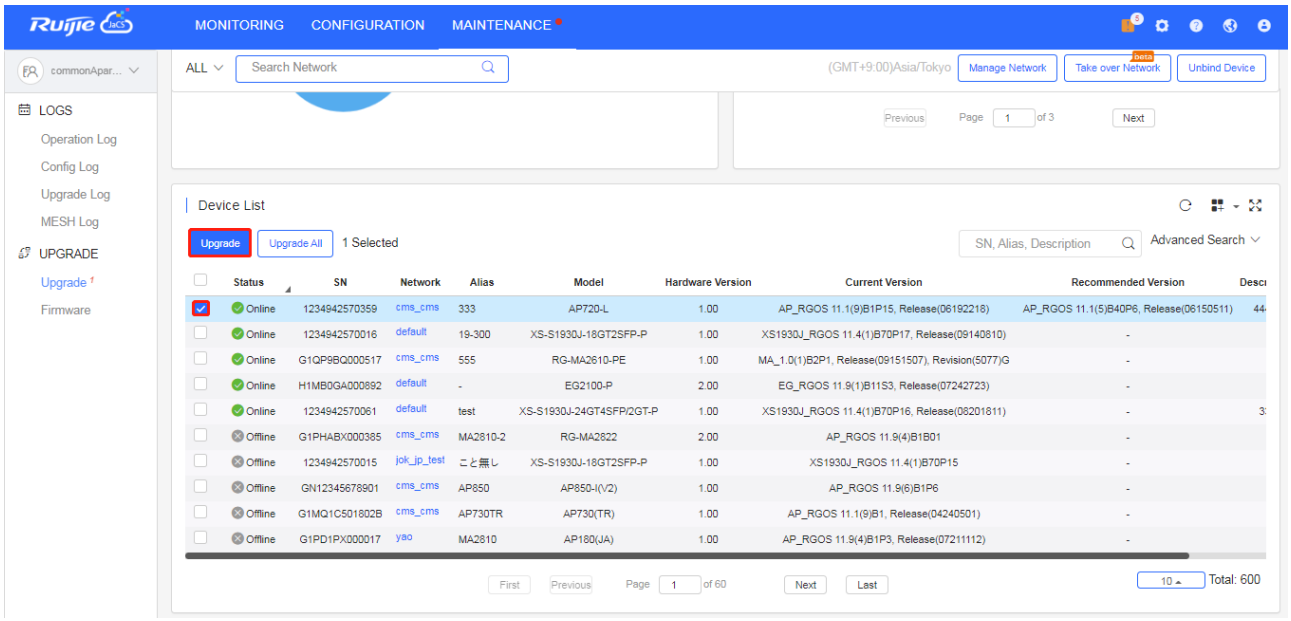
For convenience, two upgrade modes are provided:

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.

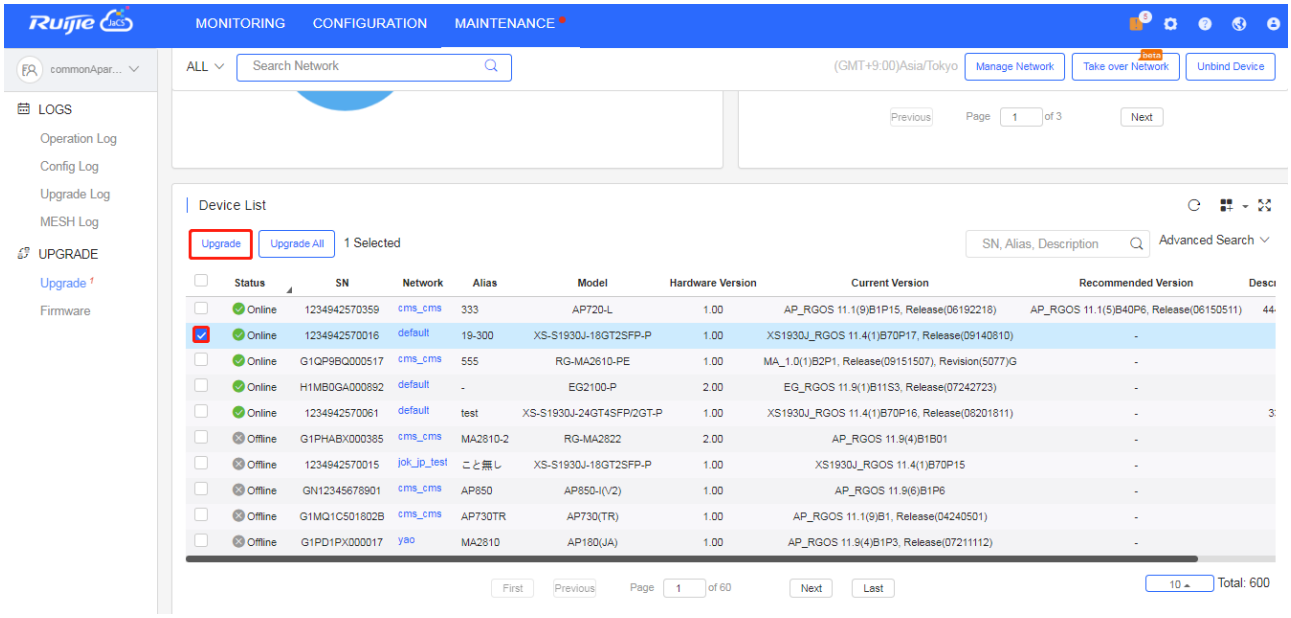
- **Upgrade Selected**

Step 1: Select a network on the left, select a target AP, and click **Upgrade.**



Step 2: Select a firmware version.

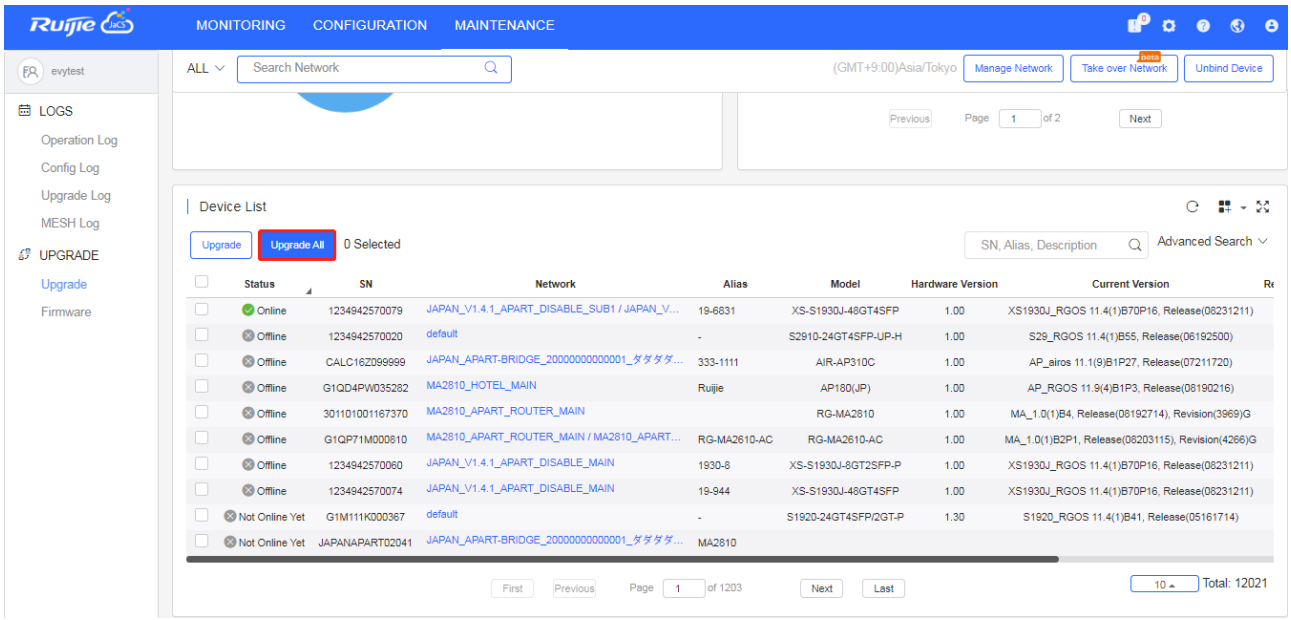
On the **Equipment Upgrade** page, you can check the device information and the details of versions, choose a version (the recommended version is the latest one), enable scheduled upgrade and set retry times if the upgrade fails.



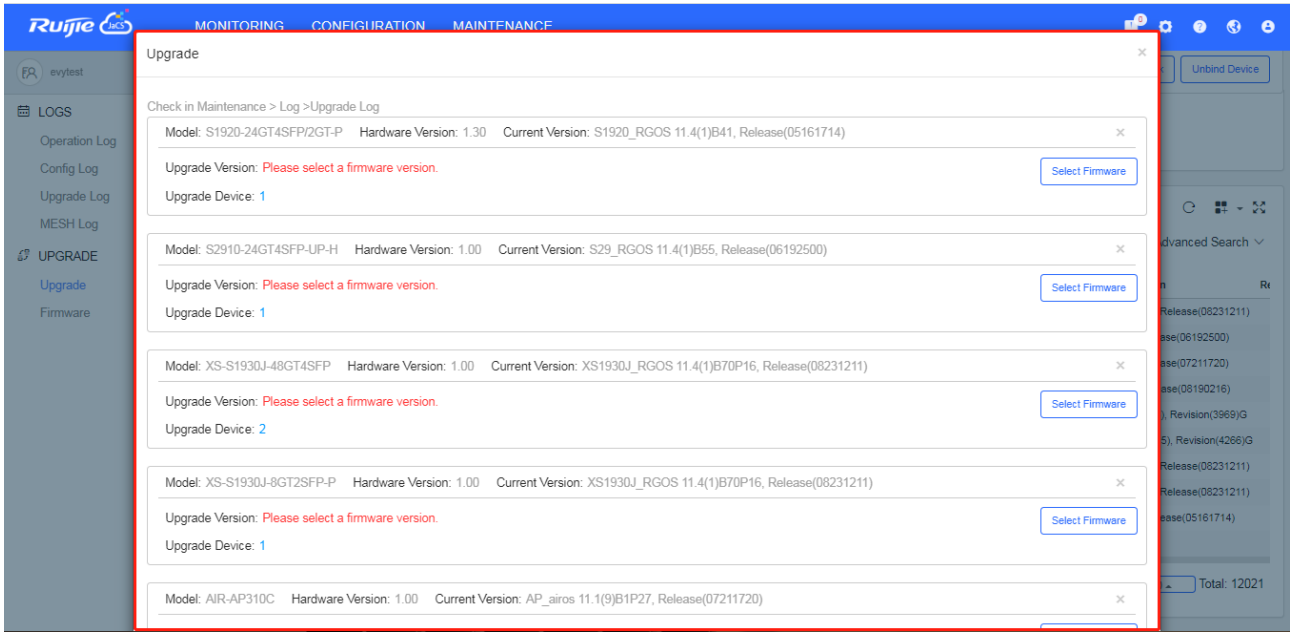
Step 3: Upgrade the selected APs

- **Upgrade All**

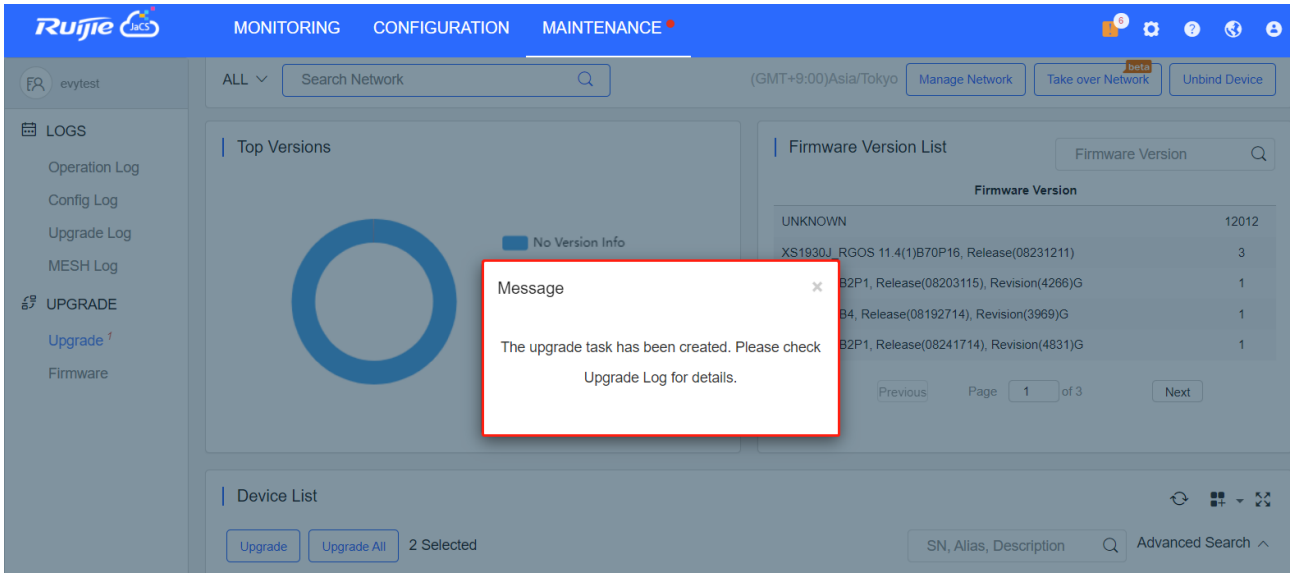
Step 1: Check the devices list based on a condition, and click **Upgrade All.**

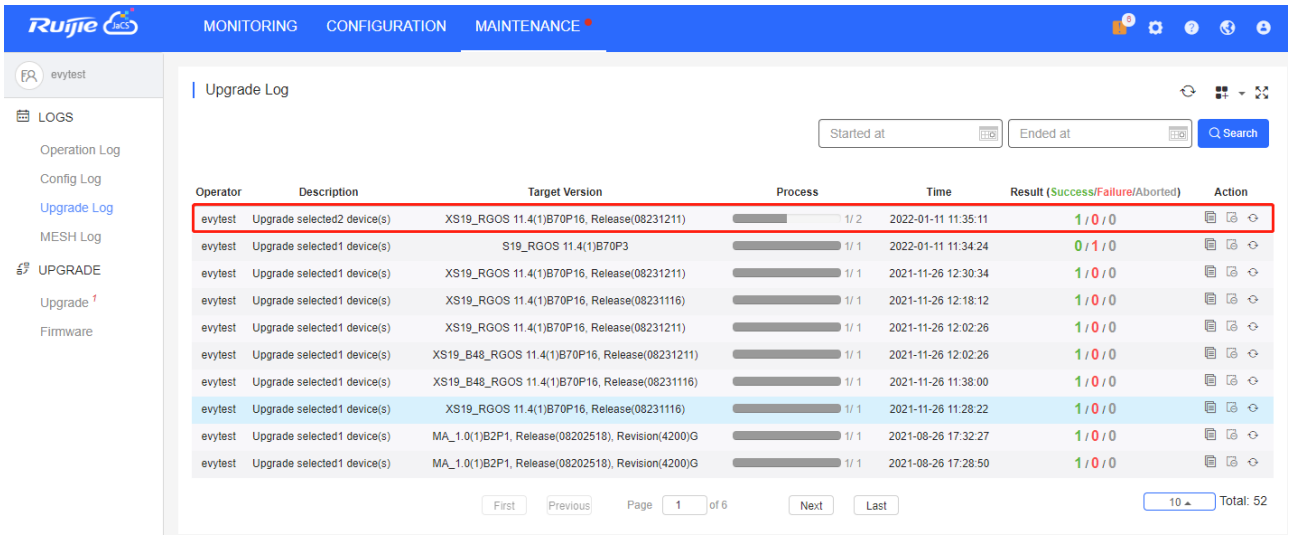


Step 2: Select the version and click **Start Upgrade**

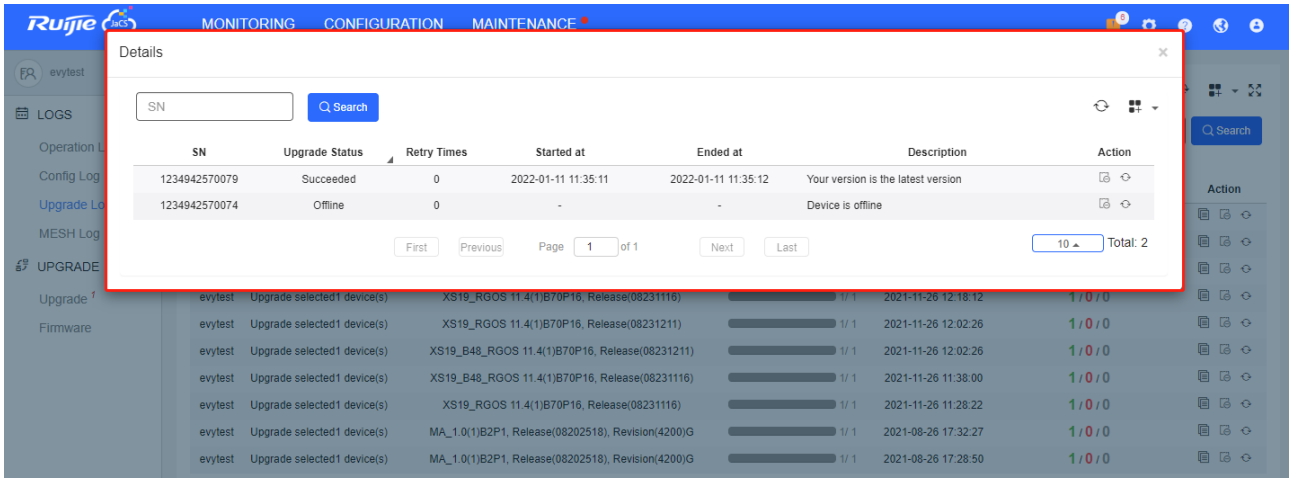


Set the update criteria and click **Start Upgrade**, and a message box will pop up. Users can check details in **LOGS > Upgrade Log**.

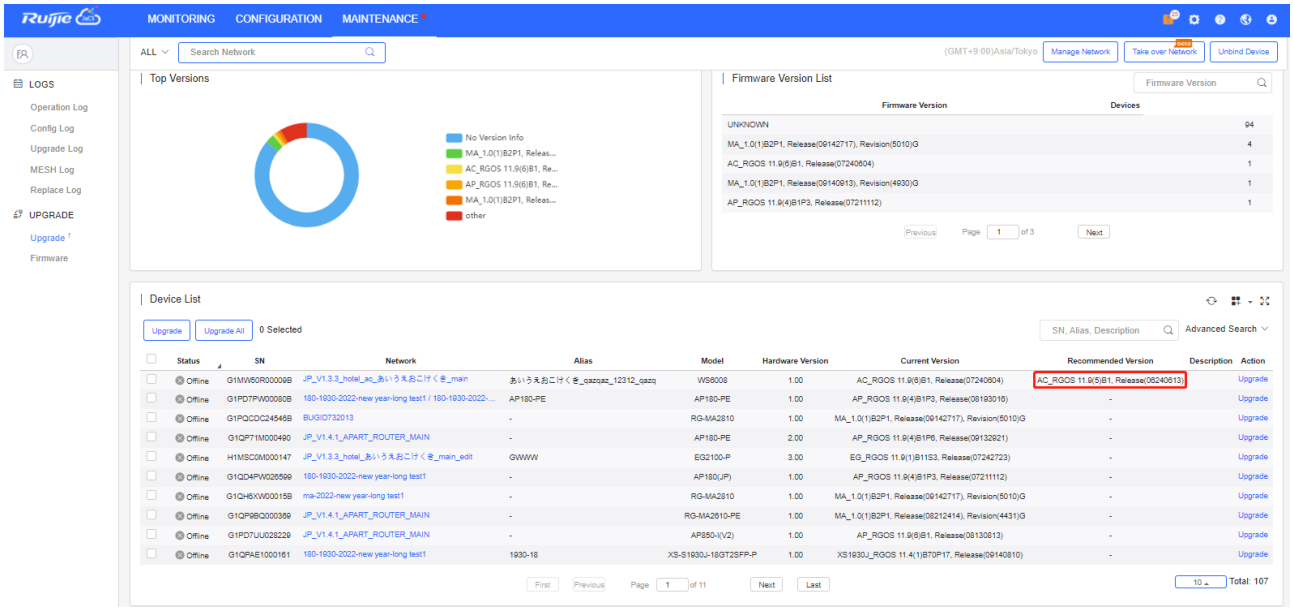




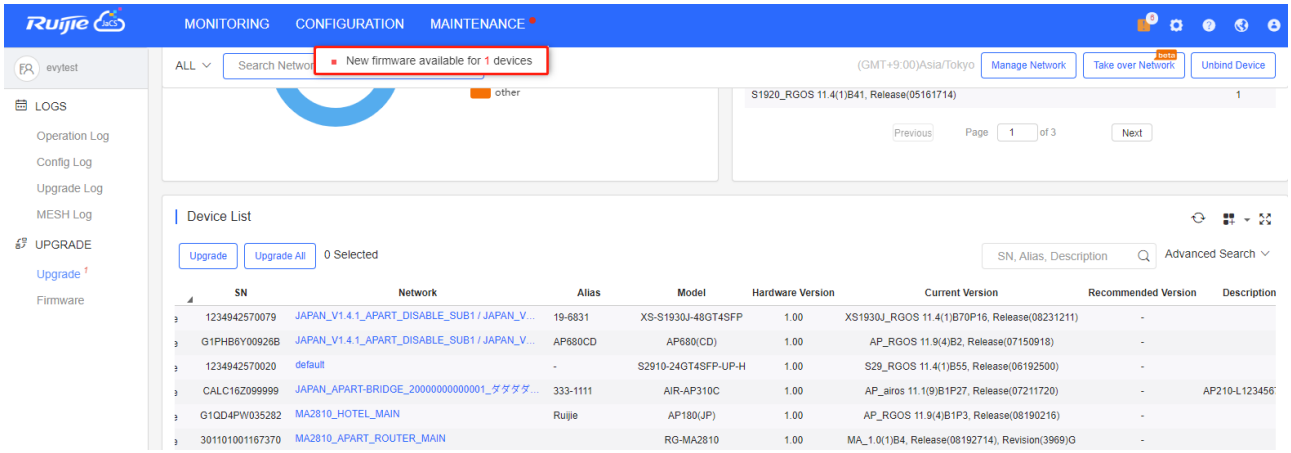
If the upgrade is successful, log will show **Upgrade succeeded**.



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



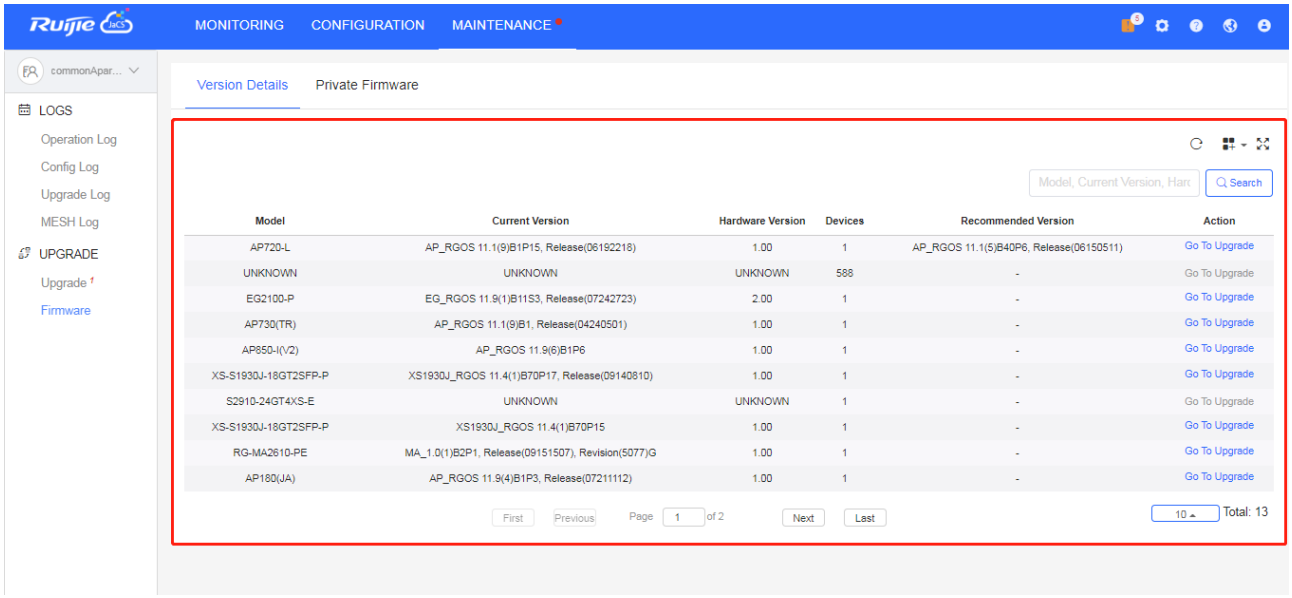
The numbers of devices which have available firmware for upgrade in **MAINTENANCE** Menu and **Upgrade** in Navigation Bar will change accordingly.



7.2.2 Firmware

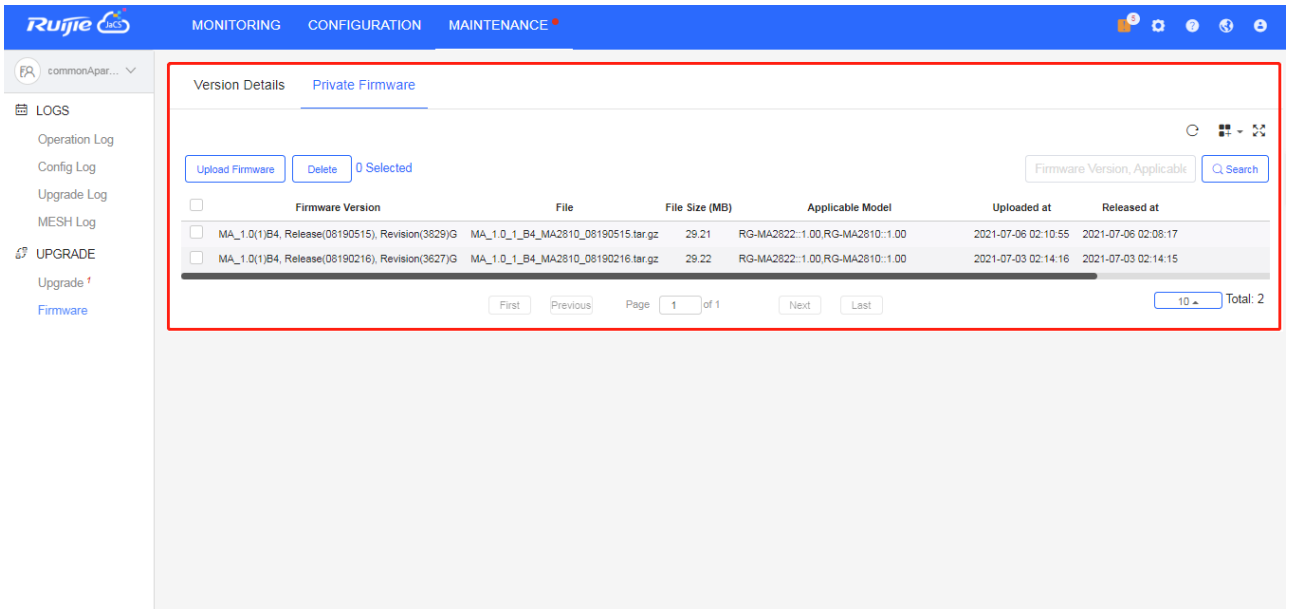
7.2.2.1 Version Details

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.

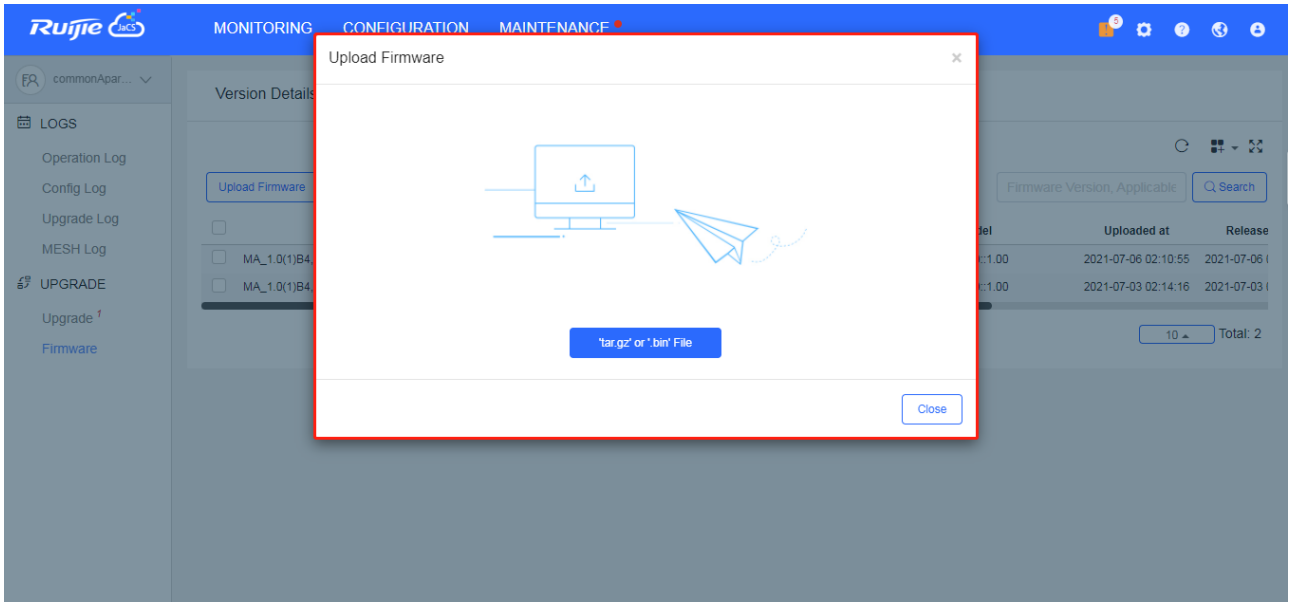


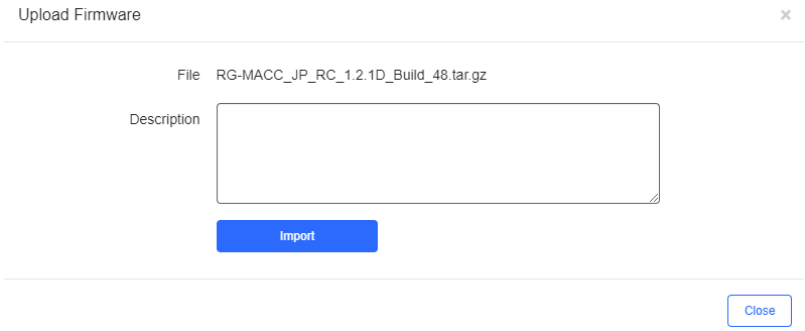
7.2.2.2 Private Firmware

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

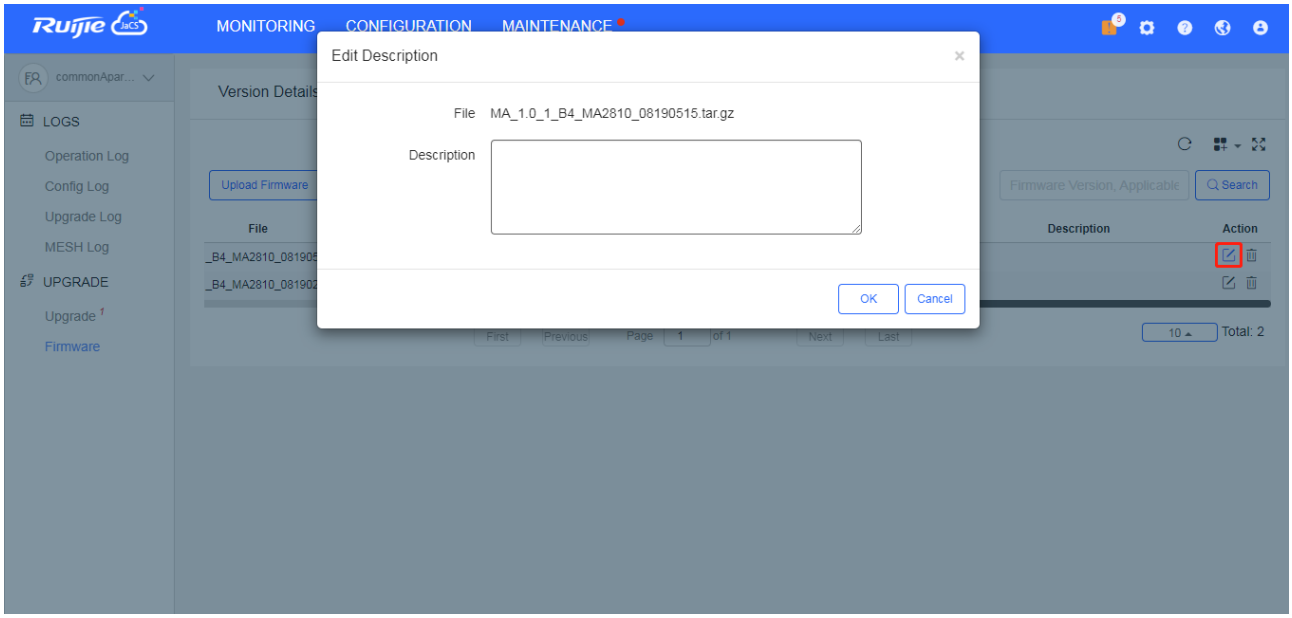


Click **Upload Firmware** to upload private firmware.

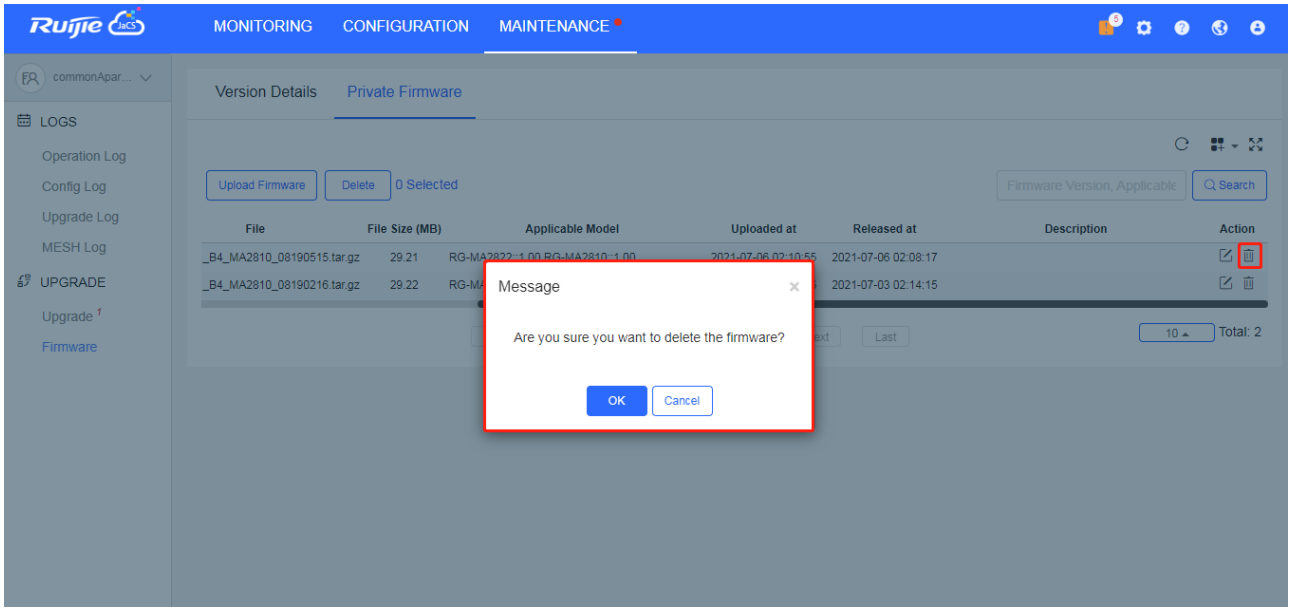




Click  in the **Action** column to edit the **Description** of firmware.



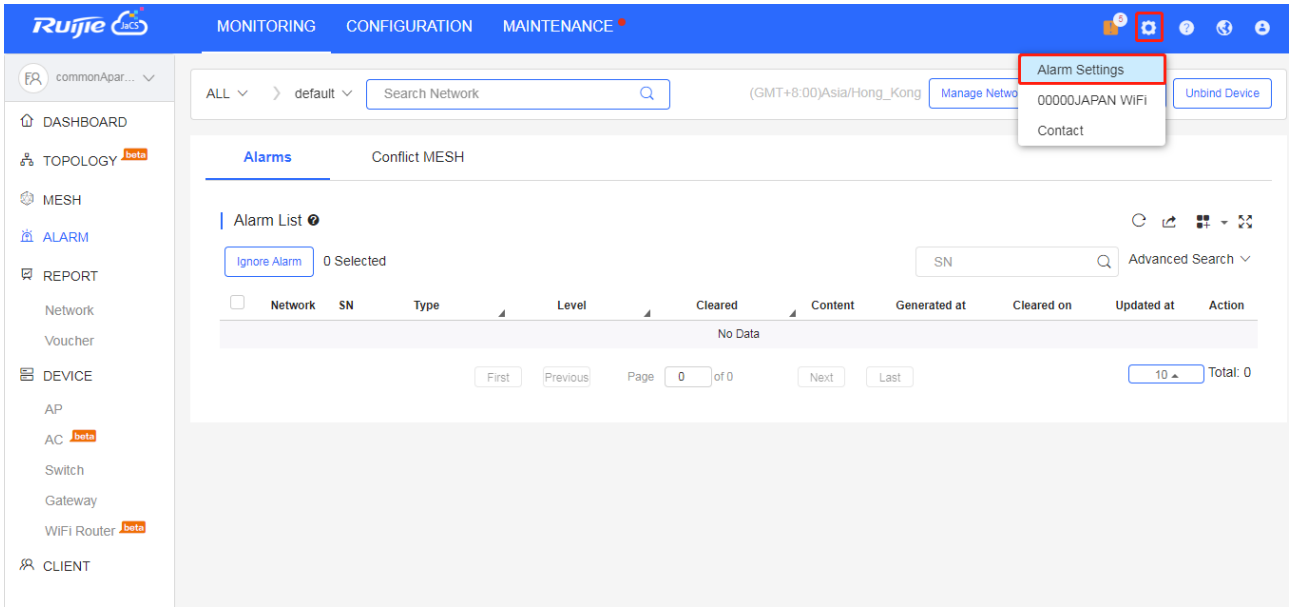
Click **Delete** or  in the **Action** column to delete private firmware.



8 System Settings

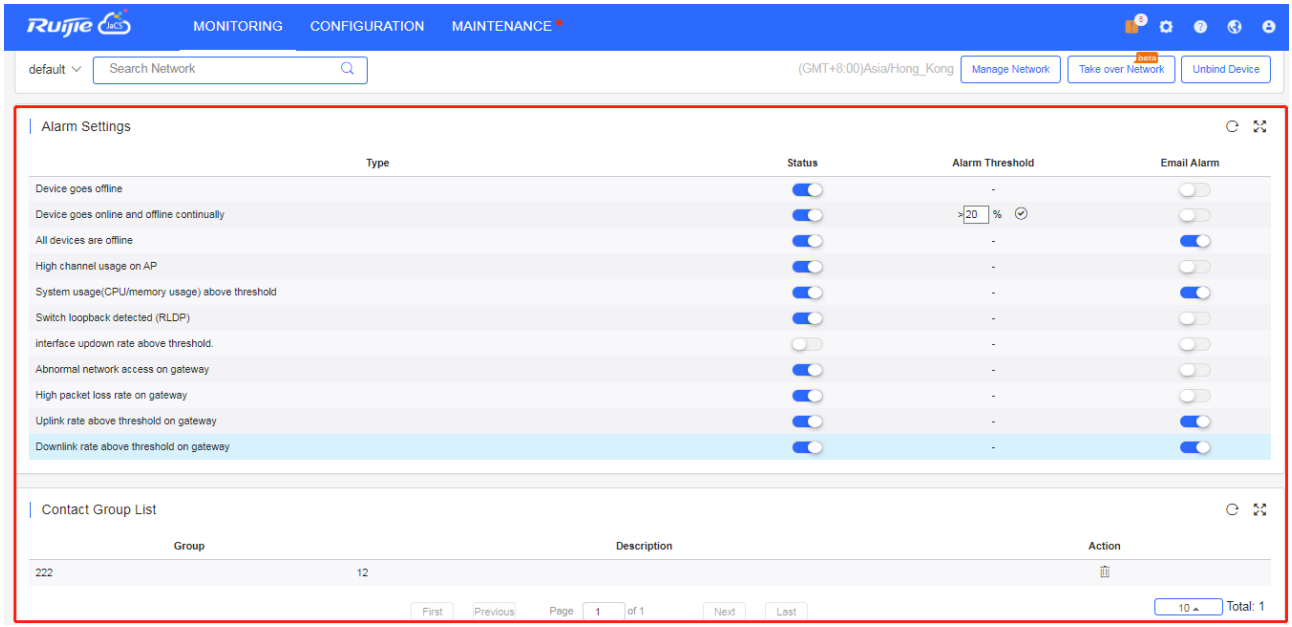
8.1 Alarm Settings

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.



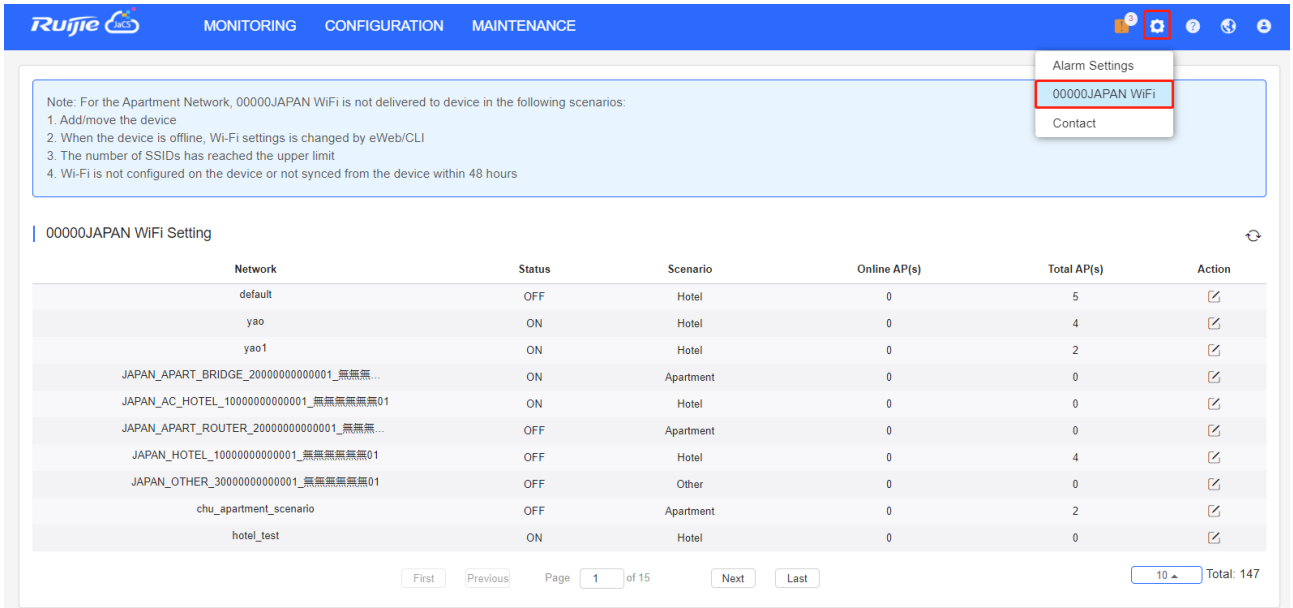
To use the **Email Alarm** function, click and select **System Settings** to preset the account and password of the SMTP server for sending Emails on the **Advanced** page via the administrator account.

8.2 00000JAPAN WiFi

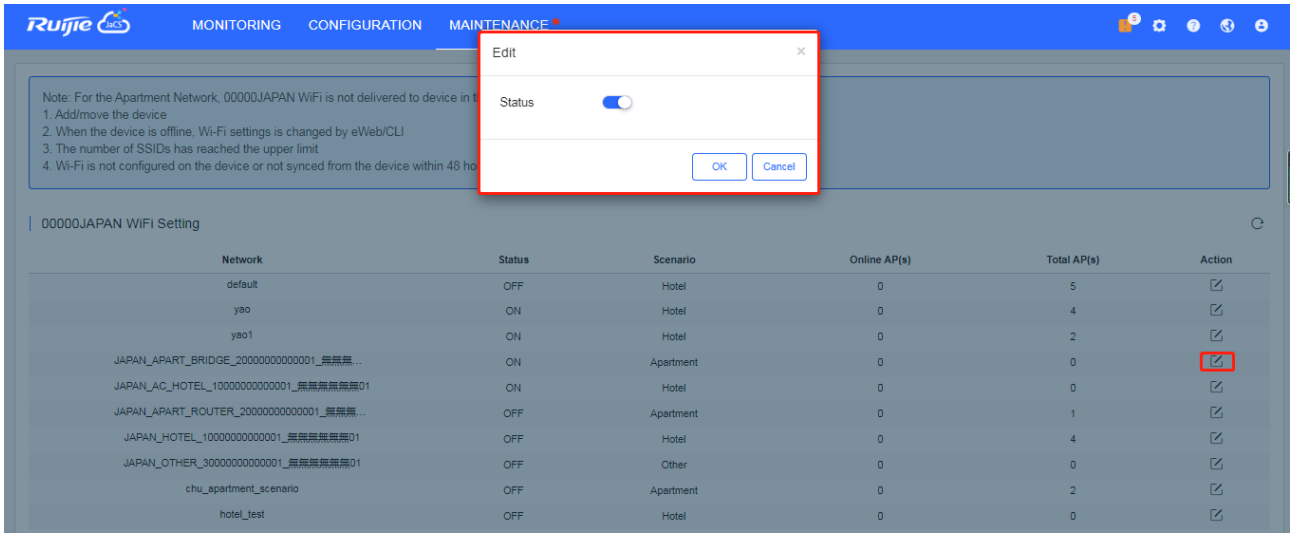
00000JAPAN WiFi is a free Wi-Fi with no requirement for authentication. In disaster, it can be quickly enabled and deployed to provide Internet access.

00000JAPAN WiFi can be enabled by one click. As long as the layer-1 network is enabled, the devices of this network and its sub networks will be turned on as well. When the layer-1 network is disabled, the devices will be turned off.

Click in the upper right corner, and select **00000JAPAN WiFi** to open the configuration page.



Click  in the **Action** column to edit the 00000JAPAN WiFi setting.

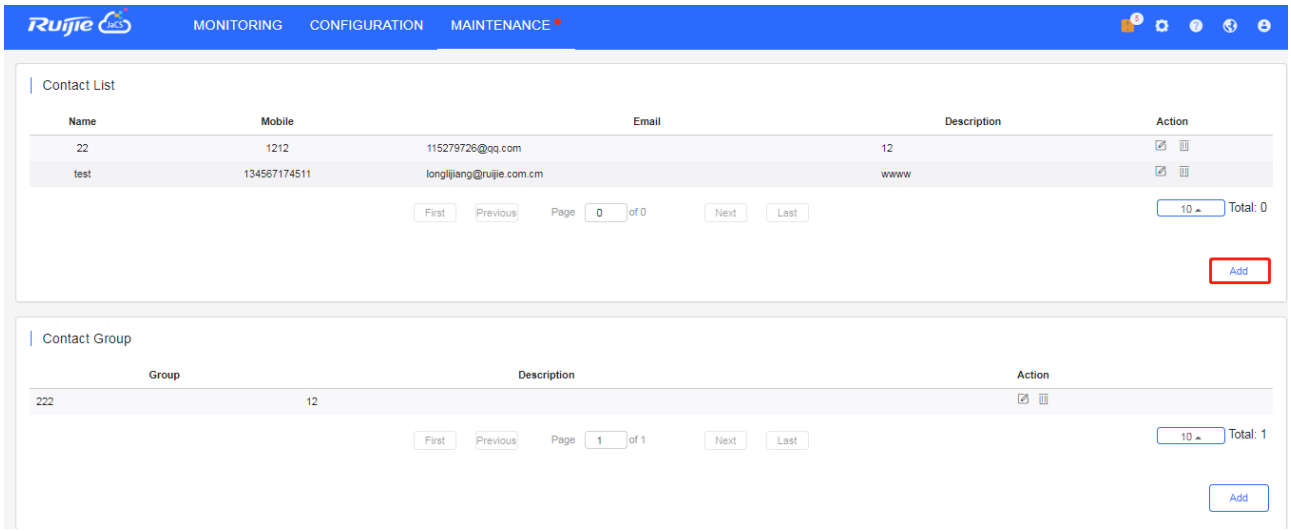


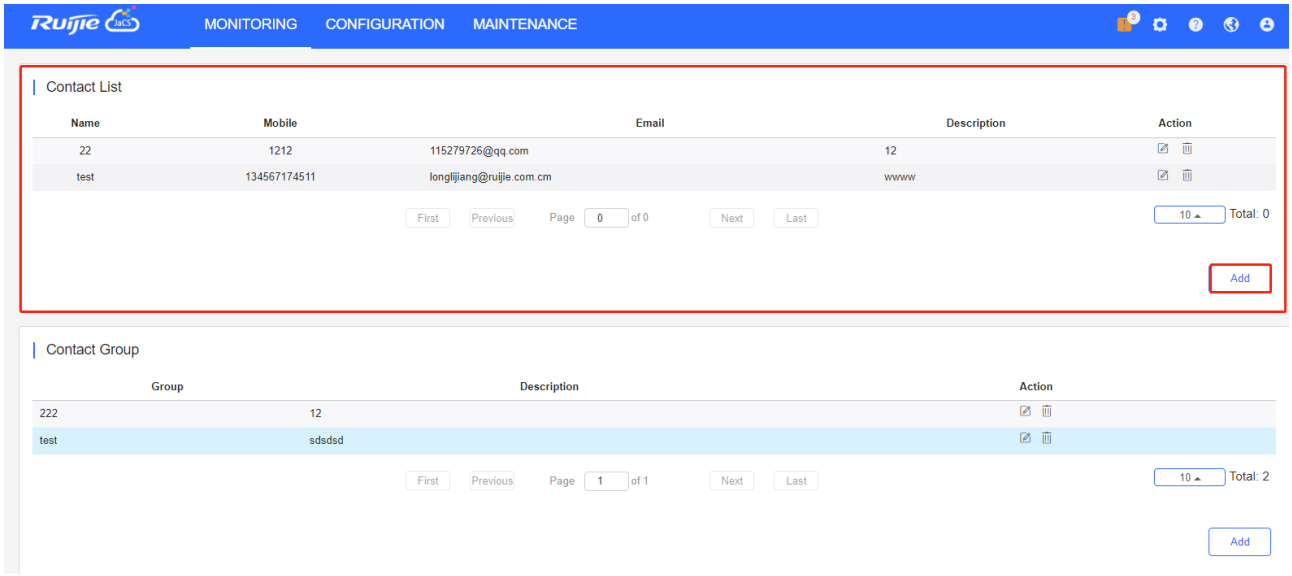
8.3 Contact

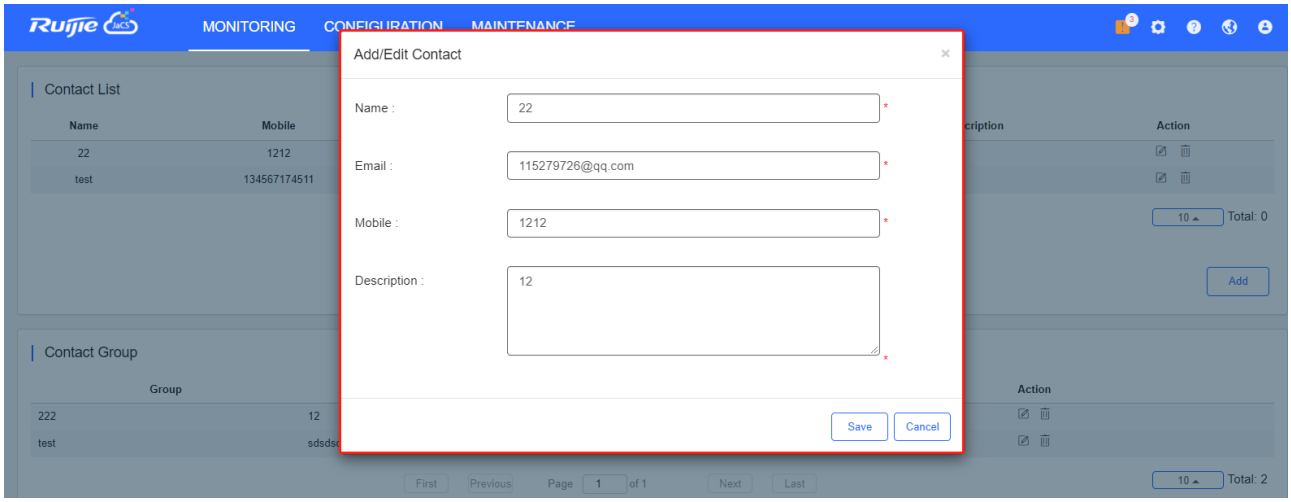
On the **Contact** page, you can create contact groups, and add contacts to contact groups.

8.3.1 Contact List

Add a contact as the Email recipient.

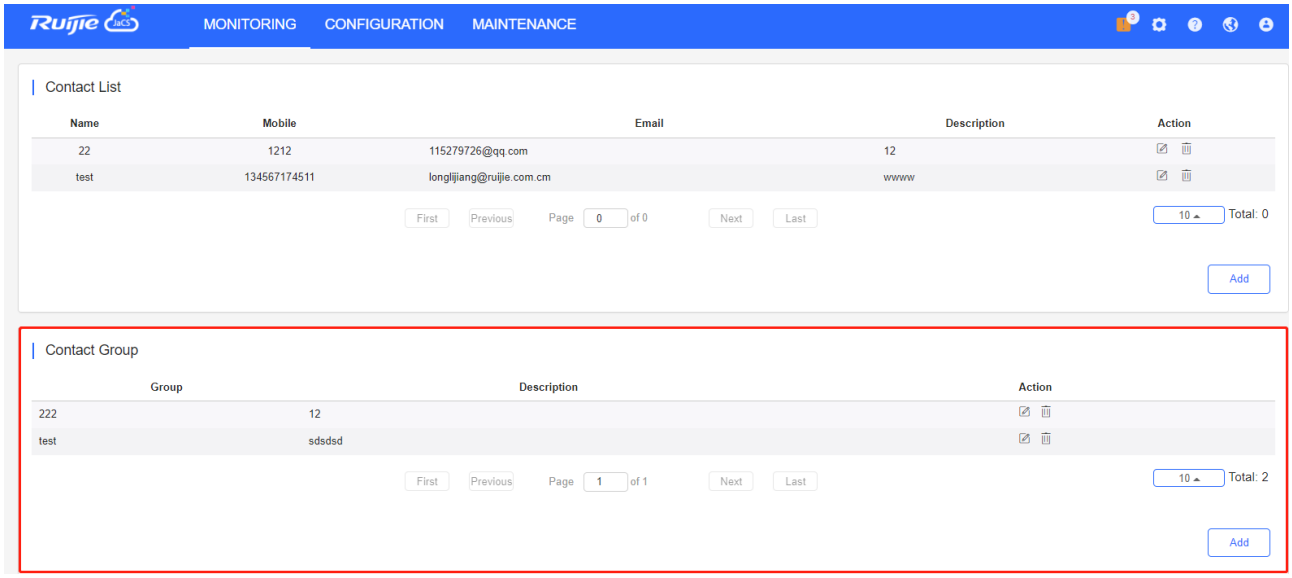


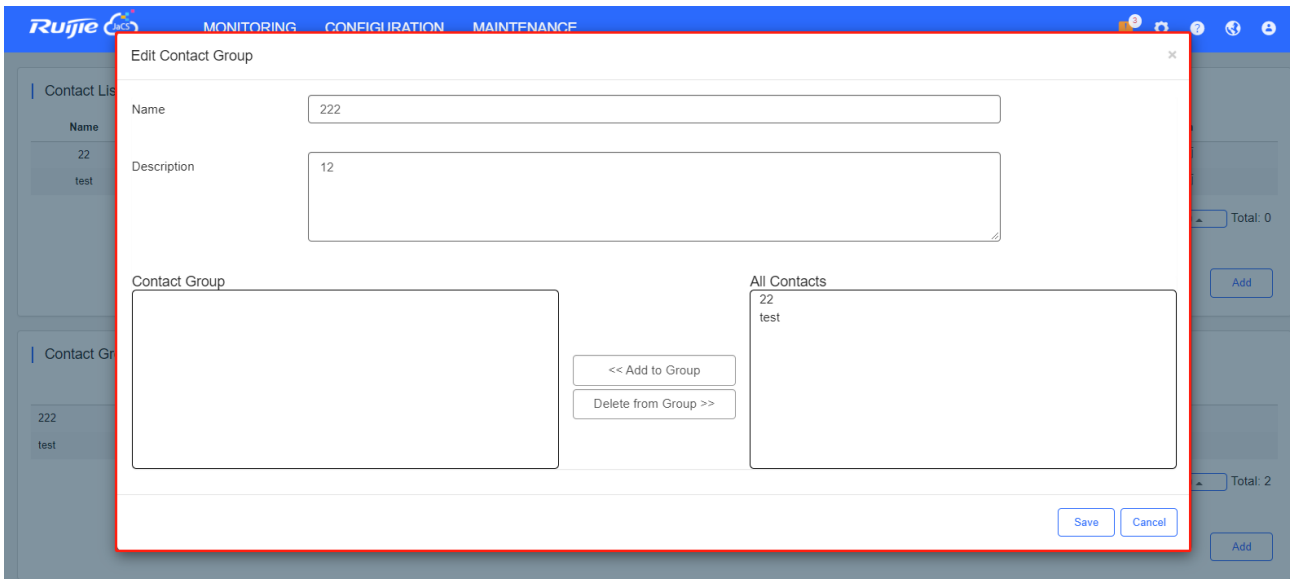




8.3.2 Contact Group

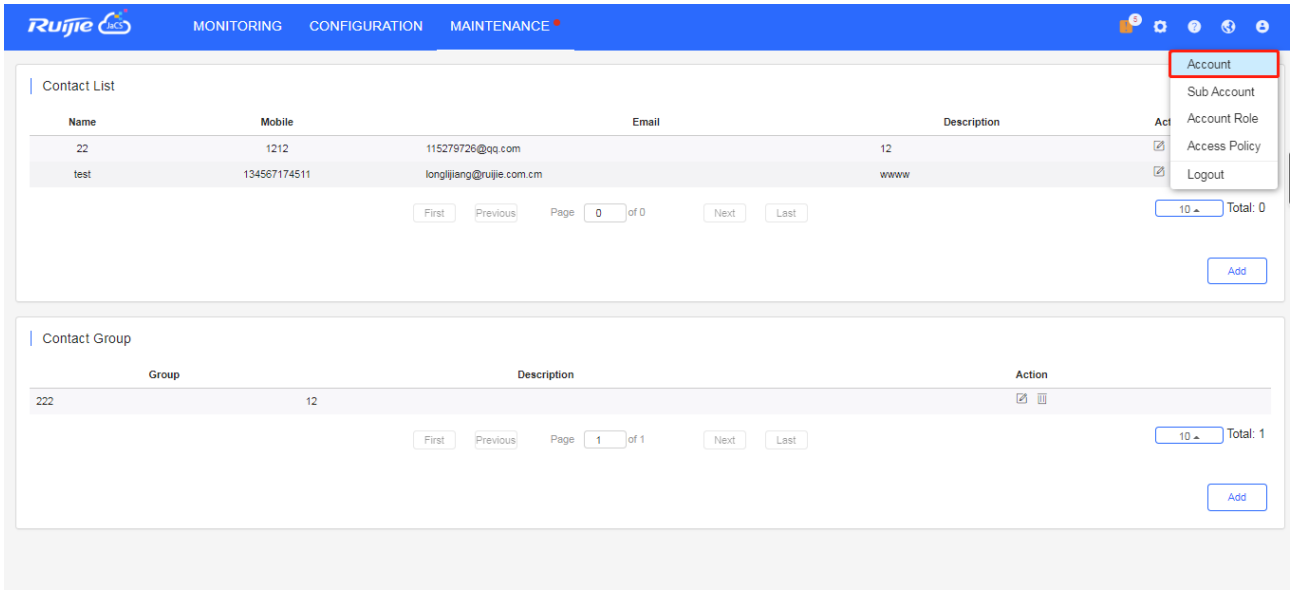
Add a group and move the contacts to the group.


MONITORING
CONFIGURATION
MAINTENANCE
Contact List
Name
Mobile
Email
Description
Action
22
1212
115279726@qq.com
12
test
134567174511
longlijiang@ruijie.com.cn
wwww
First
Previous
Page
0
of 0
Next
Last
10
Total: 0
Add
Contact Group
Group
Description
Action
222
12
test
sdsdsd
First
Previous
Page
1
of 1
Next
Last
10
Total: 2
Add


MONITORING
CONFIGURATION
MAINTENANCE
Edit Contact Group
Name
222
Description
12
Contact Group
All Contacts
22
test
<< Add to Group
Delete from Group >>
Save
Cancel

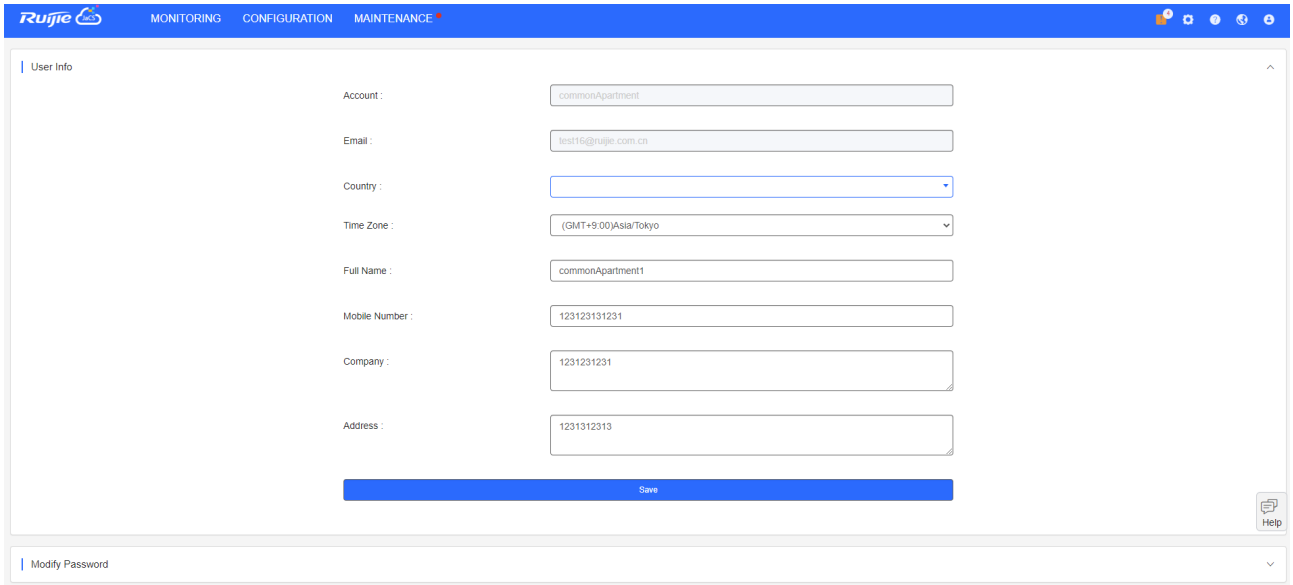
9 Account

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



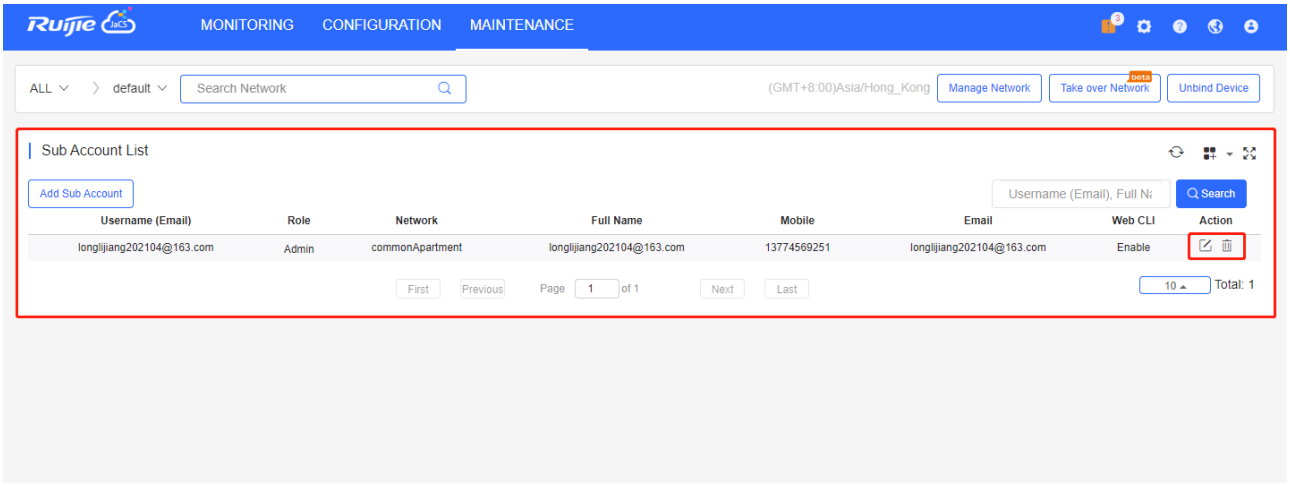
9.1 Account

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.



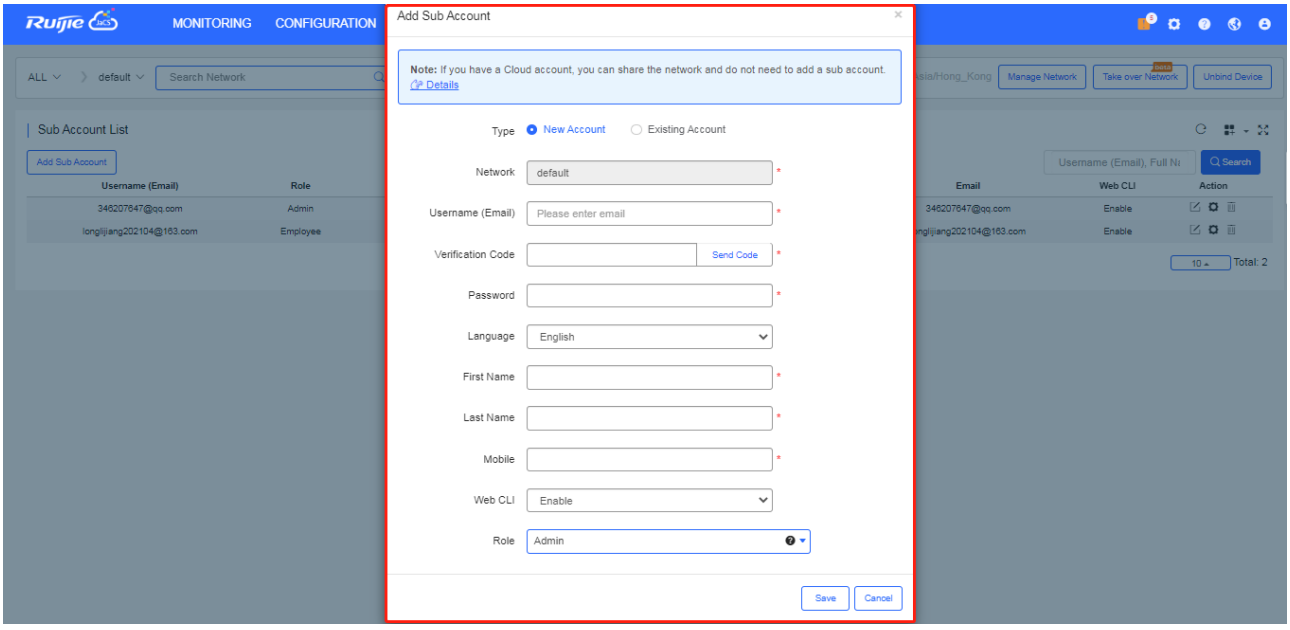
9.2 Sub Account

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.

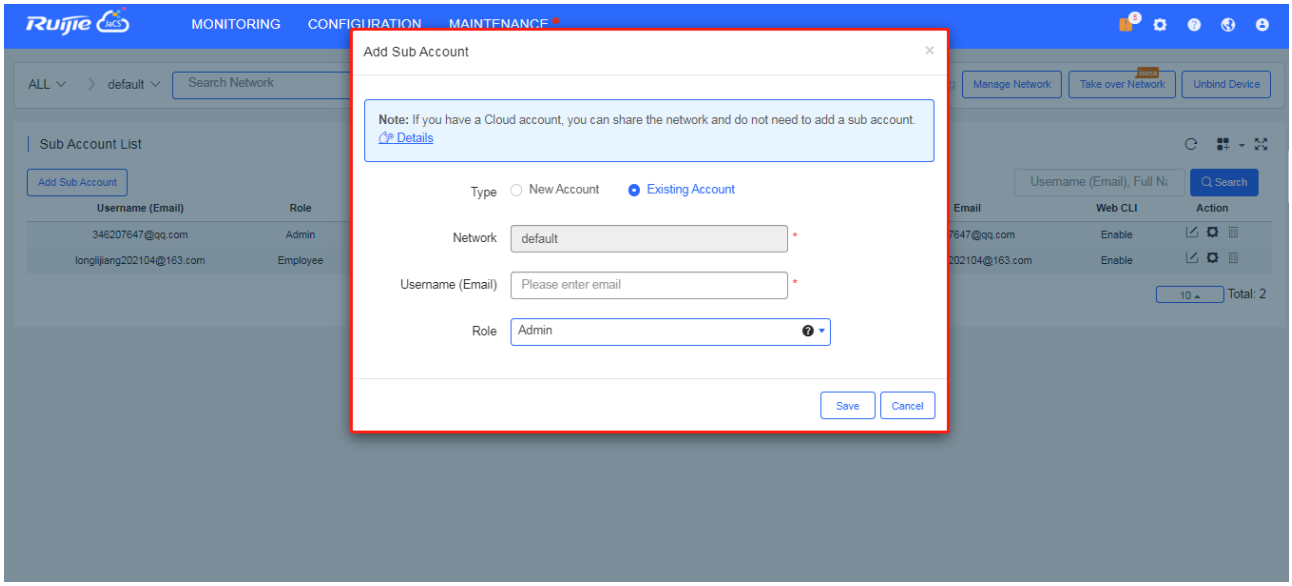


Click **Add Sub Account** to add a new sub account. Select the network, enter the Email in the **Username** box and click **Send Code**. Enter the security code contained in the Email, set the password, language, full name, expiration date, mobile and role, and click **Save**.

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.For the custom role, you can customize its read and write permissions.

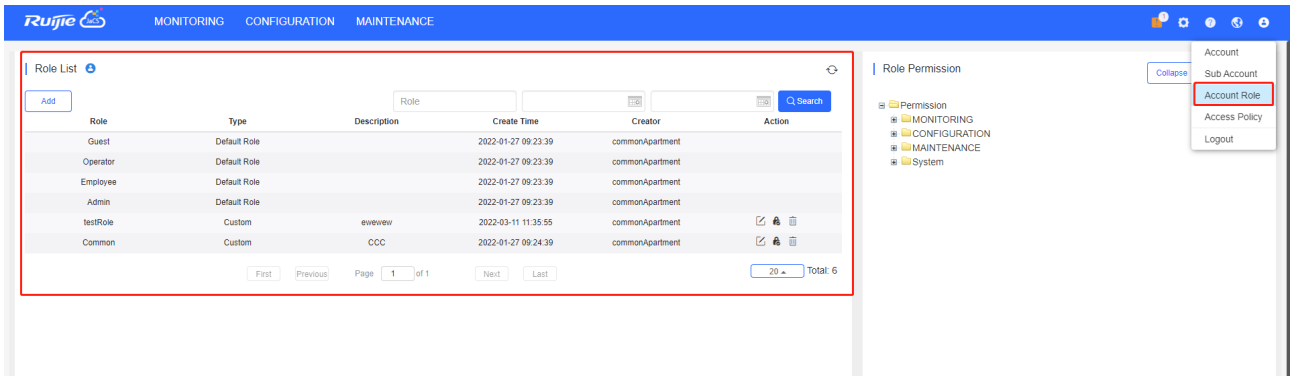


The existing sub account can be added to the network so that a sub account can manage multiple networks.

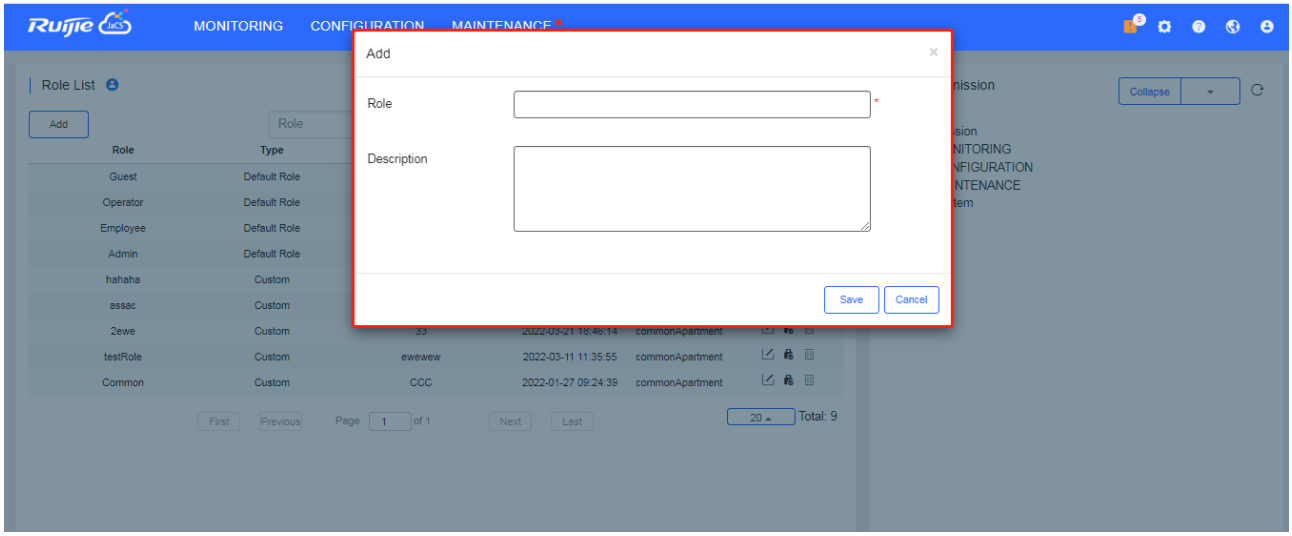


9.3 Account Role

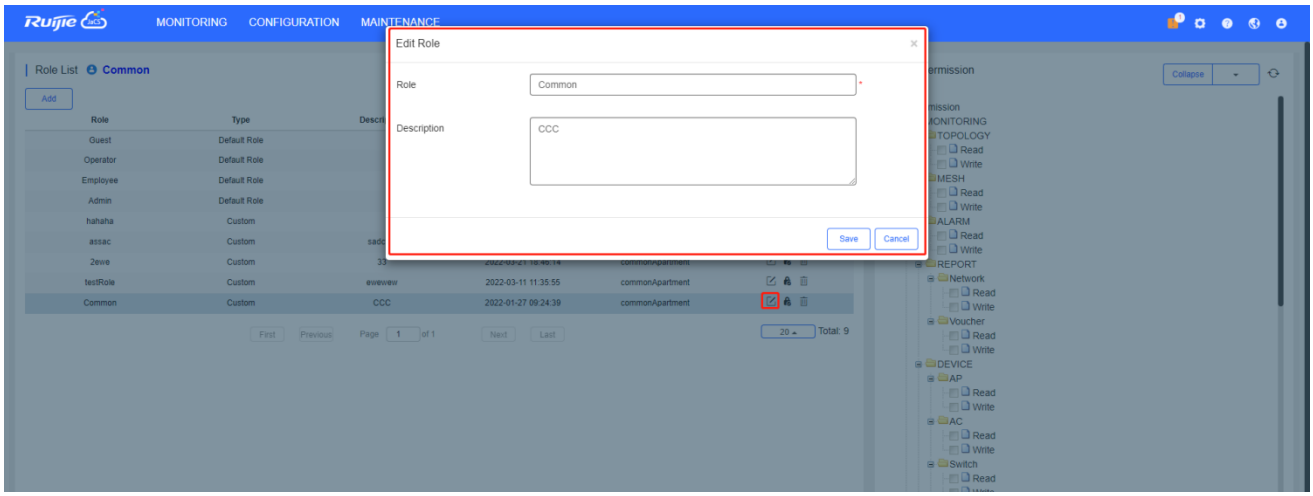
The **Role List** displays all default roles and custom roles of the tenant.

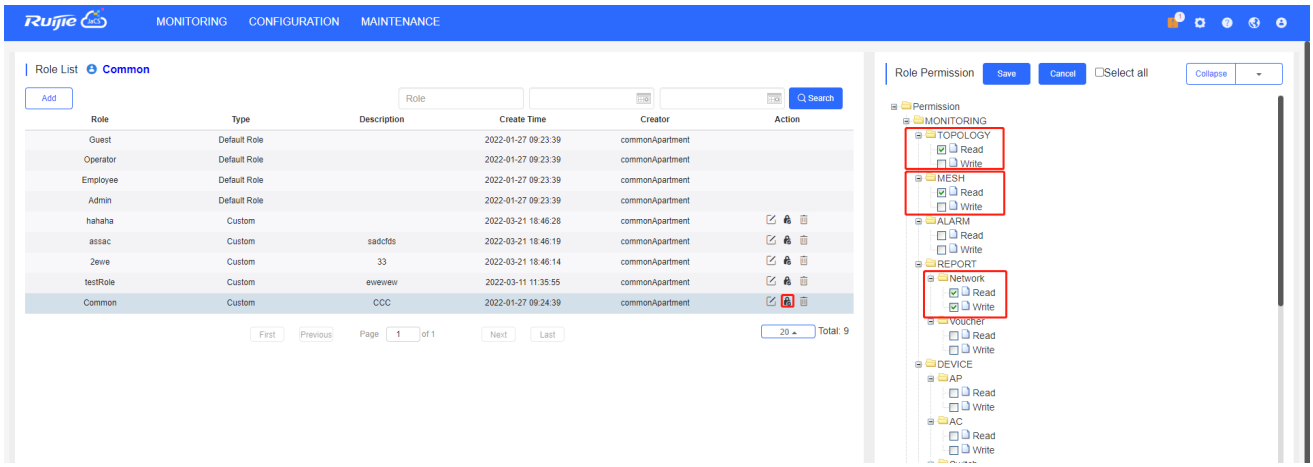


Click **Add** to add a custom role.



Click  to edit the role; click  to configure the role permissions.

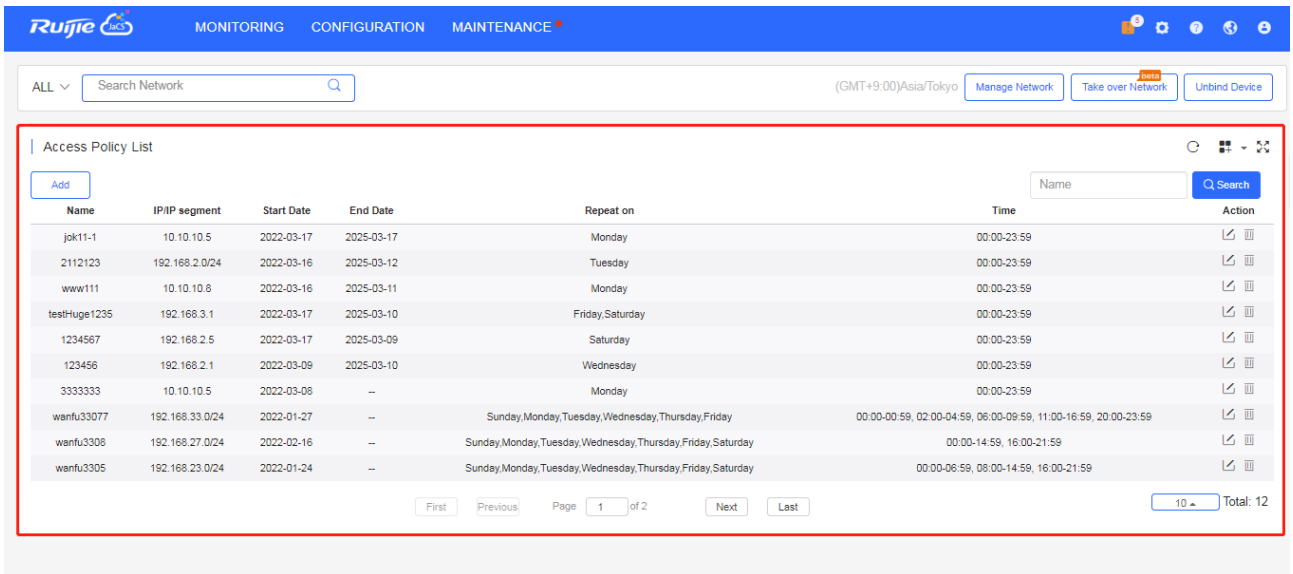




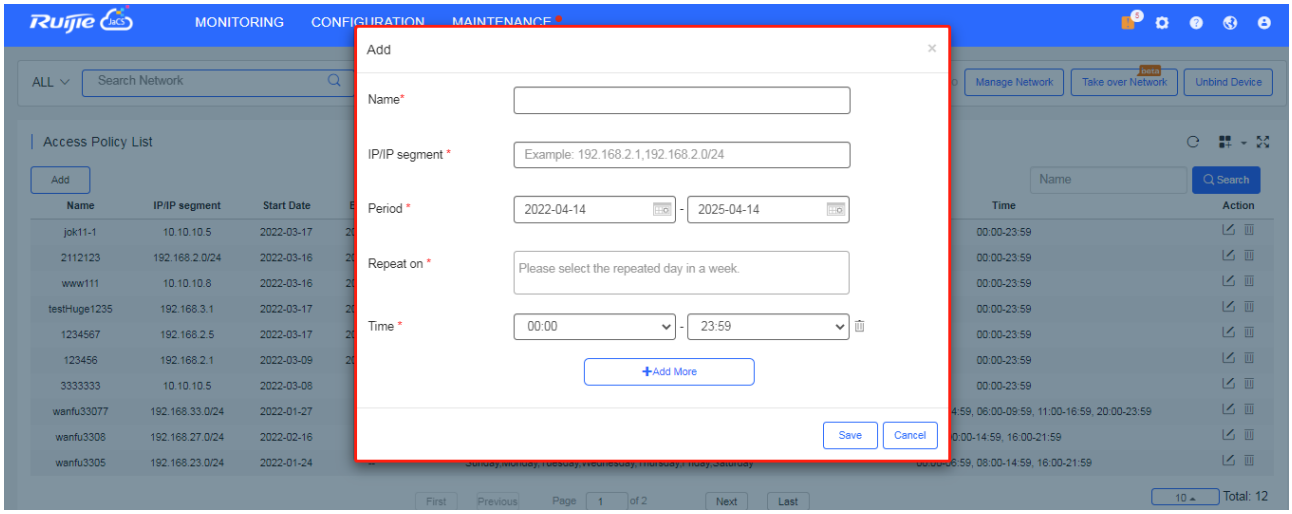
Click  to delete the custom role.

9.4 Access Policy

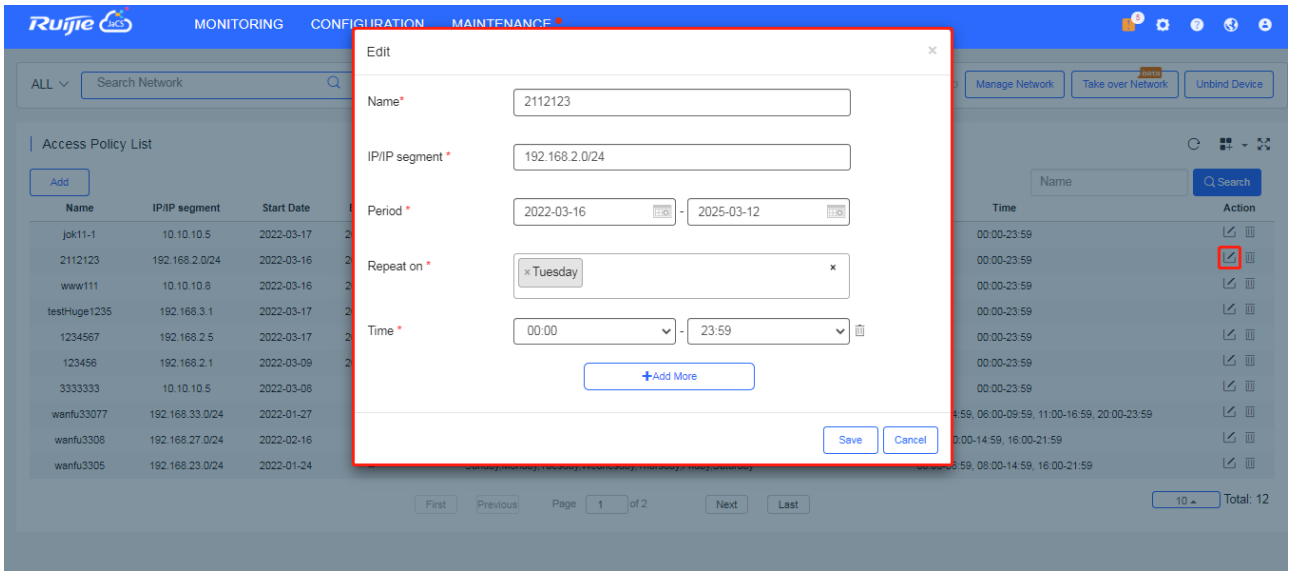
The **Access Policy List** displays all access policies of the tenant.



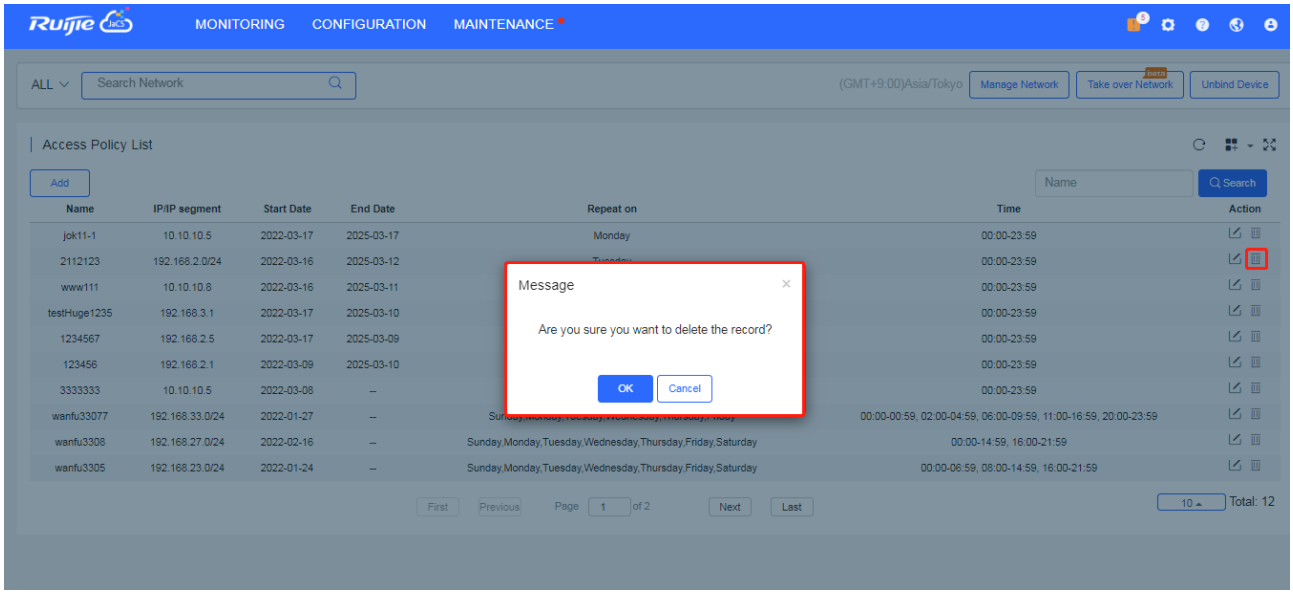
Click **Add** to add a new access policy.



Click  to edit the existing policy.



Click  to delete the access policy.

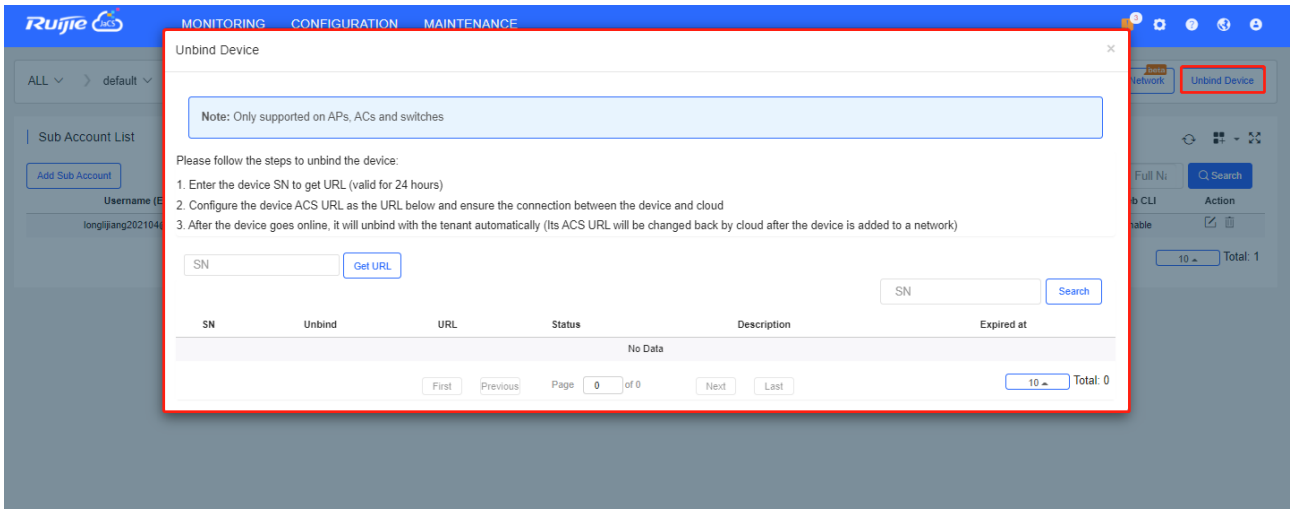


9.5 Logout

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

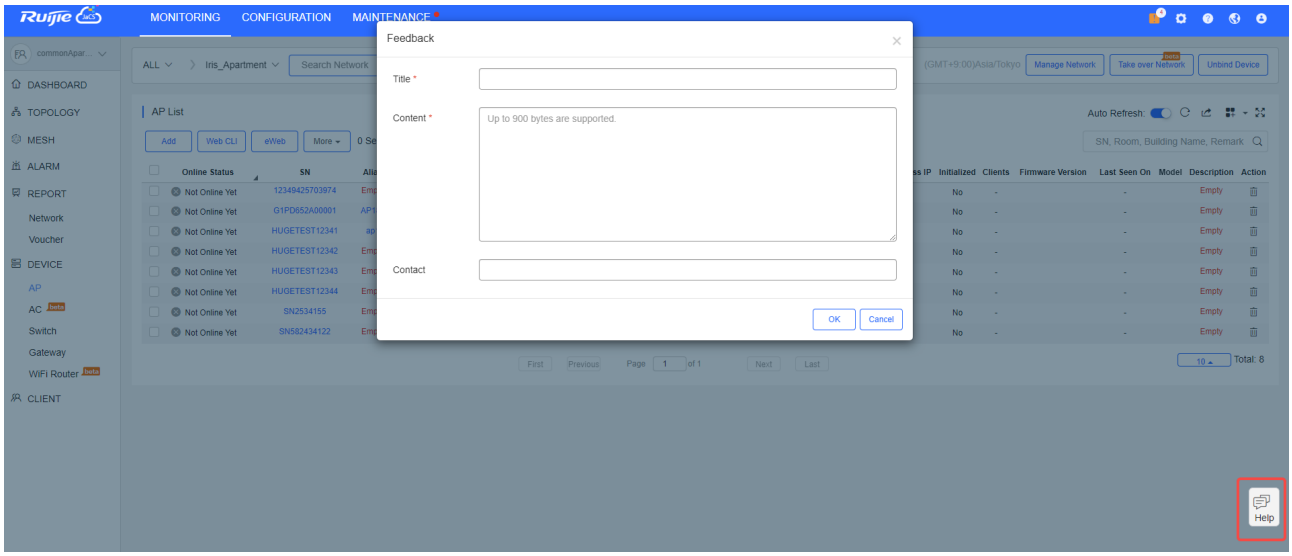
10 Unbind Device

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



11 Feedback

You can click the **Help** icon to give feedbacks on the issues you meet or offer suggestions to us.



12 Appendix

12.1 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

12.2 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.

12.3 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 will fail to deliver them after they are synchronized to the Cloud.
8	00000JAPAN WiFi	In the Apartment Scenario, if the device goes offline after 00000JAPAN Wi-Fi is enabled, and then goes online after 00000JAPAN Wi-Fi disabled, Cloud will not re-configure the Wi-Fi settings on device. You need to clear 00000JAPAN Wi-Fi configuration manually.
9	AP	In non-apartment Scenario, please clear the configuration on devices except AP180 before bring them online; otherwise, the configuration on devices may be conflict with that on Cloud, and the client may not be able to access the Internet.
10	AP	In non-apartment Scenario, if the working mode (bridge mode or routing mode) of AP180 is different from that on Cloud, the client may not be able to access the Internet.
11	TOPOLOGY	Only devices connected to the downlink port of the switch can be detected. Only access points (excluding MA series access points) and switches can be displayed in the Topology.
12	TOPOLOGY	The uplink ports of some switches cannot be shielded in the topology as the Cloud fails to identify them. Included: XS-S1930J-8GT2SFP, XS-S1930J-8GT2SFP-P

		XS-S1930J-18GT2SFP, XS-S1930J-18GT2SFP-P XS-S1930J-24GT4SFP/2GT, XS-S1930J-24GT4SFP/2GT-P XS-S1930J-48GT4SFP
13	Initial Configuration Template	The template can only be applied to AP180 series access points in Apartment networks.
14	CLI Command	Only for AP and CAP series products.
15	WPA3-SAE	Only for MA2610 and MA2810 access points in hotel networks.
16	Device Details-Back Up	Only for apartment networks.
17	Network Management	Level 5 subnetwork group is supported.