Ruijie Japanese Cloud System (JaCS)

User Guide

Document Version: V2.3
Date: 2025-01-24

Copyright

Disclaimer

The products, services, or features that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained in this manual does not constitute any explicit or implicit warranties.

Preface

Target Audience

This manual is suitable for the following people to read

- Network Engineer
- Technical Extension Staff
- Network Administrator

Technical Support

- 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

Conventions

1. Conventions

Symbols	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items.	1. Click <OK>. 2. Click <Download Template>
>	Multi-level menus items	[System Settings] > [Administrator]

2. Signs

The signs used in this document are described as follows:

Caution

An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation.

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

3. Notes

Some information displayed in this manual (such as product model, description, port types, software interfaces, etc.) is for reference only. For specific information, please refer to the actual product version used.

Contents

1 Overview

Ruijie Japan Cloud Service (JaCS) is Ruijie's easy and efficient cloud solutions for Japanese apartments and hotels. JaCS provides equipment deployment, network monitoring, network optimization and 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.

1.1 Supported Browsers

Browser	Version
Chrome	125.0.6422.61
Safari	10.1
Firefox	126.0

Note

It is recommended to use Chrome browser.

1.2 Addresses and Ports to be Permitted

Source IP	Destination Address	Source Port	Destination Port	Protocol	Description	Devices 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 a 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 CLI commands to devices	AP/AC/Switch/Gateway
Your network	cdn-japan.ruijienetworks.com	Any port	80 , 443	TCP	Ruijie Cloud Authentication Server	STA
Your network	rylog-japan.ruijienetworks.com	Any port	80,443	TCP	Device log upload	AP/ AC/ Switch/ Gateway

1.3 Supported Models

Device Types	Models
AP	RG-AP180(JA)
	RG-AP180(JP)
	RG-AP180-PE
	RG-AP180-AC
	RG-AP850-I-JPV2
	RG-AP680CD-JP
	RG-MA2610-PE
	RG-MA2610-AC
	RG-MA2810
	RG-HA3515-DG
Switch	RG-HS2310-16GH2GT1XS
	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
Gateway	RG-EG2100-P V2
	RG-EG3250
	RG-EG3230
	RG-EG5210-JP
Lite-PON	RG-MT3002
	RG-MU3064

2 Getting Started with JaCS

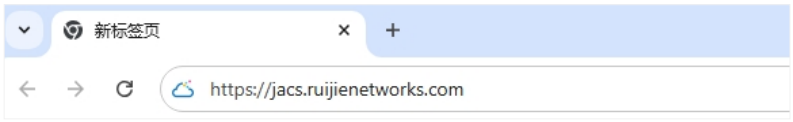
The chapter introduces how to start use JaCS, including:

- Registering an Account
- Logging into JaCS
- Resetting Password

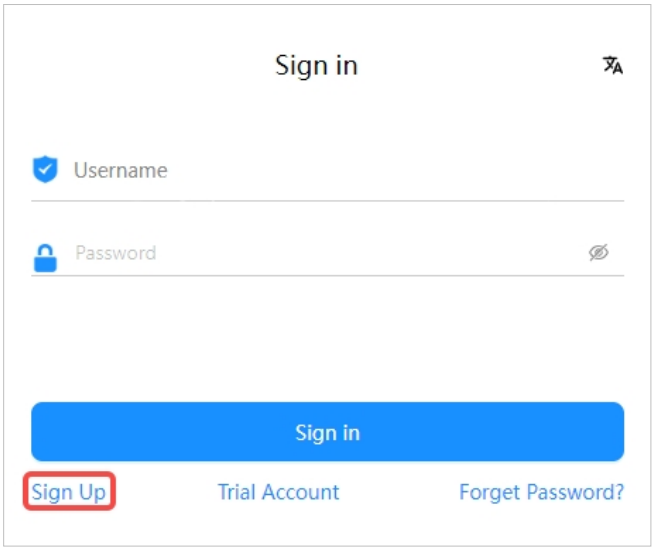
2.1 Registering an Account

JaCS currently only supports account registration via emails. The registration steps are as follows:

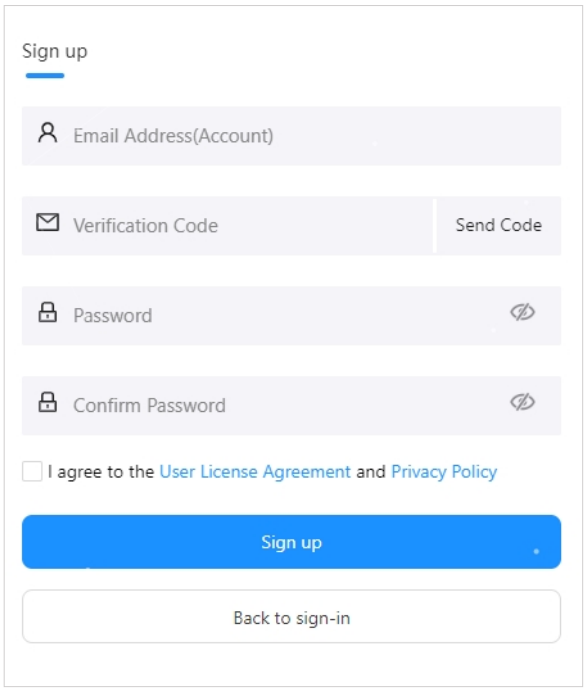
1 Use a browser to visit: https://jacs.ruijienetworks.com.



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



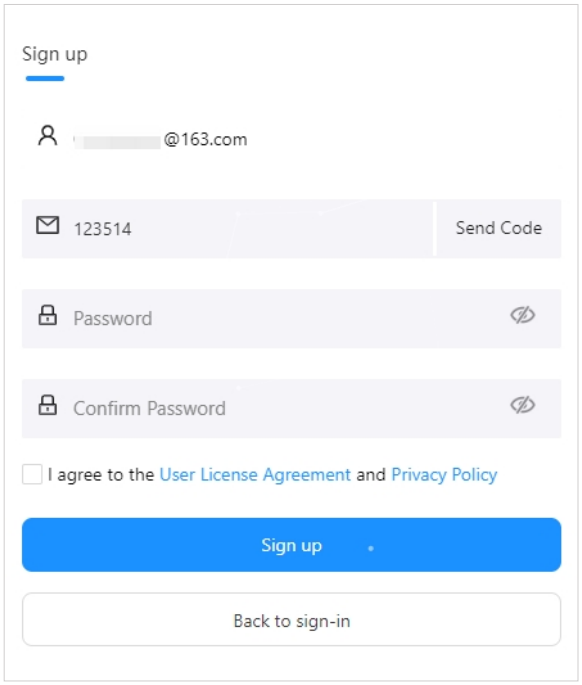
3 Enter your Email address, and then click **Send Code**.



Note

One Email address can be registered once only. If the Email address you entered has been registered on JaCS, the system will prompt “This email is already registered."

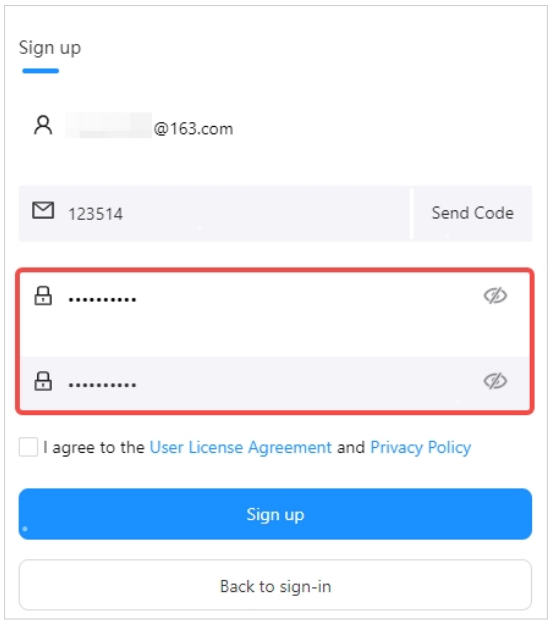
4 Enter the verification code received.



Note

The verification code is valid for 10 minutes. If you do not receive the verification code, please click **Send Code** again after 1 minute.

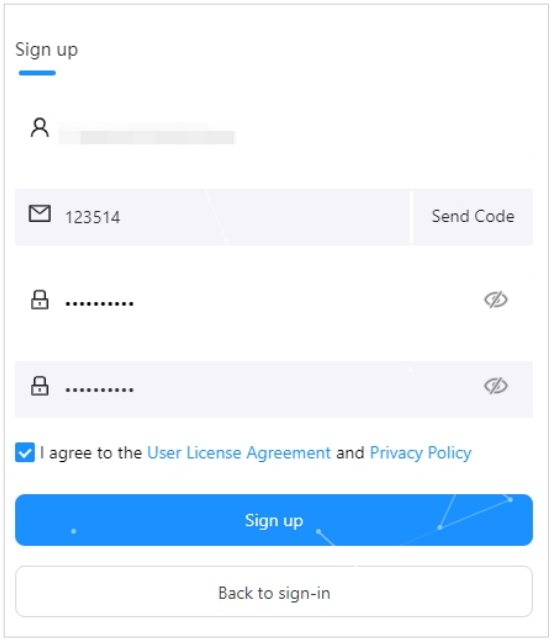
5 Enter the password twice in succession.



Note

- Click icon on the right side of the password input box to view the password.
- Please make sure the two passwords you enter are consistent.
- The password must contain three types of the following characters: uppercases, lowercases, digital numbers and special characters. Spaces are not allowed to be available on the password. The password length ranges from 8 to 16 characters.

6 Check “I agree to the User License Agreement and Privacy Policy”, and then click **Sign up** to complete the registration.



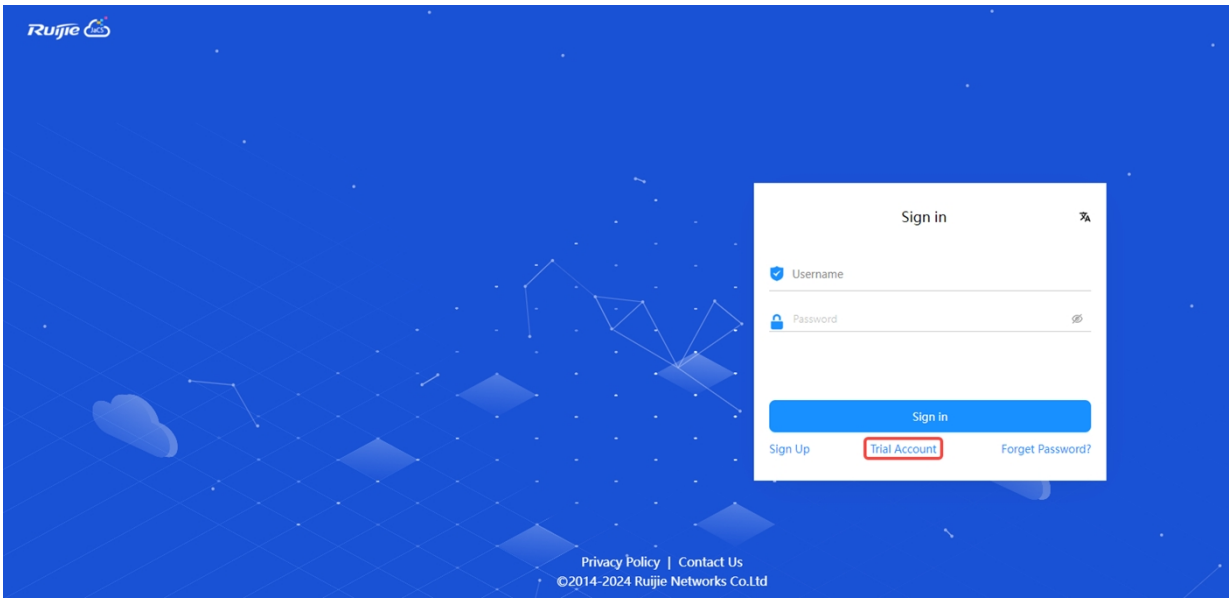
After the account registration is completed, the user can use the account to log in.

Note

The account registration cannot complete if you do not agree to our **User License Agreement** and **Privacy Policy**.

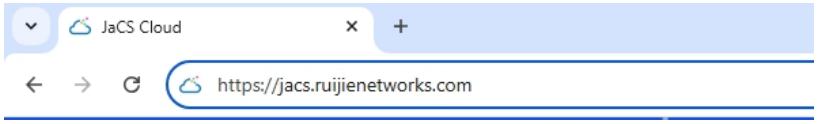
2.2 Logging into JaCS

Before logging in, please confirm that you have registered an account. If you have not registered an account before, please refer to Section 2.1 to complete the account registration first. If you do not want to register an account, you can click **Trial Account** on the login page to experience the system.

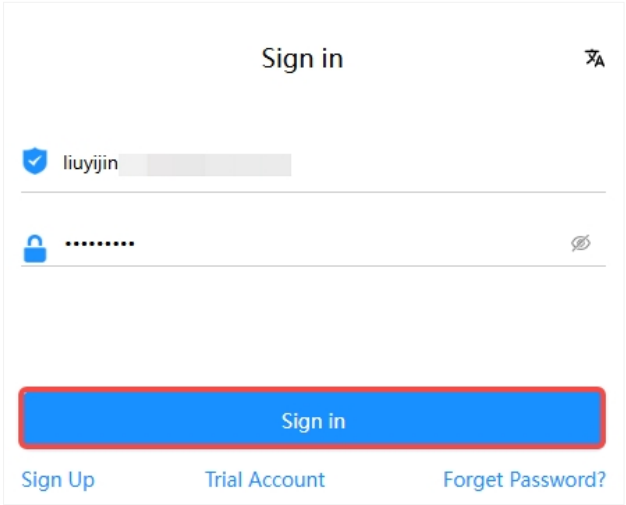


If you already have an account, please follow the steps below to log into the system:

1 Use a browser to visit: https://jacs.ruijienetworks.com.



2 Enter your email address and password, and click **Sign in**.



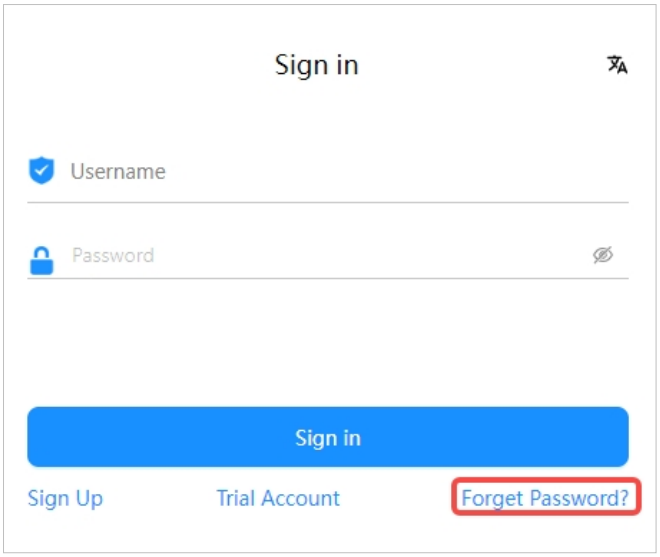
Note

After a login error occurs, a slider for verification will appear.

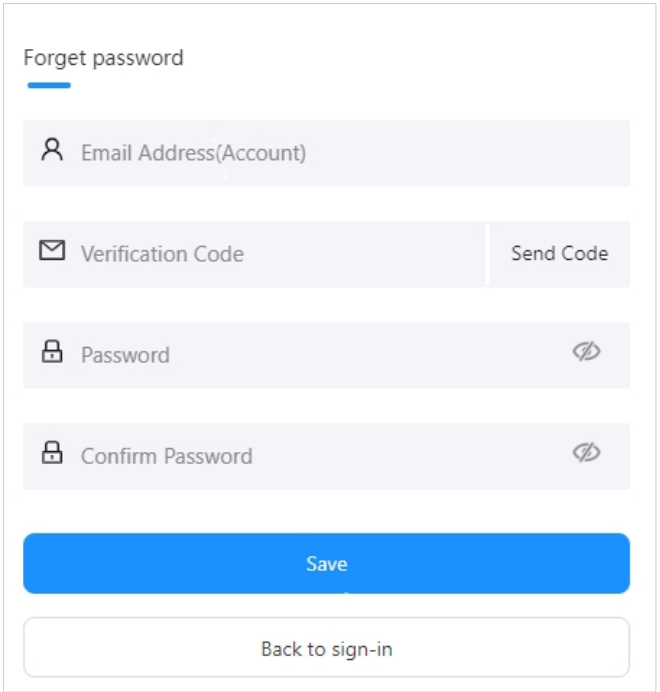
2.3 Resetting Password

If you forget your password, you can follow the steps below to reset it:

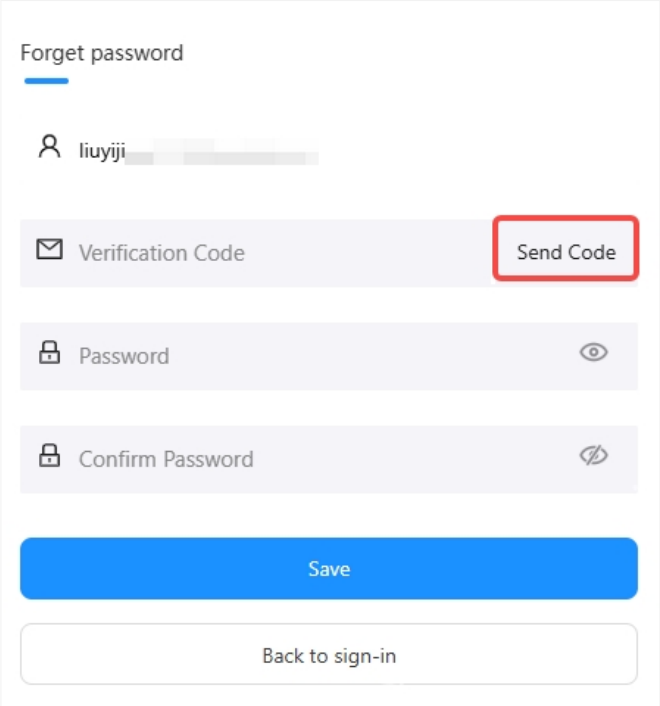
1 Click **Forget Password?** to go to the password reset page.



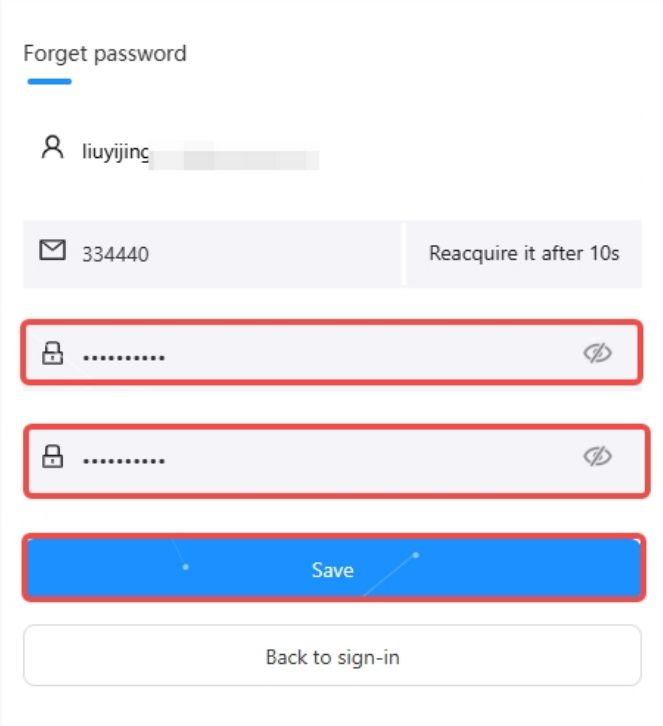
2 Enter your email address used for registration.



3 Click **Send Code,** and enter the verification code received.



4 Enter the new password twice and click **Save**.



After the password is reset, you can use the new password to log into Ruijie JaCS.

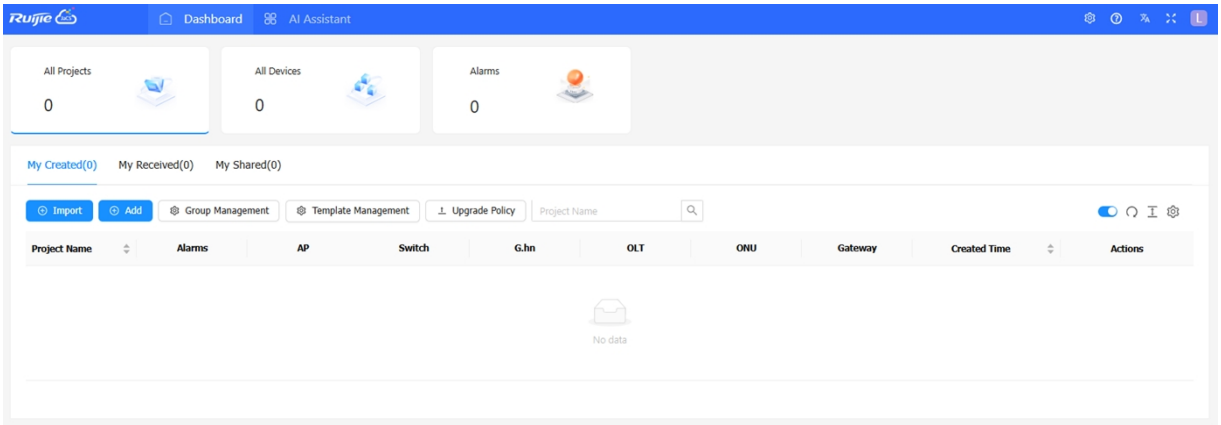
2.4 Interface Introduction

Ruijie JaCS consists of the following three interfaces:

- Dashboard Interface
- Project Management Interface
- AI Assistant

2.4.1 Dashboard Interface

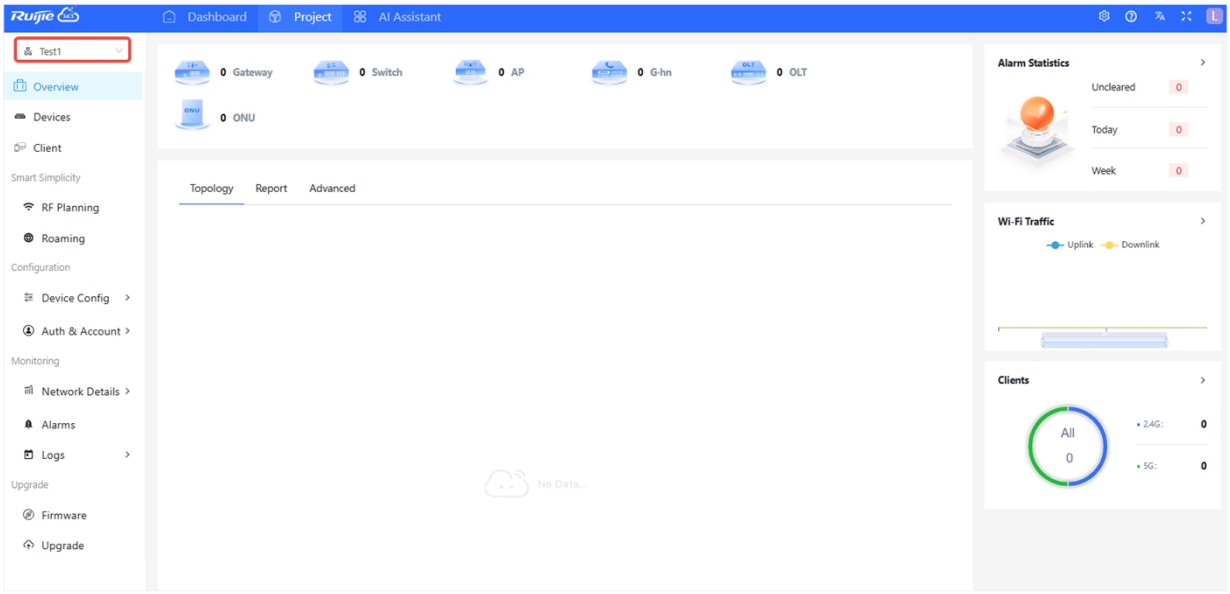
After successfully logging into the JaCS, you will enter the dashboard interface by default.



Items	Description
All Projects	Click **All Projects** to view all currently created projects. The number displayed under **All Projects** is the total number of currently created projects.
All Devices	Click **All Devices** to view all devices of all projects in the current account. The number displayed under **All Devices** is the total number of devices imported.
Alarms	Click **Alarms** to view all warning information. The number displayed below **Alarms** is the total number of generated alarms.
	Fullscreen button. If you want exit the full screen mode, press **Esc** on the keyboard or click  button.
	System language switch button. Click this icon to switch the system language. Three languages are supported: Chinese, English, and Japanese.
	Click this icon to display more options, including Account, Sub Account, Account Role, Access Policy and Logout.

2.4.2 Project Management Interface

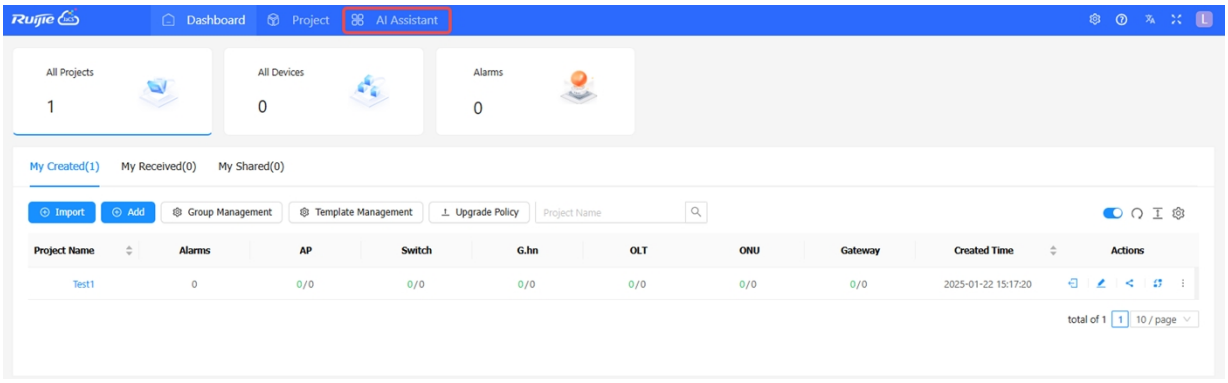
After creating a project on the **Dashboard** interface, a Project menu will appear at the top of the interface. Click the **Project** to enter the project management interface. Click the project switch box in the upper left corner to switch projects.

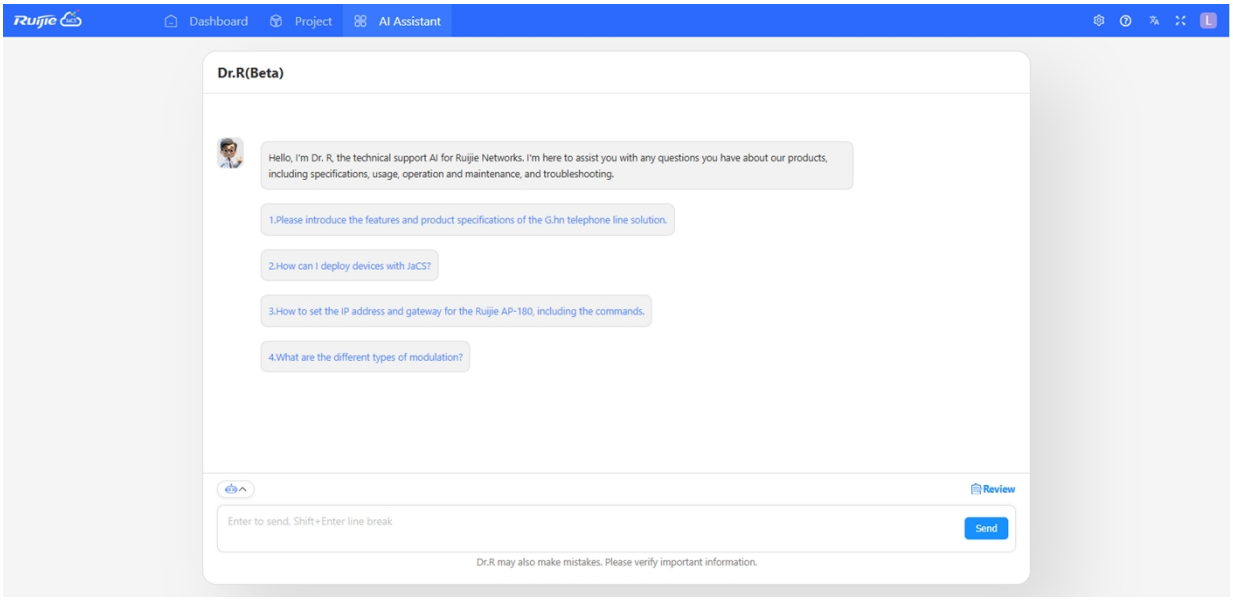


Menus	Description
Overview	In this interface, you can view the overall status of a project, including device number, topology, alarm statistics, Wi-Fi traffic and clients.
Devices	In this interface, you can manage the devices in a project. JaCS supports managing APs, switches, gateways, G.hn devices, OLT devices and ONU devices. For specific supported models, refer to Section 1.3.
Client	In this interface, you can view the client information in the current project.
Device Config	In this interface, you can configure and manage the initialization configuration template and device-specific configuration template, and set basic wireless configuration.
Auth & Account	In this interface, you can configure the following authentication types, including voucher authentication, account authentication (providing account and password management, configuring limits on speed, traffic, number of terminals and validity period), PPSK (providing account and password management and terminal binding), and captive portal (supporting customized portal pages, including background style, background image customization, languages, terms, copyright, login button, marketing advertisement, welcome message, login method, online time, jump page after login, etc.).
Network Details	In this menu page, you can monitor the network information of a project, including channel distribution and utilization, device statistics, and client statistics.
Alarms	In this interface, you can view and manage all alarm information in the current project.
Logs	In this interface, you can check logs. Six types of logs are supported, including operation logs, configuration logs, upgrade logs, Mesh logs, configuration replacement logs, and device-specific configuration logs.
Policy	In this interface, you can set upgrade policies.
Upgrade	In this interface, you can upgrade your devices.
Firmware	In this interface, you can view the existing firmware version in the current project, and upload and manage your private firmware.

2.4.3 AI Assistant

Ruijie JaCS carries an AI assistant. You can use the AI assistant to obtain information and configuration steps of related products.





3 Project Management

This chapter introduces how to manage projects on JaCS, including:

- Creating a Project
- Creating Projects in Batches
- Creating a Project Group
- Editing a Project
- Sharing a Project
- Handing over a Project

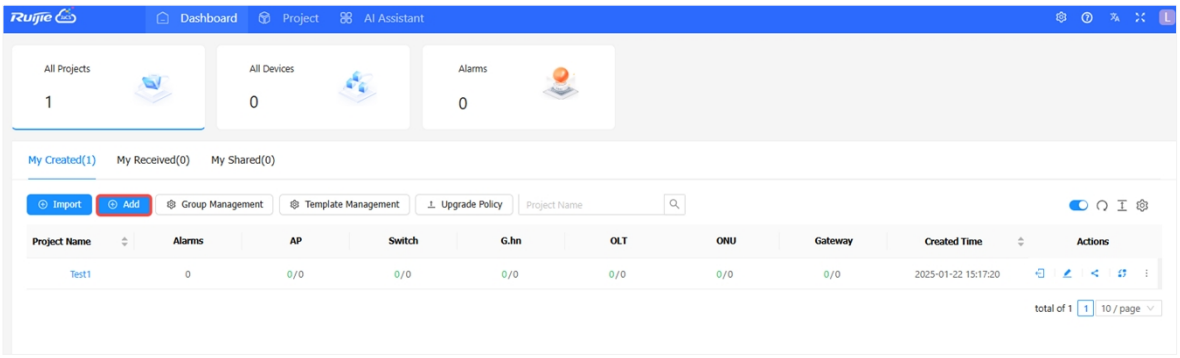
Note

- The maximum number of projects/project groups are 21,000. A new project or group cannot be created under an existing project.
- The maximum level of each project group/project is 5. Each project supports importing up to 6,000 devices.

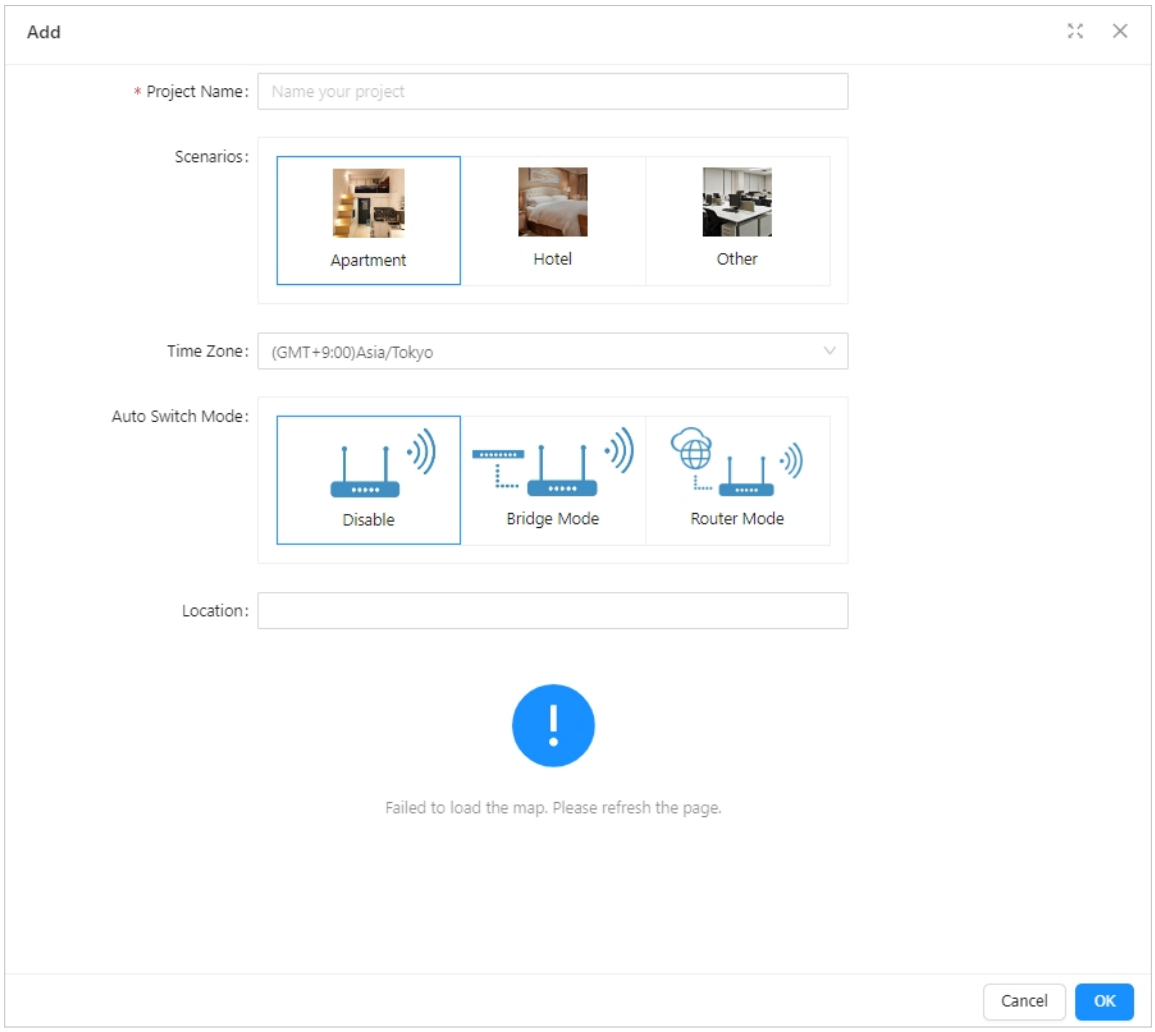
3.1 Creating a Project

Follow the steps below to create a project.

1 Click **Dashboard** > **All Projects** to enter the project management interface, and then click **Add**.



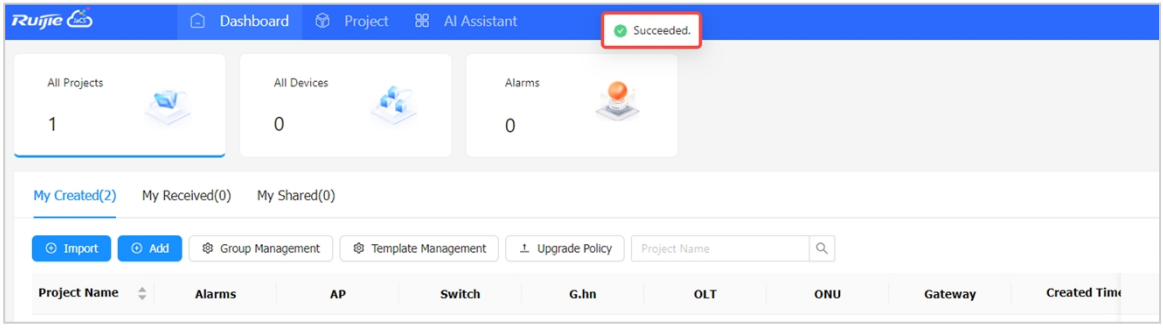
2 Set basic project information.



Items	Description
Project Name	Required. Set the network name. A maximum of 256 characters are supported.
Scenario	Required. **Defaults:** Apartment scenario **Options:** • Apartment • Hotel • Others **Note** For hotels and other scenarios, you can set the same SSID and password for all devices imported to the project. For apartment scenario, you can set a different SSID and password for each device imported to the project.
Time Zone	**Default value**: (GMT+9:00)Asia/Tokyo
Auto Switch Mode	Required. **Defaults**: Disabled **Options:** • Disable: Disabling the automatic switching mode function. • Bridge: After selecting this option, the working modes of the devices imported into the project will be automatically switched to bridge mode after they go online for the first time. • Router: After selecting this option, the working modes of the device imported into the project will be automatically switched to routing mode when they go online for the first time.

Type	**Defaults**: Cloud +AP (Manage AP devices through the cloud.)
Bind Location	After binding the geographic location, the number of terminal devices added to the project will be marked and displayed on the Google map.

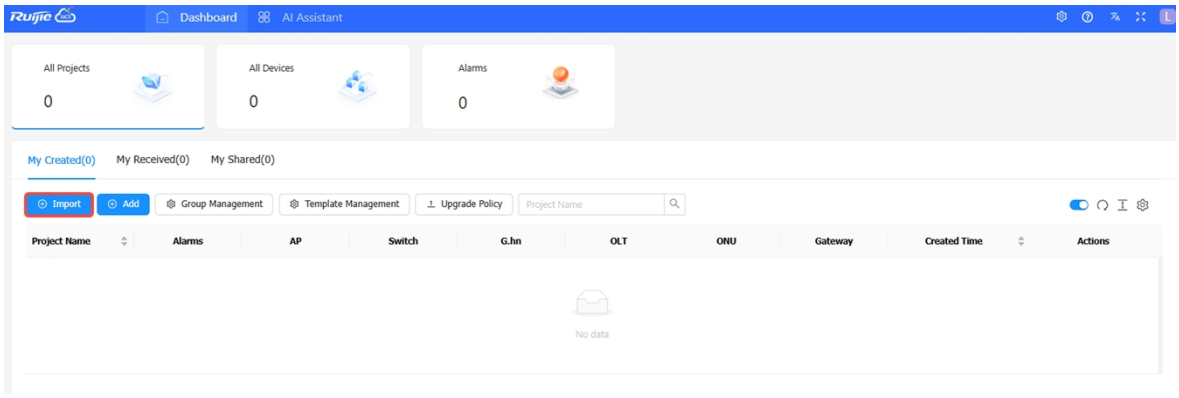
3 After the "Succeeded" prompt appears, the project is created successfully.



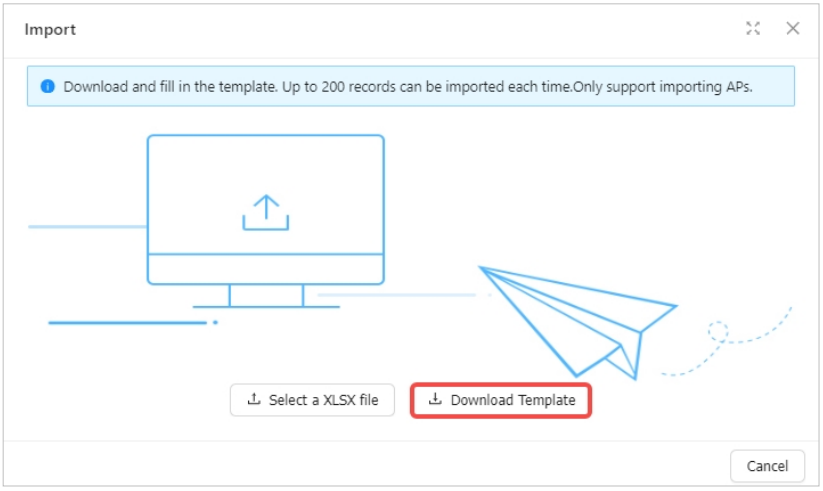
3.2 Creating Projects in Batches

Follow the steps below to create projects in batches:

1 Click **Dashboard** > **All Projects** to go to the project management page, and then click **Import**.



2 Click **Download Template**.



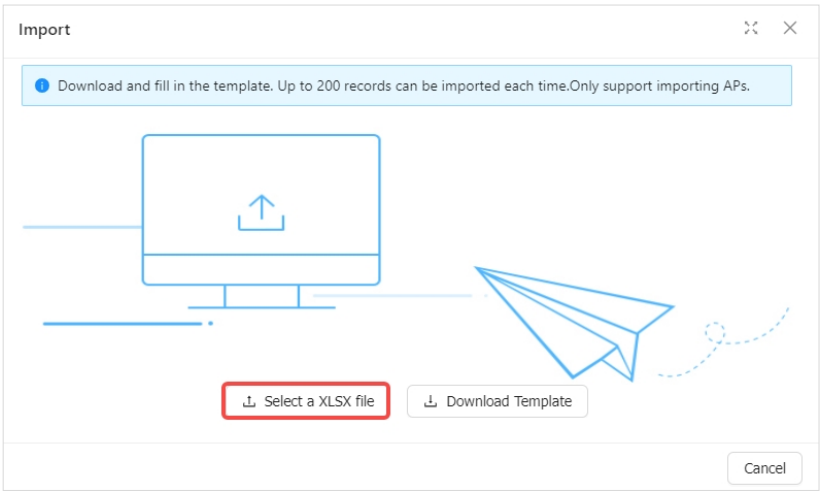
3 Fill in the template.

Project	SN	Alias	Room	Building Name	Remark

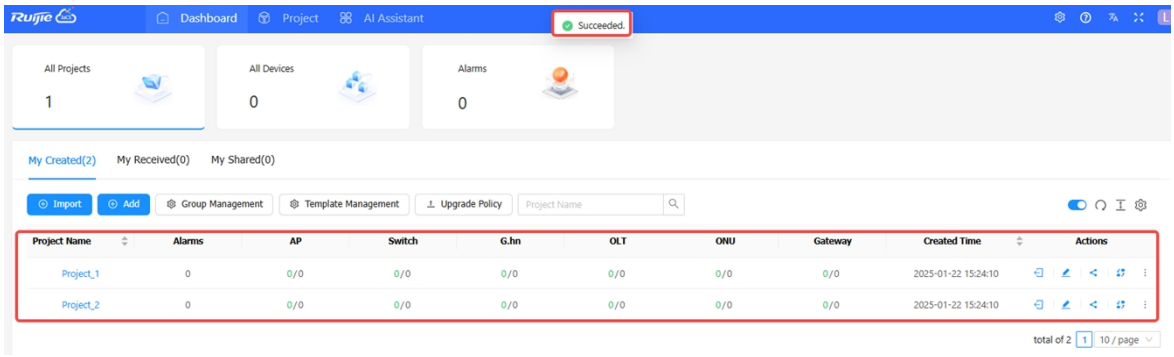
Items	Description
Project	Required. Specify project names. The length of a project name cannot exceeds 256 characters.
SN	Optional. Specify the SN of the AP devices.
Alias	Optional.
Room	Optional. Specify the room number where the AP is located. For example: 301. Supports entering 1 to 32 characters.
Building Name	Optional. Specify the building name. Up to 32 characters can be configured.

Remark	Optional. Up to 32 characters can be entered.

4 After filling in the template, click **Select a XLSX file** to upload the template.



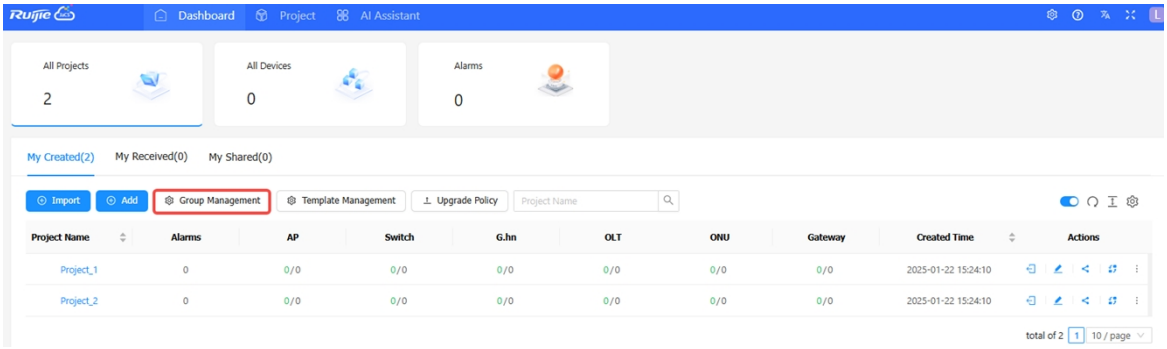
5 After the "Succeeded" prompt appears, the batch creation is completed. The created project information will be displayed in the list below.



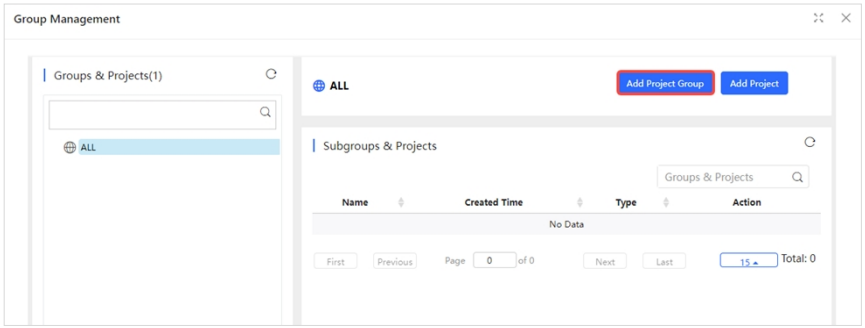
3.3 Creating a Project Group

Follow the steps below to create a project group:

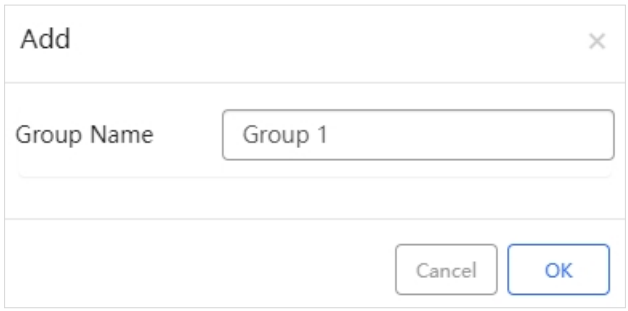
1 Click **Dashboard** > **All Projects** to go to the project management page, and then click **Group Management**.



2 Click **Add Project Group**.



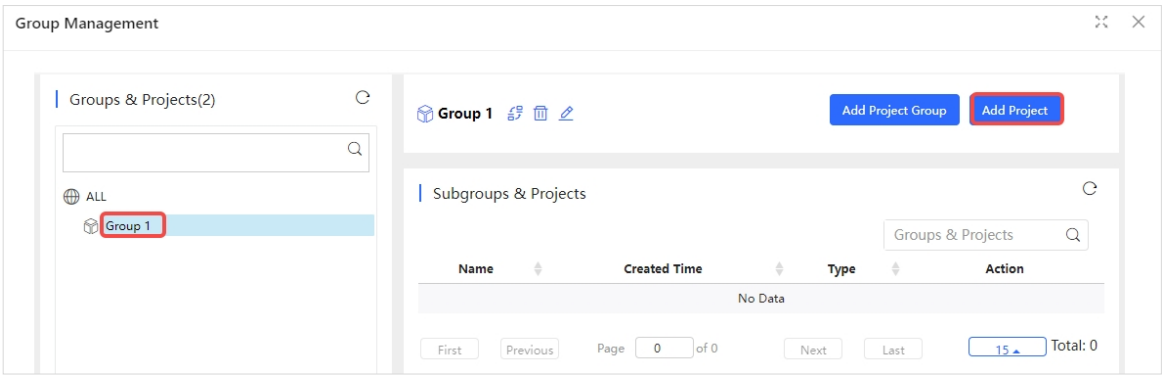
3 Enter a project group name and click **OK**.



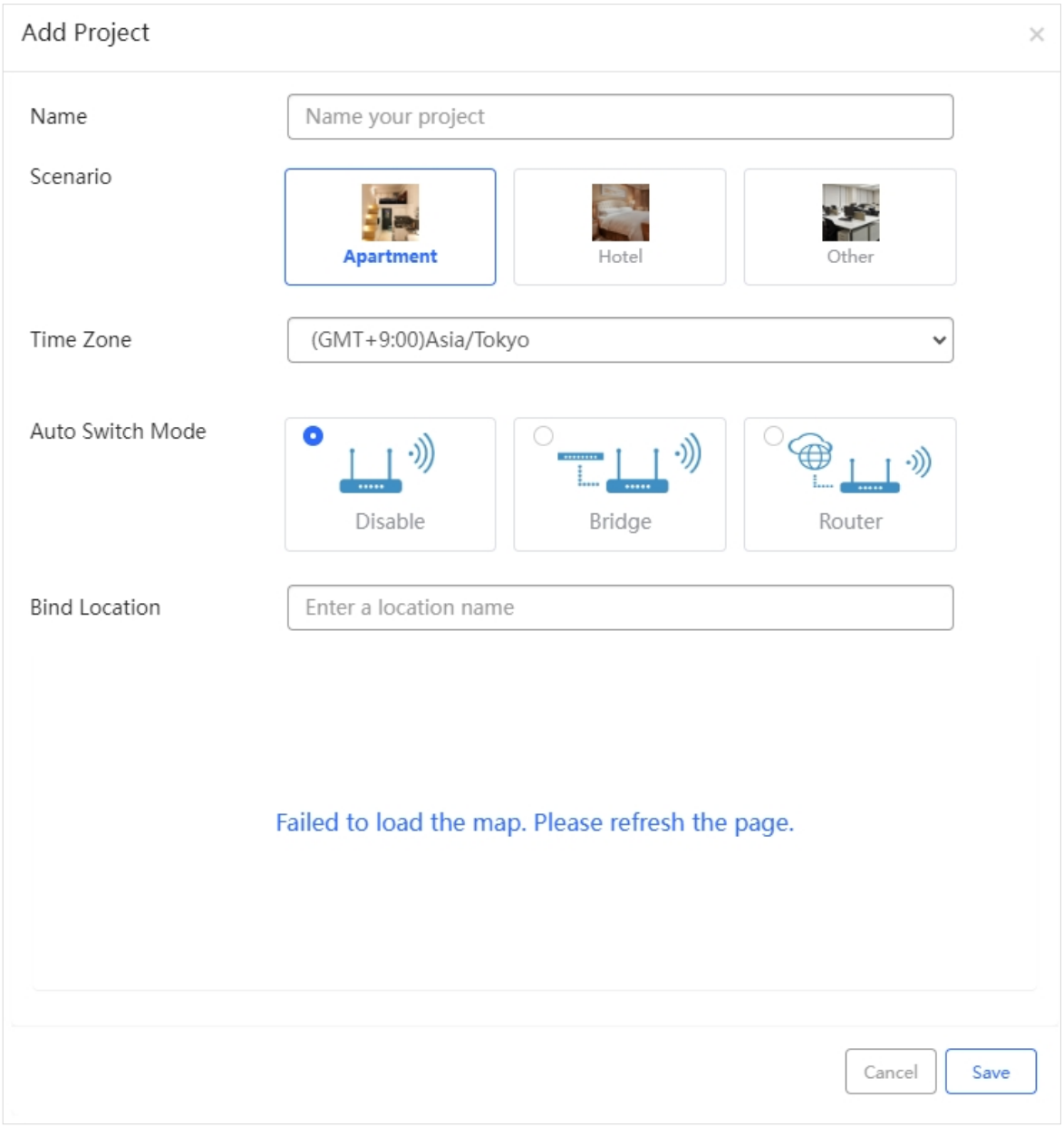
Note

The length of a project group name cannot exceed 256 characters.

4 After creating a project, select the project group and click **Add Project** to add a project to the project group.



5 After setting the basic project information, click **Save**.



Settings	Description
Project Name	Required. Set the network name. The length of a project name cannot exceed 256 characters.
Scenario	Required.

	Defaults: Apartment **Options**: ● Apartment ● Hotel ● Others **Note** For hotels and other scenarios, you can set the same SSID and password for all devices imported to the project. For apartment scenario, you can set a different SSID and password for each device imported to the project.
Time Zone	**Defaults**: (GMT+9:00)Asia/Tokyo
Automatic switching mode	Required. **Defaults**: Disable **Options**: ● Disable: Disabling the automatic switching mode function. ● Bridge: After selecting this option, AP devices imported into the project will automatically switch to bridge mode after they go online for the first time. ● Router: After selecting this option, AP devices imported into the network will automatically switch to routing mode when they go online for the first time.
Type	Defaults: Cloud +AP (Manage AP devices through the cloud .)
Location Binding	After binding the geographic location, the number of terminal devices added to the project will be marked and displayed on the Google map.

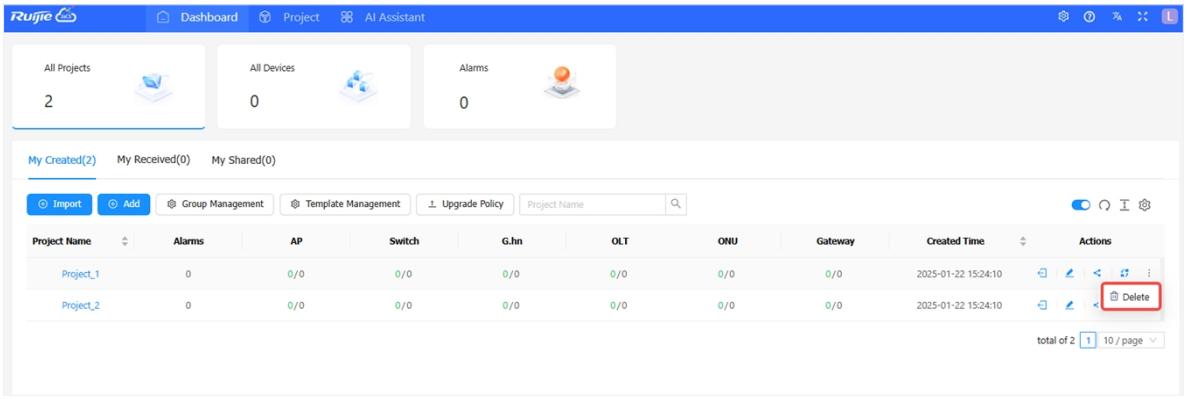
3.4 Deleting a Project

Follow the steps below to delete a project.

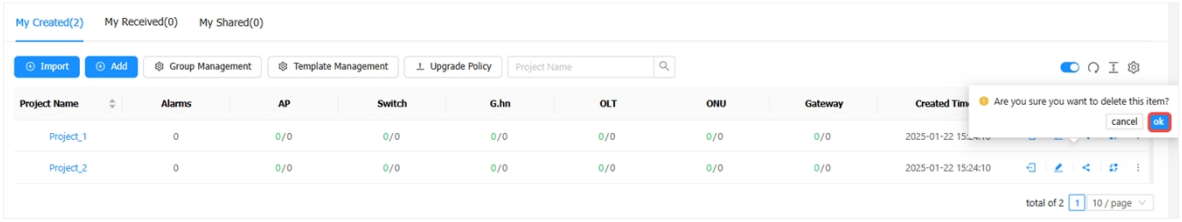
Note

- The project shared with other tenants cannot be deleted.
- If a project has a device bound to it, it cannot be deleted. To delete it, please remove the device from the project first.

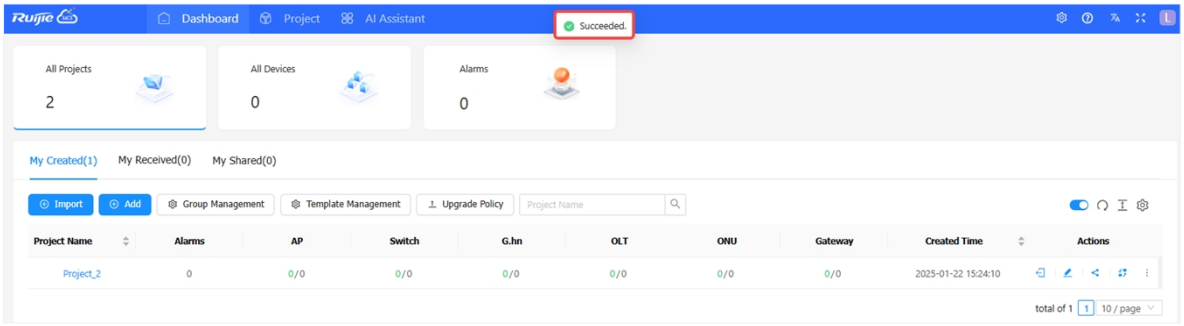
1 Navigate to the **Dashboard** > **All Project** > **My Created** configuration interface, put the mouse in the ⋮ in the **Action**, and then click **Delete**.



2 When the message “Are you sure you want to delete this item?” appears, click **OK**.



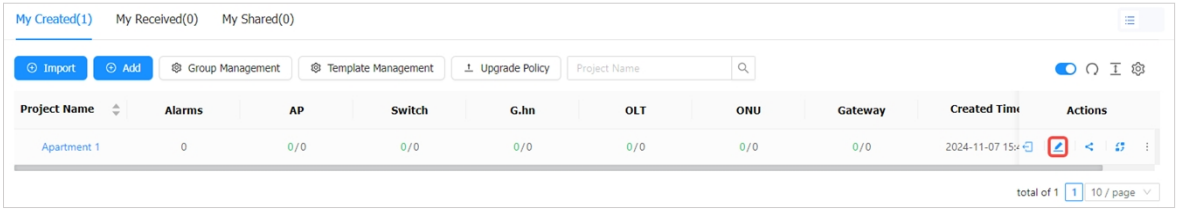
3 When the “Succeeded” prompt appears, the deletion is completed.



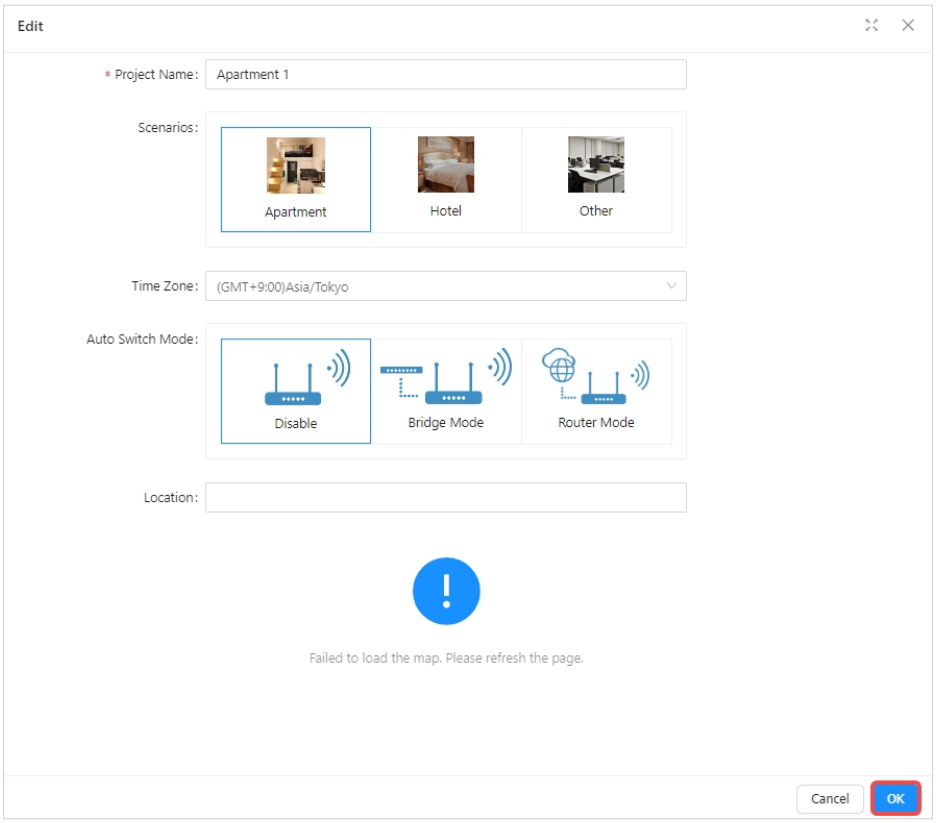
3.5 Editing a Project

Follow the steps below to modify the information of an existing project.

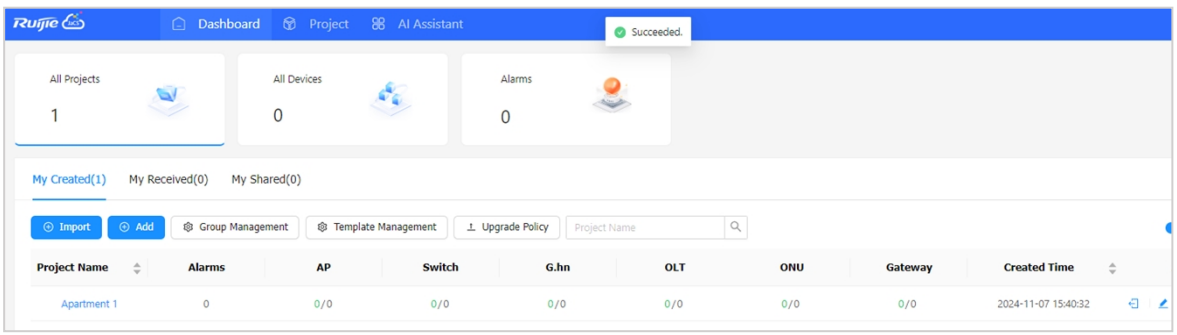
1 Click the edit icon in the **Action** column of the project that needs to be modified.



2 After modifying the information as needed, click **OK** to save the configuration.



3 After the “Succeeded” prompt appears, the operation is completed.

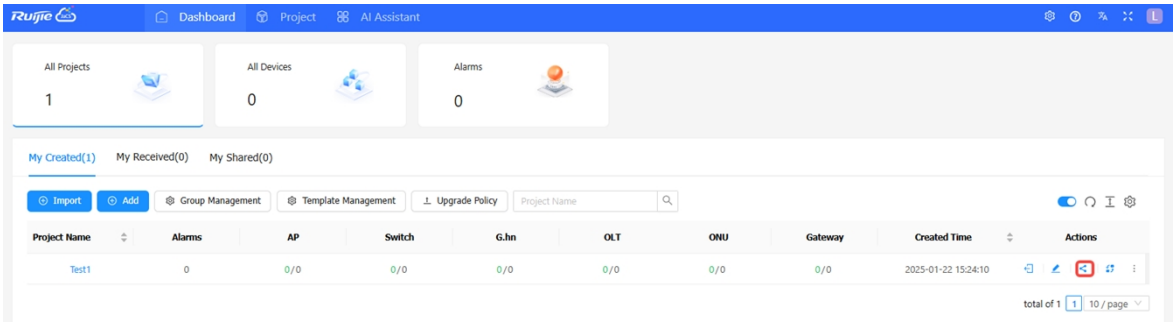


3.6 Sharing a Project

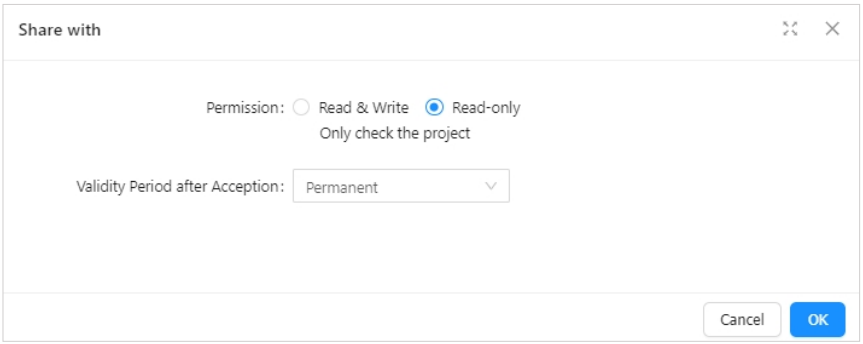
JaCS supports sharing projects with other tenants for joint management. When the specified sharing period expires, the sharing will be automatically cancelled.

The specific steps are as follows:

1 Click the share icon in the **Action** column of the project to be shared.

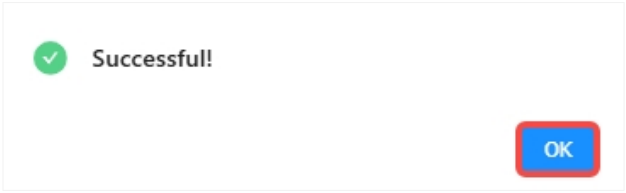


2 Set the permission and validity period, and then click **OK**.

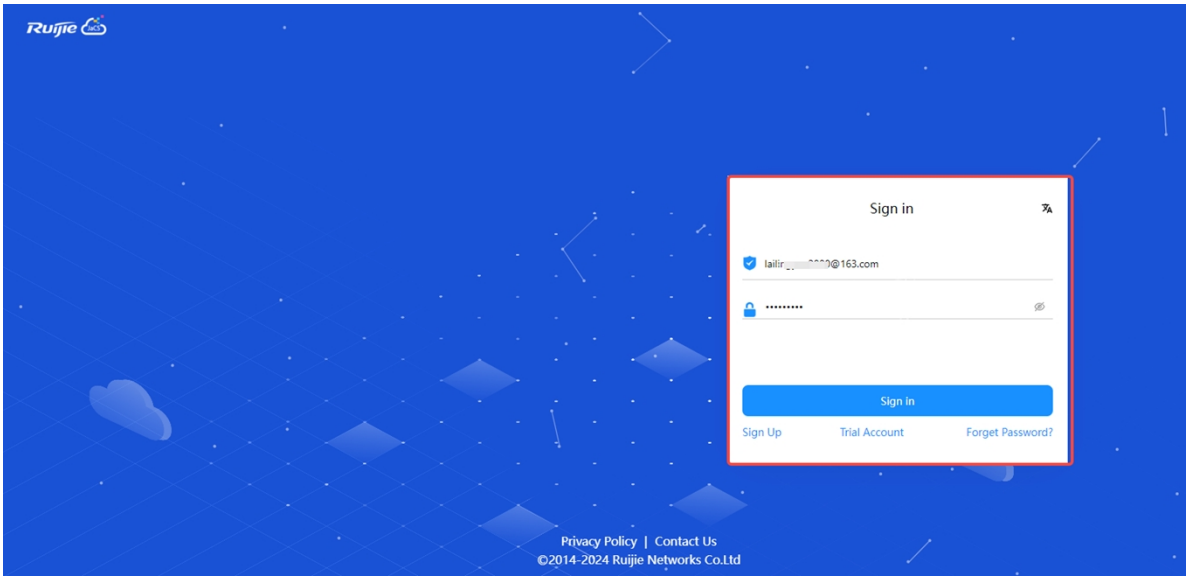


Items	Description
Permission	**Defaults**: Read &Write **Options**: • Read &Write: The sharing recipient can view and manage the project. • Read-Only: The sharing recipient can only view the project configuration but cannot manage the project.
Validity Period after Acception	**Defaults**: Permanent **Options**: Permanent/1 day/1 week/1 month/1 year/Custom. When you select **Custom**, you need to specify a concert expiration date. For example, if you set the expiration date to December 31, 2030, the system default validity period is " December 31, 2030 23:59:59 ".

3 Click **Copy** to copy the sharing link.

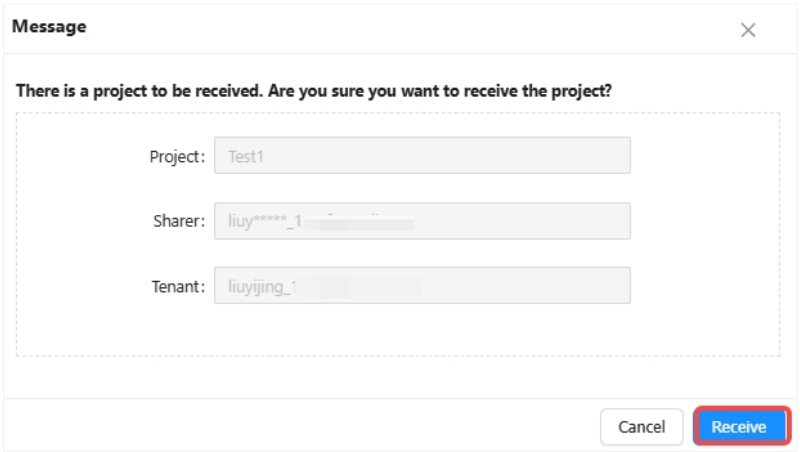


4 Log into the recipient account.



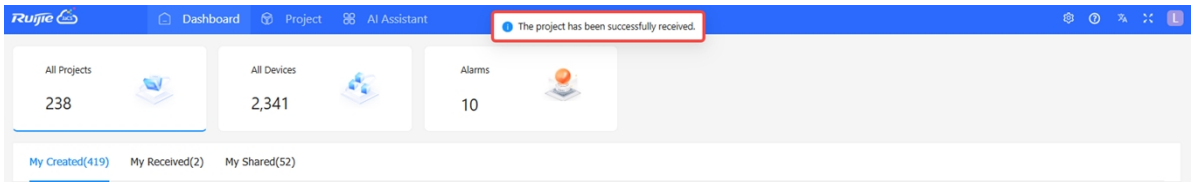
5 After logging in to the recipient account, paste the shared link copied in the step 4 in the address bar of the browser and press **Enter**.

6 In the pop-up window, click **Receive**.

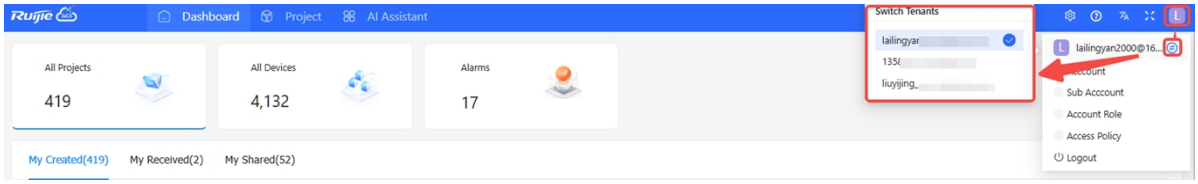


Items	Description
Project	Displays the shared project name.
Sharer	Displays the tenant account to which the shared project belongs.
Tenants	Displays the tenant name to which the shared project belongs.

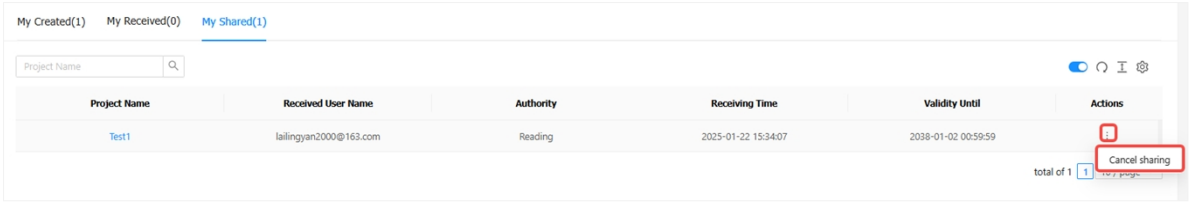
7 After the “The project has been successfully received" prompt appears, the operation is completed.



After successfully accepting the shared project, you can switch accounts in the upper right corner of the interface.



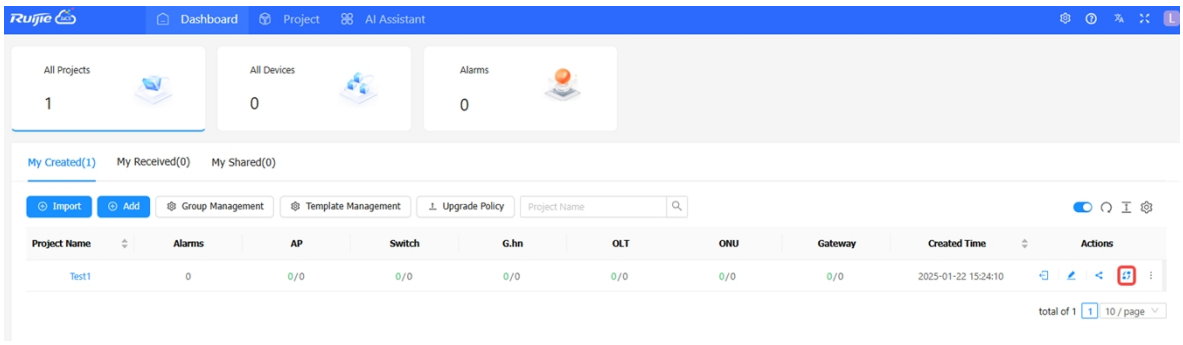
If you don’t want the project to be shared with another tenant, you can click **Cancel sharing** on the **My Shared** page to cancel the sharing.



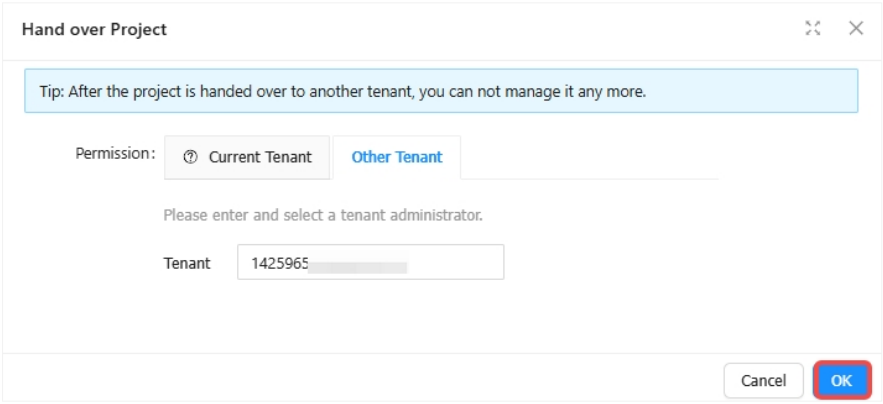
3.7 Handing over a Project

JaCS supports hand over a project to another tenant for management. The specific steps are as follows:

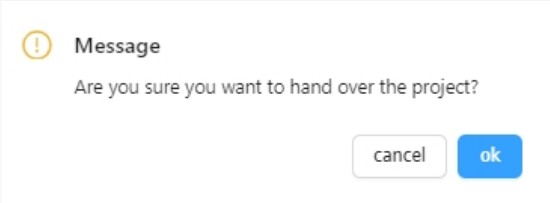
1 Click the handover icon in the **Action** column of the project.



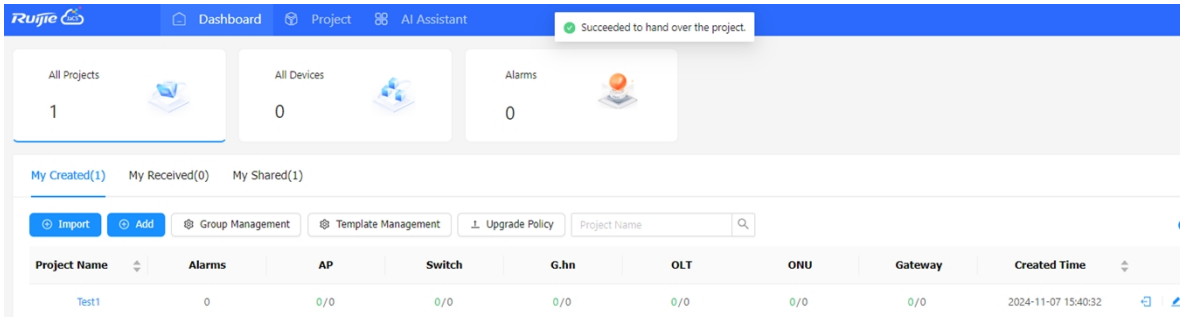
2 Click **Other Tenant**, then enter the recipient's email address and click **OK**.



3 When the “Are you sure you want to hand over the project?" message appears, click **OK**.



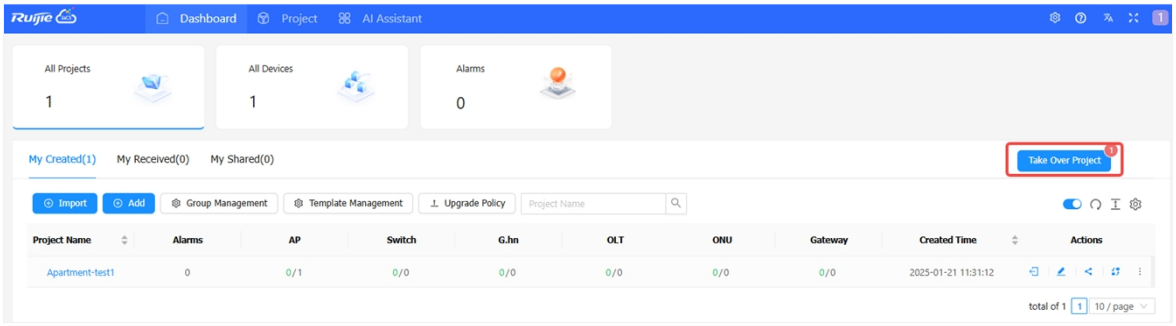
4 After the "Succeeded to hand over the project" appears, the handover is initiated.



Note

While the recipient has not received the project, the original tenant can still manage the project. Once the project is received by the recipient tenant, the original tenant cannot manage the project any more.

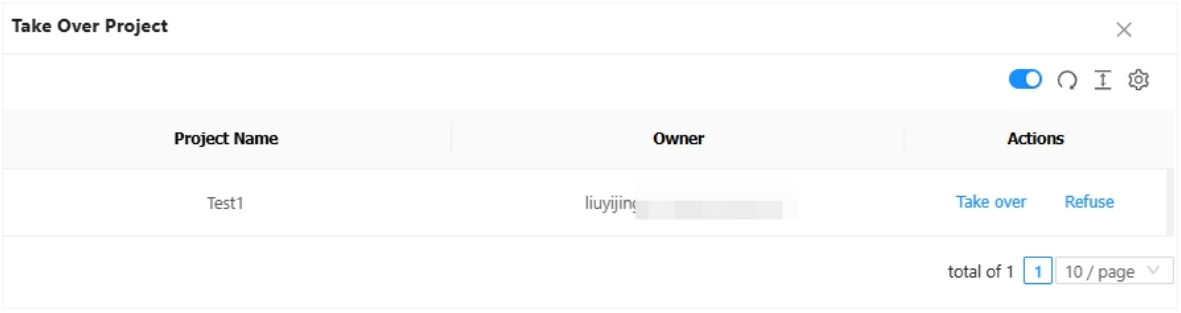
5 After the project handover is initiated, the recipient needs to log in to the system and click the **Take Over Project** on the **My Created** interface to receive the project.



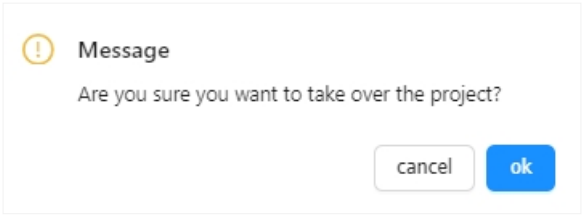
Note

The number in the red circle in the upper right corner of the **Take Over Project** button represents the number of projects currently waiting to be received.

6 Click **Take Over** to take over the project. If you do not want to take over the project, please click **Refuse**.

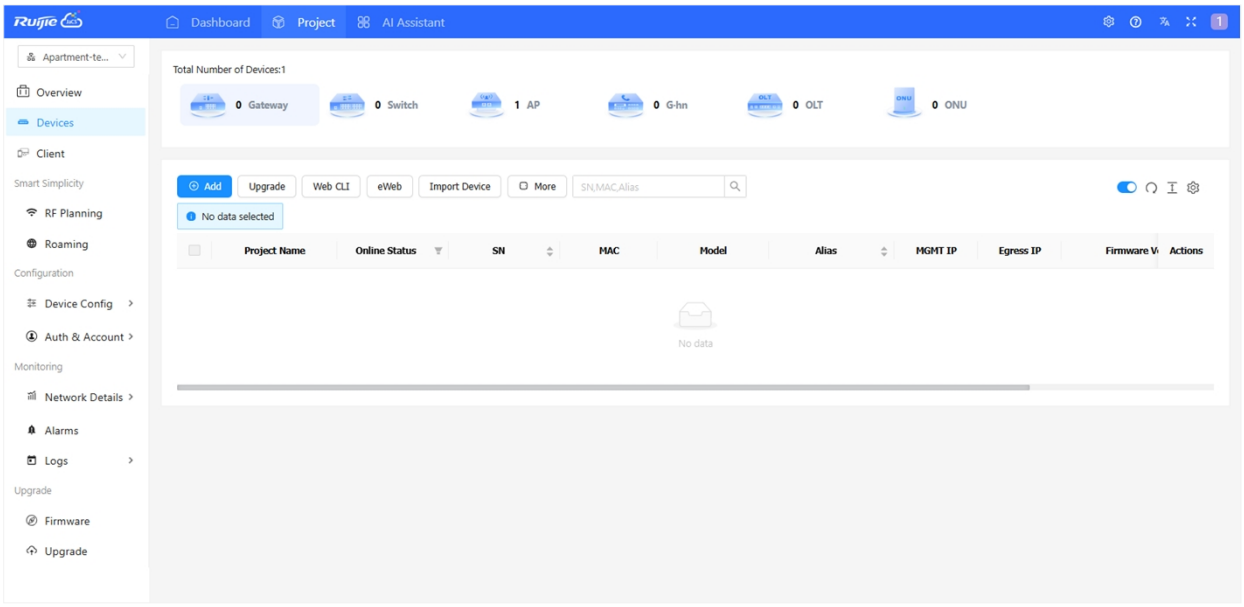


7 When “Are you sure you want to take over the project” appears, click **OK** to complete the operation.



4 Device Management

Currently, JaCS supports manage APs, switches, G.hn, OLT, ONU and gateways. For specific supported models, refer to Section 1.3. Click the device type icon to enter the corresponding management interface.



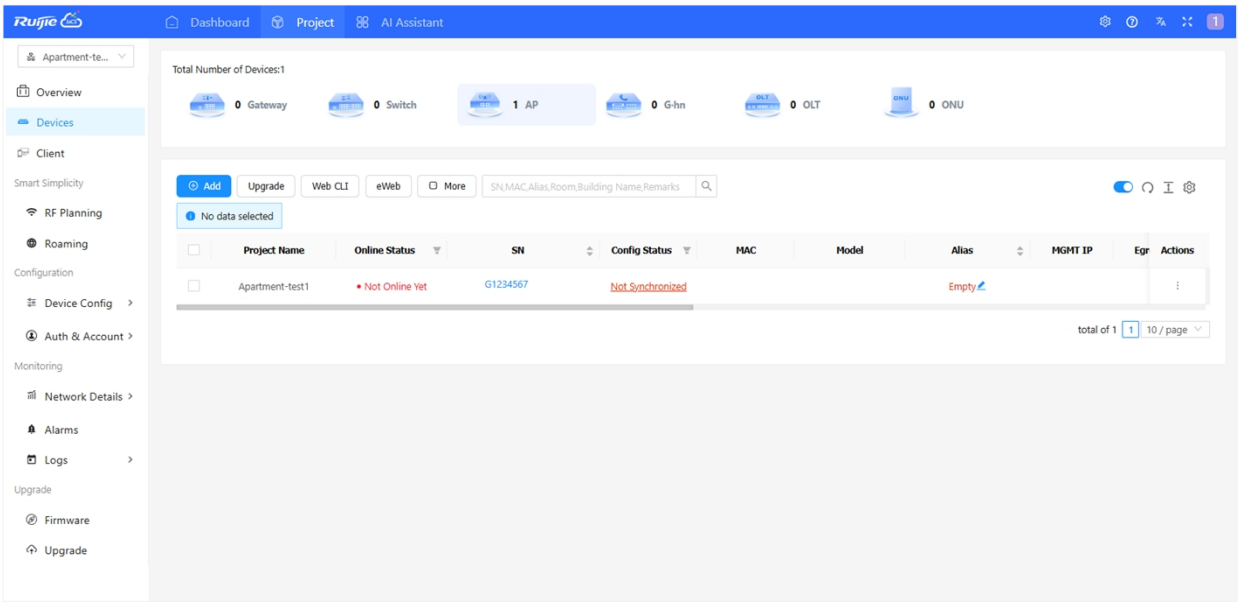
4.1 AP

This section mainly introduces the AP management interface and management operation steps, including:

- AP Management Interface: Introduces to the AP management interface of JaCS.
- Adding APs : Introduces how to add or batch add APs to an existing project.
- Deleting APs: Introduces how to delete or batch delete APs from a project.
- Moving APs: Introduces how to move an AP from its current project to another project.
- Restarting APs: Introduces how to remotely restart an AP through JaCS.
- Restoring APs to Factory Settings: Introduces how to restore an AP to factory settings through JaCS.
- Delivering Configuration via Web CLI: Introduces how to send configurations to APs via the WEB CLI.
- Accessing the AP's eWeb: Introduces how to use JaCS to create a tunnel to access the WEB GUI of an AP.
- Initial Configuration Template Management: Introduces how to use the initial configuration template to configure the AP180 series access points in the project.
- Device-specific Configuration Template Management : Introduces how to use and manage the device-specific configuration template to configure APs.

4.1.1 AP Management Interface

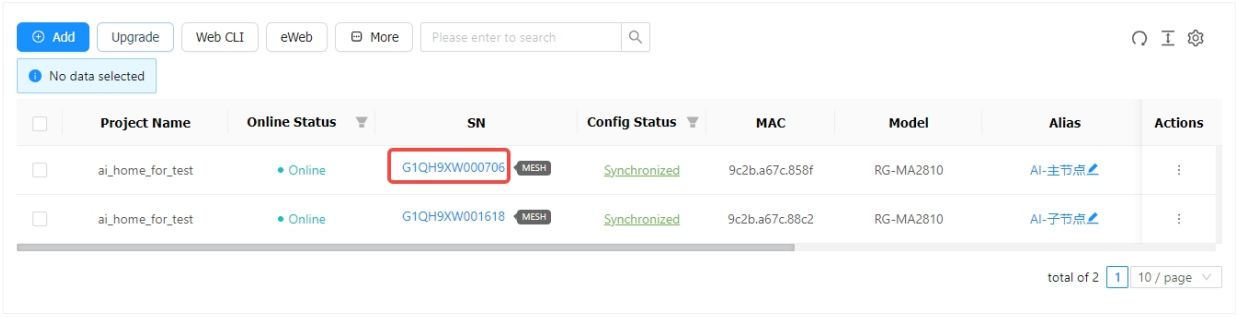
After creating a project, click **Project** > **AP** to enter its AP management interface.

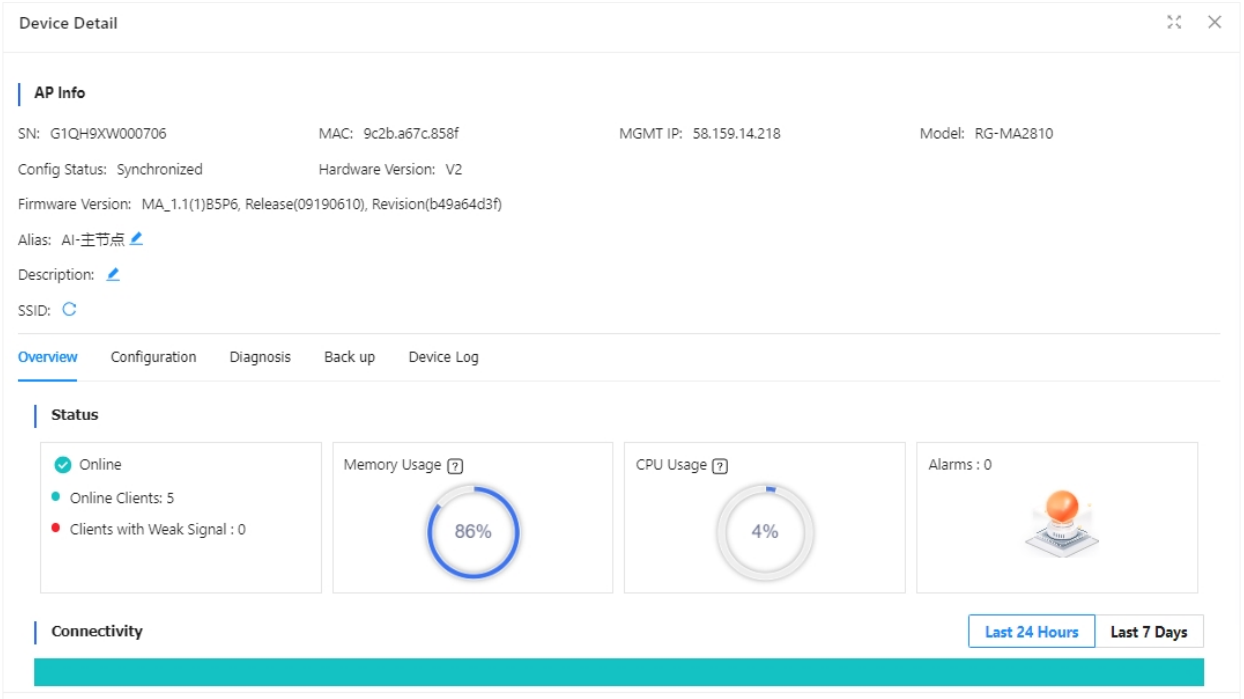


Items	Description
Project Name	Displays the names of the projects where APs reside.
SN	Displays the serial numbers of APs. Click the SN of an AP to display its detailed information.
Online Status	Displays the online status of APs on the cloud. The status of the device includes: Online/Offline/Not Online Yet. Click the filter icon to filter devices by online status. **Note:** ● **Online**: The device is online and communicating with the cloud normally. After the device is online, it will maintain a connection with the cloud every 3 minutes. ● **Offline**: The device has been disconnected from the cloud, but the physical connection is not affected. If the device fails to connect for three consecutive times, it will change from the Online state to the Offline state. ● **Not Online Yet**: The device has never been connected to the cloud. When an AP is added to a project on the cloud, but is not powered on, its status will also be shown as “Not Online Yet”.
Config Status	Displays the configuration status of APs. The configuration status includes: Switching mode/Not Synchronized/Synchronizing/Synchronized/Synchronize Failed. Click the filter icon to filter devices according to their configuration status.
MAC	Displays the MAC addresses of APs.
Model	Displays AP models.
Alias	Displays the aliases of APs.
MGMT IP	Displays the management IP addresses of APs.
Egress IP	Displays the egress IP addresses of APs.
Firmware Version	Displays the firmware versions of APs.
Last See On	Displays the last online time of the APs.
Actions	Delete button is available on the **Action** column. Click the delete button to remove the device from the project.

Button	Description
Add	Add button. Click this button to enter the device adding interface.
Upgrade	Upgrade button. After selecting the device, click this button to remotely upgrade the device.
Web CLI	Web CLI button. Click this button to enter WEB CLI page to deliver configurations to the device.
eWeb	eWeb button. Select an AP, and click this button to can access the eWeb of the device.
More	Click this button to display more operation buttons, including **move to**, **delete**, **reboot**, **set initial settings** and **restore factory settings**.
	Automatic refresh switch button. The automatic refresh function is enabled by default. When it is enabled, the AP device list will automatically refresh once every minute.
	Refresh button. Click this button manually to refresh the AP device list.
	Row height adjustment button. Click this button to adjust the row height.
	Click this button to customize the displayed items in the AP list.

After clicking the SN of a device in the AP list, you can view its details information





Tabs	Description
Overview	In this tab, you can view the device's statistics, including memory usage, CPU usage, alarms, connection status with the cloud platform, traffic information, radio frequency information, client information, etc.
Configuration	In this tab, you can set the AP's eWeb password.
Diagnosis	In this tab, you can diagnose the device through the Web CLI, tunnels and log collection.
Back up	In this tab, you can back up and export the current configuration of the AP.
Device Log	In this tab, you can view the logs of the device.

Note

The tabs displayed in the Device Detail page vary from different device models. Please subject to the actual tabs displayed.

4.1.2 Adding APs

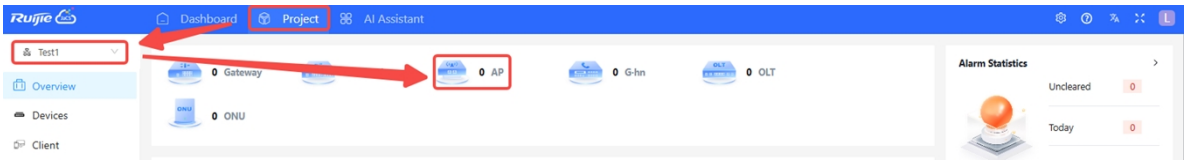
JaCS provides two ways to add APs to a specific project.

- Adding an AP
- Adding APs in Batches

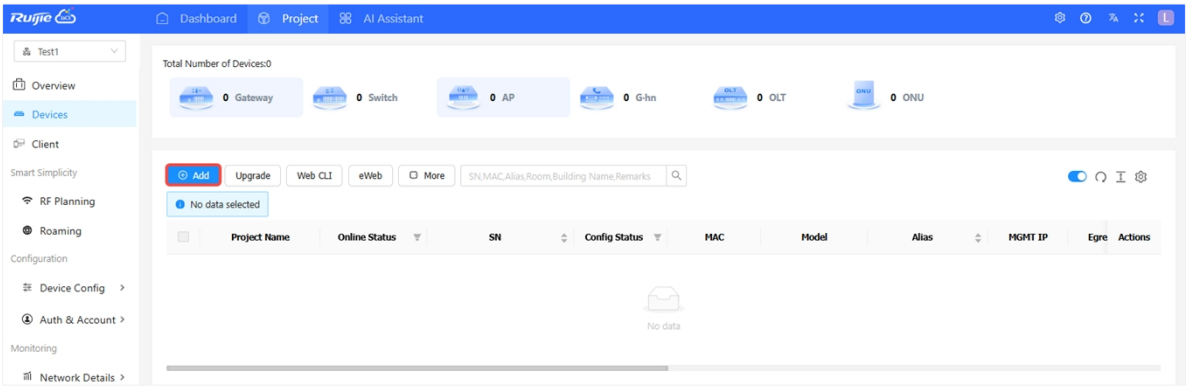
4.1.2.1 Adding an AP

This method is suitable for scenarios where you only need to add a few devices to an existing project. The specific steps are as follows:

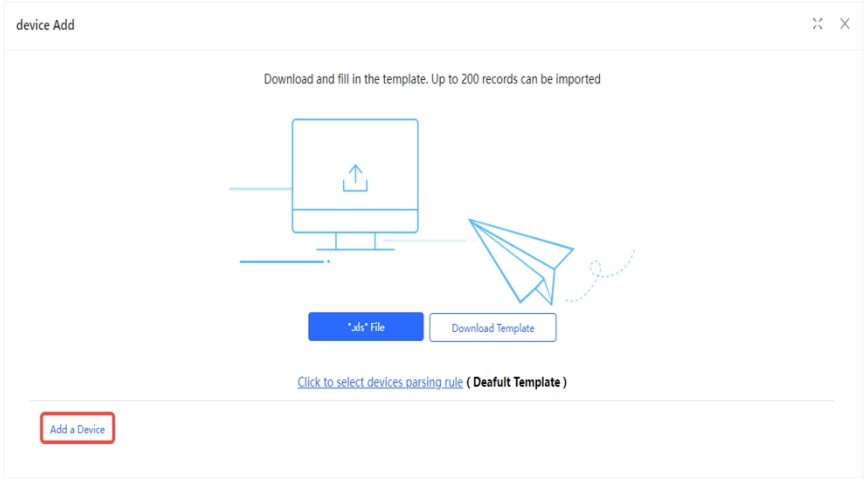
1 Enter the **Project** interface, select the project where the AP is going to be added, and then click **AP** to go to the AP management interface.



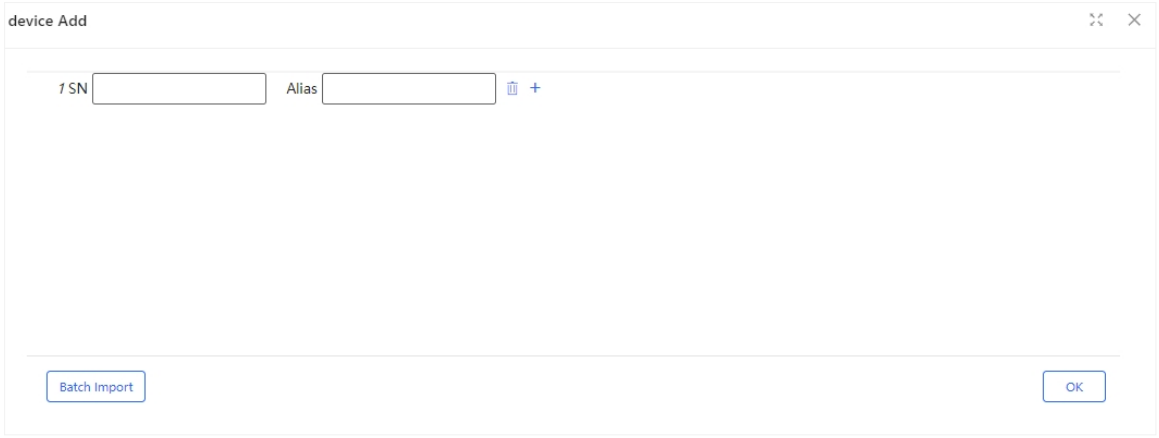
2 Click **Add** to go to the adding interface.



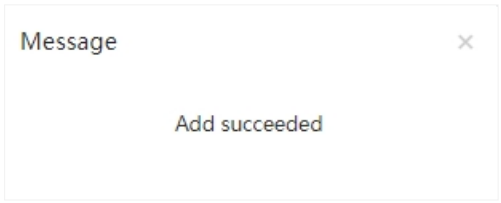
3 Click **Add a Device**.



4 Enter the device's SN (required) and alias (optional). If you need to add multiple APs, click + to add them. After enter the SN, click **OK**.



5 After the "Add Succeeded" appears, the operation is completed. The added device will be displayed in the AP list.

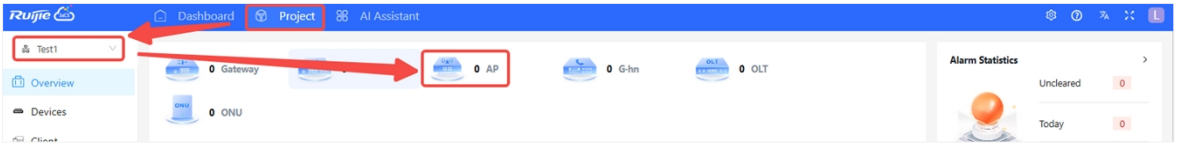


4.1.2.2 Adding APs in Batches

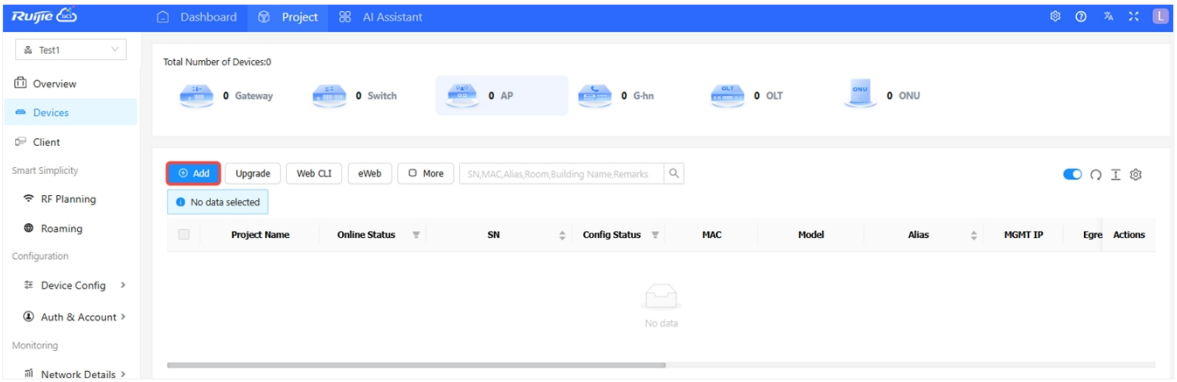
This method is suitable for the situation where no more than 200 devices need to be imported in batches at one time.

Follow the steps below to import APs into an existing project in batches for management.

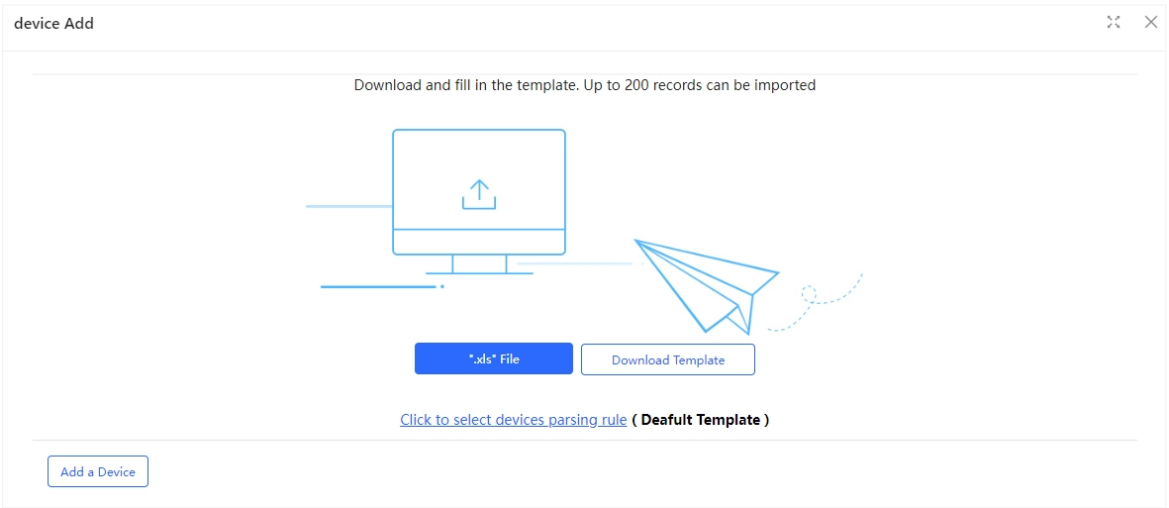
1 Enter the **Project** interface, select the project where the APs is going to be imported, and then click **AP** to go to the AP management interface.



2 Click **Add** to go to the adding interface.



3 Click **Download Template**. (Up to 200 devices can be imported via the template each time.)



4 Fill in the template, and then click **".xls" File** to upload the template or your custom template. The imported device will be displayed in the AP list.

- **Introduction to the default batch import template:**

If the project scenario is set to hotel or others, the batch import template is as follows:

	A	B	C	D
1	SN	Alias	Latitude	Longitude
2				
3				

Items	Description
SN	Required. Enter the SN of the device. The length should range from 6 to 20 characters. Example: G1PD7PW00060B
Alias	Optional. Specify the alias of the device. Up to 64 characters can be entered.
Latitude	Optional. Latitude range: - 90° to 90°
Longitude	Optional. Longitude range: -180° to 180°

If the project scenario is set to the apartment, the batch import template is as follows:

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

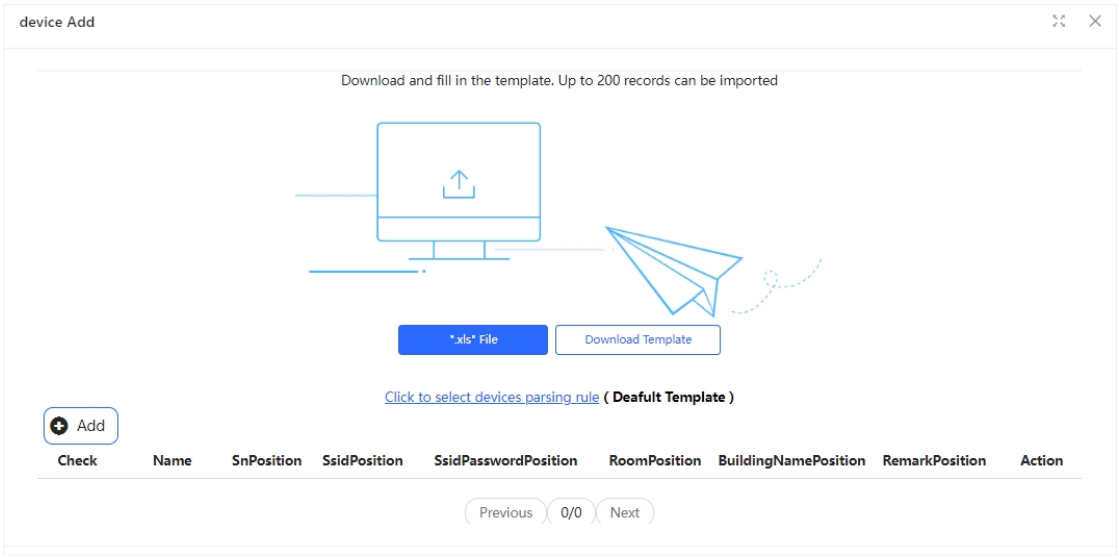
Items	Description
Model	Optional. Enter the product model. For example: RG-AP180-PE
SN	Required. Specify the device SN. The SN length ranges from 6 to 20 characters. For example: G1PD7PW00060B
MAC	Optional. Specify the MAC address of the device.
PN	Optional. Specify the part number, which can be left blank.
SSID	Optional. The length of the SSID ranges from 4 to 32 characters. The supported characters include letters, numbers, and special symbols ("_", "-", "." or "@"). When setting multiple SSIDs, separate them with commas (,), such as: ssid-test1, ssid-test2.
SSID Password	Optional. The length of the password should range from 8 to 32 characters. The supported characters include letters, numbers, and special symbols (@!*#<>=[]()._-). When setting multiple passwords, separate them with commas (,), such as: 8888888rrrrr, 999999ddddd.
Alias	Optional. Specify the alias of the device. Up to 64 characters can be configured.
Room	Optional. Specify the room number where the AP is located. For example: 301. Supports entering 1 to 32 characters.
Building Name	Optional. Specify the building name. Up to 32 characters can be configured.
Remark	Optional.

	Up to 32 characters can be entered.

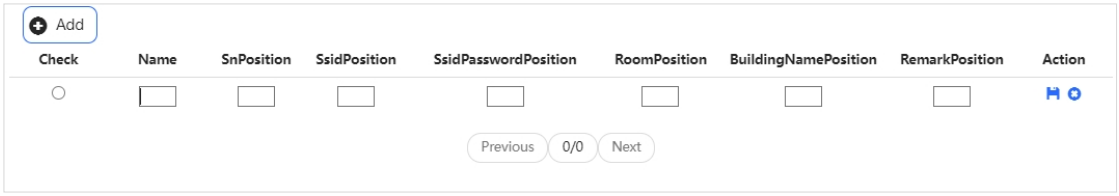
➢ **Introduction to the custom batch import template:**

To use a custom configuration template, follow these steps to customize a template:

1) Click "Click to select devices parsing rule".



2) Click to modify the default parsing rules, or click the **Add** button to add new rules.

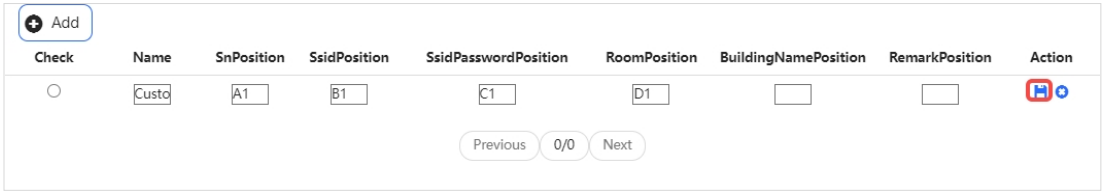


Items	Description
Name	Specifies the template name.
SnPosition	Specifies the starting column position of SNs in the template.
SsidPosition	Specifies the starting column position of SSIDs in the template.
SsidPasswordPosition	Specifies the starting column position of SSID passwords in the template.
RoomPosition	Specifies the starting column position of room numbers in the template.
BuildingNamePosition	Specifies the starting column position of building names in the template.
RemarkPosition	Specifies the starting column position of remarks in the template.

Note

- Users can customize the parsing rules in Excel files from columns A1-Z1 and rows 1-15.
- The custom template format supports .xls only.
- If an entry is left blank, it will not be imported when the template is uploaded.

3) After setting the rules, click the save icon. When "Do you want to save the parsing rule" appears, click **OK**.



4) After the "The parsing rule added successfully" prompt appears, the rule is added.

5) Create a new blank .xls file, fill in the relevant information in the corresponding position and save it.

	A	B	C	D
1	12345667	SSID-TEST	admin@ruijie	101
2				

4.1.3 Deleting APs

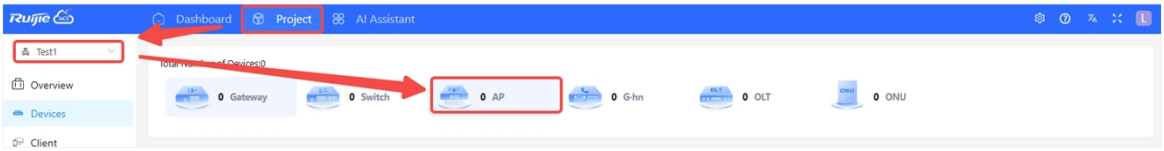
JaCS provides two ways to delete an imported AP from a specific project.

- Deleting a AP
- Deleting APs in Batches

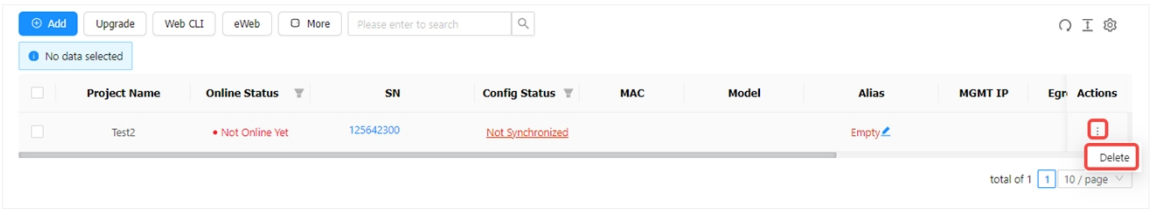
4.1.3.1 Deleting a AP

Follow the steps below to delete an AP from a specific project.

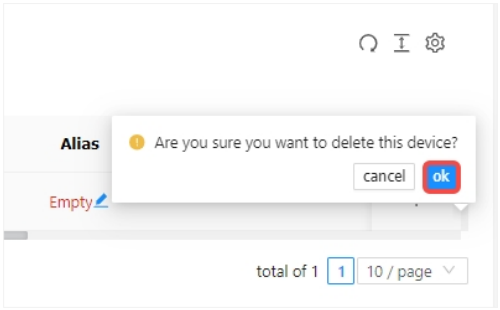
1 On the **Project** interface, select the project where the AP resides, and then click **AP** to enter the AP management interface.



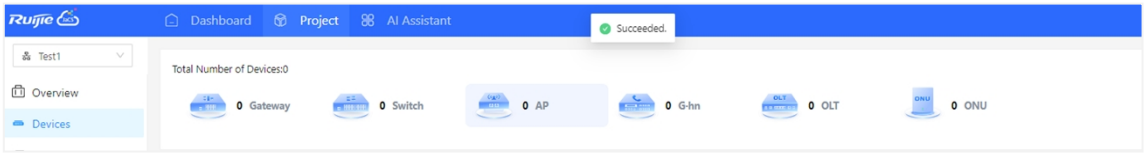
2 Hang over your cursor on the ⋮ icon in the **Action** column of the AP to be deleted, and then click **Delete**.



3 When the deletion confirmation prompt appears, click **OK**.



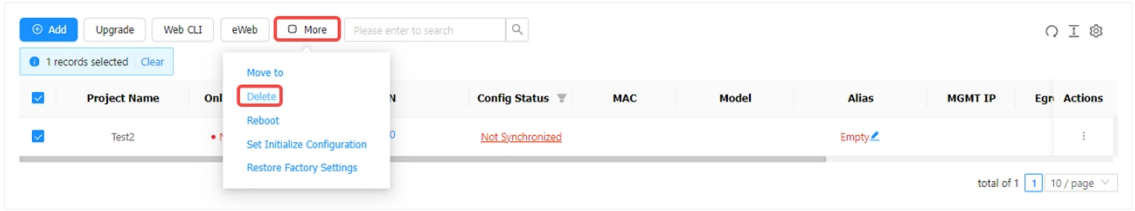
4 When the "Succeeded" prompt appears, the operation is completed.



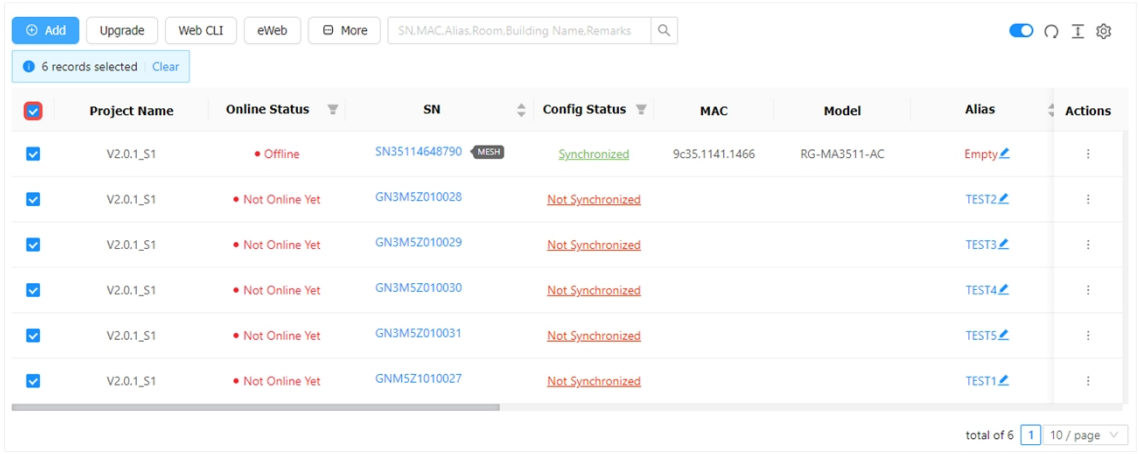
4.1.3.2 Deleting APs in Batches

Follow the steps below to delete APs in batches:

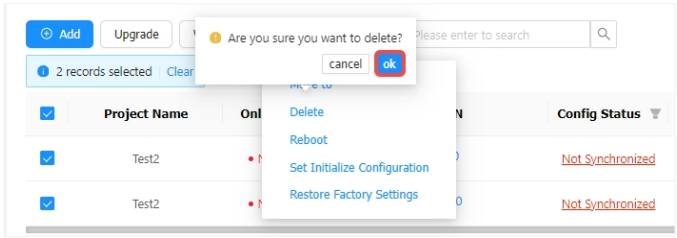
1 Select the APs to be deleted, click **More**, and then click **Delete**.



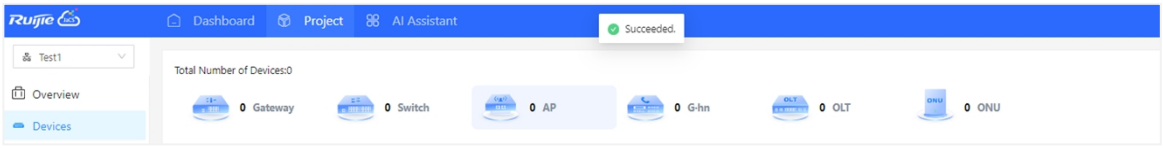
If you want to delete all APs, you can check the **Select All** checkbox.



2 After "Are you sure you want to delete the device?" prompt appears, click **OK**.



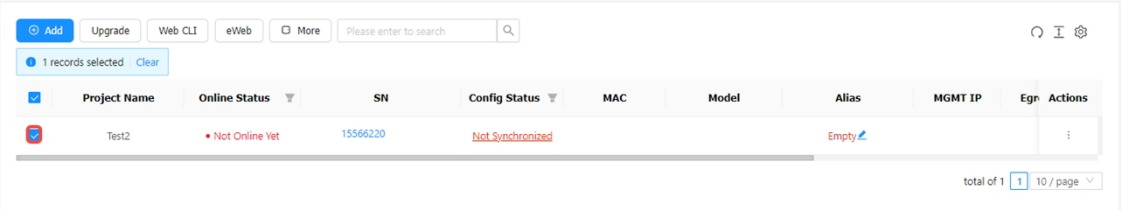
3 After the "Succeeded" prompt appears, the operation is completed.



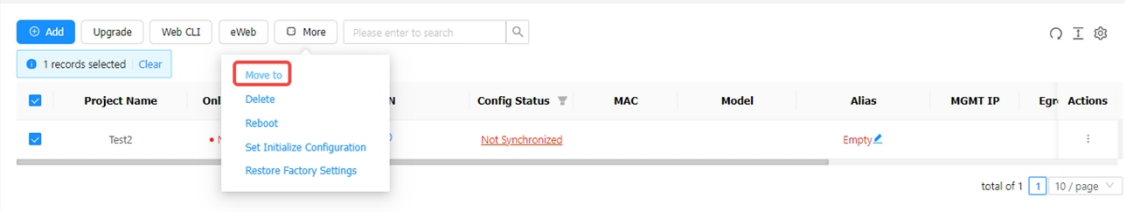
4.1.4 Moving APs

Follow the steps below to move an AP of a project to another project. After moving, all configurations and rules of the new project will be applied to the AP.

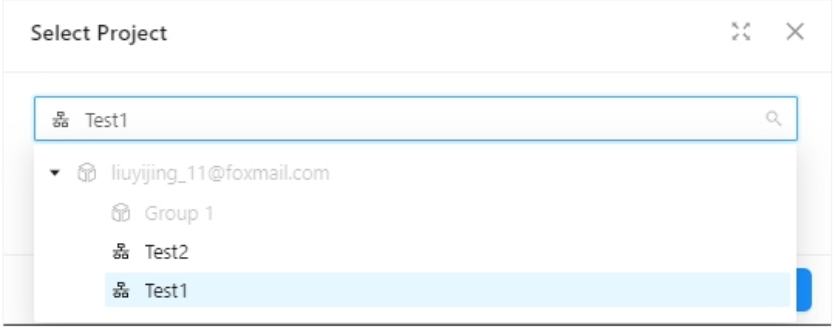
1 Select the AP to be moved.



2 Click **More** and select **Move to**.



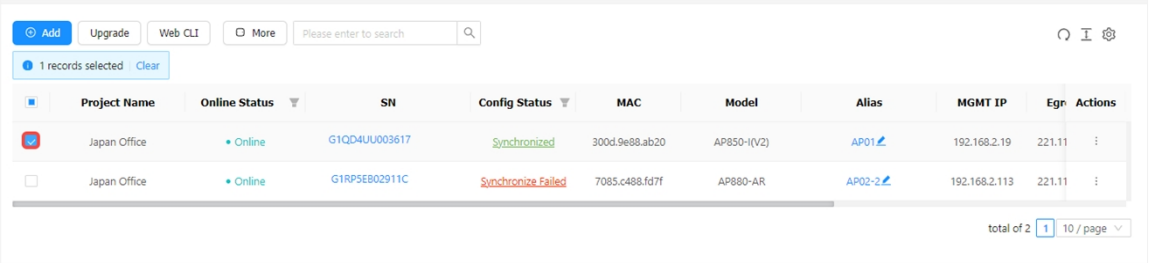
3 Select the new project and click **OK** to complete the operation.



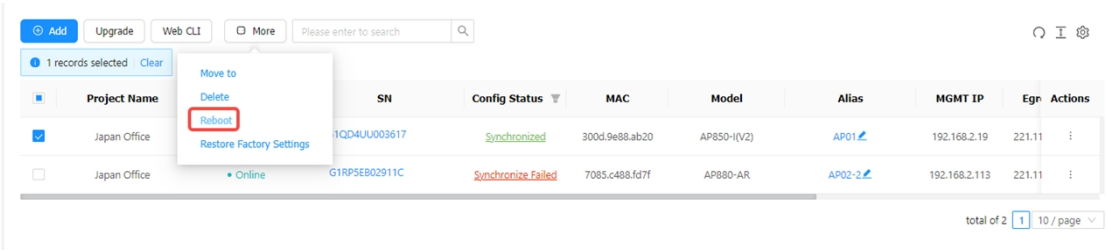
4.1.5 Restarting APs

Follow the steps below to restart a AP remotely via JaCS.

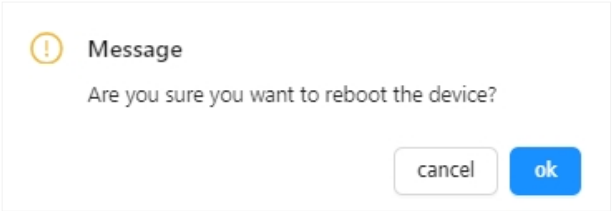
1 Select the devices that need to be restarted.



2 Click **More**, and then click **Reboot**.



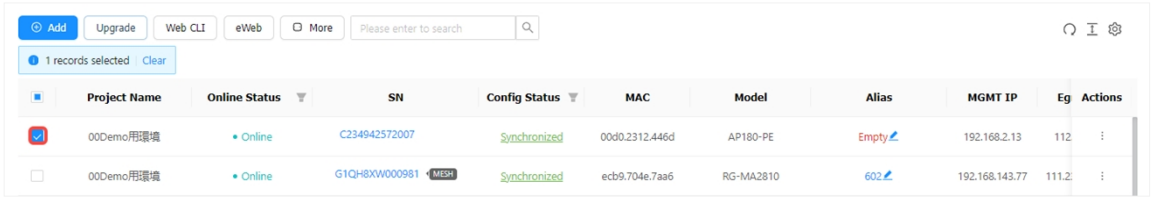
3 When the operation confirmation box appears, click **OK** to complete the operation.



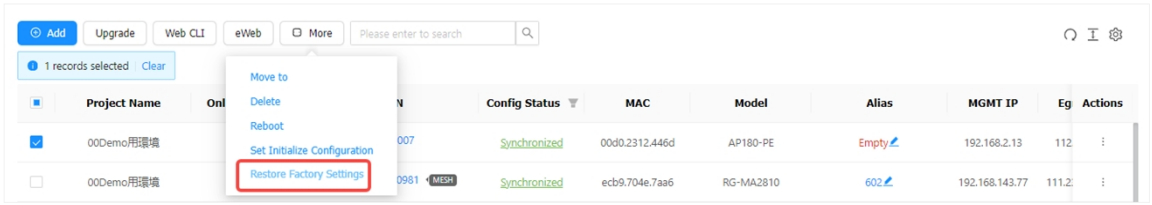
4.1.6 Restoring APs to Factory Settings

Follow the steps below to restore an AP to factory settings. This function is only supported on RG-AP180 series access points.

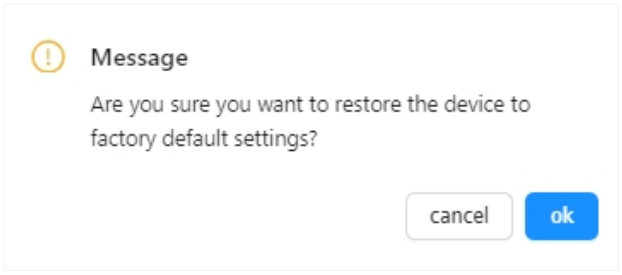
1 Select the AP to be restored to factory settings.



2 Click **More**, and then click **Restore Factory Settings**.

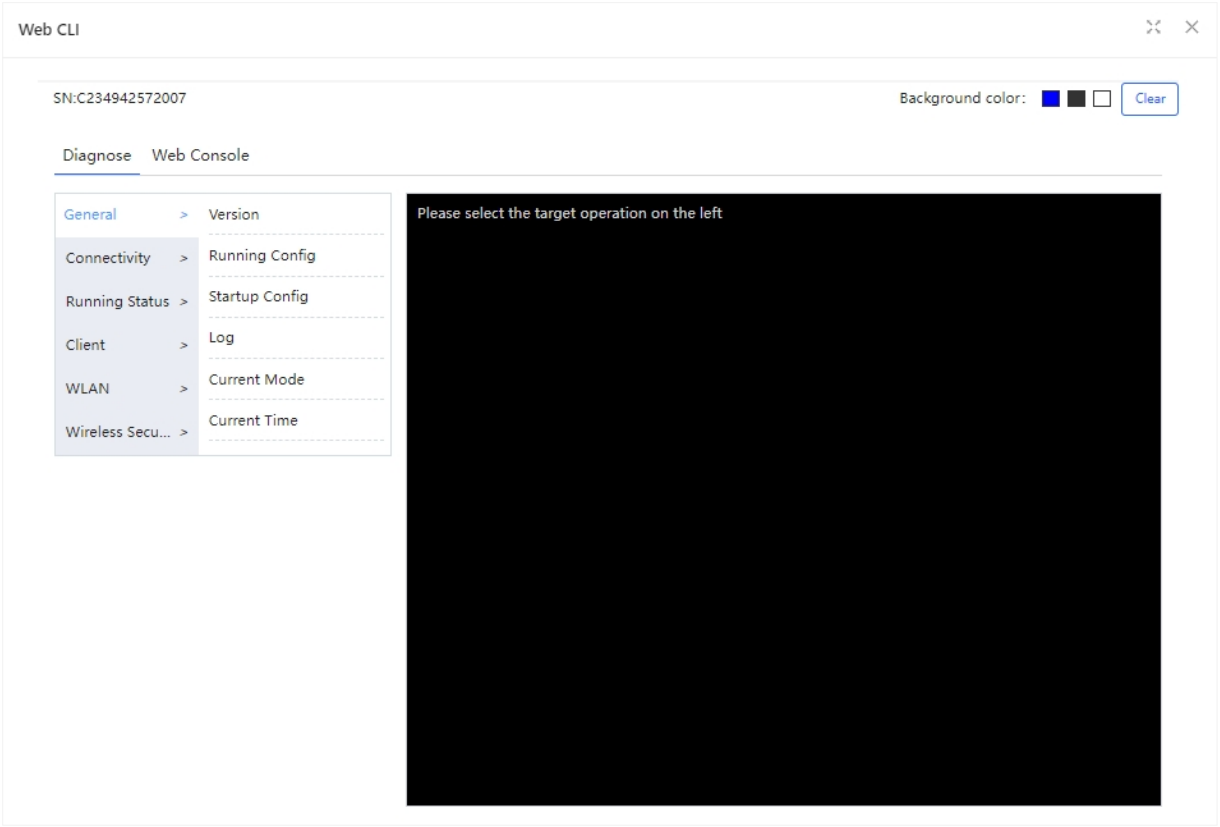


3 When the confirmation box appears, click **OK** to complete the operation.



4.1.7 Delivering Configuration via Web CLI

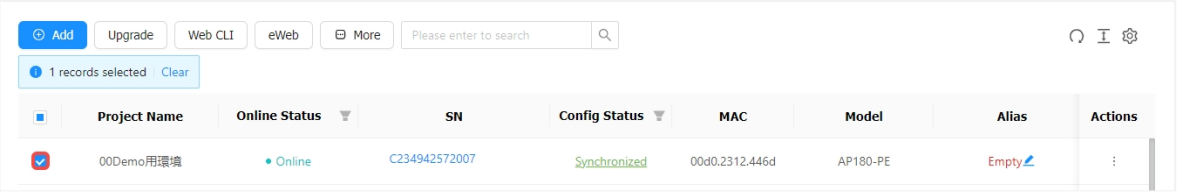
Click **Web CLI** to open the device's Web CLI interface. Web CLI is mainly used to view device configuration information, diagnose device connectivity, and view device operating status. Also, Web Console provides a function similar to Telnet, which can remotely connect to the device and manage the device by entering the CLI commands, which is convenient and easy to use.



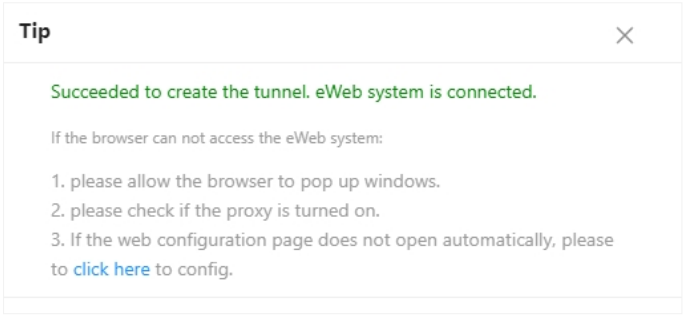
4.1.8 Accessing the AP's eWeb

Follow the steps below to access the AP's eWeb via JaCS:

1 Select the device and click **eWeb**.



2 After creating the tunnel, the eWeb interface of the device will automatically open in a new tab. If the eWeb of the device does not open automatically, you can click **click here** to jump manually or try to recreate the tunnel.



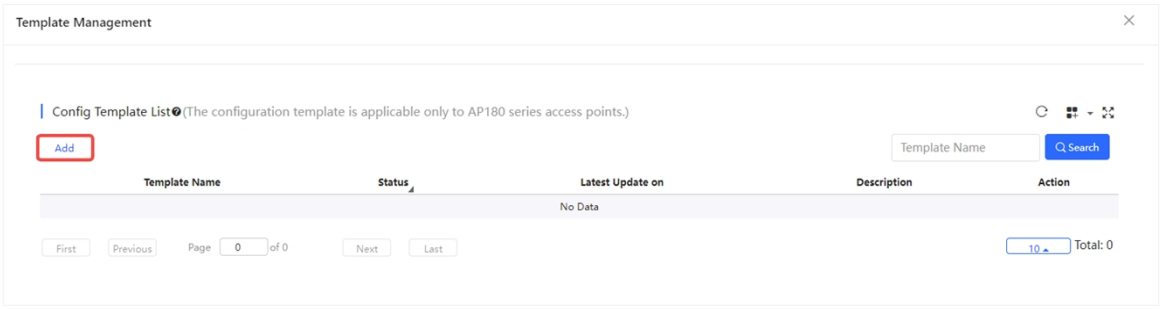
4.1.9 Initial Configuration Template Management

Once an initial configuration template is applied to a project, JaCS will send the configuration in the template to the APs in the project when they go online for the first time. Currently, this function only supports RG-AP180 series access points and RG-MA3511 series products.

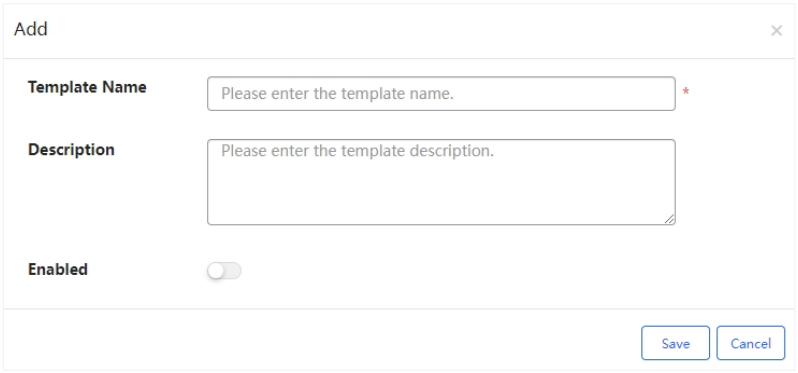
4.1.9.1 Creating an Initial Configuration Template

Navigate to **Dashboard** > **My Created** > **Template Management** to enter the initial template configuration management interface. And then follow the steps below to create an initial configuration template:

1 Click **Add**.



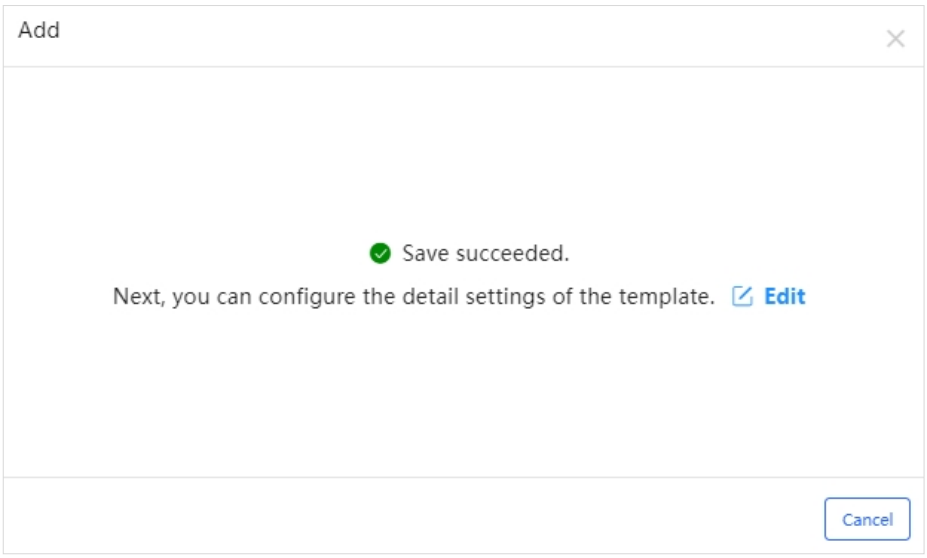
2 Enter the template name (required), template description (optional), select the template status, and then click **Save**.



Note

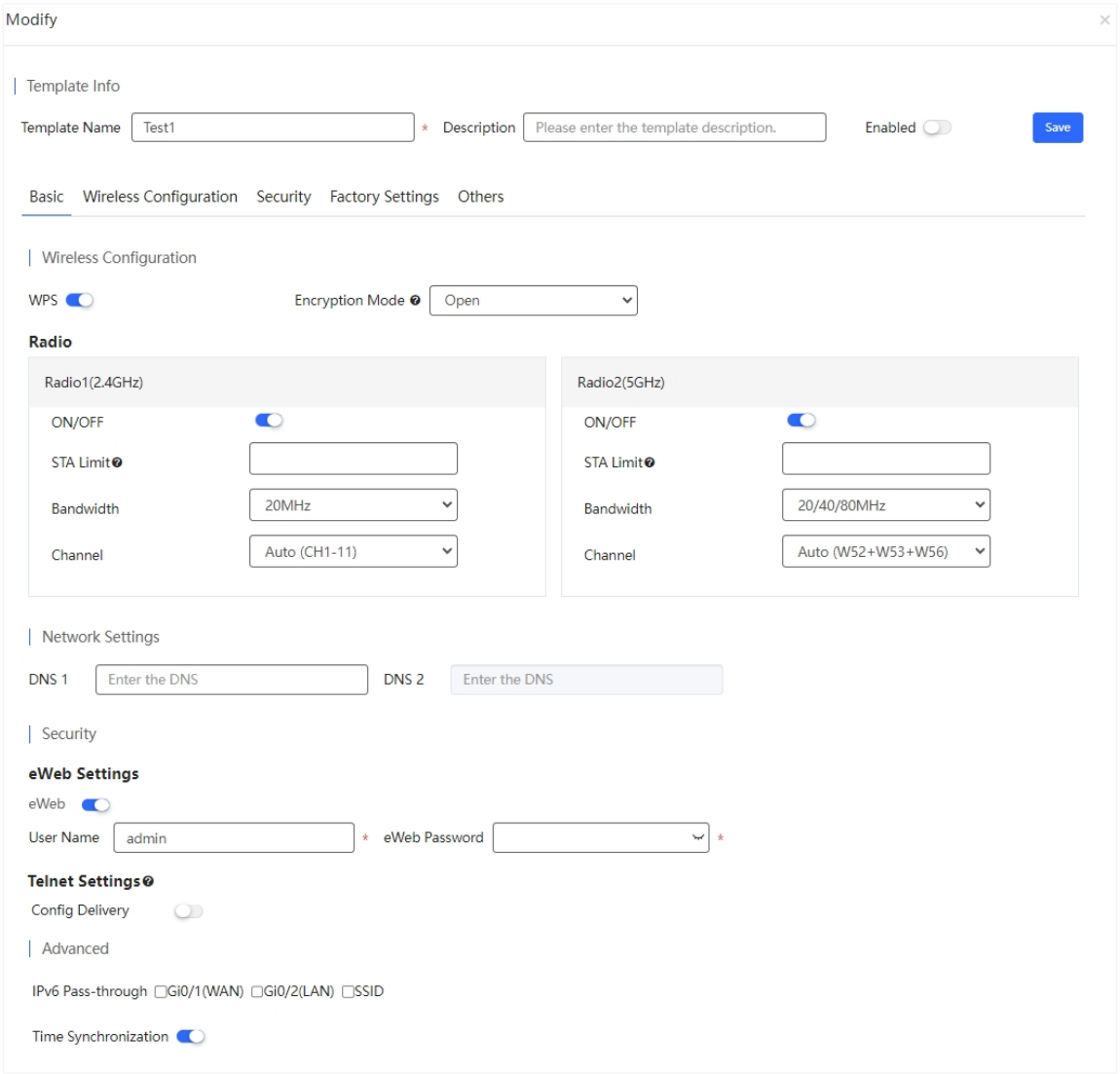
- The template is disabled be default.
- The length of template name cannot exceed 64 bytes, and the length of the description cannot exceed 128 bytes.

3 After saving the template, click **Edit** to further configure the template.



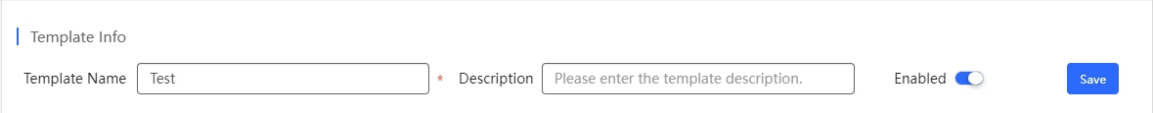
4 Set the initial template configuration as needed. After the specifying the configuration, click **Save**.

The initial configuration template consists of the following parts: template basic information, basic configuration, wireless configuration, security configuration, factory configuration and other configuration interfaces.



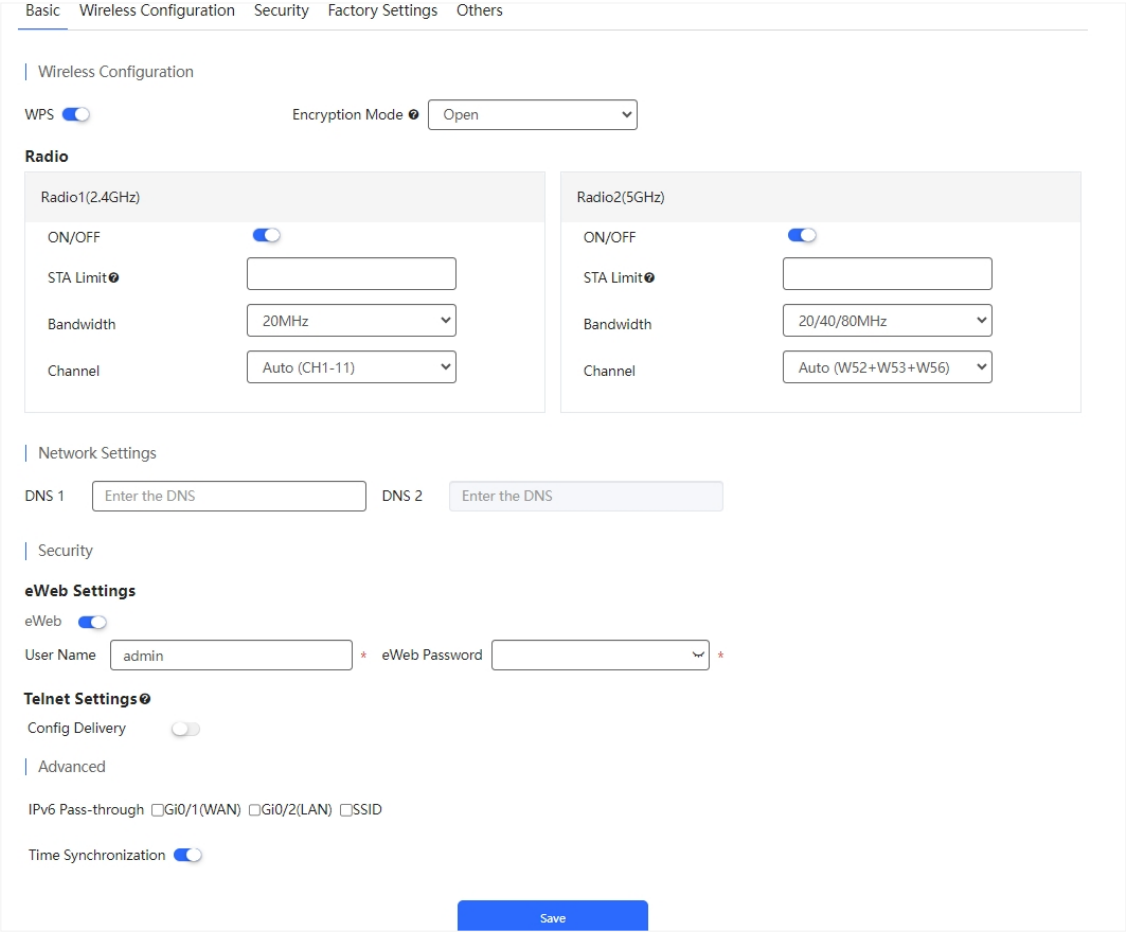
(1) Template Information

In the template configuration tab, you can modify the template name, template description and template status. After modifying the information, click **Save**.



(2) Basic Configuration

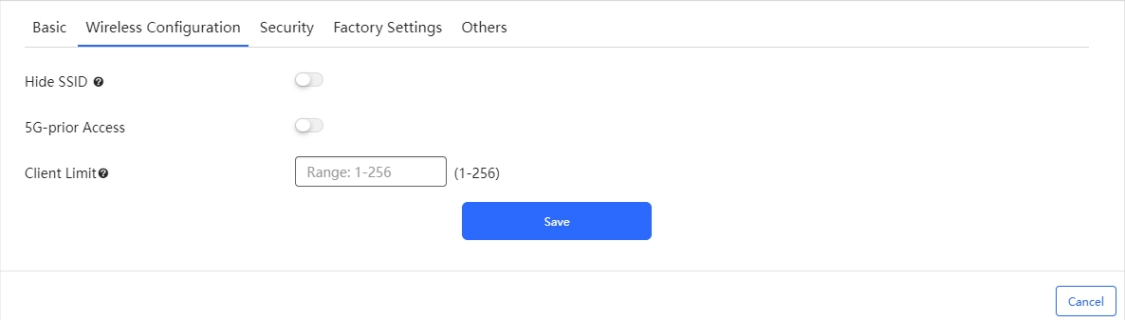
The Basic configuration tab includes wireless configuration, network settings, security settings and advanced settings. The specific configuration items are as follows:



Items	Description
Wireless Configuration	
WPS	The WPS is enabled by default. WPS, or Wi-Fi Protected Setup, is a network security designed to simplify the process of connecting devices to a secure wireless network. It was developed by the Wi-Fi Alliance to make it easier for users to set up and manage their Wi-Fi networks without needing to remember complex passwords or go through complicated configuration processes.
Encryption	**Defaults**: Open. **Options:** Open, WPA -PSK, WPA2-PSK, and WPA/WPA2-PSK

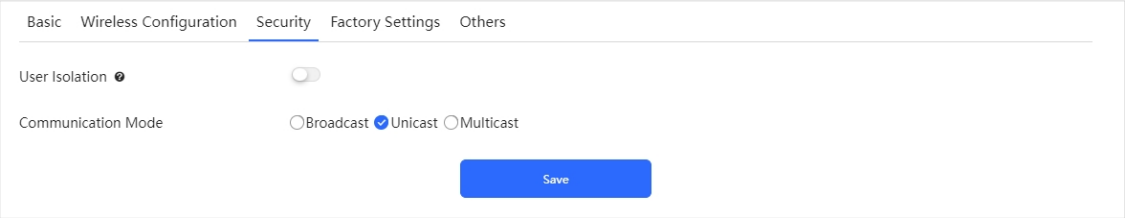
Radio Frequency	
ON/OFF	Radio frequency switch button. Radio 1 (2.4GHz) and Radio 2 (5GHz) are enabled by default.
SAT Limit	Optional. Set the limited number of SATs allowed to access the AP. Range: 1-100.
Bandwidth	**Defaults**: Radio1 (2.4GHz) —— 20 MHz ; Radio2 (5GHz) —— 20/40/80MHz. **Options**: Radio1 (2.4GHz): 20 MHz and 20/40 MHz Radio2(5GHz): 20 MHz; 40 MHz; 80 MHz; 20/40 MHz; 20/40/80 MHz; 20/40/80/160 MHz
Channel	**Defaults:** Radio1(2.4GHz) —— Auto (CH1-11) ; Radio2(5GHz) —— Auto (W52+W53+W56) **Options:** Radio1(2.4GHz): Auto (CH1-11); Auto (CH1-13) Radio2(5GHz): Auto (W52+W53); Auto (W52); Auto (W52+W53+W56)
Network Settings	
DNS 1	Optional. Set the preferred DNS.
DNS 2	Set the alternative DNS.
Security Settings	
eWeb 	The eWeb is enabled by default**.**
User name	Set the eWeb login account name. **Defaults**: admin
eWeb	Set the login password for eWeb. The password length must range from 8 to 31 characters. The supported characters include letters, numbers, and special characters (@!*#<>=[]()._-).
Telnet	
Config Delivery	**Defaults**: Disabled. It is not recommended to enable this feature. If this feature is enabled and a Telnet password is configured, the Telnet password will be sent to the device. If this feature is enabled but a Telnet password is not configured , the Telnet password configuration of the device will be cleared.
Advanced Settings	
IPv6 Pass-through	**Defaults**: N/A. You can configure the IPv6 pass-through function to control the device's ability to forward IPv6 packets. If the IPv6 pass-through function is disabled, the device will discard received IPv6 packets, thus preventing irrelevant IPv6 packets in the network from occupying device operating resources and affecting network performance. **Options**: Gi0/1(WAN), Gi0/2(LAN) and SSID
Time Synchronization	**Defaults**: Enabled. When the time synchronization is enabled, the device time can be synchronized through the NTP protocol so that the device time will be consistent with the time on the NTP service.

(3) Wireless Configuration Tab



Items	Description
Hide SSID	**Defaults**: Disabled.
5G-prior Access	**Defaults**: Disabled. When the 5G-prior access is enabled, the device preferentially guides clients to access the 5GHz band.
Client Limit	Optional. Set the limited number of clients that can be connected to each AP (Range: 1-256). If it is left blank, it means that no number limit.

(4) Security Configuration Tab



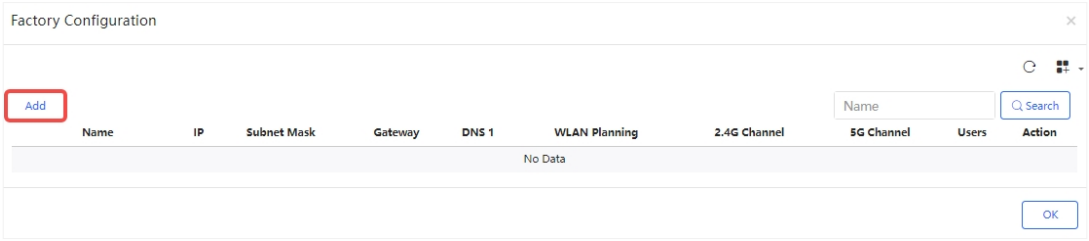
Items	Description
User Isolation	**Defaults**: Disabled Set user isolation mode. Currently only supports Layer 2 isolation. When user isolation is enabled, intra-SSID isolation, inter-SSID isolation, and LAN - WLAN isolation are automatically enabled by default. **Options**: Inter-SSID: When the inter-SSID isolation is enabled, clients under different SSIDs will not be able to communicate with each other. Intra-SSID: When the intra-SSID isolation is enabled, clients under the same SSID will not be able to communicate with each other. LAN-WAN: When the LAN-WAN isolation is enabled, clients under the LAN and SSID will not be able to communicate with each other.
Communication Mode	**Defaults**: Unicast. **Options**: Broadcast/Unicast/Multicast

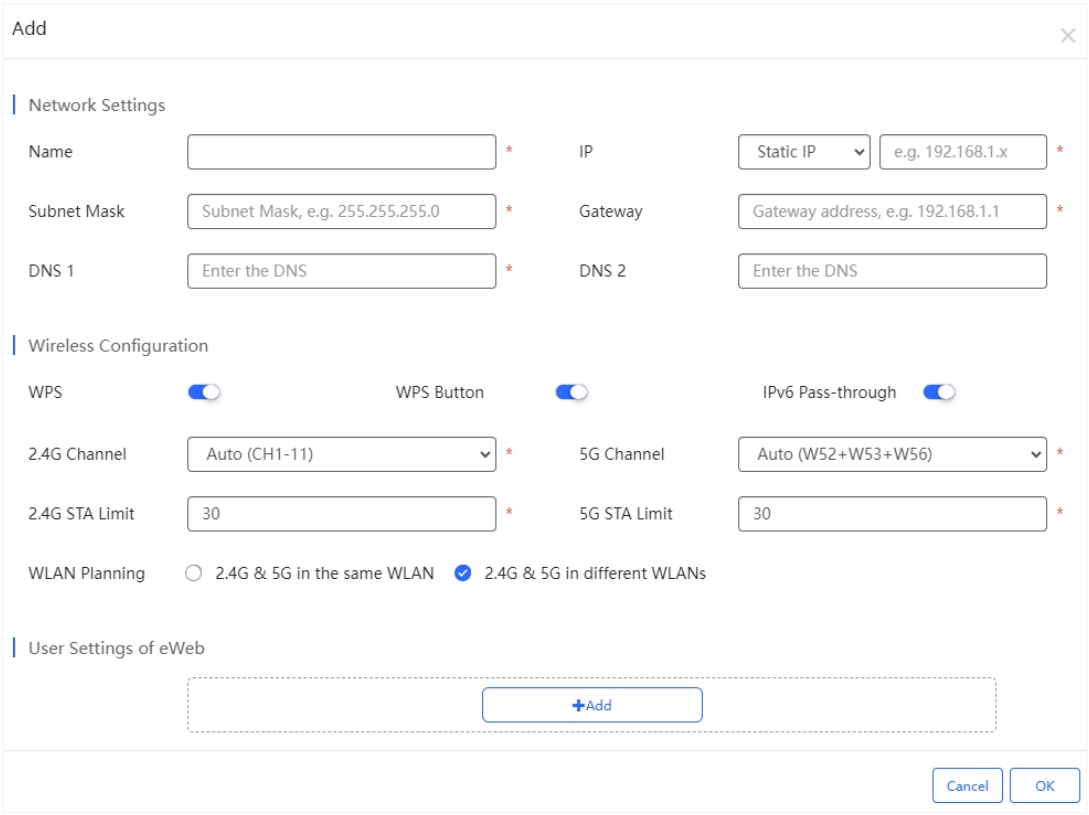
(5) Factory Configuration Tab

The factory settings refer to the configurations kept after the device is restored to factory settings. The factory settings take effect only after resetting the device by pressing its reset button. After the factory settings take effect, all global configurations and other configurations will be cleared.

You can use an existing template or click **Manage** to create a new one. The specific steps are as follows:

a. Click **Add** to enter the template creation interface.

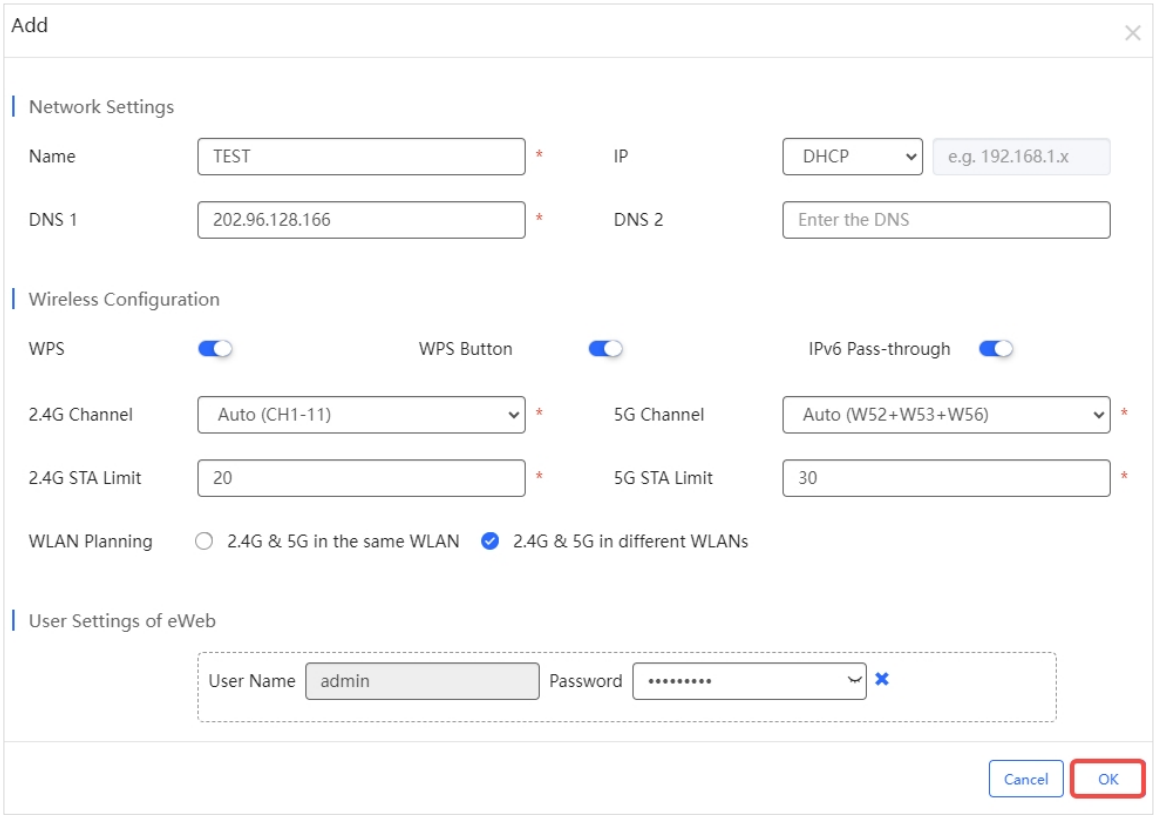




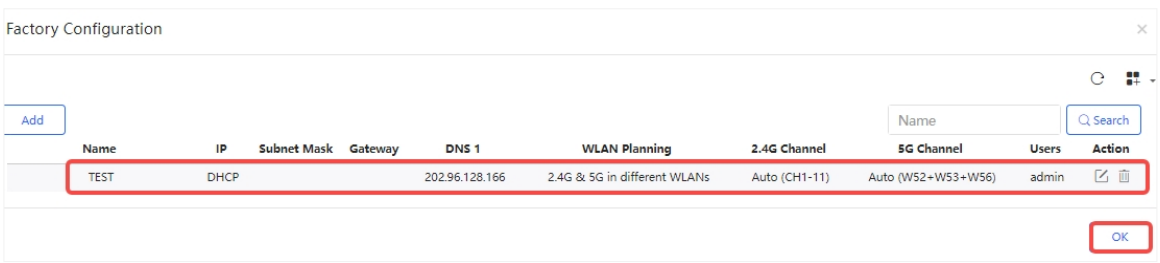
Items	Description
Network Settings	
Name	Required. Specify the template name.
IP	Optional. Specify the IP address. Supports configuring static IP or obtaining IP address through DHCP.
Subnet Mask	Required. Specify the subnet mask.
DNS 1	Required. Set the preferred DNS.
DNS 2	Optional. Set the alternative DNS address.
Wireless Setup	
WPS	**Defaults**: Enabled
WPS Button	**Defaults:** Enabled. Used to control whether the WPS button on the device panel works.
IPv6 Pass-through	**Defaults:** Enabled.

2.4G Channel	**Defaults**: Auto (CH1-11). **Options**: Auto (CH1-11) /Auto (CH1-13)
5G Channel	**Defaults**: Auto (W52+W53+W56). **Options**: Auto (W52+W53); Auto (W52); Auto (W52+W53+W56)
2.4G STA Limit	Required. Set the limit number of STAs allowed to access 2.4 GHz. **Defaults**: 30
5G STA Limit	Required. Set the limited number of STAs allowed to access 5GHz. **Defaults**: 30
WLAN Planning	**Defaults**: 2.4G and 5G are in different WLANs. **Options**: 2.4G & 5G in the same WLAN; 2.4G & 5G in different WLANs .
eWeb Account Settings	
Username	**Defaults**: admin.
Password	Set the password for the admin user.

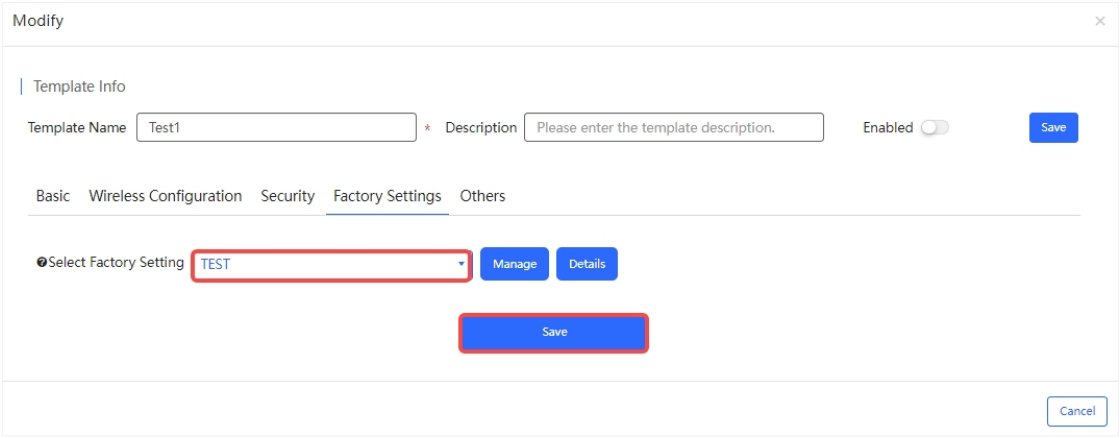
b. After filling in the required information, click **OK** to save the factory configuration template.



c. Once a template is created, it will be displayed in the list. Click **OK** to return to the factory setting page.



d. Pull down the selection box and select the newly created template, and then click **Save**.

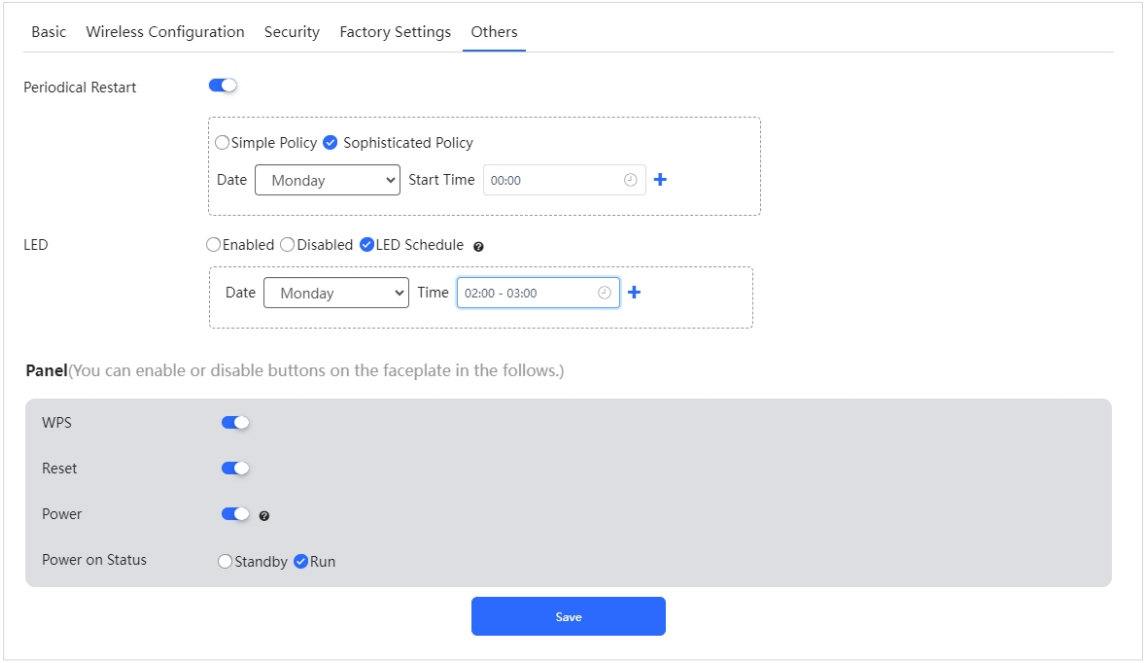


Note

- After restoring factory settings, you need to press the device's reset button to make the factory settings take effect. After the settings take effect, all global configurations and other configurations will be cleared.
- If you change the factory settings of the template, it will take effect in all projects to which the template is applied. Only the factory setting template that has not been applied can be deleted.

(6) Other Configuration Tabs

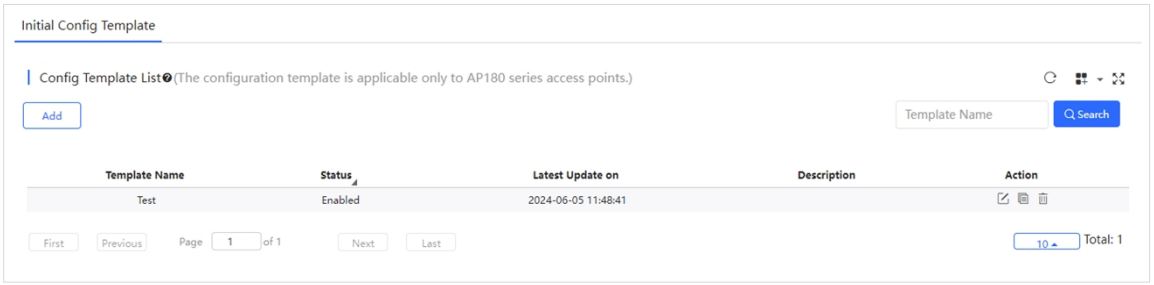
The Other configuration tab supports setting scheduled restarts, managing LED lights, and remotely disabling or enabling the buttons on the device.



Items	Description
Periodical Restart	Restart the switch in a specific time. This function is disabled by default. After it is enabled, you can configure the scheduled restart policy. Currently, two types of policies are supported, simple policy and complex policy. Simple policy can specify a fixed time of a day to restart the device. Complex policy can specify a certain time of day to restart the device every week. Click the + icon to add multiple time periods.

LED	The LED is enabled by default. You can specify a time period from Monday to Sunday to turn the LED on at a scheduled time. Click the + icon to set multiple time periods.
Panel	On the Panel interface, you can turn on or off the device's WPS button, reset button and power button, and set the power status. **Defaults**: Turn on the WPS button, reset button, and power button, and set the power state to running.

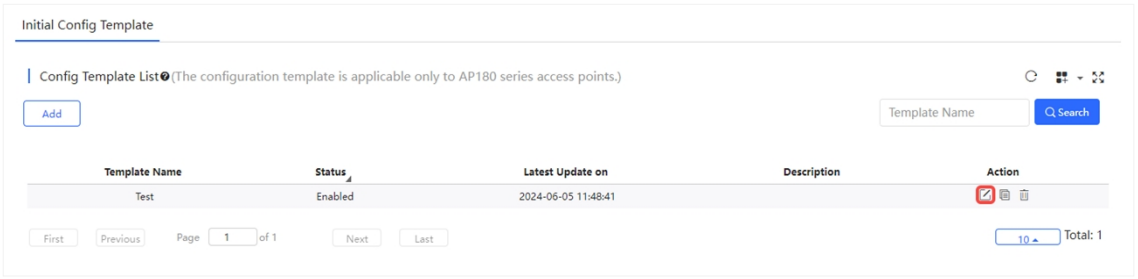
Click the buttons in the **Action** column to edit, copy and delete a template.



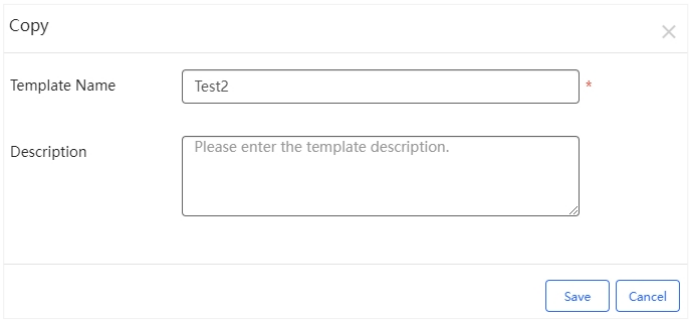
4.1.9.2 Copying an Initial Configuration Template

Follow the steps below to copy an initial configuration template:

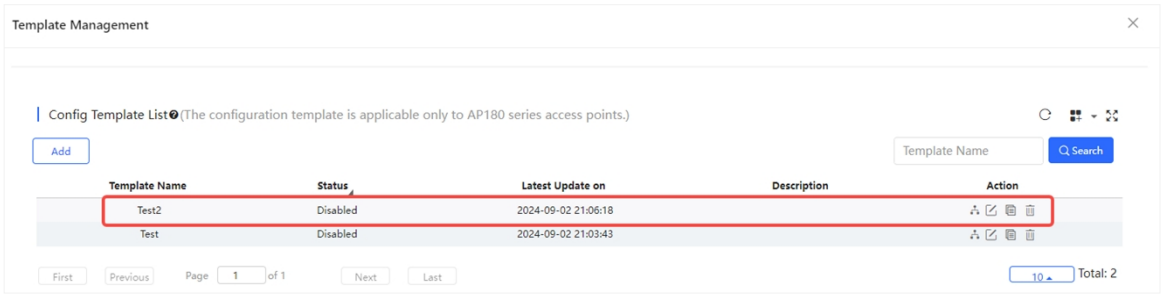
1 Click the button in the **Action** column of the template you want to copy.



2 Enter a new template name (required) and description (optional), then click **Save**.



3 The copied initial configuration template will be displayed in the list. Except for the template name and description, the other configurations of the copied template are the same as the original one.

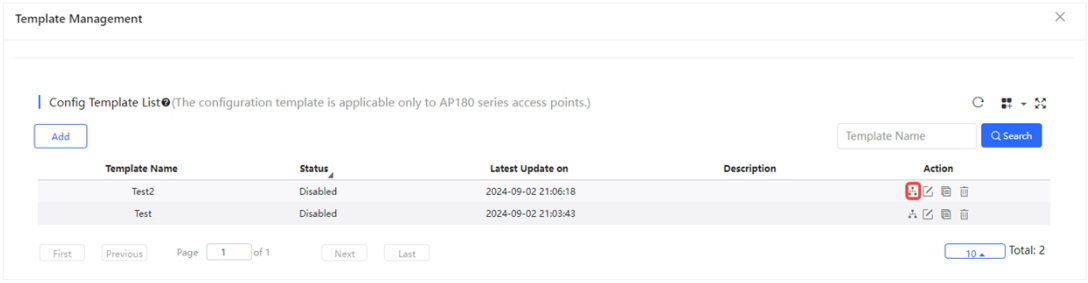


4.1.9.3 Applying an Initial Configuration Template to a Project

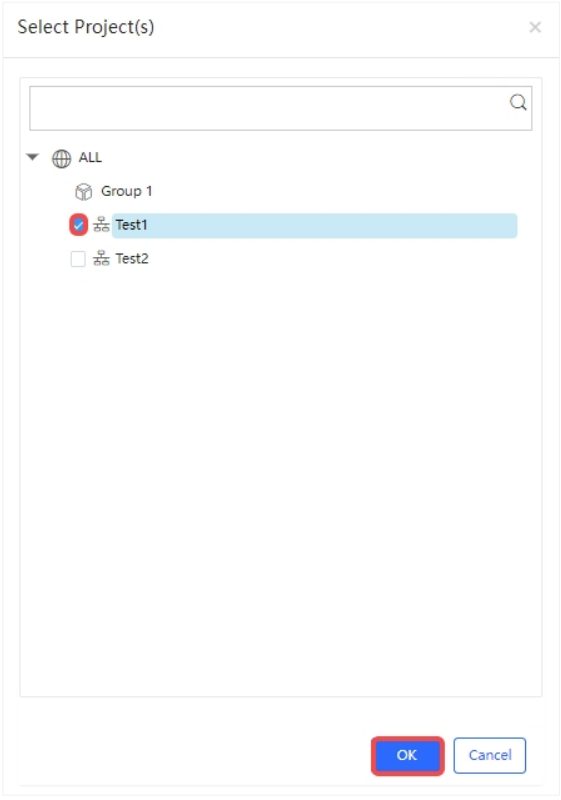
Initial configuration templates can only be used for configuring AP180 series access points now. The RG-MA3511 series devices will be supported in the future. When an initial configuration template is applied to a project, the configuration set in the template will be delivered to all AP180 series access points in this project when they go online for the first time.

Follow the steps below to apply a template to a project:

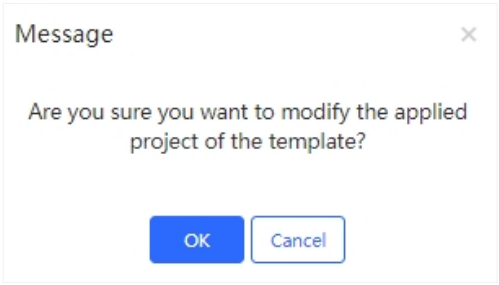
1 Click the in the **Action** column of the template.



2 Select the project and click **Save**.

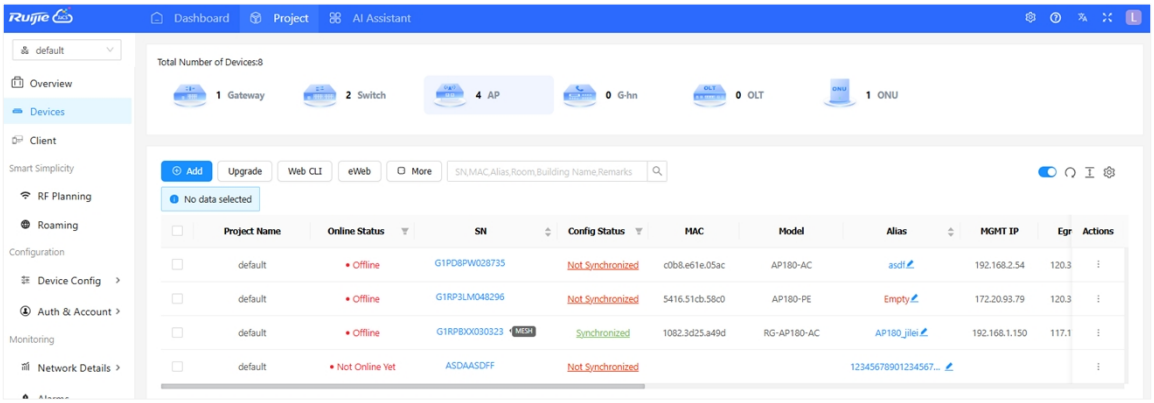


3 When the confirmation prompt box appears, click **OK**.

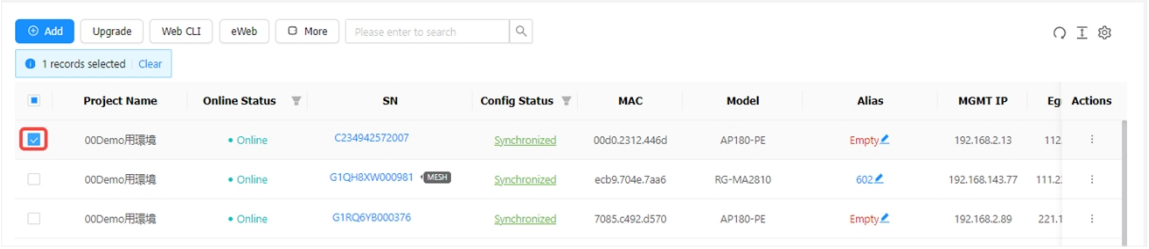


Follow the steps below to apply a template to a specific device:

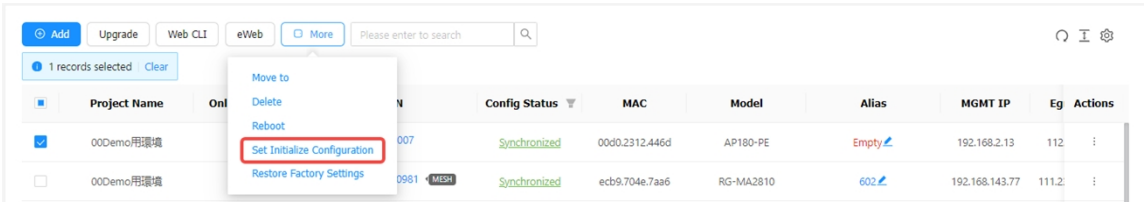
1 Enter the AP management page.



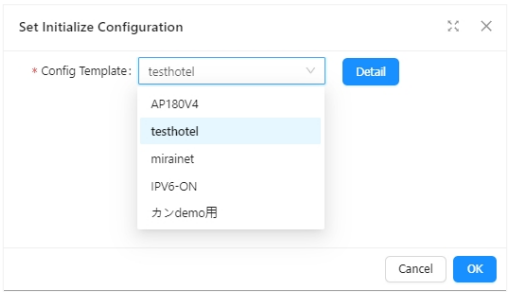
2 Select an AP180 device for which the configuration template should be initialized.



3 Click **More**, and select **Set Initialize Configuration**.



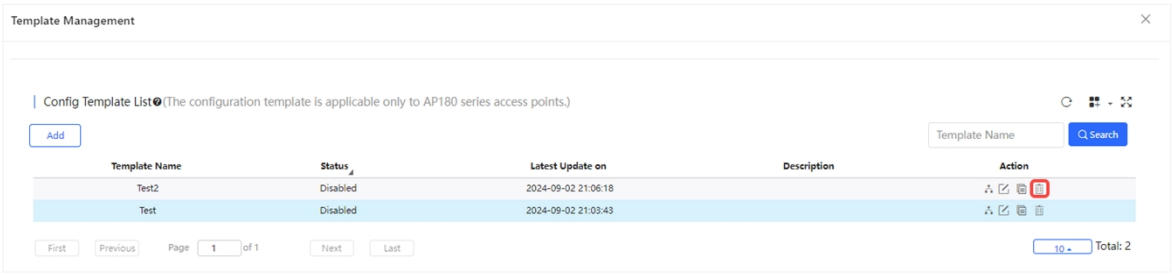
4 Select an initial configuration template, and then click **OK**. To view and modify the initial configuration template information, click **Detail**.



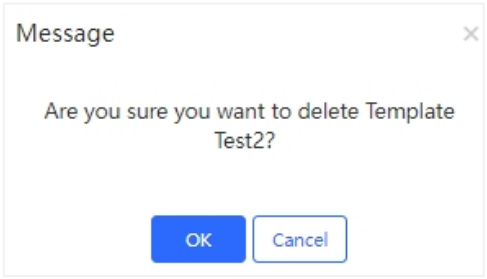
4.1.9.4 Deleting an Initial Configuration Template

Follow the steps below to delete an initial configuration template:

1 Click the icon in the **Action** column of the template to be deleted.



2 When the confirmation box appears, click **OK**.



4.1.10 Device-Specific Configuration Template Management

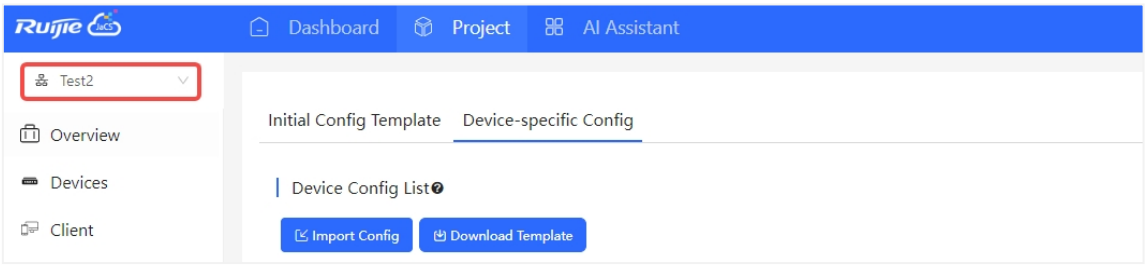
JaCS supports configuring APs in a project via using a device-specific configuration template. The configurable items include IP addresses, gateway addresses, DNS, SSIDs and passwords.

Note

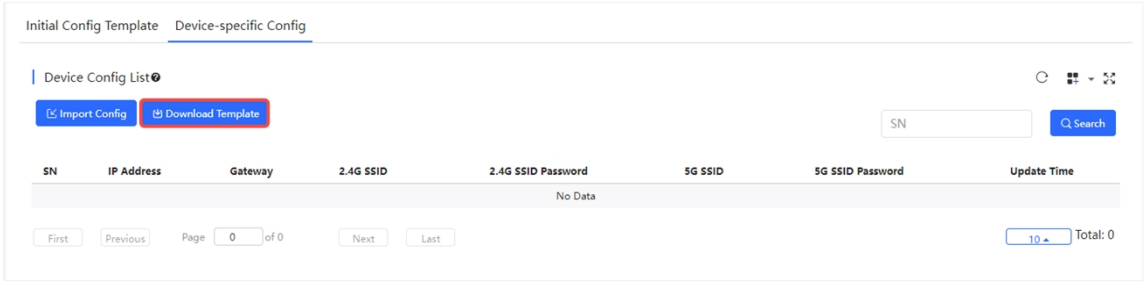
Up to 200 devices can be configured each time.

The specific steps are as follows:

1 Select the project. And navigate to **Device Config** > **AP Template** > **Device-specific Config** to enter the device-specific configuration template management interface.



2 Click **Download Template** to download the device-specific configuration template.



3 Fill in the template.

Items	Description
SN	Required. A SN length ranges from 6 to 32 characters, such as: G1PD7PW00060B.
IP Address	Set the device's IP address and subnet mask. Both the IP address and subnet mask can be left blank. If left blank, the device will obtain the IP address and subnet mask through DHCP.
Subnet Mark	
Gateway	Optional. Set the gateway address. If the IP address is set to a static address, you need to fill in the gateway address.
2.4G SSID	Optional. If the 2.4G SSID is not specified, the original SSID of the device will be kept. The length of a SSID ranges from 4 to 32 characters. The supported characters include letters, numbers, "_", "-", "." and "@". If you want to set multiple different SSIDs, use commas (,) to separate them, for example: SSID-test1, SSID-test2. Up to 3 SSIDs can be

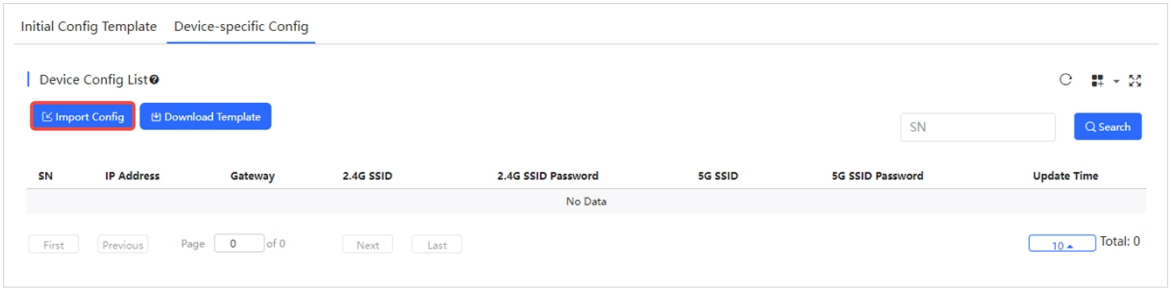
	configured. Note: The SSID is required if the password has been set.
2.4G SSID Password	Optional. If the 2.4G SSID password is left blank in the template, clients can access the SSID without a password. The length of a password ranges from 8 to 32 characters. Letters, numbers, and special characters (@!*#<>=@[)_-) can be contained in a password. If you need to set multiple different passwords, separate them with commas (,), such as “88888888rrrrr, 999999ddddd”. A maximum of 3 passwords can be configured. The SSID and password must correspond to each other in order.
5G SSID	Optional. If the 5G SSID is not specified, the original SSID of the device will be kept. The length of a SSID ranges from 4 to 32 characters. Letters, numbers, and special characters ("_", "-", ".", "@") can be contained. If you want to set multiple different SSIDs, separate them with commas (,) such as “SSID-test1, SSID-test2”. Up to 3 SSIDs can be configured.
5G SSID Password	Optional. If the 5G SSID password is left blank in the template, clients can access the SSID without a password. The password length is 8-32 characters. Letters, numbers, and special characters (@!*#<>=@[)_-) can be contained. If you need to set multiple different passwords, separate them with commas (,), such as “88888888rrrrr, 999999ddddd”. Up to 3 passwords can be configured. The SSID and password must correspond to each other in order.

4 After filling in the information, click **Import Config** to import the template. When importing a template, the system will verify the parameters in the template. The import process will be stopped when one of the following situations occurs:

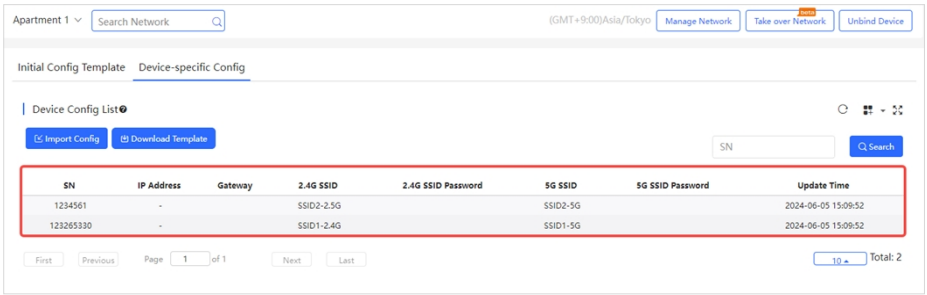
(1) The SN in the template is not available in the current project;

(2) The IP address format is incorrect.

(3) The number of SSIDs and the number of passwords are different.



After importing, the device configuration will be displayed in the **Device Config List**, including the device's SN, the IP address, the 2.4G SSID, the 2.4G SSID password, the 5G SSID, the 5G SSID password, and update time.



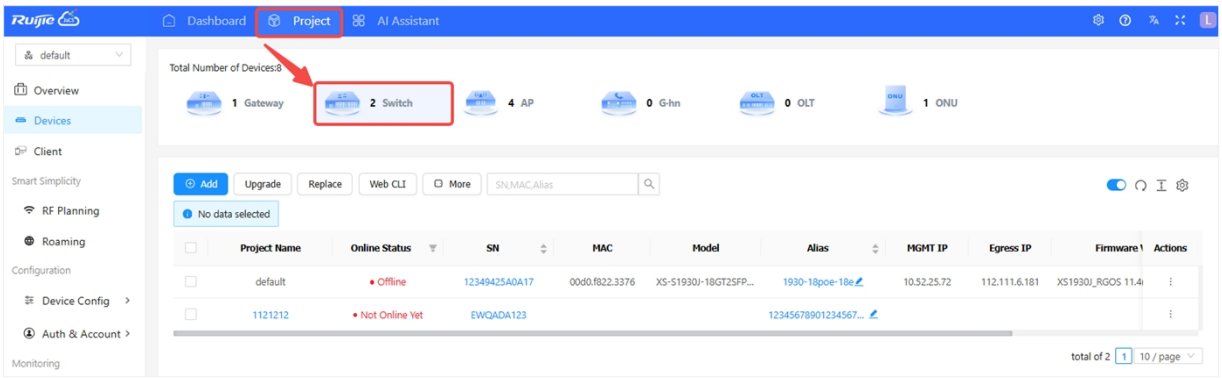
4.2 Switch

This section gives a brief introduction to the switch management interface and operation steps on JaCS, including:

- Switch Management Interface: Introduces the switch management interface of JaCS.
- Adding Switches: Introduces how to add or batch add switches to an existing project.
- Deleting Switches in Batches: Introduces how to delete or batch delete switches from an existing project.
- Moving Switches: Introduces how to move a switch from the project it resides to another project.
- Restarting Switches: Introduces how to remotely restart an online switch device through JaCS.
- Configuration Replacement: Introduces how to synchronize the configuration of an imported switch to a new switch.
- Delivering Configuration via Web CLI: Describes how to use the WEB CLI interface to send configurations to switch devices.

4.2.1 Switch Management Interface

Click **Project** > **Switch** to go to the switch management interface. The switch device list will display the information of all switches in the current project by default.

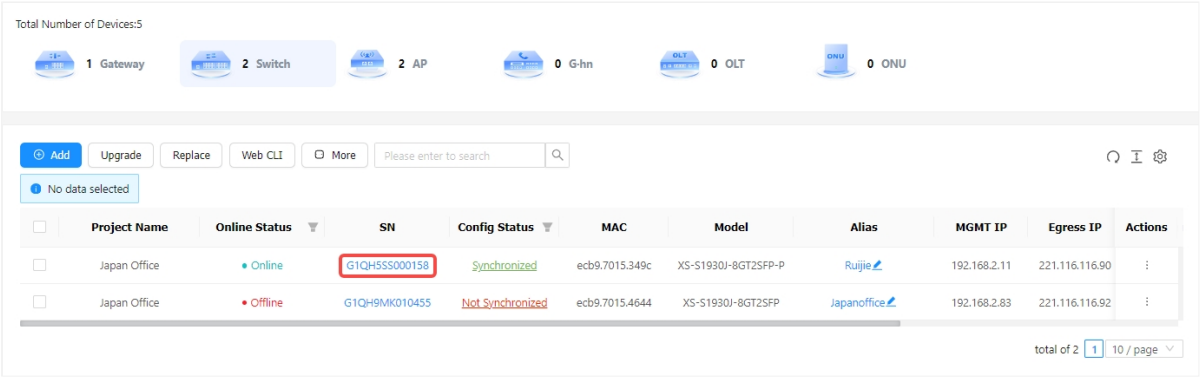


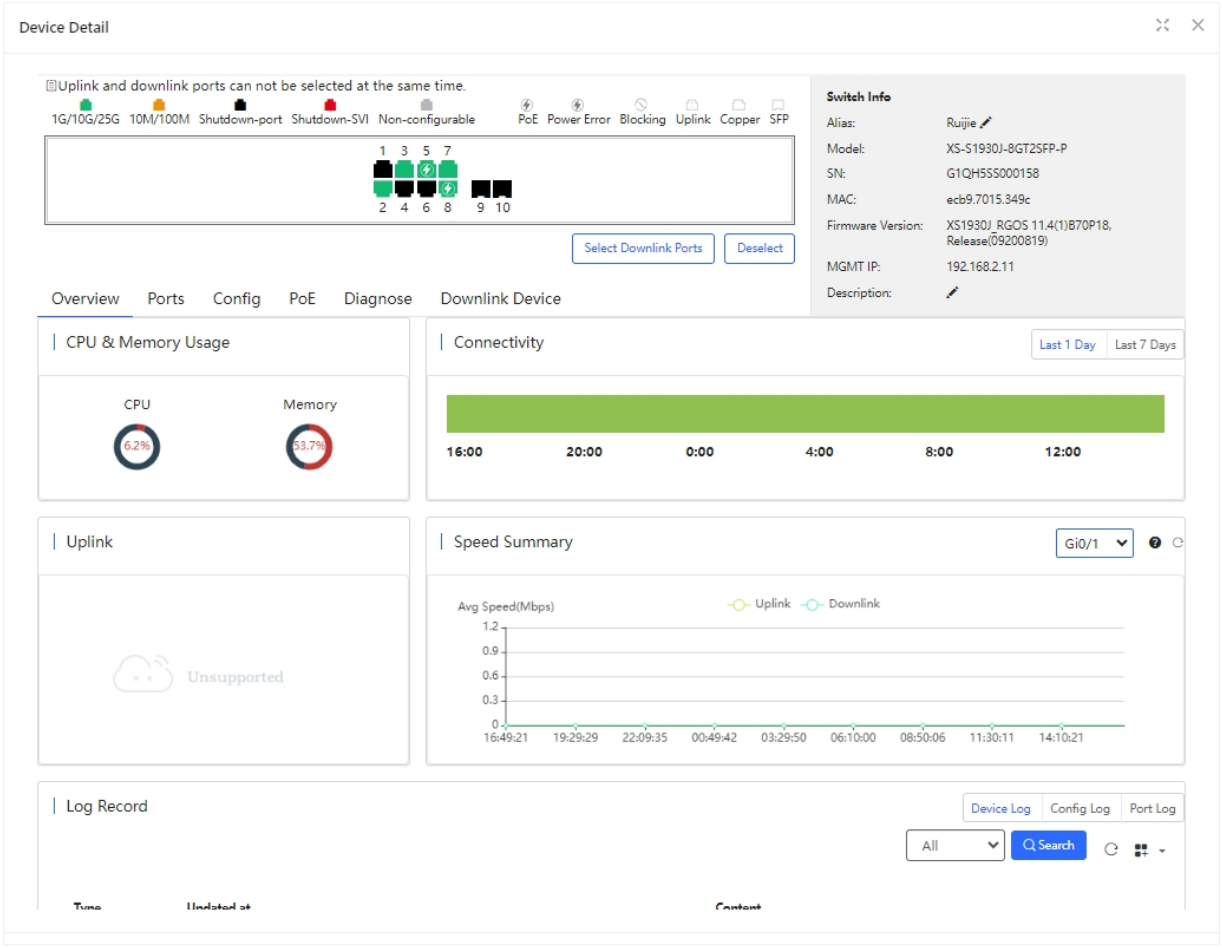
Items	Description
Project Name	Displays the name of the project where the device is located.
Online Status	Displays the online status of the device. The status of the device includes: Online/Offline/Not Online Yet. Click the filter icon to filter devices by online status.
SN	Displays the SN of the device. Click the SN number of a device to view its details.
Configuration Status	Displays the configuration status of the device. Click the filter icon to filter the devices by configuration status.
MAC	Displays MAC information of the device .
Model	Displays device models.
Alias	Displays aliases of devices.
MGMT IP	Displays the management addresses of devices.
Egress IP	Displays egress IP addresses of devices.

Firmware Version	Displays firmware versions of the devices.
Last See On	Displays last online time of devices.
Action	Delete button is available in the **Action** column. Click the delete button to remove the device from the project.

Buttons	Description
Add	Add button. Click this button to enter the device adding interface.
Upgrade	Upgrade button.
Replace	Configuration replacement button. You can synchronize the configuration of an old device to a new one of the same model. After configuration replacement task is created, the configuration of the old device will be sent to the new one when it is online.
Web CLI	Web CLI button. Select the device and click this button to send configuration to the device through Web CLI.
More	Click this button to display more operation buttons, including: Move, Delete, and Restart.
	Automatic refresh button. The automatic refresh button is enabled by default. When it is enabled, the switch device list will automatically refresh once every minute.
	Manual refresh button. Click this button to manually refresh the switch list.
	Row height adjustment button. Click this button to adjust the row height.
	Click this button to customize the displayed items in the switch list.
SN,MAC,Alias	Search box. Supports searching switches by SN, MAC, or alias.

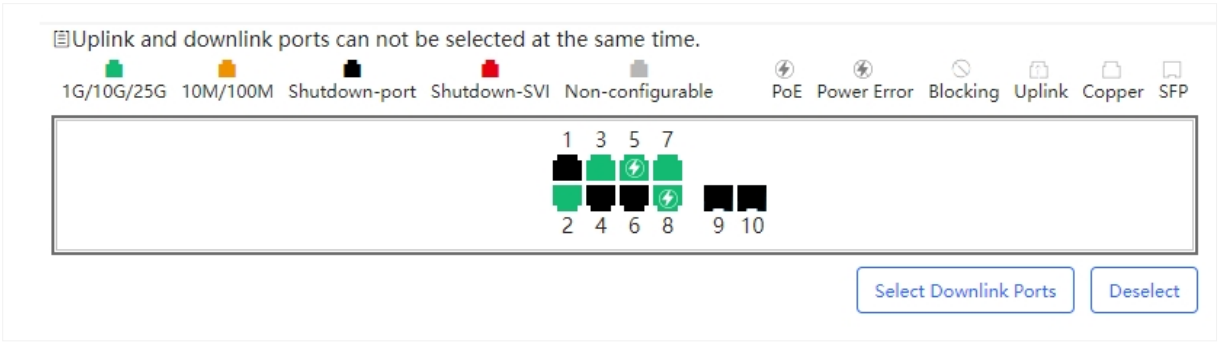
Click the **SN** of a switch in the switch list to check its detailed information. The detailed interface consists of port panel, basic information, device overview, device port, configuration, PoE, diagnosis and downstream devices.

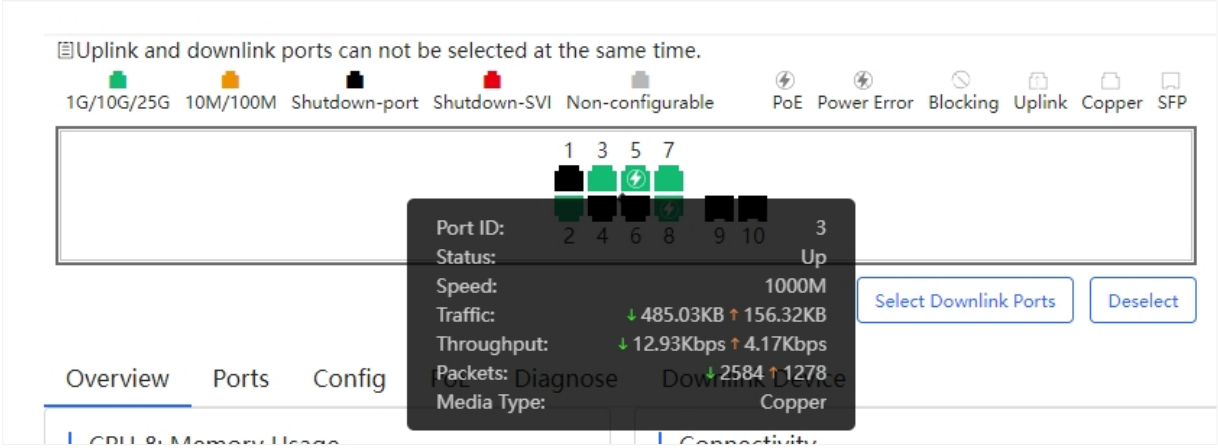




(1) Port Panel

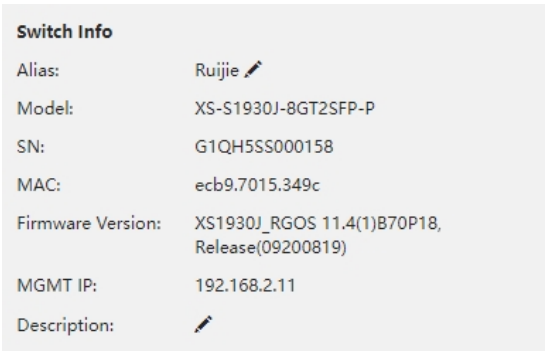
The port panel displays the port type, status and speed. When you hover the mouse over a port, you can view its port ID, traffic, rate, type and other information of the port.



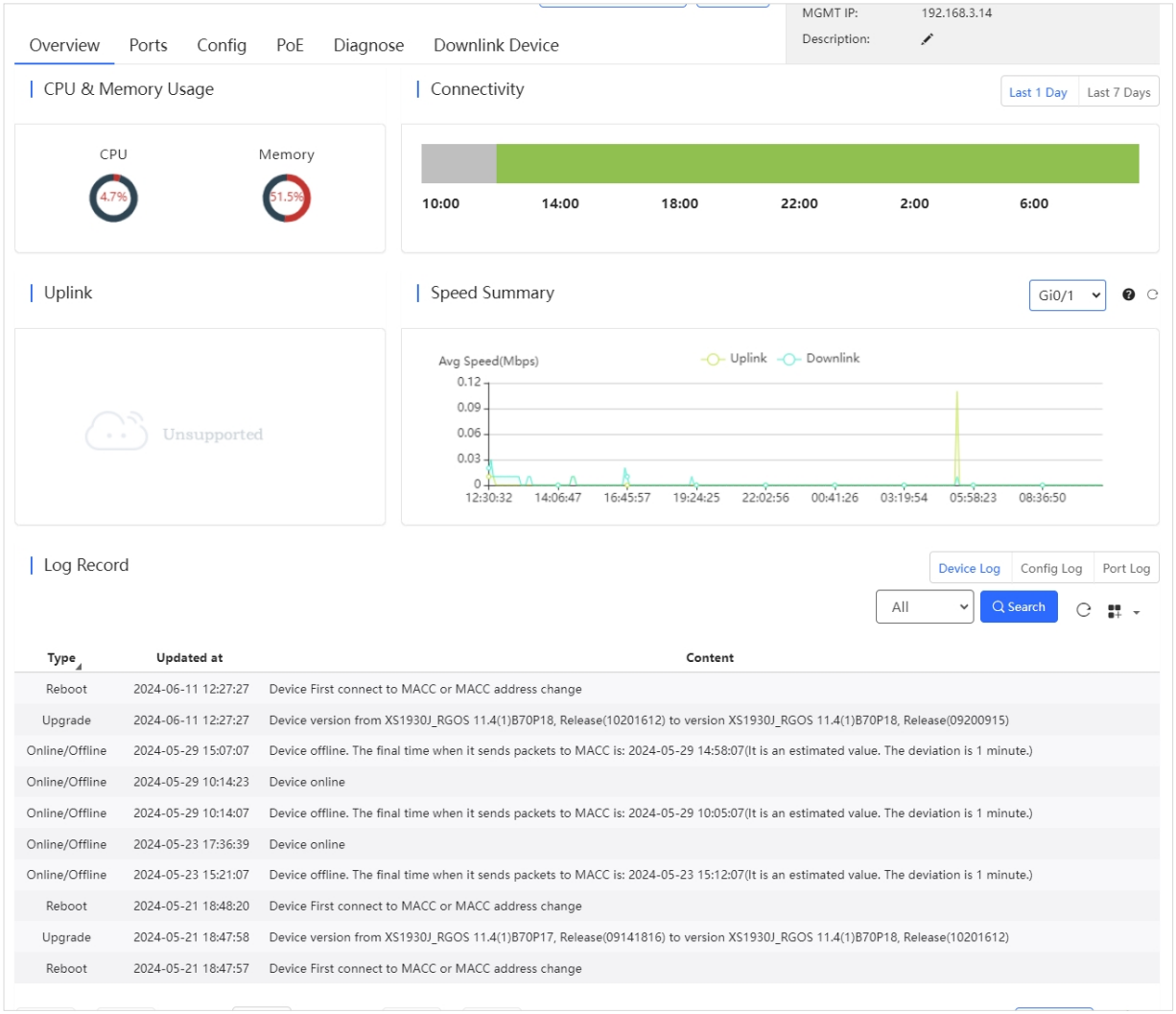


(2) Switch Information

The switch information table displays alias, model, SN, MAC address, firmware version, management IP and description. You can click the edit icon to modify the alias and description of the switch.

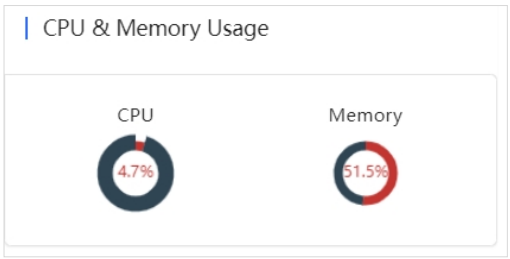


(3) Overview Tab



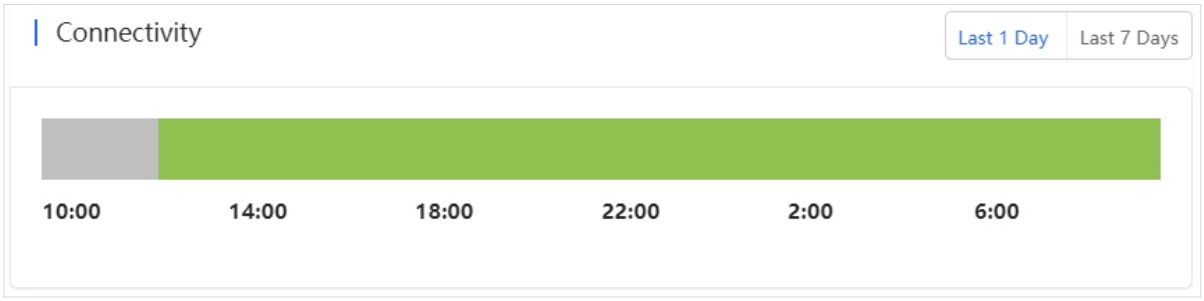
- CPU & Memory Usage

Displays the CPU and memory usages of the switch.



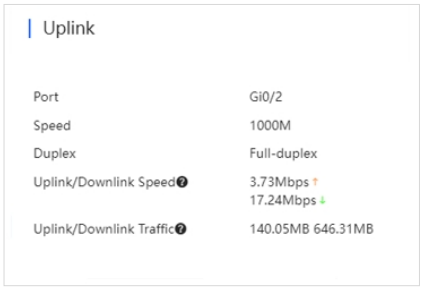
- Connection

Displays the connection status between the switch and the Cloud in the last 1 day or 7 days.



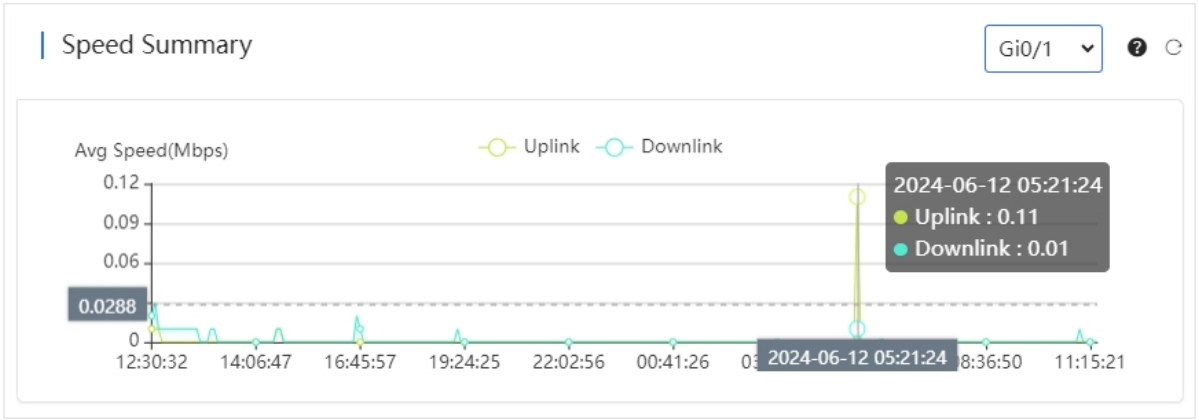
- Uplink

Display uplink information, including port, speed, duplex, uplink/downlink speed, and uplink/downlink traffic.



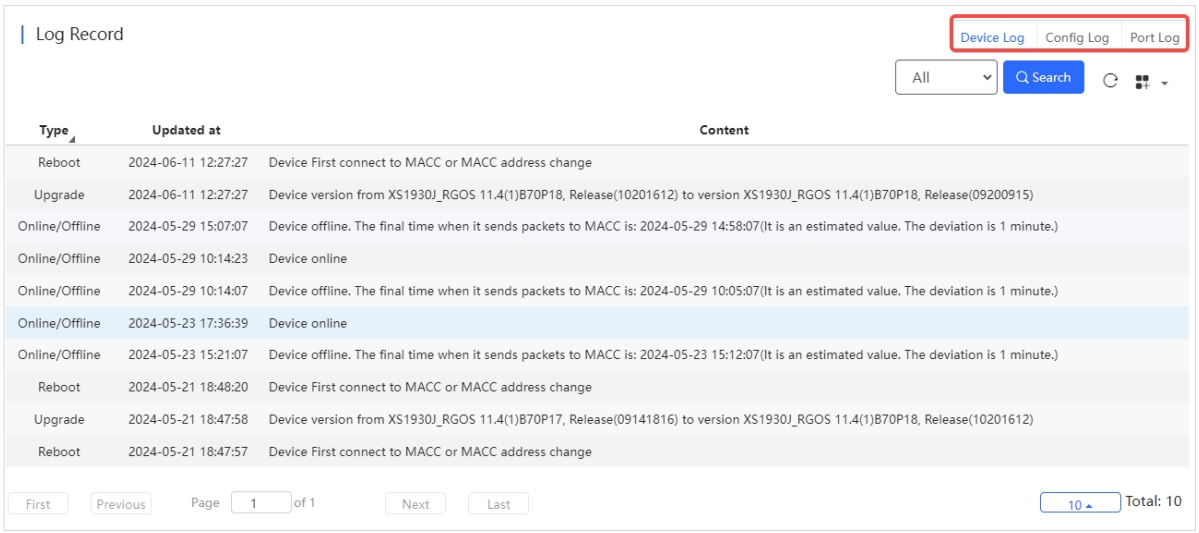
- Speed Summary

Displays the device's uplink and downlink rates in the last 24 hours. Hover the mouse over a time in the chart to view the device's uplink and downlink rates at that time.



- Log Record

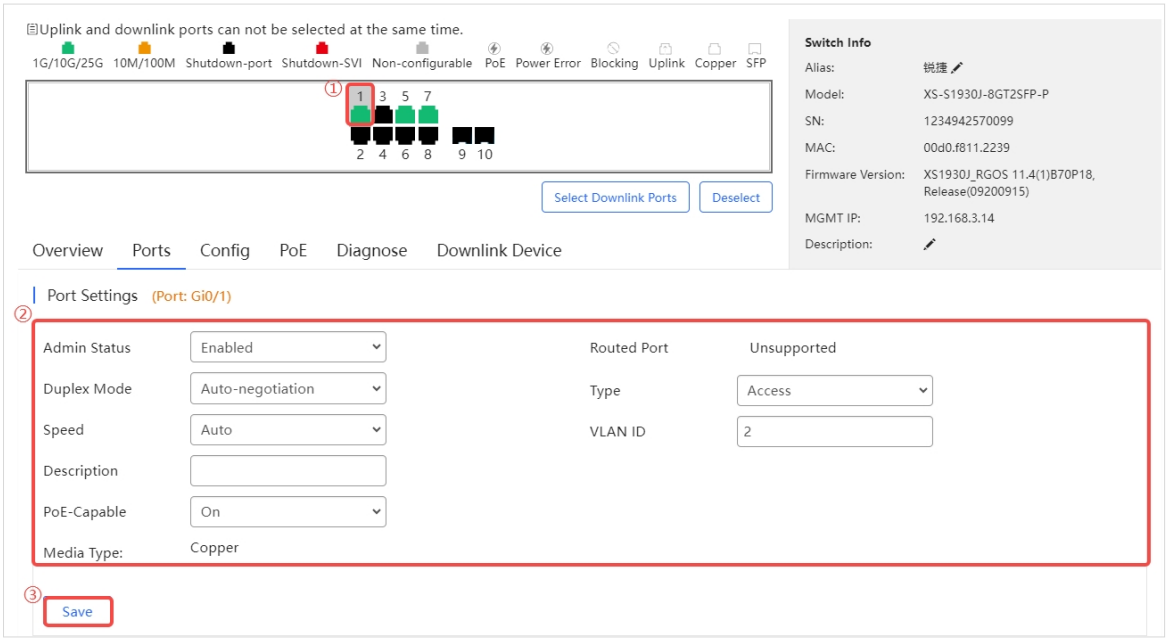
Support viewing three types of device logs, including device logs, configuration logs, and port logs. Logs can be filtered based on log types and time.



(4) Ports Tab

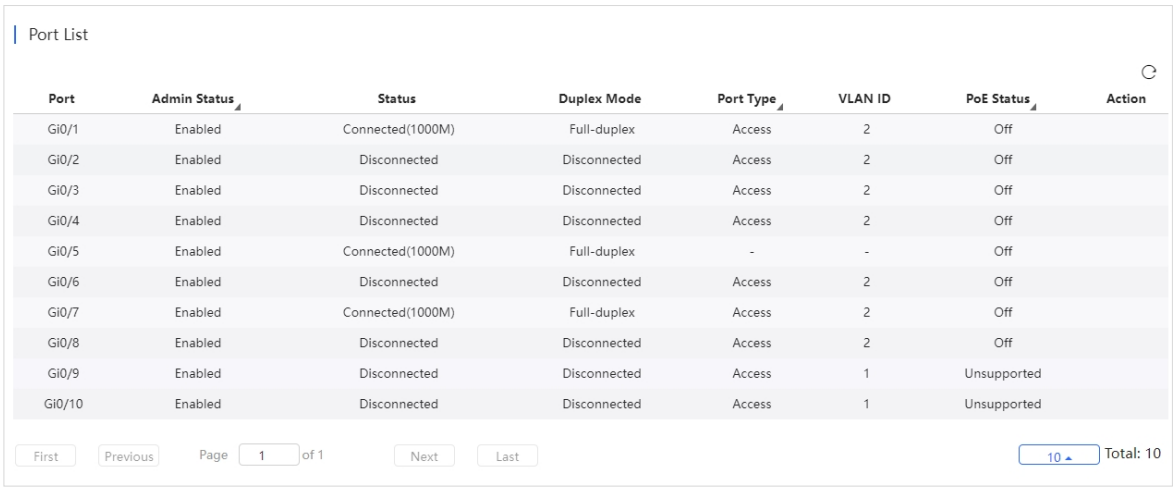
- Port Settings

  Support setting the port's admin status, duplex mode, speed, description, PoE, port type, and VLAN ID. After completing the settings, click **Save**.



- Port List

  The port list displays the information of all ports of the device, including port ID, management status, port status, duplex mode, port type, VLAN ID and PoE status. Click the icon of the **Admin Status**, **Port Type** and **PoE Status** to filter the port information.



(5) Configuration Tab

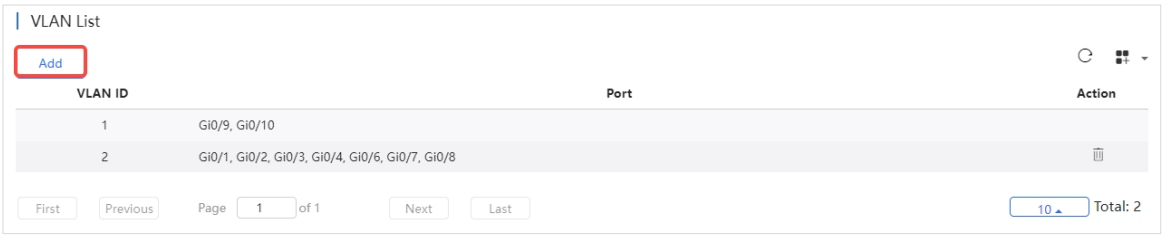
The Configuration tab consists of seven parts, including VLAN List, SVI&DHCP, DHCP Snooping, RLDP, Device Config, Service List and Configuration Backup List.

- **VLAN List**

VLAN List displays the current VLAN ID and the corresponding port number. Click **Add** to add a VLAN ID.

The specific steps are as follows:

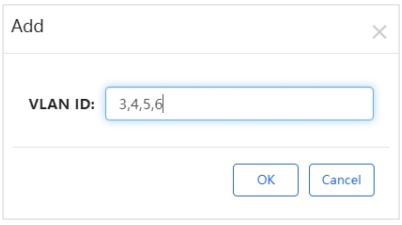
1 Click **Add**.



2 Enter the VLAN ID.

Two methods are provided for you to add multiple VLAN IDs:

Method 1: Use commas (,) to separate VLAN IDs. Up to 10 VLAN IDs can be created at one time.

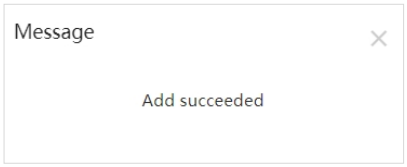


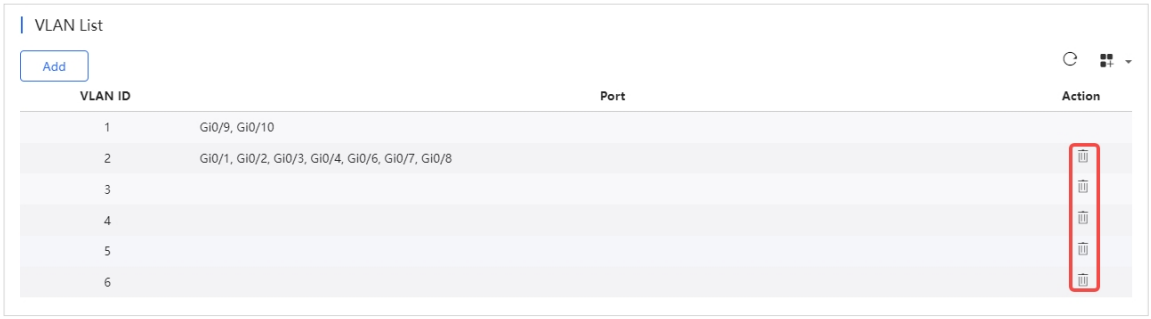
Method 2: Use dashes (-) to separate VLAN IDs. This method can be used to create VLANs in batches without any quantity limit, as long as the VLAN range is within 1-4094.

Note

Commas and dashes cannot be used together.

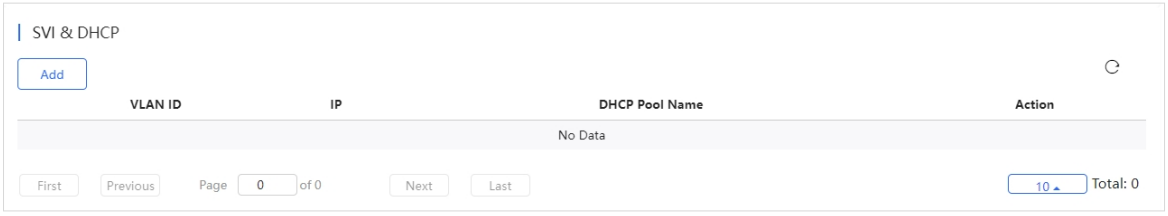
3 After setting the VLAN IDs, click **OK**. When the "Added succeeded" prompt appears, the operation is completed. The created VLAN ID will be displayed in the VLAN list. To delete a VLAN ID, click the delete icon in the **Action** column.



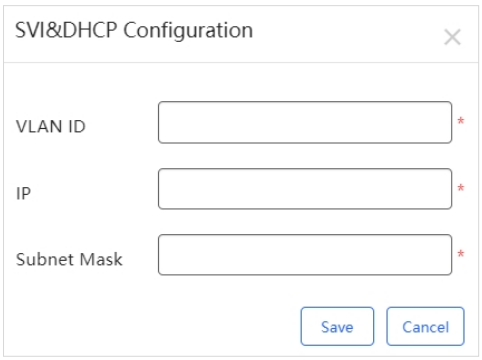


- **SVI & DHCP**

SVI & DHCP list displays the VLAN ID, SVI, and DHCP pool name.



Click **Add**, and configure the VLAN ID, IP and subnet mask, and then click **Save**.

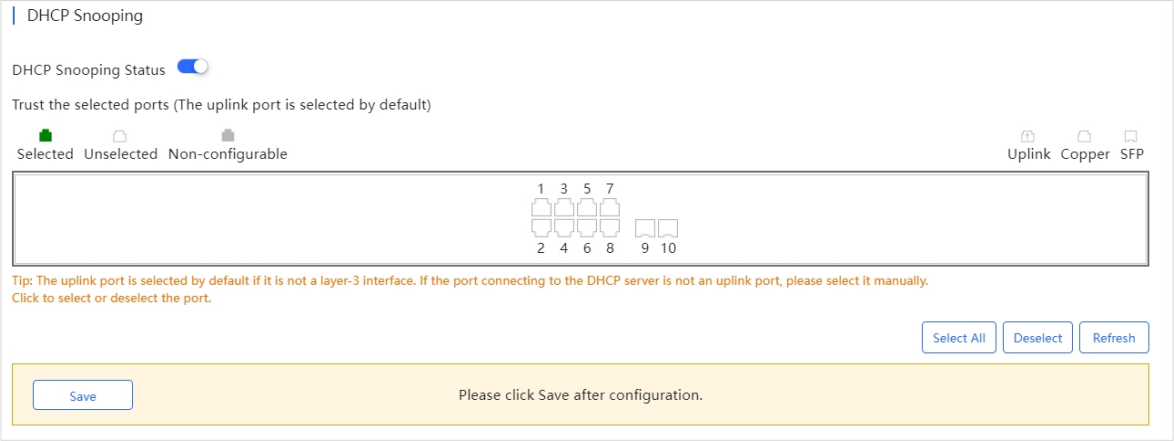


Note

VLAN ID range is 1-4094.

- **DHCP Snooping**

DHCP Snooping is disabled by default. After enabling it, select a port and click **Save**. If the selected port is not a routing port, the uplink port is selected by default. If the port connected to the DHCP server is not an uplink port, you need to select it manually.

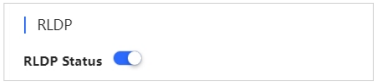


- **R LDP Status**

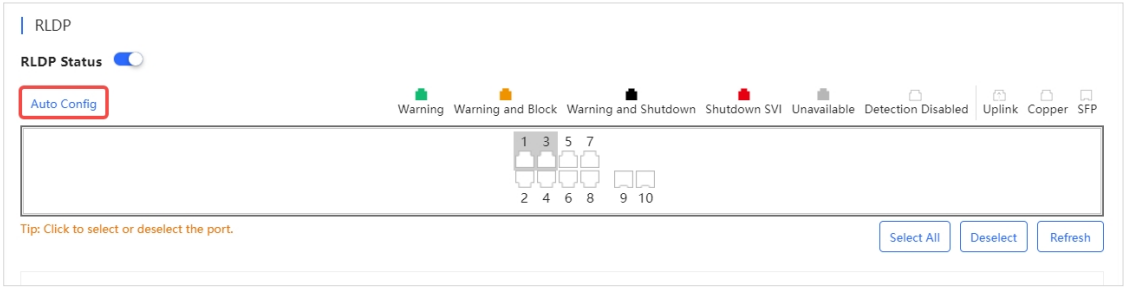
Rapid Link Detection Protocol (RLDP) is a link protocol used to quickly detect Ethernet link faults. After it is enabled, if a fault is detected, it will handle the fault according to the rule set on the device, including generating alarm, port shutdown, disabling the SVI where the port is located, etc. The RLDP is disabled by default. It supports automatic configuration and custom configuration.

Automatic Configuration:

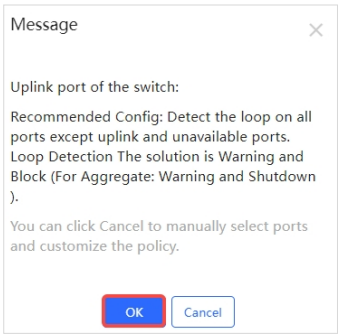
1 Enable RLDP status.



2 Click **Auto Config** to use the system default configuration, that is, to perform loop detection on all ports except uplink ports and unavailable ports, and set the loop fault handling mode to **Block** and **Alarm**. For loops on aggregate ports, the fault handling mode is **Alarm** and **Close**.

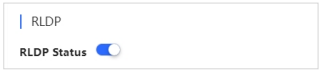


3 Click **OK** in the confirmation box to complete the operation.

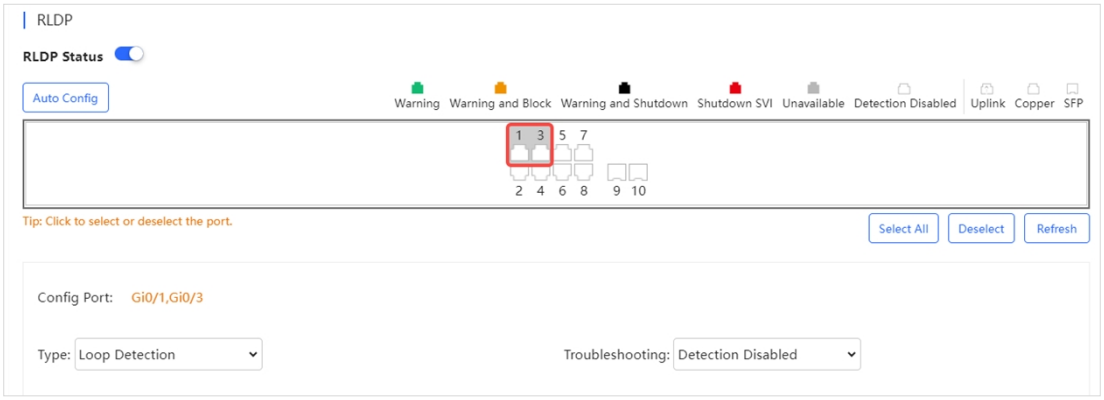


Custom Configuration:

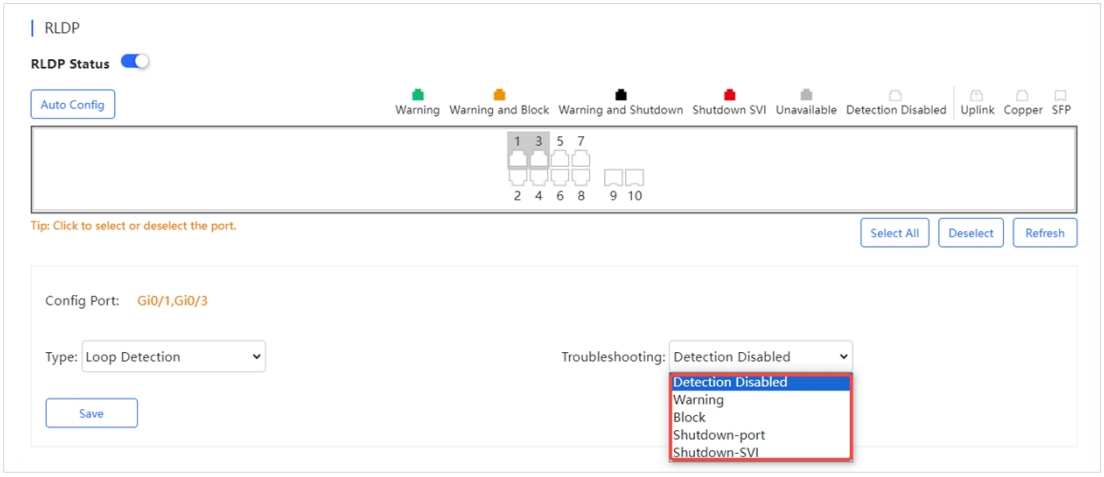
1 Enable RLDP Status.



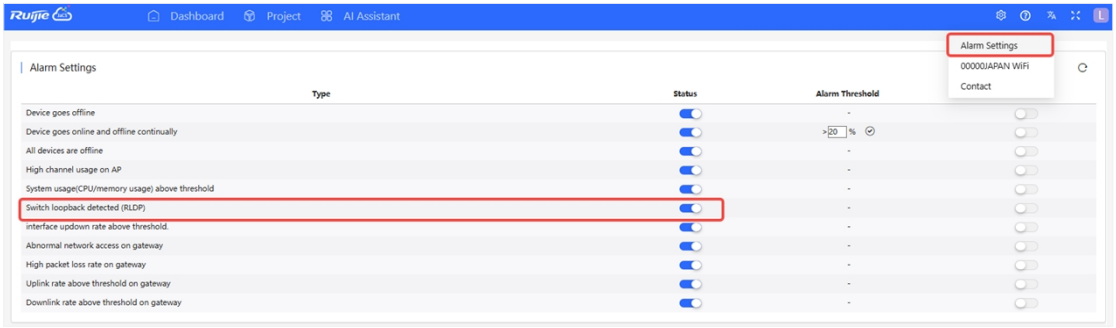
2 Select the port(s) to be detected. If you want to select all ports, click **Select All**. To cancel the selection, click **Deselect**.



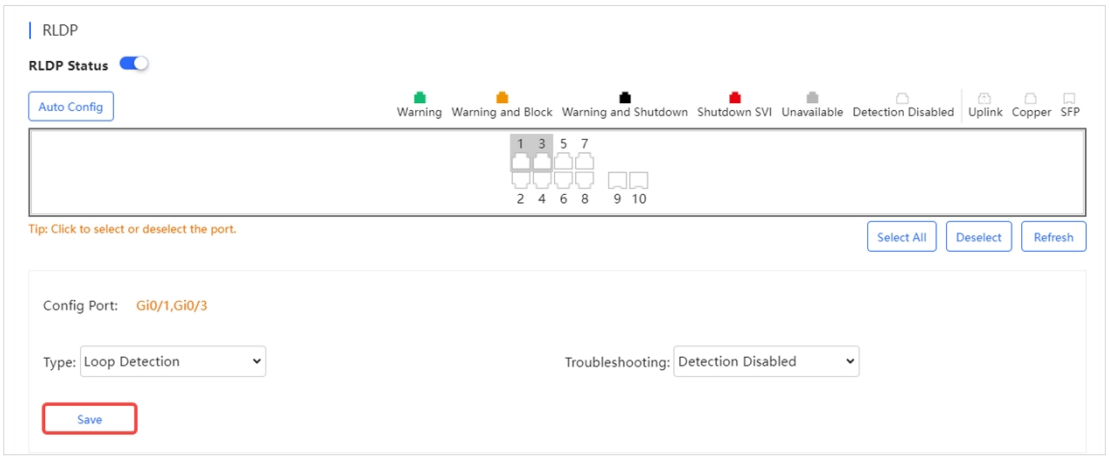
3 Select a troubleshooting method. Five troubleshooting methods are provided: **Detection Disabled**, **Warning**, **Block**, **Shutdown-port**, and **Shutdown-SVI**.



Before setting the troubleshooting method to **Warming**, make sure that the RLDP alarm has been enabled in the **Alarm Settings** interface.



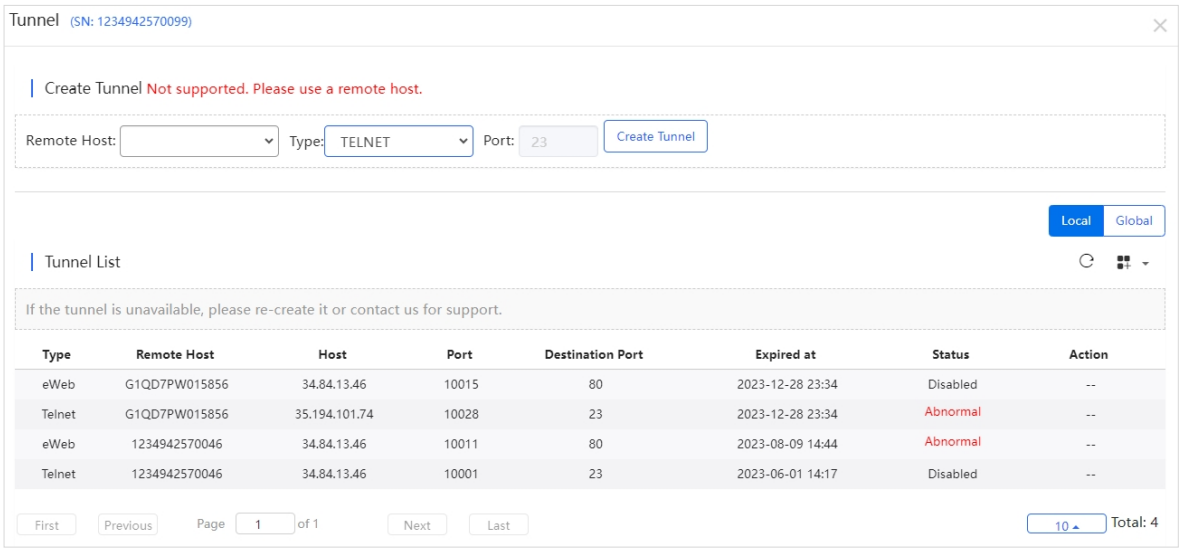
4 After selecting the port(s) and configuring the troubleshooting method, click **Save**. When the "Save Succeeded" prompt appears, the operation is completed.



- **Device Configuration**

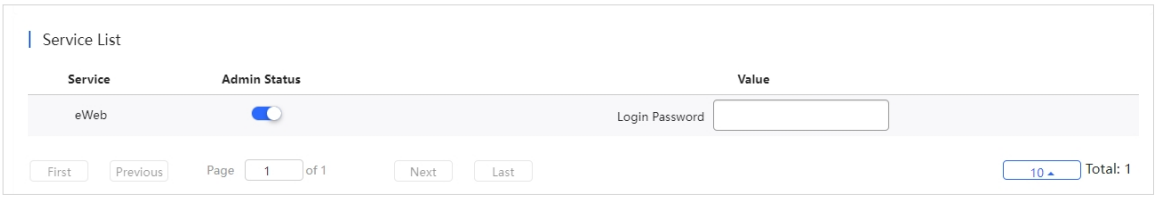
  In the **Device Configuration** interface, you can create a tunnel.

  Click **Tunnel** to enter the tunnel creation interface. Fill in the destination address of the tunnel, select the tunnel type and port, and then click **Create Tunnel**.



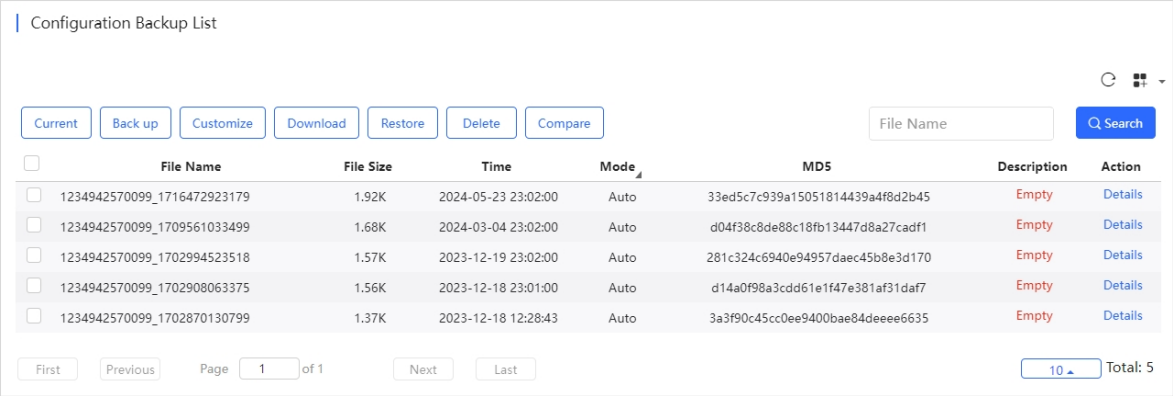
- **Service List**

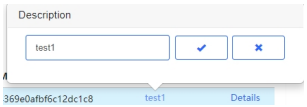
  Supports configuring account status and login password of the device's eWeb. The password length is 8-31 characters.



- **Configuration Backup List**

  Supports backing up configuration. The information displayed in the backup list includes configuration file name, file size, time, mode, MD5 and description.

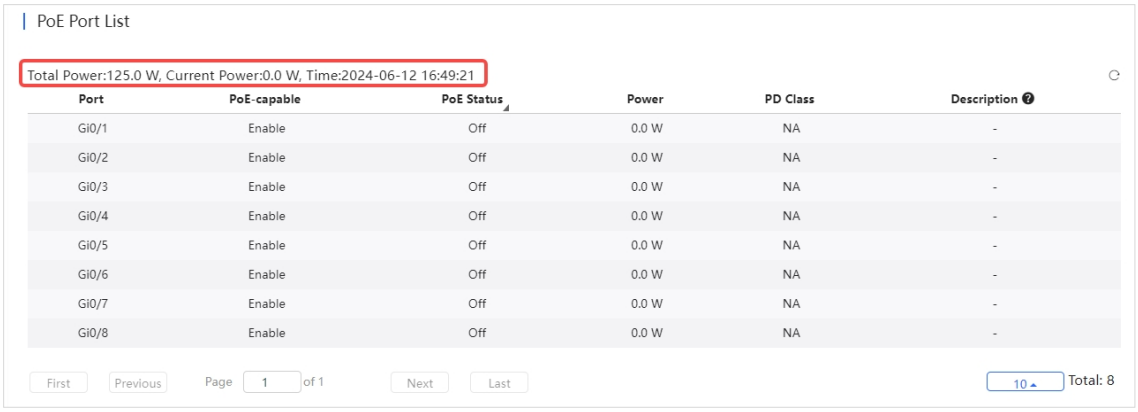


Buttons	Description
Current	Click this button to display the current configuration of the device. If you want to back up the configuration, click **Backup** in the **Config Details** interface. After backup, click ↻ to refresh the list, and the backed up file will be displayed in the list.
Back up	Click this button to back up the current configuration of the device. When the operation confirmation box appears, click **OK**. After backup, click ↻ to refresh the list, and the backed up file will be displayed in the list.
Customize	Configuration file customization button. Select one of the files in the **Configuration Backup List**, and then click this button to modify the configuration. After setting the file name and changing the configuration, click **Save** to complete the operation.
Download	Configuration file download button. Select a configuration file in the **Configuration Backup List**, and click **Download** to download the configuration file. When the operation confirmation box appears, click **OK**. Only one configuration file can be downloaded at a time.
Restore	Backup file restore button. Check a configuration file and click **Restore** to restore the current configuration file of the device to the selected configuration file. Only one file can be restored at a time.
Delete	Delete button. Select a configuration file to be deleted, click **Delete**, and when the operation confirmation box appears, click **OK** to delete the configuration file.
Compare	Comparison button. Select two configuration files to be compared and click **Compare** to compare the two profiles to find out their differences.
Details	Click this button in the **Action** column to view the detailed configuration of a file.
Description	Click the words in the **Description** column to modify the profile description. 

(6) PoE

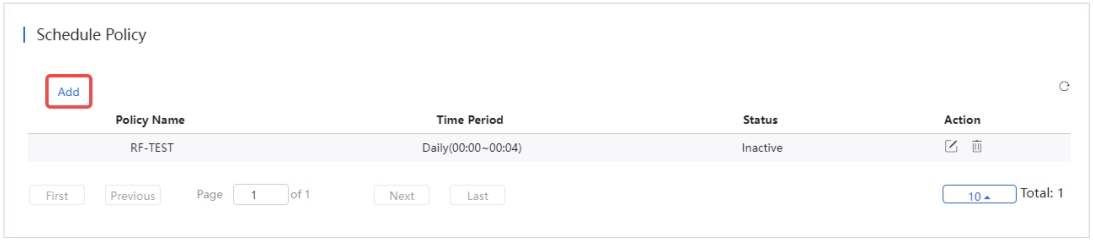
- **PoE Settings**

The PoE statistics are displayed above the PoE list, including total power, current power, and time.

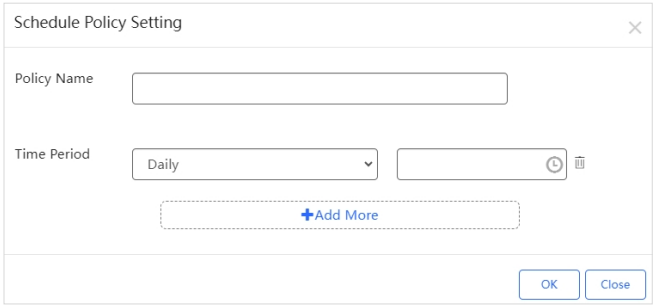


To shut down the PoE port at a specific time:

1 Click **Add**.

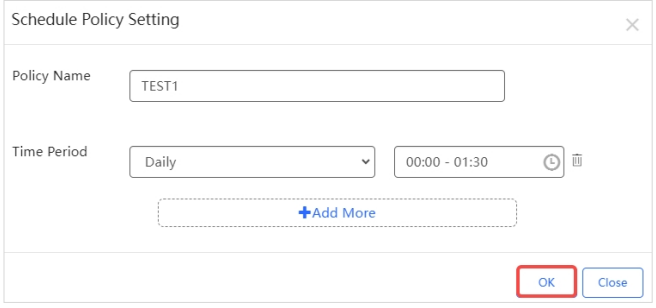


2 Set the policy name and specify the time period.



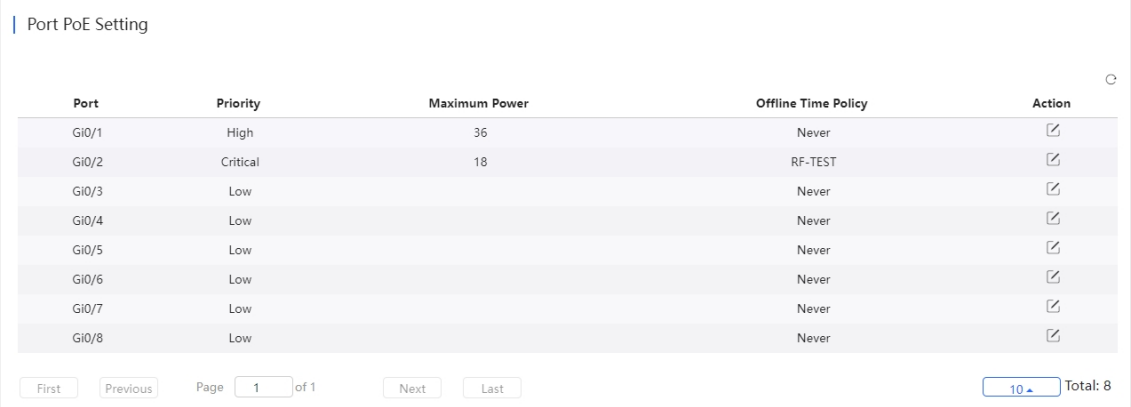
Items	Description
Policy Name	Required. Set the policy name.
Time Period	Required. Set the time period.
Add More	Click **+ Add More** to set multiple time periods.

3 Click **OK**.



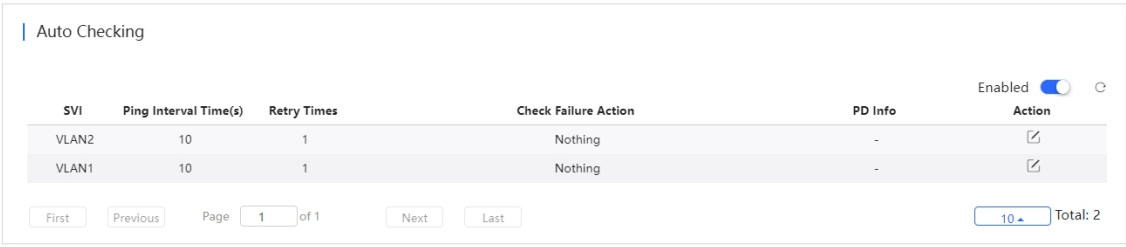
- **PoE Settings**

  Click in the **Action** column to modify the priority, maximum power, and power supply stop policy.



- **Auto Checking**

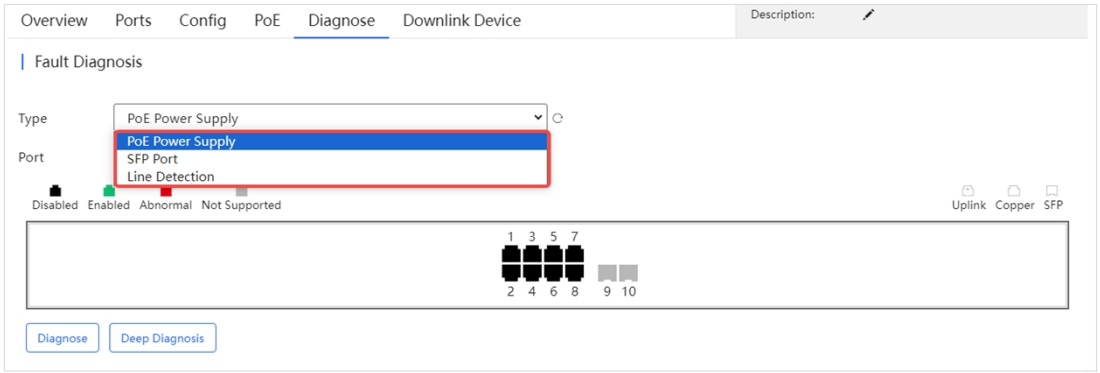
  After the PoE self-check function is enabled, the system will automatically detect the configured ports. When the PD device is detected to be offline, a trap notification is sent by default; if the reboot-remote-pd option is configured, it will automatically restart the PD device.



(7) Diagnose

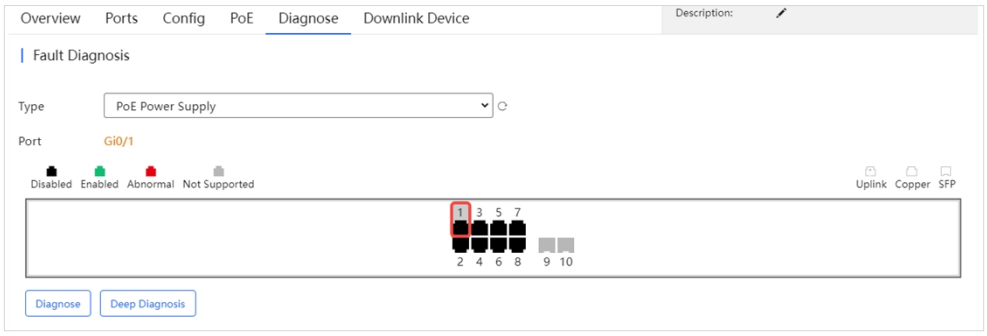
Supports port fault detection. The specific steps are as follows:

1 Select the type.

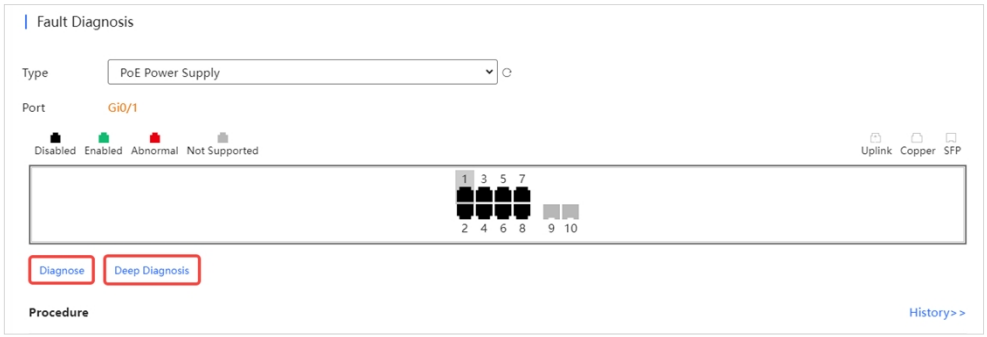


Items	Description
PoE Power Supply	Used to detect whether the PoE power supply is normal.
SFP Port	Used to detect whether the SFP port is normal.
Line Detection	Used to detect whether the line detection is normal.

2 Select the port to be diagnosed on the panel.

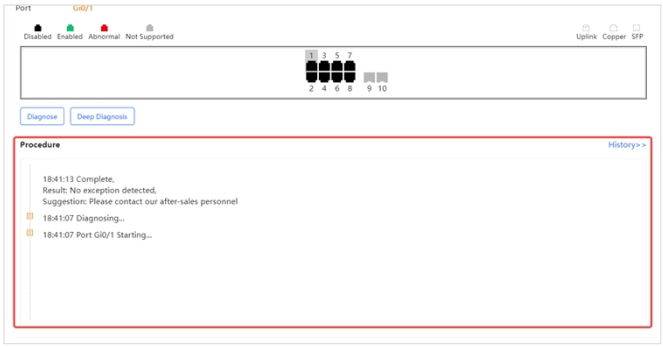


3 Select the diagnosis type: normal diagnosis or deep diagnosis.

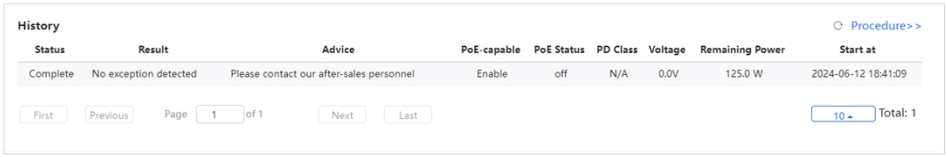


Items	Description
Diagnose	The cloud server sends CLI commands to collect switch information, and the diagnosis is performed on the cloud server.
Deep Diagnose	Diagnostics are performed on the switch and the results are reported to the cloud server.

4 Waiting for the diagnosis result.

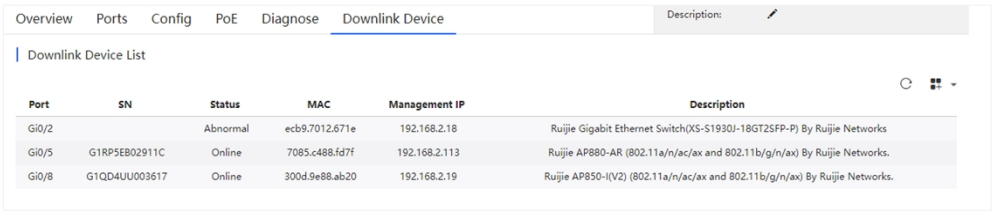


Click History>> to display the historical records.



(8) Downlink Device

Display the downlink device information of the switch.



4.2.2 Adding Switches

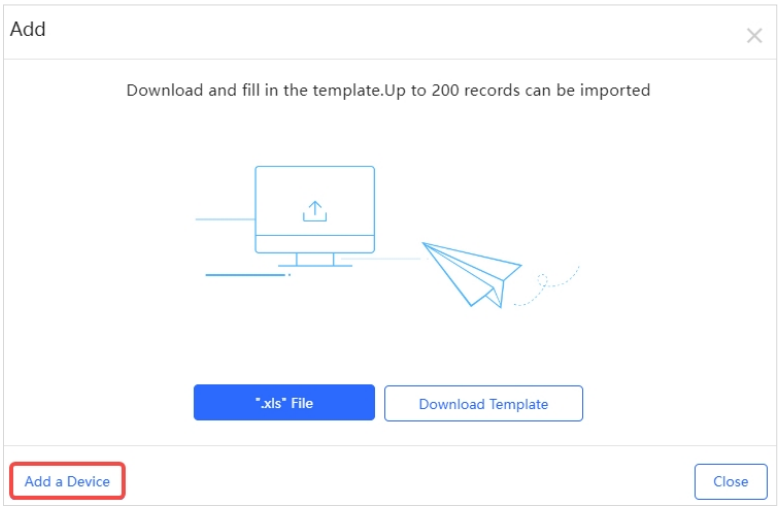
JaCS provides two ways to add APs to a specific project.

- Adding a Switch
- Adding Switches in Batches

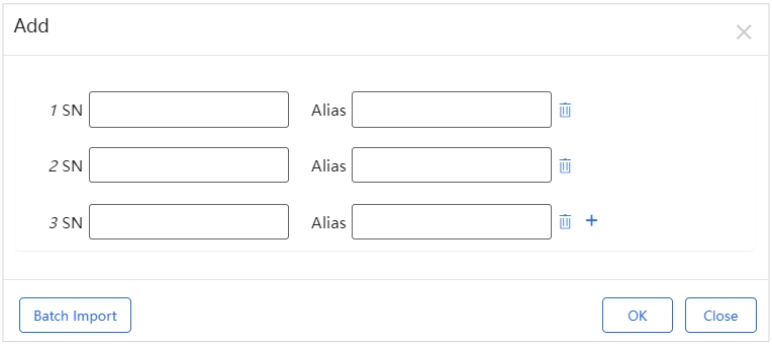
4.2.2.1 Adding a Switch

If there are only a few devices that needs to be imported, you can refer to the following steps to quickly add them to an existing project:

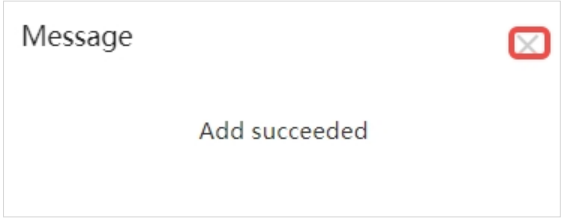
1 Click **Add a Device**.



2 Enter the device's SN (required) and alias (optional). The length of the SN ranges from 6 to 20 characters, and the length of an alias cannot exceed 64 characters. To add more SNs, click **+**; to delete a SN, click .



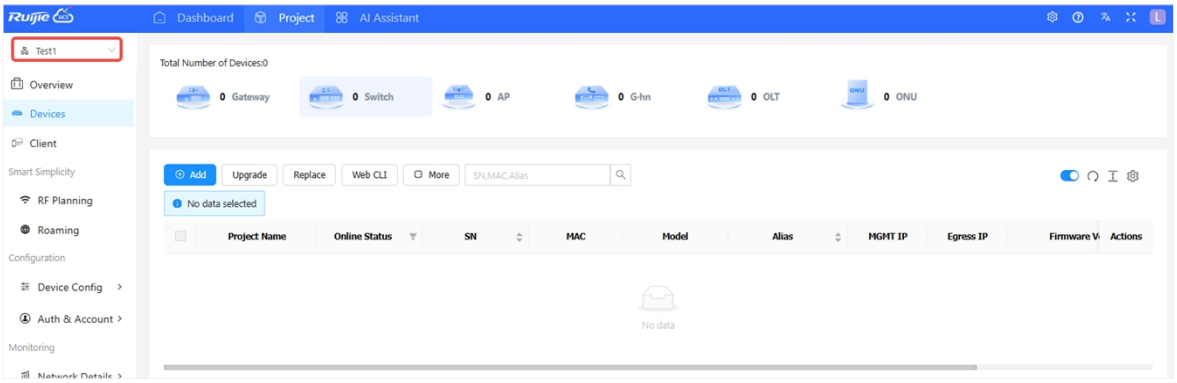
3 After filling in the information, click **OK**. When the "Add succeeded" prompt appears, click **X** to close the prompt box and complete the operation. The added device will be displayed in the switch list.



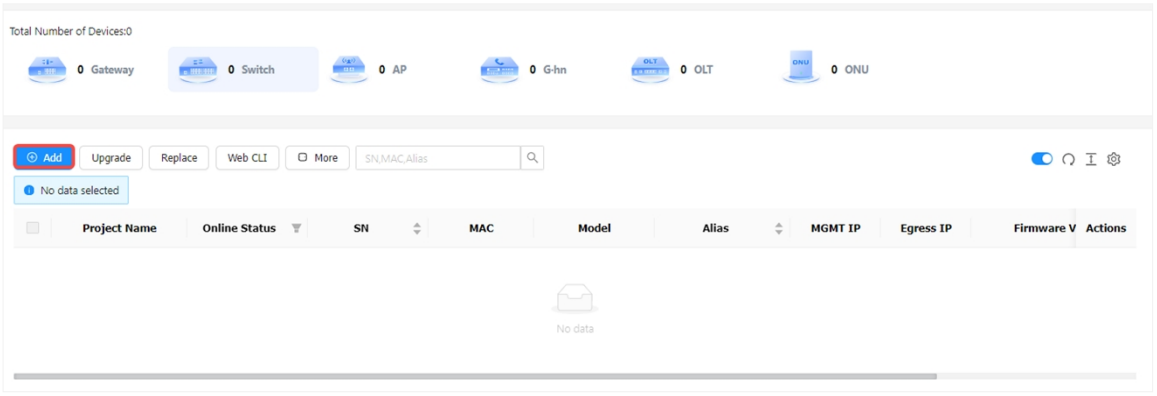
4.2.2.2 Adding Switches in Batches

JaCS supports adding switches in batches, which is suitable for scenarios where no more than 200 devices need to be added at a time. The specific steps are as follows:

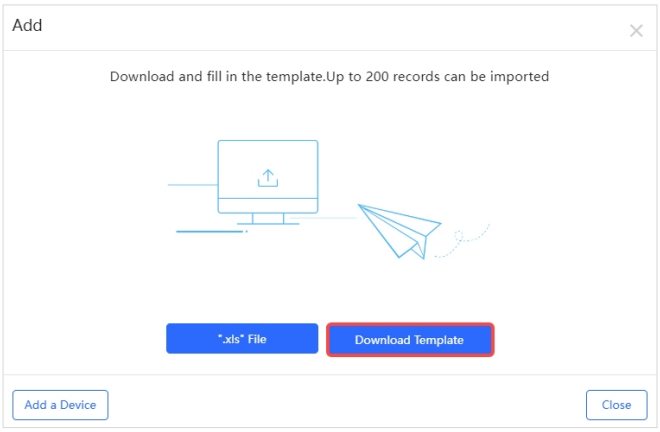
1 Select the project.



2 Click **Add**.



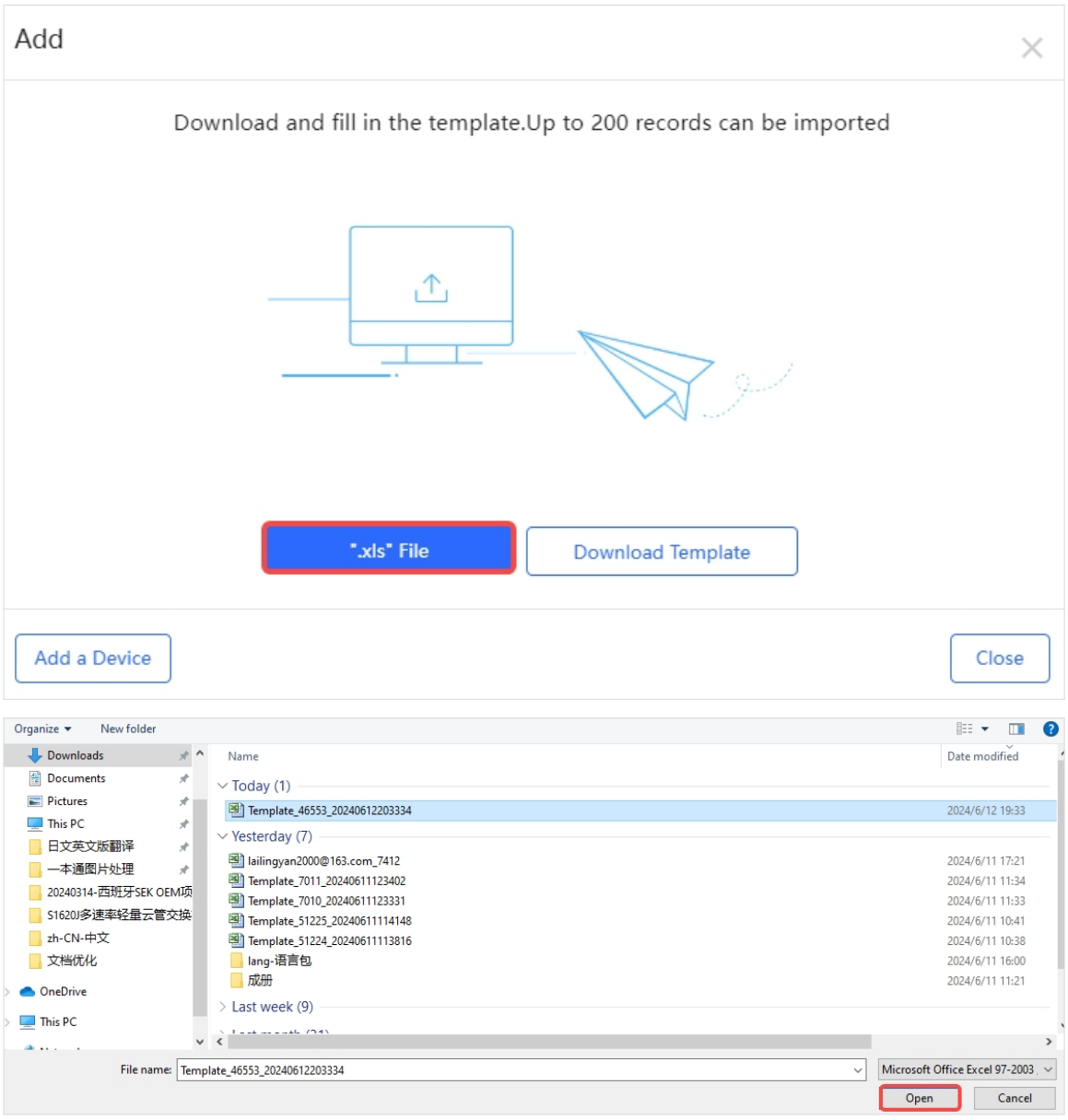
3 Click **Download Template** to download the template.



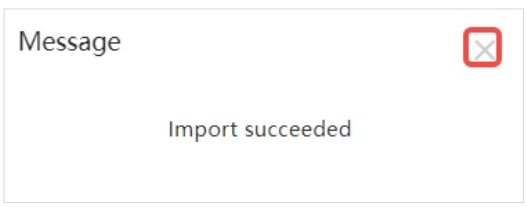
4 Fill in the template. The SN is required, while the alias is optional. Up to 200 devices can be imported at a time.

	A	B
1	SN	Alias
2		
3		

5 Click **".xls" File** to upload the template.



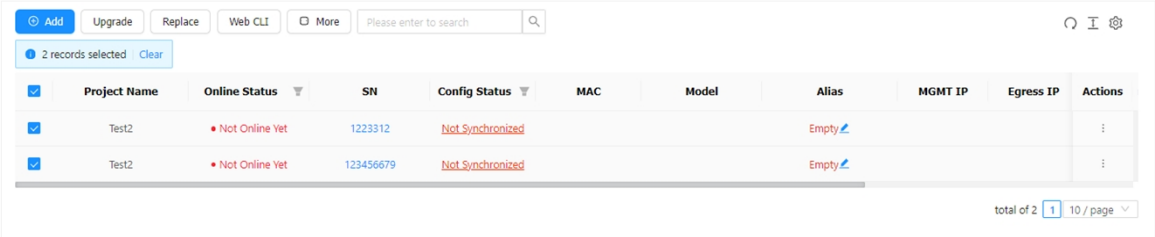
6 When the "Import Succeeded" prompt appears, click **X** to close the prompt box and complete the operation. The imported device will be displayed in the switch list.



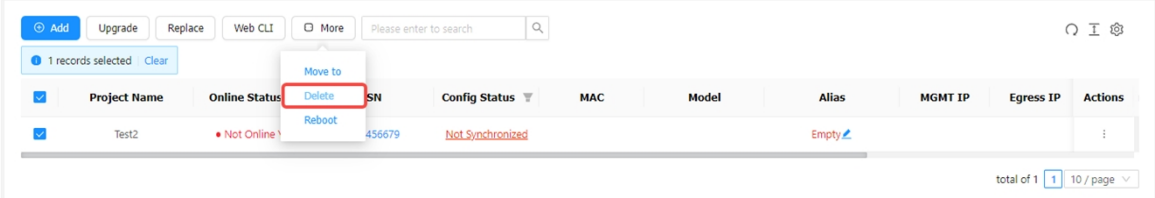
4.2.3 Deleting Switches in Batches

To delete switches from a project in batches.

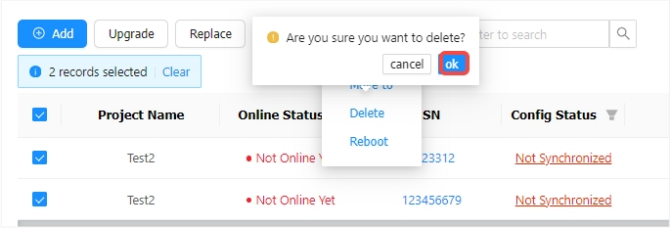
1 Select the switch to be deleted.



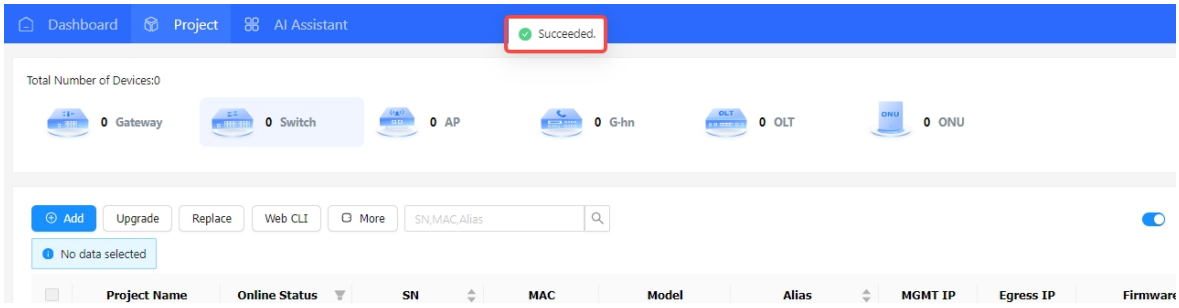
2 Click **More,** and then click **Delete**.



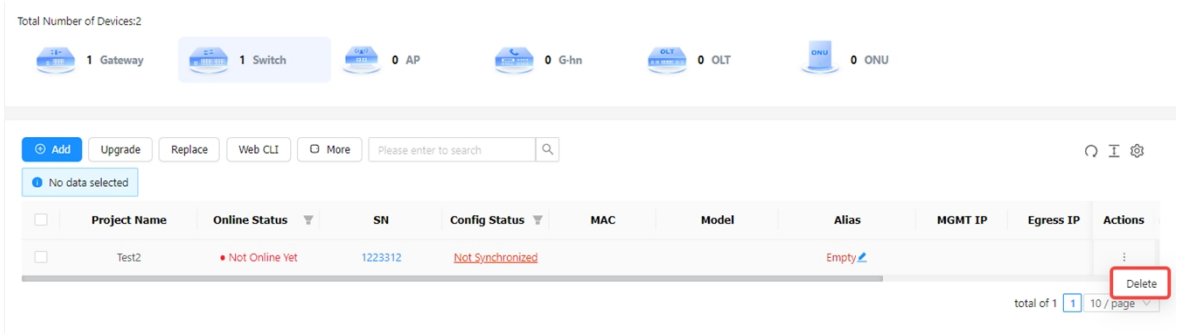
3 Click **OK** in the operation confirmation box.



4 After the "Succeeded" prompt appears, the devices are deleted.



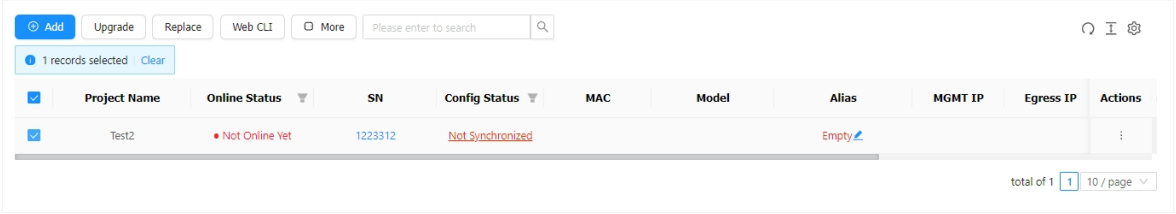
In addition to the above deletion methods, users can also delete devices one by one through the **Delete** button in the **Action** column.



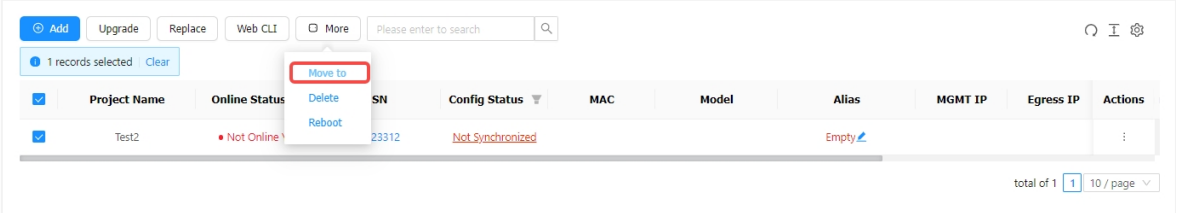
4.2.4 Moving Switches

To move a switch from the project it resides to another project for management:

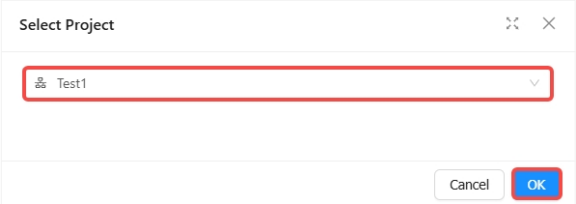
1 Select the switch you want to move to another project.



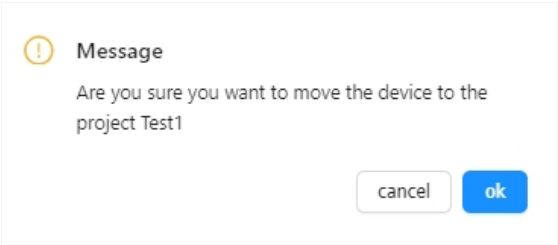
2 Click **More** and then click **Move to**.



3 Select a new project and click **OK**.



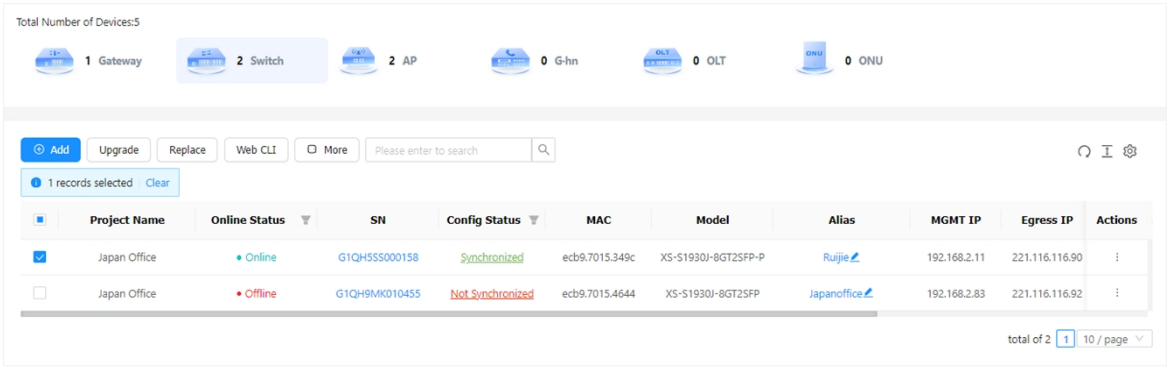
4 When the operation confirmation box appears, click **OK**.



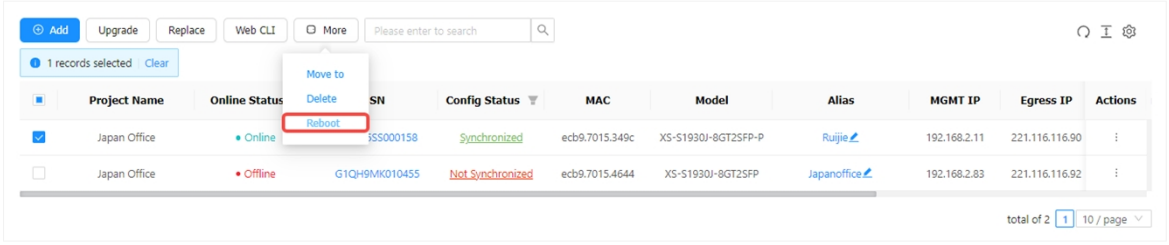
4.2.5 Restarting Switches

To restart an online switch remotely through JaCS:

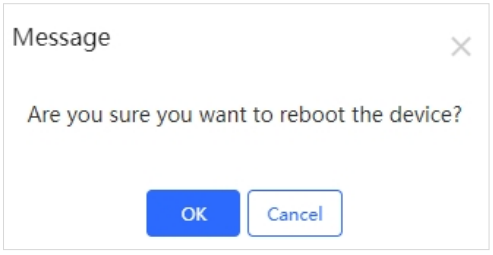
1 Select the switch to be restarted.



2 Click **More** and then click **Reboot**.



3 Click **OK** in the operation confirmation box, and wait for the device to restart.



4.2.6 Configuration Replacement

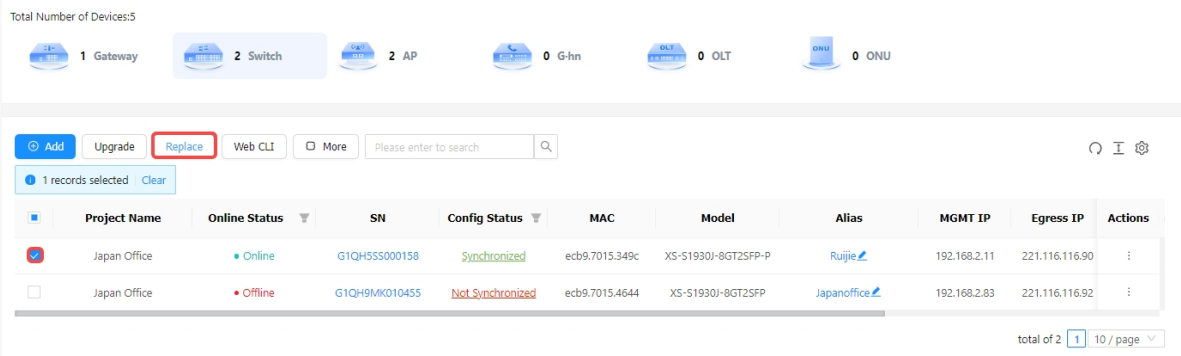
The configuration replacement function can synchronize the configuration of an old or faulty device to a new device of the same model. After the configuration replacement task is complete, the JaCS will send the configuration of the old device to the new one when it goes online. In this way, users do not need to manually configure the new device again, help to improve O&M efficiency.

Note

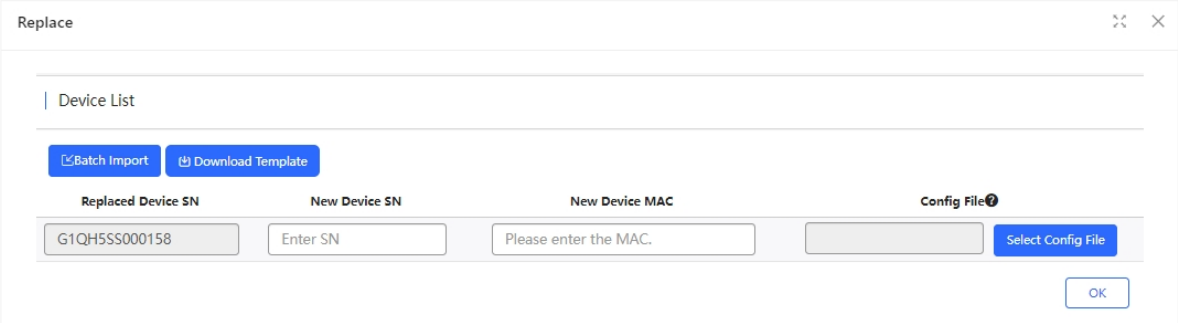
Switch configuration replacement can only be performed between switches of the same model.

The specific steps are as follows:

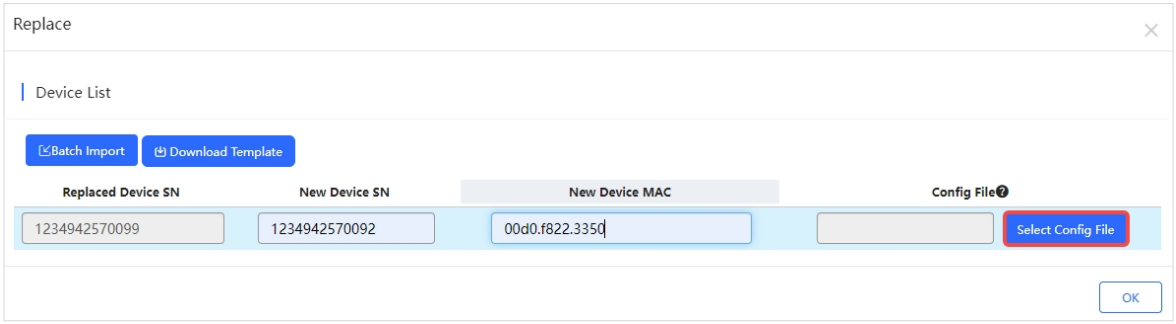
1 Select an existing device and click **Replace**.



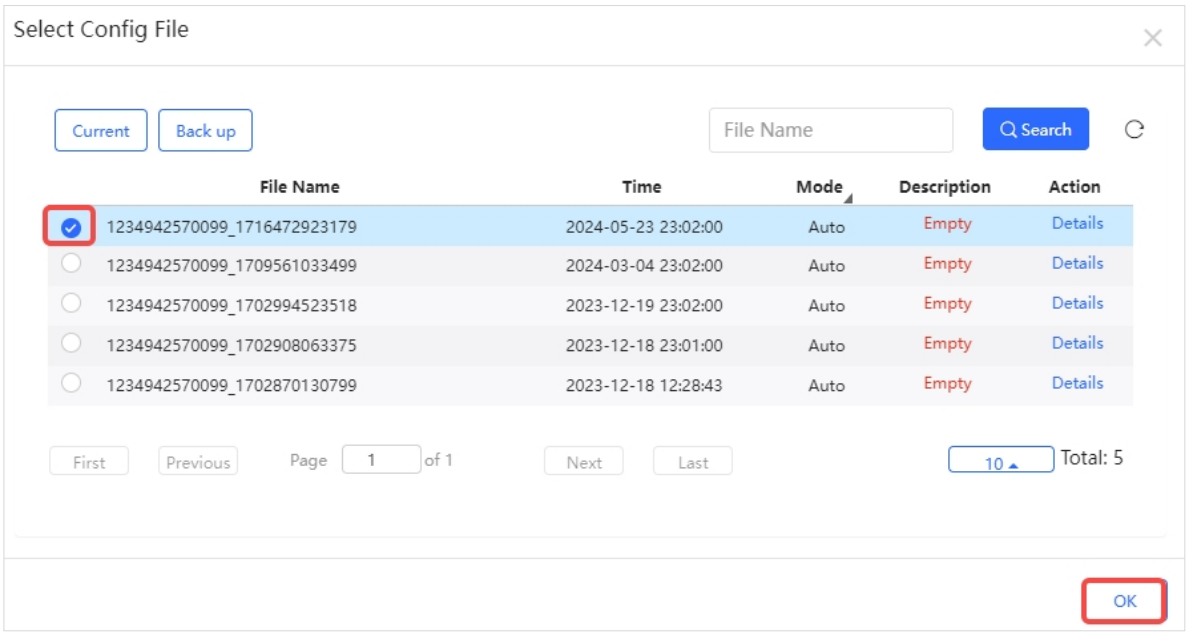
2 Enter the SN and MAC address of the new device. Please make sure that the SN and MAC of the new device match each other.



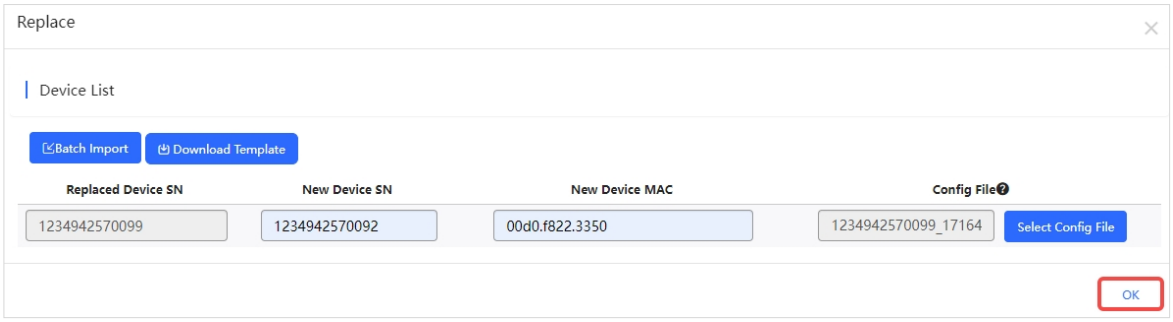
3 Click **Select Config File** and select the configuration file of the existing device, and then click **OK**.



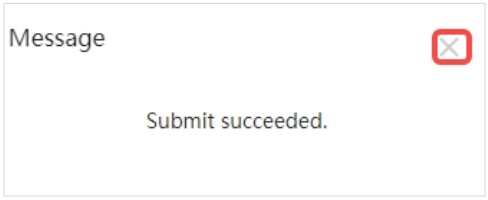
Click **Current**, you can view the current device configuration; click **Backup**, you can to back up the current device configuration.



4 After selecting the configuration file, click **OK**.

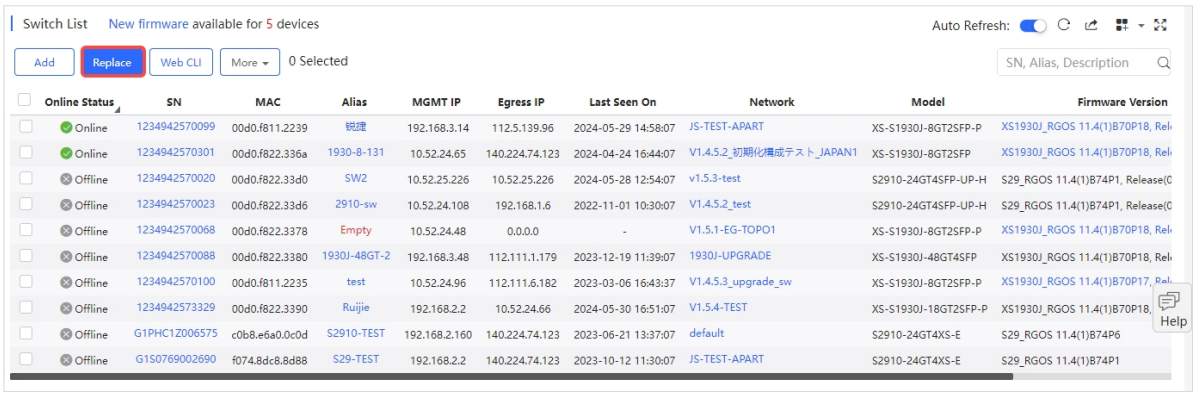


5 After the "Submit Succeeded" prompt appears, click **X** to close the box and complete the operation.

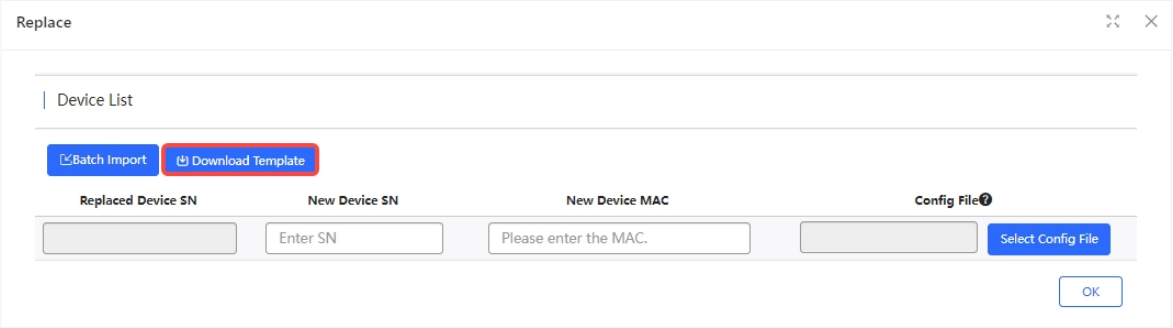


If you need to replace configuration in batches, you can follow the steps below:

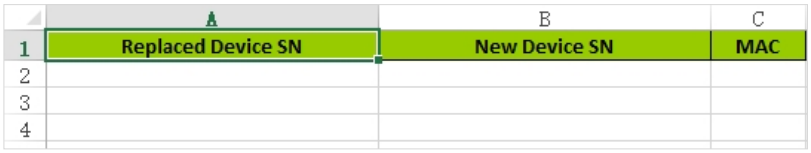
1 Click **Replace**.



2 Click **Download Template** to download the template.

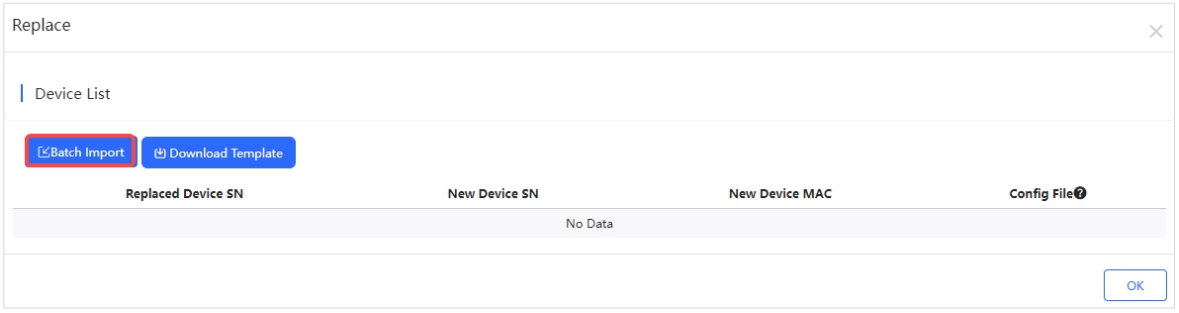


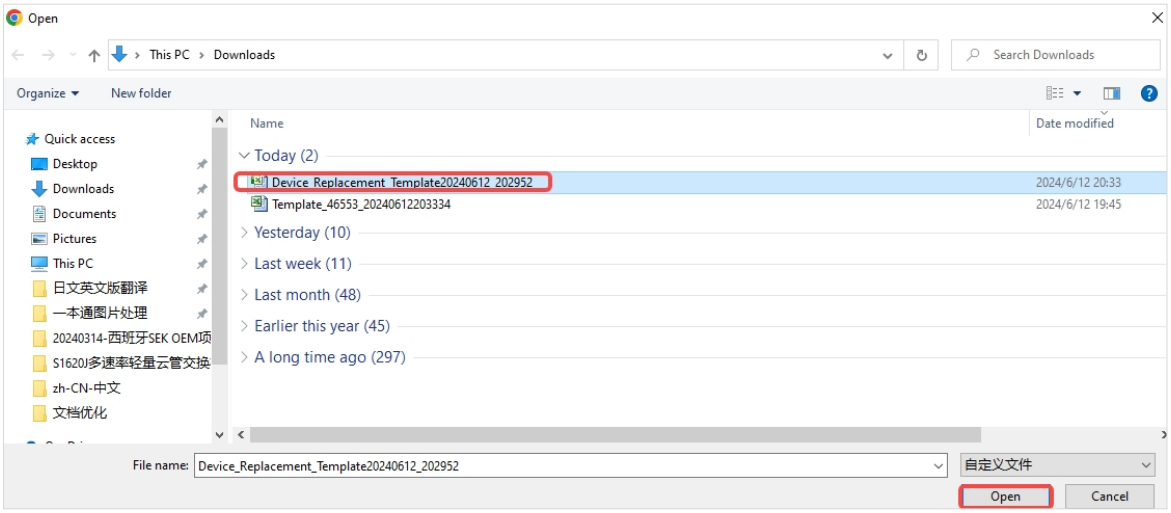
3 Fill in the template. You can fill in up to 200 items at a time.



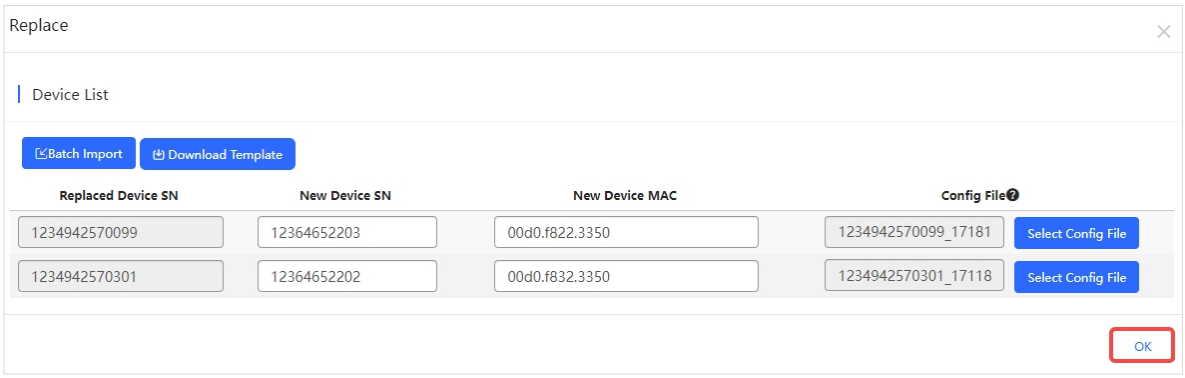
Items	Description
Replaced Device SN	Enter the SN of the existing device .
New Device SN	Enter the SN of the new device .
MAC	Enter the MAC address of the new device.

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

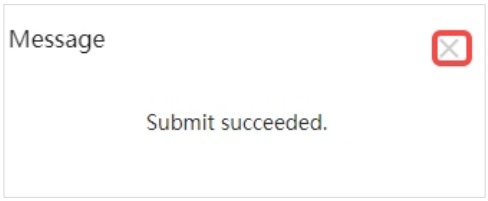




5 Select the configuration file for your new switches and click **OK**.

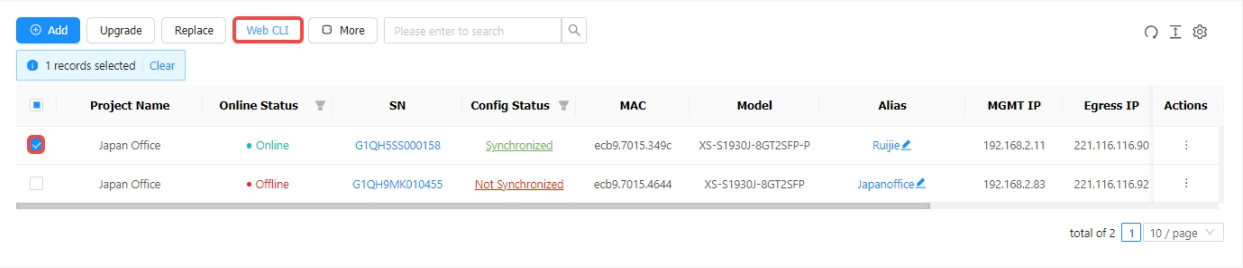


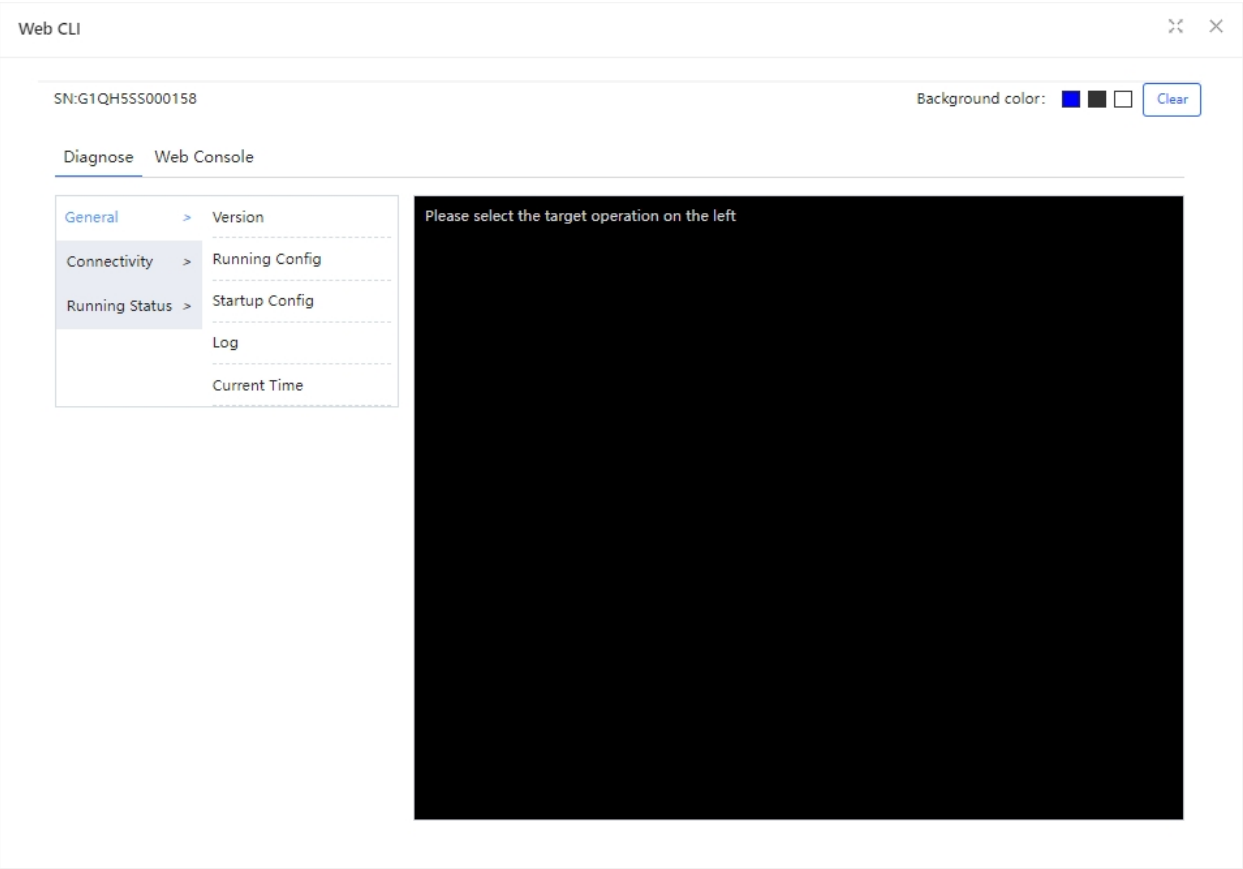
6 After the "Submit Succeeded" prompt appears, click **X** to complete the operation.



4.2.7 Delivering Configuration via Web CLI

Ruijie JaCS supports managing switches via Web CLI. Select the switch to be managed and click **Web CLI**. Commonly used CLI commands are provided on the left side of the Web CLI page. Click a command or enter a command manually to send the relevant configuration to the device.





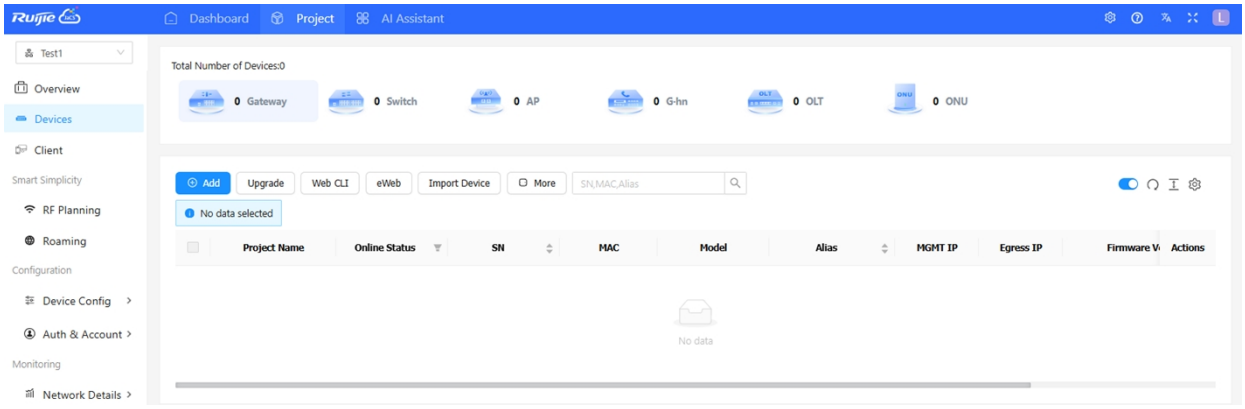
4.3 Gateway

This section gives a brief introduction to the gateway management interface and operation steps on the JaCS, including:

- Gateway Managament Interface: Introduce the gateway management interface of the JaCS.
- Adding Gateways: Introduce how to add or batch add gateways to an existing project.
- Deleting Gateways: Introduce how to delete or batch delete gateways from a project.
- Moving Gateways : Introduce how to move a gateway from the project it resides to another one.
- Restarting Gateways: Introduce how to restart an online gateway remotely via the JaCS.
- Delivering Configuration via Web CLI: Introduce how to use the WEB CLI interface to deliver configurations to gateways.
- Accessing the Gateway's eWeb : Introduces how to access the gateway's eWeb through the JaCS.
- Creating a Tunnel: Introduces how to create a Web-based tunnel to access the eWeb system of the gateway to achieve more monitoring and management functions.

4.3.1 Gateway Management Interface

Click **Project** > **Gateway** to go to the gateway management interface. After selecting a specific project, you can manage the gateway devices in this project.

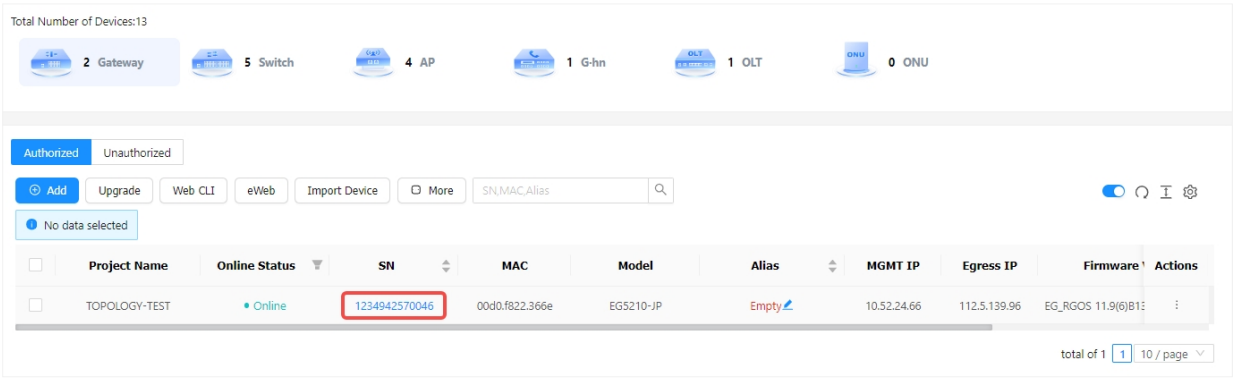


Items	Description
Project Name	Displays the name of the project where the gateway is located.
Online Status	Displays the online status of the gateway. The online status of the device includes: Online/Offline/Not Online Yet. Click the filter icon to filter devices by online status.
SN	Displays SNs of gateways. Click the SN number of a gateway, you can view its detailed information.
MAC	Displays MAC addresses of gateways.
Model	Displays the models of gateways.
Alias	Displays the aliases of gateways.
MGMT IP	Displays the management addresses of gateways.
Egress IP	Displays egress IP addresses of gateways.

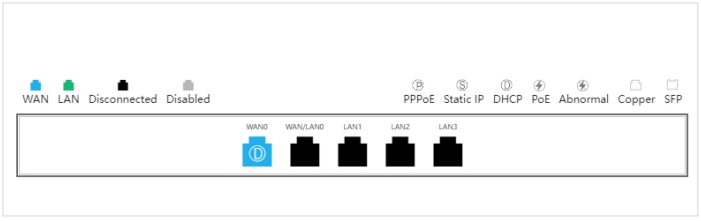
Firmware Version	Displays firmware versions of gateways.
Last See On	Displays the last online time of gateways.
Actions	Click the **Delete** icon in the **Action** column, you can remove the gateway from the project.

Button	Description
Add	Add button. Click this button to go to the device adding interface.
Upgrade	Upgrade button. After selecting the device, click this button to remotely upgrade the device.
Web CLI	Web CLI button. Click this button to enter WEB CLI page to deliver configurations to the device.
eWeb	eWeb button. Select an gateway, and click this button to can access its eWeb.
Import Device	Batch import gateway button. Click this button to add gateways in batches to a project.
More	Click this button to display more operation buttons, including **Move to**, **Delete**, and **Restart**.
	Refresh button. Click this button manually to refresh the gateway list.
	Row height adjustment button. Click this button to adjust the row height.
	Click this button to customize the displayed items in the gateway list.
	Automatic refresh switch button. The automatic refresh function is enabled by default. When it is enabled, the gateway device list will automatically refresh once every minute.
SN,MAC,Alias	Search box. Supports searching gateways according to their SN, MAC addresses, and aliases.

Click the **SN** of a gateway in the gateway list to enter its detailed information interface. The detailed interface consists of the following tabs: **port panel**, **basic information**, **device overview**, **WAN**, **LAN**, **configuration**, **alarm**, and **tunnel**.

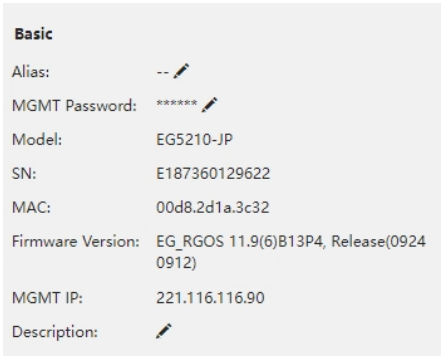


(1) Port Panel

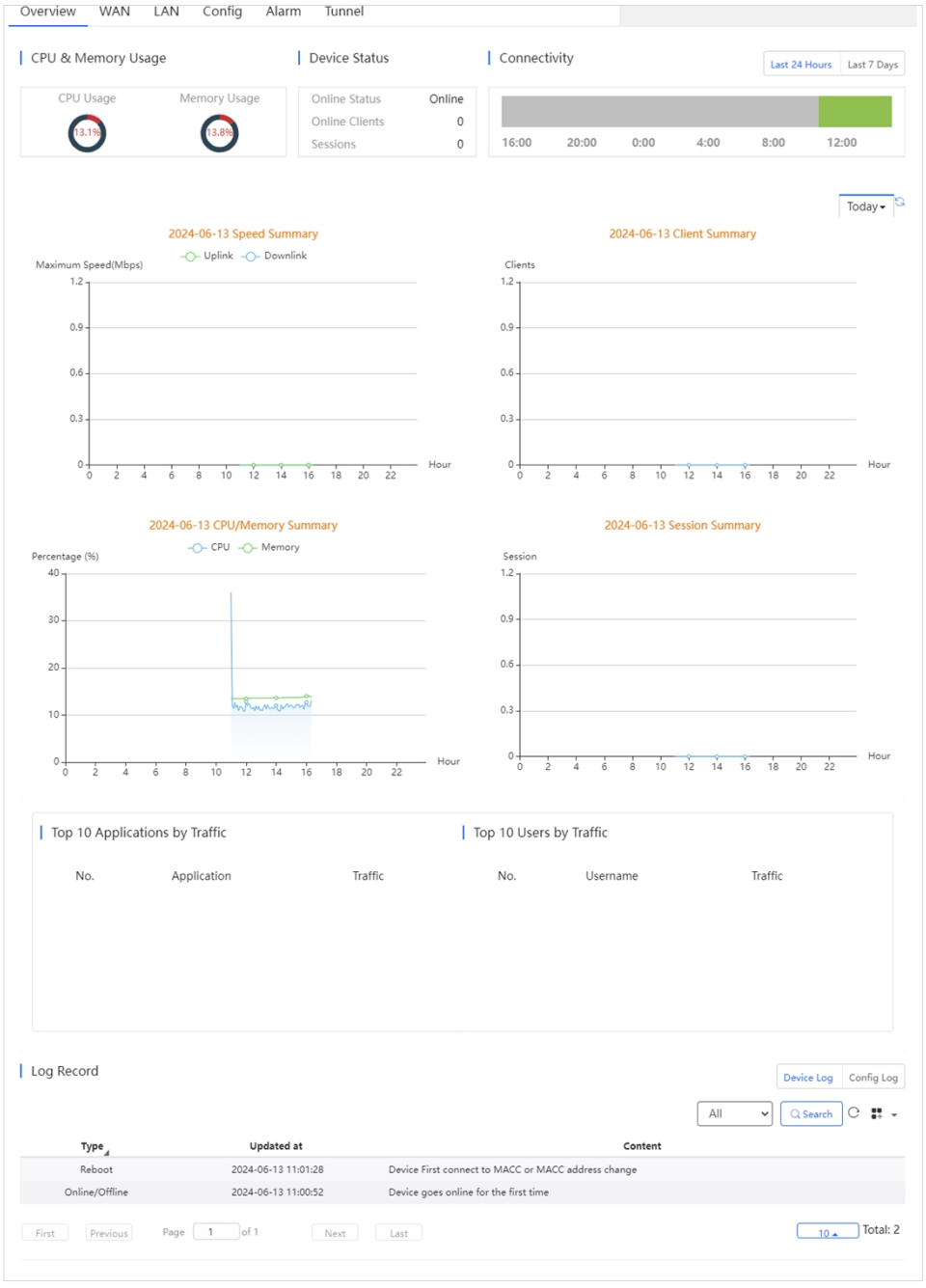


(2) Basic Information

The basic information tab displays the alias, the model, the SN, the MAC address, the firmware version, the management IP and the description of the gateway. Click the edit icon next to the alias, description and management password to edit them.



(3) Overview Tab

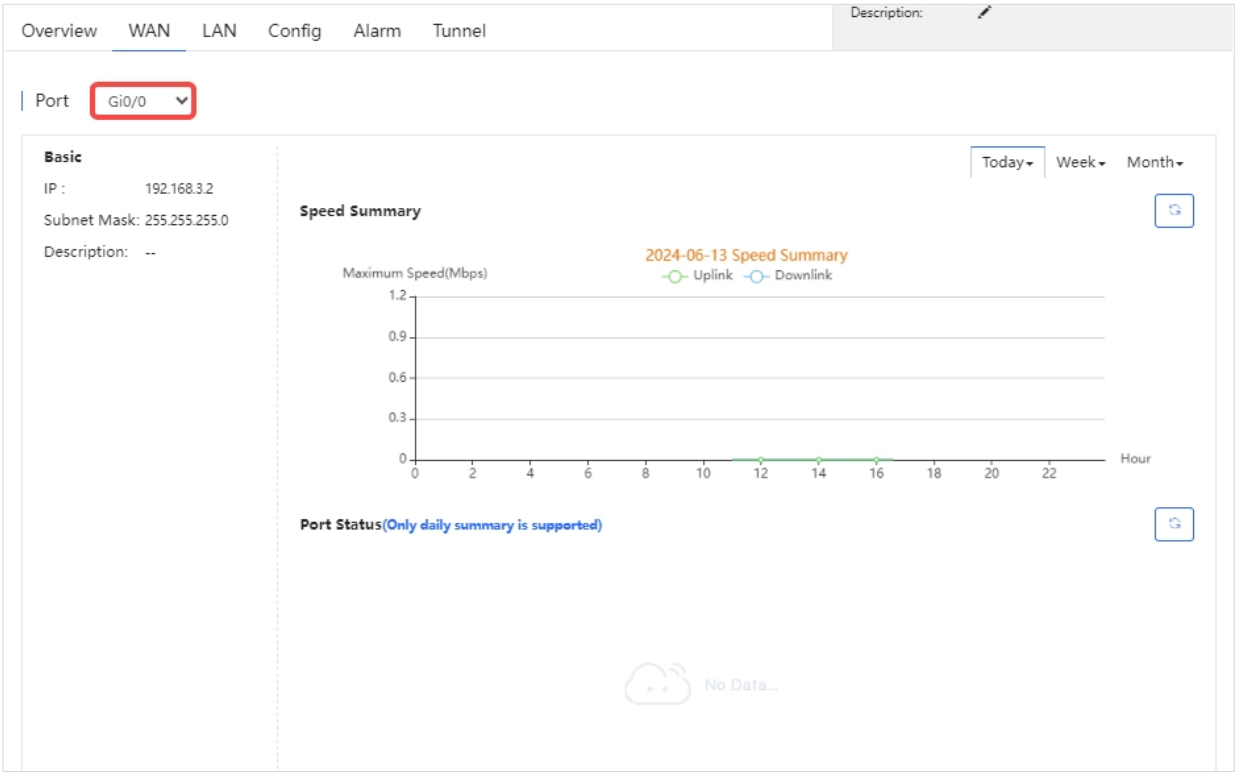


Items	Description
CPU & Memory Usage	Displays CPU and memory usage.

Device Status	Displays device status including device online status, number of online clients, and number of sessions.
Connectivity	Displays the connection status between the gateway and the cloud in the last 24 hours or 7 days.
Speed Summary	Displays the device's uplink/downlink rate statistics for a certain day in the last 1 to 3 days. By default, the statistics for the current day are displayed. Hover the mouse over a certain time to view the information at that time.
Client Summary	Displays the client statistics of a certain day in the last 1 to 3 days. By default, the statistics of the current day are displayed.
CPU/Memory Summary	Displays the CPU and memory statistics of the device for a certain day in the last 1 to 3 days. By default, the statistics for the current day are displayed.
Session Summary	Displays the session statistics of the device for a certain day in the last 1 to 3 days. By default, the statistics for the current day are displayed.
Top 10 Applications by Traffic	Top 10 applications by downlink traffic are displayed.
Top 10 Users by Traffic	Top 10 users by downlink traffic are displayed.
Log Record	Supports viewing device logs and operation logs.

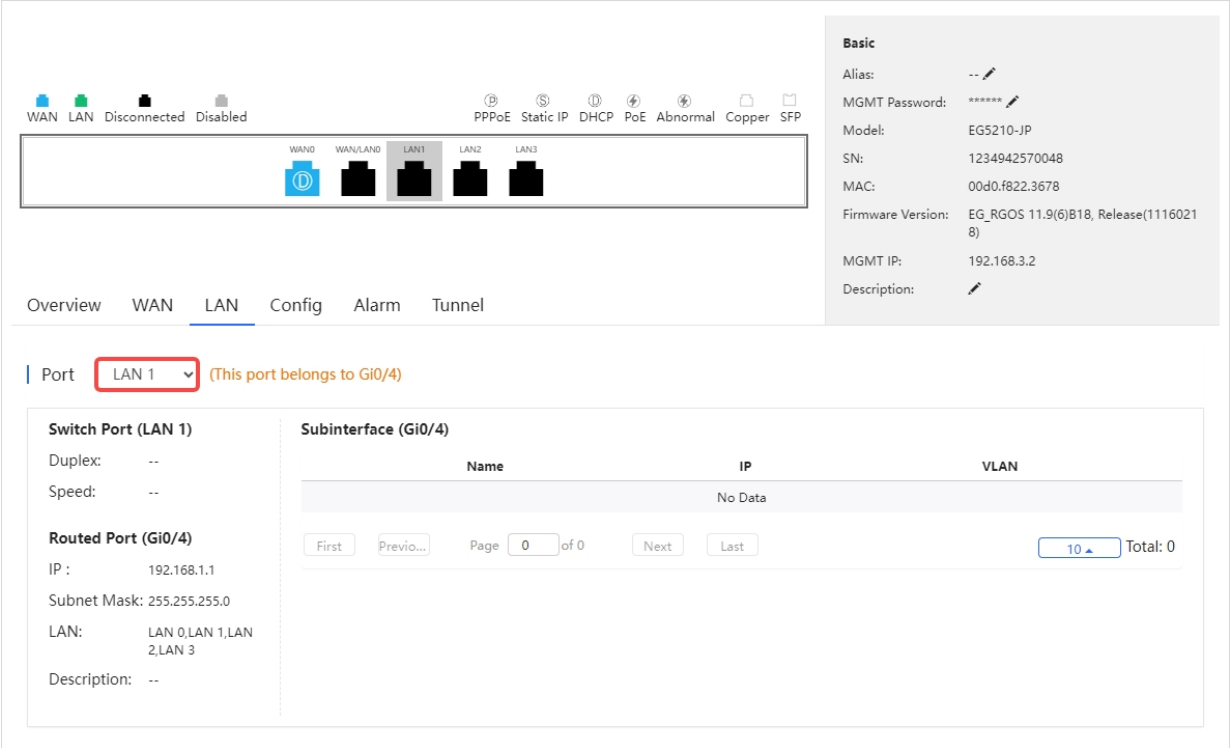
(4) WAN

Select a WAN port to view its port information and the rate statistics in a specific time period (today/week/month). Hover the mouse to a certain time, you can view the rate information at that time.



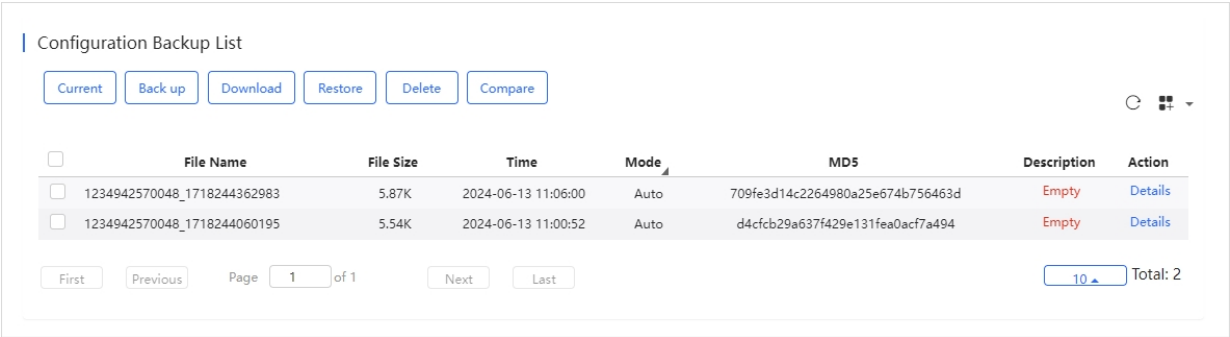
(5) LAN

Select a LAN port to display the corresponding information of its switch port, routing port, and sub-interface.

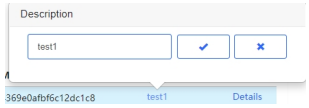


(6) Configuration Tab

In this tab, you can back up the gateway configuration. The information displayed in the backup list includes the configuration file name, file size, backup time, mode, MD5 and description.

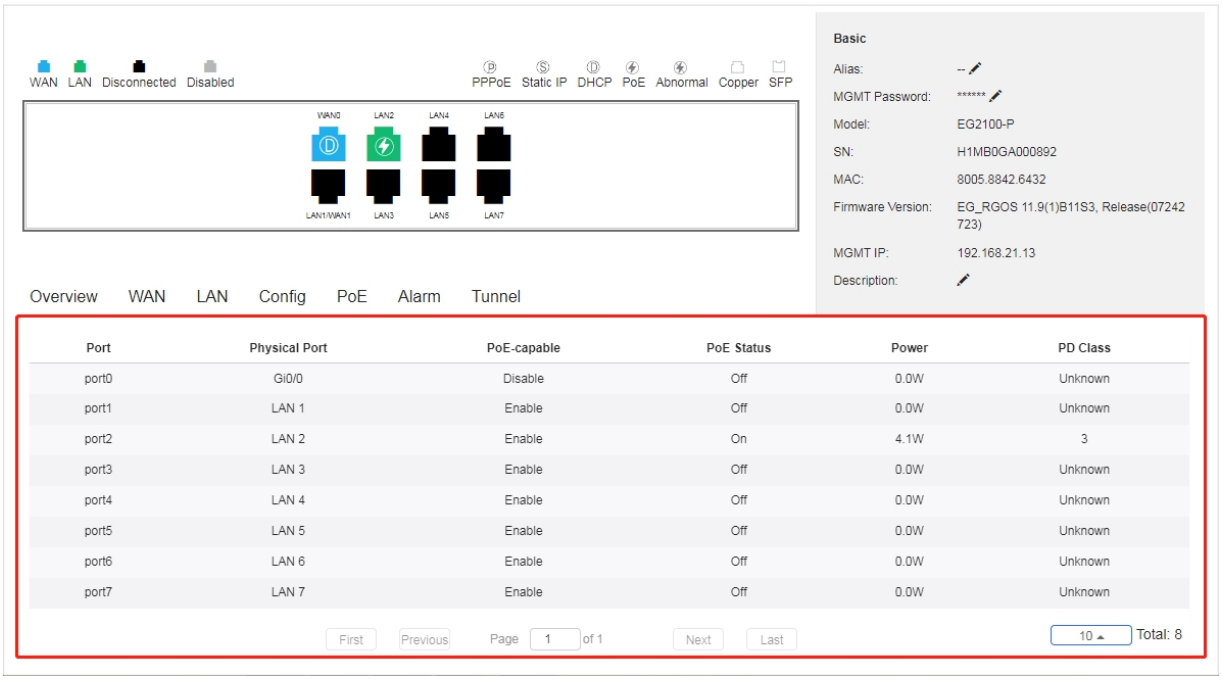


Button	Description
Current	Click the Current button to display the current configuration of the device. Click the **Backup** on the current device configuration interface, you can back up the configuration. After the backup, click ↻ to refresh the list, and the backed up file will be displayed in the list.
Back up	Configuration backup button. Click the **Backup**, and click **OK** in the operation confirmation box to back up the current device configuration. After the backup, click ↻ to refresh the list, and the backed up file will be displayed in the list.
Download	Download button. Select the configuration file to be exported, click **Download**, and then click **OK** in the operation confirmation box. Only one configuration file can be downloaded at a time.
Restore	Backup file restore button. Select a configuration file and click **Restore** to restore the current configuration file of the device to the selected configuration file. Only one file can be restored at a time.
Delete	Delete button. Select the configuration file to be deleted, click **Delete**, and when the operation confirmation box appears, click **OK**.
Compare	Profile comparison button. Select two configuration files to be compared and click **Compare** to compare them to figure out their differences.
Details	Click the **Details** in the **Action** column to view the detailed information.

Description	Click the words in the description column to modify the description. 

(7) PoE (Only for PoE Gateways)

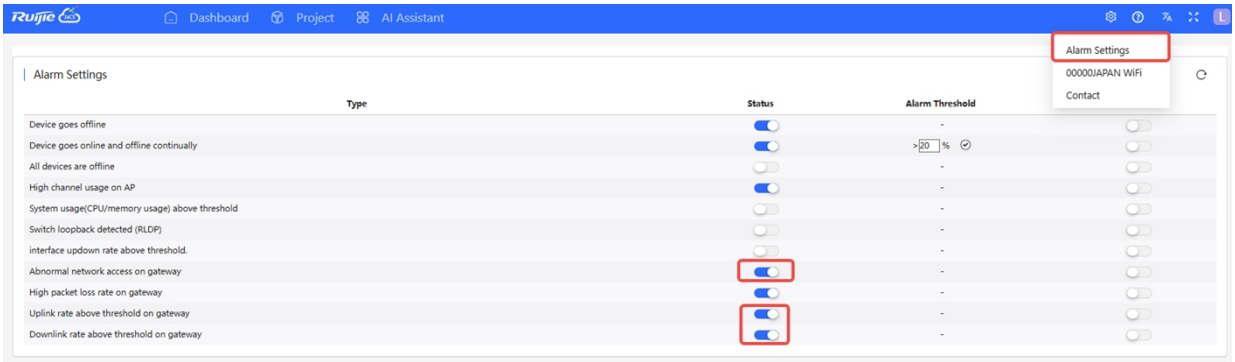
The PoE tab displays the information of ports, physical ports, PoE-capable status, PoE status, power, and PD classes.



(8) Alarm

In this tab, you can set alarm conditions, including sending alarms based on the number of times of exceeding the bandwidth thresholds, the number of ping failures, and the packet loss rate within a certain period of time.

If you want to send an alarm based on the number of times of exceeding the bandwidth thresholds, make sure that "**Uplink rate above threshold on gateway** " and "**Downlink rate above threshold on gateway** " in the **Alarm Settings** interface are enabled before configuration. If you want to configure an alarm based on the number of ping failures, make sure that "**Abnormal network access on gateway**" in the **Alarm Settings** interface is enabled before configuration.

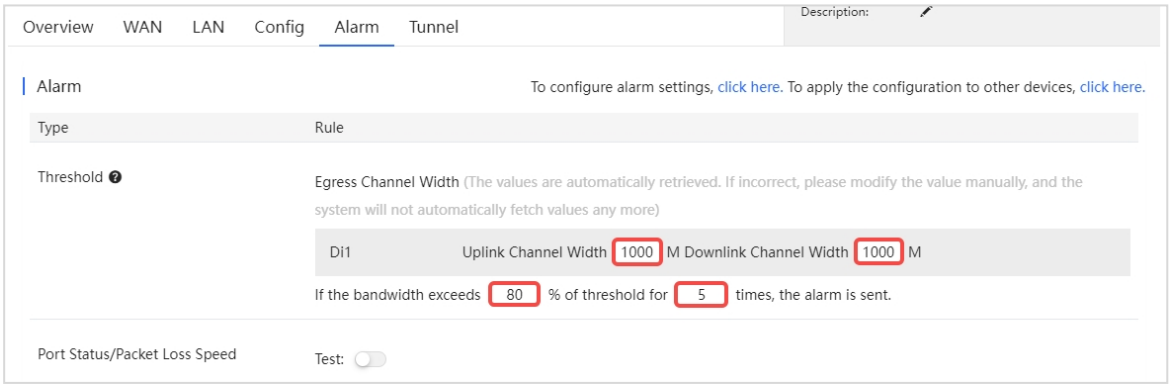


- **Sending Alarms based on the Number of Times of Exceeding the Bandwidth Threshold**

  By default, the system sets the upstream bandwidth to 1000 M, the downstream bandwidth to 1000 M, the threshold to 80%, and the number of times of exceeding the thresholds to 5. That is, when the bandwidth exceeds 80% of the total bandwidth for 5 times, an alarm will be generated. After modifying as needed, remember to click **Save** to save the configuration.

Note

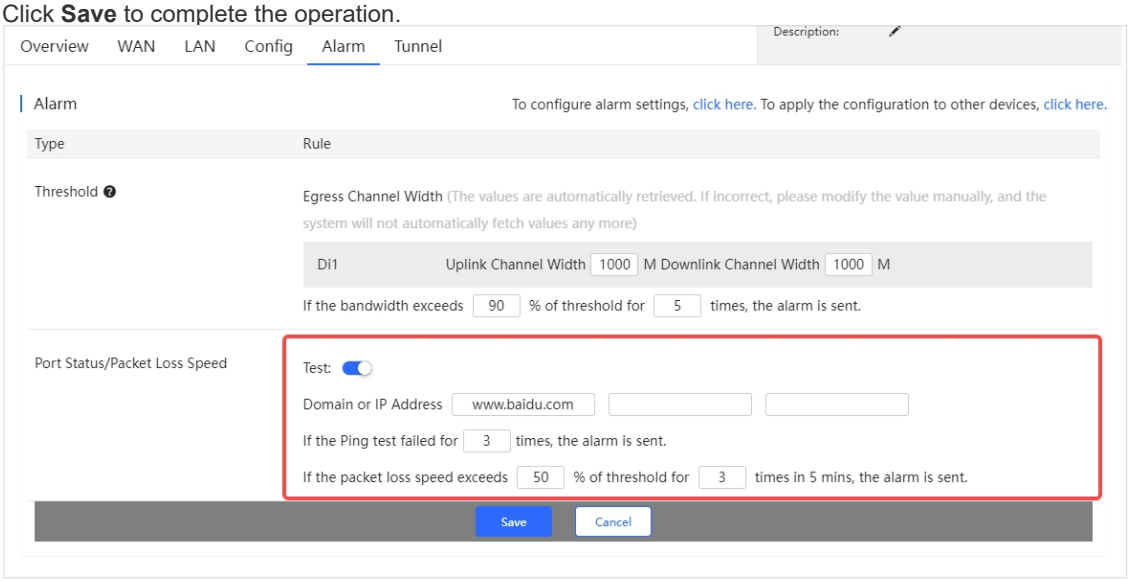
Threshold range: 1-100%; frequency range: 1-6 times.



- **Sending Alarms Based on the Number of Ping Failures and Packet Loss Rate within a Certain Period**

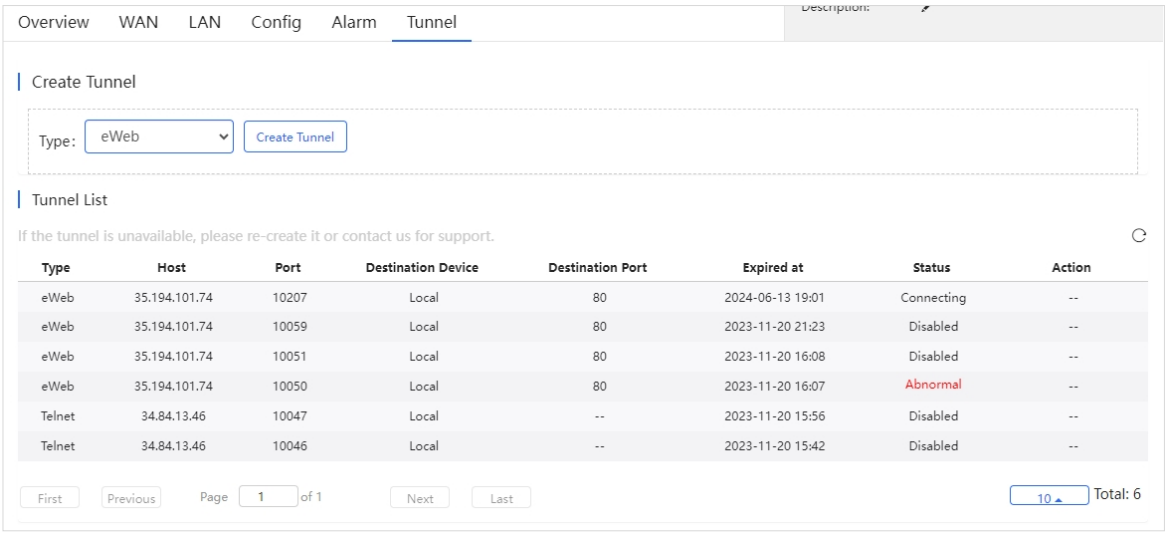
The specific steps are as follows:

1) Enable the Test.
2) Set the domain name or IP address. Up to 3 domain names or IP addresses can be entered.
3) Set the number of Ping test failures. The supported number range is 1-10 times.
4) Set the packet loss rate threshold and the number of times within 5 minutes. (Threshold range: 1-100 %; number range: 1-100 times.)
5) Click **Save** to complete the operation.



(9) Tunnels Tab

In this tab, you can create a tunnel. The tunnel types supported by JaCS are Telnet, eWeb, and SSH. Different devices support different types of tunnels. Please refer to the actual device. After selecting the type of tunnel you want to create, click **Create Tunnel**. The created tunnel will be displayed in the tunnel list.



Note

A tenant can create up to 10 tunnels, and up to 5 tunnels can be created for a device. When the number of created tunnels has reached the limit, please close unused tunnels and try again.

4.3.2 Adding Gateways

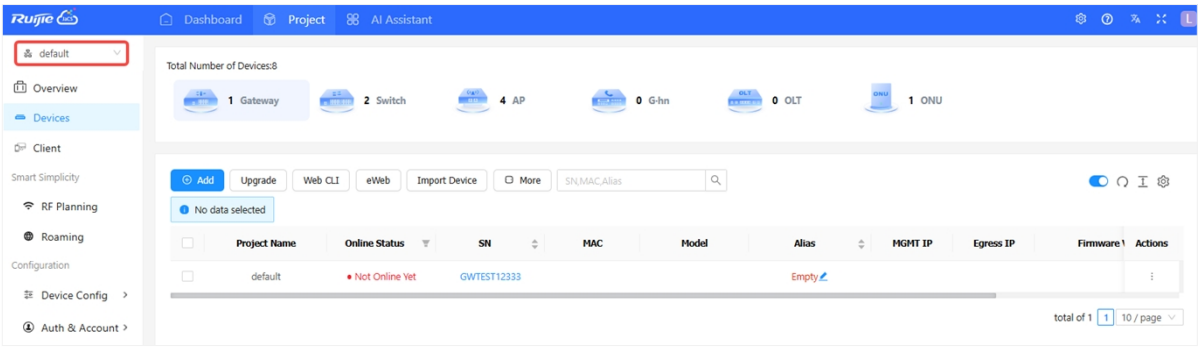
JaCS provides two ways to add gateways to a specific project.

- Adding a Gateway
- Adding Gateways in Batches

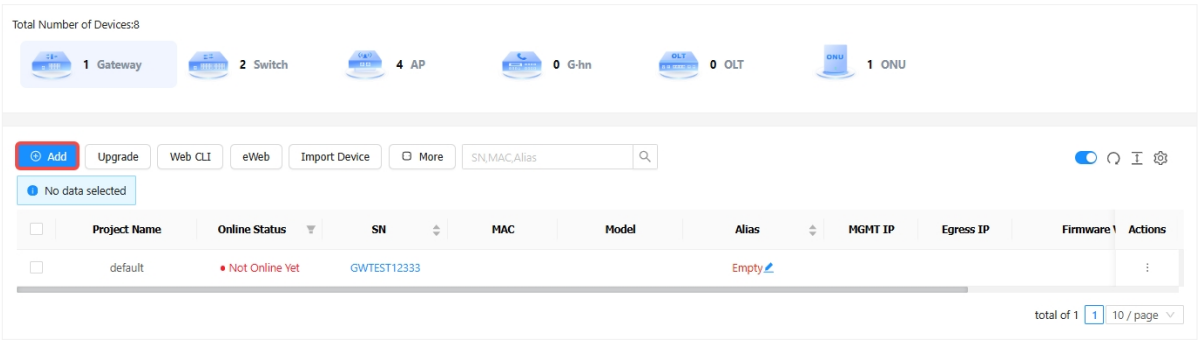
4.3.2.1 Adding a Gateway

Follow the steps below to add the gateway to a project.

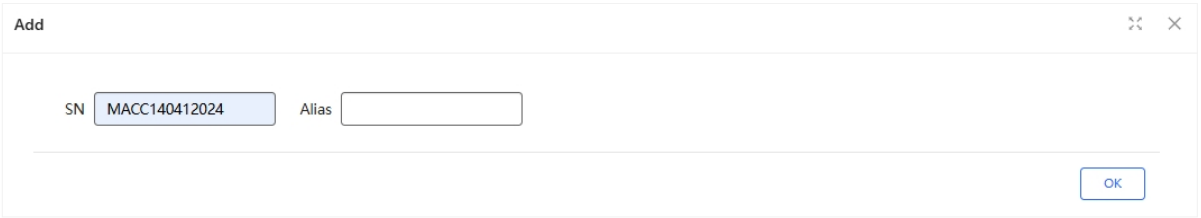
1 Select the project to which the gateway need to be added.



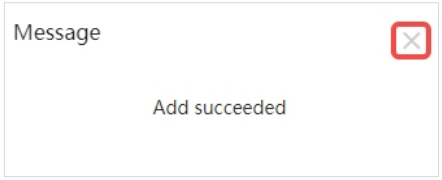
2 Click **Add**.



3 Enter the SN (required) and alias (optional). Only one gateway can be added in this interface.



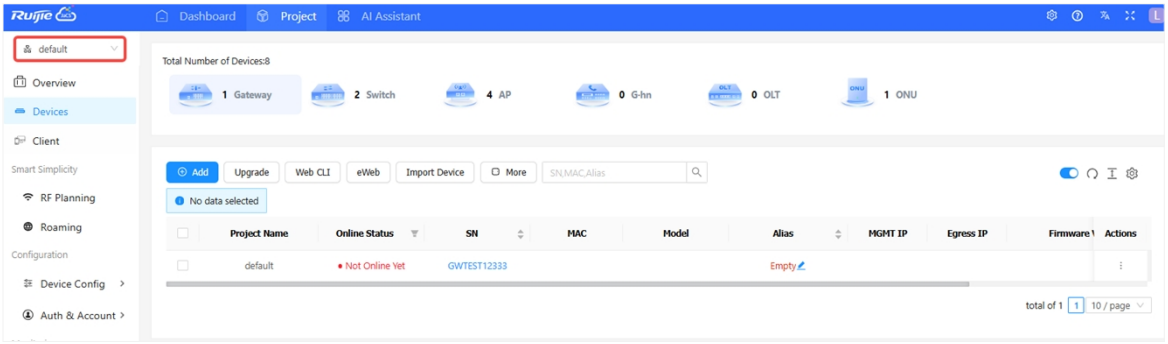
4 After filling in the information, click **OK**. When the "Add succeeded" prompt appears, click **X** to close the prompt box and complete the operation.



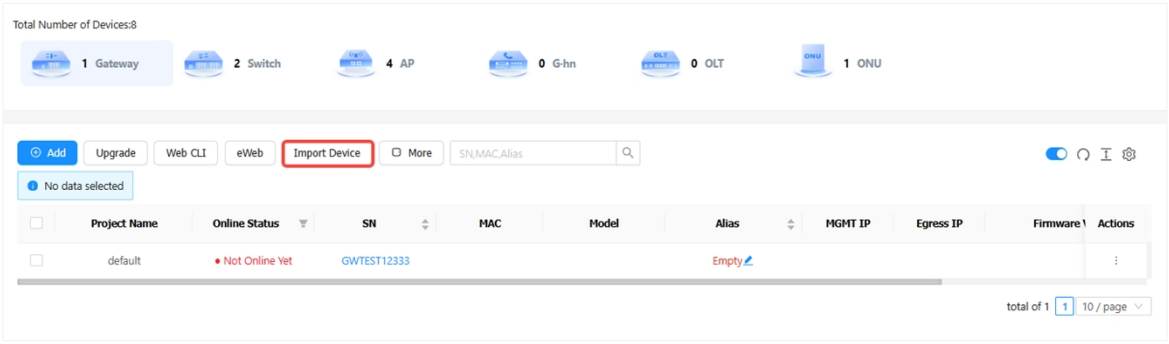
4.3.2.2 Adding Gateways in Batches

Follow the steps below to add gateways to a project in batched.

1 Select the project.

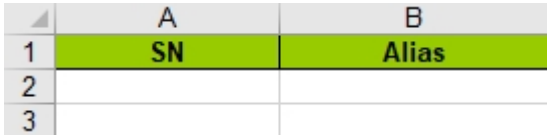


2 Click **Import Device**.



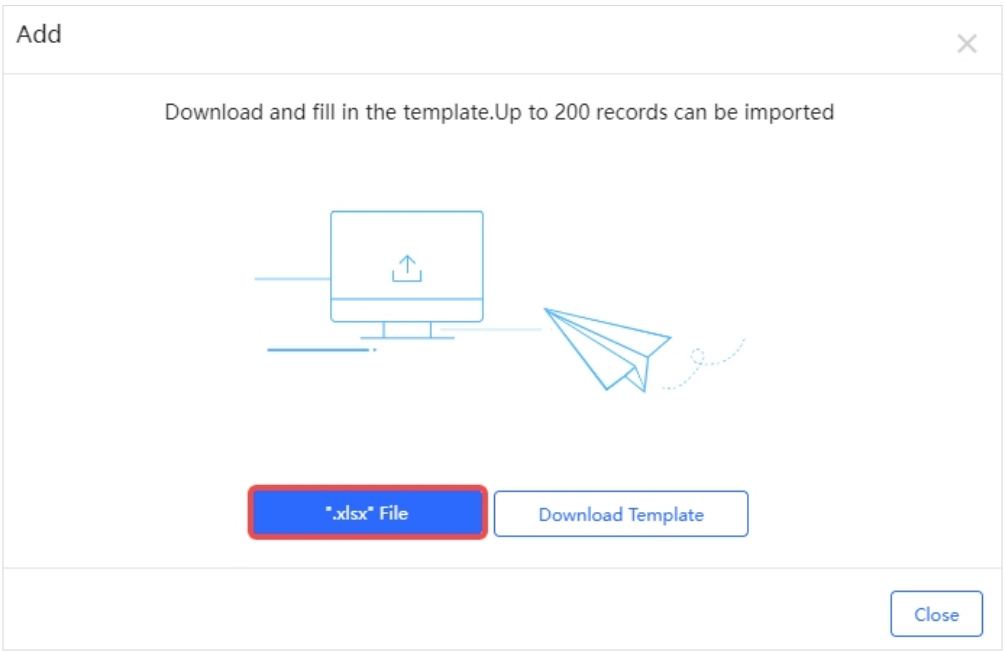
3 Click **Download Template** to download the template.

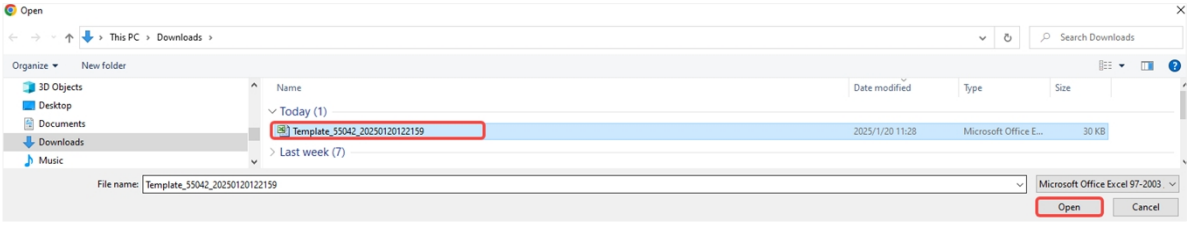
4 Fill in the template. SN is required, while the alias is optional. Up to 200 devices can be imported into a project each time.



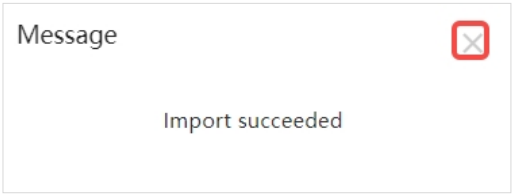
Items	Description
SN	Required. The length of a SN should range from 6 to 21 characters.
Alias	Optional. The length of an alias should range from 1 to 64 characters.

5 Click **".xlsx " File** to upload the template.





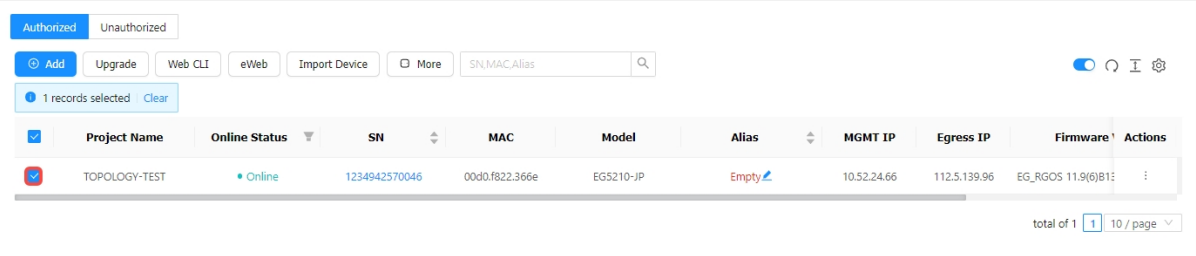
6 When the "Import Succeeded" prompt appears, click **X** to close the prompt box. The imported device will be displayed in the gateway list.



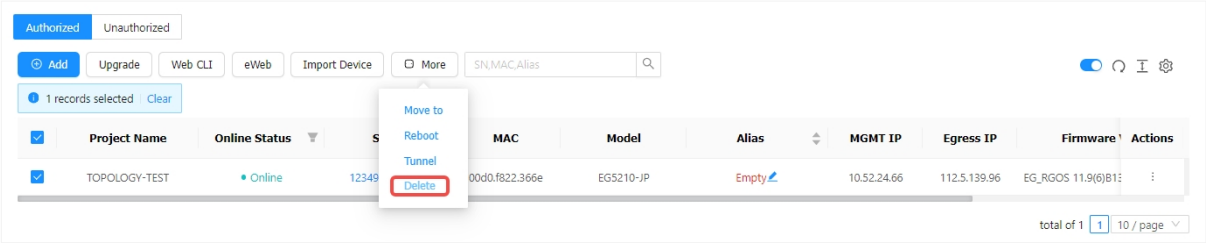
4.3.3 Deleting Gateways

Follow the steps below to batch remove gateways from a project:

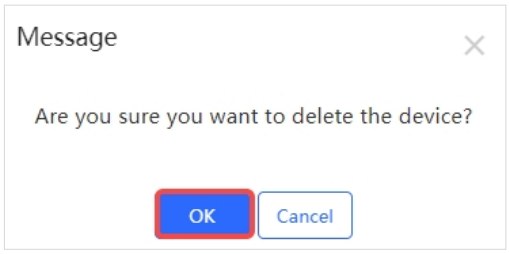
1 Select the gateways you want to delete. Multiple selections are supported.



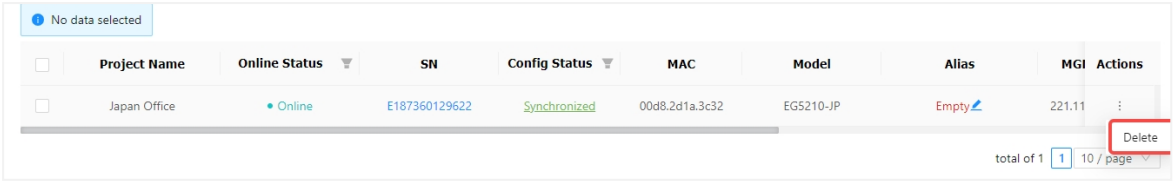
2 Click **More**, and then click **Delete**.



3 Click **OK** in the operation confirmation box to complete the operation.



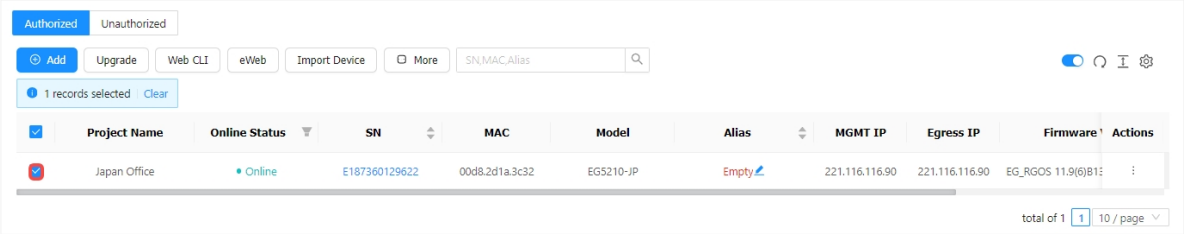
In addition to the above deletion methods, you can also delete devices through the **Delete** button in the **Action** column of the gateway list.



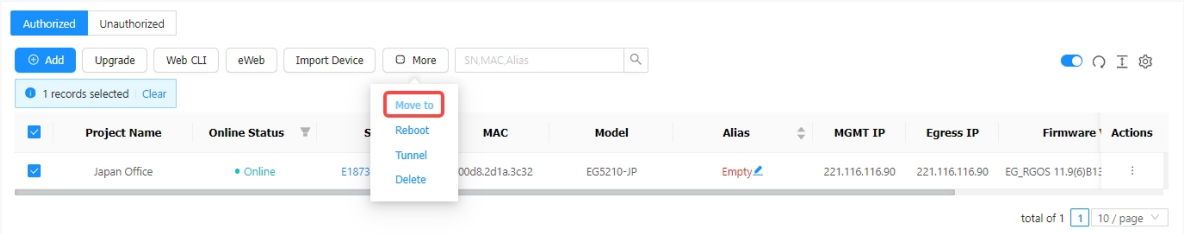
4.3.4 Moving Gateways

Follow the steps below to move a gateway to another project.

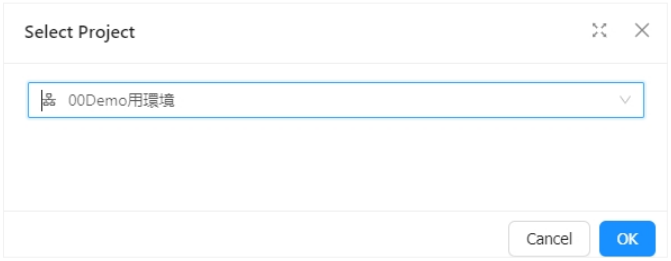
1 In the gateway list, select the gateway you want to move.



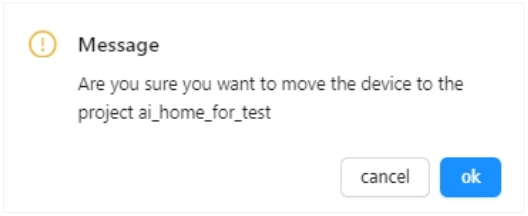
2 Click **More**, and then click **Move to**.



3 Select a new project and click **OK**.



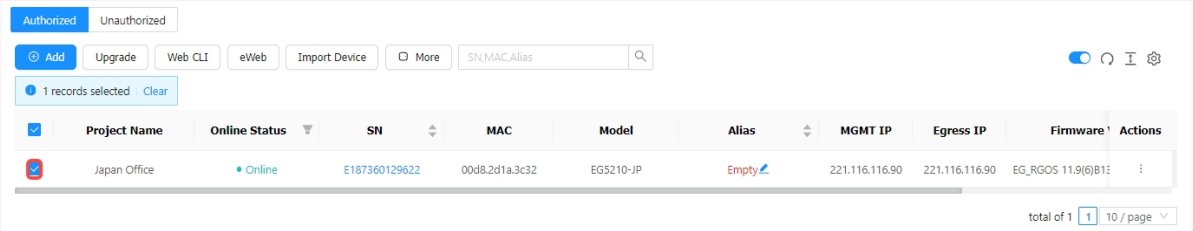
4 When the operation confirmation box appears, click **OK**.



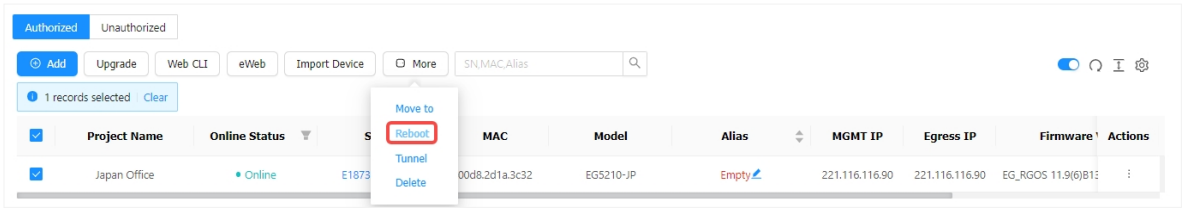
4.3.5 Restarting Gateways

Follow the steps below to remotely restart the gateway.

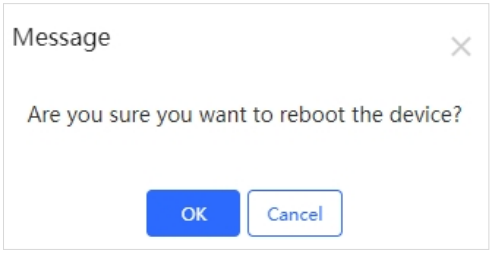
1 Select the gateway to be restarted.



2 Click **More,** and then select **Reboot**.

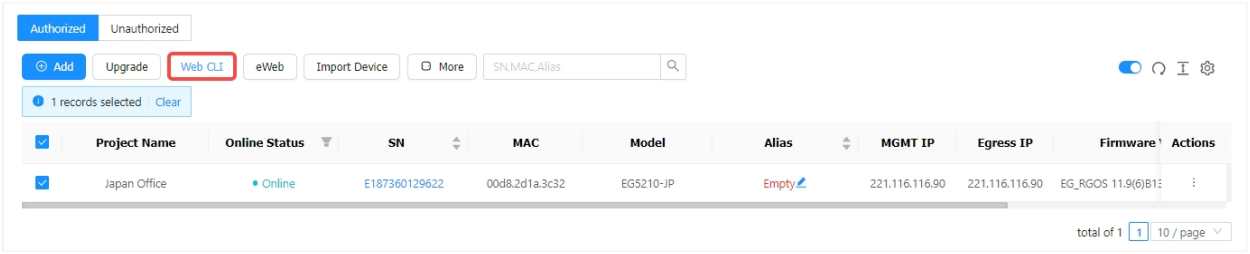


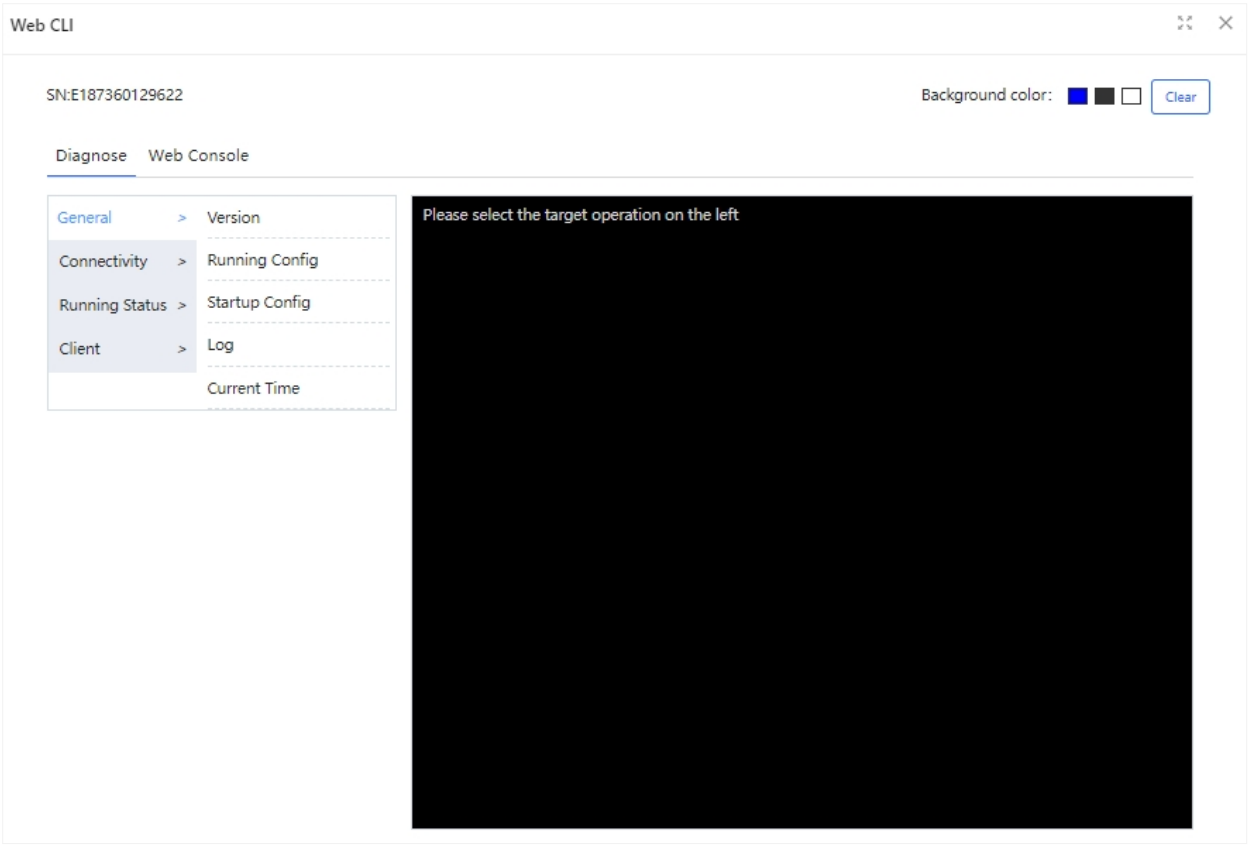
3 Click **OK** in the operation confirmation box, and wait for the device to restart.



4.3.6 Delivering Configuration via Web CLI

Ruijie JaCS supports configuring gateways via Web CLI. Select the gateway to be managed and click **Web CLI**. Commonly used CLI commands are provided on the left side of the Web CLI page. Click a command or enter a command manually to send the relevant configuration to the device.



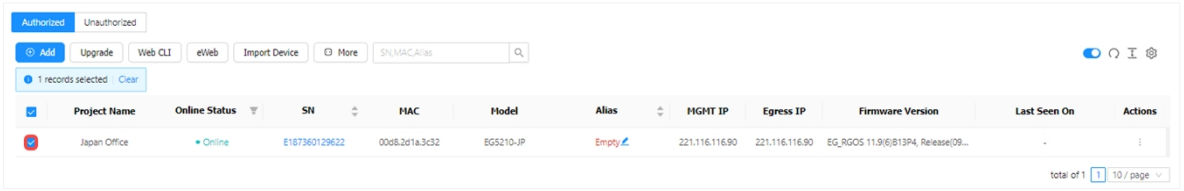


4.3.7 Accessing the Gateway's eWeb

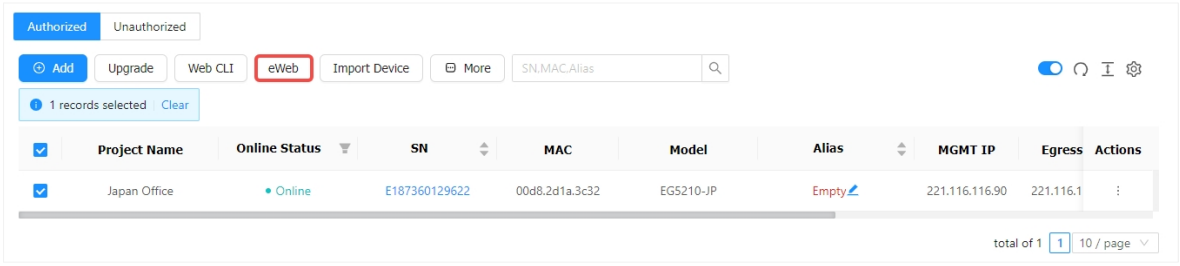
Ruijie JaCS supports accessing the eWeb interface of a gateway through a tunnel.

The specific steps are as follows:

1 Select the gateway.

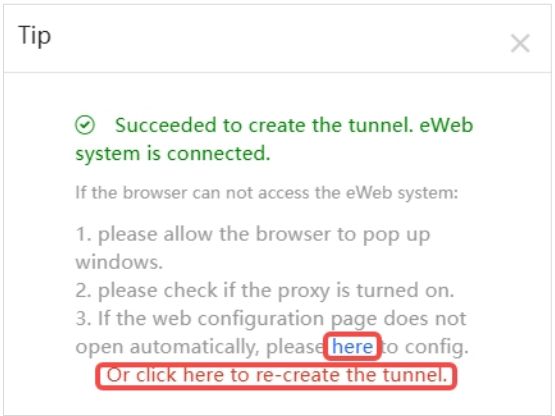


2 Click **eWeb**.



3 After creating the tunnel, the eWeb interface of the device will automatically open in a new tab.

If the eWEB does not open automatically, you can click "**here**" to jump to the eWEB or try to re-create the tunnel.



4.3.8 Creating a Tunnel

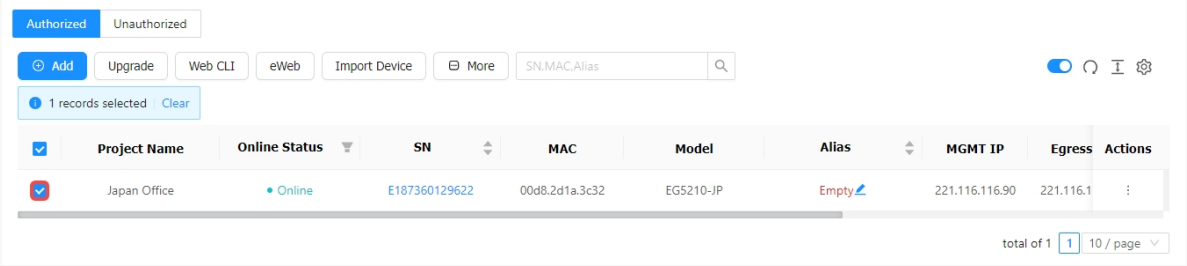
Users can create a Web-based tunnel to access the gateway's eWeb system to achieve more monitoring and management functions.

Note

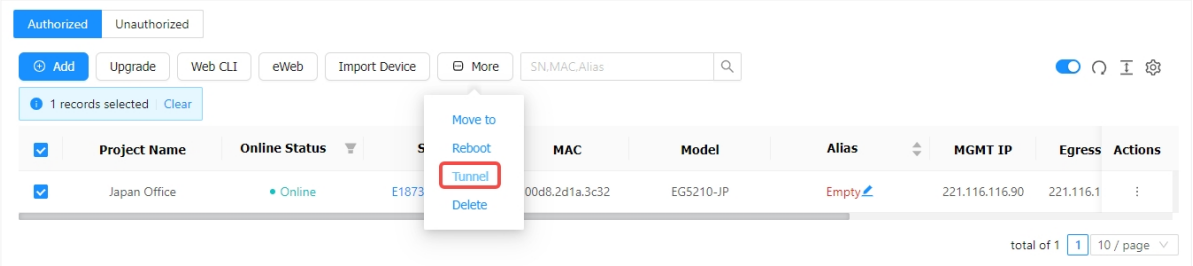
If there is any security system present in the network, such as a firewall, traffic to destination TCP ports 10000-12000 should be allowed.

Follow the steps below to create a tunnel:

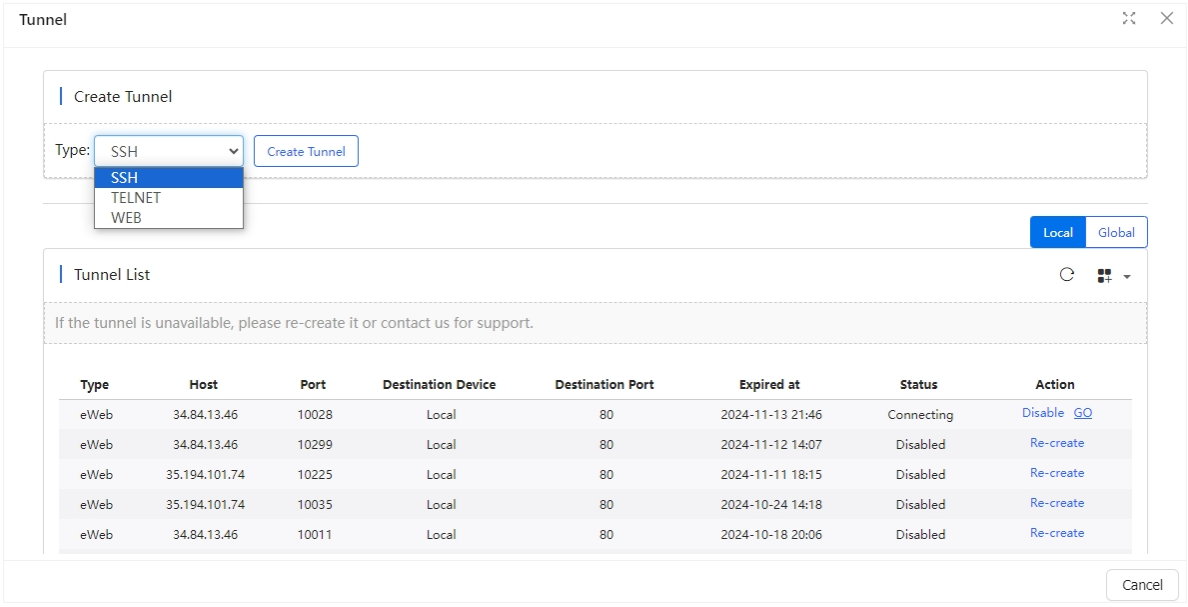
1 Select a gateway.



2 Click **More,** and then click **Tunnel**.



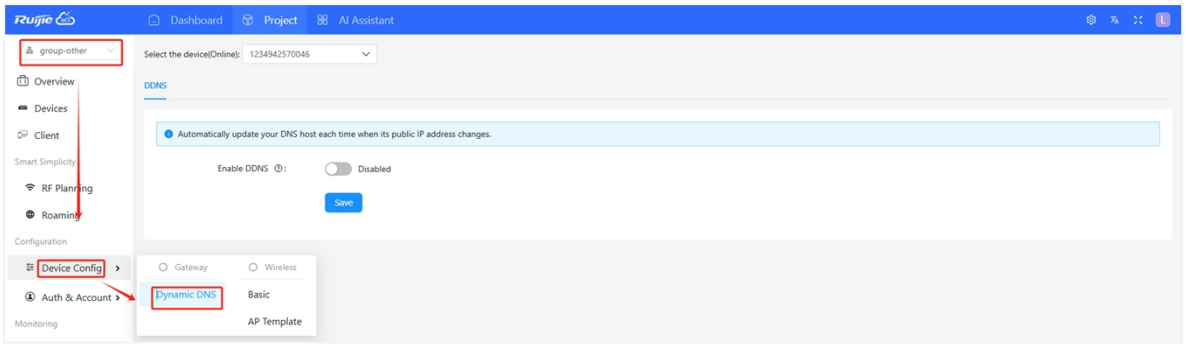
3 Select a tunnel type, and click **Create Tunnel**. Different products support different tunnel types.



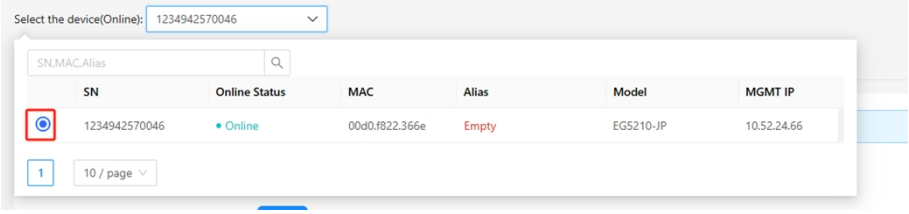
4.3.9 Configuring Dynamic DNS

To configure the dynamic DNS:

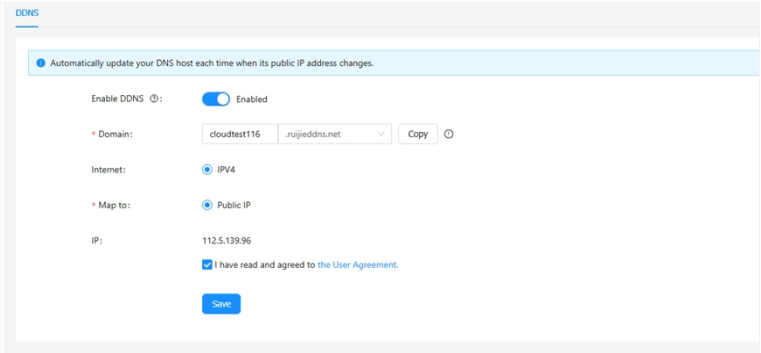
1 Select a project, and navigate to **Device Config** > **Dynamic DNS** to go to the configuration page.



2 Select an online device.



3 Configuring the DDNS information, and then click **Save**.



Items	Description
Enable DDNS	Whether to enable DDNS.
Domain	Specify a domain name address (the length of an address ranges from 1 to 32 character.)
Internet	The IPv4 is set by default.
Map to	Mapped to a public IP address by default.
IP	Displays the public IP address.

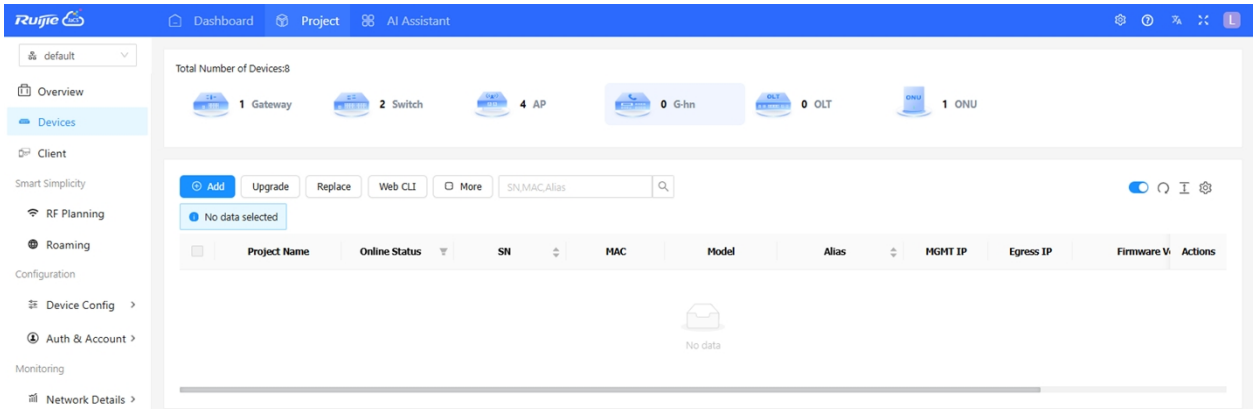
4.4 G.hn Devices

This section gives a brief introduction to the management interface and operation steps of the G.hn device RG-HS2310-16GH2GT1XS on the JaCS, including:

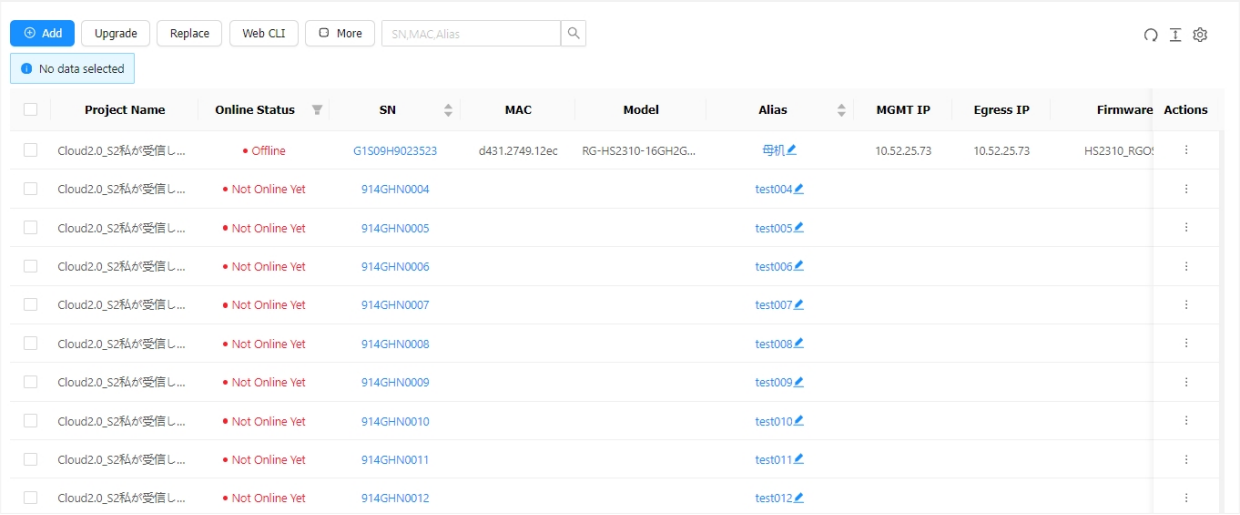
- G.hn Management Interface: Introduce the G.hn management interface on the JaCS.
- Basic Operation: Introduce the basic operations for managing the G.hn device.

4.4.1 G.hn Management Interface

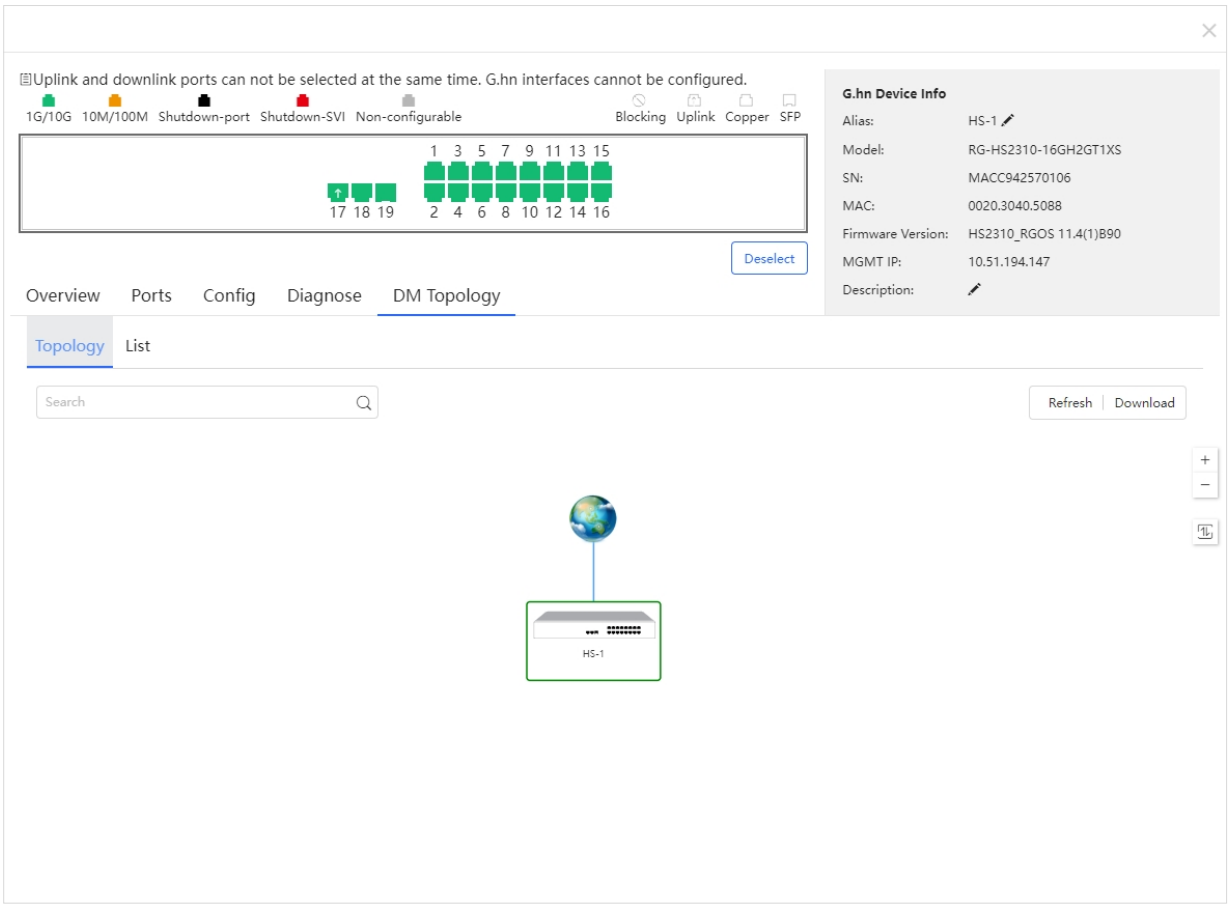
Navigate to **Project** > **G.hn** to enter the G.hn device management interface. The G.hn device list is the same as the switch list, please refer to 4.2.1 Switch Management Interface .



Click the **SN** in a G.hn device list to go to its detailed information interface. The details interface of a G.hn device is similar to that of a switch. For details, see Section 4.2.1. Only the **DM topology** tab is introduced here.



DM Topology tab displays the topology information of the main telephone line unit (RG- HS2310-16GH2GT1XS) and the child telephone line unit (RG-HA3515-DG).



4.4.2 Basic Operations

The operations for G.hn devices, such as device addition, device deletion, configuration replacement, device restart, device movement, and WEB CLI, are similar to switch operations. Please refer to operations introduced in the Section 4.2 Switch.

4.5 OLT

This section gives a brief introduction to the management interface and operation steps of OLT (Optical Line Terminal) on the JaCS, including:

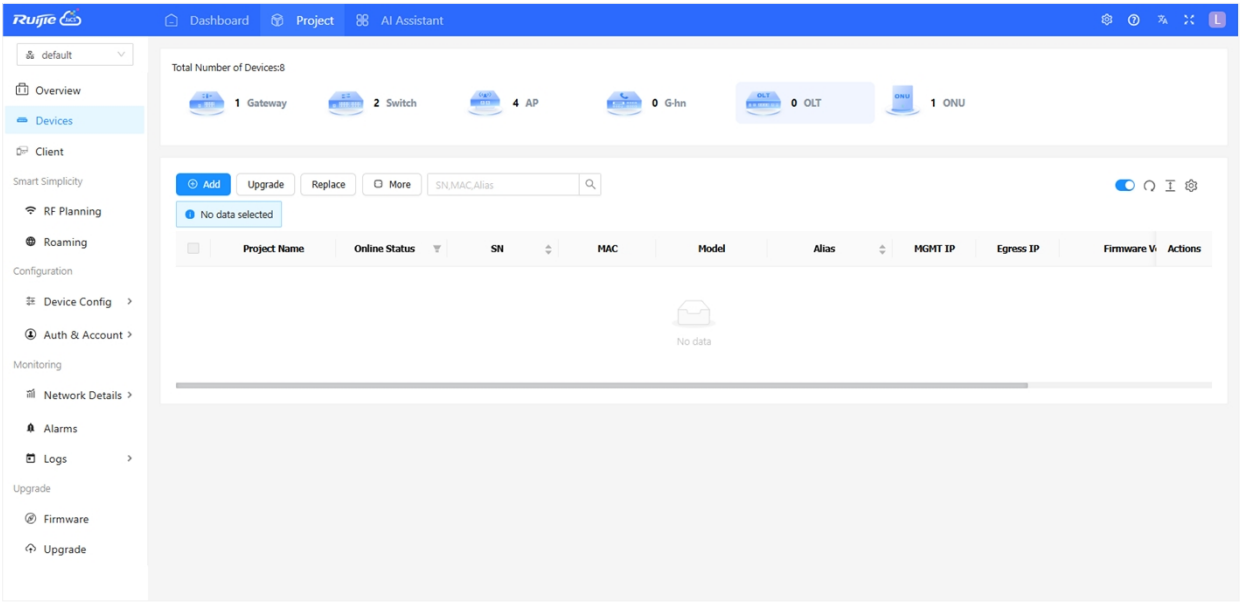
- OLT Management Interface: Introduces the OLT management interface.
- Adding OLTs: Introduces how to add or batch add OLTs to an existing project.
- Deleting OLTs: Introduces how to delete or batch delete the OLT(s) from a project.
- Moving OLTs: Introduces how to move the OLT(s) to another project.
- Upgrading OLTs: Introduces how to remotely upgrade the OLT(s) through the JaCS.
- Restarting OLTs: Introduces how to remotely restart an online OLT through the JaCS.
- Configuration Replacement: Introduces how to synchronize the configuration of an imported OLT to a new one.
- Creating a Tunnel: Introduces how to create a tunnel.

Note

Now, the supported OLT is RG-MT3002.

4.5.1 OLT Management Interface

Click **Project** > **OLT** to enter the OLT management interface. Click the **SN** of an OLT in the list to view its detailed information.

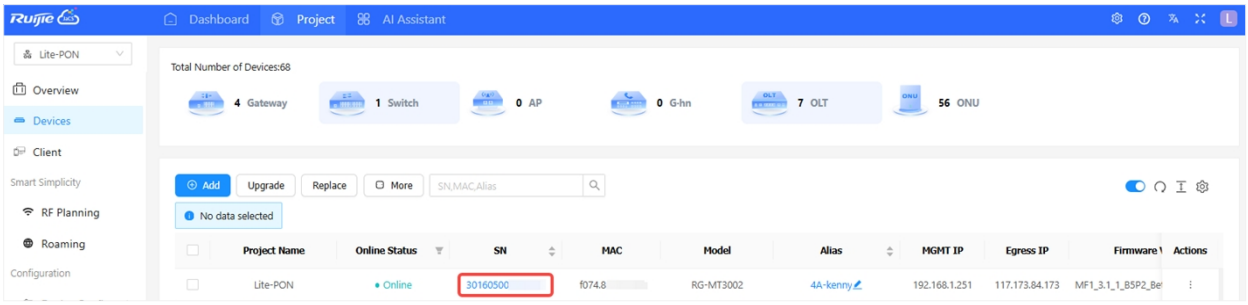


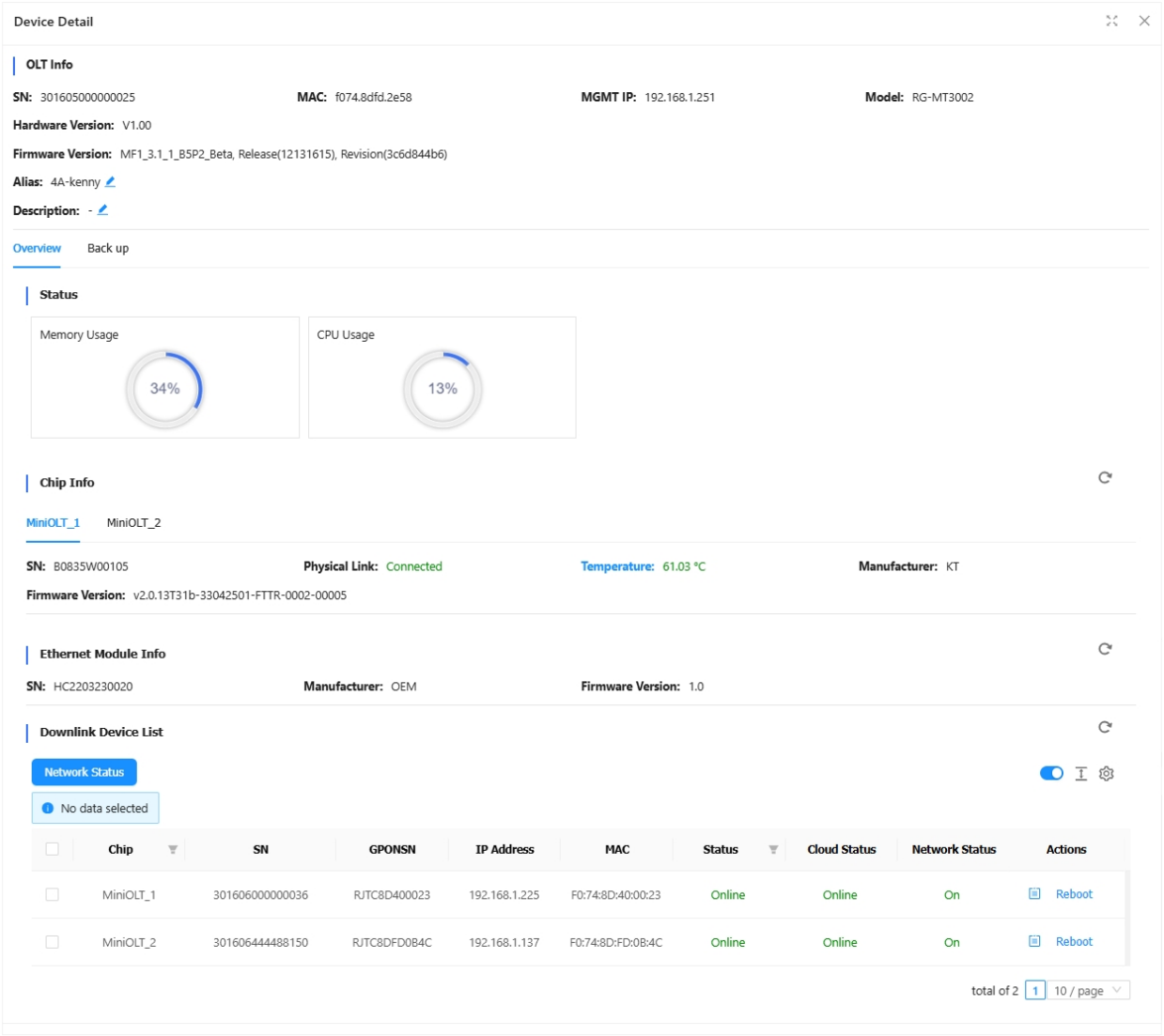
Items	Description
Project Name	Displays the name of the project where the OLT is located.
Online Status	Displays the online status of the OLT. The online status of the device includes: Online/Offline/Not Online Yet. Click the filter icon to filter the OLTs by online status.
SN	Displays the SNs of OLTs. Click the SN of an OLT to view its details information.
MAC	Displays MAC addresses of OLTs.
Model	Displays OLT models.

Alias	Displays the aliases of OLTs.
MGMT IP	Displays the management addresses of OLTs.
Egress IP	Displays the egress IP addresses of OLTs.
Firmware Version	Displays the firmware versions of OLTs.
Last See On	Displays the last online time of OLTs.
Action	Action column. Click the **Delete** button in the **Action** column to remove the device from the project.

Button	Description
Add	Add button. Click this button to go to the adding interface.
Upgrade	Upgrade button. After selecting the device, click this button to remotely upgrade the device.
Replace	Configuration replacement Button. You can synchronize the configuration of the old device to a new device of the same model. After configuration, when the new device is online, the configuration of the old device will be sent to it automatically.
More	Click this button to display more operation buttons, including **Move to**, **Delete**, **Restart**, and **Tunnel**.
	Refresh button. Click this button manually to refresh the OLT device list.
	Automatic refresh button. When it is enabled, the OLT device list will automatically refresh once every minute.
	Row height adjustment button. Click this button to adjust the row height.
	Click this button to customize the displayed items in the OLT list.
SN,MAC,Alias	Search box. Supports searching an OLT by its MAC, SN, or alias.

Click the SN of a OLT device to go to device detail page.



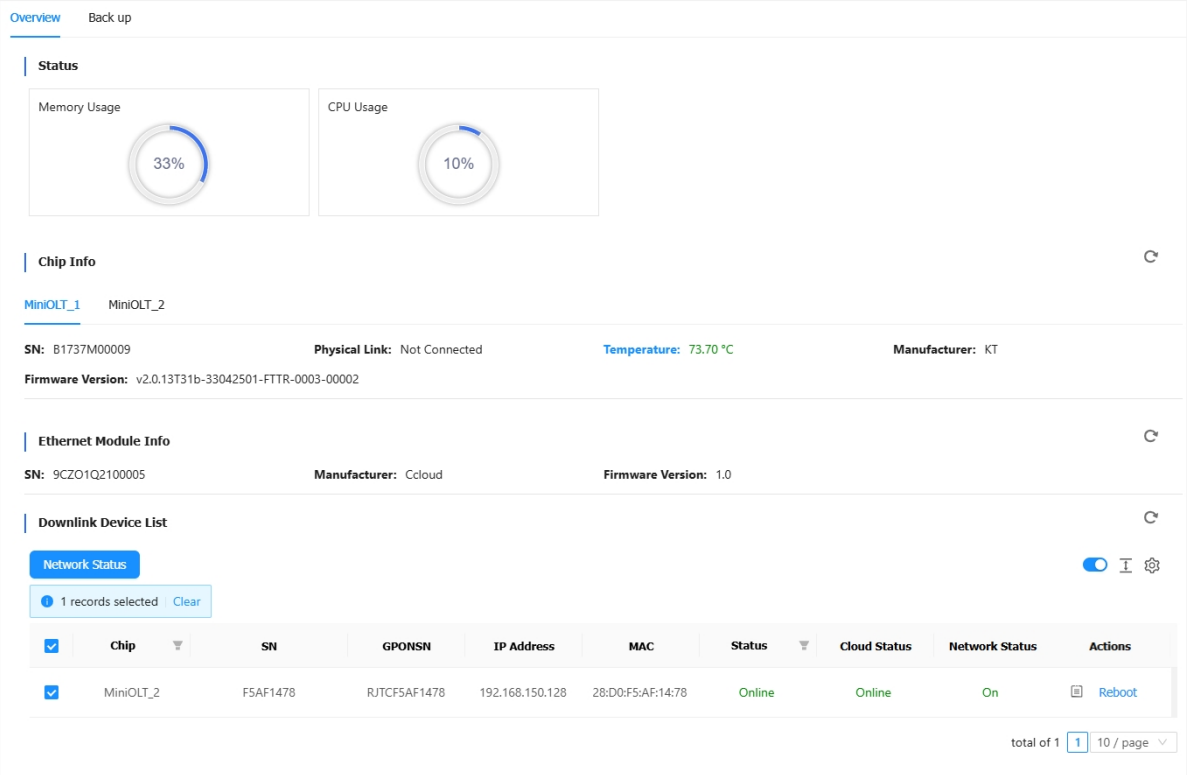


(1) OLT Information

The OLT infor displays the device's SN, MAC address, MGMT IP address, model, hardware version, firmware version, alias and description.

(2) Overview Tab

The Overview tab consists of four parts: **Status**, **Chip Information**, **Ethernet Module Information** and **Download Device List**.

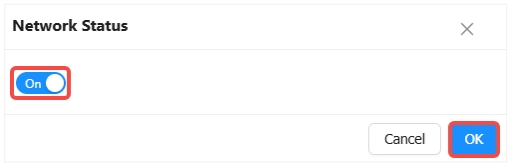


In the **Download Device List**, you can change the network status of its downlink devices.

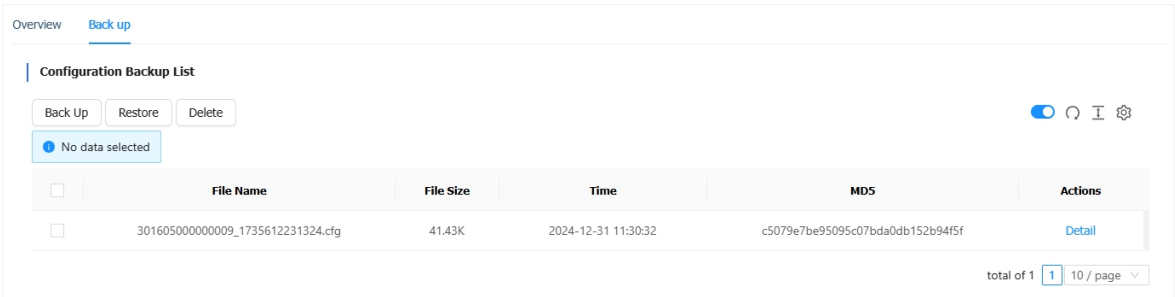
To change the network status of its downlink devices:

1 Select a downlink device, and then click **Network Status**.

2 Change the status and click **OK**.



(3) Back up Tab



Button	Description
Back Up	Click this button to back up the configuration of the OLT device.
Restore	Select a backup configuration file and then click this button to restore the device to the selected configuration backuped.
Delete	Select a configuration file and then click **Delete** to delete it.
Details	Click **Details** in the **Action** column to view the details of the configuration.

4.5.2 Adding OLTs

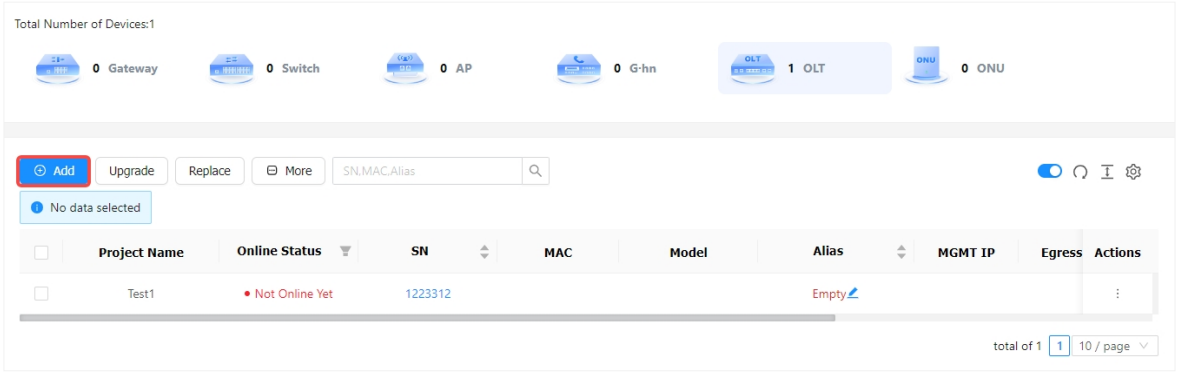
JaCS provides two ways to add optical line terminals to a specific project.

- Adding an OLT
- Adding OLT in Batches

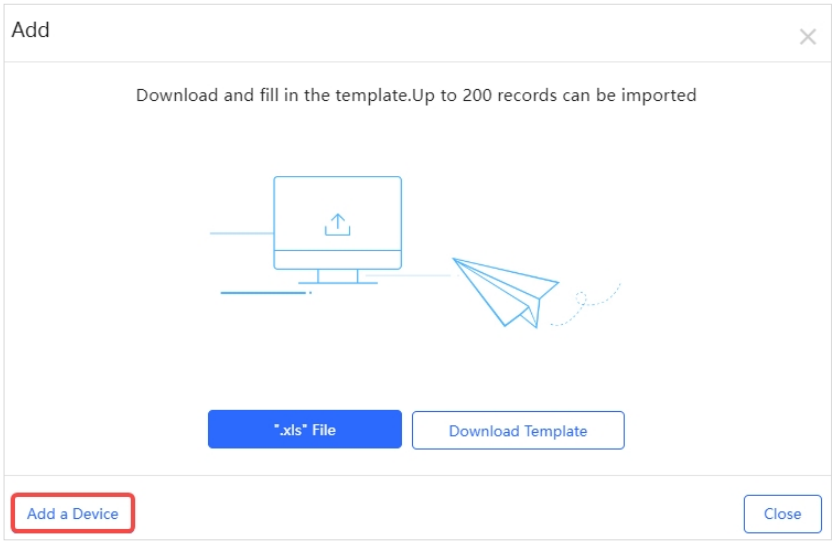
4.5.2.1 Adding an OLT

Follow the steps below to manually add an OLT to an existing project. This method is suitable for adding a small number of OLTs:

1 In the OLT management interface, click **+ Add**.

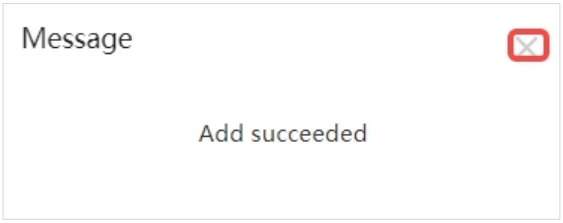


2 Click **Add a Device**.



3 Enter the SN (required) and Alias (optional). The length of the SN should be between 6 and 20 characters, and the length of an alias cannot exceed 64 characters. Click to delete the filled SN, and click **+** to add more SNs.

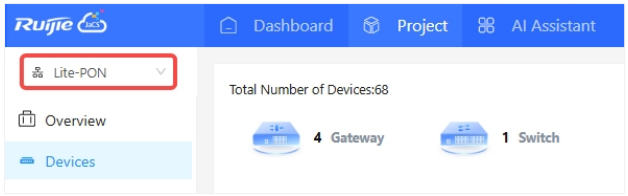
4 After filling in the information, click **OK**. When the "Add succeeded" prompt appears, click **X** to close the prompt box. The added device will be displayed in the OLT list.



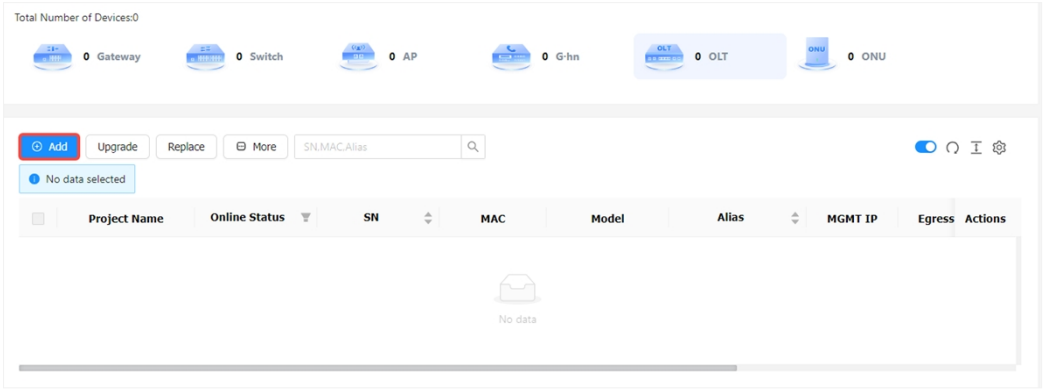
4.5.2.2 Adding OLTs in Batches

Follow the steps below to add OLT devices to a specified project in batches.

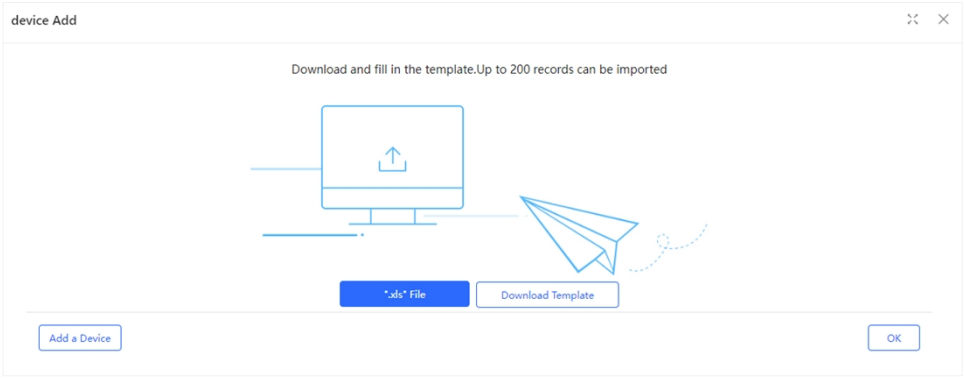
1 Select the project.



2 Click **Add**.



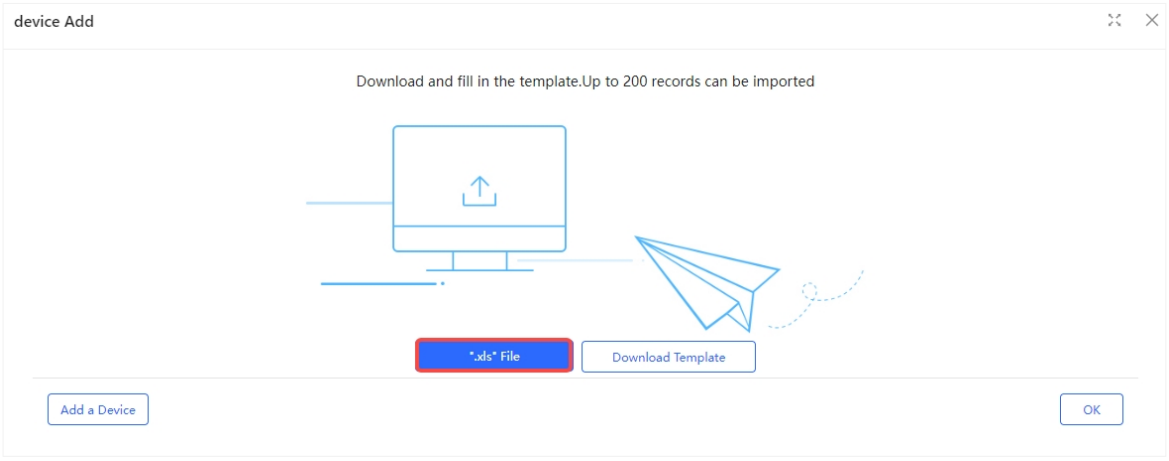
3 Click **Download Template** to download the template.

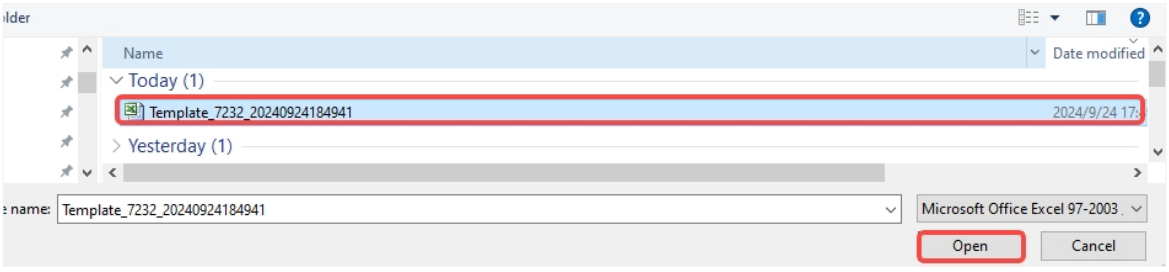


4 Fill in the template. SN is required, while the alias is optional. Up to 200 devices can be imported each time.

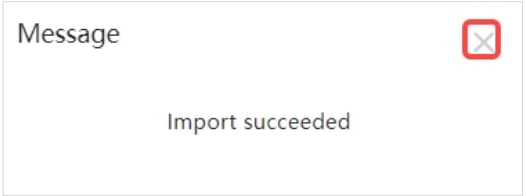
	A	B
1	SN	Alias
2		
3		

5 Click **".xls" File** to upload the completed document.





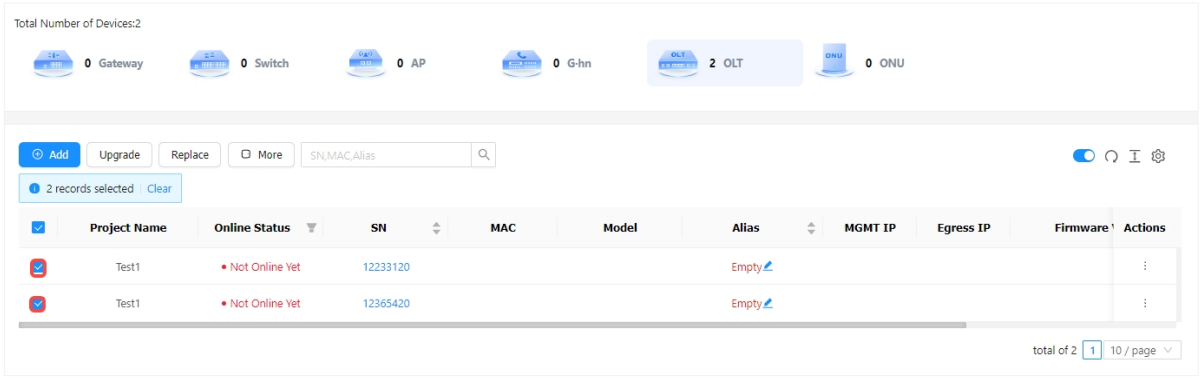
6 When the "Import succeeded" prompt appears, click **X** to close the prompt box. The imported devices will be displayed in the OLT list.



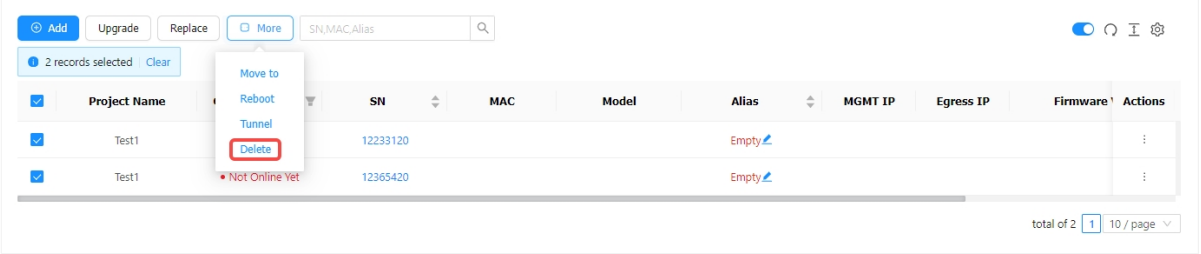
4.5.3 Deleting OLTs

Follow the steps below to delete the OLT(s) from an existing project.

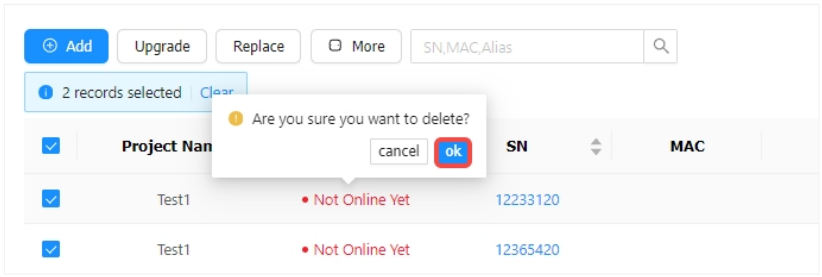
1 Select the OLTs to be deleted.



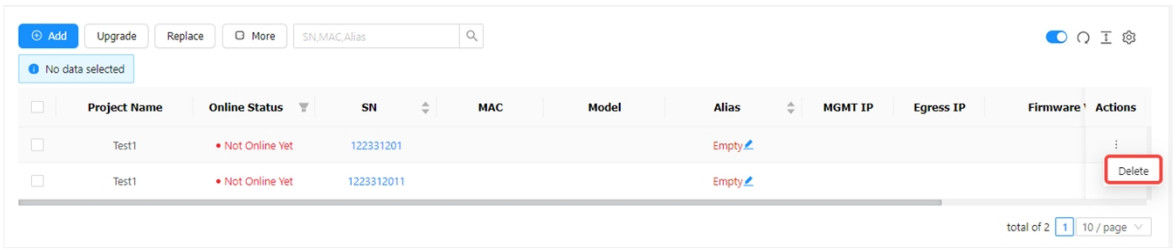
2 Click **More**, and then click **Delete**.



3 Click **OK** in the operation confirmation box. When the "Succeeded" prompt appears, the operation is completed.



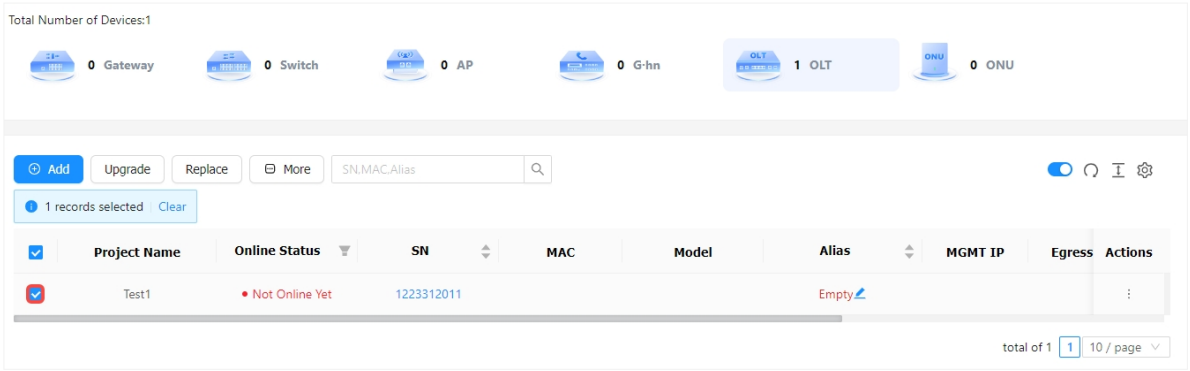
In addition to the above deletion method, users can also hover the mouse over the ⋮ icon in the **Action** column of the OLT to be deleted, and then click **Delete** to delete the device.



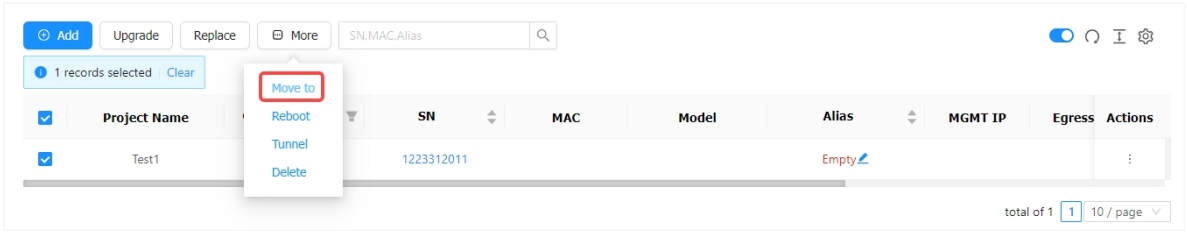
4.5.4 Moving OLTs

Follow the steps below to moving the OLT(s) to another project.

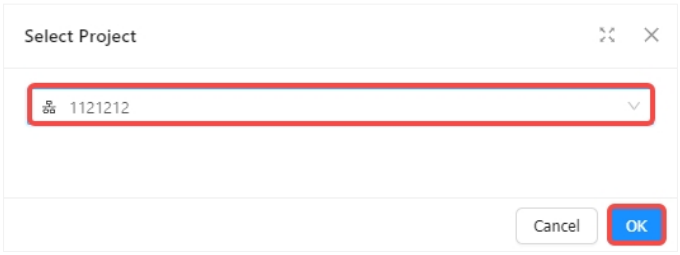
1 Select the OLT that needs to be moved.



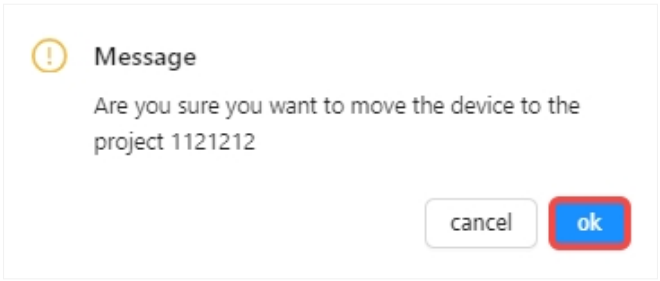
2 Click **More**, and then click **Move to**.



3 Select a new project and click **OK**.



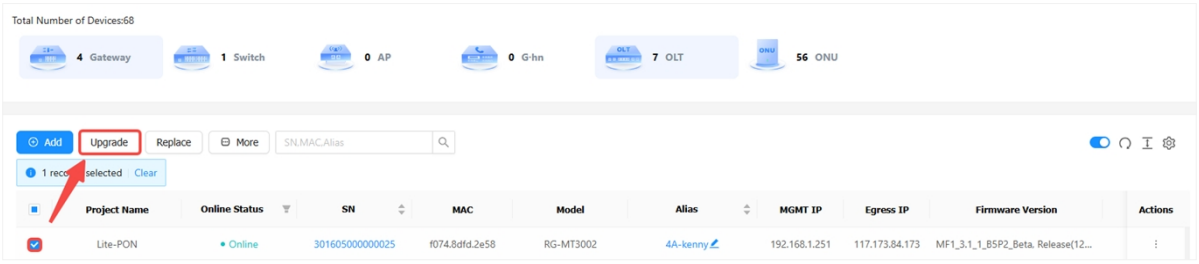
4 When the operation confirmation box appears, click **OK**.



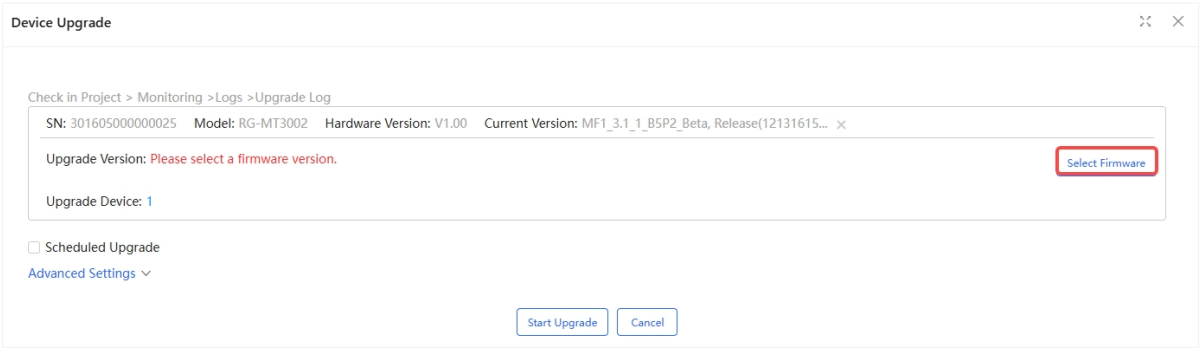
4.5.5 Upgrading OLTs

Follow the steps below to remotely upgrade the OLT(s) via the JaCS.

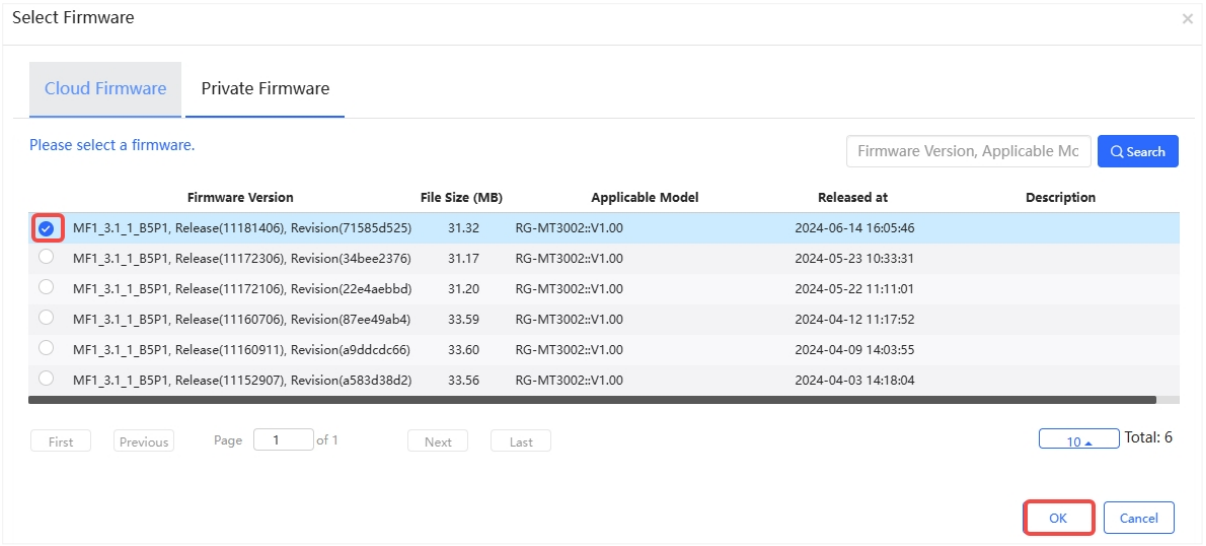
1 Select the device to be upgraded, and then click **Upgrade**.



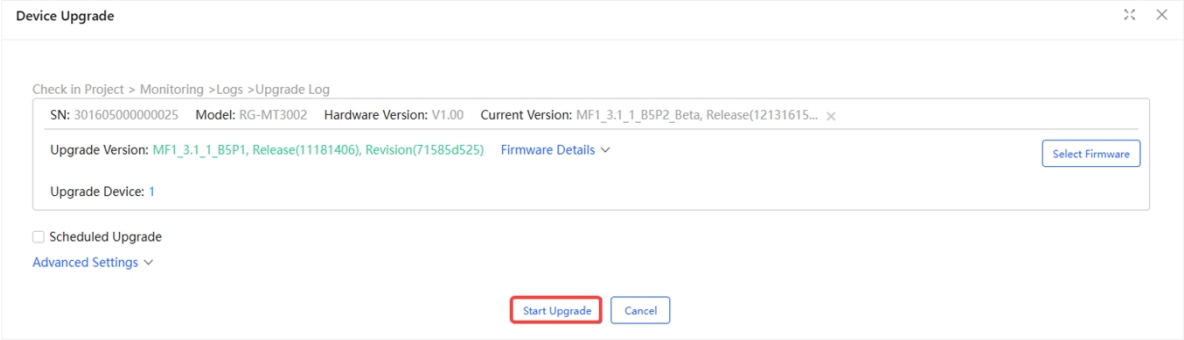
2 Click **Select Firmware** to select a firmware version.



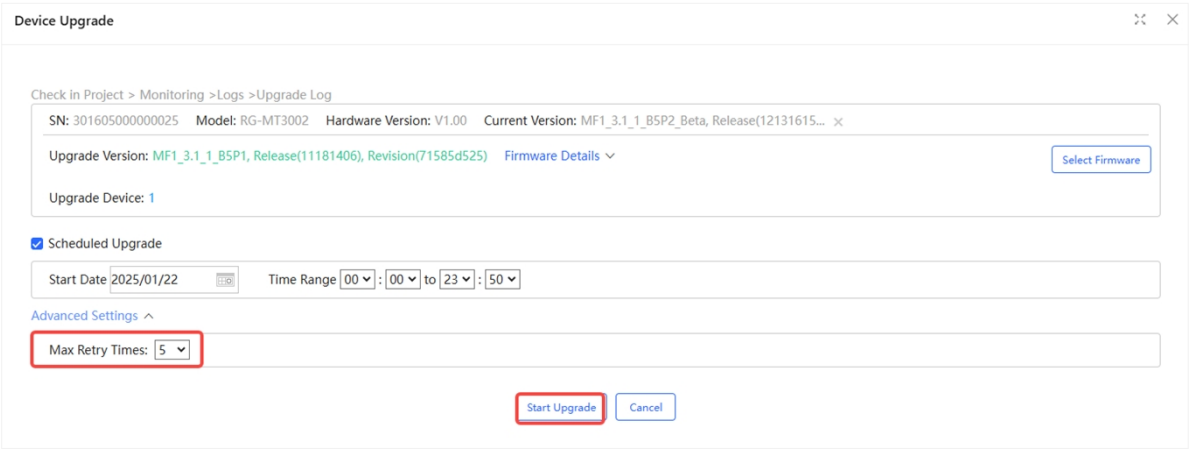
3 After selecting the firmware version, click **OK**.



4 Click **Start Upgrade** to create an upgrade task.



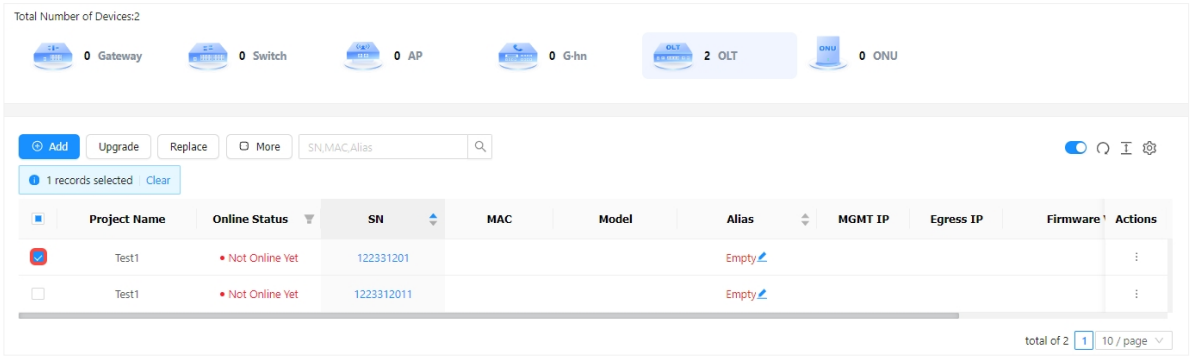
If you need to upgrade the device at a specific time, you need to check **Scheduled Upgrade**, and then set the upgrade time. After that, click **Start Upgrade**. The default number of upgrade attempts is 5.



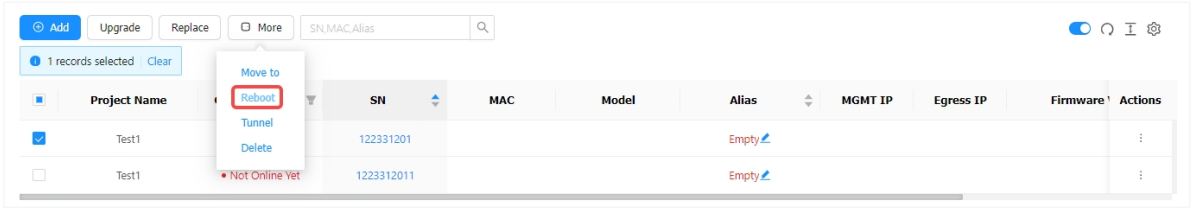
4.5.6 Restarting OLTs

Follow the steps below to remotely restart the OLT through the JaCS.

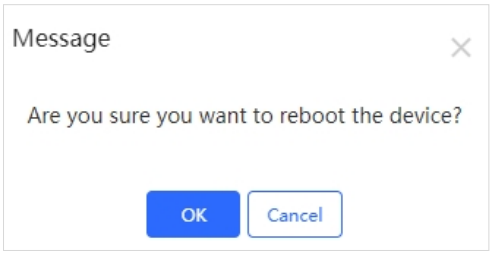
1 Select the OLT to be restarted.



2 Click **More**, and select **Reboot**.



3 Click **OK** in the operation confirmation box, and wait for the device to restart.



4.5.7 Configuration Replacement

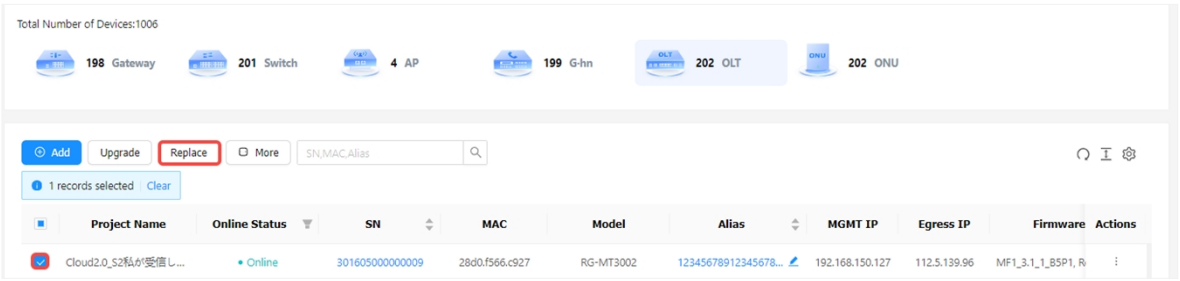
The configuration replacement function can synchronize the configuration of an old or faulty device to a new device of the same model. After the configuration replacement task is complete, Ruijie JaCS will send the configuration of the old device to the new one when it goes online. In this way, users do not need to manually configure the new device again, helping improving operation and maintenance efficiency.

Note

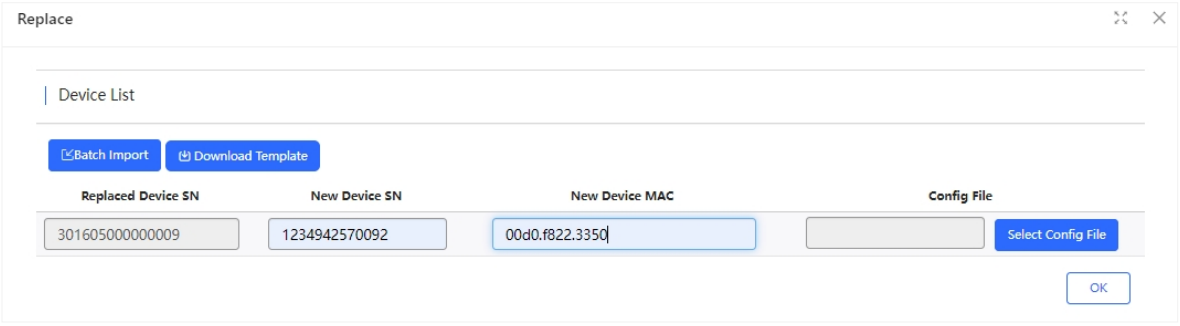
The configuration replacement is only applicable to the OLTs of the same model.

The specific steps are as follows:

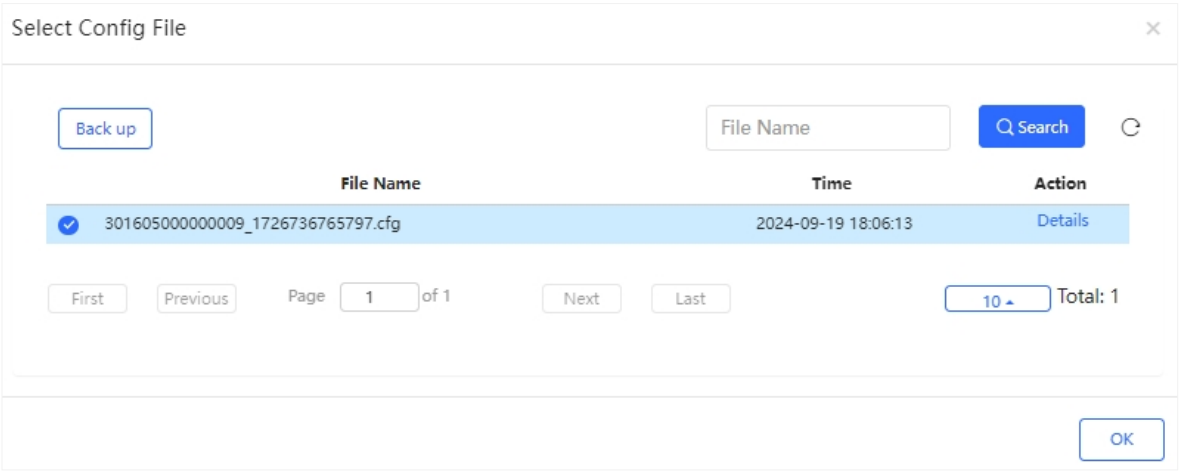
1 Select an existing device and click **Replace**.



2 Enter the SN and MAC address of the new device. Please make sure that the SN and MAC of the new device match each other.

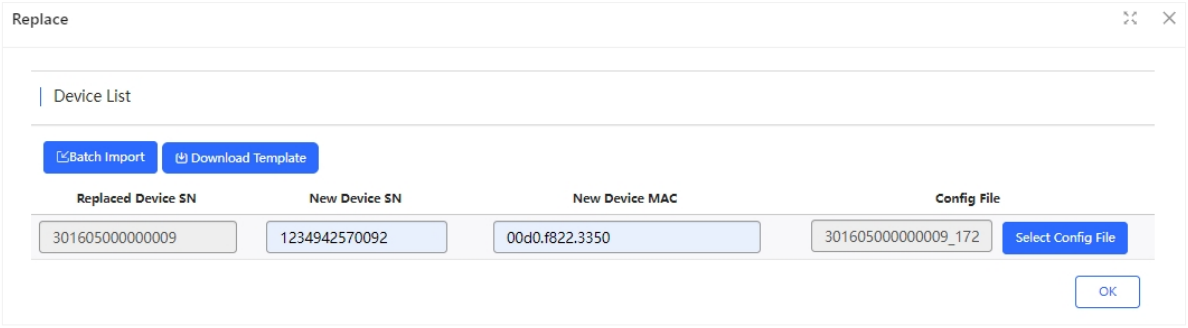


3 Click **Select Config File** and select the configuration file of the existing device. After selecting, click **OK**.

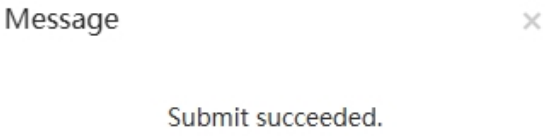


In the **Select Config File** interface, click **Backup** to back up the current device configuration.

4 After selecting the configuration file, click **OK**.

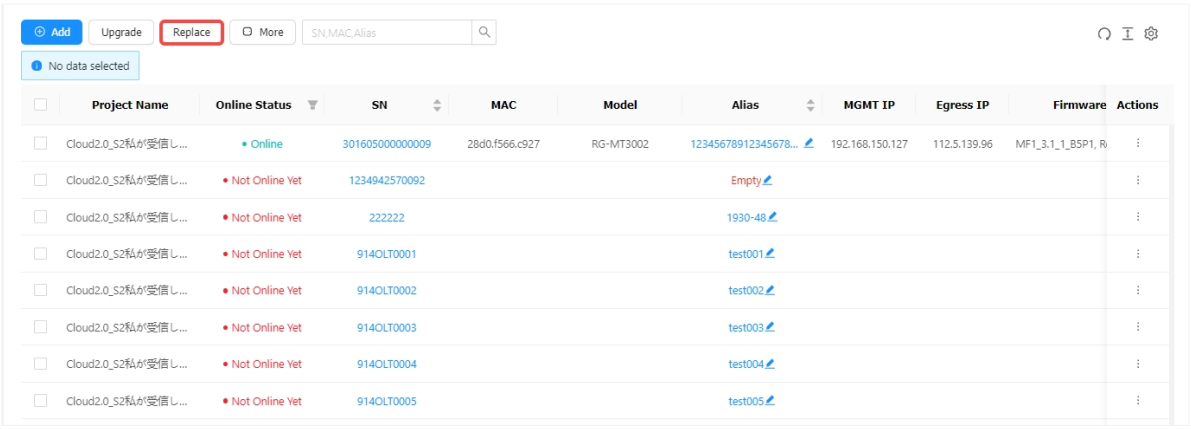


5 After the prompt message appears, click **X** to complete the operation.

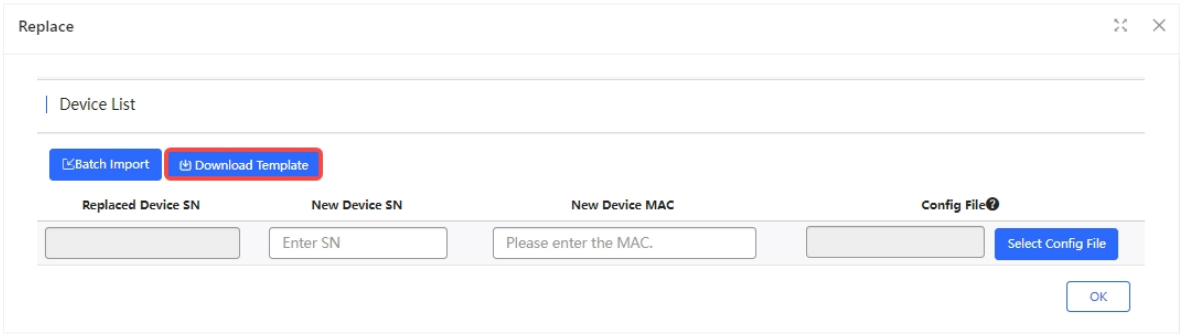


To replace the configuration of OLTs in batches:

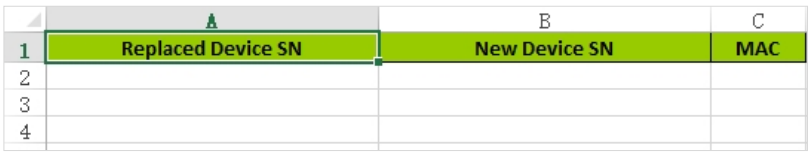
1 Click **Replace**.



2 Click **Download Template** to download the template.

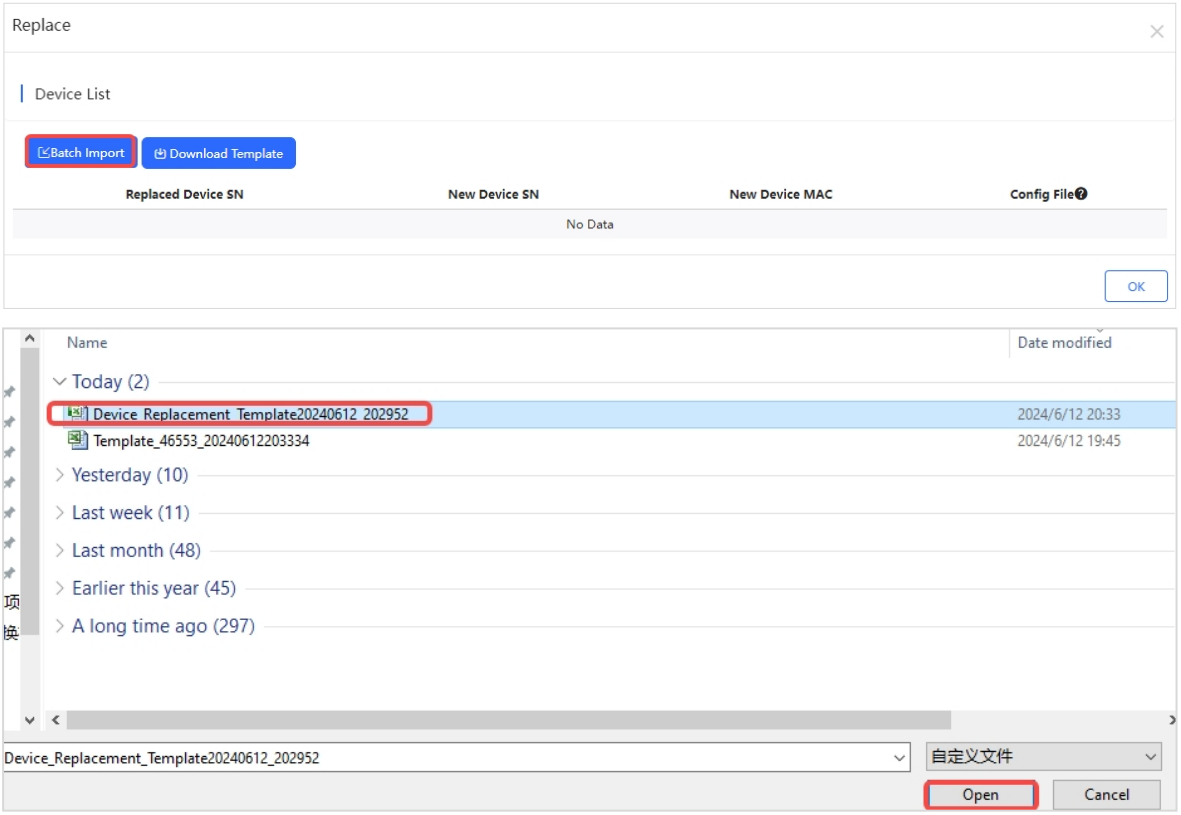


3 Fill in the template. Up to 200 devices can be imported each time.

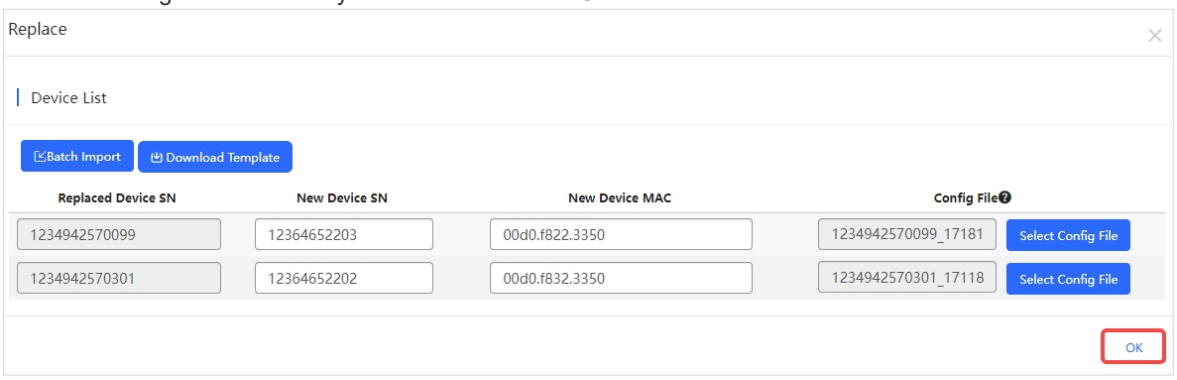


Items	Description
Replaced Device SN	Enter the SN of the existing device.
New Device SN	Enter the SN of the new device.
M AC	Enter the MAC address of the new device.

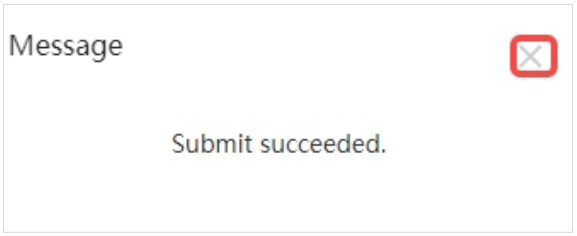
4 Click **Batch Import** to import the filled template.



5 Select the configuration files for your devices and click **OK**.



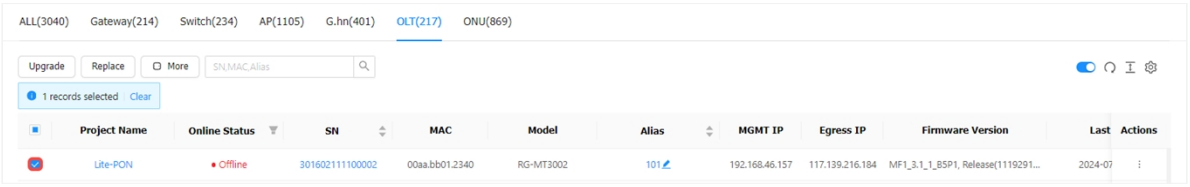
6 After the "Submit succeeded " prompt appears, click **X** to close the prompt box.



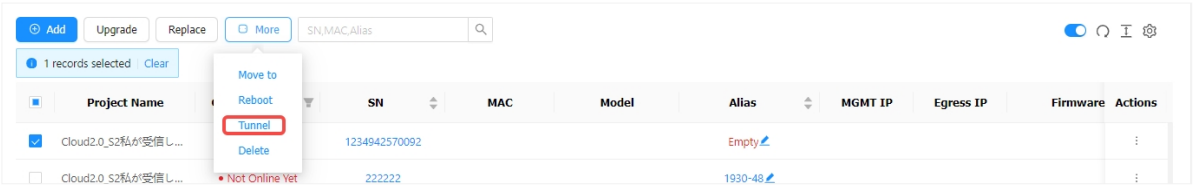
4.5.8 Creating a Tunnel

Follow the steps below to create a tunnel. Before creating a tunnel, make sure the device is online:

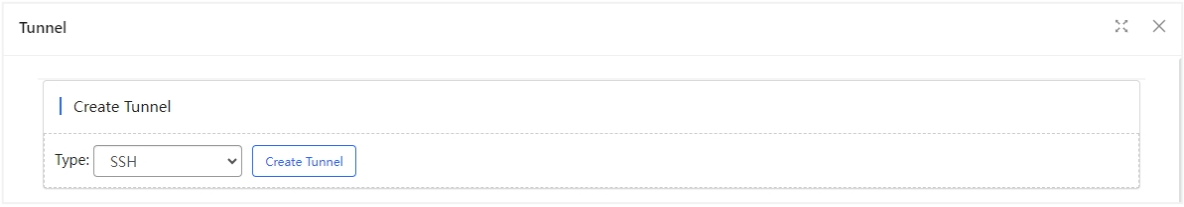
1 Select the device.



2 Click **More**, and then click **Tunnel**.



3 Select a tunnel type and click **Create Tunnel**.



4.6 ONU

This section gives a brief introduction to the management interface and operation steps of ONU (Optical Network Unit) on the JaCS, including:

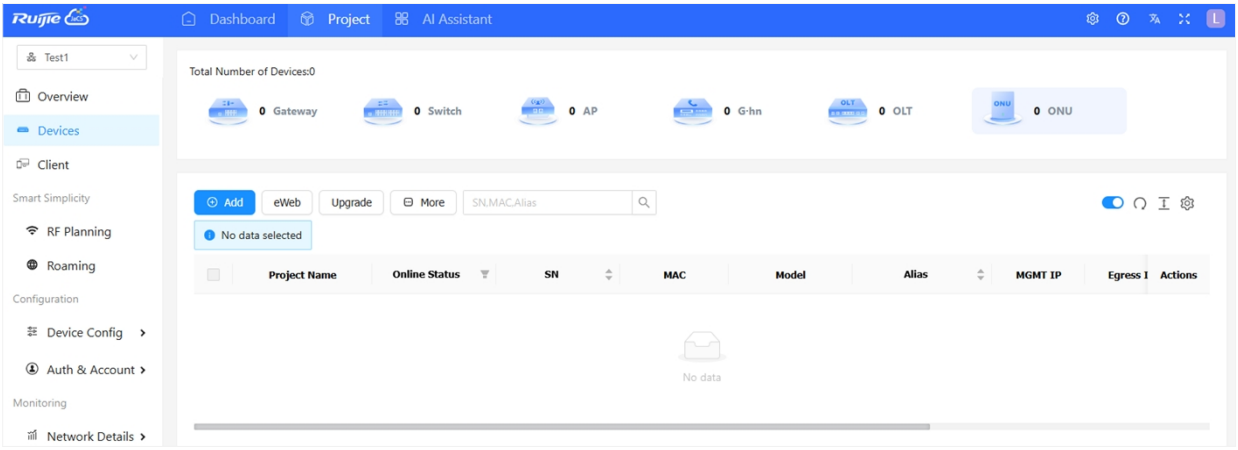
- ONU Management Interface: Introduces the ONU management interface of the JaCS.
- Adding ONUs: Introduces how to add or batch add the ONU(s) to an existing project.
- Deleting ONUs: Introduces how to delete or batch delete the ONU(s) from an existing project.
- Moving ONUs: Introduces how to move the ONU(s) to another project.
- Upgrading ONUs : Introduces how to remotely upgrade the ONU(s) through the JaCS.
- Restarting ONUs: Introduces how to remotely restart the online ONU(s) through the JaCS.

Note

Currently, the supported ONU model is RG-MU3064.

4.6.1 ONU Management Interface

Click **Project** > **ONU** to go to the ONU management interface. Click the **SN** of an ONU, you can view its detailed information.

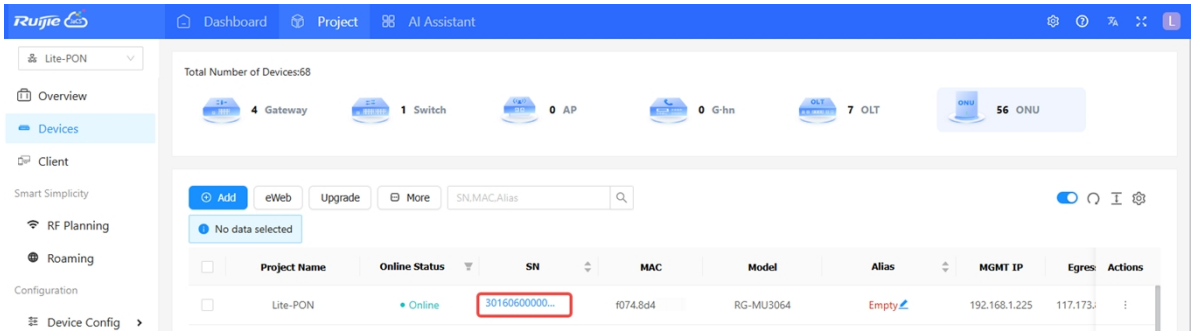


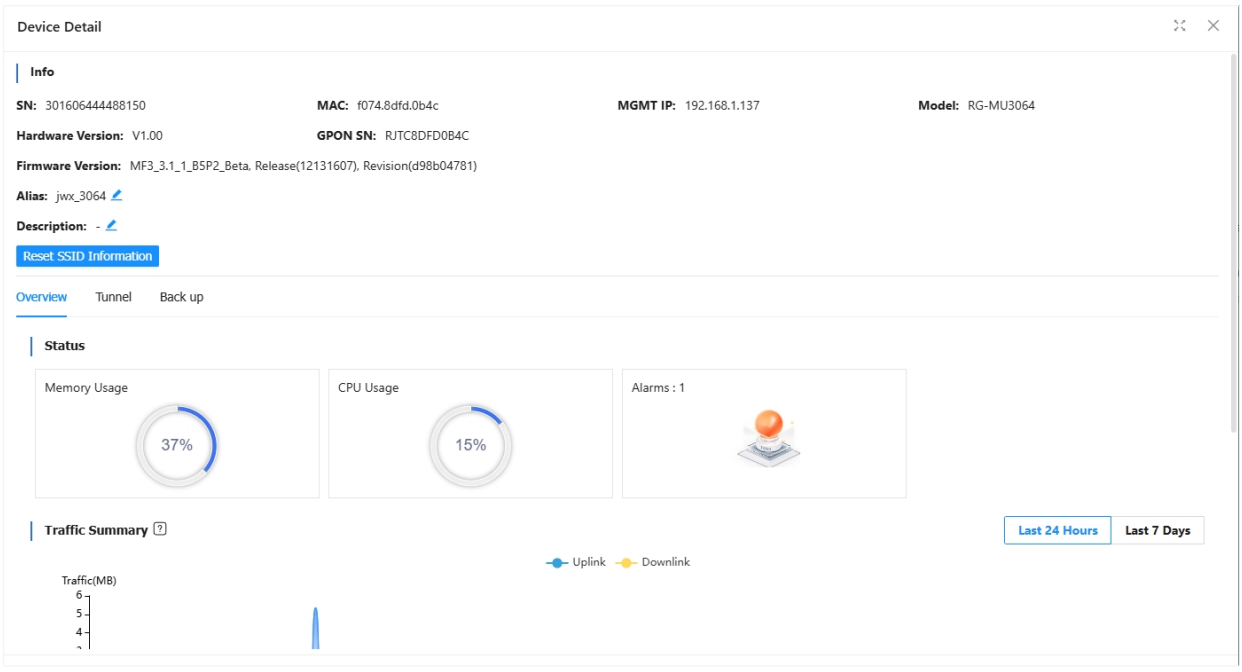
Items	Description
Project Name	Displays the name of the project where the ONU is located.
Online Status	Displays the online status of the ONU. The online status of the device includes: Online/Offline/Not Online Yet. Click the filter icon to filter devices by online status.
SN	Displays the SN of the device. Click the SN number of an ONU to view its details.
MAC	Displays the MAC addresses of ONUs.
Model	Displays ONU models.
Alias	Displays the aliases of ONUs.
MGMT IP	Displays the management addresses of ONUs.
Egress IP	Displays the egress IP addresses of ONUs.
Firmware Version	Displays the firmware version information of the ONU.
Last See On	Displays the last online time of the ONU.

Actions	Hover the cursor over the ⋮ in the **Action** column. When the **Delete** button appears, click it to remove the device from the project.

Button	Description
Add	Add button. Click this button to enter the adding interface.
eWeb	eWeb button. Select an ONU, and click this button to can access its eWeb.
Upgrade	Upgrade button. After selecting the ONU, click this button to remotely upgrade the device.
More	Click this button to display more operation buttons, including: **Move to**, **Delete**, and **Reboot**.
	Refresh button. Click this button manually to refresh the ONU list.
	Automatic refresh switch button. The automatic refresh function is enabled by default. When it is enabled, the ONU device list will automatically refresh once every minute.
	Row height adjustment button. Click this button to adjust the row height.
	Click this button to customize the displayed items in the ONU list.
SN,MAC,Alias	Search box. Supports searching an ONU by its SN, MAC, or alias.

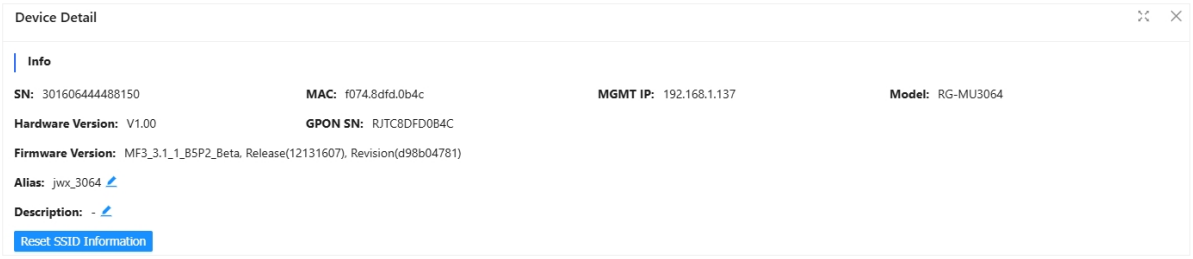
Click the SN of a ONU device to go to the **Device Detail** page. The **Device Detail** page contains four parts: **Device Information**, **Overview**, **Tunnel** and **Back up**.





(1) Device Information

The device information displays the device's SN, MAC address, MGMT IP address, model, hardware version, firmware version, alias and description. To reset the device SSID, click **Reset SSID Information**.

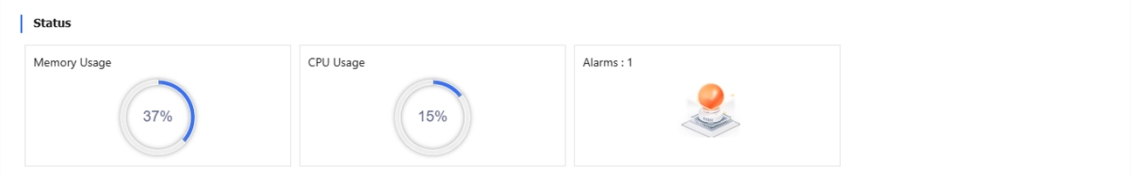


(2) Overview Tab

The Overview tab consists of three parts: **Status**, **Traffic Summary** and **SSID List**.

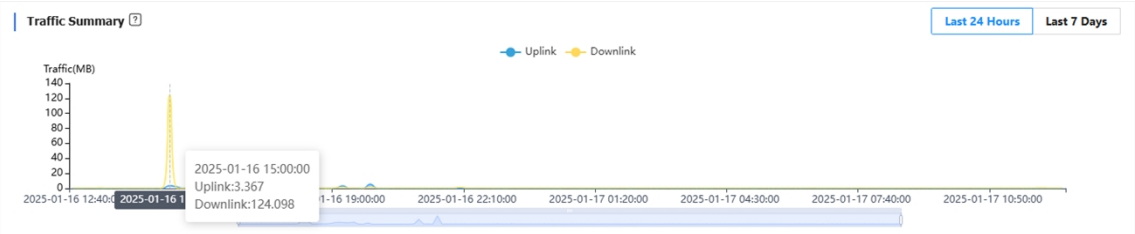
- **Status**

  Displays the memory and CPU usages and the number of alarms.



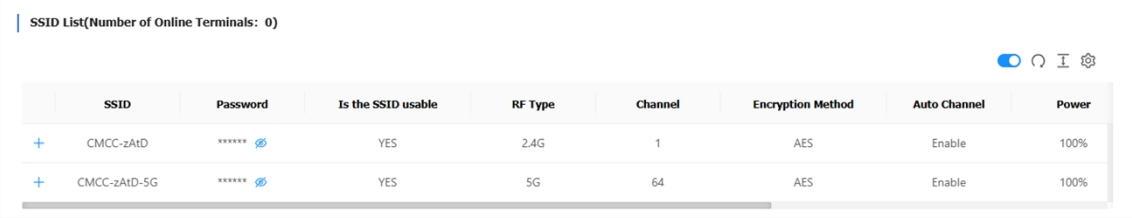
- **Traffic Summary**

  Displays the traffic statistics in the last 24 hours or 7 days. Hover your cursor at a time to check its uplink and downlink traffic.



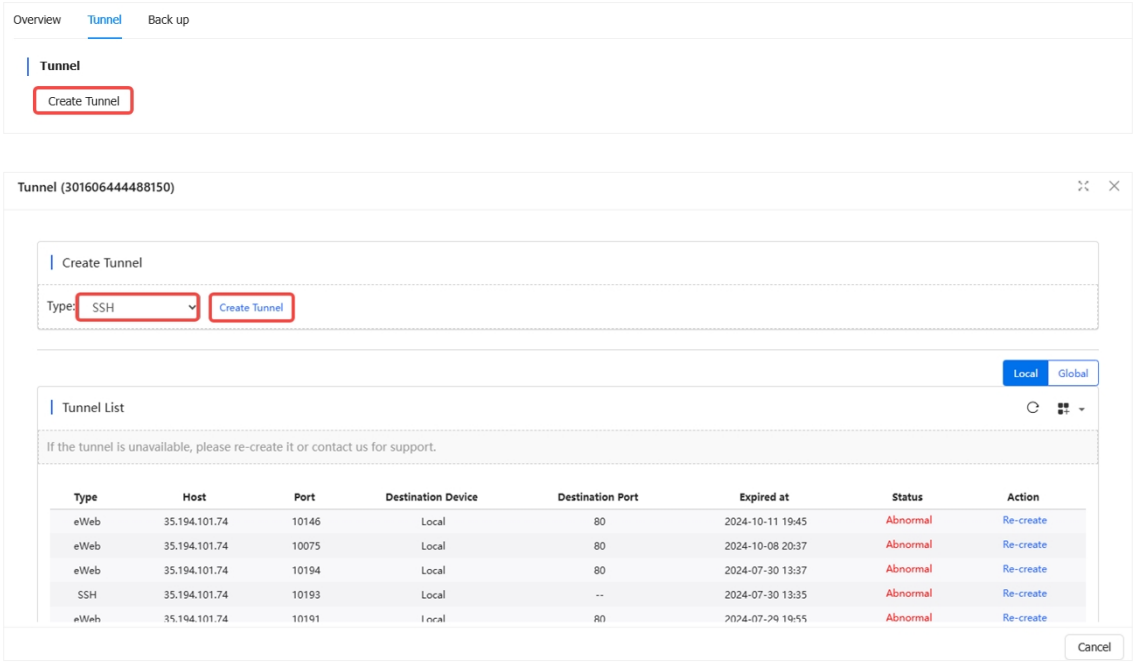
- **SSID List**

  Displays the SSID information of the device.

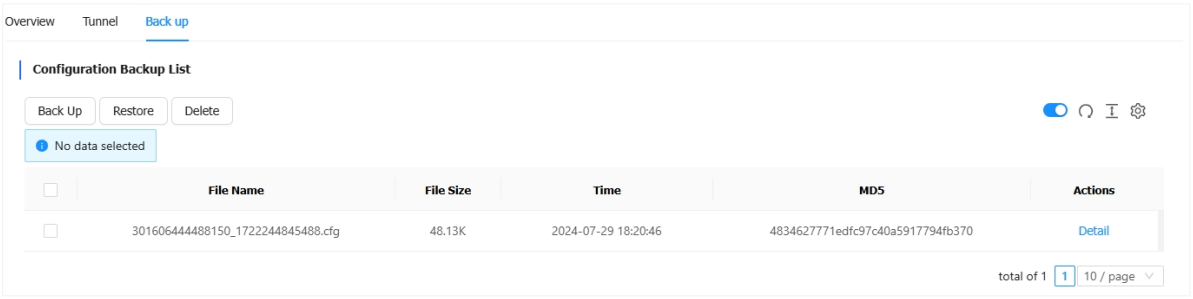


- **Tunnel**

  Click **Create Tunnel** to go to the Tunnel page. Select a tunnel type and then click Create Tunnel to create a tunnel for the device.



(3) Back up Tab



Button	Description
Back Up	Click this button to back up the configuration of the OLT device.
Restore	Select a backup configuration file and then click this button to restore the device to the selected configuration backuped.
Delete	Select a configuration file and then click **Delete** to delete it.
Details	Click **Details** in the **Action** column to view the details of the configuration.

4.6.2 Add ONUs

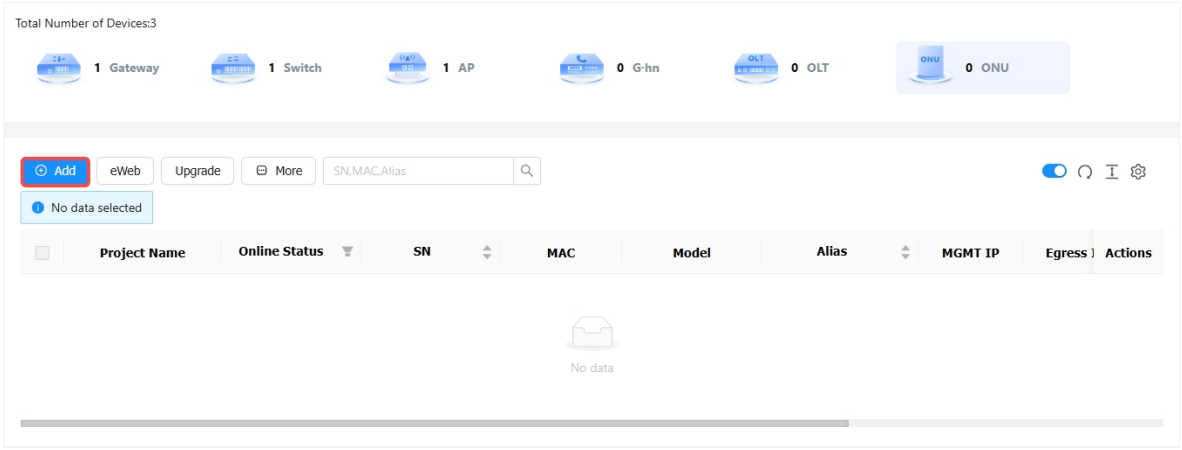
JaCS provides two ways to add optical network units to a specific project.

- Adding an ONU
- Adding ONUs in Batches

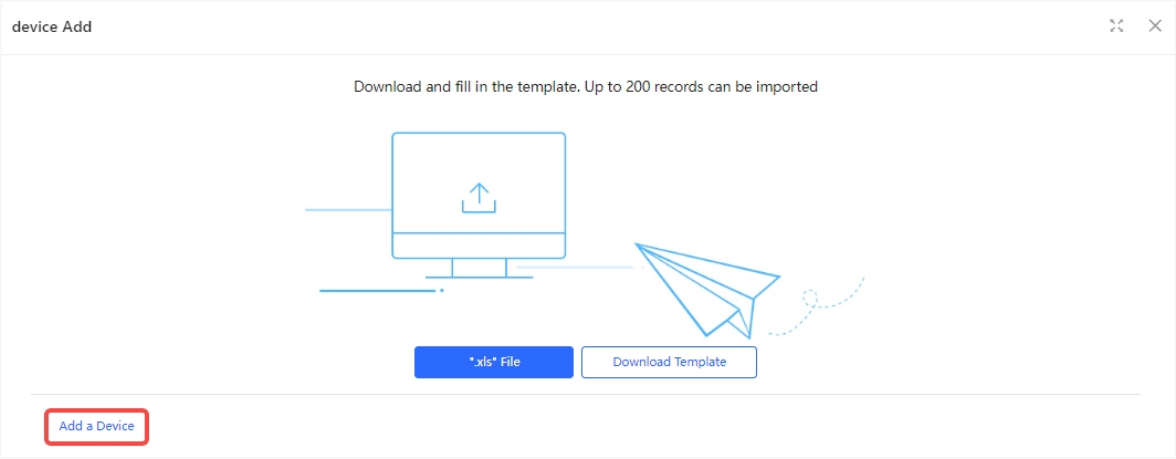
4.6.2.1 Adding an ONU

Follow the steps below to add an ONU. This method is suitable to add a small number of ONUs.

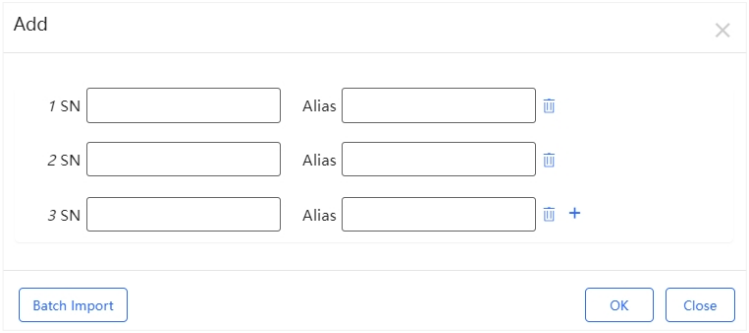
1 Click **Add** in the ONU management interface.



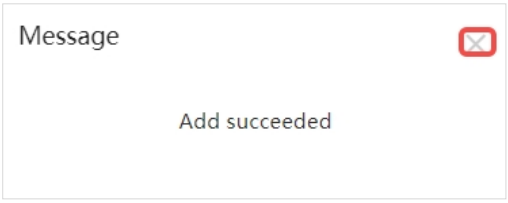
2 Click **Add a Device**.



3 Enter the device's SN (required) and Alias (optional). The length of a SN should be between 6 and 20 characters, and the length of an alias cannot exceed 64 characters. Click to delete the filled SN, and click + to add more SNs .



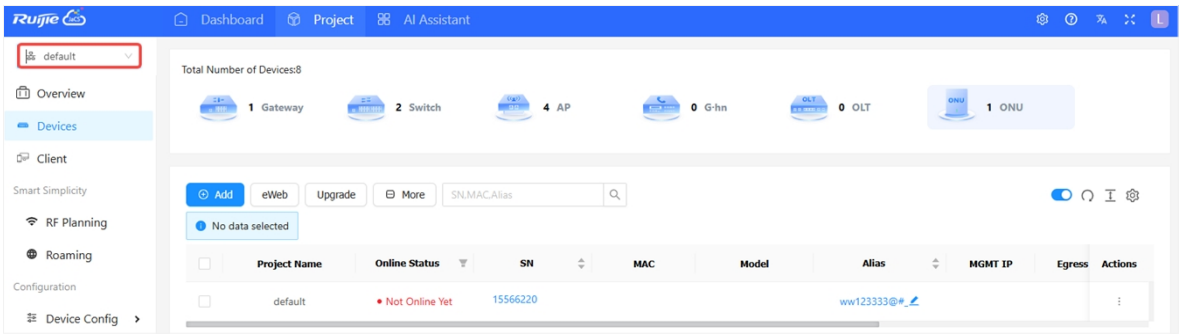
4 After filling in the information, click **OK**. When the "Add succeeded" prompt appears, click **X** to close the prompt box. The added device will be displayed in the ONU list.



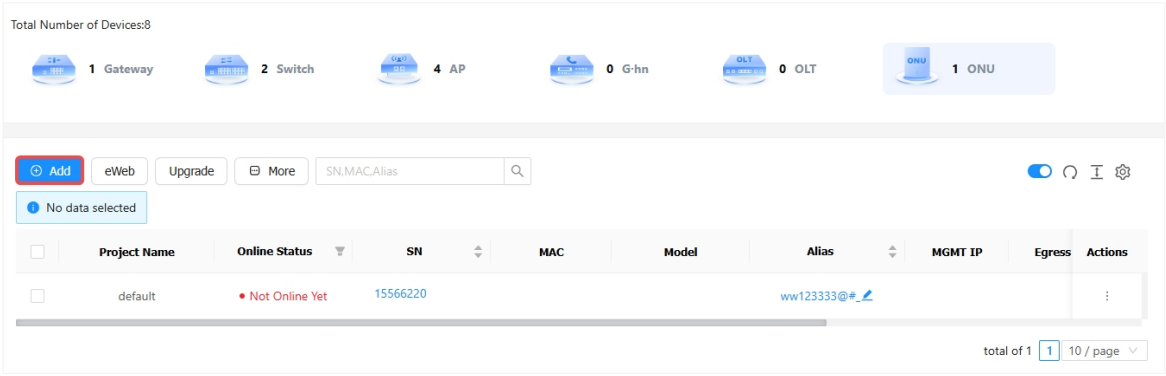
4.6.2.2 Adding ONUs in Batches

To add ONUs in batches:

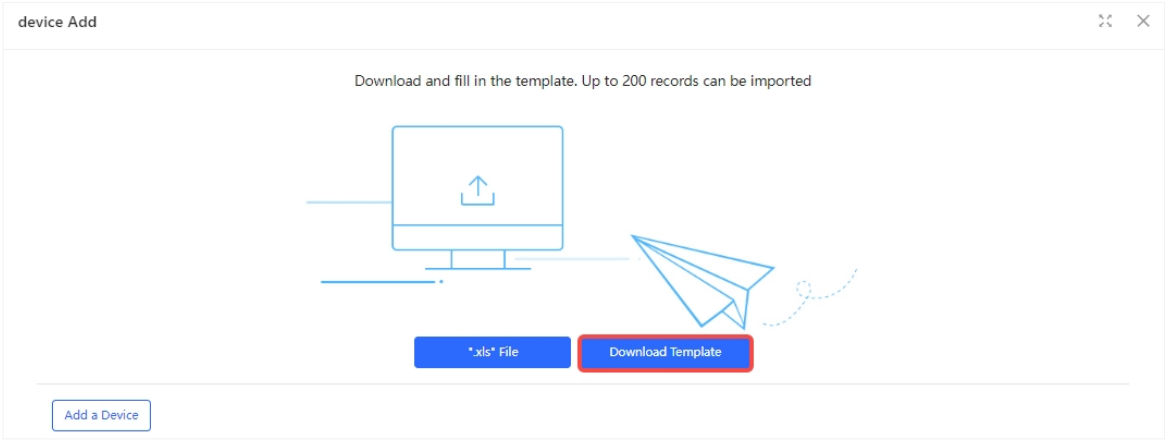
1 Select the project.



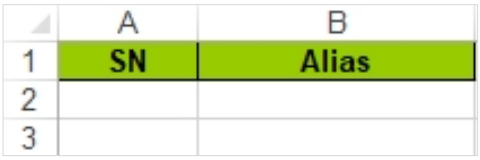
2 Click **Add**.



3 Click **Download Template** to download the template.

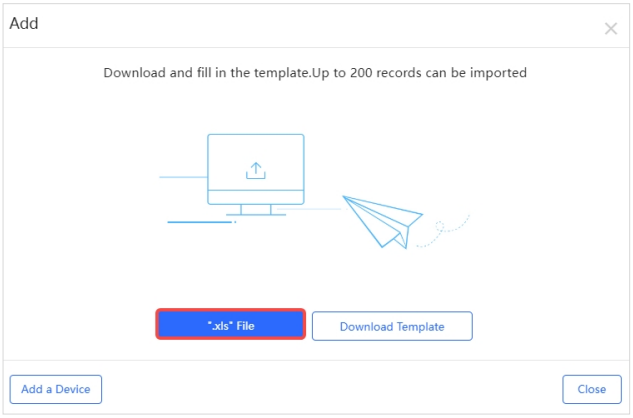


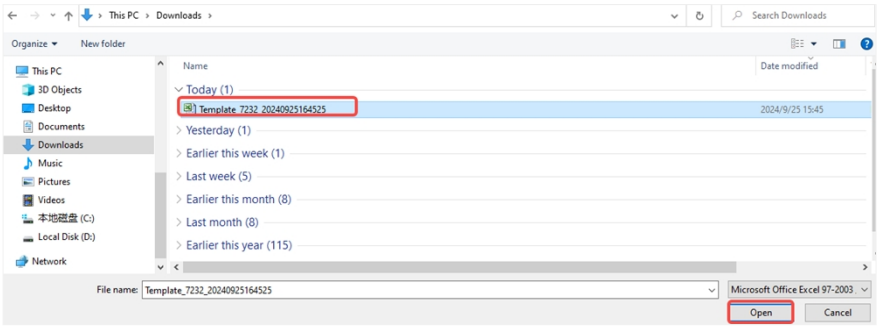
4 Fill in the template. SN is required while the alias is optional. Up to 200 devices can be imported each time.



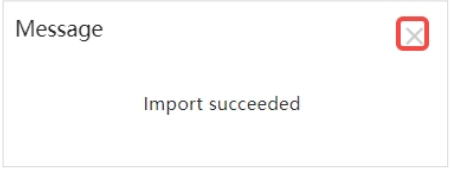
	A	B
1	SN	Alias
2		
3		

5 Click **".xls" File** to upload the template.





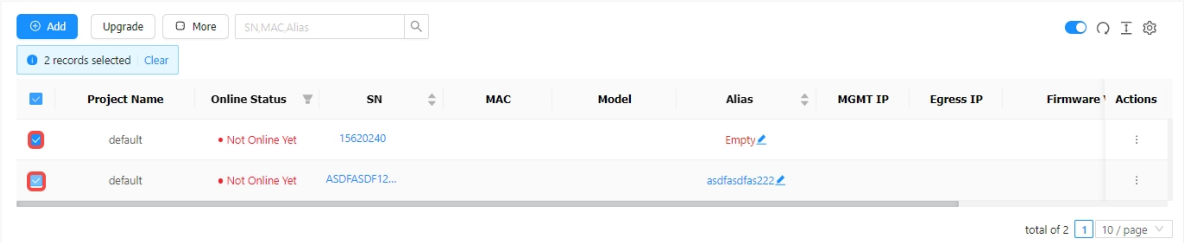
6 When the "Import succeeded" prompt appears, the operation is complete. The imported devices will be displayed in the ONU list.



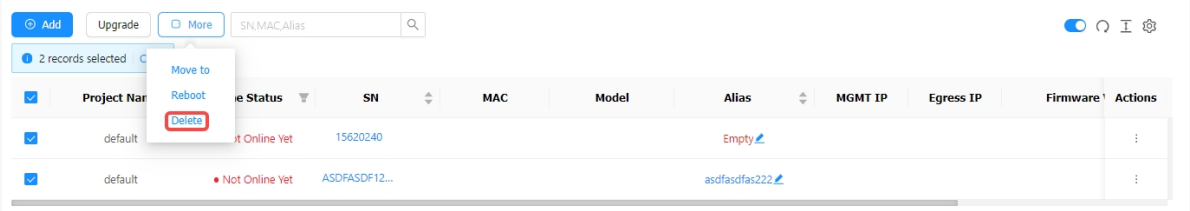
4.6.3 Deleting ONUs

Follow the steps below to delete the ONU(s) from a project.

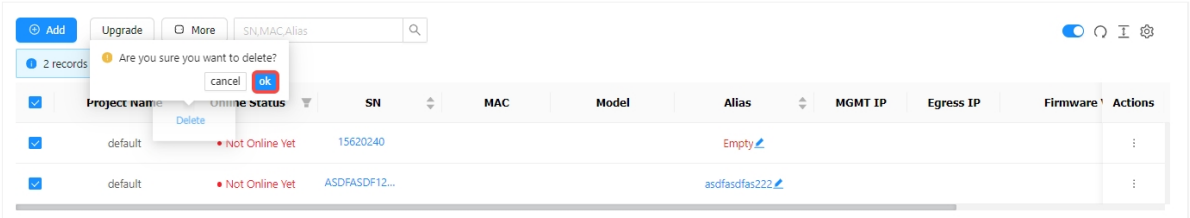
1 Select the ONU device to be deleted.

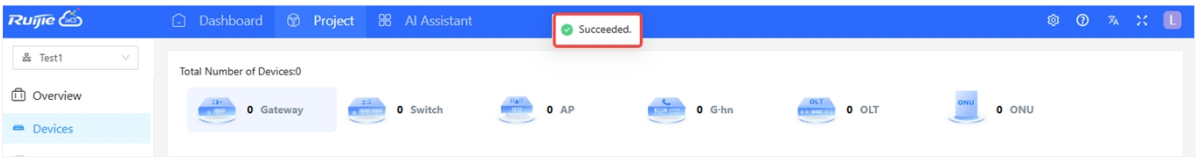


2 Click **More**, and then click **Delete**.

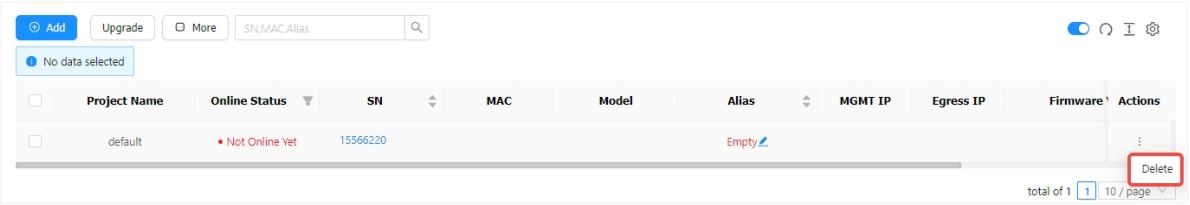


3 Click **OK** in the operation confirmation box. When the "Succeeded" prompt appears, the operation is completed.





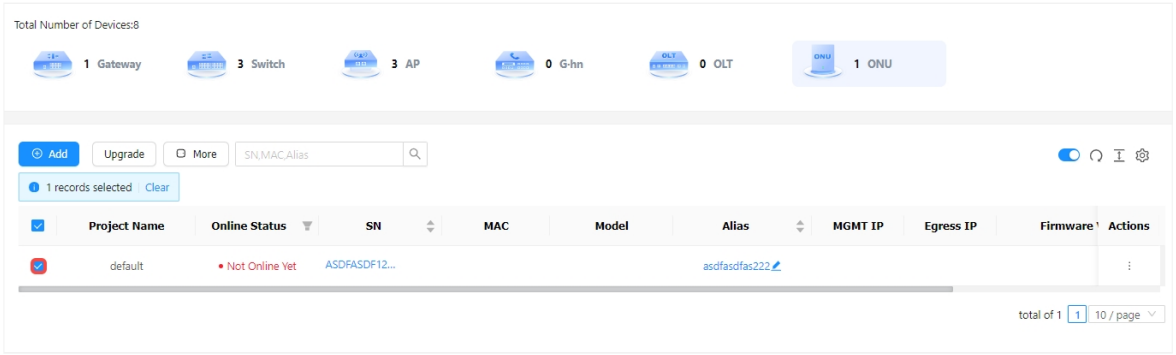
In addition to the above deletion method, you also can hover the cursor over the ⋮ icon in the **Action** column of the ONU to be deleted and click **Delete** to delete it.



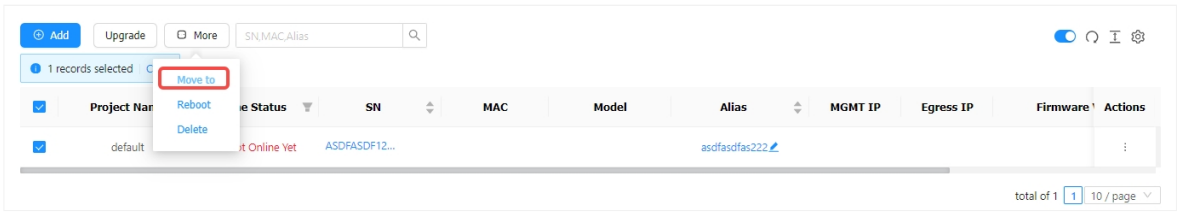
4.6.4 Moving ONUs

Follow the steps below to move the ONU(s) to another project.

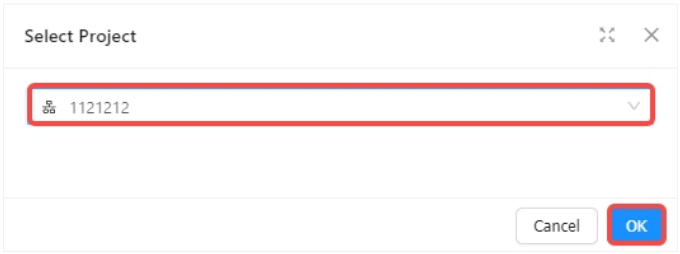
1 Select the ONU to be moved in the ONU list.



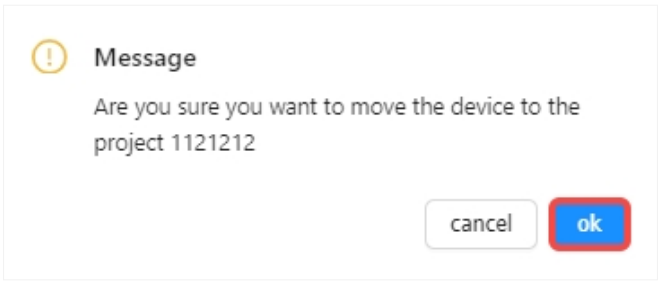
2 Click **More**, and click **Move to**.



3 Select a new project, and then click **OK**.



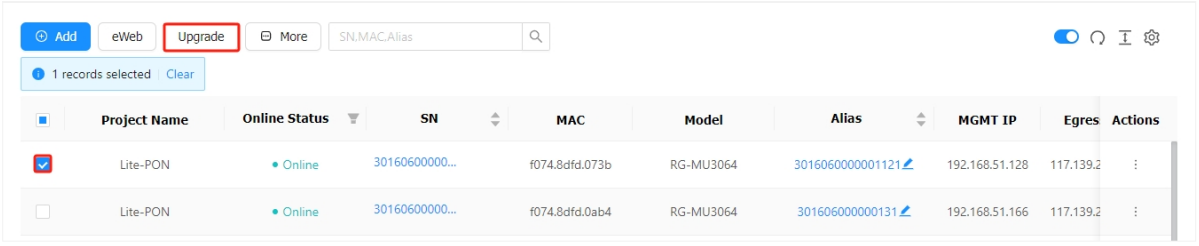
4 When the operation confirmation box appears, click **OK**.



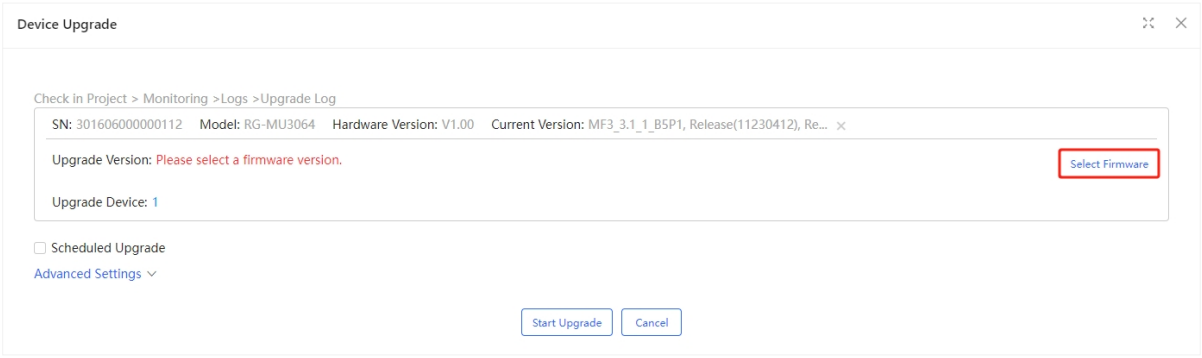
4.6.5 Upgrading ONUs

Follow the steps below to upgrade an online ONU.

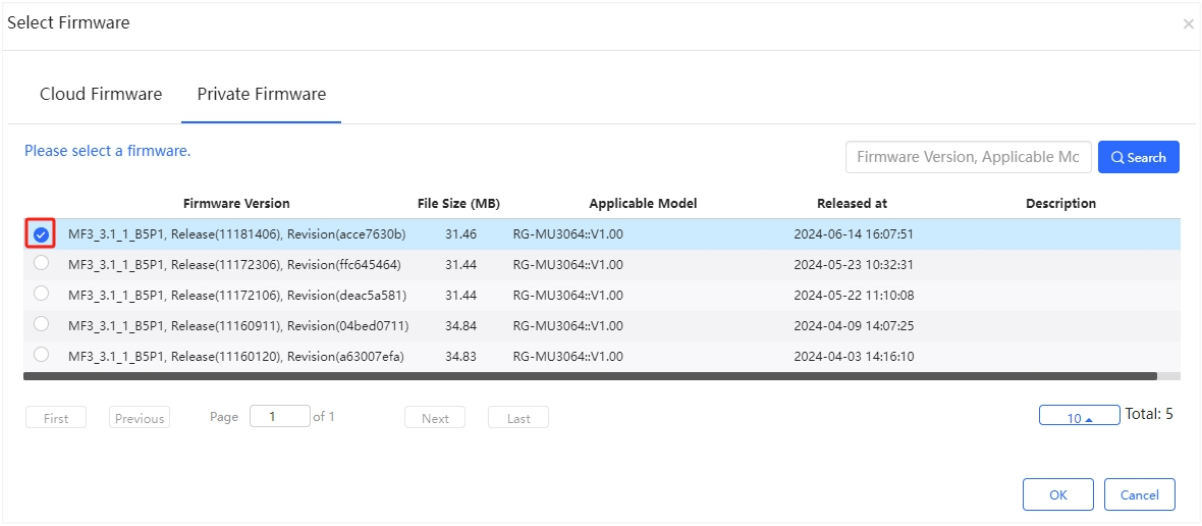
1 Select the device to be upgraded, and click **Upgrade**.



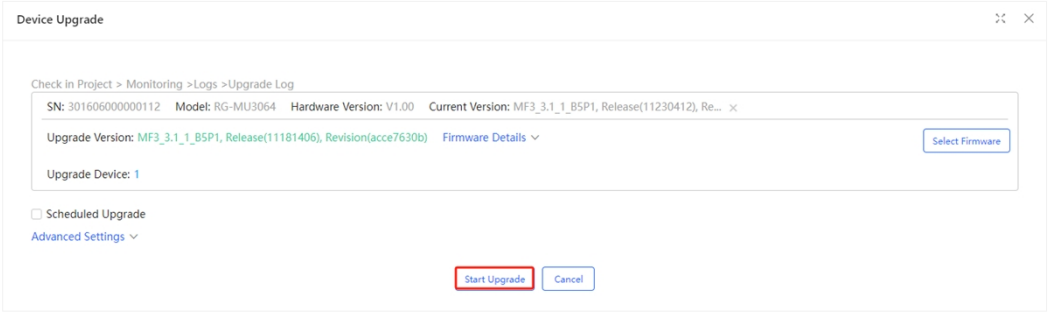
2 Click **Select Firmware** to select a firmware version.



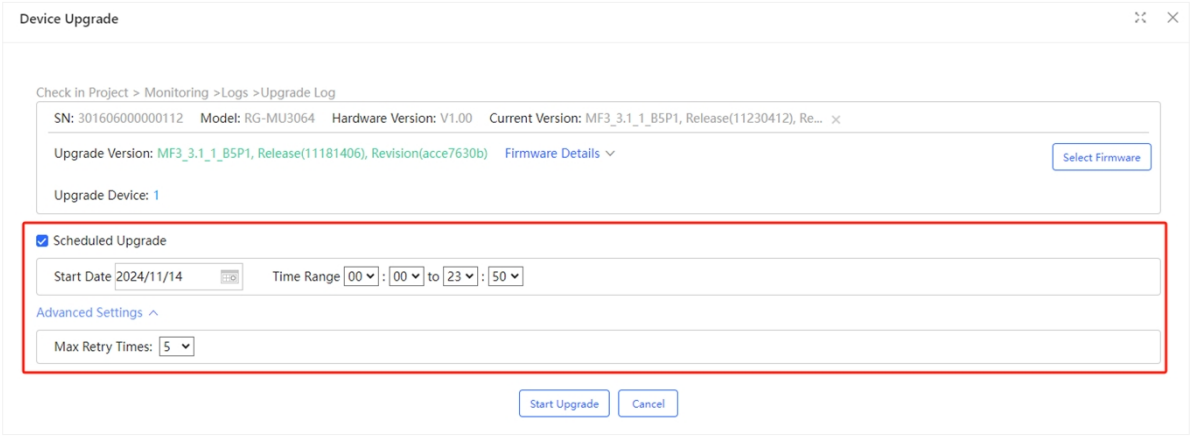
3 After selecting the firmware version, click **OK**.



4 Click **Start Upgrade** to create an upgrade task.



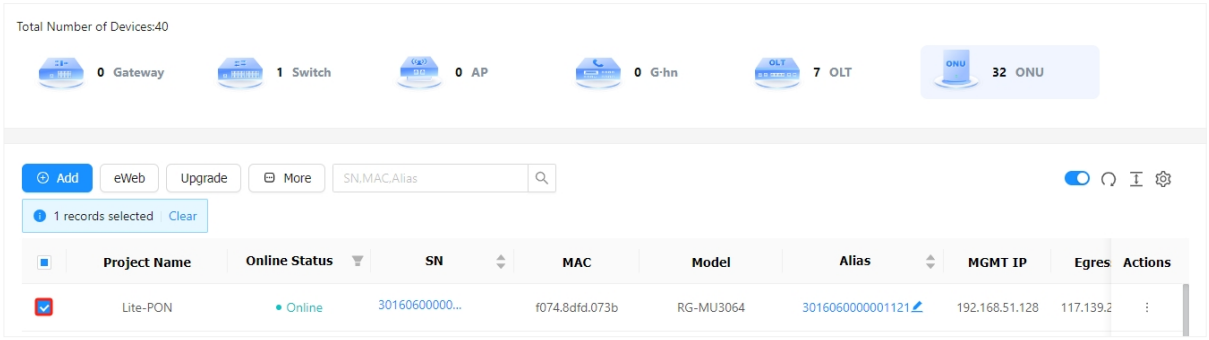
If you need to upgrade the device at a specific time, you need to check **Scheduled Upgrade**, and set the upgrade time. After that, click **Start Upgrade**. The default number of upgrade attempts is 5.



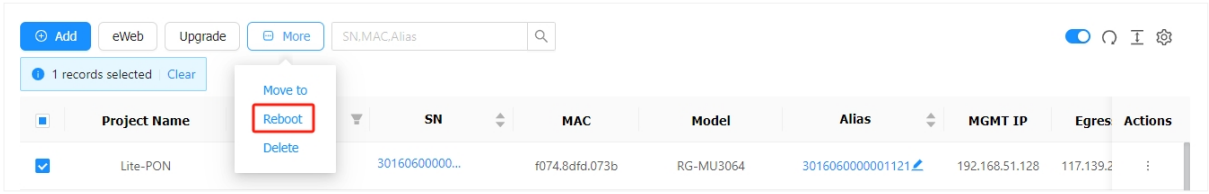
4.6.6 Restarting ONUs

Follow the steps below to remotely restart the ONU(s) through the JaCS.

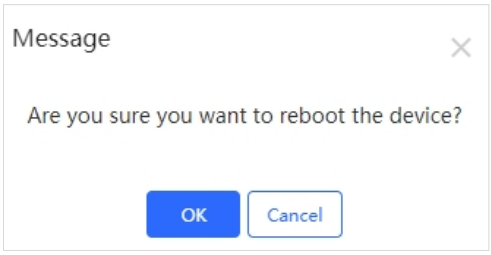
1 Select the ONU device to be restarted.



2 Click **More** and then select **Reboot**.



3 Click **OK** in the operation confirmation box, and wait for the device to restart.



5 Basic Wireless Configuration

5.1 Wireless Configuration for Apartment Project

This section introduces how to set wireless configuration in an apartment-based project:

- Setting the SSID and Password
- Sending Configurations to APs through Web CLI

5.1.1 Setting SSIDs and Passwords

This section mainly introduces how to set the SSID and password of the AP:

- Manually Setting SSIDs and Passwords
- Automatically Configuring SSID and Pssword
- Synchronizing the SSID and the Password
- Delivering Configuration via the Web CLI

Note

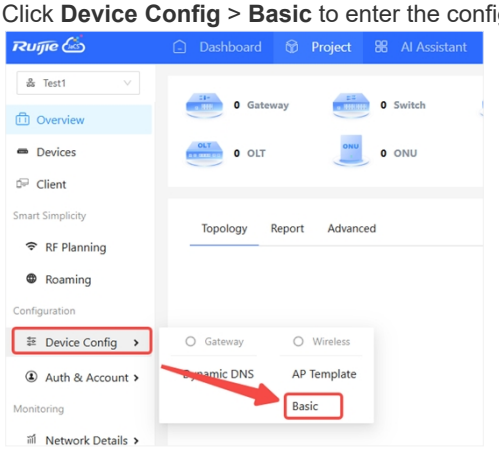
This function is only applicable when the project scenario is set to the apartment.

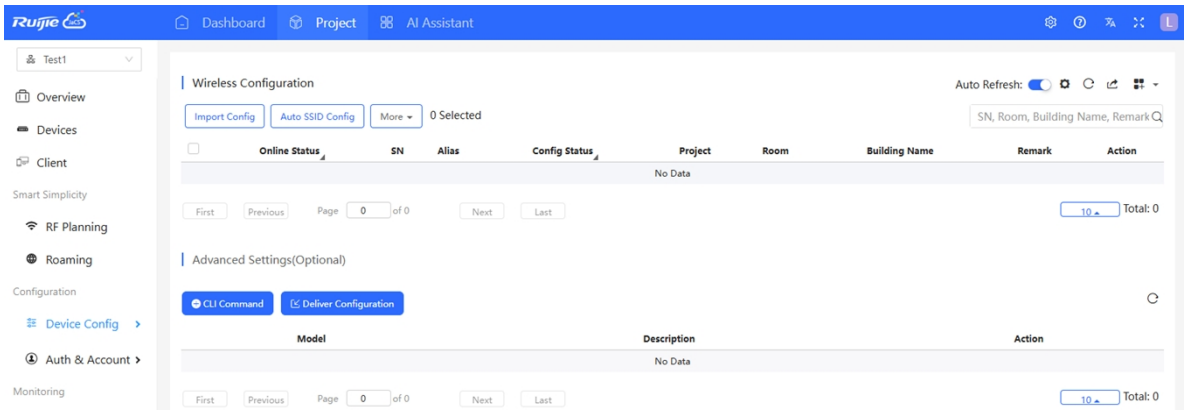
5.1.1.1 Manually Setting SSIDs and Passwords

Follow the steps below to set the SSID and the password of the AP:

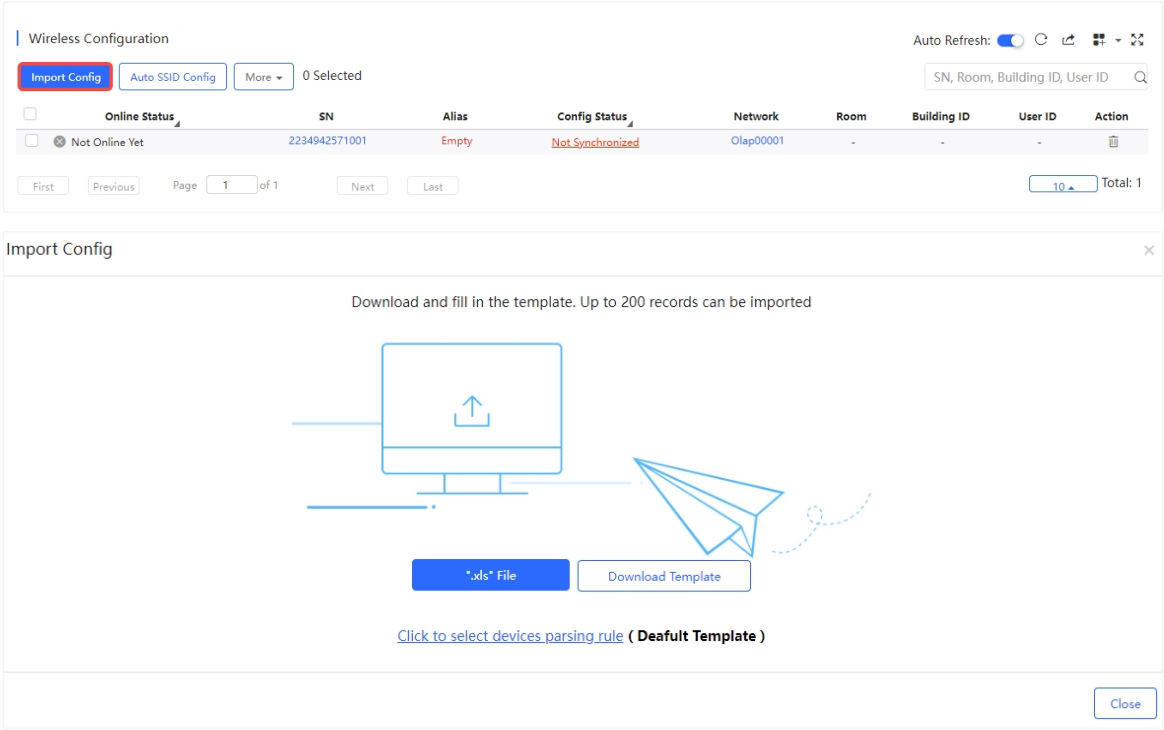
1 Click **Project** to go to the project management interface, and then select the project.

2 Click **Device Config** > **Basic** to enter the configuration interface.





3 Click **Import Config** to manually configure the SSID and the password. After the device is connected to the cloud, the configuration will be delivered to the device directly.



4 Click **Download Template** to use the system default template for configuration or use a custom configuration template.

➢ **Introduction to the system default template:**

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

Item	Description
Model	Optional. Enter product models. For example: AP520-I
SN	Required. Enter SNs. The length of a SN should range from 6 to 20 characters. For example: G1PD7PW00060B
MAC	Optional. Enter MAC addresses of devices.

PN	Enter part numbers. This field can be ignored.
SSID	Required. Enter SSIDs. A SSID is 4 to 32 characters and supports letters, numbers, and special symbols ("_", "-", "." or "@"). When setting multiple SSIDs, separate them with commas(,), such as “ssid-test1, ssid-test”.
SSID Password	Required. Set passwords. A password is 8 to 32 characters and supports letters, numbers and special symbols (@!*#<>=[]()._-) . When setting multiple passwords, separate them with commas(,), such as “8888888rrrrr , 999999ddddd”.
Alias	Optional. Up to 64 characters are supported.
Room	Optional. Specify the room number where the AP is located. Support 1-32 characters. For example: 301.
Building Name	Optional. Specify the building name. Supports up to 32 characters.
Remark	Optional. Up to 32 characters is supported.

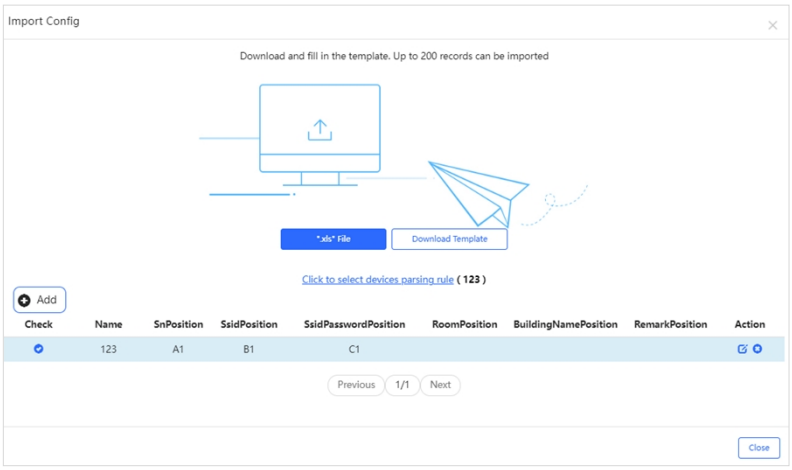
Note

Up to 200 devices can be configured by using the template each time.

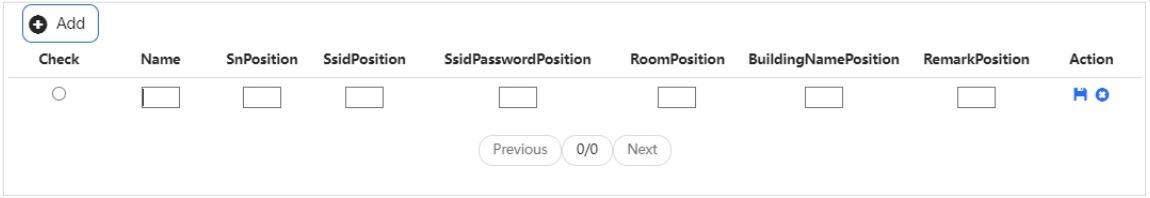
➢ **Introduction to the Customized Template:**

If you do not want to use the default template, you can customize the template by the following steps:

1) Click "**Click to select devices parsing rule**".



2) Click **+ Add** to add a new parsing rule.



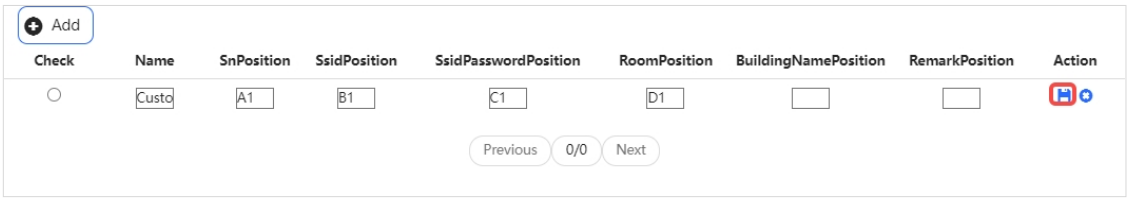
Items	Description
Name	Specify the template name.
SnPosition	Specify the column where the SNs are located in the template.
SsidPasswordPosition	Specify the column where the SSID passwords are located in the template.

RoomPosition	Specifies the column where the room numbers are located in the template.
BuildingNamePosition	Specifies the column in the template where the building names are located in the template.
RemarkPosition	Specifies the column where the remarks are located in the template.

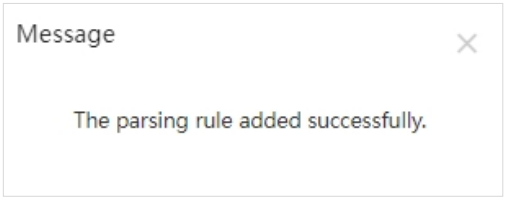
Note

- Users can customize the parsing rules in Excel files from columns A1 to Z1 and rows 1 to 15.
- The custom template format only supports .xls documents, and documents other than this format cannot be parsed.
- If an entry is left blank, it will not be imported.

3) After setting the rules, click the save icon. When "Do you want to save the parsing rule" appears, click **OK**.



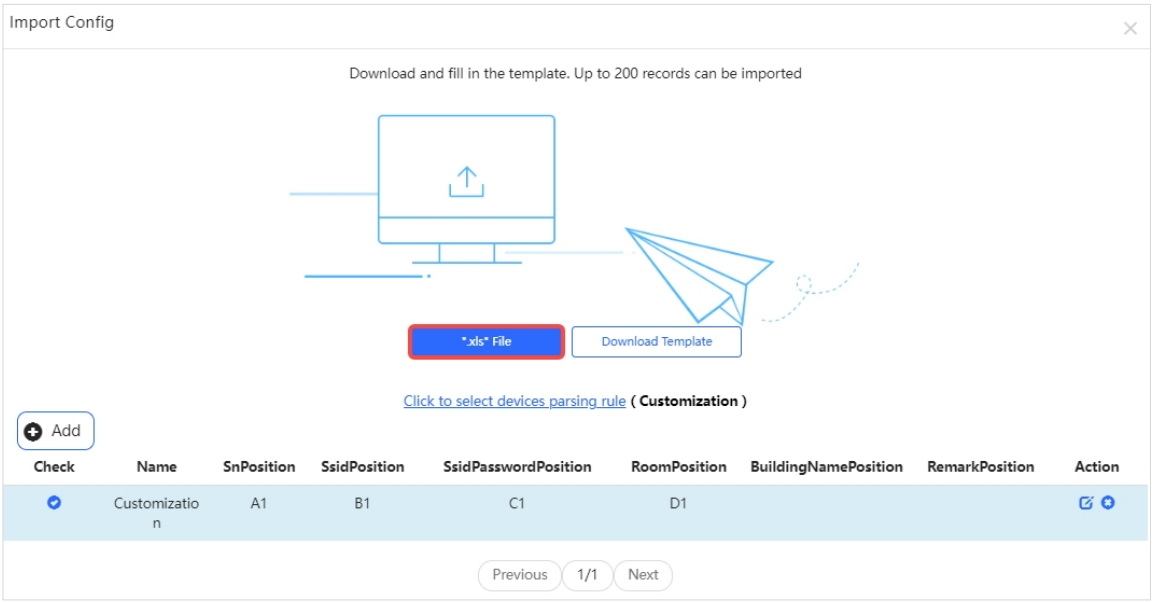
4) After the prompt "The parsing rule added successfully " appears, the rule is added successfully.

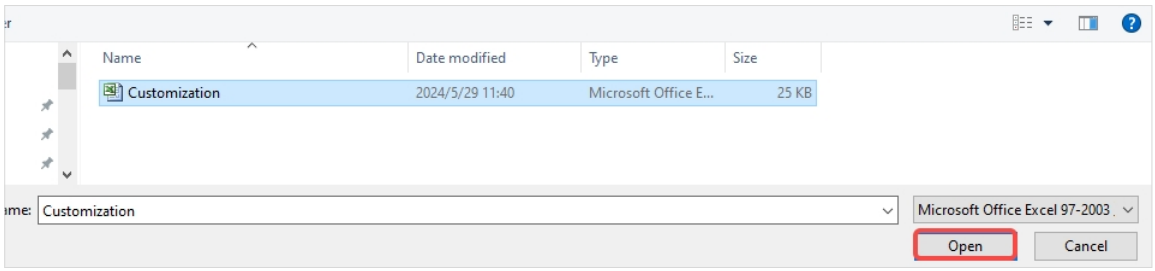


5) Create a new .xls document, and fill in the relevant information in the corresponding position.

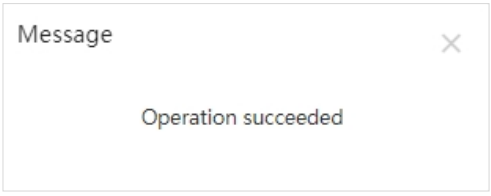
	A	B	C	D
1	12345667	SSID-TEST	admin@ruijie	101
2				

5 Click **".xls" File** to upload the default template or custom template.

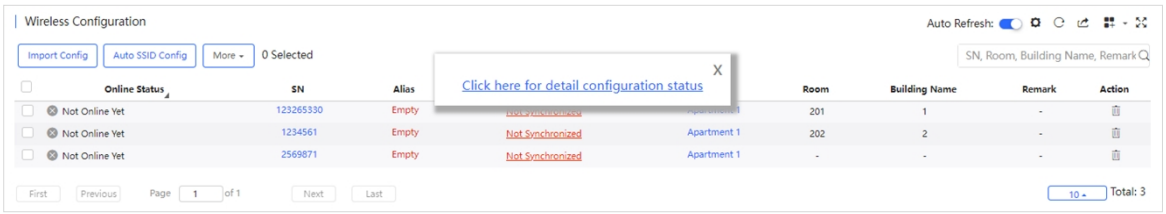




6 After the "Operation successful" prompt appears, the operation is finished.



After the configuration is completed, a link "**Click to view detailed configuration information**" will appear on the interface. Click the link to jump to the configuration log interface.

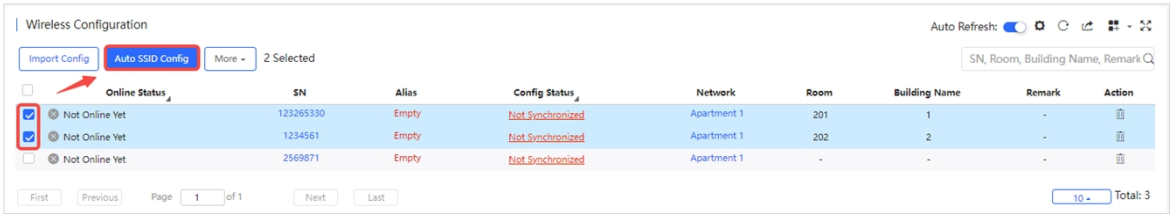


In addition, after the configuration is completed, you can hover the mouse over the SN of the device to view the configured SSID, password, and RF supported by the device.

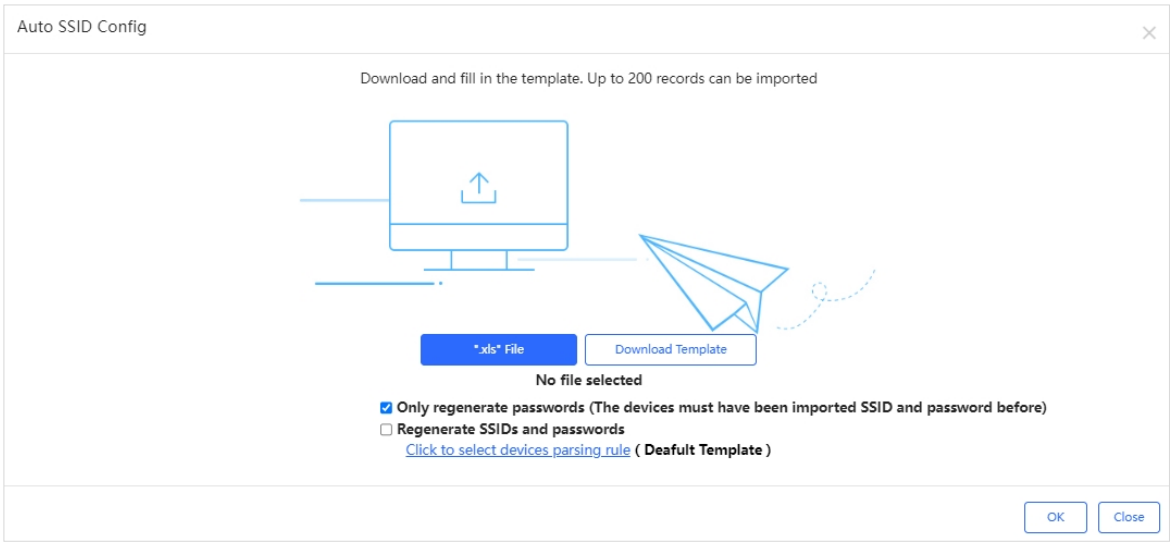
5.1.1.2 Automatically Configuring SSIDs and Passwords

Follow the steps below to automatically configure SSIDs and passwords:

1 Select a device or several devices to be configured, and then click **Auto SSID Config**.

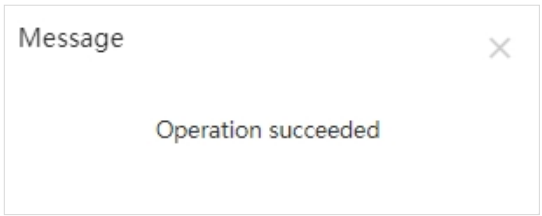


2 Select "**Only regenerate passwords**" or "**Regenerate SSIDs and passwords**".

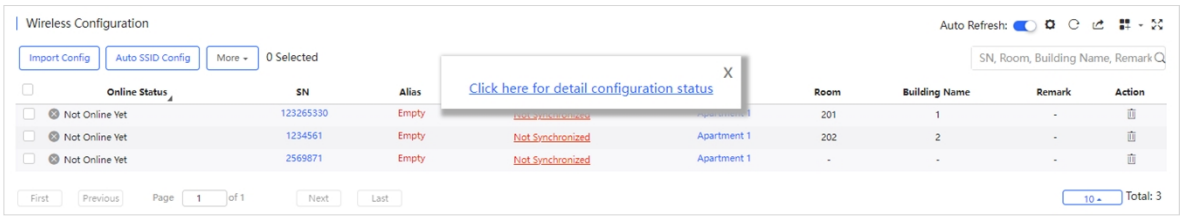


Items	Description
Only regenerate passwords	When this option is selected, only passwords will be automatically regenerated for devices. Make sure that the devices have been configured with SSIDs and passwords before, otherwise, the password cannot be automatically generated.
Regenerate SSIDs and passwords	When this option is selected, both SSIDs and passwords will be regenerated automatically for devices. Up to 4 SSIDs can be configured each device (the default value is 1).

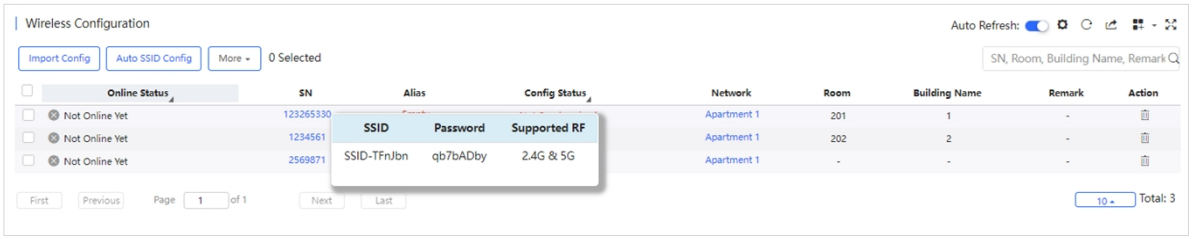
3 After setting the regeneration type, click **OK**. When the "Operation succeeded" prompt appears, the setting is completed.



After the configuration is completed, a link "**Click to view detailed configuration information**" will appear on the interface. Click the link to jump to the configuration log interface.



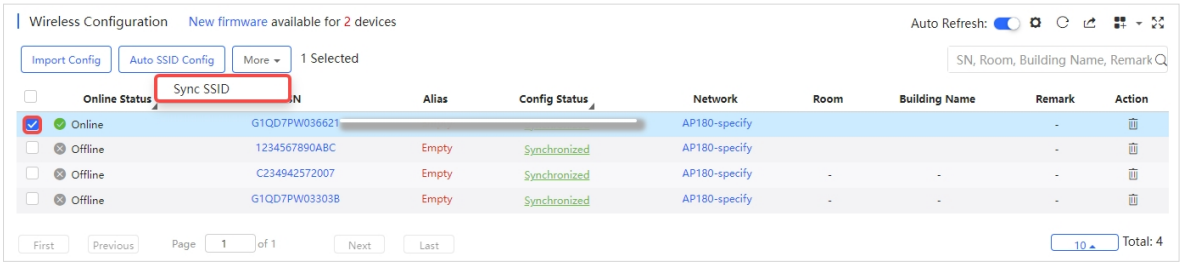
In addition, after the configuration is completed, you can hover the mouse over the SN of a device to view its configured SSID, password, and supported RF.



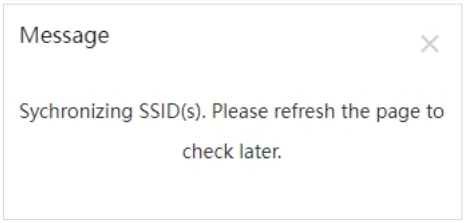
5.1.1.3 Synchronizing SSIDs and Passwords

Ruijie JaCS supports acquiring the device SSIDs. Up to 100 devices can be selected at a time. After synchronization is completed, hover the mouse over the SN of a device to display its SSID and password.

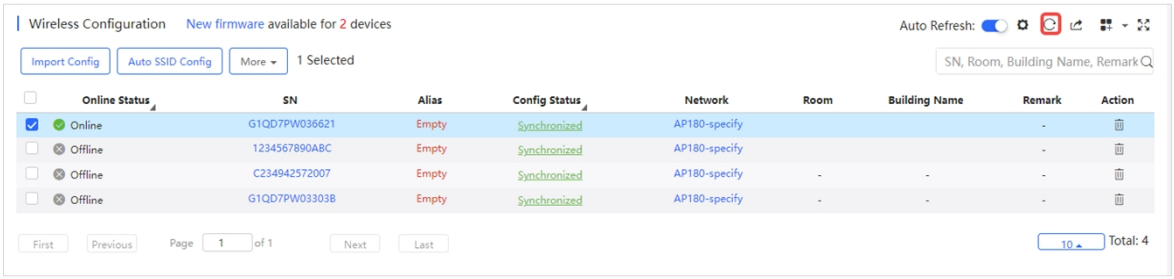
1 Select the online devices that you want to know the SSID and password, and then select **More** > **Sync SSID**.



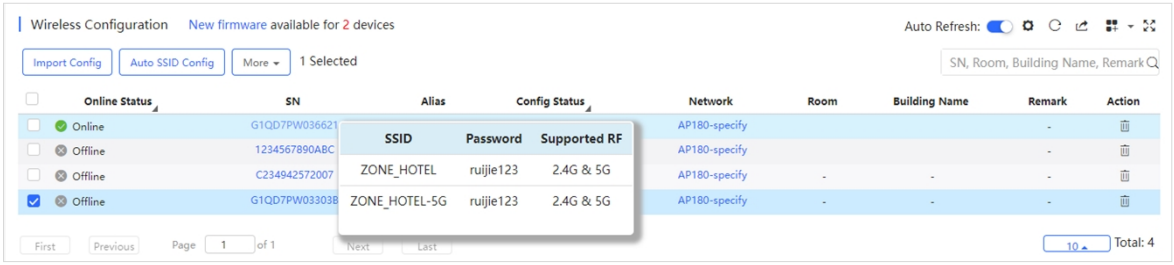
2 Click **X** to close the window and wait for the SSID and password to be synchronized.



3 Click the ↻ icon to refresh the list.



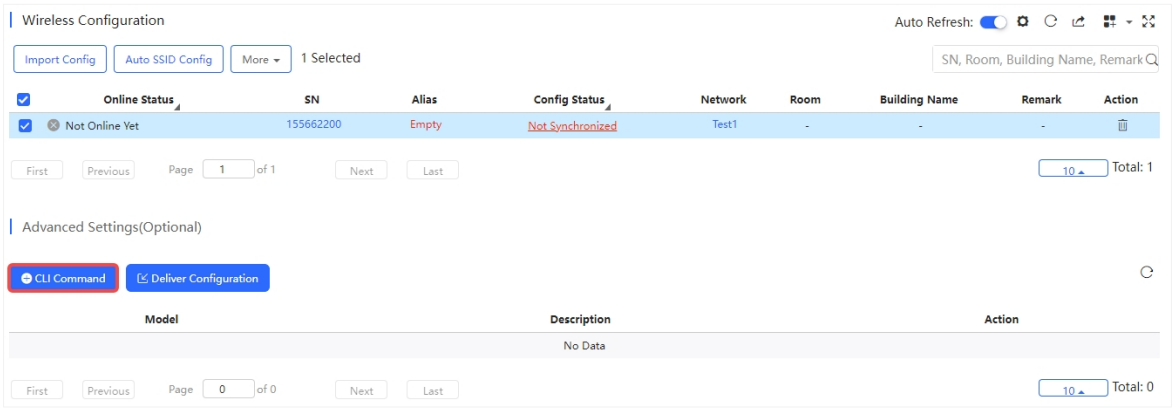
4 Hover the mouse over the SN of a device to view its SSID and password.



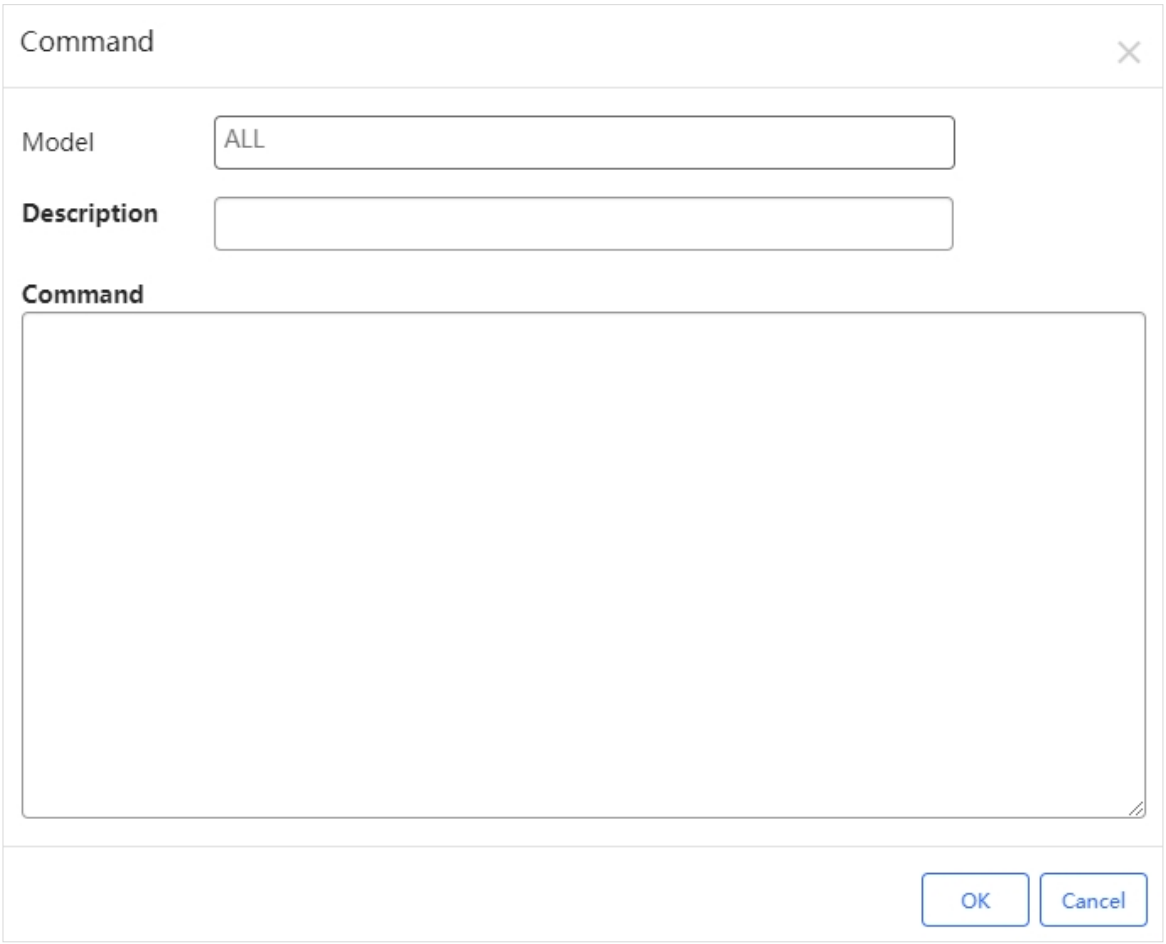
5.1.2 Sending Configuration to APs through Web CLI

Ruijie JaCS supports sending configurations to APs through Web CLI.

1 Navigate to **Project** > **Device Config** > **Basics** > **Advanced Setting** and click **+ CLI Command**.



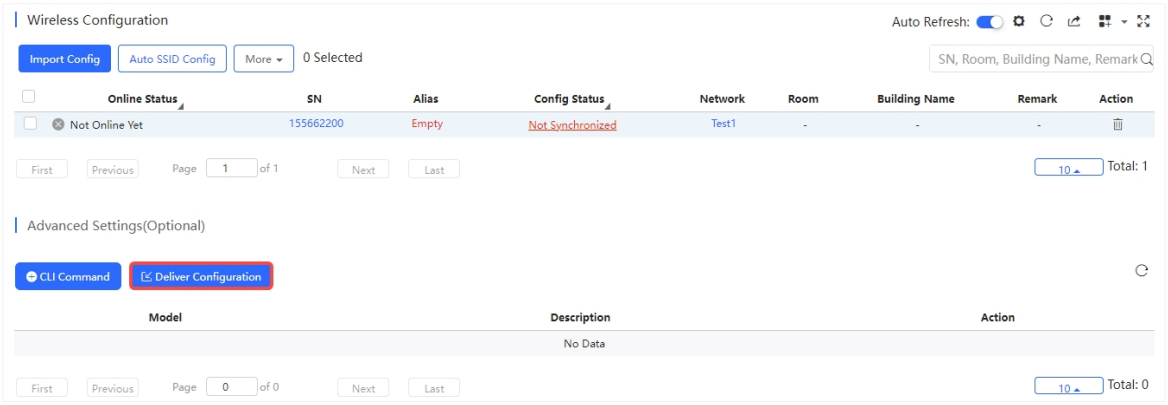
2 Specify the device model, description and enter CLI commands. If you select "**All**", the system will send the configuration to all online APs in the current project.



Items	Description
Model	Required. Defaults: ALL. Select the device model (only supports sending configuration to online devices.)

Description	Required. Defaults: N/A.
Command	Enter the CLI commands.

3 After entering the CLI command, click **OK**. Then, click **Deliver Configuration** to deliver the configuration to the specified device model.

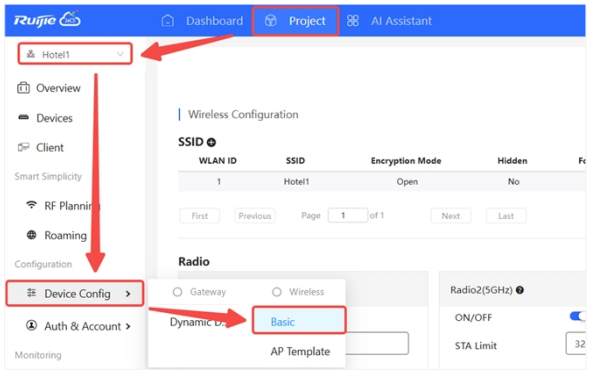


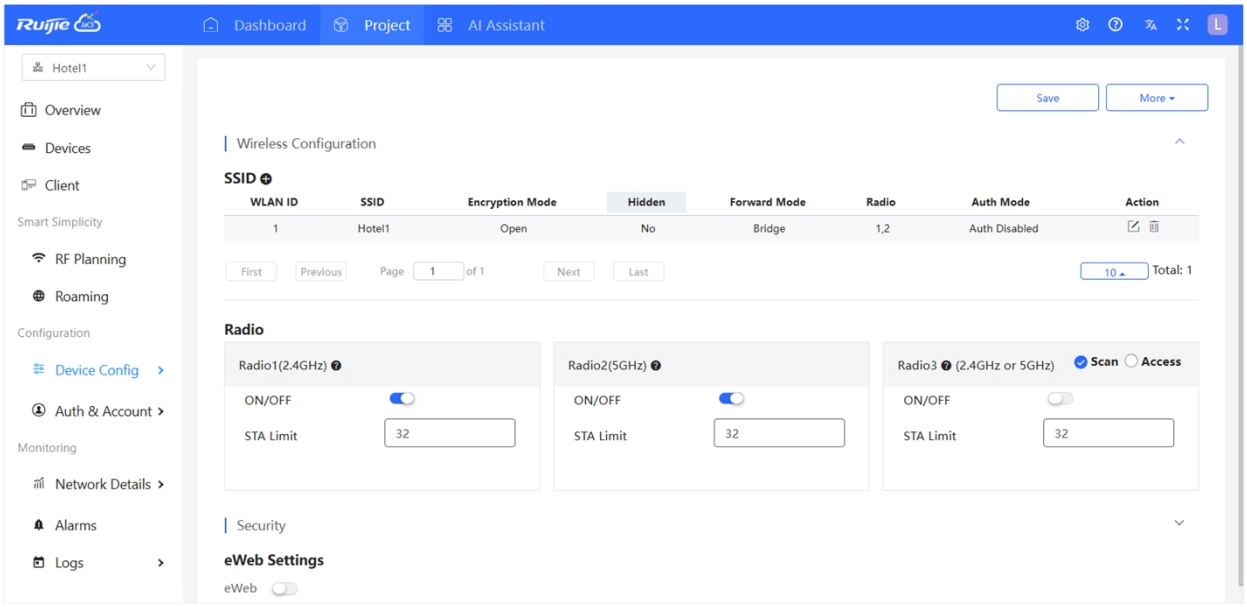
5.2 Wireless Configuration for Non-Apartment Projects

Note

The following operations are applicable only to the project with the scenario set to "Hotel" or "Other".

Click **Project**, select a non-apartment project, and then click **Device Config** > **Basic** to enter the enter the wireless configuration interface. The wireless configuration consists of three parts: "**Wireless Settings**", "**Security Features**", and "**Advanced Settings**".



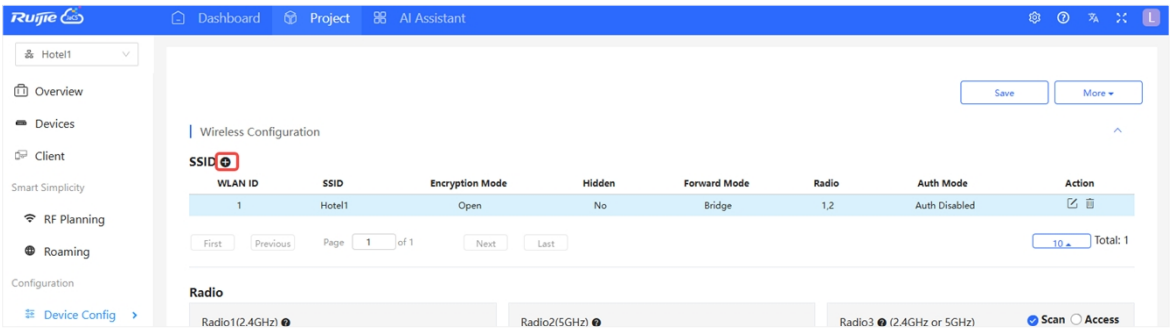


Tabs	Description
Wireless Configuration	Supports configuring SSIDs and radios.
Security	Supports configuring Web passwords, Telnet passwords, client isolation, and wireless intrusion detection.
Advanced Settings (Optional)	Supports configuring scheduled shutdown of RF, adding whitelists, and issuing configurations to APs through the Web CLI.

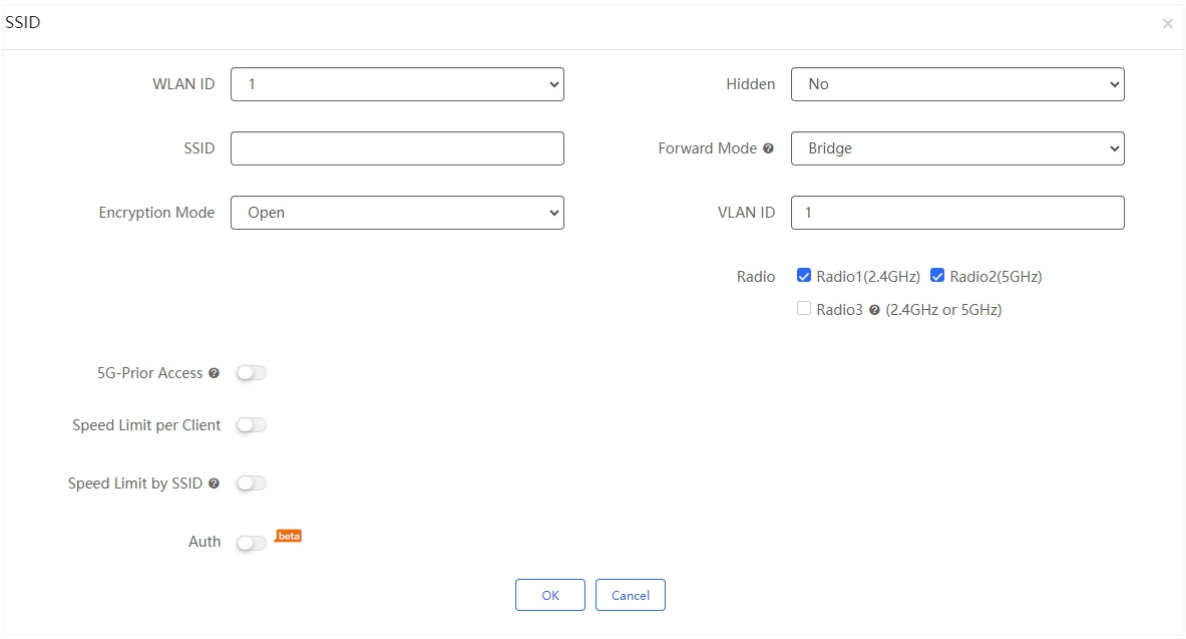
5.2.1 Adding SSIDs

Follow the steps below to add a SSID:

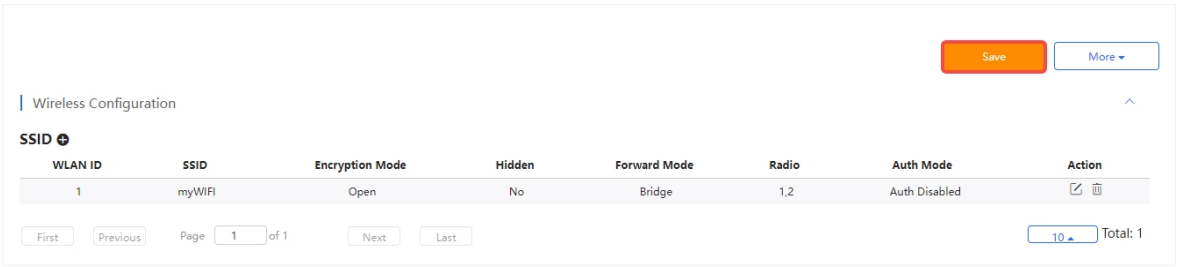
1 Click **+** icon.



2 Specifying the parameters according to the actual needs, and then click **OK**.



3 The added SSID will be displayed in the list. If you do not need to modify it, click **Save** to save the configuration. After the configuration is saved, the configuration will be sent to the APs in the project after they go online.



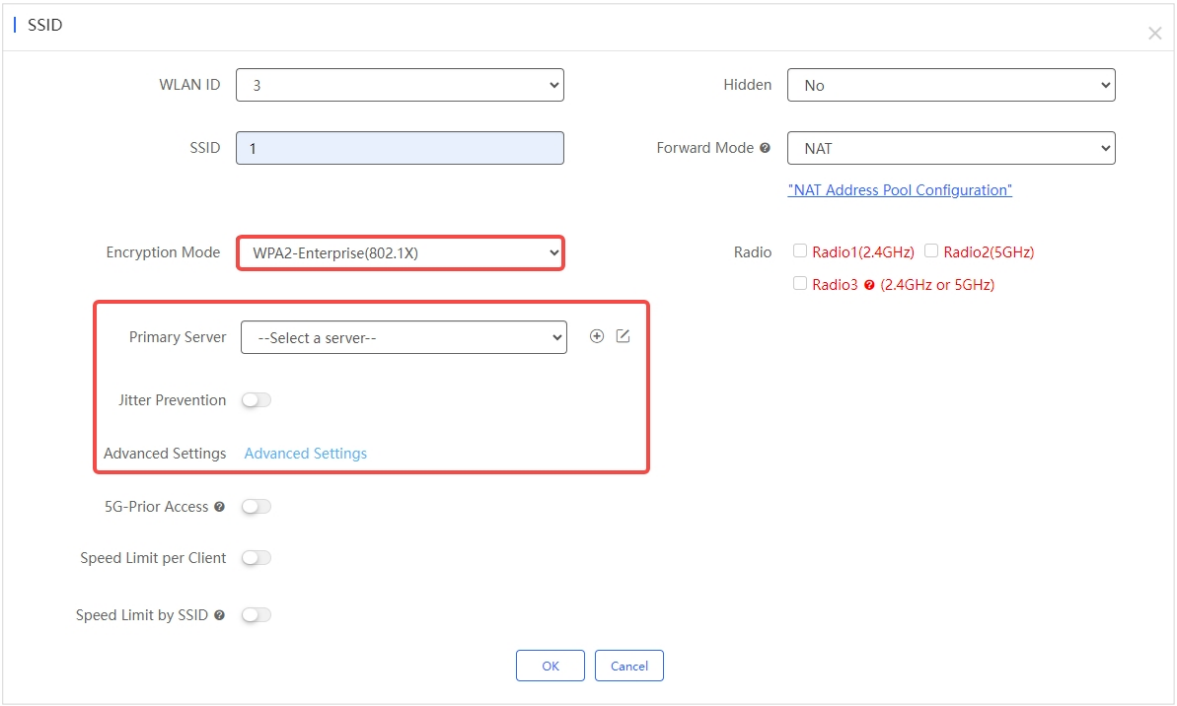
Introduction to the configuration items in SSID setting page.

Items	Description
WLAN ID	Required. Select a WLAN ID. SSID and WLAN ID must correspond one to one. WLAN ID is only specified when adding a SSID. Once it is set, it cannot be changed. WLAN ID range: 1-16.

Hidden	Required. Set whether to hide the SSID. Defaults: No. If you need to hidden the SSID, set it to "Yes".
SSID	Required. Set the SSID name. Up to 32 characters are supported. Letters, numbers, spaces, underscores (_), hyphens (-), periods (.), and @ can be contained. If a SSID name contains spaces, its length cannot exceed 30 characters .
Forward Mode	Required. Configure the forwarding mode of the AP. Defaults: Bridge. Options: ● NAT: The AP assigns the IP address to the client. ● Bride: The IP address is assigned to the client by the AP's uplink device. **Note** RG- MA2810, RG-MA2610-PE, and RG-MA2610-AC only support setting forwarding mode globally. Therefore, if the forwarding mode of one SSID is changed, the forwarding modes of other SSIDs will be changed synchronously.
Encryption Mode	Required. Defaults: Open Options: ● Open: Allows any device to connect to the network without authentication. ● WPA-PSK: WPA-PSK is a security standard for networks. It uses a pre-shared key for encryption. Users are required to enter a pre-shared key before connecting to the network. This is an old Wi-Fi security standard that has been replaced by more secure protocols. ● WPA2-PSK: WPA2-PSK is a more secure encryption standard that uses a pre-shared key for encryption. It is one of the most widely used Wi-Fi security protocols and provides stronger security than WPA-PSK. ● WPA/WPA2-PSK: WPA/WPA2-PSK allows devices that support both WPA and WPA2 to connect to the network. This setting is often used to provide service to devices that are compatible with different security standards. ● WPA3-PERSONAL: WPA3-PERSONAL is the latest Wi-Fi security standard launched by the Wi-Fi Alliance, providing stronger encryption and authentication mechanisms to defend against attacks. ● WPA2/WPA3-PERSONAL: WPA2/WPA3-PERSONAL allows devices that support both WPA2 and WPA3 to connect to the network. It has been gradually migrated to the more secure standard WPA3. ● WPA2-ENTERPRISE (802.1X): WPA2-ENTERPRISE uses the 802.1X authentication protocol and requires a dedicated authentication server to verify the user's identity. It is usually used in enterprise-level networks. It provides personalized user authentication and features stronger security. ● PPSK: PPSK means that each terminal device is bound to a unique Wi-Fi account and key. After selecting the PPSK mode, you need to configure your account in **Project** > **Auth & Account** > **PPSK**.
VLAN ID	Configure a VLAN ID. This field is only required when the forwarding mode is configured as "Bridge". The VLAN ID range is 1-4094.
Radio	Required. Defaults: Radio1(2.4GHz) and Radio2(5GHz). Options: Radio1(2.4GHz) , Radio2(5GHz) , Radio 3 (2.4GHz or 5GHz)
5G -Prior Access	Defaults: Disabled After it is enabled, when the SSID of a dual-band AP is associated with Radio 1 and Radio 2 , clients that support dual-band will access the 5 GHz band first to reduce the load on the 2.4 GHz band so as to improve user experience.
Speed Limit per Client	Set the speed limit based on client.

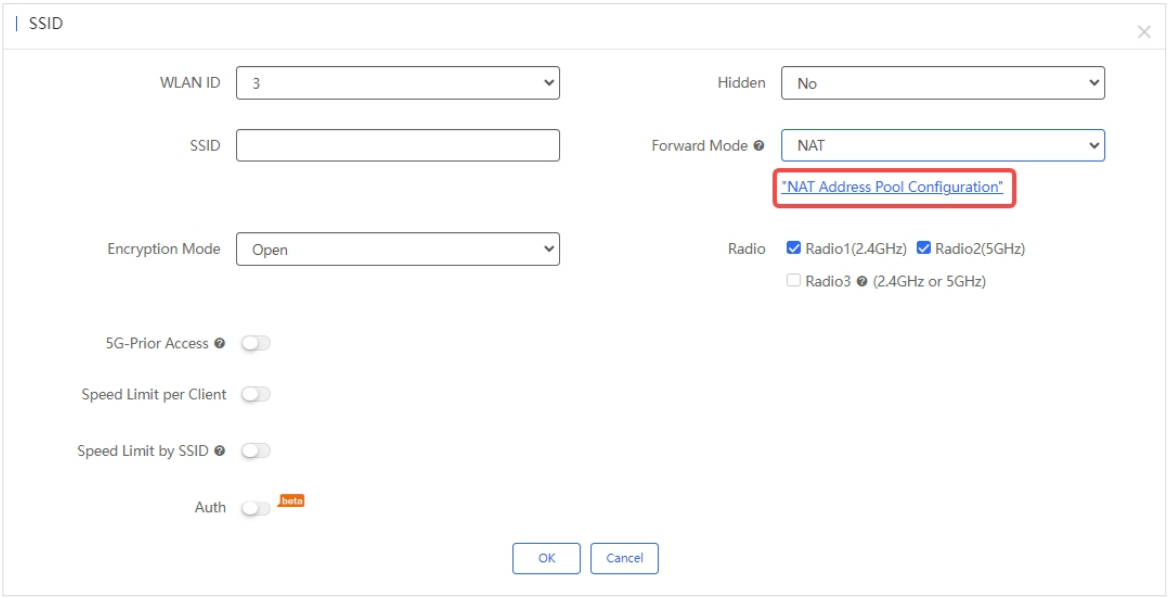
	Defaults: Disabled. If this function is enabled, set the uplink and downlink speed limits.
Speed Limit by SSID	Set the speed limit based on SSIDs. Defaults: Disabled. If this function is enabled, set the uplink and downlink speed limits.
Auth	Defaults: Disabled. After it is enabled, clients will be redirected to the designated portal for authentication when they access the network. Only authenticated clients can access the Internet. Two authentication methods are supported: ● External Portal: After it is set, users connected to the network will be redirected to the external authentication server for authentication. Only authenticated users can access the Internet normally. ● Captive Portal: After it is set, users connected to the network will be redirected to the mandatory authentication webpage for authentication. Only authenticated users can access the Internet normally. (For specific operation steps, please refer to the following text).

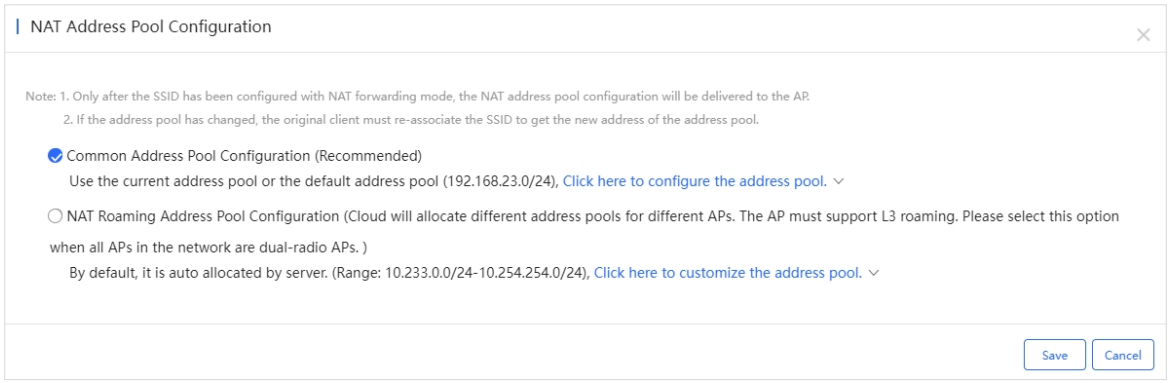
If the encryption mode is configured as " **WPA2-Enterprise (802.1x) ",** the following interface will appear:



Items	Description
Primary Server	Select the primary server. Click the **+** icon to set up the Radius server. When the server is set, you need to configure the server name (required), server address (required), authentication port, accounting port and key (required). **Note** If the authentication port and accounting port are left blank, they are set to 1812 and 1813 by default.
Jitter Prevention	Defaults: Disabled After it is enabled, you need to set the anti-jitter duration (0-600s). During the anti-jitter period, the client will not go offline. The default anti-jitter duration of the AP is 2 seconds. If the AP version is too low, it may not support the anti-jitter function.
Addition Settings	Click **Advance Settings** to enter the advanced settings page, which supports configuring NAS IP address (available in NAT environment) and accounting update interval (unit: minutes).

If the forward mode is configured as NAT, you can click the "**NAT Address Pool Configuration**" link below to configure the address pool. After selecting the address pool configuration type, click the corresponding blue font to configure it. After configuration, click **Save**.

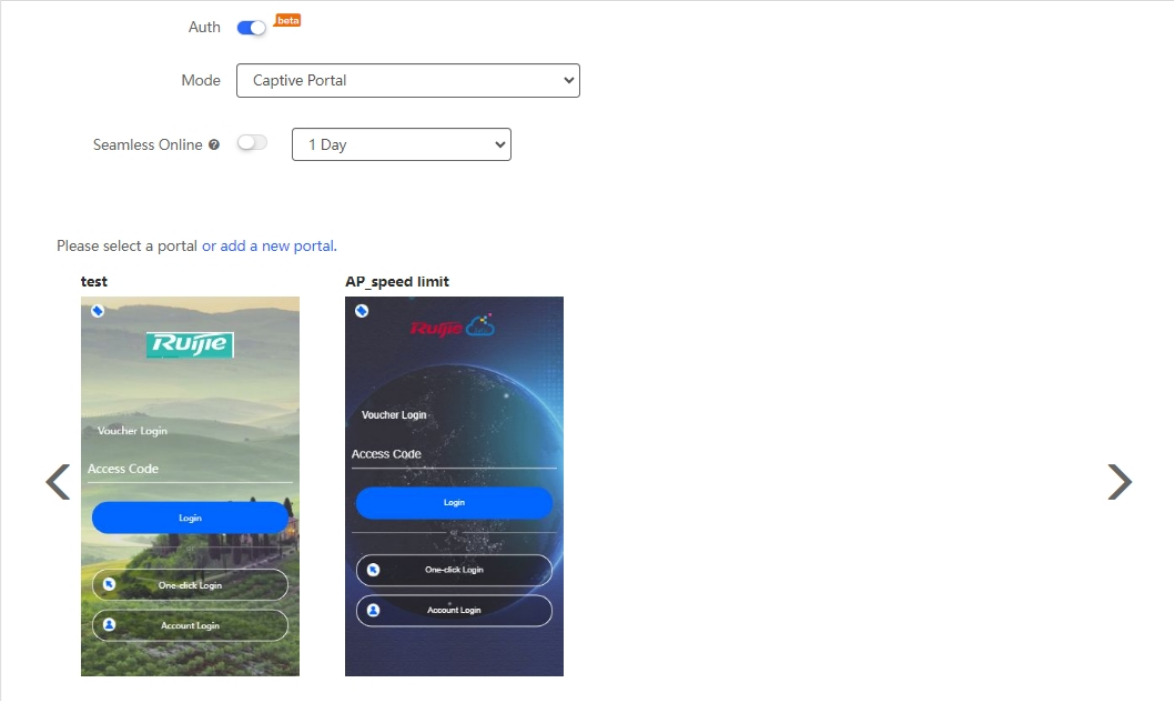




Items	Description
Command Address Pool Configuration (Recommended)	After selecting this option, the address pool (192.168.23.0/24) is used by default. If you need to change it, click "**Click here to configure the address pool**" to configure the IP address and mask.
NAT Roaming Address Pool Configuration	After selecting this option, the default address is assigned by the server (10.233.0.0/24-10.254.254.0/24). If you need to change it, please click "**Click here to customize the address pool.**" and set the start address and end address.

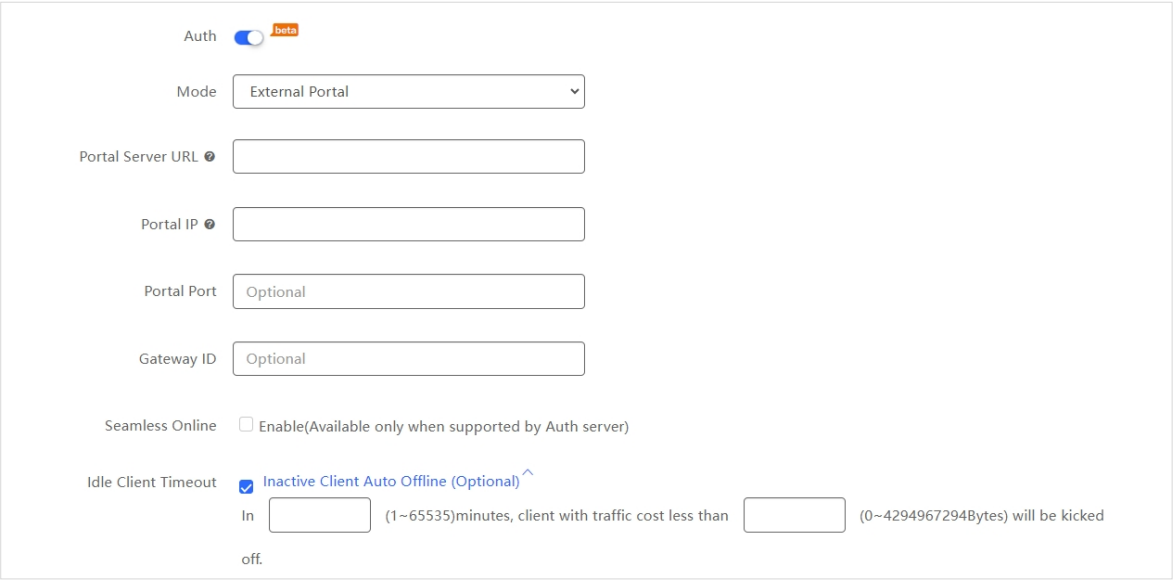
By default, the authentication function of SSID is disabled. After the authentication function is enabled, you can choose to set a captive portal or an external portal.

If you select captive portal, the following configuration items will appear:



Items	Description
Seamless Online	It is disabled by default. When it is enabled, once a client passes the authentication it does not need to authenticate again within the specified period. Supported time periods: 1 day/1 month/1 year/permanent.
Portal Selection	Required. You can select an existing authentication portal. If you want to create a new portal, click "**or add a new portal**". For the steps to add a captive portal, see "5.3 Configuring Captive Portal".

If you choose the external portal, the following interface will appear:



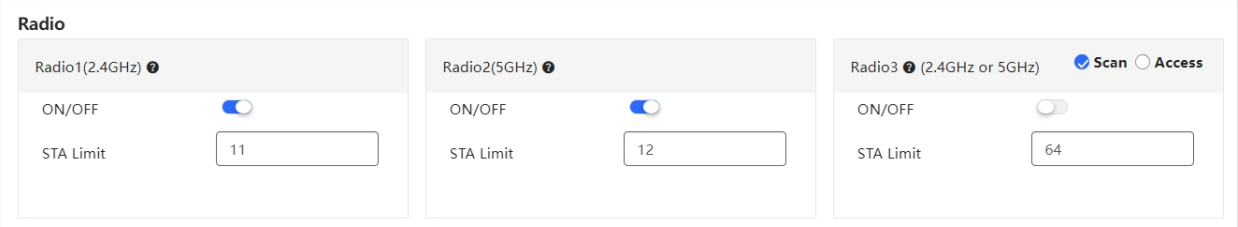
Items	Description
Portal Server IP	Required. After it is set, unauthenticated users will be redirected to this URL for authentication before they can access the Internet.
Portal IP	Required. Set the IP address of the authentication portal .
Portal Port	Specify the portal port.

Gateway ID	Specify the gateway ID.
Seamless Online	Defaults: Disabled. When it is enabled, once a user passes authentication for the first time, there is no need to authenticate again.
Idle Client Timeout	Defaults: Enabled. When it is enabled, clients with traffic less than the set value (0-4,294,967,294 bytes) will be forced offline within the specified time (1-65,535 minutes).

5.2.2 RF Configuration

In the Radio interface, you can configure the radio frequency of the AP. After configuration, click the **Save** button in the upper right corner of the interface to save.

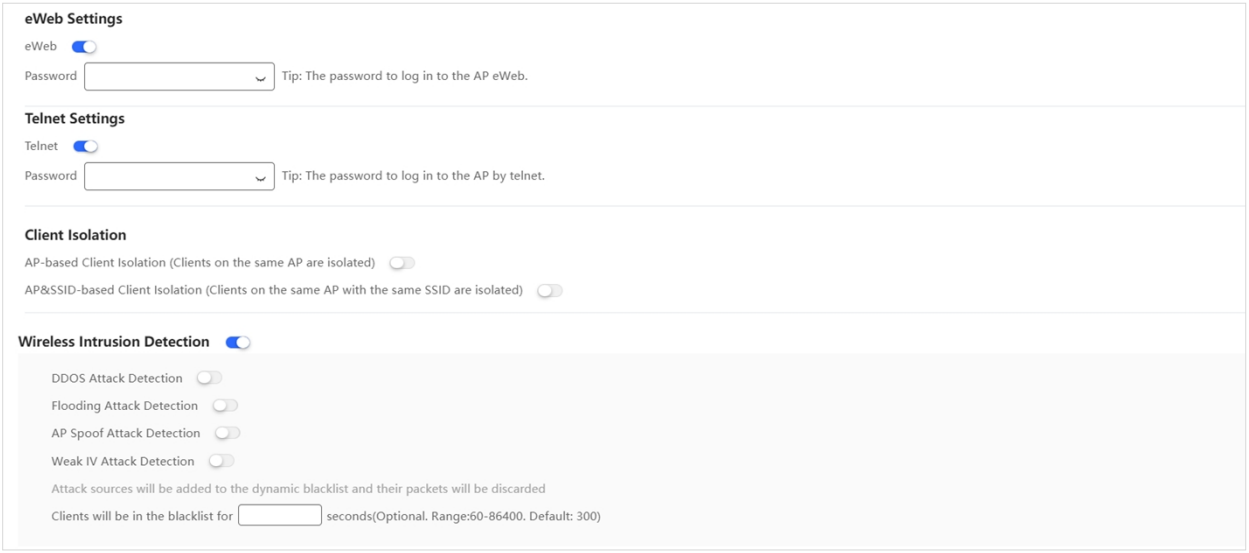
The configuration items are described as follows:



Items	Description
ON/OFF*	By default, Radio1 (2.4GHz) and Radio2 (5GHz) are turned on.
STA Limit	Set the number of clients that can access each frequency band (range: 1-100). If this field is left blank, there is no limit on the number of clients. If the devices that access the Radio 1 (2.4GHz) or Radio 2 (5GHz) need to be set with different limited number of clients, you need to go to the "Advance Settings (Optional)" interface and use the CLI command to set them separately.
Scan	This configuration item is only available for Radio 3 (2.4GHz or 5GHz). After selecting this item, Radio 3 is used to collect RF information around the AP, but STAs are not allowed to access the AP.
Access	This configuration item is only available for Radio 3 (2.4GHz or 5GHz). After selecting this item, Radio 3 is used to provide wireless signals and allow STAs to access the AP.

5.2.3 Security Configuration

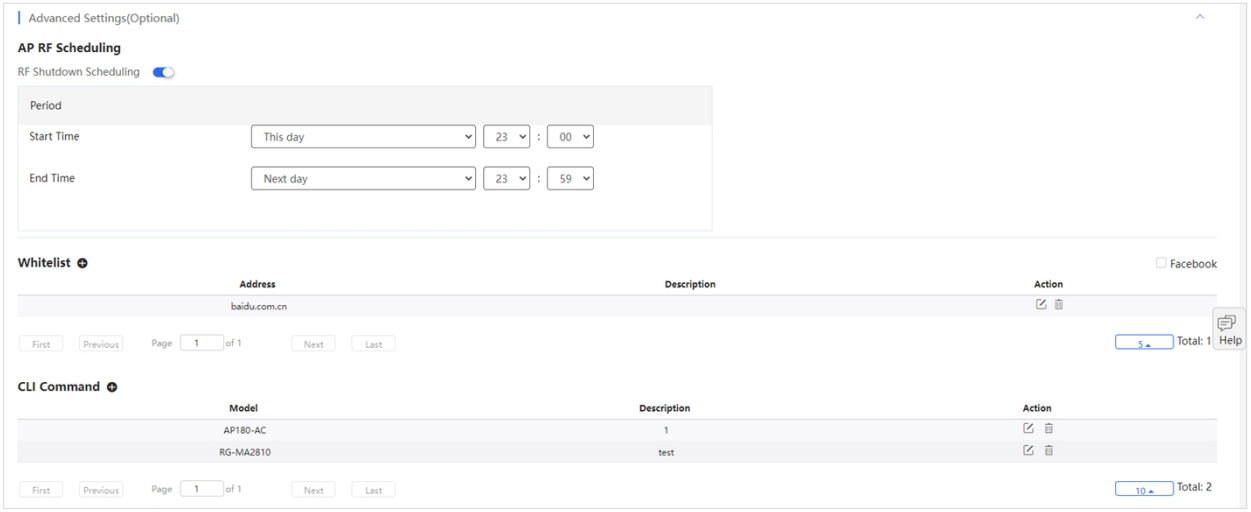
On the security configuration page, you can set the eWeb password, Telnet, client isolation, wireless intrusion detection, etc. After configuration, you need to click the **Save** button in the upper right corner of the interface to save, otherwise the configuration will not take effect.



Items	Description
eWeb	Defaults: Disabled. When it is enabled, you can set the Web login password for accessing the AP's eWeb. When the password is not configured, the system will not send the password to the AP.
Telnet	Defaults: Disabled. When it is enabled, you can set a Telnet password. The password cannot be left empty and its length must be between 8 and 25 characters.
Client Isolation	With the feature enabled, clients will be isolated without affecting the network access to ensure that the clients cannot communicate with each other so as to ensure security. You can choose to isolate the clients based on APs or AP&SSID. AP-based Client Isolation: Disabled by default. When it is enabled, all Layer 2 clients connected to the same AP cannot communicate with each other. AP&SSID-based Client Isolation: Disabled by default. When it is enabled, clients connected to the same AP and the same SSID cannot communicate with each other.
Wireless Intrusion Detection	Disabled by default. Supports four types of attack detection: DDOS attack detection, flood attack detection, AP spoofing attack detection, and weak IV attack detection. If this function is enabled, at least one of the above four detection modes must be enabled. Clients detected to have attack actions will be added to the dynamic blacklist, and their messages will be discarded. Supports setting the duration of the client in the blacklist. The supported duration range is 60-86,400 seconds , and the default value is 300 seconds.

5.2.4 Advanced Settings

On this **Advanced Settings** interface, you can configure AP radio scheduling, whitelists, and CLI commands. After configuration, you need to click the **Save** button in the upper right corner of the interface to save the configuration, otherwise the configuration will not take effect.

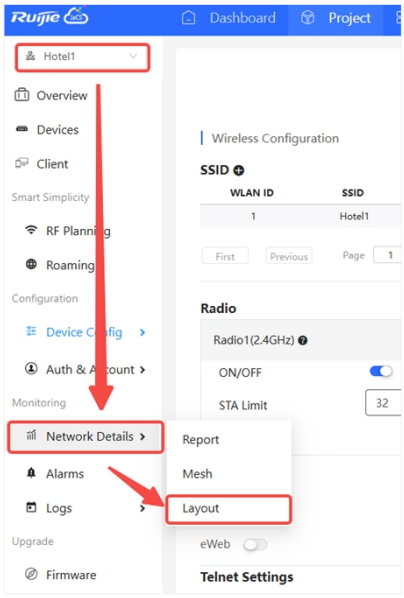


Items	Description
RF Shutdown Schedule	Defaults: Disabled. When RF scheduling is disabled, the AP will broadcast the SSID. When it is enabled, you need to configure the time for Wi-Fi to be enabled and disabled. The maximum supported time period is 24 hours.
Whitelist	Set up whitelist websites and websites that can be accessed directly without identity verification. Click ⊕ to set up a whitelist. After configuring the domain name (required) and description (optional), click **OK** to complete the operation. To remove or edit a website in the whitelist, click ✎ and 🗑 in the **Action** column to perform the corresponding operation.
CLI Command	Click ⊕ to enter the CLI configuration interface. In this interface, you can set the commands to be sent to the AP. To remove or edit the existing CLI commands, click ✎ and 🗑 in the **Action** column.

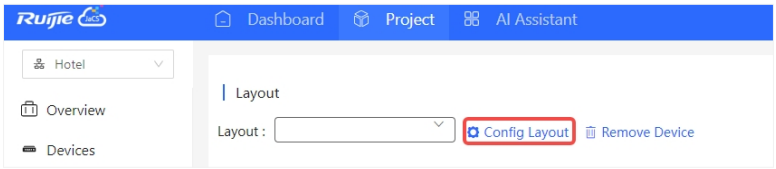
5.2.5 Binding AP location

In the **Layout** interface, you can bind an AP in a specific project to a specific location. The specific steps are as follows:

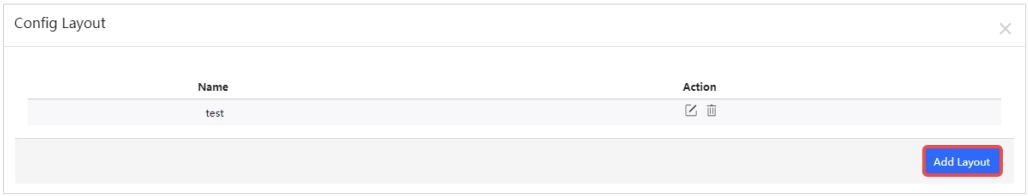
1 After selecting a non-apartment project, click **Network Details** > **Layout** to go to the configuration interface.



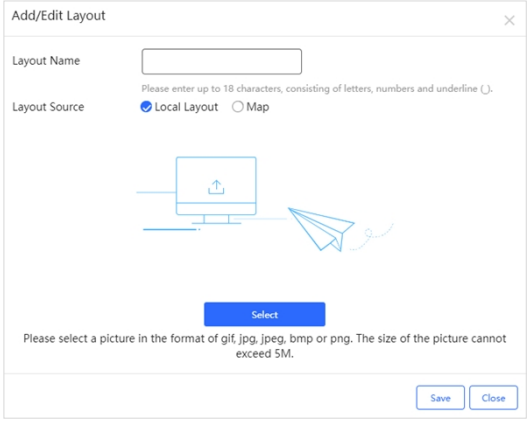
2 Click **Config Layout**.



3 Click **Add Layout** to add a layout.

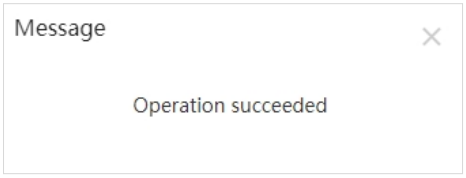


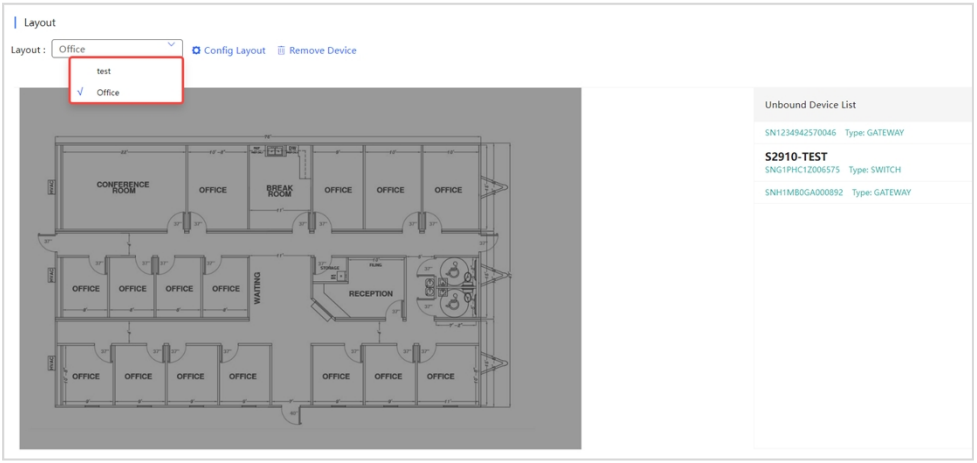
4 After setting the layout name, layout type, and image, click **Save**.



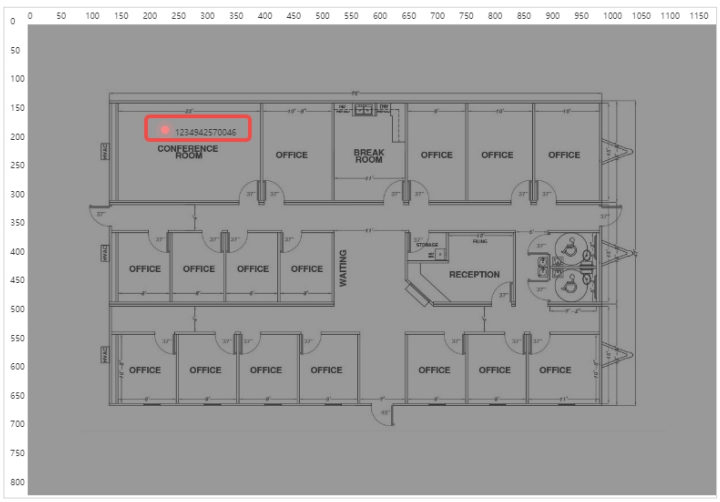
Items	Description
Layout Name	Required. Set the layout name. You can enter up to 18 characters. The following character types are supported: letters, numbers, and underscores (_).
Layout Source	Defaults: Local Layout. Options: ● Local Layout: Local layout can be used to bind the location of indoor APs. ● Map: Map layout can be used to bind the location of outdoor APs.
Select	Click **Select** to upload a picture if you set the loayout source to local layout. You can upload a picture in the format of GIF, JPG, JEPG, BMP or PNG. The size of a single picture cannot exceed 5M.
Bind Location	If you set the layout source to **Map**, you need to specify the location to be bound.

5 When the "Operation succeeded " appears, the setting is completed. Then, you can pull down the layout selection box to select the newly created layout.





6 Select the device you want to bind from the unbound device list on the right and drag it to the target location. After dragging it in, a red dot will appear to mark the device. If you need to change the device location, place the mouse on the red dot and drag it to another location.



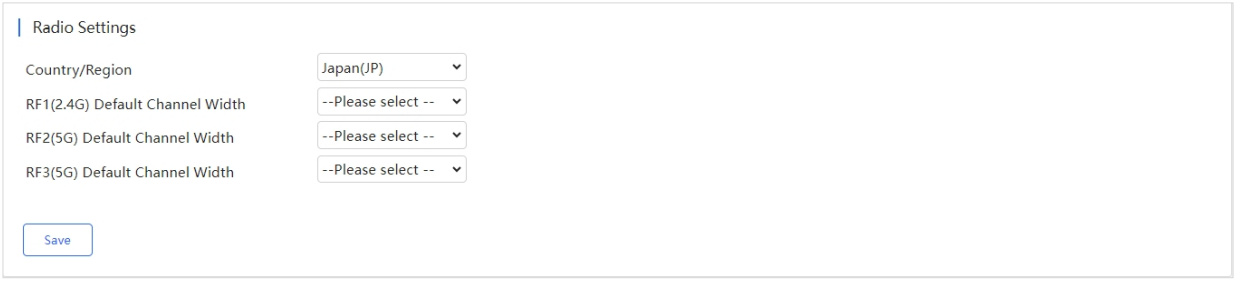
After the device is bound, you can unbind it in the following way:

Method: Select the device to be unbound, and then click **Remove Device**. When the prompt appears, click **OK** to complete the operation.

5.2.6 Radio Frequency Planning

Radio planning can adjust the channels and power of APs in the same area network, thereby optimizing the channel allocation and power of APs. Reasonable radio configuration planning can reduce channel interference, improve channel utilization, and enhance the overall performance and capacity of the wireless network. Click **Project** > **RF Planning** to enter the radio planning settings interface, which consists of three parts: **Radio Settings**, **Smart RRM**, and **Manual Planning**.

5.2.6.1 RF Settings



Items	Description
Country/Region	Defaults: Japan(JP)
RF1(2.4G) Default Channel Width	Defaults: N/A Options: 20 MHz/40 MHz
RF2(5G) Default Channel Width	Defaults: N/A Options: 20 MHZ/40 MHz/80 MHZ/160 MHZ
RF3(5G) Default Channel Width	Defaults: N/A Options: 20 MHZ/40 MHz/80 MHZ/160 MHZ **Note:** For Ruijie devices, RF3 is used to support the 5G 11ax (Wi-Fi 6) standard, which means it can deliver higher bandwidth and better performance.

5.2.6.2 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.

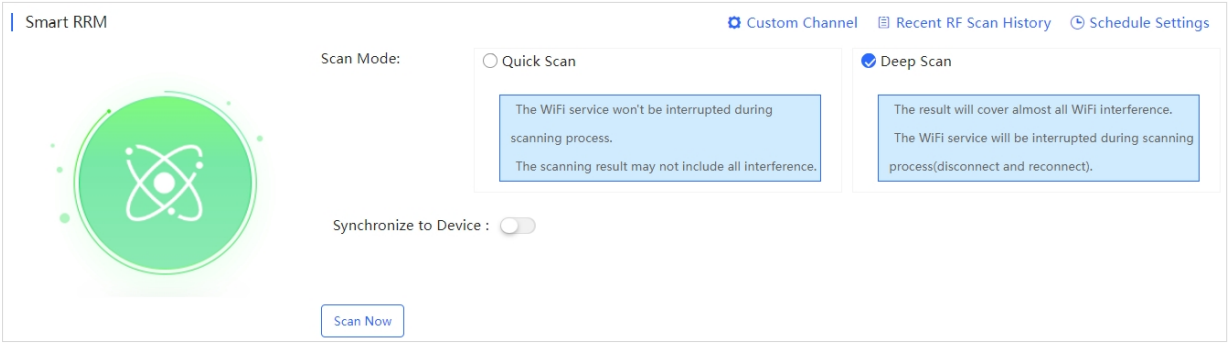
The entire process of the automatic RF planning includes three parts:

- 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.

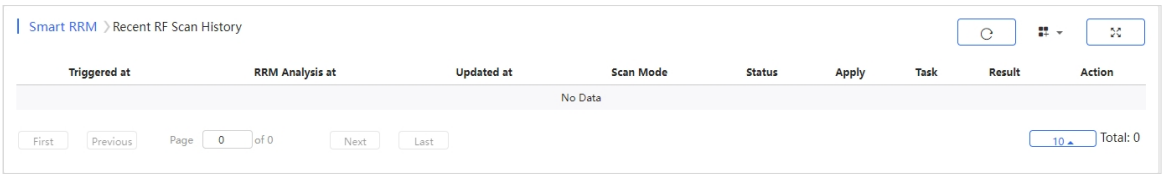
On **Smart RRM** page, the APs of a network can be triggered to scan the RF, display recommended RF configurations calculated after scanning, and save the recommended RF configurations to APs.



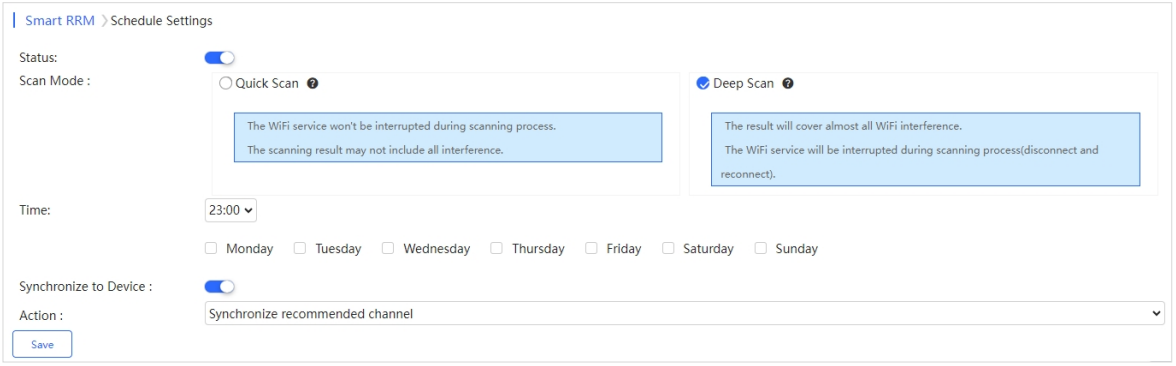
Items	Description
Scan Mode	Defaults: Deep Scan Options: ● Quick Scan: This mode enables APs to provide the Wi-Fi service properly during scanning. However, data acquired in this mode is not as accurate as that in the Deep Scan mode. This mode is applied when it is expected that the current network is 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 if you can accept that the clients go offline during the scanning.
Synchronize to device	Defaults: Disabled. When it is enabled, the RF scan results will be automatically pushed to the AP. The push types including: ● Synchronize recommended channels ● Synchronize recommended channels and power ● Synchronize recommended power of current channel 🕮 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.

- Click **Custom Channel** to enter the configuration interface. This function is disabled by default. When enabled, you can customize the 2.4 GHz and 5 GHz channels. After setting the channel according to the actual situation, click **Save** to complete the configuration.

- Click **Recent RF Scan History** to view the historical records of automatic RF scanning and planning. Each record displays the information obtained each time it is triggered, including the automatic RF scan trigger time, RRM analysis start time, update time, scan mode, status (Initializing/Scanning/RRM analysis/Finish/Failure), application status, results, and other information.



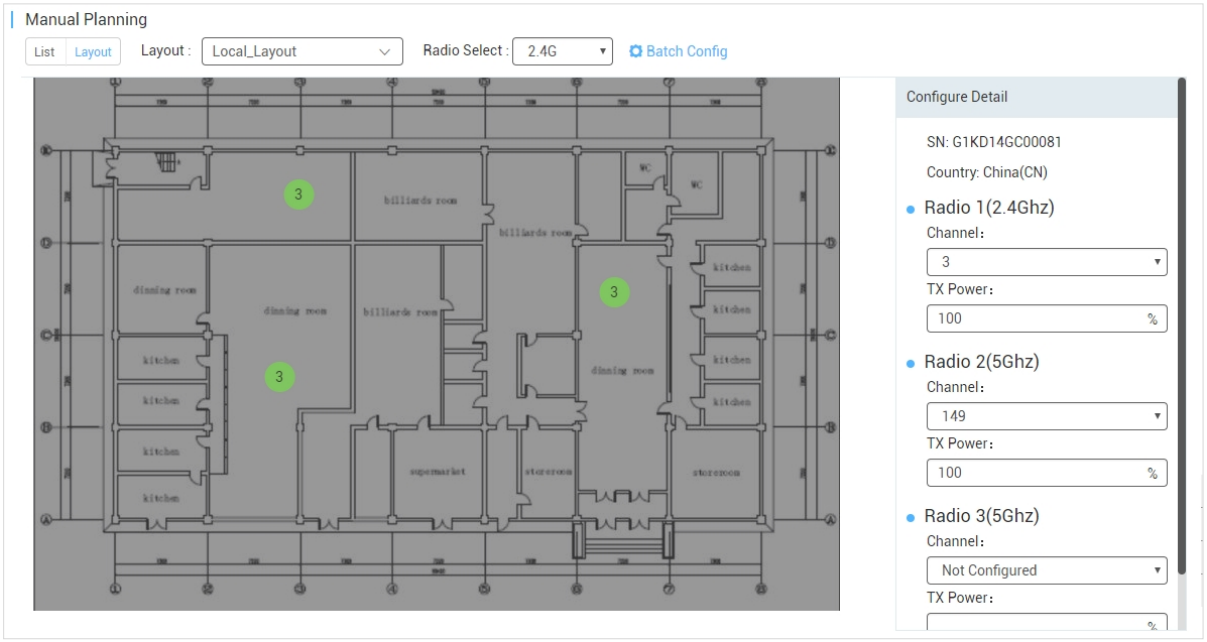
- Click **Schedule Settings** to start the RF automatic scan at a scheduled time. The scheduled scan function is disabled by default. After enabling it, you need to select the scan mode, set the time, and choose whether to synchronize the results to the device. And then click **Save** to complete the operation.



5.2.6.3 Manual RF Planning

On 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.

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.



Note

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

To perform manual RF planning, set the RF configurations of a location in one of the following ways:

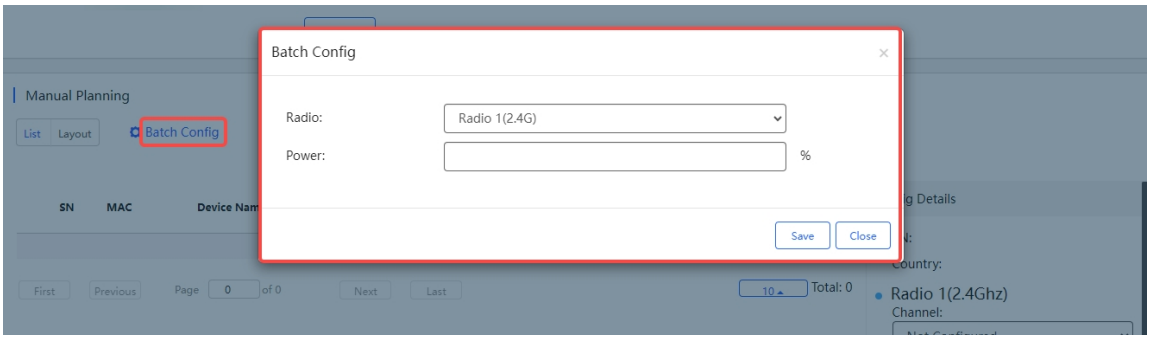
- Configure one location

  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 select the radio and configure the power percentage for all locations on a project.



If you need to synchronize the RF configuration of the corresponding location to the bound AP, click **Apply** above the location diagram to synchronize the RF configurations of the corresponding location to the bound AP. If you need to perform batch operations, click each location continuously and then click **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.

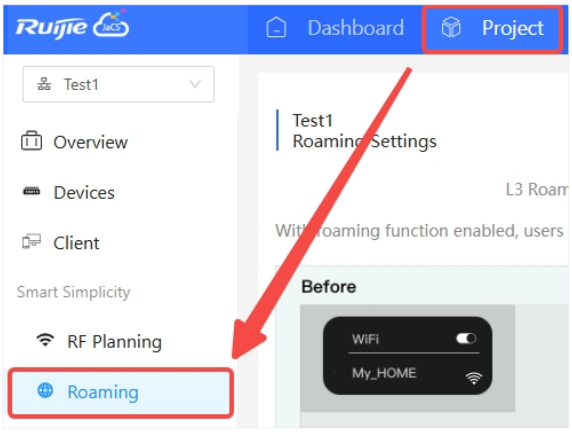
Note

If an unbind operation is performed, RF synchronization configuration will be removed from the AP.

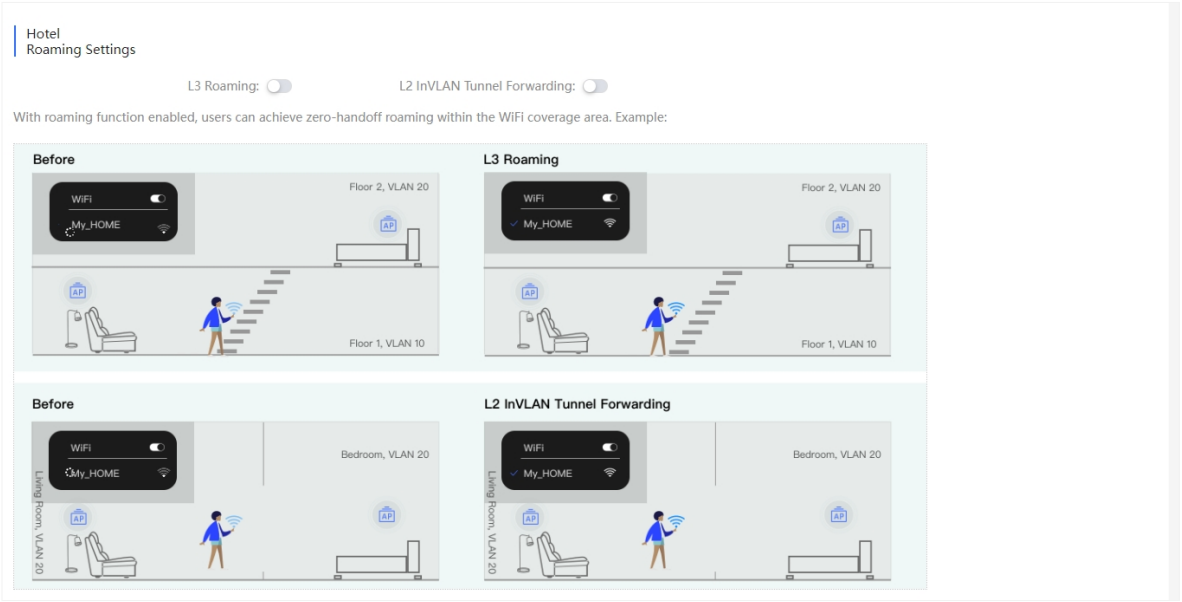
5.2.7 Roaming

Ruijie JaCS supports configuring the roaming function for a project with the scenario set to the **Hotel** or **Other**. With the roaming function enabled, users can achieve zero roaming within the Wi-Fi coverage area. The specific steps are as follows:

1 Click **Project** > **Roaming** to go to the wireless configuration interface.



2 Enable **L3 roaming** and **L2 InVLAN Tunnel Forwarding** as needed. L2 InVLAN forwarding mode and L3 roaming are disabled by default. These two roaming modes can be enabled at the same time.



Note

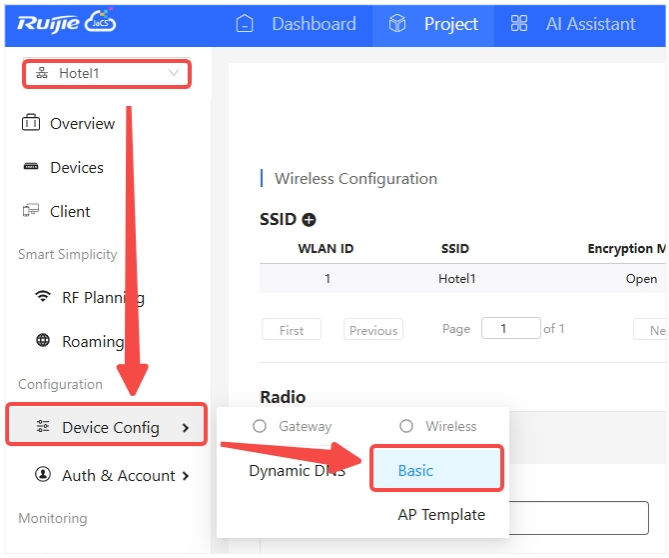
- The SSID signal must be consistent, otherwise roaming may fail.
- L2 roaming is suitable for small or medium-sized networks, especially offices, schools, or small businesses. It is recommended to be performed if all devices are in the same subnet and do not need to move across subnets. L3 roaming is suitable for large enterprises, campus networks, or places that require wide coverage. It is recommended to be performed if devices need to move between different subnets.

5.3 Configuring Captive Portal

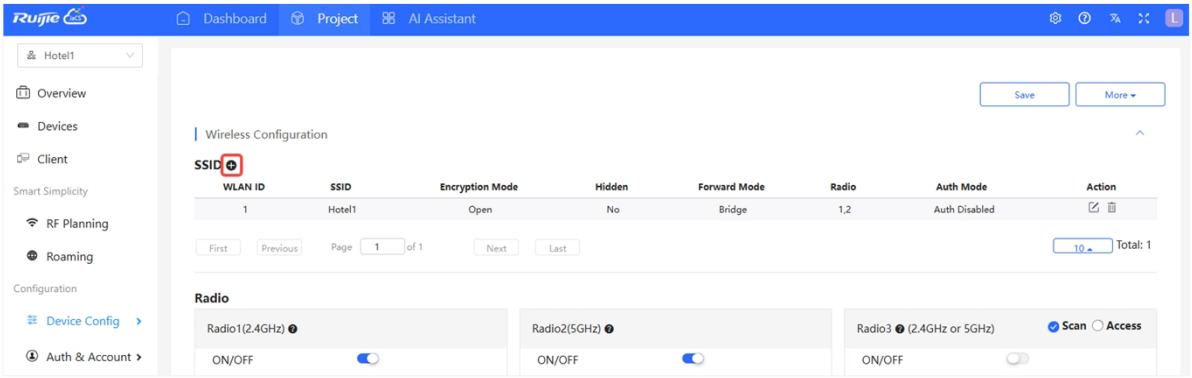
Ruijie JaCS supports configuring network WEB authentication for projects with the scenario set to Hotel or Other.

The specific steps are as follows:

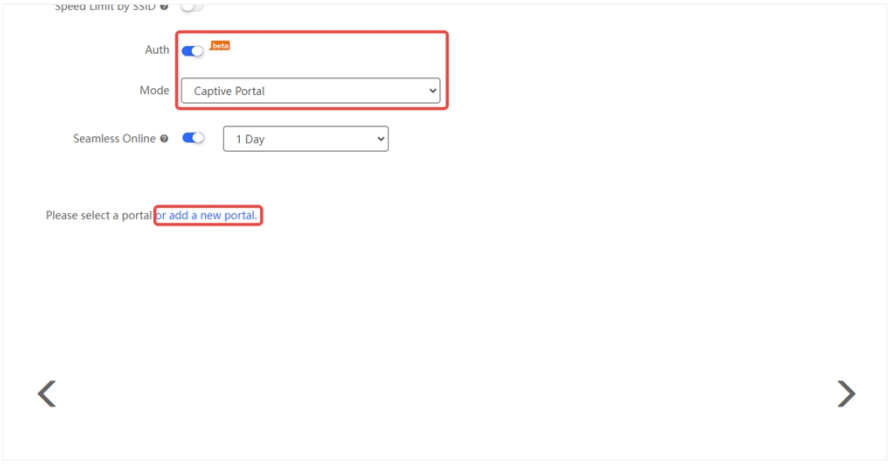
1 After selecting the project to be configured, click **Device Config** > **Basic** to enter the SSID creation interface.



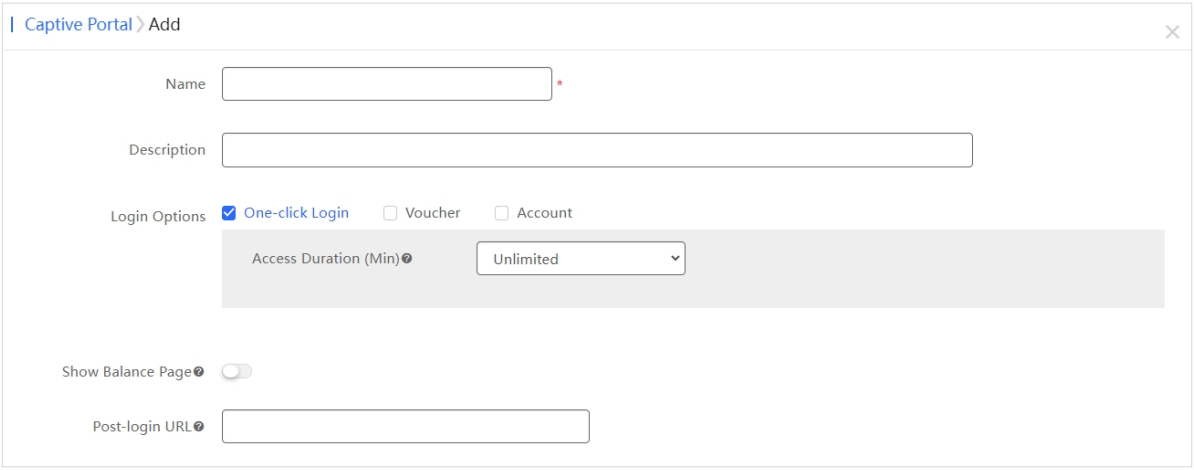
2 Click the **+** next to SSID to create an SSID. Or click to edit an existing SSID.



3 Turn on the authentication button, select **Captive Portal** as the authentication mode, and then click **or add a new portal** to create a captive portal.



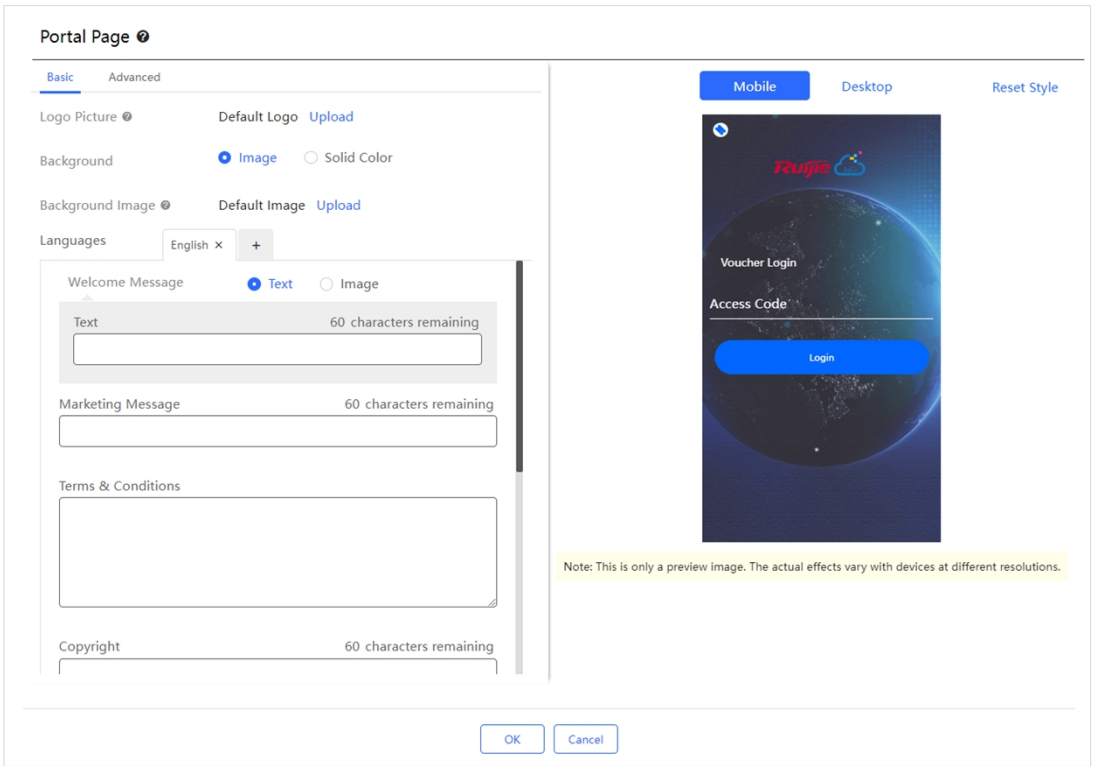
4 Set up the captive portal according to your actual needs.



Items	Description
Name	Required. Set the captive authentication portal name.
Description	Optional. Enter the description. Up to 200 characters are supported.
Login Options	**Defaults**: One-clink Login Options: One -click Login, Voucher, Account. (Multiple selection is supported.)
Show Balance Page	**Defaults**: Disabled. When this feature is enabled, the duration, number of times, or data available after portal authentication will be displayed. This function is invalid for gateway authentication.
Post-login URL	Set the URL. It must start with http or https, such as https://www.google.com.

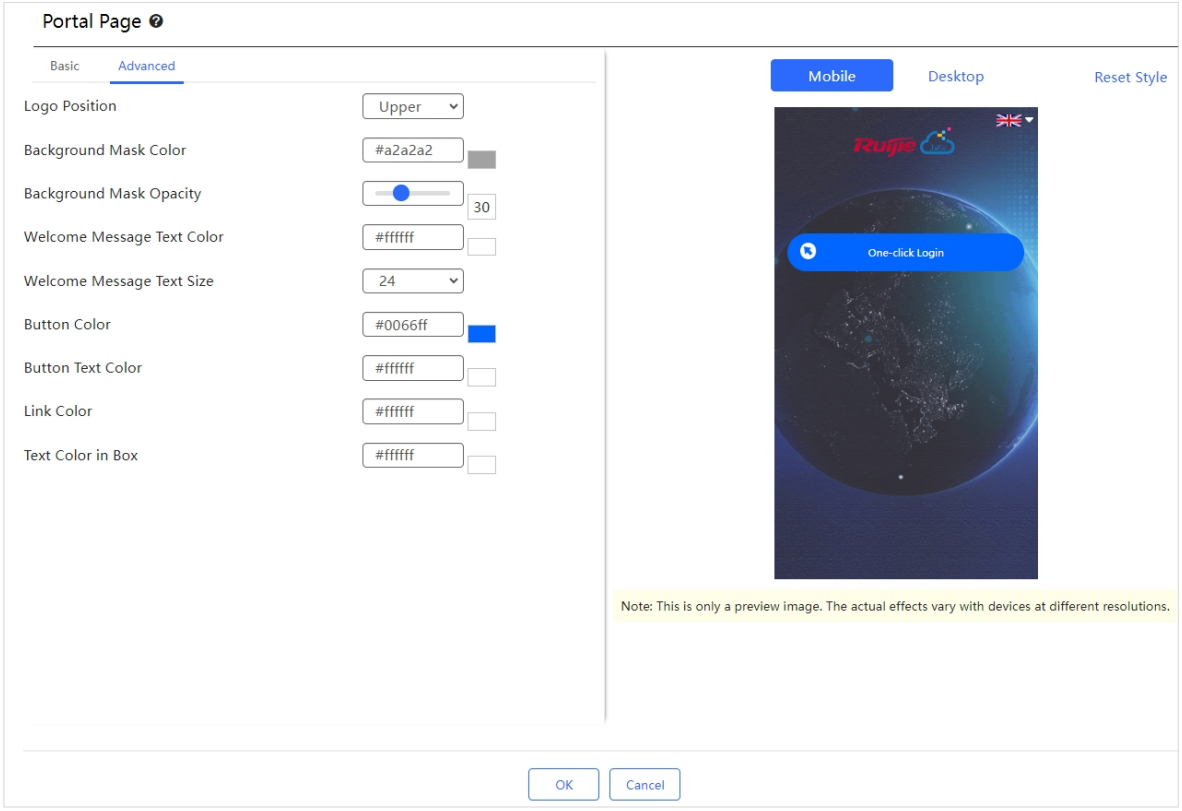
Customize the authentication portal interface. There are two types of interface settings: "Basic Settings" and "Advanced Settings".

Basic settings interface:



Items	Description
Login Picture	Set the logo to be displayed on the login interface. If no logo image is uploaded, the system logo will be used by default. Supported image formats: tif, pjp, jfif, ico, tiff, gif, svg, xbm, jxl, jpeg, svgz, jpg, webp, png, bmp, pjpeg and avif.
Back ground	Set the background image for the login interface. The default setting image is used. If you need to customize the background image, click **Upload** to upload a new one. If you need to set a solid color background, click **Solid Color** and select the background color.
Languages	Set the language of the authentication interface and the information displayed on the authentication interface. Support setting welcome message, marketing information, terms and permissions, as well as copyright information. Currently, up to three languages can be set each time. User can switch the language using the language switch icon in the upper right corner of the authentication interface.

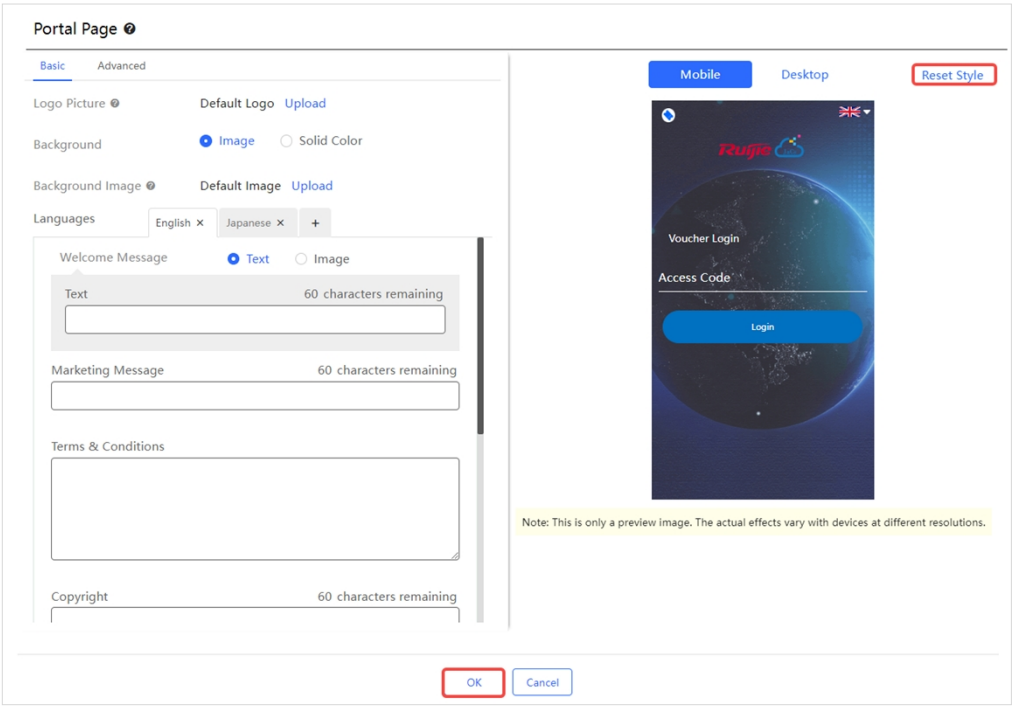
Advanced settings interface:



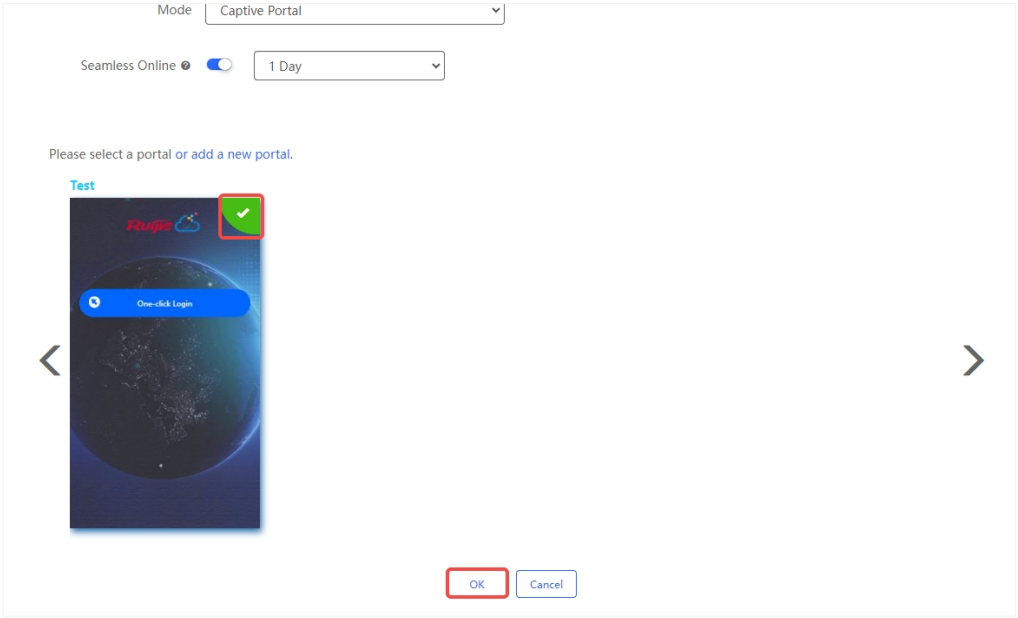
Items	Description
Log Position	Set the logo position on the authentication page. Defaults: upper. Options: Upper/Middle/Lower
Background Mask Color	Set the background mask color. Defaults: #a2a2a2
Background Mask Color	Set the background mask transparency. Defaults: 30
Welcome Message Text Color	Set the welcome message text color. Defaults: #fffff
Welcome Message Text Size	Set the font size of the welcome message text. Defaults: 24
Button Color	Set the button color.

	Defaults: #0066ff
Button Text Color	Set the button text color. Defaults: #ffffff
Link Color	Set the link color. Defaults: #ffffff
Text Color in Box	Set the color of the text in the box. Default: #ffffff

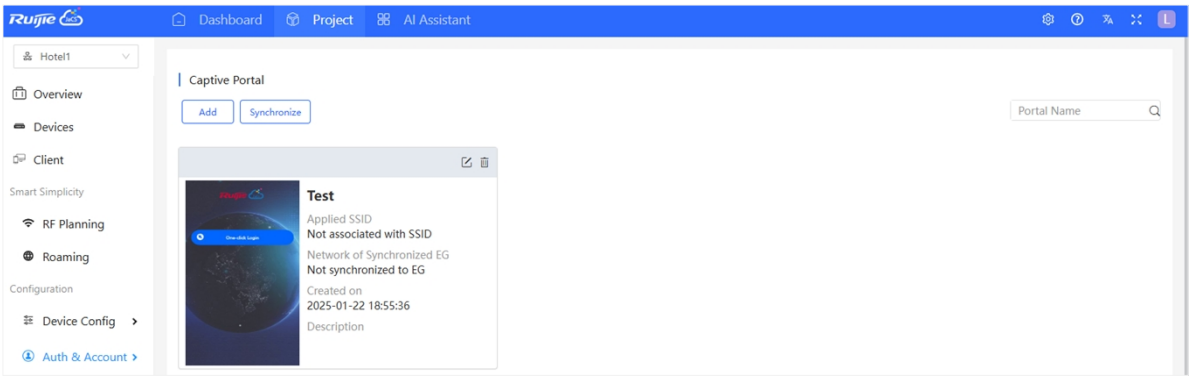
5 After configuring the authentication interface, you can preview the it on the right. If you need to reset the interface, click **Reset Style**. Otherwise, click **Save** directly.



6 After creating a new Captive Portal, you need to select the portal interface and click **OK** to complete the operation.



Click **Auth&Account** > **Captive Portal** to enter the Captive Portal management interface. All created Captive Portals will be displayed here. Click  and  in the upper left corner of the authentication portal to edit and delete it. If you need to synchronize the captive authentication portal to the EG product, click **Synchronize**. If the portal has been associated with an SSID or has been used in an EG product, you must cancel the association before deleting it.

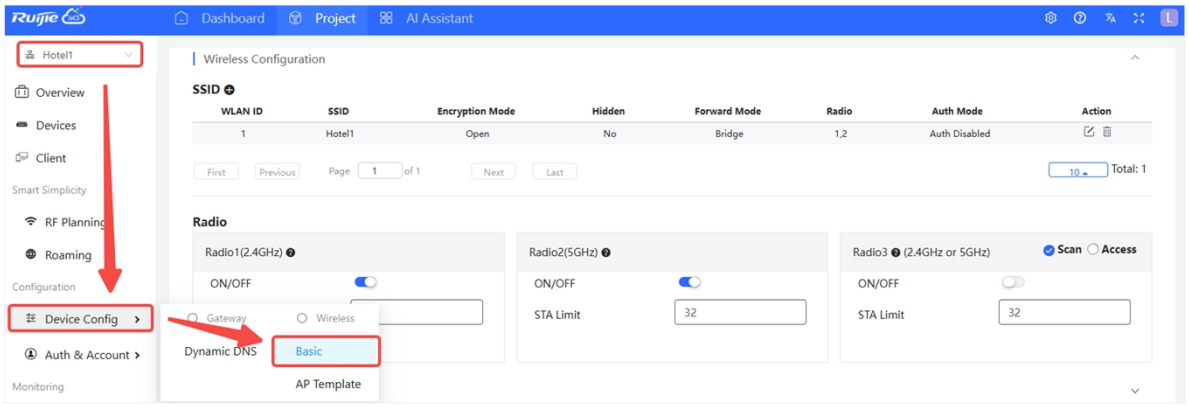


5.4 Configuring Voucher Authentication

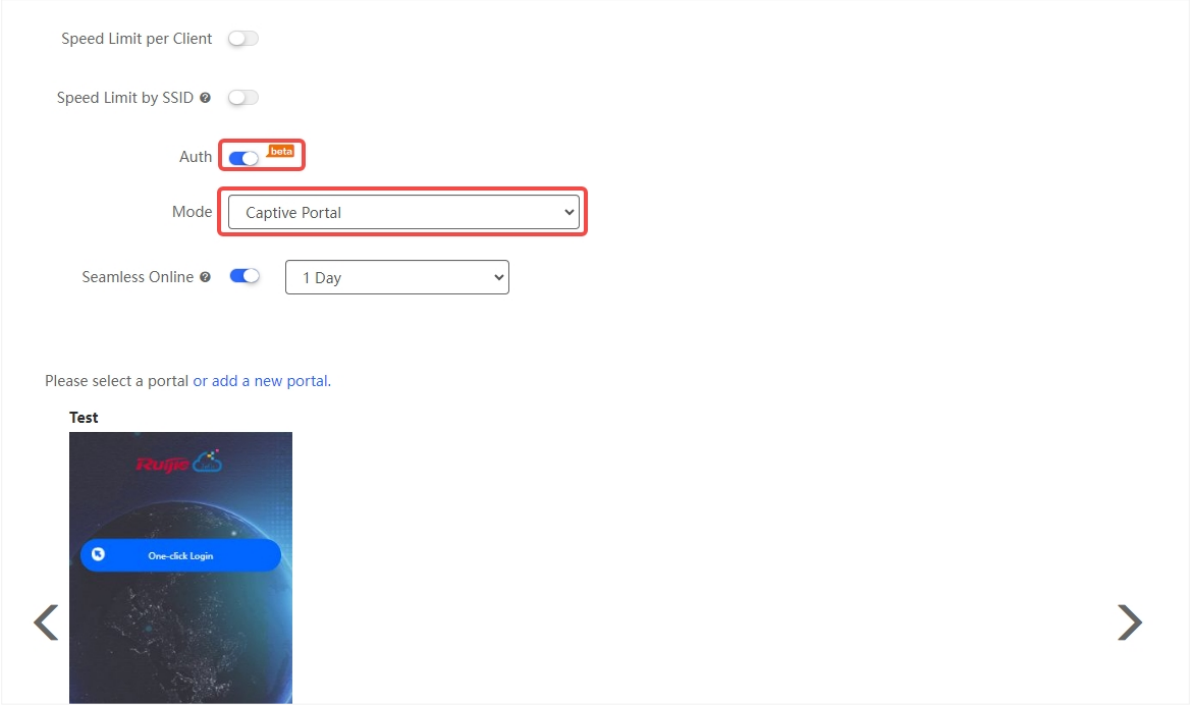
Voucher authentication is a simple portal authentication. Voucher authentication on Ruijie JaCS allows you to create access codes to guest for passing authentication and accessing wireless network. The number of concurrent users, network access duration and network speed limit and fees can be customized and offered to your guests.

The specific configuration steps are as follows:

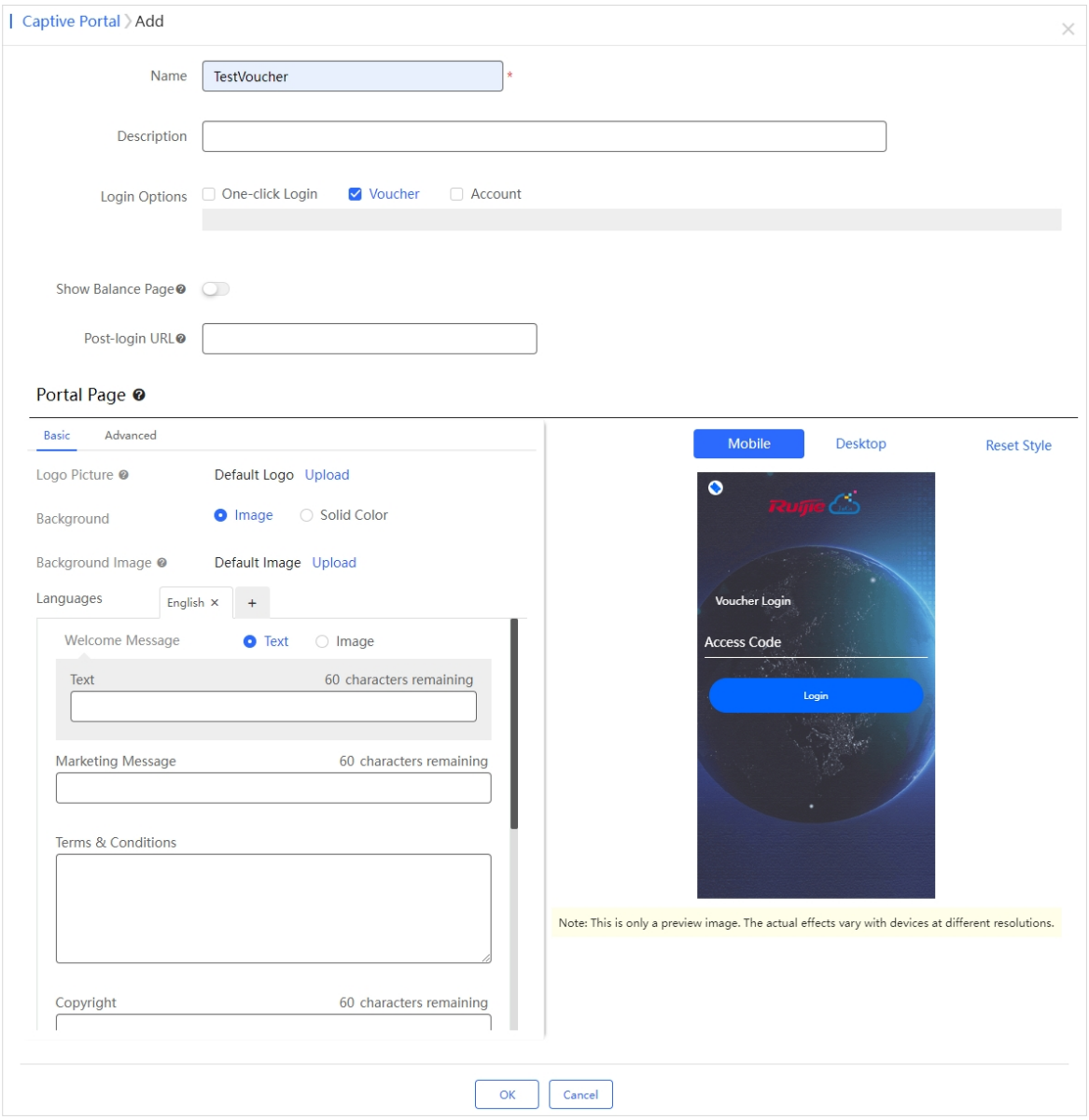
1 Select the project to be configured, and click **Device Config** > **Basic**.



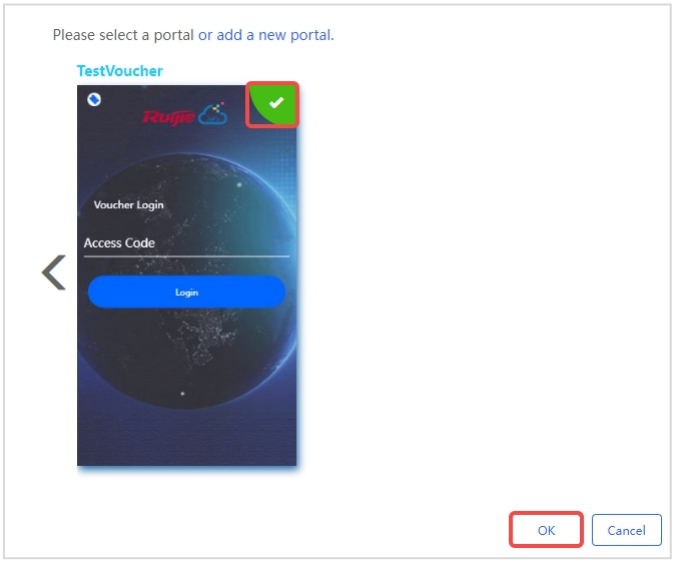
2 Click ⊕ to add a new SSID or click ✎ icon to edit an existing SSID. Enable the authentication function, and set the authentication mode to Captive Portal.



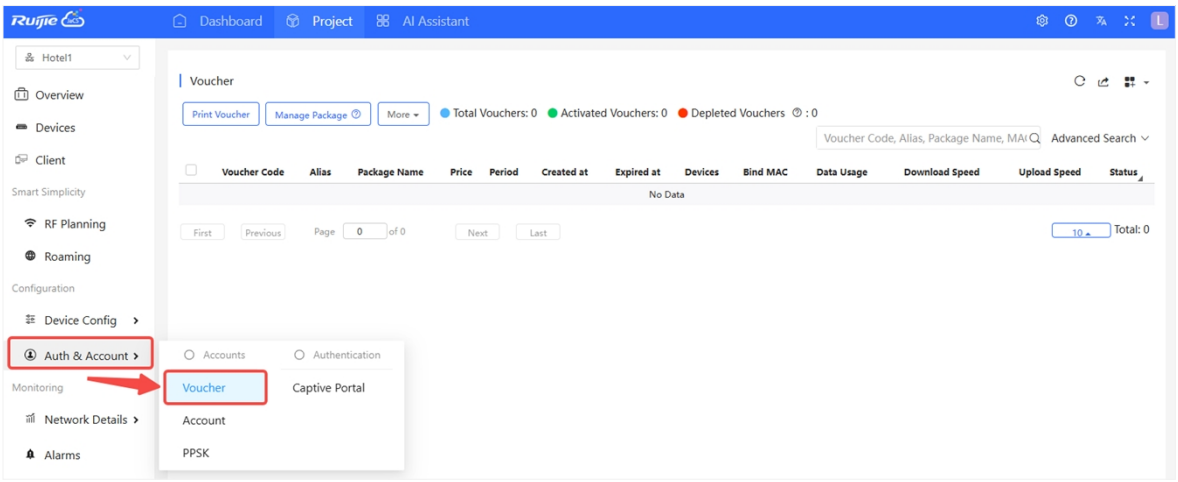
3 Click "**or add a new portal**", and fill in the basic portal information, including name, description, login options (remember to select **Voucher** in the login options), and authentication address, etc., and click **Save** to save the portal settings. For detailed introduction to the items in the captive portal setting page, refers to the Section 5.3.



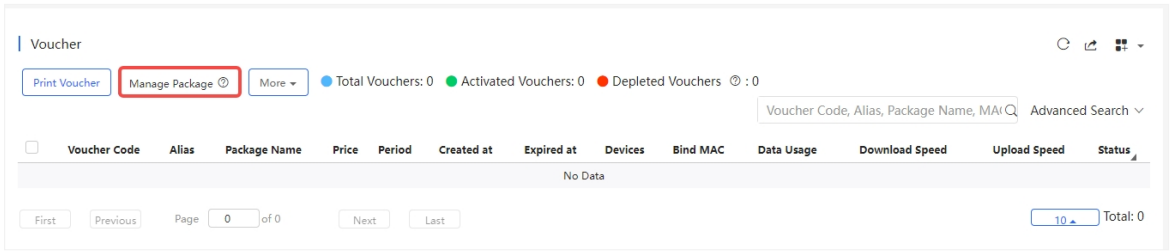
4 After setting the authentication interface, check the portal and click **OK** to complete the setting.

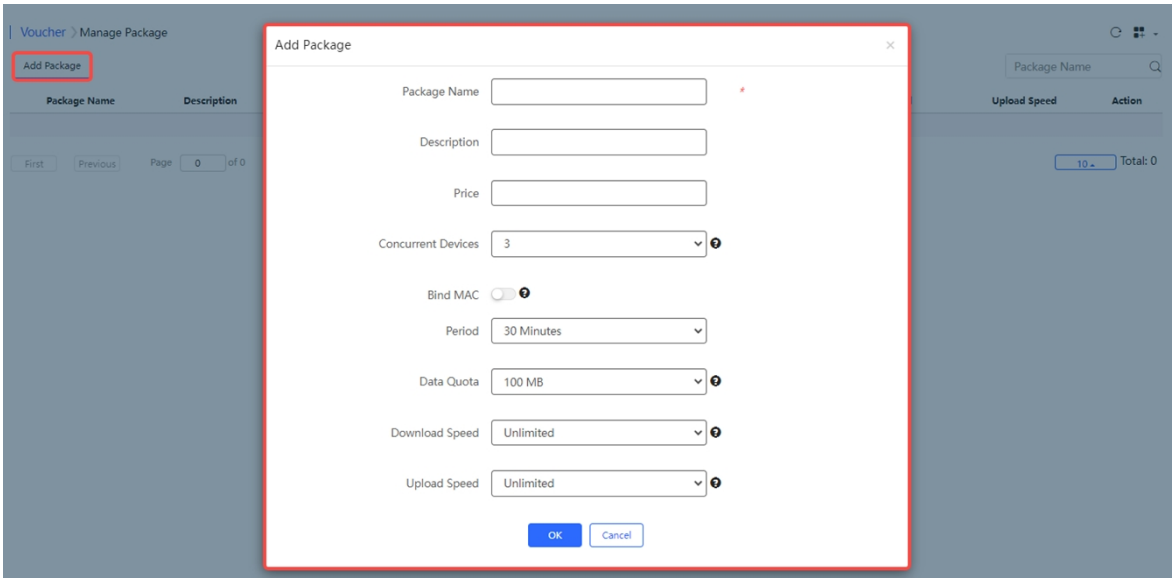


5 Click **Voucher** to go to the voucher management interface.



6 Click **Manage Package** to enter the management interface, click **Add Package** to add a package and then click **OK**.

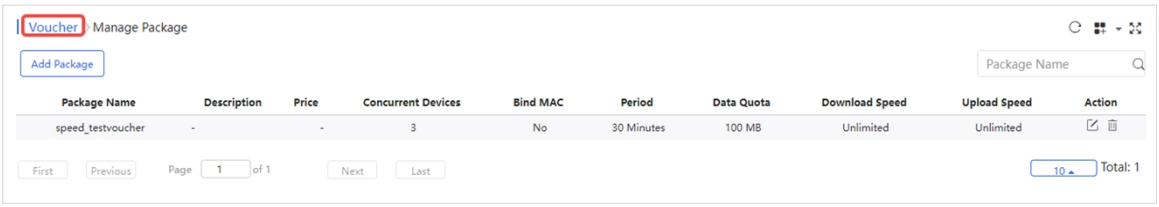




Items	Description
Package Name	Required. Enter a package name. Up to 32 characters is supported. Numbers, letters, and underscores are supported to be contained.
Description	Optional. Set the description of the voucher.
Price	Optional. Set the charge price. Support entering a price with two decimal places, and the maximum value is 100,000,000.00.
Concurrent Devices	Set the number of concurrent clients. The default value is 3.

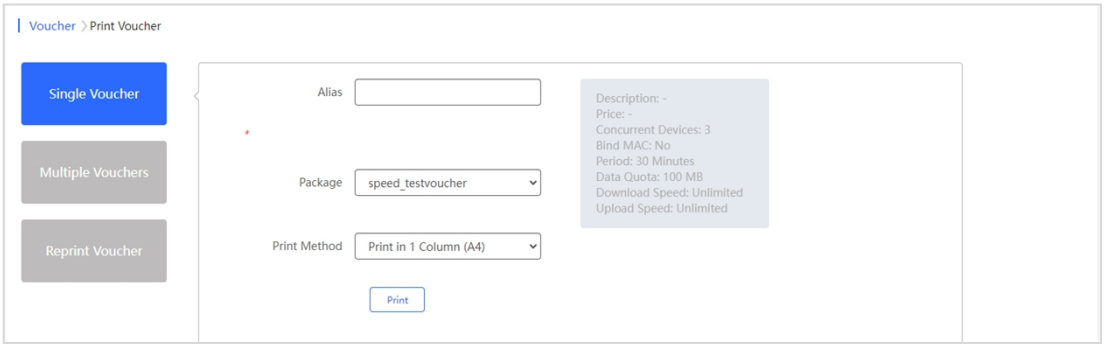
	Options: Unlimited /1/2/3/4/5/6/7/8/9
Bind MAC	Defaults: Disabled. When it is enabled, the voucher code used by a device will be bound with its MAC address.
Period	Set the validity period. During this validity period, the client is allowed to use the code to access the network. Defaults: 30 minutes. Options: Unlimited/30 minutes/1 hour/2 hours/1 day/2 days/1 week/2 weeks/30 days/Custom.
Data Quota	Set the data quota. Defaults: 100MB. Options: Unlimited/ 100M/200M/500M/1G/2G/Custom
Download Speed	Set download speed limit. Defaults: Unlimited. Options: Unlimited/256 Kbps/512 Kbps/1 Mbps/2 Mbps/5 Mbps/10 Mbps/Custom
Upload Speed	Set the upload speed limit. Defaults: Unlimited. Options: Unlimited/ 256 Kbps/512 Kbps/1 Mbps/2 Mbps/5 Mbps/10 Mbps/Custom

7 After configuration, the package will be displayed in the list. Click **Voucher** to return to the voucher management interface.



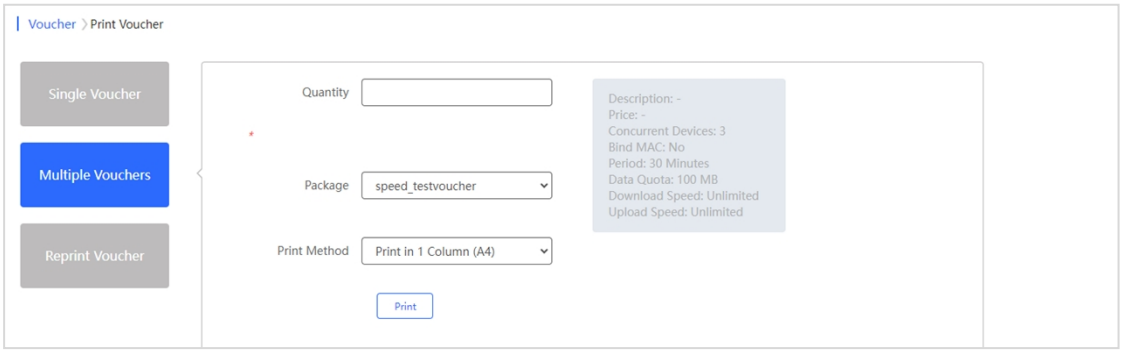
8 Click **Print Voucher** to enter the voucher printing interface. The printing interface supports printing single or multiple vouchers.

- **Print a single voucher:**



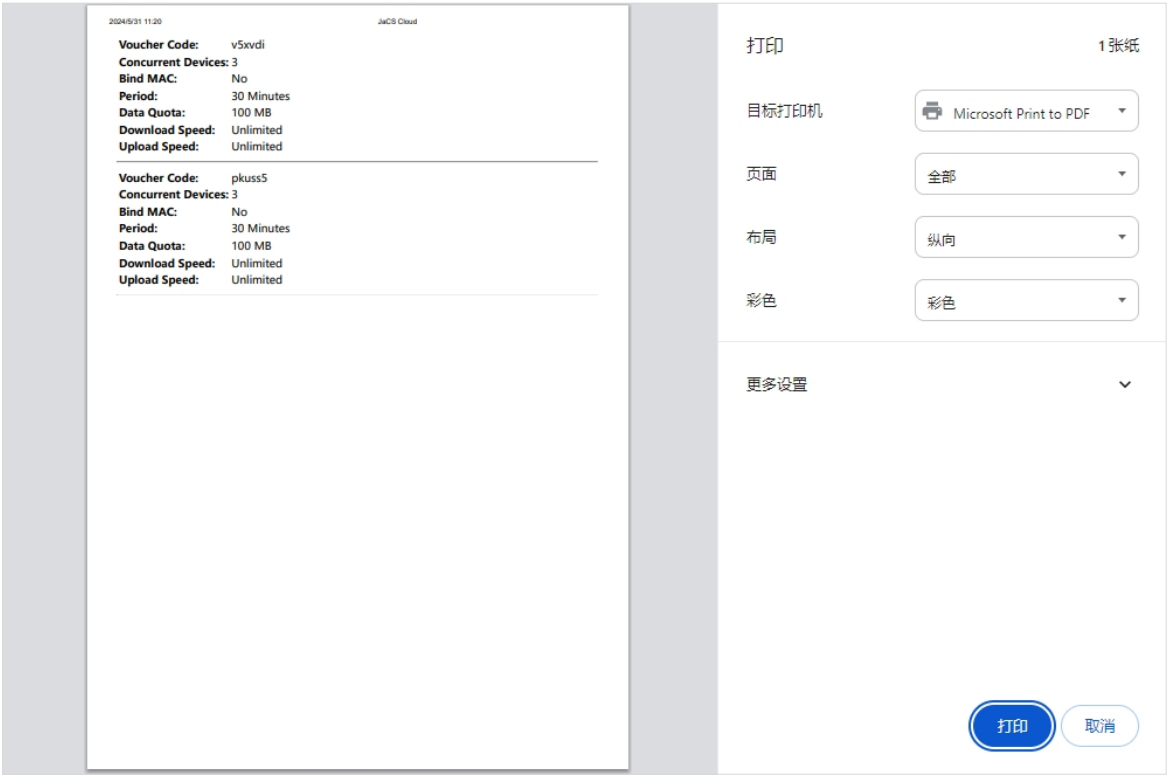
Items	Description
Alias	Up to 20 characters are supported.
Package	Select the voucher package you want to print.
Print Method	Defaults: Print in 1 Column (A4). Options: Print in 1 Column (A4)/Print on POS Receipt

- **Print multiple vouchers:**

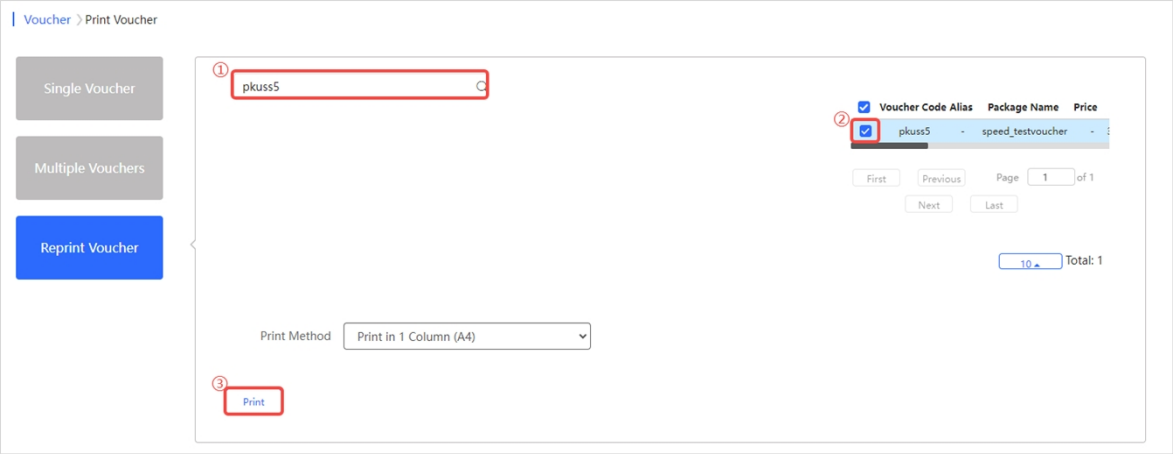


Items	Description
Quantity	Required. Set the number of packages to be printed. A maximum of 100 packages can be printed at a time.
Package	Select the voucher package you want to print.
Print Method	Defaults: Print in 1 Column (A4). Options: Print in 1 Column (A4) / Print on POS Receipt

9 After setting, click **Print** and a preview of the voucher will appear. After confirmation, click **Print** (the interface here is a preview of printing multiple vouchers).

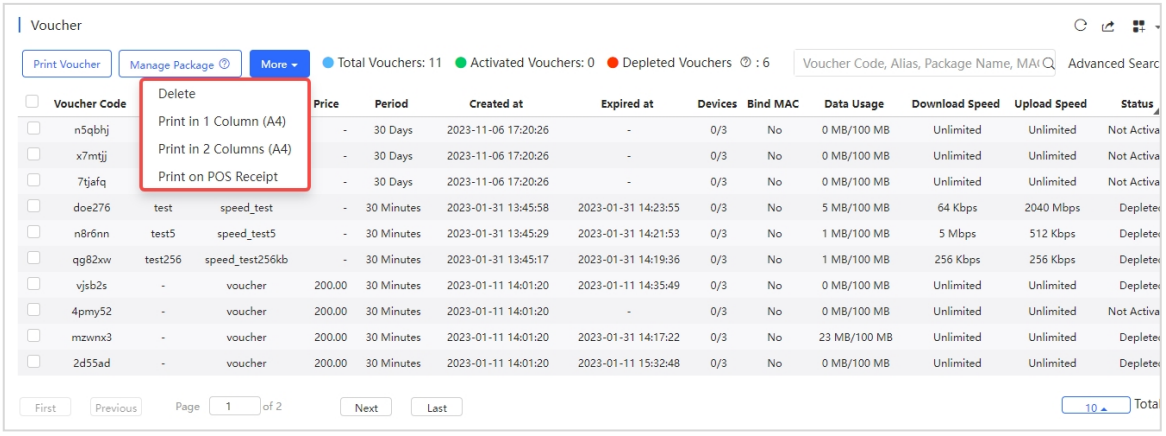


After printing, the voucher codes can be distributed to users, so that they can use the codes to pass authentication and access the network. If you need to reprint a previous voucher package, you can search for the previously printed voucher by voucher code, alias, voucher name, or bound MAC address, and select it, and then click **Print** to print it again.



All printed voucher package will be displayed in the **Voucher** list. When the MAC binding is enabled on a package, you can bind a device's MAC address with the voucher code. When the voucher status is activated or exhausted, you can click in the **Bind MAC** column to unbind the MAC address.

Click **More** to delete the selected print records, or change the print method.

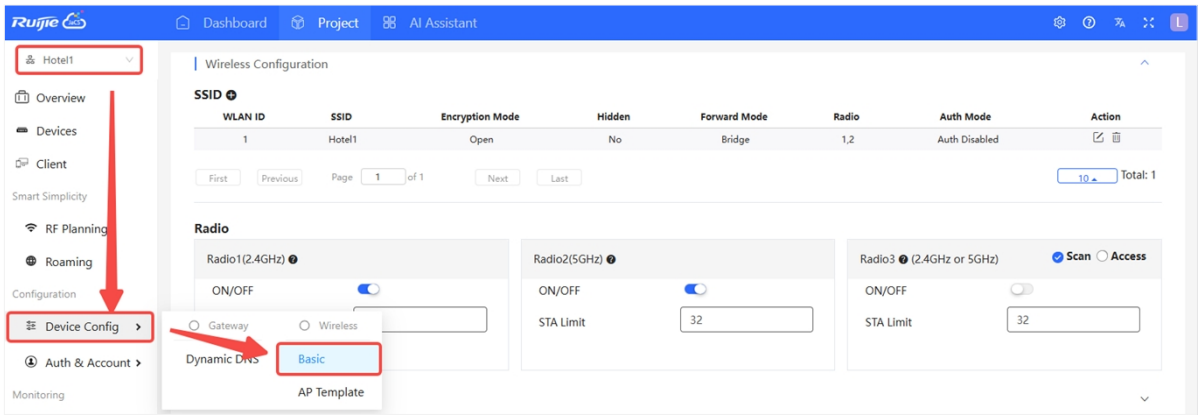


5.5 Configuring Account Authentication

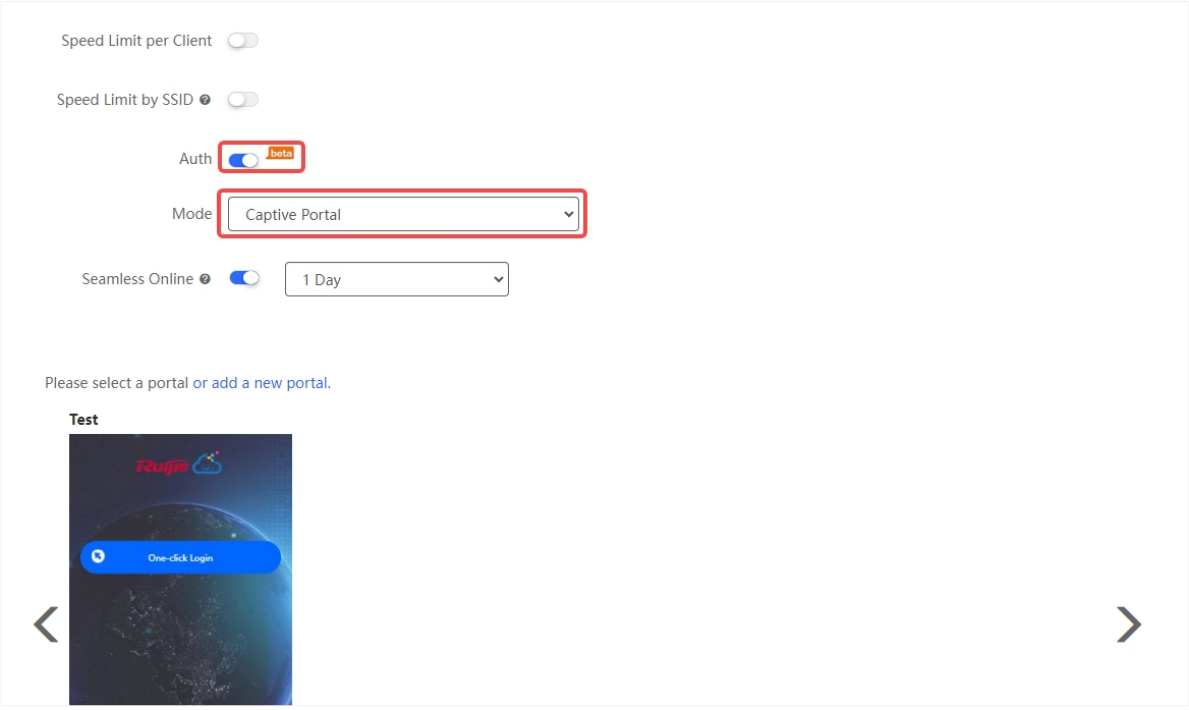
After the account authentication function is configured, the client needs to enter a valid account and password before accessing the Internet. It supports configuring the number of concurrent clients, time period, and traffic limit.

The specific steps are as follows:

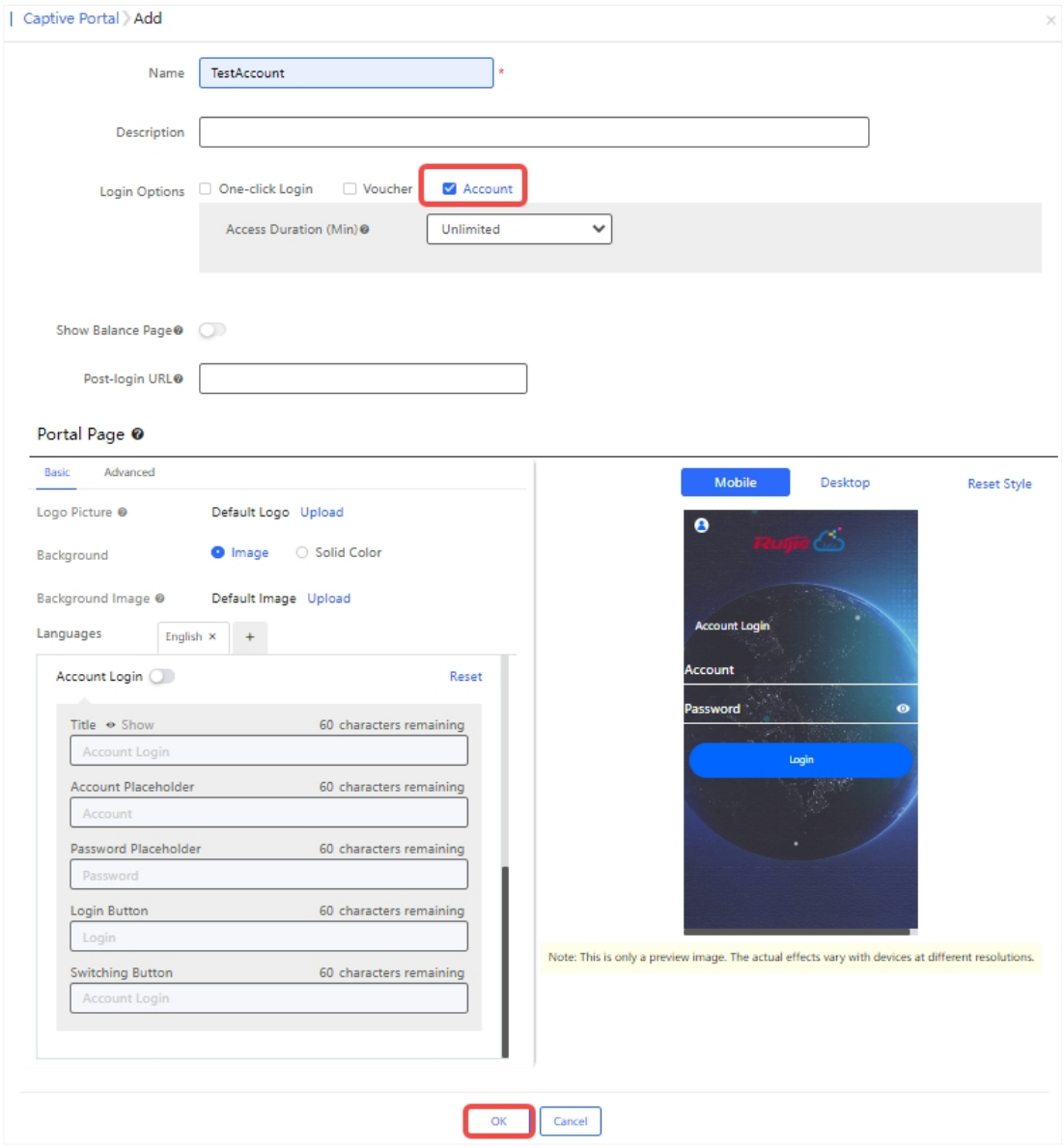
1 Select the project to be configured, and click **Device Config** > **Basic**.



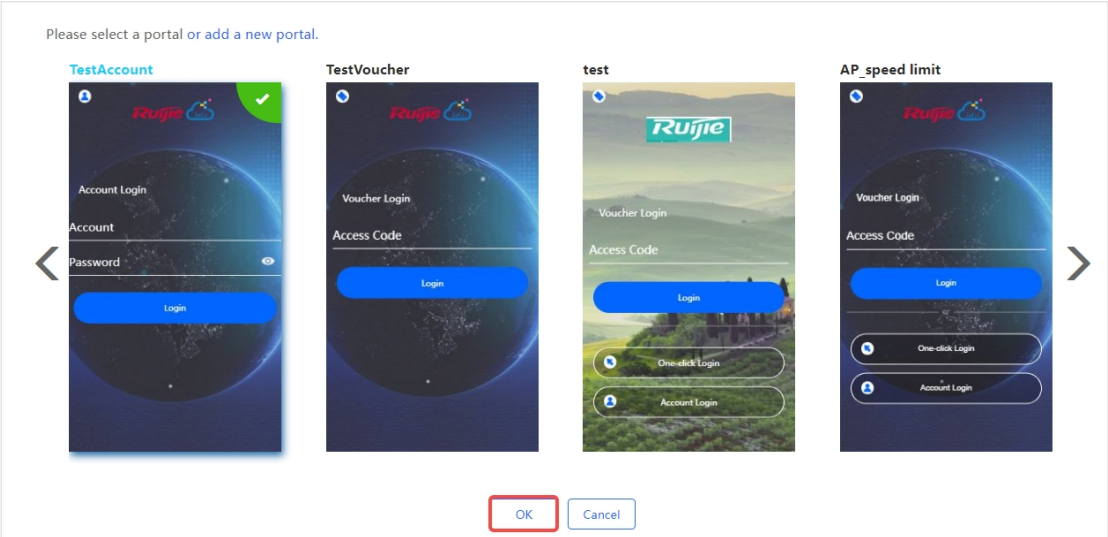
2 Click ⊕ to add a new SSID, or click ✎ to edit a SSID. Enable the authentication function for the SSID, and set the authentication mode to Captive Portal.



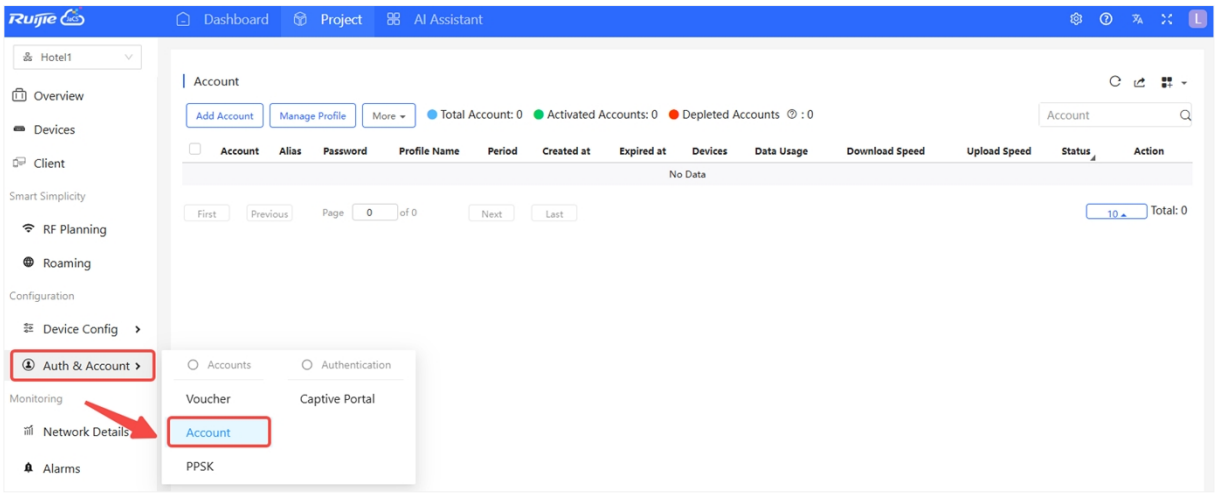
3 Click "**or add a new portal"** to create a new portal**.** In captive portal setting page, fill in the basic portal information, and check **Account** in the login options, set the portal page as needed, and then click **OK**.



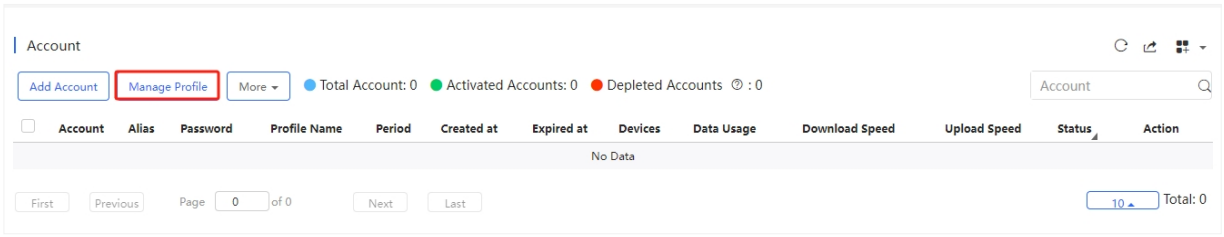
4 After setting up the portal authentication interface, select the portal, click **OK** to apply to the SSID.

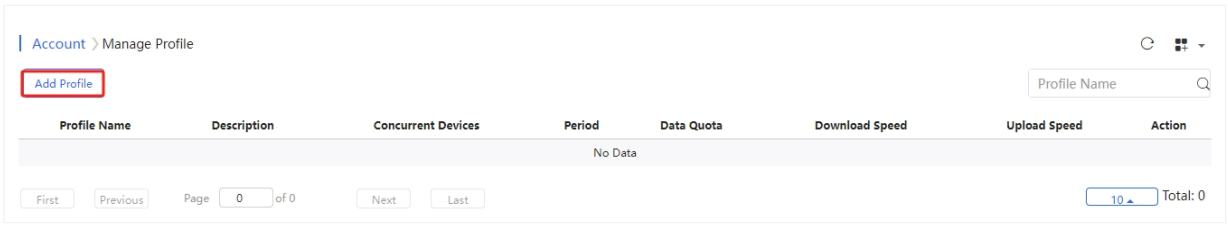


5 Click **Auth & Account** > **Account** to enter the account authentication configuration interface.

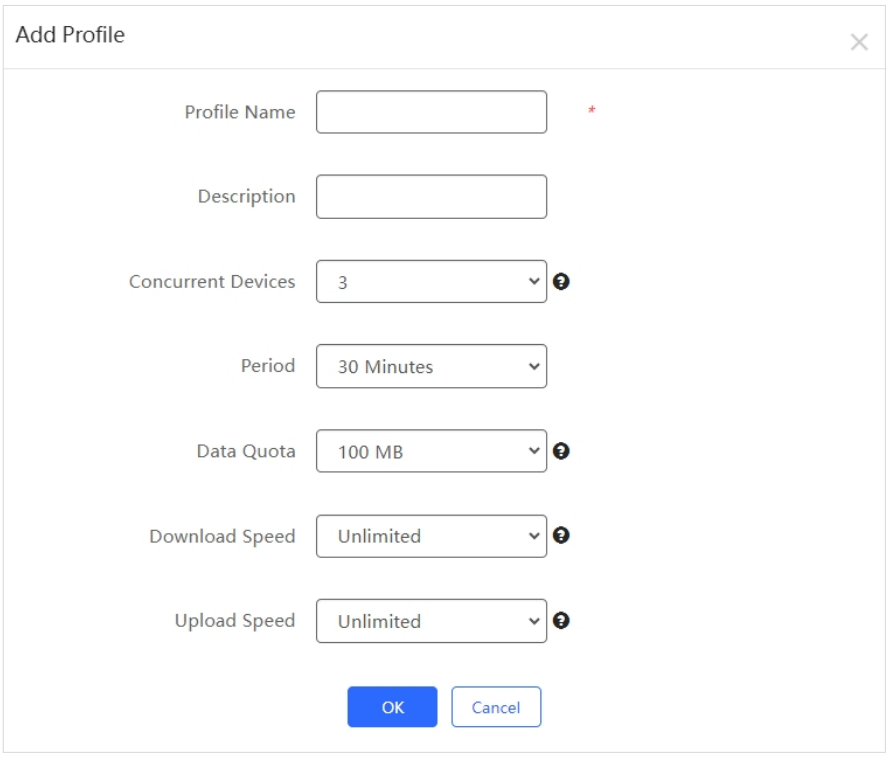


6 Click **Manage Profile**, and click **Add profile** to add a profile.



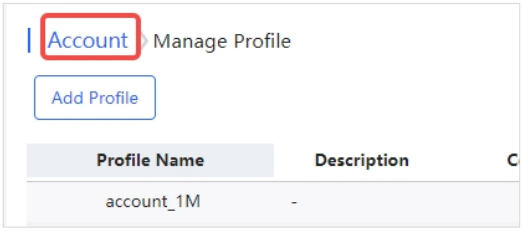


7 Fill in the profile information, and the click **OK**.



Items	Description
Profile Name	Required. Enter a profile name. The supported name length is up to 32 characters. Numbers, letters, and underscores can be contained.
Description	Optional. Up to 28 characters are supported.
Concurrent Devices	Set the number of concurrent devices. Defaults: 3. Options: Unlimited/1/2/3/4/5/6/7/8/9
Period	Set the validity period. During this validity period, the client is allowed to use the account and password to access the network. Defaults: 30 minutes. Options: Unlimited/30 minutes/1 hour/2 hours/1 day/2 days/1 week/2 weeks/30 days/Custom.
Data Quota	Set the traffic quota. Defaults: 100MB. Options: Unlimited/100M/200M/500M/1G/2G/Custom
Download Speed	Set download speed limit. Defaults: Unlimited Options: Unlimited/256 Kbps /512 Kbps /1 Mbps/2 Mbps/5 Mbps/10 Mbps/ Custom
Upload Speed	Set the upload speed limit. Defaults: Unlimited. Options: Unlimited/ 256 Kbps /512 Kbps /1 Mbps/2 Mbps/5 Mbps/10 Mbps/ Custom

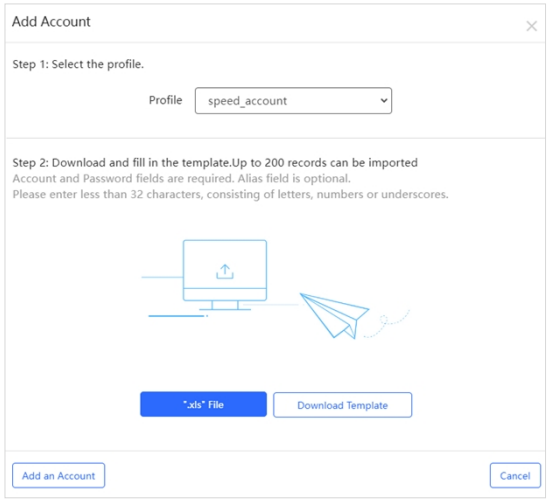
8 After configuring the profile, click **Account** to return to the account management interface.



9 Click **Add Account** to set account information. You can set account information in batches or for a single account.

Batch settings:

1) Select a profile.

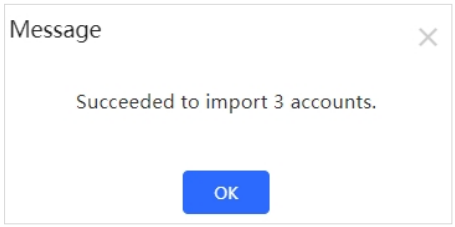


2) Click **Download Template** to download and fill in the template. You can configure up to 200 account information at a time.

Account	Password	Alias

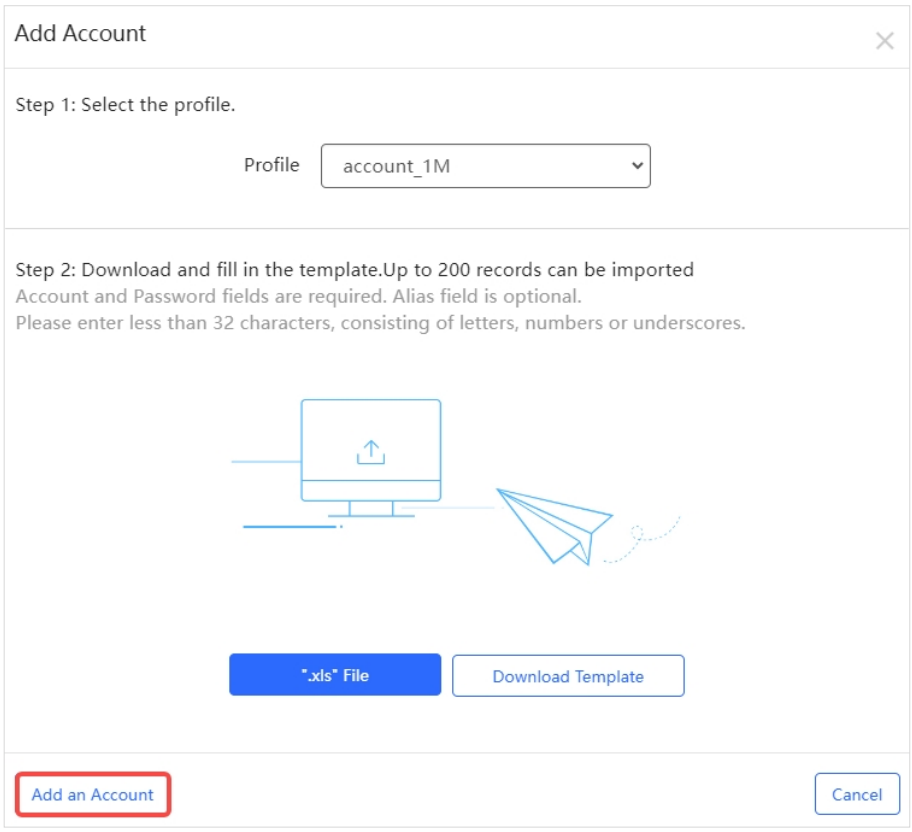
Items	Description
Account	Required. Set the account name.
Password	Required. A password can be up to 32 characters and can contain letters, numbers, and underscores.
Alias	Optional. Set an alias.

3) After filling in the template, click **".xls" File** to upload the template. After the prompt appears, the configuration is completed.

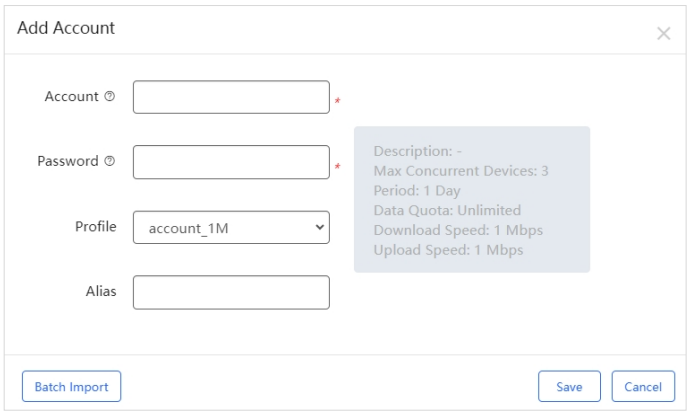


To create a single account:

1) Click **Add an Account**.

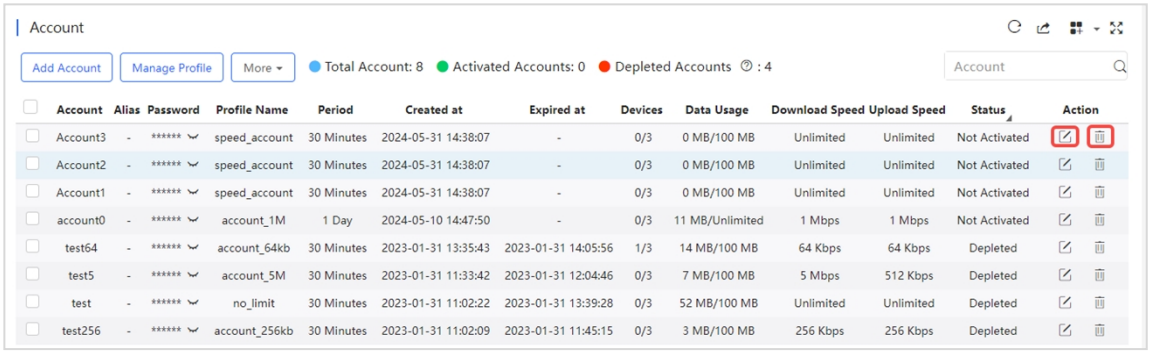


2) After setting the account information, click **Save**.

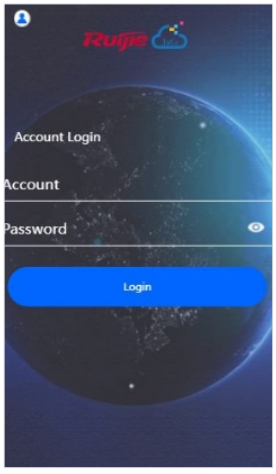


Items	Description
Account	Required. Set the account name.
Password	Required. A password can be up to 32 characters and contain letters, numbers, and underscores.
Profile	Required. Select a profile.
Alias	Optional. Set an alias. The alias should be between 2 and 32 characters and contain letters, numbers, and underscores.

After the import is successful, the account information will be displayed in the account list. If you need to edit the account information, you can click the icon in the **Action** column to edit it; if you need to delete the account information, you can click to delete it.



With the account authentication enabled, clients will be required to enter the account name and password, and the click Login to access the network when they connect to the SSID.



5.6 Configuring PPSK

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”.

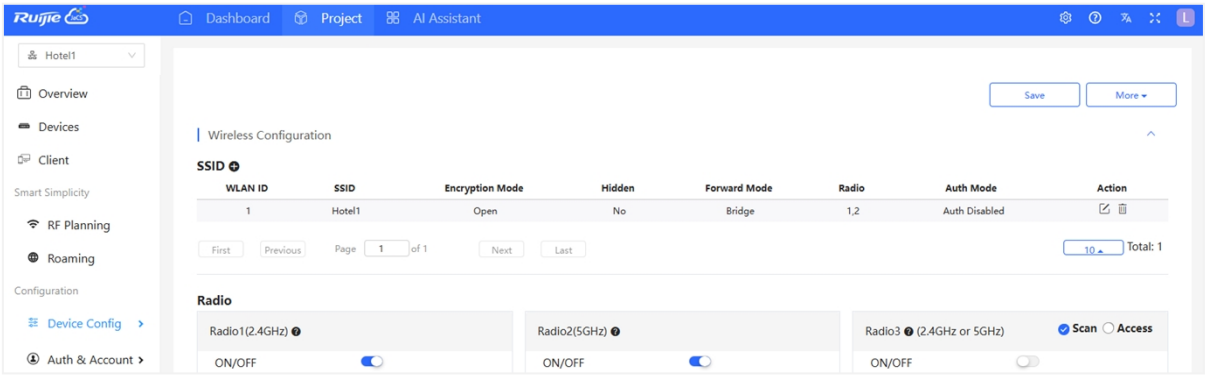
The main tasks of the PPSK administrator are:

- 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 batches.

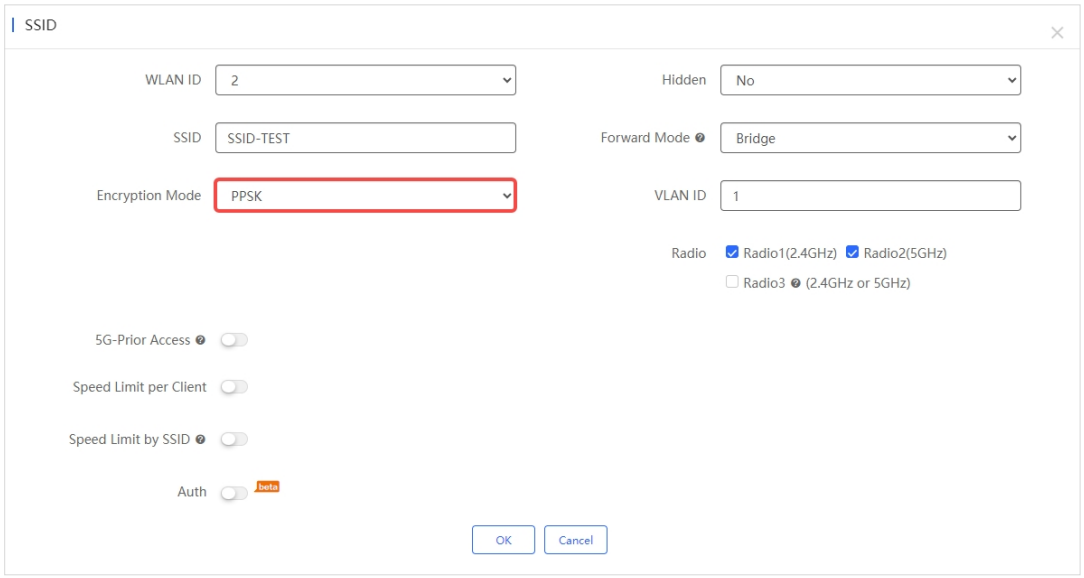
Staffs can connect to the SSID with a unique WiFi key allocated by the administrator to access the Internet.

The specific configuration steps are as follows:

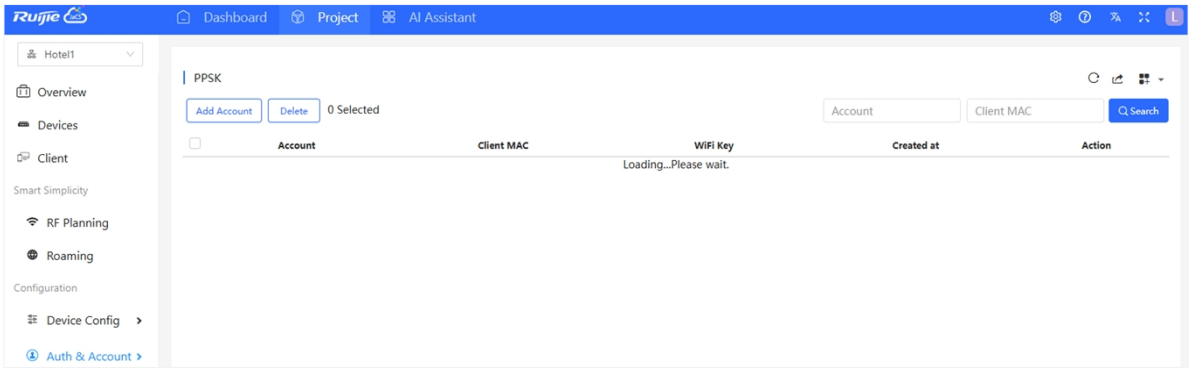
1 Select the project to be configured, and click **Device Config** > **Basic**.



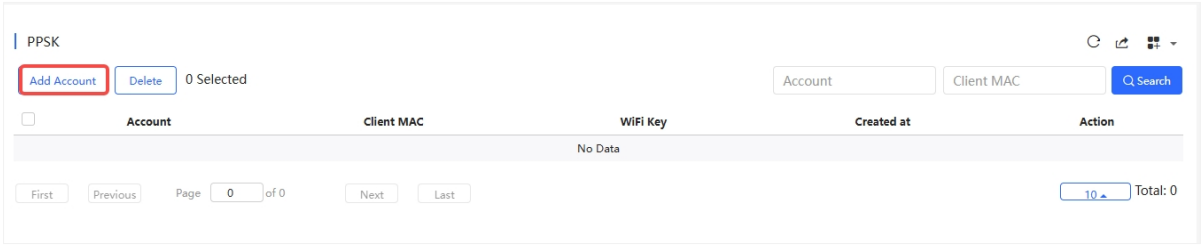
2 Click ⊕ to add a new SSID or click the ✎ to modify an existing SSID. In the SSID configuration page, set the encryption mode of the SSID PPSK, and then click **OK**.



3 After the configuring the SSID, click **Auth&Account** > **PPSK** to enter the PPSK configuration interface.



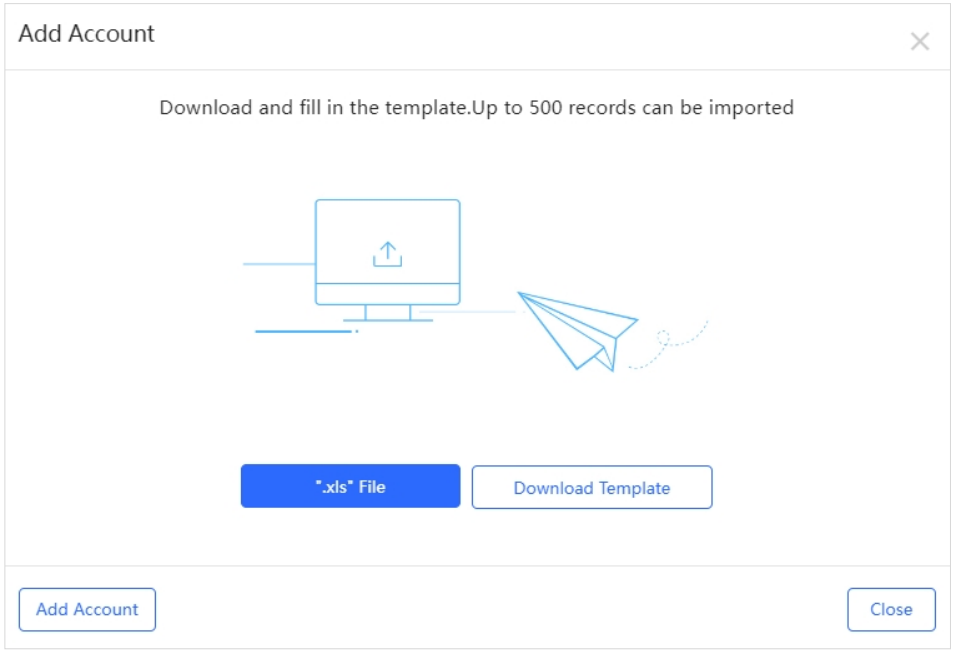
4 Click **Add Account** to enter the creation interface.



- Creating account in batches:

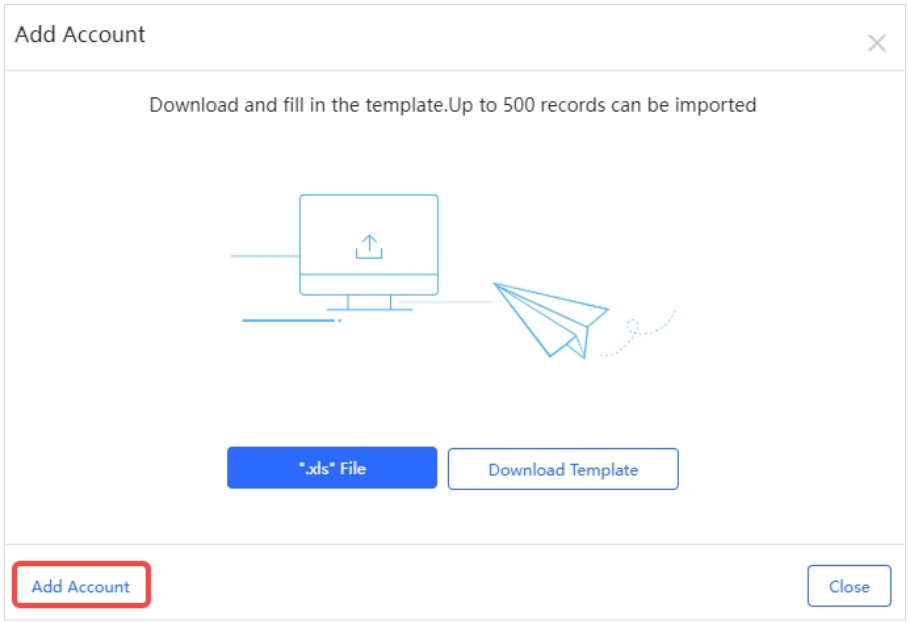
  1) Click **Download Template** to download the batch configuration template.

  2) After filling in the account information in the template, click **".xls" File** to upload the template.

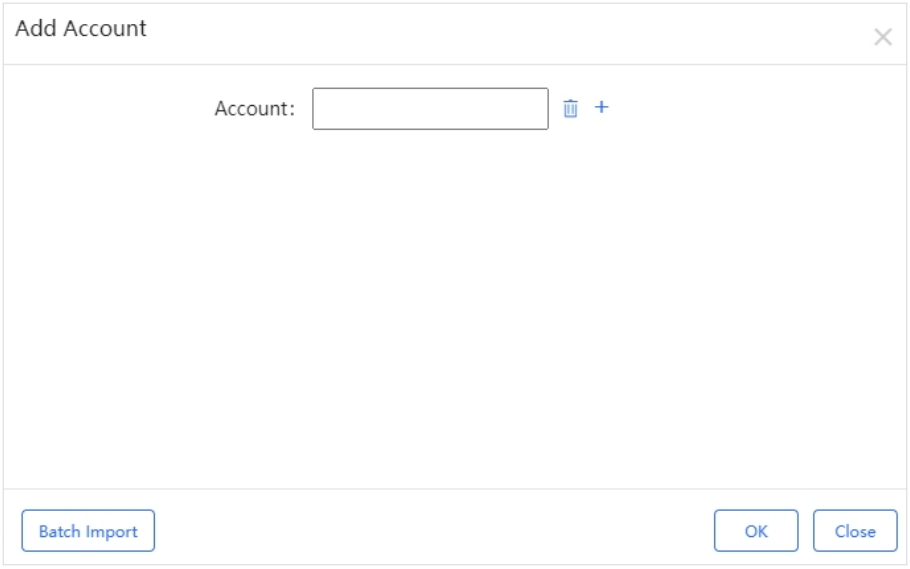


- Create a single account:

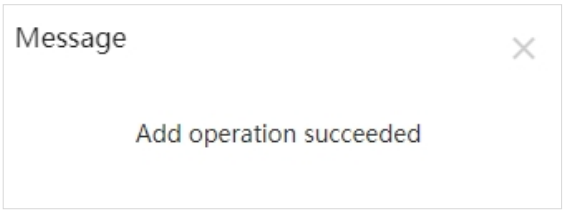
  1) Click **Add Account**.



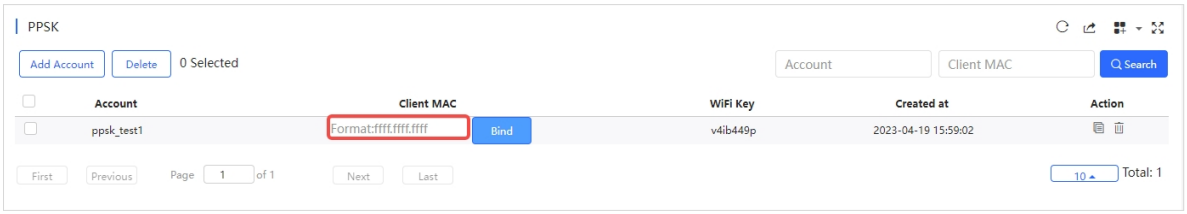
2) Enter the account name (up to 32 characters can be entered), and then click **OK**. To add multiple accounts, click **+** to add them.



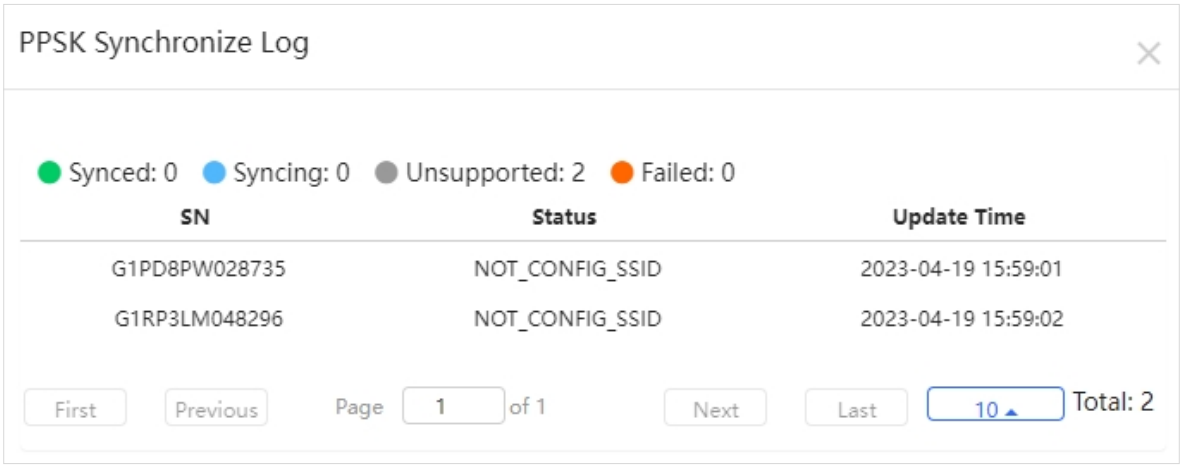
3) When the "Add operation succeeded" prompt appears, the operation is completed. The added account will be displayed in the PPSK list.



5 Enter the MAC address, and then click **Bind** to bind the MAC address. If the MAC address is not bound, the configuration will not take effect on any client.

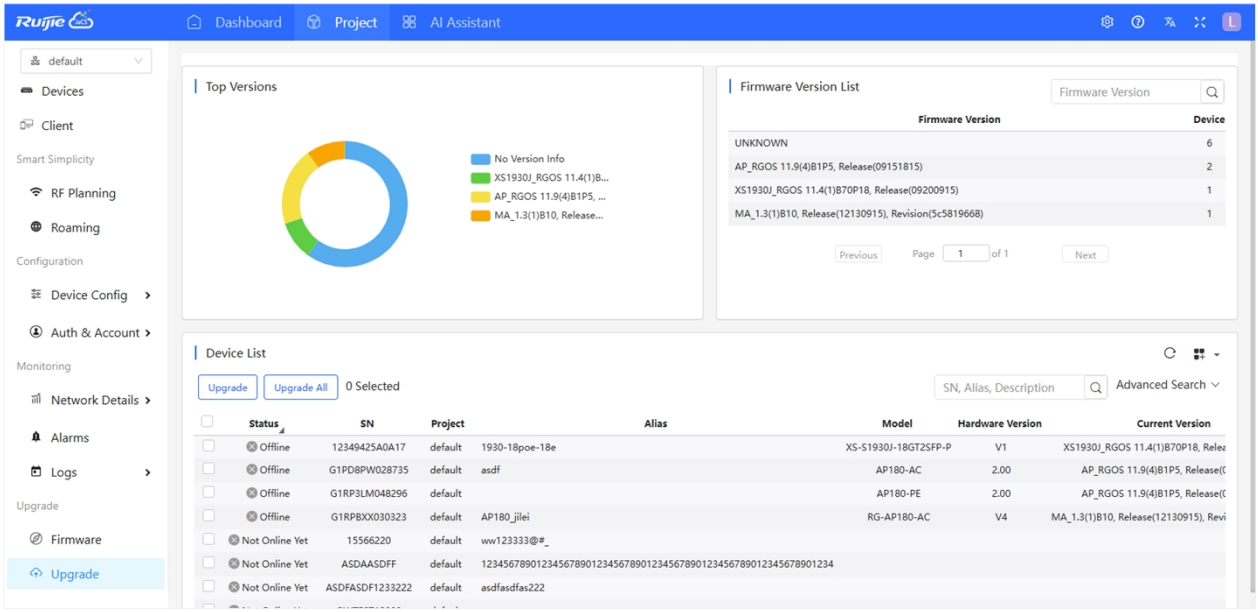


Click  in the **Action** column to view the synchronization log of PPSK.



6 Device Upgrade

Ruijie JaCS supports online upgrade of device firmware. Administrators can easily manage firmware versions on the project, upgrade devices or view firmware versions through the JaCS.

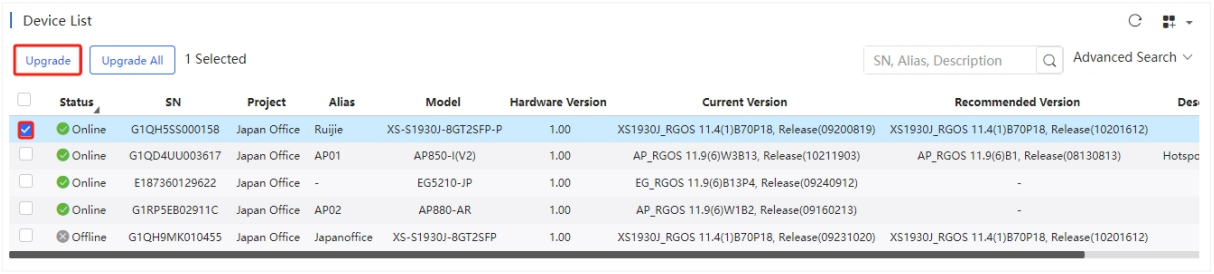


Modules	Description
Top Version	Displays the top 5 firmware versions in the current project.
Firmware Version List	Displays the firmware versions available in the project and the number of devices to which the firmware version can be applied.
Device List	Displays the device information in the current project. You can perform online firmware upgrades on the device in this interface.

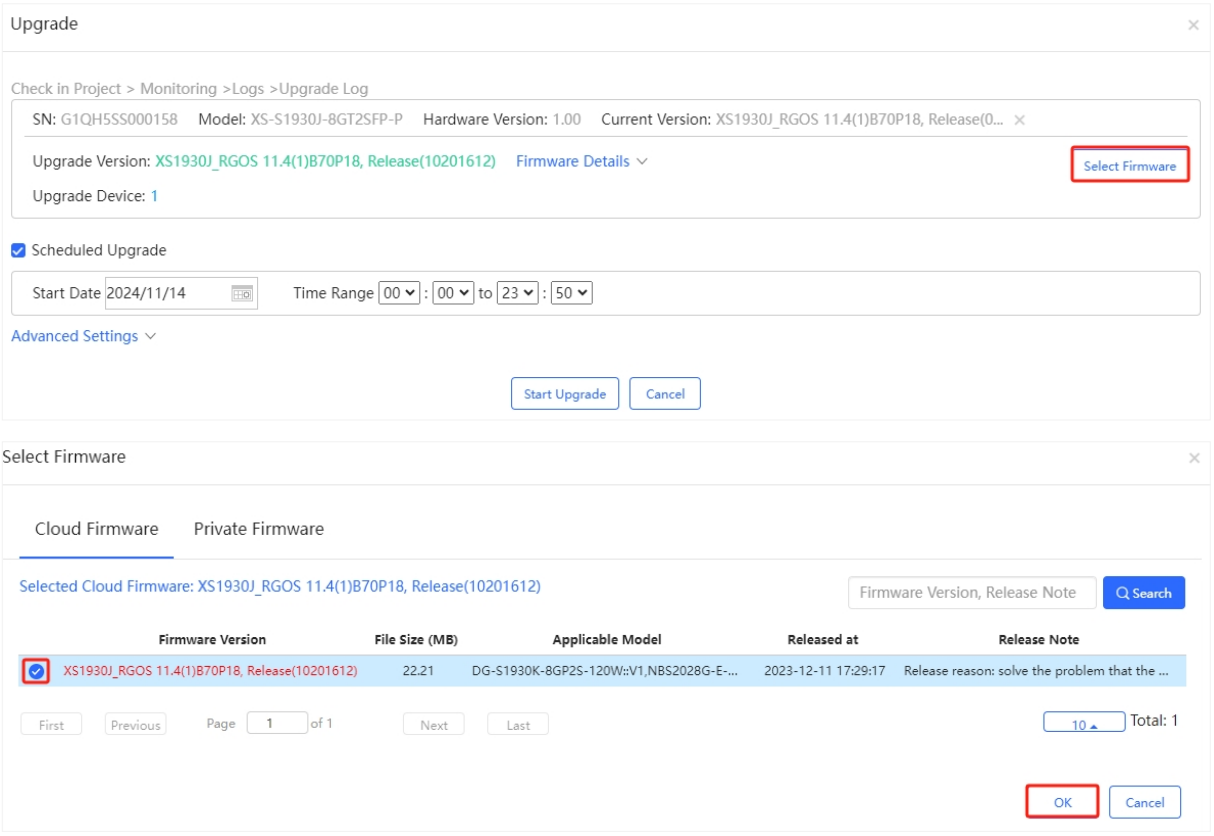
6.1 Upgrading Devices

Follow the steps below to upgrade a small number of devices:

1 Select the device to be upgraded, and then click **Upgrade**.

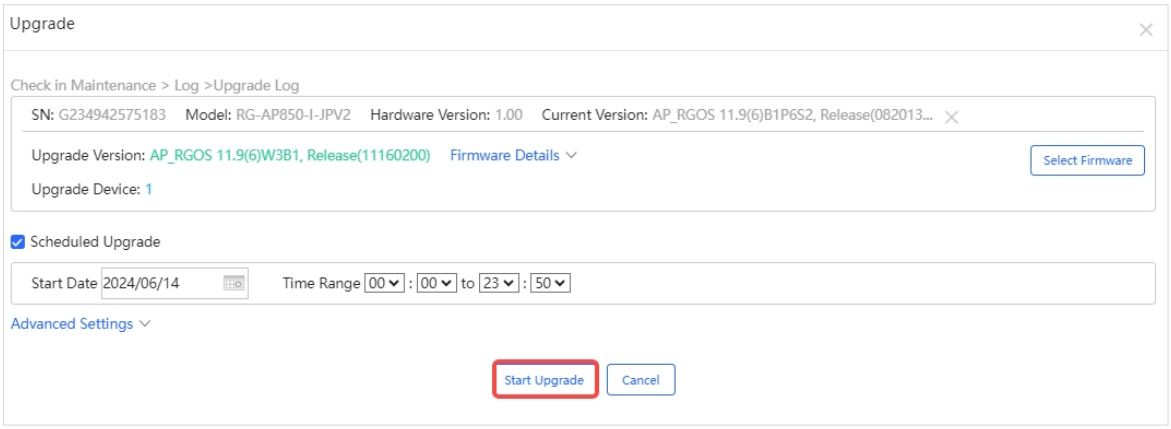


2 Select the firmware version, and set a scheduled upgrade time if it is needed.

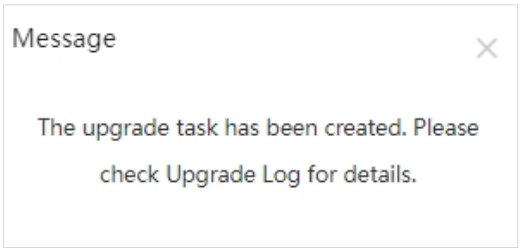


Items	Description
Upgrade Version	If the system has a recommended firmware version, it will be selected by default and displayed here. If there is no recommended version, you need to click **Select Firmware** and select the version you need.
Firmware Details	Click **Firmware Details** to display the information of the selected firmware version.
Scheduled Upgrade	Scheduled upgrade function. This function is disabled by default. After enabling it, you need to set the time period, so that the system will upgrade devices one by one from the start time. The upgrade interval for each device is equal to the set time period divided by the number of devices.
Max Retry Times	After clicking **Advanced Settings**, you can set the number of upgrade retries. The default number of retries is 5.

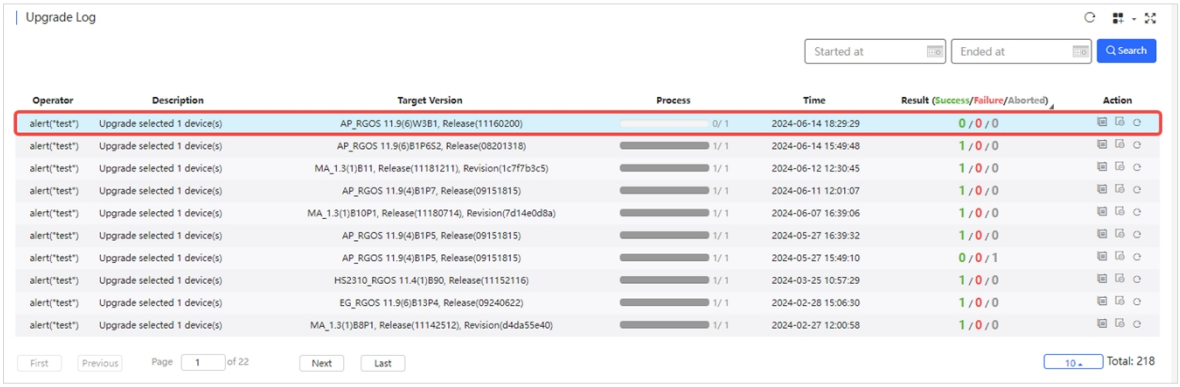
3 After selecting the firmware version for upgrading, click **Start Upgrade**.



4 When the prompt appears, click **X** to close the prompt box to complete the upgrade task creation.



After the operation task is created, you can click **Logs** > **Upgrade Log** to go to the upgrade log interface. The created upgrade task will be displayed in the log list. Click the three buttons in the **Action** column to view, cancel, and retry the upgrade task.

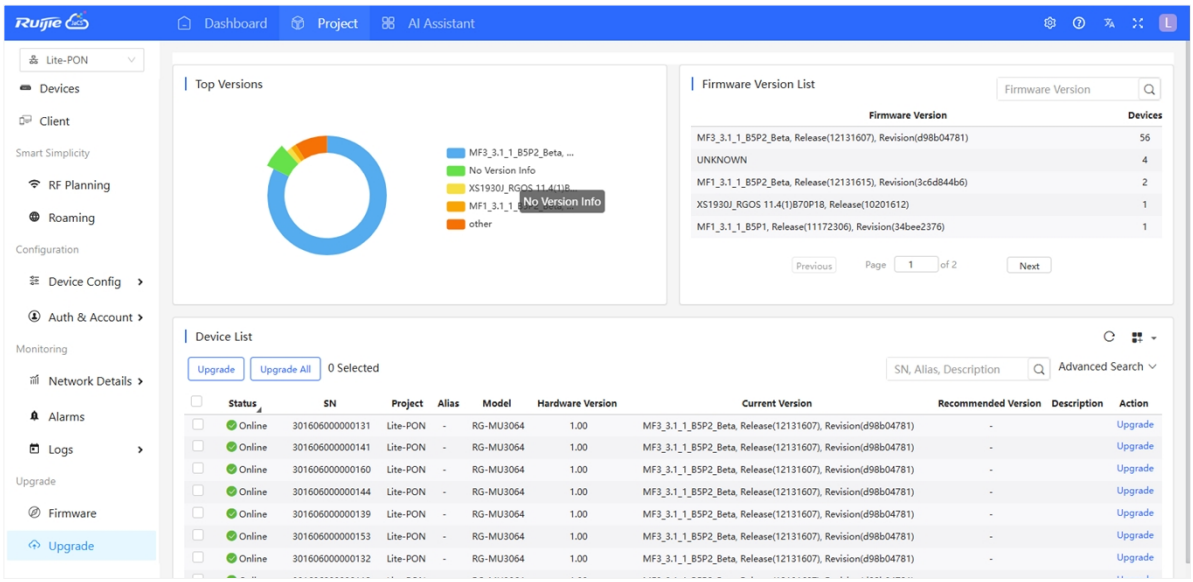


Buttons	Description
	Click this icon to view the details of an upgrade task.
	Click this icon to cancel an upgrade task.
	Click this icon to try an upgrade again.

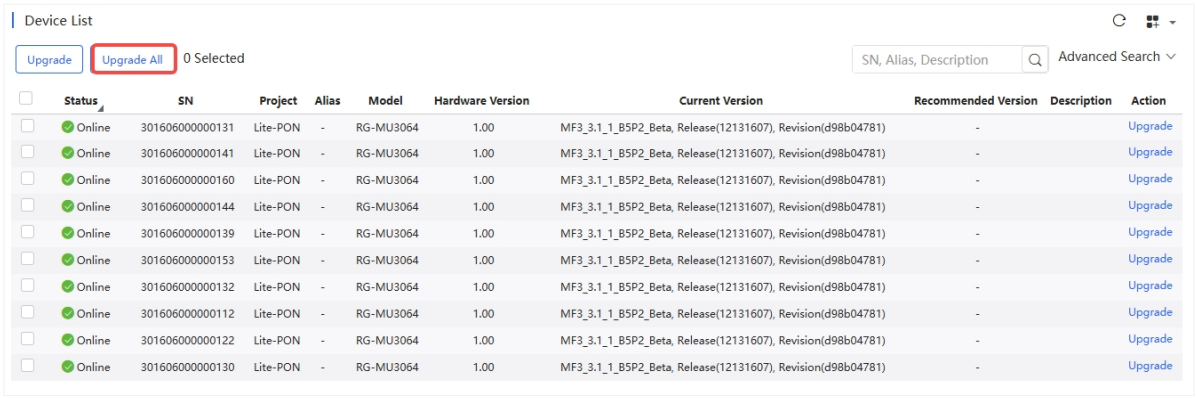
6.1.1 Upgrading Devices in Batches

To upgrade all devices in the project:

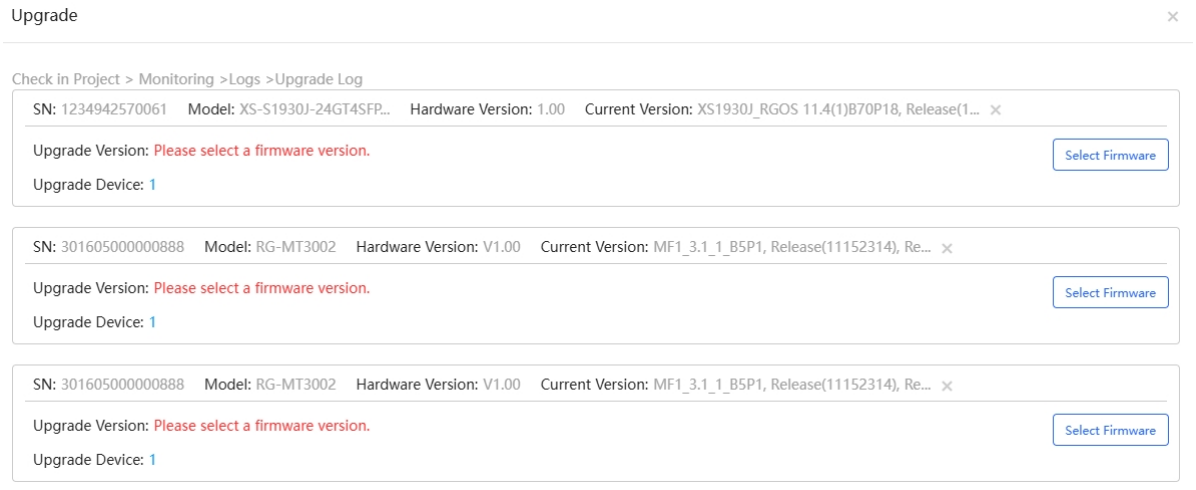
1 Select the project where the devices reside.



2 Click **Upgrade All**.

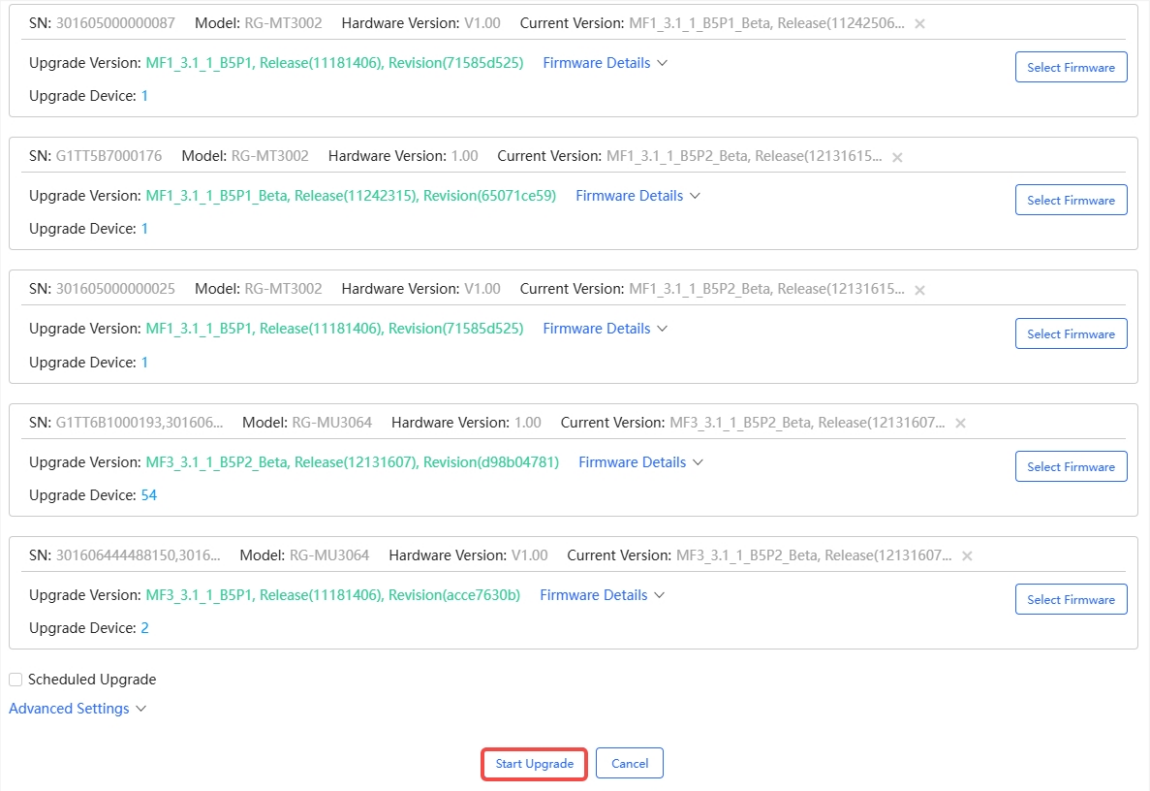


3 Select the firmware versions for the devices, and set the scheduled upgrade and upgrade retry times as needed. If the device is offline, the upgrade task will be executed after the device goes online.

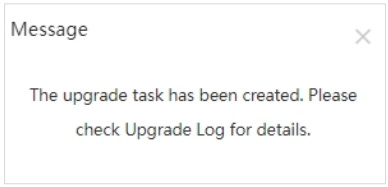


Items	Description
Upgrade Version	If the system has a recommended firmware version, it will be selected by default and displayed here. If there is no recommended version, you need to click **Select Firmware** to select the version you need.
Firmware Details	Click the **Firmware Details** to display the information of the selected firmware version.
Scheduled Upgrade	Scheduled upgrade function. This function is disabled by default. After enabling it, you need to set the time period.
Max Retry Times	After clicking **Advanced Settings**, you can set the number of upgrade retries. The default number of retries is 5.

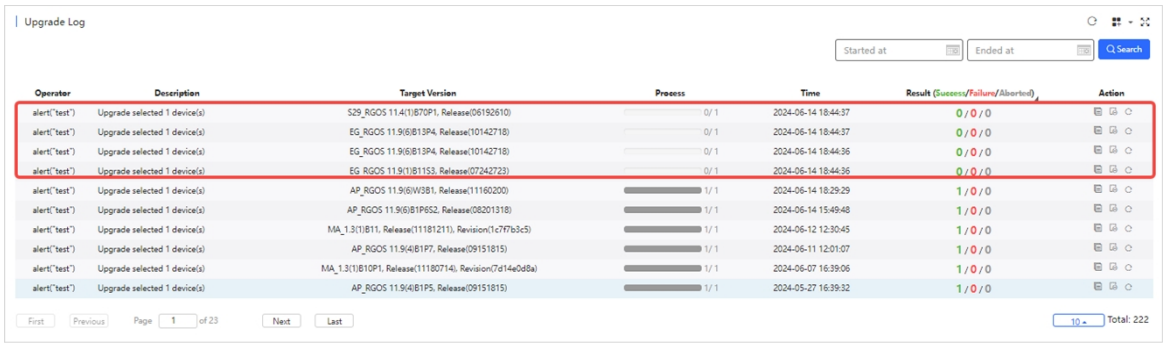
4 After selecting the firmware, click **Start Upgrade**.



5 When the prompt appears, click **X** to close the prompt box to complete the upgrade task creation.



After the upgrade task is created, you can click **Logs** > **Upgrade Log** to go to the upgrade log interface. The created upgrade task will be displayed in the log list. Three buttons are available in the **Action** column for you to view, cancel, and retry the upgrade task.



Buttons	Description
	Click this button to view the upgrade task details, including the upgrade results, and the description of the failure.
	Click this button to cancel the upgrade task.
	Click this button to try the upgrade again.

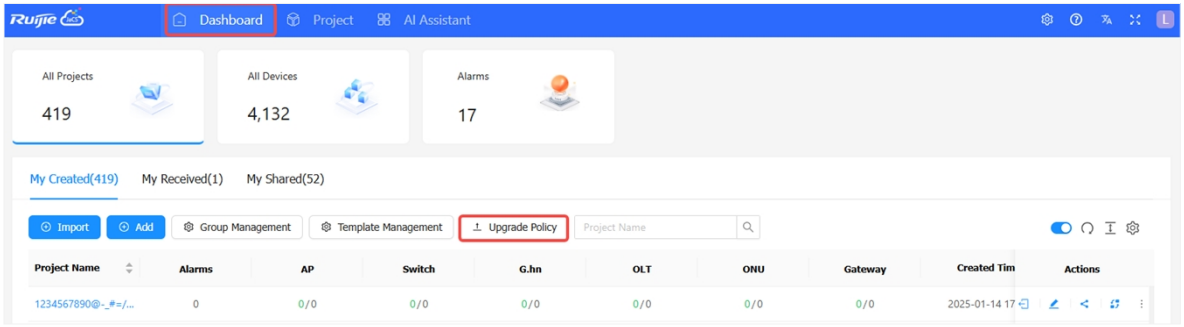
6.1.2 Setting Upgrade Policies

Ruijie JaCS supports creating upgrade policies for MA series access points, AP180 series access point and RG-HA3515-DG. This function allows you to upgrade the devices of these models in a project at specific time.

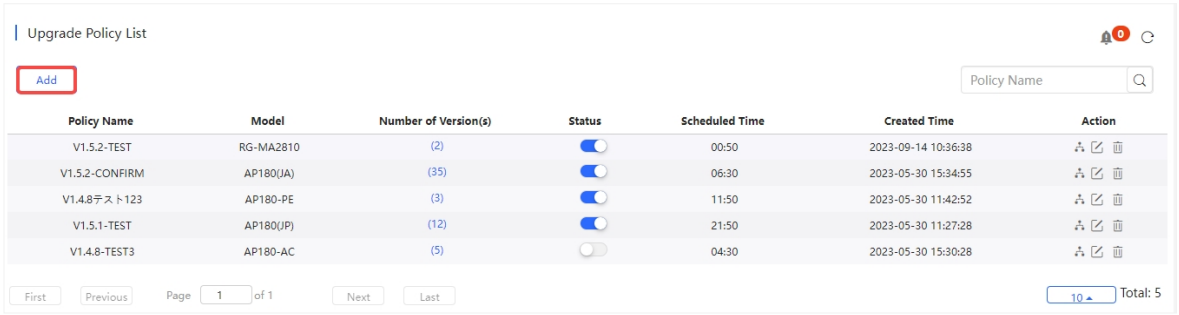
Note

- Subaccounts do not support creating upgrade policies.
- Upgrade policies cannot be applied to devices in a shared project.

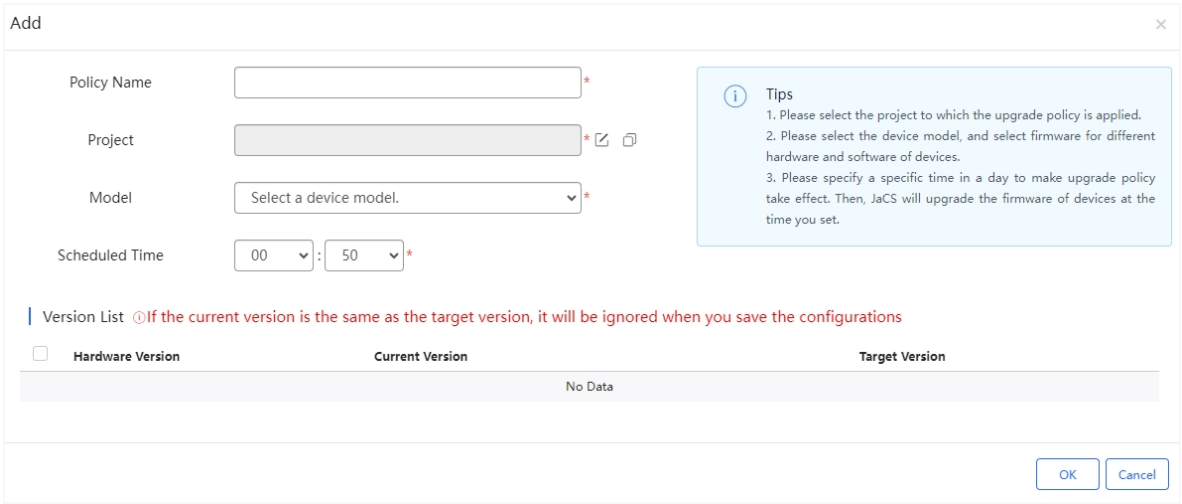
1 Click **Upgrade Policy** in the **Dashboard** interface.



2 Click **Add** to enter the policy adding interface.



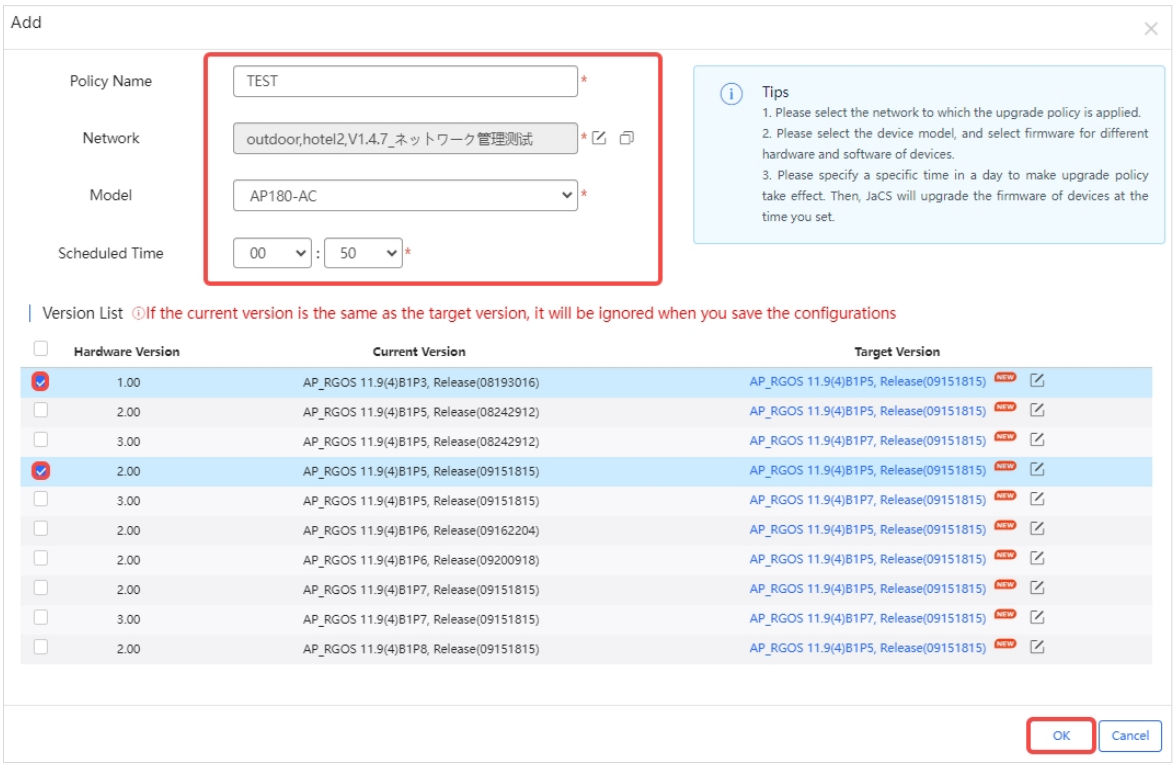
3 Set the policy name, the project to which the policy applies, the model, and the scheduled time.



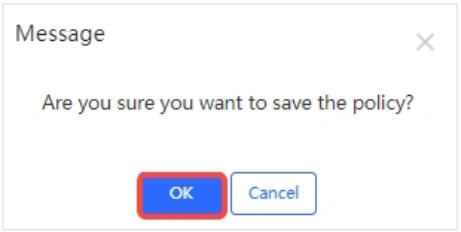
Items	Description
Policy Name	Required. Set the upgrade policy name. The length of a policy name should range from 1 to 64 characters. Numbers, letters, spaces, and special symbols (-, _, , #, /, ., [], (), =, :, + or @) are supported.

Project	Required. Click the icon to select the project where the device resides. Click to select a project set in an existing policy.
Model	Required. Select the device model to which the upgrade policy is applied. Only supports MA series access points, AP180 series access points and RG-HA3515-DG. After selecting a model, the upgrade policy will be applied to all devices of this model in the project.
Scheduled Time	Required. Set the time for scheduled upgrade.
Version List	Required. Select the firmware version. The version displayed in the **Target Version** column is the recommended version. If you do not want the recommended version, you can click the icon to modify it.

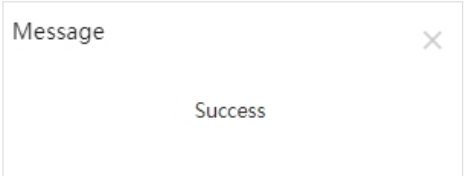
4 After configuring the policy, click **OK**.



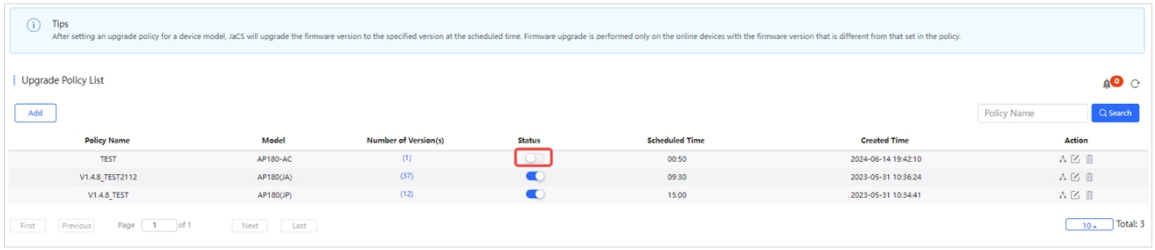
5 When the operation confirmation prompt appears, click **OK**.



6 When the "Success" prompt appears, click **X** to close the prompt box and complete the operation.

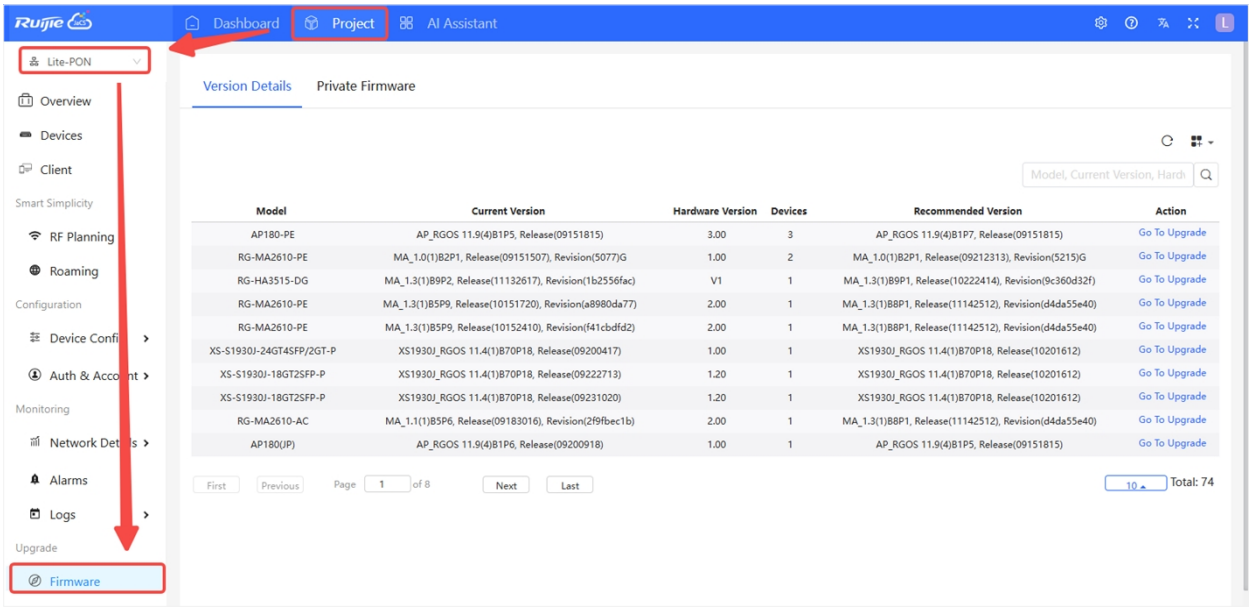


Once an upgrade policy is created, it appears in the upgrade policy list and is disabled by default. When enabled, JaCS will upgrade the devices in the specified project at the scheduled time, following the policy's configured settings.

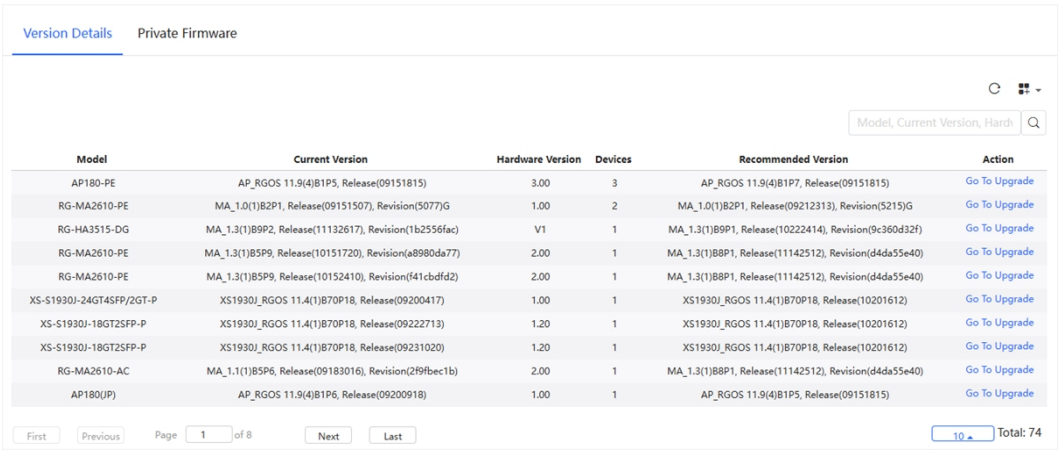


6.1.3 Firmware Management

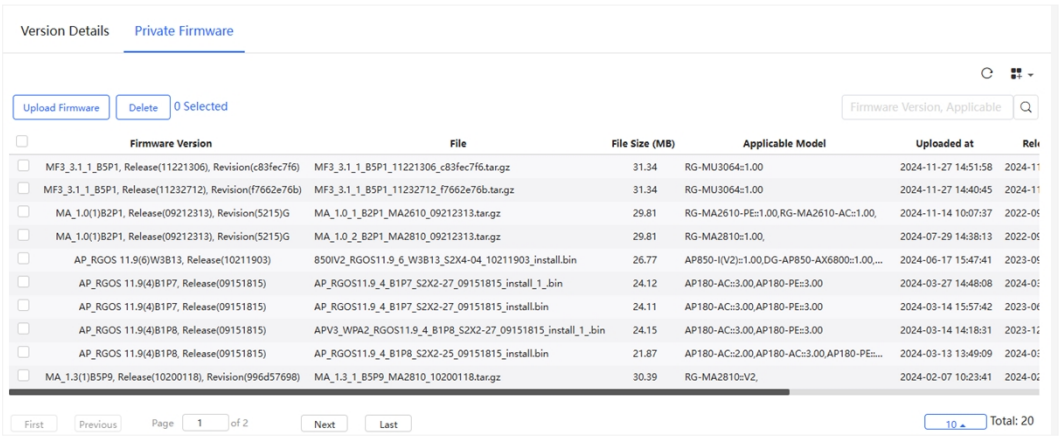
Click **Project** to go to the project interface. After selecting a project, click **Firmware** to manage the firmware in the specified project. The firmware management interface consists of two parts: **Version Details** and **Private Firmware**.



Version Details displays the firmware versions installed on all devices in this project. Click **Go To Upgrade** in the **Action** column to go to the upgrade interface. For detailed upgrade steps, please refer to Section 6.1.



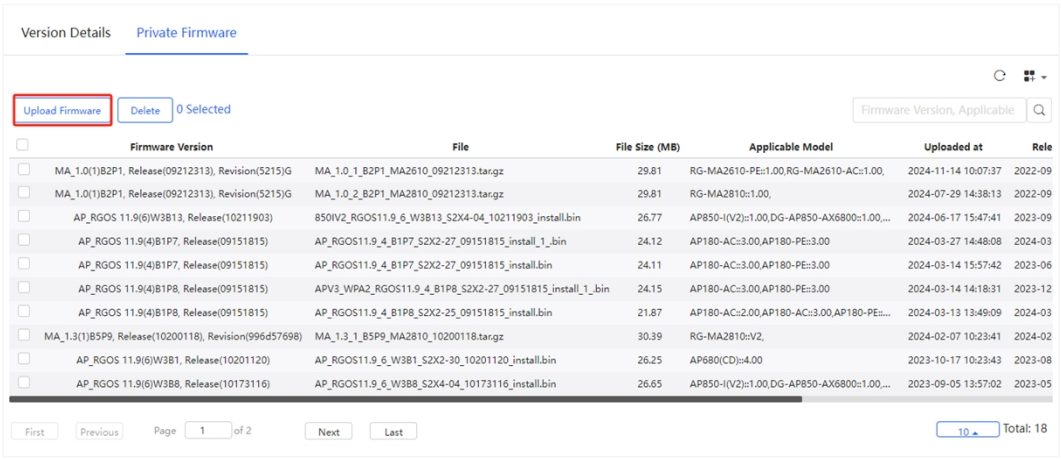
Private Firmware list displays the private firmware uploaded by all accounts under the tenant.



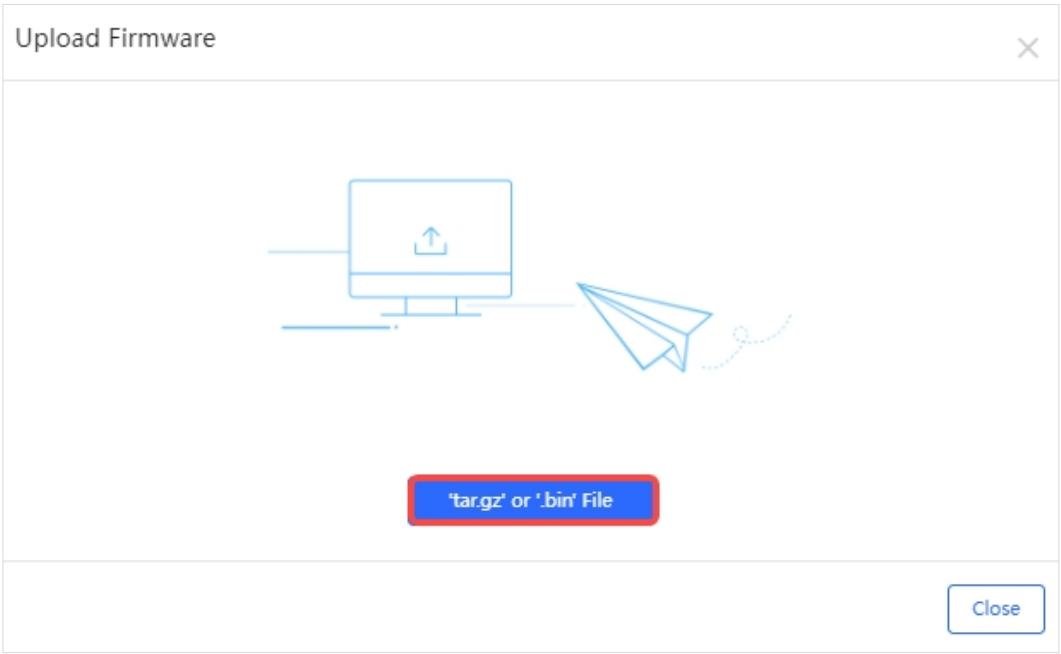
6.1.3.1 Uploading Private Firmware Versions

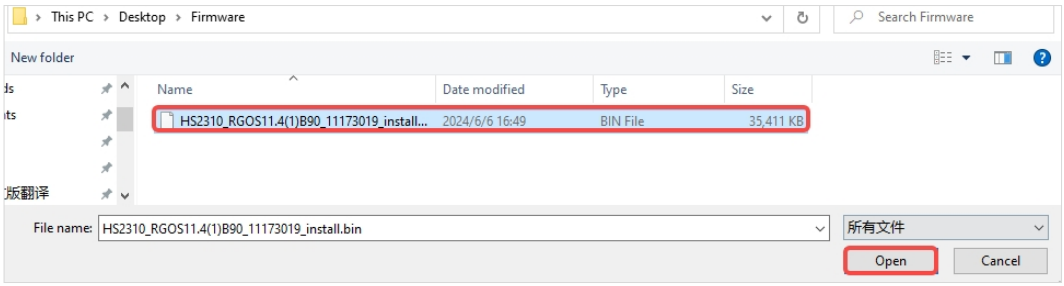
Follow the steps below to upload your local private firmware versions to the JaCS:

1 Click **Upload Firmware** to go to the upload interface.

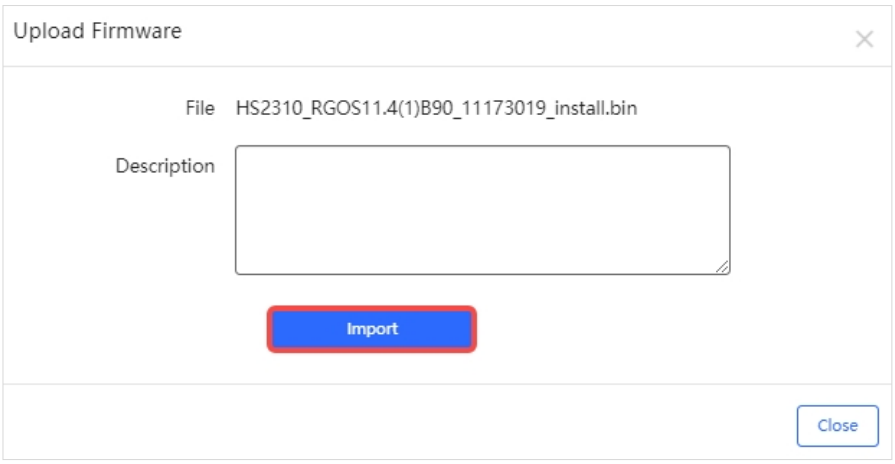


2 Click **'tar.gz' or '.bin' File** and select the firmware version to be uploaded.

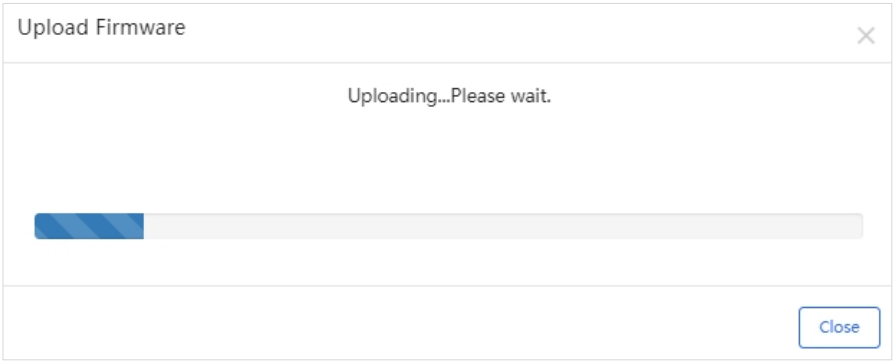




3 Click **Import** to upload the firmware version. You can add description information for the firmware version (up to 255 characters can be entered.)

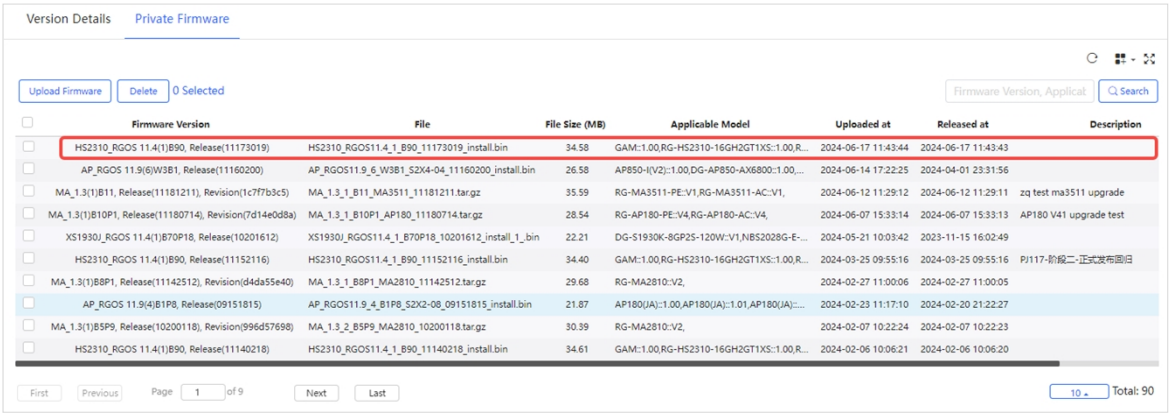


4 Wait for the firmware version to be uploaded.



5 When the “Upload firmware succeeded” prompt appears, click **X** to close the prompt box to complete the operation.

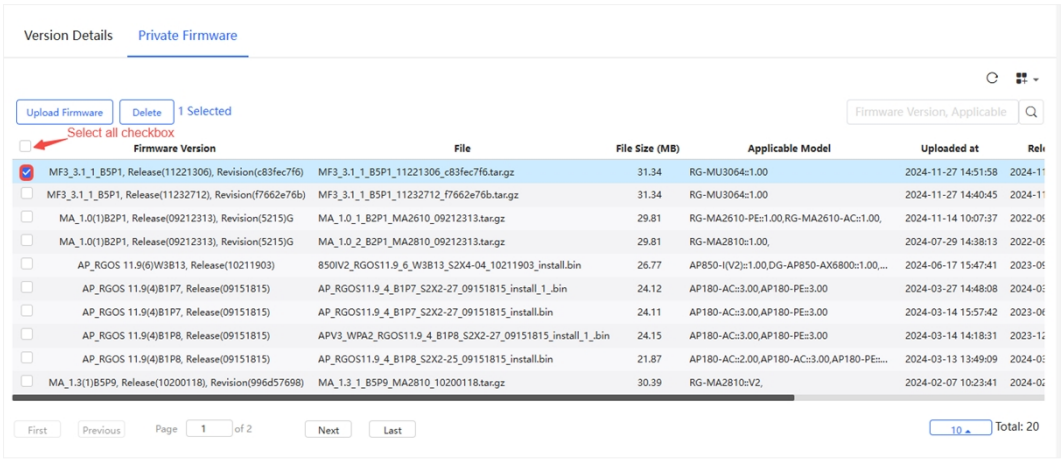
Once a firmware has been uploaded, it is displays in the **Private Firmware** list.



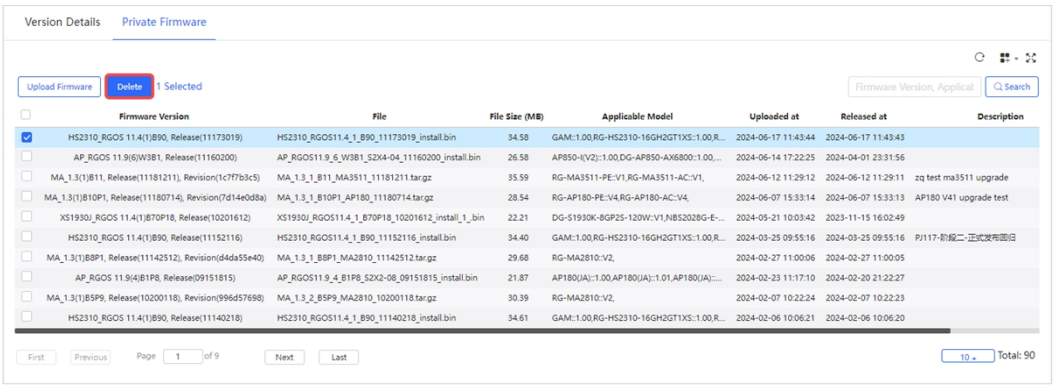
6.1.3.2 Deleting Private Firmware Versions

To remove a private firmware version from the JaCS:

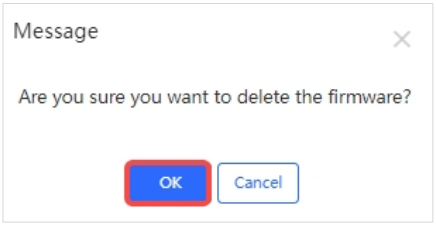
1 Select the firmware version to be deleted. Multiple selections are supported. If you need to select all, check the **Select all checkbox**.



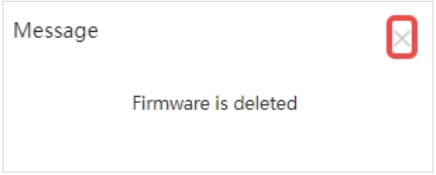
2 Click **Delete.**



3 When the confirmation prompt appears, click **OK**.



4 When the “Firmware is deleted” prompt appears, click **X** to close the prompt box and complete the operation.



7 Operation and Maintenance

7.1 Viewing Network Topology

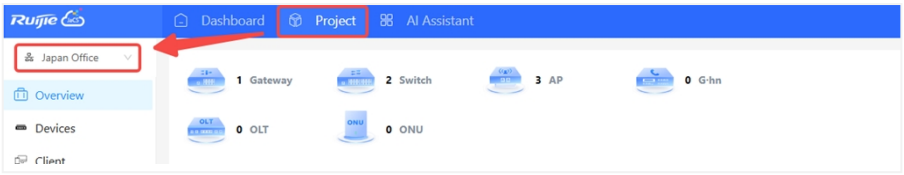
Ruijie JaCS supports viewing the network topology of some devices in the project. The topology interface displays the topology of the downlink devices of an online device in the current project. It enables the diagnosis of all online devices within the project and generates comprehensive diagnostic reports.

Note

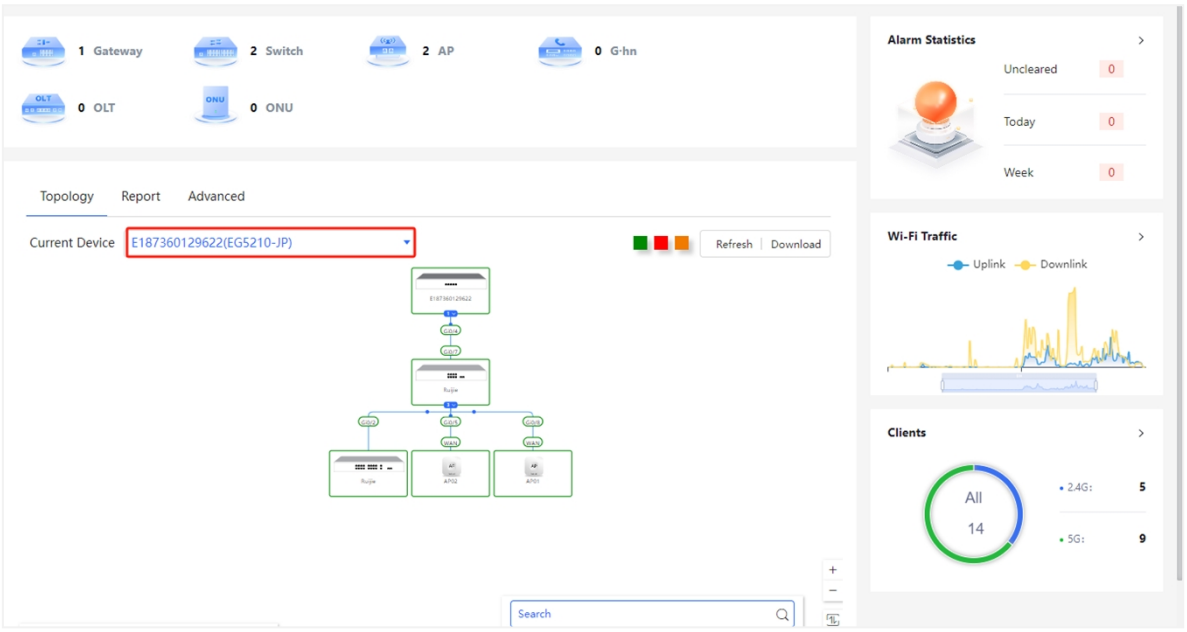
Ruijie JaCS currently only supports displaying the topology of the following models: RG-EG5210-JP, RG-HS2310-16GH2GT1XS, RG-MT3002 and RG-MU3064.

The specific steps are as follows:

1 Click **Project**, and the select the project where the device is located.



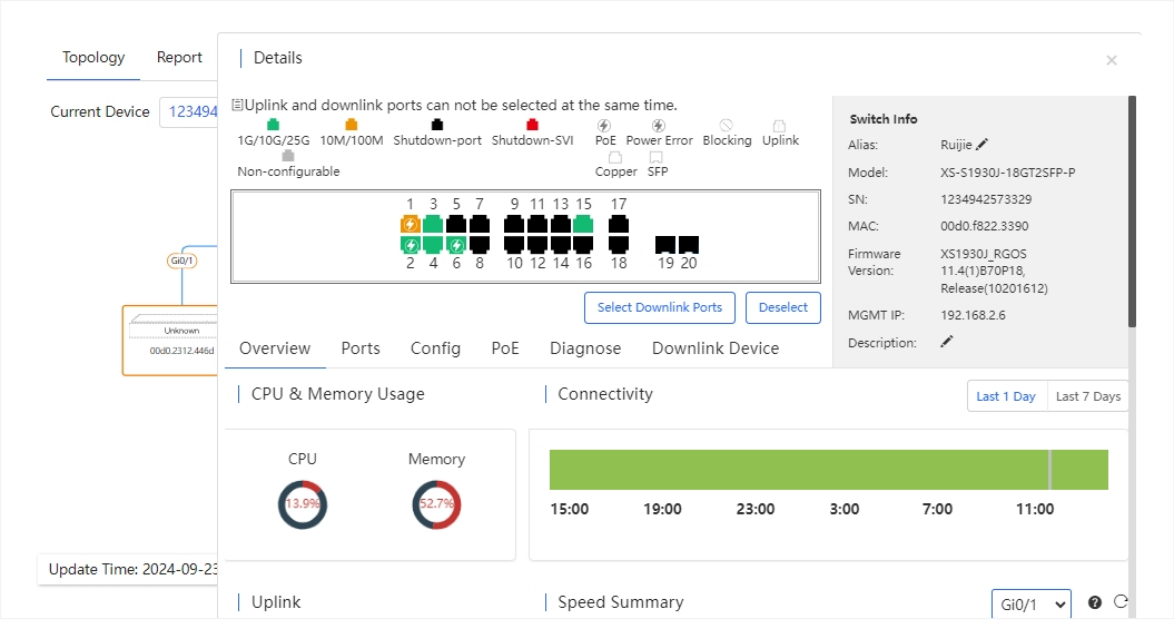
2 Click **Overview** > **Topology** to go to the topology interface. Select the device you want to view. After selecting, the topology of the device will be displayed below.



Different colors in the topology represent different link states.

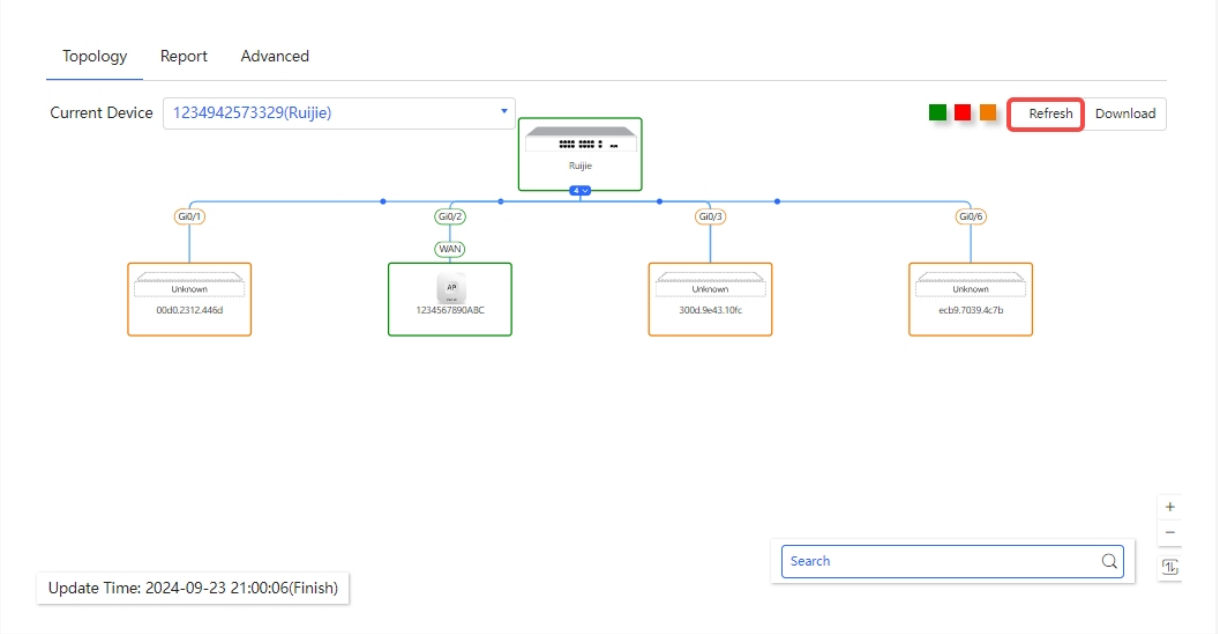
- Green means the device is functioning normally.
- Red indicates the device is offline or disconnected from the switch.
- Orange means the device is not connected to the cloud or belongs to another account.

Click a device image, you can view its detailed information.


Topology
Report
Details
Current Device
Uplink and downlink ports can not be selected at the same time.
1G/10G/25G
10M/100M
Shutdown-port
Shutdown-SVI
PoE
Power Error
Blocking
Uplink
Non-configurable
Copper
SFP
1 3 5 7 9 11 13 15 17
2 4 6 8 10 12 14 16 18 19 20
Select Downlink Ports
Deselect
Switch Info
Alias: Ruijie
Model: XS-S1930J-18GT2SFP-P
SN: 1234942573329
MAC: 00d0.f822.3390
Firmware Version: XS1930J_RGOS 11.4(1)B70P18, Release(10201612)
MGMT IP: 192.168.2.6
Description:
Overview
Ports
Config
PoE
Diagnose
Downlink Device
CPU & Memory Usage
Connectivity
Last 1 Day
Last 7 Days
CPU
Memory
13.9%
52.7%
15:00
19:00
23:00
3:00
7:00
11:00
Gi0/1
Unknown
Update Time: 2024-09-23
Uplink
Speed Summary
Gi0/1

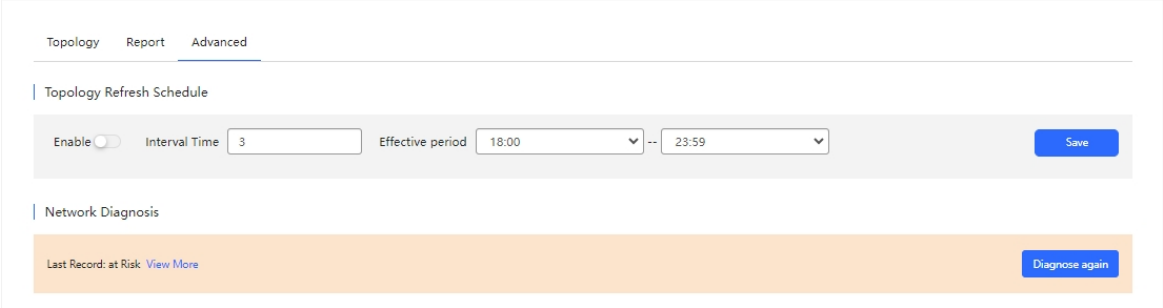
7.1.1 Refreshing Topology

Click **Refresh** to refresh the downlink topology of the device. The refresh interval should be greater than 10 minutes, otherwise a prompt will appear indicating frequent operations. The topology update is triggered when the switch is selected for the first time.

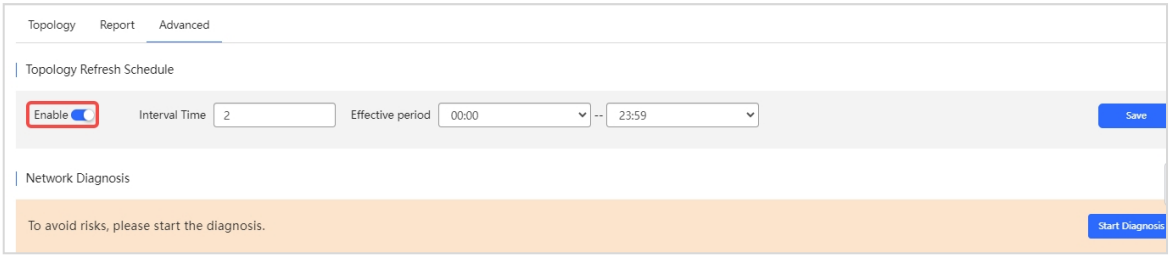


To refresh the topology regularly:

1 Click **Advance** to go to the setting page.



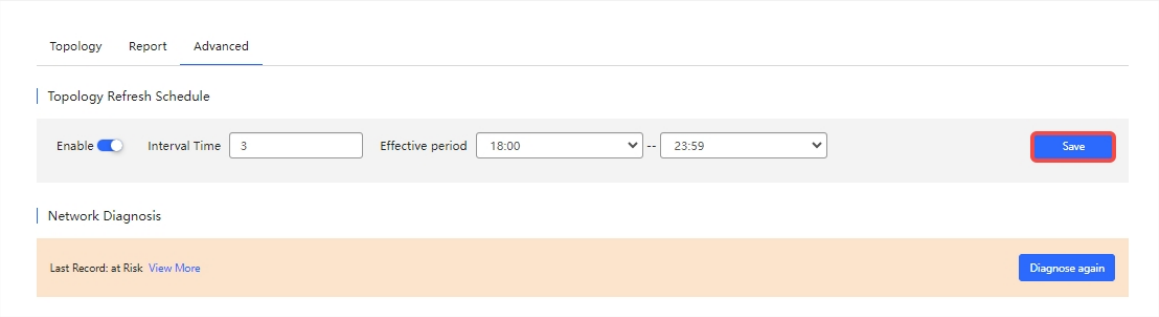
2 Enable the schedule refresh function.



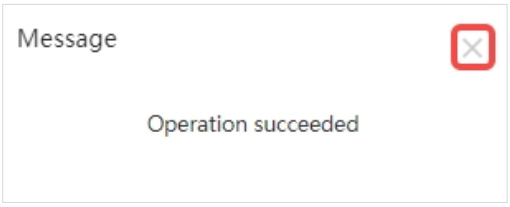
3 Set the refresh interval and effective time period, and then click **Save**.

Note

The minimum interval time supported is 2 hours, and the maximum interval time supported is 23 hours.

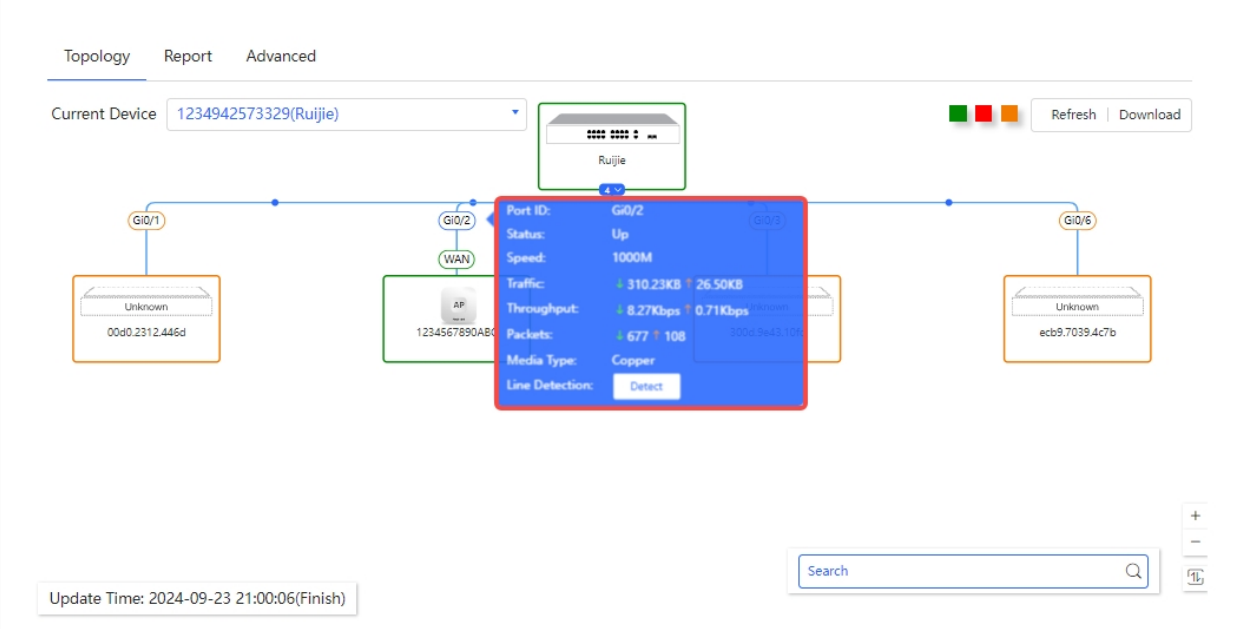


4 After the "Operation succeeded" prompt appears, click **X** to close the prompt box and complete the operation.



7.1.2 Viewing Port Information

Click a port icon in the topology, you can view its detailed information. The port information includes: port ID, port status, speed, upstream and downstream traffic, throughput, upstream and downstream packet rates, and port types.



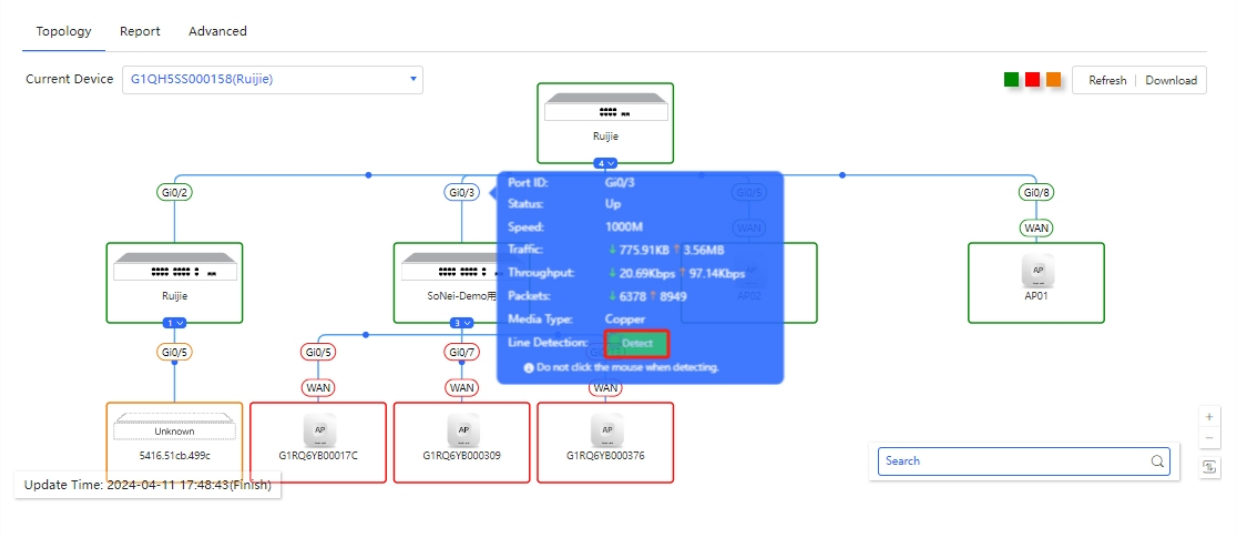
Note

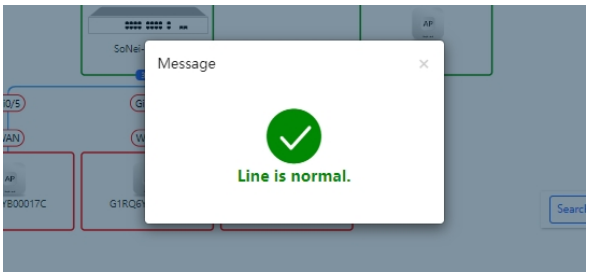
RG-HS2310-16GH2GT1XS is connected to RG-HA3515-DG through the G.hn port via a telephone line. The G.hn port is displayed as Ghnx/x on the page. Clicking a G.hn port number will display the detailed information of the port. The speed displayed in the Speed item is the actual downlink speed. The speed of other devices is displayed as 100M/1000M.

7.1.3 Physical Link Detection

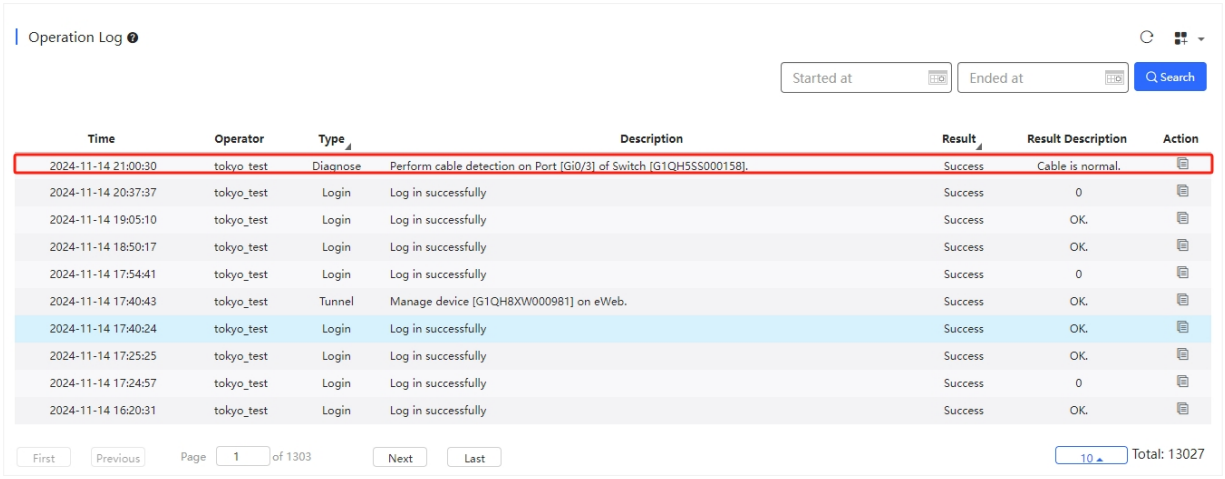
In the topology, hover the cursor over a port to view its detailed information. In the detailed information box, click **Detect** to initiate link detection. Do not perform any operations during the detection process. The possible outcomes are: link normal, link fault, or no link.

> **Note**
>
> The physical link detection function is not available for RG-EG5210-JP.



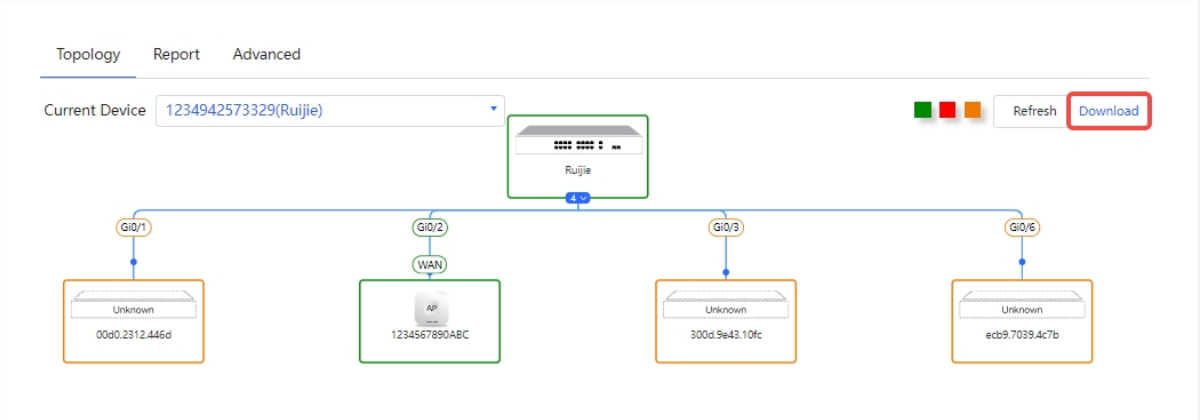


After the detection is completed, you can view the operation log in **Operation Log** interface.



7.1.4 Exporting Topology Diagram

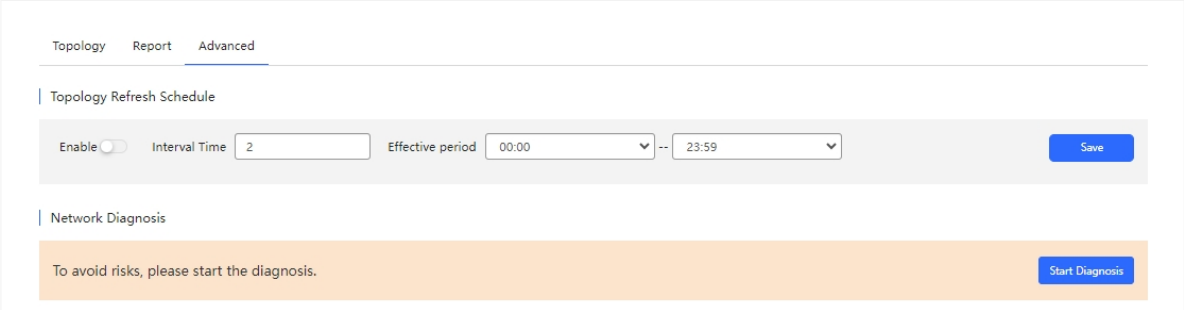
Click **Download** to export the current topology diagram.



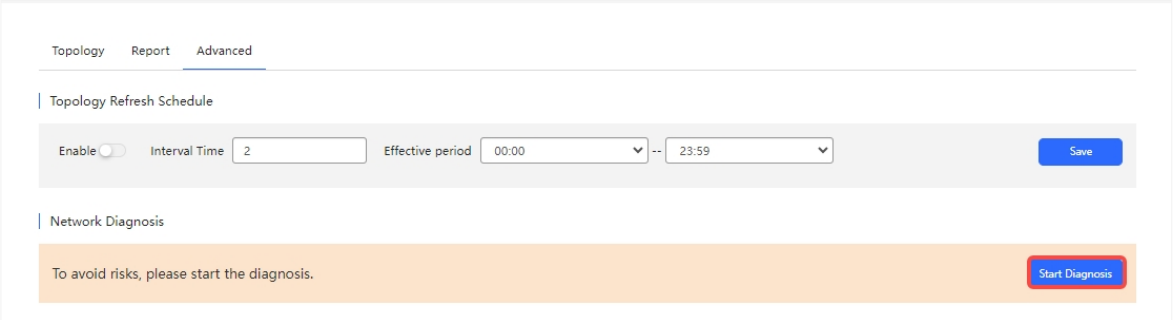
7.1.5 Network Diagnostics

Follow the steps below to diagnose the network:

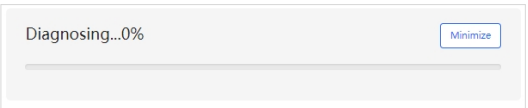
1 Click **Advanced** to go to the setting page.



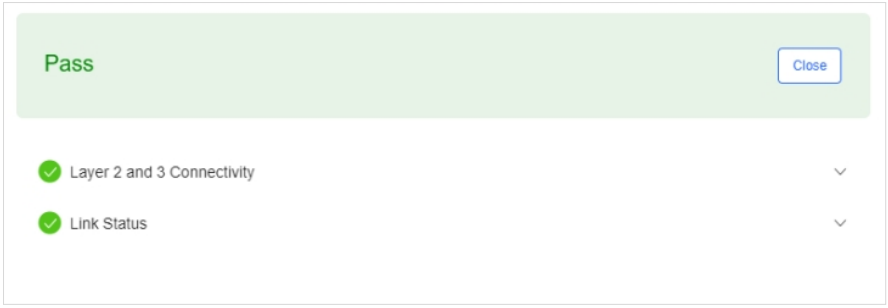
2 Click **Start Diagnosis** to start diagnosis.



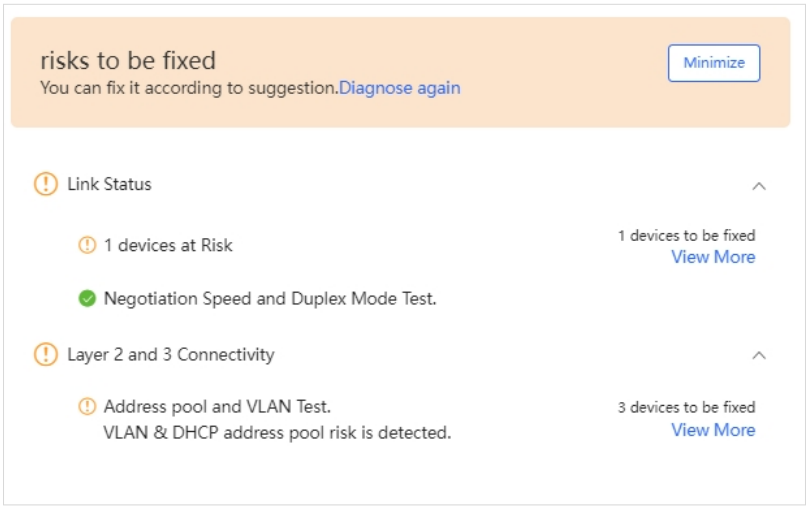
3 Wait for diagnosis results.

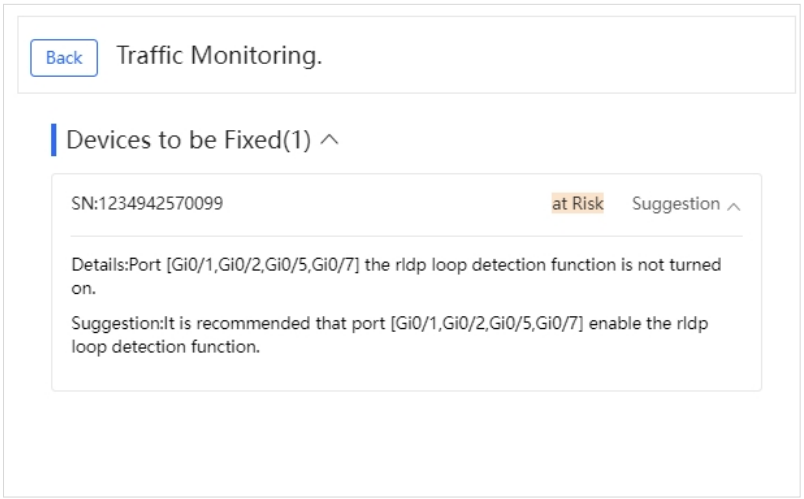


If no risk is detected, the following interface will be displayed:



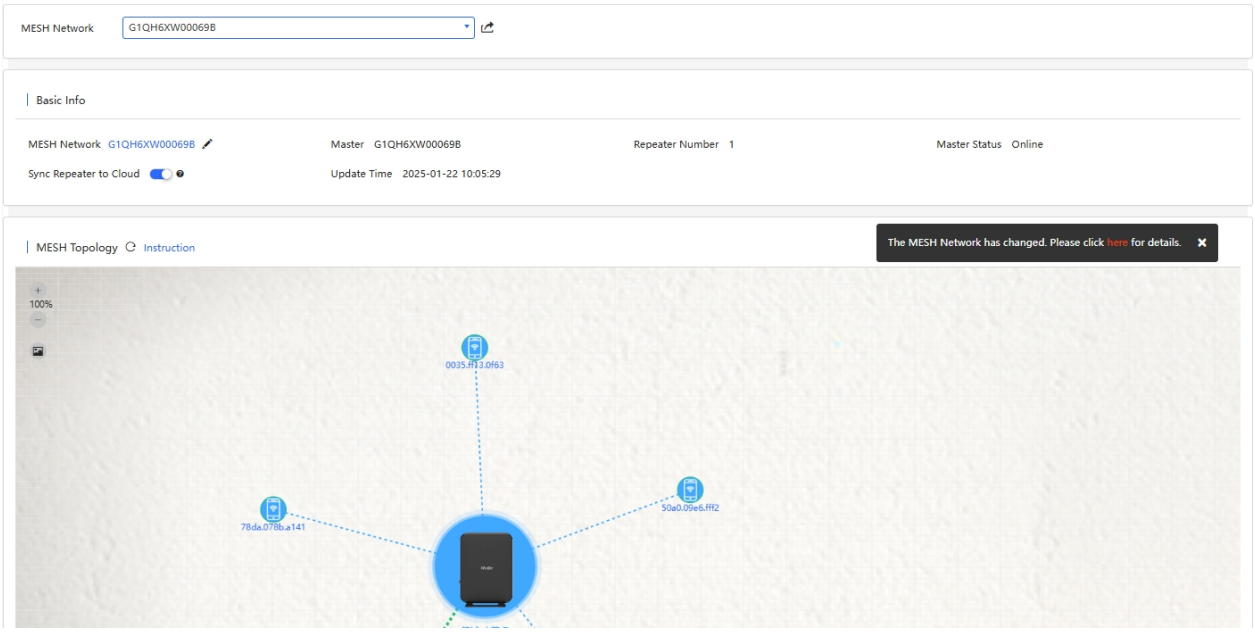
If a risk is detected, the following interface will be displayed. Click **View More** to view the details and the recommended handling methods.



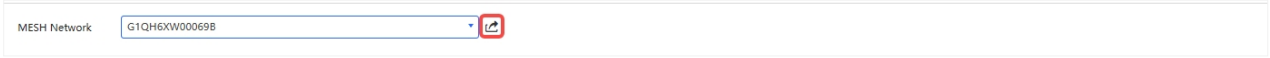


7.2 Mesh

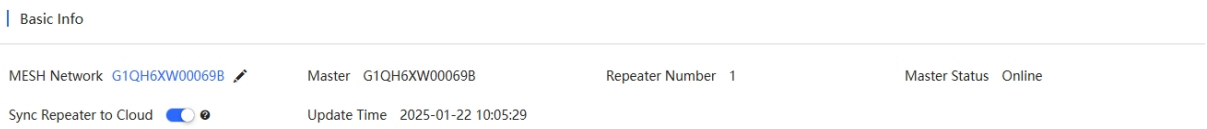
On the **Project** interface, click **Network Details** > **Mesh** to enter the Mesh management interface. The Mesh network management interface includes three parts: **Mesh Network**, **Basic Information** and **Mesh Topology**.



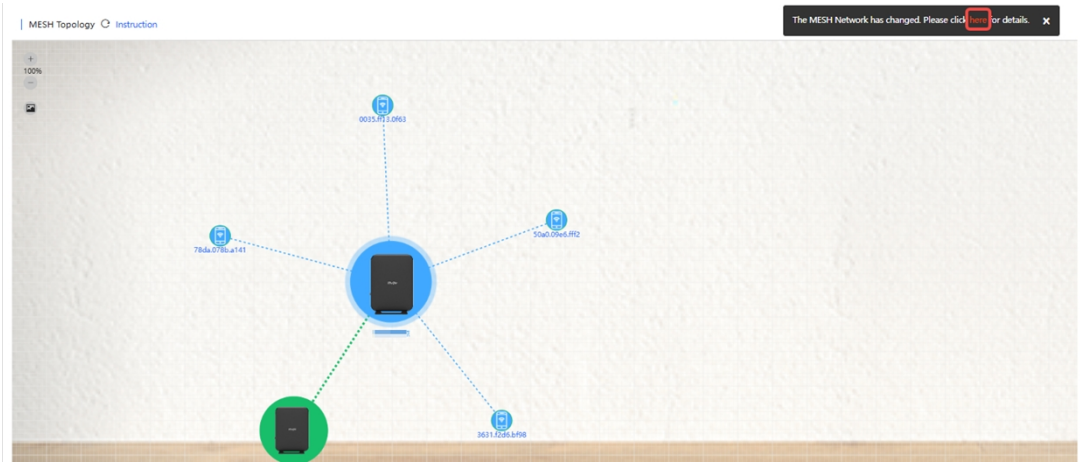
Select the specified Mesh network in the **Mesh Network** box. If you want to export the Mesh network report, click to export it.



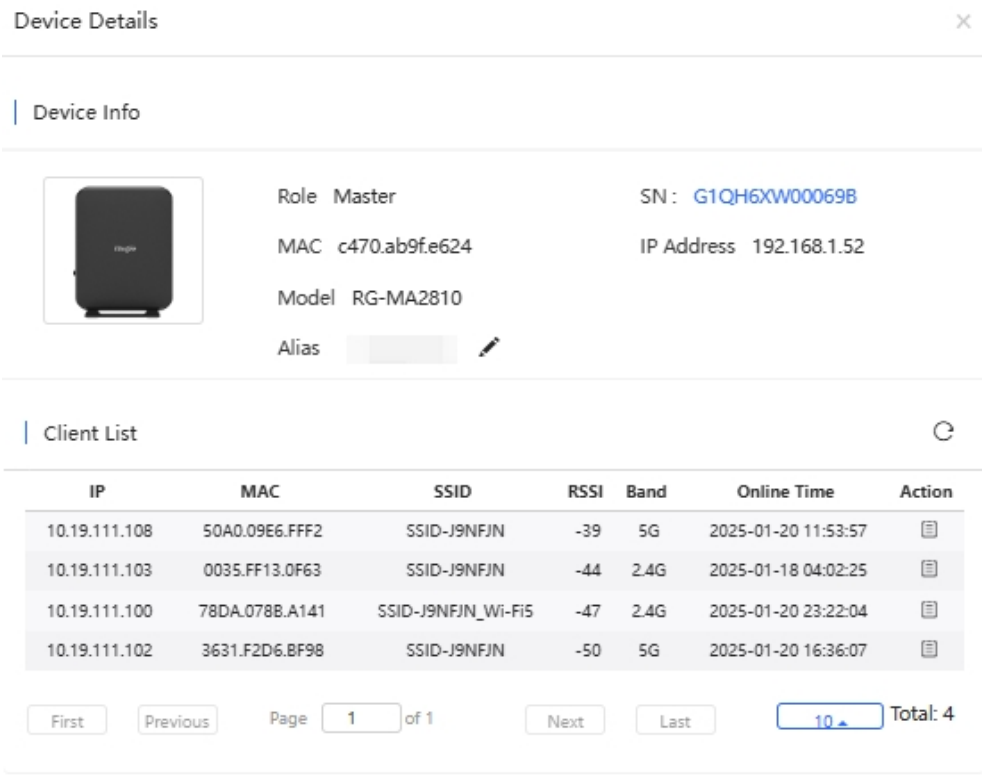
Basic Info displays basic information of the Mesh network. Click next to the Mesh network to modify the Mesh network name. After the **Sync Repeater to Cloud** is disabled, the device may not be synchronized to the cloud. Therefore, you cannot view some Mesh network information, such as device model, SN, or link status.



The Mesh topology interface displays the current Mesh topology, including device and client information. If the topology changes, a prompt "The MESH Network has changed. Please click here for details " will appear. Click "**here**" to go to the Mesh log page.

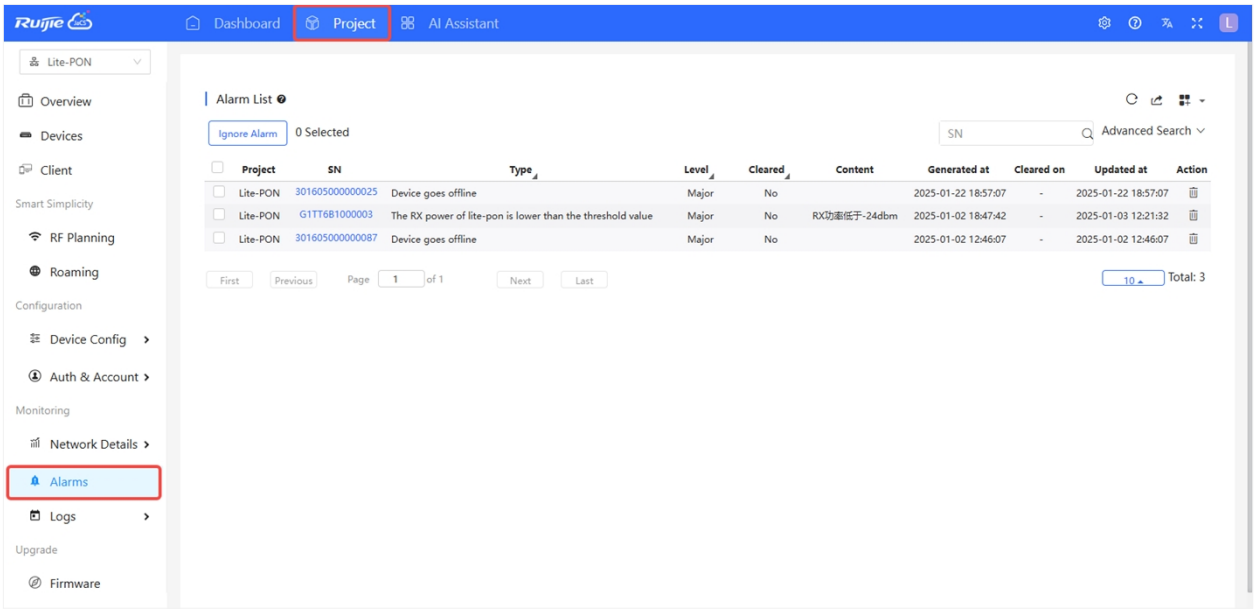


Click a device icon to view its detailed information.



7.3 Alarm Management

In the project management interface, click **Alarms** to enter the alarm management interface. In this interface, you can view the alarm information in the current project. An alarm can be searched based on the AP's serial number, alarm type, alarm level, and alarm occurrence time.

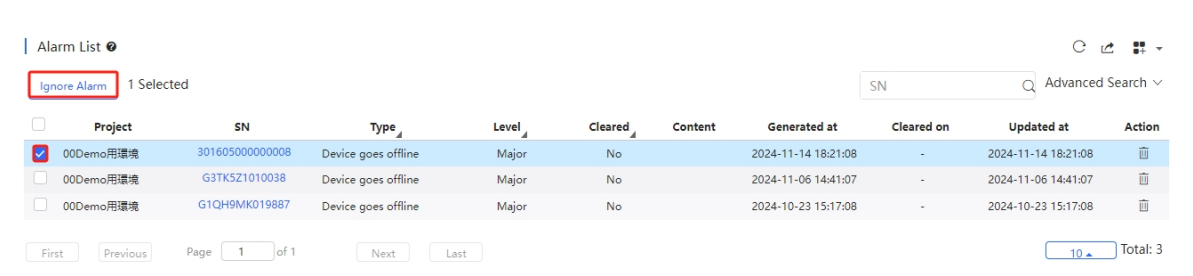


Type	Status	Description
Device goes offline	The AP is offline.	The AP is disconnected from the cloud or is powered off.
Device goes offline and online continually.	The times of the AP going online or offline within two hours exceeds the default threshold.	The connection between the AP and the JaCS is unstable, or the AP has a firmware or hardware failure.
All devices are offline	All APs in the project are offline.	N/A
High channel usage on AP	The RF channel utilization exceeds 80%.	The RF channel utilization is too high and the interference is strong. It is recommended to change the channel.
System usage(CPU/memory usage) above threshold	The CPU or memory usage of the AP/switch/gateway exceeds the threshold.	For APs, the default thresholds for CPU usage and memory usage are both 85%. For switches, the default threshold for CPU usage is 50%, and the default threshold for memory usage is 65%. For gateways, the default threshold for CPU usage is 50%, and the default threshold for memory usage is 65%. Custom values are not supported.
Switch loopback detected (RLDP)	A loop occurs on the switch.	N/A
Abnormal network access on gateway	The gateway port was unable to successfully ping the specified domain or IP address multiple times.	When the number of ping test failures reaches the specified number, an alarm will be issued. The number of times and domains/IP addresses can be manually configured.
High packet loss speed on gateway	The packet loss rate on the gateway exceeds the threshold.	When the packet loss rate exceeds the threshold multiple times within 5 minutes, an alarm is generated. The number of times and the threshold can be manually configured.

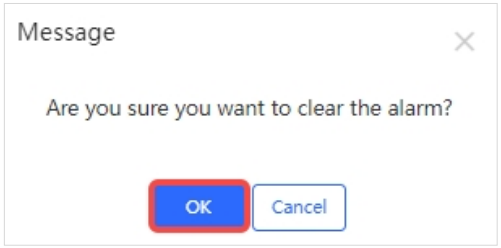
Uplink speed above threshold on gateway	The uplink rate exceeds the threshold multiple times.	When the uplink rate exceeds the threshold multiple times, an alarm is generated. The threshold, number of times, and percentage can be manually configured.
Downlink speed above threshold on gateway	The downlink rate exceeds the threshold multiple times.	When the downlink rate exceeds the threshold multiple times, an alarm is generated. The threshold, number of times, and percentage can be manually configured.
Imported MAC, SSID and/or password checks	Importing devices.	When the imported MAC is inconsistent with the actual MAC, or the SSID/password is changed, an alarm is generated.
The RX power of lite-pon is higher than the threshold value	The RX power is higher than the threshold value.	Once the RX power exceeds the threshold value, an alarm is generated.
The RX power of lite-pon is lower than the threshold value	The RX power is lower than the threshold value.	Once the RX power is lower than the threshold value, an alarm is generated.
The TX power of lite-pon is higher than the threshold value	The TX power exceeds the threshold value.	Once the TX power exceeds the threshold value, an alarm is generated.
The TX power of lite-pon is lower than the threshold value	The TX power is lower than the threshold value.	Once the TX power is lower than the threshold value, an alarm is generated.

The **Alarm List** shows the all alarms of the current project. To ignore generated alarms:

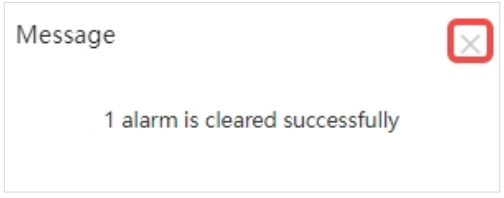
1 Select the alarm to be ignored, and then click **Ignore Alarm**.



2 When the operation confirmation box appears, click **OK**.

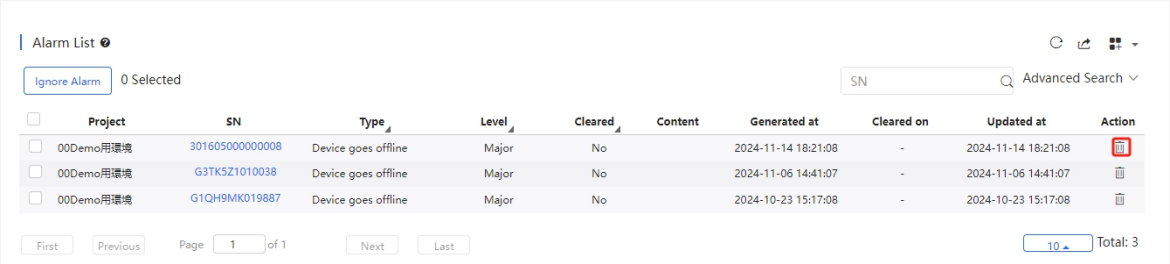


3 After successfully ignoring the alarm, click **X** to close the prompt box and complete the operation.

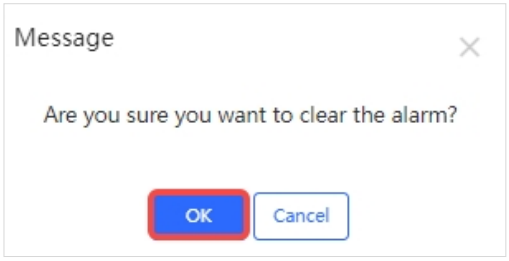


To clear the alarm in the list:

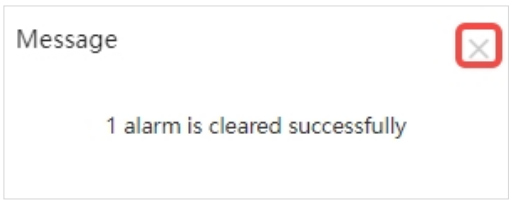
1 Click the in the **Action** column of the alarm to be cleared.



2 When the confirmation box appears, click **OK**.



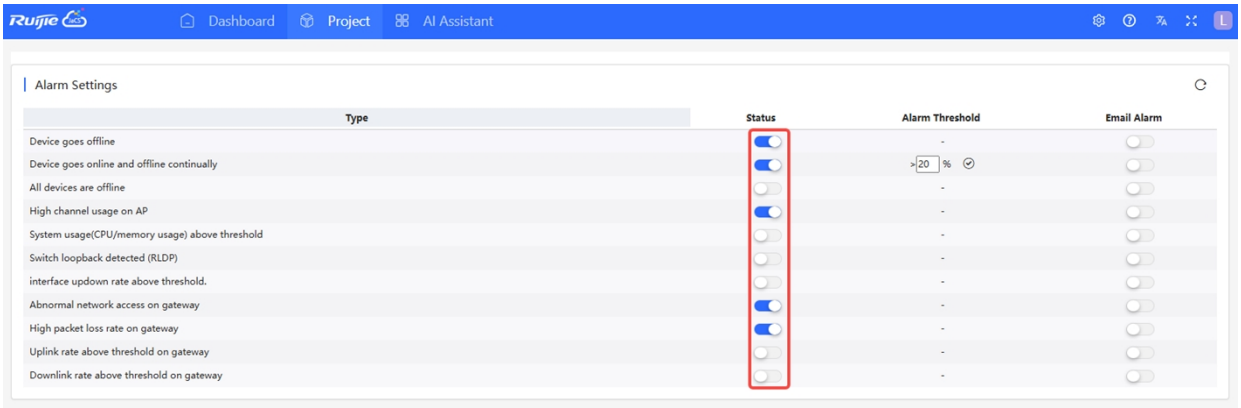
3 After successfully clearing the alarm, click **X** to close the prompt box and complete the operation.



7.3.1 Alarm Condition Settings

Click and select **Alarm Settings** to go to the alarm interface. If the alarm conditions are not configured, the global settings are used.

Users can click the switch in **Status** to enable the corresponding alarm condition according to actual needs.

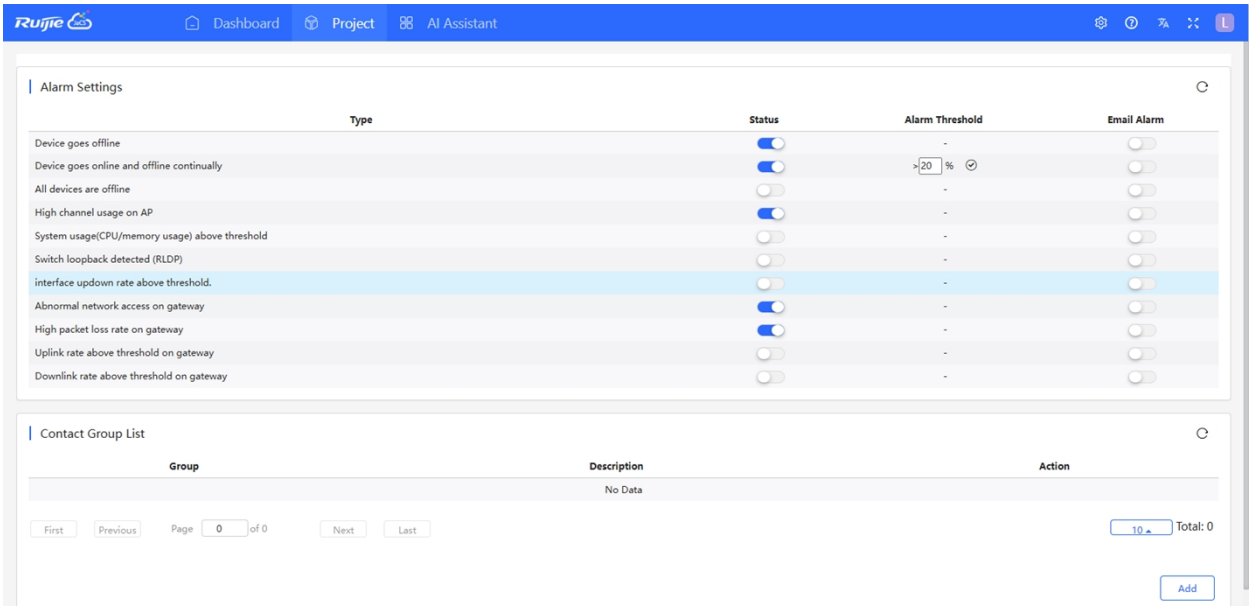


Conditions	Description
Device goes offline	Defaults: Enabled. An alarm will be generated, when a device in the project goes offline.
Device goes online and offline continually	Defaults: Enabled. An alarm will be generated, when a device in the project is constantly going online and offline. When it is enabled, you can set the threshold (the default value is 20%).
All devices are offline	Defaults: Disabled. An alarm will be generated when all devices in the project go offline.
High channel usage on AP	Defaults: Enabled. An alarm will be generated when the channel usage of AP is too high.
System usage(CPU/memory usage) above threshold	Defaults: Disabled. An alarm will be generated, when the system usage (CPU/memory usage) is higher than the threshold.
Switch loopback detected (RLDP)	Defaults: Disabled.
interface updown rate above threshold.	Defaults: Disabled.
Abnormal network access on gateway	Defaults: Enabled.
High packet loss rate on gateway	Defaults: Enabled. An alarm is generated when the packet loss rate of the gateway is high.
Uplink rate above threshold on gateway	Defaults: Enabled. An alarm is generated when the uplink rate of the gateway exceeds the threshold.
Downlink rate above threshold on gateway	Defaults: Disabled. An alarm is generated when the downlink rate of the gateway exceeds the threshold.

7.3.2 Sending Alarms via Email

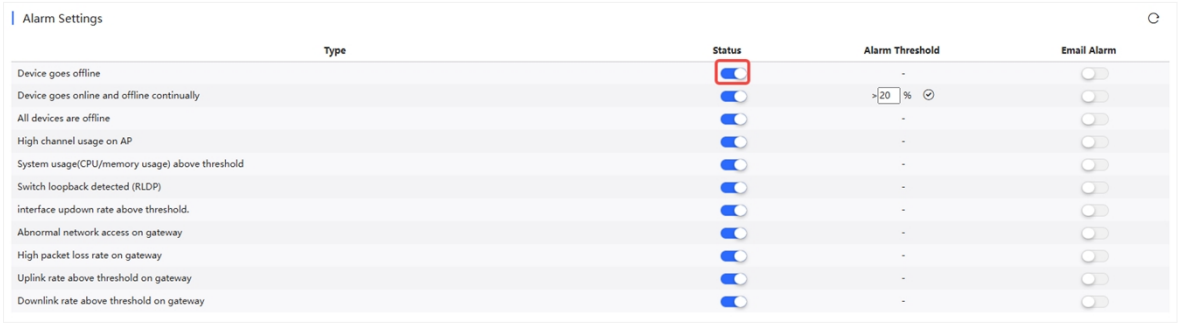
On the alarm settings page, you can set whether to send alarms via email. Alarms can only be sent via email when the alarm status is turned on. When email alarm function is enabled, the alarm will be sent via Email to contacts in the contact group.

The **Contact Group List** displays the contact groups used for receiving alarm.

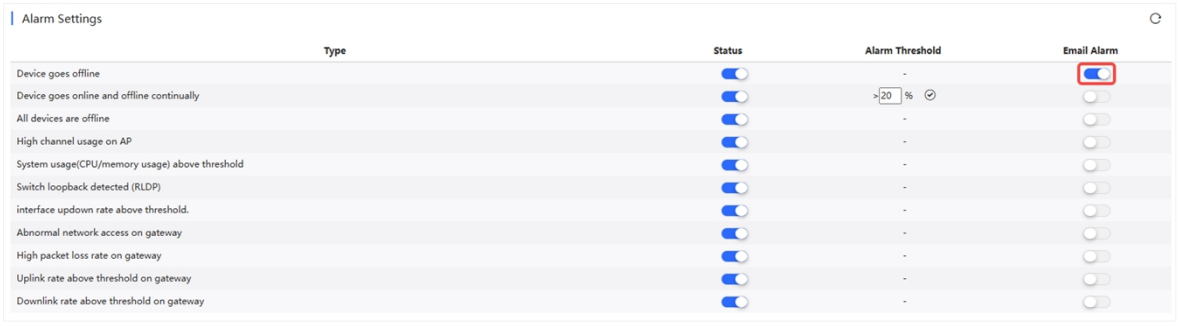


Follow the steps below to sending a specific alarm to the mailbox:

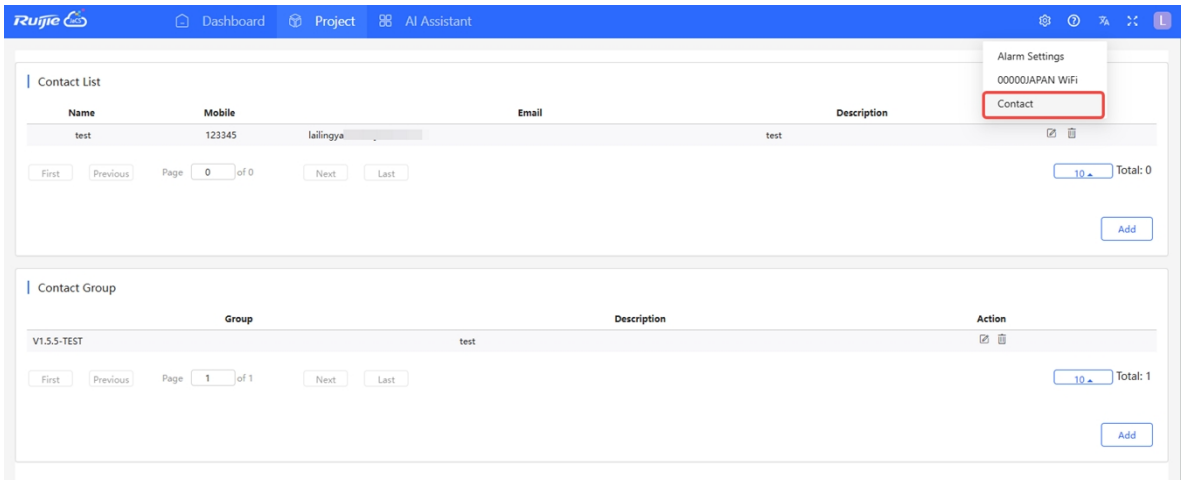
1 In the alarm setting page, turn on an alarm generation condition as needed.



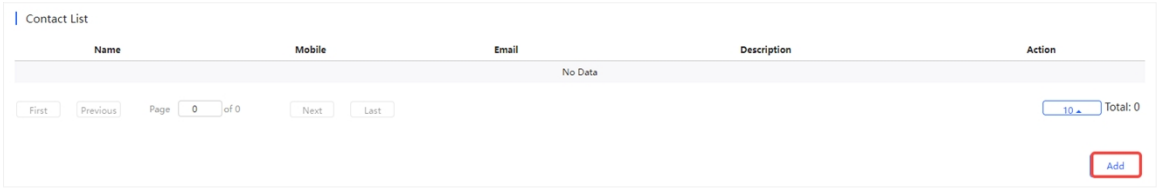
2 Enable email alarm function.



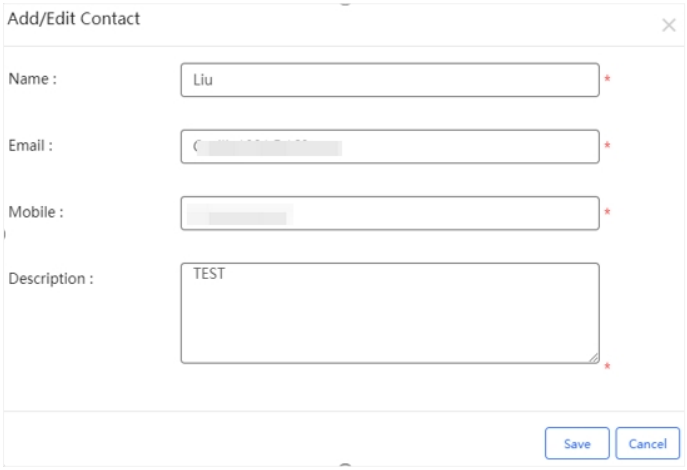
3 Click  and select **Contact**.



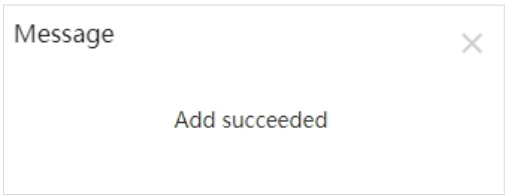
4 Click **Add** in **Contact List** to enter the contact setting page.

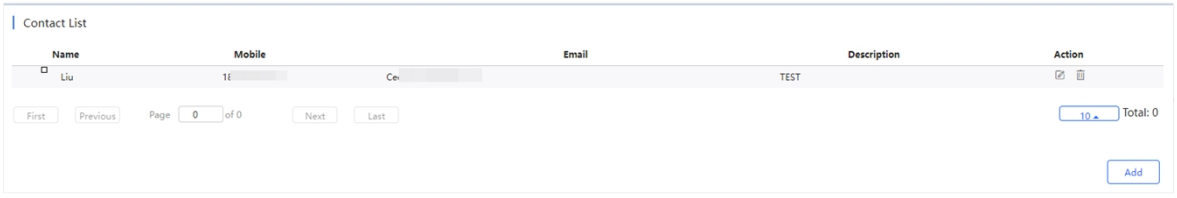


5 Specify the name, email address, mobile phone number and description, and then click **Save**.



6 When the "Added succeeded" prompt appears, click **X** to close the prompt box and complete the operation. The created contact will be displayed in the **Contact List**.

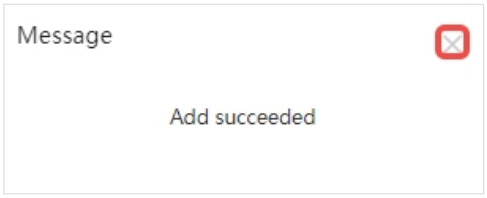




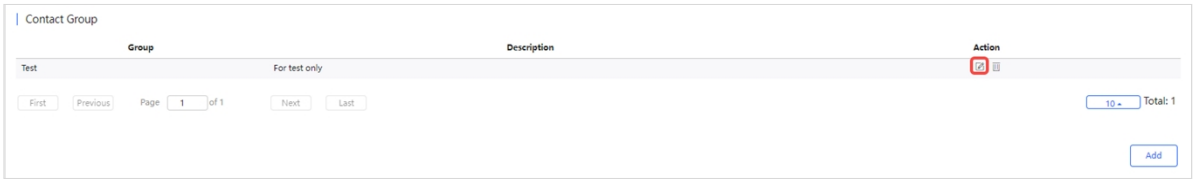
7 Click **Add** in **Contact Group** to create a contact group.

8 After setting the contact group name and description, click **Save**. The name and description are required.

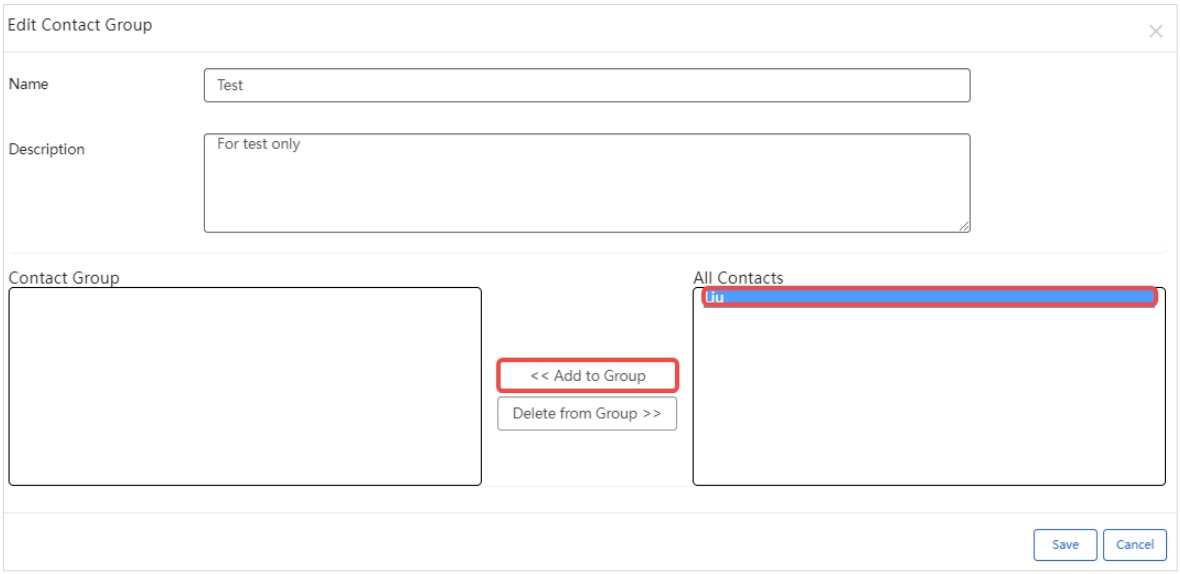
9 After the “Add succeeded” prompt appears, click **X** to close the prompt box.



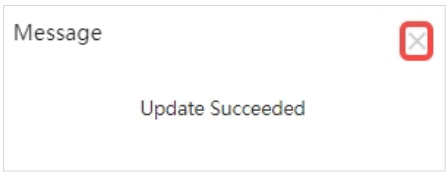
10 The created contact group will be displayed in the list. Click the  in the **Action** column of the contact group to add a contact to the contact group.



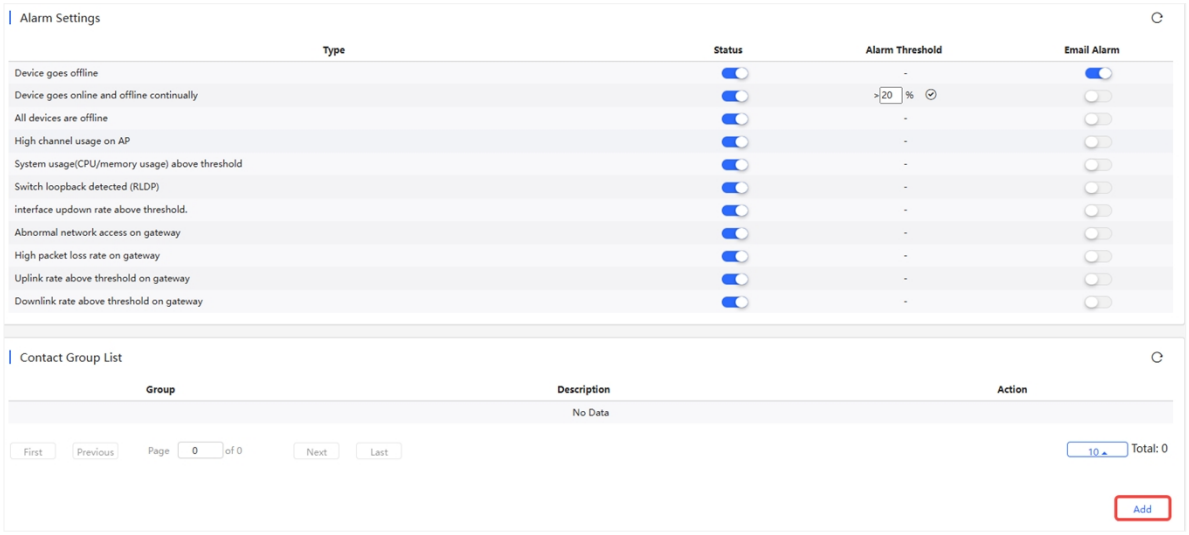
11 The contact information that has been created will be displayed in the **All Contacts** list. Select the contact you want to add and click **Add to Group** to add it.



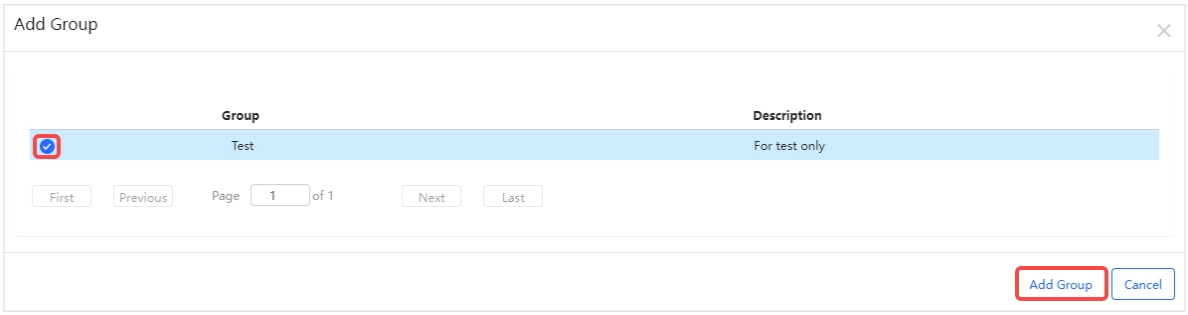
12 After adding, click **Save**. When the “Update succeeded” prompt appears, click **X** to close the prompt box.



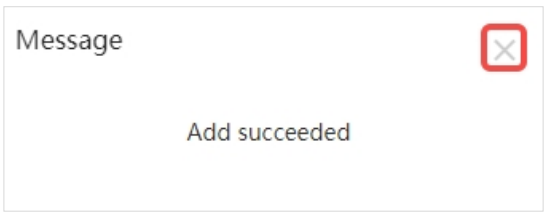
13 After creating the contact and adding it to the contact group, return to the alarm setting interface. In the **Contact List**, click **Add**.



14 Select the contact group you need and click **Add Group**.



15 After the “Add succeeded” prompt appears, click **X** to close the prompt box and complete the operation.



The added contact group will be displayed in the **Contact Group List**. After the contact group is added, when the device reaches the alarm condition, the alarm will be sent to the email address of the contacts in the contact group.

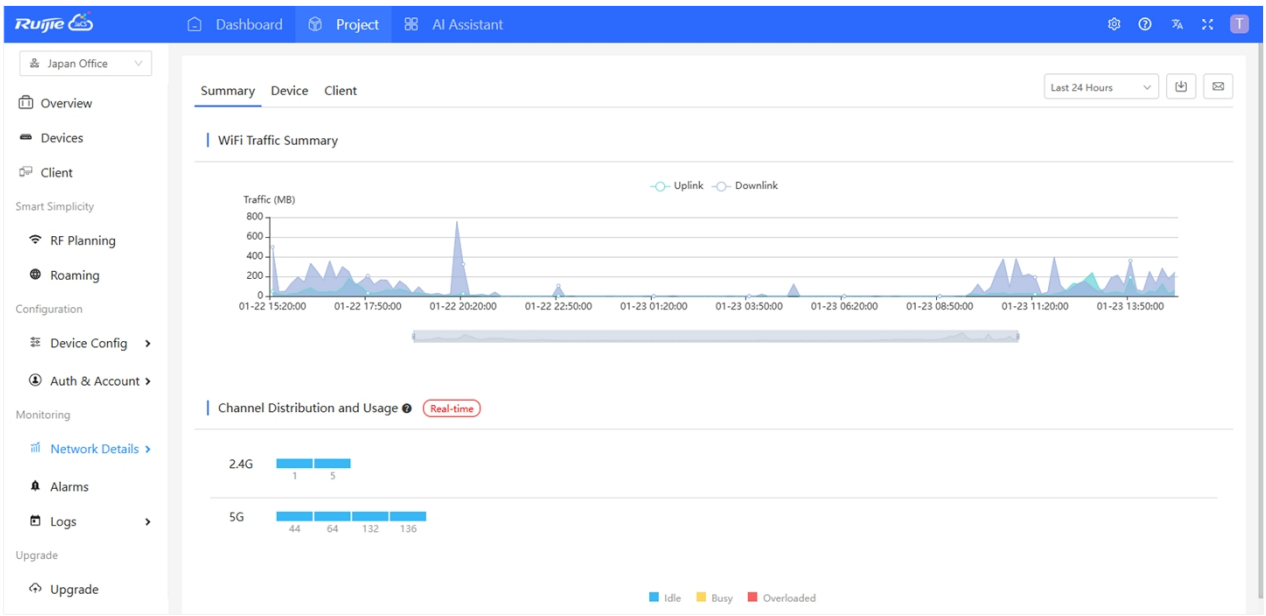
Note

If you enable email alarm function but do not add a contact group in the **Contact Group List**, you will not be able to receive alarms via emails.

7.4 Network Report

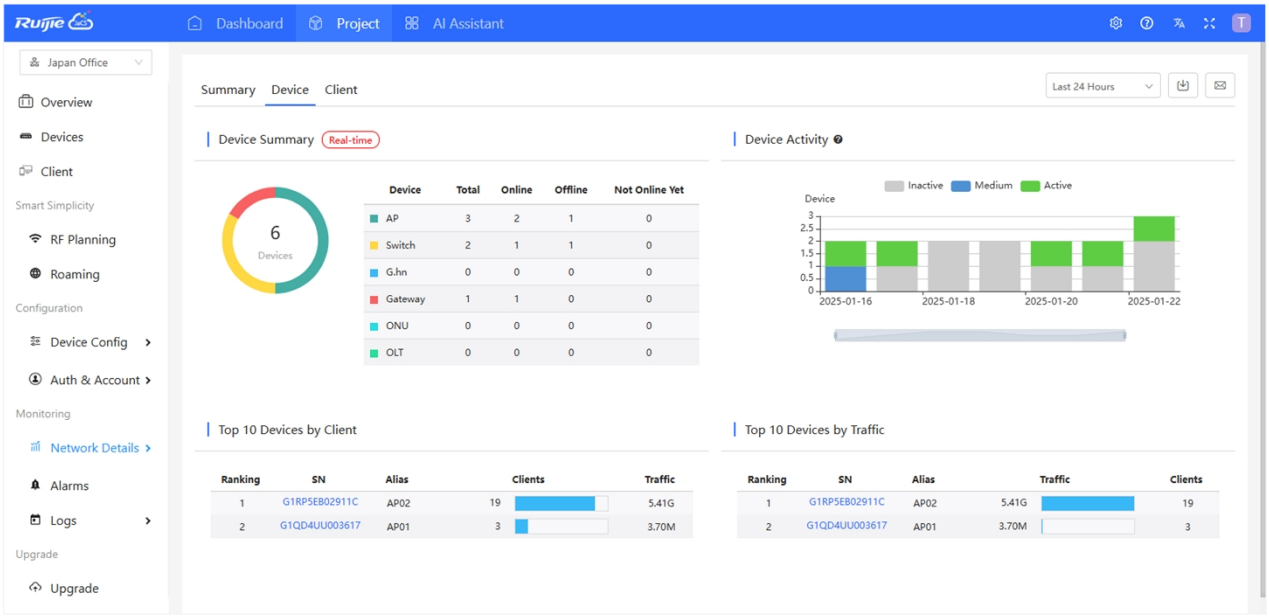
Click **Project** > **Network Details** > **Report** to go to the network report management interface. This interface consists of three parts: **Summary**, **Device**, and **Client**.

■ **Summary:**



Items	Description
WiFi Traffic Summary	Displays wireless traffic data for the last 24 hours/last 7 days/last 30 days/custom time period. Hover the cursor over a time to view the uplink and downlink rates at that time.
Channel Distribution and Usage	Displays channel distribution and usage of the selected project. Click a channel to view its detailed information. The channel usage is graded as: ● Idle: 0% to 59%; ● Busy: 60% to 79%; ● Overloaded: 80% to 100%
SSIDs by Client	Displays ranking information of the number of clients connected to the selected network by SSID in the last 24 hours/last7 days/last 30 days /custom time period
SSIDs by Traffic	Displays the SSIDs ranked by client number of the selected project in the past 24 hours/last 7 days/last 30 days/custom time period.
RSSI Statistics	Displays the real-time wireless signal strength of the selected project during the specific period. The signal intensity is defined as: (1) Weak: RSSI ≤-80dB; (2) Medium: -80dB < RSSI≤-70dB; (3) Strong: RSSI > -70dB.

■ **Device:**



Items	Description
Device Summary	Displays the online status of devices in the project during a specific period.
AP Activity	Displays the AP activity of the selected project 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. (1) Inactive: <5 active clients (2) Medium: 5-9 active customers (3) ≥10 active clients.
Top 10 APs by Client	Displays the top 10 APs ranked by client number of the selected project during the specific period.
Top 10 APs by Traffic	Displays the top 10 APs ranked by traffic of the selected project during the specific period.
Firmware Version	Displays the proportion of firmware versions of the selected project during the specific period.
Hardware Version	Displays the proportion of hardware versions of the selected project during the specific period.
PoE Utilization	Displays the numbers of PoE switches above and below the selected utilization percentage.
PoE Power Summary	Displays the power summary of the entire PoE device, including the total power and used power.

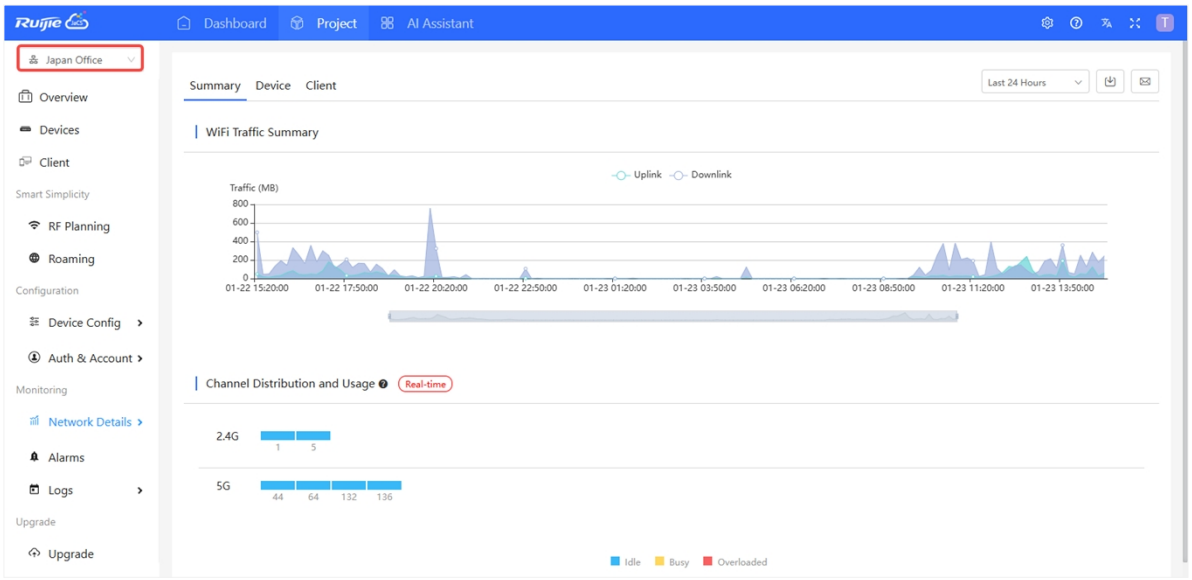
■ Client

Items	Description
WiFi Client Summary	This chart shows the client summary of the selected project during the specific period. Hover the cursor over a moment to view the number of clients at that moment.
WiFi Client Activity	This chart shows the client activity of the selected project during the specific period. The chart does not support searching data in the last 24 hours. (1) Inactive: ≤100KB traffic (2) Minimal: Any time and 100KB traffic (3) Low: 1h/d and 500K traffic (4) Medium: 2h/d time and 2M traffic (5) High: 4h/d time and 5MB traffic (6) Extreme: 8h/d time and 10MB traffic
2.4G/5G Clients	This chart shows the proportion of STAs using 2.4G/5G of the selected project during the specific period.
Top 10 WiFi Clients by Traffic	Displays the top 10 clients ranked by traffic of the selected network during the specific period.
Captive Portal	This chart shows the numbers and proportions of different portal authentication methods in the selected project. The statistics are refreshed every hour. Now 3 authentication methods (one-click, voucher and account) are supported.
Experience	This chart shows the experience status during the specified time and collects data every 5 minutes. You can switch between 2.4GHz and 5 GHz. Hover your cursor over a specific time to view the experience status at that time. (1) Excellent: HDV and online game are available. (2) Good: Communication application, Web page and VoIP are available. (3) Poor: Go offline frequently or hard to go online. (4) Inactive: Checks whether the client is inactive based on 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.

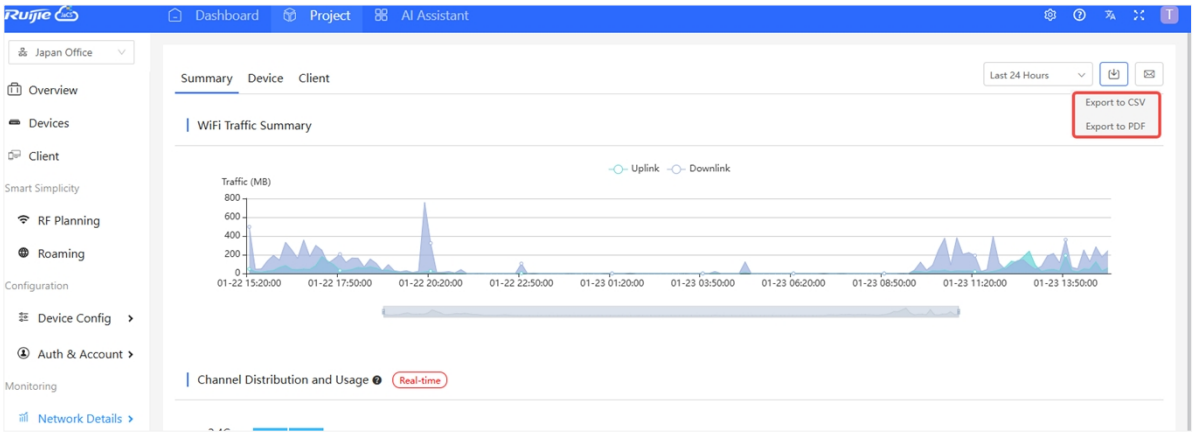
7.4.1 Exporting a Network Report

Follow the steps below to export a network report:

1 Select the project.



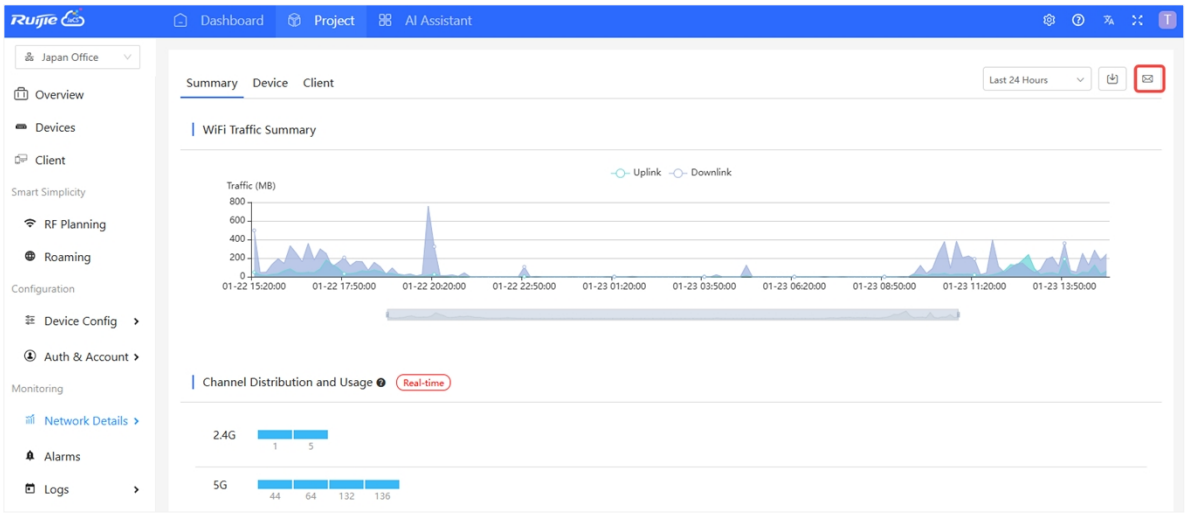
2 Click  and select the format. Supported formats include: CSV and PDF.



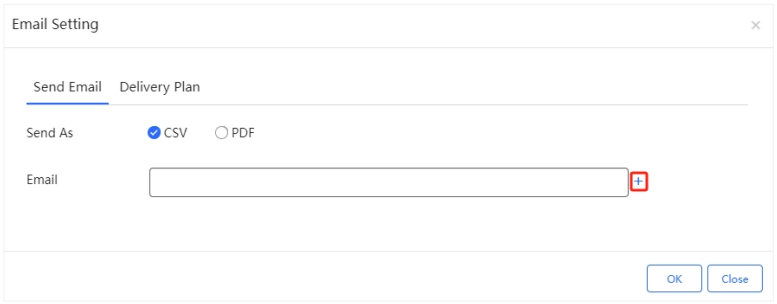
7.4.2 Sending Network Report to a Specified Mailbox

To send a network report to a specific Email address:

1 Select the project and go to the **Network Details** interface, and click in the network client interface.

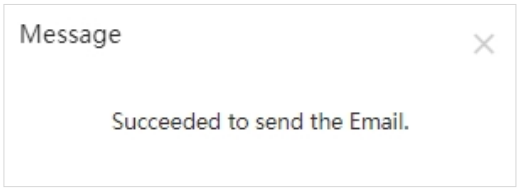


2 Select the report format and enter the email address. Click the **+** next to the email address to add more Email addresses. Up to 3 addresses are supported.



3 After filling in the information, click **OK**.

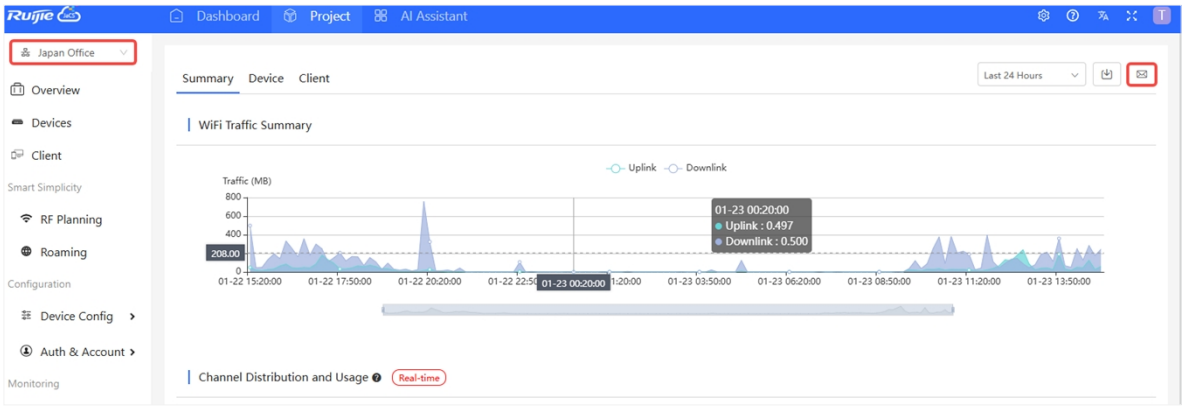
4 When the “Succeeded to send the Email” prompt appears, click **X** to close the prompt box and complete the operation.



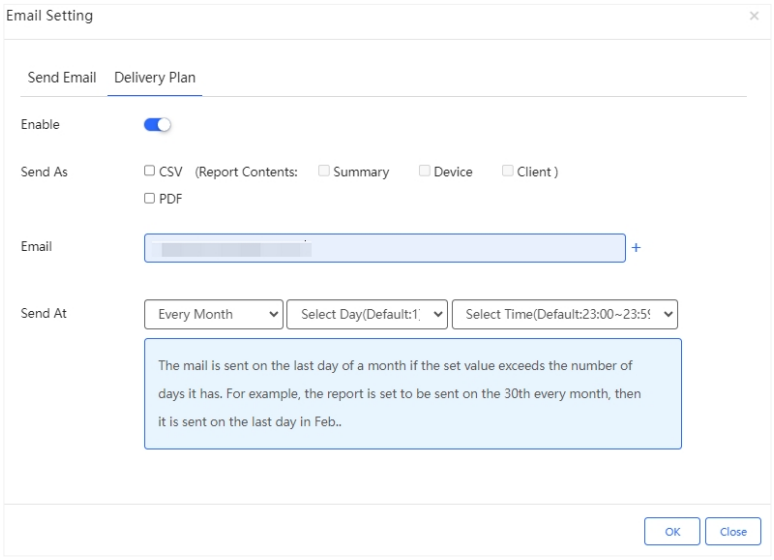
7.4.3 Sending Network Reports to a Specified Mailboxes Regularly

Follow the steps below to send network reports to your mailbox at a specific time:

1 Select a project and then click ✉.



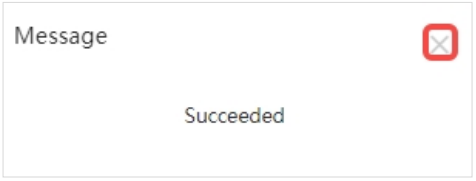
2 Switch to the **Delivery Plan** interface. Enable the scheduled delivery function, select the report format, enter the email address, and set the scheduled delivery time, then click **OK**.



Note

- Click the **+** next to the email address to add multiple email addresses. Up to 3 email addresses are supported.
- If the report document format is set to CSV, you can select the report content. If it is set to PDF, the entire content will be sent by default.

3 After the “Succeeded” prompt appears, click **X** to close the prompt box and complete the operation.



7.5 Viewing Client Information

In the **Project** interface, click **Client** to go to the client interface. In this interface, you can view the client information in a project. Click the **MAC address** of a client in the client list to view its detailed information.

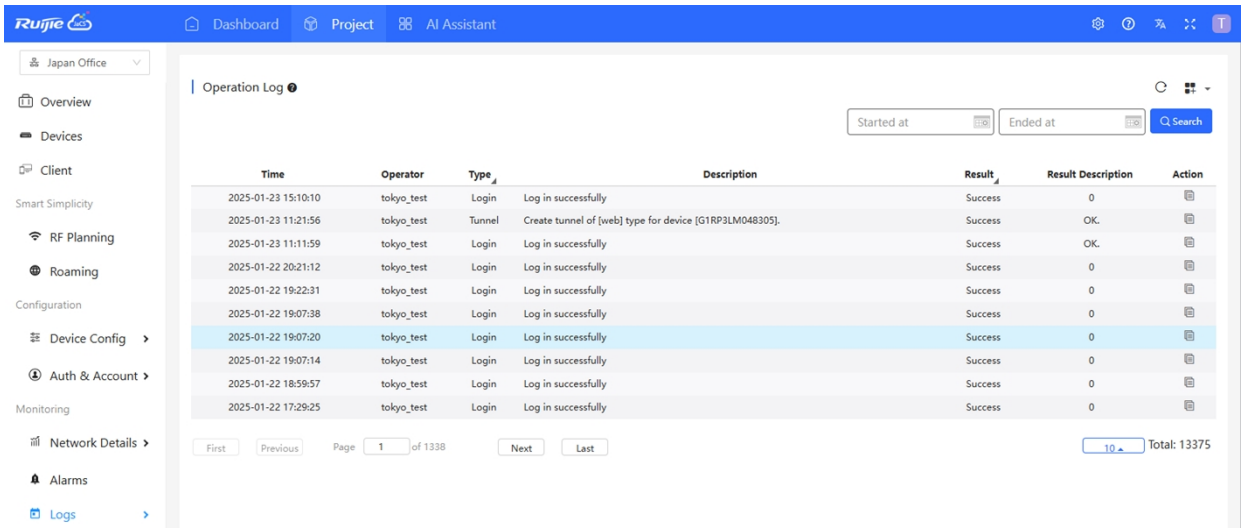
7.6 Viewing Logs

O&M personnel can view user's operation records in the JaCS. JaCS supports six types of log types, including:

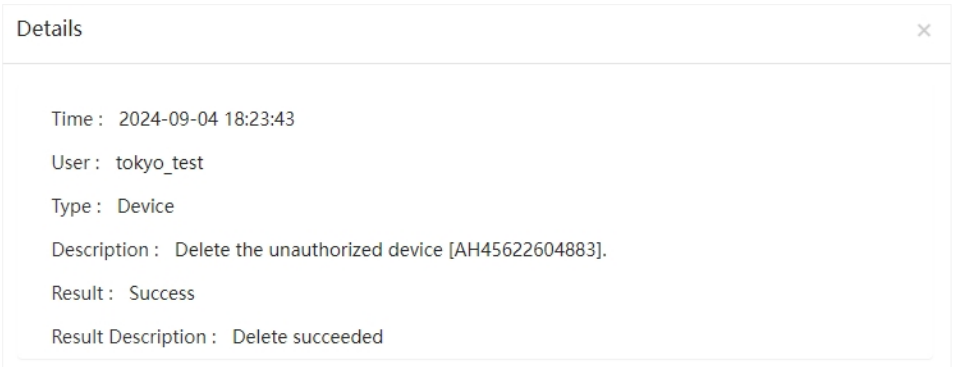
- Operation Logs
- Configuration Logs
- Upgrade Logs
- MESH Logs
- Replace Logs
- Setting Logs

7.6.1 Viewing Operation Logs

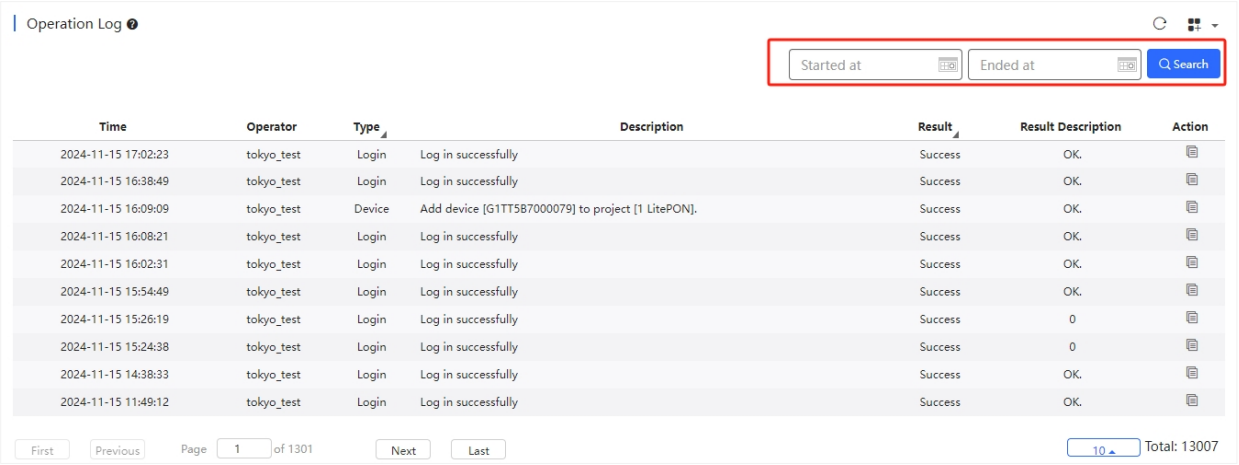
Click **Logs** > **Operation Log** to view all operation logs in the current project, including operation time, operator, operation type, operation description, result, and result description.



Click in the **Action** column to view the log details.



Supports filtering logs based on time periods.

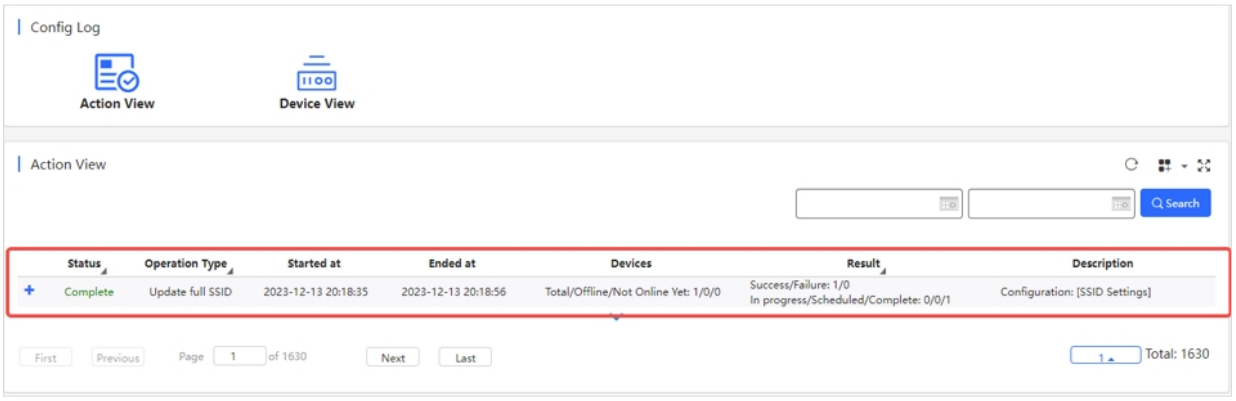

Operation Log
Started at
Ended at
Search
Time
Operator
Type
Description
Result
Result Description
Action
2024-11-15 17:02:23 tokyo_test Login Log in successfully Success OK.
2024-11-15 16:38:49 tokyo_test Login Log in successfully Success OK.
2024-11-15 16:09:09 tokyo_test Device Add device [G1TT5B7000079] to project [1 LitePON]. Success OK.
2024-11-15 16:08:21 tokyo_test Login Log in successfully Success OK.
2024-11-15 16:02:31 tokyo_test Login Log in successfully Success OK.
2024-11-15 15:54:49 tokyo_test Login Log in successfully Success OK.
2024-11-15 15:26:19 tokyo_test Login Log in successfully Success 0
2024-11-15 15:24:38 tokyo_test Login Log in successfully Success 0
2024-11-15 14:38:33 tokyo_test Login Log in successfully Success OK.
2024-11-15 11:49:12 tokyo_test Login Log in successfully Success OK.
First
Previous
Page 1 of 1301
Next
Last
10
Total: 13007

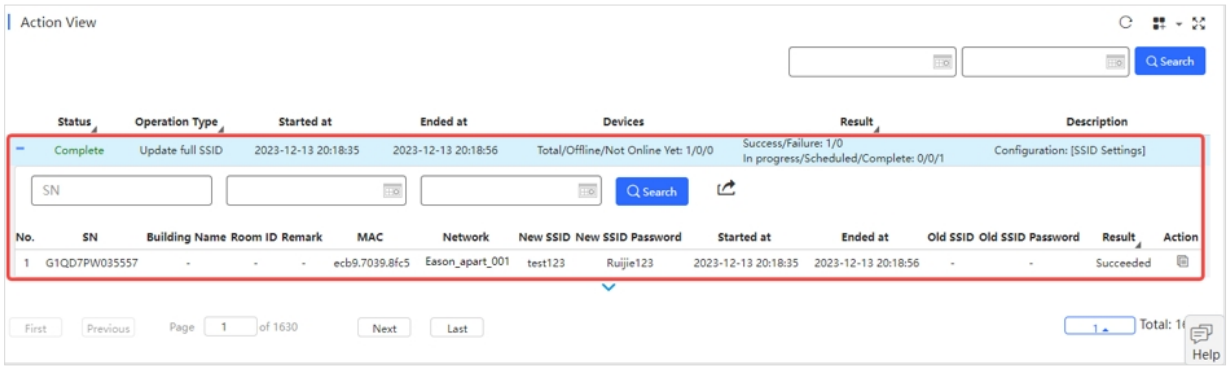
7.6.2 Viewing Configuration Logs

Click **Logs** > **Config Log** to go to the configuration log interface. The configuration log interface is divided into two parts: **Action View** and **Device View**, which shows different viewing dimensions. **Action View** is based on the operation type, and **Device View** is based on the device SN.

■ **Action View**

The **Activity View** displays the latest record by default. Click **+** to view more information about the log.



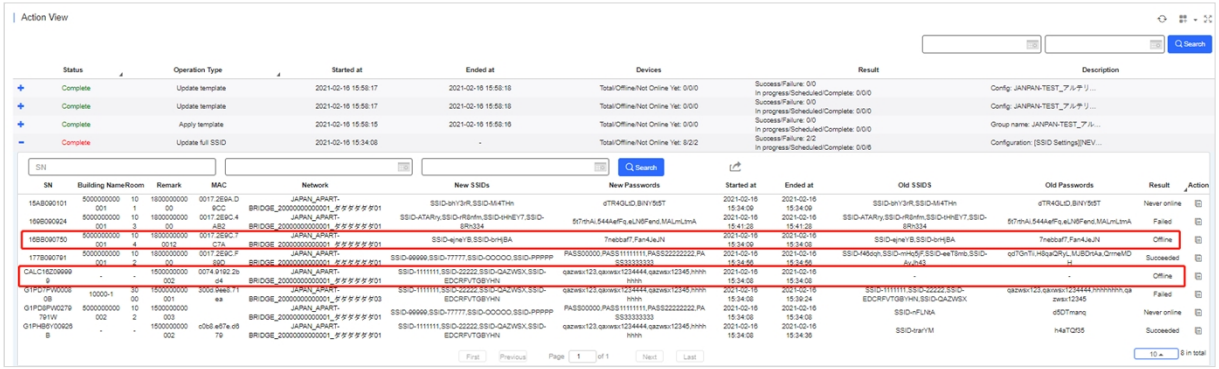


If you need to export an operation log, click to export the it. The imported configuration file is shown below:

	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				ecb9.7039.8fc5	Eason_apart_001	test123	Ruijie123	2023 12/13 07:18	2023 12/13 07:18			Succeeded
4													
5													

■ Configuring SSID and password for offline devices

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

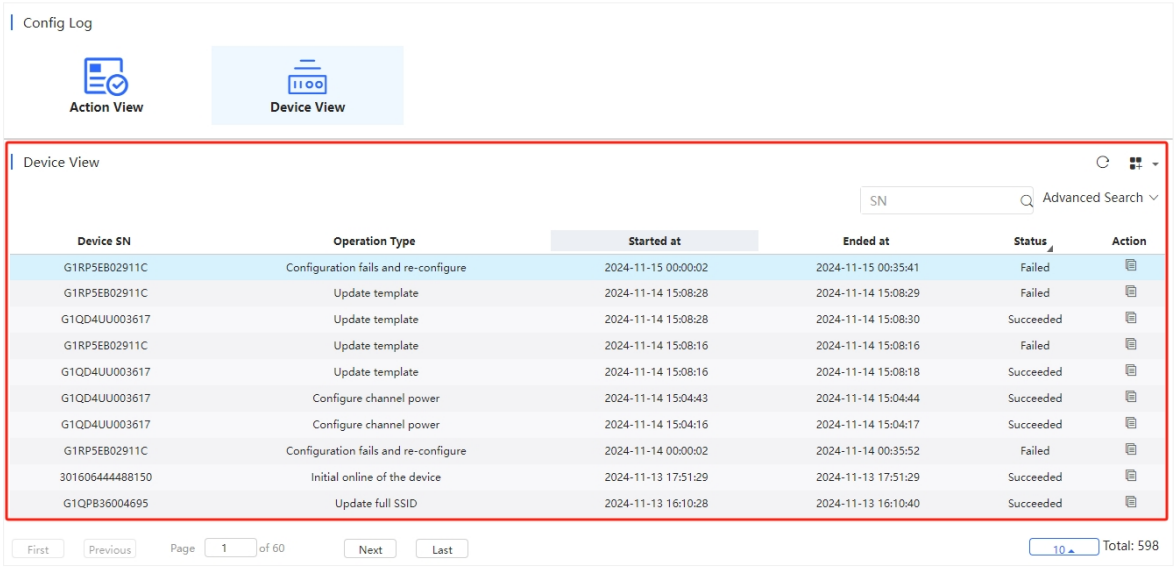


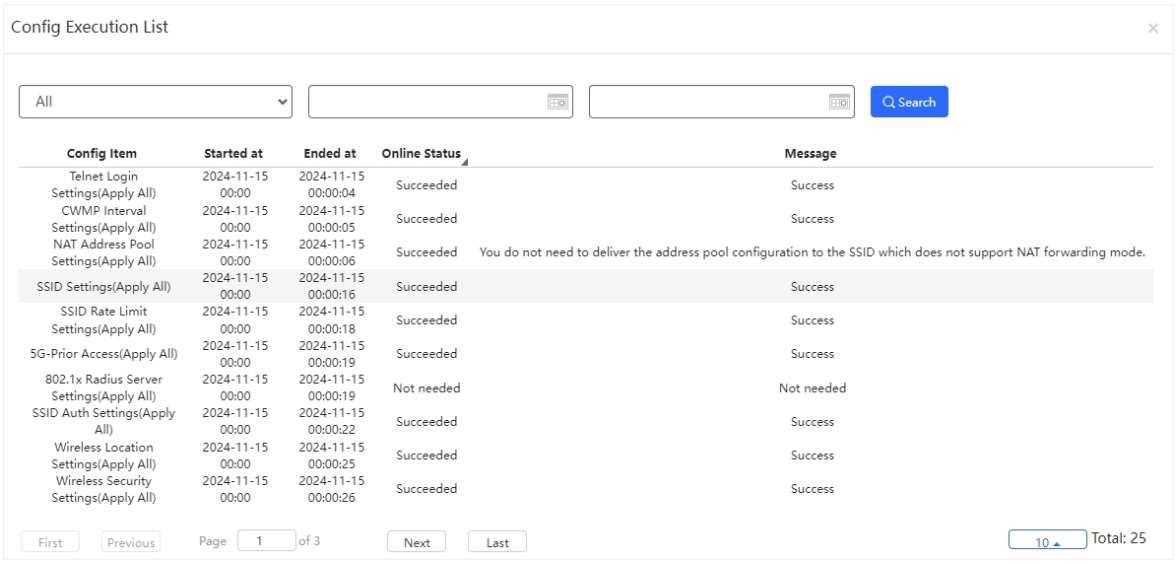
Although there are offline devices waiting for SSID and password configuration, the overall configuration is completed. The operator can export result and send new SSIDs/passwords to the tenant. When the offline devices go online, the new SSIDs and passwords will be synchronized to the devices automatically.

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	SSID and Password Change Form (Output)												
2	ID	Building Name	Room	Remark	MAC	Network	New SSIDs	New Passwords	Started	Ended	Old SSIDs	Old Passwords	Result
3	1	5000000000001	101	180000000000	0017.2E9A.D9CC	)GE_20000000000	-bhY3rR,SSID-MiTR4GLtD,BiNY5t5		2021 02/16 15:34	2021 02/16 15:34	)-bhY3rR,SSID-MiTR4GLtD,BiNY5t5		Never online
4	2	5000000000001	103	180000000000	0017.2E9C.4AB2	)GE_20000000000	-rR8nfm,SSID-tHl:AefFq,eLN6Fend,		2021 02/16 15:41	2021 02/16 15:41	)-rR8nfm,SSID-tHl:AefFq,eLN6Fend,		Failed
5	3	5000000000001	104	180000000000012	0017.2E9C.7C7A	)GE_20000000000	-ejneYB,SSID-brl*nebbaf7,Fan4JeJl		2021 02/16 15:34	2021 02/16 15:34	)-ejneYB,SSID-brl*nebbaf7,Fan4JeJl		Offline
6	4	5000000000001	102	180000000000	0017.2E9C.F89D	)GE_20000000000	-77777,SSID-OOC111111,PASS222		2021 02/16 15:34	2021 02/16 15:34	-mHq5iF,SSID-eeTqaQRyL,MJBDrtA		Succeeded
7	5			1500000000002	0074.9192.2bd4	)GE_20000000000	22,SSID-QAZWSXsx1234444,qazws		2021 02/16 15:34	2021 02/16 15:34			Offline
8	6	10000-1	3000	1500000000001	300d.9ee8.71ea	)GE_20000000000	22,SSID-QAZWSXsx1234444,qazws		2021 02/16 15:34	2021 02/16 15:39	22,SSID-EDCRFVsx1234444,hhhhhl		Failed
9	7	5000000000002	102	1500000000003		)GE_20000000000	-77777,SSID-OOC111111,PASS222		2021 02/16 15:34	2021 02/16 15:34	SSID-nFLNtA	d5DTmanq	Never online
10	8			1500000000002	c0b8.e67e.d679	)GE_20000000000	22,SSID-QAZWSXsx1234444,qazws		2021 02/16 15:34	2021 02/16 15:34	SSID-trarYM	h4aTQf35	Succeeded

Device View

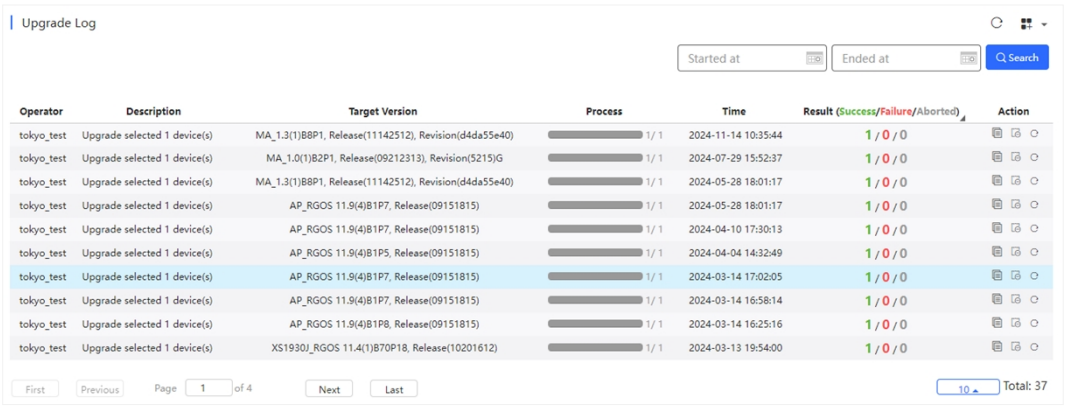
In the **Device View** interface, you can view the configuration log according to the device's SN. Click  in the **Action** column to view the push status of each configuration item.





7.6.3 Viewing Upgrade Logs

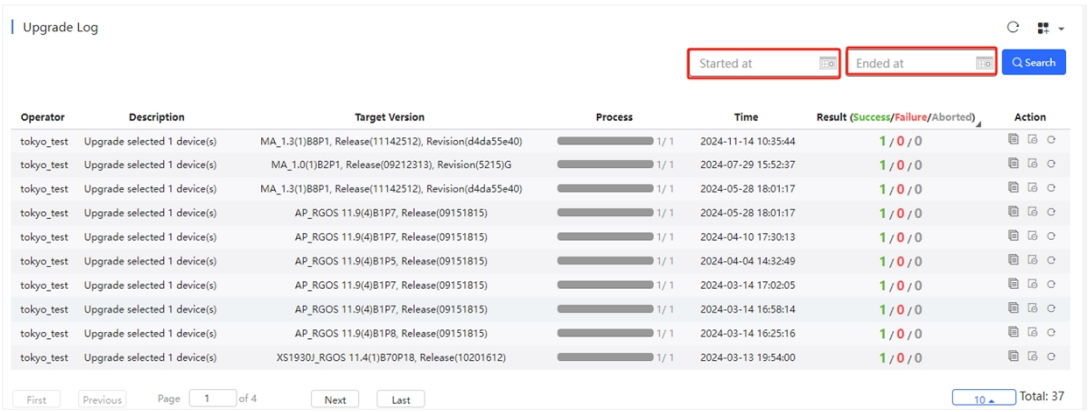
Click **Logs** > **Upgrade Log** to go to upgrade log interface. Here, you can track the upgrade results.

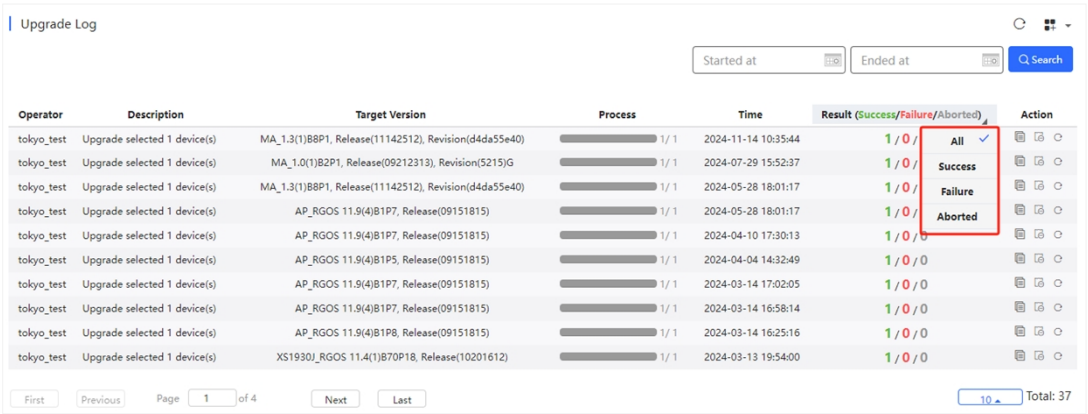


In the upgrade log operation column, three buttons are provided:

Buttons	Description
	Click this icon to view the details of the upgrade task.
	Click this icon to abandon the upgrade task.
	Click this icon to try the upgrade again.

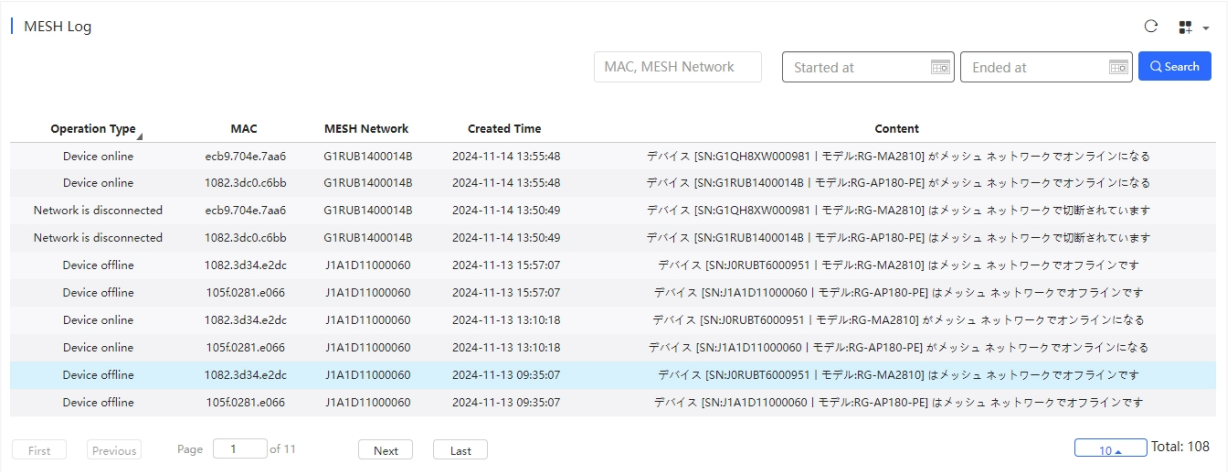
You can filter logs by setting a time period, or click the icon in the lower left corner of the **Result** column to filter logs based on upgrade results.





7.6.4 Viewing Mesh Logs

Click **Logs** > **Mesh Log** to go the mesh log interface. In this interface, you can view all Mesh-related log information, including operation type, MAC information, Mesh network, etc.



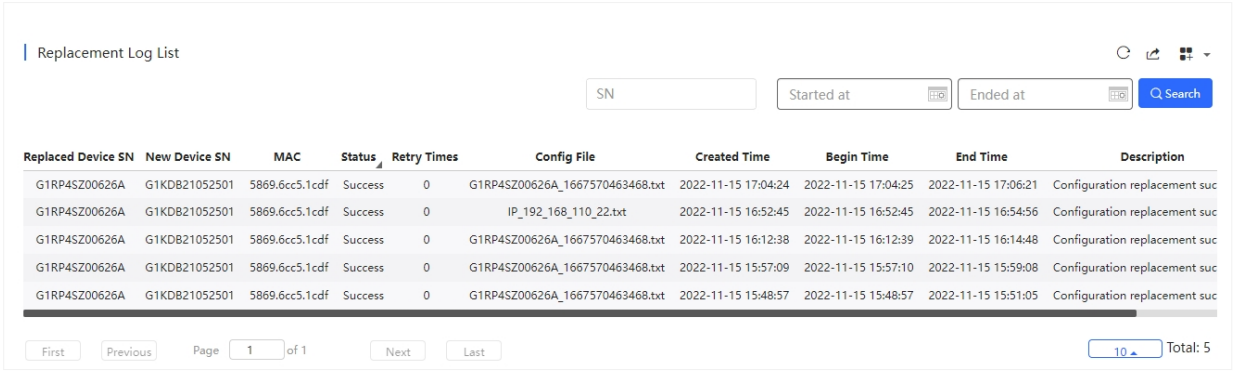
7.6.5 Viewing Replace Logs

Click **Logs** > **Replace Log** to go to the configuration replacement log interface. The log list displays the device's SN number, status, project, IP address, start time, end time, and creation time.

Five status are available in the **Status** column:

- Failed: The configuration of the old device failed to be applied to the new device.
- Success: The configuration of the old device has been applied to the new device.
- Waiting: Waiting for a new device to come online.
- Replacing: Configuration replacement is in progress.
- Abort: Configuration replacement task is terminated.

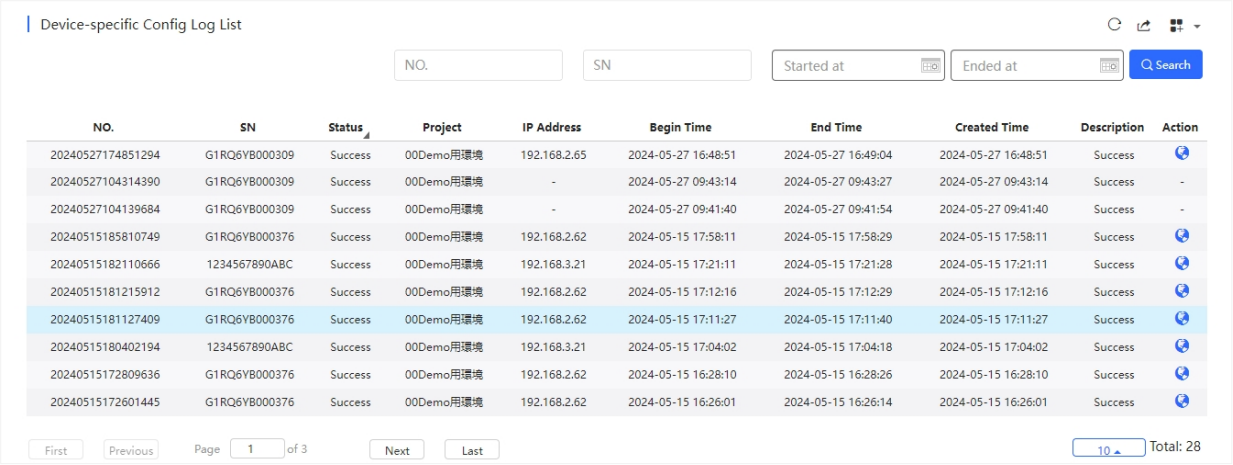
Click the ◢ icon on the lower right corner of **Status** column to filter the logs according to the replacement status, or filter the operation logs according to the device's SN and operation time period.



If the replacement status is "Waiting" and you need to terminate the configuration replacement task, you can click the icon in the **Action** column. After the confirmation prompt appears, click **OK**.

7.6.6 Viewing Setting Logs

Click **Logs** > **Setting Logs** to go to the setting log interface. The setting log interface displays the device-specific configuration logs. The log list displays the batch number, SN, status, project, IP address, start time, end time, creation time, and description. The log can be filtered by status, batch number, and time period. Click in the **Action** column to jump to the eWeb interface of the device.

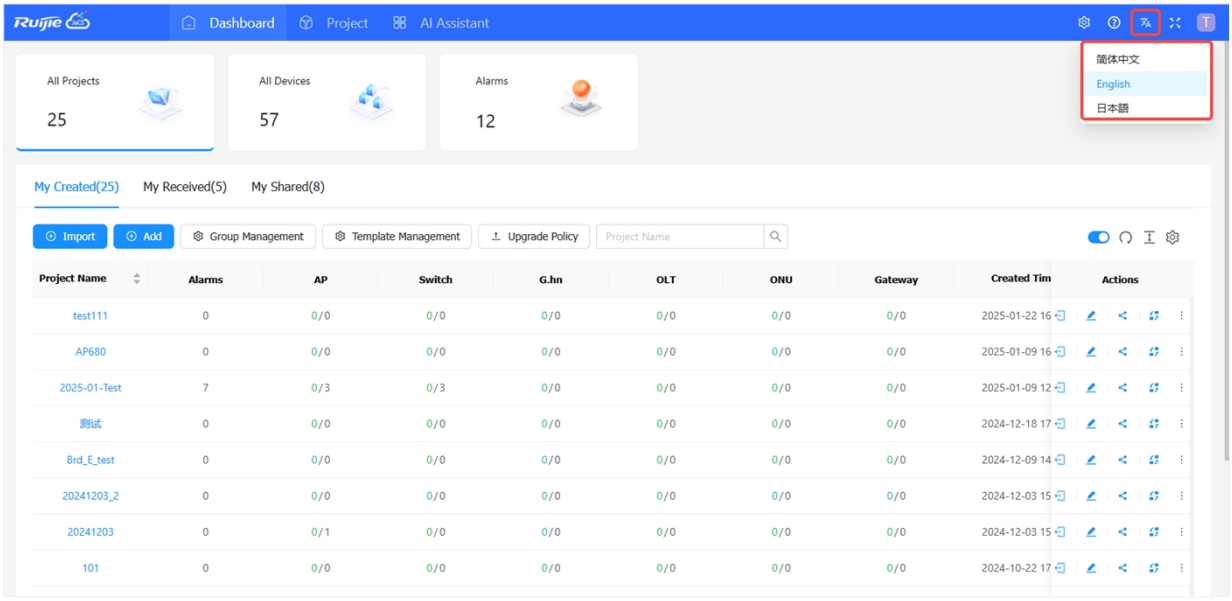


8 System Settings

8.1 Switching the System Language

Currently, Ruijie JaCS supports three languages: Simplified Chinese, English, and Japanese. The system language follows the browser language by default.

To switch the system language, click the icon and then select the language you need.



8.2 00000JAPAN Wi-Fi Setting

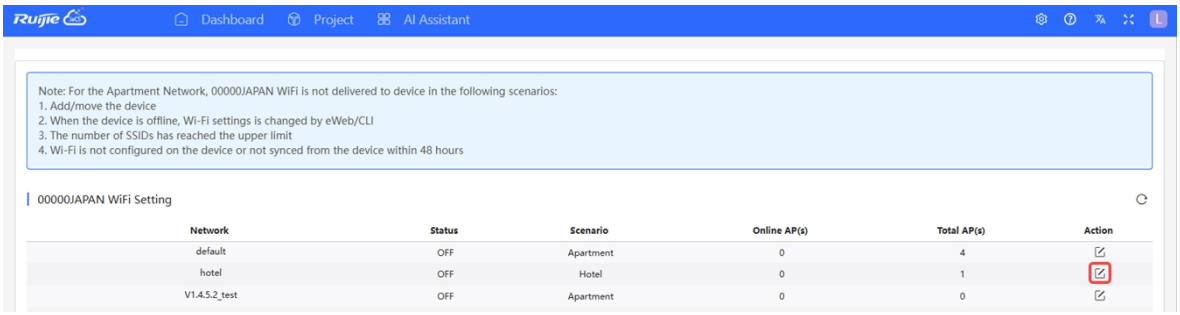
00000JAPAN WiFi is a free Wi-Fi with no requirement for authentication. When a disaster occurs, it can be quickly enabled and deployed to provide Internet access.

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.

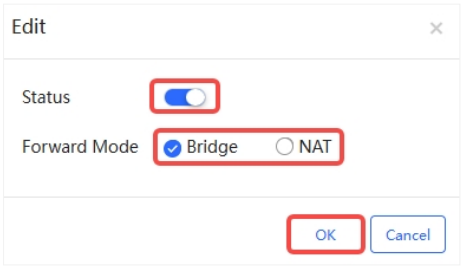
00000JAPAN WiFi is globally disabled by default. To enable 00000JAPAN WiFi, click and then click **00000JAPAN WiFi** to go to the setting interface. The interface shows the names of all layer-1 networks (root networks) under the current tenant. When the 00000JAPAN WiFi function in the network is enabled, all the devices in the subnetworks will simultaneously enable 00000JAPAN WiFi.

Follow the steps below to enable 00000JAPAN WiFi on your network:

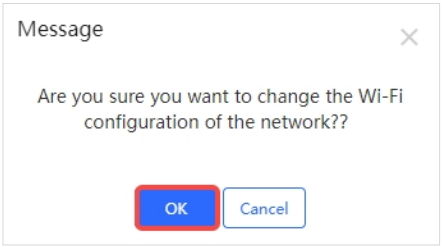
1 Click in the **Action** column of the corresponding network name.



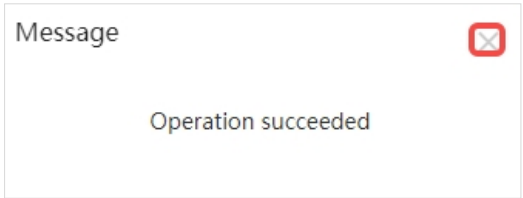
2 Enable the function, select the forward mode (only available for non-apartment scenario), and click **OK**.



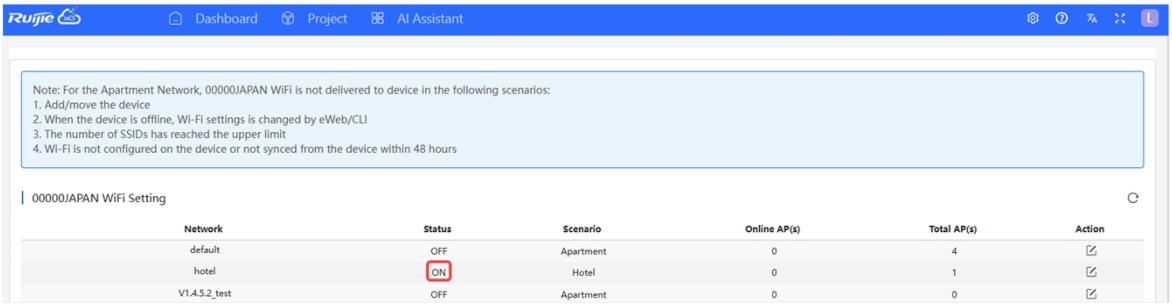
3 When the confirmation prompt appears, click **OK**.



4 When the "Operation succeeded" prompt appears, click **X** to close the prompt box and complete the operation.

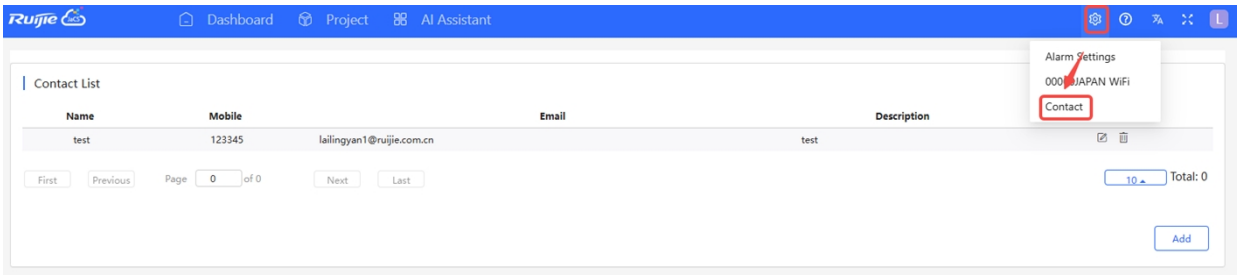


After the 0000JAPAN WiFi is enabled, “ON” is displayed in the status column.



8.3 Contact/Contact Group Management

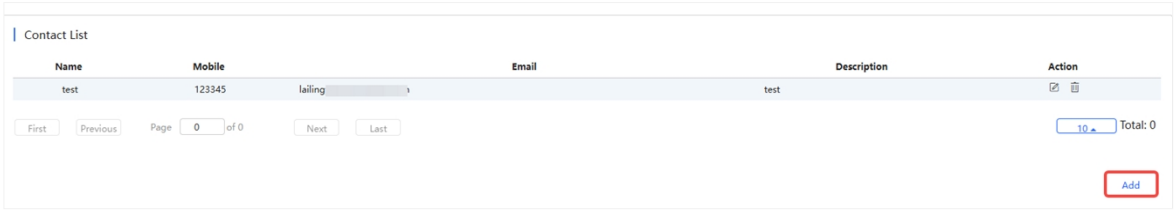
Click , and then click **Contact** to enter the setting interface. In the **Contact** configuration interface, you can create contacts and contact groups for receiving alarm information.



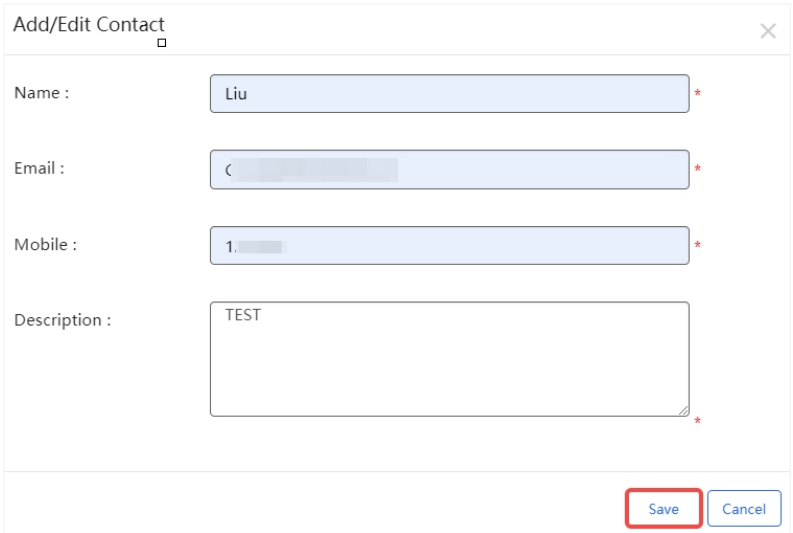
8.3.1 Adding a Contact

Follow the steps below to add a contact:

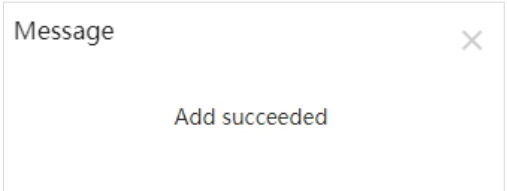
1 Click **Add**.



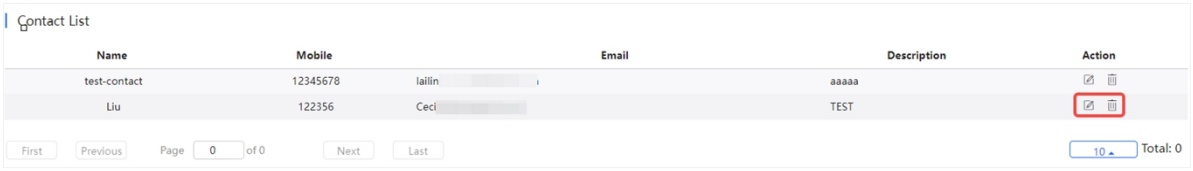
2 Fill in the information, and the click **Save**. Name, email address, mobile phone number and description are required.



3 When the "Added succeeded" prompt appears, click X to close the prompt box. The created contact will be displayed in the Contact List.



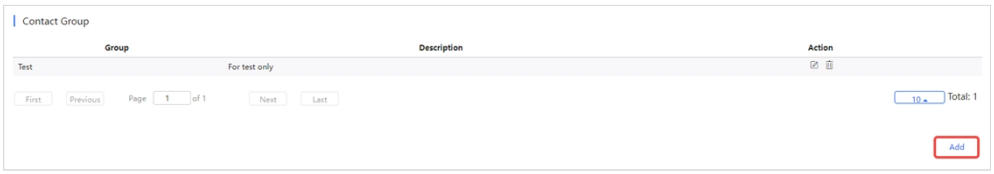
To edit a contact, click the in the Action column; To delete a contact, click to delete it.



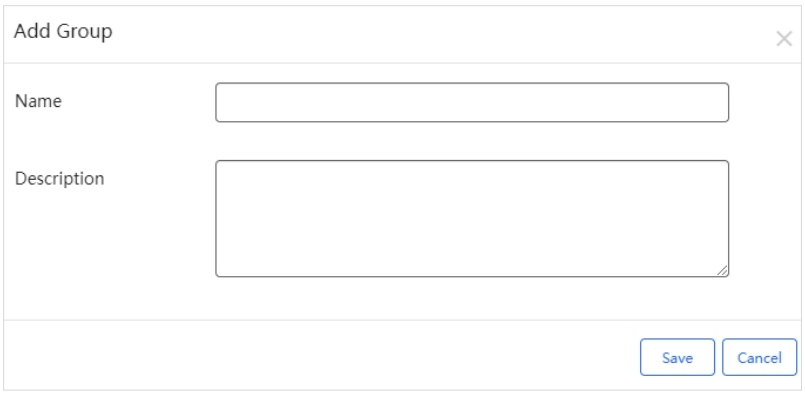
8.3.2 Creating a Contact Group

Follow the steps below to create a new contact group:

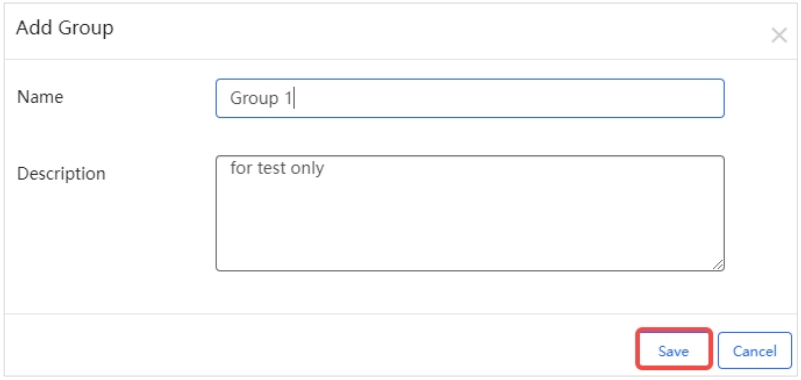
1 Click **Add**.



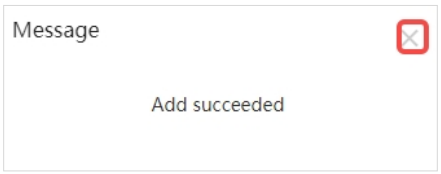
2 Enter a contact group name and description. Both name and description are required.



3 After filling in the form, click **Save** to complete the operation.



4 When the successful addition prompt appears, click **X** to close the prompt box and complete the operation.

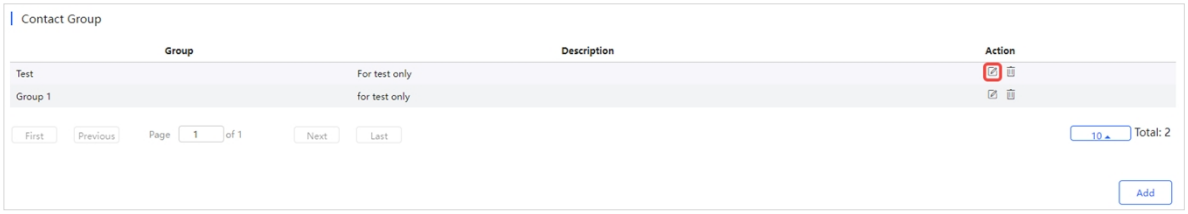


Once a contact group has been added, it will be displayed in the contact group list. To edit its information, click  in the **Action** column. To delete the contact group, click  in the **Action** column.

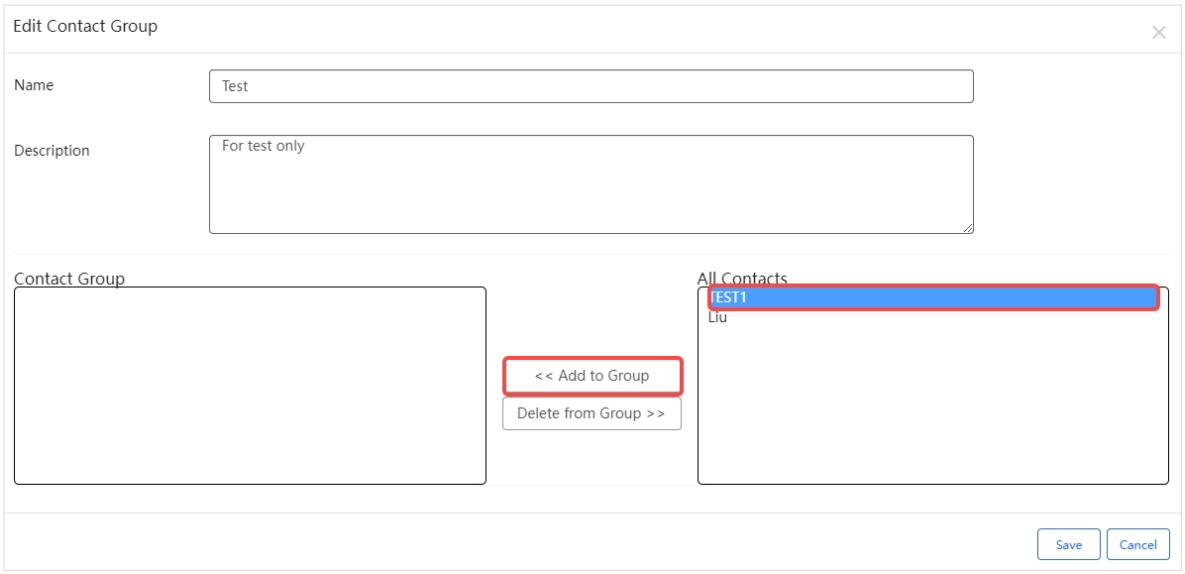
8.3.3 Adding Contacts to a Contact Group

To add a contact to an existing contact group:

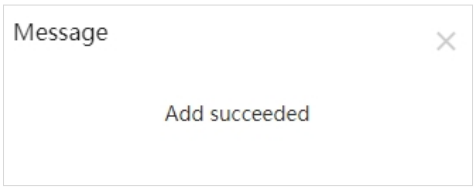
1 In the **Contact Group** list, click  in the **Action** column of a contact group.



2 The contacts that have been created will be displayed in the **All Contacts** box. Select the contact you want to add and click **Add to Group** to add it to the contact group. After adding the contact, click **Save**.



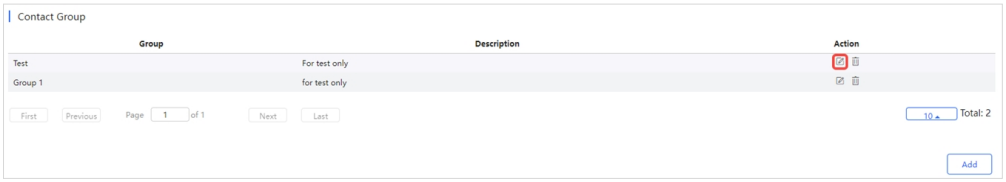
3 When the “Add succeeded” prompt appears, click **X** to close the prompt box and complete the operation.



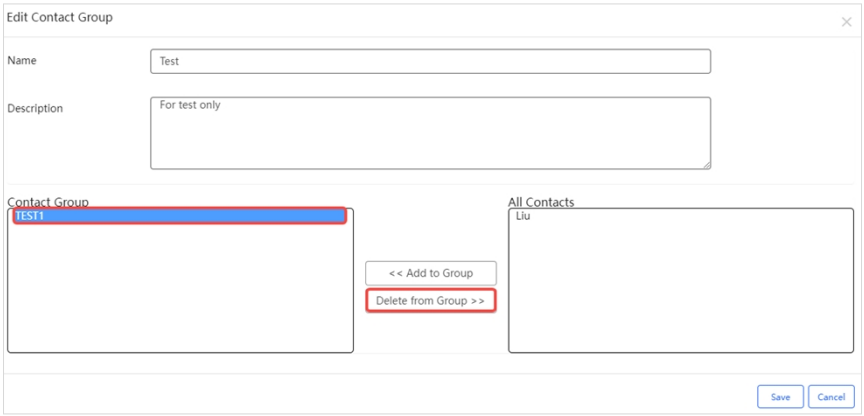
8.3.4 Removing a Contact from a Contact Group

To remove a contact from a contact group:

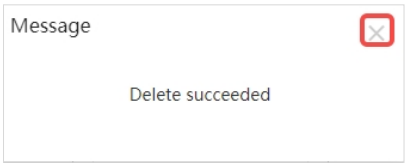
1 In the **Contact Group** list, click  in the **Action** column of a contact group.



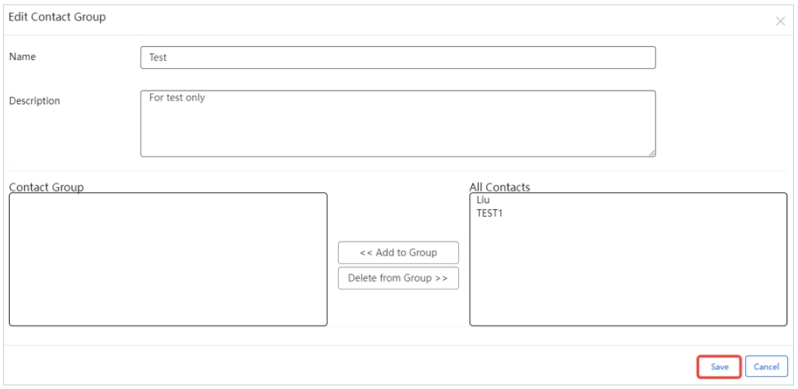
2 After selecting the contact to be removed from the contact group, click **Delete from Group**.



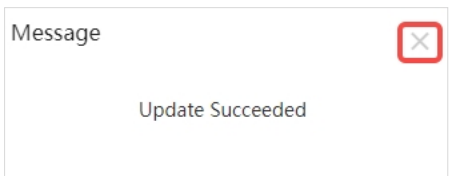
3 When the “Delete succeeded” prompt appears, click **X** to close the prompt box.



4 The removed contacts will be displayed in the **All Contacts** box on the right. Click **Save**.



5 After the “Update Succeeded” prompt appears, click **X** to close the prompt box and complete the operation.

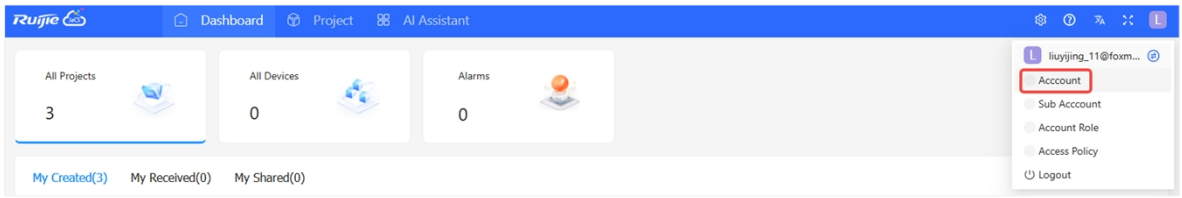


9 Account Management

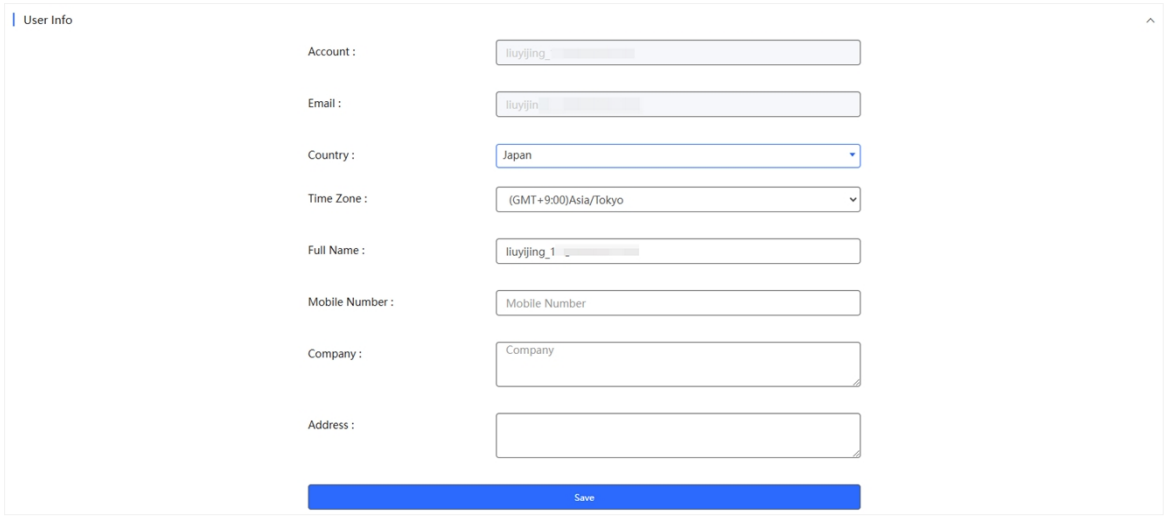
9.1 Changing the Account Information

Follow the steps below to modify the basic information of the account. The account name and registered email address cannot be changed.

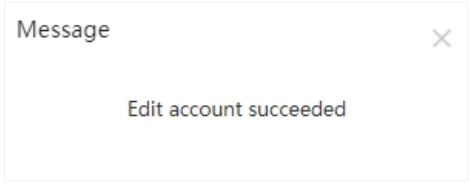
1 Click **Account** to enter the modification interface.



2 You can modify the country, time zone, full name, mobile phone number, company name and address of your account. Mobile phone number, company name and address are not mandatory items. After modifying as needed, click **Save**.



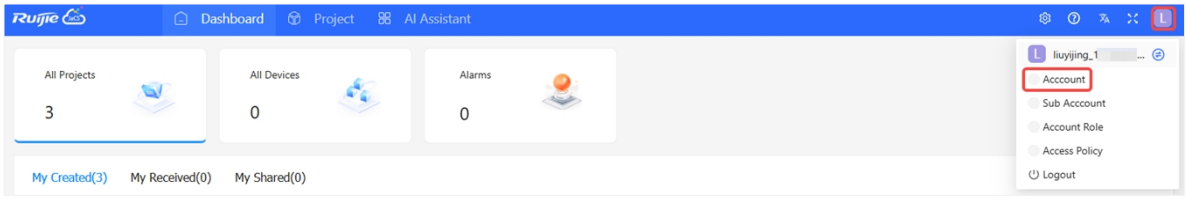
3 After the "Edit account succeeded" prompt appears, click **X** to close the prompt box and complete the modification.



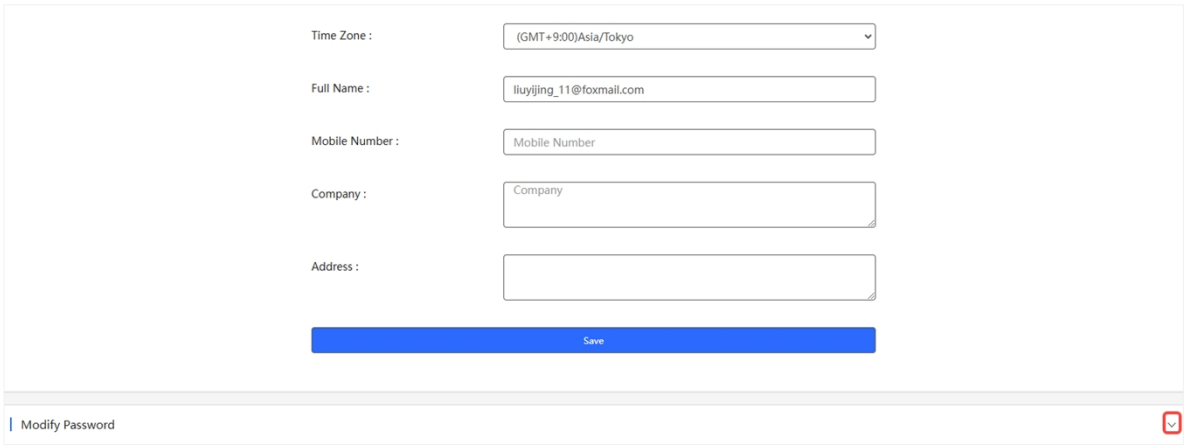
9.2 Changing the Account Password

To changing your account password:

1 Click the account icon and select **Account** to enter the modification interface.



2 Click the icon on the **Modify Password** interface to expand the password modification interface.



3 After entering the old password and setting a new password, you need to enter the new password again for confirmation, and then click **Save**.

4 When the "Password change succeeded" prompt appears, click **X** to close the prompt box and complete the operation.

Note

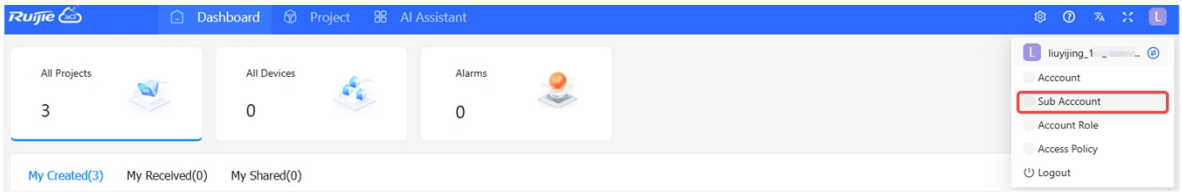
If you forget your original account password, please refer to 2.3 Resetting Password to reset it.

9.3 Sub-account Management

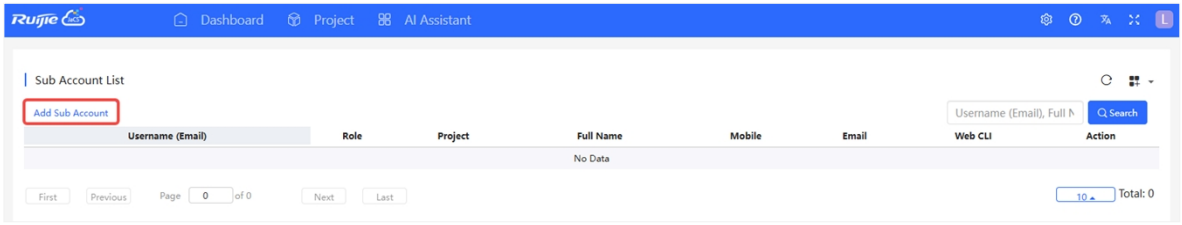
9.3.1 Creating a Sub-account

Follow the steps below to create a sub-account for a project:

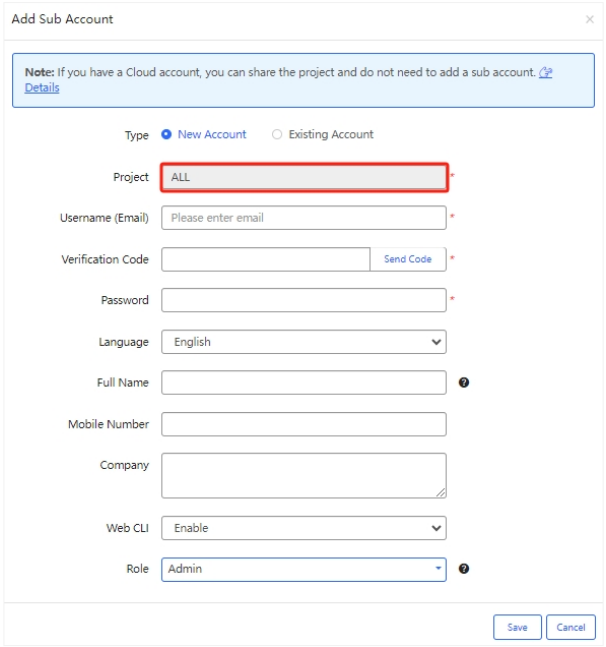
1 Click **Subaccount** to go to the subaccount management interface.



2 Click **Add Sub Account**.



3 Select **New Account**, and then set the project to be managed by the sub-account and fill in the subaccount information.



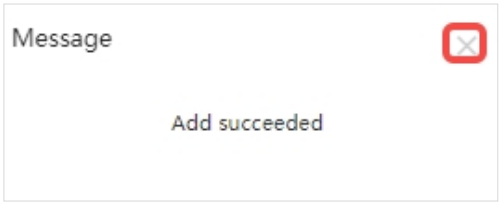
Items	Description
Username (Email)	Required. Set the user name (email address). The entered email address must have not been registered on the JaCS.
Verification Code	Required. Enter the verification code sent to your mailbox.

Password	Required. Set a subaccount password. The password must contain at least three of the following character types: uppercase letters, lowercase letters, numbers, and special symbols. The password length is 8-16 characters.
Language	The default language is English. Japanese and Chinese are also supported.
Full Name	Set the account name. If it is left blank, it will be set to the username (email address) by default.
Mobile Number	Optional. Set your phone number.
Company	Optional. Set company information. Up to 255 characters can be entered.
Web CLI	Enable or disable Web CLI function. This function is enabled by default.
Role	Set the subaccount role. Four roles are supported by default: ● Admin: owns the administration permissions; ● Employee: owns the administration permissions; ● Operator: owns the permissions to manage authentication; ● Guest: only owns read permission. Support customizing roles. For specific operation steps, please refer to section 9.3.3 Customizing Sub-account Roles.

Note

If the sub-account only needs reading permissions, you need to set the Web CLI to "Disable". If the sub-account needs operation permissions, set the Web CLI to "Enable" and set the role to "admin".

4 After filling in the information, click **Save** to save it. When the "Added succeeded" prompt appears, click **X** to close the prompt box and complete the operation. The added sub-account will be displayed in the sub-account list.

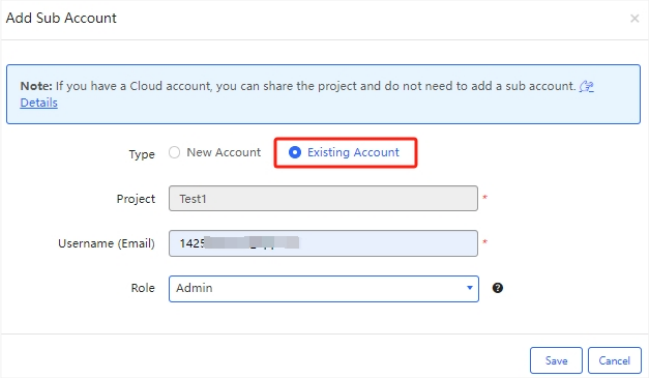


9.3.2 Setting an Existing Account to be a Sub-account

To set an existing account to be sub-account to manage projects:

1 Click **Add Sub Account**.

2 Select **Existing Account**, enter the email address, set the role, and click **Save** to complete the operation.

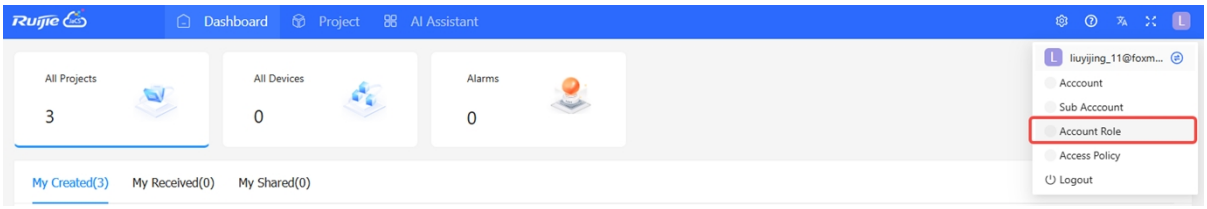


9.3.3 Customizing Subaccount Roles

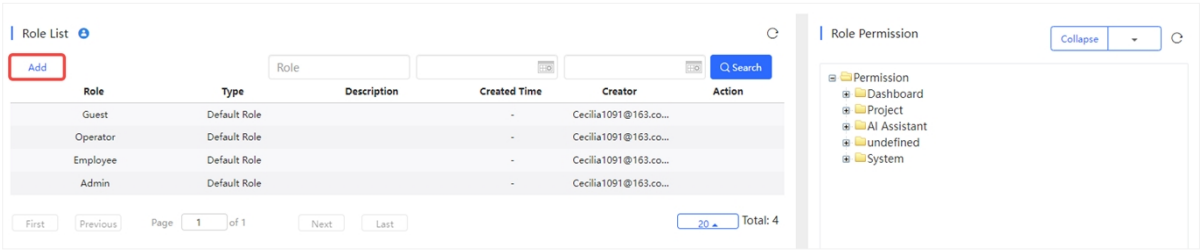
Ruijie JaCS supports four kinds of sub-account roles by default: **Admin** (owns management permissions), **Employee** (owns management permissions), **Operator** (only owns authentication management permissions), and **Guest** (only owns read permissions). These four default roles cannot be deleted.

In addition to these four roles, the JaCS allows users to customize sub-account roles to define the permissions by themselves. The specific steps are as follows:

1 Click **Account Role** to go to the role management interface.



2 Click **Add**.

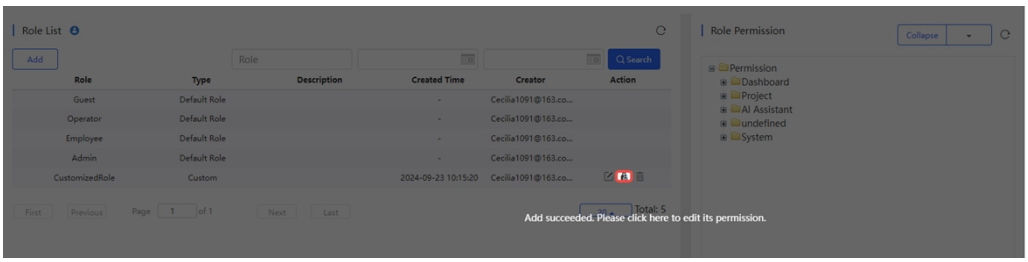


3 Set the role name (required), and description (optional), then click **Save**.

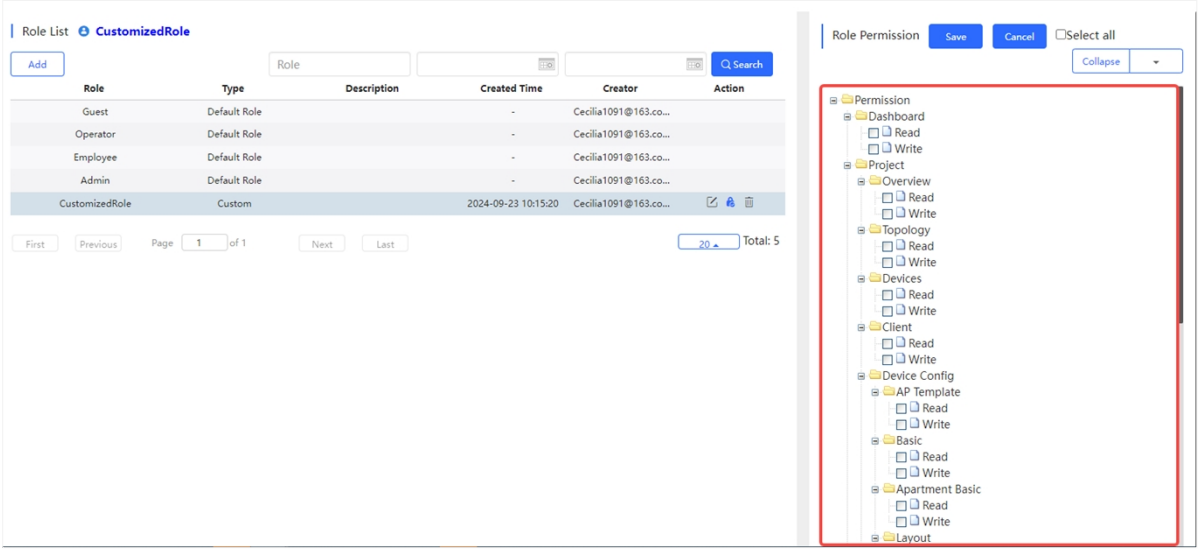
Note

- The description can contain up to 128 characters.
- The role name only supports numbers, letters, dashes (-), underscores (_), and special characters (“#”, “.” and “@”). The supported length is 1-64 characters.

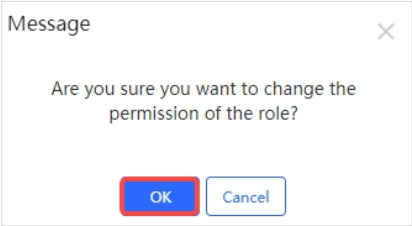
4 After setting the role information click  to configure account permissions.



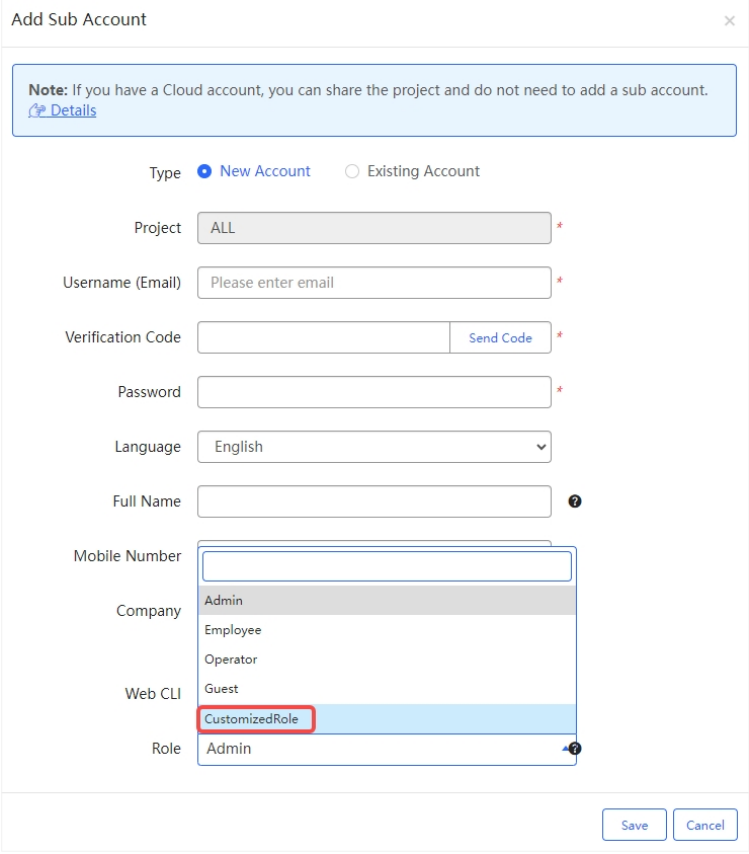
5 On the **Role Permission** page on the right, check the permissions according to your needs, and then click **Save**.



6 When the operation confirmation box appears, click **OK** to complete the configuration.



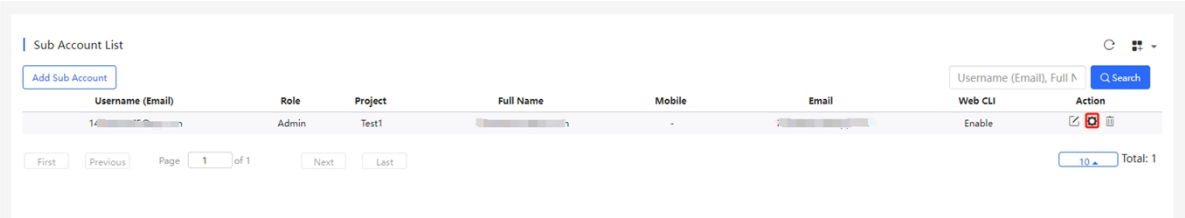
After the custom role is created, you can select the custom role on the sub-account adding or editing interface.



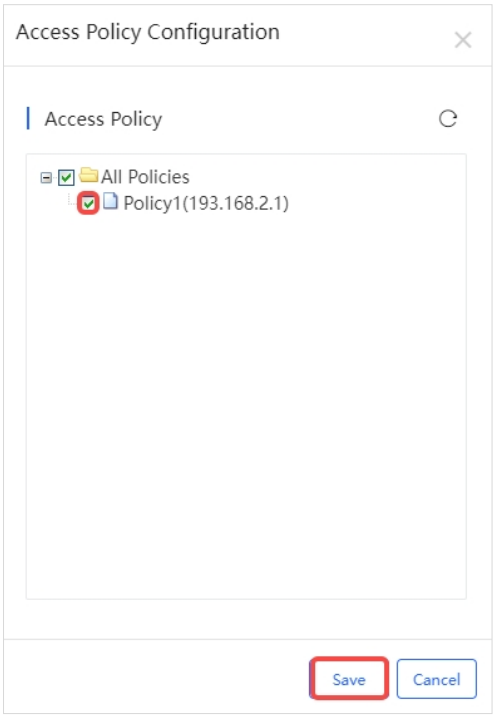
9.3.4 Configuring Access Policies for Subaccounts

Follow the steps below to create an access policy for an existing sub-account:

1 Click the icon in the **Action** column of an existing subaccount.



2 Select the access policy to be applied and click **Save** to complete the operation.



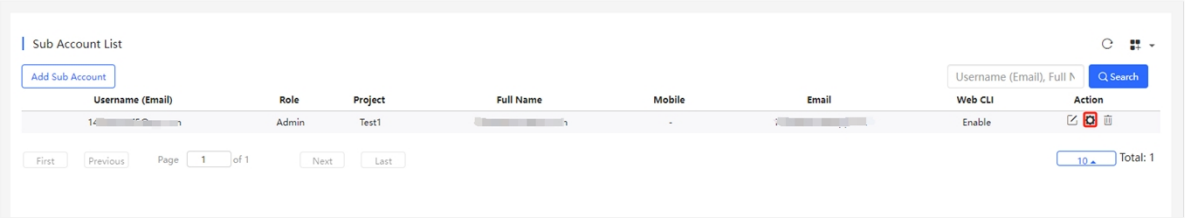
Note

If there is no access policy, refer to 9.4.1 Creating an Access Policy to create an access policy first, and then apply it to the subaccount.

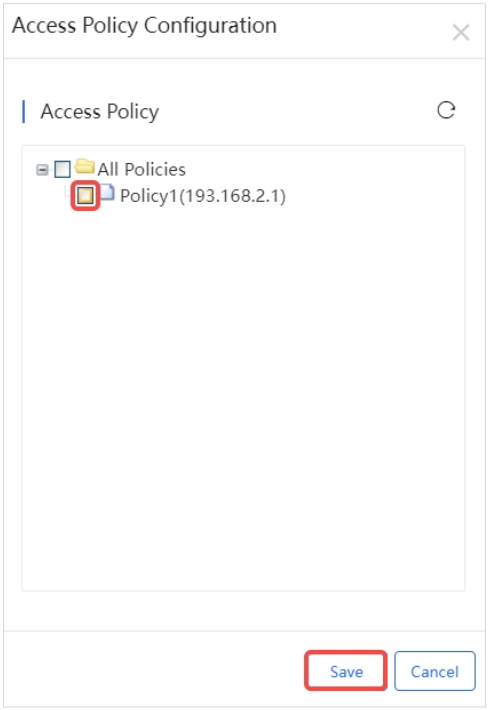
9.3.5 Canceling the Access Policy Applied to the Sub-account

Follow the steps below to cancel the access policy applied to a sub-account.

1 Click the icon in the **Account** column of the sub-account.



2 Uncheck the access policy, and click **Save** to complete the operation.

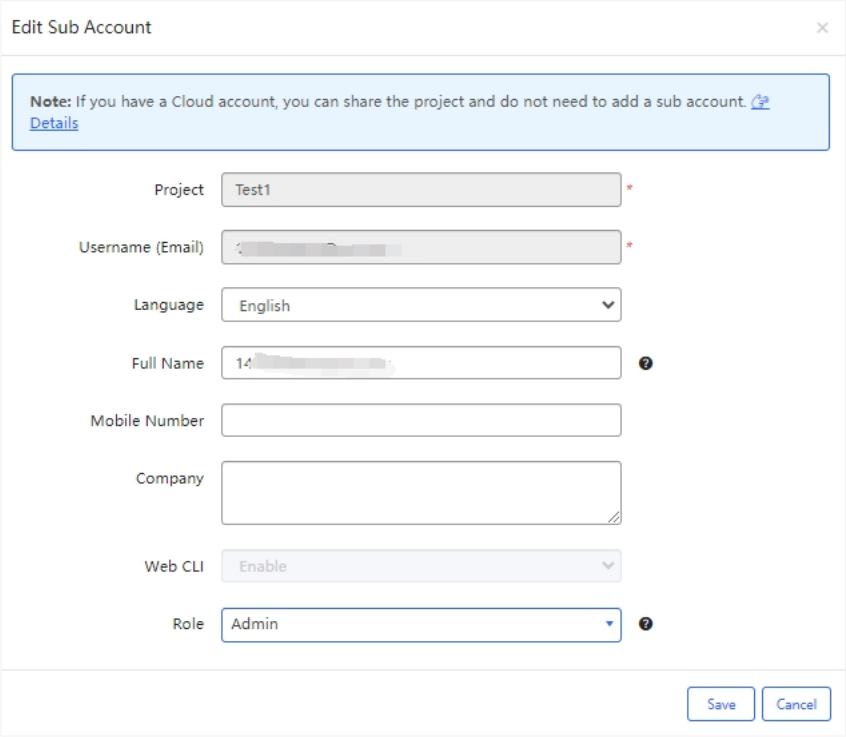


9.3.6 Editing Subaccount Information

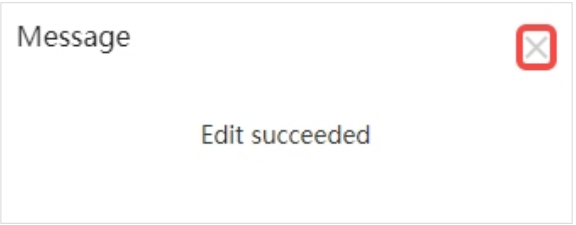
Follow the steps below to edit the information of an existing subaccount:

1 Click the in the **Action** column of the subaccount to be edited.

2 After modifying the sub-account information, click **Save**. The Email address and project cannot be changed.



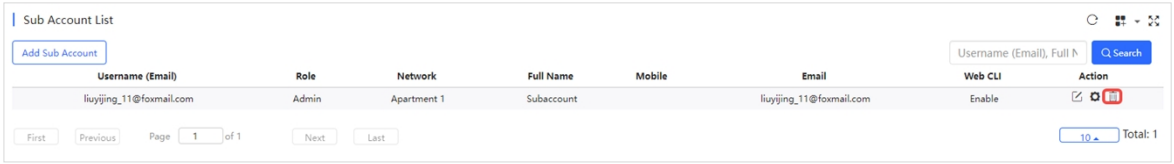
3 When the “Edit succeeded” prompt appears, click **X** to close the prompt box and complete the operation.



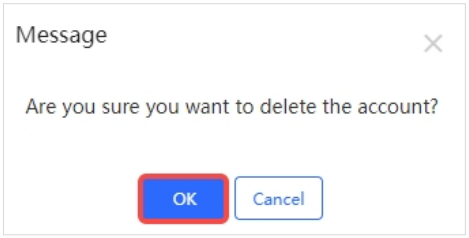
9.3.7 Deleting Subaccounts

Follow the steps below to delete the sub-account information:

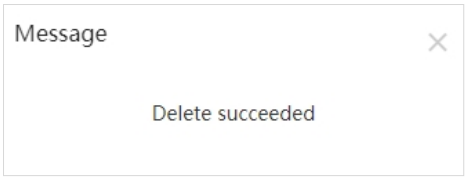
1 Click the in the **Action** column of the sub-account to be deleted.



2 When the operation prompt box appears, click **OK** to close the prompt box and complete the deletion.

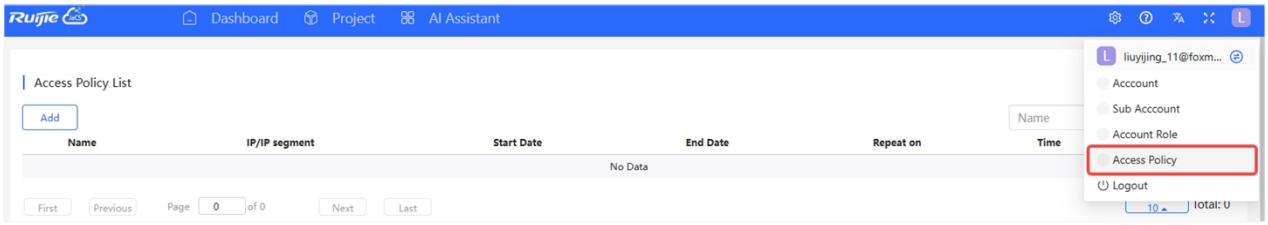


3 After the “Delete succeeded” prompt is displayed, click **X** to close the prompt box and complete the operation.



9.4 Access Policy Management

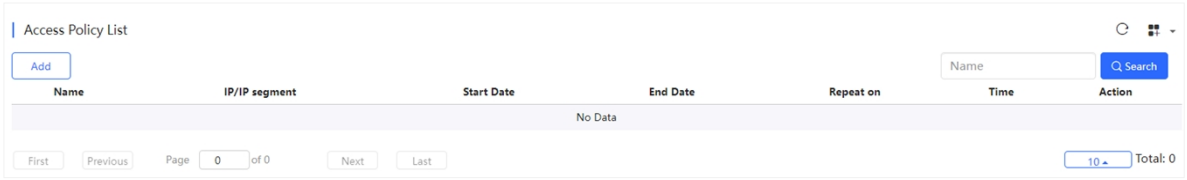
Click account icon and click **Access Policy** to go to the access policy management interface. Here, you can configure access policies for subaccounts. By default, the access policy list displays all configured policies under the tenant. Access policies can only be applied to subaccounts. Once an access policy is applied, only the IP addresses specified in the policy are permitted to log in to the subaccount.



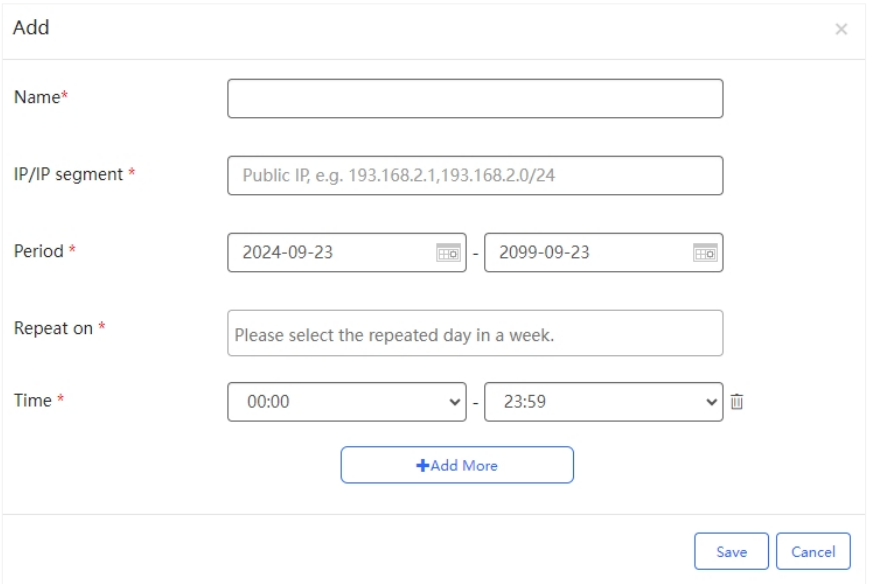
9.4.1 Creating Access Policies

To create an access policy:

1 Click **Add** to go to the access policy management interface.



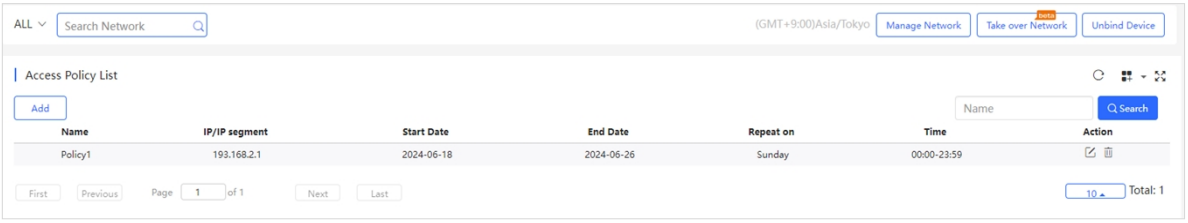
2 Fill in the information and click **Save**.



Items	Description
Name	Required. Set the policy name. Length: 1-64 characters. Letters, numbers, and special symbols (-, _ , #, @) are supported.
IP/IP segment	Required. Set IP or IP network segment, such as “193.168.2.1, 193.168.2.0/24”.

Period	Required. Set the date range that allows the IP address to access.
Repeat on	Required. Set a repeat day each week. Options: ALL/Monday/Tuesday/Wednesday/Thursday/Friday
Time	Required. Set the time period that allows the IP address to access. To set multiple period, click **+Add More**.

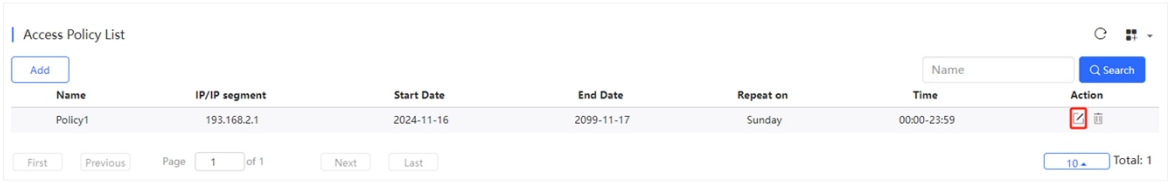
3 After the policy is added, it is displayed in the **Access Policy List**. Access policies can only be set for subaccounts.



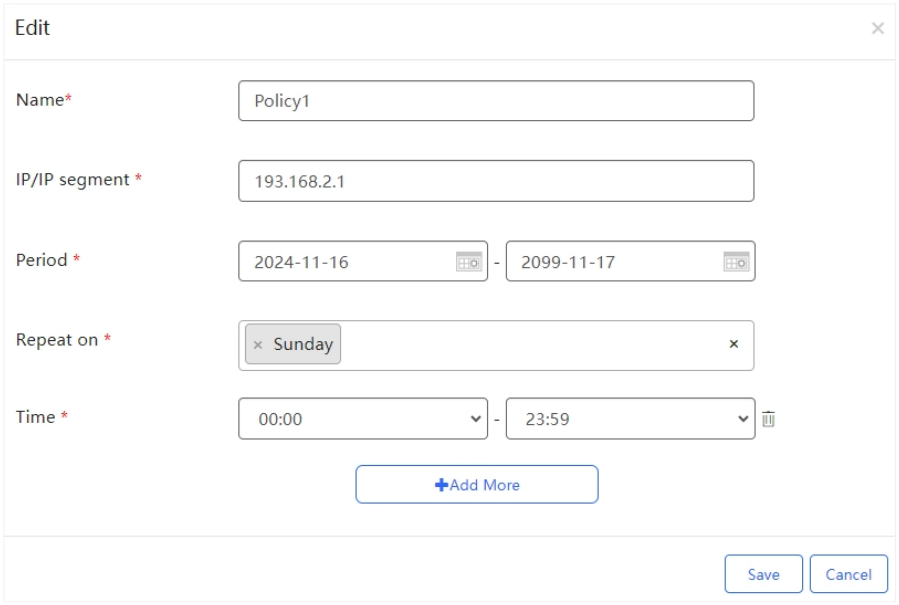
9.4.2 Editing Access Policies

Follow the steps below to edit an existing access policy:

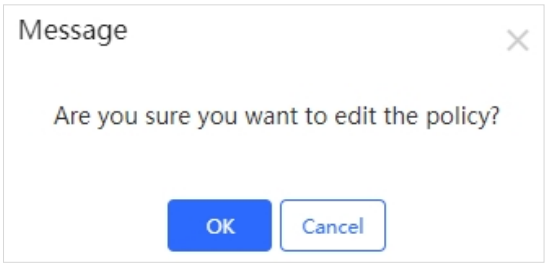
1 Click the icon in the **Action** column of the an access policy.



2 After modifying the access policy information as needed, click **Save**.



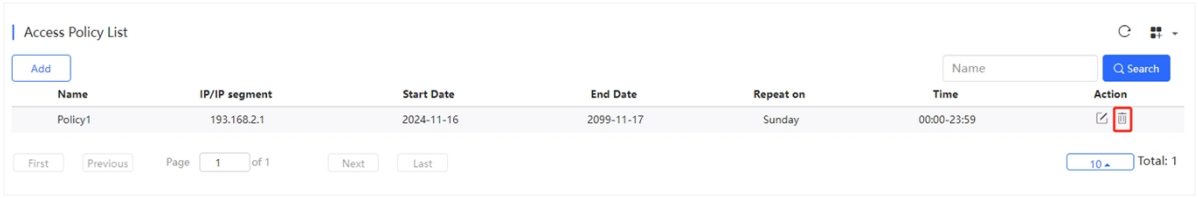
3 When the operation confirmation message appears, click **OK** to complete the operation.



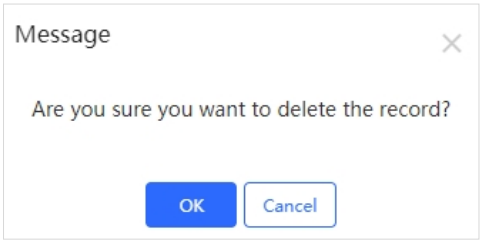
9.4.3 Deleting Access Policies

Follow the steps below to delete the corresponding access policy.

1 Click the icon in the **Action** column of the access policy to be deleted.



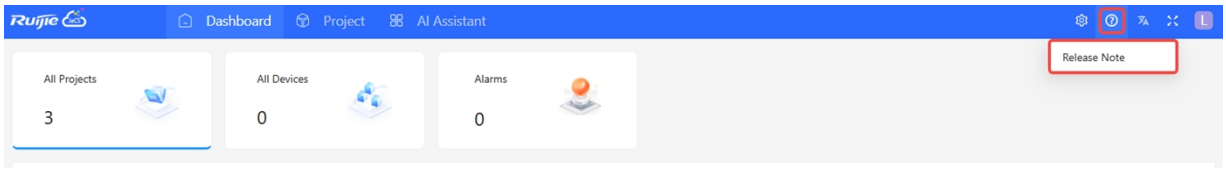
2 When the operation confirmation message appears, click **OK**.



10 Others

10.1 Online Documentation

You can click the icon to read the online documentation of Ruijie JaCS.



10.2 System Usage Restrictions

No.	Module	Description
1	Importing Devices in Batches	Up to 200 devices can be imported each time.
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	SSID	SSIDs can contain numbers, English letters, and “-“.
4	Custom excel template	For an custom Excel template, A to Z columns and 1 to 15 rows are supported to be used.
5	AP	Account-based policies may not be created for 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.
6	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.
7	00000JAPAN WiFi	In the apartment project, 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.
8	AP	In non-apartment project, except for AP180 series access points, please clear the configuration on access points before bringing 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.
9	AP	In non-apartment project, if the working mode (bridge mode or routing mode) of an AP180 access point is different from that on Cloud, the client may not be able to access the Internet.
10	Topology	1. Only devices connected to the downlink port of the switch can be detected. 2. Only RG-EG5210-JP, XS-1930J series switches, APs, RG-HS2310-16GH2GT1XS and RG-HA3515-DG can be displayed in the topology. 3. Only the devices in the same network and subnetwork can be displayed in the topology. 4. DHCP Diagnosis: only supports dynamic IP; the IP address of device can be recognized correctly only after four hours when its address pool range is changed. 5. When the downlink devices of RG-EG5210-JP are offline, they still can be displayed in the topology for 1 hour, but the traffic information of interfaces cannot be displayed. 6. Loop detection is not supported. 7. RG-HS2310-16GH2GT1XS and RG-HA3515-DG are displayed in the **Topology** page only when the root node is RG-HS2310-16GH2GT1XS or when the RG-HS2310-16GH2GT1XS is directly connected to RG-EG5210-JP.
11	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
12	Initial Configuration Template	Now, the template can be applied only to RG-AP180 series access points in project where the scenario is set to apartment.
13	CLI Command	Only for AP and CAP series products.
14	WPA3-SAE	Only for RG-MA2610 and RG-MA2810 access points in project where the scenario is set to hotel.
15	Device Details-Back Up	Only for the project where the scenario is set to apartment.
16	Project Group Level	Supports a 5-level grouping structure. The final level can only be a project, and no additional projects or groups can be created beneath it.
17	Upgrade Policy	1. Upgrade policies cannot be created in sub accounts and the project being shared. 2. Only for MA and AP180 series access points. 3. Only one upgrade policy can be configured for a device model.
18	Quick Deployment (Supported in the future)	1. This feature is applicable only to AP180 series access points. 2. Switches only can detect the APs that can access wide area networks.
19	RG-HS2310-16GH2GT1XS	Ruijie JaCS doesn’t support displaying the configurations of G.hn ports as well as delivering configurations to them.
20	Project	Up to 200 projects can be created each time when you use the batch template to create projects.