



Ruijie RG-WIS Cloud Management Network Solution

RG-WIS_5.23(b1)

User Manual

Copyright

Copyright © 2023 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademark  and  are owned by Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Ruijie Networks Website: <https://www.ruijienetworks.com/>
- Technical Support Website: <https://ruijienetworks.com/support>
- Case Portal: <https://caseportal.ruijienetworks.com>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Live Chat: <https://www.ruijienetworks.com/rita>

Conventions

1. Conversions

Convention	Description
Bold font	Commands, command options, and keywords are in bold font .
<i>Italic font</i>	Arguments for which you supply values are in <i>italic font</i> .
[]	Elements in square brackets are optional.
{ x y z }	Alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
&<1-n>	The argument before the sign (&) can be input for consecutive 1 - n times.
//	Double slashes at the beginning of a line of code indicate a comment line.

2. Signs

The signs used in this document are described as follows:

 **Warning**

An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage.

 **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.

 **Specification**

An alert that contains a description of product or version support.

3. Note

The manual offers configuration information (including model, port type and command line interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Contents

Preface	I
1 Product Overview	1
2 Logging In to WIS Cloud Network.....	2
2.1 Logging In to WIS Cloud Network	2
2.2 Visitor Login	4
2.3 Registering an Account.....	6
3 Project Management.....	8
3.1 Project List	8
3.2 Creating a Project	9
3.3 Transferring a Project	10
3.4 Project Management.....	10
3.4.1 Adding a Device	10
3.4.2 Setting as Default Project	11
3.4.3 Editing a Project.....	12
3.4.4 Deleting a Project.....	13
3.4.5 User Management	13
3.5 Opening a Project	14
4 Quick Start.....	15
4.1.1 Organizational Planning.....	15
4.1.2 Network Configuration	16
4.1.3 Device Access.....	18
5 Home	20
5.1 Traffic	20

5.2 Alarm.....	21
5.3 Online STA.....	21
5.4 Site.....	23
6 My Network	25
6.1 Site Overview.....	25
6.1.1 Site List	25
6.1.2 Site Overview Info.....	25
6.1.3 Switching a Site	26
6.1.4 Network Indicators	26
6.2 Network Configuration	30
6.2.1 Binding a Template	31
6.2.2 Personalized Configuration.....	31
6.3 Device Management.....	35
6.3.1 Device List.....	36
6.3.2 Adding a Device	37
6.3.3 Importing Devices	38
6.3.4 Deleting a Device.....	43
6.3.5 Device Details	43
6.3.6 Unbinding a Device.....	48
6.3.7 Delivering the Configuration	49
6.3.8 Upgrading Devices.....	51
6.3.9 Moving a Device	52
6.3.10 Restarting a Device.....	53
6.3.11 Backing Up the Configuration	54

6.3.12 Command Debugging.....	55
6.3.13 Restoring the Configuration from Backups.....	56
6.3.14 Accessing eWeb	57
6.3.15 Accessing Telnet	59
6.4 Network Topology	61
6.4.1 Device Query	61
6.4.2 Topology View	62
6.4.3 Device List.....	64
6.4.4 Device Details	65
6.5 Network Optimization.....	77
6.5.1 WLAN Optimization.....	77
6.5.2 Roaming Optimization.....	84
6.6 STA Insight	86
6.6.1 STA Monitoring.....	86
6.6.2 STA Experience.....	87
6.7 Access Security	90
6.7.1 Authentication Configuration.....	90
6.7.2 Authentication Logs.....	124
6.7.3 Blacklist/Whitelist	125
6.8 Alarm Management	130
6.8.1 Active Alarm	130
6.8.2 Alarm Setup.....	134
6.8.3 History Alarm.....	136
6.9 Report	138

7 Management and Maintenance	139
7.1 Organizational Planning.....	139
7.1.1 Adding a Site	139
7.1.2 Editing a Site	140
7.1.3 Deleting a Site.....	141
7.2 Configuration Management	141
7.2.1 Configuration Template	141
7.2.2 Configuration Task	154
7.2.3 Configuration Backup.....	159
7.3 Tunnel Management	161
7.4 STA Management	163
7.4.1 OS	163
7.4.2 STA Type	165
8 Intelligent Analysis.....	167
8.1 Area.....	167
8.2 Monitoring	167
8.2.1 Overview	167
8.2.2 Experience	175
8.2.3 Clients	185
8.2.4 Devices	189
8.2.5 Environment.....	193
8.3 Optimization	196
8.3.1 One Key Diagnosis	196
8.3.2 One-Click Network Optimization.....	198

8.3.3 Access Optimization.....	203
8.3.4 Config Planning.....	205
8.4 Big Data	205
8.4.1 Regional Analysis.....	205
8.4.2 Scheduled Change	206
8.4.3 Client Capacity	207
8.4.4 Manufacturer Analysis.....	207
8.4.5 Baseline	208
8.5 Panel	208
9 System Management	211
9.1 User Management	211
9.2 Role Management.....	212
10 Appendix.....	215
10.1 Configuring a Facebook App	215
10.1.1 Registering as a Facebook Developer	215
10.1.2 Applying for a Facebook Login App	218
10.1.3 Applying for an Instagram App.....	224
10.1.4 Releasing an App.....	231

1 Product Overview

RG-WIS cloud management network ("WIS Cloud Network" for short) provides full-lifecycle intelligent network management services covering network procurement, planning, deployment, acceptance, and O&M. It integrates the big data, cloud computing, and AI technologies to improve the efficiency in network construction and O&M management for enterprises and partners. WIS Cloud Network provides rich northbound interfaces regardless of whether it is deployed in public cloud, private cloud, or hybrid cloud mode. It helps customers better operate networks and facilitates digital transformation of enterprises.

The digital transformation of enterprises is accompanied by various network use changes such as service cloudification, use of wireless STAs, and diversified access modes. The network O&M architecture is also required to meet the needs of elastic expansion. Traditional network management is confronted with difficulties in access, analysis, and expansion. For example, a network management system (NMS) reads data through the Simple Network Management Protocol (SNMP), but it cannot access devices that span a wide area network (WAN). When traditional relational databases are used to store data, data cannot be stored or analyzed if the volume of collected data is ultralarge. In addition, for large parks and multi-branch chain enterprises, the access of over ten thousand devices to the network is beyond the management capacity of the traditional NMS.

Cloud management network is a new network form that integrates IT cloud with the communication technology (CT) network. It migrates the management, control, and O&M functions in the traditional network architecture to the cloud, and provides the functions as services for many different enterprises. The local network infrastructure of enterprises provides only data forwarding capability. WIS Cloud Network uses the cloud native, big data, AI, and other cutting-edge technologies to build a highly reliable, scalable, and intelligent analysis platform architecture. It can meet requirements for the access of mass devices as well as the storage and real-time analysis of big data, and supports intelligent applications such as prediction, optimization, and diagnosis.

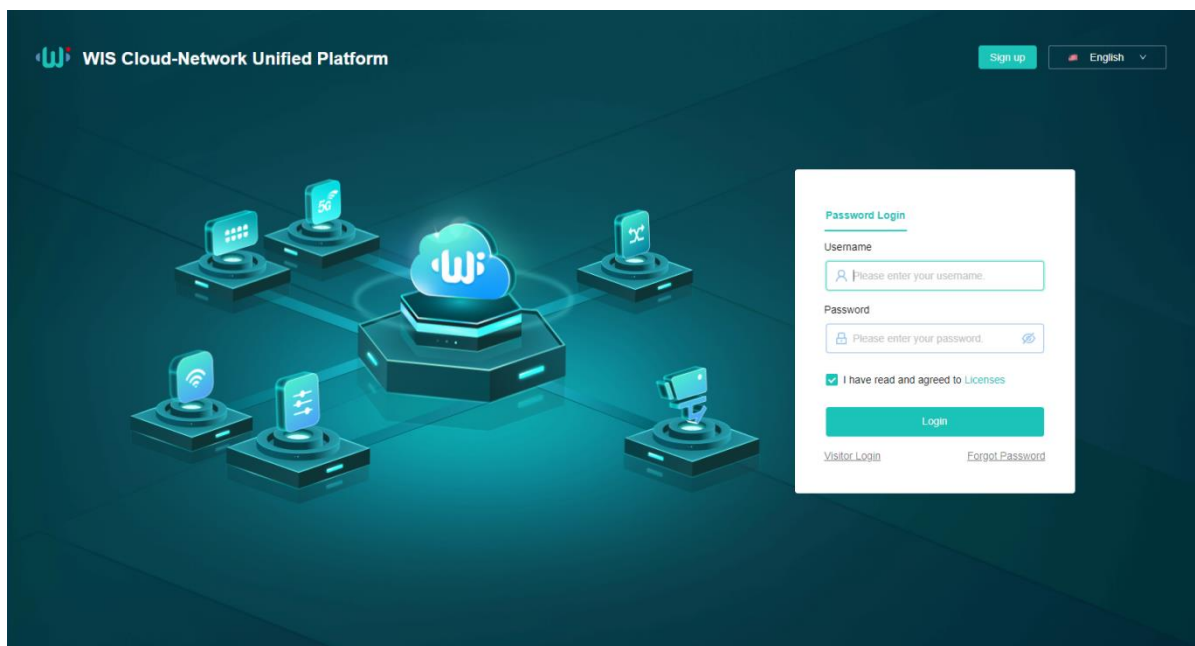
2 Logging In to WIS Cloud Network

2.1 Logging In to WIS Cloud Network

On Google Chrome, visit the address of WIS Cloud Network: <https://wiscloud.ruijienetworks.com>. Enter the correct username and password and click **Login** to log in to WIS Cloud Network.

If you have no account, register one before login. For the account registration process, see [Registering an Account](#).

Figure 2-1 Logging In to WIS Cloud Network



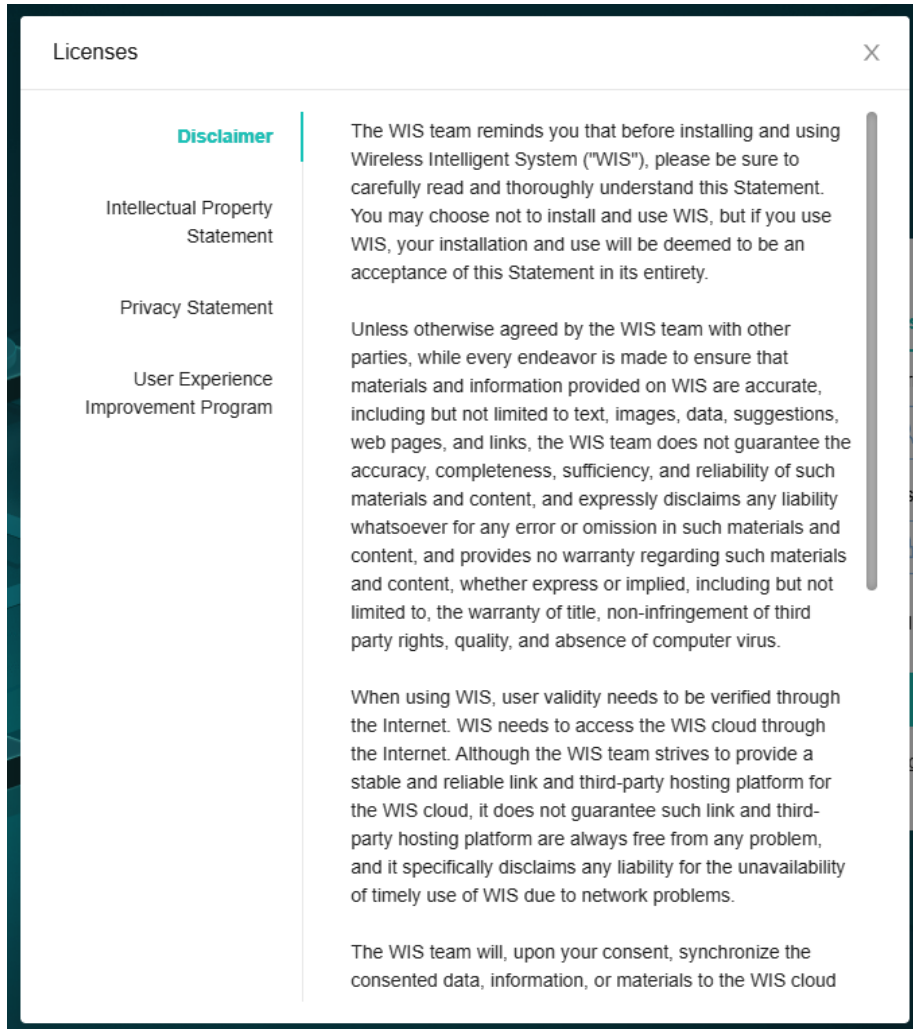
You are required to read and agree to **Licenses** before login. Click **Licenses** to learn about detailed content in **Disclaimer**, **Intellectual Property Statement**, **Privacy Statement**, and **User Experience Improvement Program**. Please read through the content before using WIS Cloud Network formally. If you agree to clauses in **Licenses**, select **I have read and agreed to Licenses**, and enter the correct username and password to log in to WIS Cloud Network.

Figure 2-2 Selecting and Viewing Licenses

The screenshot displays a login interface with the following elements:

- Section Header:** "Password Login" in teal text, underlined.
- Username Field:** A text input box with a person icon and the placeholder text "Please enter your username."
- Password Field:** A text input box with a lock icon, the placeholder text "Please enter your password.", and an eye icon for toggling visibility.
- License Agreement:** A checked checkbox followed by the text "I have read and agreed to Licenses".
- Login Button:** A teal button with the text "Login".
- Links:** Two underlined links at the bottom: "Visitor Login" and "Forgot Password".

Figure 2-3 Details in Licenses



2.2 Visitor Login

WIS Cloud Network allows you to log in as a visitor to view demo projects.

Figure 2-4 Visitor Login

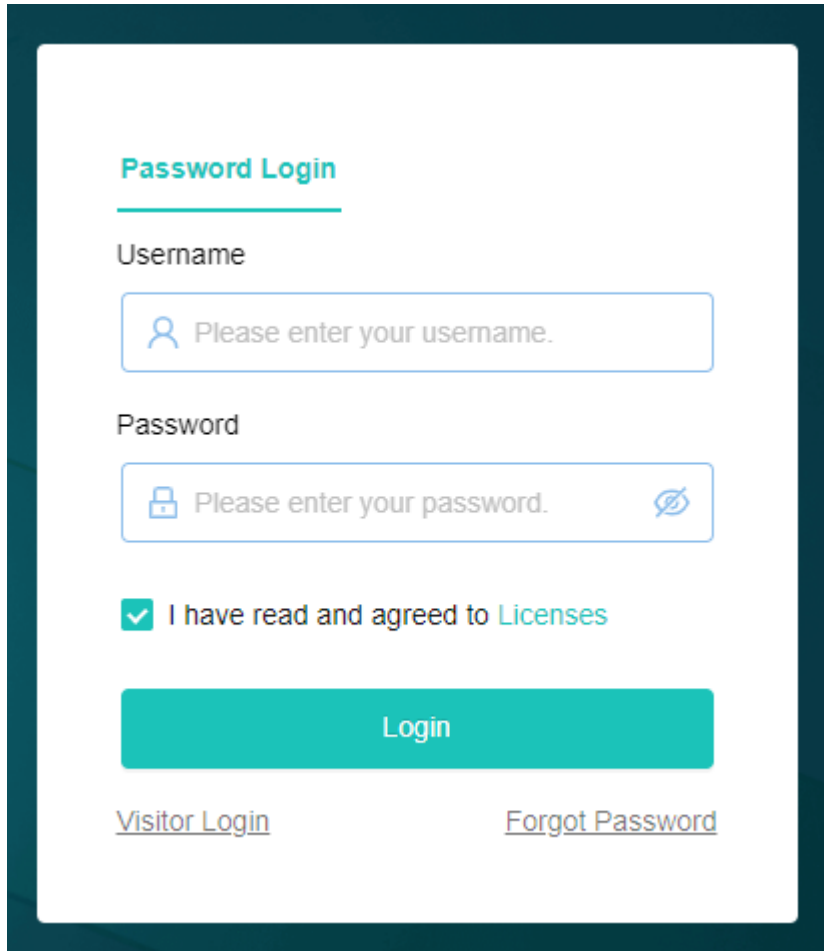
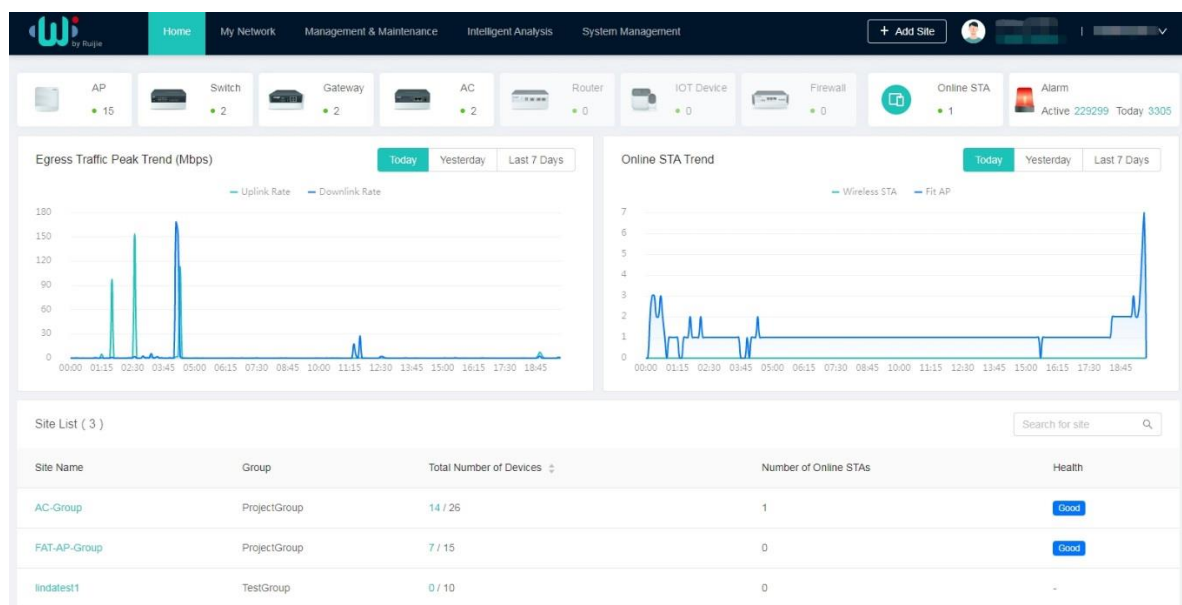


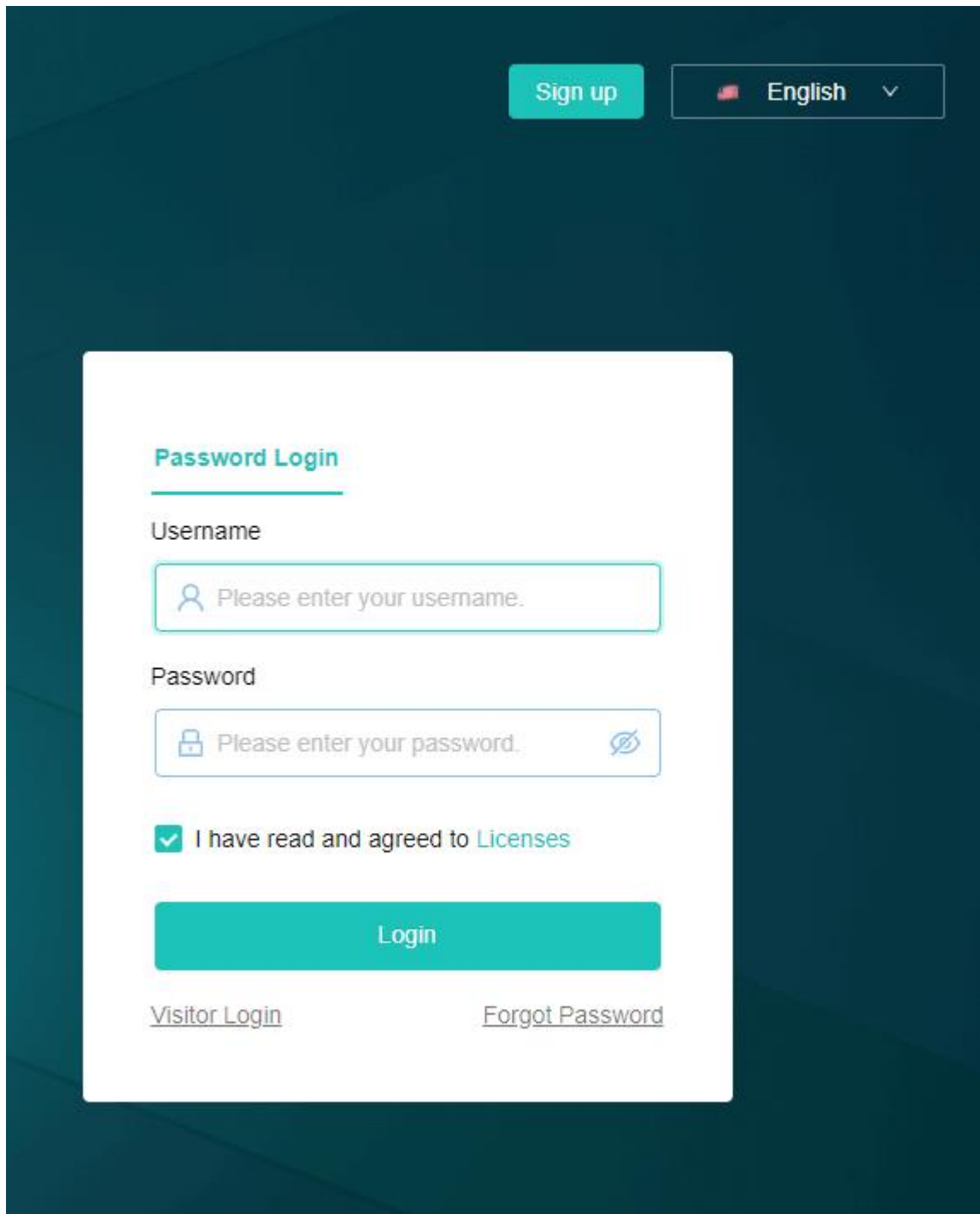
Figure 2-5 Demo Projects



2.3 Registering an Account

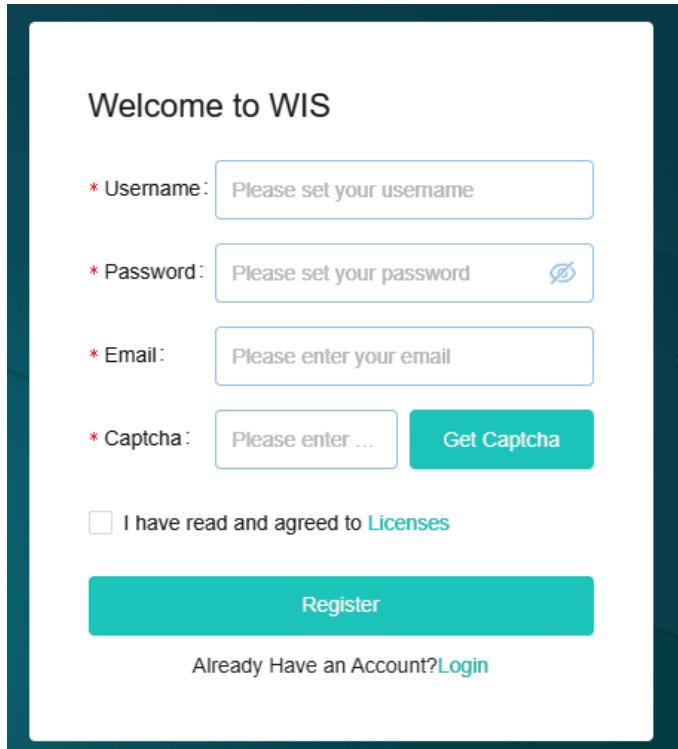
If you are using WIS Cloud Network for the first time, you'll need to register an account first. Visit <https://wiscloud.ruijienetworks.com> on Google Chrome. Click **Sign up** in the upper right corner of the page to redirect to the account registration page.

Figure 2-6 Account Registration Entry



On the registration page, enter your username, password, email address, and captcha, select **I have read and agreed to Licenses**, and click **Register**. After successful registration, WIS Cloud Network automatically redirects to the login page. Enter the registered username and password to log in to WIS Cloud Network.

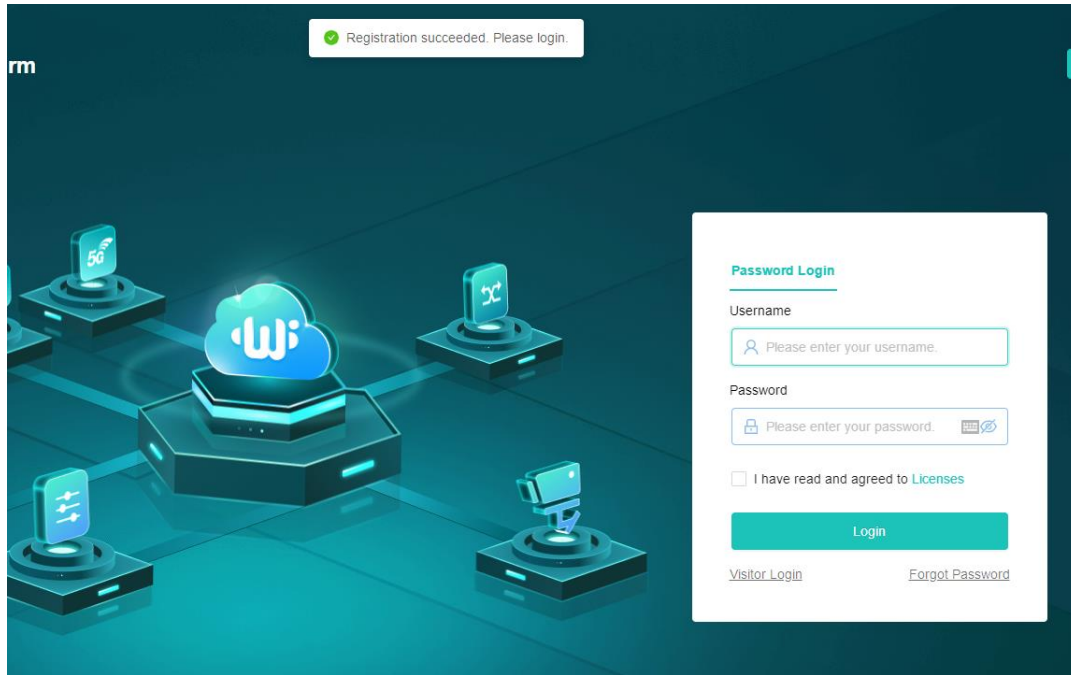
Figure 2-7 Registering an Account



The screenshot displays a registration form titled "Welcome to WIS". It includes the following elements:

- Username:** A text input field with the placeholder "Please set your username".
- Password:** A text input field with the placeholder "Please set your password" and a toggle icon for password visibility.
- Email:** A text input field with the placeholder "Please enter your email".
- Captcha:** A text input field with the placeholder "Please enter ..." and a teal "Get Captcha" button.
- Agreement:** A checkbox followed by the text "I have read and agreed to [Licenses](#)".
- Register Button:** A large teal button labeled "Register".
- Login Link:** The text "Already Have an Account? [Login](#)".

Figure 2-8 Registration Succeeded



3 Project Management

Service providers bear responsibilities for maintaining and constructing customers' networks. For service providers, each customer is a separate tenant, or project.

3.1 Project List

When you log in to WIS Cloud Network for the first time, the **Project Management** page is displayed by default, on which you can view the project list.

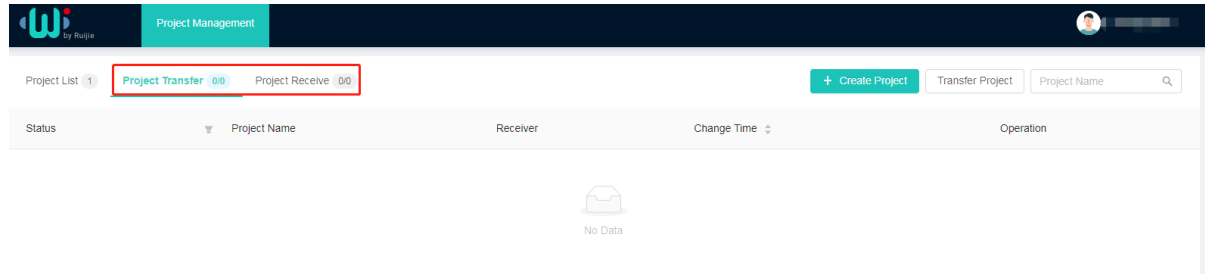
Figure 3-1 Tenant List

Project Name	Management Type	Industry	Creator	Site Quantity	Online Devices/Total Devices	Creation Time	Operation
[Redacted]	[Redacted]	General Education	[Redacted]	3	21/51	2022-07-21 10:40:12	Add Device ...

The project list displays the project name, management type, industry, creator, site quantity, number of online devices/total devices, and creation time. You can search for a specified project by project name.

You can click the **Project Transfer** or **Project Receive** tab to view applications for project transfer to other managers or applications for project transfer from other managers.

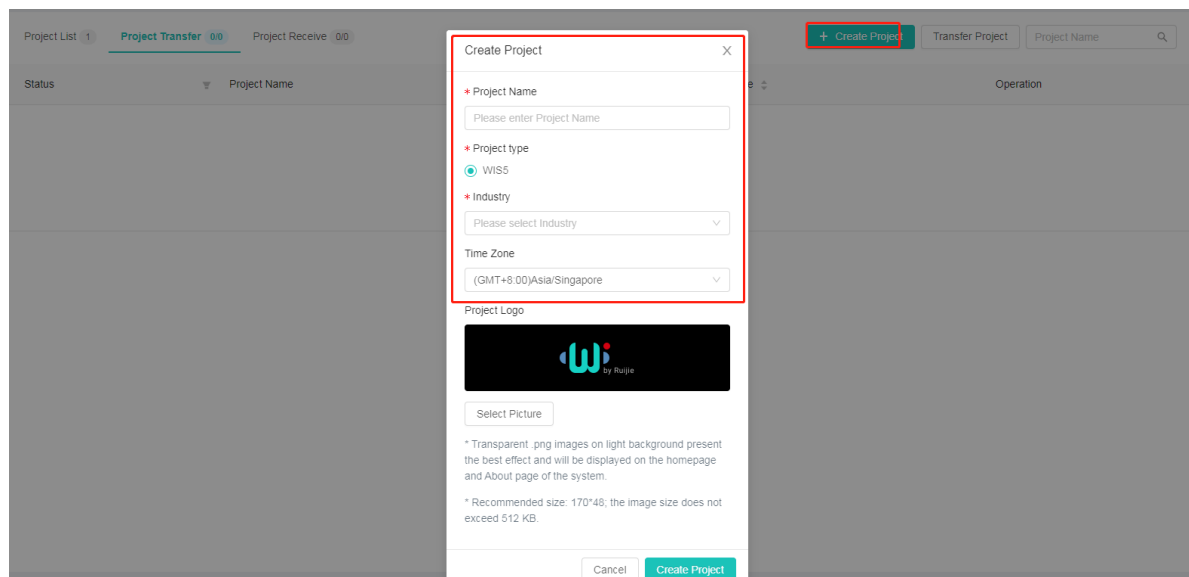
Figure 3-2 Project Transfer and Project Receive



3.2 Creating a Project

Click **Create Project** and add information about a new project.

Figure 3-3 Creating a Project



Enter the following information when creating a project:

- **Project Name:** (Required) It identifies a tenant. It is a string of up to 50 characters containing only letters, digits, underscores (_), hyphens (-), @, and &.
- **Industry:** (Required) Select the proper industry scenario type from the drop-down list.
- **Project Logo:** (Optional) You can set a personalized logo for a tenant.

3.3 Transferring a Project

Click **Transfer Project**. Enter the account of a user who receives a project and the name of the project to be transferred, and click **Continue Transfer**.

Figure 3-4 Transferring a Project

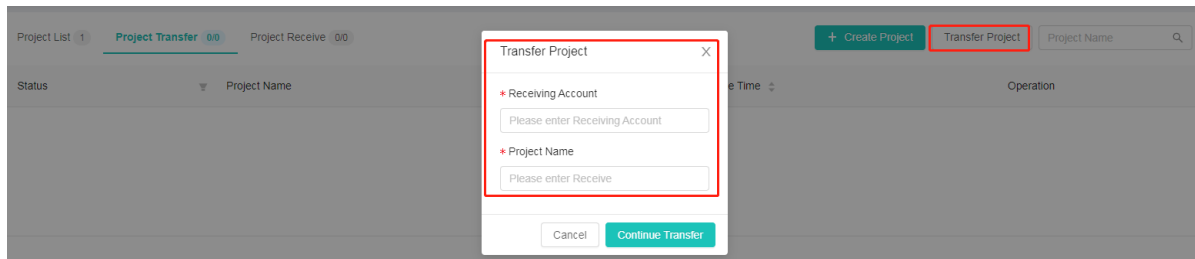
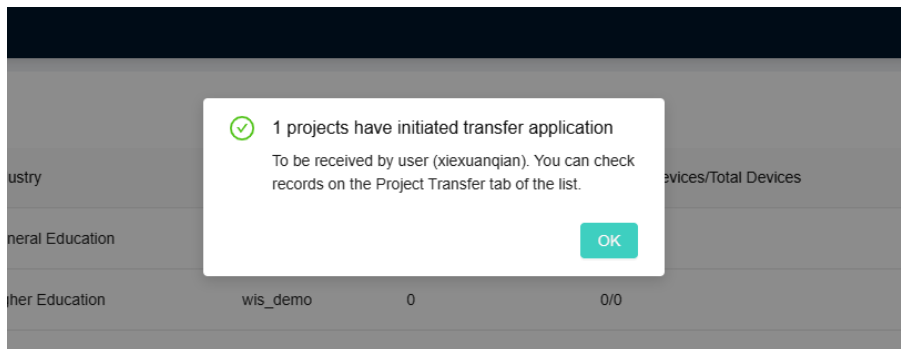


Figure 3-5 Successful Initiation of a Transfer Application



3.4 Project Management

3.4.1 Adding a Device

Click **Add Device** in the **Operation** column for a project. The **Device Management** page of the project is displayed, on which you can add devices to the project. For details about how to add a device, see "Adding a Device" in "My Network" > "Device Management."

Figure 3-6 Adding a Device

Creator	Site Quantity	Online Devices/Total Devices	Creation Time	Operation
[Redacted]	3	21/51	2022-07-21 10:40:12	Add Device ...

1-1 of 1 items < 1 > 10 / page

3.4.2 Setting as Default Project

After a project is created, if you want WIS Cloud Network to automatically open the project each time you log in to WIS Cloud Network, you can set the project as the default project. Click ... in the **Operation** column for a project and select **Set as Default Project** to set the project as the default project.

Figure 3-7 Setting as Default Project

Project Name	Creation Time	Operation
[Redacted]	2022-09-24 18:13:31	Add Device ...
[Redacted]	2022-09-21 22:38:...	[Redacted]
[Redacted]	2022-09-20 18:13:...	☆ Set as Default Project
[Redacted]	2022-09-20 09:49:30	Add Device ...

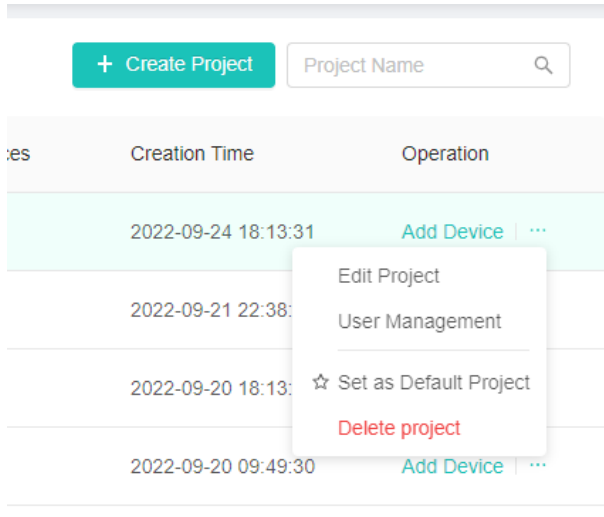
⚠ Caution

- After a project is set as the default project, the tenant project is automatically opened each time you log in to WIS Cloud Network.
- Only one project can be set as the default project at a time.
- If the default project already exists and you set another project as the default project, the default project configuration of the original default project will be automatically canceled.

3.4.3 Editing a Project

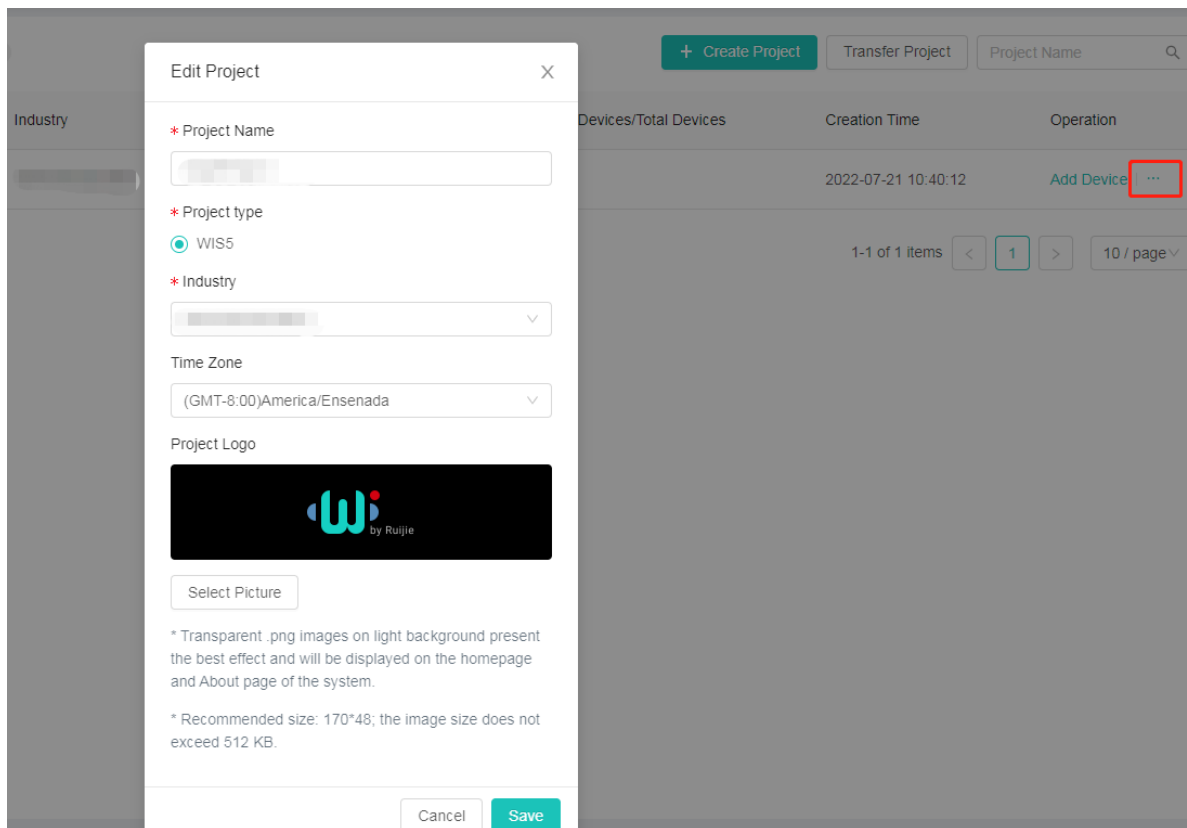
Click ... in the **Operation** column for a project and select **Edit Project** to edit the project information.

Figure 3-8 Entry for Editing a Project



The requirements for parameters for editing a project are the same as those for parameters for creating a project. After editing, click **Save**.

Figure 3-9 Editing a Project



3.4.4 Deleting a Project

Click ... in the **Operation** column for a project and select **Delete project** to delete the project. When a project is of the invited management type, the project cannot be deleted directly. If the project is no longer managed, you can click **Exit Project**.

Figure 3-10 Entry for Deleting a Project

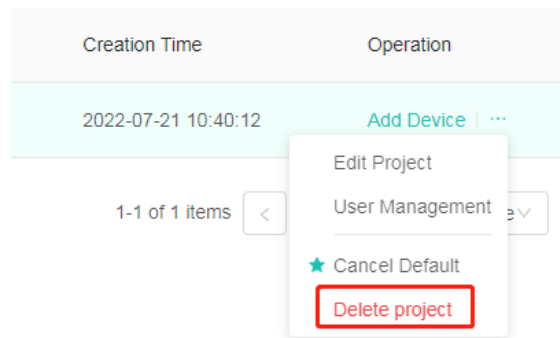


Figure 3-11 Deleting a Project

Are you sure you want to delete the project?

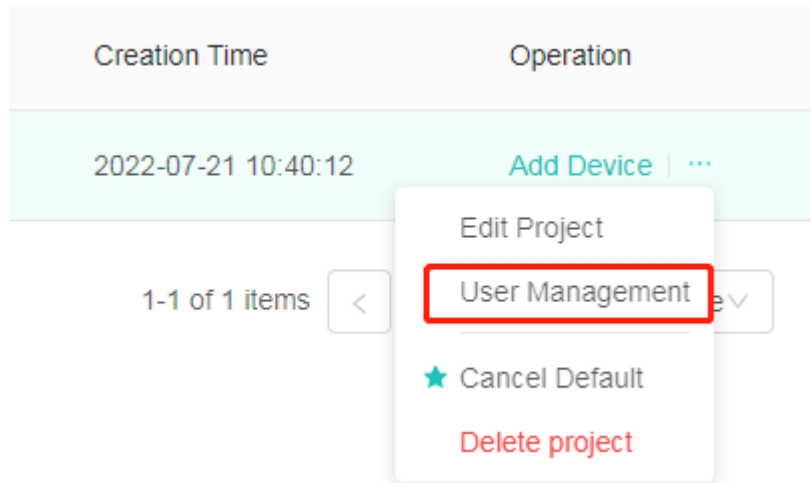
Cancel

OK

3.4.5 User Management

Click ... in the **Operation** column for a project and select **User Management** to manage members of the project. For details about the member management function, see the description in "System Management" > "User Management."

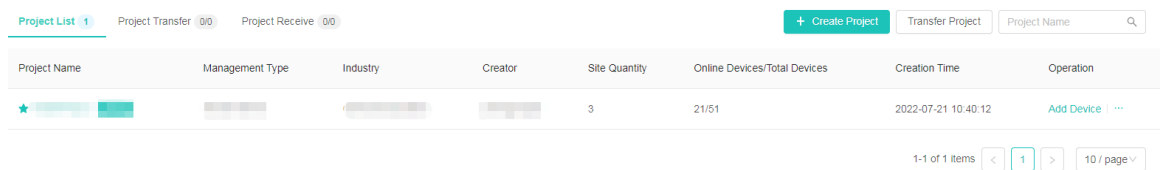
Figure 3-12 User Management



3.5 Opening a Project

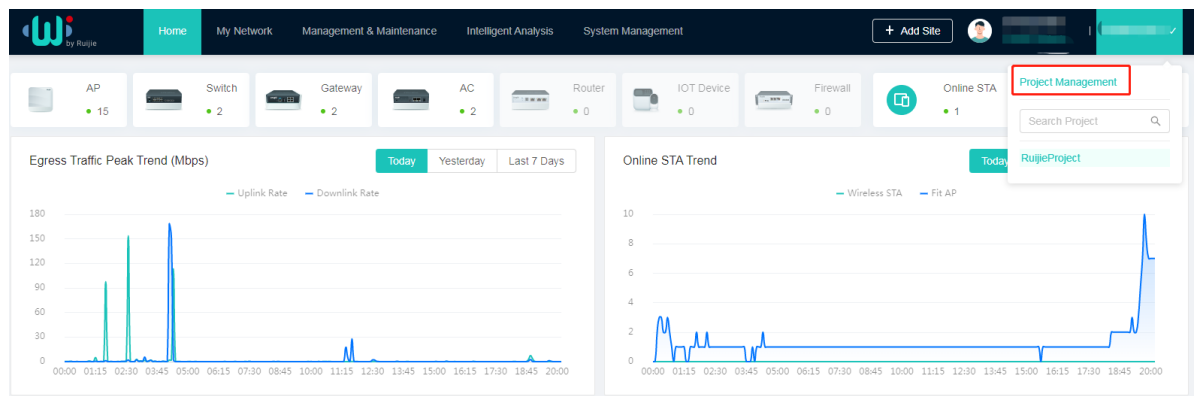
On the **Project List** tab page, click a project name to open the project.

Figure 3-13 Opening a Project



If you have opened a project, you can click the project name in the upper right corner and select **Project Management** to return to the **Project Management** page.

Figure 3-14 Returning to the Project Management Page



4 Quick Start

4.1.1 Organizational Planning

WIS Cloud Network supports branch-based network management. Therefore, make organizational planning before connecting the devices to WIS Cloud Network.

Choose **Management & Maintenance > Organizational Planning** to go to the **Organizational Planning** page. Add branches and sites to the organizational tree. Branches can be added at multiple levels. A site is the smallest unit of network management. One or more sites can be added under each branch. You can click **Batch Import** to bulk add sites.

Note

For details about operations in organizational planning, see the description in "Management & Maintenance" > "Organization Planning."

Figure 4-1 Adding a Branch

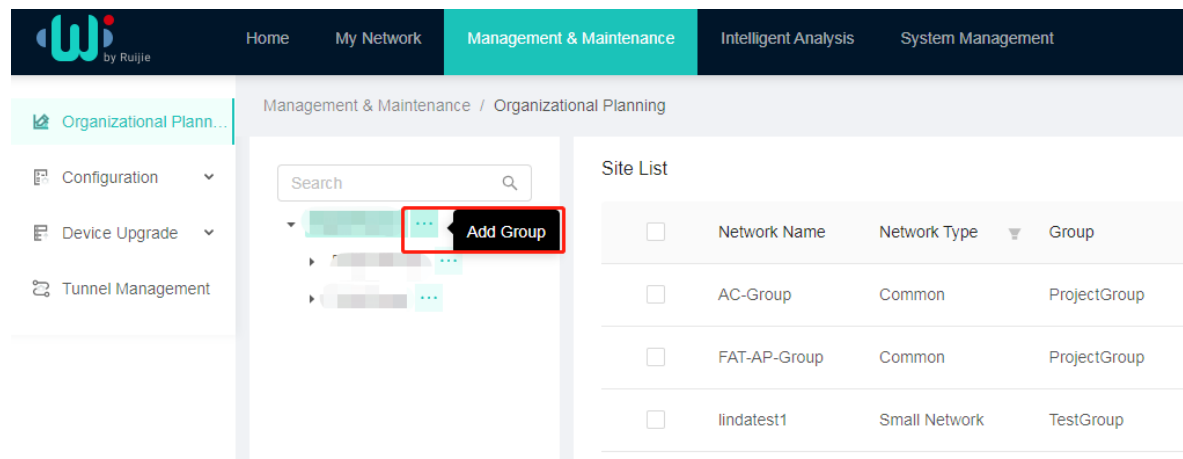
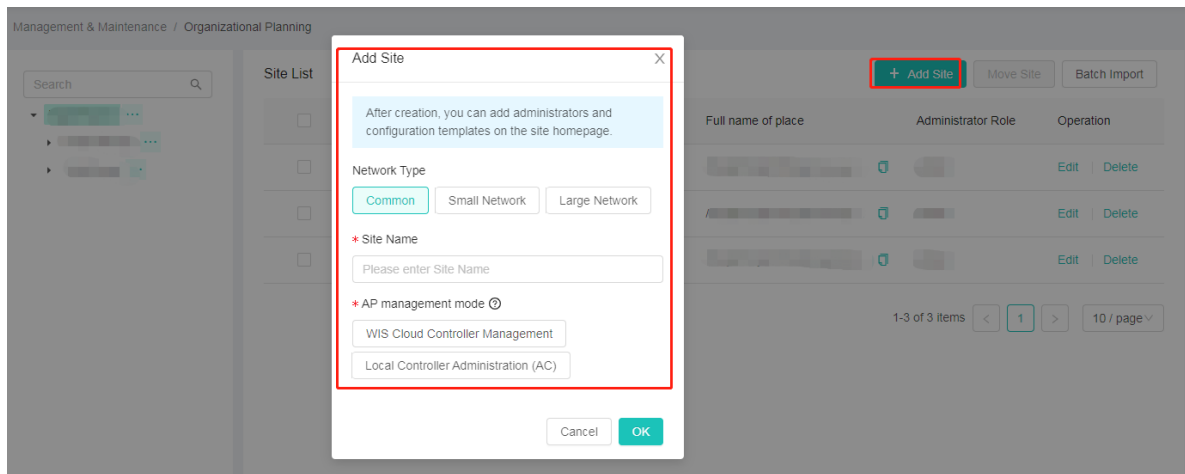


Figure 4-2 Adding a Site



4.1.2 Network Configuration

WIS Cloud Network automatically delivers configurations to new online devices. The administrator can create a configuration template and bind the template to a specific branch or site. After the configuration template is bound, all new online devices in the branch or site will automatically obtain the configuration of the configuration template.

Choose **Management & Maintenance > Configuration > Template** to add configurations. A template can be configured in WLAN SSID configuration mode and CLI command set configuration mode. The WLAN SSID configuration mode is used to configure WLANs such as SSIDs of cloud APs and the configuration does not take effect on devices other than cloud APs. CLI command sets apply to all devices regardless of the device type.

Note

For details about network configuration, see the description in "Management & Maintenance" > "Configuration."

Figure 4-3 Adding an SSID

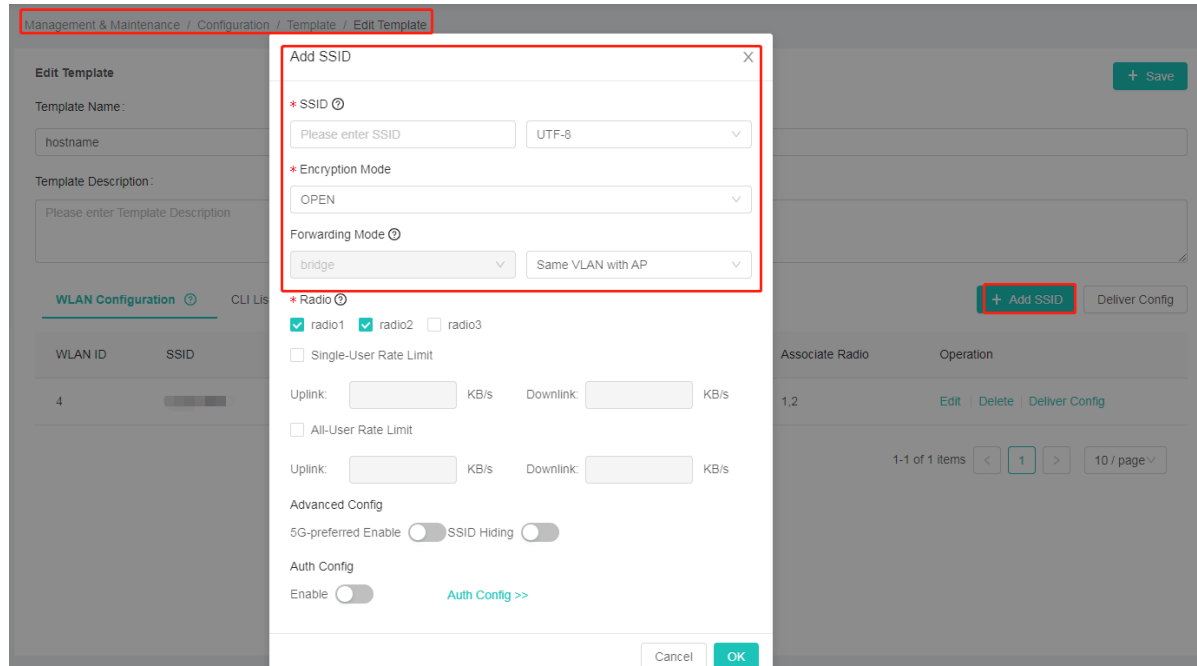
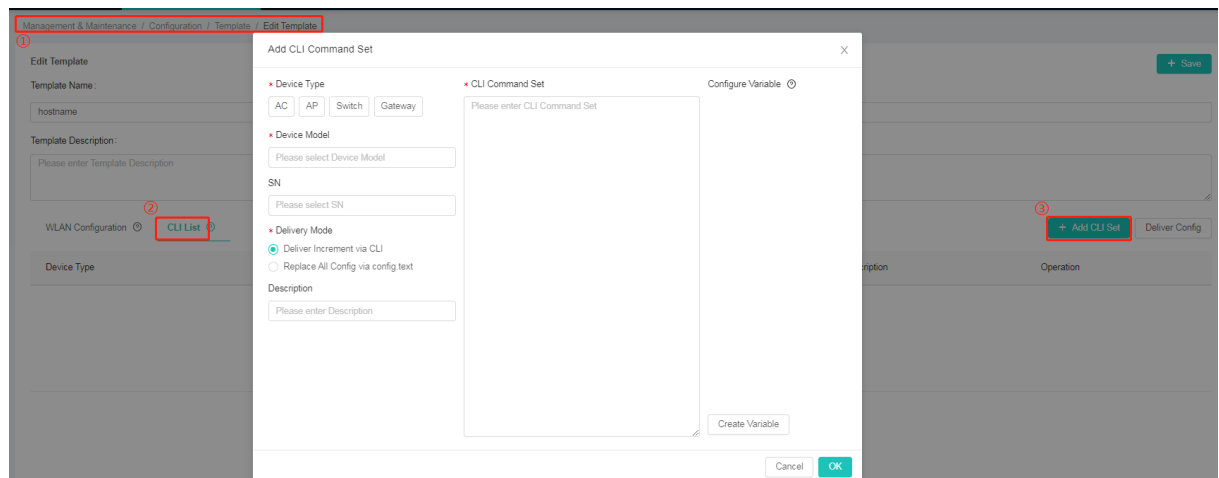


Figure 4-4 Adding a CLI Command Set



CLI command sets can be delivered in two modes: incremental CLI delivery and full replacement. APs do not support the full replacement mode.

- Incremental delivery: A device incrementally executes a user-defined CLI command set based on the current configuration. This mode applies to incremental configuration scenarios.
- Full replacement: The **config.text** configuration file of a device is directly replaced. After replacement, the device automatically restarts for the configuration to take effect. This mode is suitable for the full replacement of the system configuration or for scenarios, in which incremental configuration cannot meet requirements, for example, incremental configuration may cause network path changes (resulting in device disconnection),

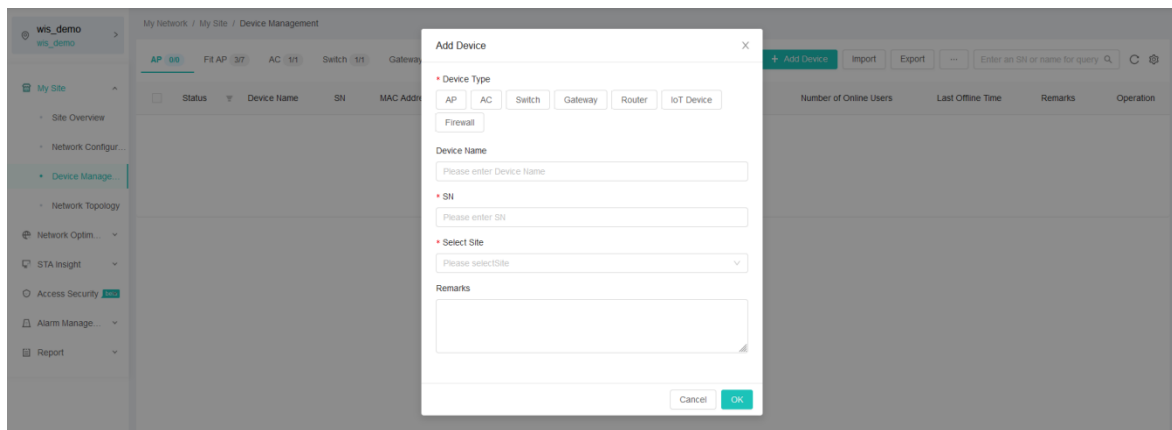
and configuration involves multiple interactions and command transformation (resulting in interaction and command identification timeout).

4.1.3 Device Access

1. Adding a Device

Choose **My Network > My Site > Device Management** to go to the **Device Management** page. Click **Add Device**. Select the device type and enter the device name, or enter a device SN to add a device.

Figure 4-5 Adding a Device



A device SN can be obtained in two ways:

- **Command query:** Run the **show version** command on a device to display the device SN.

The following uses an AC as an example. G1L60EW000233 is the SN of the AC.

```
Ruijie#show version
System description : Ruijie Gigabit Wireless Switch(WS6008) By Ruijie
Networks.
System start time : 2020-06-07 11:52:26
System uptime : 0:01:38:50
System hardware version : 1.00
System software version : AC_RGOS 11.9(5)B1T2
System patch number : NA
System serial number : G1L60EW000233
System boot version : 1.2.12
Module information:
Slot 0 : WS6008
Hardware version : 1.00
Boot version : 1.2.12
Software version : AC_RGOS 11.9(5)B1T2
Serial number : G1L60EW000233
```

- **Label query:** Check the label on the back of a product to obtain the device SN.

2. Configuring Device Access Addresses

The device access addresses can be configured in two ways:

- Manual configuration

Run the following commands on the device to be connected to configure the CPE WAN Management Protocol (CWMP) and domain name system (DNS) (the actual DNS address shall prevail).

```
Hostname#config
Hostname(config)#ip name-server 8.8.8.8
Hostname(config)#cwmp
Hostname(config-cwmp)#acs url http://wiscloud.ruijienetworks.com/acs
Hostname(config-cwmp)#cpe inform interval 60
Hostname(config-cwmp)#end
Hostname#write
```

- Use DHCP Option 43 to distribute CWMP interconnection addresses (for devices obtaining addresses via DHCP).

Run the following commands on the DHCP server (the actual addresses shall prevail).

```
Hostname#config
Hostname(config)#ip dhcp pool pool_Gi0/0
Hostname(dhcp-config)#option 43 ascii http://wiscloud.ruijienetworks.com/acs
Hostname(dhcp-config)#lease 0 8 0
Hostname(dhcp-config)#network 192.168.1.0 255.255.255.0
Hostname(dhcp-config)#dns-server 8.8.8.8
Hostname(dhcp-config)#default-router 192.168.1.1
Hostname(dhcp-config)#end
Hostname#write
```

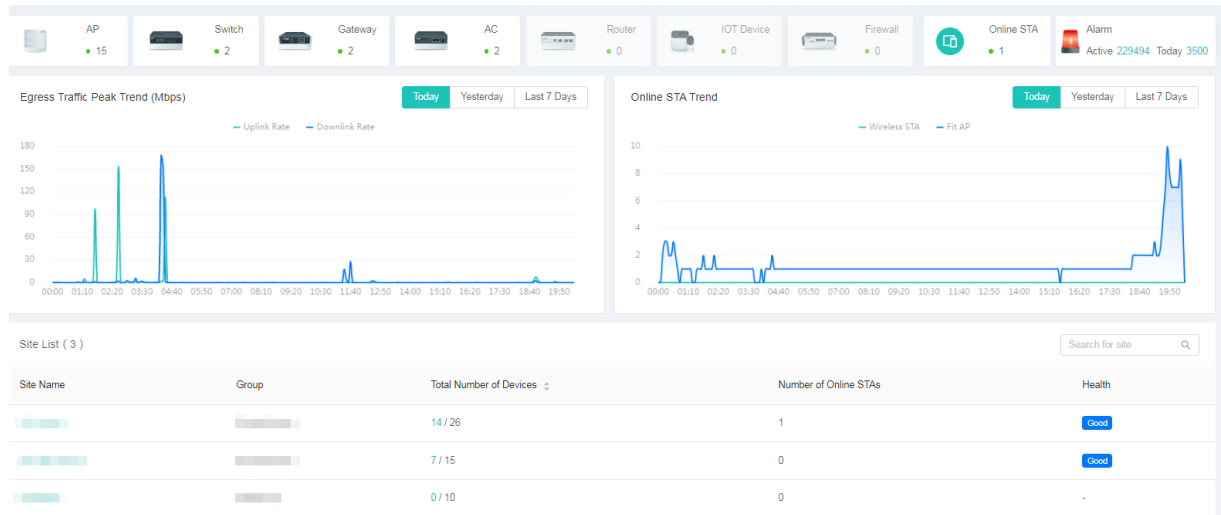
3. Device Go-Online

If a device can connect to WIS Cloud Network properly, you can view the device status on the **Device Management** page of WIS Cloud Network 3–6 minutes after you complete the configuration above.

5 Home

As shown in [Figure 5-1](#), the home page displays basic information about a tenant's network, such as network traffic, alarms, devices, and STAs. The following describes each area of the page.

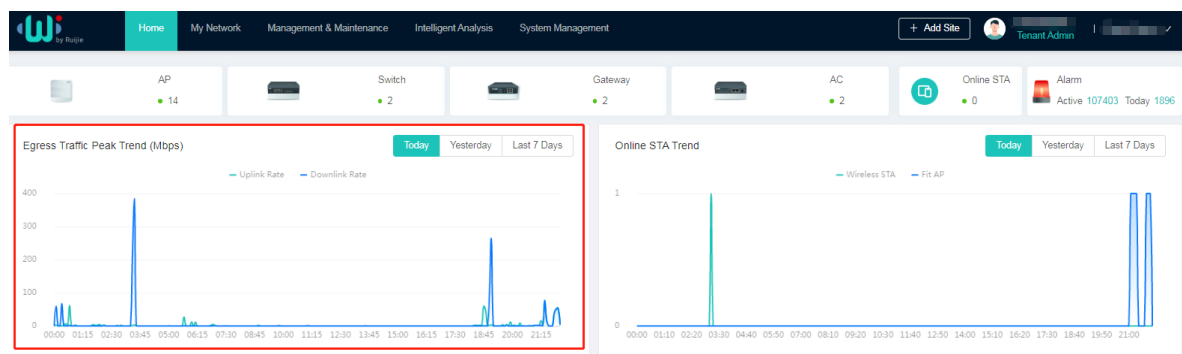
Figure 5-1 Home



5.1 Traffic

As shown in [Figure 5-2](#), traffic information, that is, **Egress Traffic Peak Trend**, is displayed in the upper left area.

Figure 5-2 Traffic Information

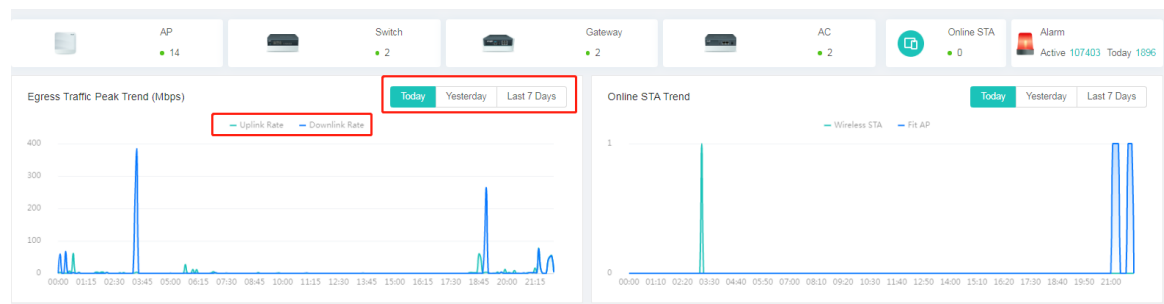


- **Egress Traffic Peak Trend (Mbps):** Displays the peak traffic of the egress at different time points of today, yesterday, and the last 7 days on a graph, in Mbps. The horizontal axis represents the time. The statistics interval of today and yesterday is 5 minutes, and the statistics interval of the last 7 days is 1 hour. The vertical axis represents the peak traffic, rounded to two decimal places. Hover the cursor over a curve to view the

uplink/downlink peak rate at a specified time point.

- **Uplink Rate:** Indicates the uplink peak rate of the egress traffic, represented by a green curve.
- **Downlink Rate:** Indicates the downlink peak rate of the egress traffic, represented by a blue curve.
- **Today:** Collects statistics on the uplink and downlink peak rates of today's egress traffic.
- **Yesterday:** Collects statistics on the uplink and downlink peak rates of yesterday's egress traffic.
- **Last 7 Days:** Collects statistics on the uplink and downlink peak rates of egress traffic in the last seven days (including the current day).

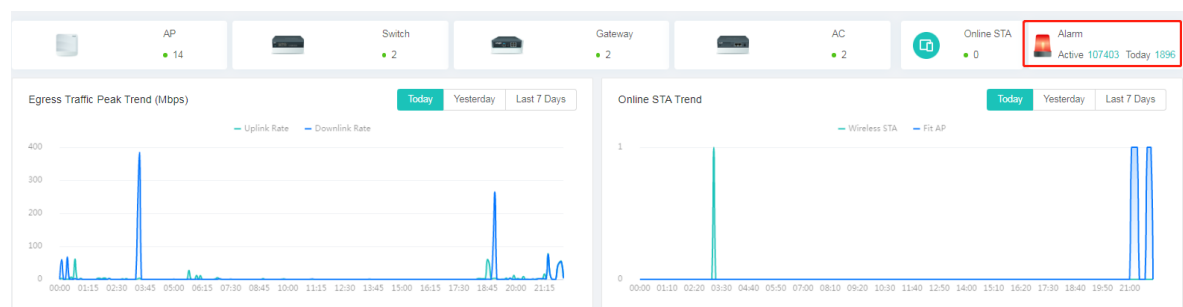
Figure 5-3 Egress Traffic Peak Trend



5.2 Alarm

As shown in [Figure 5-4](#), this area displays the number of active alarms and the number of today's alarms. You can click the alarm area to redirect to the alarm management page. For details about alarms, see [Alarm Management](#).

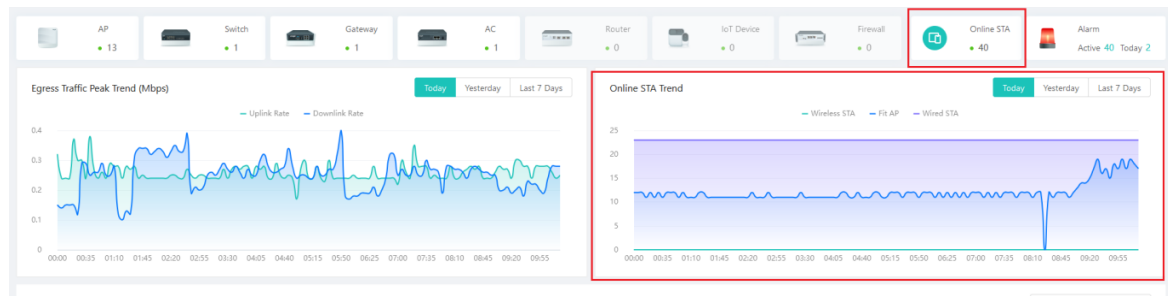
Figure 5-4 Alarm



5.3 Online STA

As shown in [Figure 4-5](#), this area displays information about devices on the current network. It includes **Online STA** and **Online STA Trend**.

Figure 5-5 Online STA



● **Online STA**

The **Online STA** area displays the total number of online STAs. When you hover the cursor over **Online STA**, the quantities of STAs connected to different types of devices are displayed. The devices include cloud APs and fit APs.

Figure 5-6 Viewing the Number of Online/Offline Devices

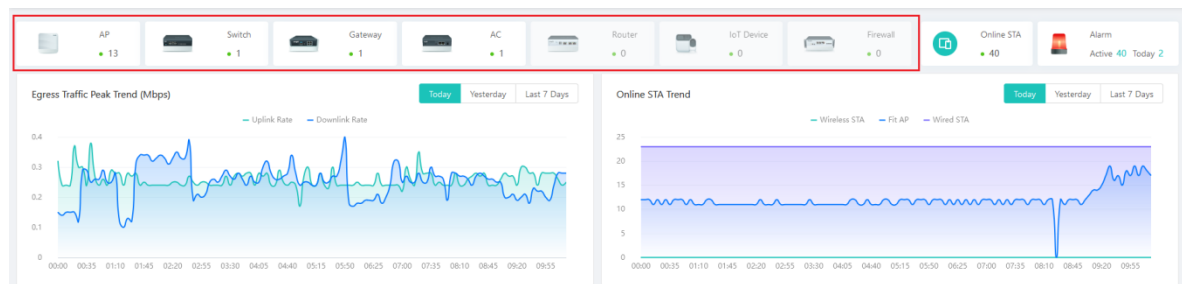
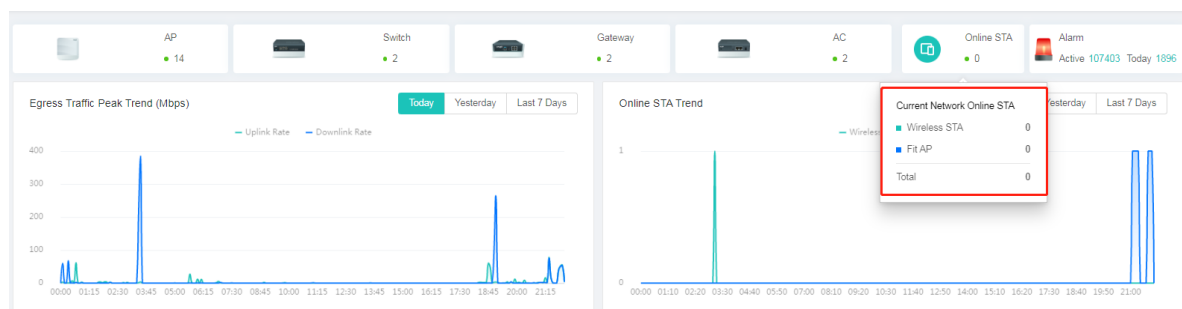


Figure 5-7 Viewing Online STAs



Click the device or STA icon to go to the device or STA management page. For details about the device/STA management, see Management and Maintenance.

● **Online STA Trend**

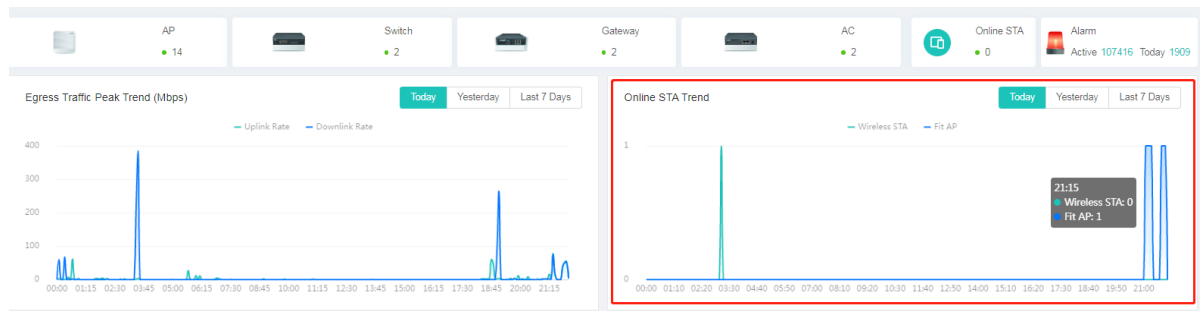
This area shows the number of online STAs at different time points on a graph. The graph is described as follows:

- **Date:** You can view graphs of different dates. You can select **Today**, **Yesterday**, or **Last 7 Days**.
- **Horizontal axis:** The horizontal axis represents the time. When you select **Today** or **Yesterday**, the

statistics interval is 5 minutes. When you select **Last 7 Days**, the statistics interval is 1 day and the number is the total number of online STAs on that day. Hover the cursor on the graph to view the number of online STAs at a specific time point.

- **Vertical axis:** The vertical axis represents the number of online STAs at a certain time point.
- **Sky blue curve:** Indicates the number of online wired STAs.
- **Blue curve:** Indicates the number of online fit APs.
- **Green curve:** Indicates the number of online cloud APs.

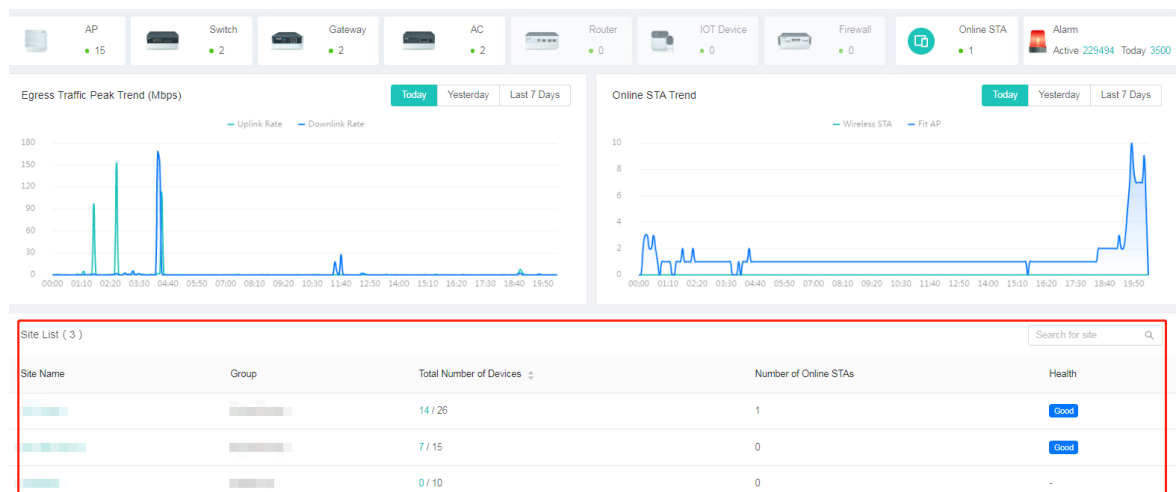
Figure 5-8 Online STA Trend Graph



5.4 Site

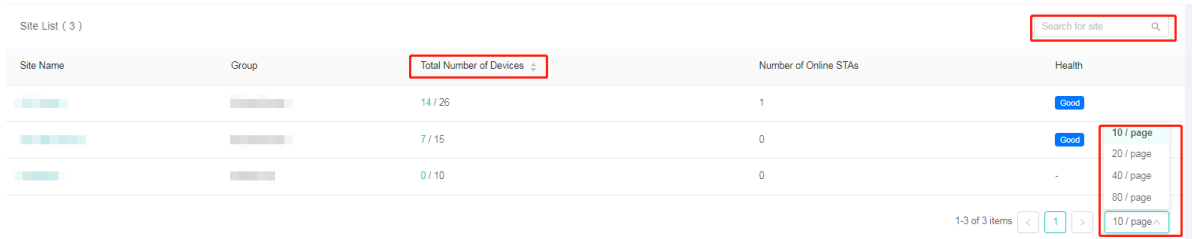
As shown in [Figure 5-9](#), this area lists the sites, where devices are located.

Figure 5-9 Site Area



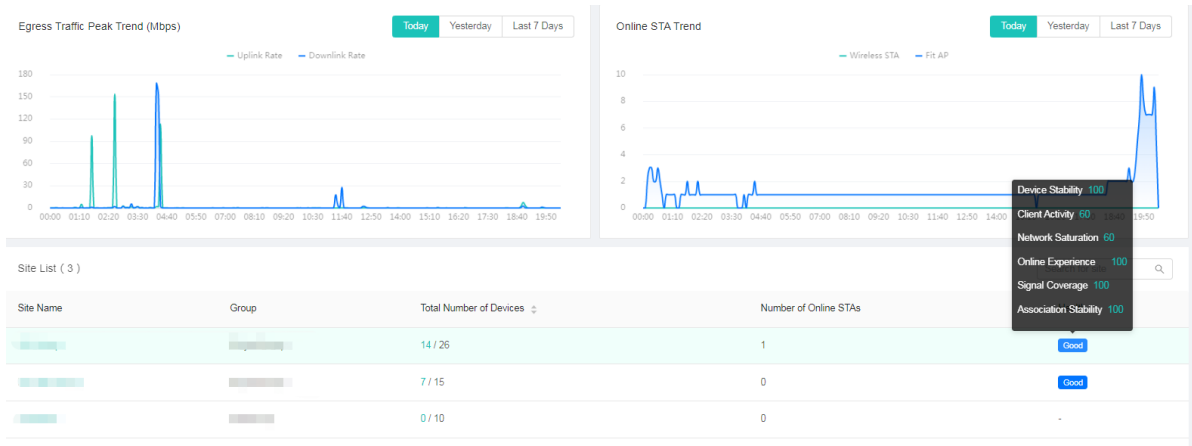
The site list displays the site name, location, group, total number of devices, number of online STAs, and health. You can search for site records by site name and specify the number of items to be displayed on each page. The list can be sorted by the total number of devices.

Figure 5-10 Site List



Click a site name to go to the **Site Overview** page. For details about site management, see [Site Overview](#). Currently, health check is available at sites that have ACs. The health check scope is all devices at the site. The health check results include excellent, good, fair, and poor. Health check items include device stability, client activity, network saturation, online experience, signal coverage, and association stability. You can hover the cursor over a health check result to view the results of different health check items.

Figure 5-11 Site Name and Health



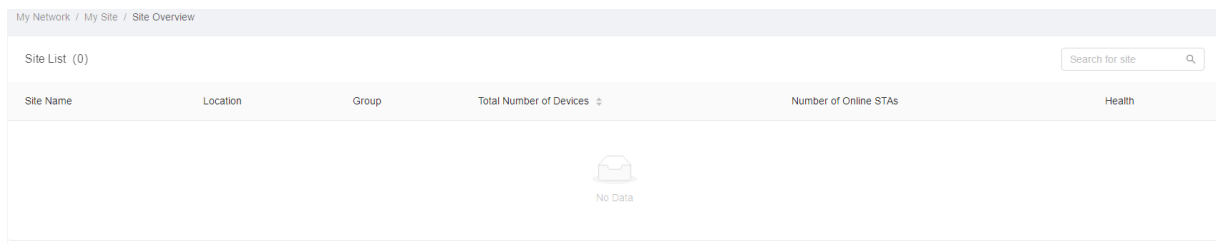
6 My Network

6.1 Site Overview

6.1.1 Site List

Choose **My Network > My Site > Site Overview** to go to the site list. The site list displays the site name, location, group, total number of devices, number of online STAs, and health.

Figure 6-1 Site List

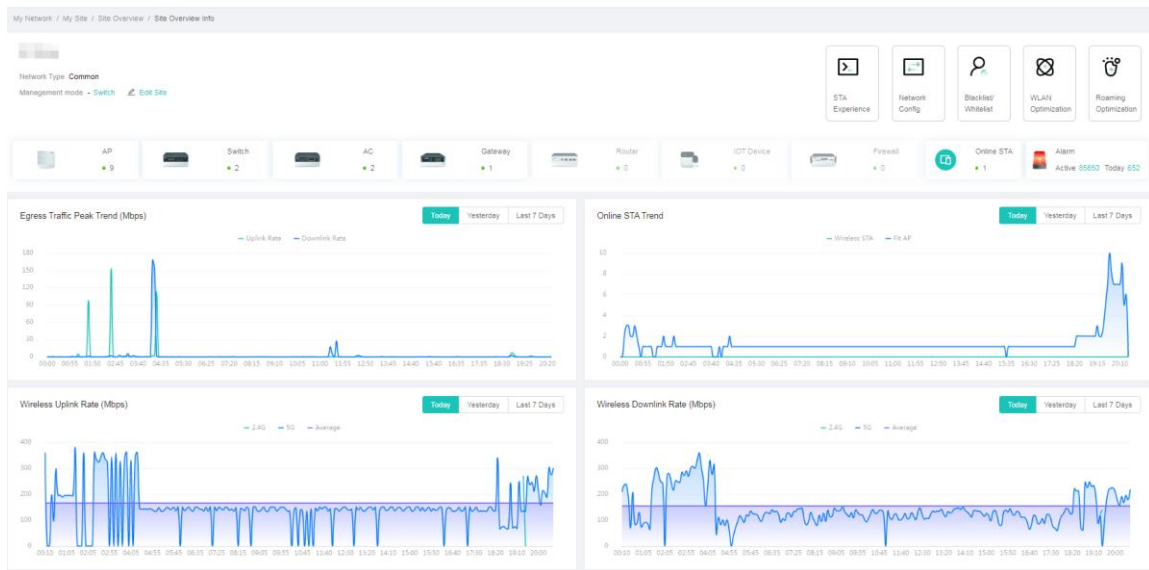


In the site list, you can set the number of items to be displayed on each page (10 items/page, 20 items/page, 40 items/page, or 80 items/page) and sort the site list by the total number of devices.

6.1.2 Site Overview Info

Click a site name to go to the **Site Overview Info** page, which displays site information such as the number of online STAs, alarms, and wireless network indicators. The page provides quick entries for STA experience, network configuration, blacklist/whitelist, WLAN optimization, and roaming optimization.

Figure 6-2 Site Overview Info



At the top of the page, information about the current site is displayed, including the site name, location, and network type. The page also provides an entry for network configuration, which will be described in later sections.

In the middle and lower parts of the page, the network overview of the site is provided, including the number of online STAs, number of alarms, egress traffic peak trend, online STA trend, statistics on wireless uplink and downlink rates, wireless latency statistics, and wireless packet loss rate (%) statistics. The number of online STAs, number of alarms, egress traffic peak trend, and online STA trend graph are similar to those in [Home](#) except that the dimension is accurate to site. Therefore, they are not described here. Other network indicators are described in [Network Indicators](#).

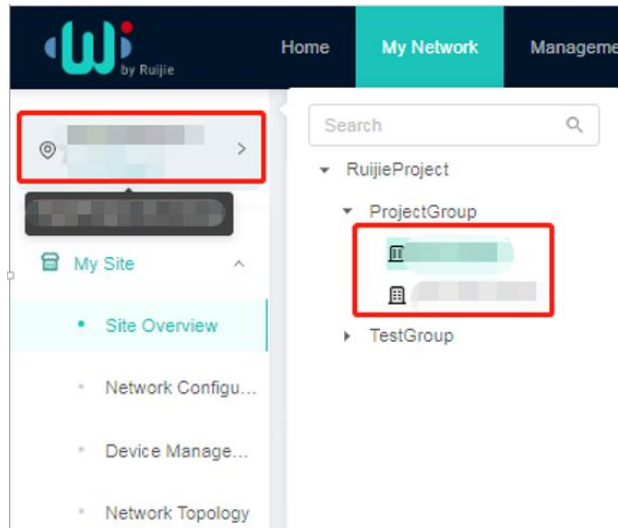
6.1.3 Switching a Site

You can click the site area in the upper left corner to switch to a different site, as shown in [Figure 6-3](#). Site switching allows you to search for a specified site by site name. Click a site name to view the information about the site.

Note

When you click a level-1 site, the system returns to the site list page.

Figure 6-3 Switching a Site

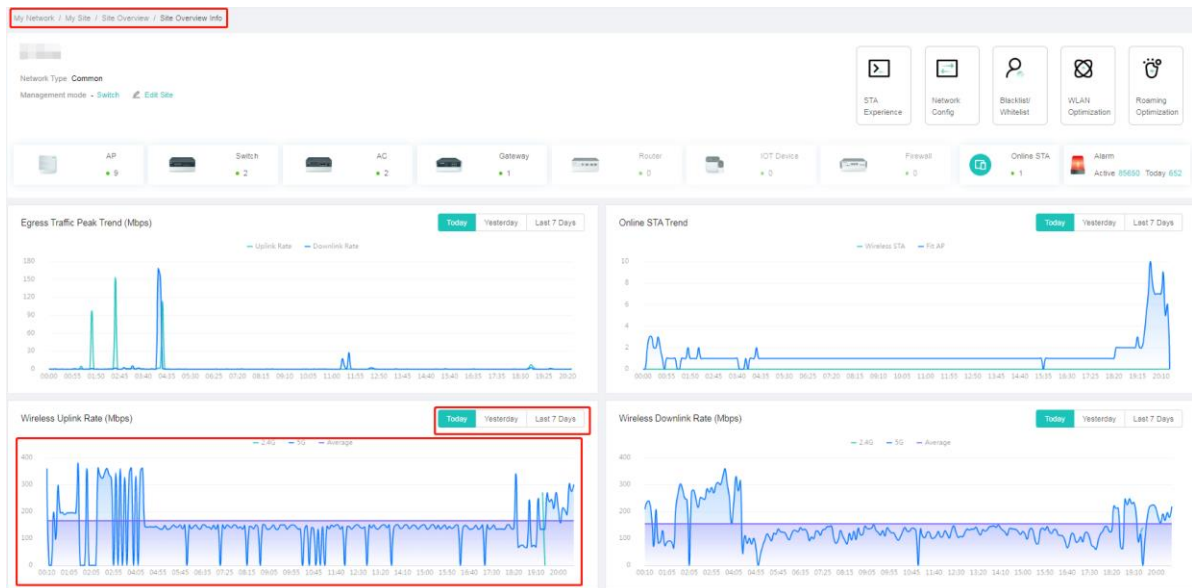


6.1.4 Network Indicators

- **Wireless Uplink Rate**

This graph shows statistics on the uplink rates and average uplink rates of different types of wireless STAs at different time points.

Figure 6-4 Wireless Uplink Rate Curve Graph

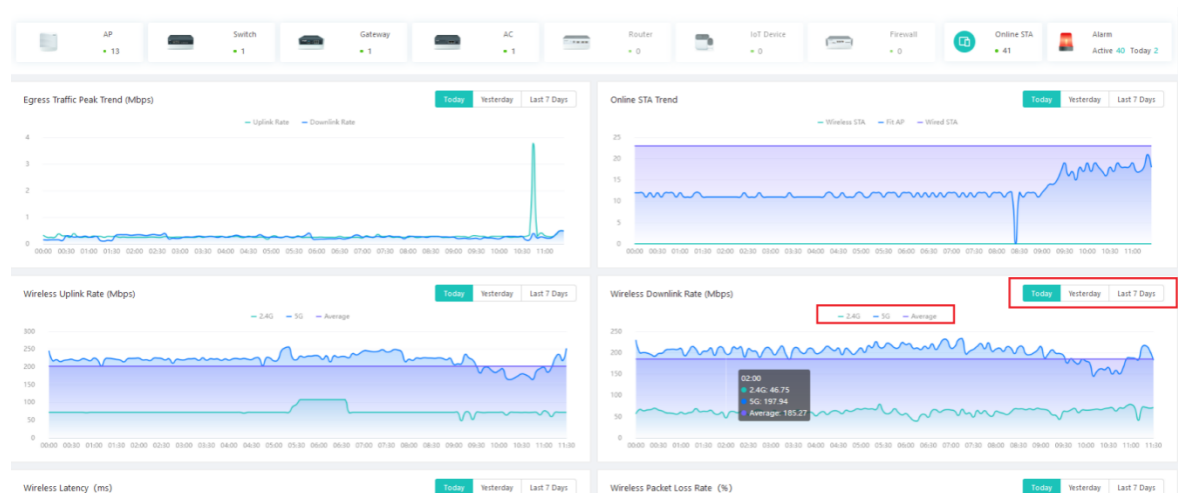


The graph is described as follows:

- **Green curve:** Indicates the uplink rate of 2.4 GHz wireless STAs.
 - **Blue curve:** Indicates the uplink rate of 5 GHz wireless STAs.
 - **Purple curve:** Indicates the average uplink rate of wireless STAs.
 - **Date:** The available dates include **Today**, **Yesterday**, and **Last 7 Days**.
 - **Horizontal axis:** Represents time. The statistics interval is 5 minutes. You can hover the cursor over a curve to view the uplink rates and average uplink rates of different types of STAs at a specified time point.
 - **Vertical axis:** Represents the uplink rate, in Mbps.
- **Wireless Downlink Rate**

This graph shows statistics on the downlink rates and average downlink rates of different types of wireless STAs at different time points.

Figure 6-5 Wireless Downlink Rate Curve Graph



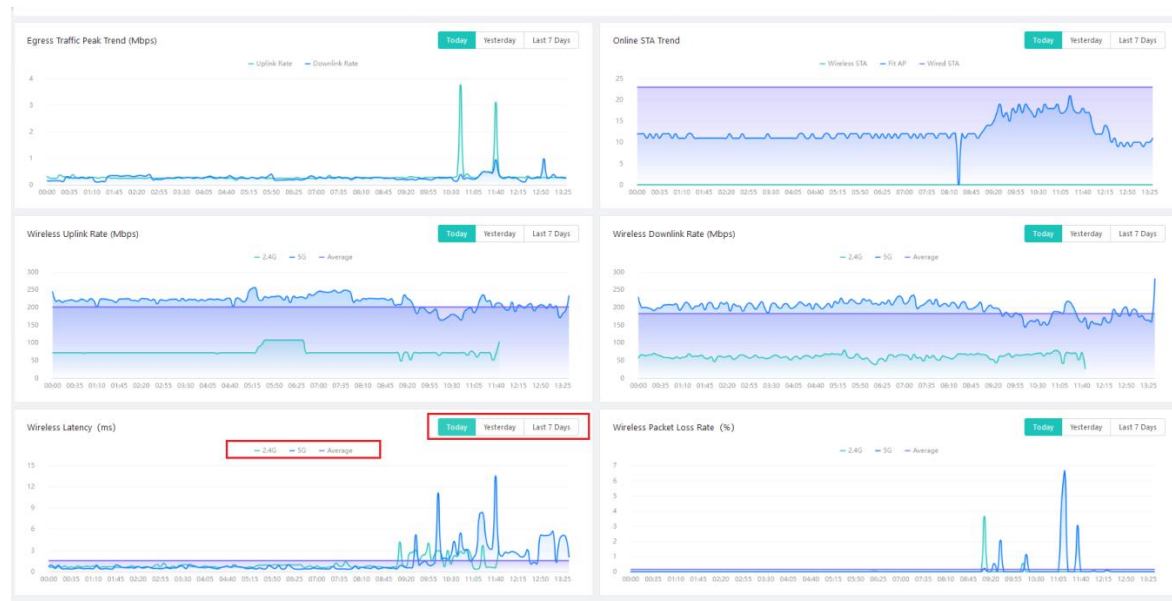
The graph is described as follows:

- **Green curve:** Indicates the downlink rate of 2.4 GHz wireless STAs.
- **Blue curve:** Indicates the downlink rate of 5 GHz wireless STAs.
- **Purple curve:** Indicates the average downlink rate of wireless STAs.
- **Date:** The available dates include **Today**, **Yesterday**, and **Last 7 Days**.
- **Horizontal axis:** Represents time. The statistics interval is 5 minutes. You can hover the cursor over a curve to view the downlink rates and average downlink rates of different types of STAs at a specified time point.
- **Vertical axis:** Represents the downlink rate, in Mbps.

● **Wireless Latency**

This graph shows the wireless latency and average latency of different types of wireless STAs at different time points.

Figure 6-6 Wireless Latency Curve Graph

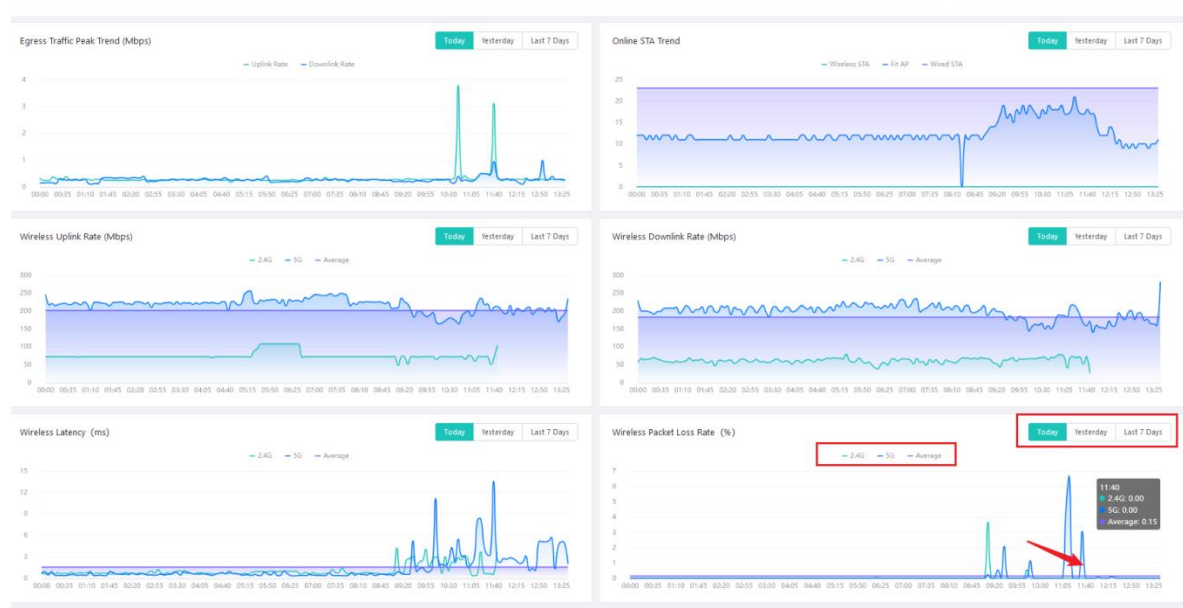


The graph is described as follows:

- **Green curve:** Indicates the latency of 2.4 GHz wireless STAs.
 - **Blue curve:** Indicates the latency of 5 GHz wireless STAs.
 - **Purple curve:** Indicates the average latency of wireless STAs.
 - **Date:** The available dates include **Today**, **Yesterday**, and **Last 7 Days**.
 - **Horizontal axis:** Represents time. The statistics interval is 5 minutes. You can hover the cursor over a curve to view the latency and average latency of different types of STAs at a specified time point.
 - **Vertical axis:** Represents the wireless latency, in ms.
- **Wireless Packet Loss Rate (%)**

This graph shows the packet loss rates and average packet loss rates of different types of wireless STAs at different time points.

Figure 6-7 Wireless Packet Loss Rate Curve Graph



The graph is described as follows:

- **Green curve:** Indicates the packet loss rate of 2.4 GHz wireless STAs.
- **Blue curve:** Indicates the packet loss rate of 5 GHz wireless STAs.
- **Purple curve:** Indicates the average packet loss rate of wireless STAs.
- **Date:** The available dates include **Today**, **Yesterday**, and **Last 7 Days**.
- **Horizontal axis:** Represents time. The statistics interval is 5 minutes. You can hover the cursor over a curve to view the packet loss rates and average packet loss rates of different types of STAs at a specified time point.
- **Vertical axis:** Represents the packet loss rate of wireless STAs, in percentage.

6.2 Network Configuration

The network configuration function allows you to perform network configuration for devices based on sites, such as WLAN configuration and CLI command sets. The configuration includes template configuration and personalized configuration.

⚠ Caution

- Modifying a configuration template and personalized configurations affects only newly connected devices. For already online devices, the configuration changes take effect on them only after **Deliver Config** is clicked.
- When a configuration template is inconsistent with a personalized configuration template, the personalized configuration overwrites the configuration template, that is, the personalized configuration takes precedence over the configuration template.

6.2.1 Binding a Template

As shown in [Figure 6-8](#), if no configuration template has been bound to a site, you can click **Bind Template** to go to the configuration template management page, on which you can bind a configuration template to the site. For details about configuration template management, see the description in "Management & Maintenance" > "Configuration" > "Template."

Figure 6-8 Binding a Configuration Template

The screenshot shows the 'Network Configuration' page. At the top, the breadcrumb 'My Network / My Site / Network Configuration / Network Configuration Info' is highlighted with a red box. Below it, there are tabs for 'Network Config' and 'Common Scenarios'. A blue information box contains text about applying templates. Under 'Current Template', the 'Bind Template' button is highlighted with a red box. Below this, there are tabs for 'WLAN Configuration' and 'CLI List'. A table lists three WLAN configurations with columns for WLAN ID, SSID, Encryption Mode, SSID Hiding, Forwarding Mode, Associate Radio, and Operation. The 'Operation' column for each row contains 'Edit', 'Delete', and 'Deliver Config' links. At the bottom right, there is a pagination control showing '1-3 of 3 items' and '10 / page'.

6.2.2 Personalized Configuration

Personalized configuration includes WLAN configuration and CLI list. WLAN configuration is used to configure SSIDs of cloud APs (fat APs) and other WLANs. It does not take effect on devices other than cloud APs (fit APs indirectly managed via AC management). The CLI list applies to all devices regardless of the device type.

1. WLAN Configuration

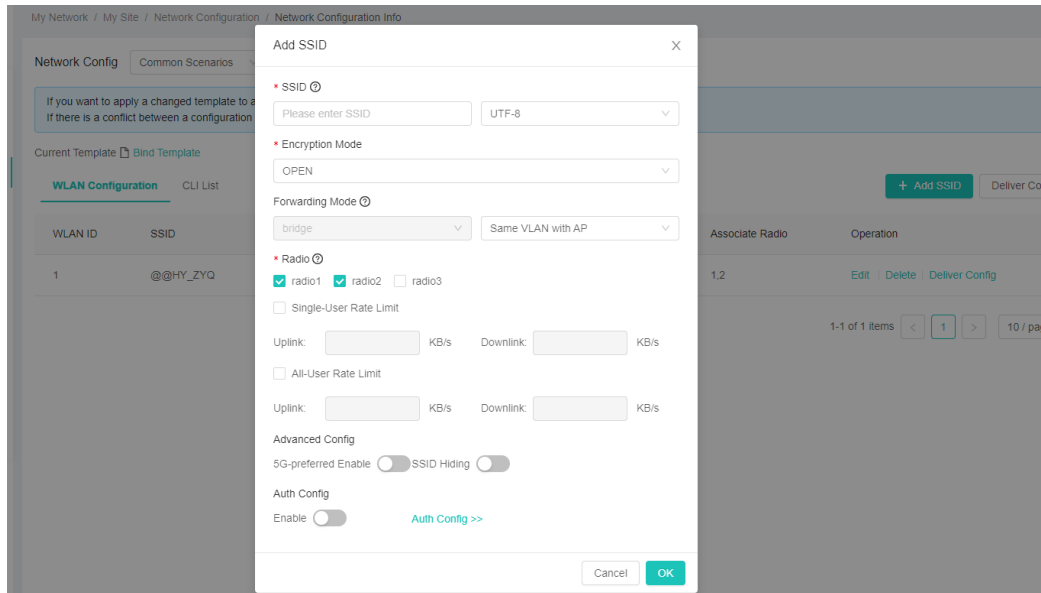
The WLAN configuration list is shown in [Figure 6-9](#). You can set the number of items to be displayed on each page and filter items by encryption mode or forwarding mode. You can click **Edit** or **Delete** in the **Operation** column to edit or delete WLAN configuration.

Figure 6-9 WLAN Configuration List

The screenshot shows the 'Network Configuration' page. At the top, the breadcrumb 'My Network / My Site / Network Configuration / Network Configuration Info' is highlighted with a red box. Below it, there are tabs for 'Network Config' and 'Common Scenarios'. A blue information box contains text about applying templates. Under 'Current Template', the 'Bind Template' button is highlighted with a red box. Below this, there are tabs for 'WLAN Configuration' and 'CLI List'. A table lists three WLAN configurations with columns for WLAN ID, SSID, Encryption Mode, SSID Hiding, Forwarding Mode, Associate Radio, and Operation. The 'Operation' column for the first row contains 'Edit', 'Delete', and 'Deliver Config' links, with the 'Edit' link highlighted by a red box. At the bottom right, there is a pagination control showing '1-3 of 3 items' and '10 / page'.

You can configure a personalized network template by adding an SSID. Click **Add SSID**, enter SSID information, and click **OK** to complete the personalized template configuration. To apply the configuration to a connected device, click **Deliver Config** to trigger the configuration delivery and make the configuration take effect.

Figure 6-10 Adding an SSID



Set the following parameters when adding an SSID:

- **SSID:** (Required) Enter an SSID name. You need to select the SSID encoding format. The default value is **UTF-8** and the options include **UTF-8** and **GBK**. If an SSID contains Chinese characters, garbled characters are displayed when an STA does not support UTF-8 encoding format.
- **Encryption Mode:** (Required) Select a value from the drop-down list. The options include **OPEN**, **WPA-PSK**, **WPA2-PSK**, and **WPA-PSK/WPA2-PSK**. When you select an encryption mode other than **OPEN**, you need to enter a password.

Note

OPEN: Indicates the open non-encryption authentication mode.

WPA2-PSK: Indicates a new encryption authentication mode based on WPA-PSK. It adopts the CCMP encryption mode and is compatible with the TKIP encryption mode.

- **Forwarding Mode:** The bridge mode is supported by default. To switch to the NAT mode, run CLI commands. You can set **VlanType** to **Same VLAN with AP** or use other VLANs. If you select other VLANs, enter the VLAN ID. The VLAN ID range is from 2 to 232 and from 234 to 4094.
- **Radio:** (Required) You can select one or more radios from radio1 to radio3. You can select **Single-User Rate Limit** and **All-User Rate Limit** and set uplink and downlink rate limits for them separately.

Caution

The SSID is valid only when the selected radio is in access mode.

- **Advanced Config:** (Optional) Advanced configuration includes **5G-preferred** and **SSID Hiding**. **5G-preferred** indicates that, when a radio provides both 2.4 GHz and 5 GHz bands and an STA supports both 2.4 GHz access and 5 GHz access, the STA connects to the 5 GHz band preferentially. **SSID Hiding** indicates that wireless networks are hidden and network signals cannot be searched out by STAs.

After the configuration is completed, new online devices automatically obtain the configuration of the current site. For already online devices, you need to click **Deliver Config** to make the configuration take effect on them.

Figure 6-11 Delivering the Configuration

My Network / My Site / Network Configuration / Network Configuration Info

Network Config Common Scenarios

If you want to apply a changed template to a device already in the network, please deliver the configuration after changing the template. If there is a conflict between a configuration template and a custom template, the custom template overrides the configuration template.

Current Template Bind Template

WLAN Configuration CLI List + Add SSID Deliver Config

WLAN ID	SSID	Encryption Mode	SSID Hiding	Forwarding Mode	Associate Radio	Operation
1	@@HY_ZYQ	OPEN	No	bridge	1,2	Edit Delete Deliver Config

1-1 of 1 items < 1 > 10 / page

2. CLI List

Click the **CLI List** tab to switch to the **CLI List** tab page. You can click **Edit** or **Delete** in the **Operation** column to edit or delete a CLI command set.

Figure 6-12 CLI Set List

My Network / My Site / Network Configuration / Network Configuration Info

Network Config Common Scenarios

If you want to apply a changed template to a device already in the network, please deliver the configuration after changing the template. If there is a conflict between a configuration template and a custom template, the custom template overrides the configuration template.

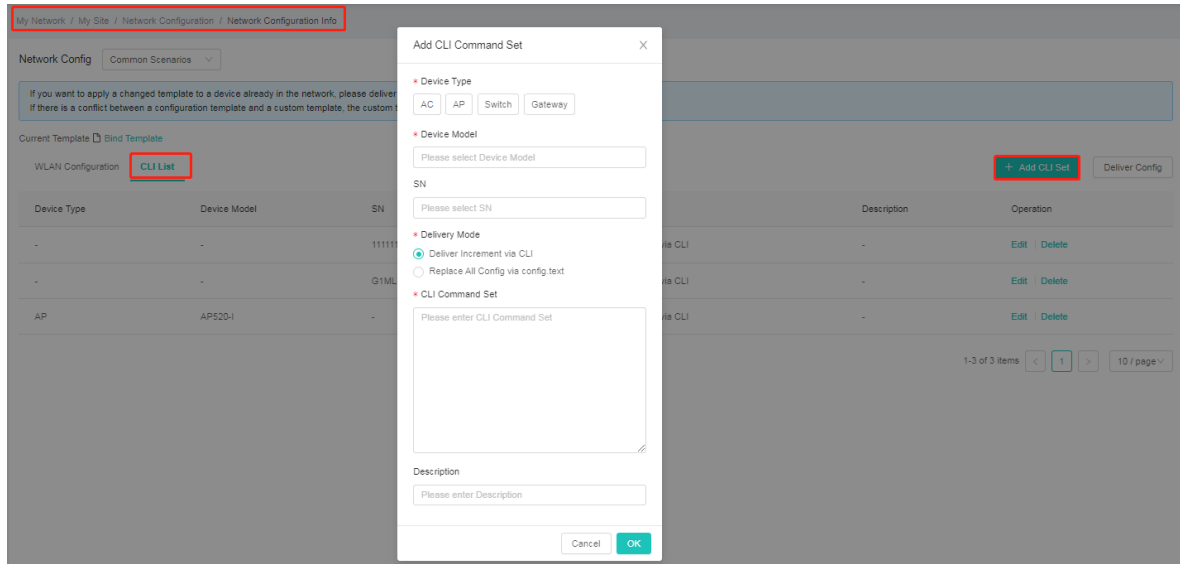
Current Template Bind Template

WLAN Configuration CLI List + Add CLI Set Deliver Config

Device Type	Device Model	SN	Delivery Mode	Description	Operation
No Data					

Click **Add CLI Set** to add a CLI command set for the network.

Figure 6-13 Adding a CLI Command Set



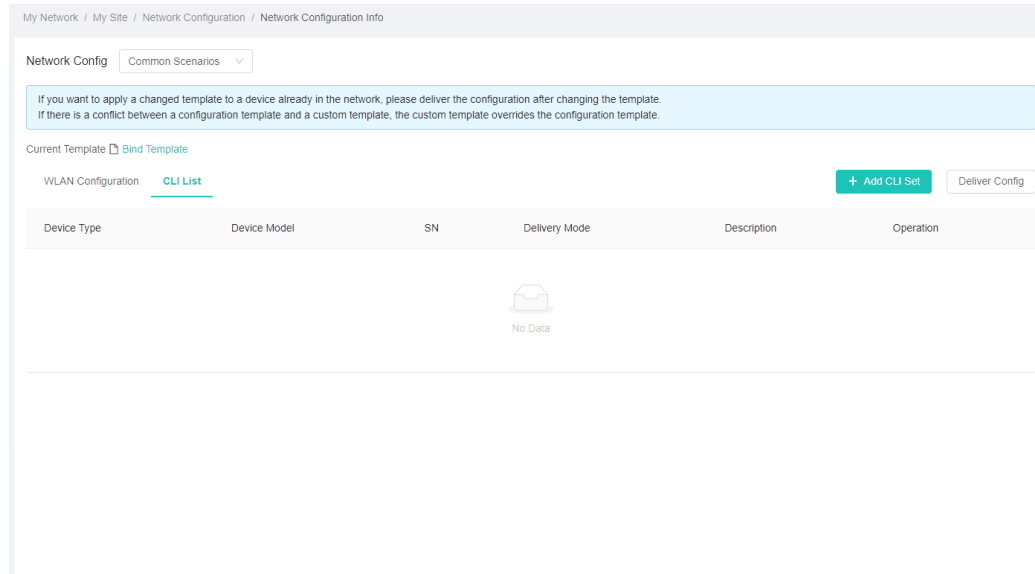
Configure the following parameters when adding a CLI command set:

- **Device Type:** (Required) Select the type of devices, to which the CLI command set is to be delivered. The options include **AC**, **AP**, **Switch**, **Gateway**, and **Router**. You can select only one of them.
- **Device Model:** (Required) Select the model of the devices, to which the CLI command set is to be delivered. Select a device model from the drop-down list. Multiple models can be selected.
- **SN:** (Optional) Select an existing SN from the drop-down list. If an SN is selected, the command set will be delivered only to the device matching the SN. If no SN is selected, the command set will be delivered based on the selected device model.
- **CLI Command Set:** (Required) Enter CLI commands to be configured for devices.
- **Description:** (Optional) Enter a description of the command set. It can be used as a remark.

After the configuration is completed, new online devices automatically obtain the configuration of the current site.

For already online devices, you need to click **Deliver Config** to make the configuration take effect on them.

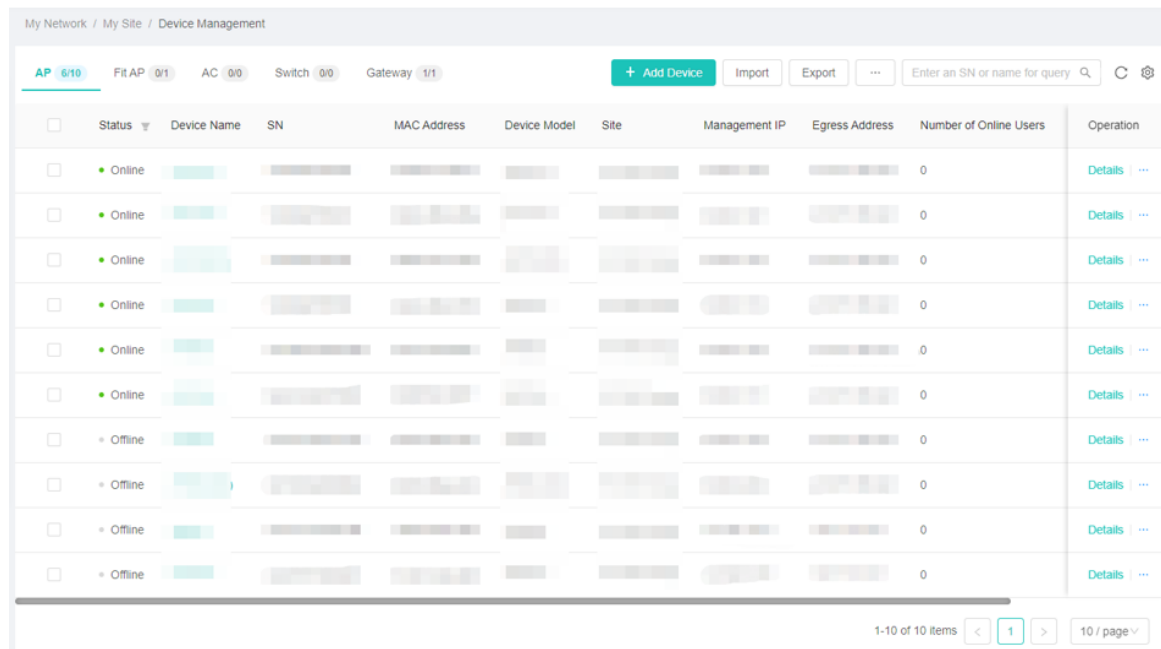
Figure 6-14 Delivering the Configuration



6.3 Device Management

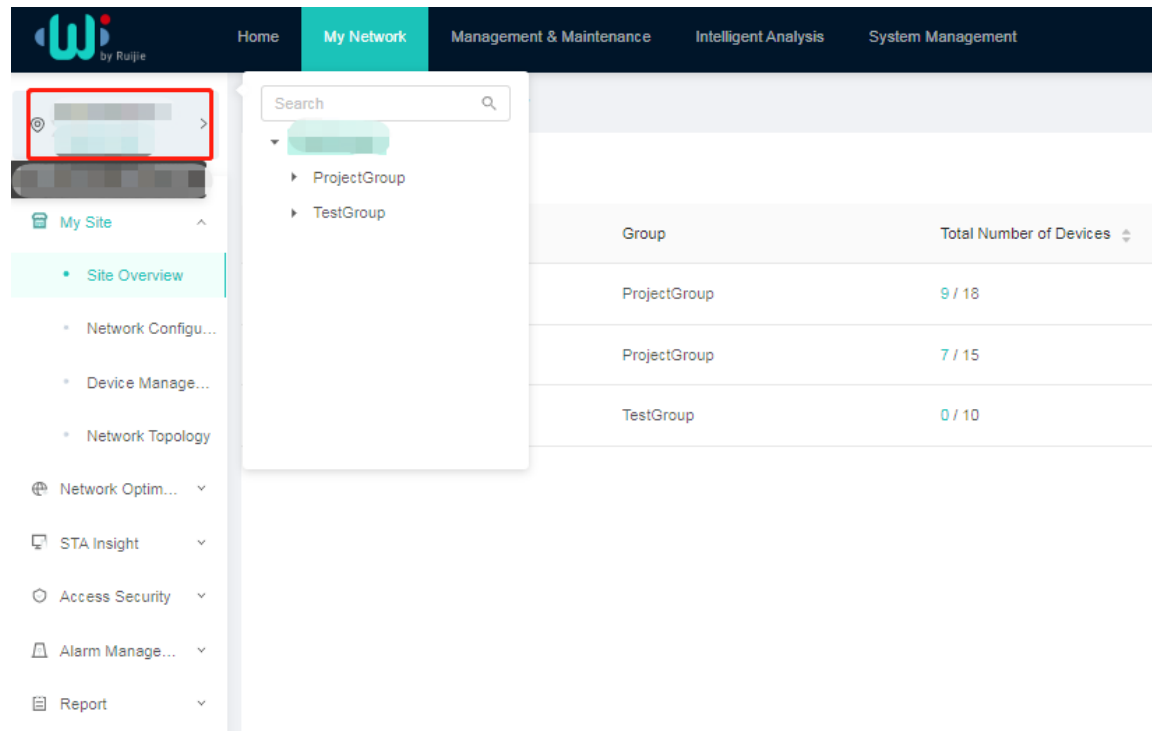
Choose **My Network > My Site > Device Management** to go to the **Device Management** page. Device management is to manage all types of devices in terms of site and present basic information about the devices.

Figure 6-15 Device Management



You can select different sites to quickly manage devices at different sites.

Figure 6-16 Switching a Site



Device management includes the management of fat APs, fit APs, ACs, switches, gateways, routers, IoT devices, and firewalls. The supported management functions are slightly different for different devices. The following uses the management of fat APs as an example.

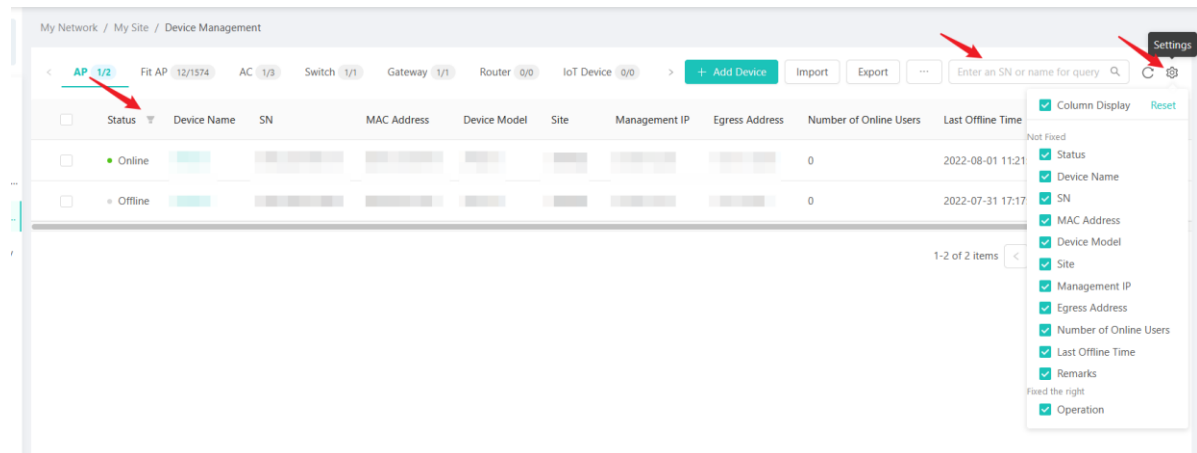
6.3.1 Device List

The AP list displays the AP status, device name, SN, MAC address, device model, site, last offline time, remarks, and other information. The list supports device query by SN or name. You can manually refresh the list and define fields to be displayed in the list. The list allows you to filter data by device status.

⚠ Caution

The fields displayed in the device list may vary with the device.

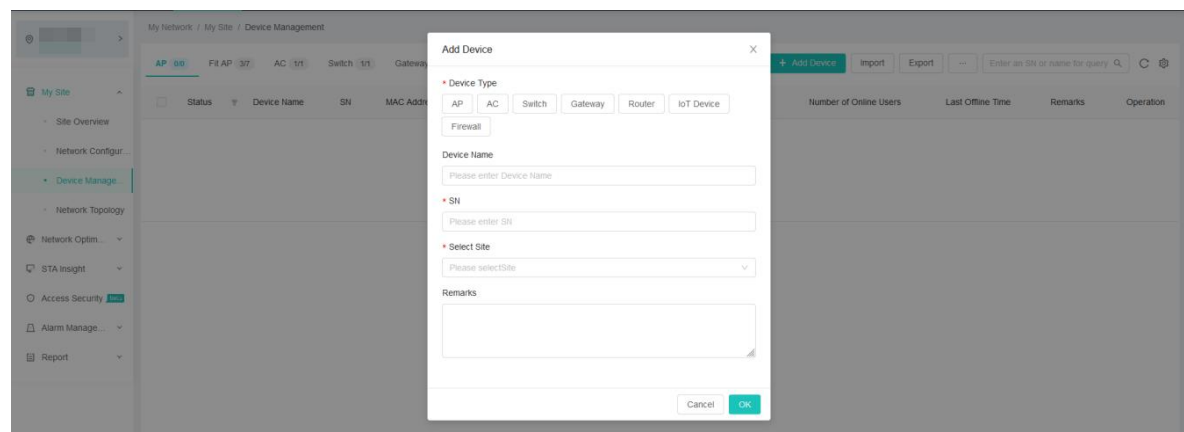
Figure 6-17 Device List



6.3.2 Adding a Device

Before a device goes online, you need to complete the device registration on WIS Cloud Network. Click **Add Device** to add a device.

Figure 6-18 Adding a Device



The parameters used to add a device are described as follows:

- **Device Type:** (Required) Select the type of device to be added. The options include **AP**, **AC**, **Switch**, **Gateway**, **Router**, and **IOT Device**.
- **Device Name:** (Required) It identifies a device. It is a string of up to 50 characters containing Chinese characters, letters, digits, underscores (_), hyphens (-), @, and &.
- **SN:** (Required) Enter the device SN. The value is a string of 13–15 characters containing digits or digits+letters.

A device SN can be obtained in two ways:


- **Command query:** Run the **show version** command on a device to display the device SN.

The following uses an AC as an example. G1L60EW000233 is the SN of the AC.

```
Ruijie#show version
System description : Ruijie Gigabit Wireless Switch(WS6008) By Ruijie Networks.
System start time : 2020-06-07 11:52:26
System uptime : 0:01:38:50
System hardware version : 1.00
System software version : AC_RGOS 11.9(5)BIT2
System patch number : NA
System serial number : G1L60EW000233
System boot version : 1.2.12
Module information:
Slot 0 : WS6008
Hardware version : 1.00
Boot version : 1.2.12
Software version : AC_RGOS 11.9(5)BIT2
Serial number : G1L60EW000233
```

- **Label query:** Check the label on the back of a product to obtain the device SN.
- **Device ID:** This parameter is required only for IoT devices, which are identified by device MAC address. The value is a string of no more than 100 characters.
- **Select Site:** (Required) Select the site, where the device is located.
- **Remarks:** (Optional) Enter the remarks of the device. The value is a string of no more than 400 characters.

After completing the configuration above, ensure that the device connects to WIS Cloud Network properly and then the **Device Management** page shows that the device is in the online state 3–6 minutes later.

 **Caution**

The SN and device type must be correct. Otherwise, the device cannot go online.

6.3.3 Importing Devices

WIS Cloud Network supports batch import of devices. The procedure is as follows:

- (1) Click **Import**.

Click **Import**. The **Batch Import Device** dialog box is displayed.

Figure 6-19 Bulk Importing Devices

Batch Import Device

* Select Site

1. Download the template and edit content in the .xls file.
(Note: A maximum of 500 records can be imported at a time.)

Download Template

2. Upload the template file.

Please select a .xls file.

Drag the template file to the box for fast uploading.

(2) Enter information.

Select the site, to which the devices to be imported belong.

Figure 6-20 Entering Information

Batch Import Device

* Select Site

1. Download the template and edit content in the .xls file.
(Note: A maximum of 500 records can be imported at a time.)

Download Template

2. Upload the template file.

Please select a .xls file.

Drag the template file to the box for fast uploading.

(3) Download a template.

Click **Download Template** to download the device import template to the local device.

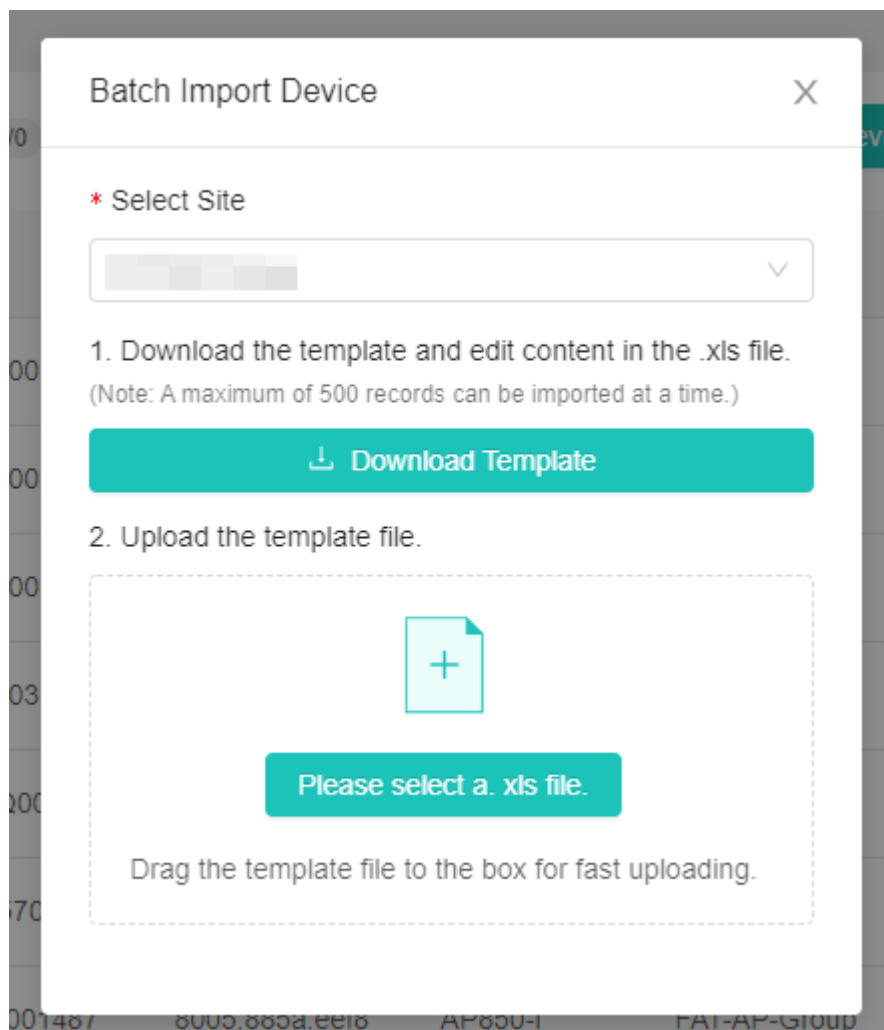
Parameters in the template are described as follows:

- **SN:** (Required) Enter the actual device SN. The value is a string of 13–15 characters containing digits or letters.
- **Device Type:** (Required) Select the actual device type.
- **Device Name:** (Required) It identifies a device. It is a string of up to 50 characters containing Chinese characters, letters, digits, underscores (_), hyphens (-), @, and &.
- **Device ID:** This parameter is required for IoT devices and is set to the device MAC address. The value is a string of no more than 100 characters.
- **Remarks:** (Optional) Enter the remarks of the device. The value is a string of no more than 400 characters.

(5) Upload the template.

Drag the template file to the specified area or click **Please select a.xls file.** and select the template file. Then, the system automatically imports devices that meet requirements from the template.

Figure 6-23 Uploading the Template



6.3.4 Deleting a Device

Click ... in the device list and select **Delete** to delete a specified device. Devices can be bulk deleted.

Figure 6-24 Deleting a Device

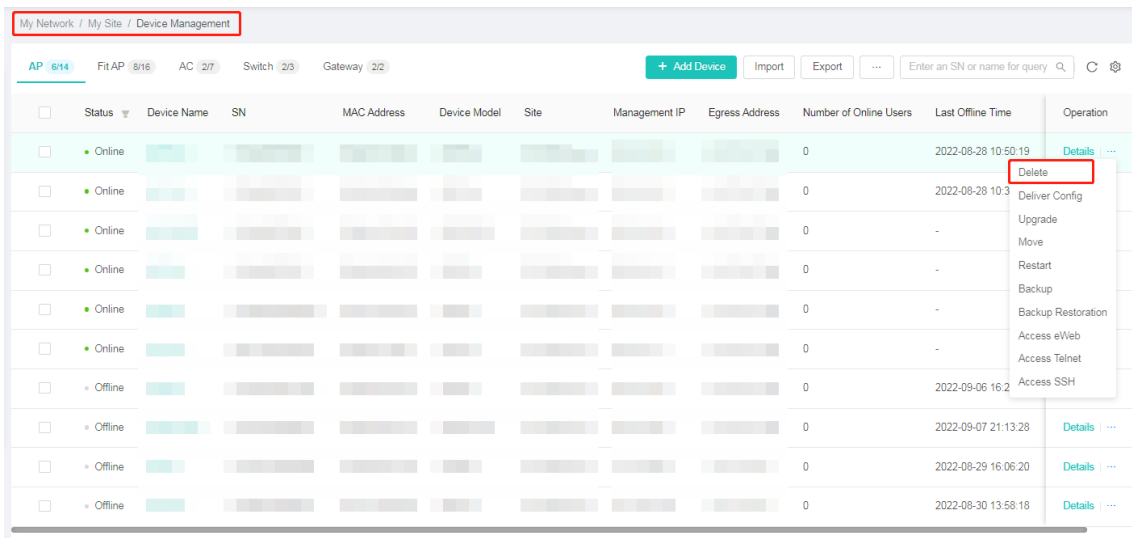
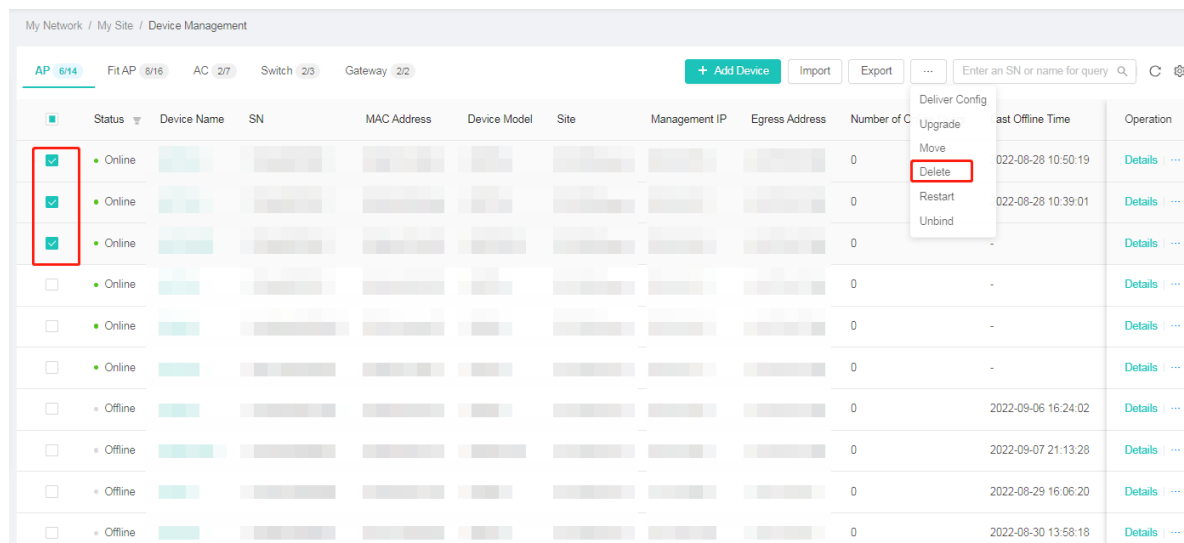


Figure 6-25 Bulk Deleting Devices



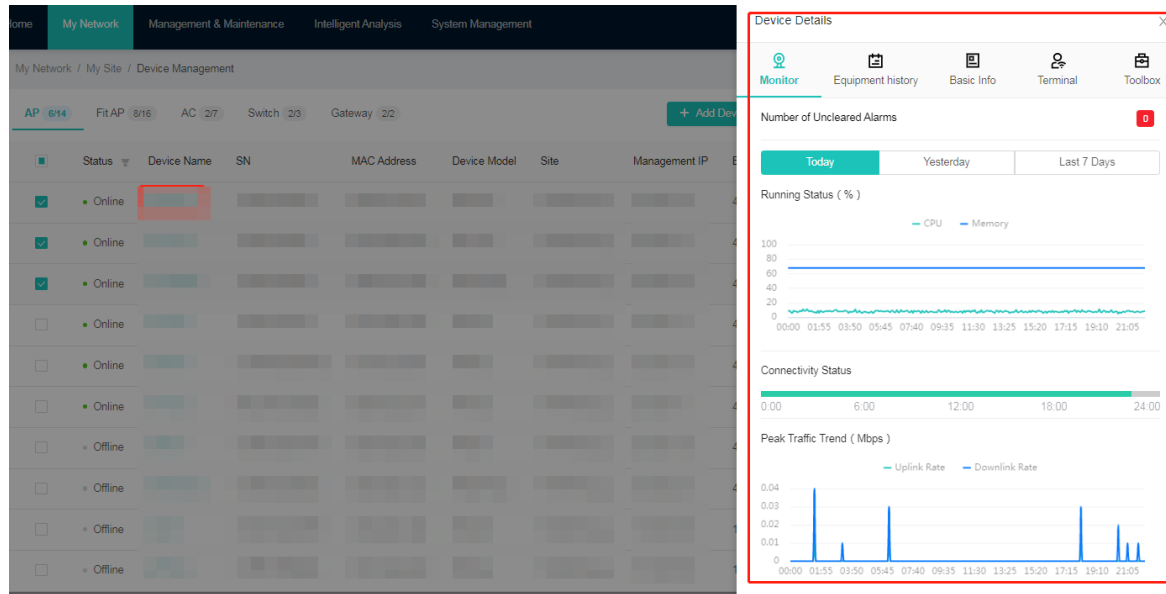
6.3.5 Device Details

Click a device name in the list or click **Details** in the **Operation** column for a device to view device details. The device details mainly include network indicators, basic information, details, and configuration functions of the device.

Caution

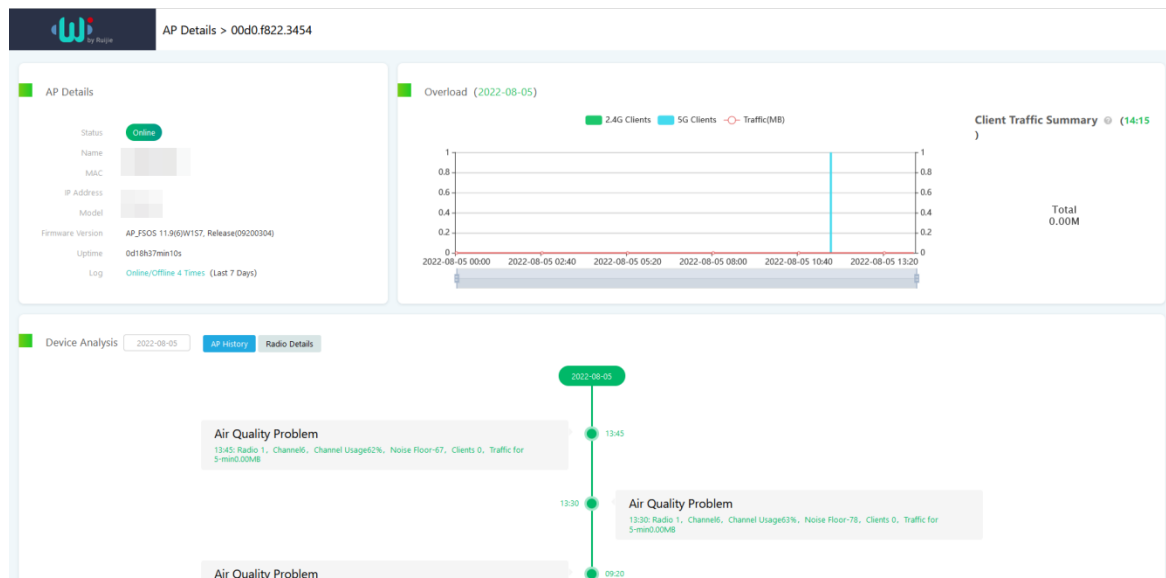
Items contained in device details vary with devices. This section uses the details of a fat AP as an example for description.

Figure 6-26 Device Details



The details of a fit AP are displayed on an independent page. The device details page displays basic information about the device, device load, and device analysis information.

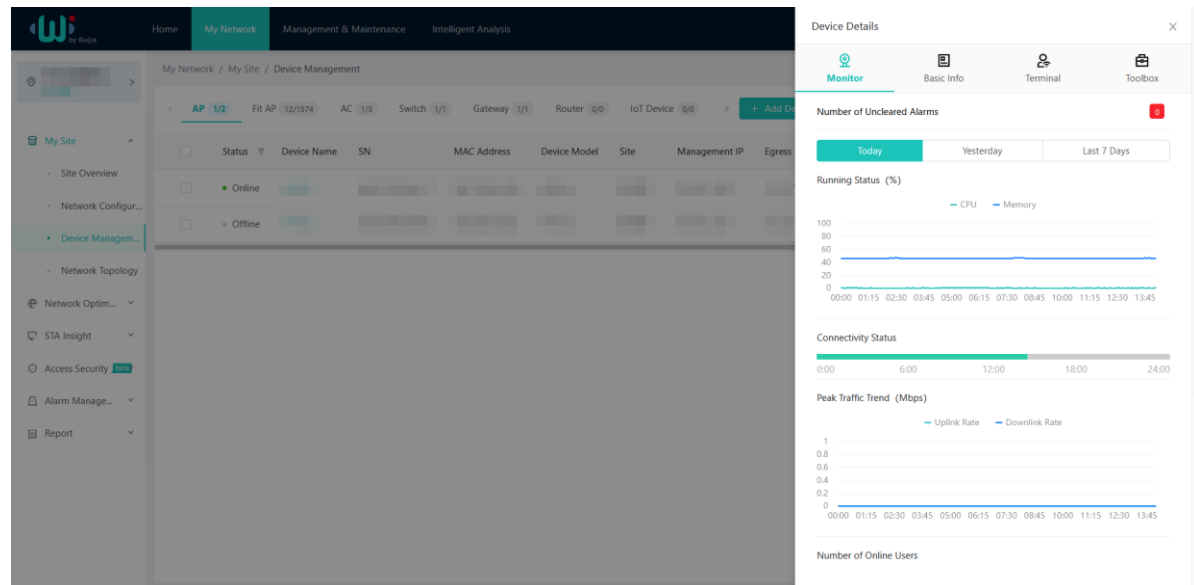
Figure 6-27 Details Page of a Fit AP



1. Monitor

Click a device name in the list or click **Details** in the **Operation** column for a device to view device details. Click the first icon in **Device Details** to view device status monitoring, including the number of uncleared alarms, running status, connectivity status, peak traffic trend, number of online users, and channel utilization.

Figure 6-28 Network Status Monitoring of a Device



Status monitoring details are described as follows:

- **Number of Uncleared Alarms:** Shows the number of uncleared alarms on the device. You can click the alarm quantity to go to the alarm management page.
- **Time:** You can switch the time bar to view network details in different periods. The time can be **Today**, **Yesterday**, or **Last 7 Days**.
- **Running Status (%):** Shows the CPU utilization and memory utilization, in percentage.
- **Connectivity Status:** Shows the connectivity status of the device in different periods.
- **Peak Traffic Trend (Mbps):** Shows the curve graph of peak traffic in different periods.
- **Number of Online Users:** Shows the number of currently online users served by the device.
- **Channel Utilization:** Shows the utilization of different channels on the device at different time points.

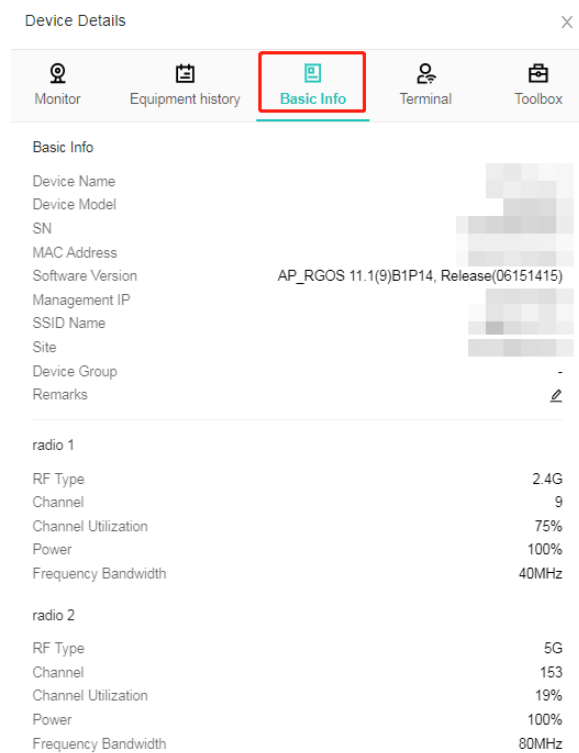
Monitoring information varies with devices and is described as follows:

- For cloud APs, status monitoring includes the number of uncleared alarms, running status, connectivity status, peak traffic trend, number of online users, and channel utilization.
- For fit APs, status monitoring includes device details, device load, and device analysis.
- For switches and ACs, status monitoring includes the number of uncleared alarms and running status.
- For routers, status monitoring includes the number of uncleared alarms, running status, and port rate trend.

2. Basic Info

Click a device name in the list or click **Details** in the **Operation** column for a device to view device details. Click the second icon **Basic Info** in **Device Details** to view basic information about the device, including the device name, model, MAC address, version, SSID, and channel. You can modify the device name and remarks on this page. Basic information about an AP also includes basic information about radios, and basic information about an RSR router also includes basic information about SIM cards.

Figure 6-29 Basic Info



Device Details

Monitor Equipment history **Basic Info** Terminal Toolbox

Basic Info

Device Name
 Device Model
 SN
 MAC Address
 Software Version AP_RGOS 11.1(9)B1P14, Release(06151415)
 Management IP
 SSID Name
 Site
 Device Group -
 Remarks

radio 1

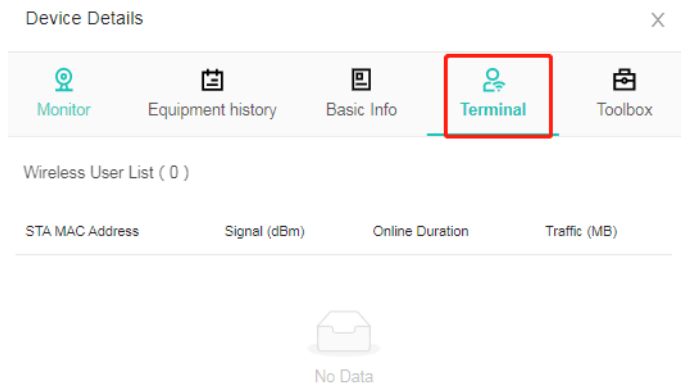
RF Type	2.4G
Channel	9
Channel Utilization	75%
Power	100%
Frequency Bandwidth	40MHz

radio 2

RF Type	5G
Channel	153
Channel Utilization	19%
Power	100%
Frequency Bandwidth	80MHz

3. Terminal

Click a device name in the list or click **Details** in the **Operation** column for a device to view device details. Click the third icon **Terminal** in **Device Details** to view the list of STAs connected to the current AP. The list provides the STA MAC address, signal, online duration, and traffic.

Figure 6-30 Wireless User List

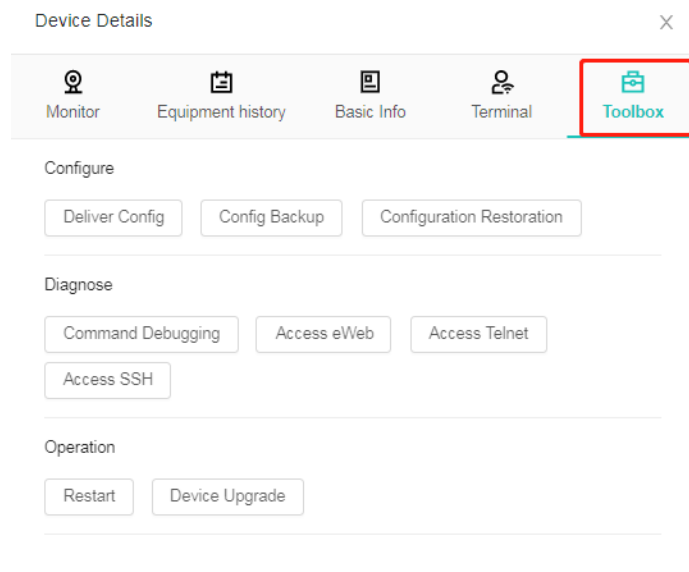
4. Toolbox

Click a device name in the list or click **Details** in the **Operation** column for a device to view device details. Click the fourth icon in **Device Details** to go to the **Toolbox** tab page. This page provides various management tools, including configuration, diagnosis, and operation tools, which meet various device management and control requirements.

- **Configure:** Includes **Deliver Config**, **Config Backup**, **Configuration Restoration**.
- **Diagnosis:** Includes **Command Debugging**, **Access eWeb**, and **Access Telnet**.
- **Operation:** Includes **Restart** and **Device Upgrade**.

Entries for these functions are also provided on the device list page. These functions will be described in subsequent sections.

Figure 6-31 Toolbox



6.3.6 Unbinding a Device

If the device to be added has been bound to the system and the device is by your side (you can configure commands on the device console), you can unbind the device. Click **...** and select **Unbind**. Follow the steps prompted on the page to unbind a device.

Figure 6-32 Unbinding a Device

My Network / My Site / Device Management

AP 6/14 Fit AP 8/16 AC 2/7 Switch 2/3 Gateway 2/2 [+ Add Device](#) [Import](#) [Export](#) ... Enter an SN or name for query

<input type="checkbox"/>	Status	Device Name	SN	MAC Address	Device Model	Site	Management IP	Egress Address	Number of C	Deliver Config	Upgrade	Last Offline Time	Operation
<input checked="" type="checkbox"/>	Online								0			2022-08-28 10:50:19	Details ...
<input checked="" type="checkbox"/>	Online								0			2022-08-28 10:39:01	Details ...
<input checked="" type="checkbox"/>	Online								0			-	Details ...
<input type="checkbox"/>	Online								0			-	Details ...
<input type="checkbox"/>	Online								0			-	Details ...
<input type="checkbox"/>	Offline								0			2022-09-06 16:24:02	Details ...
<input type="checkbox"/>	Offline								0			2022-09-07 21:13:28	Details ...
<input type="checkbox"/>	Offline								0			2022-08-29 16:06:20	Details ...
<input type="checkbox"/>	Offline								0			2022-08-30 13:58:18	Details ...

To unbind a device, do as follows:

- (1) Enter the device SN and click **Submit** to request device unbinding.

Note

- For details about how to view the device SN, see the SN acquisition method described in "Adding a Device."
- After submitting a request, complete unbinding within 15 minutes. Otherwise, you need to submit another request after the request expires.

(2) On the device to be unbound, run the unbinding command. The platform will automatically unbind the device after receiving the device unbinding request. The unbinding commands are as follows:

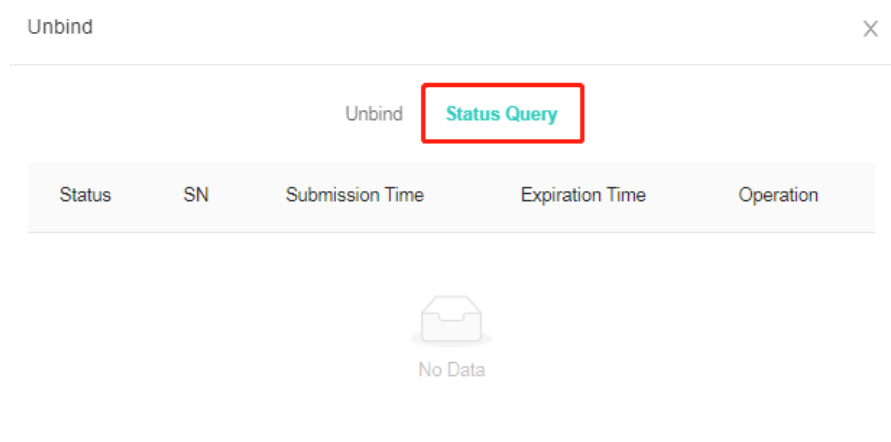
```
config
cwmp
acs url http://wiscloud.ruijienetworks.com/device/unbind
```

(3) Go to **Status Query** to check the unbinding result.

Note

If you need to add an unbound device to another project, configure the **acs url** `http://wiscloud.ruijienetworks.com/acs` command.

Figure 6-33 Status Query



6.3.7 Delivering the Configuration

Click ... in the device list and select **Deliver Config** to deliver a CLI command set to a device. Configuration delivery is a common task in the configuration management component. After delivery, you can view the configuration execution in **Management & Maintenance > Configuration > Task**.

Figure 6-34 Delivering the Configuration (01)

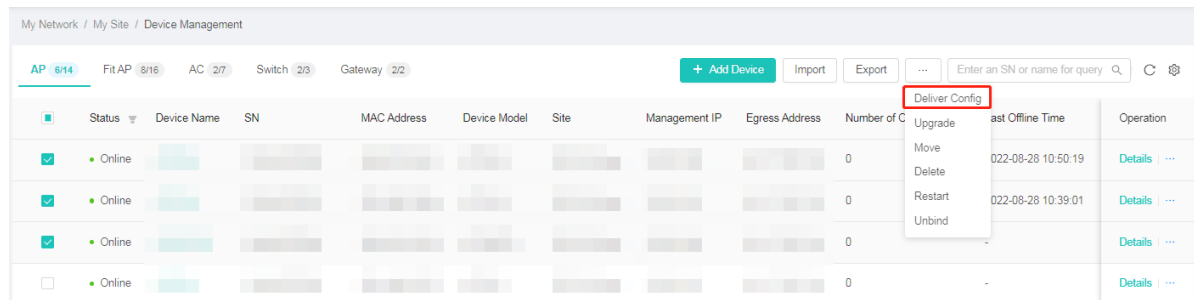
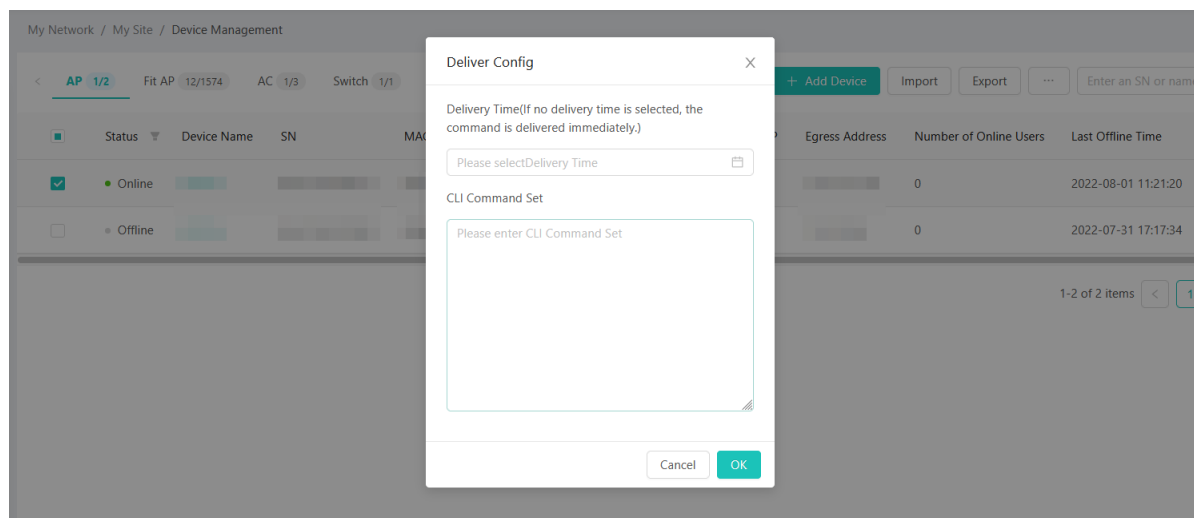


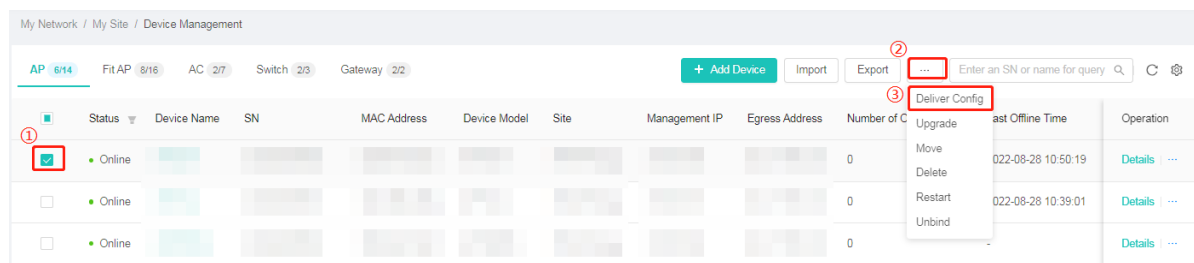
Figure 6-35 Delivering the Configuration (02)



Parameters for configuration delivery are described as follows:

- **Delivery Time:** (Optional) Specify the time for delivering a CLI command set. If no delivery time is specified, the CLI command set is immediately delivered.
- **CLI Command Set:** (Required) Edit the command set to be delivered to a device.

Figure 6-36 Bulk Delivering the Configuration



6.3.8 Upgrading Devices

Click ... in the device list and select **Upgrade** to upgrade a device. Batch upgrade is supported.

Figure 6-37 Upgrading a Device (01)

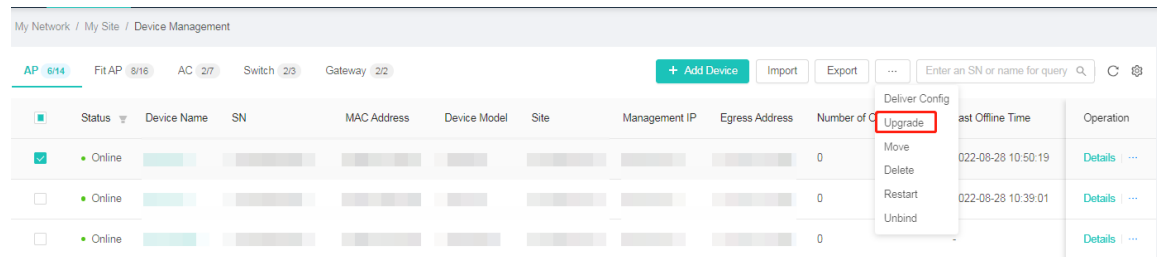
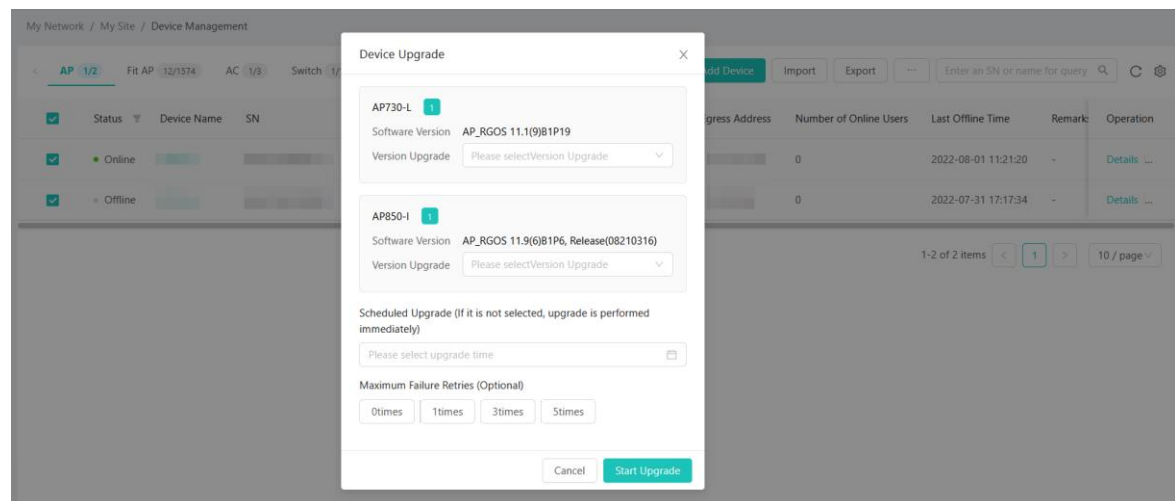


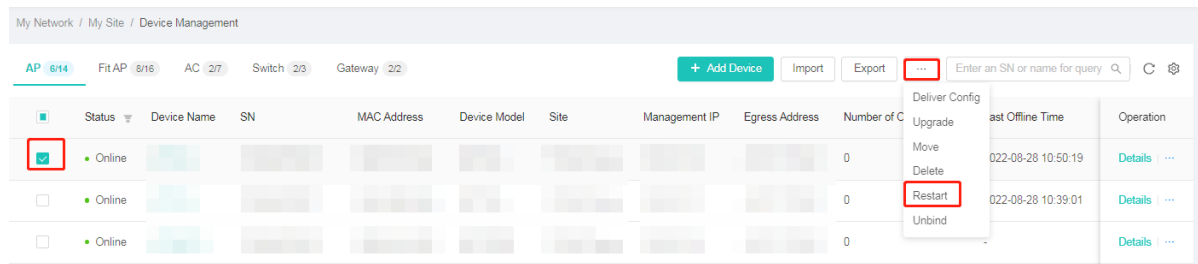
Figure 6-38 Upgrading a Device (02)



Device upgrade policies are described as follows:

- **Version Upgrade:** (Required) Select the target version of the upgrade. A device can be upgraded to any available version.
- **Scheduled Upgrade:** (Optional) Select the upgrade time. If the upgrade time is not specified, upgrade is performed immediately. No upgrade time is set by default.
- **Maximum Failure Retries:** (Optional) Set the maximum number of retries after an upgrade failure. The options include **0times**, **1times**, **3times**, and **5times**. No value is selected by default, indicating 0 retries.

Figure 6-39 Bulk Upgrading Devices



6.3.9 Moving a Device

Click ... in the device list and select **Move** to change the site, to which a device belongs. Devices can be bulk moved.

⚠ Caution

After a device is moved, the system will deliver the configuration of the new site to the device.

Figure 6-40 Moving a Device (01)

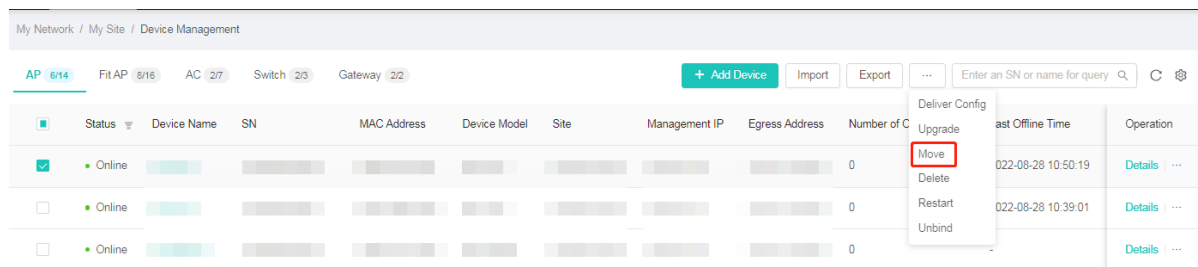


Figure 6-41 Moving a Device (02)

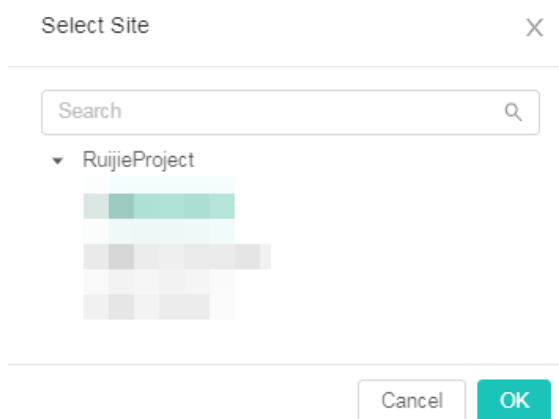
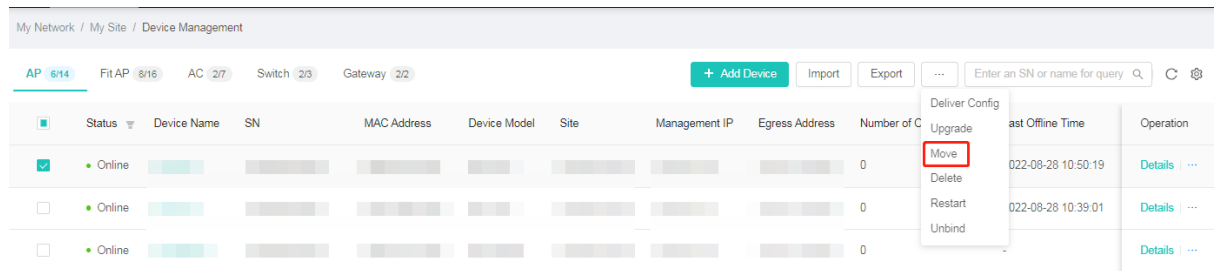


Figure 6-42 Bulk Moving Devices



6.3.10 Restarting a Device

Click ... in the device list and select **Restart** to restart a specified device. Perform this operation in a period, in which services are not affected. Batch restart is supported.

Figure 6-43 Restarting a Device (01)

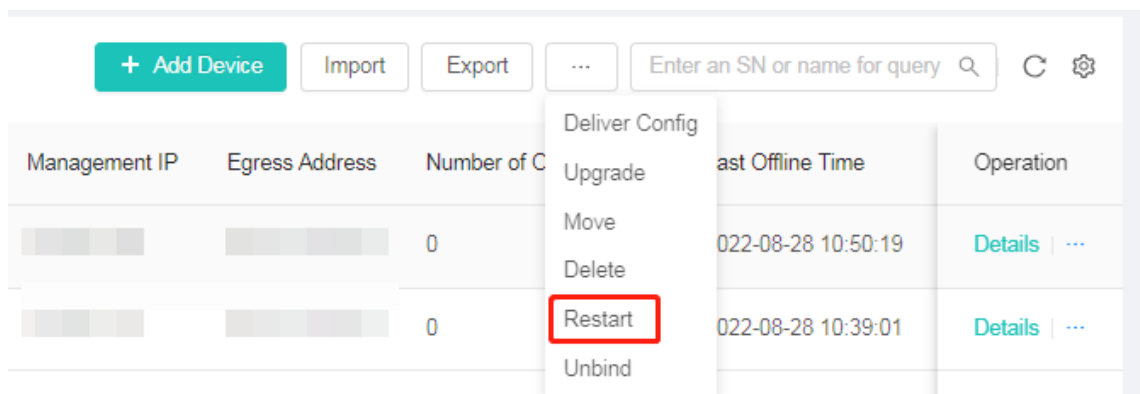


Figure 6-44 Restarting a Device (02)

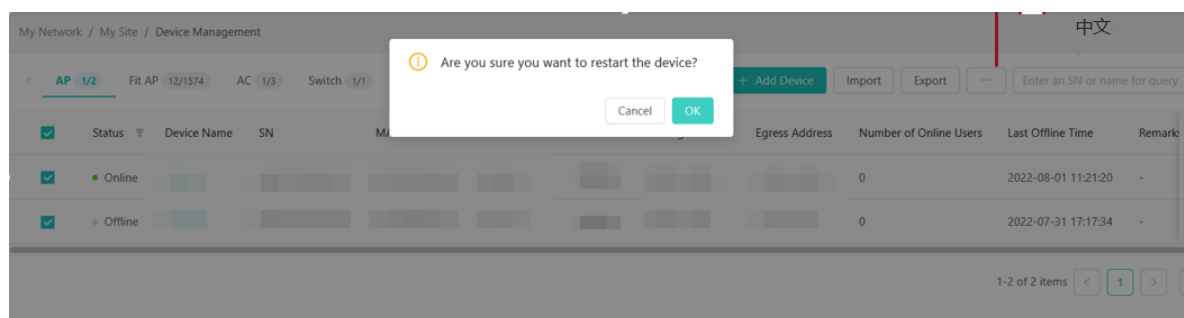
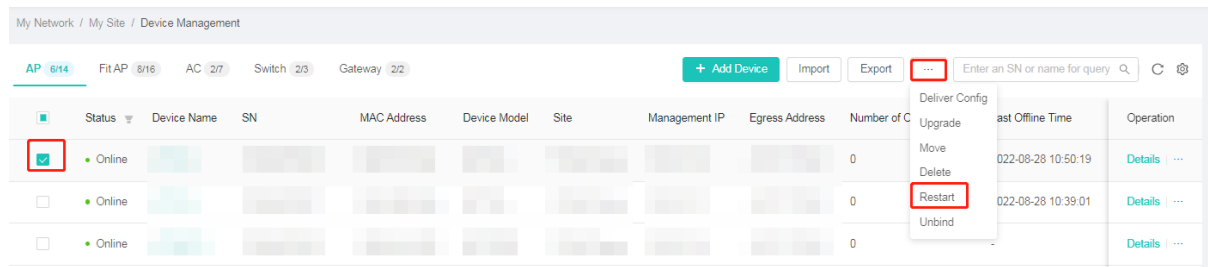


Figure 6-45 Bulk Restarting Devices



6.3.11 Backing Up the Configuration

Click ... in the device list for a specific device and select **Backup** to back up all current configurations of the device. After the backup is completed, you can view the operation configuration backup status of the device on the backup page.

Figure 6-46 Backing Up the Configuration (01)

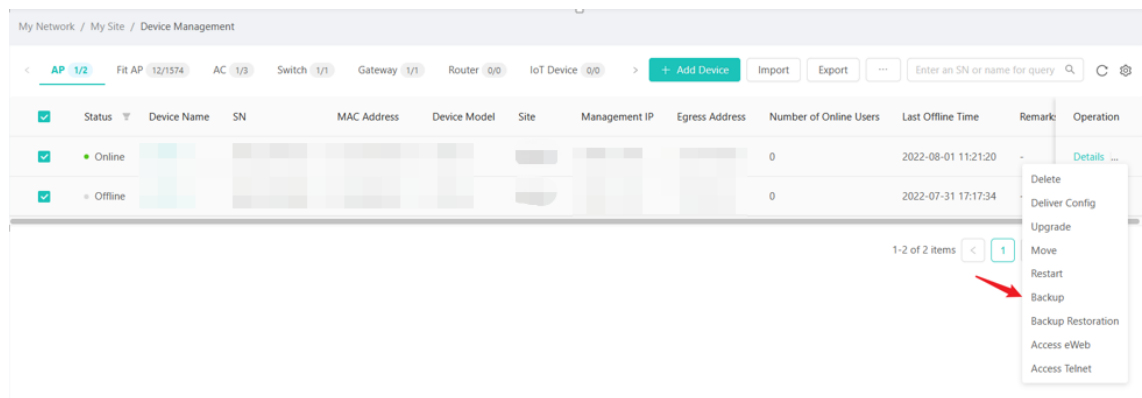


Figure 6-47 Backing Up the Configuration (02)

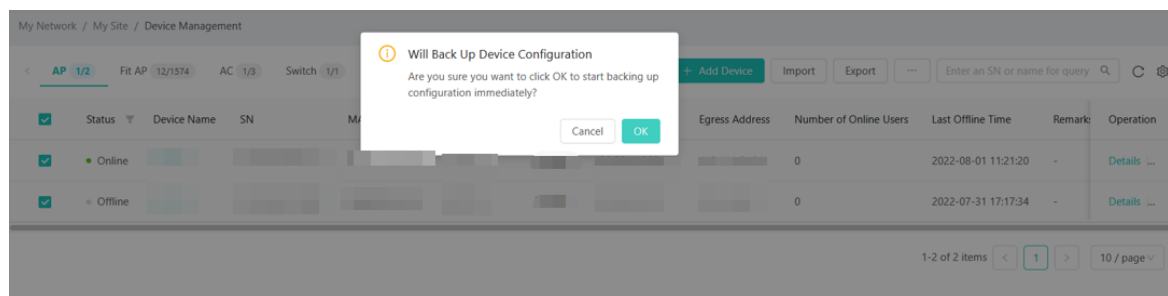
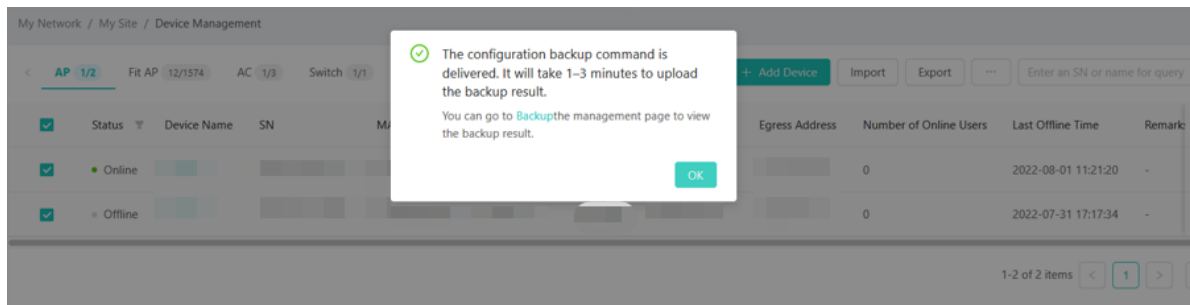


Figure 6-48 Successful Delivery of the Backup Command

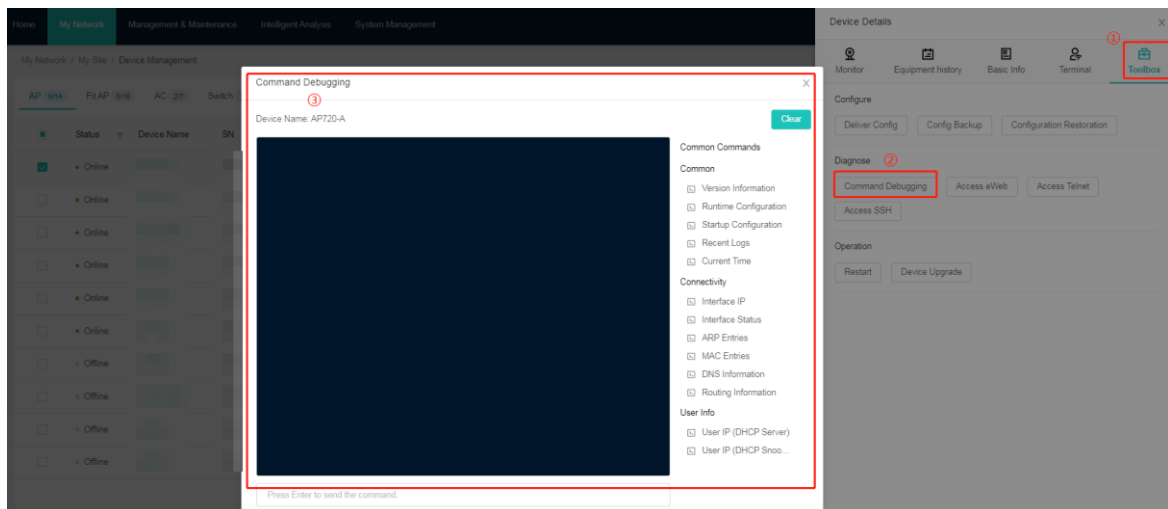


Click **Backup** in the pop-up box to redirect to the configuration backup management page and view the backup result.

6.3.12 Command Debugging

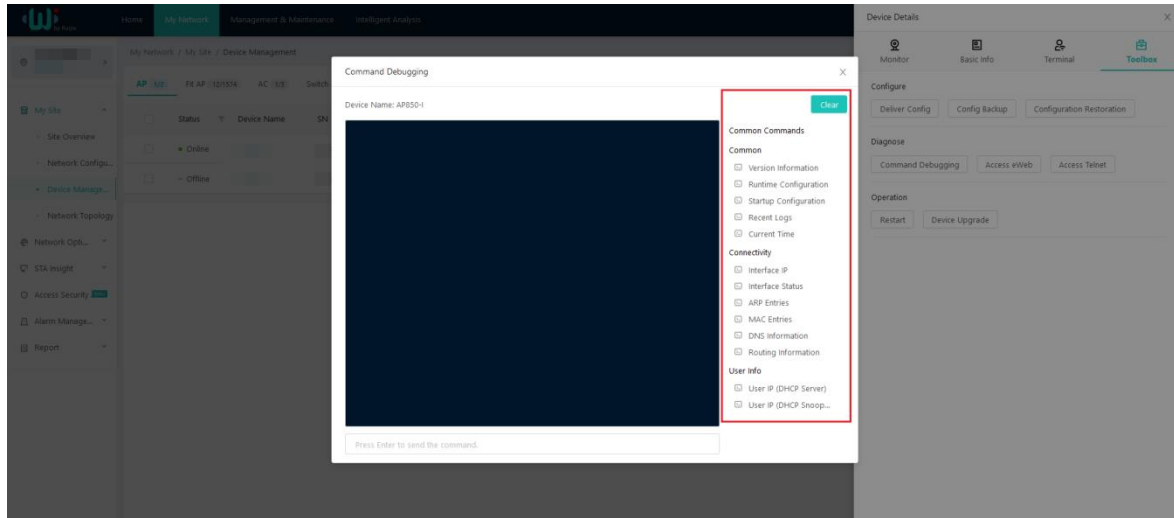
On the **Device Details** page, click the **Toolbox** tab and then click **Command Debugging** to go to the debugging window. Enter commands in the input box and press **Enter** to remotely debug a device. The command execution results are displayed in the black area shown in the figure.

Figure 6-49 Command Debugging



The command debugging window provides shortcut buttons for common commands, such as **Version Information**, **Runtime Configuration**, **ARP Entries**, **Routing Information**, and **User IP**. You can click a common command and view command output rapidly. Click **Clear** to clear information on the current screen.

Figure 6-50 Shortcut Common Commands



6.3.13 Restoring the Configuration from Backups

Click **...** in the device list and select **Backup Restoration** to restore the required configuration from configuration backups. You can restore the configuration from configuration backups on the local device or restore the configuration from configuration backups in other similar devices to the local device. The backup list displays the name of the backed up device, backup time, and remarks. You can quickly identify different backups based on information in the backup list, and search for backups by remarks or device name. Select a specified backup and click **Restore to Device** to trigger the backup restoration.

Figure 6-51 Restoring the Configuration from Backups

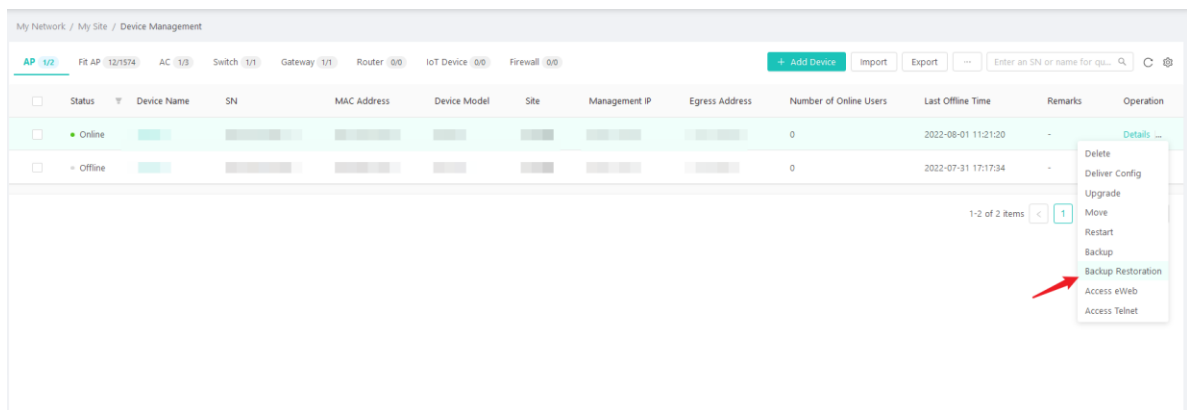


Figure 6-52 Restoring the Configuration from Backups in the Local Device

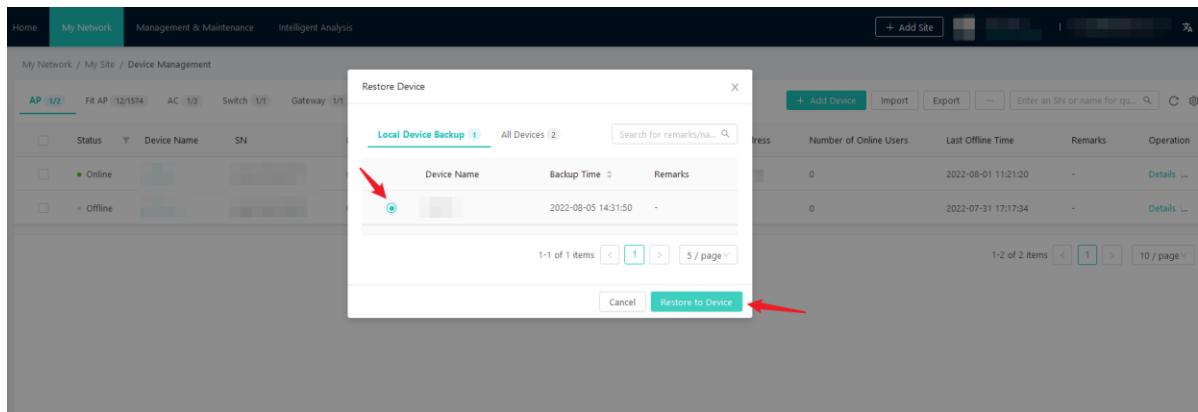
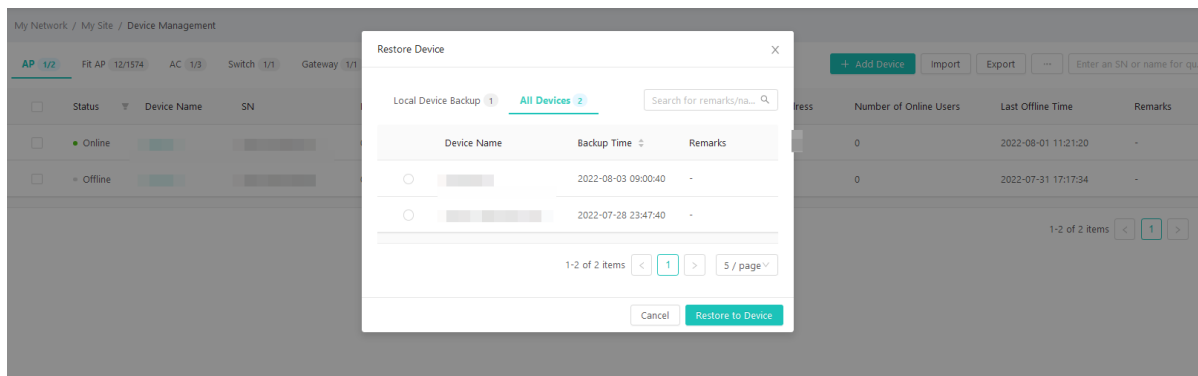


Figure 6-53 Restoring the Configuration from Backups in All Devices



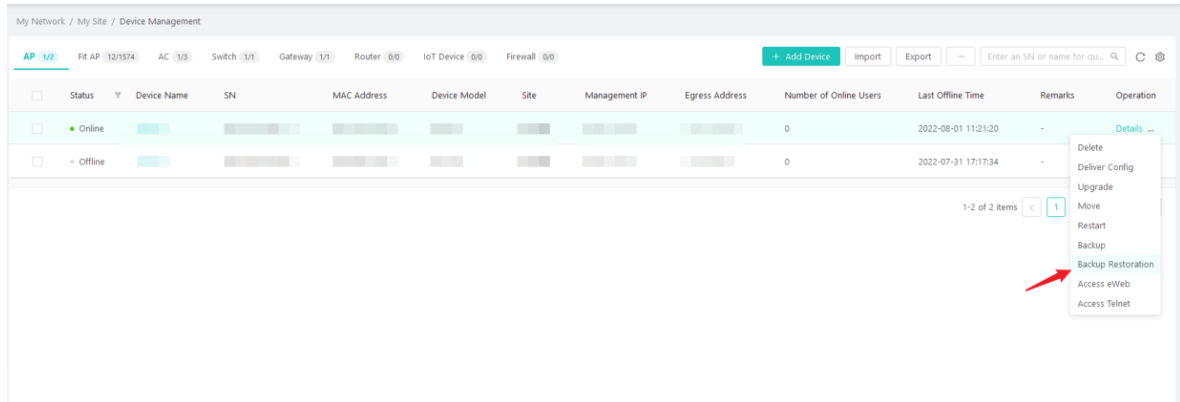
6.3.14 Accessing eWeb

Click ... in the device list and select **Access eWeb** for a device. The system creates a tunnel with the device and the Web management page of the device can be accessed through the tunnel. If the device is offline, the tunnel fails to be created.

Caution

The eWeb window may be blocked by the browser. Therefore, configure the browser to allow the eWeb window.

Figure 6-54 Accessing eWeb



If the current device does not support the eWeb tunnel, you need to create a tunnel through a transfer device that supports the eWeb tunnel.

Figure 6-55 Creating a Tunnel

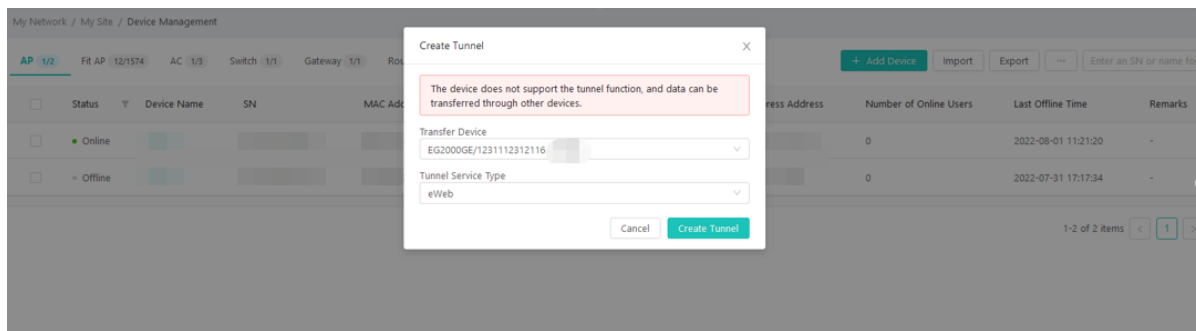
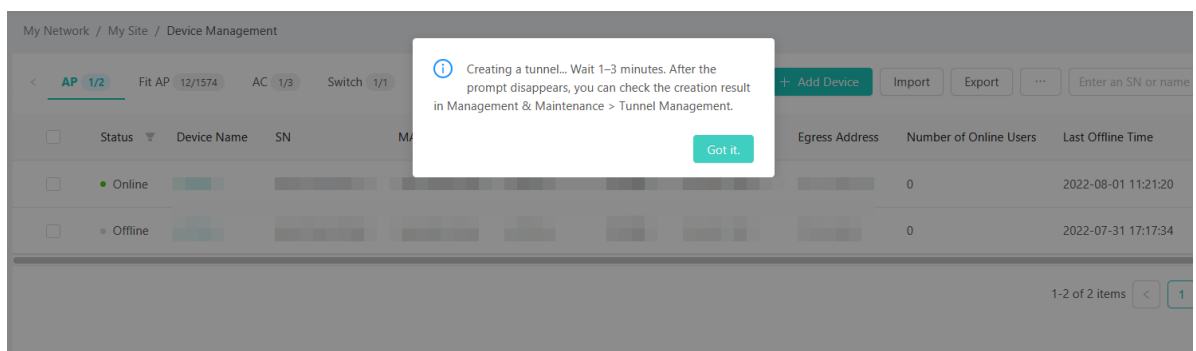
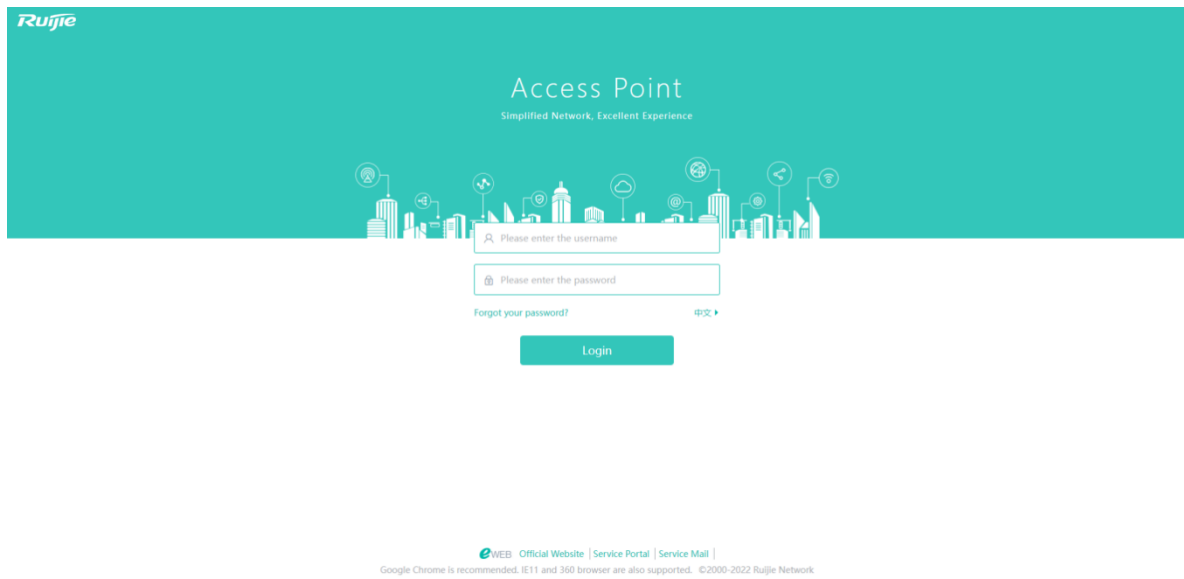


Figure 6-56 A Tunnel Is Being Created



After a tunnel is created successfully, the system automatically redirects to the eWeb login page.

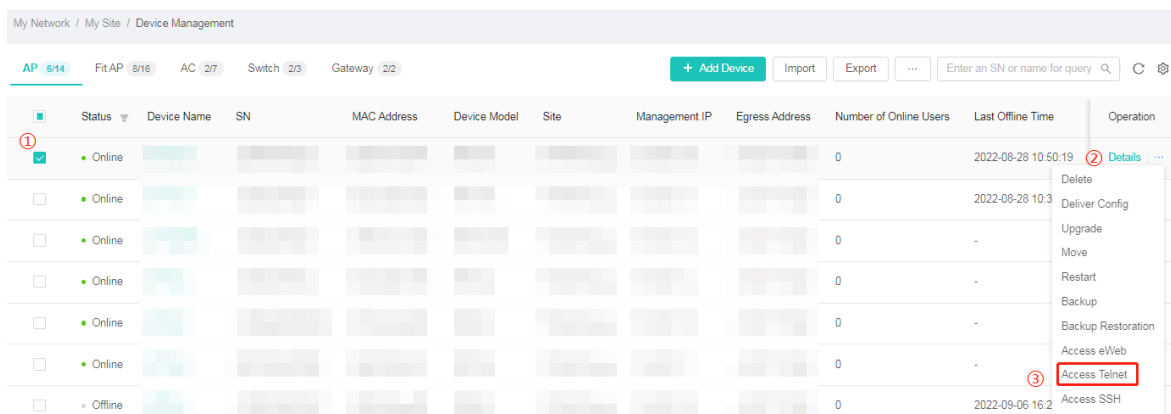
Figure 6-57 eWeb Login Page



6.3.15 Accessing Telnet

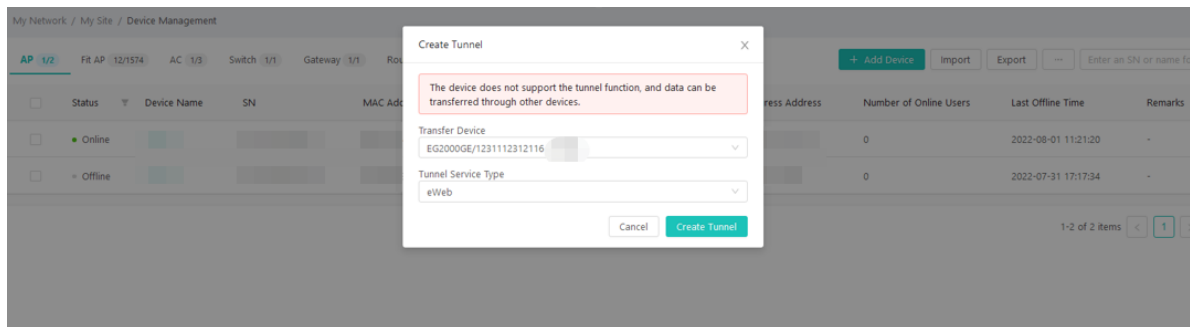
Click ... in the device list and select **Access Telnet** for a device. The system creates a tunnel with the device and the console of the device can be remotely accessed through the tunnel.

Figure 6-58 Accessing Telnet



If a device (such as AP or switch) does not support the telnet tunnel function, data needs to be transferred through other devices.


Figure 6-59 Creating a Telnet Tunnel



Parameters for the configuration transfer are described as follows:

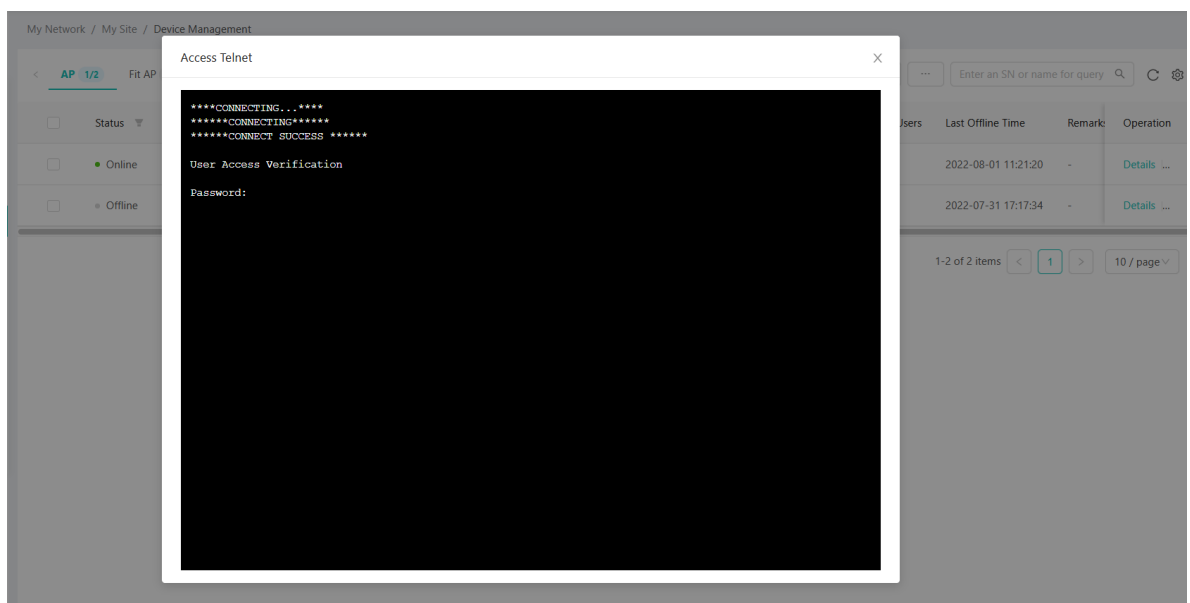
- **Transfer Device:** (Required) A transfer device transfers tunnel data. All types of devices except APs can serve as transfer devices.
- **Tunnel Service Type:** (Required) Specify the type of the tunnel to be created. It can be set to **eWeb** or Telnet.

Figure 6-60 A Tunnel Is Being Created

 Creating a tunnel... Wait 1–3 minutes. After the prompt disappears, you can check the creation result in Management & Maintenance > Tunnel Management.

Got it.

Figure 6-61 Accessing Telnet



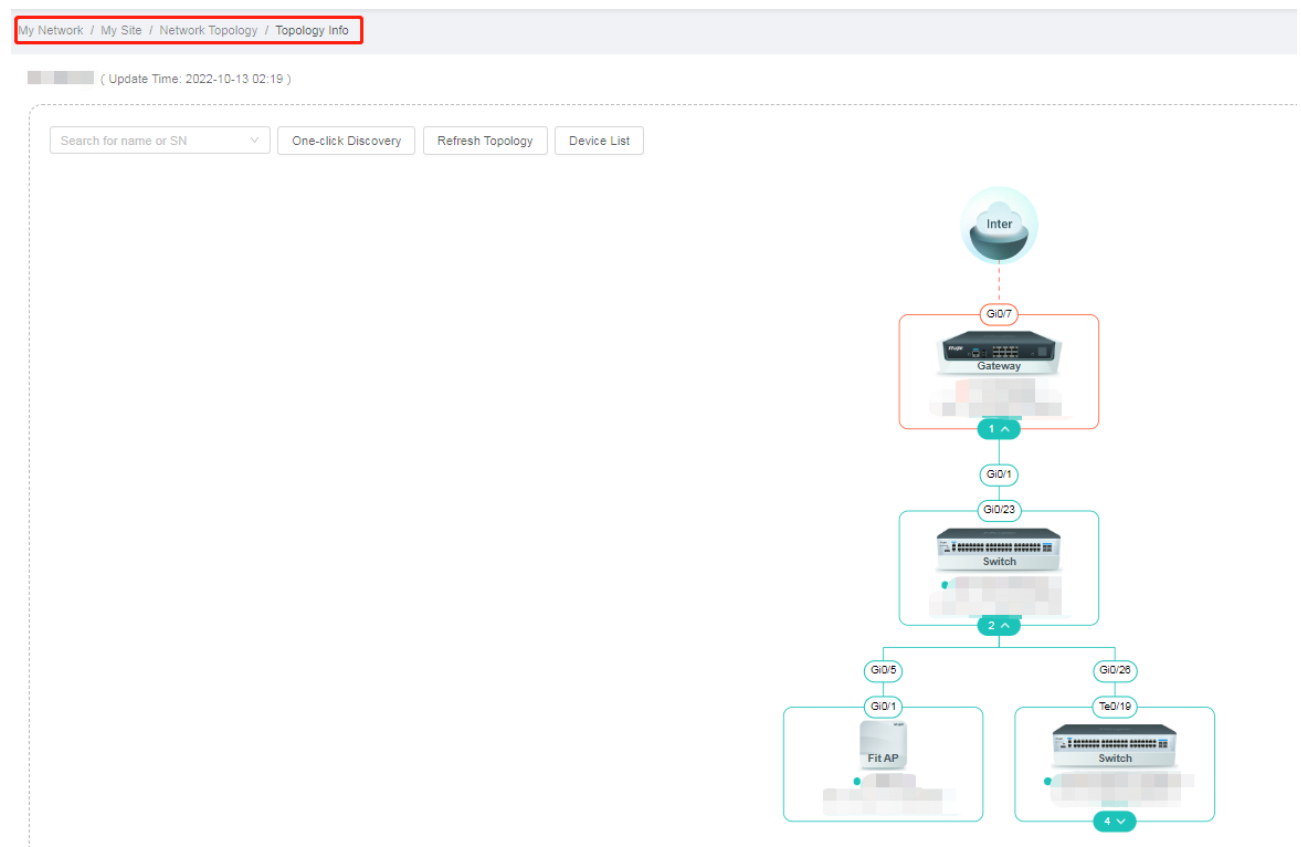
6.4 Network Topology

Choose **My Network > My Site > Network Topology** to view the topology of the current network. The system automatically generates the topology based on the actual network topology.

⚠ Caution

- (1) If there is no gateway or router on a network, the network topology function is unavailable.
- (2) If multiple gateways are added to a network, only one gateway is displayed in the topology.
- (3) If a switch is a third-party switch or is not managed by WIS Cloud Network, the system can only calculate the existence of the switch based on relationships between the switch and other devices, but cannot figure out the status and ports of a switch.
- (4) Devices that never go online are displayed in gray.

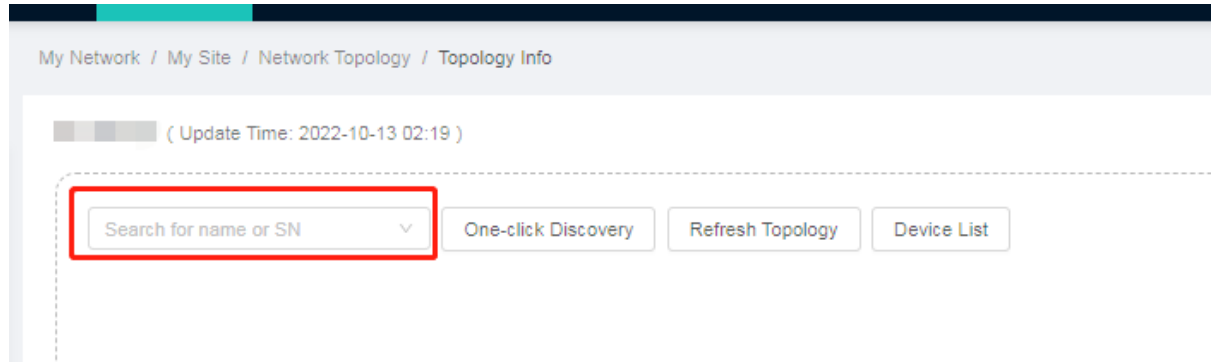
Figure 6-62 Network Topology



6.4.1 Device Query

You can search for a specified device by device name or device SN.

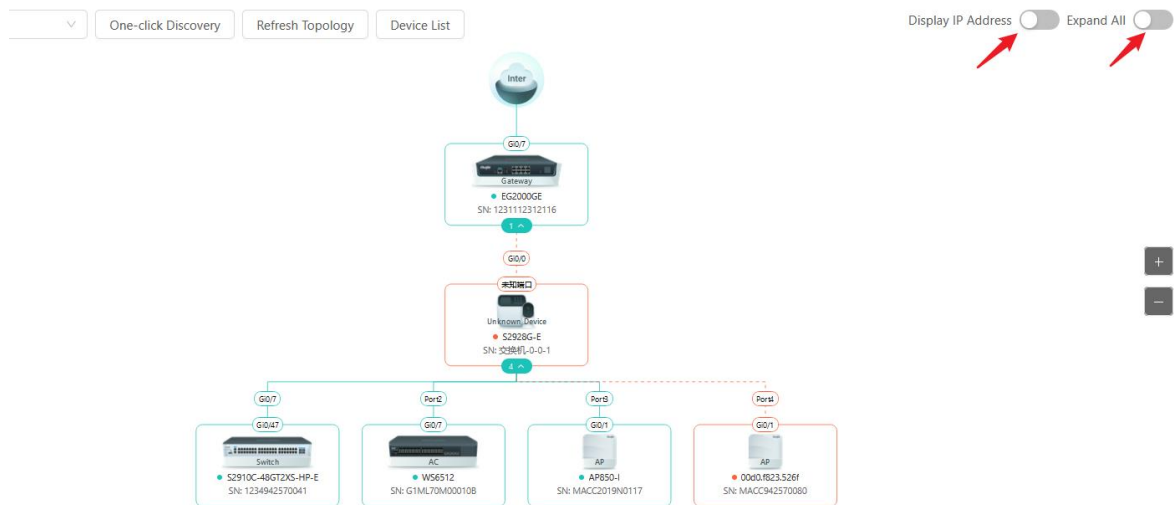
Figure 6-63 Searching for a Device



6.4.2 Topology View

- Turn on or off **Display IP Address** to display the IP addresses or SNs of devices in the topology. Device SNs are displayed by default.
- Turn on or off **Expand All** to expand or collapse branches under Level 3 in the topology.

Figure 6-64 Switching the Topology View



Click **One-click Discovery**. The system automatically detects information about devices in the topology, including the device name, device type, device model, IP address, MAC address, and SN. The detection is performed by the gateway or router. A device can be successfully detected only after it connects to the WIS. A device can be registered with WIS in two ways:

- Automatic registration: A detected Ruijie device (judged based on OUI) will automatically register with WIS.
- Manual registration: Non-Ruijie devices can be added to the network manually.

You can click **Device List** to view detection results.

Figure 6-65 One-click Discovery

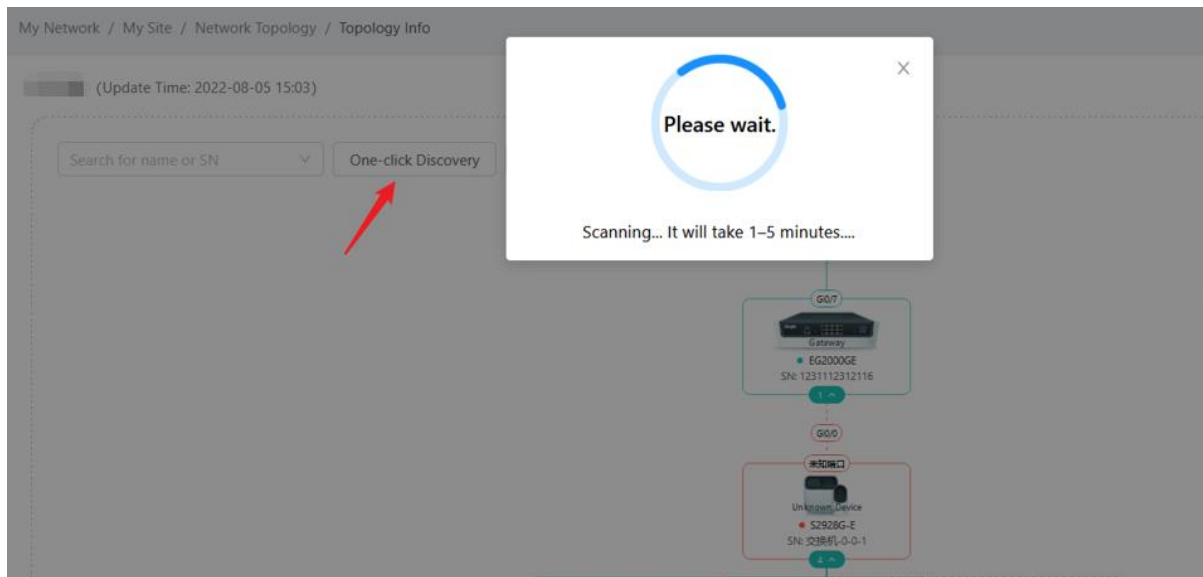
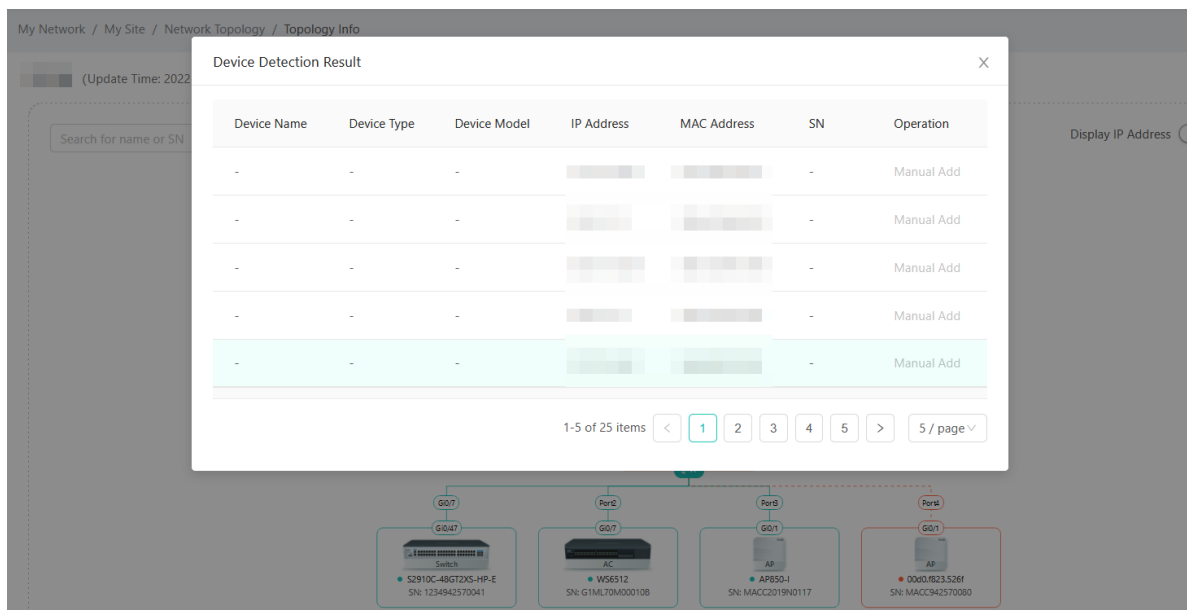
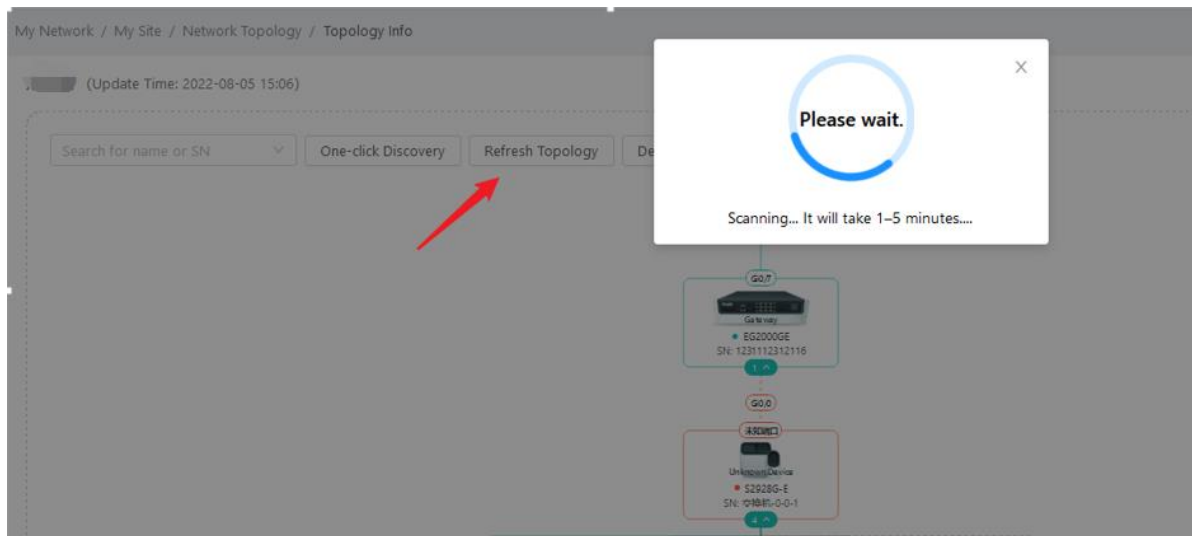


Figure 6-66 Detection Result



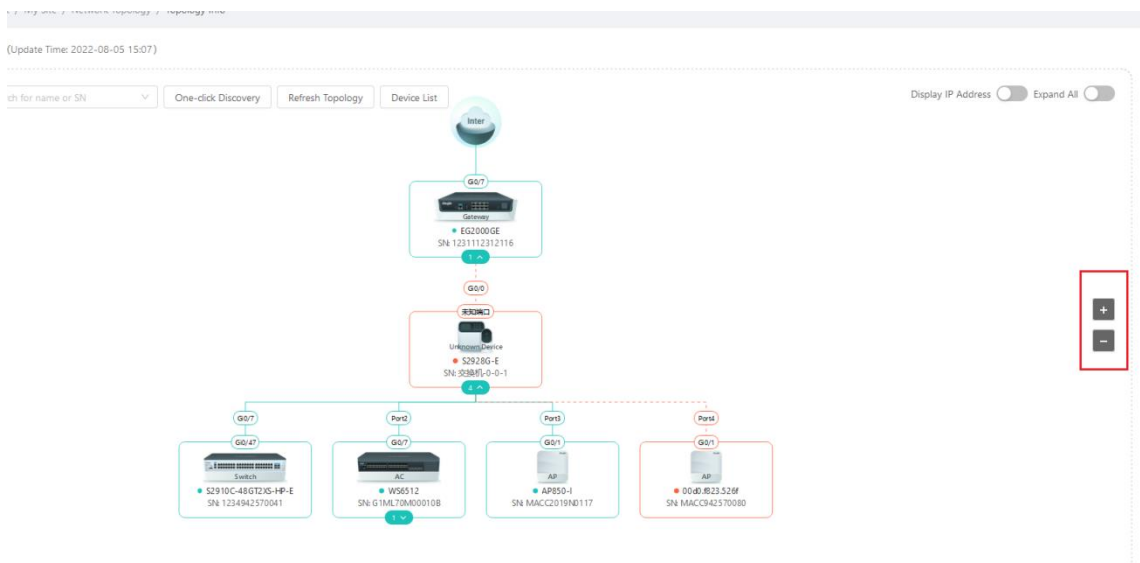
Click **Refresh Topology** to re-detect devices on the current network and generate the latest network topology. The time required for refreshing the topology depends on the device quantity and usually takes 1–5 minutes.

Figure 6-67 Refreshing the Topology



Click the zoom icon +/- or scroll the mouse wheel to zoom in/out the topology view.

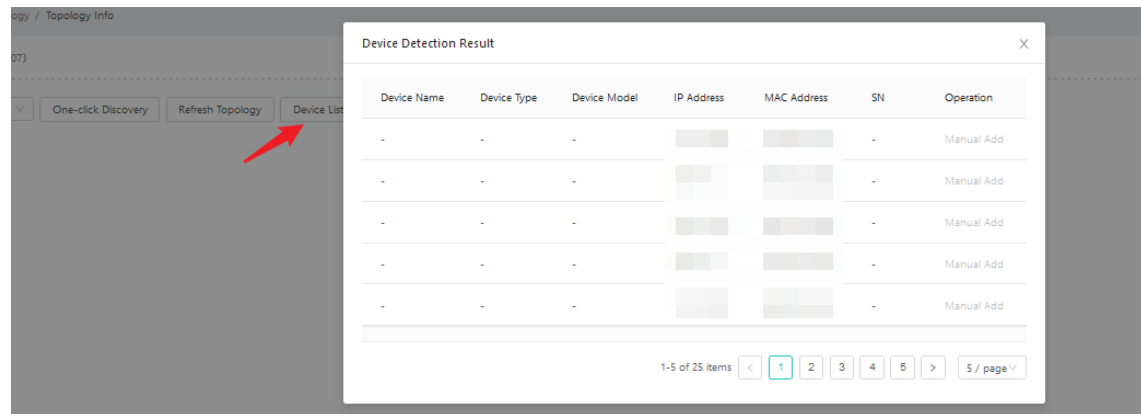
Figure 6-68 Zooming In/Out the Topology



6.4.3 Device List

You can click **Device List** to view a list of detected devices (last detection result).

Figure 6-69 Device List



6.4.4 Device Details

You can click a device in the topology to view its basic status and perform routine O&M configuration operations in the right pane.

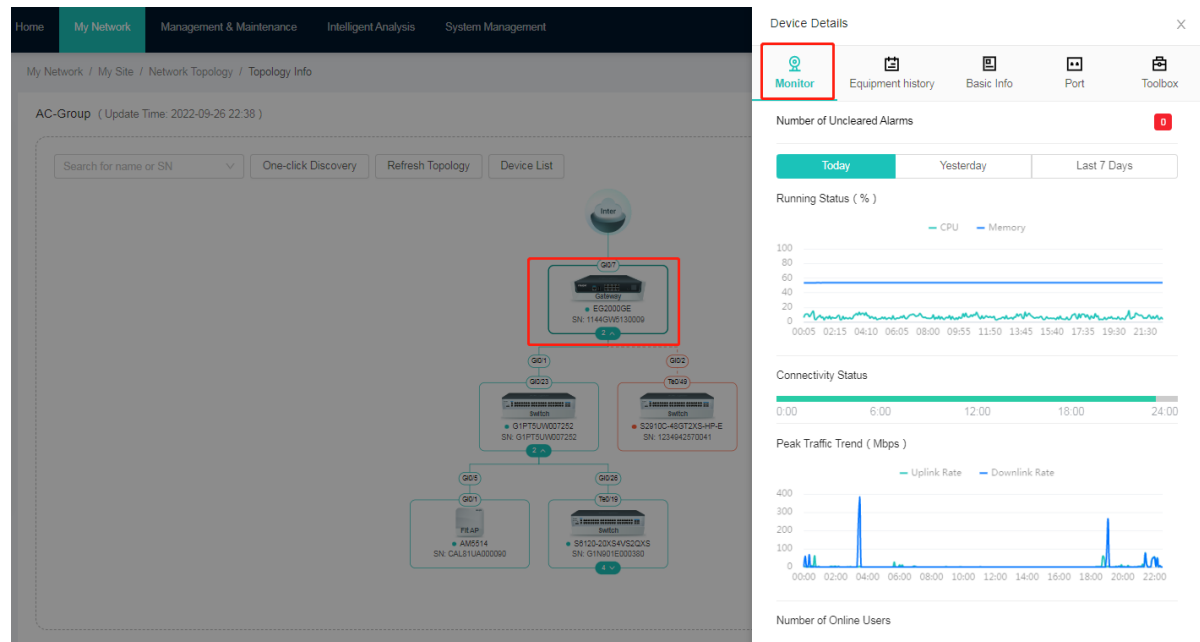
Caution

Items displayed on the **Device Details** page vary with devices. This section uses the details of a gateway as an example for description.

1. Monitor

Click a device in the topology. Network details of the device are displayed by default, including the number of uncleared alarms, running status, connectivity status, peak traffic trend, number of sessions, number of online users, Top10 app traffic, and Top10 user traffic.

Figure 6-70 Network Status Monitoring of a Device



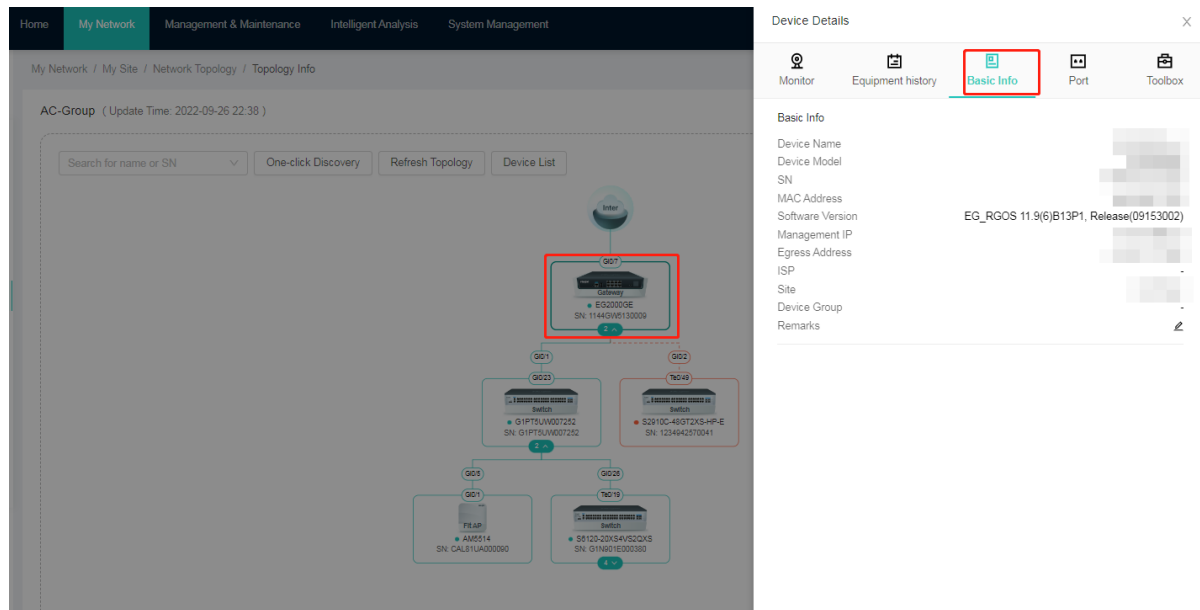
Parameters on the **Monitor** tab page of **Device Details** are described as follows:

- **Number of Uncleared Alarms:** Shows the number of uncleared alarms on the device. You can click the alarm quantity to go to the alarm management page.
- **Time:** You can switch the time bar to view network details in different periods. The time can be **Today**, **Yesterday**, or **Last 7 Days**.
- **Running Status (%):** Shows the CPU utilization and memory utilization, in percentage.
- **Connectivity Status:** Shows the connectivity status of the device in different periods.
- **Peak Traffic Trend (Mbps):** Shows the curve graph of peak traffic in different periods.
- **Number of Online Users:** Shows the number of currently online users served by the device.
- **Session Quantity:** Shows the number of valid session connections on the device.
- **App Traffic TOP10:** Shows the top 10 apps that occupy the most traffic.
- **User Traffic TOP10:** Shows the top 10 users who occupy the most traffic.

2. Basic Info

Click the second icon to switch to the **Basic Info** tab page. You can view basic information about the device, including the device name, model, MAC address, version, and IP address. You can modify the device name and remarks.

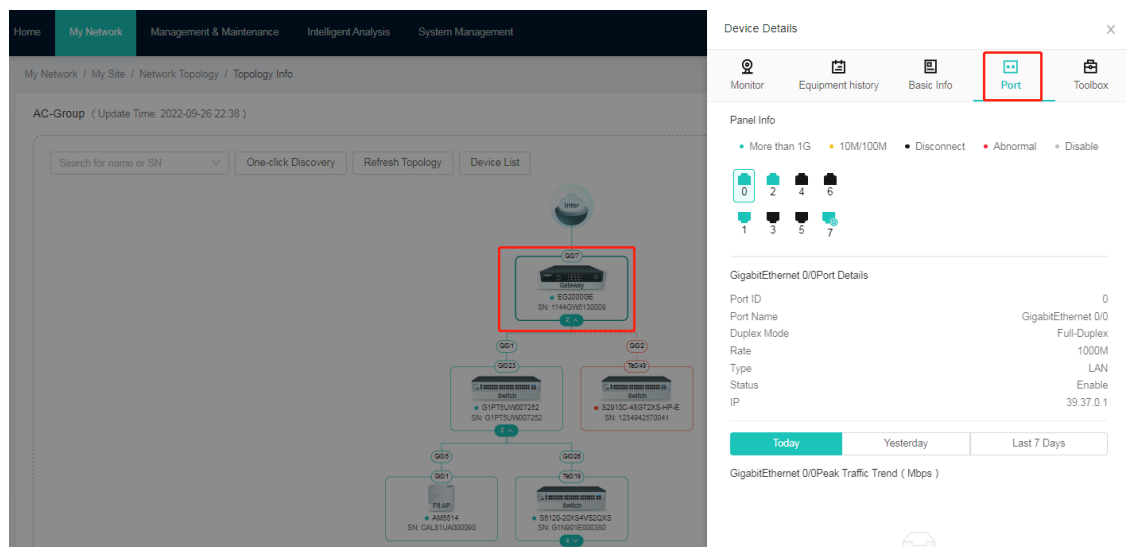
Figure 6-71 Basic Info



3. Panel Info

Click the third icon to switch to the **Port** tab page. You can view panel information, Ethernet port details, and port peak traffic trend of the device.

Figure 6-72 Panel Info



Panel information is described as follows:

- **Panel Info:** Shows the status of ports on the panel. Green indicates the port rate higher than 1 Gbps, yellow indicates the 10M/100M rate, black indicates that a port is disconnected, red indicates that a port malfunctions, and gray indicates that a port is disabled.

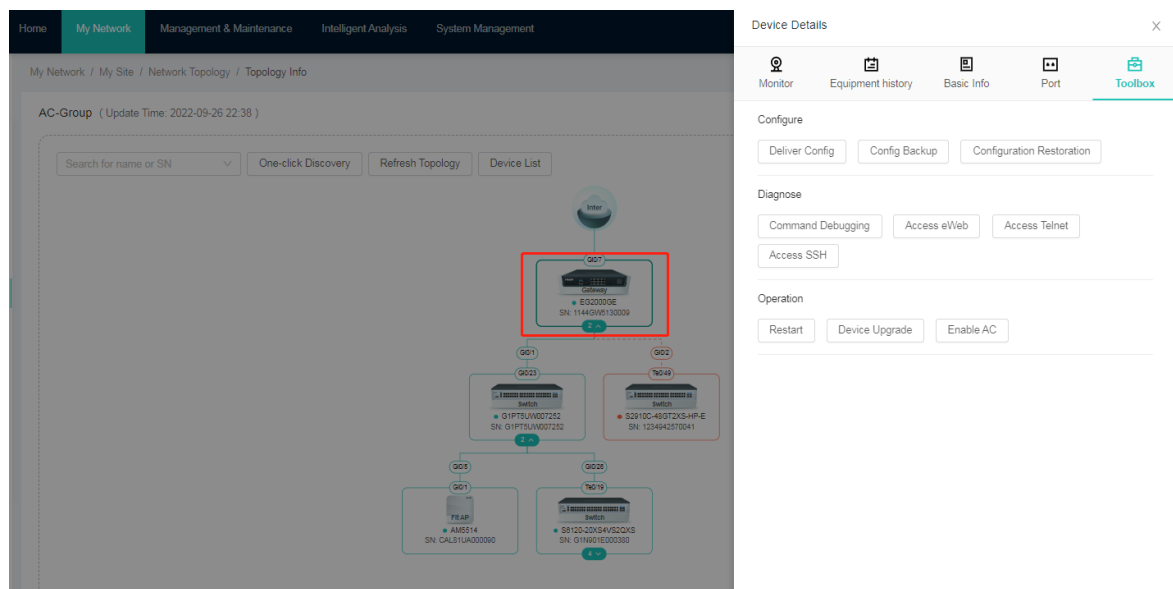
- **GigabitEthernet 0/0Port Details:** Shows details of the wired network port, including the port name, duplex mode, rate, port type, status, and IP address. On the panel information page of a switch, you can directly configure ports in port details.
- **GigabitEthernet 0/0Peak Traffic Trend (Mbps):** Shows the peak traffic curve graph of the port on the current day.

4. Toolbox

Click the **Toolbox** icon to configure, diagnose, and perform operations on the device.

- **Configure:** Includes **Deliver Config**, **Config Backup**, **Configuration Restoration**.
- **Diagnosis:** Includes **Command Debugging**, **Access eWeb**, and **Access Telnet**.
- **Operation:** Includes **Restart**, **Device Upgrade**, and **Enable AC**.

Figure 6-73 Toolbox



The functions of the tools are described as follows:

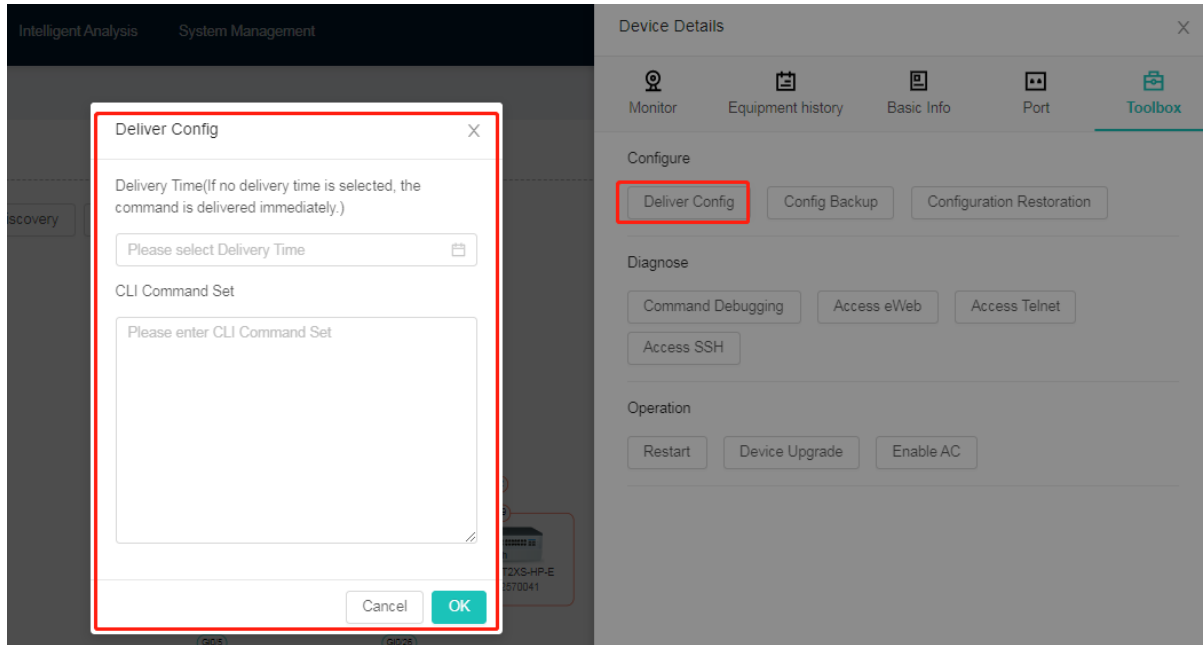
(1) Deliver Config

Click **Deliver Config**. Edit a CLI command set to be delivered, and specify the delivery time. If no delivery time is specified, commands are delivered immediately. After commands are successfully delivered, you can view the configuration execution in **Management & Maintenance > Configuration > Task**.

Note

Commands can be delivered successfully only when a device is online.

Figure 6-74 Delivering the Configuration



(2) Config Backup

Click **Config Backup** to back up all configurations of the current device.

Figure 6-75 Backing Up the Configuration

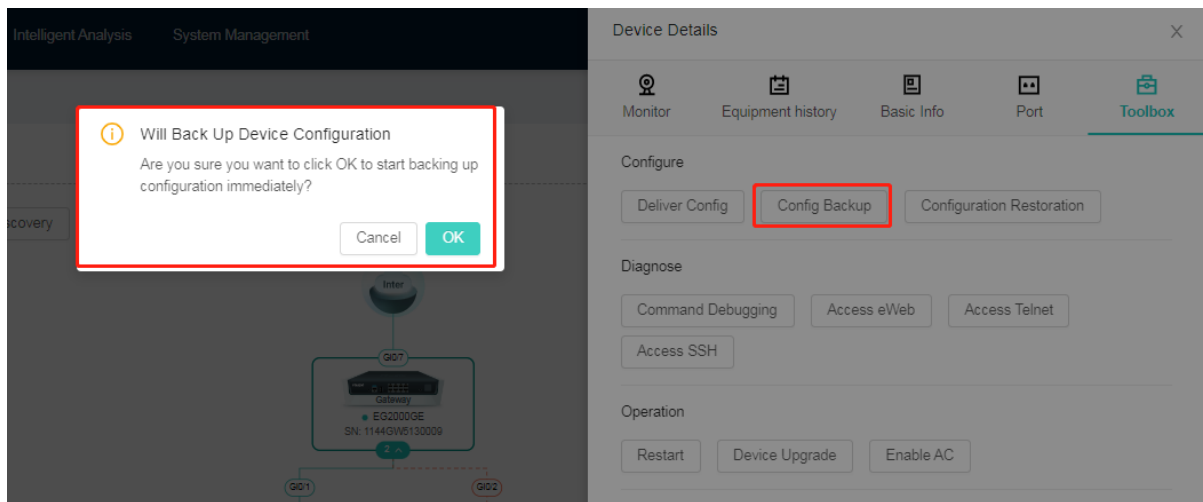
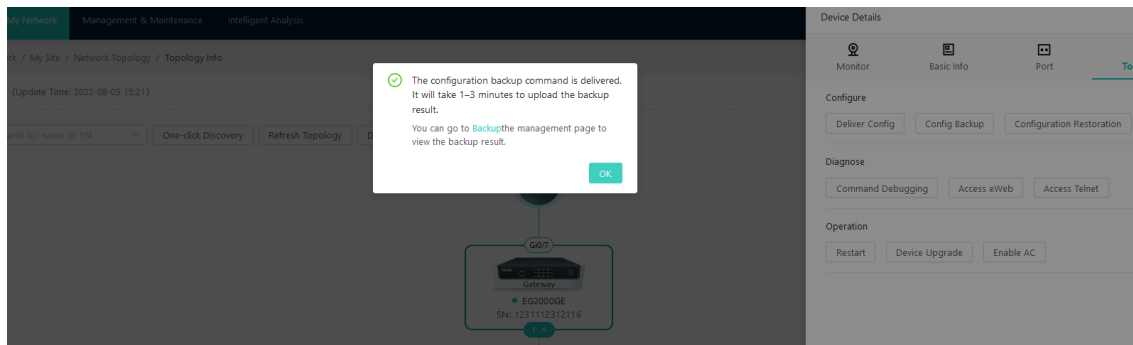


Figure 6-76 Successful Delivery of the Backup Command

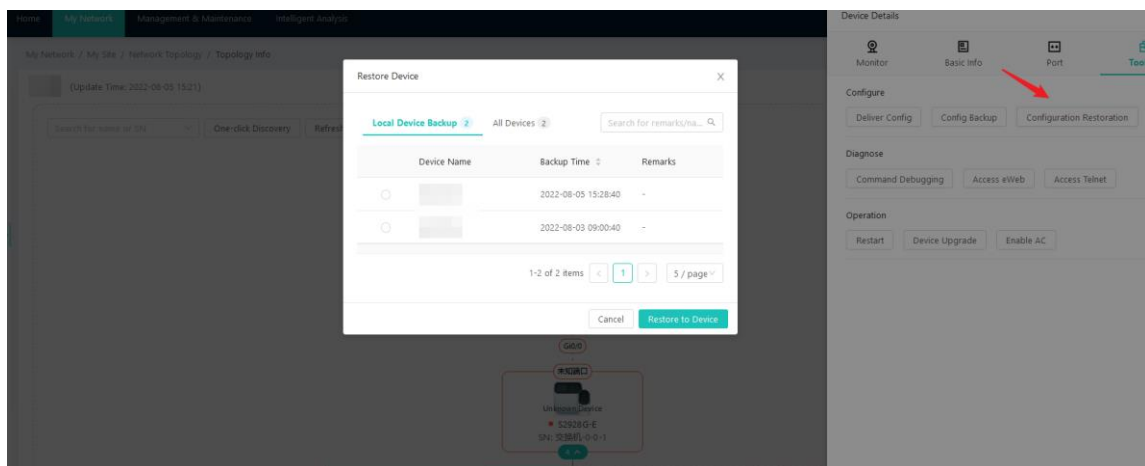


After the command is delivered, you can view the backup status of the device on the backup page. Click **Config Backup** in the pop-up box to redirect to the configuration backup management page and view the backup result.

(3) Configuration Restoration

Click **Configuration Restoration** to restore the required configuration from configuration backups. You can restore the configuration from configuration backups on the local device or restore the configuration from configuration backups on other similar devices to the local device. The backup list displays the name of the backed up device, backup time, and remarks. You can quickly identify different backups based on information in the backup list, and search for backups by remarks or device name. Select a specified backup and click **Restore to Device** to trigger the backup restoration.

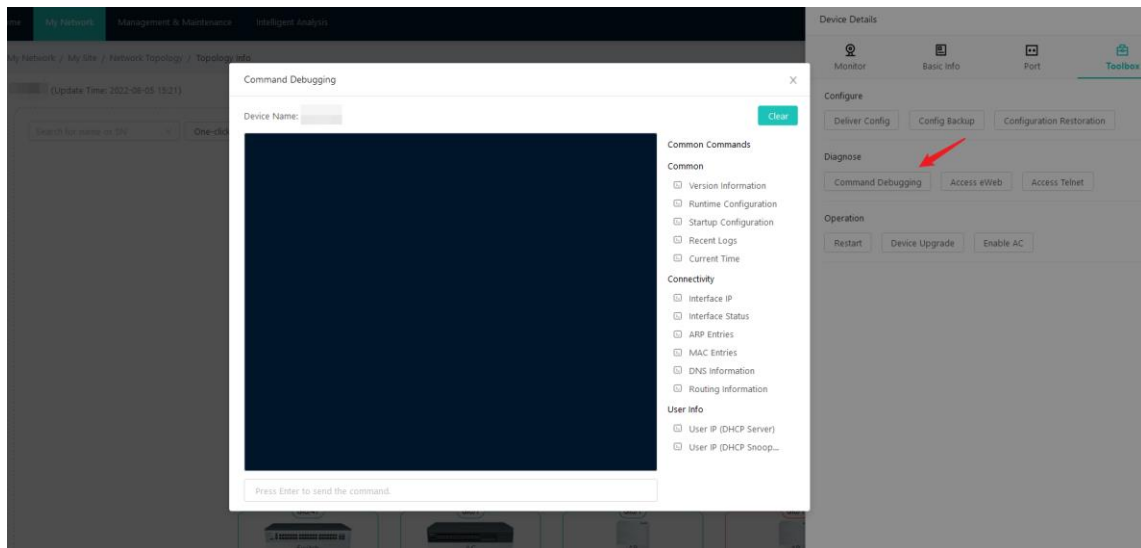
Figure 6-77 Restoring the Configuration



(4) Command Debugging

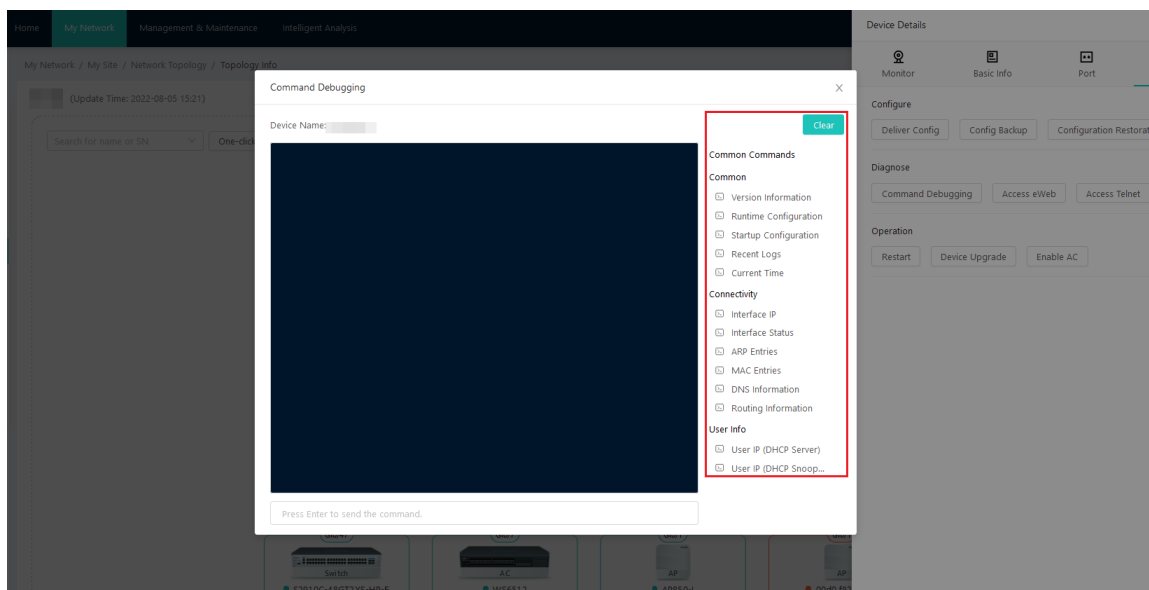
On the **Device Details** page, click the **Toolbox** tab and then click **Command Debugging** to go to the debugging window. Enter commands in the input box and press **Enter** to remotely debug a device. The command execution results are displayed in the black area shown in the figure.

Figure 6-78 Command Debugging



The command debugging window provides shortcut buttons for common commands, such as **Version Information**, **Runtime Configuration**, **ARP Entries**, **Routing Information**, and **User IP**. You can click a common command and view command output rapidly. Click **Clear** to clear information on the current screen.

Figure 6-79 Shortcut Common Commands

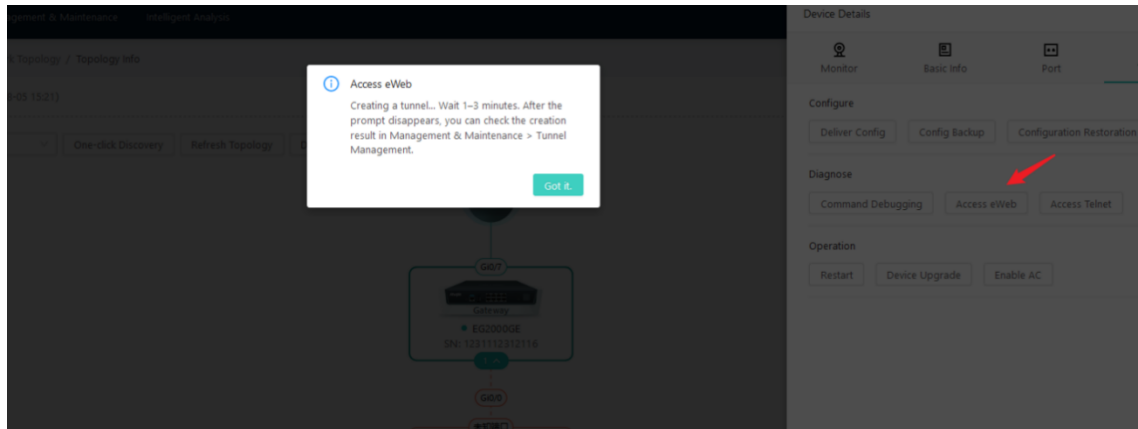


(5) Access eWeb

Click **Access eWeb**. The system creates a tunnel between the WIS and the eWeb of the device. If the device is offline, the tunnel fails to be created.

⚠ Caution

Some devices (such as APs and switches) do not support tunnel creation and a gateway is needed to transfer data. In this case, select a transfer device.

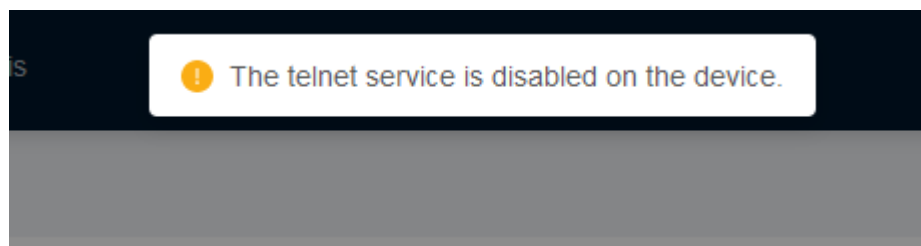
Figure 6-80 Accessing eWeb

After a tunnel is created successfully, the system automatically redirects to the eWeb login page of the device.

Figure 6-81 eWeb Login



Figure 6-82 Tunnel Creation Failure



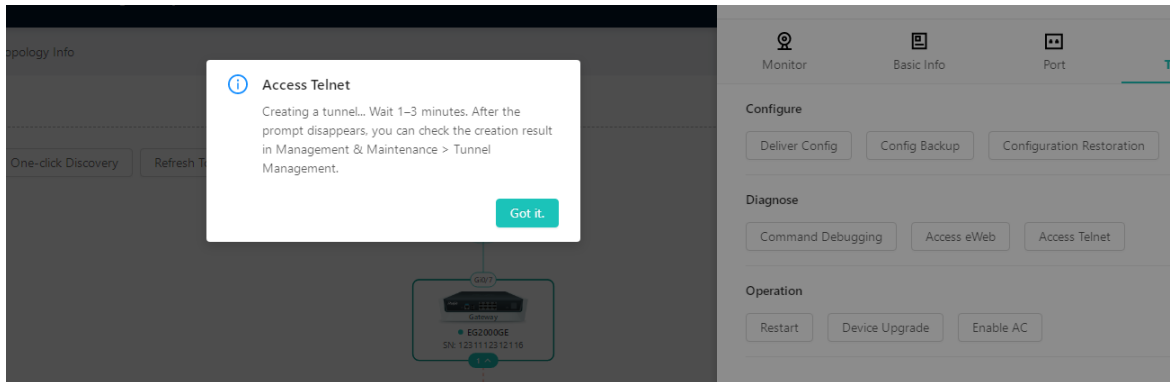
Click **View More** in the pop-up dialog box to view the cause for the tunnel creation failure on the tunnel management page.

(6) Access Telnet

Click **Access Telnet**. The system creates a telnet tunnel between the WIS and the device. If the device is offline, the tunnel fails to be created.

⚠ Caution

Some devices (such as APs and switches) do not support tunnel creation and a gateway is needed to transfer data. In this case, select a transfer device.

Figure 6-83 Accessing Telnet

The telnet page is displayed after a telnet tunnel is created successfully.

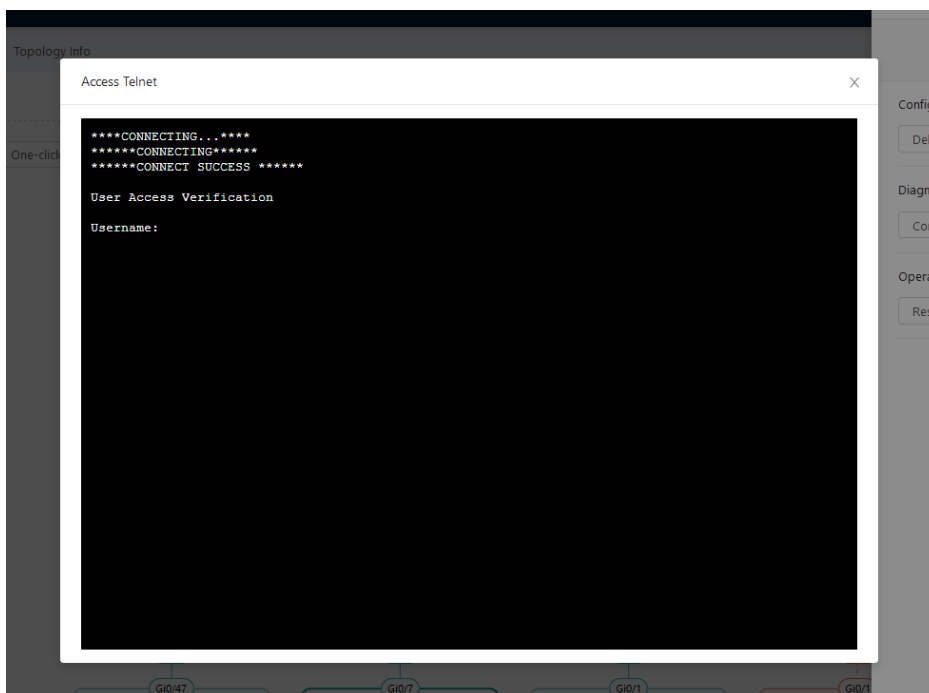
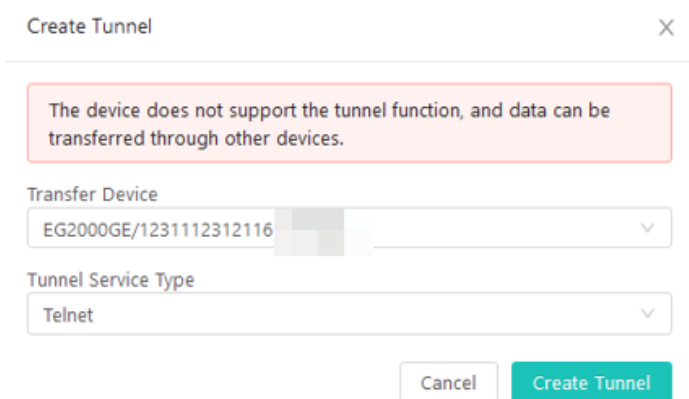
Figure 6-84 Telnet Tunnel Created Successfully

Figure 6-85 Telnet Tunnel Creation Failed

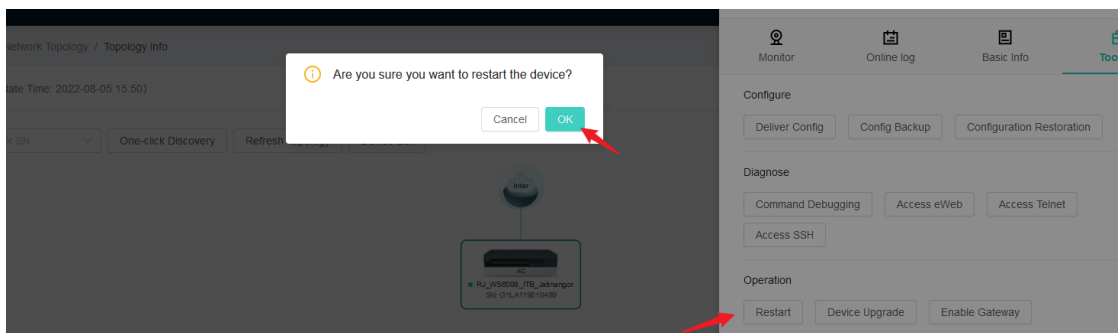


Click **View More** in the pop-up dialog box to view the cause for the tunnel creation failure on the tunnel management page.

(7) Restart

Click **Restart** to deliver the restart command to the current device. Perform this operation in a period, in which services are not affected. After the command is delivered, you can check the restart status on the device list page.

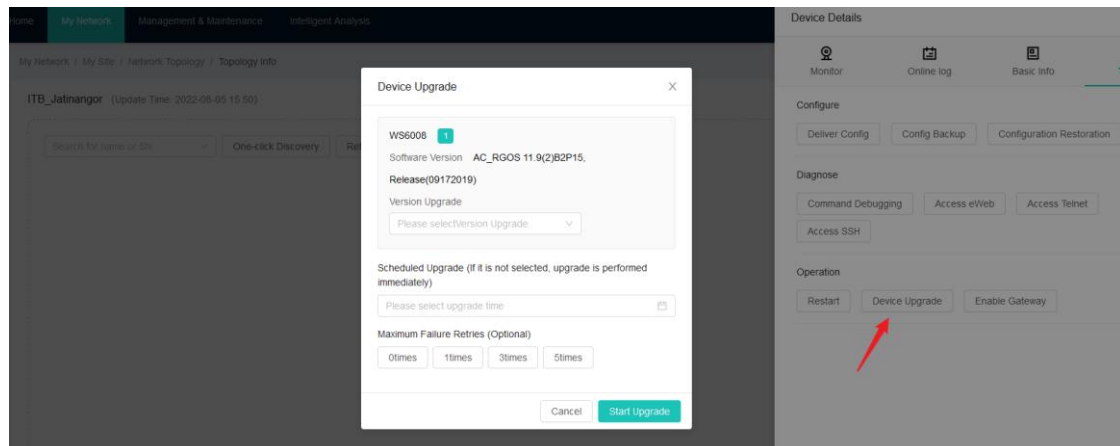
Figure 6-86 Restart



(8) Device Upgrade

Click **Device Upgrade** to configure an upgrade policy for the current device, including the upgrade target version, upgrade time, and upgrade failure retries. After an upgrade task is delivered, you can check the task information, upgrade status, and upgrade results in **Management & Maintenance > Device Upgrade > Upgrade Task**.

Figure 6-87 Device Upgrade



Configuration parameters are described as follows:

- **Version Upgrade:** (Required) Select the target version of the upgrade. You can upload the upgrade file on the **Version Management** page.
- **Scheduled Upgrade:** (Optional) Select the upgrade time. If the upgrade time is not specified, upgrade is performed immediately. No upgrade time is set by default.
- **Maximum Failure Retries:** (Optional) Set the maximum number of retries after an upgrade failure. The options include **0times**, **1times**, **3times**, and **5times**. No value is selected by default.

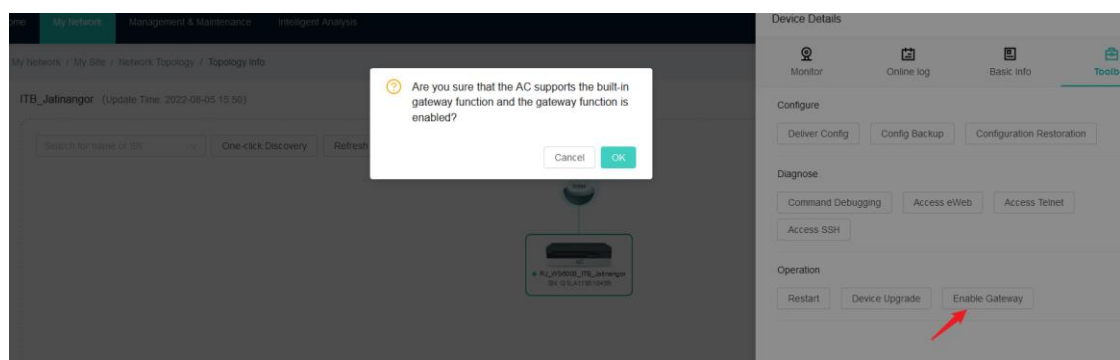
(9) Enable Gateway

Click **Enable Gateway** to enable the embedded AC function on the gateway.

Caution

This function can be enabled only on a gateway that supports the AC function.

Figure 6-88 Enable Gateway

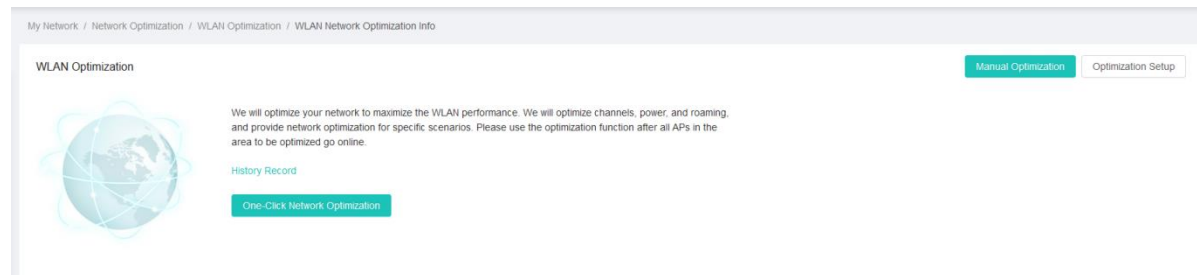


6.5 Network Optimization

6.5.1 WLAN Optimization

Choose **My Network > Network Optimization > WLAN Optimization** to optimize a WLAN.

Figure 6-89 WLAN Optimization



1. One-Click Network Optimization

Click **One-Click Network Optimization**. The WIS automatically adjusts the channel, power, roaming, and other WLAN parameters of devices by collecting air interface information obtained through AP scanning at the site, so as to maximize the WLAN performance.

Caution

- (1) Use this function only after all APs in the region to be optimized go online.
 - (2) During optimization, channel switching will occur on devices, which will bring users offline and affect user experience. Therefore, plan the network optimization execution period (you can click **Optimization Setup** to configure scheduled optimization execution time so that the system automatically executes network optimization when the specified time is up).
 - (3) The entire process takes about 15–30 minutes (depending on the device scale). After the process is complete, the system automatically switches to the **Network Optimization Details** page, which shows the channel and power configuration changes of each AP. A configuration task will be generated for delivery based on network optimization planning results. If there are a large number of devices, this process takes a period of time. You can filter tasks by radio optimization type on the **Configuration Task** menu to view the optimization result.
-

Figure 6-90 One-Click Network Optimization

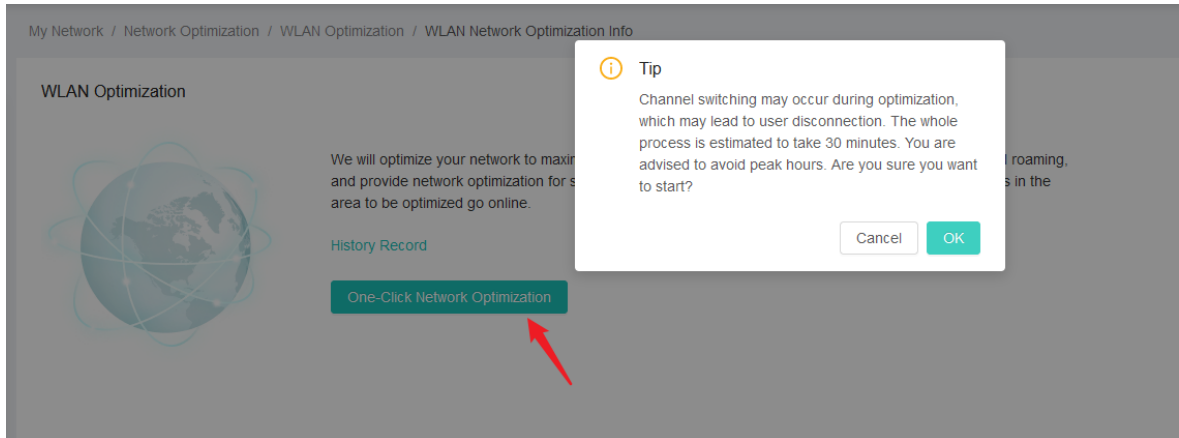


Figure 6-91 Network Optimization In Progress

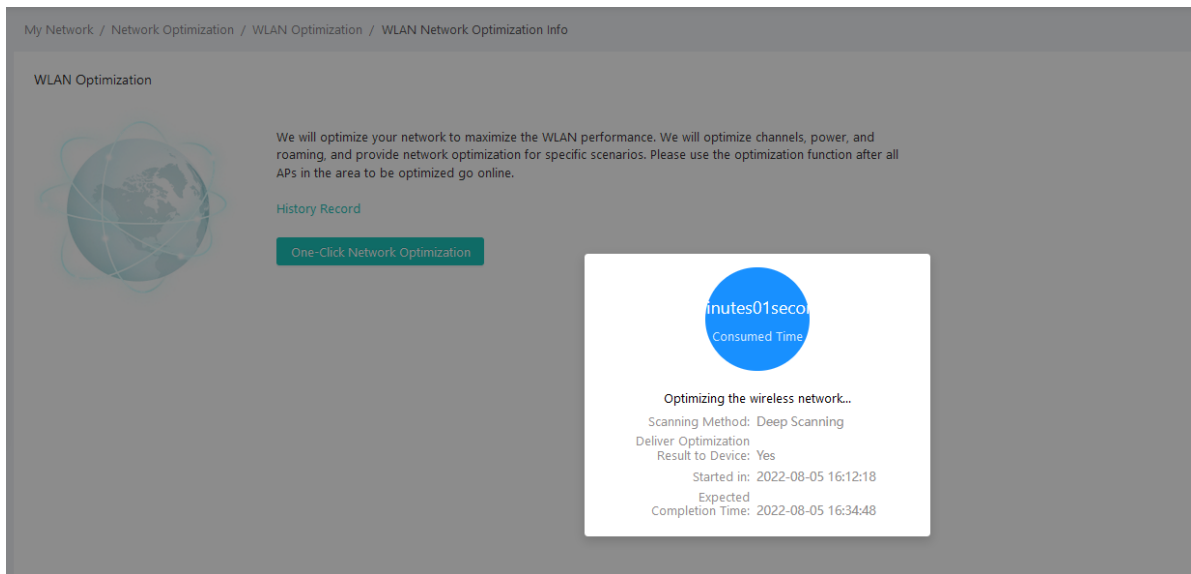


Figure 6-92 Network Optimization Details

My Network / Network Optimization / WLAN Optimization / Network Optimization Details

Network Optimization Details

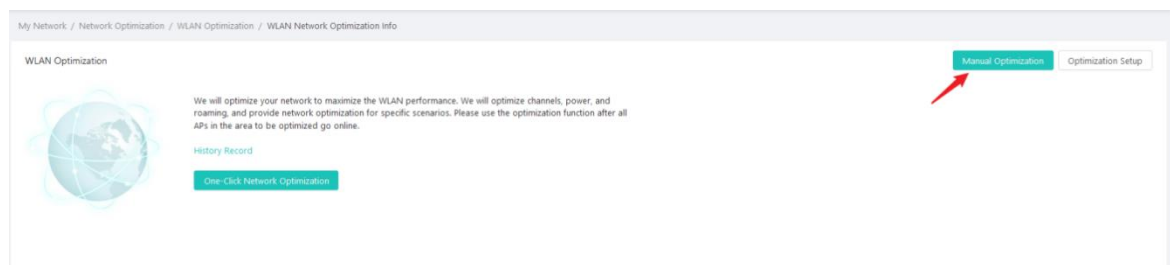
SN	Radio ID	RF Type	Device MAC Address	Current Channel	Recommended Channel	Channel Change	Current Power (%)	Recommended Power of Current	Recommended Power of Recomm
	1	2.4G		6	6	No Change	100	100	100
	2	5G		157	157	No Change	100	100	100
	3	5G		36	36	No Change	100	100	100
	1	2.4G		1	1	No Change	100	100	100
	2	5G		36	36	No Change	100	100	100
	3	5G		149	149	No Change	100	100	100

1-6 of 6 items < 1 > 10 / page

2. Manual Optimization

Click **Manual Optimization** to go to the **Manual Optimization** page.

Figure 6-93 Manual Optimization



In the manual optimization list, you can configure radio channels and radio power globally or for a single AP. Click **Apply to Device** to trigger the configuration delivery.

Figure 6-94 Manual Optimization List

My Network / Network Optimization / WLAN Optimization / Manual Optimization

Manual Optimization

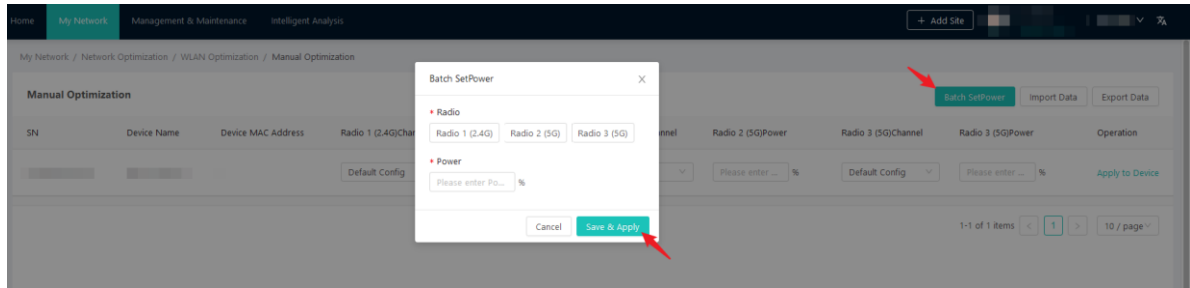
Batch SetPower Import Data Export Data

SN	Device Name	Device MAC Address	Radio 1 (2.4G)Channel	Radio 1 (2.4G)Power	Radio 2 (5G)Channel	Radio 2 (5G)Power	Radio 3 (5G)Channel	Radio 3 (5G)Power	Operation
			Default Config	Please enter ... %	Default Config	Please enter ... %	Default Config	Please enter ... %	Apply to Device

1-1 of 1 items < 1 > 10 / page

You can bulk set power for different radios of different devices.

Figure 6-95 Bulk Setting Power



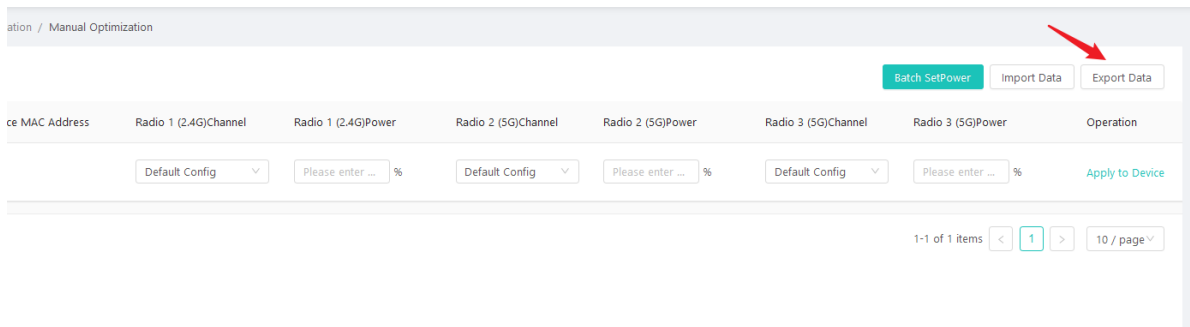
Batch power setting is based on radios and power needs to be set for radios separately. You can set the power of one radio at a time.

- **Radio:** (Required) Select the radio (such as Radio 1).
- **Power:** (Required) Enter the power percentage for a radio. The value is an integer in the range of 1 to 100.

You can bulk configure channels and power by importing a table. The procedure is as follows:

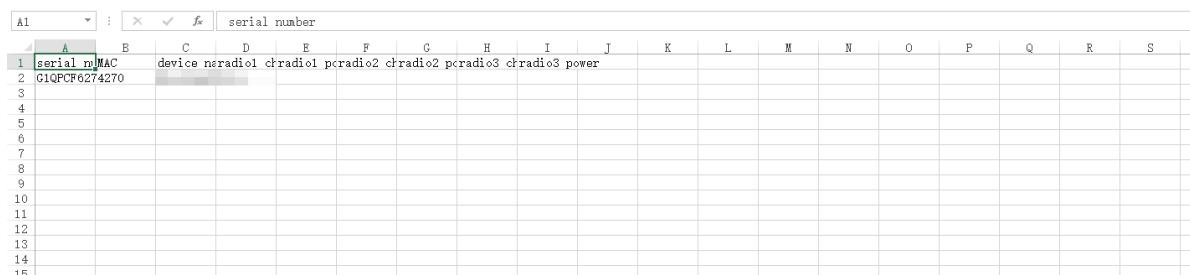
- (1) Click **Export Data** to export the current network optimization list.

Figure 6-96 Exporting Data



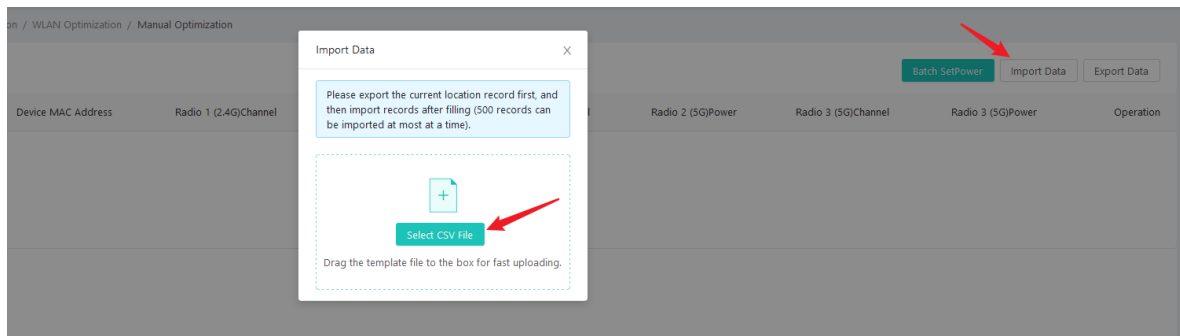
- (2) Open the exported table and fill in the channels and power of Radio 1 to Radio 3 in the table. The value ranges of channel and power are the same as those of channel and power on the manual optimization page.

Figure 6-97 Filling in the Form



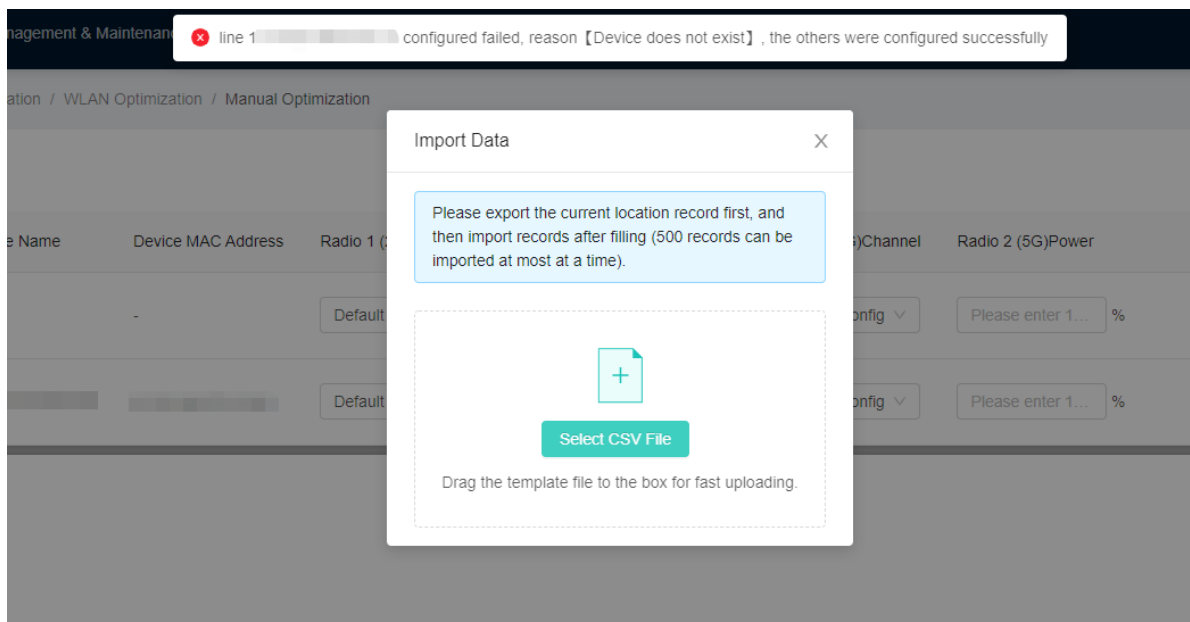
Click **Select CSV File**. Select the completed form to import it for network optimization. A maximum of 500 pieces of data can be imported at a time.

Figure 6-98 Importing Data



If a device is not managed by WIS Cloud Network or a device to be imported is offline, the network optimization fails.

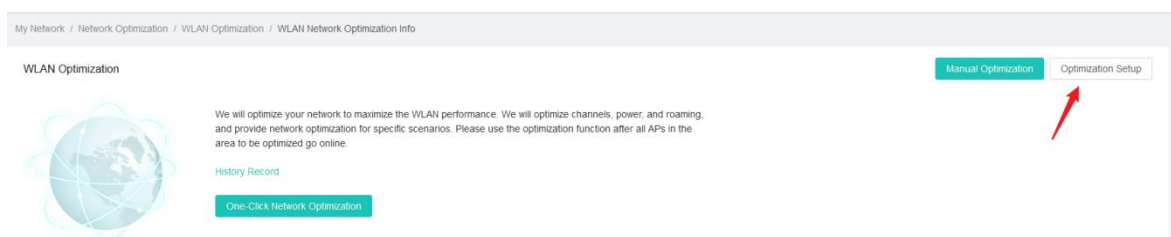
Figure 6-99 Network Optimization Failed



3. Optimization Setup

Click **Optimization Setup** to set network optimization parameters.

Figure 6-100 Optimization Setup



On the **Optimization Setup** page, you can customize channels, and configure scheduled network optimization tasks, synchronization policies, and radio parameters. Radios are automatically planned. By default, radios are planned based on the recommended channel of the selected country code or region code. 20 MHz is adopted for 2.4 GHz/5 GHz. In general, the default configuration is recommended and you do not need to configure channel customization. If 2.4 GHz/5 GHz uses other bandwidth or there are special requirements for candidate channels that are automatically planned, you can use **Channel Customization** to set candidate channels for automatic channel planning.

Figure 6-101 Customizing Network Optimization Parameters

My Network / Network Optimization / WLAN Optimization / Optimization Setup

Optimization Setup

Note: Radio frequencies are automatically planned. By default, radio frequencies are planned based on the recommended channel of the selected country code or region code. 20 MHz is adopted for 2.4 GHz/5 GHz. In general, the default configuration is recommended and you do not need to configure channel customization.
If 2.4 GHz/5 GHz uses other bandwidth or there are special requirements for candidate channels that are automatically planned, you can use Channel Customization to set candidate channels for automatic channel planning.

Channel Customization:

Scheduled Network Optimization:

Auto Delivery of Network Optimization Results to AP:

Configuration Type: Synchronize only Recommended... ▾

The system automatically allocates channels when a device goes online for the first time: When an AP goes online for the first time, if the 2.4G and 5G channels of the AP are the default channels 1 and 149, the WIS automatically configures channels according to the algorithm.

Radio Parameters

Country and Region: CHINA ▾

Default Bandwidth of Radio 1 (2.4 GHz): Please set... ▾

Default Bandwidth of Radio 2 (5 GHz): Please set... ▾

Default Bandwidth of Radio 3 (5 GHz): Please set... ▾

Save

Network optimization parameters are described as follows:

- **Channel Customization:** (Optional) It is disabled by default. You can define channels (including 2.4 GHz channel and 5 GHz channel) that can be allocated for network optimization.
- **Scheduled Network Optimization:** (Optional) It is disabled by default. You can define the network optimization execution time, accurate to hour. The task is a single task. You can set the time to Monday to Sunday, and time point to 00:00 to 23:00. Select the hour from the drop-down list.
- **Auto Delivery of Network Optimization Results to AP:** (Optional) It is enabled by default. If it is disabled, the configuration will not be delivered to APs after network optimization is completed.
- **Configuration Type:** (Required) Only recommended channel configuration is synchronized by default. The options include **Synchronize only Recommended Channel Config**, **Synchronize Recommended Channel Config and Recommended Power Config**, and **Synchronize Recommended Power Config in Current Channel**.
- **The system automatically allocates channels when a device goes online for the first time:** (Optional) The system allocates channels to new online APs in sequence. For example, common channels for 2.4 GHz are channels 1, 6, and 11, channel 6 is allocated to AP 1 after it goes online, and channel 11 is allocated to

AP 2 after it goes online.

- **Country and Region:** (Required) The default value is **CHINA**. To switch the country and region, select a value from the drop-down list.
- **Default Bandwidth of Radio 1 (2.4 GHz):** (Optional) Select the default bandwidth of Radio 1 (2.4 GHz) from the drop-down list. The available bandwidths include 20 MHz, 40 MHz, and 60 MHz.
- **Default Bandwidth of Radio 2 (5 GHz):** (Optional) Select the default bandwidth of Radio 2 (5 GHz) from the drop-down list. The available bandwidths include 20 MHz, 40 MHz, and 60 MHz.
- **Default Bandwidth of Radio 3 (5 GHz):** (Optional) Select the default bandwidth of Radio 3 (5 GHz) from the drop-down list. The available bandwidths include 20 MHz, 40 MHz, and 60 MHz.

4. History Record

Click **History Record** to check WLAN optimization execution records.

Figure 6-102 History Record

WLAN Optimization



We will optimize your network to maximize the WLAN performance. We will optimize channels, power, and roaming, and provide network optimization for specific scenarios. Please use the optimization function after all APs in the area to be optimized go online.

[History Record](#)

[One-Click Network Optimization](#)

The history record list displays the network optimization trigger time, update time, optimization execution status, whether to deliver configuration, whether optimization is a scheduled task, and execution result. You can filter history records by execution status, whether to deliver configuration, and whether optimization is a scheduled task.

Figure 6-103 History Record List

My Network / Network Optimization / WLAN Optimization / History Record						
History Record						
Trigger Time	Update Time	Status	Deliver Config	Schedule Task	Result	Operation
2022-08-05 16:14:48	2022-08-05 08:14:48	Failed	Yes	No	There is no online device in the group	View
2022-08-05 16:12:06	2022-08-05 08:12:06	Failed	Yes	No	There is no online device in the group	View

1-2 of 2 items < 1 > 10 / page ▼

In the history record list, click **View** in the **Operation** column for a history record to redirect to the **Network Optimization Details** page. The **Network Optimization Details** page displays the device SN, radio ID, RF type, device MAC address, channel parameters, and other information.

Figure 6-104 Network Optimization Details

My Network / Network Optimization / WLAN Optimization / Network Optimization Details

Network Optimization Details

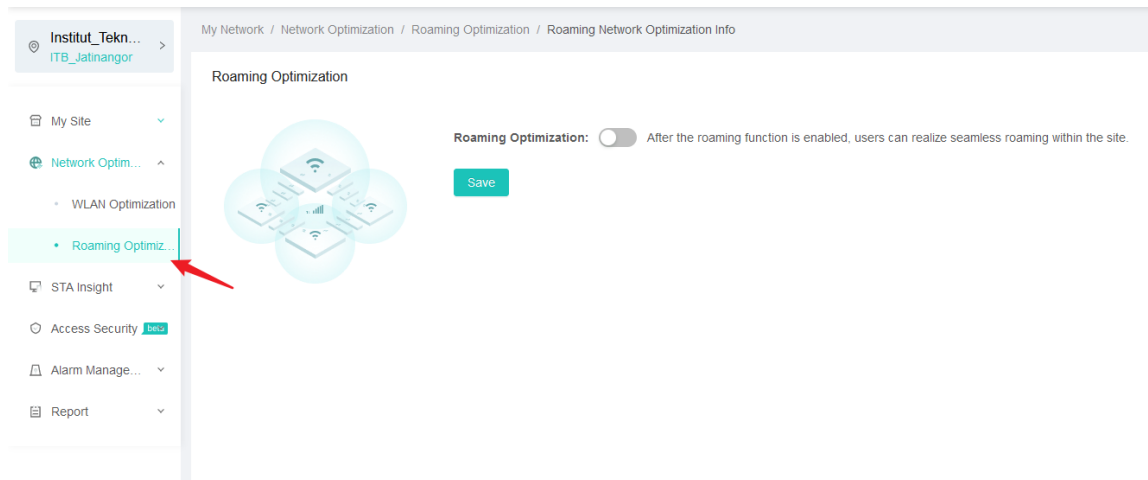
SN	Radio ID	RF Type	Device MAC Address	Current Channel	Recommended Channel	Channel Change	Current Power (%)	Recommended Power of Current	Recommended Power of Recomm
[blurred]	1	2.4G	[blurred]	6	6	No Change	100	100	100
[blurred]	2	5G	[blurred]	157	157	No Change	100	100	100
[blurred]	3	5G	[blurred]	36	36	No Change	100	100	100
[blurred]	1	2.4G	[blurred]	1	1	No Change	100	100	100
[blurred]	2	5G	[blurred]	36	36	No Change	100	100	100
[blurred]	3	5G	[blurred]	149	149	No Change	100	100	100

1-6 of 6 items < 1 > 10 / page

6.5.2 Roaming Optimization

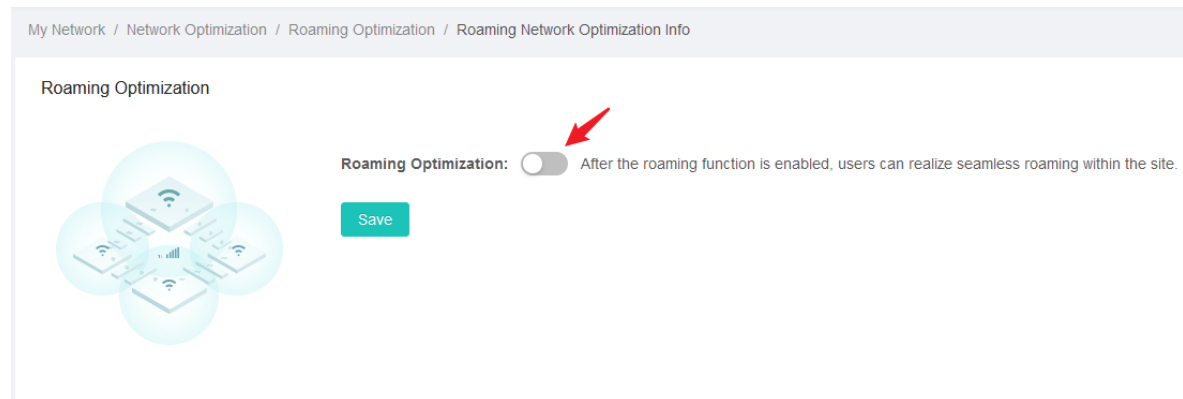
Choose **My Network > Network Optimization > Roaming Optimization** to configure roaming optimization.

Figure 6-105 Roaming Optimization



Click **Roaming Optimization** to perform roaming optimization, improve the roaming experience of wireless users, and implement seamless roaming for users at a site.

Figure 6-106 Enabling Roaming Optimization



Roaming optimization parameters are described as follows:

- **Auto Adjustment:** (Optional) It is enabled by default. After it is enabled, network optimization parameters are automatically adjusted to balance signal coverage and roaming optimization after each auto radio frequency planning.

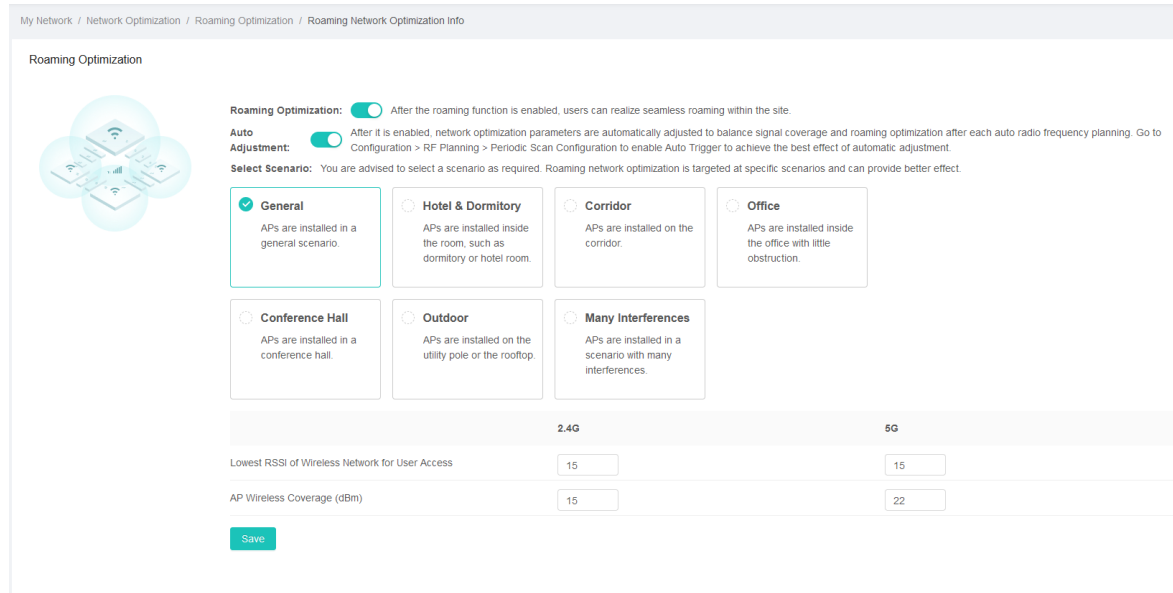
⚠ Caution

Auto adjustment takes effect only after **Auto Trigger** is enabled in **Configuration > RF Planning > Periodic Scan Configuration**.

- **Select Scenario:** (Required) The default scenario is **General**. You can select an appropriate scenario based on the actual site conditions and deliver preset roaming optimization parameters (access threshold and coverage) or manually adjust the parameters. Optional scenarios include the following:
 - **General:** Indoor APs are deployed in general scenarios such as teaching buildings and shopping malls.
 - **Hotel & Dormitory:** One AP is installed in one room to provide wireless services. Such scenarios include school dormitories, hotel rooms, and school office compartments.
 - **Corridor:** An AP is installed in the corridor outside a room, and the signal must cover the room or multiple rooms at the same time.
 - **Office:** In a large zone in an office, APs are visible to each other and high-density office and teaching services are carried out in this scenario.
 - **Conference Hall:** In a rapid deployment scenario, APs are densely deployed within a small distance, and are installed on the ceiling or under a seat.
 - **Outdoor:** APs need to be installed outdoors such as on the utility poles and rooftops, to cover plazas and roads.
 - **Many Interferences:** There are many interference signals around an AP, such as operator network signals and other companies' wireless AP signals.
- **Lowest RSSI of Wireless Network for User Access:** (Required) The default value varies according to scenarios. You can set the minimum RSSIs for the 2.4G and 5G channels. The value range is from 1 to 30.
- **AP Wireless Coverage:** (Required) The unit is dBm. The default value varies according to scenarios. You

can set the wireless network coverage scopes for the 2.4G and 5G channels. The value range is from 1 to 32.

Figure 6-107 Configuring Roaming Optimization



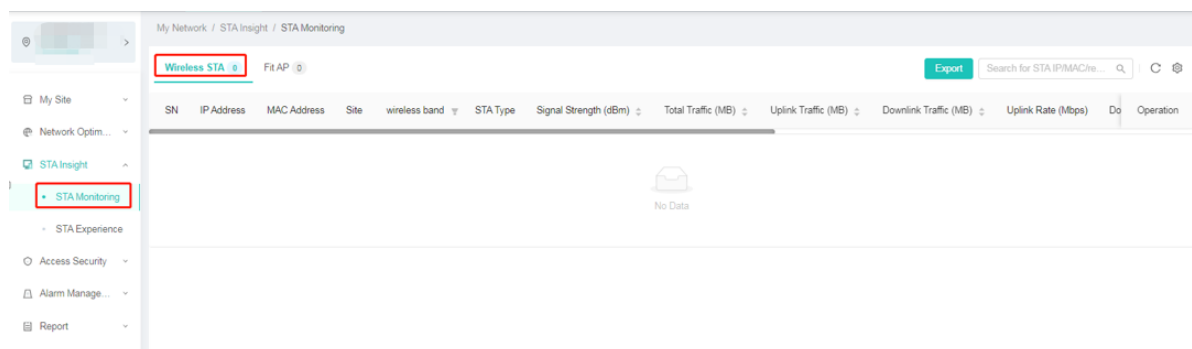
6.6 STA Insight

6.6.1 STA Monitoring

Choose **My Network > STA Insight > STA Monitoring** to go to the STA list. You can click a required tab page to view information about different types of STAs. The list allows you to set the number of items to be displayed on each page. You can search for STAs by STA IP address, MAC address, remarks, and status, define fields to be displayed, and manually refresh the list.

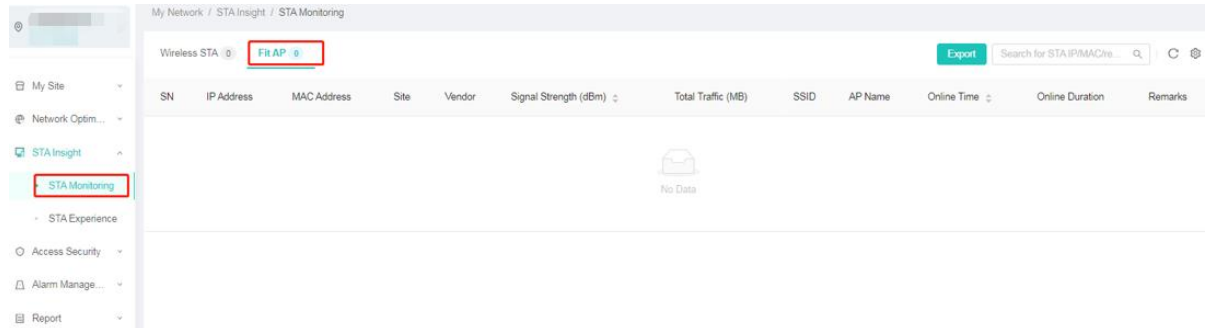
The cloud AP list displays the STA type, MAC address, STA signal, network indicators, AP name, and online duration.

Figure 6-108 Wireless STA List



The fit AP list displays the IP address, MAC address, vendor, signal strength, total traffic, SSID, AP name, online time, online duration, and other information.

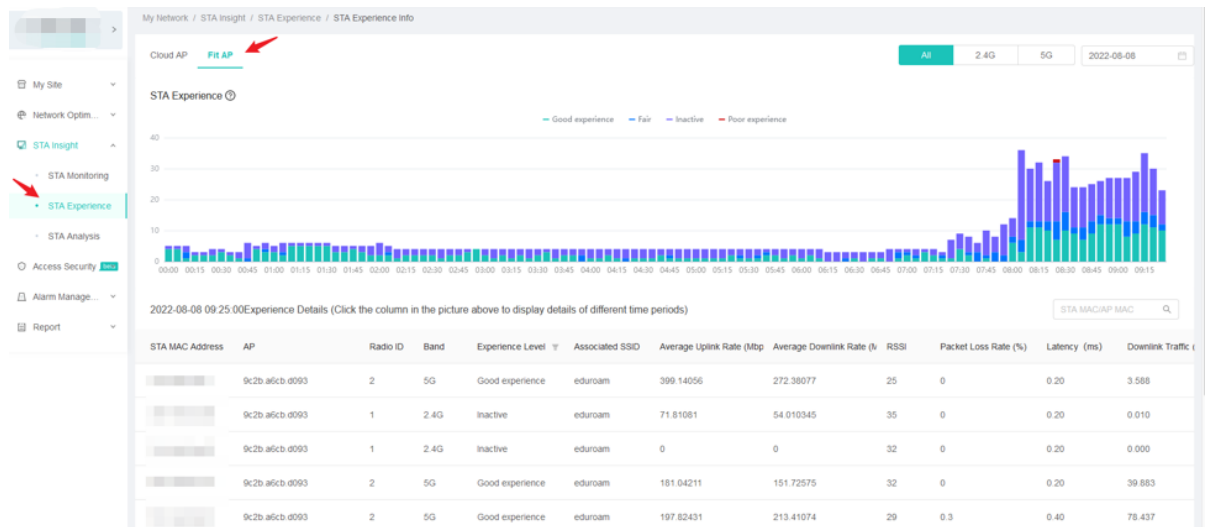
Figure 6-109 Fit AP List



6.6.2 STA Experience

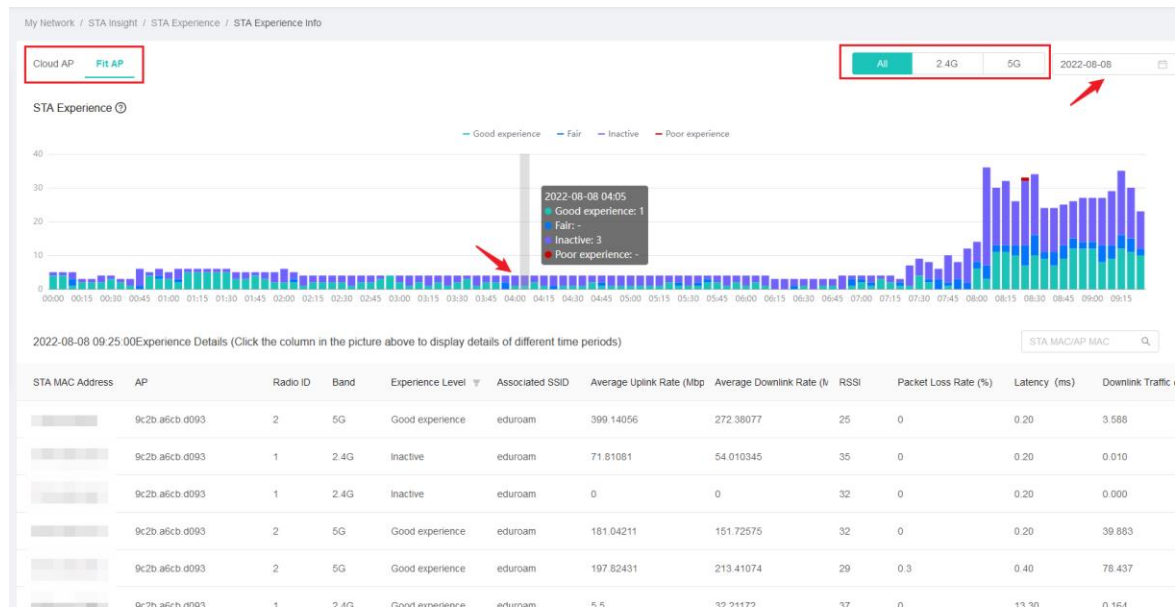
Choose **My Network > STA Insight > STA Experience** to go to the STA experience statistics page. This page displays STA experience in a bar graph and lists the STA rate, signal, packet loss rate, and other network experience indicators.

Figure 6-110 STA Experience



You can switch the tab page to view experience information of cloud APs and fit APs. The bar graph allows you to view the experience graph of all STAs, 2.4 GHz STAs, or 5 GHz STAs, as well as data of a specified date. The statistics interval is 5 minutes. You can hover the cursor over the graph to view the number of STAs at different experience levels at a specified time point.

Figure 6-111 STA Experience Bar Graph

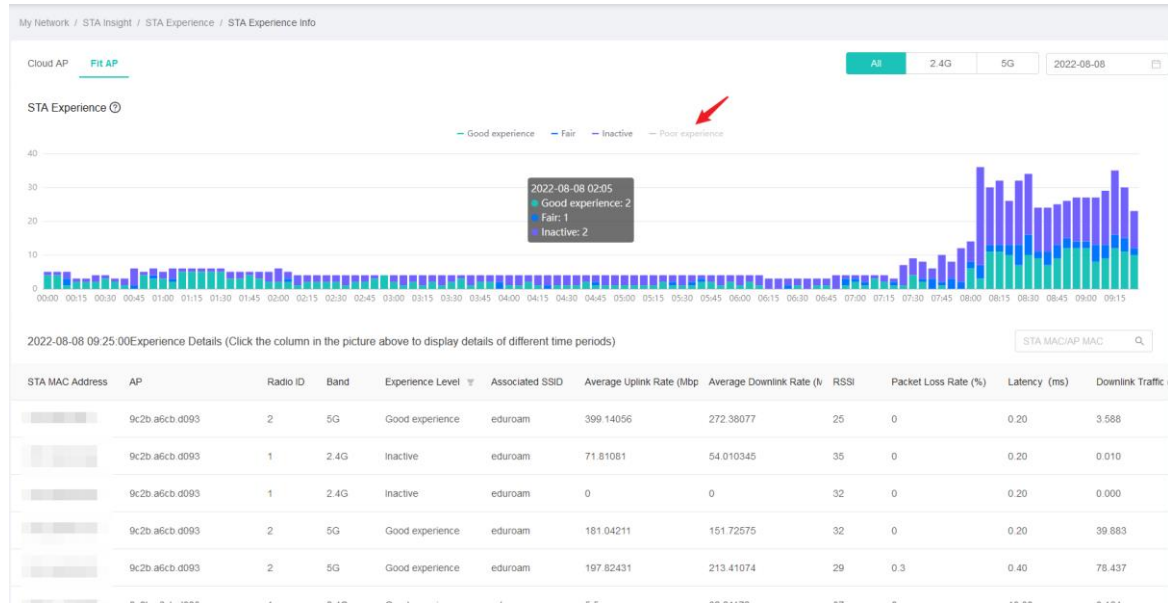


There are four levels of STA experience: inactive, fair, poor experience, good experience, which are described as follows:

- **Good experience:** HD videos and games can be played smoothly.
- **Fair:** WeChat, Web pages, and VoIP can be used normally.
- **Poor experience:** The network disaster area provides poor Internet access experience.
- **Inactive:** The experience is evaluated based on the STA traffic and power saving status.

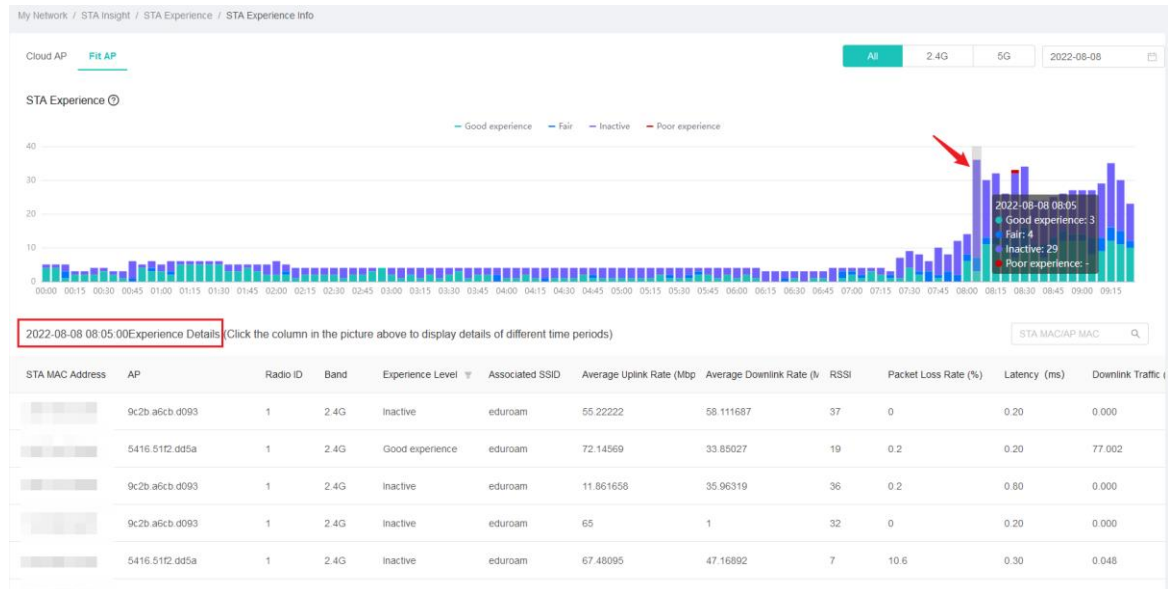
STAs support hiding/displaying data of a specified experience level. You can click the color icon of an experience level to control the display/hiding of data of a specified experience level. By default, data of all levels is displayed.

Figure 6-112 Hiding Data of the Poor Experience Level



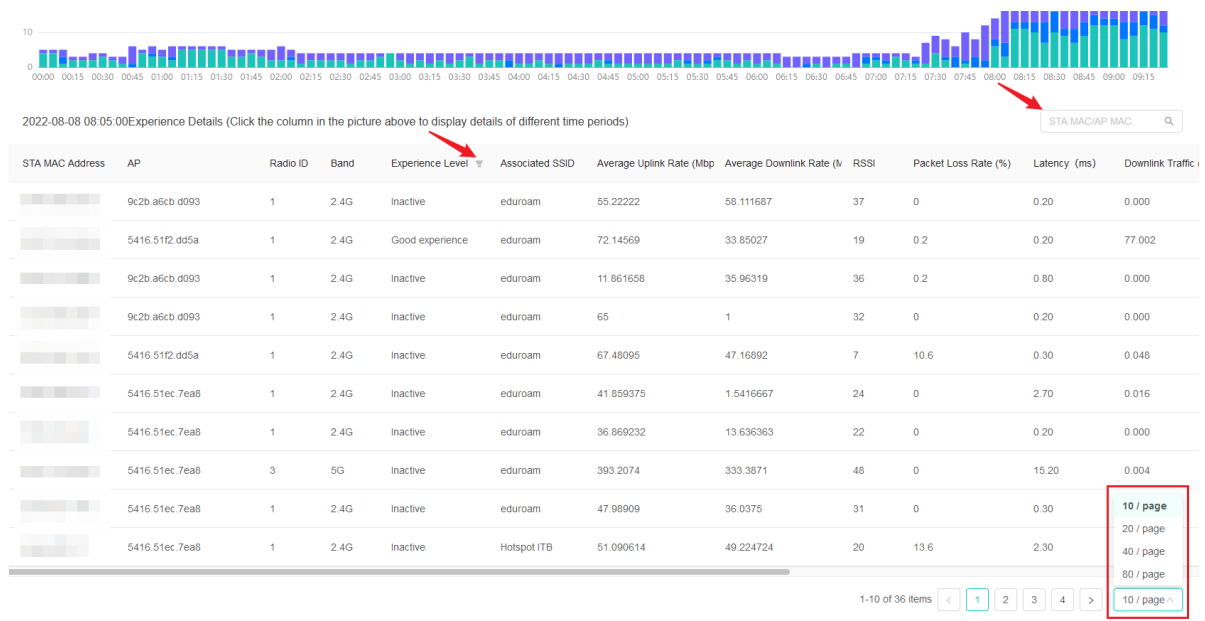
The list in the lower part provides experience details. You can click any time point in the bar graph to view experience details at the specified time point. The experience details list displays the STA MAC address, AP, band, uplink and downlink rates, RSSI, packet loss rate, and channel utilization. You can move the horizontal scroll bar to view the details.

Figure 6-113 Experience Details List



In the experience details list, you can search for STAs by STA MAC address, AP MAC address, and experience level, and define the number of STA items to be displayed on each page.

Figure 6-114 STA Search and Display



6.7 Access Security

6.7.1 Authentication Configuration

1. One-Click Login

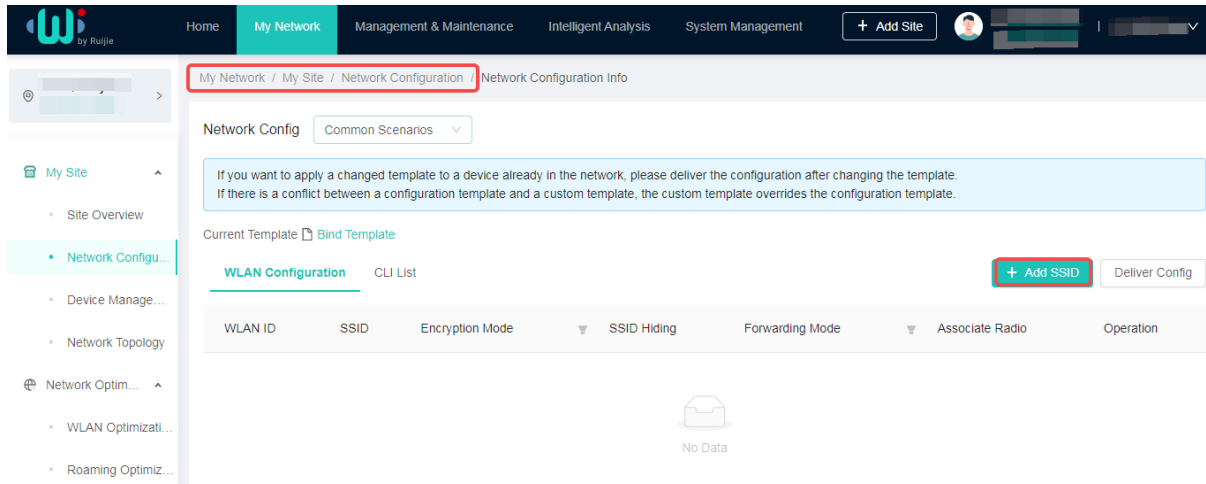
Scenario

One-click login is a simple access authentication mode. After a user connects to a WLAN, the user can click **Authenticate** on the authentication page to access the network. This authentication mode applies to public places with low security requirements.

Procedure

- (1) Add an SSID.

Choose **My Network > My Site > Network Configuration**.



Click **Add SSID**.

Add SSID
X

*** SSID** ⓘ

UTF-8

*** Encryption Mode** ⓘ

WPA-PSK/WPA2-PSK

.....

Forwarding Mode ⓘ

bridge

Same VLAN with AP

*** Radio** ⓘ

radio1
 radio2
 radio3

Single-User Rate Limit

Uplink: KB/s Downlink: KB/s

All-User Rate Limit

Uplink: KB/s Downlink: KB/s

Advanced Config

5G-preferred Enable SSID Hiding

Auth Config

Enable [Auth Config >>](#)

Cancel OK

The SSID is added.

My Network / My Site / Network Configuration / Network Configuration Info

Network Config Common Scenarios

If you want to apply a changed template to a device already in the network, please deliver the configuration after changing the template.
If there is a conflict between a configuration template and a custom template, the custom template overrides the configuration template.

Current Template Bind Template

WLAN Configuration CLI List + Add SSID Deliver Config

WLAN ID	SSID	Encryption Mode	SSID Hiding	Forwarding Mode	Associate Radio	Operation
1	wireless-staff	WPA-PSK/WPA2-PSK	No	bridge	1,2	Edit Delete Deliver Config

1-1 of 1 items < 1 > 10 / page

Click **Deliver Config** to deliver the configuration to the devices connected to the WIS Cloud Network.

My Network / My Site / Network Configuration / Network Configuration Info

Network Config Common Scenarios

If you want to apply a changed template to a device already in the network, please deliver the configuration after changing the template.
If there is a conflict between a configuration template and a custom template, the custom template overrides the configuration template.

Current Template Bind Template

WLAN Configuration CLI List + Add SSID Deliver Config

WLAN ID	SSID	Encryption Mode	SSID Hiding	Forwarding Mode	Associate Radio	Operation
1	wireless-staff	WPA-PSK/WPA2-PSK	No	bridge	1,2	Edit Delete Deliver Config

1-1 of 1 items < 1 > 10 / page

Deliver Config

When a template is applied, devices connected to the site automatically obtain the configuration in the template.

Select the configuration delivery time.

Select date

The current configuration is backed up when the template is applied. (Go to Configuration > Configuration Backup to view or restore backup records.)

Cancel Deliver Config

A pop-up window is displayed, indicating that the delivery takes 1–3 minutes.

i Tip

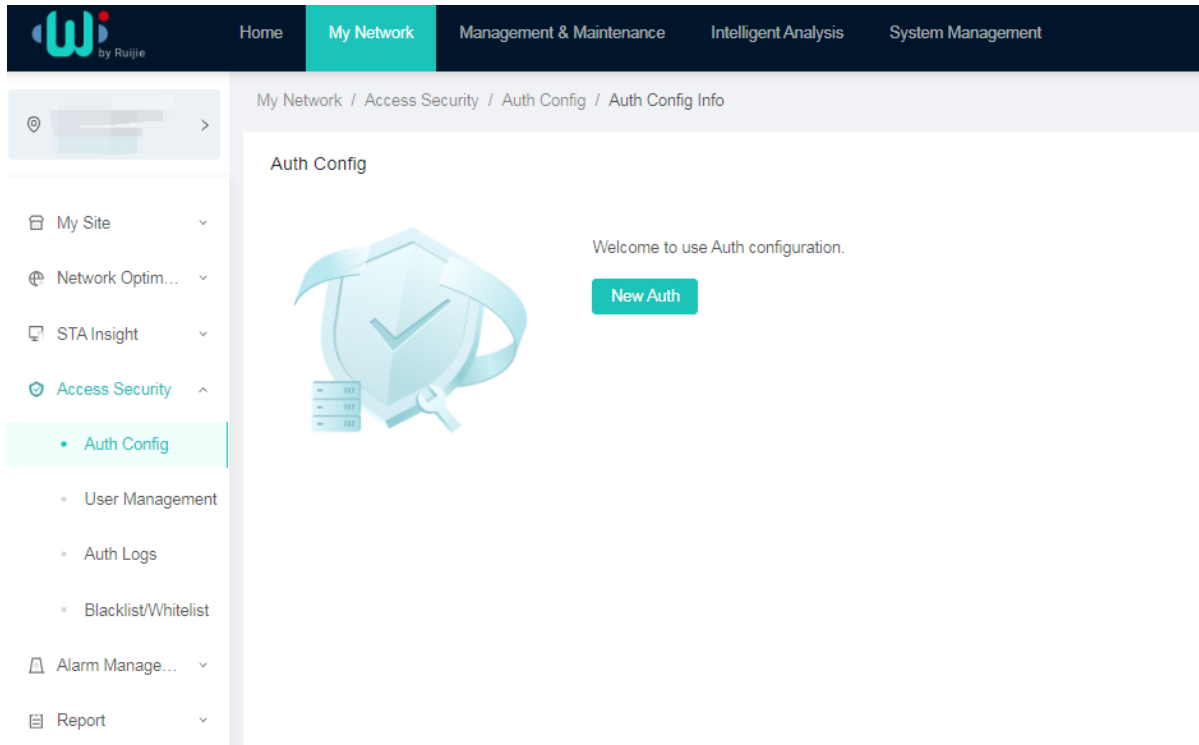
The system will immediately and apply the site is user-defined template (it should take about 1–3 minutes). Network fluctuation or temporary network disconnection may occur at these sites. Please confirm that you are aware of it and click OK for the configuration to take effect.



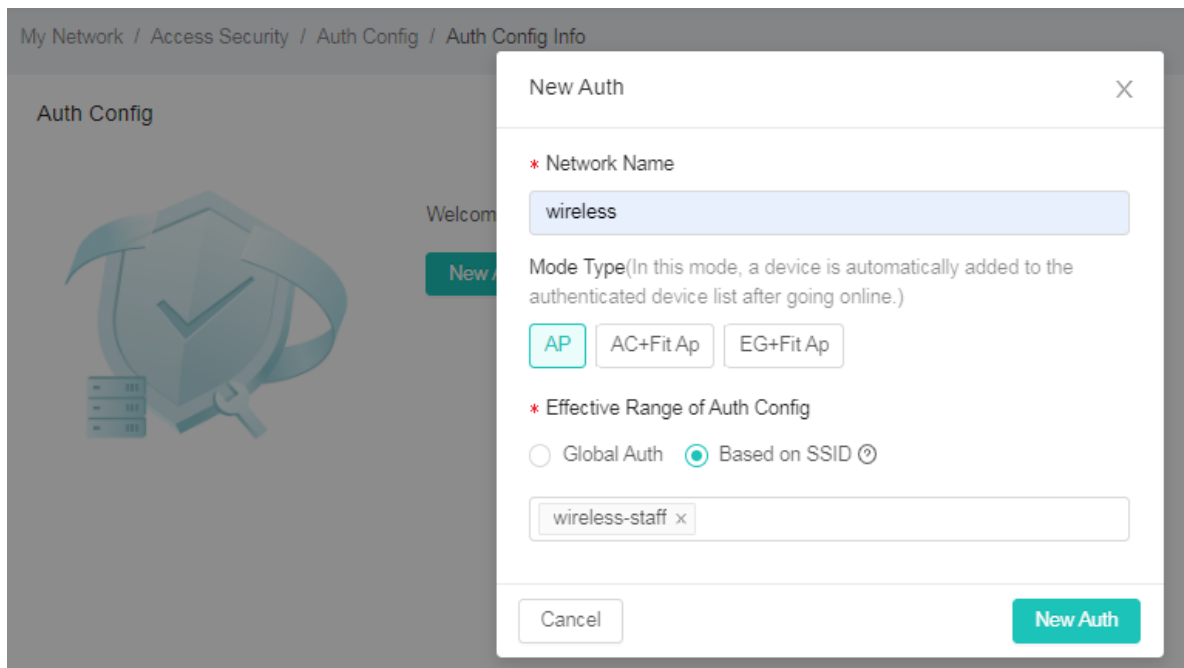
Click **OK**.

(2) Add a network.

Choose **My Network > Access Security > Auth Config**.



Click **New Auth** and add a network whose **Mode Type** is **AP**.



You can also add a network whose **Mode Type** is **EG+Fit Ap**.

New Auth
X

*** Network Name**

Please enter Network Name

Mode Type(In this mode, a device is automatically added to the authenticated device list after going online.)

AP

AC+Fit Ap

EG+Fit Ap

*** Effective Range of Auth Config**

Global Auth
 Based on SSID ⓘ
 based on IP range

Please enter start IP

-

Please enter end IP

Cancel

New Auth

Table 6-1 Fields on the New Auth page

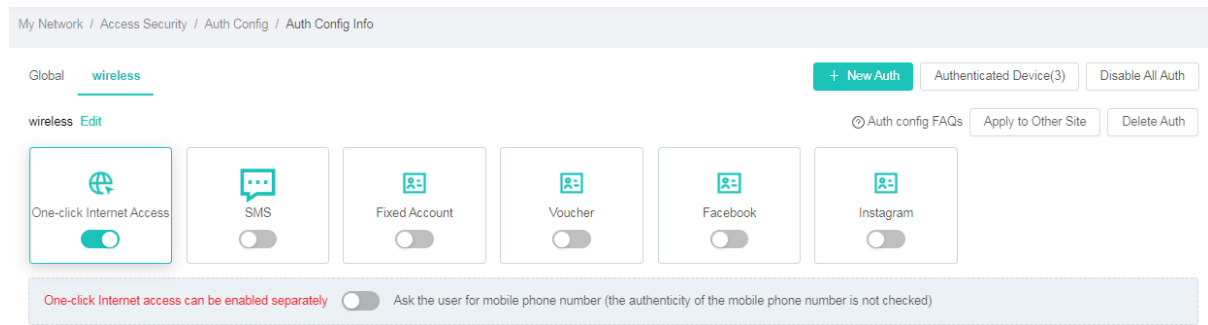
Field	Description
Network Name	Indicates the network name, which can be customized as required. This field is mandatory.
Mode Type	Indicates the authentication mode used to authenticate new devices. This field is optional.
Effective Range of Auth Config	<p>Indicates the authentication range. This field is optional.</p> <ul style="list-style-type: none"> ● Global Auth: Authentication applies to all users connecting to the network. ● Based on SSID: Authentication applies to specific SSIDs. If you select this option, enter the SSID names. ● based on IP range: Authentication applies to specific IP segments. If you select this option, enter the start and end IP addresses.

Click **New Auth**.

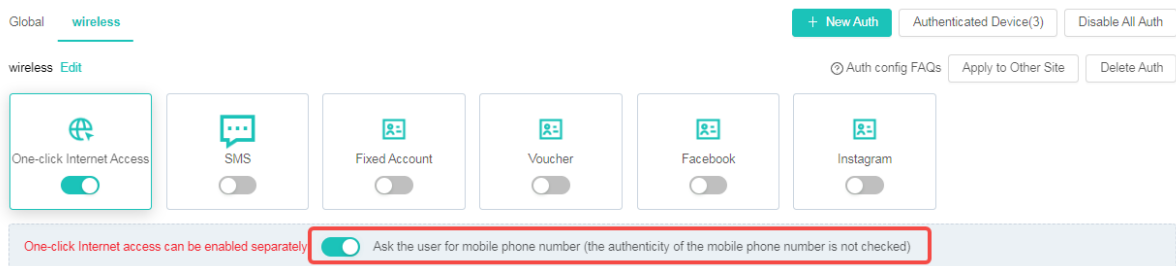
(3) Enable one-click login.

On **Auth Config**, click the newly created network **wireless** and turn on **One-click Internet Access**.

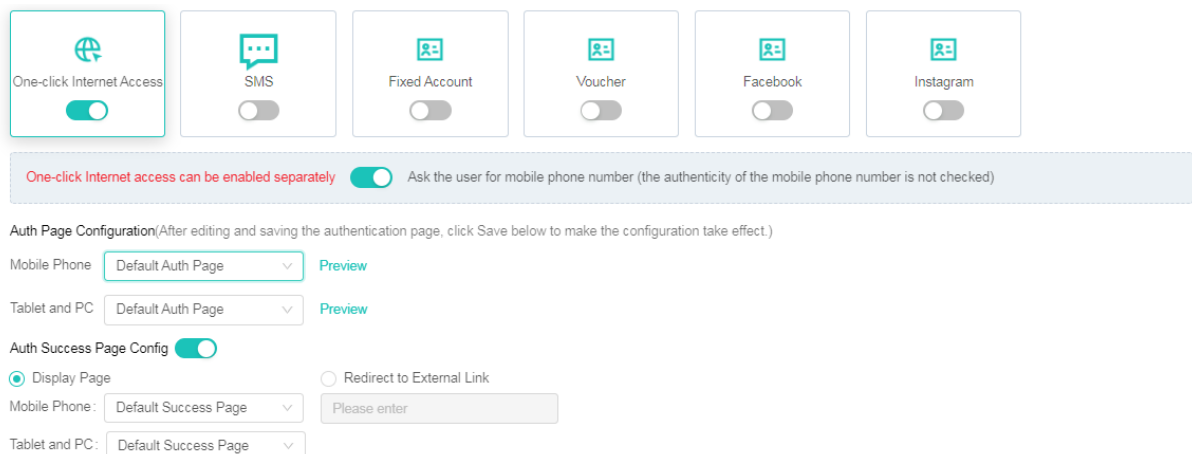
Figure 6-115 Enabling One-Click Login



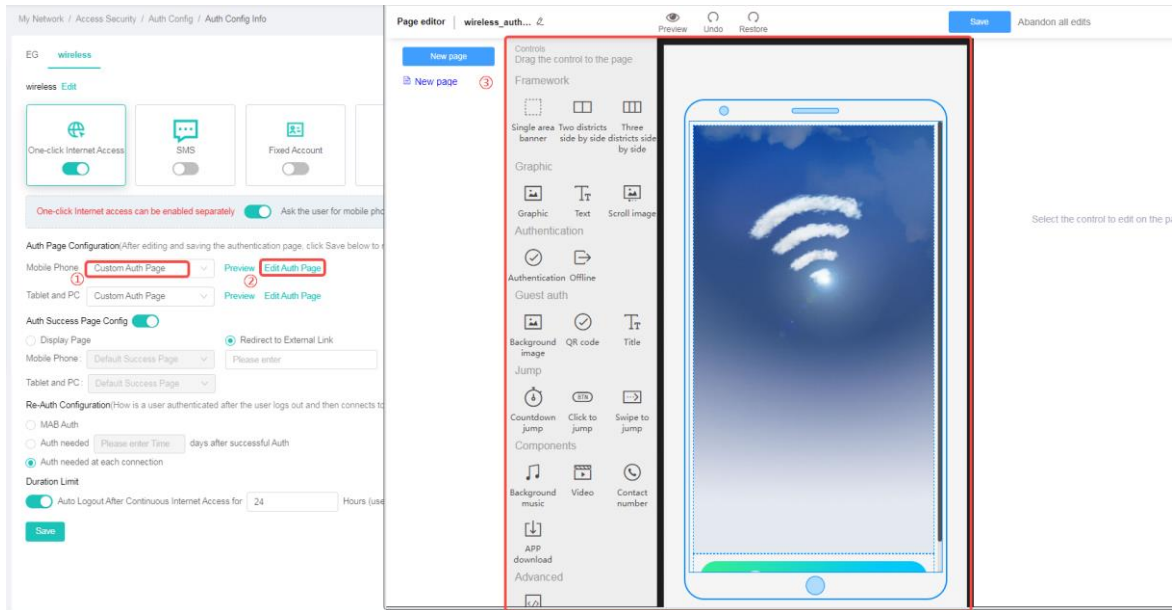
You can turn on **Ask the user for phone number (the authenticity of the mobile phone number is not checked)** as required. This toggle collects users' phone numbers but does not verify their authenticity. If this toggle is turned on, a user needs to enter the phone number when accessing the network. If this toggle is turned off, the user can click **Authenticate** to access the network.



(4) Configure the authentication pages.



- **Auth Page Configuration:** Indicates the portal page during authentication, including the login page, advertisements, and notifications. You can select the portal page of the system or a custom portal page based on actual requirements. If you need to use a custom portal page, click **Edit Auth Page**. Then, you can customize the authentication page as required.



- **Auth Success Page Config:** Indicates the portal page after authentication is successful. Two options are available: 1. After authentication is successful, the authentication success page is displayed. 2. After authentication is successful, the page is redirected to an external link.

(5) Configure an authentication policy.

You can select either of the following policies based on the network deployment requirements: **MAB Auth**, **Auth needed *n* days after successful Auth**, and **Auth needed at each connection**.

Re-Auth Configuration(How is a user authenticated after the user logs out and then connects to the network again)

- MAB Auth
- Auth needed days after successful Auth
- Auth needed at each connection

(6) Configure the time limit.

You can force a user to go offline once the time limit is reached.

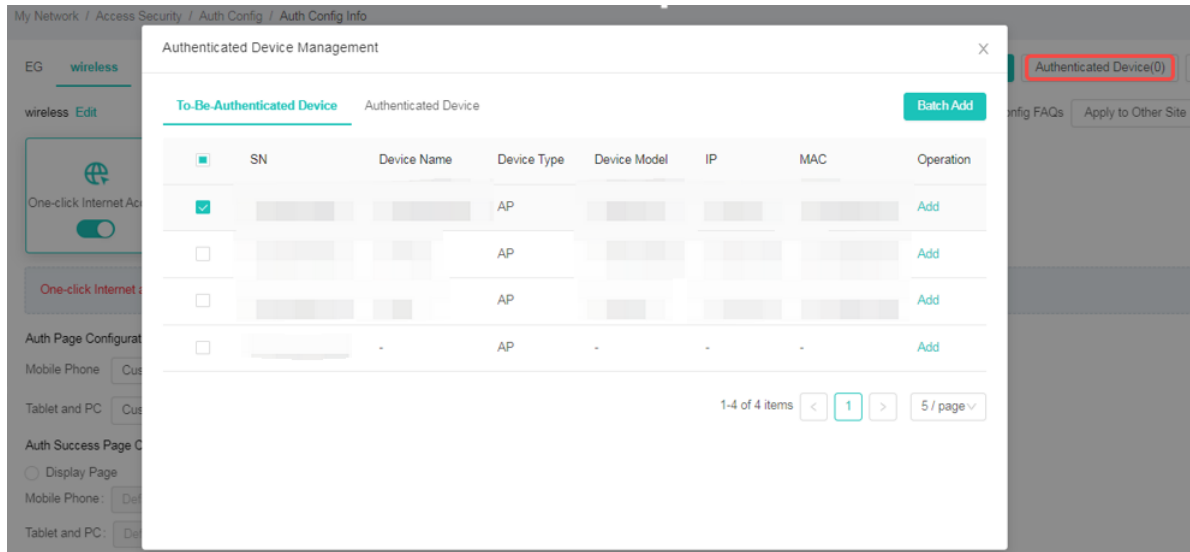
Duration Limit

Auto Logout After Continuous Internet Access for Hours (users can still connect to the network for Internet access again)

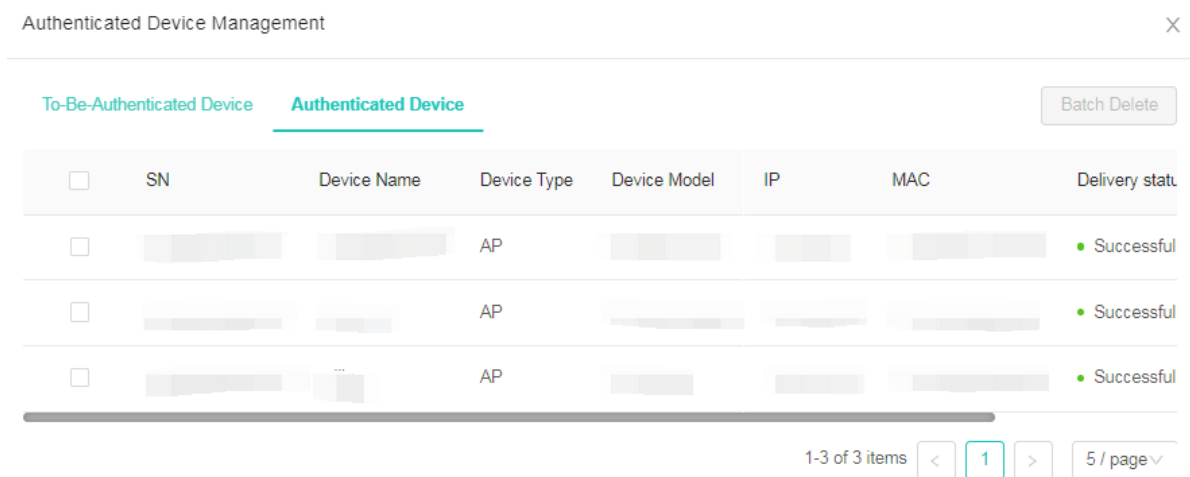
Click **Save** to complete the authentication configuration.

(7) Add authenticated devices.

Select **Authenticated Device**. On **Authenticated Device Management**, select a device and click **Add**. Alternatively, select multiple devices and click **Batch Add** to add the devices to **Authenticated Device**.



If **Delivery status** of a device is **Successful**, the device authentication configuration is successfully delivered.



After you click **Add** or **Batch Add**, the system delivers the authentication commands to the devices, including the authentication template, imperceptible authentication, and authentication enabling commands.

- Authentication template command

```
web-auth template wifidog_1 wifidog
ip 54.255.12.17
nas-ip 1.2.3.4
url https://auth-wiscloud.ruijienetworks.com/auth/wifidogAuth
redirect js
```

- Imperceptible authentication command

```
ip dhcp snooping
web-auth sta-perception enable
```

- Authentication enabling command

```
wlansec 1
web-auth portal wifidog_1
webauth
```

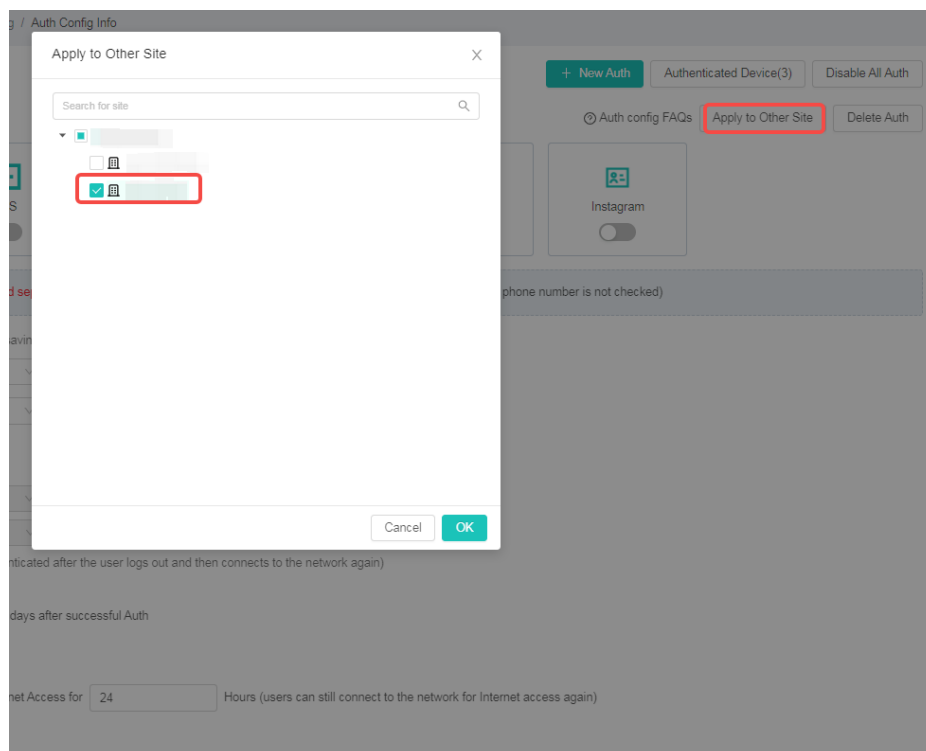
Note

- It takes about 1–3 minutes for the authentication configuration to take effect for added devices.
- A maximum of 100 devices can be added to **Authenticated Device** in a single batch.
- The commands vary depending on the authentication mode. The commands described in this section apply to one-click login.

Click  to return to the authentication configuration page.

(8) (Optional) Apply the authentication policy to other sites.

If you need to apply the authentication policy of the current site to another site, click **Apply to Other Site** and select a site.



Click **OK** to apply the authentication policy.

Verifying the Configurations

After a user connects to the WLAN, the authentication page is automatically displayed. Due to differences in terminals, the authentication page may not be automatically displayed on some terminals. Users can open a browser and visit an external website to redirect to the authentication page.

Figure 6-116 Authentication Page When Phone Number Is Required

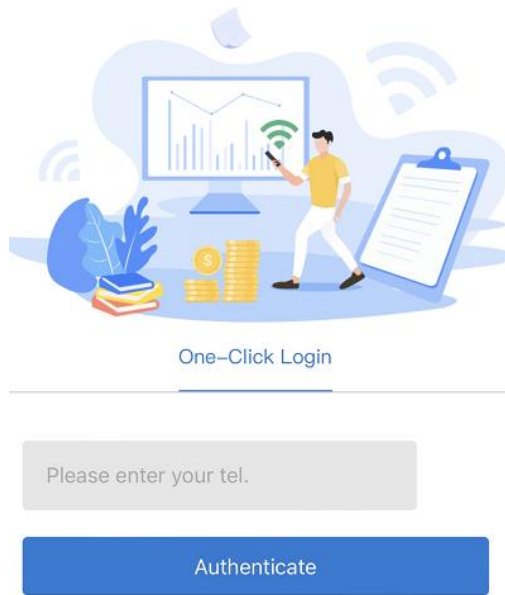


Figure 6-117 Authentication Page When Phone Number Is Not Required



Click **Authenticate** to connect to the network.



After successful authentication, you can find the user among the online users in the system.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User | Internet Access History Record | Auth Failure Record

Clear Auth Info | Authenticated Account/IP

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time	Total Online Duration
<input type="checkbox"/>	Online	1	32:2B:17: [redacted]	192.168.1.8	32:2B:17: [redacted]	One-click Internet Access	15	2022-12-27 17:09:20	-

If the user's phone number is required, the username is the phone number of the user.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User | Internet Access History Record | Auth Failure Record

Clear Auth Info | Authenticated Account/IP

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time	Total Online Duration
<input type="checkbox"/>	Online	1	136: [redacted]	192.168. [redacted]	32:2B:17: [redacted]	One-click Internet Access	16	2022-12-27 17:11:47	-

1-1 of 1 items | 1 | 10 / page

2. SMS Authentication

Scenario

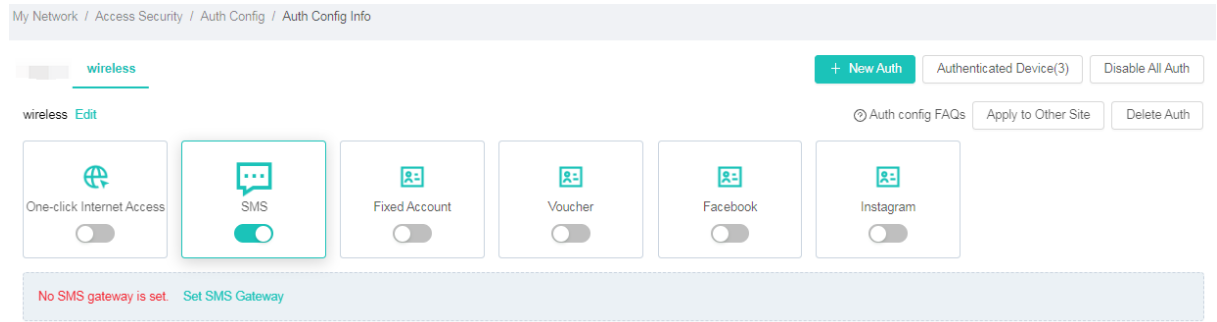
SMS authentication is a value-added, convenient, and quick authentication mode. After a smart terminal accesses a WLAN with SMS authentication enabled, the user only needs to enter the phone number and verification code returned by the SMS operator to complete identity verification and access network resources. This ensures WLAN access security.

Procedure

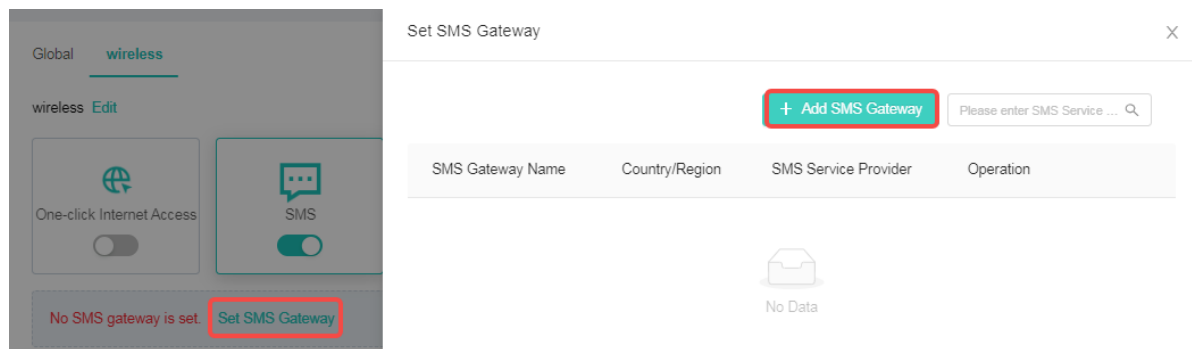
- (1) [Add an SSID.](#)
- (2) [Add a network.](#)
- (3) Enable SMS authentication.

On **Auth Config**, click the newly created network **wireless** and turn on **SMS**.

Figure 6-118 Enabling SMS Authentication



Click **Set SMS Gateway** > **Add SMS Gateway** to configure an SMS gateway.



On the SMS gateway configuration page, enter the SMS gateway information.

Perform the following steps to complete settings:
If no desired SMS service provider is available or you have any problem in use, click the robot icon and choose Problems & Feedback the lower right corner and leave a message or call 4006-208-818 (pre-sale) or 4008-111-000 (after-sale) for consultation.

* SMS Gateway Name

* Country/Region

* SMS Service Provider

* Connect URL

Password

Region

Userid

SMS Verification Code Content

Cancel

OK

⚠ Caution

The WIS Cloud Network supports GUODULINK's Hong Kong, Macao and Taiwan SMS platform and Alibaba Cloud's international SMS platform.

Click **OK** to complete the SMS gateway configuration.

Set SMS Gateway
✕

+ Add SMS Gateway

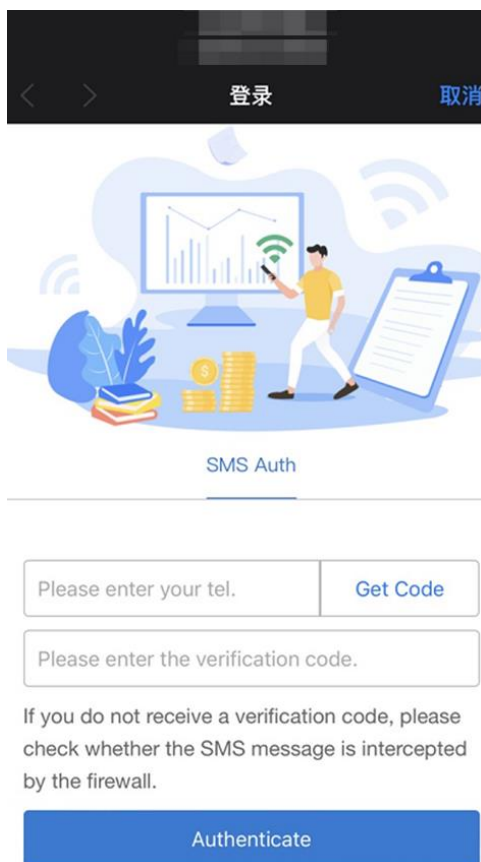
SMS Gateway Name	Country/Region	SMS Service Provider	Operation
[Placeholder]	China	Beijing Guodu Internet(HTTP)	Edit Send a test messag...
[Placeholder]	China	Beijing Guodu Internet(HTTP)	Edit Send a test messag...

1-2 of 2 items
<
1
>
5 / page

- (4) [Configure the authentication pages.](#)
- (5) [Configure an authentication policy.](#)
- (6) [Configure the time limit.](#)
- (7) [Add authenticated devices.](#)
- (8) [\(Optional\) Apply the authentication policy to other sites.](#)

Verifying the Configurations

After a user connects to the WLAN, the authentication page is automatically displayed.



The user can enter the phone number and verification code for Internet access authentication.



After successful authentication, you can find the user among the online users in the system.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User Internet Access History Record Auth Failure Record

<input type="checkbox"/>	Status ▾	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode ▾	Cumulative Online Count	Online Time	Total Online Duration
<input type="checkbox"/>	● Online	1	2471; [redacted]	192.168; [redacted]	32:2B:17:2E; [redacted]	SMS	14	2022-12-27 17:02:44	-

1-1 of 1 items

3. Fixed Account Authentication

Scenario

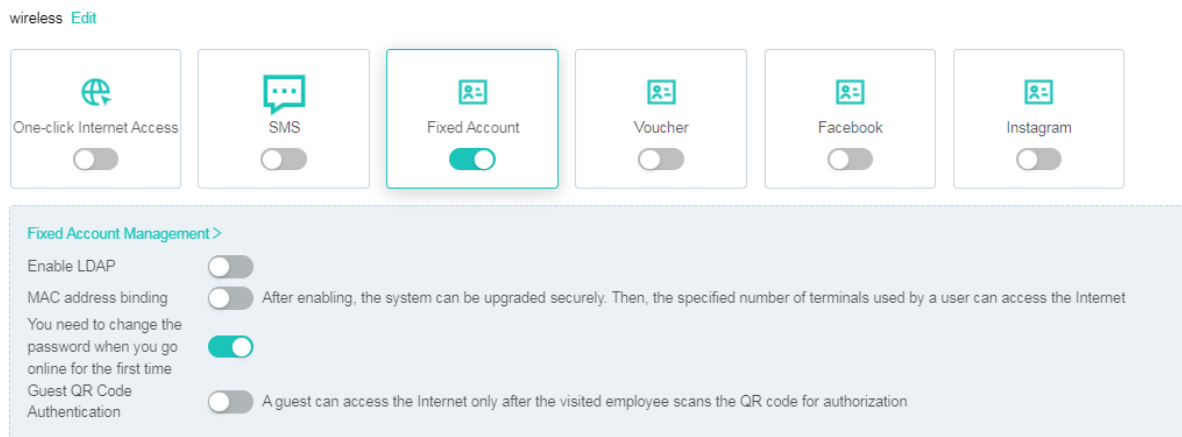
Users can use fixed accounts added through system identity sources or third-party identity sources (such as LDAP) and passwords for Internet access authentication.

Procedure

- (1) [Add an SSID.](#)
- (2) [Add a network.](#)
- (3) Enable fixed account authentication.

On **Auth Config**, click the newly created network **wireless** and turn on **Fixed Account**.

Figure 6-119 Enabling Fixed Account Authentication

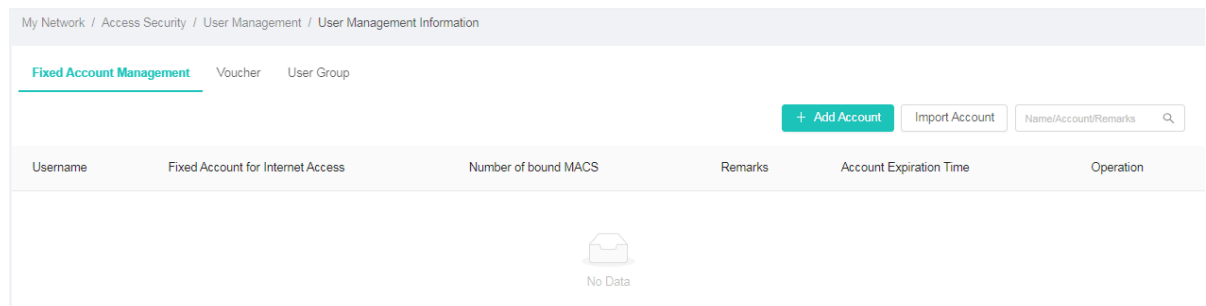


- (4) Configure the identity source used for fixed account authentication.

The identity source can be an account created on the WIS Cloud Network server or from a third-party account management server, such as LDAP. Users can use proper accounts as identity sources based on the live network deployment requirements.

- a Create an account on the WIS Cloud Network server.

Click **Fixed Account Management**.



Click **Add Account** and fill in account information.

Add Fixed Account
✕

*** Username**

*** Fixed Account for Internet Access**

*** Password**

*** Type of Account Validity Period**

Permanently Valid
 Auto Suspension upon Expiration

Bound MAC address

Remarks

Cancel
OK

Click **OK**.

Fixed Account Management
Voucher
User Group

+ Add Account
Import Account
Name/Account/Remarks
🔍

Username	Fixed Account for Internet Access	Number of bound MACS	Remarks	Account Expiration Time	Operation
guest	guest	-	-	Permanently Valid	Edit Delete

b Configure an account from the remote LDAP server.

Click **Enable LDAP > Set** to enter the **LDAP Domain Configuration** page.

Fixed Account Management >

Enable LDAP

LDAP Domain Configuration
⊙ Not configured
Set >

MAC address binding After enabling, the system can be upgraded securely. Then, the specified number of terminals used by a user can access the Internet

You need to change the password when you go online for the first time

Guest QR Code Authentication A guest can access the Internet only after the visited employee scans the QR code for authorization

Fill in LDAP server information.

106

LDAP Domain Configuration
✕

* LDAP server IP

* Server port

* Directory tree root nod...

Admin account

* Account

* Password

* LDAP auth... Identity Verification When LDAP User Information Is Queried
 Identity Verification When a User Logs in to the LDAP Server

The system queries user information based on two attributes: user objectClass and attribute name of username

* User objectClass

* Attribute Name of User...

* Attribute Name of User...

* Attribute Name of User...

Click **Save**.

wireless [Edit](#)

 One-click Internet Access <input type="checkbox"/>	 SMS <input type="checkbox"/>	 Fixed Account <input checked="" type="checkbox"/>	 Voucher <input type="checkbox"/>	 Facebook <input type="checkbox"/>	 Instagram <input type="checkbox"/>
---	-------------------------------------	--	---	--	---

Fixed Account Management >

Enable LDAP

LDAP Domain Configuration ✔ Configured [Set >](#)

MAC address binding After enabling, the system can be upgraded securely. Then, the specified number of terminals used by a user can access the Internet

You need to change the password when you go online for the first time

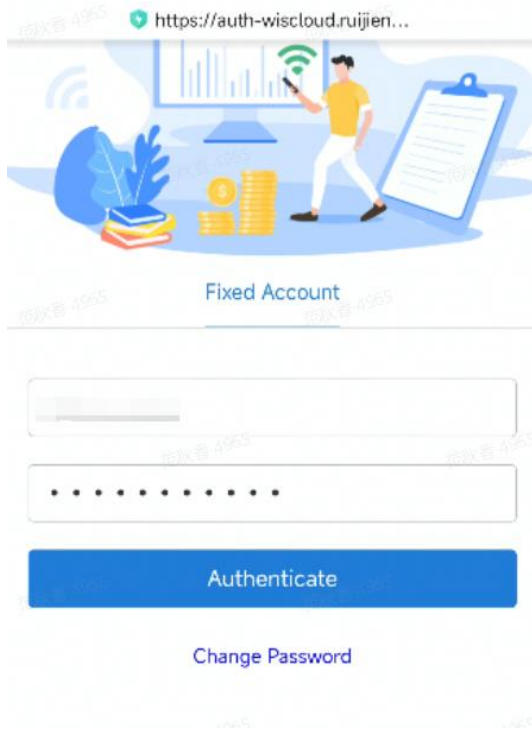
Guest QR Code Authentication A guest can access the Internet only after the visited employee scans the QR code for authorization

- (5) [Configure the authentication pages.](#)
- (6) [Configure an authentication policy.](#)
- (7) [Configure the time limit.](#)
- (8) [Add authenticated devices.](#)

(9) [\(Optional\) Apply the authentication policy to other sites.](#)

Verifying the Configurations

After a user connects to the WLAN, the authentication page is automatically displayed. Due to differences in terminals, the authentication page may not be automatically displayed on some terminals. Users can open a browser and visit an external website to redirect to the authentication page.



The user can enter the account and password for Internet access authentication.



After successful authentication, you can find the user among the online users in the system.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User | Internet Access History Record | Auth Failure Record | [Clear Auth Info](#)

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time
<input type="checkbox"/>	Online	1		192.168		Fixed Account	12	2022-12-27 16:49:13

4. QR Code Authentication for Visitors

Scenario

When a user connects to the WLAN where QR code authentication is enabled for visitors and accesses an external IP address, the user is redirected to the QR code page returned by the server. The user can use an authenticated client app to scan the QR code to access network resources. Generally, this function applies to enterprise network management. For example, employees of the enterprise use fixed account authentication. When external visitors enter the enterprise and need to access the network, employees of the enterprise can scan the QR code for visitors to authorize the visitors to access the network.

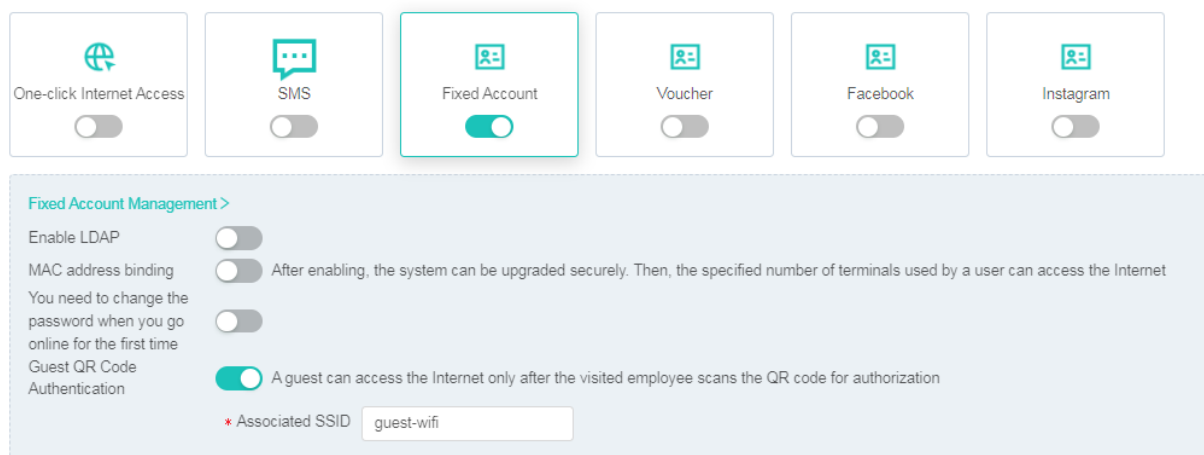
Procedure

- (1) [Add an SSID.](#)
- (2) [Add a network.](#)
- (3) Enable fixed account authentication and QR code authentication for visitors.

On **Auth Config**, click the newly created network **wireless**.

Turn on **Fixed Account** and **Guest QR Code Authentication** and set **Associated SSID** to **guest-wifi**.

Figure 6-120 Enabling Fixed Account Authentication and QR Code Authentication for Visitors



- (4) Configure the identity source used for fixed account authentication.

The identity source can be an account created on the WIS Cloud Network server or from a third-party account management server, such as LDAP. Users can use proper accounts as identity sources based on the live network deployment requirements.

- a Create an account on the WIS Cloud Network server.
- b Configure an account from the remote LDAP server.

- (5) Configure the authentication pages.

The authentication pages for QR code authentication include the employee authentication page, visitor authentication page, and authentication success page.

- **Employee Authentication Page:** Indicates the employee authentication page.

- **Guest Authentication Page:** Indicates the visitor authentication page.
- **Auth Success Page Config:** Indicates the page after successful authentication.

Auth Page Configuration(After editing and saving the authentication page, click Save below to make the configuration take effect.)

Employee Authentication Page **Guest Authentication Page**

Mobile Phone: Default Auth Page

Tablet and PC: Default Auth Page

Auth Success Page Config

Display Page Redirect to External Link

Mobile Phone: Custom Auth Success Page

Tablet and PC: Custom Auth Success Page

You can customize the employee authentication and authentication success pages as required. Customization of the visitor authentication page is not allowed.

Auth Page Configuration(After editing and saving the authentication page, click Save below to make the configuration take effect.)

Employee Authentication Page Guest Authentication Page

Mobile Phone: Custom Auth Page

Tablet and PC: Custom Auth Page

Auth Success Page Config

Display Page Redirect to External Link

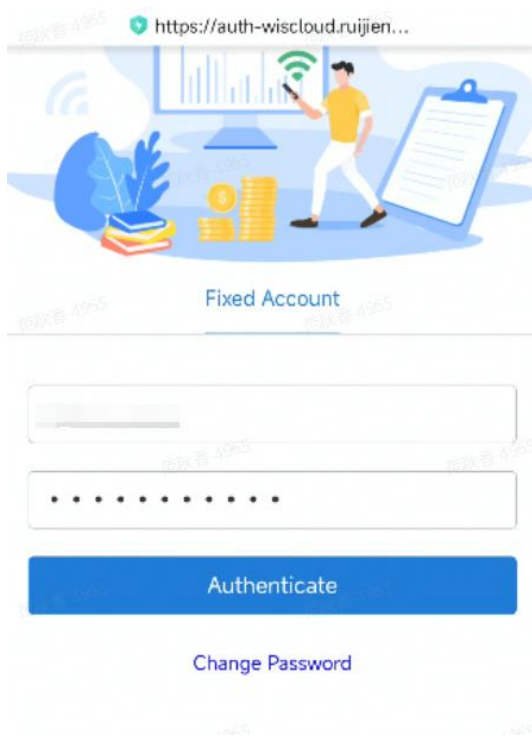
Mobile Phone: Custom Auth Success Page

Tablet and PC: Custom Auth Success Page

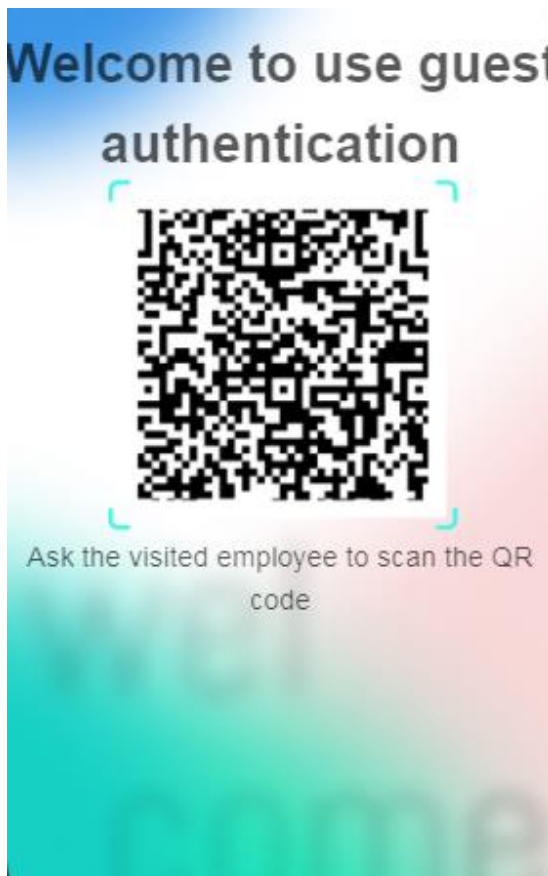
- (6) [Configure an authentication policy.](#)
- (7) [Configure the time limit.](#)
- (8) [Add authenticated devices.](#)
- (9) [\(Optional\) Apply the authentication policy to other sites.](#)

Verifying the Configurations

After an employee connects to the WLAN, the authentication page is automatically displayed. Due to differences in terminals, the authentication page may not be automatically displayed on some terminals. Users can open a browser and visit an external website to redirect to the authentication page.



Visitors can scan the QR code to connect to the SSID.



After successful authentication, you can find the visitor among the online users in the system.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User Internet Access History Record Auth Failure Record [Clear Auth Info](#)

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time	Total Online Duration
<input type="checkbox"/>	Online	1	[REDACTED]	192.168.1.[REDACTED]	32:2B:17-[REDACTED]	Guest	21	2022-12-27 18:24:30	-
<input type="checkbox"/>	Online	1	[REDACTED]	192.168.1.[REDACTED]	8E:D4:73-[REDACTED]	Fixed Account	6	2022-12-27 18:21:40	-

1-2 of 2 items [1](#) [10 / page](#)

5. Voucher Authentication

Scenario

Voucher accounts are dynamically generated using the system identity sources, and users can use specific vouchers for Internet access authentication.

Limitation

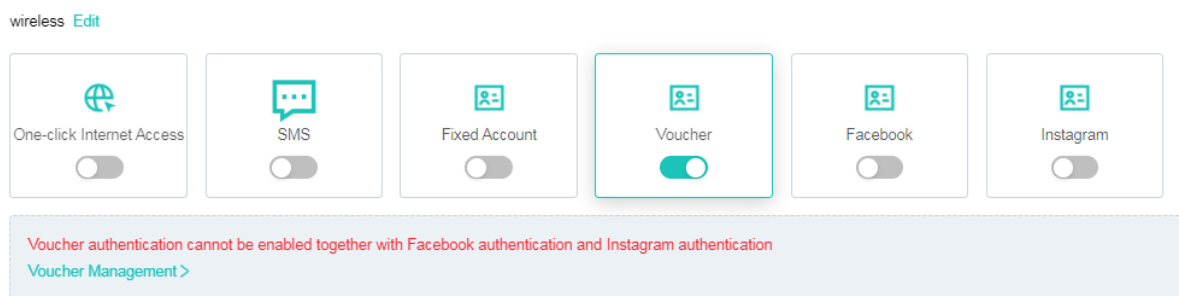
Voucher authentication cannot be enabled together with Facebook authentication and Instagram authentication.

Procedure

- (1) [Add an SSID.](#)
- (2) [Add a network.](#)
- (3) Enable voucher authentication.

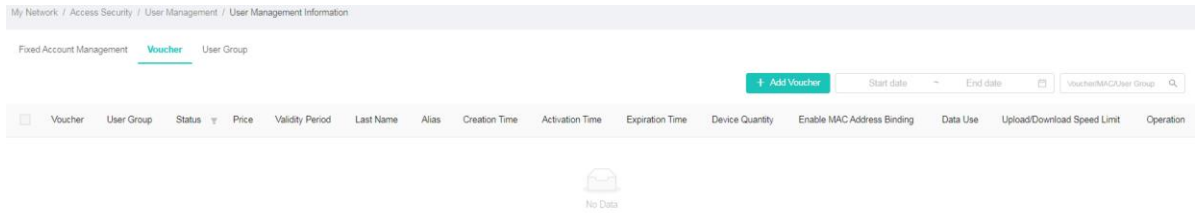
On **Auth Config**, click the newly created network **wireless** and turn on **Voucher**.

Figure 6-121 Enabling Voucher Authentication

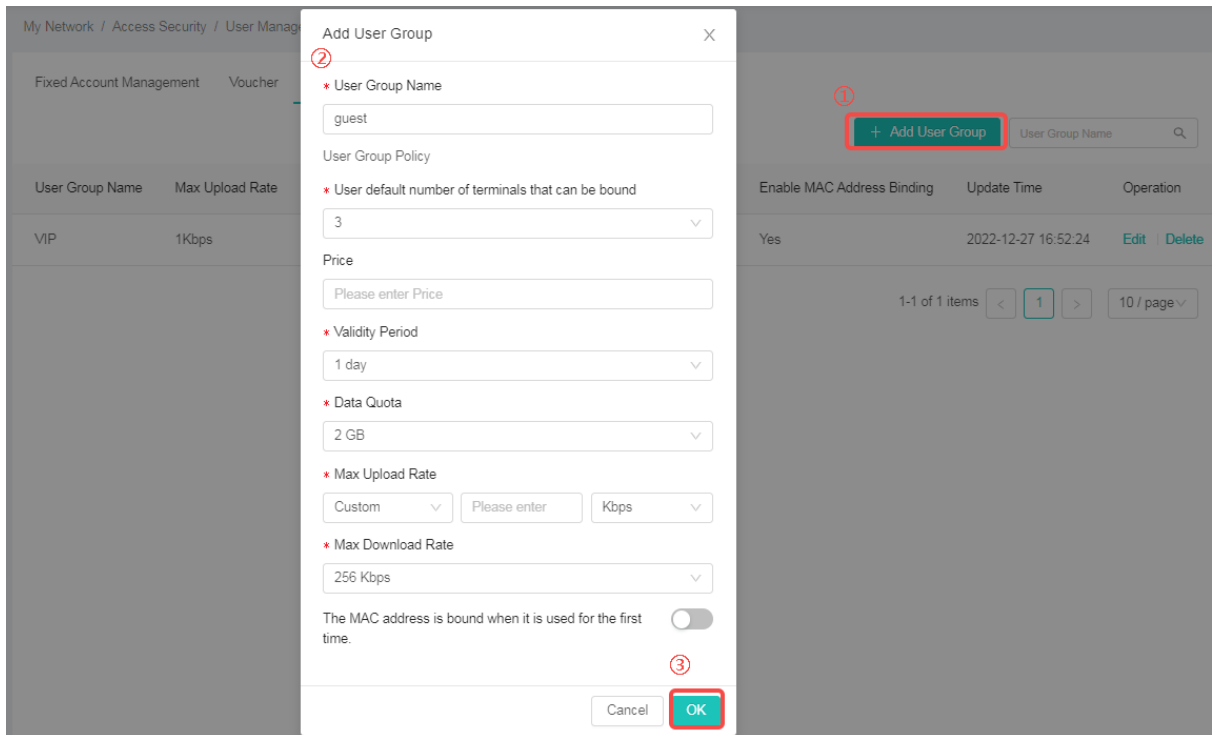


- (4) Configure voucher accounts.

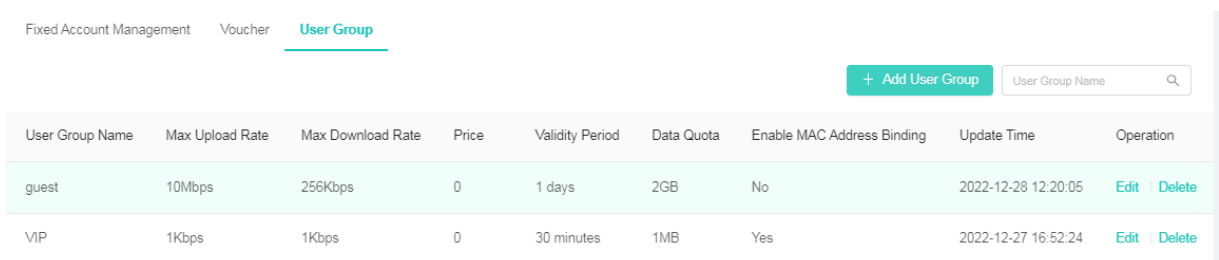
Click **Voucher Management**.



Click the **User Group** tab and click **Add User Group**.



Click **OK**.



Click **Add Voucher** and add five voucher accounts.

Add Voucher
✕

*** Quantity**

*** User Group**

guest
▼

User Info Config ▼

Last Name

First Name

Email

Mobile Phone Number

Alias

Advanced Settings >

Click **OK**.

Fixed Account Management
Voucher
User Group

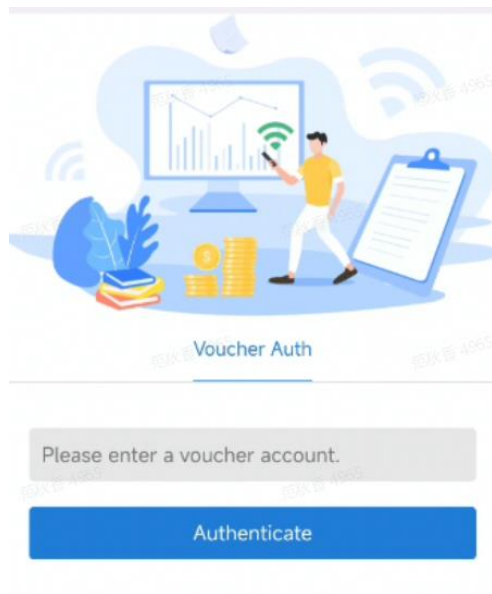
+ Add Voucher
Start date ~ End date 📅
Voucher/MAC/User Group 🔍

<input type="checkbox"/>	Voucher	User Group	Status	Price	Validity Period	Last Name	Alias	Creation Time	Activation Time	Operation
<input type="checkbox"/>	fiukw6	guest	● Unused	-	1 days	-	-	2022-12-28 12:21:59	-	Edit Reset Delete
<input type="checkbox"/>	u8l5bb	guest	● Unused	-	1 days	-	-	2022-12-28 12:21:59	-	Edit Reset Delete
<input type="checkbox"/>	auhjob	guest	● Unused	-	1 days	-	-	2022-12-28 12:21:59	-	Edit Reset Delete
<input type="checkbox"/>	x4s3xg	guest	● Unused	-	1 days	-	-	2022-12-28 12:21:59	-	Edit Reset Delete
<input type="checkbox"/>	8fivq8	guest	● Unused	-	1 days	-	-	2022-12-28 12:21:59	-	Edit Reset Delete

- (5) [Configure the authentication pages.](#)
- (6) [Configure an authentication policy.](#)
- (7) [Configure the time limit.](#)
- (8) [Add authenticated devices.](#)
- (9) [\(Optional\) Apply the authentication policy to other sites.](#)

Verifying the Configurations

After a user connects to the WLAN, the authentication page is automatically displayed. Due to differences in terminals, the authentication page may not be automatically displayed on some terminals. Users can open a browser and visit an external website to redirect to the authentication page.



Please enter a voucher account.

Authenticate

The user can enter the voucher account for Internet access authentication.



After successful authentication, you can find the user among the online users in the system.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User Internet Access History Record Auth Failure Record Clear Auth Info

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time
<input type="checkbox"/>	Online	1	233234	192.168.1.1	32:2B:11:00:00:00	Voucher	13	2022-12-27 16:52:56

6. Facebook Authentication

Scenario

Facebook authentication is dedicated for users who have registered with Facebook. Users can use their Facebook accounts to connect to the network.

Limitation

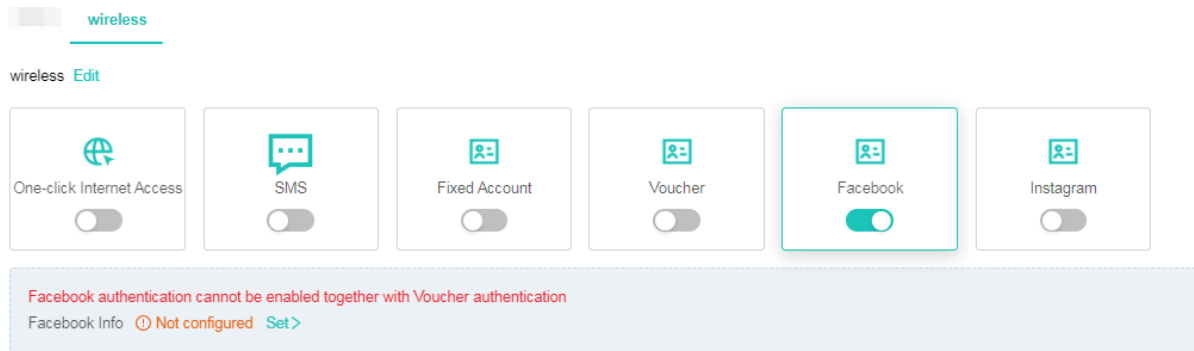
Facebook authentication cannot be enabled together with voucher authentication.

Procedure

- (1) [Add an SSID.](#)
- (2) [Add a network.](#)
- (3) Enable Facebook authentication.

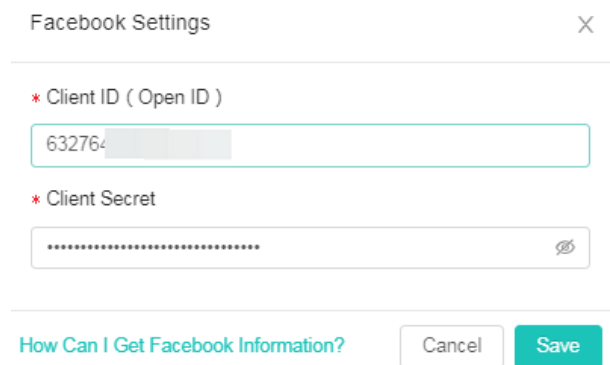
On **Auth Config**, click the newly created network **wireless** and turn on **Facebook**.

Figure 6-122 Enabling Facebook Authentication

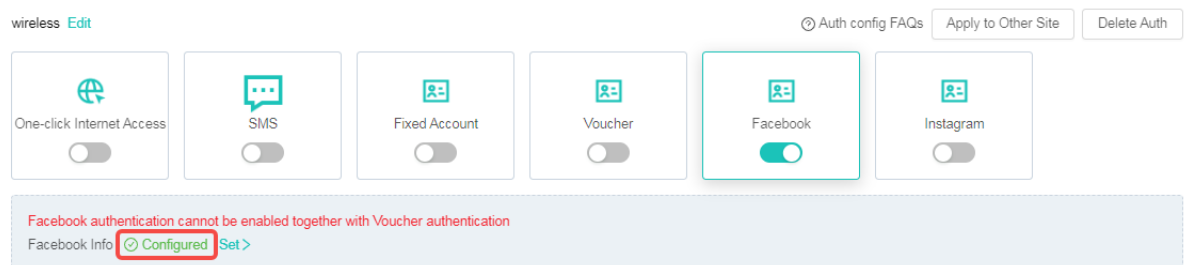


- (4) Configure an authentication account.

Click **Set** to enter the **Facebook Settings** page and set **Client ID** and **Client Secret**.



Click **Save** to complete the authentication account configuration.



- (5) [Configure the authentication pages.](#)
- (6) [Configure an authentication policy.](#)

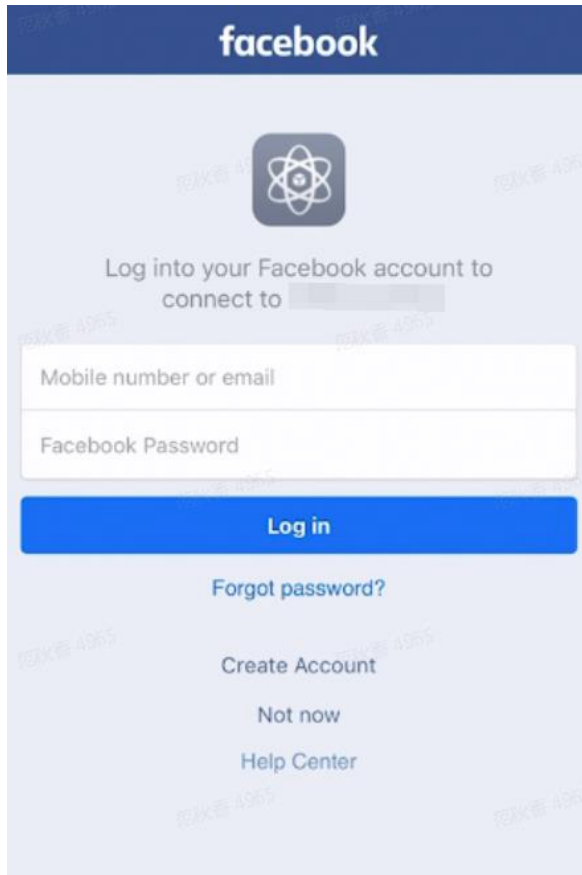
- (7) [Configure the time limit.](#)
- (8) [Add authenticated devices.](#)
- (9) [\(Optional\) Apply the authentication policy to other sites.](#)

Verifying the Configurations

After a user connects to the WLAN, the authentication page is automatically displayed. Due to differences in terminals, the authentication page may not be automatically displayed on some terminals. Users can open a browser and visit an external website to redirect to the authentication page.



Click **Click here to login on Facebook** to enter the Facebook login page.



The user can enter the Facebook account and password for Internet access authentication.



After successful authentication, you can find the user among the online users in the system.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User | Internet Access History Record | Auth Failure Record

Clear Auth Info | Authenticated Account/IP

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time	Total Online Duration
<input type="checkbox"/>	Online	1				Facebook	8	2022-12-27 16:09:00	-

1-1 of 1 items | 1 / page

7. Instagram Authentication

Scenario

Instagram authentication is dedicated for users who have registered with Instagram. Users can use their Instagram accounts to connect to the network.

Limitation

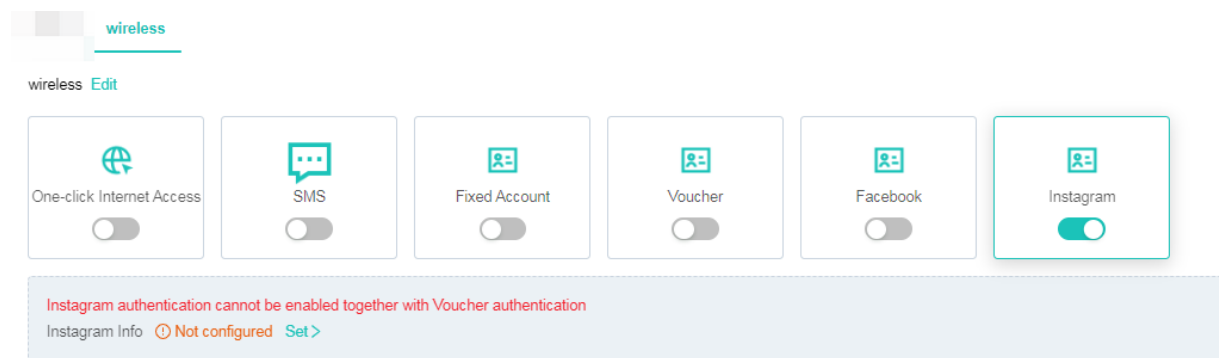
Instagram authentication cannot be enabled together with voucher authentication.

Procedure

- (1) [Add an SSID.](#)
- (2) [Add a network.](#)
- (3) Enable Instagram authentication.

On **Auth Config**, click the newly created network **wireless** and turn on **Instagram**.

Figure 6-123 Enabling Instagram Authentication



- (4) Configure an authentication account.

Click **Set** to enter the **Instagram Settings** page and set **Client ID** and **Client Secret**.

Instagram Settings
✕

*** Client ID (Open ID)**


*** Client Secret**


[How Can I Get Instagram Information?](#)


Click **Save** to complete the authentication account configuration.


Global wireless


wireless [Edit](#)



 One-click Internet Access


 SMS


 Fixed Account


 Voucher


 Facebook


 Instagram

Instagram authentication cannot be enabled together with Voucher authentication

Instagram Info ✔ Configured [Set >](#)

- (5) [Configure the authentication pages.](#)
- (6) [Configure an authentication policy.](#)
- (7) [Configure the time limit.](#)
- (8) [Add authenticated devices.](#)
- (9) [\(Optional\) Apply the authentication policy to other sites.](#)

Verifying the Configurations

After a user connects to the WLAN, the authentication page is automatically displayed. Due to differences in terminals, the authentication page may not be automatically displayed on some terminals. Users can open a browser and visit an external website to redirect to the authentication page.



Click **Click here to login on Instagram** to enter the Instagram login page.



The user can enter the Instagram account and password for Internet access authentication.



After successful authentication, you can find the user among the online users in the system.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User | Internet Access History Record | Auth Failure Record | [Clear Auth Info](#)

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time
<input type="checkbox"/>	Online	1				Instagram	9	2022-12-27 16:18:41

8. Hybrid Authentication

Scenario

Authentication modes include fixed account authentication, one-click login, SMS authentication, and voucher authentication. You can select two or more authentication methods based on actual network scenarios. When one of the authentications is successful, you can access network resources.

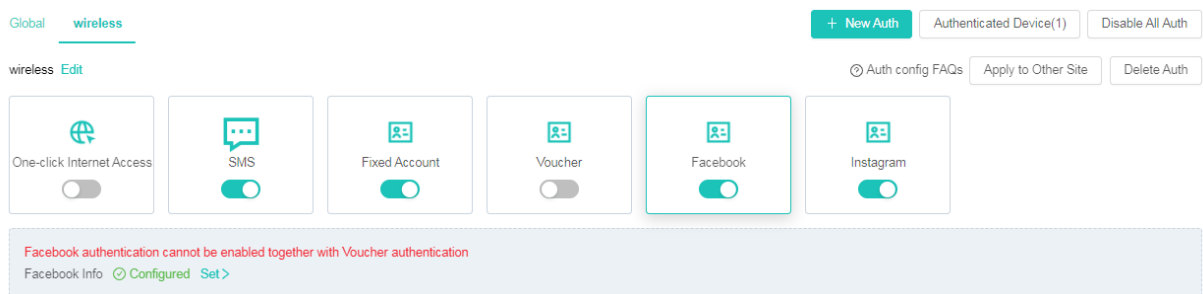
Limitation

- Voucher authentication cannot be enabled together with Facebook authentication and Instagram authentication.
- One-click login cannot be enabled with any other authentication method.

Procedure

- (1) [Add an SSID.](#)
- (2) [Add a network.](#)
- (3) Configure a hybrid authentication consisting of SMS, fixed account, Facebook, and Instagram authentication.

On **Auth Config**, click the newly created network **wireless** and turn on **SMS, Fixed Account, Facebook, and Instagram.**



Note

For details about how to configure each authentication method, see the previous sections.

- (4) [Configure the authentication pages.](#)
- (5) [Configure an authentication policy.](#)
- (6) [Configure the time limit.](#)
- (7) [Add authenticated devices.](#)
- (8) [\(Optional\) Apply the authentication policy to other sites.](#)

Verifying the Configurations

After a user connects to the WLAN, the authentication page is automatically displayed. Due to differences in terminals, the authentication page may not be automatically displayed on some terminals. Users can open a browser and visit an external website to redirect to the authentication page.

Figure 6-124 Hybrid Authentication Page

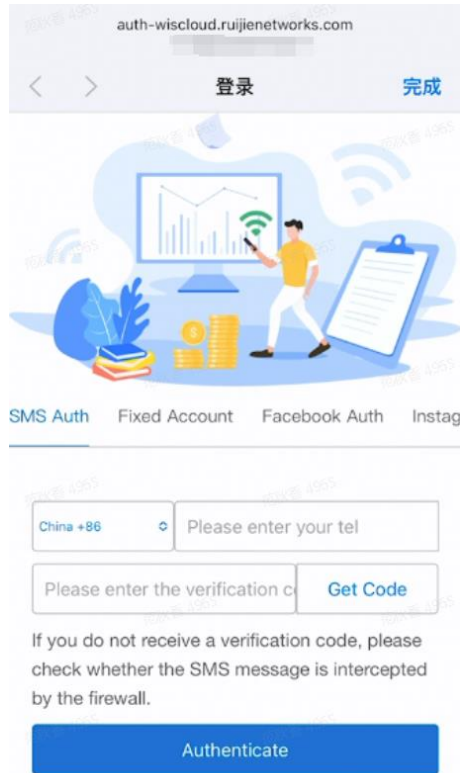
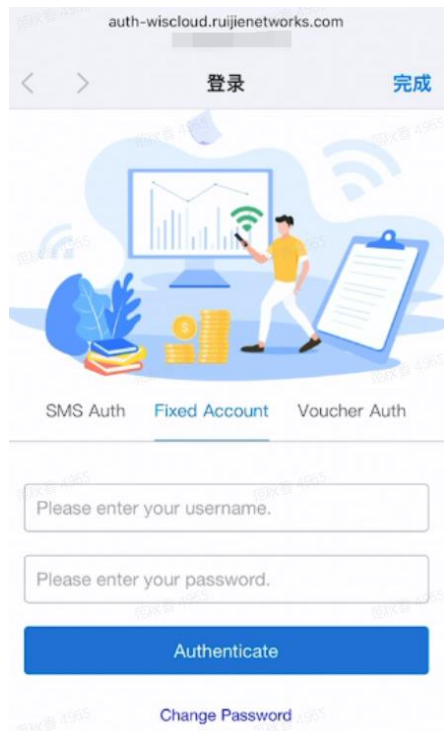


Figure 6-125 Hybrid Authentication Page



After connecting to a WLAN, select an authentication mode and enter the authentication information for Internet access authentication.



After successful authentication, you can find the user among the online users in the system.

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User | Internet Access History Record | Auth Failure Record Clear Auth Info

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time
<input type="checkbox"/>	Online	1				Instagram	9	2022-12-27 16:18:41

6.7.2 Authentication Logs

Choose **My Network > Access Security > Auth Logs** and view authentication logs on the **Authenticated Users**, **Internet Access History Record**, and **Auth Failure Record** tabs.

1. Authenticated User

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User | Internet Access History Record | Auth Failure Record Clear Auth Info | Authenticated AccountSP 🔍

<input type="checkbox"/>	Status	Related STA count	Authenticate Account	IP Address	MAC Address	Auth Mode	Cumulative Online Count	Online Time	Total Online Duration
<input type="checkbox"/>	Online	1				Facebook	8	2022-12-27 16:09:00	-

1-1 of 1 items < 1 > 10 / page

2. Internet Access History Record

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User **Internet Access History Record** Auth Failure Record Export Record Start date ~ End date Authenticated Account/IP

Authenticate Account	IP Address	MAC Address	Auth Mode	Online Time	Offline Time	Go-offline Cause
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Voucher	2022-12-27 16:52:56	2022-12-27 16:55:38	Device notification offline
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Fixed Account	2022-12-27 16:49:13	2022-12-27 16:51:43	Device notification offline
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Facebook	2022-12-27 16:32:27	2022-12-27 16:39:37	Device notification offline
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Instagram	2022-12-27 16:26:27	2022-12-27 16:27:46	Device notification offline
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Instagram	2022-12-27 16:18:41	2022-12-27 16:21:52	Device notification offline
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Facebook	2022-12-27 16:09:00	2022-12-27 16:10:44	Device notification offline
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Facebook	2022-12-27 15:06:01	2022-12-27 15:15:05	Device notification offline
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Instagram	2022-12-27 14:58:24	2022-12-27 15:04:34	Device notification offline
[Redacted]	192.168.[Redacted]	32:2B:17:25 [Redacted]	Facebook	2022-12-27 14:32:08	2022-12-27 14:42:03	Device notification offline

1-9 of 9 items < 1 > 10 / page v

3. Auth Failure Record

My Network / Access Security / Auth Logs / Auth Log Info

Authenticated User Internet Access History Record **Auth Failure Record** Authenticated Account

Authenticate Account	IP Address	MAC Address	Auth Mode	Online Time	Failure Cause
No Data					

6.7.3 Blacklist/Whitelist

Choose **My Network > Access Security > Blacklist/Whitelist** to go to the wireless STA blacklist/whitelist configuration page and manage the access of STAs at a site based on the blacklist/whitelist.

Figure 6-126 Blacklist/Whitelist

My Network / Access Security / Blacklist/Whitelist / Blacklist/Whitelist Info

Based on SSID
 *Hotspot
 *Freehotspot
 *eduroam
 Global
 Global Setup

Blacklist Whitelist + Add MAC Address Deliver Config Synchronize AC Config ... Search MAC Address

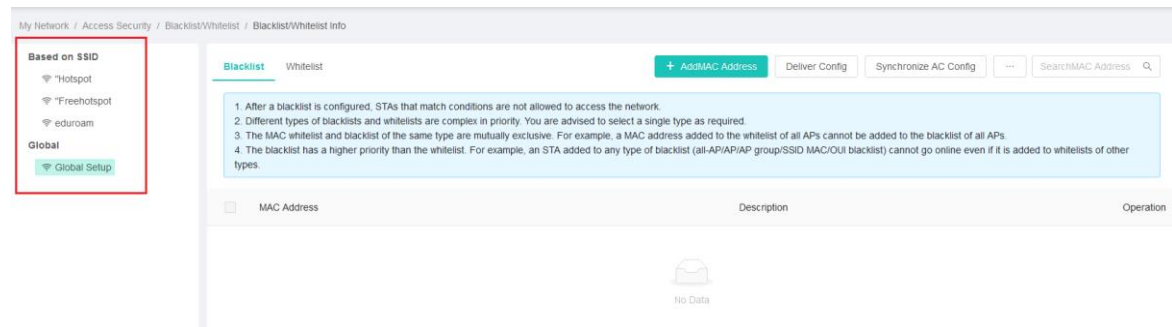
- After a blacklist is configured, STAs that match conditions are not allowed to access the network.
- Different types of blacklists and whitelists are complex in priority. You are advised to select a single type as required.
- The MAC whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of all APs cannot be added to the blacklist of all APs.
- The blacklist has a higher priority than the whitelist. For example, an STA added to any type of blacklist (all-API/AP group/SSID MAC/OUI blacklist) cannot go online even if it is added to whitelists of other types.

<input type="checkbox"/>	MAC Address	Description	Operation
No Data			

Click **Based on SSID** or **Global** in the left pane to determine whether to configure a blacklist/whitelist globally or based on a specified SSID.

- **Global:** The configuration is based on an entire device. The device allows or denies STAs according to the blacklist/whitelist for all its SSIDs.
- **Based on SSID:** The device manages the access of STAs according to the configured blacklist/whitelist only for a specific SSID.

Figure 6-127 Blacklist/Whitelist Setting Dimensions



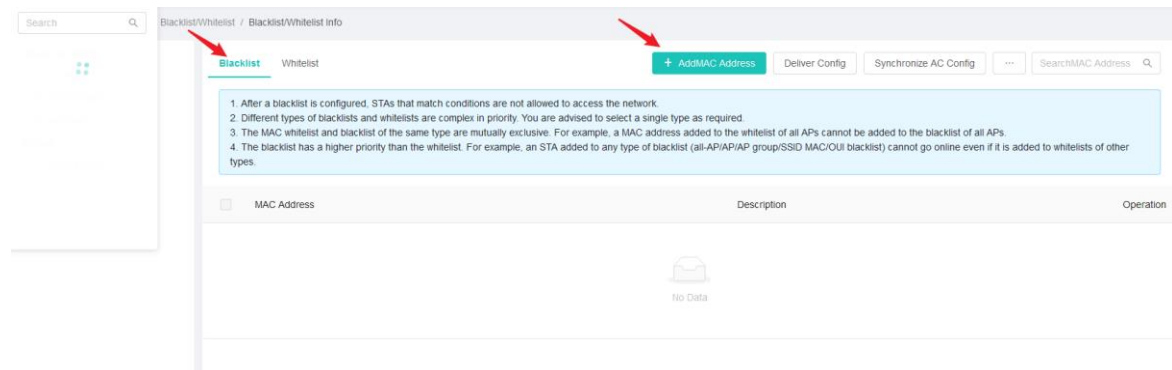
1. Blacklist

Click **Add MAC Address** to add a wireless device blacklist.

Caution

- (1) After a blacklist is configured, STAs that match conditions are not allowed to access the network.
- (5) Different types of blacklists and whitelists are complex in priority. You are advised to select a single type as required.
- (6) The MAC whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device.
- (7) The blacklist has a higher priority than the whitelist. For example, an STA added to any type of blacklist (system/AP/AP group/SSID MAC/OUI blacklist) cannot go online even if it is added to whitelists of other types.
- (8) If the blacklist is enabled, an online STA that matches the blacklist will be kicked offline immediately.

Figure 6-128 Creating a Blacklist



MAC addresses can be blacklisted based on OUIs or complete MAC addresses.

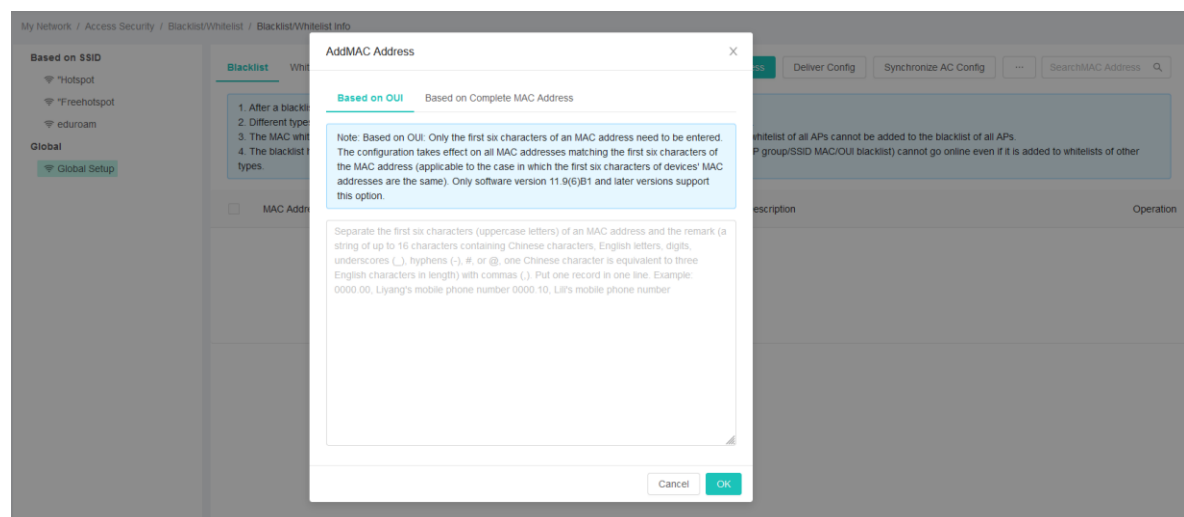
- Based on OUI

Only the first six characters of a MAC address need to be entered. The configuration takes effect on all MAC addresses matching the first six characters of the MAC address (applicable to the case in which the first six characters of devices' MAC addresses are the same). Multiple MAC addresses can be added at the same time, with one MAC address record in one row. MAC address remarks can be added. The remarks must be in the same line as MAC addresses and are separated from MAC addresses by commas.

⚠ Caution

Only software version RGOS11.9(6)B1 and later versions support the based on OUI mode.

Figure 6-129 Adding MAC Addresses Based on OUIs



Filling requirements:

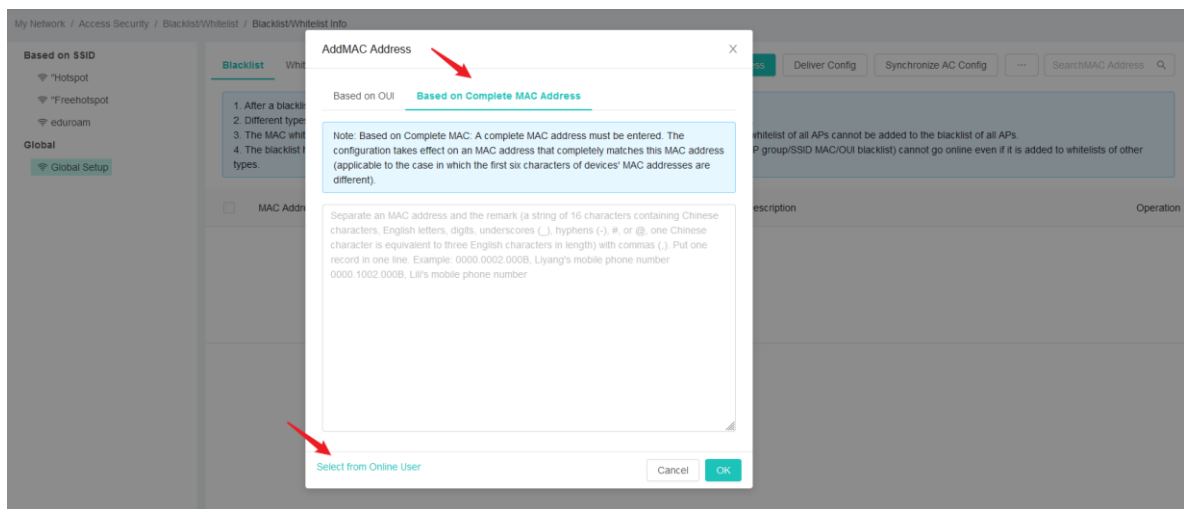
- **MAC:** (Required) The letters need to be capitalized.
- **Remark:** (Required) The value is a string of up to 16 characters containing Chinese characters, English

letters, digits, underscores (_), hyphens (-), #, or @. One Chinese character is equal to three English characters.

- Based on Complete MAC Address

A complete MAC address must be entered. The configuration takes effect on a MAC address that completely matches this MAC address (applicable to the case in which the first six characters of devices' MAC addresses are different). Multiple MAC addresses can be added at the same time, with one MAC address record in one row. MAC address remarks can be added. The remarks must be in the same line as MAC addresses and are separated from MAC addresses by commas.

Figure 6-130 Creating a Blacklist Based on Complete MAC Addresses



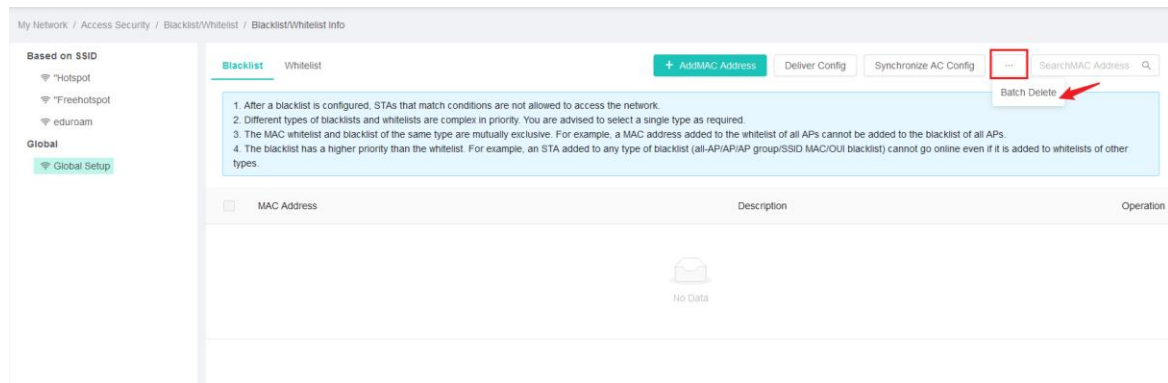
Filling requirements:

- **MAC:** (Required) The letters need to be capitalized.
- **Remark:** (Required) The value is a string of up to 16 characters containing Chinese characters, English letters, digits, underscores (_), hyphens (-), #, or @. One Chinese character is equal to three English characters.

To blacklist an online user, click **Select from Online User** in the lower left corner to add it to a blacklist rapidly.

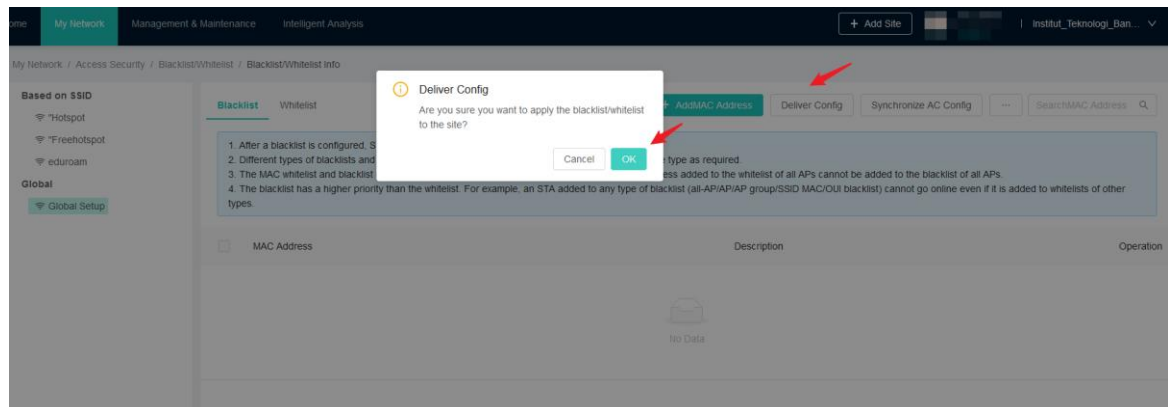
Users in a blacklist can be deleted separately or in batches.

Figure 6-131 Deleting Users from a Blacklist



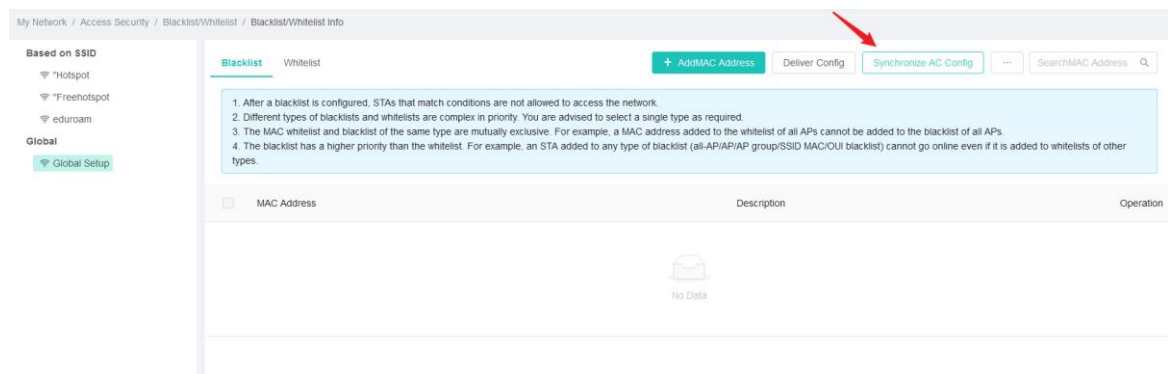
After a blacklist is configured, click **Deliver Config** to apply the blacklist to a site.

Figure 6-132 Delivering a Blacklist



Click **Synchronize AC Config** to synchronize configurations related to blacklist/whitelist (such as WLANs and SSIDs) on cloud APs or ACs to the WIS.

Figure 6-133 Synchronizing Device Configuration



2. Whitelist

Click the **Whitelist** tab page to switch to the whitelist configuration page. On this page, functions of adding MAC addresses, delivering configurations, synchronizing AC configurations, and deleting entries from the whitelist are the same as those on the **Blacklist** tab page. Pay attention to the following points when configuring a whitelist.

 **Caution**

- (1) After a whitelist is configured, only STAs that match conditions are allowed to access the network.
 - (2) If there is no data in the whitelist, all STAs are allowed to access the network. If there is data in the whitelist, STAs not listed in the whitelist are immediately banned from accessing the network.
 - (3) Different types of blacklists and whitelists are complex in priority. You are advised to select a single type as required.
 - (4) The MAC whitelist and blacklist of the same type are mutually exclusive. For example, a MAC address added to the whitelist of a device cannot be added to the blacklist of the device.
 - (5) The blacklist has a higher priority than the whitelist. For example, an STA added to any type of blacklist (system/AP/AP group/SSID MAC/OUI blacklist) cannot go online even if it is added to whitelists of other types.
 - (6) When an entry is added to the whitelist, other STAs will not be kicked offline.
-

6.8 Alarm Management

6.8.1 Active Alarm

Choose **My Network > Alarm Management > Active Alarm** to go to the active alarm management page.

1. Alarm List

The active alarm list provides information about uncleared alarms, including the alarm severity, alarm name, alarm type, alarm source, acknowledgment status, clearing status, repetition times, occurrence time, update time, and remarks.

In the list, you can search for alarm records by alarm time range, alarm source, alarm severity, alarm type, acknowledgment status, and clearing status.

Figure 6-134 Alarm List

Severity	Name	Type	Source	Ack Status	Clearance Status	Repetition Times	Occurrence Time	Update Time	Remark	Operation
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-06 02:04:38	-	GI0/39 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 20:35:43	-	GI0/14 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 15:57:44	-	GI0/14 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 10:05:12	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 10:04:36	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[W56512-[G1M70M000]...	Unacked	Uncleared	0	2022-08-04 20:04:17	-	V11 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:20:57	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:20:23	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:19:32	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:13:47	-	GI0/41 Down	More

Some fields in the list are described as follows:

- **Severity:** The alarm severity is critical, major, minor, and warning in descending order.
- **Type:** Alarms include communication alarms, environment alarms, QoS alarms, device alarms, processing error alarms, and OMC alarms.
- **Repetition Times:** It indicates the number of occurrence times of an alarm since the first occurrence of the alarm. After the alarm is cleared, the count will be reset.

2. Alarm Details

Click **More** and select **Details** in the **Operation** column of the list to view details about an alarm.

Figure 6-135 Alarm Details (01)

Severity	Name	Type	Source	Ack Status	Clearance Status	Repetition Times	Occurrence Time	Update Time	Remark	Operation
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-06 02:04:38	-	GI0/39 Down	More Details Ack Clear
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 20:35:43	-	GI0/14 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 15:57:44	-	GI0/14 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 10:05:12	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 10:04:36	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[W56512-[G1M70M000]...	Unacked	Uncleared	0	2022-08-04 20:04:17	-	V11 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:20:57	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:20:23	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:19:32	-	GI0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:13:47	-	GI0/41 Down	More

Figure 6-136 Alarm Details (02)

My Network / Alarm Management / Active Alarm / Active Alarm Info / Alarm Details

Alarm Details

Number	1234942570041ALARM_TP_DEVICE_INTERFACE_DOWN1659722678	Suggested Action	Status
Name	Device Interface Down Major		Unacked Uncleared
Type	Device Alarm		
Source	[S2910C-48GT2XS-HP-E]-[1234942570041]-[SWITCH]		
Repetition Times	0		Ack Clear
Cause			
Symptom	This alarm is generated when the device interface changes from up to down.		
Remark	Gi0/39 Down		

3. Alarm Acknowledgment

Click **More** and select **Ack** in the **Operation** column of the list to acknowledge an alarm, indicating that the alarm is identified. You can select multiple alarms and click **Ack** to bulk acknowledge the alarms. You can click **Ack** on the **Alarm Details** page to acknowledge an alarm.

Figure 6-137 Alarm Acknowledgment

My Network / Alarm Management / Active Alarm / Active Alarm Info

Active Alarm

Ack
Cancel Ack
Clear
Export
Start date - End date [v]
Search Alarm Source [q]

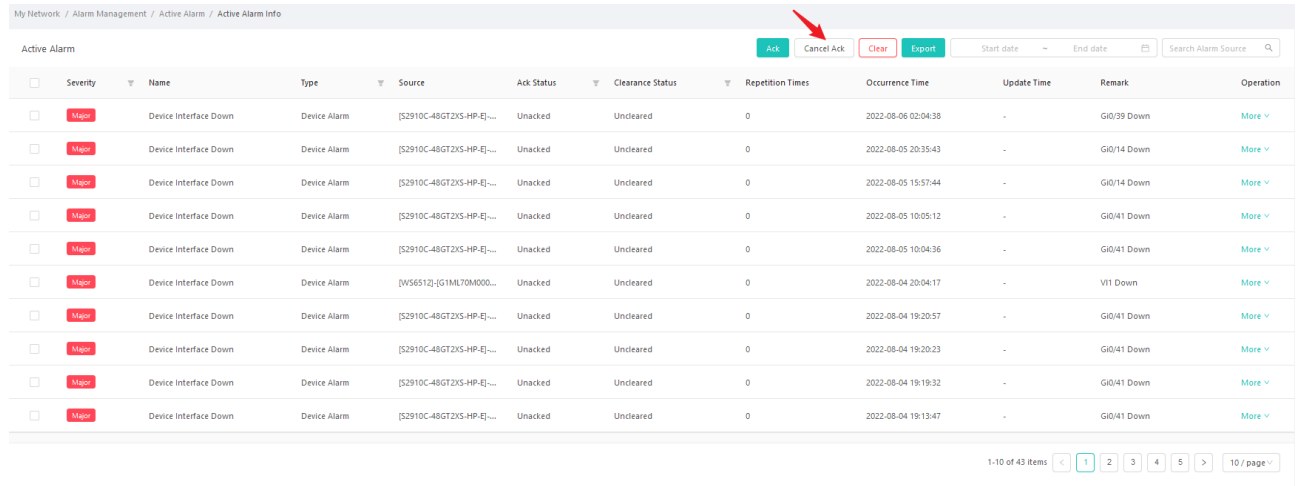
<input type="checkbox"/>	Severity	Name	Type	Source	Ack Status	Clearance Status	Repetition Times	Occurrence Time	Update Time	Remark	Operation
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-05 02:04:38	-	Gi0/39 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-05 20:35:43	-	Gi0/14 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-05 15:57:44	-	Gi0/14 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-05 10:05:12	-	Gi0/41 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-05 10:04:36	-	Gi0/41 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[W56512]-[G1ML70M000...	Unacked	Uncleared	0	2022-08-04 20:04:17	-	V11 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-04 19:20:57	-	Gi0/41 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-04 19:20:23	-	Gi0/41 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-04 19:19:32	-	Gi0/41 Down	More v
<input type="checkbox"/>	Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]-...	Unacked	Uncleared	0	2022-08-04 19:13:47	-	Gi0/41 Down	More v

1-10 of 43 items < 1 2 3 4 5 > 10/page

4. Canceling Acknowledgment

The acknowledgment of alarms can be bulk cleared to set the alarms to the unacknowledged state.

Figure 6-138 Canceling Acknowledgment



My Network / Alarm Management / Active Alarm / Active Alarm Info

Active Alarm

Buttons: Ack, Cancel Ack, Clear, Export

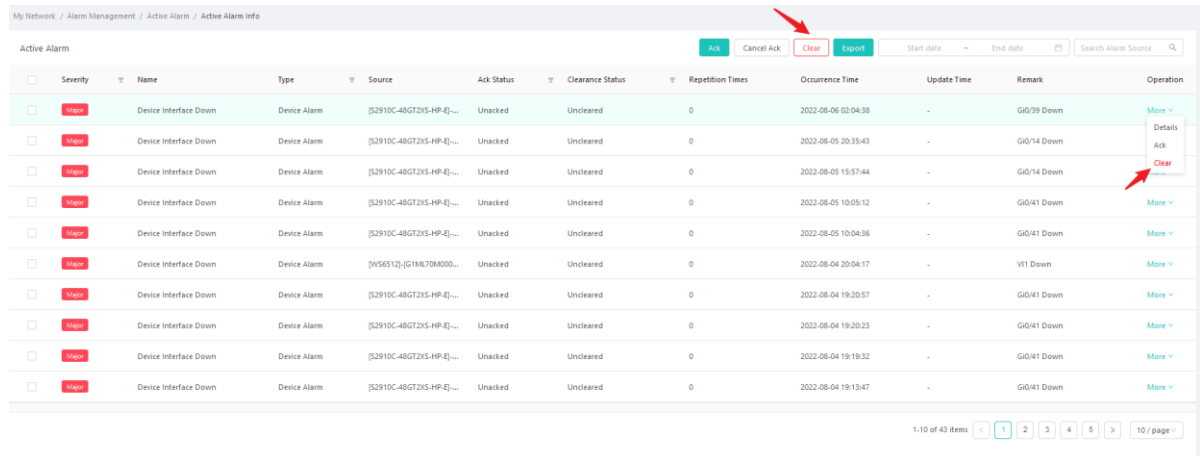
Severity	Name	Type	Source	Ack Status	Clearance Status	Repetition Times	Occurrence Time	Update Time	Remark	Operation
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-06 02:04:38	-	Gi0/39 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 20:35:43	-	Gi0/14 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 15:57:44	-	Gi0/14 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 10:05:12	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 10:04:36	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[W56512]-[G1ML70M000]...	Unacked	Uncleared	0	2022-08-04 20:04:17	-	V11 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:20:57	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:20:23	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:19:32	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:13:47	-	Gi0/41 Down	More

1-10 of 43 items | 1 2 3 4 5 | 10/page

5. Clearing an Alarm

Click **More** and select **Clear** in the **Operation** column of the list to clear an alarm. Cleared alarms will be added to the history alarm list. You can bulk clear alarms. You can click **Clear** on the **Alarm Details** page to clear an alarm.

Figure 6-139 Clearing an Alarm



My Network / Alarm Management / Active Alarm / Active Alarm Info

Active Alarm

Buttons: Ack, Cancel Ack, Clear, Export

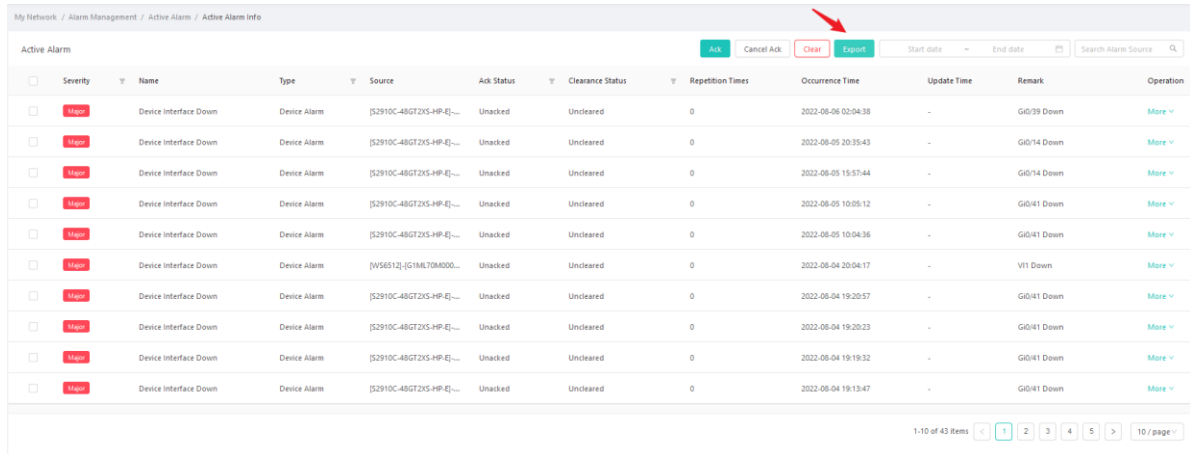
Severity	Name	Type	Source	Ack Status	Clearance Status	Repetition Times	Occurrence Time	Update Time	Remark	Operation
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-06 02:04:38	-	Gi0/39 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 20:35:43	-	Gi0/14 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 15:57:44	-	Gi0/14 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 10:05:12	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-05 10:04:36	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[W56512]-[G1ML70M000]...	Unacked	Uncleared	0	2022-08-04 20:04:17	-	V11 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:20:57	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:20:23	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:19:32	-	Gi0/41 Down	More
Major	Device Interface Down	Device Alarm	[S2910C-48GT2XS-HP-E]...	Unacked	Uncleared	0	2022-08-04 19:13:47	-	Gi0/41 Down	More

1-10 of 43 items | 1 2 3 4 5 | 10/page

6. Exporting Alarms

Click **Export** to export the alarm list to the local device.

Figure 6-140 Exporting Alarms



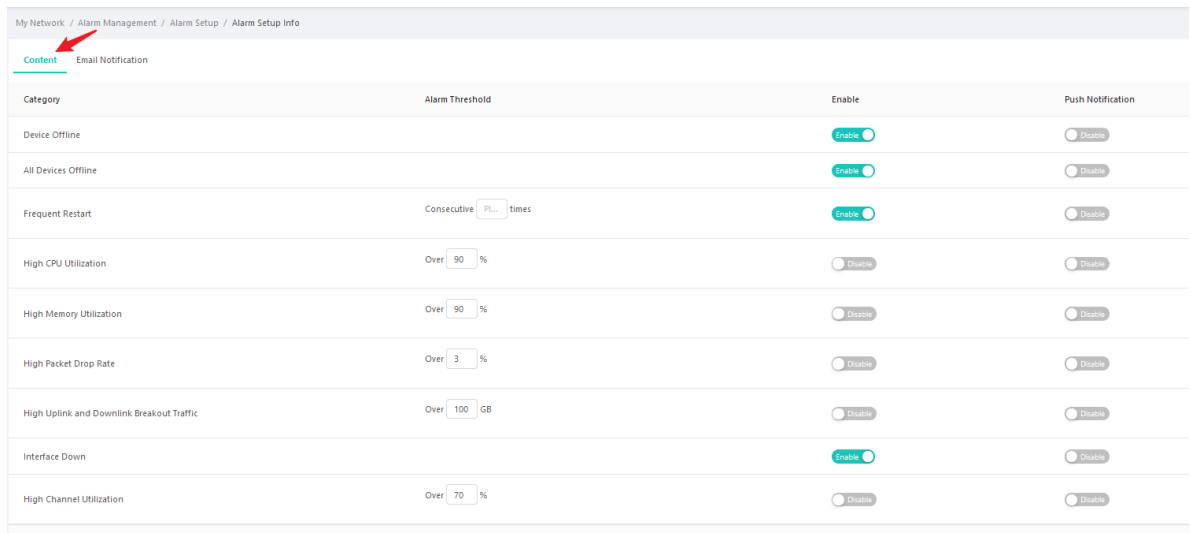
6.8.2 Alarm Setup

The alarm setup function allows you to configure the alarm content, thresholds, detection switch, and push switch. Alarm information can be pushed by email, WeCom, and DingTalk.

1. Alarm Content

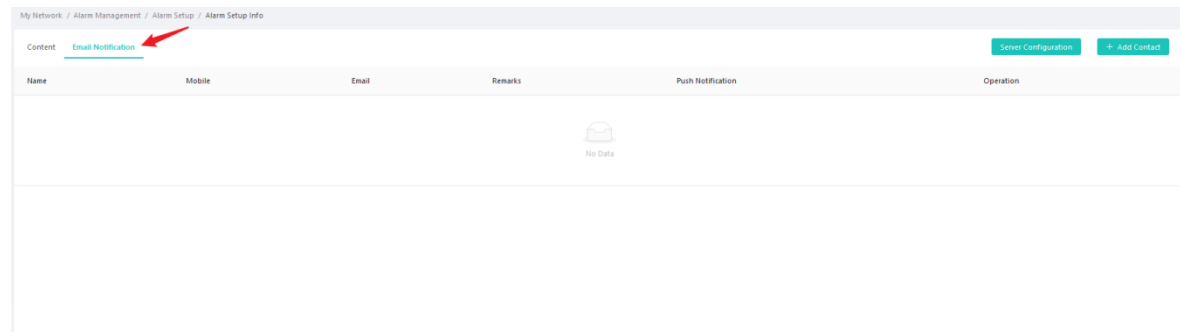
On the **Content** tab page, you can define alarm thresholds, alarm switch, and push switch for different categories of alarms. If the value of an alarm category exceeds the current threshold and the alarm function is enabled, the system generates an alarm record.

Figure 6-141 Setting Alarm Content

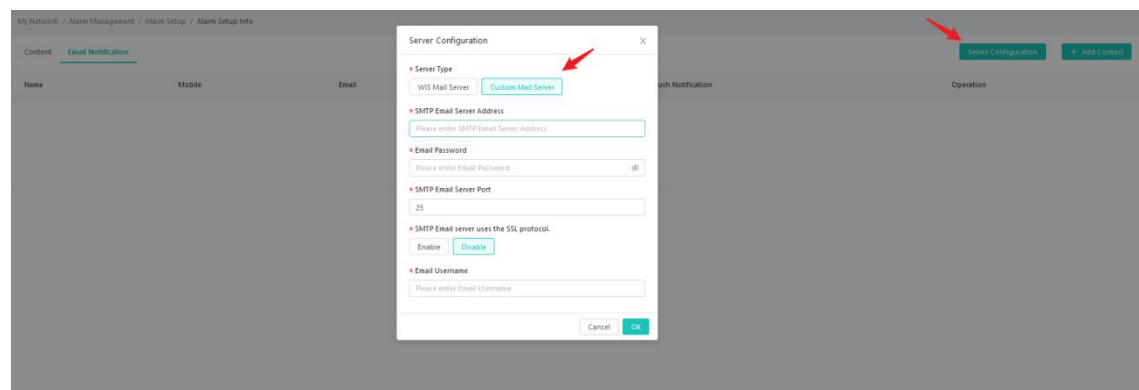


2. Email Notification

Email notification includes two configuration items: **Server Configuration** and **Add Contact**. The two configuration items are described as follows:

Figure 6-142 Email Notification**(1) Server Configuration**

Click **Server Configuration** to configure the server of the email box that pushes alarms. There are two types of email servers: WIS email server and custom email server. The WIS email server does not need to be configured. The default email server of the WIS is used.

Figure 6-143 Server Configuration

The custom server configuration is described as follows:

- **SMTP Email Server Address:** (Required) Indicates the server address of an email box that pushes alarms. Enter the actual server address.
- **Email Password:** (Required) Indicates the email password for pushing alarms.
- **SMTP Email Server Port:** (Required) Indicates the server port that sends emails. Enter the actual port ID.
- **SMTP Email server uses the SSL protocol:** (Required) Indicates whether the SMTP service uses the SSL protocol for encryption.
- **Email Username:** Indicates the email username for pushing alarms.

i Note

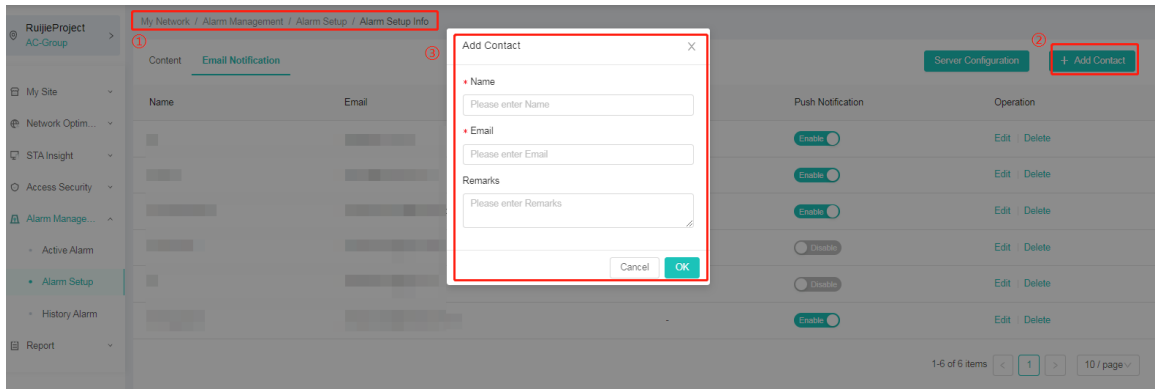
The Simple Mail Transfer Protocol (SMTP) server address is a set of specifications used to transmit mails from the source address to the destination address. It controls the transfer mode of mails. The SMTP

protocol belongs to the TCP/IP protocol suite and helps each PC find the next destination when sending or forwarding mails. The SMTP server is a mail transfer server that complies with the SMTP protocol. Different mail providers use different SMTP server addresses.

(2) Contact Configuration

Click **Add Contact** to add an object, to which alarm emails are to be pushed.

Figure 6-144 Adding a Contact

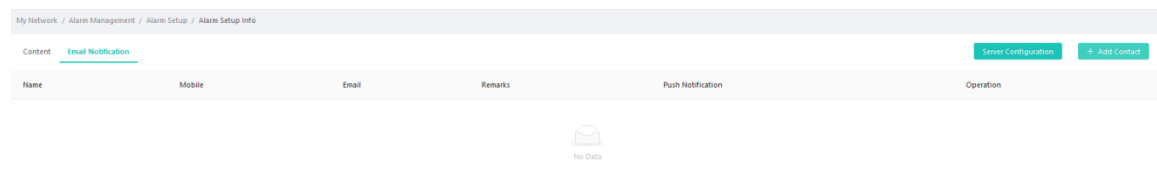


The contact configuration is described as follows:

- **Name:** (Required) Enter the name of a contact. It is a string of up to 50 characters containing only Chinese characters, letters, digits, underscores (_), hyphens (-), @, and &.
- **Email:** (Required) Enter the contact's email address for receiving pushed alarms.
- **Remarks:** (Optional) Enter the remarks of the contact. The value is a string of no more than 200 characters.

In the contact list, you can configure the push switch, edit contacts, and delete contacts.

Figure 6-145 Contact List



6.8.3 History Alarm

On the **Historical Alarm** page, you can view cleared alarms and acknowledged history alarms.

1. Alarm List

In the history alarm list, you can filter alarm records by alarm time range, alarm severity, alarm type, acknowledgment status, and clearing status, and search for alarms by alarm source.

Figure 6-146 History Alarm List

Severity	Name	Type	Source	Ack Status	Clearance Status	Repetition Times	Occurrence Time	Update Time	Remark	Operation
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-06 18:25:51 Clear	0	2022-08-06 17:38:16	-	-	Details
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-06 06:33:10 Clear	0	2022-08-06 06:26:26	-	-	Details
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-06 05:36:42 Clear	0	2022-08-06 04:56:32	-	-	Details
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-06 04:40:22 Clear	0	2022-08-06 04:11:12	-	-	Details
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-05 03:23:27 Clear	0	2022-08-04 22:37:12	-	-	Details

2. Alarm Details

Click **Details** in the **Operation** column of the list to view details about an alarm.

Figure 6-147 Alarm Details (1)

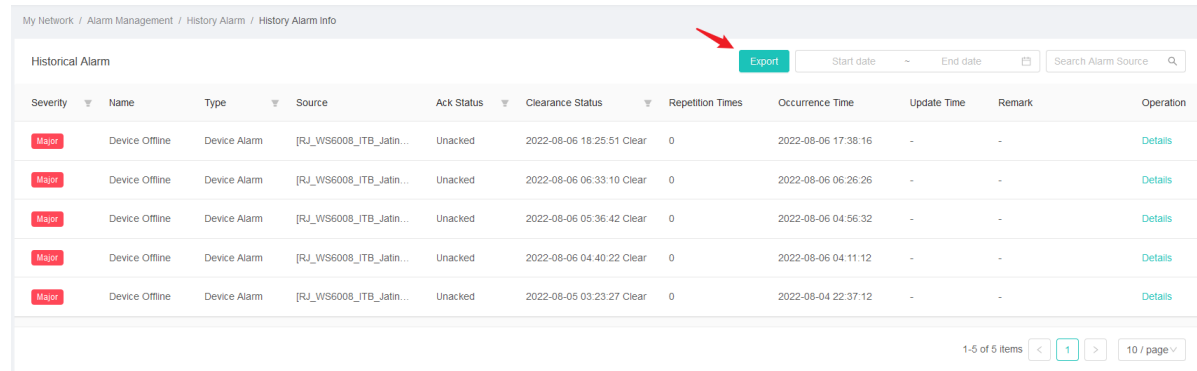
Figure 6-148 Alarm Details (2)

Number	---	Suggested Action	Status
Name			Unacked
Type			Uncleared
Source			
Repetition Times			
Cause			
Symptom			
Remark			

3. Exporting Alarms

Click **Export** to export the alarm list to the local device.

Figure 6-149 Exporting Alarms



My Network / Alarm Management / History Alarm / History Alarm Info

Historical Alarm [Export](#) Start date ~ End date Search Alarm Source

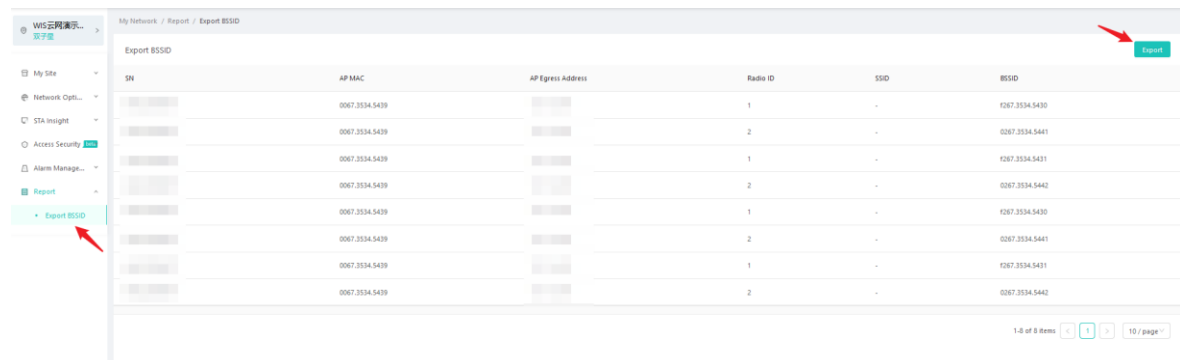
Severity	Name	Type	Source	Ack Status	Clearance Status	Repetition Times	Occurrence Time	Update Time	Remark	Operation
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-06 18:25:51 Clear	0	2022-08-06 17:38:16	-	-	Details
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-06 06:33:10 Clear	0	2022-08-06 06:26:26	-	-	Details
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-06 05:36:42 Clear	0	2022-08-06 04:56:32	-	-	Details
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-06 04:40:22 Clear	0	2022-08-06 04:11:12	-	-	Details
Major	Device Offline	Device Alarm	[RJ_WS6008_ITB_Jatin...	Unacked	2022-08-05 03:23:27 Clear	0	2022-08-04 22:37:12	-	-	Details

1-5 of 5 items < 1 > 10 / page

6.9 Report

Choose **My Network > Report** to go to the report management page. On the **Export BSSID** page, click **Export** in the upper right corner of the page to export all BSSID information to the local device.

Figure 6-150 Exporting BSSIDs



My Network / Report / Export BSSID

Export BSSID [Export](#)

SN	AP MAC	AP Egress Address	Radio ID	SSID	BSSID
	0067.3534.5439		1	-	0267.3534.5430
	0067.3534.5439		2	-	0267.3534.5441
	0067.3534.5439		1	-	0267.3534.5431
	0067.3534.5439		2	-	0267.3534.5442
	0067.3534.5439		1	-	0267.3534.5430
	0067.3534.5439		2	-	0267.3534.5441
	0067.3534.5439		1	-	0267.3534.5431
	0067.3534.5439		2	-	0267.3534.5442

1-8 of 8 items < 1 > 10 / page

7 Management and Maintenance

7.1 Organizational Planning

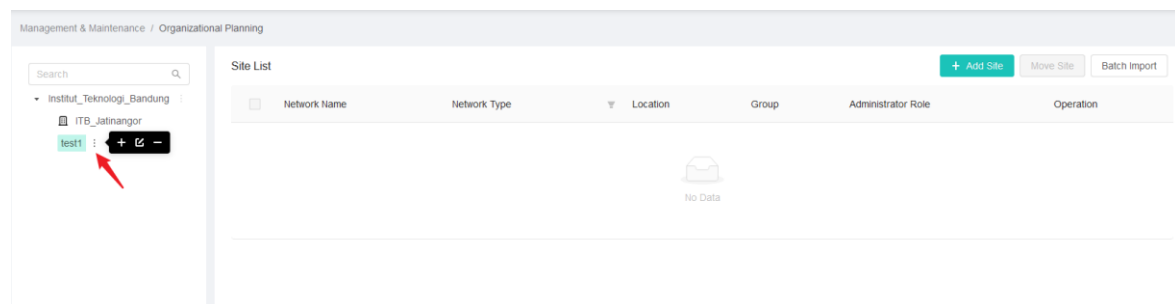
WIS Cloud Management supports the unified management of multiple branches and personalized organizational planning.

Choose **Management & Maintenance > Organizational Planning**. In the organization tree, you can add branches at up to 11 levels. You can also edit and delete branches.

Caution

If a branch has a sub-branch or site, it cannot be deleted. To delete it, you need to delete the sub-branch and site first.

Figure 7-1 Organization Tree



7.1.1 Adding a Site

Site is the smallest unit of network management. A branch can be added with multiple sites. Click **Add Site**, enter the following information, and click **OK**.

- **Site Name:** (Required) The value can contain no more than 20 characters of letters, digits, underscore (_), hyphen (-), at sign (@), and ampersand (&).
- **Time Zone:** (Required) The default time zone of a site is **(GMT+8:00)China**.
- **Location:** (Optional) You can enter a location or select one from the drop-down list box.
- **Network Type:** (Required) The default option is **Common**. Other available options include **Small Network** and **Large Network**.
- **Industry:** (Optional) You can select an industry from the drop-down list box.

You can add sites in batches or move sites to another branch.

Figure 7-2 Adding a Site

Add Site

After creation, you can add administrators and configuration templates on the site homepage.

Network Type

Common Small Network Large Network

* Site Name

Please enter Site Name

Cancel OK

7.1.2 Editing a Site

You can click **Edit** in the **Operation** column to edit an existing site.

Figure 7-3 Editing a Site

Edit Site

Network Type

Common Small Network Large Network

* Site Name

AC-Group

Cancel OK

7.1.3 Deleting a Site

To delete a site, click **Delete** in the **Operation** column. In the displayed confirmation box, click **OK**.

⚠ Caution

When a device exists under a site, the site cannot be directly deleted. You need to delete the device before deleting the site.

Figure 7-4 Deleting a Site

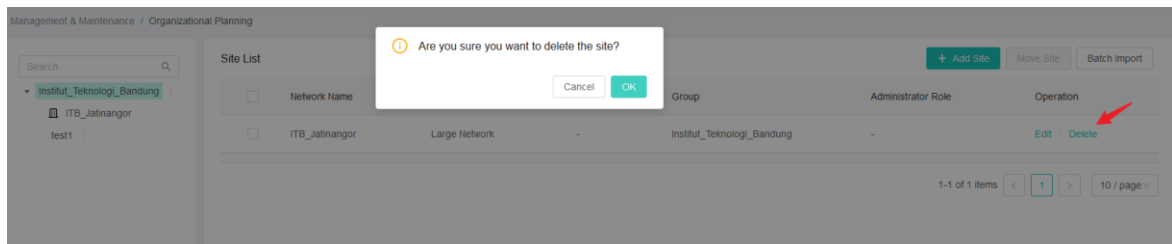
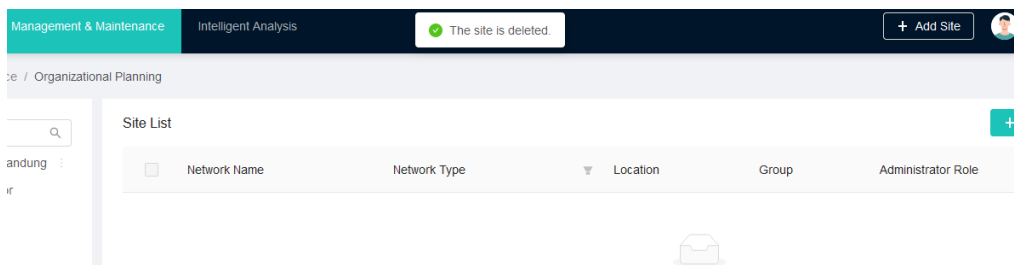


Figure 7-5 Site Deleted



7.2 Configuration Management

On WIS Cloud Management, you can manage device configuration, mainly including deployment configuration, network optimization configuration, common configuration tasks, application configuration tasks, configuration backup, blacklist and whitelist.

7.2.1 Configuration Template

A configuration template contains preset configurations delivered to devices based on the site, that is, configurations sent to a device when the device goes online. After a configuration template is bound with a site, when a device goes online for the first time at the site, the device will automatically obtain the configuration preset in the template, and complete initial configuration.

1. Template List

Choose **Management & Maintenance > Configuration > Template**. A template list displays **Template Name**, **Template Description**, **Application Site**, **Creation Time**, and **Update Time**. You can customize the number of templates displayed on each page of the list, and sort the templates by **Creation Time** or **Update Time**.

Figure 7-6 Configuration Template List

Template Name	Template Description	Application Site	Creation Time	Update Time	Operation
[redacted]	-	0	2022-07-15 16:10:16	2022-07-15 08:10:16	Edit View Result Bind Site

You can click a number in the **Application Site** column to display information about the application sites where the template is applied.

Figure 7-7 Application Site

Template Name	Template Description	Application Site	Creation Time	Update Time
[redacted]	-	0	2022-07-15 16:10:16	2022-07-15 08:10:16

Figure 7-8 Displaying Site List of a Template

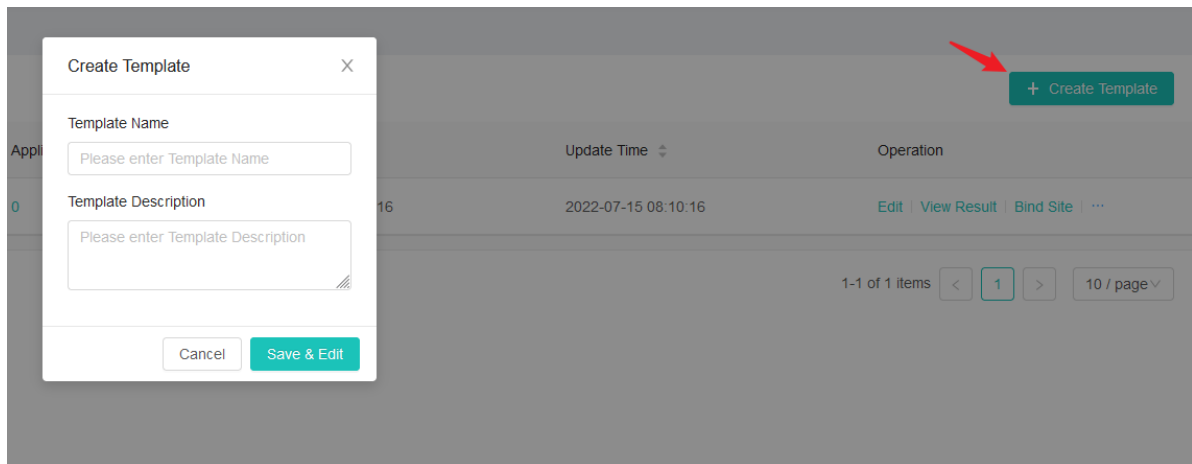
Site List

Group	Name	Site Type
No Data		

2. Creating a Template

Click **Create Template** to enter the new template configuration page.

Figure 7-9 Creating a Template



Configuration description:

- **Template Name:** (Optional) The value can contain no more than 50 characters of letters, digits, underscore (_), hyphen (-), at sign (@), and ampersand (&).
- **Template Description:** (Optional) The value can contain no more than 400 characters.

Click **Save & Edit** to edit the detailed information of the template.

3. Editing a Template

You can click **Edit** in the **Operation** column of the template list to edit the configuration of the specified template.

Figure 7-10 Editing a Template 1

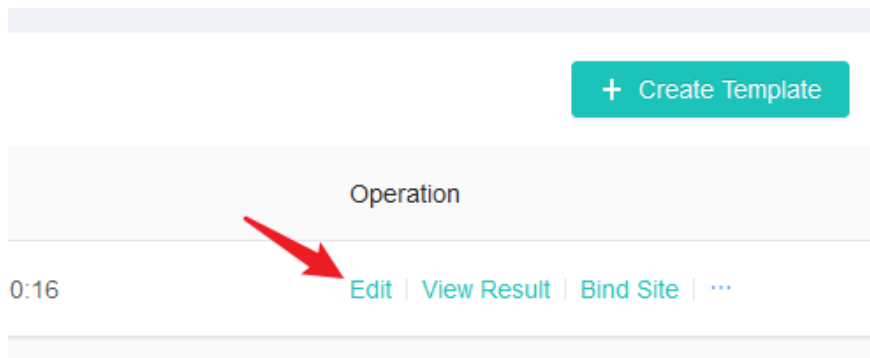


Figure 7-11 Editing a Template 2

Management & Maintenance / Configuration / Template / Edit Template

Edit Template + Save

Template Name:

Template Description:

WLAN Configuration CLI List + Add SSID Deliver Config

WLAN ID	SSID	Encryption Mode	SSID Hiding	Forwarding Mode	AssociateRadio	Operation
No Data						

Configuration description:

- **Template Name:** (Optional) The value can contain no more than 50 characters of letters, digits, underscore (_), hyphen (-), at sign (@), and ampersand (&).
- **Template Description:** (Optional) The value can contain no more than 400 characters.

After the editing, click **Save** in the upper right corner to save the modification.

The configuration in a template includes **WLAN Configuration** (SSID) and **CLI List**:

(1) WLAN Configuration

- **WLAN List**

A WLAN list displays **WLAN ID**, **SSID**, **Encryption Mode**, **SSID Hiding**, **Forwarding Mode**, and **AssociateRadio**. You can filter data in the list by **Encryption Mode** and **Forwarding Mode**.

Caution

WLAN configuration is effective only on cloud APs, and the priority is lower than that of CLI configuration.

Figure 7-12 WLAN Configuration List

Management & Maintenance / Configuration / Template / Edit Template

Edit Template + Save

Template Name:

Template Description:

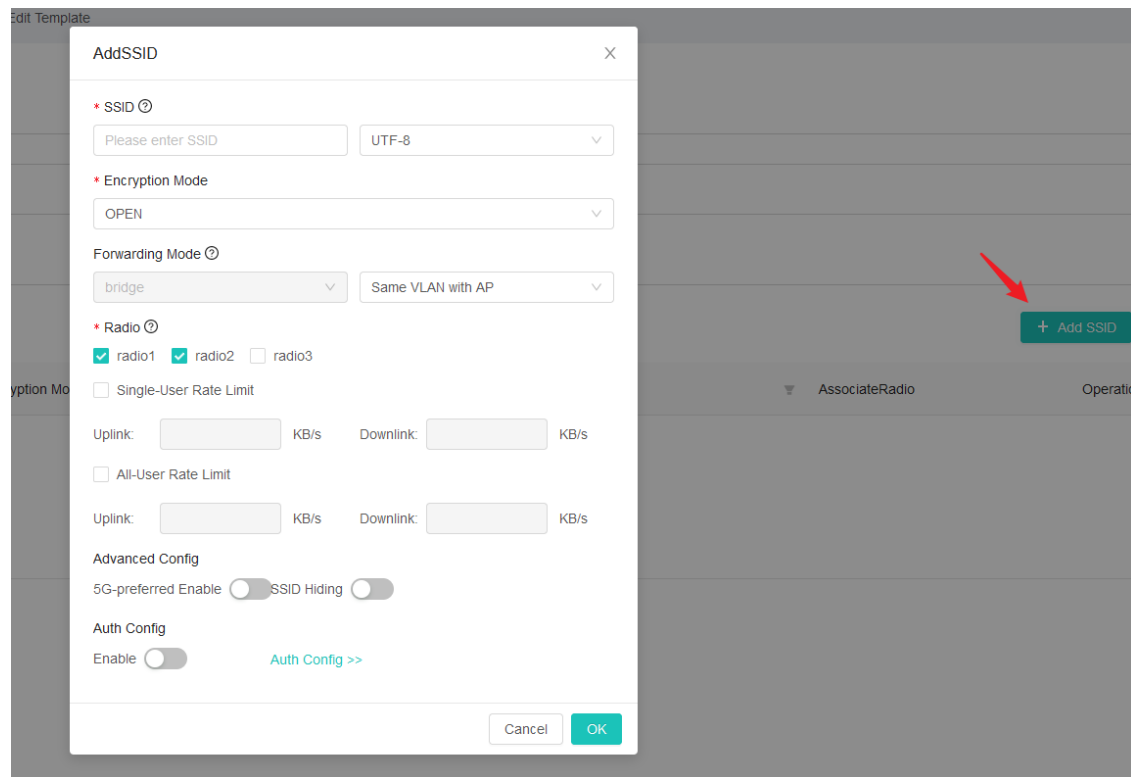
WLAN Configuration CLI List + Add SSID Deliver Config

WLAN ID	SSID	Encryption Mode	SSID Hiding	Forwarding Mode	AssociateRadio	Operation
No Data						

- **Adding an SSID**

Click **Add SSID** to add a new WLAN configuration in the template.

Figure 7-13 Adding an SSID



SSID configuration description:

- **SSID:** (Required) You also need to select the encoding format, which is **UTF-8** by default and can be changed to **GBK**. If an SSID contains Chinese characters, garbled characters are displayed when an STA does not support UTF-8 encoding format.
- **Encryption Mode:** (Required) Select a value from the drop-down list. The options include **OPEN**, **WPA-PSK**, **WPA2-PSK**, and **WPA-PSK/WPA2-PSK**. When an encryption mode other than **OPEN** is selected, you need to enter the password.

Note

OPEN: Indicates the open non-encryption authentication mode.

WPA-PSK: Indicates the authentication mode using wired equivalent privacy (WEP) pre-shared keys. It adopts the TKIP encryption mode and users are authenticated when they use correct pre-shared keys.

WPA2-PSK: Indicates a new encryption authentication mode based on WPA-PSK. It adopts the CCMP encryption mode and is compatible with the TKIP encryption mode.

- **Forwarding Mode:** The bridge mode is supported by default. To switch to the NAT mode, run CLI commands. You can set **VlanType** to **Same VLAN with AP** or use other VLANs. If you select other VLANs, enter the VLAN ID. The VLAN ID range is from 2 to 232 and from 234 to 4094.

- **Radio:** (Required) You can select one or more radios from radio1 to radio3. You can select **Single-User Rate Limit** and **All-User Rate Limit** and set uplink and downlink rate limits for them separately.

⚠ Caution

If **radio3** is selected, the SSID of radio3 is effective only when radio3 is in access mode and not effective when radio3 is in scan mode.

- **Advanced Config:** (Optional) Advanced configuration includes **5G-preferred** and **SSID Hiding**. **5G-preferred** indicates that, when a radio provides both 2.4 GHz and 5 GHz bands and an STA supports both 2.4 GHz access and 5 GHz access, the STA connects to the 5 GHz band preferentially. **SSID Hiding** indicates that wireless networks are hidden and network signals cannot be searched out by STAs.

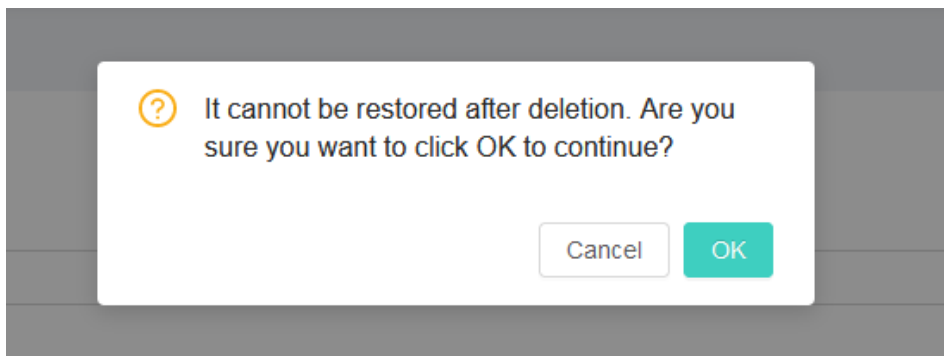
- **Editing an SSID**

To change the configuration of an added SSID, click **Edit** in the **Operation** column of the WLAN list. The process of editing an SSID is similar to that of adding an SSID, and is omitted here.

- **Deleting an SSID**

To delete an SSID, click **Delete** in the **Operation** column of the WLAN list.

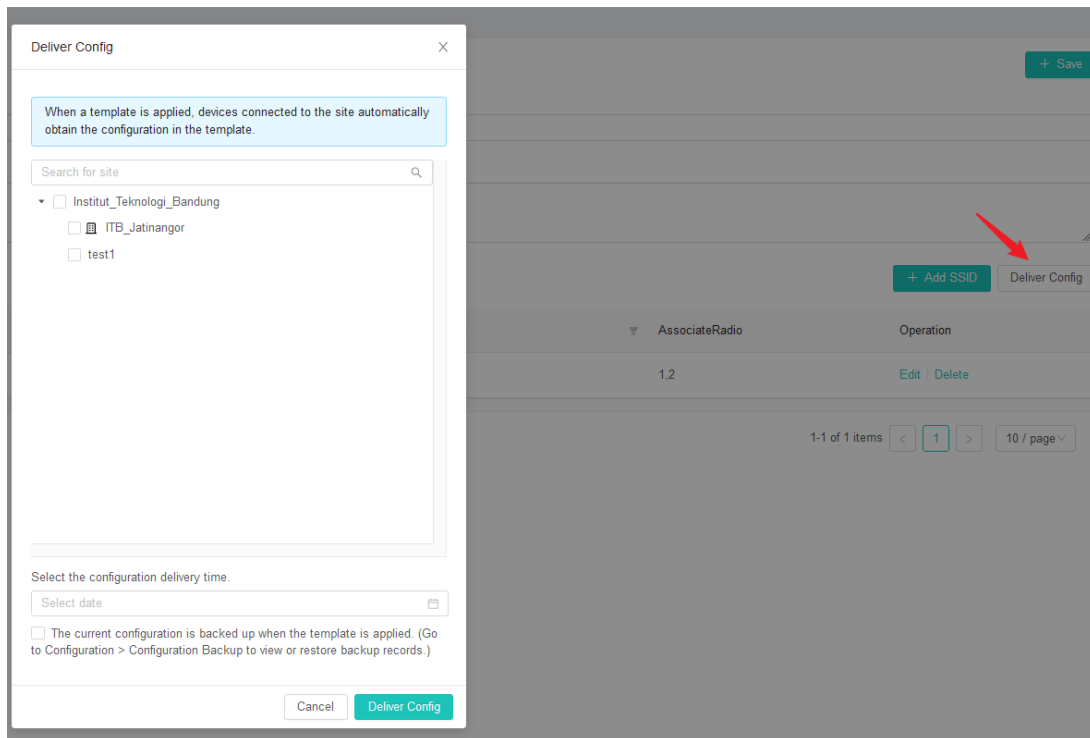
Figure 7-14 Deleting an SSID



- **Delivering the Configuration**

A new configuration takes effect only on STAs that go online after the configuration is added. To make the configuration effective on existing STAs, click **Deliver Config** to deliver the configuration to devices at the current site.

Figure 7-15 Delivering the Configuration



Parameters for configuration delivery are described as follows:

- **Site:** (Required) Select one or more sites in the site tree to apply the template.
- **Configuration delivery time:** (Optional) You can set the time to deliver the template configuration to devices. If no time is set, the configuration is delivered immediately.
- **Backup:** (Optional) You can select whether to back up the current configuration of the site when the configuration template is applied to the site. If you select the check box, you can view or restore backup records in **Configuration Backup**.

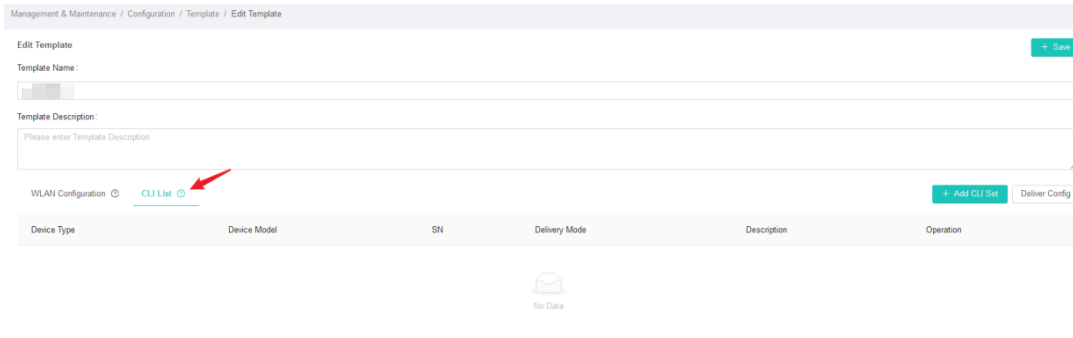
(2) CLI configuration

Click **CLI List** to switch to CLI configuration.

- **CLI list**

A CLI list displays **Device Type**, **Device Model**, **SN**, **Delivery Mode**, and **Description**.

Figure 7-16 CLI List



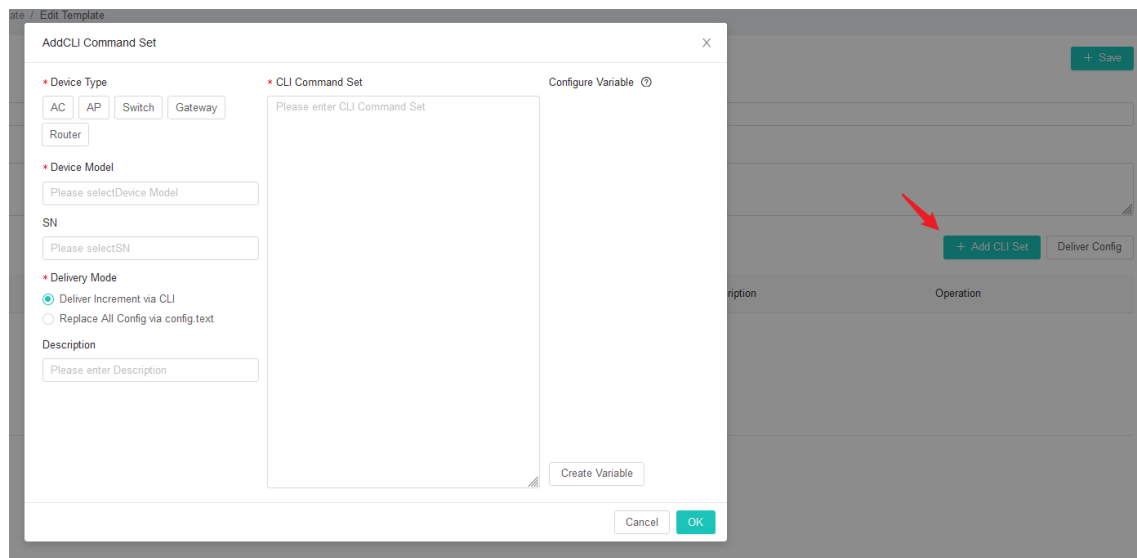
● **Adding a CLI Set**

Click **Add CLI Set** to add a customized CLI set to the configuration template.

Caution

- A device model that already has CLI configuration cannot be selected repeatedly.
- If the configuration for all devices and the configuration for a single device model are present simultaneously, only the configuration for a single device model is delivered to this model.

Figure 7-17 Adding a CLI Set



Configuration description:

- **Device Type:** (Required) Select the type of devices, to which the CLI command set is to be delivered. The options include AC, AP, Switch, Gateway, and Router. You can select only one of them.
- **Device Model:** (Required) Select the model of the devices, to which the CLI command set is to be

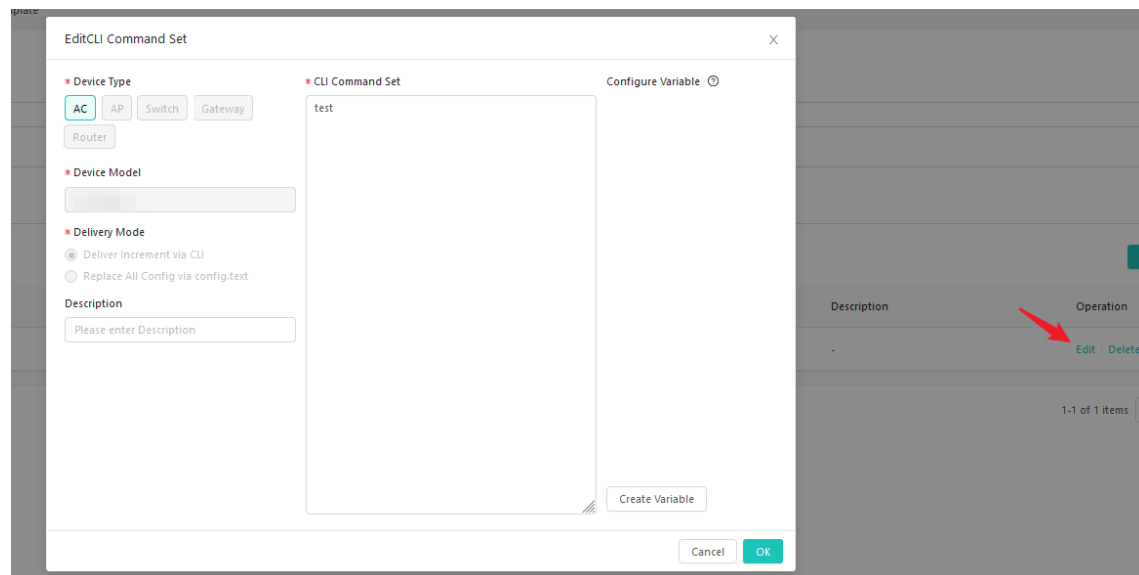
delivered. Select a device model from the drop-down list. Multiple models can be selected.

- **SN:** (Optional) Select an existing SN from the drop-down list. If an SN is selected, the command set will be delivered only to the device matching the SN. If no SN is selected, the command set will be delivered based on the selected device model.
- **Delivery Mode:** (Required) APs do not support the delivery mode of **Replace All Config via config.txt**. In **Deliver Increment via CLI** mode, the device incrementally executes the customized CLI command set based on the existing configuration. This mode is applicable to scenarios requiring certain incremental configuration. In **Replace All Config via config.txt** mode, the device configuration file **config.txt** is directly replaced. Then, the device automatically restarts to make the configuration effective. This mode is applicable to the following scenarios:
 - Scenarios where the entire device configuration needs to be replaced
 - Scenarios where incremental configuration cannot meet the requirements, for example, incremental configuration will cause network path change (device disconnection)
 - Scenarios where various interactions and command conversions are involved (causing interaction and command identification timeout)
- **CLI Command Set:** (Required) Enter the CLI command set customized for the device.
- **Description:** (Optional) Enter a description of the command set. It can be used as a remark.

● Editing a CLI Set

To change the configuration of an added CLI set, click **Edit** in the **Operation** column of the CLI list. On the **Edit CLI Command Set** page, you can edit only **CLI Command Set** and **Description**. To change **Device Type** and **Device Model**, add a new CLI command set.

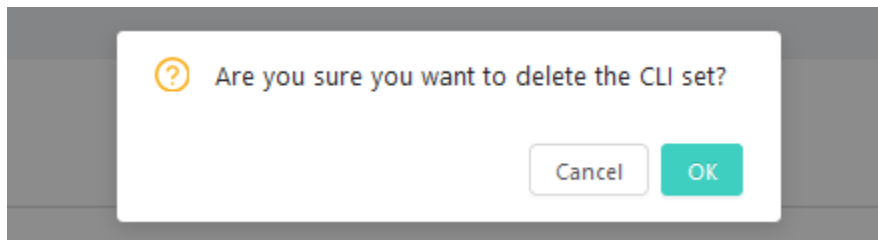
Figure 7-18 Editing a CLI Set



● Deleting a CLI Set

To delete a CLI set, click **Delete** in the **Operation** column of the CLI list.

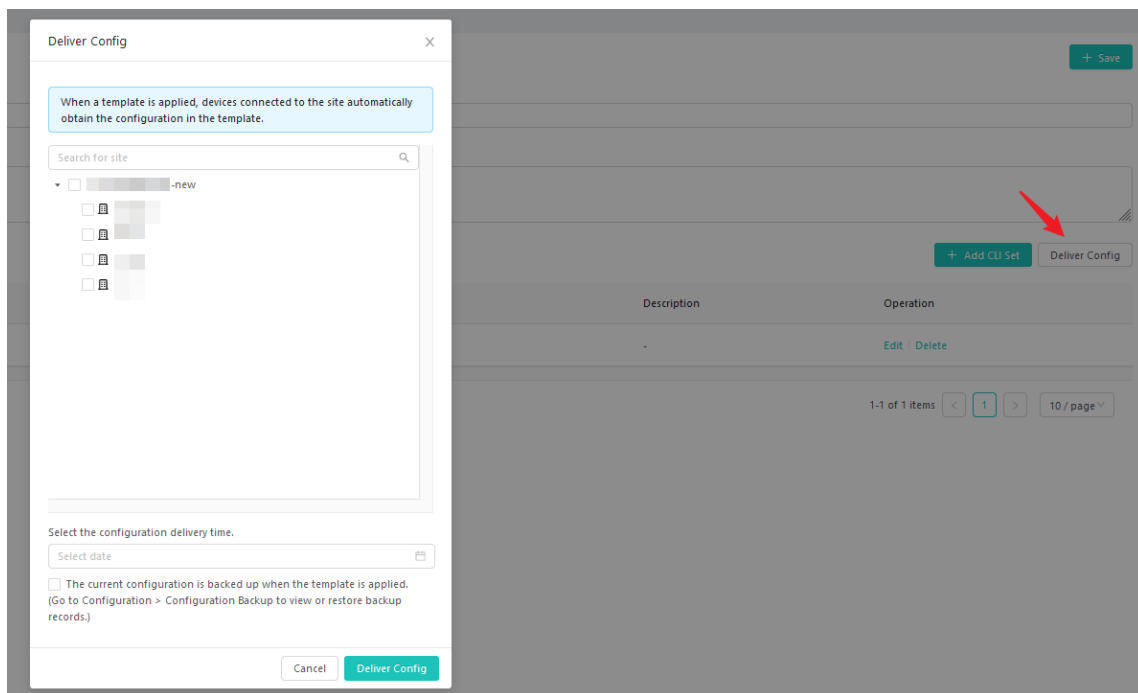
Figure 7-19 Deleting a CLI Set



- **Delivering the Configuration**

A new configuration takes effect only on STAs that go online after the configuration is added. To make the configuration effective on existing STAs, click **Deliver Config** to deliver the configuration to devices at the current site.

Figure 7-20 Delivering CLI Set Configuration



Parameters for configuration delivery are described as follows:

- **Site:** (Required) Select one or more sites in the site tree to apply the template.
- **Configuration delivery time:** (Optional) You can set the time to deliver the template configuration to devices. If no time is set, the configuration is delivered immediately.
- **Backup:** You can select whether to back up the current configuration of the site when the configuration template is applied to the site. If you select the check box, you can view or restore backup records in **Configuration Backup**.

4. Viewing Results

You can click **View Result** in the **Operation** column of the template list to jump to the configuration task list, which displays the detailed information and execution results of configuration delivery tasks.

Figure 7-21 Viewing Results

Template Name	Template Description	Application Site	Creation Time	Update Time	Operation
h...	-	0	2022-07-21 05:06:48	2022-07-20 21:06:48	Edit View Result Bind Site ...
...	-	0	2022-08-31 05:02:56	2022-08-31 05:02:56	Edit View Result Bind Site ...
...	-	0	2022-09-01 01:00:27	2022-09-01 01:00:27	Edit View Result Bind Site ...
...	-	0	2022-09-08 04:35:34	2022-09-08 04:35:36	Edit View Result Bind Site ...

5. Binding a Site

Click **Bind Site** in the **Operation** column of the template list to bind the configuration template to specific sites. Then, when devices go online and access the sites for the first time, they will automatically obtain the configuration in the template. For existing devices, you need to manually deliver the configuration.

Figure 7-22 Binding a Site

Management & Maintenance / Configuration / Template

Configuration Template List

Template Name Template Description

hostname -

111 -

test -

123 -

Bind Site

After a template is bound, a new device connected to the site automatically obtains the configuration in the template when it goes online for the first time.

Search for site

RuijieProject

2022-07-20 21:06:48 Edit View Result Bind Site ...

2022-08-31 05:02:56 Edit View Result Bind Site ...

2022-09-01 01:00:27 Edit View Result Bind Site ...

2022-09-08 04:35:36 Edit View Result Bind Site ...

1-4 of 4 items 1 10 / page

6. Delivering the Configuration

Click **... > Deliver Config** in the **Operation** column of the template list to deliver the configuration to all devices of the site. If you perform this operation after you edit a template or bind a template to sites, the configuration in the template will be delivered to existing devices of the sites.

Figure 7-23 Delivering the Configuration (01)

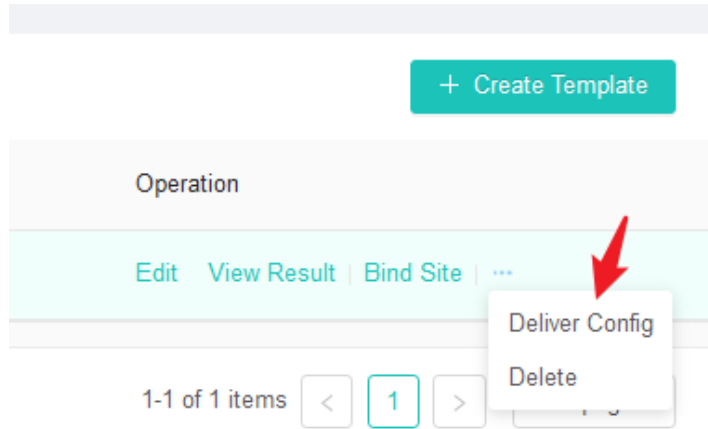


Figure 7-24 Delivering the Configuration (02)

Deliver Config

When a template is applied, devices connected to the site automatically obtain the configuration in the template.

Search for site

- Institut_Teknologi_Bandung
 - ITB_Jatinangor
 - test1

Select the configuration delivery time.

Select date

The current configuration is backed up when the template is applied. (Go to Configuration > Configuration Backup to view or restore backup records.)

Cancel Deliver Config

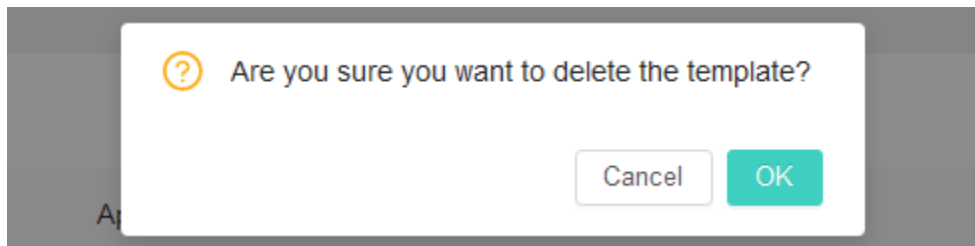
Parameters for configuration delivery are described as follows:

- **Site:** (Required) Select one or more sites in the site tree to apply the template.
- **Configuration delivery time:** (Optional) You can set the time to deliver the template configuration to devices. If no time is set, the configuration is delivered immediately.
- **Backup:** You can select whether to back up the current configuration of the site when the configuration template is applied to the site. If you select the check box, you can view or restore backup records in **Configuration Backup**.

7. Deleting a Template

Click ... > **Delete** in the **Operation** column of the template list to delete the configuration template.

Figure 7-25 Deleting a Template



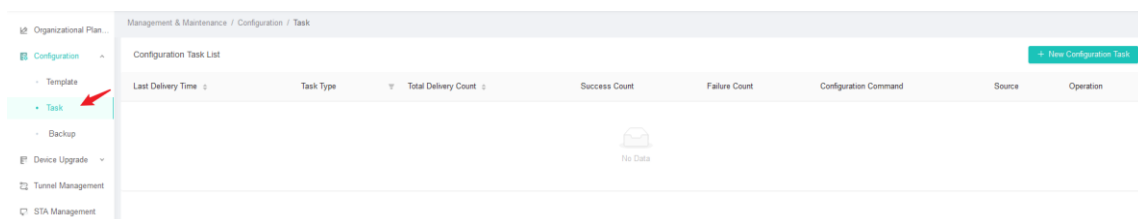
7.2.2 Configuration Task

Choose **Management & Maintenance > Configuration > Task** to enter the configuration task management page where you can monitor and manage the tasks delivered by the template configuration to devices. Using configuration tasks, you can deliver configuration to devices in batches and on time from the cloud.

1. Task List

A configuration task list displays **Last Delivery Time**, **Task Type**, **Total Delivery Count**, **Success Count**, **Failure Count**, and **Source**. You can sort the tasks by **Last Delivery Time** and **Total Delivery Count**, and filter the tasks by **Task Type**.

Figure 7-26 Task List

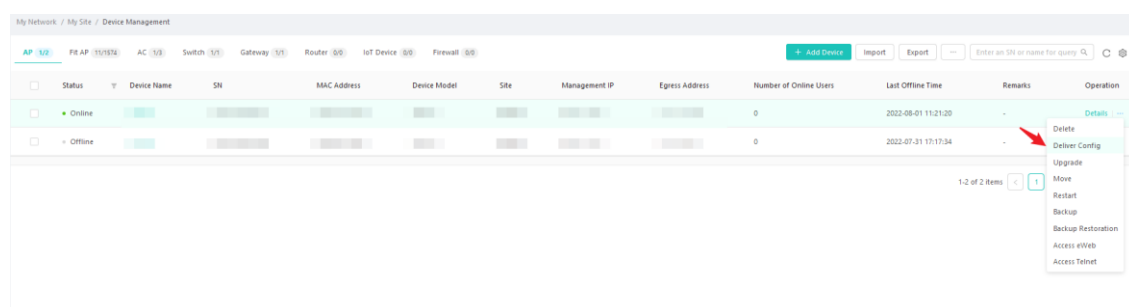


2. Task Type

(1) Common task

A common task is triggered by delivered configuration in device management. To operate a common task, choose **My Network > My Site > Device Management** and click the corresponding button in the **Operation** column of the device list. A common task facilitates the personalized configuration of devices of the same type.

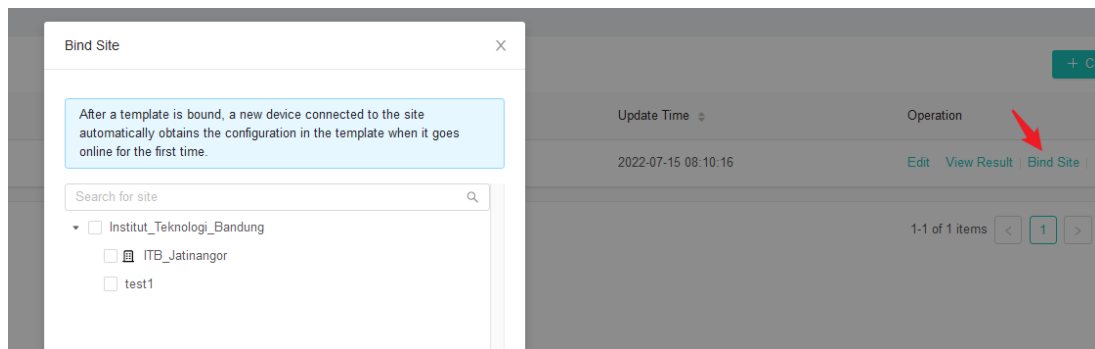
Figure 7-27 Generating a Common Task



(2) Deployment task

After creating a configuration template, you can bind the template to sites. Then, when devices go online for the first time at these sites, the devices are automatically matched according to the match method in the template. The configuration will be delivered to the matched devices according to the delivery method in the template. In this way, the deployment configuration of devices is implemented, and this process is a deployment task.

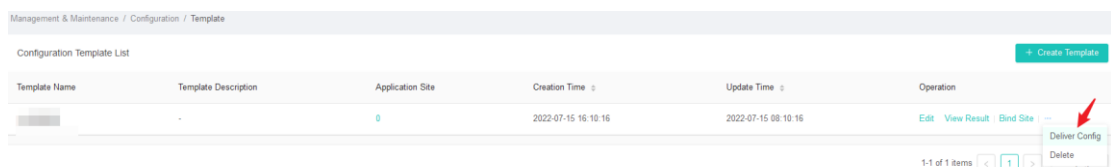
Figure 7-28 Generating a Deployment Task



(3) Template task

You can manually click the **Deliver Config** button in the configuration template list or in a template to deliver the configuration in the template to devices at the selected sites and synchronize the configuration on existing devices of the sites.

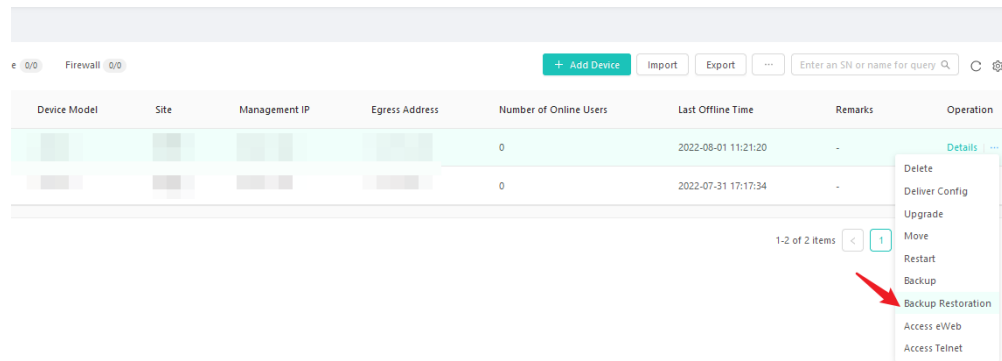
Figure 7-29 Generating a Template Task



(4) Backup restoration task

When you click **Backup Restoration** in the device list of **My Network > My Site > Device Management** or **Device Details > O&M Tool**, the configuration task list will generate a backup restoration task and display the task execution status.

Figure 7-30 Generating a Backup Restoration Task



(5) Radio optimization task

After intelligent network optimization analysis is implemented in the network optimization module, network optimization configuration will be delivered by the configuration management module. (For the detailed network optimization process, see the "Network Optimization" section.) The configuration task list will list the radio optimization task and display the delivery status.

Figure 7-31 Radio Optimization Task

The screenshot shows the 'Configuration Task List' interface. It includes a breadcrumb 'Management & Maintenance / Configuration / Task' and a '+ New Configuration Task' button. The table has columns: Last Delivery Time, Task Type, Total Delivery Count, Success Count, Failure Count, Configuration Command, Source, and Operation. Two rows are shown: one for 'Radio Optimization' (highlighted with a red box) and one for 'Common Task'. A pagination control at the bottom shows '1-2 of 2 items' and '10 / page'.

Last Delivery Time	Task Type	Total Delivery Count	Success Count	Failure Count	Configuration Command	Source	Operation
2022-08-05 16:40:27	Radio Optimization	1	1	0	View Command	-	View Result
2022-07-31 11:39:33	Common Task	1	1	0	View Command	-	View Result

(6) Blacklist/Whitelist task

After a blacklist/whitelist is read and set in the blacklist/whitelist module, the blacklist/whitelist configuration will be delivered by the configuration management module. (For the detailed blacklist/whitelist operation process, see the [Blacklist/Whitelist](#).) The configuration task list will list the blacklist/whitelist task and display the delivery status.

Figure 7-32 Blacklist/Whitelist Task

Management & Maintenance / Configuration / Task

Configuration Task List + New Configuration Task

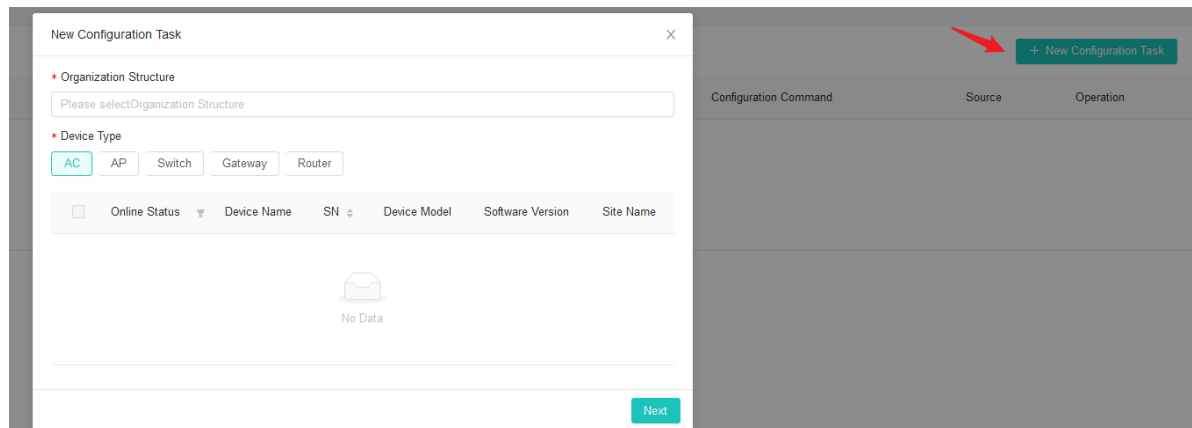
Last Delivery Time	Task Type	Total Delivery Count	Success Count	Failure Count	Configuration Command	Source	Operation
2022-08-08 11:18:31	Blacklist Whitelist	1	0	1	View Command	-	View Result Stop
2022-08-08 11:18:31	Blacklist Whitelist	1	1	0	View Command	-	View Result
2022-08-08 11:18:31	Blacklist Whitelist	1	0	1	View Command	-	View Result Stop
2022-08-08 11:18:31	Blacklist Whitelist	1	0	1	View Command	-	View Result Stop
2022-08-08 11:18:31	Blacklist Whitelist	1	0	0	View Command	-	View Result Stop
2022-08-05 16:40:27	Radio Optimization	1	1	0	View Command	-	View Result
2022-07-31 11:39:33	Common Task	1	1	0	View Command	-	View Result

1-7 of 7 items 1 10/page

3. New Configuration Task

Click **New Configuration Task** to create a new configuration delivery task.

Figure 7-33 New Configuration Task 1



Description:

- **Organization Structure:** (Required) Select one or more target branches or sites for the task from the organization tree.
- **Device Type:** (Required) Select a device type from AC, AP, switch, gateway, and router.
- **Device list:** After you select a device type, all available devices will be listed below.

Select devices to deliver the task and click **Next** to configure the delivery time and CLI command set.

Figure 7-34 New Configuration Task 2

Description:

- **Last Delivery Time:** (Required) Set the execution time of the configuration delivery task. The time cannot be earlier than the current time and can be precise to second.
- **CLI Command Set:** (Required) Configure the CLI command set to be delivered.

After the configuration, click **Create Task** to complete the task creation.

4. View Command

In the configuration task list, you can click **View Command** in the **Configuration Command** column to display the command set of the specified task.

Figure 7-35 View Command

Management & Maintenance / Configuration / Task

Configuration Task List + New Configuration Task

Last Delivery Time	Task Type	Total Delivery Count	Success Count	Failure Count	Configuration Command	Source	Operation
2022-06-08 11:18:31	Blacklist Whitelist	1	0	1	View Command	-	View Result Stop
2022-06-08 11:18:31	Blacklist Whitelist	1	1	0	View Command	-	View Result
2022-06-08 11:18:31	Blacklist Whitelist	1	0	1	View Command	-	View Result Stop
2022-06-08 11:18:31	Blacklist Whitelist	1	0	1	View Command	-	View Result Stop
2022-06-08 11:18:31	Blacklist Whitelist	1	0	0	View Command	-	View Result Stop
2022-06-05 16:40:27	Radio Optimization	1	1	0	View Command	-	View Result
2022-07-31 11:39:33	Common Task	1	1	0	View Command	-	View Result

1/7 of 7 items 1 / page

5. View Result

In the configuration task list, you can click **View Result** in the **Operation** column to display the execution result of the specified task. The execution result list displays **Execution Status**, **Failure Cause** (if any), **Device Name**, **SN**, **Device Model**, **Site Name**, and **Last Delivery Time**.

Figure 7-36 View Result

Execution Status	Failure Cause	Device Name	SN	Device Model	Site Name	Last Delivery Time
● Execution Succeeded	-	[Redacted]	[Redacted]	[Redacted]	[Redacted]	2022-07-31 11: [Redacted]

1-1 of 1 items < 1 > 5 / page ▾

7.2.3 Configuration Backup

Choose **Management & Maintenance > Configuration > Backup**. On the configuration backup management page, you can view, manage, and download the backups of device configurations.

1. Backup List

The list of device configuration backups displays **Device Type**, **Device Name**, **SN**, **Backup Type**, **Backup Time**, and **Current Status**. You can filter data by specifying a time range or a backup type (auto, manual, or timed), and search for backup by device name, remarks or SN.

Figure 7-37 Backup List

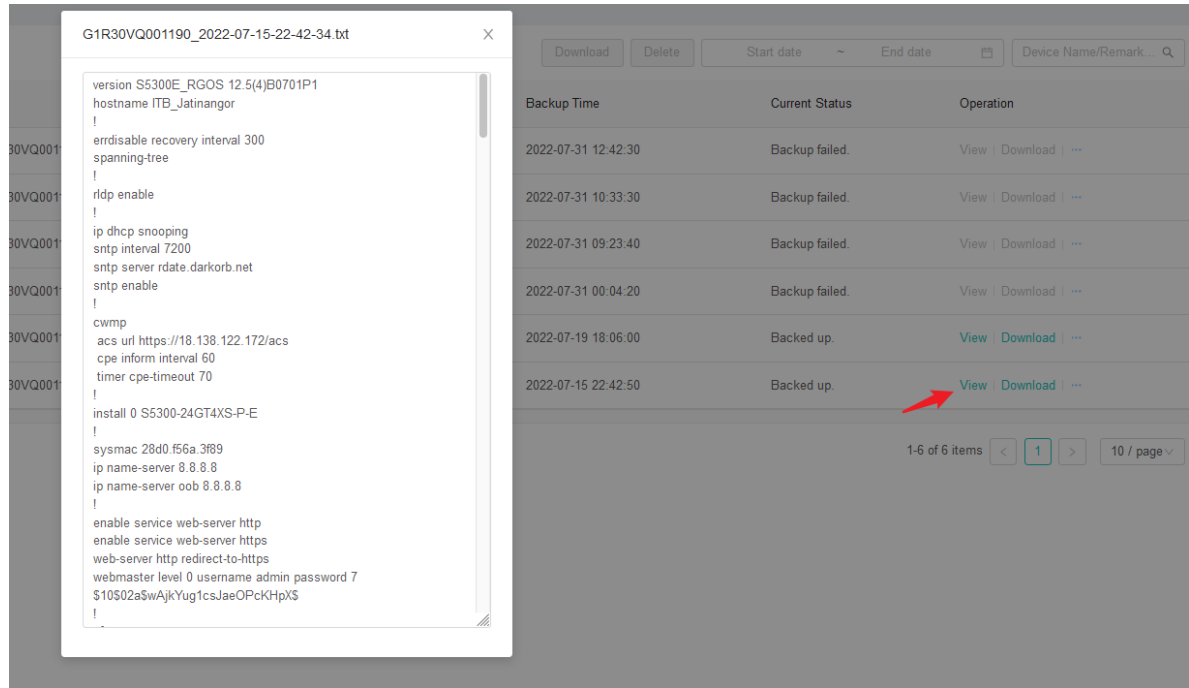
Device Type	Device Name	SN	Backup Type	Remarks	Backup Time	Current Status	Operation
<input type="checkbox"/>	SWITCH	[Redacted]	Auto	-	2022-07-31 12:42:30	Backup failed	View Download --
<input type="checkbox"/>	SWITCH	[Redacted]	Auto	-	2022-07-31 10:33:30	Backup failed	View Download --
<input type="checkbox"/>	SWITCH	[Redacted]	Auto	-	2022-07-31 09:23:40	Backup failed	View Download --
<input type="checkbox"/>	SWITCH	[Redacted]	Auto	-	2022-07-31 00:04:20	Backup failed	View Download --
<input type="checkbox"/>	SWITCH	[Redacted]	Auto	-	2022-07-19 18:06:00	Backed up	View Download --
<input type="checkbox"/>	SWITCH	[Redacted]	Auto	-	2022-07-15 22:42:50	Backed up	View Download --

1-6 of 6 items < 1 > 10 / page ▾

2. Viewing Backup

Click **View** to display the detailed configuration information of the specified backup.

Figure 7-38 Viewing Backup



3. Editing Backup

Click ... > **Edit** in the **Operation** column of the backup list to edit the remarks of the backup. To save edited remarks, click **Save**. To exit editing, click **Cancel**.

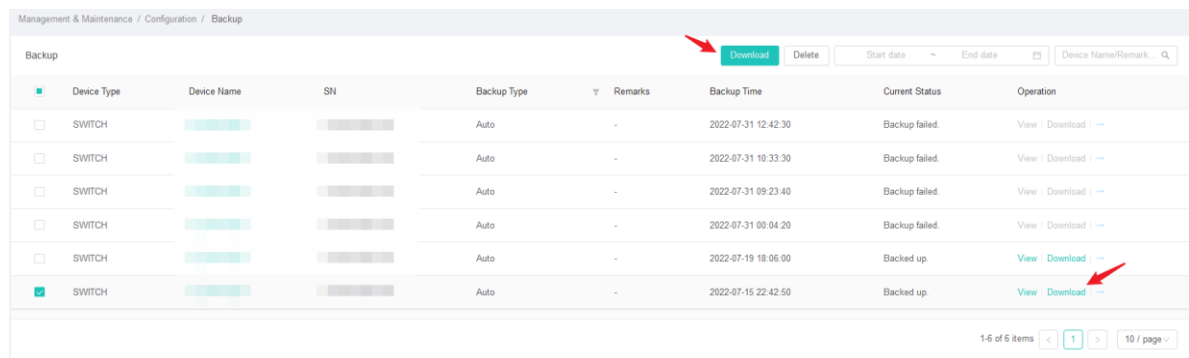
Figure 7-39 Editing Backup



4. Downloading Backup

You can click **Download** to download specified backup data in batches to a local path.

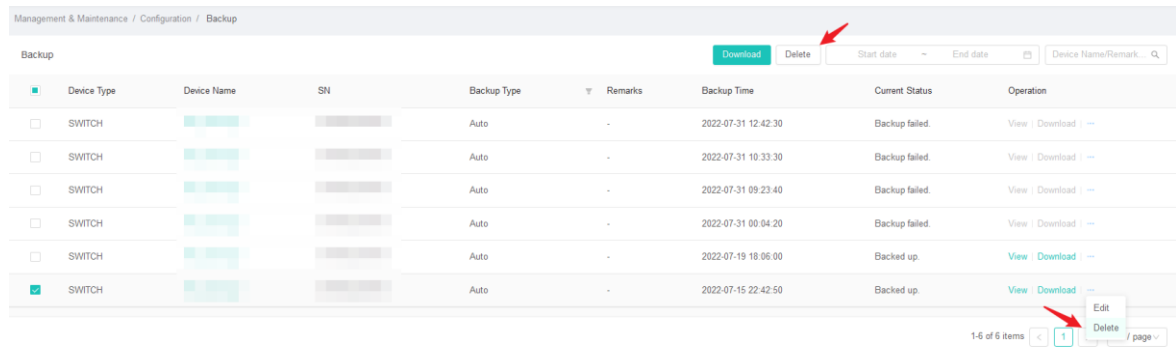
Figure 7-40 Downloading Backup



5. Deleting Backup

You can click ... > **Delete** in the **Operation** column of the backup list to delete the specified backup, or select backups and click **Delete** in the upper part to delete backups in batches.

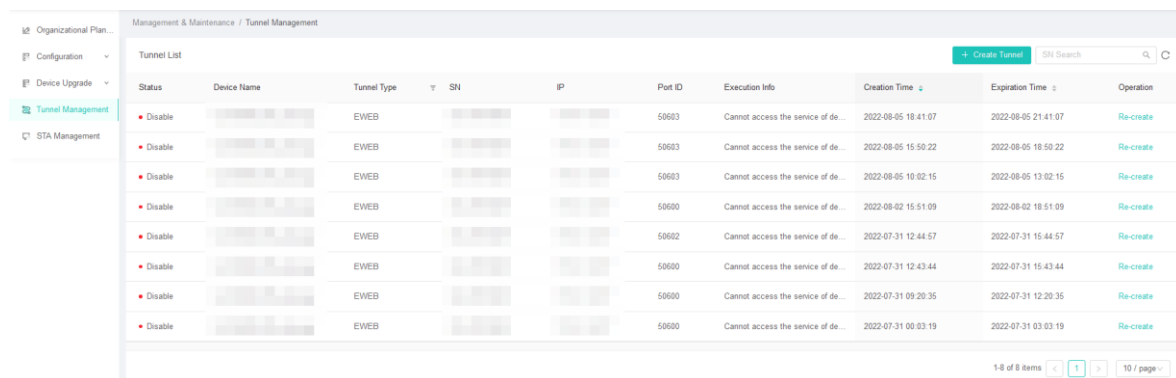
Figure 7-41 Deleting Backup



7.3 Tunnel Management

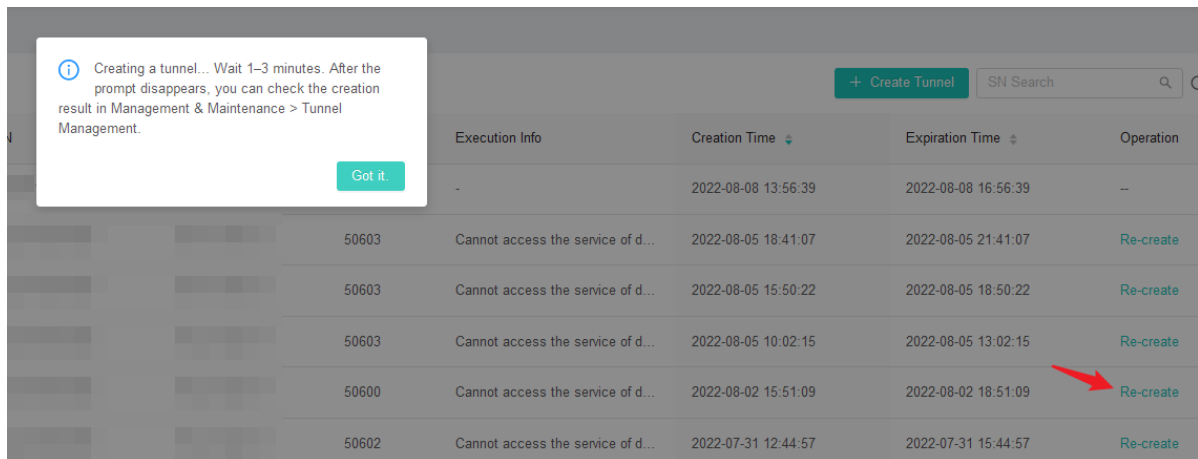
Tunnel Management records the creation of device tunnels. You can re-initiate the creation of an overdue or failed tunnel, create a new tunnel, and query a specified device by the device SN in the list.

Figure 7-42 Tunnel List



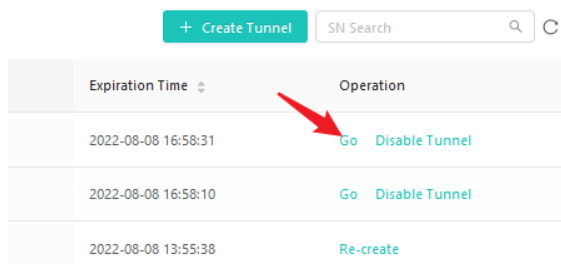
Click **Re-create** to create an overdue or creation-failed tunnel again.

Figure 7-43 Re-creating a Tunnel



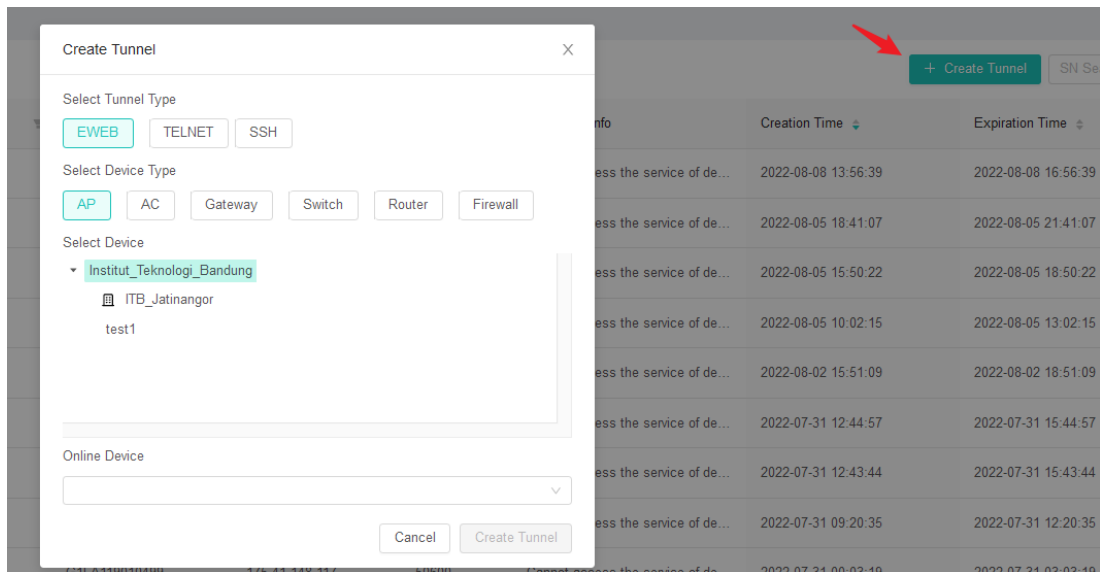
If a tunnel is connected, you can manage the tunnel by clicking **Go** or **Disable Tunnel** in the **Operation** column of the list.

Figure 7-44 Tunnel Management



Click **Create Tunnel** to create a new tunnel. Two tunnel types are available: eWeb and TELNET. On certain devices (such as APs and switches), tunnels cannot be directly created, and need to be exchanged by gateways.

Figure 7-45 Creating a Tunnel



Configuration description:

- **Tunnel Type:** (Required) **EWEB** and **TELNET** types can be selected, and the default value is **EWEB**.
- **Device Type:** (Required) You can create a tunnel on APs, ACs, gateways, switches, and router devices. **AP** is selected by default.
- **Site.** (Required) You need to select the site where the device to be created with a tunnel locates. A level-1 site is selected by default.
- **Online Device:** (Required) Select the device to be created with a tunnel. The device must be online.
- **Transfer Device:** Optional, but required when **Device Type** is **AP** or **Switch**.

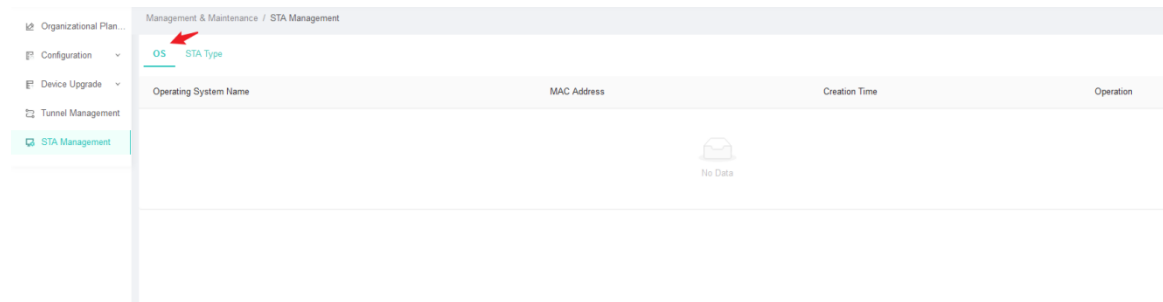
7.4 STA Management

This function enables you to manage different operating systems (OSs) and STA types, and customize STA statistics.

7.4.1 OS

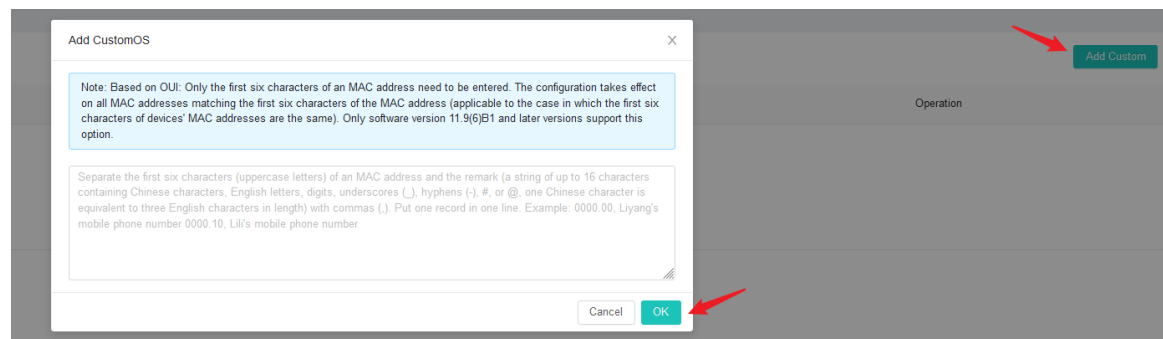
An OS list displays customized **Operating System Name**, **MAC Address**, and **Creation Time**. You can customize the number on each page of the list.

Figure 7-46 OS List



You can click **Add Custom** to add a customized OS type.

Figure 7-47 Adding a Customized OS

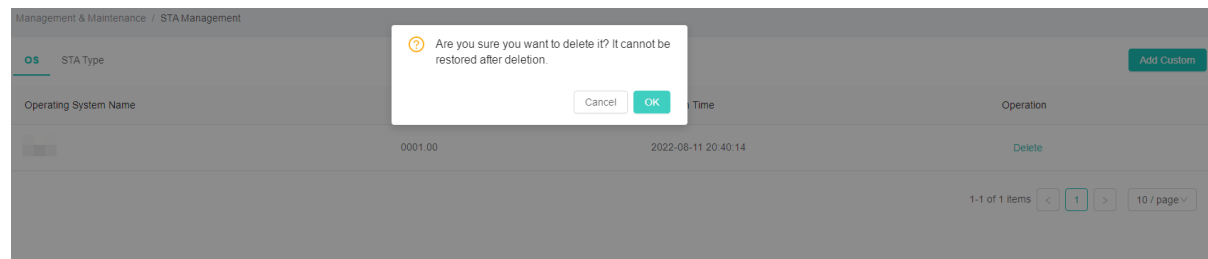


Based on the organizationally unique identification (OUI), you need to enter only the first six characters of a MAC address. Then, the configuration is effective on all devices whose MAC addresses have the same first six characters.

You can add OSs in batches by placing a record in a line, and separating the first six characters (in upper case) of a MAC address and a remark with a comma (,). A remark corresponds to an OS name in the list, and can contain up to 16 characters including English letters, digits, underscore (_), hyphen (-), number sign (#), or at sign (@).

To delete an OS, click **Delete** in the **Operation** column of the OS list.

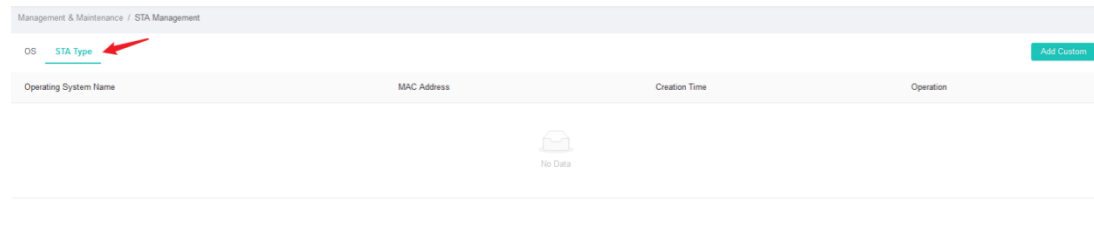
Figure 7-48 Deleting an OS



7.4.2 STA Type

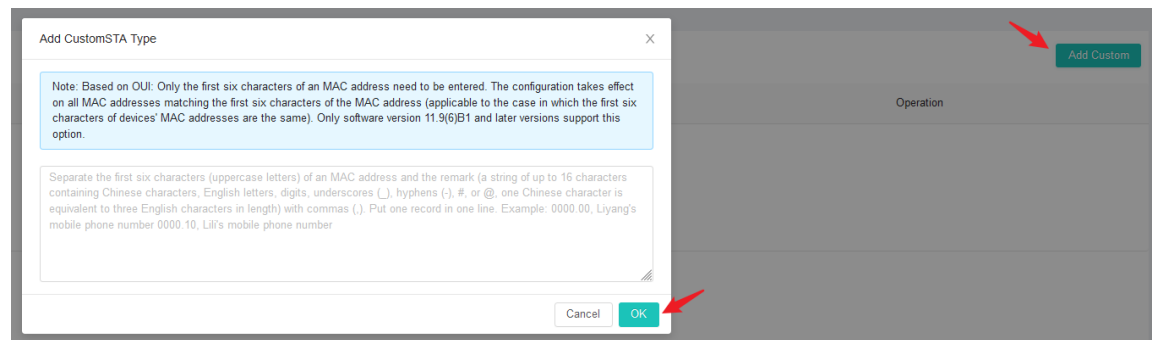
On the **STA Type** tab, a list of customized STA types displays **Operating System Name**, **MAC Address**, **Creation Time**.

Figure 7-49 STA Type List



You can click **Add Custom** to add a customized STA type.

Figure 7-50 Adding a Customized STA Type

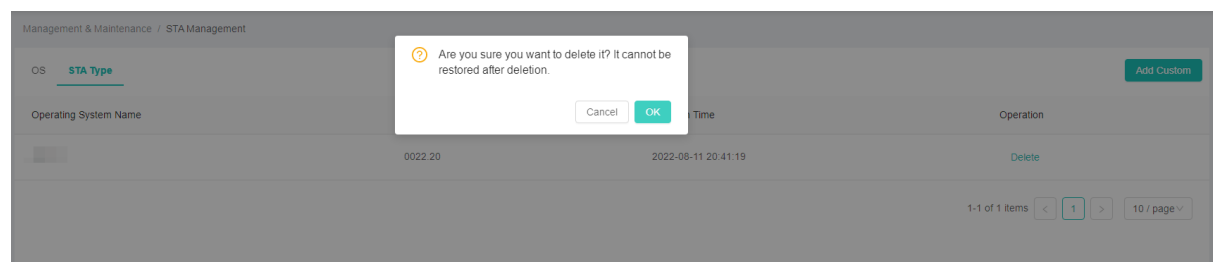


Based on the OUI, you need to enter only the first six characters of a MAC address. Then, the configuration is effective on all devices whose MAC addresses have the same first six characters.

You can add STA types in batches by placing a record in a line, and separating the first six characters (in upper case) of a MAC address and a remark with a comma (,). A remark corresponds to an STA type name in the list, and can contain up to 16 characters including English letters, digits, underscore (_), hyphen (-), number sign (#), or at sign (@).

To delete an STA type, click **Delete** in the **Operation** column of the STA type list.

Figure 7-51 Deleting an STA Type



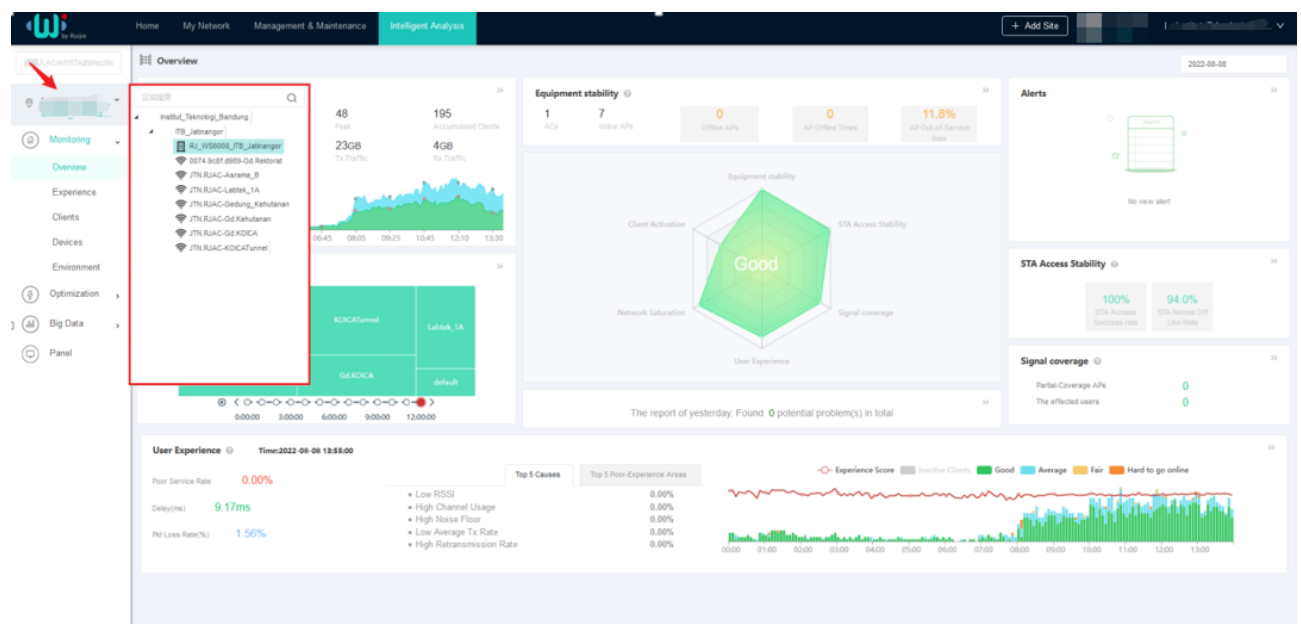
8 Intelligent Analysis

The intelligent analysis module provides wireless experience analysis, diagnosis, and network optimization functions.

8.1 Area

On the **Intelligent Analysis** page, click the project name and switch the area to rapidly display the data analysis result of different areas.

Figure 8-1 Switching Area

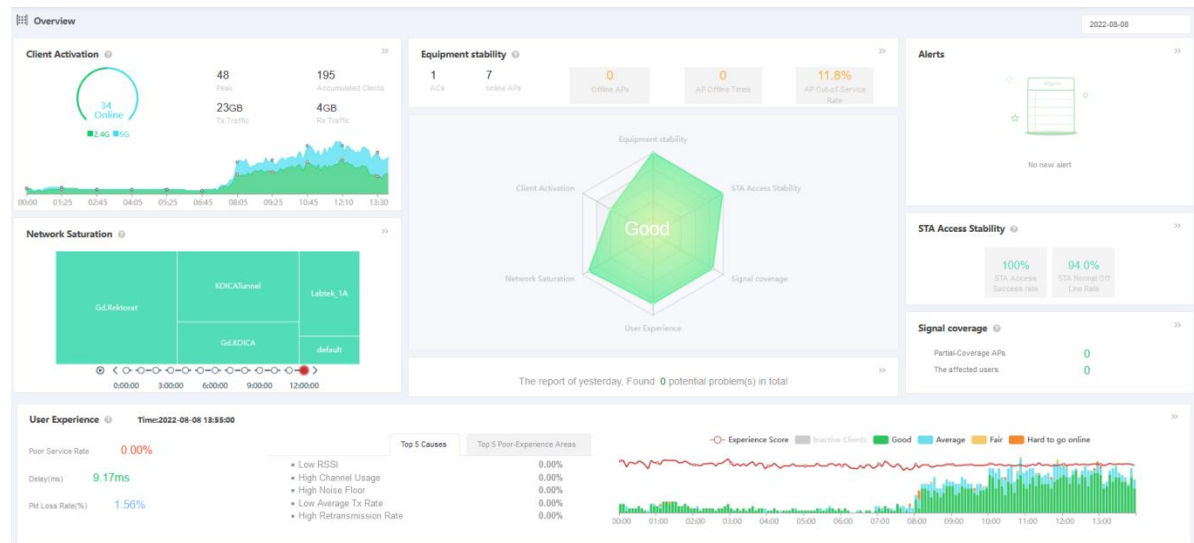


8.2 Monitoring

8.2.1 Overview

Choose **Intelligent Analysis > Monitoring > Overview** to check the overall situation of the entire network. Using the date selector in the upper right corner, you can display data on different dates.

Figure 8-2 Overview



The **Overview** page displays the following information:

- **Basic network status:** equipment stability, STA access stability, signal coverage, etc.
- **Client use status:** client activation (network dependency), user online experience and analysis
- **Network saturation:** network capacity utilization and channel usage

The three parts are described as follows:

- Basic network status

Helps you learn about the equipment stability and STA access stability, so as to determine the stability of wired and wireless lines and whether there are poor coverage areas with high network requirements, thereby providing an effective basis for device supplement.

- Client use status

Helps you assess client dependency on the WLAN by time and traffic. It displays values of the WLAN construction in an intuitive way. User online experience is graded into Good, Average, Fair, Hard to go online, and Inactive Clients based on the packet loss rate, delay, and traffic data. You can assess the user experience of the entire network according to portions of the five user experience levels and locate causes for poor experience.

- Network saturation

Helps you learn about client distribution in different areas clearly via the network capacity utilization, and rapidly identify busy areas at each time point and channel usage of each area, providing data support for network deployment and optimization.

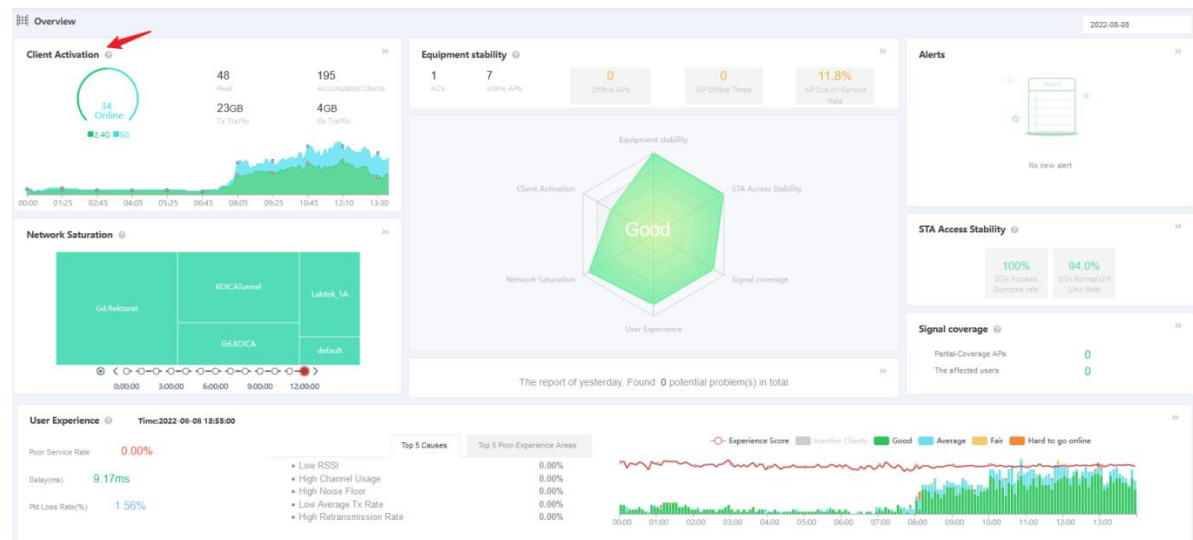
⚠ Caution

The update frequency of each type of data varies with requirements. For example, the online client quantity is updated every five minutes. **Accumulated Clients**, **Peak**, **Tx. Traffic**, and **Rx.Traffic** are statistics of the current day. Experience data is updated every five minutes. Client activation data is updated every hour.

1. Client Activation

The **Client Activation** pane displays the proportions of online users on different wireless networks (2.4G/5G), **Peak**, **Accumulated Clients**, **Tx. Traffic**, and **Rx. Traffic**. You can click >> in the upper right corner to jump to the client activation analysis page.

Figure 8-3 Client Activation



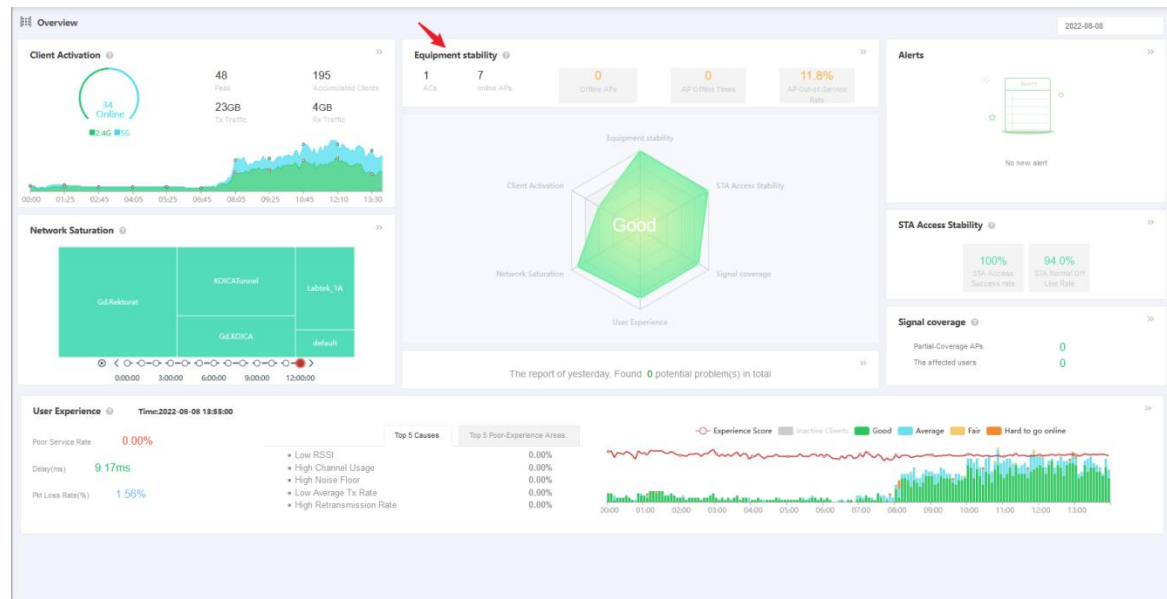
Description:

- **Peak:** The data is sampled every five minutes, and the maximum value of the day is displayed.
- **Accumulated Clients:** The data is sampled every five minutes, and the number of accumulative access clients on the current day is collected, deduplicated, and displayed.
- **Tx. Traffic** and **Rx. Traffic:** accumulative uplink and downlink traffic on the current day

2. Equipment stability

This pane displays the quantities of ACs and APs, and the out-of-service rate of APs. You can click >> in the upper right corner to jump to the device overview page.

Figure 8-4 Equipment stability



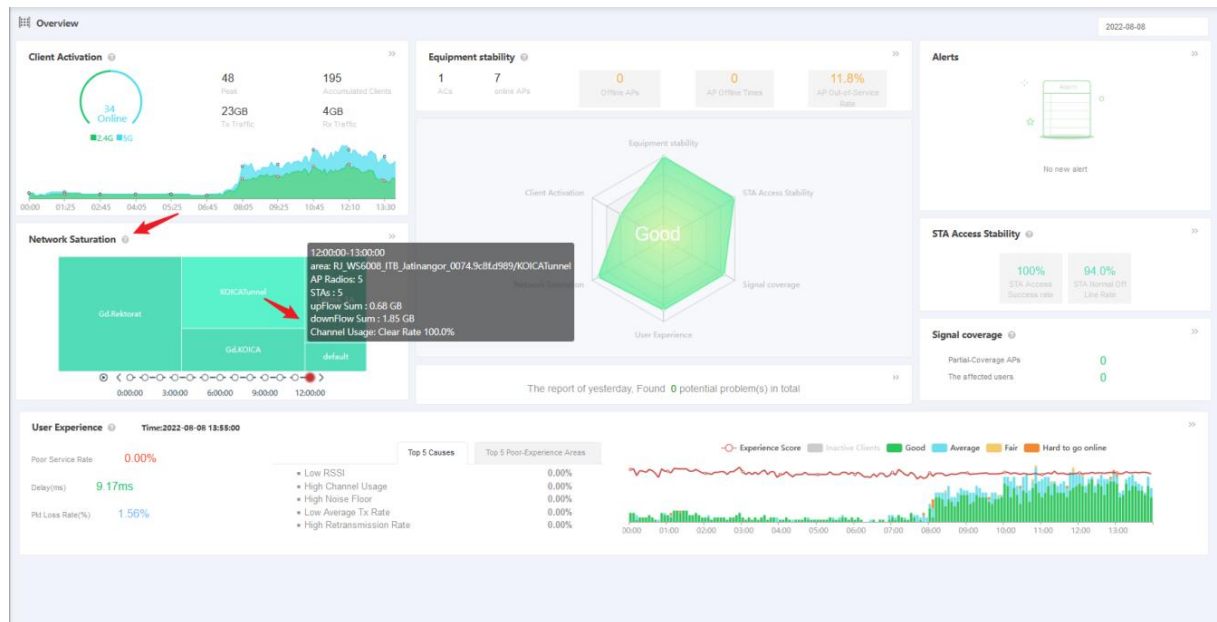
Description:

- **ACs**: number of ACs connected to the WIS Cloud Network
- **online APs**: number of online APs. An i-Share mini AP is counted as one.
- **Offline APs**: number of offline APs, excluding offline i-Share mini APs and APs whose MAC addresses are not sent to ACs
- **AP Offline Times**: Every time an AP goes offline is counted as one, and if an AP goes online multiple times, the actual number of times is counted.
- **AP Out-of-Service Rate**: Number of sampled offline APs (every time an AP is sampled as offline is counted as one)/Total number of sampled APs

3. Network Saturation

This pane displays the network status of different AP groups in every time range, and indicates the channel usage with different colors. You can place the cursor in an area to display the detailed network information and click the time axis to switch the time range. Click the play icon in front of the time axis to enable loop play, and click >> in the upper right corner to jump to the cause analysis page.

Figure 8-5 Network Saturation



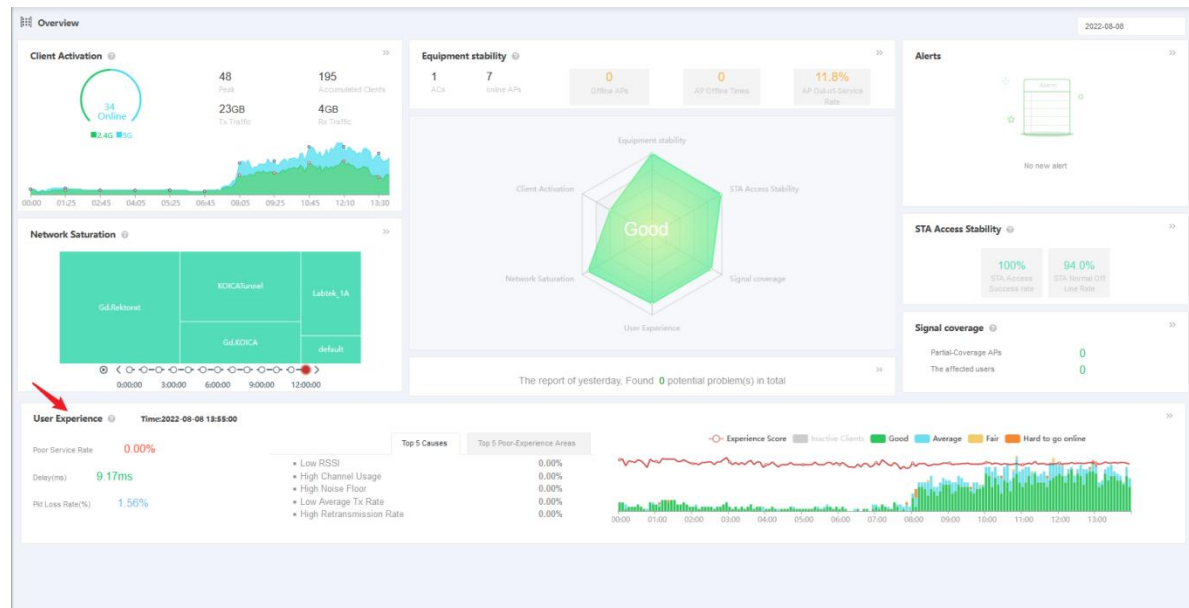
Description:

- **Channel usage:** busyness of the current air interface. A channel is busy because the load in the current frequency band is large, and the load source can be an interference of the local or any other wireless device. Channel usage needs to be lower than 60%. When it is greater than 80%, wireless signal receiving failure, network stalling, and STA disconnection may occur.
- **Status:** The status of an AP radio channel can be graded into congested, busy, and idle by channel usage. The color is determined based on the portions of AP radios in the three statuses.

4. Online Experience

The **User Experience** pane displays three network indicators: **Poor Service Rate**, **Delay**, and **Pkt Loss Rate**. Based on intelligent analysis of the network, this pane lists the top 5 causes of poor experience and top 5 poor-experience areas. Then, the system uses machine learning algorithms to comprehensively evaluate the delay, packet loss, signal strength, and other parameters of STAs, calculate the experience score, and present the result in charts.

Figure 8-6 Online Experience



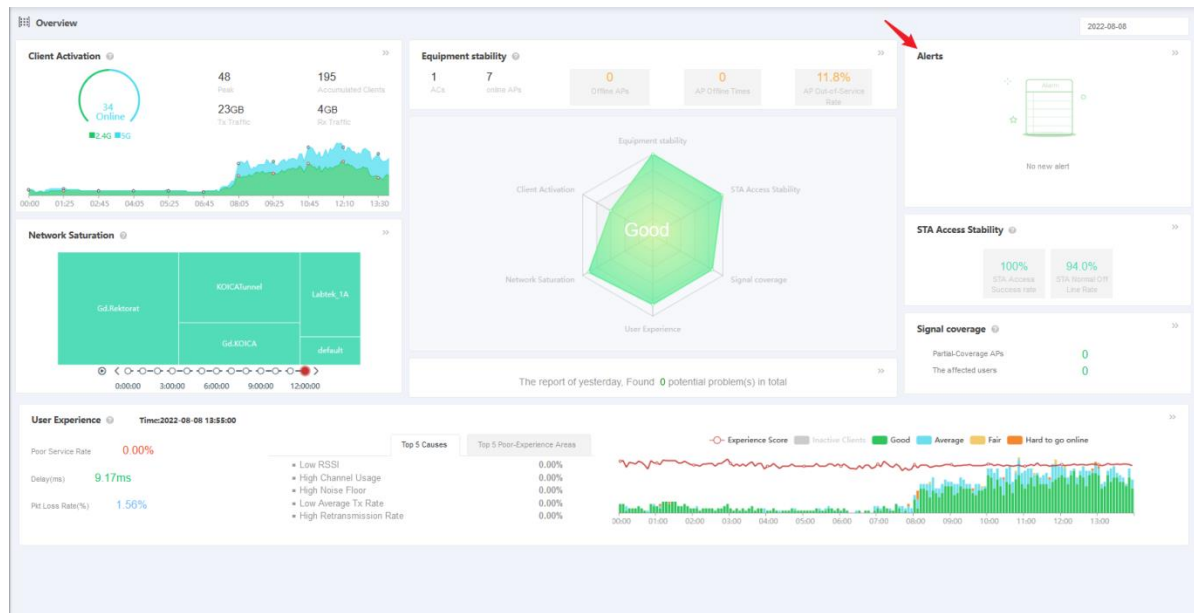
Description of online experience levels:

- **Good:** STAs can play high definition (HD) videos and games.
- **Average:** STAs can use WeChat, browse web pages, and enjoy VoIP.
- **Fair:** In a poor-experience area, even the minimum-resource text applications cannot be smoothly guaranteed.
- **Hard to go online:** STAs frequently fail to go online and often go offline.
- **Inactive Clients:** These clients are assessed based on the traffic usage and power saving of STAs.

5. Alerts

This pane displays alarms of all types on the current day.

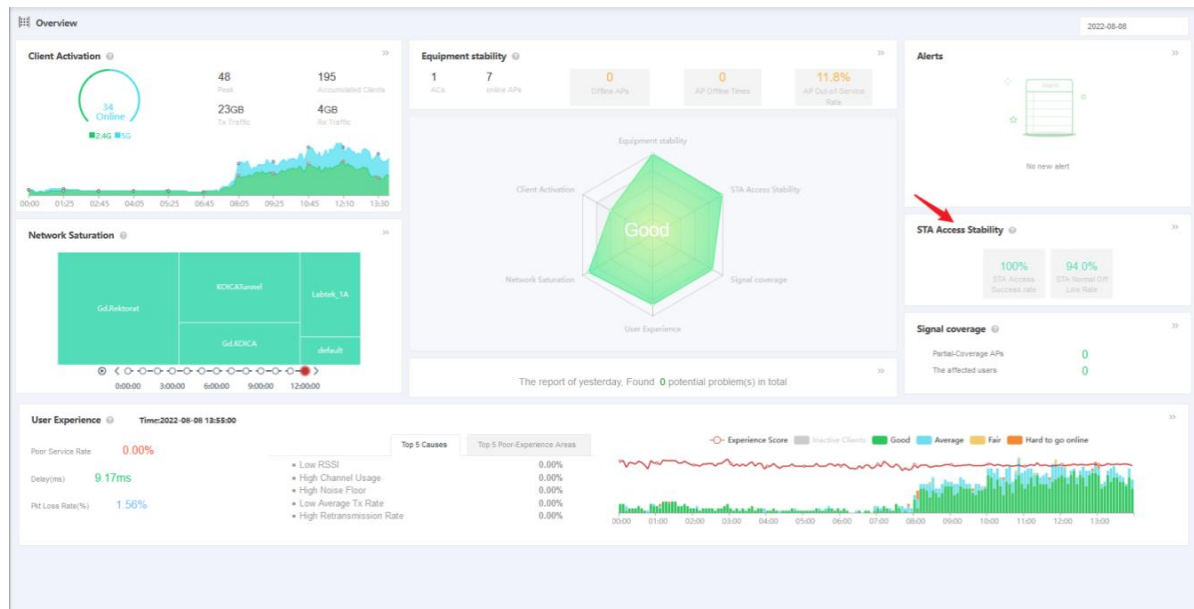
Figure 8-7 Alerts



6. STA Access Stability

This pane displays **STA Access Success Rate** and **STA Normal Off Line Rate**.

Figure 8-8 STA Access Stability



Description:

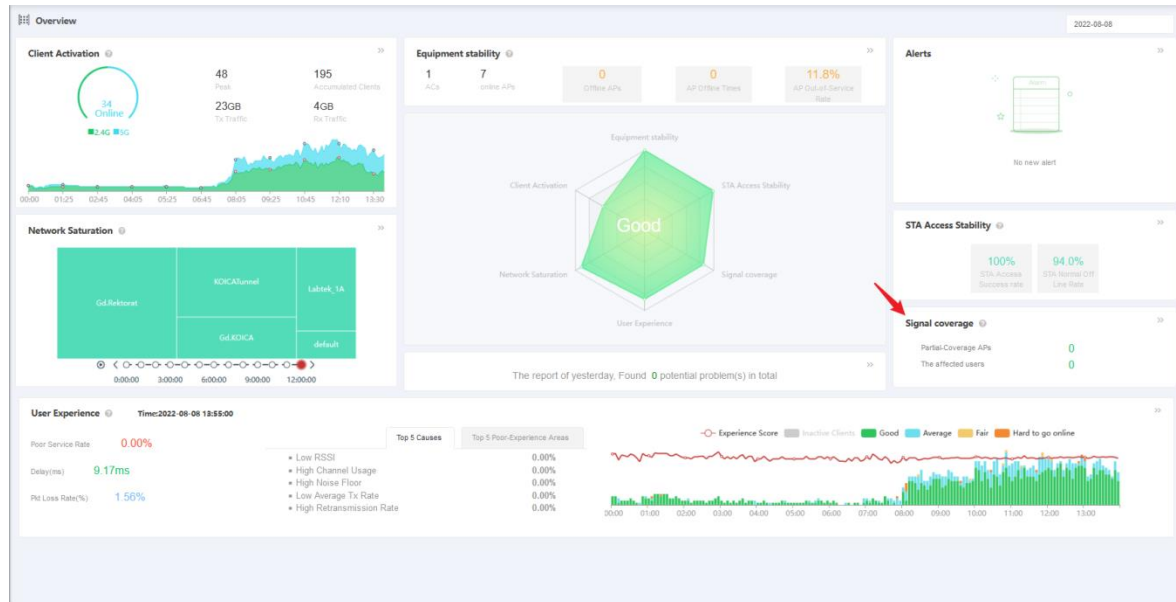
- **STA Access Success Rate:** Times of STA going-online successes/Total times of STA going-online on the current day

- **STA Normal Off Line Rate:** Times of STA going-offline successes/Total times of STA going-offline on the day

7. Signal Coverage

This pane displays the number of APs with partial coverage and the number of affected users.

Figure 8-9 Signal Coverage



Description:

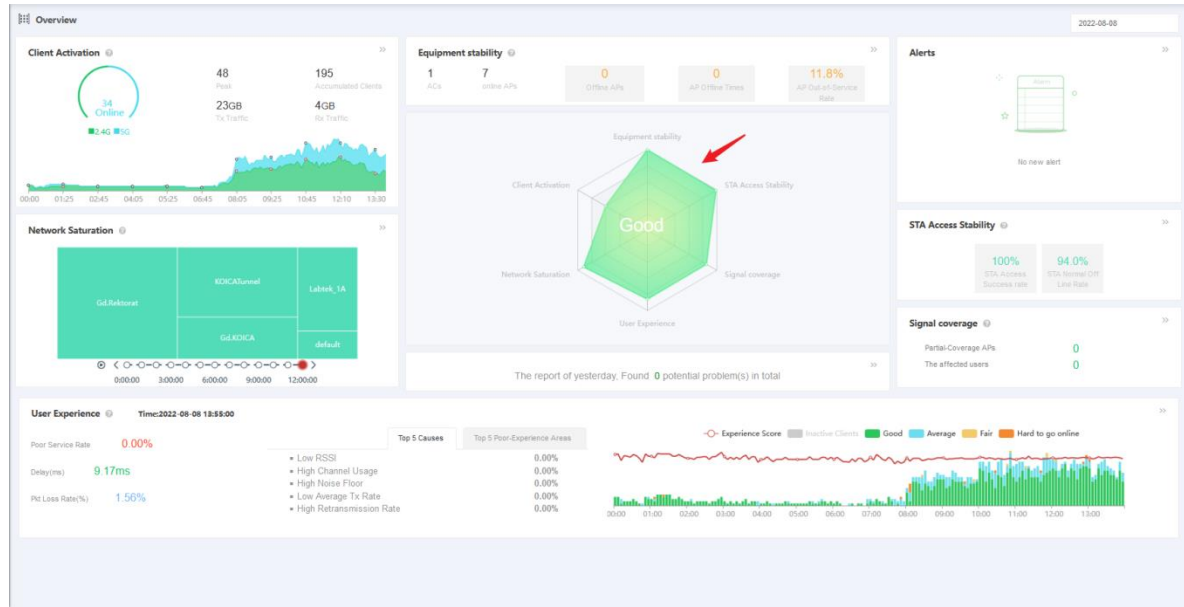
- **Partial-Coverage APs:** number of APs with coverage problems
- **The affected users:** number of users affected by coverage problems

8. Six-Dimensional Network Condition Diagram

This diagram intuitively displays the current network conditions from the dimensions of **Client Activation**, **Equipment stability**, **STA Access Stability**, **Signal coverage**, **User Experience**, and **Network Saturation**. You can place the cursor on a dimension to display the score of each indicator.

Below the six-dimensional diagram, the system indicates the information diagnosis result on the previous day and the number of potential problems. You can click >> in the upper right corner to jump to the **One Key Diagnosis** page to check detailed diagnosis information.

Figure 8-10 Six-Dimensional Network Condition Diagram



8.2.2 Experience

WIS Cloud Network employs machine learning algorithms to assess intuitive user experience based on various types of indicators and parameters involved in the communication process of each STA that accesses the wireless network. The parameters include signal strength, delay, packet loss, traffic, channel quality, and access process. The user experience is graded into Good, Average, Fair, Hard to go online, and Inactive Clients. For descriptions of the experience levels, see the "Overview" section.

Choose **Intelligent Analysis > Monitoring > Experience**. The network experience analysis page summarizes multi-dimensional network condition indexes at different times, and analyzes the causes. By switching the date and wireless network type, you can display the corresponding experience analysis result.

Figure 8-11 Experience



1. Overview

The **Overview** page displays the user experience assessment and user experience distribution in different time ranges (with a granularity of one hour) on the specified date. The three areas on the **Overview** page are described as follows:

(1) Experience Levels in Different Time Ranges

This area displays the network experience in different time ranges of the current day in a ring. Green indicates good experience, blue indicates average experience, and orange indicates poor experience.

Figure 8-12 Experience Levels in Different Time Ranges



Below the ring, network indexes of **Delay**, **Pkt Loss Rate**, **Rx Rate**, and **Tx Rate** are indicated. You can click > to display the line graphs of the indexes on the day.

Figure 8-13 Index Line Graphs on the Day



(2) STA Experience Distribution

This area combines a bar graph and a line graph to display the distribution of the numbers of STAs with different experience levels in different time ranges. When you click any time position in the graph, the **Poor-Experience Client List** area will display detailed information about the network with poor user experience in the time range. The time granularity of the graph is five minutes, that is, the time interval of the horizontal axis is five minutes. The bars of different colors in the graph represent different experience levels.

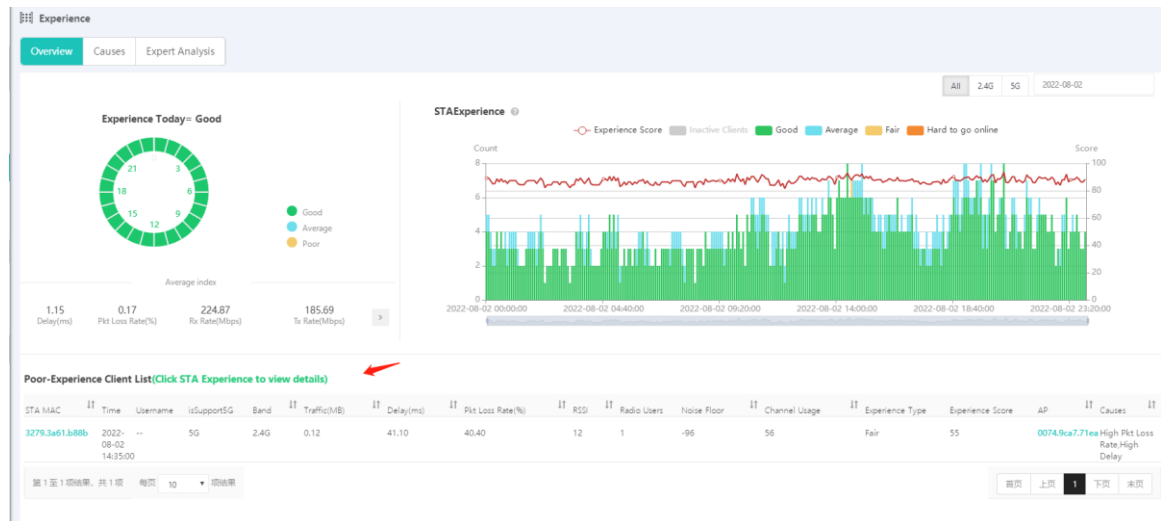
Figure 8-14 STA Experience Distribution



(3) Poor-Experience Client List

This list displays only clients with poor experience at the specified time point. When the experience level is Good or Average, the user experience is good. When the experience level is Fair or Hard to go online, the user experience is poor. The list indicates network indexes of an STA at the specified time point, including **Traffic**, **Delay**, **Pkt Loss Rate**, **RSSI**, **Radio Users**, **Noise Floor**, and **Channel Usage**, and analyzes the main causes of the poor experience according to the indexes.

Figure 8-15 Poor-Experience Client List



You can click a MAC address in the **STA MAC** column of the list to jump to client details, or click a MAC address in the **AP** column of the list to jump to device details.

Figure 8-16 Client Details

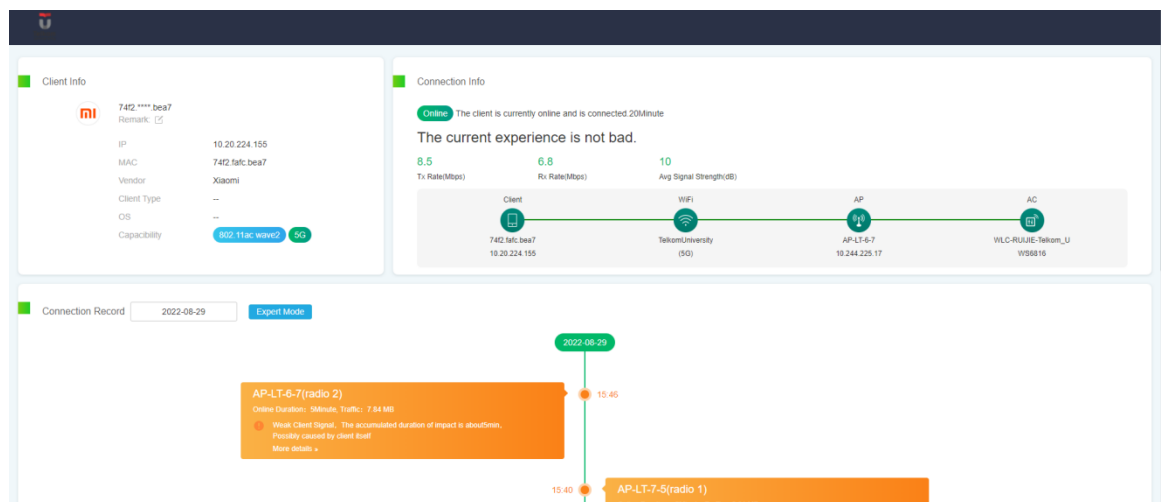
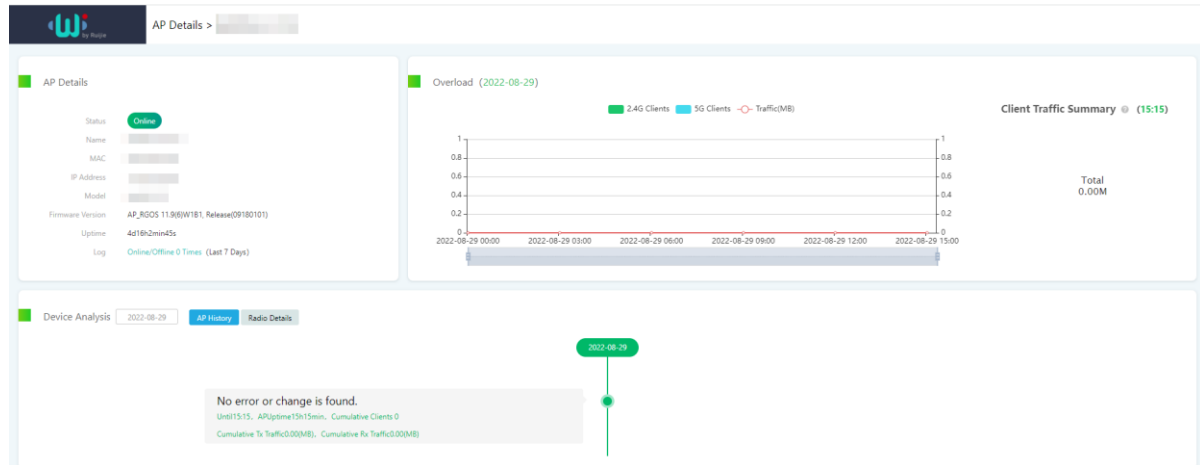


Figure 8-17 Device Details



2. Causes

This page provides detailed analysis on the five aspects that affect user experience of the wireless network, including **Area Analysis**, **Interference**, **Coverage**, **Access**, and **Authentication**.

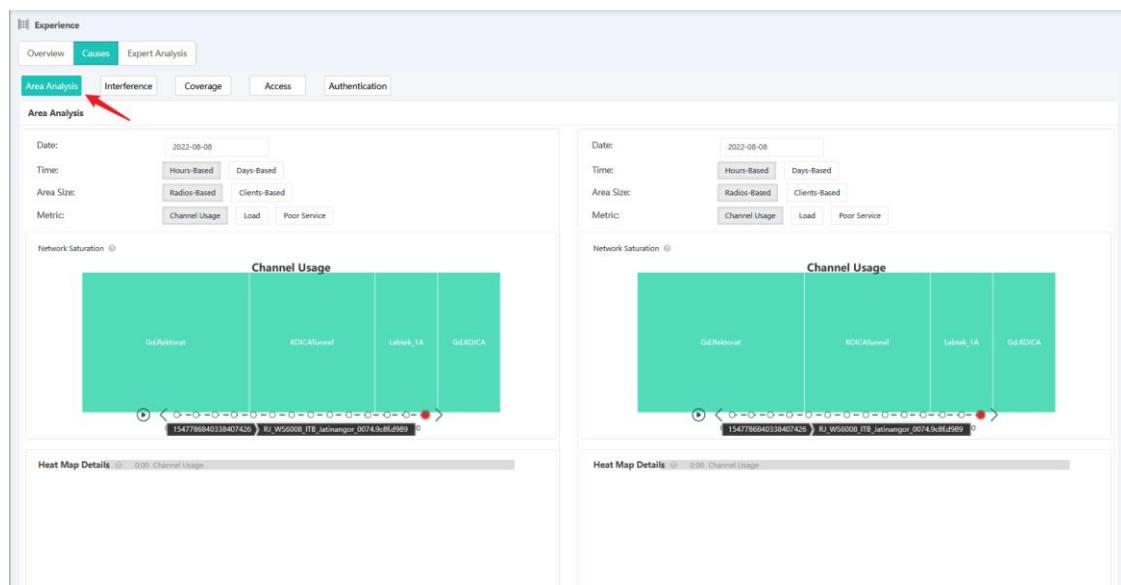
Five Aspects Affecting User Experience	
Group Analysis	Compares network indexes of the same AP group at different times.
Interference	Shows the signal interference of the local network and other networks and the impact with reference to the channel usage and current client traffic, so as to find out busy channels. In the channel usage diagram, the y-axis indicates channel and the x-axis indicates time, to display the hourly channel status. The network saturation diagram displays the percentages of private signals of the local network and other networks. The interference diagram displays the interference caused by private Wi-Fi signals to the network. The density of private Wi-Fi signals indicates the interference severity. The statistics of private Wi-Fi signals can be obtained only after the corresponding function is enabled on the Environment page.
Coverage	Displays signal coverage of each area. The coverage status is graded into Good, Average, and Fair. You can select an area with a coverage problem to display the coverage status of the whole day and details about the AP that generates the coverage problem at a certain moment. In this way, you can find out the areas with poor coverage and the number of affected clients.
Access	Provides access experience assessment based multiple dimensions such as the access failure percentage, abnormal network dropout percentage, access time consumption, and access stability. You can find out the improvement points of network access experience by analyzing the causes (such as client limitation, RSSI, remote association, and equipment instability) for access failure and abnormal network dropout.

<p>Authentication</p>	<p>Provides analysis and comparison of the success rates and efficiency of different authentication manners, so as to recommend the most stable authentication manner to users. You can also track the authentication data of a single STA, to rapidly work out the authentication improvement method.</p>
-----------------------	--

(1) **Area Analysis**

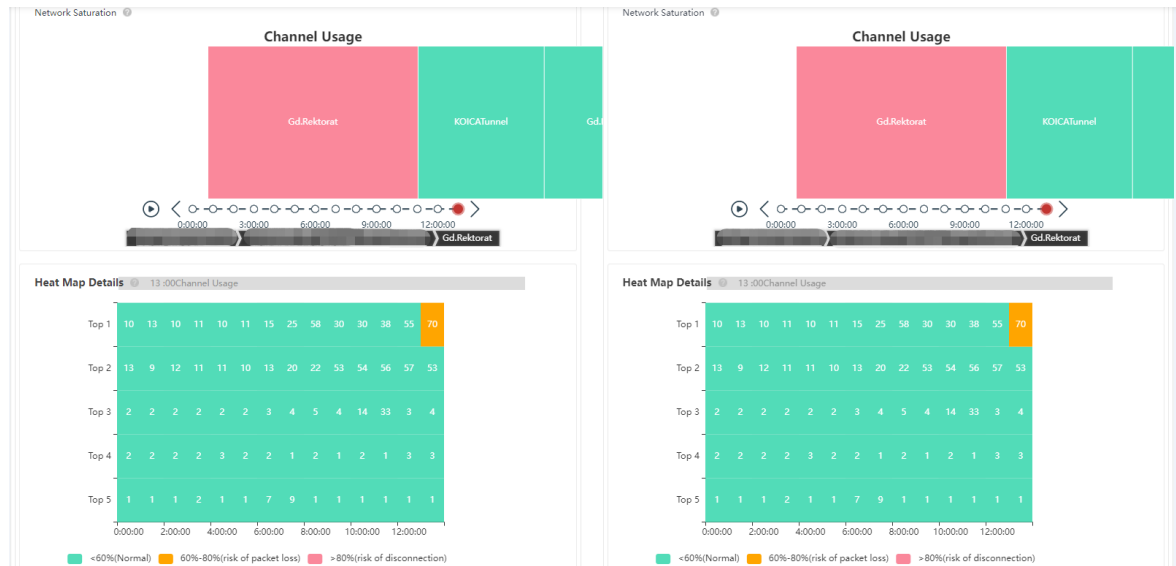
This tab can simultaneously display the network saturation and network indexes of two dates. You can select to display the statistics based on hour or day, sort area sizes by the number of radios or clients, and set metric to channel usage, load, or poor experience.

Figure 8-18 Area Analysis



When you click a network saturation area, the **Heat Map Details** of the area will be displayed.

Figure 8-19 Heat Map Details




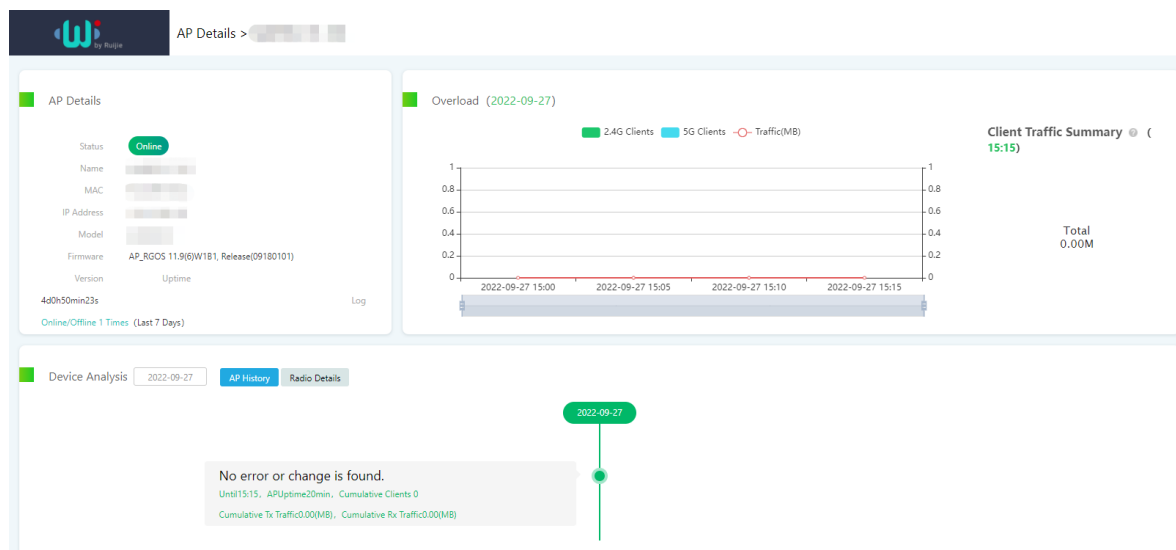
To display the descriptions of indicators in **Network Saturation** and **Heat Map Details** graphs, move the cursor to  next to the graph name. Click any block in the **Heat Map Details** graph to display device details.

Figure 8-20 Device Details



(2) **Interference**

The **Channel Usage Analysis** graph represents a channel with interference in red, and displays the usage of different channels. Click the usage of different channels at different time points to display STA details in the right


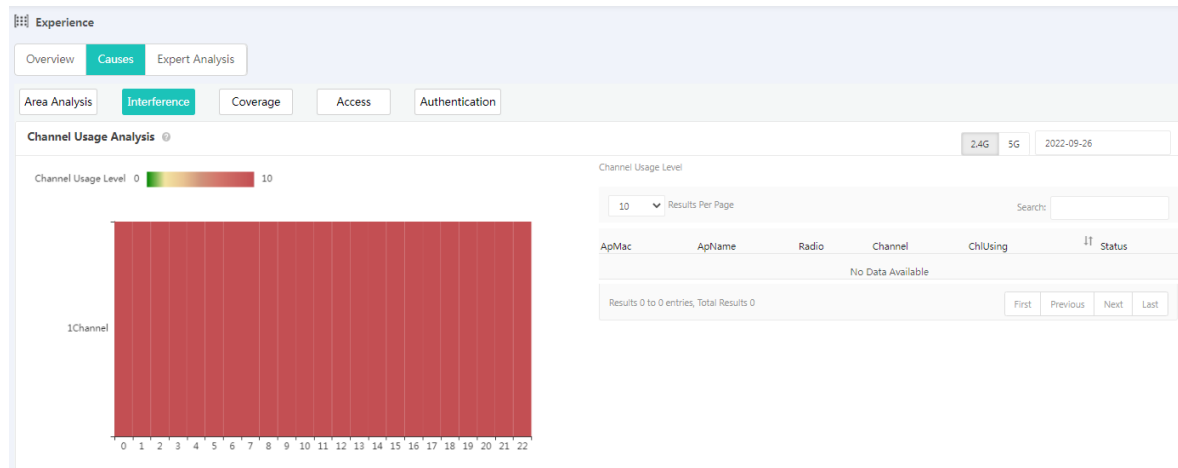
list. Click a client MAC address to display device details. To display the descriptions of indicators, move the cursor to  next to the graph name.

Figure 8-21 Interference



(3) Coverage


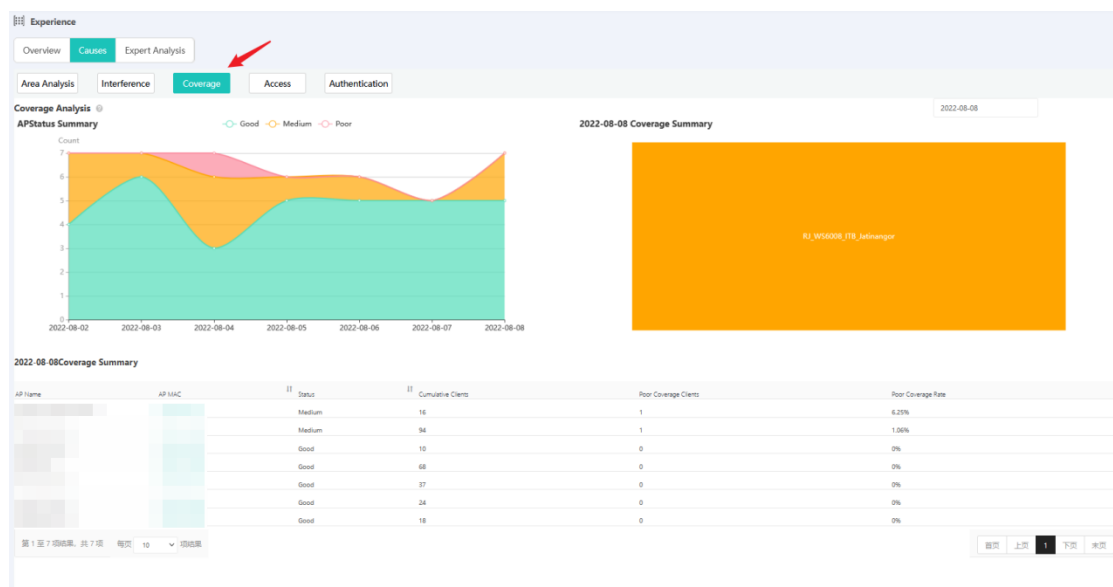
This tab shows AP status trends in the previous two days. You can select a date to display the signal coverage in different areas on the specified day. The AP list displays **AP Name**, **AP MAC**, **Status**, **Cumulative Clients**, **Poor Coverage Clients**, and **Poor Coverage Rate**. You can click a MAC address of an AP to display device details. To display the descriptions of indicators, move the cursor to  next to the graph name.

Figure 8-22 Coverage



(4) Access


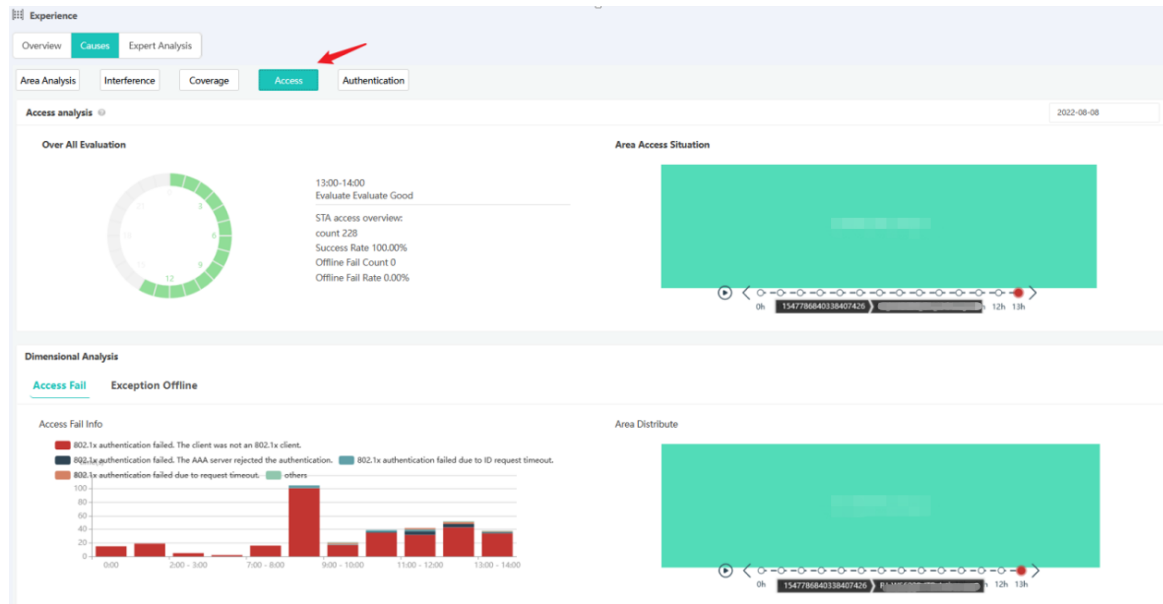
This tab displays **Over All Evaluation**, **Area Access Situation**, **Access Fail**, and **Exception Offline**. To display the descriptions of indicators, move the cursor to  next to the graph name.

Figure 8-23 Access Analysis



Click the bar graph on the **Access Fail** or **Exception Offline** tab to display STA details.

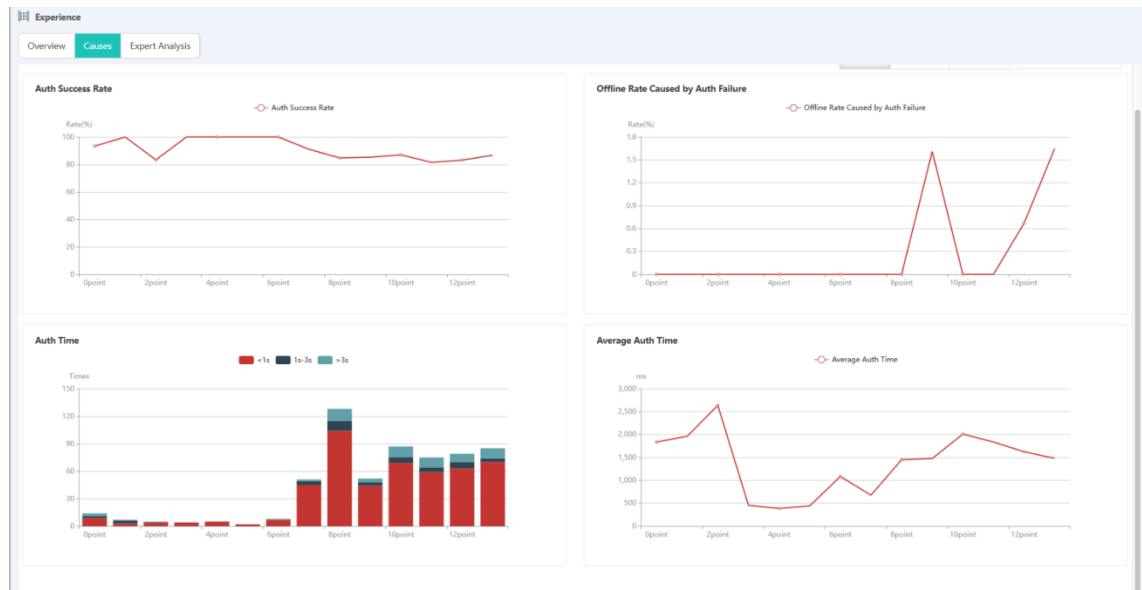
Figure 8-24 Access Fail



(5) **Authentication**

This tab presents **Auth Success Rate**, **Offline Rate Caused by Auth Failure**, **Auth Time** distribution, and **Average Auth Time** in charts. You can select to display the analysis by day, week, or month.

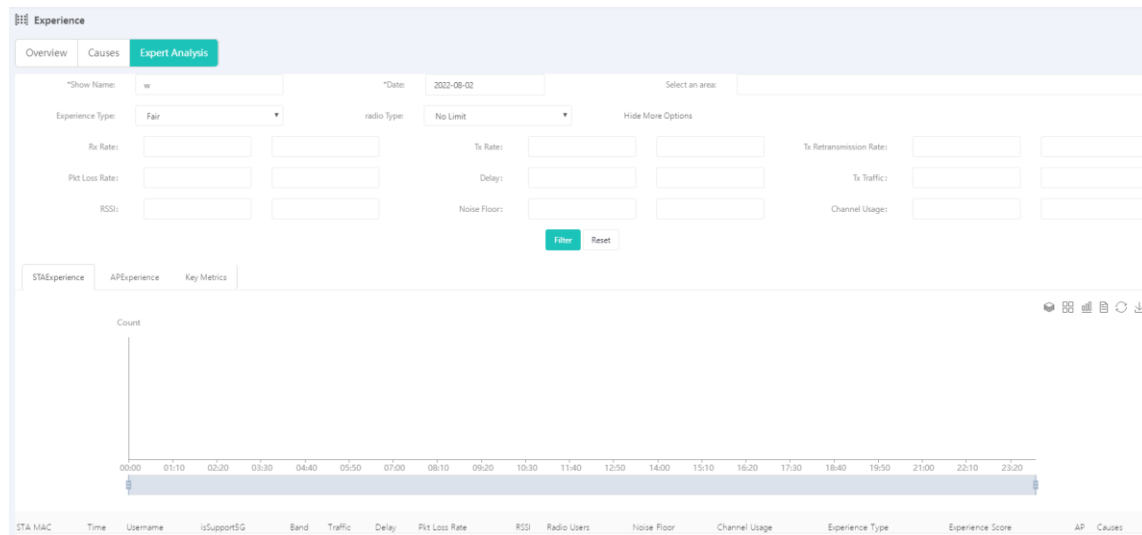
Figure 8-25 Authentication Views



3. Expert Analysis

On this page, you can specify an area, a date, and the value ranges of indicators to filter data meeting the conditions. The queried result shows **STA Experience**, **AP Experience**, and **Key Metrics**, indicating the user experience at a time.

Figure 8-26 Expert Analysis



8.2.3 Clients

1. Overview


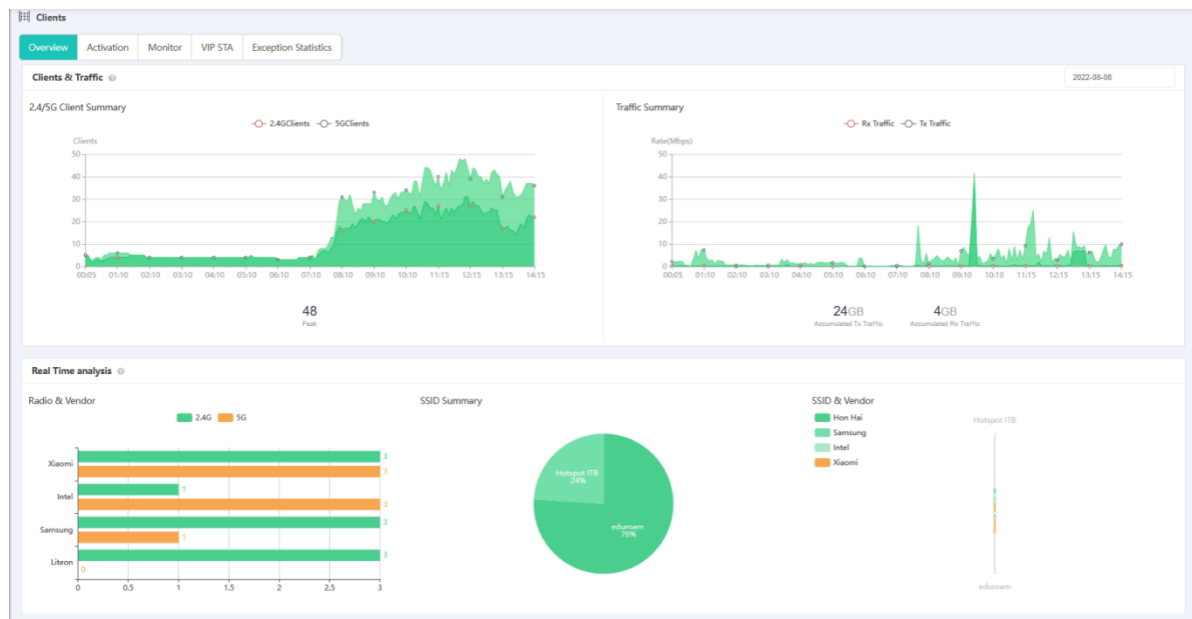
This tab displays the online client quantity of the entire network (including 2.4G/5G clients), Rx/Tx traffic trend, accumulated Rx/Tx traffic, as well as client and traffic distribution of each area, which enables you to learn about the peak hours and dense areas. To display the descriptions of indicators, move the cursor to  next to the graph name.

Figure 8-27 Overview



2. Activation


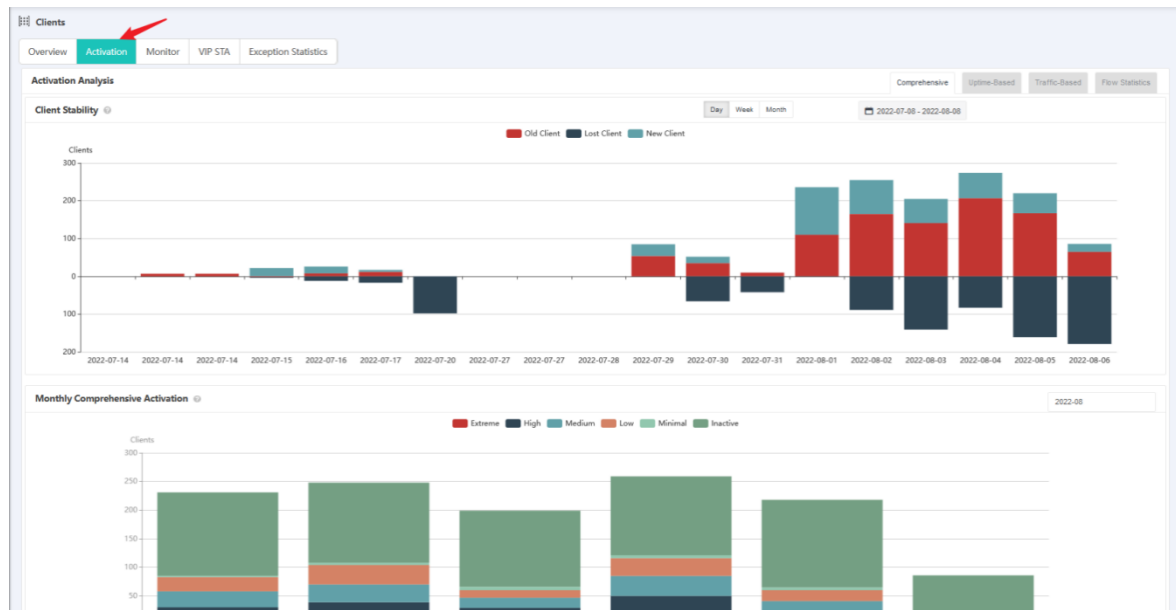
This tab analyzes clients' activation from the dimensions of client stability, retention rate, comprehensive activation, time-based activation, traffic-based activation, and flow statistics, intuitively presenting the client group change and the dependency on the network. To display the descriptions of indicators, move the cursor to  next to the graph name.

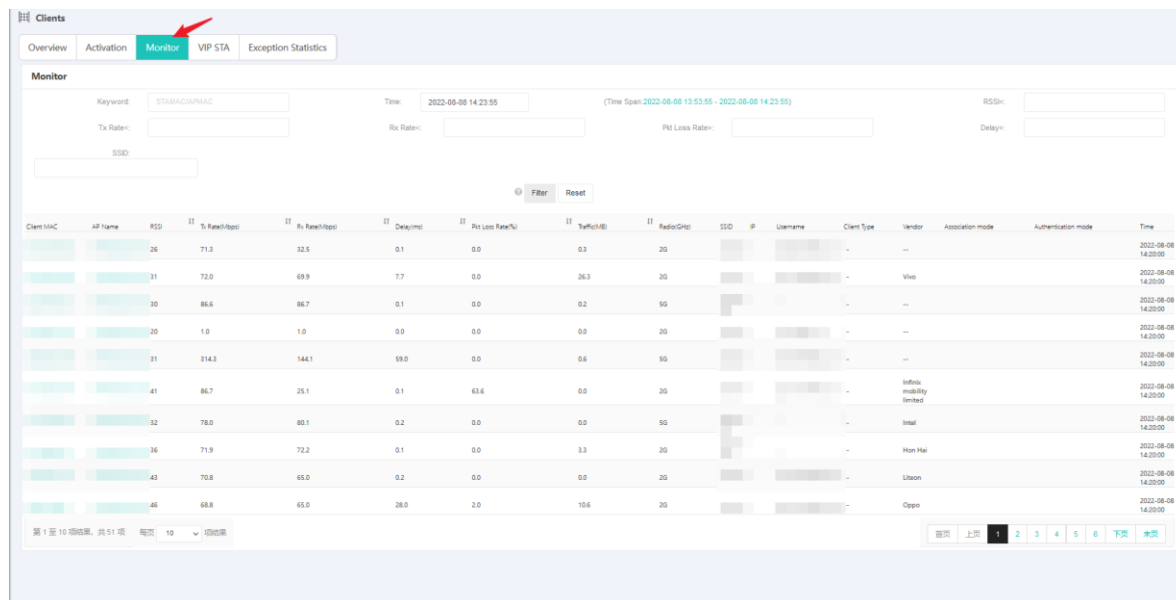
Figure 8-28 Activation Analysis



3. Monitor

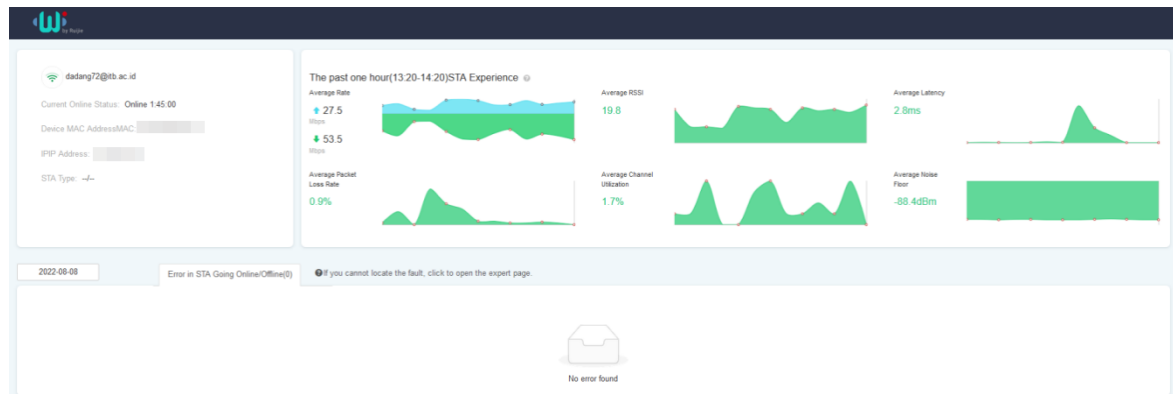
This tab displays details about all online clients by default. The details are updated once every five minutes. You can specify the MAC address, time (for displaying the history), and network parameters for filtering.

Figure 8-29 Client Details



Click a client MAC address to display client details. You can track client traces, including the comprehensive experience scores, historical score trend, online/offline history, roaming trace, and so on.

Figure 8-30 Client Details



Click an AP name in the client list to display device details, including basic information of the device, device load, client traffic proportions, and device analysis records.

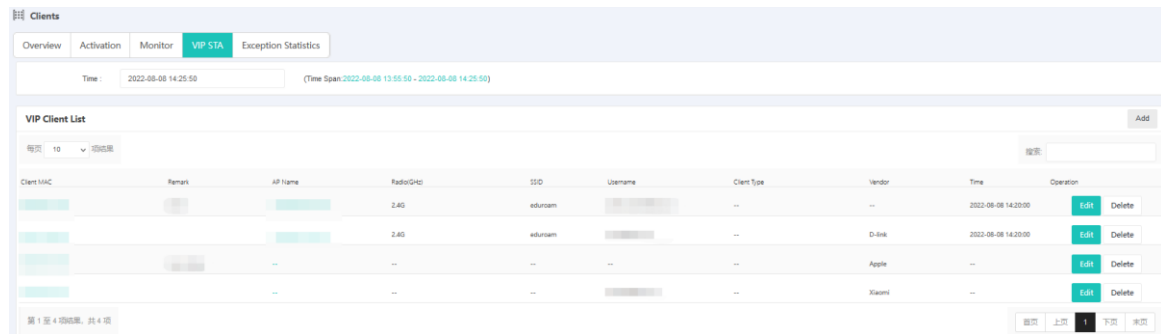
Figure 8-31 Device Details



4. VIP STA

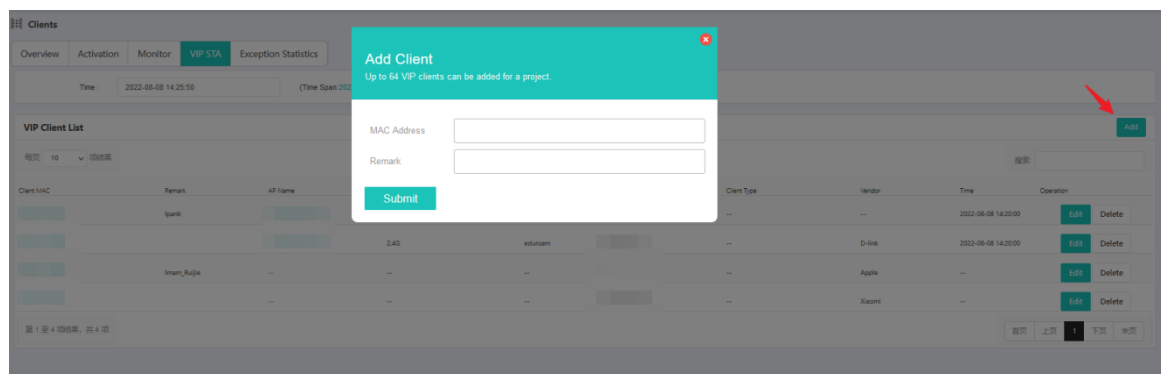
You can manually set key clients to be monitored as VIP clients. The **VIP Client List** displays the details about all VIP clients.

Figure 8-32 VIP Client List



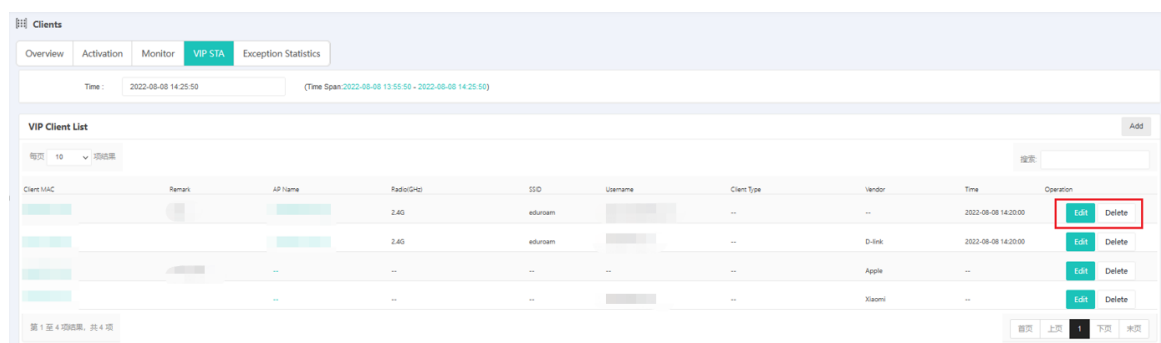
Click **Add** to manually add a VIP client.

Figure 8-33 Adding a VIP Client



You can also edit and delete VIP clients.

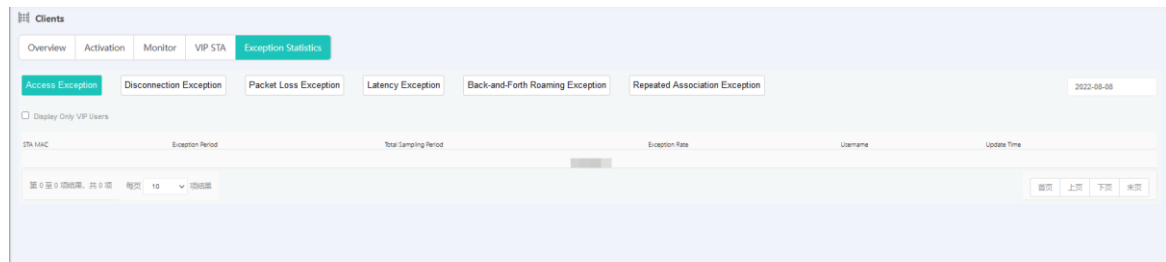
Figure 8-34 Editing or Deleting a VIP Client



5. Exception Statistics

This tab displays **Access Exception**, **Disconnection Exception**, **Packet Loss Exception**, **Latency Exception**, **Back-and-Forth Roaming Exception**, and **Repeated Association Exception**. The client exception list displays detailed information.

Figure 8-35 Exception Statistics

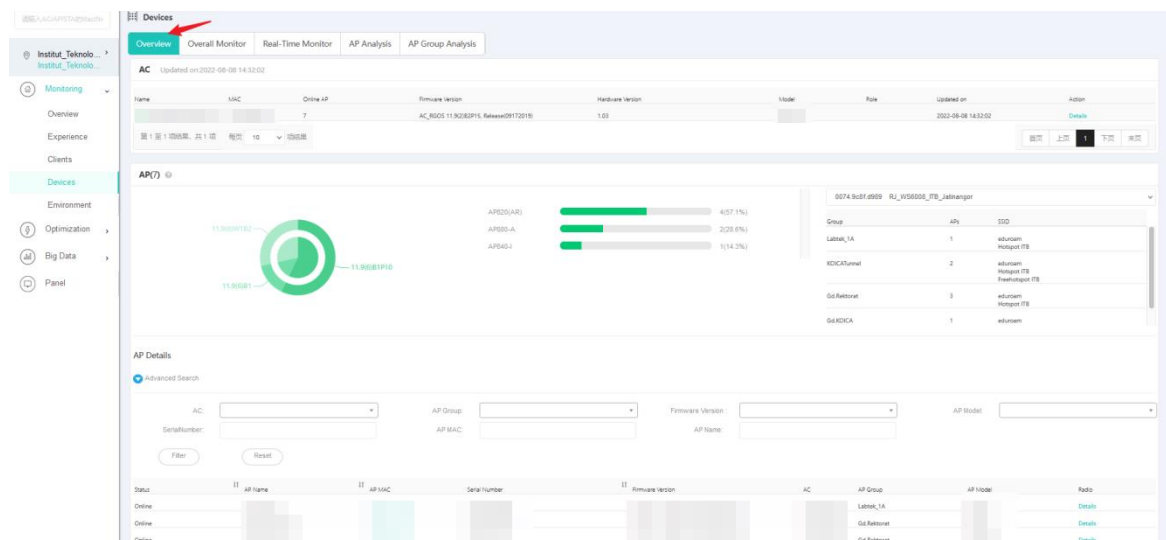


8.2.4 Devices

1. Overview

This tab displays basic information about ACs and APs, including online/offline statuses, device models, firmware versions, and hardware versions.

Figure 8-36 AC Overview



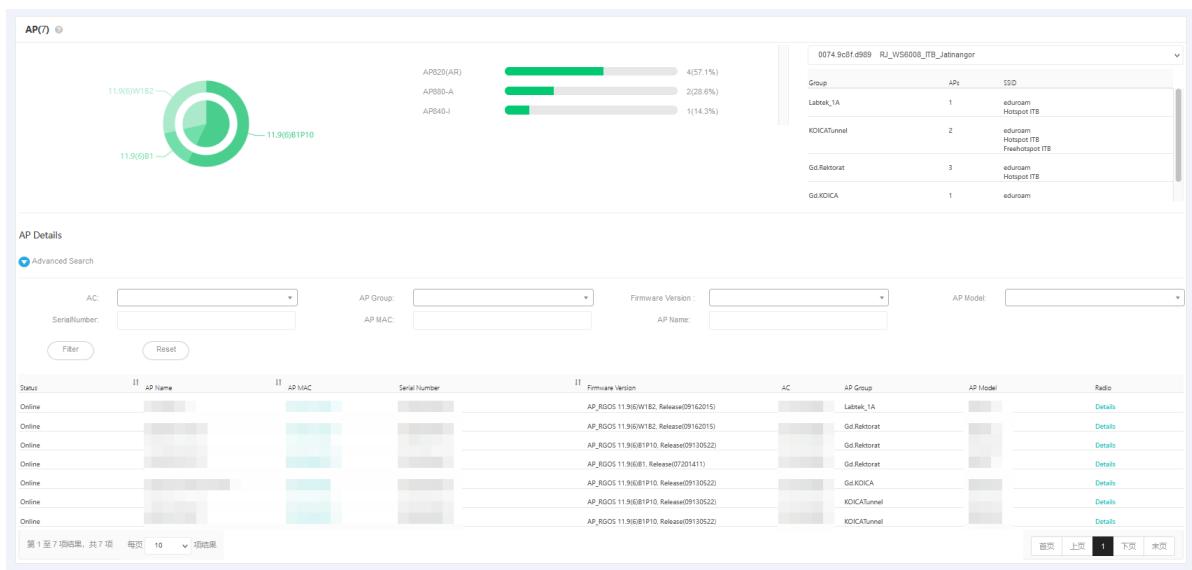
An AC list displays **Name**, **MAC**, **Online AP**, **Firmware Version**, **Hardware Version**, **Model**, and **Role** of ACs. You can click **Details** to display device details, which shows the basic information, load, and performance of the AC.

Figure 8-37 AC Details



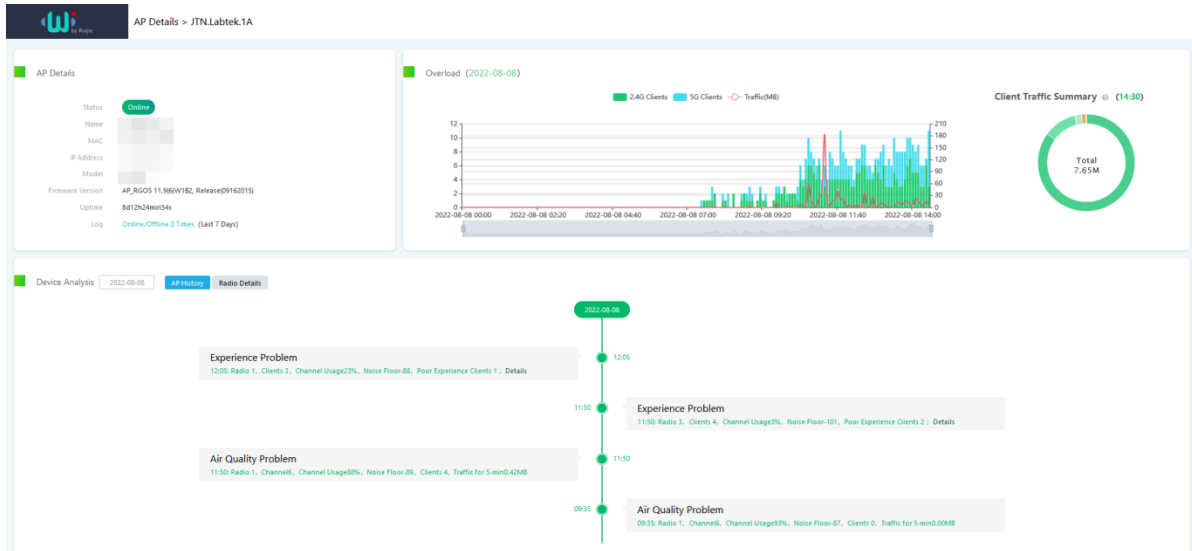
The AP overview page displays the version distribution, model distribution, and details of APs.

Figure 8-38 AP Overview



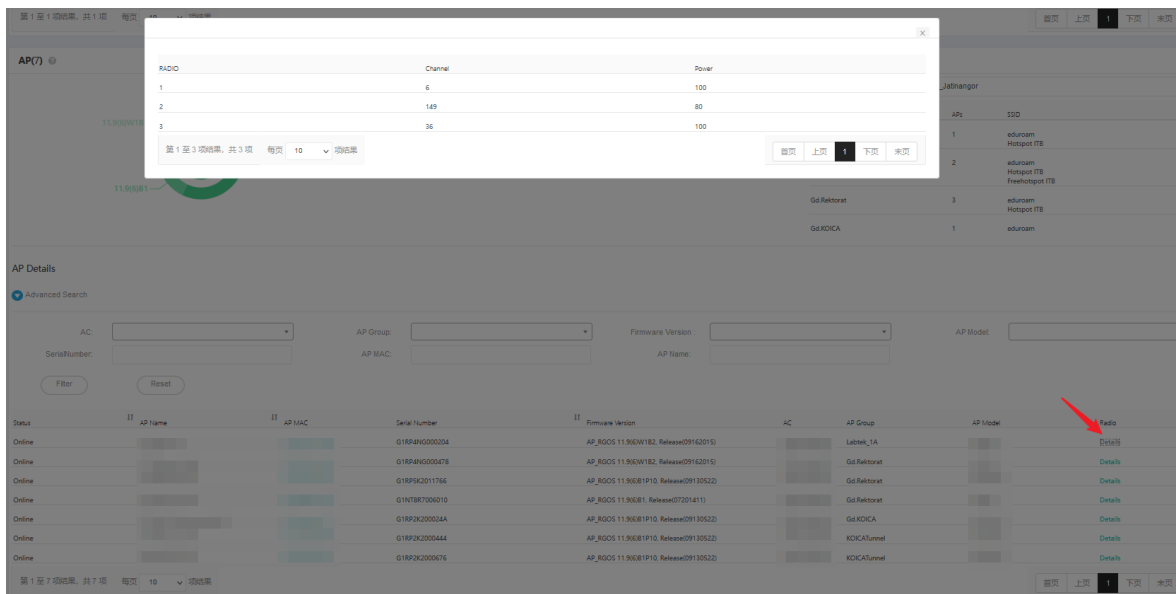
Click the MAC address of an AP to display the AP details, including basic information of the device, load, client traffic proportions, and device analysis records.

Figure 8-39 AP Details



Click **Details** to display radio details.

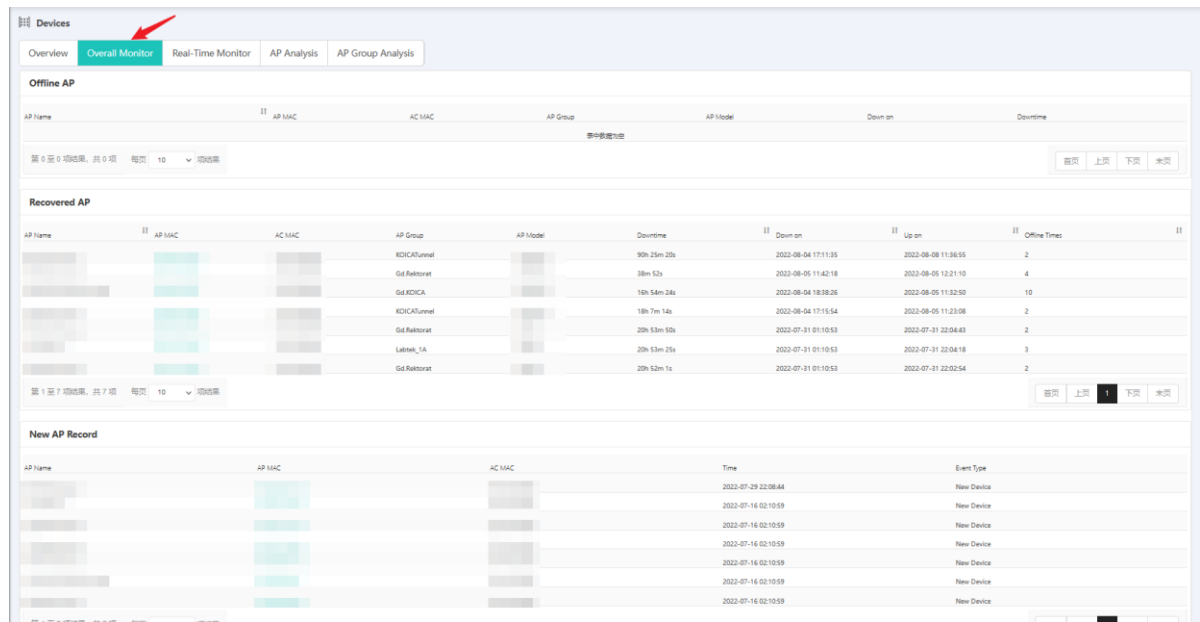
Figure 8-40 Radio Details



2. Overall Monitor

On this page, you can monitor and manage devices, and check offline APs, recovered APs after going offline, new APs, AP going-online/offline alarms, and other detailed information. You can click a MAC address of an AP to display AP details.

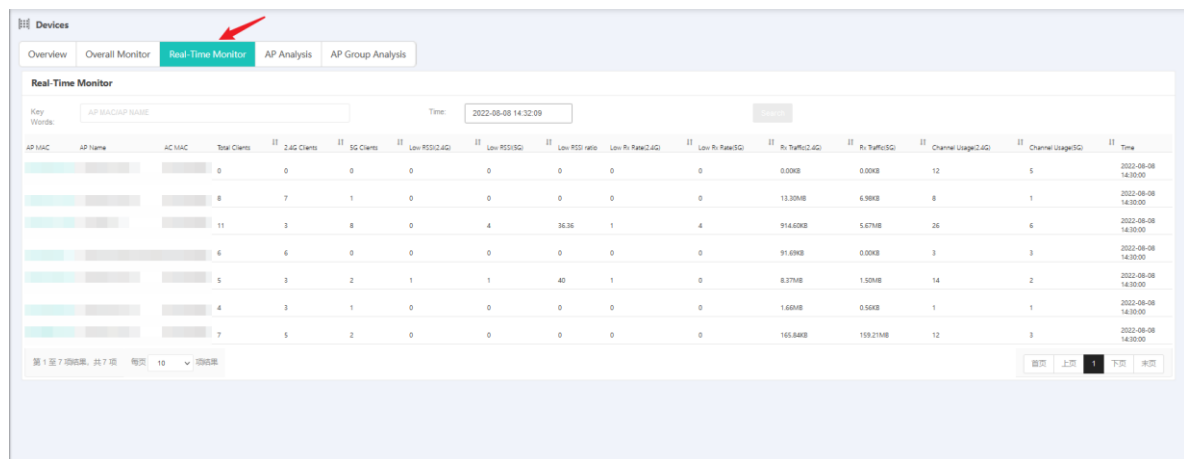
Figure 8-41 Overall Monitor



3. Real-Time Monitor

This tab displays the running statuses of all online devices by default. The statuses are updated once every five minutes. This tab page shows the number of the clients that access the AP, the 2.4G/5G client distribution, the Rx/Tx traffic, and the channel usage. You can filter data by the AP MAC address, AP name, and time. Click a MAC address of an AP in the list to display device details.

Figure 8-42 Real-Time Monitor



4. AP Analysis


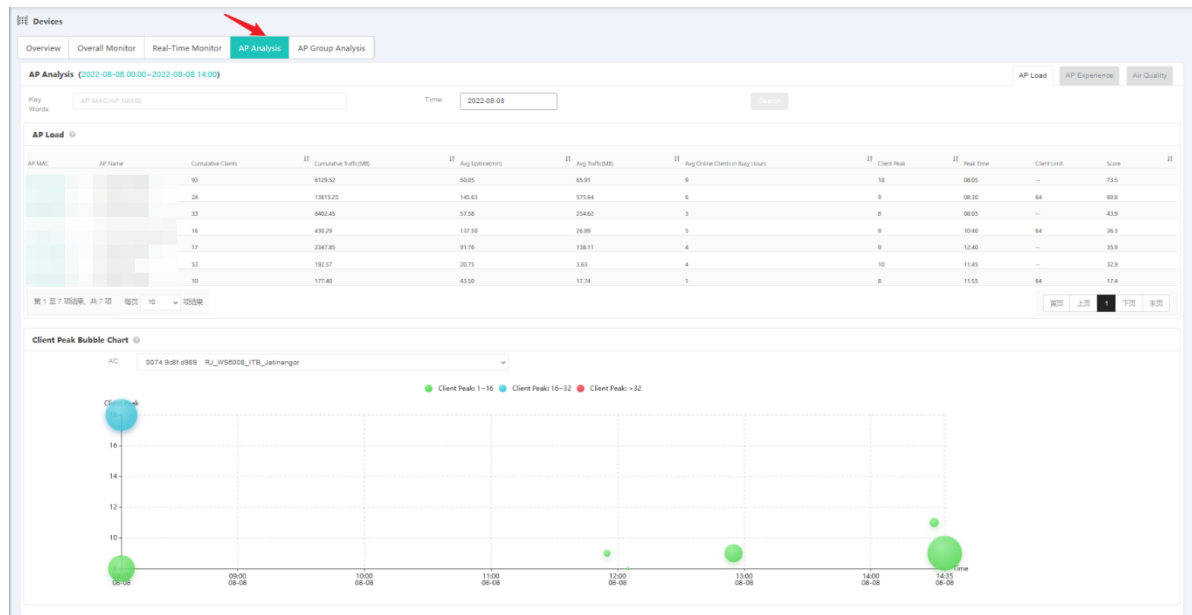
This tab displays the load, peak clients distribution, experience, and air interface of each AP. To display the descriptions of indicators, move the cursor to  next to the graph name.

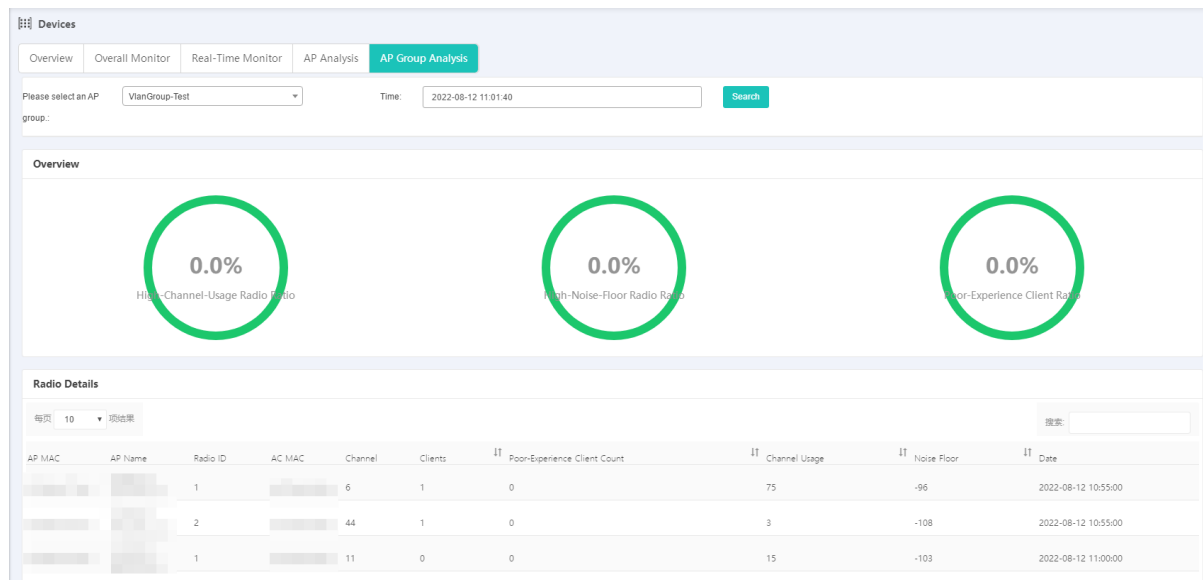
Figure 8-43 AP Analysis



5. AP Group Analysis

This tab performs statistical analysis of AP information based on AP groups.

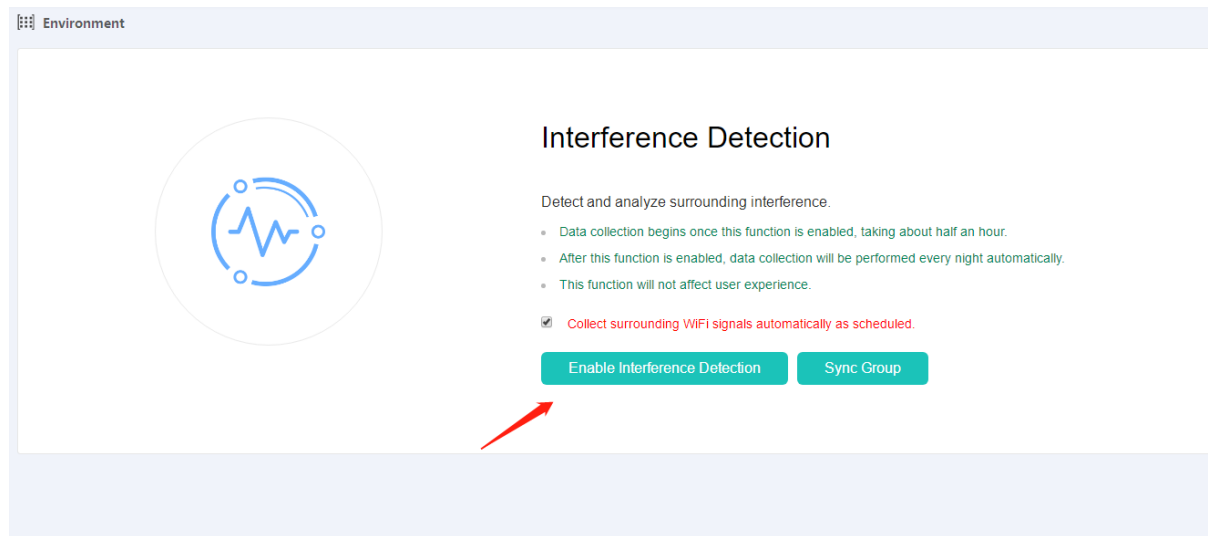
Figure 8-44 AP Group Analysis



8.2.5 Environment

This function is used to check external interference (private Wi-Fi signals). You need to enable it manually. After it is enabled, the environment information will be collected immediately and at 3:00 every early morning.

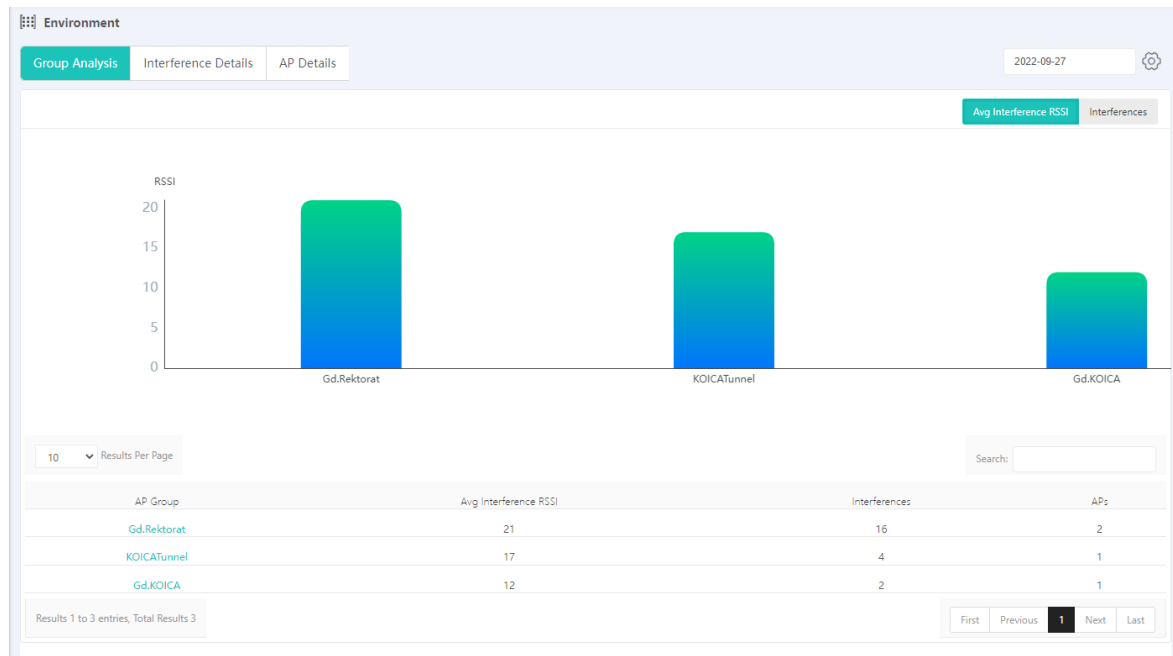
Figure 8-45 Environmental Perception



2. Group Analysis

You can collect interference based on each AP group, and present the statistics by RSSI and the number of interferences.

Figure 8-46 Group Analysis



3. Interference Details

The list displays all scanned interfering signals and the number of radios being affected in the local network. You can click a number to display details of the affected radios.

Figure 8-47 Interference Details

Manufacturer	SSID	BSSID	First Seen on	Influenced APs
Ruckus	eduroam	dcae.eb85.b6bc	2022-07-18 16:06:20	2
Ruckus	Hotspot ITB	dcae.eb45.b6bc	2022-07-18 16:06:20	2
Ruckus	eduroam	389f.36d2.2b4c	2022-08-06 03:10:00	1
Ruckus	Hotspot ITB	389f.36d2.2b4c	2022-08-01 03:10:00	1
Ruckus	Hotspot ITB	dcae.eb45.e6f8	2022-08-01 03:10:00	1
Ruckus	Hotspot ITB	dcae.eb45.e6f8	2022-07-17 20:16:46	1
Ruckus	eduroam	dcae.eb85.e6fc	2022-08-06 03:10:00	1
Ruckus	Hotspot ITB	389f.36d2.2a48	2022-08-01 03:10:00	1
Ruckus	Hotspot ITB	389f.36d2.2b98	2022-08-02 03:10:00	1
Ruckus	Hotspot ITB	dcae.eb45.e6fc	2022-08-06 03:10:00	1

Figure 8-48 Details of Affected Radios

AP Name	AP Mac	Radio ID	Channel	RSSI
		2	149	11
		3	0	5

4. AP Details

This tab displays the details of APs suffering from external interference.

Figure 8-49 AP Interference List

AP Name	AP MAC	Radio ID	Interference
		2	8
		1	6
		1	3
		1	2
		3	2
		2	2
		3	2
		2	2
		1	1

Click a number of interfaces to display details of the external interferences.

Figure 8-50 Interference Details

Manufacturer	BSSID	SSID	RSSI
Ruckus	88E3442.245C	edunam	18
Ruckus	88E3442.2457		18
Ruckus	5478.188a.54ac	edunam	12
Ruckus	5478.188a.54ac	Hongque ITB	12
Ruckus	54ac.3F23.653c	Hongque ITB	12
Ruckus	54ac.3F23.653c	edunam	11
Ruckus	88E3442.284c	edunam	11
Ruckus	88E3442.284c	Hongque ITB	11

8.3 Optimization

8.3.1 One Key Diagnosis

Choose **Intelligent Analysis > Optimization > One Key Diagnosis**. The network diagnosis module is fixed to check the running status of the entire network on the previous day every night, and provide a network health index according to the results of the test items. You can quickly understand the health status of the current network from the network health index, and click **Get Real-Time Result** to obtain the current diagnosis result.

Figure 8-51 One Key Diagnosis

2022-08-07, Network Health Index 100.0

Found hidden problems: 0 Problem(s)

Get Real-Time Result

Device check

- AC Performance Analysis**
The CPU usage and memory usage of the AC are sampled on a day. If the CPU usage and memory usage are found to be higher than the threshold for three times, the AC is a risk. The CPU usage threshold is 80% and the memory usage threshold is 85%. [Suggestion](#)
- Risky ACs**
- AP Offline Check**
 - Single AP Goes Offline: 0**
Check AP offline status. If an AP is found to go offline for eight times a day, a risk occurs. [Suggestion](#)
 - Multiple APs Go Offline: No Risk**
Check AP offline status. If an AP goes offline more than twice in average in an hour, or more than 80% APs go offline, or over five APs go offline, a risk occurs. [Suggestion](#)
 - Offline AP: 0**
Check offline AP list [Suggestion](#)

Configuration check

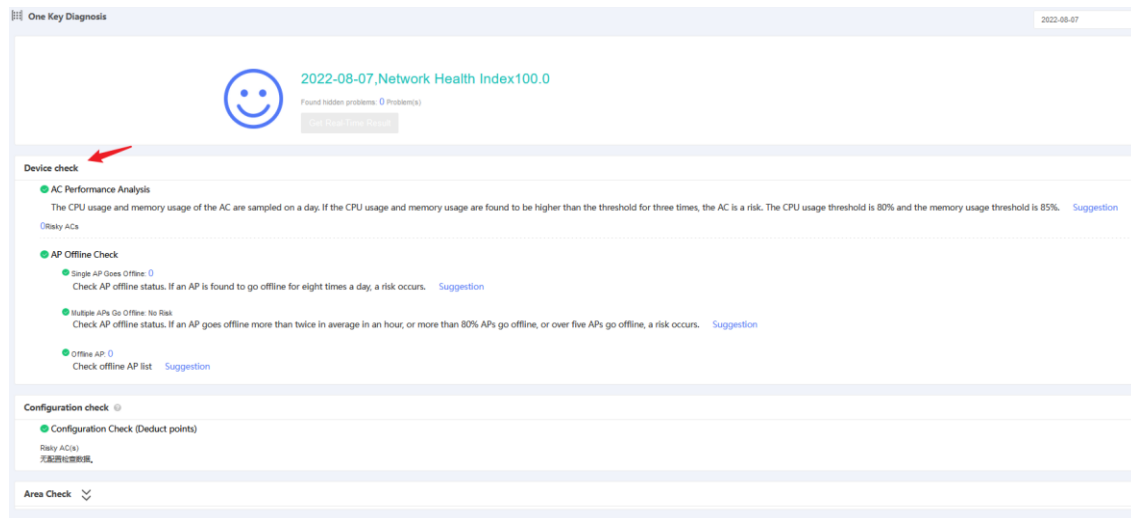
- Configuration Check (Deduct points)**
Risky AC(s)
无配置检查数据。

Area Check

(1) Device Check

This function checks for exceptions and risks on ACs and APs, which are the most basic components of the wireless network. The check items include AC performance analysis and AP offline check. After the check, you can click **Suggestion** to obtain optimization suggestions provided by the system.

Figure 8-52 Device Check



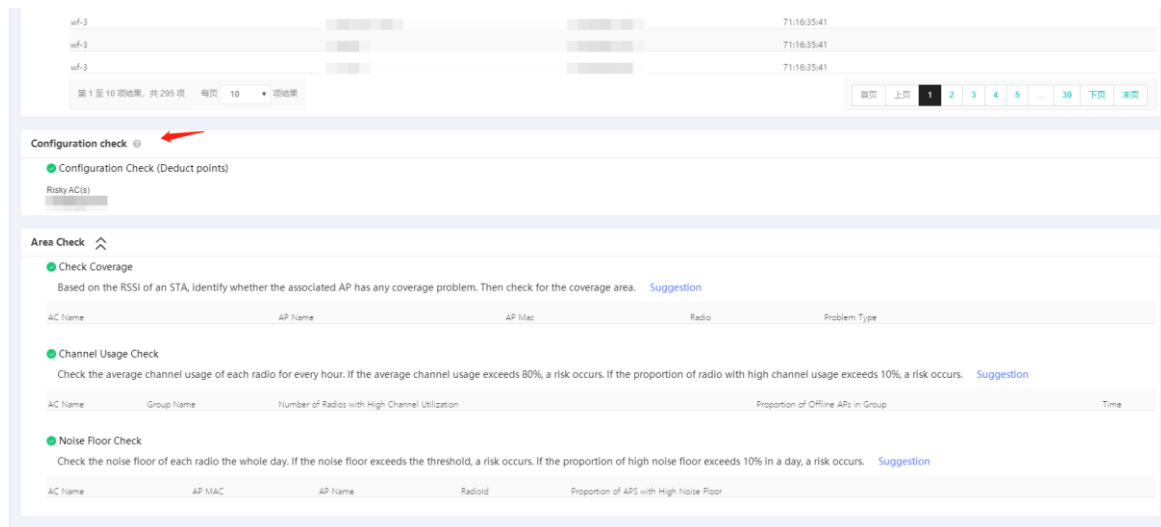
(2) Configuration Check

This function collects device configurations and checks for configuration risks based on the WISPI rule library on cloud.

Caution

This function requires that the server can access wispi.ruijie.com.cn.

Figure 8-53 Configuration Check



(3) Area Check

This function performs the following checks on air interfaces in the network for common risks:

- o **Check Coverage:** Check whether a coverage problem occurs on an AP based on the RSSI of STAs

associated with the AP, and figure out whether the coverage is too large or insufficient based on Coverage.

- **Channel Usage Check:** Check the average channel usage of an AP radio in an hour. If the usage exceeds 80%, the AP radio is considered to be at risk in channel usage. If the proportion of radios with high channel usage in a group exceeds 10%, the group may have risks. In this case, it is necessary to determine whether channels in the area are too congested (due to too much co-channel interference or over-high load), and whether more devices are required for coverage.
- **Noise Floor Check:** Test the noise floor of each AP radio all day long. If the noise floor of an AP radio exceeds the threshold, the AP radio is considered to have the risk of high noise floor. If the proportion of an AP radio's tests with high noise floor to the total test count exceeds 10%, the AP radio is considered to be at risk.

Figure 8-54 Area Check

The screenshot shows the 'Area Check' interface with three sections:

- Check Coverage:** Based on the RSSI of an STA, identify whether the associated AP has any coverage problem. Then check for the coverage area. [Suggestion](#)

AC Name	AP Name	AP Mac	Radio	Problem Type

- Channel Usage Check:** Check the average channel usage of each radio for every hour. If the average channel usage exceeds 80%, a risk occurs. If the proportion of radio with high channel usage exceeds 10%, a risk occurs. [Suggestion](#)

AC Name	Group Name	Number of Radios with High Channel Utilization	Proportion of Offline APs in Group	Time

- Noise Floor Check:** Check the noise floor of each radio the whole day. If the noise floor exceeds the threshold, a risk occurs. If the proportion of high noise floor exceeds 10% in a day, a risk occurs. [Suggestion](#)

AC Name	AP MAC	AP Name	Radio	Proportion of APs with High Noise Floor

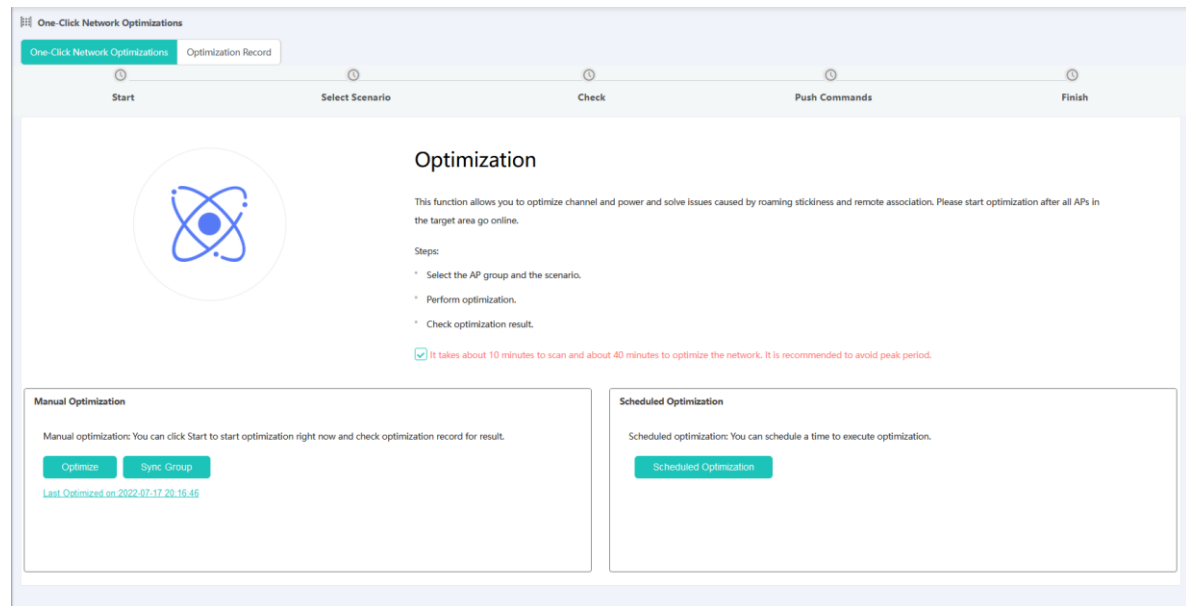
8.3.2 One-Click Network Optimization

This function is used for automatic planning of AP channels and power in the wireless network environment to improve user experience in the WLAN. After the function is triggered, the server collects information about AP radios, calculates and allocates channel resources in a unified manner, and delivers the optimized configuration to devices.

Caution

- Use this function after all APs in the area to be optimized go online. After the optimization starts, do not turn on or off APs or radios.
- During the optimization, the channels of devices will switch, causing clients go offline and affecting the experience. Therefore, please properly arrange the network optimization time period.
- You can set the time of scheduled optimization in network optimization configuration, and the background will automatically perform the optimization at the time.
- The process will take about 15–30 minutes (depending on the device scale). After it is completed, network optimization details will be displayed, showing the channel and power configuration changes of APs.
- The planning result of network optimization will be delivered as a configuration task. This process may take some time if there are many devices. (You can filter out "radio optimization" in the configuration task list.)

Figure 8-55 One-Click Network Optimization



Two optimization methods are available:

- **Manual Optimization:** Optimization is performed at once.
- **Scheduled Optimization:** You can specify the optimization time, and the system will automatically perform the optimization at the specified time.

Based on the collected scan data, WIS Cloud Network calculates channel optimization solutions that are applicable to various scenarios in the background. To ensure the accuracy of the channel optimization solution, you need to manually select the scenario of each group.

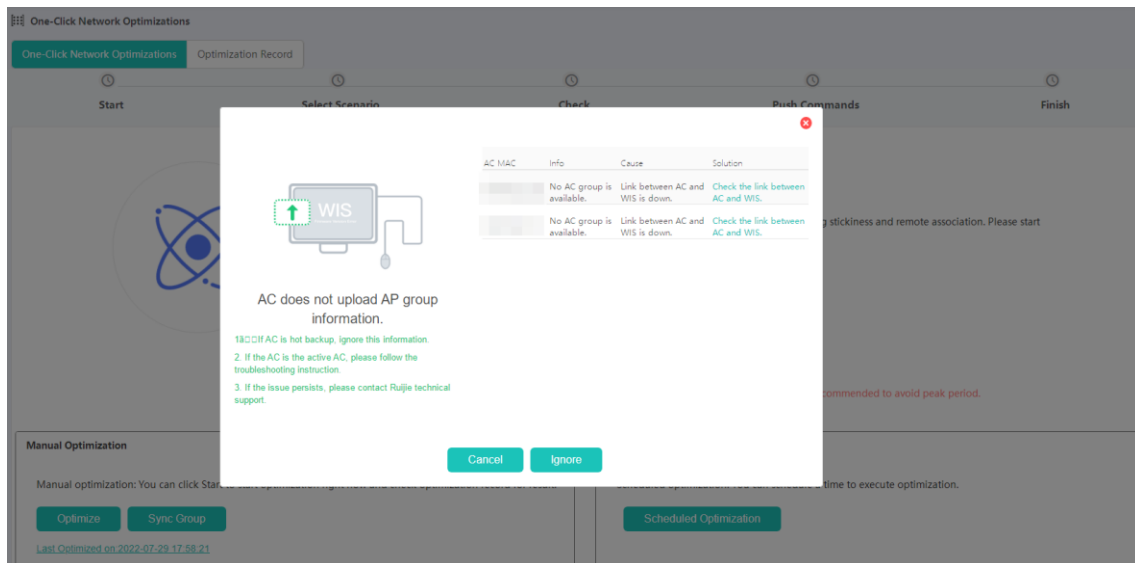
After the scan is completed, check data integrity. For groups with a data loss rate exceeding 10%, you are advised to scan the data again. If the data loss rate is less than 10%, proceed to the next step.

Procedure for one-click optimization:

(2) **Start**

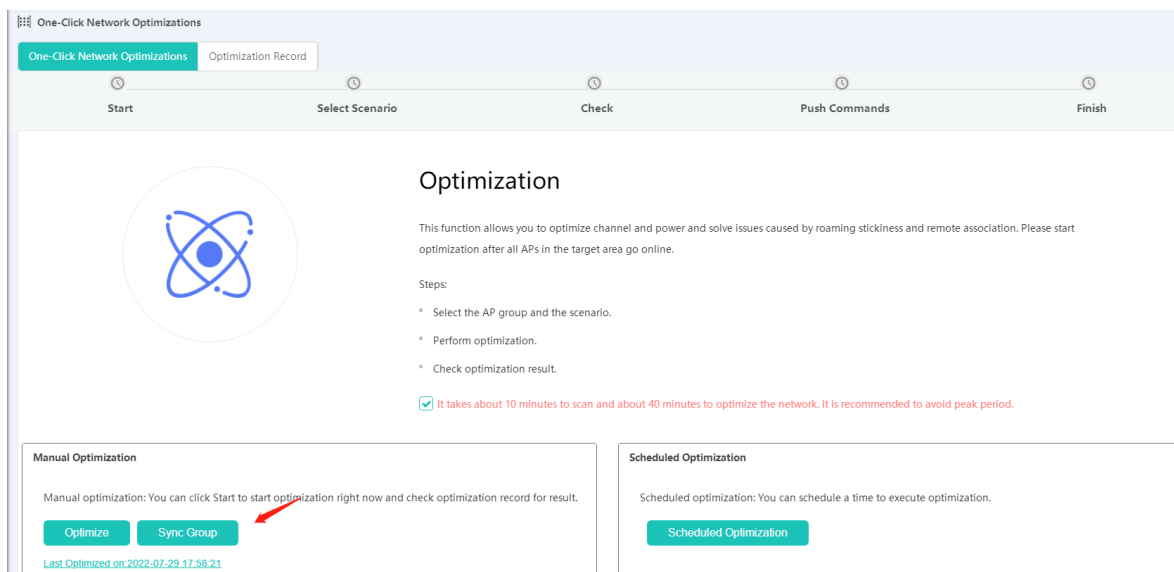
Click **Start**. Then, the system automatically detects the statuses of ACs. If an AC does not report AP group information, the AC cannot be optimized.

Figure 8-56 Optimization Detection



To ensure that the current group data is the latest, you can update the group data before optimization. Update will take five minutes.

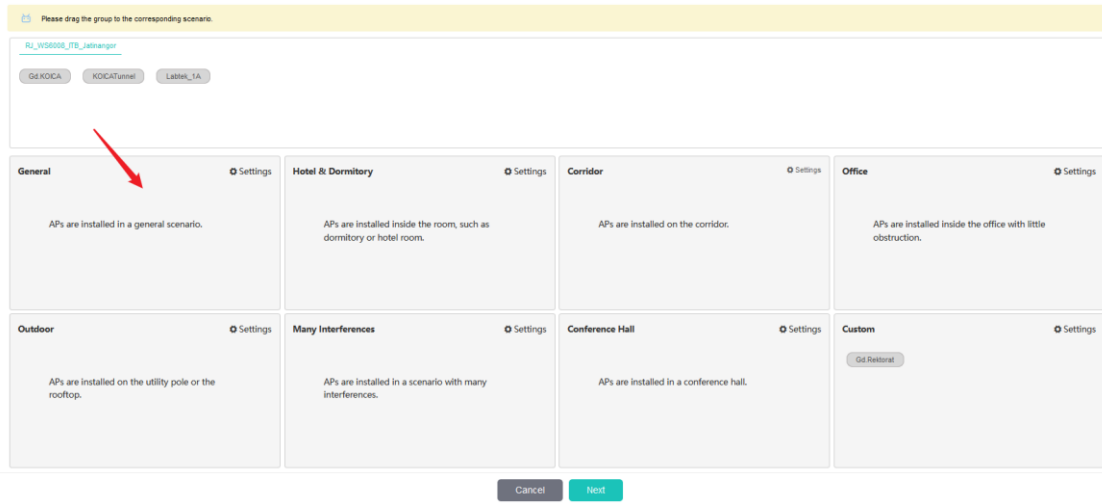
Figure 8-57 Updating Group Data



(2) **Select Scenario**

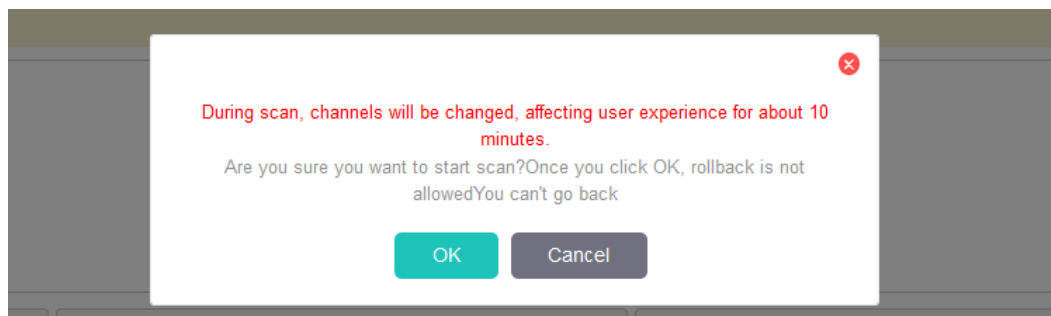
Drag groups to corresponding scenarios based on the actual situation.

Figure 8-58 Select Scenario



During wireless signal scanning, the channels of APs will switch, and the network will be disconnected for about 10 minutes. Avoid peak business hours.

Figure 8-59 Scan Prompt



(3) Check

Figure 8-60 Check

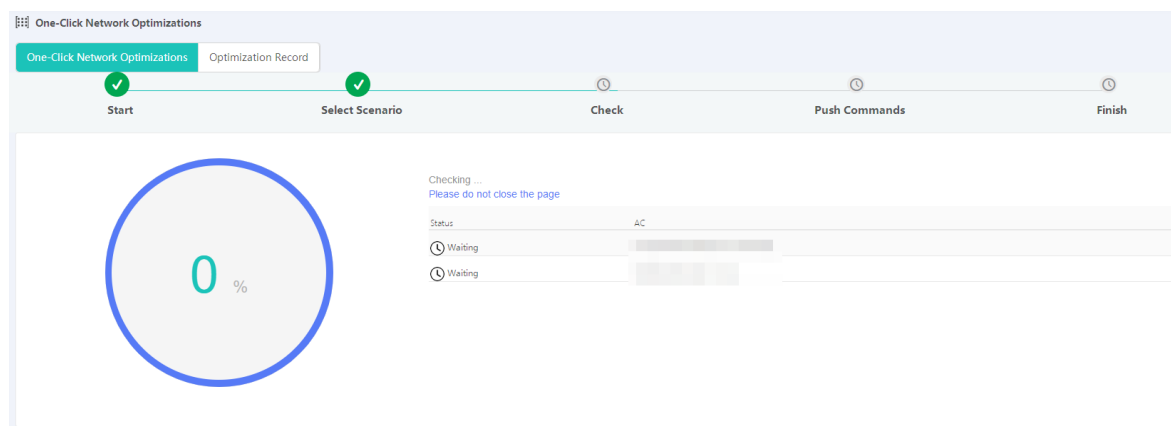
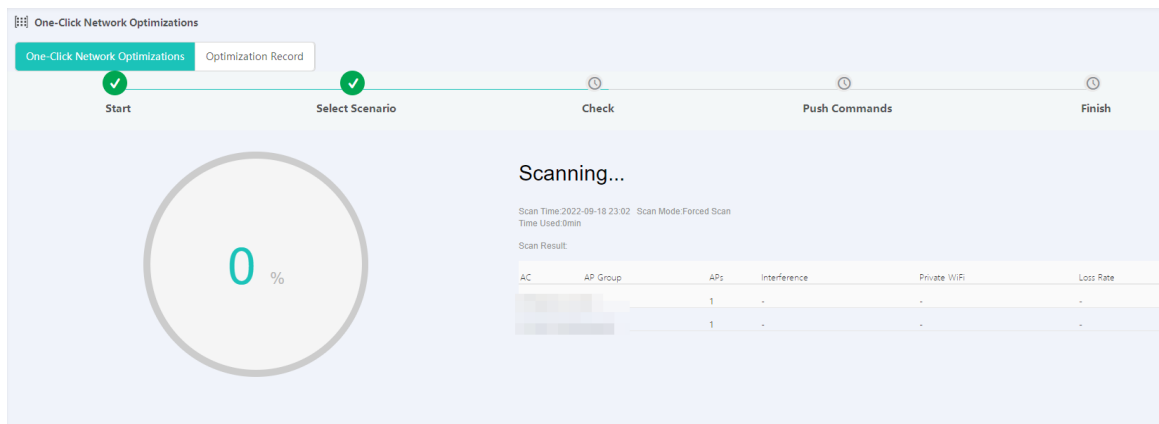


Figure 8-61 Scanning

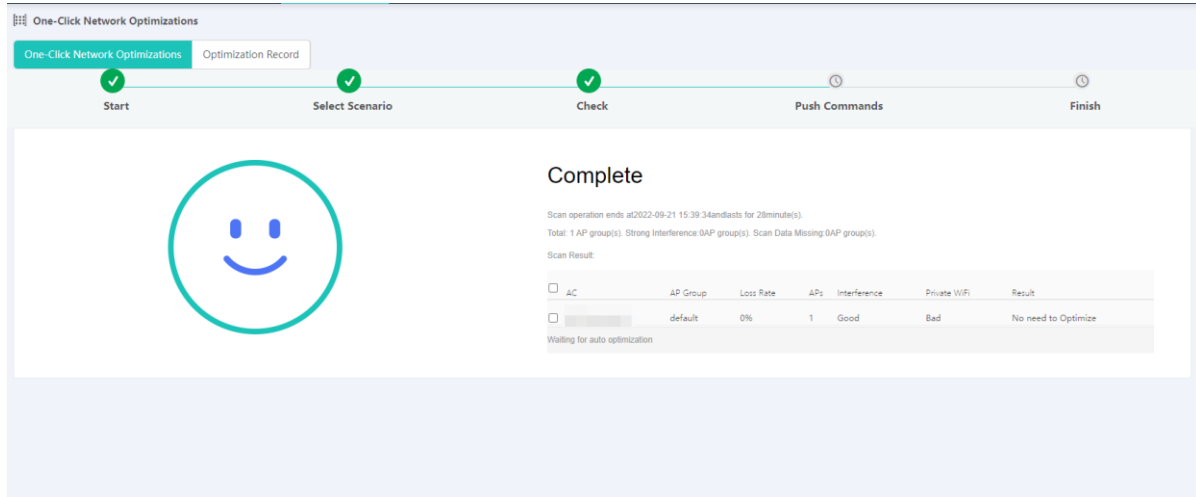


If the system fails in automatically delivering the command, manually copy the command to the AC and run it.

(4) Push Commands

After the scan, the system will display the check result, and schedule to automatically deliver the optimized configuration.

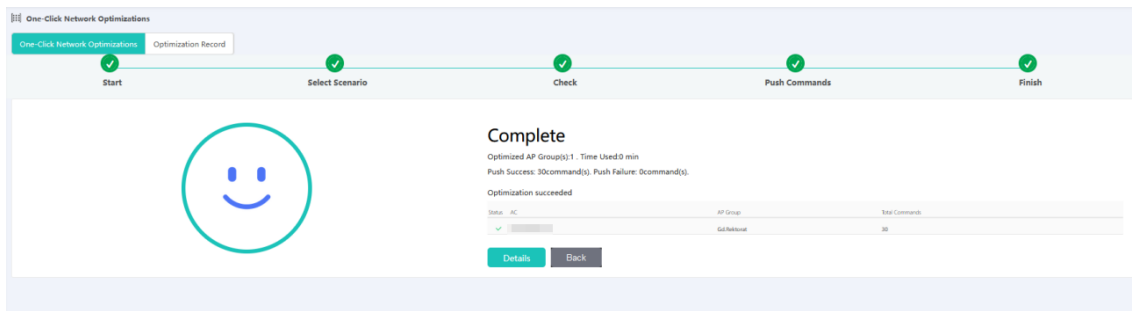
Figure 8-62 Push Commands



(5) Finish

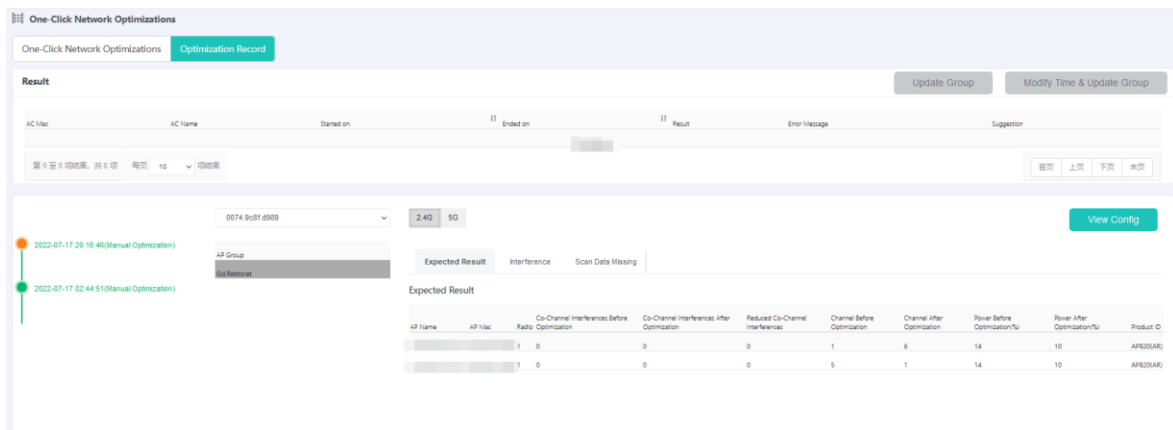
Wait for the optimization completion and check the result on the page.

Figure 8-63 Finish



The system records all network optimizations, and you can restore the configuration before the optimization when necessary.

Figure 8-64 Optimization Record



8.3.3 Access Optimization

WIS Cloud Network provides intelligent access for roaming stickiness and remote association. You can monitor and observe the data for a period of time, and consider whether to enable optimization.

Figure 8-65 Access Optimization

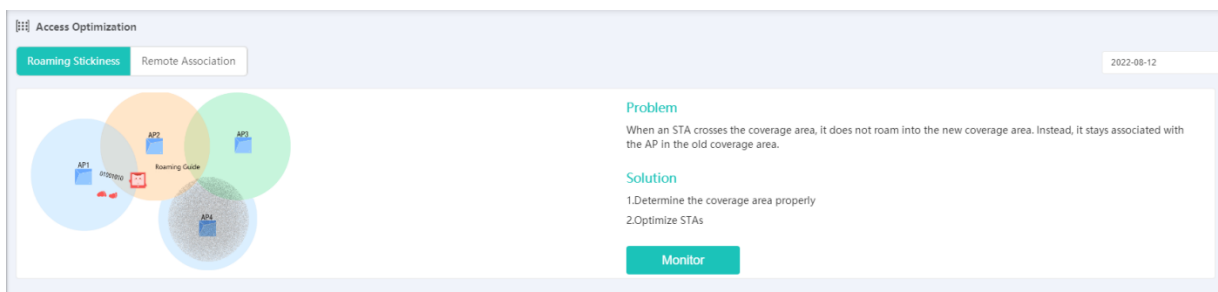
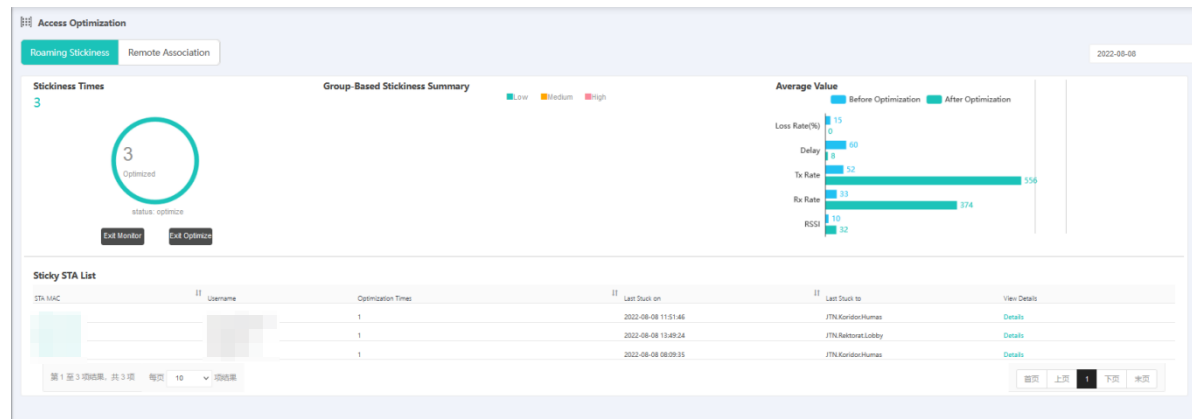
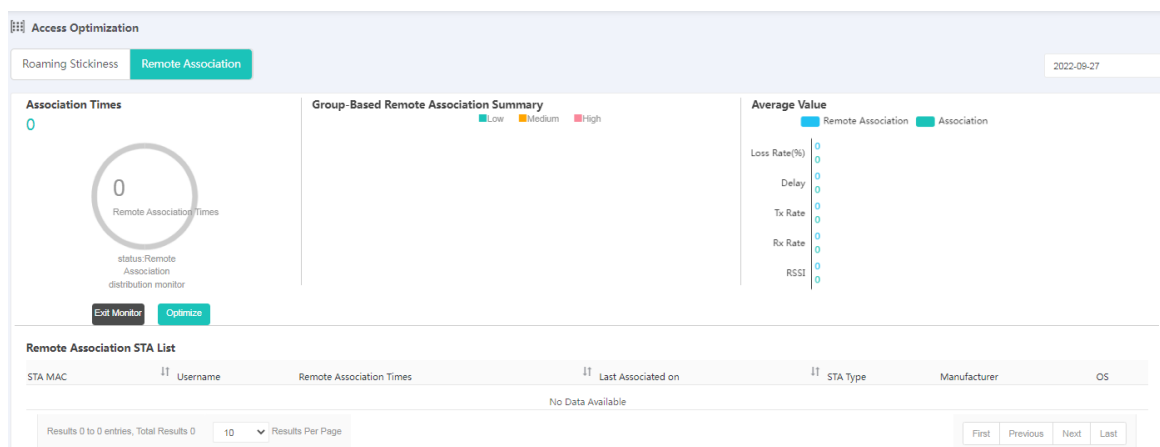


Figure 8-66 Roaming Stickiness



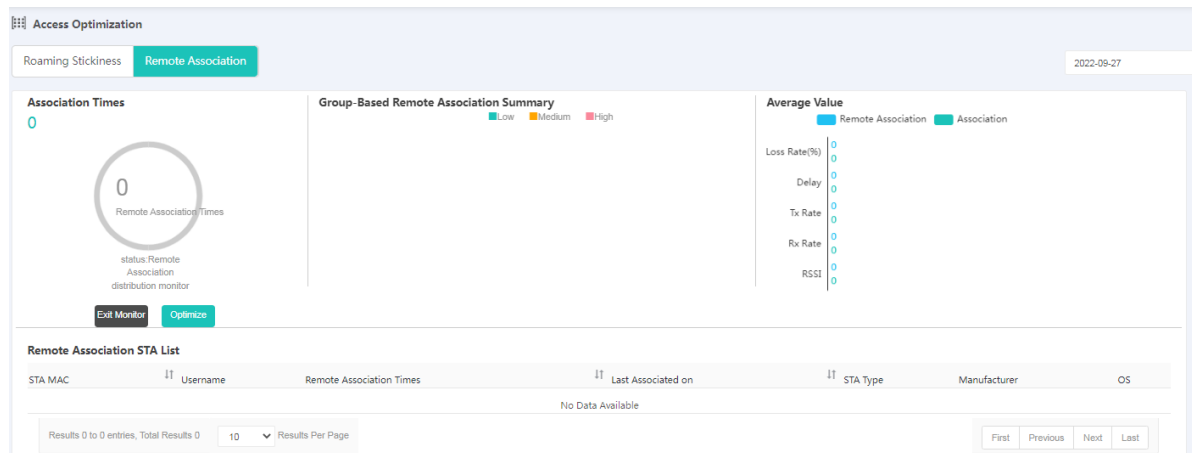
This page displays roaming stickiness times, distribution, average values of network indicators, and sticky STAs.

Figure 8-67 Remote Association



Remote association indicates that when an AP can connect to a better AC, it still connects to the previously connected AC, affecting the network experience. Click **Detect** to detect remote association of APs in the current network. You can adjust the power of AP management packets, or the access range, to ensure that only one AP provides strong signals within the coverage, and therefore solve the problem of AP remote association.

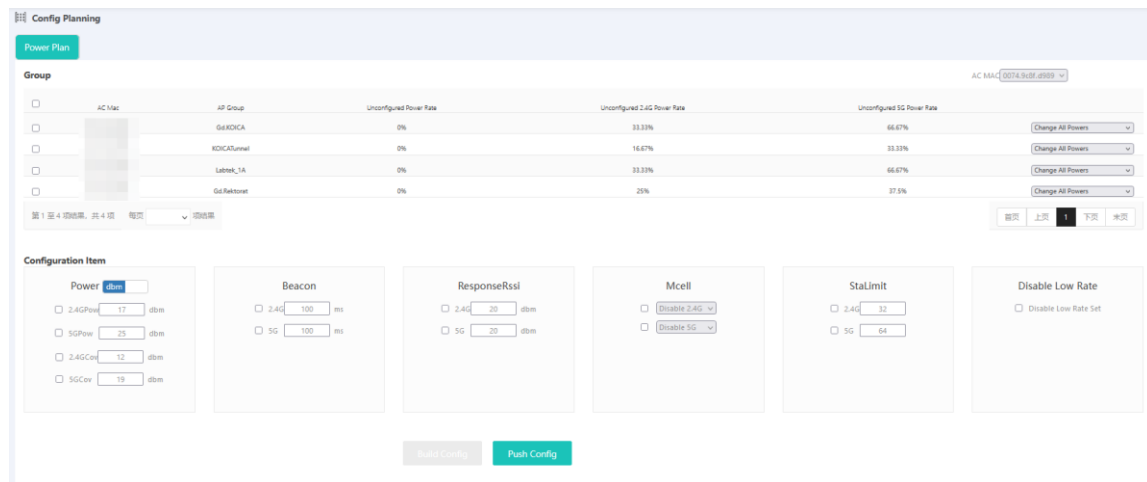
Figure 8-68 Remote Association Detection Result



8.3.4 Config Planning

On this page, you can visually configure common radio parameters, and then select to generate configuration, manually copy the configuration to the AC, and execute it, or automatically deliver the configuration.

Figure 8-69 Config Planning



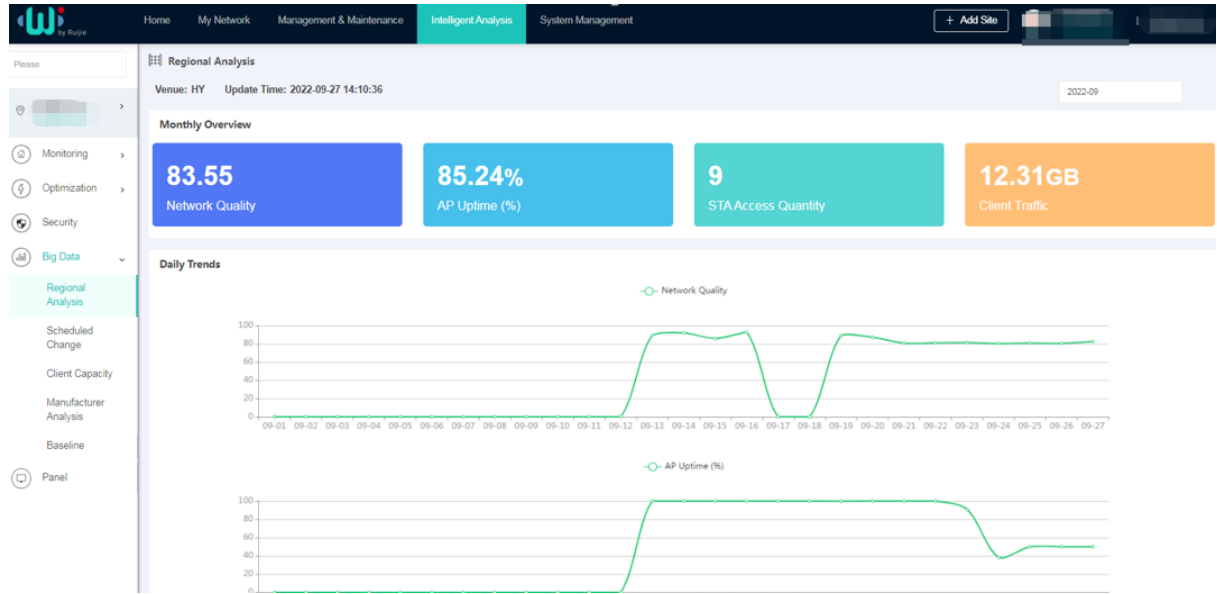
8.4 Big Data

8.4.1 Regional Analysis

This page displays the following information:

- Network quality, AP online rate, STA access quantity, and STA traffic of the project and all subareas (divided by AP group)
- Monthly indicators of subareas
- Daily trends of indicators

Figure 8-70 Regional Analysis



8.4.2 Scheduled Change

This page displays all configuration change and network optimization records. Click a point to display the change details.

Figure 8-71 Scheduled Change

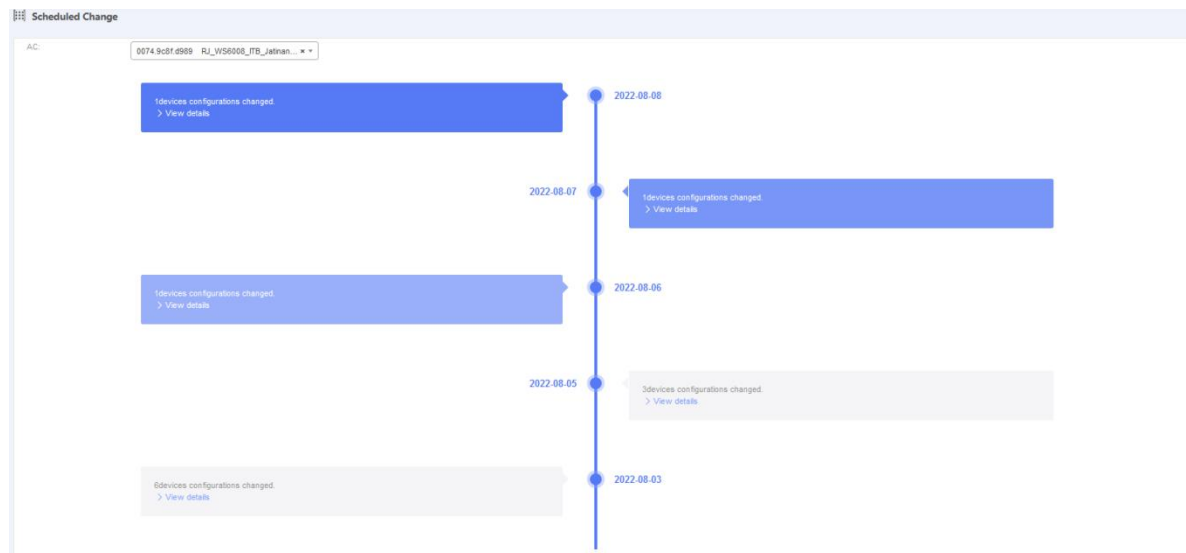
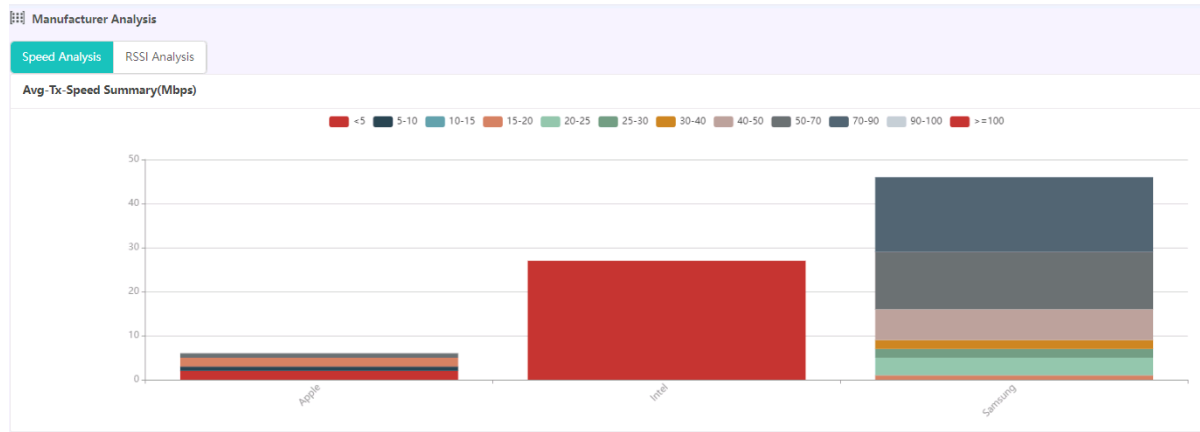


Figure 8-73 Speed Analysis



8.4.5 Baseline


This function analyzes network KPIs based on baselines to detect exceptions. Network KPIs include: **STA Traffic**, **Association Failures**, **Avg Packet Loss Rate (2.4G)**, **Avg Delay (2.4G)**, **Avg Packet Loss Rate (5G)**, and **Avg Delay (5G)**. To display the descriptions of indicators, move the cursor to  next to the graph name.

Figure 8-74 Baseline



8.5 Panel

The system provides the panel function with two preset templates.

Figure 8-75 General Panel

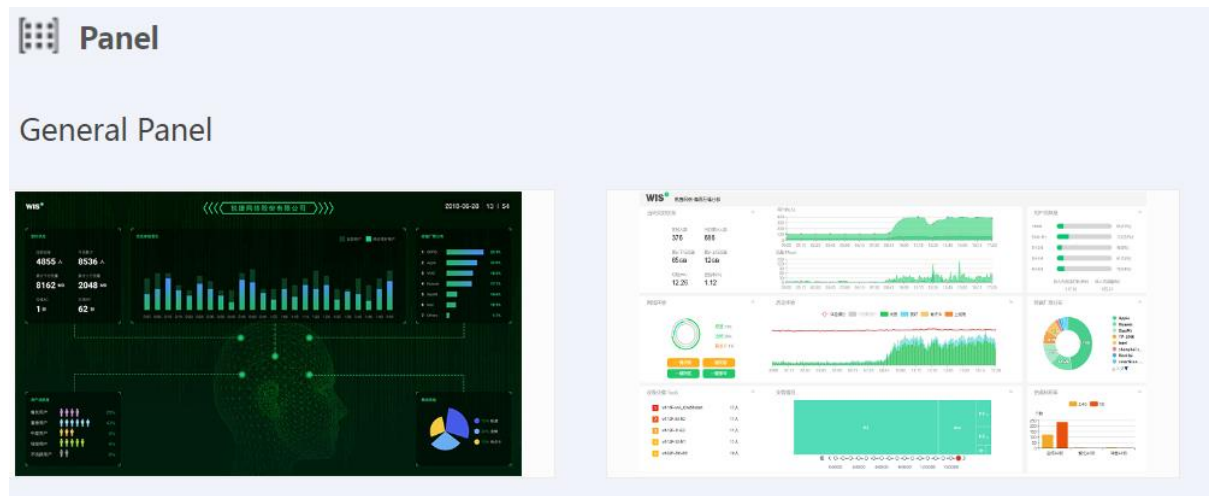


Figure 8-76 Preset Panel 1

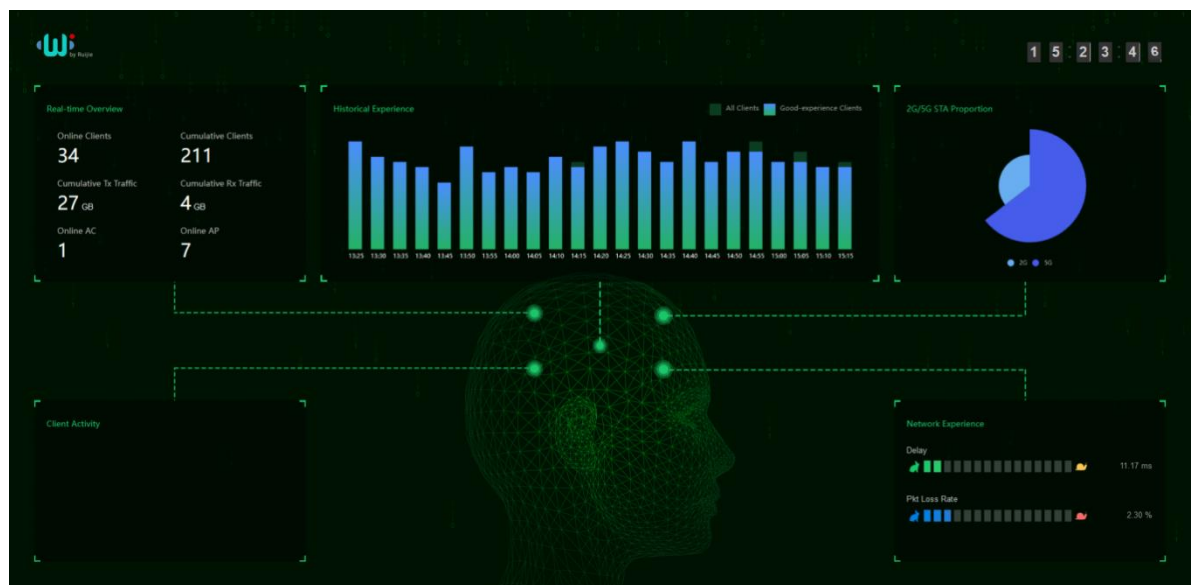
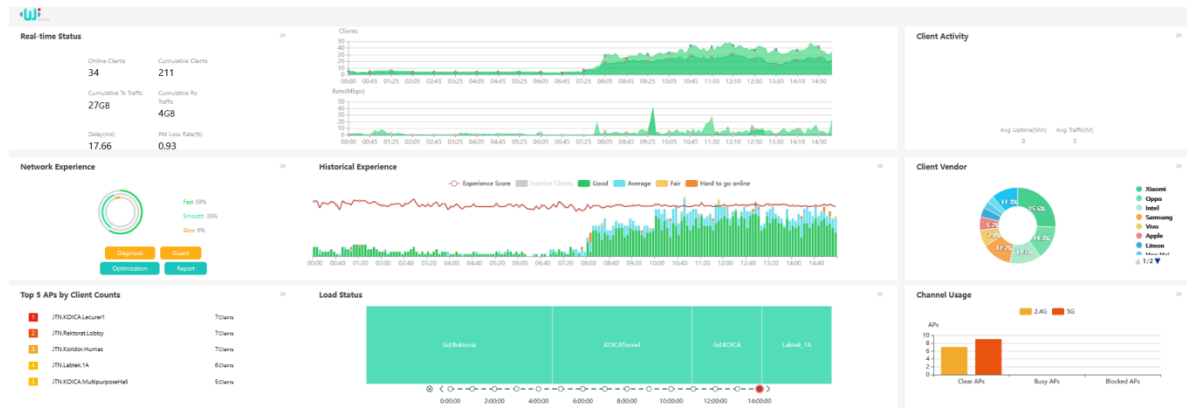


Figure 8-77 Preset Panel 2

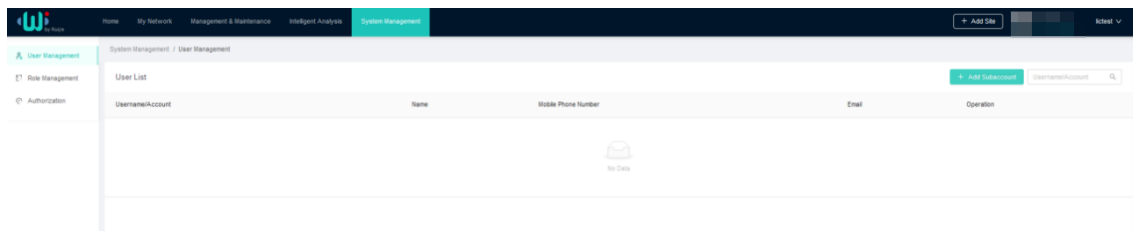


9 System Management

9.1 User Management

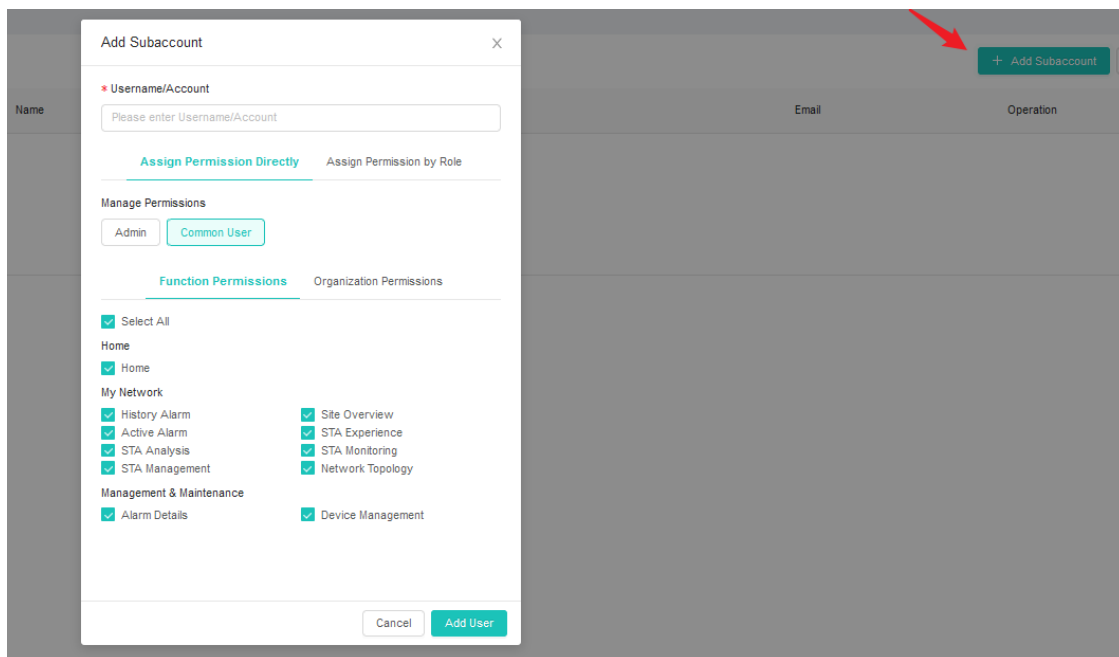
Choose **System Management > User Management**.

Figure 9-1 User Management



Click **Add Subaccount** to add a new system subaccount.

Figure 9-2 Add Subaccount



The following configurations are required:

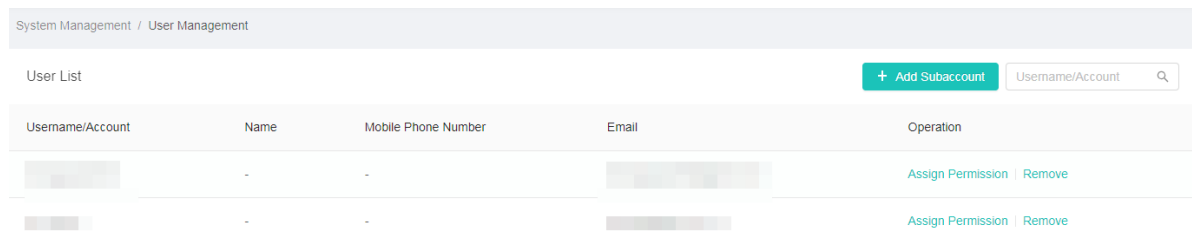
- **Username/Account:** (Required) The username of a new subaccount can contain letters, digits, underscore (_), hyphen (-), and at sign (@).
- **Manage Permissions:** Two options are available: **Admin** and **Common User**. An admin account has configuration-related function permissions, and a common user has only viewing-related function

permissions.

- **Function Permissions:** These permissions, or menu permissions, are assigned by function. Functions without assigned permissions will be unavailable.
- **Organization Permissions:** (Required) These permissions are assigned by organization and area. Organizations and areas without assigned permissions will be unavailable.
- **Assign Permission by Role:** Assign a role for the new account, and the account accesses the system with permissions assigned to the role.

You can click **Assign Permission** or **Remove** in the **Operation** column to re-assign permissions to an existing account or delete the account.

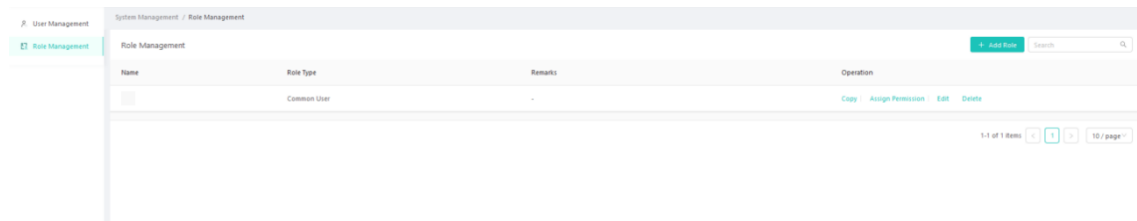
Figure 9-3 Assign Permission and Remove



9.2 Role Management

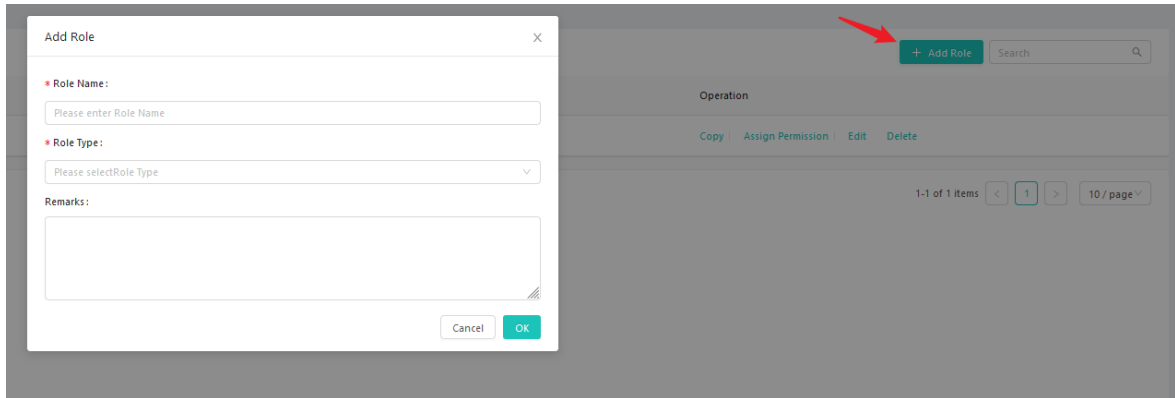
On this page, you can create a new role, assign menu and data permissions to roles, and manage existing roles, such as modifying them, deleting them, or assigning permissions to them.

Figure 9-4 Role Management



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

Figure 9-5 Adding a Role

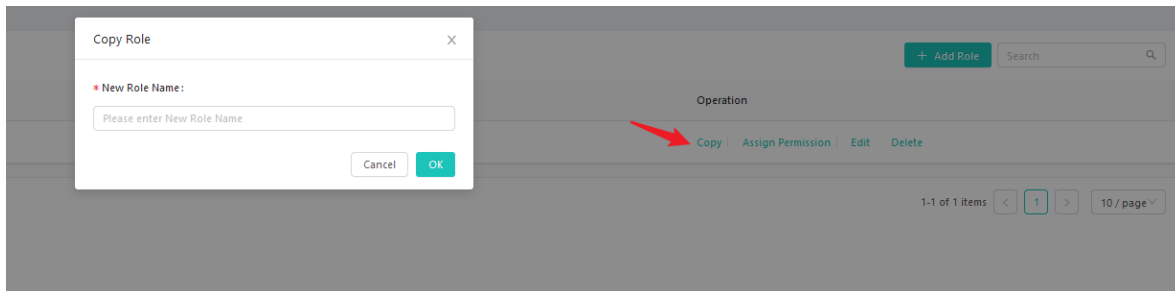


Configuration description:

- **Role Name:** (Required) The value can contain no more than 50 characters of letters, digits, underscore (_), hyphen (-), at sign (@), and ampersand (&).
- **Role Type:** (Required) The value can be **Admin** or **Common User**. An admin has management permissions, while a common user has only viewing permissions.
- **Remarks:** (Optional) The role remarks can contain no more than 400 characters.

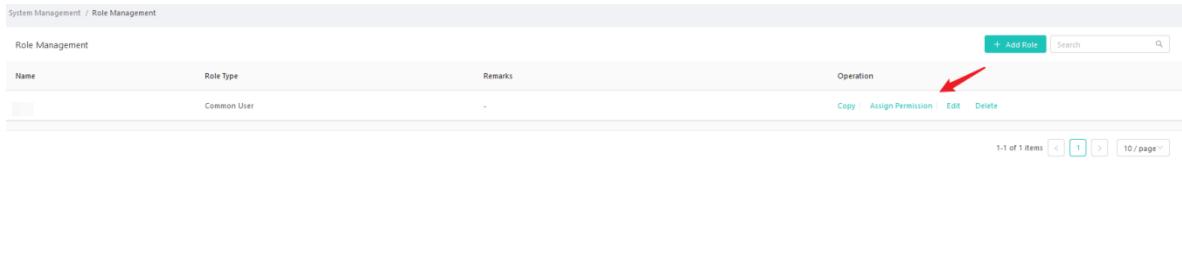
You can click **Copy** to add a role quickly, and the permissions of the new role are the same as those of the original role.

Figure 9-6 Copy Role



You can assign, modify, or delete the permissions of existing roles, and delete roles. If a role is bound to a user, you need to delete or unbind the user before you can delete the role. That is, a role that is bound to a user cannot be directly deleted.

Figure 9-7 Assign Permission and Remove



10 Appendix

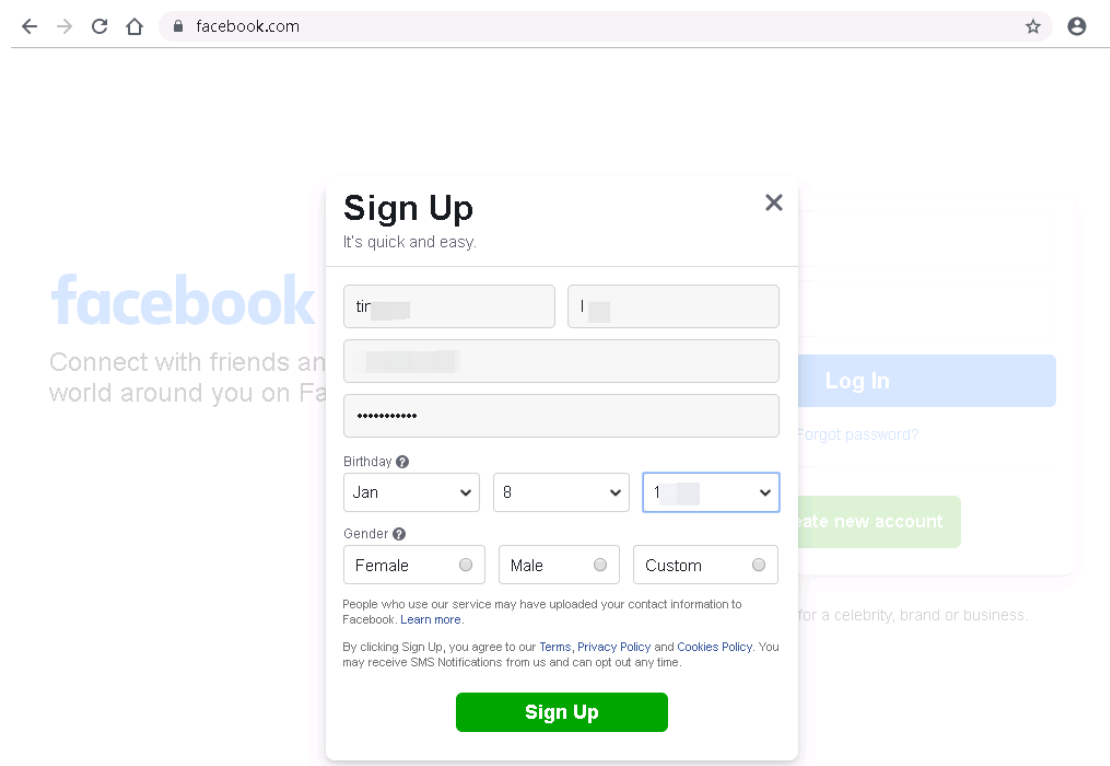
10.1 Configuring a Facebook App

This section explains how to register as a Facebook developer and gain access to the App development tools.

10.1.1 Registering as a Facebook Developer

1. Create a Facebook Account

Enter www.facebook.com in the address bar of a browser. Click **Create new account** to create a Facebook account.

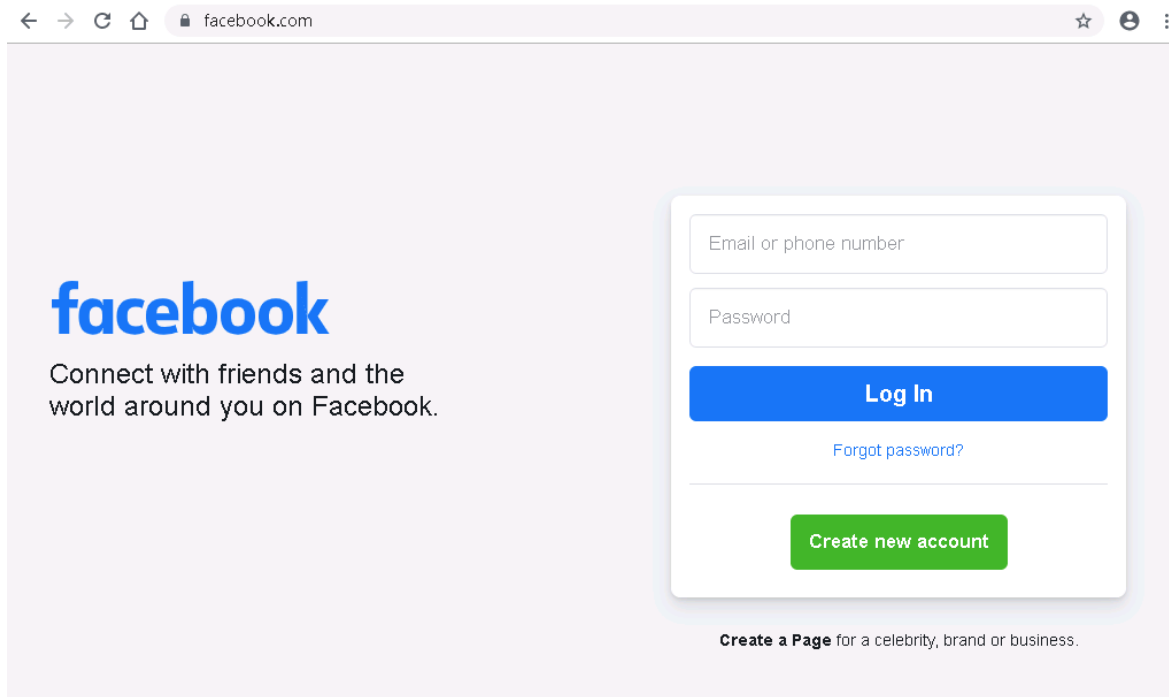


The image shows a browser window with the address bar containing "facebook.com". A "Sign Up" modal form is overlaid on the page. The form includes the following fields and options:

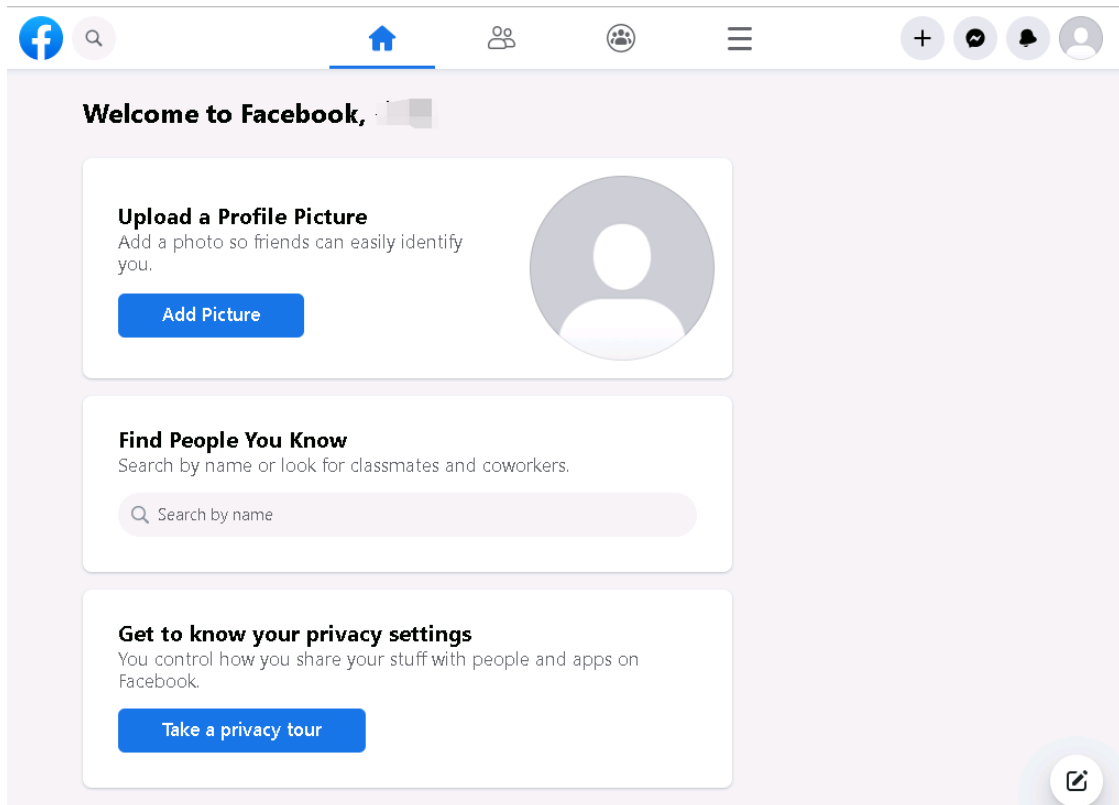
- First name: "tir"
- Last name: "l"
- Phone number: [Redacted]
- Password: [Redacted]
- Birthday: Jan 8, 1
- Gender: Female (selected), Male, Custom

Below the form, there is a green "Sign Up" button. The background shows the Facebook logo and the text "Connect with friends and the world around you on Facebook".

If you already have a Facebook account, enter your username and password.

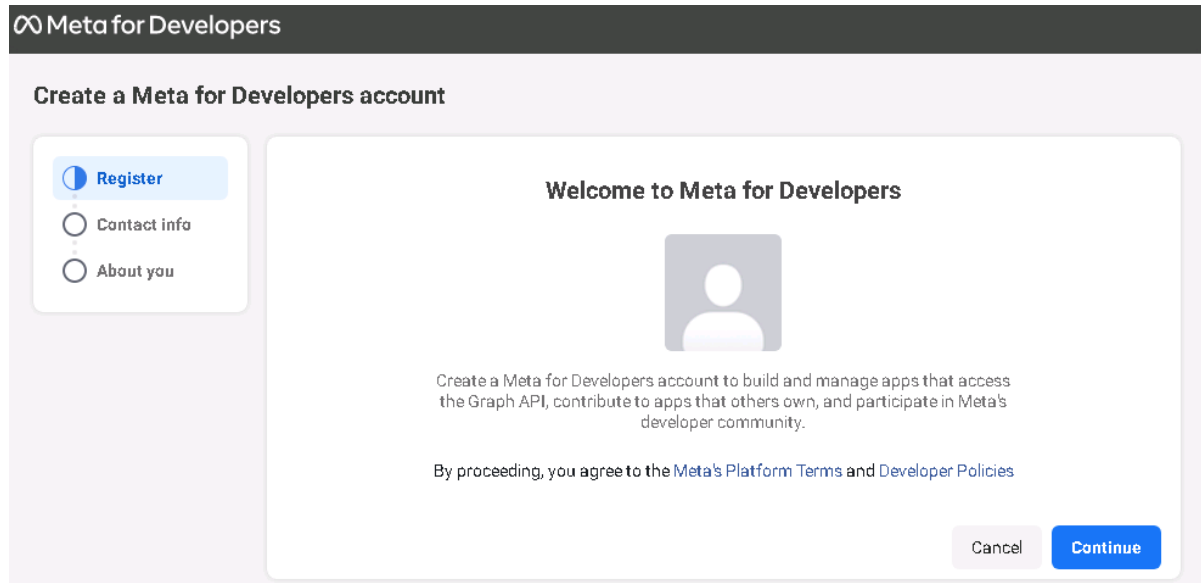


Click **Log In** to enter Facebook.



2. Agree to the Meta's Platform Terms and Developer Policies

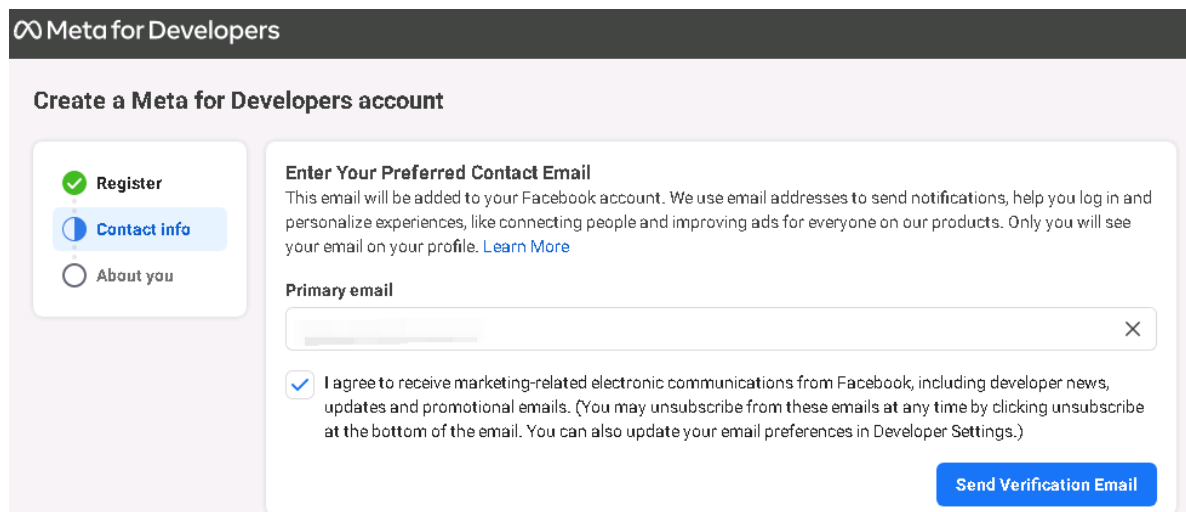
After successful login, go to <https://developers.facebook.com/async/registration>. Click **Continue** on the **Meta for Developer** page.



The screenshot shows the 'Meta for Developers' registration page. At the top, there is a dark header with the Meta logo and the text 'Meta for Developers'. Below the header, the main heading is 'Create a Meta for Developers account'. On the left side, there is a vertical list of three options: 'Register' (selected with a blue circle), 'Contact info' (unselected), and 'About you' (unselected). The main content area is titled 'Welcome to Meta for Developers' and features a placeholder profile picture. Below the profile picture, there is a paragraph explaining the purpose of the account: 'Create a Meta for Developers account to build and manage apps that access the Graph API, contribute to apps that others own, and participate in Meta's developer community.' Below this paragraph, there is a line of text: 'By proceeding, you agree to the [Meta's Platform Terms and Developer Policies](#)'. At the bottom right of the main content area, there are two buttons: 'Cancel' and 'Continue'.

3. Verify Your Account

Enter your email address for account verification.



The screenshot shows the 'Enter Your Preferred Contact Email' verification page. At the top, there is a dark header with the Meta logo and the text 'Meta for Developers'. Below the header, the main heading is 'Create a Meta for Developers account'. On the left side, there is a vertical list of three options: 'Register' (selected with a green checkmark), 'Contact info' (unselected), and 'About you' (unselected). The main content area is titled 'Enter Your Preferred Contact Email' and features a paragraph explaining the purpose of the email: 'This email will be added to your Facebook account. We use email addresses to send notifications, help you log in and personalize experiences, like connecting people and improving ads for everyone on our products. Only you will see your email on your profile. [Learn More](#)'. Below this paragraph, there is a section titled 'Primary email' with a text input field. Below the input field, there is a checkbox that is checked, with the text: 'I agree to receive marketing-related electronic communications from Facebook, including developer news, updates and promotional emails. (You may unsubscribe from these emails at any time by clicking unsubscribe at the bottom of the email. You can also update your email preferences in Developer Settings.)'. At the bottom right of the main content area, there is a blue button labeled 'Send Verification Email'.

Enter the confirmation code in the email and click **Continue**.

Meta for Developers

Create a Meta for Developers account

Register
 Contact info
 About you

Enter the Code from Your Email
Let us know this email belongs to you. Enter the code in the email sent to [redacted]

[Send Email Again](#)

[Update Email](#) [Continue](#)

4. Select Your Occupation

Meta for Developers

Create a Meta for Developers account

Register
 Contact info
 About you

Which of the following best describes you?
Help us improve your experience by telling us which of the following roles best describe you.

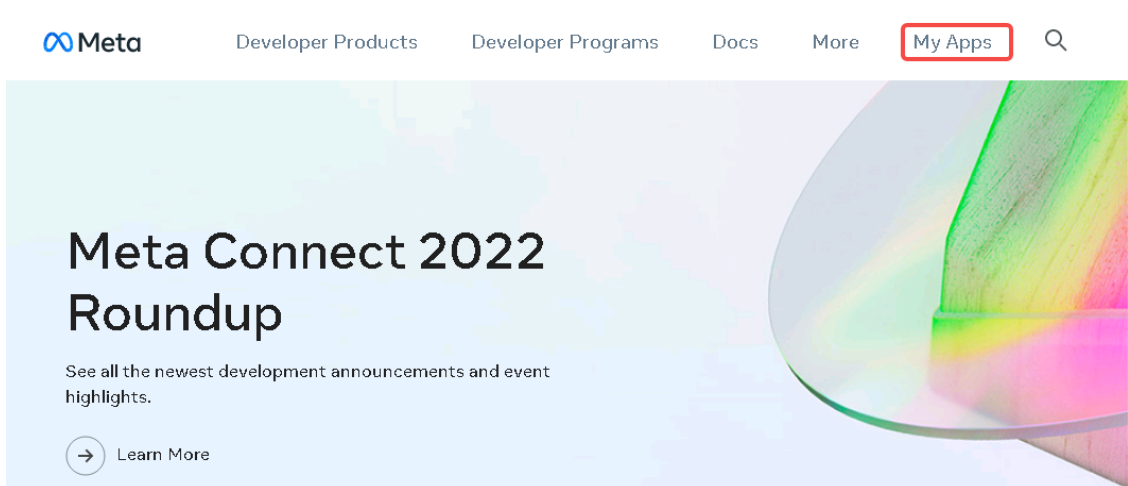
<input checked="" type="radio"/> Developer	<input type="radio"/> Marketer
<input type="radio"/> Analyst	<input type="radio"/> Product manager
<input type="radio"/> Student	<input type="radio"/> Owner/founder
<input type="radio"/> Other	

[Complete Registration](#)

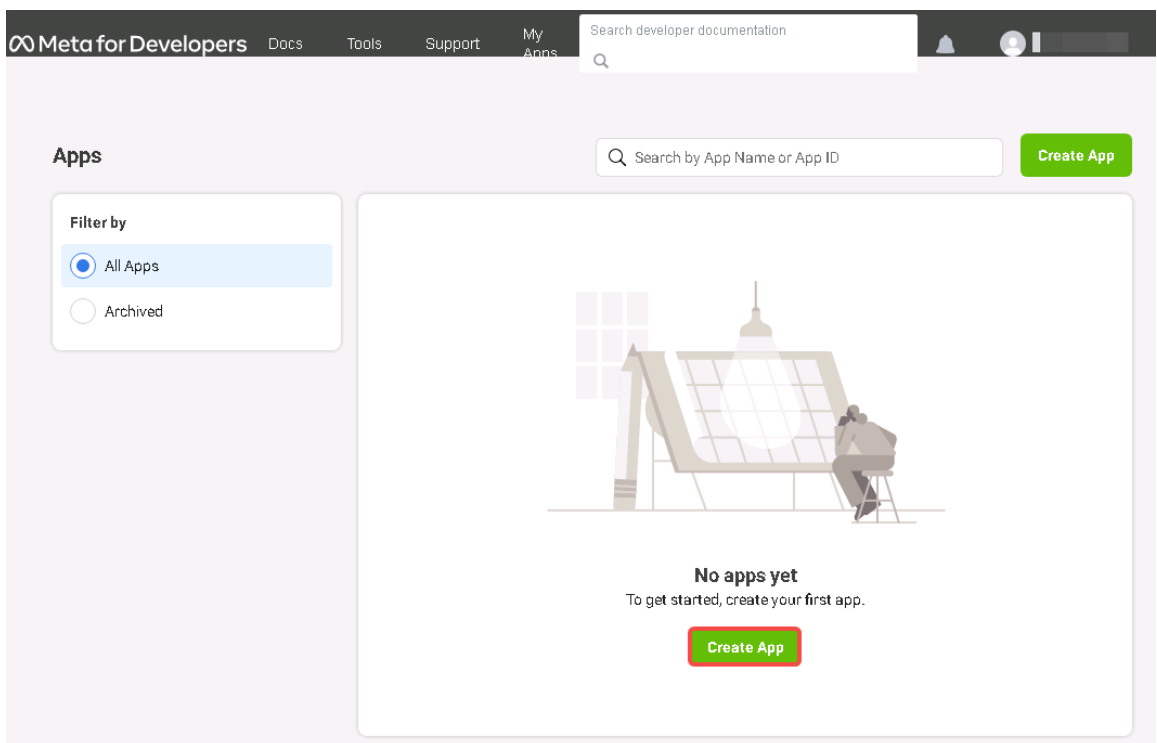
Select an occupation and click **Complete Registration**.

10.1.2 Applying for a Facebook Login App

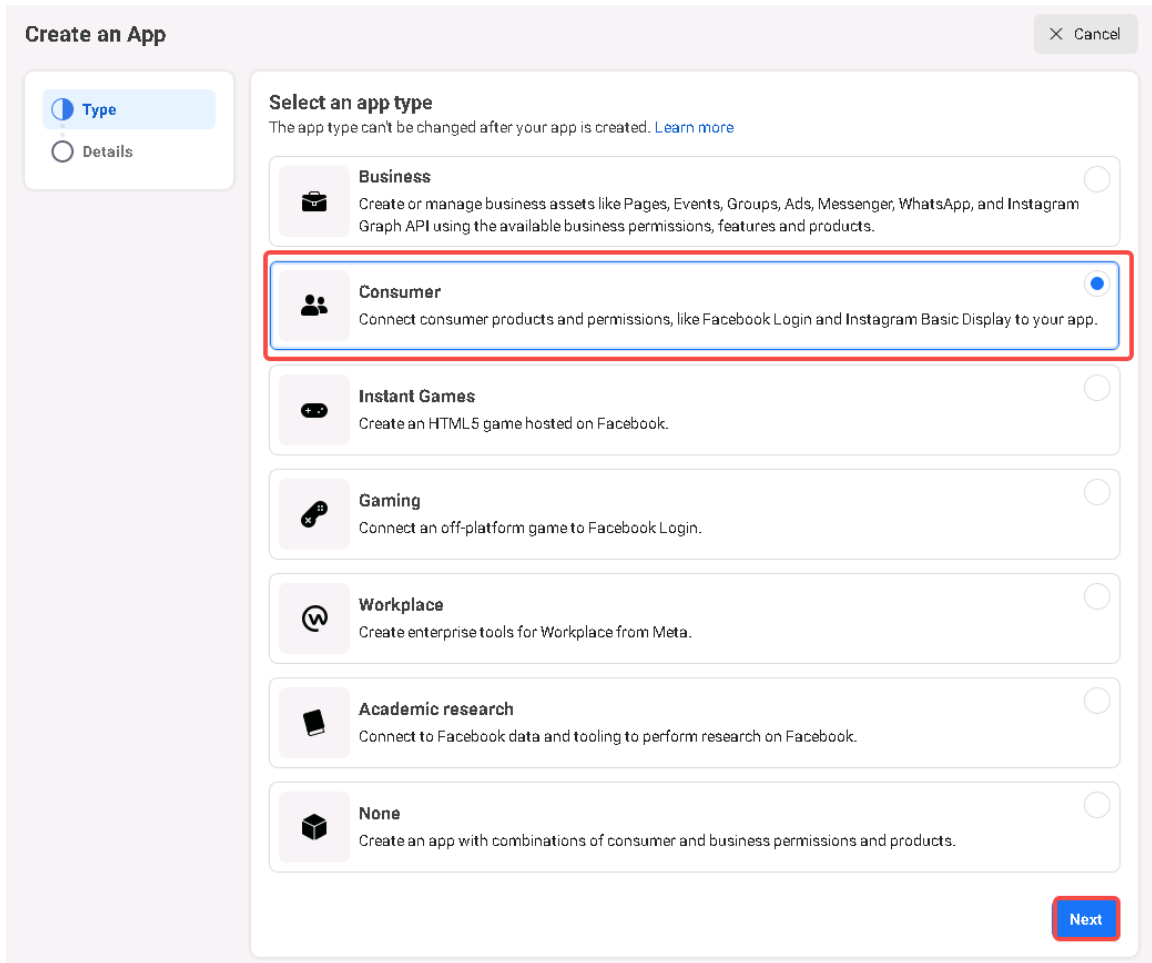
- (1) Enter <https://developers.facebook.com/> in the address bar of a browser. Log in to the Facebook developer center.



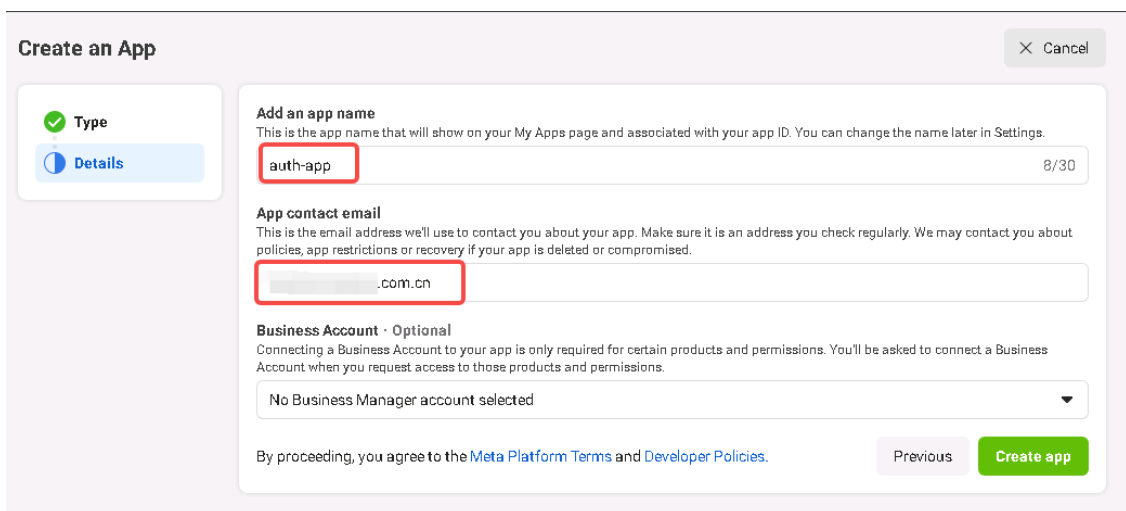
(2) Choose **My Apps**, and click **Create App** to create an App.



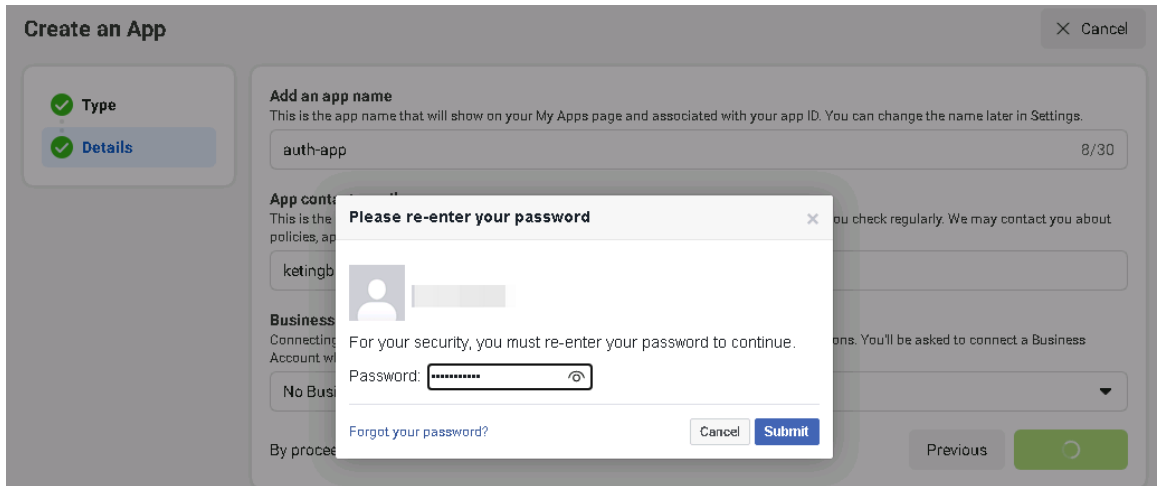
(3) Select **Consumer** on the pop-up page. Click **Next**.



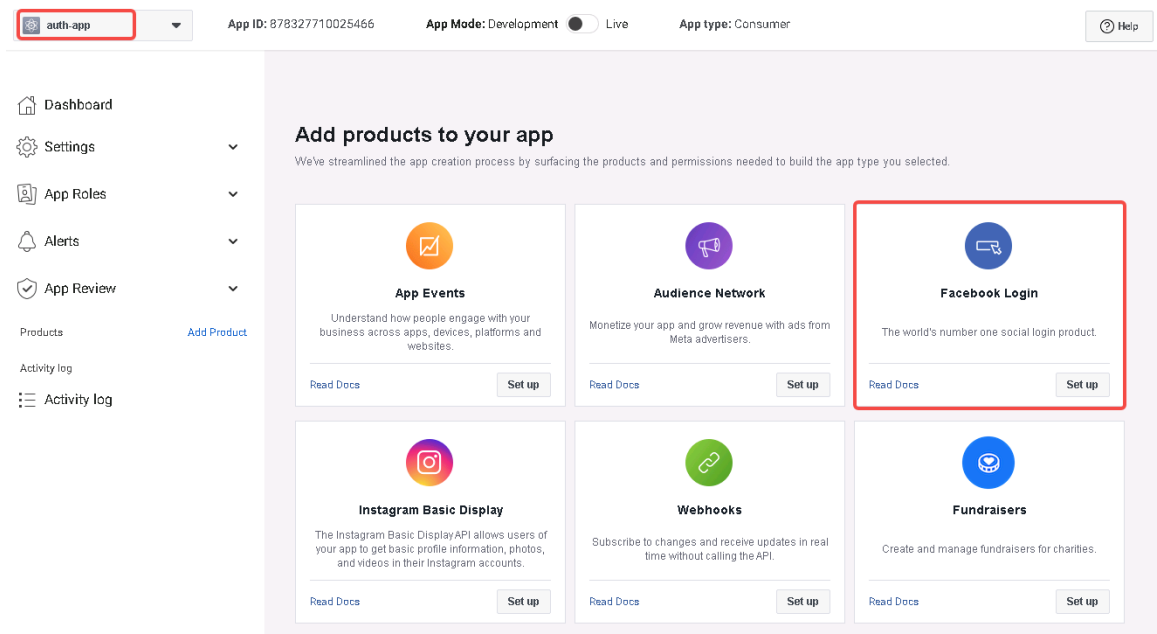
(4) Enter an App name and email address. Click **Create app**.



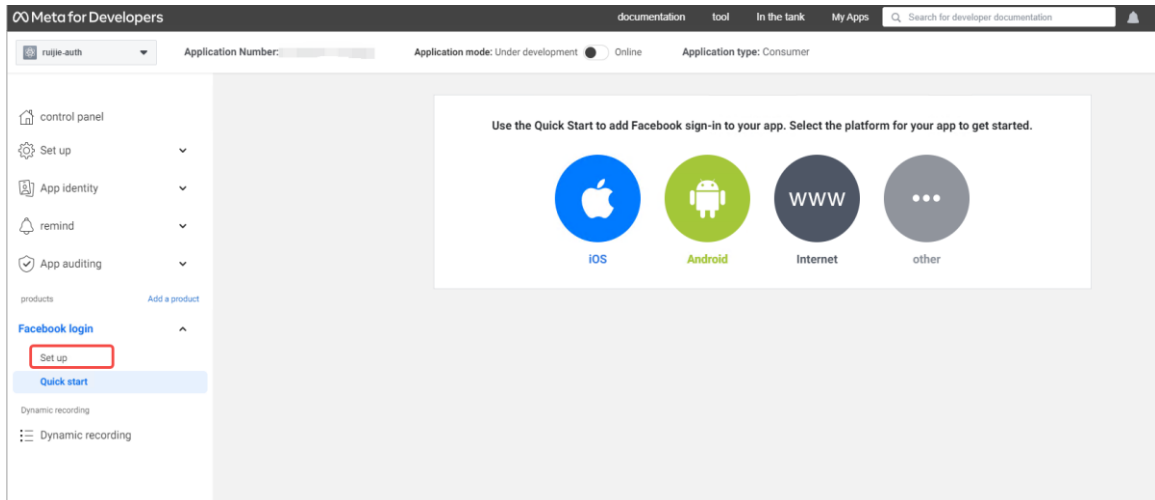
For account security, enter your password again.



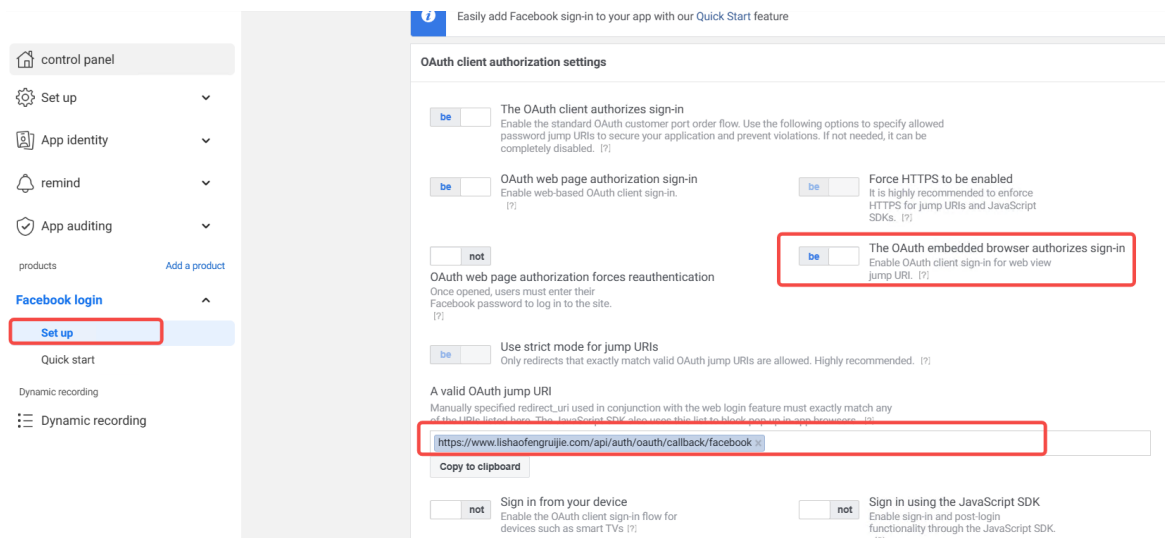
(5) Select **Facebook Login** on the **App Dashboard**. Click **Set up**.



(6) You are redirected to the **Facebook login** page. Click **Set up** under **Facebook login** on the left.



- (7) Enable **The OAuth embedded browser authorizes sign-in**. Configure the callback address of **Facebook Login**.



Caution

In the **A valid OAuth jump URI** item, enter a real domain name <https://www.xxx.com>. The remaining part "/api/auth/oauth/callback/facebook" keeps unchanged.

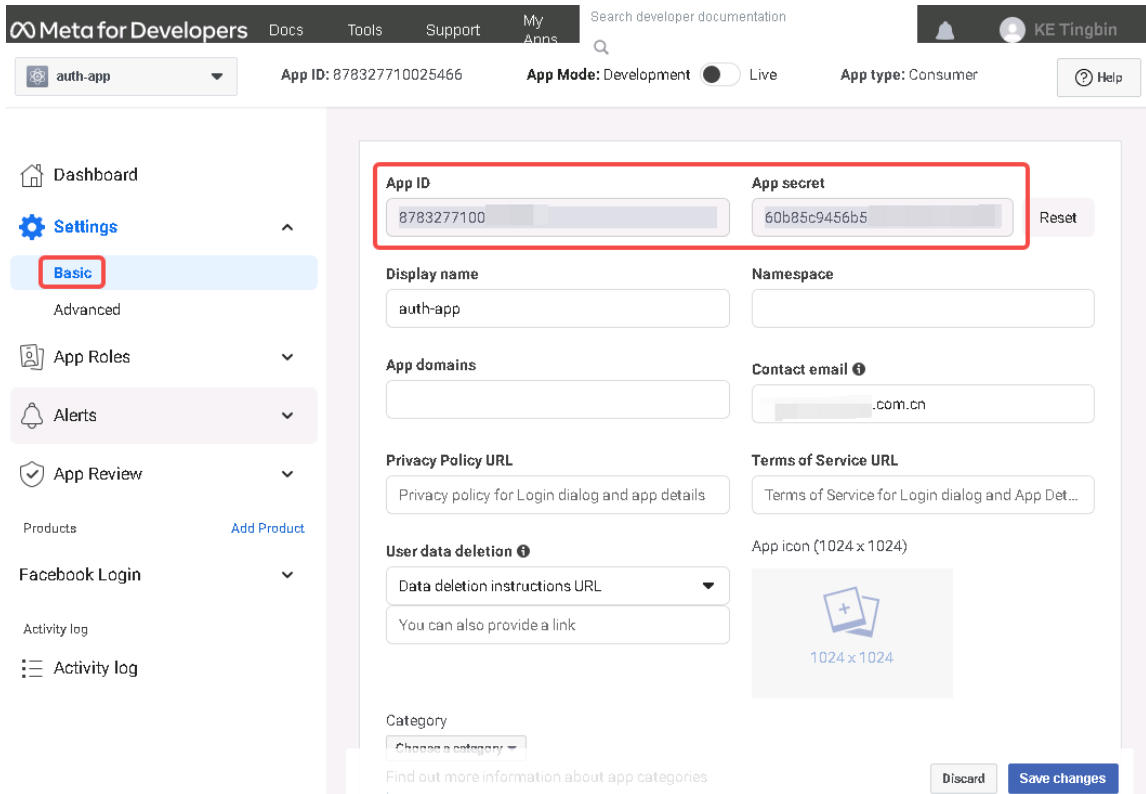
The domain name of WIS public cloud is <https://auth-wiscloud.rujiinetworks.com>.

- (8) Obtain an App ID and set App Secret.

Choose **Settings > Basic**. You can view the App ID and App secret.

Note

WIS field description: The field **Client ID** on the WIS Cloud Network maps to **App ID**, and **Client Secret** maps to **App secret**.



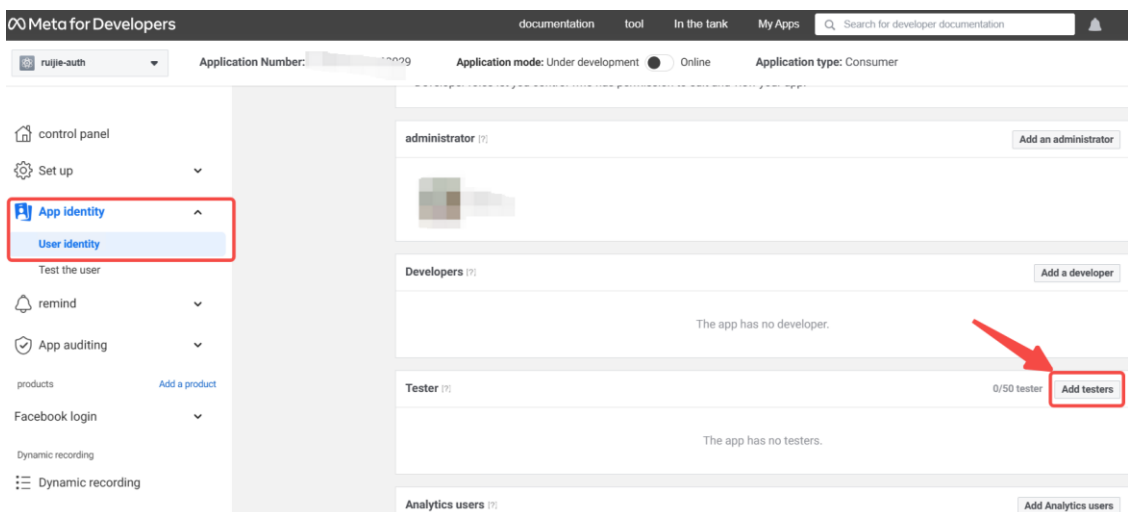
Click **Save changes** to save the configuration.

(9) Add a test account for verification test.

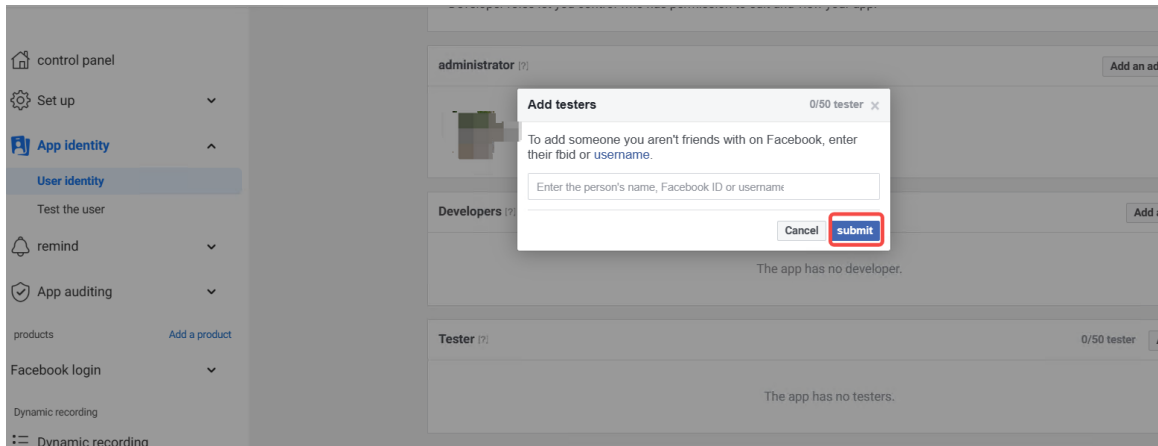
Note

Before the App is released, you need to add a test account for verification test. Other accounts except the test account cannot be used for login.

Choose **App identity > User identity**. Click **Add testers**.



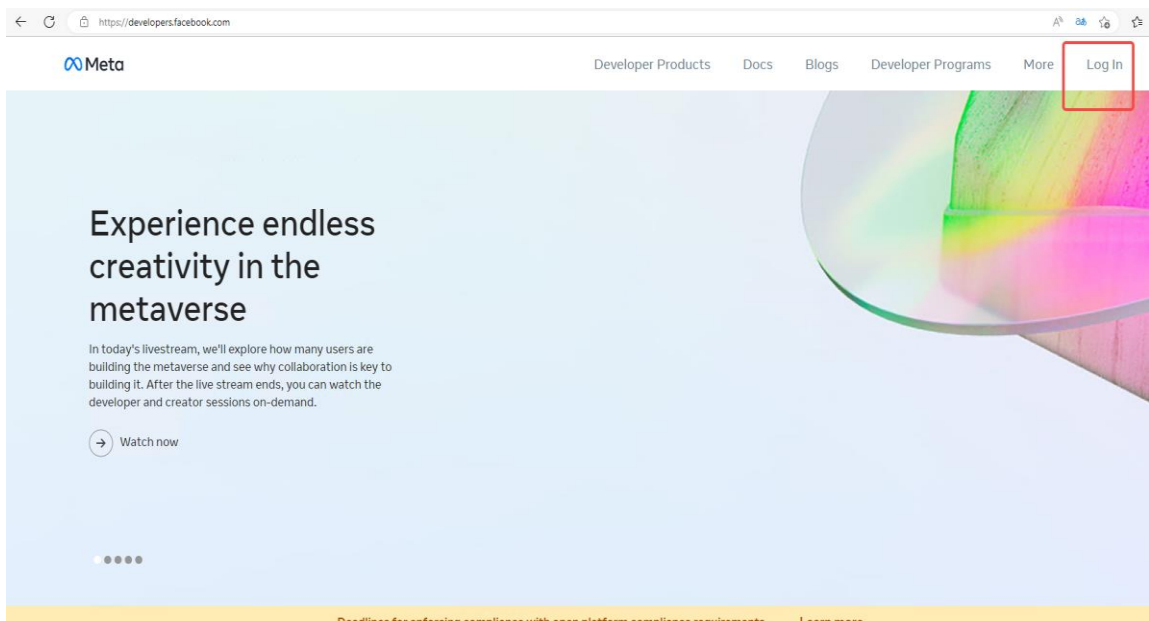
Enter the person's name, Facebook ID or username. Click **submit**.



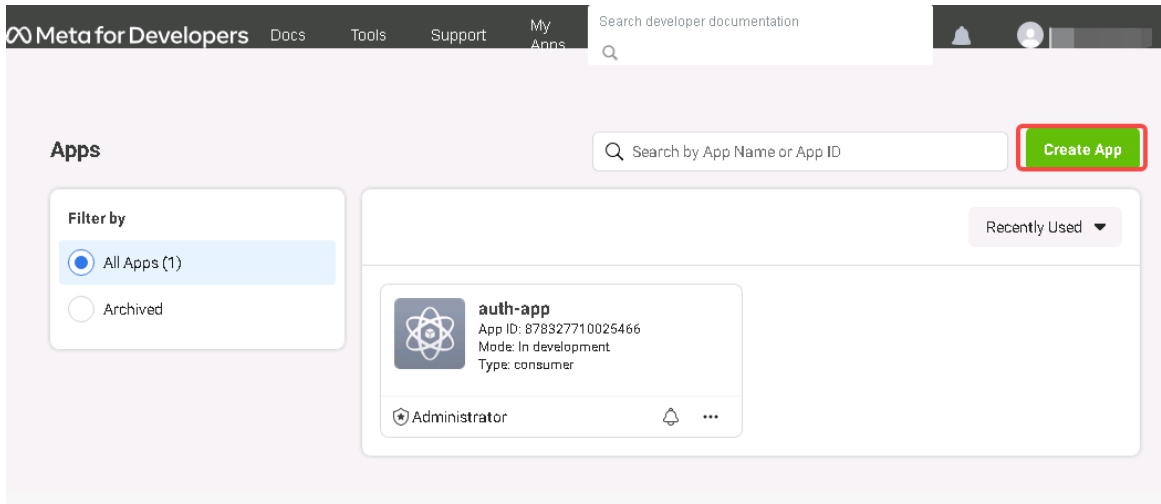
10.1.3 Applying for an Instagram App

1. Create an App

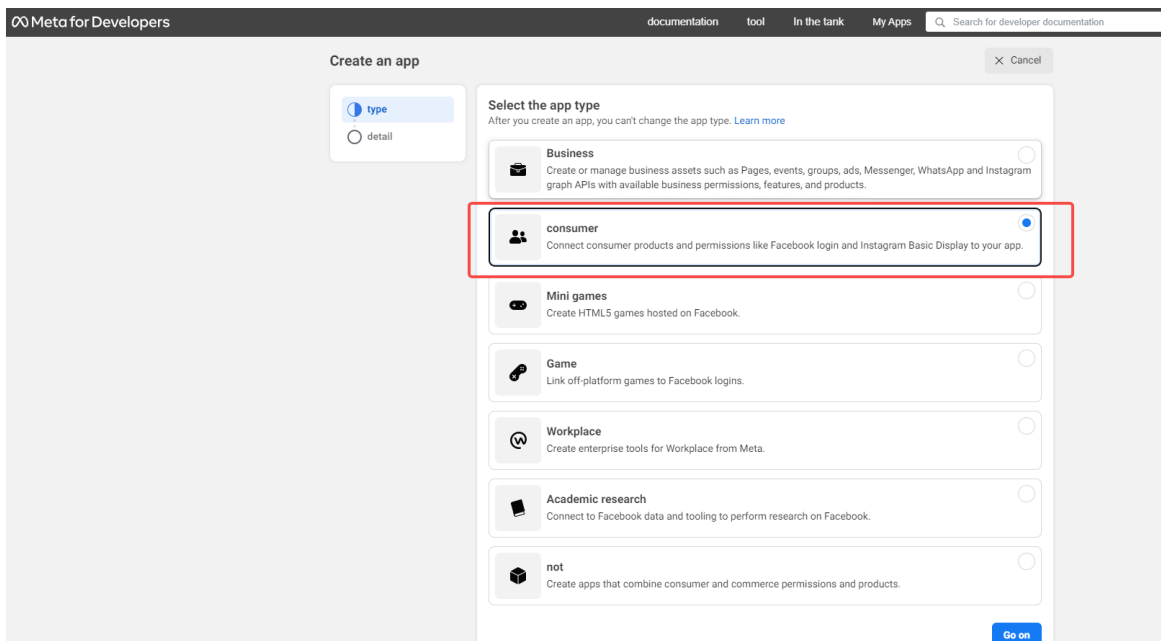
- (1) Enter <https://developers.facebook.com/> in the address bar of a browser. Log in to the Facebook developer center.



- (2) Choose **My Apps**, and click **Create App** to create an App.



(3) Select **consumer** in the pop-up window, and click **Go on**.



(4) Enter an App name and email address according to the instructions. Click **Create app**.

Meta for Developers Docs Tools Support My Apps Search developer documentation

Type **Details**

Add an app name
This is the app name that will show on your My Apps page and associated with your app ID. You can change the name later in Settings.

Ins-Auth 8/30

App contact email
This is the email address we'll use to contact you about your app. Make sure it is an address you check regularly. We may contact you about policies, app restrictions or recovery if your app is deleted or compromised.

.....com.cn

Business Account · Optional
Connecting a Business Account to your app is only required for certain products and permissions. You'll be asked to connect a Business Account when you request access to those products and permissions.

No Business Manager account selected

By proceeding, you agree to the [Meta Platform Terms](#) and [Developer Policies](#). Previous Create app

- (5) After creating an App on the **App Dashboard**, choose **Settings > Basic**. Move down to the bottom of the page, and click **Add platform**.

Meta for Developers Docs Tools Support My Apps Search developer documentation

Ins-Auth App ID: 1020306965612819 App Mode: Development Live App type: Consumer Help

Dashboard Settings Basic Advanced App Roles Alerts App Review Products Add Product Activity log Activity log

Union to designate a Data Protection Officer who people can contact for information about how their data is being processed. This contact information will be available to people on Facebook along with other information about your app or website. [Learn More](#).

Name · Optional Email

Address

Street Address

Apt/Suite/Other · Optional

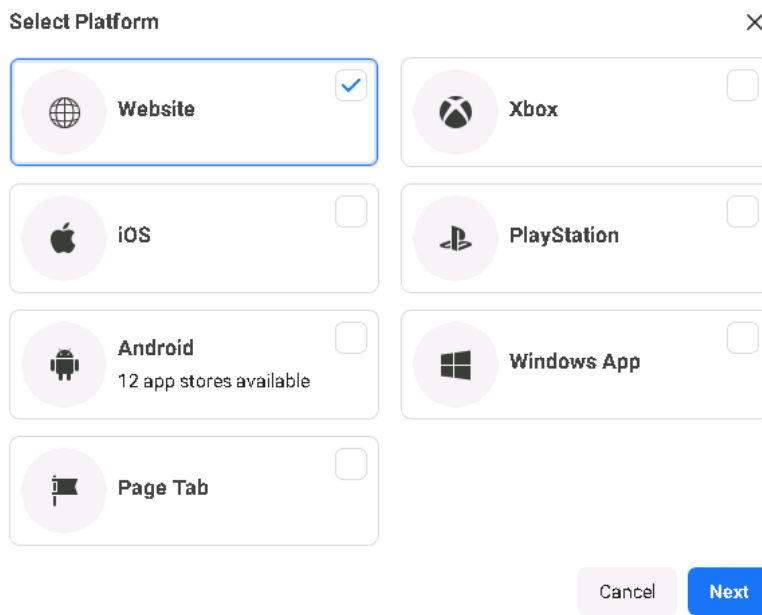
City/District

State/Province/Region ZIP/Pastal Code Country United States

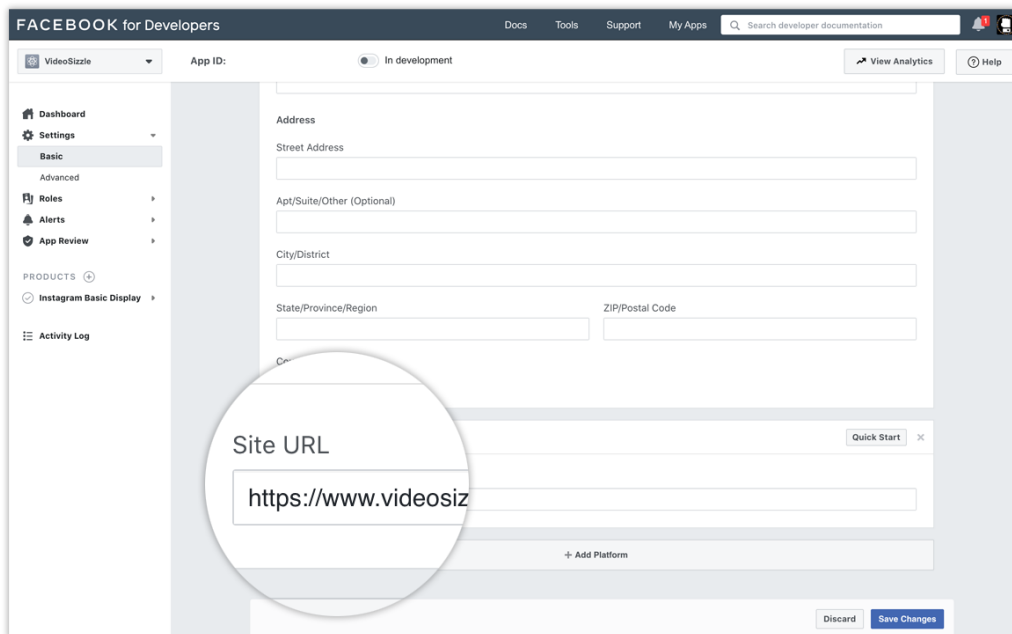
+ Add platform

Discard Save changes

- (6) Select **Website**, and click **Next**.

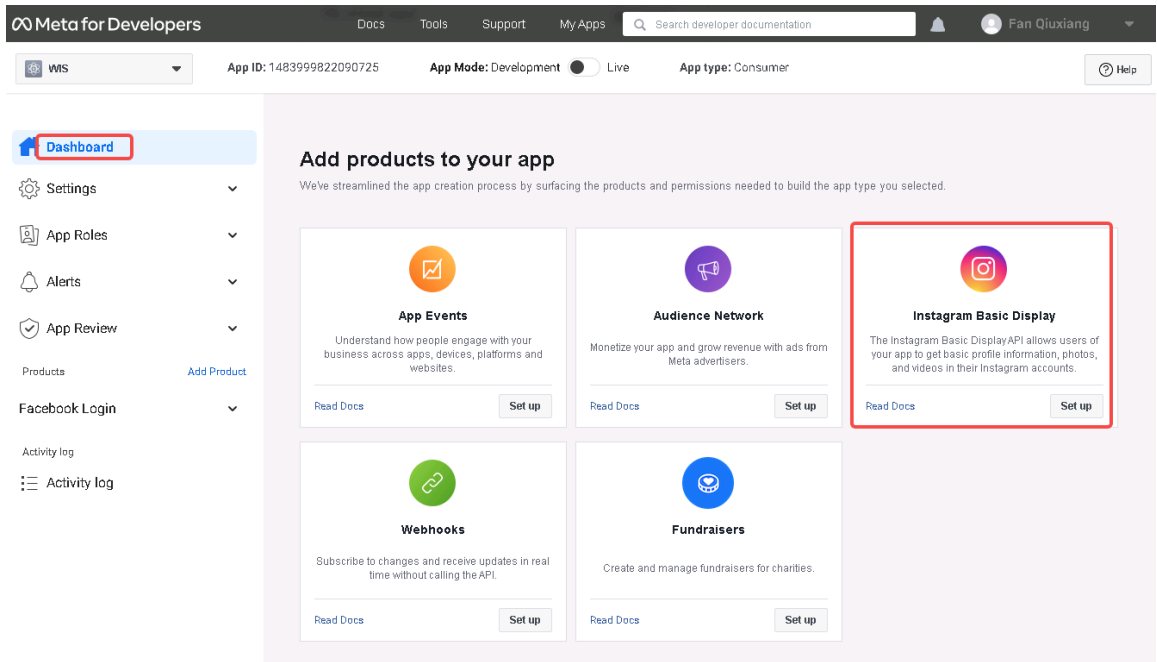


(7) Enter the site URL of WIS public cloud: <https://auth-wiscloud.rujiienetworks.com>. Click **Save Changes**.

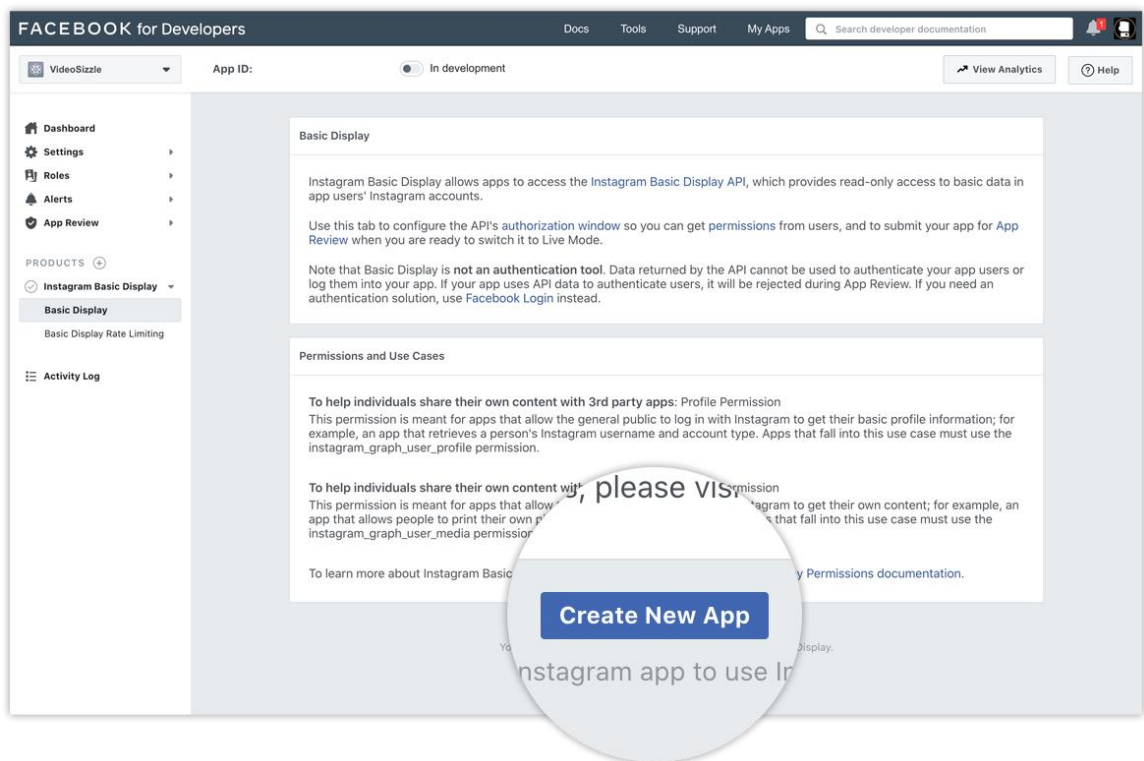


2. Set the Instagram Basic Display

Choose **Dashboard > Instagram Basic Display**. Click **Set up** to add it to your App.



Move down to the bottom of the page. Click **Create New App**.



Enter the name of the created Facebook App in the **Display name** item.

Create a New Instagram App ID

You must create a new Instagram Basic Display specific app. When naming your app, please avoid Instagram branding violations. [Learn more](#).

Display name

By proceeding, you agree to the [Instagram Platform Policies](#)

Click **Create app**. Enter the parameters on the pop-up settings page.

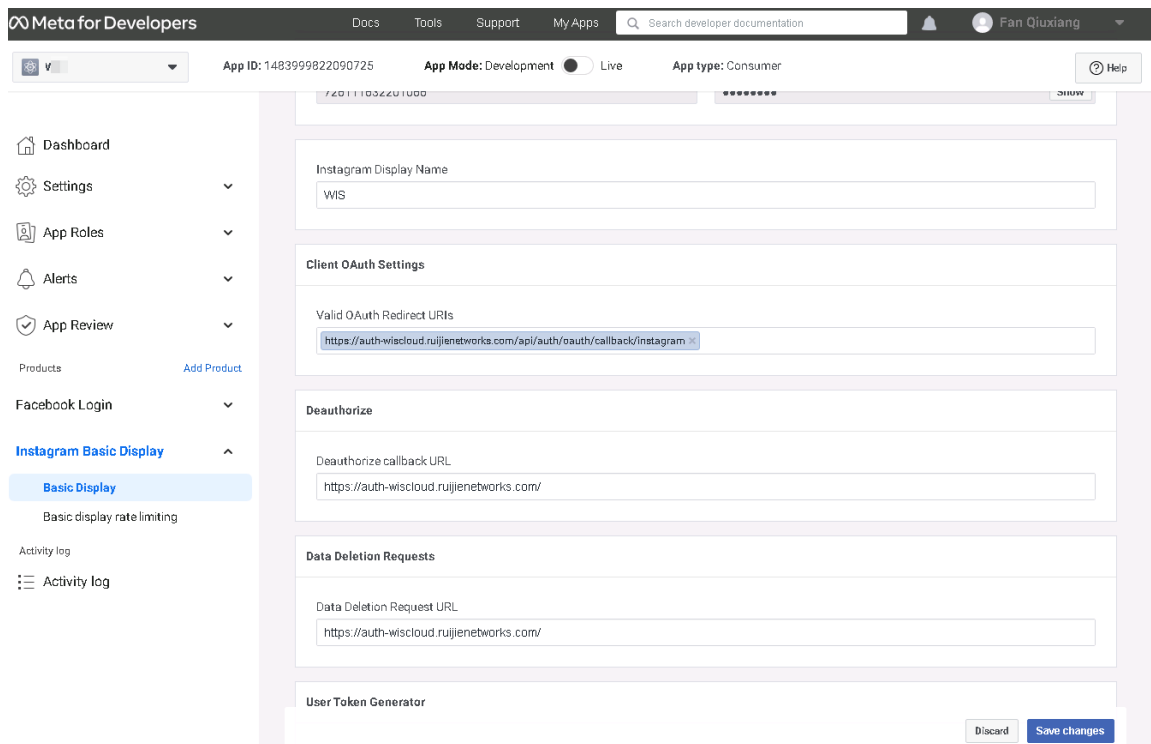


Table 10-1 Parameter Description

Parameter	Description
Valid OAuth Redirect URIs	Indicates a unique URI used to obtain redirection query strings.
Deauthorize callback URL	Indicates a URL used to handle de-authorization notifications.
Data Deletion Request URL	Indicates a URL used to handle data deletion requests.

⚠ Caution

In the **A valid OAuth jump URI** item, enter a real domain name <https://www.xxx.com>. The remaining part `"/api/auth/oauth/callback/instagram"` keeps unchanged.

The domain name of WIS public cloud is <https://auth-wiscloud.rujiienetworks.com>.

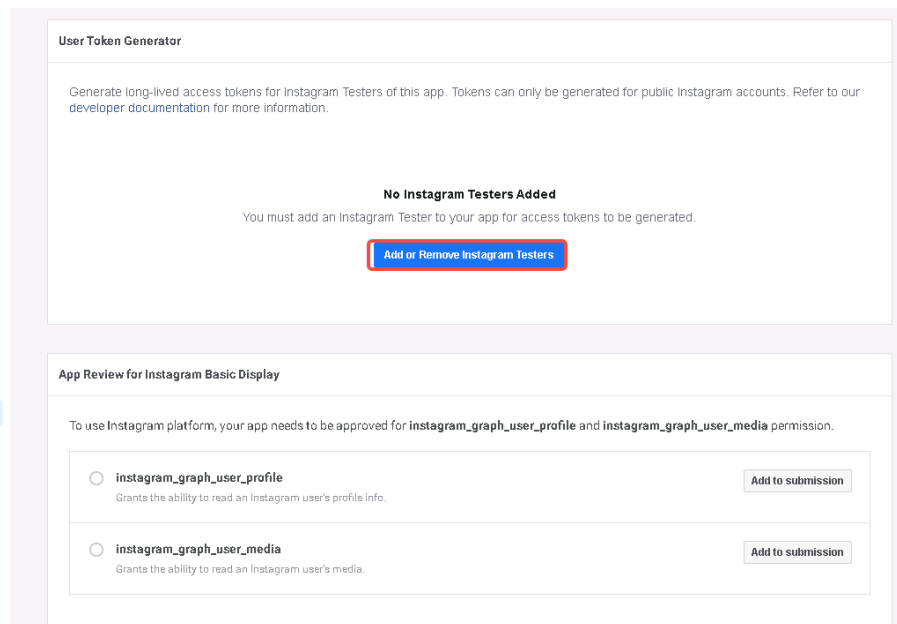
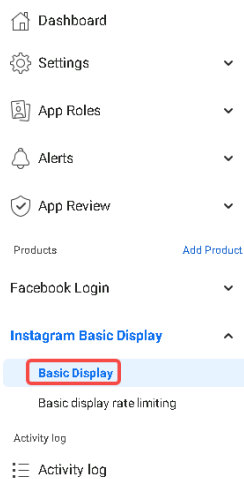
In WIS public cloud environment, enter <https://auth-wiscloud.rujiienetworks.com> for **Deauthorize callback URL** and **Data Deletion Request URL**.

Click **Save changes** to complete the configuration.

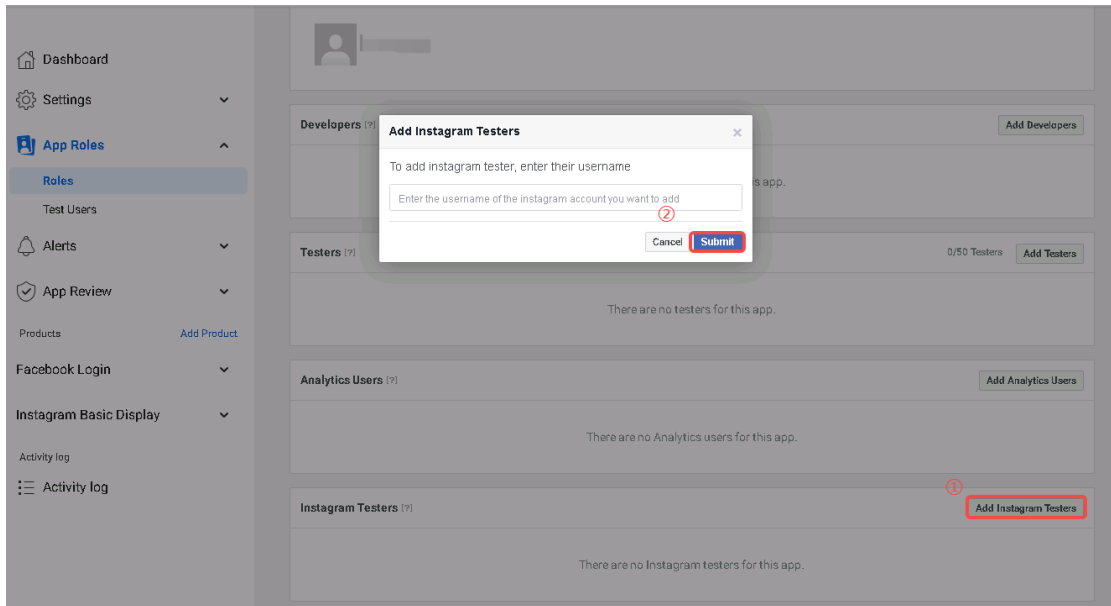
3. Add a test account for verification test**i Note**

Before the App is released, you need to add a test account for verification test. Other accounts except the test account cannot be used for login.

Choose **Instagram Basic Display > Basic Display**. Click **Add or Remove Instagram Testers** on the right.



Click **Add Instagram Testers**. Enter the username of the Instagram account to be added.



Click **Submit** to complete the configuration.

10.1.4 Releasing an App

Once you have completed App development and testing, you can release your App, making your App available to users who do not have a role on the App itself. For the instructions on how to release an App successfully, access <https://developers.facebook.com/docs/development/release> to obtain the official document.