



## Maipu Matrix View

## User Manual

V1.0

## Copyright

Copyright ©2020, Maipu Communication Technology Co., Ltd. All Rights Reserved.

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Maipu Communication Technology Co., Ltd.

**MAIPU** and 迈普 are trademarks of Maipu Communication Technology Co., Ltd.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

The information in this document is subject to change without notice. In no event shall Maipu be liable for any direct, indirect, incidental, special, exemplary, or consequential damages (including, but not limited to, procurement of substitute goods or services; loss of use, data, or profits; or business interruption) however caused and on any theory of liability, whether in contract, strict liability, or tort (including negligence or otherwise) arising in any way out of the use of this manual or the related content on the website, even if advised of the possibility of such damage.

## Security Statement

Important! Before powering on and starting the product, please read the security and compatibility information of the product.

## Environmental protection

This product has been designed to comply with the environmental protection requirements. The storage, use, and disposal of this product must meet the applicable national laws and regulations.

# Preface

---

## Manual Introduction

This manual mainly describes how to use the integrated network management platform of Maipu. This manual tries to put every function of the system in the same chapter, so that when you need to use a certain function, you only need to check the corresponding chapter. For the use of some interleaved functions, if they cannot be put together, this manual will specifically specify.

## Product Version

The corresponding product versions of the manual are as follows:

Product Name	Product Version
Maipu Integrated Service Management System	Maipu Matrix View3.2.0

## Version Description

The revision history accumulates the description of each manual update. The latest version of the manual contains the updates to all previous manual versions.

Version No.	Product Version	Revision Date
V1.0	1.0	2020-07-22

## Audience

This documentation is intended for:

- Software Debugging Engineer
- Field maintenance engineers
- System maintenance engineers

## Conventions

Conventions of screen output format:

Format	Description
--------	-------------

Format	Description
Screen print	Represents the output information of the screen
Keywords of Screen print	The red part represents the key information in the screen output

Symbol conventions:

Format	Description
 <b>Note</b>	An alert that contains additional or supplementary information.
 <b>Caution</b>	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
 <b>Warning</b>	An alert that calls attention to important information that if not understood or followed can result in personal injury or device damage.

Command conventions:

Convention	Description
<b>Boldface</b>	Bold text represents commands and keywords that you enter literally as shown.
<i>Italic</i>	Italic text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x   y   ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[ x   y   ... ]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x   y   ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select

	at least one.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

The icons used in the manual and the meanings:

Icon	Description
	Represents a generic switch
	Represents a generic router

## Technical Support

- Technical supporting hotline: 400-886-8669
- Fax: (+8628)85148948

## Contents

<b>PREFACE</b> .....	<b>I</b>
<b>1. SYSTEM LOGIN</b> .....	<b>1</b>
<b>2. TOPOLOGY MANAGEMENT</b> .....	<b>1</b>
<b>2.1. TOPOLOGY VIEW MANAGEMENT</b> .....	<b>1</b>
2.1.1. ADD TOPOLOGY PHYSICAL VIEW .....	1
2.1.2. ADD TOPOLOGY LOGICAL VIEW .....	2
2.1.3. GENERATE TOPOLOGY PHYSICAL VIEW SYNCHRONOUSLY WHEN ADDING DEVICE GROUP	2
2.1.4. MODIFY/DELETE TOPOLOGY .....	4
<b>2.2. TOPOLOGY VIEW</b> .....	<b>5</b>
2.2.1. FUNCTION BUTTON AREA .....	6
2.2.2. SEARCH AREA .....	12
2.2.3. TOOL BAR .....	12
2.2.4. AERIAL VIEW .....	13
2.2.5. RIGHT-CLICK MENU.....	13
<b>3. RESOURCE MANAGEMENT</b> .....	<b>1</b>
<b>3.1. DEVICE MANAGEMENT</b> .....	<b>1</b>
3.1.1. DEVICE MANAGEMENT.....	1
3.1.2. DEVICE DETAILS .....	18
3.1.2.1. Basic Information .....	19
3.1.2.2. Alarm Information .....	19
3.1.2.3. Interface Information .....	19
3.1.2.4. Route Table.....	21
3.1.2.5. ARP Table .....	21
3.1.2.6. MAC Table .....	22
3.1.2.7. Configuration File.....	22
3.1.2.8. Device Certificate .....	23
3.1.2.9. Device Panel .....	24
<b>3.2. DEVICE TYPE MANAGEMENT</b> .....	<b>37</b>
3.2.1. DEVICE TYPE MANAGEMENT.....	38

3.2.2.	DEVICE MODEL MANAGEMENT .....	40
<b>3.3.</b>	<b>NETWORK DISCOVERY .....</b>	<b>41</b>
3.3.1.	NETWORK DEVICE DISCOVERY .....	41
3.3.2.	STATUS MONITORING CONFIGURATION .....	50
<b>3.4.</b>	<b>CERTIFICATE MANAGEMENT .....</b>	<b>50</b>
3.4.1.	SNMP CERTIFICATE MANAGEMENT .....	50
3.4.2.	TELNET CERTIFICATE MANAGEMENT .....	54
3.4.3.	SSH CERTIFICATE MANAGEMENT .....	56
3.4.4.	SECURITY CERTIFICATE MANAGEMENT .....	58
<b>3.5.</b>	<b>INTERFACE GROUPING .....</b>	<b>61</b>
<b>4.</b>	<b>CONFIGURATION MANAGEMENT .....</b>	<b>1</b>
<b>4.1.</b>	<b>SOFTWARE PACKAGE MANAGEMENT .....</b>	<b>1</b>
4.1.1.	SOFTWARE PACKAGE MANAGEMENT .....	1
4.1.2.	SOFTWARE PACKAGE UPDATE .....	4
<b>4.2.</b>	<b>CONFIGURATION FILE MANAGEMENT .....</b>	<b>13</b>
4.2.1.	CONFIGURATION FILE MANAGEMENT .....	13
4.2.2.	CONFIGURATION CHANGE TASK .....	19
<b>4.3.</b>	<b>CONFIGURATION COMMAND DELIVERING .....</b>	<b>31</b>
4.3.1.	COMMAND TEMPLATE MANAGEMENT .....	31
4.3.2.	COMMAND DELIVERY TASK .....	34
4.3.3.	SECURITY POLICY TEMPLATE MANAGEMENT .....	43
<b>4.4.</b>	<b>POLICY OBJECT MANAGEMENT .....</b>	<b>48</b>
4.4.1.	APPLICATION OBJECT .....	48
4.4.2.	URL OBJECTS .....	49
4.4.3.	SERVICE OBJECT .....	50
<b>5.</b>	<b>PERFORMANCE MANAGEMENT .....</b>	<b>51</b>
<b>5.1.</b>	<b>MONITORING TASK .....</b>	<b>51</b>
5.1.1.	SYSTEM MONITORING .....	52
5.1.2.	INTERFACE MONITORING .....	57
5.1.3.	MONITORING TASK OPERATION .....	62

<b>5.2. MONITORING DATA</b> .....	<b>64</b>
5.2.1. SYSTEM MONITORING DATA .....	65
5.2.2. INTERFACE MONITORING DATA .....	70
<b>5.3. CUSTOMIZE MONITORING INDEX</b> .....	<b>74</b>
<b>5.4. LINK DETECTION</b> .....	<b>79</b>
5.4.1. LINK DETECTION CONFIGURATION .....	79
5.4.2. LINK DETECTION .....	80
<b>6. ALARM MANAGEMENT</b> .....	<b>89</b>
<b>6.1. ALARM INFORMATION</b> .....	<b>89</b>
<b>6.2. ALARM CONFIGURATION</b> .....	<b>96</b>
6.2.1. ALARM NOTIFICATION RULE .....	96
6.2.2. NOTIFICATION CONTENT TEMPLATE .....	102
6.2.3. ALARM SHIELDING RULE .....	105
6.2.4. ALARM AUTO PROCESSING RULE .....	110
6.2.5. ALARM LEVEL REDEFINITION .....	110
6.2.6. ALARM BASIC CONFIGURATION .....	113
6.2.7. ALARM DUMP .....	116
6.2.8. ALARM TYPE MANAGEMENT .....	117
6.2.9. MAINTENANCE EXPERIENCE MANAGEMENT .....	120
<b>6.3. SYSLOG LOG</b> .....	<b>121</b>
<b>6.4. UNRECOGNIZED TRAP</b> .....	<b>122</b>
<b>7. REPORTS</b> .....	<b>1</b>
<b>7.1. REPORT TASK MANAGEMENT</b> .....	<b>1</b>
<b>7.2. REPORT FILE MANAGEMENT</b> .....	<b>5</b>
<b>7.3. REPORT CLEANUP POLICY CONFIGURATION</b> .....	<b>7</b>
<b>8. SYSTEM MANAGEMENT</b> .....	<b>9</b>
<b>8.1. ORGANIZATION MANAGEMENT</b> .....	<b>9</b>
<b>8.2. OPERATION LOGS</b> .....	<b>11</b>
<b>8.3. USER AND AUTHORITY MANAGEMENT</b> .....	<b>12</b>
8.3.1. ROLE MANAGEMENT .....	12

8.3.2. USER AND AUTHORITY .....	14
<b>8.4. SYSTEM SETTING .....</b>	<b>16</b>
8.4.1. LICENSE .....	17
8.4.2. PASSWORD POLICY CONFIGURATION .....	17
8.4.3. SMS GATEWAY CONFIGURATION .....	18
8.4.4. EMAIL SERVICE CONFIGURATION .....	21
8.4.5. WECHAT CONFIGURATION .....	22
9.4.5.1 Wechat Public Number Management .....	22
9.4.5.2 Bind System User .....	24
8.4.6. SUPERIOR NMS MANAGEMENT .....	25
8.4.7. USER INFORMATION .....	25
<b>8.5. SYSTEM LOG MANAGEMENT .....</b>	<b>26</b>
8.5.1. SYSTEM LOG CONFIGURATION .....	26
8.5.2. LOG NOTIFY CONFIGURATION .....	27
8.5.3. SYSTEM LOG .....	29
<b>9. DATA VISUALIZATION .....</b>	<b>31</b>
<b>9.1. HOME .....</b>	<b>31</b>
<b>9.2. BIG SCREEN .....</b>	<b>36</b>
<b>9.3. COMPONENTS .....</b>	<b>42</b>
9.3.1. BASIC NETWORK .....	42
9.3.1.1. Concerned Interface Rate Monitoring .....	42
9.3.1.2. Rate Statistics of Concerned Interface .....	46
9.3.1.3. Bandwidth Utilization Statistics of Concerned Interface .....	49
9.3.1.4. Bandwidth Utilization Monitoring of Concerned Interface .....	51
9.3.1.5. Interface Rate TOP N .....	53
9.3.1.6. Interface Bandwidth Utilization TOP N .....	55
9.3.1.7. Interface Lost Packets TOP N .....	57
9.3.1.8. Single Interface Rate Monitoring .....	58
9.3.1.9. Interface Integrated Monitoring TOP N .....	60
9.3.1.10. Device Response Time TOP N .....	62

---

9.3.1.11.	Concerned Device Health	64
9.3.1.12.	Device Status Statistics	65
9.3.1.13.	Availability Monitoring of Concerned Device	66
9.3.1.14.	Device Availability Comprehensive Monitoring TOP N	68
9.3.1.15.	Real-time Statistics of Link Status	70
9.3.1.16.	Delay Packet Loss Monitoring of Concerned Link	71
9.3.1.17.	Delay Statistics of Concerned Link	72
9.3.1.18.	Topology View	74
9.3.1.19.	Alarm Statistics of Concerned Device	75
9.3.1.20.	Alarm Device TOP N	77
9.3.1.21.	Alarm Level Statistics	80
9.3.1.22.	Alarm Type TOP N	83
9.3.1.23.	Alarm Radar	85
9.3.1.24.	Recent Alarm List	86
9.3.2.	OTHERS	88
9.3.2.1.	Big Screen External Component	88
9.3.2.2.	Welcome	89
9.3.2.3.	Pictures	91
9.3.2.4.	Time	92

# 1. System Login

Open the browser, access the IP address of the server where the Maipu integrated service management system is located (for example: <https://IP:443>), and enter the system login interface. When accessing the system for the first time, because the HTTPS signing certificate used by the system is automatically generated by the system according to the current server configuration, the browser may prompt that the certificate is not safe (as shown in Figure 1-1 and Figure 1-2) before entering the system, and directly ignore the relevant prompt. If you need to solve this problem, you can apply to the authority certification authority for the certificate, and replace the certificate generated by the system with the applied certificate. At this time, you can enter the login interface, as shown in Figure 1.3. At the same time, because some functions in the system need the browser to support HTML5 and other features, it is recommended to use Google Chrome v59 and IE10 or above to achieve the best experience effect. The system is attached with the installation files of two browser versions ie10 and chrome 59. Users can click the corresponding icon in the login interface to download and use.

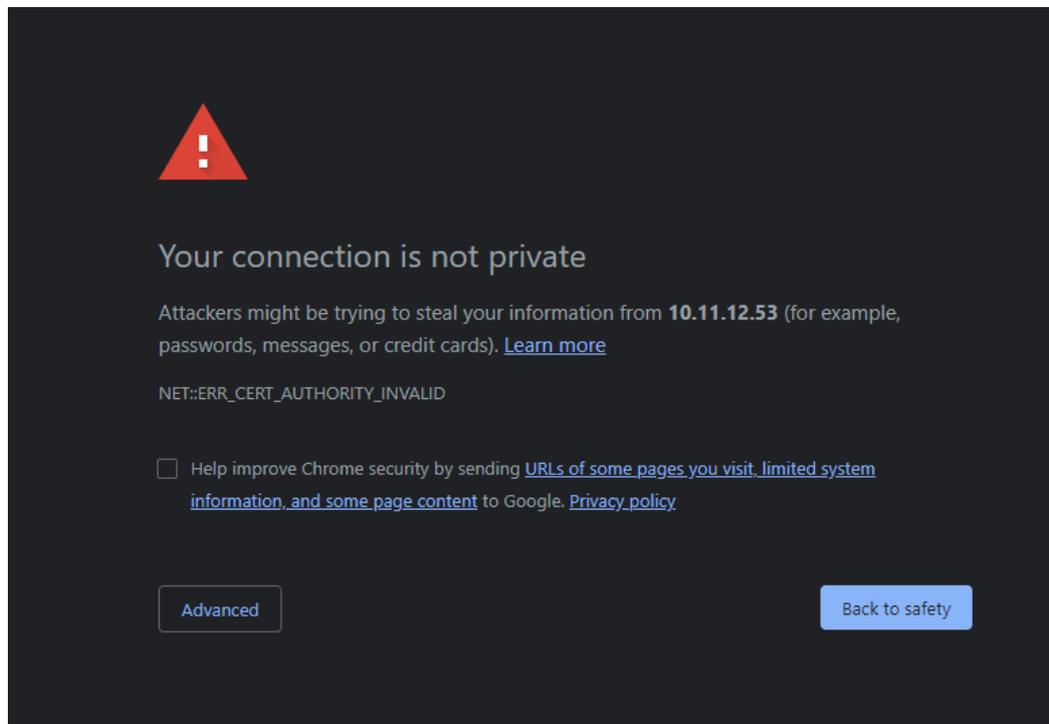


Figure 1-1 chrome warning

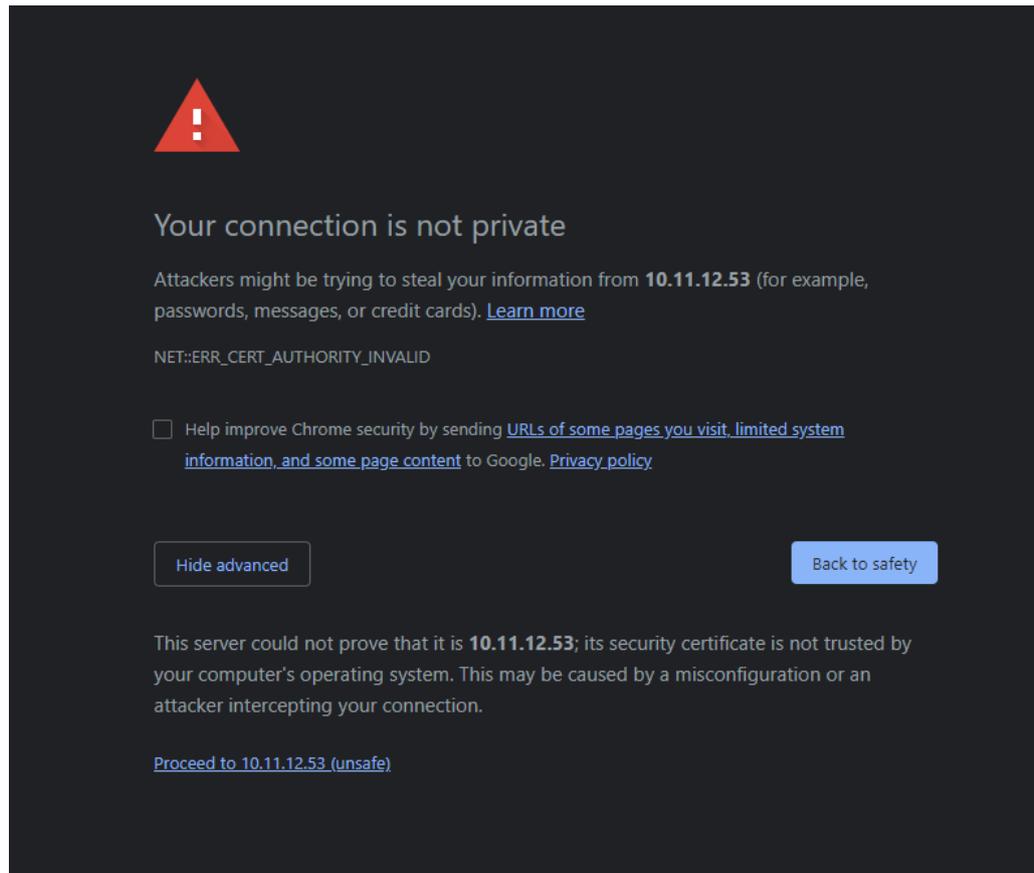


Figure 1-2 ie warning

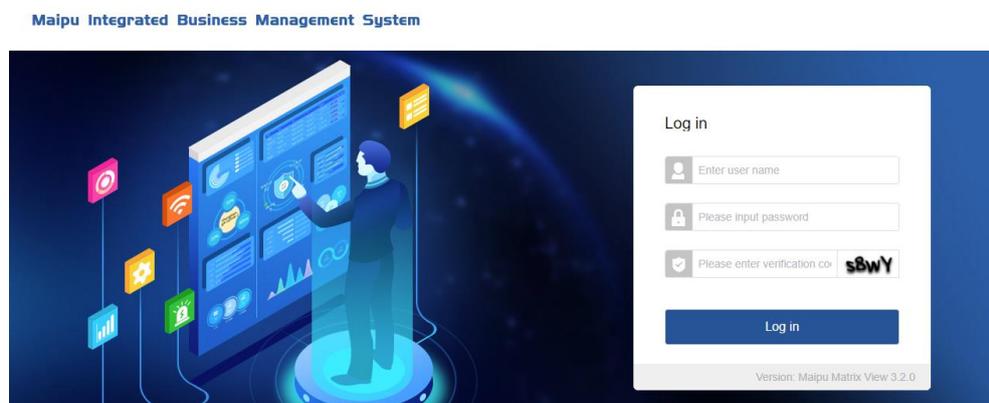


Figure 1-3 Login interface

For the newly installed system, after entering the login interface, enter the default user name and password (both are admin) and the correct verification code, the system will require the user to modify the initial login password, as shown in Figure 1-4. After you change the password correctly according to the system prompt, you will enter the login interface again and enter a new password to enter the system successfully.

Account

Old password

New password  ⓘ

Confirm password

Phone number

Email

Figure 1-4 Modify initial password

Some functions of the system need to import the license before use. The newly installed system does not provide any license, so there will be the prompt information as shown in Figure 1-5 when logging into the system. In order to use all functions of the system normally, please purchase and import the license in time.

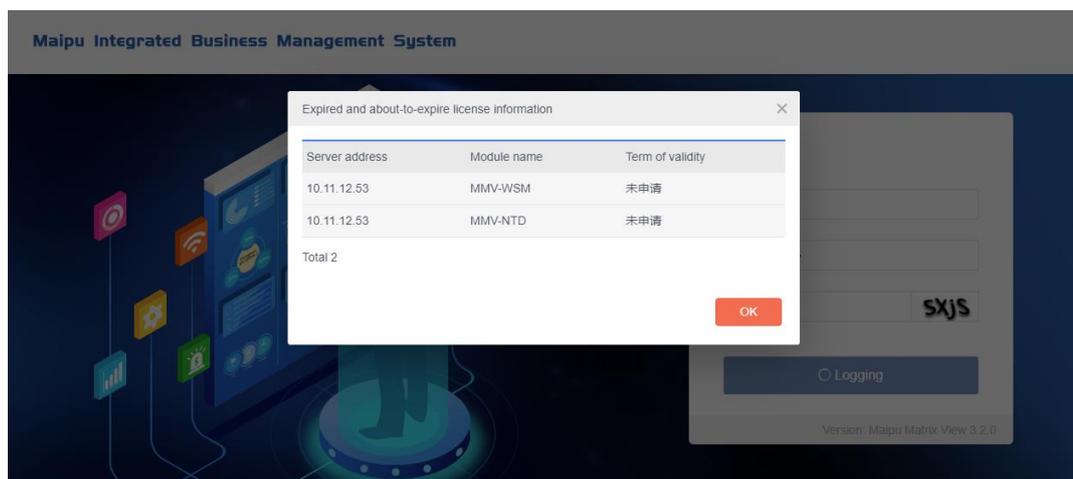


Figure 1-5 license prompt information

## Note

- The default port number is 433.
- The system recommends that the resolution width of the display is 1440, and some pages may have display problems in other resolutions.
- The default password rule is: the password must be at least 6 characters long and contain uppercase letters, lowercase letters, numbers and special characters (~! @ \$% ^ & \* # ()\_ +- = {} [] | "< > /), and cannot contain the user name.

## 2. Topology Management

### 2.1. Topology View Management

#### 2.1.1. Add Topology Physical View

Click "**Topology**" in the top menu bar to open the topology management interface, click **+** in the upper left corner, select "Physical View" in the pop-up "Add" page, and complete the inputting of other items, as shown in Figure 2-1; click "**OK**" to generate the topology physical view, as shown in Figure 2-2;

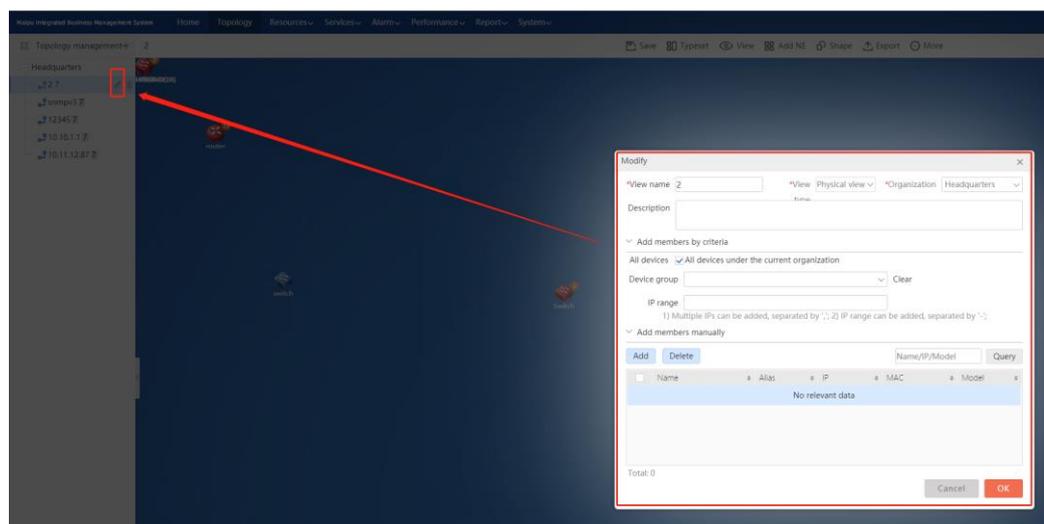


Figure 2-1 Add topology physical view

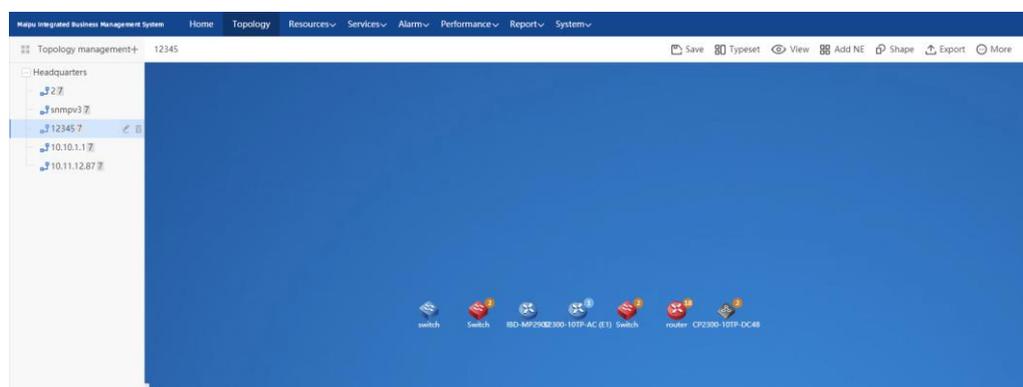


Figure 2-2 Generated topology physical view

### 2.1.2. Add Topology Logical View

Click **"Topology"** in the top menu bar to open the topology management interface, click **+** in the upper left corner, select **"Logical View"** in the pop-up **"Add"** page, and complete the inputting of other items, as shown in Figure 2-3; click **"OK"** to generate the topology logical view, as shown in the following figure;

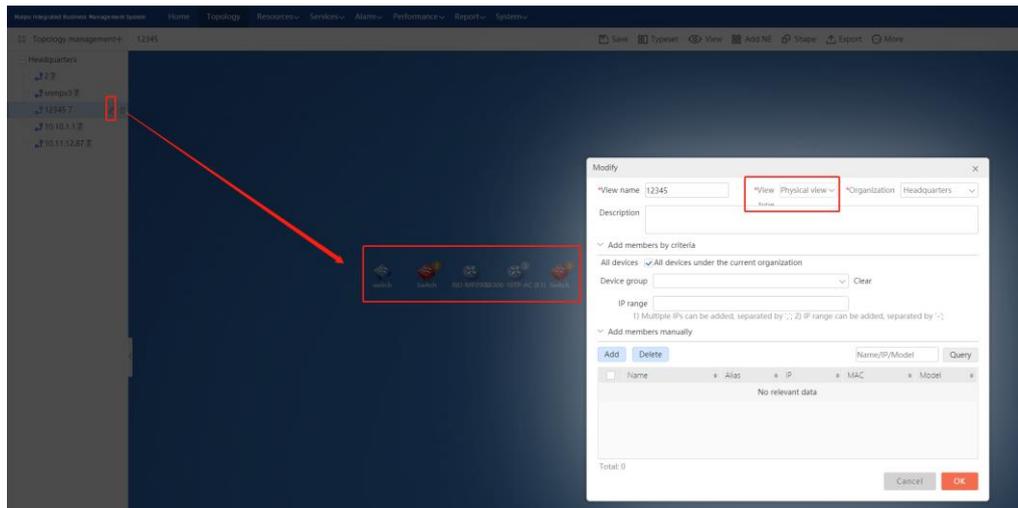


Figure 2-3 Add topology logical view

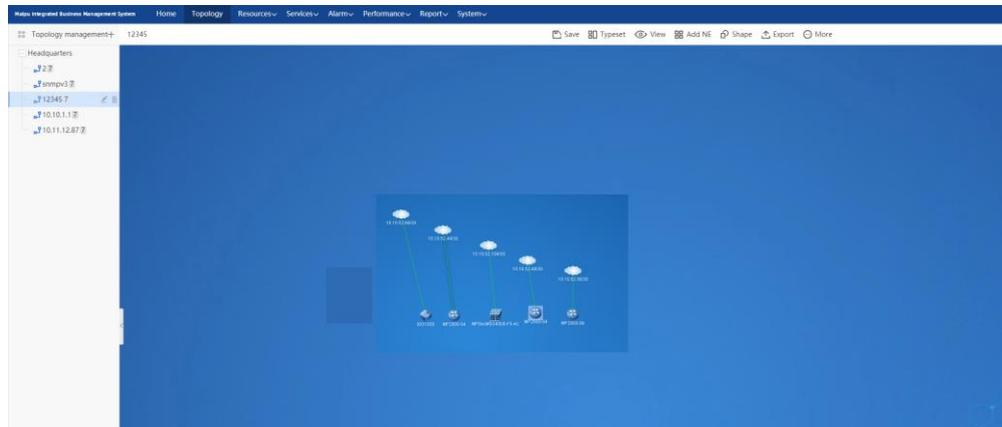


Figure 2-4 Generated topology logical view

### 2.1.3. Generate Topology Physical View Synchronously When Adding Device Group

Click **"Resources"** - > **"Device Management"** in the top menu bar to open the device management interface;

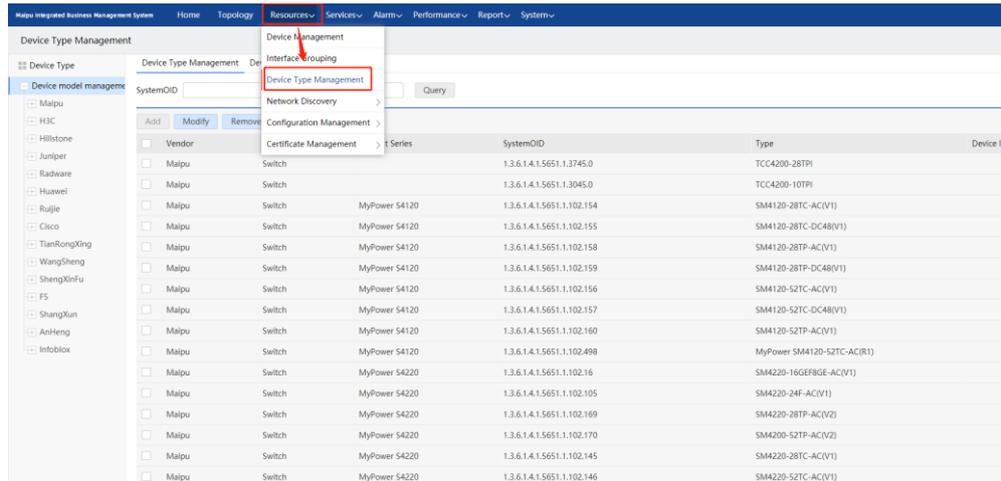


Figure 2-5 Device management

Click **+** in the upper left corner to open the interface of adding device group, check “Generate topology synchronously” in this page, edit the device group, and click **Save**. When the device group is saved successfully, the topology will be generated synchronously, as shown in the following figure.

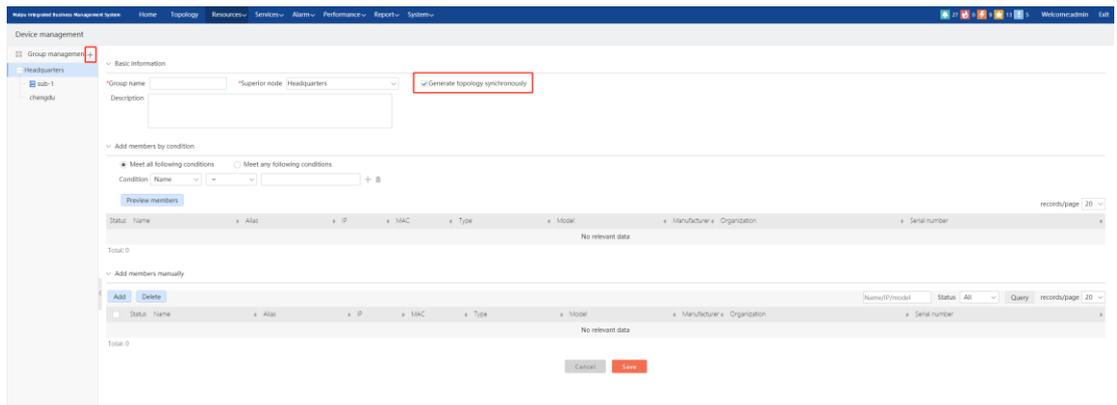


Figure 2-6 Add device group

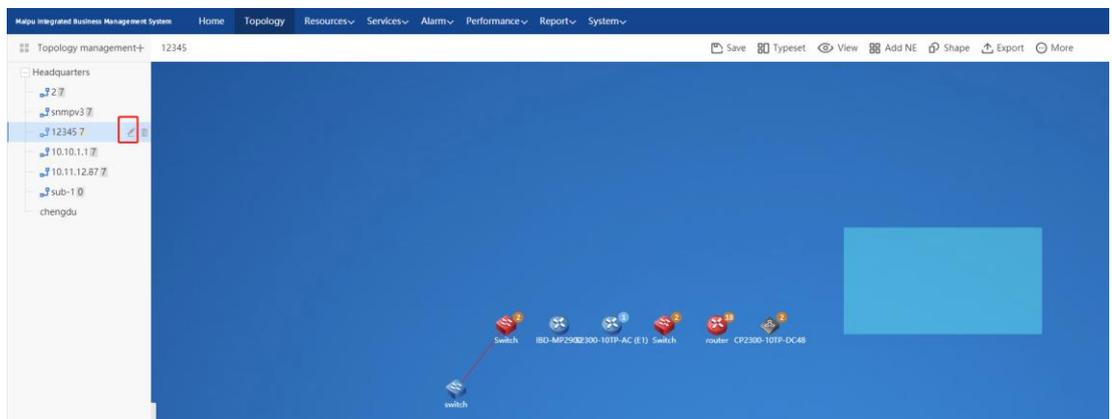


Figure 2-7 Synchronously generated topology physical view

### 2.1.4. Modify/Delete Topology

Click "**Topology**" on the top menu bar to open the topology interface, find the topology to be edited on the left tree, click , edit the basic topology information and member in the pop-up "**Modify**" interface, and click "**OK**" to complete the topology modification, as shown in the following figure.

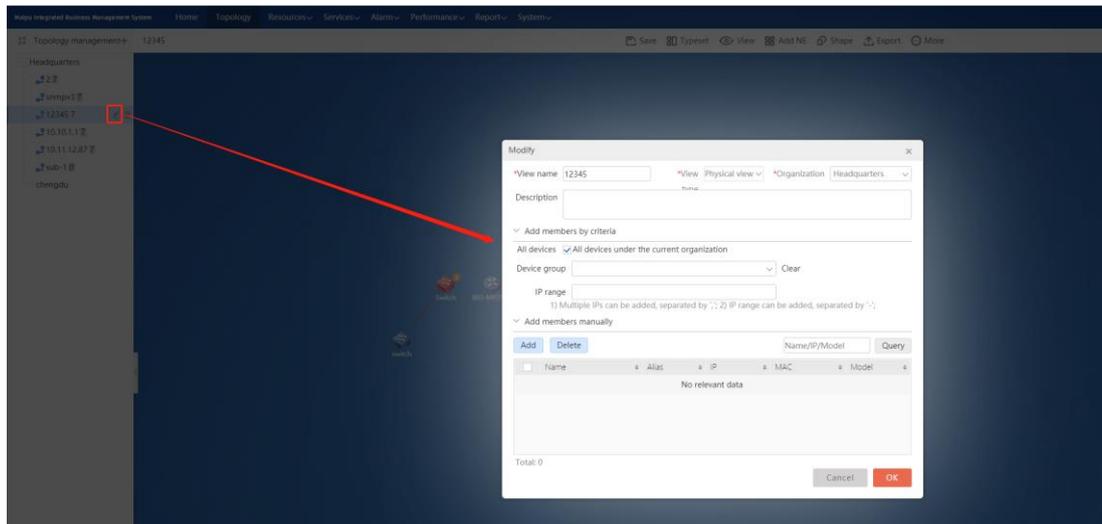


Figure 2-8 Modify the topology

Click "Topology" on the top menu bar to open the topology interface, find the topology to be deleted on the left tree, and click  to delete the topology.

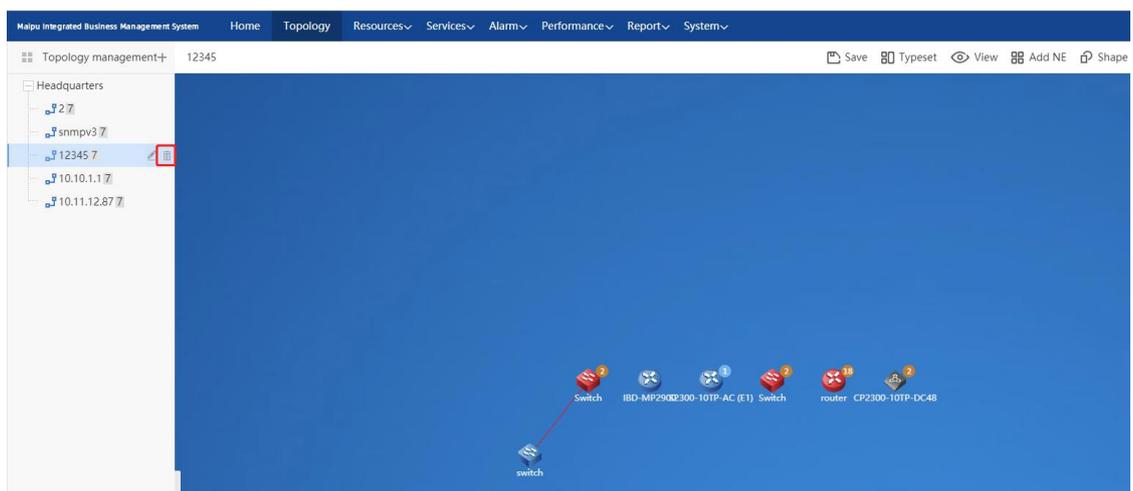


Figure 2-9 Delete the topology

#### Note

- For the concept of device group, please refer to Chapter 3 Resource Management.

- The tree on the left side of the topology management page is a hybrid tree of organization + topology, showing all organizations and the topologies attached to the organization. There is no default topology for the organization, so you can add topology to the organization.
- Once the topology view is added successfully, "View Type" and "Organization" can no longer be modified. If you need to modify, please delete the existing topology view before adding a new one.
- When adding/modifying the topology view, you can add device members by conditions or manually. Both methods can take effect at the same time.

## 2.2. Topology View

The topology view page shows the topology map of a specific topology view and provides the editing and viewing for the topology.

You can enter this page by clicking the "**Topology**" in the top menu bar, or you can enter this page by clicking  in the "**Device List**" and "**Alarm List**"; clicking the menu and the system will load the recently accessed topology of the login user; the effect is shown in the following figure.

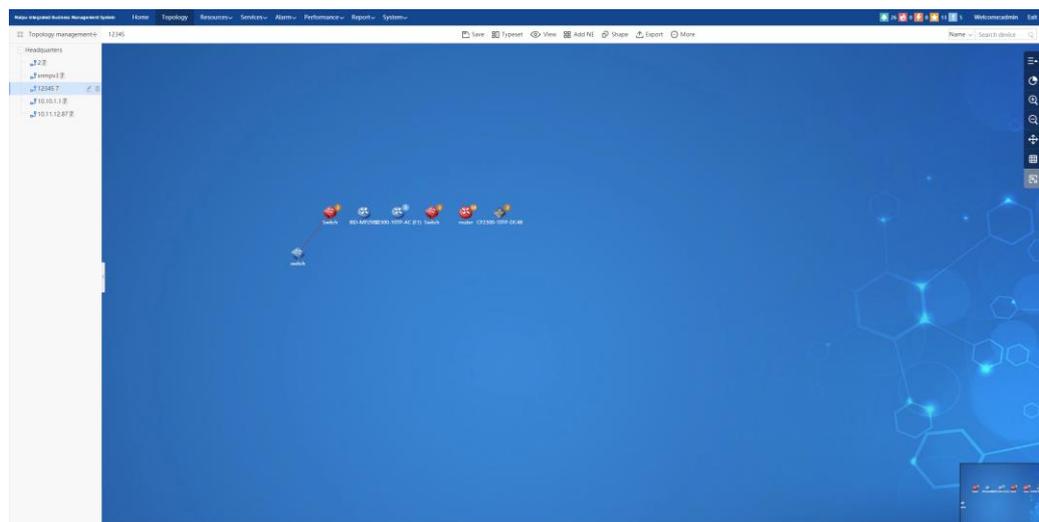


Figure 2-10 Topology view

For big-scale networks, there are many devices in the topology, and the relationship between devices is complex. In order to facilitate the monitoring and management for the big-scale network, the network management system provides various operation interfaces for topology display. Users can easily zoom in, zoom out, drag, and drop, change layout, search specific devices, save the current topology and so on.

When the network management system performs network discovery, some factors (such as device breakdown, network management protocol not enabled.) may cause the network management system not to discover the connection relationship between a certain device or two devices. The network administrator can perform network discovery

again, and also can add or remove devices and edit links manually in this topology view. In addition, it also provides topology view background setting, font color setting, create sub view, and other operations.

As shown in Figure 2-10, several functional areas in the topology view are described as follows:

### 2.2.1. Function Button Area



: Save the layout, display information, and edit results of the current topology



: Choose different ways to rearrange the topology.

NE: select different layout methods to rearrange the topology (grid, star, tree);

Link layout: select different connection types to redisplay link connections (straight line, arc, polyline).



: Select the device display information (the number of links, alarm, device name, device IP, device MAC) in the topology map.



: Add network elements (virtual nodes (unique to physical topology), devices, and topology links) to the topology view.



Virtual network node: Hold and drag to the topology view to add a virtual node at the drag-drop location, and set the name, model and IP information.



Device: Hold and drag to the topology view, and select the devices to be added to the topology view in the pop-up selection box. You can add devices to the current view. When you select multiple devices, they are arranged in a circle centered on the drag-drop position.



Topology connection: Hold and drag to the topology view, and select other topology views in the pop-up selection box, which can be displayed in the form of topology link at the drag-drop location.



China telecom: Hold and drag to the topology view to add a Telecom carrier icon at the drag-drop location.



China unicom: Hold and drag to the topology view to add a Unicom operator icon at the drag-drop location.



China Mobile: Hold and drag to the topology view to add a Mobile operator icon at the drag-drop location.



网络云 : Hold and drag to the topology view to add a network cloud at the drag-drop location, set the name of the network cloud, and drag the size.



Export : Export the topology in the picture format.



Shape : Add shapes to the topology view (basic shape, text editing, set, support dragging size).

Basic shapes (common background, support setting the text and appearance, refer to the figure below for details)



: Hold and drag to the topology view to add a rectangular background at the drag-drop location.



: Hold and drag to the topology view to add a rounded rectangular background at the drag-drop location.



: Hold and drag to the topology view to add an elliptical background at the drag-drop location.

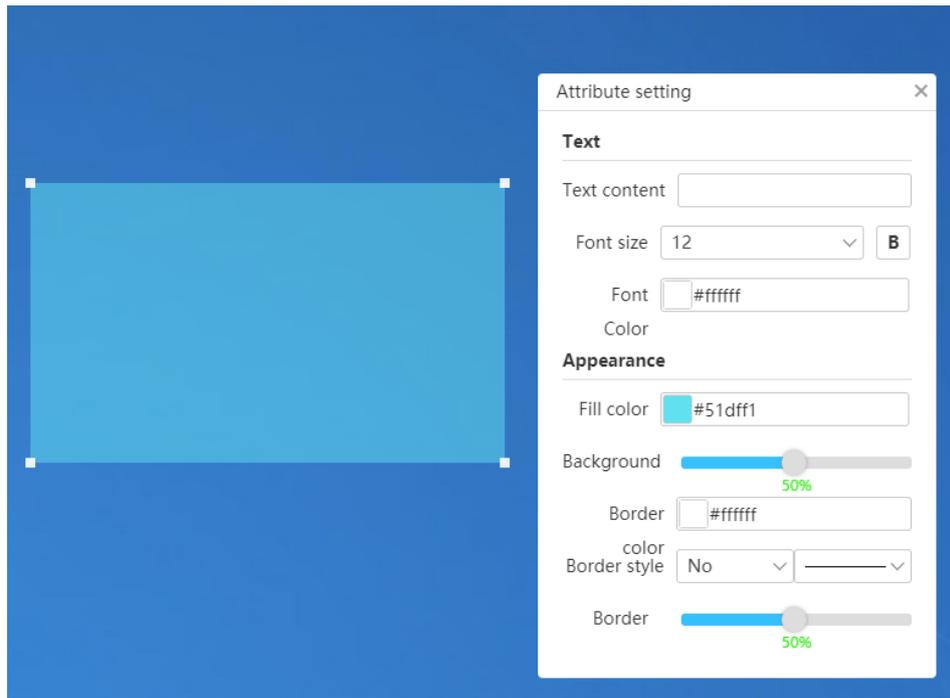


Figure 2-11 Basic shape attribute setting

Text editing (horizontal or vertical text box, support text setting, see the figure below for details)

 : Hold and drag to the topology view to add a text box at the drag-drop location.

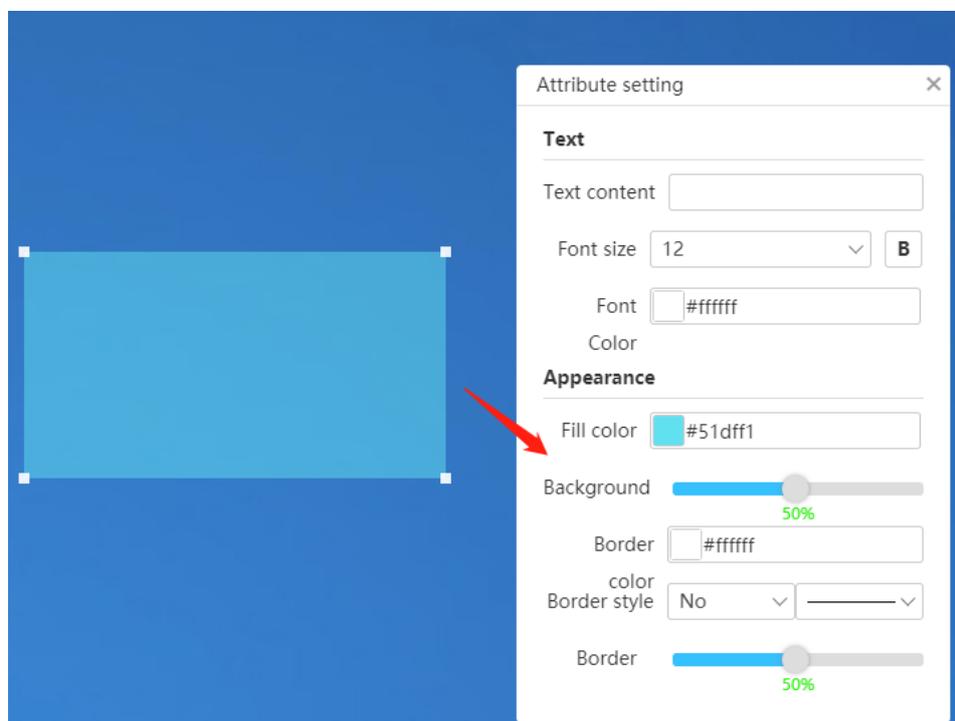


Figure 2-12 Text editing attribute setting

Collection (collection container, the device node can be added/removed from the collection by dragging and dropping, and the text can be set, as shown in the figure

below)

 : Hold and drag to the topology view to add an ellipse collection at the drag-drop location.

 : Hold and drag to the topology view to add a rectangular collection at the drag-drop location.

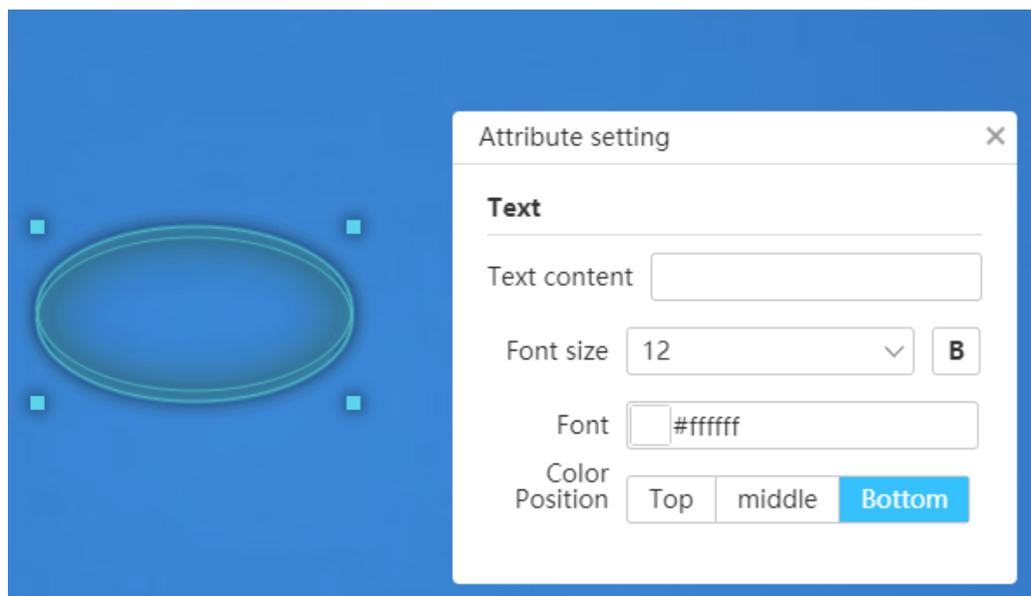


Figure 2-13 Set attribute setting

 **Subnet** : Display/hide the subnet in the topology. This function is unique to the logical view, as shown in the following figure.



Figure 2-14 Subnet filtering

 **more** : Other function options (background setting, font color setting, streamer effect setting, acceptance rate setting, legend description).

### Background setting

Two kinds of background styles are built in the system. At the same time, new background styles can be uploaded through "**Upload Material**". You can click the mouse to select the background style, preview the background style through the "**Preview**" button, and save the background style change through the "Use" button, as shown in the following figure.

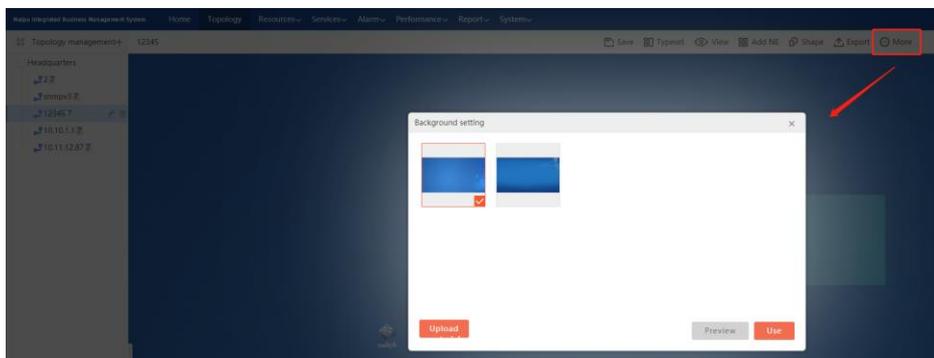


Figure 2-15 Topology view background setting

### Font color setting

Set the font color in the topology view and provide 72 colors for selection, as shown in the following figure.

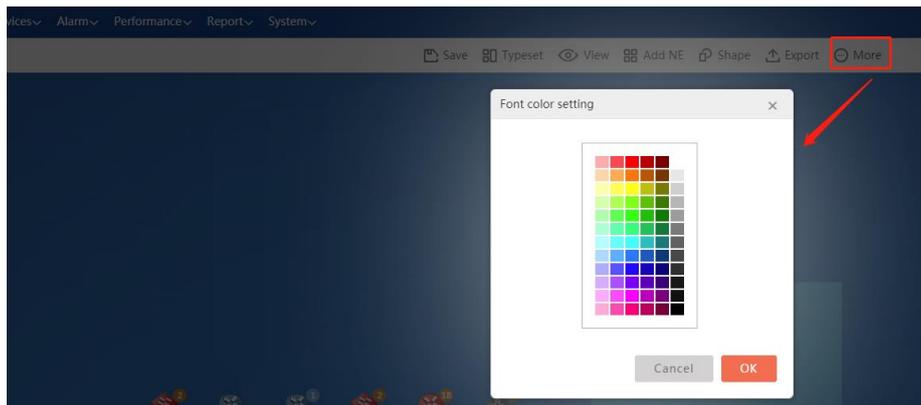


Figure 2-16 Front color setting of the topology view

StreBy setting "Streamer Effect in the "More" menu, you can set the streamer effect of the topology link globally.

Enable: Click to enable the streamer effect;

Disable: Click to disable the streamer effect;

Speed setting: configure the threshold value of streamer speed, as shown in the following figure.

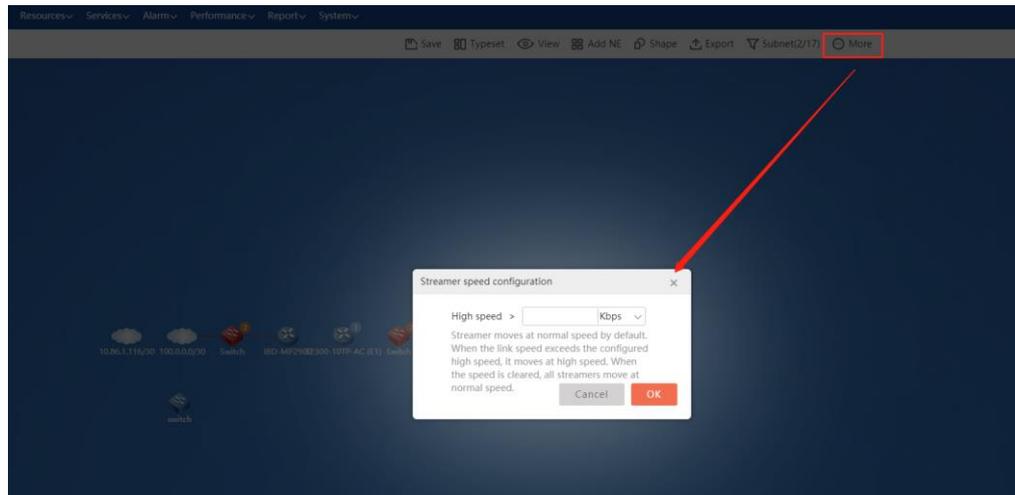


Figure 2-17 Streamer speed setting

### Receive rate

By setting "Receive rate" in the "More" menu, you can display and hide the receive rate of the topology link globally.

Enable: Click to display the receive rate;

Disable: click to hide receive rate.

### Legend description

Click "Legend Description" in the "More" icon, and you can view the legend description of the topology view, as shown in the following figure.

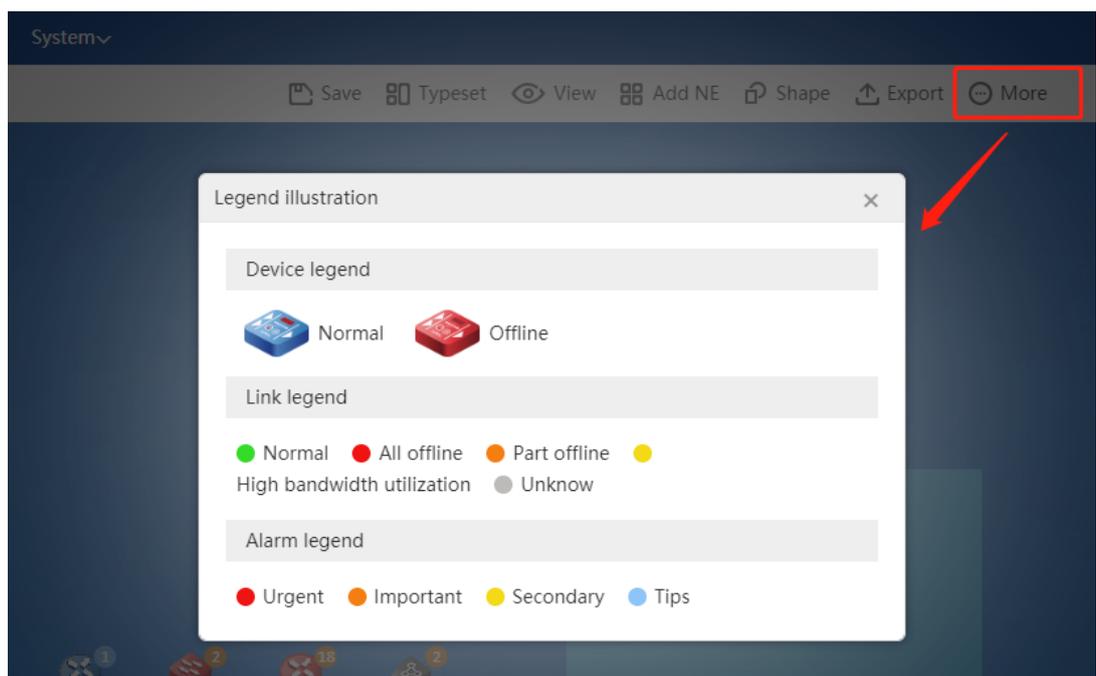


Figure 2-18 Legend description

## 2.2.2. Search Area

Within the scope of the current topology view, the device can be queried according to the device name, alias, IP, MAC information

## 2.2.3. Tool Bar

: Expand/Hide toolbar

: Display the topology statistics information, click to pop up the statistics window, as shown in Figure 2-19

: Enlarge the topology

: Narrow the topology

: Topology anchor, mouse drag-drop topology switch

: Open/close the aerial view

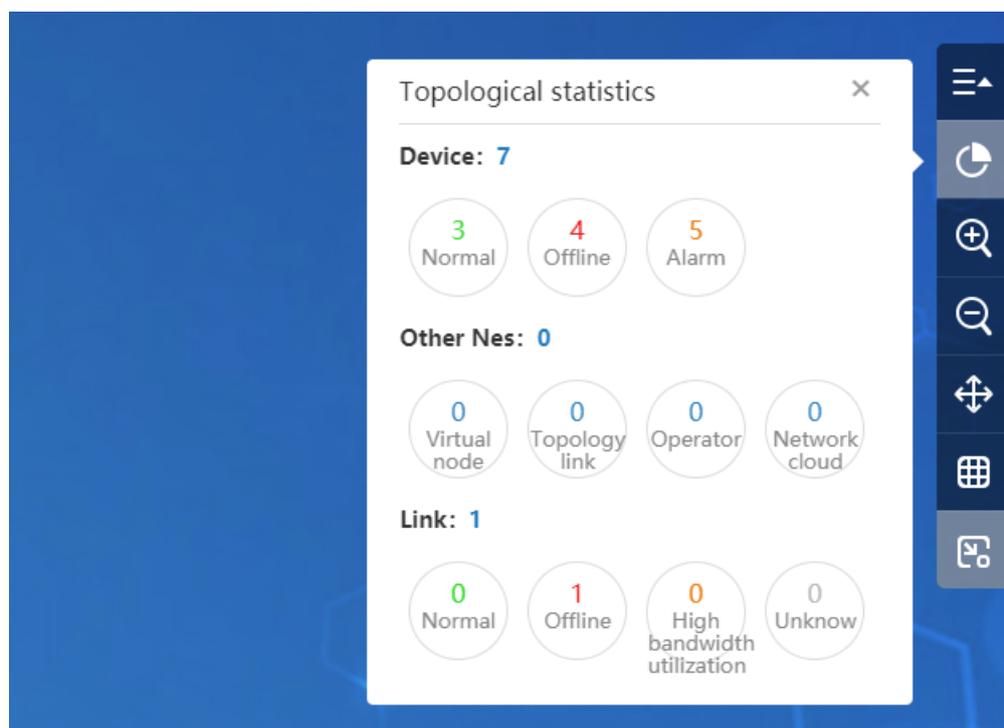


Figure 2-19 Topology statistics

## 2.2.4. Aerial View

By dragging the display area of the current screen in the aerial view, you can view the part of the topology map that is not displayed on the screen.

Double-click the current screen display area in the aerial view, and you can locate the double-click position in the middle of the screen.

## 2.2.5. Right-click Menu

Right-click "NE" or "Link" to pop up the corresponding function menu. The details are as follows:

### The right-click menus of the network element

- View details:

To view the details of the device information, you can also double-click a device in the topology view, as shown in the figure below. Some main information of the device is displayed in the device information box. To view more information of the device, you can click the "View Details" button at the bottom of the device information box.

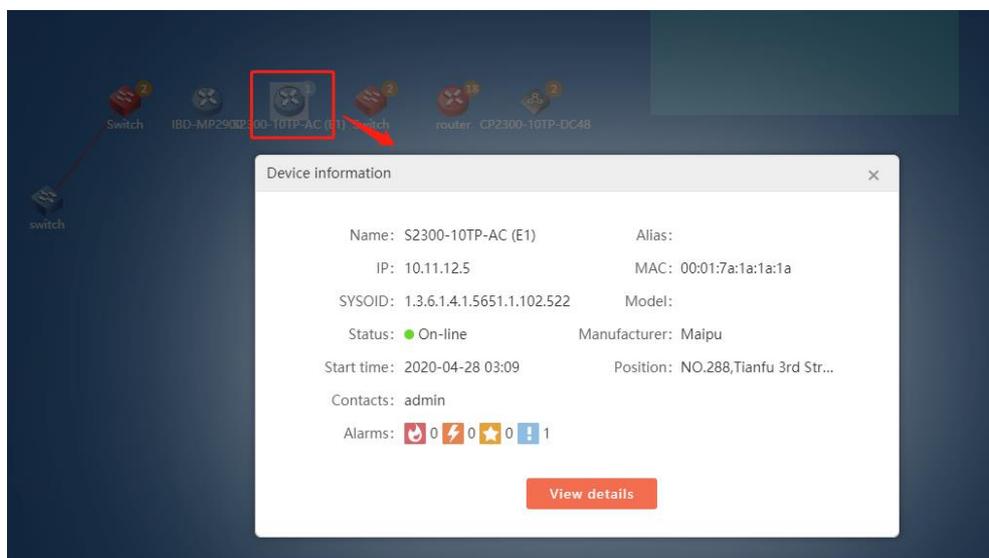


Figure 2-20 Device information box

- Add links:

Add the link between the network elements in the topology view. This menu is only supported in the topology physical view. This function is available for single and dual selection of network elements. After selecting the information on both ends of the link, click **Add** to add the link in advance. The pre-added link can be deleted by "Batch delete" or . Click "OK" to confirm the adding, and click "Cancel" to give up the adding, as shown in the figure below.

Add link
✕

Source node

Source NE

Source port

Peer node

Peer NE

Peer port

Selected

<input type="checkbox"/>	Source NE	Source interface	Peer NE	Peer interface	Operation
No relevant data					

Figure 2-21 Add the link

### Note

- The link added in the topology view is only displayed in the current topology view and does not disappear with the re-discovery of the network.

- Display stacking:

The menu is available only after right-clicking the stacking device. Click it to display the details in the stacking and return to the topology view through the "Back" button.

- Remove NE:

In the topology view, "Virtual node", "Device" and "Topology link" can be removed. After the NE is removed, it will only not be displayed in the current topology view. After the device NE is removed, it will not be displayed again with the network rediscovery.

- Create topology:

Select more than one device network elements in the topology view, and create a new topology view through this function menu.

- Detection tool:

Provide the ping detection, traceroute detection and remote connection tools.

- Device panel:

Provide the jump function to jump to the device panel page of the selected device.

- Refresh device:

Provide the status of refreshing selected devices on the topology view.

- Enter the view:

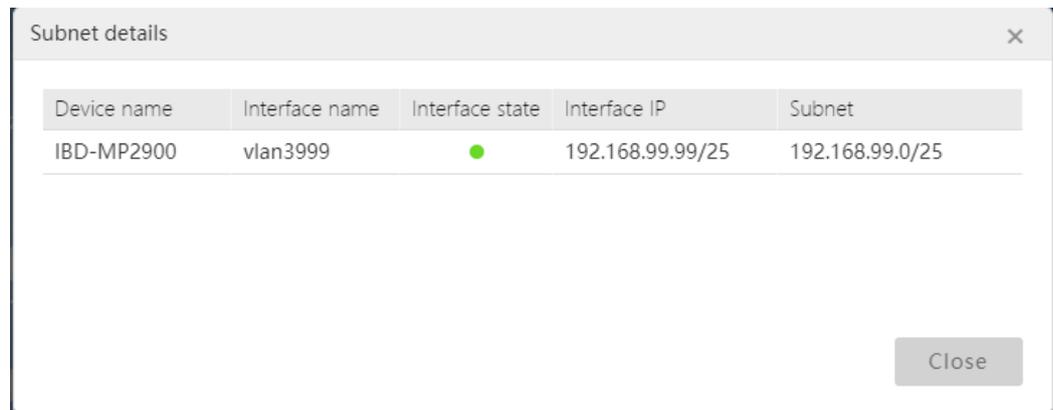
The menu is available only by right-clicking the topology link. You can jump to the topology view page of the link, and return to the current topology through the "Back" button.

- Enter the subnet:

The menu is available only by right-clicking the subnet. The jump page displays the physical topology view of all devices in the subnet, and you can return to the current topology through the "Back" button.

- Subnet details:

The menu is available only by right-clicking the connection between the device and the subnet in the topology logic view, as shown in the figure below. The subnet information of the device and interface is displayed in the subnet details box.



Device name	Interface name	Interface state	Interface IP	Subnet
IBD-MP2900	vlan3999	●	192.168.99.99/25	192.168.99.0/25

Figure 2-22 Subnet details box

- Place at the top: The menu is available only by right-clicking the shape, and click to put the corresponding shape at the top of all shapes.
- Move up one layer: The menu is available only by right-clicking the shape, and click to move up one layer of the corresponding shape among all shapes.
- Move down one layer: The menu is available only by right-clicking the shape. Click to move the corresponding shape down one layer among all shapes.
- Place at the bottom: The menu is available only by right-clicking the shape. Click to place the corresponding shape at the bottom of all shapes.

### The right-click menus of the link

- Link details:

The menu is available only by right-clicking the link in the topology physical view, as shown in the following figure. The link details box displays the detailed information of the two ends of the link. Click , and you can delete the link. Click "OK" to confirm the

deleting, and click “Cancel” to drop the deleting.



Figure 2-23 Link details box

- Delete link: The menu is available only by right-clicking the link in the topology physical view. Click to delete the selected link.
- Add the interface to monitoring: Click to add the interfaces at the two sides of the selected link to monitoring.
- Set bandwidth: Click to set the bandwidth for the interfaces at the two sides of the link, as shown in the following figure.

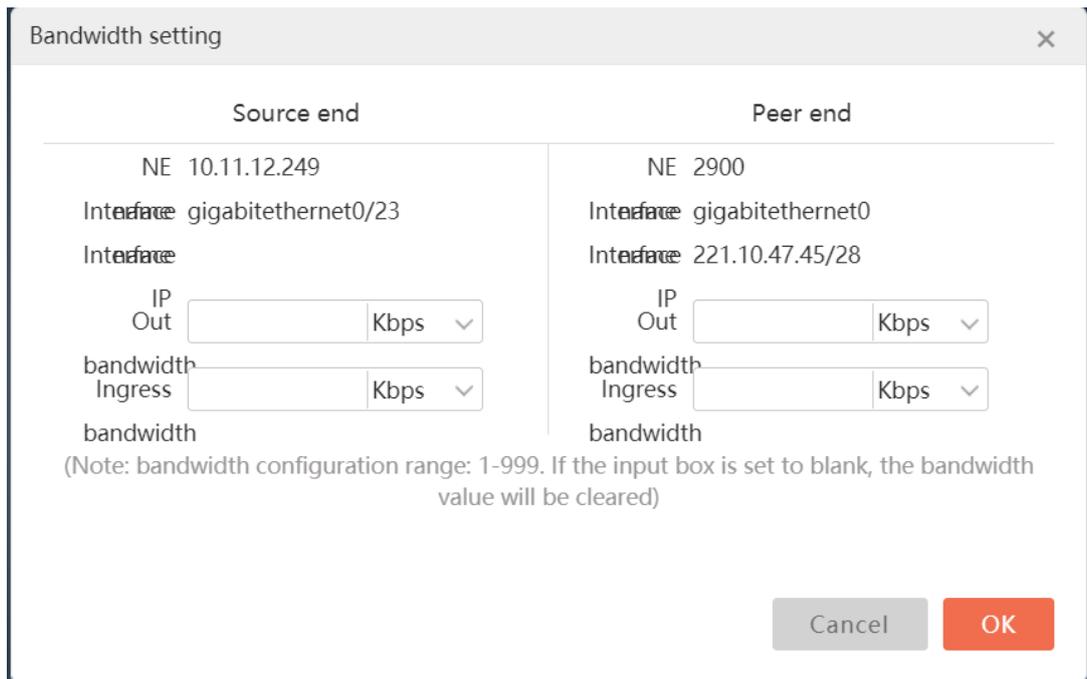


Figure 2-24 Bandwidth setting box

- Real-time performance: Click to open the performance monitoring page, displaying the real-time monitoring data of the interfaces at both ends of the link.
- Historical performance: Click to open the performance monitoring page, displaying the historical monitoring data of the interfaces at both ends of the link.
- Receive rate: Click Enable/Disable to display/hide the receive rate of the selected link.
- Streamer effect: click Enable/Disable to enable/disable the streamer effect of the selected link.

- Straight line: Click to set the connection type of the selected link as straight line.
- Arc: Click to set the connection type of the selected link as arc.
- Broken line: Click to set the connection type of the selected link as broken line.

### Note

- The confirmed deleted link in the link details box is deleted only from the current topology view, and will not appear with the network discovery again.

### Alarm statistics:

The topology view provides the alarm information statistics of the network devices (the total number of unconfirmed alarm information of the devices is displayed in the small circle beside the network device. If the number of alarms exceeds 99, the page will display as "99+". Click the device to view the details, and you can see the specific number of alarms. Click the corresponding number of alarms, and you can jump to the alarm information interface of the device details, as shown in the figure below).



Device information

Name: router      Alias:

IP: 10.10.1.1      MAC: 00:01:7a:97:96:6a

SYSOID: 1.3.6.1.4.1.5651.1.101.423      Model: MP1800X-40E(E2)

Status: ● Off-line      Manufacturer: Maipu

Start time: 2020-05-20 07:57      Position: Maipu Mansion,No.28...

Contacts: Maipu Communication Technology Co.,Ltd.

Alarms:  0  4  13  1

Double click will enter the alarm menu

View details

Figure 2-25 Alarm statistics

## 3. Resource Management

Resource management mainly manages all the network resources under the integrated network management platform of Maipu. Functions include device management and interface grouping, device type management, network discovery, configuration management and certificate management.

### 3.1. Device Management

#### 3.1.1. Device Management

The device management module provides management functions for all devices in the system, including grouping devices, searching for specific devices by filtering conditions, setting aliases for devices, and viewing device details. Click "Resources" -> "Device Management" in the navigation bar at the top of the system to open the "Device Management" interface, as follows:

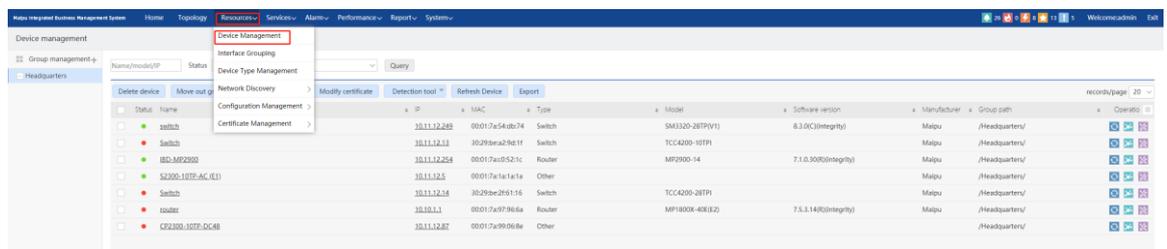


Figure 3-1 Device management

#### Device list

Open the "Device Management" interface to display all the devices in the system by default, displaying the status, name, alias, IP, MAC, type, model, software version, manufacturer, grouping path and other information of each device by lists. It also supports the "List function". You can select and save the displayed lists and their positions. The serial number, sysoid and hardware version are not checked by default. You can check and display them as needed, as shown in the following figure:

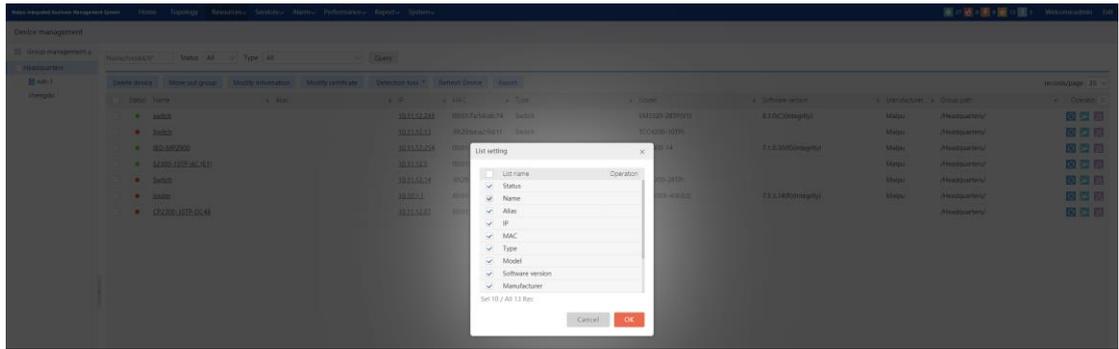


Figure 3-2 List setting

The devices displayed in the device list is determined by the group tree on the left. If the device group node is selected in the group tree on the left, the device list in the device group will be displayed in the list; if the organization node is selected in the group tree on the left, the list will display all device lists visible to the organization (including the devices of the organization and all its subordinate organizations), as shown in the following figure:

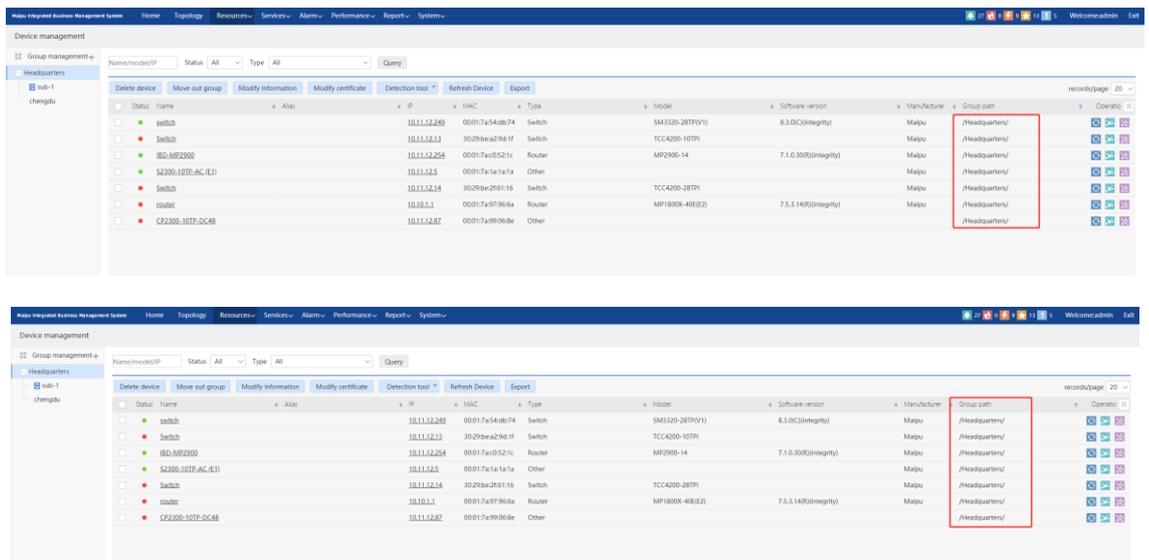


Figure 3-3 Device list display

The device lists that administrators of different organizations can view are different. They can only view the device information of the organization to which the administrator belongs and its subordinate organizations. They cannot view the device information of the superior organization or the same-level organization, as shown in the following figure:

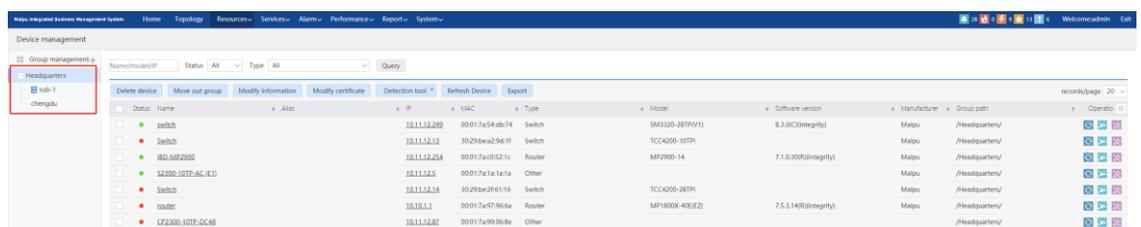


Figure 3-4 Hierarchical decentralized display

This page provides various query conditions for querying specific devices conveniently and quickly. Enter the corresponding query criteria in the query panel, and then click the "Query" button to filter all devices according to the name, alias, model, IP, status, type and other fields.

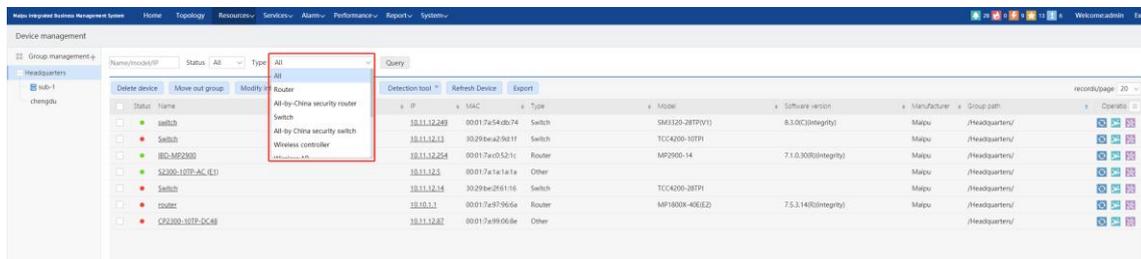


Figure 3-5 List query

Click each field in the head of the device list, and you can sort the devices according to the corresponding fields. As shown in the figure below, all "Online" routers whose name, model or IP matches the string "10.10.60.11" are found and sorted in ascending order according to the device name:

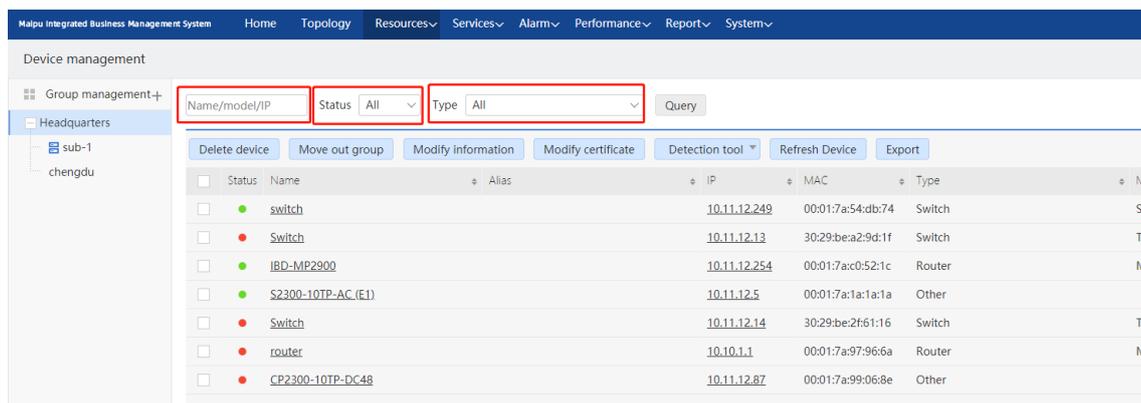


Figure 3-6 Device query and sorting

## Note

- The query input box can fuzzy match any one of the device name, model and IP, and the IP will match all the IPs of the device, including access IP and device interface IP.

### Add device group:

Network management system provides device grouping function, and reasonable grouping is more convenient for managing devices. The system implements hierarchical and decentralized management for the device groups. All device groups are attached to corresponding organizations. Administrators of different organizations can only create, modify, and delete device groups for the current level and its subordinate organizations.

Click  of the group tree on the left side of the device list to open the "Add group" page. You need to enter the name, select the parent node, enter the basic information of the device group, such as the description information, to create the group, as shown in the following

figure:

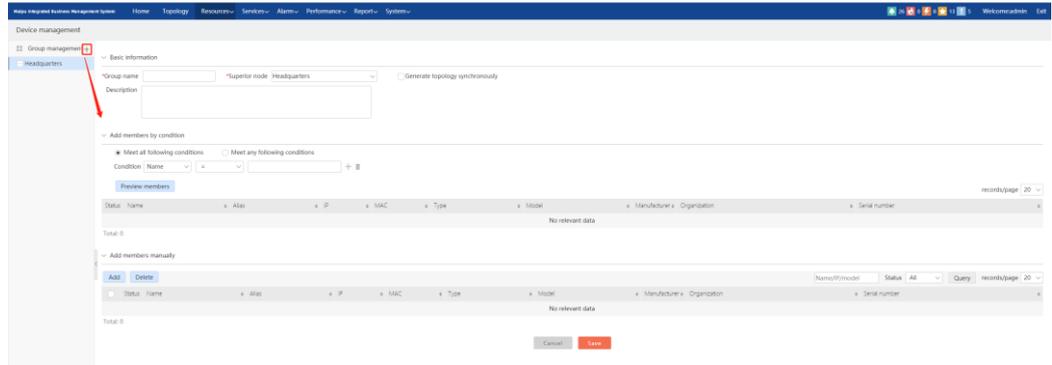


Figure 3-7 Add device group

When creating a device group, there are two ways to add devices: manually add devices and conditionally add devices, which can be used alone or in combination. Manually added devices will always remain in the device group, unless the devices are moved out of the group or transfer organization, the conditionally added devices will change with the change of conditions, which is dynamic.

Click the "Add" button to manually add devices for this device group. As shown in the following figure, in the pop-up "Select devices" dialog box, you can select the organization tree on the left, and match the devices that meet the query criteria under the selected organization by name, model, IP and status. Support "Select all" and "Delete all".

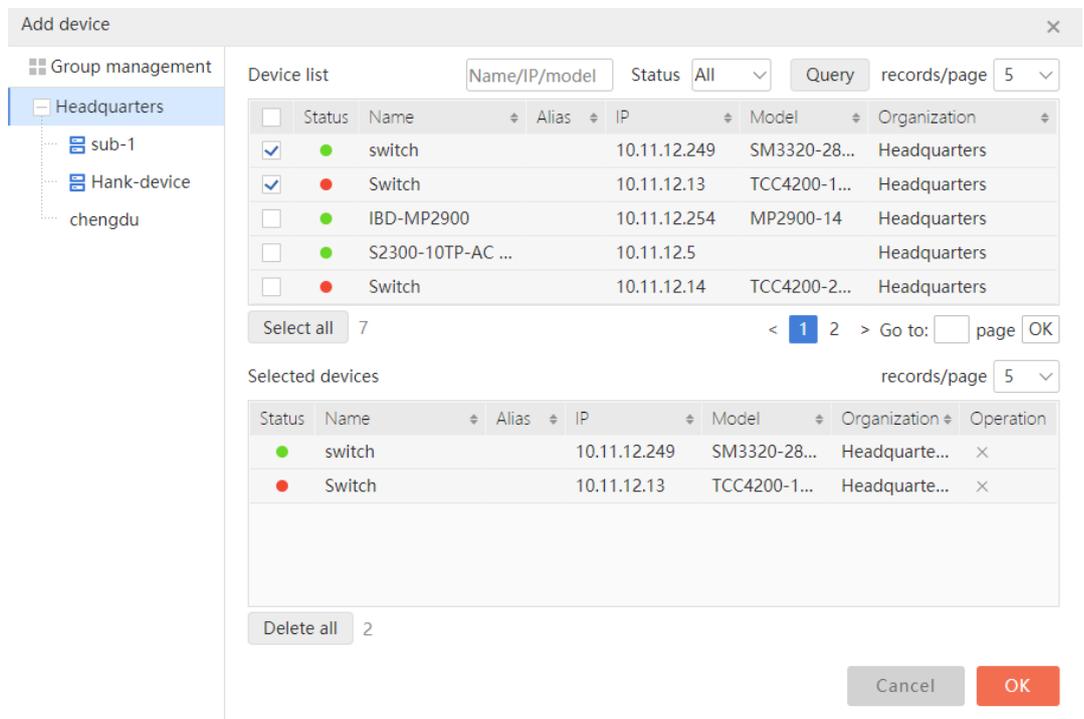


Figure 3-8 Select devices

Click "OK" after selecting the device to add the selected device to the list of manually added members.

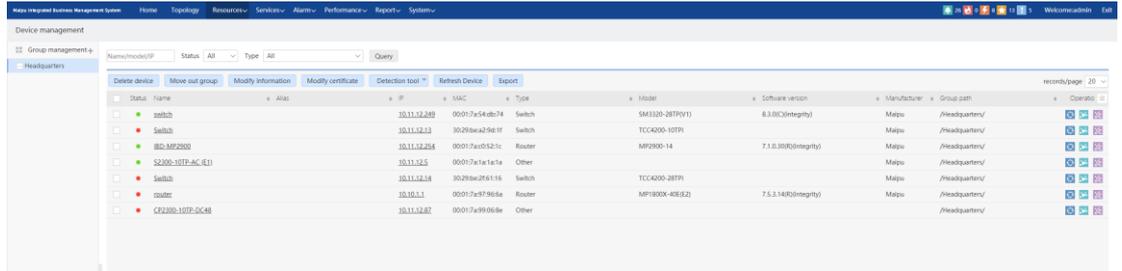


Figure 3-9 Manually add devices

For the conditionally added devices, you can match devices by creating different conditions. It supports "Meet all conditions" and "Meet any conditions", supporting matching device name, model, manufacturer, type, and IP address conditions. You also can preview the current matching results by clicking "Preview members", as shown in the following figure:

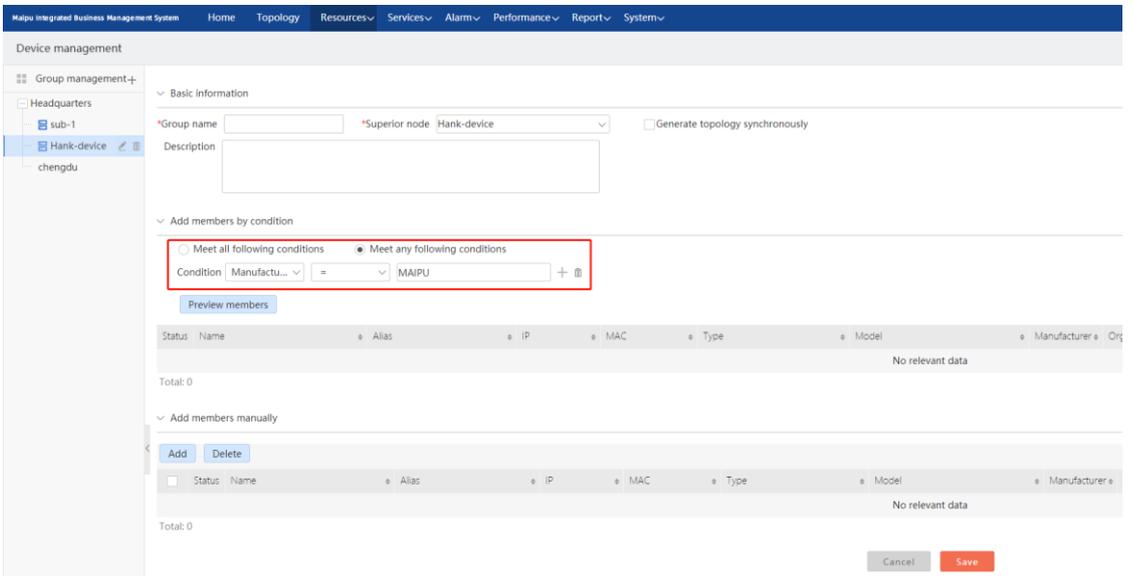
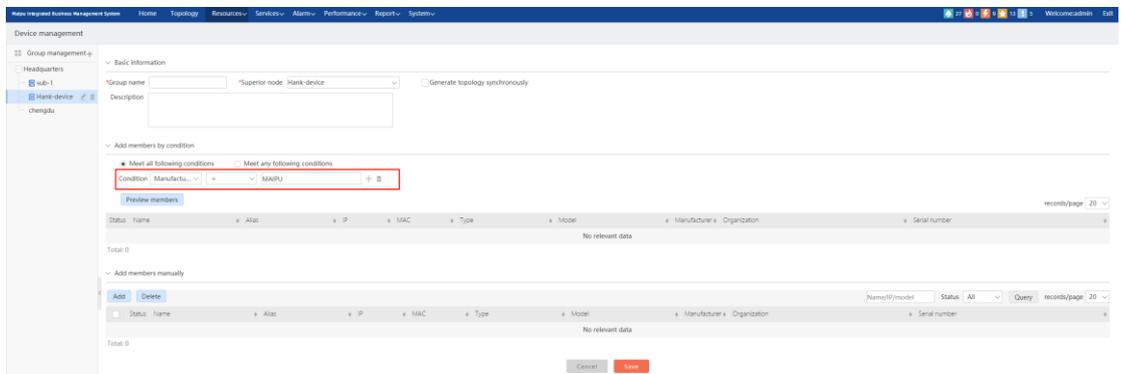


Figure 3-10 Members

**Note**

- The device range matched by the conditionally added members is the devices directly under the organization of the selected "parent node" (excluding the devices of the subordinate organization), that is, if the selected parent node is the organization node, match the device directly under the organization; if the selected

parent node is the device group node, match the device directly under the organization of the device group.

- The range of devices that can be selected as manually added members is all devices visible to the current login user.

Click “Save” to save the device group. At this time, the device group will be attached to the selected “Parent node” and displayed in a tree structure. If the manually selected members contain the devices of other organizations, the system will prompt whether to create the device group. If yes, the selected devices will be deleted from other organizations and added to the organization of the current device group.

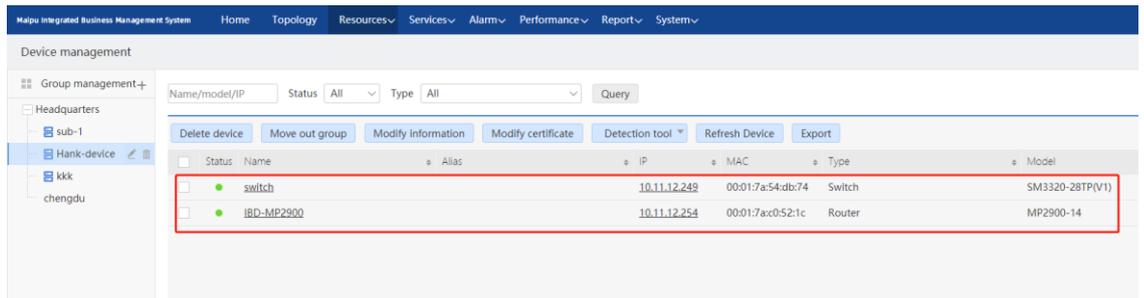
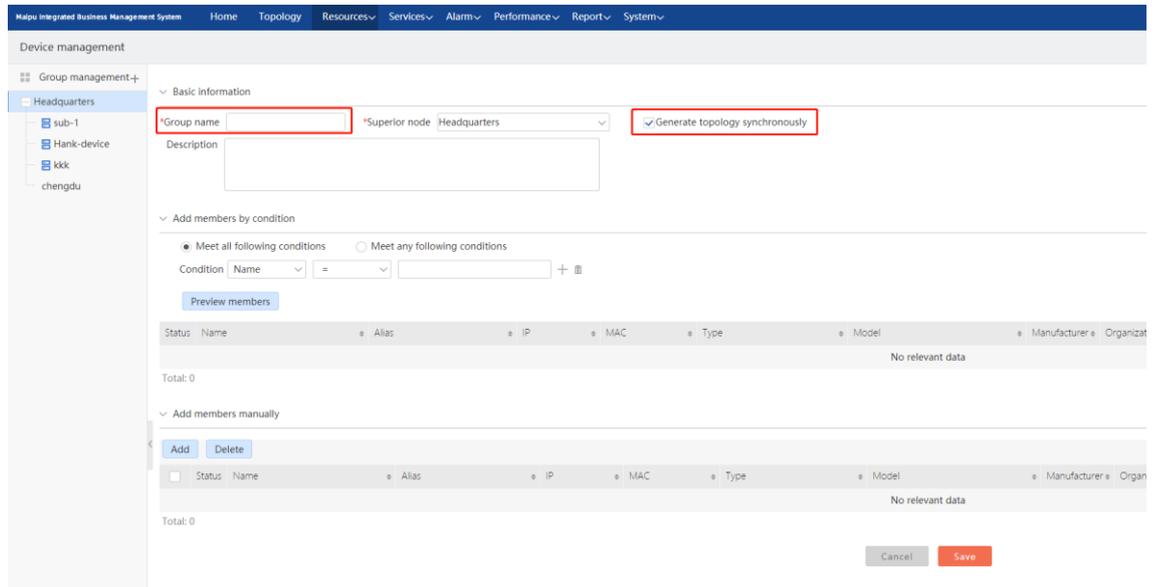


Figure 3-11 Add device group successfully

If “Generate topology synchronously” is checked when creating a device group, a topology view with the same name as the device group will be created synchronously in the topology view, and the topology of the device in the device group will be created, as shown in the following figure:



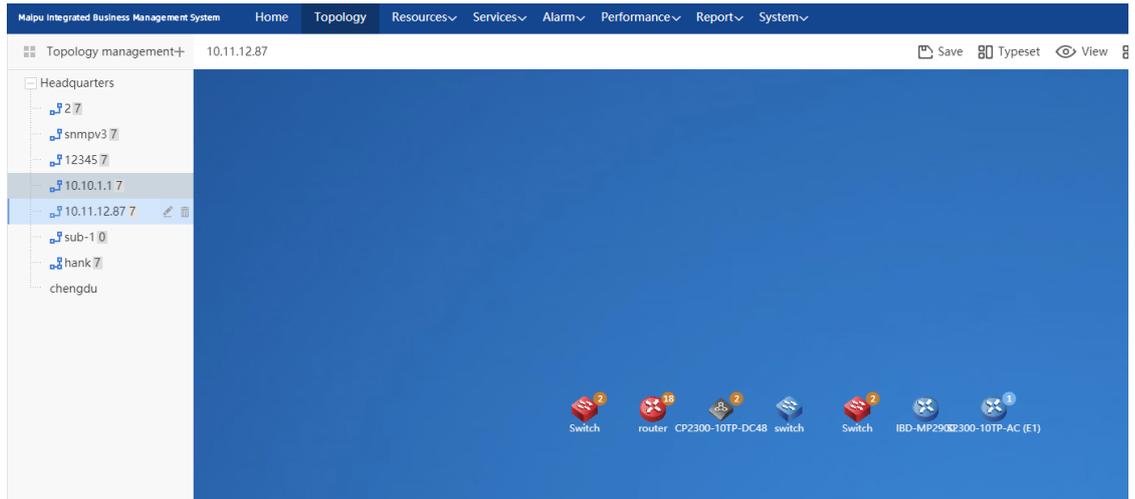


Figure 3-12 Generate the topology synchronously

**Edit device group:**

Select the device group to be edited in the left tree of the device management page, click  to enter the page of editing the device group, where you can edit the group name, description, and members in the group. "Parent node" cannot be edited, and the method of manually adding members and conditionally adding members is the same as that of adding a device group.

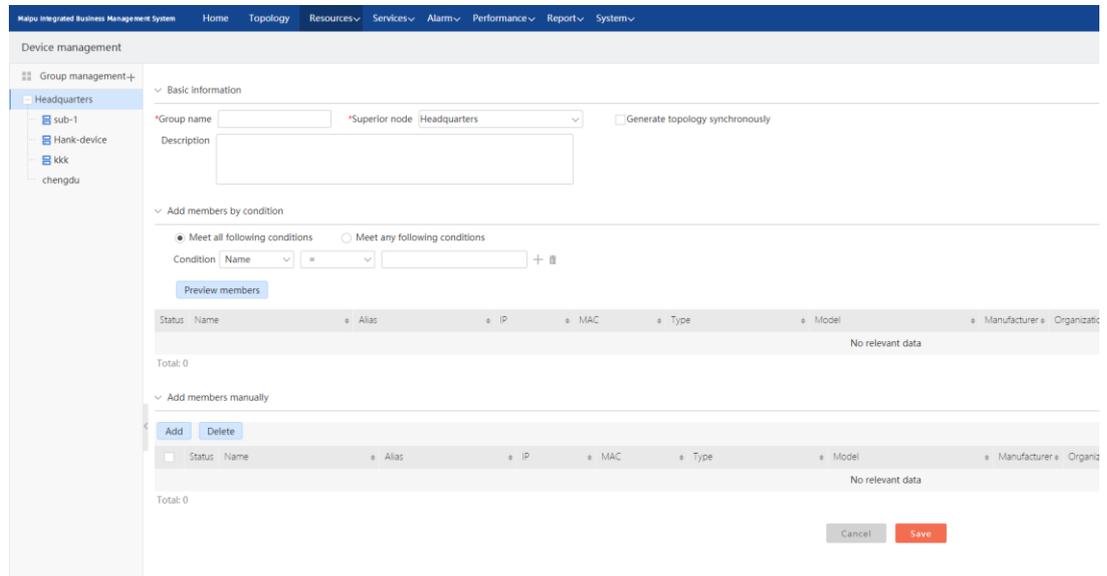


Figure 3-13 Edit device group

 **Note**

- When adding/editing a device group, the rule of duplicate name is no duplicate name under the same grouping path and no device group with the same name under the same "Parent node". If the duplicate name is used, a prompt will be given when saving the device group.
- It supports synchronously generating the topology when adding a device group, but

cannot generate topology views when editing device groups.

### Delete device group:

In the left tree of the device management interface, select the device group to be deleted, click  to open the dialog box of confirming the deleting, and then confirm to delete the device group.

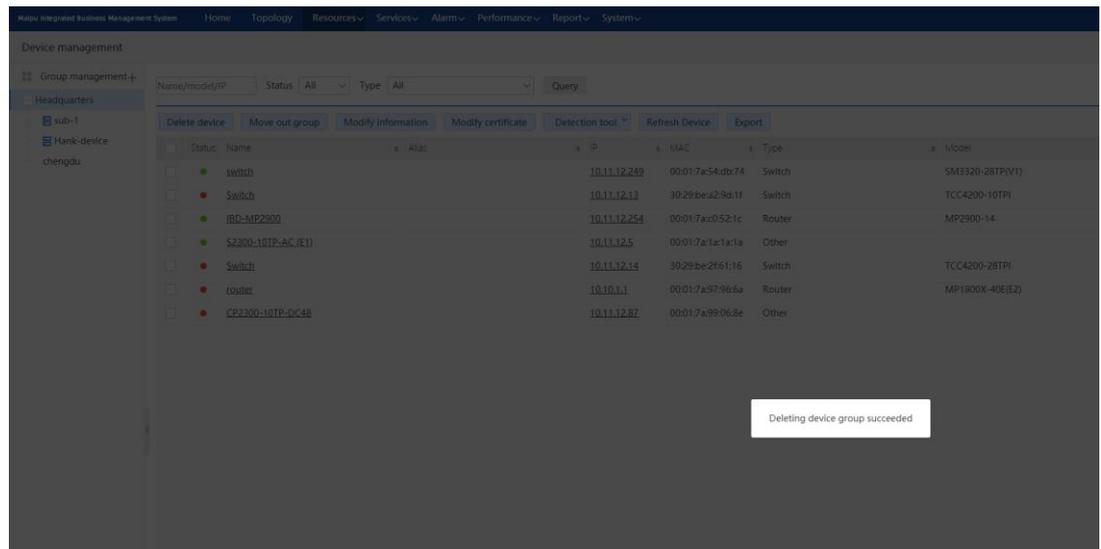
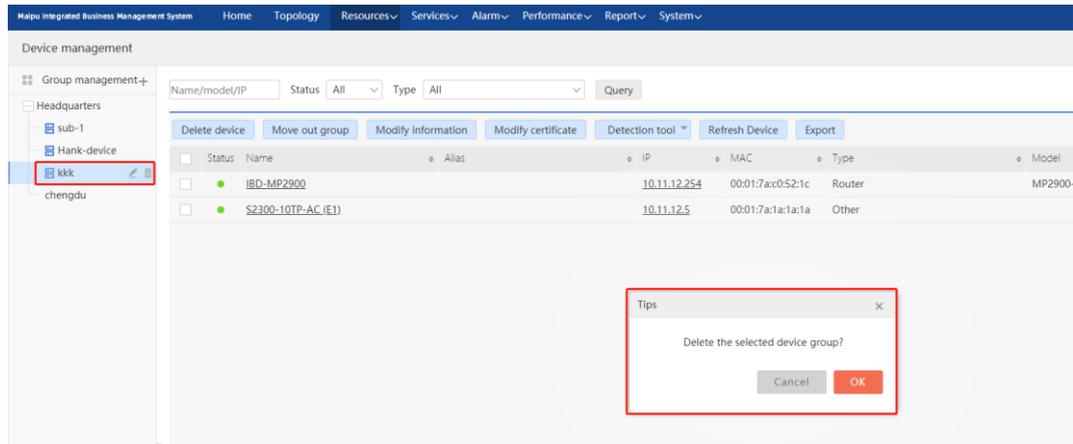


Figure 3-14 Delete device group

### Note

- If there are nested device groups, delete the parent device group, and the child device group will be deleted synchronously.
- After the device group is deleted, if the device does not belong to other device groups of the organization to which the device group belongs, the device in the group will belong to the root of the organization (that is, the ungrouped device).

### Refresh devices:

Select the device, and click "Refresh device" to perform network discovery for the device again, or click  at the right side of the device list to refresh manually. After clicking ,

the confirmation dialog box will pop up as shown in the figure below, and click the "OK" button to start refreshing.

Terminal devices and wireless APs do not need to be refreshed manually, so there is no  icon.

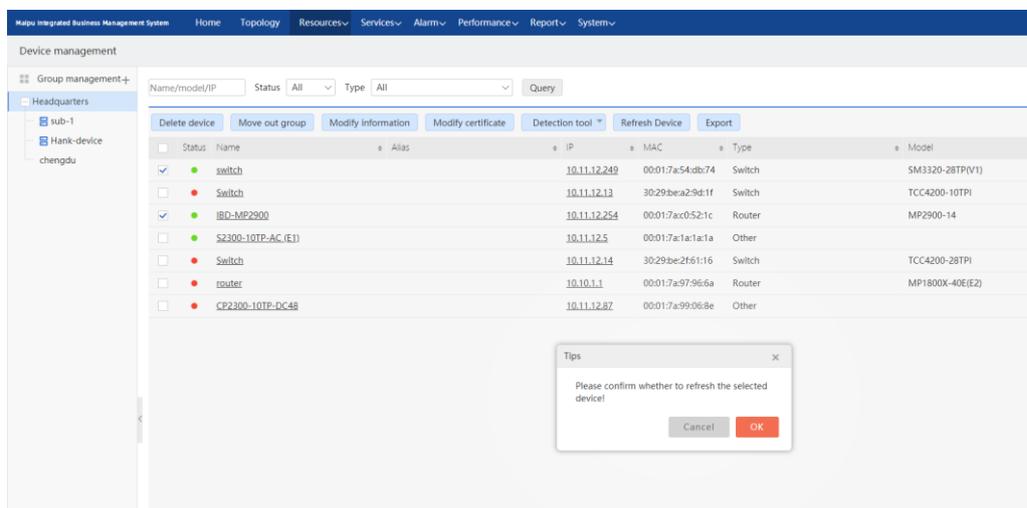


Figure 3-15 The prompt box "Refresh devices"

### Modify information:

First, check the device to be modified in the device list, and then click **Modify information** to open the following "Modify device information" dialog box. You can modify the name, alias, location, contact, organization of the device, and web management URL of the device, and click the "OK" button to modify the device information successfully.

Figure 3-16 Modify device information

When batch modifying device information, only the organization of the device can be modified, as follows:

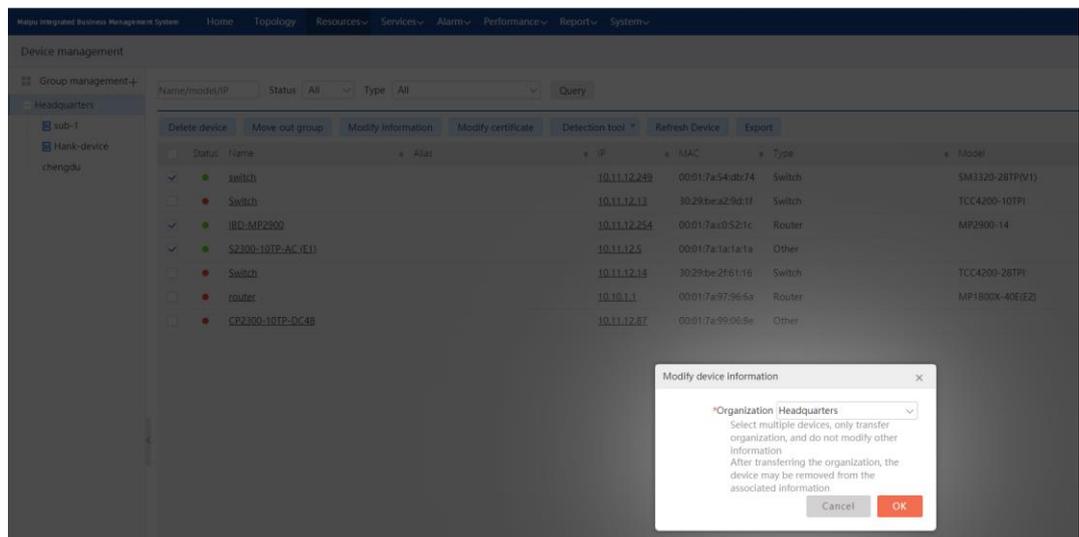


Figure 3-17 Batch modify device organizations

### Note

- The device name, device location and contact person can be modified successfully only after the device and network management system are configured with SNMP write authority at the same time;
- The web management URL can modify the access address when the device web

---

jumps;

- The function of transferring the organization of the device may cause the device to be deleted from the original organization, so if the device is selected in various tasks of the original organization, it may cause the device to be unable to be operated (if the device is transferred to the lower level organization, it has no effect; if it is transferred to the higher level or the same-level organization, it may have this problem).
  - After the device is transferred to the organization, the certificate configured by the original device can still be used, but it is not visible through the page (because the certificate is under hierarchical and decentralized management). Once the new certificate is re-configured for the device, the new certificate shall prevail, and the original certificate is invalid.
- 

### Modify certificate:

Modifying a certificate can add different certificates for the device. First check the device to modify the certificate in the device list, and then click the "Modify Certificate" button to open the following "Modify certificate" dialog box, where you can select the certificate type and name. Click "OK" to modify the certificate successfully.

Figure 3-18 Modify certificate

---

### Note

- The certificate types that can be modified include SNMP, telnet and SSH certificates (for security devices, there are also security certificates). The certificate that can be selected is the certificate of the organization of the selected device. Each device can only have one certificate of each type. Once modified, the same type of certificate that the device has configured will be overwritten.
  - When batch modifying device certificate, the selected device can only be the device of the same organization. Otherwise, a prompt will be given and the certificate cannot be modified.
- 

### Export:

The system supports the function of exporting the device list. Click the "Export" button to export the device list. The export file format is CSV format. The data and fields are the same as the data displayed in the current device list. Support querying the exported.

**Device web management:**

Device web management can manage the page operation of the device. Click the icon  of the operation list to enter the web management interface of the device.

**Locate to the topology:**

Locating to the topology supports jumping to the topology page, that is, to jump to the first topology view containing the device under the device's organization. If there is no topology view containing the device under the device's organization, it will jump to an empty view. Click the icon  of the operation list to jump to the topology interface.

**Delete the device:**

Check the device to be deleted in the device list (support multiple selection), and click the "Delete device" button to open the confirmation dialog box for deleting the device, as shown in the figure below. Click the "OK" button to confirm the deletion of the selected device, and click the "Cancel" button to cancel the deletion operation.

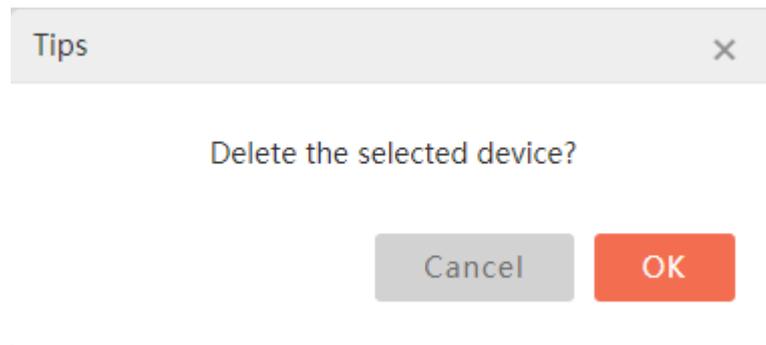


Figure 3-19 The prompt box of deleting the device

---

**Note**

- The device will be deleted from the device library by deleting the device. The device will not appear in the network management system until network discovery is performed again.

---

**Move out of group:**

Moving out of the group supports removing the selected device from the specified device group. Check the device to be removed from the group in the device list (support multiple selection), and click the "Move out of group" button to open the box for selecting the device to be removed from the group, as shown in the figure below. Select the device to be removed, click "OK" to confirm the removal of the selected device from the corresponding group, and click "Cancel" to cancel the removal operation.

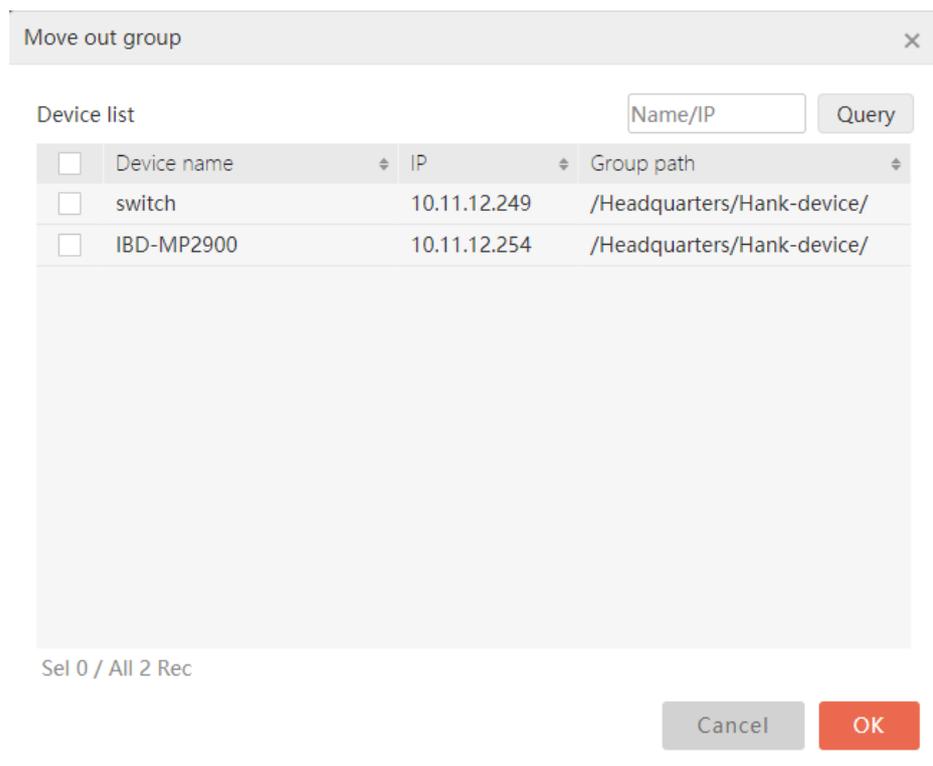


Figure 3-20 Remove the device from the group

### Note

- If the device is a member added by conditions in the device group and cannot be moved out of the group, the check box corresponding to the record in the selection box will become gray and cannot be selected. When the mouse points to it, it will prompt that "the device that is dynamically grouped into the group cannot be moved out. If you want to move out, please modify the dynamic condition of the device group".
- If the device is removed from the selected device group, the organization of the device will not change. If the device is not in any device group of the organization after being removed from the group, it will be directly mounted under the root of the organization.

### Detection tool:

The detection tool can perform the ping, traceroute, and remote connection for the device. Click the "Detection tool" button, a drop-down box will appear, in which Ping, traceroute and remote connection are displayed, and then click one of them, as shown in Figure 3-21 (take Ping as an example). Another way to use the detection tool is to select a device, and then click the "Detection tool" button to select one of them, as shown in Figure 3-22.

ping

Source type  Network management server  Device

\*Destination IP

Detection result

Figure 3-21 Ping operation

ping

Source type  Network management server  Device

\*Destination IP

Detection result

Figure 3-22 Perform the ping operation for the selected device

Ping operation:

The Ping operation is used to detect the connectivity between the local computer and the destination host. On the Ping operation interface, there is a check box, which contains the network management server and devices. Select the network management server and select a destination IP (or manually input IP), and then click the “Start” button to detect whether the network management server is connected to the destination IP. The effect is shown in Figure 3-23.

If you select a device, you need to select the source IP, destination IP, and SNMP certificate.

Then, click the “Start” button to detect whether the source IP and the destination IP are connected. The effect is shown in Figure 3-24. Note: when selecting the SNMP certificate, it is necessary to ensure that the SNMP certificate authority of the device is read-write. If there is no information in the SNMP certificate drop-down box, you need to configure the SNMP certificate of the device in the device details page.

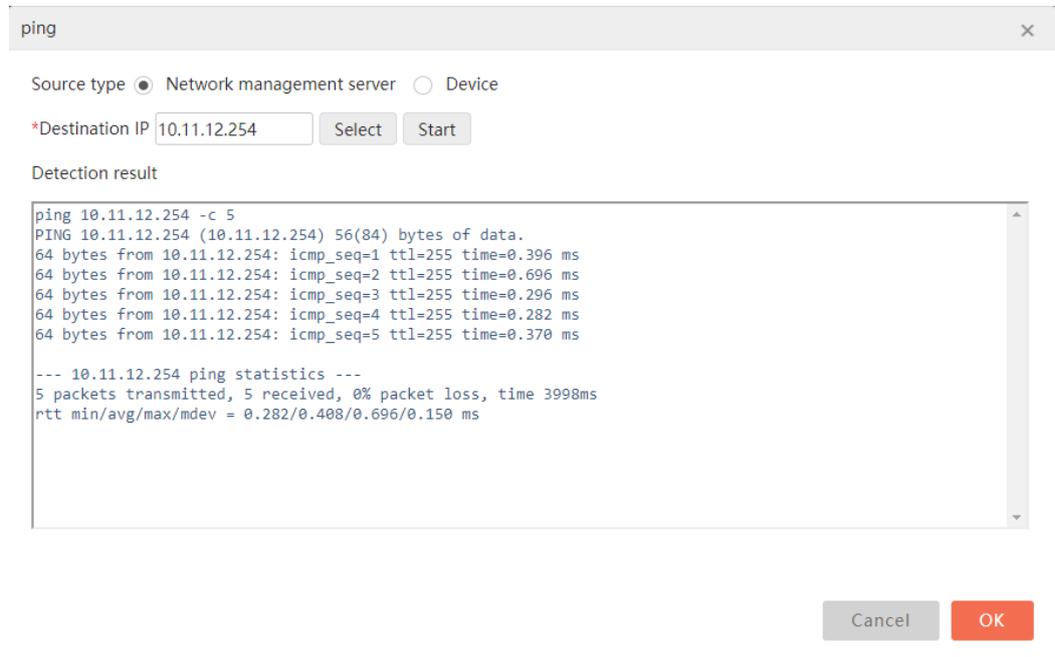


Figure 3-23 The ping operation of the network management server

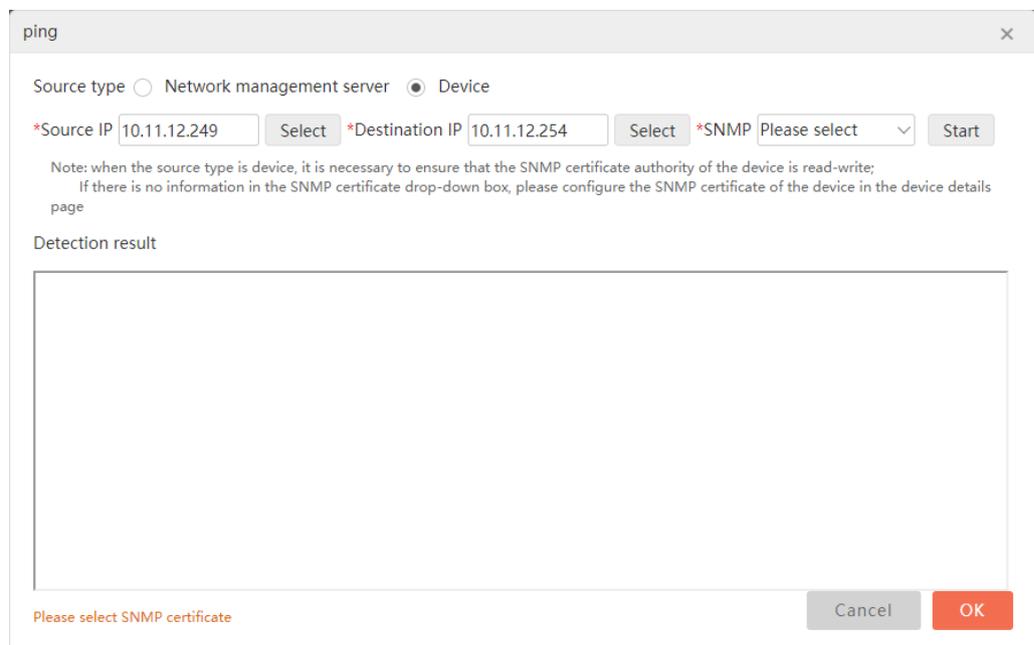


Figure 3-24 The ping operation of the device

Traceroute operation:

The Traceroute operation is a tool used to track packets to remote hosts. It will show how many hops to the destination and how much time it takes to go through each hop. On the

traceroute operation interface, you need to click the “Select” button to select the device IP (or manually input IP), and then click the “Start” button. If you want to stop the operation, directly click the “Stop” button. The effect of the traceroute operation is shown in Figure 3-25.

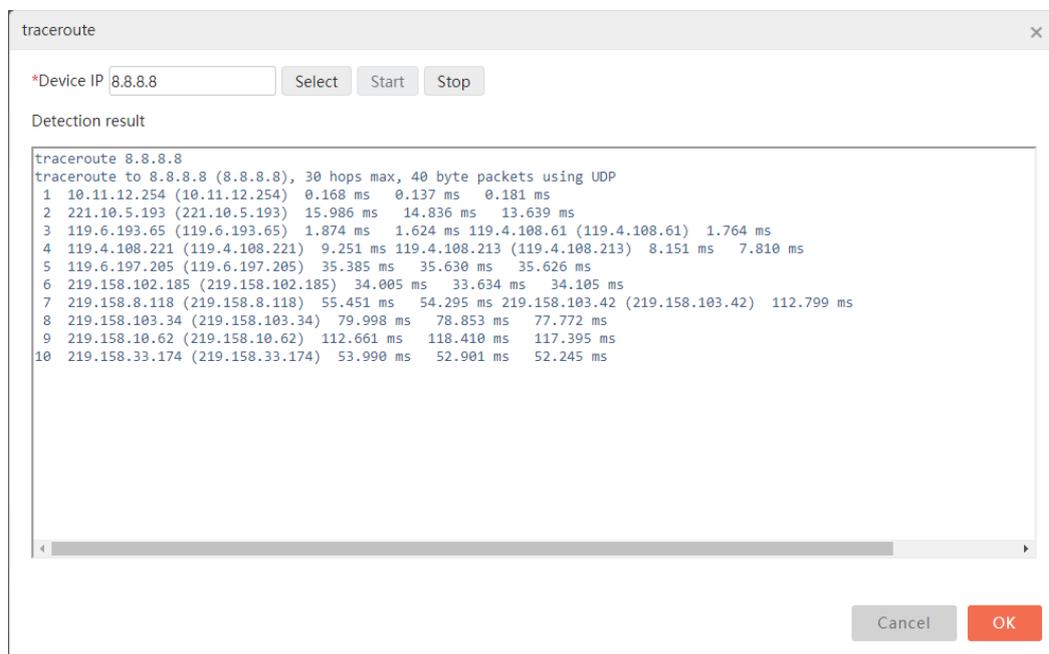
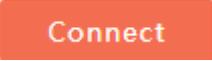


Figure 3-25 Traceroute operation

Remote connection operation:

Remote connections provide telnet and SSH connections. On the remote connection interface, the user needs to click the button, select a device, fill in the device port number, select the encoding format, and select the connection protocol, as shown in Figure 3-26.

Take the SSH operation as an example. Select the device IP and SSH protocol. The port number and encoding mode will be automatically filled in according to the protocol. Fill in the user name and password, and then click the  button to enter the SSH connection interface. The effect is shown in Figures 3-27 and 3-28.

Remote connection

\*Device IP

\*Port number

\*Code

\*Protocol

Note: 1. If you need to send Chinese command to the device, please select [GB2312] code before [connect]  
2. After [connect], a browser window will be reopened

Figure 3-26 Remote connection operation

Remote connection

\*Device IP

\*Port number

\*Code

\*Protocol

\*User name

\*Password

Note: 1. If you need to send Chinese command to the device, please select [GB2312] code before [connect]  
2. After [connect], a browser window will be reopened

Figure 3-27 ssh operation

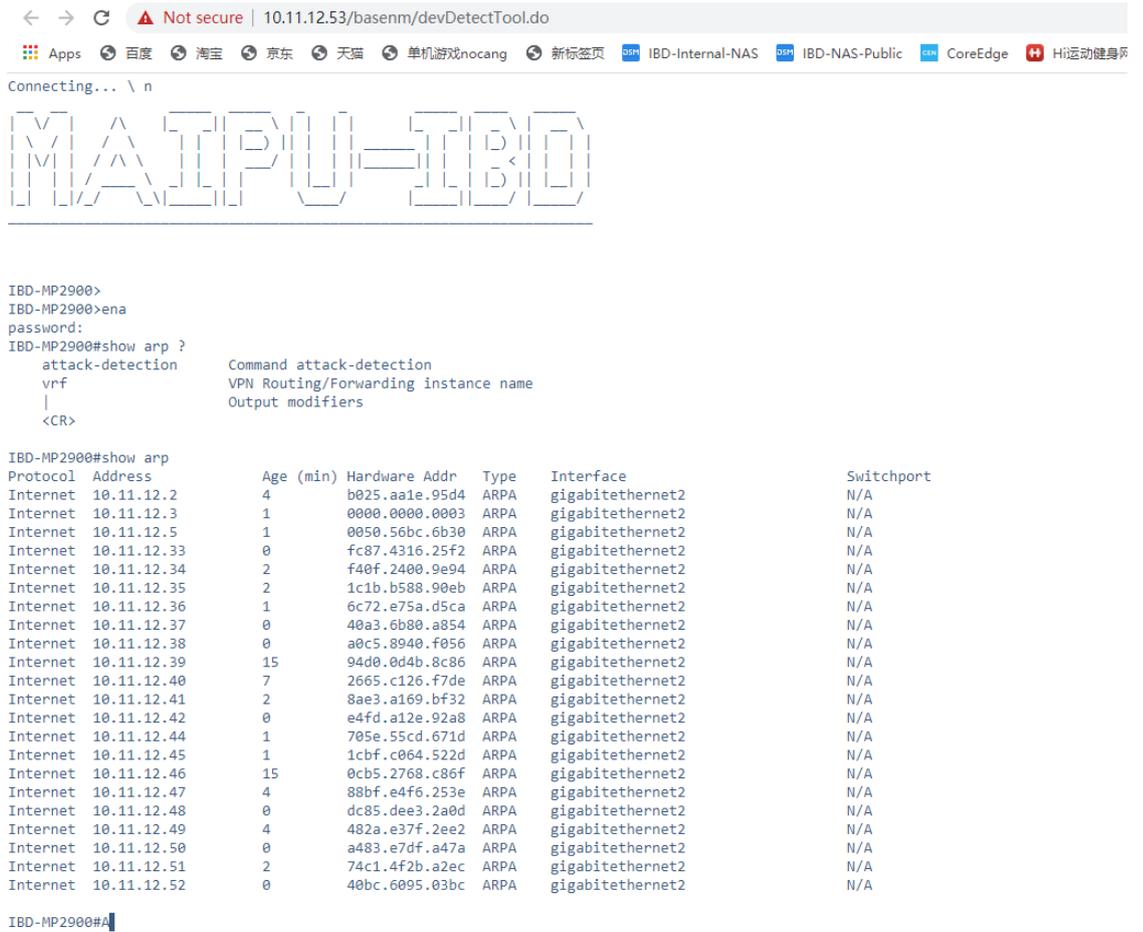


Figure 3-28 ssh connection interface

### 3.1.2. Device Details

Click the device name/IP/alias of any device information in the device list to enter the device details page, as shown in Figure 3-29 Device Details. The terminal device cannot view the device details.

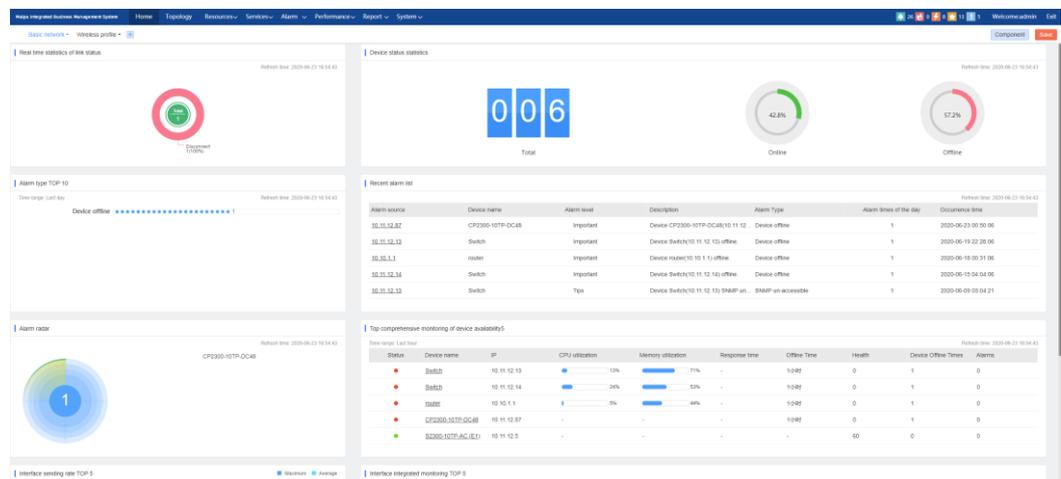


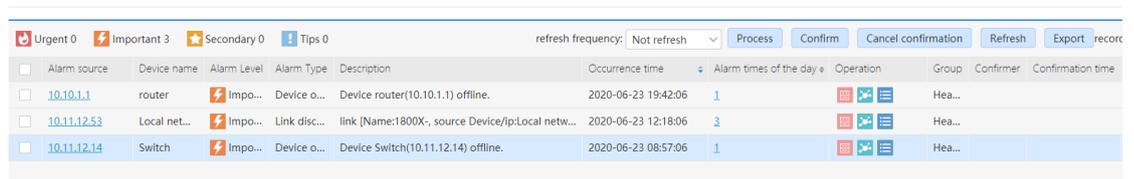
Figure 3-29 Device details

### 3.1.2.1. Basic Information

Basic information paging includes device status, alarms, performance indexes exceeding threshold, interfaces with high bandwidth utilization, device name, alias, IP, MAC, model, manufacturer, etc (System Oid, contact, location, system description information are not displayed by default, and can be seen by clicking the expand icon), as well as device health, CPU utilization, memory utilization, response time, temperature, power supply, fan, etc.

### 3.1.2.2. Alarm Information

The alarm information page displays all the unprocessed alarm information of the device, as shown in the figure below, and supports query and filtering through alarm level, confirmation status, alarm time, alarm type or filter template, etc.

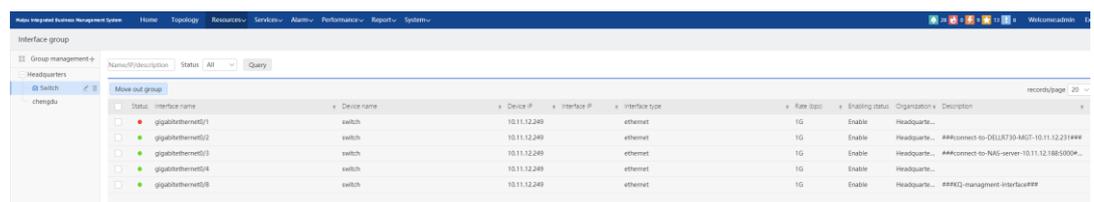


Alarm source	Device name	Alarm Level	Alarm Type	Description	Occurrence time	Alarm times of the day	Operation	Group	Confirmer	Confirmation time
<input type="checkbox"/>	10.10.1.1	router	Impo...	Device o...	Device router(10.10.1.1) offline.	2020-06-23 19:42:06	1			Hea...
<input type="checkbox"/>	10.11.12.53	Local net...	Impo...	Link disc...	link [Name:1800X-, source Device/ip:Local netw...	2020-06-23 12:18:06	3			Hea...
<input type="checkbox"/>	10.11.12.14	Switch	Impo...	Device o...	Device Switch(10.11.12.14) offline.	2020-06-23 08:57:06	1			Hea...

Figure 3-30 Device alarm details

### 3.1.2.3. Interface Information

Interface information page supports displaying all interfaces of the device, as shown in the figure below. The interface also supports querying and filtering the interface information by interface name, interface IP, interface description and link status.



Status	Interface name	Device name	Device IP	Interface IP	Interface type	Rate base	Enabling status	Organization	Description
<input type="checkbox"/>	gigabitethernet0/1	switch	10.11.12.249		ethernet	10	Enable	Headquar...	
<input type="checkbox"/>	gigabitethernet0/2	switch	10.11.12.249		ethernet	10	Enable	Headquar...	###connect to DELL730-MC2-10.11.12.231###
<input type="checkbox"/>	gigabitethernet0/3	switch	10.11.12.249		ethernet	10	Enable	Headquar...	###connect to NAC-server-10.11.12.19850004...
<input type="checkbox"/>	gigabitethernet0/4	switch	10.11.12.249		ethernet	10	Enable	Headquar...	
<input type="checkbox"/>	gigabitethernet0/8	switch	10.11.12.249		ethernet	10	Enable	Headquar...	###MQ-management-interfaces

Figure 3-31 Device interface list

Click "Batch set bandwidth" to pop up the bandwidth setting pop-up box, as shown in the figure below. Select the interface, set the egress bandwidth and ingress bandwidth, and select the unit. Click the "OK" button to set successfully. The set bandwidth and bandwidth utilization value can be displayed through the tips information by putting the mouse on the bandwidth utilization display bar.

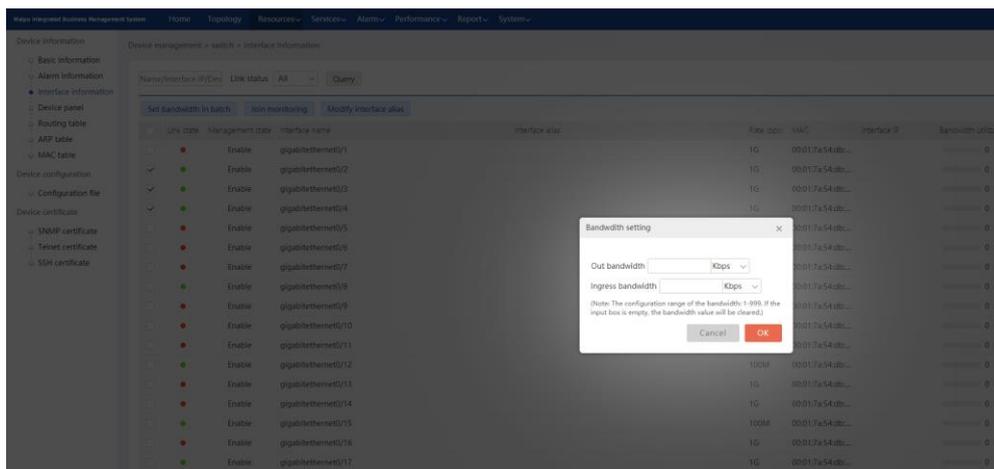


Figure 3-32 Device interface bandwidth configuration

Click the “Add to monitoring” button to add the selected interface to the interface monitoring, as shown in the figure below.

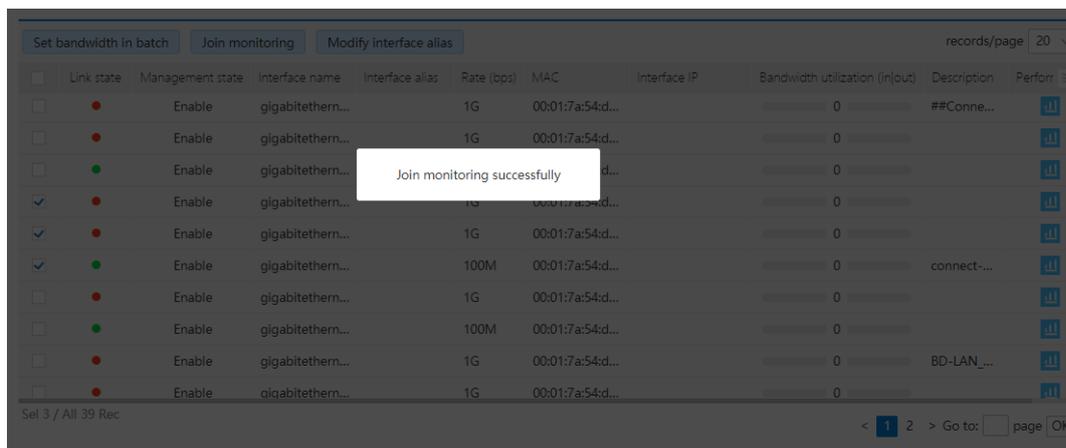


Figure 3-33 Add device interface to monitoring

Click  to modify the name of the selected interface, as shown in the figure below.

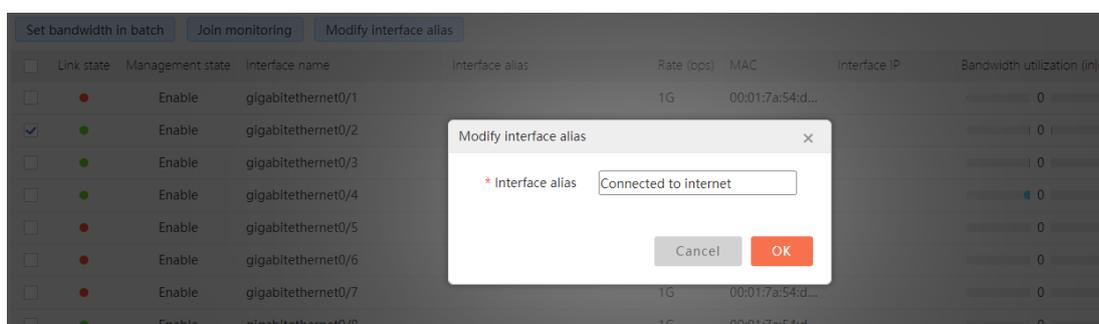


Figure 3-34 Modify device interface alias

Click the icon  in the "performance" column to jump to the corresponding monitoring

page, as shown in the figure below.

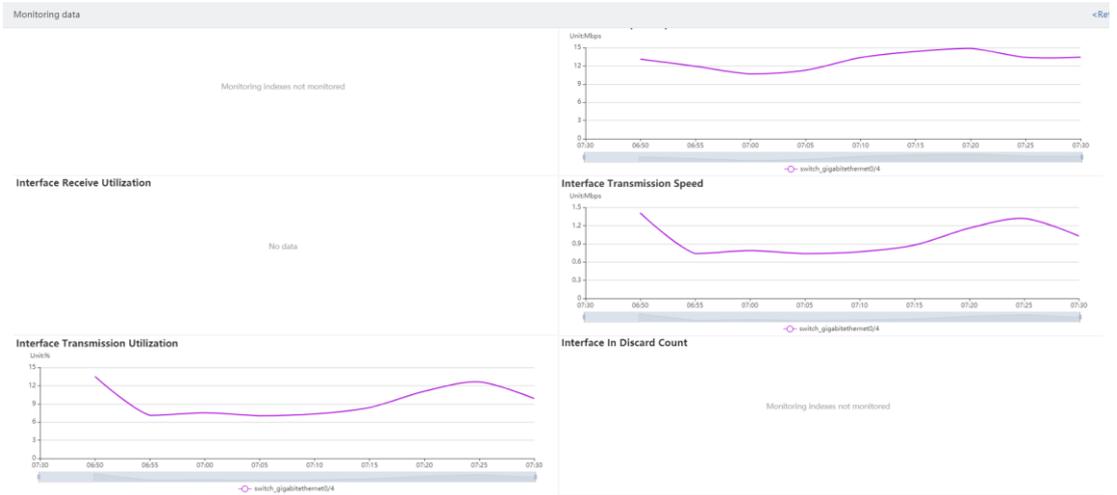


Figure 3-35 View the monitoring data of the device interface

### 3.1.2.4. Route Table

All routes of the device are displayed in the page of the route table, as shown in the figure below, and support querying and filtering by destination address, route type, and route protocol.

The screenshot shows the 'Device route table' in the Maipu Integrated Business Management System. The table contains the following data:

Destination subnet	Destination mask	Route egress interface	Route metric	Next-hop address	Routing type
0.0.0.0	0.0.0.0	vlan100	100	10.11.12.254	indirect
10.10.10.0	255.255.255.0	vlan10	0	0.0.0.0	direct
10.11.11.0	255.255.255.0	vlan1111	0	0.0.0.0	direct
10.11.12.0	255.255.255.0	vlan100	0	0.0.0.0	direct
10.37.0.0	255.255.0.0	vlan37	0	0.0.0.0	direct
99.99.99.0	255.255.255.0	vlan990	0	0.0.0.0	direct
127.0.0.0	255.0.0.0		0	0.0.0.0	direct
172.16.100.0	255.255.255.128	vlan999	0	0.0.0.0	direct
172.16.192.0	255.255.255.0	vlan192	0	0.0.0.0	direct
192.168.11.0	255.255.255.0	vlan100	0	0.0.0.0	direct
192.168.111.0	255.255.255.240	vlan100	0	0.0.0.0	direct

Figure 3-36 Device route table information

### 3.1.2.5. ARP Table

ARP table page displays the ARP table information of the device, as shown in the figure below, and supports querying and filtering by interface name, MAC address, IP address and type

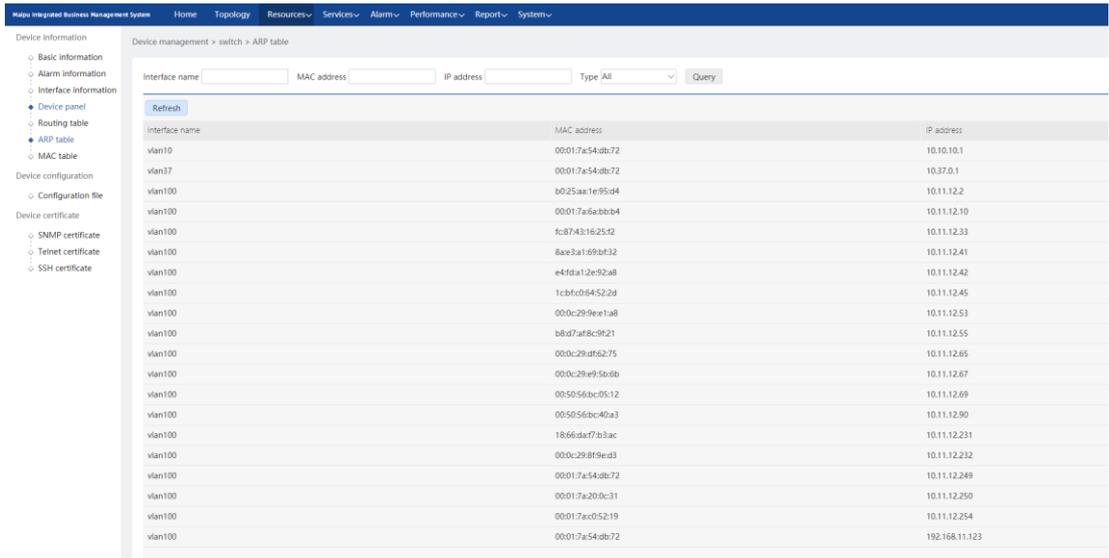


Figure 3-37 Device ARP table information

### 3.1.2.6. MAC Table

The MAC table page displays the MAC table information of the device, as shown in the figure below, and supports querying and filtering by VLAN ID, MAC address, interface name, and status.

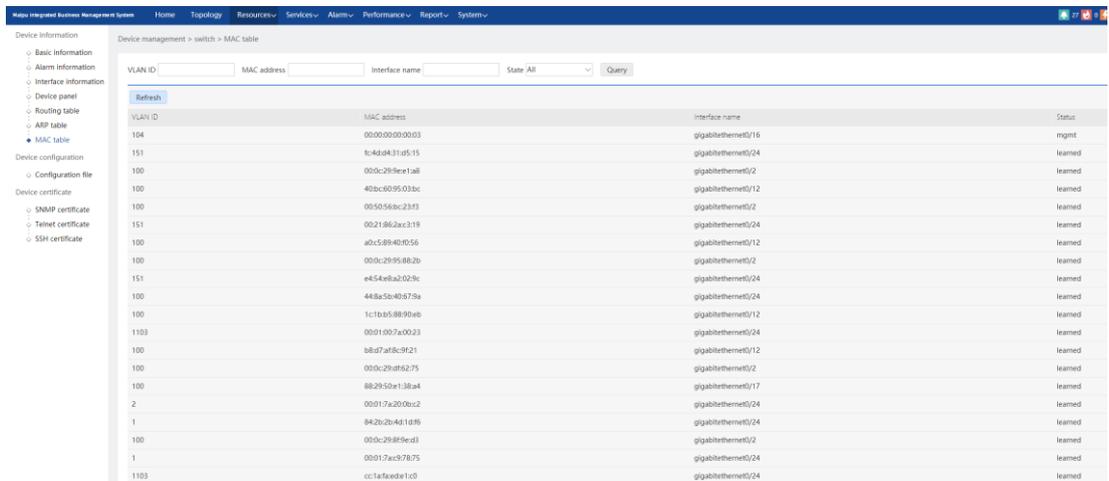


Figure 3-38 Device MAC table information

### 3.1.2.7. Configuration File

The configuration file page displays all configuration files distributed on the device, as shown in the following figure:

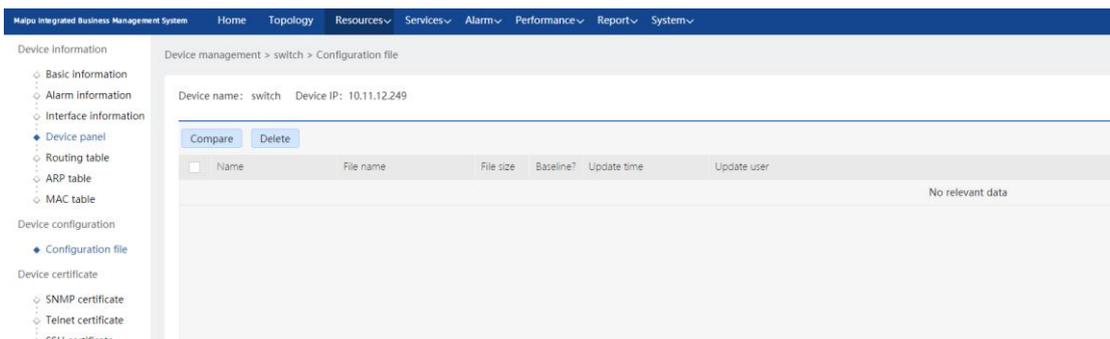


Figure 3-39 Device configuration file list

Click the icon  in the operation column to modify the configuration file, click the icon  to download the configuration file, click  to set whether the file is a baseline file, select two configuration files, and click the “Compare” button to display the configuration file comparison page, as shown in the following figure.

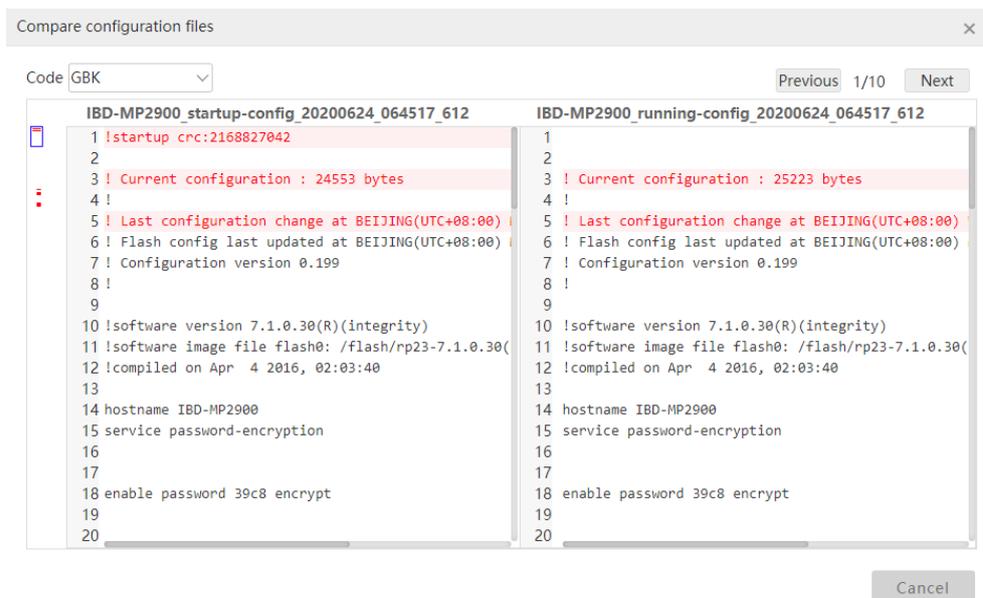


Figure 3-40 Compare configuration files

### 3.1.2.8. Device Certificate

SNMP certificate/telnet certificate/SSH certificate can display the certificate information configured by the current device and support modifying the corresponding certificate of the device, as shown in the following figure:

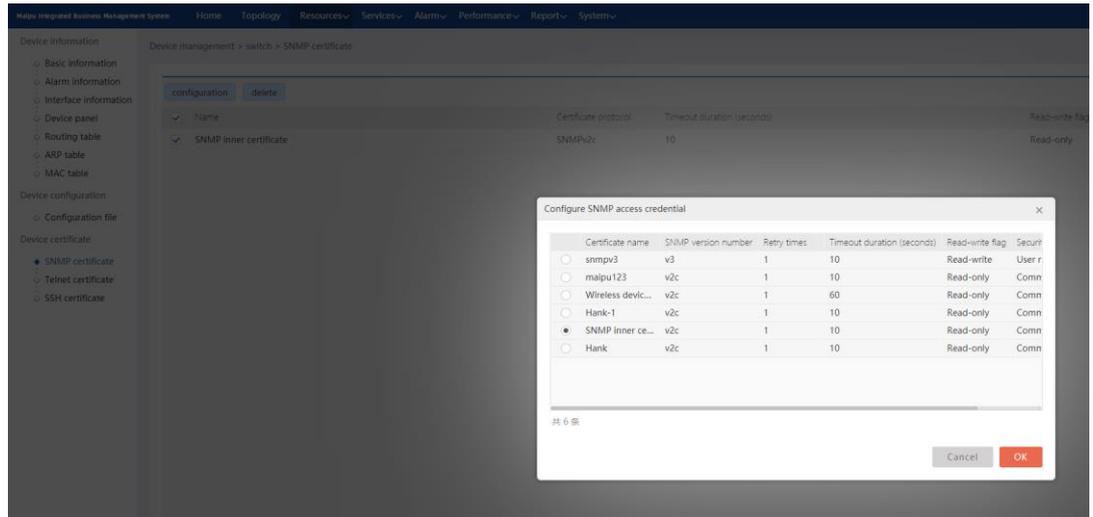


Figure 3-41 Device certificate configuration

Click the "Connection detection" link at the right side of the certificate list to check whether the corresponding certificate is available for the device.

**Note**

- When modifying the device certificate, only the certificate of the organization to which the device belongs is displayed in the optional certificate list.

### 3.1.2.9. Device Panel

The logic panel of the device is used to present the panel information of the device, mainly the interface information and board information of the device

Click the device name/device alias/IP address of any device information in the device list to enter the device details page, and then click the "Device panel" on the left to view the logical panel information of the device, as shown in the following figure:

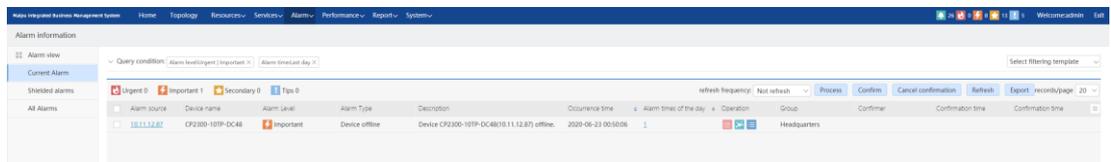


Figure 3-42 Device panel entrance 1

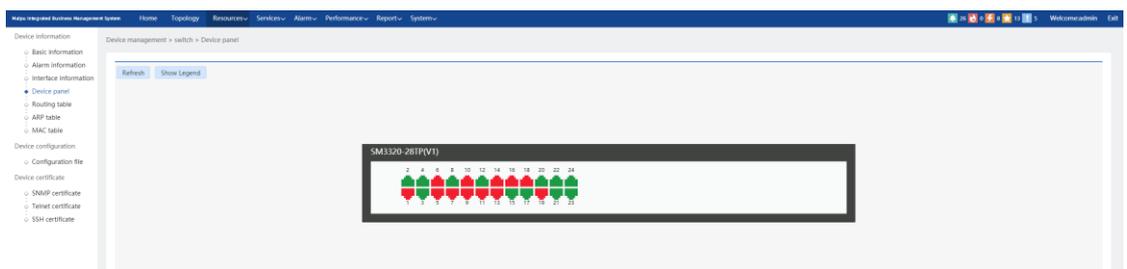


Figure 3-43 Device panel

Or click "Topology" in the menu bar at the top of the system to enter the topology management page, then select a device, and right-click to view the logical panel of the corresponding device, as shown in the following figure:

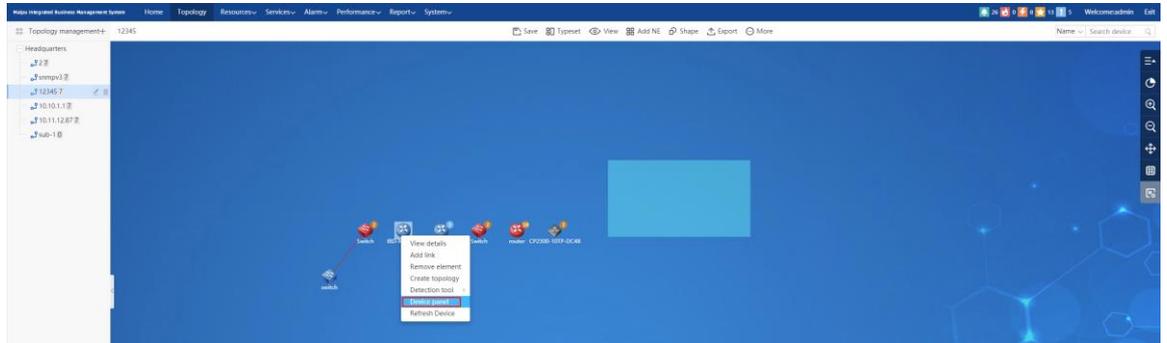


Figure 3-44 Device panel entrance 2

### Display legend

Click the "Show legend" button in the upper left corner of the device panel page to display the legend information in the upper right corner of the page, as shown in the following figure:

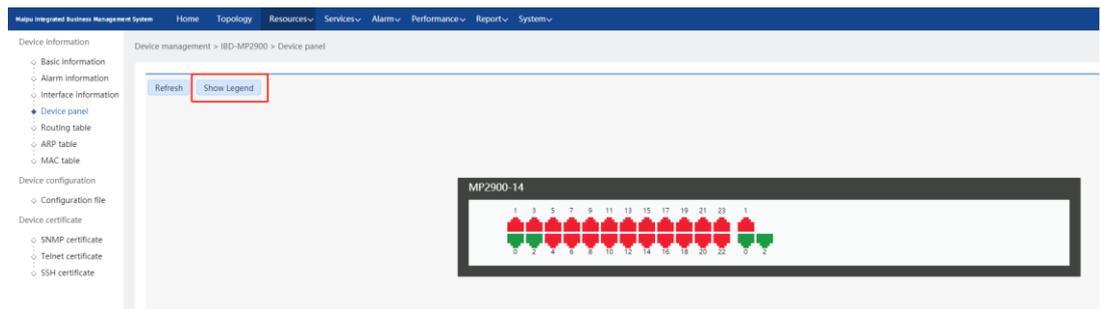


Figure 3-45 Display legend

### Interface

There are three states of the interface, which are represented by three colors: green, gray and red. Gray indicates that the management status is disabled, and red and green indicate the enabled state. Among them, green indicates that the link status is up, and red indicates that the link status is down. The device panel will automatically refresh every minute to obtain the latest interface status, as shown in the following figure:

Disabled state:

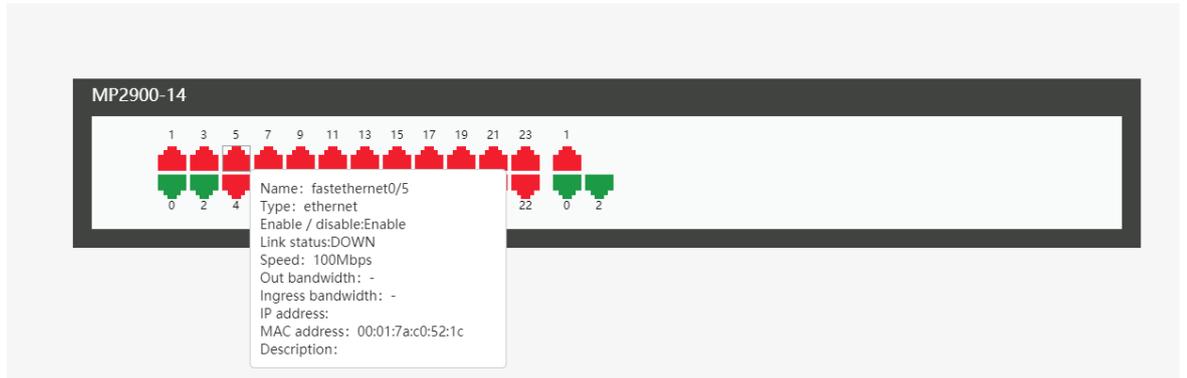


Figure 3-46 The disabled state of the interface

Enabled state and link status is UP:

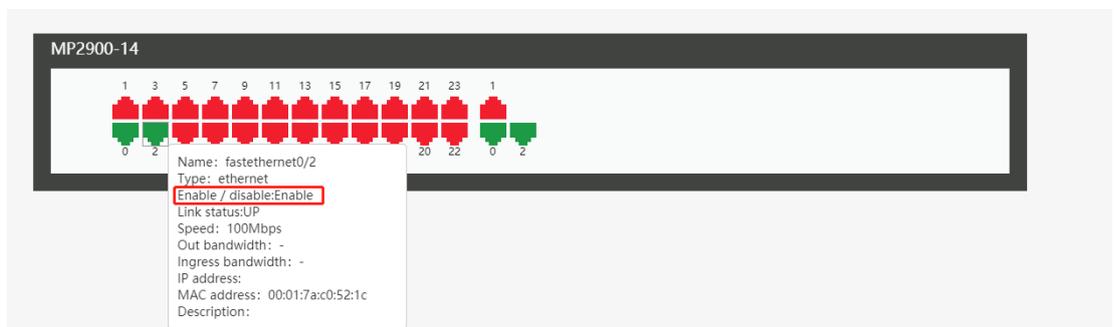


Figure 3-47 The UP state of the interface

Enabled state and link status is DOWN:

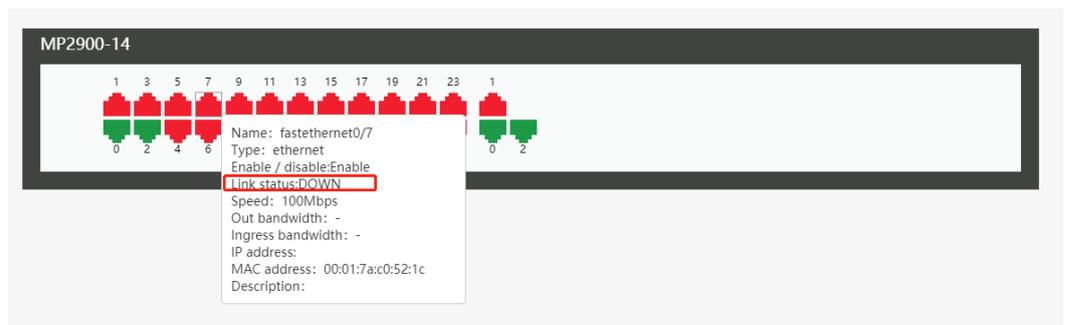


Figure 3-48 Interface DOWN state

Move the mouse to the interface, and right-click to enable or disable the interface. To enable or disable the interface, you need to configure the correct SNMP certificate with read-write authority, as shown in the figure below

After the interface is disabled, the interface status changes to disabled state and turns to gray.

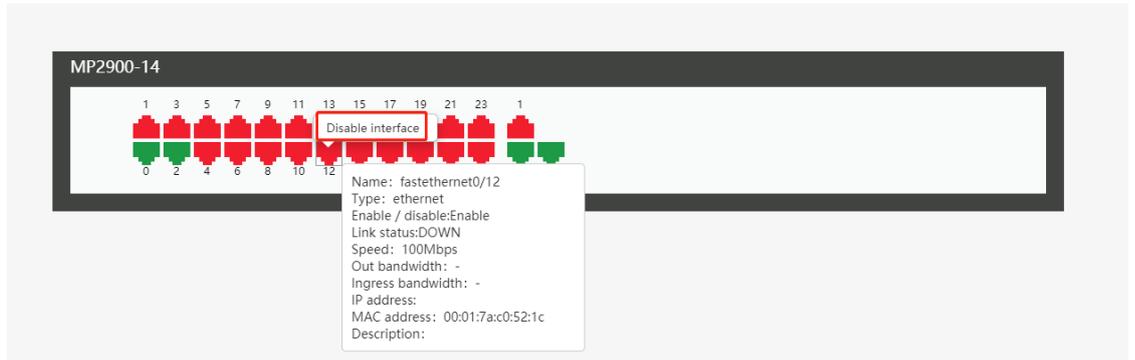


Figure 3-49 Disable interface



Figure 3-50 Confirm disabling interface

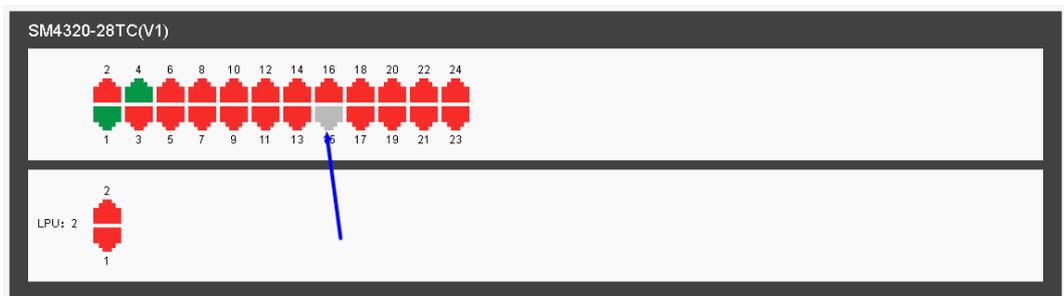


Figure 3-51 Disable the interface successfully

After enabling the interface successfully, the interface turns to the previous state.

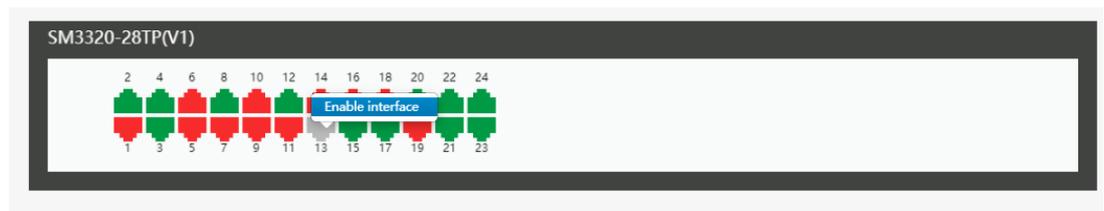


Figure 3-52 Enable the interface

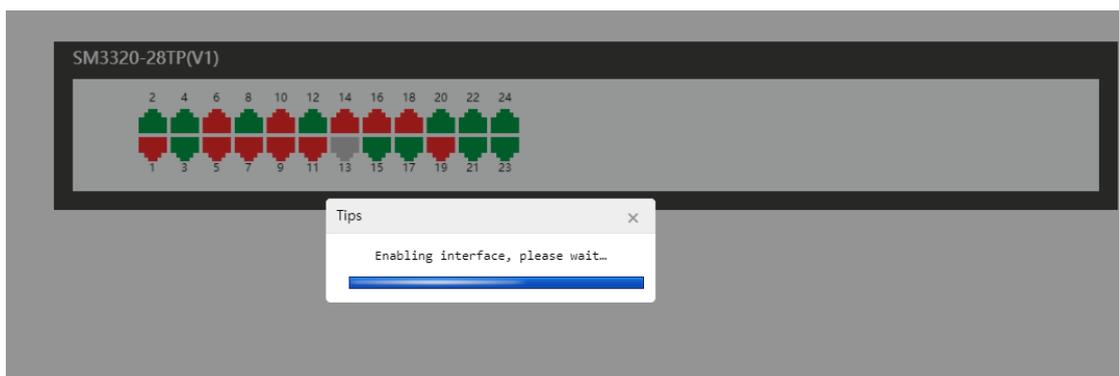


Figure 3-53 Enabling the interface

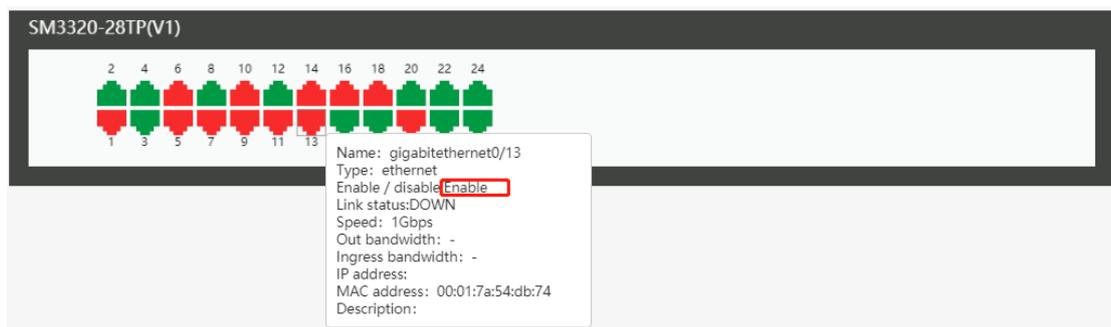


Figure 3-54 Enable the interface successfully

## Note

- To enable or disable the interface, you need to configure the correct SNMP certificate with read-write authority.
- If the interface is disabled, all services related to this interface will be interrupted
- If the device is offline, you cannot enable or disable the interface.
- To enable or disable the interface, you need to refresh the device. If the network has delay or the device route is long, it will take a long time to enable or disable the interface.

## Refresh

Click the “Refresh” button in the upper left corner of the device panel page to perform the network discovery for the device again, and obtain the latest information of the device, and then the panel will display the latest device information. If you want to swap the board, you need to click the “Refresh” button to perform the network discovery for the device again. After that, the latest device information will be displayed on the panel, as shown in the figure below:

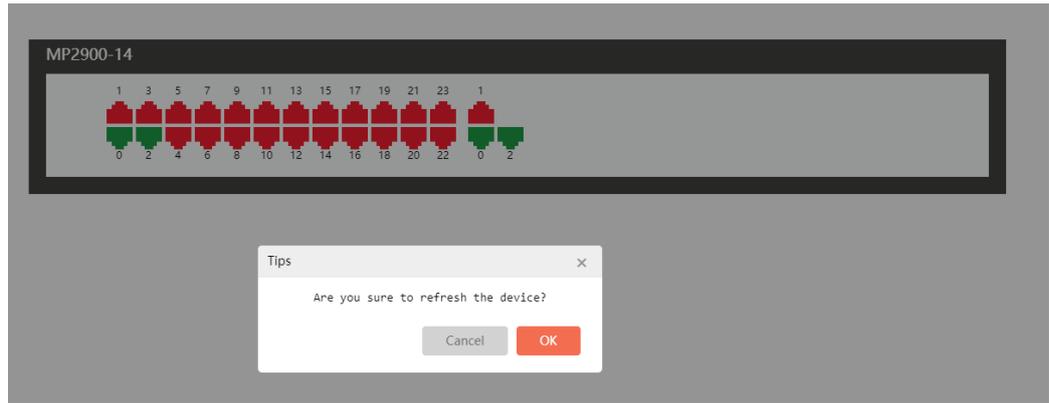


Figure 3-55 Refresh the device panel

 **Note**

- To swap the board, you need to refresh the device so that the latest panel information can be displayed.

**Tips Information of Whole Device**

The model information of the device will be displayed in the upper left corner of the device panel. If it is not displayed, you need to add it in the "Resource" -> "Device Type Management" menu bar at the top of the system, as shown in the following figure:

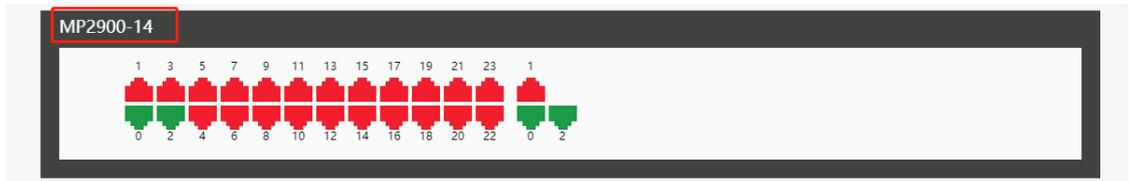


Figure 3-56 Device Model

Move the mouse to the model area at the top of the device panel to pop up the tips information of the whole device. Move the mouse out of the area and the tips information will disappear. Tips of non-stacking devices mainly display the following contents: manufacturer, name (display the alias first, if the alias is not set, display the name of the device itself), IP, status, model, software version, hardware version, device serial number, etc.; besides the above information for stacked devices, the master device adds the display of MemberID and role information, while the Member device only displays the MemberID and Role information;

As shown in the figure below:

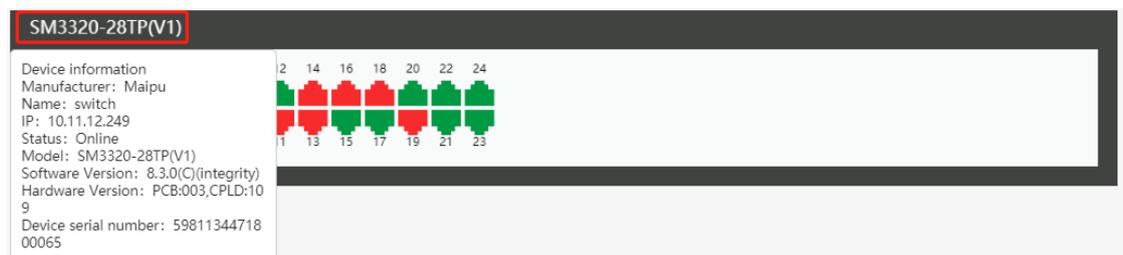


Figure 3-57 The tips information of the non-stacking device

**Interface Tips information:**

Move the mouse to the interface to pop up the tips information of the interface. The interface tips information includes: interface name (display alias first; if alias is not set, display device name), type, enable/disable, link status, rate, ingress/egress bandwidth, IP address, MAC address and interface description, as shown in the figure below:

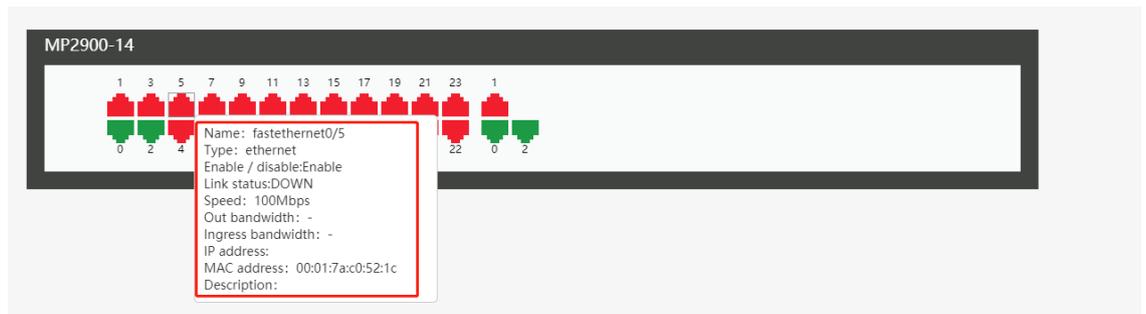


Figure 3-58 Interface tips information

**Logical Panel of Maipu Box Device**

If there is a DC0 port in the box switch, DC0 is displayed on the far left of the panel. If there is a small card, the small card and the interface on the small card will also be displayed; if there is a logical interface on the small card or there is no interface on the small card, only the board card information will be displayed, and the interfaces with different rates will be displayed separately.

The situation without small card is shown in the following figure:

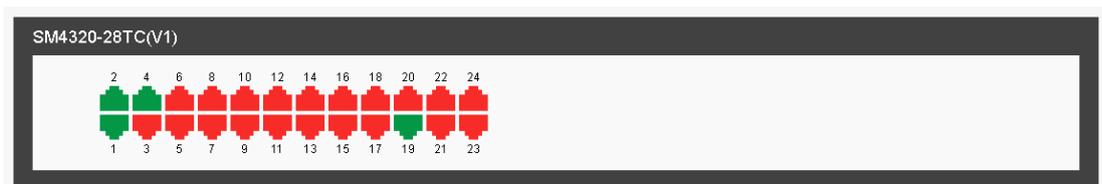


Figure 3-59 Box switch without small card

The situation with DC0 port is shown in the following figure:

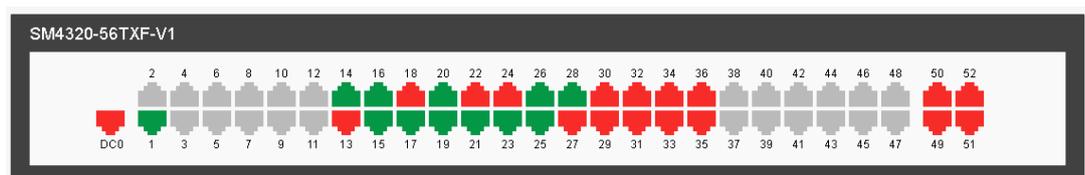


Figure 3-60 DC0 interface of the box switch

The situation with the small card is shown in the following figure:

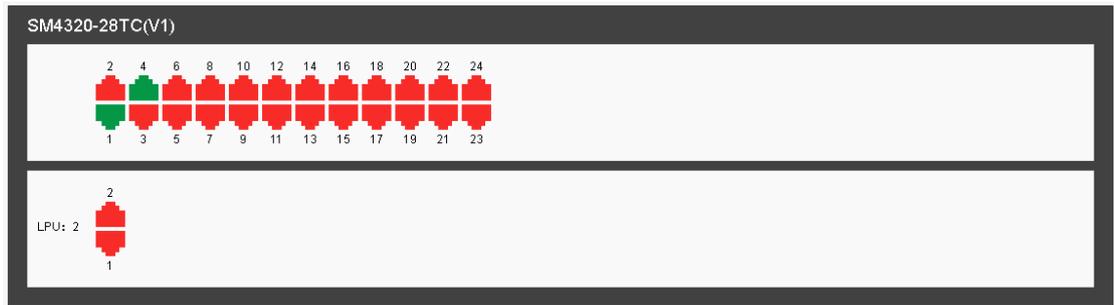


Figure 3-61 Box switch with the small card

For the box router, the first row displays the interfaces on the panel, WAN port and LAN port are displayed separately, and the second row displays the small card on the backplane and the interface information on the small card. If there is no interface on the small card or there is a logical interface on the small card, only board card message is displayed.

If the sub card of the MPU card of the box device has no interface, the sub card will not be displayed.

The box router is shown in the following figure:



Figure 3-62 Box router

The WAN port and LAN port are displayed separately, as shown in the following figure:

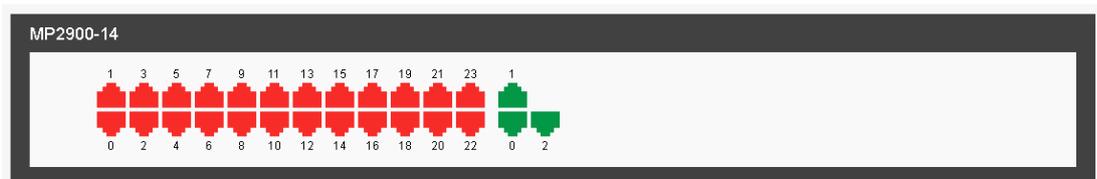


Figure 3-63 Interfaces of box router are displayed separately

The box router with the small card is shown in the following figure:



Figure 3-64 Box router with small card

There is no interface on the small card or there is logical interface on the small card, as shown in the following figure:



Figure 3-65 Box router without interface on the small card

The box device will display the name of the board card and the slot number where the board is located on the left side of each card. The slot number is displayed in the format of card type: slot index. The MPU card of the box device does not display the card name and slot number. Some devices do not have the card name, as shown in the following figure:



Figure 3-66 Card name and slot number of the box device

### Note

- The MPU card of the box device does not display the board name and card index.
- Some boards have no board name.

### Logical Panel of Maipu Frame Device

For medium and high-end switches, the card slots are displayed in the order of MPU, LPU and SFU; DC0 port is displayed on the main MPU board card; each row displays the board card information and the interface on the board card, the card name and slot number are displayed on the left side of the board card, and the interface on the board card is displayed on the right side, and the interfaces are displayed in different regions according to different rates; the switch does not display sub cards.



Figure 3-67 Frame switch

### Note

- Some boards have no board name.
- If there is no interface on the board, only board information will be displayed.
- The switch does not display the sub card.

For the medium/high-end router, the display order of the cards is: MPU, LPU, sub card, SFU; Each row displays two sub cards, arranged from left to right, from top to bottom. The left side of the card displays the card name and slot number of the card, and the right side displays the interfaces on the card. The interfaces are displayed in different regions according to different rates.

As shown in the figure below:

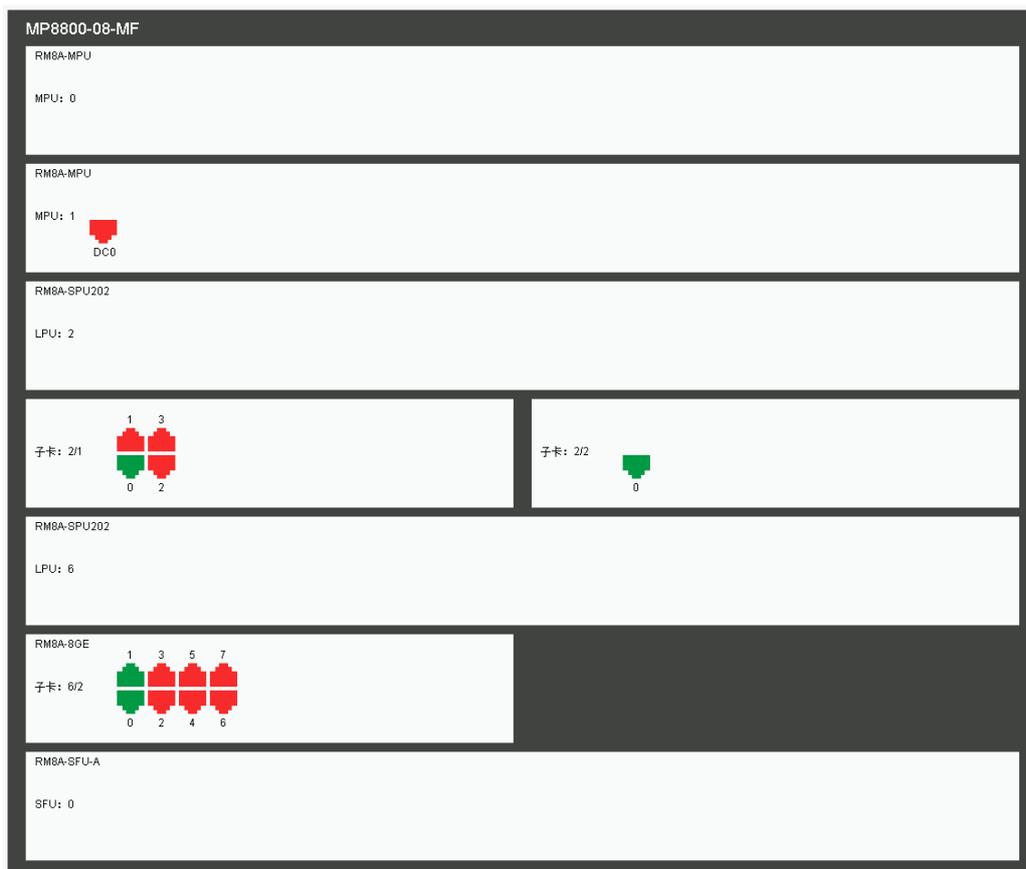


Figure 3-68 Frame router

### Note

- Some boards have no board name
- If there is no interface on the board, only board information will be displayed
- If there is a logical interface on the sub card, only the sub card information will be displayed, and the logical interface will not be displayed

### Logical Panel of Maipu Stacking Device

Each member device of the stacking device is displayed according to a single device, the master device is displayed in the first place, and the member device is displayed according to the member number. The device model is displayed in the upper left corner of each device, and the stacking member information is displayed in the upper right corner, as shown in the following figure:

Box stacking:

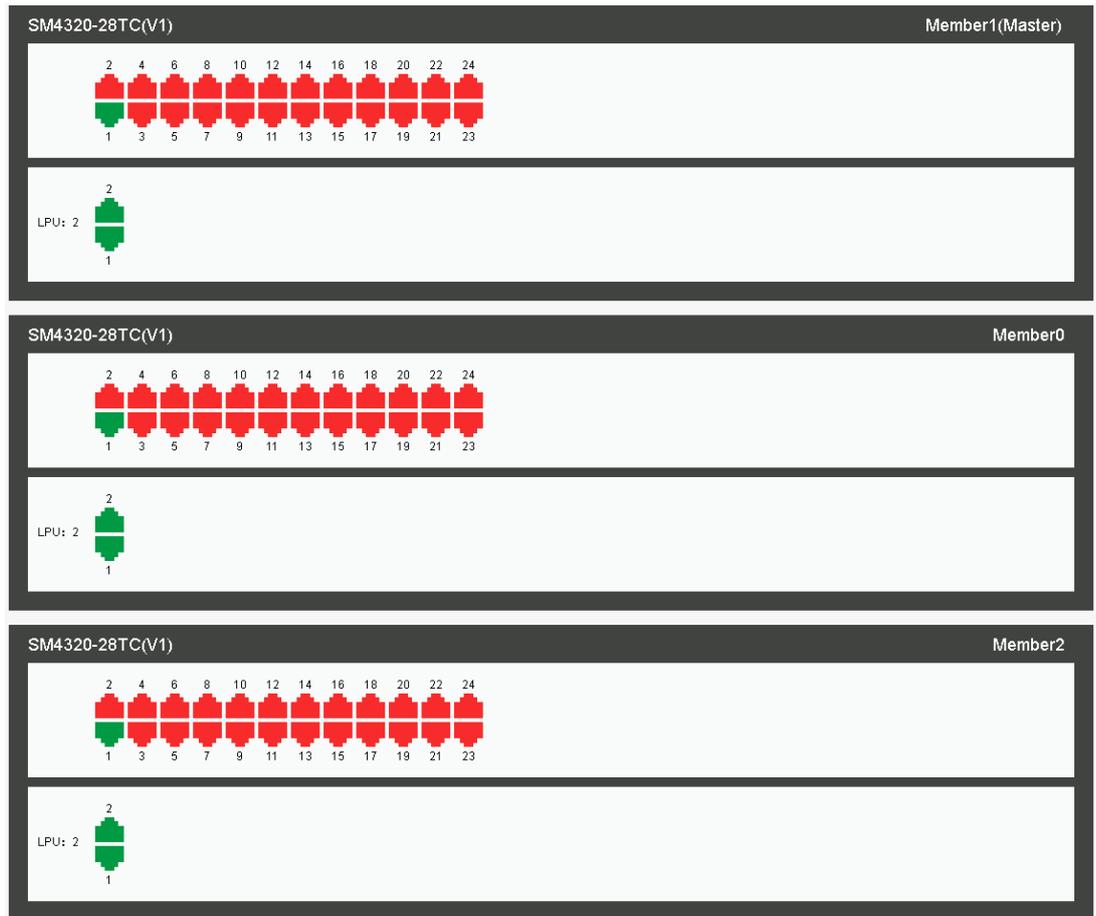


Figure 3-69 Box stacking

Frame stacking:



Figure 3-70 Frame stacking

### Logical panels of other manufacturers' devices

The device panels of the devices of the friendly manufacturer are displayed in different regions according to the interface name rules: one dimensional interface is displayed on a logical board, and two-dimensional and three-dimensional interfaces are displayed in different regions according to the first digit of the interface name. For example, 0/0, 0/1, 0/0/1 will be

displayed on a logical board, 1/0, 1/1, 1/1/0 is displayed on a board, and the four-dimensional interfaces are displayed in different regions according to the first two digits of the interface name; each row displays 16 interfaces and displays the complete number of the interface; as shown in the figure below:

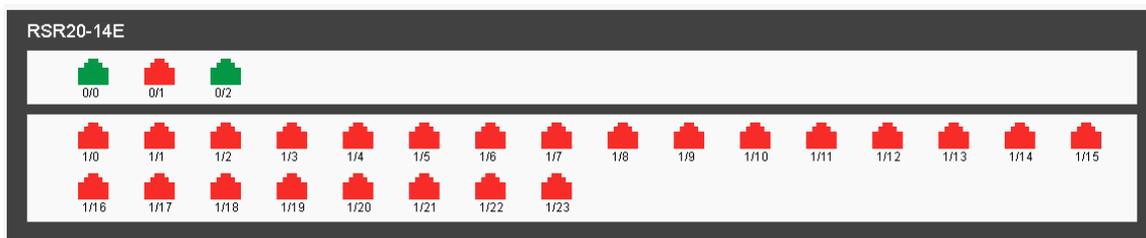


Figure 3-71 Friend manufacturer's device panel

### Note

- The board card of the device panel of the friend manufacturer is a logic board, so the name and slot number of the board are not displayed
- If the device model of the friend manufacturer is not configured in "Resource" -> "Device Type Management", the unknown model will be displayed in the upper left corner of the panel, which needs to be added in "Device Type Management".

As for abnormal display of the panel:

### Note

- If the device model in the upper left corner of the device panel is not displayed or "unknown model" is displayed, it needs to be added in "Resource" -> "Device Type Management".
- If the system is installed by version upgrade, the panel display of some devices may not be correct. For example, the sub card cannot be displayed and the interface on the sub card is displayed on other sub cards. In this case, you need to click the "Refresh" button on the panel to refresh the panel; or refresh the device in "Resources" -> "Device Management", and then enter the device panel.

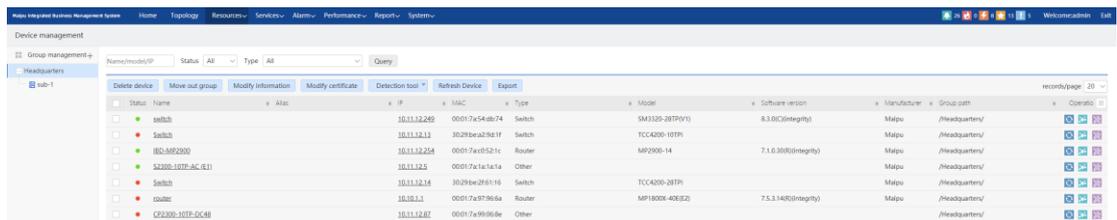
## 3.2. Device Type Management

Click "Resource Management" -> "Device Type Management" in the navigation bar at the top of the system to open the "Device Type Management" interface. The module includes device model management and device category management. The model, manufacturer information and icon display information of different states (down and up) of a device are set in this module. The module has built-in model information of some devices of Maipu. The device

models of other manufacturers need to be added manually.

### 3.2.1. Device Type Management

Open the device type management module, and click the "Device Category Management" tab to display the device category management interface, as shown in the following figure. The device categories of Maipu and other manufacturers are built in the device model tree on the left. Users can view, edit, and delete these device categories. Users can add device category information of other manufacturers.



Status	Name	alias	IP	MAC	Type	Model	Software version	Manufacturer	Group path	Control
●	switch		10.11.1.2.269	00017a54eb74	Switch	SM3326-28TP(V1)	8.3.0(C)Integrity	Maipu	/Headquarters/	⊞ ⊞ ⊞
●	switch		10.11.1.2.13	3029bea29e1f	Switch	TCC4200-10TP		Maipu	/Headquarters/	⊞ ⊞ ⊞
●	RD-MP2900		10.11.1.2.254	00017ac0527c	Router	MP2900-14	7.1.0.3083(Integrity)	Maipu	/Headquarters/	⊞ ⊞ ⊞
●	S2300-10TP-SC-RL1		10.11.1.2.5	00017a7a7a7a	Other			Maipu	/Headquarters/	⊞ ⊞ ⊞
●	switch		10.11.1.2.14	3029be2f6116	Switch	TCC4200-28TP		Maipu	/Headquarters/	⊞ ⊞ ⊞
●	router		10.10.1.1	00017a97966a	Router	MP1800X-40E(S2)	7.5.1.1463(Integrity)	Maipu	/Headquarters/	⊞ ⊞ ⊞
●	CP2300-10TP-SC-48		10.11.1.2.87	00017a99968e	Other			Maipu	/Headquarters/	⊞ ⊞ ⊞

Figure 3-72 Device type management

#### Add/edit/delete device model:

Click the "Add" button at the top of the device category list to open the add device category dialog box. You need to fill in the category name, manufacturer ID, device icon and description fields, which are optional fields and can be left blank.

The default display of the parent is "Device Model Management", which cannot be modified by the user. The system thinks that the user wants to add a piece of manufacturer information, so there is a manufacturer ID field in the "Add device category" dialog box, as shown in Figure 3-73, add a piece of manufacturer A information. Fill in the fields in the dialog box correctly and click the "OK" button to add successfully.

The effect after filling in the series products of manufacturer A in turn is shown in Figure 3-74.

In the device model management, select a category, click "Modify" at the top of the device category list to modify the device category. Click "Delete" at the top of the device category list to delete the device category. After deleting the device category, all the subcategories and device model information under the category will be deleted at the same time.

✕

### Add Device Type

\*Parent  \*

\*Device Model  \*System OID

Device Icon (Up)

Device Icon (Down)

Description

0/64 characters,you can input 64 characters!

Figure 3-73 Add/edit device category

SystemOID	Type	Query			
Add Modify Remove Import Export					
Vendor	Product Type	Product Series	SystemOID	Type	De
<input type="checkbox"/>	Maipu	Switch	1.3.6.1.4.1.5651.1.3745.0	TCC4200-28TPI	
<input type="checkbox"/>	Maipu	Switch	1.3.6.1.4.1.5651.1.3045.0	TCC4200-10TPI	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	SM4120-28TC-AC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	SM4120-28TC-DC48(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	SM4120-28TP-AC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	SM4120-28TP-DC48(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	SM4120-52TC-AC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	SM4120-52TC-DC48(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	SM4120-52TP-AC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	SM4120-52TP-DC48(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4120	MyPower SM4120-52TC-AC(R1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4220	SM4220-16GEF8GE-AC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4220	SM4220-24F-AC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4220	SM4220-28TP-AC(V2)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4220	SM4200-52TP-AC(V2)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4220	SM4220-28TC-AC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4220	SM4220-52TC-AC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4220	SM4220-52TC-AC(V2)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4220	SM4100-28TC(V2)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4320	SM4320-28FC(V1)	
<input type="checkbox"/>	Maipu	Switch	MyPower S4320	SM4320-28TC(V1)	

Figure 3-74 Product series of manufacturer

**Note**

- The device category name cannot be the same under the same category directory.
- The manufacturer ID exists in the sysoid of the device, which is an integer and cannot be repeated. Please check the correct manufacturer ID and fill it in.

### 3.2.2. Device Model Management

The device model management module provides the functions of adding/editing/deleting the specific device model in the device category. Meanwhile, it also supports the fuzzy query by the Sysoid of the device and device model. Both the topology module and the device list module query the device model, manufacturer, and the icons to be displayed in different states of the device through the device sysoid. If the status icon is not set in the found device model record, the status icon of its parent category will be used.

Open the device type management module, and the device model management interface will be displayed by default, as shown in the figure below. Click the device model tree on the left to display the device model information under the selected device category in the right list.

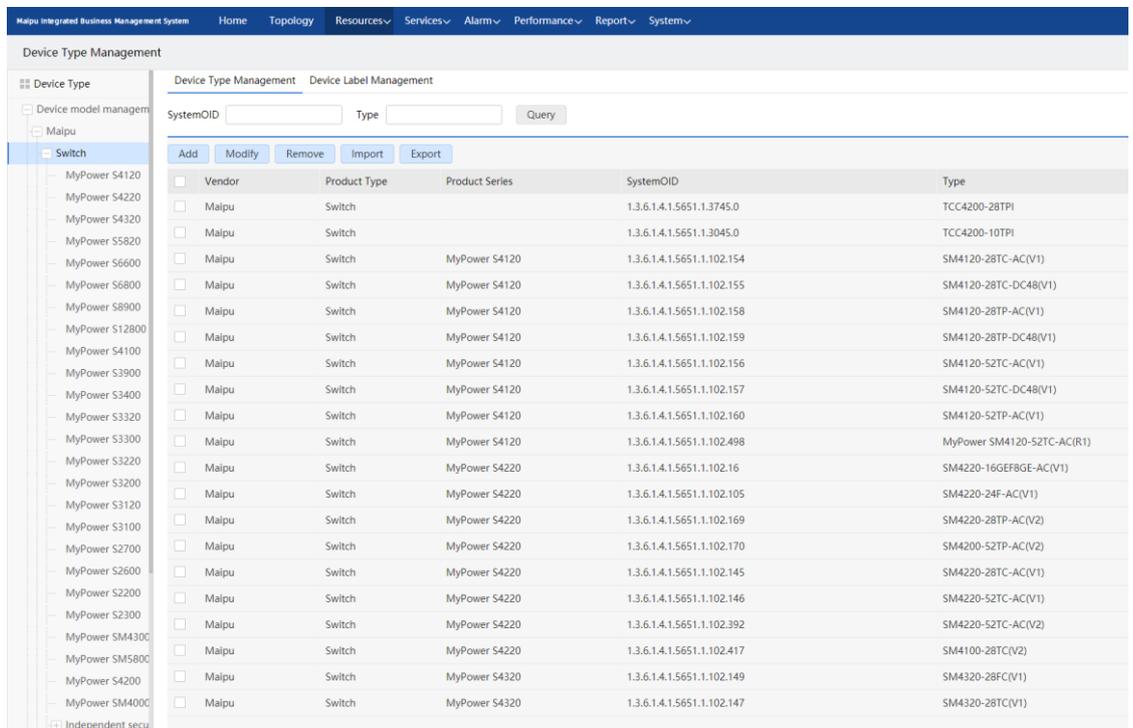


Figure 3-75 Device model management

#### Add/edit/delete device model:

First, select the manufacturer/category/product series in the left tree, and then click “Add” at the top of the device model list to open the add device model dialog box. The parent displays the manufacturer/category/product series in the tree on the left by default. You need to select the device type and fill in the device model and system oid. The device status icon and description fields are optional fields and can be left blank.

Select a certain device type, and then click “Modify” at the top of the device model list to modify the model category; click the “Delete” icon at the top of the device model list to delete the device model; click the “Import” button at the top of the device model list to import the model category; click the “Export” button at the top of the device model list to export the model

category. Select a device type and click the top of the device model list.

Modify Device Type

\*Parent  \*Device Ty...

\*Device Model  \*System OID

Device Icon (Up) 

Device Icon (Down) 

Description

Figure 3-76 Add/edit device model

### Note

- The device model name cannot be the same under the same category directory.
- The oid field of the device model system is globally unique, and cannot be repeated.
- The device category and model built in the network management system cannot be deleted.

## 3.3. Network Discovery

Click "Resource Management" -> "Network Discovery" in the navigation bar at the top of the system, and click "Network Device Discovery" to enter the corresponding interface. The module provides the search function for the network devices and security devices. Search for network or security devices that meet the requirements by creating different discovery tasks.

### 3.3.1. Network Device Discovery

Click "Resource Management" -> "Network Discovery" -> "Network Device Discovery" in the navigation bar at the top of the system to open the network device discovery page, as shown

below:

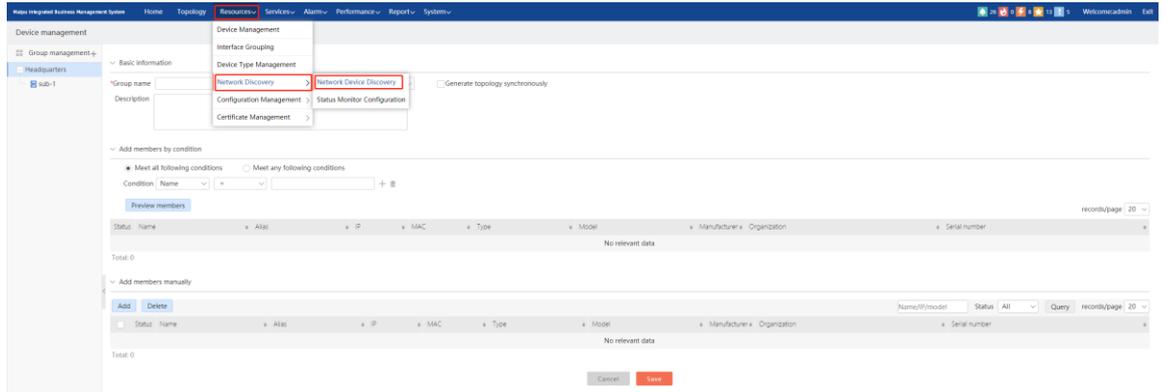


Figure 3-77 Network device discovery task

### Add discovery task

Click the "Add" button on the toolbar to open the "Add/Modify" window, as shown in the following figure. Input the task name, select the execution method (manual or auto), select the organization, enter the description, select whether to start immediately, whether to expand discovery, and whether to generate topology synchronously. Click the "Next" button to enter the next operation.

A screenshot of a dialog box titled 'Add' with a close button (X) in the top right corner. The dialog is divided into two steps: 'Step 1' (active) and 'Step 2'. Under 'Step 1', there are several input fields and options: a required '\*Task name' text box; 'Mode of execution' with radio buttons for 'Manual' (selected) and 'Auto'; a required '\*Organization' dropdown menu currently showing 'Headquarters'; a 'Description' text area; 'Start now' with a 'Yes' checkbox; 'Discovery' with checkboxes for 'Extended discovery' and '30-bit subnet interface interconnection'; and 'Topology options' with a checkbox for 'Generate topology synchronously'. At the bottom right of the dialog are 'Cancel' and 'Next step' buttons.

Figure 3-78 Add/modify discovery task–Step 1

---

 **Note**

- When "Auto" is selected as the execution mode, input the option "Scheduling frequency" (daily, weekly, or monthly). If "Daily" is selected as the scheduling frequency, there are "interval cycle", "interval minutes" (value range: 5-1440) and "scheduling time"; if "weekly" is selected as the tuning frequency, there are "scheduling date" (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday), and "Scheduling time"; if "Monthly" is selected as the scheduling frequency, there re "Scheduling date" (1st–31st) and "Scheduling time".
- The discovery option: "Extended discovery". After checking, other network devices connected to all interfaces of network devices will be discovered.
- 30-bit subnet interface interconnection: the IP addresses of the interfaces at both ends of the link are a pair of links with 30-bit subnet masks. When the device does not enable the LLDP function, some nonexistent links may be discovered based on the 30-bit subnet.
- Topology option: "Generate topology synchronously". After checking, a topology view will be created under the organization to which the discovery task belongs, and its type is physical view. (this option is only available when you add a discovery task).

---

Click the "Next" button to open the second step configuration window, as shown in the following figure: users can add, delete and import various network discovery certificate information. After inputting the correct certificate information, click the "Save" button to complete the "Add" operation.

Add
✕

1 Step 1
2 Step 2

\*Network discovery device...

\*Access certificate  Select

Add

---

Delete
Import
Template download

<input type="checkbox"/>	Device IP	Access certificate	Operation
Empty			

Sel 0 / All 0 Rec
< 1 >
Go to:  page Go

Advanced setting ▼

Cancel
Previous step
Save

Figure 3-79 Add/modify discovery task–Step 2

Extended advanced setting:

Advanced setting ▼

IP not involved in topology calculation

IP information

1) Multiple IPs can be added, separated by ','; 2) IP ranges can be added, separated by '-'

Figure 3-80 Add/modify discovery task–Step 2-Extended advanced setting

Users can input IP information that is not involved in the topology calculation, add multiple IP addresses separated by ',', or add IP ranges separated by '-'.

**Add IP and certificate information:**

Enter a single IP address or address segment in the "Network discovery device IP" input box, and click the select button of access certificate to pop up the "Add access certificate" selection box, as shown in the figure below. Switch the SNMP/telnet/SSH/security certificate tab to select different certificate types. After checking, click "OK" to complete the selection and close the selection dialog box.

Add access certificate
✕

SNMP certificate
TELNET certificate
SSH certificate
Security certificate

select	SNMP name	SNMP version number	Retry times	Timeout time	Read-write flag
<input type="radio"/>	SNMP inner certif...	v2c	1	10	Read-only
<input type="radio"/>	Wireless device S...	v2c	1	60	Read-only
<input type="radio"/>	snmpv3	v3	1	10	Read-write
<input type="radio"/>	maipu123	v2c	1	10	Read-only
<input type="radio"/>	Hank	v2c	1	10	Read-only
<input type="radio"/>	Hank-1	v2c	1	10	Read-only

Security device discovery cannot be performed without adding security device certificate

Cancel
OK

Figure 3-81 Add access certificate

## Note

- You can input more than one network discovery device IPs at a time, separated by ";", or enter the IP address range separated by "-";
- The SNMP, Telnet, SSH and security certificate are all single choice, and at least one SNMP needs to be selected; Telnet, SSH and security certificate are optional;
- When SSH certificate and telnet certificate are configured at the same time, SSH certificate has priority;
- Network discovery must be configured with security certificates to discover the information related to security devices and perform functions to view information, such as app cache, security device CPU, memory, disk, number of online users, etc.

### Delete IP and certificate information:

Check the table data under the "Delete" button, and click the "Delete" button to complete the deletion operation after confirmation prompt.

### Import IP and certificate information:

Users can batch import multiple IP addresses and corresponding certificate information through the Excel file. Click the "Import" button to open the "Import certificate information" file selection box, as shown in the figure below. After the user selects the local certificate file, click the "OK" button to complete the data importing.

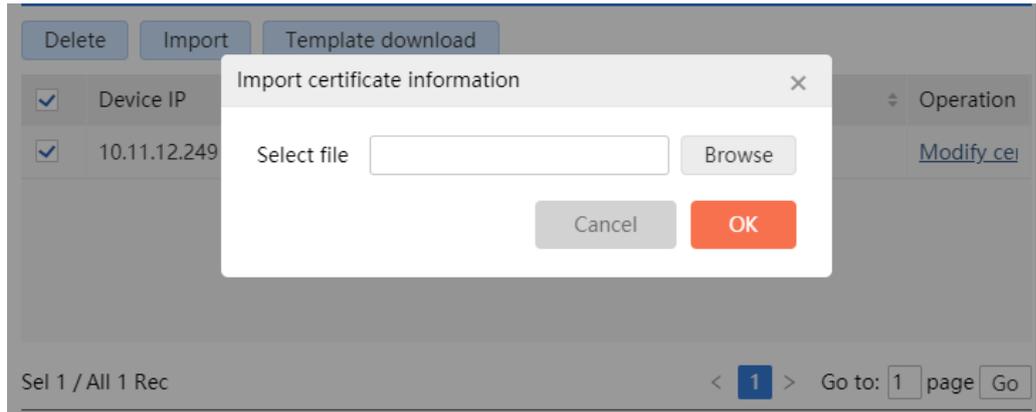


Figure 3-82 Import the certificate information

**Note**

- Please refer to the file format downloaded in "Template download" for Excel format.
- After the certificate is imported, the system will automatically match the template with the same parameters. If not, the corresponding template will be created automatically. The auto created templates can be configured in the "Template management" module.

**Template downloading:**

Click the "Template download" button, and select the file saving path to complete the downloading of the template file. The template file is shown in the figure below.

D	E
SSH Parameter	ISG Parameter
Port:22;Username: admin;Password:xxxxx;Enable Password:xxxxx;	Username: admin;Password:xxxxx;
Port:22;Username: admin;Password:xxxxx;Enable Password:xxxxx;	Username: admin;Password:xxxxx;

Figure 3-83 Download template

**Note**

- When the mouse stops at the title of the first line, the note information will pop up automatically.

**Modify discovery task**

Check the task information to be edited in the discovery task list, and click "Modify" to open

the window of adding/modifying the discovery task, as shown in the figure below. Follow the steps of "Add discovery task" to complete the modification of discovery task.

Modify

1 Step 1 2 Step 2

\*Task name 10.11.12.250

Mode of execution  Manual  Auto

\*Organization Headquarters

Description

Start now  Yes

Discovery  Extended discovery  30-bit subnet interface interconnection options

Cancel Next step

Figure 3-84 Modify discovery task

### Note

- Only one task information can be selected when modifying the discovery task.
- The started task cannot be modified.

### Delete discovery task

Check the task information to be deleted in the discovery task list (multiple selection is supported), and click the "Delete" button to open the confirmation dialog box for deleting the discovery task, as shown in the figure below. Click "OK" to confirm the deletion of the selected task information, and click "Cancel" to cancel the deletion.

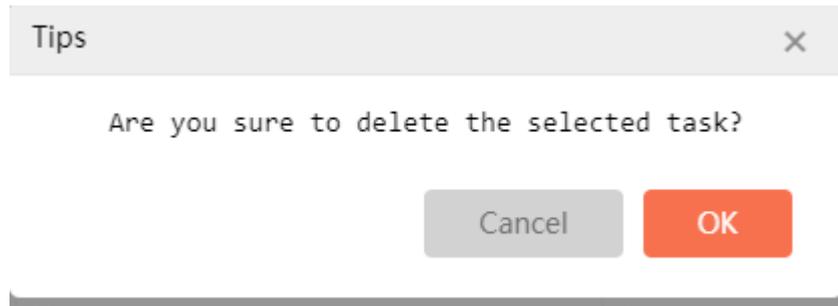


Figure 3-85 Delete the discovery task

---

**Note**

- The started task cannot be deleted.

**Start/Stop discovery task**

Check the task information to be started in the discovery task list (multiple selection is supported), and click the "Manual start" or "Stop" button to open the start (or stop) discovery task confirmation dialog box, as shown in the following figure. Click the "OK" button to confirm starting/stopping the selected task, and click the "Cancel" button to drop the start/stop operation.

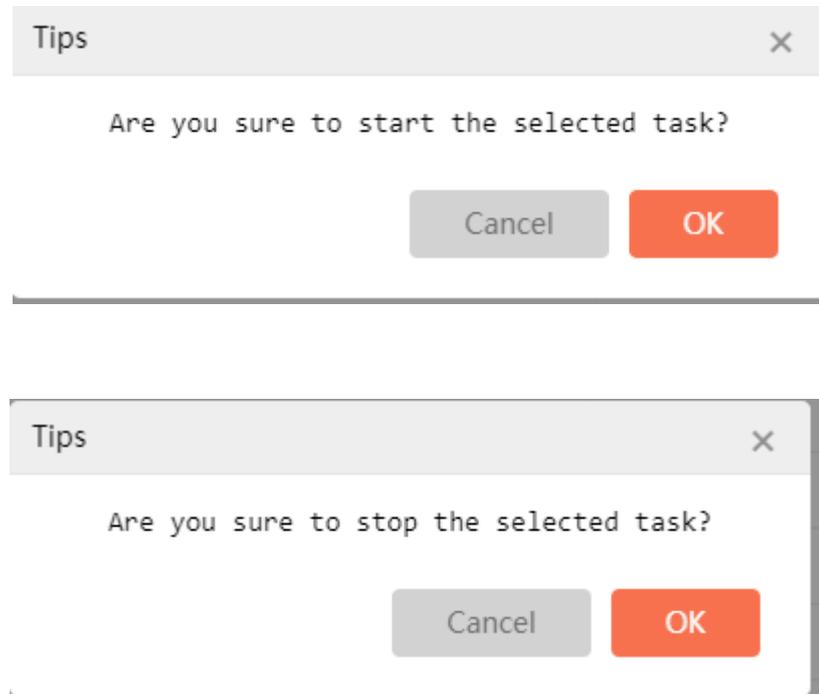


Figure 3-86 Start/stop the discovery task

---

**Caution**

- The started and stopped task cannot be modified.

### Refresh discovery task

Click the "Refresh" button above the task list to refresh the task list data.

### Query discovery task

In the task query panel, enter or select the task name, organization, execution mode and whether to expand discovery, and then click the "Query" button to filter and query the network device discovery task. The filtered data is displayed in the task list below.

Figure 3-87 Query discovery task

## ! Caution

- The name supports fuzzy query.

### Discovery task details

Click the "Discovery details" link on the far right of any discovery task to open the latest discovery details of this discovery task, as shown in the following figure.

Timestamp	Message
2020-06-24 07:18:49	The network discovery task has been started.
2020-06-24 07:18:49	SNMP device 10.11.12.250 sniffed successfully.
2020-06-24 07:18:49	SNMP device 10.11.12.254 sniffed successfully.
2020-06-24 07:18:49	SNMP device 192.168.1.8 sniffed successfully.
2020-06-24 07:18:49	SNMP device 10.11.12.249 sniffed successfully.
2020-06-24 07:18:50	SNMP device 192.168.111.1 sniffed successfully.
2020-06-24 07:18:50	SNMP device 10.11.11.1 sniffed successfully.
2020-06-24 07:18:50	SNMP device 192.168.111.2 sniffed successfully.
2020-06-24 07:18:50	SNMP device 172.16.192.1 sniffed successfully.
2020-06-24 07:18:50	SNMP device 2.2.2.2 sniffed successfully.
2020-06-24 07:18:50	SNMP device 60.1.1.2 sniffed successfully.
2020-06-24 07:18:50	SNMP device 55.55.55.55 sniffed successfully.
2020-06-24 07:18:50	SNMP device 99.99.99.99 sniffed successfully.
2020-06-24 07:18:50	SNMP device 221.10.47.45 sniffed successfully.
2020-06-24 07:18:50	SNMP device 192.168.99.99 sniffed successfully.

Figure 3-88 Network discovery details

## Note

- After saving the task, the details of the last task will not be cleared.

### 3.3.2. Status Monitoring Configuration

Click "Resources" > "Network Discovery" > "Status Monitoring Configuration" on the top navigation bar of the system to open the status monitoring configuration page, as shown below:

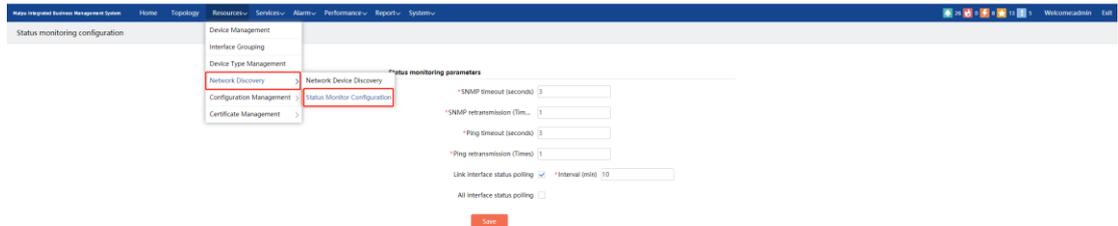


Figure 3-89 Status monitoring configuration

On the page, you can set SNMP status monitoring parameters, including SNMP timeout (seconds) and SNMP retransmission (Times), Ping timeout (seconds), Ping retransmission (Times), link interface status polling, interval time (minutes), all interface status polling, interval time (minutes). Click "Save" to save the modified information.

## 3.4. Certificate Management

Certificate management includes four parts: SNMP certificate, telnet certificate, SSH certificate and security certificate. It is the basis of network discovery, performance monitoring, configuration management, and detection tools. Users can configure the information of multiple certificates here.

### 3.4.1. SNMP Certificate Management

SNMP certificate management is used to manage the common SNMP configuration, which can add/delete/modify/query the SNMP certificate. Click "Resources" > "Certificate management" > "SNMP certificate management" in the menu bar to open the "SNMP certificate management" page, as shown below.

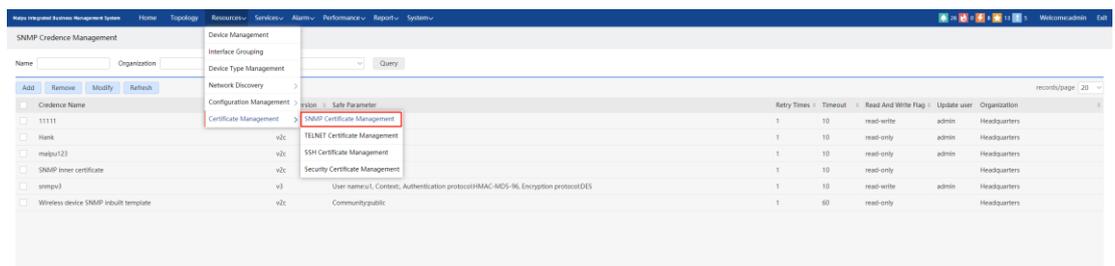


Figure 3-90 SNMP certificate management

**Query SNMP certificate:**

The SNMP certificate list supports displaying by pages, and each SNMP certificate is attached to the organization. Different users can only view the certificates of the organization to which the user belongs and all its subordinate organizations when logging in. SNMP certificate supports fuzzy query filtering by name, organization, and version number, as shown in the following figure:

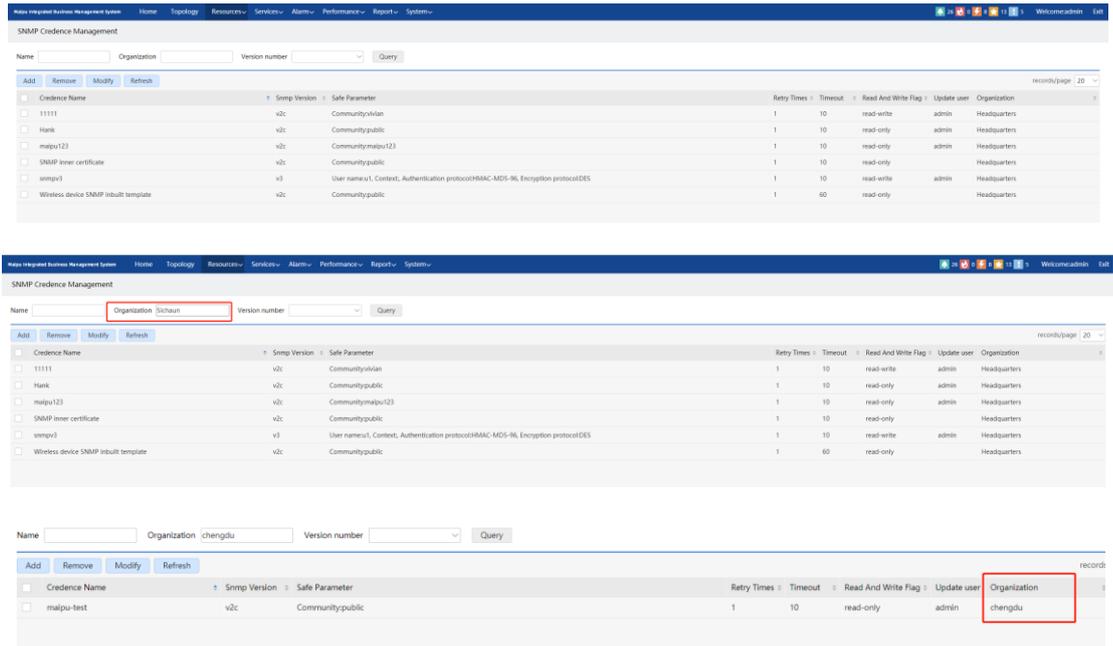


Figure 3-91 SNMP certificate query and hierarchical and decentralized display

**Add SNMP certificate:**

Click the "Add" button to open the "Add certificate" dialog box, fill in the SNMP related parameters, and click "OK" to save the newly added SNMP certificate.

Add

\*Credence Name

\*Organization

\*SNMP Version

\*Retry Times  Retry Times(1-10,default:1)

\*Timeout Interval  Timeout(1-60s, default: 10)

\*Read-Write Flag

Community  Community(default: public)

Cancel OK

Figure 3-92 Add SNMP certificate

### Note

- The input items will change dynamically when the SNMP version number is switched. Different parameters need to be configured for SNMP templates with different version numbers.
- When adding a certificate, you can specify an organization for the certificate, and the certificates under the same organization cannot have the same name.

### Modify SNMP certificate:

Select the SNMP certificate to be modified in the list (only one certificate can be modified at the same time). Click the "Modify" button to open the "Modify" dialog box (as shown in the figure below). The parameters of the SNMP certificate can be modified. The "Organization" field cannot be modified. After modification, click "OK" to save the modified settings.

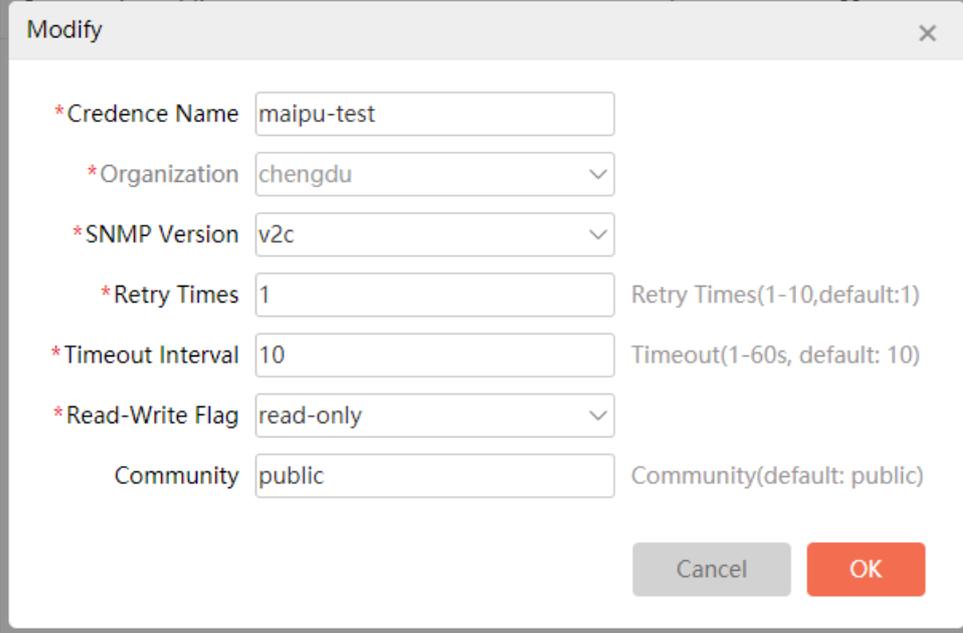


Figure 3-93 Modify the SNMP certificate

**Delete SNMP Certificate:**

Select the SNMP certificate to be deleted in the list (multiple selection is supported), click the "Delete" button, and click "OK" in the pop-up delete confirmation dialog box (as shown in the figure below) to delete the selected SNMP certificate. Click the "Cancel" button to drop the deletion operation.

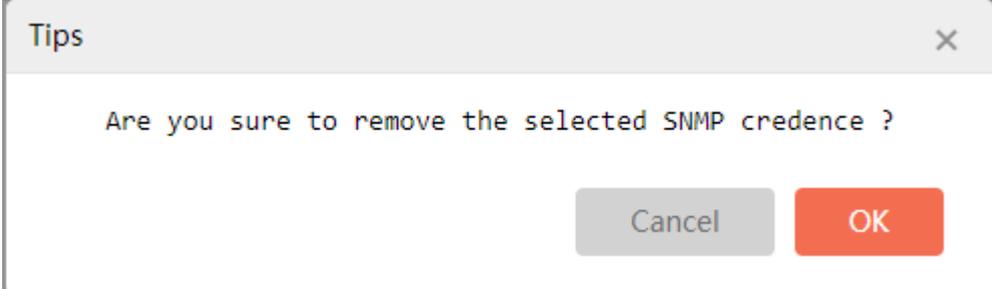


Figure 3-94 Delete the SNMP certificate

---

**! Caution**

- "SNMP inbuilt template" and "Wireless device SNMP inbuilt template" are inbuilt templates of the system and cannot be deleted.
  - Deleting the template referenced by the task will affect the execution result of the network discovery task that has referenced the template.
- 

**Refresh SNMP certificate:**

Click the “Refresh” button above the list, and you can refresh the certificate list data.

### 3.4.2. Telnet Certificate Management

SNMP certificate management is used to manage the common Telnet configuration, which can add/delete/modify/query the Telnet certificate. Click "Resources" > "Certificate management" > " Telnet certificate management" in the menu bar to open the " Telnet certificate management" page, as shown below.

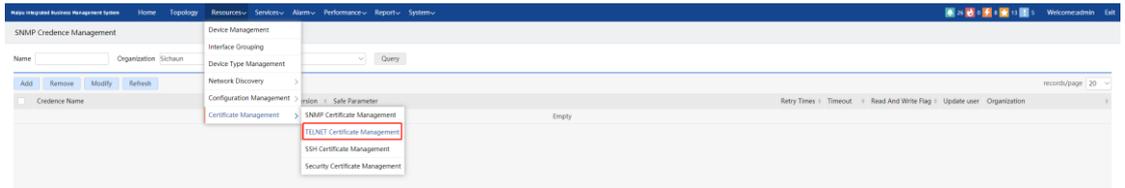


Figure 3-95 Telnet certificate management

#### Query Telnet certificate:

The Telnet certificate list supports displaying by pages, and each Telnet certificate is attached to the organization. Different users can only view the certificates of the organization to which the user belongs and all its subordinate organizations when logging in. Telnet certificate supports fuzzy query filtering by name and organization, as shown in the following figure:

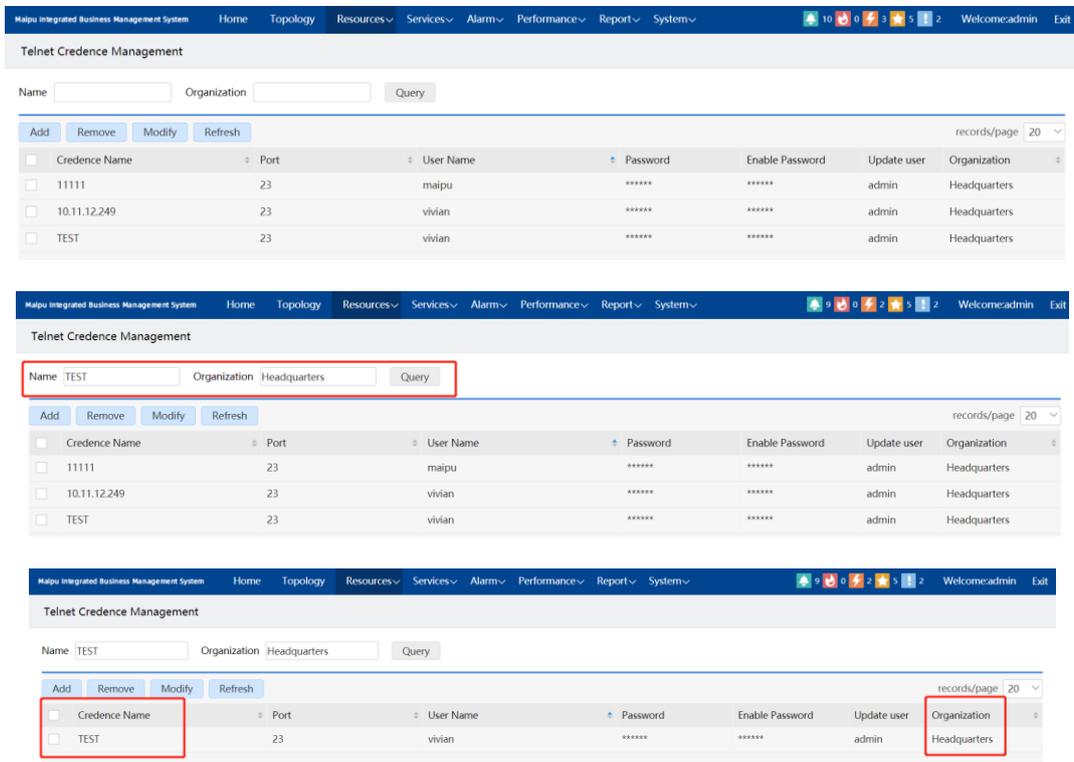
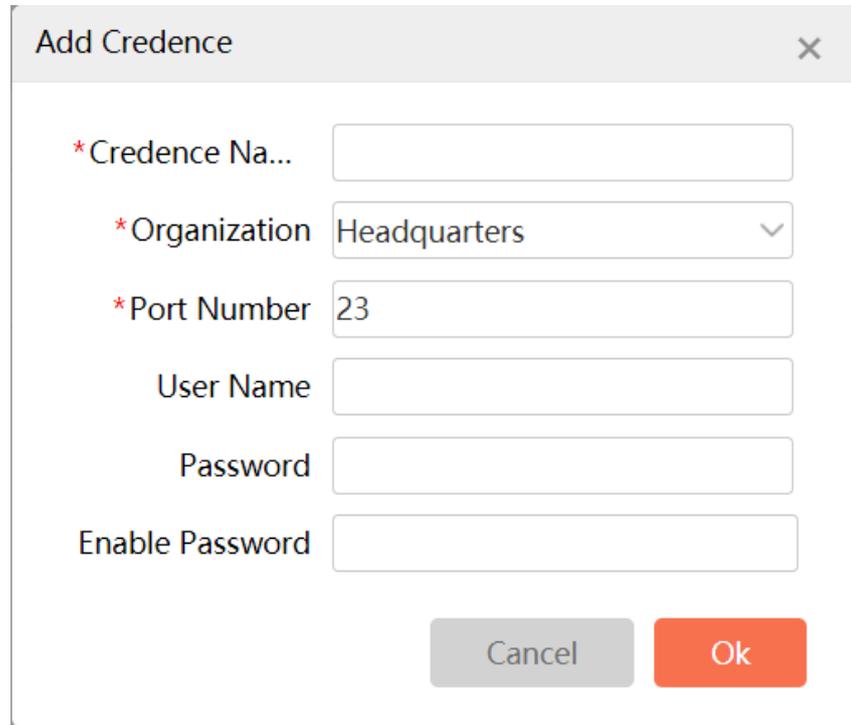


Figure 3-96 Telnet certificate query and hierarchical and decentralized display

#### Add Telnet certificate:

Click the “Add” button to open the "Add " dialog box, fill in the Telnet related parameters, and click "OK" to save the newly added Telnet certificate.



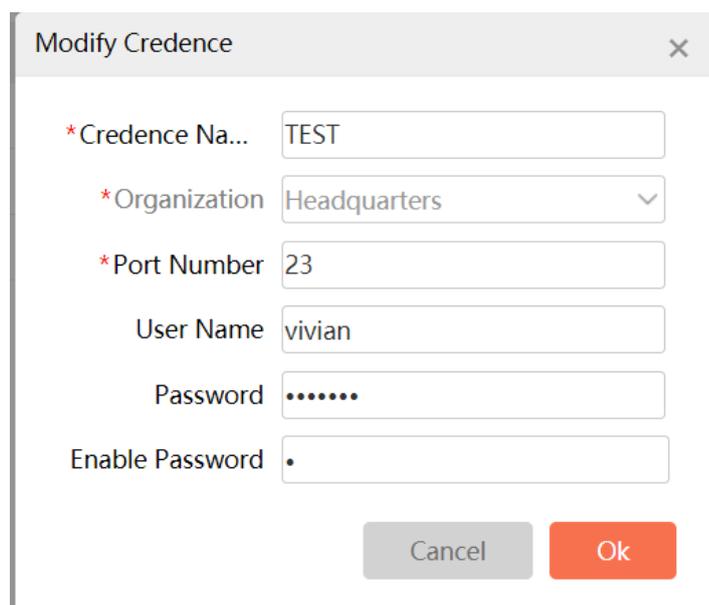
The "Add Credence" dialog box contains the following fields and controls:

- \* Credence Na...: Text input field.
- \* Organization: Dropdown menu with "Headquarters" selected.
- \* Port Number: Text input field with "23".
- User Name: Text input field.
- Password: Text input field.
- Enable Password: Text input field.
- Buttons: "Cancel" (grey) and "Ok" (orange).

Figure 3-97 Add a Telnet certificate

#### Modify Telnet Certificate:

Select the Telnet certificate to be modified in the list (only one certificate can be modified at the same time). Click the “Modify” button to open the "Modify" dialog box, as shown in the figure below. After modification, click "OK" to save the modified settings. The “Organization” cannot be modified.



The "Modify Credence" dialog box contains the following fields and controls:

- \* Credence Na...: Text input field with "TEST".
- \* Organization: Dropdown menu with "Headquarters" selected.
- \* Port Number: Text input field with "23".
- User Name: Text input field with "vivian".
- Password: Text input field with "\*\*\*\*\*".
- Enable Password: Text input field with ".".
- Buttons: "Cancel" (grey) and "Ok" (orange).

Figure 3-98 Modify a Telnet certificate

**Delete Telnet Certificate:**

Select the Telnet certificate to be deleted in the list (multiple selection is supported), click the "Delete" button, and click "OK" in the pop-up delete confirmation dialog box to delete the selected Telnet certificate. Click the "Cancel" button to drop the deletion operation.

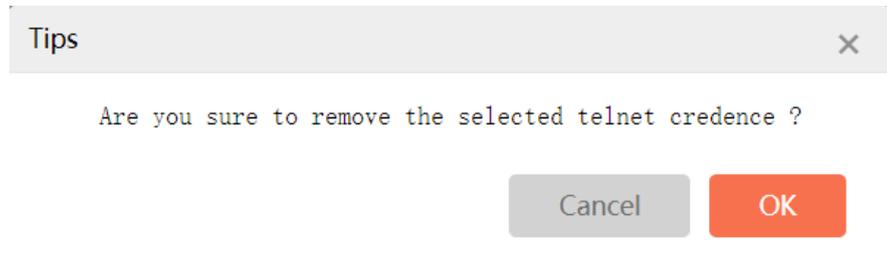


Figure 3-99 Delete a Telnet certificate

**Refresh Telnet certificate:**

Click the "Refresh" button above the list, and you can refresh the certificate list data.

**3.4.3. SSH Certificate Management**

SSH certificate management is used to manage the common SSH configuration, which can add/delete/modify/query the SSH certificate. Click "Resources" > "Certificate management" > "SSH certificate management" in the menu bar to open the "SSH certificate management" page, as shown below.

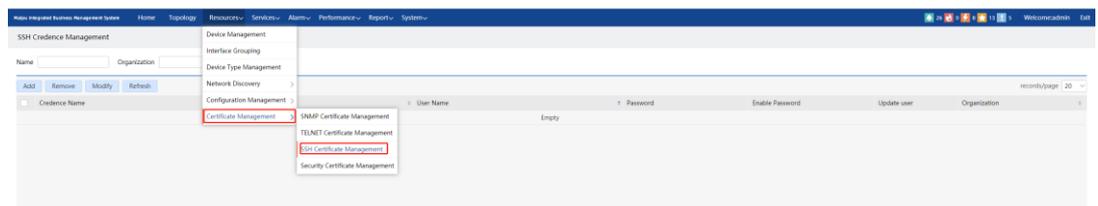


Figure 3-100 SSH certificate management

**Query SSH certificate:**

The SSH certificate list supports displaying by pages, and each SSH certificate is attached to the organization. Different users can only view the certificates of the organization to which the user belongs and all its subordinate organizations when logging in. SSH certificate supports fuzzy query filtering by name and organization, as shown in the following figure:



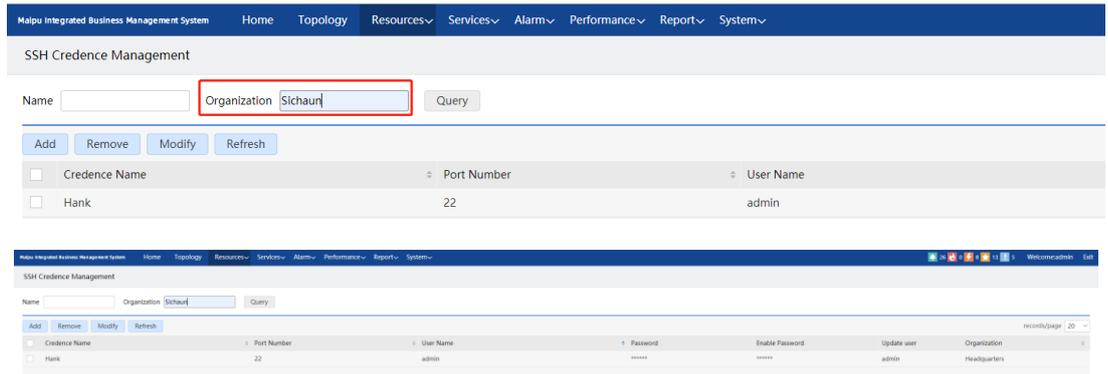


Figure 3-101 SSH certificate query and hierarchical and decentralized display

**Add SSH certificate:**

Click the “Add” button to open the "Add SSH Certificate" dialog box, fill in the SSH related parameters, and click "OK" to save the newly added SSH certificate.

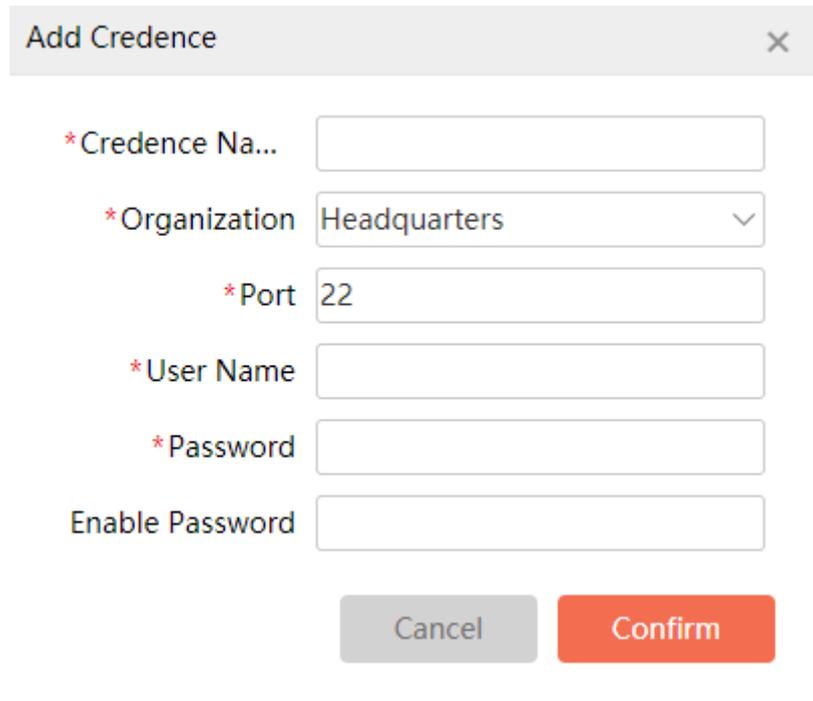


Figure 3-102 Add SSH certificate

**Modify SSH Certificate:**

Select the SSH certificate to be modified in the list (only one certificate can be modified at the same time). Click the “Modify” button to open the "Modify" dialog box, as shown in the figure below. After modification, click "OK" to save the modified settings. The “Organization” cannot be modified.

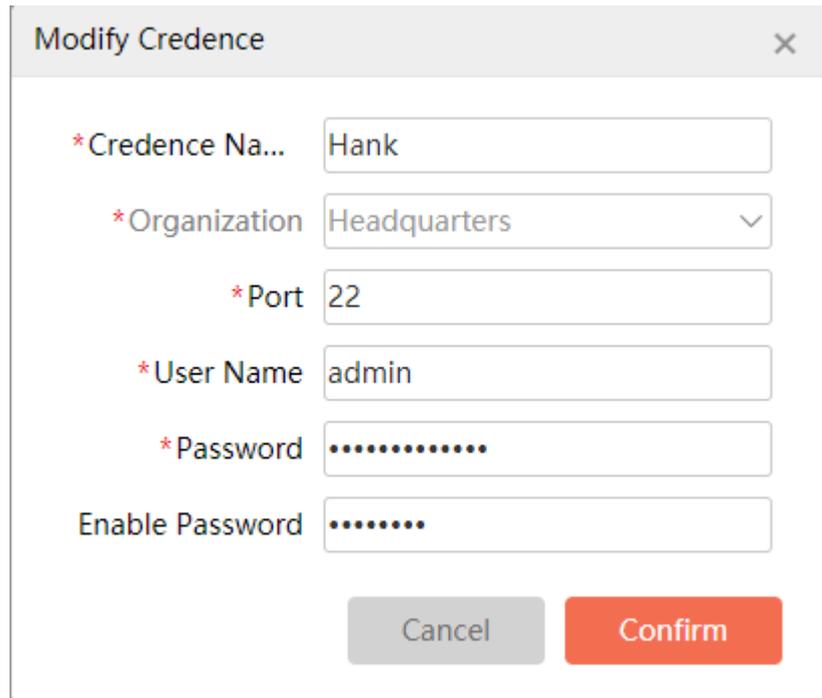


Figure 3-103 Modify SSH certificate

**Delete SSH Certificate:**

Select the SSH certificate to be deleted in the list (multiple selection is supported), click the "Delete" button, and click "OK" in the pop-up delete confirmation dialog box to delete the selected SSH certificate. Click the "Cancel" button to drop the deletion operation.

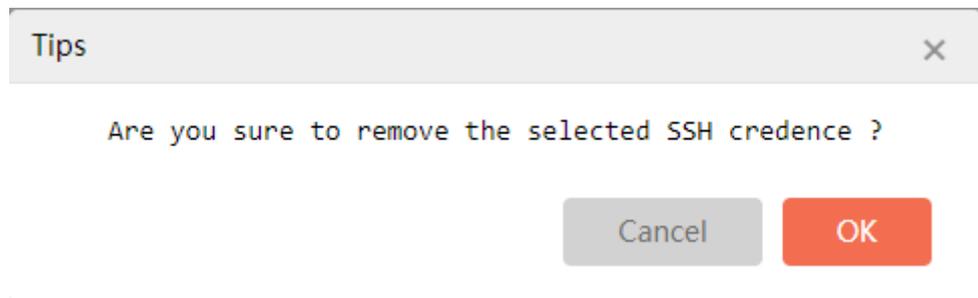


Figure 3-104 Delete SSH certificate

**Refresh SSH certificate:**

Click the "Refresh" button above the list, and you can refresh the certificate list data.

### 3.4.4. Security Certificate Management

Security certificate management is used to manage the common security configuration, which can add/delete/modify/query the security certificate. Click "Resources" > "Certificate management" > "Security certificate management" in the menu bar to open the "Security certificate management" page, as shown below.

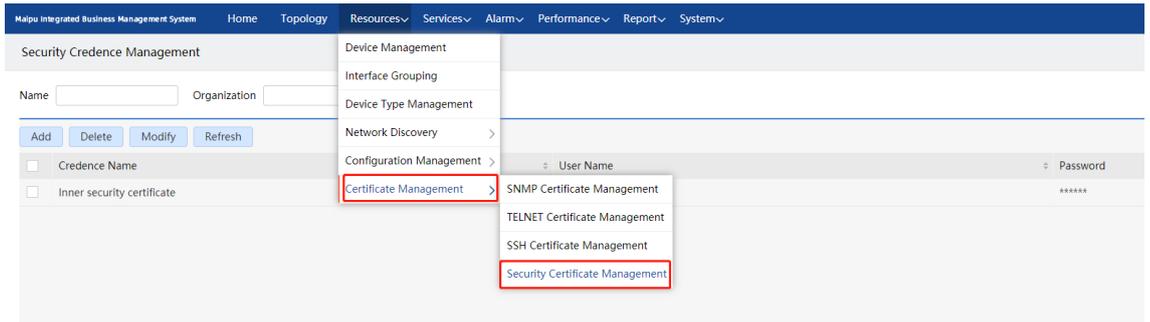


Figure 3-105 Security certificate management

**Query Security certificate:**

The security certificate list supports displaying by pages, and each security certificate is attached to the organization. Different users can only view the certificates of the organization to which the user belongs and all its subordinate organizations when logging in. The security certificate supports fuzzy query filtering by name and organization, as shown in the following figure:

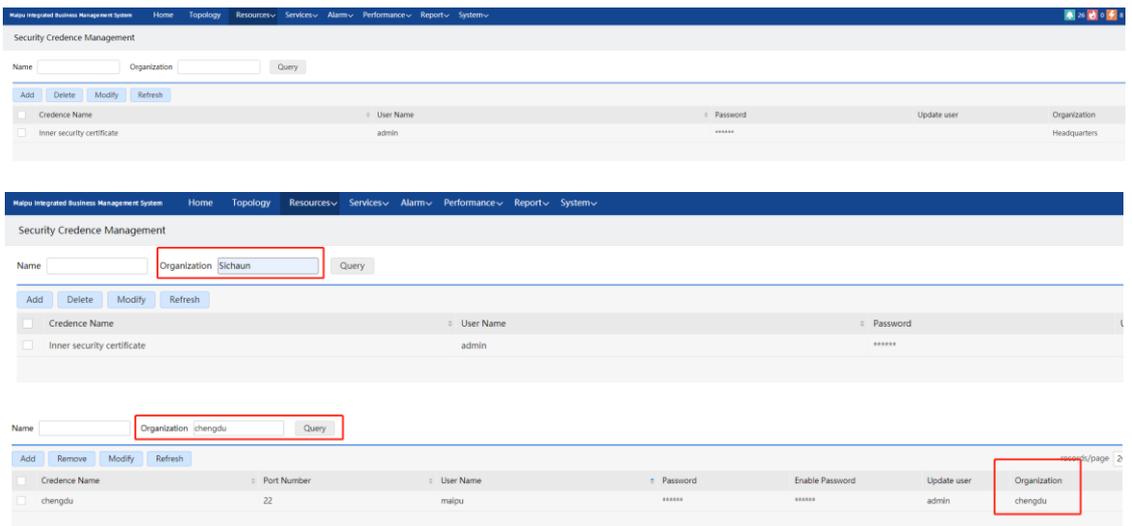
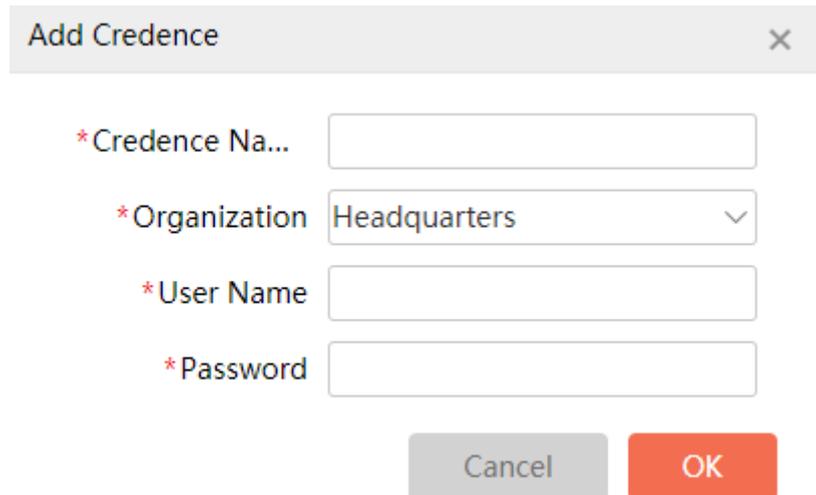


Figure 3-106 Security certificate query and hierarchical and decentralized display

**Add Security Certificate:**

Click the "Add" button to open the "Add Security Certificate" dialog box, fill in the security related parameters, and click "OK" to save the newly added security certificate.

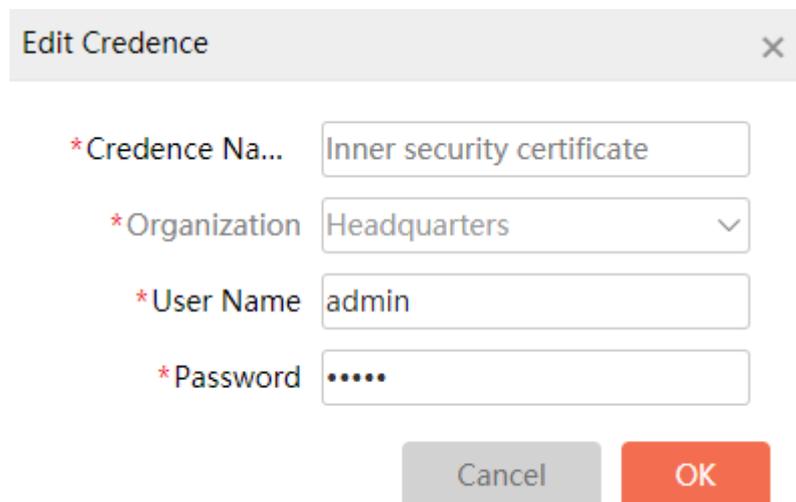


The 'Add Credence' dialog box contains four input fields: '\* Credence Na...' (text), '\* Organization' (dropdown menu with 'Headquarters' selected), '\* User Name' (text), and '\* Password' (text). At the bottom are 'Cancel' and 'OK' buttons.

Figure 3-107 Add security certificate

**Modify Security Certificate:**

Select the security certificate to be modified in the list (only one certificate can be modified at the same time). Click the "Modify" button to open the "Modify" dialog box, as shown in the figure below. After modification, click "OK" to save the modified settings. The "Organization" cannot be modified.



The 'Edit Credence' dialog box contains four input fields: '\* Credence Na...' (text with 'Inner security certificate'), '\* Organization' (dropdown menu with 'Headquarters' selected), '\* User Name' (text with 'admin'), and '\* Password' (text with '\*\*\*\*\*'). At the bottom are 'Cancel' and 'OK' buttons.

Figure 3-108 Modify security certificate

**Delete Security Certificate:**

Select the security certificate to be deleted in the list (multiple selection is supported), click the "Delete" button, and click "OK" in the pop-up delete confirmation dialog box to delete the selected security certificate. Click the "Cancel" button to drop the deletion operation.

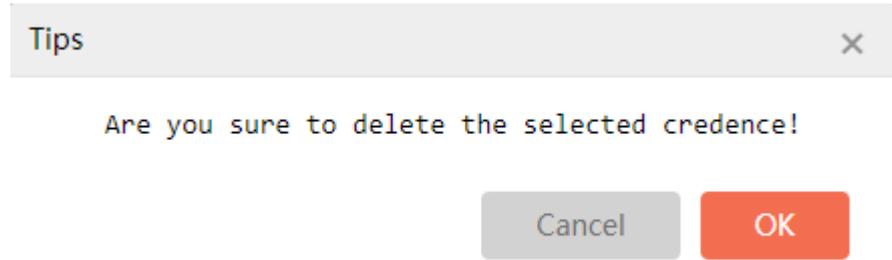


Figure 3-109 Delete security certificate

**Refresh Security certificate:**

Click the “Refresh” button above the list, and you can refresh the certificate list data.

## 3.5. Interface Grouping

The interface grouping module provides grouping function for all interfaces in the system, including grouping interfaces, searching for specific interfaces according to filtering conditions, and viewing interface details. Click "Resources" -> "Interface Group" in the navigation bar at the top of the system to open the “Interface Grouping” interface, as follows:

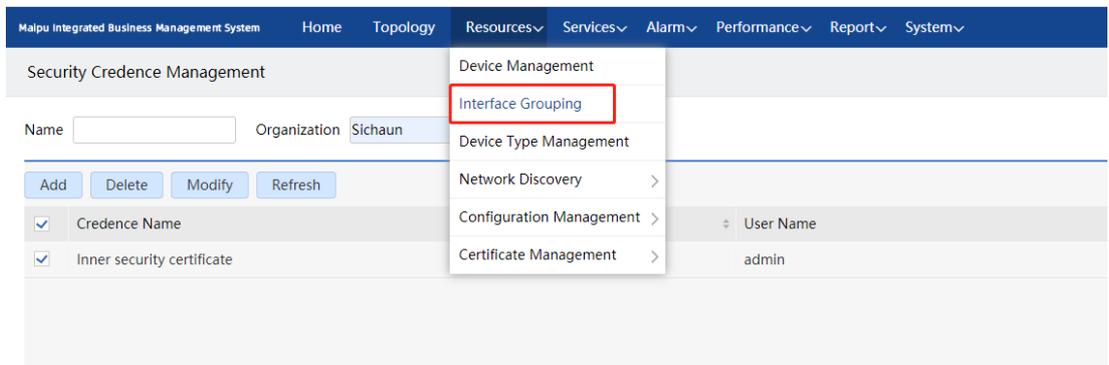


Figure 3-110 Interface grouping

**Interface List**

When the “Interface Grouping” interface is opened, no interface is displayed by default. Only the interface group node in the left group tree is selected, and the interface information in the corresponding interface group will be displayed in the right interface list, displaying the status, interface name, device name, device IP, interface IP, interface category, rate, enabled status, organization, description and other information of each interface. It also supports "List function". You can select and save the displayed lists and list positions. The interface name is required, as shown in the following figure:

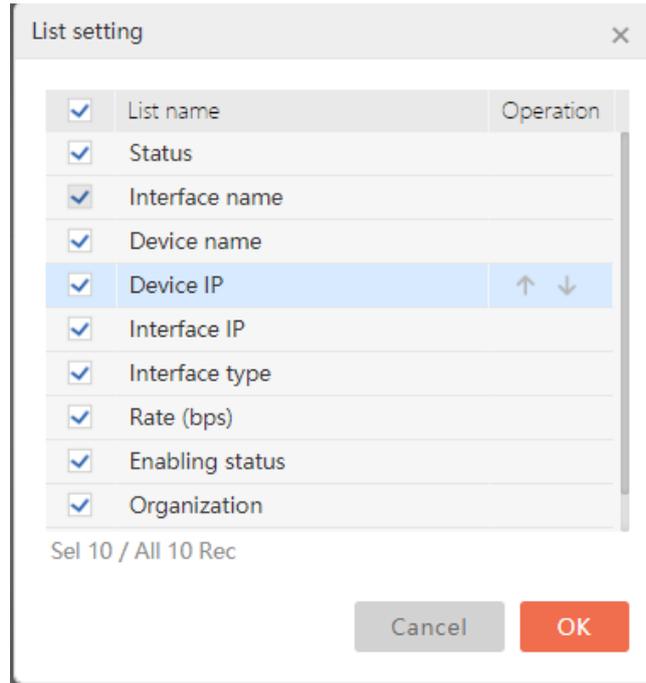


Figure 3-111 Interface list setting

The interfaces displayed in the interface list are determined by the left grouping tree. If the interface group node is selected in the left grouping tree, the interface list in the interface group will be displayed in the list, and the selected organization node will not respond, as shown in the following figure:

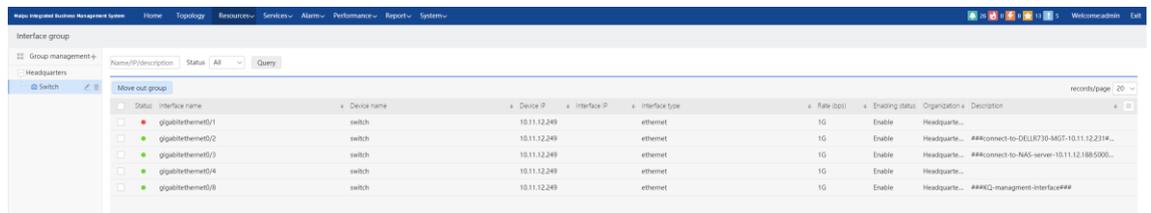
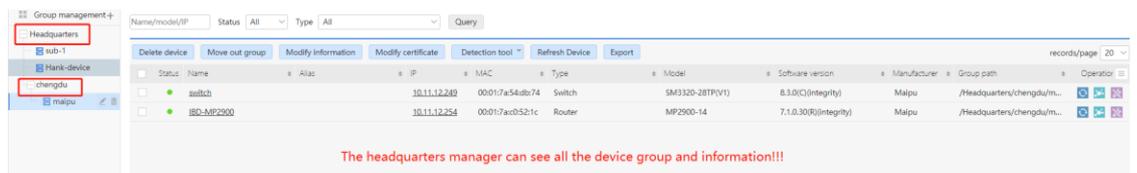


Figure 3-112 Display interfaces by groups

The interface lists that administrators of different organizations can view are different. They can only view the interface group and interface information of the organization to which the administrator belongs and its subordinate organizations, but not the information of the parent organization or the same level organization, as shown in the following figure:



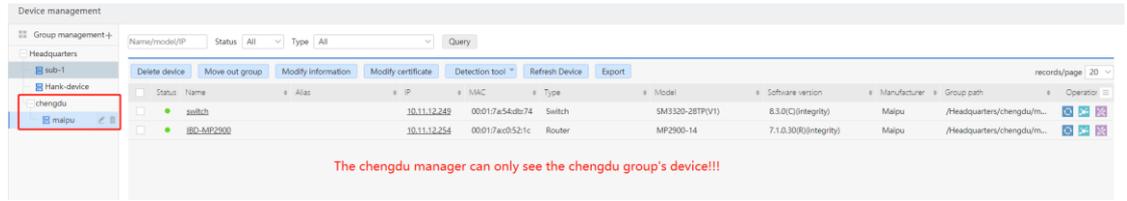


Figure 3-113 Interface list display

This page provides a variety of query conditions, you can easily and quickly query specific interfaces. Enter the corresponding query conditions in the query panel, and then click the "Query" button to filter the interfaces in the group according to the interface name, device name, interface IP, device IP, interface status and other fields. As shown in the figure below, query all interfaces in the total line interface group with the status of "up" and any of the name, IP and description can match the string "null":

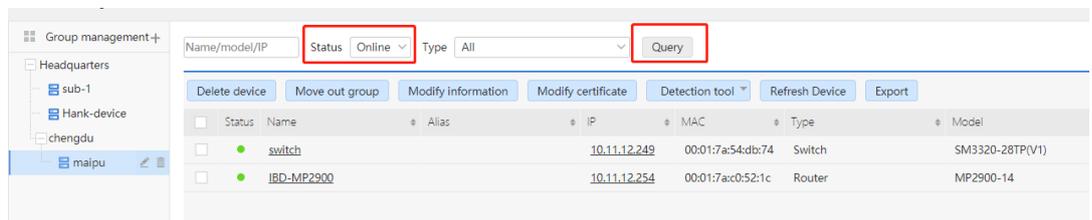


Figure 3-114 Interface list query

**Note**

- The query input box can fuzzy match any one of the interface name, device name, interface IP, and device IP of the interface, and the device IP will match all IPs of the device, including access IP and device interface IP.

**Add Interface Group:**

Network management system provides interface grouping function, reasonable grouping can be more convenient for interface management. The system carries out hierarchical and decentralized management of interface groups. All interface groups are mounted under the corresponding organization and cannot be nested. Administrators of different organizations can only create, modify, and delete interface groups for the current level and lower level organizations.

Click the add icon  in the left group tree of the interface list to open the "Add " interface. You need to enter the group name, select the organization of the interface group, and enter the basic information of the interface group, such as description information, to create the group, as shown in the following figure:

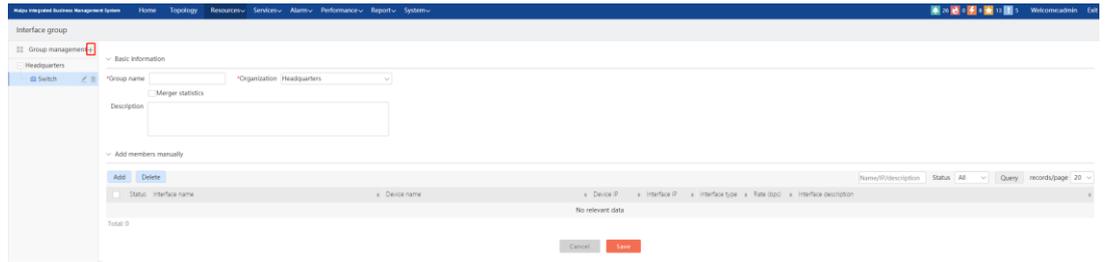


Figure 3-115 Add interface group

Merge statistics: the data of multiple interfaces are aggregated into the data of an interface group, and participate in the interface performance statistics, such as interface traffic, bandwidth utilization, etc.

To manually select the interface when creating an interface group, click the "Add" button to manually add the interface for the interface group. As shown in the figure below, in the pop-up "Select interfaces" dialog box, you can select the grouping tree on the left (select organization/device group node), and the "Device" drop-down box in the upper query panel will dynamically match the devices under the selected node, and then the interfaces can be filtered by interface name, description and interface IP. Support the "Select all" and "Delete all" functions, but there will be a certain number restriction when selecting all.

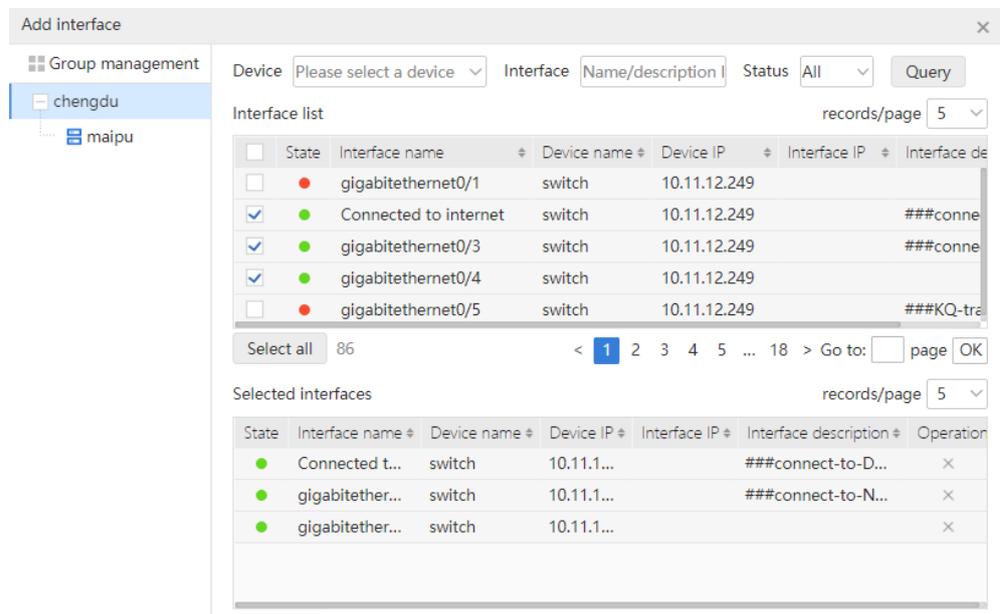


Figure 3-116 Select interfaces

After selecting the interface, click "OK" to add the selected interfaces to the list of manually added members.

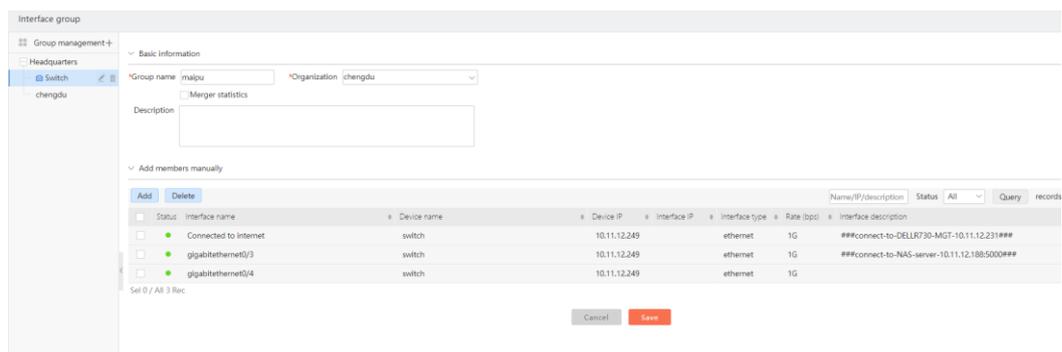


Figure 3-117 Manually add members

Click the "Save" button to save the interface group. At this time, the interface group will be mounted under the selected "Organization" and displayed in a tree structure.

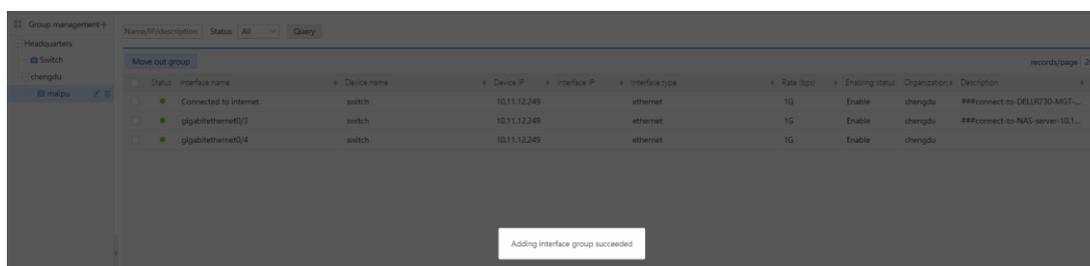


Figure 3-118 Adding interface group succeeded

## Note

- When adding/editing an interface group, the upper limit of interfaces in the interface group is 500. In the interface selection pop-up box, if the number of selected interfaces exceeds 500, it cannot be added any more, and a prompt will be given.

### Edit Interface Group:

Select the interface group to be edited in the left tree of the interface grouping page, and click the edit icon  to enter the interface group editing page. You can edit the name, description, and members of the group. The "Organization" cannot be edited.

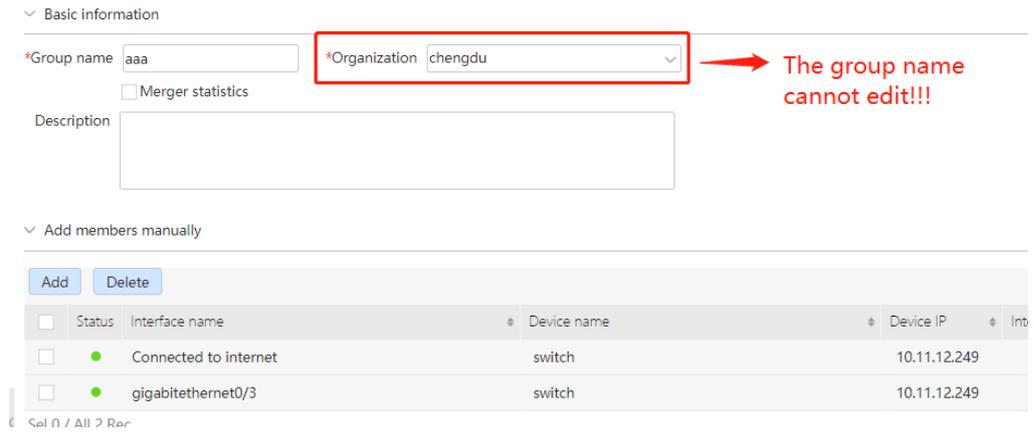


Figure 3-119 Edit interface group

**Note**

- When adding/editing an interface group, the duplicate name rule is no duplicate name under the same organization, that is, the same organization cannot have the interface groups with the same name. If there is a duplicate name, a prompt will be given when saving the interface group

**Delete Interface Group:**

Select the interface group to be deleted in the left tree of the interface grouping interface, and click the delete icon  to open the deletion confirming dialog box. After confirming, the interface group can be deleted.

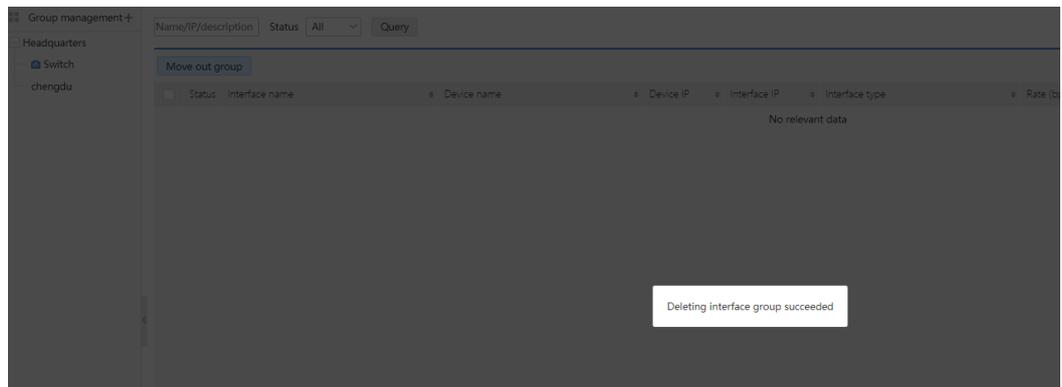
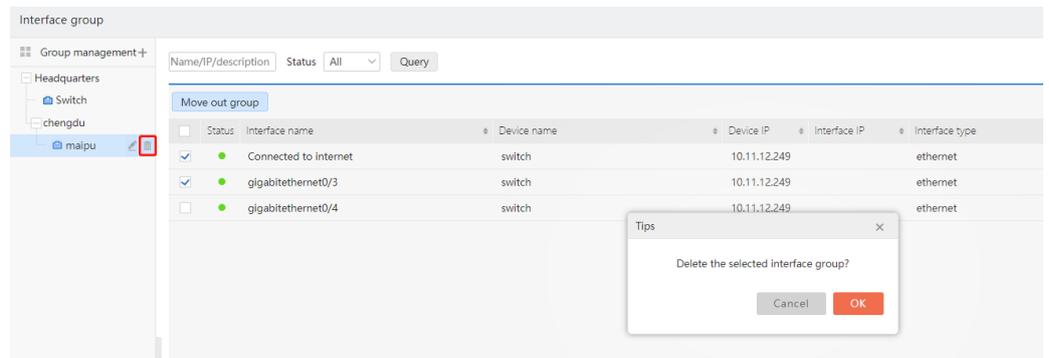


Figure 3-120 Delete interface group

### Move out group:

The “Move out group” function supports removing the selected interface from the specified interface group. Check the interface to be removed from the group in the interface list (multiple selection is supported). Click the button “Move out group” to open the prompt box for confirming the removal, as shown in the figure below. Click the "OK" button to confirm the removal of the selected interface from the corresponding group, and click the "Cancel" button to drop the removal operation.

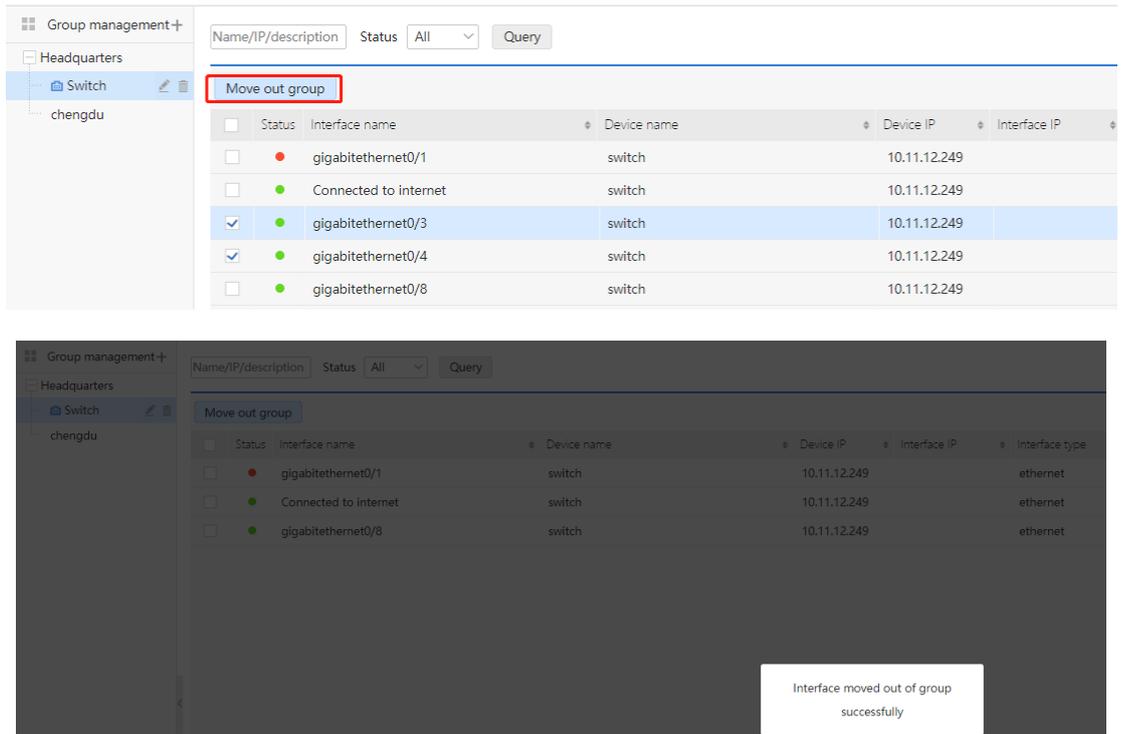


Figure 3-121 Move the interface out of the group

# 4. Configuration Management

Configuration management mainly manages the configuration of the device, including four functions: software package management, configuration file management, configuration command delivering, and policy object management. Click "Resources" --> "Configuration Management" at the top navigation bar of the system to enter the corresponding sub module for operations.

## 4.1. Software Package Management

### 4.1.1. Software Package Management

The software package management module provides the management of software upgrade package for devices in the system, including adding, modifying, deleting, downloading software packages, and querying software packages. Click "Resources" > "Configuration Management" > "Software Package Management" > "Software Package Management" in the navigation bar at the top of the system to open the "Package Management" page, as follows:

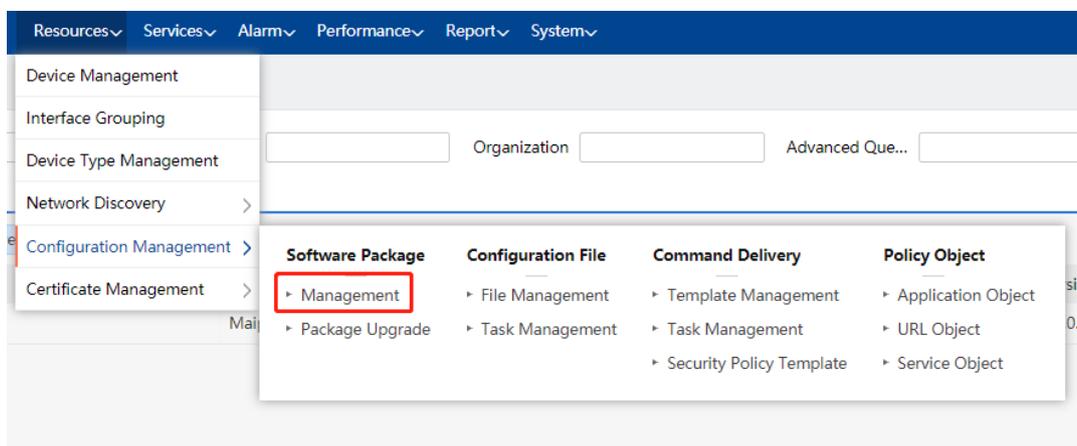


Figure 4-1 Software package management

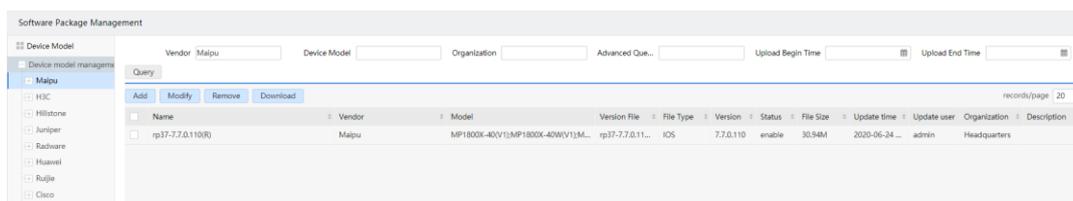
#### Software Package List:

Open the "Software Package Management" interface and display all the software packages in the system by default, displaying the name, manufacturer, model, version file, file type, version number, status, file size, update time, update user, organization, description, and other information of each software package.

This page provides a variety of query conditions, you can easily and quickly query specific software packages. Enter the corresponding query conditions in the "Software

Package Query" panel, and then click the button "Query" to query all software packages according to the manufacturer information, device model, organization, advanced query, upload start time, upload end time, and other fields; among them, advanced query can be based on version name and file name. Click the fields in the header of the package list to sort the packages according to the corresponding fields.

As shown in the figure below, all software package information with manufacturer information of "Maipu", device model of "MP1800X", organization of headquarters, and name of "IOS" are found and sorted according to the software package name:



The screenshot shows the 'Software Package Management' interface. At the top, there are search filters for Vendor (Maipu), Device Model, Organization, Advanced Query, Upload Begin Time, and Upload End Time. Below the filters is a 'Query' button and a table of results. The table has columns for Name, Vendor, Model, Version File, File Type, Version, Status, File Size, Update time, Update user, Organization, and Description. A single record is displayed with the following details:

Name	Vendor	Model	Version File	File Type	Version	Status	File Size	Update time	Update user	Organization	Description
rp37-7.7.0.110(R)	Maipu	MP1800X-40(V1);MP1800X-40(W1);M...	rp37-7.7.0.11...	IOS	7.7.0.110	enable	30.94M	2020-06-24 ...	admin	Headquarters	

Figure 4-2 Software package query and sorting

## ! Caution

- Organization: the organization and its subordinate organizations of the current administrator

### Add Software Package:

Click the "Add" button in the software package list panel to open the "Add" window, select the device model, file type, version file, status, fill in the version name, version number, description, etc., as shown in the following figure:

The 'Add' dialog box contains the following fields and controls:

- \*Device Model:** A dropdown menu with the value 'Maipu;Router;MP1800X;MF'.
- \*File Type:** A dropdown menu with the value 'IOS'.
- \*Version File:** A text input field next to a 'Browse' button.
- Status:** Radio buttons for 'Enable' (selected) and 'Disable'.
- \*Version Na...:** A text input field.
- \*Version:** A text input field.
- Description:** A larger text input area.
- Warning:** 'Please select a software package file type!' in orange text.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

Figure 4-3 Add software package

Click the “OK” button to complete the adding of the package. The process of modifying the software package is the same as above. Select the software package to be modified in the package management list and click the “Modify” button to modify it.

**Note**

- Status: enabled: the package can be selected in the "Software Package Update" task; disabled: the package cannot be selected in the "Software Package Update" task.

**Delete Software Package:**

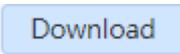
In the package management list, select the software package to be deleted, and then click the button . After the prompt message, click to delete the software package that is no longer used.

The 'Tips' dialog box contains the following elements:

- Title:** 'Tips' with a close button (X).
- Message:** 'Are you sure to remove the selected software package?' in blue text.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom right.

Figure 4-4 Delete software package

**Download Software Package:**

Select the software package to be downloaded from the package management list, and then click the button . After the prompt message, click  to download the selected software package.

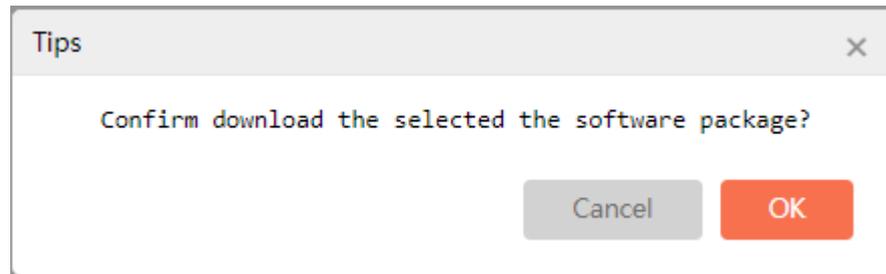


Figure 4-5 Download software package

**4.1.2. Software Package Update**

The software package update management module can update the software package of the specified device, including adding, modifying, deleting, manually starting, stopping, and refreshing the software package update task, and querying the software package update task.

Click "Resources" > "Configuration Management" > "Software Package Management" > "Software Package Update" in the top navigation bar of the system to open the "Software Package Update Task Management" page, as follows:

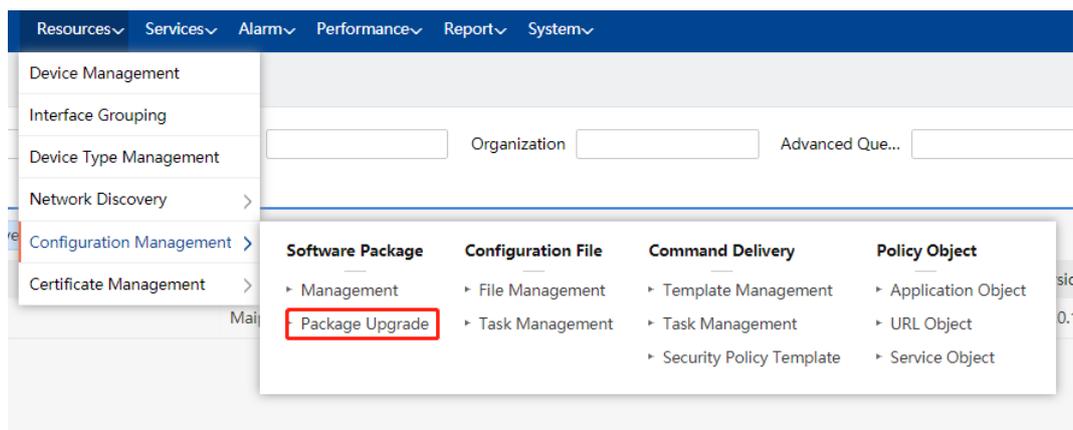


Figure 4-6 Software package update task management

**Task list:**

Open the "Software Package Update Task Management" interface, and display all the software package update tasks in the system by default. The name, status, last start time, last end time, scheduling information, description, recent execution, update user, details,

history, and other information of each task are displayed by lists.

This page provides a variety of query conditions, you can easily and quickly query specific tasks, input the corresponding query conditions, and then click the button "Query" to query all tasks according to the name, status, organization, start time, end time and other fields. Click the "Organization" field in the head of the task list to sort the list data.

As shown in the figure below, all tasks with the name of "software package update task", status of "Completed" and organization of "Headquarters" are found out.

The screenshot shows a web interface for querying tasks. At the top, there are input fields for Name, Status, Organization, Startup time, and End time, along with a 'Query' button. Below the input fields is a table with the following data:

Name	Status	Last startup time	Last end time	Scheduling information	Description	Recent execution (success/failure/total)	Update user	Organization	Details	History
1900X	Completed	2020-06-24 08:35:03	2020-06-24 08:35:05			0/1/1	admin	Headquarters	<a href="#">Details</a>	<a href="#">History</a>

Figure 4-7 Software package update task query

**! Caution**

- Organization: the organization and its subordinate organizations of the current administrator.

**Add/Modify Task:**

Click the "Add" button in the task list or select a task and click the "Modify" button to open the "Add/Modify task information" window, as shown in the figure below. Fill in the task name and description, select whether to restart the device, and select the file server and execution mode. By selecting the advanced configuration option, you can also set the number of auto retries, timeout, whether to delete files, and whether to support VRF.

Add
✕

1 **Basic information**
2 **Device selection**
3 **File selection**

---

**\*Name**

Reboot device  Yes  NO    Auto save configuration  Yes  No

File server  Local TFTP  Local FTP  Remote FTP  HTTP (only support ISG device V4. X)

Mode of execution  Execute immediately  Timing execution

Description

---

Advanced configuration ^

**\*Auto retry times**       **\*Timeout (min)**

Auto delete files  Yes  No

Support VRF  Yes  NO

5/32 characters,you can input 27 characters!

Cancel
Next step

Figure 4-8 Add/Modify the task information- Step 1

## Caution

- In the software package update task, the device concurrency number of the current single task is 5, and the task concurrency number is 1.
- The default number of auto retries is 1 and the timeout is 60 minutes.
- By default, select not support VRF.

Auto delete files: the default value is "Yes". After checking, if the storage space of the device is insufficient, the existing software package will be automatically deleted and then the software package will be updated. If "No" is selected, it will not be deleted and an error message will be returned.

Whether to reboot device: after the device software package is updated successfully, the device will be restarted. If the update fails, the error message will be recorded, and the device will not be restarted.

File server: By default, configuration change uses the local TFTP server for transferring files. If some devices do not support the local TFTP command upgrade, you can use the local FTP server to upgrade. When choosing TFTP, you do not need to input the user name and password, but FTP needs to input the user name and password (FTP user

name and password are the FTP user name and password configured by the user when installing the network management system).

You can also use the remote FTP server to upgrade. When selecting the remote FTP server, you need to input the FTP address, file name, file type (IOS, monitor, uboot), user name and password; for ISG device version 4. X, you can also select HTTP mode for upgrade. When selecting HTTP mode, you need to input IP address, file name and file type (IOS, monitor, uboot).

Execution mode: When "Execute immediately" is selected, the task can be executed immediately after the task information is configured; if "Timing execution" is selected, the task will be executed after the set time period.

Auto retry times: If adding software package fails, it will automatically retry. The number of retries is the given value.

Timeout: When the task is executed, the time for waiting device response exceeds the set timeout, and the task execution fails.

Automatic delete files: By default, Yes is selected, that is, after the package is added, the files are automatically deleted to reduce the space occupation.

Support VRF: By default, it is "No". VRF is VPN routing forwarding table, which is a special entity established and maintained by PE for directly connected sites.

Click "Next Step" to enter the "Device selection" window, as shown in the figure below

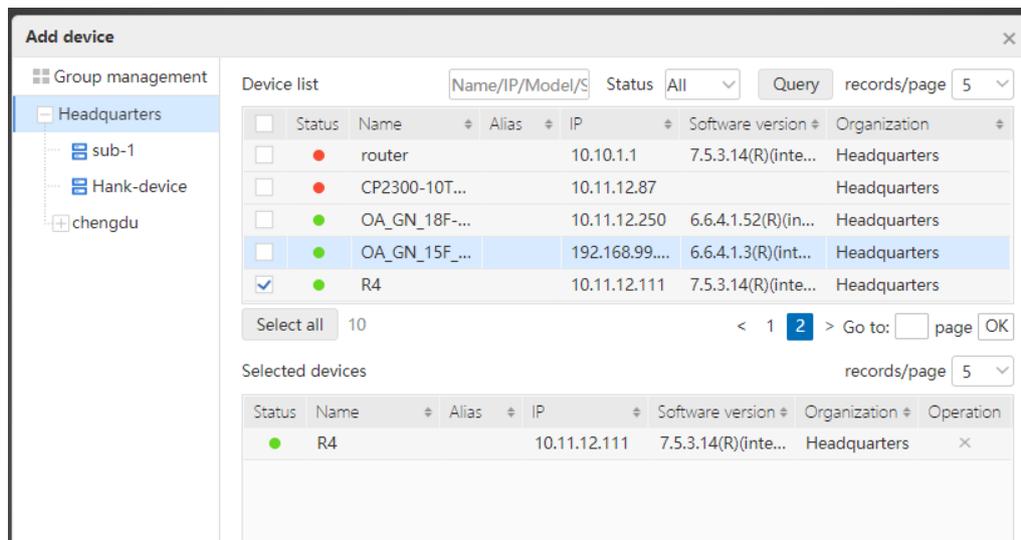


Figure 4-9 Add/modify task information-Step 2

Click "Add device", select the corresponding device for the task, and enter the "Select device" window, as shown in the figure below:

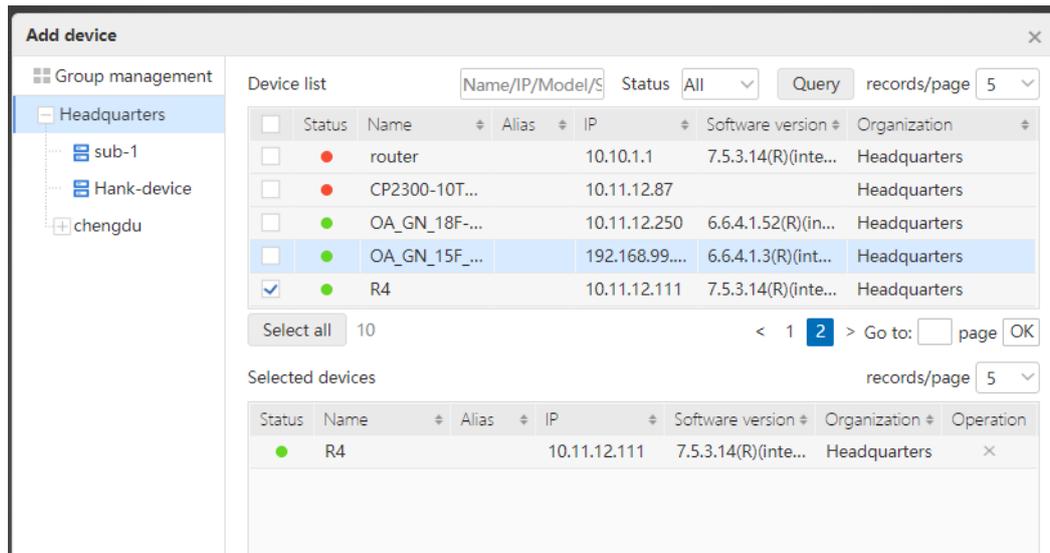


Figure 4-10 Select devices

### Note

- The devices of the same model must be selected. Otherwise, the system cannot select a unified software upgrade package for it, and the software upgrade package will not be found in the "File selection" step.

Select the device, and click **OK** to select the device for the software package update task, as shown in the following figure:

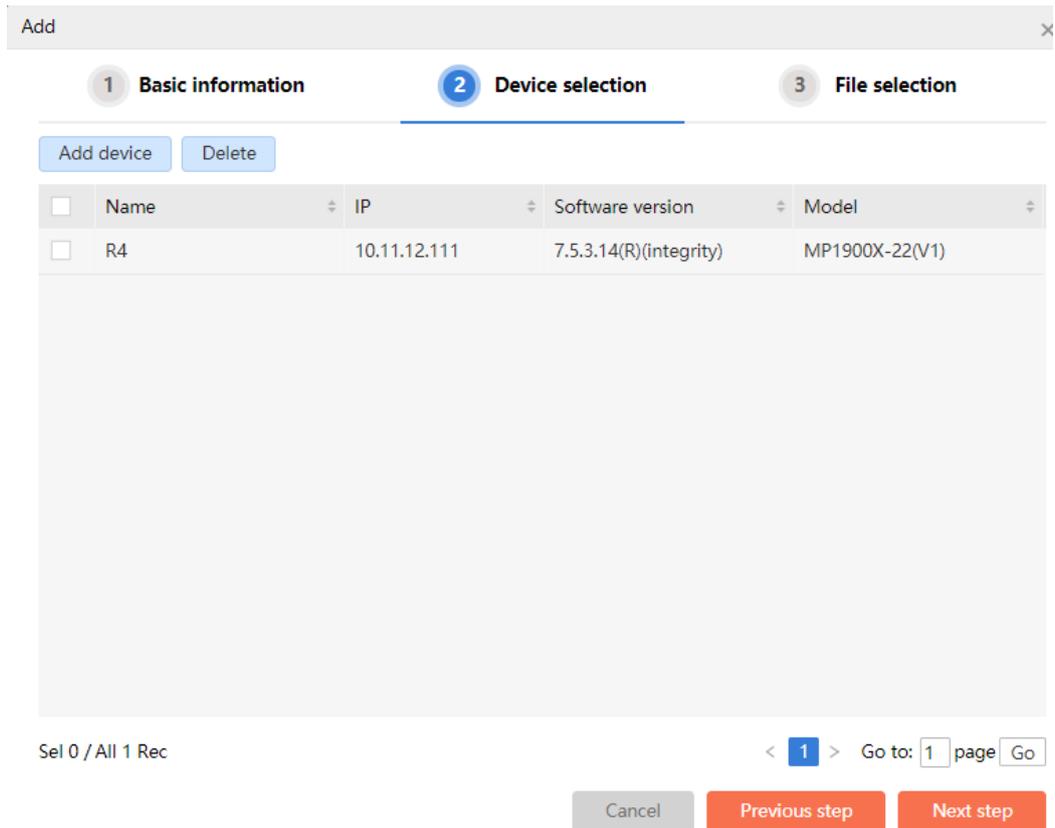


Figure 4-11 Add/modify task information-Step 2

Click “Next Step” to enter the “File selection” window, as shown in the following figure:

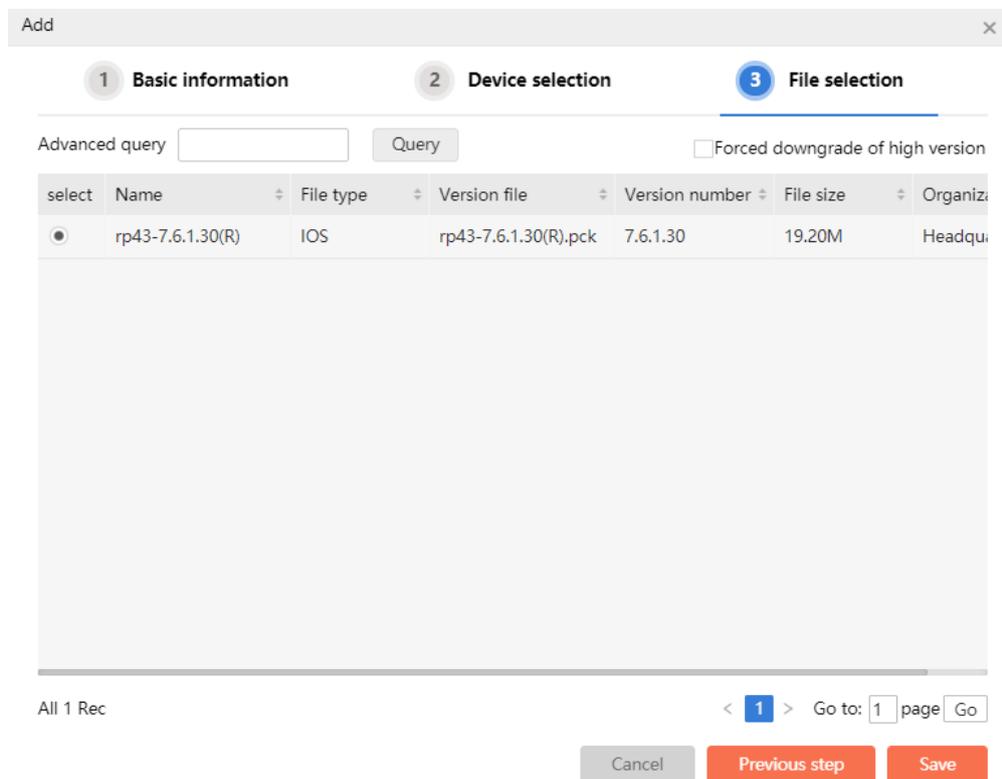


Figure 4-12 Add/modify task information-Step 3

In advanced query, you can query by name and version file.

Click **Save**, and adding software package update task is completed, the device starts to update the software package. The process of modifying the task is the same as above. Select the task to be modified in the task list, click the **Modify** button, and you can modify the task information.

**Note**

- If the file type is IOS, you can check the box of "Forced downgrade of high version" to perform version degradation.

**Delete the task:**

Select the task to be deleted in the task list, and then click **Delete** to delete the task that is no longer needed.

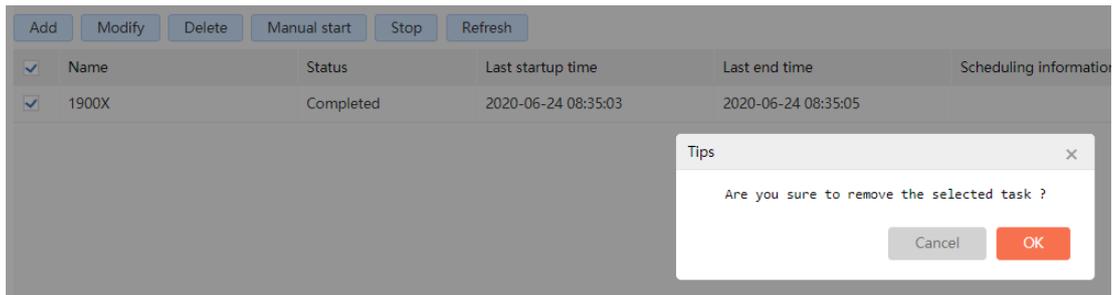


Figure 4-13 Delete the task information

**Note**

- The task in progress cannot be deleted. It can only be deleted after the task stops or runs.

**Manually enable/stop the task:**

Select a desired task and click **Stop** to stop the task. When the task stops, the device that has started continues to execute, and the device that has not started stops executing.

Select a stopped task and click **Manual start**. The task can run from the beginning again. At this time, the status of the task changes to "In progress".

**Refresh the task:**

Click "Refresh" in the task list box to immediately update the running status of all tasks, which is convenient for relevant personnel to view.

**View task details:**

Click "Details" of any task in the task list to open the "Task details" window of the task, as shown below:

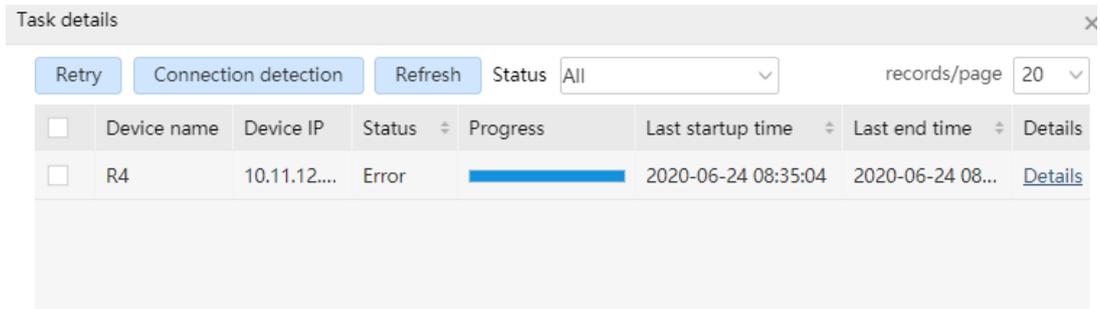


Figure 4-14 Task details

The "Task details" interface displays different devices under the same task by pages, showing the device name, device IP, status, progress, last start time, last end time, details and other information.

Select a piece of device update information and click **Retry** to restart the upgrade task of the device.

Select a piece of device update information and click **Connection detection** to view the connection status of the device, as shown in the following figure:

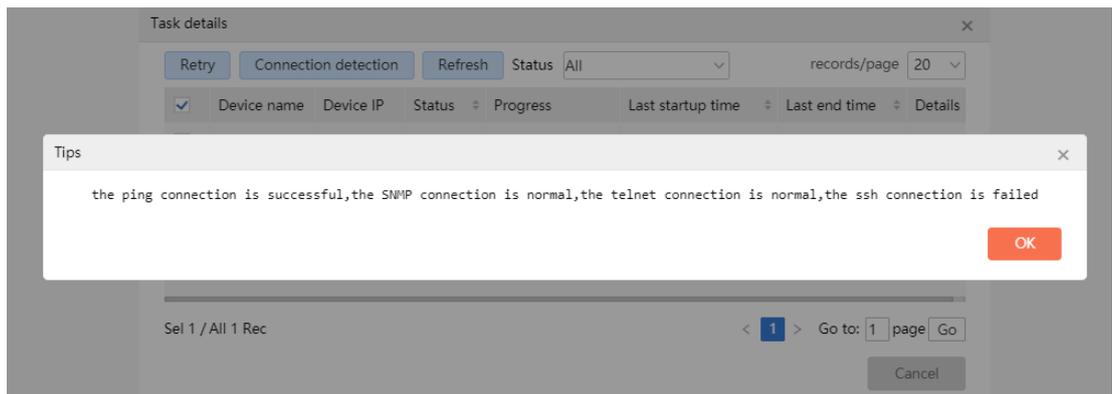


Figure 4-15 Device connection status

Click **Refresh** in the "Task details" window to update the status of all devices immediately.

Click "Details" of any device update in the task details list, and the "Execution details" window of the device will pop up, showing the detailed process of the device update, as

shown below:

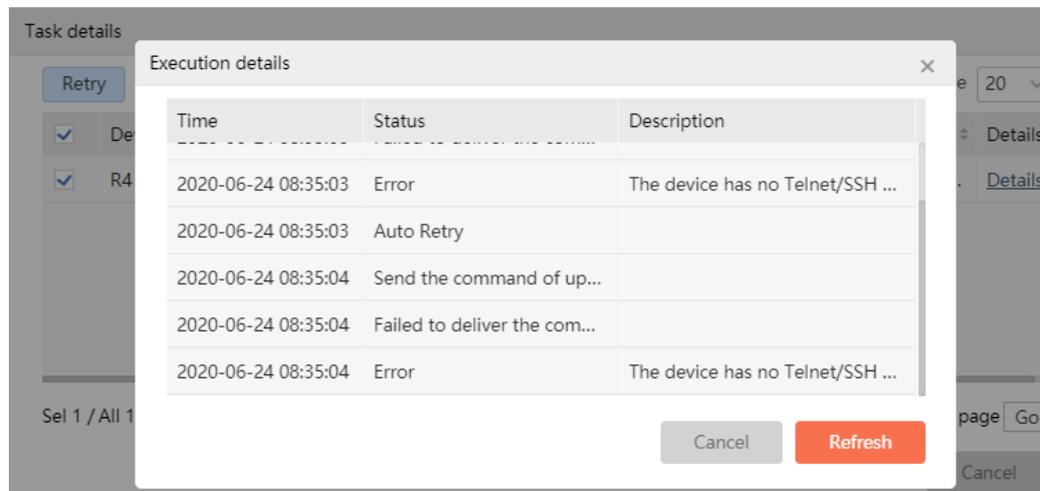


Figure 4-16 Device update execution details

**View task history:**

Click the history of any task in the task list to open the “Task history details” window of the task, as shown below:

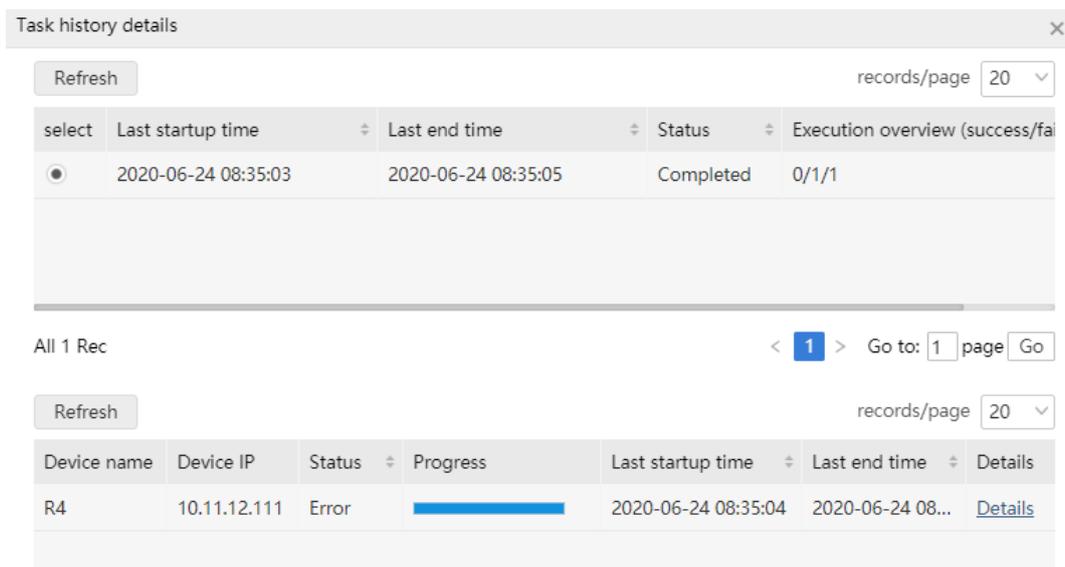


Figure 4-17 Task history details

The “Task history details” window is divided into two tables: “Historical execution” and “Details”.

The "Details" table is the same as the "Details" window of the device update, and you can view the specific details of the device update.

Select the corresponding device update history in the "History execution status" table, and the "Details" table will switch to the corresponding device update history task.

---

 **Note**

- For the newly added "in progress" tasks, their history cannot be viewed during operation. Only when the tasks are completed can the running history of tasks be viewed.
- 

The cases that the software package update may fail:

---

 **Note**

- The task execution fails, and connect/transfer timeout is reported in details.
- Reason: When discovering the device, discover by the management address of the network management server, and the management address of the network management server and device is reachable, but when the default routing egress interface address of the device cannot be reached, the task selects TFTP and FTP servers. When the device is used as the client to download the file, communicate by the default route egress interface address by default, and the files fail to be transmitted.
- Judgment method: Log into the device, ping the network management server address on the device, but ping is not successful; Ping can be connected by using the management address as the source address
- Solution: specify the source address of FTP/TFTP transmission on the device as the address accessible to the network management server. For example, configure the following command on the device (10.10.100.24 is the management address of the device)

```
ip ftp source-address 10.10.100.24
```

```
ip tftp source-address 10.10.100.24
```

---

## 4.2. Configuration File Management

### 4.2.1. Configuration File Management

The configuration file management module provides the management of device configuration files in the system, including adding, modifying, deleting, exporting, comparing configuration files, and querying configuration files.

Click "Resources" > "Configuration Management" > "Configuration File management" > "Configuration File management" in the top navigation bar of the system to open the "Configuration File management" interface, as follows:

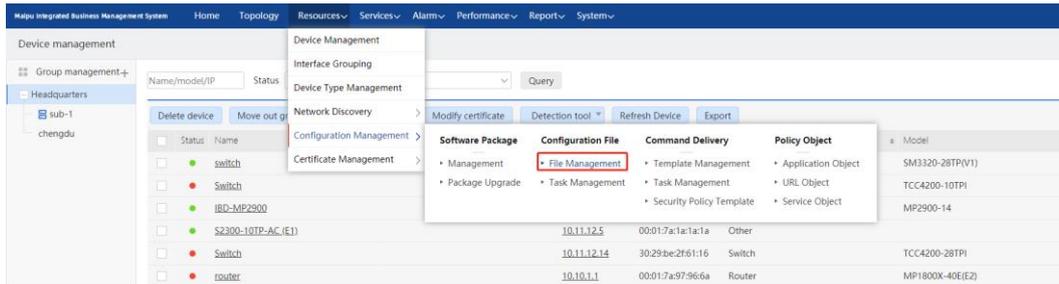


Figure 4-18 Configuration file management

**Configuration File list:**

Open the "Configuration File Management" interface and display all the device configuration files in the system by default, showing the name, device name, device alias, device IP, manufacturer, import type, file name, file size, baseline, update user, update time, affiliation, description, operation and other information of each configuration file by lists.

This page provides a variety of query conditions, you can easily and quickly query specific configuration files. Enter the corresponding query criteria in the configuration file query panel, and then click  to query all configuration files according to the fields such as name, device (name/alias/IP), whether it is baseline, warehousing start time, warehousing end time; click the fields in the header of configuration file list to sort the configuration files according to the corresponding fields.

As shown in the figure below, all configuration files with the name of "MP2900" and device IP of "10.11.12.254" are found and sorted according to the names of the configuration files:

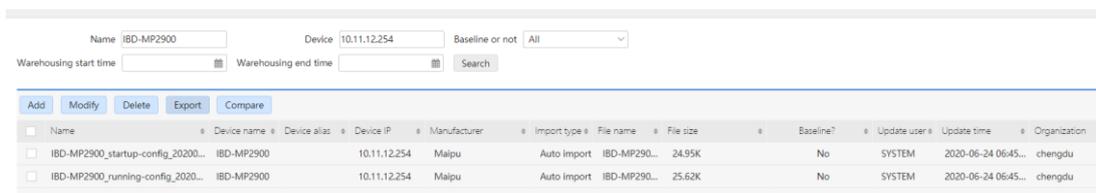


Figure 4-19 Configuration file query and sorting

**Caution**

- Organization: the organization and its subordinate organizations of the current administrator.

**Add/modify configuration file:**

Click  in the configuration file list panel to open the "Add" window, select the device and configuration file, fill in the name and description of the configuration file, as

shown in the following figure:

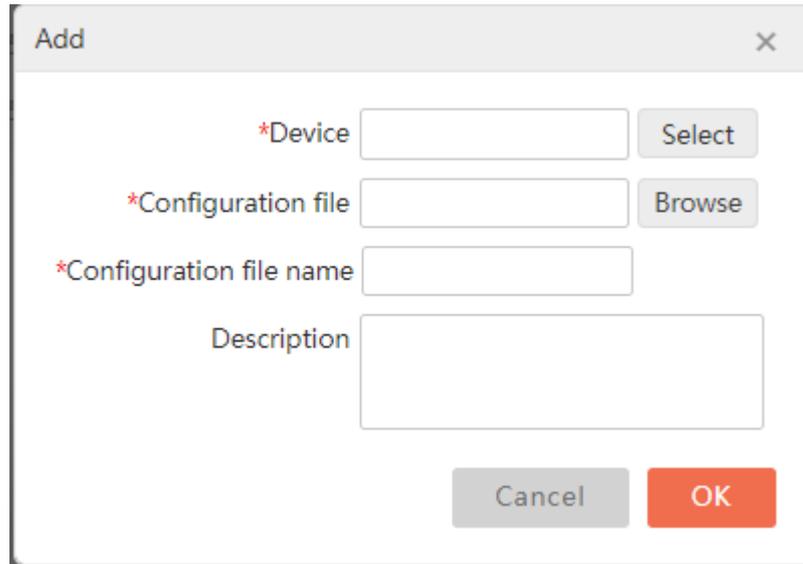


Figure 4-20 Add configuration file

Click **OK** to add the configuration file. The process of modifying the configuration file is the same as above. Select the configuration file to be modified in the configuration file management list and click **Modify** to modify it.

**Export configuration file:**

Select the desired configuration file from the configuration file management list and click **Export** to export the configuration file.

**Delete configuration file:**

Select the desired configuration file in the configuration file list, and click **Delete** to delete the configuration file, as shown in the following figure:

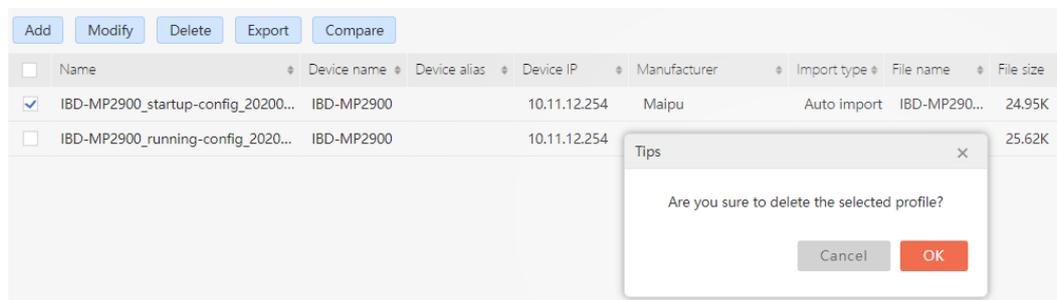


Figure 4-21 Delete configuration file

**Compare configuration files:**

Select the two desired configuration files in the configuration file list, and click **Compare** to compare the configuration files, as shown in the following figure:

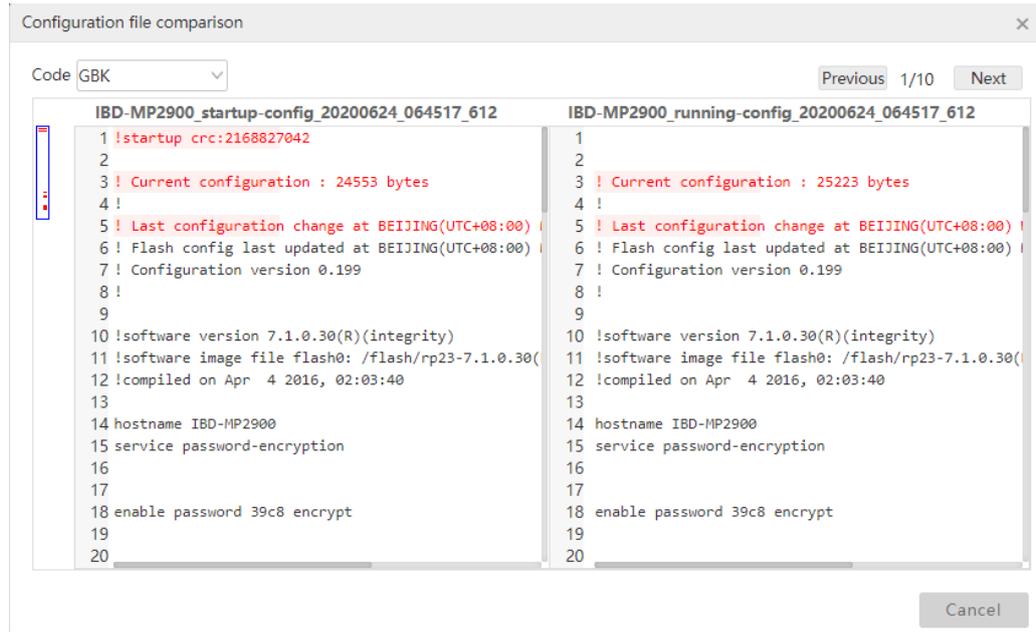


Figure 4-22 Compare configuration files

**Modify configuration files:**

Select the desired configuration file in the configuration file list, and click  to enter the interface of modifying the configuration file, as shown in the following figure:

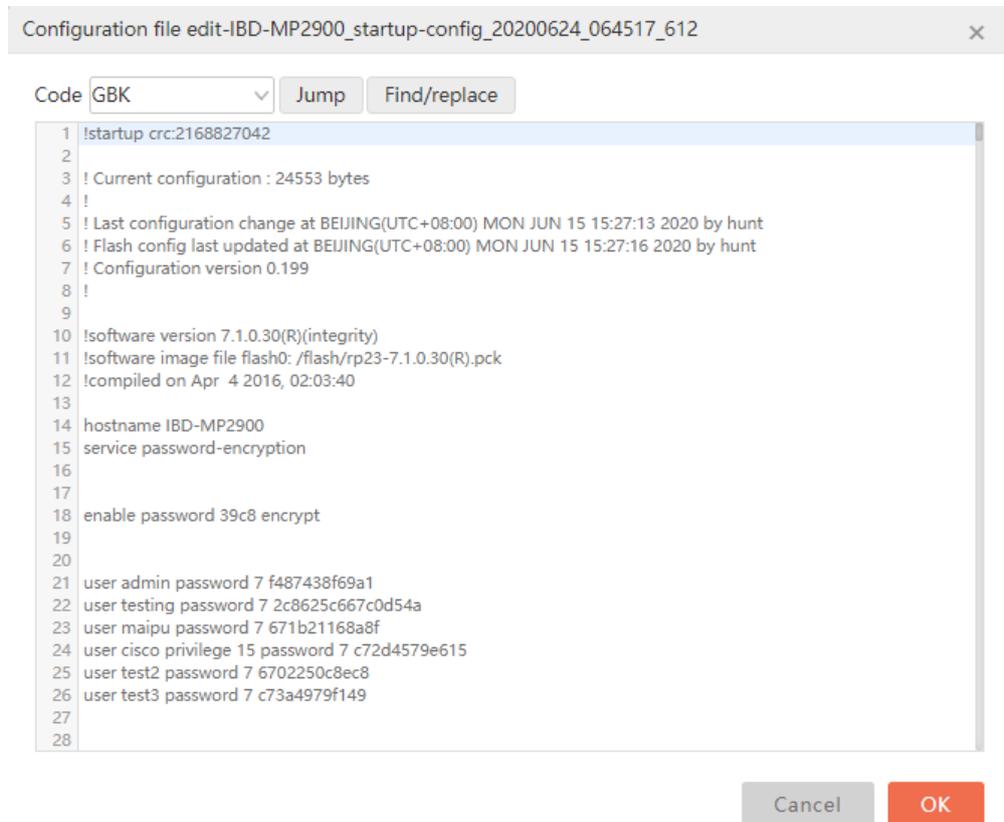


Figure 4-23 Modify configuration file

Click the "Jump" button to jump to the corresponding configuration line, as shown in the

figure below.

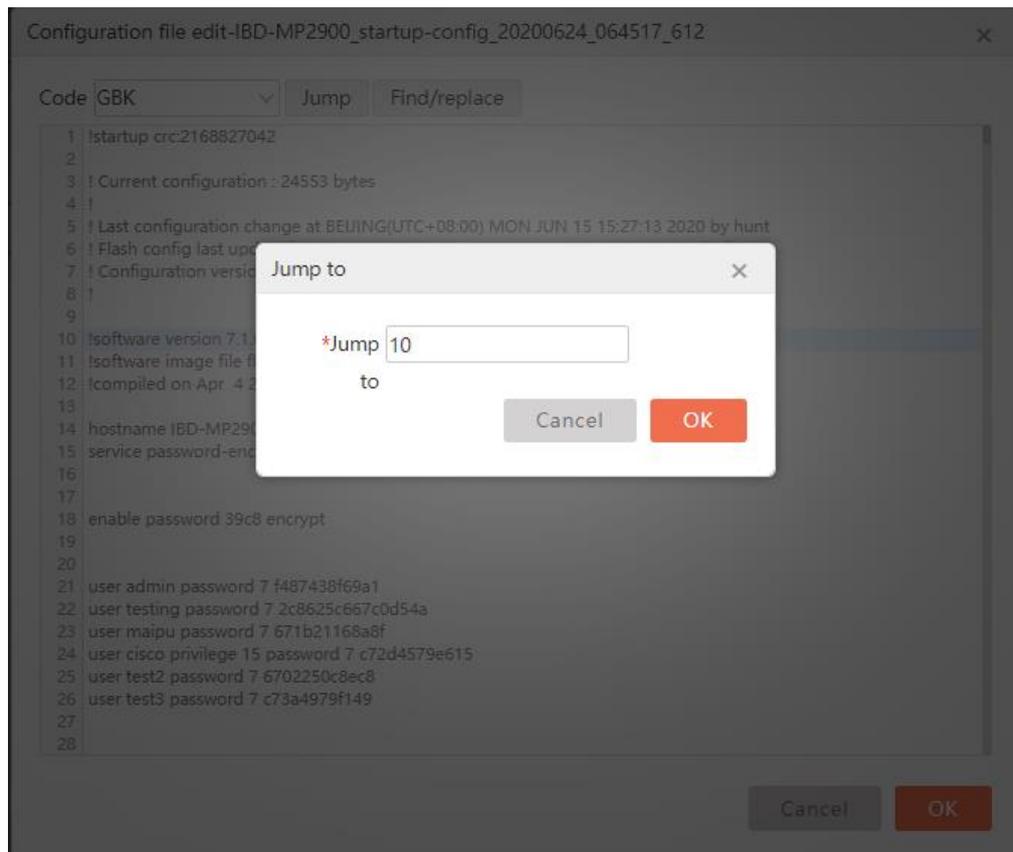


Figure 4-24 Jump to the specified line

Click the "Find/Replace" button to search and replace the configuration file. At the same time, you can choose whether to use case sensitive and whether to use regular expressions, as shown in the following figure:

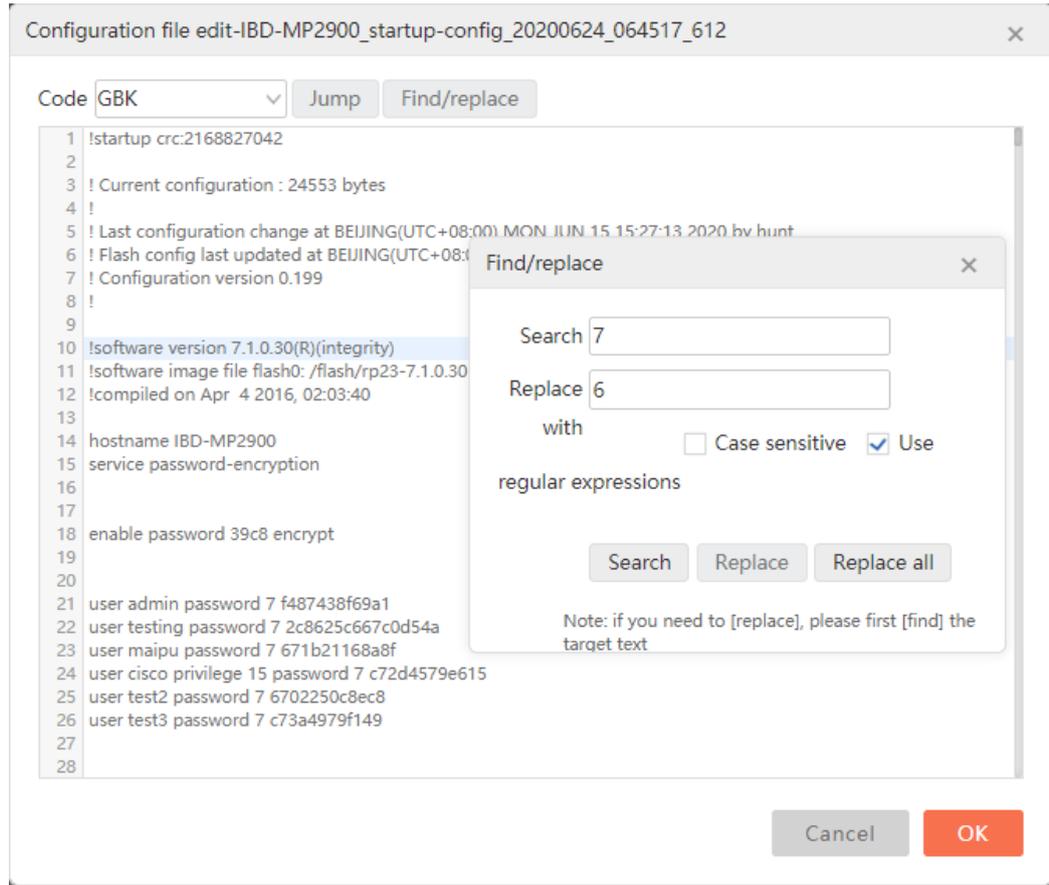


Figure 4-25 Search/replace configuration file

**Set baseline:**

Select the desired configuration file in the configuration file list, click , and the file can be set as the baseline file, as shown in the following figure:

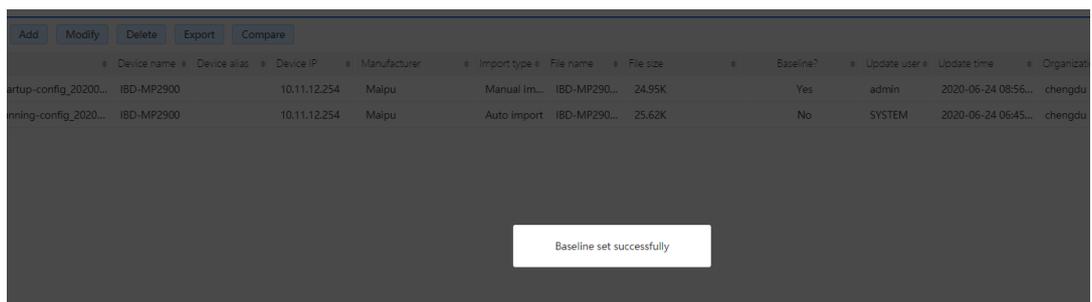


Figure 4-26 Set the file as baseline

**Cancel baseline:**

Select the desired configuration file in the configuration file list, click , and you can cancel the baseline, as shown in the following figure:

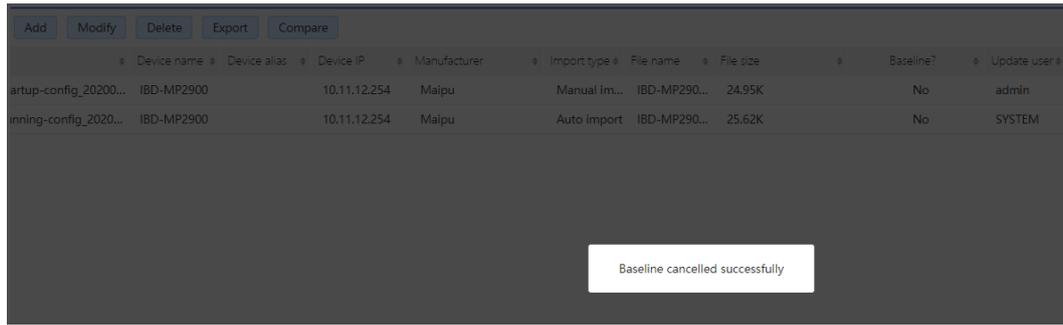


Figure 4-27 Cancel the baseline

One device can only have one baseline file. If the device already has baseline file, the system will prompt when setting repeatedly, as shown in the following figure:

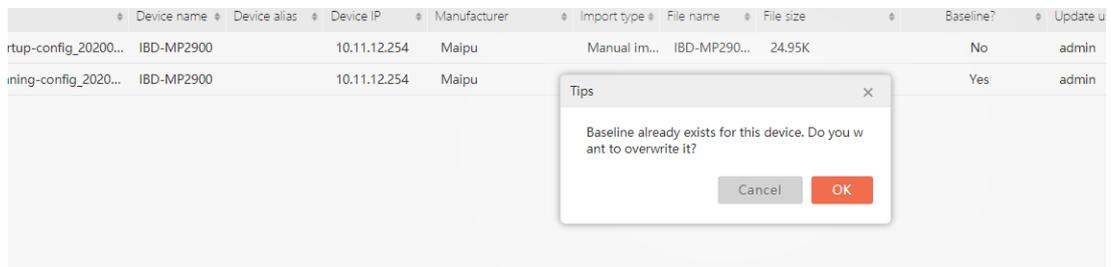


Figure 4-28 Set baseline repeatedly

Click  to overwrite the previous set baseline. Click , and the previous set baseline will not be overwritten.

### 4.2.2. Configuration Change Task

The configuration change task management module can back up or restore the configuration file of the specified device, including adding, modifying, deleting, manually starting, stopping and refreshing the configuration change task, and querying the configuration change task.

Click "Resources" > "Configuration Management" > "Configuration File Management" > "Configuration Change Task" on the top navigation bar of the system to open the "Configuration Change Task Management" page, as follows:

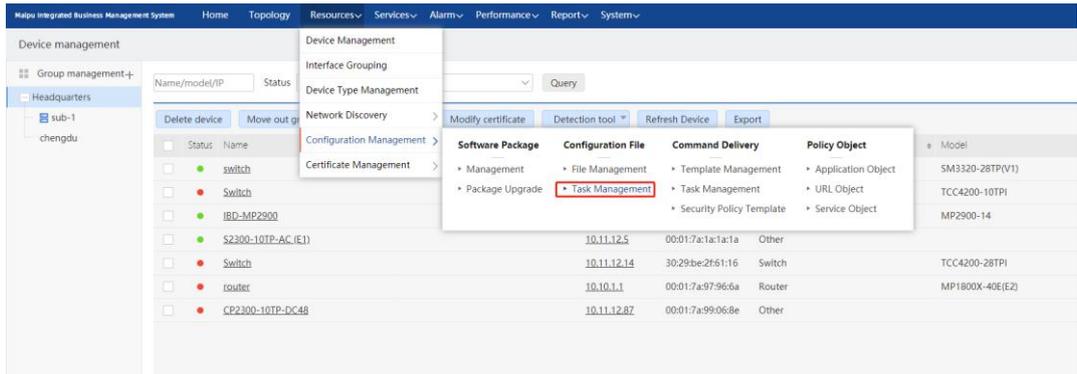


Figure 4-29 Configuration change task management

**Task list:**

Open the "Configuration Change Task Management" interface and display all configuration change tasks in the system by default, showing the name, status, type, last start time, last end time, scheduling information, baseline comparison, description, recent execution, update user, organization, details and history of each task by lists.

This page provides a variety of query conditions, you can easily and quickly query specific tasks, enter the corresponding query criteria, and then click the "Query" button to query all tasks according to the name, organization, status, type, start time, end time and other fields; you can click the "Organization" field in the head of the task list to sort;

As shown in the figure below, all tasks with the name of "Configuration Change Task", the organization of "Headquarters" and the status of "completed" are found out

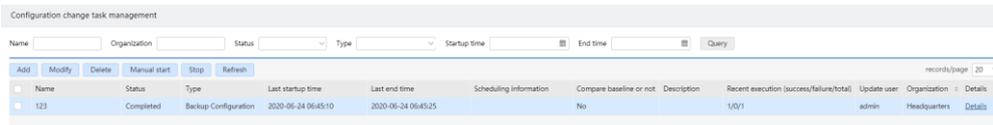


Figure 4-30 Configuration change task query

**! Caution**

- Organization: the organization and its subordinate organizations of the current administrator.

**Add/Modify configuration backup task:**

Click **Add** in the task table panel to open the "Add" window, as shown in the figure below. Fill in the task name, select the task type, baseline comparison, file server, execution method and description. Select the "Advanced configuration" option, you can also set the auto retry times, timeout, and whether to support VRF.

Figure 4-31 Add configuration backup task-Step 1

## Caution

- In the configuration change task, the device concurrency number of the current single task is 10, and the task concurrency number is 3.
- By default, the auto retry times is 1, and the timeout is two minutes.
- By default, select “Not support VRF”.

Baseline comparison: Only tasks of type "configuration backup" have baseline comparison option. When "Yes" is selected, if the device has not set baseline file, the backup startup file will be automatically set as the baseline file. If the device has set baseline file, the backup startup file and baseline file will be used for comparison. If it is different from baseline file, send alarm; When "no" is selected, it will neither be compared with the baseline file, nor will the backup startup file be set as the baseline file.

File server: By default, configuration change uses the local TFTP server for transferring files. If some devices do not support the TFTP command upgrade, you can use the local FTP server to upgrade. When choosing TFTP, you do not need to input the user name and password, but FTP needs to input the user name and password (FTP user name and password are the FTP user name and password configured by the user when installing the network management system). You can also use the remote FTP server to upgrade. When selecting the remote FTP server, you need to input the FTP address, user name

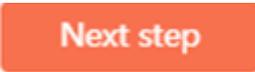
and password.

Execution mode: When "Execute immediately" is selected, the task can be executed immediately after the task information is configured; if "Timing execution" is selected, the task will be executed after the set time period; if "loop execution" is selected, start execution in a fixed time range of a fixed period.

Auto retry times: If adding software package fails, it will automatically retry. The number of retries is the given value.

Timeout: When the task is executed, the time for waiting device response exceeds the set timeout, and the task execution fails.

Support VRF: By default, it is "No". VRF is VPN routing forwarding table, which is a special entity established and maintained by PE for directly connected sites.

Click  to enter the "Device selection" window, as shown in the figure below:

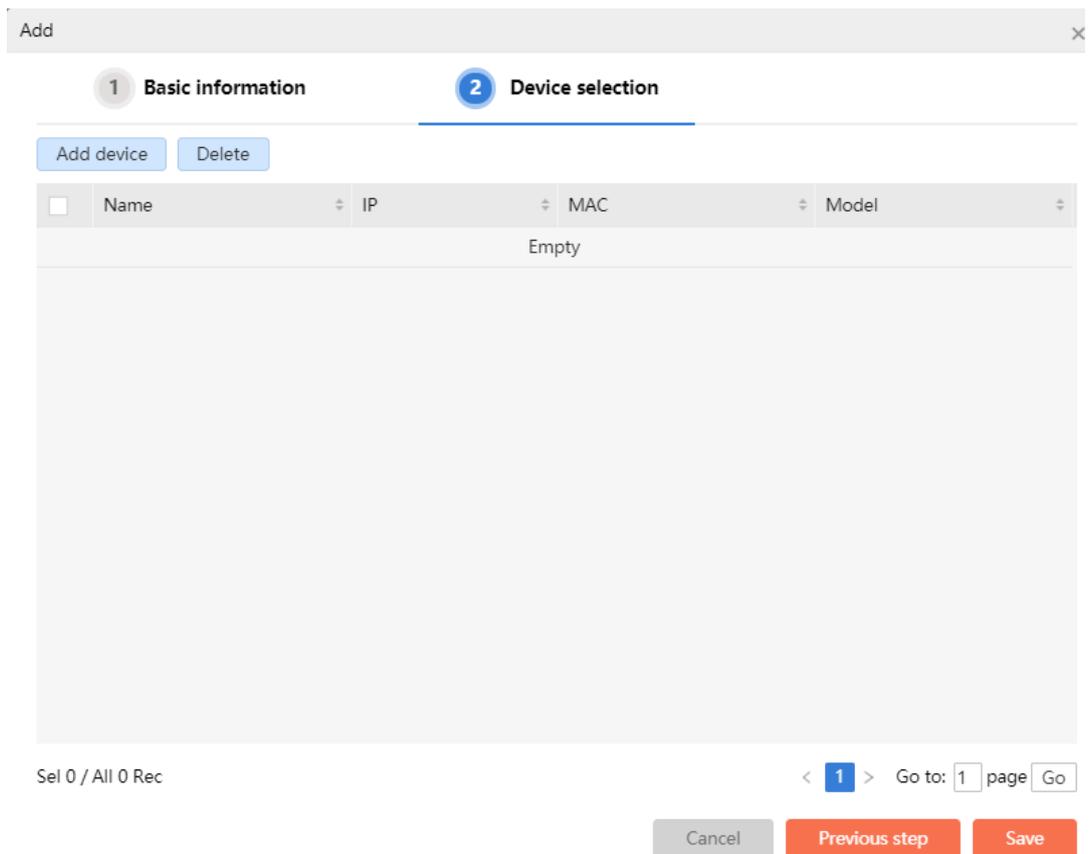


Figure 4-32 Add configuration backup task-step 1

Click "Add device", select the corresponding device for the task, and enter the "Select device" window, as shown in the figure below:

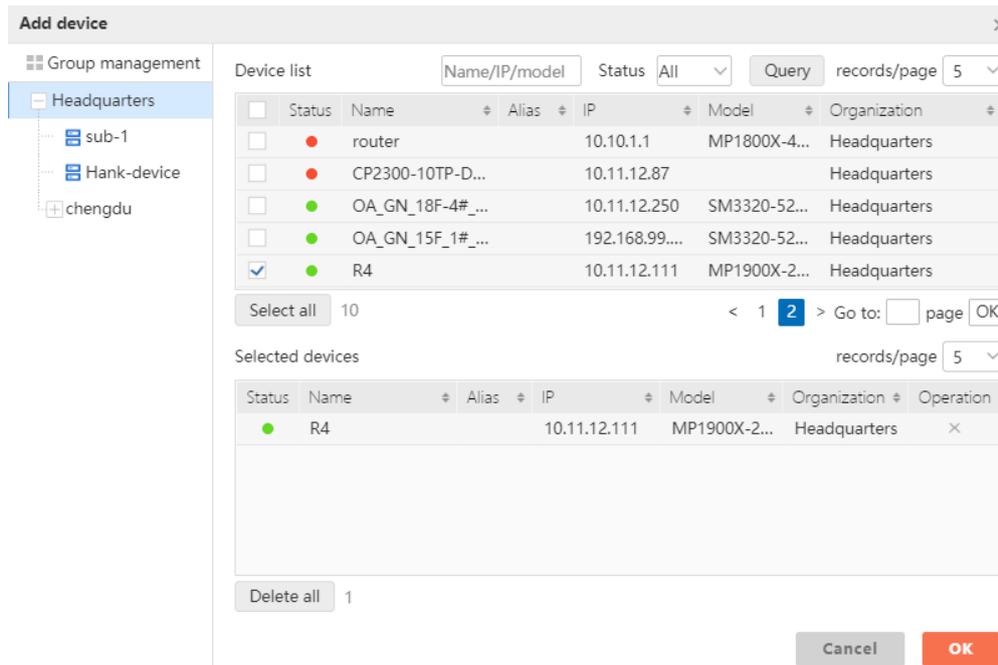


Figure 4-33 Select the device

Select the device, support multiple selection, and click “OK” to select the device for the configuration backup task, as shown in the following figure:

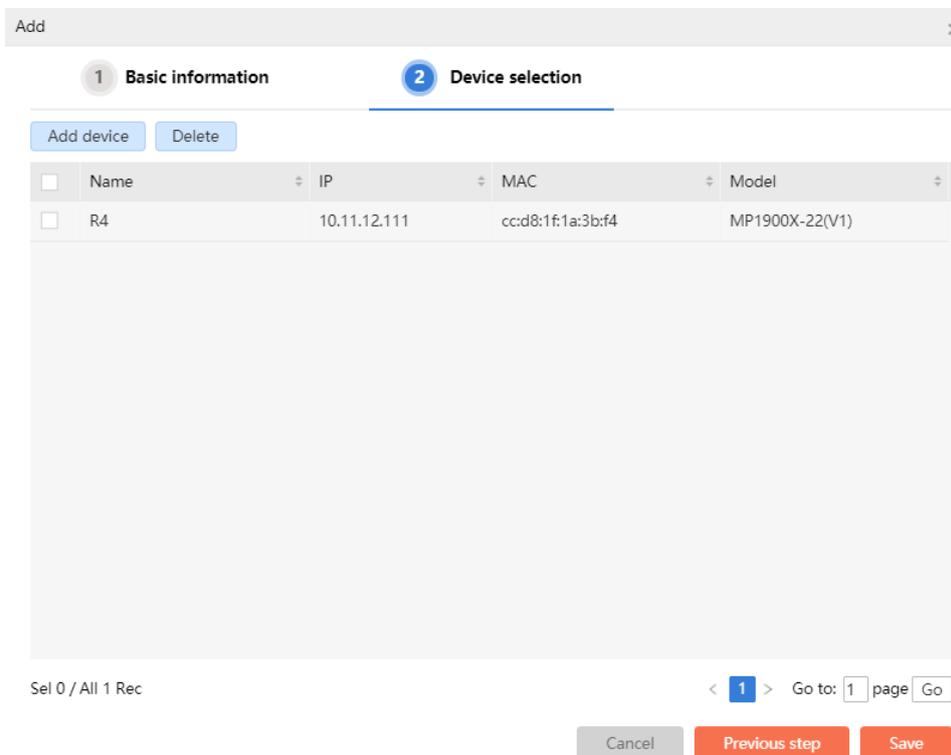
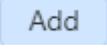


Figure 4-34 Add configuration backup task-step 2

Click **Save** to add the configuration backup task, and the device starts the configuration backup task. The process of modifying the task is the same as above.

Select the desired task in the task list and click  to modify the task information.

**Add/modify configuration recovery task:**

Click  in the task table panel to open the "Add" window, fill in the task name, select "Configuration Recovery" for the type, fill in auto retry times, timeout, and description, and select the corresponding options, as shown in the following figure:

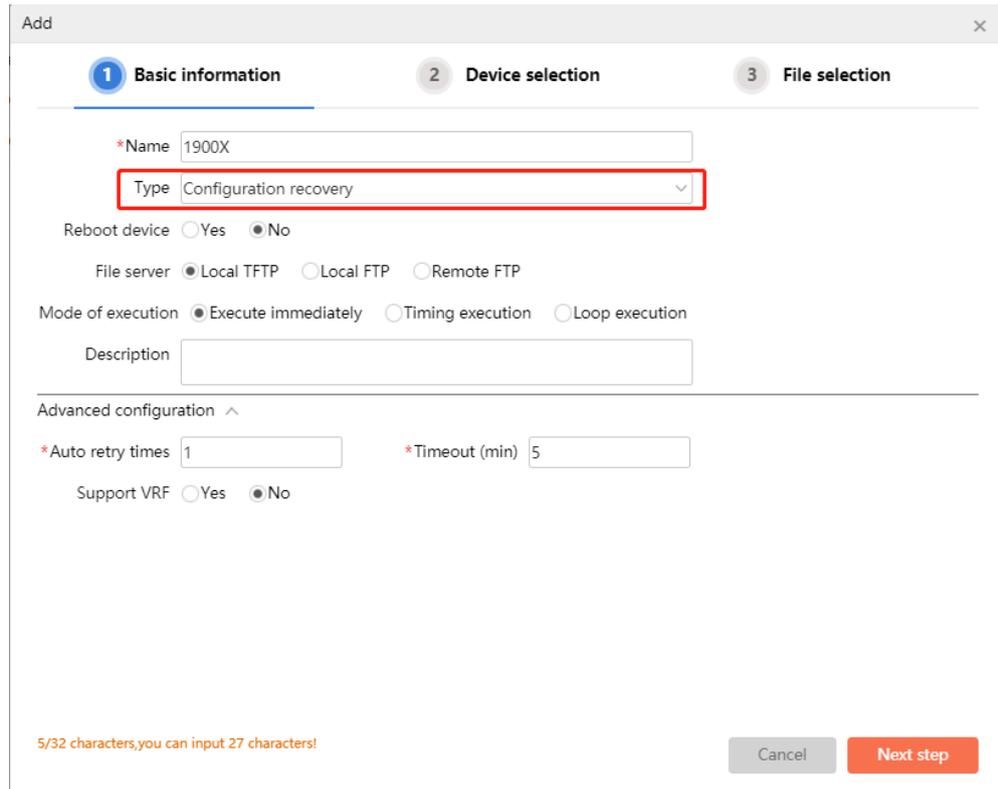


Figure 4-35 Add configuration recovery task-step 1

**File server:** By default, configuration change uses the local TFTP server for transferring files. If some devices do not support the TFTP command upgrade, you can use the local FTP server to upgrade. When choosing TFTP, you do not need to input the user name and password, but FTP needs to input the user name and password (FTP user name and password are the FTP user name and password configured by the user when installing the network management system). You can also use the remote FTP server to upgrade. When selecting the remote FTP server, you need to input the FTP address, user name and password.

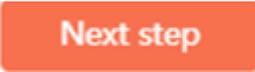
**Reboot device:** If it is checked, the device will be restarted after the device configuration recovered successfully. If the recovery fails, record the error message, and do not restart the device.

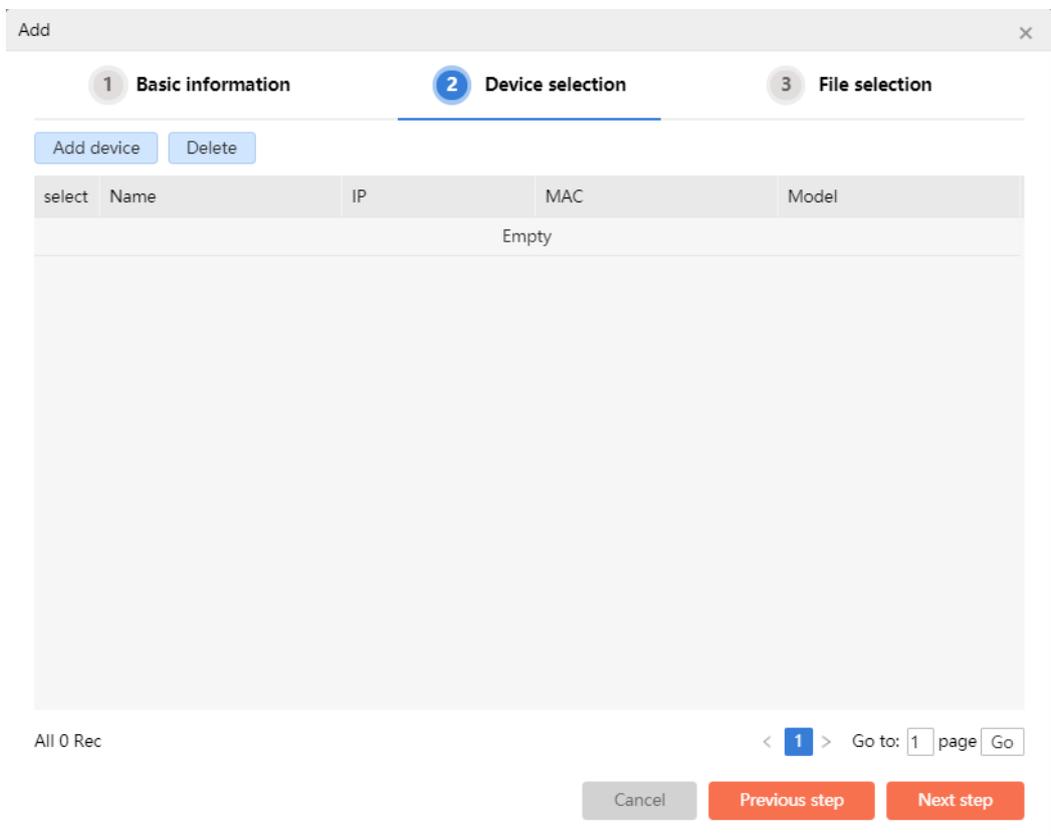
**Auto retry times:** If adding software package fails, it will automatically retry. By default, it

is once.

**Timeout:** When the task is executed, the time for waiting device response exceeds the set timeout, and the task execution fails.

**Execution mode:** When "Execute immediately" is selected, the task can be executed immediately after the task information is configured; if "Timing execution" is selected, the task will be executed after the set time period; if "loop execution" is selected, start execution in a fixed time range of a fixed period.

Click  to enter the "Device selection" window, as shown in the figure below:



select	Name	IP	MAC	Model
Empty				

Figure 4-36 Add configuration recovery task-step 2

Click "Add device", select the device, and you can only select one device, as shown in the figure below:

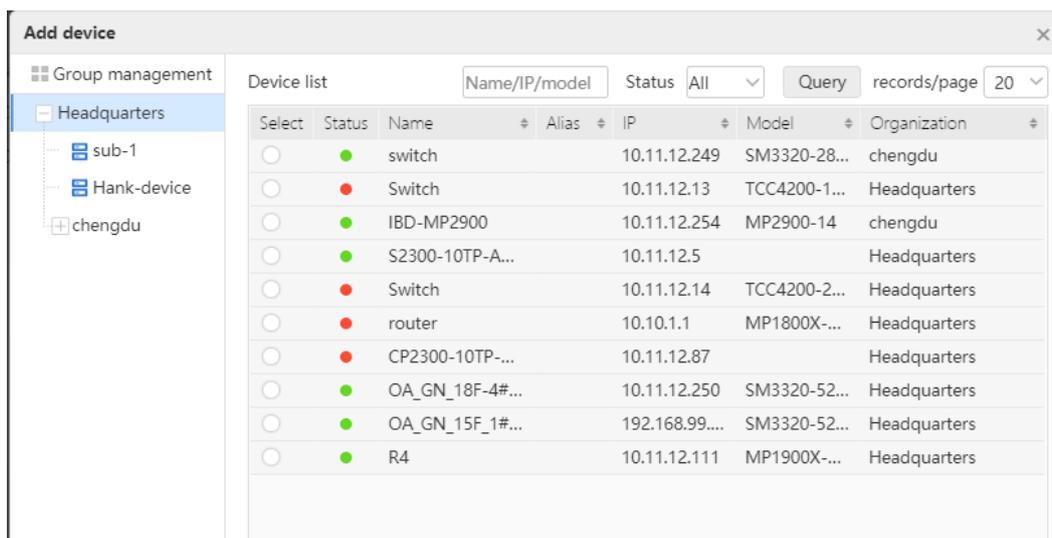


Figure 4-37 Add configuration recovery task-step 3

Click **OK** to complete the selecting of the device, as shown in the following figure:

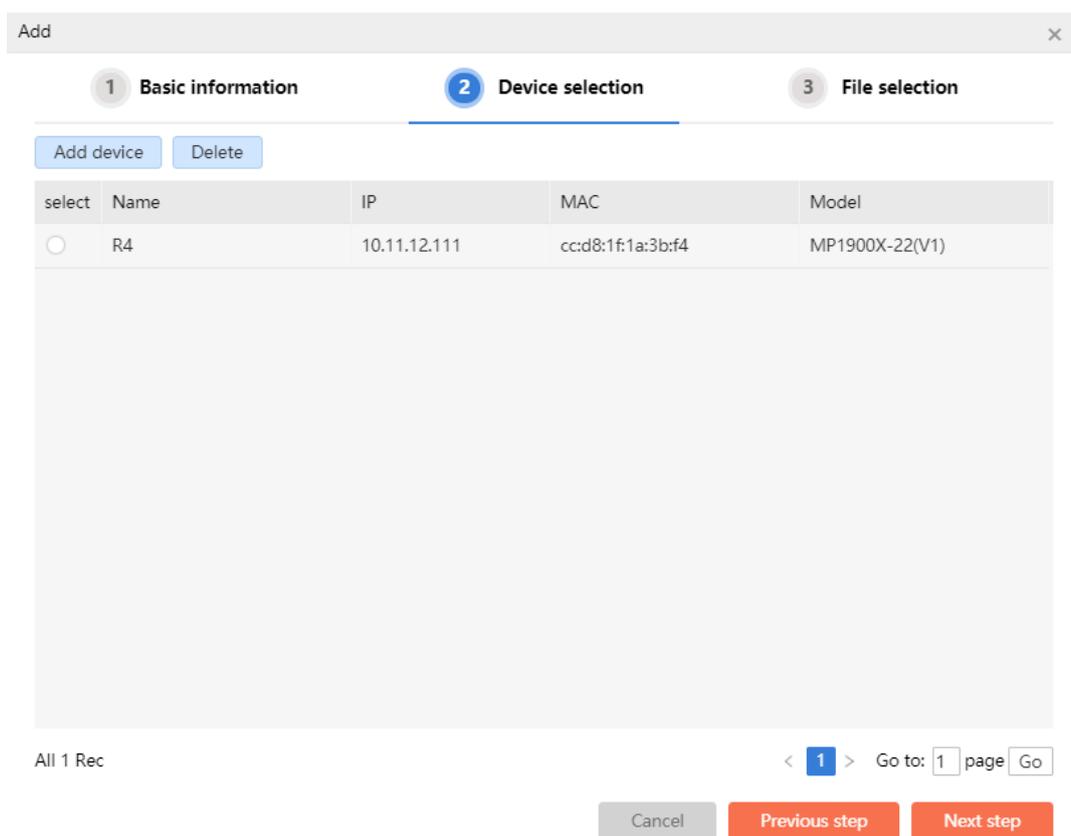


Figure 4-38 Add configuration recovery task-step 4

Click **Next step** and select the configuration file. The configuration file will be matched according to the selected device. You can also query the configuration file according to the name and storage time, as shown in the following figure:

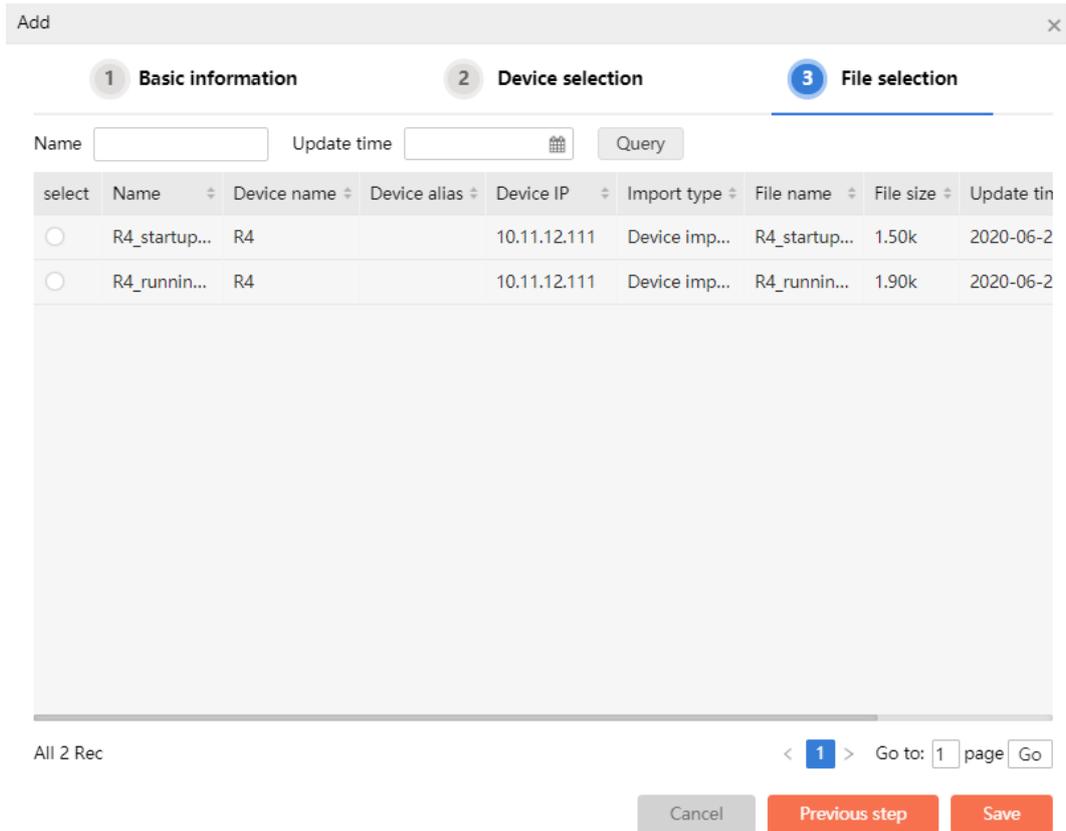


Figure 4-39 Add configuration recovery task-step 5

Click **Save**, adding configuration recovery task is completed, and the device starts the configuration recovery task. The process of modifying the task is the same as above.

Select the desired task in the task list, click the **Modify** button, and you can modify the task information.

**Delete the task:**

Select the desired task in the task list, and then, click **Delete** to delete the task that is no longer needed.

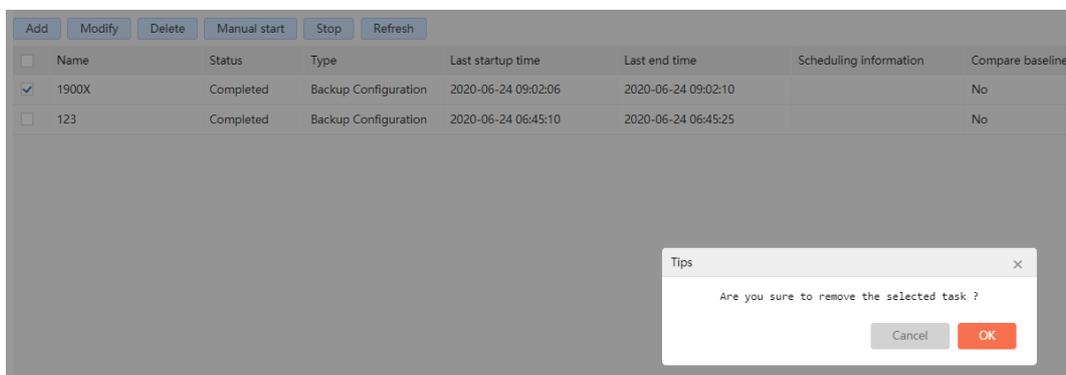


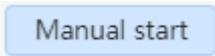
Figure 4-40 Delete the task information

 **Note**

- The task in progress cannot be deleted. It can only be deleted after the task stops or runs.

**Manually start/stop the task:**

Select a desired task, and click  to stop the task. When the task stops, the device that has started continues to execute, and the device that has not started stops executing.

Select a stopped task and click . The task can run from the beginning again. At this time, the status of the task changes to "in progress".

**Refresh the task:**

Click  in the task list box to immediately update the running status of all tasks, which is convenient for relevant personnel to view.

**View task details:**

Click the details of any task in the task list to open the "Task details" window, as shown below:

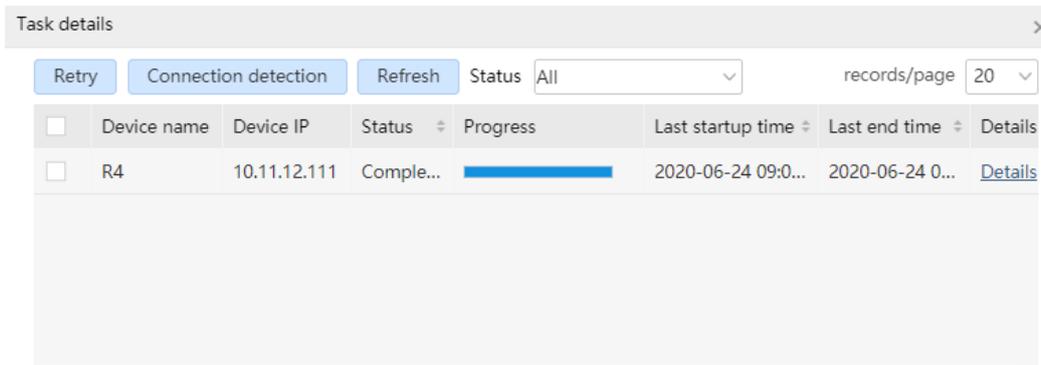
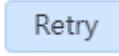


Figure 4-41 Task details

The "Task details" interface displays different devices under the same task by pages, showing the device name, device IP, status, progress, last start time, last end time, details and other information of the device configuration.

Select a piece of device configuration information and click  to restart the configuration task of the device.

Select a piece of device configuration information and click  to

view the connection status of the device, as shown in the following figure:

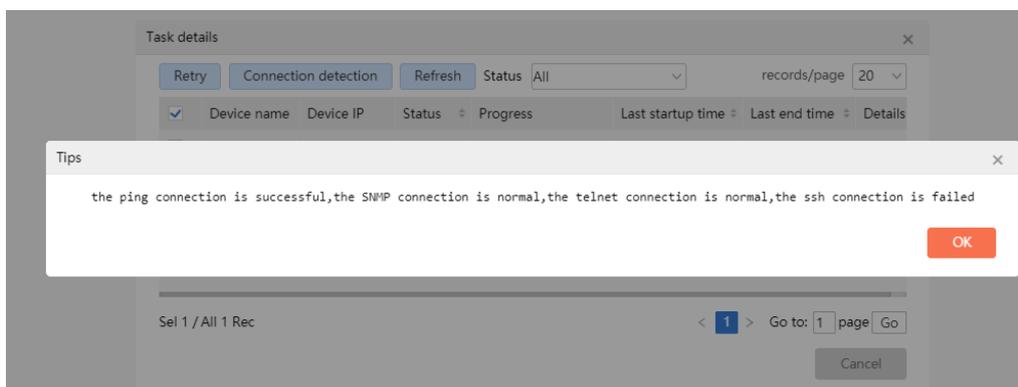


Figure 4-42 Device connection status

Click **Refresh** in the "Task details" window to update the status of all tasks immediately.

Click "Details" of any configuration task in the task details list, and the "Execution details" window of the device will pop up, showing the detailed process of the configuration file backup, as shown below:

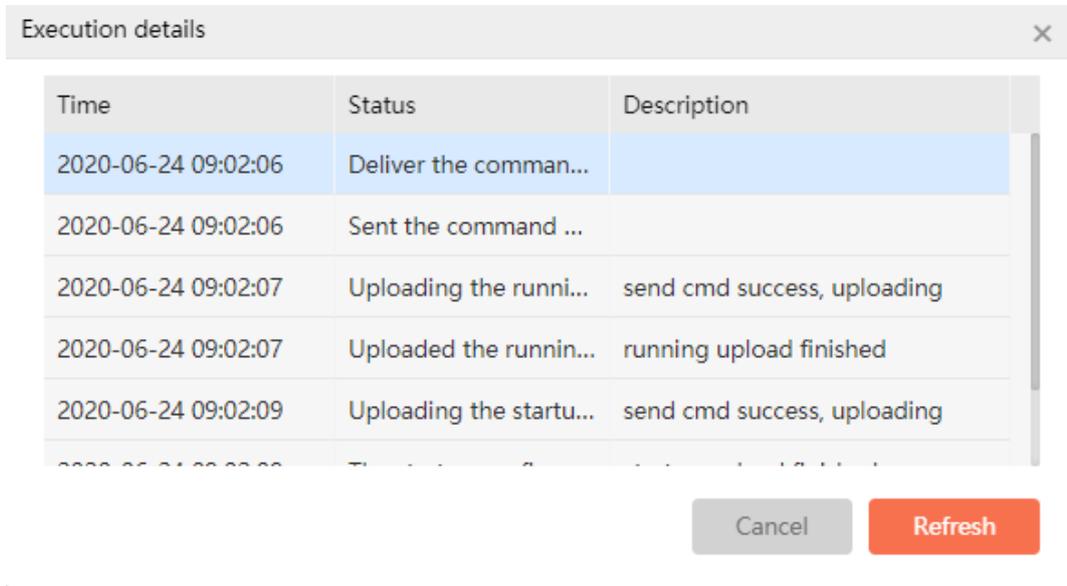


Figure 4-43 Execution details of the configuration backup

**View task history:**

Click the history of any task in the task list to open the "Task history details" window of the task, as shown below:

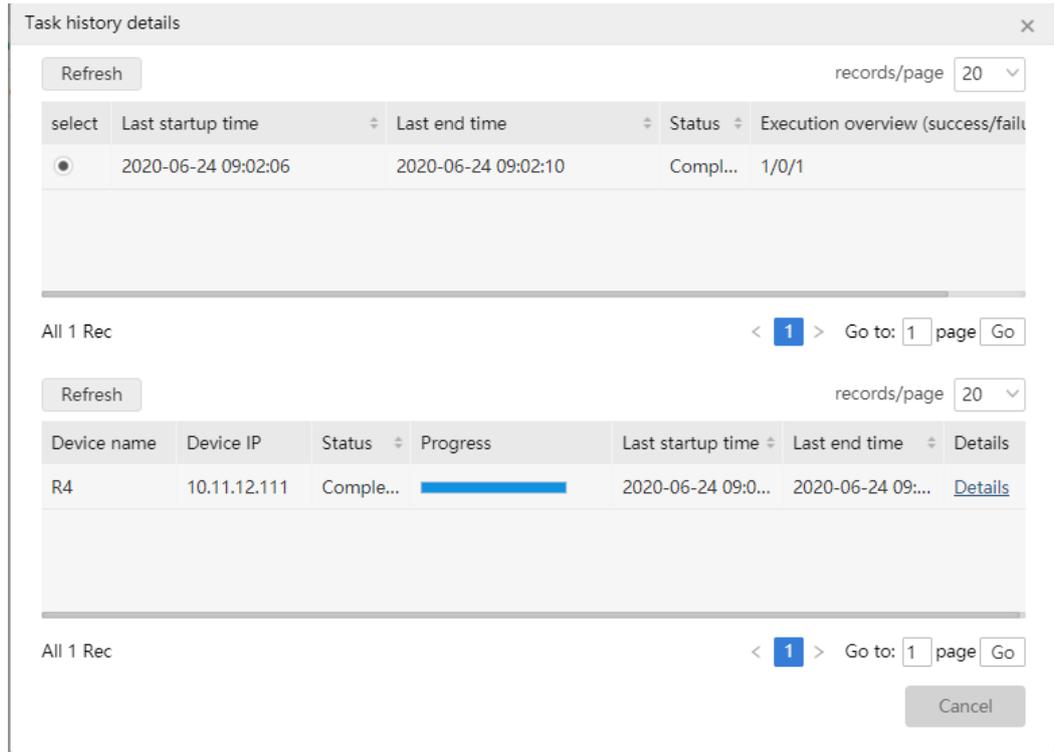


Figure 4-44 Task history details

The "Task history details" window is divided into two tables: "Historical execution" and "Details".

The "Details" table is the same as the "Details" window of the device configuration, and you can view the specific details of the device configuration.

Select the corresponding device configuration history in the "History execution status" table, and the "Details" table will switch to the corresponding device configuration history task.

 **Note**

- For the newly added "in progress" tasks, their history cannot be viewed during operation. Only when the tasks are completed can the running history of tasks be viewed.

The cases that the task execution may fail:

 **Note**

- The task execution fails, and connect/transfer timeout is reported in details.
- Reason: When discovering the device, discover by the management address of the network management server, and the management address of the network management server and device is reachable, but when the default routing egress

interface address of the device cannot be reached, the task selects TFTP and FTP servers. When the device is used as the client to download the file, communicate by the default route egress interface address by default, and the files fail to be transmitted.

- Judgment method: Log into the device, ping the network management server address on the device, but ping is not successful; Ping can be connected by using the management address as the source address
- Solution: specify the source address of FTP/TFTP transmission on the device as the address accessible to the network management server. For example, configure the following command on the device (10.10.100.24 is the management address of the device)

```
ip ftp source-address 10.10.100.24
```

```
ip tftp source-address 10.10.100.24
```

### 4.3. Configuration Command Delivering

#### 4.3.1. Command Template Management

The command template management module provides the management for the configuration command template delivered to the device, including adding, importing, modifying and deleting command template, as well as the query of command template.

Click "Resources" > "Configuration Management" > "Configuration Command Delivery" > "Command Template Management" on the top navigation bar of the system to open the "Command Template Management" page, as follows:

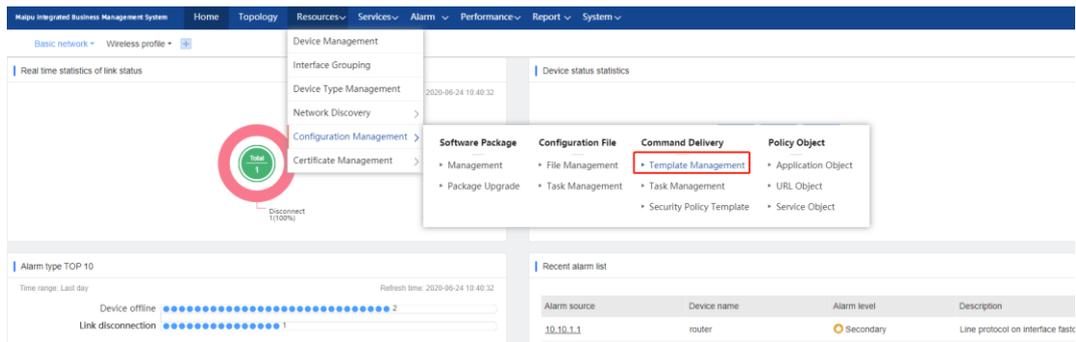


Figure 4-45 Command template management

#### Command template list:

Open the "Command Template Management" interface and display all the command templates in the system by default. The name, description, update time, update user, organization, and view content of each command template are displayed by lists. The page provides various query conditions, convenient for querying specific command templates quickly.

In the command template query panel, you can query the corresponding template according to the organization and advanced query. The advanced query can query according to the template name; enter the corresponding query criteria, and then click  to find the matching template; click the fields in the head of the command template list to sort the command templates according to the corresponding fields.

As shown in the figure below, the command template with "Headquarters" as its organization and "Command Template" as advanced query are found:



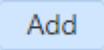
Template name	Description	Update time	Update user	Organization	View content
switch-Testing	switch	2020-05-27 08:29:45	admin	Headquarters	View content

Figure 4-46 Command template query

## Caution

- Organization: the organization and its subordinate organizations of the current administrator

### Add a command template:

Click  in the command template list panel to open the "Add" window, and fill in the template name, template content and template description, as shown in the following figure:

**Add** [X]

\*Template name

\*Template content

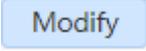
The command must be a configuration command, which is executed in configuration mode by default.

**Note:**  
After modifying the contents of the command template, you need to reselect the template in the task.

Template description

Cancel OK

Figure 4-47 Add a command template

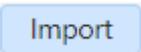
Click  to add the command template. The process of modifying the command template is the same as above. Select the desired command template in the command template management list and click  to modify it.

---

## Caution

- The command to be delivered must be a configuration command, which will be executed in the configuration mode by default.
  - After modifying the command template, it is necessary to re select the template in the task.
- 

### Import the command template:

Click  in the command template list panel to open the "Import" window, fill in the template name and template description, and select the template file, as shown in the following figure:

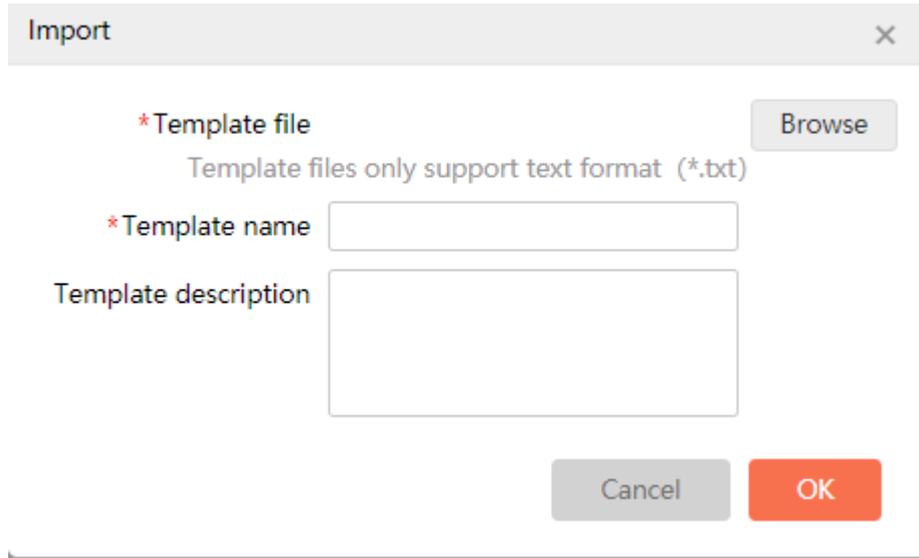
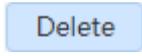


Figure 4-48 Import the command template

Click  to complete the importing of the command template.

**Delete the command template:**

Select the desired command template from the command template list, and click

 to delete the command template file, as shown in the following figure:

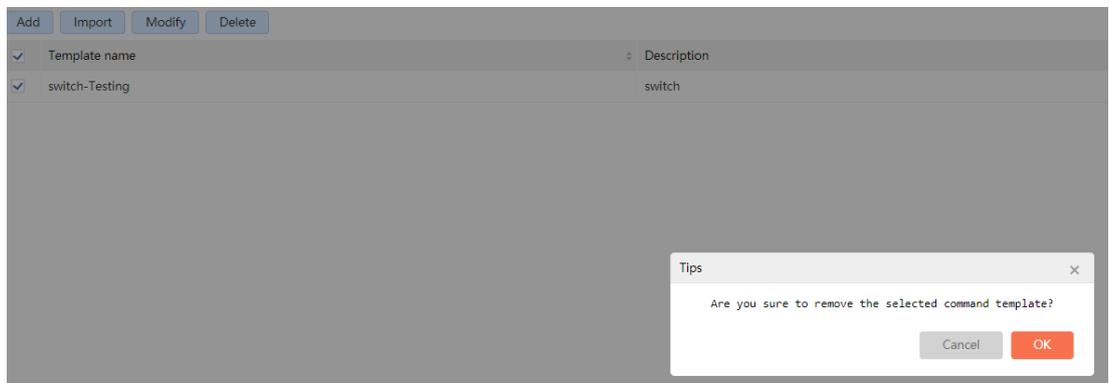


Figure 4-49 Delete the command template

**4.3.2. Command Delivery Task**

Command delivery task management module can deliver the configuration commands for the specified device, including adding, modifying, deleting, manually starting, stopping, refreshing and other operations of configuration command delivery tasks, as well as query of command delivery tasks.

Click "Resources" > "Configuration Management" > "Configuration Command Delivery" > "Command Delivery Task" on the top navigation bar of the system to open the "Command Delivery Task Management" page, as follows:

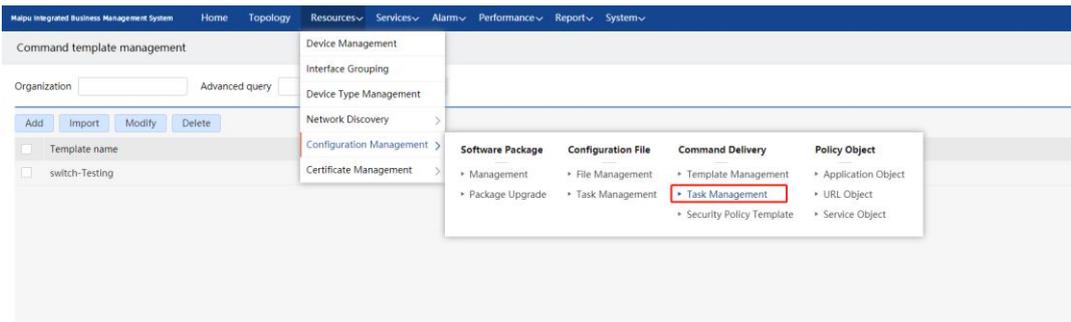


Figure 4-50 Command delivery task management

**Task list:**

Open the "Command Delivery Task Management" interface, and display all tasks in the system by default. The name, status, last start time, last end time, scheduling information, description, recent execution status, update user, organization, view command, details, and history of each task are displayed by lists.

This page provides a variety of query conditions, and you can easily and quickly query specific tasks. Enter the corresponding query criteria, and then click Query to query all tasks according to the name, organization, status, start time, end time and other fields; click the "Organization" field in the head of the task list to sort by organization.

As shown in the figure below, all tasks with the name of "Command delivery task", the organization of "Headquarters" and the status of "completed" are found out.

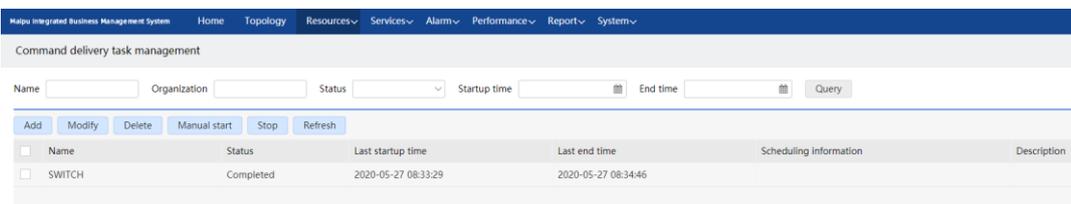


Figure 4-51 Command delivery task query

**! Caution**

- Organization: the organization and its subordinate organizations of the current administrator

**Add a task:**

Click Add in the task table panel to open the "Add" window, fill in the task name, execution method, whether to save the configuration file, description, and other information. Select the "Advanced Configuration" option to set the auto retry times and timeout, as shown in the figure below:

The screenshot shows a web-based configuration window titled 'Add' with a close button (X) in the top right corner. Below the title bar, there are four numbered steps: 1 Basic information (highlighted with a blue underline), 2 Device, 3 Template, and 4 Command Preview. The 'Basic information' section contains the following fields and options:

- \*Name: A text input field.
- Mode of execution: Two radio buttons, 'Execute immediately' (selected) and 'Timing execution'.
- Save configuration: Two radio buttons, 'Yes' (selected) and 'No'.
- Description: A text input field.
- Advanced configuration: A section header with a caret icon (^).
- \*Auto retry times: A text input field containing the value '1'.
- \*Timeout (min): A text input field containing the value '2'.

At the bottom right of the form, there are two buttons: 'Cancel' (grey) and 'Next step' (orange).

Figure 4-52 Add task information-step 1

## ! Caution

- The number of concurrent devices of a single task is 3 and the number of concurrent tasks is 3.
- By default, the auto retry times is 1 and the timeout is 2 minutes.

Execution mode: When "Execute immediately" is selected, the task can be executed immediately after the task information is configured; if "Timing execution" is selected, a "specified time" text box will appear, and you can set a time and execute the task after the set time period.

Auto retry times: If adding a task fails, the program will automatically try again according to the given times.

Timeout: When the task is executed, the time of waiting for the device response exceeds the set timeout, and the task execution fails.

Click  to enter the "Device Selection" window, as shown in the following figure:

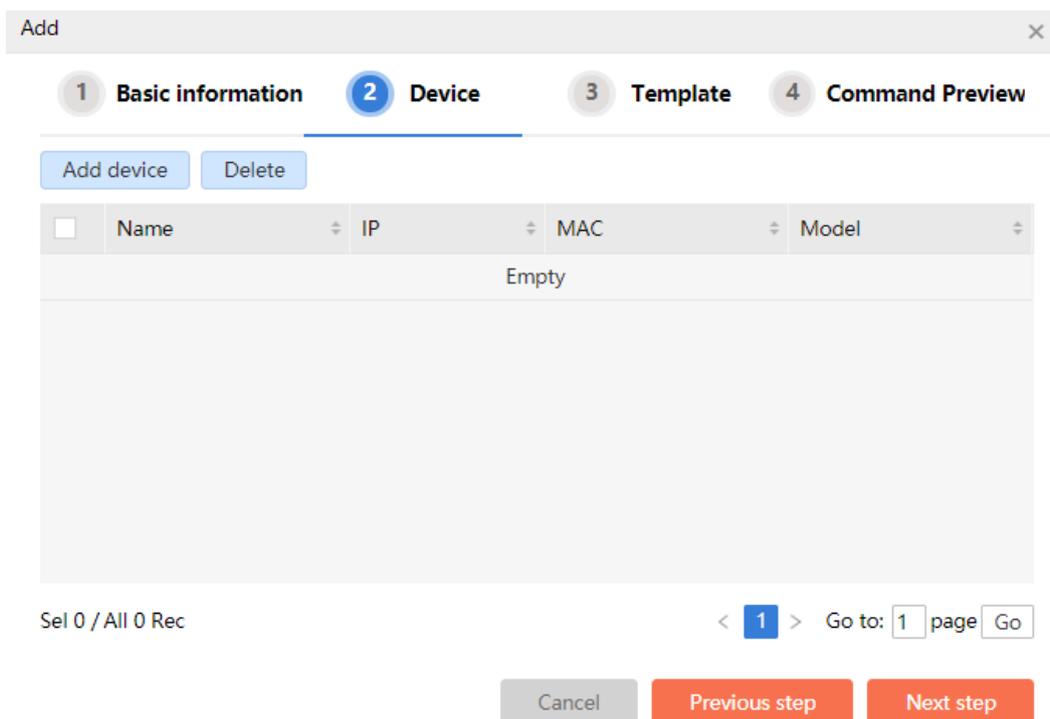


Figure 4-53 Add the task information-step 2

Click “Add device” to select the corresponding device for the task. Enter the “Select device” window, as shown in the following figure:

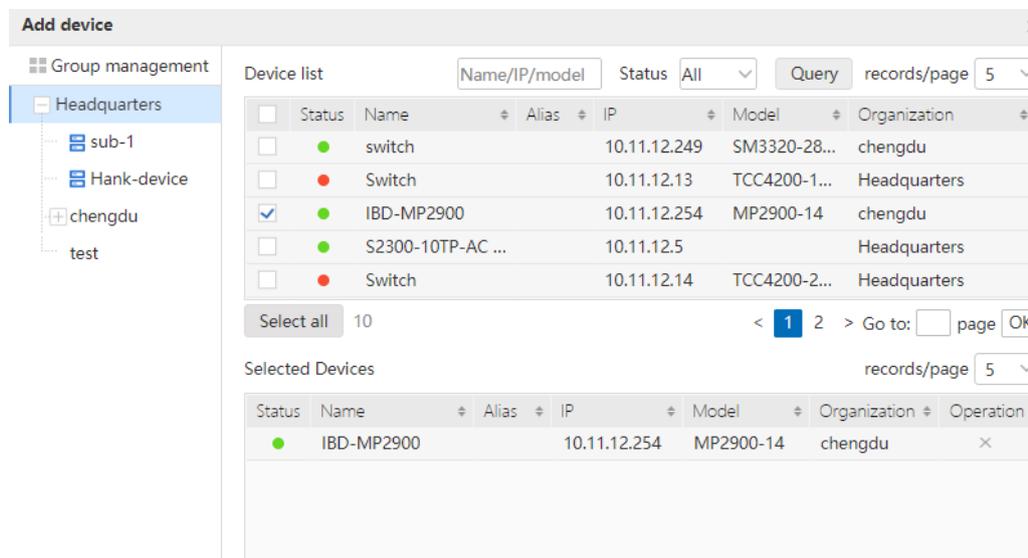


Figure 4-54 Select the device

Select the device, support selecting multiple, and click  to select the device for the command delivery task, as shown in the following figure:

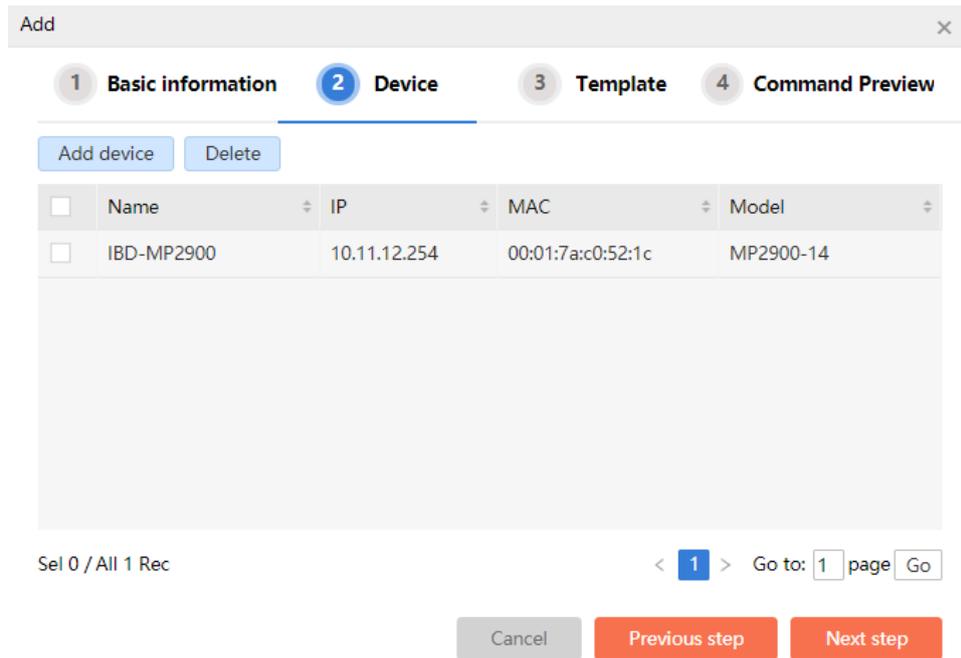
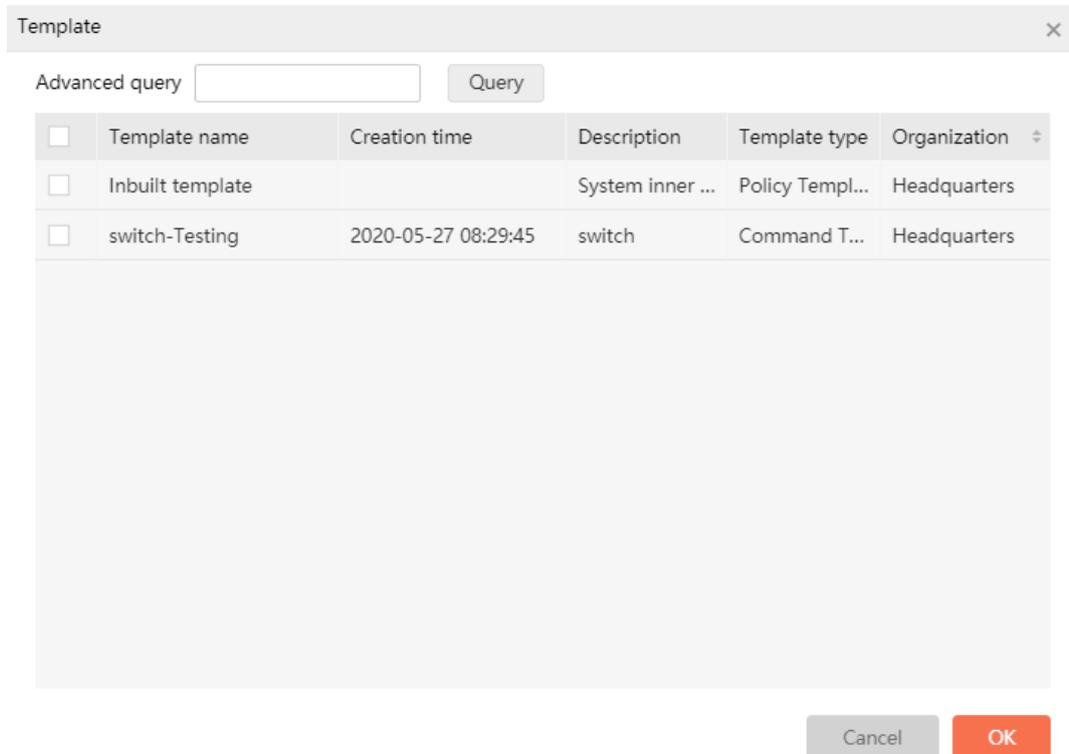


Figure 4-55 Add the task information-step 2

Click **Next step** to enter “Select template” window, as shown in the following figure:



In the "Select template " window, you can select the templates in the list of command templates, and it provides the advanced query function for fuzzy query of template name. Multiple templates can be selected at the same time. Click “OK” to select the template

successfully.

Select a single template, and click **Move down** or **Move upward** to sort the templates. The order of templates determines the order of command preview and command delivery. Then, click **Next step** to preview the commands in the selected template, click **Save** to complete the adding of the configuration command delivery task. The configuration command starts to be delivered.

Add

1 Basic information 2 Device 3 Template 4 Command Preview

\*Content

```
vlan 10
interface vlan 10
ip address 10.10.10.1 255.255.255.0
exit
```

Cancel Previous step Save

Figure 4-56 Add the task information-step 4

The process of modifying the task is the same as above. Select the desired task in the task list and click **Modify** to modify the task information.

### Note

- It is not necessary to select any template in the "Template selection" interface, and the command can be input directly in the command preview text box.

### Delete the task:

Select the desired task in the task list, and then click **Delete** to delete the task that is no longer needed.

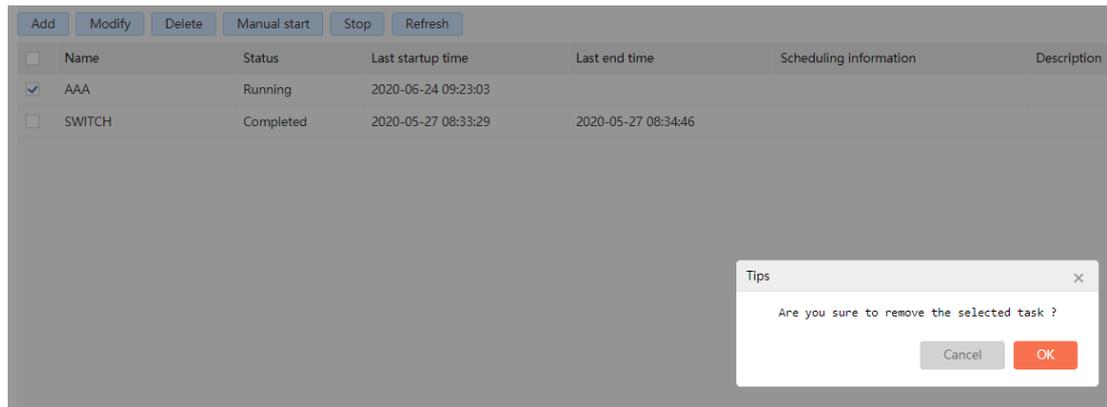


Figure 4-57 Delete the task information

### Note

- The task in progress cannot be deleted. It can only be deleted after the task stops or runs.

#### Manually start/stop the task:

Select a desired task, and click **Stop** to stop the task. When the task stops, the device that has started continues to execute, and the device that has not started stops executing.

Select a stopped task and click **Manual start**. The task can run from the beginning again. At this time, the status of the task changes to "in progress".

#### Refresh the task:

Click **Refresh** in the task list box to immediately update the running status of all tasks, which is convenient for relevant personnel to view.

#### View the command:

Click "View command" of any task in the task list, and the "Command details" window of the task will pop up, as shown below:

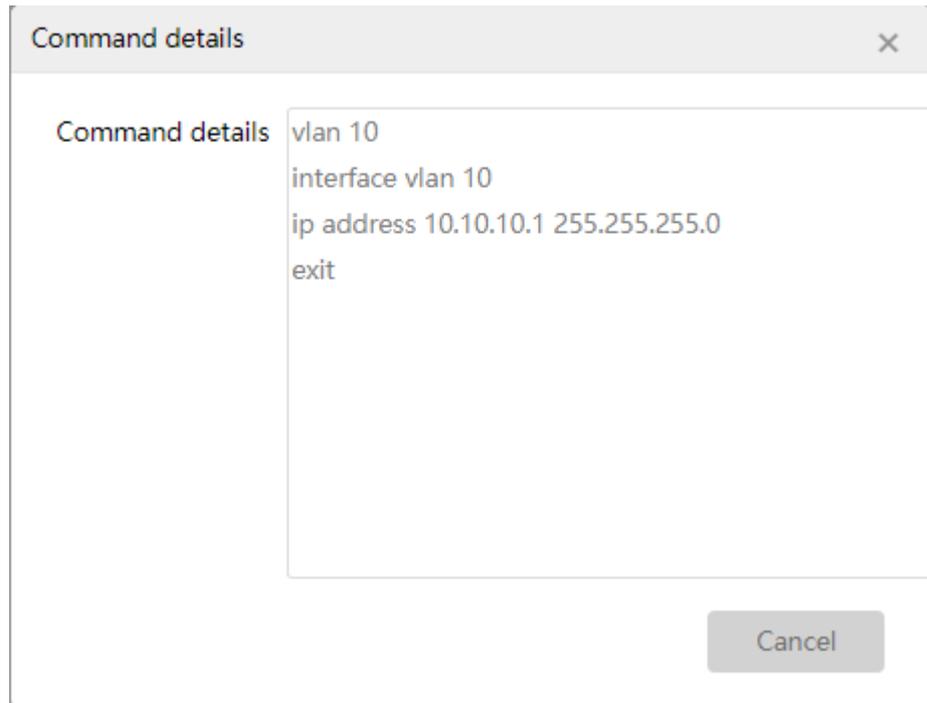


Figure 4-58 Command details

**View task details:**

Click “Details” of any task in the task list to open the “Task details” window, as shown below:

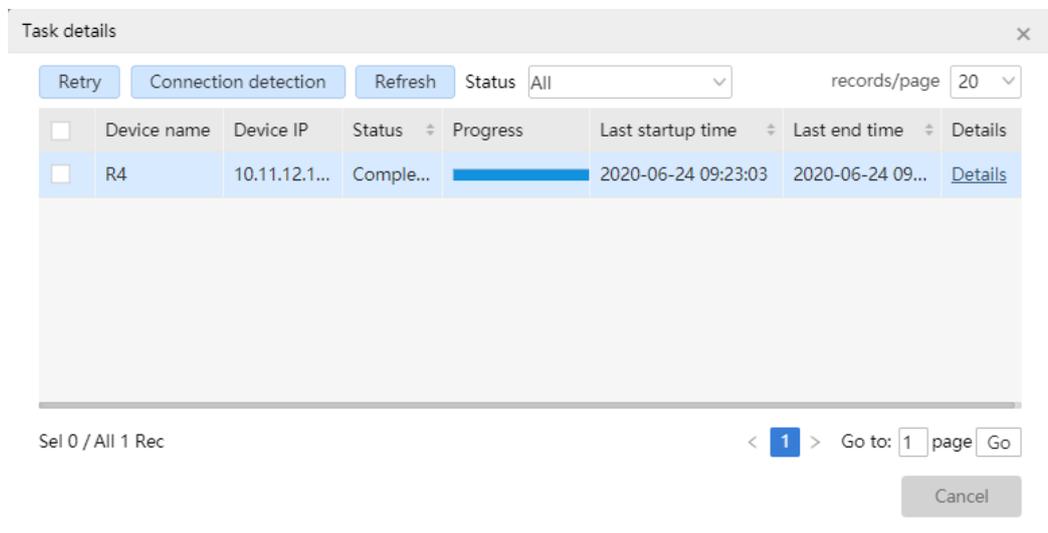


Figure 4-59 Task details

The "Task details" interface displays different devices under the same task by pages, showing the device name, device IP, status, progress, last start time, last end time, details and other information of the command delivery.

Select a piece of command delivery information, and click [Retry](#) to restart the command delivery task of the device.

Select a piece of command delivery information, and click **Connection detection** to view the connection status of the device, as shown in the following figure:

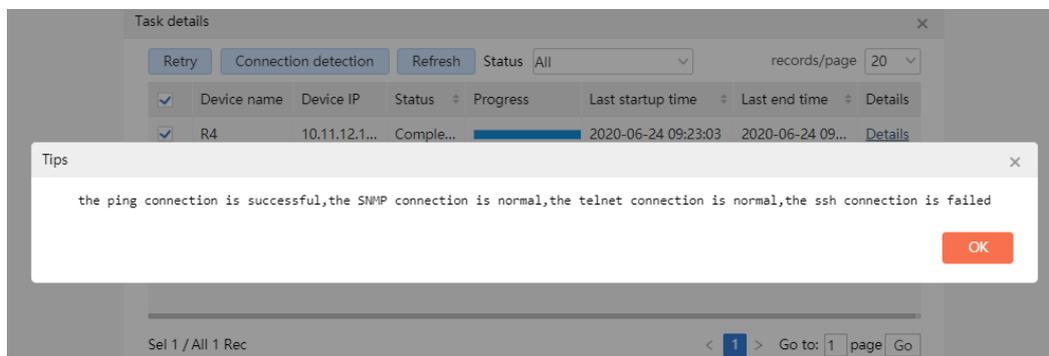


Figure 4-60 Device connection status

Click **Refresh** in the "Task details" window to update the status of all device updating immediately.

Click the details of any command delivery in the task details list, and the "Execution details" window of the device will pop up, showing the detailed process of command delivery, as shown below:

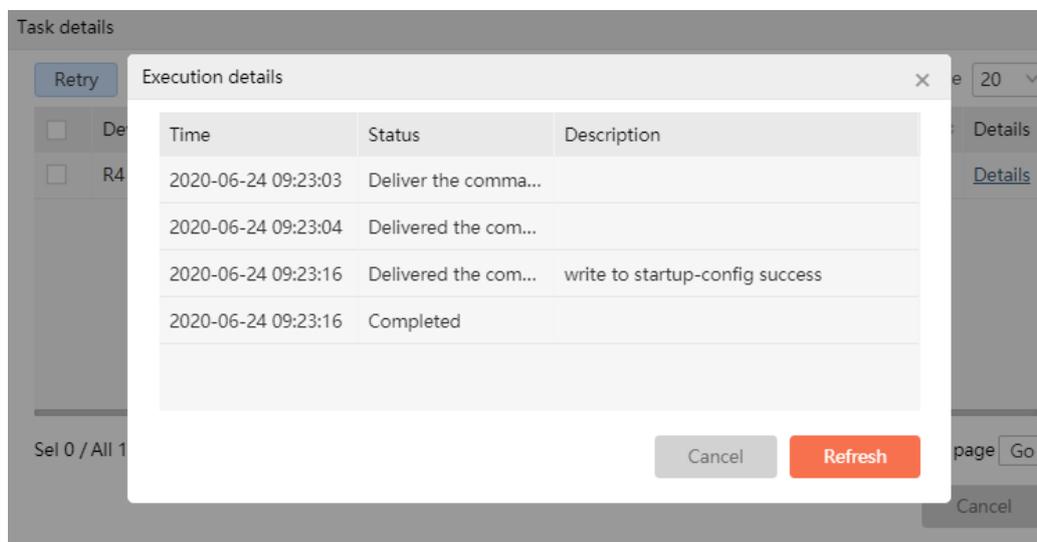


Figure 4-61 Command delivery execution details

**View task history:**

Click the history of any task in the task list to open the "Task history details" window, as shown below:

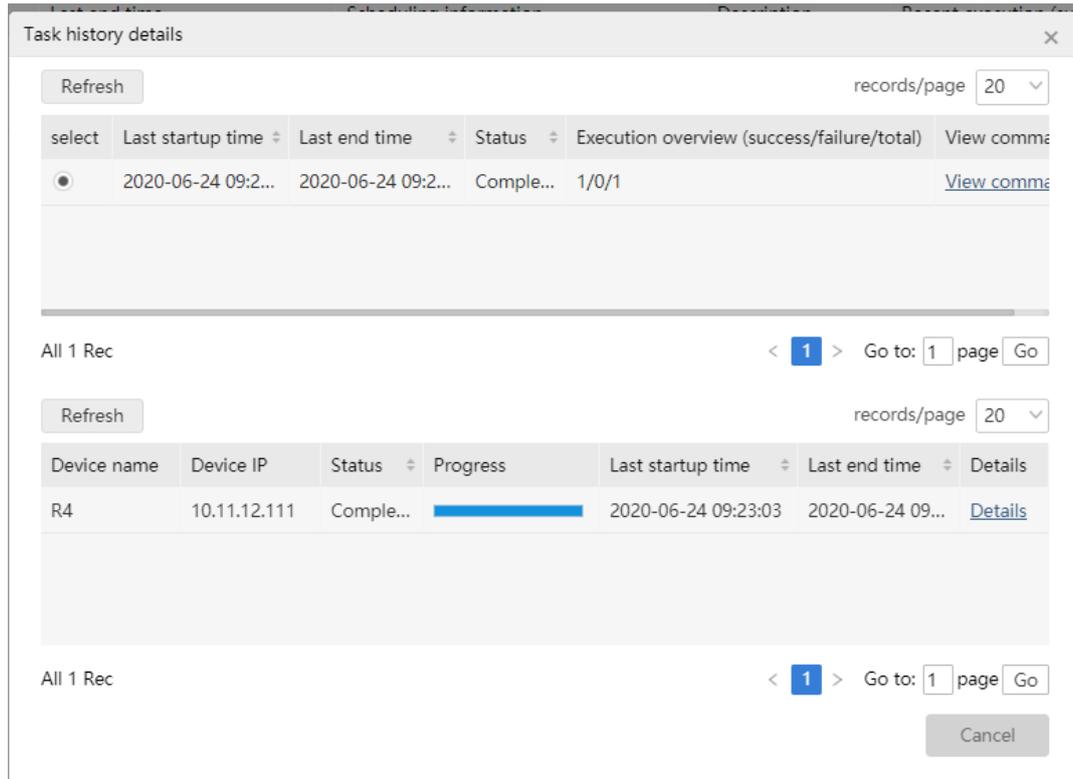


Figure 4-62 Task history details

The “Task history details” window is divided into two tables: “History execution status” and “Details”.

The "Details" table is the same as the "Details" window of the command delivery, and you can view the specific details of the command delivery.

Select the corresponding command delivery history in the "History execution status" table, and the "Details" table will switch to the corresponding command delivery history task.

 **Note**

- When adding the “In progress” tasks, their history cannot be viewed during operation. Only when the tasks are completed can the running history of tasks be viewed.

**4.3.3. Security Policy Template Management**

The security policy template management module provides the management for the security template delivered to the device, including adding, importing, modifying, deleting, copying, and querying security policy template.

Click "Resources" > "Configuration Management" > "Configuration Command Delivery" > "Security Policy Template Management" on the top navigation bar of the system to open the "Security Policy Template Management" page, as follows:

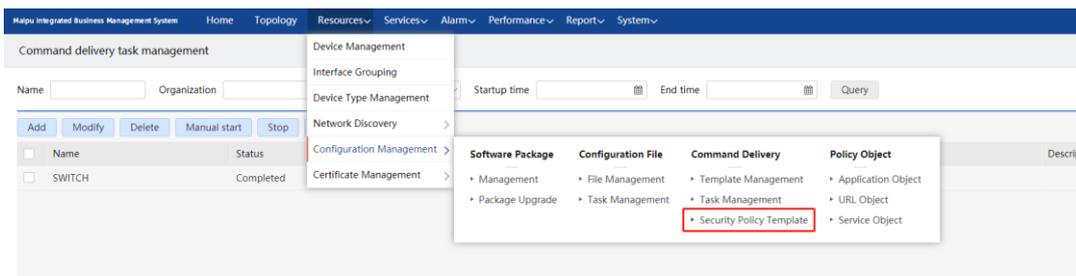


Figure 4-63 Security policy template management

**! Caution**

- The security policy template management function only supports Maipu ISG, MSG series products.

**Security policy template list:**

Open the "Security Policy Template Management" interface and display all the security policy templates in the system by default. The name, description, update time, update user, organization, and view content of each security policy template are displayed by lists. Click the fields in the head of the security policy template list to sort the security policy templates according to the corresponding fields.

This page provides a variety of query conditions, and you can easily and quickly query specific security policy templates. Enter the corresponding query conditions in the query panel, and then click **Query**, and you can query all security policy templates according to the template name and the organization.

Query the security policy template with the name of "Inbuilt template" and the organization of "Headquarters", as follows:

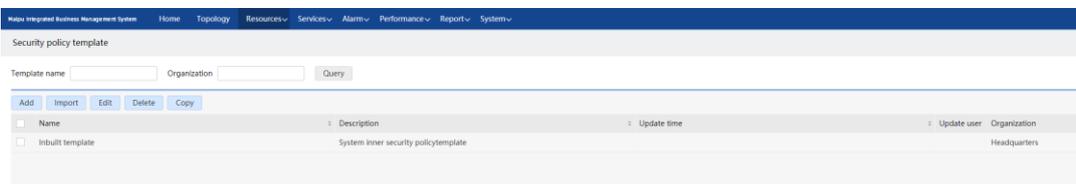


Figure 4-64 Security policy template query

**! Caution**

- Organization: the organization and its subordinate organizations of the current administrator.

**Add security policy template:**

Click **Add** in the template list panel to open the "Add" window, and fill in the template name, template content and template description, and select the template type and object, as shown in the following figure:

The screenshot shows a dialog box titled "Add" with a close button (X) in the top right corner. The dialog contains the following fields and controls:

- \*Name**: A text input field.
- Type**: A dropdown menu.
- \*Content**: A large text area containing the placeholder text "Please select a template".
- Description**: A text input field.
- Buttons on the right**: A vertical stack of buttons: "Add", a question mark icon, "Address Object", "Service Object", "App Object", "Time Object", "Key Object", "URL Object", and "Policy ID".
- Buttons at the bottom**: "Cancel" and "OK" buttons.

Below the content area, there is a note: "Note: \${param} in the command is the parameter to be modified. Click the question mark prompt button to display the detailed usage of the command in the line where the cursor is".

Figure 4-65 Add security policy template

Select a template type and click **Add** on the right. The corresponding command will appear in the content box, where `${param}` is the parameter to be modified. If you click the question mark prompt button, the command help dialog box will pop up, showing the detailed use method of the command on the cursor line, as shown in the following figure

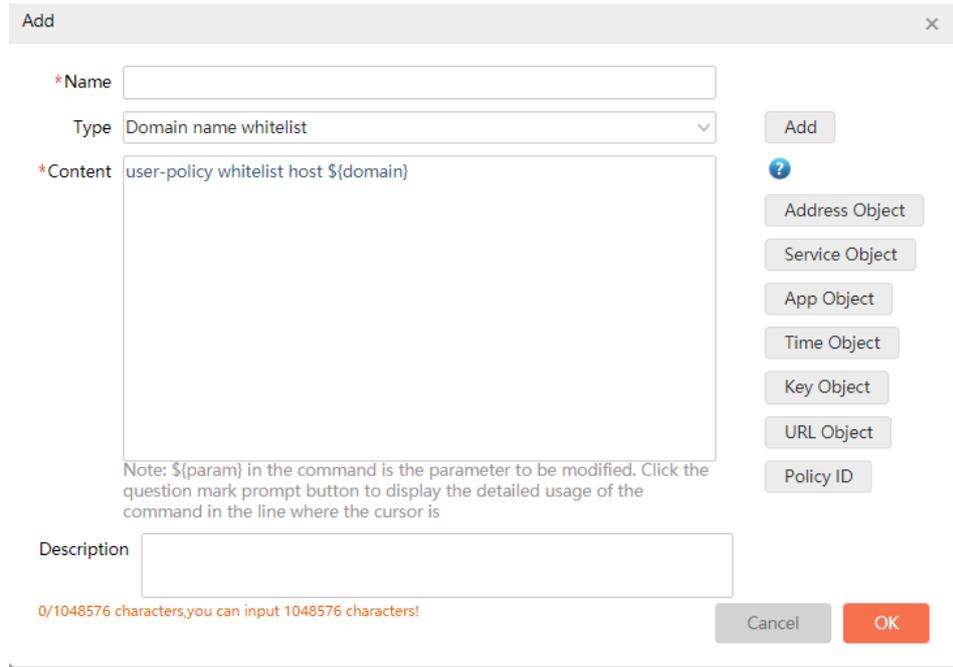


Figure 4-66 Select the template type

Click the various object buttons on the right to open the “Select Objects” dialog box, displaying all the object lists of this type by default. You can query objects by object name and type. Select the object and click . The command corresponding to the object will appear in the command box, as shown in the following figure

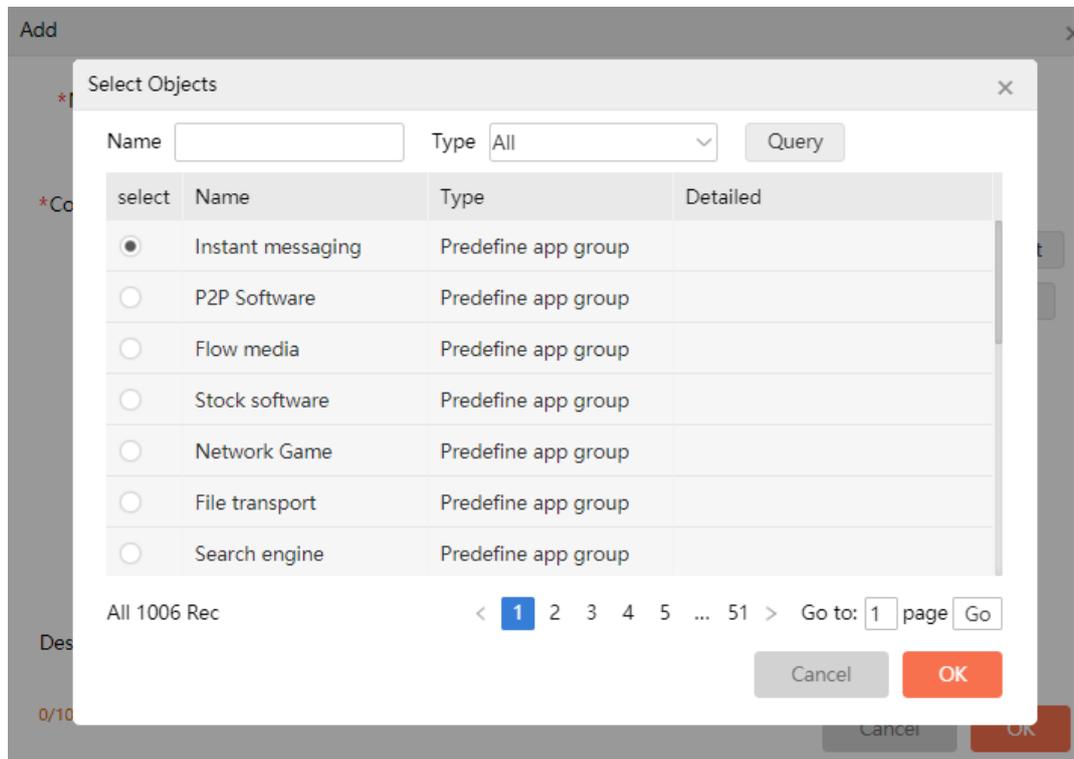


Figure 4-67 Select the objects

Click  to add a security policy template. The process of modifying the security policy template is the same as above. Select the desired security policy template in the security policy template management list and click  to modify it.

### Import the security policy template:

Click  in the template list panel to open the "Import" window, fill in the template name and template description, and select the template file (only the TXT format file can be imported), as shown in the following figure:

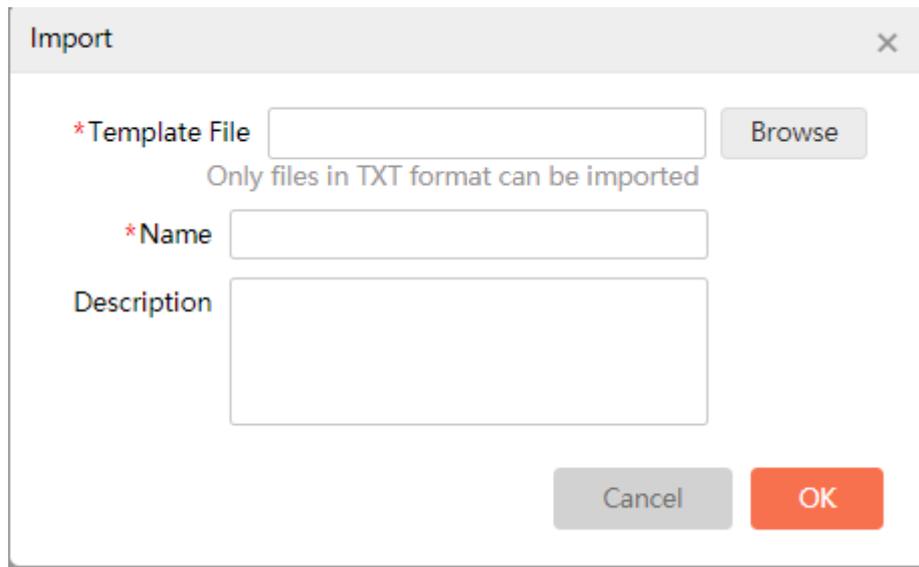
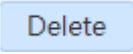


Figure 4-68 Import the security policy template

Click  to complete the importing of the security policy template.

### Delete the security policy template:

Select the desired security policy template in the template list, and click  to delete the security policy template file, as shown in the following figure:

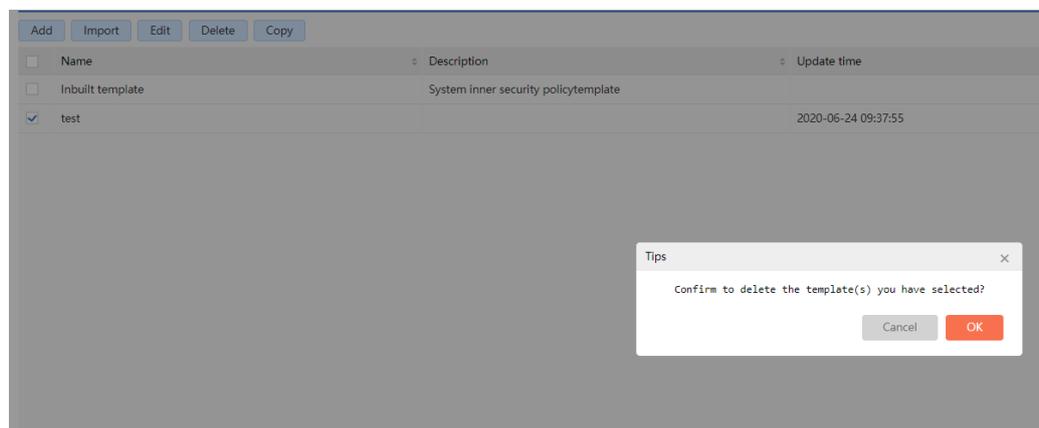


Figure 4-69 Delete the security policy template

**Copy the security policy template:**

Select the desired security policy template from the template list, and click  to open the “Add/ modify policy template” dialog box. All options and contents are the same as the template to be copied. You only need to make some modifications to add a new security policy template.

## 4.4. Policy Object Management

### 4.4.1. Application Object

Application object provides the querying and importing for the application object.

Click "Resources" - > "Configuration Management" > "Policy Object Management" > "Application Object" at the top navigation bar of the system to open the "Application Object" page. By default, all the application lists are displayed by pages, as shown below:

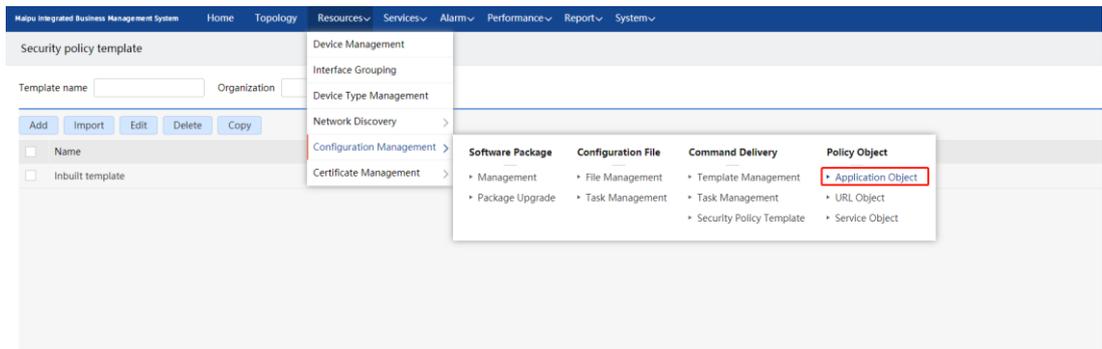
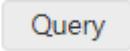


Figure 4-70 Application object interface

The "Application Object" column on the left side displays all application classifications. Click an application classification, and the corresponding application objects will be displayed in the application object list on the right side, including object name, platform, risk level, popularity, and description. Click the "Risk level" and "Popularity" field names to sort the application objects.

This page provides a variety of query conditions, AND you can easily and quickly query specific application objects. Enter the corresponding query criteria in the query panel, and then click  to carry out advanced query filtering for all application object name, risk level, and popularity fields.

Click  in the application object list to open the “Application Import” dialog

box, as follows. Select the corresponding file to import the application object.

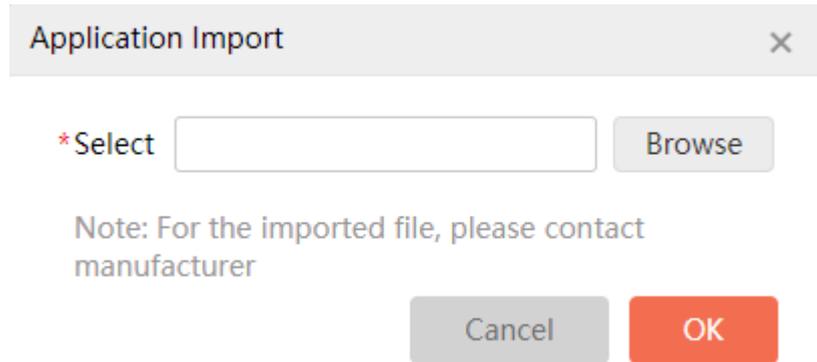


Figure 4-71 Application import

### 4.4.2. URL Objects

URL object provides the querying and importing for the URL object.

Click “Resource” > “Configuration Management” > “Policy Object Management” > “URL object” in the top navigation bar of the system to open the "URL object" page, as shown below:

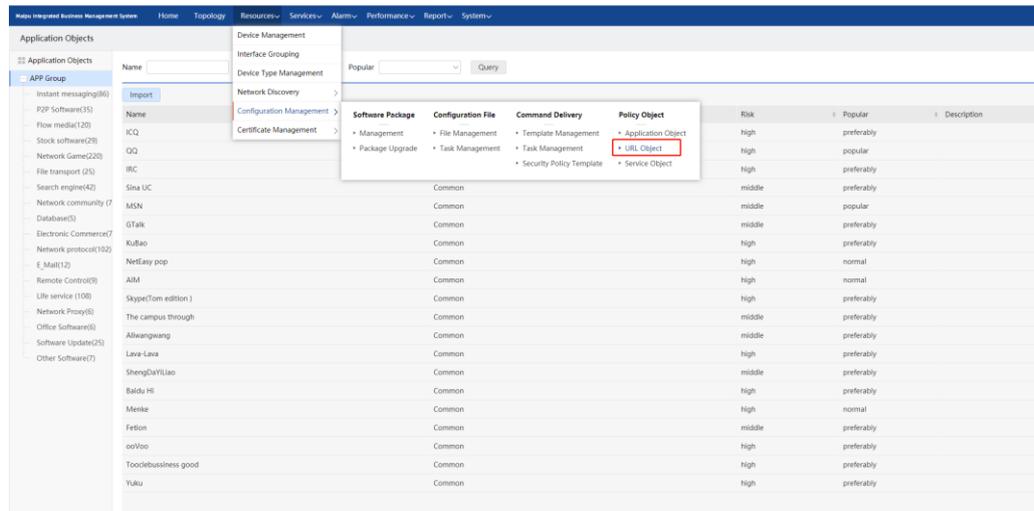


Figure 4-72 URL object interface

The list of inbuilt URL classes displays all built-in URL objects by default, including the name and description of URL objects.

This page provides fuzzy query for the URL object name by keyword. Enter the corresponding query criteria in the query panel, and then click  to query and filter all URL object names.

Click  in the list of built-in URL classes to pop up the “URL Import” dialog box, as follows. Select the corresponding file to import the URL object.

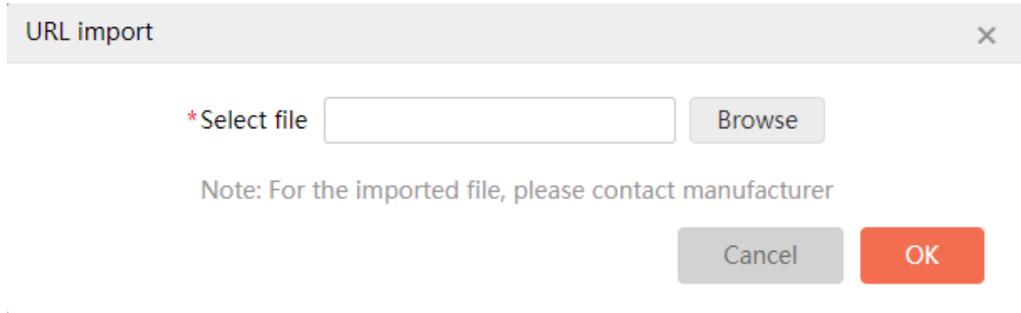


Figure 4-73 URL import

### 4.4.3. Service Object

Service object provides the querying for the service object.

Click “Resource” > “Configuration Management” > “Policy Object Management” > “Service object” in the top navigation bar of the system to open the "Service object" page, as shown below:

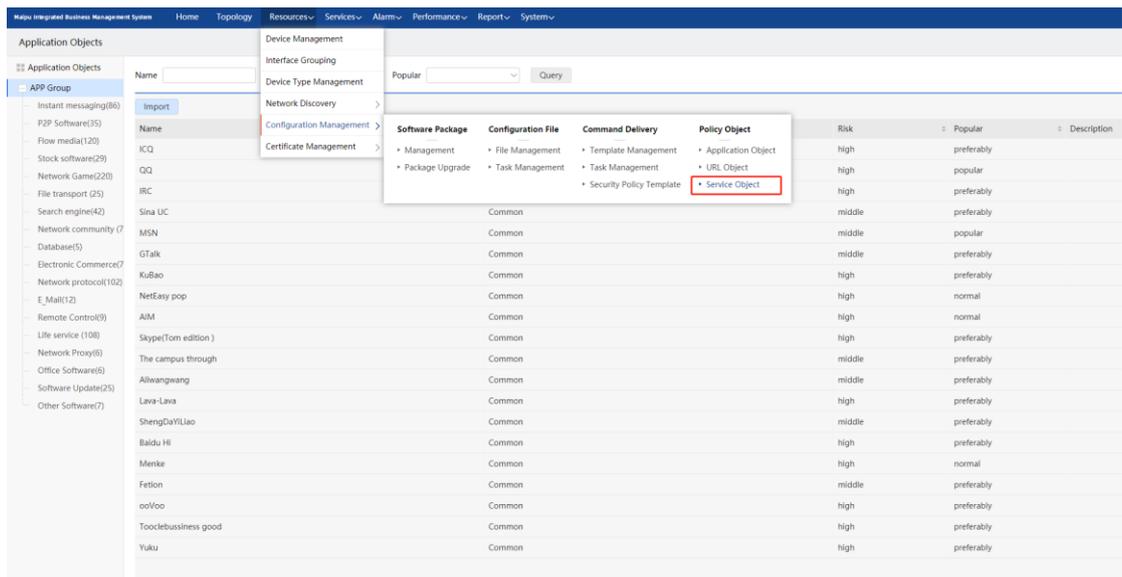
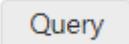


Figure 4-74 Service object interface

The list of service objects displays all service objects by default, including service object name, protocol, details, and description. You can sort by clicking the "Name" field of the service object.

This page provides the fuzzy query for the service object name and protocol by keyword.

Enter the corresponding query criteria in the query panel, and then click  to query and filter all service object names and protocols.

# 5. Performance Management

The performance module is responsible for monitoring task management, monitoring data viewing and exporting, and customized monitoring index management.

## 5.1. Monitoring Task

Click "Performance" -> "Monitoring Task" in the menu bar to open the "Monitoring Task" page, including system monitoring, interface monitoring and security device monitoring, as follows:

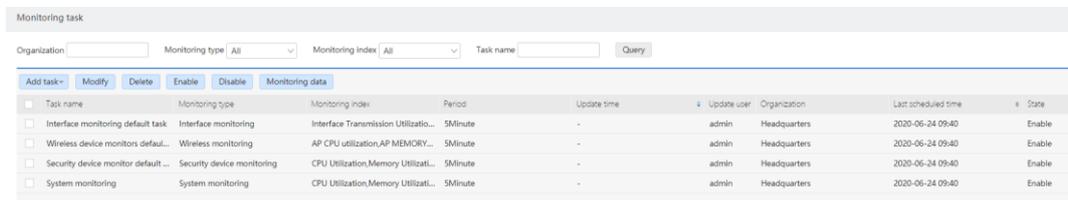


Figure 5-1 Monitoring task

Monitoring tasks can be queried by organization, monitoring type, monitoring index and task name. Only the monitoring tasks of the current administrator's organization and its subordinate organizations can be queried and edited. The organization of the new monitoring task is the organization of the current administrator.

If different monitoring types are selected, the contents of the drop-down box of the monitoring index will change accordingly. The monitoring types, monitoring indexes and their corresponding relationships are shown in the table below:

Monitoring type	System monitoring	Interface monitoring	Security device monitoring
Monitoring index	CPU utilization	Interface traffic	CPU utilization
	Memory utilization	Interface inflow	Memory utilization
	Forwarding traffic	Output flow of interface	Disk utilization
	Received traffic	Interface receive rate	Number of online users
	Lost packets of the device	Interface receiving bandwidth utilization	Upstream traffic
	Packet loss rate	Interface send rate	Downstream traffic
	Power input voltage	Interface transmission bandwidth utilization	Total flow

	Power output voltage	Lost packets received by the interface	Device response time
	Power input current	Lost packets sent by the interface	
	Power output current		
	temperature		
	Fan speed		
	Device response time		

Figure 5-2 Monitoring indexes

There are three default monitoring tasks in the monitoring task, which are default task of system monitoring, default task of interface monitoring, and default task of security device monitoring.

 **Note**

- The system supports creating up to 800 monitoring tasks.
- A monitoring task can select up to 2000 resources.

### 5.1.1. System Monitoring

#### Add system monitoring task

Click “System monitor” under “Add task”, as follows:

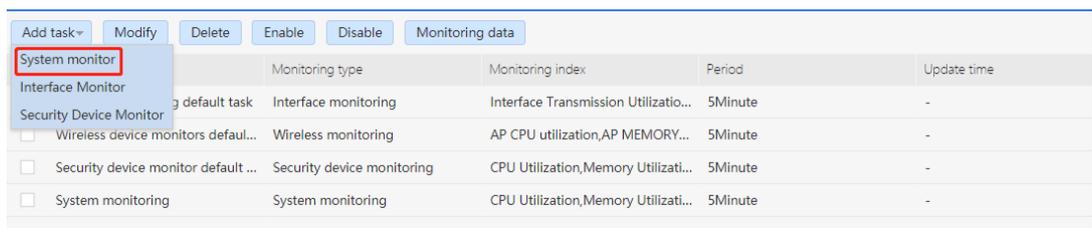


Figure 5-3 The entrance of adding system monitoring task

Enter the interface of adding a system monitoring task, as follows:

Monitoring task

Task information

\*Task name  (1-64 words)

\*Collection cycle

Monitoring index

Select index

Resource selection

Select resources Delete

Name	IP	MAC	Type	Description
No relevant data				

Cancel Save

Figure 5-4 Add system monitoring task

When adding a system monitoring task, you need to input the task name, select the collection cycle (5 minutes, 15 minutes, 30 minutes), select monitoring index, and select monitoring resources.

Click **Select index** to open the dialog box for selecting the index, as follows:

Select index

<input type="checkbox"/>	Index
<input type="checkbox"/>	CPU Utilization
<input type="checkbox"/>	Memory Utilization
<input type="checkbox"/>	Forwarding Data Flow
<input type="checkbox"/>	Reception Data Flow
<input type="checkbox"/>	Device Packet Loss
<input type="checkbox"/>	Device Packet Loss Rate
<input type="checkbox"/>	Voltage Input

Cancel OK

Figure 5-5 Select the index

### Note

- Only two monitoring indexes of CPU utilization and memory utilization are supported by the devices of the friend manufacturer.

After selecting the monitoring index, you can set the threshold alarm value for each monitoring index, as follows:



Figure 5-6 Set the threshold

 **Note**

- When multiple levels of alarm thresholds are configured, send the highest-level alarm if meeting all alarm thresholds and reaching the repeating times.
- Send the recovery alarm only when the send recovery alarm is checked and the threshold alarm is sent. The recovery alarm will be sent only once.
- The threshold alarm rules of interface monitoring task and security device monitoring task are consistent with the system monitoring task.

Click  to display the “Select resources” dialog box, as follows:

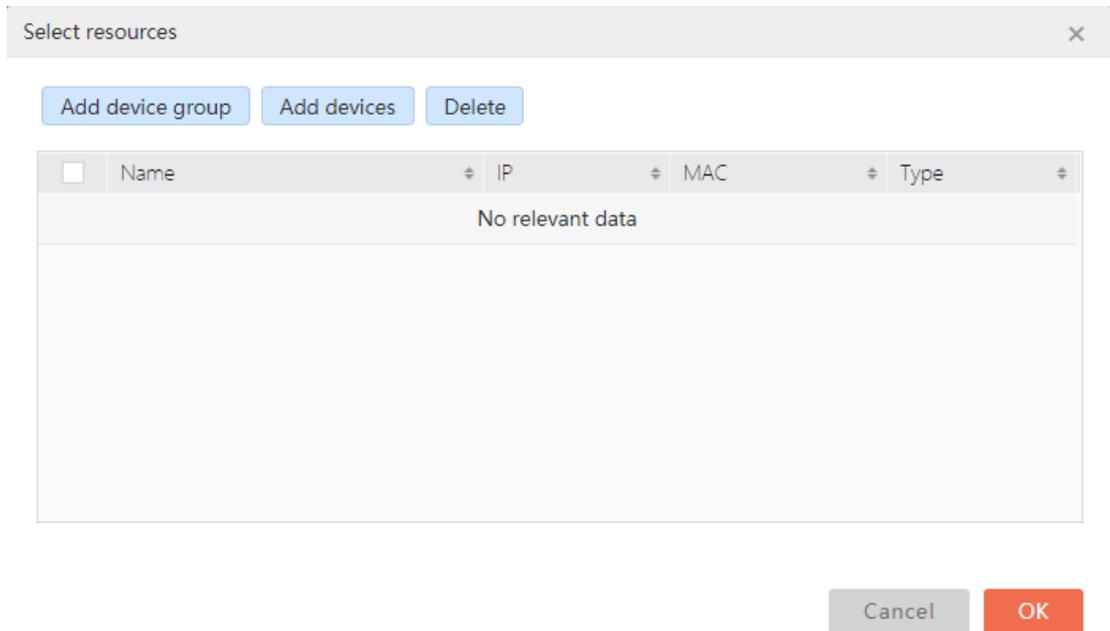


Figure 5-7 Select resources

You can add “Device” or “Device group” resource.

Click  to display the “Add device” dialog box, as follows:

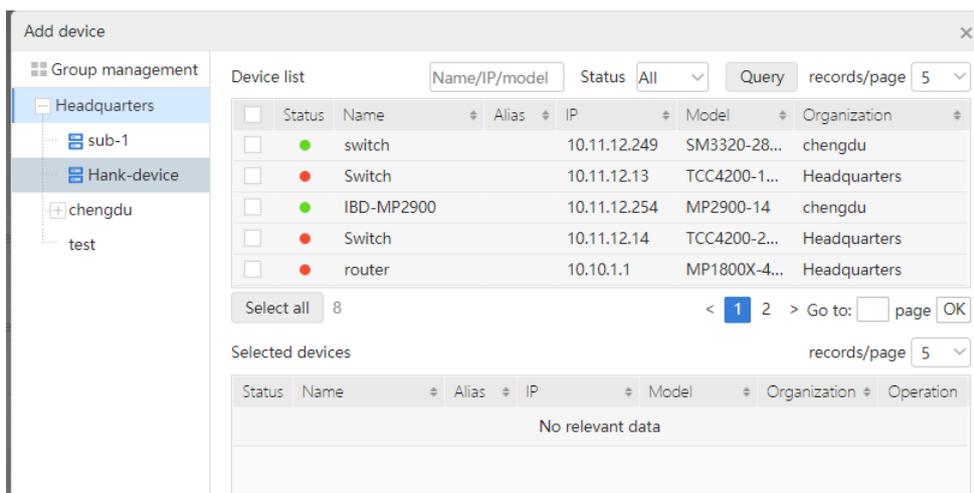


Figure 5-8 Select the device

The “Add device” page supports querying devices by device group, device name, device IP, device model and device status. Select the desired device and click **OK**, as follows:

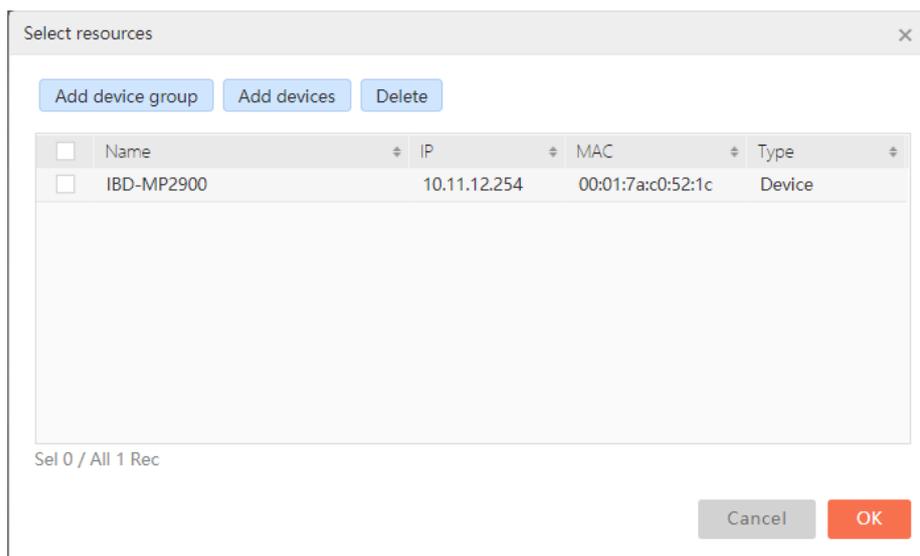


Figure 5-9 Select the device

When adding resources in the system monitoring task, the “Add device” dialog box will only display Maipu network devices and all devices of other manufacturers.

Click **Add device group** to open the “Add device group” dialog box, as follows:

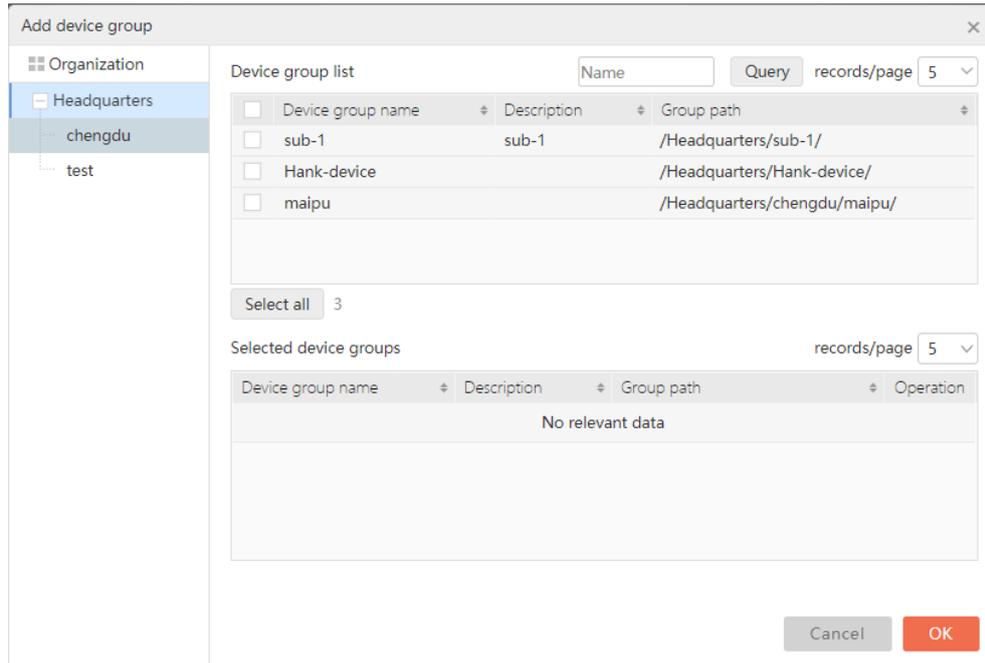


Figure 5-10 Select the device group

On the “Add device group” page, you can query the device group by organization and device group name. Select the desired device group and click  , as follows:

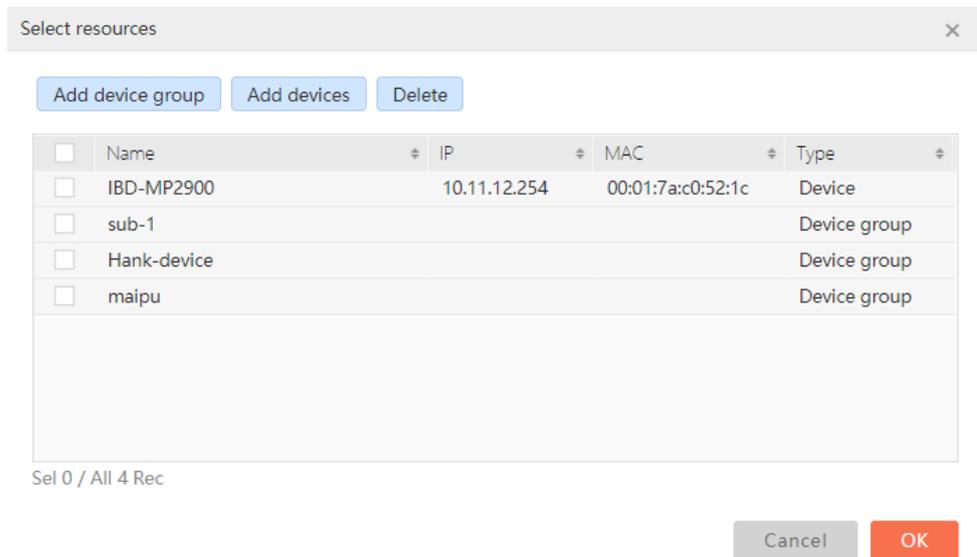


Figure 5-11 Select the device group

Click  to complete the adding of the monitoring task.

**Modify the system monitoring task:**

In the monitoring task list, select the desired system monitoring task, and click the "Modify" button, as follows:

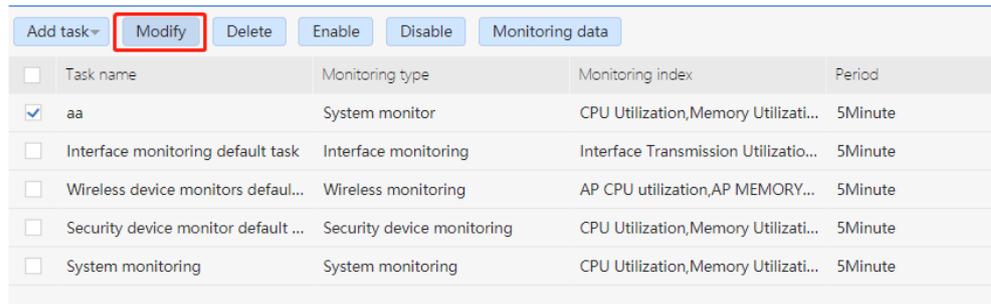


Figure 5-12 Modify the system monitoring task

Enter the interface of modifying the monitoring task, as follows:

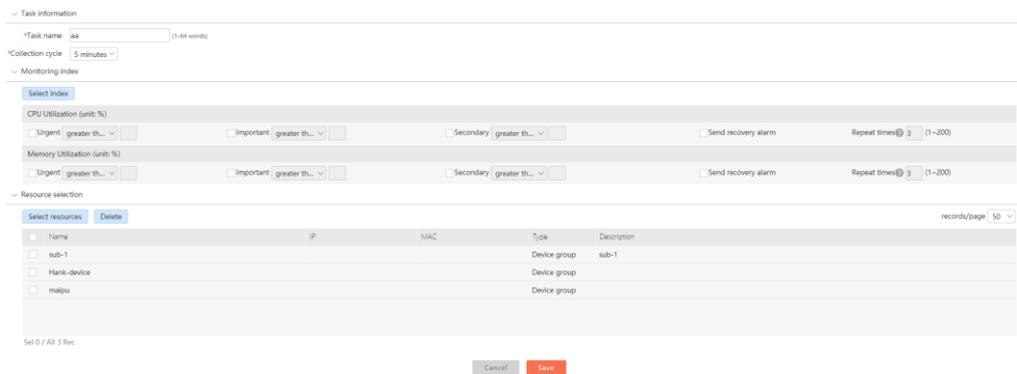


Figure 5-13 Modify the system monitoring task

You can modify the task name, collection cycle, monitoring index, alarm threshold and monitoring resources. Click **Save** to complete the modifying of the monitoring task.

### 5.1.2. Interface Monitoring

#### Add interface monitoring task

Click “Interface monitor” under “Add task”, as follows:

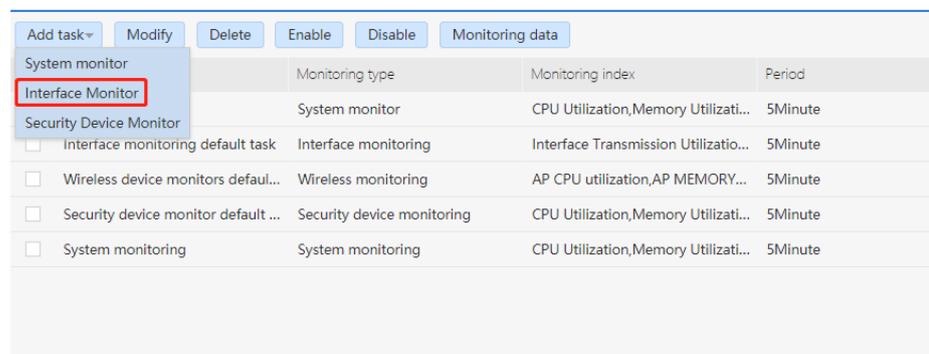


Figure 5-14 Add interface monitoring task

Enter the interface of adding an interface monitoring task, as follows:

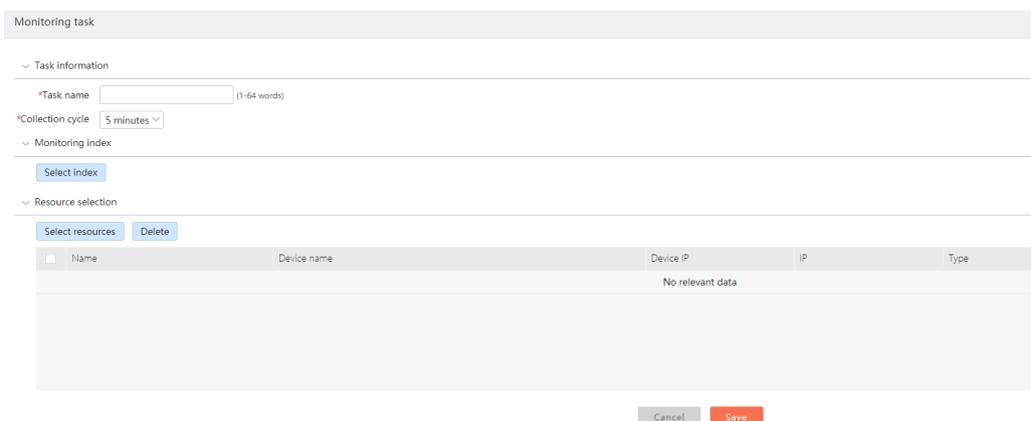


Figure 5-15 Add interface monitoring task

When adding an interface monitoring task, you need to input the task name, select the collection cycle (5 minutes, 15 minutes, 30 minutes), select monitoring index, and select monitoring resources.

Click **Select index** to open the dialog box for selecting the index, as follows:

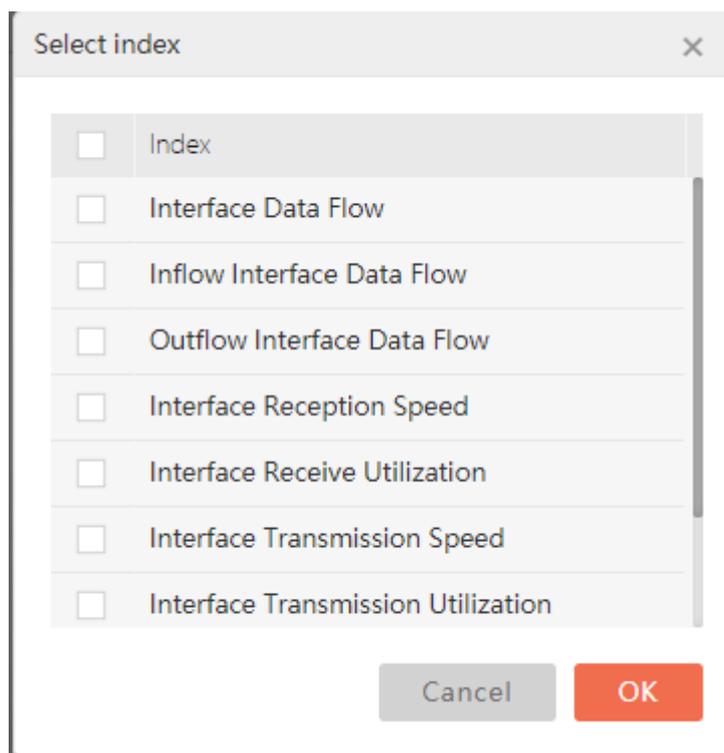


Figure 5-16 Select the index

After selecting the monitoring index, you can set the threshold alarm value for each monitoring index, as follows:



Figure 5-17 Set the threshold

Click **Select resources** to display the “Select resources” dialog box, as follows:

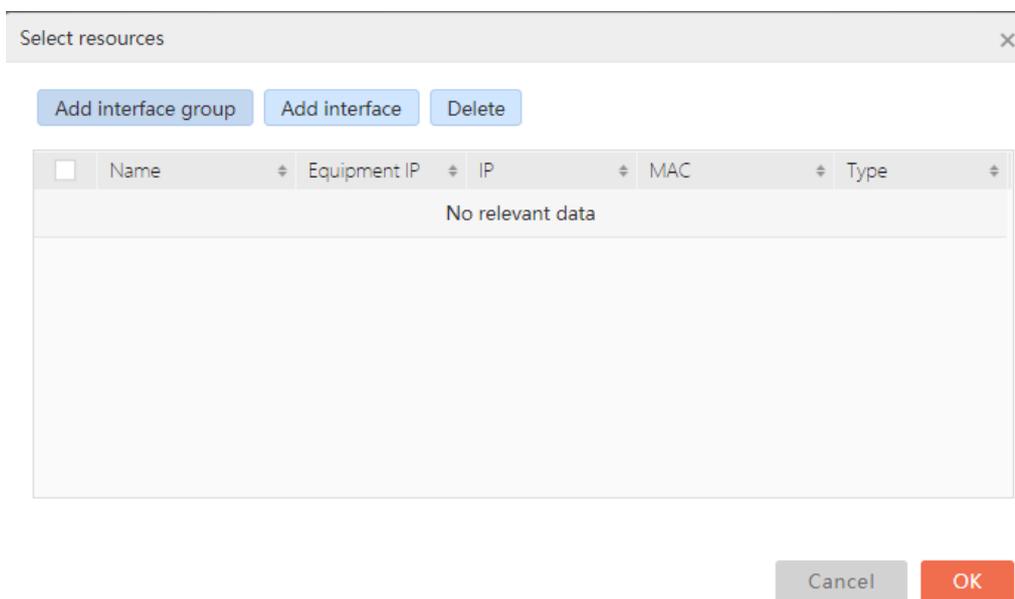


Figure 5-18 Select the resource

You can add “Interface” or “Interface group” resource.

Click **Add interface** to display the “Add interface” dialog box, as follows:

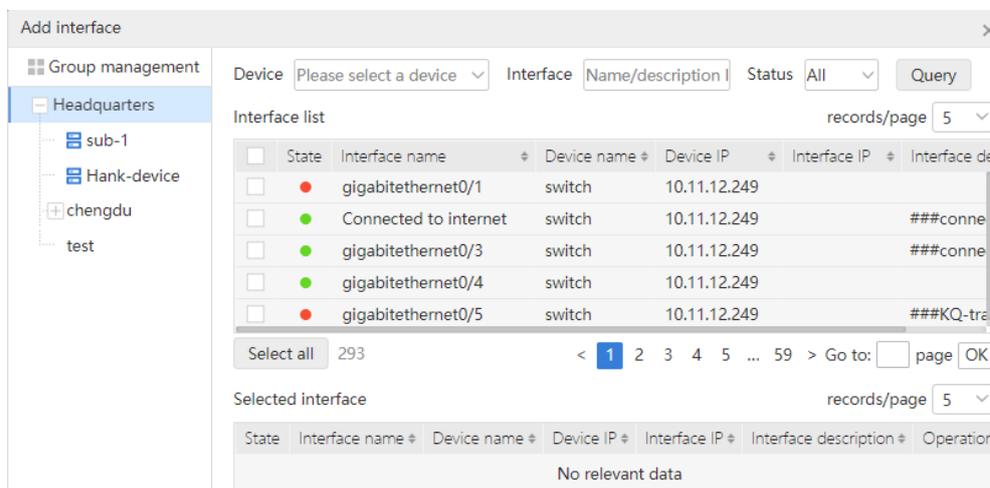


Figure 5-19 Select the interface

The “Add interface” page supports querying interfaces by interface group, device, interface name, interface description, IP and interface status. Select the desired device, select the desired interface, and click “OK”, as follows:

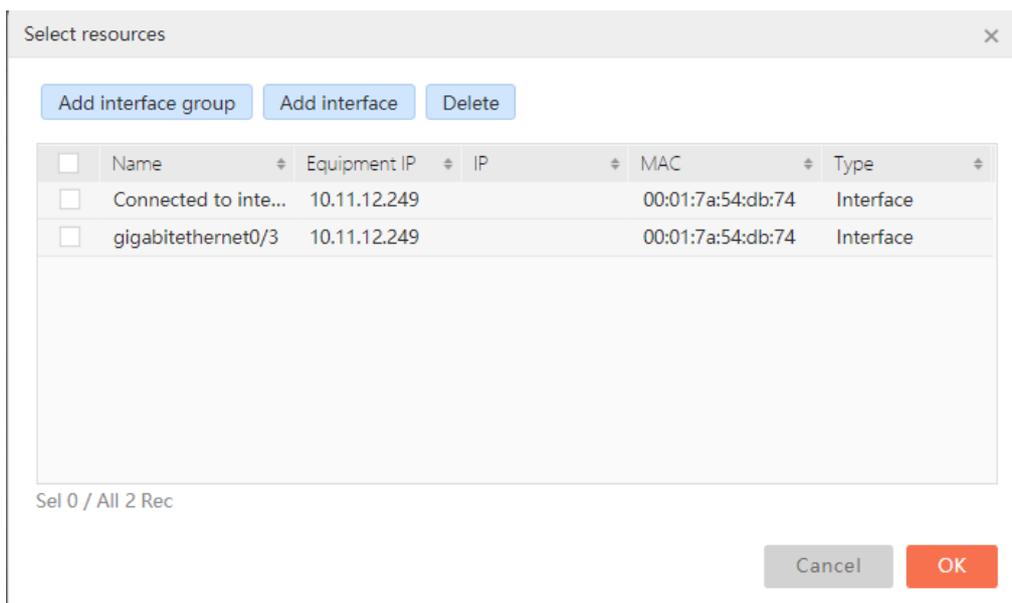


Figure 5-20 Select the interface

Click **Add interface group** to display the “Add interface group” dialog box, as follows:

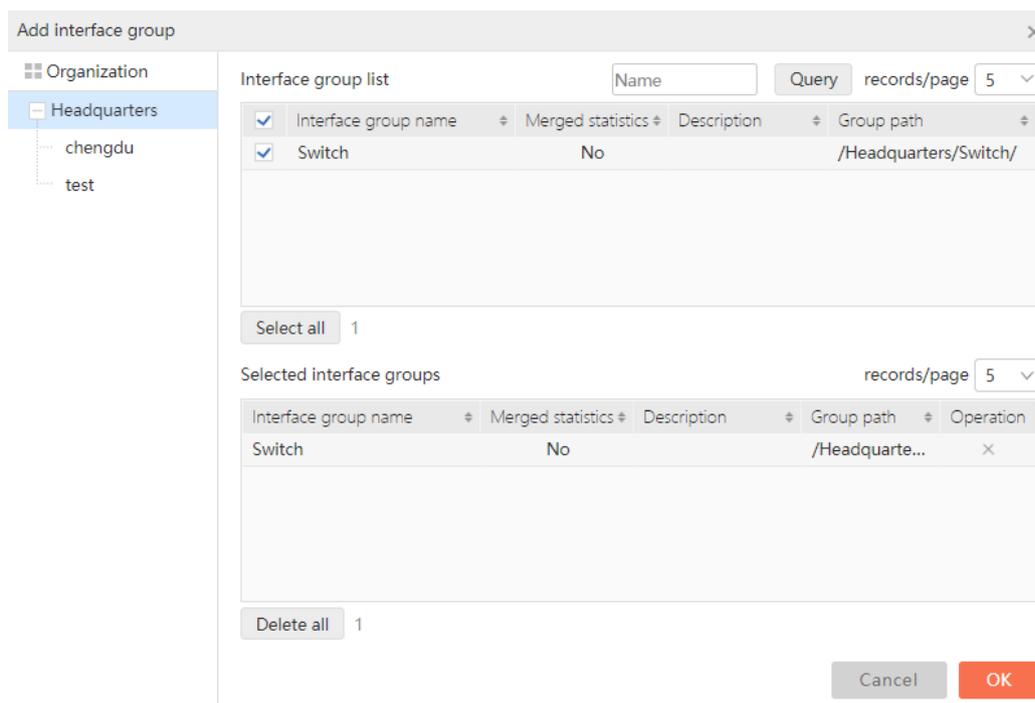


Figure 5-21 Select the device group

In the “Add interface” page, you can query the interface group by organization and interface group name. Select the desired interface group and click **OK**, as follows:

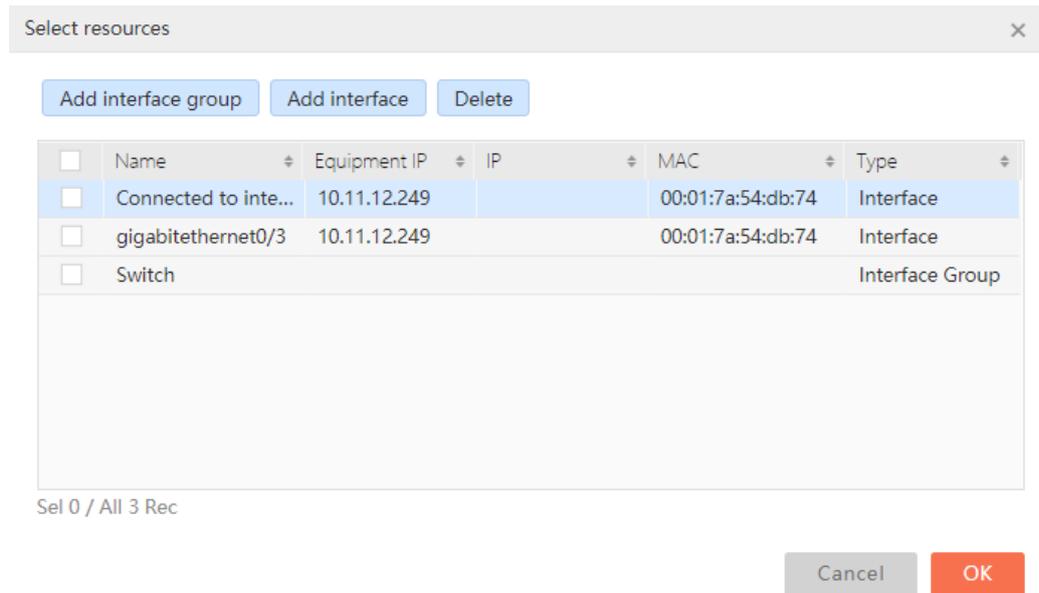


Figure 5-22 Select the device group

Click  to complete the adding the monitoring task.

### Modify the interface monitoring task:

In the monitoring task list, select the desired interface monitoring task, and click the "Modify" button, as follows:

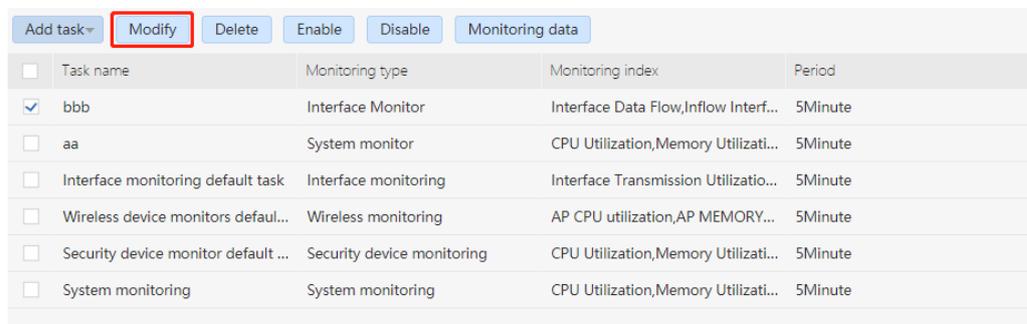


Figure 5-23 Modify the interface monitoring task

Enter the interface of modifying the monitoring task, as follows:

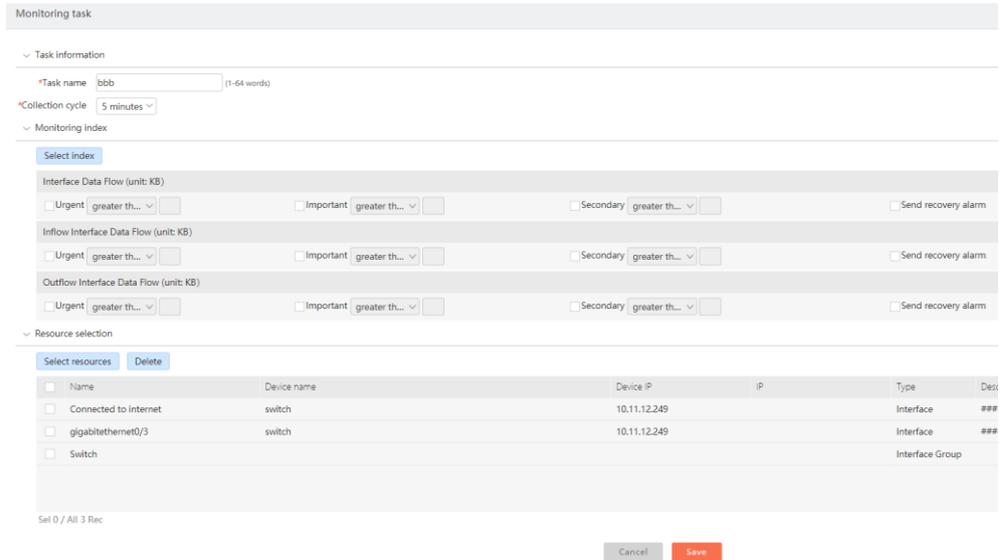


Figure 5-24 Modify the interface monitoring task

You can modify the task name, collection cycle, monitoring index, alarm threshold and monitoring resources. Click **Save** to complete the modifying of the monitoring task.

### 5.1.3. Monitoring Task Operation

#### Enable the monitoring task

In the monitoring task list, select one or more disabled monitoring tasks, and click the "Enable" button to enable the selected monitoring tasks, as follows:

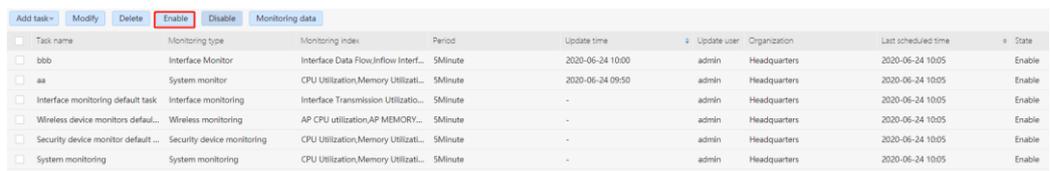


Figure 5-25 Enable the monitoring task

#### Disable the monitoring task

In the monitoring task list, select one or more enabled monitoring tasks, and click the "Disable" button to disable the selected monitoring tasks, as follows:

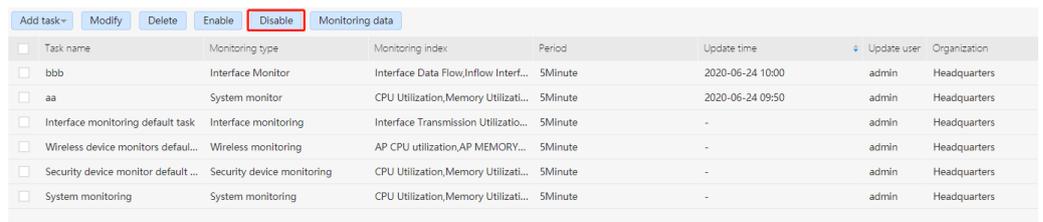
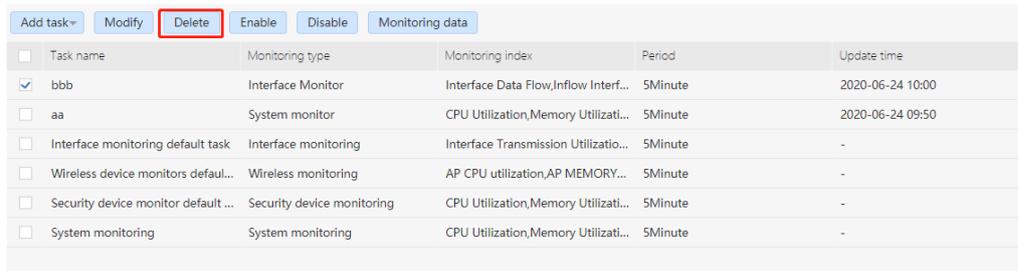


Figure 5-26 Disable the monitoring task

#### Delete the monitoring task

In the monitoring task list, select one or more monitoring tasks, and click the "Delete" button to delete the selected monitoring tasks.

button, as follows:



<input type="checkbox"/>	Task name	Monitoring type	Monitoring index	Period	Update time
<input checked="" type="checkbox"/>	bbb	Interface Monitor	Interface Data Flow,Inflow Interf...	5Minute	2020-06-24 10:00
<input type="checkbox"/>	aa	System monitor	CPU Utilization,Memory Utilizati...	5Minute	2020-06-24 09:50
<input type="checkbox"/>	Interface monitoring default task	Interface monitoring	Interface Transmission Utilizatio...	5Minute	-
<input type="checkbox"/>	Wireless device monitors default...	Wireless monitoring	AP CPU utilization,AP MEMORY...	5Minute	-
<input type="checkbox"/>	Security device monitor default ...	Security device monitoring	CPU Utilization,Memory Utilizati...	5Minute	-
<input type="checkbox"/>	System monitoring	System monitoring	CPU Utilization,Memory Utilizati...	5Minute	-

Figure 5-27 Delete the monitoring task

Display the dialog box of confirming the deletion, as follows:

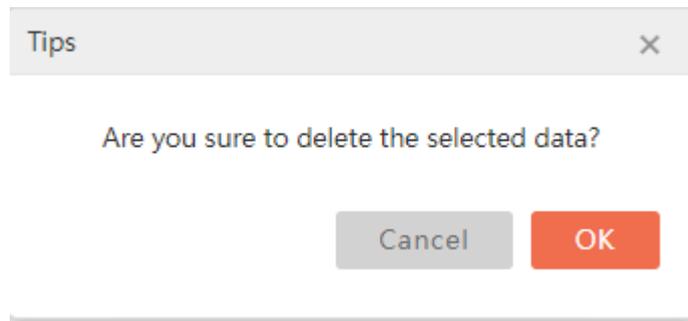


Figure 5-28 Delete the monitoring task

Click  to delete the selected monitoring task.

If there are monitoring tasks in the status of "enabled" in the selected monitoring tasks, the following prompt will appear when clicking :

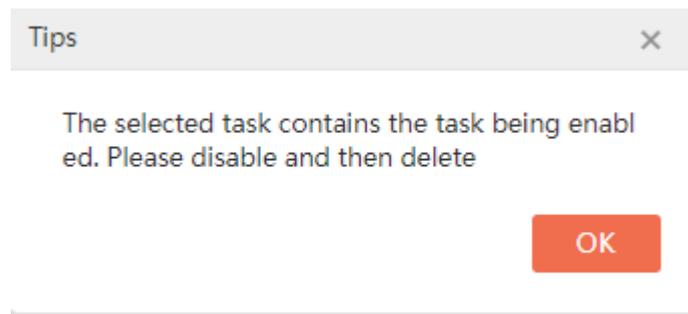


Figure 5-29 Delete the monitoring task

### Monitoring data

In the monitoring task list, select a monitoring task and click the "Monitoring data" button to enter the monitoring data page of the resources monitored by the task, as follows:

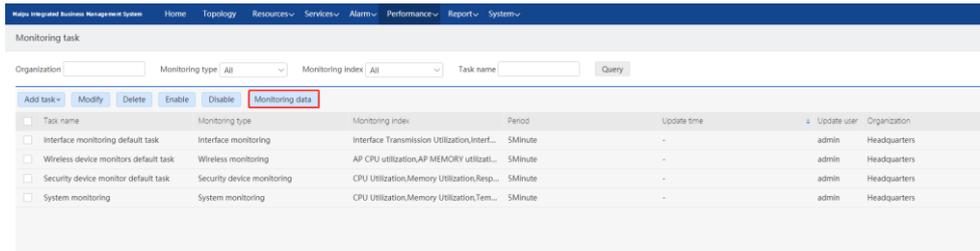


Figure 5-30 Monitoring data

The monitoring data page is as follows (this page will only list the resources monitored by the monitoring task)

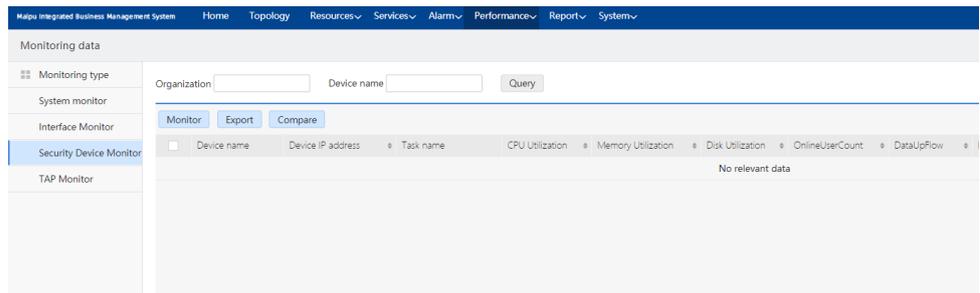


Figure 5-31 Monitoring data

For the related operations of the monitoring data, refer to the introduction of section 5.2 Monitoring Data.

## 5.2. Monitoring Data

Click "Performance" -> "Monitoring data" in the menu bar to open the "Monitoring data" page, including system monitoring, interface monitoring and security device monitoring, as follows:

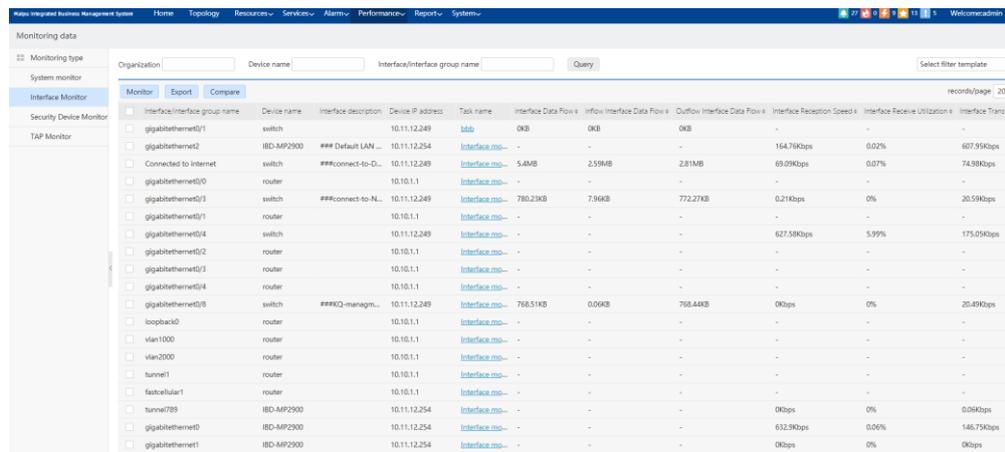


Figure 5-32 Monitoring data

Support the query of monitoring data according to the organization, device name / IP.

The monitoring data list item supports customizing. Click "List setting" on the right side of

the list header, as follows:

Device name	Device IP address	Task name	CPU Utilization	Memory Utilization	Organization
switch	10.11.12.249	System monitoring_aa	0%	63%	chengdu
Switch	10.11.12.13	System monitoring	-	-	Headquarters
IBD-MP2900	10.11.12.254	System monitoring_aa	0%	75%	chengdu
Switch	10.11.12.14	System monitoring	-	-	Headquarters
router	10.10.1.1	System monitoring	-	-	Headquarters
OA_GN_18F_4#_S3320	10.11.12.250	System monitoring	0%	57%	Headquarters
OA_GN_15F_1#_S3320	192.168.99.125	System monitoring	0%	57%	Headquarters
R4	10.11.12.111	System monitoring	5%	22%	Headquarters

Figure 5-33 Monitoring data

Display the “List setting” dialog box, as follows:

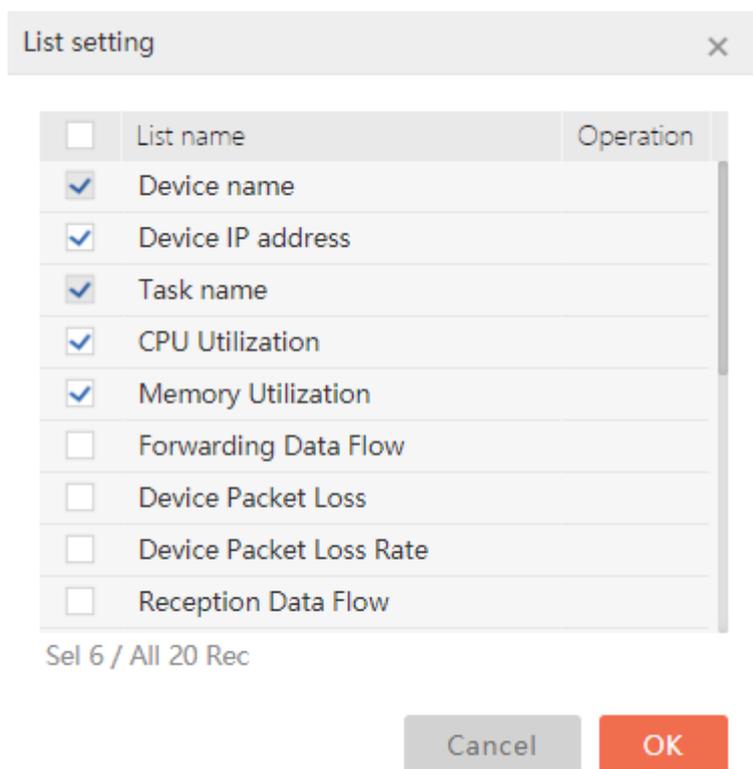


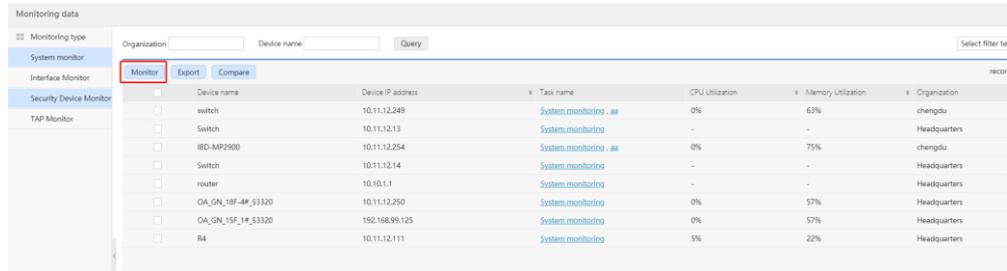
Figure 5-34 Select the index

You can check those lists and click  on the right to adjust the display order of the list in front or back.

### 5.2.1. System Monitoring Data

#### View monitoring data details

In the system monitoring data list, select one or more monitoring objects and click the "Monitor" button, as follows:



Device name	Device IP address	Task name	CPU Utilization	Memory Utilization	Organization
switch	10.11.12.249	System_monitoring_aa	0%	63%	chengdu
Switch	10.11.12.13	System_monitoring_aa	-	-	Headquarters
H3C-MP2900	10.11.12.254	System_monitoring_aa	0%	75%	chengdu
Switch	10.11.12.14	System_monitoring_aa	-	-	Headquarters
router	10.10.1.1	System_monitoring_aa	-	-	Headquarters
OA_GN_18F_4#_S3320	10.11.12.250	System_monitoring_aa	0%	57%	Headquarters
OA_GN_15F_1#_S3320	192.168.99.125	System_monitoring_aa	0%	57%	Headquarters
RA	10.11.12.111	System_monitoring_aa	5%	22%	Headquarters

Figure 5-35 Enter the monitoring data details interface

Enter the monitoring data details interface, as follows:

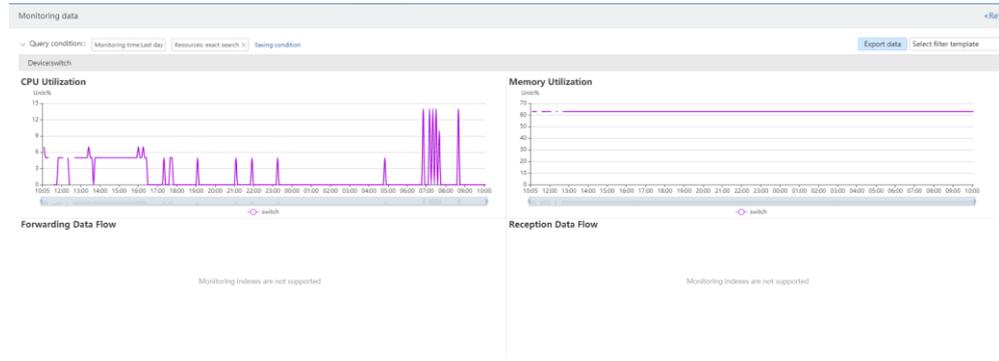


Figure 5-36 Monitoring data details

 **Note**

- The monitoring data details interface supports viewing up to 100 monitoring data charts.

The monitoring data details page will present the monitoring data of the selected monitoring indexes and the selected monitoring time in the form of chart.

The query conditions of monitoring data include monitoring indexes, monitoring time and resources

See Figure 5.1.2 in Chapter 5.1 Monitoring Task for monitoring indexes;

The monitoring time includes the current day, the late week, the late month, the last half year, real-time and customized;

For resources, you can select devices or device groups;

Click [Saving condition](#) to open the “Saving condition” dialog box, as follows:

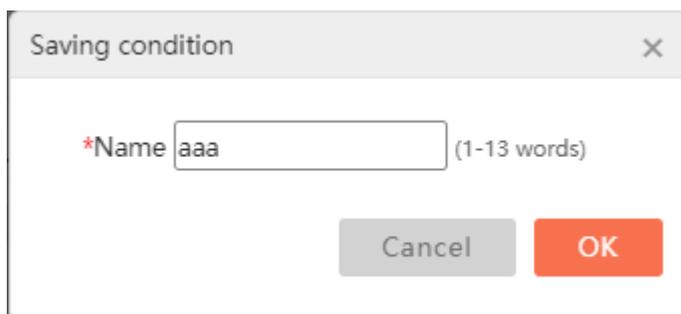


Figure 5-37 Saving condition

Enter the name of the saved query condition and click "OK" to save the query condition.

The query criteria will appear in the drop-down box of the filter template, as follows:

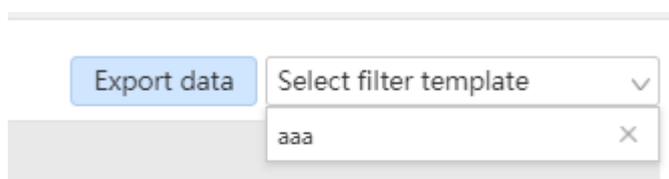


Figure 5-38 Filter template

Click this query condition to query the monitoring data according to the query condition.

You can click the "x" button to delete the query condition, as follows:

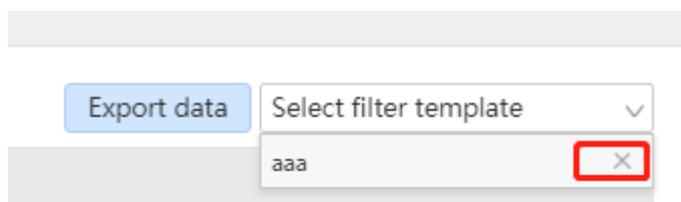


Figure 5-39 Delete the template

Click the "X" button to display the dialog box of confirming the deletion, as follows:

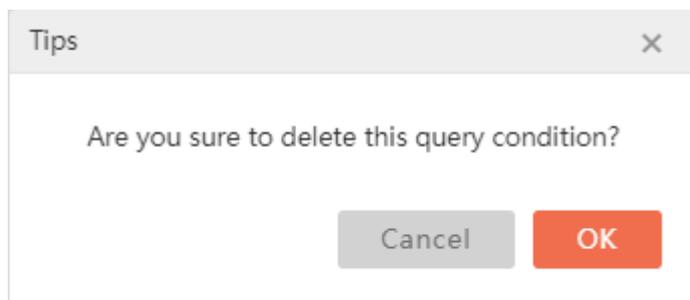


Figure 5-40 Confirm the deletion

Click  to delete the query condition.

Click **Export data** to export all the monitoring data details of this page to excel, as follows:



Figure 5-41 Export monitoring data details

In the monitoring data details page, you can also add or modify the monitoring object. Click the "Select resource" button to open the "Select resources" dialog box, as follows:

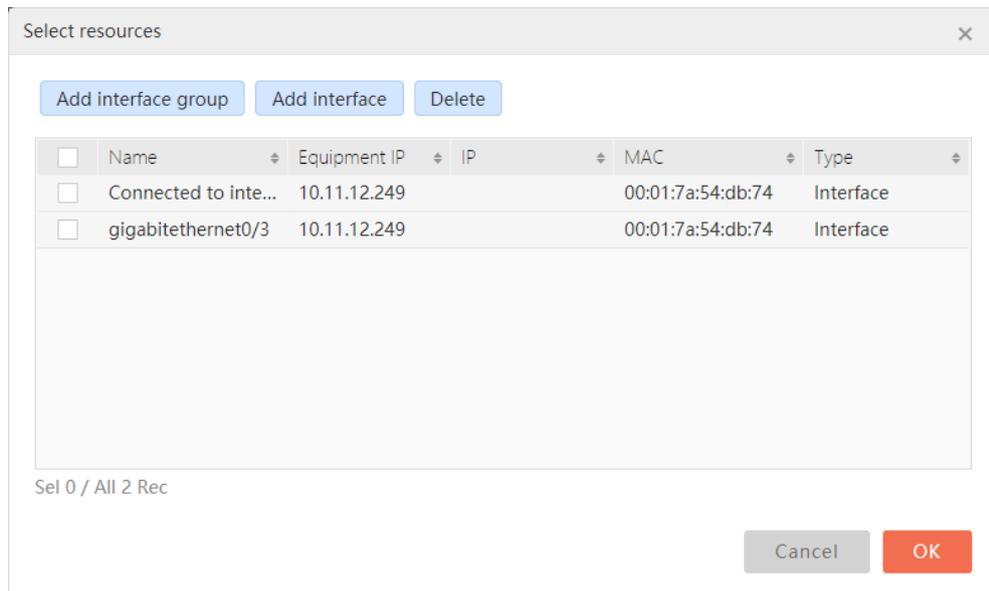


Figure 5-42 Select the resource

You can delete the selected resource or add the "Device" or "Device group" resource. For the adding of the device or device group, please refer to the section of *Select Resource* in Chapter 5.1.1 *System Monitoring*.

### Monitoring data comparison

In the system monitoring data list, select five or more than five monitoring objects, and click the "Compare" button, as follows:

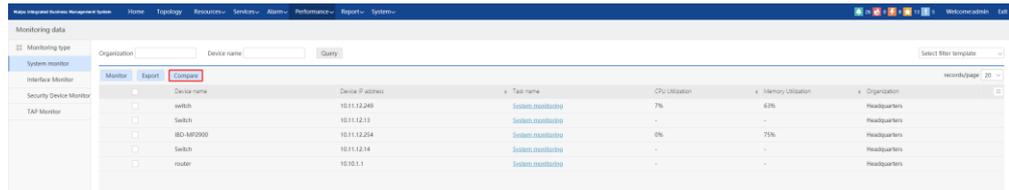


Figure 5-43 Compare monitoring data

Enter the monitoring data comparison interface, as follows:

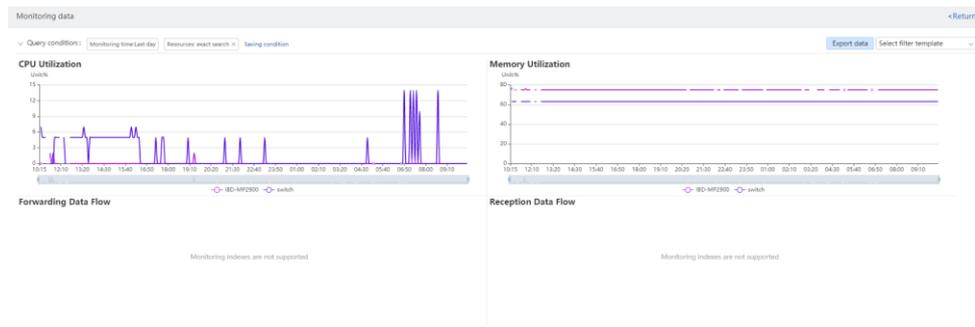


Figure 5-44 Compare monitoring data

The monitoring data comparison page will compare and present the monitoring indexes of the selected multiple monitoring objects and the monitoring data within the monitoring time in the form of charts.

Click **Export data** to export all monitoring data of this page to excel, as follows:

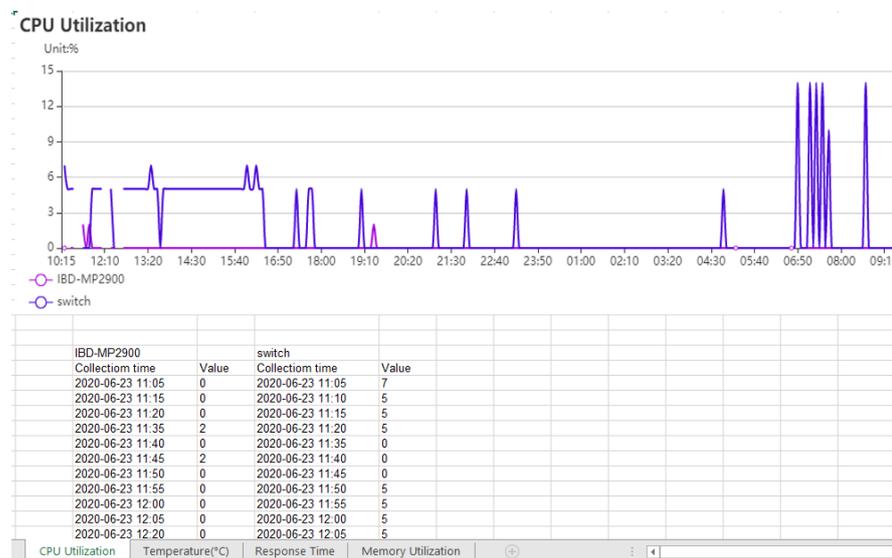


Figure 5-45 Compare and export the monitoring data

### Export the monitoring data

On the system monitoring data list page, click the "Export" button to export all monitoring data meeting the query conditions to excel, as follows:

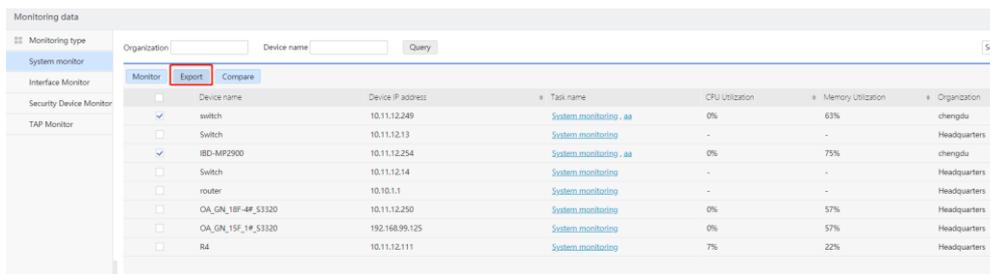


Figure 5-46 Export the monitoring data

The exported data is as follows:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Device name	Device IP	Task name	CPU Utiliza	Memory U	Forwarding	Reception	Device Pac	Device Pac	Voltage In	Voltage O	Current In	Current O	Temperatu	Fan speed	Response
switch	10.11.12.249	System m	0.0%	63.0%									57.0°C		1.0ms
Switch	10.11.12.13	System m	0.0%												
IBD-MP2900	10.11.12.254	System m	0.0%	75.0%									69.0°C		0.0ms
Switch	10.11.12.14	System m	0.0%												
router	10.10.1.1	System m	0.0%												
OA_GN_18	10.11.12.250	System m	0.0%	57.0%									77.0°C		1.0ms
OA_GN_15	192.168.99	System m	0.0%	57.0%									69.0°C		2.0ms
R4	10.11.12.11	System m	7.0%	22.0%									55.0°C		0.0ms

Figure 5-47 The exported monitoring data

### 5.2.2. Interface Monitoring Data

#### View monitoring data details

In the interface monitoring data list, select one or more monitoring objects and click the "Monitor" button, as follows:

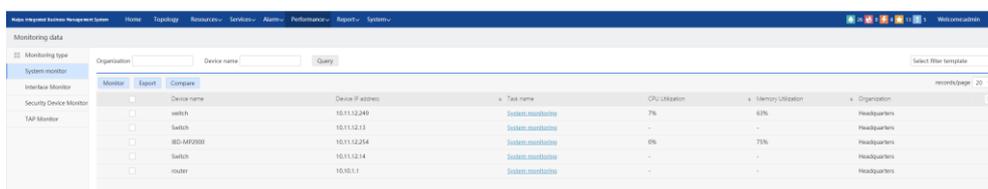


Figure 5-48 Enter the monitoring data details

Enter the monitoring data details page, as follows:

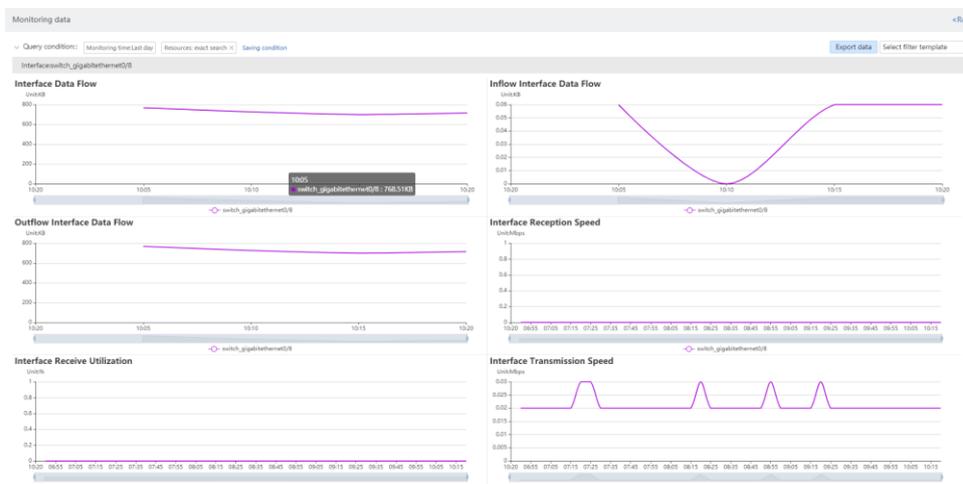


Figure 5-49 Monitoring data details

The monitoring data details page will present the monitoring data of the selected monitoring indexes and the selected monitoring time in the form of chart.

The query conditions of monitoring data include monitoring indexes, monitoring time and resources

See Figure 5.1.2 in Chapter 5.1 Monitoring Task for monitoring indexes;

The monitoring time includes the current day, the late week, the late month, the last half year, real-time and customized;

For resources, you can select the interface or interface group;

For the storage, deletion and use of query conditions of monitoring data, please refer to the section View monitoring data details of chapter 5.2.1 System Monitoring Data.

Click **Export data** to export all the monitoring data details of this page to excel, as follows:

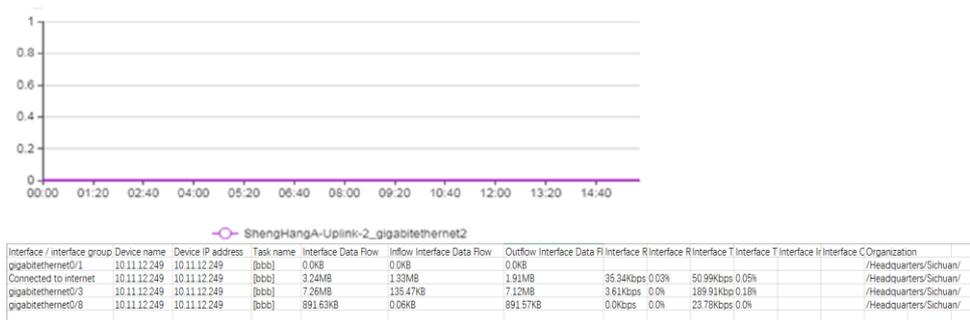


Figure 5-50 Export the monitoring data

In the monitoring data details page, you can also add or modify the monitoring object. Click the "Select resource" button to open the "Select resources" dialog box, as follows:

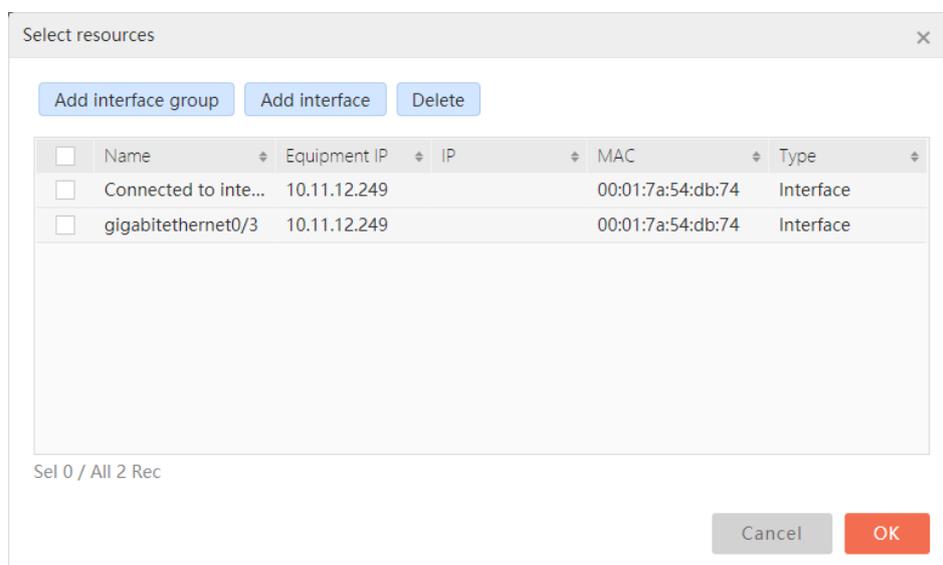


Figure 5-51 Select the resource

You can delete the selected resource or add the “Interface” or “Interface group” resource. For the adding of the interface or interface group, please refer to the section of *Select Resource* in Chapter 5.1.1 *System Monitoring*.

### Compare the monitoring data

In the interface monitoring data list, select five or more than five monitoring objects, and click the "Compare" button, as follows:

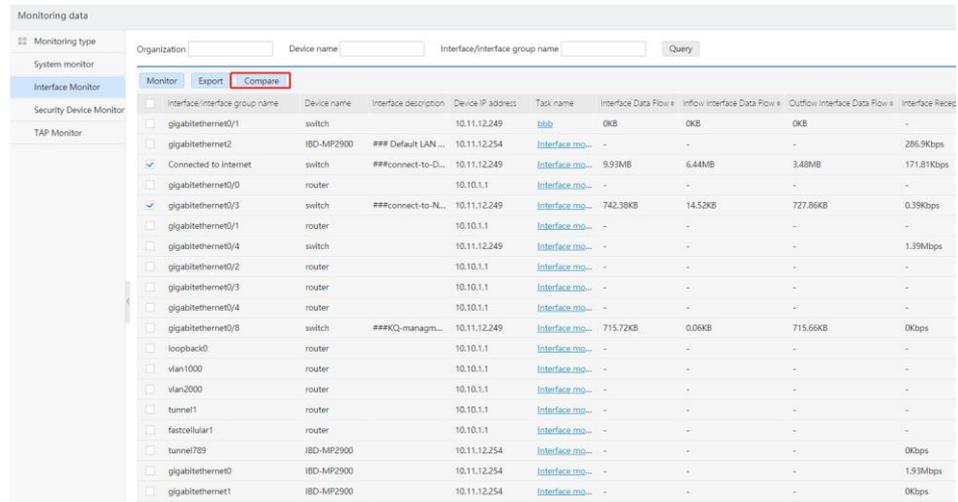


Figure 5-52 Compare the monitoring data

Enter the monitoring data comparison interface, as follows:

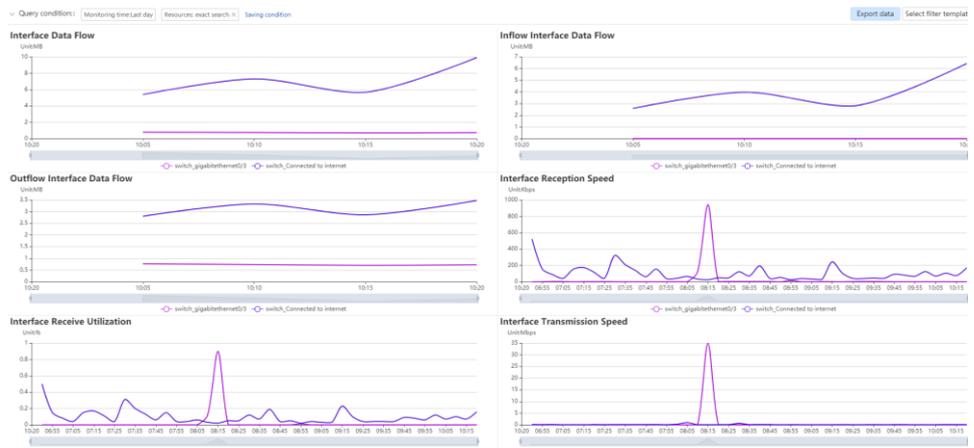


Figure 5-53 Compare the monitoring data

The monitoring data comparison page will compare and present the monitoring indexes of the selected multiple monitoring objects and the monitoring data within the monitoring time in the form of charts.

Click  to export all monitoring data of this page to excel, as follows:

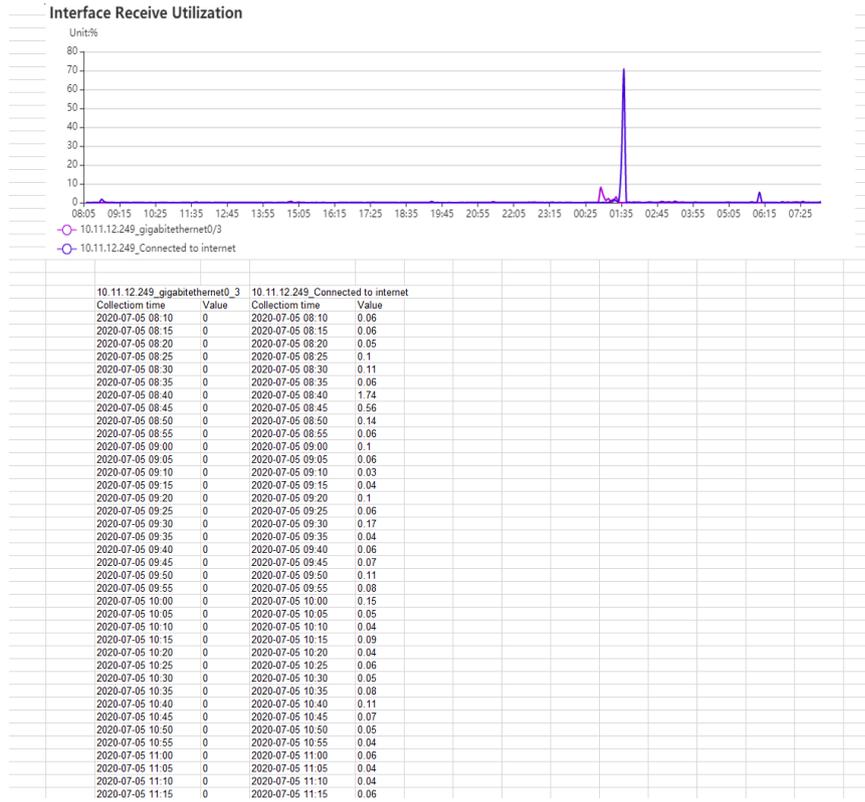


Figure 5-54 Compare and export the monitoring data

### Export the monitoring data

On the interface monitoring data list page, click the "Export" button to export all monitoring data meeting the query conditions to excel, as follows:

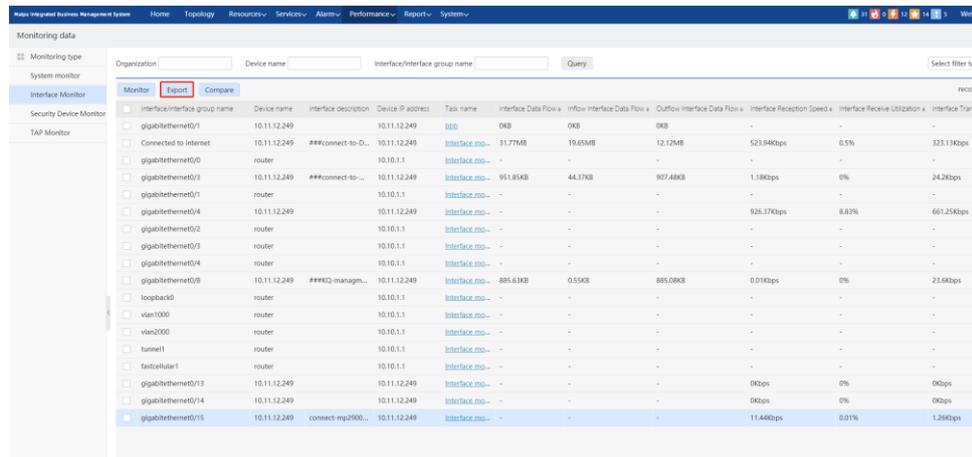


Figure 5-55 Export the monitoring data

The exported data is as follows:

Interface / interface group name	Device name	Device IP	Task name	Interface C	Inflow	Inte	Outflow	In	Interface R	Interface R	Interface T	Interface T	Interface I	Interface C	Organization
gigabitethernet0/1	10.11.12.249	10.11.12.24	(bbb)	0.0KB	0.0KB	0.0KB									/Headquarters/Sichuan/
Connected to internet	10.11.12.249	10.11.12.24	Interface r	31.77MB	19.65MB	12.12MB			523.94Kbp	0.5%	323.13Kbp	0.31%			/Headquarters/Sichuan/
gigabitethernet0/0	router	10.10.1.1	Interface r												/Headquarters/
gigabitethernet0/3	10.11.12.249	10.11.12.24	Interface r	951.85KB	44.37KB	907.48KB			1.18Kbps	0.0%	24.2Kbps	0.02%			/Headquarters/Sichuan/
gigabitethernet0/11	router	10.10.1.1	Interface r												/Headquarters/
gigabitethernet0/4	10.11.12.249	10.11.12.24	Interface r						926.37Kbp	8.83%	661.25Kbp	6.31%			/Headquarters/Sichuan/
gigabitethernet0/2	router	10.10.1.1	Interface r												/Headquarters/
gigabitethernet0/3	router	10.10.1.1	Interface r												/Headquarters/
gigabitethernet0/4	router	10.10.1.1	Interface r												/Headquarters/
gigabitethernet0/8	10.11.12.249	10.11.12.24	Interface r	885.63KB	0.55KB	885.08KB			0.01Kbps	0.0%	23.6Kbps	0.0%			/Headquarters/Sichuan/
loopback0	router	10.10.1.1	Interface r												/Headquarters/
vlan1000	router	10.10.1.1	Interface r												/Headquarters/
vlan2000	router	10.10.1.1	Interface r												/Headquarters/
tunnel1	router	10.10.1.1	Interface r												/Headquarters/
fastcellular1	router	10.10.1.1	Interface r												/Headquarters/
gigabitethernet0/13	10.11.12.249	10.11.12.24	Interface r						0.0Kbps	0.0%	0.0Kbps	0.0%			/Headquarters/Sichuan/
gigabitethernet0/14	10.11.12.249	10.11.12.24	Interface r						0.0Kbps	0.0%	0.0Kbps	0.0%			/Headquarters/Sichuan/
gigabitethernet0/15	10.11.12.249	10.11.12.24	Interface r						11.44Kbps	0.01%	1.26Kbps	0.0%			/Headquarters/Sichuan/

Figure 5-56 The exported monitoring data

### 5.3. Customize Monitoring Index

Click "Performance" -> "Customize monitoring index" in the menu bar to open the "Custom monitoring indexes" page, where you can customize the system monitoring indexes, as follows:

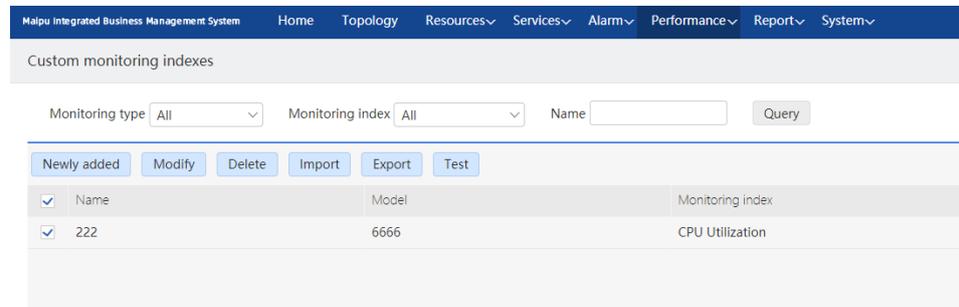


Figure 5-57 Customize the monitoring index

You can query the customized monitoring indexes by monitoring type, monitoring index, and name.

#### Add the monitoring index

On the "Custom monitoring indexes" interface, click "Add", as follows:

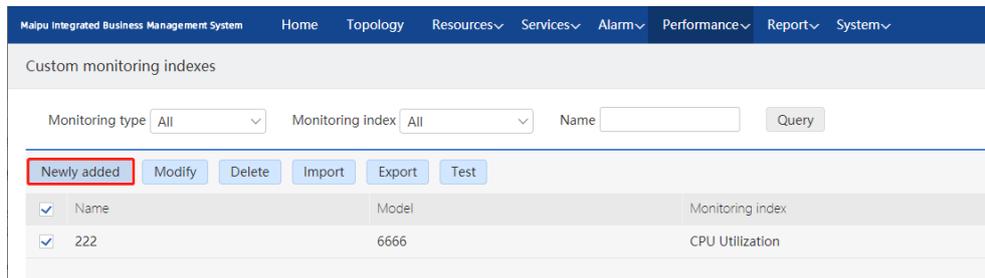


Figure 5-58 Add the monitoring index

Display the dialog box of adding the monitoring index, as follows:

Add monitoring index ✕

Index formula Description: “#” is the prefix and suffix character of the index node (MIB OID). All index nodes need to be enclosed by this character. It supports “+”, “-”, “\*”, “/”, and brackets. Rate followed by oid indicates (difference)/time period, Diff followed by oid indicates the difference between two calculations, DF64 and RT64 followed by oid indicates that the value obtained needs to be turned correspondingly.

Example 1: #1.3.6.1.2.1.11.1# indicates directly obtaining the MIB node value as the performance index collection value.

Example 2:#1.1.1.1.1.1.1Rate# indicates (the latest collection value of this node - the last collection value) / time period.

Example 3: #1.1.1.1.1.1.1Diff# represents the difference between two collection values.

\*Name  (1~64 words)

\*Monitoring type

\*Monitoring index

\*Company

\*Model

\*Formula  (1-320 words)

Figure 5-59 Add the monitoring index

Enter the monitoring indicator name (it cannot be repeated), select the monitoring type (system monitoring), select the monitoring index (CPU utilization, memory utilization), select the device model, enter the calculation formula of monitoring results, and click OK to add a monitoring indicator.

The device model is managed in the "Resources" – “Device type management” page.

### Modify the monitoring index

On the “Custom monitoring indexes” interface, select one monitoring index, and click “Modify”, as follows:

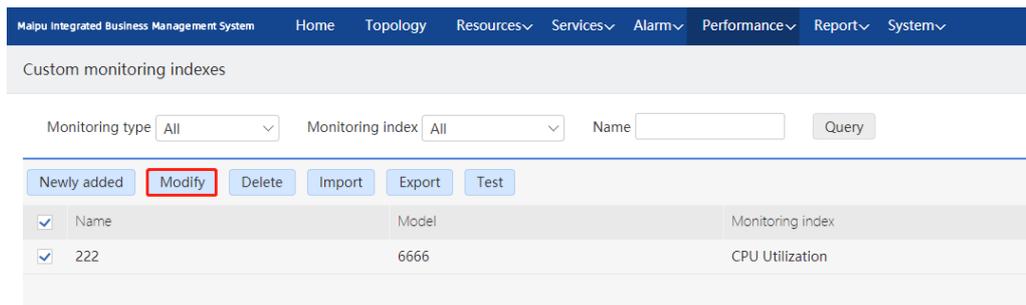


Figure 5-60 Modify the monitoring index

Display the “Modify monitoring index” dialog box, as follows:

Modify monitoring index

Index formula Description: “#” is the prefix and suffix character of the index node (MIB OID). All index nodes need to be enclosed by this character. It supports “+”, “-”, “\*”, “/”, and brackets. Rate followed by oid indicates (difference)/time period, Diff followed by oid indicates the difference between two calculations, DF64 and RT64 followed by oid indicates that the value obtained needs to be turned correspondingly.

Example 1: #1.3.6.1.2.1.11.1# indicates directly obtaining the MIB node value as the performance index collection value.  
Example 2:#1.1.1.1.1.1Rate# indicates (the latest collection value of this node - the last collection value) / time period.  
Example 3: #1.1.1.1.1.1Diff# represents the difference between two collection values.

\*Name  (1~64 words)

\*Monitoring type

\*Monitoring index

\*Company

\*Model

\*Formula  (1-320 words)

Cancel OK

Figure 5-61 Modify the monitoring index

You can modify the name, model and formula, and click **OK** to complete the modification of monitoring indexes.

### Delete the monitoring index

On the “Custom monitoring indexes” interface, select one ore more monitoring indexes, and click ‘Delete’, as follows:

Maipu Integrated Business Management System Home Topology Resources Services Alarm Performance Report System

Custom monitoring indexes

Monitoring type  Monitoring index  Name  Query

Newly added Modify **Delete** Import Export Test

<input checked="" type="checkbox"/>	Name	Model	Monitoring index
<input checked="" type="checkbox"/>	222	6666	CPU Utilization

Figure 5-62 Delete the monitoring index

Display the dialog box of confirming the deletion, as follows:

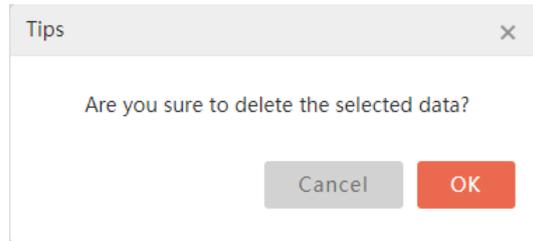


Figure 5-63 Delete the monitoring index

Click , and you can delete the selected monitoring index.

### Note

- Deleting the customized monitoring indexes in use will lead to the failure of monitoring tasks to collect corresponding data.

## Import the monitoring index

On the “Custom monitoring indexes” interface, click “Import”, as follows:

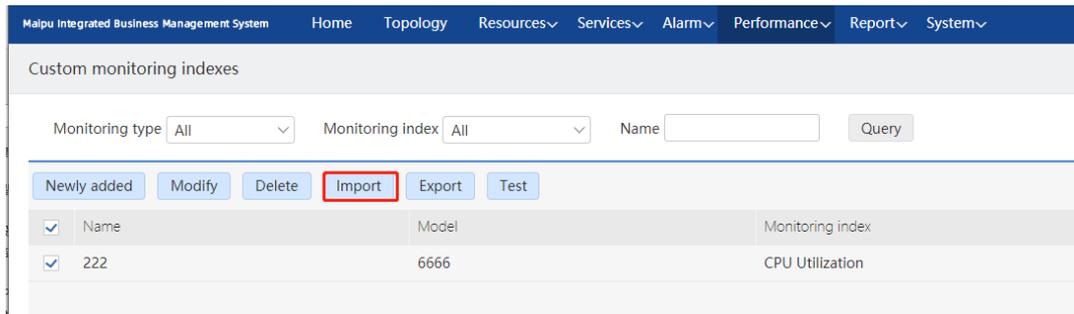


Figure 5-64 Import the monitoring index

Display the import dialog box, as follows:

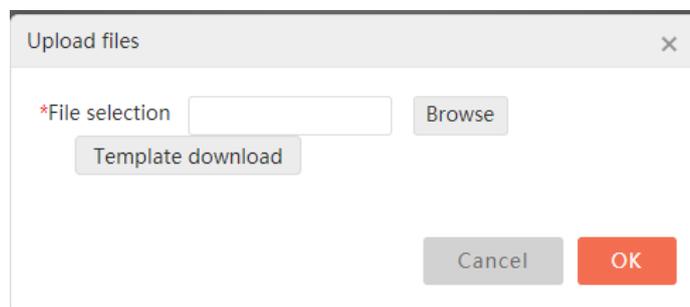


Figure 5-65 Import the monitoring index

Click the "Template download" button to download the import template. After filling in the desired monitoring index data according to the template requirements, click the "Browse"

button, select the desired file, and click  to complete the importing.

The contents of the import template are as follows:

Model	Monitor Index	Formula	Name
6666	CPU Utilization	#1.3.6.1.2.1.11.1#	222

Figure 5-66 Template

Move the mouse to the header, and the corresponding prompt information will appear to prompt the data filling requirements, as follows:

A	B	
Model		
Custom device model	M	1.4.1.5651.1.2.1.1.2.12.

请参看Sheet2输入设备型号，多个型号间以英文“,”逗号分隔

Figure 5-67 Import the monitoring index

After the importing fails, you will be prompted to download the import failure result, as follows:

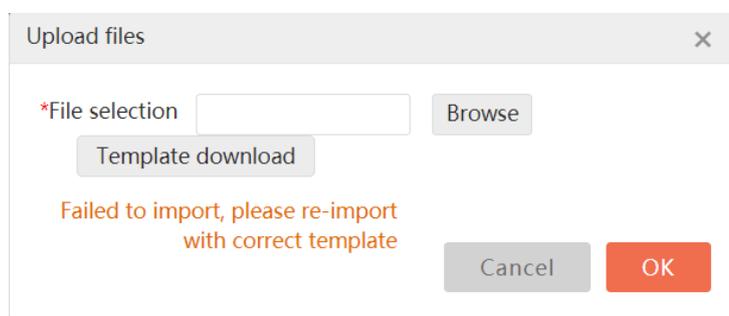


Figure 5-68 Import the monitoring index

Click "Download" to download the failure result file to the device and view it, as follows:

A	B	C	D	E	F
型号	监控指标	公式	名称		
SM-TET	内存利用率	(#1.3.6.1.4.1.5651.1.2.1.1.2.12.0#-#1.3.6.1.4.1.5651.1.2.1.1.test123	test123	[设备型号无效]	

Figure 5-69 Import the monitoring index

### Note

- A device type cannot be configured with multiple same monitoring indexes.
- Please refer to *Maipu Integrated Network Management Platform Troubleshooting V4.0* for specific import failure reasons and treatment methods.

## Export the monitoring index

On the "Custom monitoring indexes" interface, click "Export", as follows:

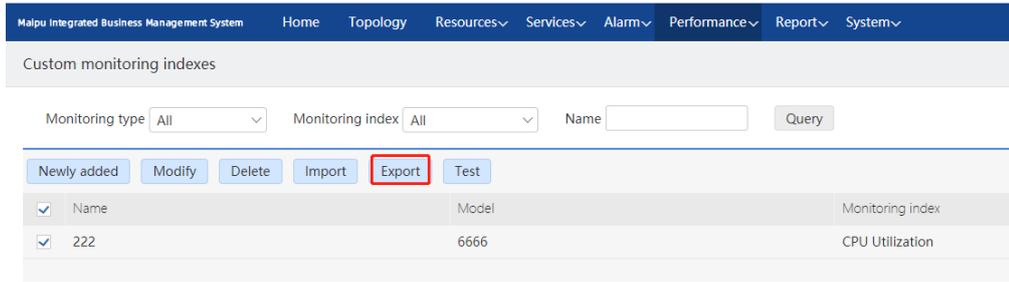


Figure 5-70 Export the monitoring index

You can export the customized monitoring indexes to the excel file, as follows:

Model	Monitor Index	Formula	Name
6666	CPU Utilization	#1.3.6.1.2.1.11.1#	222

Figure 5-71 Export the monitoring index

## 5.4. Link Detection

Link detection module uses the ping command to detect whether there is connectivity between devices or between network management server and devices.

### 5.4.1. Link Detection Configuration

The link detection configuration module provides the configuration for link detection time, link detection concurrency, etc.

Click "Performance" -> "Link Detection" -> "Link Detection Configuration" in the top navigation bar of the system to enter the link detection configuration page, as follows:

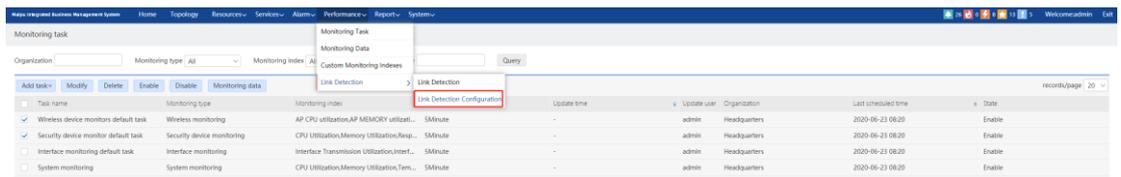


Figure 5-72 The entrance of the link detection configuration

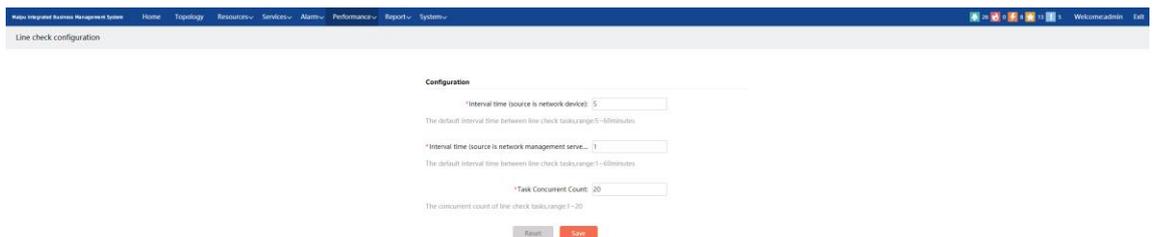
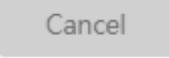


Figure 5-73 Link detection configuration

Interval time: The default interval (minutes) of link detection task execution can be

divided into two situations: one is that the source is the network device, the configurable time interval is 5-60, and the default is 5 minutes; the other is that the source is the network management server, the configurable time interval is 1-60, and the default is 1 minute.

Task concurrent count: the number of concurrent link detection tasks.

Click  to display the dialog box of confirming the saved parameter, as follows. Click  to confirm saving the current configuration information, and click  to drop the saving operation.

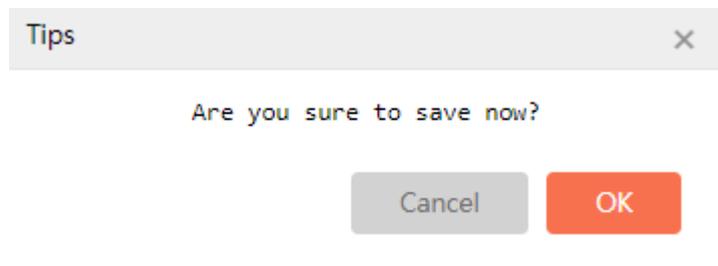


Figure 5-74 Save the link detection configuration

Click  to restore the interval time and task concurrency to the default value. The default value is the configuration parameter loaded from the page for the first time.

---

### Caution

- If you click the "Save" button, save the configuration and refresh the browser, and the value of the latest configuration will be restored when resetting.
- 

## 5.4.2. Link Detection

By default, the link detection list displays all link detection tasks, including name, source device name, source device IP, peer device name, peer device IP, status, update user, organization, latest detection result, recent packet loss rate, recent average delay, latest detection time, historical details and description, etc. You can sort these fields. You also can add, modify, delete, import, and refresh the link detection tasks. Besides, you can perform fuzzy query according to the name, organization, latest detection time, detection result, source device and peer device.

Click "Performance" - > "Link Detection" - > "Link Detection" in the top navigation bar of the system to enter the link detection page, as follows:

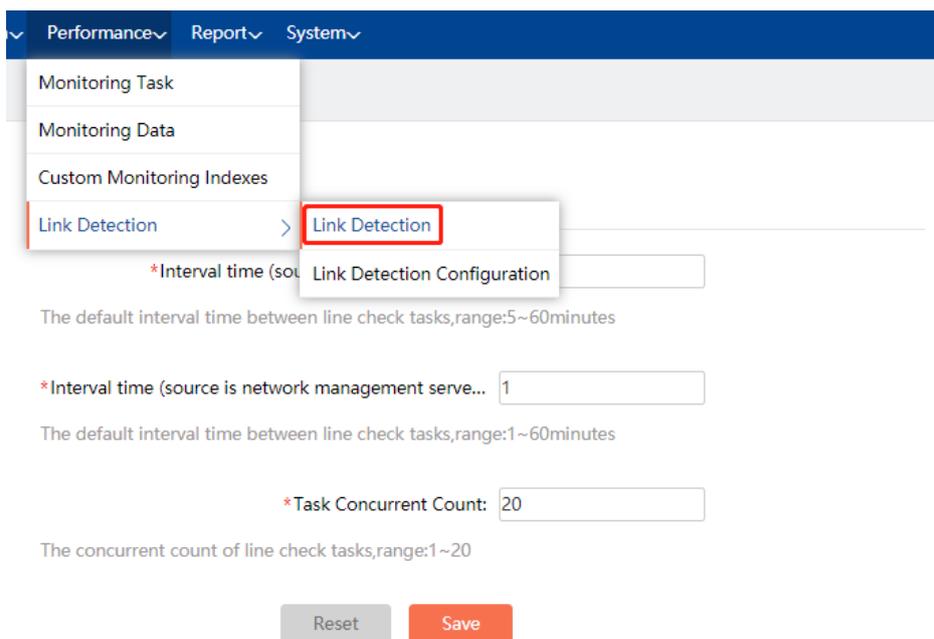


Figure 5-75 The entrance of link detection

Link detection

Name  Organization  Last detection time  Detection result: all

Source device  End-to-end device  Query

Name	Source device name	Source device IP	Peer device name	Peer device IP	Status	Update user	Organization	Recent test results	Recent packet loss
1	S2300-10TP-AC (E1)	10.11.12.5	CP2300-10TP-D...	10.11.12.87	Ready	admin	Headquarters		
1800X-	NMServer		router	10.10.1.1	Ready	admin	Headquarters	●	100%

Figure 5-76 Link detection

## ! Caution

- Organization: If the source is a network device, the organization is the organization of the network device; if the source is a network server, the organization is the organization of the current administrator.
- Link detection status: to be detected and being detected
- Detection results: there are four kinds of detection results: unknown, normal, packet loss and disconnection, respectively corresponding colors: unknown ●, normal ●, packet loss ● and disconnection ●.

## Add link detection task

Click **Add** in the link detection list to pop up the "Add" dialog box, as follows. Enter the link name and description, select the source device type (network device, network management server), source device/interface and peer device, and click "Save" to add a link detection task.

Figure 5-77 Add the link detection task

### **!** Caution

- If "Network device" is selected as the source device type, the source device must be configured with the correct Telnet certificate or SSH certificate.

Click **Choose** behind the source device/interface to enter the "Select source device" dialog box, as shown in the figure below. Click the device tree on the left, and you can select the corresponding interface in the right interface information list. At the same time, it supports fuzzy query for the device name and interface IP. Select the device and interface and click **OK** to save the selected source device/interface information. The selection mode of the peer device is the same as above.

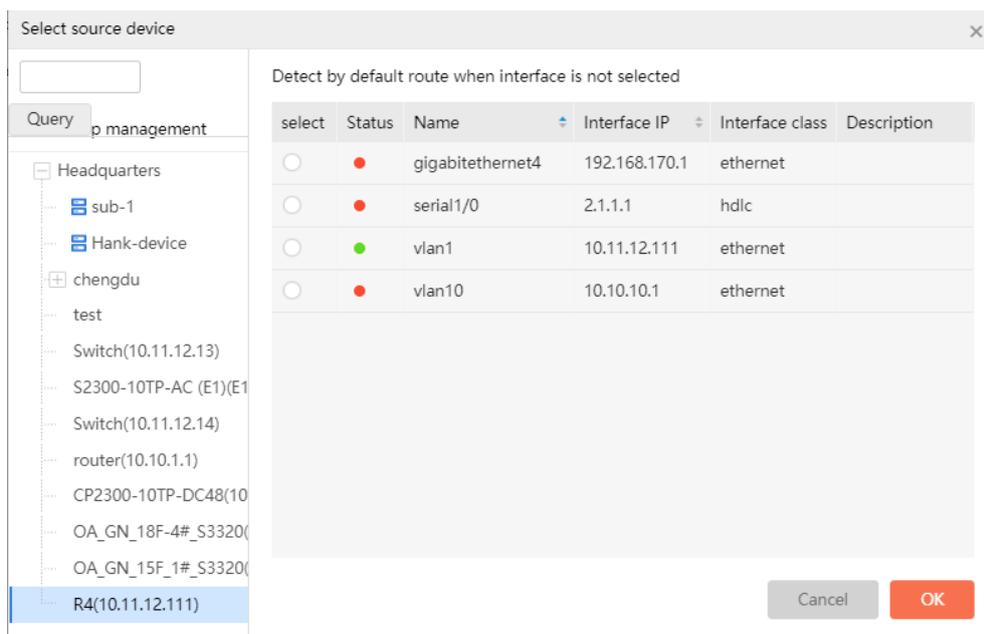


Figure 5-78 Select the source device

## Caution

- When selecting the source device, it is not necessary to select the source device interface. If not selecting, use the access IP of the device for detection by default.
- The interface of the peer device is mandatory, and you can input the IP address manually.

Select the advanced configuration option, and you can configure packets and alarms, including the number of packets, packet size (bytes), allowable delay (MS), packet loss rate threshold, continuous disconnection threshold, and continuous packet loss threshold. The specific configuration information is shown in the following table:

Add
×

\*Link name

Source device type  Network devices  Network management server

\*Source device/interface

Some devices do not support source interface Ping

\*End-to-end device

IP address can be entered manually

Description

---

Advanced configuration ^

Packet configuration

---

\*Number of packets  (range: 3-20)

\*Message size (byt...  (range: 76-1024)

\*Allowed delay (ms)  (range: 50-2000)

Alarm configuration

---

\*Packet loss rate threshold (%)  (range: 0-100)

\*Continuous packet loss threshold

3/64 characters,you can input 61 characters!

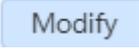
Figure 5-79 Advanced configuration information

## Note

- The default value of each option under advanced configuration have been given as above.
- Some devices do not support packet configuration, and the packet configuration is invalid.
- Select the network device/network server by the source device type option. When the network server is selected, the source device/interface option cannot be configured
- For the peer device, you can input IP manually.
- When the source type is "Network management server", the allowed delay is not configurable.

Click , and you can successfully add a link detection task.

## Modify link detection task

Select a link detection task, click  of the link detection list, and the "Modify" dialog box will pop up. The link name, description and advanced configuration information can be modified. The source device type, source device/interface and peer device options cannot be modified. Click  to save the modification.



\*Link name

Source device type  Network devices  Network management server

\*Source device/interface    
Some devices do not support source interface Ping

\*End-to-end device    
IP address can be entered manually

Description

---

Advanced configuration 

Packet configuration

---

\*Number of packets  (range: 3-20)

\*Message size (byt...  (range: 76-1024)

\*Allowed delay (ms)  (range: 50-2000)

Alarm configuration

---

\*Packet loss rate threshold (%)   
(range: 0-100)

\*Continuous packet loss threshold

Figure 5-80 Modify the link detection task

### Delete link detection task

Select one or more link detection tasks, and click  of the link detection list to open the dialog box of confirming the detection, as shown below. Click  to delete the link detection task, and click  to drop the deletion.

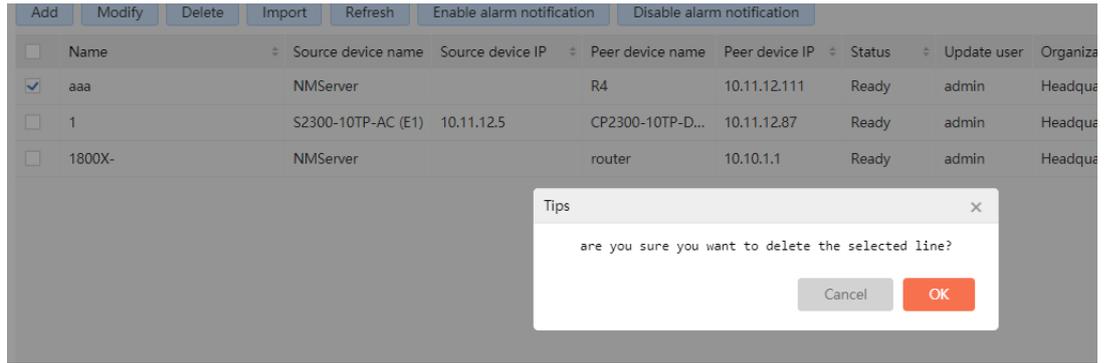


Figure 5-81 Confirm the deletion

**Note**

- The being detected task cannot be deleted.

**Import link detection task**

Click **Import** of the link detection list to open the “Import” dialog box, as shown in the following figure:

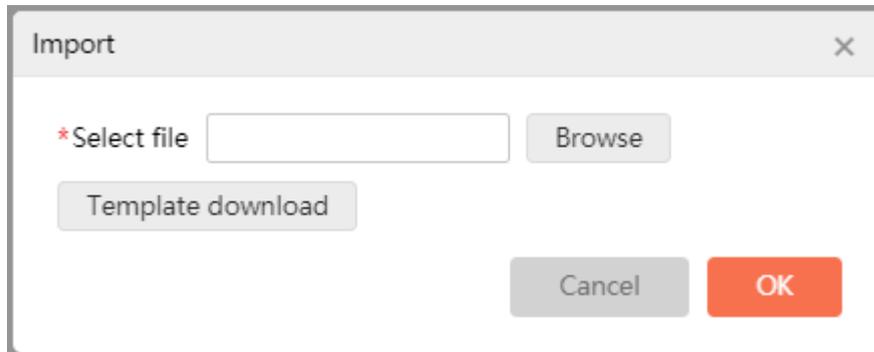


Figure 5-82 Import the link detection task

Click **Browse** to select the desired file. and then click **OK** to import the link detection task. The file template can be downloaded through the button **Template download**; the template contains the link name, source device IP, peer device IP, packet size, packet quantity, allowed delay, packet loss rate threshold, continuous packet loss threshold, continuous disconnection threshold, and description information, as shown in the following figure:

Continuous break threshold	description
1	test
1	test

Figure 5-83 Link import template

## Note

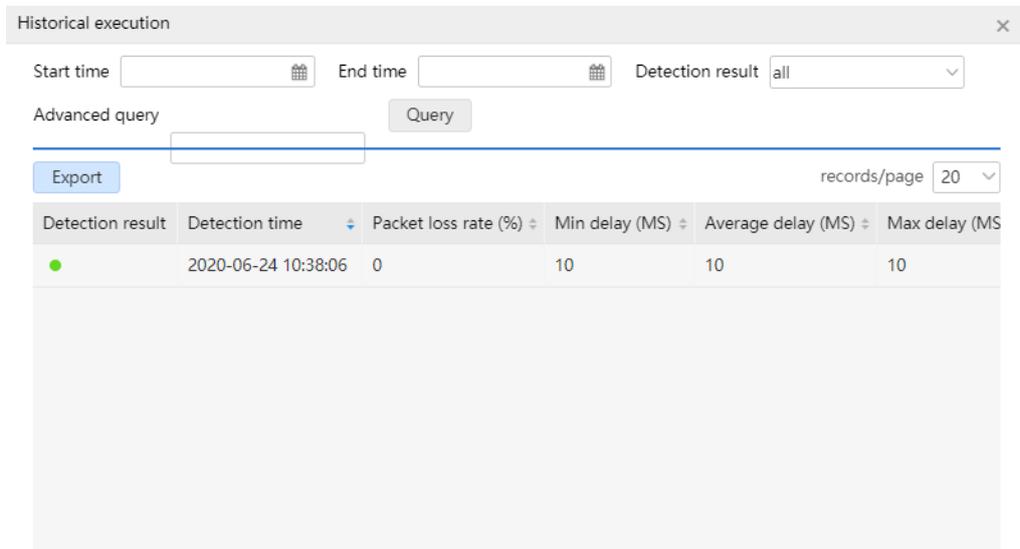
- When the imported link source is the network management server, the IP is 127.0.0.1.
- Required items: link name, source device IP, peer device IP, packet size, packet quantity, allowed delay, packet loss rate threshold, continuous packet loss threshold, continuous disconnection threshold.

### Refresh link detection task

Click  of the link detection list to refresh the link detection tasks in the current list, refreshing the link status and the latest detection results.

### View historical details

Click the "Historical details" after each task in the link detection list to pop up the "Historical execution" dialog box as follows. You can query the historical execution status of the task through the start time, end time, detection results and advanced query box. Click the header detection time, packet loss rate, minimum delay, average delay and maximum delay to sort. You can click  to export the detection results.



Detection result	Detection time	Packet loss rate (%)	Min delay (MS)	Average delay (MS)	Max delay (MS)
●	2020-06-24 10:38:06	0	10	10	10

Figure 5-84 Historical details dialog box

## Caution

- Detection results: there are four kinds of detection results: unknown, normal, packet loss and disconnection, respectively corresponding colors: unknown , normal , packet loss  and disconnection .

A	B	C	D	E	F	G	H
Line name	Detection time	Packet loss(%)	Minimum delay(ms)	Average delay(ms)	Maximum delay(ms)	Detection result	description
1900X	2020-06-24 10:38:06	0	10	10	10	normal	

Figure 5-85 Export detection result

### Link query

This page supports the query of link detection tasks, as shown in the figure below. In the link query panel, you can perform the fuzzy query by name, organization, latest detection time, detection results, source device, peer device, etc.

Link detection

Add
Modify
Delete
Import
Refresh
Enable alarm notification
Disable alarm notification

<input type="checkbox"/>	Name	Source device name	Source device IP	Peer device name	Peer device IP	Status	Update user	Organization	Recent test results	Recent packet loss rate
<input type="checkbox"/>	1900X	NMServer		R4	10.11.12.111	Ready	admin	Headquarters	<span style="color: green;">●</span>	0%
<input type="checkbox"/>	1	S2300-10TP-AC (E1)	10.11.12.5	CP2300-10TP-D...	10.11.12.87	Ready	admin	Headquarters	<span style="color: gray;">●</span>	
<input type="checkbox"/>	1800X-	NMServer		router	10.10.1.1	Ready	admin	Headquarters	<span style="color: red;">●</span>	100%

Figure 5-86 Query link detection task

## 6. Alarm Management

The alarm module is responsible for storing the alarm information generated by the device and other modules, and providing it to the user on the interface. In addition, the alarm module also provides various configurations, such as alarm notification configuration, alarm shielding configuration, alarm level redefinition, etc. The alarm notification configuration can encapsulate some important messages (such as device offline, device load is too big, etc.) in the network management system or the messages concerned by the administrator into alarm information, which can be sent to the administrator in the form of SMS, e-mail, voice or wechat, so that the network administrator can timely and dynamically understand the operation of the network, and perceive the possible problems in the network in advance, improving the management efficiency and early warning capability.

### 6.1. Alarm Information

Click "Alarm" -> "Alarm information" in the menu bar to open the alarm information page of network management system. The navigation on the left side of the alarm information interface includes current alarms, shielded alarms and all alarms. The alarm events triggered by all components can be found in the alarm event view, and the effect is shown in Figure 6-1.



Figure 6-1 Alarm information

#### Current alarms

What the current alarm presents to the user is the unprocessed alarm information. Users can query by the alarm level, confirmation status and alarm time accurately in the current alarm interface, and can also perform fuzzy query for the alarm source, alarm type, organization and description. At the same time, it also supports accurate query through alarm type and alarm source. The effect is shown in Figure 6-2.

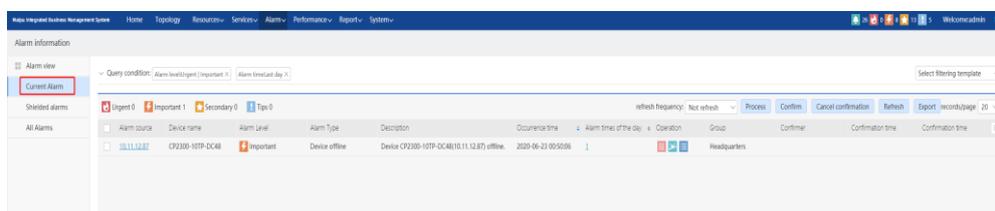


Figure 6-2 Current alarms

Users can query accurately by alarm type. First, select the alarm type to accurate matching, and then click the select button of “Alarm type”. Then the “Add alarm type” dialog box will appear, and the user can add the alarm type. Finally, click “OK” to query accurately according to the alarm type. The effect is shown in Figure 6-3.

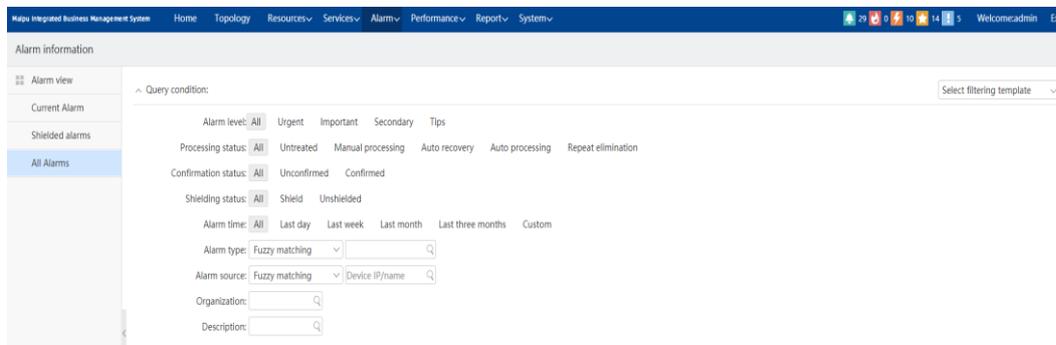


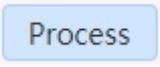
Figure 6-3 Query by the alarm type accurately

Users can also accurately query through the alarm source. First, select the alarm source to accurate matching, click the select button of “Alarm source”, and then, the “Add alarm source” dialog box will appear. The user can add the alarm source by adding device group, adding device, adding interface group, and adding local network management. Finally, click “OK” to query accurately according to the alarm source. The effect is shown in Figure 6-4.

Alarm source	Device name	Alarm Level	Alarm Type	Description	Occurrence time	Alarm times of the day	Operation	Group	Confirmer	Confirmation time	Confirmation time	
<input type="checkbox"/>	10.11.12.87	CP2300-10TP-DIC48	Important	Device offline	Device CP2300-10TP-DIC48(10.11.12.87) offline.	2020-06-23 00:50:06	1					Headquarters

Figure 6-4 Query by the alarm source accurately

In addition, users can also process, confirm, cancel confirmation and export the alarm information. Processing, confirming, and canceling confirmation support batch operation.

Select the desired alarm event, click  on the current alarm interface, and a pop-up box will appear. The user needs to fill in the processing opinions in the pop-up

box (required), and finally click  (see the figure below) to process the selected alarm event. The processed alarm information can only be viewed in all alarm information, and the current alarm will not be displayed.

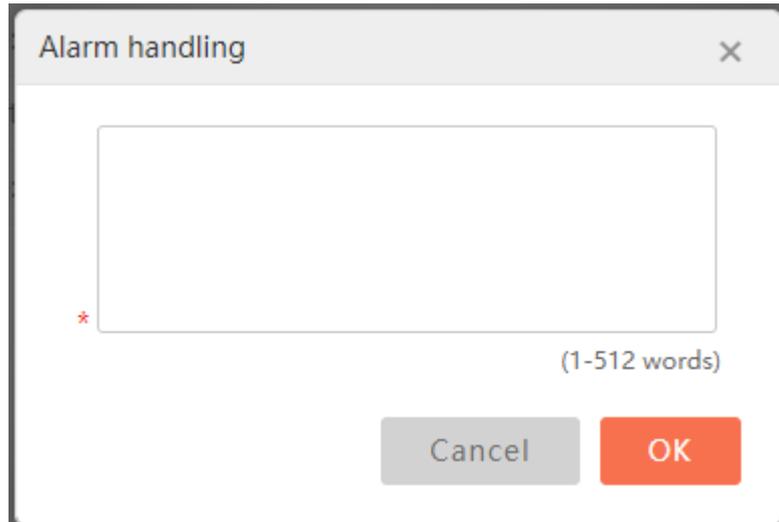


Figure 6-5 Process alarm event

Select the desired alarm event (not including the confirmed alarm event), click “Confirm” in the current alarm interface, and a pop-up box will appear. The user needs to fill in the confirmation opinion in the pop-up box, and finally click “OK” (see the figure below) to confirm the selected alarm event.

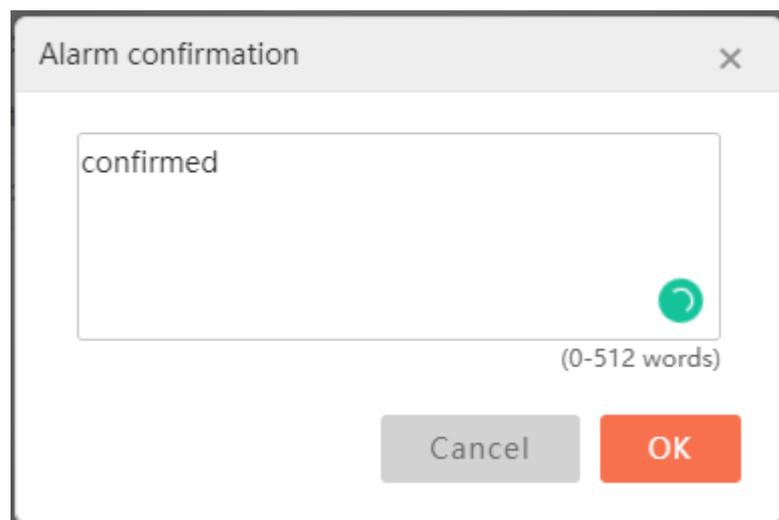


Figure 6-6 Confirm the alarm event

Select the desired alarm event (not including the confirmed alarm event), click “Cancel confirming” in the current alarm interface, and then, a pop-up box will appear. Click “OK” (see the figure below) to cancel the confirmation of the selected alarm event.

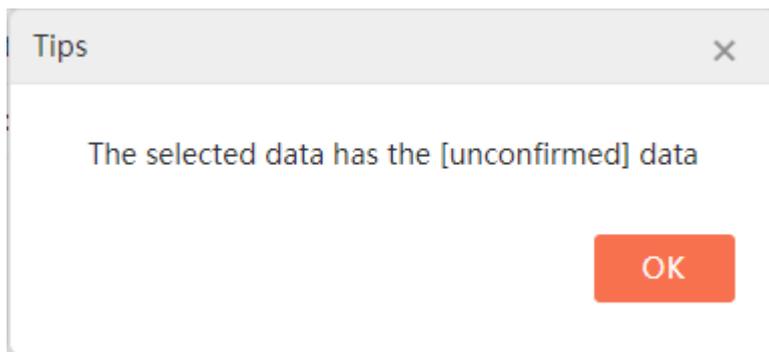


Figure 6-7 Cancel confirming the alarm event

After the user queries the desired alarm, click  to export all the alarm events in the list (including paging alarm events).

Alarm source	Device name	Alarm Level	Alarm Type	Description	Occurrence time	Operation	Group	Confirmer	Confirmation time	Confirmation time	Processor	Proce
<input type="checkbox"/>	10.11.12.5	S2300-10...	Seco...	Link che...	link [Name:1, source Device/ip:52300-10TP-AC ...	2020-06-24 10:50:00		Hea...				
<input type="checkbox"/>	10.11.12.5	S2300-10...	Seco...	Link che...	link [Name:1, source Device/ip:52300-10TP-AC ...	2020-06-24 10:45:00		Hea... system	2020-06-24 10...		system	2020-06-
<input type="checkbox"/>	10.11.12.5	S2300-10...	Seco...	Link che...	link [Name:1, source Device/ip:52300-10TP-AC ...	2020-06-24 10:40:00		Hea...	2020-06-24 10...		system	2020-06-
<input type="checkbox"/>	10.11.12.5	S2300-10...	Seco...	Link che...	link [Name:1, source Device/ip:52300-10TP-AC ...	2020-06-24 10:30:00		Hea... system	2020-06-24 10...		system	2020-06-
<input type="checkbox"/>	10.11.12.53	Local net...	Impo...	Link disc...	link [Name:1800X-, source Device/ip:Local netw...	2020-06-24 10:29:07		Hea...				
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP ac...	Device IBD-MP2900(10.11.12.254) SNMP avalla...	2020-06-24 08:49:18		che... system	2020-06-24 08...		system	2020-06-
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP u...	Device IBD-MP2900(10.11.12.254) SNMP unava...	2020-06-24 08:46:21		che... system	2020-06-24 08...		system	2020-06-
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP ac...	Device IBD-MP2900(10.11.12.254) SNMP avalla...	2020-06-24 06:57:18		Hea... system	2020-06-24 06...		system	2020-06-
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP u...	Device IBD-MP2900(10.11.12.254) SNMP unava...	2020-06-24 06:43:21		Hea... system	2020-06-24 06...		system	2020-06-
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP ac...	Device IBD-MP2900(10.11.12.254) SNMP avalla...	2020-06-24 06:35:15		Hea... system	2020-06-24 06...		system	2020-06-
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP u...	Device IBD-MP2900(10.11.12.254) SNMP unava...	2020-06-24 06:27:21		Hea... system	2020-06-24 06...		system	2020-06-
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP ac...	Device IBD-MP2900(10.11.12.254) SNMP avalla...	2020-06-24 06:08:15		Hea... system	2020-06-24 06...		system	2020-06-
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP u...	Device IBD-MP2900(10.11.12.254) SNMP unava...	2020-06-24 06:05:21		Hea... system	2020-06-24 06...		system	2020-06-
<input type="checkbox"/>	10.11.12.254	IBD-MP29...	Tips	SNMP ac...	Device IBD-MP2900(10.11.12.254) SNMP avalla...	2020-06-24 05:17:21		Hea... system	2020-06-24 05...		system	2020-06-

Figure 6-8 Export the alarm event

### Shielded Alarms

What the shielded alarm presents to the user is the shielded alarm information. Users can query accurately through the alarm level and alarm time on the shielded alarm interface, and can also make fuzzy query for the alarm source, alarm type, organization and description. At the same time, it also supports accurate query by alarm type and alarm source. The effect is shown in Figure 6-9.

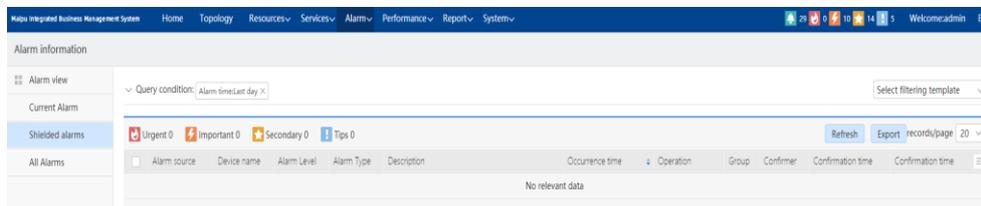


Figure 6-9 Shielded alarms

After the user queries the desired shielded alarm information, click  to export all the shielded alarm events in the list (including paging shielded alarm events).

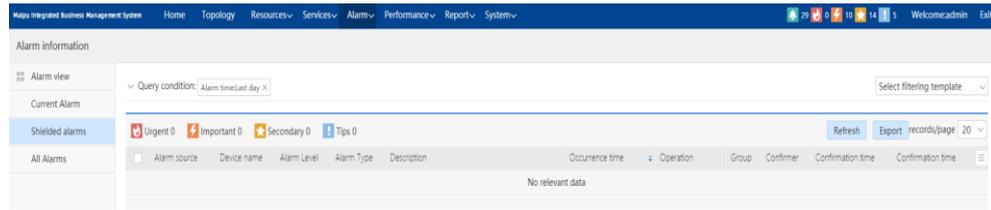


Figure 6-10 Exported the shielded alarm information

Similarly, the function of saving filter conditions is also supported on the shielded alarm interface, and there is no need to repeat here.

### All alarms

All alarm modules present the current alarm, shielded alarm, processed alarm, and auto recovery, auto processing, and de-duplication alarm to the user. Users can accurately query through alarm level, processing status, confirmation status and alarm time on all alarm interfaces, and can also make fuzzy query for alarm source, alarm type, organization and description, and also support accurate query through alarm type and alarm source.

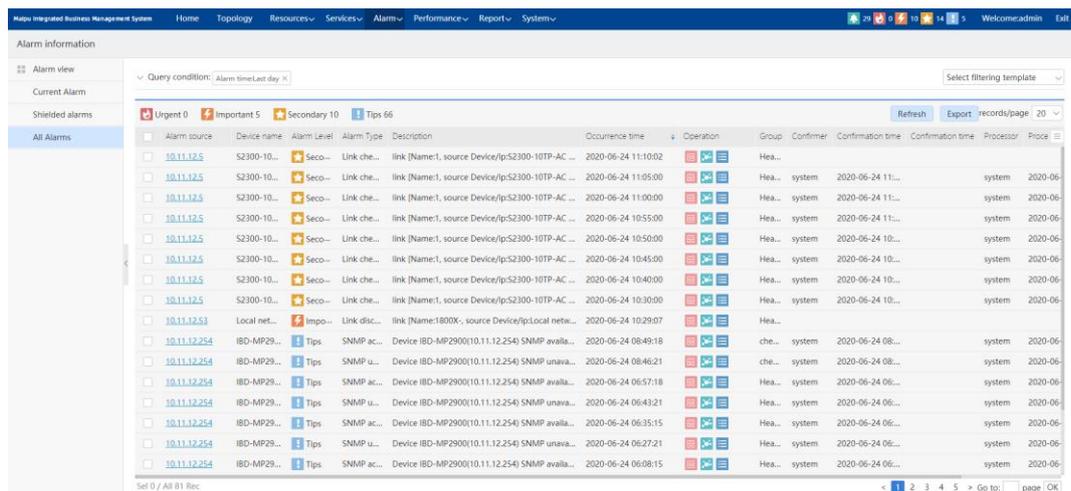


Figure 6-11 All alarms

After users query the desired alarm information, click  to export all the alarm events in the list (including paging alarm events).

Warning	Device name	Alarm level	Alarm Type	Description	Occurrence time	Organization	Confirmer	Confirmation time	Confirmer	Dealer	Processing	Processing result
10.11.12.5	S2300-10	Secondary	Link check link	link (Name:1, source Device/ps2300-10TP-AC...	6/24/2020 11:10	/Headquarters/						
10.11.12.5	S2300-10	Secondary	Link check link	link (Name:1, source Device/ps2300-10TP-AC...	6/24/2020 11:05	/Headqua system		6/24/2020 11:10		system	#####	Repeat elimination of the day
10.11.12.5	S2300-10	Secondary	Link check link	link (Name:1, source Device/ps2300-10TP-AC...	6/24/2020 11:00	/Headqua system		6/24/2020 11:05		system	#####	Repeat elimination of the day
10.11.12.5	S2300-10	Secondary	Link check link	link (Name:1, source Device/ps2300-10TP-AC...	6/24/2020 10:55	/Headqua system		6/24/2020 11:00		system	#####	Repeat elimination of the day
10.11.12.5	S2300-10	Secondary	Link check link	link (Name:1, source Device/ps2300-10TP-AC...	6/24/2020 10:50	/Headqua system		6/24/2020 10:55		system	#####	Repeat elimination of the day
10.11.12.5	S2300-10	Secondary	Link check link	link (Name:1, source Device/ps2300-10TP-AC...	6/24/2020 10:45	/Headqua system		6/24/2020 10:50		system	#####	Repeat elimination of the day
10.11.12.5	S2300-10	Secondary	Link check link	link (Name:1, source Device/ps2300-10TP-AC...	6/24/2020 10:40	/Headqua system		6/24/2020 10:45		system	#####	Repeat elimination of the day
10.11.12.5	S2300-10	Secondary	Link check link	link (Name:1, source Device/ps2300-10TP-AC...	6/24/2020 10:30	/Headqua system		6/24/2020 10:40		system	#####	Repeat elimination of the day
10.11.12.5	Local netv	Important	Link disco	link (Name:1800X- source Device/ps.Local netw...	6/24/2020 10:29	/Headquarters/						
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 8:49	/Headqua system		6/24/2020 8:49		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 8:46	/Headqua system		6/24/2020 8:49		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 6:57	/Headqua system		6/24/2020 6:57		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 6:43	/Headqua system		6/24/2020 6:57		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 6:35	/Headqua system		6/24/2020 6:35		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 6:27	/Headqua system		6/24/2020 6:35		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 6:08	/Headqua system		6/24/2020 6:08		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 6:05	/Headqua system		6/24/2020 6:08		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 5:17	/Headqua system		6/24/2020 5:17		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 5:16	/Headqua system		6/24/2020 5:17		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 5:15	/Headqua system		6/24/2020 5:15		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 5:14	/Headqua system		6/24/2020 5:15		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 5:05	/Headqua system		6/24/2020 5:05		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 5:04	/Headqua system		6/24/2020 5:05		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 5:03	/Headqua system		6/24/2020 5:03		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 4:58	/Headqua system		6/24/2020 5:03		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP acc	Device IBD-MP2900(10.11.12.254) SNMP availa...	6/24/2020 4:19	/Headqua system		6/24/2020 4:19		system	#####	Auto alarm recovery
10.11.12.2	IBD-MP25	Tips	SNMP un	Device IBD-MP2900(10.11.12.254) SNMP unava...	6/24/2020 4:14	/Headqua system		6/24/2020 4:19		system	#####	Auto alarm recovery

Figure 6-12 Export all alarm information

The function of saving filter conditions is also supported on all alarm interfaces, and there is no need to repeat here.

The current alarms, shielded alarms and all alarms support clicking the alarm source IP to view all the alarm information generated by the alarm source; click the alarm level statistics icon, and you can view all the alarm information of the same alarm level, and the effect is shown in Figure 6-13 and Fig. 6-14.

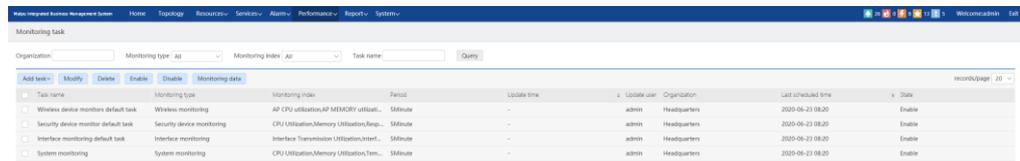


Figure 6-13 Query by alarm source

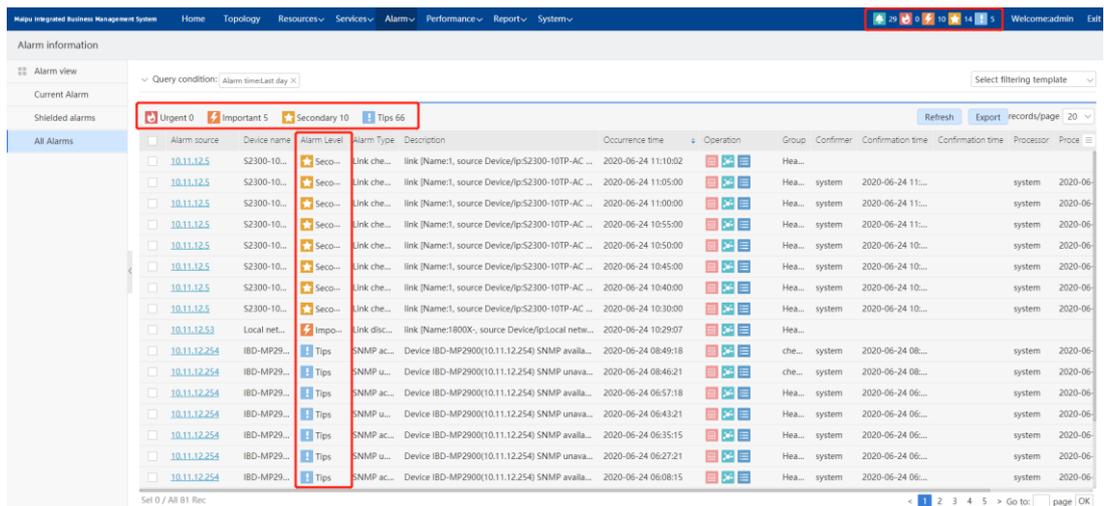


Figure 6-14 Query by the alarm level

The current alarms, shielded alarms, and all alarms support jumping to the topology and locating to the topology. The effect is shown in Figure 6-15.

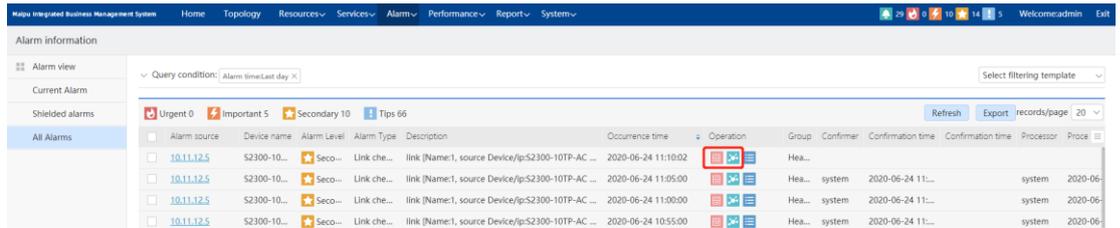


Figure 6-15 Locate to the device and topology

The current alarms, shielded alarms, and all alarms support viewing the alarm details, and the effect is shown in Figure 6-16.

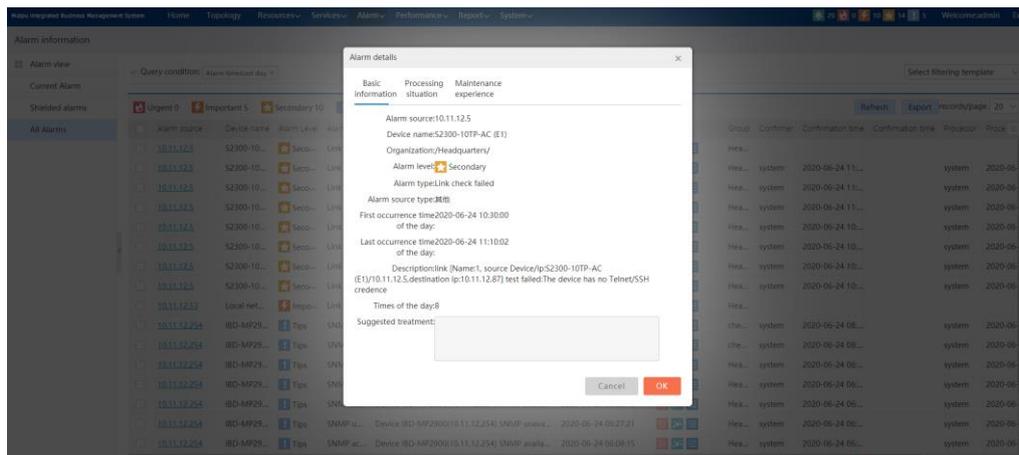


Figure 6-16 Alarm details

The current alarms, shielded alarms and all alarms supports adding alarm maintenance experience for the alarm, and the effect is shown in Figure 6-17.

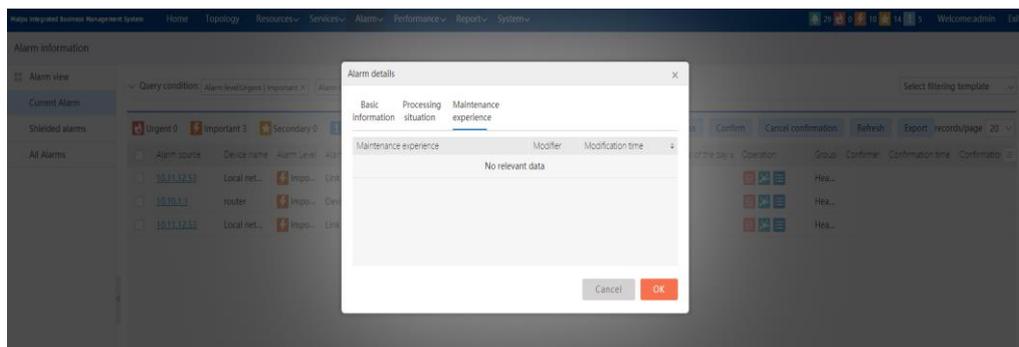


Figure 6-17 Add alarm maintenance experience

**Note**

- In the current alarms, shielded alarms and all alarms, do not support the function of locating the alarm information with the device name as the local network management system to the device and the topology.
- After adding the interface to the device, the alarm generated when the device does not refresh to this interface can only be queried through the interface information and alarm description information, but cannot be queried by the interface accurately.

## 6.2. Alarm Configuration

Click "Alarm" -> "Alarm configuration" in the menu bar to open the "Alarm configuration" page. The left navigation of alarm configuration interface includes alarm notification rules, notification content template, alarm voice configuration, alarm shielding rules, alarm auto processing rules, alarm level redefinition, alarm basic configuration, alarm dump, alarm type management and maintenance experience management. The effect is shown in Figure 6-18.

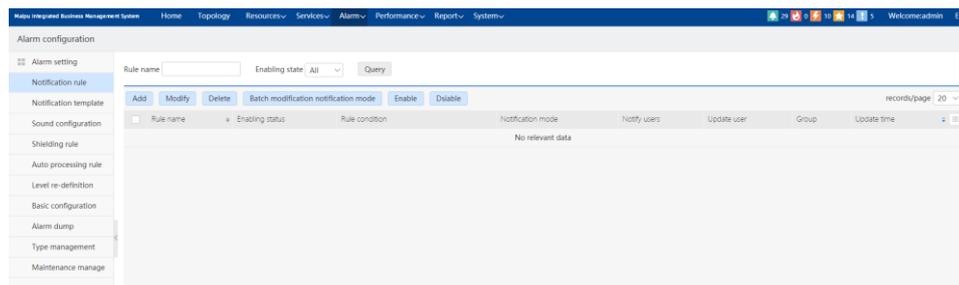


Figure 6-18 Alarm configuration

### 6.2.1. Alarm Notification Rule

Alarm notification rules are used to configure the alarm information to be notified to users by Email, SMS, wechat or voice. The alarm information of which alarm source or type of alarm information can be configured, and what kind of notification method is used to notify the user. On the alarm notification configuration interface, users can query the notification rules through the name of the rule, or query the notification rules accurately for the enabled status. The effect is shown in Figure 6-19.

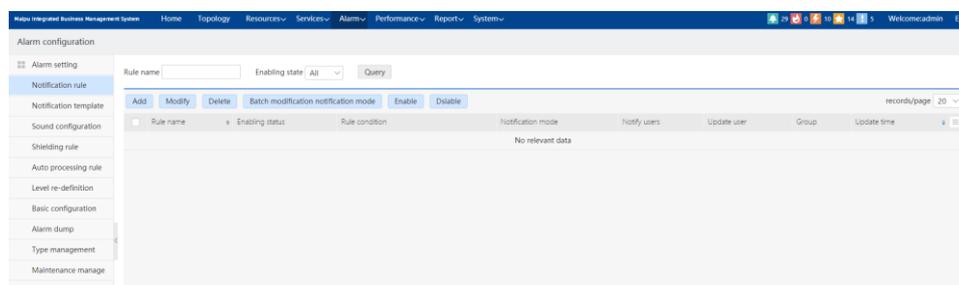


Figure 6-19 Alarm notification rule

The user can click the "Add" button to add an alarm notification rule. The effect is shown in Figure 6-20.

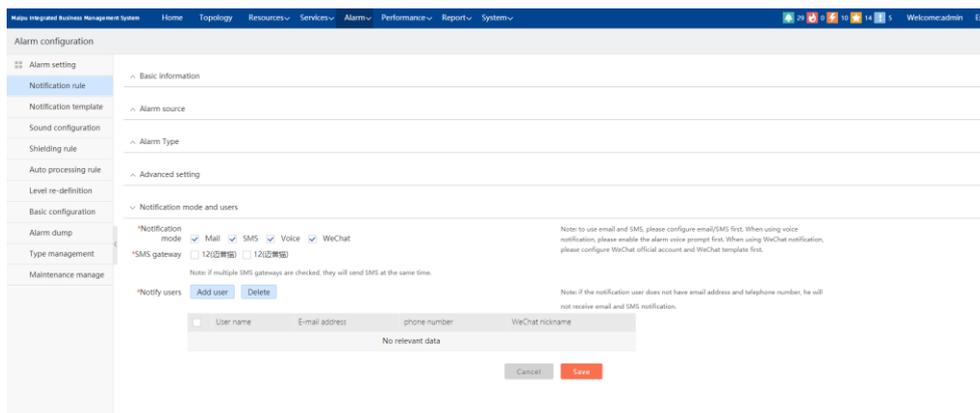


Figure 6-20 Add the alarm notification rule

### Basic information:

The basic information is used to configure the name of the alarm notification rule (required), the enabling status of the rule, and the organization to which the rule belongs (the lower-level configured alarm notification rules can only be seen by the administrators at the same level and higher level). The effect is shown in Figure 6-21.

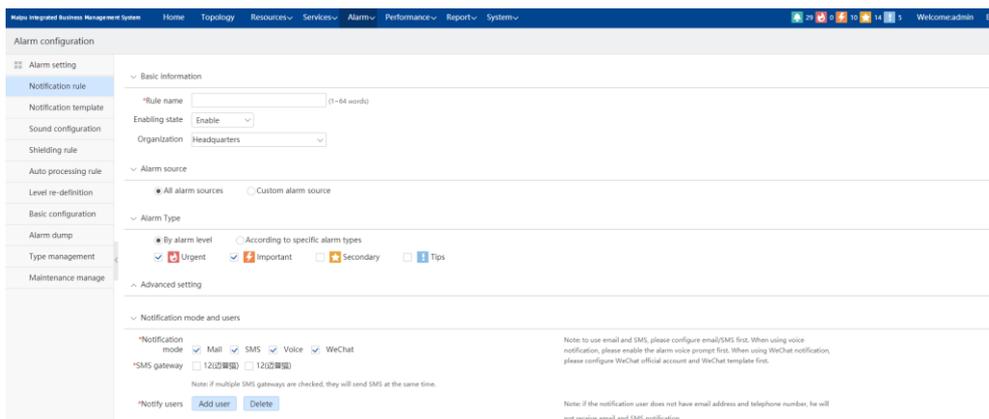


Figure 6-21 Basic information configuration of the notification rule

### Alarm source:

The alarm source is used to determine which alarm information needs to be notified. In addition, the alarm source can only select the device, device group, interface and interface group of the current level and lower level organizations of the organization to which the rule belongs. When all alarm sources are selected, only the alarms generated by the alarm sources of the same level and lower level organizations will send alarm notification. Alarm source rules include all alarm sources and custom alarm sources. When the user selects a customized alarm source, a list will appear. The user can click the “Add alarm source” button to select the specific alarm source. The effect is shown in Figure 6-22.

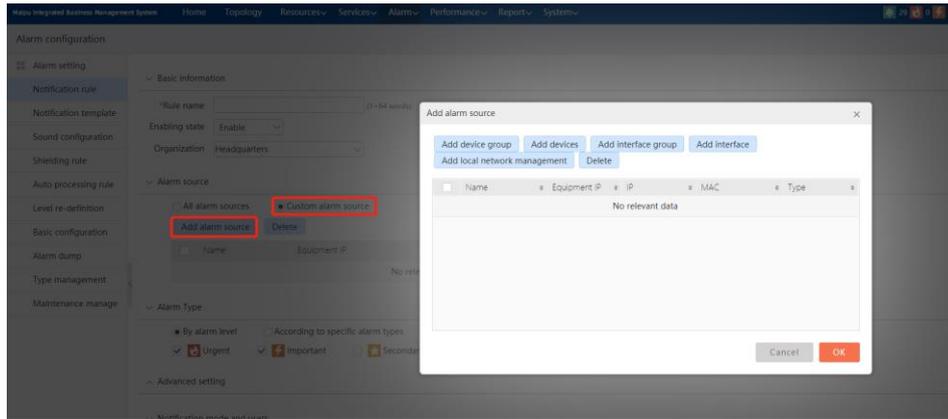


Figure 6-22 Alarm resource configuration

Alarm type:

The alarm type is used to determine which type of alarm information needs to be notified. The alarm type rules include by alarm level and by specific alarm type. If the user selects the alarm level, there will be four alarm levels for the user to select. If the user selects a specific alarm type, a list will appear. The user can click “Add alarm type” to select the specific alarm type. The effect is shown in Figure 6-23.

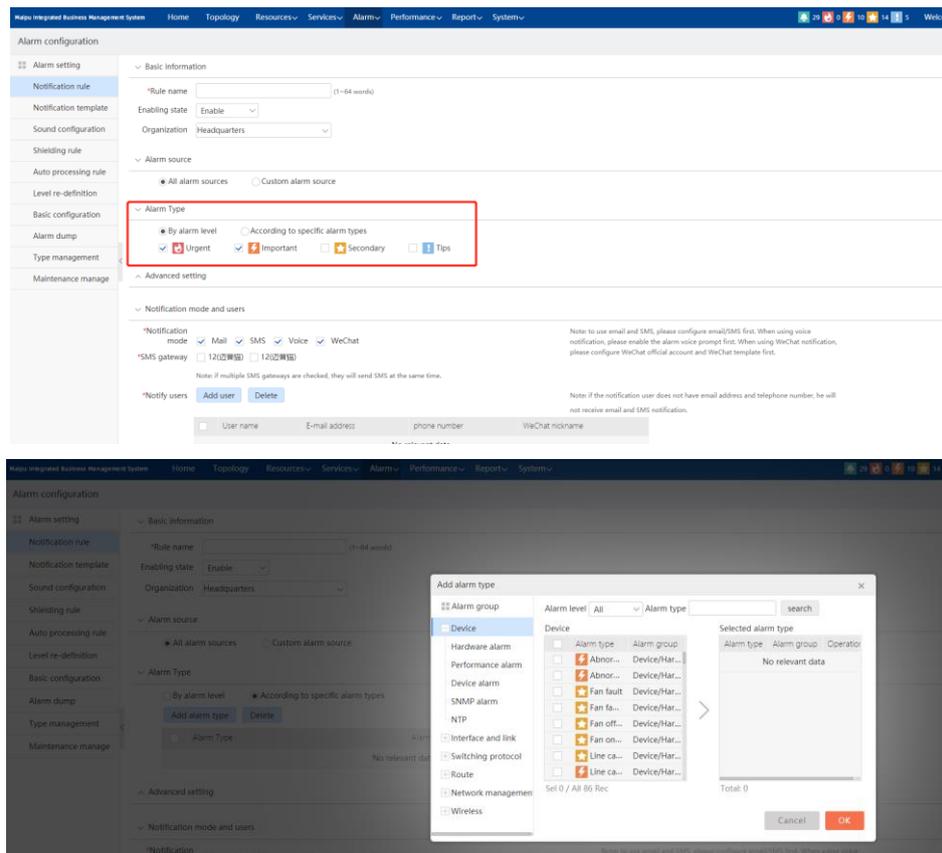


Figure 6-23 Alarm type configuration

Advanced configuration:

The advanced configuration includes two configurations, namely, within the same day,

only the first alarm notification and rule effective date are sent for the same alarm. The effective date includes permanent and period-based. If the user chooses period-based, a time list will appear. The user can select the time in the time list (the ordinate represents the date, and the abscissa represents the time scale). The effect is shown in Figure 6-24.

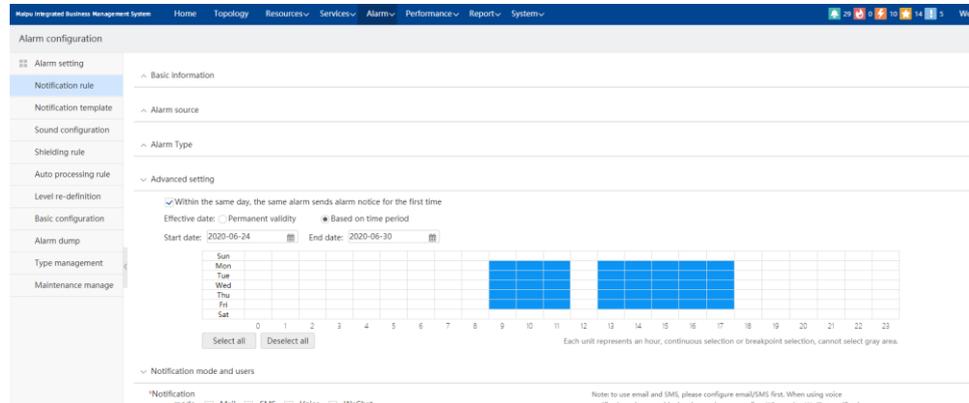


Figure 6-24 Advanced configuration

Notification mode and user:

Notification methods include Email, SMS, wechat and voice. If SMS is selected, a SMS gateway must be selected (the configuration of SMS network management is in "System" > "System Settings" > "SMS Gateway configuration"). If you choose WeChat, you need to configure the WeChat official account first, and bind the system administrator with the WeChat user (For the configuration of wechat, refer to "System" -> "System Settings" -> "WeChat configuration"), then configure the WeChat notification template in the notification content template (for the template configuration, refer to "Alarm" > "Alarm configuration" > "Notification content template"). The gateway user can click the "Add user" button to select the user to be notified (the user can only select the user of the current level and lower level organization of the organization to which the rule belongs, and the user must have the authority of the alarm source to send the alarm notice). The effect is shown in Figure 6-25.

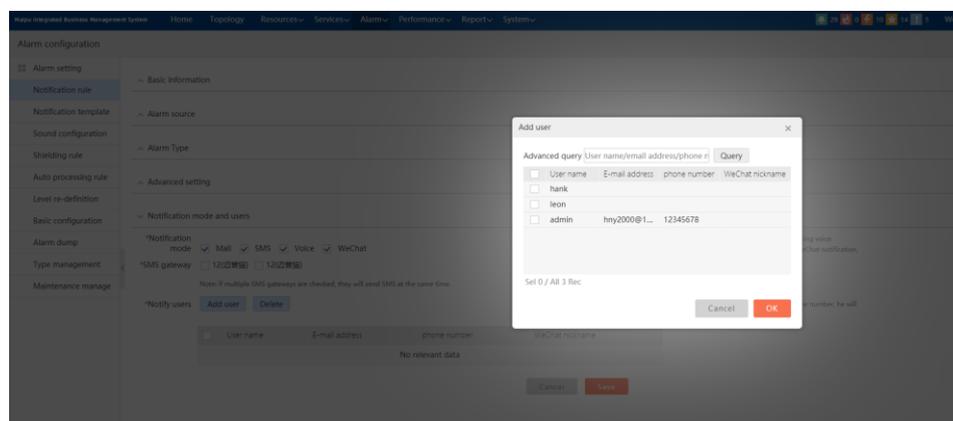


Figure 6-25 Notification mode and user configuration

Users can modify the alarm notification rules. Select an alarm notification rule and click

the “Modify” button. For the basic information, you can only modify the enabling status, but the alarm source, alarm type, advanced settings, notification mode and user all can be modified. After modification, click the “Save” button, and the effect is shown in Figure 6-26.

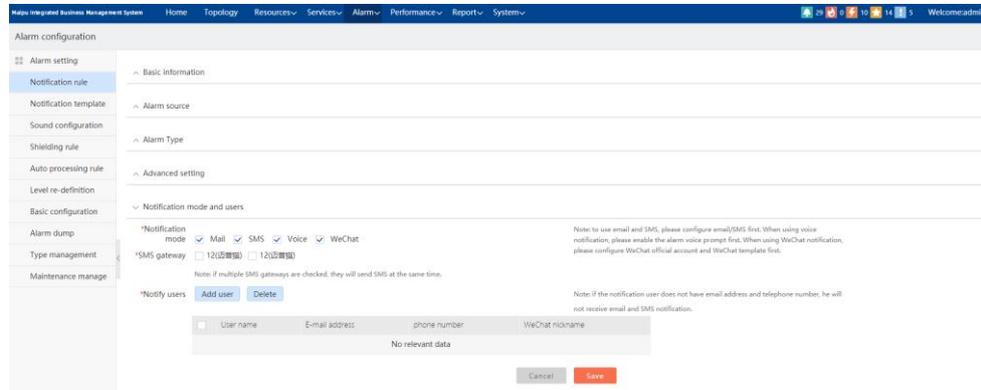


Figure 6-26 Modify alarm notification rule

Users can delete the alarm notification rules. Select an alarm notification rule, and then click the “Delete” button. A prompt box will appear, and then click “OK” in the prompt box. The effect is shown in Figure-6-27.

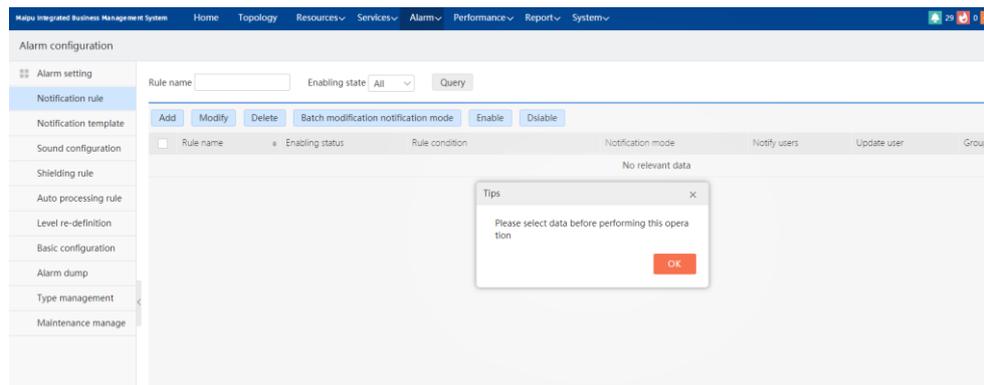


Figure 6-27 Delete alarm notification rule

Users can modify the notification mode in batch for the alarm notification rules. The user can select one or more alarm notification rules, and then click “Batch modify notification mode” to open the notification mode dialog box. The user can select the appropriate notification method in the dialog box, and then click . The effect is shown in Figure 6-28.

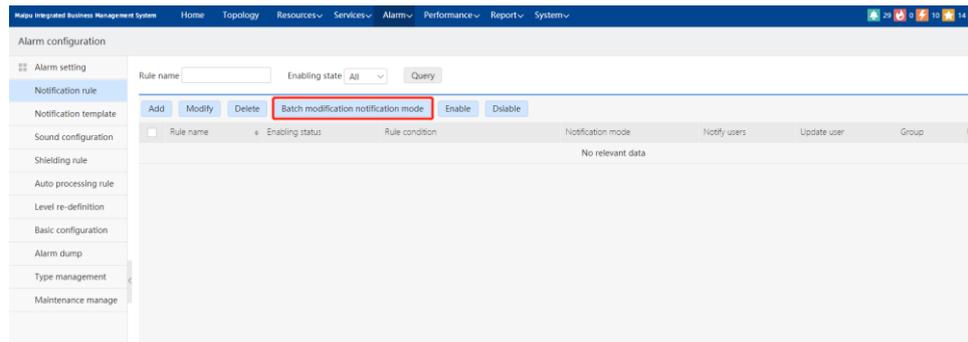


Figure 6-28 Batch modify notification mode

Users can enable the alarm notification rules (support batch operation). The user selects one or more alarm notification rules on the interface (it can only be in the disabled state), and then click “Enable” to pop up a dialog box, and then click  on the dialog box. The effect is shown in Figure 6-29.

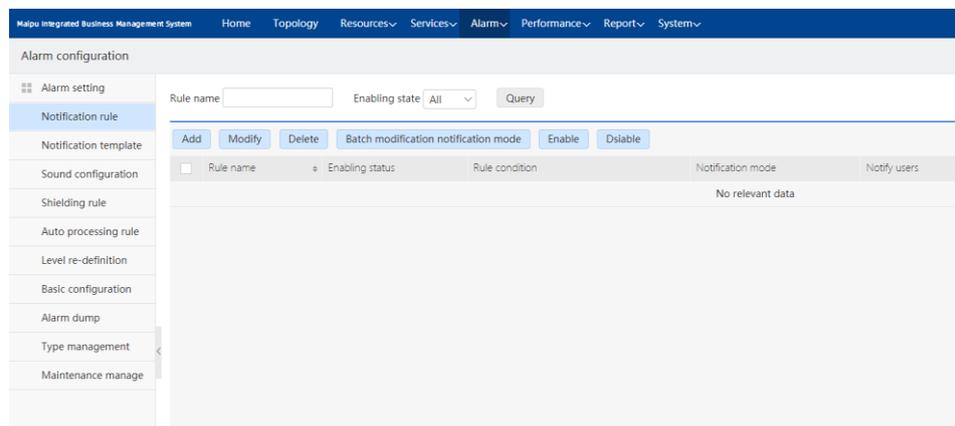


Figure 6-29 Enable alarm notification rule

Users can disable the alarm notification rules (batch operation is supported). The user selects one or more alarm notification rules on the interface (only in the enabled state), and then, click “Disable” to pop up a dialog box, and then click  on the dialog box. The effect is shown in Figure 6-30.

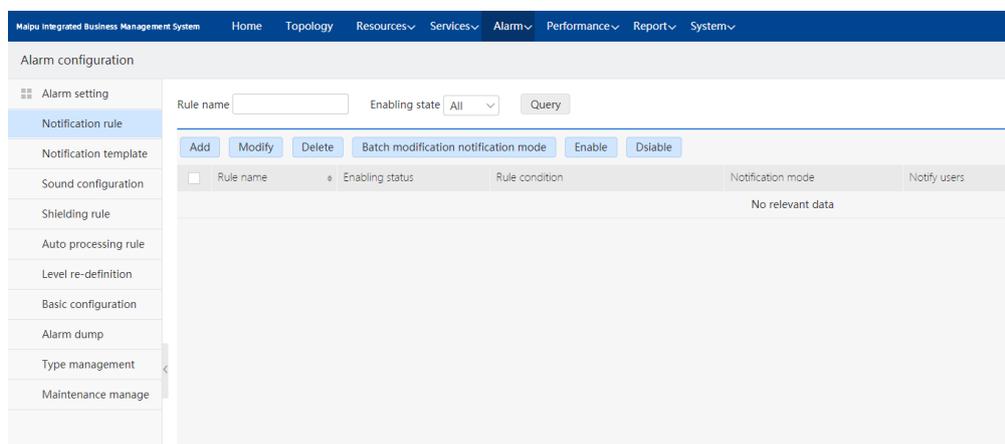


Figure 6-30 Disable the alarm notification rule

## Note

- During an alarm push cycle (3 seconds), only one round of the highest-level sound will be played.
- The information and status (success or failure) of the notification can be viewed in the alarm notification record.
- The correct mail server should be configured for mail sending.
- The sound notification can only take effect when it is enabled in the alarm sound configuration.
- Network management recommendation cannot use WeChat official account grading configuration. For example, if Sichuan users are bound with the official account of WeChat in Sichuan, users in Sichuan do not have the right to configure WeChat content template. The notification will fail when selecting WeChat for notification mode. Subordinate administrators recommend inheriting the wechat configuration of the headquarters.

## 6.2.2. Notification Content Template

The notification content template is a template that assembles alarm information into notification content and sends it to users. The notification content template supports customizing the e-mail, SMS and WeChat content templates. The left side of the tab is email, the middle is SMS, and the right side is WeChat. The effect is shown in Figure 6-31.

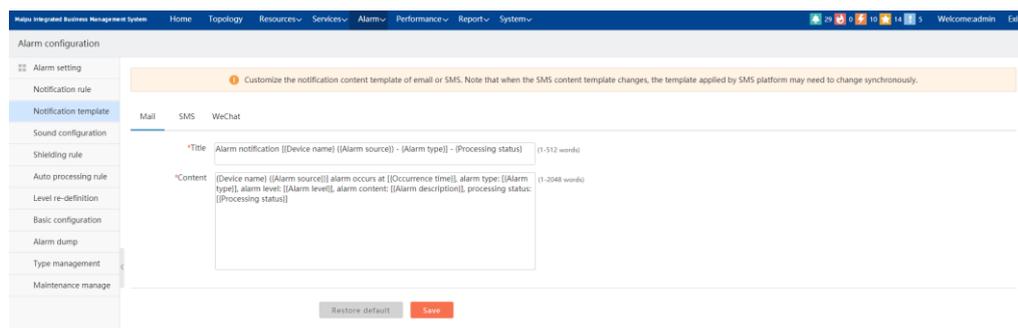


Figure 6-31 Notification content template

Email:

Users can make a template for the mail. When the user clicks the edit box, a dialog box will appear. The user can select the required options or remove the unnecessary options. At the same time, it also supports users to fill in the title manually, just fill in the title edit box. The content of the email is the same as the email title. You can also select the content and also support inputting manually. After selection, click **Save**, and the effect is shown in Figure 6-32.

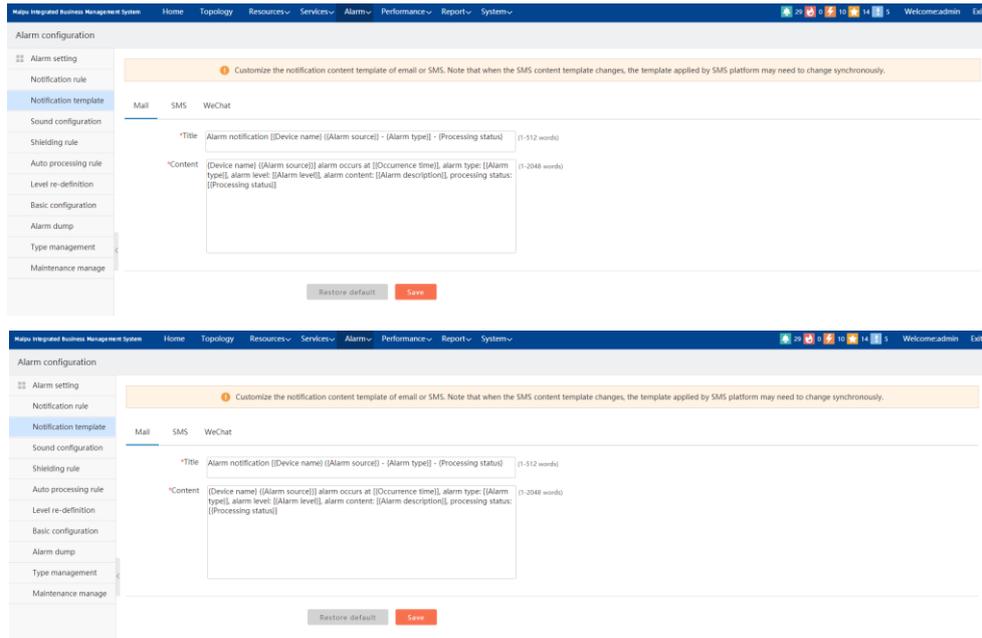


Figure 6-32 Email template

SMS:

Users can make templates for SMS. When the user clicks the edit box, a dialog box will appear. The user can select the required options or remove the unnecessary options. At the same time, it also supports the user to fill in the SMS content manually, just fill in the content edit box, and click **Save** after selection. The effect is shown in Figure 6-33.

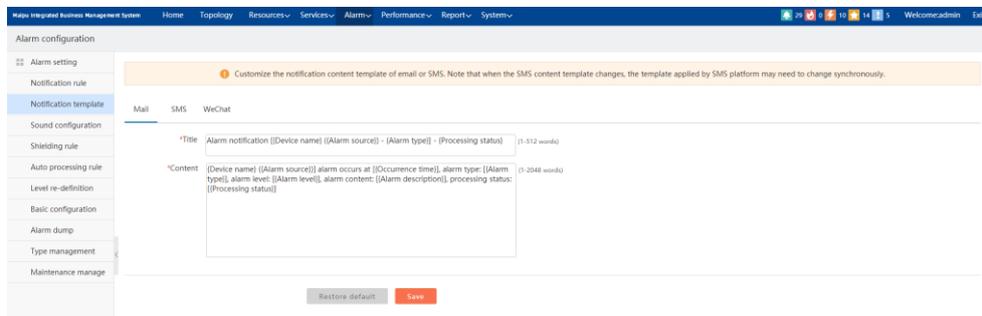


Figure 6-33 SMS template

Users can also restore the default configuration of email and SMS content templates by clicking **Restore default**.

Wechat:

To configure WeChat template, first configure WeChat official account (for WeChat's related configuration, refer to "System" -> "System Settings" -> "WeChat configuration"), and add WeChat template to the official account background. On the management page of wechat public platform, click "Function" -> "Template message" -> "Template library", and input the alarm in the search box to search the related message template of the current industry alarm.

The alarm sound configuration is used to play the prompt sound when the alarm information is notified to the user. Different alarm levels provide two different prompt sounds, and the effect is shown in Figure 6-34.

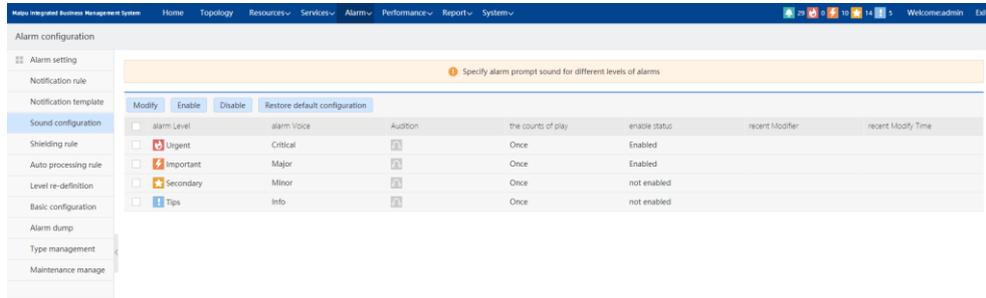


Figure 6-34 Alarm sound configuration

Users can modify the sound configuration. Select an alarm level on the interface, and then click **Modify**. An alarm sound modification dialog box will appear. The dialog box has alarm sound selection and alarm times drop-down box. There are two kinds of alarm sounds for users to choose. Users can also click to listen to the sound. For the play times, there are once, three times, and loop for the user to select. After selection, click **OK**, and the effect is shown in Figure-35.

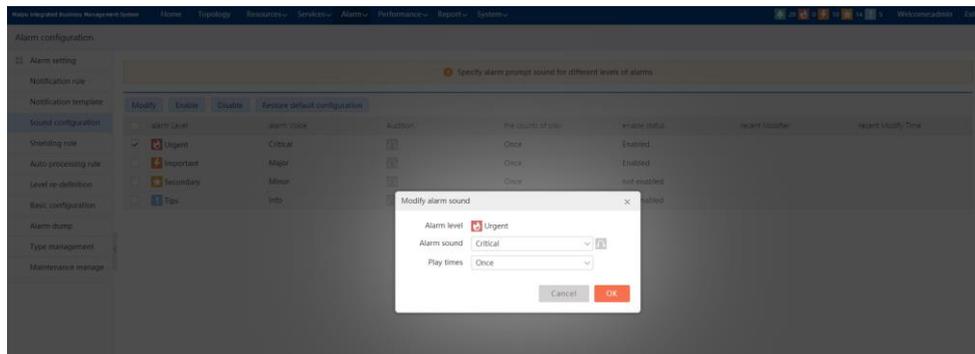


Figure 6-35 Modify the alarm sound configuration

Users can batch enable the alarm sound. Select one or more alarm levels on the interface (only if it is not enabled), and then click “Enable”, a prompt dialog box will appear. Click **OK**, and the effect is shown in Figure 6-36.

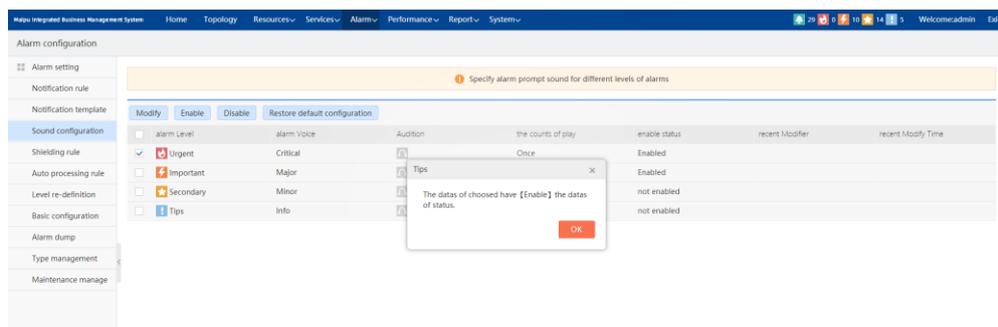


Figure 6-36 Enable the alarm sound configuration

Users can stop the alarm sound in batches. Select one or more alarm levels on the

interface (only in the enabled state), and then click “Disable” to display a prompt dialog box. Click , and the effect is shown in Figure 6-37.

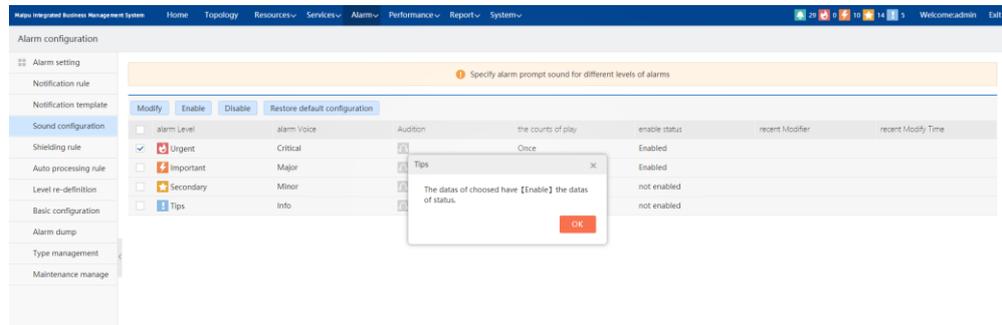


Figure 6-37 Disable the alarm sound configuration

Users can batch restore the default configuration for the alarm sound. Click “Restore default configuration” on the interface, and a prompt dialog box will appear. Click “OK”, and the effect is shown in Figure 6-38.

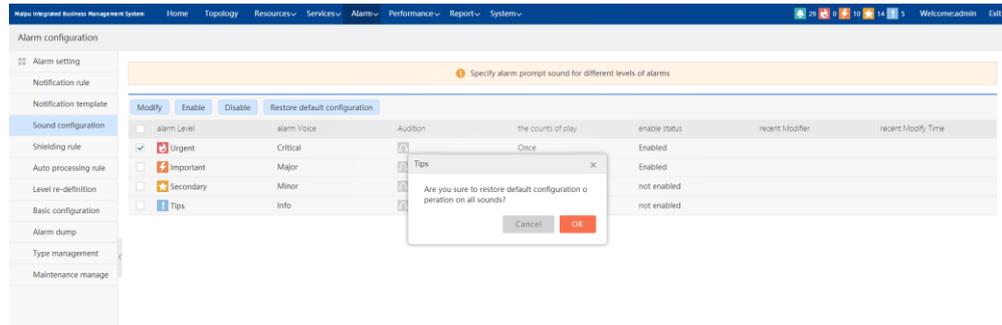


Figure 6-38 Restore default configuration

### 6.2.3. Alarm Shielding Rule

Alarm shielding rules are used to configure how alarm information is processed, including shielding, rejecting and receiving. The alarm information of which type of alarm source or type of alarm can be configured, and at which time period the alarm information is processed. In the alarm shielding rule interface, users can query the shielding rules through the name of the rule, and can also query the shielding rules accurately for the enabled status and shielding mode. The effect is shown in Figure 6-39.

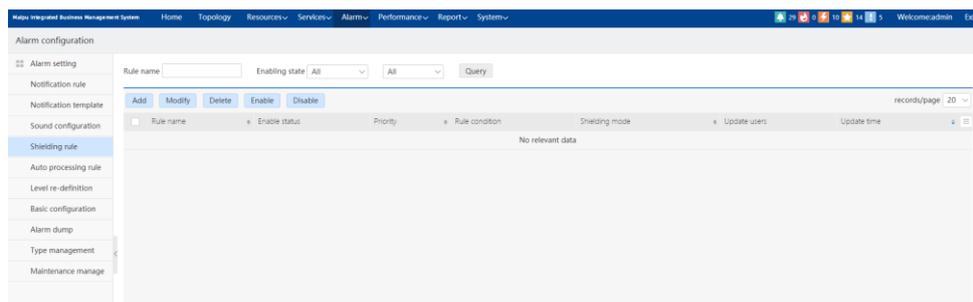


Figure 6-39 Alarm shielding rule

The user can click **Add** to add one alarm shielding rule, and the effect is as shown in Figure 6-40.

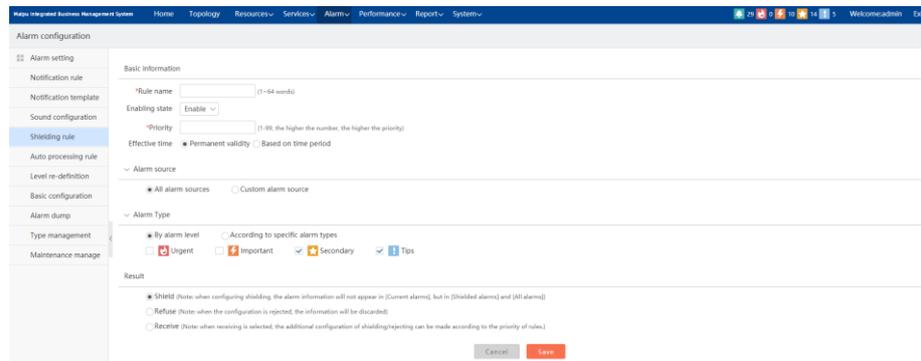


Figure 6-40 Add an alarm shielding rule

**Basic information:**

The basic information is used to configure the name (required item) of the alarm shielding rule, the enabling status of the rule, the priority of the rule (required item, the greater the value, the higher the priority) and the effective time of the rule. The effect is shown in Figure 6-41.

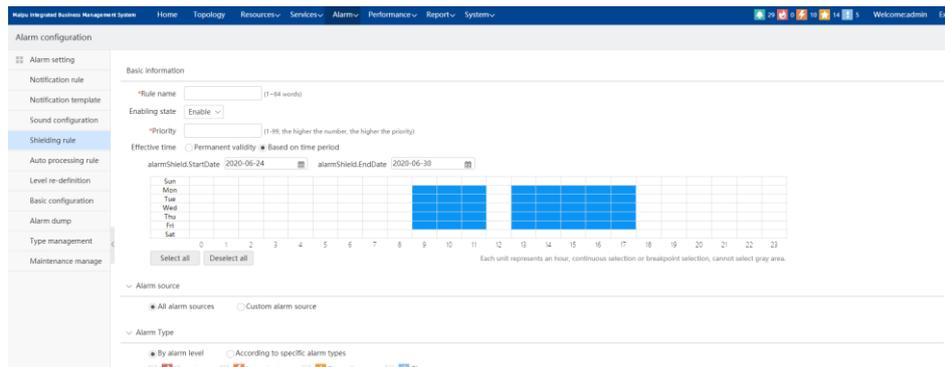


Figure 6-41 Configure the basic information of the notification rule

**Alarm source:**

The alarm source is used to determine which alarm information needs to be processed. Alarm source rules include all alarm sources and custom alarm sources. When the user selects the custom alarm source, a list will appear. The user can click “Add alarm source” to select the specific alarm source. The effect is shown in Figure 6-42.

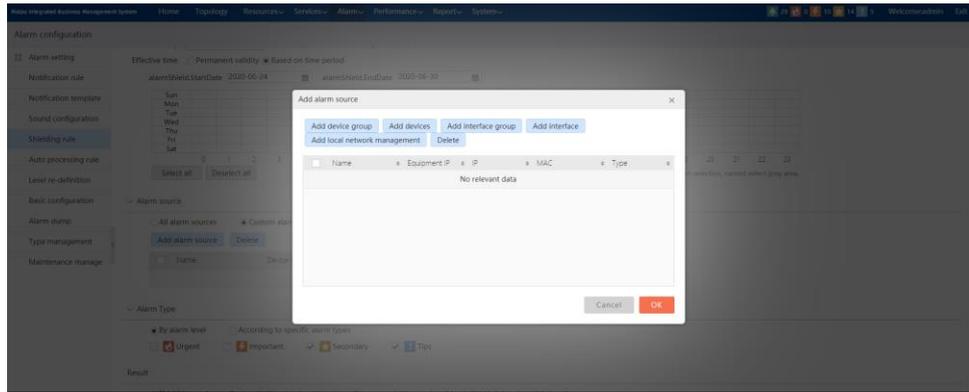


Figure 6-42 Alarm source configuration

Alarm type:

The alarm type is used to determine which type of alarm information needs to be processed. The alarm type rules include by alarm level and by specific alarm type. If the user selects the alarm level, there will be four alarm levels (urgent, important, secondary, tips) for the user to select, as shown in Figure 6-43;

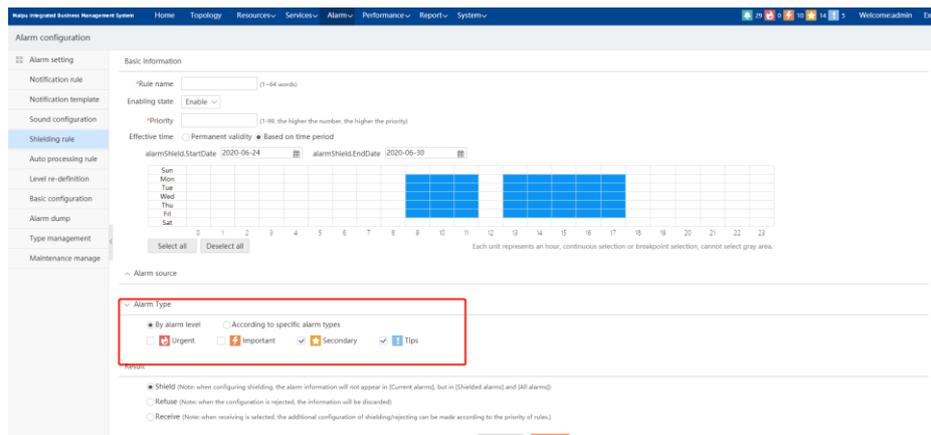


Figure 6-43 Alarm type configuration 1

If the user selects by specific alarm type, a list will appear. The user can click “Add alarm type” to select the specific alarm type. The effect is shown in Figure 6-44.

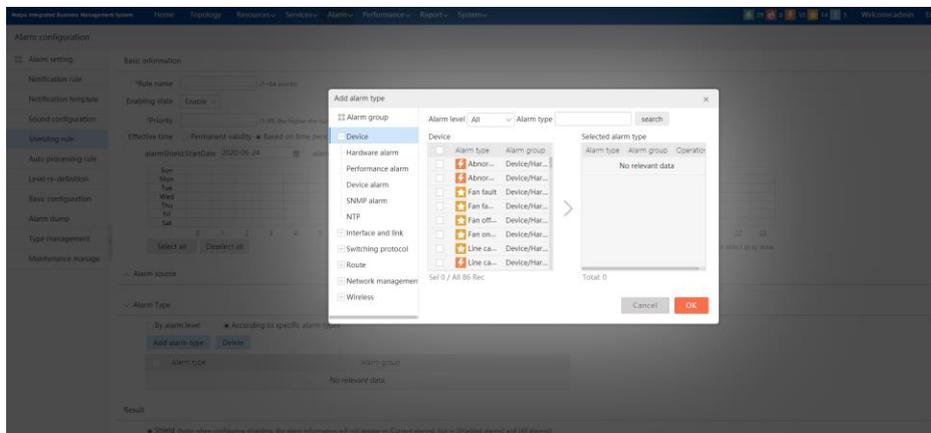


Figure 6-44 Alarm type configuration 2

Result configuration:

The advanced configuration includes three configurations: shield, refuse and receive. Among them, the shielding processing is to shield the alarm information, and the user can view it in the shielded alarms and all alarm information; the reject processing is to discard the alarm information directly; the receive processing is to store the alarm information. When selecting receive, the exception configuration of shield/reject can be made with the rule priority. The effect is shown in Figure 6-45.

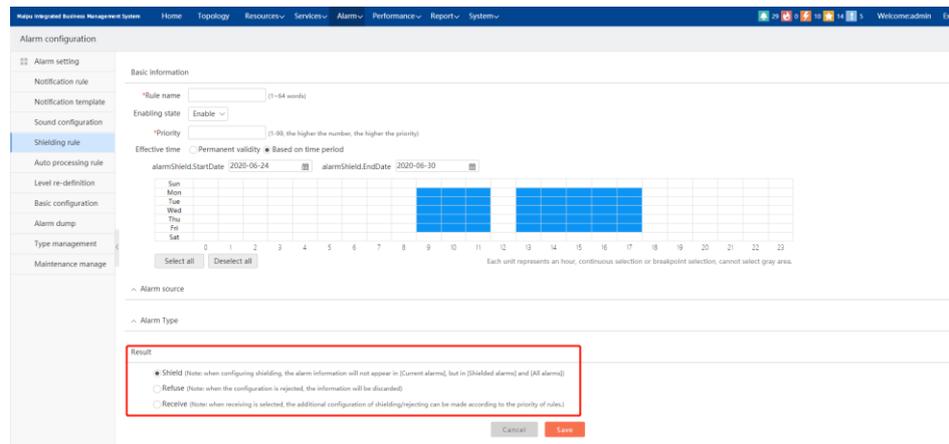


Figure 6-45 Result configuration

Users can modify the alarm shielding rules. Select an alarm shielding rule, and then click “Modify”. For the basic information, the user can only modify the enabling status and priority, while the alarm source, alarm type and result setting all can be modified. After modification, click “Save”, and the effect is shown in Figure 6-46.

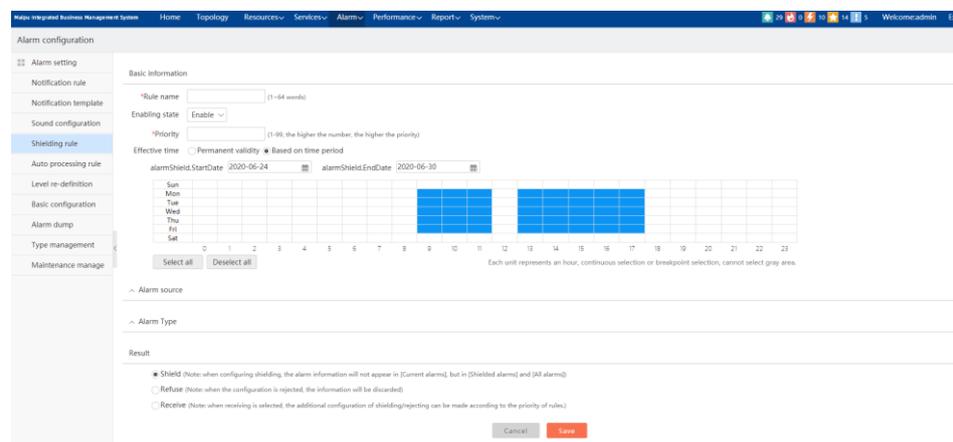


Figure 6-46 Modify the alarm shielding rule

Users can delete the alarm shielding rules. Select an alarm shielding rule, and then click **Delete**, a prompt box will appear, and then click “OK” in the prompt box. The effect is shown in Figure 6-47.

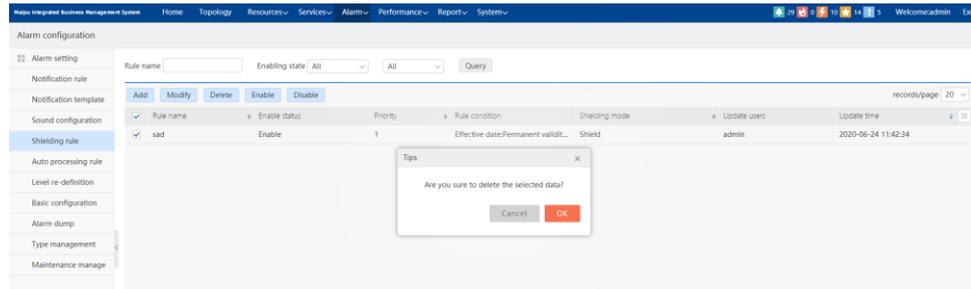


Figure 6-47 Delete the alarm shielding rule

Users can enable the alarm shielding rules (support batch operation). The user can select one or more alarm shielding rules on the interface (only if it is not enabled), and then click “Enable” to pop up a dialog box, and then click “OK” on the dialog box. The effect is shown in Figure 6-48.

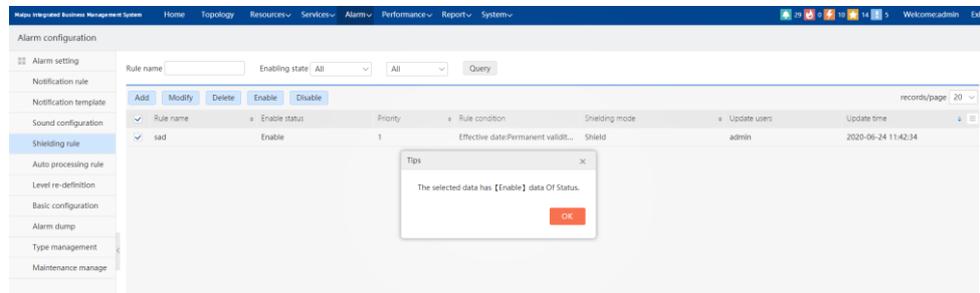


Figure 6-48 Enable the alarm shielding rule

Users can disable the alarm shielding rules (support batch operation). The user can select one or more alarm shielding rules (it can only be enabled) on the interface, and then click “Disable” to pop up a dialog box, and then click “OK” on the dialog box. The effect is shown in Figure 6-49.

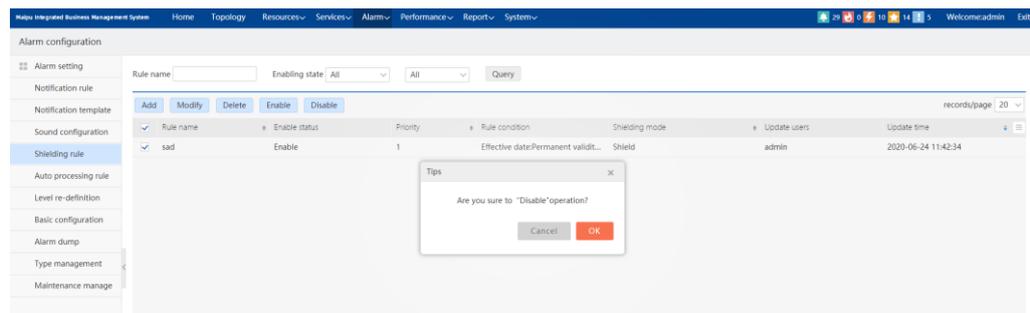


Figure 6-49 Disable the alarm shielding rule

## Note

- The alarm can only match one shielding rule at a time. The one with higher priority is prior. When the priorities are the same, the rule with the latest time is prior. When both priority and time are the same, the matching rule matches by the rule ID.

## 6.2.4. Alarm Auto Processing Rule

Auto alarm processing rules are used to configure that the alarm information (not processed alarm information) will be automatically processed by the system within a certain period. Different auto processing periods can be configured for different alarm levels, and the effect is shown in Figure 6-50.

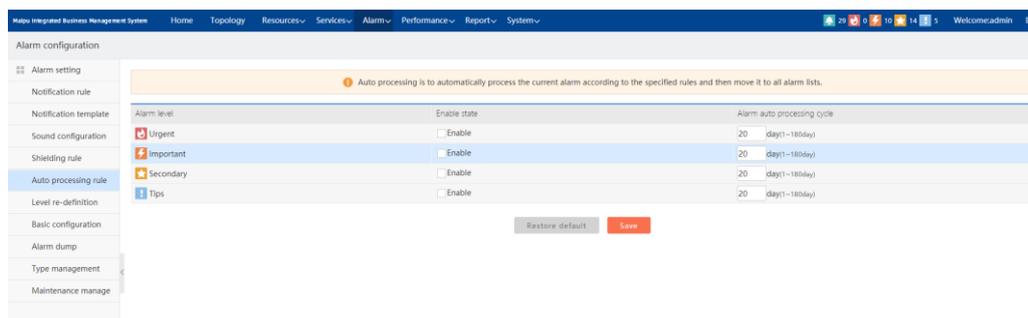


Figure 6-50 Alarm auto processing rule

Users can configure the enabling state (enabled or not enabled) and alarm auto processing period for different alarm types on the alarm auto processing rule interface. The user can also restore the default operation for the alarm auto processing rules, and the effect is shown in Figure 6-51.

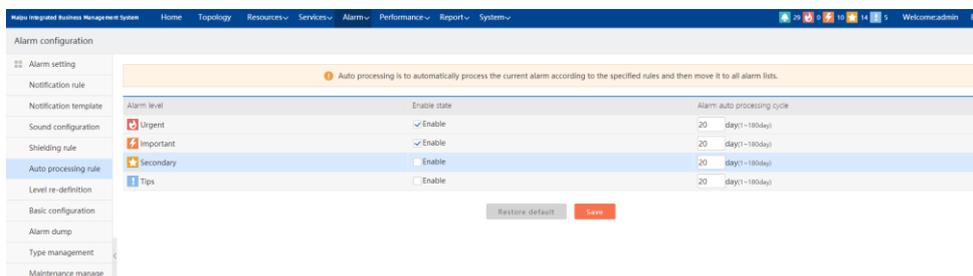


Figure 6-51 Configure alarm auto processing rule

### Note

- Auto alarm processing is carried out at 2 am every day.

## 6.2.5. Alarm Level Redefinition

The alarm level redefinition is used to configure how to redefine the level of the alarm information. The processing methods include level redefinition and level auto upgrade. The alarm information of which alarm source can be configured or the level of alarm information of which type is redefined. In the alarm level redefinition interface, users can perform fuzzy query rules through the rule name, and can also accurately query rules for the enabling status and rule type. The effect is shown in Figure 6-52.

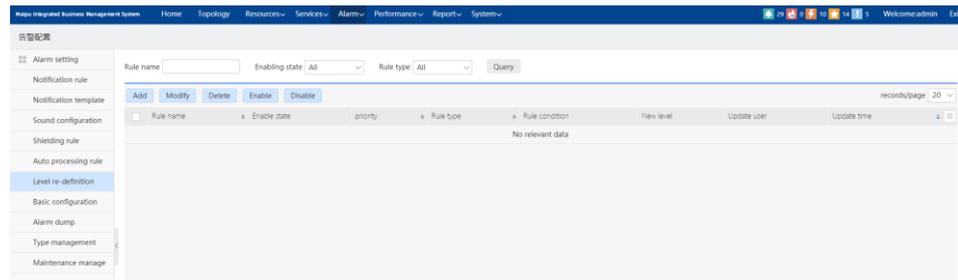


Figure 6-52 Alarm level redefinition

The user can click “Add” to add an alarm level redefinition, as shown in Figure 6-53.

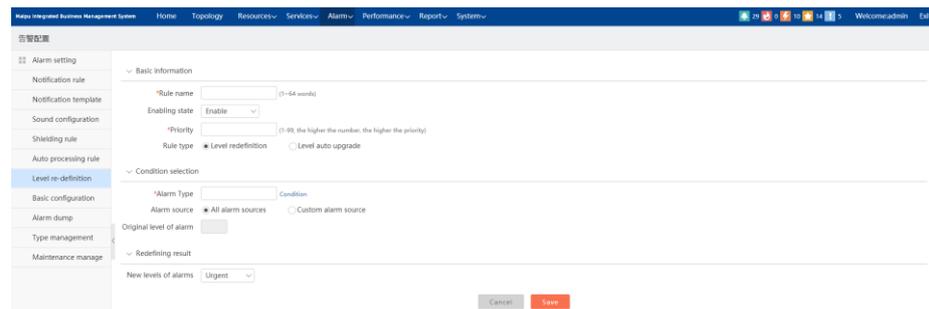


Figure 6-53 Add the redefinition rule of the alarm level

Basic information:

The basic information is used to configure the redefinition rule name of the alarm level (required), enabling status of the rule, rule priority (required item, the bigger the value, the higher the priority) and the rule type. The effect is shown in Figure 6-54.

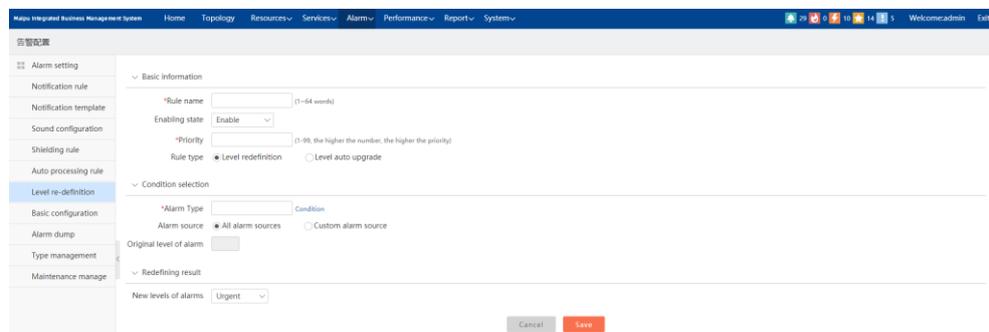


Figure 6-54 Basic information configuration of level redefinition

If the user selects the level redefinition, it is necessary to configure the redefinition result. If the level is upgraded automatically, it is necessary to configure the policy settings. The effect is shown in Figure 6-55.

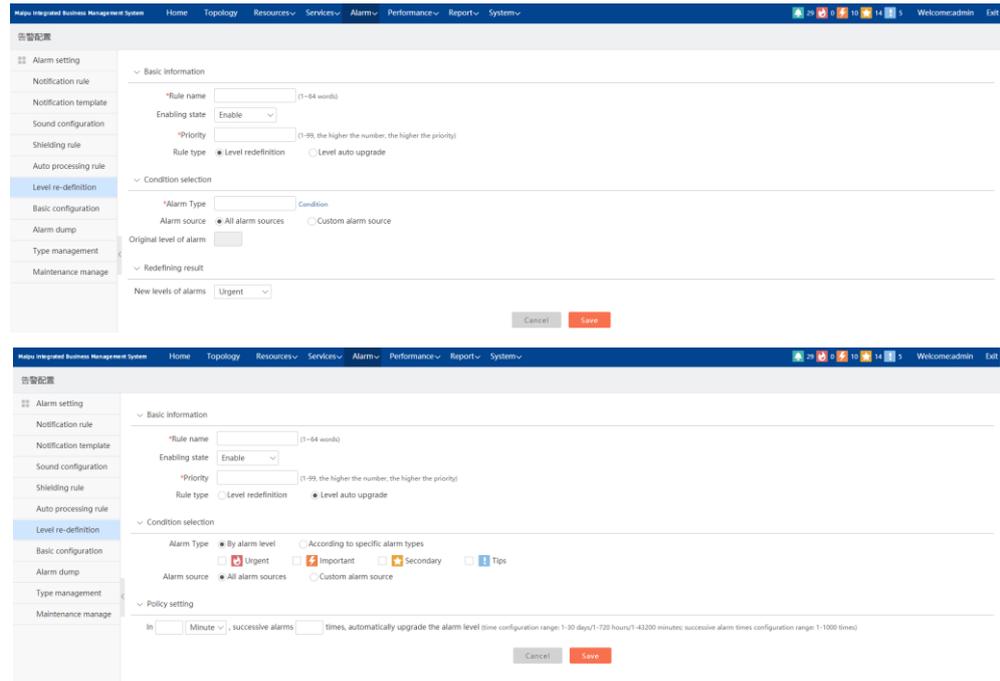


Figure 6-55 Rule type configuration

Condition selection:

The alarm type is used to determine which type of alarm information needs to be redefined. When the user clicks the alarm type, a list will appear. The user can select the specific alarm type by clicking “Add alarm type” again. The effect is shown in Figure 6-56.

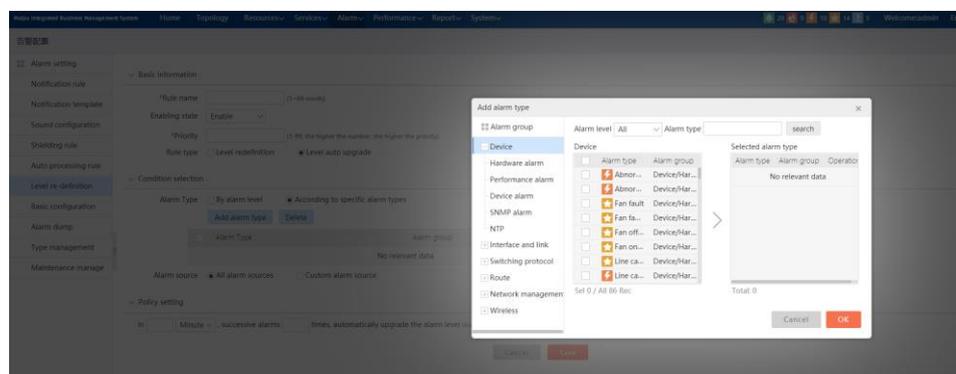


Figure 6-56 Alarm type configuration

The alarm source is used to determine which alarm information needs to be redefined. Alarm source rules include all alarm sources and custom alarm sources. When the user selects a custom alarm source, a list will appear. The user can click **Add alarm type** to select the specific alarm source. The effect is shown in Figure 6-57.

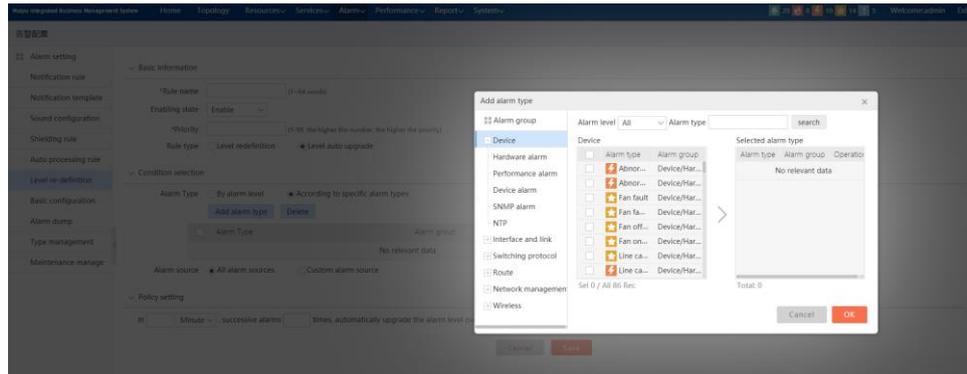


Figure 6-57 Alarm source configuration

Redefinition result configuration:

If the rule type is selected as level redefinition, it is necessary to configure the level after redefinition, including four levels: urgent, important, secondary and tips. If the rule type is level auto upgrade, you need to configure the level policy. For the effect, refer to the level type of the basic information.

Users can modify the definition of alarm level. Select an alarm level redefinition rule, and then click **Modify**. For the basic information, you can only modify the enabling status and priority, while the alarm source, alarm type and result settings all can be modified.

After modification, click **Save**, and the effect is shown in Figure 6-58.

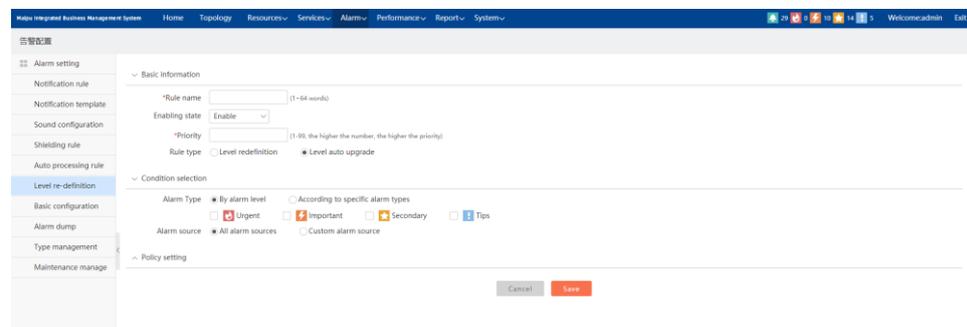


Figure 6-58 Modify alarm level redefinition

## 6.2.6. Alarm Basic Configuration

The basic alarm configuration is used to configure the SYSLOG receive port number, TRAP receive port number, EngineID, and whether to enable the alarm flash-off filtering configuration and alarm repeated filtering configuration. If the flash filtering and repeated filtering configuration are enabled, it is necessary to configure the flash and repeated filtering period. In addition, users can add, modify and delete TRAP SNMP V3 security users. The effect is shown in Figure 6-59.

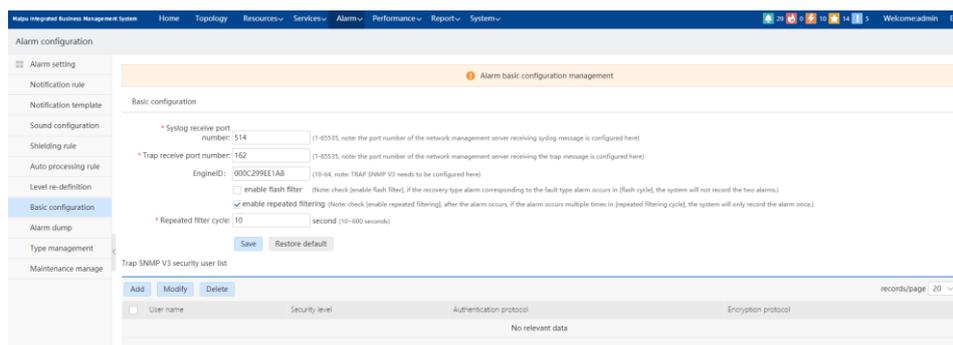


Figure 6-59 Basic configuration of the alarm

Basic configuration:

Syslog receive port is the port number used by the NMS server to receive syslog messages. The port number is required here.

TRAP receive port number is the port number used by the network management server to receive TRAP messages. The port number is required here.

Flash filtering is used to record the two alarm messages in the network management server if there is a fault type alarm in a flash period, and then the recovery alarm corresponding to the fault type alarm appears. If the flashing filter configuration is enabled, the flashing period must be configured.

Repeated filtering is used to record the alarm only once in the repeated filtering period after the alarm occurs and the alarm occurs many times. If the flashing filter configuration is enabled, the repeated filtering period must be configured.

After the above parameters are configured, click “Save”, and the effect is shown in Figure 6-60.

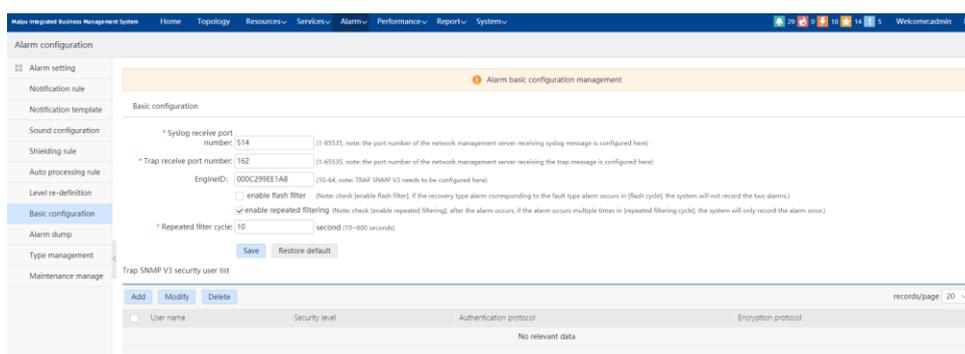


Figure 6-60 Basic configuration

If the user wants to restore the basic configuration, just click [Restore default](#). Among them, the syslog receive port number is 514, the trap receive port number is 162, engineid is \* \* \* (automatically generated according to the environment), flash filtering is not enabled by default, repetitive filtering is on by default, and repeated filtering period is 10 seconds. The effect is shown in Figure 6-61.

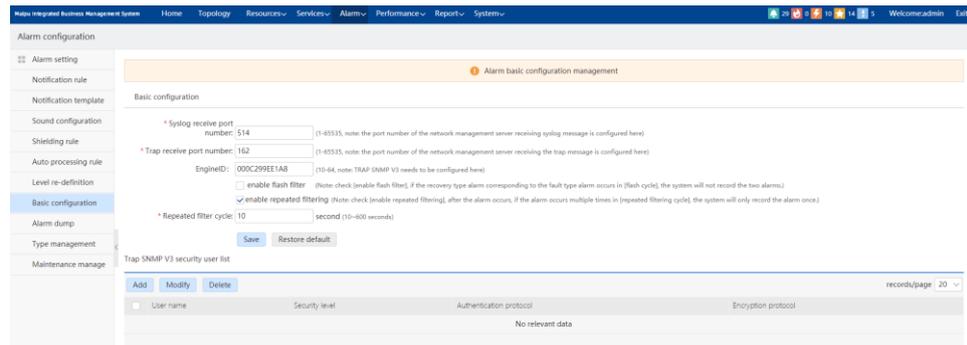


Figure 6-61 Restore default basic configuration

TRAP SNMP V3 security users are used to add, modify and delete SNMP V3 users. The effect is shown in Figure 6-62.

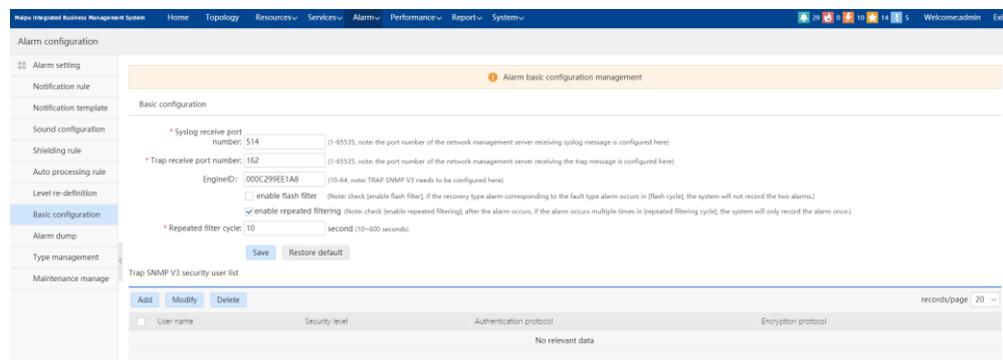


Figure 6-62 Security user list

Add a security user:

First, click **Add** in the upper left corner of trap SNMP V3 security user list to pop up an interface of adding a security user. The user needs to fill in the agent user name and select the security level. If both authentication and encryption are selected for security level, authentication protocol and password should be selected, encryption protocol and encryption password should be filled in. If only authentication without encryption is selected as the security level, authentication protocol and authentication password need to be selected. If the user selects no authentication and no encryption, click the OK button, and the effect is shown in Figure 6-63.

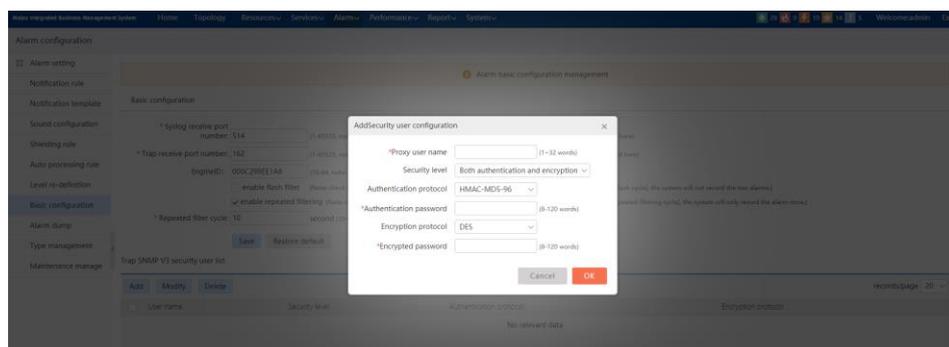


Figure 6-63 Add a security user

Edit security user:

First, select a security user in the TRAP SNMP V3 security user list, and then click **Modify** in the upper left corner of the user list to open a security user configuration modification interface. Users can modify the user configuration as desired. Only the proxy user name cannot be modified. The effect is shown in Figure 6-64.

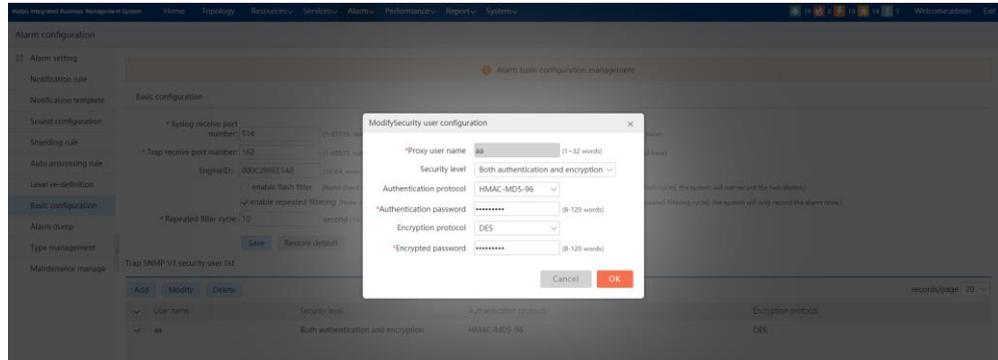


Figure 6-64 Modify a security user

Delete a security user:

First, select one or more security users in the TRAP SNMP V3 security user list, then click **Delete** in the upper left corner of the user list to pop up a prompt box, and then click **OK** in the prompt box. The effect is shown in Figure 6-65.

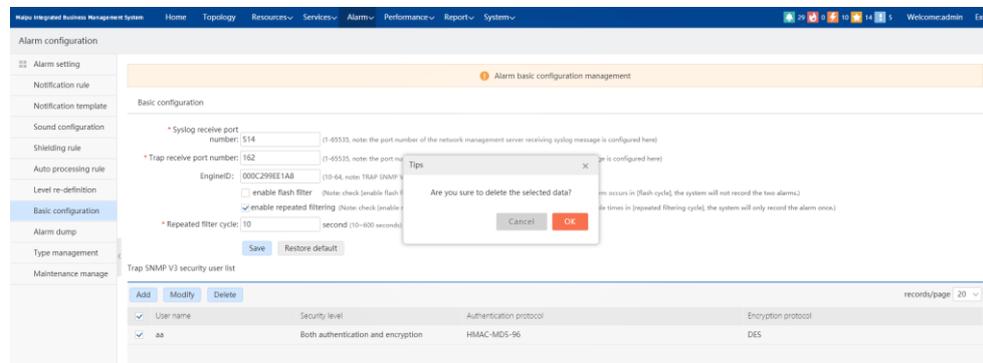


Figure 6-65 Delete a security user

## 6.2.7. Alarm Dump

Alarm dump configuration is used to configure the conditions that trigger alarm dump operation. Only one parameter of maximum reserved number needs to be configured. If it is not modified, the default value is 5 million. When the alarm data exceeds 5 million, trigger the alarm dump operation, and the dumped file will be displayed on the interface. In addition, the alarm dump is checked at 1:00 a.m. every day, and the effect is shown in Figure 6-66.

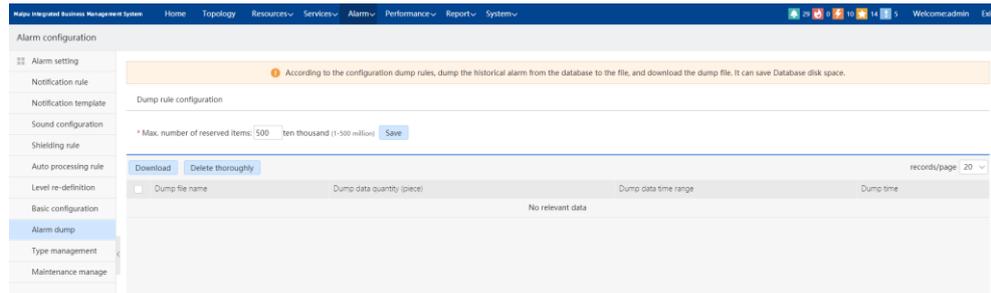


Figure 6-66 Alarm dump

The user can also download and delete the dump file completely on the interface.

The user selects one or more files in the dump list, and then clicks **Download** to download the dump file. The user selects one or more files and then clicks **Delete thoroughly** to delete the selected dump files. The effect is shown in Figure 6-67.

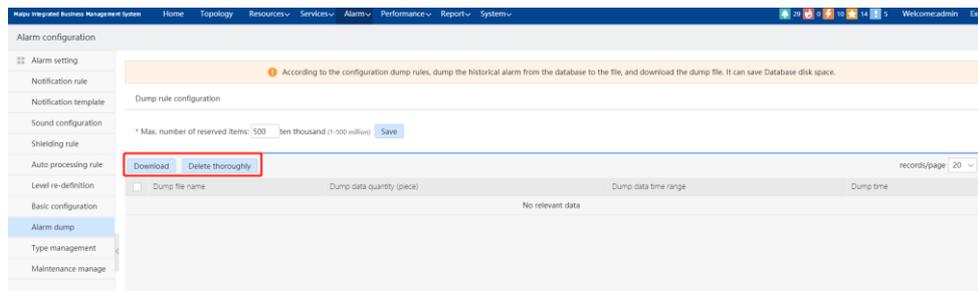


Figure 6-67 Download/delete the alarm dump file

### 6.2.8. Alarm Type Management

Alarm type management is used to manage alarm types. Users can query, add, edit, delete and export alarm types (only the new alarm types can be edited and deleted, and the inbuilt alarm types cannot be edited or deleted). In the alarm type configuration interface, the user can query the alarm type by the name of the alarm type, or select the group of the alarm type, category, and whether it is an inbuilt condition to accurately query the alarm type. The effect is shown in Figure 6-68.

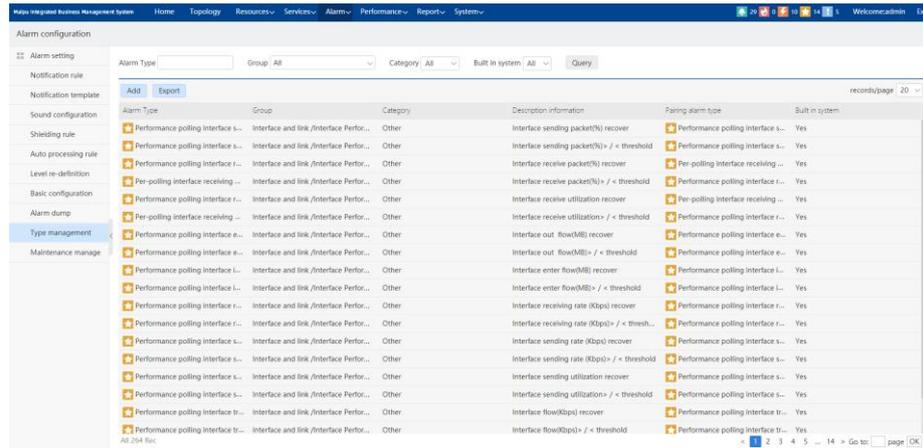


Figure 6-68 Alarm type management

The user can click **Add** to add an alarm type. The information to be filled in is the name of the alarm type, the selected group and the alarm level. The information is required, and the effect is shown in Figure 6-69.

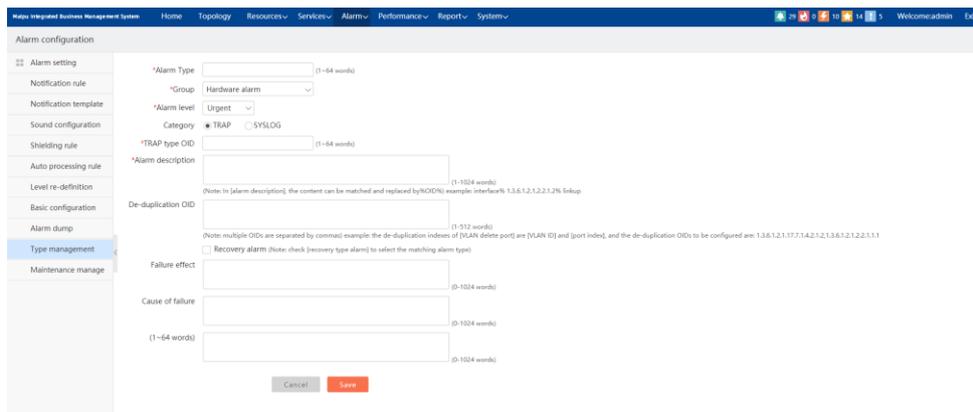


Figure 6-69 Add an alarm type

Type:

There are two types, TRAP and SYSLOG. If the user selects TRAP, the information to be filled in is TRAP OID (required), alarm description (required), de-duplication OID, fault effect, cause of failure, and processing suggestions. The effect is shown in Figure 6-70.

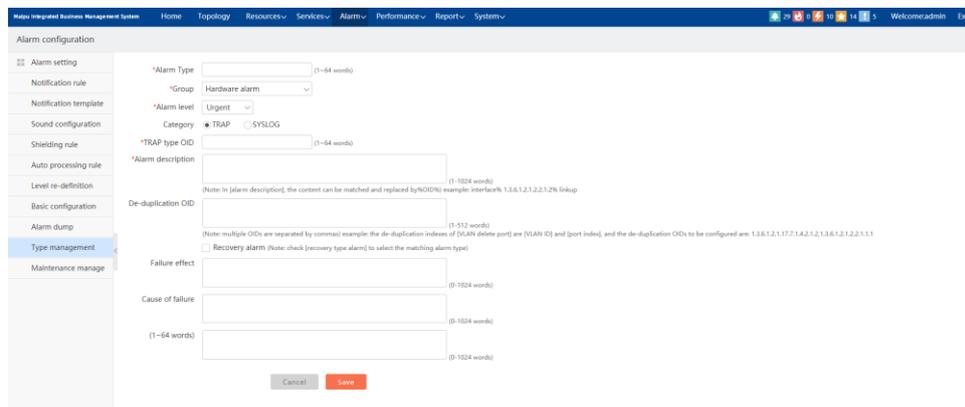


Figure 6-70 Add a Trap alarm type

If the user selects the recovery alarm, the new alarm type and the selected alarm type are paired (the paired alarms must be in the same group), and the effect is shown in Figure 6-71.

The screenshot shows the 'Alarm configuration' page in the Maipu Integrated Business Management System. The left sidebar lists various configuration options, with 'Type management' selected. The main area is titled 'Alarm configuration' and contains several fields:
 

- \*Alarm Type: (1-64 words)
- \*Group: Hardware alarm
- \*Alarm level: Urgent
- Category:  TRAP  SYSLOG
- \*TRAP type OID: (1-64 words)
- \*Alarm description: (1-1024 words)
- De-duplication OID: (1-512 words)
- Failure effect: (1-1024 words)
- Cause of failure: (1-1024 words)
- (1-64 words): (1-1024 words)
- (1-1024 words): (1-1024 words)

 At the bottom, there are 'Cancel' and 'Save' buttons.

Figure 6-71 TRAP alarm pairing operation

If the user selects SYSLOG, the information to be filled in is the log keyword (required), de-duplication judging regular expression, fault influence, fault cause and treatment suggestion, and the effect is shown in Figure 6-72.

The screenshot shows the 'Alarm configuration' page with the 'SYSLOG' category selected. The fields are:
 

- \*Alarm Type: (1-64 words)
- \*Group: Hardware alarm
- \*Alarm level: Urgent
- Category:  TRAP  SYSLOG
- \*Log key: (1-256 words)
- De-duplication regular expression: (1-512 words)
- Failure effect: (1-1024 words)
- Cause of failure: (1-1024 words)
- (1-64 words): (1-1024 words)
- (1-1024 words): (1-1024 words)

 At the bottom, there are 'Cancel' and 'Save' buttons.

Figure 6-72 Add SYSLOG alarm type

If the user selects the recovery of alarm, the new alarm type is paired with the selected alarm type, and the effect is shown in Figure 6-73.

The screenshot shows the 'Alarm configuration' page with the 'SYSLOG' category selected. A new field, '\*Pairing alarm type', has appeared with a 'Select' button next to it. The other fields remain the same as in Figure 6-72. At the bottom, there are 'Cancel' and 'Save' buttons.

Figure 6-73 SYSLOG alarm pairing operation

The user can modify the alarm type (new alarm type). Find the desired alarm type, and then click . For the two alarm types, you cannot modify the alarm type name. Here.

for the Trap alarm type, you cannot modify TRAP type OID, and the others can be modified (for the paired alarm type, you cannot modify its group), and the effect is shown in Figure 6-74.

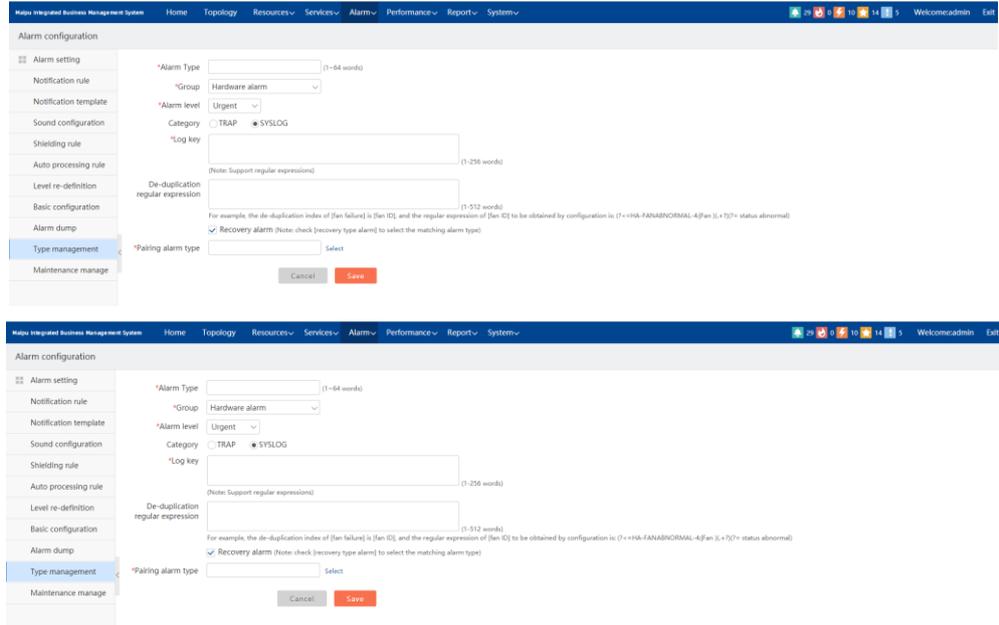


Figure 6-74 Modify the alarm type

### 6.2.9. Maintenance Experience Management

The maintenance experience management is used to add maintenance experience for the alarm type. The user can query, edit, delete, and export the alarm maintenance experience. In the maintenance experience management interface, the user can perform fuzzy query for the alarm type by the alarm type name and maintenance experience, or select the grouping condition of the alarm type to accurately query the alarm type. The effect is shown in Figure 6-75.

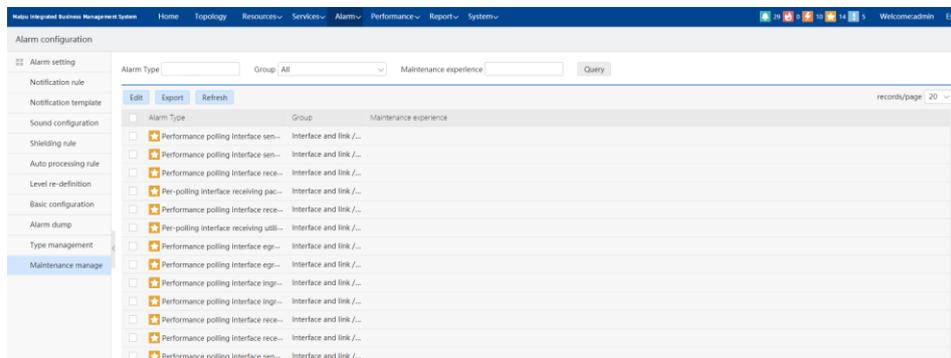


Figure 6-75 Maintenance experience management

Users can select an alarm type on the interface, and then click **Modify** to add maintenance experience for the alarm type. The information to be filled in is alarm maintenance experience (required), and the effect is shown in Figure 6-76.

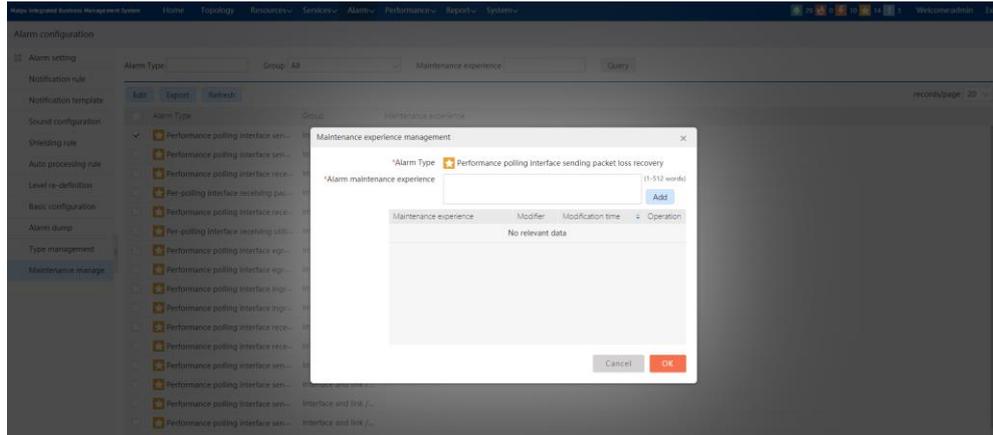


Figure 6-76 Add the alarm maintenance experience

### 6.3. Syslog Log

Click "Alarm" -> "Syslog Log" in the menu bar to open the Syslog log page. Users can query accurately through log level, matching alarm and occurrence time in the Syslog log interface, and can also perform fuzzy query for the device and content. At the same time, it also supports the accurate query for the device. The effect is shown in Figure 6-77.

Device IP	Device name	Log level	Matching alarm	Content	Organization	Occurrence time
10.10.1.1	router	Important	Un-matching	rtr : (537)LogMsg-STOP-4: Syslog auto stop	Headquarters	2020-05-26 06:47:44
10.10.1.1	router	Important	Matching	rtr : (1177)LINK-LINEPROTO_DOWN-3: Line protocol on interface vlan200...	Headquarters	2020-05-20 10:01:55
10.10.1.1	router	Important	Matching	rtr : (115)PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface ...	Headquarters	2020-05-20 10:01:55
10.10.1.1	router	Important	Matching	rtr : (115)LINK-INTERFACE_DOWN-3: Interface vlan2000, changed state...	Headquarters	2020-05-20 10:01:55
10.10.1.1	router	Important	Un-matching	rtr : (155)LogMsg-STOP-4: Syslog auto stop	Headquarters	2020-05-20 07:51:30
10.10.1.1	router	Important	Un-matching	rtr : (577)LogMsg-STOP-4: Syslog auto stop	Headquarters	2020-05-20 07:30:38
10.10.1.1	router	Important	Matching	rtr : (217)LINK-LINEPROTO_DOWN-3: Line protocol on interface vlan200...	Headquarters	2020-05-20 06:07:58
10.10.1.1	router	Important	Matching	rtr : (19)PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface gi...	Headquarters	2020-05-20 06:07:58
10.10.1.1	router	Important	Matching	rtr : (209)LINK-INTERFACE_DOWN-3: Interface vlan2000, changed state t...	Headquarters	2020-05-20 06:07:58
10.10.1.1	router	Important	Matching	rtr : (155)LINK-LINEPROTO_DOWN-3: Line protocol on interface vlan200...	Headquarters	2020-05-20 06:07:53
10.10.1.1	router	Important	Matching	rtr : (145)LINK-INTERFACE_DOWN-3: Interface vlan2000, changed state t...	Headquarters	2020-05-20 06:07:53
10.10.1.1	router	Important	Matching	rtr : (137)PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface gi...	Headquarters	2020-05-20 06:07:53

Figure 6-77 Syslog log

Users can also perform the accurate query through the device. First, select the alarm source to accurately match, then click the "Select device" button, and then the dialog box of selecting the device will appear. Users can add devices by adding device groups, adding devices, and adding local network management. Finally, click "OK" to query accurately by device. The effect is shown in Figure 6-78.

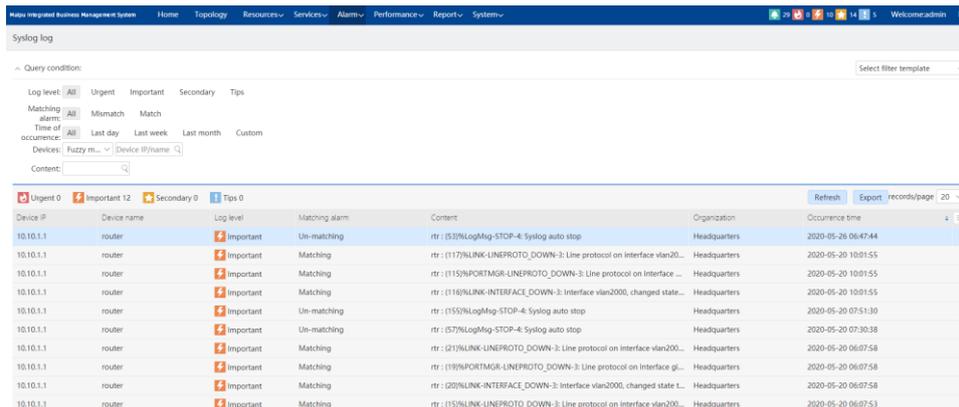


Figure 6-78 Accurate query by the device

After querying the desired Syslog logs, users can click “Export” to export the syslog logs in the list (including paged syslog logs).

10.10.1.1	router	Important	不匹配	rtr : (53)%LogMsg-STOP-4: Syslog auto stop	5/26/2020 6:47 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (117)%LINK-LINEPROTO_DOWN-3: Line protocol on interface vlan2000, changed state to down.	5/20/2020 10:01 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (115)%PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/2, changed state to down.	5/20/2020 10:01 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (116)%LINK-INTERFACE_DOWN-3: Interface vlan2000, changed state to down.	5/20/2020 10:01 /Headquarters/
10.10.1.1	router	Important	不匹配	rtr : (155)%LogMsg-STOP-4: Syslog auto stop	5/20/2020 7:51 /Headquarters/
10.10.1.1	router	Important	不匹配	rtr : (57)%LogMsg-STOP-4: Syslog auto stop	5/20/2020 7:30 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (21)%LINK-LINEPROTO_DOWN-3: Line protocol on interface vlan2000, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (119)%PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/2, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (20)%LINK-INTERFACE_DOWN-3: Interface vlan2000, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (15)%LINK-LINEPROTO_DOWN-3: Line protocol on interface vlan2000, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (14)%LINK-INTERFACE_DOWN-3: Interface vlan2000, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important	匹配	rtr : (13)%PORTMGR-LINEPROTO_DOWN-3: Line protocol on interface gigabitethernet0/2, changed state to down.	5/20/2020 6:07 /Headquarters/

Figure 6-79 Export the Syslog log

## 6.4. Unrecognized Trap

Click "Alarm" -> "Unrecognized trap" in the menu bar to open the unrecognized trap interface. The user can make accurate query through the occurrence time in the unrecognized trap interface, and can also make fuzzy query for the device and type oid. At the same time, it also supports accurate query for the device. The effect is shown in Figure 6-80.

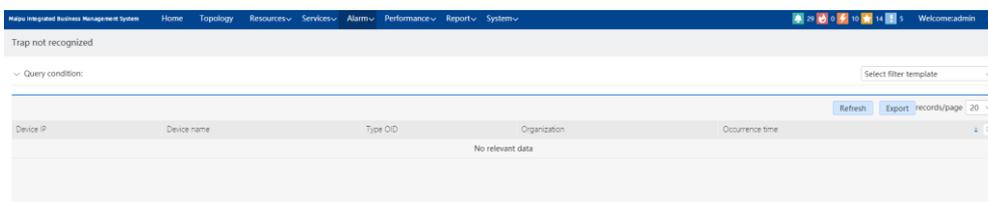


Figure 6-80 Unrecognized Trap

Users can also perform the accurate query through the device. First, select the alarm source to accurately match, then click the “Select device” button, and then the dialog box of selecting the device will appear. Users can add devices by adding device groups, adding devices, and adding local network management. Finally, click “OK” to query accurately by device. The effect is shown in Figure 6-81.

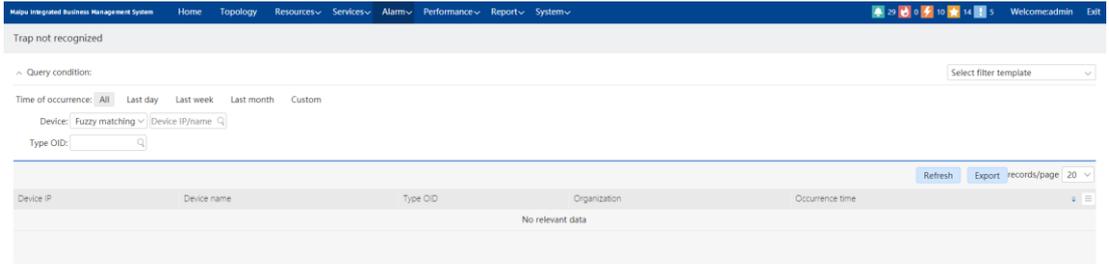


Figure 6-81 Accurate query by the device

After users queried the desired unrecognized trap information, click **Export** to export the unrecognized trap information in the list (including paged unrecognized trap information).

Device IP	Device name	Type OID	Organization	Occurrence time
10.10.1.1	router	Important 不匹配	rtr: (53)%LogMsg-STOP-4. Syslog auto stop	5/26/2020 6:47 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (117)%LINK-LINEPROTO_DOWN-3. Line protocol on interface vlan2000, changed state to down.	5/20/2020 10:01 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (115)%PORTMGR-LINEPROTO_DOWN-3. Line protocol on interface gigabitethernet0/2, changed state to down.	5/20/2020 10:01 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (116)%LINK-INTERFACE_DOWN-3. Interface vlan2000, changed state to down.	5/20/2020 10:01 /Headquarters/
10.10.1.1	router	Important 不匹配	rtr: (155)%LogMsg-STOP-4. Syslog auto stop	5/20/2020 7:51 /Headquarters/
10.10.1.1	router	Important 不匹配	rtr: (57)%LogMsg-STOP-4. Syslog auto stop	5/20/2020 7:30 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (21)%LINK-LINEPROTO_DOWN-3. Line protocol on interface vlan2000, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (19)%PORTMGR-LINEPROTO_DOWN-3. Line protocol on interface gigabitethernet0/2, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (20)%LINK-INTERFACE_DOWN-3. Interface vlan2000, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (15)%LINK-LINEPROTO_DOWN-3. Line protocol on interface vlan2000, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (14)%LINK-INTERFACE_DOWN-3. Interface vlan2000, changed state to down.	5/20/2020 6:07 /Headquarters/
10.10.1.1	router	Important 匹配	rtr: (13)%PORTMGR-LINEPROTO_DOWN-3. Line protocol on interface gigabitethernet0/2, changed state to down.	5/20/2020 6:07 /Headquarters/

Figure 6-82 Export the unrecognized Trap information

# 7.Reports

## 7.1. Report Task Management

Click "Report" - > "Report Task" in the menu bar to open the report task management interface as follows. Click the report tree on the left, and the report tasks of the corresponding type will appear in the right report task list. At the same time, this page provides the functions of adding, modifying, deleting, querying, enabling, disabling, and generating report tasks.

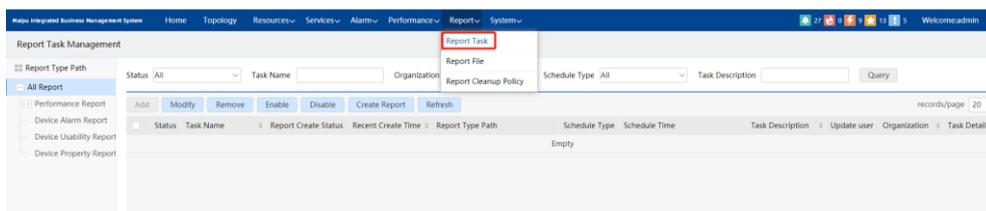


Figure 7-1 Report task management

### Add the report task

Click "Add" to open the dialog box of adding/ modifying the report task, as follows:

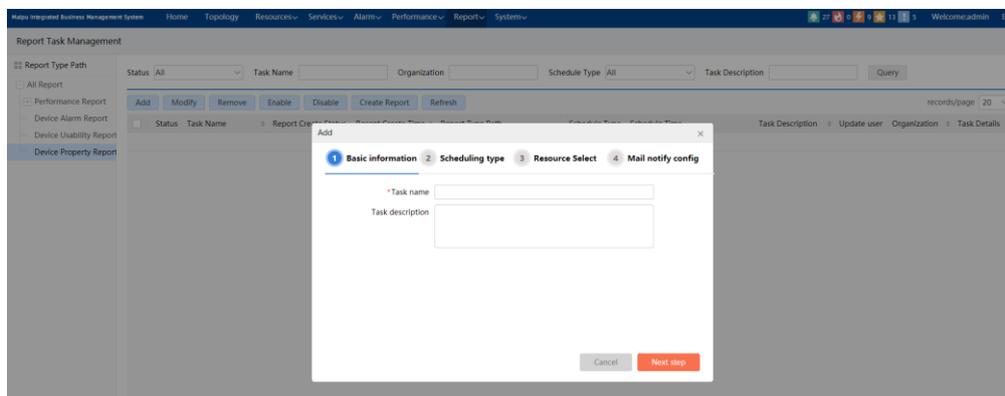


Figure 7-2 Add/modify the report task-Step 1

Fill in the task name and task description information, and click "Next step" to select the scheduling type, as follows:

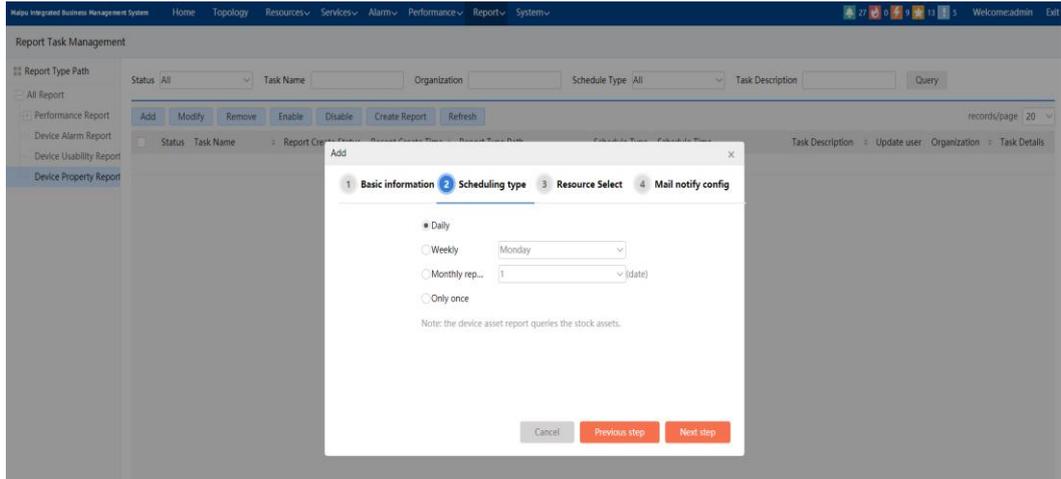


Figure 7-3 Add/modify the report task-Step 2

In this page, you can select the scheduling type of the report: daily, weekly, monthly, only once. Only one item can be selected. When selecting weekly and monthly, you can select which day of the week or which day of the month to carry out the report task. For the "only once" option, you can set the time period by yourself. Click "Next step" to enter the interface of selecting the device, as follows:

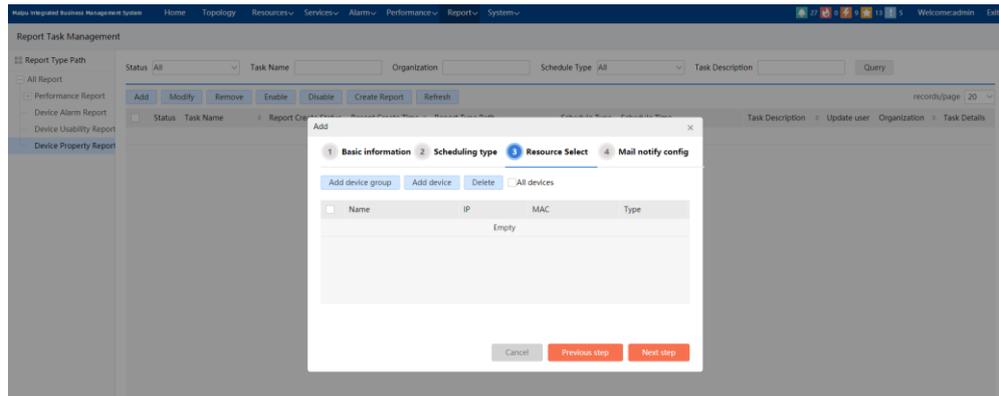


Figure 7-4 Add/modify the report task-Step 3

Click "Add device group", "Add device" and "Delete" button to add and delete device/device group. Select "All devices" to add all devices in the system. Select the device and click "Next step" to enter the email notification configuration interface, as follows:

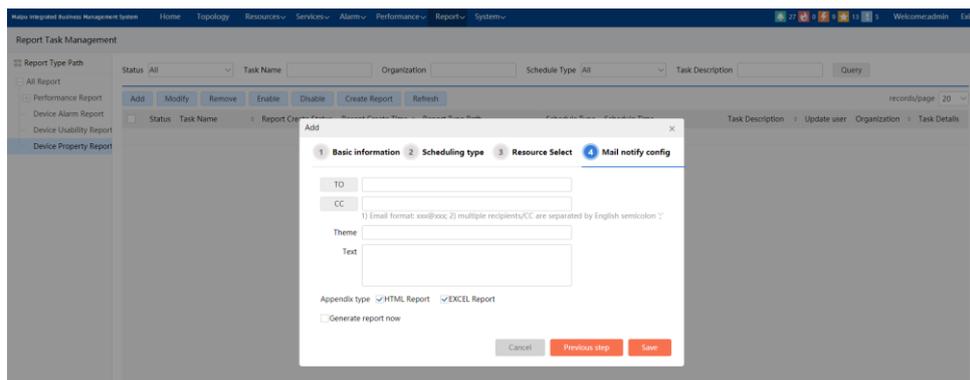


Figure 7-5 Add/modify the report task-Step 4

On the interface, you need to fill in the recipient, email body, subject and other information, select the attachment type (HTML report/excel report) and whether to generate the report immediately, and click "Save" to generate the report task.

### Note

- The execution time of daily, weekly and monthly reports: the default value is 3:00 a.m., which can be configured through /home/mpup/mpup/plugins/basenm/conf/report/ReportConfig.xml.
- Only when a specific report type of the left report type tree is selected can the report task be added; otherwise, the report task cannot be added.
- The email notification configuration only supports sending mail to standard protocol mailbox, but does not support non-standard protocol mailbox, such as QQ mailbox.

### Modify the report task

Select a report task and click "Modify" to modify the selected report task. The steps are the same as that of "Add report task".

### Delete the report task

Select the report task and click "Delete". The prompt box for confirming the deletion will pop up as follows. Click "OK" to delete.

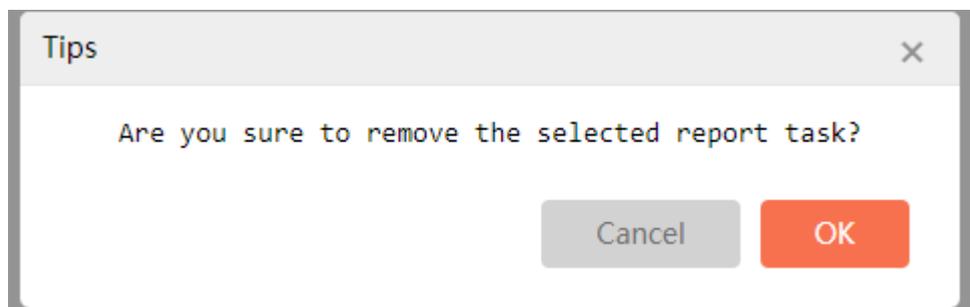


Figure 7-6 Confirm deleting prompt box

### Enable the report task

Select the report task and click the "Enable" button to open the confirmation dialog box as follows. Click "OK" to enable the disabled report task.

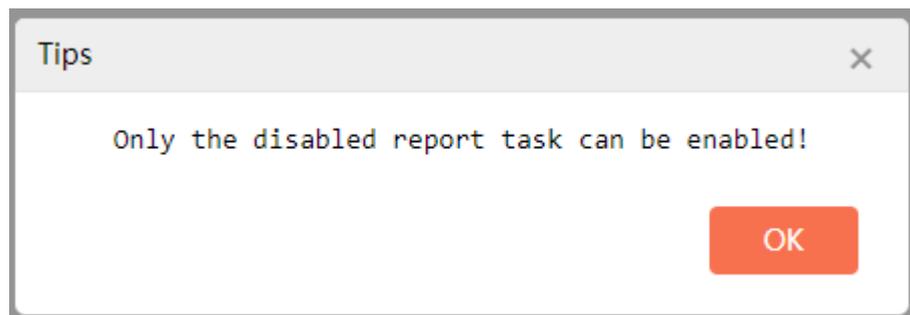


Figure 7-7 Confirm enabling dialog box

### Disable the report task

Select a report task and click "Disable" to open the confirmation dialog box as follows. Click OK to disable the enabled report task.

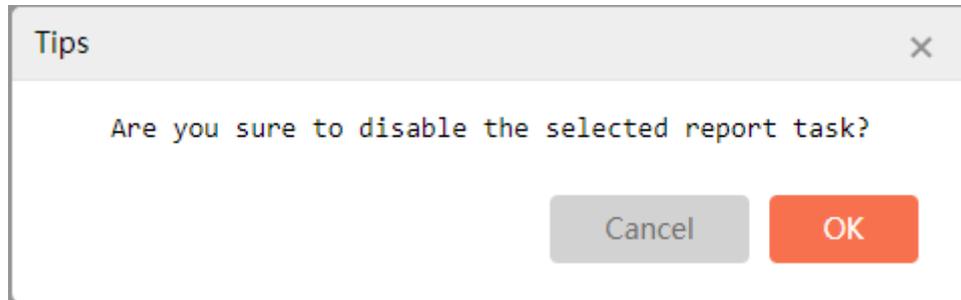


Figure 7-8 Confirm disabling dialog box

---

### ● Note

- Only disabled report tasks can be enabled, and only enabled report tasks can be disabled.
- 

### Generate the report

Select the report task and click the "Generate report" button to open the dialog box of confirming generating the report, as shown in the figure below. Click "OK" to prompt that the report is generated successfully.

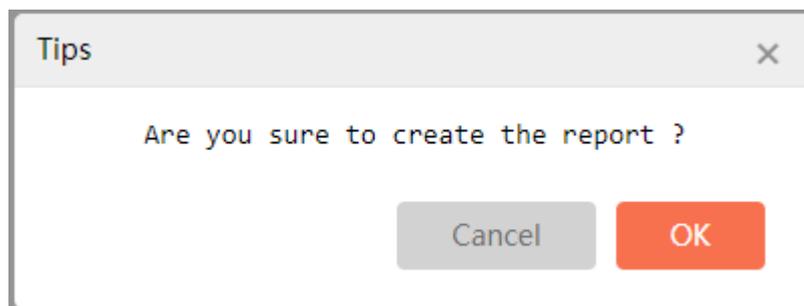


Figure 7-9 Confirm generating the report

### View the task details

Click "View" under the task details field in the report task to open the task details dialog box, as shown in the figure below, from which you can view the basic information of the task and the selected resource information.

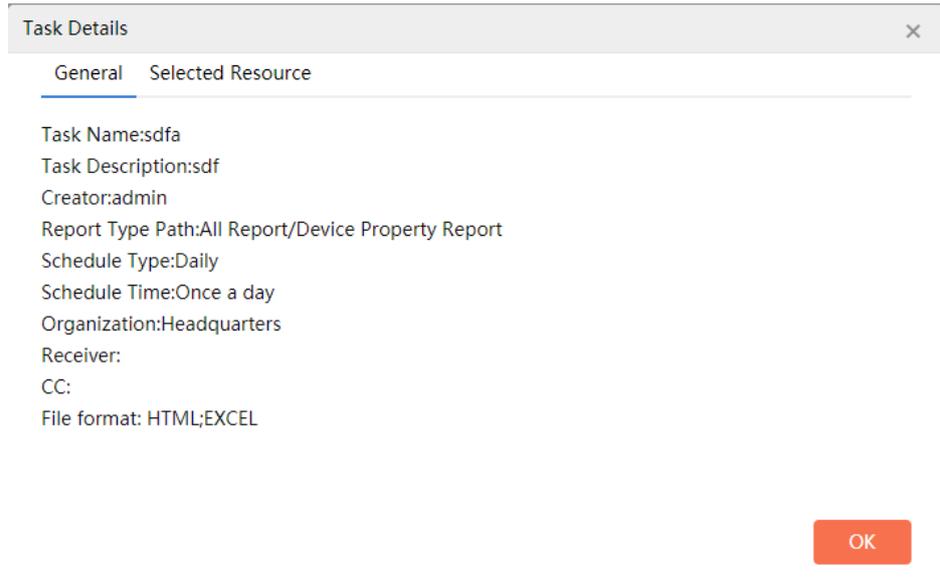


Figure 7-10 Task details

**Query the report task**

This page provides the query operation for report tasks, as shown in the figure below. Advanced query filtering can be performed by selecting task status, organization, scheduling type, and keyword task name and task description.



Figure 7-11 Task query

**7.2. Report File Management**

Click "Report" -> "Report File" in the menu bar to open the report file management page as follows. By default, the report file list displays all report files by pages, including report file, report type path, task name, creation time, size, download and preview fields. At the same time, this page has the function of querying, deleting, downloading, and previewing the report file.

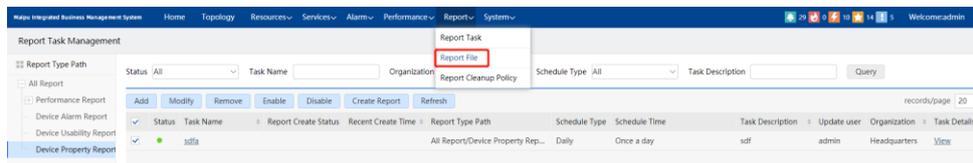


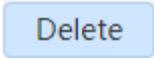
Figure 7-12 Report file management

**Query the report file**

In the report file query section, you can perform advanced query filtering for report files through the start time, end time, report file, and report type path fields, as shown in the following figure:

Start time  End time  Report file  Organization  Report type path

### Delete the report file

Select the desired report file, click , and a prompt box for confirming deletion will pop up as follows. Click "OK" to delete.

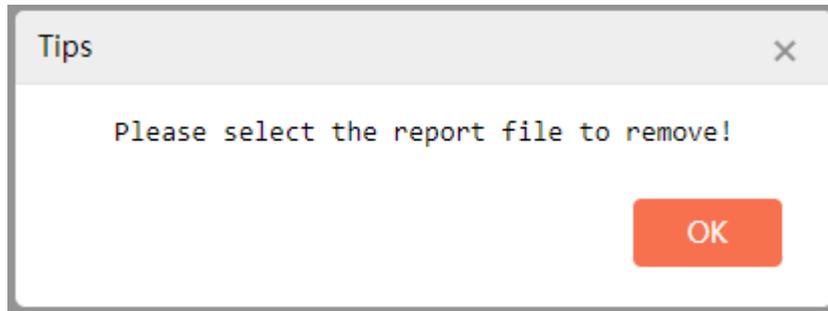
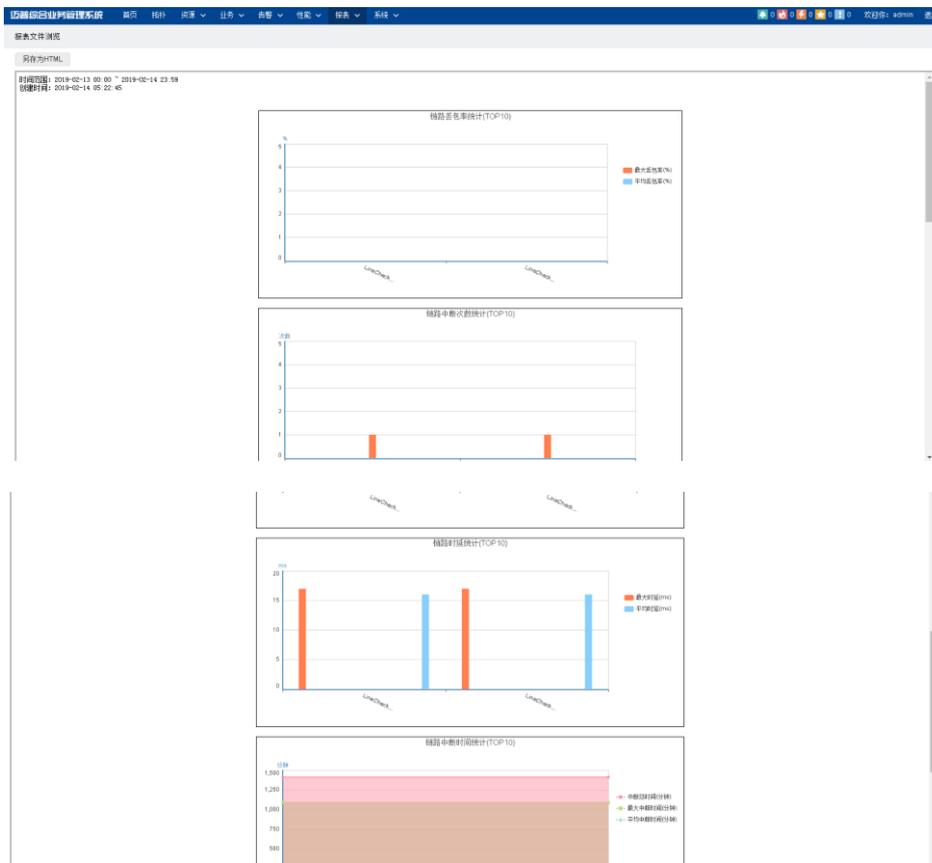


Figure 7-13 Confirm deleting

### Preview the report file

Click "Preview" after the report file to enter the report file browsing page. As shown in the figure below, the report file browsing page of the device alarm report is displayed, including the statistics of alarm type, alarm level and device alarms.



网络系包量统计

排名	链路名称	最大吞吐量 (K)	平均吞吐量 (K)
1	LineCheckCenter200	0.0	0.0
2	LineCheckCenter199	0.0	0.0

网络中程次数统计

排名	链路名称	中程次数
1	LineCheckCenter200	0
2	LineCheckCenter199	0

网络时延统计

排名	链路名称	最大时延 (ms)	平均时延 (ms)
1	LineCheckCenter200	17.0	16.0
2	LineCheckCenter199	19.0	18.0

网络中程时间统计

排名	链路名称	中程总时间 (分钟)	最大中程时间 (分钟)	平均中程时间 (分钟)
1	LineCheckCenter200	0.415	0.000	0.000
2	LineCheckCenter199	0.415	0.000	0.000

Figure 7-14 Preview the report file

**Note**

- Only the HTML format report file can support the file preview function, while the XLS format report file can only be downloaded and cannot be previewed.

**Download the report file**

Click "Download" after the report file to download the report file in the corresponding format.

**7.3. Report Cleanup Policy Configuration**

Click "Report" -> "Report cleaning policy" in the menu bar to open the report cleanup policy configuration page as follows.

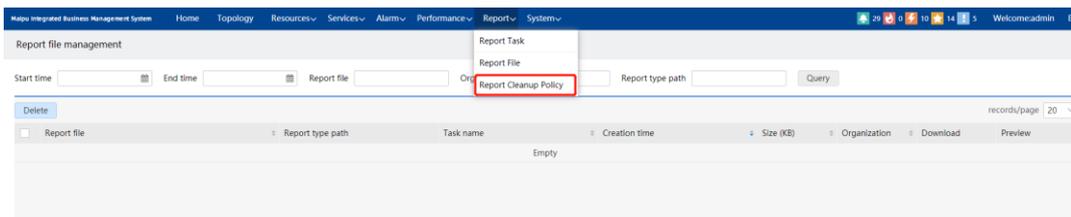


Figure 7-15 Report cleanup policy management

The page configuration includes the cleanup triggering condition and cleanup action. For the triggering condition, there are two parameters to set: the longest storage time (days) and the maximum disk space (M). For the clearing action, you can choose to dump to the specified folder, upload to FTP, or delete directly. The server IP, FTP port, user name and password need to be configured for uploading to FTP. Click the "Save" button to save the configuration information, and click the "Reset" button to restore all configurations to the default state.

**Note**

- The maximum storage time is 90 days by default, and the maximum disk space is

---

800M by default.

- The default dump address is /opt/mpup/plugins/basenm/ReportFiles4Move.
  - The default FTP port is port 21.
-

# 8. System Management

## 8.1. Organization Management

Organization management provides the management of enterprise organization or the division of the device area. Click "System" -> "Organization management" in the top menu bar to open the "Organization Management" page. It provides the functions of querying, adding, modifying, deleting, importing, exporting and downloading the import template.



Figure 8-1 Organization management

### Query the organization

At the top of the organization management view is the organization query module, as shown in the following figure. You can query according to the name, code and abbreviation of the organization. The query content will be displayed by pages in the organization list below.

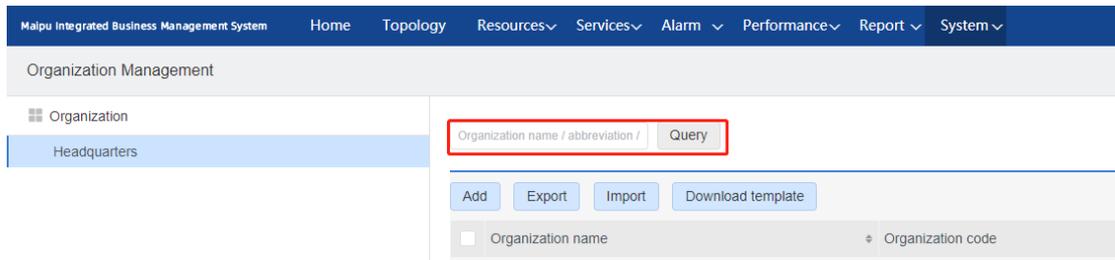


Figure 8-2 Organization query

### Add an organization

Click **Add** to open the "Add/Modify organization" dialog box, fill in the organization name, organization abbreviation, organization code, organization address and description information, select the superior, and click "OK" to save the new organization.

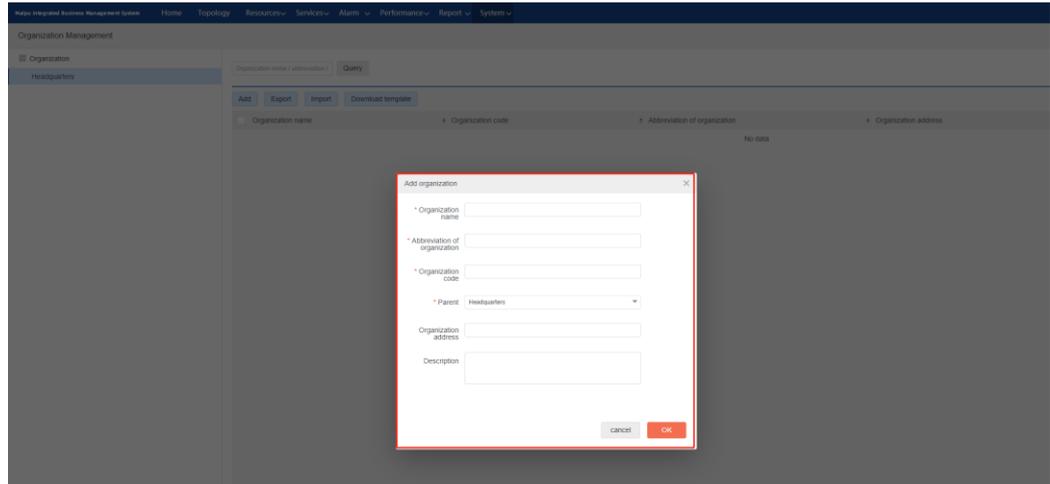


Figure 8-3 Add an organization

### Modify an organization

In the organization list, select the desired organization (only one organization can be modified at the same time), and click the icon after the organization to open the “Edit” dialog box to modify all the information of the organization in the dialog box. After the modification, click the "OK" button to save the modification information.

### Delete an organization

Select the desired organization in the organization list, click , and click "OK" in the pop-up dialog box to delete the selected organization.

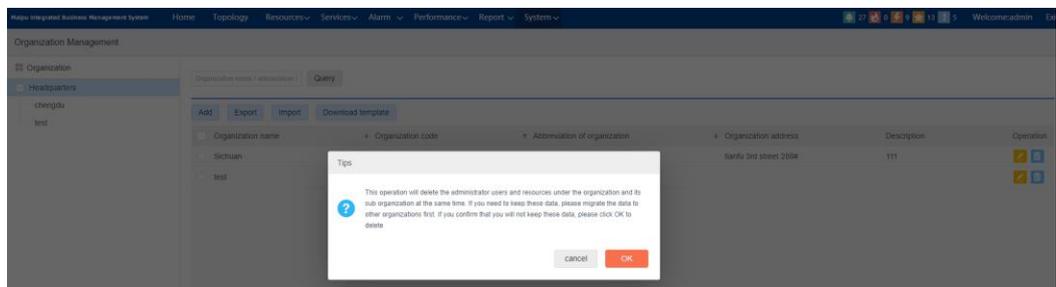


Figure 8-4 Delete an organization

### Note

- The headquarters cannot be deleted.
- If you need to edit the information of the headquarters, you can enter "headquarters" in the query conditions, and then follow the steps of the above editing organization after the information of the head office is found.
- Deleting the organization will delete the users, official account, WeChat public address, equipment and other resources under the organization synchronously. Please confirm that the relevant resources have been properly processed before executing the delete operation.

### Import the organization

The imported organization needs to meet the organization import template. Otherwise, it cannot be imported correctly. Click **Download template** to download the import template. After downloading the template, fill in the organization information according to the template requirements. Click **Import** and select the desired organization file. After importing successfully, you can query the new imported organization in the organization management interface.

### Export the organization

Click **Export** to export and save all the current organizations as Excel files.

## 8.2. Operation Logs

The operation log module records all the important operations in the current system. The operation log module records the user operations from the operation user, IP address, log type, operation time and operation content, and provides the query and export function for the log information. Users can find the desired log information by user name, operation start and end time, log type and content. Click "System" -> "Operation log" in the menu bar to open the "Operation log management" page, as shown in the figure below.



Figure 8-5 Operation log interface

### Export the logs

Click the "Export" button in the log list to export the log information in the list to excel file.

10000	0	Headquarters	Headquarters	Headquarters	Headquarters
028	10000	Sichuan	chengdu	tianfu 3rd street 288#	111

Figure 8-6 Log excel file

### Log details

If the log content is too long to view in the form, you can view the log information through the log details. Click the "Details" field in the log list to open the "Details" dialog box, as shown in the figure below. You can get the operation user, log type, creation time and details of the log.

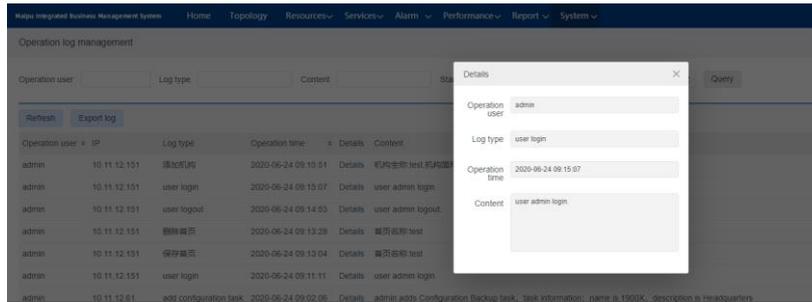


Figure 8-7 Log details

## Note

- The user name is "system", and IP is the operation log record of the current system installation server IP, which indicates some operations automatically executed within the system. These operations need no human intervention and are automatically executed by the system according to the current system status.

## 8.3. User and Authority Management

### 8.3.1. Role Management

#### Introduction to Role Management

Maipu integrated network management platform adopts matrix authority management, and users need to have two latitude authorities: role authority and management area authority. User and privilege management provides centralized management for users and their authorities.

Click “System” > “User and authority management” > “Role management” in the menu bar to open the “Role management” interface.

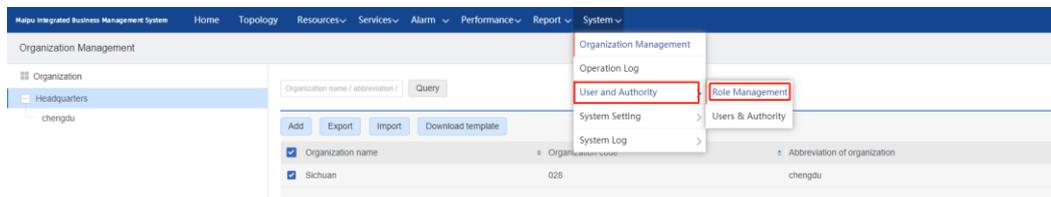


Figure 8-8 Role management

## Note

- The system administrator role has the authority of all modules in the system.

### Add a role

Click **Add** to open the "Add/Modify role" dialog box, fill in the role name and role description, select the authority, and click "OK", the role is added successfully.

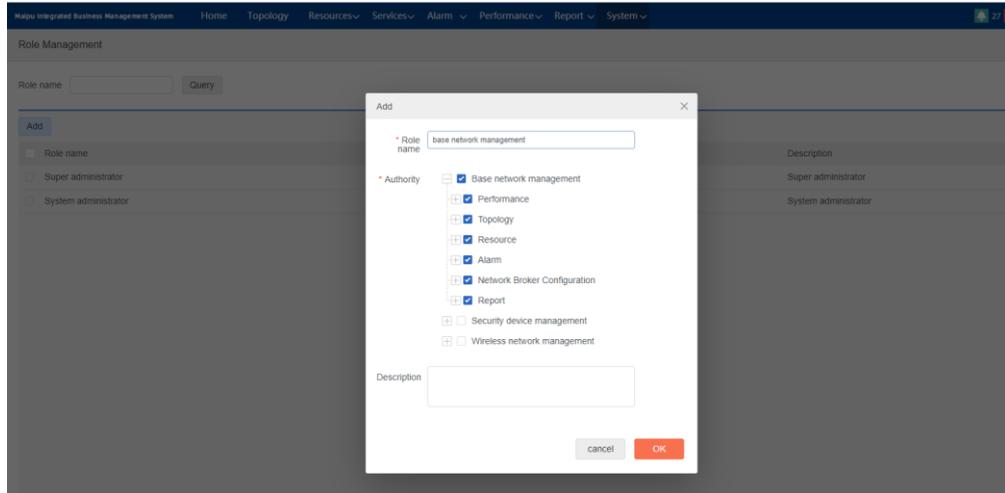


Figure 8-9 Add a role

### Note

- The new role has the user information, home page management and license viewing rights by default, and there is no need to specify.

### Modify a role

Click **✎** in the column of the desired role operation (Fig. 9.3.1.3) to open the "Modify role" dialog box to modify all parameters. Click "OK" after the modification, and the modification is successful.

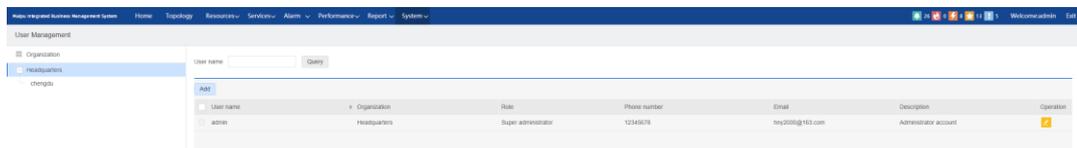


Figure 8-10 Modify the role

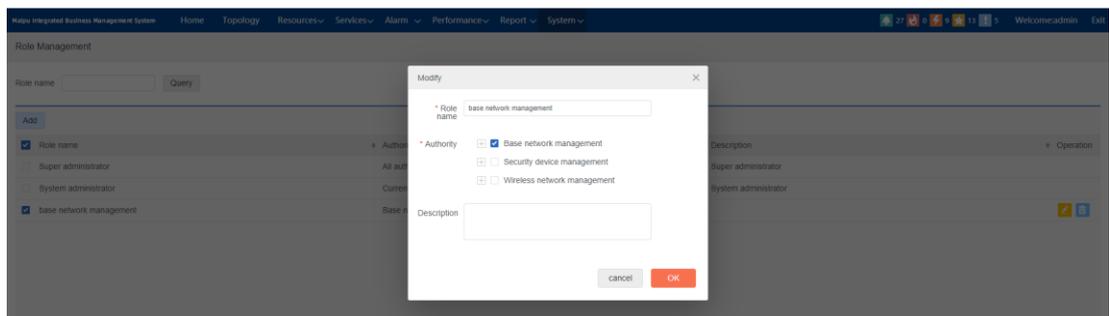


Figure 8-11 Modify a role

### Delete a role

Select the desired role, click  to open the delete confirmation dialog box, and click "OK" to delete successfully. The inbuilt roles of the system (administrator, system administrator) cannot be deleted.

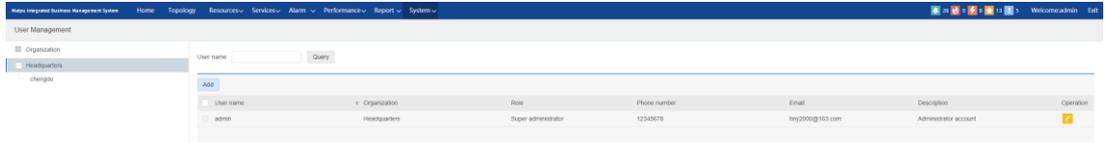


Figure 8-12 Delete a role

### Caution

- The inbuilt roles of the system (system administrator, super administrator) cannot be modified or deleted.

### Query the role

This page provides the query operation for the role, input the keywords in the role query panel to perform fuzzy query for the role name, as shown in the figure below:

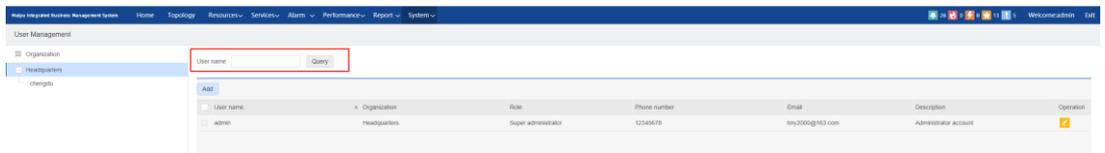


Figure 8-13 Query the role

## 8.3.2. User and Authority

Click "System" > "User and Authority Management" > "User & Authority" in the menu bar to open the "User & Authority" page, as shown in the figure below.

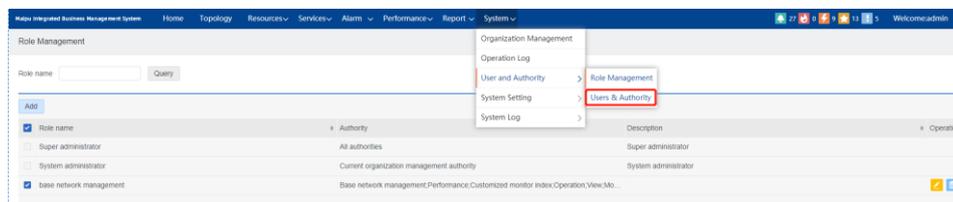


Figure 8-14 User and authority management

### Caution

- The default user information and its authorities of the system cannot be

---

modified.

---

### Add a user

Click  to open the "Add" dialog box, fill in the user name, password, contact information, email address, description, select the organization and role, click "OK", and the new user is added successfully.

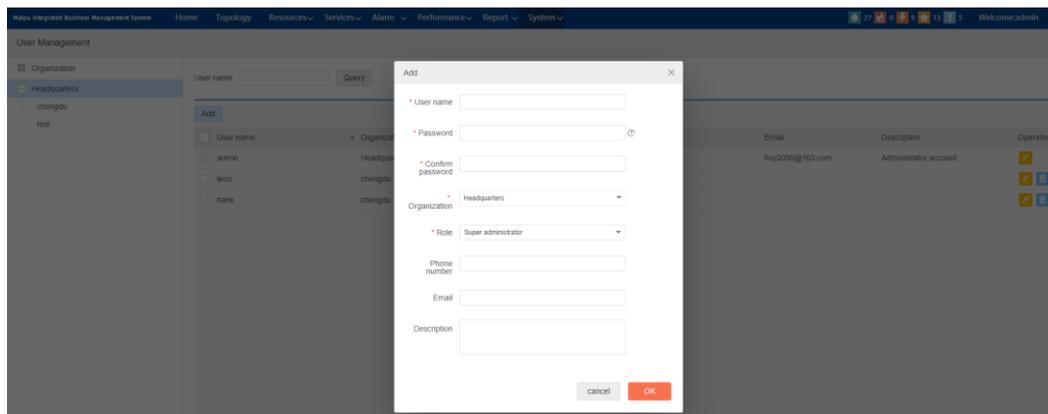


Figure 8-15 Add a user

## Caution

- The user password needs to meet the password policy set by the current system (which can be configured in the system settings). When adding a user, the cursor can be moved to the "?" after the password. The password policy set by the current system can be displayed.

### Modify the user information

Select the desired user and click  to open the "Modify" dialog box, where all parameters in the dialog box can be modified. Click "OK" after the modification, and the modification is successful.

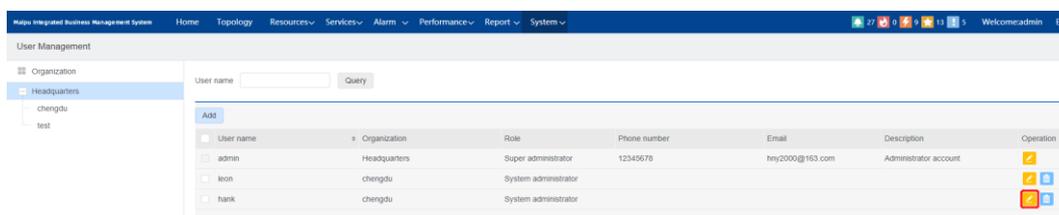


Figure 8-16 Modify the user

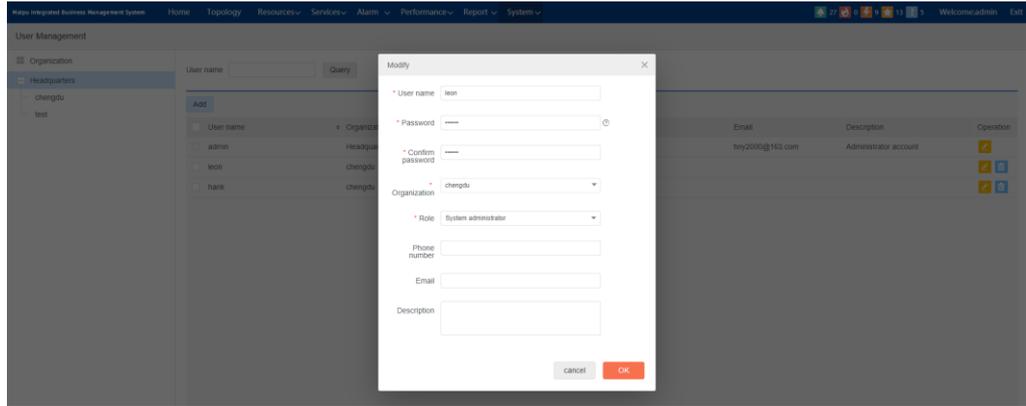


Figure 8-17 Modify the user

### Delete a user

Select the desired user, click , and the delete confirmation dialog box will pop up. Click "OK" to delete successfully. The system built-in user (admin) cannot be deleted.

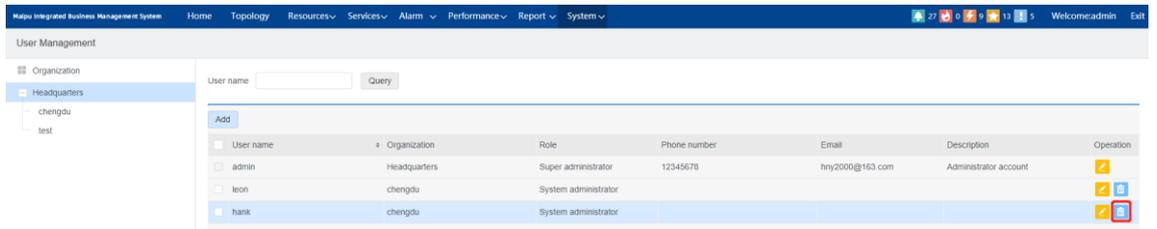


Figure 8-18 Delete a user

### Query the user

This page provides the query operation for the user, by inputting keywords in the query condition panel to perform the fuzzy query for the user name, as shown in the figure below:

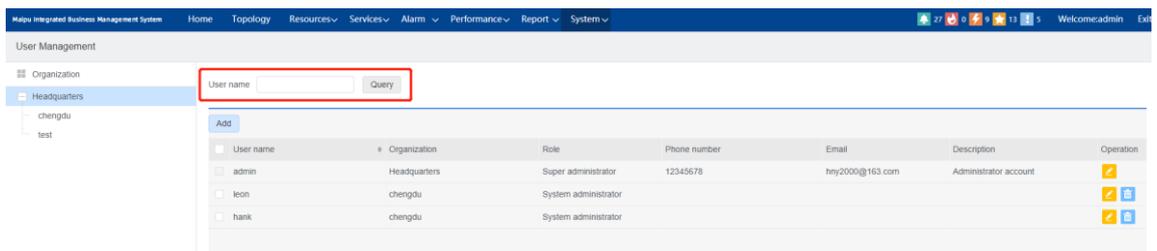


Figure 8-19 Query the user

## 8.4. System Setting

This module is mainly used to configure some basic data and configuration of the system, including license management, password policy configuration, SMS Gateway configuration, mailbox service configuration, Wechat configuration, superior network management configuration, and password modification.

### 8.4.1. License

The license is used to manage the license of each component of MIPO integrated network management. With this function, you can view the relevant license authorization information, machine code and other information, and import the license on this page.

Click “System” > “System Settings” > “License” in the menu bar to enter the license management interface.

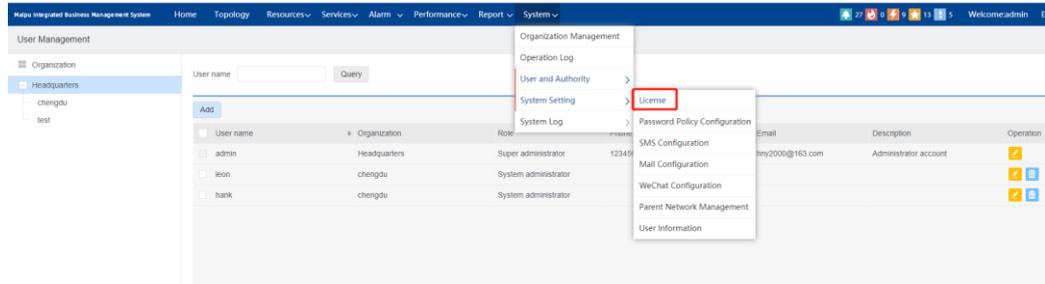
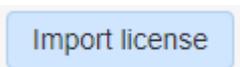


Figure 8-20 License management

All current licenses are displayed in the license list by default, including server address, module name, validity period, number of nodes, machine code and description

information. Click  to refresh the license list.

Click  to select the license file to import.

#### Caution

- The license file needs to be purchased from Maipu, and the license file is not carried in the system.

### 8.4.2. Password Policy Configuration

Password policy configuration is used to configure the complexity of user login password, the minimum length, whether to change the initial password, etc. The user password set by the administrator or the password modified by the user should meet the password policy configured by the password policy.

Click "System" -> "System Settings" -> "Password Policy Configuration" in the menu bar to enter the "Password Policy Configuration" page.

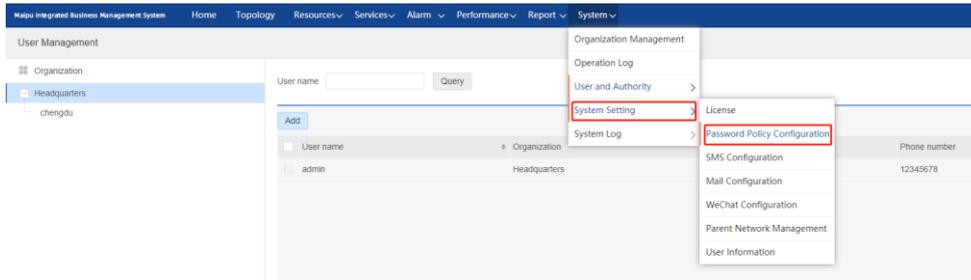


Figure 8-21 Password policy configuration

### 8.4.3. SMS Gateway Configuration

Maipu integrated network management platform supports the SMS function and SMS gateways such as "MIPO cat", "Tianyi cloud", "cloud MAS".

Before using SMS function, SMS Gateway should be set up first. Click "System" -> "System Settings" -> "SMS Gateway configuration" in the menu bar to enter the "SMS Gateway configuration" interface.

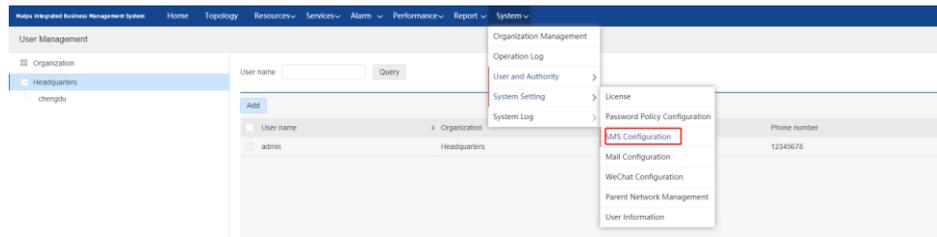


Figure 8-22 SMS gateway configuration

### Gateway Instance

Click the "Gateway Instance" button to enter the gateway instance section, which provides the operations of adding, modifying, deleting and querying gateway instances, as shown in the following figure:

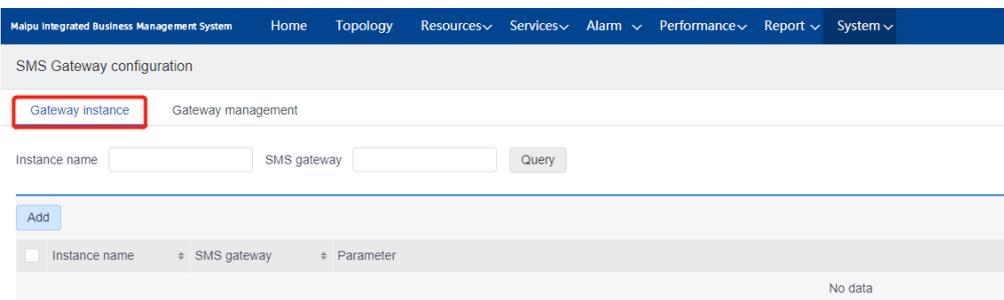


Figure 8-23 Gateway instance section

### Add a gateway instance

Click  to open the "Add gateway instance" dialog box, as shown below. Fill in the instance name and description, select the SMS gateway, and fill in the relevant

information of the selected SMS gateway to add a new gateway instance.

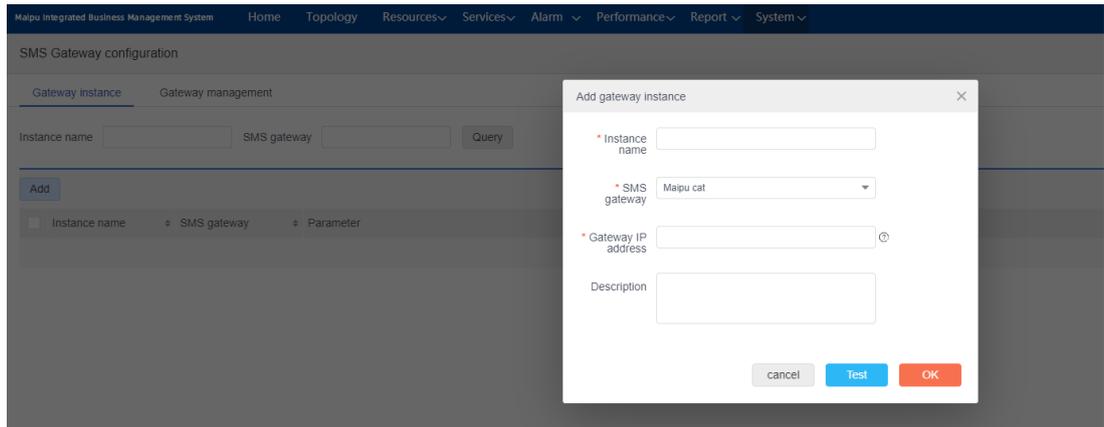


Figure 8-24 Add a gateway instance

To test whether the gateway configuration is correct, click the test button in the “Add” dialog box to send test messages. After clicking the test button, the test dialog box will pop up, as shown in the figure. Enter the test SMS receive number and test content, and click “OK”.

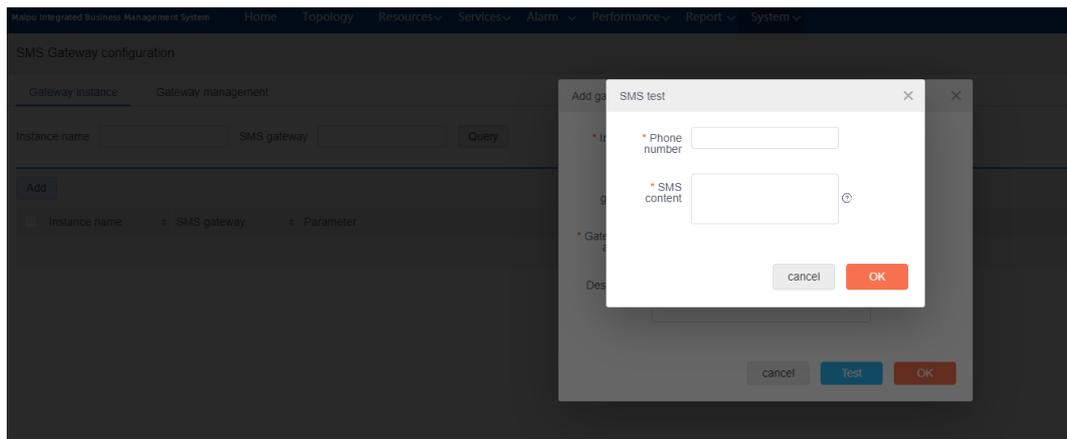


Figure 8-25 Send test SMS

## ! Caution

- The test SMS content format should conform to the SMS content template applied in SMS gateway. Otherwise, it will affect the receiving of test SMS.

### Modify a gateway instance:

Select the desired gateway instance in the gateway instance list, click  to open the “Edit gateway instance” dialog box (as shown in Figure 8-26). Modify the relevant configuration items according to the actual requirements, and click “OK”.

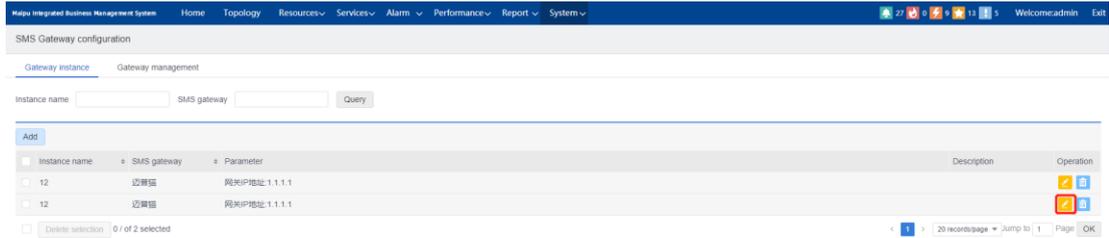


Figure 8-26 Edit the gateway instance

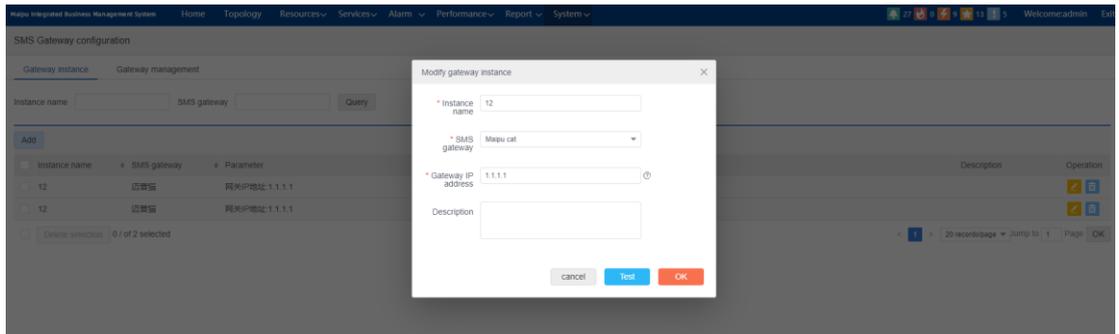


Figure 8-27 Modify the gateway instance

### Delete the gateway instance

Select the desired gateway instance in the gateway instance list, click **Delete** to open the prompt box for confirming deletion, and click "OK" to delete the gateway instance.

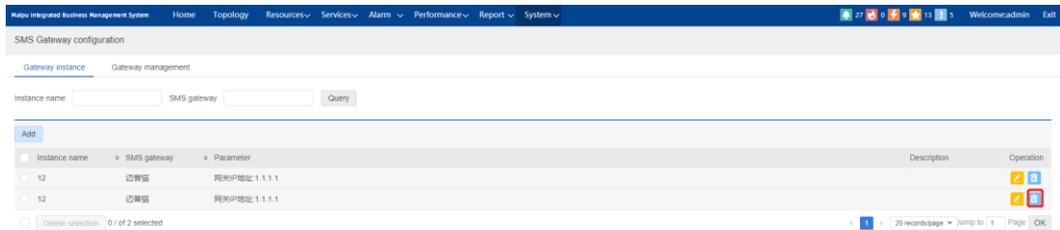


Figure 8-28 Delete the gateway instance

### Query the gateway instance:

This page provides the query operation for the gateway instance, as shown in the figure below. You can perform the fuzzy query for the gateway instances by "Instance name" and "SMS gateway".

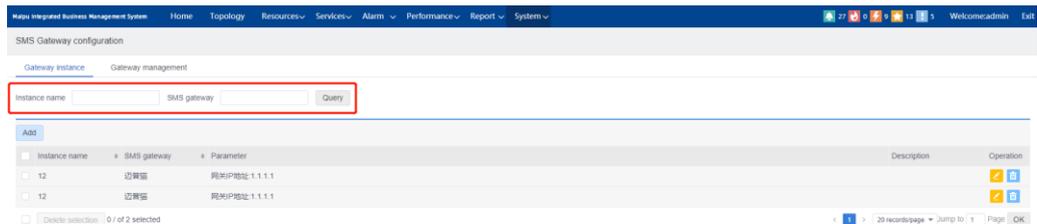


Figure 8-29 Query the gateway instance

## Gateway management

Click the "Gateway management" button to enter the gateway management section, as shown in the figure below, which provides the display and query functions of SMS gateway. Enter the name of SMS gateway to query the specified SMS gateway information.

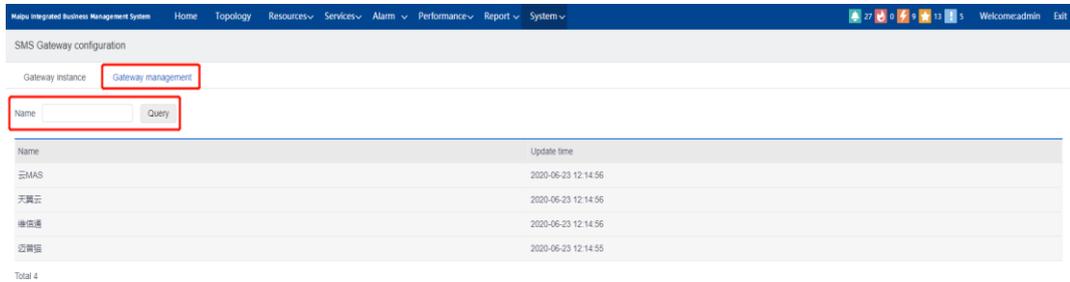


Figure 8-30 Gateway instance section

### 8.4.4. Email Service Configuration

Email sending is used for each component of MIPP integrated network management integration. Before using, it is necessary to configure relevant parameters of mail server, such as mail server address, mail server port, system sender email address, whether to enable authentication, authentication user name, authentication password, test recipient, etc.

Click "System" -> "System Settings" -> "Mail Service Configuration" in the menu bar to enter the "Mail Server Configuration" interface.

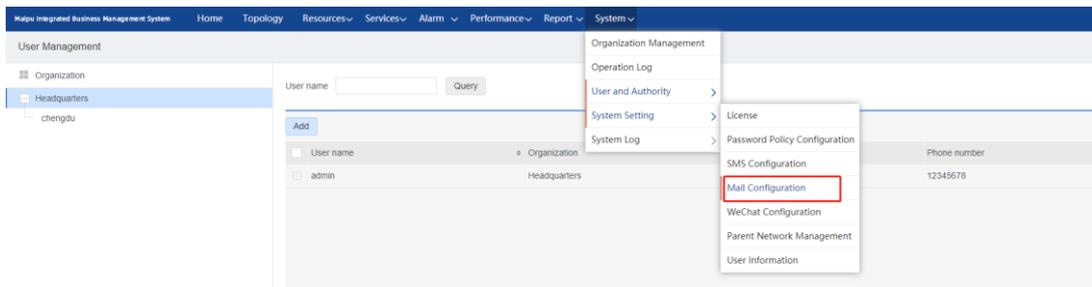


Figure 8-31 Email service setting menu

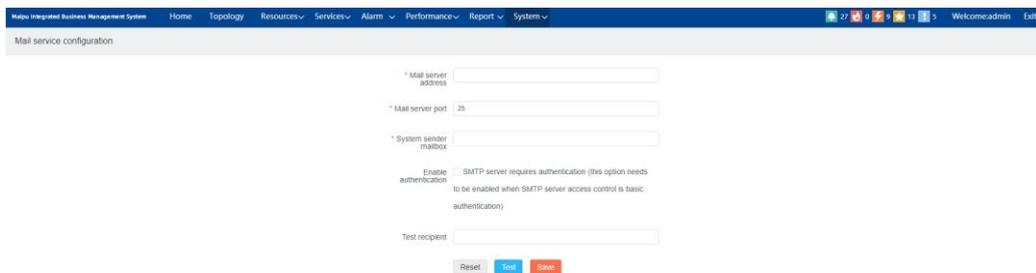


Figure 8-32 Email service setting interface

## Note

- The e-mail server address supports the configuration of domain name, and the DNS server or corresponding domain name resolution should be configured well when using the domain name.

### 8.4.5. Wechat Configuration

WeChat configuration module is used by WeChat official account management and binding system users to the concerned users of WeChat official account. Click "System" -> "System Settings" -> "Wechat Configuration" in the menu bar to enter the Wechat configuration interface.

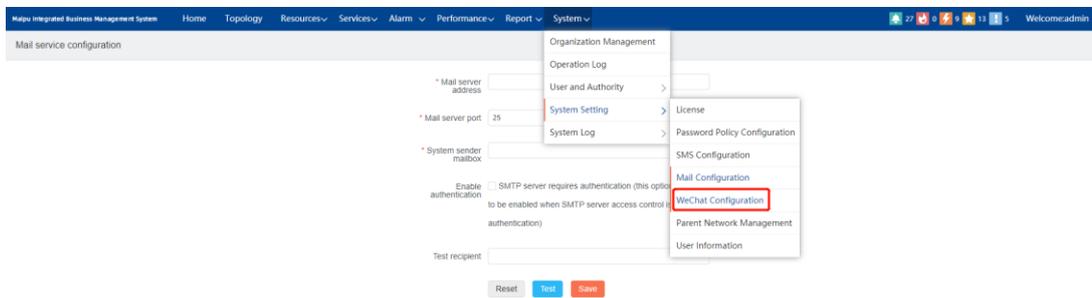


Figure 8-33 Wechat configuration menu

#### 9.4.5.1 Wechat Public Number Management

##### Add public number

Click  to open the official account dialog box, enter the public number name, official account number APPID, and APP SECRET, choose the organization to which the public number belongs and the public number type, and click the "OK" button, to add the public number.

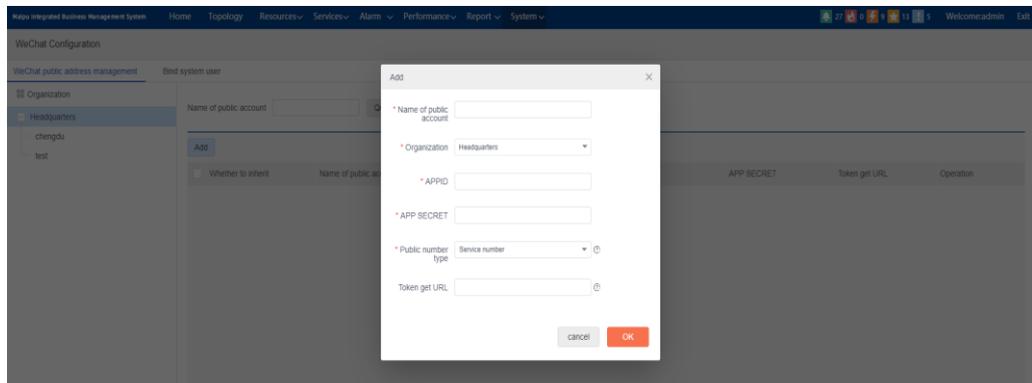


Figure 8-34 Add Wechat public number

## Caution

- The official account number APPID and APP SECRET need to be applied from WeChat, and WeChat will provide support and maintenance, which is independent of the system.
- By default, the token get URL is the token get URL provided by WeChat official account.
- To add WeChat official account, URL get token is required for accessibility judgment, so URL got by the accessible token is needed. Please ensure that the current server can communicate with the token get server fluently (by default, it is WeChat server api.weixin.qq . com).

## Reset Calling Times of Official Account Interface

The calling interface of the official account is not unlimited. To prevent the load abnormality caused by the program error of the official account, the calling interfaces of each official account cannot exceed the limit. When exceeding the limit, the interface calling will be wrong. If this happens, click  below to reset the calling times of the official account interface.



Figure 8-35 Wechat official account operation

## View QR Code of Official Account

The system provides the function of viewing the QR code of the official account. Click  in Figure 8-35, and you can see the two-dimensional code of the designated official account, scan the two-dimensional code, and follow the official account.

## Modify Official Account Information

Click  in Figure 8-36, open the dialog box of editing the official account, modify the relevant content as required, click the "OK" button to modify the official account information.

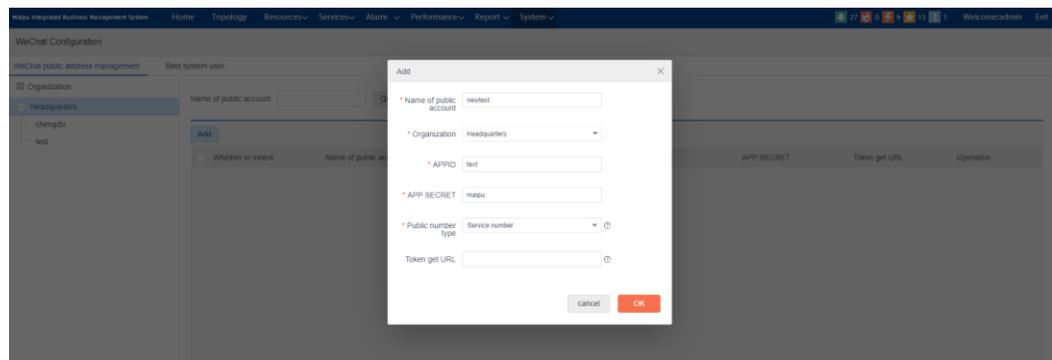


Figure 8-36 Modify the official account

## Delete Official Account

Click  in Figure 8-35, and you can delete the specified official account.

## Caution

- Deleting the official account will delete the user binding information under the official account.

### Query Official Account

Support querying the official account according to the name of the official account.



Figure 8-37 Query the official account

### 9.4.5.2 Bind System User

WeChat configuration module supports binding the system account and WeChat official account, and users can bind the system user to the designated follow account in the official account.

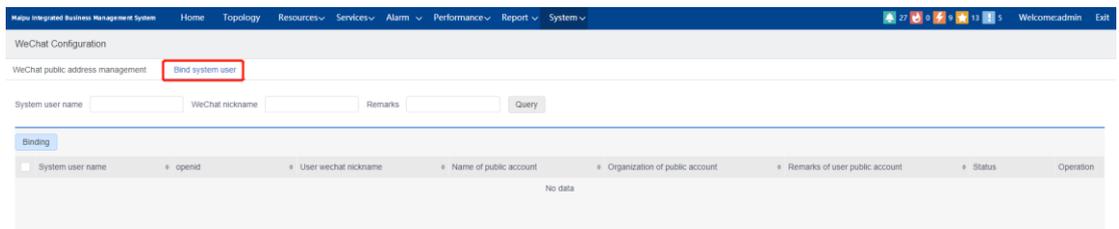
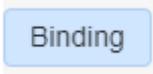


Figure 8-38 Bind the system user interface

### Bind System User

Click , select the system user and WeChat official account according to the organization, then select the WeChat user nickname to bind, click “OK”, as shown in Figure 8-39.

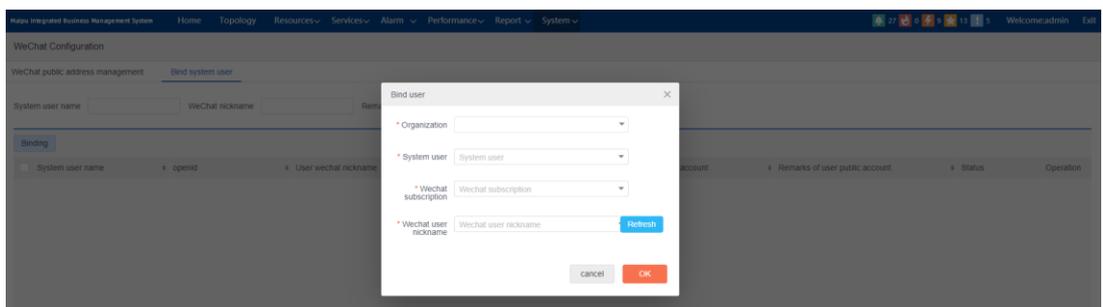


Figure 8-39 Bind the system user

### Unbind System User

Click  after the binding information to unbind the system user.

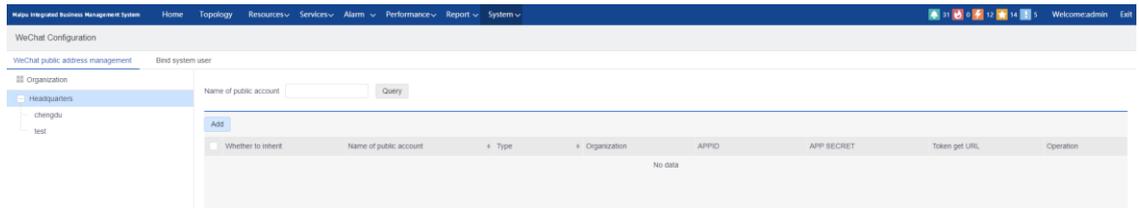


Figure 8-40 Unbind the system user

### Query Binding Information

The user can query the binding relationship according to the system user name, WeChat user nickname and official account name, as shown in Figure 8-41.

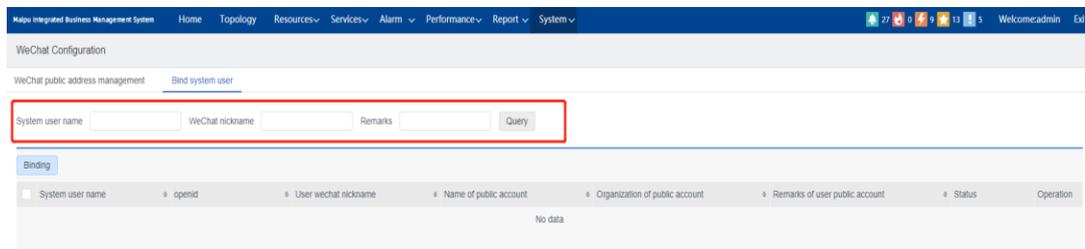


Figure 8-41 Query the binding information

### 8.4.6. Superior NMS Management

It is used to configure the scenario of hierarchical network management.

Click “System” > “System Settings” > “Superior NMS Configuration” in the menu bar to enter the interface of multi-level network management configuration, as shown in the figure below.

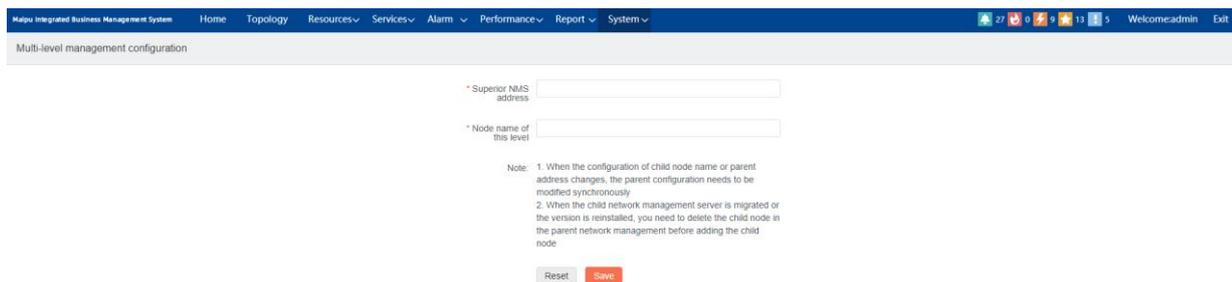
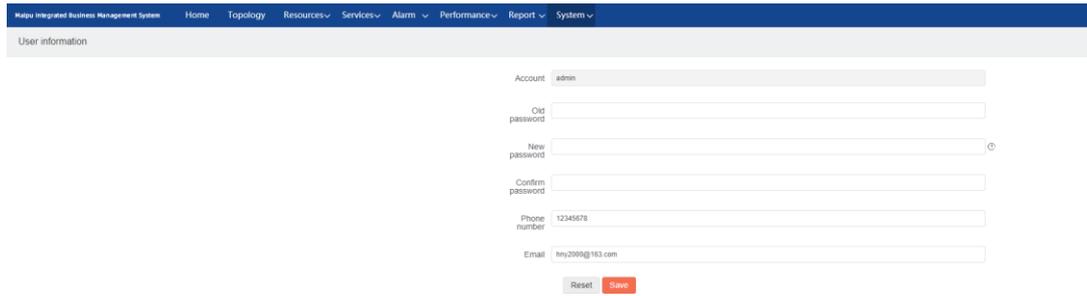


Figure 8-42 Superior NMS configuration

### 8.4.7. User Information

It is used to change the password of the current login user.

Click “System” > “System Management” > “User Information” to enter the interface of modifying the password, as shown below.



The screenshot shows a web interface for a user account. At the top, there is a navigation bar with the following items: Maipu Integrated Business Management System, Home, Topology, Resources, Services, Alarm, Performance, Report, and System. Below the navigation bar is a header section labeled "User information". The main content area contains a form with the following fields: Account (admin), Old password, New password, Confirm password, Phone number (12345678), and Email (my2000@163.com). At the bottom of the form, there are two buttons: "Reset" and "Save".

Figure 8-43 Modify the password

Input the old password, new password and confirm password on this page, click "Save" button to modify the password successfully, and click "Reset" button to clear the content of the current page. The new password needs to meet the password policy of the current system.

## 8.5. System Log Management

### 8.5.1. System Log Configuration

System log configuration is used to control the filtering type of system log. It allows the system to automatically de-duplicate the log.

There are four filtering types, described as follows:

- "Natural date + content": for the logs with the same content, only one log is recorded every day
- "Natural date + type": for the logs of the same type, only one log is recorded every day
- Time interval + content: within the set time interval, for the logs with the same content, only one log is recorded
- Time interval + type: within the set time interval, for the logs of the same type, only one log is recorded

Click "System" > "System Log Management" > "System Log Configuration" to enter the system log configuration interface, as shown below.

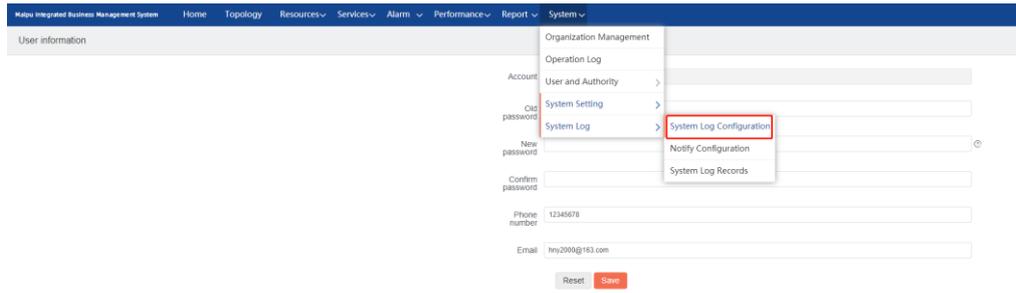


Figure 8-44 System log management

### Query the Log Configuration

This page provides the query operation of log configuration items, as shown in the figure below. You can filter and query through the "component name" and "log type" fields.

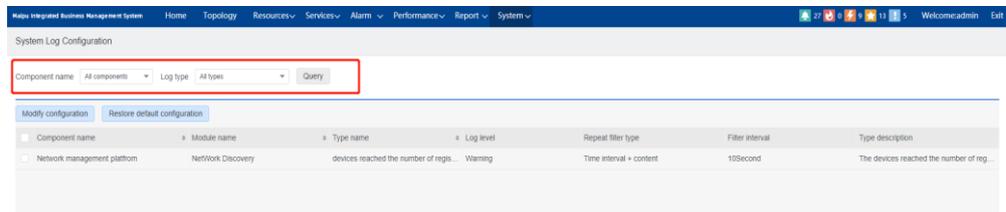


Figure 8-45 Query the system log configuration

### Modify System Log Configuration

Click **Modify configuration** to open the "System Log Filtering Configuration" dialog box, as shown in the following figure:

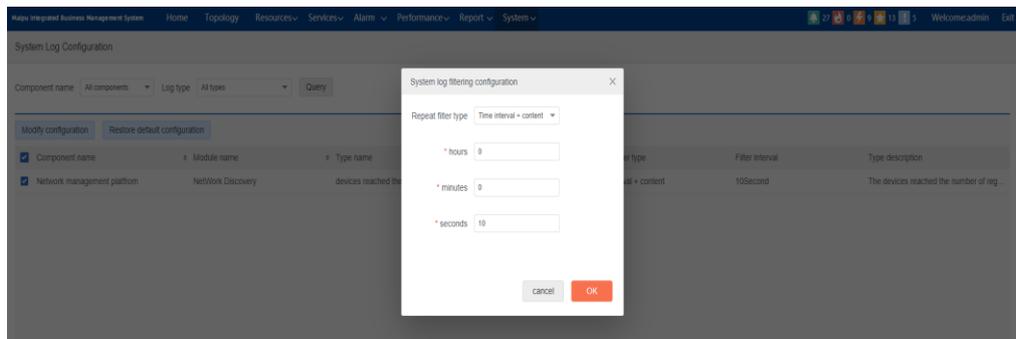


Figure 8-46 System log filtering configuration

### Restore Default Configuration

Click **Restore default configuration** to restore the system default configuration.

## 8.5.2. Log Notify Configuration

Log notification configuration can notify some qualified system logs, including email notification and SMS notification.

Click "System" > "System Log Management" > "Log Notification Configuration" to enter

the configuration interface, as shown in the figure below.

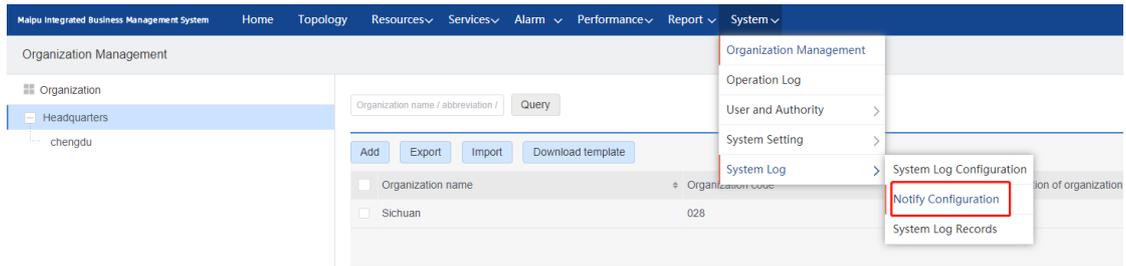


Figure 8-47 Log notify configuration

### Query Log Notify Configuration

This page provides the query operation of log notification configuration items, as shown in the figure below. You can filter and query through "component module", "log type", "log level" and keywords.

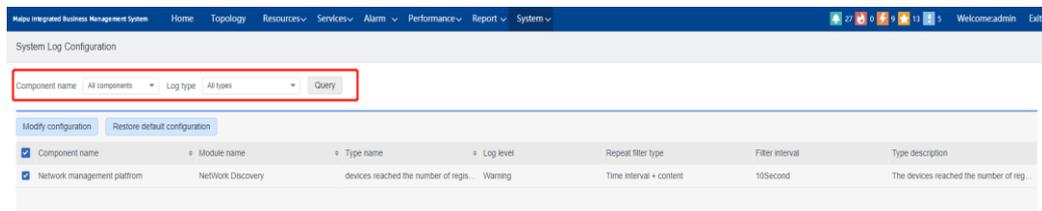


Figure 8-48 Query log notification configuration

### Add Log Notify Configuration

Click **Add** to open the "Add log notification configuration" dialog box, and you can add new log notification items, as shown in the figure below.

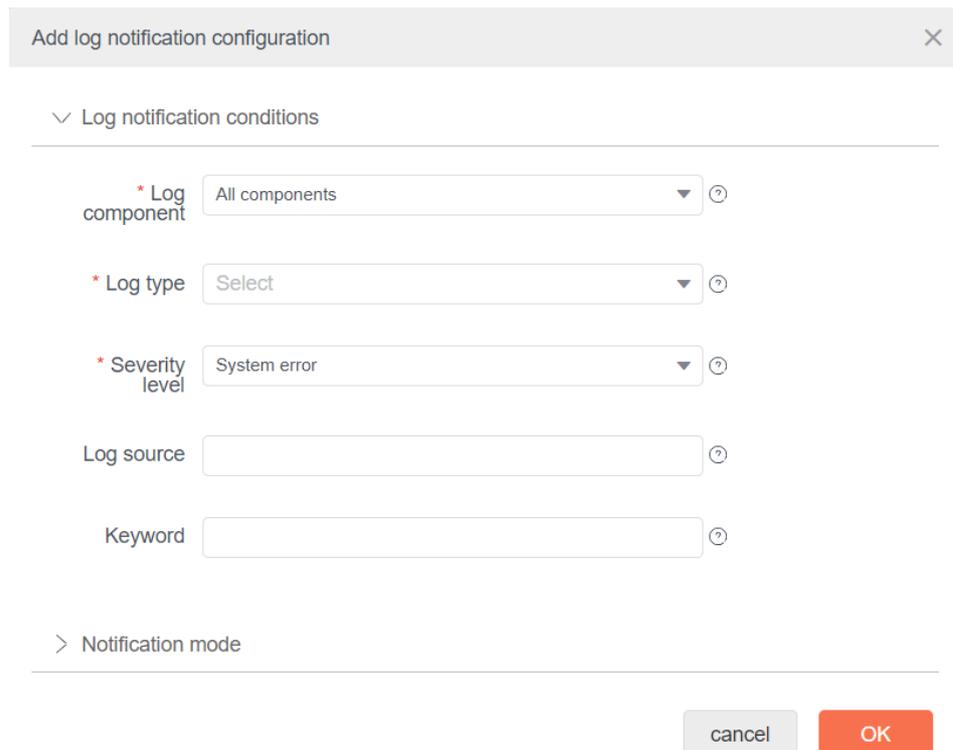


Figure 8-49 Add log notification configuration

### Modify Log Notification Configuration

Click  of the specified notification configuration to open the "Log notification configuration" dialog box to modify the selected organization configuration items, as shown in the figure below.

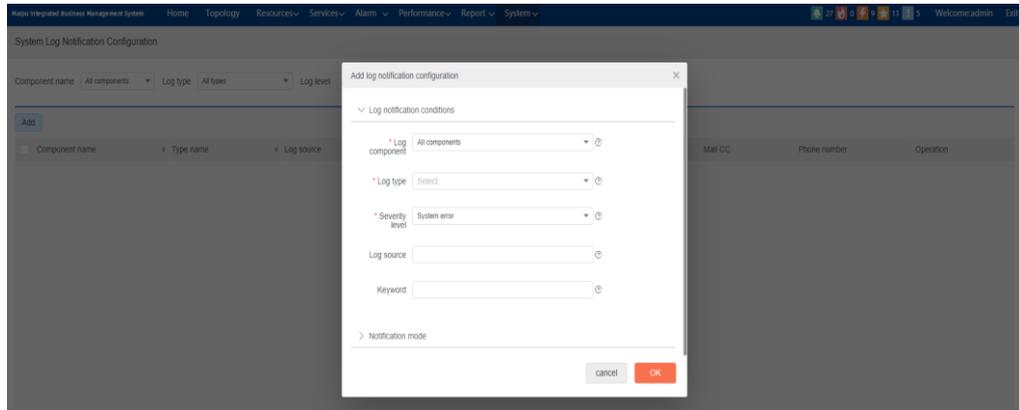


Figure 8-50 Modify the log notification configuration

### Delete Log Notification Configuration

Click , and you can delete the selected configuration item.

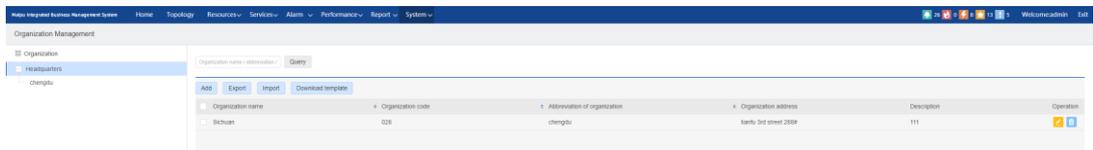


Figure 8-51 Delete the log notification configuration

## 8.5.3. System Log

You can view the list of all the system logs that have happened.

Click "System" > "System log management" > "System log" to enter the browsing interface, as shown in the figure below.

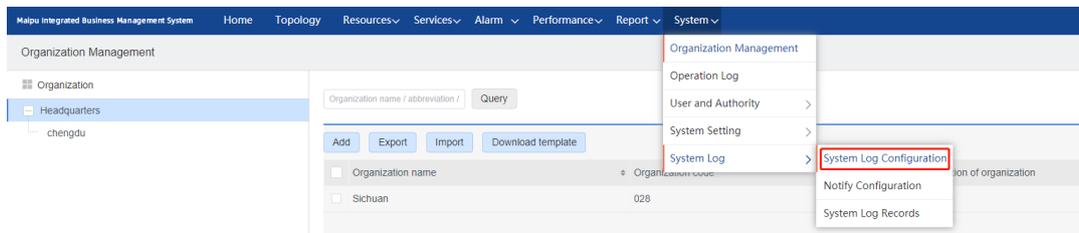


Figure 8-52 System logs

### Query System Logs

This page provides the filtering query of the system log, as shown in the figure below. You can filter and query through "component name", "type" and "advanced query".

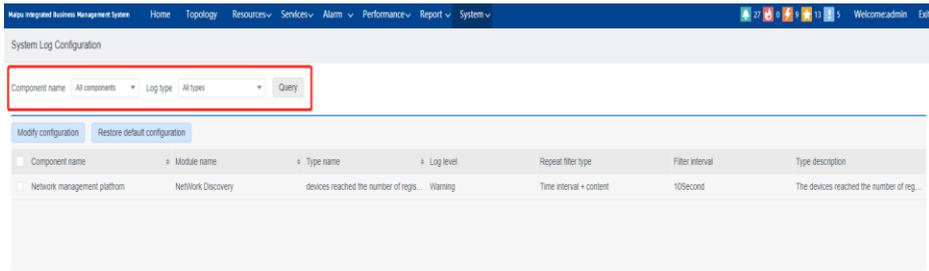


Figure 8-53 Query the system logs

# 9. Data Visualization

## 9.1. Home

After logging into the management system, the user enters the home page by default. In the home page, users can configure and view the data to be monitored. On the home page, there is already a "Basic network" data display page by default. The home page is as follows:

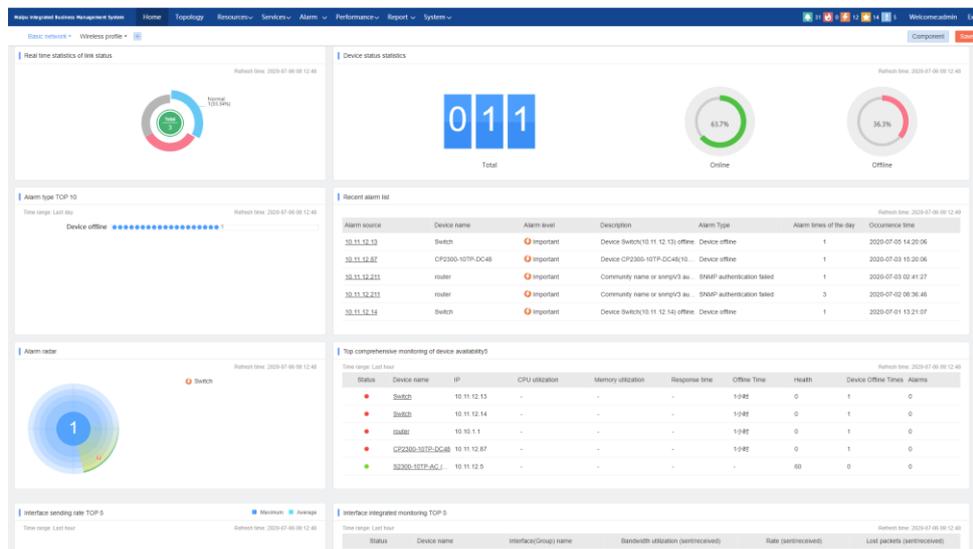


Figure 9-1 Home page

The functions on the home page are introduced in turn as follows:

### Add a Template

Users can add templates by clicking . The current templates are divided into blank templates and basic network, as shown in the figure below:

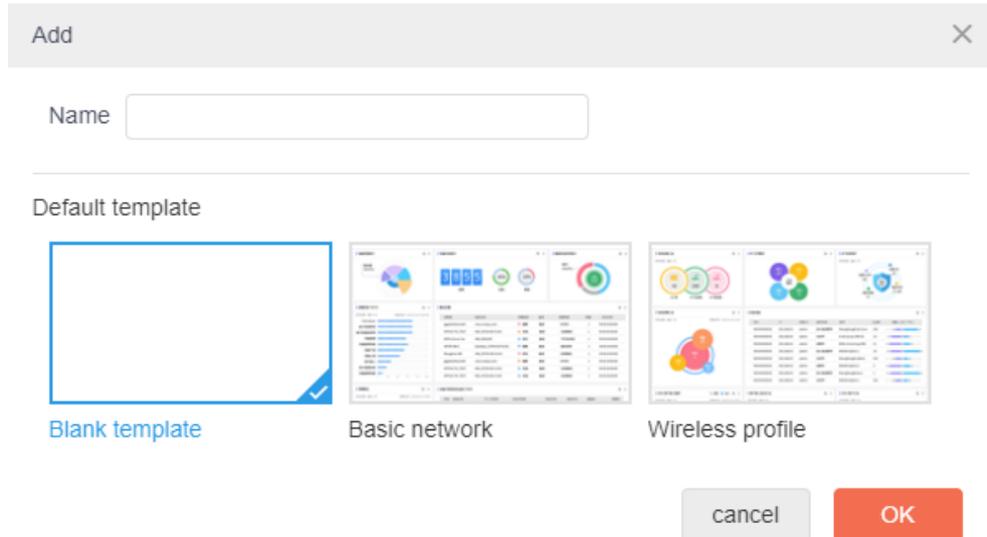


Figure 9-2 Add a template

The blank template does not contain any components. Users need to add components that need to be monitored to the template.

The basic network template already contains some basic network components, which can be directly used by users.

After the template is added successfully, you can click the drop-down button next to the template name to expand the template operation information. There are two types of template drop-down operation information. The default template (the system's own templates, including the basic network) has the function of restoring default, but not have the deletion function; the customized template (the template added by the user) does not have the function of restoring the default, but have the deletion function, as shown in the following figure:

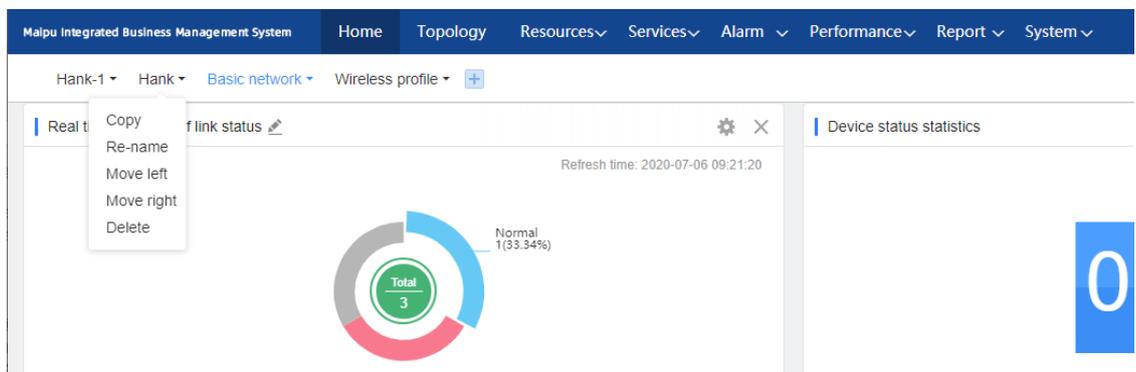


Figure 9-3 Edit a template

### Copy the template

Click "Copy" in the above figure to pop up a pop-up layer containing the name input box. After entering the name, click "OK" to copy the current template content to the new

template.

### **Rename the template**

Click "Rename" in Figure 9-3, and the template name will be displayed in an editable state. After the user re-edits the template name, the input box will lose focus and the edited content can be saved.

### **Move the template left and right**

Click "Move left" or "Move right" as shown in Figure 9-3, and the template name will move left or right.

### **Restore the default template**

Click "Restore default" as shown in Figure 9-3. Click "OK" to restore the default according to the prompt, and the template will return to the default state, that is, the state before user configuration.

### **Delete the template**

Click "Delete " in Figure 9-3, and click "OK" according to the prompt to delete the template added by the user.

### **Save the template**

Click  in the top right corner of the home page to save all the information in the template.

### **Add a component**

Click  on the top right corner of the home page, a pop-up layer appears, which contains all the components in the system. Click  next to the component to add the component to the home page. At the same time, "+1" will appear next to the component to indicate that a component has been added to the current template. If you continue to add this component, the number changes to "+2.". The components are added as follows:

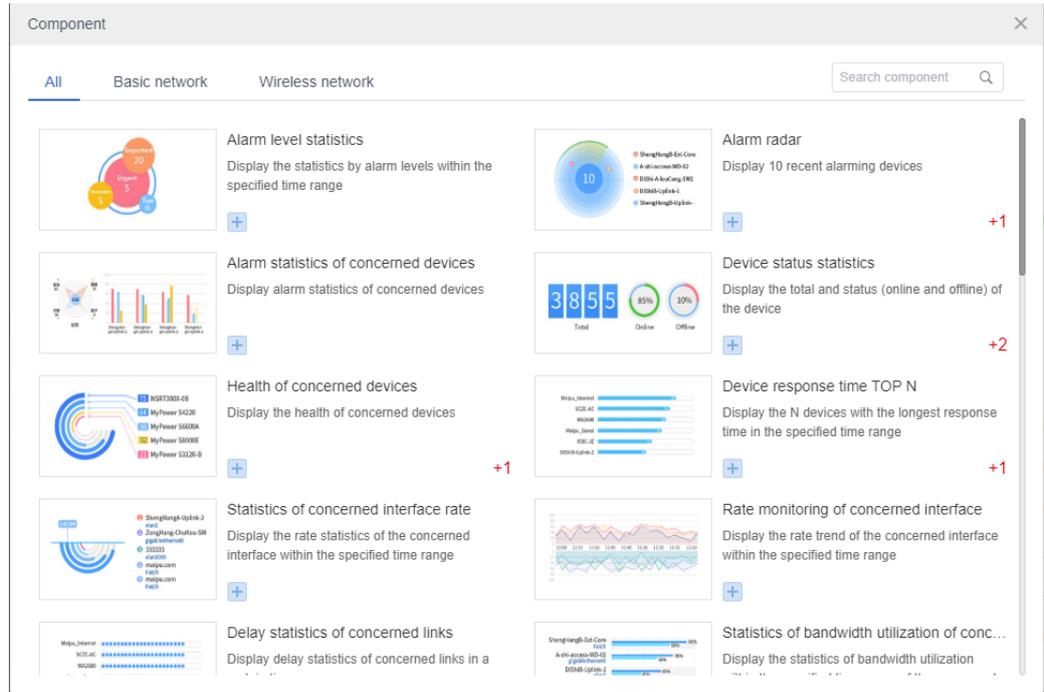


Figure 9-4 Component list

**Configure the component**

When a component is selected to the page, there is generally no data. You need to click  in the upper right corner of the component to configure the component, and then the data can be displayed according to the configuration conditions. Each component has different configuration conditions according to its characteristics. The configuration method of each configuration condition is introduced with "Alarm device TOP N". The configuration interface is shown in the following figure:

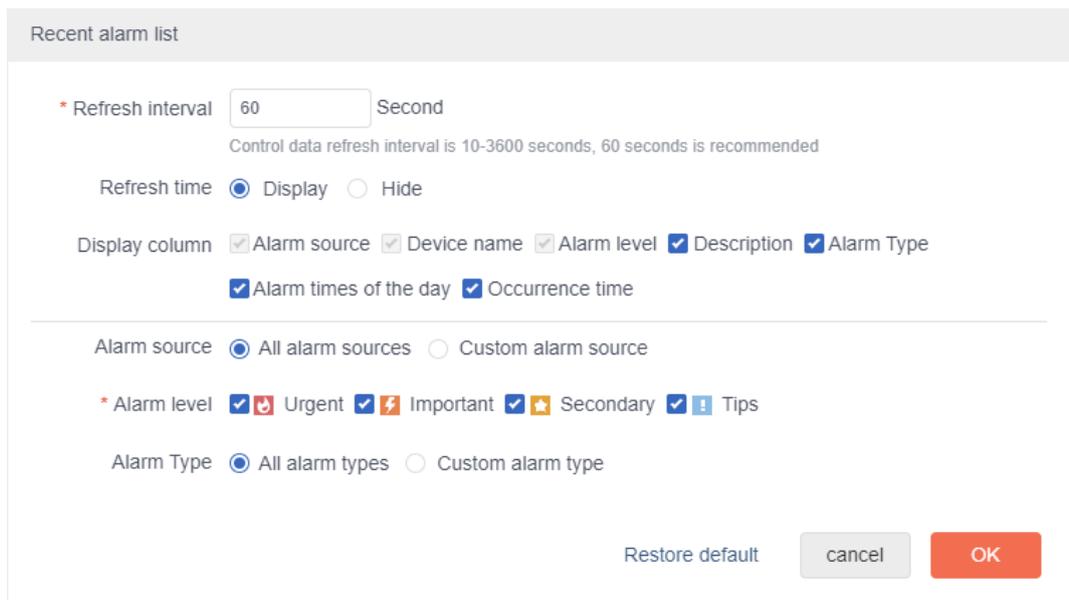


Figure 9-5 TOPN configuration of the alarm device

**Time range:** Select the time range to be monitored through the drop-down box. The range you can select includes the last day, the last week, the last month, and the last March. For some controls, you can also select the last hour.

**TOP N:** The TOPN control can set how much data to display by configuring TOP N. The optional values are 5, 10, 15 and 20, and 5 is displayed by default.

**Refresh interval:** each control can configure the refresh interval to control the interval of refreshing the component data.

**Refresh time:** Select "Display" or "Hide", and you can configure the time range and refresh time display or hide in the component.

The above is the common configuration of components. Each component has its own configuration items. Please follow the prompts to configure the unique configuration items.

For more detailed configuration of all components, please refer to the "Components" section.

### Edit the component name

Click  in the upper left corner of the component to enter the editing state. After the component name is edited, the edit box loses focus and the editing is completed.

### Remove the component

Click  in the upper right corner of the component to prompt the deletion of the component. Operate according to the prompt.

### Component Tooltips

For the components on the home page, you can view the tooltips of the chart by placing the mouse on the component diagram, and the tooltips will display more detailed information of the chart, as shown in the figure below:

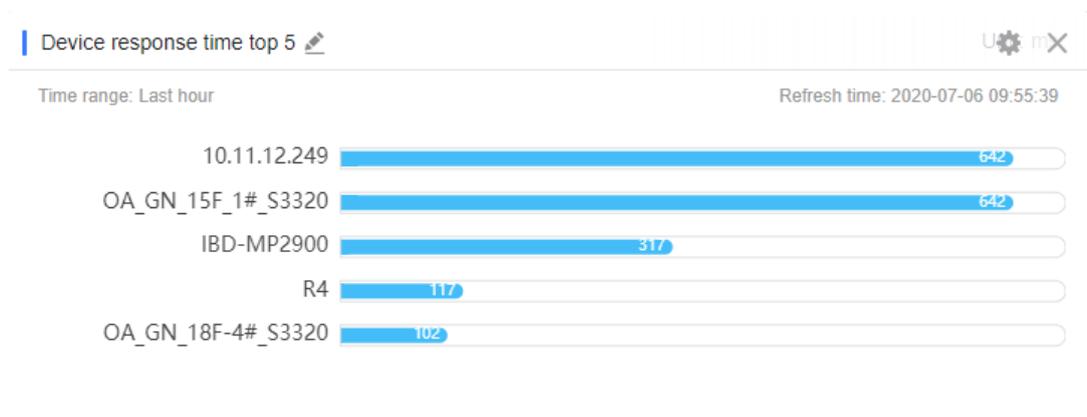


Figure 9-6 Device response time TOPN

### Hyperlink jump

If a hand shape is displayed after putting the mouse on the legend or name of each component in the home page, it means that this part can be clicked to jump to the corresponding device, interface or other pages, as shown in the following figure:

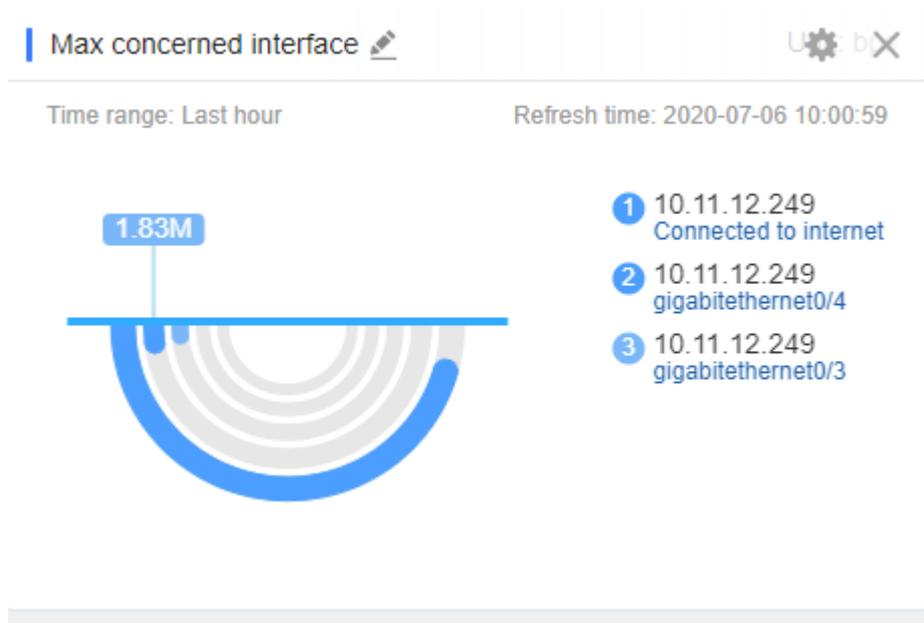


Figure 9-7 Legend jump

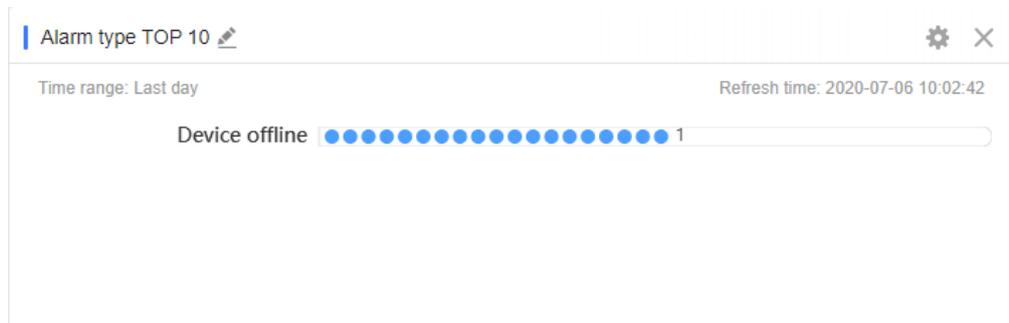


Figure 9-8 Name jump

Alarm source	Device name	Alarm level	Description	Alarm Type	Alarm times of the day	Occurrence time
10.11.12.5	S2300-10TP-AC (E1)	Secondary	link (Name:1, source Device/Ip:S...	Link check failed	161	2020-06-24 11:40:00
10.11.12.13	Switch	Tips	Device Switch(10.11.12.13) SN...	SNMP un-accessible	1	2020-06-09 03:04:21
10.11.12.87	CP2300-10TP-DC48	Tips	Device CP2300-10TP-DC48(10...	SNMP un-accessible	1	2020-05-27 06:16:21
10.10.1.1	router	Tips	Device router(10.10.1.1) SNMP ...	SNMP un-accessible	1	2020-05-27 03:02:21
10.10.1.1	router	Secondary	Line protocol on interface fastcel...	Interface link protocol UP	1	2020-05-25 08:35:15

Figure 9-9 List jump

## 9.2. Big Screen

Click "Services" > "Big Screen" to enter the big screen page, as shown in the following

figure:

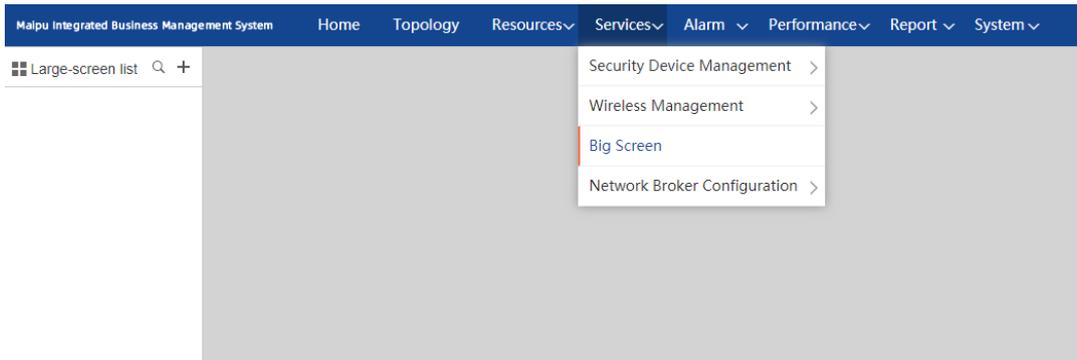


Figure 9-10 Big screen

The following will introduce the functions of the big screen from left to right:

### Add a big screen

The big screen page does not have any big screen items initially. The user needs to manually click **+** in the upper left corner of the page. After clicking the “Add” button, a pop-up window as shown in the following figure will appear:

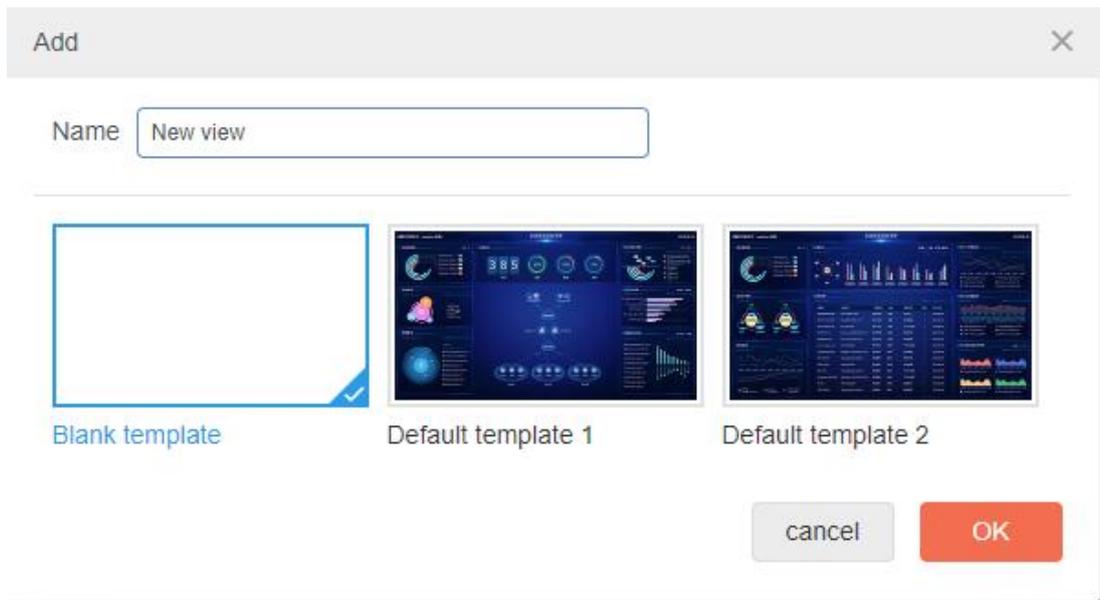


Figure 9-11 Add a big screen

In the pop-up window of adding a big screen, there are three kinds of templates to choose: blank template and default template 1 and 2 with default components configured. Users can choose according to their own needs. Now, take adding default template 1 as an example, and the page after adding is as follows:

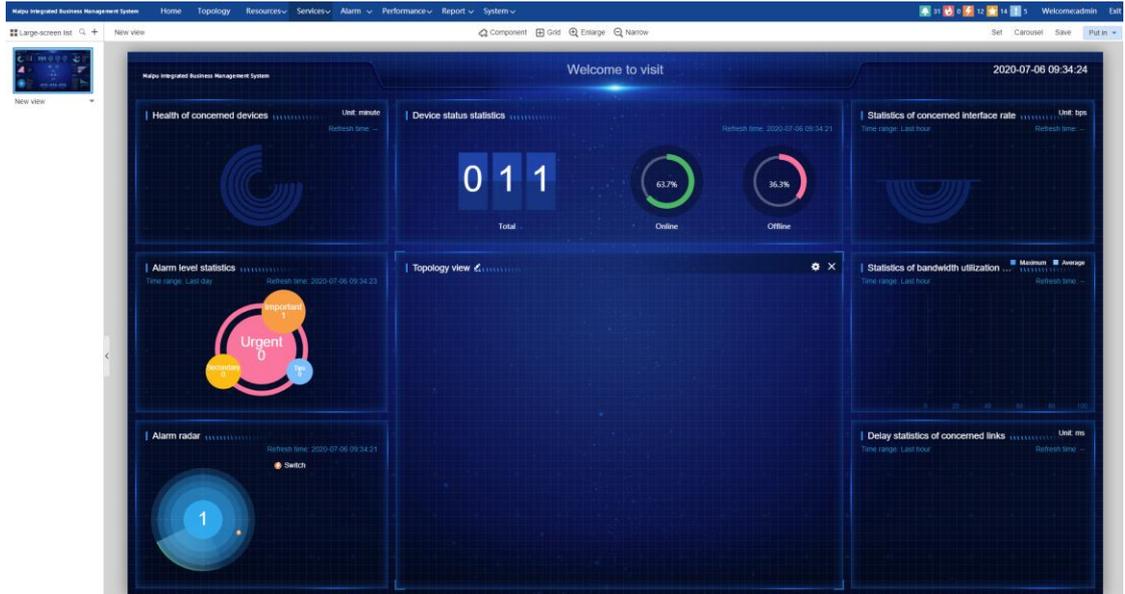


Figure 9-12 Big screen display

### Edit a big screen

All new big screens will appear in the big screen list on the left side of the page. Click the drop-down button ▼ next to the big screen name to expand the operation items for editing big screen information, as shown in the following figure:

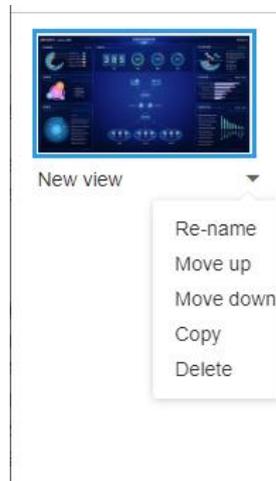


Figure 9-13 Edit the big screen

Similar to edit the template in the home page, click each operation item and operate according to the prompt to complete the editing of the big screen.

### Search for big screen

Click 🔍 on the left side of the page, and the search box will appear in the big screen list. Enter the keyword of the big screen name in the search box to search for the big screen to be queried, as shown in the following figure:

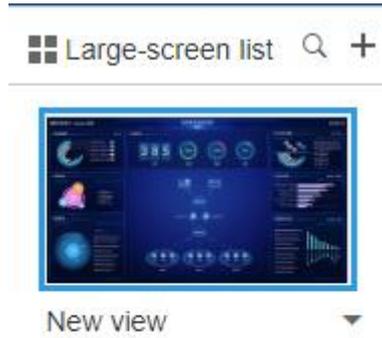


Figure 9-14 Search for the big screen

### Add a component

Click  **Component** at the bottom of the menu bar of the page to pop up the pop-up layer of adding a component. The pop-up layer is basically the same as that of adding a component in the home page. Please refer to the "Configure the component" section of the home page for specific operations. Please refer to the "Components" section for the configuration of all components.

### Grid

When creating a big screen, in order to facilitate the layout of the component location, the grid is opened by default. Click  **Grid** below the menu bar to close and open the grid. The interface of configuring the big screen after closing the grid is shown in the following figure:

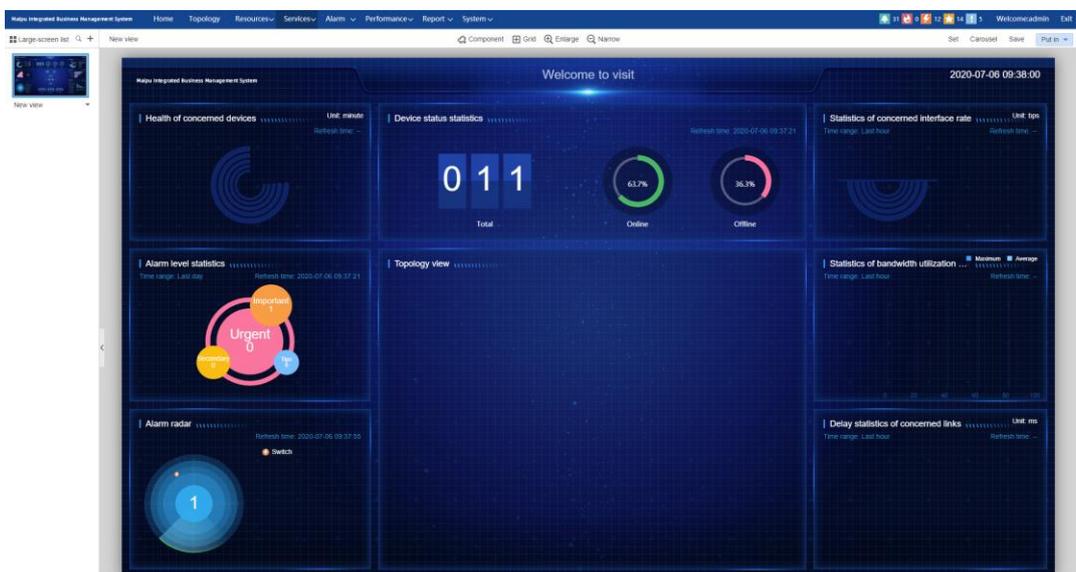


Figure 9-15 Big screen grid

### Enlarge and Narrow the big screen

In the big screen configuration interface, in order to view the overall layout of the big screen, the big screen view page is narrowed to 59% of the original size by default. After zooming out, the contents of the components may not be clearly seen. At this time, you can easily check the details of the components and whether the overall layout is beautiful with the help of the zoom-in and zoom-out functions.

### Setting

Click the “Set” button in the upper right corner of the big screen page to set the view size and screen matrix, as shown in the following figure:

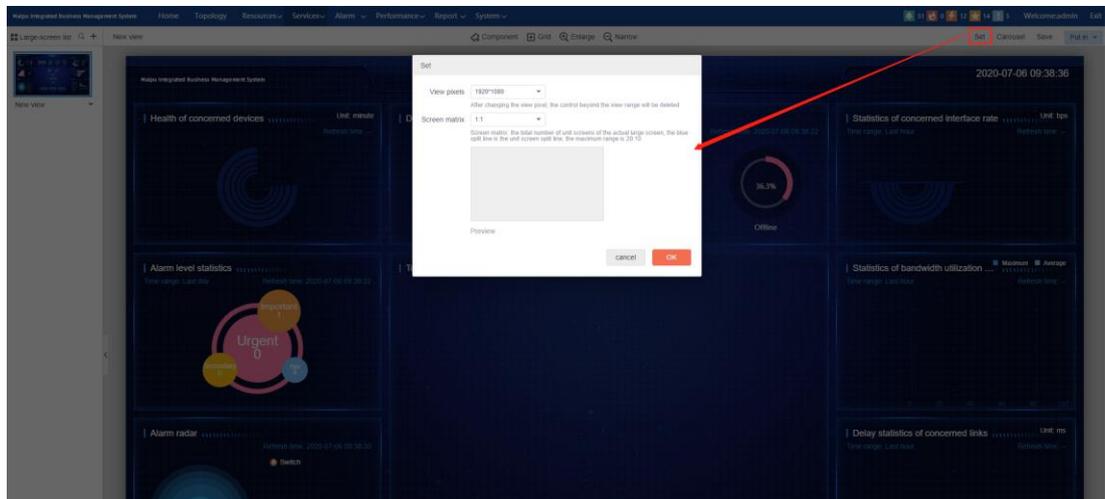


Figure 9-16 Big screen setting

For the view pixels, you can choose the default pixels, or you can customize the settings. It should be noted that when the newly set view pixels cannot accommodate all the existing components, the components beyond the view range will be deleted. As shown in Figure 9-17, the translucent components beyond the view will be deleted after the view pixels are set.

The screen matrix is mainly used to preview the big screen configuration effect of the splicing screen. For the screen matrix, you can choose the ratio given by default, or it can be customized. The maximum range of custom setting is 20:10. When setting the screen matrix, you can see the effect of the configuration in the preview below.

### Carousel

Click the “Carousel” button in the upper right corner of the big screen page to add the carousel page through the pop-up window, as shown in the following figure:

Carousel ×

\* Carousel name

\* Carousel interface  ▼  
It is recommended to select a large screen with the same resolution in the same carousel. Otherwise, the display will be abnormal

\* Carousel mode  ▼

\* Carousel interval  Second  
The duration of carousel interval is 10-180 seconds, 10 seconds is recommended

---

Carousel list

Carousel name	Carousel interface	Carousel mode	Carousel interval	Operation
No data				

Figure 9-17 Add the big screen carousel

On the carousel page, the configured large screen views can be checked through the drop-down box. For the selected big screen views, ensure that its resolution is the same. Otherwise, abnormal display may occur.

The carousel mode is divided into move left, right, up and down, and users can choose according to their own needs.

After the name and interval of the carousel are configured, click the “Add” button to add the configured carousel to the carousel list for later selection.

## Saving

After the big screen view is configured, click the “Save” button to save the view configuration in time to prevent the configuration from losing due to some reasons. If the user's big screen configuration item is changed, but not saved in time, when the user leaves the big screen configuration page, the system will pop up a prompt asking whether to save the view data before leaving, as shown in the following figure:



Figure 9-18 Saving prompt

## Launch

Click the “Put in” button in the upper right corner of the page to release the view of this page by default. If you click the drop-down button next to the “Put in” button, you can select the view list or the carousel list to launch in the expanded information, as shown in the following figure:



Figure 9-19 Big screen launching

## 9.3. Components

The component is mainly used to show the changes of network parameters monitored by users.

Adding a component has been specifically introduced in the home page and the big screen, so there is no need to repeat in this section. This section mainly introduces the configuration method and display effect of all components in the system.

As the control configuration interfaces in the home page and the large screen are exactly the same, and the display effect is only different in color, so this section only introduces the component configuration and display effect in the home page.

### 9.3.1. Basic Network

#### 9.3.1.1. Concerned Interface Rate Monitoring

This component is used to display the rate trend of the concerned interface within a specified time range.

#### Display Effect



Figure 9-20 Rate monitoring of the concerned interface

Depending on the number of interfaces configured, the component presents two effects as shown in Figure 9-21. When the number of selected interfaces exceeds 3, they will be displayed in the upper and lower columns as shown in the left figure; when the number of interfaces is less than or equal to 3, it will be displayed as shown in the right figure.

The legend of the component is located at the bottom of the diagram. Each legend has two lines, the top black font is the device name, and the bottom blue font is the interface name. If you select an interface group, the legend displays only the name of the interface group.

### Configuration Method

The component configuration interface is shown in the following figure:

×
Statistics of concerned interface rate

Time range Last hour ▾

Flow direction  Send  Receive

Refresh interval 5 minutes ▾

Refresh time  Display  Hide

Way of value selection Maximum ▾

Interface
Interface Group

Up to 5 interfaces can be selected: 3/5

☐	Status	Name	Device name	Device IP	Interface IP	Description	Type	↕	Operation
☐	●	Conn...	10.11.12.249	10.11.12....		###connec...	Interface		Delete
☐	●	gigab...	10.11.12.249	10.11.12....		###connec...	Interface		Delete
☐	●	gigab...	10.11.12.249	10.11.12....			Interface		Delete

☐ Delete selection 0 / of 3 selected

Restore default
cancel
OK

Figure 9-21 Rate monitoring configuration of the concerned interface

**Time range:** One of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month, and the last three months;

**Flow direction:** There are two flow directions, that is, send and receive. After selecting, the title in the component display effect will change with the user's choice, and the number of statistics will also change.

**Refresh interval:** The refresh interval can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to display and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Interface and interface group:** Only 6 pieces of data can be selected at most. The interface for selecting the interface and interface group is as follows:

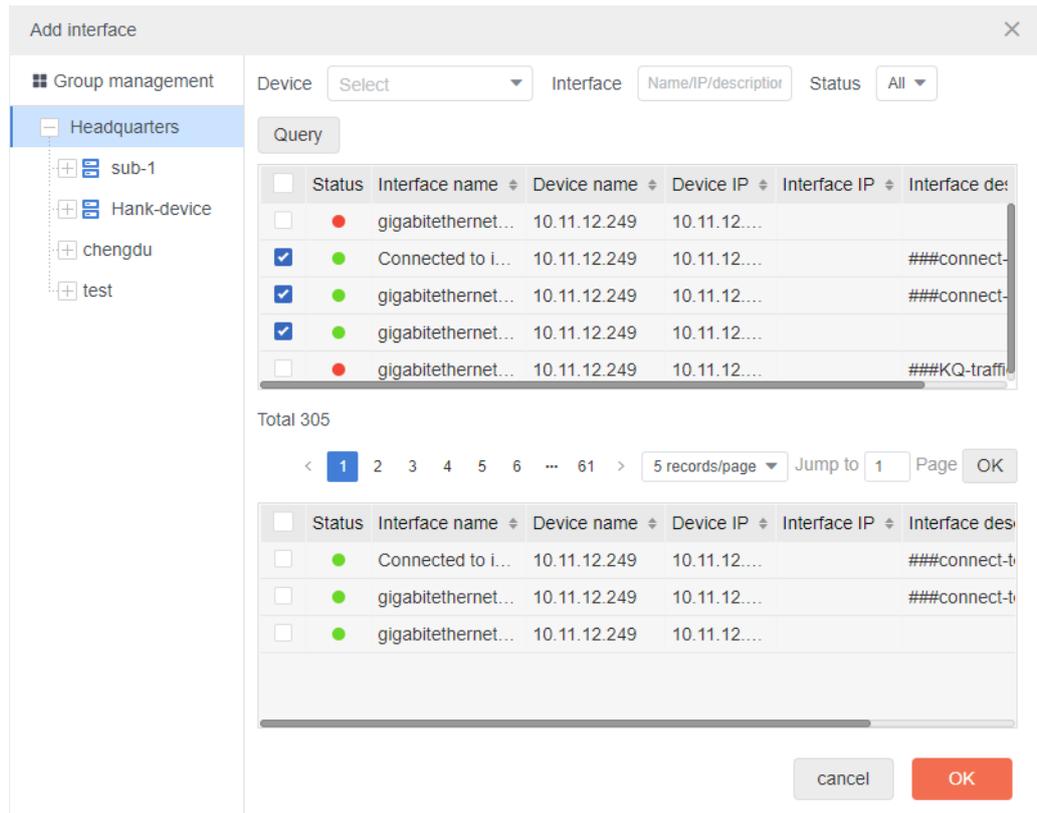


Figure 9-22 Select the interface

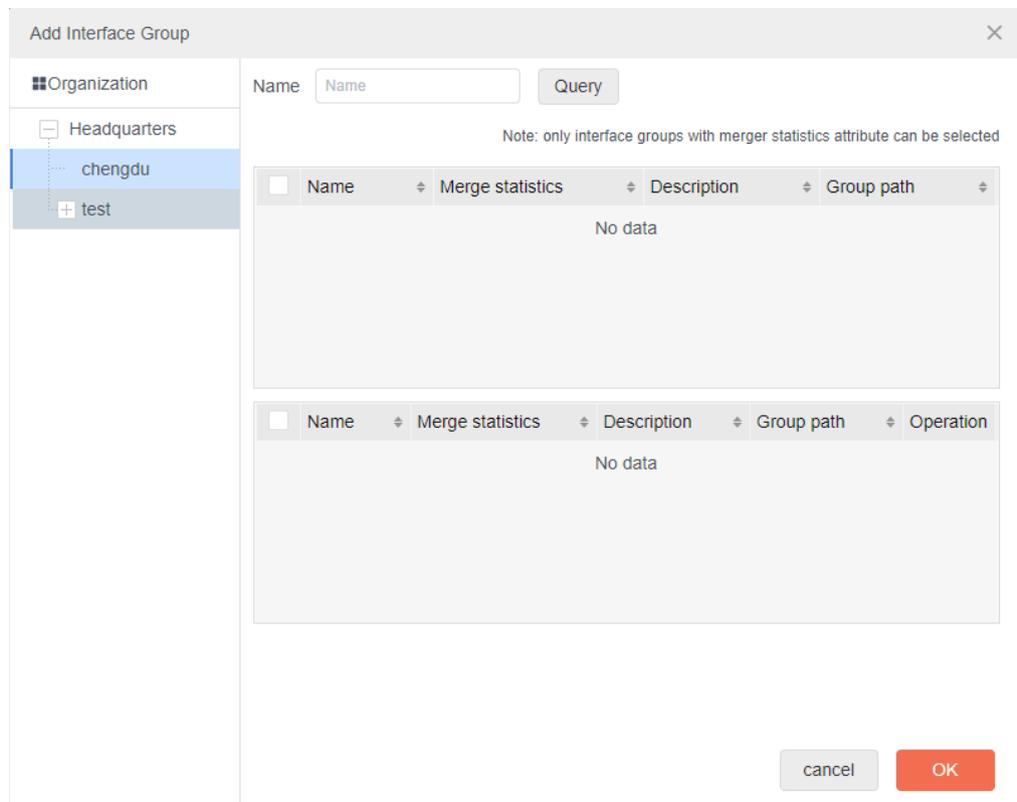


Figure 9-23 Select the interface group

### 9.3.1.2. Rate Statistics of Concerned Interface

This component is used to display the rate statistics of the concerned interface within the specified time range.

#### Display Effect

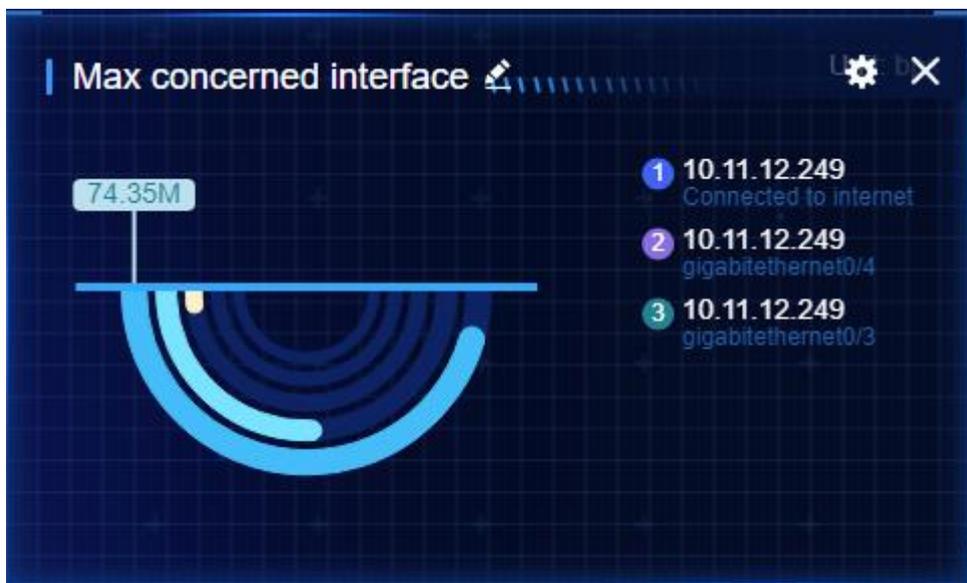


Figure 9-24 Rate statistics of the concerned interface

The display effect of the component is shown in the figure above. The title can be changed according to different configuration items. This component can display the rate statistics data of up to five interfaces/interface groups, and the statistical data values will be displayed one by one.

Move the mouse to the chart to display the details, but only on the home page, and there is no such prompt in the big screen.

The component legend is located on the right side of the chart. Each legend has two lines. The black font on the top is the device name, and the blue font at the bottom is the interface name. If it is an interface group, the legend displays only the name of the interface group. You can click the legend to jump to the monitoring data details page.

#### Configuration Method

The component configuration interface is shown in the following figure:

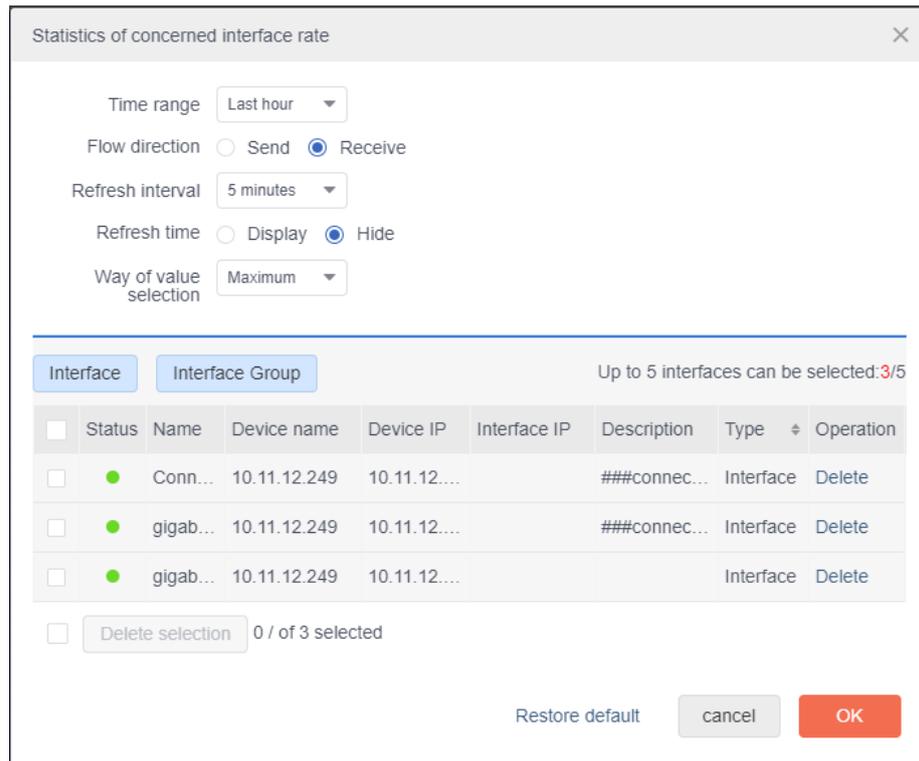


Figure 9-25 Rate statistics configuration interface of the concerned interface

**Time range:** One of five time periods can be selected from the drop-down box to count the change of data. The five time periods are, the last hour, the last day, the last week, the last month, and the last three months;

**Flow direction:** It can be divided into send and receive. After the selection, the title in the component display effect will change with the user's choice, and the number of statistics will also change.

**Refresh interval:** It can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Way of value selection:** the maximum and average can be selected from the drop-down box. After selecting, the title in the component display effect will change with the user's choice, and the number of statistics will also change.

**Interface and Interface Group:** at most 5 pieces of data can be selected, and they are required. The interfaces for selecting interface and interface group are shown in the following figure:

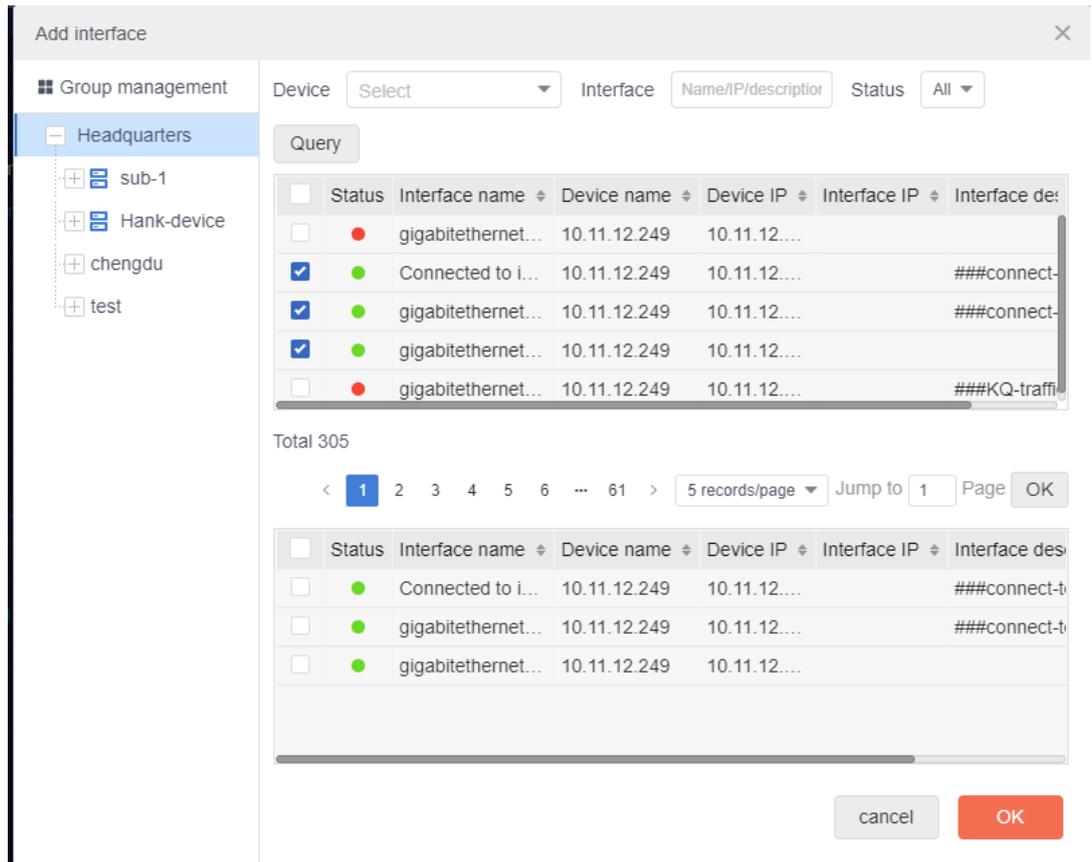


Figure 9-26 Select the interface

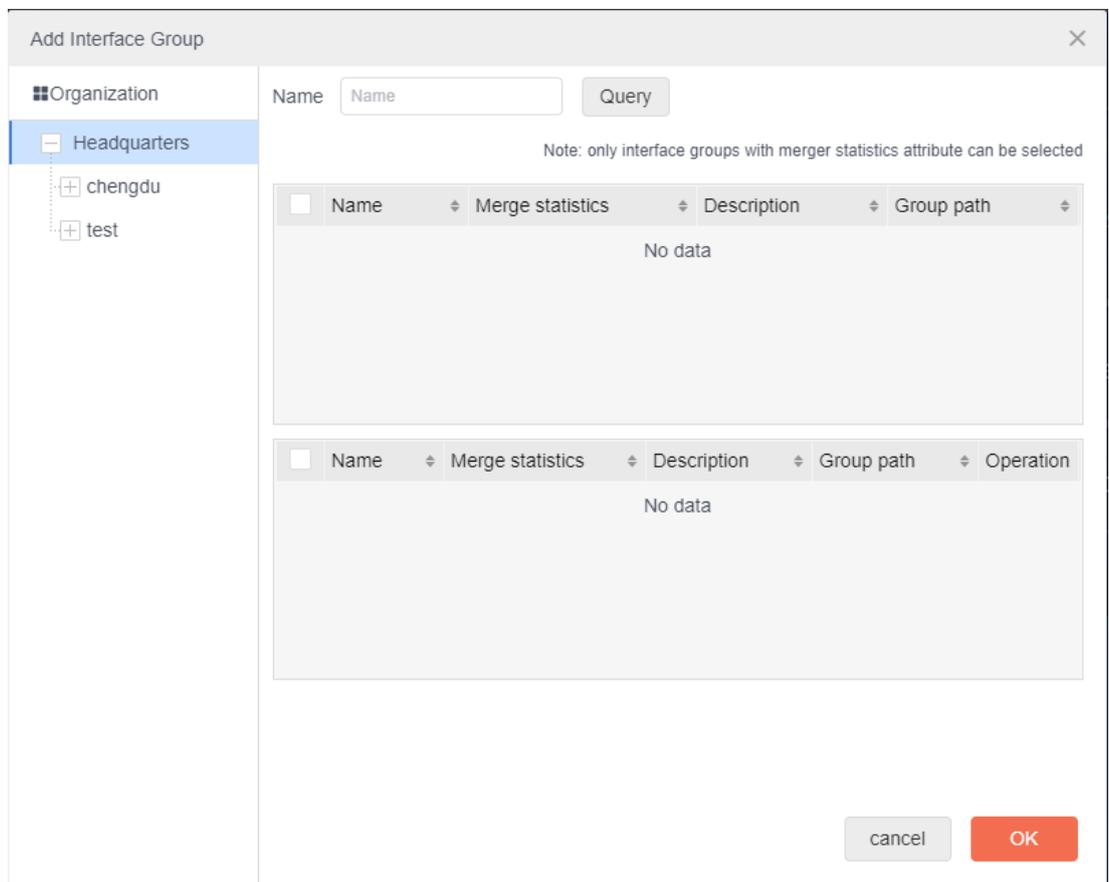


Figure 9-27 Select the interface group

After the configuration is completed, click the "OK" button to take effect, or click the "Cancel" button to cancel the current configuration. You can also click "Restore default" to restore the default configuration.

### 9.3.1.3. Bandwidth Utilization Statistics of Concerned Interface

This component is used to display the bandwidth utilization statistics of the concerned interface within the specified time range.

#### Display Effect



Figure 9-28 Bandwidth utilization statistics of the concerned interface

The display effect of the component is shown in the figure above. The title can be changed according to different configuration items. This component can display the bandwidth utilization statistics data of up to five interfaces/interface groups.

Move the mouse to the chart to display the details, but only on the home page, and there is no such prompt in the big screen.

The component legend is located on the left side of the chart. Each legend has two lines. The black font on the top is the device name, and the blue font at the bottom is the interface name. If it is an interface group, the legend displays only the name of the interface group. You can click the legend to jump to the monitoring data details page.

#### Configuration Method

The component configuration interface is shown in the following figure:

Statistics of concerned interface rate

Time range: Last hour

Flow direction:  Send  Receive

Refresh interval: 5 minutes

Refresh time:  Display  Hide

Way of value selection: Maximum

Interface | Interface Group | Up to 5 interfaces can be selected: 3/5

<input type="checkbox"/>	Status	Name	Device name	Device IP	Interface IP	Description	Type	Operation
<input type="checkbox"/>	●	Conn...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
<input type="checkbox"/>	●	gigab...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
<input type="checkbox"/>	●	gigab...	10.11.12.249	10.11.12....			Interface	Delete

Delete selection 0 / of 3 selected

Restore default | cancel | OK

Figure 9-29 Bandwidth utilization statistics configuration interface of the concerned interface

**Time range:** One of five time periods can be selected from the drop-down box to count the change of data. The five time periods are the last hour, the last day, the last week, the last month, and the last three months;

**Refresh interval:** It can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Flow direction:** It can be divided into send and receive. After the selection, the title in the component display effect will change with the user's choice, and the number of statistics will also change.

**Interface and Interface Group:** Only 5 pieces of data can be selected at most, and they are required. For the selection interface of interfaces and interface groups, please refer to the configuration items of interfaces and interface groups in the rate statistics of concerned interfaces.

After the configuration is completed, click the "OK" button to take effect, or click the "Cancel" button to cancel the current configuration. You can also click "Restore default"

to restore the default configuration.

#### 9.3.1.4. Bandwidth Utilization Monitoring of Concerned Interface

This component is used to display the bandwidth utilization trend of the concerned interface within a specified time range.

##### Display Effect



Figure 9-30 Bandwidth utilization monitoring of the concerned interface

The display effect of the component is shown in the figure above. The title can be changed according to different configuration items. This component can display the bandwidth utilization trend of up to six interfaces/interface groups.

Move the mouse to the chart to display the details, but only on the home page, and there is no such prompt in the big screen.

The component legend is located at the bottom of the chart. Each legend has two lines. The black font on the top is the device name, and the blue font at the bottom is the interface name. If it is an interface group, the legend displays only the name of the interface group. You can click the legend to jump to the monitoring data details page.

##### Configuration Method

The component configuration interface is shown in the following figure:

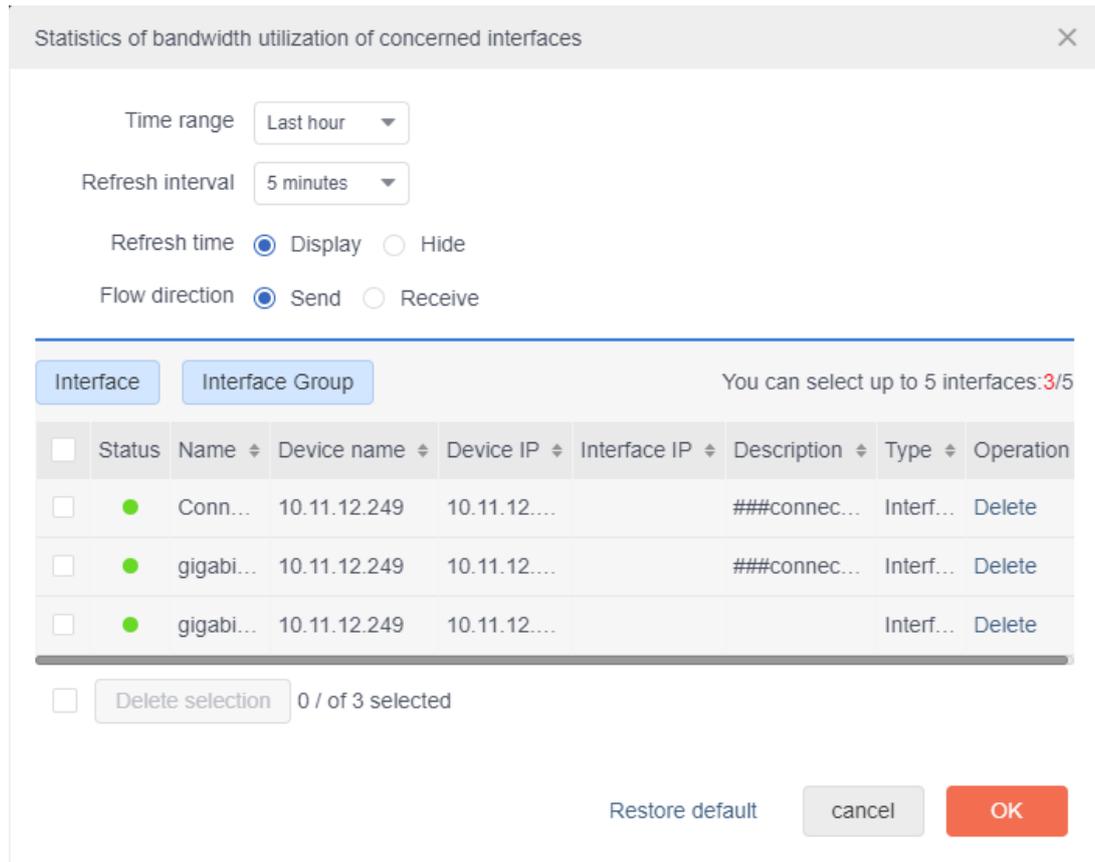


Figure 9-31 Bandwidth utilization monitoring configuration interface of the concerned interface

**Time range:** One of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month, and the last three months;

**Flow direction:** It can be divided into send and receive. After the selection, the title in the component display effect will change with the user's choice, and the number of statistics will also change.

**Refresh interval:** It can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Interface and Interface Group:** Only 6 pieces of data can be selected at most, and they are required. For the selection interface of interfaces and interface groups, please refer to the configuration items of interfaces and interface groups in the rate statistics of concerned interfaces.

After the configuration is completed, click the "OK" button to take effect, or click the "Cancel" button to cancel the current configuration. You can also click "Restore default" to restore the default configuration.

### 9.3.1.5. Interface Rate TOP N

The component is used to display the N interfaces with the maximum interface rate within the specified time range.

#### Display Effect



Figure 9-32 Interface rate TOP N

The display effect of the component is shown in the above figure. The title can be changed according to different configuration items. This component displays the rate data of interfaces/interface groups in descending order, with a maximum of 20.

Move the mouse to the chart to display the details, but only on the home page, and there is no such prompt in the big screen.

The component legend is located at the left side of the chart. Each legend has two lines. The black font on the top is the device name, and the blue font at the bottom is the interface name. If it is an interface group, the legend displays only the name of the interface group. You can click the legend to jump to the monitoring data details page.

#### Configuration Method

The component configuration interface is shown in the following figure:

Statistics of concerned interface rate
✕

Time range

Flow direction  Send  Receive

Refresh interval

Refresh time  Display  Hide

Way of value selection

Interface
Interface Group
Up to 5 interfaces can be selected: 3/5

<input type="checkbox"/>	Status	Name	Device name	Device IP	Interface IP	Description	Type	Operation
<input type="checkbox"/>	●	Conn...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
<input type="checkbox"/>	●	gigab...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
<input type="checkbox"/>	●	gigab...	10.11.12.249	10.11.12....			Interface	Delete

0 / of 3 selected

Figure 9-33 TOP N configuration interface of the interface rate

**Time range:** One of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month, and the last three months;

**Flow direction:** It can be divided into send and receive. After the selection, the title in the component display effect will change with the user's choice, and the number of statistics will also change.

**TOP N:** It can be set to 5, 10, 15, and 20.

**Refresh interval:** It can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Select interface:** By default, it is all, which can be configured by the user. Please refer to interface and interface group configuration items of "Rate Statistics of Concerned Interface".

After the configuration is completed, click the "OK" button to take effect, or click the "Cancel" button to cancel the current configuration. You can also click "Restore default" to restore the default configuration.

### 9.3.1.6. Interface Bandwidth Utilization TOP N

The component is used to display the N interfaces with the highest interface bandwidth utilization within the specified time range.

#### Display Effect

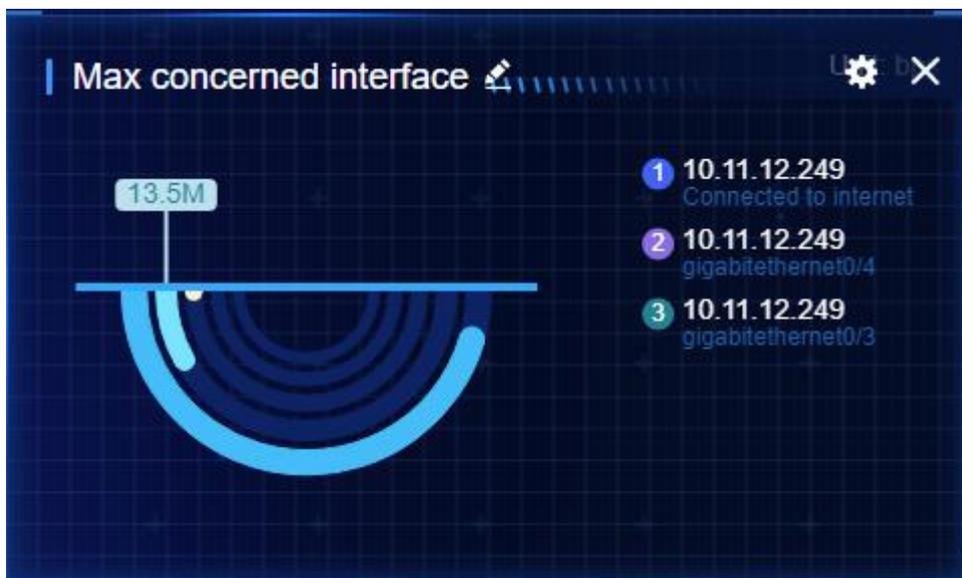


Figure 9-34 Interface bandwidth utilization TOP N

The display effect of the component is shown in the above figure. The title can be changed according to different configuration items. This component displays the bandwidth utilization data of interfaces/interface groups in descending order, with a maximum of 20.

Move the mouse to the chart to display the details, but only on the home page, and there is no such prompt in the big screen.

The component legend is located at the left side of the chart. Each legend has two lines. The black font on the top is the device name, and the blue font at the bottom is the interface name. If it is an interface group, the legend displays only the name of the interface group. You can click the legend to jump to the monitoring data details page.

#### Configuration Method

The component configuration interface is shown in the following figure:

Statistics of concerned interface rate
✕

Time range

Flow direction  Send  Receive

Refresh interval

Refresh time  Display  Hide

Way of value selection

---

Up to 5 interfaces can be selected: 3/5

<input type="checkbox"/>	Status	Name	Device name	Device IP	Interface IP	Description	Type	Operation
<input type="checkbox"/>	●	Conn...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
<input type="checkbox"/>	●	gigab...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
<input type="checkbox"/>	●	gigab...	10.11.12.249	10.11.12....			Interface	Delete

0 / of 3 selected

Figure 9-35 Interface bandwidth utilization TOP N configuration interface

**Time range:** One of five time periods can be selected from the drop-down box to count the change of data. The five time periods are the last hour, the last day, the last week, the last month, and the last three months;

**Flow direction:** It can be divided into send and receive. After the selection, the title in the component display effect will change with the user's choice, and the number of statistics will also change.

**TOP N:** It can be set to 5, 10, 15, and 20.

**Refresh interval:** It can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Select interface:** By default, it is all, which can be configured by the user. Please refer to interface and interface group configuration items of "Rate Statistics of Concerned Interface".

After the configuration is completed, click the "OK" button to take effect, or click the "Cancel" button to cancel the current configuration. You can also click "Restore default" to restore the default configuration.

### 9.3.1.7. Interface Lost Packets TOP N

The component is used to display the N interfaces with the maximum lost packets within the specified time range.

#### Display Effect

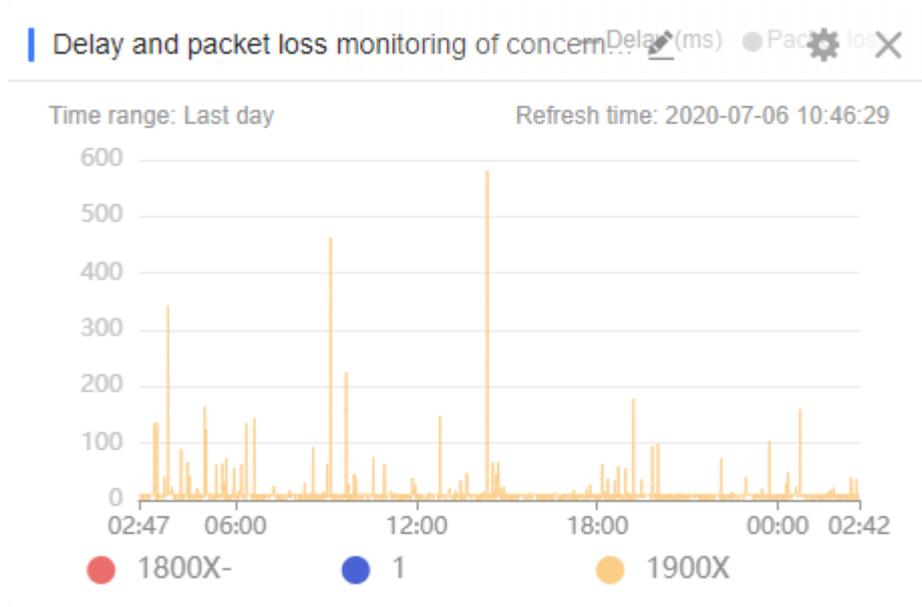


Figure 9-36 Interface lost packets TOP N

The display effect of the component is shown in the above figure. The title can be changed according to different configuration items. This component displays the rate statistics data of interfaces/interface groups in descending order, with a maximum of 20.

Move the mouse to the chart to display the details, but only on the home page, and there is no such prompt in the big screen.

The component legend is located at the left side of the chart. Each legend has two lines. The black font on the top is the device name, and the blue font at the bottom is the interface name. If it is an interface group, the legend displays only the name of the interface group. You can click the legend to jump to the monitoring data details page.

#### Configuration Method

The component configuration interface is shown in the following figure:

Delay and packet loss monitoring of concerned links

Time range Last day

Refresh interval One minute

Refresh time  Display  Hide

Link Up to 6 links can be selected: 3/6

<input type="checkbox"/>	Status	Link name	Source device name	Source device IP	Peer device name	Peer device IP	Op
<input type="checkbox"/>	●	1800X-	NMServer		router	10.10.1.1	De
<input type="checkbox"/>	●	1	S2300-10TP-AC (...	10.11.12.5	CP2300-10TP-...	10.11.12.87	De
<input type="checkbox"/>	●	1900X	NMServer		R4	10.11.12.111	De

Delete selection 0 / of 3 selected

Restore default
cancel
OK

Figure 9-37 Interface lost packets TOP N configuration interface

**Time range:** One of five time periods can be selected from the drop-down box to count the change of data. The five time periods are the last hour, the last day, the last week, the last month, and the last three months;

**Flow direction:** It can be divided into send and receive. After the selection, the title in the component display effect will change with the user's choice, and the number of statistics will also change.

**TOP N:** It can be set to 5, 10, 15, and 20.

**Refresh interval:** It can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Select interface:** By default, it is all, which can be configured by the user. Please refer to interface and interface group configuration items of "Rate Statistics of Concerned Interface".

After the configuration is completed, click the "OK" button to take effect, or click the "Cancel" button to cancel the current configuration. You can also click "Restore default" to restore the default configuration.

### 9.3.1.8. Single Interface Rate Monitoring

This component is used to display the rate trend of single interface receiving and sending

within the specified time range.

### Display Effect

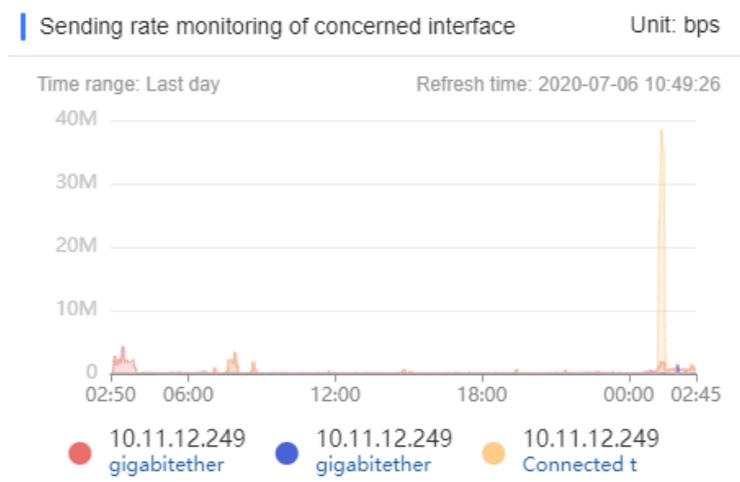


Figure 9-38 Single interface rate monitoring

The display effect of the component is shown in the above figure. This component only shows the average rate trend of a single interface, and also shows the difference between the maximum rate and the minimum rate using a histogram.

Move the mouse to the chart to display the details, but only on the home page, and there is no such prompt in the big screen.

Click the interface name at the top of the chart to jump to the monitoring data details page.

### Configuration Method

The component configuration interface is shown in the following figure:

Rate monitoring of concerned interface

Time range: Last day

Flow direction:  Send  Receive

Refresh interval: 5 minutes

Refresh time:  Display  Hide

Interface Interface Group Up to 6 interfaces can be selected: 3/6

<input type="checkbox"/>	Status	Name	Device name	Device IP	Interface IP	Description	Type	Operation
<input type="checkbox"/>	●	Conn...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
<input type="checkbox"/>	●	gigab...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
<input type="checkbox"/>	●	gigab...	10.11.12.249	10.11.12....			Interface	Delete

Delete selection 0 / of 3 selected

Restore default cancel OK

Figure 9-39 Single interface rate monitoring configuration interface

**Time range:** One of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month, and the last three months;

**Refresh interval:** It can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Select interface:** It is mandatory, and you can only select one interface. For the interface of selecting the interface, refer to interface configuration items of “Rate Statistics of Concerned Interface”.

After the configuration is completed, click the “OK” button to take effect, or click the “Cancel” button to cancel the current configuration. You can also click “Restore default” to restore the default configuration.

### 9.3.1.9. Interface Integrated Monitoring TOP N

This component is used to display the interface rate, interface packet loss and interface bandwidth within the specified time range.

#### Display Effect

Status	Name	Device name	Device IP	Interface IP	Description	Type	Operation
●	Conn...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
●	gigab...	10.11.12.249	10.11.12....		###connec...	Interface	Delete
●	gigab...	10.11.12.249	10.11.12....			Interface	Delete

Figure 9-40 Interface integrated monitoring TOP N

The display effect of the component is shown in the above figure. The component displays the comprehensive data of interfaces/interface groups in descending order, with a maximum of 20.

Click the interface name of the list, and you can jump to the monitoring data details page.

### Configuration Method

The component configuration interface is shown in the following figure:

Interface integrated monitoring TOP N

Time range

Sorting mode

TOPN

Refresh interval

Refresh time  Display  Hide

Display column  Status  Device name  Interface(Group) name  Bandwidth utilization  Rate  
 Lost packets

Select interface  All  Custom

[Restore default](#)

Figure 9-41 TOP N configuration interface of interface integrated monitoring

**Time range:** One of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month, and the last three months;

**Sorting mode:** Bandwidth utilization, rate and the number of lost packets can be selected.

**TOP N:** It can be set to 5, 10, 15, and 20.

**Refresh interval:** It can be set to 5 minutes, 15 minutes and 30 minutes.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Display column:** Status, device name and interface name are required. Bandwidth

utilization, rate and packet loss are optional. However, the "Sorting mode" option cannot be cancelled and is also required.

Select interface: By default, it is all, which can be configured by the user. Please refer to interface and interface group configuration items of "Rate Statistics of Concerned Interface".

After the configuration is completed, click the "OK" button to take effect, or click the "Cancel" button to cancel the current configuration. You can also click "Restore default" to restore the default configuration.

### 9.3.1.10. Device Response Time TOP N

Displays the N devices with the longest response time in the specified time range.

#### Display Effect



Figure 9-42 Device response time TOP N

According to the configuration items, the configuration display can be divided into two cases as shown in the above figure: all normal data on the left side and all abnormal data on the right side. Click the device name, and you can jump to the corresponding device details page.

#### Configuration Method

Device response time TOP N

Time range: Last hour

TOP N: 5

Refresh interval: 5 minutes

Refresh time:  Display  Hide

Select device:  All  Custom

Device	Device group						
Status	Name	Alias	IP	Model	Organization	Type	Operation
<input type="checkbox"/>	●	10.11.12.249	10.11.12.249	SM3320-2...	chengdu	Device	Delete
<input type="checkbox"/>	●	IBD-MP2900	10.11.12.254	MP2900-14	chengdu	Device	Delete
<input type="checkbox"/>	●	S2300-10T...	10.11.12.5		Headquarters	Device	Delete

Delete selection 0 / of 3 selected < 1 > 20 records/page Jump to 1 Page OK

Restore default cancel OK

Figure 9-43 Device response time TOP N configuration interface

### Configuration Items

Time range (last hour, current day, last week, last month, last three months): drop-down box, select the data to display the time range;

TOP N (5, 10, 15, 20): drop-down box, select the latest data quantity to display. When the control title is not modified on the interface, the title TOP (N) will be displayed synchronously;

Refresh interval (5 minutes, 15 minutes, 30 minutes): drop-down box, select the interval of refreshing the data;

Refresh time (display, hide): the radio button, select whether the refresh time is displayed or not, and whether the time range is displayed synchronously;

Select devices (all, custom): radio button, select all devices or customize the devices and device groups to be displayed,

Refer to the same controls for the functions of devices and device groups. After custom is selected, do not select the device or device group, and click "OK" to have the correct prompt information.

---

**Note**

- Do not display the offline devices or the offline devices in the device group.
- 

**9.3.1.11. Concerned Device Health**

Display the health of the specified device.

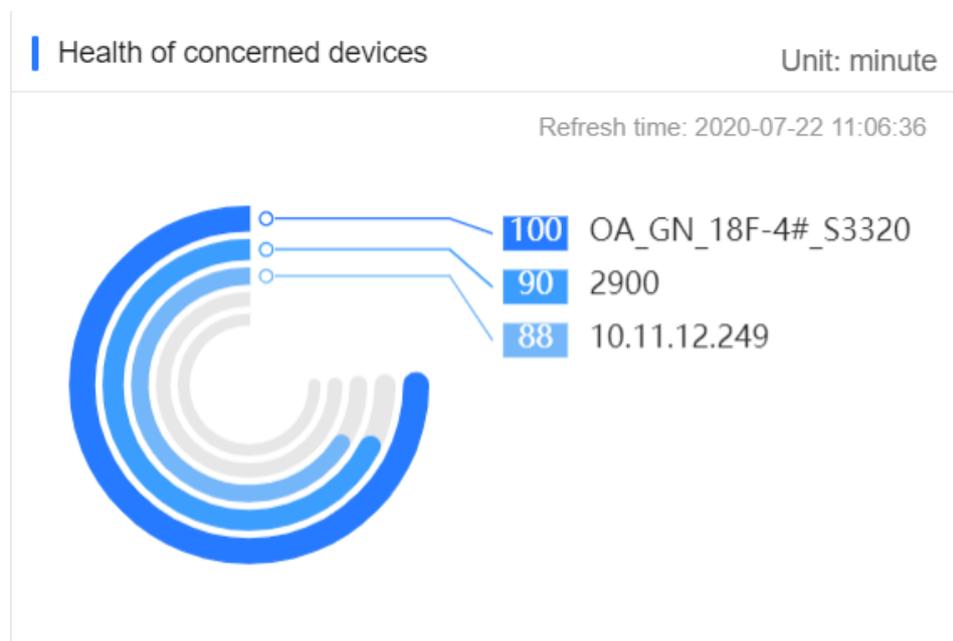
**Display Effect**

Figure 9-44 Concerned device health

According to the configuration items, the configuration display can be divided into two cases as shown in the above figure. On the left side, select the device to display the health of the device, and on the right side, it is the default display of the un-selected device. Click the device name to jump to the corresponding device detail page.

**Configuration Method**

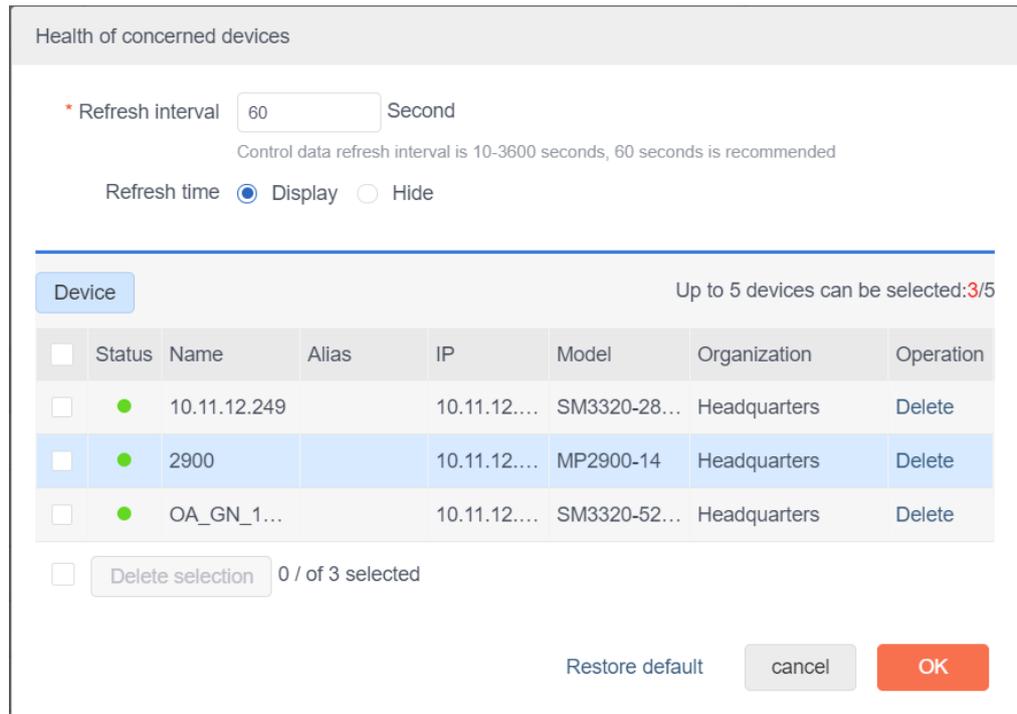


Figure 9-45 Health configuration interface of the concerned device

**Configuration Items:**

Refresh interval (custom): mandatory, update period, refresh interval, the refresh interval of control data is 10 – 3600 seconds, 60 seconds is recommended; if the filled value is not within the allowed range, there will be a prompt message;

Refresh time (display, hide): radio button, select whether the refresh time is displayed or not, and whether the time range is displayed synchronously;

Device: button, click to select the device to be displayed, up to 5 devices can be selected. Please refer to the same control for selecting device function. If not selecting the device, click OK, and there will be the correct prompt information.

**9.3.1.12. Device Status Statistics**

Display the total number and status of devices (online and offline).

**Display Effect**

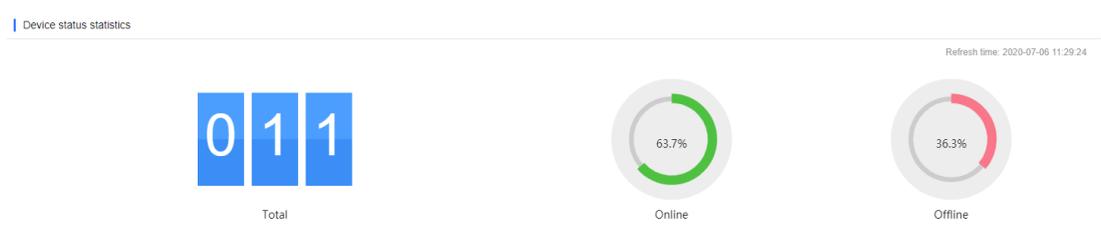


Figure 9-46 Device status statistics

Click the "Online" and "Offline" status to jump to the device list page.

## Configuration Method

Device status statistics

\* Refresh interval  Second  
Control data refresh interval is 10-3600 seconds, 60 seconds is recommended

Refresh time  Display  Hide

Select device  All  Custom

Device Device group

<input type="checkbox"/>	Status	Name	Alias	IP	Model	Organization	Type	Operation
<input type="checkbox"/>	●	10.11.12...		10.11.12...	SM3320...	chengdu	Device	Delete
<input type="checkbox"/>	●	IBD-MP...		10.11.12...	MP2900...	chengdu	Device	Delete
<input type="checkbox"/>	●	S2300-1...		10.11.12.5		Headquarte	Device	Delete

Delete selection 0 / of 3 selected

< 1 > 20 records/page Jump to 1 Page OK

Restore default cancel OK

Figure 9-47 Device status statistics configuration interface

### Configuration Items:

Refresh interval (custom): mandatory, update period, refresh interval, the refresh interval of control data is 10 – 3600 seconds, 60 seconds is recommended; if the filled value is not within the allowed range, there will be a prompt message;

Refresh time (display, hide): radio button, select whether the refresh time is displayed or not, and whether the time range is displayed synchronously;

Device: button, click to select the device to be displayed, up to 5 devices can be selected. Please refer to the same control for selecting device function. If not selecting the device, click , and there will be the correct prompt information.

### 9.3.1.13. Availability Monitoring of Concerned Device

Display the real-time information of CPU, memory and response time of the specified device.

### Display Effect

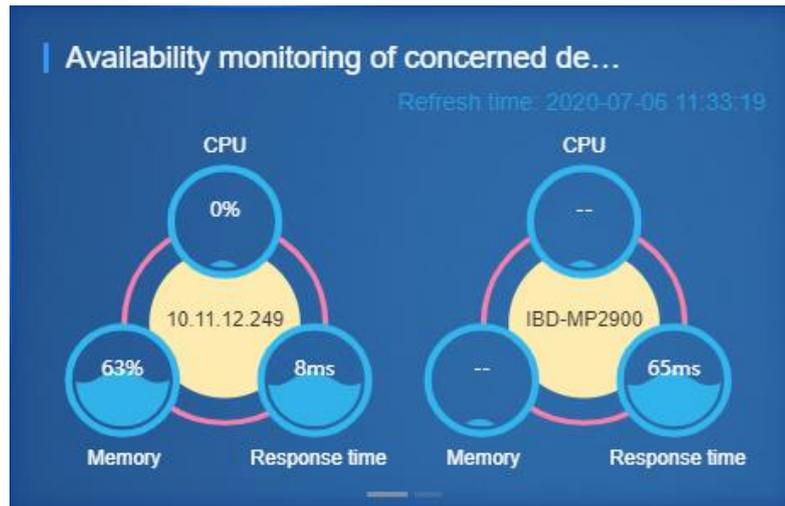


Figure 9-48 Availability monitoring of the concerned device

According to the configuration items, the configuration display can be divided into two cases as shown in the above figure. On the left side, it is the display of the configured data. On the right side, it is the default display. Click the device name, and you can jump to the corresponding device detail page. If there are multiple devices to monitor, you can switch to display automatically, and it also supports switching to display manually.

### Configuration Method

Availability monitoring of concerned devices ✕

\* Refresh interval  Second  
Control data refresh interval is 10-3600 seconds, recommended 10 seconds

Refresh time  Display  Hide

---

Device Up to 10 devices can be selected: 3/10

<input type="checkbox"/>	Status	Name	Alias	IP	Model	Organization	Operation
<input type="checkbox"/>	●	10.11.12.249		10.11.12....	SM3320-28...	chengdu	Delete
<input type="checkbox"/>	●	IBD-MP2900		10.11.12....	MP2900-14	chengdu	Delete
<input type="checkbox"/>	●	S2300-10T...		10.11.12.5		Headquarters	Delete

Delete selection 0 / of 3 selected

Figure 9-49 Availability monitoring configuration interface of the concerned device

### Configuration Items:

Refresh interval (custom): mandatory, update period, refresh interval, the refresh interval of control data is 10 – 3600 seconds, 60 seconds is recommended; if the filled value is not within the allowed range, there will be a prompt message;

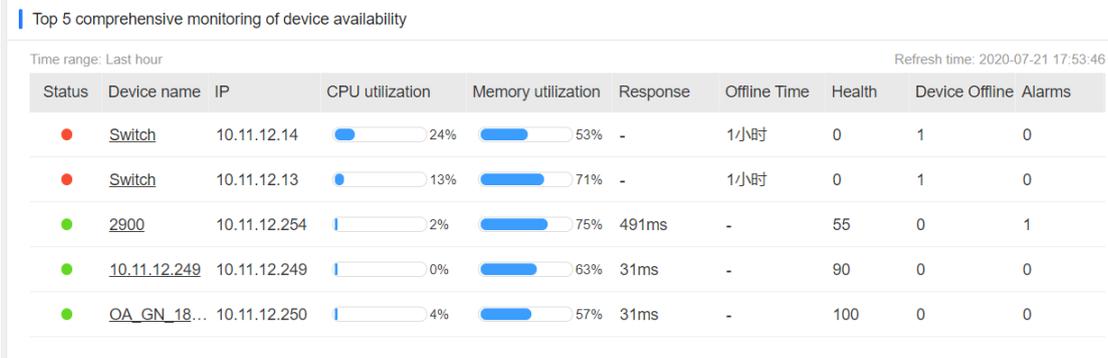
Refresh time (display, hide): radio button, select whether the refresh time is displayed or not, and whether the time range is displayed synchronously;

Device: button, click to select the device to be displayed, up to 5 devices can be selected. Please refer to the same control for selecting device function. If not selecting the device, click , and there will be the correct prompt information.

### 9.3.1.14. Device Availability Comprehensive Monitoring TOP N

Display the availability index of the TOP N devices in the health ranking.

#### Display Effect



Status	Device name	IP	CPU utilization	Memory utilization	Response	Offline Time	Health	Device Offline	Alarms
●	<a href="#">Switch</a>	10.11.12.14	24%	53%	-	1小时	0	1	0
●	<a href="#">Switch</a>	10.11.12.13	13%	71%	-	1小时	0	1	0
●	<a href="#">2900</a>	10.11.12.254	2%	75%	491ms	-	55	0	1
●	<a href="#">10.11.12.249</a>	10.11.12.249	0%	63%	31ms	-	90	0	0
●	<a href="#">OA_GN_18...</a>	10.11.12.250	4%	57%	31ms	-	100	0	0

Figure 9-50 Device availability comprehensive monitoring TOP N

According to the configuration items, the configuration display can be divided into two cases as shown in the above figure. The upper side is displayed according to the health by default, and the lower side is the display of the configured data. Click the device name, and you can jump to the corresponding device details page.

Support column width drag;

Support manual switching display. If there is multi-page device monitoring, you can automatically switch display;

#### Configuration Method

Availability monitoring of concerned devices

\* Refresh interval  Second  
Control data refresh interval is 10-3600 seconds, recommended 10 seconds

Refresh time  Display  Hide

---

Device Up to 10 devices can be selected: 3/10

<input type="checkbox"/>	Status	Name	Alias	IP	Model	Organization	Operation
<input type="checkbox"/>	●	10.11.12.249		10.11.12....	SM3320-28...	chengdu	Delete
<input type="checkbox"/>	●	IBD-MP2900		10.11.12....	MP2900-14	chengdu	Delete
<input type="checkbox"/>	●	S2300-10T...		10.11.12.5		Headquarters	Delete

Delete selection 0 / of 3 selected

Figure 9-51 Device availability comprehensive monitoring TOP N configuration interface

### Configuration Items:

Time range (last hour, current day, last week, last month, last three months): drop-down box, select the data to display the time range;

Refresh interval (custom): mandatory, update period, refresh interval, the refresh interval of control data is 10 – 3600 seconds, 60 seconds is recommended; if the filled value is not within the allowed range, there will be a prompt message;

Refresh time (display, hide): radio button, select whether the refresh time is displayed or not, and whether the time range is displayed synchronously;

TOP N (5, 10, 15, 20): drop-down box, select the latest data quantity to display. When the control title is not modified on the interface, the title TOP (N) will be displayed synchronously;

Display column: check box, select the column to be displayed. The display column includes status, device name, IP, CPU utilization, memory utilization, response time, offline duration, health, offline times, and alarm quantity. The  check box is a required display column and cannot be operated.

Select devices (all, custom): radio button, select all devices or customize the devices and device groups to be displayed,

Refer to the same controls for the functions of devices and device groups. After custom is selected, do not select the device or device group. Click , and there will be the correct prompt information.

### 9.3.1.15. Real-time Statistics of Link Status

Display the link (connected, disconnected, unknown) statistics.

#### Display Effect

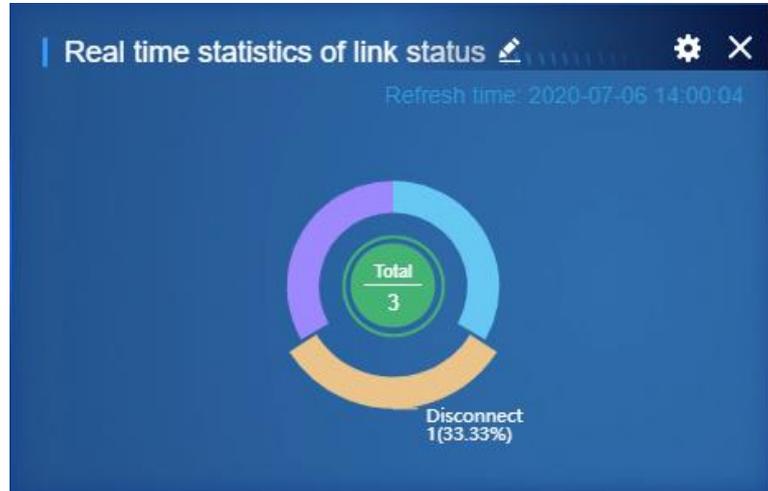


Figure 9-52 Real-time statistics of the link status

■ indicates the normal links, ■ indicates the disconnected links, ■ indicates the unknown links. If the control has multiple states, the link has the witching effect.

#### Configuration Method

The configuration interface includes the following settings:

- Refresh interval: One minute (dropdown)
- Refresh time:  Display  Hide
- Select link:  All  Custom

Below the settings is a table with the following columns: Link, Status, Link name, Source device name, Source device IP, Peer device name, Peer device IP, and Operation.

Link	Status	Link name	Source device name	Source device IP	Peer device name	Peer device IP	Operation
	<input type="checkbox"/>	111	10.11.12.249	10.11.12.249		10.11.12.62	Delete

At the bottom of the table, there is a 'Delete selection' button, a '0 / of 1 selected' indicator, a page navigation bar showing '1' of 1 page, and a '5 records/page' dropdown. At the bottom right, there are 'Restore default', 'cancel', and 'OK' buttons.

Figure 9-53 Real-time statistics configuration interface of the link status

#### Configuration Items:

Interval (1 minute, 5 minutes, 15 minutes, 30 minutes): drop-down box, select data update period, refresh interval;

Refresh time (display, hide): radio button, select whether the refresh time is displayed or not;

Select links (all, custom): radio button, select all devices or customize the link to be displayed. After selecting custom, do not select link data. Click , and there will be correct prompt information.

Select links:

Device

<input checked="" type="checkbox"/>	Status	Link name	Source device name	Source device IP	Peer device name	Peer device IP	Organiz
<input checked="" type="checkbox"/>	●	1900X	NMServer		R4	10.11.12.111	Headqu
<input checked="" type="checkbox"/>	●	1	S2300-10TP-AC (...	10.11.12.5	CP2300-10TP-...	10.11.12.87	Headqu
<input checked="" type="checkbox"/>	●	1800X-	NMServer		router	10.10.1.1	Headqu

Total 3 < 1 > 5 records/page Jump to 1 Page

<input checked="" type="checkbox"/>	Status	Link name	Source device name	Source device IP	Peer device name	Peer device IP	Org
<input checked="" type="checkbox"/>	●	1900X	NMServer		R4	10.11.12.111	Hez
<input checked="" type="checkbox"/>	●	1	S2300-10TP-AC (E1)	10.11.12.5	CP2300-10TP-DC...	10.11.12.87	Hez
<input checked="" type="checkbox"/>	●	1800X-	NMServer		router	10.10.1.1	Hez

Delete selection 3 / of 3 selected < 1 > 5 records/page Jump to 1 Page

Figure 9-54 Select links

### 9.3.1.16. Delay Packet Loss Monitoring of Concerned Link

Display the delay and packet loss trend of the specified link in a certain time range.

#### Display Effect

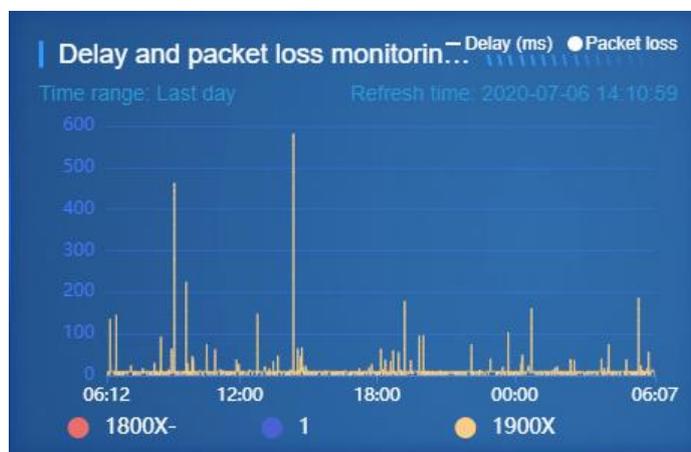


Figure 9-55 Delay packet loss monitoring of the concerned link

According to the configuration items, the configuration display can be divided into two situations as shown in the above figure: the left side displays the configured data, and the right side is the default display. Click the link name, and you can jump to the corresponding link detection list page, which supports displaying up to 6 links.

## Configuration Method

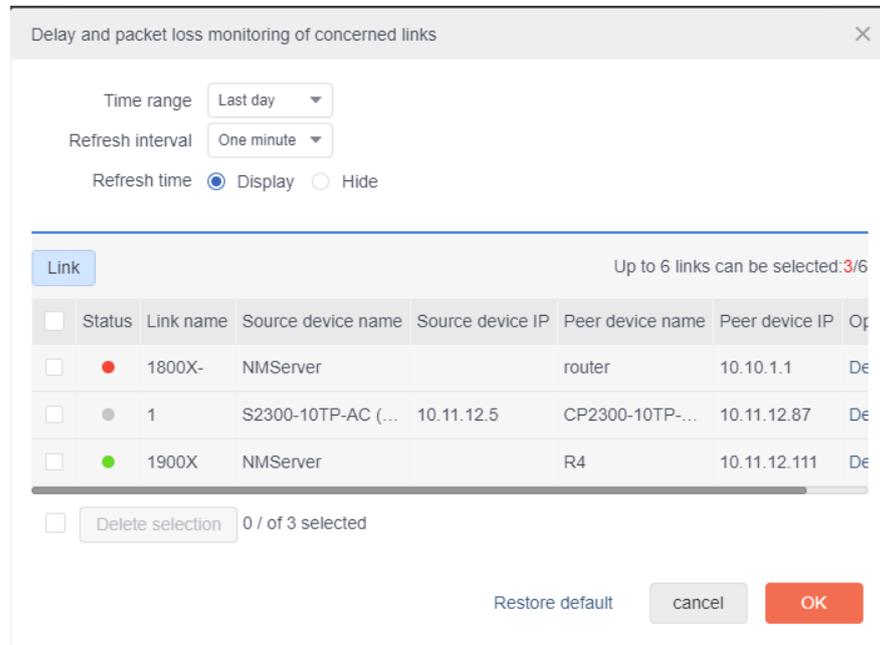


Figure 9-56 Delay packet loss monitoring configuration interface of the concerned link

### Configuration Items:

Time range (last hour, current day, last week, last month, last three months): drop-down box, select the data to display the time range;

Interval (1 minute, 5 minutes, 15 minutes, 30 minutes): drop-down box, select data update period, refresh interval;

Refresh time (display, hide): radio button, select whether the refresh time is displayed or not;

Link: button, select the link to be displayed. If not selecting the link data, click



, and there is the correct prompt information.

### 9.3.1.17. Delay Statistics of Concerned Link

Display the delay statistics of the specified link in a certain time range.

### Display Effect



Figure 9-57 Delay statistics of the concerned link

According to the configuration items, the configuration display can be divided into two situations as shown in the above figure: the left side displays the configured data, and the right side is the default display. Click the link name, and you can jump to the corresponding link detection list page, which supports displaying up to 10 links.

## Configuration Method

Link	Status	Link name	Source device name	Source device IP	Peer device name	Peer device IP	Op
	●	1800X-	NMServer		router	10.10.1.1	De
	●	1	S2300-10TP-AC (...	10.11.12.5	CP2300-10TP-...	10.11.12.87	De
	●	1900X	NMServer		R4	10.11.12.111	De

Figure 9-58 Delay statistics configuration interface of the concerned link

## Configuration Items:

Time range (last hour, current day, last week, last month, last three months): drop-down box, select the data to display the time range;

Interval (1 minute, 5 minutes, 15 minutes, 30 minutes): drop-down box, select data update period, refresh interval;

Refresh time (display, hide): radio button, select whether the refresh time is displayed or not;

Link: button, select the link to be displayed. If not selecting the link data, click



, and there is the correct prompt information.

### 9.3.1.18. Topology View

Display the specified topology view.

#### Display Effect

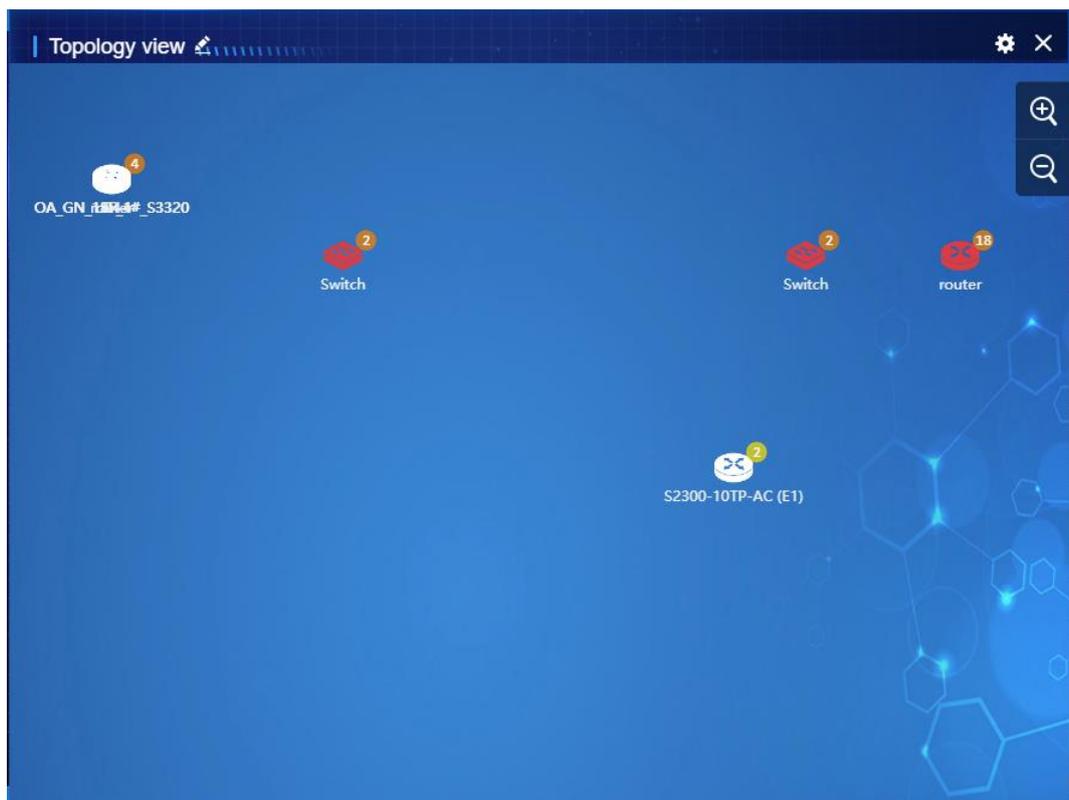


Figure 9-59 Topology view

According to the configuration items, the configuration display can be divided into two cases as shown in the figure above. The configured topology is displayed on the left side and the default display is on the right side.

Support translating, zooming in and zooming out the topology view.

## Configuration Method

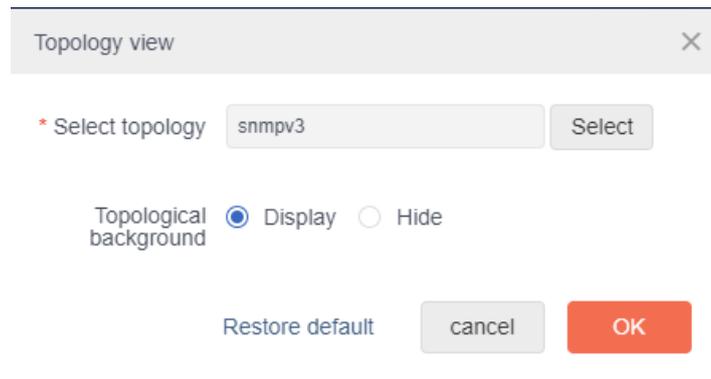


Figure 9-60 Topology view configuration interface

### Configuration Items:

Select topology: select the file, select the topology view to be displayed. If not selecting the link data, click **OK**, and there will be the pop-up prompt information.

Topology background (display, shadow): radio button, select whether to display topology background;

### 9.3.1.19. Alarm Statistics of Concerned Device

The component is used to display the alarm statistics of the concerned device.

#### Display Effect

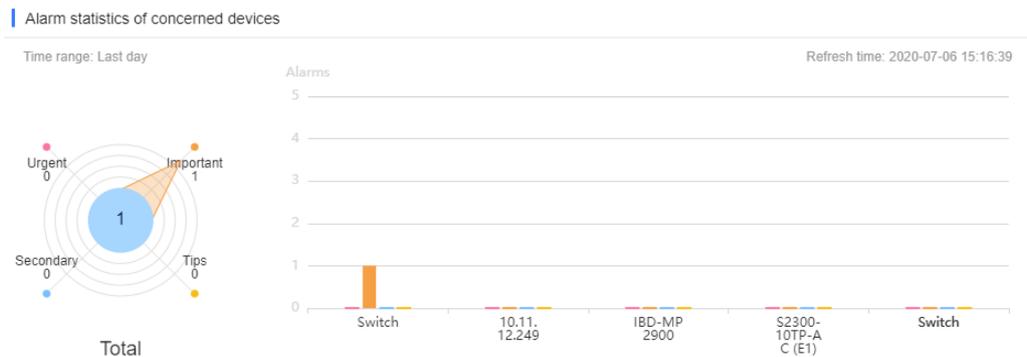


Figure 9-61 Alarm statistics of the concerned device

The component is divided into two parts. The left side is the alarm statistics summary chart of the selected device, the right side is the alarm detail diagram of the selected device, and the abscissa of the detail diagram on the right side is the name of each device.

### Configuration Method

The component configuration interface is shown in the following figure:

Alarm statistics of concerned devices

Time range Last day

\* Refresh interval 60 Second  
Control data refresh interval is 10-3600 seconds, 60 seconds is recommended

Refresh time  Display  Hide

Device
Up to 20 devices can be selected:2/20

<input checked="" type="checkbox"/>	Status	Name	Alias	IP	Model	Organization	Operation
<input checked="" type="checkbox"/>	●	10.11.1...		10.1...	SM332...	Headquarters	Delete
<input checked="" type="checkbox"/>	●	2900		10.1...	MP290...	Headquarters	Delete

Delete selection 2 / of 2 selected

Restore default
cancel
OK

Figure 9-62 Alarm statistics configuration interface of the concerned device

Time range: one of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month and the last three months.

Refresh interval: The interval of refreshing the component data. When the time range is the last day or the last week, the optional range is 10-3600 seconds. When the time range is the last month or the last three months, it can only be 300 seconds.

Refresh time, which can be set to show and hide. When set to hidden, the time range and refresh time in the chart are hidden.

Devices: only 20 pieces of data can be selected at most. The interface of selecting the device is shown in the following figure:

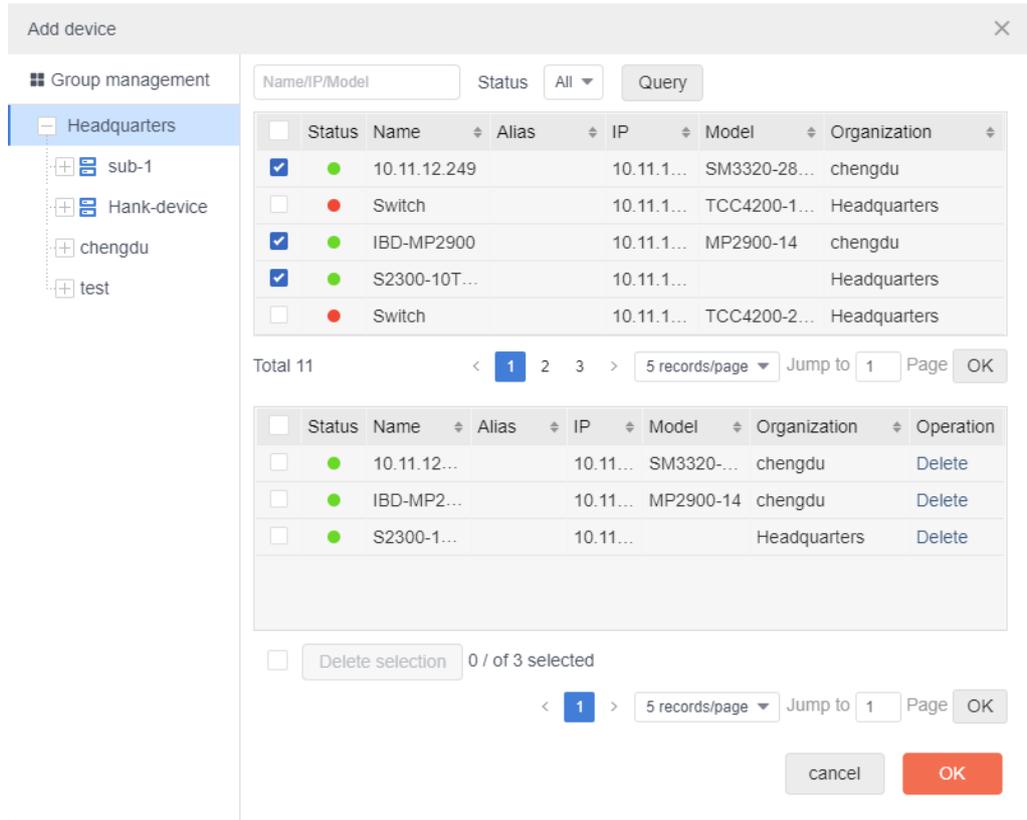


Figure 9-63 Select the device

### 9.3.1.20. Alarm Device TOP N

This component is used to display N devices with the largest number of alarms within a specified time range.

#### Display Effect



Figure 9-64 Alarm device TOP N

The black font on the left side of the component data bar is the name of the alarm device, and the number on the data bar is the alarm number of the current device.

## Configuration Method

The component configuration interface is shown in the following figure:

Figure 9-65 Alarm device TOP N configuration interface

**Time range:** one of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month and the last three months.

**TOP N:** Set the quantity of displayed data by configuring TOP N. The optional values are 5, 10, 15 and 20, and 10 is displayed by default. After selection, the title in the component display effect will change with the user's choice.

**Refresh interval:** The interval of refreshing the component data. When the time range is the last day or the last week, the optional range is 10-3600 seconds. When the time range is the last month or the last three months, it can only be 300 seconds.

**Refresh time,** which can be set to show and hide. When set to hidden, the time range and refresh time in the chart are hidden.

**Alarm source:** Select the alarm source to be counted. The sources are divided into four categories: device group, device, interface group and interface. Select all or custom. The interface for selecting the alarm source is as follows:

Select resources:

Select resources						
<input type="checkbox"/>	Name	Device IP	IP	Type	Operation	
No data						

Figure 9-66 Select the resource

Select device group:

Select device group

Organization

- Headquarters
  - chengdu
  - test

Name:  Query

<input checked="" type="checkbox"/>	Name	Description	Group path
<input checked="" type="checkbox"/>	sub-1	sub-1	/Headquarters/sub-1/
<input checked="" type="checkbox"/>	Hank-device		/Headquarters/Hank-device/
<input checked="" type="checkbox"/>	maipu		/Headquarters/chengdu/m...

Total 3 < 1 > 5 records/page Jump to 1 Page OK

<input type="checkbox"/>	Name	Description	Group path	Operation
<input type="checkbox"/>	sub-1	sub-1	/Headquarters/sub-1/	Delete
<input type="checkbox"/>	Hank-device		/Headquarters/Hank-d...	Delete
<input type="checkbox"/>	maipu		/Headquarters/chengd...	Delete

Delete selection 0 / of 3 selected < 1 > 5 records/page Jump to 1 Page OK

cancel OK

Figure 9-67 Select the device group

Select interface and interface group: Refer to “Rate Monitoring of Concerned Interface”.

Alarm level: Select the alarm level to be counted, urgent, important, secondary, and tips, at least one of which should be selected.

Alarm type: Select the alarm type to be counted, all or custom. The interface for selecting alarm type is as follows:

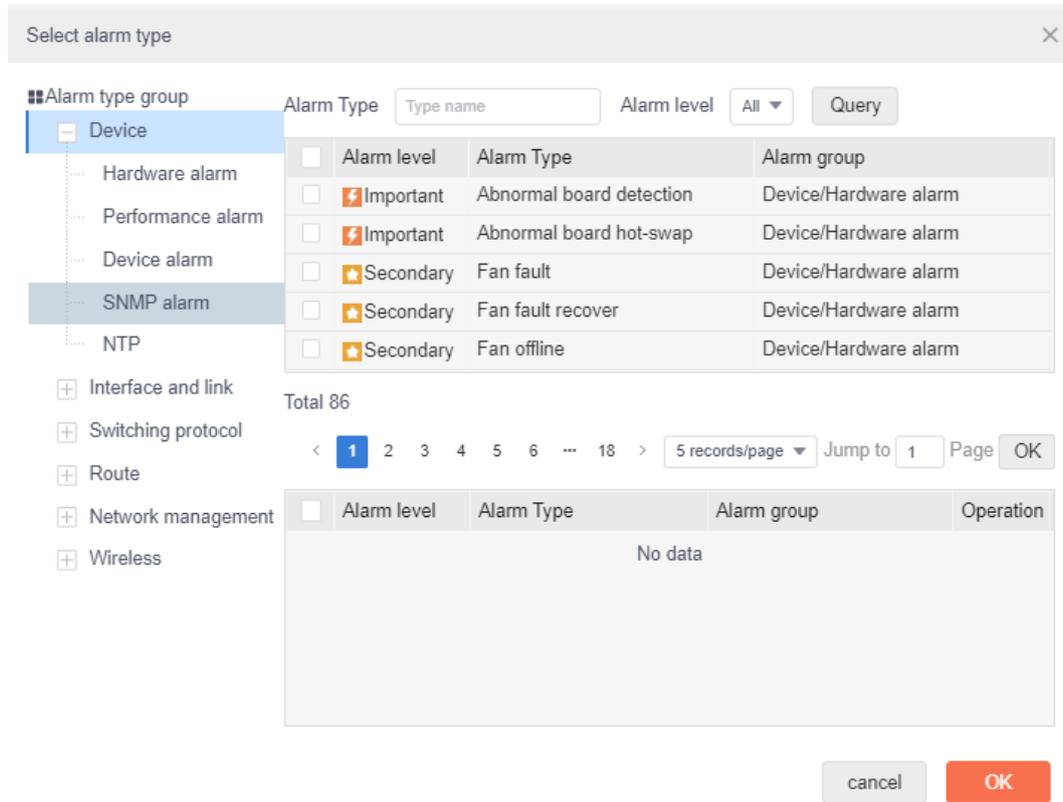


Figure 9-68 Select the alarm type

### 9.3.1.21. Alarm Level Statistics

This component is used to display statistics by alarm level within a specified time range.

#### Display Effect



Figure 9-69 Alarm level statistics

The word in each circle of the component is the alarm level, and the number is the number of devices under the current alarm level. Click the word, and you can jump to the corresponding alarm interface.

## Configuration Method

The component configuration interface is shown in the following figure:

Alarm level statistics

Time range

\* Refresh interval  Second  
Control data refresh interval is 10-3600 seconds, 60 seconds is recommended

Refresh time  Display  Hide

Alarm source  All alarm sources  Custom alarm source

Select resources

<input type="checkbox"/>	Name	Device IP	IP	Type	Opera
No data					

\* Alarm level  Urgent  Important  Secondary  Tips

Alarm Type  All alarm types  Custom alarm type

Restore default

Figure 9-70 Alarm level statistics configuration interface

**Time range:** one of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month and the last three months.

**Refresh interval:** The interval of refreshing the component data. When the time range is the last day or the last week, the optional range is 10-3600 seconds. When the time range is the last month or the last three months, it can only be 300 seconds.

**Refresh time,** which can be set to show and hide. When set to hidden, the time range and refresh time in the chart are hidden.

**Alarm source:** Select the alarm source to be counted. The sources are divided into five categories: device group, device, interface group, interface, and local network management. Select all or custom. The interface for selecting the alarm source is as follows:

Select the source:

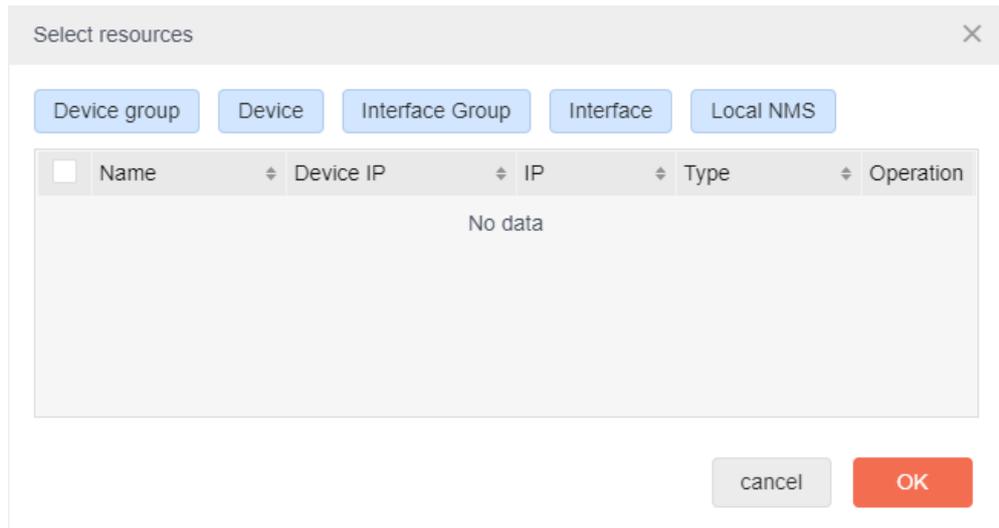


Figure 9-71 Select the source

Select device group: Refer to “Alarm Device TOP N”.

Select device: Refer to “Device Alarm Statistics of Concerned Device”.

Select interface and interface group: Refer to “Rate Monitoring of Concerned Interface”.

Select the local network management:

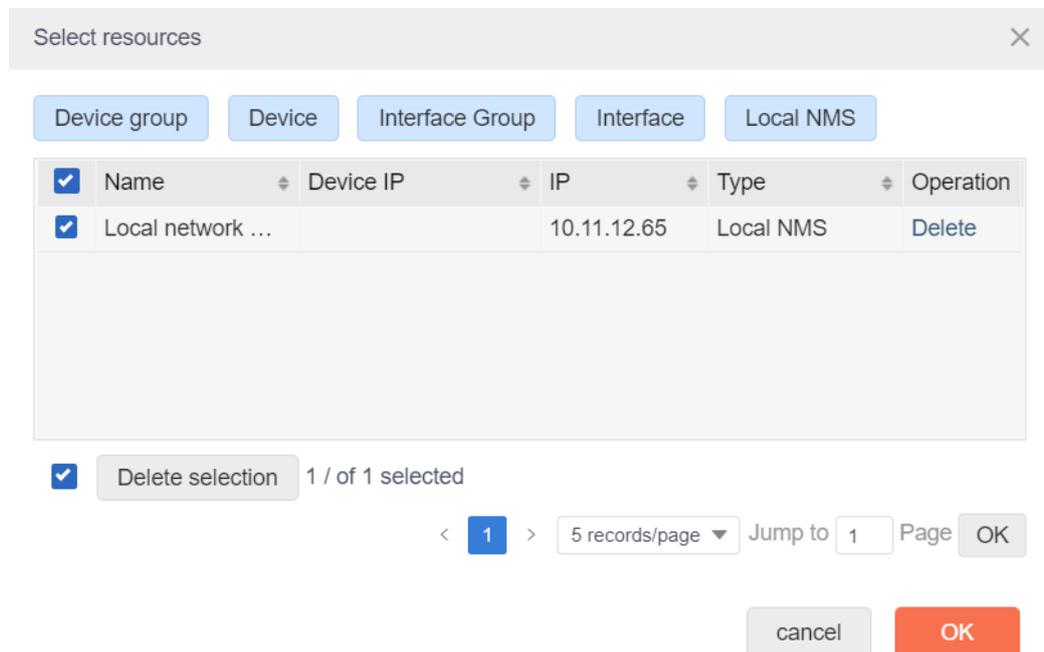


Figure 9-72 Select the local network management

Alarm level: Select the alarm level to be counted, urgent, important, secondary, and tips, at least one of which should be selected.

Alarm type: Select the alarm type to be counted, all or custom. For the interface for selecting alarm type, refer to “Alarm Device TOP N”.

### 9.3.1.22. Alarm Type TOP N

This component is used to display the rate trend of the concerned interface within a specified time range.

#### Display Effect



Figure 9-73 Alarm type TOP N

The black font on the left side of the component data bar is the name of the alarm type, and the number on the data bar is the alarm number of the current device type.

#### Configuration Method

The component configuration interface is shown in the following figure:

Alarm type TOP N

Time range: Last day

TOP N: 10

\* Refresh interval: 60 Second  
Control data refresh interval is 10-3600 seconds, 60 seconds is recommended

Refresh time:  Display  Hide

Alarm source:  All alarm sources  Custom alarm source

Select resources

<input type="checkbox"/>	Name	Device IP	IP	Type	Delete
<input type="checkbox"/>	10.11.12.249		10.11.12.249	Device	Delete
<input type="checkbox"/>	Switch		10.11.12.13	Device	Delete
<input type="checkbox"/>	IBD-MP2900		10.11.12.254	Device	Delete

Restore default cancel OK

Figure 9-74 Alarm type TOP N configuration interface

**Time range:** one of four time periods can be selected from the drop-down box to count the change of data. The four time periods are the last day, the last week, the last month and the last three months.

**TOP N:** Set the quantity of displayed data by configuring TOP N. The optional values are 5, 10, 15 and 20, and 10 is displayed by default. After selection, the title in the component display effect will change with the user's choice.

**Refresh interval:** The interval of refreshing the component data. When the time range is the last day or the last week, the optional range is 10-3600 seconds. When the time range is the last month or the last three months, it can only be 300 seconds.

**Refresh time,** which can be set to show and hide. When set to hidden, the time range and refresh time in the chart are hidden.

**Alarm source:** Select the alarm source to be counted. The sources are divided into four categories: device group, device, interface group and interface. Select all or custom. The interface for selecting the alarm source is as follows:

Select the source: Refer to "Alarm Level Statistics".

Select device group: Refer to "Alarm Device TOP N".

Select device: Refer to "Device Alarm Statistics of Concerned Device".

Select interface and interface group: Refer to "Rate Monitoring of Concerned Interface".

Select the local network management: Refer to “Alarm Level Statistics”.

Alarm level: Select the alarm level to be counted, urgent, important, secondary, and tips, at least one of which should be selected.

Alarm type: Select the alarm type to be counted, all or custom. For the interface for selecting alarm type, refer to “Alarm Device TOP N”.

### 9.3.1.23. Alarm Radar

This component is used to display the 10 alarm devices that have alarms recently.

#### Display Effect



Figure 9-75 Alarm radar

The black font at the right of the component is the name of the alarm device, and the number in the chart is the number of the alarm devices.

#### Configuration Method

The component configuration interface is shown in the following figure:

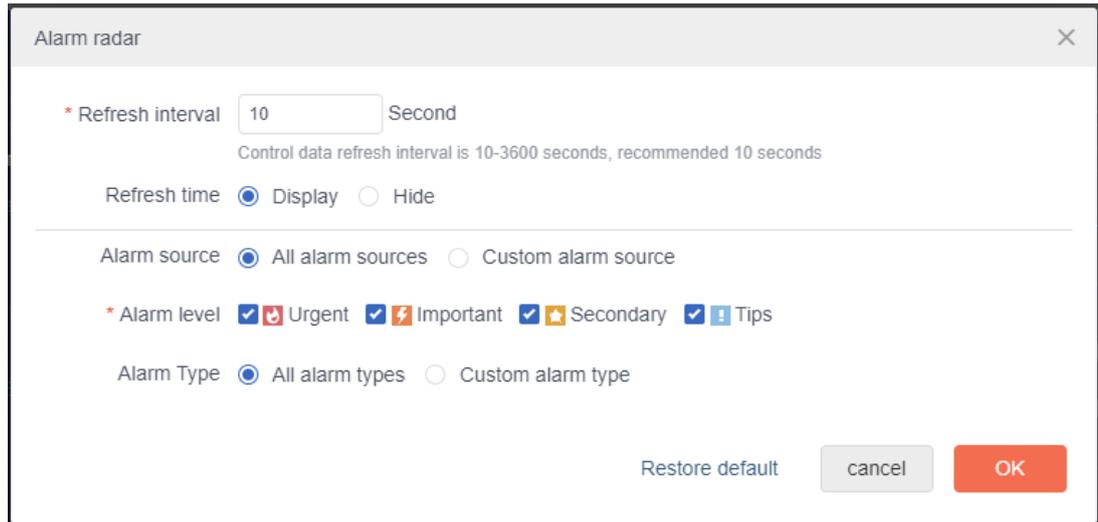


Figure 9-76 Alarm radar configuration interface

**Refresh interval:** used to control the refresh interval of the component data. The optional range is 10 – 3600 seconds.

**Refresh time,** which can be set to show and hide. When set to hidden, the time range and refresh time in the chart are hidden.

**Alarm source:** Select the alarm source to be counted. The sources are divided into four categories: device group, device, interface group and interface. Select all or custom. The interface for selecting the alarm source is as follows:

Select the source: Refer to “Alarm Level Statistics”.

Select device group: Refer to “Alarm Device TOP N”.

Select device: Refer to “Device Alarm Statistics of Concerned Device”.

Select interface and interface group: Refer to “Rate Monitoring of Concerned Interface”.

**Alarm level:** Select the alarm level to be counted, urgent, important, secondary, and tips, at least one of which should be selected.

**Alarm type:** Select the alarm type to be counted, all or custom. For the interface for selecting alarm type, refer to “Alarm Device TOP N”.

#### 9.3.1.24. Recent Alarm List

The component is used to display the recent 50 alarms.

##### Display Effect

Alarm source	Device name	Alarm level	Description	Alarm Type	Alarm times of the day	Occurrence time
<a href="#">10.11.12.211</a>	router	Important	Community name or snmpV3 au...	SNMP authentication failed	1	2020-07-03 02:41:27
<a href="#">10.11.12.211</a>	router	Important	Community name or snmpV3 au...	SNMP authentication failed	3	2020-07-02 08:36:46
<a href="#">10.11.12.14</a>	Switch	Important	Device Switch(10.11.12.14) offline.	Device offline	1	2020-07-01 13:21:07
<a href="#">10.11.12.211</a>	router	Important	Community name or snmpV3 au...	SNMP authentication failed	1	2020-07-01 01:17:34
<a href="#">10.11.12.211</a>	router	Important	Configuration file change, curren...	Device configuration change	1	2020-06-28 03:27:11

Figure 9-77 Recent alarm list

This component uses the form of list to display the basic information of the latest 50 alarms. Click the alarm source, and you can jump to the corresponding alarm interface.

### Configuration Method

The component configuration interface is shown in the following figure:

Recent alarm list

\* Refresh interval  Second  
Control data refresh interval is 10-3600 seconds, 60 seconds is recommended

Refresh time  Display  Hide

Display column  Alarm source  Device name  Alarm level  Description  Alarm Type  
 Alarm times of the day  Occurrence time

---

Alarm source  All alarm sources  Custom alarm source

\* Alarm level  Urgent  Important  Secondary  Tips

Alarm Type  All alarm types  Custom alarm type

Select alarm type

<input type="checkbox"/>	Alarm level	Alarm Type	Alarm group	Operation
No data				

Restore default

Figure 9-78 Recent alarm list configuration interface

**Refresh interval:** used to control the refresh interval of the component data. The optional range is 10 – 3600 seconds.

**Refresh time:** It can be set to show and hide. When set to hide, the time range and refresh time in the chart are hidden.

**Show column:** Display the fields in the chart. Alarm source, device name and alarm level are required, which cannot be modified. Description, device type, alarm times of the day and occurrence time are optional.

**Alarm source:** Select the alarm source to be counted. The sources are divided into five categories: device group, device, interface group, interface, and local network management. Select all or custom. The interface for selecting the alarm source is as follows:

Select the source: Refer to “Alarm Level Statistics”.

Select device group: Refer to “Alarm Device TOP N”.

Select device: Refer to “Device Alarm Statistics of Concerned Device”.

Select interface and interface group: Refer to “Rate Monitoring of Concerned Interface”.

Select local network management: Refer to “Alarm Level Statistics”.

Alarm level: Select the alarm level to be counted, urgent, important, secondary, and tips, at least one of which should be selected.

Alarm type: Select the alarm type to be counted, all or custom. For the interface for selecting alarm type, refer to “Alarm Device TOP N”.

## 9.3.2. Others

### 9.3.2.1. Big Screen External Component

This component can be embedded in external system link page.

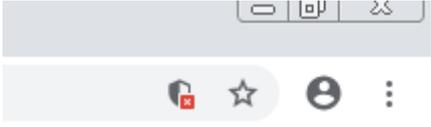
#### Display Effect



Figure 9-79 Big screen external component

Pay attention to the following points when configuring the link with HTTP protocol:

Google Browser: After the configuration is completed, click the alarm information on the

right side of the address bar , click “Load script”, and reload the page.

IE browser: Complete the configuration, save the component, click the alarm information below to display all contents, and then click to leave this page.

#### Configuration Method

The component configuration interface is shown in the following figure:

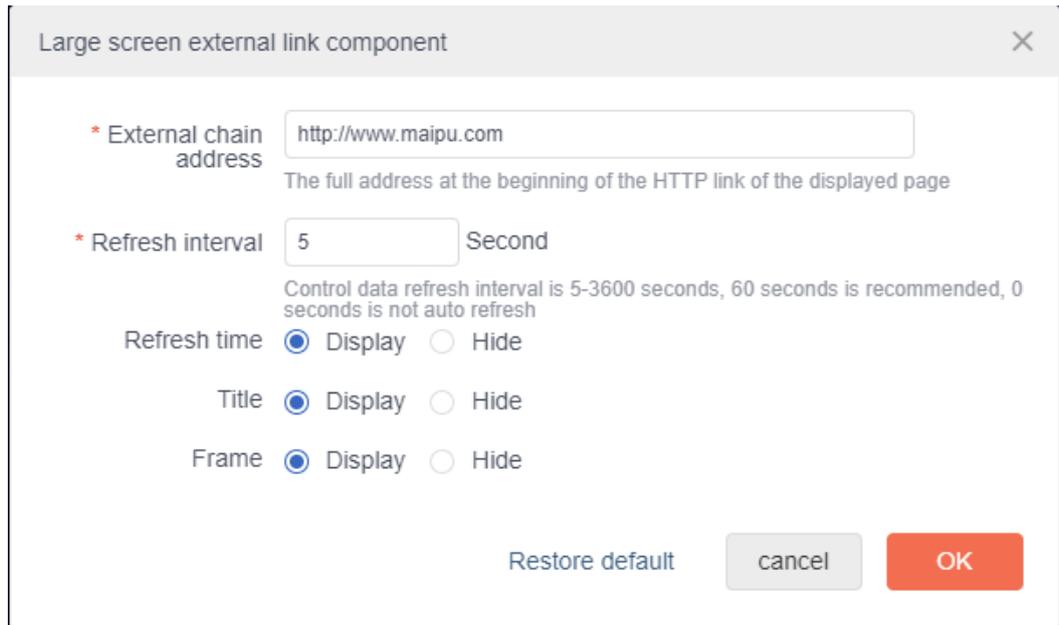


Figure 9-80 Big screen external component configuration interface

External address, the full address of the component embedded in the page, it must start with http.

Refresh interval: It controls the refresh interval of the component. The optional range is 5 – 3600 seconds, and 0 seconds means no auto refresh.

Refresh time: It can be set to display and hide. When it is set to hide, the refresh time in the chart is hidden.

Title: It can be set to display and hide. When it is set to hide, the title in the chart is hidden.

Frame: It can be set to display and hide. When it is set to hide, the frames in the chart are hidden.

### 9.3.2.2. Welcome

This component is the title running-horse lantern.

#### Display Effect

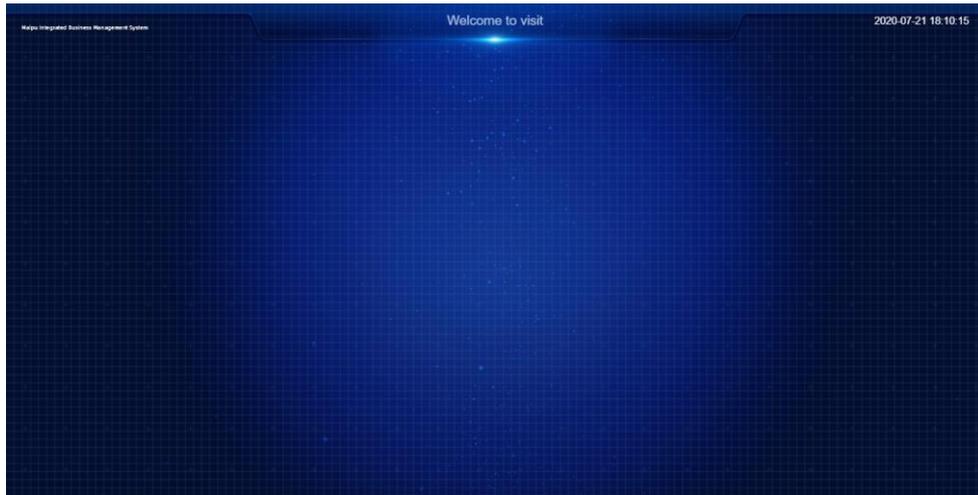


Figure 9-81 Welcome

The component consists of three parts: the logo image on the left, the title name in the middle, and the refresh time on the right.

### Configuration Method

The component configuration interface is shown in the following figure:

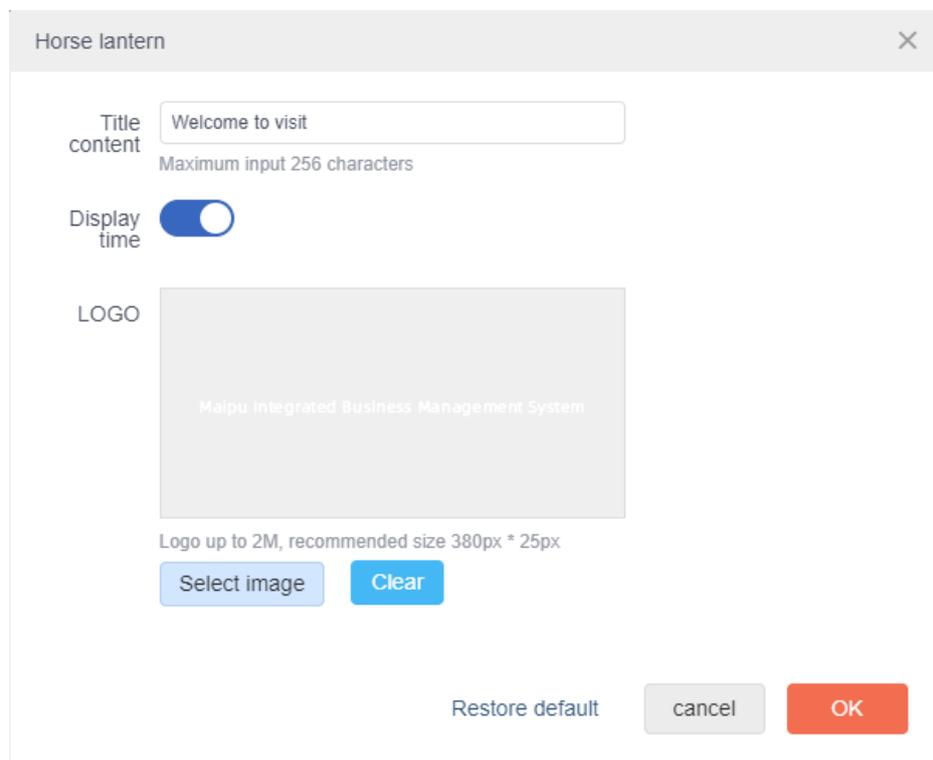


Figure 9-82 Welcome component configuration interface

Title content: The title displayed by the component, which can be input by oneself, and cannot exceed 256 characters.

Display time: It can be set to on/off state. When the setting is off, the refresh time in the

displayed content will be hidden.

LOGO: Control the logo on the left of the displayed content. Click “Select image” to select the logo image. The size cannot exceed 2M.

### 9.3.2.3. Pictures

The component is used to display the LOGO and other pictures.

#### Display Effect

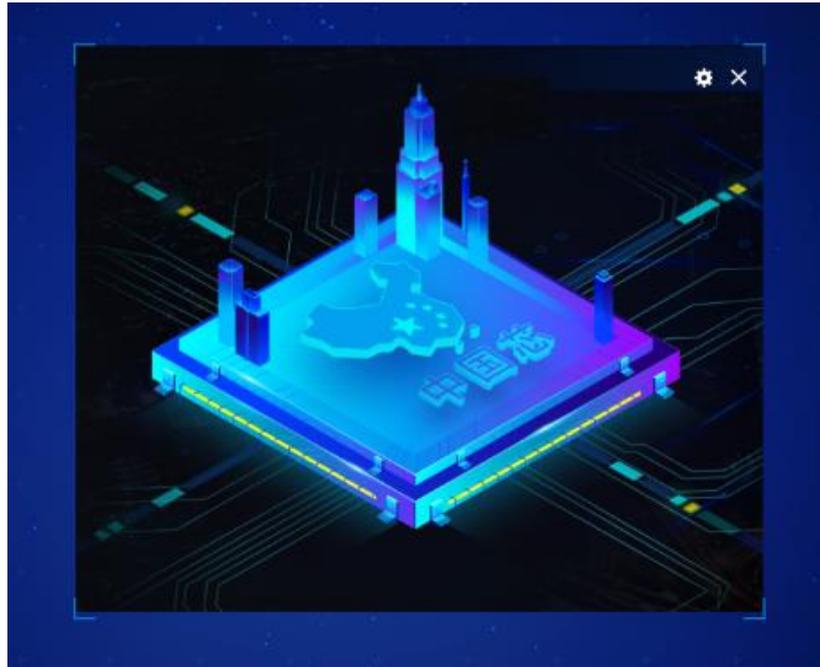


Figure 9-83 Picture component

After selecting the display picture on the component configuration interface, the effect as shown in the figure will be displayed.

#### Configuration Method

The component configuration interface is shown in the following figure:

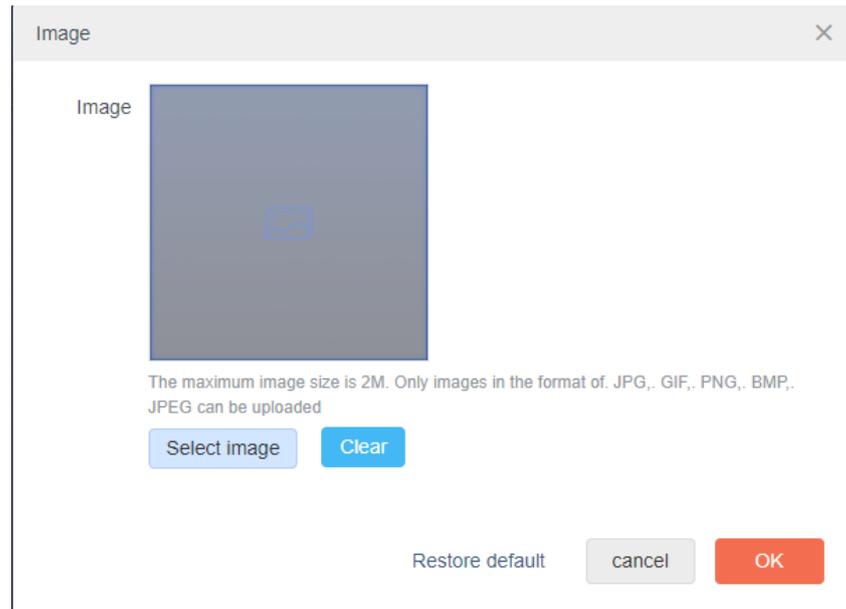


Figure 9-84 Picture component configuration interface

Picture: The selected picture is the displayed content of the component. Click “Select image” to select.

#### 9.3.2.4. Time

The component is used to display the time.

##### Display Effect

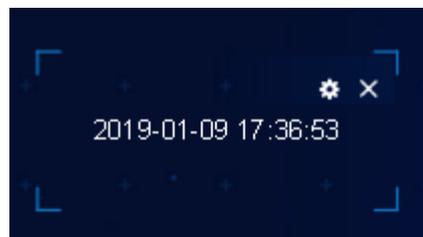
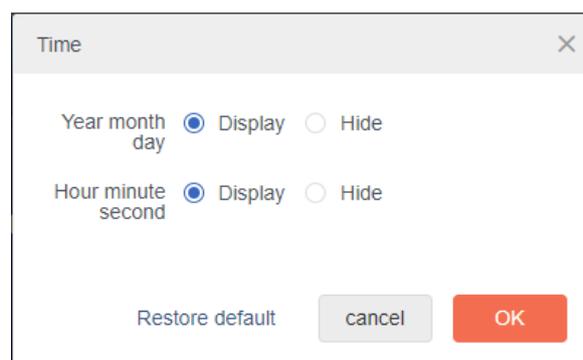


Figure 9-85 Time component

##### Configuration Method

The component configuration interface is shown in the following figure:



### Figure 9-86 Time component configuration interface

Year month day: It can be set to display and hide. When set to hide, the year, month and day in the displayed content will be hidden.

Hour minute second: It can be set to display and hide. When it is set to hide, the hours, minutes and seconds in the displayed content will be hidden (you must choose one of year month day and hour minute second).