BD-LAN Controller

User Manual

V2.1.1

迈普通信技术股份有限公司
www.maipu.com

Copyright

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 BD-LAN Controller. This manual tries to put each function of the system in the same chapter, so that when you need to use a certain function, you only need to view the corresponding chapter. The manual will specify the use of some interlaced functions if they cannot be put together.

I hope this manual can be helpful to your work!

Product Versions

The corresponding product versions of the manual are as follows:

Product Name	Product Model
BD-LAN Controller	BD-LAN V2.1.1

Version Description

The revision records describe all manual update information. The latest manual version contains all the previous manual update content.

Version No.	Product Version	Revision Date	Revised Content
V2.0	BD-LAN V2.1.1	2022-4-19	BD-LAN V2.1.1 released version, user manual

Audience

This documentation is intended for:

- Commissioning engineers
- 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

Conventions:

Format	Description
Note	An alert that contains additional or supplementary information.
Caution	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.
Warning	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
Boldface	Bold text represents commands and keywords that you enter literally as shown.
Italic	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

Obtaining Documentation

You can access the most up-to-date Maipu product documentation on the World Wide Web at www.maipu.com.

Technical Support

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

Documentation Feedback

You can feed back your opinions and suggestions by:

- Email: techsupport@maipu.com
- Technical hotline: 400-886-8669

Contents

1 Cluster Management

1.1 Overview

As the service requirements become larger and larger, the performance requirements for the service system become higher and higher. The traditional stand-alone deployment cannot meet the existing services, so the cluster mode based on distributed deployment appears to solve this problem. The cluster management system independently developed by the company has the characteristics of high availability, high performance and high concurrency, and can support horizontal and vertical expansion.

By entering the access address in the browser https://IP:8443, you can enter the login interface shown in the figure below to log in to the cluster management system. The default user name and password are admin.

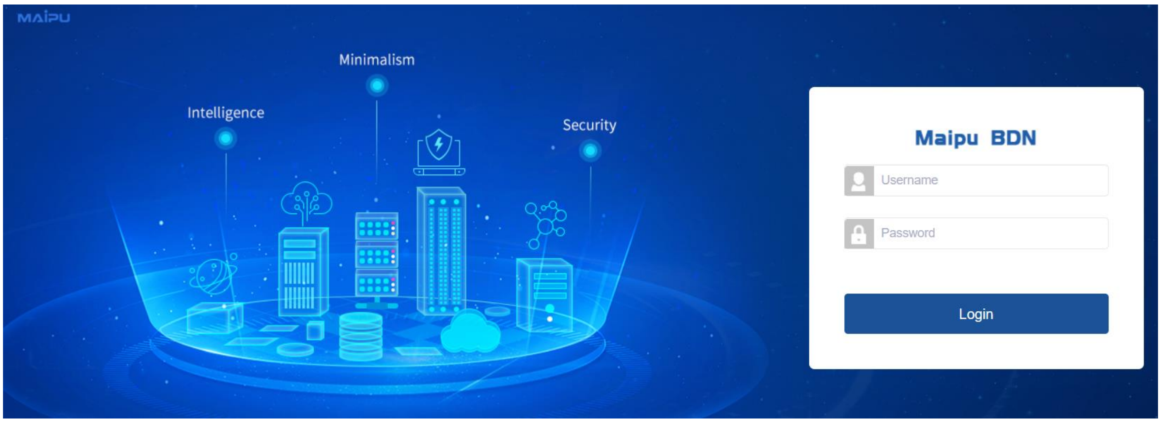
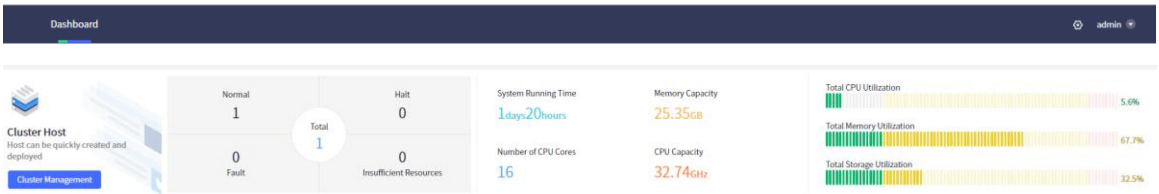


Figure 1.1.1 Login interface of cluster management

1.2 Cluster Deployment

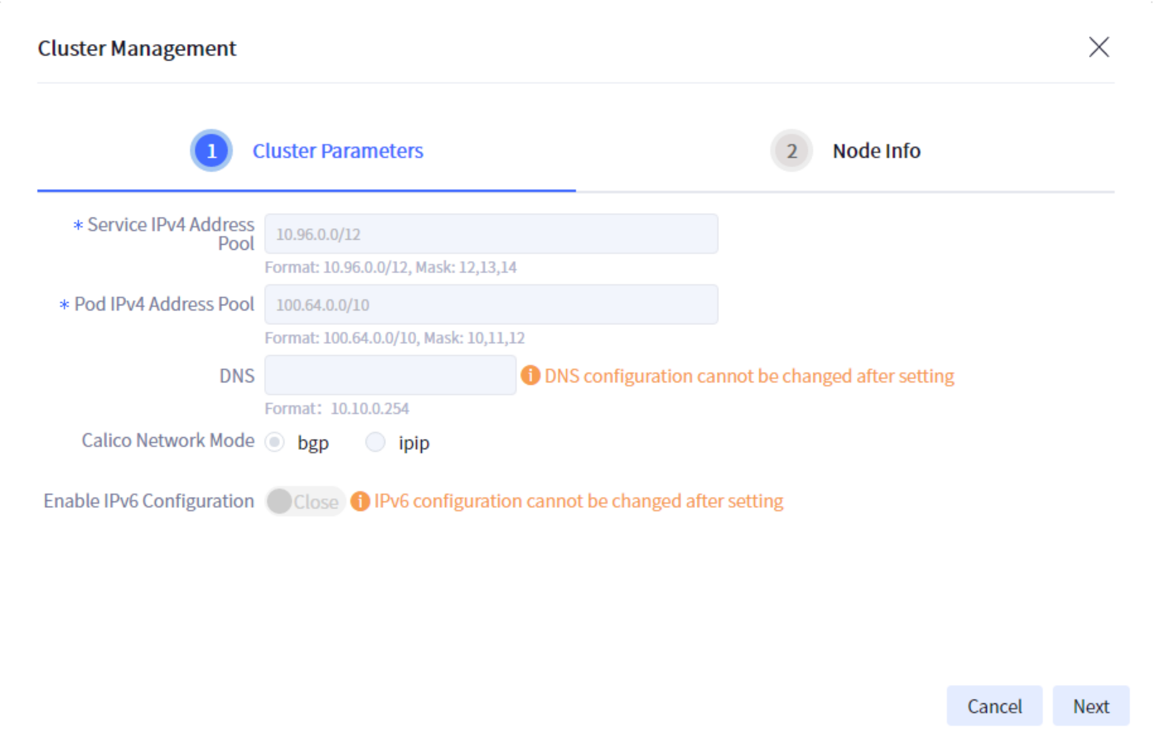
After logging in, enter the home page of the cluster management, as shown in the following figure:



Normal 1
Halt 0
Total 1
Fault 0
Insufficient Resources 0
System Running Time 1days20hours
Memory Capacity 25.35GB
Number of CPU Cores 16
CPU Capacity 32.74GHz
Total CPU Utilization 5.6%
Total Memory Utilization 67.7%
Total Storage Utilization 32.5%

Figure 1.2.1 Home page of cluster management

Click the **Cluster Management** button, and you can start to deploy the cluster, as shown in the following figure:



Cluster Management

1 Cluster Parameters

2 Node Info

* Service IPv4 Address Pool: 10.96.0.0/12

Format: 10.96.0.0/12, Mask: 12,13,14

* Pod IPv4 Address Pool: 100.64.0.0/10

Format: 100.64.0.0/10, Mask: 10,11,12

DNS:

DNS configuration cannot be changed after setting

Format： 10.10.0.254

Calico Network Mode: ● bgp ○ ipip

Enable IPv6 Configuration: Close

IPv6 configuration cannot be changed after setting

Figure 1.2.2 Cluster deployment parameters

Note

- Service and pod address pools generally do not need to be modified. If the address segment in the default address pool overlaps with the existing IP address segment in the current network, the default value needs to be modified.
- Calico network mode is bgp by default, and ipip is applicable to public cloud or scenarios with strict restrictions on host outgoing IP.
- IPv6 can only be enabled in the scenario where IPv6 is required, and the host needs to enable the IPv6 network.

The cluster parameters adopt the default values. Click **Next** to configure the node information.

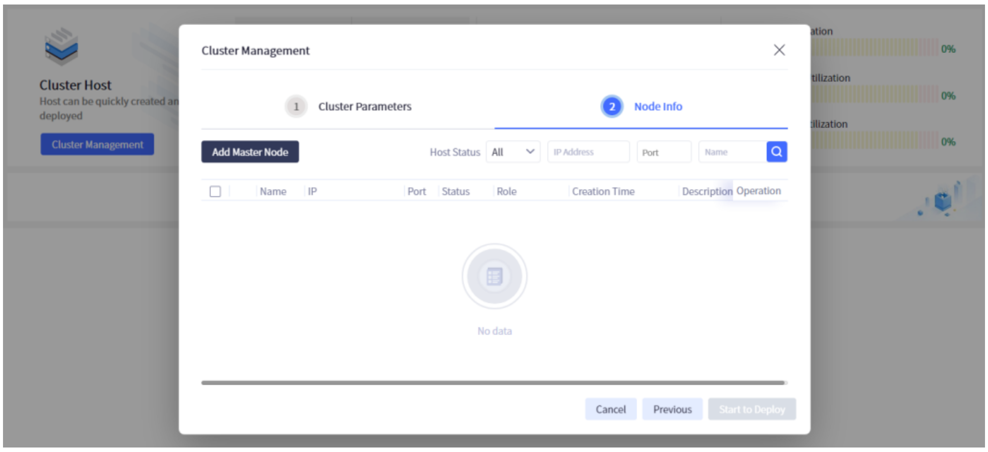
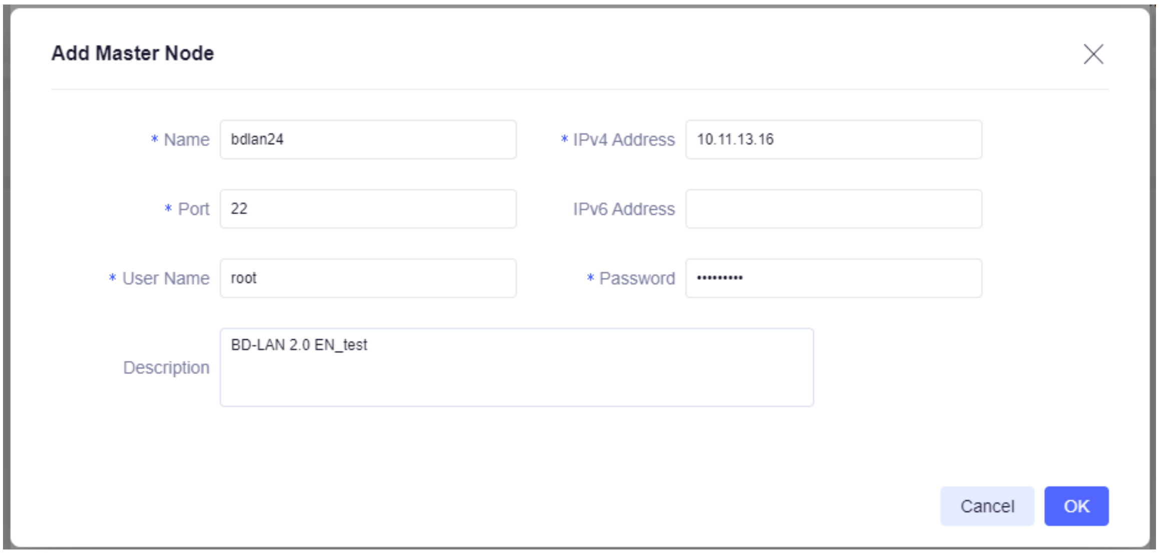


Figure 1.2.3 Cluster node information management

Click the "Add Master Node" button to set the master node information, where the IPv4 address is the IP address of the server where the cluster management system is installed; After the configuration is completed correctly, click **OK**.



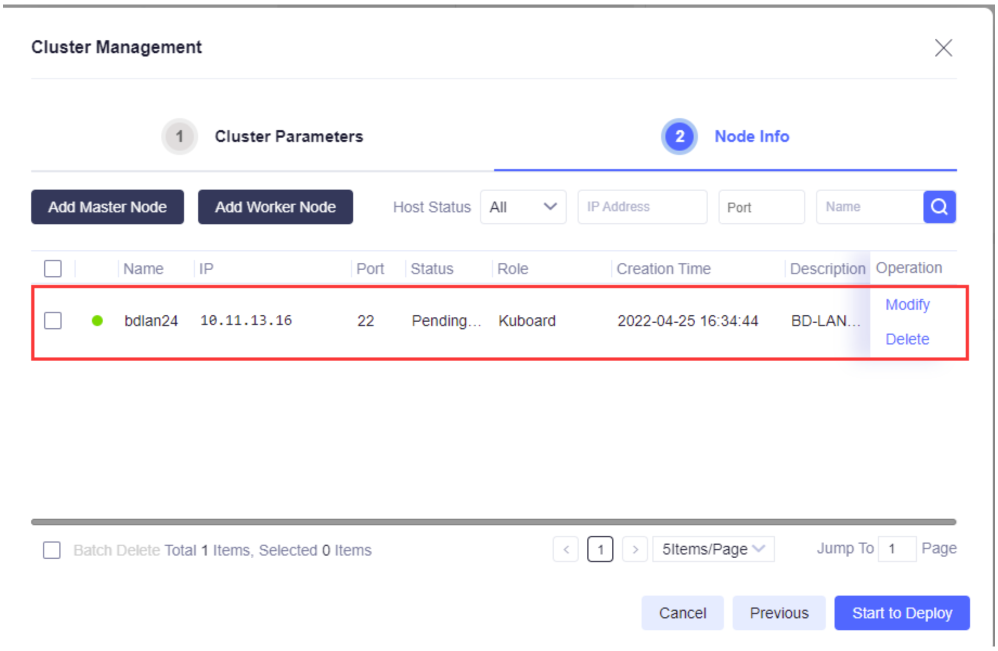
* Name: bdlan24
* IPv4 Address: 10.11.13.16
* Port: 22
IPv6 Address:
* User Name: root
* Password: •••••••••
Description: BD-LAN 2.0 EN_test

Figure 1.2.4 Cluster node information configuration

Note

- When adding the host, you can only use the root account.

After adding master node, click “Start to Deploy” to install automatically, and wait for the installation to be completed:



☐	Name	IP	Port	Status	Role	Creation Time	Description	Operation
☐ ●	bdlan24	10.11.13.16	22	Pending...	Kuboard	2022-04-25 16:34:44	BD-LAN...	Modify Delete

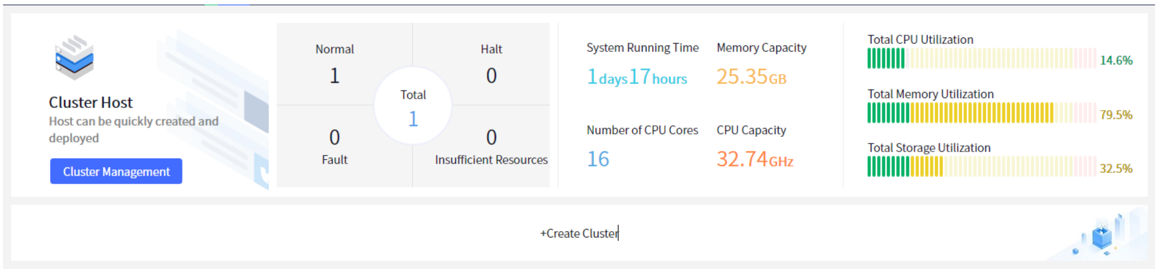
☐ Batch Delete Total 1 Items, Selected 0 Items

Figure 1.2.5 Cluster deployment node

Note

- Only stand-alone mode and 3+N cluster mode are supported. Stand-alone mode does not support highly available production environment and is not recommended.
- Click **Start to Deploy** after all hosts are added.

After installation, you need to add the cluster node, and click “Create Cluster”:



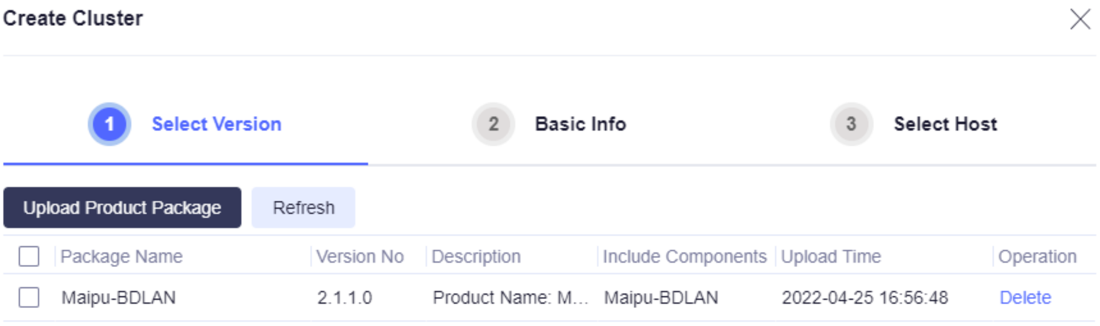
Normal 1
Halt 0
Total 1
Fault 0
Insufficient Resources 0

System Running Time 1days17hours
Memory Capacity 25.35GB
Number of CPU Cores 16
CPU Capacity 32.74GHz

Total CPU Utilization 14.6%
Total Memory Utilization 79.5%
Total Storage Utilization 32.5%

Figure 1.2.6 Create cluster

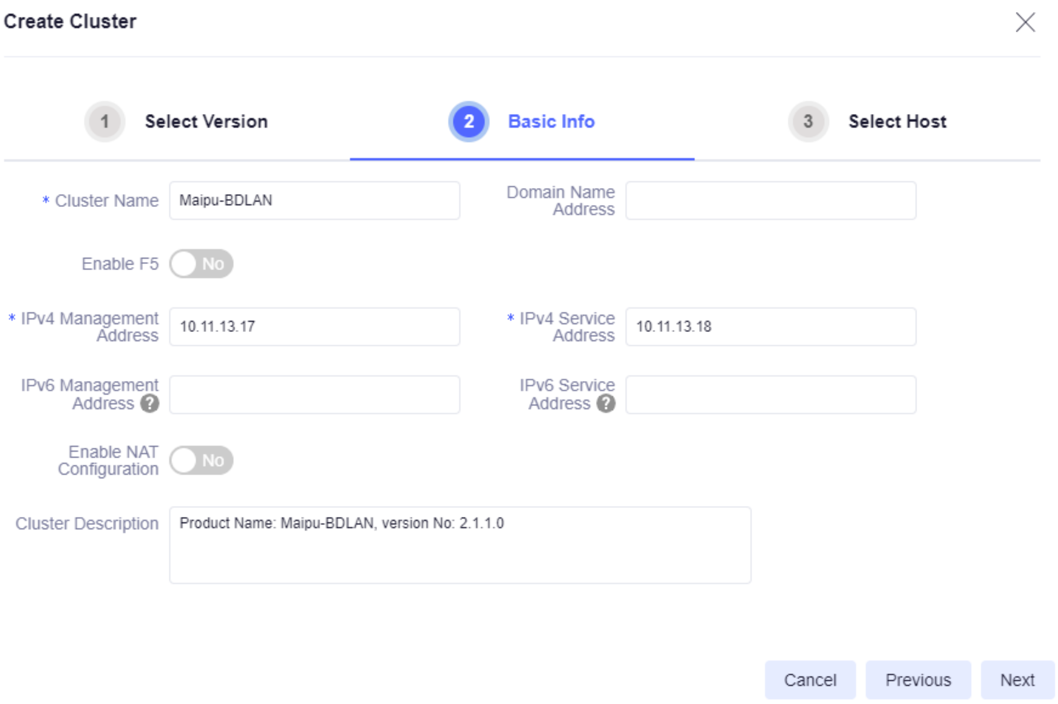
In the window of adding the cluster, upload the product package correctly:



☐	Package Name	Version No	Description	Include Components	Upload Time	Operation
☐	Maipu-BDLAN	2.1.1.0	Product Name: M...	Maipu-BDLAN	2022-04-25 16:56:48	Delete

Figure 1.2.7 Upload product package

Configure the basic information of the cluster node:


Create Cluster

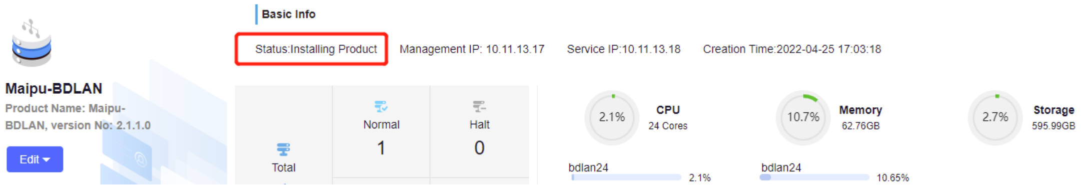
1 Select Version · 2 Basic Info · 3 Select Host

* Cluster Name: Maipu-BDLAN
Domain Name Address:
Enable F5: No
* IPv4 Management Address: 10.11.13.17
* IPv4 Service Address: 10.11.13.18
IPv6 Management Address:
IPv6 Service Address:
Enable NAT Configuration: No
Cluster Description: Product Name: Maipu-BDLAN, version No: 2.1.1.0

Figure 1.2.8 Configure service cluster information

Select cluster node host. It is not necessary to select the host during stand-alone installation. By default, click "Start to Create":

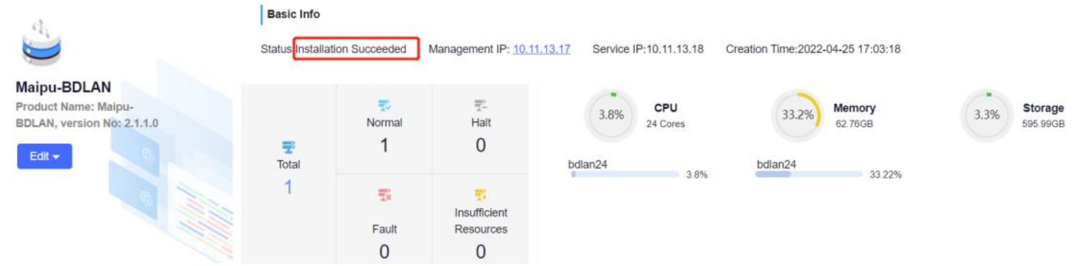
The system automatically installs cluster nodes. The status in the basic information of the node is displayed as "Installing Product". Users can wait for the auto installation to complete:


Maipu-BDLAN
Product Name: Maipu-BDLAN, version No: 2.1.1.0

Basic Info
Status:Installing Product   Management IP: 10.11.13.17   Service IP:10.11.13.18   Creation Time:2022-04-25 17:03:18

Figure 1.2.9 Wait for the service cluster to deploy

Wait until the status in the cluster node is displayed as "Installation succeeded", that is, the installation process is completed. The management IP is the IP address of the user accessing the page through the web, while the service IP is the IP address for interactive communication with the device. Many virtual IPs are built in the cluster for internal communication, and the external load balancer can automatically judge the load and send service requests to achieve high-performance operation, as shown in the following figure:


Maipu-BDLAN
Product Name: Maipu-BDLAN, version No: 2.1.1.0

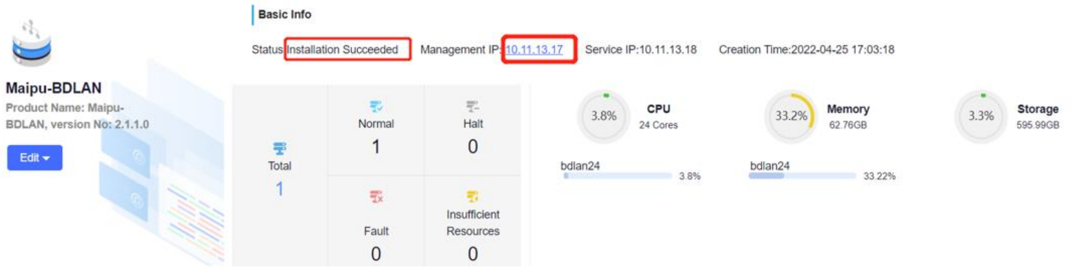
Basic Info
Status Installation Succeeded   Management IP: 10.11.13.17   Service IP:10.11.13.18   Creation Time:2022-04-25 17:03:18

Figure 1.2.10 Cluster deployment completed

Note

- Using external F5 requires adding corresponding load balancing rules to the external load balancer.

After deployment, the user can click **Management IP** to directly jump to the deployed cluster system, as shown in the following figure.



Basic Info

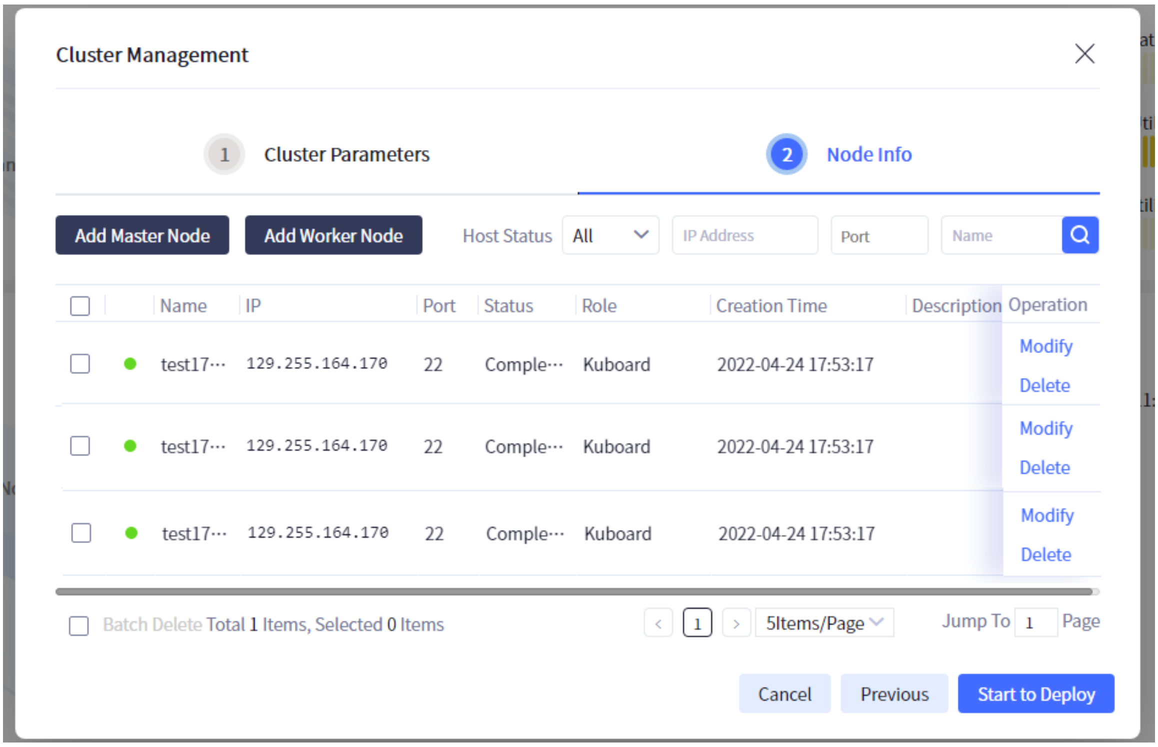
Status Installation Succeeded Management IP 10.11.13.17 Service IP:10.11.13.18 Creation Time:2022-04-25 17:03:18

Maipu-BDLAN

Product Name: Maipu-BDLAN, version No: 2.1.1.0

Figure 1.2.11 Jump to cluster system

If it is the deployment of the 3+N cluster mode, that is, add three master nodes as described above. After the three hosts are created, check the three hosts to start deployment at the same time.



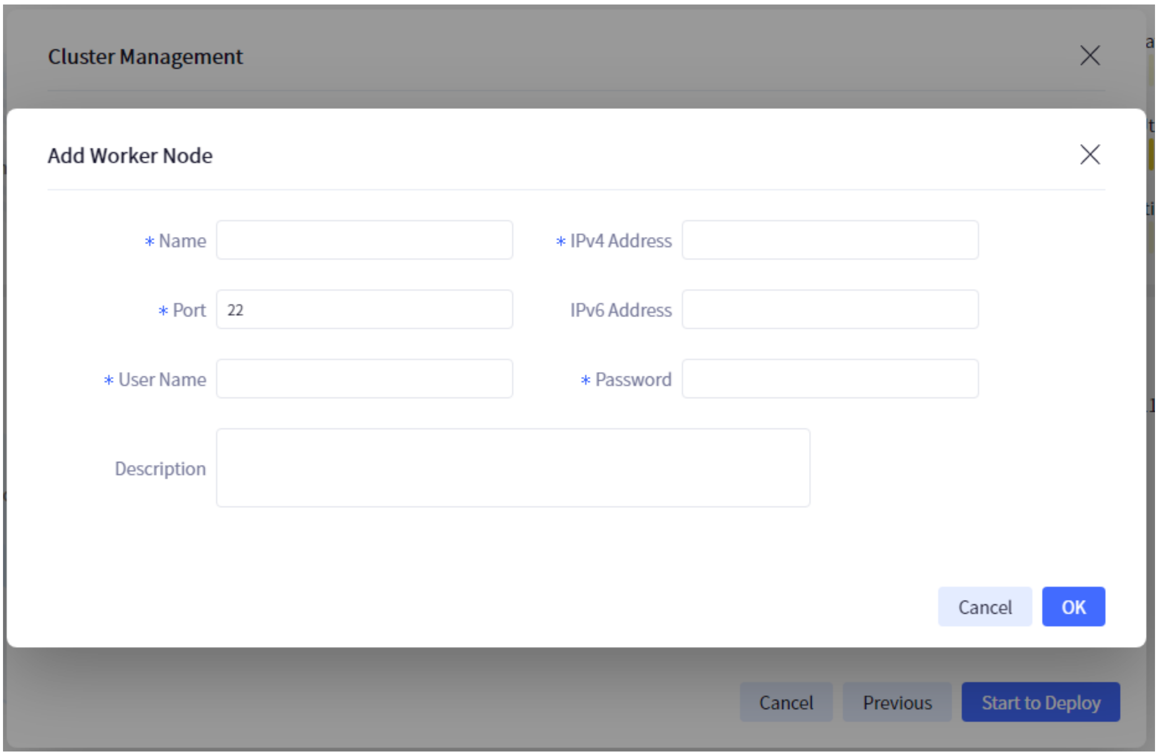
Cluster Management

☐		Name	IP	Port	Status	Role	Creation Time	Description	Operation
☐	●	test17···	129.255.164.170	22	Comple···	Kuboard	2022-04-24 17:53:17		Modify Delete
☐	●	test17···	129.255.164.170	22	Comple···	Kuboard	2022-04-24 17:53:17		Modify Delete
☐	●	test17···	129.255.164.170	22	Comple···	Kuboard	2022-04-24 17:53:17		Modify Delete

☐ Batch Delete Total 1 Items, Selected 0 Items

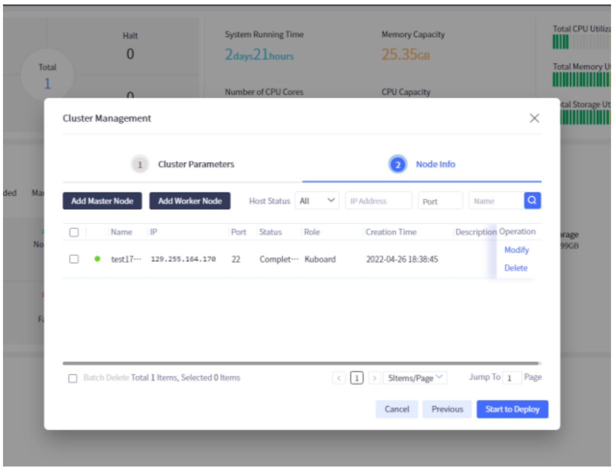
Figure 1.2.12 Three Master nodes

After the deployment of the three hosts is completed, create the cluster as described above. After the cluster is created, click **Cluster Management** again to add the worker node. After the worker node is created, click **Start to Deploy**, as shown in the following figure:



* Port 22

Figure 1.2.14 Add Worker node

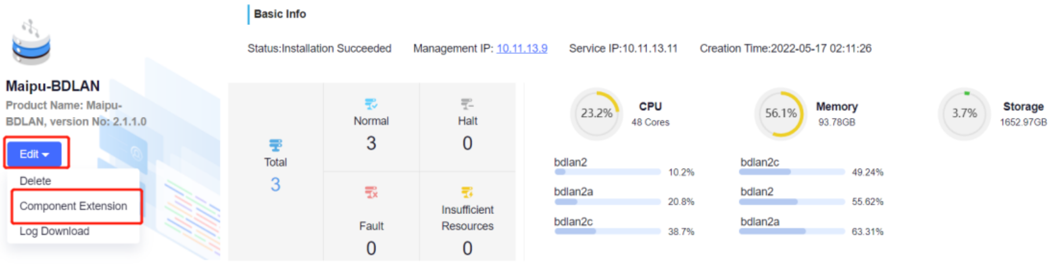


☐		Name	IP	Port	Status	Role	Creation Time	Description	Operation
☐	●	test17···	129.255.164.170	22	Complet···	Kuboard	2022-04-26 18:38:45		Modify Delete

Total 1 Items, Selected 0 Items

Figure 1.2.15 Deploy worker node

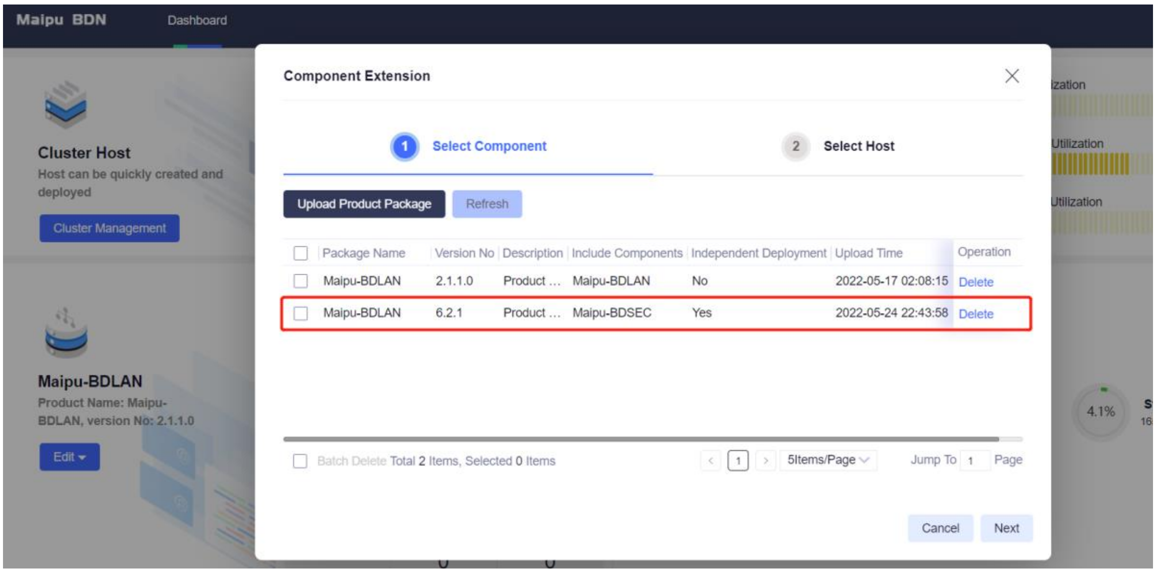
After the deployment of the worker node is completed, click **Edit**, select **Component Extension**, upload the installation package to be extended, click **Next**, select the worker host just deployed, and then click **Start to Extend** to wait for the installation to be completed, as shown in the following figure:



Status:Installation Succeeded Management IP: 10.11.13.9 Service IP:10.11.13.11 Creation Time:2022-05-17 02:11:26

Product Name: Maipu-BDLAN, version No: 2.1.1.0

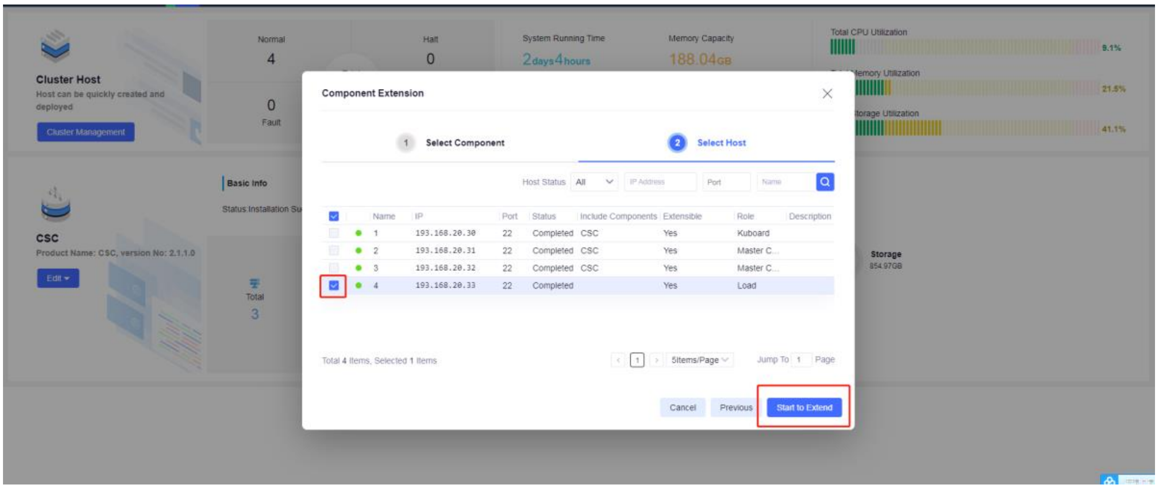
Figure 1.2.16 Component extension



☐	Package Name	Version No	Description	Include Components	Independent Deployment	Upload Time	Operation
☐	Maipu-BDLAN	2.1.1.0	Product ...	Maipu-BDLAN	No	2022-05-17 02:08:15	Delete
☐	Maipu-BDLAN	6.2.1	Product ...	Maipu-BDSEC	Yes	2022-05-24 22:43:58	Delete

Total 2 Items, Selected 0 Items 1 5Items/Page Jump To 1 Page

Figure 1.2.16 Upload product package



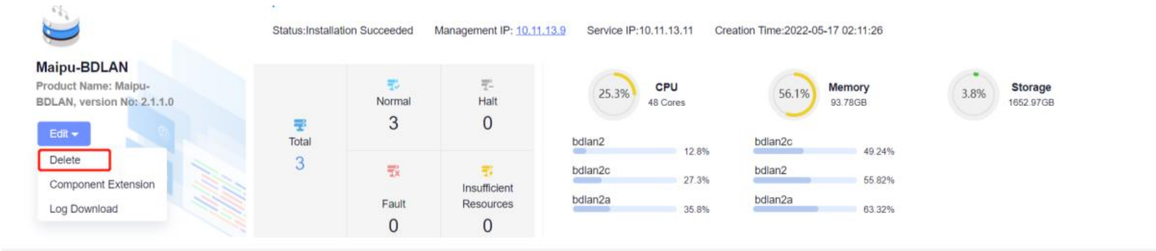
Host Status All

☑		Name	IP	Port	Status	Include Components	Extensible	Role	Description
☐	●	1	193.168.20.30	22	Completed	CSC	Yes	Kuboard	
☐	●	2	193.168.20.31	22	Completed	CSC	Yes	Master C...	
☐	●	3	193.168.20.32	22	Completed	CSC	Yes	Master C...	
☑	●	4	193.168.20.33	22	Completed		Yes	Load	

Total 4 Items, Selected 1 Items 1 5Items/Page Jump To 1 Page

Figure 1.2.17 Select the installation node of extension product package

The user can select to delete the deployed cluster, as shown in the following figure:



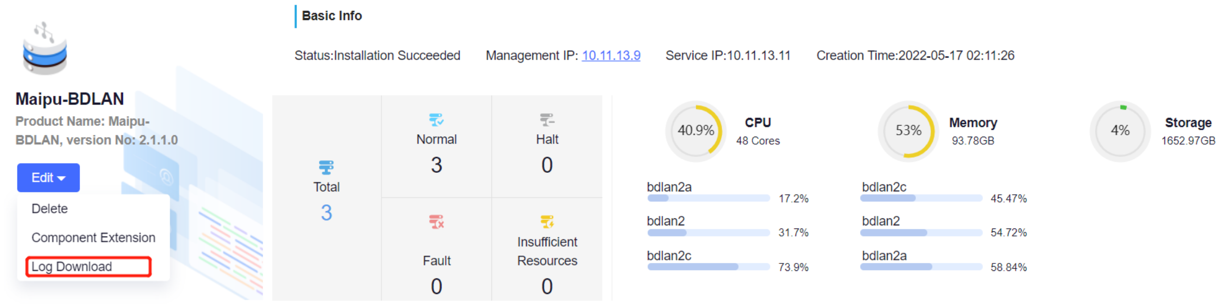
Status:Installation Succeeded Management IP: 10.11.13.9 Service IP:10.11.13.11 Creation Time:2022-05-17 02:11:26

Figure 1.2.18 Delete the cluster

Caution

- After deleting a service cluster, all service data will be deleted. Be careful.

The user can select to download the cluster log, as shown in the following figure:



Product Name: Maipu-BDLAN, version No: 2.1.1.0

Status:Installation Succeeded Management IP: 10.11.13.9 Service IP:10.11.13.11 Creation Time:2022-05-17 02:11:26

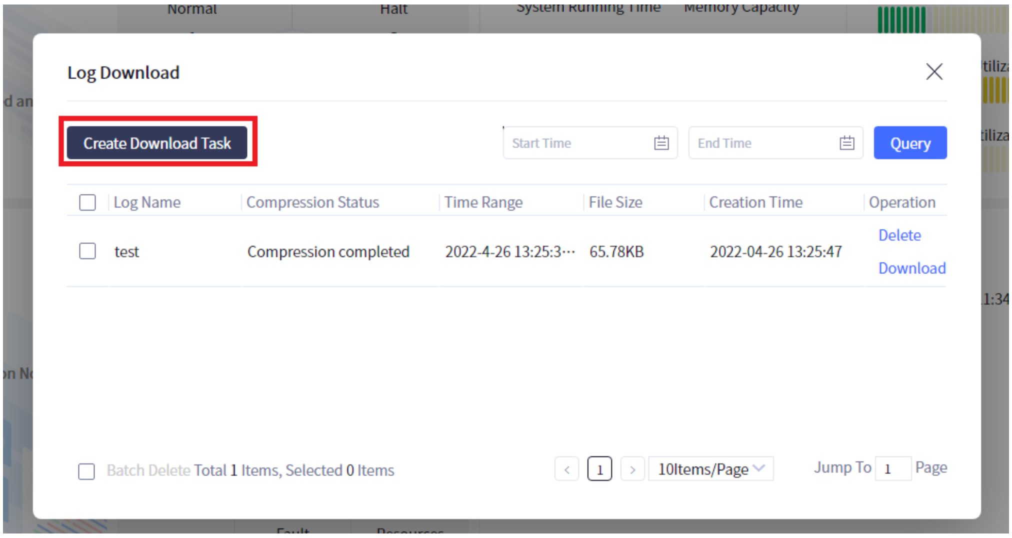
Total	3
Normal	3
Halt	0
Fault	0
Insufficient Resources	0

CPU 40.9% 48 Cores
Memory 53% 93.78GB
Storage 4% 1652.97GB

CPU		Memory	
bdlan2a	17.2%	bdlan2c	45.47%
bdlan2	31.7%	bdlan2	54.72%
bdlan2c	73.9%	bdlan2a	58.84%

Figure 1.2.19 Download cluster logs

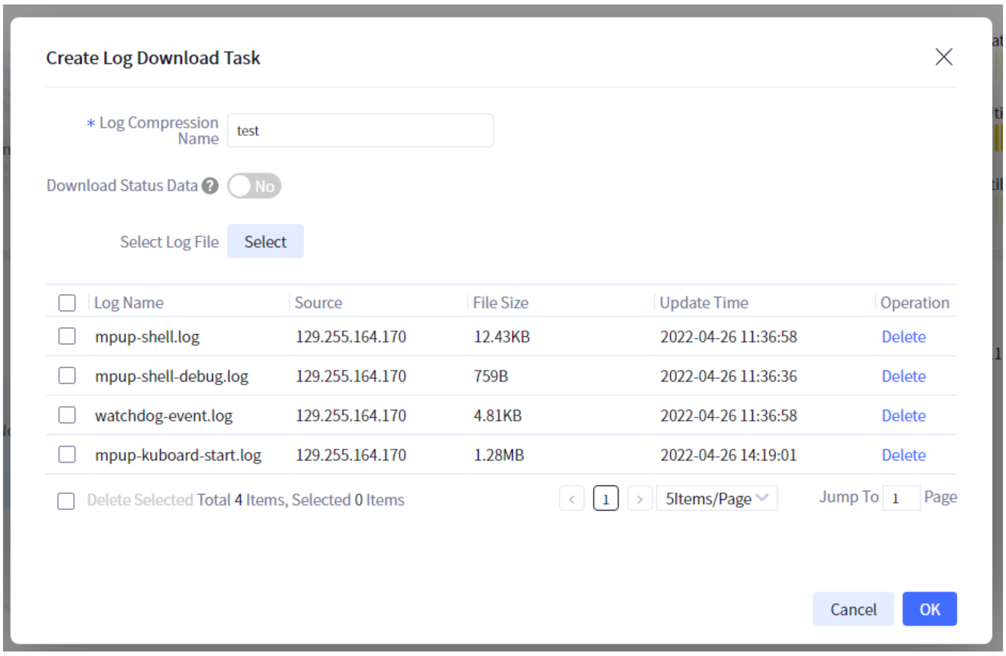
Click the **Log Download** button to enter the log download pop-up page. Click the **Create Download Task** button to start creating a log download task. The log compression name is required. You can choose whether to download status data. If choosing **Yes**, you can create a task directly without selecting log files. You can select multiple log files to download at the same time.



☐	Log Name	Compression Status	Time Range	File Size	Creation Time	Operation
☐	test	Compression completed	2022-4-26 13:25:3···	65.78KB	2022-04-26 13:25:47	Delete Download

☐ Batch Delete Total 1 Items, Selected 0 Items

Figure 1.2.20 Log downloading



* Log Compression Name: test

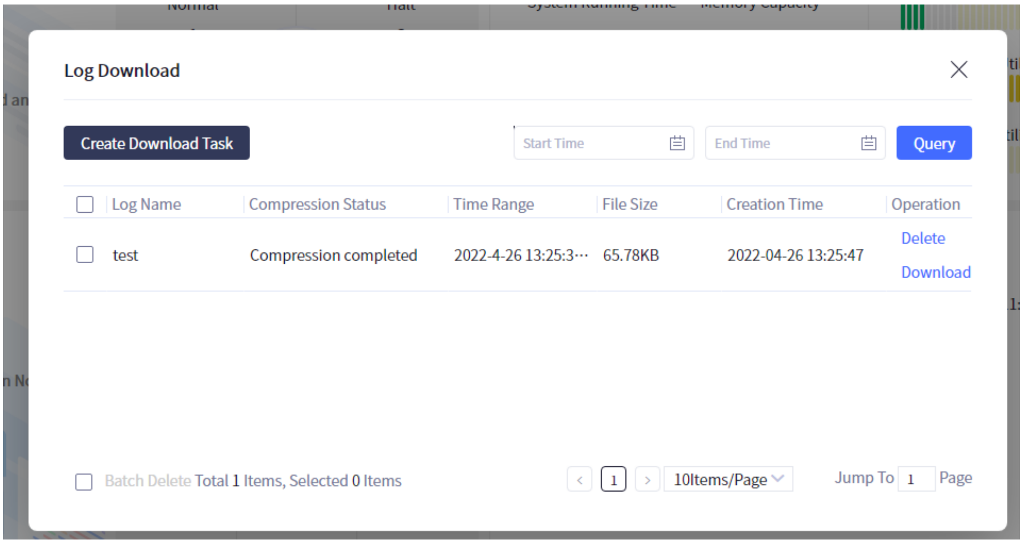
Download Status Data: No

Select Log File: Select

☐	Log Name	Source	File Size	Update Time	Operation
☐	mpup-shell.log	129.255.164.170	12.43KB	2022-04-26 11:36:58	Delete
☐	mpup-shell-debug.log	129.255.164.170	759B	2022-04-26 11:36:36	Delete
☐	watchdog-event.log	129.255.164.170	4.81KB	2022-04-26 11:36:58	Delete
☐	mpup-kuboard-start.log	129.255.164.170	1.28MB	2022-04-26 14:19:01	Delete

☐ Delete Selected Total 4 Items, Selected 0 Items

Figure 1.2.21 Create log download task



☐	Log Name	Compression Status	Time Range	File Size	Creation Time	Operation
☐	test	Compression completed	2022-4-26 13:25:3···	65.78KB	2022-04-26 13:25:47	Delete Download

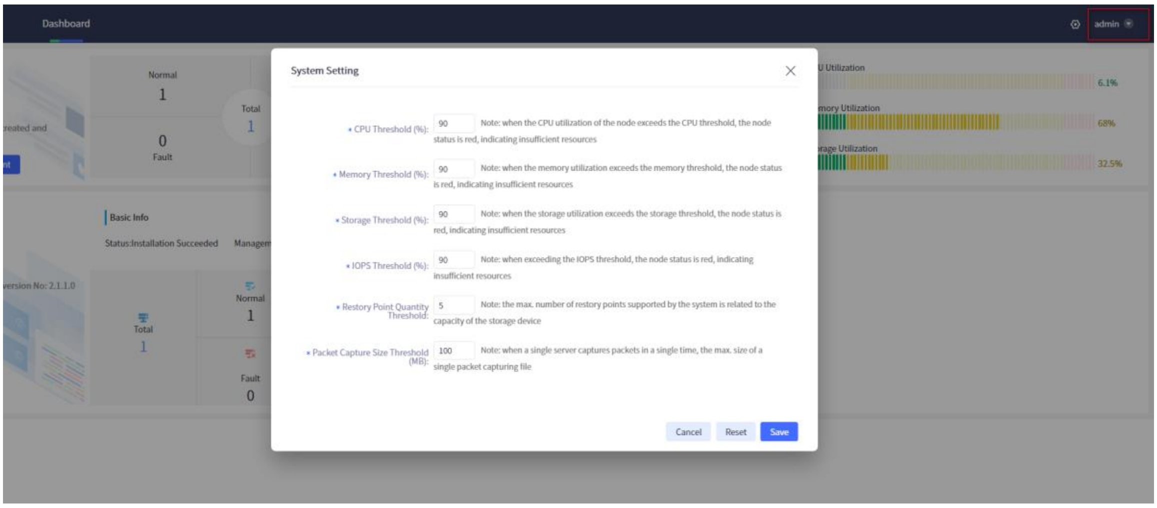
☐ Batch Delete Total 1 Items, Selected 0 Items

Figure 1.2.22 Creating log downloading task completed

You can choose to delete and download the created task, and download the log compressed package in zip format.

1.3 Cluster Configuration

Users can set the configuration of cluster management. Click the **Setting** button to customize the threshold of each configuration item, as shown in the figure below.



- CPU Threshold (%): 90 Note: when the CPU utilization of the node exceeds the CPU threshold, the node status is red, indicating insufficient resources
- Memory Threshold (%): 90 Note: when the memory utilization exceeds the memory threshold, the node status is red, indicating insufficient resources
- Storage Threshold (%): 90 Note: when the storage utilization exceeds the storage threshold, the node status is red, indicating insufficient resources
- IOPS Threshold (%): 90 Note: when exceeding the IOPS threshold, the node status is red, indicating insufficient resources
- Restory Point Quantity Threshold: 5 Note: the max. number of restory points supported by the system is related to the capacity of the storage device
- Packet Capture Size Threshold (MB): 100 Note: when a single server captures packets in a single time, the max. size of a single packet capturing file

Figure 1.3.1 Threshold configuration

Click the **Modify Password** button to modify the admin user password of cluster management, as shown in the following figure.

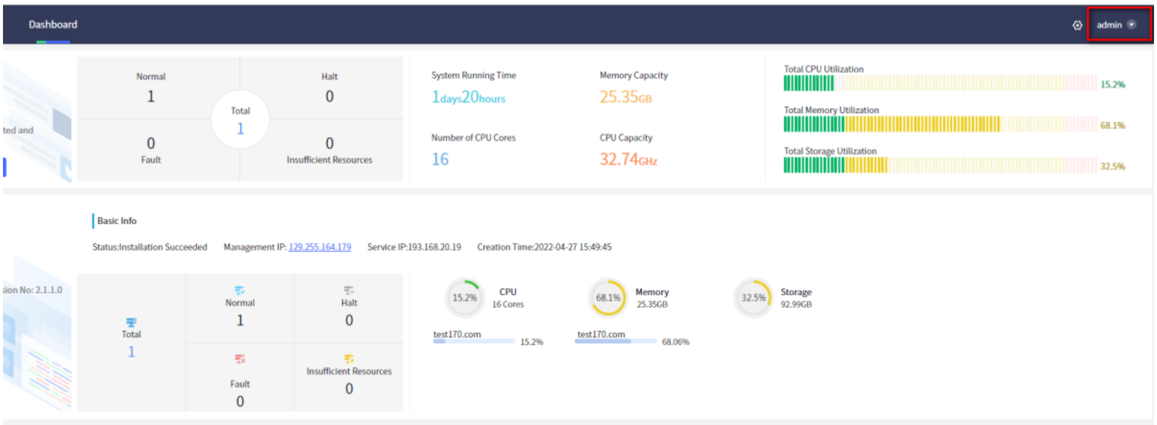


Figure 1.3.2 Modify admin password of cluster management

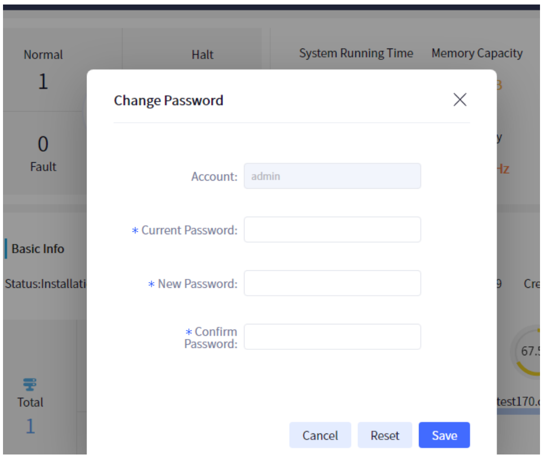


Figure 1.3.3 Modify password configuration

Click the **Exit** button, and you can exit the current cluster management system, as shown in the figure below.

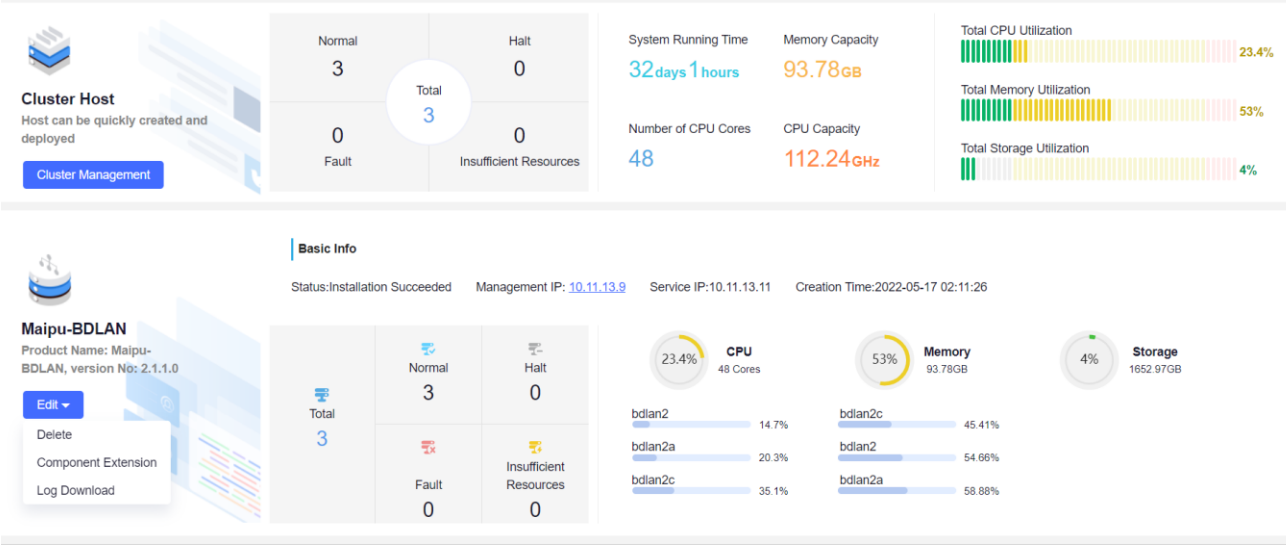
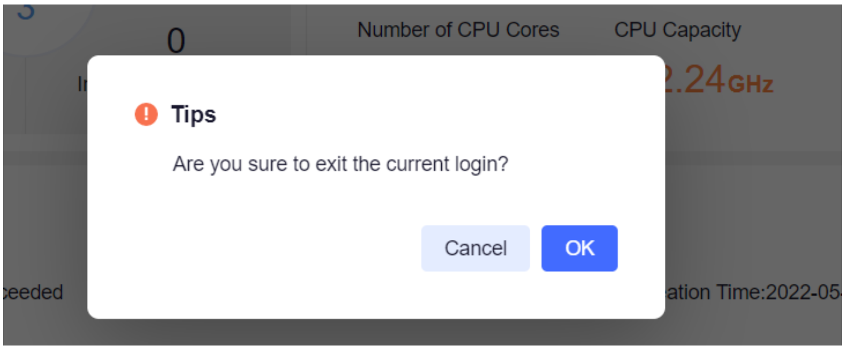


Figure 1.3.4 Exit system button



Tips

Are you sure to exit the current login?

Figure 1.3.5 Exit system

2 System Login

Click the cluster system management IP in the cluster management system, or use the browser to enter the cluster system management address (such as: https://192.168.100.7), and you can access the system login interface. Enter the username and password: *admin/admin* (the default administrator user of the system) to enter the system home page, as shown in the figure below. Since some functions in the system require the browser to support HTML5 and other features, the system recommends using Google Chrome V59 and the latest stable version above to achieve the best experience effect. Click the "Browser" icon to download the browser. For example, click the "Google browser" icon to download Google Chrome.

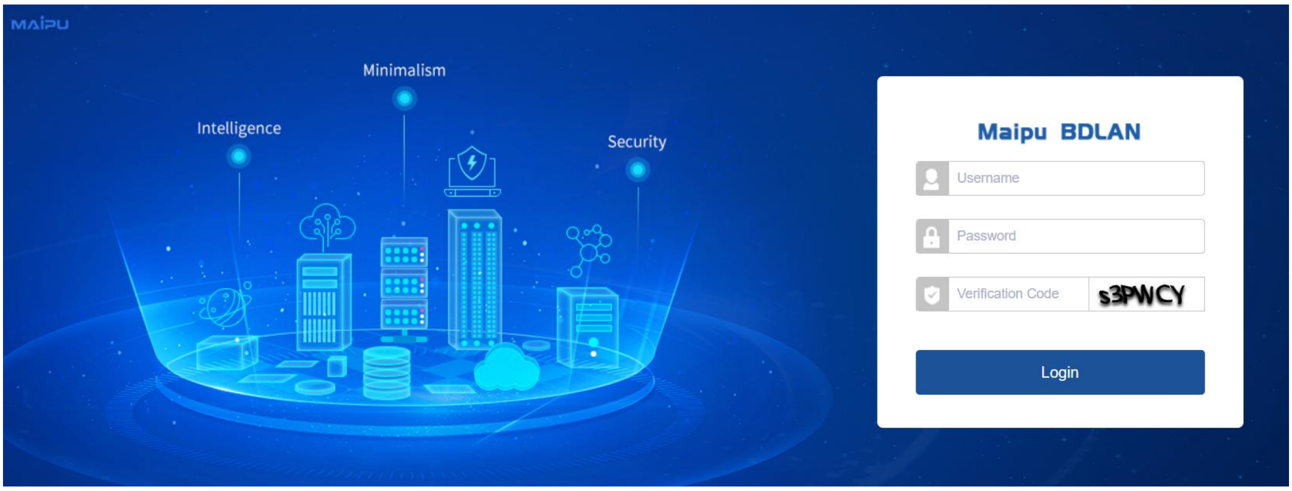
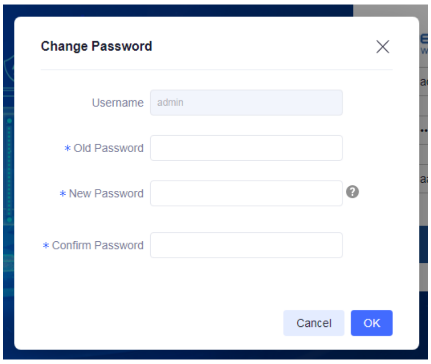


Figure 1.3 System login

The user needs to modify the password when logging in for the first time.



Username: admin

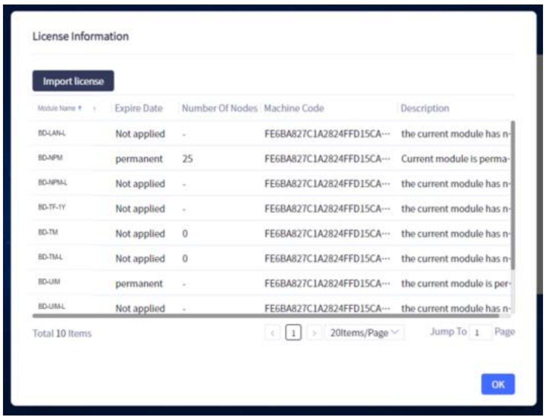
* Old Password

* New Password

* Confirm Password

Figure 1.3 Modify the password

After the first login, you will be prompted that there is no license information. In the prompt interface, you can click the button to import the license. After importing successfully, click the **OK** button to log in to the system. All license modules must be purchased and imported before entering the system. There will be a prompt on this page only when the license is not imported or the license is about to expire.


License Information

Module Name	Expire Date	Number Of Nodes	Machine Code	Description
BD-LAN-L	Not applied	-	FE6BA827C1A2824FFD15CA···	the current module has n-
BD-NPM	permanent	25	FE6BA827C1A2824FFD15CA···	Current module is perma-
BD-NPM-L	Not applied	-	FE6BA827C1A2824FFD15CA···	the current module has n-
BD-TF-1Y	Not applied	-	FE6BA827C1A2824FFD15CA···	the current module has n-
BD-TM	Not applied	0	FE6BA827C1A2824FFD15CA···	the current module has n-
BD-TM-L	Not applied	0	FE6BA827C1A2824FFD15CA···	the current module has n-
BD-UM	permanent	-	FE6BA827C1A2824FFD15CA···	the current module is per-
BD-UM-L	Not applied	-	FE6BA827C1A2824FFD15CA···	the current module has n-

Total 10 Items

Figure 1.3 Import license

After logging in successfully, enter the home page. For details, refer to Chapter 3 “Home Page”.

3 Home Page

The home page will generate two default templates by default: overview and basic network. The overview is selected by default. The display content is mainly the statistics of some data that the controller pays attention to. By default, the overview includes 7 components: System score, terminal authentication statistics, terminal types, basic network topology, asset statistics, counterfeit terminal, and recent alarms. By default, the basic network includes six components: device status statistics, alarm type statistics, device type statistics, comprehensive monitoring of device availability, recent alarm list and comprehensive monitoring of interface (the number of real-time alarms displayed at the top of the page will be displayed on each page). Their contents will be introduced respectively below:

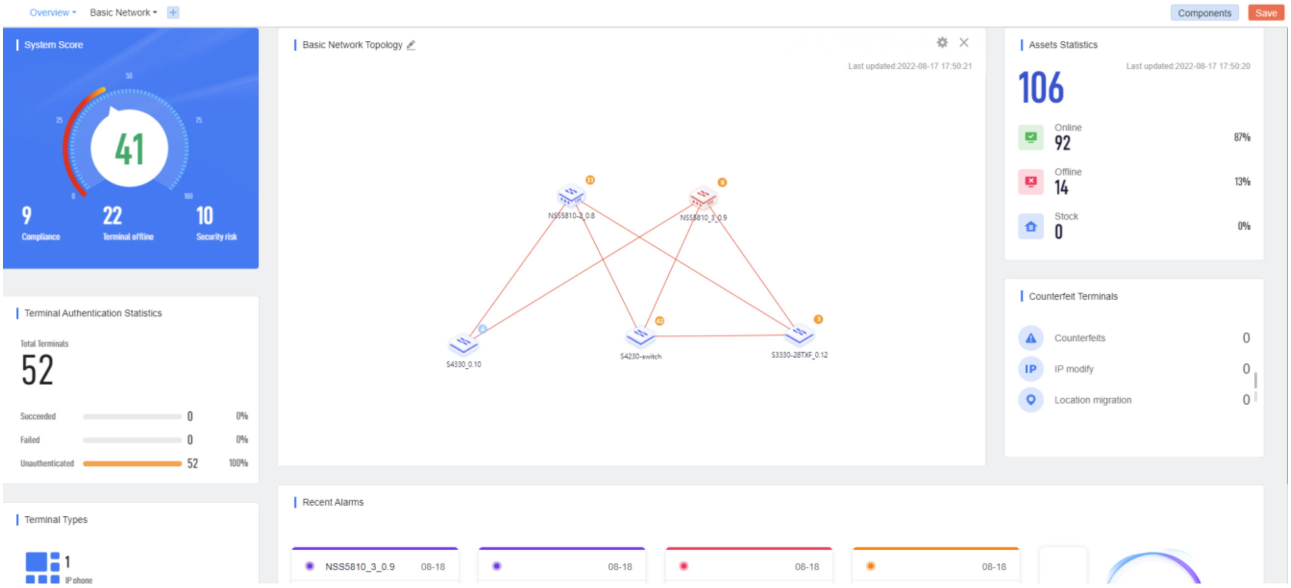


Figure 3.1 Home page

The following introduces the functions on the home page in turn:

Add template

The user can customize the template by clicking +. The current template is divided to three kinds: blank template, overview, and basic network, as shown in the following figure:

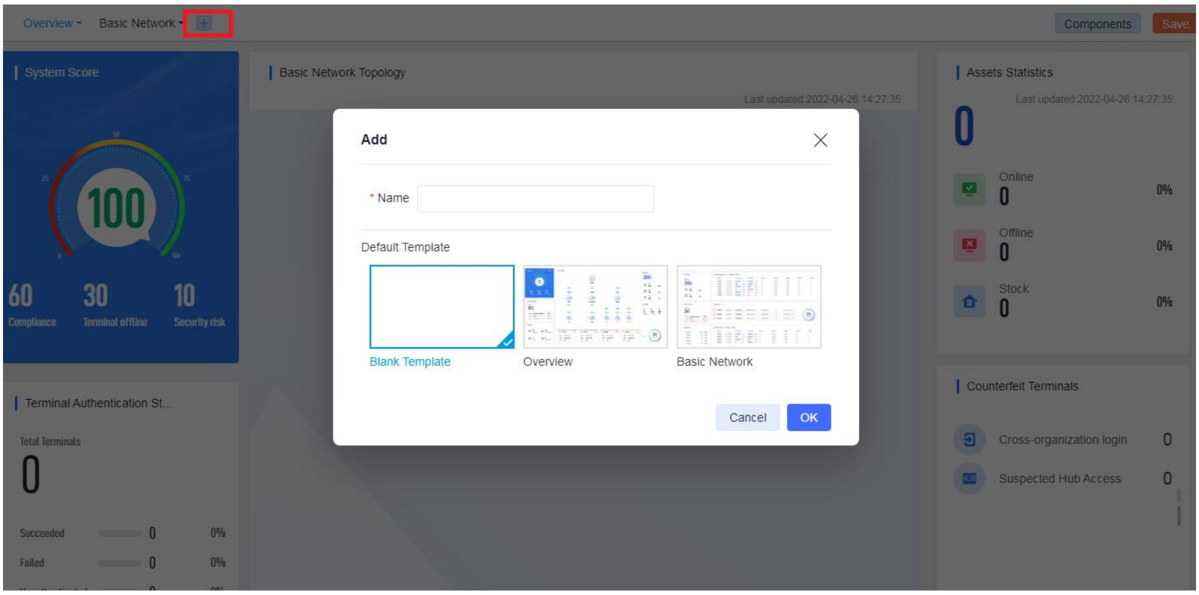


Figure 3.2 Add a template

The blank template does not contain any components. Users need to add the components to be monitored to the template by themselves.

The overview template contains the components of some terminals and asset statistics and alarms, which can be used directly by users.

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 template includes asset profile and basic network) has no deletion function; The customized template (the template added by the user) does not restore the default function, but has the deletion function, as shown in the following figure:

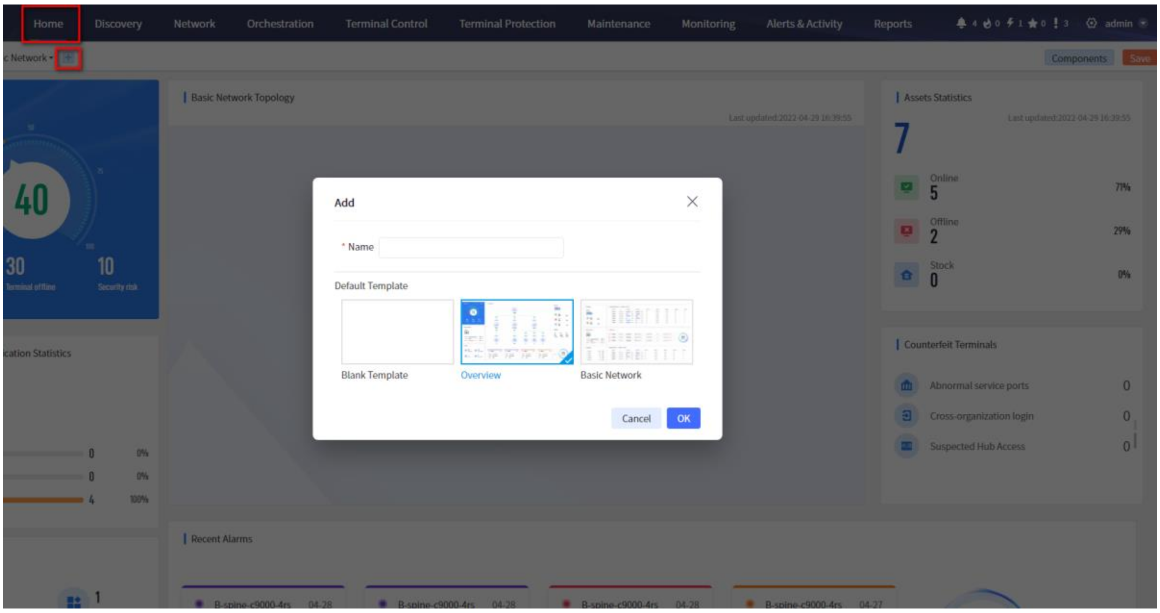


Figure 3.3 Edit default template

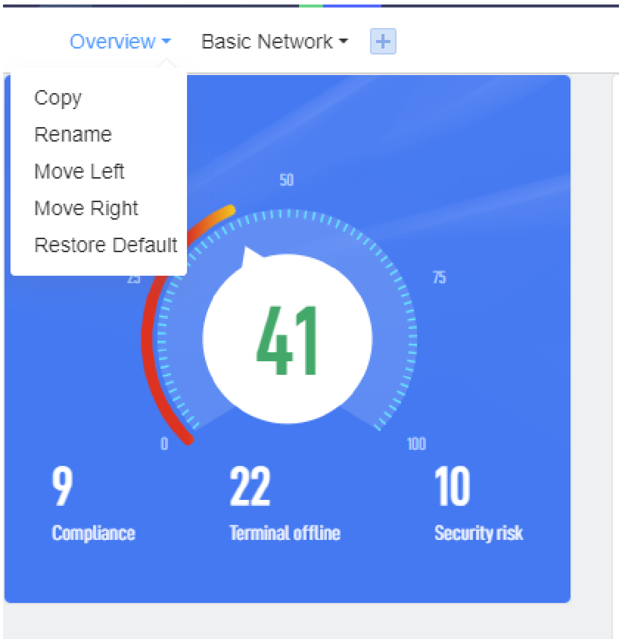


Figure 3.4 Edit customized template

Copy template

Click "Copy" in the above figure to pop up a pop-up layer containing the name input box. Enter the name and click **OK** to copy the content of the current template to the new template.

Rename template

Click "Rename" in Figure 3.4, and the template name will be presented in editable state. After the user edits the template name again, the edited content can be saved by losing the focus of the input box.

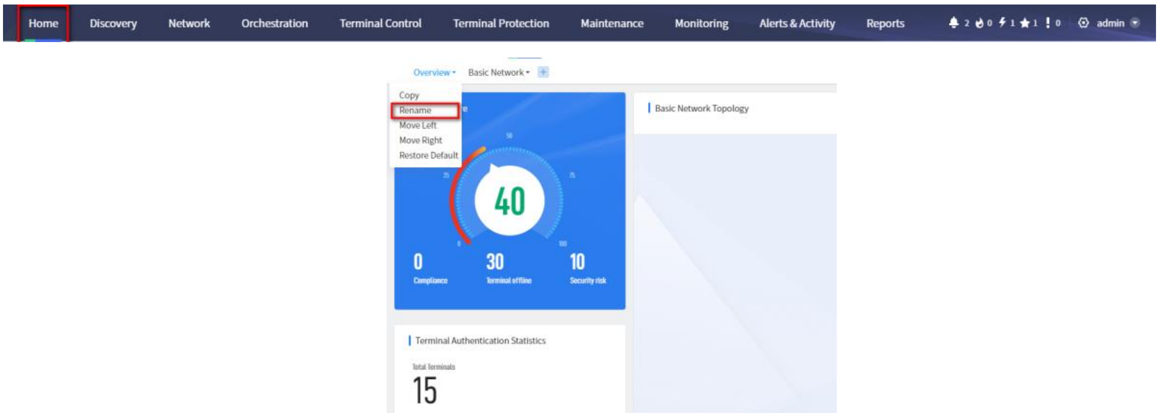


Figure 3.5 Rename the template

Move left and move right the template

Click “Move Left”, “Move Right” in Figure 3.4, and the template name will be moved left or right.

Delete the template

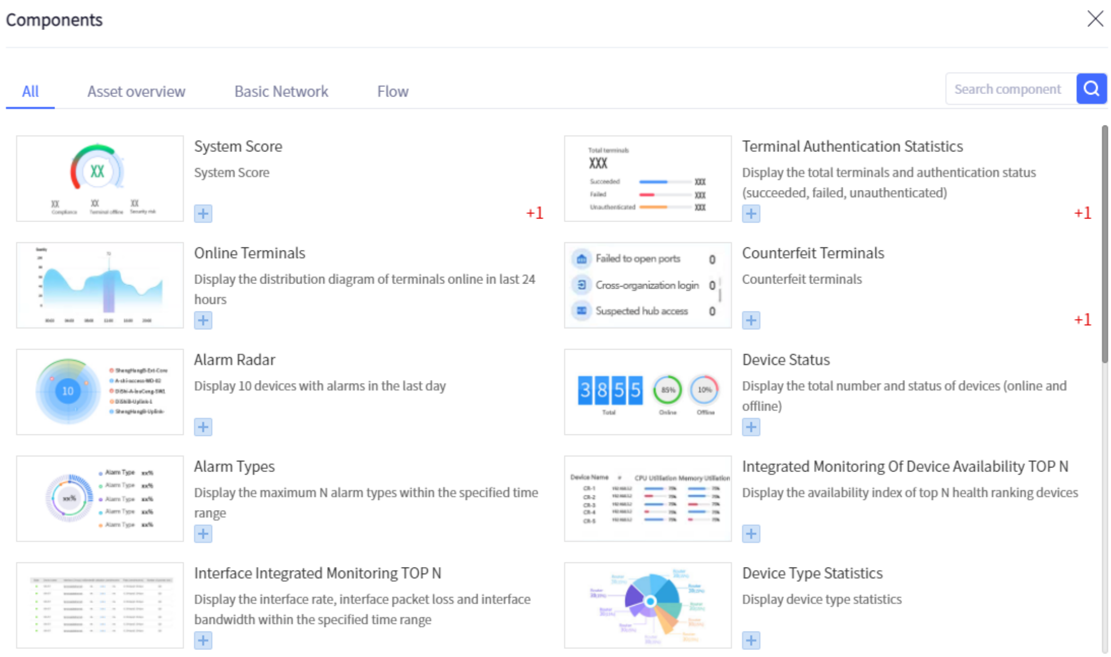
Click “Delete” in Figure 3.4, click OK according to the prompt, and the uer can delete the template added by himself.

Save the template

Click **Save** in the top right corner of the home page, and you can save all information in the template.

Add components

Click **Components** in the upper right corner of the home page, and a pop-up layer will appear, which contains all components in the system. Click the + button next to the component to add the component to the home page, and "+1" will appear next to the component, indicating that this component has been added to the current template. If you continue to add this component, the number will change to "+2". Add components as shown in the figure below:



Components

All | Asset overview | Basic Network | Flow

Search component

System Score
System Score
+ +1

Terminal Authentication Statistics
Display the total terminals and authentication status (succeeded, failed, unauthenticated)
+ +1

Online Terminals
Display the distribution diagram of terminals online in last 24 hours
+

Counterfeit Terminals
Counterfeit terminals
+ +1

Alarm Radar
Display 10 devices with alarms in the last day
+

Device Status
Display the total number and status of devices (online and offline)
+

Alarm Types
Display the maximum N alarm types within the specified time range
+

Integrated Monitoring Of Device Availability TOP N
Display the availability index of top N health ranking devices
+

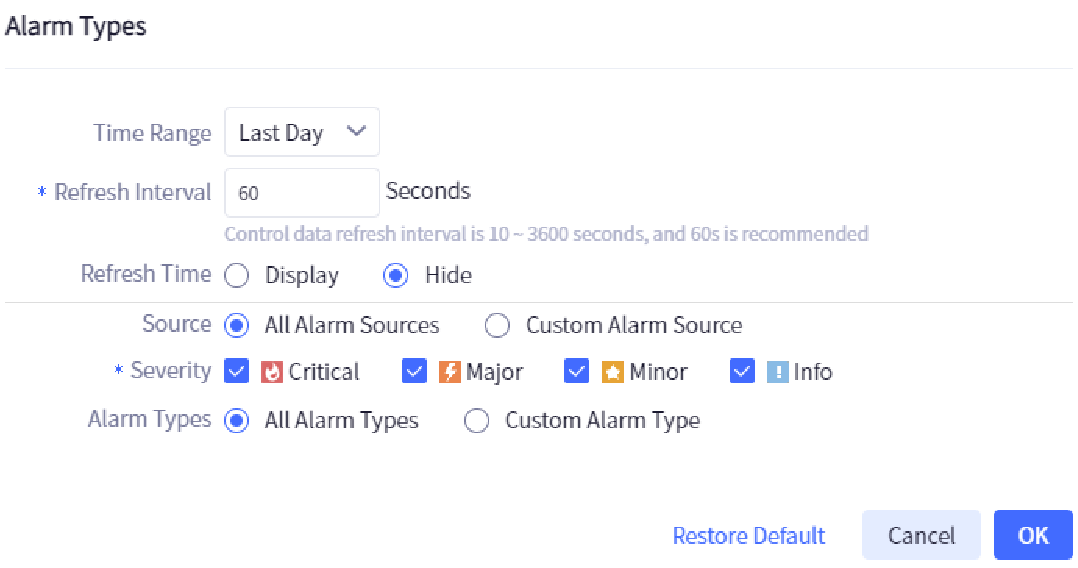
Interface Integrated Monitoring TOP N
Display the interface rate, interface packet loss and interface bandwidth within the specified time range
+

Device Type Statistics
Display device type statistics
+

Figure 3.6 Component list

Configure components

When a component is selected into the page, there is generally no data. You need to click ⚙ in the upper right corner of the component to configure the component before displaying the data according to the configuration conditions. Each component has different configuration conditions according to its characteristics. Now use "Alarm Types" to introduce the configuration method of each configuration condition. The configuration interface is shown in the figure below:



Alarm Types

Time Range: Last Day

* Refresh Interval: 60 Seconds

Control data refresh interval is 10 ~ 3600 seconds, and 60s is recommended

Refresh Time: ○ Display ● Hide

Source: ● All Alarm Sources ○ Custom Alarm Source

* Severity: ☑ Critical ☑ Major ☑ Minor ☑ Info

Alarm Types: ● All Alarm Types ○ Custom Alarm Type

Restore Default | Cancel | OK

Figure 3.7 Alarm type configuration

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 three months. Some controls can also select the last hour.

Refresh interval: Each control can configure the refresh interval to control the refresh interval of component data.

Refresh time: By selecting show or hide, you can configure the time range, refresh time display or hide in the component.

The above is the common configuration of components. Each component also has its own configuration items. Please configure the unique configuration items as prompted.

For more detailed configuration of all components, see the "Components" section.

Edit component name

Click ✎ in the upper left corner of the component to enter the edit state. After editing the component name, the editing is completed after the edit box loses focus.

Delete component

Click ✕ in the upper right corner of the component to pop up a prompt to delete the component. You can operate according to the prompt.

Hyperlink jump

If the legend or name of each component in the home page is displayed as the hand shape after the mouse is placed on it, it means that you can click this part to jump to the corresponding device, interface, alarm or other pages, as shown in the following figure:

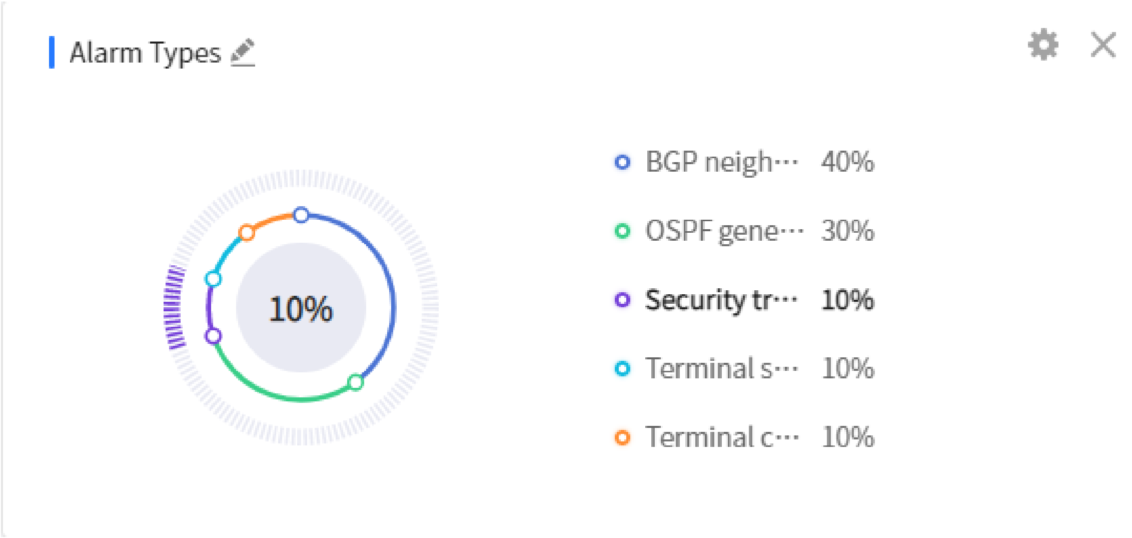
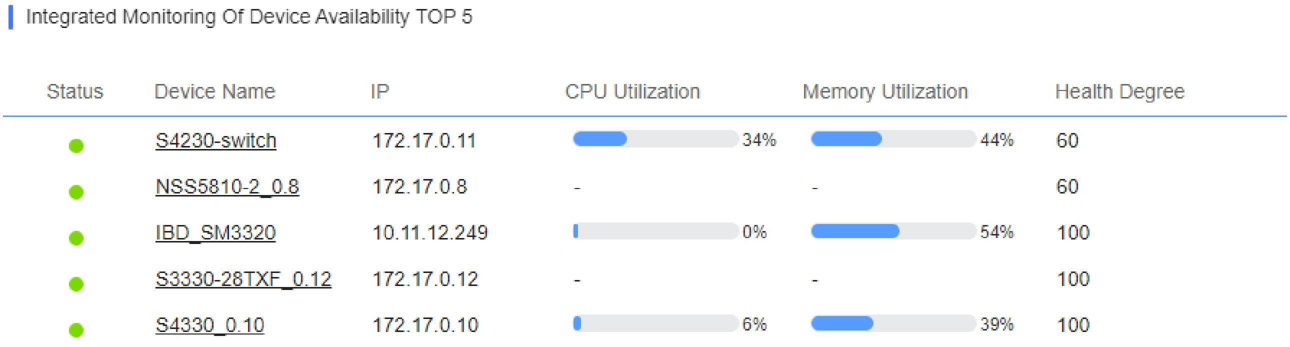


Figure 3.8 Legend jump


Integrated Monitoring Of Device Availability TOP 5

Status	Device Name	IP	CPU Utilization	Memory Utilization	Health Degree
●	S4230-switch	172.17.0.11	34%	44%	60
●	NSS5810-2_0.8	172.17.0.8	-	-	60
●	IBD_SM3320	10.11.12.249	0%	54%	100
●	S3330-28TXF_0.12	172.17.0.12	-	-	100
●	S4330_0.10	172.17.0.10	6%	39%	100

Figure 3.9 List jump

4 Basic Network

4.1 Network Devices

4.1.1 Device Management

The device management module provides management function for all devices in the system, including grouping devices, searching for specific devices according to filter conditions, setting aliases for devices, viewing device details, etc. Click "Discovery" on the navigation bar at the top of the system to open the "Device Management" interface, as shown in the following figure:

Group Management

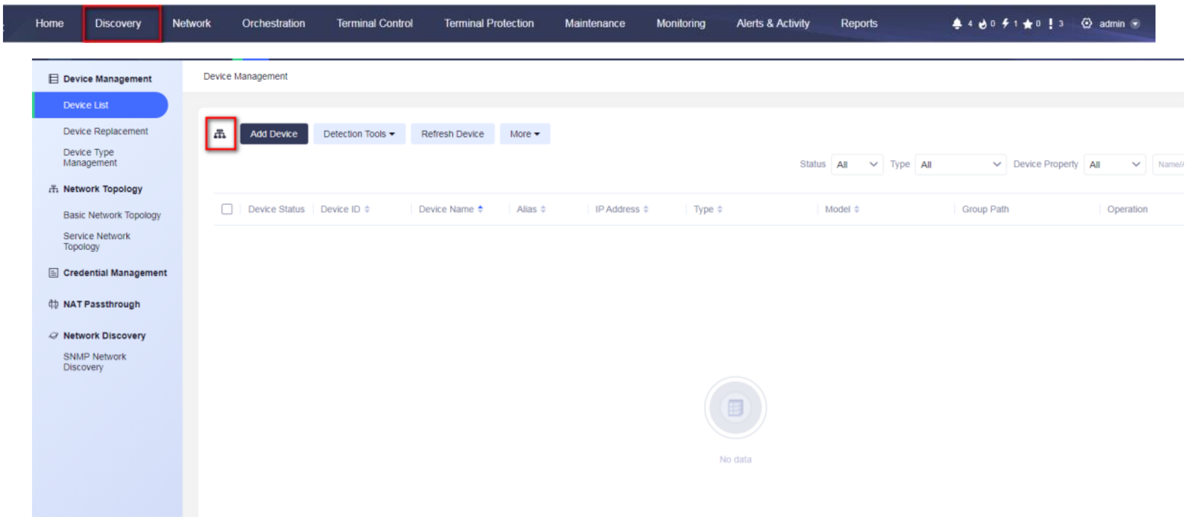


Figure 4.1 Group management

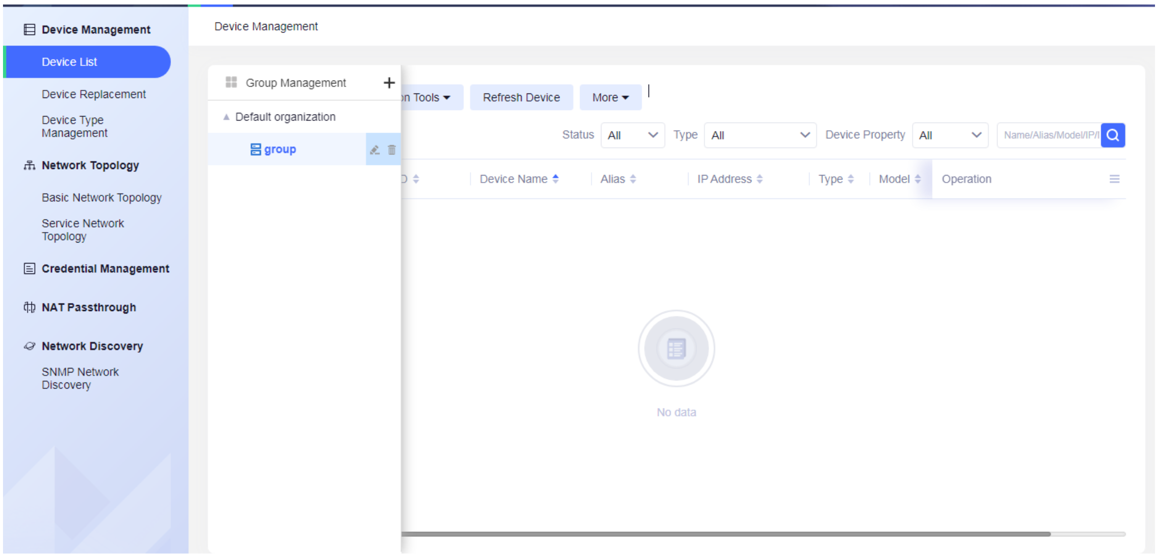


Figure 4.2 Group Management

Add device:

The “Add device” function supports adding devices manually. Click the **Add Device** button to pop up the “Add Device” dialog box, fill in the corresponding information, and click the "OK" button.

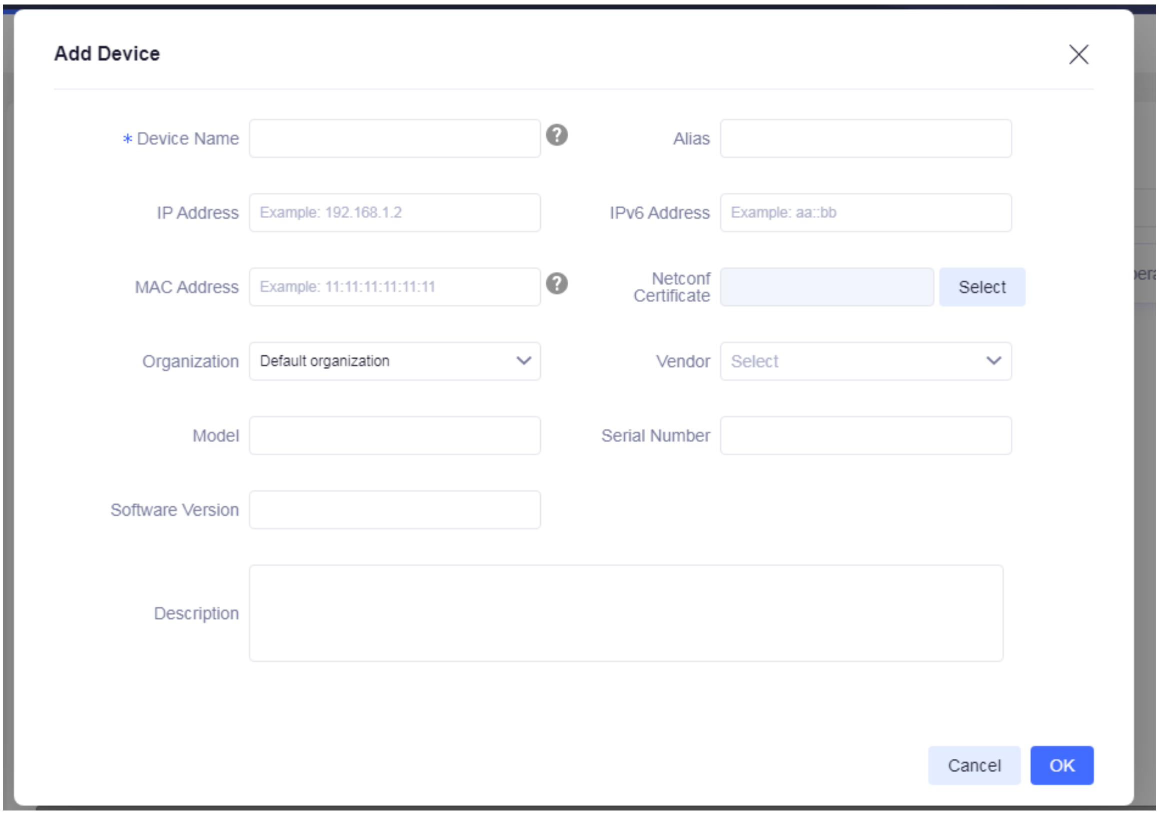
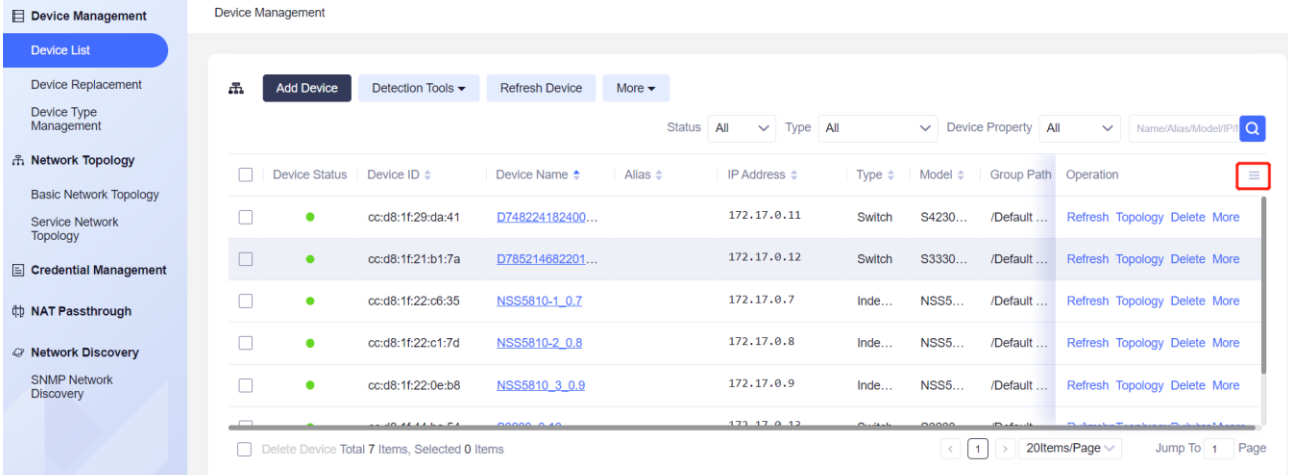


Figure 4.3 Add device

Device list:

Open the "Device Management" interface to display all devices in the system by default, displaying the status, name, alias, IP, MAC, model, software version, manufacturer, grouping path, serial number, sysoid, hardware version and other information of each device by columns. It also supports the "Sorting function". You can select and save the displayed columns and column positions. You can check the display as needed. The name column and operation column must be displayed and cannot be removed, as shown below:

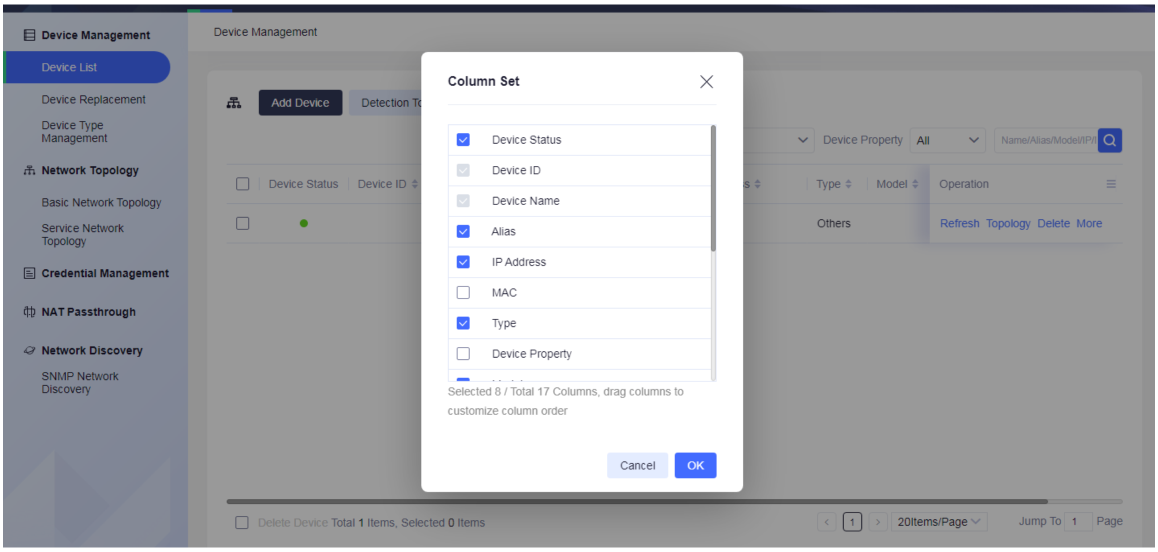


Status: All · Type: All · Device Property: All

☐	Device Status	Device ID	Device Name	Alias	IP Address	Type	Model	Group Path	Operation
☐	●	cc:d8:1f:29:da:41	D748224182400...		172.17.0.11	Switch	S4230...	/Default ...	Refresh Topology Delete More
☐	●	cc:d8:1f:21:b1:7a	D785214682201...		172.17.0.12	Switch	S3330...	/Default ...	Refresh Topology Delete More
☐	●	cc:d8:1f:22:c6:35	NSS5810-1_0.7		172.17.0.7	Inde...	NSS5...	/Default ...	Refresh Topology Delete More
☐	●	cc:d8:1f:22:c1:7d	NSS5810-2_0.8		172.17.0.8	Inde...	NSS5...	/Default ...	Refresh Topology Delete More
☐	●	cc:d8:1f:22:0e:b8	NSS5810_3_0.9		172.17.0.9	Inde...	NSS5...	/Default ...	Refresh Topology Delete More

Total 7 Items, Selected 0 Items

Figure 4.4 Column setting



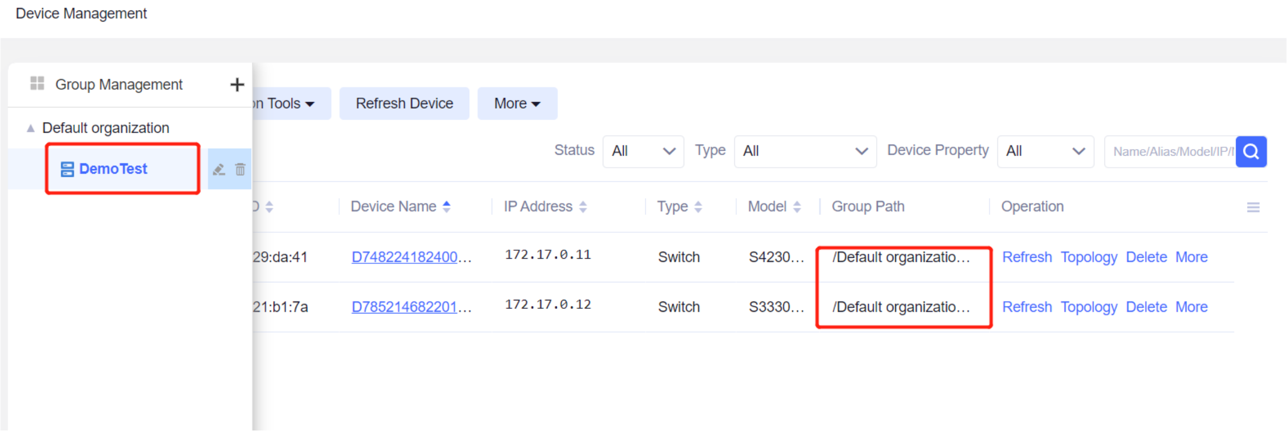
Column Set

☑ Device Status
☑ Device ID
☑ Device Name
☑ Alias
☑ IP Address
☐ MAC
☑ Type
☐ Device Property

Selected 8 / Total 17 Columns, drag columns to customize column order

Figure 4.5 Column setting

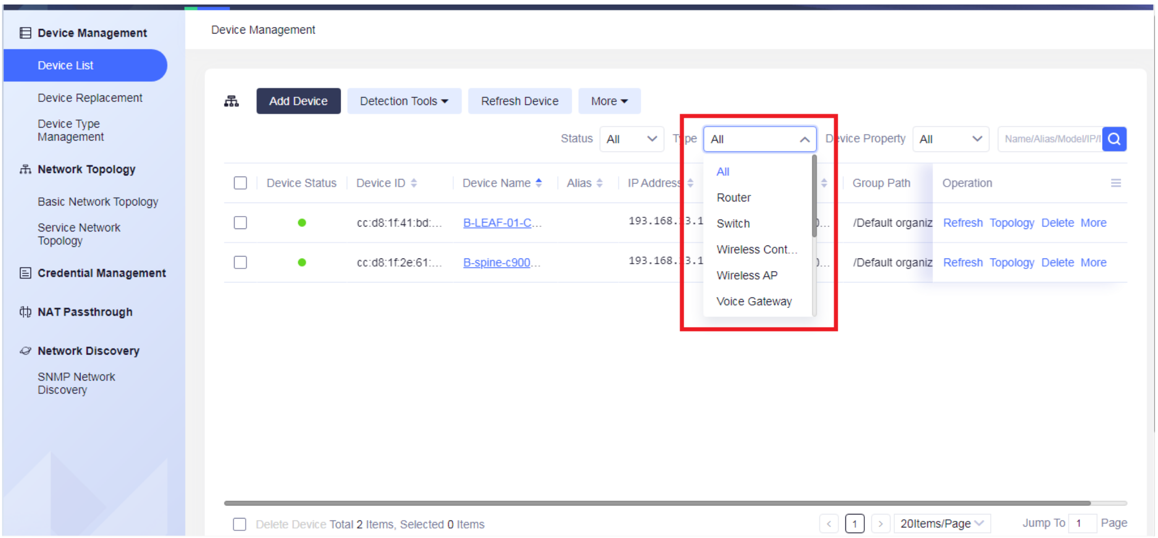
The devices displayed in the device list are determined by the device grouping tree on the left. If the device group node is selected in the grouping tree on the left, the device list in the device group (including the devices of the group and all its subordinate groups) will be displayed in the list;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



D	Device Name	IP Address	Type	Model	Group Path	Operation
29:da:41	D748224182400…	172.17.0.11	Switch	S4230…	/Default organizatio…	Refresh Topology Delete More
21:b1:7a	D785214682201…	172.17.0.12	Switch	S3330…	/Default organizatio…	Refresh Topology Delete More

Figure 4.6 Device list display

This page provides various query criteria, which can query 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, model, IP, MAC, status, type and other fields (case fuzzy query is supported).



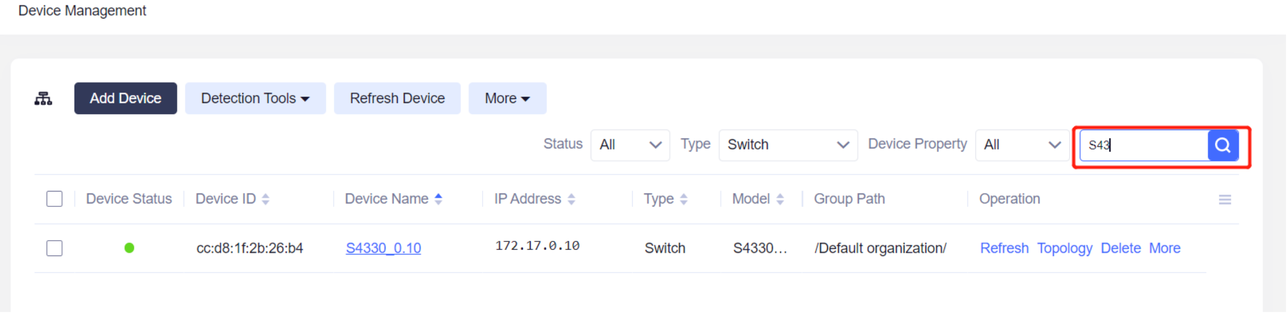
Status: All | Type: All | Device Property: All | Name/Alias/Model/IP/I

☐	Device Status	Device ID	Device Name	Alias	IP Address	Group Path	Operation
☐	●	cc:d8:1f:41:bd:...	B-LEAF-01-C...		193.168.3.1	/Default organiz	Refresh Topology Delete More
☐	●	cc:d8:1f:2e:61:...	B-spine-c900...		193.168.3.1	/Default organiz	Refresh Topology Delete More

Total 2 Items, Selected 0 Items

Figure 4.7 Device list query

Click each field in the head of the device list to sort the devices according to the corresponding field. As shown in the figure below, find out all routers in the "Online" state and whose name, model, IP and MAC can match the string "s43", and sort them in ascending order according to the device alias:



Status: All | Type: Switch | Device Property: All | S43

☐	Device Status	Device ID	Device Name	IP Address	Type	Model	Group Path	Operation
☐	●	cc:d8:1f:2b:26:b4	S4330_0.10	172.17.0.10	Switch	S4330...	/Default organization/	Refresh Topology Delete More

Figure 4.8 Device query and sorting

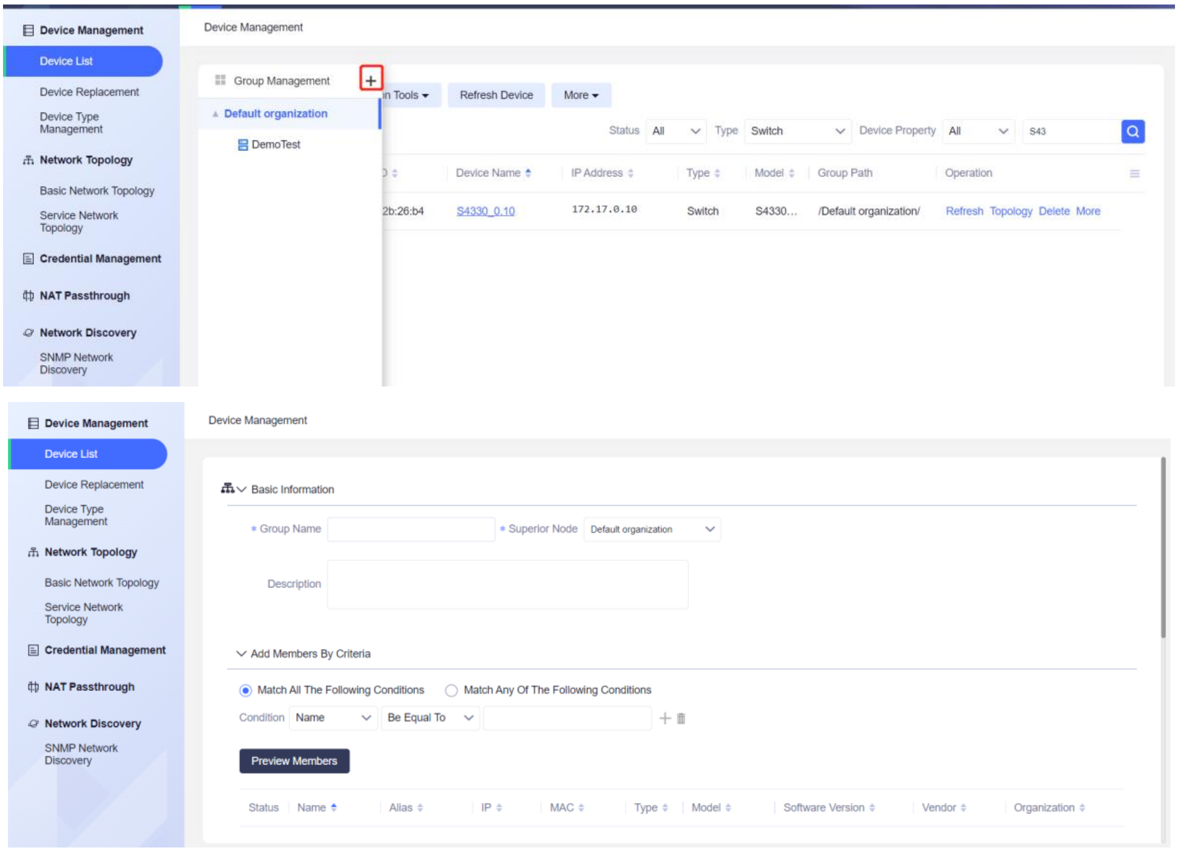
Note

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

Add device group:

The controller provides device grouping function, and reasonable grouping can more conveniently manage the devices. All device groups are attached to the corresponding organization, and the administrator can create, modify and delete device groups.

Click the Add icon + in the grouping tree on the left of the device list to open the "Add Group" page. You need to enter the name, select the parent node, and enter the basic information of the device group such as description information to create a group, as shown in the following figure:



Status All Type Switch Device Property All S43

D	Device Name	IP Address	Type	Model	Group Path	Operation
2b:26:b4	S4330_0.10	172.17.0.10	Switch	S4330...	/Default organization/	Refresh Topology Delete More

* Group Name

* Superior Node Default organization

Description

● Match All The Following Conditions ○ Match Any Of The Following Conditions

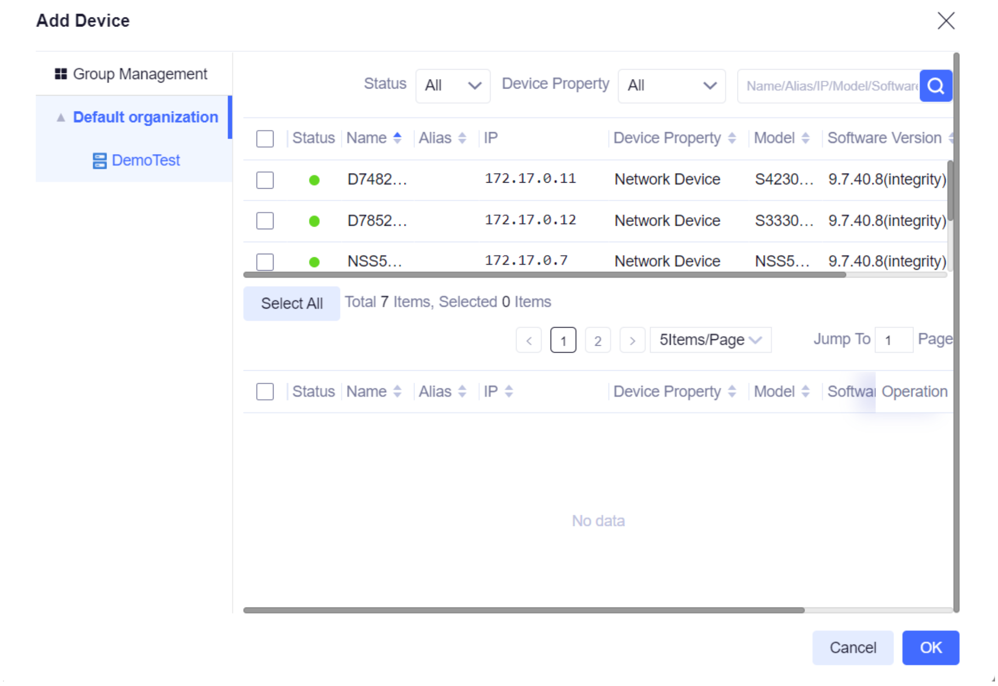
Condition Name Be Equal To

Status	Name	Alias	IP	MAC	Type	Model	Software Version	Vendor	Organization

Figure 4.9 Add device group

When creating a device group, there are two ways to add devices: manually adding devices and conditionally adding devices, which can be used alone or mixed. Manually added devices will always remain in the device group unless moving the devices from the group or transferring the organization, conditionally added devices will change according to 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 "Device selection" dialog box, you can select the organization tree on the left and select the devices that meet the query criteria by matching the name, model, IP and status of the selected organization. Support "Select All" and "Delete All" functions.



☐	Status	Name	Alias	IP	Device Property	Model	Software Version
☐	●	D7482…		172.17.0.11	Network Device	S4230…	9.7.40.8(integrity)
☐	●	D7852…		172.17.0.12	Network Device	S3330…	9.7.40.8(integrity)
☐	●	NSS5…		172.17.0.7	Network Device	NSS5…	9.7.40.8(integrity)

Total 7 Items, Selected 0 Items

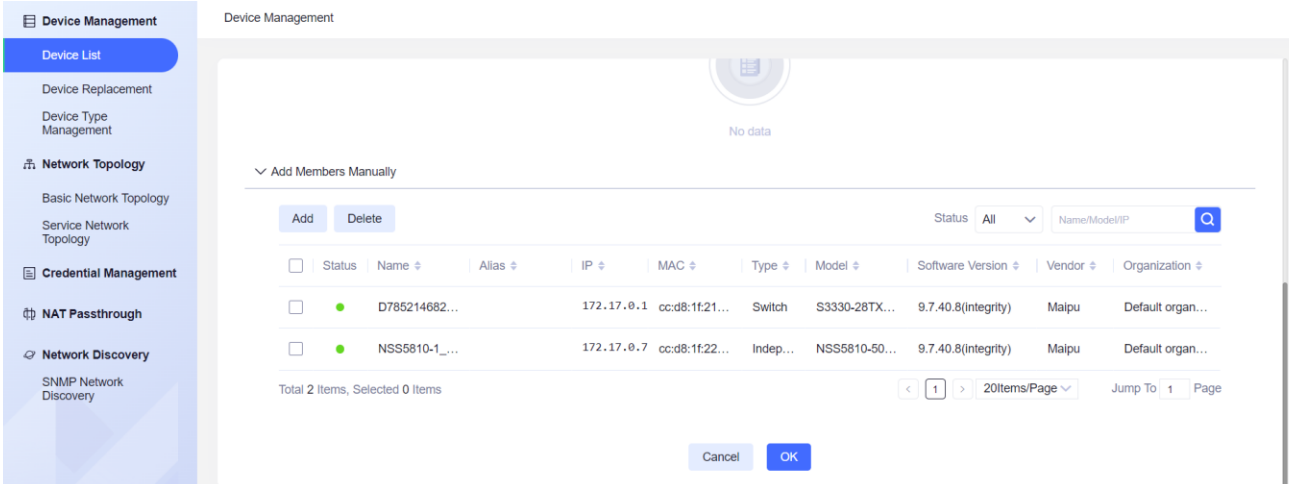
‹ 1 2 › 5Items/Page Jump To 1 Page

☐	Status	Name	Alias	IP	Device Property	Model	Softwa	Operation

No data

Figure 4.10 Select devices

After selecting devices, click “OK” to add the selected devices to the member list manually.



☐	Status	Name	Alias	IP	MAC	Type	Model	Software Version	Vendor	Organization
☐	●	D785214682…		172.17.0.1	cc:d8:1f:21…	Switch	S3330-28TX…	9.7.40.8(integrity)	Maipu	Default organ…
☐	●	NSS5810-1_…		172.17.0.7	cc:d8:1f:22…	Indep…	NSS5810-50…	9.7.40.8(integrity)	Maipu	Default organ…

Total 2 Items, Selected 0 Items

‹ 1 › 20Items/Page Jump To 1 Page

Figure 4.11 Manually add members

Adding devices conditionally can match devices by creating different conditions. It supports "Match All The Following Conditions" and "Match Any og The Following Conditions". It supports matching device name, model, manufacturer, type and IP address conditions, and previews the current matching results through the "Preview Members" button, as shown in the following figure:

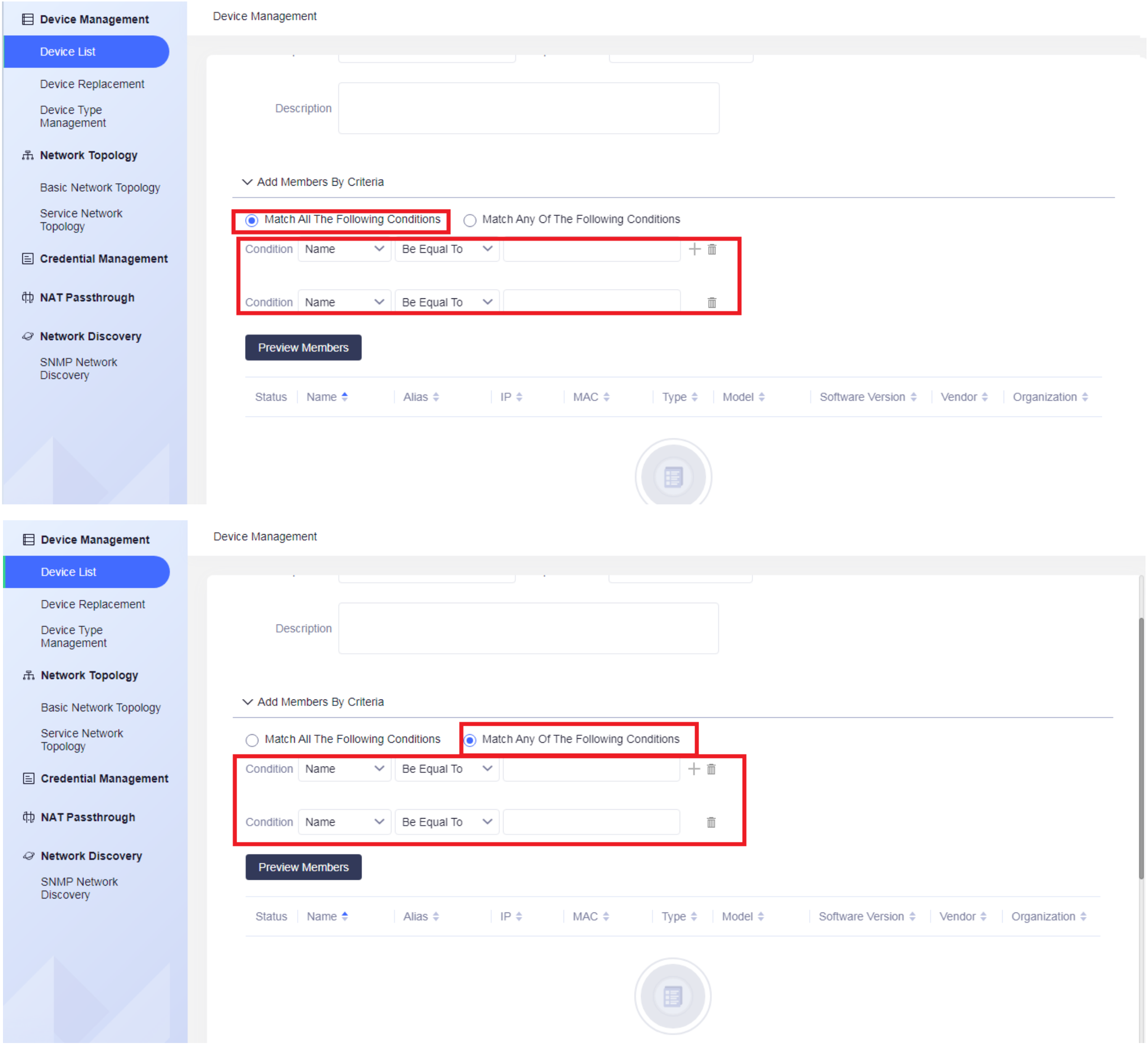
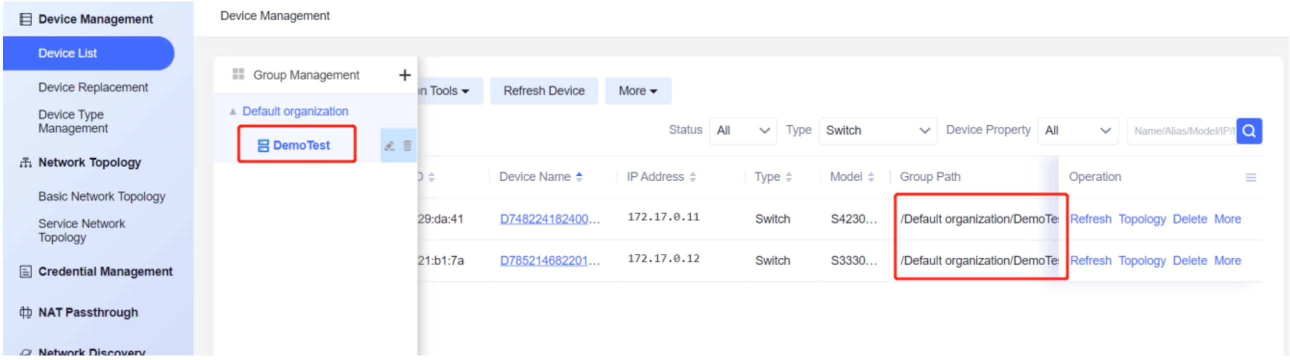


Figure 4.12 Add members by conditions

Note

- The device range matched by conditionally adding 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 an organization node, the direct devices of the organization will be matched. If the selected parent node is an device group node, the direct devices of the organization of the device group will be matched
- The range of devices that can be selected by manually adding 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 include the devices of other organizations, you will be prompted whether to create the device group. If yes, the selected devices will be deleted from other organizations and added to the organization to which the current device group belongs.



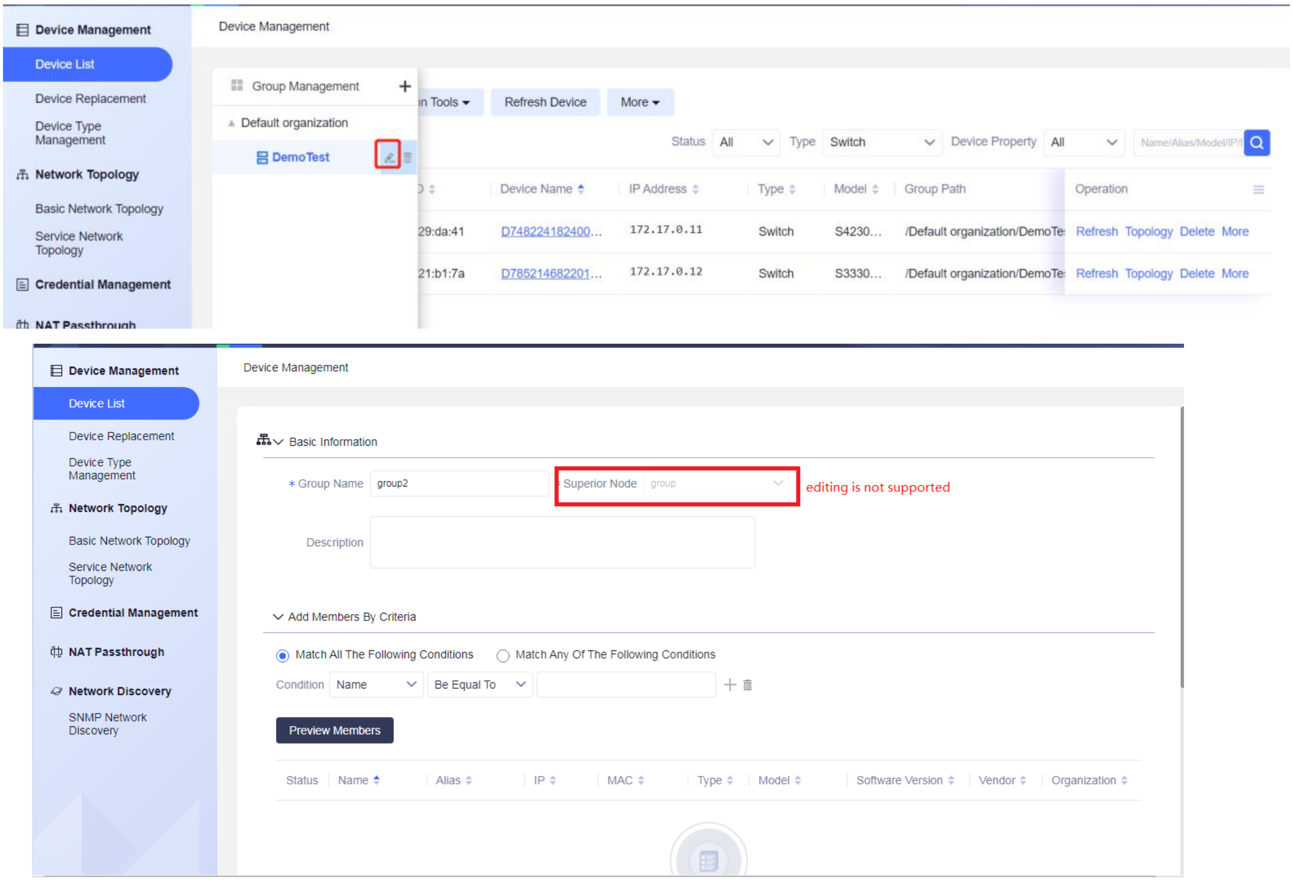
Status All Type Switch Device Property All

D	Device Name	IP Address	Type	Model	Group Path	Operation
29:da:41	D748224182400...	172.17.0.11	Switch	S4230...	/Default organization/DemoTe	Refresh Topology Delete More
21:b1:7a	D785214682201...	172.17.0.12	Switch	S3330...	/Default organization/DemoTe	Refresh Topology Delete More

Figure 4.13 Adding devices to device group succeeded

Edit Device Group:

Select a desired group in the left tree of the device management page, and click the “Edit” icon ✎ to enter the page of editing the device group. You can edit the group name, description and members in the group. "Parent Node" cannot be edited. The mode of adding members manually and conditionally is the same as adding a new device group.



Status All Type Switch Device Property All

D	Device Name	IP Address	Type	Model	Group Path	Operation
29:da:41	D748224182400...	172.17.0.11	Switch	S4230...	/Default organization/DemoTe	Refresh Topology Delete More
21:b1:7a	D785214682201...	172.17.0.12	Switch	S3330...	/Default organization/DemoTe	Refresh Topology Delete More

* Group Name group2

Superior Node group

editing is not supported

Description

● Match All The Following Conditions ○ Match Any Of The Following Conditions

Condition Name Be Equal To

Figure 4.14 Edit device group

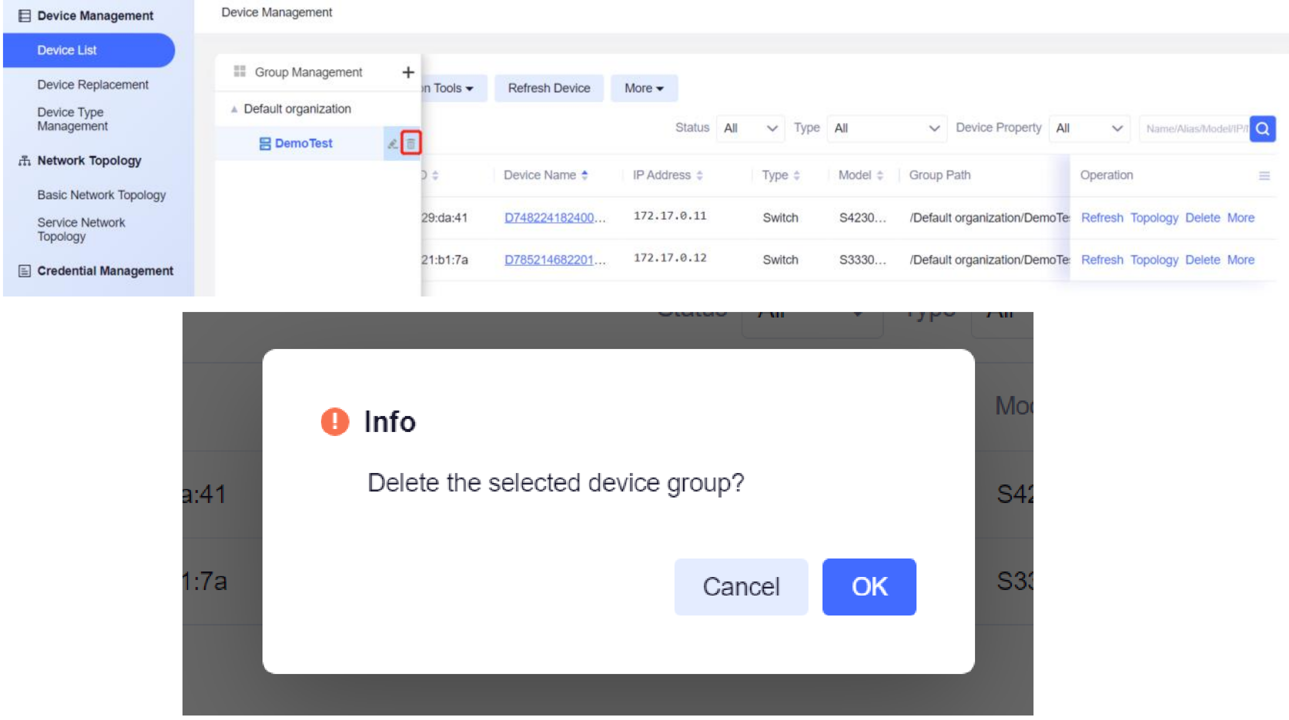
Note

- When adding/editing a device group, the duplicate name rule is that there is no duplicate name under the same group path, and there cannot be the device groups with the same name under the same "parent node". If the name is duplicate, a prompt will be given when saving the device group

- The function of synchronously generating topology is supported when adding a device group, but the topology view cannot be synchronously generated when editing a device group

Delete device group:

Select a desired device group in the left tree of the device management interface, click , and a dialog box of confirming the deletion appears. After confirming, you can delete the device group.



Info

Delete the selected device group?

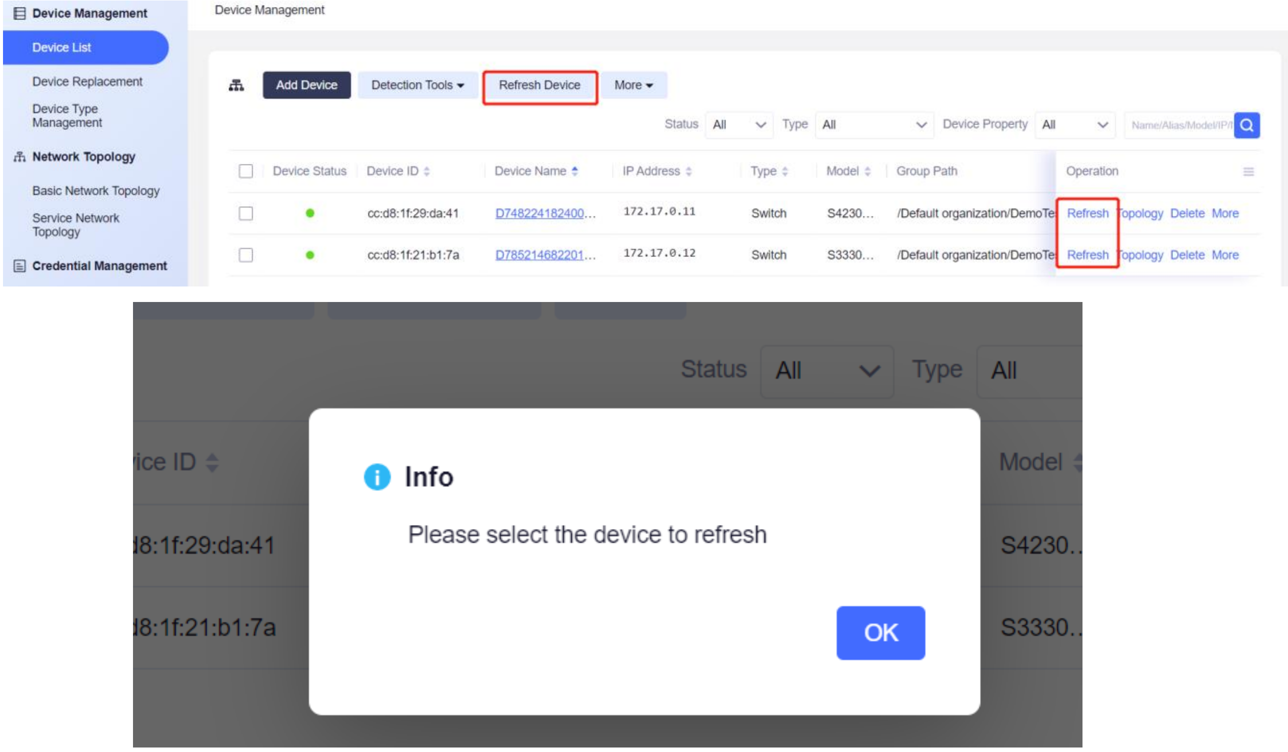
Figure 4.15 Delete a device group

Note

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

Refresh devices:

Select a device and click **Refresh Device** to perform network discovery on the device again, or click the **Refresh** button on the right side of the device list to refresh manually. After clicking the **Refresh** button, a confirmation dialog box will pop up, as shown in the figure below. Click the "OK" button to start refreshing. Only the devices containing SNMP credentials can be refreshed successfully.



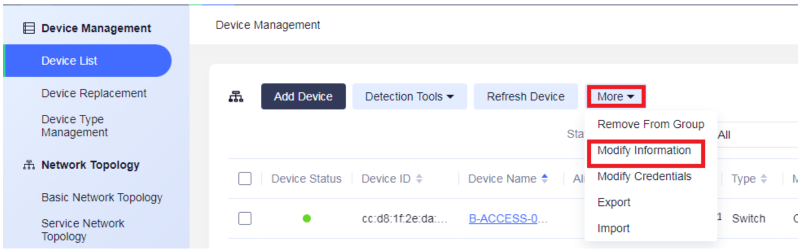
☐	Device Status	Device ID	Device Name	IP Address	Type	Model	Group Path	Operation
☐	●	cc:d8:1f:29:da:41	D748224182400…	172.17.0.11	Switch	S4230…	/Default organization/DemoTe	Refresh opology Delete More
☐	●	cc:d8:1f:21:b1:7a	D785214682201…	172.17.0.12	Switch	S3330…	/Default organization/DemoTe	Refresh opology Delete More

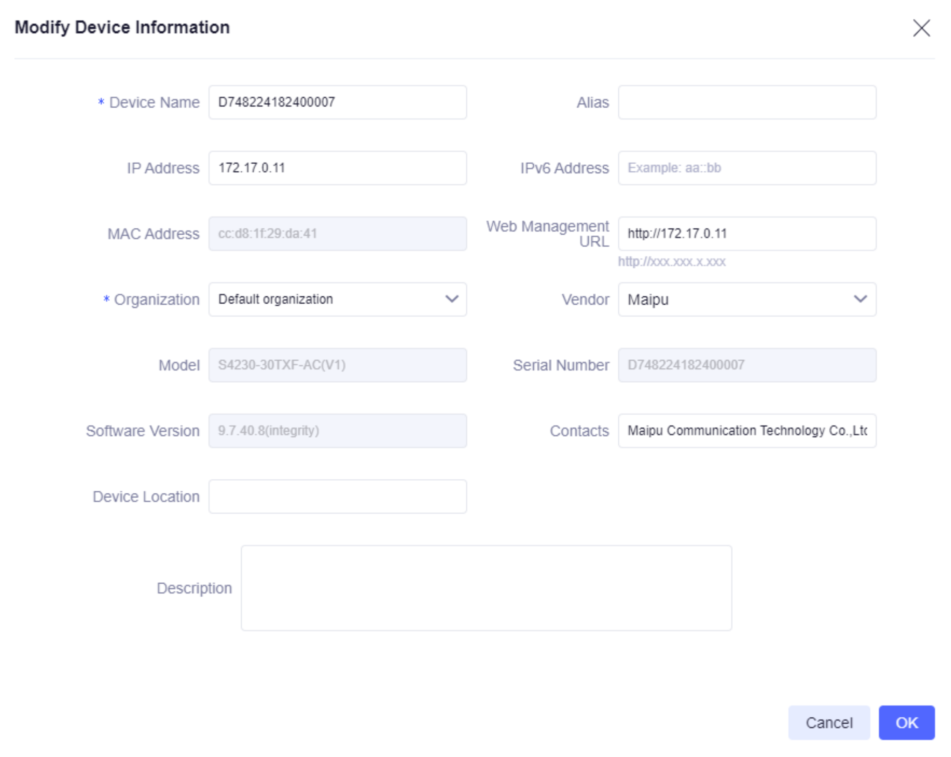
Please select the device to refresh

Figure 4.16 Refresh devices

Modify information:

First check a desired device in the device list, then click the **More** button, and then click the **Modify Information** button to pop up the following "**Modify Device Information**" dialog box. The name, alias, location, contact person, organization and web management URL of the device can be modified, and click the "OK" button to modify the device information successfully.



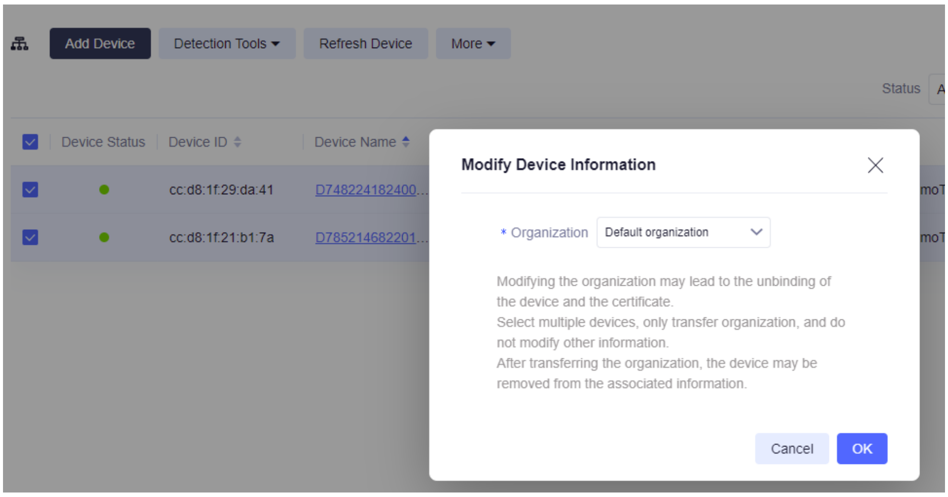


Modify Device Information

* Device Name: D748224182400007
Alias:
IP Address: 172.17.0.11
IPv6 Address: Example: aa::bb
MAC Address: cc:d8:1f:29:da:41
Web Management URL: http://172.17.0.11
http://xxx.xxx.x.xxx
* Organization: Default organization
Vendor: Maipu
Model: S4230-30TXF-AC(V1)
Serial Number: D748224182400007
Software Version: 9.7.40.8(integrity)
Contacts: Maipu Communication Technology Co.,Ltc
Device Location:
Description:

Figure 4.17 Modify device information

When modifying the device information in batch, you can only modify the organization of the device, as shown in the following figure:

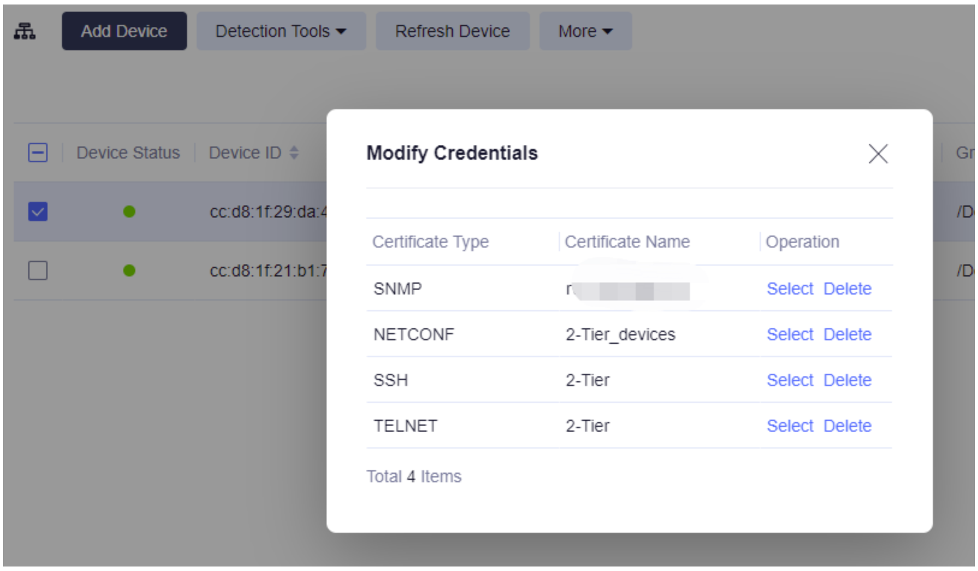


☑	Device Status	Device ID	Device Name
☑	●	cc:d8:1f:29:da:41	D748224182400...
☑	●	cc:d8:1f:21:b1:7a	D785214682201...

Modify Device Information

* Organization: Default organization

Modifying the organization may lead to the unbinding of the device and the certificate.
Select multiple devices, only transfer organization, and do not modify other information.
After transferring the organization, the device may be removed from the associated information.



Modify Credentials

Certificate Type	Certificate Name	Operation
SNMP	[redacted]	Select Delete
NETCONF	2-Tier_devices	Select Delete
SSH	2-Tier	Select Delete
TELNET	2-Tier	Select Delete

Total 4 Items

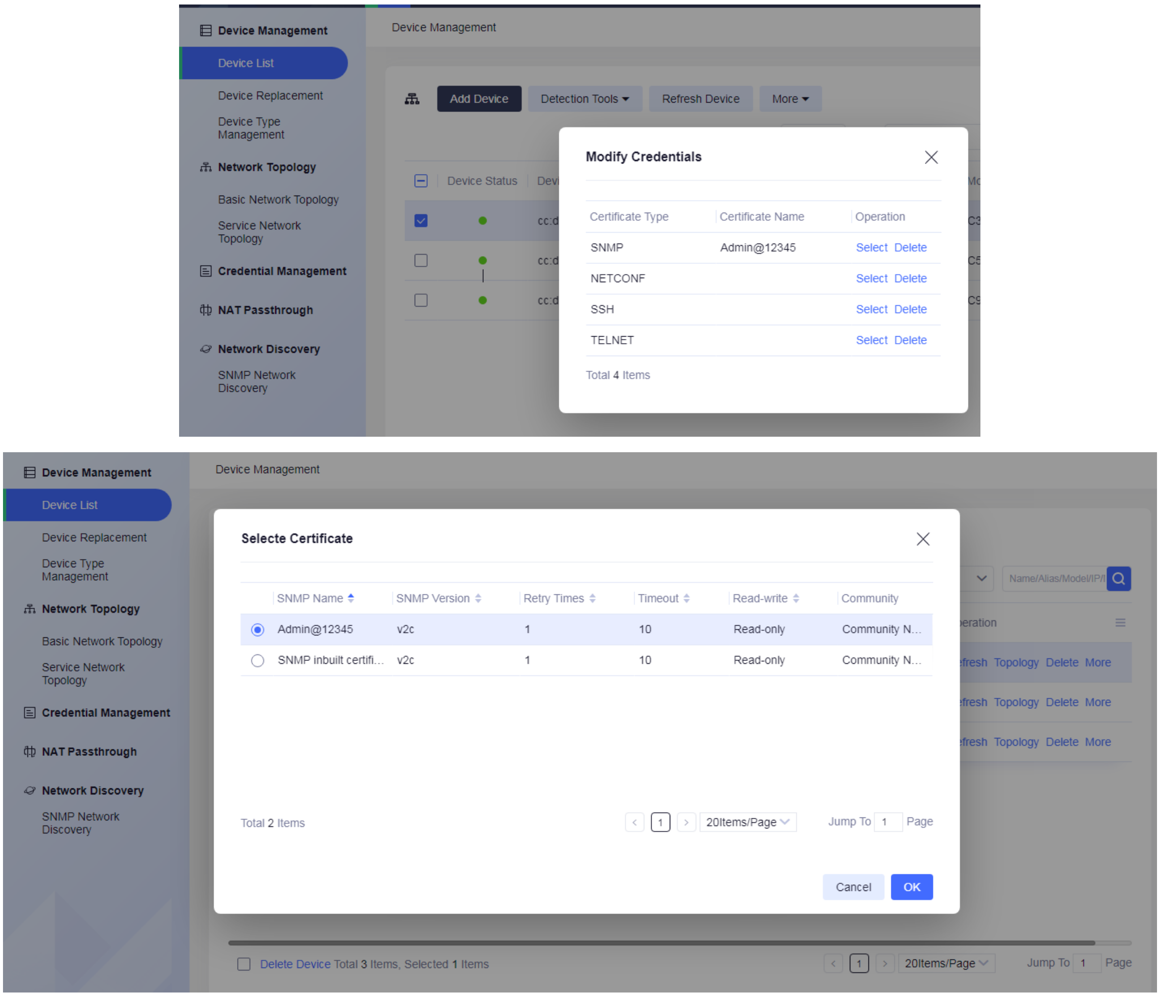
Figure 4.18 Modify the device information in batches

Note

- The device name, device location and contact person can be modified successfully only if the device and controller are configured with SNMP write authority at the same time;
- The web management URL can modify the access address when the device jumps to the web;
- The function of transferring the device organization may cause the device to be deleted from the original organization. Therefore, if the device is selected in various tasks of the original organization, it may not be able to operate the device (the device will not be affected if it is transferred to a subordinate organization, but this problem may occur if it is transferred to a superior or peer organization)
- When the device is transferred to the organization, the credential configured by the original device can still be used, but it is not visible through the page (because the credential is hierarchically and decentralized managed). Once a new credential is configured for the device again, the new credential will prevail and the original credential will become invalid.

Modify credential:

Modifying a credential can add different credentials to the device. First, check the desired device in the device list, click **More**, and then, click **Modify Credentials**, and pop up the following “Modify Credentiasl” dialog box. You can select the desired credential type, and click **Select** to pop up the credential list. Select the corresponding credential, and click **OK** to modify the credential successfully.



Modify Credentials

Certificate Type	Certificate Name	Operation
SNMP	Admin@12345	Select Delete
NETCONF		Select Delete
SSH		Select Delete
TELNET		Select Delete

Total 4 Items

Selecte Certificate

	SNMP Name	SNMP Version	Retry Times	Timeout	Read-write	Community
●	Admin@12345	v2c	1	10	Read-only	Community N...
○	SNMP inbuilt certifi...	v2c	1	10	Read-only	Community N...

Total 2 Items

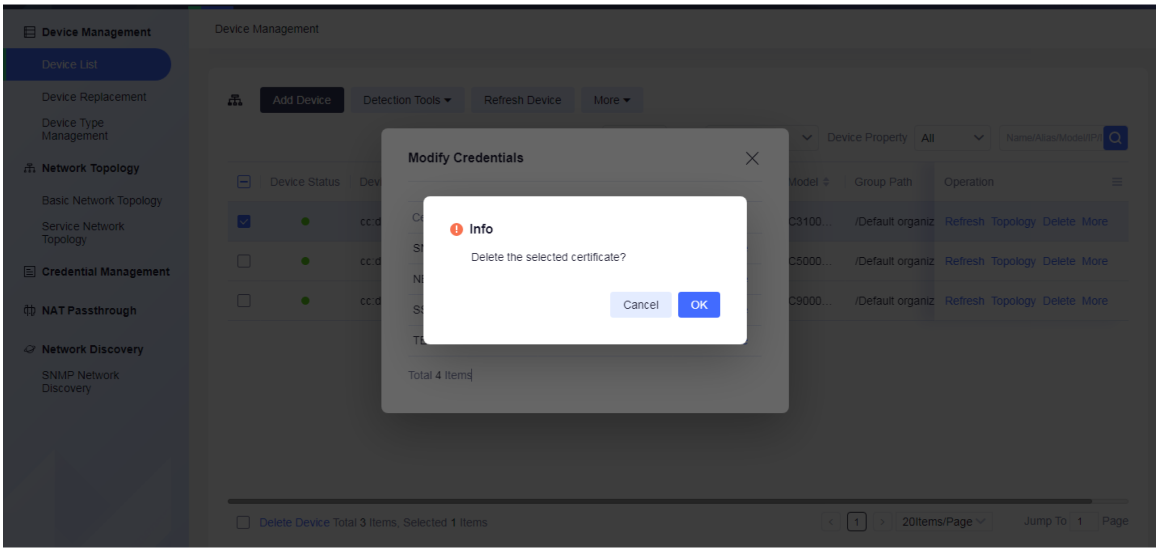
Figure 4.19 Modify device certificate

Note

- The credential types that can be modified include SNMP, Telnet, NETCONF and SSH credentials. The selectable credentials are the credentials of the organization to which the selected device belongs. Each device can only have one credential of each type. Once modified, it will overwrite the configured credentials of the same type of the device.
- When modifying device credentials in batch, the selected device can only be the device of the same organization. Otherwise, a prompt will be given and the credential cannot be modified.

Delete the certificate:

Deleting the credential can delete different credentials for the device. First, check a desired device in the device list, then click **More**, and then click **Modify Credentials** to open the following "Modify Credential" dialog box, where you can select the credential type you want to delete. Click "Delete" to open the confirmation dialog box for deleting credentials. Click **OK** to delete the credential successfully.



Info

Delete the selected certificate?

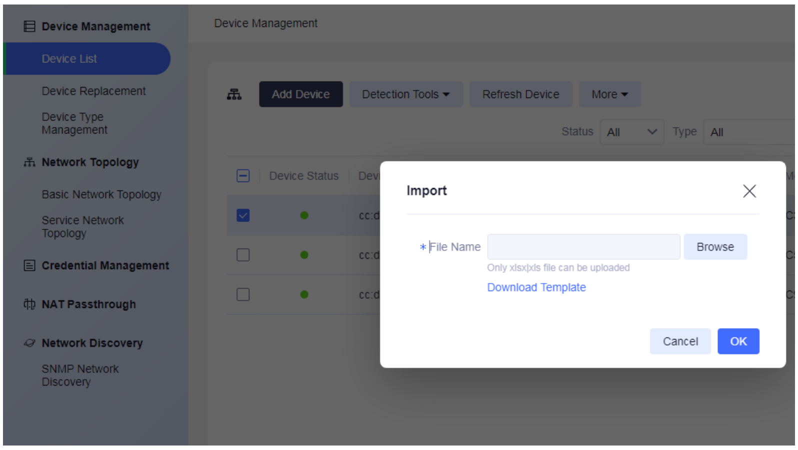
Figure 4.20 Delete the device credential

Export:

The system supports the function of exporting the device list. Click the **More** button, and then, click the **Export** button to export the device list. The exported file format is .xlsx format. The data and fields are the same as those displayed in the current device list. Support query and export.

Import:

The system supports the function of importing the device list. Click the **More** button, and then, click the **Import** button to pop up the **Import** dialog box. Download the import template and complete it. Select the filled template, click "OK" and wait for the import to complete.



Only xlsx|xls file can be uploaded

Figure 4.21 Import devices

Locate to Topology:

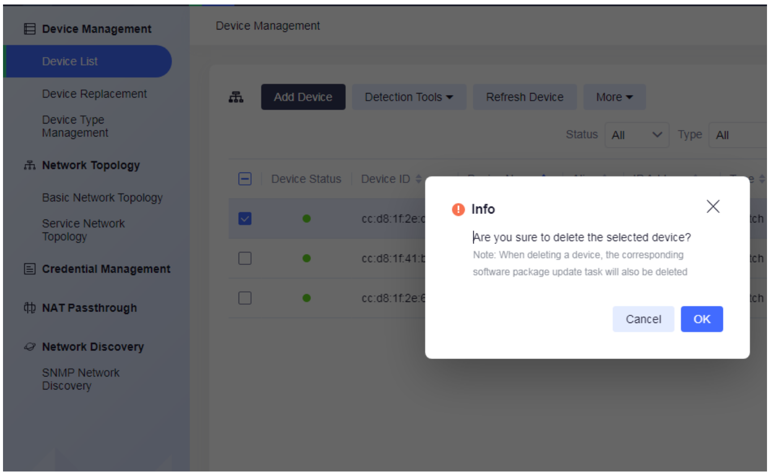
The function of locating to the topology supports jumping to the topology page, that is, jump to the first topology view containing the device under the organization to which the device belongs. If there is no topology view containing the device under the organization to which the device belongs, jump to an empty view. Click the **Locate to Topology** button in the operation column to jump to the topology interface.

Web Management:

The function of locating to the web management supports jumping to the web management page. Click the **More** button in the operation column and click the **Web Management** button to jump to the web management interface.

Delete device:

Check the desired device in the device list (support multiple selections), and click **Delete** to pop up the confirmation dialog box for deleting the device, as shown in the following figure. Click **OK** to confirm the deletion of the selected device, and click **Cancel** to abort the deletion.



Are you sure to delete the selected device?

Note: When deleting a device, the corresponding software package update task will also be deleted

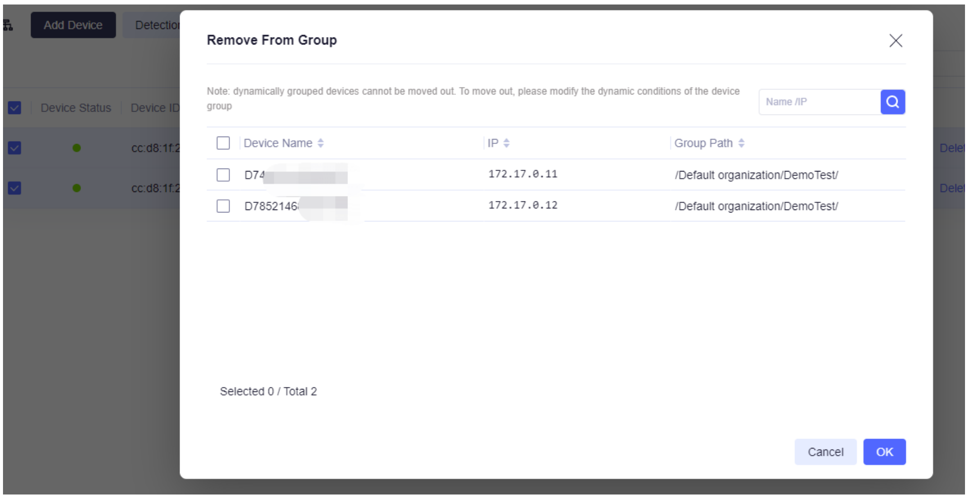
Figure 4.22 Delete the device

Note

- Deleting a device will delete the device from the device library. The device will not appear in the controller until network discovery is performed again. In addition, if the EDP task is not deleted, delete a device, and the device will be automatically found by the task again.

Move from Group:

The function of moving out of the group supports moving the selected device from the specified device group. Check a desired device in the device list (support multiple selection), click the **More** button, and then click the **Remove From Group** button to pop up the selection box, as shown in the following figure. Select the desired device and group, and click the "OK" to move the selected device from the corresponding group. Click "Cancel" to drop the operation.



Note: dynamically grouped devices cannot be moved out. To move out, please modify the dynamic conditions of the device group

☐ Device Name	IP	Group Path
☐ D74[redacted]	172.17.0.11	/Default organization/DemoTest/
☐ D7852146[redacted]	172.17.0.12	/Default organization/DemoTest/

Selected 0 / Total 2

Figure 4.23 Remove the device from the group

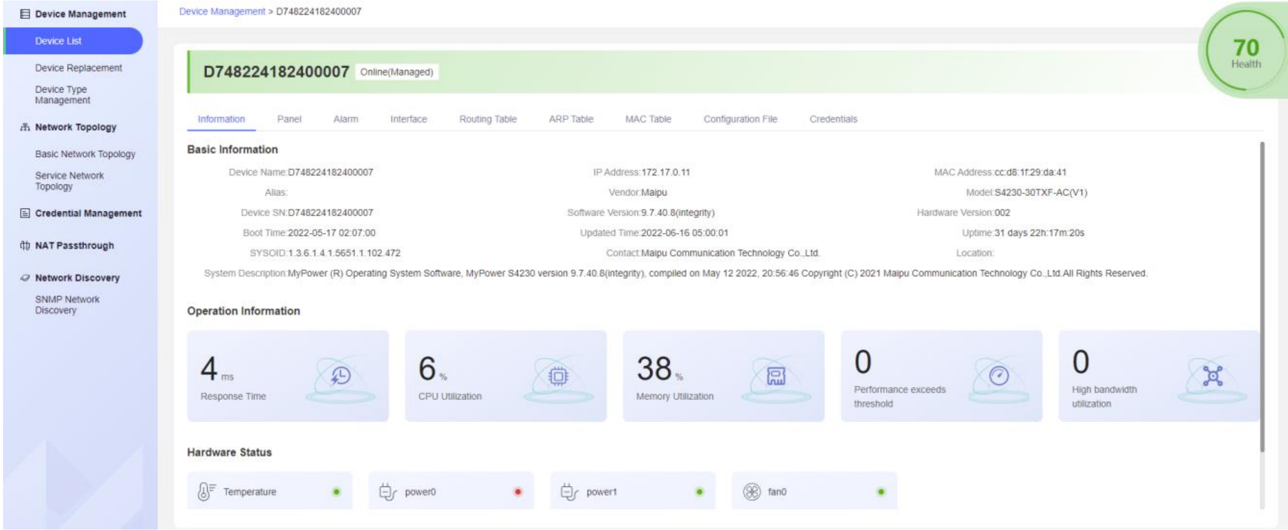
Note

- If the device is a member added by conditions in the device group and cannot be moved out of the group, the check box of the record corresponding to the selection box will be grayed out and cannot be selected. A prohibition icon will be displayed on the mouse, indicating that the device is dynamically added and cannot be removed.

- When 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 attached to the root of the organization.

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 the figure. For terminal devices, they don't have device details.



D748224182400007 Online(Managed)

Basic Information

Device Name:D748224182400007
IP Address:172.17.0.11
MAC Address:cc:d8:1f:29:da:41
Alias:
Vendor:Maipu
Model:S4230-30TXF-AC(V1)
Device SN:D748224182400007
Software Version:9.7.40.8(integrity)
Hardware Version:002
Boot Time:2022-05-17 02:07:00
Updated Time:2022-06-16 05:00:01
Uptime:31 days 22h:17m:20s
SYSOID:1.3.6.1.4.1.5651.1.102.472
Contact:Maipu Communication Technology Co.,Ltd.
Location:
System Description:MyPower (R) Operating System Software, MyPower S4230 version 9.7.40.8(integrity), compiled on May 12 2022, 20:56:46 Copyright (C) 2021 Maipu Communication Technology Co.,Ltd.All Rights Reserved.

Operation Information

4 ms Response Time
6 % CPU Utilization
38 % Memory Utilization
0 Performance exceeds threshold
0 High bandwidth utilization

Hardware Status

Figure 4.24 Device details

Device Information

Basic information page includes device status, alarm, performance indexes exceeding the threshold, interfaces with high bandwidth utilization, device name, alias, IP, MAC, model, manufacturer, and other device basic information (System OID, contact, location, system description information, as well as device health, CPU utilization, memory utilization, response time, temperature, power supply, fan, etc.).

Panel Information

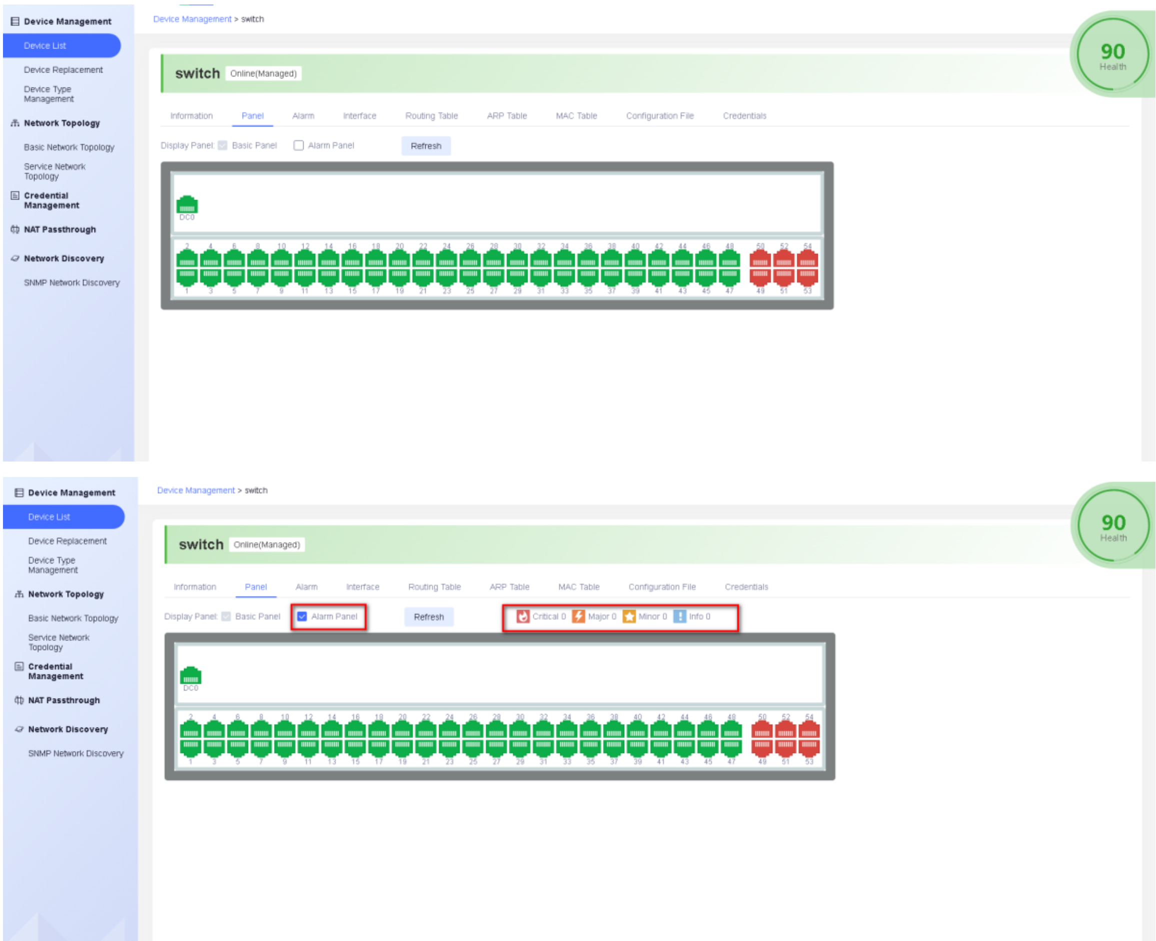


Figure 4.25 Panel details

Alarm Information

The alarm information page displays all 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.

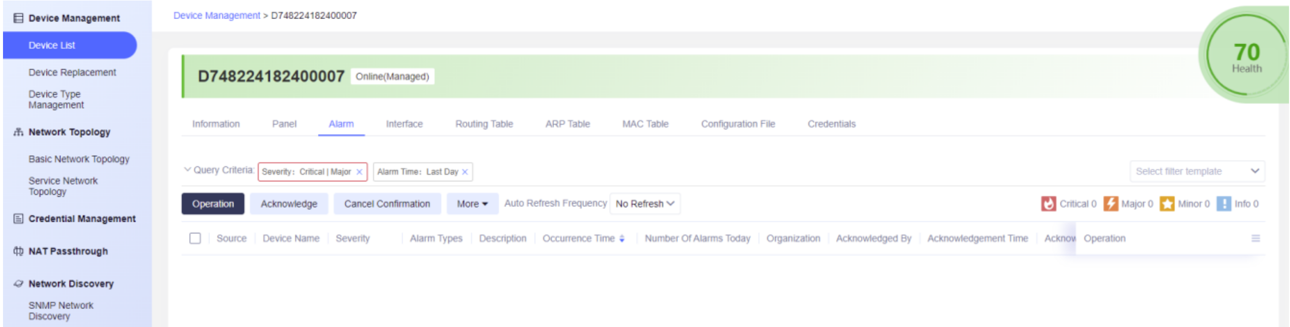
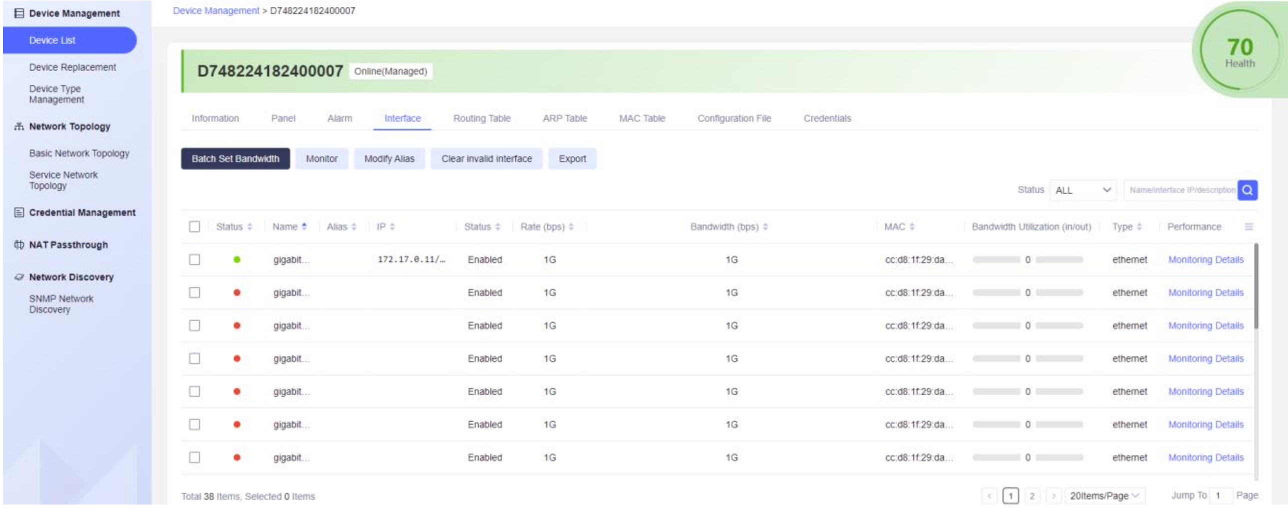


Figure 4.26 Device alarm details

Interface Information

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

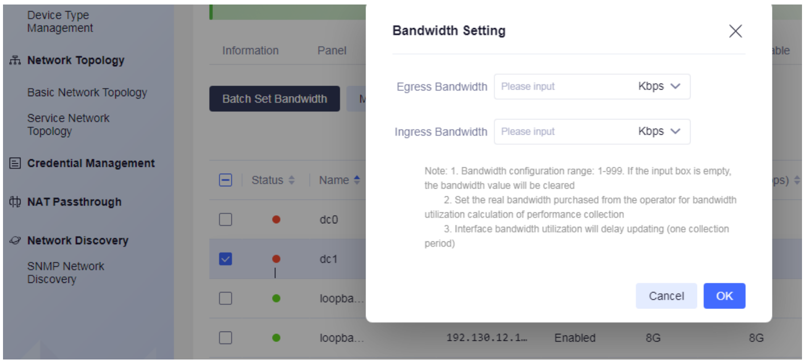


☐	Status	Name	Alias	IP	Status	Rate (bps)	Bandwidth (bps)	MAC	Bandwidth Utilization (in/out)	Type	Performance
☐	●	gigabit...		172.17.0.11/...	Enabled	1G	1G	cc:d8:1f:29:da...	0	ethernet	Monitoring Details
☐	●	gigabit...			Enabled	1G	1G	cc:d8:1f:29:da...	0	ethernet	Monitoring Details
☐	●	gigabit...			Enabled	1G	1G	cc:d8:1f:29:da...	0	ethernet	Monitoring Details
☐	●	gigabit...			Enabled	1G	1G	cc:d8:1f:29:da...	0	ethernet	Monitoring Details
☐	●	gigabit...			Enabled	1G	1G	cc:d8:1f:29:da...	0	ethernet	Monitoring Details
☐	●	gigabit...			Enabled	1G	1G	cc:d8:1f:29:da...	0	ethernet	Monitoring Details
☐	●	gigabit...			Enabled	1G	1G	cc:d8:1f:29:da...	0	ethernet	Monitoring Details

Total 38 Items, Selected 0 Items

Figure 4.27 Device interface information

Click the **Batch Set Bandwidth** button 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 it successfully. The set bandwidth and bandwidth utilization value can be displayed in the tips information by placing the mouse on the bandwidth utilization display bar.



Bandwidth Setting

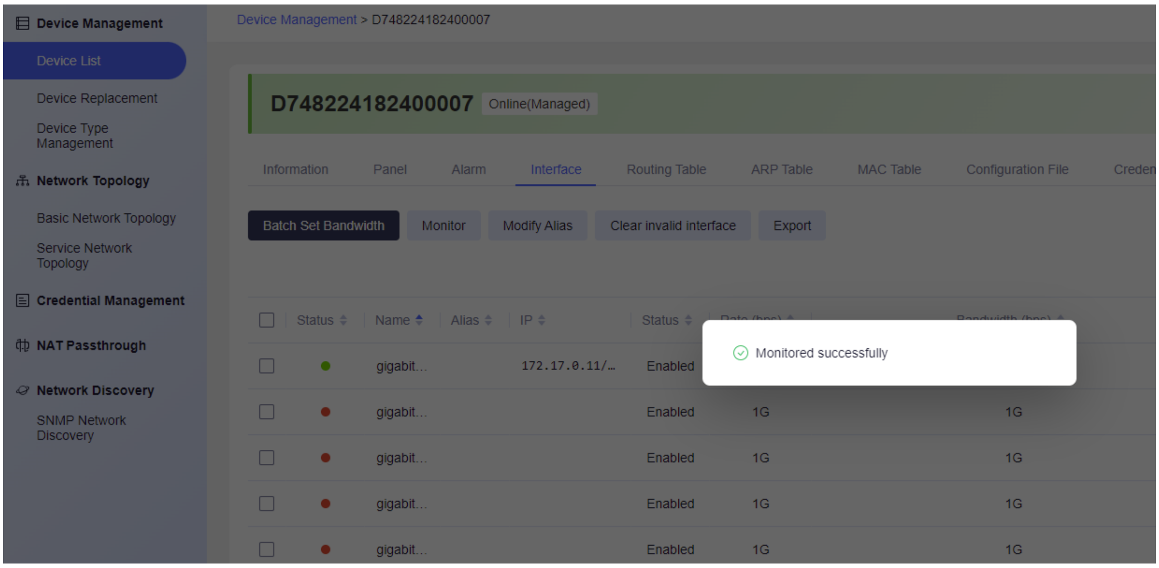
Egress Bandwidth: Please input Kbps

Ingress Bandwidth: Please input Kbps

Note: 1. Bandwidth configuration range: 1-999. If the input box is empty, the bandwidth value will be cleared
2. Set the real bandwidth purchased from the operator for bandwidth utilization calculation of performance collection
3. Interface bandwidth utilization will delay updating (one collection period)

Figure 4.28 Batch set bandwidth

Click **Monitor**, and you can add the selected interface to the interface monitoring, as shown in the following figure:



Monitored successfully

Figure 4.29 Add the device interface to monitoring

Click **Modify Alias**, and you can modify the interface alias of the selected interface, as shown in the following figure:

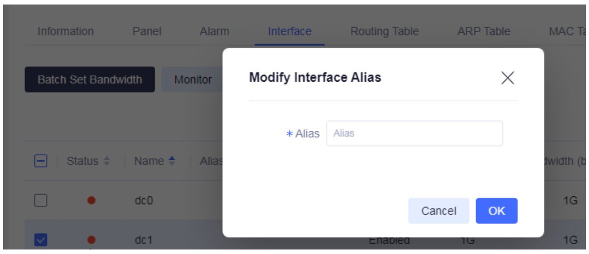


Figure 4.30 Modify the interface alias

Click the **Clear invalid interface** button to clear the interfaces that do not exist on the device in the interface list (only tunnel, loopback and VLAN interfaces can be cleared).

Click the **Monitor Data** button in the "Performance" column to jump to the corresponding monitoring page, as shown in the following figure:

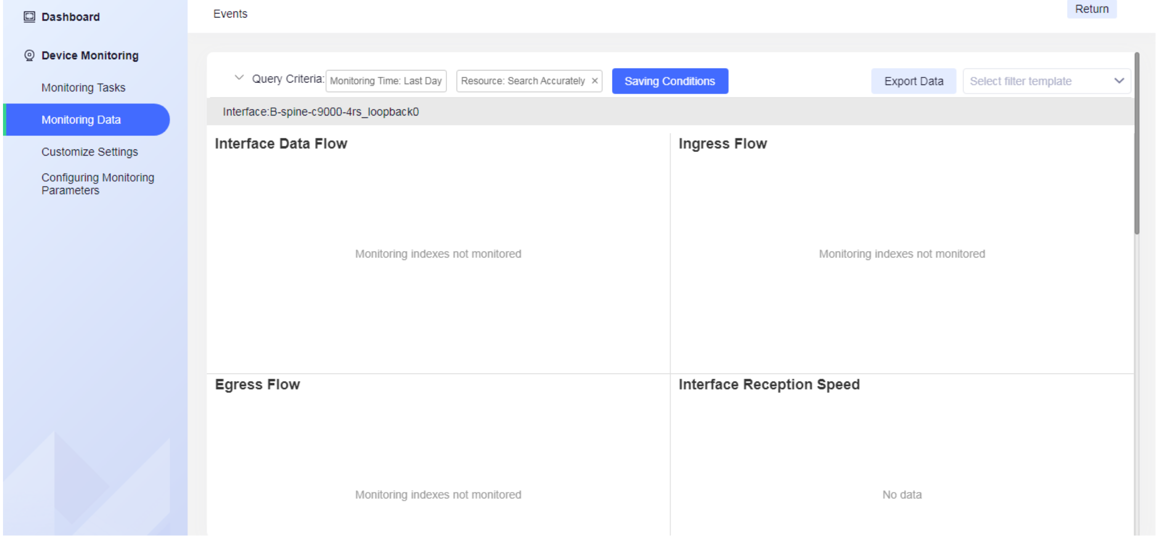
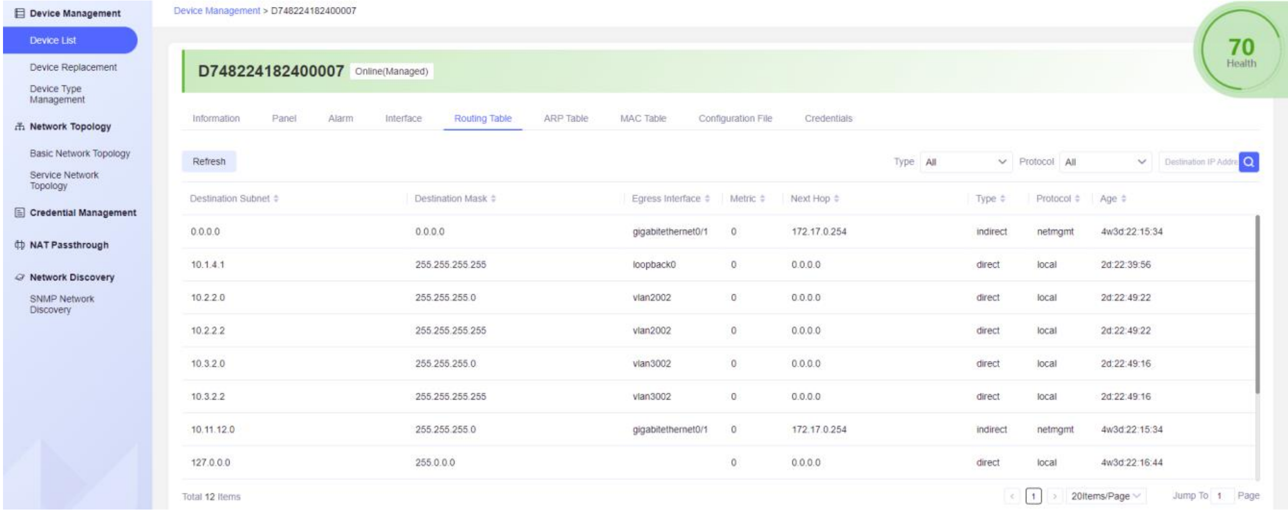

Dashboard
Device Monitoring
Monitoring Tasks
Monitoring Data
Customize Settings
Configuring Monitoring Parameters
Events
Return
Query Criteria:
Monitoring Time: Last Day
Resource: Search Accurately
Saving Conditions
Export Data
Select filter template
Interface:B-spine-c9000-4rs_loopback0
Interface Data Flow
Monitoring indexes not monitored
Ingress Flow
Monitoring indexes not monitored
Egress Flow
Monitoring indexes not monitored
Interface Reception Speed
No data

Figure 4.31 Interface monitoring

Route Table

The route table displays all routes of the device in pages, as shown in the figure below, and supports query and filtering through destination address, routing type and routing protocol.

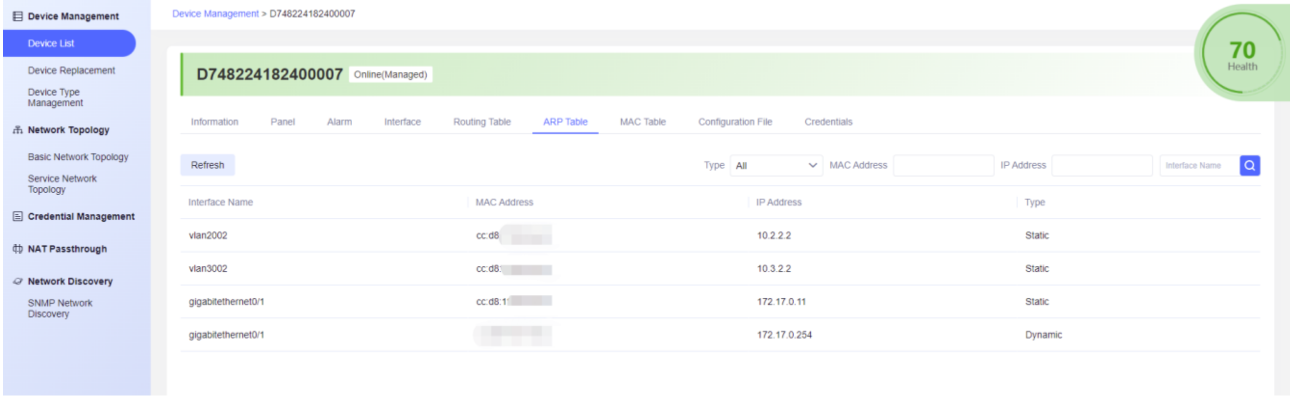


Destination Subnet	Destination Mask	Egress Interface	Metric	Next Hop	Type	Protocol	Age
0.0.0.0	0.0.0.0	gigabitethernet0/1	0	172.17.0.254	indirect	netmgmt	4w3d:22:15:34
10.1.4.1	255.255.255.255	loopback0	0	0.0.0.0	direct	local	2d:22:39:56
10.2.2.0	255.255.255.0	vlan2002	0	0.0.0.0	direct	local	2d:22:49:22
10.2.2.2	255.255.255.255	vlan2002	0	0.0.0.0	direct	local	2d:22:49:22
10.3.2.0	255.255.255.0	vlan3002	0	0.0.0.0	direct	local	2d:22:49:16
10.3.2.2	255.255.255.255	vlan3002	0	0.0.0.0	direct	local	2d:22:49:16
10.11.12.0	255.255.255.0	gigabitethernet0/1	0	172.17.0.254	indirect	netmgmt	4w3d:22:15:34
127.0.0.0	255.0.0.0		0	0.0.0.0	direct	local	4w3d:22:16:44

Figure 4.32 Route table

ARP Table

The ARP table displays the ARP table information of the device in pages, as shown in the figure below, and supports query and filtering by interface name, MAC address, IP address and type.

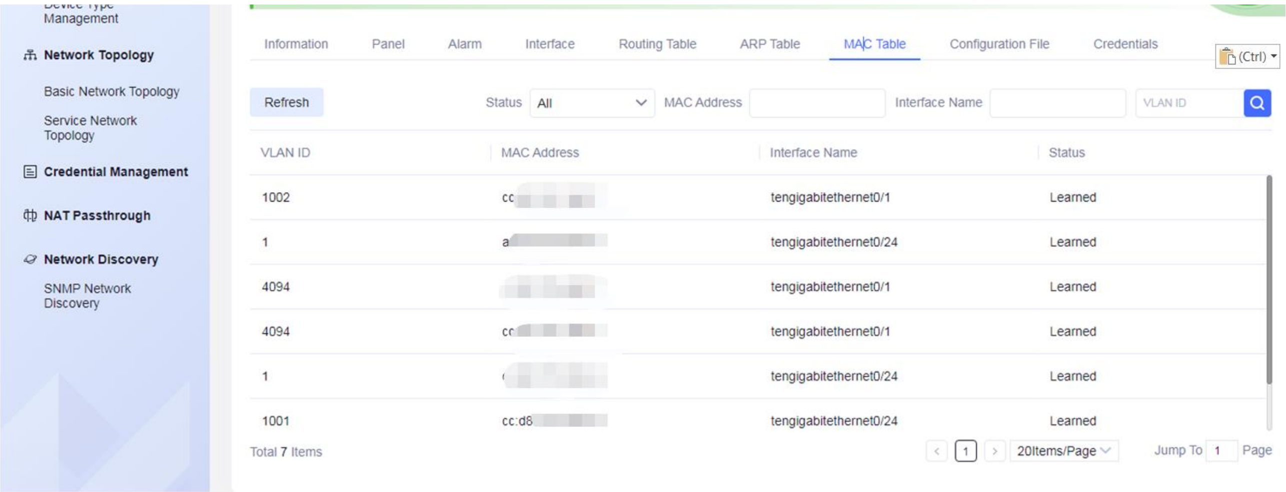


Interface Name	MAC Address	IP Address	Type
vlan2002	cc:d8[redacted]	10.2.2.2	Static
vlan3002	cc:d8[redacted]	10.3.2.2	Static
gigabitethernet0/1	cc:d8:1[redacted]	172.17.0.11	Static
gigabitethernet0/1	[redacted]	172.17.0.254	Dynamic

Figure 4.33 ARP table

MAC Table

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

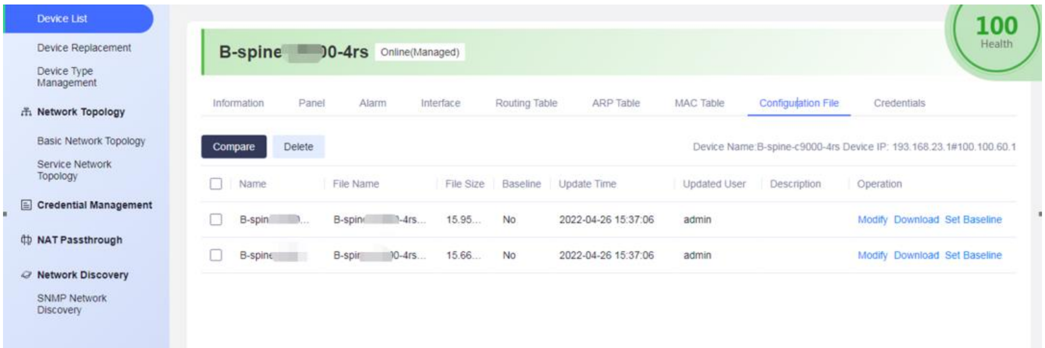


VLAN ID	MAC Address	Interface Name	Status
1002	cc[redacted]	tengigabitethernet0/1	Learned
1	a[redacted]	tengigabitethernet0/24	Learned
4094	[redacted]	tengigabitethernet0/1	Learned
4094	cc[redacted]	tengigabitethernet0/1	Learned
1	[redacted]	tengigabitethernet0/24	Learned
1001	cc:d8[redacted]	tengigabitethernet0/24	Learned

Figure 4.34 MAC table

Configuration File

Configuration files are the management of configuration files backed up by devices. You can compare two configuration files and download configuration files



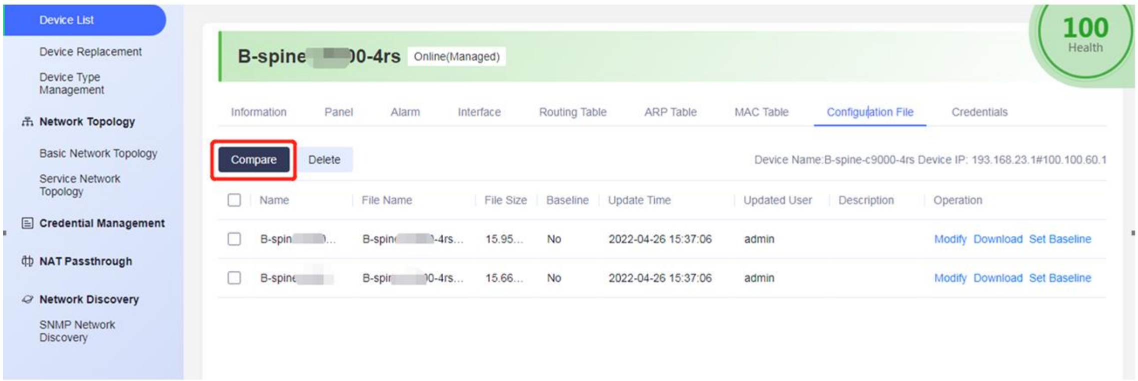
Device Name:B-spine-c9000-4rs Device IP: 193.168.23.1#100.100.60.1

☐	Name	File Name	File Size	Baseline	Update Time	Updated User	Description	Operation
☐	B-spin[redacted]...	B-spin[redacted]-4rs...	15.95...	No	2022-04-26 15:37:06	admin		Modify Download Set Baseline
☐	B-spine[redacted]	B-spir[redacted]0-4rs...	15.66...	No	2022-04-26 15:37:06	admin		Modify Download Set Baseline

Figure 4.35 Device configuration file

Compare configuration files:

You can compare the similarities and differences between the two configuration files, as shown in the following figure:



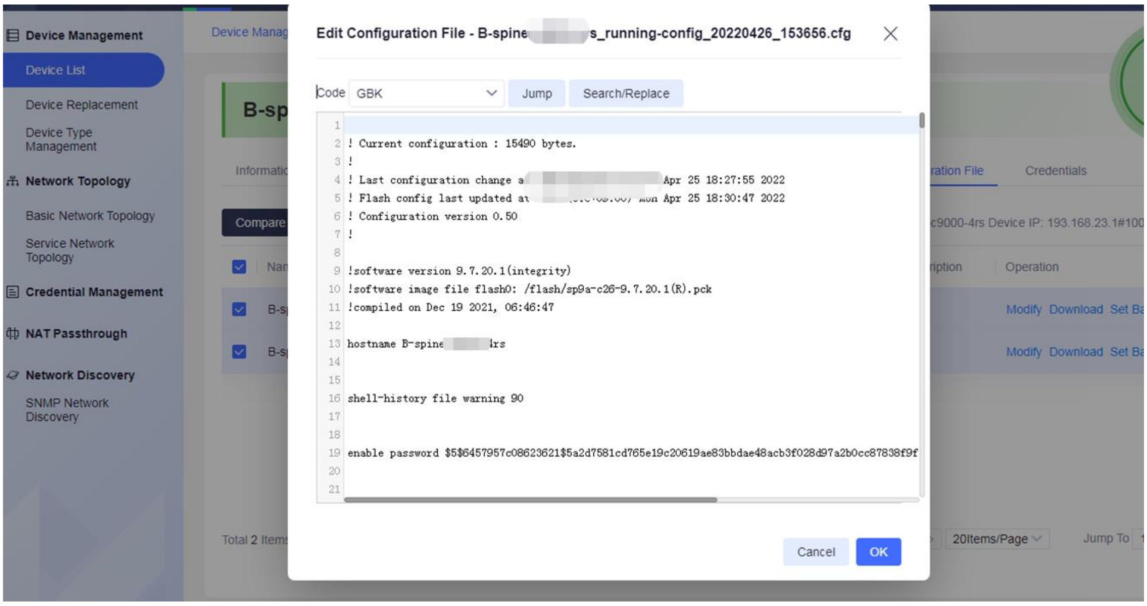
Device Name:B-spine-c9000-4rs Device IP: 193.168.23.1#100.100.60.1

☐	Name	File Name	File Size	Baseline	Update Time	Updated User	Description	Operation
☐	B-spin[redacted]...	B-spin[redacted]-4rs...	15.95...	No	2022-04-26 15:37:06	admin		Modify Download Set Baseline
☐	B-spine[redacted]	B-spir[redacted]0-4rs...	15.66...	No	2022-04-26 15:37:06	admin		Modify Download Set Baseline

Figure 4.36 Compare the configuration files

Modify configuration files:

You can modify the code of the configuration file, find the file content, and jump to the specified number of lines of the file:

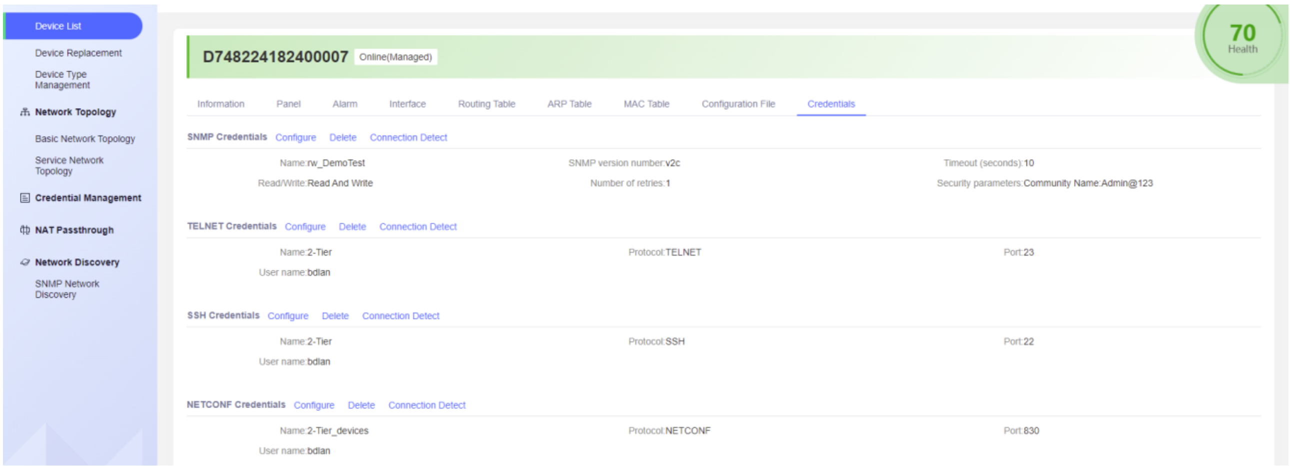


```
! Current configuration : 15490 bytes.
!
! Last configuration change a[redacted]Apr 25 18:27:55 2022
! Flash config last updated at[redacted]Apr 25 18:30:47 2022
! Configuration version 0.50
!

!software version 9.7.20.1(integrity)
!software image file flash0: /flash/sp9a-c26-9.7.20.1(R).pck
!compiled on Dec 19 2021, 06:46:47

hostname B-spine[redacted]lrs


shell-history file warning 90


enable password $5$6457957c08623621$5a2d7581cd765e19c20619ae83bbdae48acb3f028d97a2b0cc87838f9f


```

Figure 4.37 Modify device configuration file

Device Credential

snmp credential/telnet credential/ssh credential/netconf credential can display the credential information configured by the current device in pages and support modifying the corresponding credential of the device, as shown in the following figure:



D748224182400007 Online(Managed)

SNMP Credentials
Name:rw_DemoTest
SNMP version number:v2c
Timeout (seconds):10
Read/Write:Read And Write
Number of retries:1
Security parameters:Community Name:Admin@123

TELNET Credentials
Name:2-Tier
Protocol:TELNET
Port:23
User name:bdlan

SSH Credentials
Name:2-Tier
Protocol:SSH
Port:22
User name:bdlan

NETCONF Credentials
Name:2-Tier_devices
Protocol:NETCONF
Port:830
User name:bdlan

Figure 4.38 Device credential

Click the "Connection Detect" link in the credential list to check whether the corresponding credential is available to the device.

Note

- When modifying a device credential, only the credentials of the organization to which the current device belongs are displayed in the optional credential list.

4.1.2 Replace by One Key

Caution

- The configuration file used by the auto selection of device replacement is the startup configuration file backed up by the old device last time or the configuration file uploaded manually. The configuration file automatically selected by the stacking device replacement is the configuration file used by the member in the last DHCP opening;
- Device replacement needs to ensure that the model, software and hardware version and physical connection of the old and new devices are consistent;
- Stacking device replacement only supports DHCP starting mode replacement. In order to prevent loop, disconnect the connection from other member devices to the upper connection port;

Device replacement: Use this function when the device fails or other cases require smooth transition from the new device to the current network; The configuration file of the corresponding device needs to be backed up (if it is a non-stacked device, it also supports manual uploading of the configuration file for replacement). At present, Telnet, SSH and DHCP starting modes are supported for replacement respectively. After confirming the existence of the backup file or manually uploading the file, it can be replaced. The telnet and SSH replacement process is to distribute the backup configuration file to the new device through telnet or SSH. The DHCP starting replacement needs to go through the start process on the device side, and the configuration file used is the configuration file used in the last starting of the member device to be replaced; Click "Basic Network" - > " Device Management" - > "Device Replacement" on the navigation bar at the top of the system, as shown in the figure:

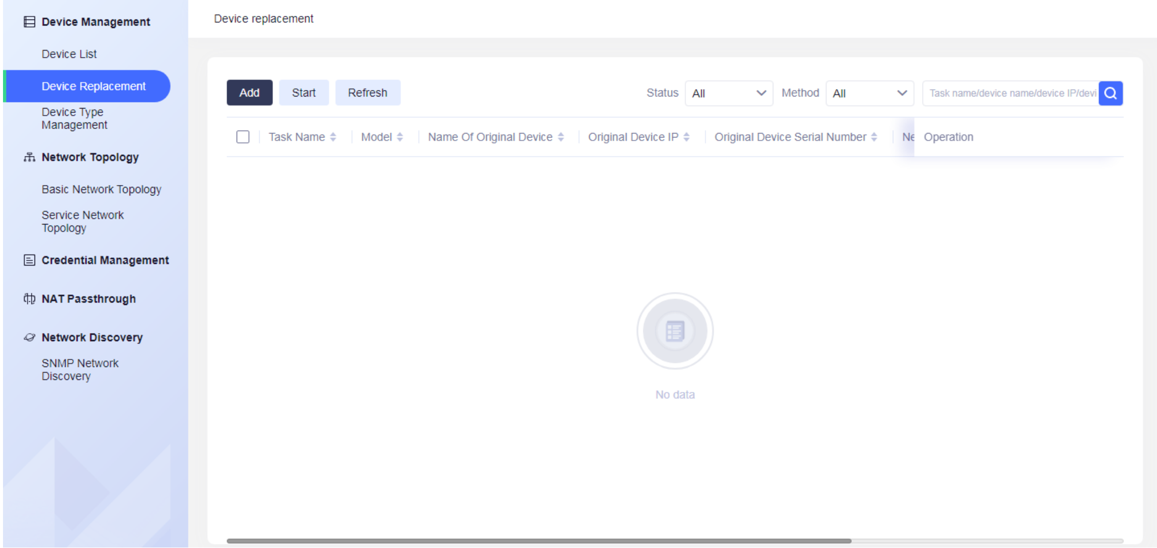


Figure 4.39 Replace by one key

Replacing Task Management Interface

After entering the device replacement page, the main functions include creating tasks, modifying, starting, stopping, deleting, refreshing, etc. The query function can be paged through task status, distribution method, task name, device name, IP and other keywords, as shown in the figure:

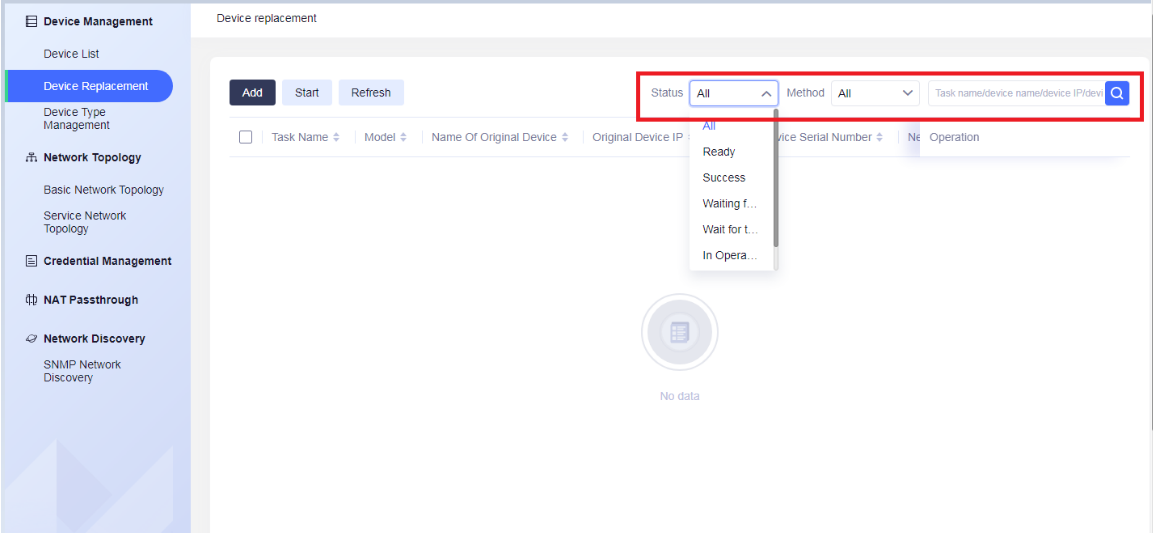
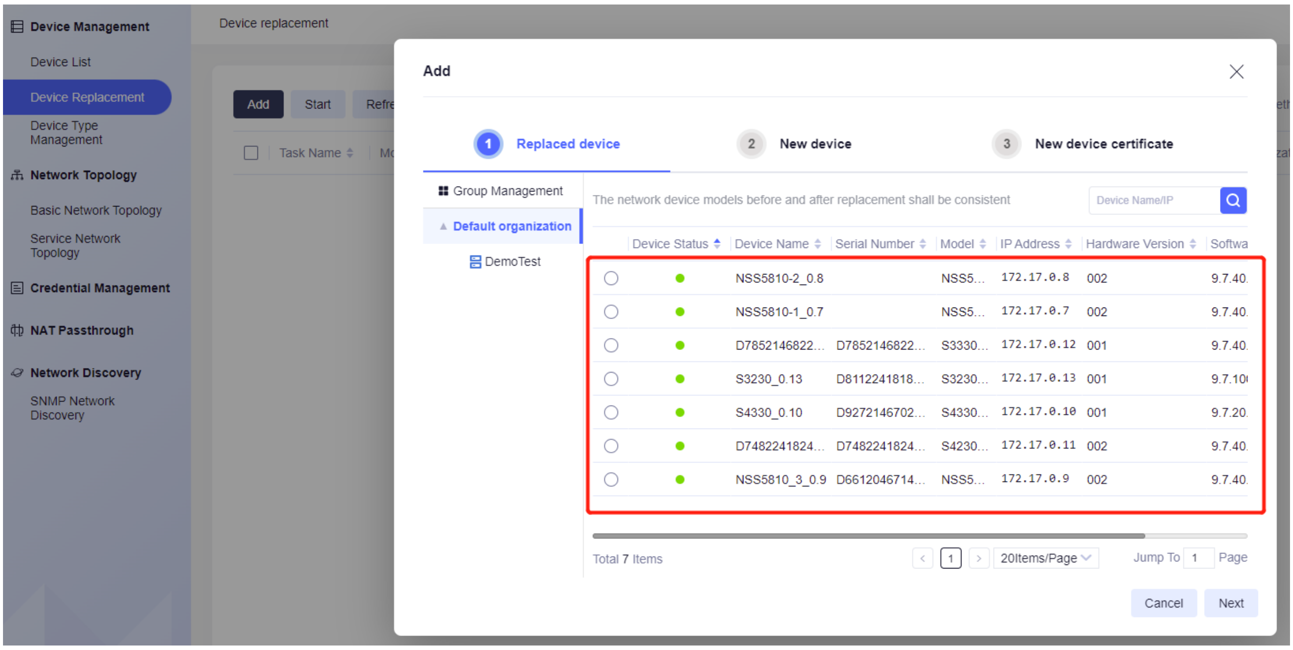


Figure 4.40 One-key replacement query

Create Replacement Task

Select the device to be replaced:

Enter the device replacement page and click the "Add" button in the upper left corner to create a new replacement task. Non-stacked devices support Telnet, SSH and DHCP replacement. Stacked devices currently only support DHCP start replacement. The new operation is shown in the figure, showing the pages of non-stacking device and stacking device replacement respectively:



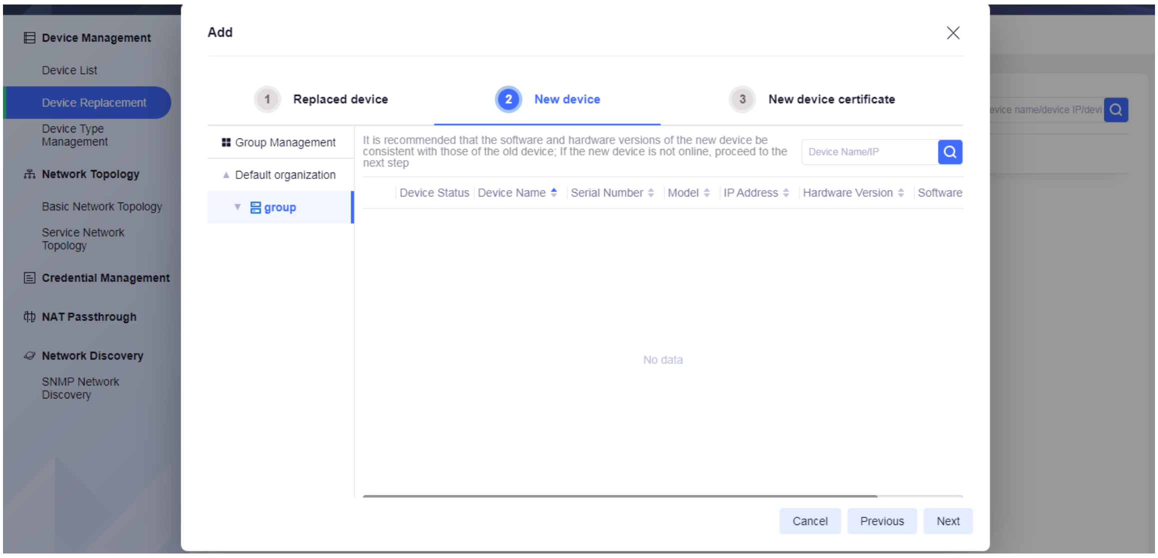
The network device models before and after replacement shall be consistent

	Device Status	Device Name	Serial Number	Model	IP Address	Hardware Version	Softwa
○	●	NSS5810-2_0.8		NSS5...	172.17.0.8	002	9.7.40.
○	●	NSS5810-1_0.7		NSS5...	172.17.0.7	002	9.7.40.
○	●	D7852146822...	D7852146822...	S3330...	172.17.0.12	001	9.7.40.
○	●	S3230_0.13	D8112241818...	S3230...	172.17.0.13	001	9.7.10
○	●	S4330_0.10	D9272146702...	S4330...	172.17.0.10	001	9.7.20.
○	●	D7482241824...	D7482241824...	S4230...	172.17.0.11	002	9.7.40.
○	●	NSS5810_3_0.9	D6612046714...	NSS5...	172.17.0.9	002	9.7.40.

Figure 4.41 Step 1 of adding replacement task (non-stacked device)

Select new device:

After selecting a desired old device, click **Next**. If the device is online, a prompt box will pop up. If it is a non-stacked device, you can select the discovered device as the new device. If the new device is not discovered, you can skip this step; If it is a stacked member device, the second step will be skipped automatically, and directly enter the third step to configure the relevant configuration of DHCP start replacement; See the figure below for details:



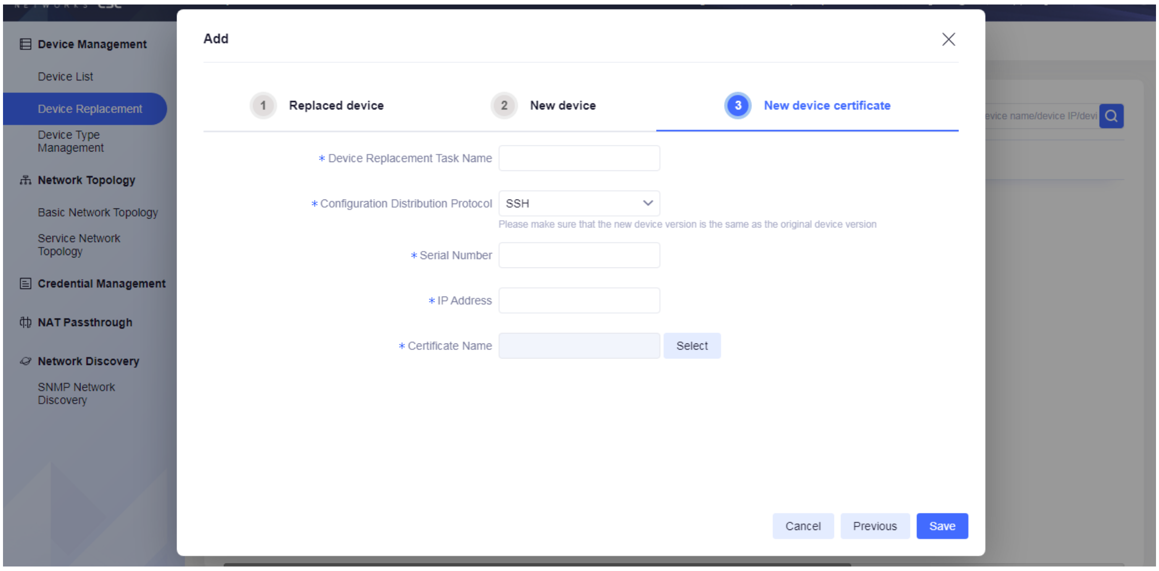
It is recommended that the software and hardware versions of the new device be consistent with those of the old device; If the new device is not online, proceed to the next step

Figure 4.42 Step 2 of adding replacement task (non-stacked device)

Note that the new device page will force matching the device model of the old device for filtering. Only the devices with the same software and hardware version will be listed. The devices with the same model but different software and hardware versions will be displayed, but cannot be selected; If the new device is not discovered, you can skip this step and configure it in the third step (new device connection information).

New device certificate:

There are four configuration distribution protocols currently supported, as shown in the figure:



∗ Device Replacement Task Name

∗ Configuration Distribution Protocol: SSH

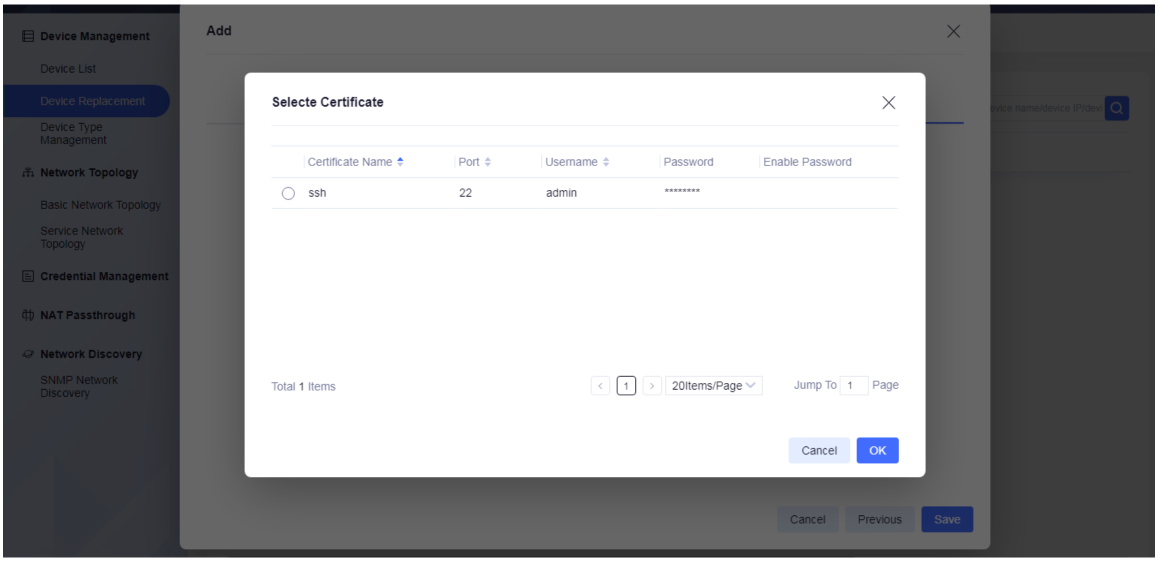
Please make sure that the new device version is the same as the original device version

∗ Serial Number

∗ IP Address

∗ Certificate Name

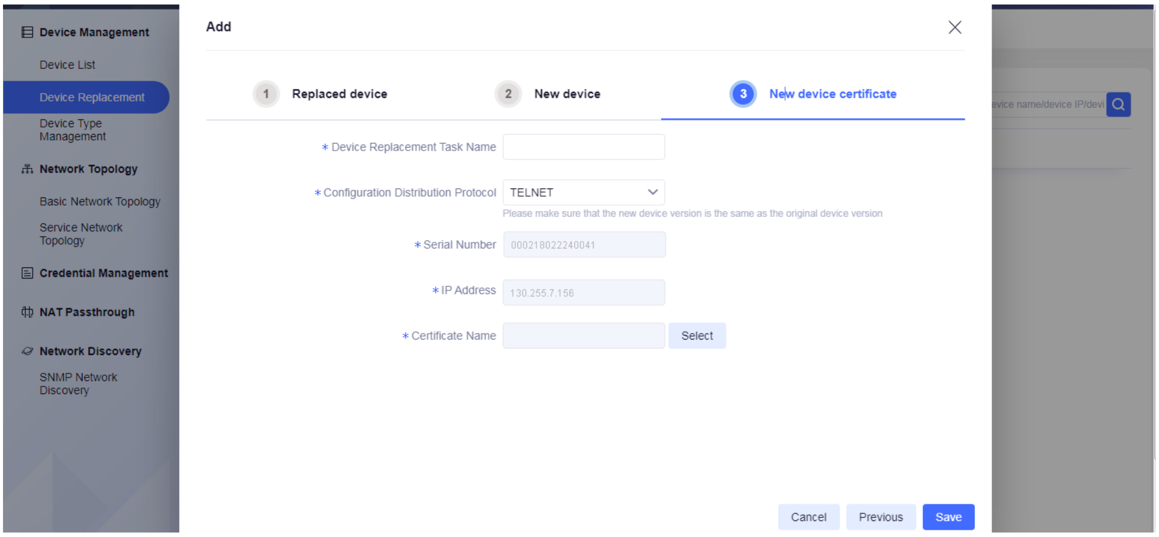
Figure 4.43 Add replacement task-SSH configuration distribution



	Certificate Name	Port	Username	Password	Enable Password
○	ssh	22	admin	********	

Total 1 Items 1 20Items/Page Jump To 1 Page

Figure 4.44 Add replacement task-SSH configuration distribution-select SSH certificate



∗ Device Replacement Task Name

∗ Configuration Distribution Protocol: TELNET

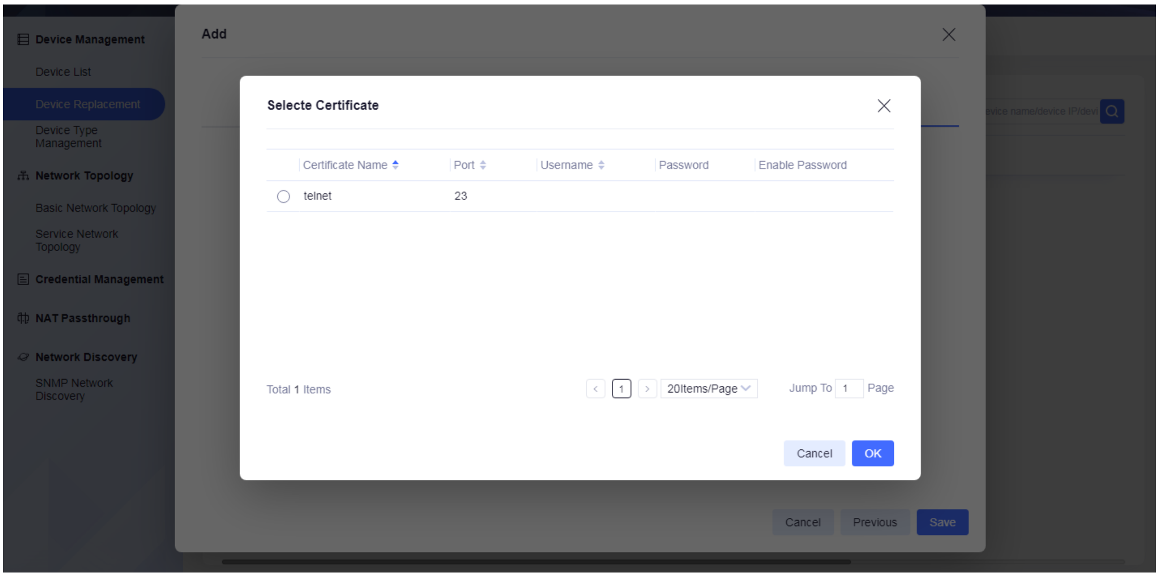
Please make sure that the new device version is the same as the original device version

∗ Serial Number: 000218022240041

∗ IP Address: 130.255.7.156

∗ Certificate Name

Figure 4.45 Add replacement task-TELNET configuration distribution

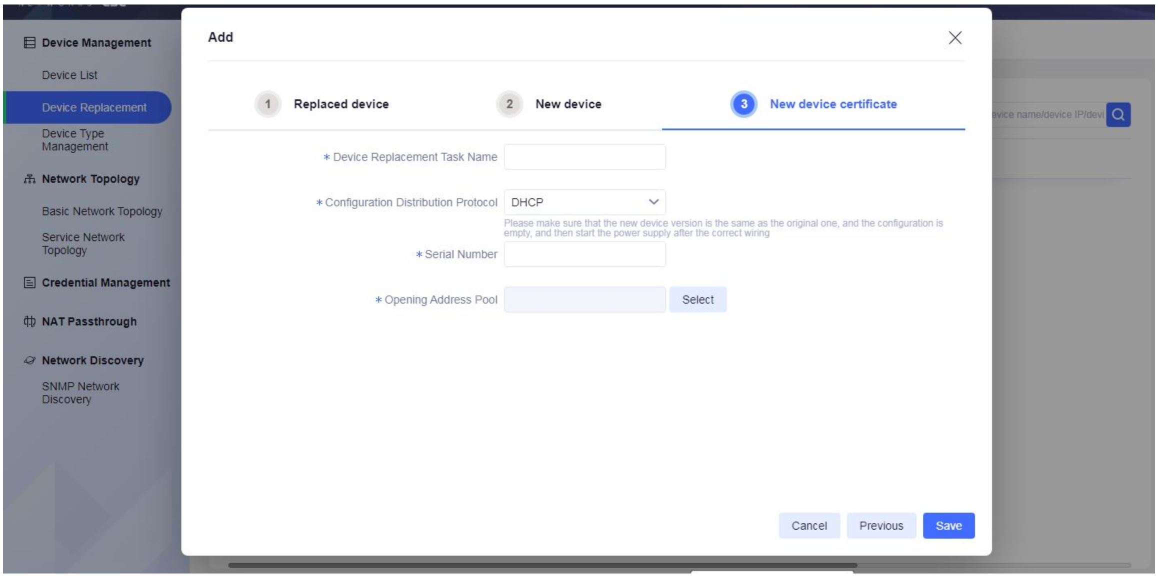


Selecte Certificate

	Certificate Name	Port	Username	Password	Enable Password
○	telnet	23			

Total 1 Items

Figure 4.46 Add replacement task –TELNET configuration distribution – Select TELNET certificate



* Device Replacement Task Name

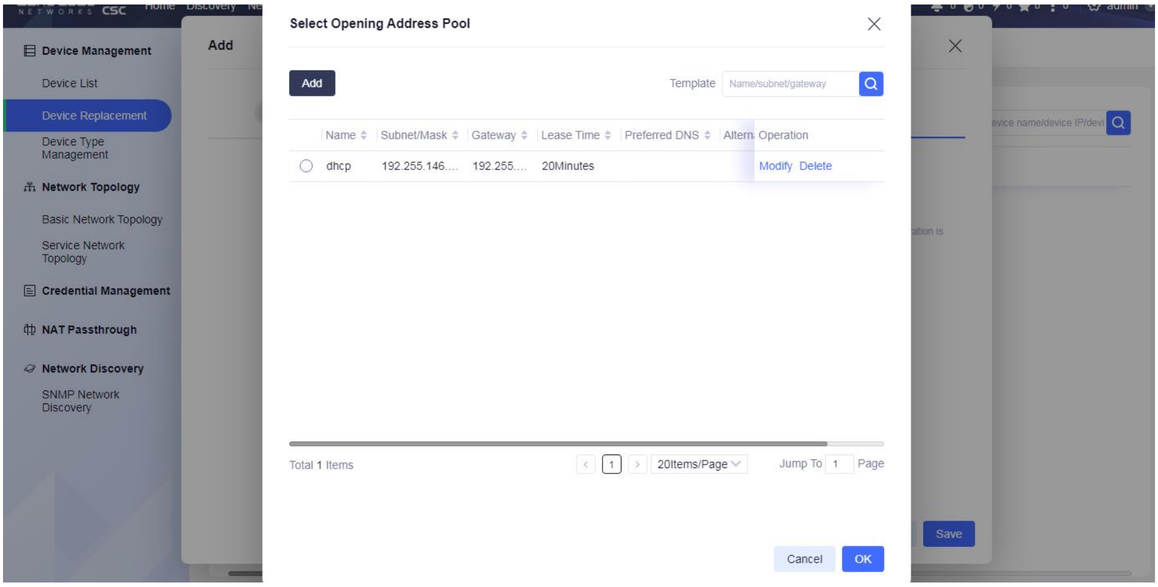
* Configuration Distribution Protocol: DHCP

Please make sure that the new device version is the same as the original one, and the configuration is empty, and then start the power supply after the correct wiring

* Serial Number

* Opening Address Pool

Figure 4.47 Add replacement task –DHCP configuration distribution



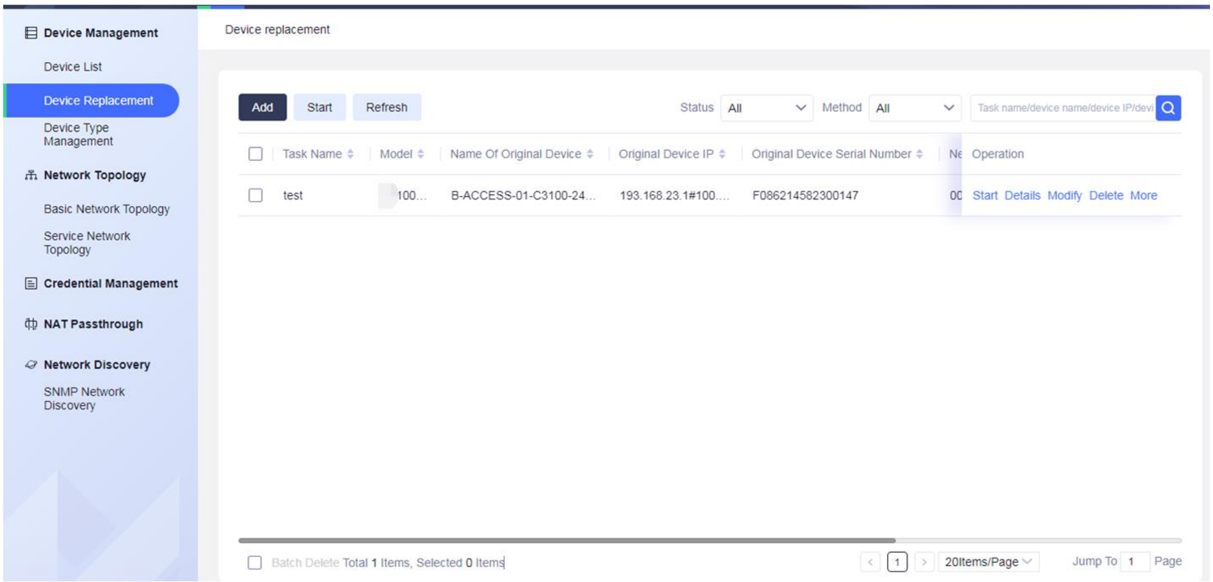
Select Opening Address Pool

	Name	Subnet/Mask	Gateway	Lease Time	Preferred DNS	Altern	Operation
○	dhcp	192.255.146....	192.255....	20Minutes			Modify Delete

Total 1 Items

Figure 4.48 Add replacement task - DHCP configuration distribution –Select DHCP opening address pool

After filling in the configuration information of the new device, click the "Save" button at the bottom right. In the telnet and SSH channel mode, if the new device is not selected in the second step, the new device will be automatically connected. After passing the verification, the new device will be saved to the network management. The corresponding device replacement task will be created successfully and displayed as ready.



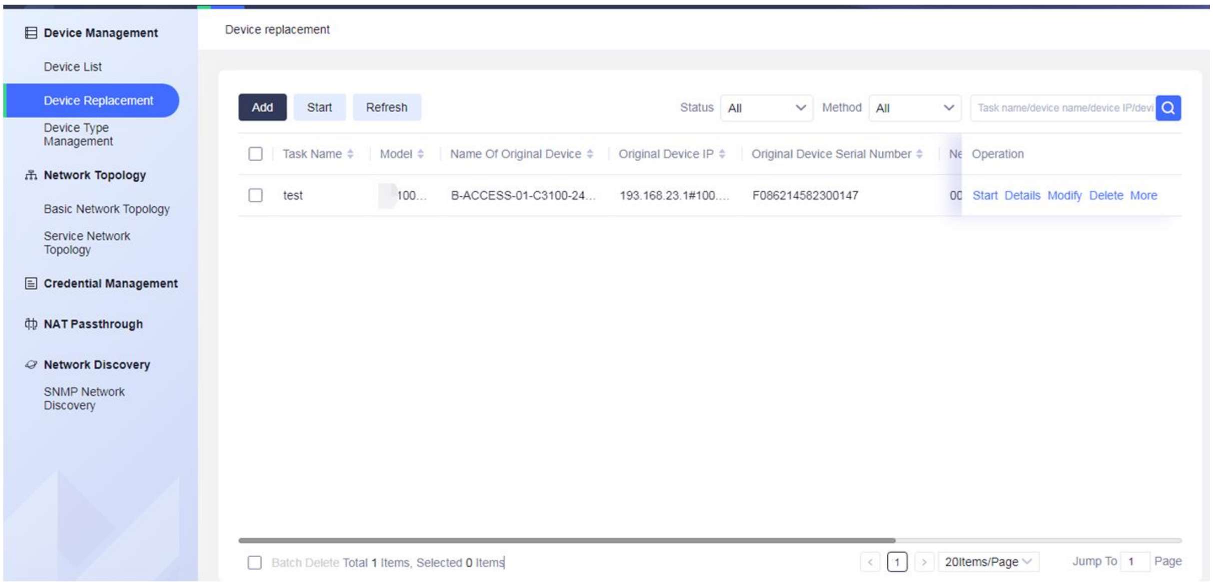
☐	Task Name	Model	Name Of Original Device	Original Device IP	Original Device Serial Number	Ne	Operation
☐	test	100...	B-ACCESS-01-C3100-24...	193.168.23.1#100....	F086214582300147	00	Start Details Modify Delete More

Total 1 Items, Selected 0 Items

Figure 4.49 Add replacement task successfully

Execute Replacement Task

The newly created device replacement task is ready. At this time, it is necessary to ensure that the physical connection of the new device has been connected. The replacement methods of telnet and SSH ensure that the configuration can be restored through the IP and credential information, and the DHCP method needs to ensure that the DHCP network can be accessed. Click the **Start** button and the device will start to replace. If it is required by DHCP mode, it will be in the state of "Wait for the device to start". Please carry out the start steps on the device side (see the DHCP start operation process for details). After the device is connected to the DHCP server, it will change to the state of "In progress".

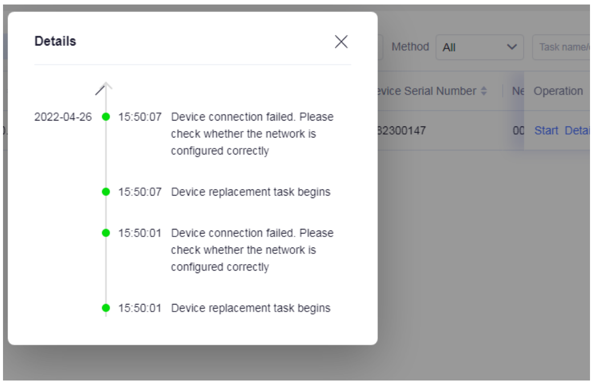


☐	Task Name	Model	Name Of Original Device	Original Device IP	Original Device Serial Number	Ne	Operation
☐	test	100...	B-ACCESS-01-C3100-24...	193.168.23.1#100....	F086214582300147	00	Start Details Modify Delete More

Total 1 Items, Selected 0 Items

Figure 4.50 Start replacement task

The details of the replacement steps can be viewed by clicking the "Details" icon in the "Operation bar", as shown in figures 8.3.2 and 8.3.3 (the replacement process of SSH mode is the same as that of Telnet):



2022-04-26 15:50:07 Device connection failed. Please check whether the network is configured correctly

15:50:07 Device replacement task begins

15:50:01 Device connection failed. Please check whether the network is configured correctly

15:50:01 Device replacement task begins

Figure 4.51 Replacement task details

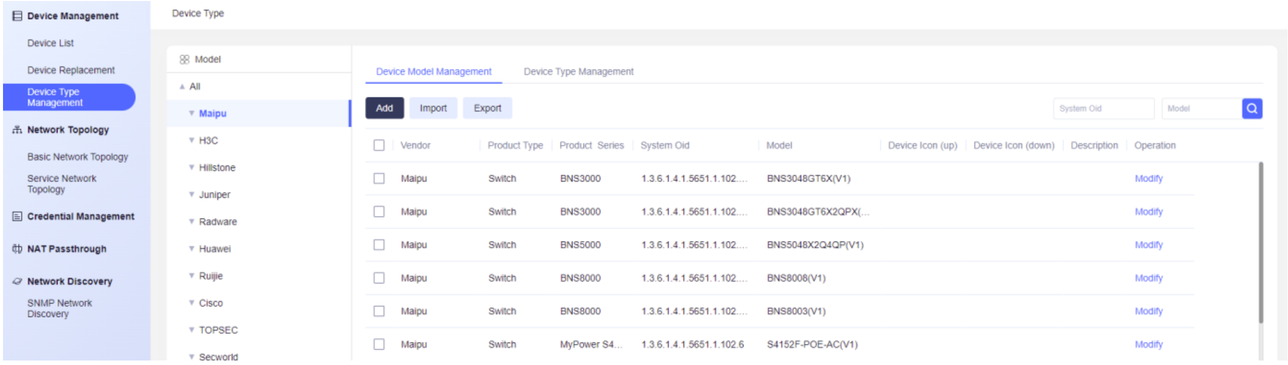
After the replacement of non-stacked devices, check whether the physical information systemid, MAC, serial number, etc. of the replaced device have been replaced with the physical information of the new device, and whether other credential information is normal; For stacking devices, please check whether the physical properties of device member information have changed. You can check it on the page of selecting old devices for the replacement function.

Caution

- The overall replacement of stacking devices requires the establishment of multiple DHCP replacement tasks.

4.1.3 Device Type Management

Click "Basic Network" in the navigation bar at the top of the system to open the interface of "Device Management" > "Device Type Management". The module includes device model management and device type management. The model and manufacturer information of a device and the icon display information in different states (down, up and unknown) in the topology are set in this module. The module is inbuilt with the model information of some Maipu devices. For the device models of other manufacturers, you need to add manually, as shown below



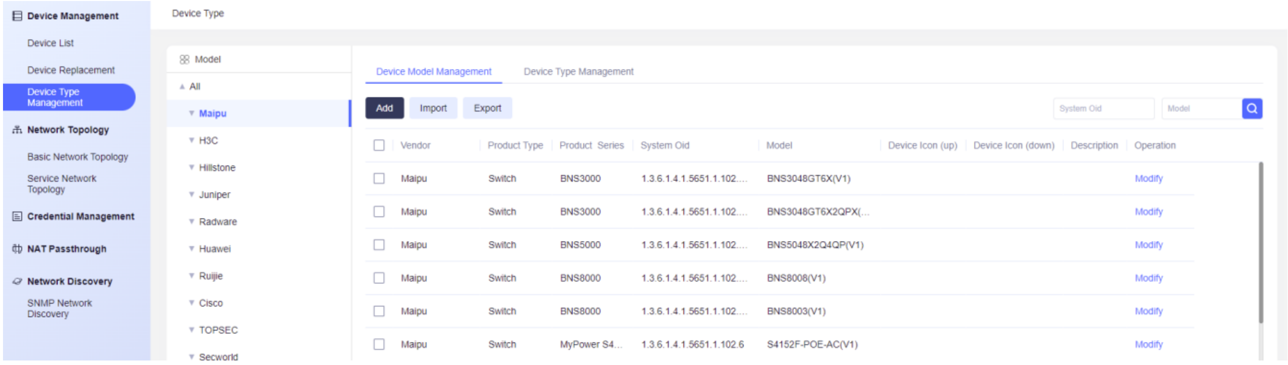
☐	Vendor	Product Type	Product Series	System Oid	Model	Device Icon (up)	Device Icon (down)	Description	Operation
☐	Maipu	Switch	BNS3000	1.3.6.1.4.1.5651.1.102....	BNS3048GT6X(V1)				Modify
☐	Maipu	Switch	BNS3000	1.3.6.1.4.1.5651.1.102....	BNS3048GT6X2QPX(...				Modify
☐	Maipu	Switch	BNS5000	1.3.6.1.4.1.5651.1.102....	BNS5048X2Q4QP(V1)				Modify
☐	Maipu	Switch	BNS8000	1.3.6.1.4.1.5651.1.102....	BNS8008(V1)				Modify
☐	Maipu	Switch	BNS8000	1.3.6.1.4.1.5651.1.102....	BNS8003(V1)				Modify
☐	Maipu	Switch	MyPower S4...	1.3.6.1.4.1.5651.1.102.6	S4152F-POE-AC(V1)				Modify

Figure 4.52 Device type management

Device Model Management

The device model management module provides the function of adding/editing/deleting specific device models under the device type. At the same time, it also supports fuzzy query through the sysoid and device model of the device. Both the topology module and the device list module query the model, manufacturer and icons to be displayed in different states of the device in this module through the sysoid of the device.

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



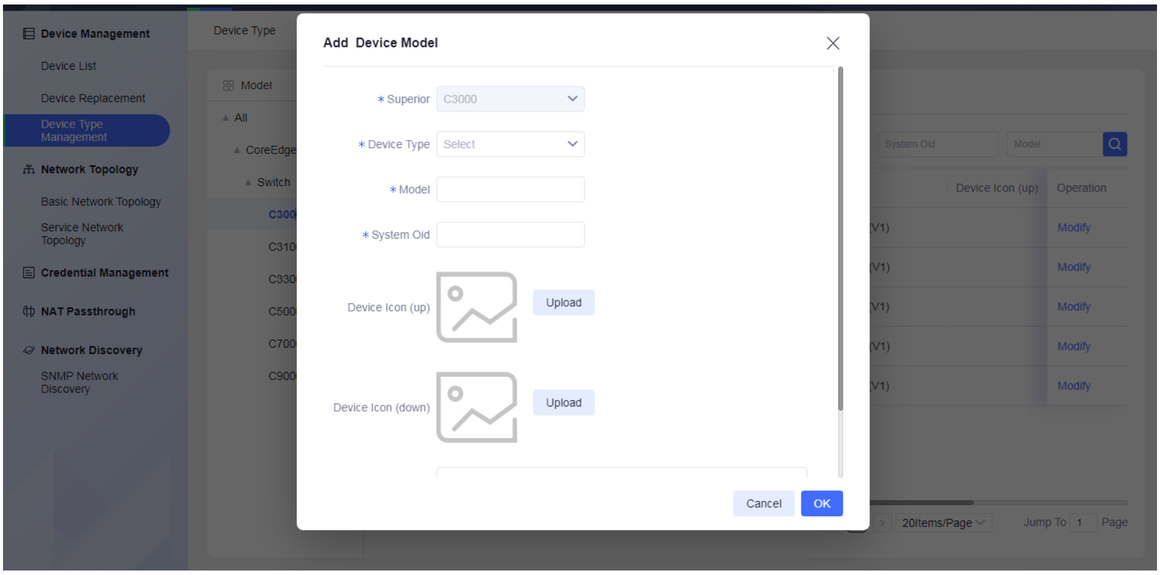
☐	Vendor	Product Type	Product Series	System Oid	Model	Device Icon (up)	Device Icon (down)	Description	Operation
☐	Maipu	Switch	BNS3000	1.3.6.1.4.1.5651.1.102....	BNS3048GT6X(V1)				Modify
☐	Maipu	Switch	BNS3000	1.3.6.1.4.1.5651.1.102....	BNS3048GT6X2QPX(...				Modify
☐	Maipu	Switch	BNS5000	1.3.6.1.4.1.5651.1.102....	BNS5048X2Q4QP(V1)				Modify
☐	Maipu	Switch	BNS8000	1.3.6.1.4.1.5651.1.102....	BNS8008(V1)				Modify
☐	Maipu	Switch	BNS8000	1.3.6.1.4.1.5651.1.102....	BNS8003(V1)				Modify
☐	Maipu	Switch	MyPower S4...	1.3.6.1.4.1.5651.1.102.6	S4152F-POE-AC(V1)				Modify

Figure 4.53 Device model management

Add/edit/delete device model:

First select the manufacturer/type/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 superior displays the manufacturer/type/product series in the left tree 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 device model, and then click the **Modify** button at the top of the device model list to modify the model; 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; Click the **Export** button at the top of the device model list to export the model type. Select a device type and click on the top of the device model list.



* Superior: C3000

Figure 4.54 Add device model

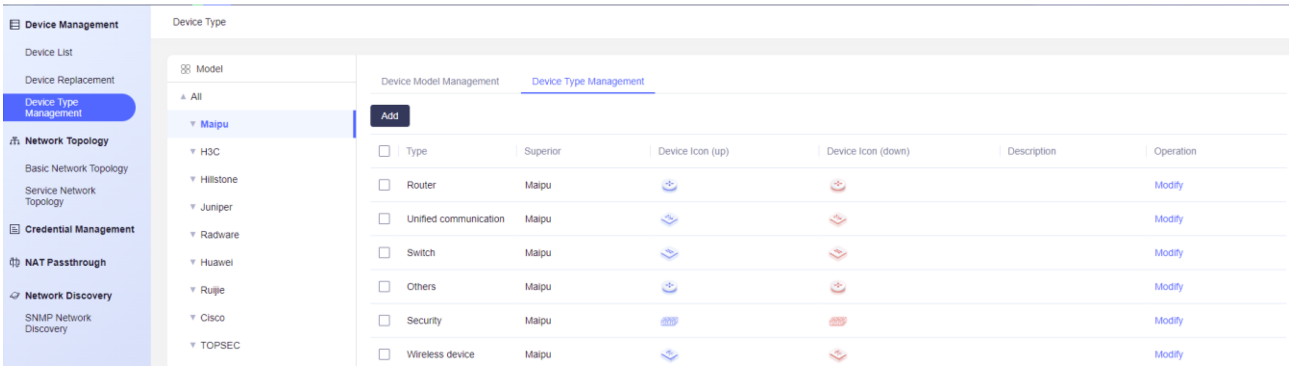
Note

- Under the same type directory, the device model name cannot be the same.
- The device model system oid field is globally unique and cannot be duplicated.

- The built-in device type and device model of the controller cannot be deleted.

Device Type Management

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



☐	Type	Superior	Device Icon (up)	Device Icon (down)	Description	Operation
☐	Router	Maipu				Modify
☐	Unified communication	Maipu				Modify
☐	Switch	Maipu				Modify
☐	Others	Maipu				Modify
☐	Security	Maipu				Modify
☐	Wireless device	Maipu				Modify

Figure 4.55 Device type management

Add/edit/delete device type:

Click the **Add** button at the top of the device type list to open the “Add Device Category” dialog box. You need to fill in the type name, manufacturer ID, device icon and description fields, which are optional fields and can be left blank.

The superior displays "All" by default, which cannot be modified by the user. The system will think 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 A.2, add one piece of information of manufacturer A. After correctly filling in all fields in the dialog box, click the **OK** button to add successfully.

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

In device type management, select a type, click **Modify** at the top of the device type list to modify the device type, and click **Delete** at the top of the device type list to delete the device type. After deleting the device type, all sub-types and device model information under the type will be deleted at the same time.

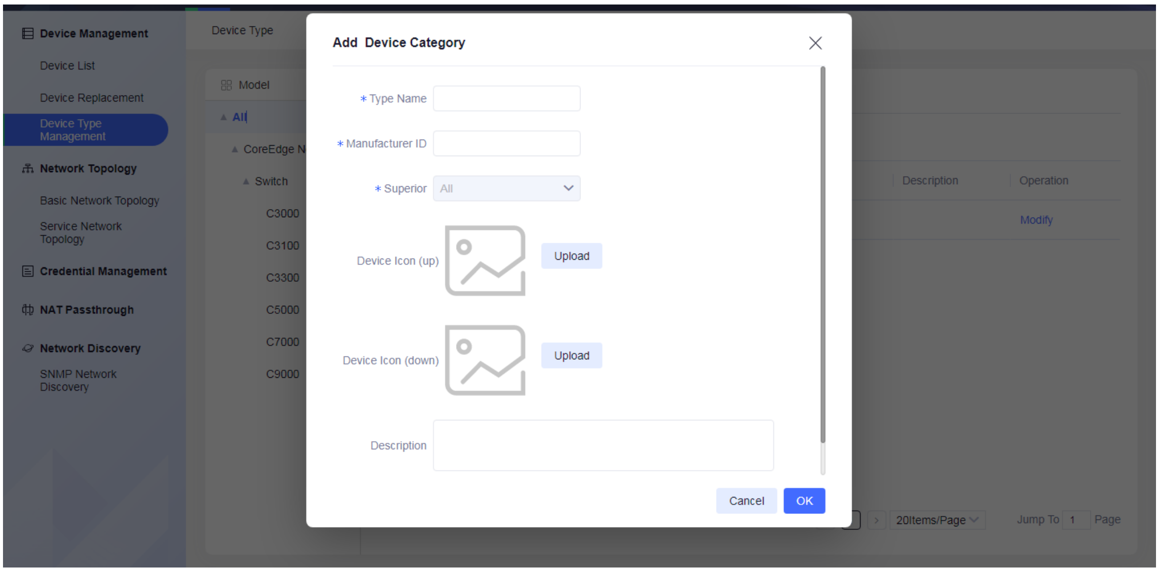


Figure 4.56 Add device type

Note

- Under the same type directory, the device type name cannot be the same.
- The manufacturer ID exists in the device sysoid and is an integer and cannot be repeated. Please query the correct manufacturer ID and fill it in.

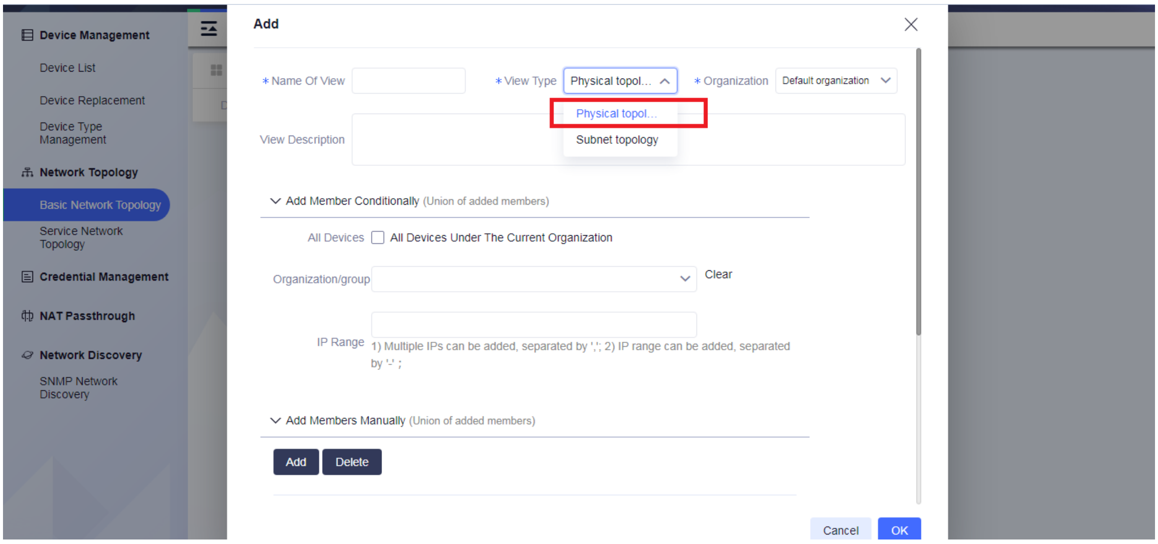
4.2 Network Topology

4.2.1 Basic Network Topology

View Management

Add Physical Topology

Click "Basic Network" in the top menu bar, select "Network Topology" submenu, open the topology management page, click the icon ☰ and the icon + in the upper left corner, select "Physical Topology" on the pop-up "Add" page, and complete the input of the other items, as shown in the figure;



* View Type: Physical topol...

* Organization: Default organization

All Devices ☐ All Devices Under The Current Organization

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

Figure 4.57 Add physical topology view

Click **OK** to generate the physical topology view, as shown in the following figure:

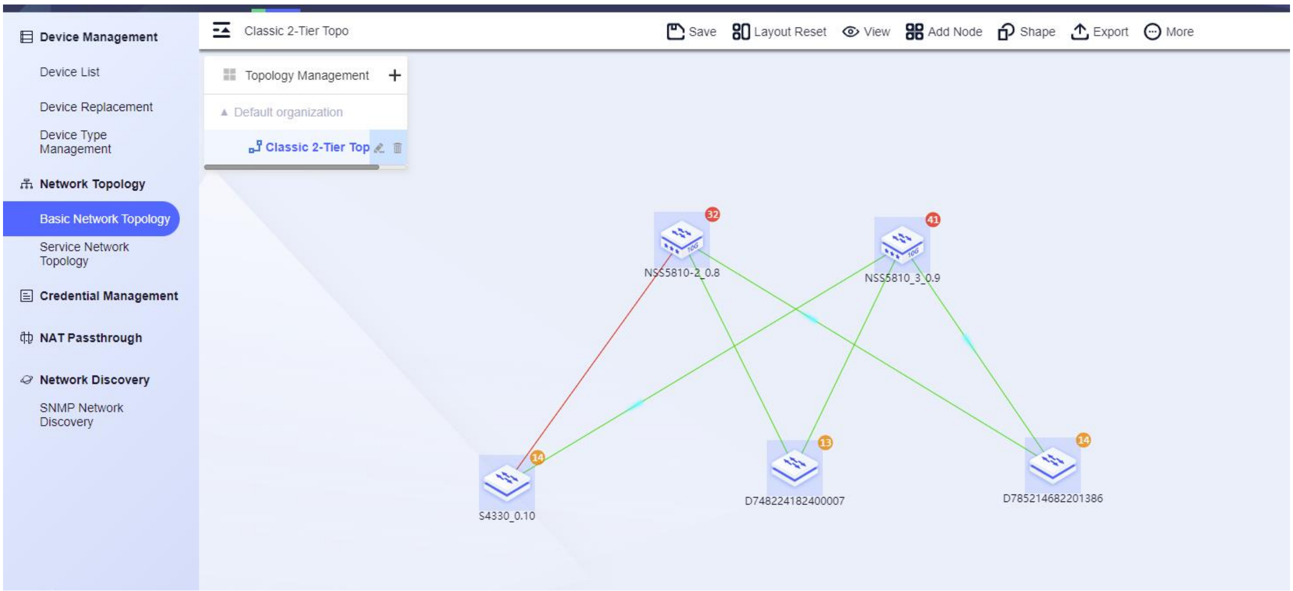
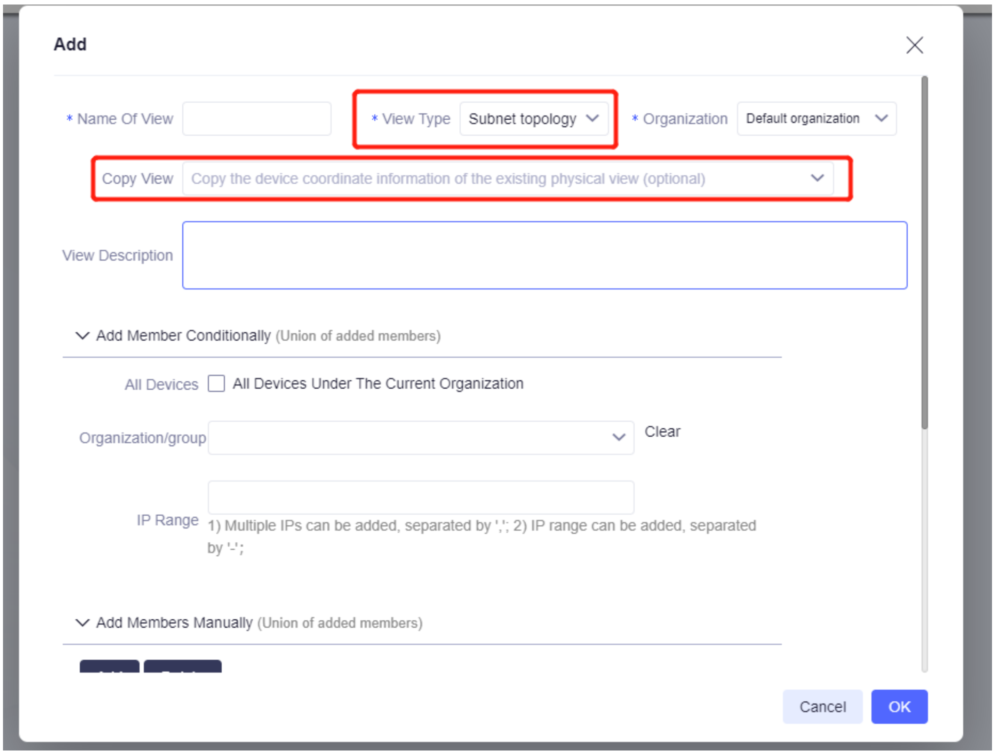


Figure 4.58 Generated physical topology view

Add Sub Topology

Click "Basic Network" in the top menu bar, select "Network Topology" submenu, open the topology management page, click the icon ☰ and the icon + in the upper left corner, select "Subnet topology" on the pop-up "Add" page. You can select “Copy View” to use the configuration of the existing physical view or select "None" without copying to generate a new subnet view. After entering the other items, click "OK" to generate the subnet topology view, as shown in the following figure.


Add

* Name Of View

* View Type: Subnet topology

* Organization: Default organization

Copy View: Copy the device coordinate information of the existing physical view (optional)

View Description

Add Member Conditionally (Union of added members)

All Devices ☐ All Devices Under The Current Organization

Organization/group

IP Range: 1) Multiple IPs can be added, separated by ','; 2) IP range can be added, separated by '-';

Add Members Manually (Union of added members)

Figure 4.59 Add subnet topology view

After adding a subnet topology, you need to list the subnets to be displayed in the subnet filter. There are no subnets by default.

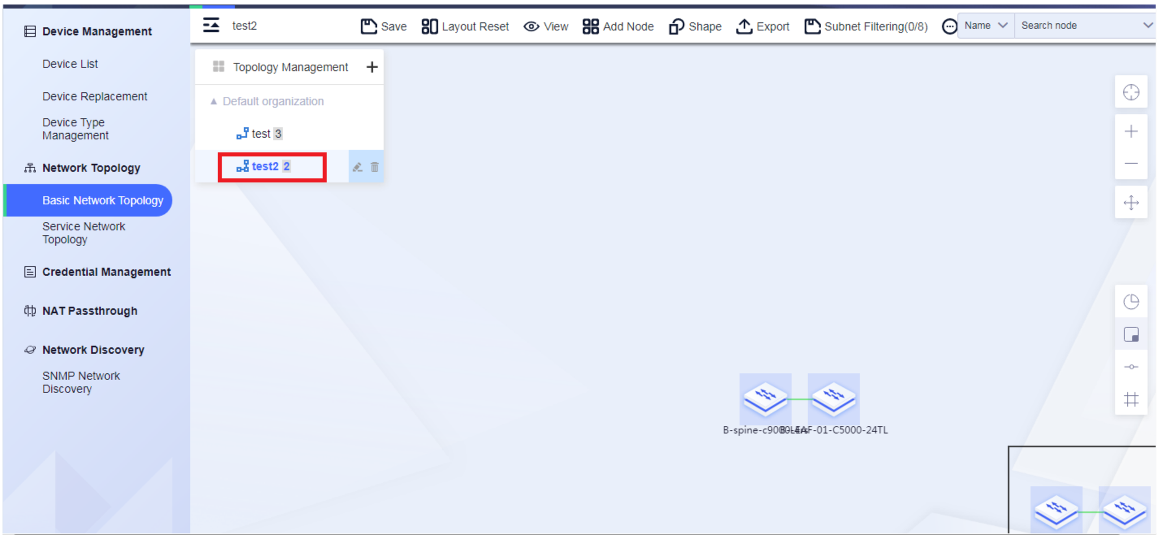
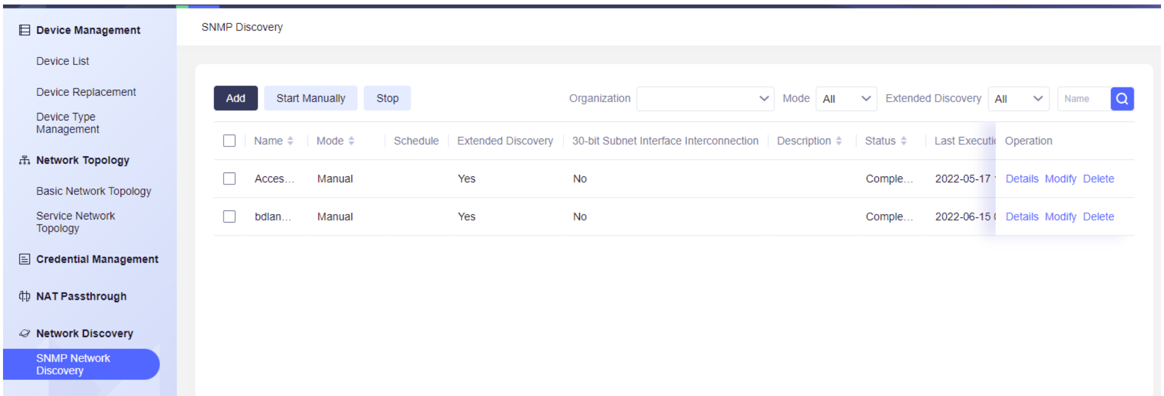


Figure 4.60 Generated topology subnet view

Synchronously Generate Physical Topology During Network Discovery

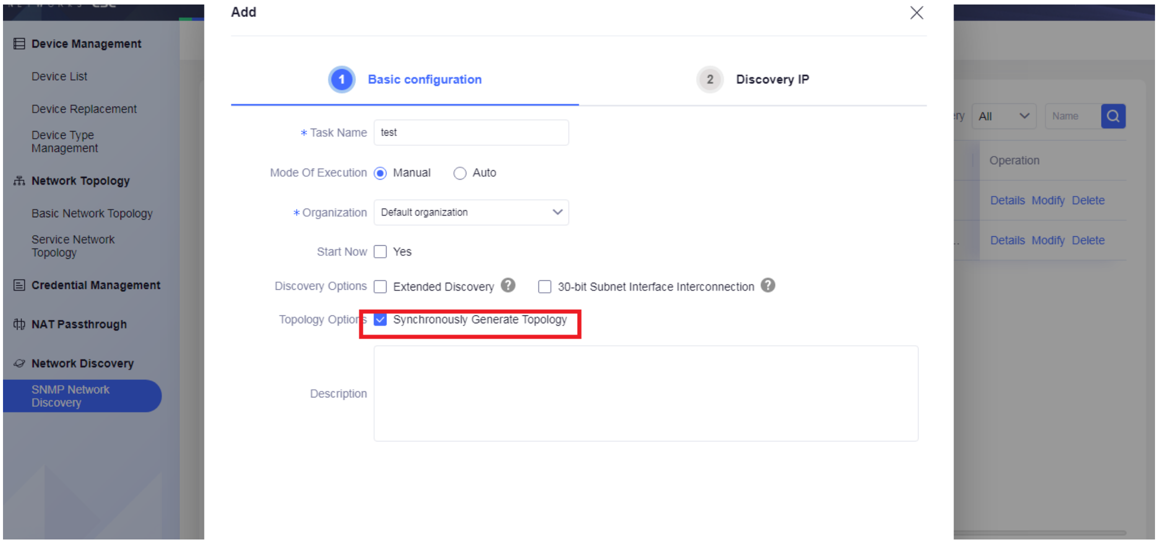
Click "Basic Network" in the top menu bar and select the "SNMP Discovery" menu on the left to open the SNMP discovery page;



☐	Name	Mode	Schedule	Extended Discovery	30-bit Subnet Interface Interconnection	Description	Status	Last Executi	Operation
☐	Acces...	Manual		Yes	No		Comple...	2022-05-17	Details Modify Delete
☐	bdlan...	Manual		Yes	No		Comple...	2022-06-15	Details Modify Delete

Figure 4.61SNMP discovery task configuration interface

On the SNMP discovery page, click the "Add" button, and check the "Synchronously Generate Topology" option in the pop-up page. When the task is executed, the corresponding physical topology view will be generated at the same time, as shown in the following figure.



∗Task Name test

Mode Of Execution ● Manual ○ Auto

∗Organization Default organization

Start Now ☐ Yes

Discovery Options ☐ Extended Discovery ☐ 30-bit Subnet Interface Interconnection

Topology Options ☑ Synchronously Generate Topology

Description

Figure 4.62 Synchronously generate topology during SNMP discovery

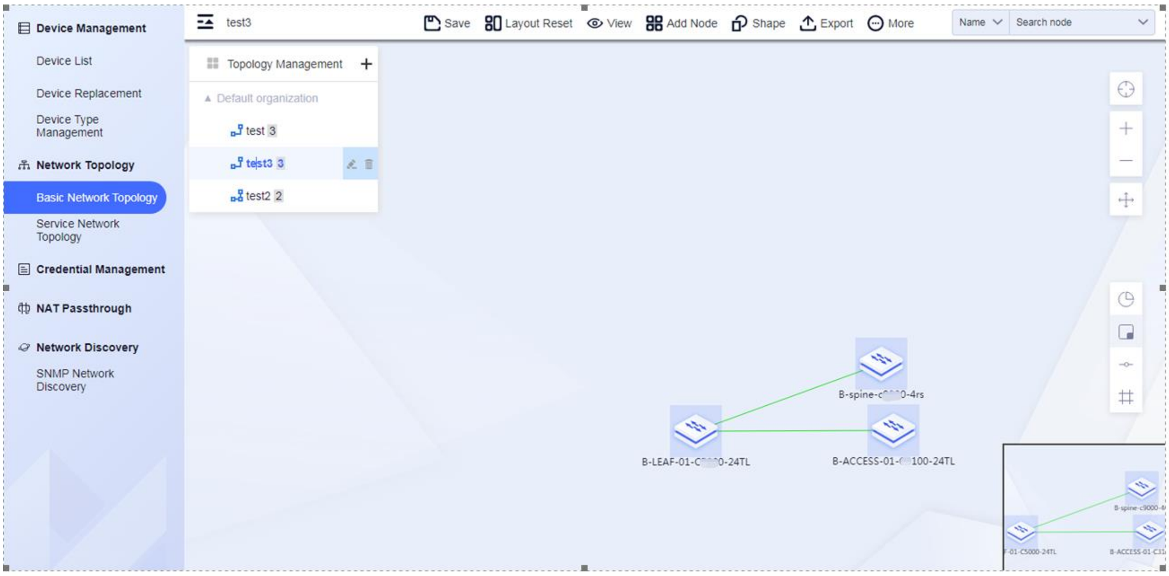
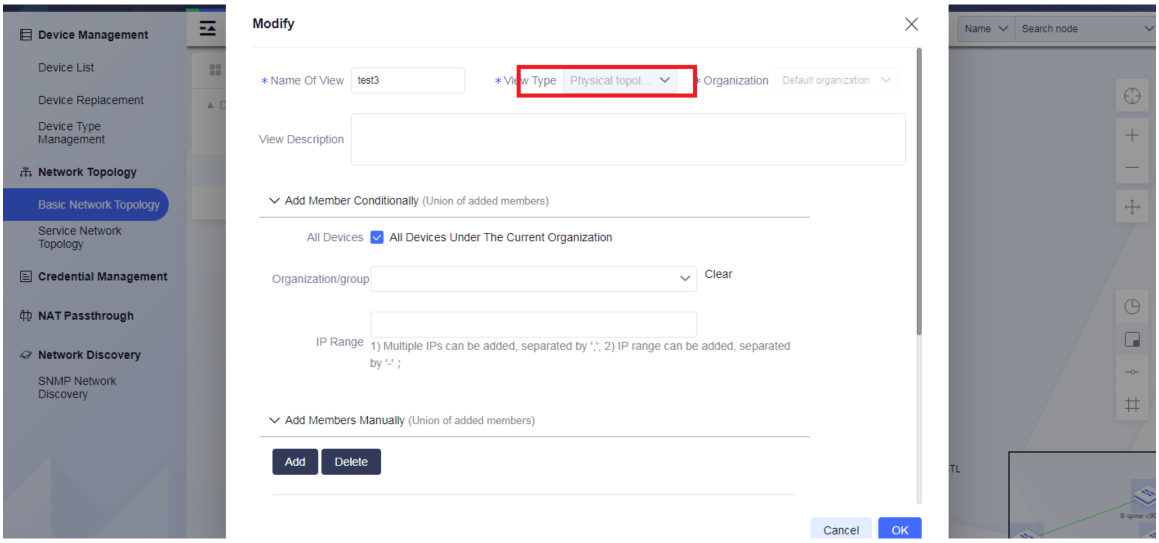


Figure 4.63 Synchronously generated physical topology view

Modify/Delete Topology

Click "Basic Network" in the top menu bar, select "Network Topology" submenu, open the topology management page, click the icon ☰ in the upper left corner, find the topology to be edited in the left tree, click the icon ✎, complete the editing of basic topology information and members in the pop-up "Modify" page, and click "OK" to complete the topology modification, as shown in the following figure.



Modify

* Name Of View: test3
* View Type: Physical topol...
* Organization: Default organization
View Description

Add Member Conditionally (Union of added members)

All Devices ☑ All Devices Under The Current Organization

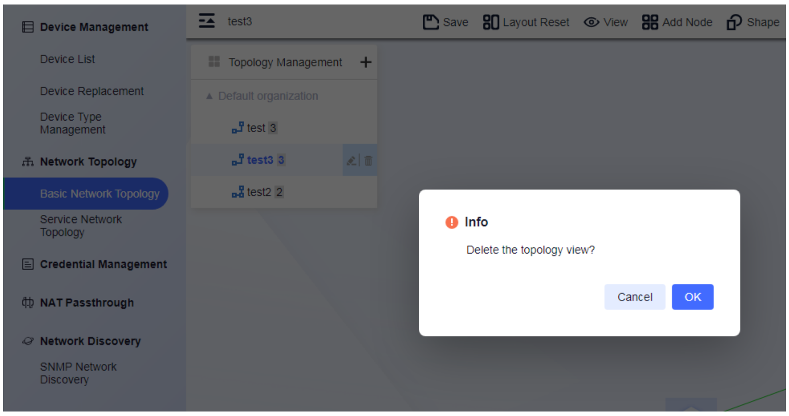
Organization/group — Clear

IP Range — 1) Multiple IPs can be added, separated by ','; 2) IP range can be added, separated by '-';

Add Members Manually (Union of added members)

Figure 4.64 Modify the topology

Click "Basic Network" in the top menu bar, select "Network Topology" submenu, open the topology management page, click the icon ☰ in the upper left corner, find the topology to be deleted in the left tree, and click the icon 🗑 to delete the topology.



Info

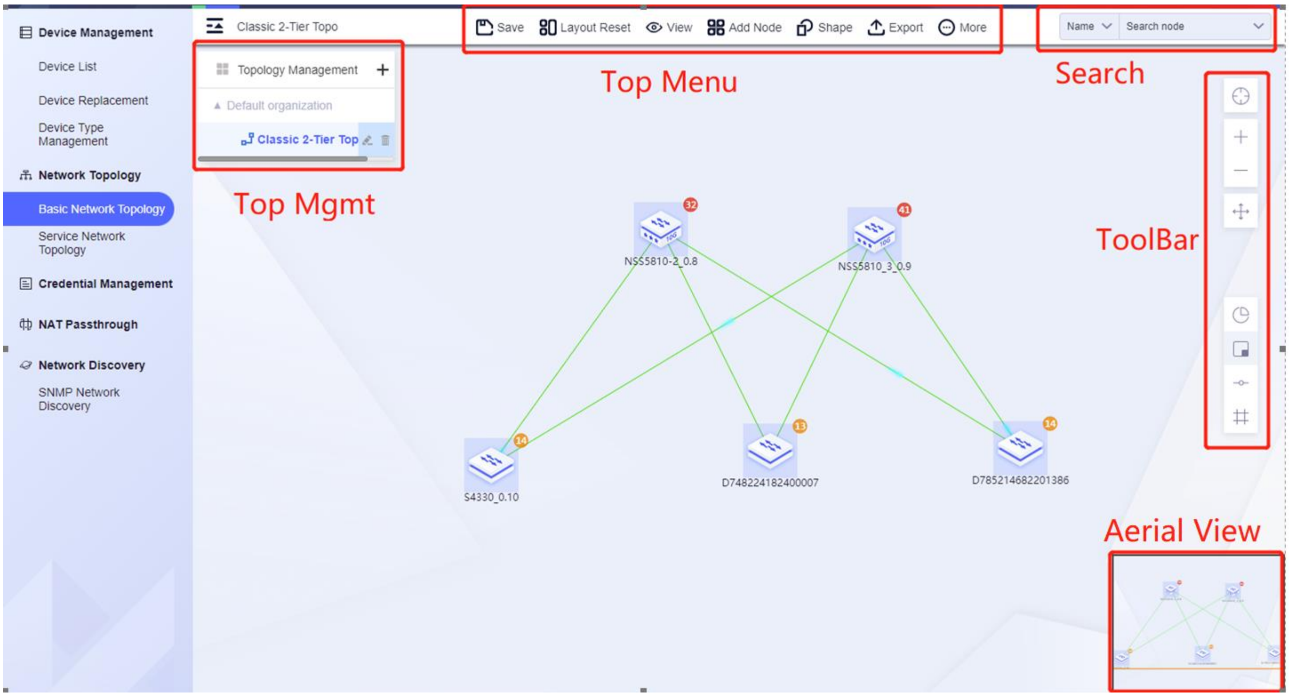
Delete the topology view?

Figure 4.65 Delete topology

Topology View

The topology view page displays the topology of a specific topology view and provides editing and viewing of the topology.

You can enter this page by clicking "Topology" in the top menu bar and selecting "Topology Management" submenu. Click the menu mode, and the system will load the topology recently accessed by the login user; The effect is shown in the figure below.



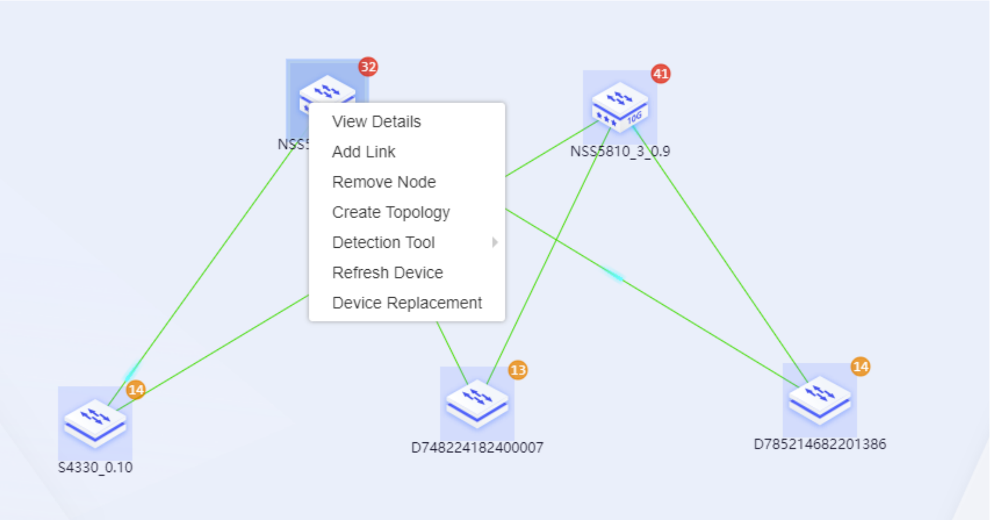


Figure 4.66 Topology view

For large networks, there are many devices in the topology and the relationship between devices is complex. In order to facilitate the monitoring and management of large-scale networks, the controller 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, etc.

When performing network discovery on the controller, some factors (such as device downtime, failure to enable the network management protocol) may cause the controller to not discover a device or the connection relationship between two devices. The network administrator can perform network discovery again, or manually add or remove devices and edit links in this topology view. In addition, it also provides operations such as topology view background setting, font color setting, and creating sub views.

As shown in the figure above, several functional areas in the topology view are described as follows:

Function Button Area

Save : Save the layout, display information, editing results, etc. of the current topology.

Layout Reset : Choose a different way to rearrange the topology.

NE: Select different typesetting methods to rearrange the topology (grid, star, tree);

Link layout: Select different connection types to re-display the link connection (straight line, arc and broken line).

View : Select the device display information in the topology view (the number of links, alarms, device name, device IP, and device MAC)

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

Virtual Node : Press and drag to the topology view, and you can add virtual nodes in the drag and drop position, and set the name, model and IP information.

Device: Press and drag to the topology view, and select a desired device in the pop-up selection box to add the device to the current view. When multiple devices are selected, they are arranged in a circle centered on the dragged position.

Topology Link: Press and drag to the topology view, and select other topology views in the pop-up selection box, which can be presented in the form of topology links at the drag and drop position.

Telecom: Press and drag to the topology view to add the telecom operator icon in the drag and drop position.

Unicom: Press and drag to the topology view to add Unicom operator icon in the drag and drop position.

Mobile: Press and drag to the topology view to add the mobile operator icon in the drag and drop position.

Network Cloud: Press and drag to the topology view to add a network cloud at the drag and drop location, set the name of the network cloud, and drag the size.

Export: Export the topology in picture format.

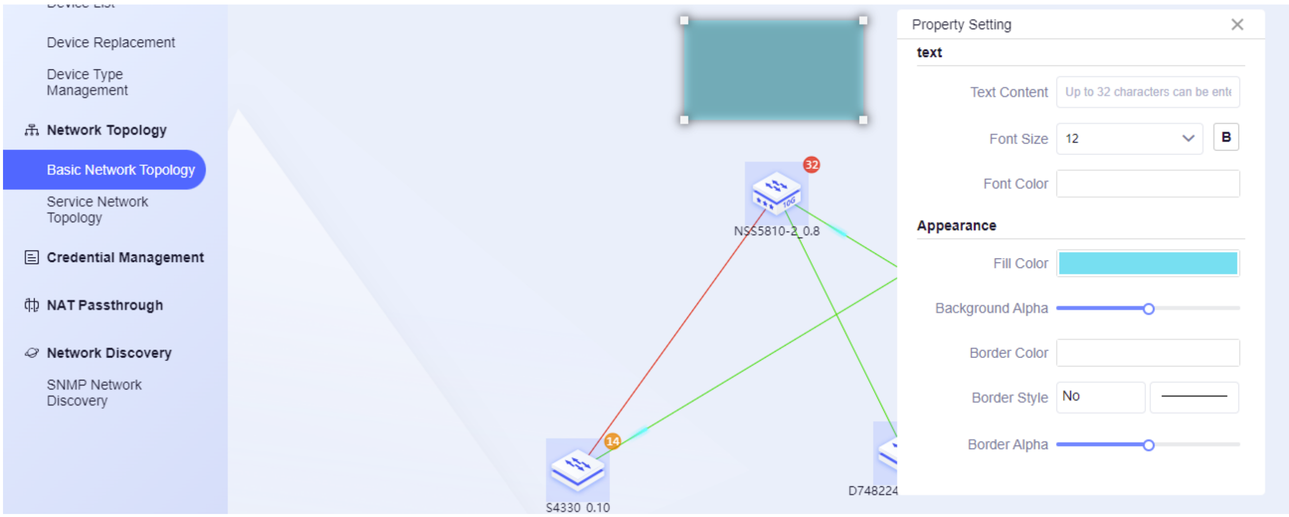
Shape: Add shapes to the topology view (basic shape, text editing, collection, support dragging size).

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

▭: Hold and drag to the topology view, and you can add a rectangular background to the drag and drop position.

▢: Hold and drag to the topology view, and you can add a rounded rectangular background to the drag and drop position.

⬭: Hold and drag to the topology view, and you can add an ellipse background to the drag and drop position.

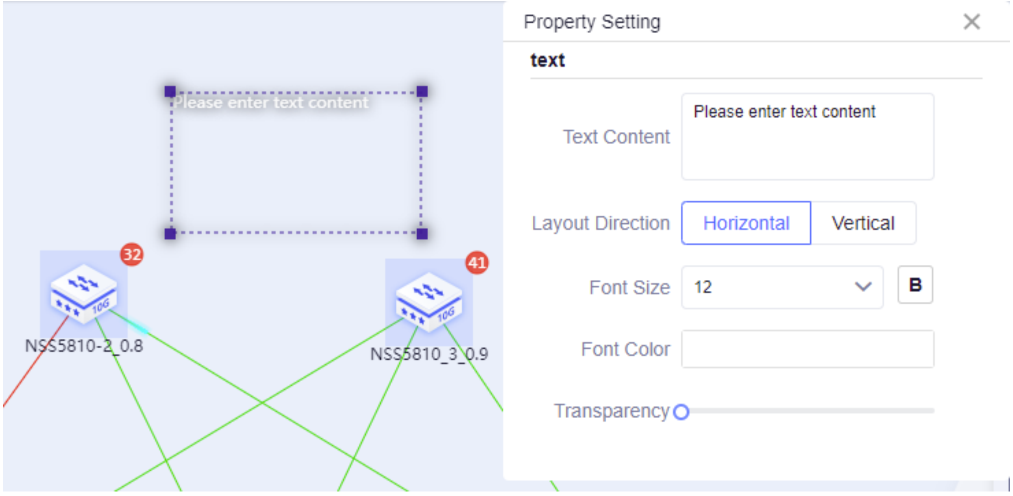


Text Content: Up to 32 characters can be ente
Font Size: 12
Font Color:
Fill Color:
Background Alpha:
Border Color:
Border Style: No
Border Alpha:

Figure 4.67 Basic shape attribute setting

- Text editing (horizontal or vertical text boxes, supporting text setting, see the figure below for details)

: Press and drag to the topology view, and you can add a text box in the drag and drop position.



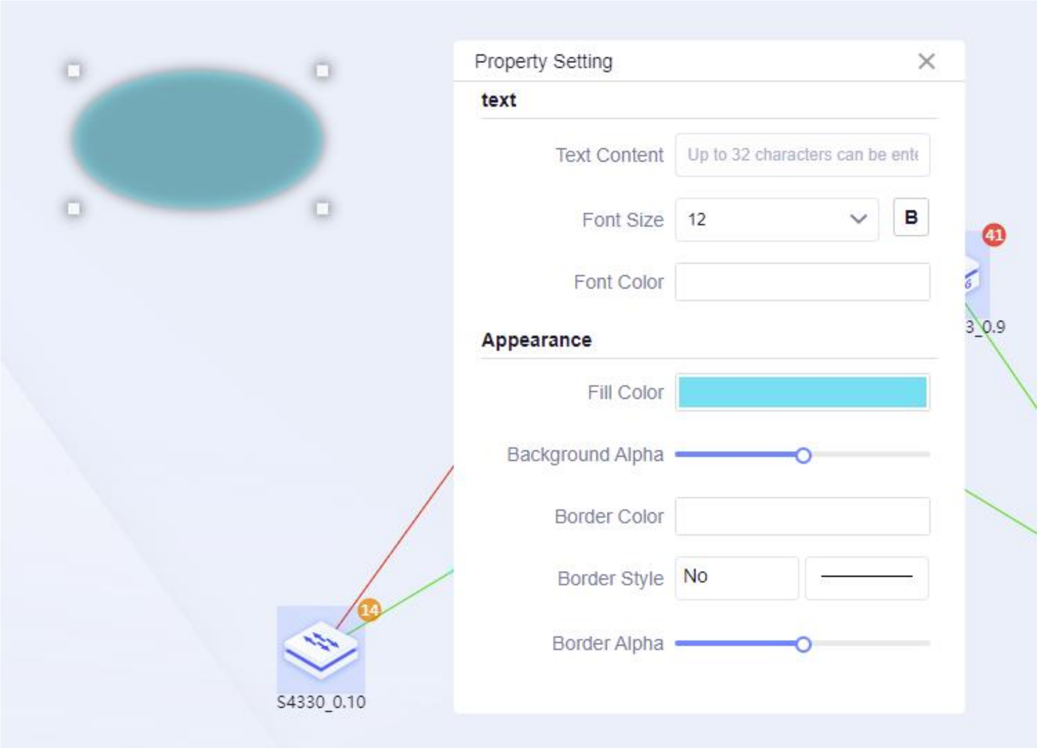
Text Content: Please enter text content
Layout Direction: Horizontal
Font Size: 12
Font Color:
Transparency

Figure 4.68 Text edit property setting

- Collection (collection container, you can add/remove device nodes from the collection by dragging and dropping, and support text setting, as shown in the figure below)

: Press and drag to the topology view, and you can add an ellipse collection at the drag and drop position.

: Press and drag to the topology view, ad you can add a rectangular collection at the drag and drop location.



Property Setting

text

Text Content: Up to 32 characters can be ente

Font Size: 12

Font Color:

Appearance

Fill Color:

Background Alpha

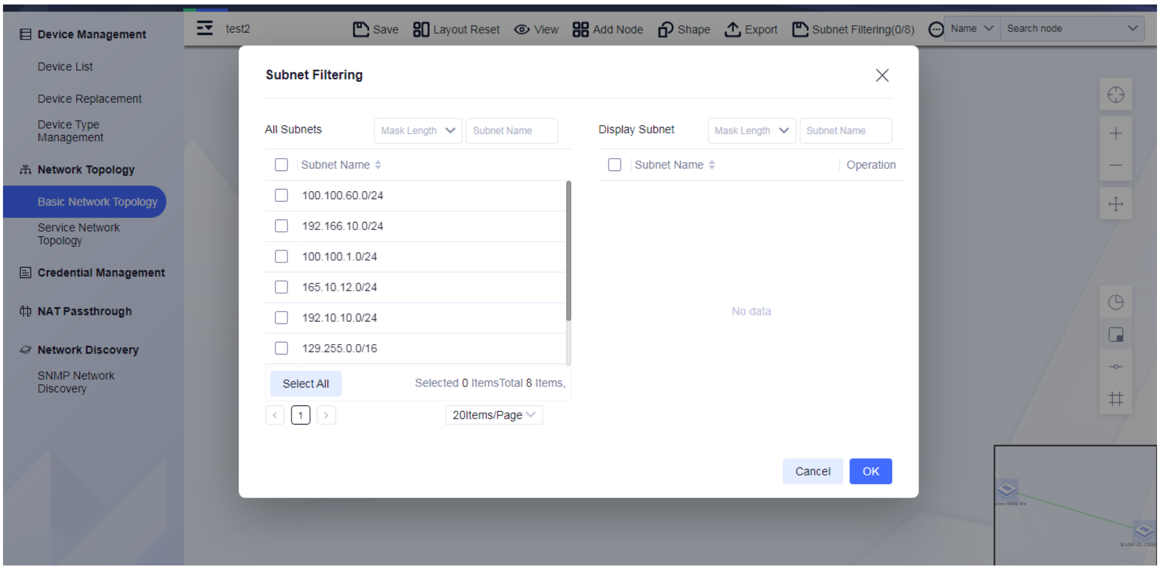
Border Color:

Border Style: No

Border Alpha

Figure 4.69 Collection property settings

Subnet Filtering(0/0) : Display/hide the subnet in the topology. This function is unique to the subnet view, as shown in the following figure.



Subnet Filtering

All Subnets — Mask Length — Subnet Name

☐	Subnet Name
☐	100.100.60.0/24
☐	192.166.10.0/24
☐	100.100.1.0/24
☐	165.10.12.0/24
☐	192.10.10.0/24
☐	129.255.0.0/16

Select All — Selected 0 ItemsTotal 8 Items,

1 — 20Items/Page

Display Subnet — Mask Length — Subnet Name

☐	Subnet Name	Operation

No data

Figure 4.70 Subnet filtering

More : Other function options (background setting, font color setting, streamer effect setting, accept rate setting, legend description).

- Background setting

The system has three built-in background styles, and supports uploading new background styles through "Upload Materials"; You can click the mouse to select the background style, preview the background style through the "Preview" button, and save the replacement of the background style through the "Use" button, as shown in the following figure.

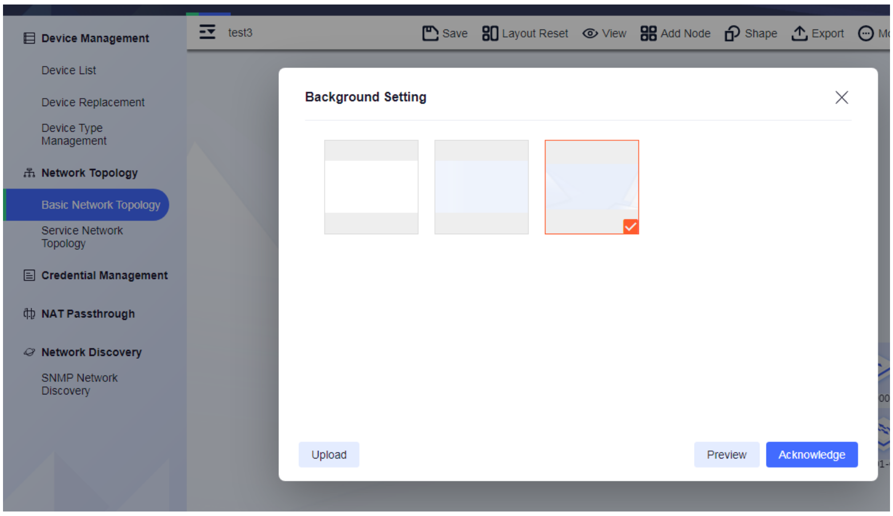


Figure 4.71 Topology view background setting

- Font color settings

Set the font color in the topology view, and 72 colors are available, as shown in the following figure.

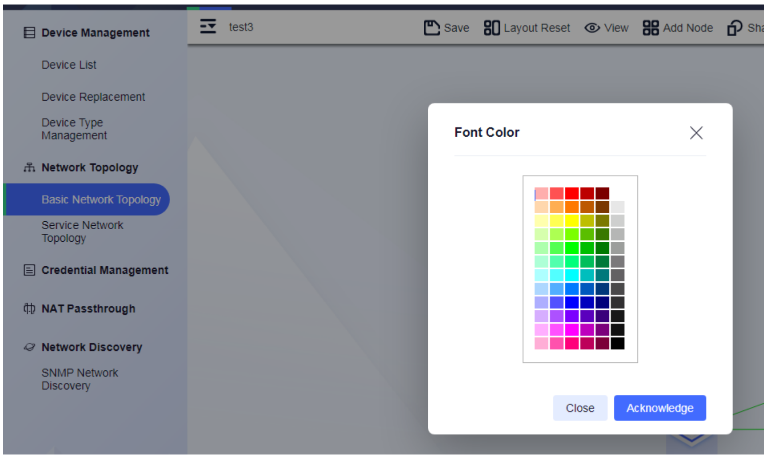


Figure 4.72 Front color setting of the topology view

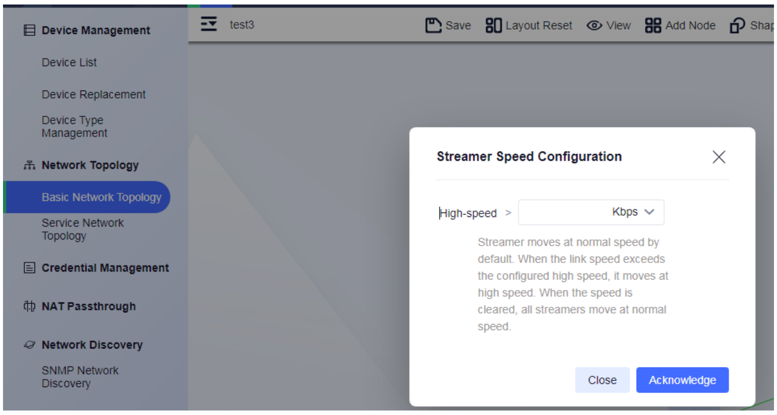
- Streamer effect

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

Open: Click to enable the streamer effect;

Close: Click to disable the streamer effect;

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



Streamer moves at normal speed by default. When the link speed exceeds the configured high speed, it moves at high speed. When the speed is cleared, all streamers move at normal speed.

Figure 4.73 Streamer speed setting

- Receive Rate

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

Enable: Click to display the receive rate;

Disable: Click to hide the receive rate.

- Legend illustration

Click "Legend Illustration" in the "More" icon to view the legend description of the topology view, as shown in the following figure.

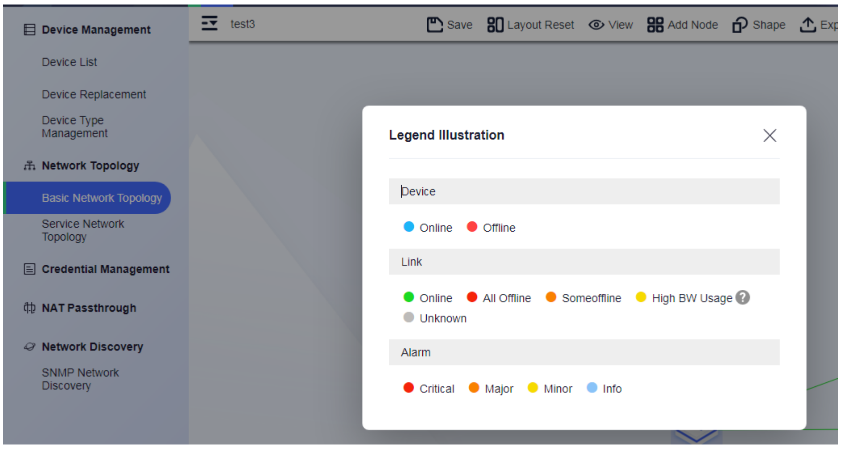


Figure 4.74 Legend description

Search Area

Within the scope of the current topology view, you can query the device according to the device name, alias, IP and MAC information.

Tools Bar

◷ : Display the topology statistics information, and click to pop up the statistics window, as shown in the figure

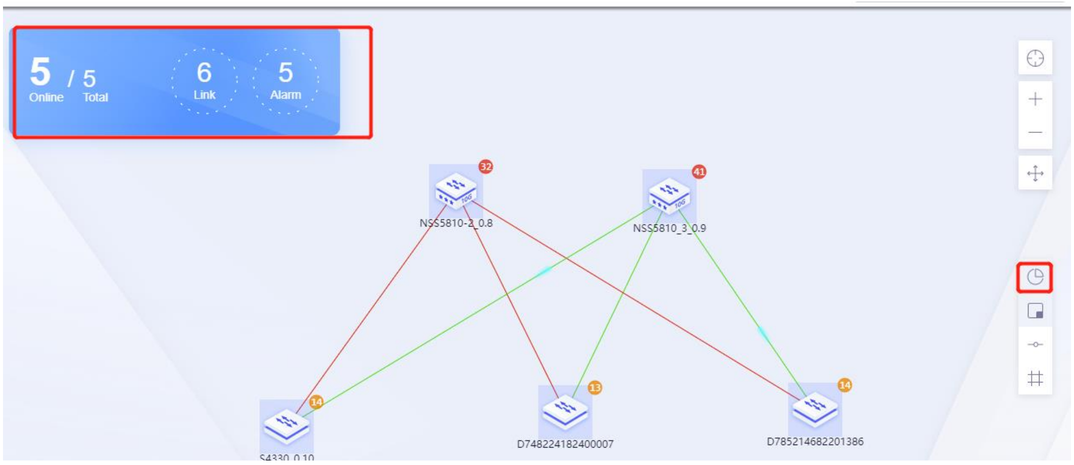


Figure 4.75 Topology statistics

+ : Zoom in the topology

— : Zoom out the topology

✥ : Topology anchor, mouse drag and drop topology switch

◪ : Turn on/off aerial view

Aerial View

1. By dragging the current screen display area in the aerial view, you can view the part of the topology map that cannot be displayed on the screen.
2. By double-clicking the current screen display area in the aerial view, you can locate the double-click position to the middle of the screen.

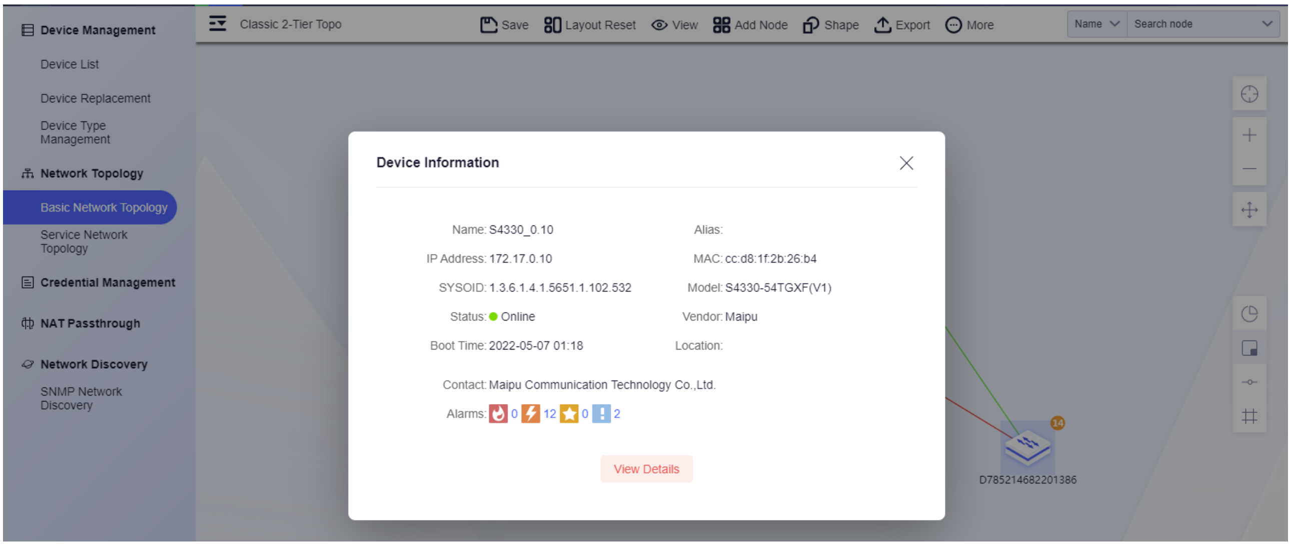
Right-click Menus

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

Right-click Menus of NE

- View details:

To view the details of the device information, you can also double-click a device in the topology view to achieve the same purpose, 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.



Device Information

Name: S4330_0.10
Alias:
IP Address: 172.17.0.10
MAC: cc:d8:1f:2b:26:b4
SYSOID: 1.3.6.1.4.1.5651.1.102.532
Model: S4330-54TGXF(V1)
Status: ● Online
Vendor: Maipu
Boot Time: 2022-05-07 01:18
Location:
Contact: Maipu Communication Technology Co.,Ltd.
Alarms: 0 12 0 2

Figure 4.76 Device information box

- Add link:

Add the links between network elements in the topology view. This menu is only supported in the topology physical view. This function is available when selecting a single network element and double network elements. After selecting the information at both ends of the link, click the "Add" button to pre-add a link. The pre added links can be deleted through the "Batch Delete" or the icon ✕, click the "OK" button to confirm the addition, or click the "Cancel" button to abandon the addition, as shown in the following figure.

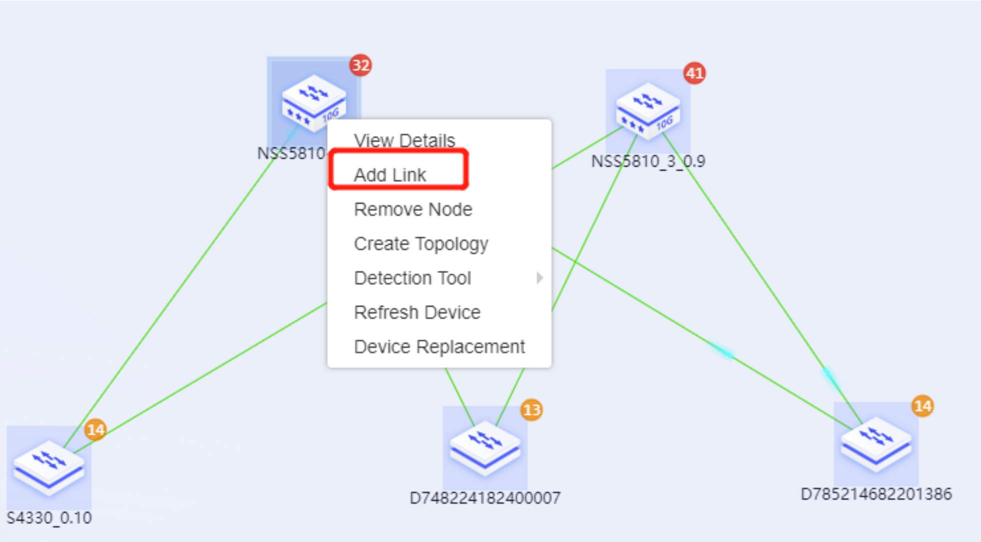


Figure 4.77 Add a link

Note

- The links added in the topology view are only displayed in the current topology view and will not disappear with network rediscovery

- Display stacking:

This menu can only be seen by right-clicking the stacking device. After clicking, the details in the stack can be displayed, and you can 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 appear again with network discovery.

- Create topology:

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

- Detection tools:

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

- Refresh devices:

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

- Enter the view:

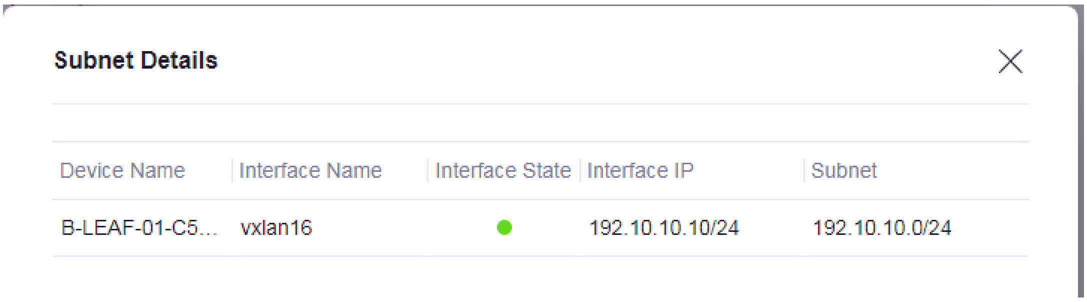
This menu can only be seen by right-clicking the topology link. You can jump to the linked topology view page and return to the current topology through the "Back" button.

- Enter the subnet:

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

- Subnet details:

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



Subnet Details

Device Name	Interface Name	Interface State	Interface IP	Subnet
B-LEAF-01-C5...	vxlan16	●	192.10.10.10/24	192.10.10.0/24

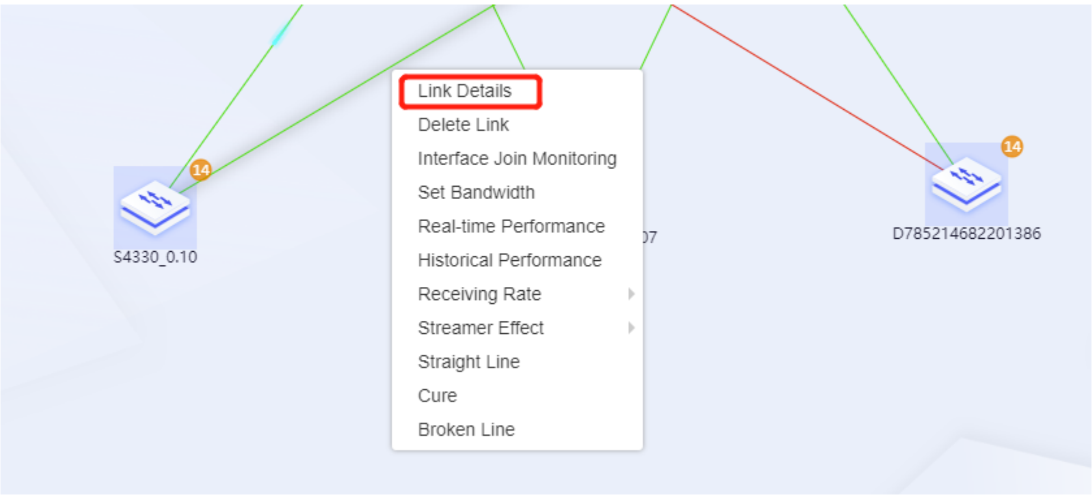
Figure 4.2.1.1 Subnet details box

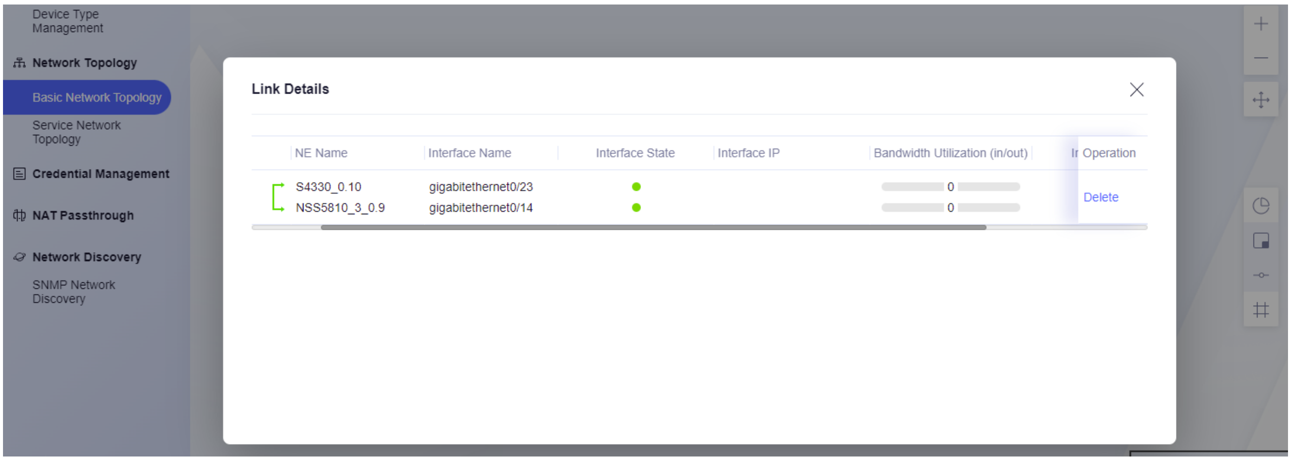
- Put on top layer: This menu can be seen only by right-clicking on the shape. Click to place the corresponding shape on the top layer of all shapes.
- Move up one layer: This menu can be seen only by right-clicking on the shape. Click to move the corresponding shape up one layer among all shapes.
- Move down one layer: This menu can be seen only by right-clicking on the shape. Click to move the corresponding shape down one layer among all shapes.
- Place at the bottom layer: This menu can be seen only by right-clicking on the shape. Click to place the corresponding shape at the bottom layer of all shapes.

Right-click menus of the link

- Link details:

This menu can only be seen when you right-click a link in the topology physical view, as shown in the figure below. The details of both ends of the link are displayed in the link details box. Click 🗑, and you can delete the link, click "OK" to confirm the deletion, or click "Cancel" to abort the deletion.



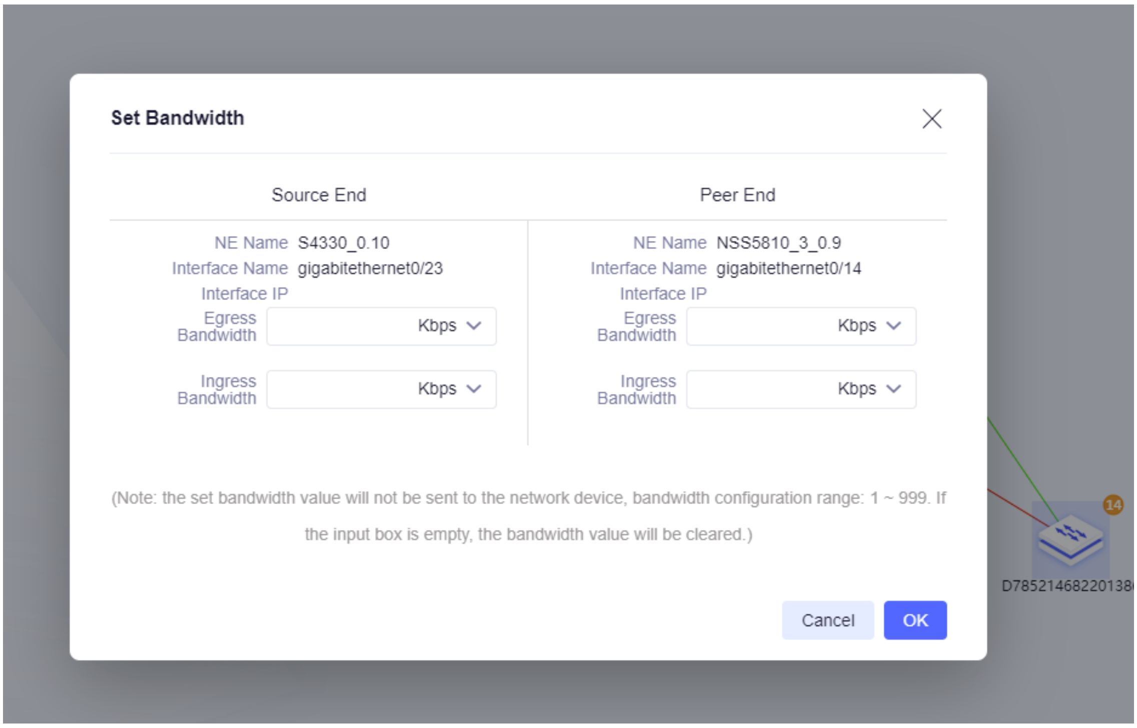


Link Details

NE Name	Interface Name	Interface State	Interface IP	Bandwidth Utilization (in/out)	Operation
S4330_0.10	gigabitethernet0/23	●		0	Delete
NSS5810_3_0.9	gigabitethernet0/14	●		0	

Figure 4.78 Link details box

- Delete link: this menu is available only when you right-click a link in the topology physical view. Click it to delete the selected link.
- Add interface to monitoring: Click to add the selected interfaces at both ends of the link to monitoring.
- Set bandwidth: Click to set the bandwidths of the interfaces at both ends of the link, as shown in the figure below.



Set Bandwidth

Source End

NE Name S4330_0.10
Interface Name gigabitethernet0/23
Interface IP
Egress Bandwidth Kbps
Ingress Bandwidth Kbps

Peer End

NE Name NSS5810_3_0.9
Interface Name gigabitethernet0/14
Interface IP
Egress Bandwidth Kbps
Ingress Bandwidth Kbps

(Note: the set bandwidth value will not be sent to the network device, bandwidth configuration range: 1 ~ 999. If the input box is empty, the bandwidth value will be cleared.)

Figure 4.79 Bandwidth setting box

- Real-time performance: Click to open the performance monitoring page and display the real-time monitoring data of the interfaces at both ends of the link.
- Historical performance: Click to open the performance monitoring page and display the historical monitoring data of the interfaces at both ends of the link.
- Receive rate: click on/off to display/hide the receive rate of the selected link.
- Streamer effect: click on/off 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.

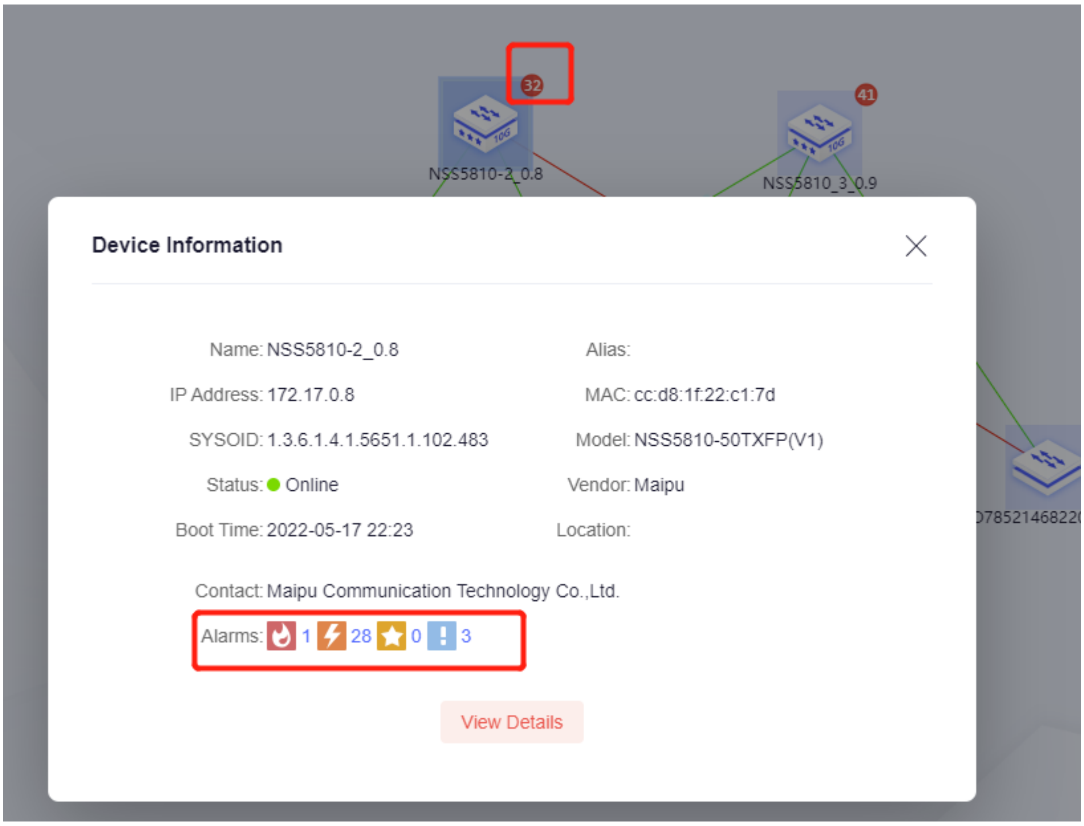
- Broken line: Click to set the connection type of the selected link as broken line.

Note

- Confirm the deleted link in the link details box. It will only be deleted in the current topology view and will not be presented with network rediscovery.

Alarm Statistics:

The topology view provides the statistics of the alarm information of network devices (the small circle next to the network device shows the total number of unprocessed alarm information of the device. If the number of alarms exceeds 99, the page displays "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 device details, as shown in the following figure).

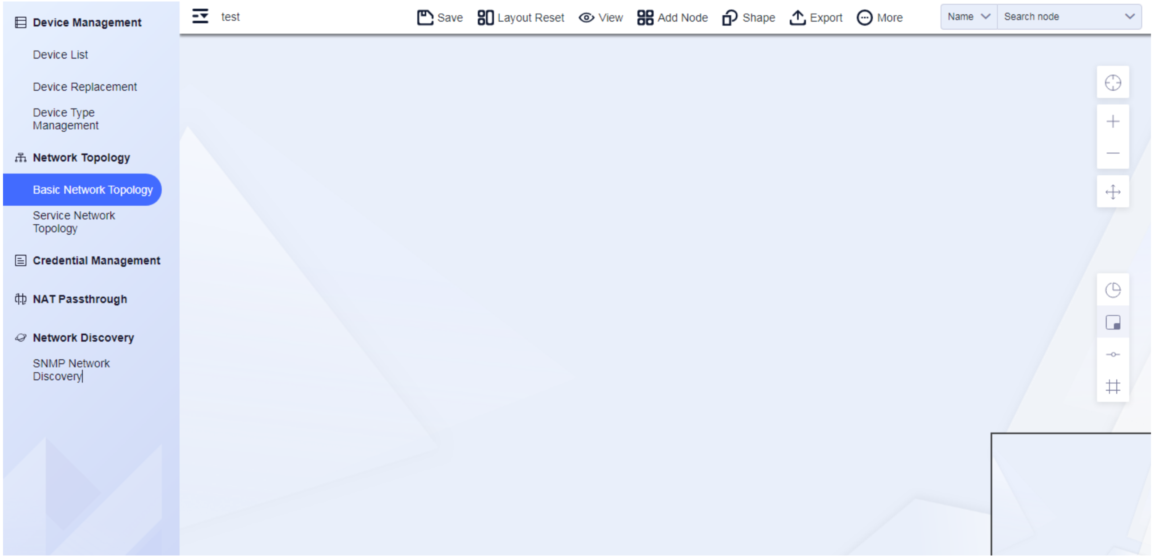


Name: NSS5810-2_0.8
Alias:
IP Address: 172.17.0.8
MAC: cc:d8:1f:22:c1:7d
SYSOID: 1.3.6.1.4.1.5651.1.102.483
Model: NSS5810-50TXFP(V1)
Status: ● Online
Vendor: Maipu
Boot Time: 2022-05-17 22:23
Location:
Contact: Maipu Communication Technology Co.,Ltd.
Alarms: 🔥 1 ⚡ 28 ★ 0 ! 3

Figure 4.80 Alarm statistics

Topology Construction

First, build the physical topology of each organization, as shown in the figure below:



Add Network Cloud

Enter the default organization topology view, click Add Node > Network Cloud, as shown in the following figure:

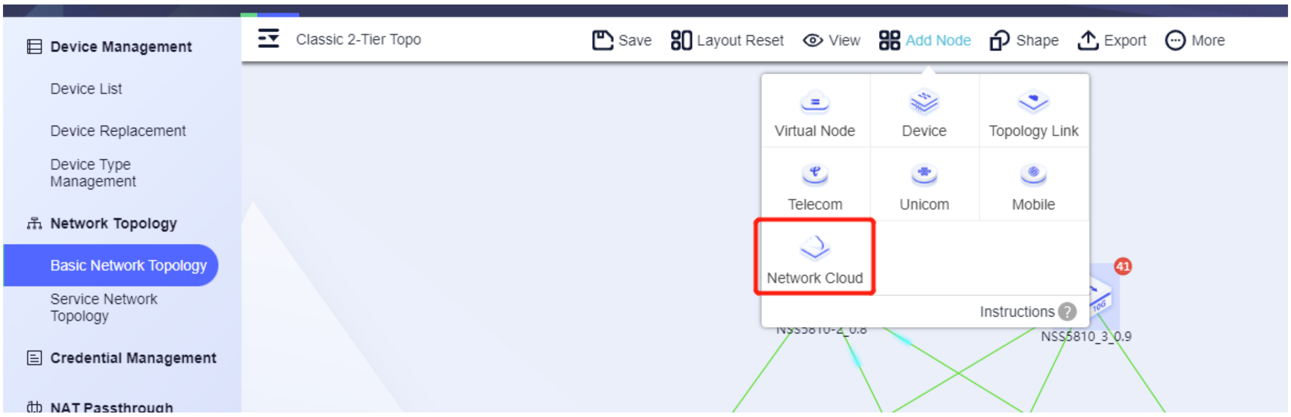


Figure 4.81 Add network cloud

Input the topology cloud name:

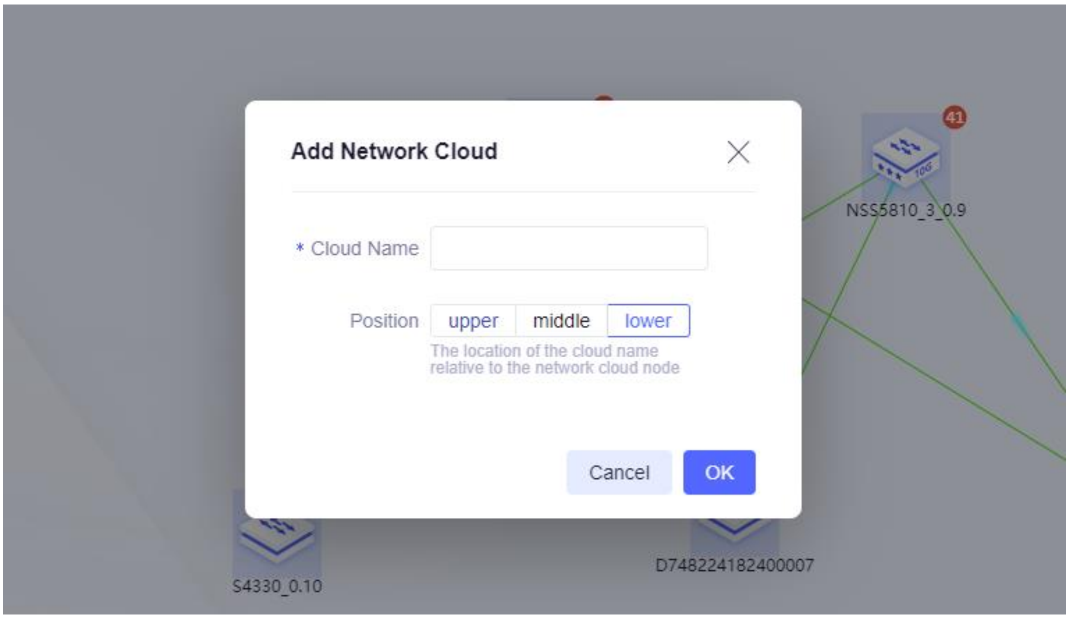
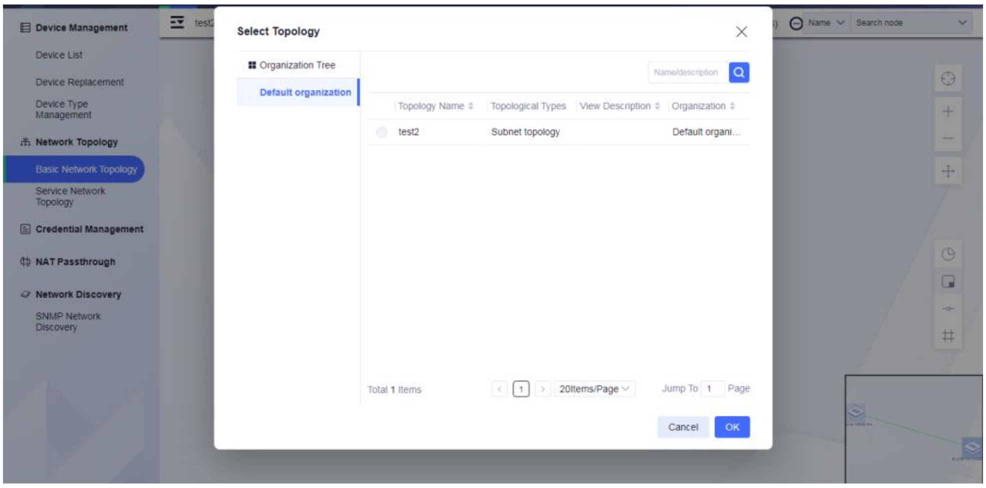


Figure 4.82 Add network cloud

Add Topology Connection

Click **Add Node** > **Topology Link**, select a specific topology connection, and click **OK**.



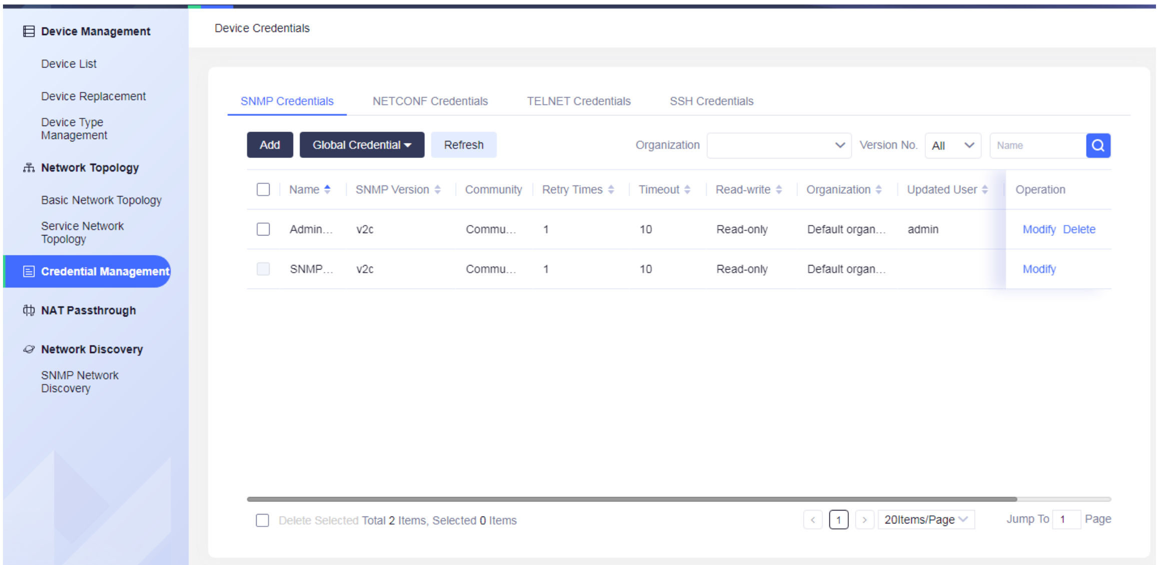
	Topology Name	Topological Types	View Description	Organization
○	test2	Subnet topology		Default organi...

Figure 4.83 Add topology link

4.3 Credential Management

4.3.1 SNMP Credential

SNMP credential management is used to manage common SNMP configurations. You can add/delete/modify/query SNMP credentials. Click "Discovery" - > "Credential Management" - > "SNMP Credentials" in the menu bar to open the "SNMP Credential Management" page, as shown below.

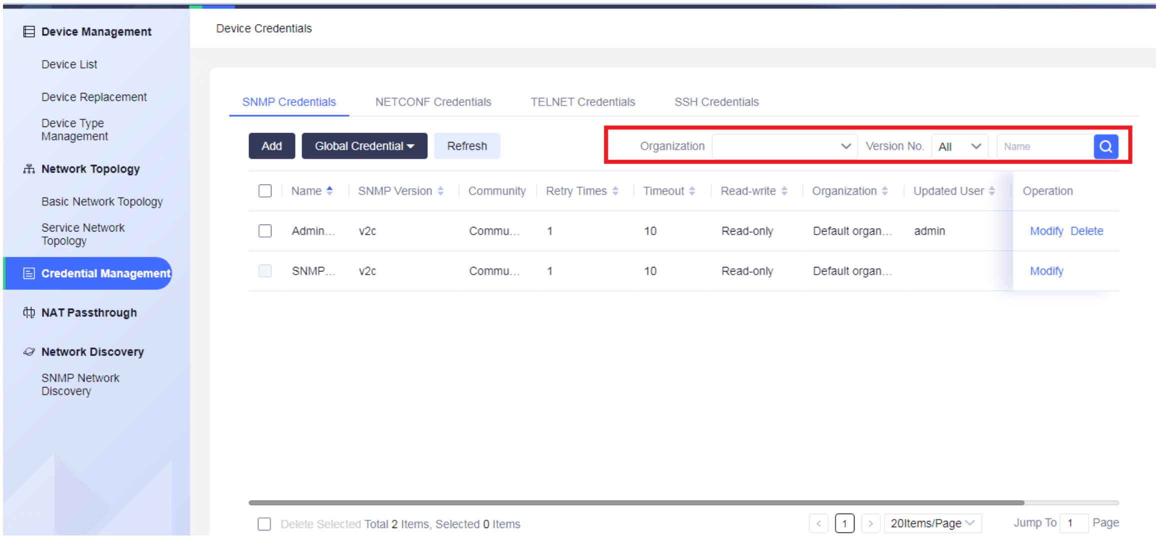


☐	Name	SNMP Version	Community	Retry Times	Timeout	Read-write	Organization	Updated User	Operation
☐	Admin...	v2c	Commu...	1	10	Read-only	Default organ...	admin	Modify Delete
☐	SNMP...	v2c	Commu...	1	10	Read-only	Default organ...		Modify

Figure 4.84 SNMP credential list

Query SNMP credentials:

The SNMP credential list supports paging display, and each SNMP credential 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 credentials support fuzzy query and filtering by name, organization and version number, as shown in the following figure:



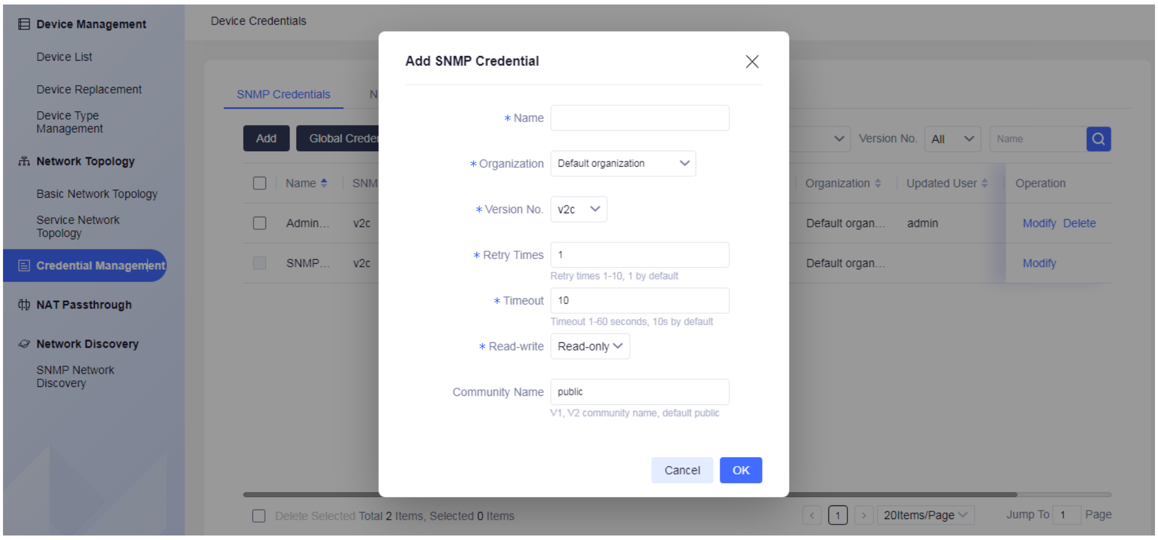
☐	Name	SNMP Version	Community	Retry Times	Timeout	Read-write	Organization	Updated User	Operation
☐	Admin...	v2c	Commu...	1	10	Read-only	Default organ...	admin	Modify Delete
☐	SNMP...	v2c	Commu...	1	10	Read-only	Default organ...		Modify

☐ Delete Selected Total 2 Items, Selected 0 Items

Figure 4.85 SNMP credential query and hierarchical and decentralized display

Add SNMP Credential:

Click **Add** to open the "Add SNMP Credential" dialog box, fill in SNMP related parameters, and click **OK** to save the new SNMP credential.



Add SNMP Credential

* Name
* Organization: Default organization
* Version No.: v2c
* Retry Times: 1
Retry times 1-10, 1 by default
* Timeout: 10
Timeout 1-60 seconds, 10s by default
* Read-write: Read-only
Community Name: public
V1, V2 community name, default public

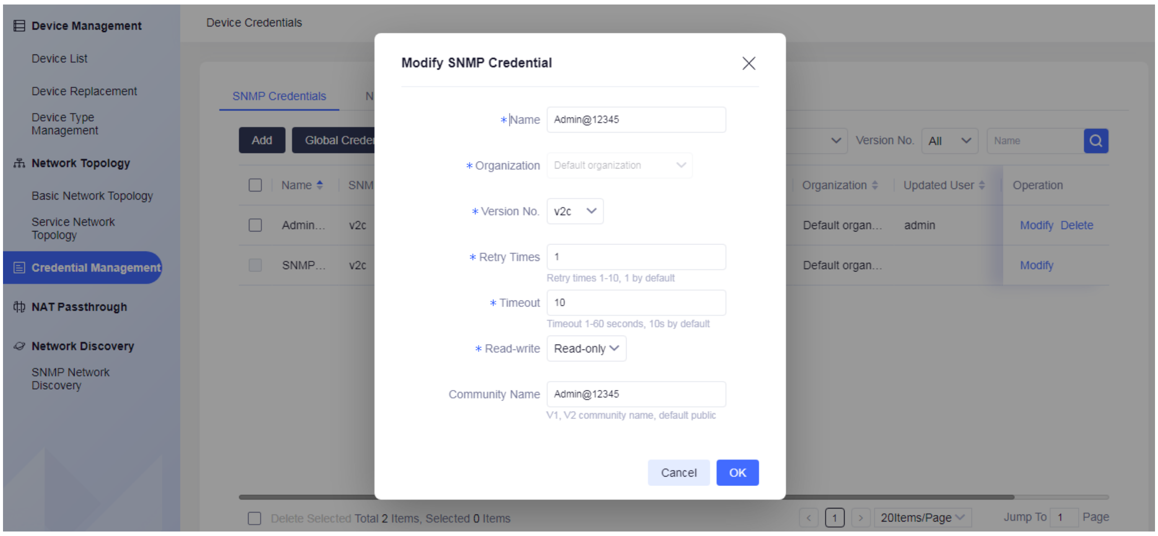
Figure 4.86 Add SNMP credential

Note

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

Modify SNMP Credential:

Select a desired SNMP credential in the list (only one credential can be modified at the same time), click the **Modify** button to open the "Modify SNMP Credential " dialog box (as shown in the figure below), you can modify the parameters of the SNMP credential, and the "Organization" field does not support modification. After modification, click **OK** to save the modified settings.



Modify SNMP Credential

*Name Admin@12345

*Organization Default organization

*Version No. v2c

*Retry Times 1

Retry times 1-10, 1 by default

*Timeout 10

Timeout 1-60 seconds, 10s by default

*Read-write Read-only

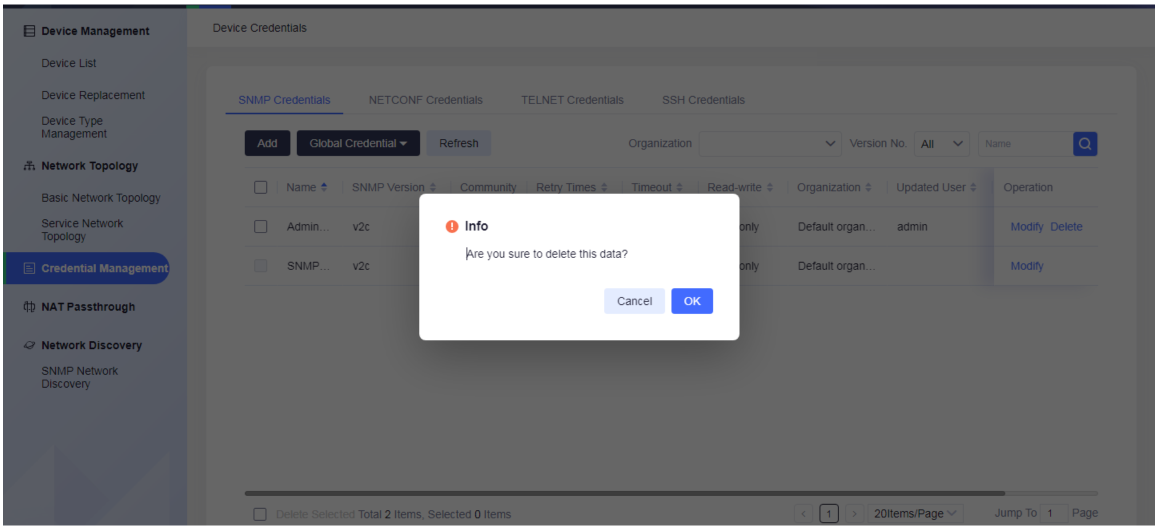
Community Name Admin@12345

V1, V2 community name, default public

Figure 4.87 Modify SNMP credential

Delete SNMP Credential:

Select a desired SNMP credential in the list (multiple selections are supported), click **Delete**, and click **OK** in the pop-up deletion confirmation dialog box (as shown below) to delete the selected SNMP credential. Click **Cancel** to abort the deletion.



Info

Are you sure to delete this data?

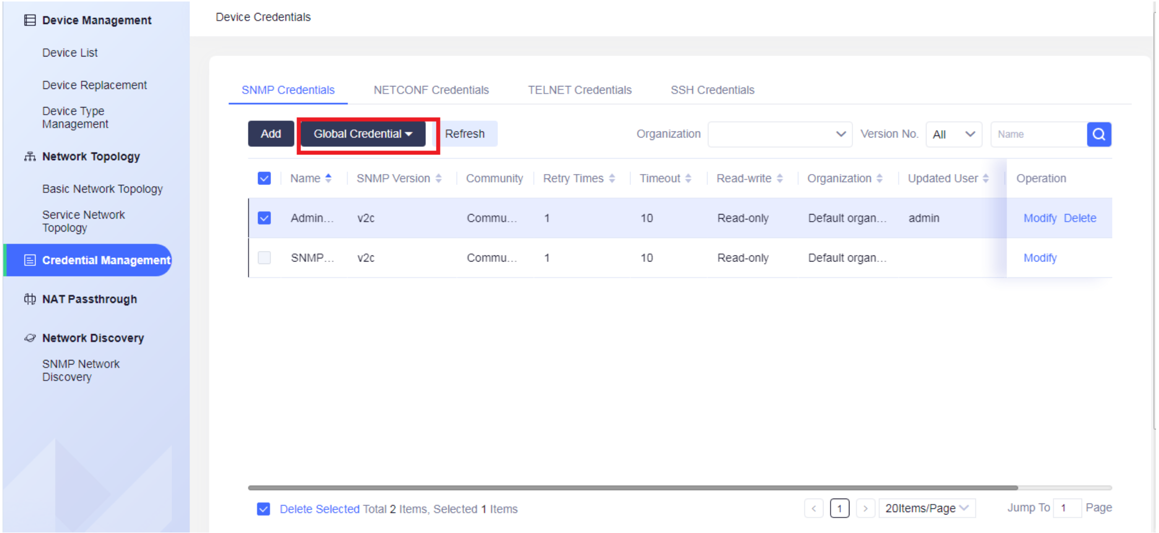
Figure 4.88 Delete SNMP credential

Caution

- "SNMP inbuilt template" is a system inbuilt template and cannot be deleted
- If the template referenced by the task is deleted, the result of executing the network discovery task that references the template will be affected

Global Credential:

The global credential function can set and cancel global credentials. When the device selects the credential, it is not limited by the organization.



☑	Name	SNMP Version	Community	Retry Times	Timeout	Read-write	Organization	Updated User	Operation
☑	Admin...	v2c	Commu...	1	10	Read-only	Default organ...	admin	Modify Delete
☐	SNMP...	v2c	Commu...	1	10	Read-only	Default organ...		Modify

Total 2 Items, Selected 1 Items

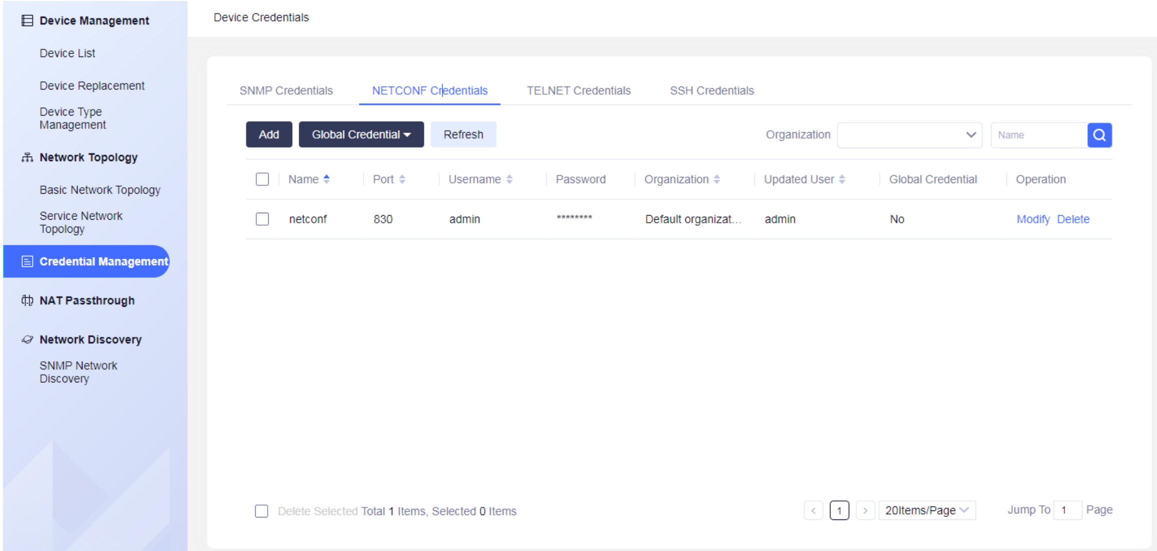
Figure 4.89 SNMP global credential

Refresh SNMP Credentials:

Click **Refresh** at the top of the list to refresh the credential list data.

4.3.2 NETCONF Credential

NETCONF credential management is used to manage common NETCONF configurations. You can add/delete/modify NETCONF credentials. Click "Discovery" - > "Credential Management" - > "NETCONF Credentials" in the menu bar to open the "NETCONF Credential Management" page, as shown below.



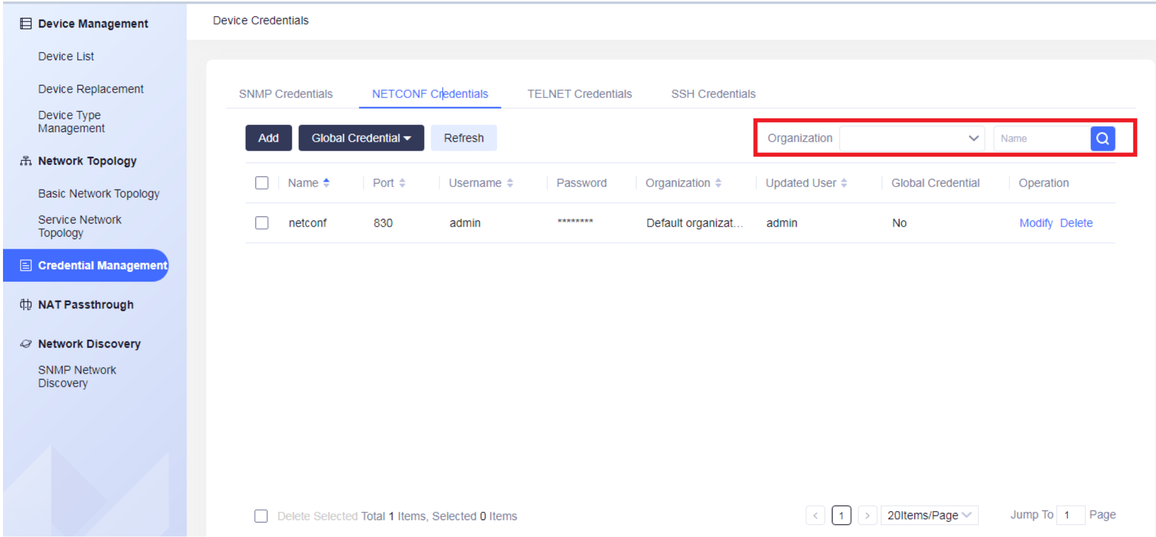
☐	Name	Port	Username	Password	Organization	Updated User	Global Credential	Operation
☐	netconf	830	admin	********	Default organizat...	admin	No	Modify Delete

Total 1 Items, Selected 0 Items

Figure 4.90 NETCONF credential list

Query Netconf credentials:

The Netconf credential list supports paging display, and each Netconf credential 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. Netconf credentials support fuzzy query and filtering by name and organization, as shown in the following figure:

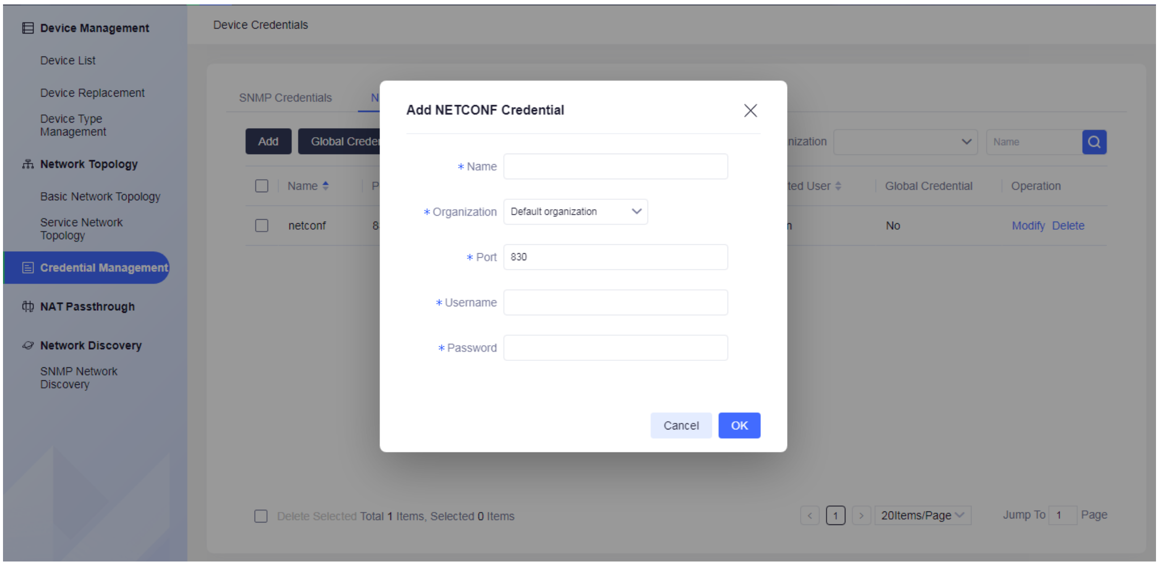


☐	Name	Port	Username	Password	Organization	Updated User	Global Credential	Operation
☐	netconf	830	admin	********	Default organizat...	admin	No	Modify Delete

Figure 4.91 Credential query and hierarchical and decentralized display

Add Netconf Credential:

Click **Add** to open the "Add NETCONF Credential" dialog box, fill in Netconf related parameters, and click **OK** to save the new Netconf credential.



* Name

* Organization: Default organization

* Port: 830

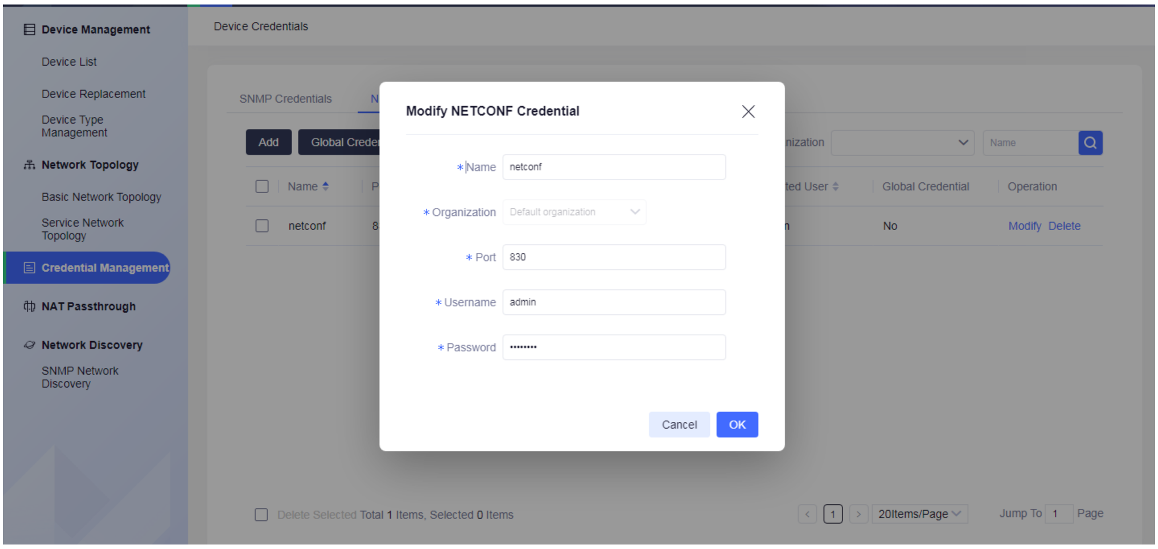
* Username

* Password

Figure 4.92 Add NETCONF credential

Modify Netconf Credential:

Select a desired Netconf credential in the list (only one credential can be modified at the same time), click the **Modify** button to open the "Modify Netconf Credential " dialog box (as shown in the figure below). After modification, click **OK** to save the modified settings. The "Organization" field cannot be modified.



Modify NETCONF Credential

*Name: netconf

*Organization: Default organization

*Port: 830

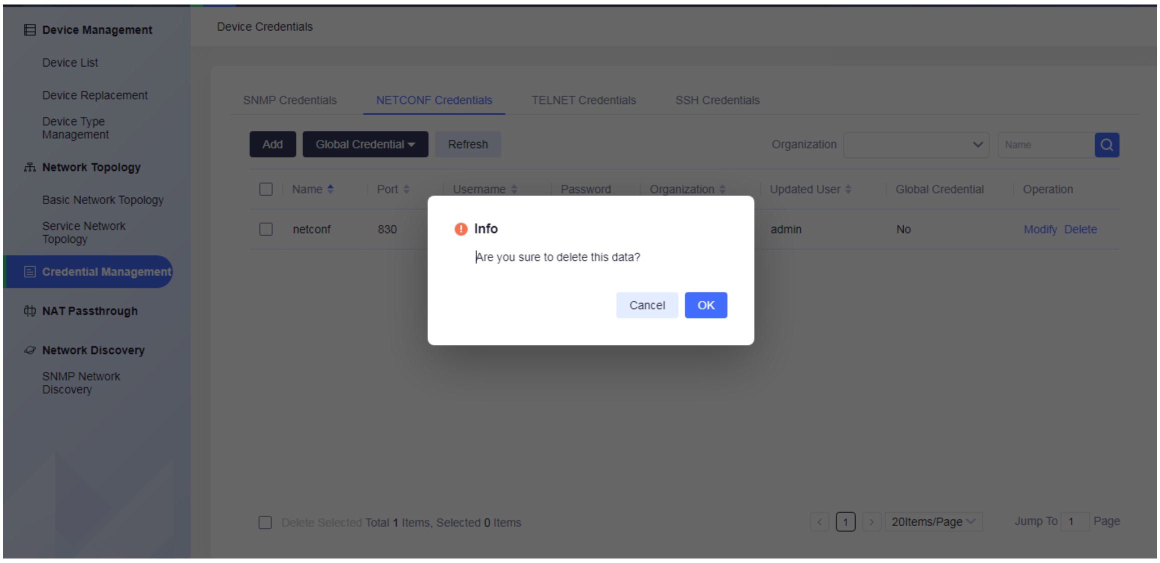
*Username: admin

*Password: ••••••••

Figure 4.93 Modify NETCONF credential

Delete Netconf Credential:

Select a desired Netconf credential in the list (multiple selections are supported), click **Delete**, and click **OK** in the pop-up deletion confirmation dialog box (as shown below) to delete the selected Netconf credential. Click **Cancel** to abort the deletion.



Name	Port	Username	Password	Organization	Updated User	Global Credential
netconf	830				admin	No

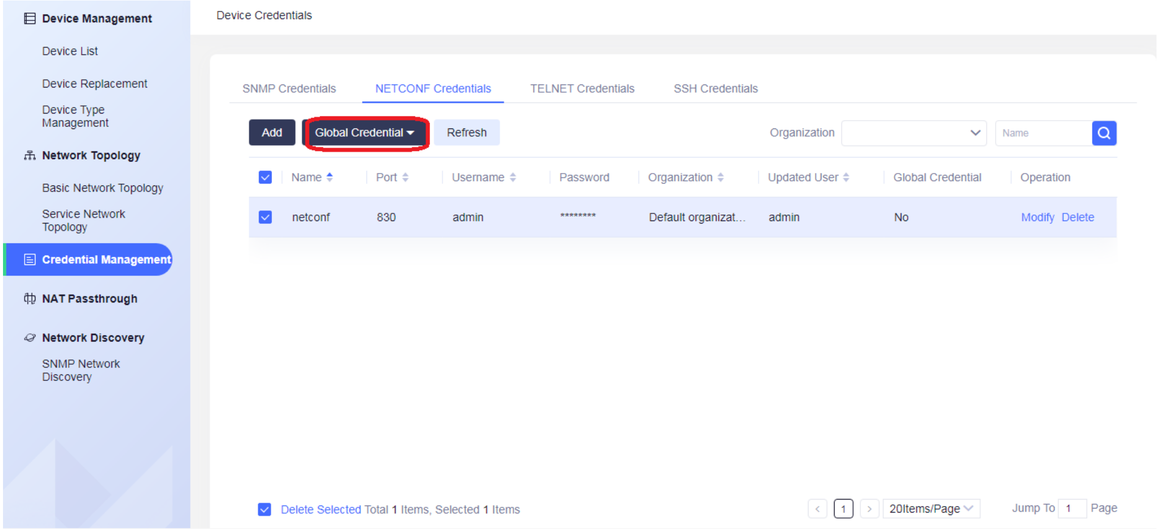
Info

Are you sure to delete this data?

Figure 4.94 Delete NETCONF credential

Global Credential:

The global credential function can set and cancel global credentials. When the device selects the credential, it is not limited by the organization.



☑	Name	Port	Username	Password	Organization	Updated User	Global Credential	Operation
☑	netconf	830	admin	********	Default organizat...	admin	No	Modify Delete

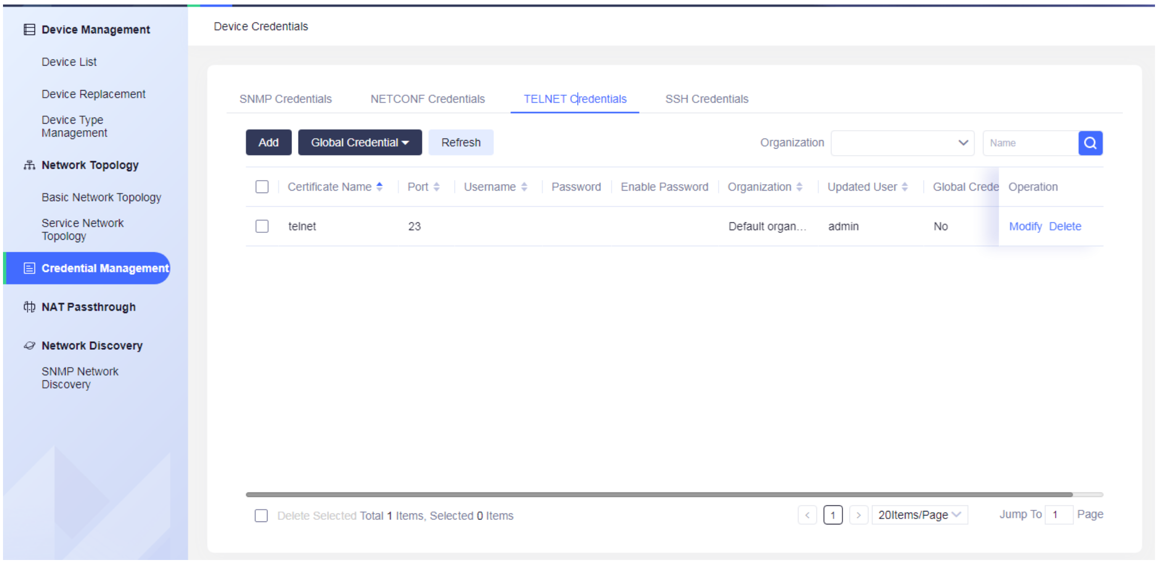
Figure 4.95 NETCONF global credential

Refresh Netconf Credentials:

Click **Refresh** at the top of the list to refresh the credential list data.

4.3.3 TELNET Credential

Telnet credential management is used to manage common Telnet configurations. You can add/delete/modify Telnet credentials. Click "Discovery" - > "Credential Management" - > "Telnet Credentials" in the menu bar to open the "Telnet Credential Management" page, as shown below.

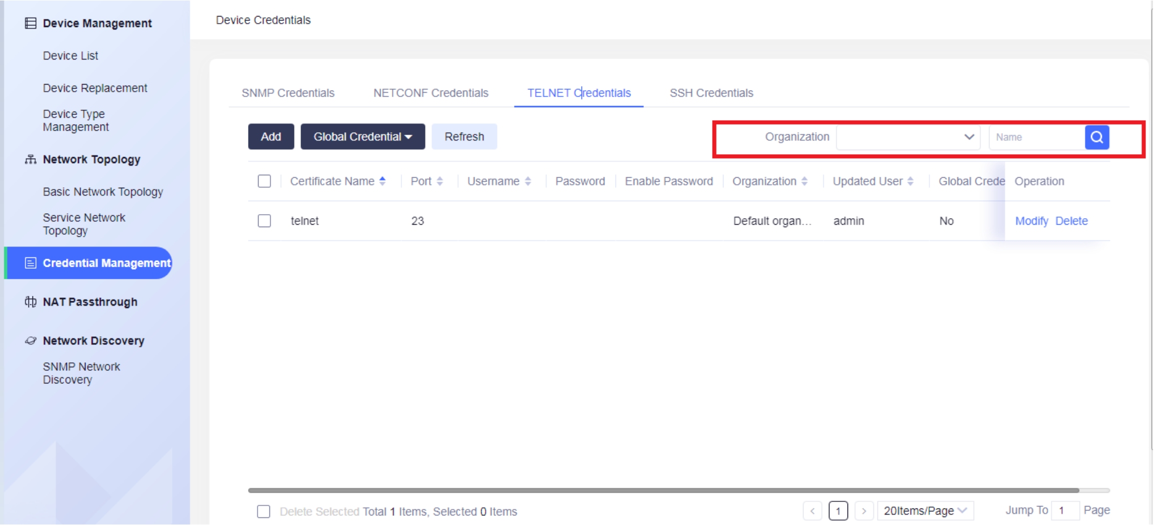


☐	Certificate Name	Port	Username	Password	Enable Password	Organization	Updated User	Global Crede	Operation
☐	telnet	23				Default organ...	admin	No	Modify Delete

Figure 4.96 TELNET credential list

Query Telnet credentials:

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



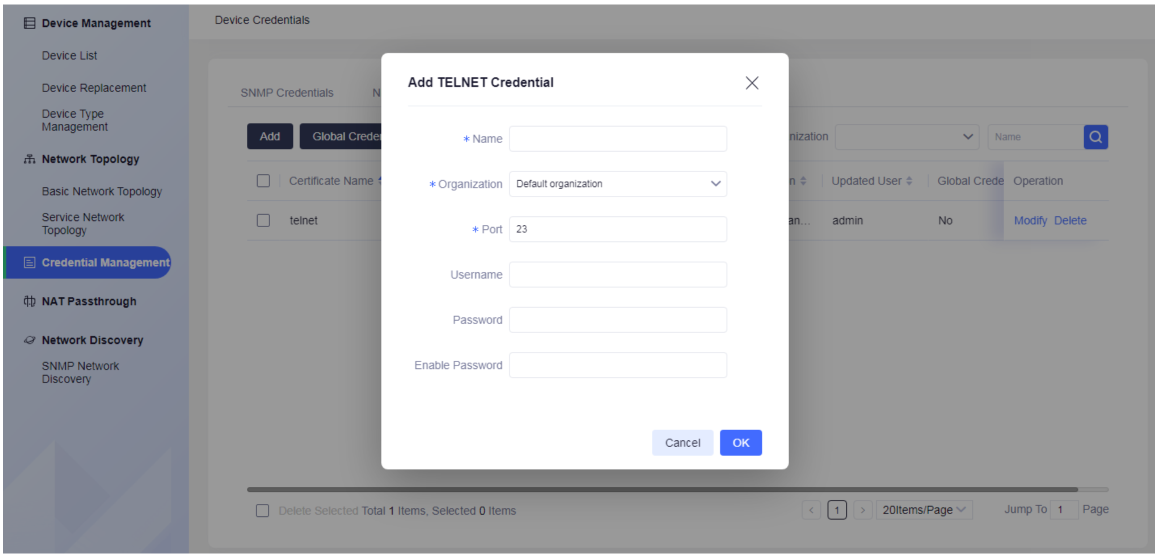
☐	Certificate Name	Port	Username	Password	Enable Password	Organization	Updated User	Global Crede	Operation
☐	telnet	23				Default organ...	admin	No	Modify Delete

☐ Delete Selected Total 1 Items, Selected 0 Items

Figure 4.97 TELNET credential list

Add Telnet Credential:

Click **Add** to open the "Add TELNET Credential" dialog box, fill in Telnet related parameters, and click **OK** to save the new Telnet credential.



Add TELNET Credential

* Name

* Organization: Default organization

* Port: 23

Username

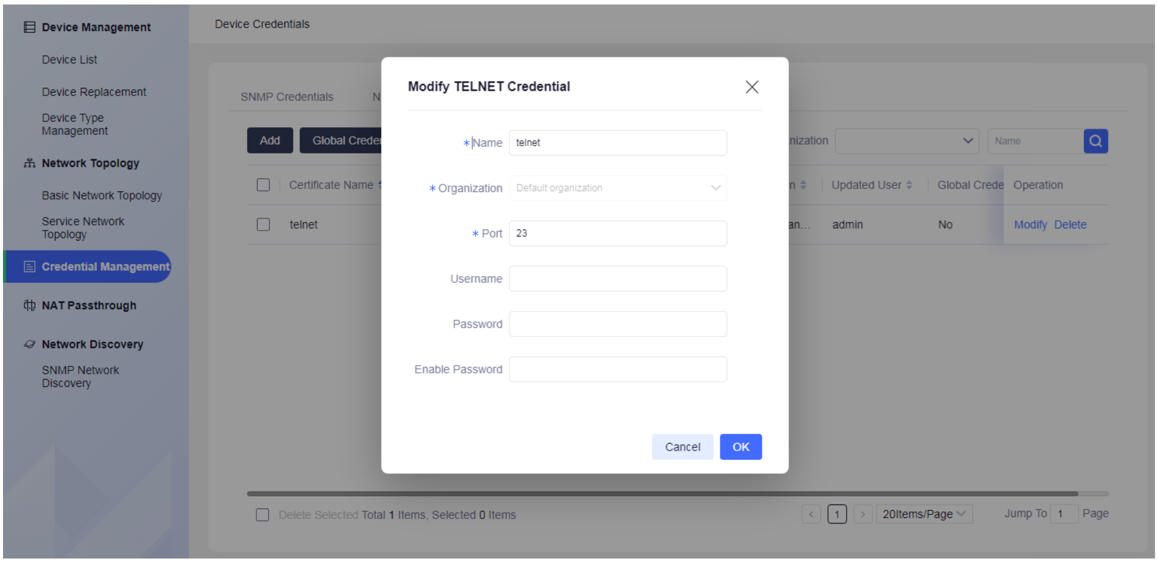
Password

Enable Password

Figure 4.98 Add TELNET credential

Modify Telnet Credential:

Select a desired Telnet credential in the list (only one credential can be modified at the same time), click the **Modify** button to open the "Modify Telnet Credential " dialog box (as shown in the figure below). After modification, click **OK** to save the modified settings. The "Organization" field cannot be modified.



Modify TELNET Credential

*Name: telnet

*Organization: Default organization

*Port: 23

Username:

Password:

Enable Password:

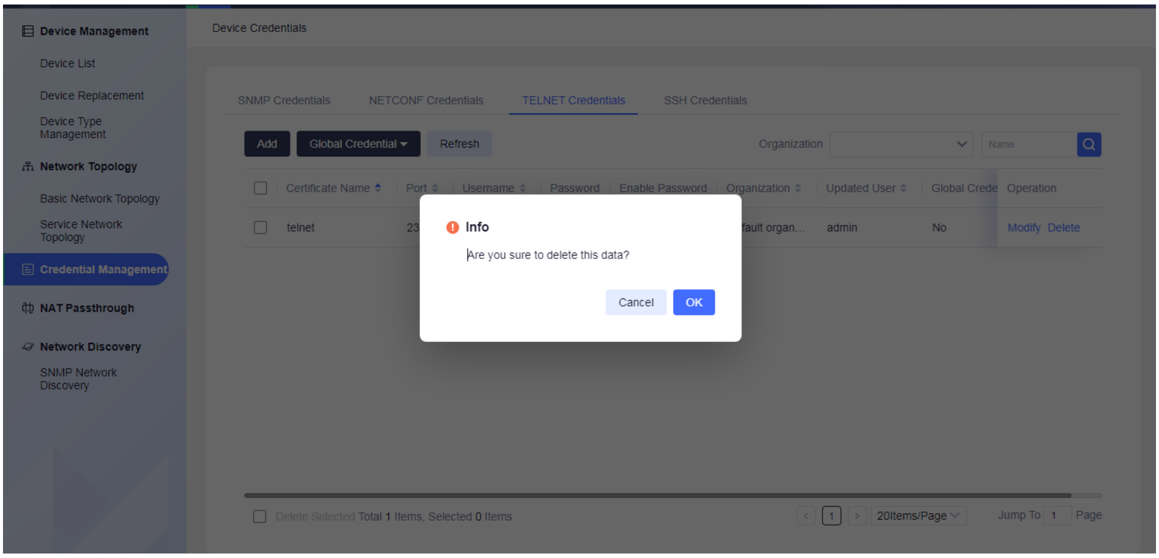
Certificate Name	…	Updated User	Global Crede	Operation
telnet	an...	admin	No	Modify Delete

Total 1 Items, Selected 0 Items

Figure 4.99 Modify the TELNET credential

Delete Telnet Credential:

Select a desired Telnet credential in the list (multiple selections are supported), click **Delete**, and click **OK** in the pop-up deletion confirmation dialog box (as shown below) to delete the selected Telnet credential. Click **Cancel** to abort the deletion.



Certificate Name	Port	Username	Password	Enable Password	Organization	Updated User	Global Crede	Operation
telnet	23				fault organ...	admin	No	Modify Delete

Total 1 Items, Selected 0 Items

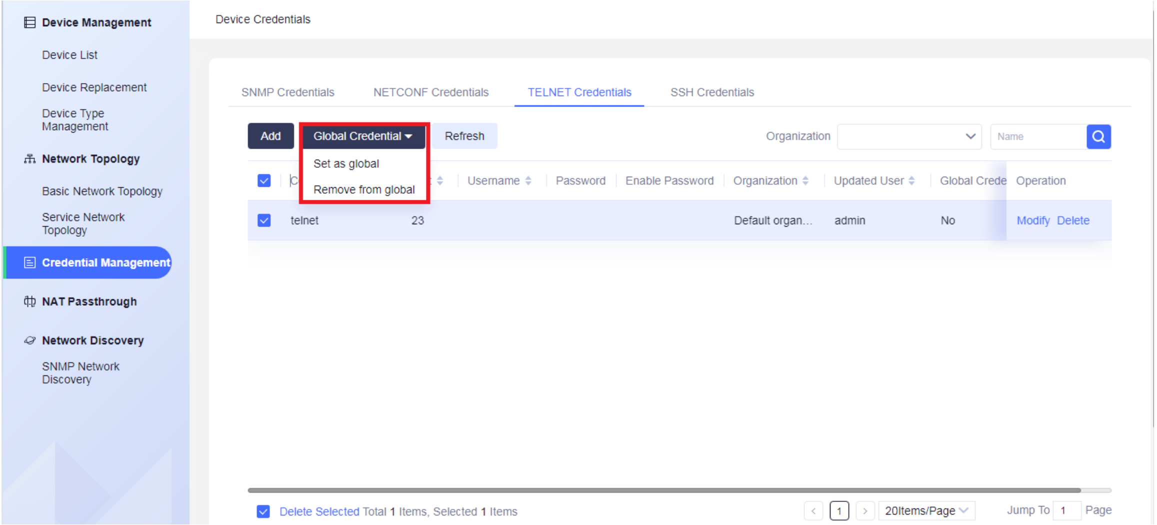
Info

Are you sure to delete this data?

Figure 4.100 Delete the TELNET credential

Global Credential:

The global credential function can set and cancel global credentials. When the device selects the credential, it is not limited by the organization.



☑	C		Username	Password	Enable Password	Organization	Updated User	Global Crede	Operation
☑	telnet	23				Default organ...	admin	No	Modify Delete

Total 1 Items, Selected 1 Items

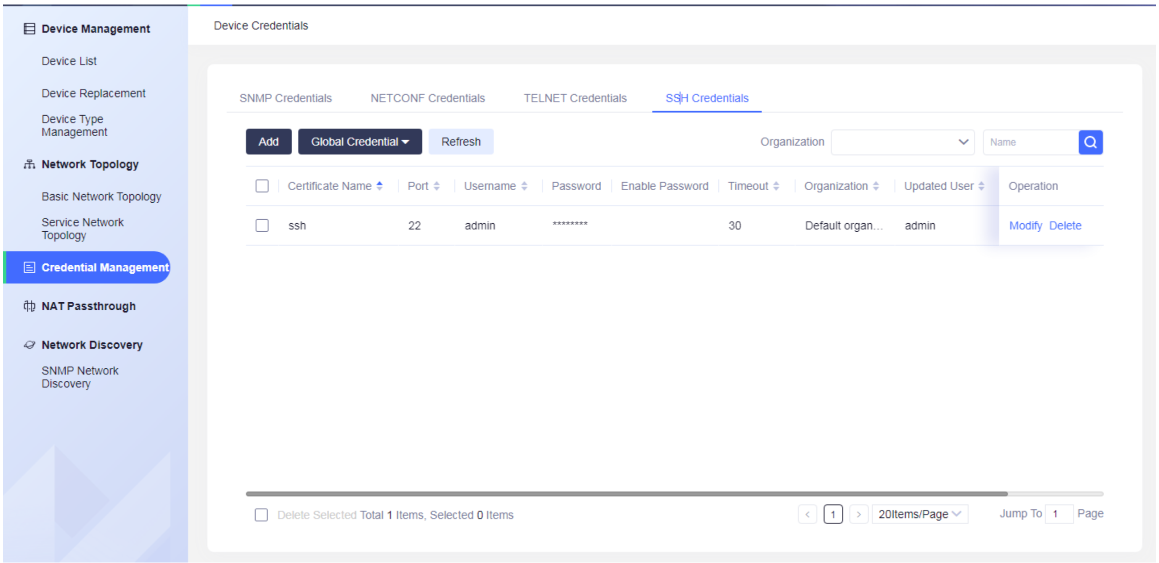
Figure 4.101 TELNET global credential

Refresh Telnet Credentials:

Click **Refresh** at the top of the list to refresh the credential list data.

4.3.4 SSH Credential

SSH credential management is used to manage common SSH configurations. You can add/delete/modify SSH credentials. Click "Discovery" - > "Credential Management" - > "SSH Credentials" in the menu bar to open the "SSH Credential Management" page, as shown below.



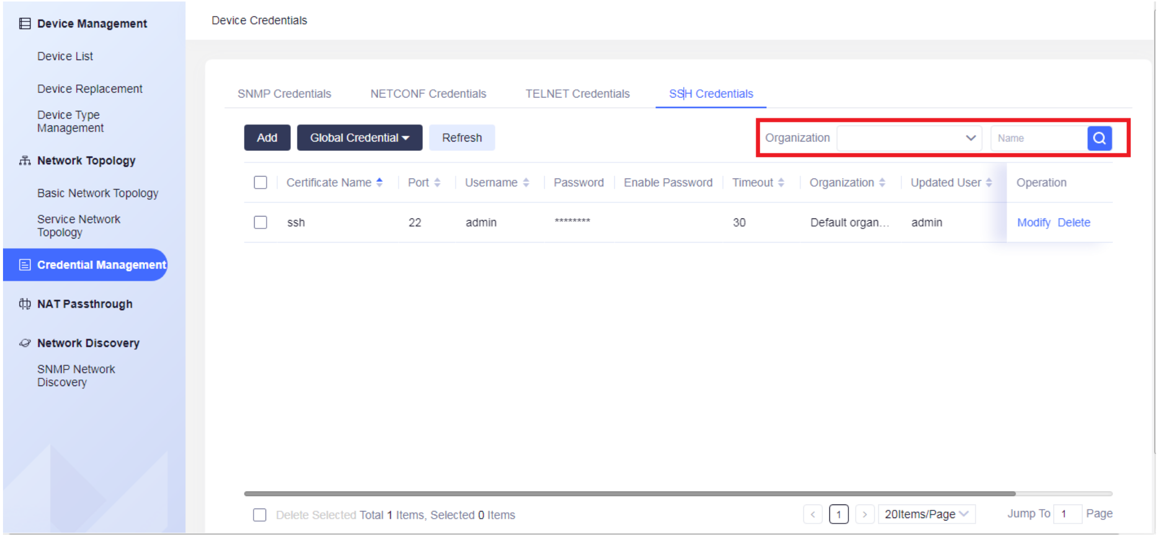
☐	Certificate Name	Port	Username	Password	Enable Password	Timeout	Organization	Updated User	Operation
☐	ssh	22	admin	********		30	Default organ...	admin	Modify Delete

Total 1 Items, Selected 0 Items

Figure 4.102 SSH credential list

Query SSH credentials:

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

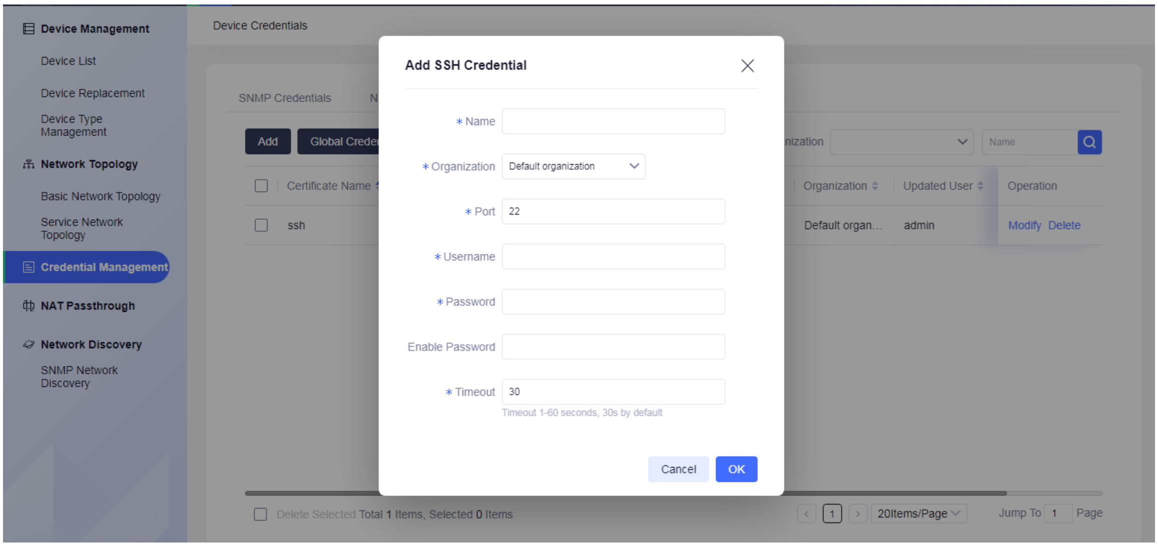


☐	Certificate Name	Port	Username	Password	Enable Password	Timeout	Organization	Updated User	Operation
☐	ssh	22	admin	********		30	Default organ...	admin	Modify Delete

Figure 4.103 SSH credential query and hierarchical and decentralized display

Add SSH Credential:

Click **Add** to open the "Add SSH Credential" dialog box, fill in SSH related parameters, and click **OK** to save the new SSH credential.

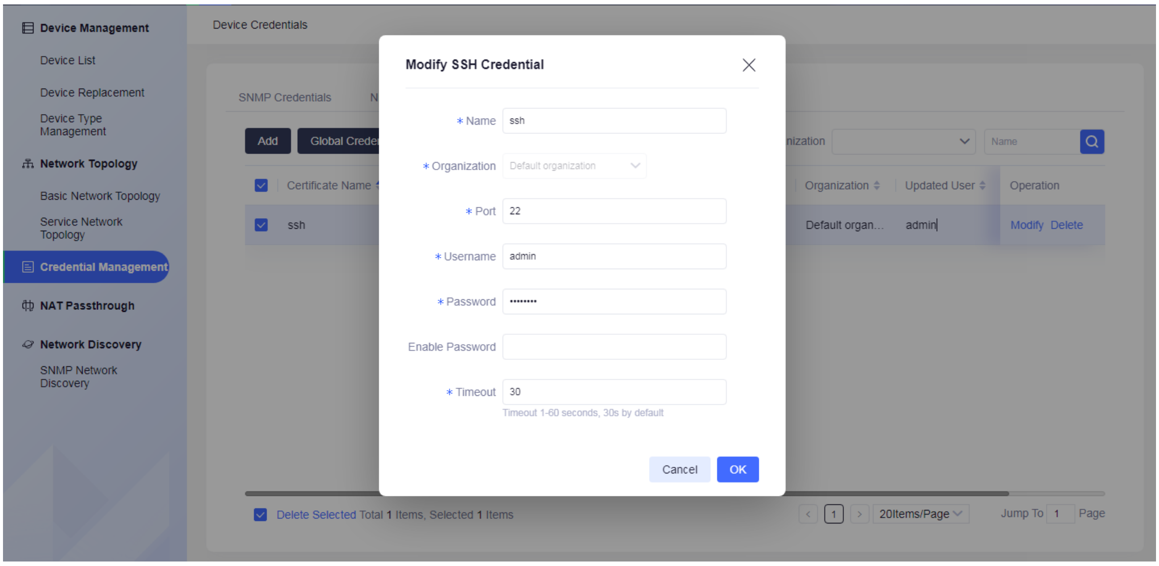


* Name
* Organization Default organization
* Port 22
* Username
* Password
Enable Password
* Timeout 30
Timeout 1-60 seconds, 30s by default

Figure 4.104 Add SSH credential

Modify SSH Credential:

Select a desired SSH credential in the list (only one credential can be modified at the same time), click the **Modify** button to open the "Modify SSH Credential " dialog box (as shown in the figure below). After modification, click **OK** to save the modified settings. The "Organization" field cannot be modified.



Modify SSH Credential

* Name: ssh
* Organization: Default organization
* Port: 22
* Username: admin
* Password: ••••••••
Enable Password:
* Timeout: 30
Timeout 1-60 seconds, 30s by default

ssh | Default organ... | admin

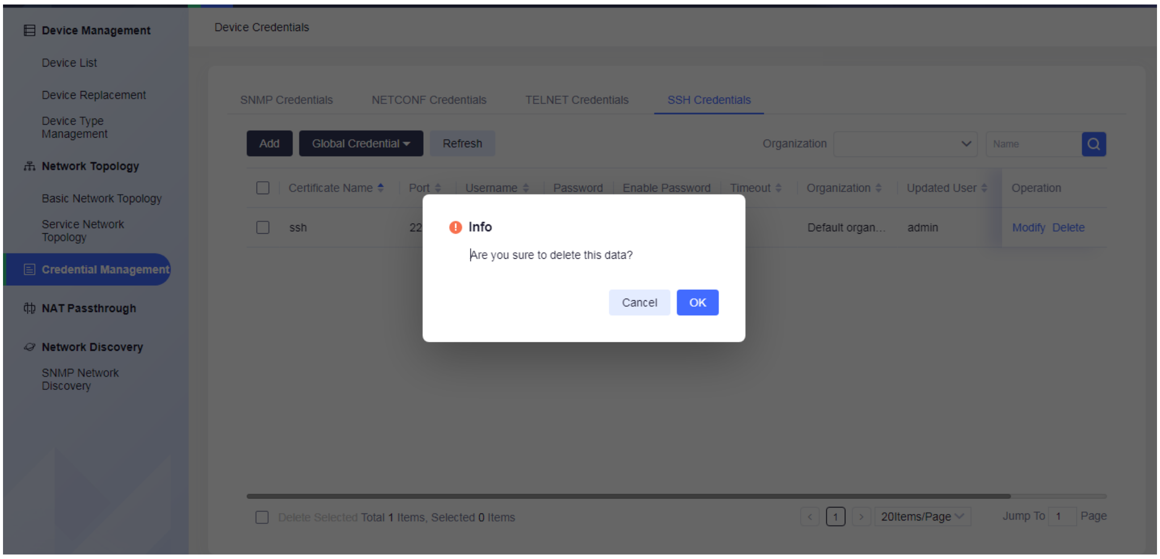
Delete Selected Total 1 Items, Selected 1 Items

1 | 20Items/Page | Jump To 1 Page

Figure 4.105 Modify SSH credential

Delete SSH Credential:

Select a desired SSH credential in the list (multiple selections are supported), click **Delete**, and click **OK** in the pop-up deletion confirmation dialog box (as shown below) to delete the selected SSH credential. Click **Cancel** to abort the deletion.



Info

Are you sure to delete this data?

ssh | 22 | Default organ... | admin

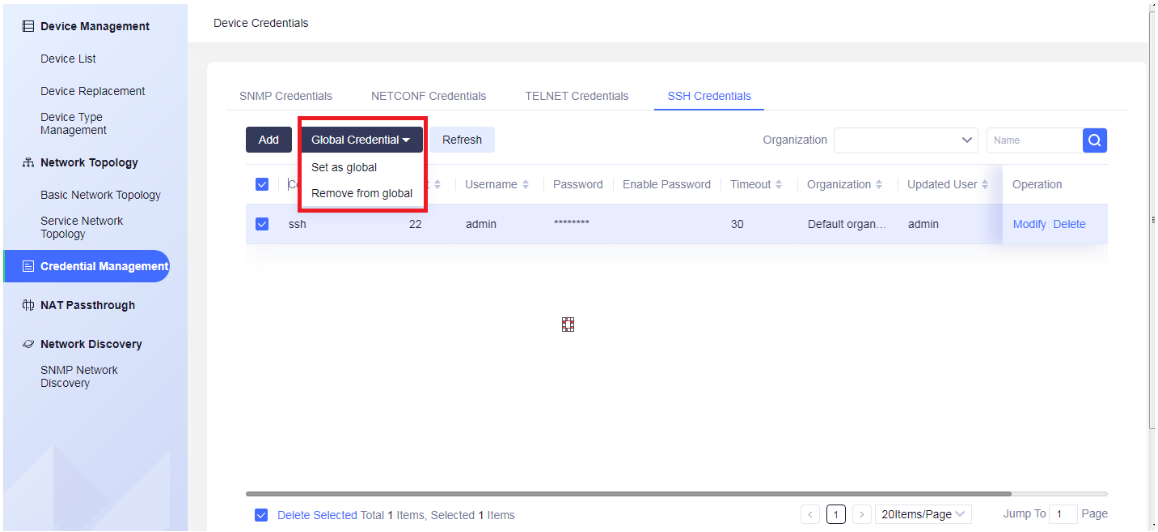
Delete Selected Total 1 Items, Selected 0 Items

1 | 20Items/Page | Jump To 1 Page

Figure 4.106 Delete the SSH credential

Global Credential:

The global credential function can set and cancel global credentials. When the device selects the credential, it is not limited by the organization.



☑			Username	Password	Enable Password	Timeout	Organization	Updated User	Operation
☑	ssh	22	admin	********		30	Default organ...	admin	Modify Delete

Figure 4.107 SSH global credential

Refresh SSH Credentials:

Click **Refresh** at the top of the list to refresh the credential list data.

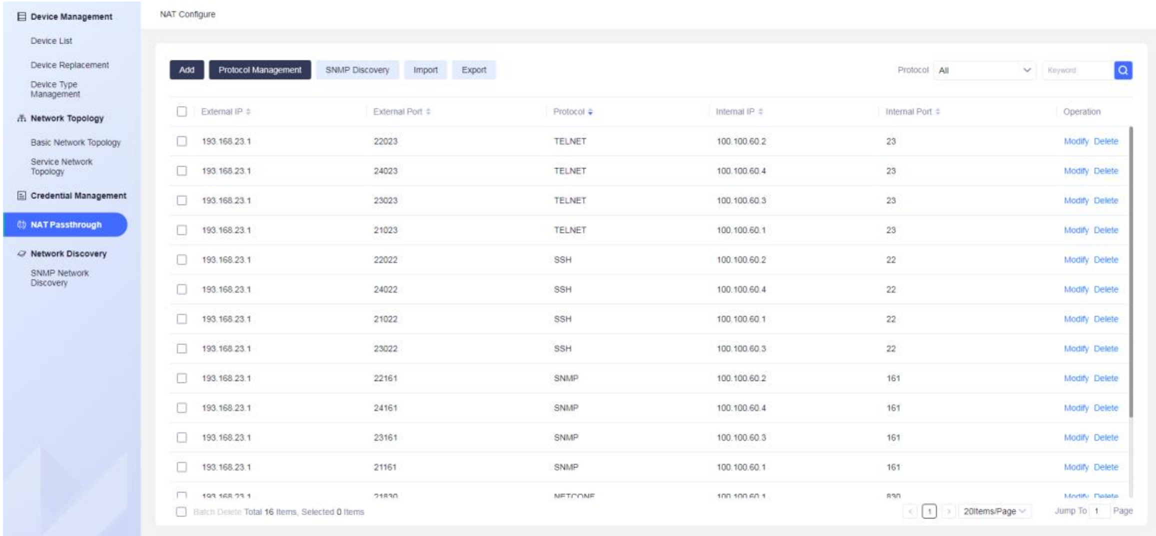
4.4 NAT Configuration

Click "Discovery" in the navigation bar at the top of the system, and then click "NAT Passthrough" in the left menu bar to enter the NAT configuration page. This function mainly provides the functions of adding, deleting, modifying, importing, exporting, jumping network discovery of NAT configuration. The controller will access the devices under NAT according to the configured external IP and external port.

4.4.1 NAT Configuration Management

Click "Discovery" - > "NAT Passthrough" on the navigation bar at the top of the system to open the NAT configuration home page, as shown below:

The list displays the external IP, port, protocol and internal IP and port information in NAT configuration in turn. The **Query** button on the right can support querying through protocol type, IP address, port and other keywords. After adding or importing the configuration, you can automatically jump to the SNMP network discovery page by jumping to the **SNMP Discovery** button, and the IP parameters in this page will automatically fill in the checked NAT configuration information.



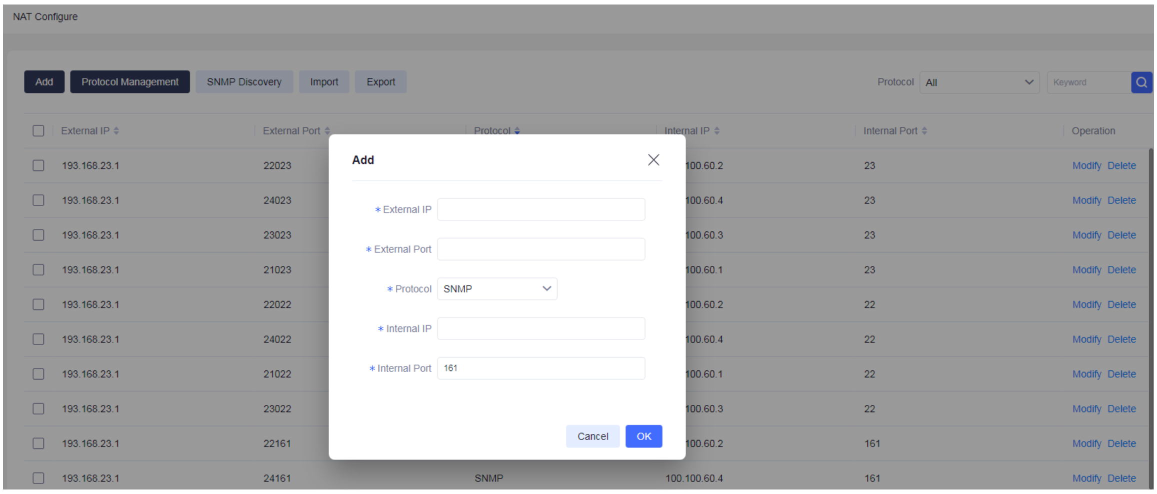
☐	External IP	External Port	Protocol	Internal IP	Internal Port	Operation
☐	193.168.23.1	22023	TELNET	100.100.60.2	23	Modify Delete
☐	193.168.23.1	24023	TELNET	100.100.60.4	23	Modify Delete
☐	193.168.23.1	23023	TELNET	100.100.60.3	23	Modify Delete
☐	193.168.23.1	21023	TELNET	100.100.60.1	23	Modify Delete
☐	193.168.23.1	22022	SSH	100.100.60.2	22	Modify Delete
☐	193.168.23.1	24022	SSH	100.100.60.4	22	Modify Delete
☐	193.168.23.1	21022	SSH	100.100.60.1	22	Modify Delete
☐	193.168.23.1	23022	SSH	100.100.60.3	22	Modify Delete
☐	193.168.23.1	22161	SNMP	100.100.60.2	161	Modify Delete
☐	193.168.23.1	24161	SNMP	100.100.60.4	161	Modify Delete
☐	193.168.23.1	23161	SNMP	100.100.60.3	161	Modify Delete
☐	193.168.23.1	21161	SNMP	100.100.60.1	161	Modify Delete
☐	193.168.23.1	21830	NETCONF	100.100.60.1	830	Modify Delete

Total 16 Items, Selected 0 Items

Figure 4.110 NAT configuration interface

Add configuration:

Click the **Add** button on the toolbar to pop up the "Add" window, as shown in the following figure. Enter the external IP and external port, select the protocol, internal IP and internal port, and click **OK** to save.



Add

∗ External IP:

∗ External Port:

∗ Protocol: SNMP

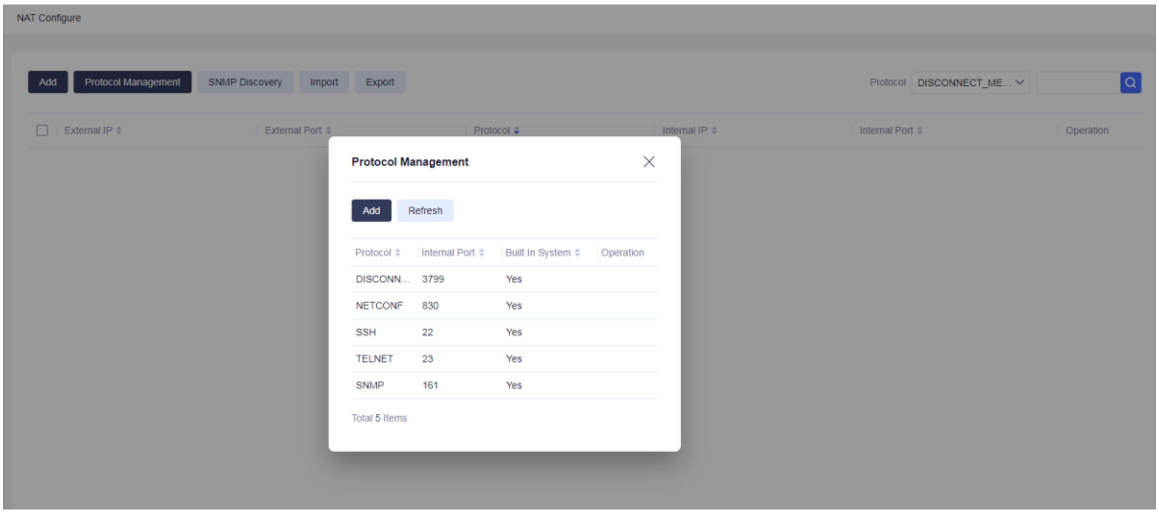
∗ Internal IP:

∗ Internal Port: 161

Figure 4.111 Add NAT configuration

Protocol Management:

Click the **Protocol Management** button on the toolbar to pop up the "**Protocol Management**" window, as shown in the following figure. The dialog box displays the built-in protocol items in the current system. If you need to add a protocol, you can click the **Add** button. Note that the protocol name needs to be composed of uppercase letters and underscores. After adding a customized protocol type, it can be deleted.

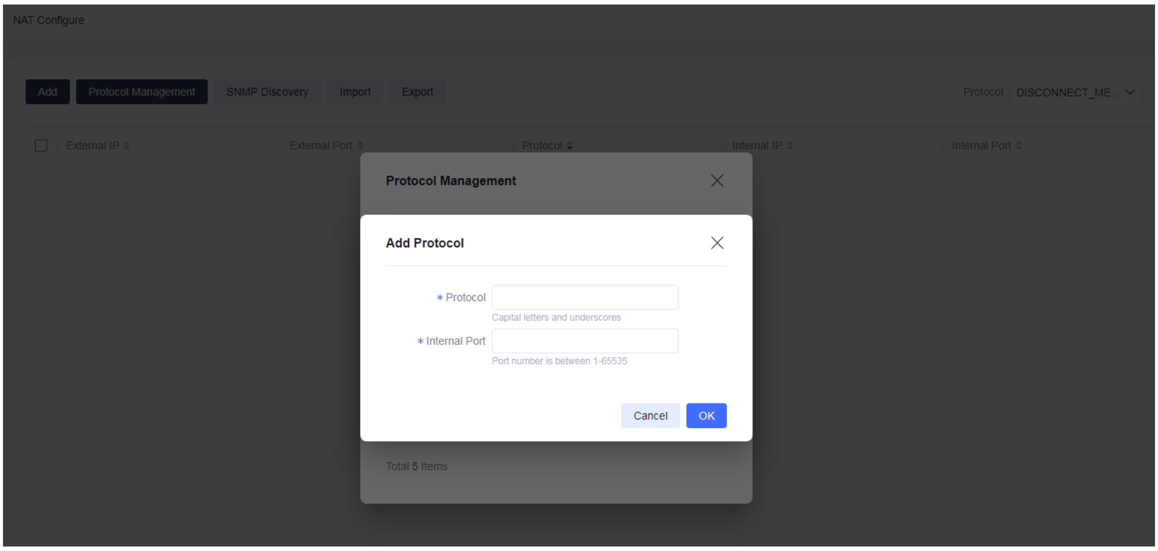


Protocol Management

Protocol	Internal Port	Built In System	Operation
DISCONN...	3799	Yes	
NETCONF	830	Yes	
SSH	22	Yes	
TELNET	23	Yes	
SNMP	161	Yes	

Total 5 Items

Figure 4.112 Protocol management page



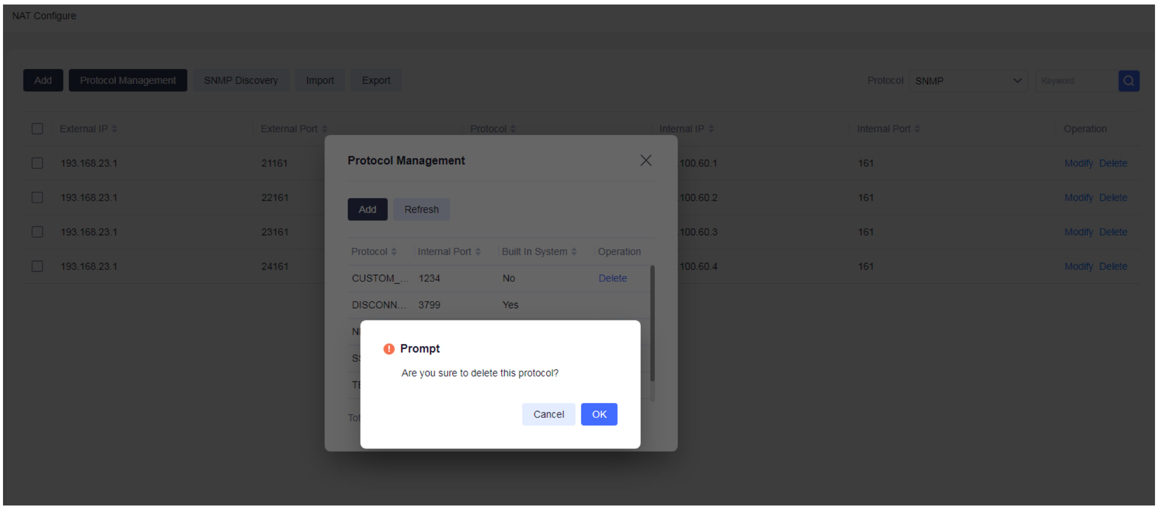
Add Protocol

* Protocol
Capital letters and underscores

* Internal Port
Port number is between 1-65535

Total 5 Items

Figure 4.113 Add customized protocol type



☐	External IP	External Port	Protocol	Internal IP	Internal Port	Operation
☐	193.168.23.1	21161		100.60.1	161	Modify Delete
☐	193.168.23.1	22161		100.60.2	161	Modify Delete
☐	193.168.23.1	23161		100.60.3	161	Modify Delete
☐	193.168.23.1	24161		100.60.4	161	Modify Delete

Protocol Management

Protocol	Internal Port	Built In System	Operation
CUSTOM_...	1234	No	Delete
DISCONN...	3799	Yes	

Prompt

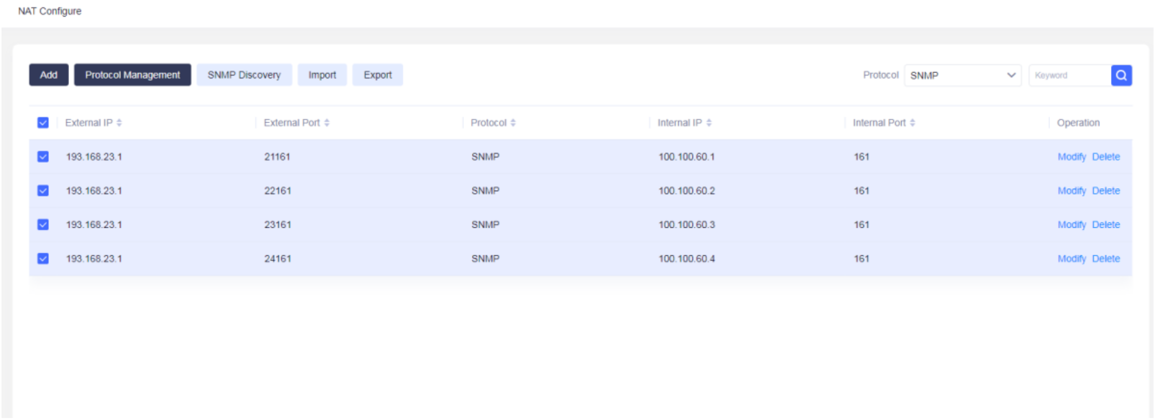
Are you sure to delete this protocol?

Figure 4.114 Delete customized protocol type

Jump SNMP network discovery:

Manually select or filter the NAT configuration entries of the SNMP protocol, and click the **SNMP Discovery** button on the toolbar to automatically jump to the SNMP discovery page. On this page, the user needs to fill in the name of the network discovery task, and then click the **Next** button.

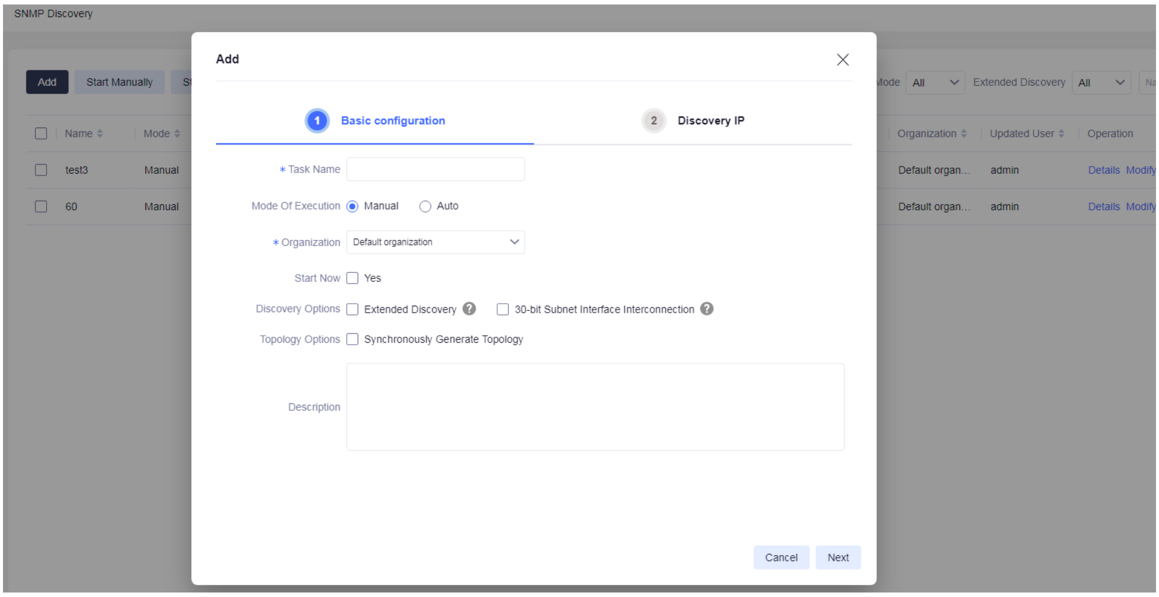
The device IP in this page has been automatically filled, so you only need to select the SNMP credential of the corresponding device to perform SNMP network discovery. Refer to Section 4.4 “Network Discovery” for specific operations of SNMP discovery.


NAT Configure

Protocol: SNMP

☑	External IP	External Port	Protocol	Internal IP	Internal Port	Operation
☑	193.168.23.1	21161	SNMP	100.100.60.1	161	Modify Delete
☑	193.168.23.1	22161	SNMP	100.100.60.2	161	Modify Delete
☑	193.168.23.1	23161	SNMP	100.100.60.3	161	Modify Delete
☑	193.168.23.1	24161	SNMP	100.100.60.4	161	Modify Delete

Figure 4.115 SNMP discovery jump button

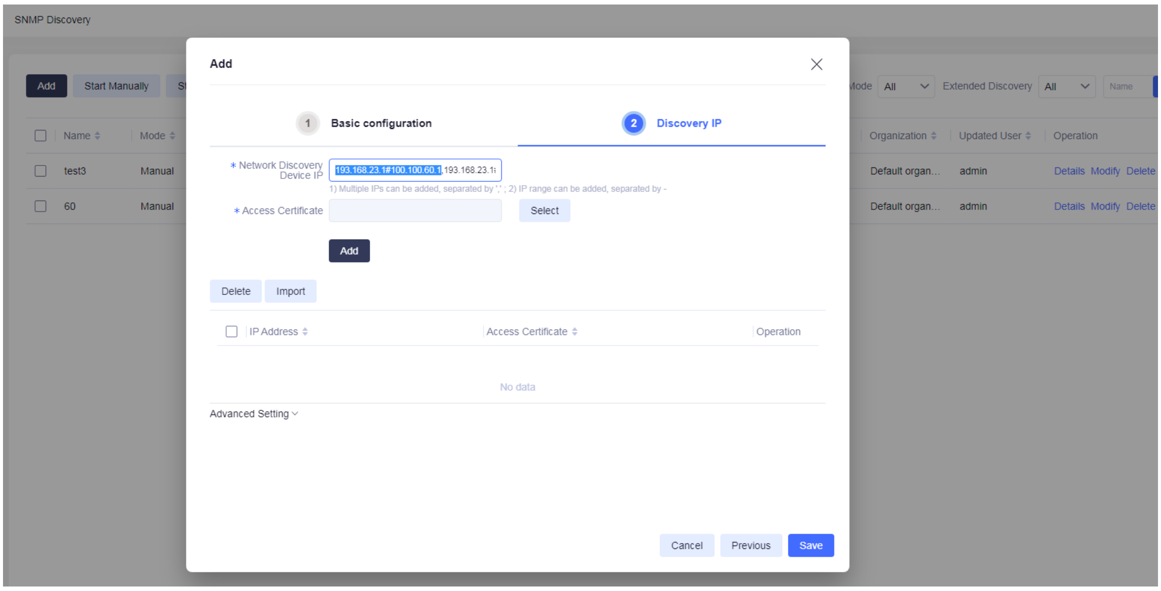

SNMP Discovery

Add

1 Basic configuration
2 Discovery IP

* Task Name:
Mode Of Execution: ● Manual ○ Auto
* Organization: Default organization
Start Now: ☐ Yes
Discovery Options: ☐ Extended Discovery ☐ 30-bit Subnet Interface Interconnection
Topology Options: ☐ Synchronously Generate Topology
Description:

Figure 4.116 Step 1 of SNMP discovery page


SNMP Discovery

Add

1 Basic configuration
2 Discovery IP

* Network Discovery Device IP: 193.168.23.1#100.100.60.1,193.168.23.1
1) Multiple IPs can be added, separated by ',' ; 2) IP range can be added, separated by -
* Access Certificate:

☐	IP Address	Access Certificate	Operation

No data

Advanced Setting

Figure 4.117 Step 2 of SNMP discovery page

Import configuration:

Click the **Import** button on the toolbar, and in the pop-up dialog box, you can download the template file required for importing. Fill in the desired NAT configuration information in the file to import the system and automatically generate NAT configuration.

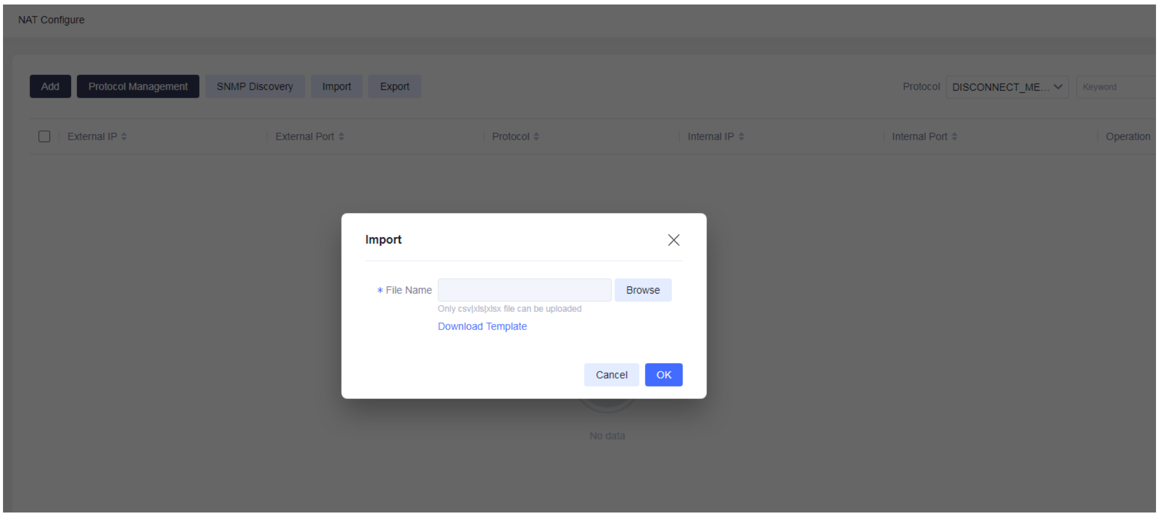


Figure 4.118 Import the configuration

Export configuration:

Click the **Export** button on the toolbar to export all NAT configurations in the current system.

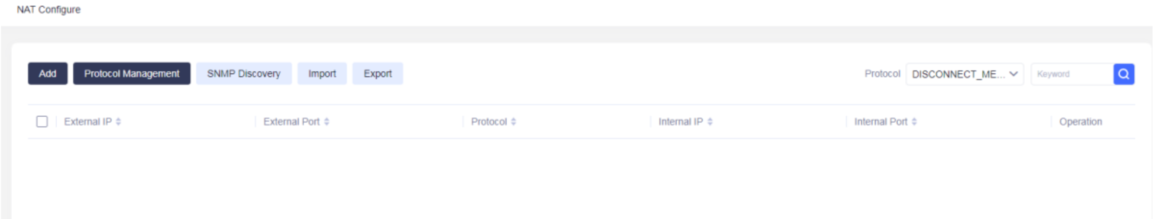
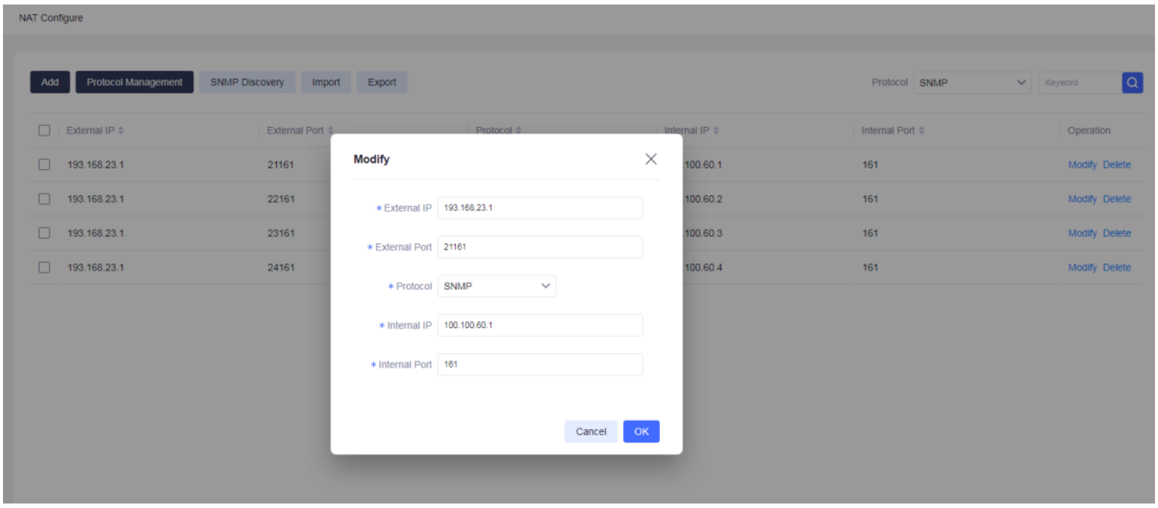


Figure 4.119 Export configuration

Modify configuration:

Click the **Modify** button at the end of NAT configuration to modify the NAT configuration. After modification, click the **OK** button to save the configuration.



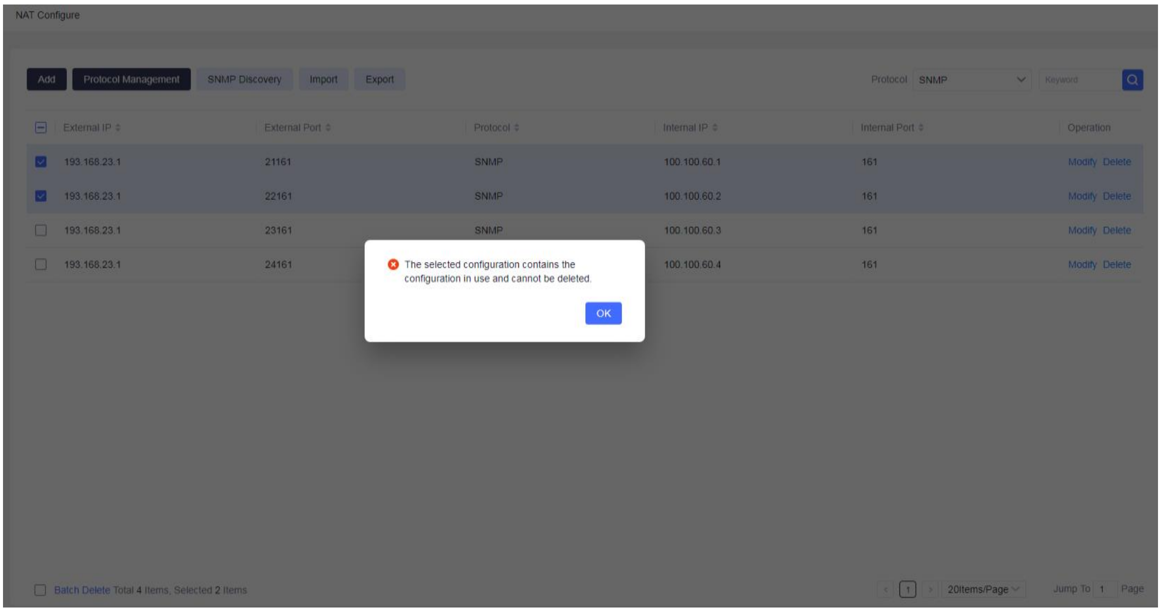
☐	External IP	External Port	Internal Port	Operation
☐	193.168.23.1	21161	161	Modify Delete
☐	193.168.23.1	22161	161	Modify Delete
☐	193.168.23.1	23161	161	Modify Delete
☐	193.168.23.1	24161	161	Modify Delete

* External IP 193.168.23.1
* External Port 21161
* Protocol SNMP
* Internal IP 100.100.60.1
* Internal Port 161

Figure 4.120 Modify NAT configuration

Delete configuration:

Click the **Delete** button at the end of NAT configuration to delete this NAT configuration. If batch deletion is required, you can click **Batch Delete** at the bottom by batch checking. It should be noted that if the deleted configuration has been used by the device, it cannot be deleted.



☐	External IP	External Port	Protocol	Internal IP	Internal Port	Operation
☑	193.168.23.1	21161	SNMP	100.100.60.1	161	Modify Delete
☑	193.168.23.1	22161	SNMP	100.100.60.2	161	Modify Delete
☐	193.168.23.1	23161	SNMP	100.100.60.3	161	Modify Delete
☐	193.168.23.1	24161		100.100.60.4	161	Modify Delete

The selected configuration contains the configuration in use and cannot be deleted.

Total 4 Items, Selected 2 Items

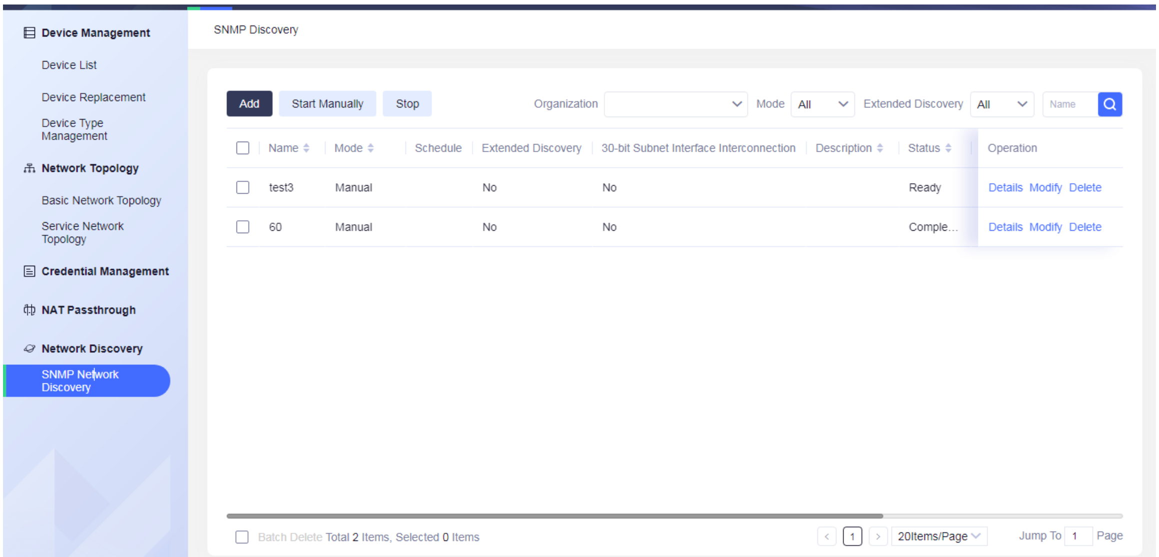
Figure 4.121 Delete NAT configuration

4.5 Network Discovery

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

4.5.1 SNMP Network Discovery

Click "Discovery" - > "Network Discovery" - > "SNMP Network Discovery" on the navigation bar at the top of the system to open the network device discovery page, as shown below:



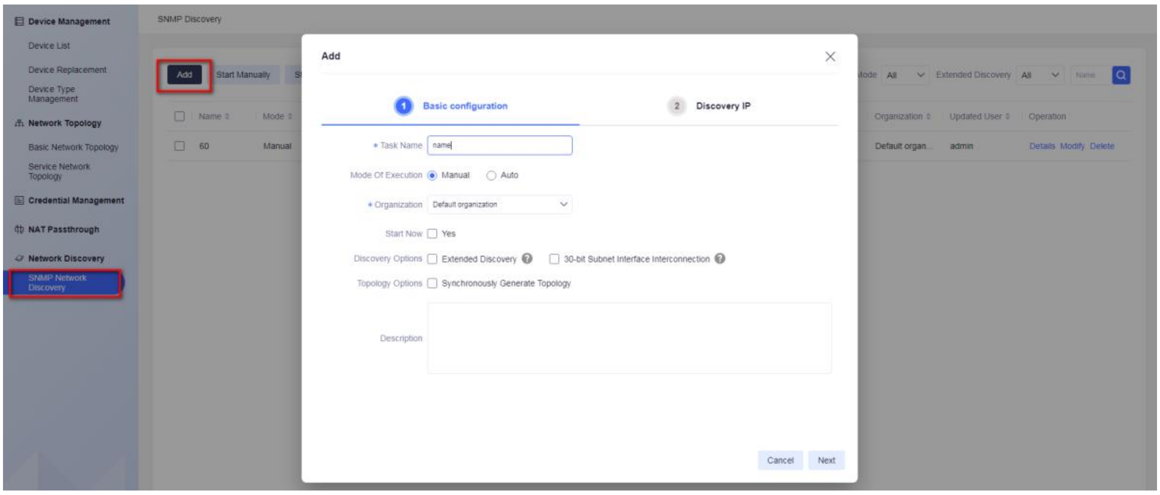
☐	Name	Mode	Schedule	Extended Discovery	30-bit Subnet Interface Interconnection	Description	Status	Operation
☐	test3	Manual		No	No		Ready	Details Modify Delete
☐	60	Manual		No	No		Comple...	Details Modify Delete

Total 2 Items, Selected 0 Items

Figure 4.122 SNMP network discovery

Add discovery task

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



Add

* Task Name: name

Mode Of Execution: ● Manual ○ Auto

* Organization: Default organization

Start Now: ☐ Yes

Discovery Options: ☐ Extended Discovery ☐ 30-bit Subnet Interface Interconnection

Topology Options: ☐ Synchronously Generate Topology

Description:

Figure 4.108 Step 1 of adding SNMP network discovery

Note

- When "Auto" is selected as the execution mode, there is an additional input 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 scheduling frequency, there are "scheduling date" (Monday, Tuesday, Wednesday, Thursday, Friday, Saturday and Sunday) and "scheduling time", If the scheduling frequency is "Monthly", there are "Scheduling date" (1st-31st) and "Scheduling time".
- Discovery Options: “Extended Discovery”, after ticking, discovery the other network devices connected by all interfaces of the network device.
- Topology Options: "Synchronously Generate Topology ". When checked, the topology view will be created under the organization to which the network discovery task belongs, and its type is physical view. (this option is available only when adding discovery tasks).

Click the **Next** button to open the second step configuration window, as shown in the figure below: users can add, delete and import SNMP network discovery credential information. After entering the correct credential information, click **Save** to complete the adding operation.

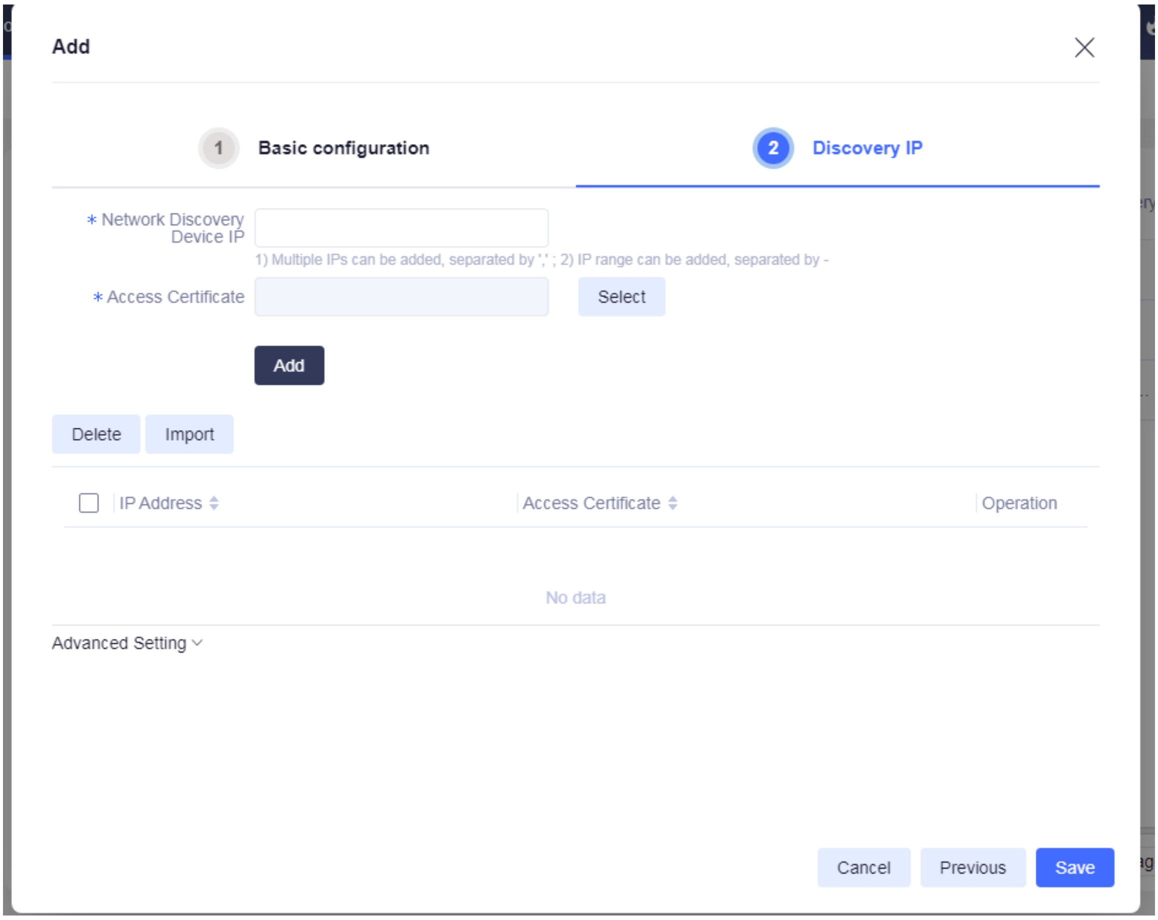
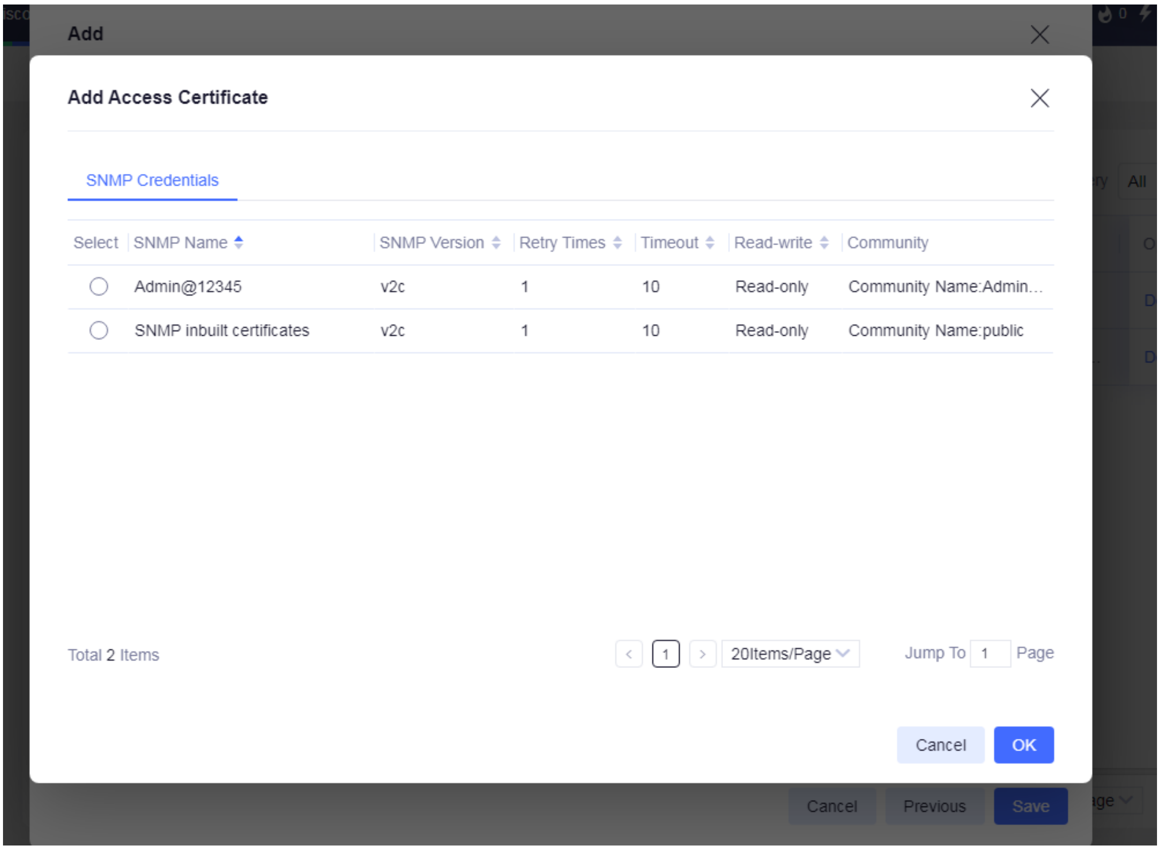


Figure 4.109 Step 2 of adding SNMP network discovery

Add IP and credential information:

Enter a single IP address or address segment in the "Network Discovery device IP" input box, click the selection button of **Access Certificate** to pop up the "Add Access Certificate" selection box, as shown in the figure below. After checking, click the "OK" button to complete the selection and close the selection dialog box.



Select	SNMP Name	SNMP Version	Retry Times	Timeout	Read-write	Community
○	Admin@12345	v2c	1	10	Read-only	Community Name:Admin...
○	SNMP inbuilt certificates	v2c	1	10	Read-only	Community Name:public

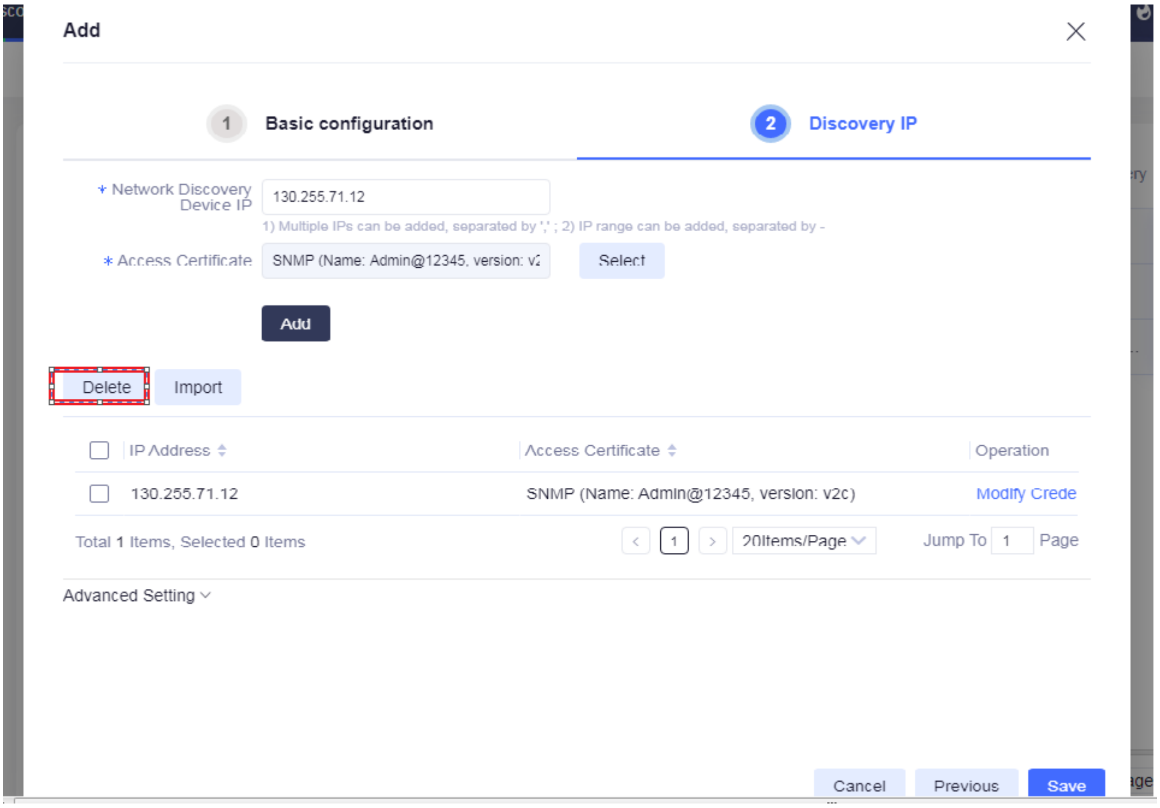
Figure 4.11025 Step 2 of SNMP network discovery –Add access certificate

Note

- For the network discovery device IP, you can input multiple IPs at one time, separated by "," (English comma); You can also enter the IP address range separated by "-";

Delete IP and credential information:

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



* Network Discovery Device IP: 130.255.71.12

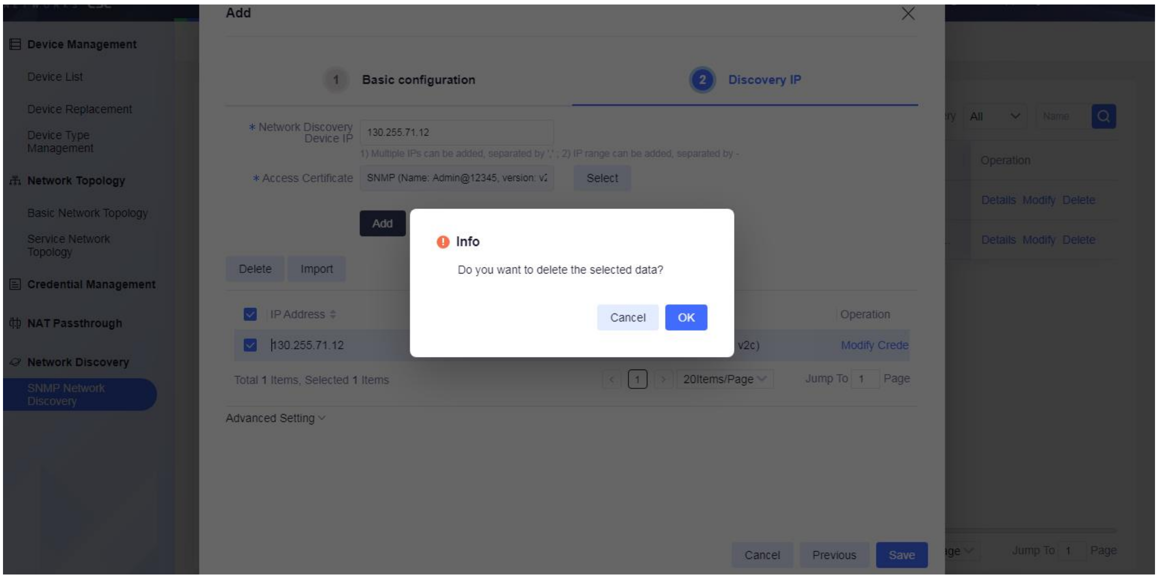
1) Multiple IPs can be added, separated by ',' ; 2) IP range can be added, separated by -

* Access Certificate: SNMP (Name: Admin@12345, version: v2

☐	IP Address	Access Certificate	Operation
☐	130.255.71.12	SNMP (Name: Admin@12345, version: v2c)	Modify Crede

Total 1 Items, Selected 0 Items

Figure 4.11126 Step 2 of adding SNMP network discovery – Delete discovery IP



Info

Do you want to delete the selected data?

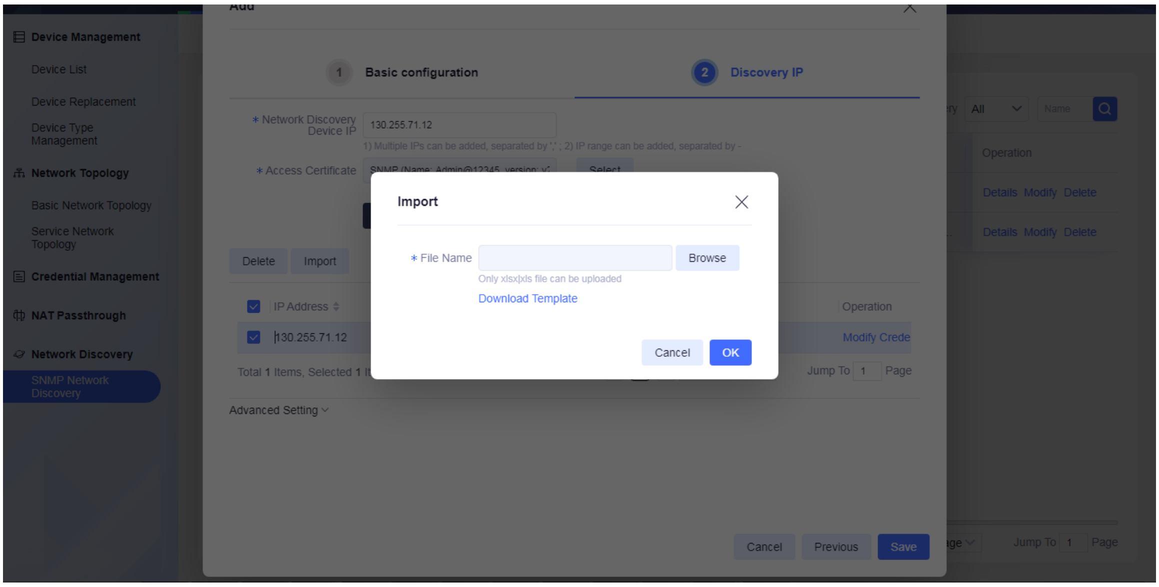
Cancel OK

Total 1 Items, Selected 1 Items

Figure 4.11227 Step 2 of adding SNMP network discovery-Delete discovery IP

Import IP and credential information:

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



* Network Discovery Device IP: 130.255.71.12

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

* Access Certificate: SNMP (Name: Admin@12345, version: v

Total 1 Items, Selected 1

Import

* File Name [ ] Browse

Only xlsx|xls file can be uploaded

Download Template

Cancel OK

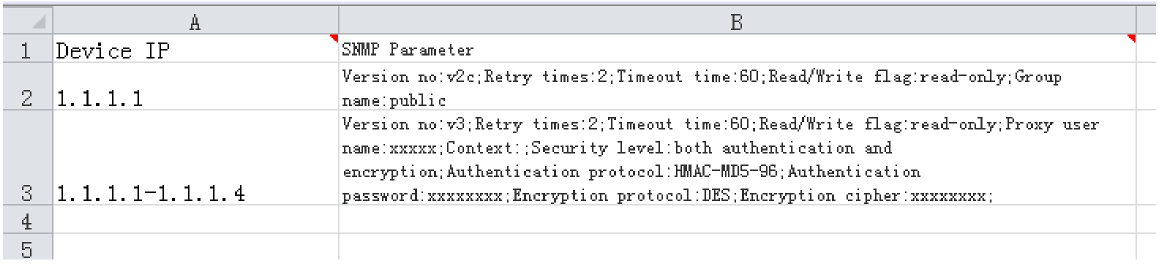
Figure 4.11328 Step 2 of adding SNMP network discovery – Import discovery IP

Note

- For Excel format, please refer to the file format downloaded in "Template Download" (see the next section for details).
- After importing the credential, the system will automatically match the credential with the same parameters. If there is no matching, create the corresponding credential automatically. Automatically created credentials can be configured in the "Device Information - > Device Credential" module.

Template downloading:

Click the **Download Template** button, select the file saving path, and you can complete the template file download. The template file is as shown in the figure below.



	A	B
1	Device IP	SNMP Parameter
2	1.1.1.1	Version no:v2c;Retry times:2;Timeout time:60;Read/Write flag:read-only;Group name:public
3	1.1.1.1-1.1.1.4	Version no:v3;Retry times:2;Timeout time:60;Read/Write flag:read-only;Proxy user name:xxxxx;Context:;Security level:both authentication and encryption;Authentication protocol:HMAC-MD5-96;Authentication password:xxxxxxxx;Encryption protocol:DES;Encryption cipher:xxxxxxxx;
4		
5		

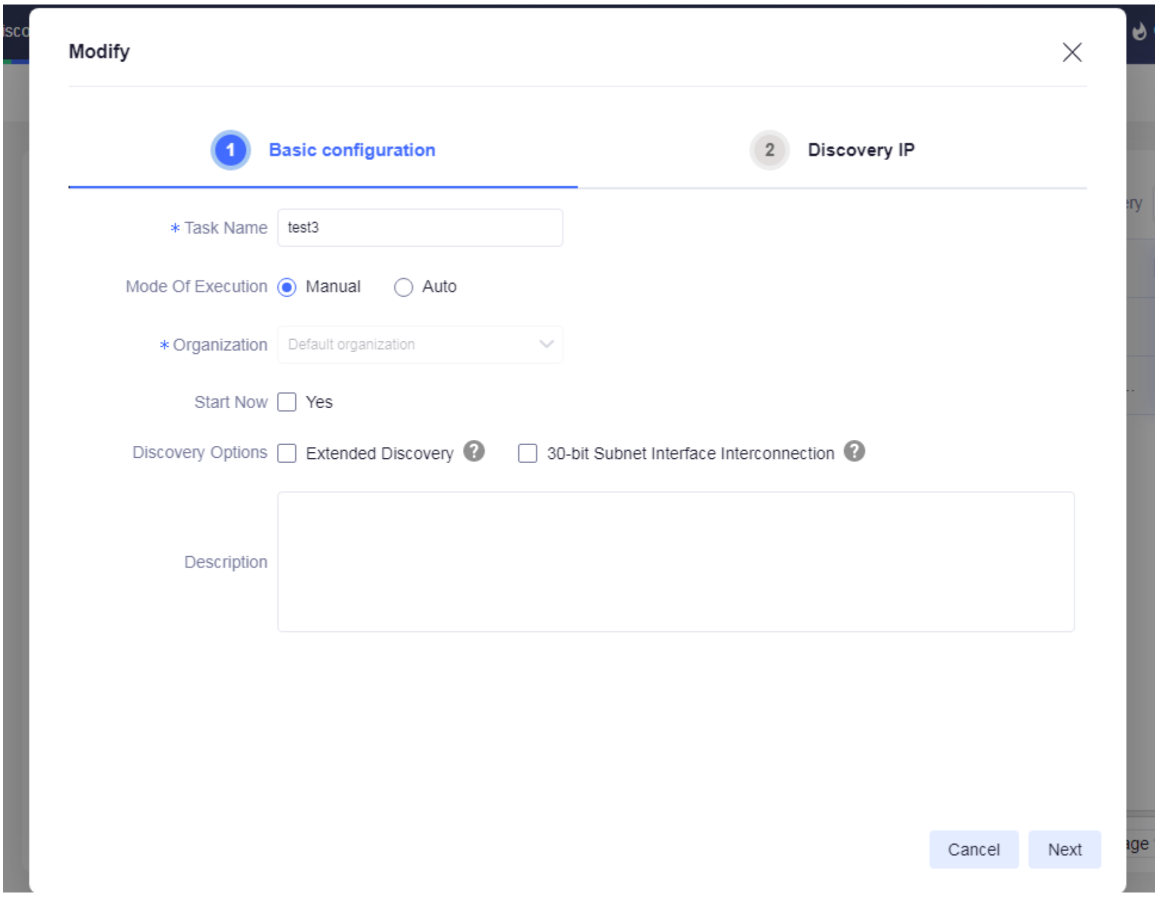
Figure 4.11429 SNMP template file

Note

- If the mouse hovers over the title of the first line, the annotation information will pop up automatically.

Modify Discovery Task

Check the desired task information in the discovery task list, and click **Modify** to open the **Modify** window, as shown in the following figure. According to the operation steps of adding a discovery task, complete the modification of the discovery task.



* Task Name: test3

Mode Of Execution: ● Manual ○ Auto

* Organization: Default organization

Start Now: ☐ Yes

Discovery Options: ☐ Extended Discovery ☐ 30-bit Subnet Interface Interconnection

Description:

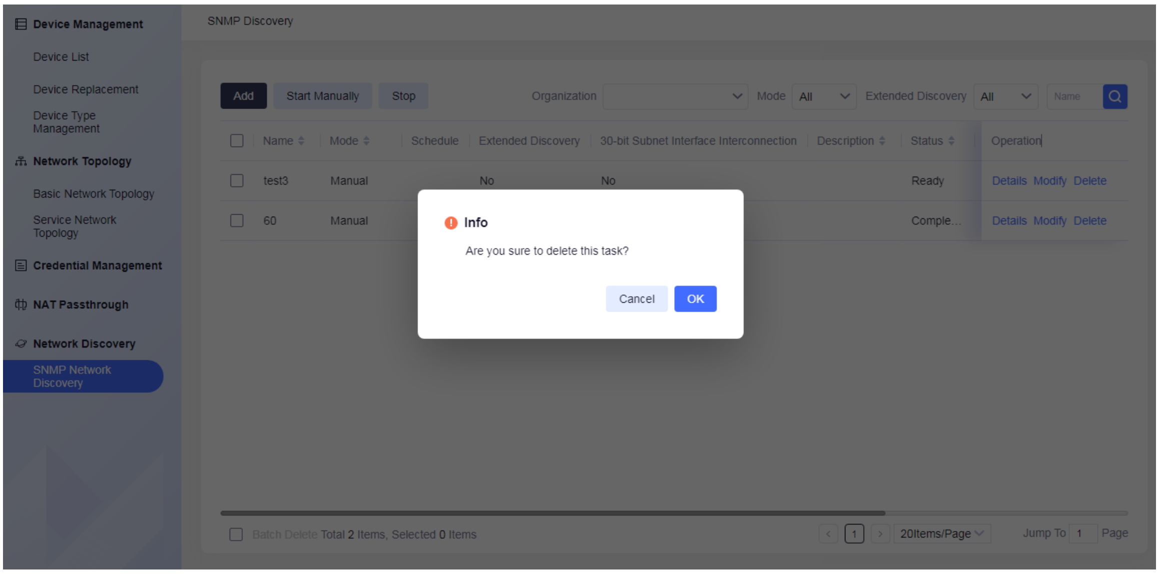
Figure 4.11530 Step 1 of modifying SNMP discovery task

Note

- Only one task information can be selected when modifying a discovery task.
- The started task cannot be modified. When modifying the network discovery task, there is no option to generate topology synchronously.

Delete discovery task

Check a desired task information in the discovery task list (multiple selections are supported), and click the **Delete** button to pop up the confirmation dialog box for deleting the discovery task, as shown in the following figure. Click **OK** to confirm the deletion of the selected task information, or click **Cancel** to abort the deletion.



☐	Name	Mode	Schedule	Extended Discovery	30-bit Subnet Interface Interconnection	Description	Status	Operation
☐	test3	Manual		No	No		Ready	Details Modify Delete
☐	60	Manual					Comple...	Details Modify Delete

Info

Are you sure to delete this task?

Cancel OK

Total 2 Items, Selected 0 Items

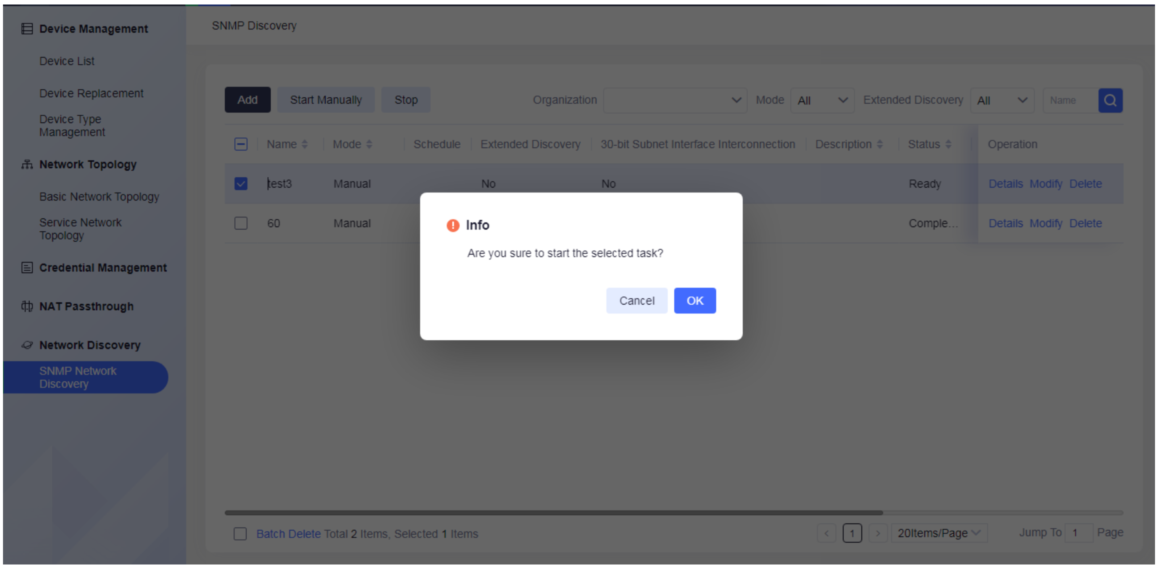
Figure 4.11631 Delete SNMP discovery task

Note

- The started task cannot be deleted.

Start/stop discovery task

Check the desired task information in the discovery task list (multiple choices are supported), and click the "Start manually" or "Stop" button to pop up the confirmation dialog box for starting (or stopping) discovery tasks, as shown in the following figure. Click "OK" to confirm starting/stopping the selected task information, or click "Cancel" to give up the start/stop operation.



☐	Name	Mode	Schedule	Extended Discovery	30-bit Subnet Interface Interconnection	Description	Status	Operation
☑	test3	Manual		No	No		Ready	Details Modify Delete
☐	60	Manual					Comple...	Details Modify Delete

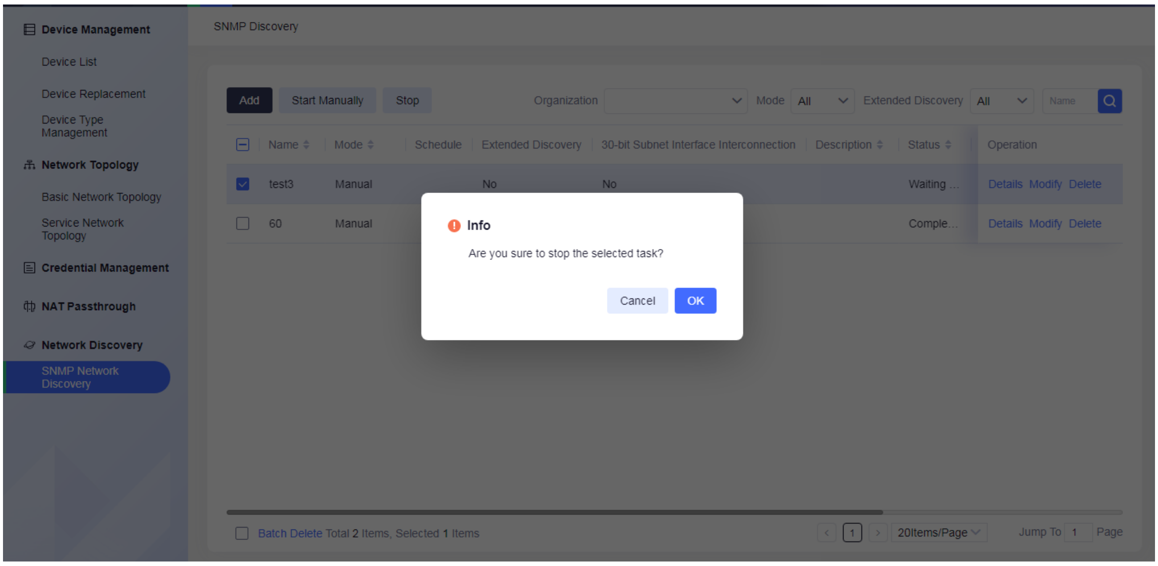
Info

Are you sure to start the selected task?

Cancel OK

Total 2 Items, Selected 1 Items

Figure 4.11732 Start SNMP discovery task



Are you sure to stop the selected task?

☑	Name	Mode	Schedule	Extended Discovery	30-bit Subnet Interface Interconnection	Description	Status	Operation
☑	test3	Manual		No	No		Waiting ...	Details Modify Delete
☐	60	Manual					Comple...	Details Modify Delete

Total 2 Items, Selected 1 Items

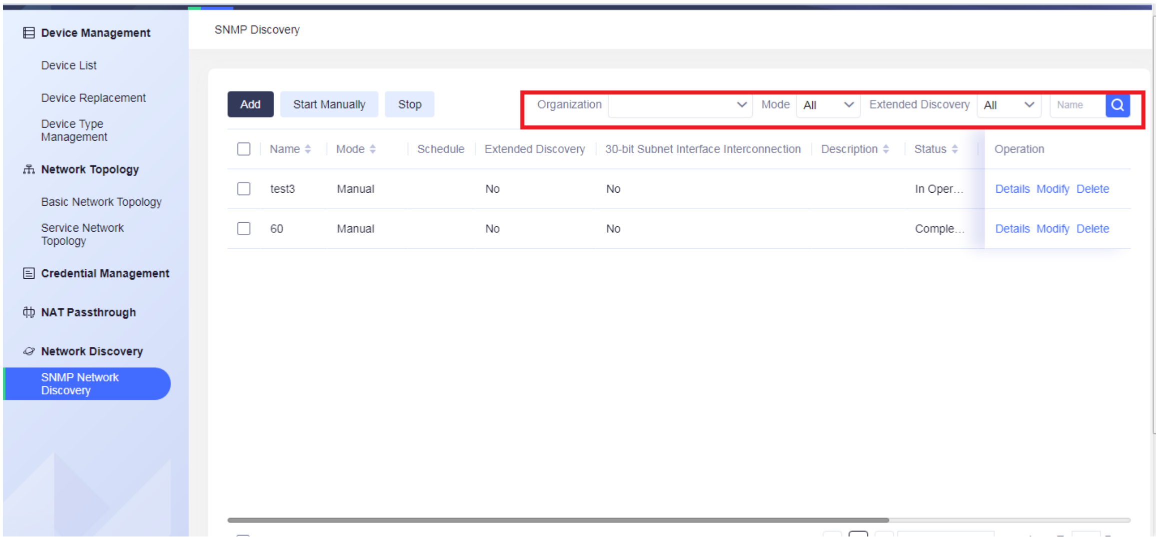
Figure 4.11833 Stop SNMP discovery task

Caution

- Started and stopped tasks cannot be modified and cannot be started or stopped repeatedly.

Query discovery task

Enter or select the task name, organization, execution method and whether to extend discovery in the task query panel and click the **Query** button to filter and query the network device discovery tasks. The filtered data is displayed in the task list below.



☐	Name	Mode	Schedule	Extended Discovery	30-bit Subnet Interface Interconnection	Description	Status	Operation
☐	test3	Manual		No	No		In Oper...	Details Modify Delete
☐	60	Manual		No	No		Comple...	Details Modify Delete

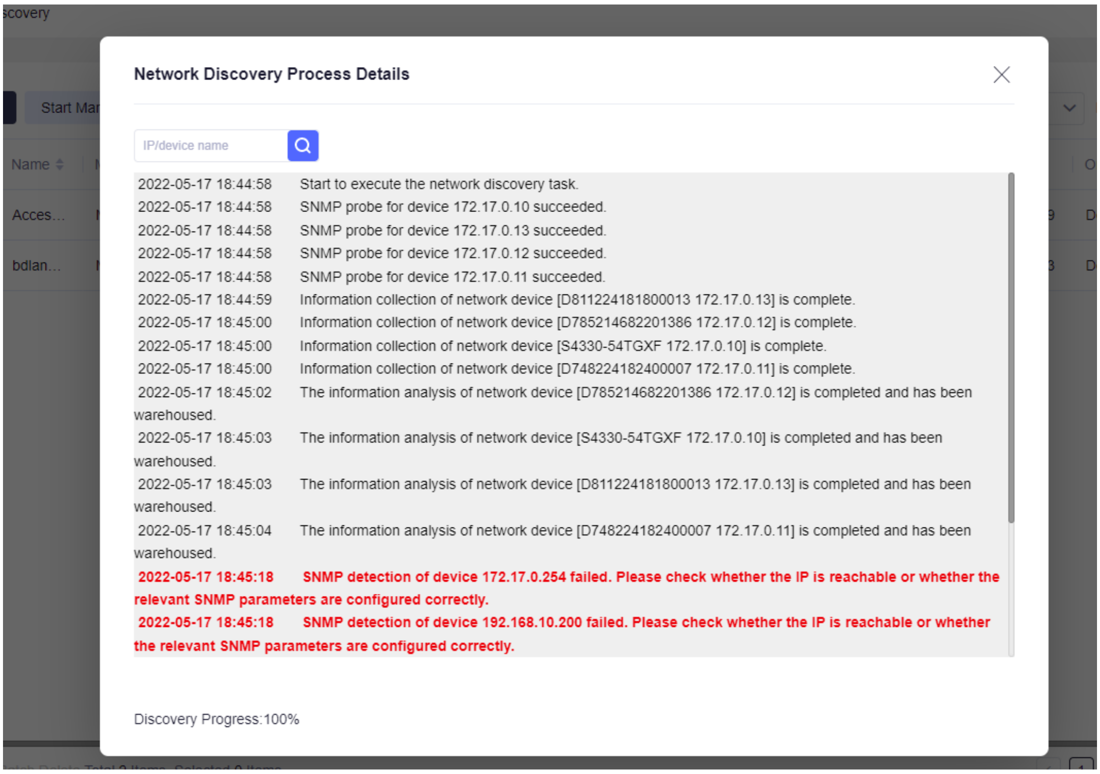
Figure 4.11934 SNMP task query

Caution

- The name supports fuzzy query.

Discovery task details

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



```
2022-05-17 18:44:58    Start to execute the network discovery task.
2022-05-17 18:44:58    SNMP probe for device 172.17.0.10 succeeded.
2022-05-17 18:44:58    SNMP probe for device 172.17.0.13 succeeded.
2022-05-17 18:44:58    SNMP probe for device 172.17.0.12 succeeded.
2022-05-17 18:44:58    SNMP probe for device 172.17.0.11 succeeded.
2022-05-17 18:44:59    Information collection of network device [D811224181800013 172.17.0.13] is complete.
2022-05-17 18:45:00    Information collection of network device [D785214682201386 172.17.0.12] is complete.
2022-05-17 18:45:00    Information collection of network device [S4330-54TGXF 172.17.0.10] is complete.
2022-05-17 18:45:00    Information collection of network device [D748224182400007 172.17.0.11] is complete.
2022-05-17 18:45:02    The information analysis of network device [D785214682201386 172.17.0.12] is completed and has been
warehoused.
2022-05-17 18:45:03    The information analysis of network device [S4330-54TGXF 172.17.0.10] is completed and has been
warehoused.
2022-05-17 18:45:03    The information analysis of network device [D811224181800013 172.17.0.13] is completed and has been
warehoused.
2022-05-17 18:45:04    The information analysis of network device [D748224182400007 172.17.0.11] is completed and has been
warehoused.
2022-05-17 18:45:18    SNMP detection of device 172.17.0.254 failed. Please check whether the IP is reachable or whether the
relevant SNMP parameters are configured correctly.
2022-05-17 18:45:18    SNMP detection of device 192.168.10.200 failed. Please check whether the IP is reachable or whether
the relevant SNMP parameters are configured correctly.
```

Discovery Progress:100%

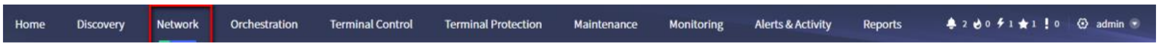
Figure 4.12035 SNMP network discovery details

Note

- After saving the task, the details of the last task will be cleared.

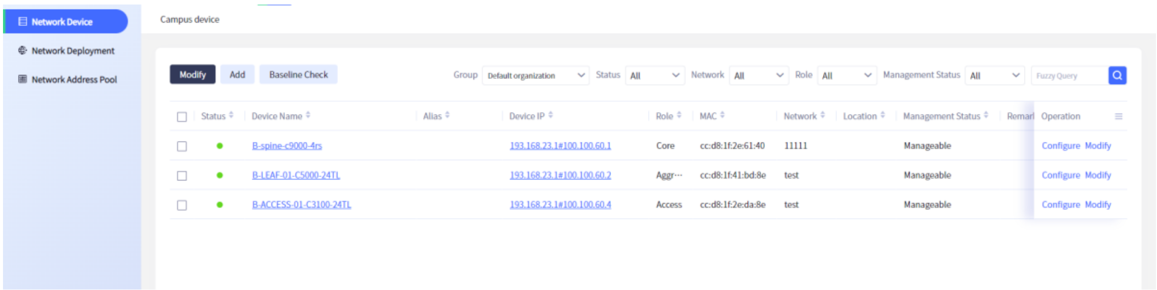
5 Campus Network

The top-level menu of the campus network module is as follows:



5.1 Campus Networks

The campus device management module provides management functions for all devices in the campus of the system, including configuration and modification of device ports. Click **Network** in the navigation bar above the system - > click **Network Device** on the left to open the **Campus device** interface, as shown in Figure 5.1 Campus Device:

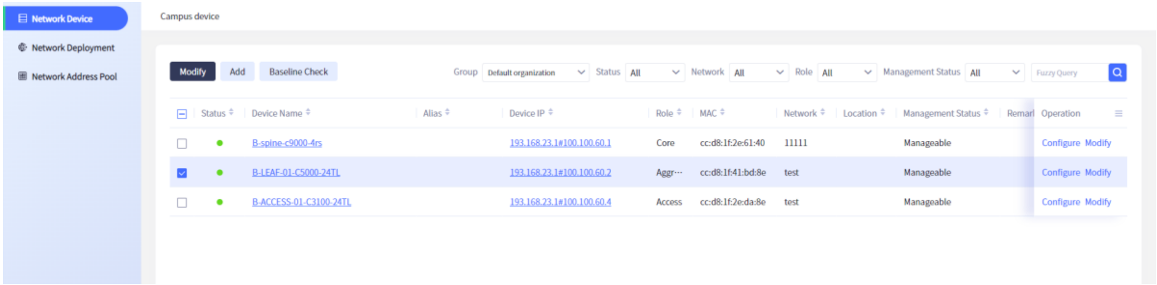


☐	Status	Device Name	Alias	Device IP	Role	MAC	Network	Location	Management Status	Remarl	Operation
☐	●	B-spine-c9000-4rs		193.168.23.1#100.100.60.1	Core	cc:d8:1f:2e:61:40	11111		Manageable		Configure Modify
☐	●	B-LEAF-01-C5000-24TL		193.168.23.1#100.100.60.2	Aggr···	cc:d8:1f:41:bd:8e	test		Manageable		Configure Modify
☐	●	B-ACCESS-01-C3100-24TL		193.168.23.1#100.100.60.4	Access	cc:d8:1f:2e:da:8e	test		Manageable		Configure Modify

Figure 5.1 Campus device

5.1.1 Campus Device List

The **Campus device** page displays all the devices in the campus by default, displaying the status, name, alias, device IP, device role, device MAC, campus, location, management status, remarks and other information of each device separately, as shown in Figure 5.1.1 Campus device list:

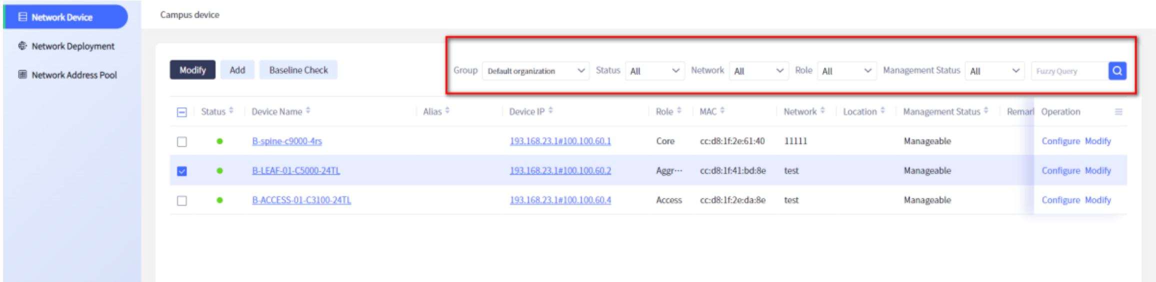


☐	Status	Device Name	Alias	Device IP	Role	MAC	Network	Location	Management Status	Remarl	Operation
☐	●	B-spine-c9000-4rs		193.168.23.1#100.100.60.1	Core	cc:d8:1f:2e:61:40	11111		Manageable		Configure Modify
☑	●	B-LEAF-01-C5000-24TL		193.168.23.1#100.100.60.2	Aggr···	cc:d8:1f:41:bd:8e	test		Manageable		Configure Modify
☐	●	B-ACCESS-01-C3100-24TL		193.168.23.1#100.100.60.4	Access	cc:d8:1f:2e:da:8e	test		Manageable		Configure Modify

Figure 5.1.1 Campus device list

5.1.2 Campus Device Query

The campus devices provide the function of querying by conditions, which can easily and quickly query the specific campus device information. Enter the corresponding query criteria in the query panel, and then click the **Query** button to display the qualified campus devices. The available query criteria include device group, device status, campus, device role, management status and keyword search, as shown in figure 5.1.2.1 Campus device query:

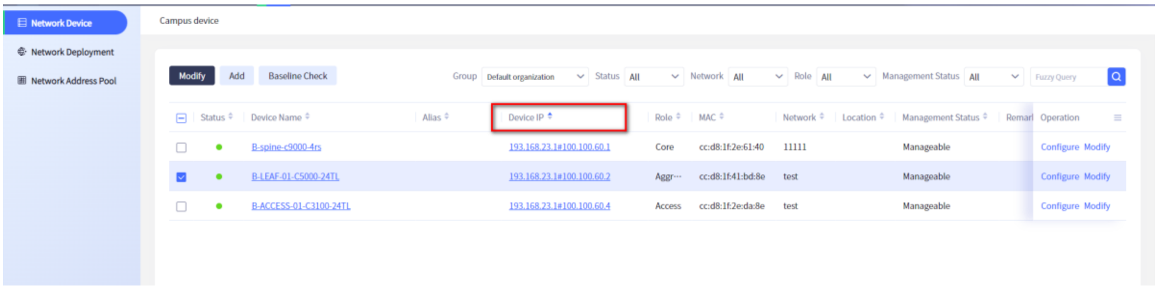


Group: Default organization; Status: All; Network: All; Role: All; Management Status: All; Fuzzy Query

☐	Status	Device Name	Alias	Device IP	Role	MAC	Network	Location	Management Status	Remark	Operation
☐	●	B-spine-c9000-4rs		193.168.23.1#100.100.60.1	Core	cc:d8:1f:2e:61:40	11111		Manageable		Configure Modify
☑	●	B-LEAF-01-C5000-24TL		193.168.23.1#100.100.60.2	Aggr···	cc:d8:1f:41:bd:8e	test		Manageable		Configure Modify
☐	●	B-ACCESS-01-C3100-24TL		193.168.23.1#100.100.60.4	Access	cc:d8:1f:2e:da:8e	test		Manageable		Configure Modify

Figure 5.1.2.1 Campus device query

Click the triangle symbol on the header of the device list to sort the devices according to the corresponding fields, as shown in figure 5.1.2.2 Campus device sorting. Click the sorting ID next to the device IP to sort the devices in ascending order according to the device IPs.



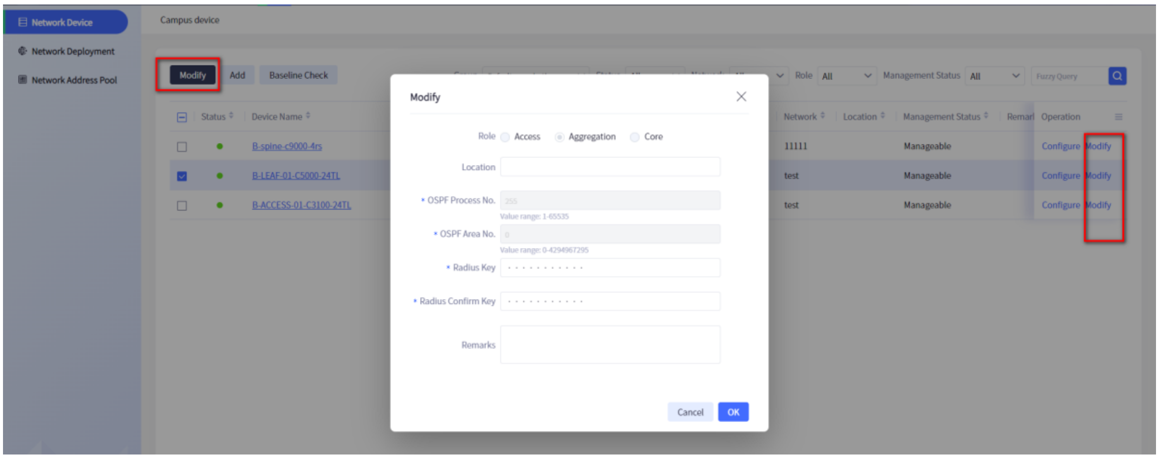
Group: Default organization; Status: All; Network: All; Role: All; Management Status: All; Fuzzy Query

☐	Status	Device Name	Alias	Device IP	Role	MAC	Network	Location	Management Status	Remark	Operation
☐	●	B-spine-c9000-4rs		193.168.23.1#100.100.60.1	Core	cc:d8:1f:2e:61:40	11111		Manageable		Configure Modify
☑	●	B-LEAF-01-C5000-24TL		193.168.23.1#100.100.60.2	Aggr···	cc:d8:1f:41:bd:8e	test		Manageable		Configure Modify
☐	●	B-ACCESS-01-C3100-24TL		193.168.23.1#100.100.60.4	Access	cc:d8:1f:2e:da:8e	test		Manageable		Configure Modify

Figure 5.1.2.2 Campus device sorting

5.1.3 Modify Campus Device

In the campus device interface, click **Modify** to enter the **Modify** interface. The modification function at the rightmost part of the information corresponding to each device is to modify a single device, as shown in figure 5.1.3 Modify campus device. You can modify the role, location, OSPF process number, OSPF area number, radius key, remarks, etc. of the device. Click **OK** to modify the device information successfully.



Modify

Role ○ Access ● Aggregation ○ Core

Location

* OSPF Process No. 255
Value range: 1-65535

* OSPF Area No. 0
Value range: 0-4294967295

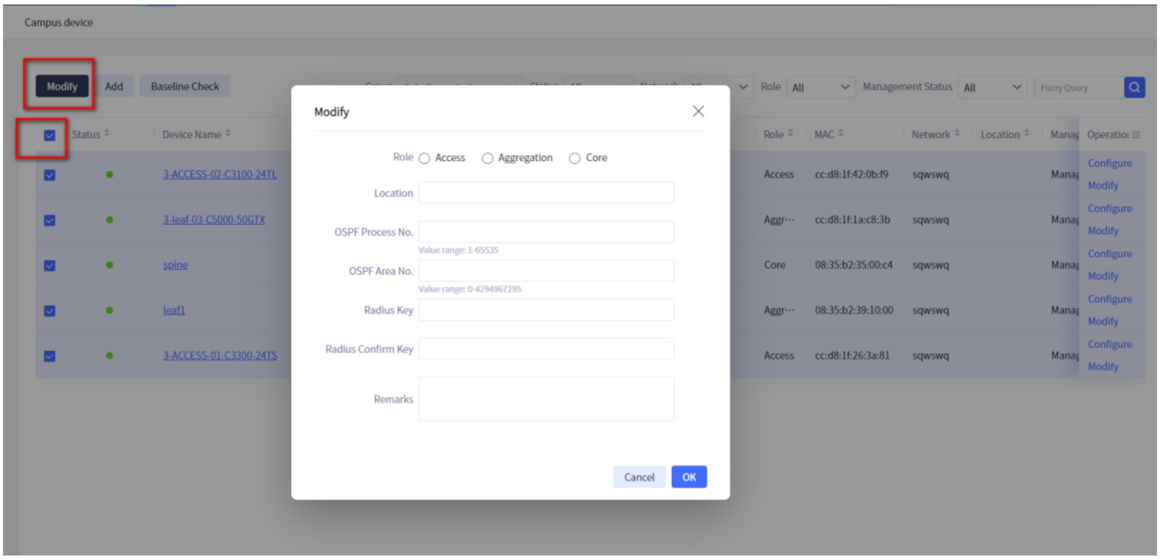
* Radius Key ············

* Radius Confirm Key ············

Remarks

Figure 5.1.3 Modify campus device

Click **Modify** above the device to perform batch modification. After the **Modify** box pops up, you can modify the device as required, as shown in the following figure:



Modify

Role ○ Access ○ Aggregation ○ Core

Location

OSPF Process No.

Value range: 1-65535

OSPF Area No.

Value range: 0-4294967295

Radius Key

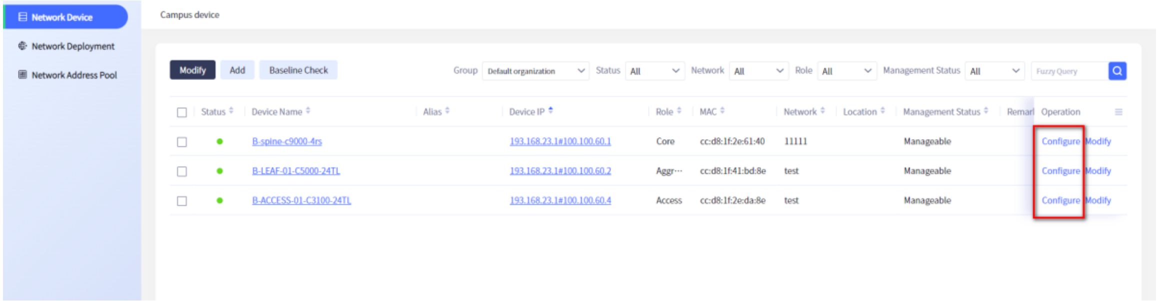
Radius Confirm Key

Remarks

☑	Status	Device Name	Role	MAC	Network	Location	Manag	Operation
☑	●	3-ACCESS-02-C3100-24TL	Access	cc:d8:1f:42:0b:f9	sqwswq		Manag	Configure Modify
☑	●	3-leaf-03-C5000-50GTX	Aggr···	cc:d8:1f:1a:c8:3b	sqwswq		Manag	Configure Modify
☑	●	spine	Core	08:35:b2:35:00:c4	sqwswq		Manag	Configure Modify
☑	●	leaf1	Aggr···	08:35:b2:39:10:00	sqwswq		Manag	Configure Modify
☑	●	3-ACCESS-01-C3300-24TS	Access	cc:d8:1f:26:3a:81	sqwswq		Manag	Configure Modify

5.1.4 Campus Device Configuration

For the devices in the deployed plan network, click **Configure** on the right of the device information to enter the device configuration interface, as shown in figure 5.1.4.1 Campus device configuration.

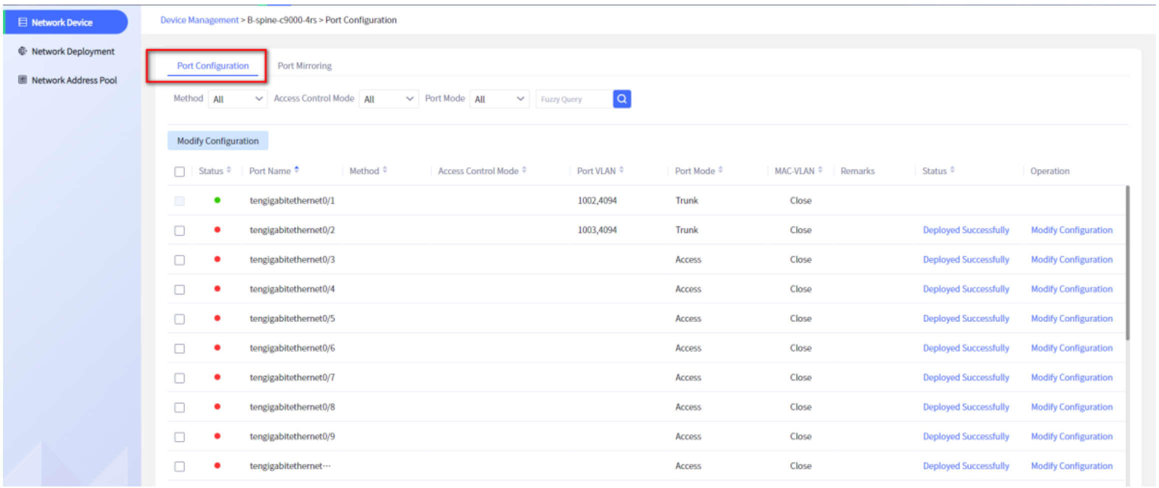


Group Default organization Status All Network All Role All Management Status All

☐	Status	Device Name	Alias	Device IP	Role	MAC	Network	Location	Management Status	Remarl	Operation
☐	●	B-spine-c9000-4rs		193.168.23.1#100.100.60.1	Core	cc:d8:1f:2e:61:40	11111		Manageable		Configure Modify
☐	●	B-LEAF-01-C5000-24TL		193.168.23.1#100.100.60.2	Aggr···	cc:d8:1f:41:bd:8e	test		Manageable		Configure Modify
☐	●	B-ACCESS-01-C3100-24TL		193.168.23.1#100.100.60.4	Access	cc:d8:1f:2e:da:8e	test		Manageable		Configure Modify

Figure 5.1.4.1 Campus device configuration

After entering the device configuration page, you can set the device port configuration and port mirroring, as shown in figure 5.1.4.2 Campus device configuration:



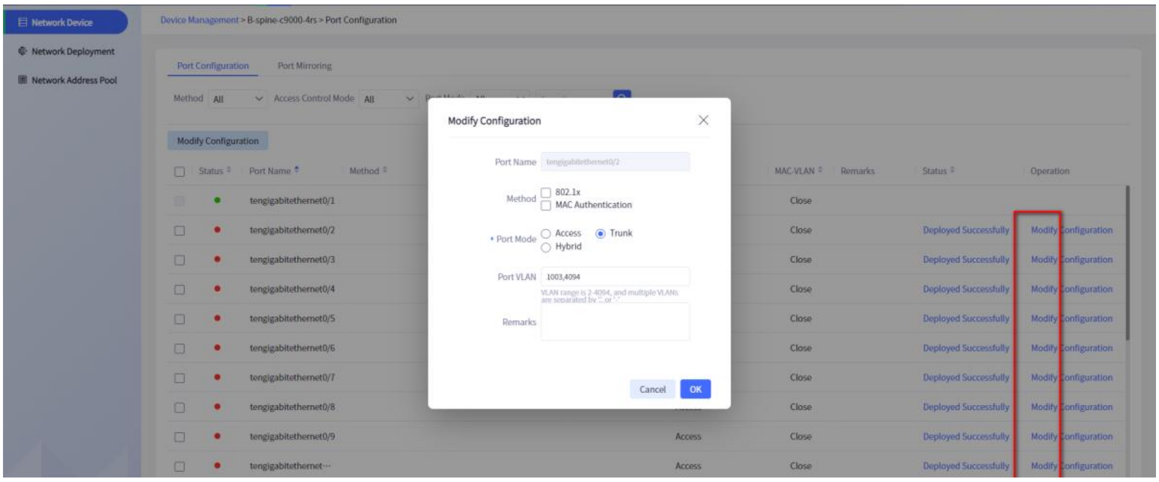
Device Management > B-spine-c9000-4rs > Port Configuration

Method All Access Control Mode All Port Mode All

☐	Status	Port Name	Method	Access Control Mode	Port VLAN	Port Mode	MAC-VLAN	Remarks	Status	Operation
☐	●	tengigabitethernet0/1			1002,4094	Trunk	Close			
☐	●	tengigabitethernet0/2			1003,4094	Trunk	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/3				Access	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/4				Access	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/5				Access	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/6				Access	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/7				Access	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/8				Access	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/9				Access	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet···				Access	Close		Deployed Successfully	Modify Configuration

Figure 5.1.4.2 Campus device configuration

Select a device and click **Modify** to open the box for modifying device configuration, where you can modify the name, authentication mode, port mode, port VLAN, remarks and other information of the device port, and click **OK** to successfully modify it, as shown in figure 5.1.4.3:



Modify Configuration

Port Name: tengigabitethernet0/2

Method: ☐ 802.1x ☐ MAC Authentication

* Port Mode: ○ Access ● Trunk ○ Hybrid

Port VLAN: 1003,4094

VLAN range is 2-4094, and multiple VLANs are separated by "," or "-"

Remarks:

☐	Status	Port Name	Method		MAC-VLAN	Remarks	Status	Operation
☐	●	tengigabitethernet0/1			Close			
☐	●	tengigabitethernet0/2			Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/3			Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/4			Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/5			Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/6			Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/7			Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/8			Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet0/9		Access	Close		Deployed Successfully	Modify Configuration
☐	●	tengigabitethernet···		Access	Close		Deployed Successfully	Modify Configuration

Figure 5.1.4.3 Campus port configuration

On the port configuration page, click the **Port Mirroring** button at the top to add the mirroring source, mirror destination, and remarks in the pop-up box. Click **OK** to successfully add the port image. After adding, you can choose to deploy the added port mirror. Click **Deploy**, as shown in figure 5.1.4.4.

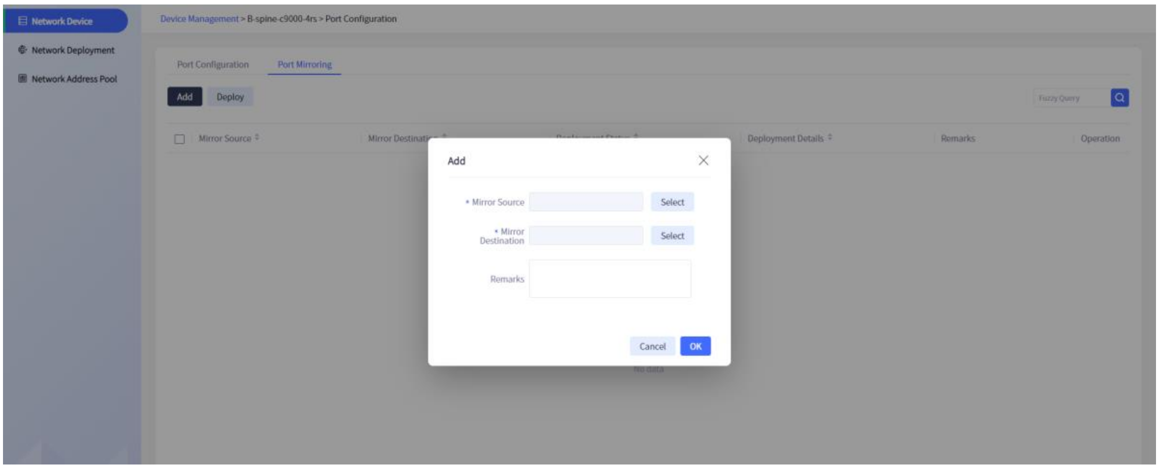
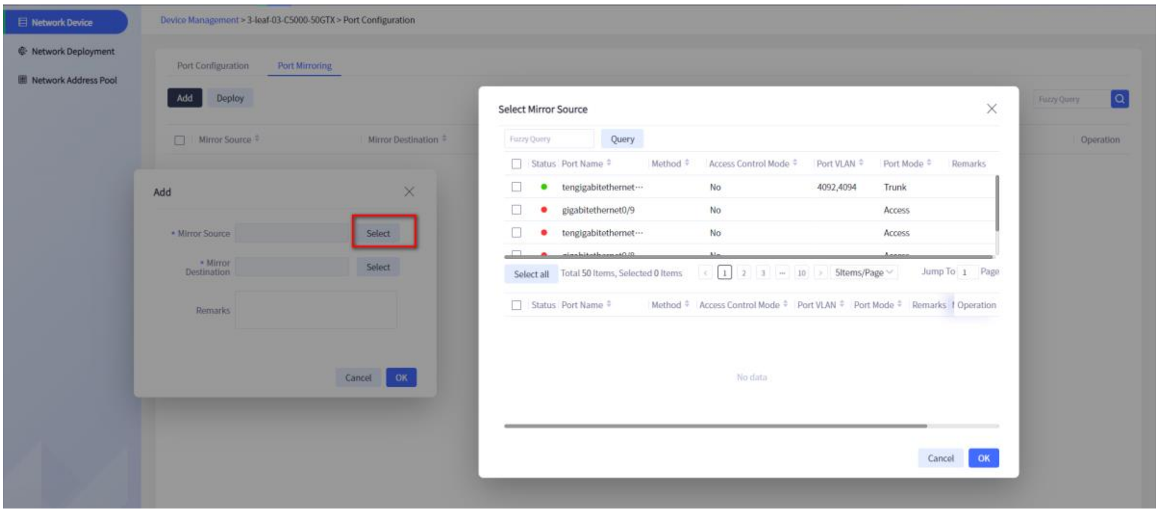


Figure 5.1.4.4 Campus port mirroring

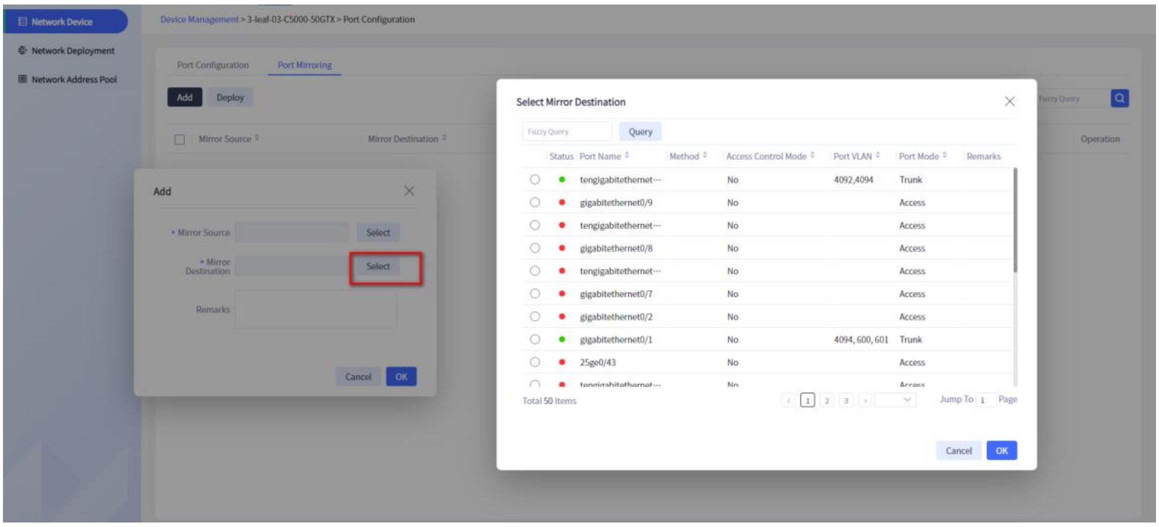
Click the **Add** button, and then click **Select** to select the mirror source or destination, as shown in the following figure:



☐	Status	Port Name	Method	Access Control Mode	Port VLAN	Port Mode	Remarks
☐	●	tengigabitethernet···		No	4092,4094	Trunk	
☐	●	gigabitethernet0/9		No		Access	
☐	●	tengigabitethernet···		No		Access	

Total 50 Items, Selected 0 Items

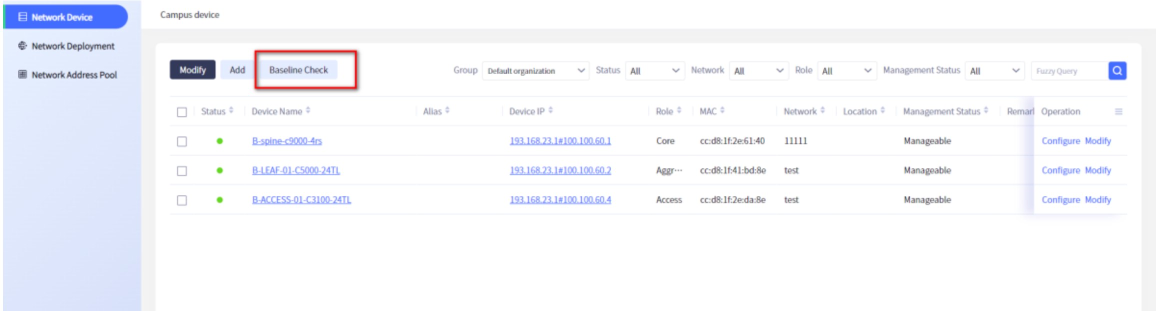
☐	Status	Port Name	Method	Access Control Mode	Port VLAN	Port Mode	Remarks	Operation



	Status	Port Name	Method	Access Control Mode	Port VLAN	Port Mode	Remarks
○	●	tengigabitethernet···		No	4092,4094	Trunk	
○	●	gigabitethernet0/9		No		Access	
○	●	tengigabitethernet···		No		Access	
○	●	gigabitethernet0/8		No		Access	
○	●	tengigabitethernet···		No		Access	
○	●	gigabitethernet0/7		No		Access	
○	●	gigabitethernet0/2		No		Access	
○	●	gigabitethernet0/1		No	4094, 600, 601	Trunk	
○	●	25ge0/43		No		Access	
○	●	tengigabitethernet···		No		Access	

5.1.5 Campus Device Reconciliation

Click to enter the campus device interface. You can distribute the configuration reconciliation function for the device that has been added and deployed to the campus. Select the qualified device and click the **Baseline Check** button as shown in Figure 5.1.5 to perform reconciliation.



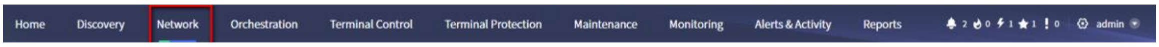
☐	Status	Device Name	Alias	Device IP	Role	MAC	Network	Location	Management Status	Remarl	Operation
☐	●	B-spine-c9000-4rs		193.168.23.1#100.100.60.1	Core	cc:d8:1f:2e:61:40	11111		Manageable		Configure Modify
☐	●	B-LEAF-01-C5000-24TL		193.168.23.1#100.100.60.2	Aggr···	cc:d8:1f:41:bd:8e	test		Manageable		Configure Modify
☐	●	B-ACCESS-01-C3100-24TL		193.168.23.1#100.100.60.4	Access	cc:d8:1f:2e:da:8e	test		Manageable		Configure Modify

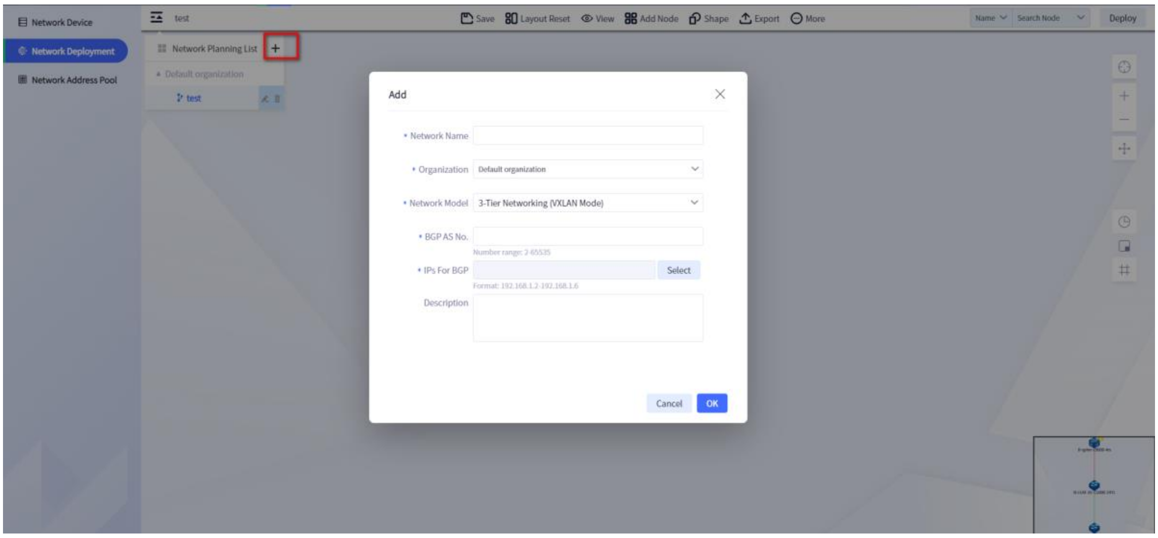
Figure 5.1.5 Campus device reconciliation

5.2 Campus Network

5.2.1 Campus Network Management

The campus network management is displayed in the form of topology view. Click the top on the left to display the view list, click the **Add** button, and enter the required contents: network name, organization, network model, BGP AS NO., IPs for BGP, and optional description, as shown in Figure 5.2.1:





- Network Name
- Organization: Default organization
- Network Model: 3-Tier Networking (VXLAN Mode)
- BGP AS No.
  Number range: 2-65535
- IPs For BGP
  Format: 192.168.1.2-192.168.1.6

Description

Figure 5.2.1 Campus network management

5.2.2 Add Devices for Campus Network

The topology view page displays the topology view of the corresponding campus network list. Click **Add Node** in the middle of the top, as shown in the figure; You can choose to add access, aggregation or core devices. Users can place the device location as desired. The topology view will automatically save the device location, as shown in figure 5.2.2.1;

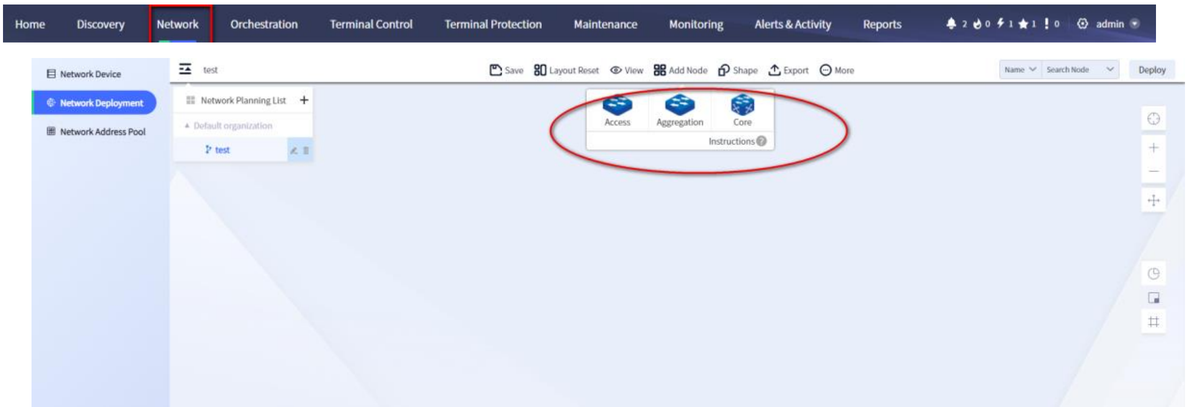
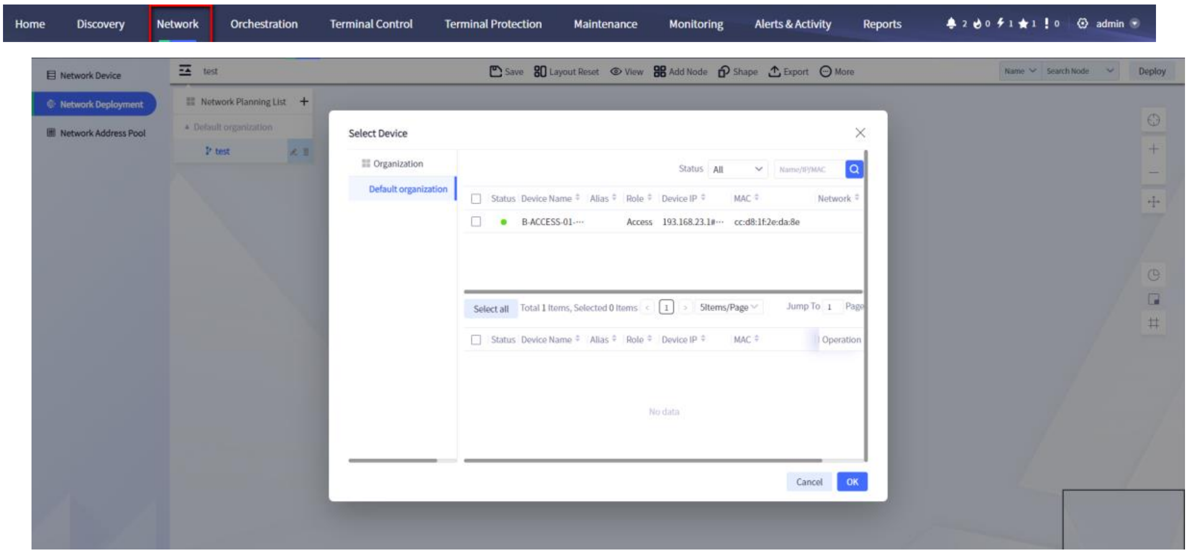


Figure 5.2.2.1 Add nodes for campus network



☐	Status	Device Name	Alias	Role	Device IP	MAC	Network
☐	●	B-ACCESS-01-···		Access	193.168.23.1#···	cc:d8:1f:2e:da:8e	

Select all Total 1 Items, Selected 0 Items 1 5Items/Page Jump To 1 Page

☐	Status	Device Name	Alias	Role	Device IP	MAC	Operation

No data

Figure 5.2.2.2 Add devices for campus network

After adding, the un-deployed status is as follows:

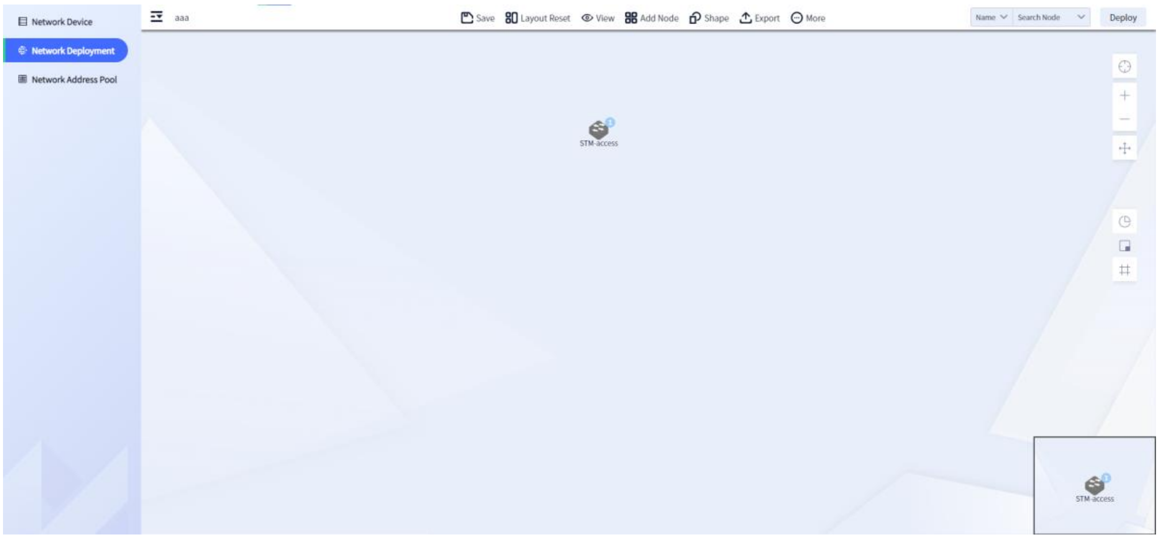
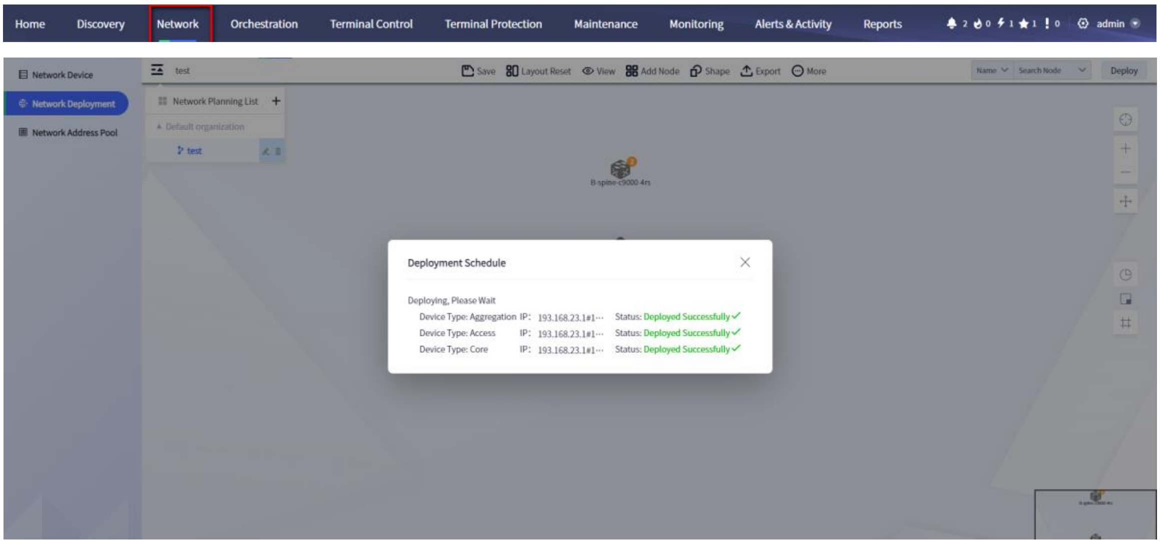


Figure 5.2.2.3 Add devices for the campus network

Click **Deploy** to pop up the **Deployment Schedule** dialog box, displaying the device type, IP, and status, as shown in Figure 5.2.2.4:



Deployment Schedule

Deploying, Please Wait

Device Type: Aggregation IP: 193.168.23.1#1··· Status: Deployed Successfully ✓
Device Type: Access IP: 193.168.23.1#1··· Status: Deployed Successfully ✓
Device Type: Core IP: 193.168.23.1#1··· Status: Deployed Successfully ✓

Figure 5.2.2.4 Deploy devices for the campus network

Note

- Users can add or reduce devices according to their needs. If they have been deployed before, they do not need to deploy again. The system will deploy automatically when adding or reducing devices (except that the uplink devices of the access device are not in the planned network).

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

You can manually add or remove devices and edit links in this topology view. In addition, you can also perform the topology view background setting, font color setting, and other operations, as shown in figure 5.2.2.4:

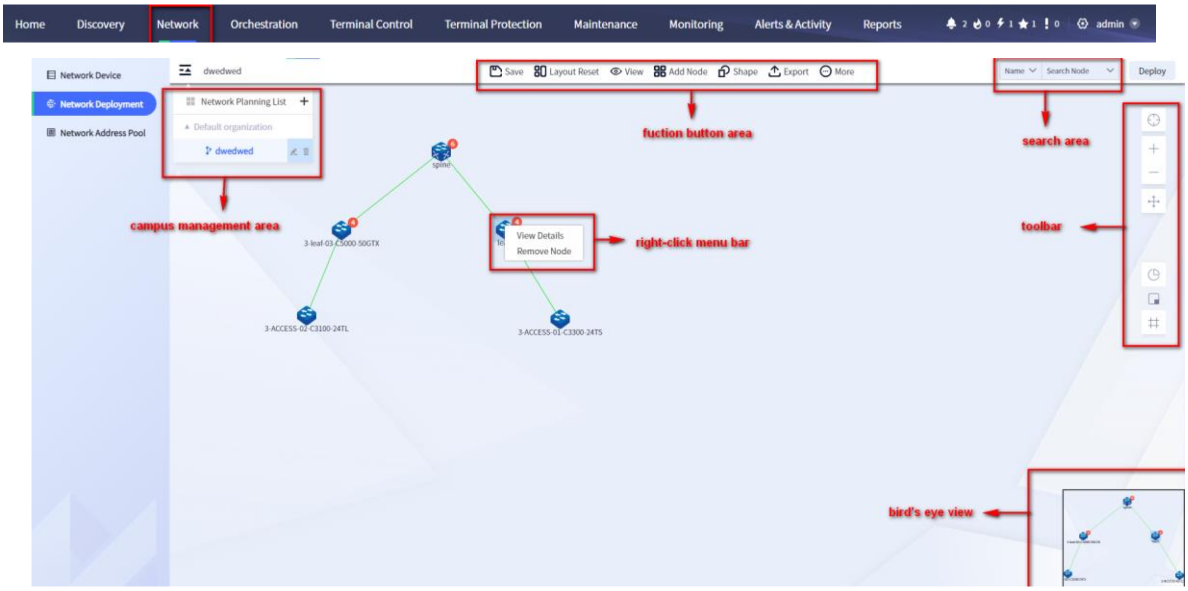


Figure 5.2.2.4 Deploy devices for the campus network

5.2.3 Function Button Area

Save : Save the layout, display information, editing results, etc. of the current topology.

Layout Reset : Reset the topology layout

View : Select the device display information in the topology view (the number of links, alarms, device name (displayed by default), device IP, and device MAC)

Add Node : Add NEs (aggregation devices and core devices) to the topology view, and you can add devices to the current view. When multiple devices are selected, they are arranged in a circle centered on the drag and drop position.

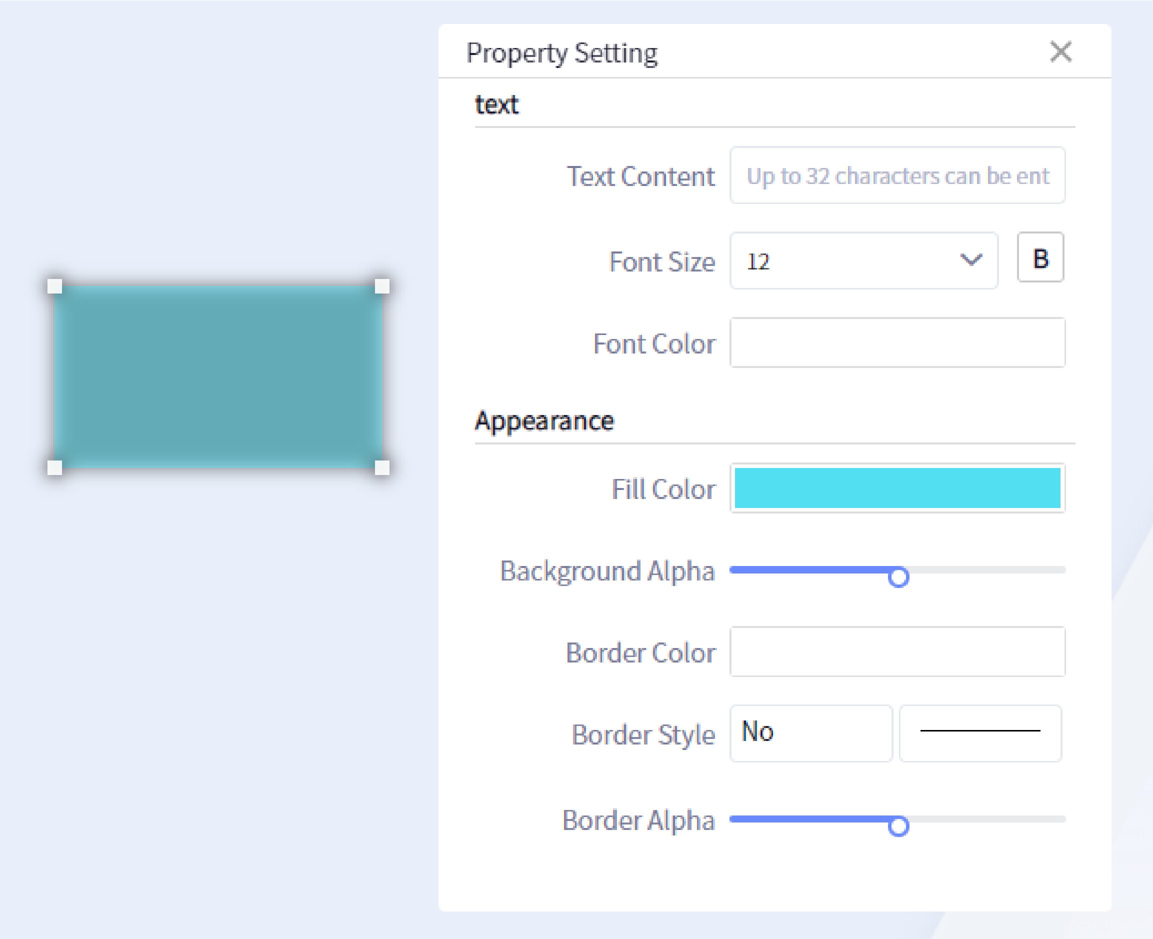
Shape :Add shapes to the topology view (basic shapes, text editing, collections, support dragging the size).

Basic shape (common background, supporting setting of text and appearance, see the following figure for details)

▭ : Press and drag to the topology view to add a right angle rectangular background at the drag and drop position.

▢: Hold and drag to the topology view, and you can add a rounded rectangular background to the drag and drop position.

⬭: Hold and drag to the topology view, and you can add an ellipse background to the drag and drop position.


Property Setting

text

Text Content: Up to 32 characters can be ent

Font Size: 12

Font Color:

Appearance

Fill Color:

Background Alpha:

Border Color:

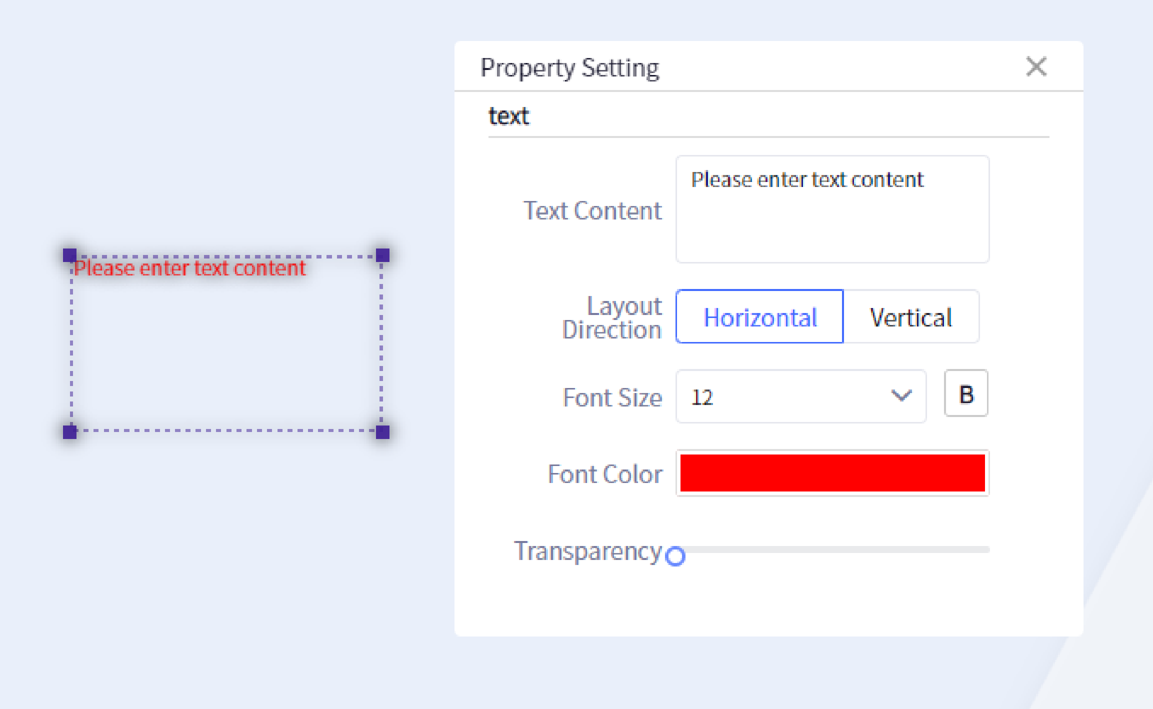
Border Style: No

Border Alpha:

Figure 5.2.3.1 Basic shape attribute setting

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

: Press and drag to the topology view, and you can add a text box in the drag and drop position.


Property Setting

text

Text Content: Please enter text content

Layout Direction: Horizontal

Font Size: 12

Font Color:

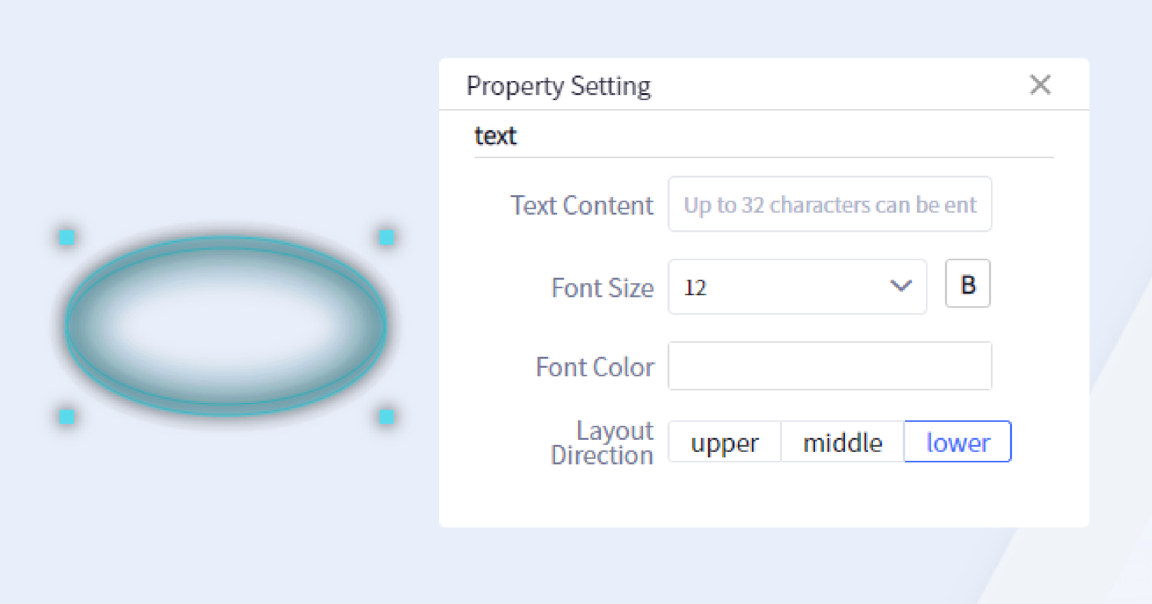
Transparency:

Figure 5.2.3.2 Text attribute edit setting

Collection (collection container, you can add/remove device nodes from the collection by dragging and dropping, and support text setting, as shown in the figure below)

⬭: Press and drag to the topology view, and you can add an ellipse collection at the drag and drop position.

▭: Press and drag to the topology view, ad you can add a rectangular collection at the drag and drop location.



Property Setting

text

Text Content: Up to 32 characters can be ent

Font Size: 12

Font Color:

Layout Direction: upper middle lower

Figure 5.2.3.3 Collection attribute setting

Export : Export the topology in picture format.

More : Other function options (background setting, font color setting, legend description, deployment details, deployment result).

- Background setting

The system has three built-in background styles, and supports uploading new background styles through "Upload Materials"; You can click the mouse to select the background style, preview the background style through the "Preview" button, and save the replacement of the background style through the "Use" button, as shown in Figure 5.2.3.4.

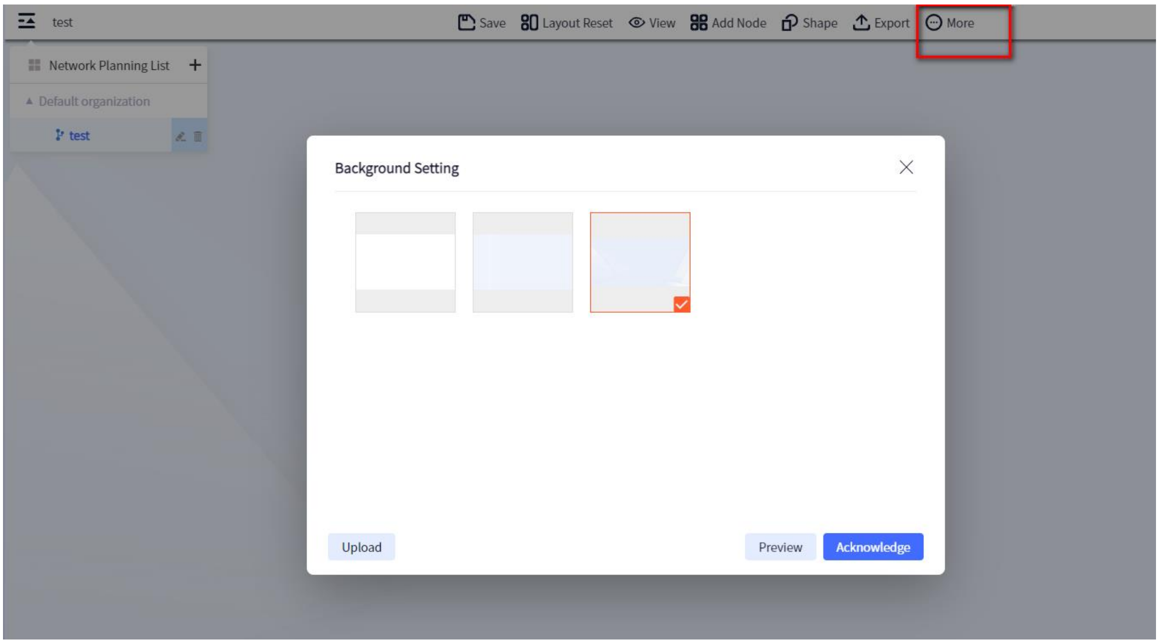


Figure 5.2.3.4 Background setting

- Font color settings

Set the font color in the topology view, and 72 colors are available, as shown in Figure 5.2.3.5.

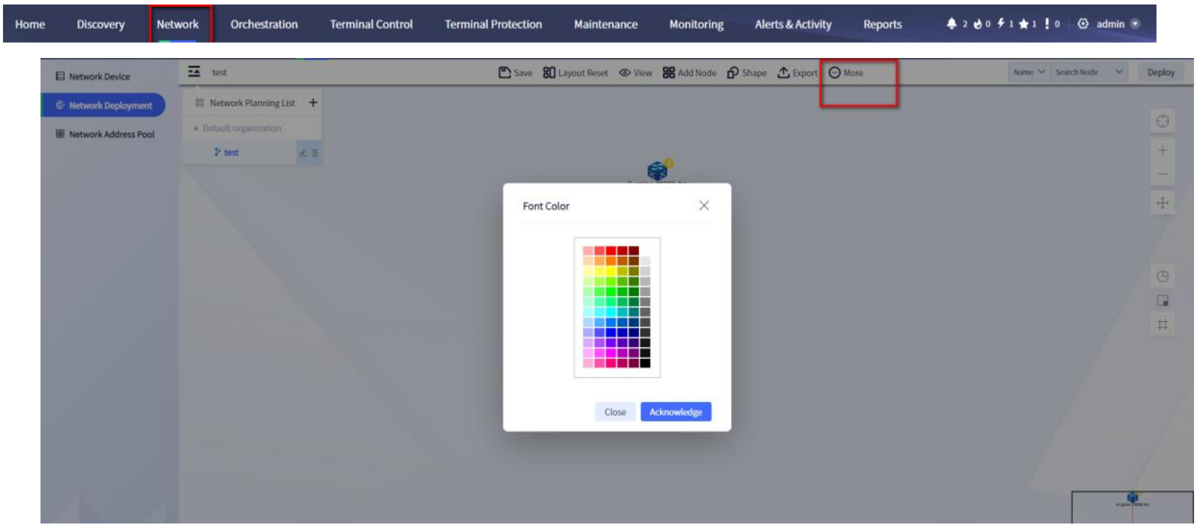


Figure 5.2.3.5 Front color settings

- Legend illustration

Click "Legend Illustration" in the "More" icon to view the legend description of the topology view, as shown in Figure 5.2.3.6.

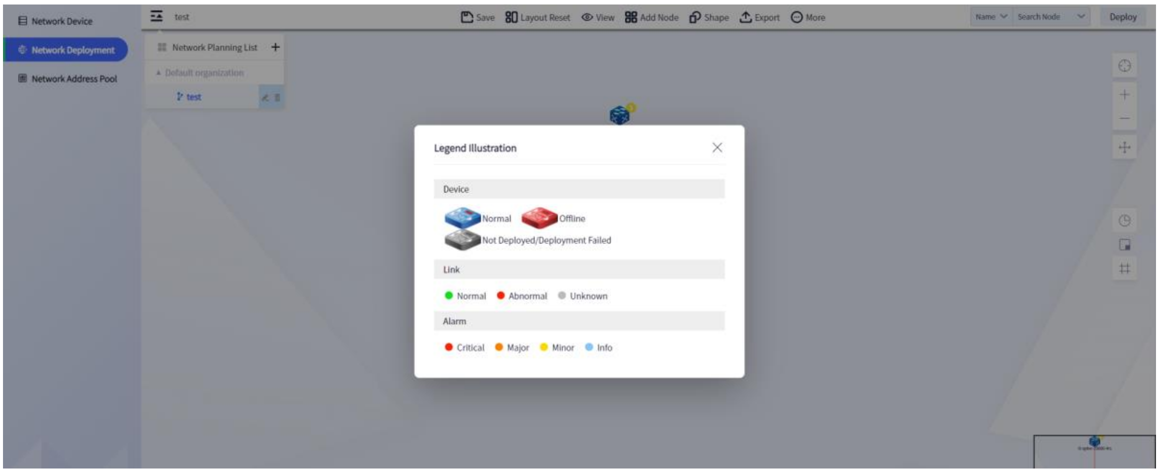
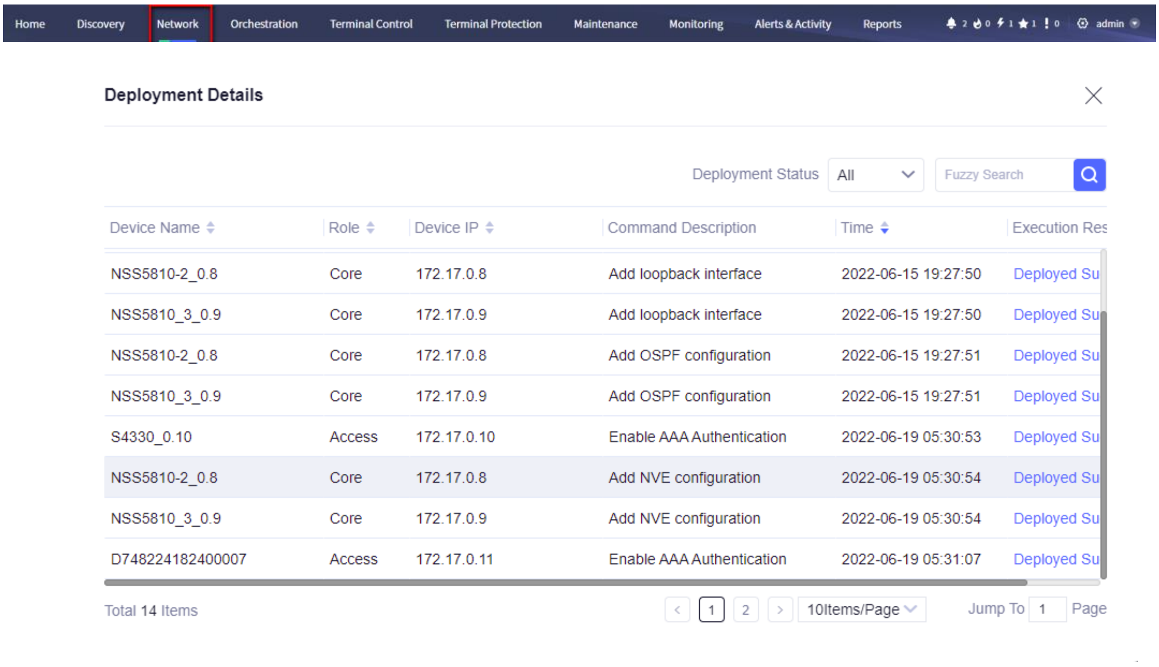


Figure 5.2.3. 6Legend description

- Deployment details

Click **Deployment Details** in the "**More**" icon to pop up the "Deployment details" list. The list displays the device name, device role, device IP, command description, time and execution results, and supports full-text fuzzy query, as shown in figure 5.2.3.7 below; Click the execution result corresponding to each device to view the detailed description of its execution result, as shown in Figure 5.2.3.8 below;



Deployment Details

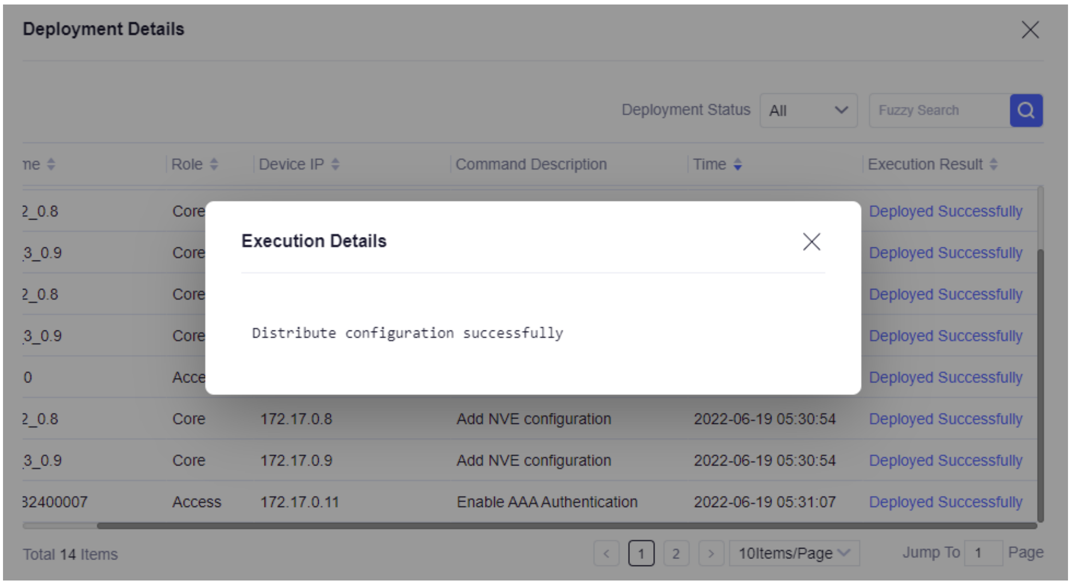
Deployment Status All

Fuzzy Search

Device Name	Role	Device IP	Command Description	Time	Execution Res
NSS5810-2_0.8	Core	172.17.0.8	Add loopback interface	2022-06-15 19:27:50	Deployed Su
NSS5810_3_0.9	Core	172.17.0.9	Add loopback interface	2022-06-15 19:27:50	Deployed Su
NSS5810-2_0.8	Core	172.17.0.8	Add OSPF configuration	2022-06-15 19:27:51	Deployed Su
NSS5810_3_0.9	Core	172.17.0.9	Add OSPF configuration	2022-06-15 19:27:51	Deployed Su
S4330_0.10	Access	172.17.0.10	Enable AAA Authentication	2022-06-19 05:30:53	Deployed Su
NSS5810-2_0.8	Core	172.17.0.8	Add NVE configuration	2022-06-19 05:30:54	Deployed Su
NSS5810_3_0.9	Core	172.17.0.9	Add NVE configuration	2022-06-19 05:30:54	Deployed Su
D748224182400007	Access	172.17.0.11	Enable AAA Authentication	2022-06-19 05:31:07	Deployed Su

Total 14 Items 1 2 10Items/Page Jump To 1 Page

Figure 5.2.3.7 Deployment details



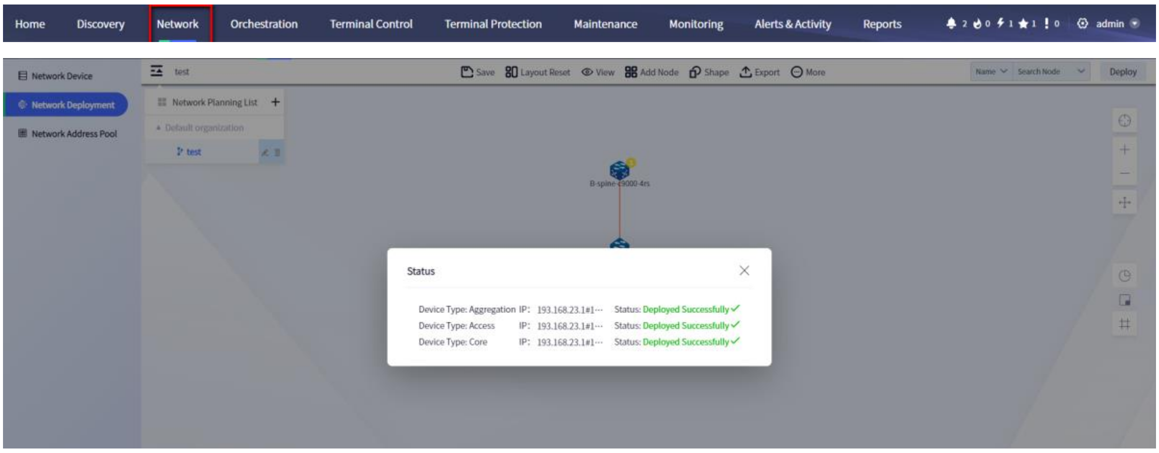
Distribute configuration successfully

ne	Role	Device IP	Command Description	Time	Execution Result
2_0.8	Core				Deployed Successfully
3_0.9	Core				Deployed Successfully
2_0.8	Core				Deployed Successfully
3_0.9	Core				Deployed Successfully
0	Acce				Deployed Successfully
2_0.8	Core	172.17.0.8	Add NVE configuration	2022-06-19 05:30:54	Deployed Successfully
3_0.9	Core	172.17.0.9	Add NVE configuration	2022-06-19 05:30:54	Deployed Successfully
32400007	Access	172.17.0.11	Enable AAA Authentication	2022-06-19 05:31:07	Deployed Successfully

Figure 5.2.3.8 Deployment execution details

- Deployment result

Click **Status**, displaying the device type, IP, and status, as shown in Figure 5.2.3.9:



Device Type: Aggregation IP: 193.168.23.1#1··· Status: Deployed Successfully ✓
Device Type: Access IP: 193.168.23.1#1··· Status: Deployed Successfully ✓
Device Type: Core IP: 193.168.23.1#1··· Status: Deployed Successfully ✓

Figure 5.2.3.9 Deployment result

5.2.4 Search Area

Within the current topology view, you can query the devices according to device name, IP, MAC, core, aggregation, and access, as shown in the figure:

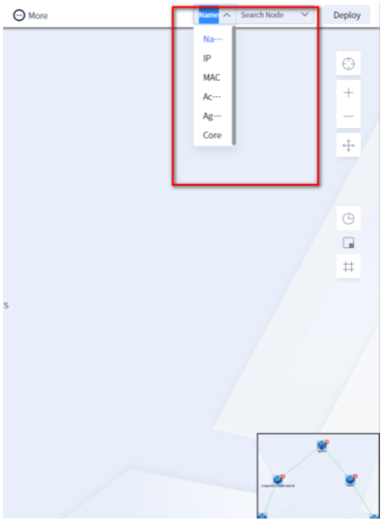


Figure 5.2.4 Campus search area

5.2.5 Tools Bar

⌖ : Click to move the campus topology to the central location

+ : Zoom in the topology

— : Zoom out the topology

✥ : Topology anchor, mouse drag and drop topology switch

◷ : Display the topology statistics, and click to pop up the statistics window, as shown in Figure 5.2.5

◲ : Turn on/off aerial view

# : Open/close the grid interface

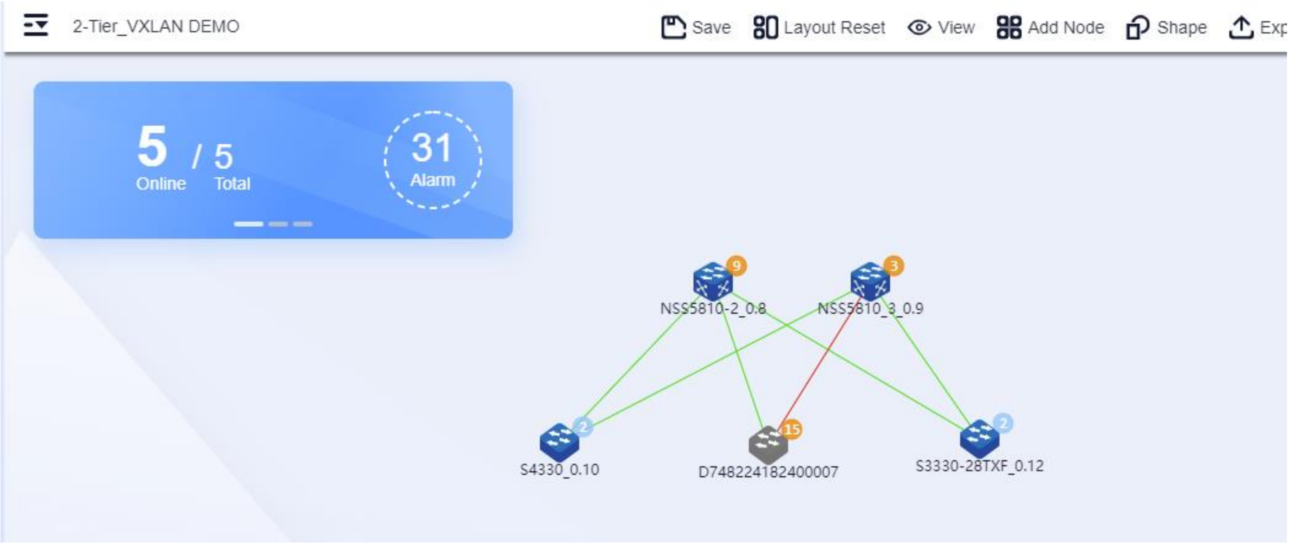
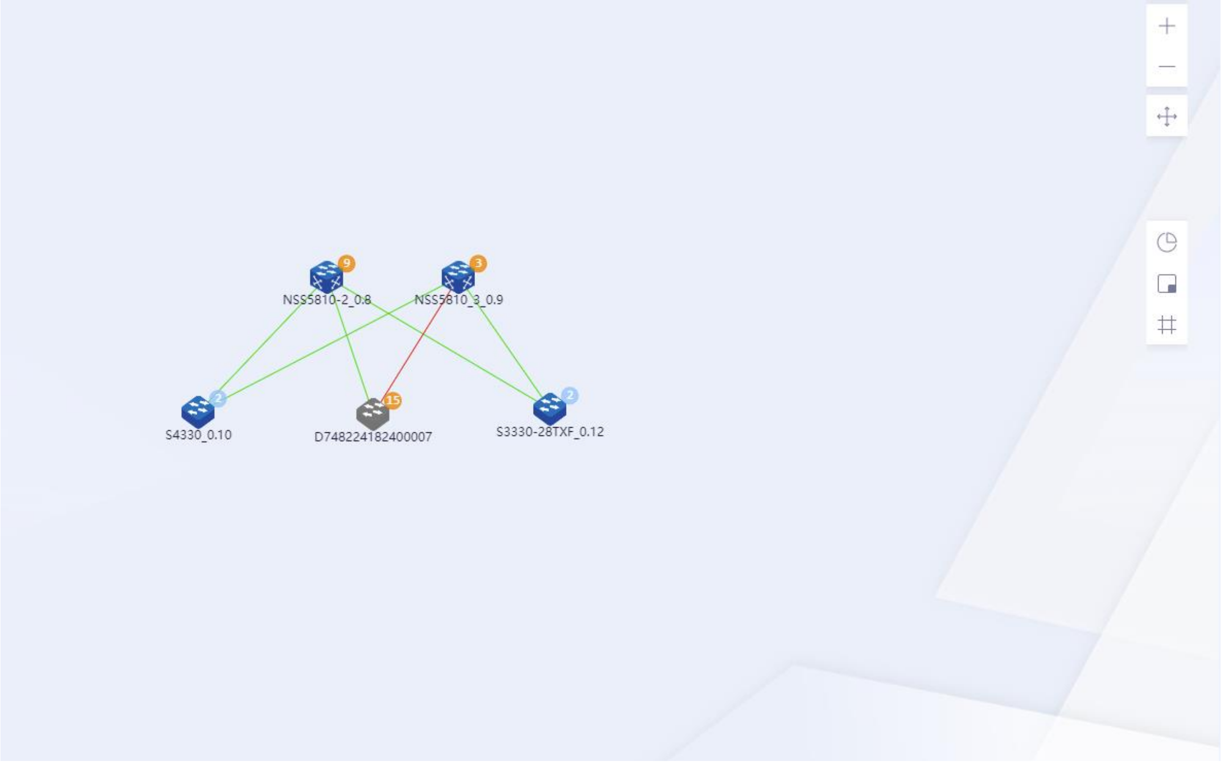


Figure 5.2.5 Topology information statistics

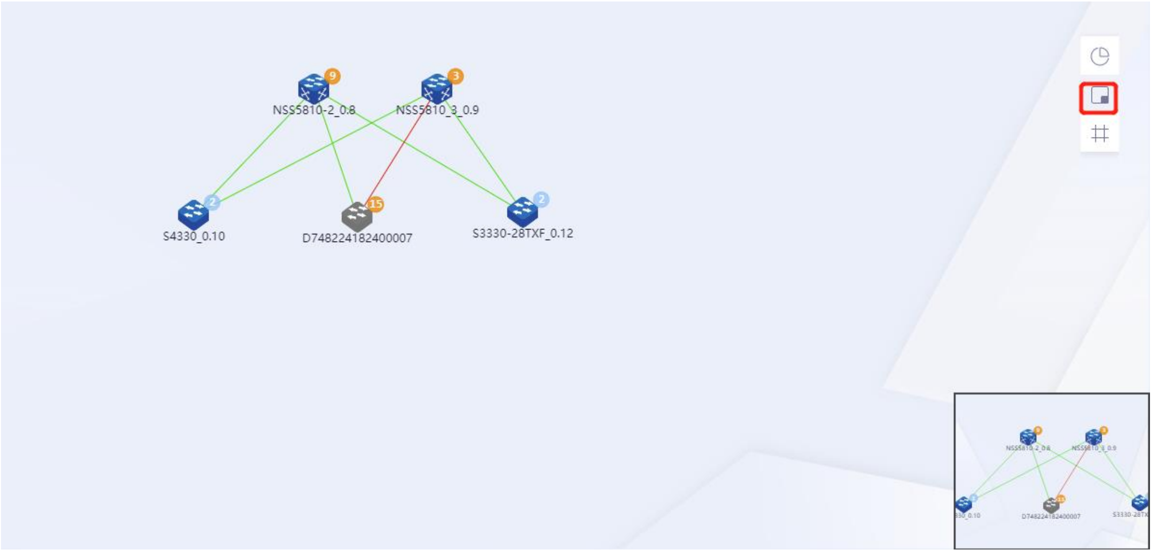
5.2.6 Aerial View

Click the function area button ◪ on the right side of the topology view to open and close the aerial view in the lower right corner of the topology view page, as shown in the following figure:

When there is no aerial view:



When there is the aerial view:



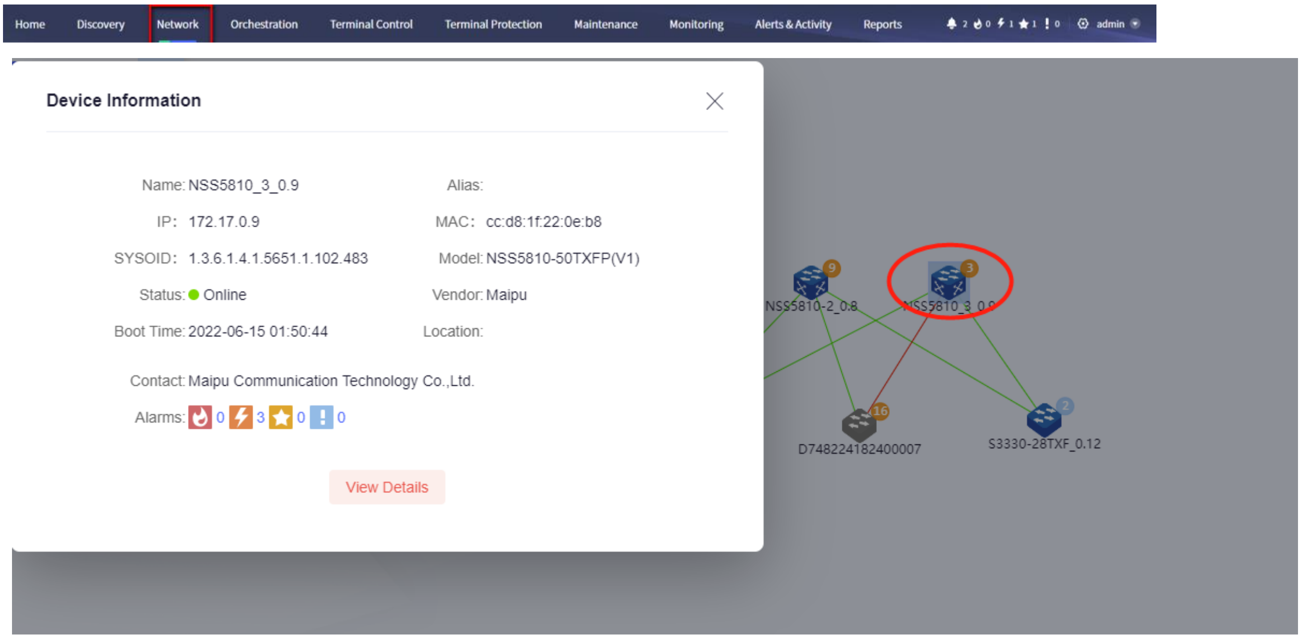
1. By dragging the current screen display area in the aerial view, you can view the part of the topology map that cannot be displayed on the screen.
2. By double-clicking the current screen display area in the aerial view, you can locate the double-click position to the middle of the screen.

5.2.7 Right-click Menus

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

- View details:

To view the device information details, you can also double-click a device in the topology view to achieve the same purpose, as shown in figure 5.2.7.1 below. Some main information of the device is displayed in the device information box. To view more information about the device, you can click the "View Details" button at the bottom of the device information box.



Device Information

Name: NSS5810_3_0.9
Alias:
IP: 172.17.0.9
MAC: cc:d8:1f:22:0e:b8
SYSOID: 1.3.6.1.4.1.5651.1.102.483
Model: NSS5810-50TXFP(V1)
Status: ● Online
Vendor: Maipu
Boot Time: 2022-06-15 01:50:44
Location:
Contact: Maipu Communication Technology Co.,Ltd.
Alarms: 0 3 0 0

View Details

Figure 5.2.7.1 View device information

- Remove elements:

The current device can be removed. It can be deployed automatically after successful removal (after the device to be removed has been successfully deployed, the administrator password needs to be entered when removing the device, and the device can be deleted only when meeting the corresponding networking rules).

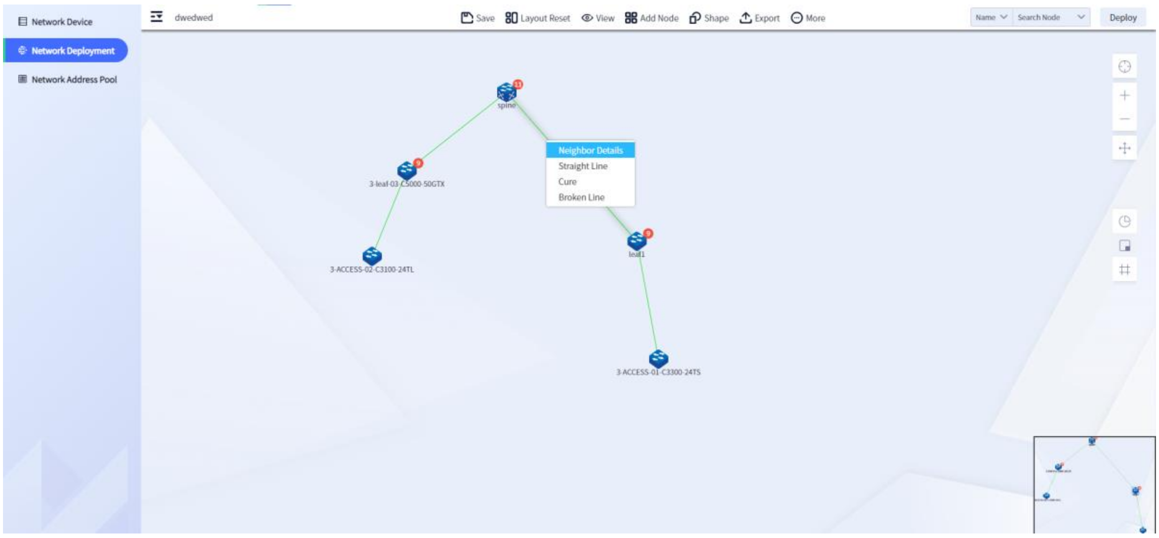
Note

- In the L3 networking vxlan mode, at least one core device and one aggregation device are required. In the L2 networking vxlan or VLAN mode, at least one core device and one access device are required.

Right-click menu of the link

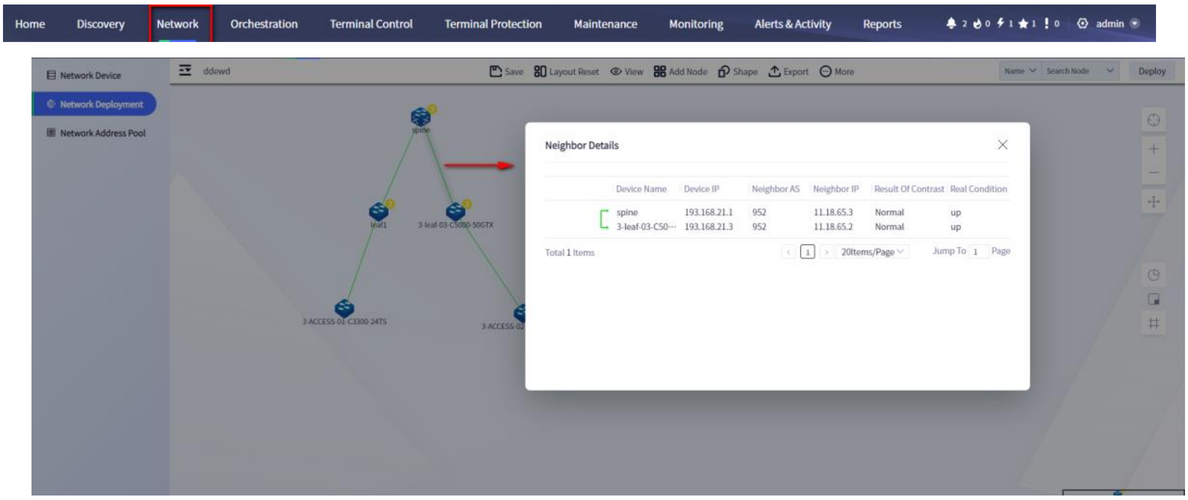
- Neighbor details:

This menu is visible when you right-click the link between the aggregation device and the core device, as shown in the following figure:



The neighbor details box displays the details of the neighbors between devices, showing the device name, device IP, neighbor as number, neighbor IP and neighbor status, as shown in figure 5.2.7.2.

- Link details: This menu is visible when you right-click the link between the aggregation device and the access device. The link details box displays the details of the link between the devices, including the NE name, interface name, interface status, interface IP, bandwidth utilization (in/out), and interface rate, as shown in figure 5.2.7.3.

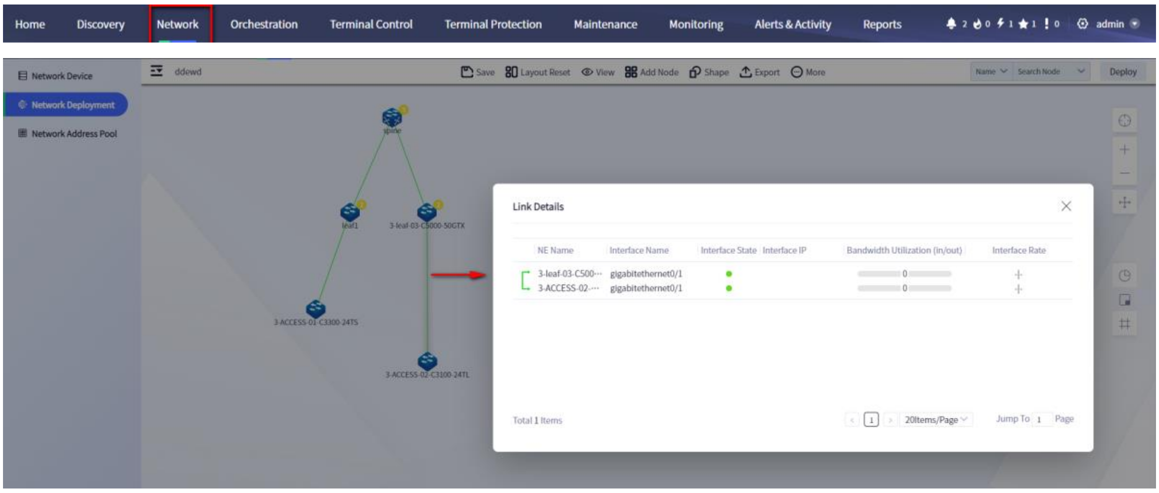


Neighbor Details

Device Name	Device IP	Neighbor AS	Neighbor IP	Result Of Contrast	Real Condition
spine	193.168.21.1	952	11.18.65.3	Normal	up
3-leaf-03-C50···	193.168.21.3	952	11.18.65.2	Normal	up

Total 1 Items   1   20Items/Page   Jump To 1 Page

Figure 5.2.7.2 Neighbor details



Link Details

NE Name	Interface Name	Interface State	Interface IP	Bandwidth Utilization (in/out)	Interface Rate
3-leaf-03-C500···	gigabitethernet0/1	●		0	
3-ACCESS-02-···	gigabitethernet0/1	●		0	

Total 1 Items

20Items/Page

Jump To 1 Page

Figure 5.2.7.3 Link details

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.

As shown in Figure 5.2.7.4:

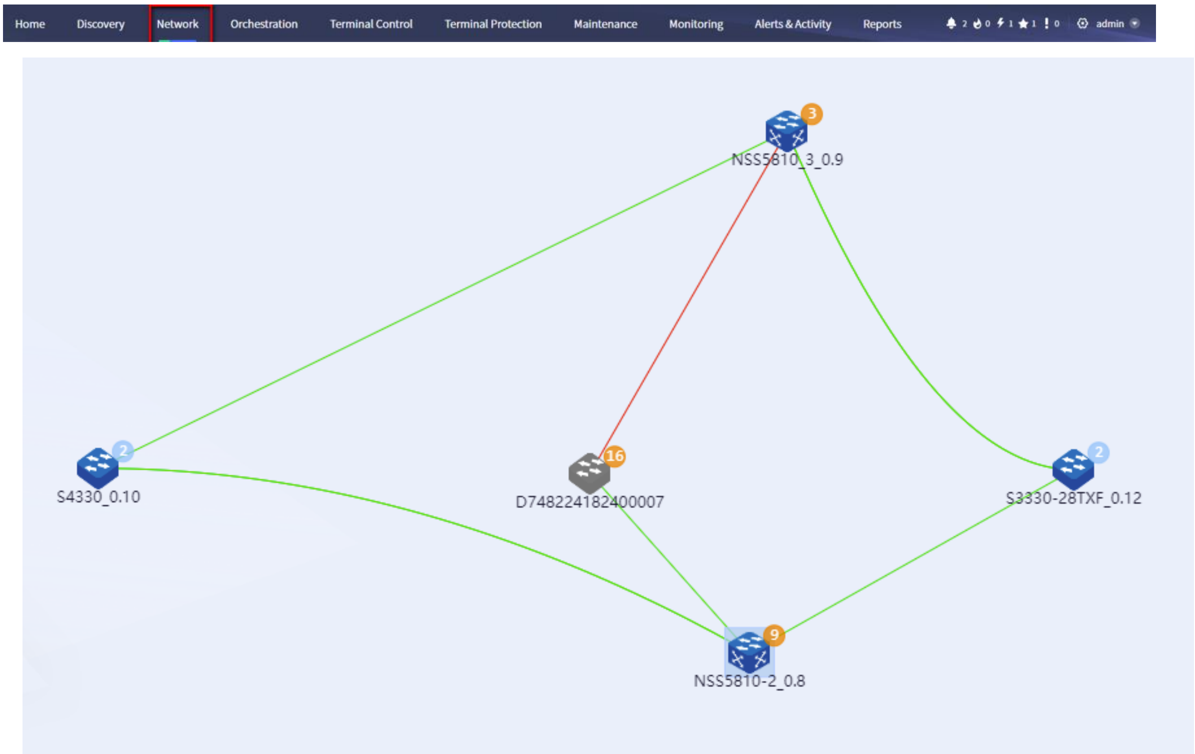


Figure 5.2.7.4 Link shape

Note: The link color is green, the neighbor status is up, the link is red, and the neighbor status is down.

Alarm statistics:

The topology view provides the alarm information statistics of network devices (as shown in figure 5.2.7.5 below).

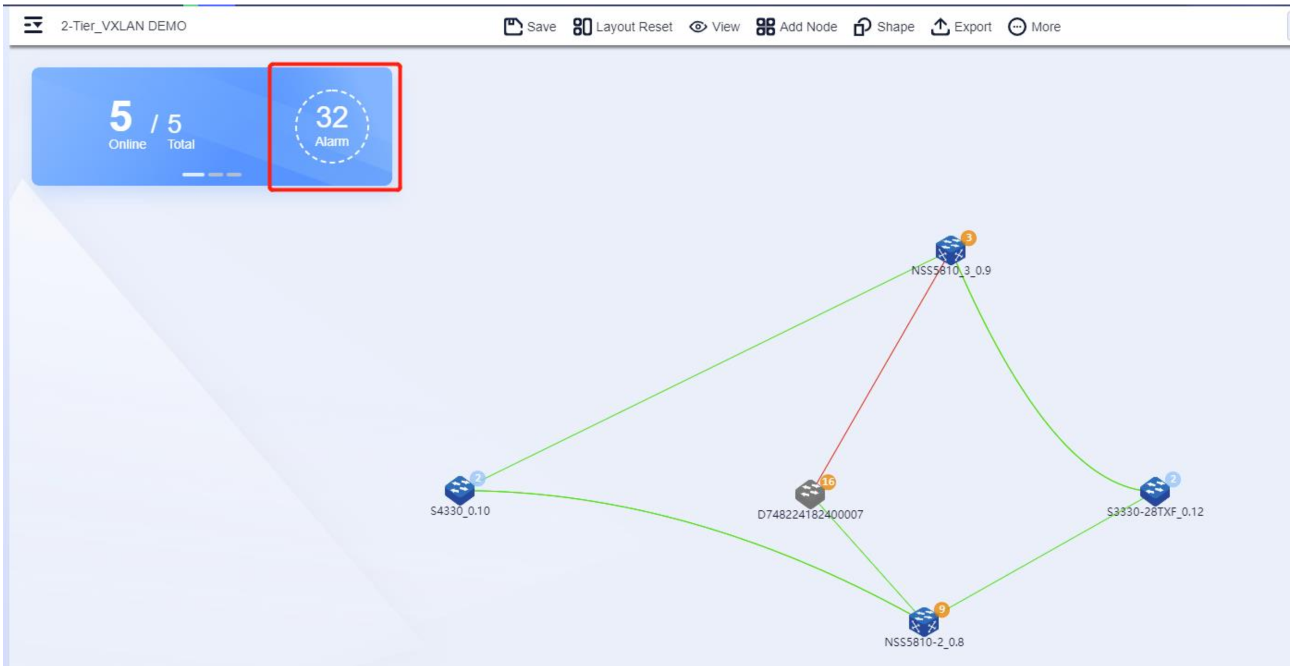
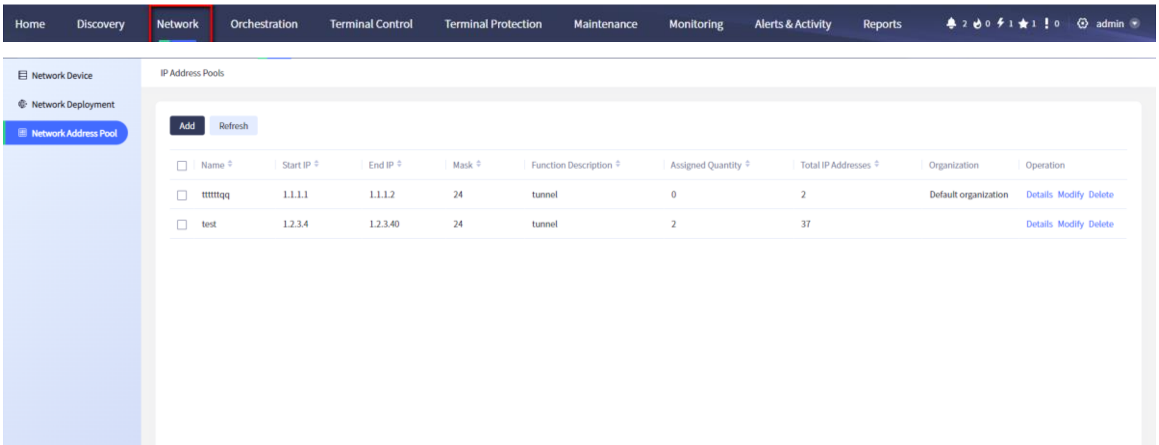


Figure 5.2.7.5 Device alarms

5.3 Campus Address Pool

Click "Network" on the navigation bar at the top of the system, and click **Network Address Pool** to enter the corresponding interface, as shown below:

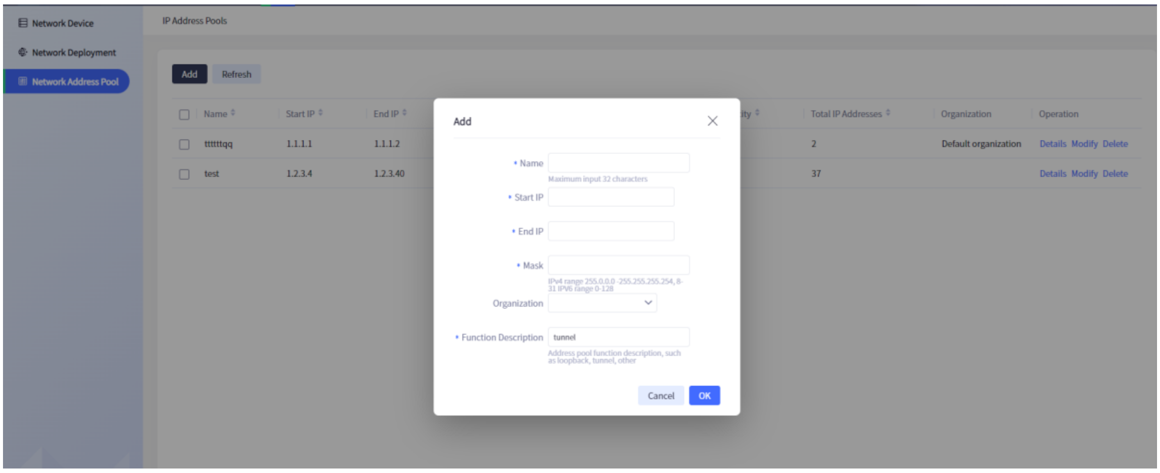


IP Address Pools

☐	Name	Start IP	End IP	Mask	Function Description	Assigned Quantity	Total IP Addresses	Organization	Operation
☐	ttttttqq	1.1.1.1	1.1.1.2	24	tunnel	0	2	Default organization	Details Modify Delete
☐	test	1.2.3.4	1.2.3.40	24	tunnel	2	37		Details Modify Delete

Figure 5.3.1 IP address pool list

Click the **Add** button to fill in the name, start IP, end IP and subnet mask. You can fill in the corresponding function descriptions, such as loopback, tunnel and other, as shown in the following figure:

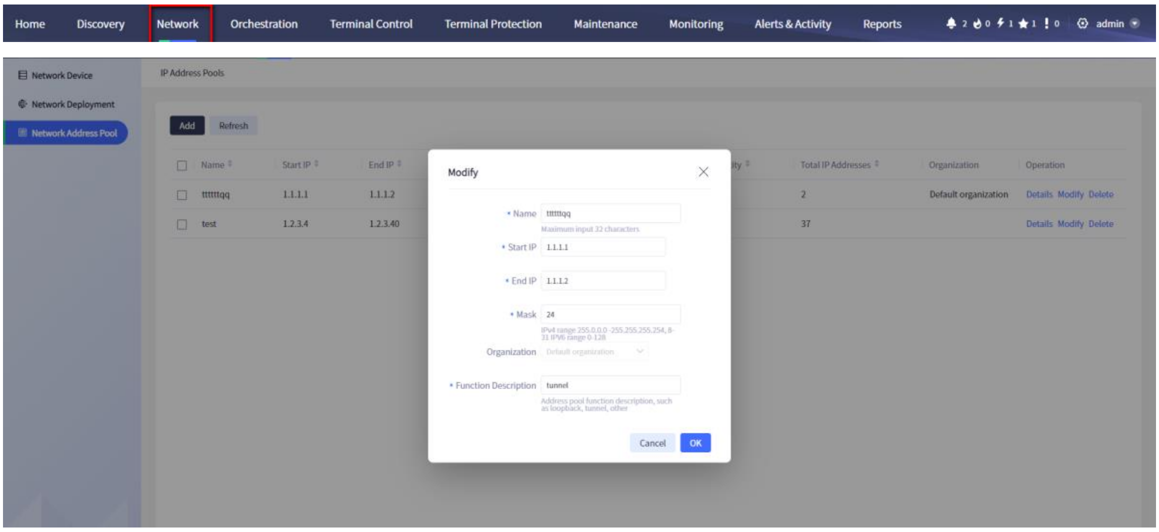

Network Device
Network Deployment
Network Address Pool
IP Address Pools
Add
Refresh
Add
Name
Maximum input 32 characters
Start IP
End IP
Mask
IPv4 range 255.0.0.0 -255.255.255.254, 8-31 IPV6 range 0-128
Organization
Function Description
Address pool function description, such as loopback, tunnel, other
Cancel
OK

Function Description: tunnel

☐	Name	Start IP	End IP	ity	Total IP Addresses	Organization	Operation
☐	tttttqq	1.1.1.1	1.1.1.2		2	Default organization	Details Modify Delete
☐	test	1.2.3.4	1.2.3.40		37		Details Modify Delete

Figure 5.3.2 Add IP address

Click **Modify** to open the dialog box as shown in the following figure. After modification, click **OK** to save the modification settings, as shown below:

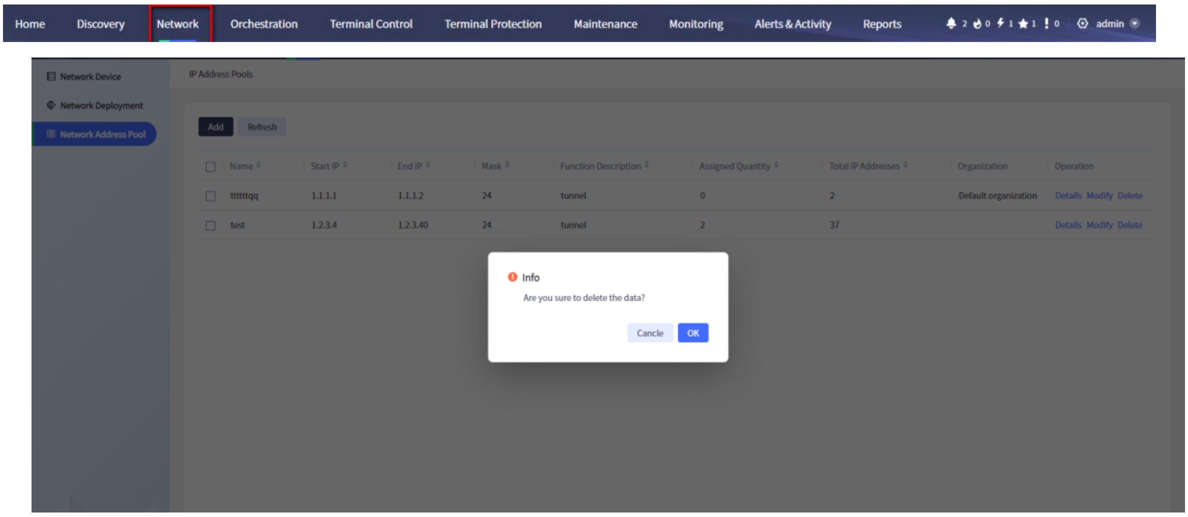


Name: tttttqq
Start IP: 1.1.1.1
End IP: 1.1.1.2
Mask: 24
Organization: Default organization
Function Description: tunnel

☐	Name	Start IP	End IP	ity	Total IP Addresses	Organization	Operation
☐	tttttqq	1.1.1.1	1.1.1.2		2	Default organization	Details Modify Delete
☐	test	1.2.3.4	1.2.3.40		37		Details Modify Delete

Figure 5.3.3 Modify ip address

Click **Delete** in the operation bar, and click **OK** in the confirmation dialog box to delete the selected data. Click **Cancel** to abort the deletion, as shown below:



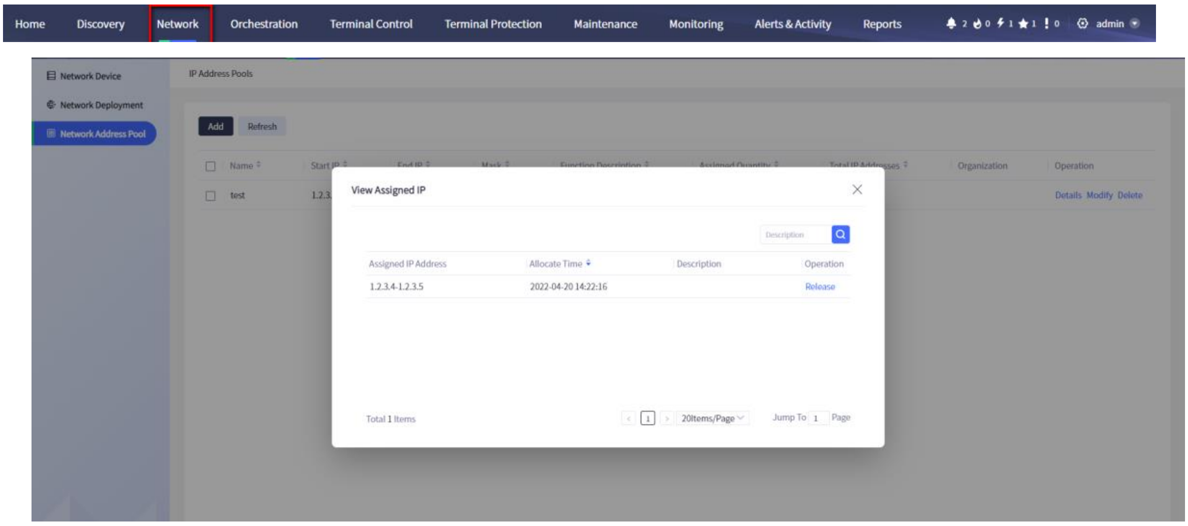
☐	Name	Start IP	End IP	Mask	Function Description	Assigned Quantity	Total IP Addresses	Organization	Operation
☐	tttttqq	1.1.1.1	1.1.1.2	24	tunnel	0	2	Default organization	Details Modify Delete
☐	test	1.2.3.4	1.2.3.40	24	tunnel	2	37		Details Modify Delete

Info

Are you sure to delete the data?

Figure 5.3.4 Delete ip address

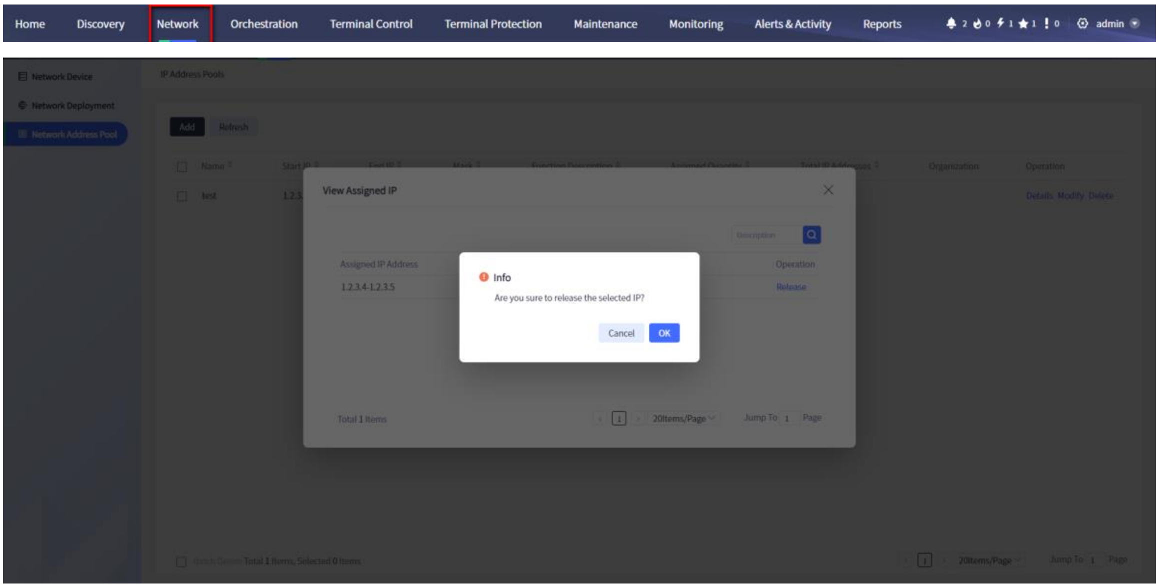
Click the **Details** button in the operation bar to view the assigned IP, as shown below:



Assigned IP Address	Allocate Time	Description	Operation
1.2.3.4-1.2.3.5	2022-04-20 14:22:16		Release

Figure 5.3.5 Assigned IP list

Click **Release**, and click **OK** in the confirmation dialog box to release the selected IP. Click **Cancel** to abort the release operation, as shown below:



Are you sure to release the selected IP?

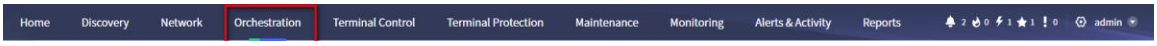
Figure 5.3.6 Release assigned ip

Refresh:

Click **Refresh** at the top of the list to refresh the IP list data. The used IP address pool cannot be deleted.

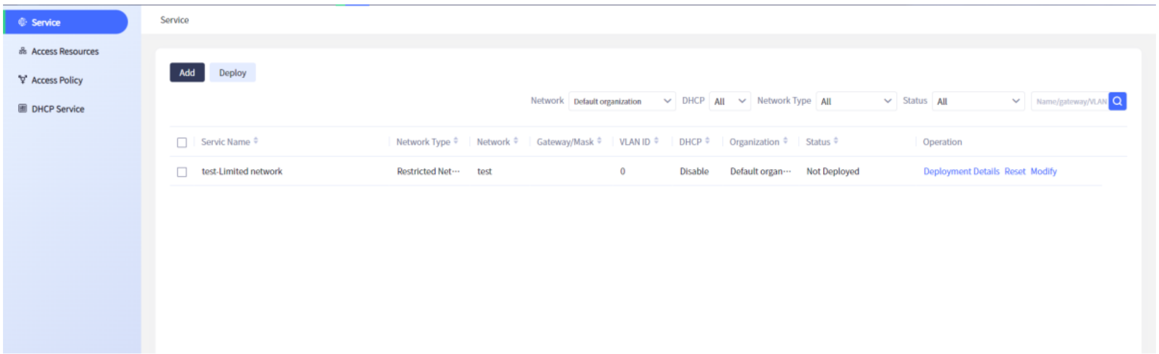
6 Service Network

The class-1 menu of the service network is as follows:



6.1 Service Network List

Click "Service" in the left menu bar to enter the service network management interface, as shown in the following figure:

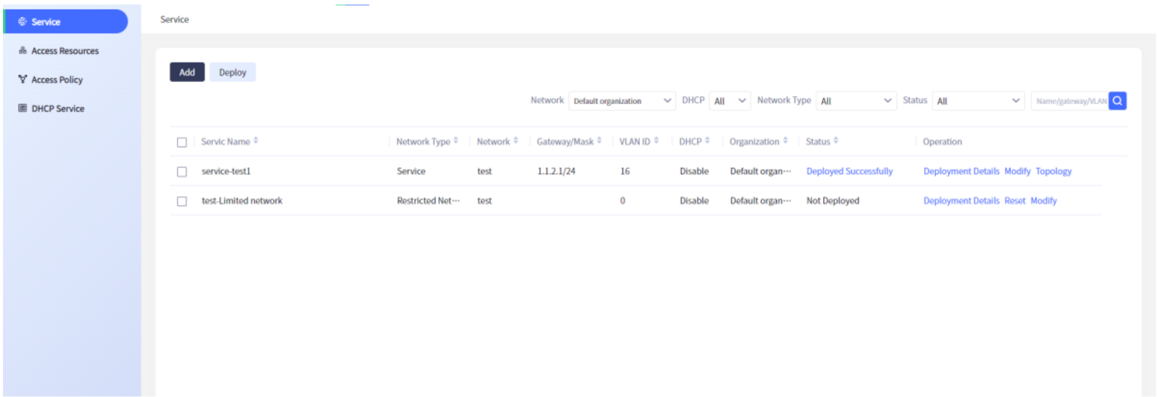


Network: Default organization   DHCP: All   Network Type: All   Status: All

☐	Servic Name	Network Type	Network	Gateway/Mask	VLAN ID	DHCP	Organization	Status	Operation
☐	test-Limited network	Restricted Net···	test		0	Disable	Default organ···	Not Deployed	Deployment Details Reset Modify

Figure 6.1.1 Enter service network management interface

Open the "Service" interface to display all the service networks under the organization by default, showing the name, network type, network, gateway/mask, VLAN ID, DHCP, organization, deployment results and other information of each service network, as shown in figure 6.1.2:

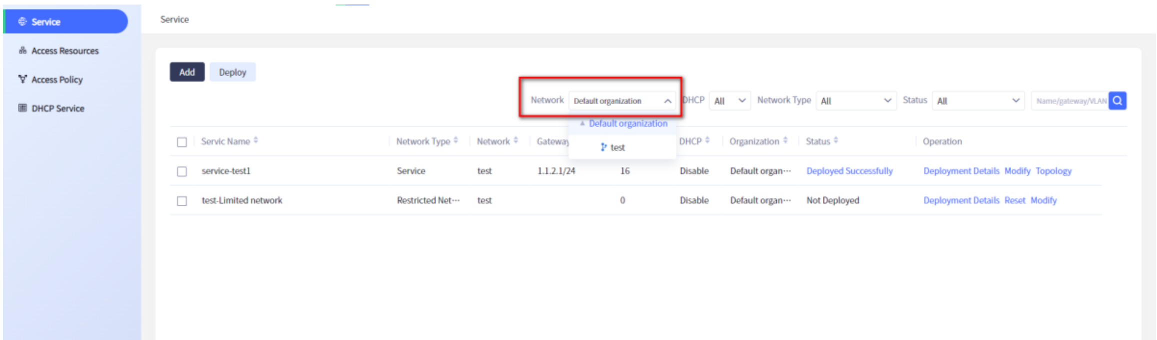


Network: Default organization   DHCP: All   Network Type: All   Status: All

☐	Servic Name	Network Type	Network	Gateway/Mask	VLAN ID	DHCP	Organization	Status	Operation
☐	service-test1	Service	test	1.1.2.1/24	16	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☐	test-Limited network	Restricted Net···	test		0	Disable	Default organ···	Not Deployed	Deployment Details Reset Modify

Figure 6.1.2 Service network list

Click the campus filter box above, and you can filter the service network according to the organization/campus planning network, as shown in figure 6.1.3:



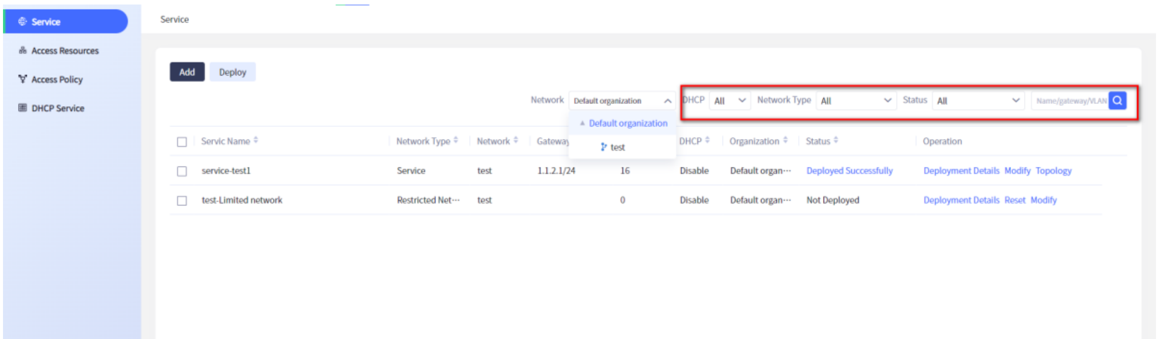
Network: Default organization · DHCP: All · Network Type: All · Status: All · Name/gateway/VLAN

▴ Default organization
test

☐	Servic Name	Network Type	Network	Gateway		DHCP	Organization	Status	Operation
☐	service-test1	Service	test	1.1.2.1/24	16	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☐	test-Limited network	Restricted Net···	test		0	Disable	Default organ···	Not Deployed	Deployment Details Reset Modify

Figure 6.1.3 Service network

This page provides a variety of query criteria to query specific service networks conveniently and quickly. Enter the corresponding query criteria in the query panel, and then click the "Query" button to filter all service networks according to DHCP, network type, deployment result, name, gateway, VLAN and other fields, as shown in figure 6.1.4:



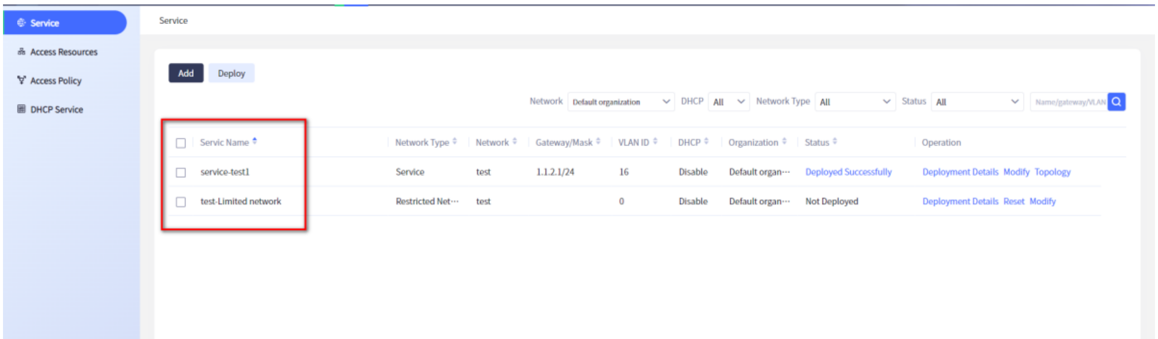
Network: Default organization · DHCP: All · Network Type: All · Status: All · Name/gateway/VLAN

▴ Default organization
test

☐	Servic Name	Network Type	Network	Gateway		DHCP	Organization	Status	Operation
☐	service-test1	Service	test	1.1.2.1/24	16	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☐	test-Limited network	Restricted Net···	test		0	Disable	Default organ···	Not Deployed	Deployment Details Reset Modify

Figure 6.1.4 Service network query

Click each field in the header of the service network list to sort the service networks according to the corresponding fields. As shown in the following figure, sort in ascending order according to the service network name:

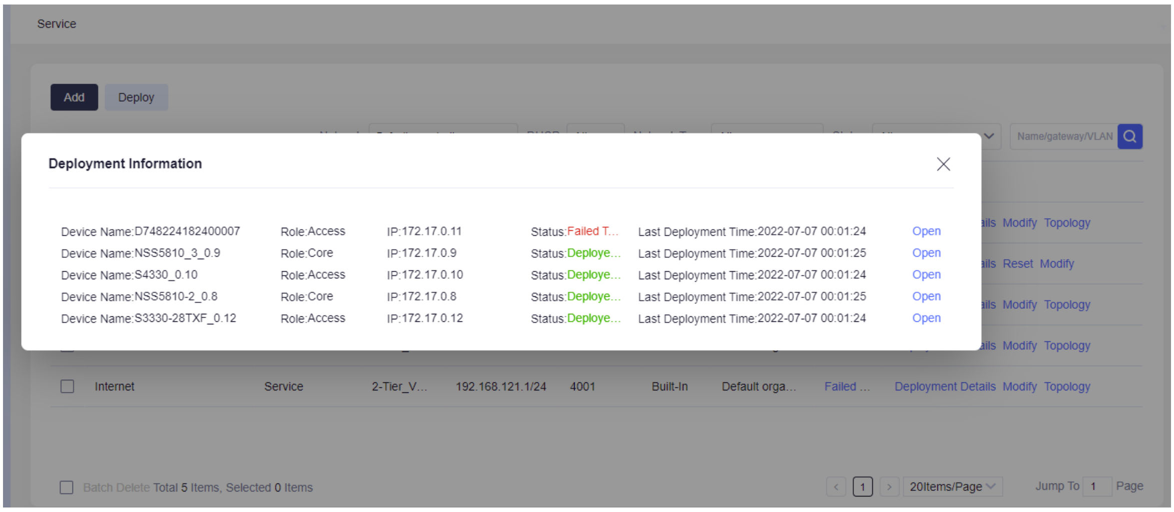


Network: Default organization · DHCP: All · Network Type: All · Status: All · Name/gateway/VLAN

☐	Servic Name	Network Type	Network	Gateway/Mask	VLAN ID	DHCP	Organization	Status	Operation
☐	service-test1	Service	test	1.1.2.1/24	16	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☐	test-Limited network	Restricted Net···	test		0	Disable	Default organ···	Not Deployed	Deployment Details Reset Modify

Figure 6.1.5 Sort by service network name

Click the blue words in the deployment result column of the service network table to view the deployment information of the service network, as shown in figure 6.1.6:


Service
Add
Deploy
Name/gateway/VLAN
ails Modify Topology
ails Reset Modify
ails Modify Topology
ails Modify Topology
Internet Service 2-Tier_V... 192.168.121.1/24 4001 Built-In Default orga... Failed ... Deployment Details Modify Topology
Batch Delete Total 5 Items, Selected 0 Items
1
20Items/Page
Jump To 1 Page

Deployment Information

Device Name:D748224182400007	Role:Access	IP:172.17.0.11	Status:Failed T...	Last Deployment Time:2022-07-07 00:01:24	Open
Device Name:NSS5810_3_0.9	Role:Core	IP:172.17.0.9	Status:Deploye...	Last Deployment Time:2022-07-07 00:01:25	Open
Device Name:S4330_0.10	Role:Access	IP:172.17.0.10	Status:Deploye...	Last Deployment Time:2022-07-07 00:01:24	Open
Device Name:NSS5810-2_0.8	Role:Core	IP:172.17.0.8	Status:Deploye...	Last Deployment Time:2022-07-07 00:01:25	Open
Device Name:S3330-28TXF_0.12	Role:Access	IP:172.17.0.12	Status:Deploye...	Last Deployment Time:2022-07-07 00:01:24	Open

Figure 6.1.6 Deployment information

Note

- The query input box can fuzzy match any one of the service network name gateway and VLAN.
- Only restricted networks can be reset.
- You can view the deployment information only for the deployed service networks.

6.2 Add, Modify Service Network&Service Network Topology

Add Restricted Network

The restricted network cannot be added manually. It is created automatically after the campus planning network is deployed. After the campus planning network is deployed, a service network named “Campus Planning Network Name - Restricted Network” will be automatically created under the corresponding campus planning network.

Add Service Network

Add an unrestricted network manually. Click the **Add** button to open the following "Add" dialog box, where you can set the name, campus network, VLAN ID, DHCP, gateway/mask, IP privacy protection, description and other information of the service network. Here, you can select whether to deploy immediately. If you tick it, and click **OK** to add the business network information successfully, the service network will begin to deploy immediately. If you do not tick it, and click **OK** to add the service network information successfully, the service network will not be deployed. You need to click **Deploy** manually, as shown in Figure 6.2.1:

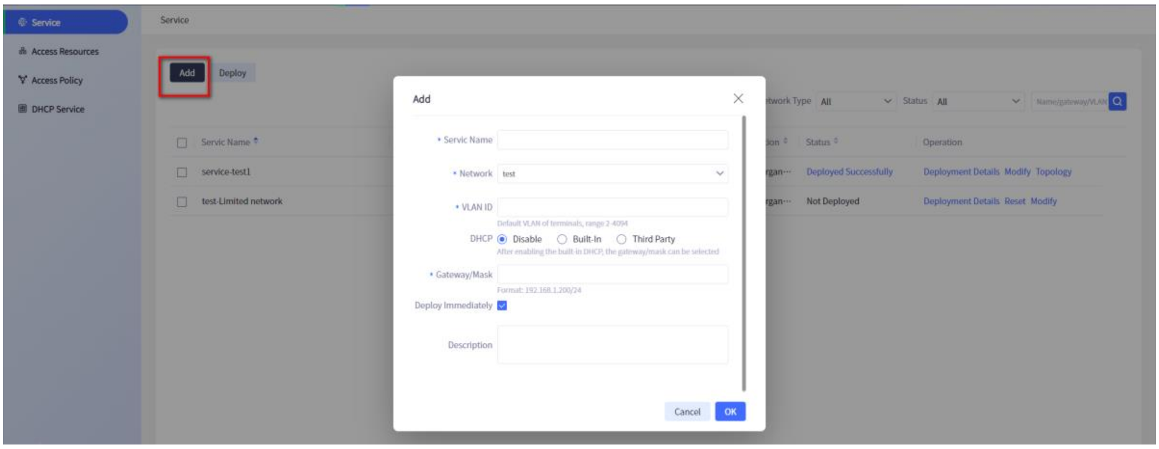


Figure 6.2.1 Add service network

The modification of the service network can be divided into three cases:

1. Modify the deployed network;
2. Modify the un-deployed network;
3. Reset the restricted network.

Modify Deployed Network

Click the **Modify** button in the operation bar on the right side of the deployed network to open the following "Modify" dialog box. You can modify the name, VLAN ID, DHCP, gateway/mask, IP privacy protection, description and other information of the service network, but cannot modify the vlanId and the network. Click "OK" to modify the service network information successfully, as shown in figure 6.1.2.2:

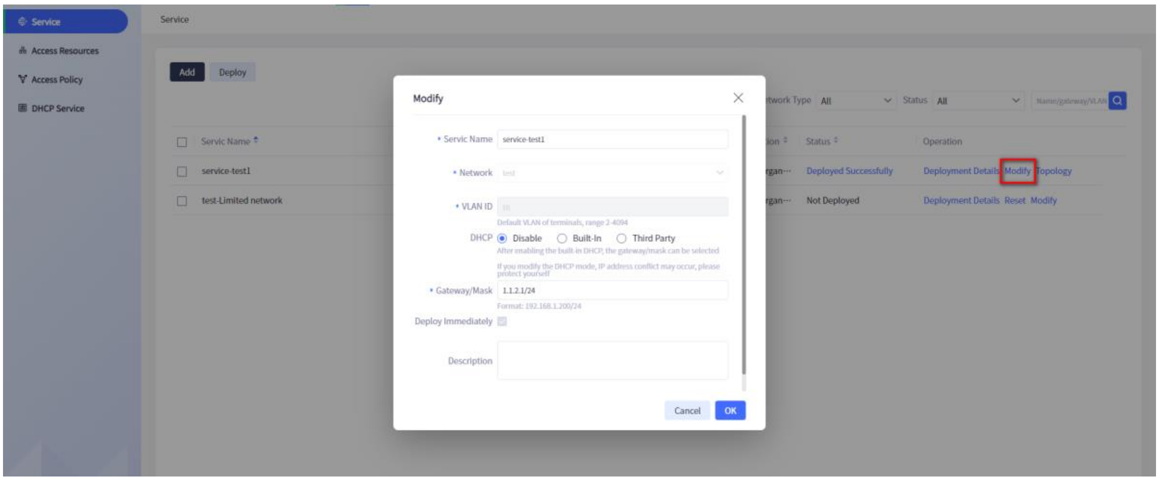
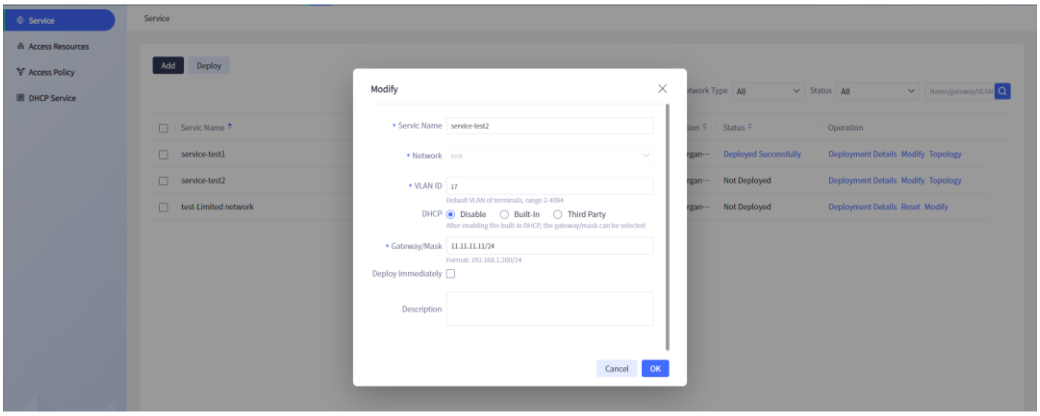

Service
Access Resources
Access Policy
DHCP Service
Add
Deploy
Servic Name
service-test1
test-Limited network
Deployed Successfully
Not Deployed
Operation
Deployment Details Modify Topology
Deployment Details Reset Modify
Modify
• Servic Name service-test1
• Network test
• VLAN ID
Default VLAN of terminals, range 2-4094
DHCP ● Disable ○ Built-In ○ Third Party
After enabling the built-in DHCP, the gateway/mask can be selected
If you modify the DHCP mode, IP address conflict may occur, please protect yourself
• Gateway/Mask 1.1.2.1/24
Format: 192.168.1.200/24
Deploy Immediately
Description
Cancel
OK

Figure 6.2.2 Modify the deployed network

Modify Un-deployed Network

Click the **Modify** button in the operation bar on the right side of the un-deployed network to open the following "Modify" dialog box. You can modify the name, VLAN ID, DHCP, gateway/mask, IP privacy protection, description and other information of the service network. Click "OK" to modify the service network information successfully, as shown in figure 6.2.3:

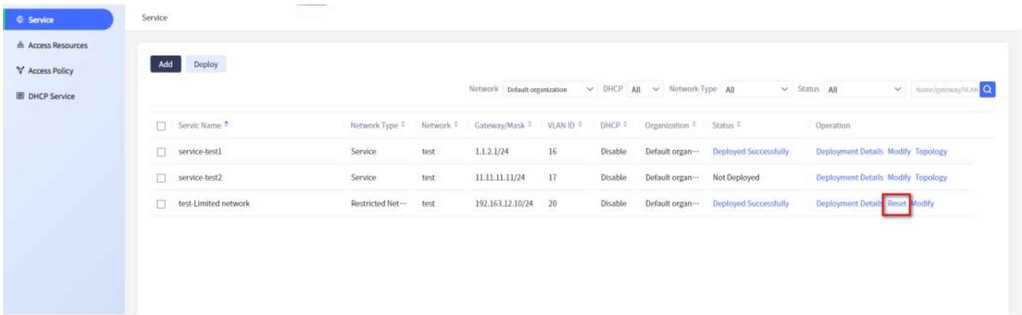


Servic Name: service-test2
Network: test
VLAN ID: 17
Default VLAN of terminals, range 2-4094
DHCP: ● Disable ○ Built-In ○ Third Party
After enabling the built-in DHCP, the gateway/mask can be selected
Gateway/Mask: 11.11.11.11/24
Format: 192.168.1.200/24
Deploy Immediately ☐
Description:

Figure 6.2.3 Modify the un-deployed network

Reset Restricted Network

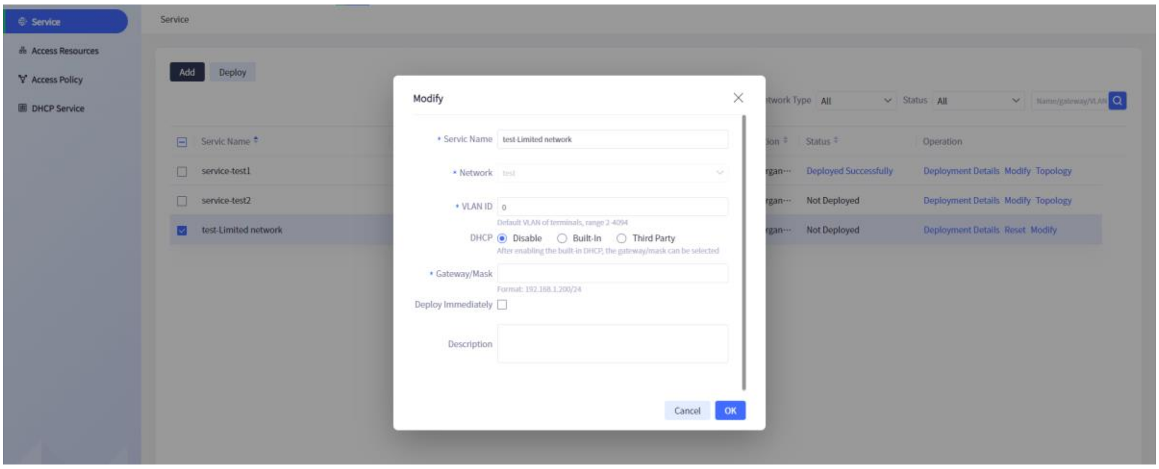
Click the **Reset** button in the operation column on the right of the restricted network to reset the restricted network. After resetting, the service network is set to the un-deployed state, and the VLAN ID, DHCP, gateway/mask information are restored, as shown in the following figure:



Network: Default organization DHCP: All Network Type: All Status: All

☐	Servic Name	Network Type	Network	Gateway/Mask	VLAN ID	DHCP	Organization	Status	Operation
☐	service-test1	Service	test	1.1.2.1/24	16	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☐	service-test2	Service	test	11.11.11.11/24	17	Disable	Default organ···	Not Deployed	Deployment Details Modify Topology
☐	test-Limited network	Restricted Net···	test	192.163.12.10/24	20	Disable	Default organ···	Deployed Successfully	Deployment Details Reset Modify

Figure 6.2.4 Click Reset



Servic Name: test-Limited network
Network: test
VLAN ID: 0
Default VLAN of terminals, range 2-4094
DHCP: ● Disable ○ Built-In ○ Third Party
After enabling the built-in DHCP, the gateway/mask can be selected
Gateway/Mask:
Format: 192.168.1.200/24
Deploy Immediately ☐
Description:

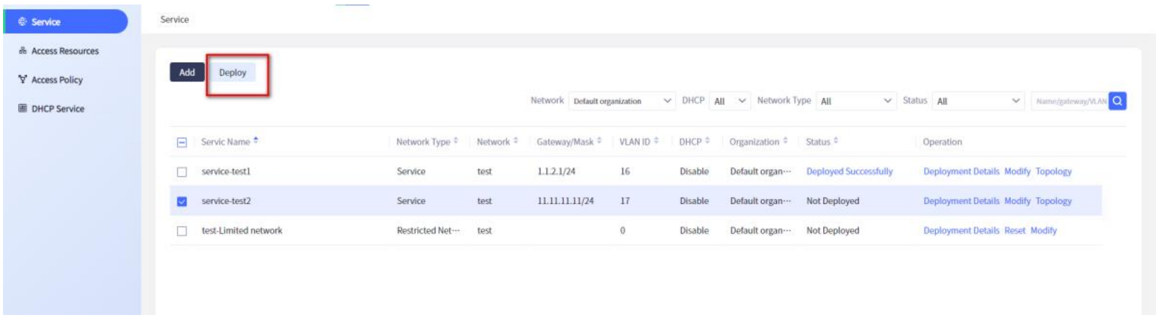
Figure 6.2.5 Effect after resetting

Note

- If the service network to be modified has been deployed, the VLAN ID cannot be modified.
- The restricted network cannot be reset until it is deployed.

6.2.1 Deployment

Check the service network first, and then click the "Deploy" button to deploy the currently selected business network immediately, as shown in figure 6.2.1.1 below:



☐	Servic Name	Network Type	Network	Gateway/Mask	VLAN ID	DHCP	Organization	Status	Operation
☐	service-test1	Service	test	1.1.2.1/24	16	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☑	service-test2	Service	test	11.11.11.11/24	17	Disable	Default organ···	Not Deployed	Deployment Details Modify Topology
☐	test-Limited network	Restricted Net···	test		0	Disable	Default organ···	Not Deployed	Deployment Details Reset Modify

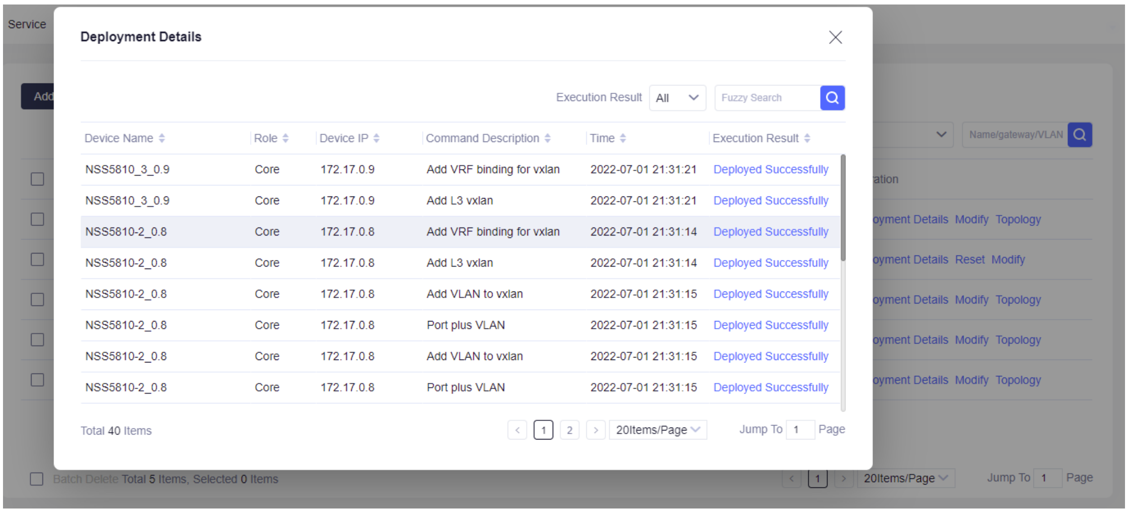
Figure 6.2.1.1 Deploy

Note

- Check **Deploy Immediately** when adding, and deploy automatically after adding.

6.2.2 Deployment Details of Service Network

Click the "Deployment Details" button in the operation column of the service network table, and you can view the deployment details list of the service network, as shown in figure 6.2.2.1:



Device Name	Role	Device IP	Command Description	Time	Execution Result
NSS5810_3_0.9	Core	172.17.0.9	Add VRF binding for vxlan	2022-07-01 21:31:21	Deployed Successfully
NSS5810_3_0.9	Core	172.17.0.9	Add L3 vxlan	2022-07-01 21:31:21	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VRF binding for vxlan	2022-07-01 21:31:14	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add L3 vxlan	2022-07-01 21:31:14	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VLAN to vxlan	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Port plus VLAN	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VLAN to vxlan	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Port plus VLAN	2022-07-01 21:31:15	Deployed Successfully

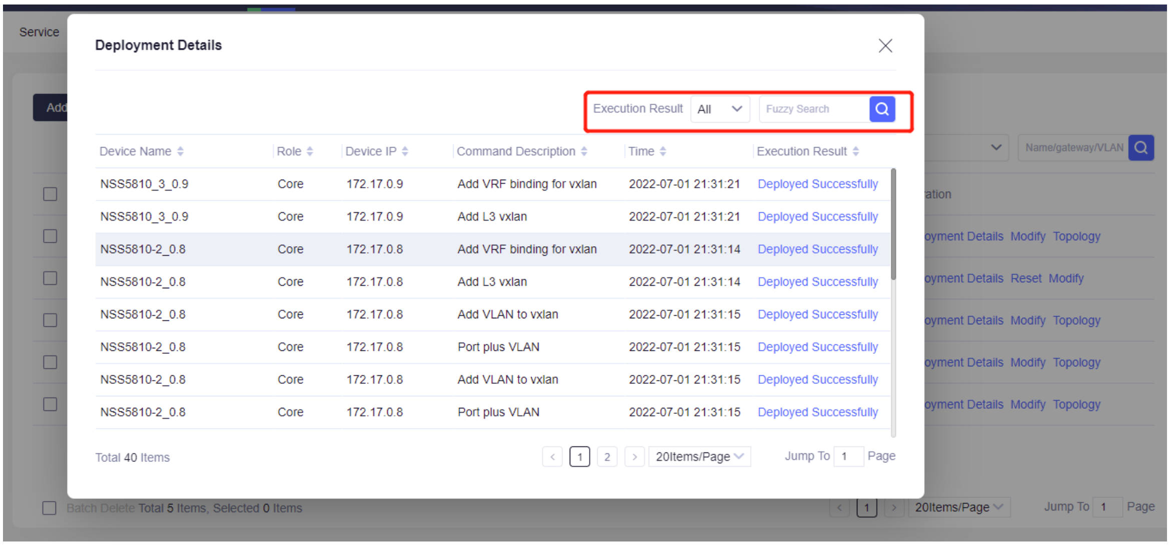
Total 40 Items

1
2
20Items/Page
Jump To 1 Page
ation
oyment Details Modify Topology
oyment Details Reset Modify
oyment Details Modify Topology
oyment Details Modify Topology
oyment Details Modify Topology
Batch Delete
1
20Items/Page
Jump To 1 Page

Total 5 Items, Selected 0 Items

Figure 6.2.2.1 Deployment details list

The deployment details list page provides various query criteria to query specific deployment details conveniently and quickly. Enter the corresponding query criteria in the query panel, and then click **Query** to filter all deployment details according to the execution results and keywords, as shown in figure 6.2.2.2:


Service
Add
Name/gateway/VLAN
ation
oyment Details Modify Topology
oyment Details Reset Modify
oyment Details Modify Topology
oyment Details Modify Topology
oyment Details Modify Topology
Batch Delete Total 5 Items, Selected 0 Items
1
20Items/Page
Jump To 1 Page

Deployment Details

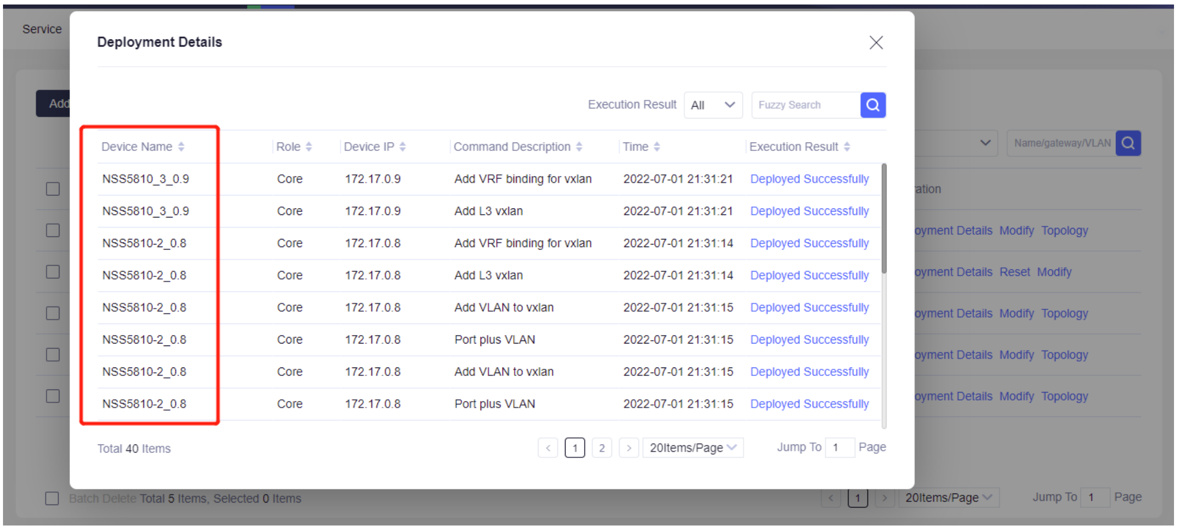
Execution Result All | Fuzzy Search

Device Name	Role	Device IP	Command Description	Time	Execution Result
NSS5810_3_0.9	Core	172.17.0.9	Add VRF binding for vxlan	2022-07-01 21:31:21	Deployed Successfully
NSS5810_3_0.9	Core	172.17.0.9	Add L3 vxlan	2022-07-01 21:31:21	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VRF binding for vxlan	2022-07-01 21:31:14	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add L3 vxlan	2022-07-01 21:31:14	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VLAN to vxlan	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Port plus VLAN	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VLAN to vxlan	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Port plus VLAN	2022-07-01 21:31:15	Deployed Successfully

Total 40 Items

Figure 6.2.2.2 Query deployment details

Click the fields in the header of the deployment details list to sort the deployment details according to the corresponding fields. As shown in the following figure, sort by the device names in ascending order:


Service
Add
Name/gateway/VLAN
ation
oyment Details Modify Topology
oyment Details Reset Modify
oyment Details Modify Topology
oyment Details Modify Topology
oyment Details Modify Topology
Batch Delete Total 5 Items, Selected 0 Items
1
20Items/Page
Jump To 1 Page

Deployment Details

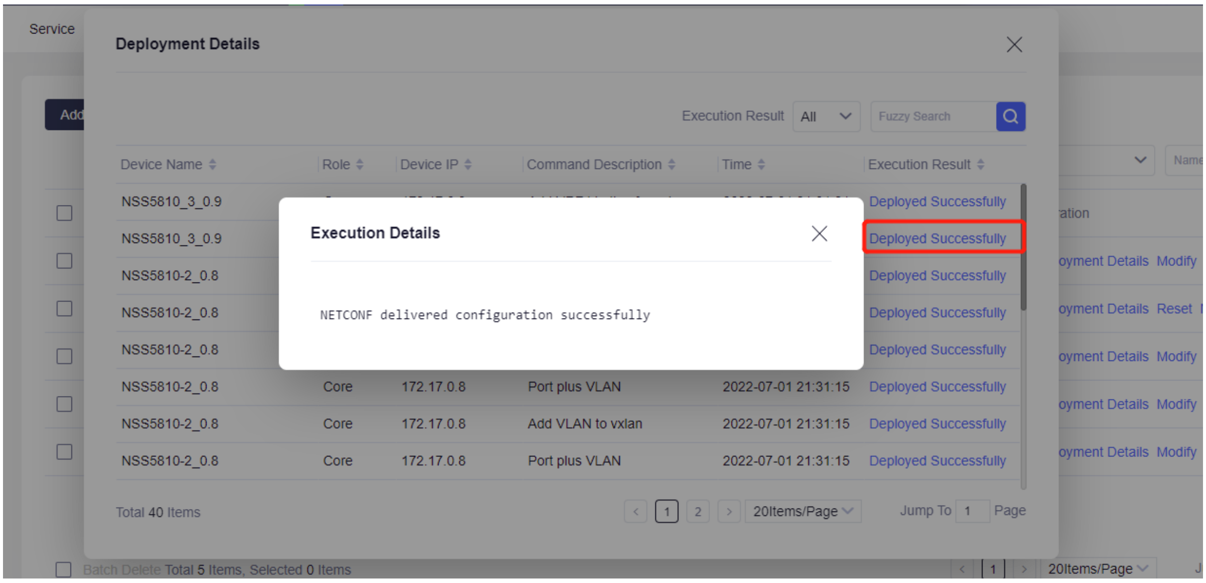
Execution Result All | Fuzzy Search

Device Name	Role	Device IP	Command Description	Time	Execution Result
NSS5810_3_0.9	Core	172.17.0.9	Add VRF binding for vxlan	2022-07-01 21:31:21	Deployed Successfully
NSS5810_3_0.9	Core	172.17.0.9	Add L3 vxlan	2022-07-01 21:31:21	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VRF binding for vxlan	2022-07-01 21:31:14	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add L3 vxlan	2022-07-01 21:31:14	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VLAN to vxlan	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Port plus VLAN	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VLAN to vxlan	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Port plus VLAN	2022-07-01 21:31:15	Deployed Successfully

Total 40 Items

Figure 6.2.2.3 Sort by device names

Click the "Execution Result" column in the operation column of the deployment details table to view the execution details, as shown in figure 6.1.4.4:



Execution Details

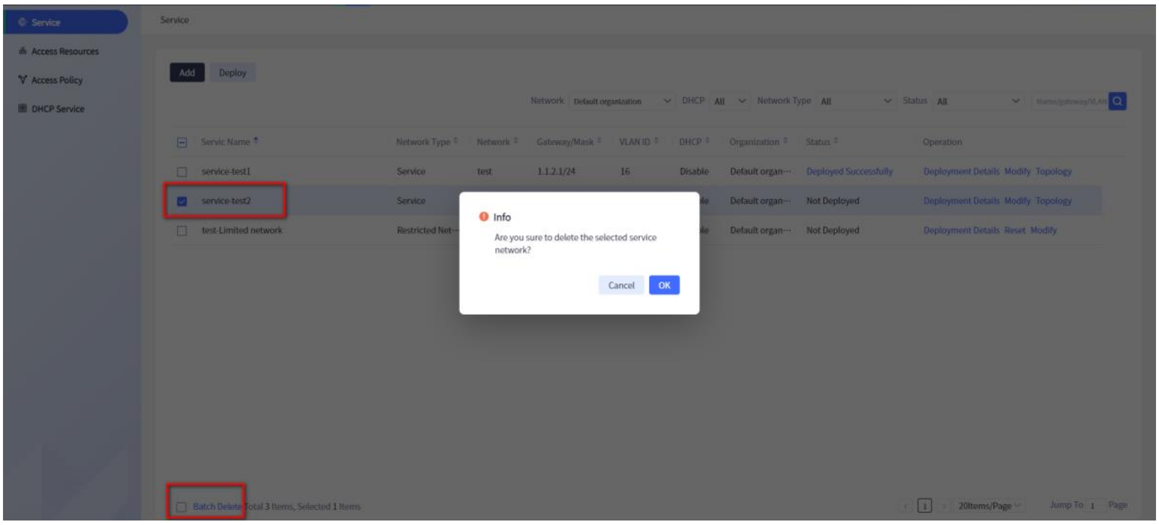
```
NETCONF delivered configuration successfully
```

Device Name	Role	Device IP	Command Description	Time	Execution Result
NSS5810_3_0.9					Deployed Successfully
NSS5810_3_0.9					Deployed Successfully
NSS5810-2_0.8					Deployed Successfully
NSS5810-2_0.8					Deployed Successfully
NSS5810-2_0.8					Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Port plus VLAN	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Add VLAN to vxlan	2022-07-01 21:31:15	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	Port plus VLAN	2022-07-01 21:31:15	Deployed Successfully

Figure 6.2.2.4 Execution details

6.2.3 Delete Service Network

First check the service networks, and then click the "Batch Delete" button to delete the selected service networks (Note: after deleting the deployed service network, the device service network configuration is deleted synchronously. In addition, it is not allowed to delete when the policy or license policy is deployed), as shown in figures 6.2.3.1 and 6.2.3.2 below:

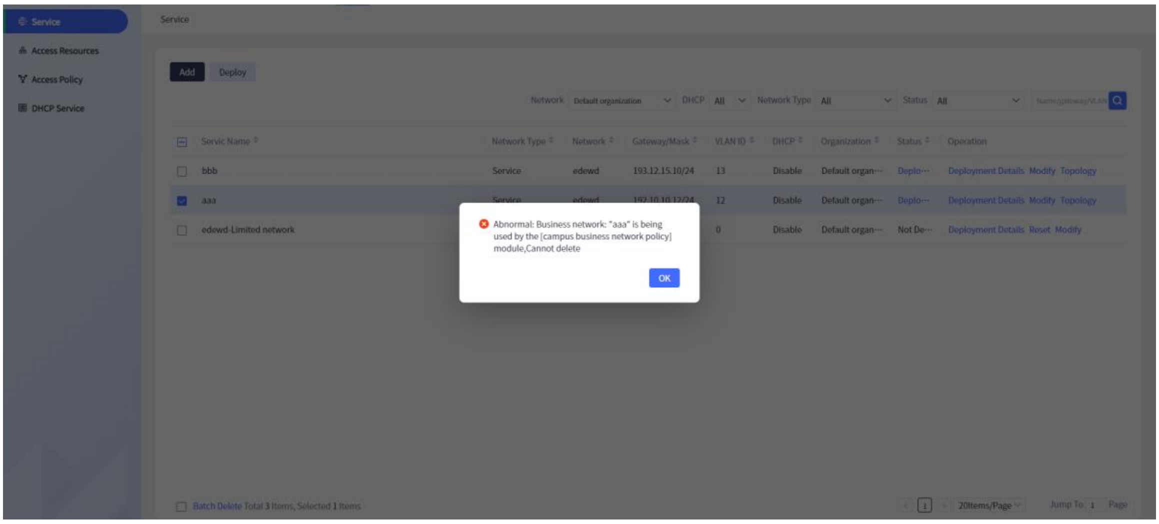


Info

Are you sure to delete the selected service network?

	Servic Name	Network Type	Network	Gateway/Mask	VLAN ID	DHCP	Organization	Status	Operation
☐	service-test1	Service	test	1.1.2.1/24	16	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☑	service-test2	Service					Default organ···	Not Deployed	Deployment Details Modify Topology
☐	test-Limited network	Restricted Net···					Default organ···	Not Deployed	Deployment Details Reset Modify

Figure 6.2.3.1 Delete



☐	Servic Name	Network Type	Network	Gateway/Mask	VLAN ID	DHCP	Organization	Status	Operation
☐	bbb	Service	edewd	193.12.15.10/24	13	Disable	Default organ···	Deplo···	Deployment Details Modify Topology
☑	aaa	Service	edewd	192.10.10.12/24	12	Disable	Default organ···	Deplo···	Deployment Details Modify Topology
☐	edewd-Limited network				0	Disable	Default organ···	Not De···	Deployment Details Reset Modify

Abnormal: Business network: "aaa" is being used by the [campus business network policy] module,Cannot delete

Batch Delete Total 3 Items, Selected 1 Items

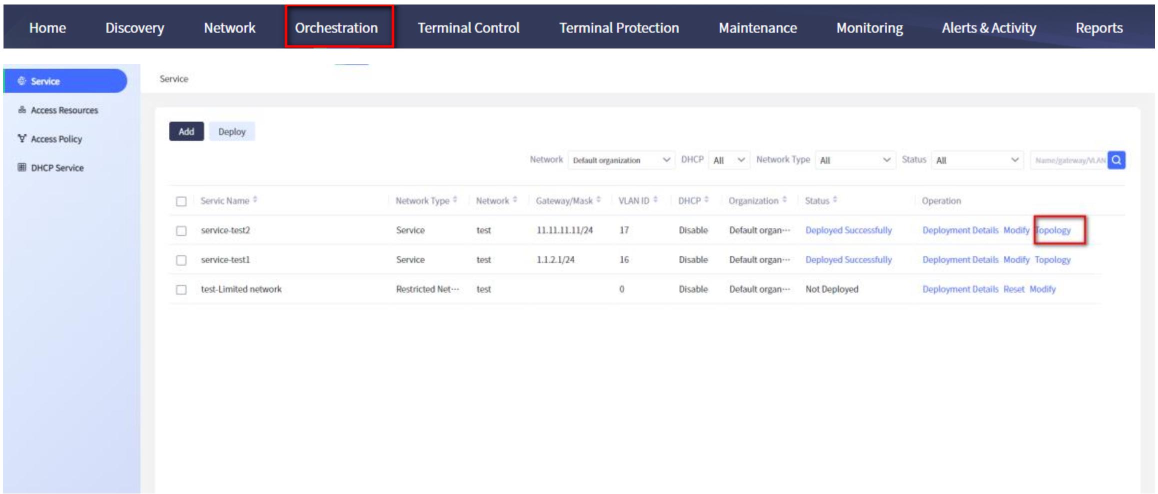
Figure 6.2.3.2 Delete

Note

- The restricted service network cannot be deleted but can only be reset.

6.2.4 Service Network Topology

Click the "Topology" button in the operation column of the service network list or click the "Discovery" at the top, and then, select "Service Network Topology" in the network topology to enter the service network topology interface, as shown in the following figure:



☐	Servic Name	Network Type	Network	Gateway/Mask	VLAN ID	DHCP	Organization	Status	Operation
☐	service-test2	Service	test	11.11.11.11/24	17	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☐	service-test1	Service	test	1.1.2.1/24	16	Disable	Default organ···	Deployed Successfully	Deployment Details Modify Topology
☐	test-Limited network	Restricted Net···	test		0	Disable	Default organ···	Not Deployed	Deployment Details Reset Modify

Figure 6.2.4.1 Click the operation column button to enter the service network topology

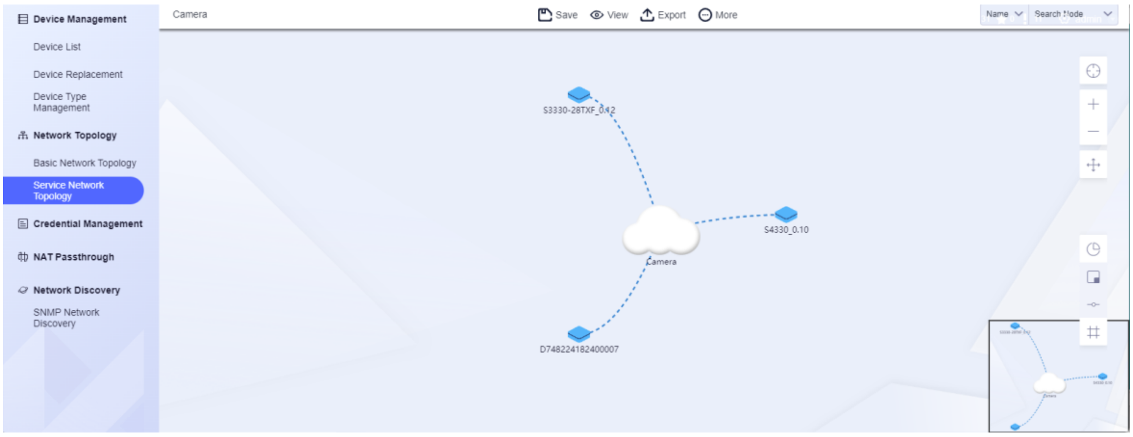


Figure 6.2.1.2 Click “Service Network Topology” to enter the service network topology

6.2.1.1 Function Button Area

Save: Save the layout, display information, editing results, etc. of the current topology.

View: Select the device display information in the topology view (the name (displayed by default), IP)

Export: Export the topology in picture format.

More: Other function options (background setting, font color setting, streamer effect setting, legend description).

- Background setting

The system has three built-in background styles, and supports uploading new background styles through "Upload Materials"; You can click the mouse to select the background style, preview the background style through the "Preview" button, and save the replacement of the background style through the "Use" button, as shown in the following figure.

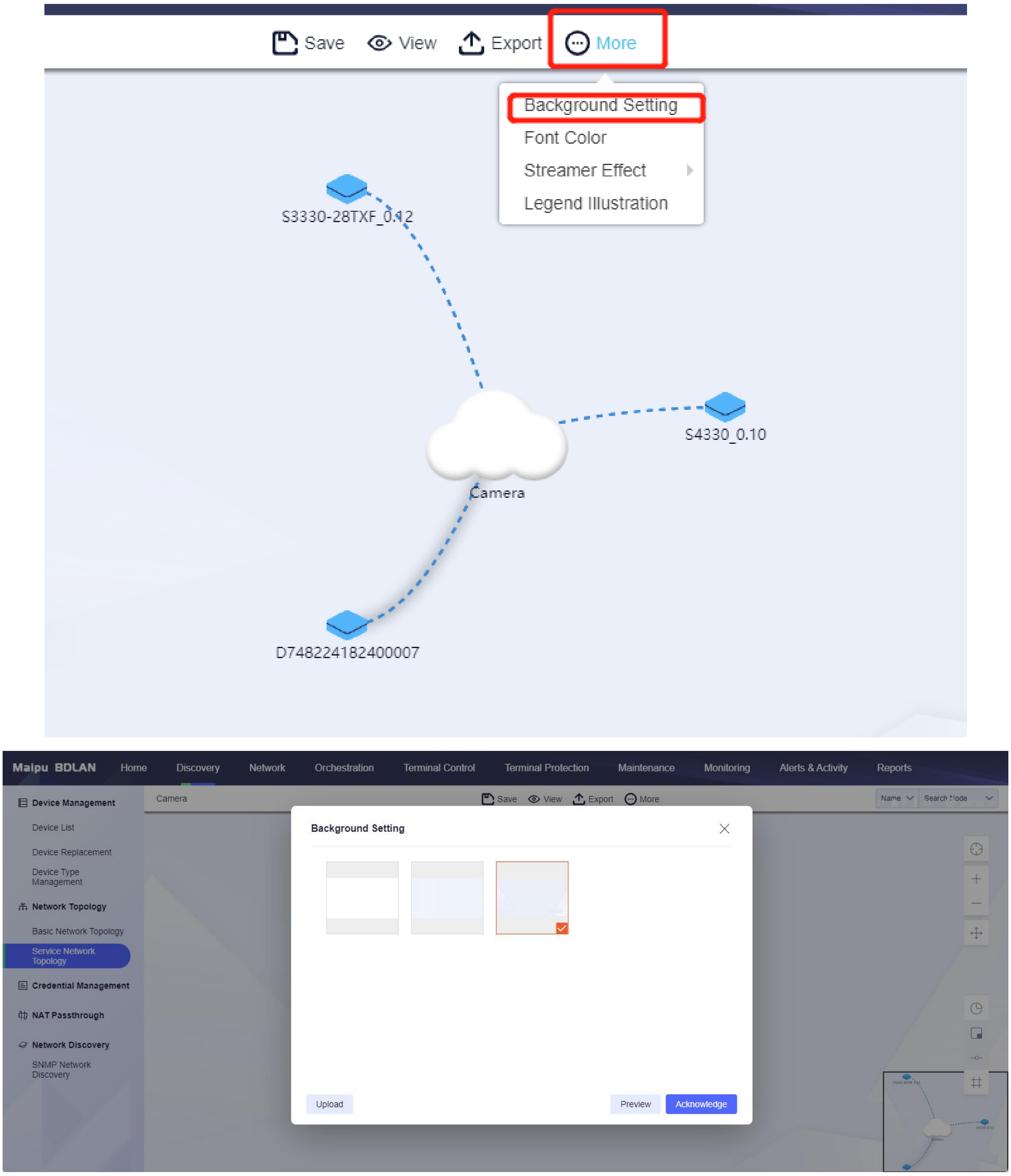


Figure 6.2.1.1.1 Background setting

- Font color settings

Set the font color in the topology view, and 72 colors are available, as shown in the following figure.

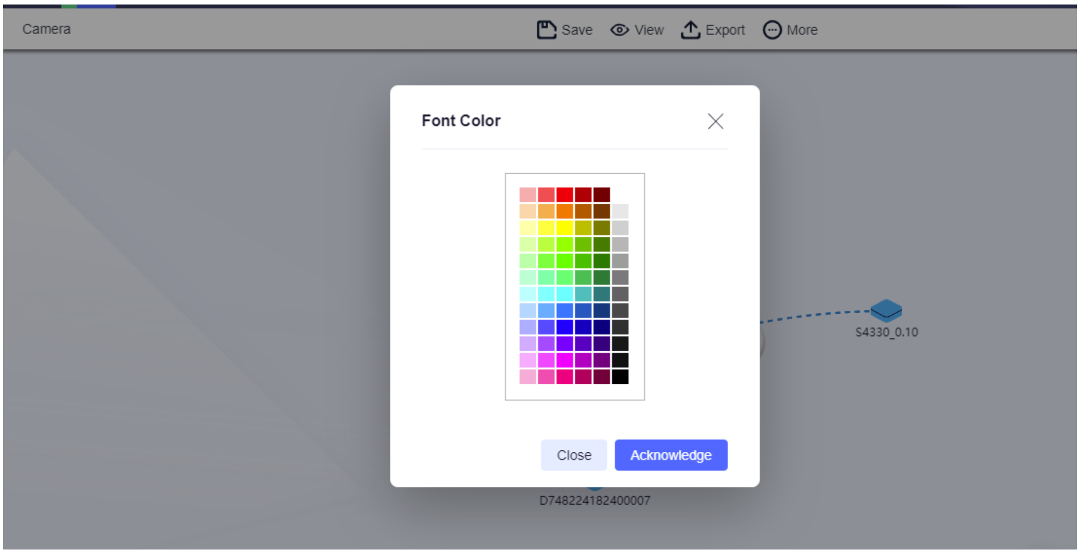


Figure 6.2.1.1.2 Font color settings

- Streamer effect

By setting "Streamer Effect" in the "More" menu, you can set the Enable/Close state of the streamer effect of the topology link, as shown in the figure below.

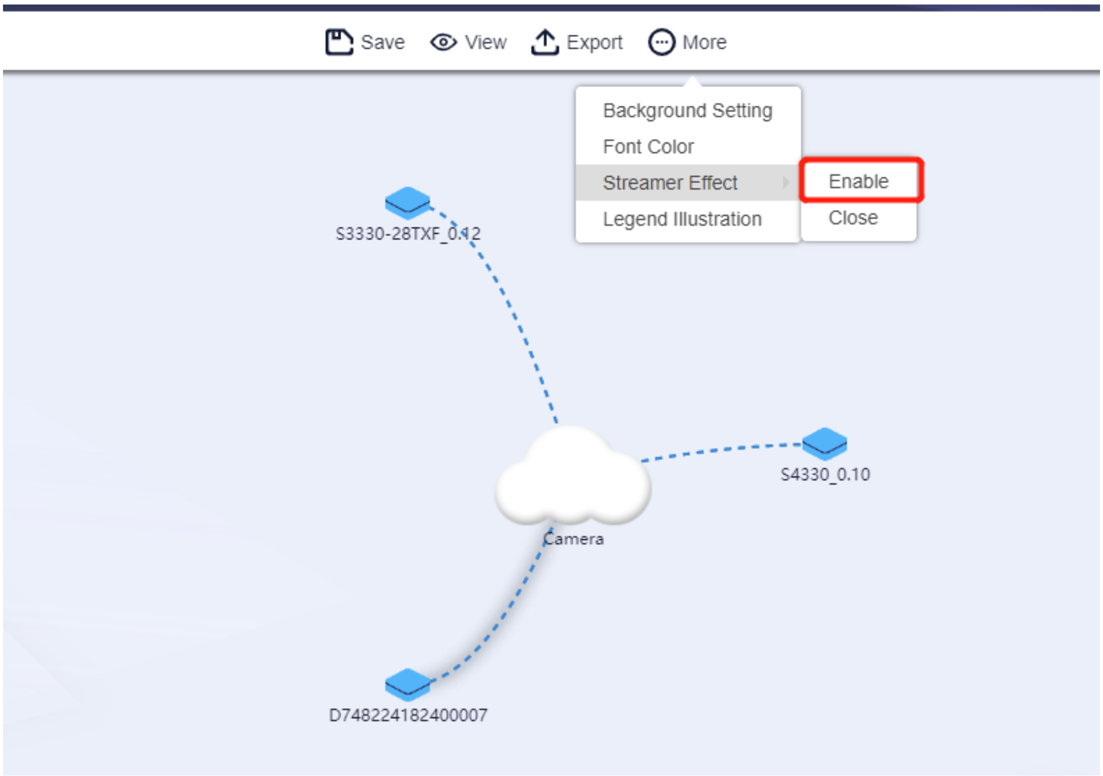


Figure 6.2.1.1.3 Streamer effect setting

- Legend illustration

Click "Legend Illustration" in the "More" icon to view the legend description of the topology view, as shown in the following figure.

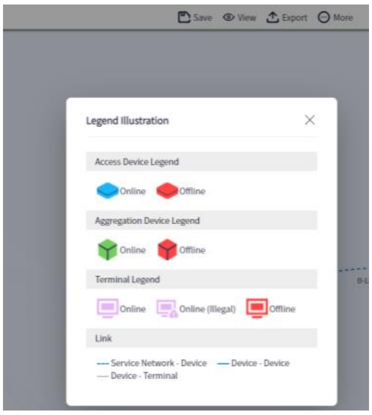


Figure 6.2.1.1.4 Legend description

6.2.1.2 Search Area

In the current topology view range, query the nodes by the name and IP.

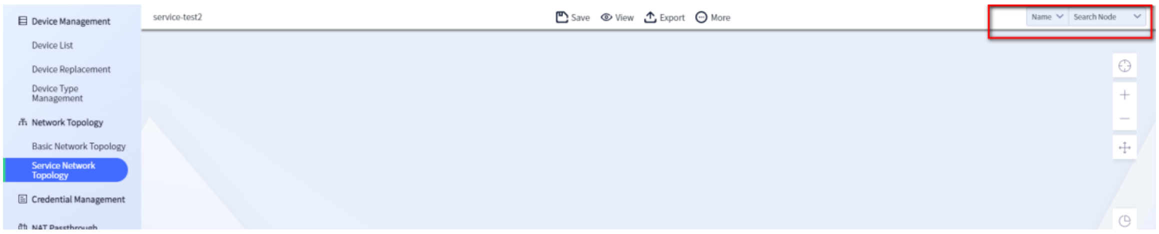


Figure 6.2.1.2.1 Search service network topology node

6.2.1.3 Tools Bar

⊕ : Move the topology view to the center point

+ : Zoom in the topology

— : Zoom out the topology

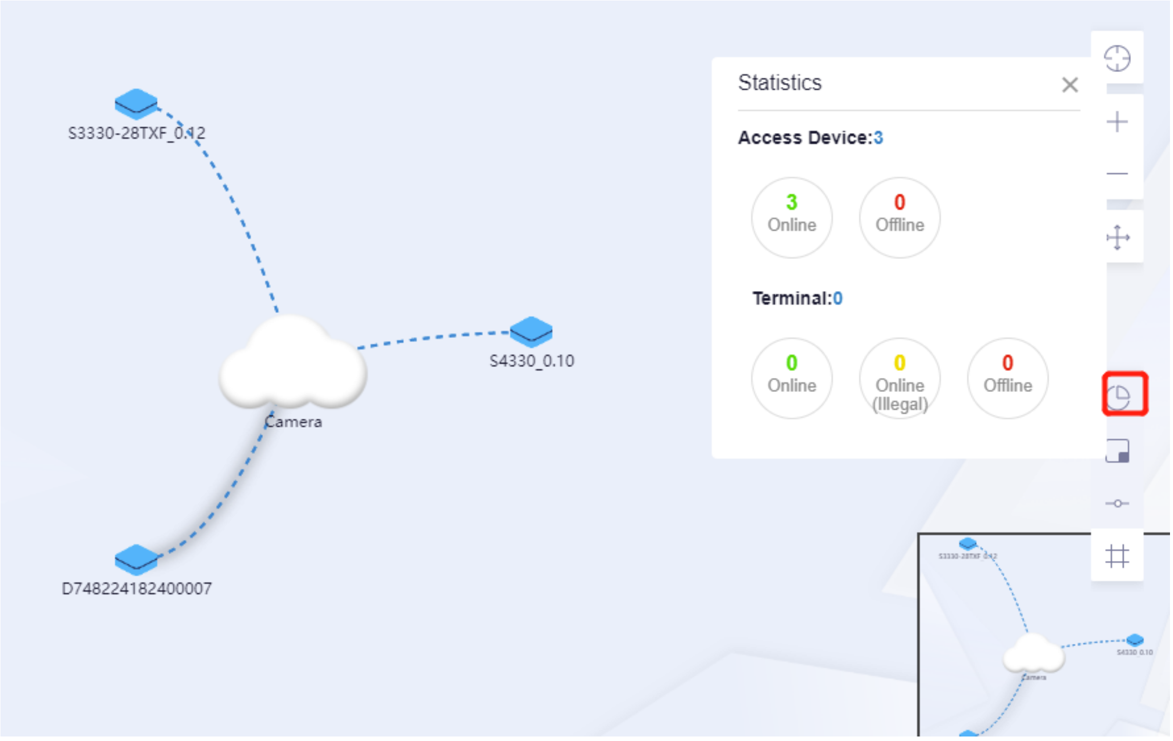
✥ : Topology anchor, mouse drag and drop topology switch

◔ : Display the topology statistics information, and click to pop up the statistics window, as shown in Figure 6.2.1.3.1. Click “Tunnel”, and you can view the tunnel information, as shown in Figure 6.2.1.3.2.

◪ : Turn on/off aerial view

-○- : Open/close the streamer effect

# : Mesh, adding a mesh to the topology background.



Statistics

Access Device:3

3 Online
0 Offline

Terminal:0

0 Online
0 Online (Illegal)
0 Offline

Figure 6.2.1.3.1 Topology statistics

6.2.1.4 Aerial View

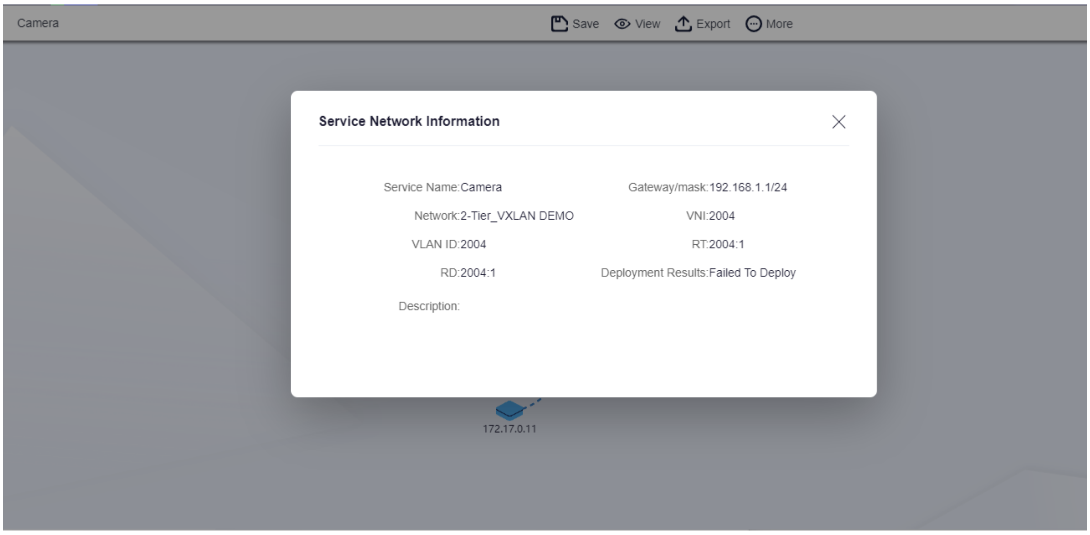
1. By dragging the current screen display area in the aerial view, you can view the part of the topology map that cannot be displayed on the screen.
2. By double-clicking the current screen display area in the aerial view, you can locate the double-click position to the middle of the screen.

6.2.1.5 Right-click Menus

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

- View details:

Right-click the cloud node and click “View Details” to view the details of the service network, as shown in Figure 6.2.1.5.1 below. Some main information of the service network is displayed in the device information box.



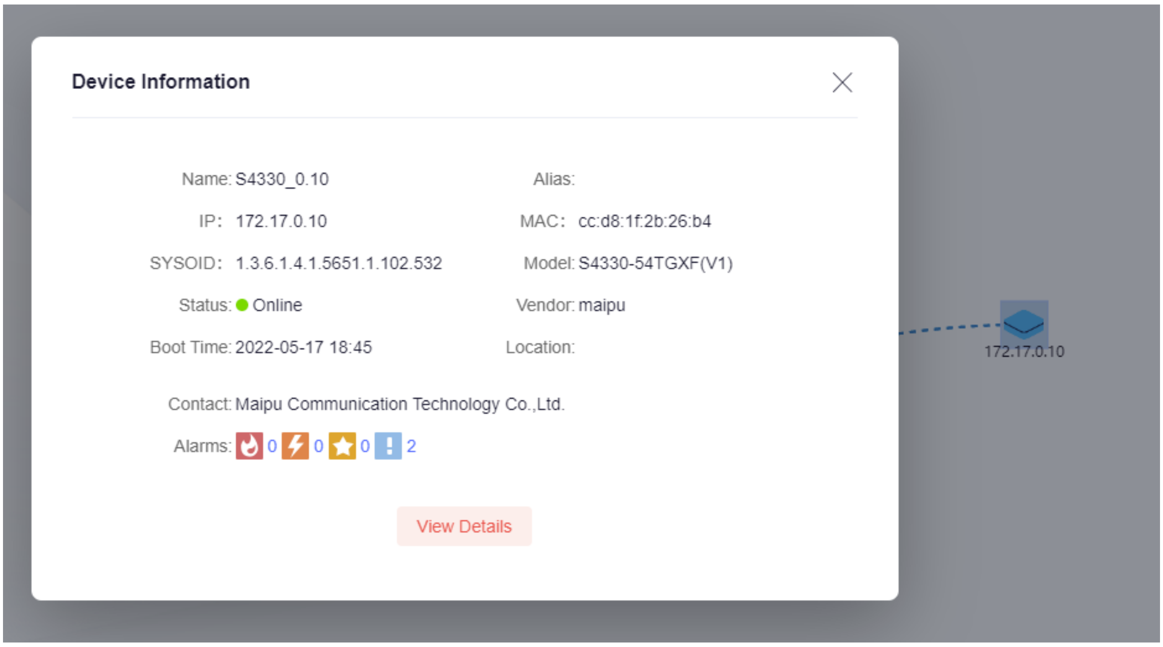
Service Network Information

Service Name:Camera
Gateway/mask:192.168.1.1/24
Network:2-Tier_VXLAN DEMO
VNI:2004
VLAN ID:2004
RT:2004:1
RD:2004:1
Deployment Results:Failed To Deploy
Description:

Figure 6.2.1.5.1 Service network details

- View device details:

Right-click the device node and click “View Details” to view the device information details, as shown in Figure 6.2.1.5.2 below. Some main device information is displayed in the device information box. To view more device information, click **View Details** at the bottom of the device information box.



Device Information

Name: S4330_0.10
Alias:
IP: 172.17.0.10
MAC: cc:d8:1f:2b:26:b4
SYSOID: 1.3.6.1.4.1.5651.1.102.532
Model: S4330-54TGXF(V1)
Status: ● Online
Vendor: maipu
Boot Time: 2022-05-17 18:45
Location:
Contact: Maipu Communication Technology Co.,Ltd.
Alarms: 0 0 0 2

View Details

Figure 6.2.1.5.2 Device details

- View terminal details:

Right click the terminal node and click "View Details" to view the terminal details. Some main information of the terminal is displayed in the terminal information box.

6.3 Access Resources

Click **Access Resources** under the campus resources to enter the main page, as shown in Figure 6.3.1:

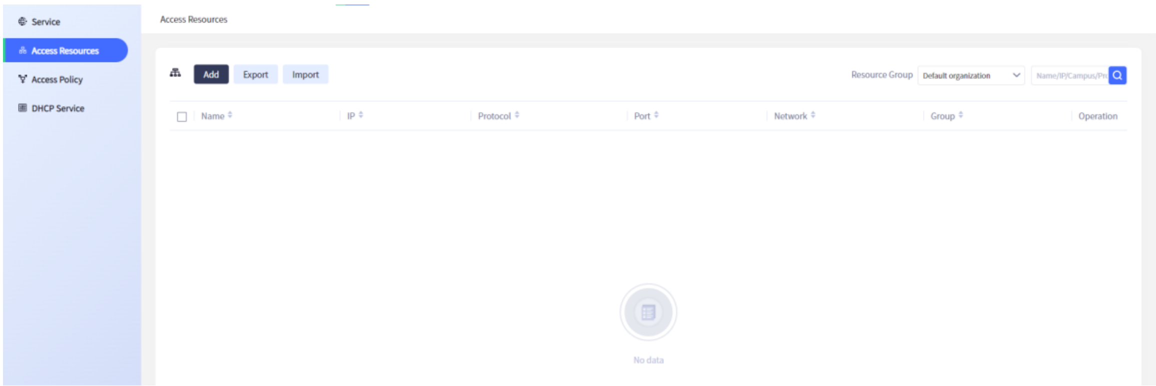
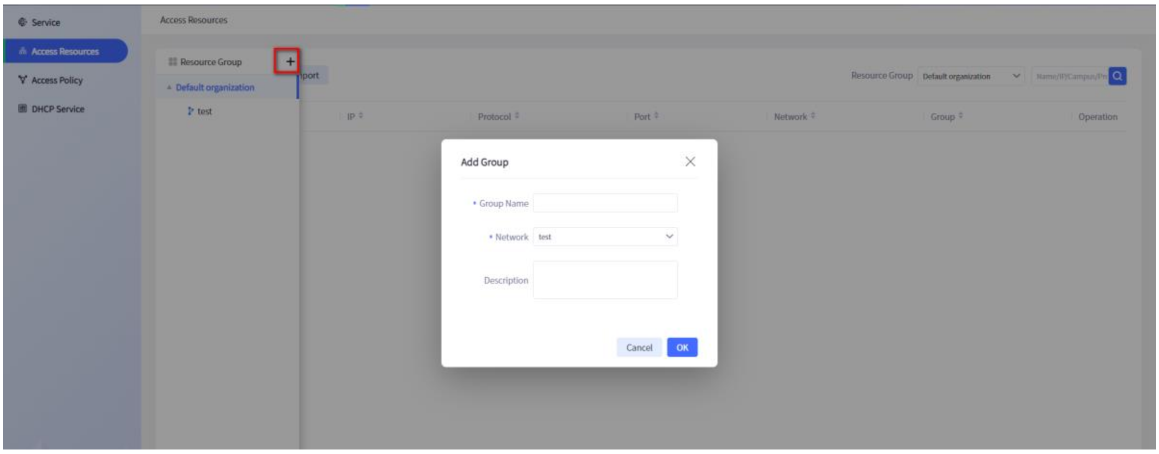


Figure 6.3.1 Access resources

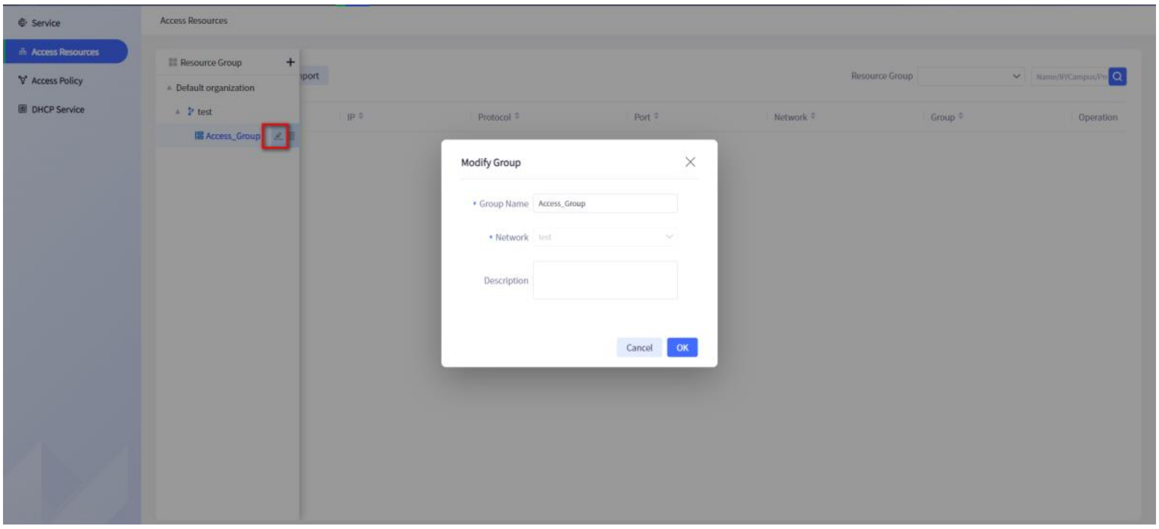
- Add group: Select the campus network in the left tree, and then click the button + to open the **Add Group** window, as shown in Figure 6.3.2 below. Fill in the group name and other relevant information. You can re-select the campus network, and click **OK** to add the access resource group.



* Group Name
* Network test
Description

Figure 6.3.2 Add group

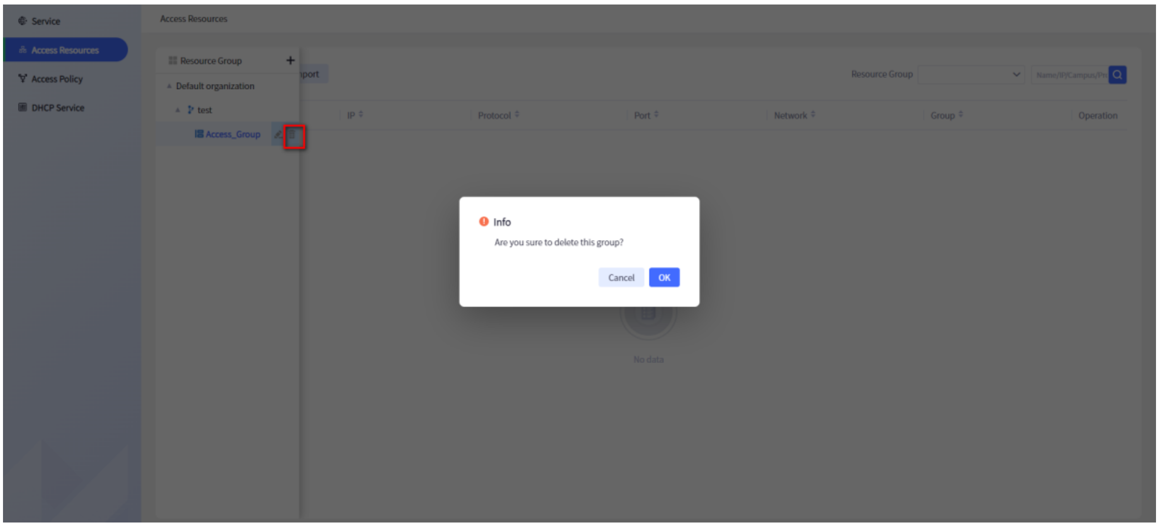
- Modify group: Expand the left tree, find the corresponding group, and click to open the **Modify Group** interface, where you can modify the name and description information, as shown in figure 6.3.3 below.



* Group Name Access_Group
* Network test
Description

Figure 6.3.3 Modify group

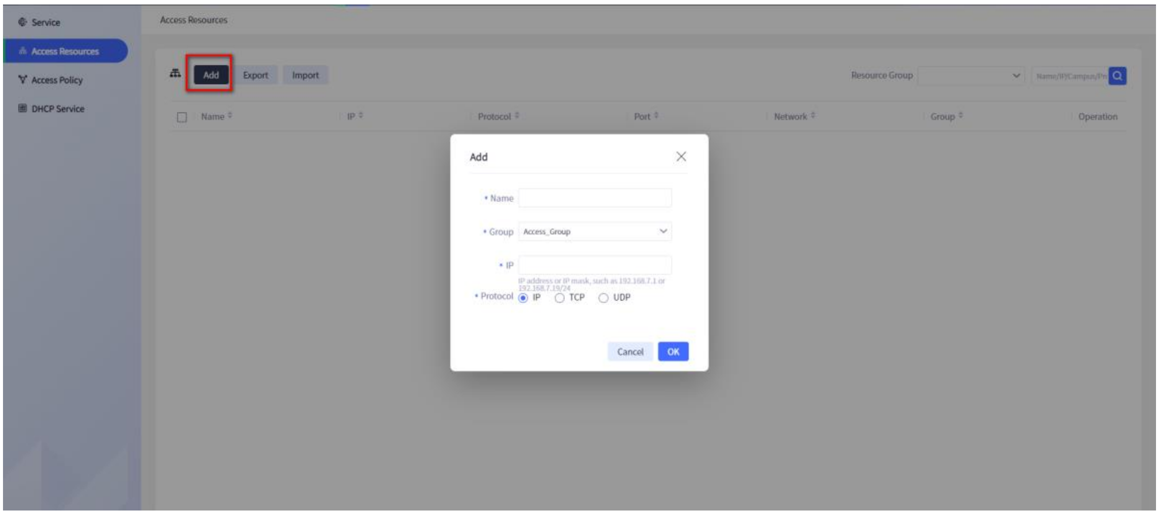
- Delete group: Expand the left tree, find the corresponding group, and click to open the confirm deletion box; Click **OK** to delete the group, or **Cancel** to abort the operation, as shown in Figure 6.3.4; When there are access resources under the group, the group cannot be deleted.



Info
Are you sure to delete this group?

Figure 6.3.4 Delete group

- Add access resource: click the button Add to open the input information box for adding access resource, as shown in figure 6.3.5 below. Fill in the information related to access resource, and click **OK** to save the information.



Add

* Name

* Group Access_Group

* IP

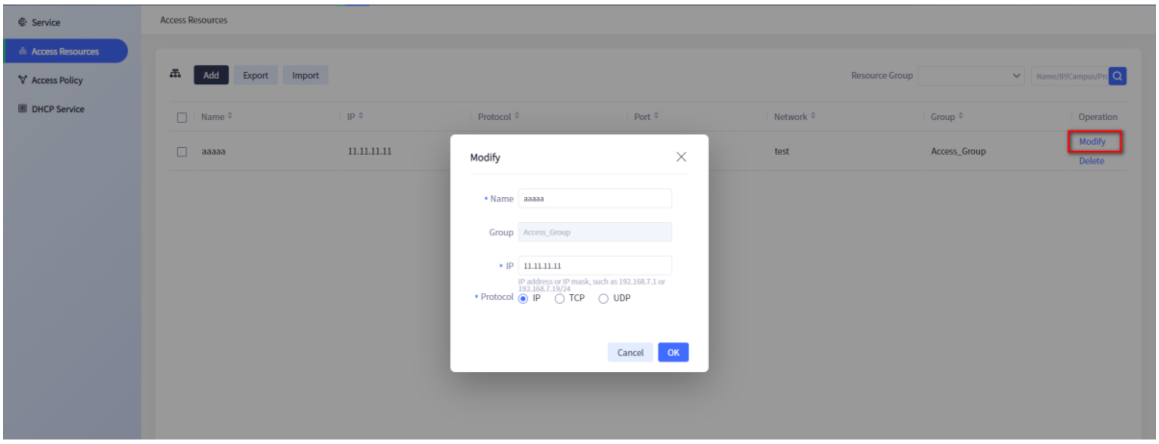
IP address or IP mask, such as 192.168.7.1 or 192.168.7.19/24

* Protocol ● IP ○ TCP ○ UDP

Cancel OK

Figure 6.3.5 Add access resources

- Modify access resource: In the operation column of the list page, click **Modify** to open the window of modifying the access resource grouping information. Modify the relevant information, and click **OK** to save the information, as shown in figure 6.3.6 below:



☐	Name	IP	Protocol	Port	Network	Group	Operation
☐	aaaaa	11.11.11.11			test	Access_Group	Modify Delete

Modify

* Name aaaaa

Group Access_Group

* IP 11.11.11.11

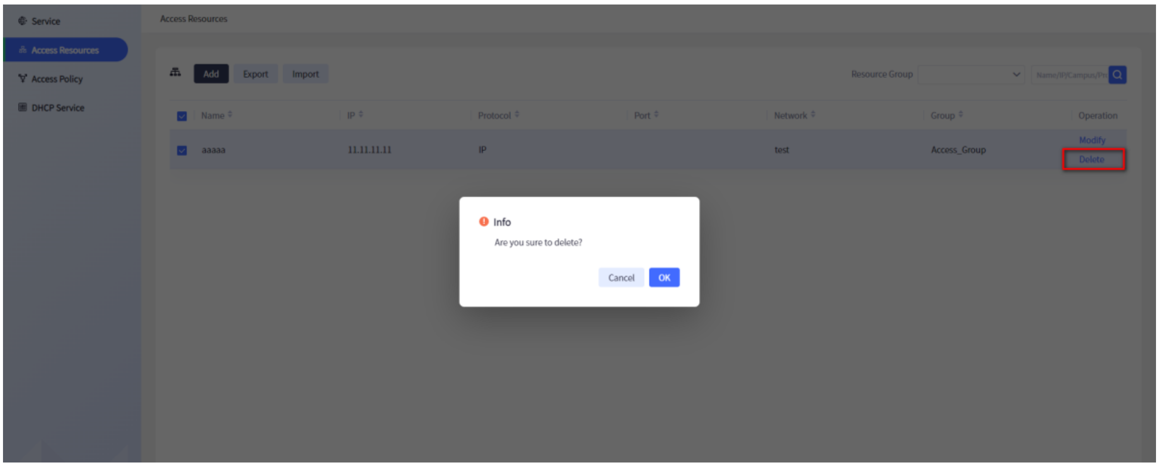
IP address or IP mask, such as 192.168.7.1 or 192.168.7.19/24

* Protocol ● IP ○ TCP ○ UDP

Cancel OK

Figure 6.3.6 Modify the access resources

- Delete access resources: In the operation column of the list page, click "Delete", or check the desired data, and click "Batch delete" below the list to pop up a prompt box, as shown in figure 6.3.7 and figure 6.3.8 below. Click **OK** to delete the access resource.

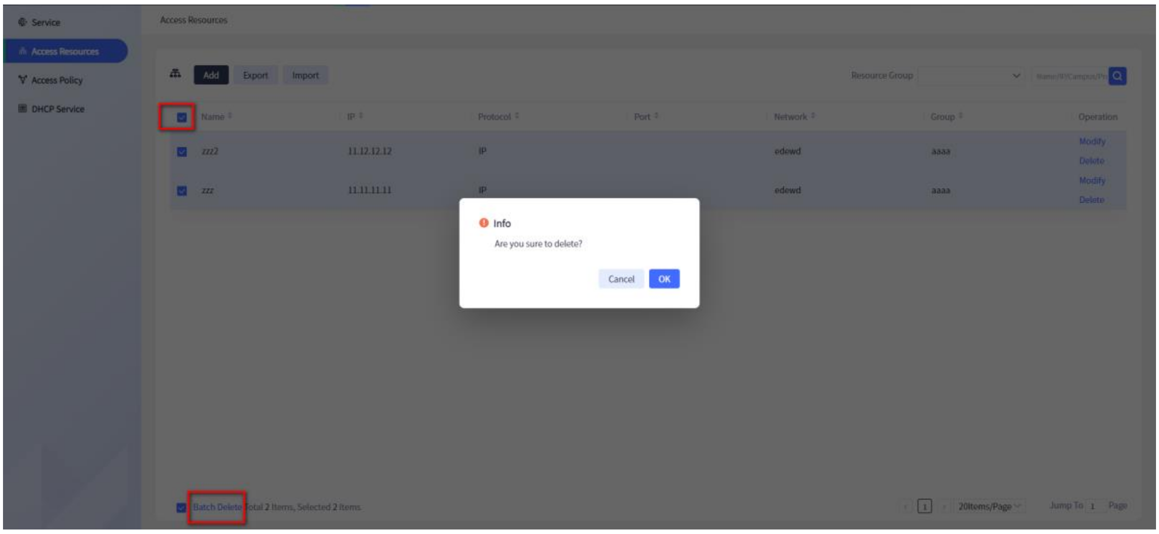


☑	Name	IP	Protocol	Port	Network	Group	Operation
☑	aaaaa	11.11.11.11	IP		test	Access_Group	Modify Delete

Info

Are you sure to delete?

Figure 6.3.7 Delete access resources



☑	Name	IP	Protocol	Port	Network	Group	Operation
☑	zzz2	11.12.12.12	IP		edewd	aaaa	Modify Delete
☑	zzz	11.11.11.11	IP		edewd	aaaa	Modify Delete

Info

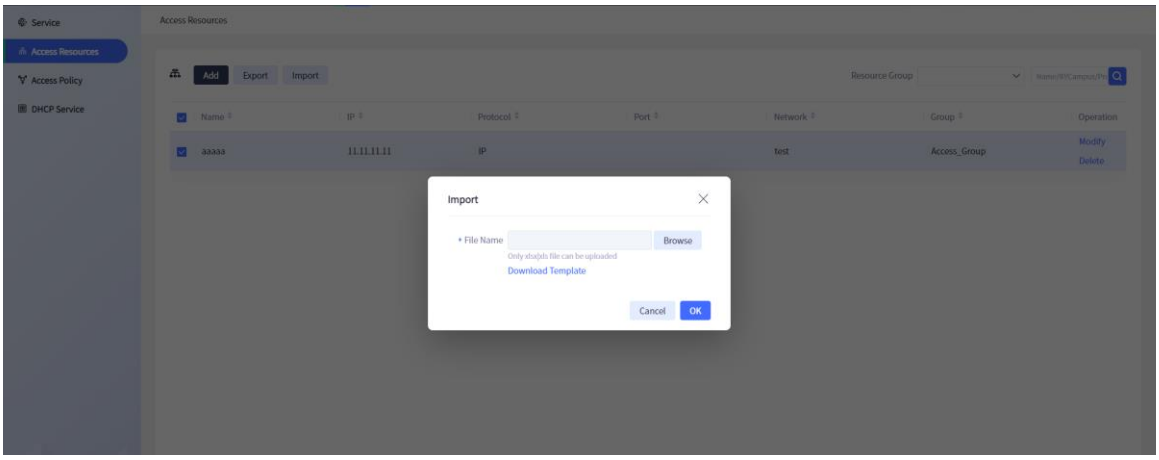
Are you sure to delete?

☑ Batch Delete Total 2 Items, Selected 2 Items

Figure 6.3.8 Batch delete access resources

- Export access resources: Click Export to export all the found data. You can select data, and click **Export** to export the selected data.

- Import access resources: click Import to open the **Import** window, as shown in figure 6.3.8: you can choose **Download Template** or import files directly.



☑	Name	IP	Protocol	Port	Network	Group	Operation
☑	aaaaa	11.11.11.11	IP		test	Access_Group	Modify Delete

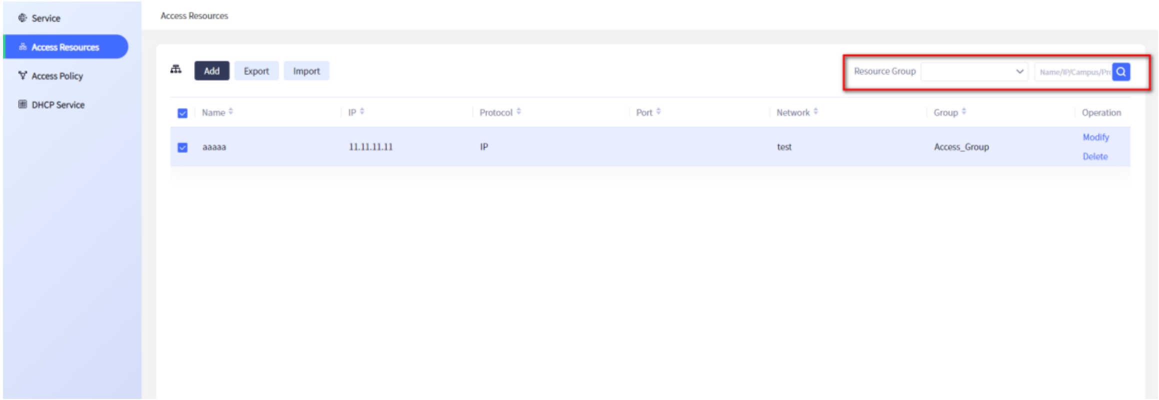
Import

* File Name

Only xlsx|xls file can be uploaded

Figure 6.3.8 Import access resources

- Query access resources: click 🔍 on the right, enter query criteria, and click **Query** to find data. Fuzzy query is supported. At the same time, click this column in the title bar of the first column of the list to sort the data in this column.

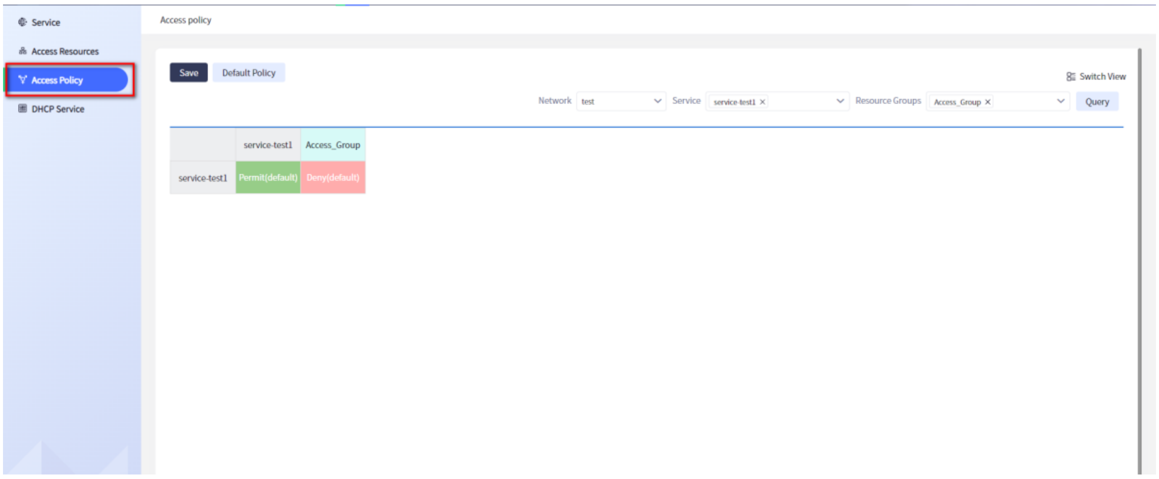


☑	Name	IP	Protocol	Port	Network	Group	Operation
☑	aaaaa	11.11.11.11	IP		test	Access_Group	Modify Delete

Figure 6.3.9 Query access resources

6.4 Access Policy

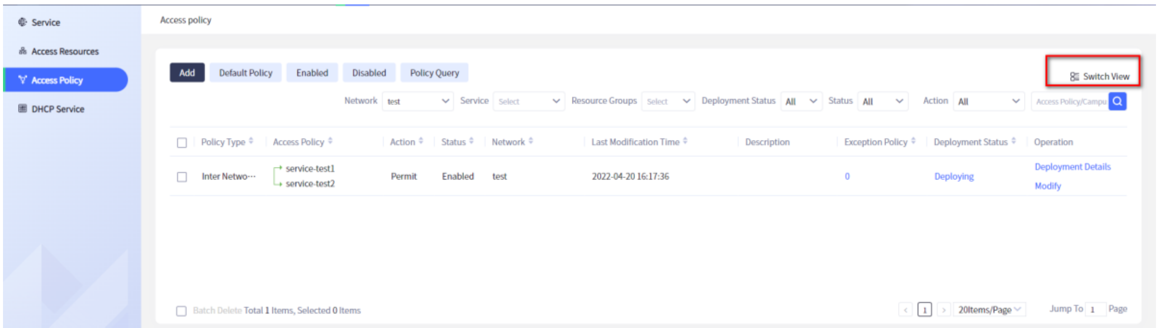
The main function of the service access policy module is to establish policies for each service network, including permit and deny. You can also establish permit and deny policies in the service network and access resource groups. By default, there are three types of default policies, permit between service networks and within service networks, deny for accessible resources, which can be modified. The display method is divided into matrix view and list view:



Network: test
Service: service-test1
Resource Groups: Access_Group

	service-test1	Access_Group
service-test1	Permit(default)	Deny(default)

Figure 6.4.1 Matrix view of the service access policy



Network: test
Service: Select
Resource Groups: Select
Deployment Status: All
Status: All
Action: All

☐	Policy Type	Access Policy	Action	Status	Network	Last Modification Time	Description	Exception Policy	Deployment Status	Operation
☐	Inter Netwo···	service-test1 service-test2	Permit	Enabled	test	2022-04-20 16:17:36		0	Deploying	Deployment Details Modify

Total 1 Items, Selected 0 Items

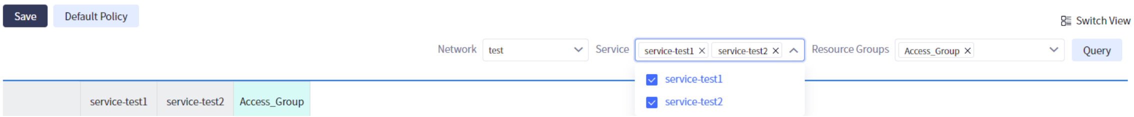
Figure 6.4.2 List view of the service access policy

6.4.1 Matrix View

Interface Distribution

The interface consists of two parts, the function menu bar on the upper side and the data display on the lower side:

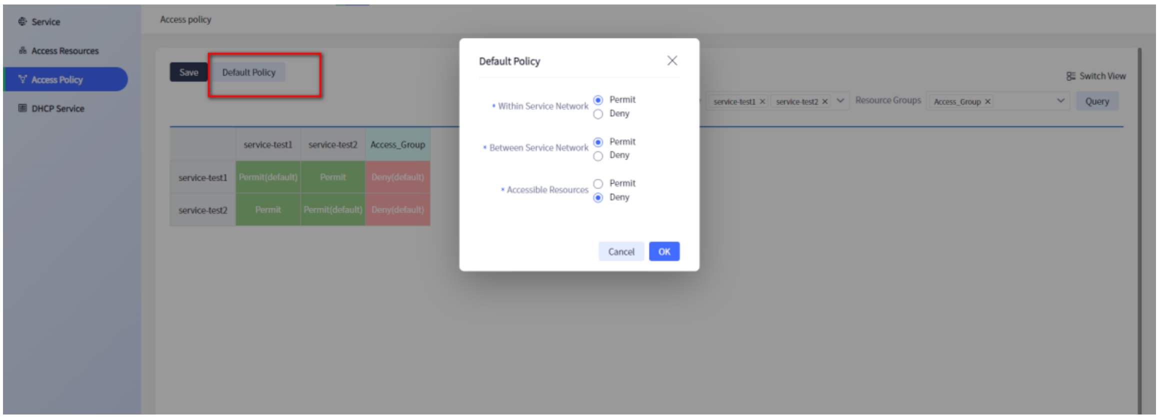
The function menu bar contains the selection boxes for campus planning network, service network and access resource group, as well as the switch view button, save button and default policy button:



Network: test
Service: service-test1, service-test2
☑ service-test1
☑ service-test2
Resource Groups: Access_Group

	service-test1	service-test2	Access_Group

Figure 6.4.1.1 Matrix view function menu bar



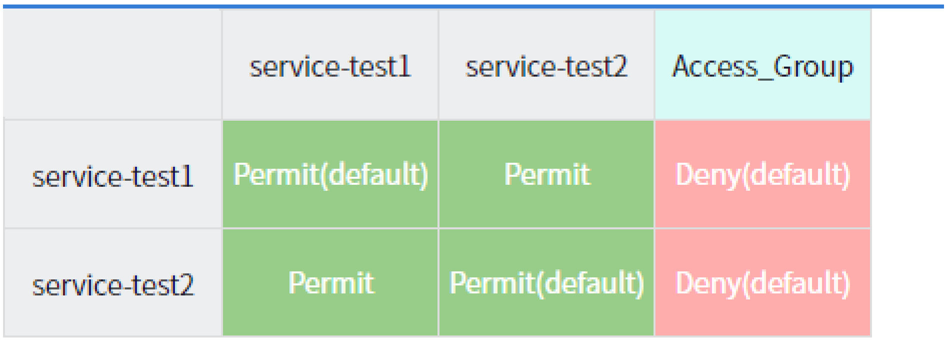
Default Policy

- Within Service Network: ● Permit ○ Deny
- Between Service Network: ● Permit ○ Deny
- Accessible Resources: ○ Permit ● Deny

Figure 6.4.1.2 Default policy setting area

Policy Matrix

The matrix will display the service network selected in the menu bar as a matrix:



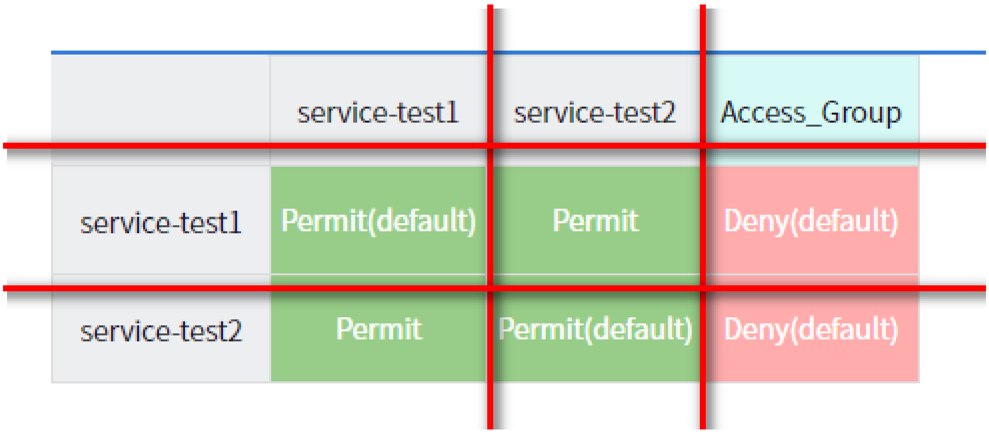
	service-test1	service-test2	Access_Group
service-test1	Permit(default)	Permit	Deny(default)
service-test2	Permit	Permit(default)	Deny(default)

Figure 6.4.1.3 Matrix diagram

Add Policy

Place the mouse over the box where the two service networks that need to distribute the policy intersect, and two symbols ✓ ⓘ will appear,

Click ✓ to issue the permit policy and click ⓘ to issue the deny policy:

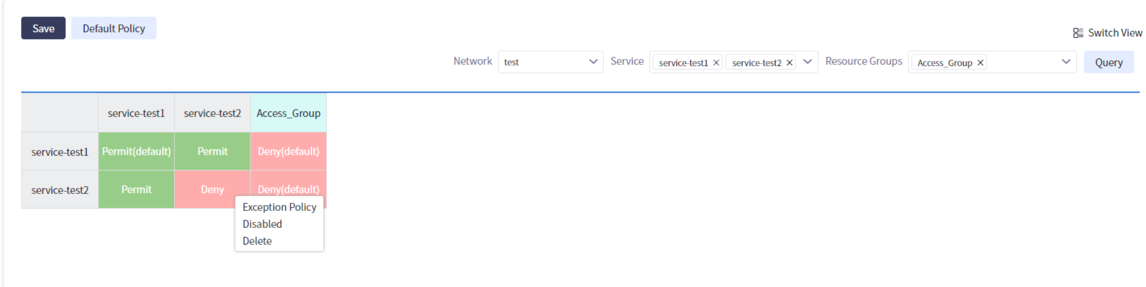


	service-test1	service-test2	Access_Group
service-test1	Permit(default)	Permit	Deny(default)
service-test2	Permit	Permit(default)	Deny(default)

Figure 6.4.1.4 Add policy

Modify Policy

Place the mouse over the desired policy, and three symbols ✓ ⓘ ••• will appear. Click ✓ to modify it to the permit policy, click ⓘ to modify it to the deny policy, and click ••• to open a pop-up window:



Network: test
Service: service-test1 × service-test2 ×
Resource Groups: Access_Group ×

	service-test1	service-test2	Access_Group
service-test1	Permit(default)	Permit	Deny(default)
service-test2	Permit	Deny	Deny(default)

Figure 6.4.1.5 Modify policy

Enable: Controls whether the policy is enabled

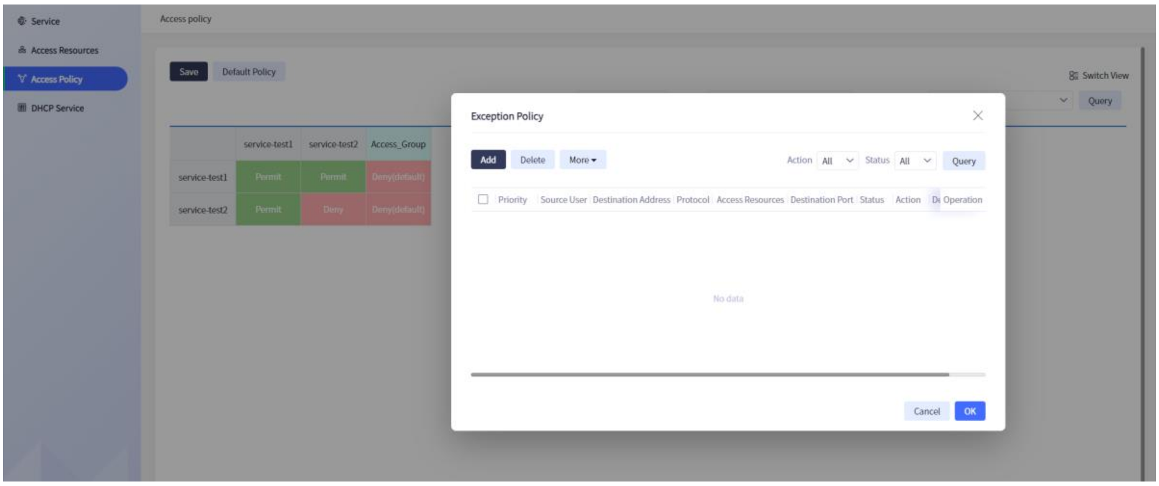
Disable: Controls whether the policy is disabled

Delete: Click to delete the policy

Exception policy: After policies are issued to two service networks, policies can be made for the terminals connected to the service network

Exception Policy

Place the mouse over the desired policy, and three symbols ✓ ⓘ ••• will appear. Click ••• , and a pop-up window will appear. Click the exception policy in the pop-up window, and a pop-up window of the exception policy list will appear:



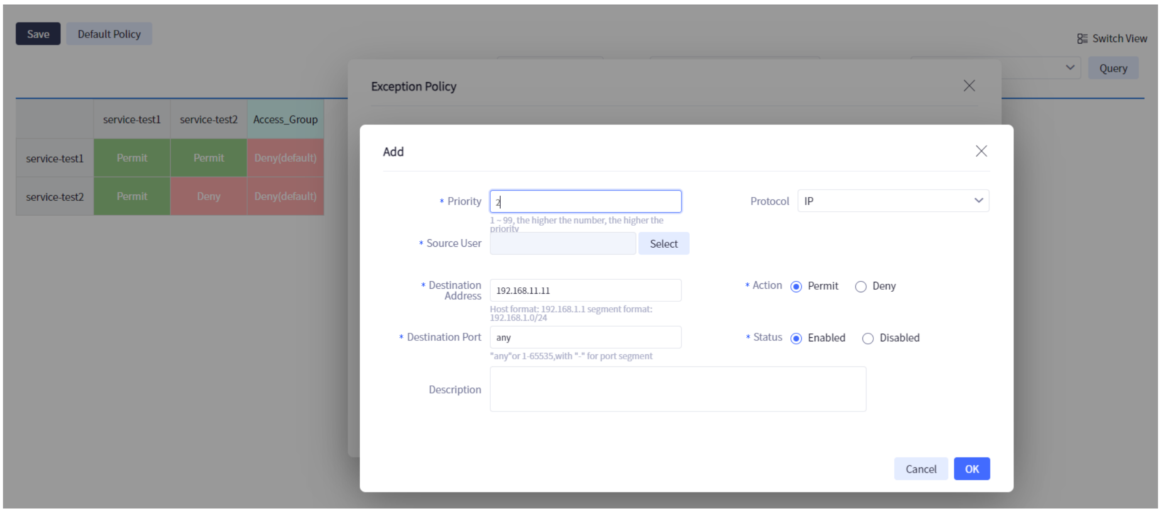
Action: All
Status: All

☐	Priority	Source User	Destination Address	Protocol	Access Resources	Destination Port	Status	Action	De	Operation

Figure 6.4.1.6 Exception policy list

Add Exception Policy

Click the **Add** button to open the pop-up window of adding the exception policy, including priority, protocol, source user, destination address, action, status, description, **OK** button and **cancel** button. After entering data, click the **OK** button to save the policy. If you need to give up adding, click the **Cancel** button:

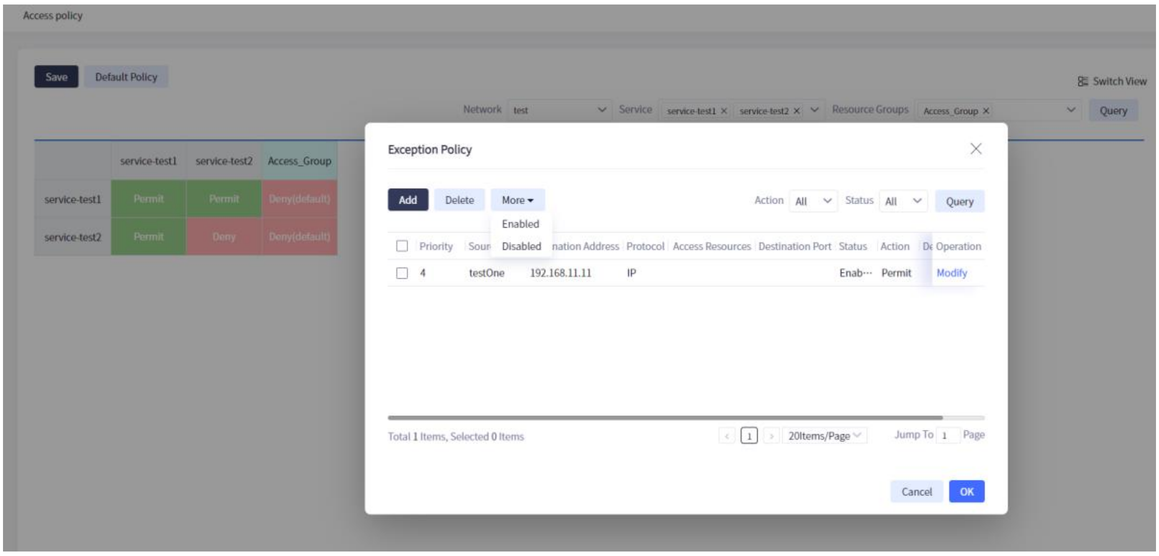


* Priority: 2 (1 ~ 99, the higher the number, the higher the priority)
Protocol: IP
* Source User:
* Destination Address: 192.168.11.11 (Host format: 192.168.1.1 segment format: 192.168.1.0/24)
* Action: ● Permit ○ Deny
* Destination Port: any ("any"or 1-65535,with "-" for port segment)
* Status: ● Enabled ○ Disabled
Description:

Figure 6.4.1.7 Add the exception policy

Enable/Disable/Delete Exception Policy

Select a desired exception policy, and click the enable/disable/delete button above to enable/disable/delete the exception policy. When disabling/deleting the policy, the policy on the device will be deleted synchronously:



Network: test Service: service-test1, service-test2 Resource Groups: Access_Group

Action: All Status: All

☐	Priority	Sour	nation Address	Protocol	Access Resources	Destination Port	Status	Action	De	Operation
☐	4	testOne	192.168.11.11	IP			Enab···	Permit		Modify

Total 1 Items, Selected 0 Items 1 20Items/Page Jump To 1 Page

Figure 6.4.1.8 Enable/disable/delete exception policy

Note

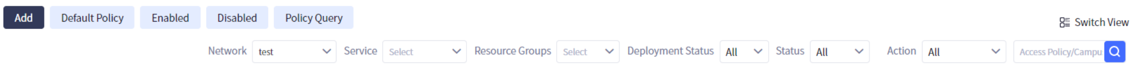
- The restricted network does not support exception policy settings, that is, the exception policy cannot be established on the restricted service network.
- After all operations of the matrix view are completed, you need to click **Save**.

6.4.2 List View

Interface Distribution

The interface consists of two parts, the function menu bar on the upper side and the data display on the lower side:

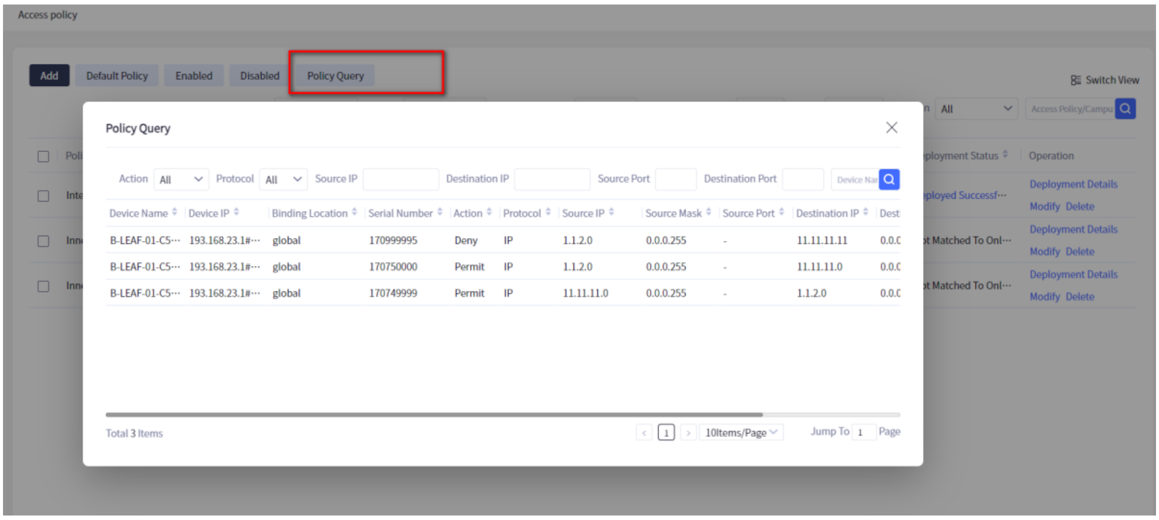
The function menu bar contains the selection boxes of campus planning network, service network and access resource group, deployment status, status, action fuzzy query, and switch view buttons, enable button, disable button, default policy button, and policy query button:



Network: test
Service: Select
Resource Groups: Select
Deployment Status: All
Status: All
Action: All

Figure 6.4.2.1 List view function menu bar

Policy query button: click this button to open a policy query pop-up window, where you can query the policy according to various attributes of the policy:



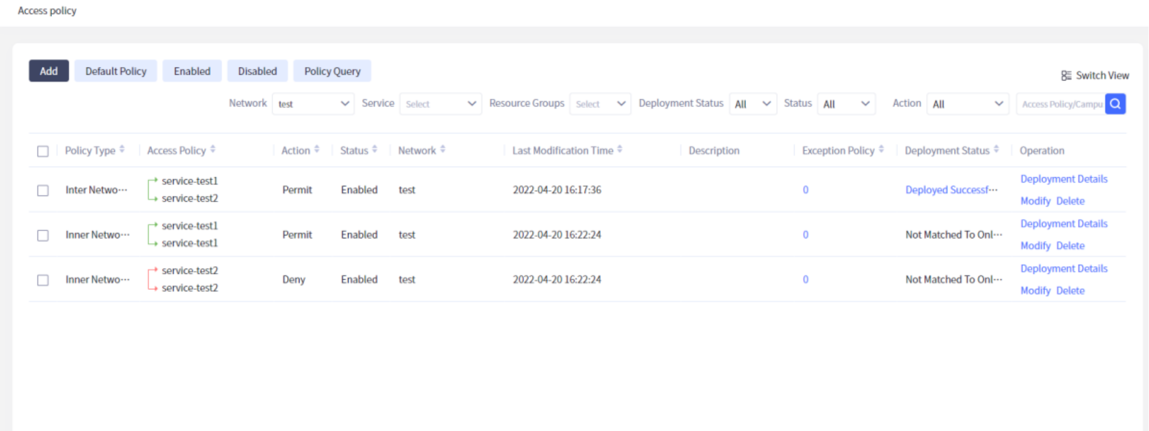
Action: All
Protocol: All
Source IP:
Destination IP:
Source Port:
Destination Port:

Device Name	Device IP	Binding Location	Serial Number	Action	Protocol	Source IP	Source Mask	Source Port	Destination IP	Dest
B-LEAF-01-C5···	193.168.23.1#···	global	170999995	Deny	IP	1.1.2.0	0.0.0.255	-	11.11.11.11	0.0.0
B-LEAF-01-C5···	193.168.23.1#···	global	170750000	Permit	IP	1.1.2.0	0.0.0.255	-	11.11.11.0	0.0.0
B-LEAF-01-C5···	193.168.23.1#···	global	170749999	Permit	IP	11.11.11.0	0.0.0.255	-	1.1.2.0	0.0.0

Figure 6.4.2.2 Policy query list

Policy List

The policies distributed between the current service networks will be displayed in the list:

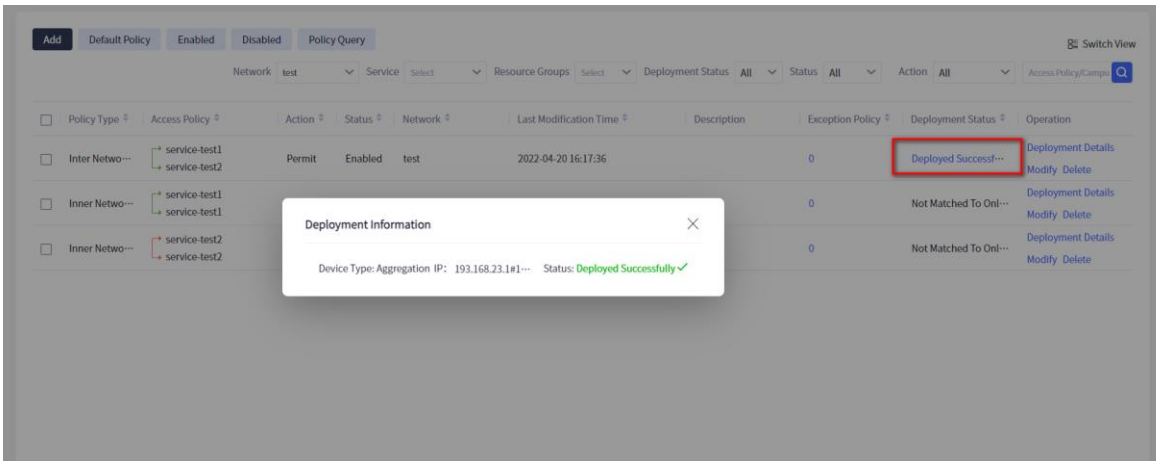


Network: test
Service: Select
Resource Groups: Select
Deployment Status: All
Status: All
Action: All

☐	Policy Type	Access Policy	Action	Status	Network	Last Modification Time	Description	Exception Policy	Deployment Status	Operation
☐	Inter Netwo···	service-test1 service-test2	Permit	Enabled	test	2022-04-20 16:17:36		0	Deployed Successf···	Deployment Details Modify Delete
☐	Inner Netwo···	service-test1 service-test1	Permit	Enabled	test	2022-04-20 16:22:24		0	Not Matched To Onl···	Deployment Details Modify Delete
☐	Inner Netwo···	service-test2 service-test2	Deny	Enabled	test	2022-04-20 16:22:24		0	Not Matched To Onl···	Deployment Details Modify Delete

Figure 6.4.2.3 Policy list

Click deployment status in the list: display the real deployment status of the policy distributed to the device:



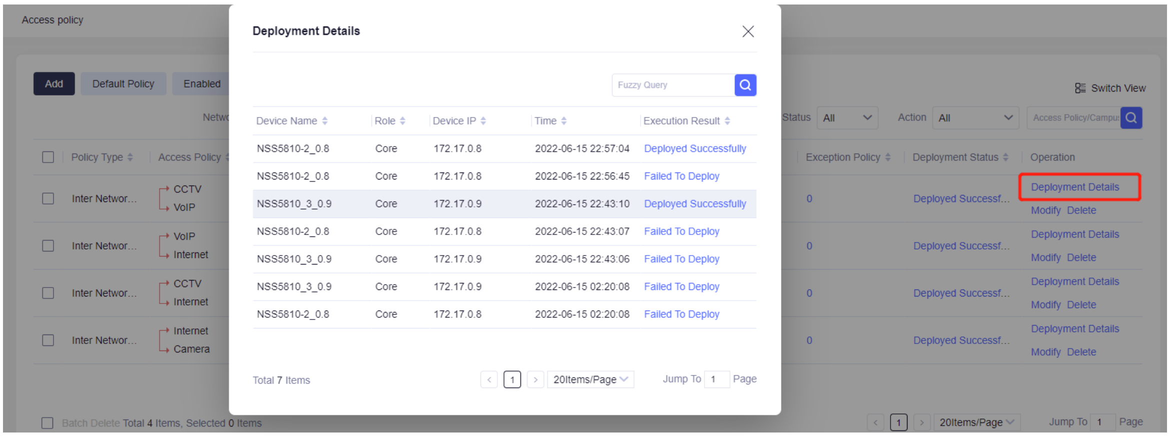
☐	Policy Type	Access Policy	Action	Status	Network	Last Modification Time	Description	Exception Policy	Deployment Status	Operation
☐	Inter Netwo···	service-test1 service-test2	Permit	Enabled	test	2022-04-20 16:17:36		0	Deployed Successf···	Deployment Details Modify Delete
☐	Inner Netwo···	service-test1 service-test1						0	Not Matched To Onl···	Deployment Details Modify Delete
☐	Inner Netwo···	service-test2 service-test2						0	Not Matched To Onl···	Deployment Details Modify Delete

Deployment Information

Device Type: Aggregation IP: 193.168.23.1#1··· Status: Deployed Successfully ✓

Figure 6.4.2.4 Deployment status

Click the deployment details in the operation column of the list, and a display box will pop up to display the details of the policy deployment:



Deployment Details

Device Name	Role	Device IP	Time	Execution Result
NSS5810-2_0.8	Core	172.17.0.8	2022-06-15 22:57:04	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	2022-06-15 22:56:45	Failed To Deploy
NSS5810_3_0.9	Core	172.17.0.9	2022-06-15 22:43:10	Deployed Successfully
NSS5810-2_0.8	Core	172.17.0.8	2022-06-15 22:43:07	Failed To Deploy
NSS5810_3_0.9	Core	172.17.0.9	2022-06-15 22:43:06	Failed To Deploy
NSS5810_3_0.9	Core	172.17.0.9	2022-06-15 02:20:08	Failed To Deploy
NSS5810-2_0.8	Core	172.17.0.8	2022-06-15 02:20:08	Failed To Deploy

Total 7 Items 1 20Items/Page Jump To 1 Page

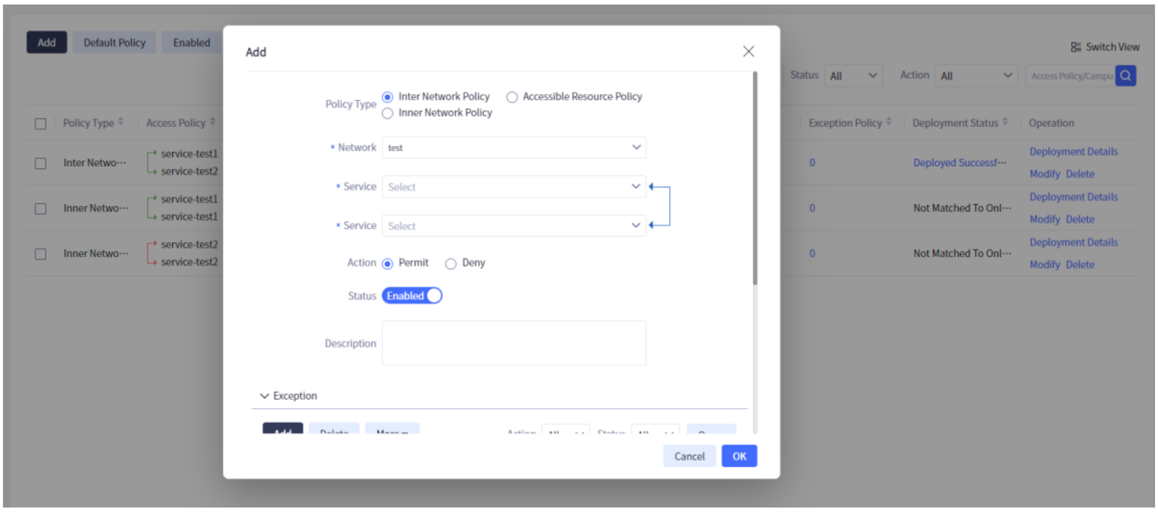
Batch Delete Total 4 Items, Selected 0 Items

Figure 6.4.2.5 Policy deployment details

Add Policy

Click the **Add** button at the top of the interface to open the **Add** interface.

After setting the policy type, network, service, action, status and description, click **OK** to complete the policy addition. Exception policies can be added at the same time:



Add

Policy Type ● Inter Network Policy ○ Accessible Resource Policy ○ Inner Network Policy

* Network: test

* Service: Select

* Service: Select

Action ● Permit ○ Deny

Status: Enabled

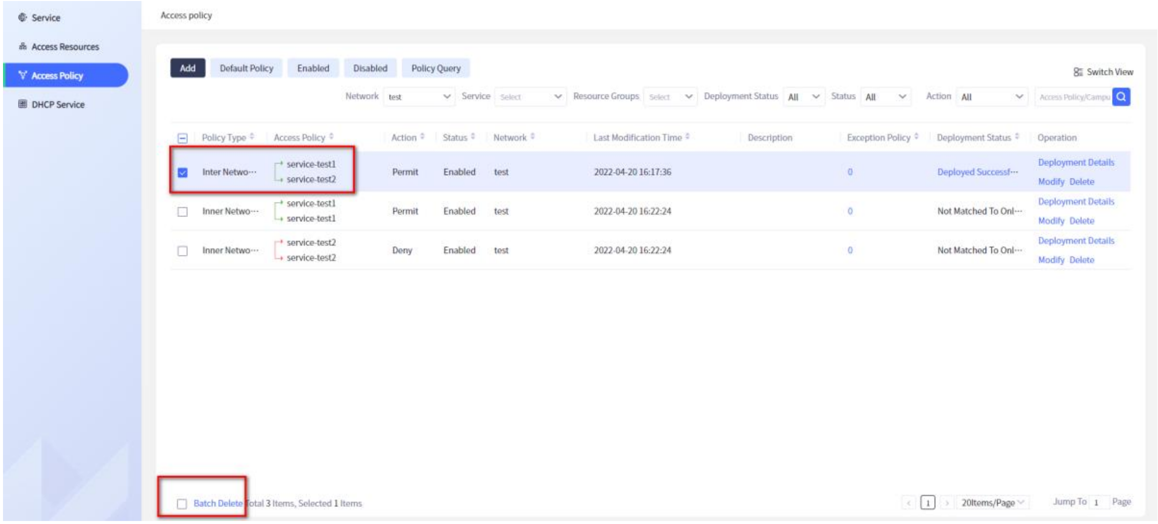
Description

Figure 6.4.2.6 Policy deployment status

Delete Policy

Deletion can be divided into batch deletion and single deletion. After deleting a policy, it will be restored to the corresponding default policy configuration.

Batch delete: Select desired policies and click the **Batch Delete** button below:



Network: test | Service: Select | Resource Groups: Select | Deployment Status: All | Status: All | Action: All

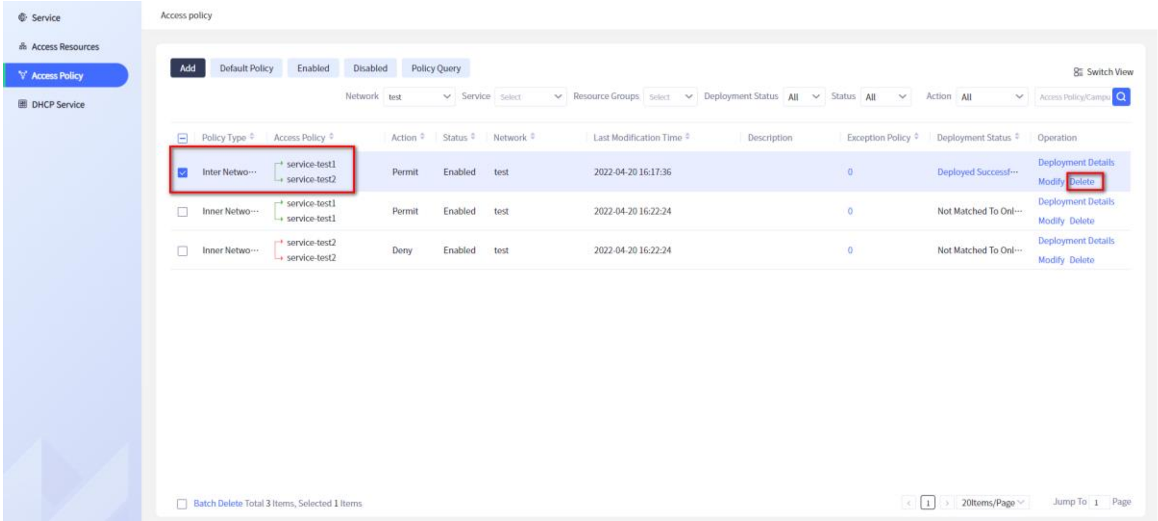
☐	Policy Type	Access Policy	Action	Status	Network	Last Modification Time	Description	Exception Policy	Deployment Status	Operation
☑	Inter Netwo···	service-test1 service-test2	Permit	Enabled	test	2022-04-20 16:17:36		0	Deployed Successf···	Deployment Details Modify Delete
☐	Inner Netwo···	service-test1 service-test1	Permit	Enabled	test	2022-04-20 16:22:24		0	Not Matched To Onl···	Deployment Details Modify Delete
☐	Inner Netwo···	service-test2 service-test2	Deny	Enabled	test	2022-04-20 16:22:24		0	Not Matched To Onl···	Deployment Details Modify Delete

☐ Batch Delete Total 3 Items, Selected 1 Items

1 | 20Items/Page | Jump To 1 Page

Figure 6.4.2.7 Batch delete policies

Single delete: Click **Delete** in the operation column of a desired policy.



Network: test | Service: Select | Resource Groups: Select | Deployment Status: All | Status: All | Action: All

☐	Policy Type	Access Policy	Action	Status	Network	Last Modification Time	Description	Exception Policy	Deployment Status	Operation
☑	Inter Netwo···	service-test1 service-test2	Permit	Enabled	test	2022-04-20 16:17:36		0	Deployed Successf···	Deployment Details Modify Delete
☐	Inner Netwo···	service-test1 service-test1	Permit	Enabled	test	2022-04-20 16:22:24		0	Not Matched To Onl···	Deployment Details Modify Delete
☐	Inner Netwo···	service-test2 service-test2	Deny	Enabled	test	2022-04-20 16:22:24		0	Not Matched To Onl···	Deployment Details Modify Delete

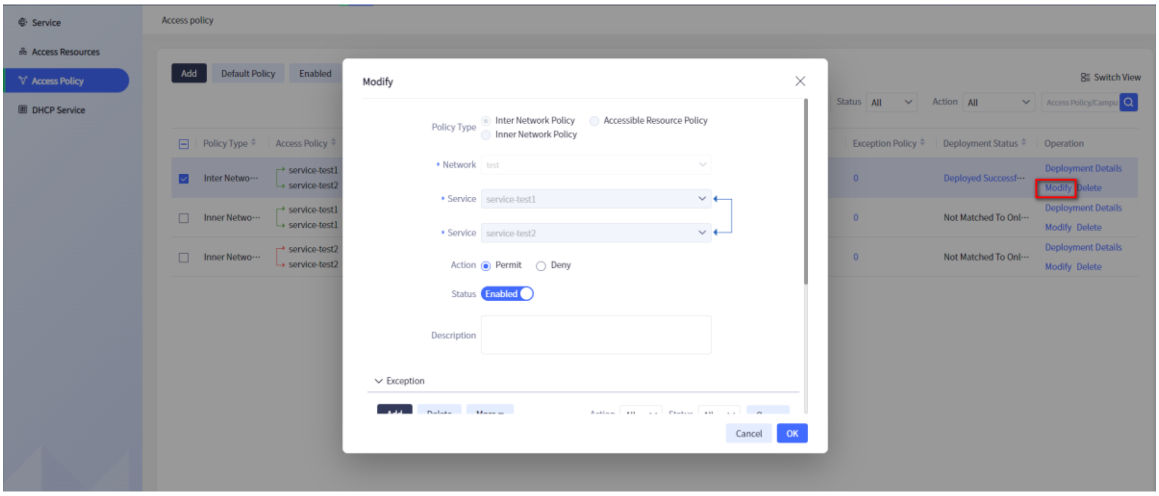
☐ Batch Delete Total 3 Items, Selected 1 Items

1 | 20Items/Page | Jump To 1 Page

Figure 6.4.2.8 Delete a single policy

Modify policy

Click **Modify** in the action column of a desired policy to open the **Modify** box, including policy type, network, service, action, status, description and exception policy. After modifying, click **OK** to save. After modifying the policy, the original policy will be automatically deleted and the modified policy will be redistributed. If you want to discard the modification, click **Cancel**:



Policy Type ● Inter Network Policy ○ Accessible Resource Policy ○ Inner Network Policy

* Network: test

* Service: service-test1

* Service: service-test2

Action ● Permit ○ Deny

Status: Enabled

Description:

Figure 6.4.2.9 Modify policy

Note

- The policy type, campus and service network of the created policy cannot be modified.

6.5 DHCP Service

6.5.1 Address Pool Configuration

Address pool configuration list:

Click “Orchestration” > “DHCP Service” > “Address Pool Configuration” to open the “Address Pool Configuration” interface, as follows:

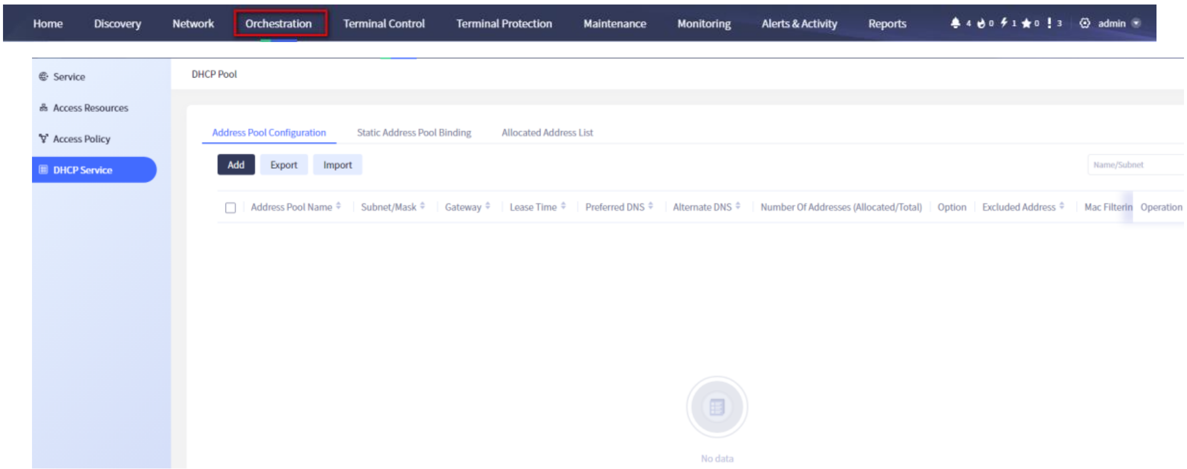
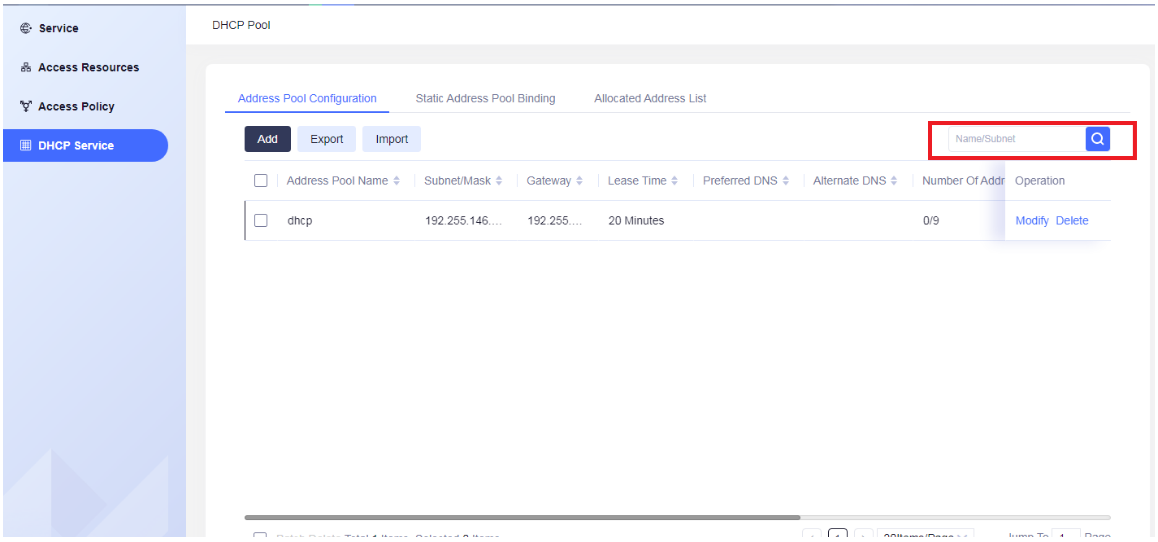


Figure 6.5.1.1 Address pool configuration list

Fuzzy query address pool configuration:

The address pool configuration supports fuzzy query filtering by name and subnet, as shown in the following figure:



☐	Address Pool Name	Subnet/Mask	Gateway	Lease Time	Preferred DNS	Alternate DNS	Number Of Addr	Operation
☐	dhcp	192.255.146....	192.255....	20 Minutes			0/9	Modify Delete

Figure 6.5.1.2 Fuzzy query of address pool configuration

Add address pool configuration:

Click **Add** to open the dialog box, fill in the related parameters of the configuration, and click **OK** to save the new address pool configuration, as shown below:

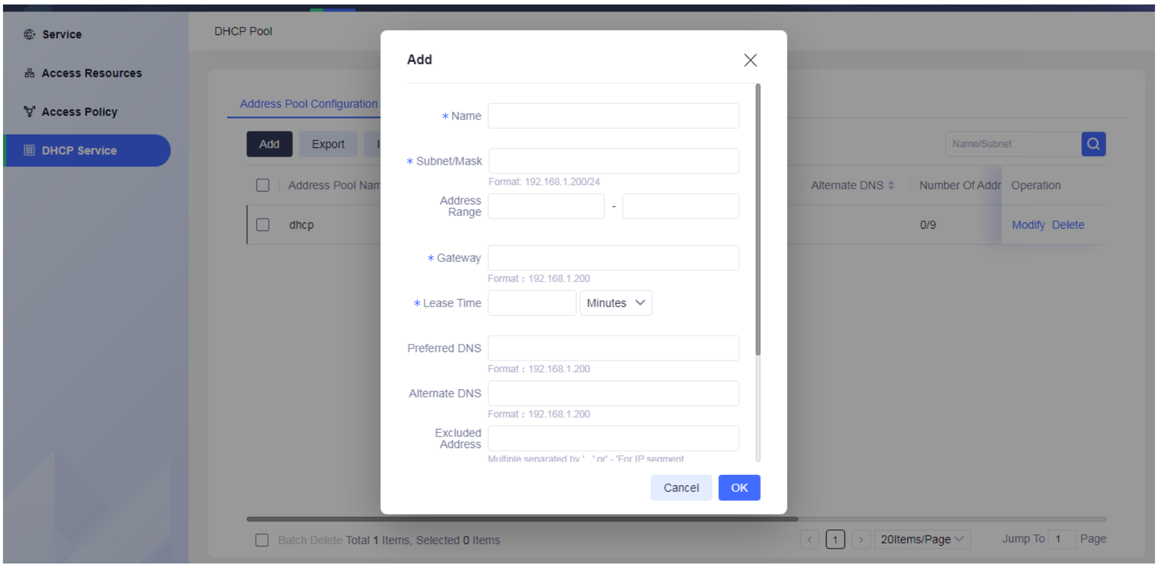
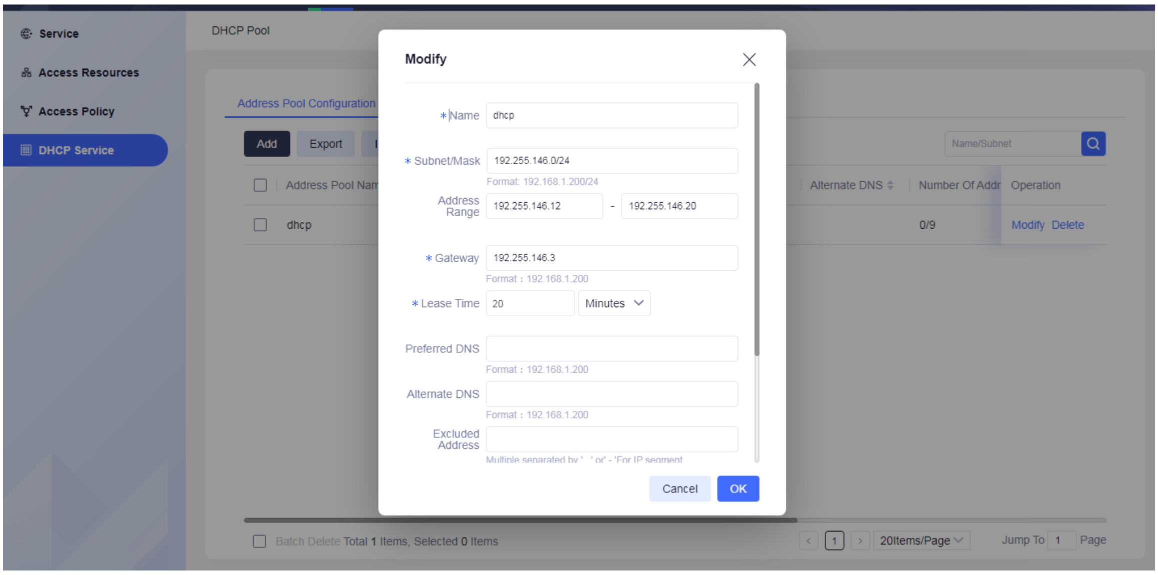


Figure 6.5.1.3 Address pool configuration

Modify address pool configuration:

Click **Modify** to open the dialog box as shown below. After modification, click **OK** to save the modification settings.



dhcp 0/9

*Name: dhcp

*Subnet/Mask: 192.255.146.0/24
Format: 192.168.1.200/24

Address Range: 192.255.146.12 - 192.255.146.20

*Gateway: 192.255.146.3
Format：192.168.1.200

*Lease Time: 20 Minutes

Preferred DNS:
Format：192.168.1.200

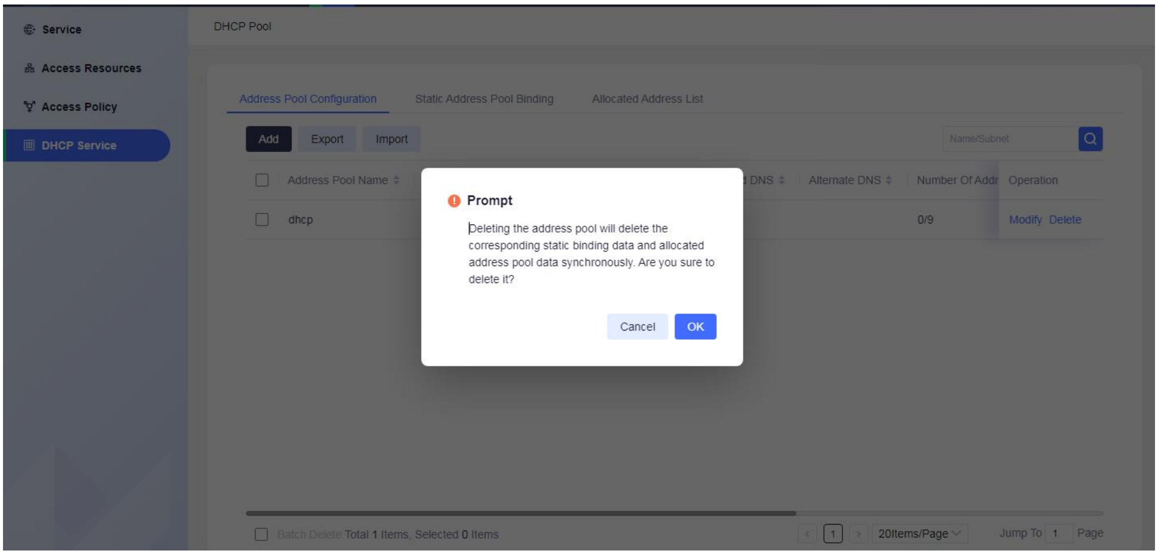
Alternate DNS:
Format：192.168.1.200

Excluded Address:
Multiple separated by ',' or '-'For IP segment

Figure 6.5. 1.4 Modify address pool configuration

Delete address pool configuration:

Click **Delete** in the menu bar, click **OK** in the confirmation dialog box to delete the selected configuration, and click **Cancel** to abort the deletion, as shown below:



dhcp 0/9

Deleting the address pool will delete the corresponding static binding data and allocated address pool data synchronously. Are you sure to delete it?

Figure 6.5.1.5 Delete address pool configuration

Set address pool configuration:

In “Option”, click **Setting**, and you can set a single configuration, as shown in the following figure:

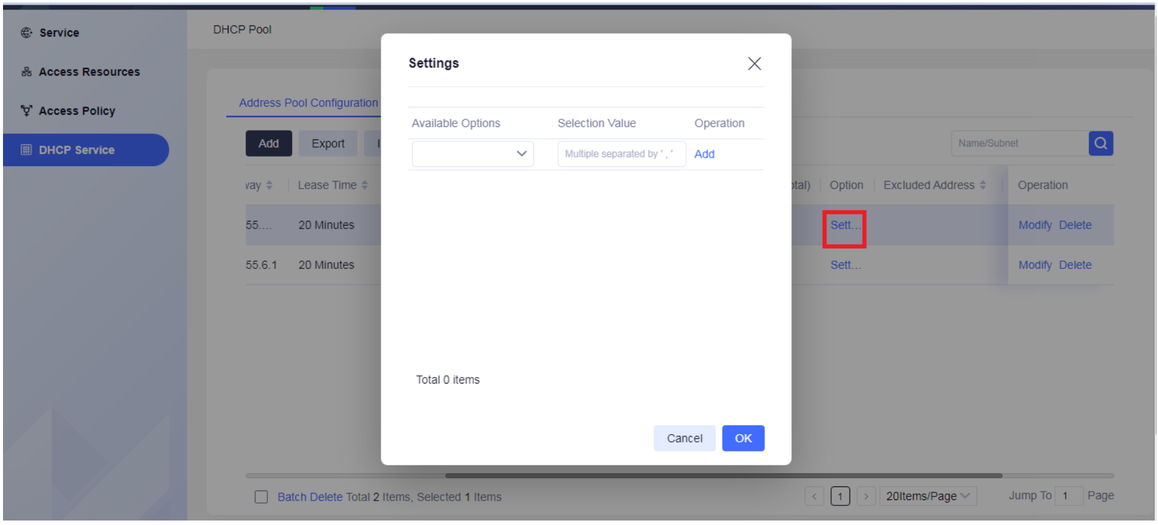
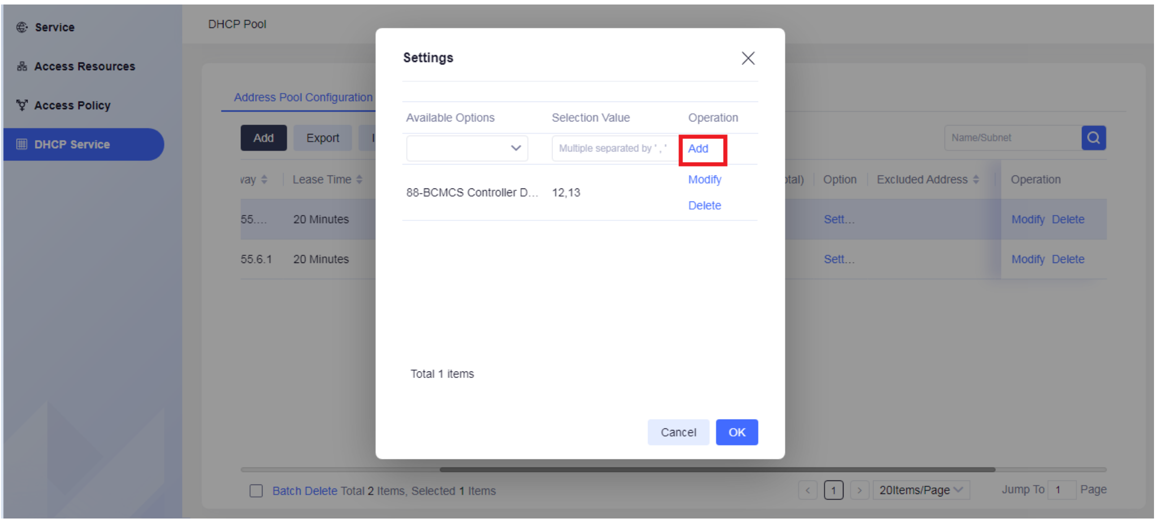


Figure 6.5. 1.6 Setting list

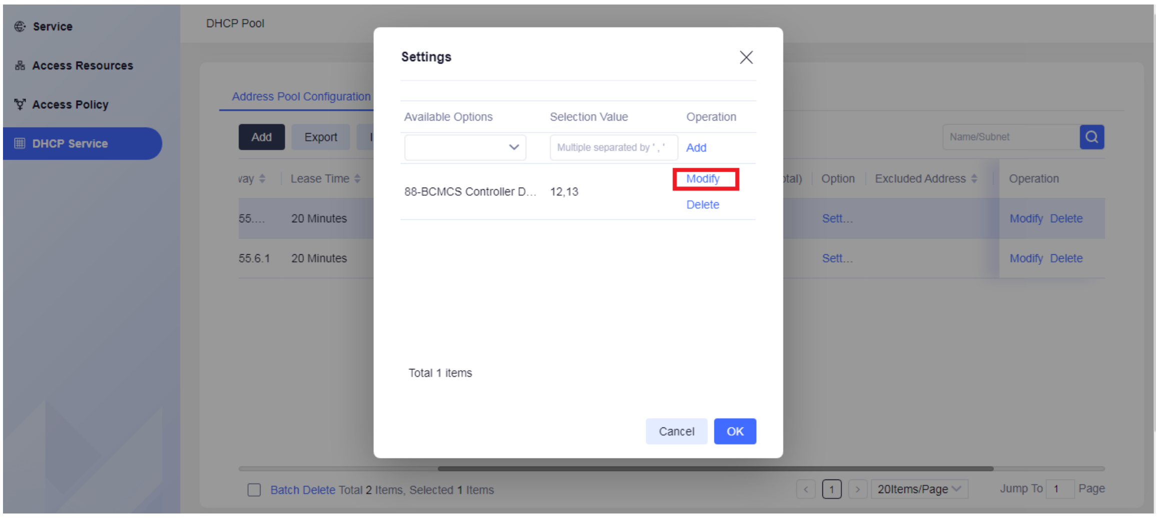
Add setting:



Available Options	Selection Value	Operation
88-BCMCS Controller D...	12,13	Modify Delete

Figure 6.5. 1.7 Add setting parameters

Modify setting:



Available Options	Selection Value	Operation
88-BCMCS Controller D...	12,13	Modify Delete

Figure 6.5. 1.8 Modify setting parameters

Delete setting:

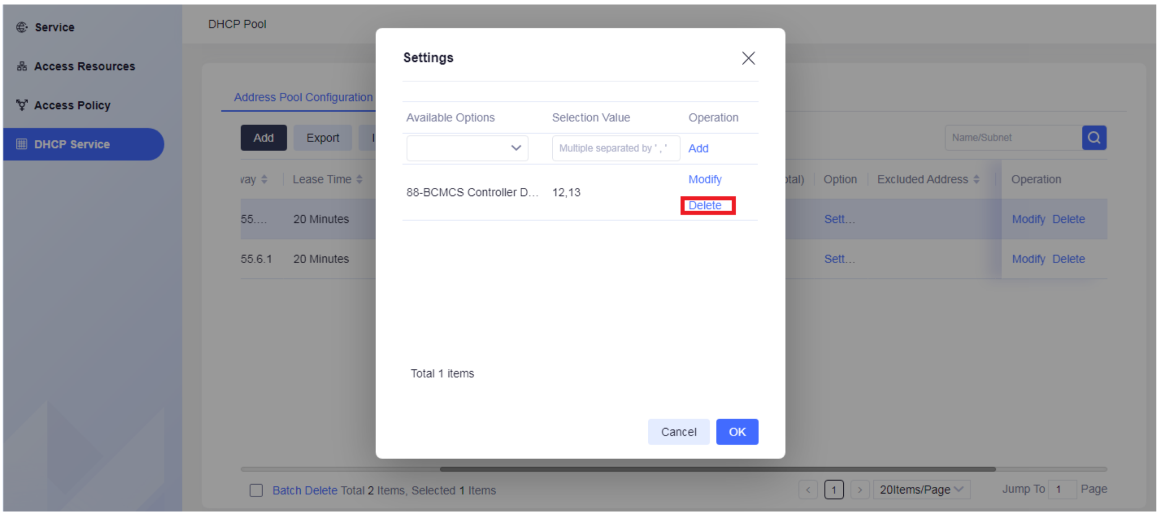


Figure 6.5. 1.9 Delete setting parameters

Export:

Click the "Export" button to export the configuration list. The exported file format is .xlsx format. The data and fields are the same as those displayed in the current configuration list. Query and export are supported.

Import:

Click the "Import" button to open the **Import** dialog box, download the import template, complete the filling, select the filled template, click "OK" and wait for the completion of the import, as shown below:

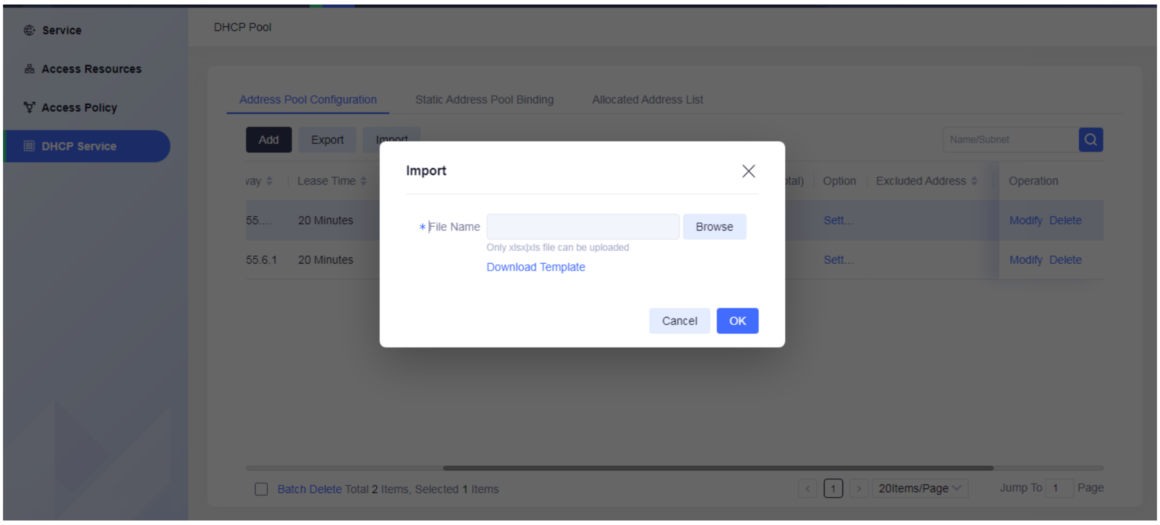


Figure 6.5. 1.10 Import configuration

6.5.2 Static Address Pool Binding

Static address pool binding list:

Click “Orchestration” > “DHCP Service” > “Static Address Pool Binding” to open the “Static Address Pool Binding” interface, as follows:

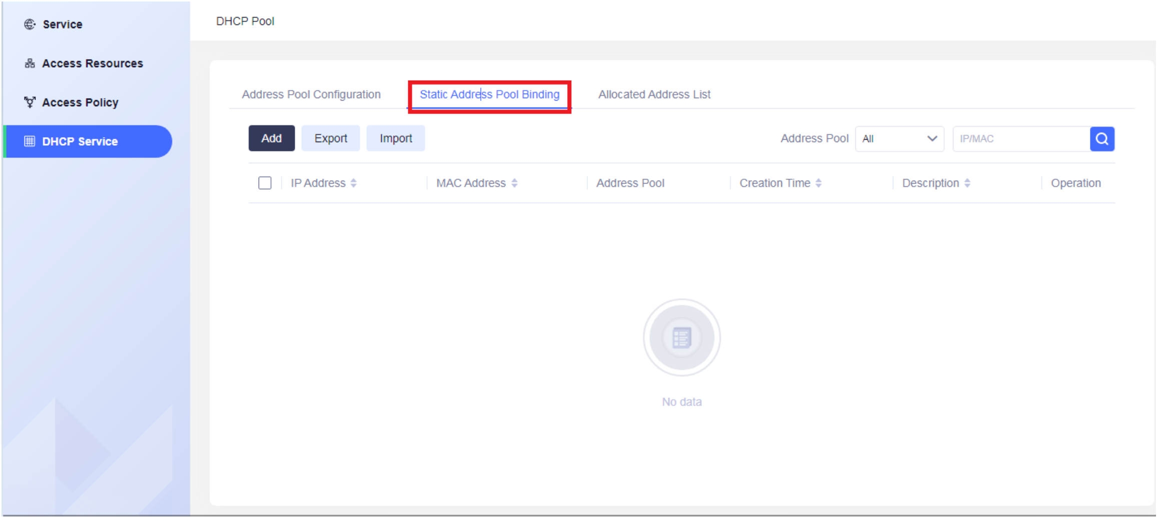


Figure 6.5.2.1 Static address pool binding list

Query:

Static address pool binding supports fuzzy query filtering through address pool, IP address and MAC address, as shown in the following figure:

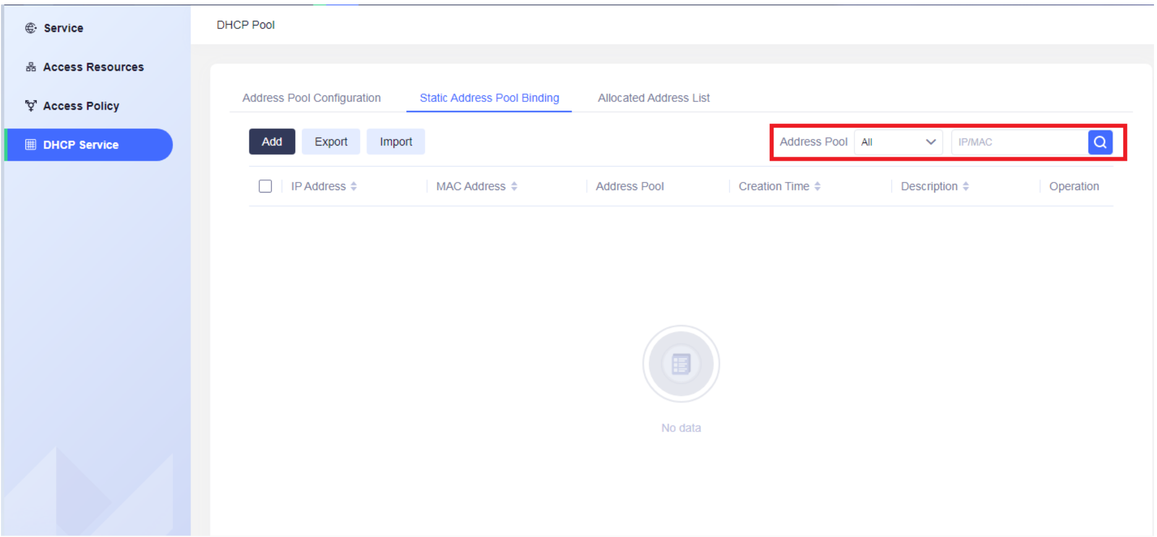


Figure 6.5.2.2 Fuzzy query static address pool

Add:

Click **Add** to open the dialog box, fill in relevant parameters, and click **OK** to save, as shown below:

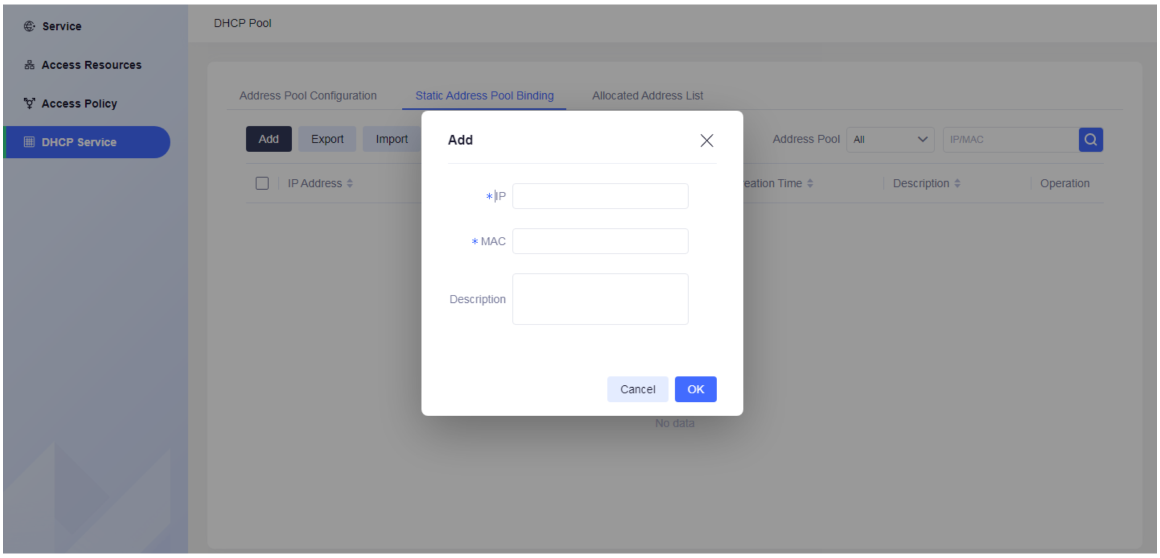
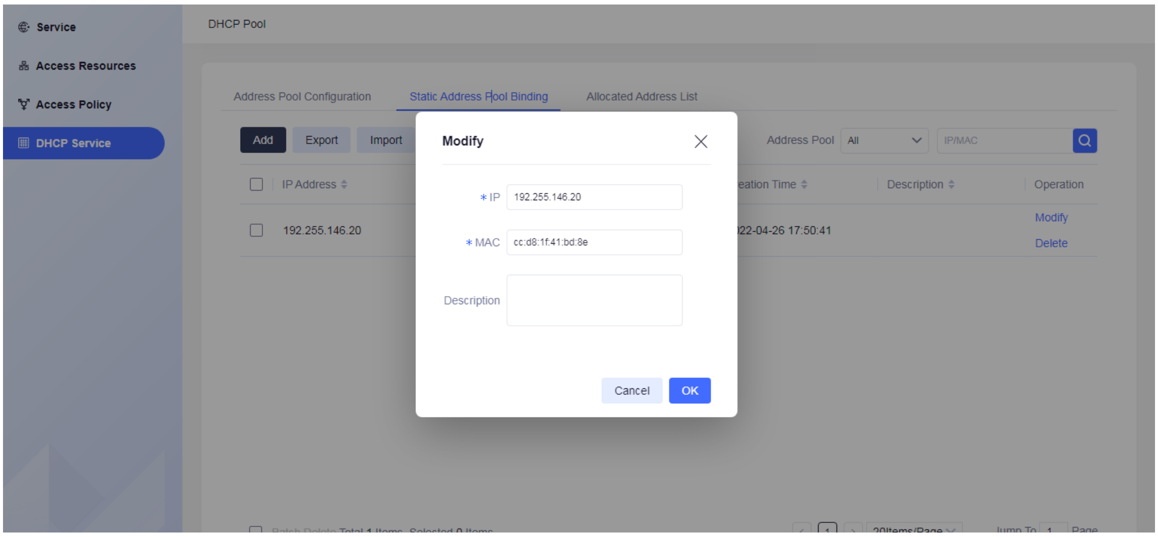


Figure 6.5.2.3 Add static address pool

Modify:

Click **Modify** to open the dialog box as shown below. After modification, click **OK** to save the modified settings.



*IP 192.255.146.20

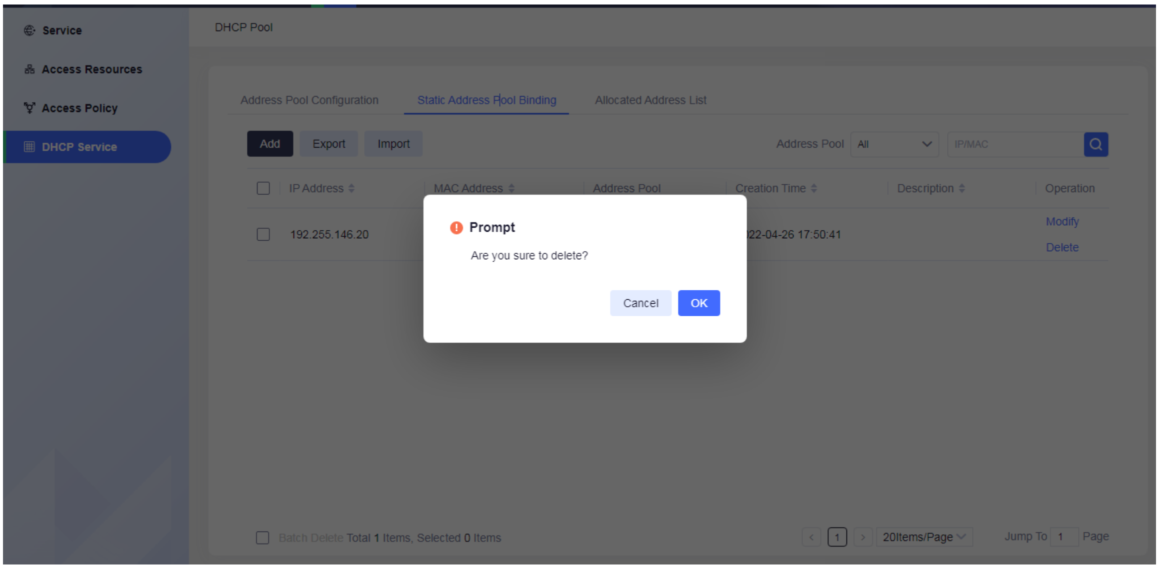
*MAC cc:d8:1f:41:bd:8e

Description

Figure 6.5.2.4 Modify static address pool

Delete address pool configuration:

Click **Delete** in the menu bar, click **OK** in the confirmation dialog box to delete the selected configuration, and click **Cancel** to abort the deletion, as shown below:



Prompt

Are you sure to delete?

192.255.146.20 … 22-04-26 17:50:41

Total 1 Items, Selected 0 Items

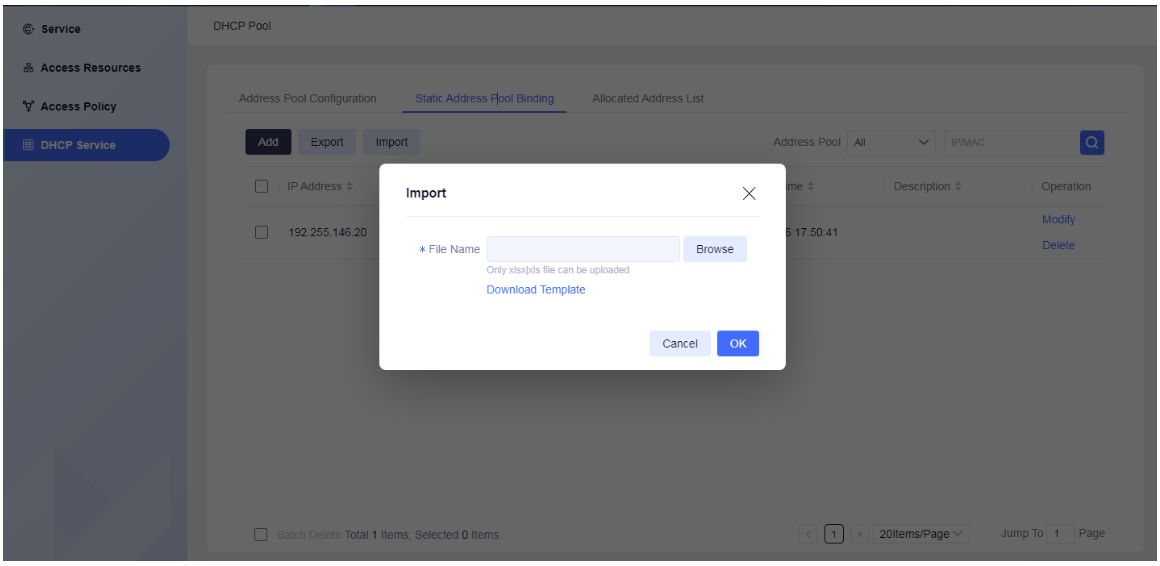
Figure 6.5.2.5 Delete static address pool

Export:

Click the "Export" button to export the configuration list. The exported file format is .xlsx format. The data and fields are the same as those displayed in the current configuration list. Query and export are supported.

Import:

Click the "Import" button to open the **Import** dialog box, download the import template, complete the filling, select the filled template, click "OK" and wait for the completion of the import, as shown below:



Only xlsx|xls file can be uploaded

192.255.146.20 … 17:50:41

Total 1 Items, Selected 0 Items

Figure 6.5.2.6 Import static address pool

6.5.3 Allocated Address List

Allocated address list:

Click “Orchestration” > “DHCP Service” > “Allocated Address List” to open the “Allocated Address List” interface, as show in the following figure:

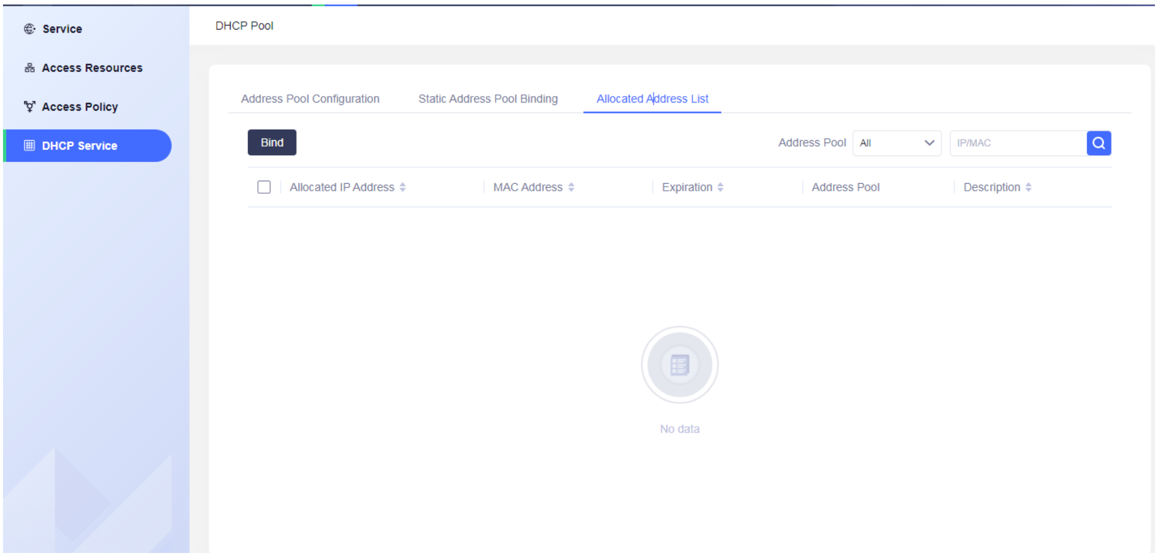


Figure 6.5.3.1 Allocated address list

Query list:

The allocated address list supports fuzzy query by the address pool, ip address, and MAC address, as shown in the following figure:

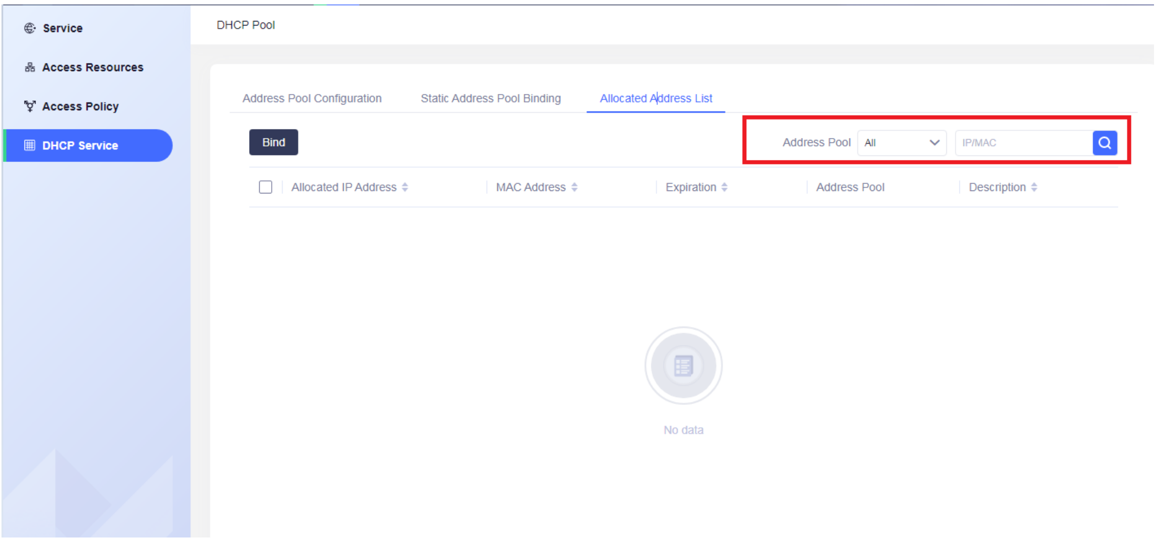


Figure 6.5.3.2 Allocated address list

Bind:

Bind the selected allocated address, as shown in the following figure:

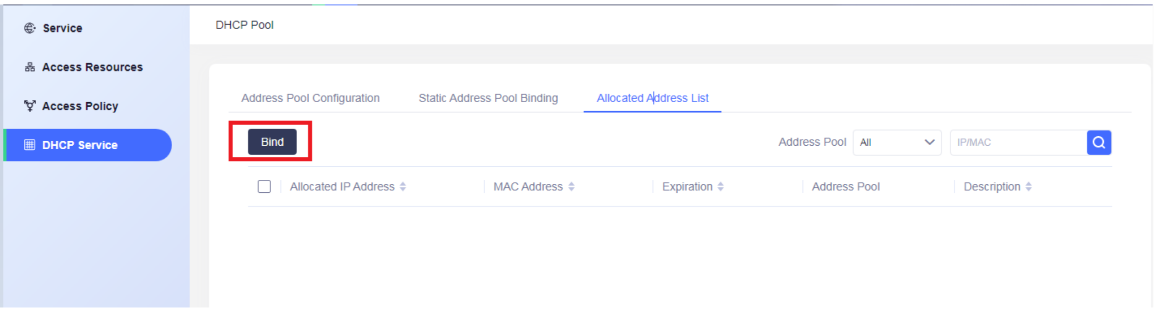


Figure 6.5.3.3 Bind the allocated address

7 Terminal Control

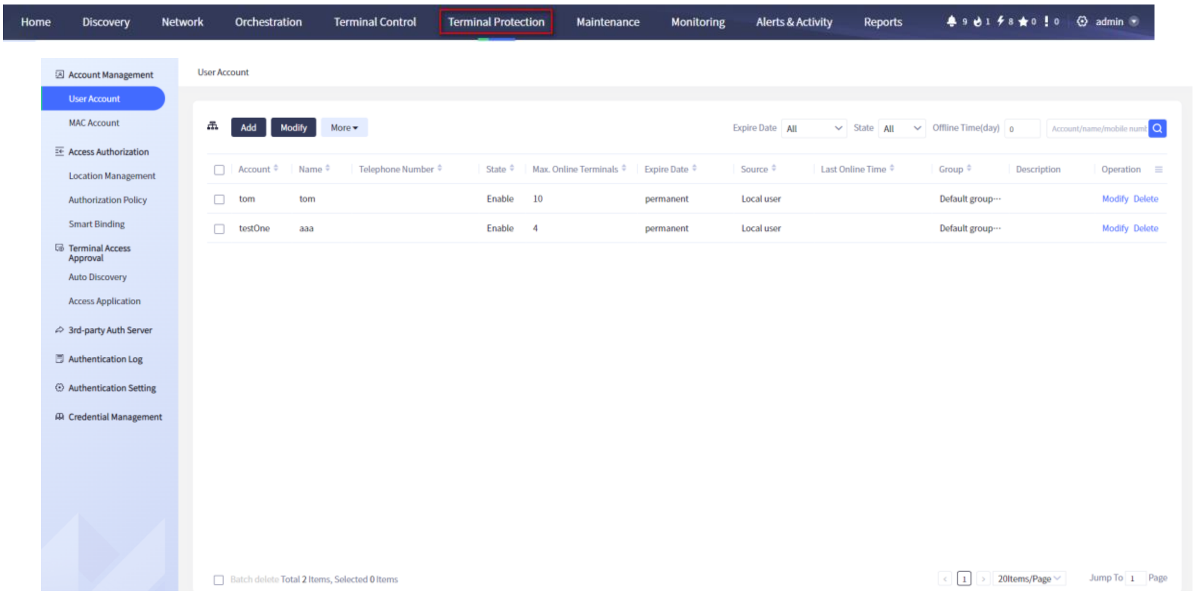
7.1 Account Management

7.1.1 User Account

Click "Terminal Control" - > "User Management" at the top, and the user management interface will display the information of all users. It provides functions such as adding, deleting, batch deleting, modifying, batch modifying, synchronizing, importing, exporting, and querying.

- User management interface

The user management interface is divided into three parts. The user group tree on the left contains all groups under the organization; The upper part of the right side is the function area, including add button, modify button, synchronize button, import button, export button, query criteria and query button. The lower part on the right is the user management list.



Expire Date All State All Offline Time(day) 0 Account/name/mobile numb

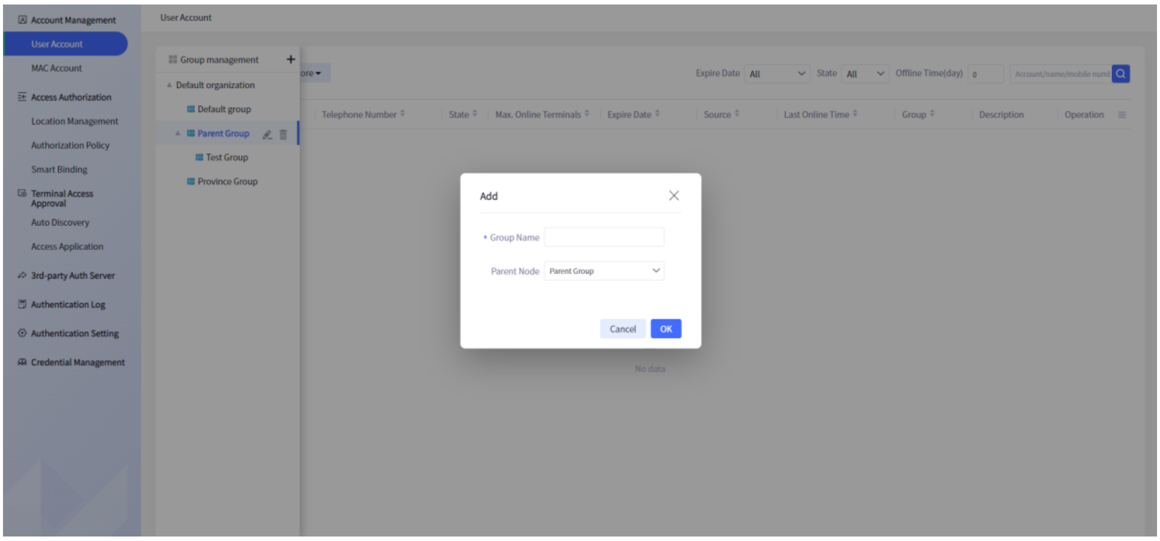
☐	Account	Name	Telephone Number	State	Max. Online Terminals	Expire Date	Source	Last Online Time	Group	Description	Operation
☐	tom	tom		Enable	10	permanent	Local user		Default group···		Modify Delete
☐	testOne	aaa		Enable	4	permanent	Local user		Default group···		Modify Delete

Total 2 Items, Selected 0 Items

Figure 7.1.1.1 User management interface

- Group management

The left group management displays all groups in the organization, providing the adding, deleting and modifying functions.



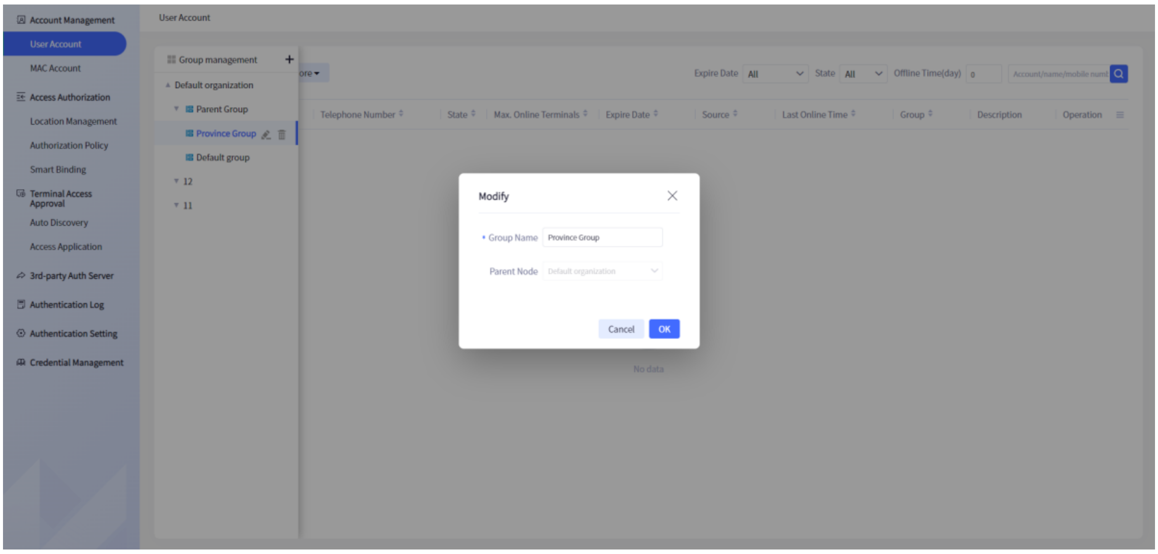
Add

* Group Name

Parent Node Parent Group

Cancel OK

Figure 7.1.1.2 Add group



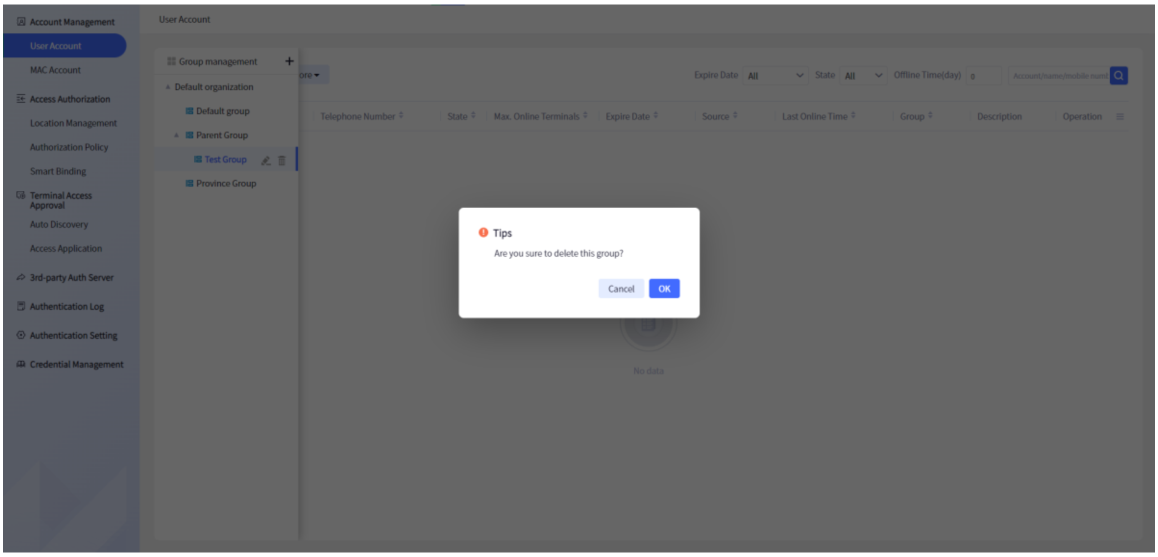
Modify

* Group Name Province Group

Parent Node Default organization

Cancel OK

Figure 7.1.1.3 Modify group



Tips

Are you sure to delete this group?

Cancel OK

Figure 7.1.1.4 Delete group

- User management function area

Add button: add user data.

Modify button: batch modify user data.

Synchronize button: synchronize users to the list according to the data of the external authentication source, as shown in figure 7.1.1.5 below.

Import button: import data and download template, as shown in figure 7.1.1.6 below.

Export button: export data. To export the user password, you need to enter the login password; otherwise, you do not enter it, as shown in figure 7.1.1.7 below.

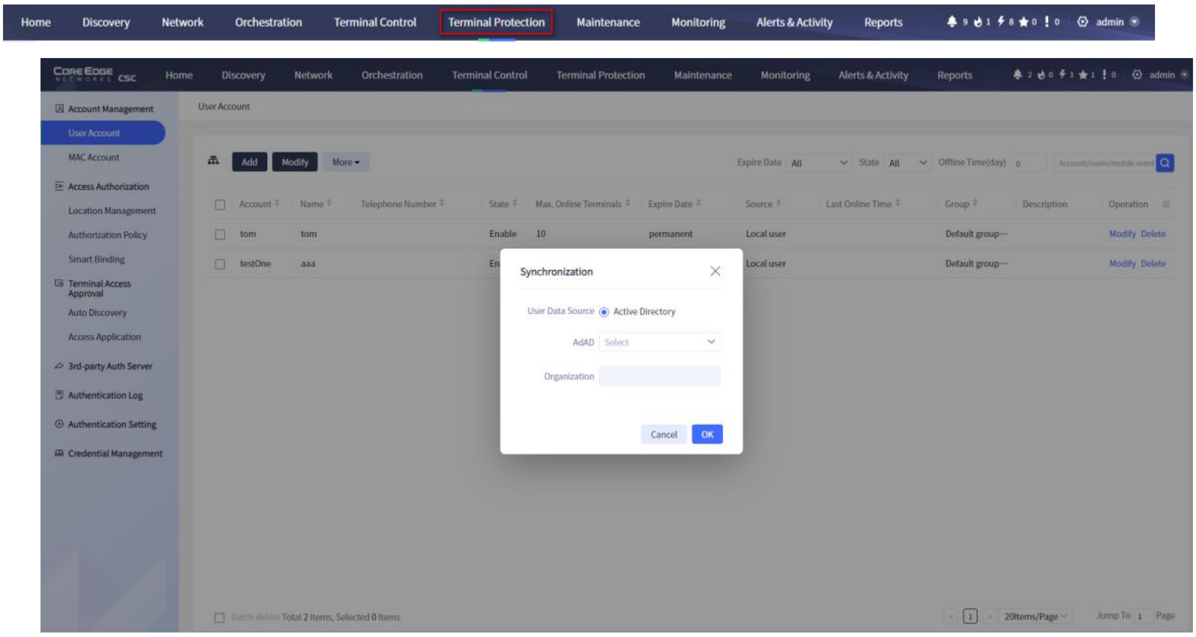
Query button: filter data according to validity period, status, offline days, and fuzzy query.

Delete: delete a single user.

Batch delete: delete the selected users in batch.

Modify: modify a single user.

Batch modify: batch modify the selected users.



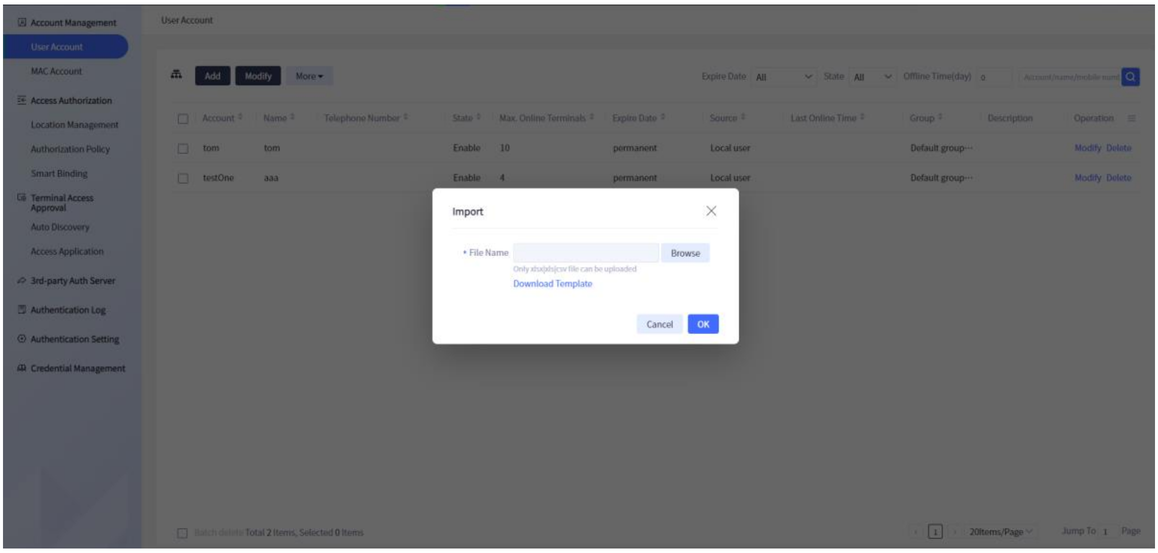
Synchronization

User Data Source: ● Active Directory

AdAD: Select

Organization:

Figure 7.1.1.5 Synchronize pop-up box



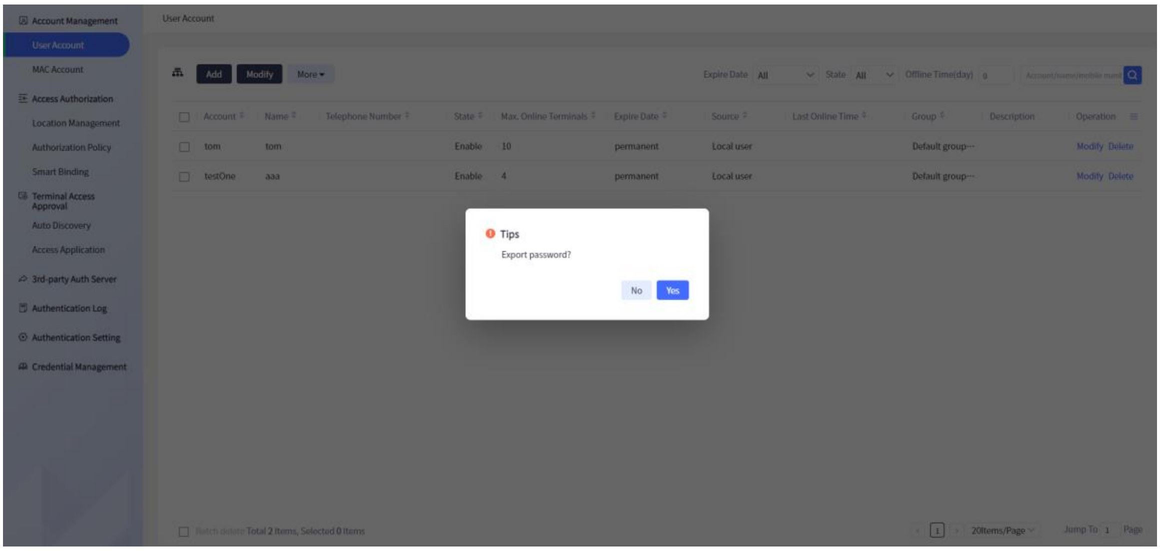
Import

* File Name:

Only xls|xlsx|csv file can be uploaded

Download Template

Figure 7.1.1.6 Import pop-up box



User Account

☐	Account	Name	Telephone Number	State	Max. Online Terminals	Expire Date	Source	Last Online Time	Group	Description	Operation
☐	tom	tom		Enable	10	permanent	Local user		Default group···		Modify Delete
☐	testOne	aaa		Enable	4	permanent	Local user		Default group···		Modify Delete

Tips

Export password?

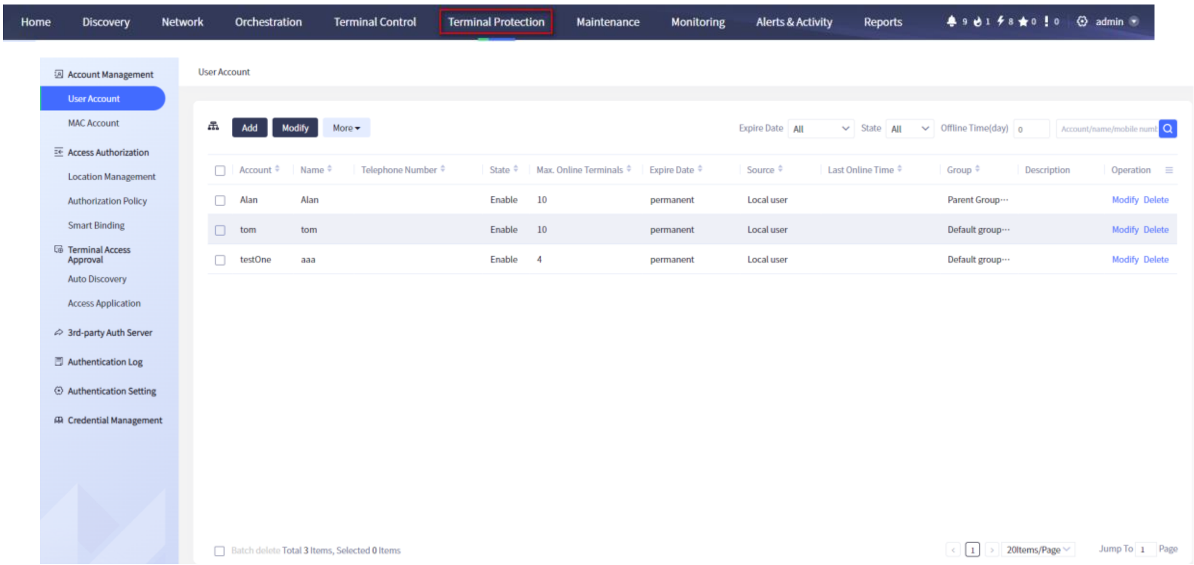
No Yes

Batch delete Total 2 items, Selected 0 items

Figure 7.1.1.7 Export pop-up box

- User management list

The user management list displays the account, name, phone number, status, maximum number of online terminals, validity period, data source, last online time, grouping, description and operation.



User Account

☐	Account	Name	Telephone Number	State	Max. Online Terminals	Expire Date	Source	Last Online Time	Group	Description	Operation
☐	Alan	Alan		Enable	10	permanent	Local user		Parent Group···		Modify Delete
☐	tom	tom		Enable	10	permanent	Local user		Default group···		Modify Delete
☐	testOne	aaa		Enable	4	permanent	Local user		Default group···		Modify Delete

Batch delete Total 3 items, Selected 0 items

Figure 7.1.1.8 User management list

- Add user

In the “Add” pop-up box, you need to fill in the account, name, password, confirm password, maximum number of online terminals, user grouping, telephone number, change password for first authentication, status, expire date, and description.

Account: required item; the length cannot be greater than 64 characters.

Name: required item; the length cannot be greater than 64 characters.

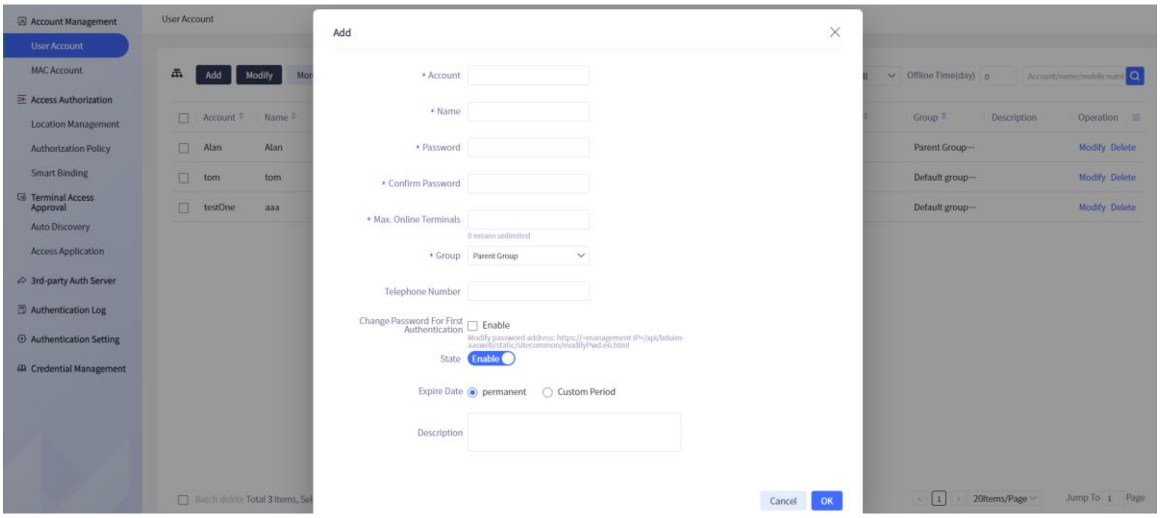
Password and **confirm password**: required items. The two entries must be identical.

Maximum number of online terminals: required item; any integer between 0 and 9223372036854775807 can be entered.

User group: required item. It is the group under the organization by default.

Change Password for First authentication: not required. Check it to enable. You can also change the password on the website according to the prompts below.

Expire date: permanent is selected by default. Click **Customize** to select the start date and end date.



Add

- * Account:
- * Name:
- * Password:
- * Confirm Password:
- * Max. Online Terminals: (0 means unlimited)
- * Group: Parent Group
- Telephone Number:
- Change Password For First Authentication: ☐ Enable
- State: Enable
- Expire Date: ● permanent ○ Custom Period
- Description:

Figure 7.1.1.9 The pop-up box of adding users

- Modify users

There are two ways to modify a user. One is to click the **Modify** button in the function area, and the other is to click the **Modify** button in the list.

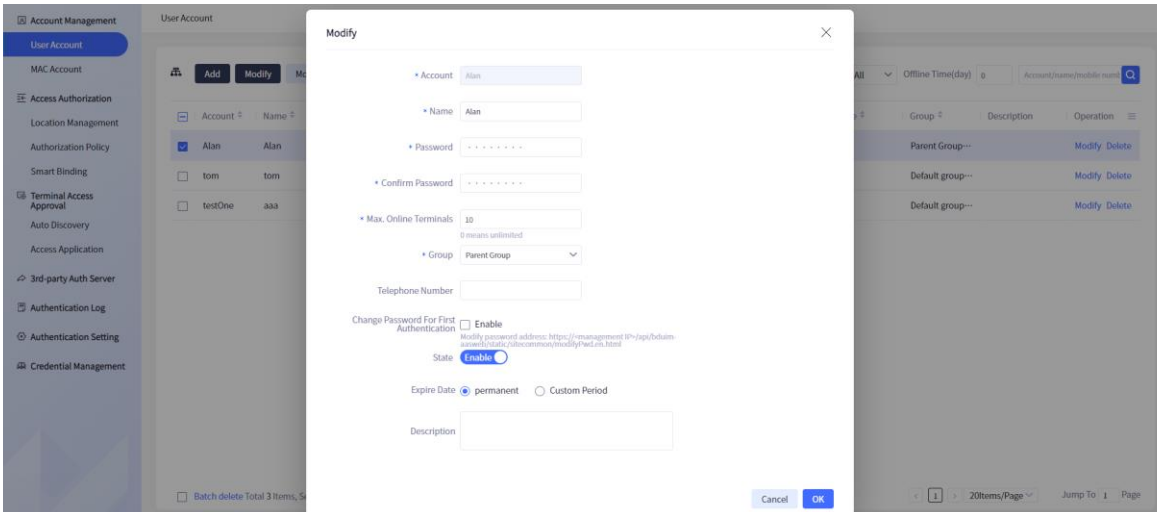
Click the **Modify** button in the list to represent a single modification, and the data of the current user will be filled into the corresponding input box.

Click the **Modify** button in the function area, and check a single user, which means a single modification. The data of the current user will be filled into the corresponding input box.

Click the **Modify** button in the functional area and check multiple users, which means batch modification. You need to check multiple users of the same data source. Because it is batch modification, the checked user data will not be displayed.

The data is the user of local data. Except for the account restrictions, other items can be modified, as shown in figure 7.1.1.10 below.

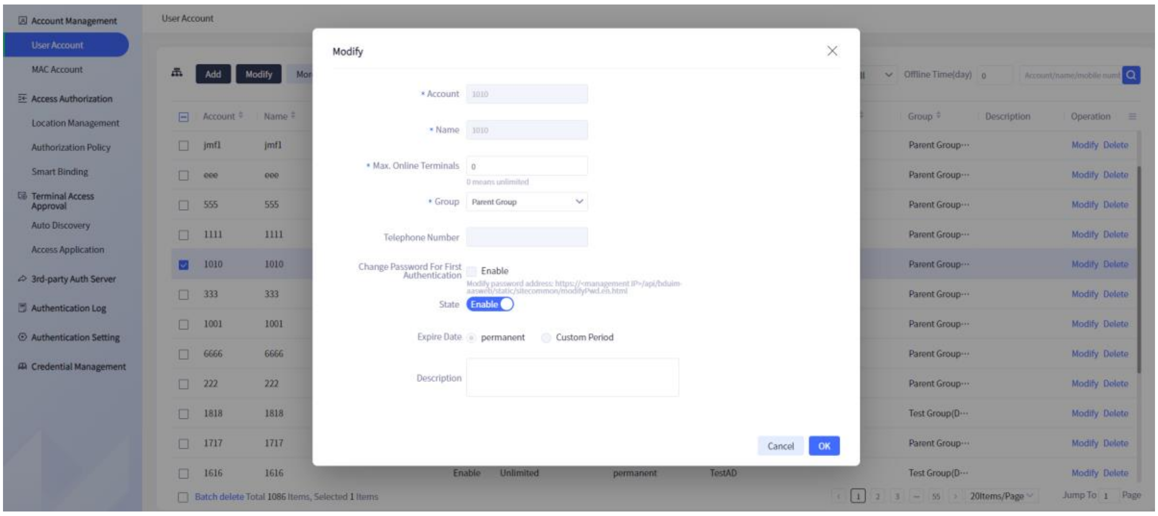
If it is an external authentication source, there will be multiple restrictions. Only the maximum number of terminals, user grouping, change password for first authentication, status, validity period and description can be modified, as shown in figure 7.1.1.11 below.



Modify

- * Account: Alan
- * Name: Alan
- * Password: ········
- * Confirm Password: ········
- * Max. Online Terminals: 10 (0 means unlimited)
- * Group: Parent Group
- Telephone Number:
- Change Password For First Authentication: ☐ Enable
- State: Enable
- Expire Date: ● permanent ○ Custom Period
- Description:

Figure 7.1.1.10 Modify local user



Modify

* Account: 1010

* Name: 1010

* Max. Online Terminals: 0

0 means unlimited

* Group: Parent Group

Telephone Number:

Change Password For First Authentication: ☐ Enable

Modify password address: https://<management IP>/api/bduim-aasweb/static/sitecommon/modifyPwd.en.html

State: Enable

Expire Date: ● permanent ○ Custom Period

Description:

Batch delete Total 1086 Items, Selected 1 Items

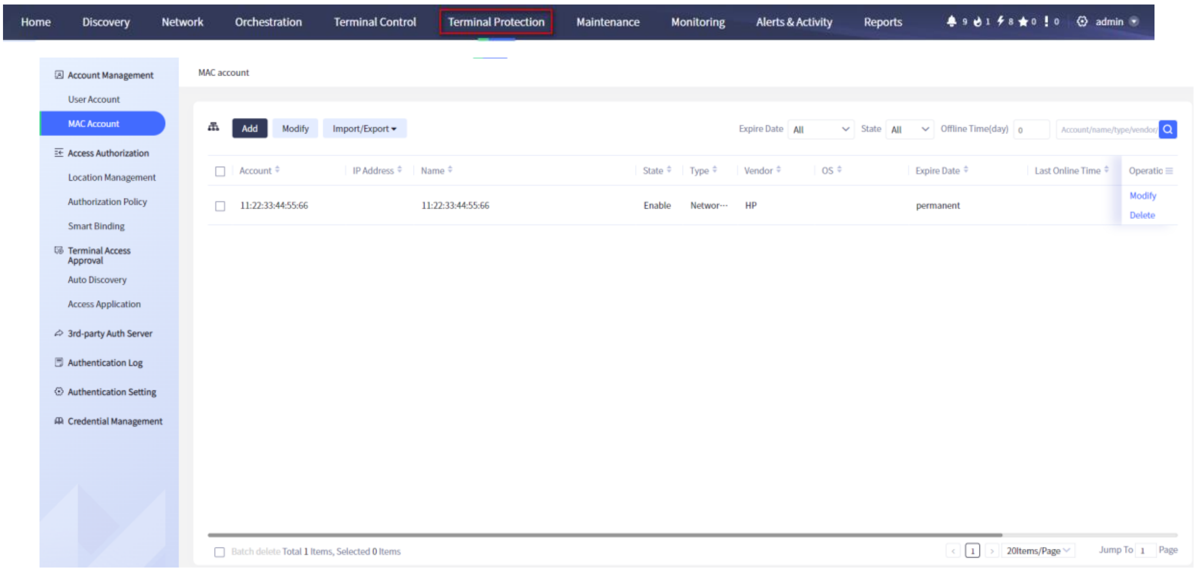
Figure 7.1.1.11 Modify external authentication source user

7.1.2 MAC Account

The MAC account interface displays all MAC account information, and provides functions such as adding, modifying, batch modifying, importing, exporting, querying, deleting, and batch deleting.

- MAC account interface

The MAC account interface is divided into three parts. The user group tree on the left contains all groups under the organization; The upper part of the right is the function area, including add button, modify button, import button, export button, query criteria and query button. The lower part on the right is the list of MAC accounts.



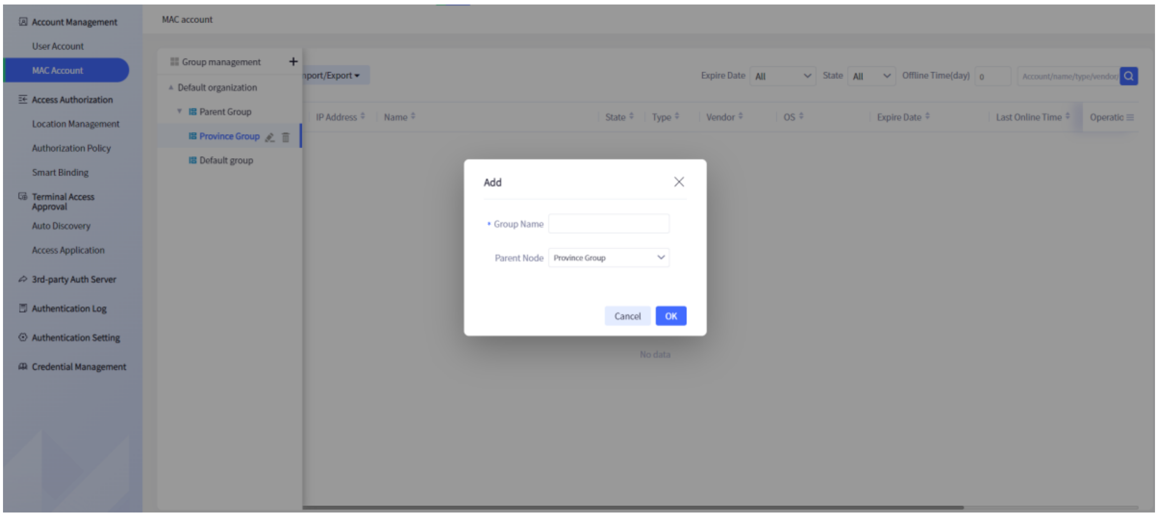
☐	Account	IP Address	Name	State	Type	Vendor	OS	Expire Date	Last Online Time	Operation
☐	11:22:33:44:55:66		11:22:33:44:55:66	Enable	Networ···	HP		permanent		Modify Delete

Batch delete Total 1 Items, Selected 0 Items

Figure 7.1.2.1 MAC account interface

- Group management

The left group management displays all groups in the organization, providing the add, delete, modify, and other functions.

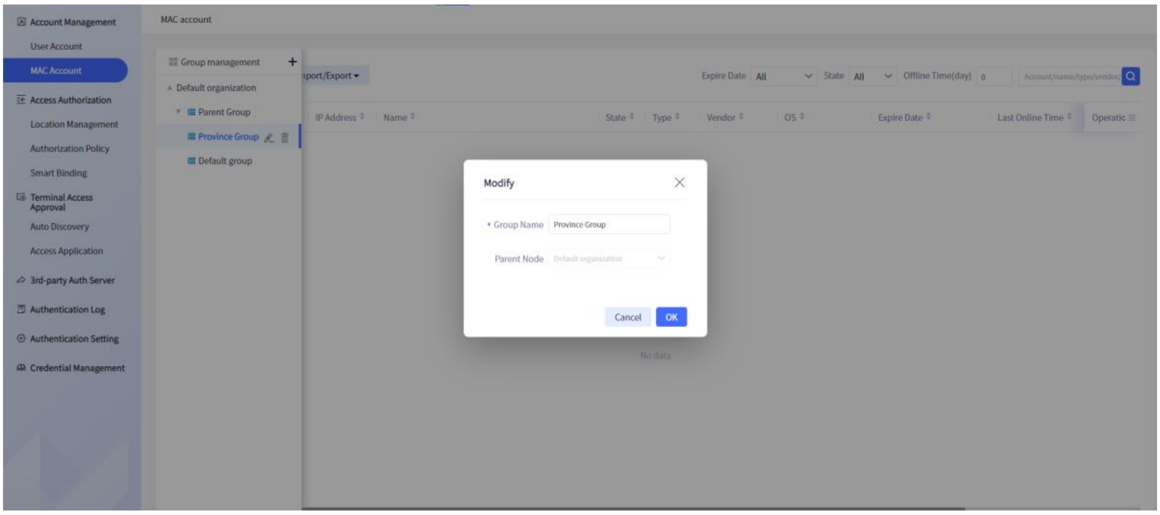


Add

* Group Name

Parent Node Province Group

Figure 7.1.2.2 Add group

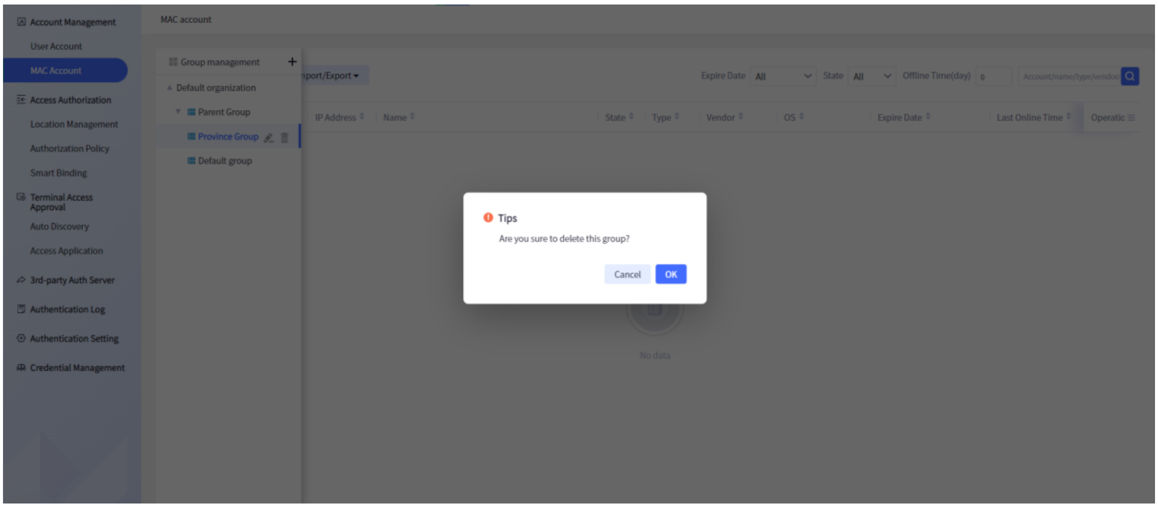


Modify

* Group Name Province Group

Parent Node Default organization

Figure 7.1.2.3 Modify group



Tips

Are you sure to delete this group?

Figure 7.1.2.4 Delete a group

- MAC account function area

  Add button: add MAC account.

  Modify button: batch modify MAC accounts.

  Export button: export data.

Import button: import data and download template, as shown in figure 6.1.2.5 below.

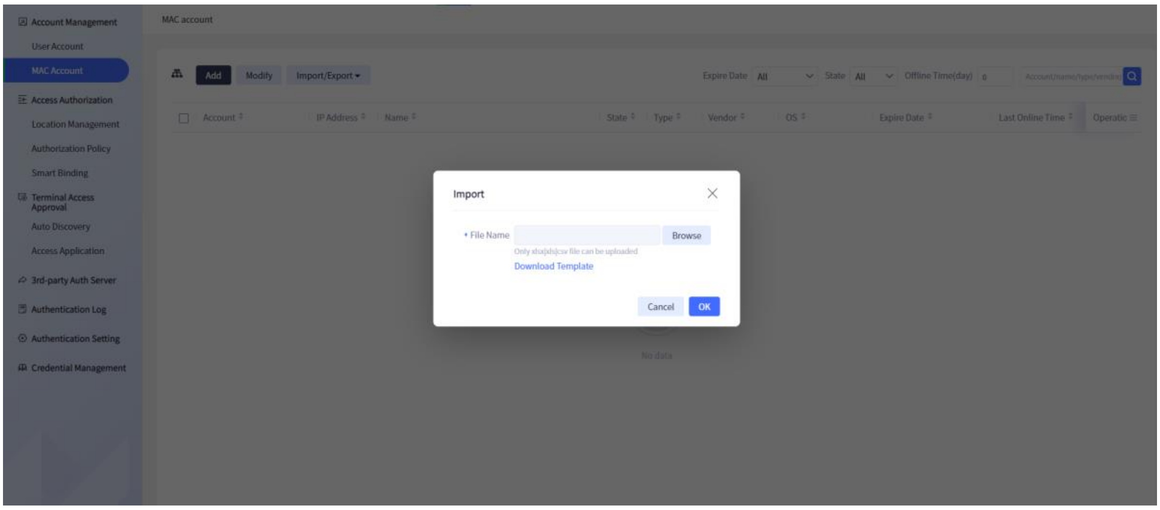
Query button: filter data according to validity period, status and fuzzy query.

Delete: delete a single MAC account.

Batch delete: batch delete the selected MAC accounts.

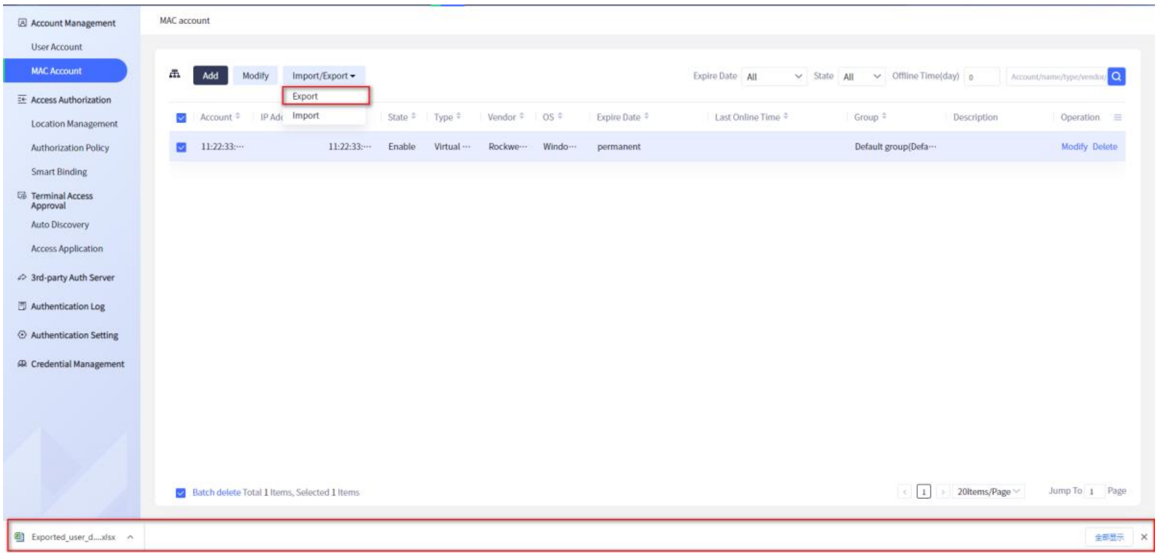
Modify: modify a single MAC account.

Batch modify: batch modify the selected MAC accounts.



Only xlsx|xls|csv file can be uploaded

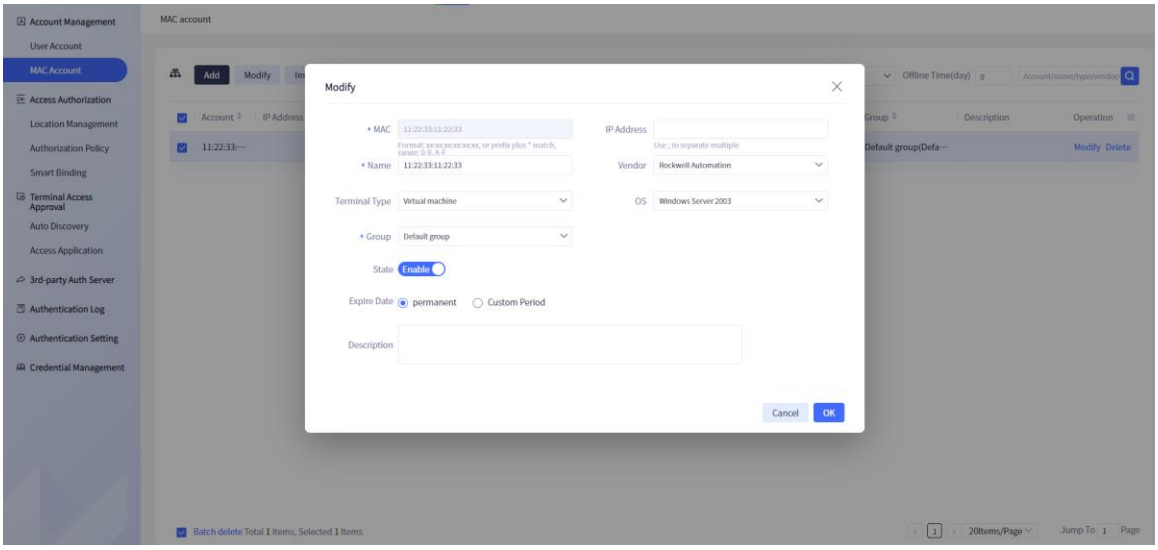
Figure 7.1.2.5 Import pop-up box



☑	Account	IP Adc	State	Type	Vendor	OS	Expire Date	Last Online Time	Group	Description	Operation
☑	11:22:33:···	11:22:33:···	Enable	Virtual ···	Rockwe···	Windo···	permanent		Default group(Defa···		Modify Delete

Total 1 Items, Selected 1 Items

Figure 7.1.2.6 Export pop-up box

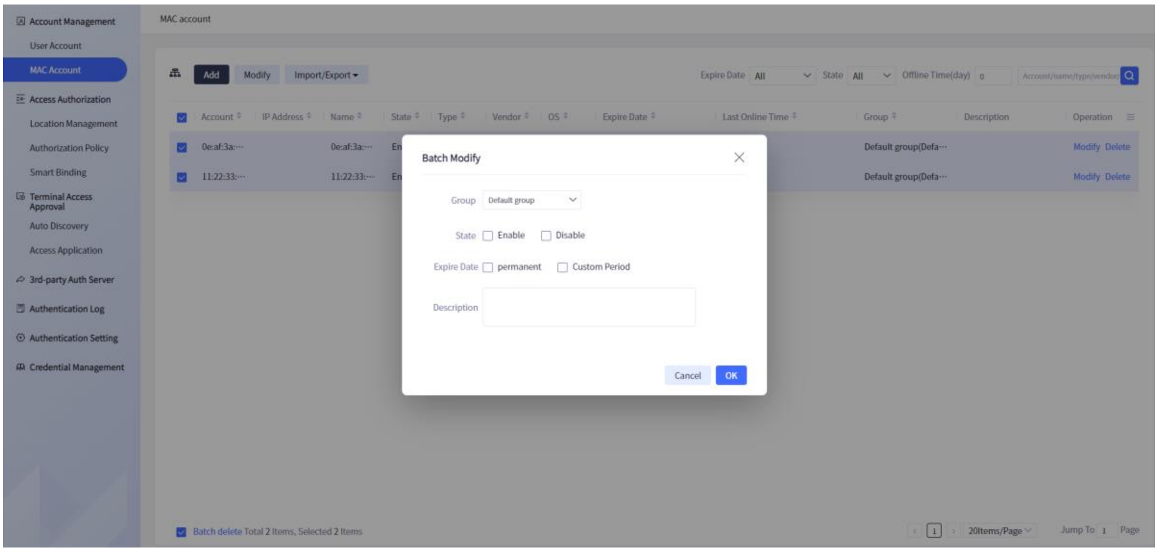


Modify

* MAC: 11:22:33:11:22:33
* Name: 11:22:33:11:22:33
IP Address:
Vendor: Rockwell Automation
Terminal Type: Virtual machine
OS: Windows Server 2003
* Group: Default group
State: Enable
Expire Date: ● permanent ○ Custom Period
Description:

Batch delete Total 1 Items, Selected 1 Items

Figure 7.1.2.7 Modify a single MAC user

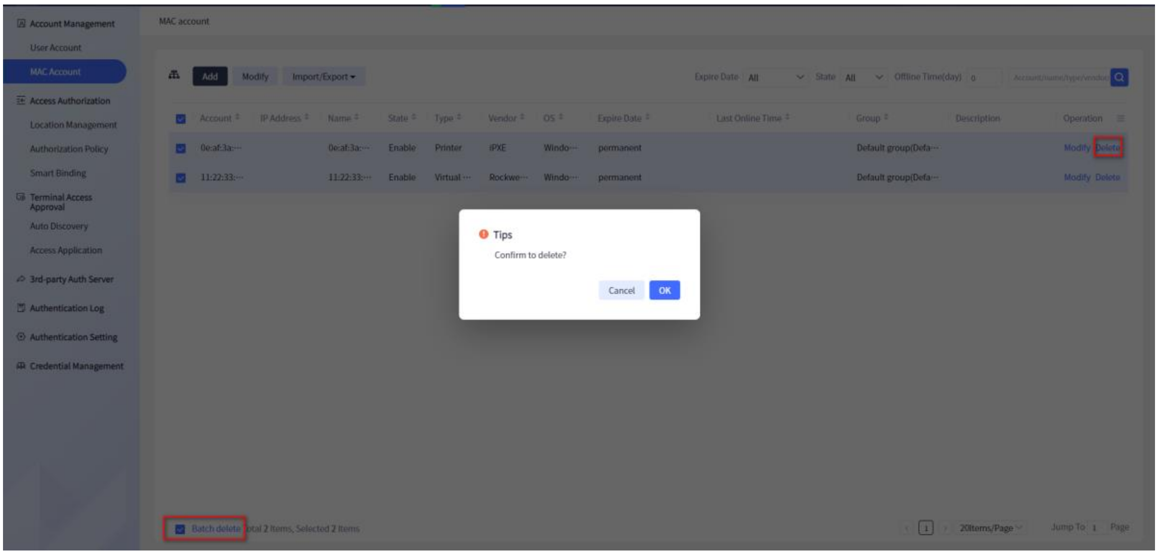


Batch Modify

Group: Default group
State: ☐ Enable ☐ Disable
Expire Date: ☐ permanent ☐ Custom Period
Description:

Batch delete Total 2 Items, Selected 2 Items

Figure 7.1.2.8 Batch modify MAC users



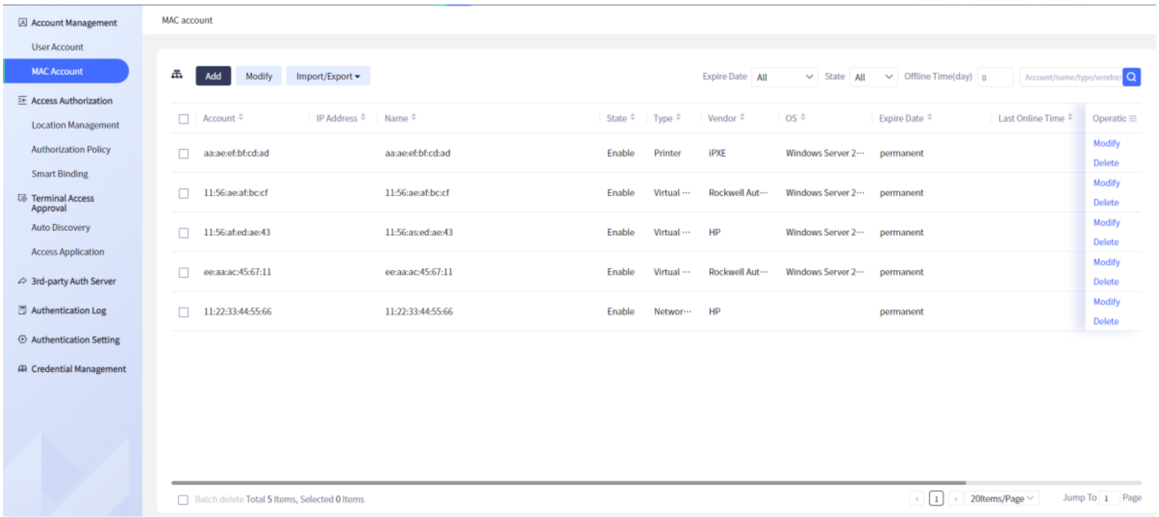
Tips

Confirm to delete?

Figure 7.1.2.9 Delete and batch delete pop-up box

- MAC account list

The MAC account list shows the account, IP address, name, status, type, manufacturer, operating system, expire date, last online time, group, description and operation.



☐	Account	IP Address	Name	State	Type	Vendor	OS	Expire Date	Last Online Time	Operatio
☐	aa:ae:ef:bf:cd:ad		aa:ae:ef:bf:cd:ad	Enable	Printer	iPXE	Windows Server 2···	permanent		Modify Delete
☐	11:56:ae:af:bc:cf		11:56:ae:af:bc:cf	Enable	Virtual ···	Rockwell Aut···	Windows Server 2···	permanent		Modify Delete
☐	11:56:af:ed:ae:43		11:56:as:ed:ae:43	Enable	Virtual ···	HP	Windows Server 2···	permanent		Modify Delete
☐	ee:aa:ac:45:67:11		ee:aa:ac:45:67:11	Enable	Virtual ···	Rockwell Aut···	Windows Server 2···	permanent		Modify Delete
☐	11:22:33:44:55:66		11:22:33:44:55:66	Enable	Networ···	HP		permanent		Modify Delete

☐ Batch delete Total 5 Items, Selected 0 Items

Figure 7.1.2.10 MAC account list

- Add MAC account

To add a MAC account, you need to fill in MAC, IP address, name, manufacturer, terminal type, operating system, user group, status, validity period and description.

MAC: required item, format xx:xx:xx:xx:xx, or matching by prefix plus *, range 0-9, a-f.

IP address: not required. Multiple IPs are separated by semicolons and cannot be longer than 64 characters.

Name: required item; length cannot be greater than 64 characters.

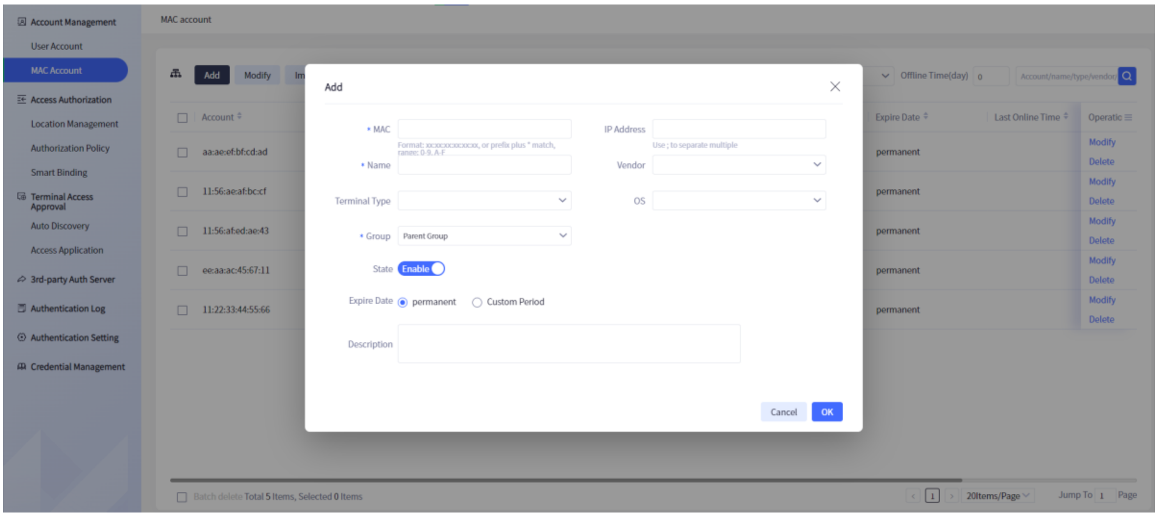
Manufacturer: not required; selected from the drop-down box.

Terminal type: not required, selected from the drop-down box.

OS: not required; selected or entered by yourself.

User grouping: required item. It is the group under the organization by default.

Expire date: permanent is selected by default. Click **Customize** to select the start date and end date.


Add
* MAC
Format: xx:xx:xx:xx:xx:xx, or prefix plus * match, range: 0-9, A-F
IP Address
Use ; to separate multiple
* Name
Vendor
Terminal Type
OS
Description
Cancel
OK

* Group: Parent Group

State: Enable

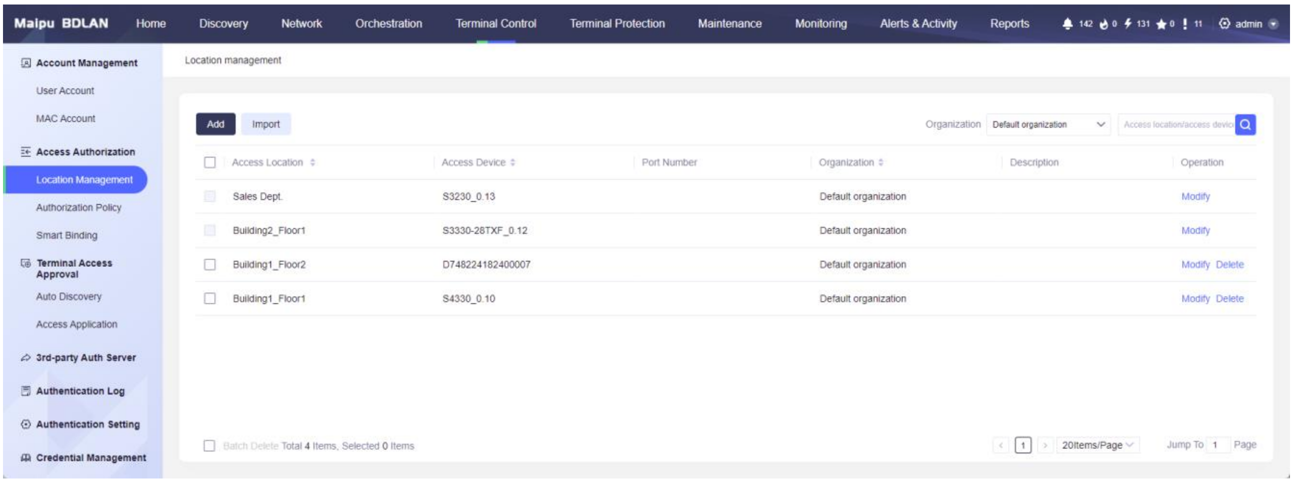
Expire Date: ● permanent ○ Custom Period

Figure 7.1.2.11 Add MAC address

7.2 Access Authorization

7.2.1 Location Management

Select "Terminal Control" > "Access Authorization" at the top navigation bar, open the "Location management" interface, display all access location data, and provide functions, such as querying, adding, modifying, deleting, and batch deleting access locations.



☐	Access Location	Access Device	Port Number	Organization	Description	Operation
☐	Sales Dept.	S3230_0.13		Default organization		Modify
☐	Building2_Floor1	S3330-28TXF_0.12		Default organization		Modify
☐	Building1_Floor2	D748224182400007		Default organization		Modify Delete
☐	Building1_Floor1	S4330_0.10		Default organization		Modify Delete

Figure 7.2.1.1 Access location navigation interface

- Location interface

The access location interface is divided into two parts. The upper part is the function area, including query input box, query button, add button and import button; The lower part is the display list of access locations.

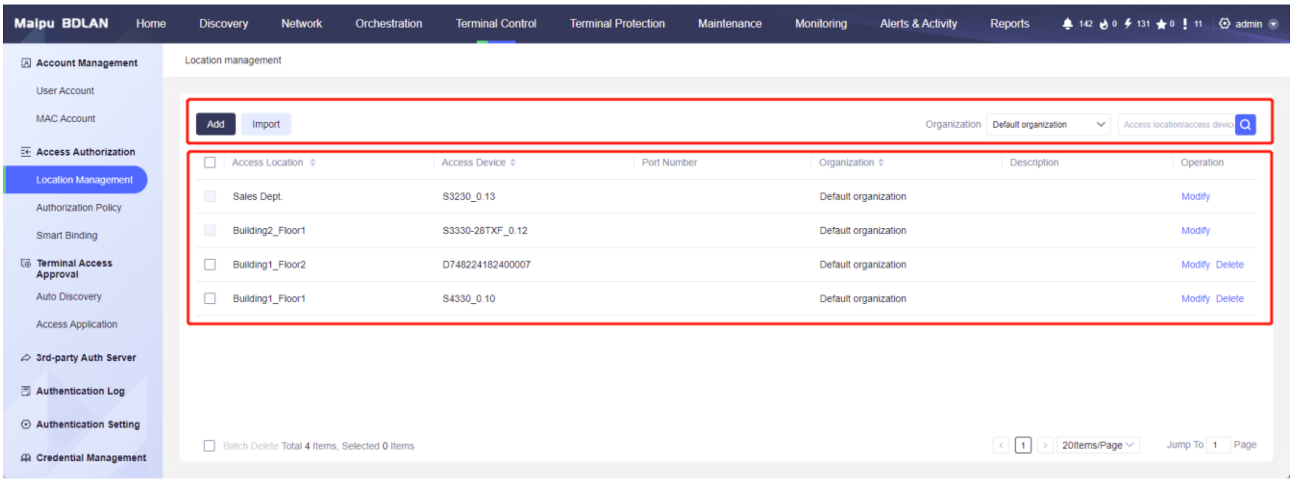


Figure 7.2.1.2 Access location interface

Access location function area:

Add button: You can add access data.

Import: You can import access locations in batches and download the import template.

Query button: query access location data according to query criteria.

Access location list:

The access location list shows the access location, access device, access port, organization, description and operation.

- Add access location

Click the **Add** button to display the “Add” pop-up box. The user needs to enter the access location name, organization, description, and select the access device and access port list. One of the access device and access interface is required, as shown in Figure 7.2.1.3.

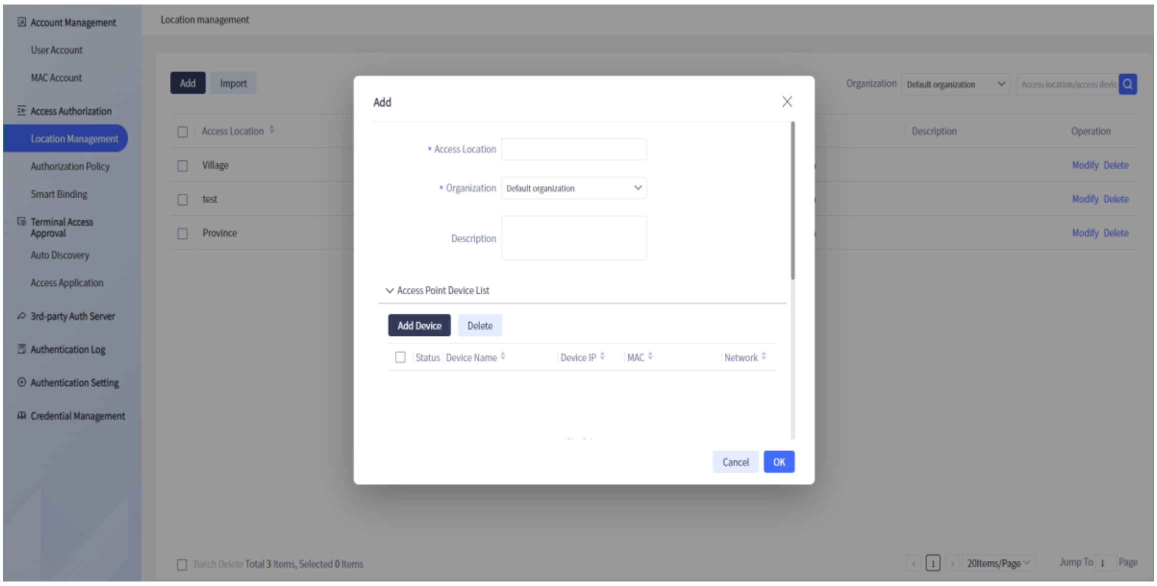


Figure 7.2.1.3 Add access location

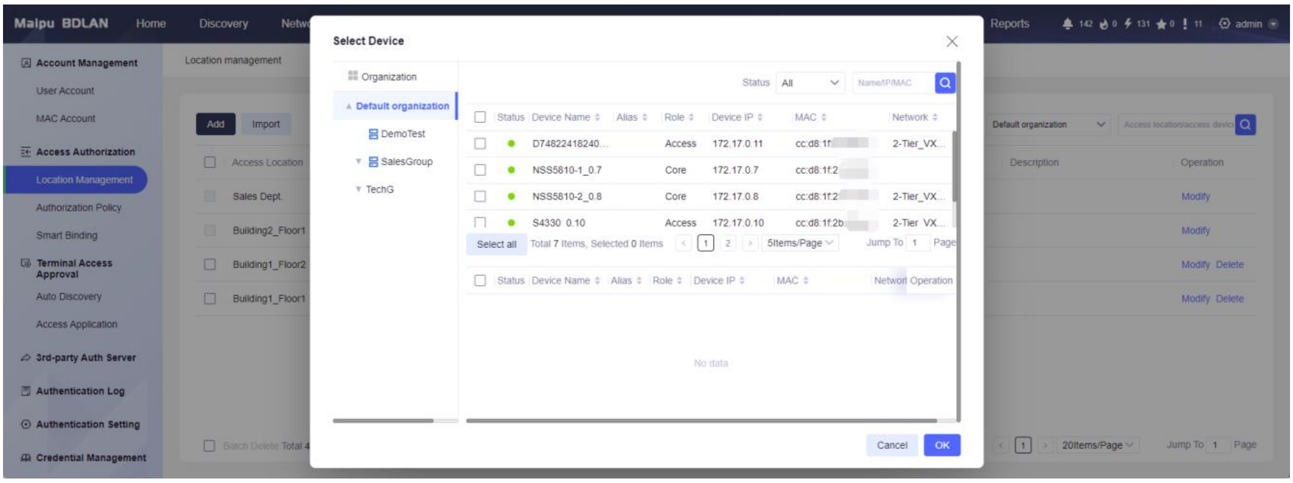
Access location name: required item; it cannot be greater than 32 characters.

Organization: required item; select the organization of the current administrator by default.

Description: optional; it cannot exceed 256 characters.

Access device list: click the “Add Device” button to display the “Select Device” pop-up box. The left side of the pop-up box displays the organization, and the right side displays two lists. Each line of the list displays the status, name, alias, role, IP, MAC, and network.

The first list shows a list of all devices in the organization. The second list displays the current selected device list. Click the “Delete” button on the right to delete the selected data. Click **OK** to return to the selected data. Click “Cancel” to cancel the device selection, as shown in Figure 7.2.1.4.



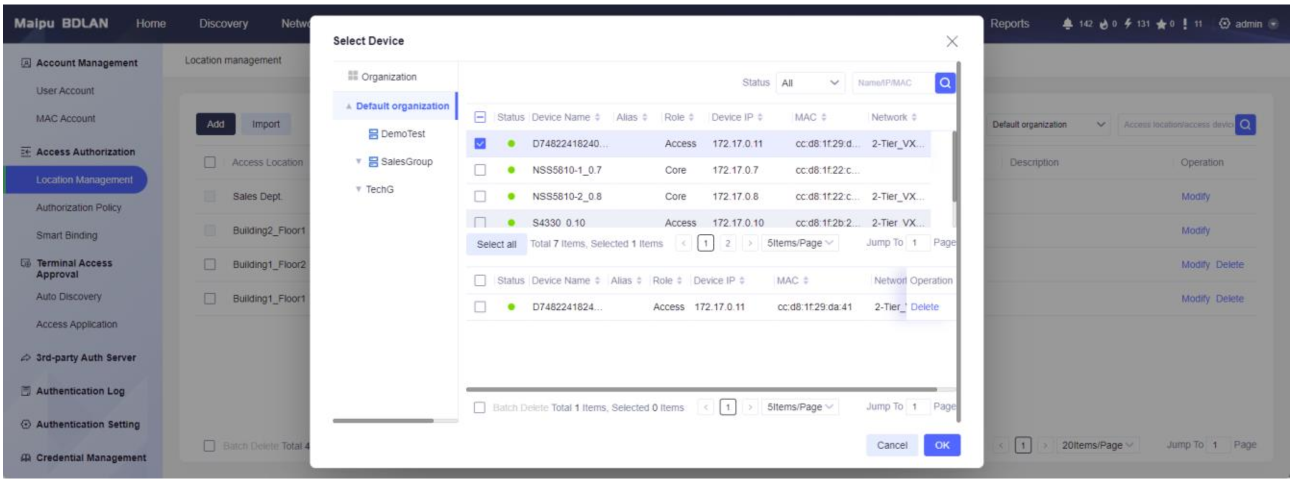
☐	Status	Device Name	Alias	Role	Device IP	MAC	Network
☐	●	D74822418240...		Access	172.17.0.11	cc:d8:1f[redacted]	2-Tier_VX...
☐	●	NSS5810-1_0.7		Core	172.17.0.7	cc:d8:1f:2[redacted]	
☐	●	NSS5810-2_0.8		Core	172.17.0.8	cc:d8:1f:2[redacted]	2-Tier_VX...
☐	●	S4330_0.10		Access	172.17.0.10	cc:d8:1f:2b[redacted]	2-Tier_VX...

Total 7 Items, Selected 0 Items 1 2 5Items/Page Jump To 1 Page

☐	Status	Device Name	Alias	Role	Device IP	MAC	Network	Operation

Figure 7.2.1.4 Select the access device

Access interface list: Click the “Add” button to display the “Select Interface” pop-up box. The left side of the pop-up box displays the organization, and the right side displays the query bar and two lists. Each line of the list displays the status, interface name, device name, device IP, interface IP and interface description. The first list displays the interface list, and the second list displays the selected interface list. Click the “Delete” button on the right to delete the selected data. Click **O**K to return to the selected data, as shown in Figure 7.2.1.5.



Status: All

Status	Device Name	Alias	Role	Device IP	MAC	Network
●	D74822418240...		Access	172.17.0.11	cc:d8:1f:29:d...	2-Tier_VX...
●	NSS5810-1_0.7		Core	172.17.0.7	cc:d8:1f:22:c...	
●	NSS5810-2_0.8		Core	172.17.0.8	cc:d8:1f:22:c...	2-Tier_VX...
●	S4330_0.10		Access	172.17.0.10	cc:d8:1f:2b:2...	2-Tier_VX...

Total 7 Items, Selected 1 Items 5Items/Page Jump To 1 Page

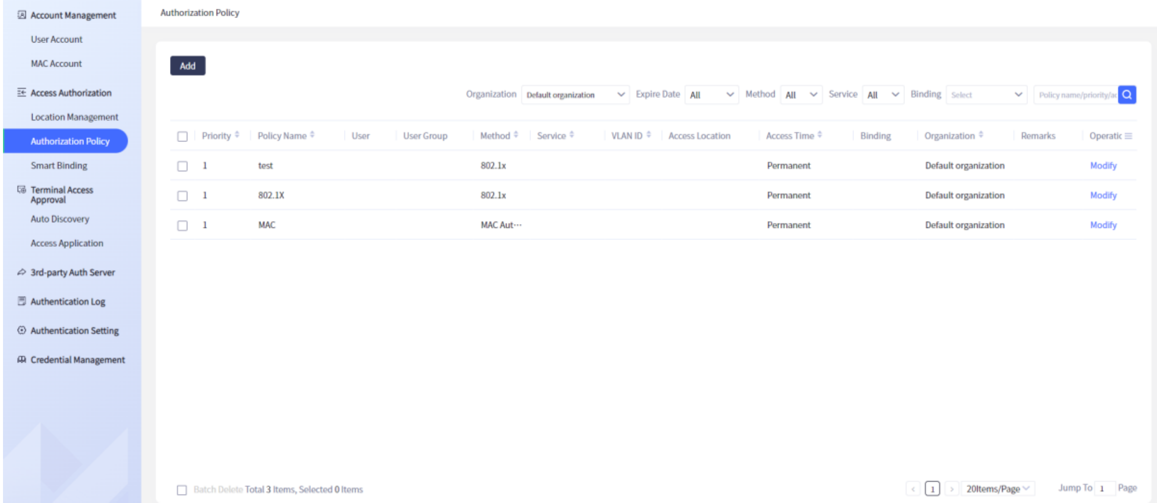
Status	Device Name	Alias	Role	Device IP	MAC	Network	Operation
●	D7482241824...		Access	172.17.0.11	cc:d8:1f:29:da:41	2-Tier_	Delete

Batch Delete Total 1 Items, Selected 0 Items 5Items/Page Jump To 1 Page

Figure 7.2.1.5 Select the access port

7.2.2 Authorization Policy

Select “Terminal Control” > “Access Authorization” at the top navigation bar, and open the "Authorization Policy" interface, which provides the functions, such as query, adding, modifying, batch deleting, and sorting.



Organization: Default organization Expire Date: All Method: All Service: All Binding: Select

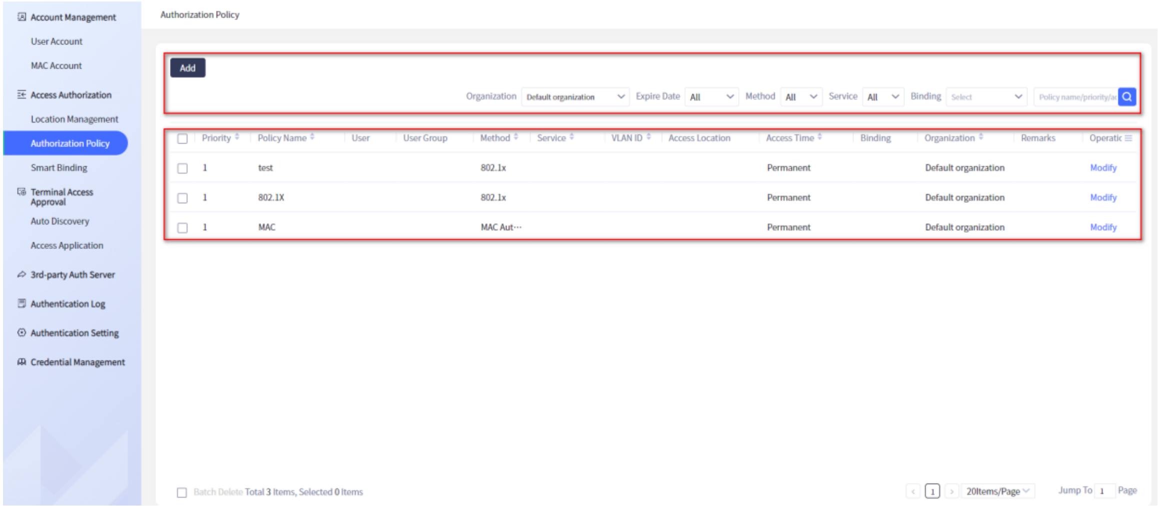
Priority	Policy Name	User	User Group	Method	Service	VLAN ID	Access Location	Access Time	Binding	Organization	Remarks	Operatic
1	test			802.1x				Permanent		Default organization		Modify
1	802.1X			802.1x				Permanent		Default organization		Modify
1	MAC			MAC Aut···				Permanent		Default organization		Modify

Batch Delete Total 3 Items, Selected 0 Items 20Items/Page Jump To 1 Page

Figure 7.2.2.1 Authorization policy navigation bar

- Authorization policy interface

The authorization policy interface is divided into two parts. The upper part is the function area, including query criteria, query button and add button; The lower part is the display list of access authorization policies. Click the icon in the list operation column, and you can customize the columns displayed in the list.



Organization: Default organization Expire Date: All Method: All Service: All

☐	Priority	Policy Name	User	User Group	Method	Service	VLAN ID	Access Location	Access Time	Binding	Organization	Remarks	Operatic
☐	1	test			802.1x				Permanent		Default organization		Modify
☐	1	802.1X			802.1x				Permanent		Default organization		Modify
☐	1	MAC			MAC Aut···				Permanent		Default organization		Modify

Total 3 Items, Selected 0 Items 1 20Items/Page Jump To 1

Figure 7.2.2.2 Authorization policy interface

Authorization policy function area:

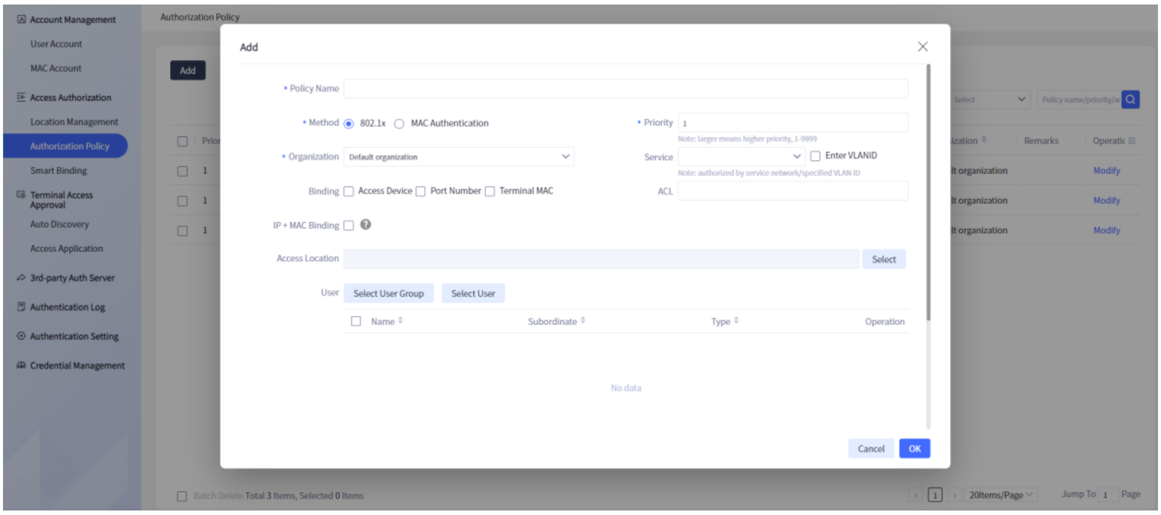
Add button: You can add the access authorization policy data.

Query button: Query the access authorization policy data according to the query criteria including organization, expire date, authentication method, service network, and authentication binding.

List of access authorization policies:

The access authorization policy list displays priority, policy name, user, user group, authentication method, service network, VLAN ID, access location, access time, authentication binding, organization, remarks and operations.

- Add access authorization policy



* Policy Name
* Method ● 802.1x ○ MAC Authentication
* Priority 1
Note: larger means higher priority, 1-9999
* Organization Default organization
Service ☐ Enter VLANID
Note: authorized by service network/specified VLAN ID
Binding ☐ Access Device ☐ Port Number ☐ Terminal MAC
ACL
IP + MAC Binding ☐
Access Location
User

Figure 7.2.2.3 Add access authorization policy

To add an access authorization policy, you need to fill in the policy name, authentication method, priority, organization, service network, VLAN ID, authentication binding, ACL, IP+MAC binding, access location, user, access time range, and remarks.

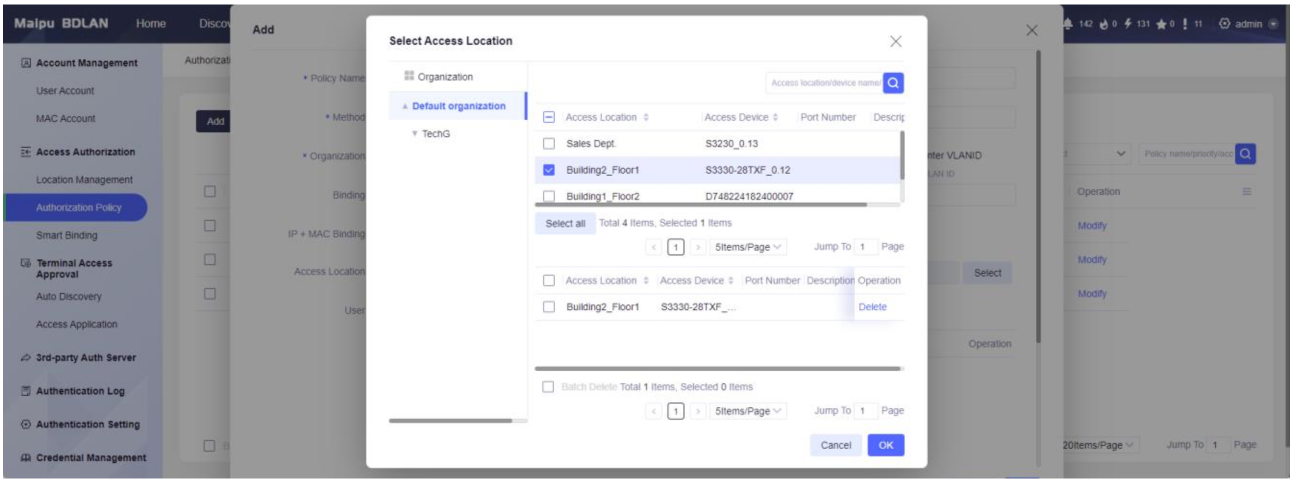
Priority: required item. The higher the number, the higher the priority. The range is 1-9999. When the priority is the same, the latest created priority is higher.

Organization: You can select the organization of the policy.

Binding: After the terminal MAC is checked, the binding quantity will appear. The default quantity is 1.

Remarks: The length of remarks shall not exceed 256 characters.

Access location: Click **Select** to display the “Select Access Location” pop-up box. The left side of the pop-up box displays the organization, and the right side displays the query bar and two lists. The first list displays the access location data, and the second displays the selected data. Click **OK** to display the selected data in the input box, as shown in the following figure.



Select Access Location

Organization
Default organization
TechG

☐	Access Location	Access Device	Port Number	Descrip
☐	Sales Dept.	S3230_0.13		
☑	Building2_Floor1	S3330-28TXF_0.12		
☐	Building1_Floor2	D748224182400007		

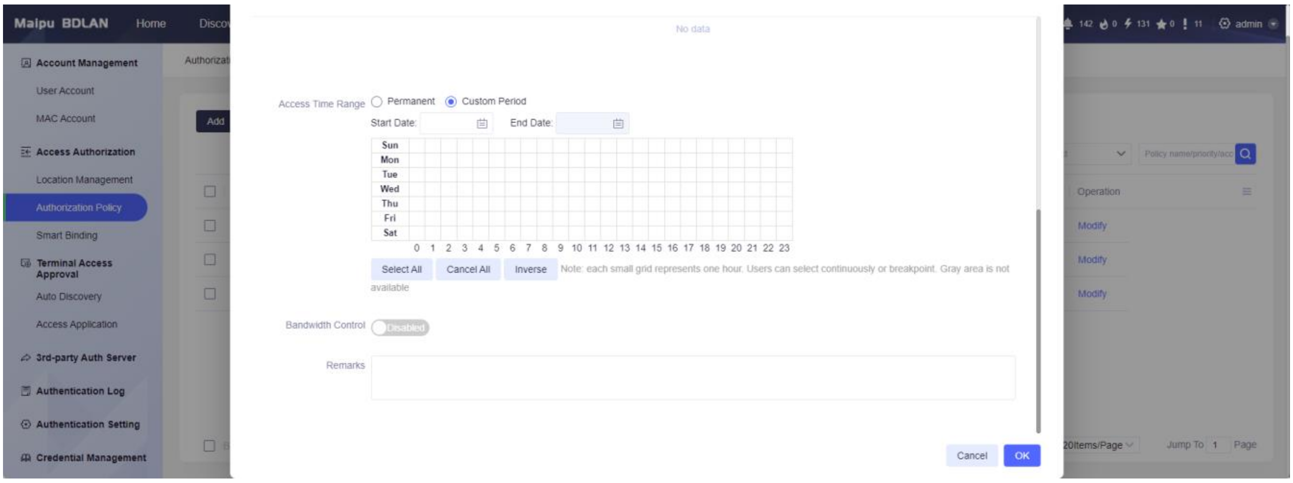
Select all Total 4 Items, Selected 1 Items

☐	Access Location	Access Device	Port Number	Description	Operation
☐	Building2_Floor1	S3330-28TXF_...			Delete

Batch Delete Total 1 Items, Selected 0 Items

Figure 7.2.2.4 Select access location

Access time range: click **Custom Period** to select start time, end time and time range. After selecting the start time and end time, you can select a specific time range. Each small box represents one hour. You can select at a breakpoint. The gray area is not optional, as shown in the following figure.



Access Time Range ○ Permanent ● Custom Period

Start Date: End Date:

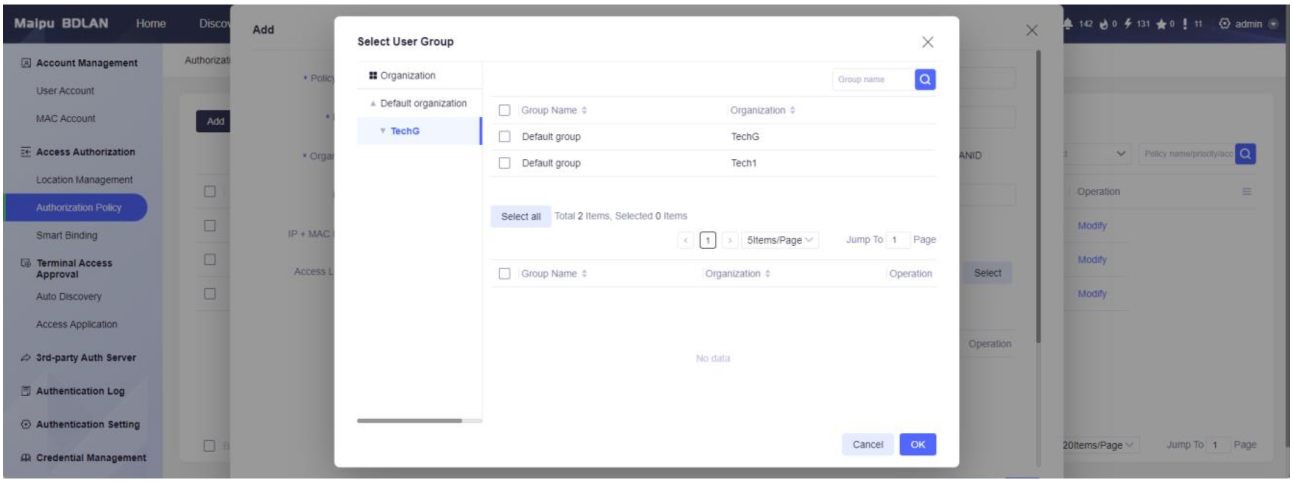
Note: each small grid represents one hour. Users can select continuously or breakpoint. Gray area is not available

Bandwidth Control: Disabled

Remarks

Figure 7.2.2.5 Access authorization time range

User list: Click **Select User Group** to display the “Select User Group” pop-up box. The left side of the pop-up box displays the organization, and the right side displays the query bar and two lists. The first list displays the user group data, and the second displays the selected data. After clicking **OK**, the selected data will be displayed in the user group list, and the data can be deleted in the user list, as shown in Figure 7.2.2.6.



Group Name	Organization
Default group	TechG
Default group	Tech1

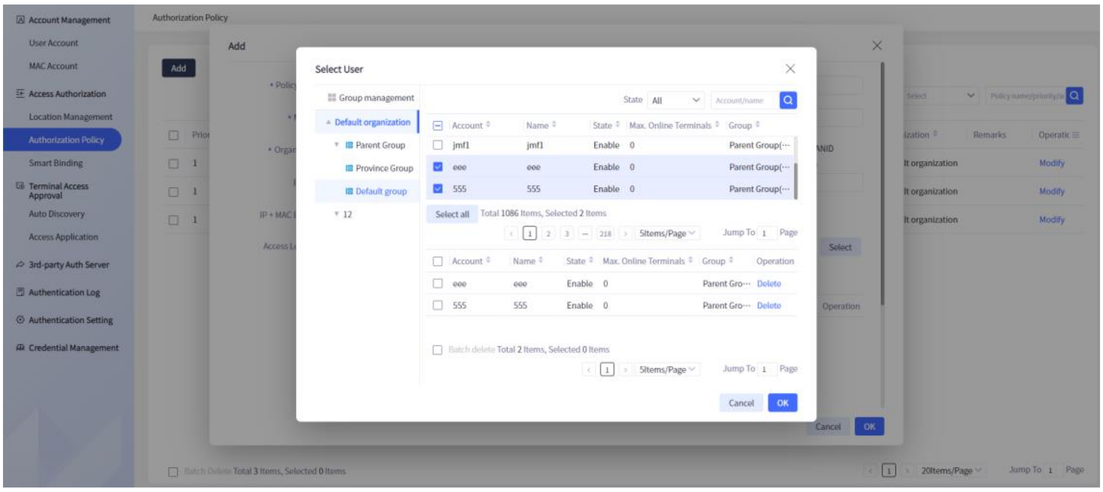
Total 2 Items, Selected 0 Items

Group Name	Organization	Operation

No data

Figure 7.2.2.6 Select user group

Click **Select User**. The left side of the pop-up box displays the organization, and the right side displays the query bar and two lists. The first list displays the selected user data, and the second displays the selected data. After clicking **OK**, the selected data will be displayed in the user list, where you can delete user groups and user data, as shown in the following figure.



Account	Name	State	Max. Online Terminals	Group
jmf1	jmf1	Enable	0	Parent Group(···
eee	eee	Enable	0	Parent Group(···
555	555	Enable	0	Parent Group(···

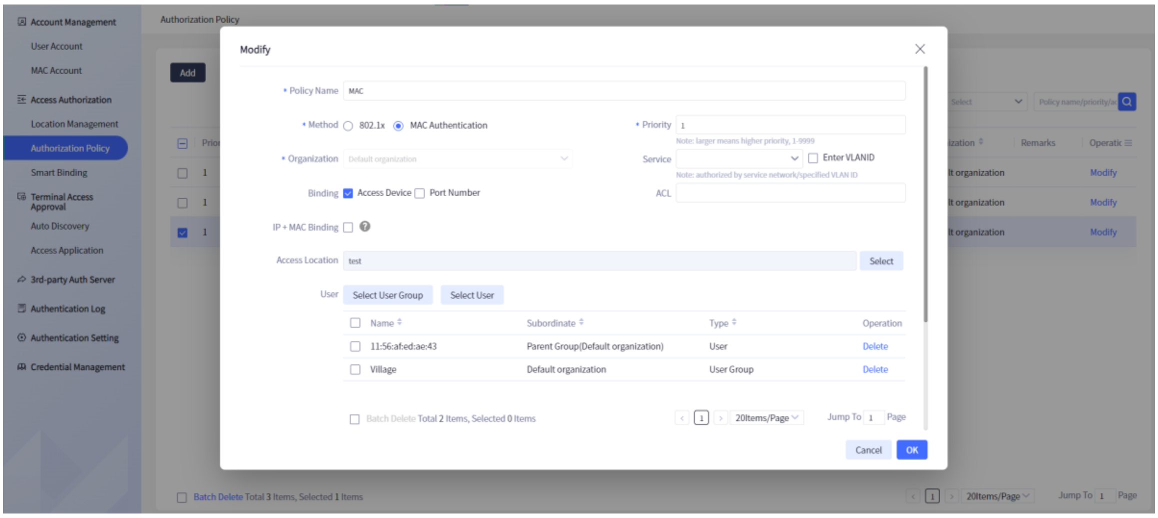
Total 1086 Items, Selected 2 Items

Account	Name	State	Max. Online Terminals	Group	Operation
eee	eee	Enable	0	Parent Gro···	Delete
555	555	Enable	0	Parent Gro···	Delete

Total 2 Items, Selected 0 Items

Figure 7.2.2.7 Select user

- Edit authorization policy


Modify
Note: larger means higher priority, 1-9999
Enter VLANID
Note: authorized by service network/specified VLAN ID
Select
Select User Group
Select User
20Items/Page
Jump To
Page
Cancel
OK

Policy Name: MAC

Method: ○ 802.1x ● MAC Authentication

Priority: 1

Organization: Default organization

Service:

Binding: ☑ Access Device ☐ Port Number

ACL:

IP + MAC Binding: ☐

Access Location: test

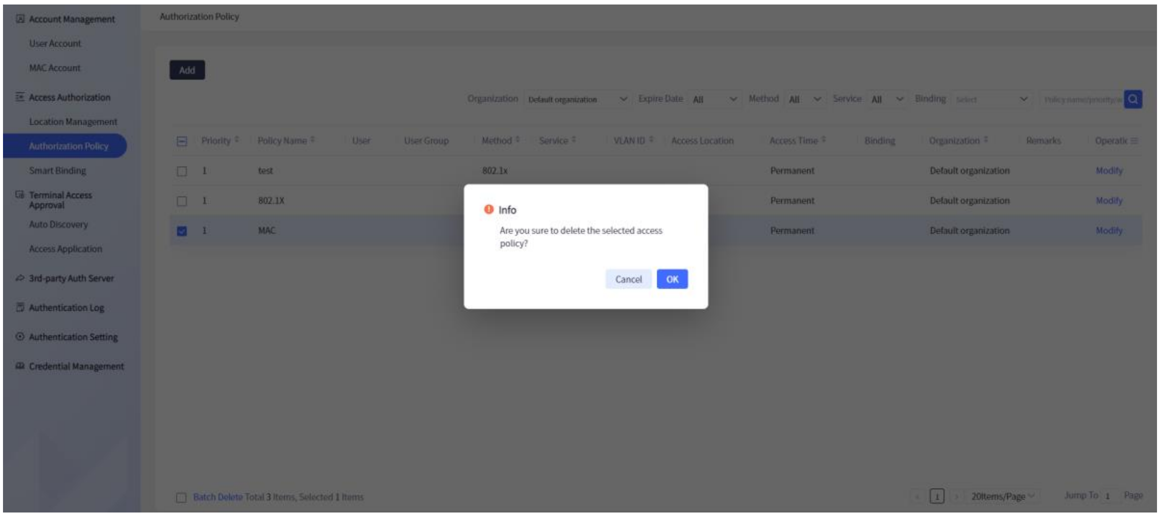
Name	Subordinate	Type	Operation
11:56:af:ed:ae:43	Parent Group(Default organization)	User	Delete
Village	Default organization	User Group	Delete

Batch Delete Total 2 Items, Selected 0 Items

Figure 7.2.2.8 Edit authorization policy

Click the **Edit** button to modify the access authorization policy. You can modify the policy name, authentication method, priority, service network, VLAN ID, authentication binding, ip+mac binding, access location, user group/user, access time range, and remarks.

- Delete authorization policy



☐	Priority	Policy Name	User	User Group	Method	Service	VLAN ID	Access Location	Access Time	Binding	Organization	Remarks	Operatic
☐	1	test			802.1x				Permanent		Default organization		Modify
☐	1	802.1X							Permanent		Default organization		Modify
☑	1	MAC							Permanent		Default organization		Modify

Info

Are you sure to delete the selected access policy?

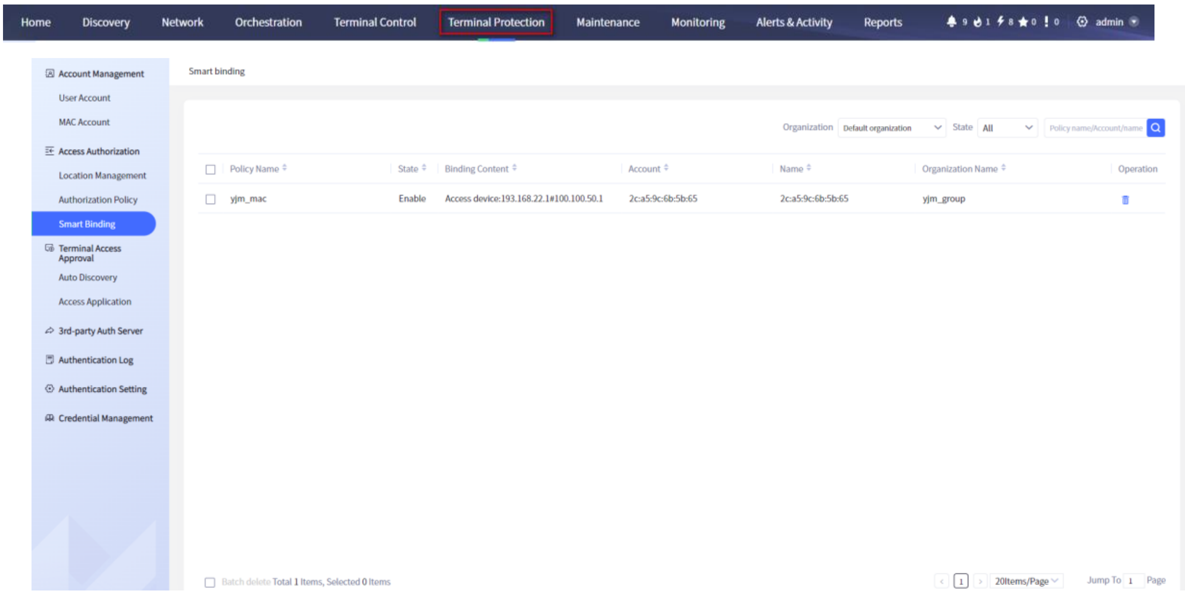
Total 3 Items, Selected 1 Items

Figure 7.2.2.9 Delete authorization policy

Select the desired access authorization policy, click the **Batch Delete** button below, and a pop-up window for confirming the deletion appears. Click **OK** to execute the deletion operation, and select **Cancel** to abort the deletion operation.

7.2.3 Smart Binding

Smart binding is to bind the instance according to the policy generated by the access authorization policy during the authentication process. In the access authorization policy, you can set the binding of access devices, access ports, terminal MAC, mac+ip and authentication accounts to authenticate and bind. During the authentication process, generate smart binding instances. If the number of instances exceeds the limit or is disabled, authentication will be rejected. Click "Terminal Control" > "Access Authorization" on the navigation bar at the top of the system to open the "Smart Binding" interface, as shown in the following figure:

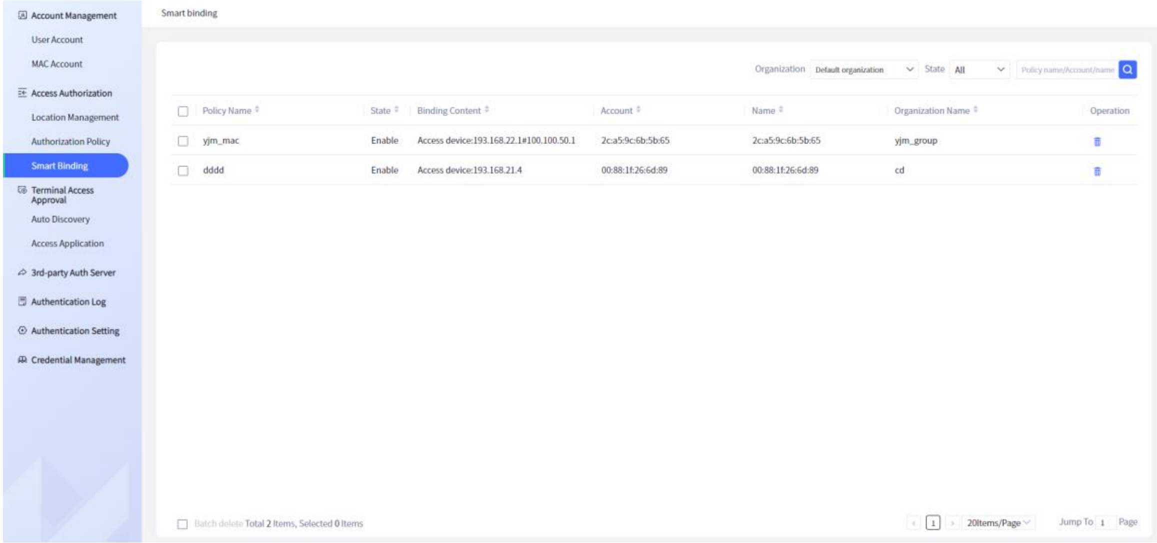


☐	Policy Name	State	Binding Content	Account	Name	Organization Name	Operation
☐	yjm_mac	Enable	Access device:193.168.22.1#100.100.50.1	2c:a5:9c:6b:5b:65	2c:a5:9c:6b:5b:65	yjm_group	🗑

Total 1 Items, Selected 0 Items

Figure 7.2.3.1 Smart binding

Smart binding information supports fuzzy query by organization, status, policy name, account and name. Click each field in the header of the smart binding list to sort the smart binding information according to the corresponding field, as shown in the following figure:

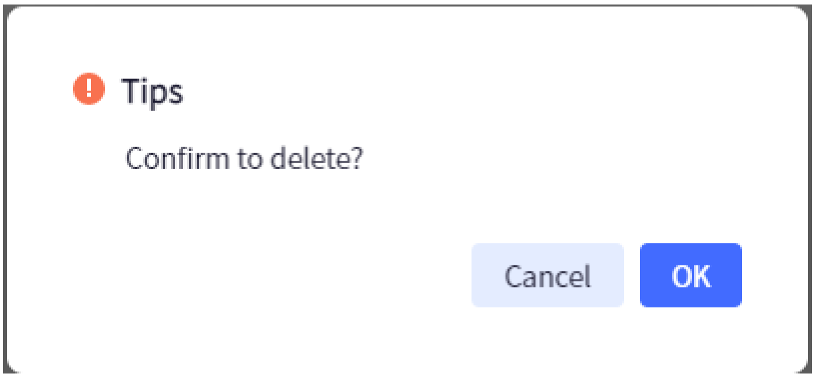


☐	Policy Name	State	Binding Content	Account	Name	Organization Name	Operation
☐	yjm_mac	Enable	Access device:193.168.22.1#100.100.50.1	2c:a5:9c:6b:5b:65	2c:a5:9c:6b:5b:65	yjm_group	🗑
☐	dddd	Enable	Access device:193.168.21.4	00:88:1f:26:6d:89	00:88:1f:26:6d:89	cd	🗑

Total 2 Items, Selected 0 Items

Figure 7.2.3.2 Query smart binding

Check the smart binding information. Click the button 🗑 behind the smart binding information and click **OK** in the pop-up window of confirming the deletion, as shown in the following figure:


Tips

Confirm to delete?

Figure 7.2.3.3 Confirm deletion

Click OK to delete the smart binding instance information.

Note

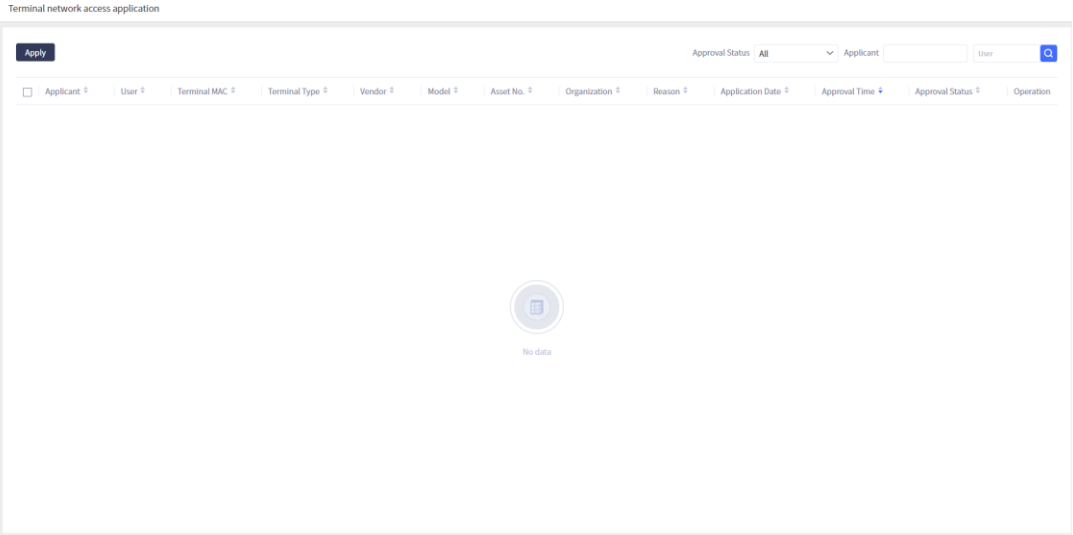
- The binding number of terminal MAC and authentication account ranges from 1 to 50.

7.3 Terminal Access Approval

7.3.1 Terminal network access application

Go to Terminal Control>Terminal Access Approval, as shown in figure 7.3.1.2

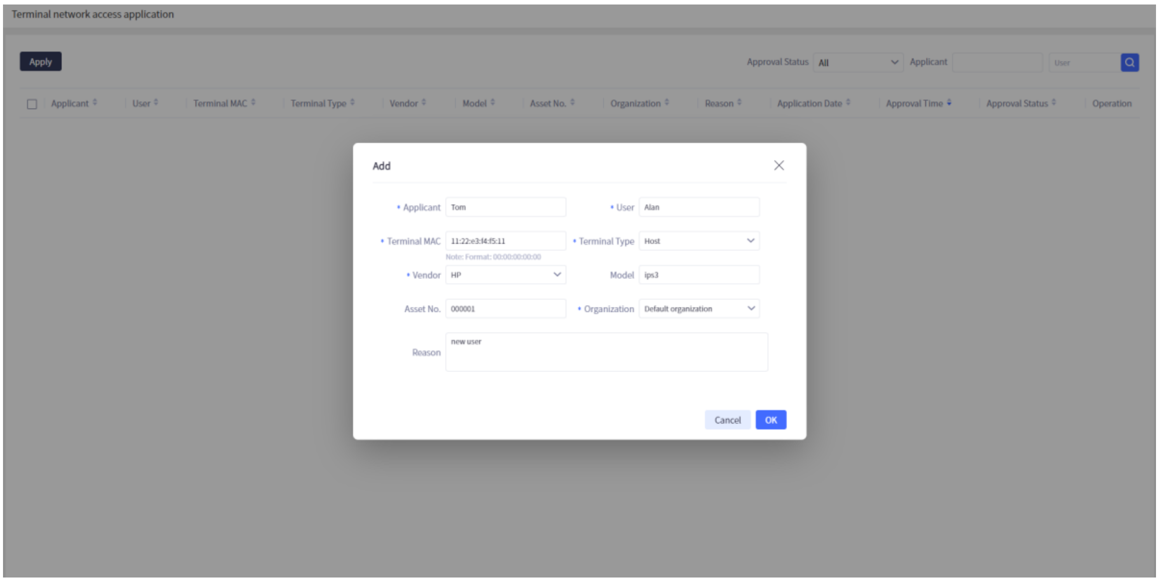
Figure 7.3.1.1 Login interface



Applicant	User	Terminal MAC	Terminal Type	Vendor	Model	Asset No.	Organization	Reason	Application Date	Approval Time	Approval Status	Operation

Figure 7.3.1.2 Terminal network access application

Click **Apply** to start adding terminal network access application, as shown in figure 7.3.1.3. Only rejected terminal applications can be edited.



Approval Status: All

* Applicant: Tom
* User: Alan
* Terminal MAC: 11:22:e3:f4:f5:11
Note: Format: 00:00:00:00:00
* Terminal Type: Host
* Vendor: HP
Model: ips3
Asset No.: 000001
* Organization: Default organization
Reason: new user

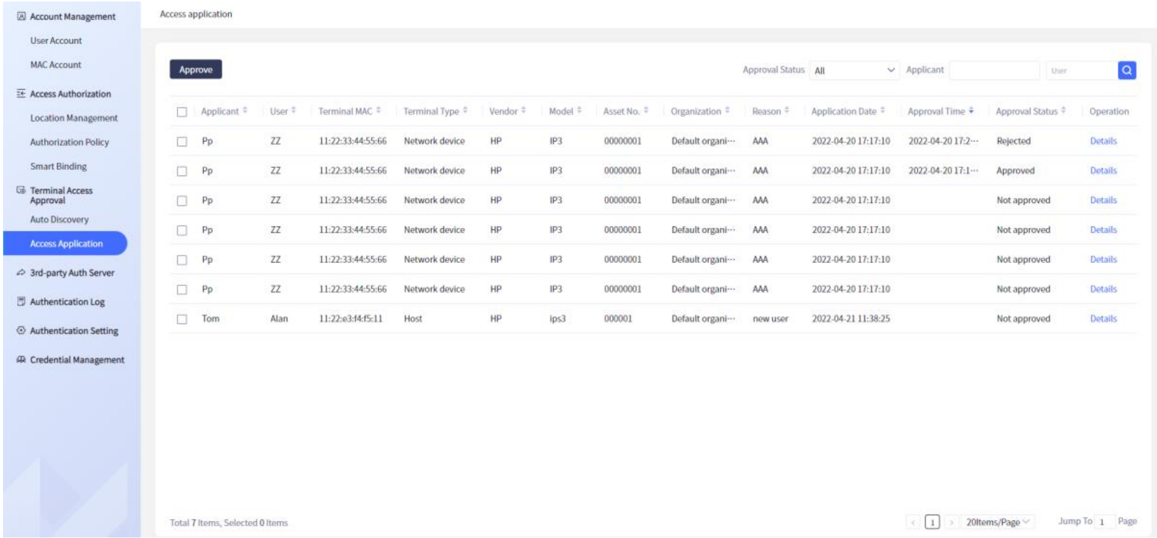
Figure 7.3.1.3 Add terminal network access application

Note

- At the terminal network access application, the application record can be queried only by the applicant or user, and fuzzy query is not supported.

7.3.2 Terminal Access Approval

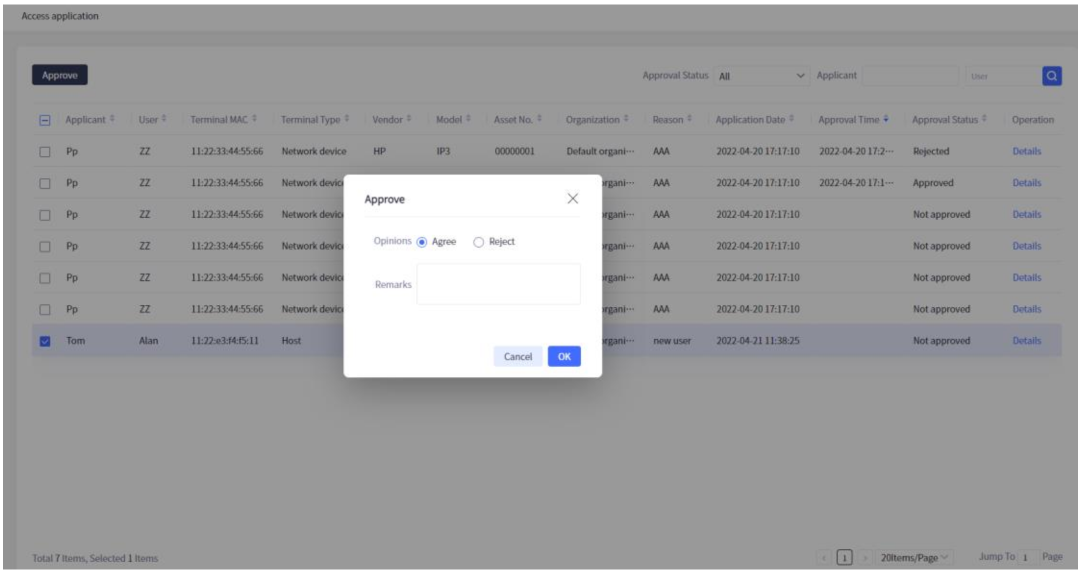
After logging into the system, you can see the terminal submitting the application in **Terminal Access Approval → Access Application**, as shown in figure 7.3.2.1:



☐	Applicant	User	Terminal MAC	Terminal Type	Vendor	Model	Asset No.	Organization	Reason	Application Date	Approval Time	Approval Status	Operation
☐	Pp	ZZ	11:22:33:44:55:66	Network device	HP	IP3	00000001	Default organi···	AAA	2022-04-20 17:17:10	2022-04-20 17:2···	Rejected	Details
☐	Pp	ZZ	11:22:33:44:55:66	Network device	HP	IP3	00000001	Default organi···	AAA	2022-04-20 17:17:10	2022-04-20 17:1···	Approved	Details
☐	Pp	ZZ	11:22:33:44:55:66	Network device	HP	IP3	00000001	Default organi···	AAA	2022-04-20 17:17:10		Not approved	Details
☐	Pp	ZZ	11:22:33:44:55:66	Network device	HP	IP3	00000001	Default organi···	AAA	2022-04-20 17:17:10		Not approved	Details
☐	Pp	ZZ	11:22:33:44:55:66	Network device	HP	IP3	00000001	Default organi···	AAA	2022-04-20 17:17:10		Not approved	Details
☐	Pp	ZZ	11:22:33:44:55:66	Network device	HP	IP3	00000001	Default organi···	AAA	2022-04-20 17:17:10		Not approved	Details
☐	Tom	Alan	11:22:e3:f4:f5:11	Host	HP	ips3	000001	Default organi···	new user	2022-04-21 11:38:25		Not approved	Details

Figure 7.3.2.1 View access application

The approval terminal can agree or reject, as shown in figure 7.3.2.2. After rejection, you can modify the application information at the re-access application and submit it again.



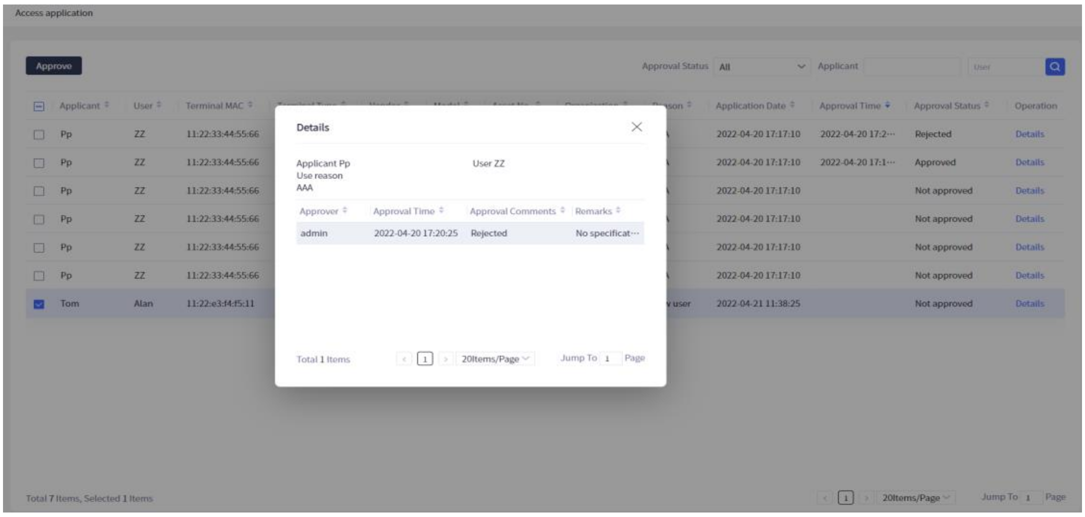
Approve

Opinions ● Agree ○ Reject

Remarks

Figure 7.3.2.2 Approve terminal access application

After approval, you can view the approval details of an application, as shown in figure 7.3.2.3.



Details

Applicant Pp
Use reason
AAA

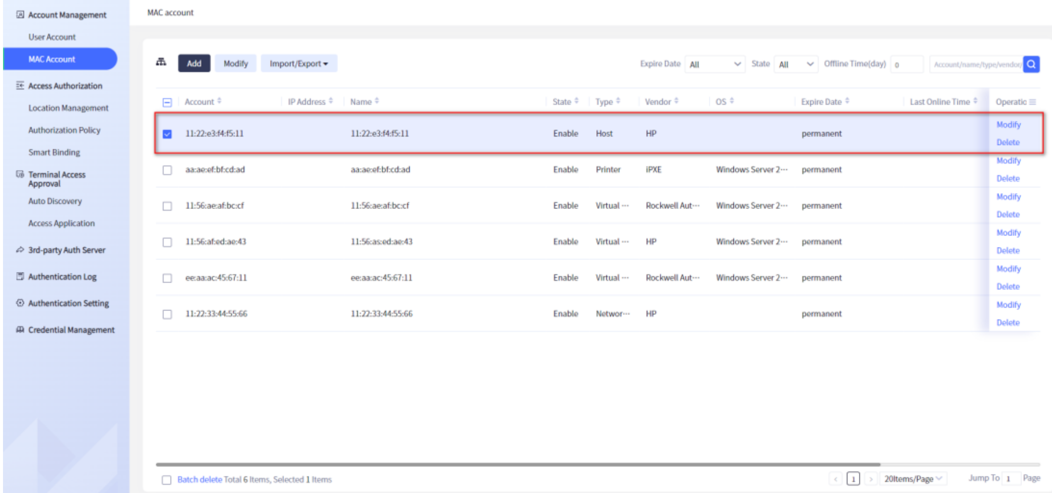
User ZZ

Approver	Approval Time	Approval Comments	Remarks
admin	2022-04-20 17:20:25	Rejected	No specificat···

Total 1 Items

Figure 7.3.2.3 View terminal network access approval details

The approved terminal can be seen in **Terminal Control → Account Management → MAC Account**, as shown in figure 7.3.2.4.



☐	Account	IP Address	Name	State	Type	Vendor	OS	Expire Date	Last Online Time	Operatio
☑	11:22:e3:f4:f5:11		11:22:e3:f4:f5:11	Enable	Host	HP		permanent		Modify Delete
☐	aa:ae:ef:bf:cd:ad		aa:ae:ef:bf:cd:ad	Enable	Printer	iPXE	Windows Server 2···	permanent		Modify Delete
☐	11:56:ae:af:bc:cf		11:56:ae:af:bc:cf	Enable	Virtual ···	Rockwell Aut···	Windows Server 2···	permanent		Modify Delete
☐	11:56:af:ed:ae:43		11:56:as:ed:ae:43	Enable	Virtual ···	HP	Windows Server 2···	permanent		Modify Delete
☐	ee:aa:ac:45:67:11		ee:aa:ac:45:67:11	Enable	Virtual ···	Rockwell Aut···	Windows Server 2···	permanent		Modify Delete
☐	11:22:33:44:55:66		11:22:33:44:55:66	Enable	Networ···	HP		permanent		Modify Delete

☐ Batch delete Total 6 Items, Selected 1 Items

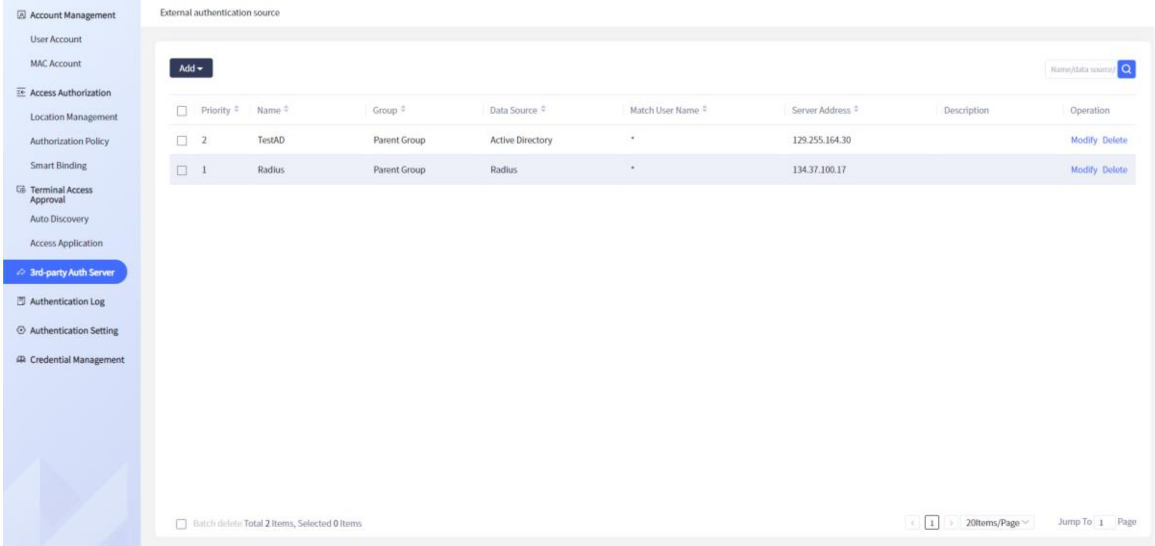
Figure 7.3.2.4 View terminal information

7.4 External Authentication Source

Click "**Terminal Control**" > "**3rd-party Auth Server**" at the top, and the external authentication source interface displays the data of the AD domain and Radius. It provides functions, such as adding, modifying, deleting, batch deleting, and querying.

- External authentication source interface

The external authentication source is divided into two parts. The top function area contains the add button and the query button. The lower part is a list of external authentication sources.



☐	Priority	Name	Group	Data Source	Match User Name	Server Address	Description	Operation
☐	2	TestAD	Parent Group	Active Directory	*	129.255.164.30		Modify Delete
☐	1	Radius	Parent Group	Radius	*	134.37.100.17		Modify Delete

☐ Batch delete Total 2 Items, Selected 0 Items

Figure 7.4.1 External authentication source interface

- External authentication source ribbon

Add button: add external authentication source through ad domain and radius.

Query button: filter data based on fuzzy query.

Delete: delete a single external authentication source data.

Batch delete: batch delete the selected external authentication source data.

Modify: modify a single external authentication source data.

- Add external authentication source AD domain

  To add an AD domain, you need to fill in the server name, domain name operation behavior, user account domain, domain controller domain name, domain management user name, match user name, user password, confirm password, port, user group, priority, user root DN and description.

  Server name: required item. The input value does not duplicate other data. The length cannot be greater than 64 characters. It can only be composed of letters and numbers.

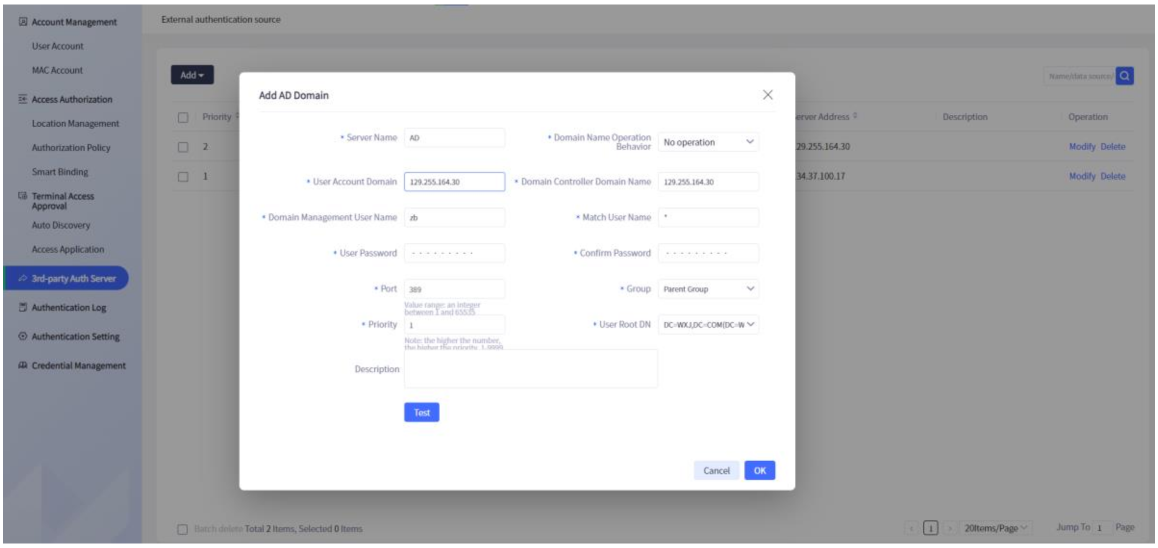
  Domain name operation behavior: no operation by default. If you select **Domain name stripping** or **Domain name adding**, you need to fill in the domain name matching method and domain name.

  User password and confirm password: required items. The two entries must be identical.

  Priority: required item. The value to be entered does not duplicate other data.

  User Root DN: You need to query according to user account domain, domain management user name, user password, port and matching user name.

  Test button: tests whether the value entered by the user can pass the verification. If it fails, a prompt will be given. If it passes, it will prompt that the test passes.



* Server Name: AD

* Domain Name Operation Behavior: No operation

* User Account Domain: 129.255.164.30

* Domain Controller Domain Name: 129.255.164.30

* Domain Management User Name: zb

* Match User Name: *

* User Password: ·········

* Confirm Password: ·········

* Port: 389

Value range: an integer between 1 and 65535

* Group: Parent Group

* Priority: 1

Note: the higher the number, the higher the priority. 1-9999

* User Root DN: DC=WXJ,DC=COM(DC=W

Description:

Total 2 Items, Selected 0 Items

Figure 7.4.2 Add AD domain

- Add external authentication source radius

  To add Radius, you need to fill in the server name, match user name, user group, master server (address, port, preshared key, priority), standby server (address, port, preshared key, priority), priority, EAP termination, and description.

  Server name: required item. The value to be entered does not duplicate other data. The length cannot be greater than 64 characters. It can only be composed of letters and numbers.

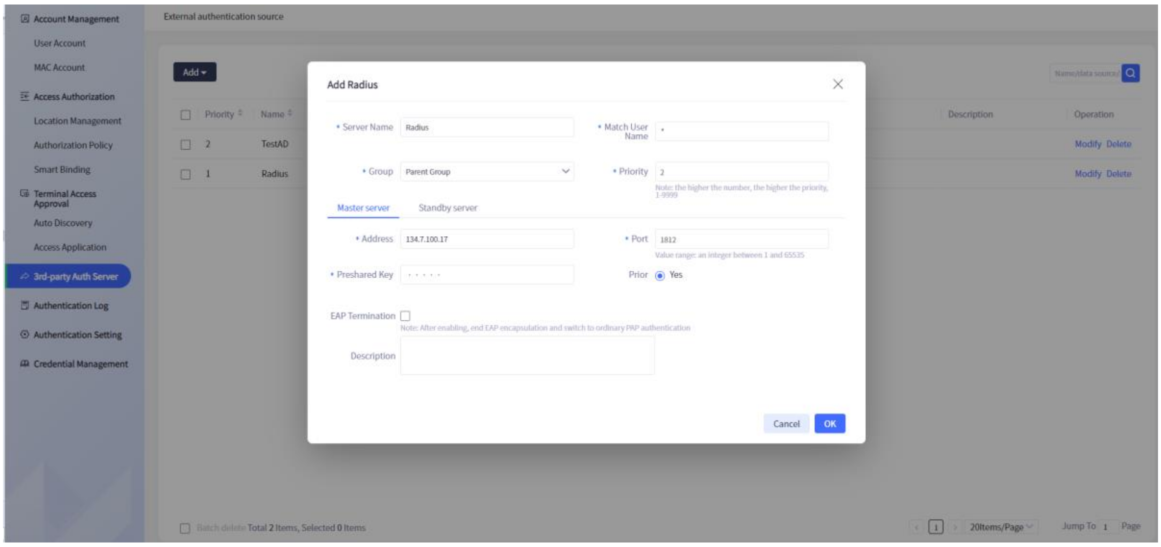
  Master Server: required items, address, port and preshared key are required, whether to choose first: from server 1 and server 2

  Select the server with "Yes" first.

  Standby Server: optional, hidden by default.

  Preshared key: required.

  Priority: required item. The value to be entered does not duplicate other data.



Add Radius

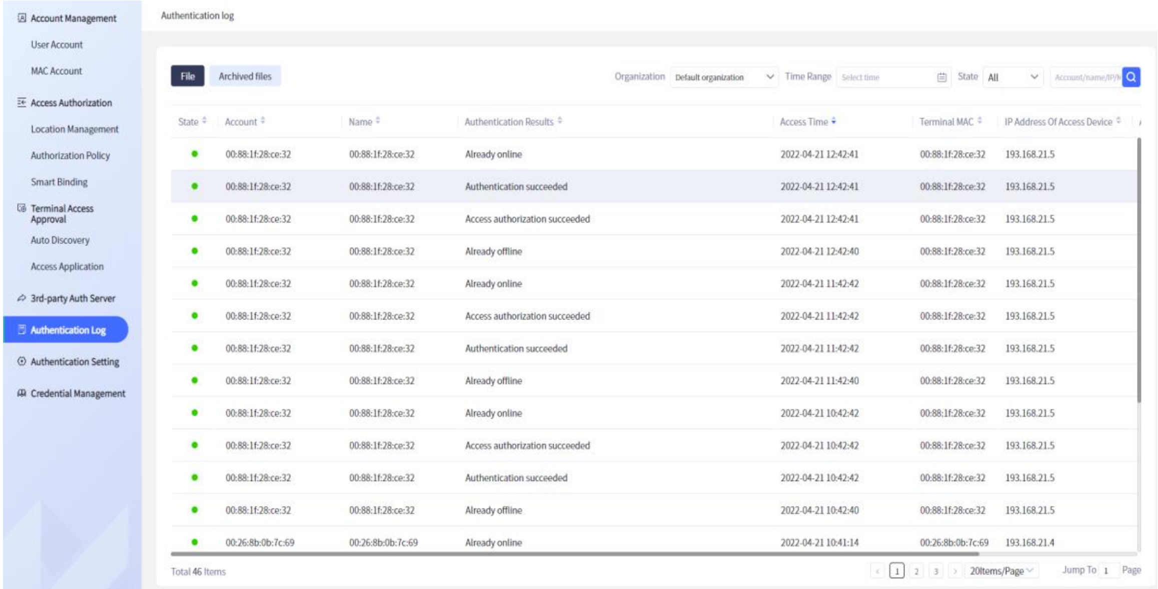
- Server Name: Radius
- Match User Name: *
- Group: Parent Group
- Priority: 2 (Note: the higher the number, the higher the priority, 1-9999)
- Master server | Standby server
- Address: 134.7.100.17
- Port: 1812 (Value range: an integer between 1 and 65535)
- Preshared Key: ······
- Prior: ● Yes
- EAP Termination: ☐ (Note: After enabling, end EAP encapsulation and switch to ordinary PAP authentication)
- Description:

Total 2 Items, Selected 0 Items

Figure 7.4.3 Add Radius

7.5 Authentication Logs

The authentication log provides the functions related to query, archiving, historical archive file query and archive file export of the log information generated by access authentication. Click "Terminal Control" > "Authentication Log" on the navigation bar at the top of the system to open the "Authentication Log" interface, as shown in the following figure:



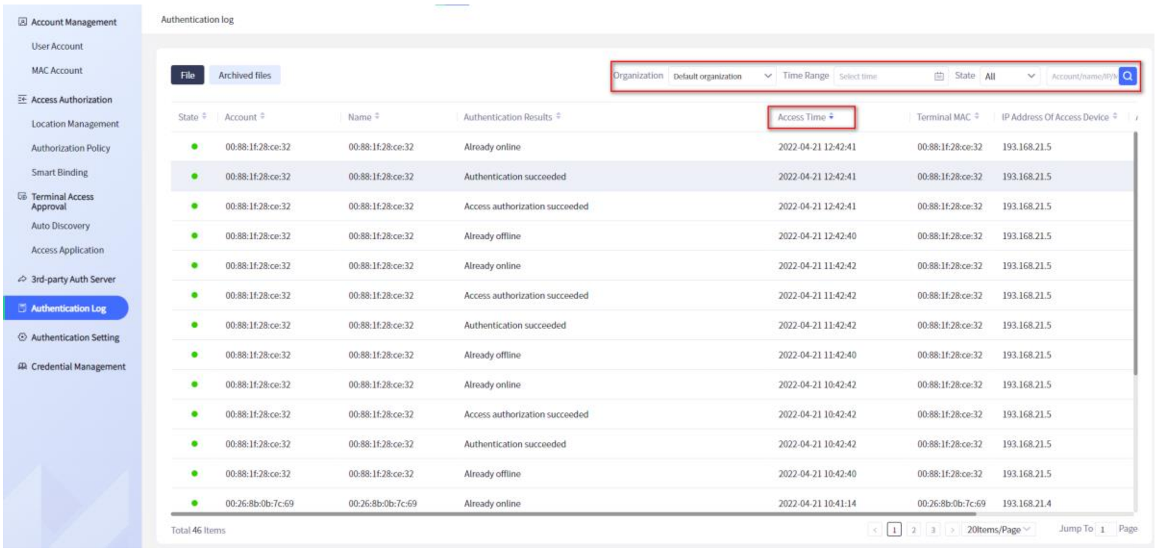
Organization: Default organization | Time Range: Select time | State: All | Account/name/IP/M

State	Account	Name	Authentication Results	Access Time	Terminal MAC	IP Address Of Access Device
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 12:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 11:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 10:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	Already online	2022-04-21 10:41:14	00:26:8b:0b:7c:69	193.168.21.4

Total 46 Items | 1 2 3 | 20Items/Page | Jump To 1 Page

Figure 7.5.1 Authentication log

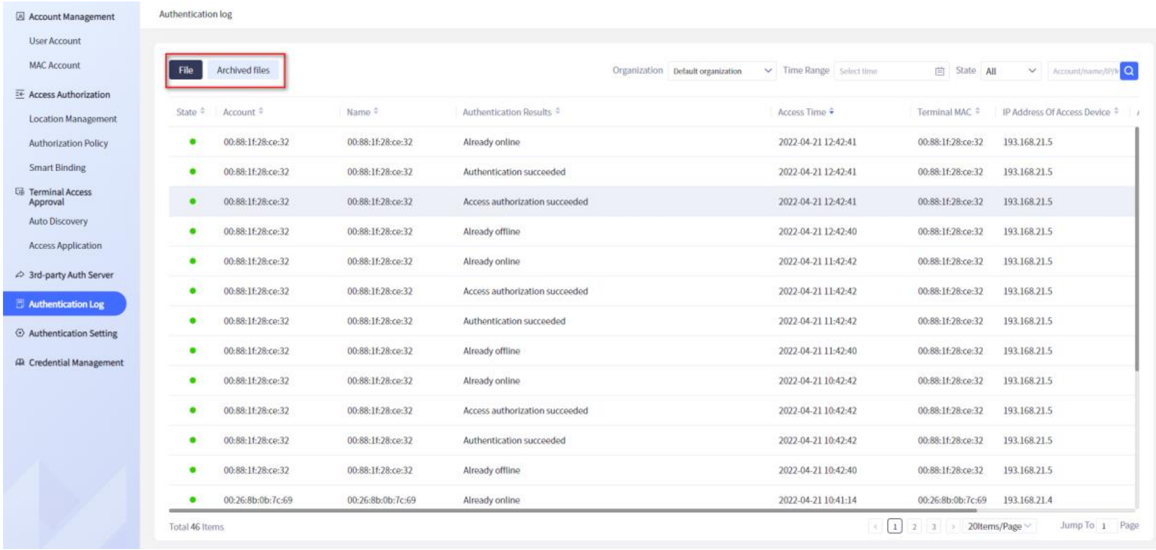
The authentication log list supports paging display, and each authentication log information is attached to the organization. Different users can only view the authentication log information used by the user and its subordinate organizations when logging in. Authentication log information supports fuzzy query through organization, time range, status, account, name, IP and MAC. Click each field in the header of the authentication log list to sort the authentication log information according to the corresponding field, as shown in the following figure:



State	Account	Name	Authentication Results	Access Time	Terminal MAC	IP Address Of Access Device
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 12:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 11:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 10:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	Already online	2022-04-21 10:41:14	00:26:8b:0b:7c:69	193.168.21.4

Figure 7.5.2 Query authentication log

Click the button File to archive the queried authentication log information, and click the button Archived files to view the historical archived file, as shown in the following figure:



State	Account	Name	Authentication Results	Access Time	Terminal MAC	IP Address Of Access Device
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 12:42:41	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 12:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 11:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 11:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already online	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Access authorization succeeded	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Authentication succeeded	2022-04-21 10:42:42	00:88:1f:28:ce:32	193.168.21.5
●	00:88:1f:28:ce:32	00:88:1f:28:ce:32	Already offline	2022-04-21 10:42:40	00:88:1f:28:ce:32	193.168.21.5
●	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	Already online	2022-04-21 10:41:14	00:26:8b:0b:7c:69	193.168.21.4

Figure 7.5.3 Archiving logs

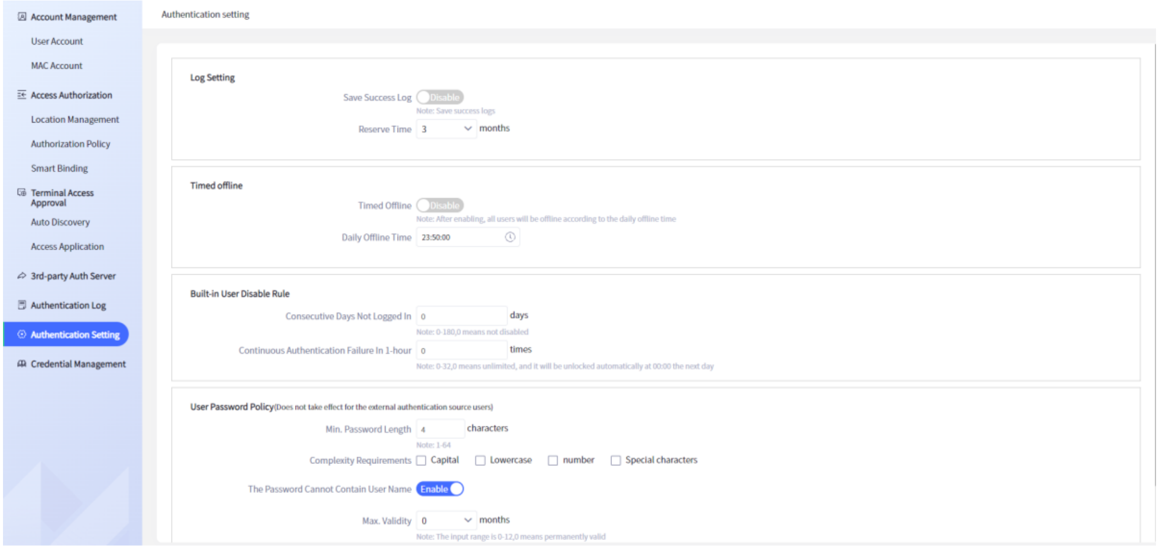
Select the file in the historical archive pop-up box, and click the **Export** button at the back to download the archived log file to the local.

Note

- The archive log file is attached to the organization of the user performing the archive operation. Different users can only view all the authentication log archive information under the user and its subordinate organizations when logging in.

7.6 Authentication Setting

Authentication configuration provides query and setting of access authentication related configurations, including user log configuration, timed offline, built-in user disable rule configuration and user password policy configuration. Click "Terminal Control" - > "Authentication Setting" on the navigation bar at the top of the system to open the "Authentication Setting" interface, as shown in the following figure:



Authentication setting

Log Setting

Save Success Log: Disable
Note: Save success logs
Reserve Time: 3 months

Timed offline

Timed Offline: Disable
Note: After enabling, all users will be offline according to the daily offline time
Daily Offline Time: 23:50:00

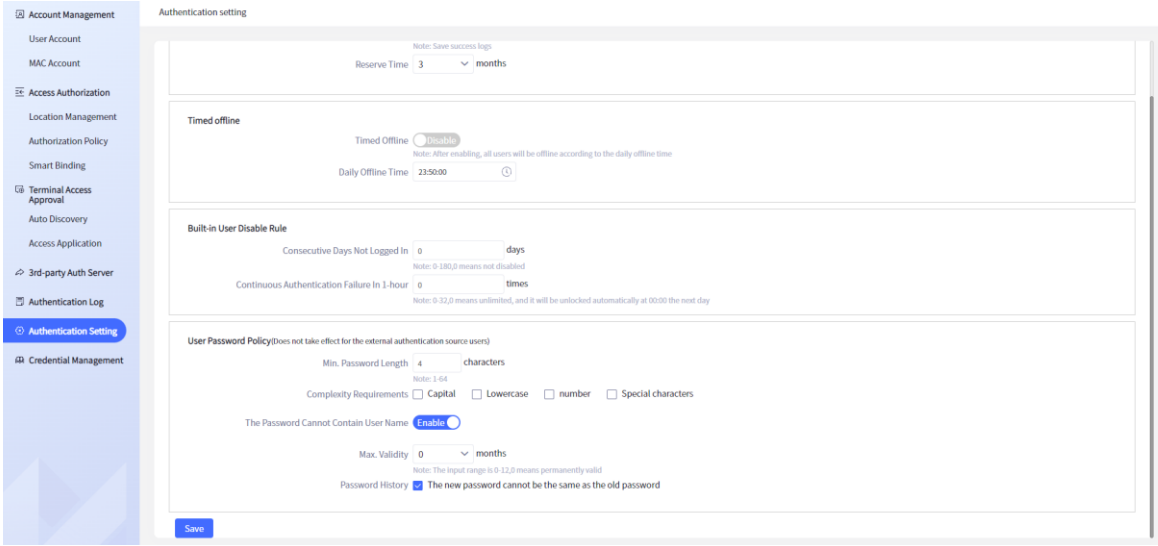
Built-in User Disable Rule

Consecutive Days Not Logged In: 0 days
Note: 0-180,0 means not disabled
Continuous Authentication Failure In 1-hour: 0 times
Note: 0-32,0 means unlimited, and it will be unlocked automatically at 00:00 the next day

User Password Policy(Does not take effect for the external authentication source users)

Min. Password Length: 4 characters
Note: 1-64
Complexity Requirements: ☐ Capital ☐ Lowercase ☐ number ☐ Special characters
The Password Cannot Contain User Name: Enable
Max. Validity: 0 months
Note: The input range is 0-12,0 means permanently valid

Figure 7.6.1 Authentication configuration



Authentication setting

Note: Save success logs
Reserve Time: 3 months

Timed offline

Timed Offline: Disable
Note: After enabling, all users will be offline according to the daily offline time
Daily Offline Time: 23:50:00

Built-in User Disable Rule

Consecutive Days Not Logged In: 0 days
Note: 0-180,0 means not disabled
Continuous Authentication Failure In 1-hour: 0 times
Note: 0-32,0 means unlimited, and it will be unlocked automatically at 00:00 the next day

User Password Policy(Does not take effect for the external authentication source users)

Min. Password Length: 4 characters
Note: 1-64
Complexity Requirements: ☐ Capital ☐ Lowercase ☐ number ☐ Special characters
The Password Cannot Contain User Name: Enable
Max. Validity: 0 months
Note: The input range is 0-12,0 means permanently valid
Password History: ☑ The new password cannot be the same as the old password

Figure 7.6.2 Authentication setting interface

The user log configuration can select whether to save the authentication authorization success log, or set the retention time of the user log archive file.

Timed offline is to customize a certain time period to force online users to offline. Of course, you can choose not to start the timed offline task.

Built-in User Disable Rule can disable the built-in user through two aspects: the number of consecutive non-login days and the number of consecutive authentication failures in one hour.

The user password configuration policy configuration specifies the minimum password length, complexity requirements, whether the password cannot contain the user name, the maximum validity period, and whether the new password cannot be the same as the old password.

Click the button Save to save the authentication configuration information.

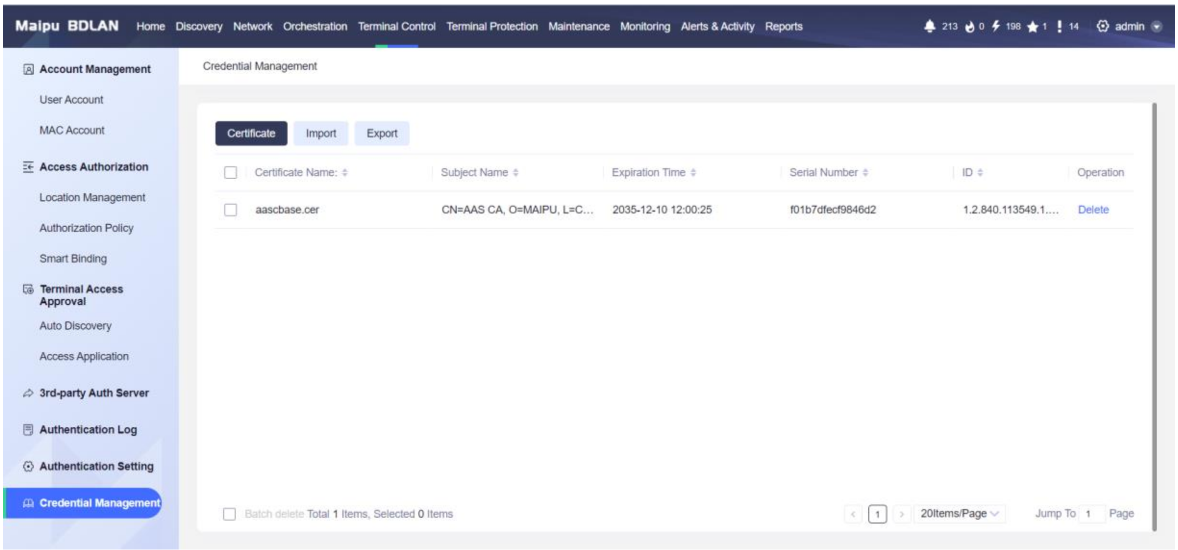
Note

- The input range of consecutive non-login days is 0~180, and 0 means unlimited;
- The input range of 1-hour continuous authentication failure times is 0-32. 0 means no limit. The users limited by continuous authentication failure times will automatically unlock at 00:00 the next day;
- The input range of the longest validity period is 0-12, and 0 represents permanent validity;

7.7 Credential Management

7.7.1 Trust Certificate

Open the **Credential Management** interface to display the trust certificate information in the system in pages by default, showing the certificate name, subject name, expiration time, serial number, ID and operation by columns. Click "Terminal Control" - > "Credential Management" on the navigation bar at the top of the system to open the "Credential Management" interface, as shown in the following figure:

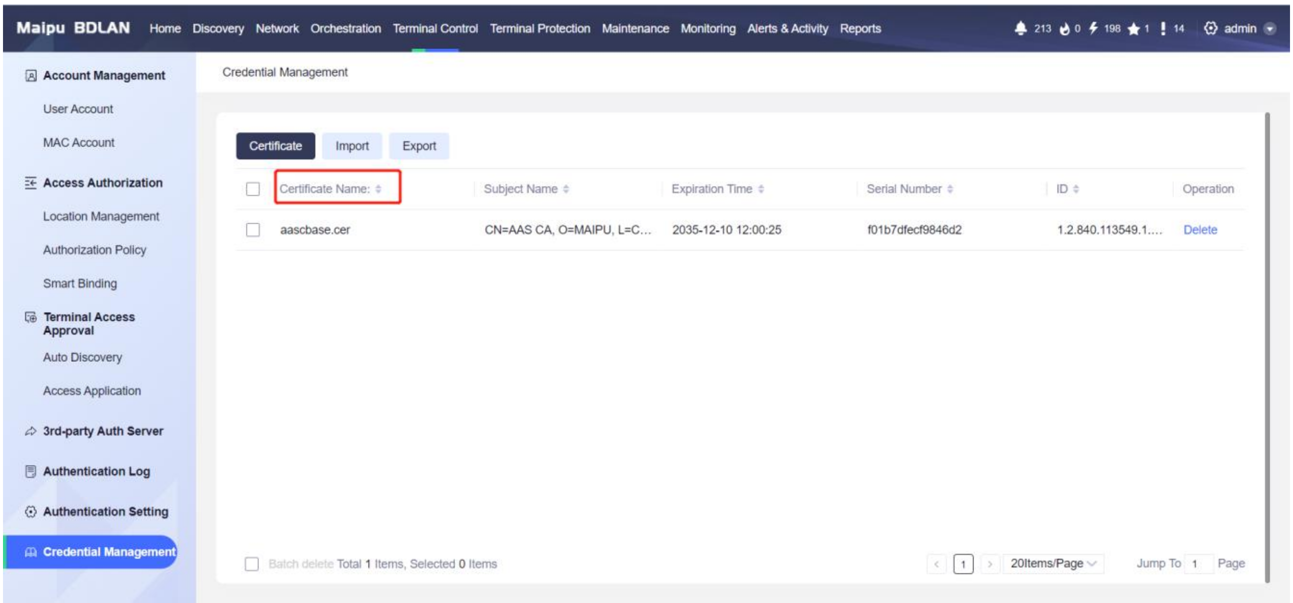


☐	Certificate Name:	Subject Name	Expiration Time	Serial Number	ID	Operation
☐	aascbase.cer	CN=AAS CA, O=MAIPU, L=C...	2035-12-10 12:00:25	f01b7dfecf9846d2	1.2.840.113549.1....	Delete

Total 1 Items, Selected 0 Items

Figure 7.7.1.1 Trust certificate query

Click each field in the head of the certificate list to sort the trust certificate information according to the corresponding field. As shown in the following figure, sort in ascending order by the certificate name:



☐	Certificate Name:	Subject Name	Expiration Time	Serial Number	ID	Operation
☐	aascbase.cer	CN=AAS CA, O=MAIPU, L=C...	2035-12-10 12:00:25	f01b7dfecf9846d2	1.2.840.113549.1....	Delete

Figure 7.7.1.2 Sort in ascending order by certificate name

Click the button Import above the certificate management list to open the "Import" pop-up window, select a file and enter the certificate name, as shown in the following figure:

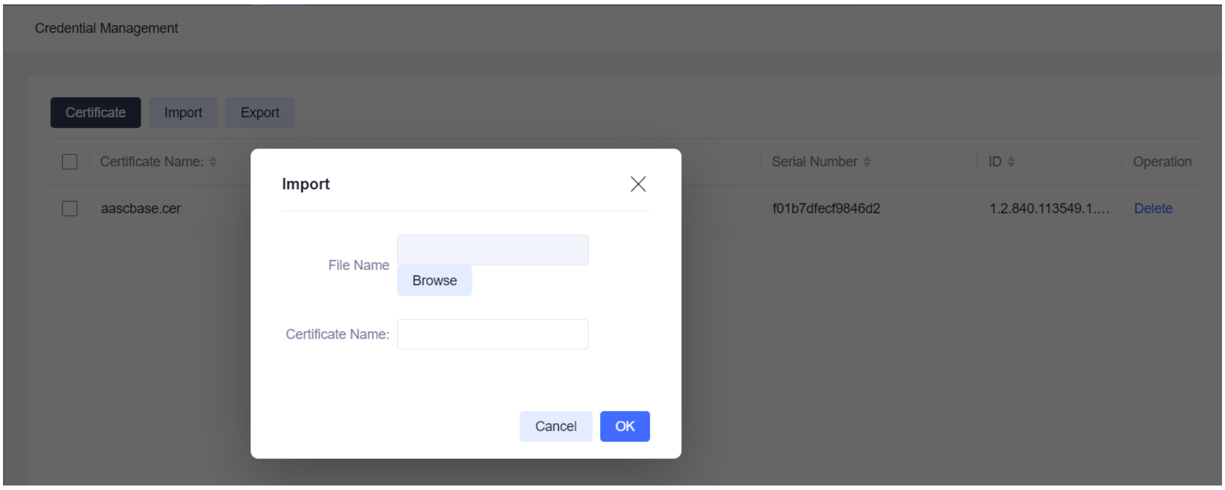
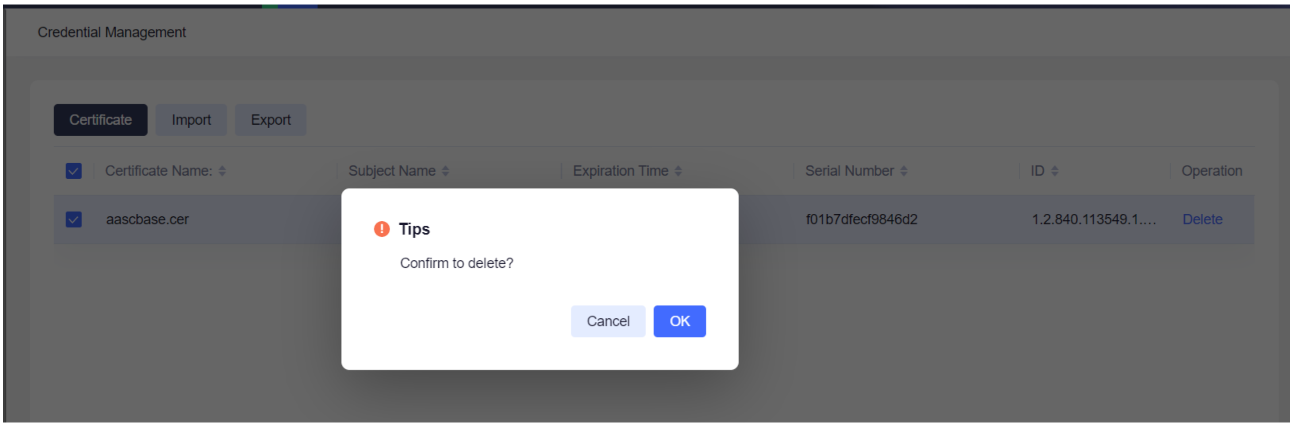


Figure 7.7.1.3 Import the trust certificate

Check a desired trust certificate in the certificate management list, and click the button Export at the top left of the trust certificate list to export the trust certificate.

The deletion of trust certificates can be divided into batch delete and delete one by one:

Batch delete: check the desired trust certificate information in the trust certificate list, click the button Batch delete below, and a pop-up window will appear to confirm the deletion, as shown in the following figure:



☑	Certificate Name:	Subject Name	Expiration Time	Serial Number	ID	Operation
☑	aascbase.cer			f01b7dfecf9846d2	1.2.840.113549.1....	Delete

Tips

Confirm to delete?

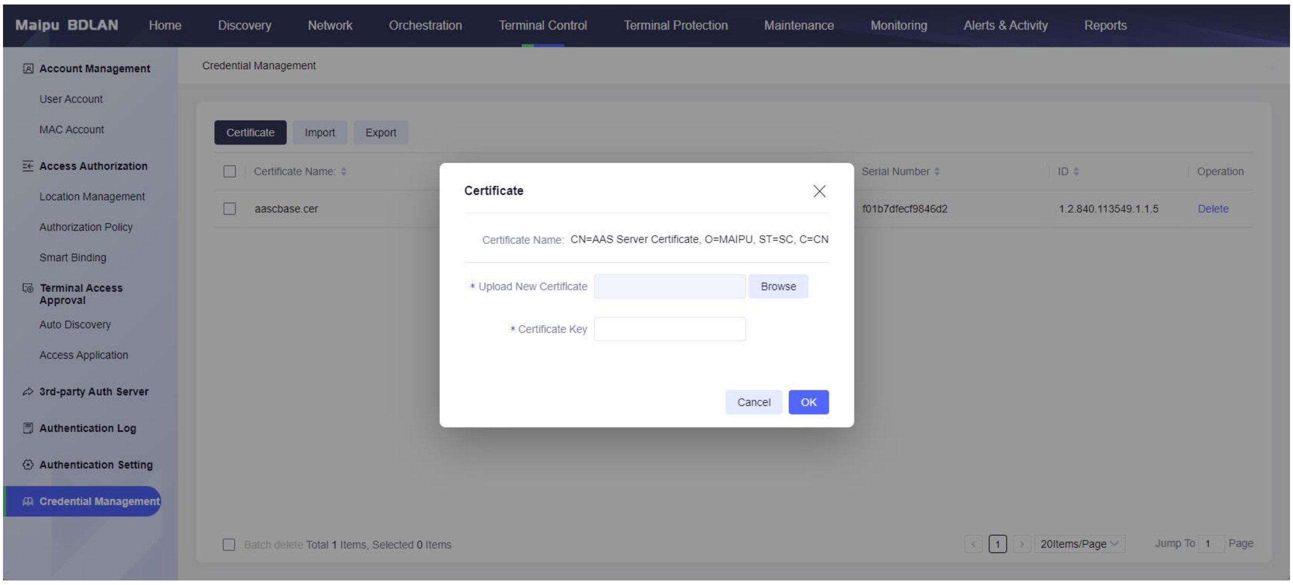
Figure 7.7.1.4 Confirm deletion

Click OK to delete the selected trust certificates in batches.

Delete one by one: click the button Delete behind the trust certificate list and confirm in the delete confirmation pop-up window to delete the trust certificate one by one.

7.7.2 Server Certificate

Click the button Certificate at the top right of the trust certificate list to open the server certificate pop-up window to view the server certificate name, as follows:



☐	Certificate Name:	Serial Number	ID	Operation
☐	aascbase.cer	f01b7dfecf9846d2	1.2.840.113549.1.1.5	Delete

Certificate

Certificate Name: CN=AAS Server Certificate, O=MAIPU, ST=SC, C=CN

* Upload New Certificate

* Certificate Key

☐ Batch delete Total 1 Items, Selected 0 Items

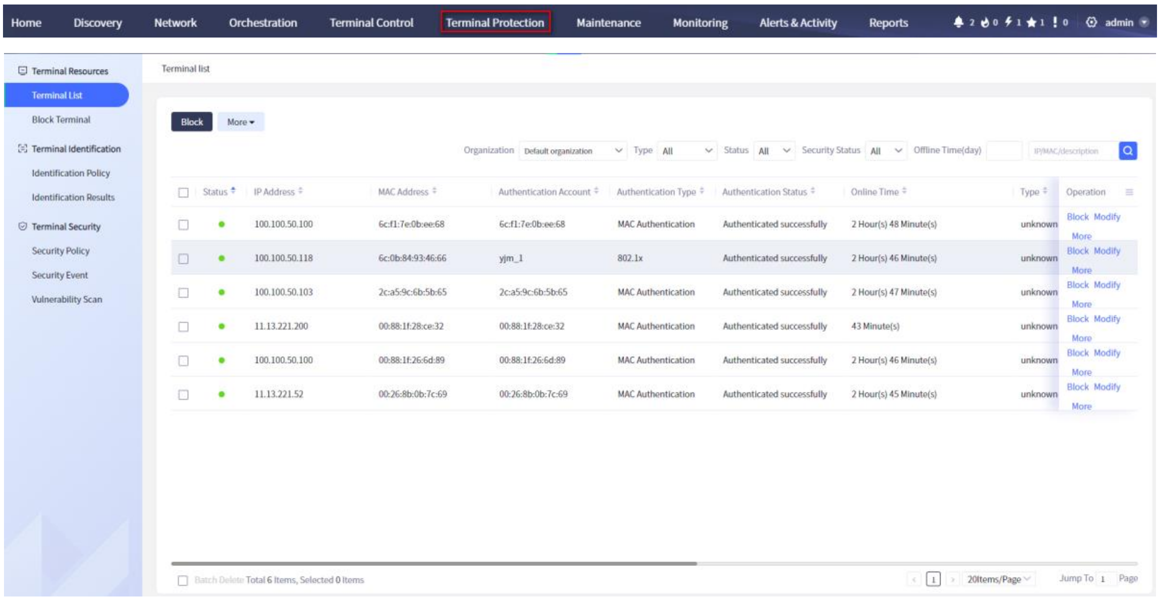
Figure 7.7.2.1 Server certificate window

Click the button Browse to select the new server certificate to be imported and enter the certificate key to import the new server certificate information.

8 Terminal Protection

8.1 Terminal Resources

Click the menu **Terminal Protection** > **Terminal Resources** at the top of the system to enter the terminal resources. Terminal resources include terminal lists and blocking terminals, which are mainly used to display and process the terminal information.



Organization: Default organization | Type: All | Status: All | Security Status: All | Offline Time(day):

☐	Status	IP Address	MAC Address	Authentication Account	Authentication Type	Authentication Status	Online Time	Type	Operation
☐	●	100.100.50.100	6c:f1:7e:0b:ee:68	6c:f1:7e:0b:ee:68	MAC Authentication	Authenticated successfully	2 Hour(s) 48 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.118	6c:0b:84:93:46:66	yjm_1	802.1x	Authenticated successfully	2 Hour(s) 46 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.103	2c:a5:9c:6b:5b:65	2c:a5:9c:6b:5b:65	MAC Authentication	Authenticated successfully	2 Hour(s) 47 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.200	00:88:1f:28:ce:32	00:88:1f:28:ce:32	MAC Authentication	Authenticated successfully	43 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.100	00:88:1f:26:6d:89	00:88:1f:26:6d:89	MAC Authentication	Authenticated successfully	2 Hour(s) 46 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.52	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	MAC Authentication	Authenticated successfully	2 Hour(s) 45 Minute(s)	unknown	Block Modify More

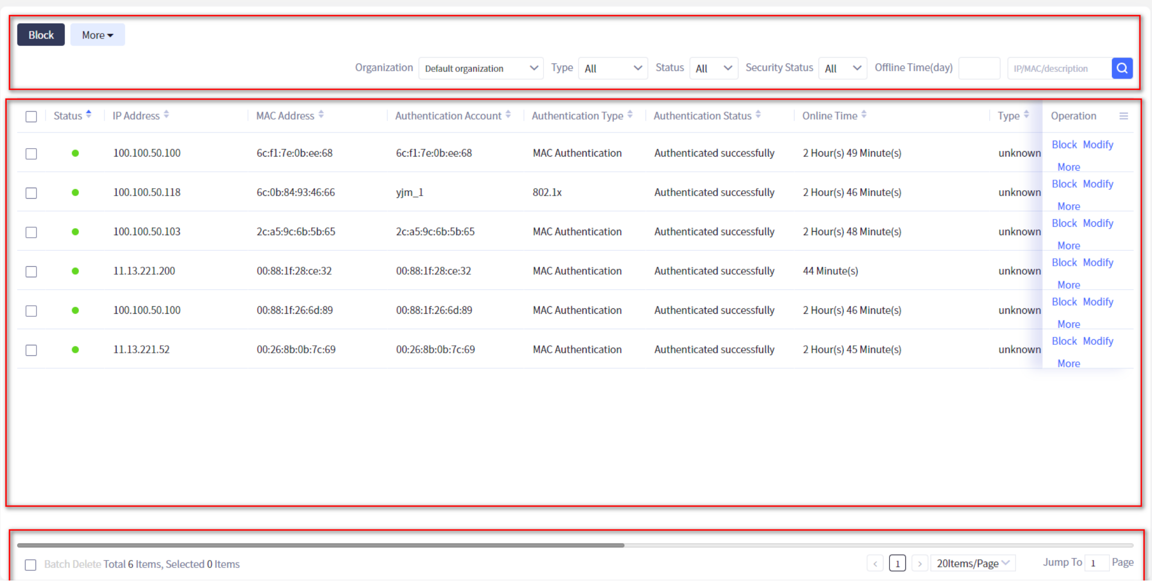
☐ Batch Delete Total 6 Items, Selected 0 Items

< 1 > 20Items/Page Jump To 1 Page

Figure 8.1.1 Terminal management

8.1.1 Terminal List

The terminal list is mainly divided into three areas: the upper part is the main functional area, the middle part is the information display area, and the lower part is the basic functional area.



Organization: Default organization | Type: All | Status: All | Security Status: All | Offline Time(day):

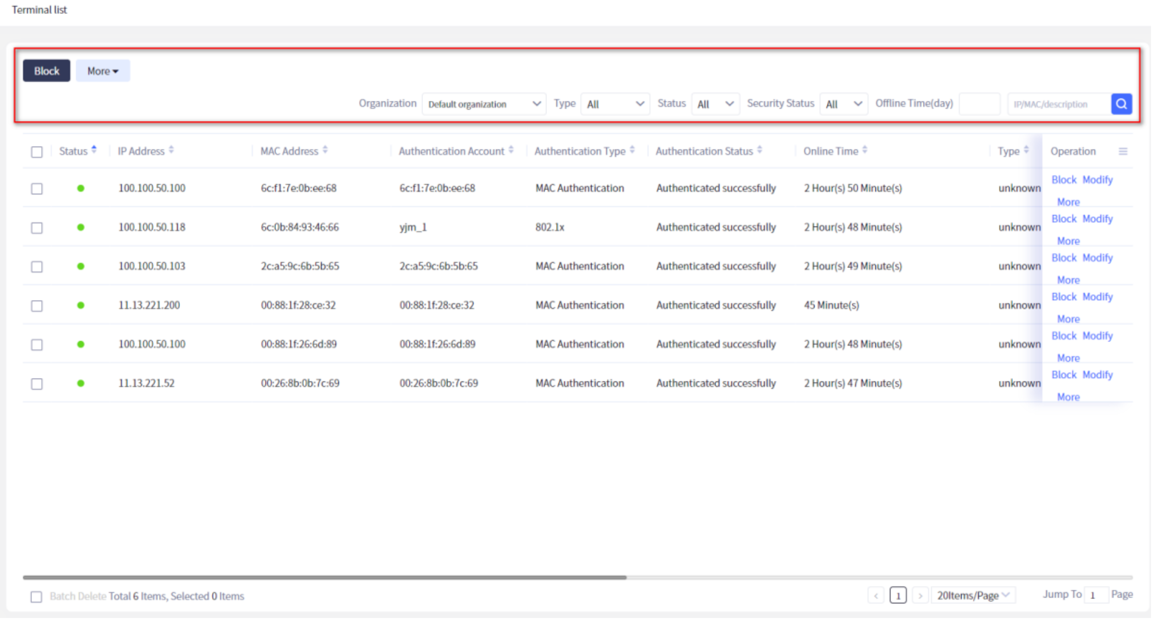
☐	Status	IP Address	MAC Address	Authentication Account	Authentication Type	Authentication Status	Online Time	Type	Operation
☐	●	100.100.50.100	6c:f1:7e:0b:ee:68	6c:f1:7e:0b:ee:68	MAC Authentication	Authenticated successfully	2 Hour(s) 49 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.118	6c:0b:84:93:46:66	yjm_1	802.1x	Authenticated successfully	2 Hour(s) 46 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.103	2c:a5:9c:6b:5b:65	2c:a5:9c:6b:5b:65	MAC Authentication	Authenticated successfully	2 Hour(s) 48 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.200	00:88:1f:28:ce:32	00:88:1f:28:ce:32	MAC Authentication	Authenticated successfully	44 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.100	00:88:1f:26:6d:89	00:88:1f:26:6d:89	MAC Authentication	Authenticated successfully	2 Hour(s) 46 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.52	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	MAC Authentication	Authenticated successfully	2 Hour(s) 45 Minute(s)	unknown	Block Modify More

☐ Batch Delete Total 6 Items, Selected 0 Items

< 1 > 20Items/Page Jump To 1 Page

Figure 8.1.1.1 Terminal list

The upper function area provides the function of blocking the terminal, more (including offline, auto discovery, discovery details, export, idle terminal alarm settings, type management), and querying according to the organization, type, status, security status, offline days and fuzzy fields.



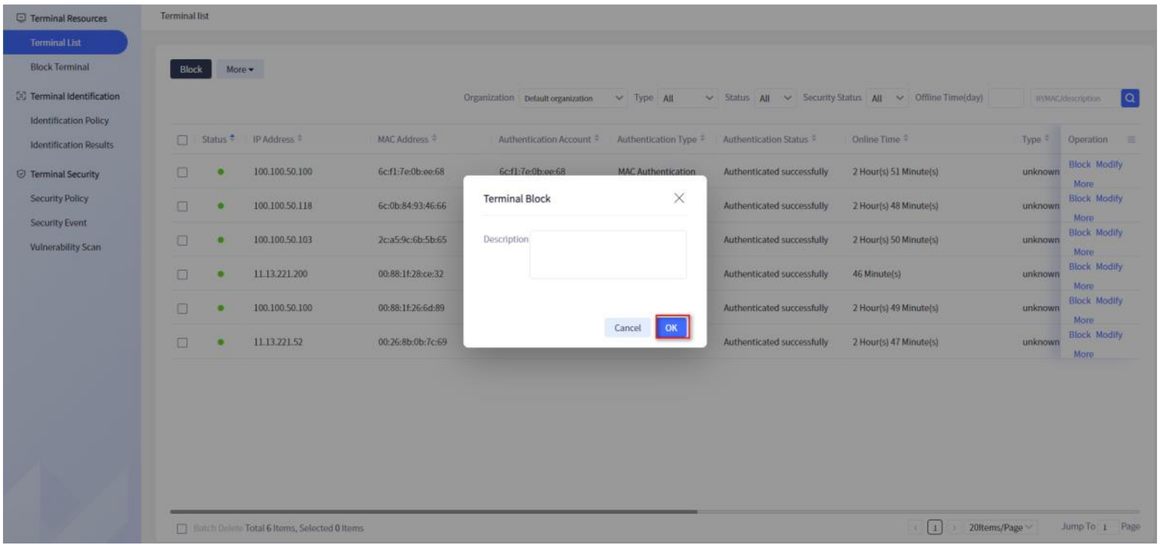
Organization: Default organization Type: All Status: All Security Status: All Offline Time(day): IP/MAC/description

☐	Status	IP Address	MAC Address	Authentication Account	Authentication Type	Authentication Status	Online Time	Type	Operation
☐	●	100.100.50.100	6c:f1:7e:0b:ee:68	6c:f1:7e:0b:ee:68	MAC Authentication	Authenticated successfully	2 Hour(s) 50 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.118	6c:0b:84:93:46:66	yjm_1	802.1x	Authenticated successfully	2 Hour(s) 48 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.103	2c:a5:9c:6b:5b:65	2c:a5:9c:6b:5b:65	MAC Authentication	Authenticated successfully	2 Hour(s) 49 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.200	00:88:1f:28:ce:32	00:88:1f:28:ce:32	MAC Authentication	Authenticated successfully	45 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.100	00:88:1f:26:6d:89	00:88:1f:26:6d:89	MAC Authentication	Authenticated successfully	2 Hour(s) 48 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.52	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	MAC Authentication	Authenticated successfully	2 Hour(s) 47 Minute(s)	unknown	Block Modify More

☐ Batch Delete Total 6 Items, Selected 0 Items

Figure 8.1.1.2 The upper function area

- Block: Select the terminal and click the **Block** button. After adding the description and confirming the block, the terminal can be blocked. The terminal will be removed from the terminal list and added to the block terminal.



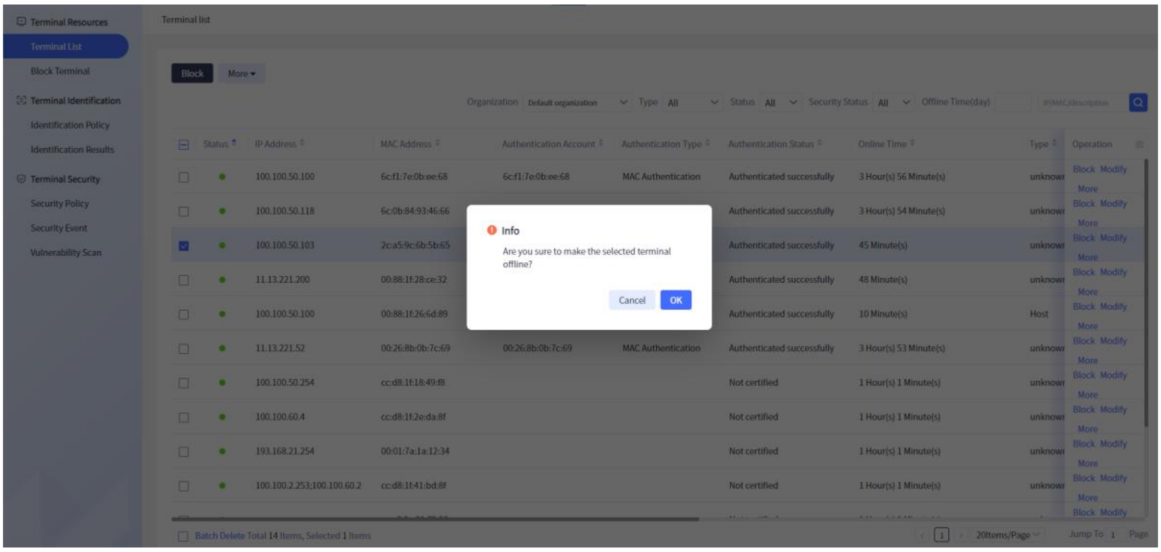
Organization: Default organization Type: All Status: All Security Status: All Offline Time(day): IP/MAC/description

☐	Status	IP Address	MAC Address	Authentication Account	Authentication Type	Authentication Status	Online Time	Type	Operation
☐	●	100.100.50.100	6c:f1:7e:0b:ee:68	6c:f1:7e:0b:ee:68	MAC Authentication	Authenticated successfully	2 Hour(s) 51 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.118	6c:0b:84:93:46:66			Authenticated successfully	2 Hour(s) 48 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.103	2c:a5:9c:6b:5b:65			Authenticated successfully	2 Hour(s) 50 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.200	00:88:1f:28:ce:32			Authenticated successfully	46 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.100	00:88:1f:26:6d:89			Authenticated successfully	2 Hour(s) 49 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.52	00:26:8b:0b:7c:69			Authenticated successfully	2 Hour(s) 47 Minute(s)	unknown	Block Modify More

☐ Batch Delete Total 6 Items, Selected 0 Items

Figure 8.1.1.3 Block terminal

- Offline: Click **More**, select a desired terminal and click **Offline**. After confirming the offline terminal, the terminal can be offline, and the online status of the terminal will change from online to offline.

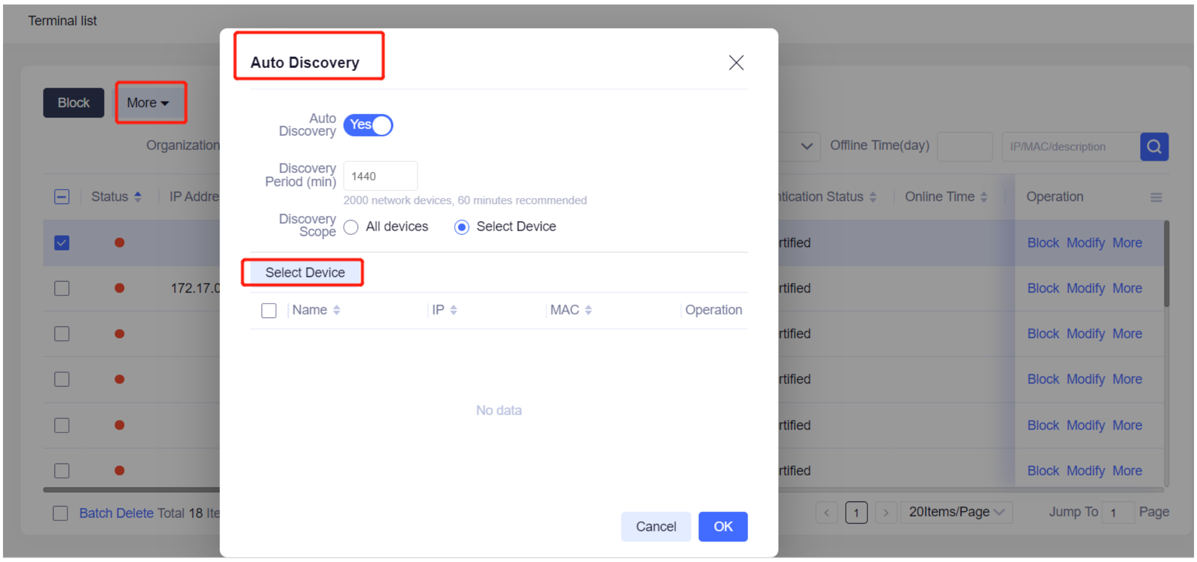


Info

Are you sure to make the selected terminal offline?

Figure 8.1.1.4 Offline terminal

- Auto discovery: click **More** and select **Auto Discovery** to open the setting window. The switch, discovery cycle and discovery range of the auto discovery terminal can be set. The switch of auto discovery terminal will automatically discover the terminal only after it is enabled. Discovery cycle sets the time interval for auto terminal discovery. The system will perform terminal discovery according to the time cycle set by the user. All devices or some devices can be selected for the discovery range. If selecting **All Devices**, perform terminal discovery for all devices by default. If selecting **Select Device**, limit the devices to discover terminals according to user needs.



Auto Discovery

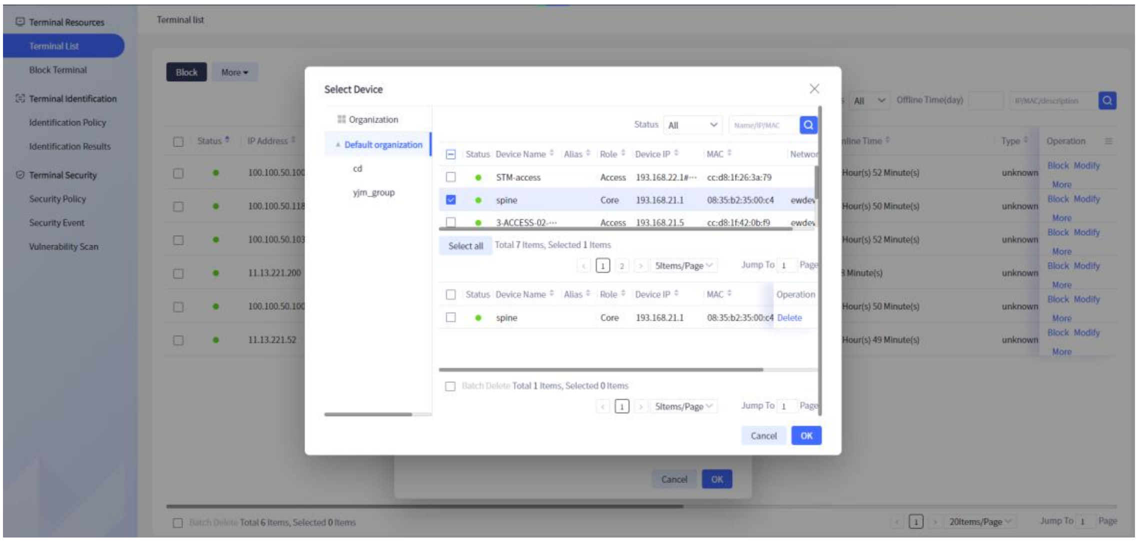
Auto Discovery: Yes

Discovery Period (min): 1440

2000 network devices, 60 minutes recommended

Discovery Scope: ○ All devices ● Select Device

Figure 8.1.1.5 Auto discovery terminal



☐	Status	Device Name	Alias	Role	Device IP	MAC	Networ
☐	●	STM-access		Access	193.168.22.1#···	cc:d8:1f:26:3a:79	
☑	●	spine		Core	193.168.21.1	08:35:b2:35:00:c4	ewdev
☐	●	3-ACCESS-02-···		Access	193.168.21.5	cc:d8:1f:42:0b:f9	ewdev

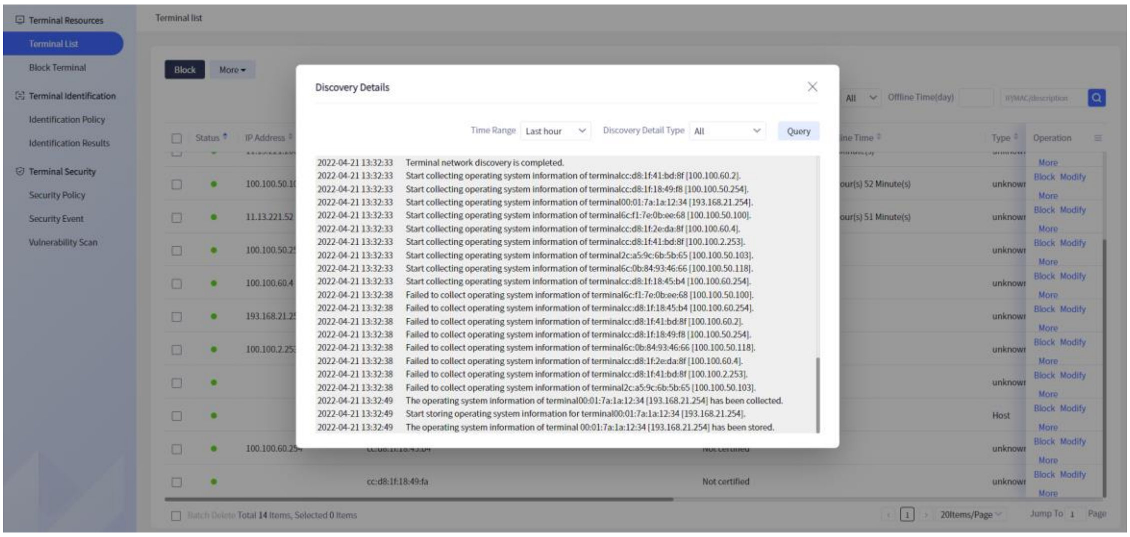
Total 7 Items, Selected 1 Items

☐	Status	Device Name	Alias	Role	Device IP	MAC	Operation
☐	●	spine		Core	193.168.21.1	08:35:b2:35:00:c4	Delete

Total 1 Items, Selected 0 Items

Figure 8.1.1.6 Select devices for auto discovery

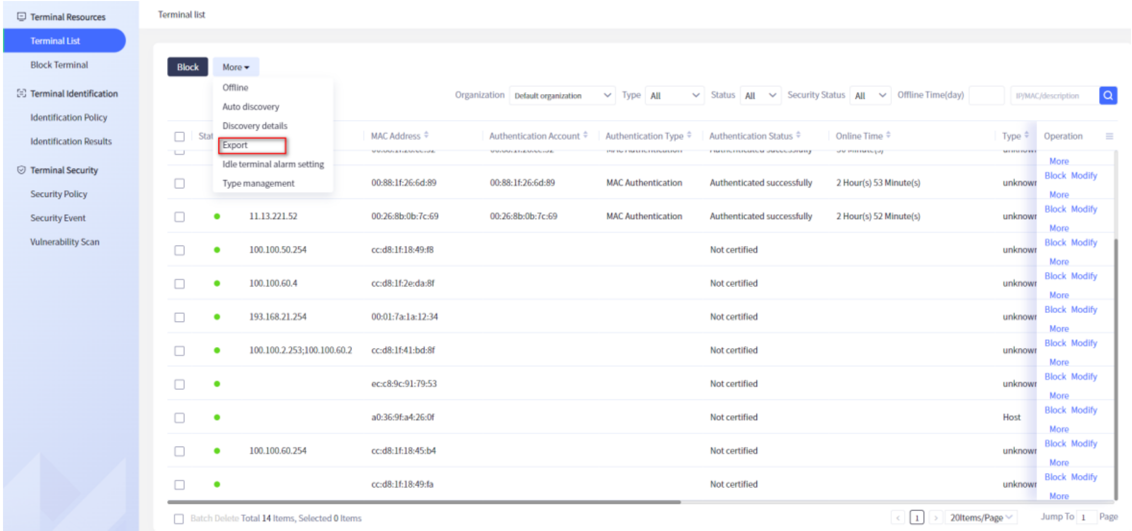
- Discovery details: Click **More** > **Discovery Details** to view the discovery process and details by time or discovery details type.



```
2022-04-21 13:32:33    Terminal network discovery is completed.
2022-04-21 13:32:33    Start collecting operating system information of terminalcc:d8:1f:41:bd:8f [100.100.60.2].
2022-04-21 13:32:33    Start collecting operating system information of terminalcc:d8:1f:18:49:f8 [100.100.50.254].
2022-04-21 13:32:33    Start collecting operating system information of terminal00:01:7a:1a:12:34 [193.168.21.254].
2022-04-21 13:32:33    Start collecting operating system information of terminal6c:f1:7e:0b:ee:68 [100.100.50.100].
2022-04-21 13:32:33    Start collecting operating system information of terminalcc:d8:1f:2e:da:8f [100.100.60.4].
2022-04-21 13:32:33    Start collecting operating system information of terminalcc:d8:1f:41:bd:8f [100.100.2.253].
2022-04-21 13:32:33    Start collecting operating system information of terminal2c:a5:9c:6b:5b:65 [100.100.50.103].
2022-04-21 13:32:33    Start collecting operating system information of terminal6c:0b:84:93:46:66 [100.100.50.118].
2022-04-21 13:32:33    Start collecting operating system information of terminalcc:d8:1f:18:45:b4 [100.100.60.254].
2022-04-21 13:32:38    Failed to collect operating system information of terminal6c:f1:7e:0b:ee:68 [100.100.50.100].
2022-04-21 13:32:38    Failed to collect operating system information of terminalcc:d8:1f:18:45:b4 [100.100.60.254].
2022-04-21 13:32:38    Failed to collect operating system information of terminalcc:d8:1f:41:bd:8f [100.100.60.2].
2022-04-21 13:32:38    Failed to collect operating system information of terminalcc:d8:1f:18:49:f8 [100.100.50.254].
2022-04-21 13:32:38    Failed to collect operating system information of terminal6c:0b:84:93:46:66 [100.100.50.118].
2022-04-21 13:32:38    Failed to collect operating system information of terminalcc:d8:1f:2e:da:8f [100.100.60.4].
2022-04-21 13:32:38    Failed to collect operating system information of terminalcc:d8:1f:41:bd:8f [100.100.2.253].
2022-04-21 13:32:38    Failed to collect operating system information of terminal2c:a5:9c:6b:5b:65 [100.100.50.103].
2022-04-21 13:32:49    The operating system information of terminal00:01:7a:1a:12:34 [193.168.21.254] has been collected.
2022-04-21 13:32:49    Start storing operating system information for terminal00:01:7a:1a:12:34 [193.168.21.254].
2022-04-21 13:32:49    The operating system information of terminal 00:01:7a:1a:12:34 [193.168.21.254] has been stored.
```

Figure 8.1.1.7 Discovery details

- Export: Click **More** > **Export**, and you can export the list information. Th format of the exported file is .xlsx.

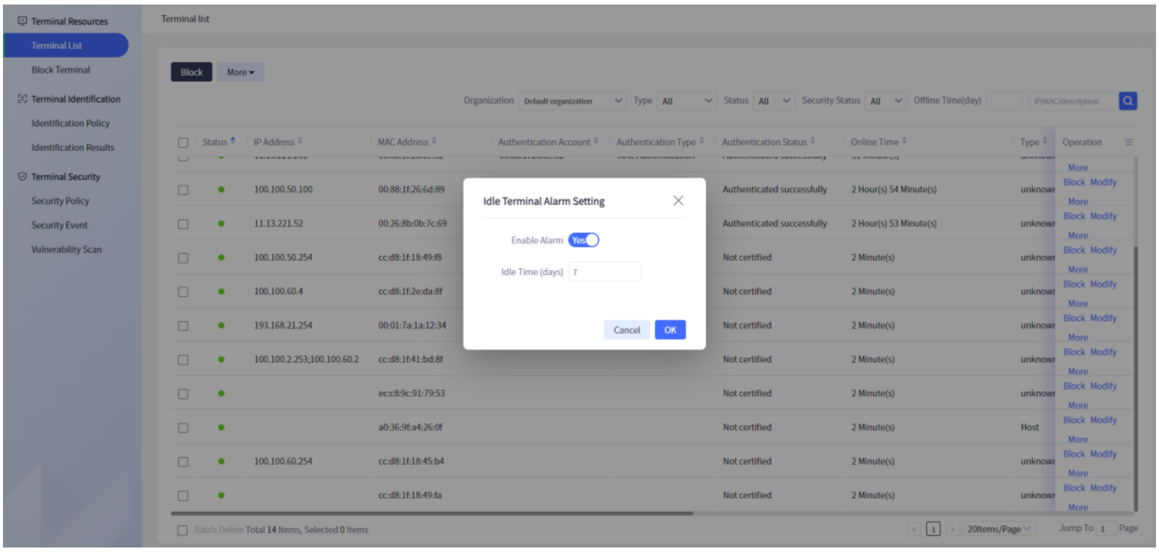


☐	Stat		MAC Address	Authentication Account	Authentication Type	Authentication Status	Online Time	Type	Operation
☐			00:88:1f:26:6d:89	00:88:1f:26:6d:89	MAC Authentication	Authenticated successfully	2 Hour(s) 53 Minute(s)	unknowr	More Block Modify
☐	●	11.13.221.52	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	MAC Authentication	Authenticated successfully	2 Hour(s) 52 Minute(s)	unknowr	More Block Modify
☐	●	100.100.50.254	cc:d8:1f:18:49:f8			Not certified		unknowr	More Block Modify
☐	●	100.100.60.4	cc:d8:1f:2e:da:8f			Not certified		unknowr	More Block Modify
☐	●	193.168.21.254	00:01:7a:1a:12:34			Not certified		unknowr	More Block Modify
☐	●	100.100.2.253;100.100.60.2	cc:d8:1f:41:bd:8f			Not certified		unknowr	More Block Modify
☐	●		ec:c8:9c:91:79:53			Not certified		unknowr	More Block Modify
☐	●		a0:36:9f:a4:26:0f			Not certified		Host	More Block Modify
☐	●	100.100.60.254	cc:d8:1f:18:45:b4			Not certified		unknowr	More Block Modify
☐	●		cc:d8:1f:18:49:fa			Not certified		unknowr	More Block Modify

Total 14 Items, Selected 0 Items

Figure 8.1.1.8 Export

- Idle terminal alarm settings: click **More** > **Idle terminal alarm setting** to configure the alarm switch and idle time. The terminal will generate an alarm only after the alarm switch is turned on. The idle time is used to enable the alarm, and when the offline time of the terminal reaches the idle time, generate the alarm.



Organization: Default organization; Type: All; Status: All; Security Status: All; Offline Time(day)

Idle Terminal Alarm Setting

Enable Alarm: Yes

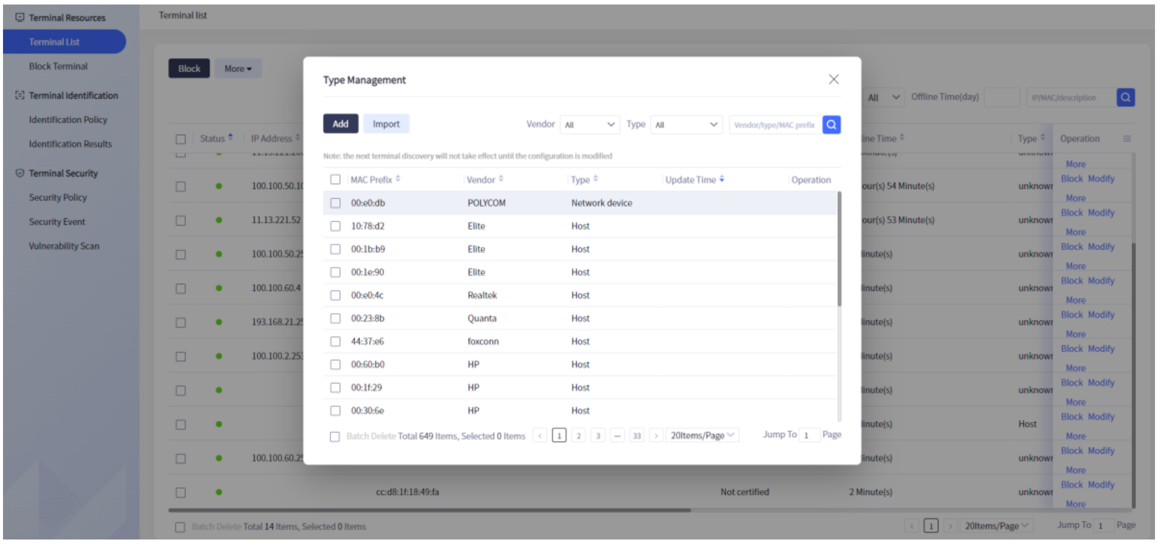
Idle Time (days): 7

☐	Status	IP Address	MAC Address	Authentication Account	Authentication Type	Authentication Status	Online Time	Type	Operation
☐	●	100.100.50.100	00:88:1f:26:6d:89			Authenticated successfully	2 Hour(s) 54 Minute(s)	unknow	Block Modify More
☐	●	11.13.221.52	00:26:8b:0b:7c:69			Authenticated successfully	2 Hour(s) 53 Minute(s)	unknow	Block Modify More
☐	●	100.100.50.254	cc:d8:1f:18:49:f8			Not certified	2 Minute(s)	unknow	Block Modify More
☐	●	100.100.60.4	cc:d8:1f:2e:da:8f			Not certified	2 Minute(s)	unknow	Block Modify More
☐	●	193.168.21.254	00:01:7a:1a:12:34			Not certified	2 Minute(s)	unknow	Block Modify More
☐	●	100.100.2.253;100.100.60.2	cc:d8:1f:41:bd:8f			Not certified	2 Minute(s)	unknow	Block Modify More
☐	●		ec:c8:9c:91:79:53			Not certified	2 Minute(s)	unknow	Block Modify More
☐	●		a0:36:9f:a4:26:0f			Not certified	2 Minute(s)	Host	Block Modify More
☐	●	100.100.60.254	cc:d8:1f:18:45:b4			Not certified	2 Minute(s)	unknow	Block Modify More
☐	●		cc:d8:1f:18:49:fa			Not certified	2 Minute(s)	unknow	Block Modify More

Total 14 Items, Selected 0 Items; Jump To 1 Page

Figure 8.1.1.9 Idle terminal alarm setting

- Type management: click **More** > **Type Management** to perform type management on the terminal. Type management includes the functions of adding, importing, searching, displaying type information, and deleting in batches.



Type Management

Vendor: All; Type: All; Vendor/type/MAC prefix

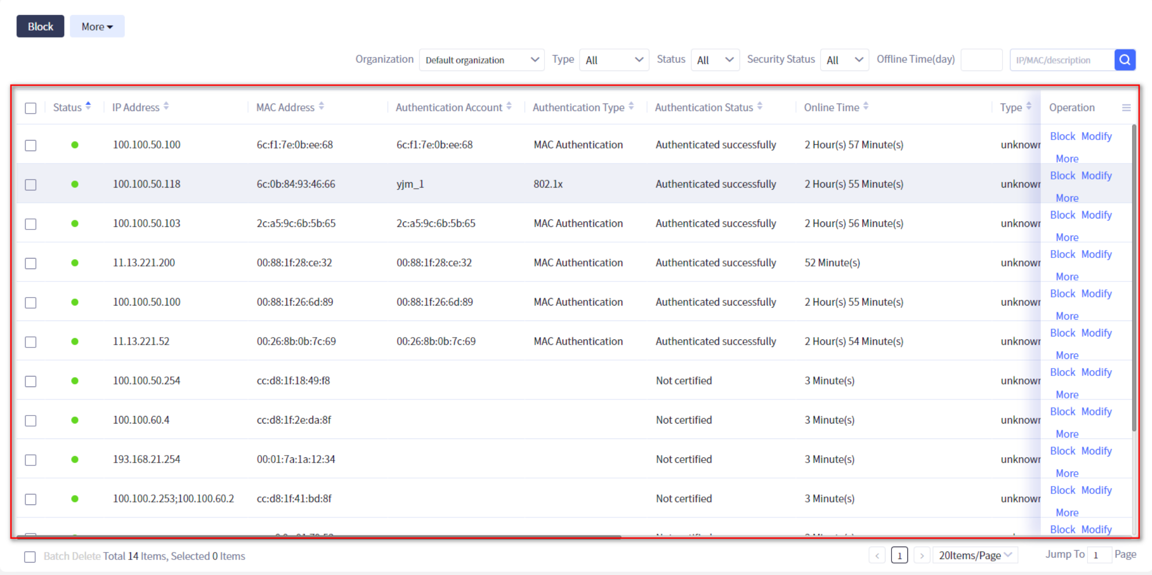
Note: the next terminal discovery will not take effect until the configuration is modified

☐	MAC Prefix	Vendor	Type	Update Time	Operation
☐	00:e0:db	POLYCOM	Network device		
☐	10:78:d2	Elite	Host		
☐	00:1b:b9	Elite	Host		
☐	00:1e:90	Elite	Host		
☐	00:e0:4c	Realtek	Host		
☐	00:23:8b	Quanta	Host		
☐	44:37:e6	foxconn	Host		
☐	00:60:b0	HP	Host		
☐	00:1f:29	HP	Host		
☐	00:30:6e	HP	Host		

Total 649 Items, Selected 0 Items; 1 2 3 … 33; Jump To 1 Page

Figure 8.1.1.10 Type management

The middle area is the display area of terminal information, including terminal online status, IP address, MAC address, authentication account, authentication type, authentication status, online duration, type, manufacturer, security status, organization, access device, access port, user grouping, latest online time and description information. It also provides operations such as blocking, modifying, and more (offline, deletion, and baseline) of a single terminal.

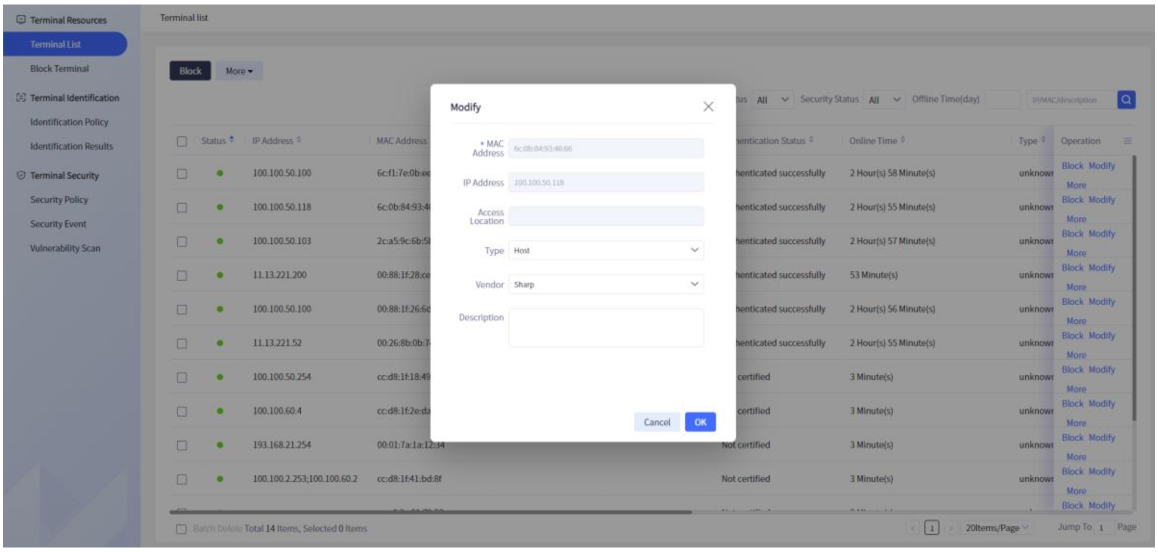


☐	Status	IP Address	MAC Address	Authentication Account	Authentication Type	Authentication Status	Online Time	Type	Operation
☐	●	100.100.50.100	6c:f1:7e:0b:ee:68	6c:f1:7e:0b:ee:68	MAC Authentication	Authenticated successfully	2 Hour(s) 57 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.118	6c:0b:84:93:46:66	yjm_1	802.1x	Authenticated successfully	2 Hour(s) 55 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.103	2c:a5:9c:6b:5b:65	2c:a5:9c:6b:5b:65	MAC Authentication	Authenticated successfully	2 Hour(s) 56 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.200	00:88:1f:28:ce:32	00:88:1f:28:ce:32	MAC Authentication	Authenticated successfully	52 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.100	00:88:1f:26:6d:89	00:88:1f:26:6d:89	MAC Authentication	Authenticated successfully	2 Hour(s) 55 Minute(s)	unknown	Block Modify More
☐	●	11.13.221.52	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	MAC Authentication	Authenticated successfully	2 Hour(s) 54 Minute(s)	unknown	Block Modify More
☐	●	100.100.50.254	cc:d8:1f:18:49:f8			Not certified	3 Minute(s)	unknown	Block Modify More
☐	●	100.100.60.4	cc:d8:1f:2e:da:8f			Not certified	3 Minute(s)	unknown	Block Modify More
☐	●	193.168.21.254	00:01:7a:1a:12:34			Not certified	3 Minute(s)	unknown	Block Modify More
☐	●	100.100.2.253;100.100.60.2	cc:d8:1f:41:bd:8f			Not certified	3 Minute(s)	unknown	Block Modify More

☐ Batch Delete Total 14 Items, Selected 0 Items

Figure 8.1.1.11 Middle display area

- Modify: Click **Modify** to modify the type, manufacturer and description of the terminal.



Modify

* MAC Address: 6c:0b:84:93:46:66

IP Address: 100.100.50.118

Access Location:

Type: Host

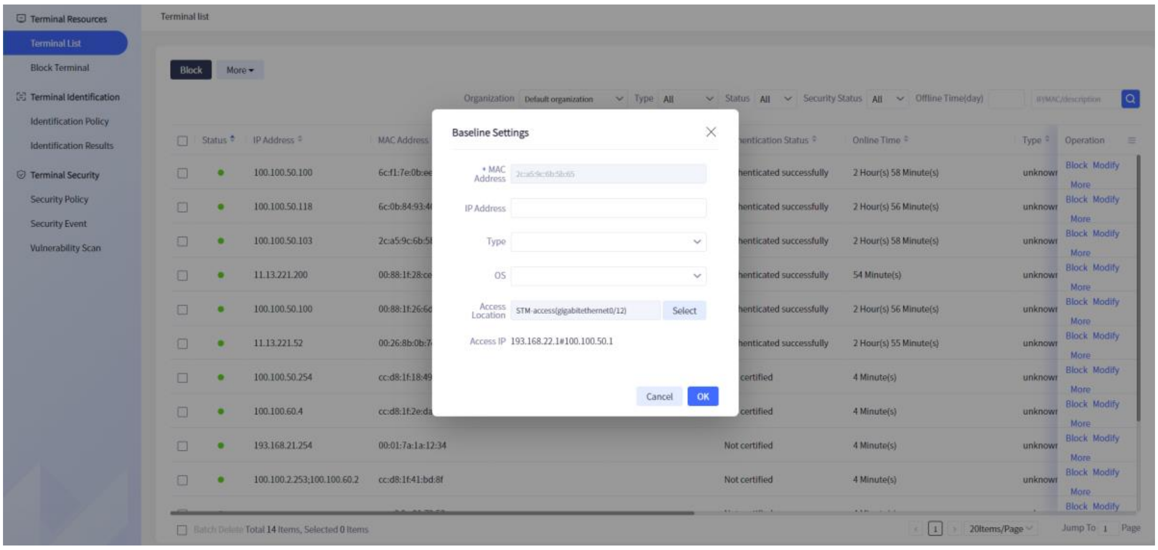
Vendor: Sharp

Description:

Figure 8.1.1.12 Modify the terminal information

- Baseline: click **Baseline** to modify the terminal baseline. The modifiable baseline information includes IP address, type, operating system and access location.

Specific device and interface can be selected for access location



Baseline Settings

* MAC Address: 2c:a5:9c:6b:5b:65

IP Address:

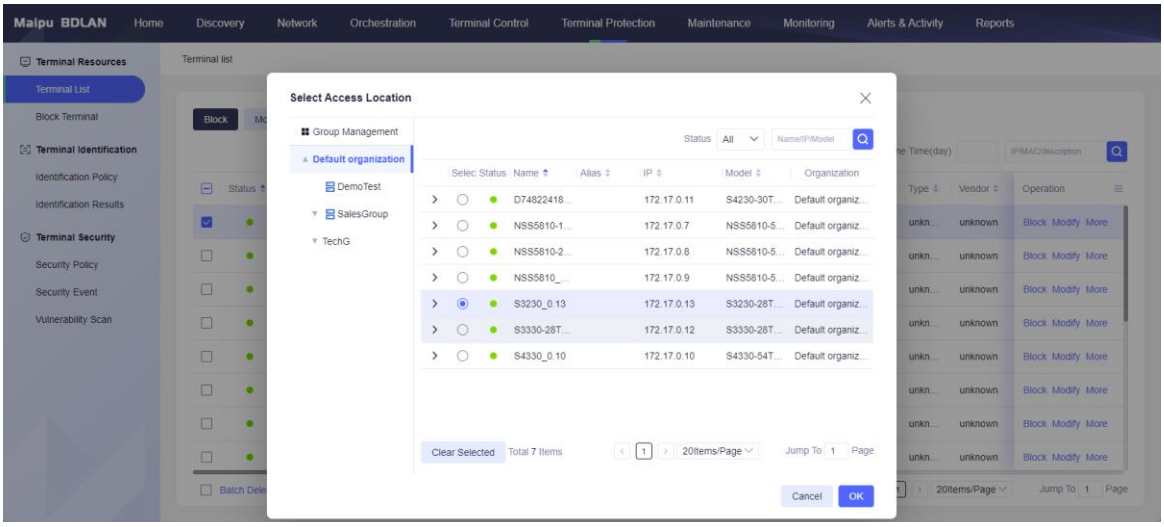
Type:

OS:

Access Location: STM-access(gigabitethernet0/12)

Access IP: 193.168.22.1#100.100.50.1

Figure 8.1.1.13 Baseline settings



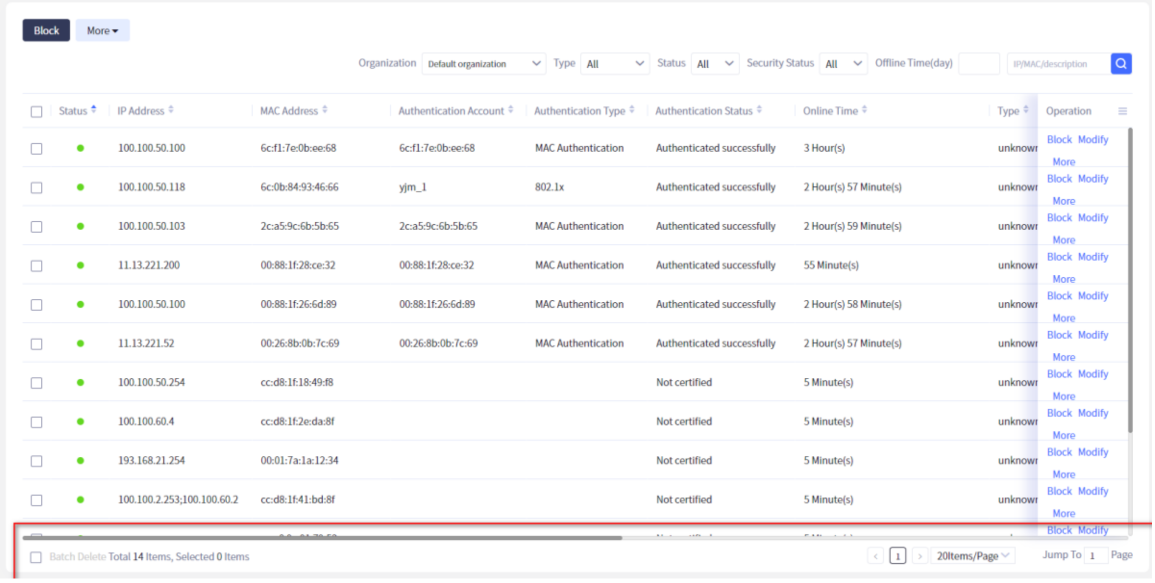
Select Access Location

	Selec	Status	Name	Alias	IP	Model	Organization
›	○	●	D74822418...		172.17.0.11	S4230-30T...	Default organiz...
›	○	●	NSS5810-1...		172.17.0.7	NSS5810-5...	Default organiz...
›	○	●	NSS5810-2...		172.17.0.8	NSS5810-5...	Default organiz...
›	○	●	NSS5810_...		172.17.0.9	NSS5810-5...	Default organiz...
›	●	●	S3230_0.13		172.17.0.13	S3230-28T...	Default organiz...
›	○	●	S3330-28T...		172.17.0.12	S3330-28T...	Default organiz...
›	○	●	S4330_0.10		172.17.0.10	S4330-54T...	Default organiz...

Total 7 Items

Figure 8.1.1.14 Select the access location

The following is the function of deleting terminals in batch and controlling paging information.



☐	Status	IP Address	MAC Address	Authentication Account	Authentication Type	Authentication Status	Online Time	Type	Operation
☐	●	100.100.50.100	6c:f1:7e:0b:ee:68	6c:f1:7e:0b:ee:68	MAC Authentication	Authenticated successfully	3 Hour(s)	unknowr	Block Modify More
☐	●	100.100.50.118	6c:0b:84:93:46:66	yjm_1	802.1x	Authenticated successfully	2 Hour(s) 57 Minute(s)	unknowr	Block Modify More
☐	●	100.100.50.103	2c:a5:9c:6b:5b:65	2c:a5:9c:6b:5b:65	MAC Authentication	Authenticated successfully	2 Hour(s) 59 Minute(s)	unknowr	Block Modify More
☐	●	11.13.221.200	00:88:1f:28:ce:32	00:88:1f:28:ce:32	MAC Authentication	Authenticated successfully	55 Minute(s)	unknowr	Block Modify More
☐	●	100.100.50.100	00:88:1f:26:6d:89	00:88:1f:26:6d:89	MAC Authentication	Authenticated successfully	2 Hour(s) 58 Minute(s)	unknowr	Block Modify More
☐	●	11.13.221.52	00:26:8b:0b:7c:69	00:26:8b:0b:7c:69	MAC Authentication	Authenticated successfully	2 Hour(s) 57 Minute(s)	unknowr	Block Modify More
☐	●	100.100.50.254	cc:d8:1f:18:49:f8			Not certified	5 Minute(s)	unknowr	Block Modify More
☐	●	100.100.60.4	cc:d8:1f:2e:da:8f			Not certified	5 Minute(s)	unknowr	Block Modify More
☐	●	193.168.21.254	00:01:7a:1a:12:34			Not certified	5 Minute(s)	unknowr	Block Modify More
☐	●	100.100.2.253;100.100.60.2	cc:d8:1f:41:bd:8f			Not certified	5 Minute(s)	unknowr	Block Modify More

☐ Batch Delete Total 14 Items, Selected 0 Items

Figure 8.1.1.15 Bottom function area

8.1.2 Block Terminal

The blocking terminal is divided into three areas: the top and bottom parts are functional areas, and the middle part is information display area.

The upper function area is the unblock button and query area.

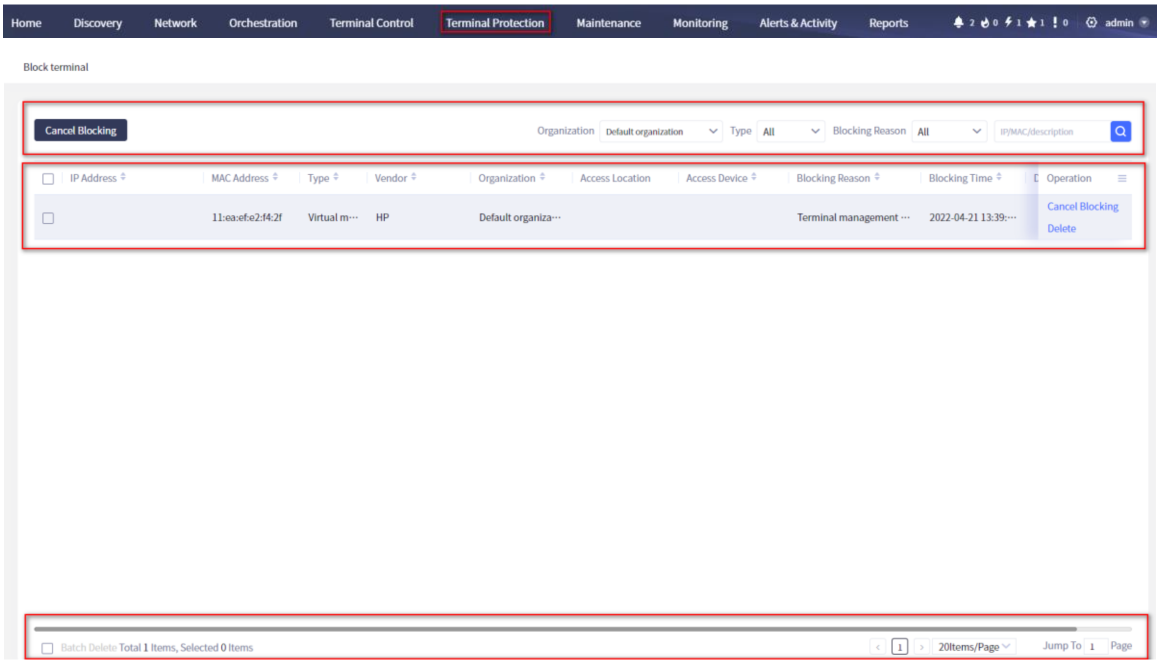
Unblock can remove the terminal from the blocked terminal list.

The search area supports querying by organization, type, blocking reason and fuzzy fields.

In the middle is the display area of the blocked terminal information, which includes IP address, MAC address, type, manufacturer, organization, access location, access device, blocking reason, blocking time, description and operation.

Each terminal message is followed by the unblocking and deletion operations of a single terminal.

The bottom function area provides batch delete terminal operations and paging settings.



Organization: Default organization Type: All Blocking Reason: All

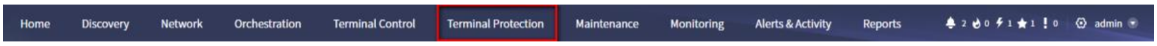
☐	IP Address	MAC Address	Type	Vendor	Organization	Access Location	Access Device	Blocking Reason	Blocking Time	Operation
☐		11:ea:ef:e2:f4:2f	Virtual m···	HP	Default organiza···			Terminal management ···	2022-04-21 13:39:···	Cancel Blocking Delete

☐ Total 1 Items, Selected 0 Items

Figure 8.1.2.1 Block terminal

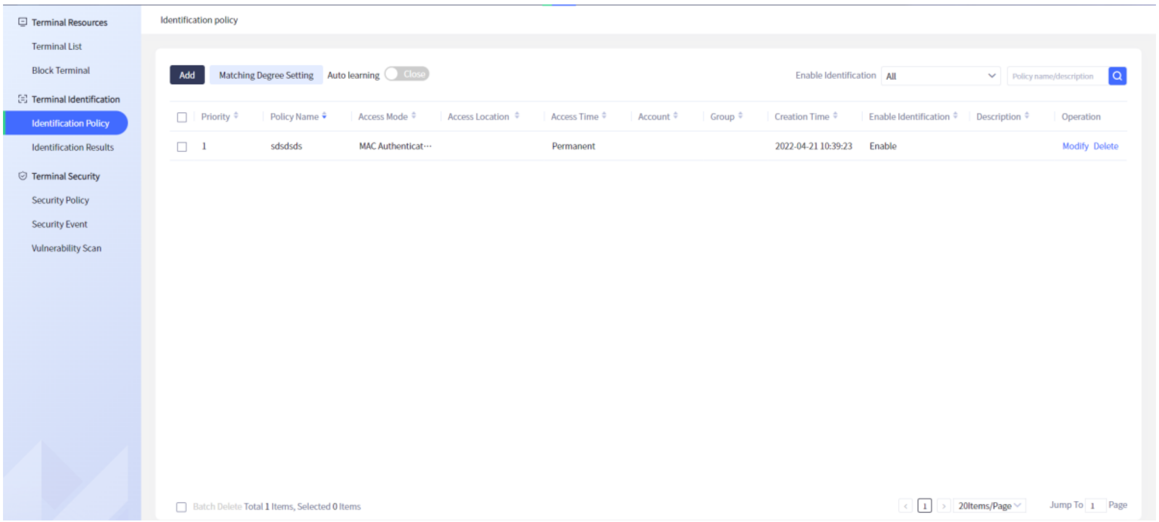
8.2 Terminal Identification

The level-1 menu of the terminal identification is as follows:



8.2.1 Identification Policy

The identification policy interface opens the “Identification policy” interface through the menu "Terminal Protection" > "Identification Policy". The identification policy interface displays all identification policies, and has the functions of adding policies, querying policies according to conditions, modifying policies and deleting policies.

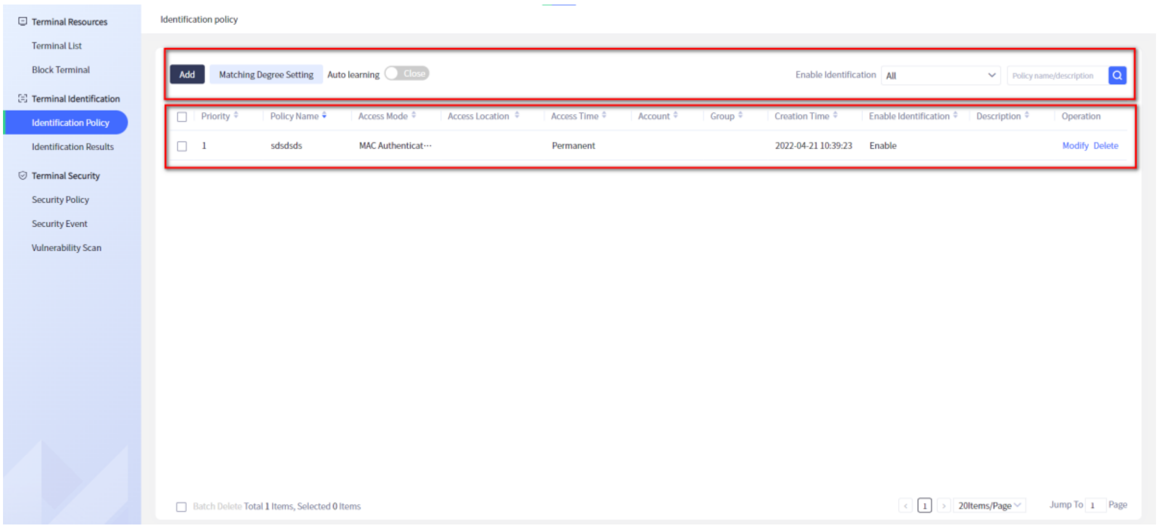


☐	Priority	Policy Name	Access Mode	Access Location	Access Time	Account	Group	Creation Time	Enable Identification	Description	Operation
☐	1	sdsdsds	MAC Authenticat···		Permanent			2022-04-21 10:39:23	Enable		Modify Delete

Figure 8.1.1.1 Identification policy navigation diagram

- Identification policy interface

The identification policy interface is divided into two parts. The top part is the function area, including the Add button, the match degree setting button, the auto learning switch, and the filter according to the identification switch and the query field; The bottom part is the display list of identification policies, including the functions of modifying and deleting a single policy. At the bottom is the batch delete button and the setting items of paging parameters, as shown in figure 8.1.1.2:

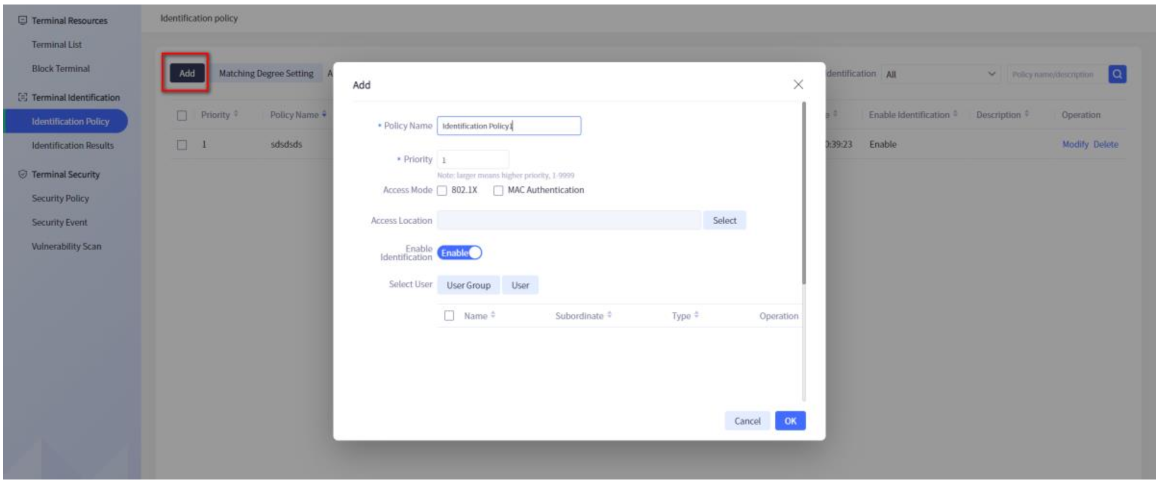


☐	Priority	Policy Name	Access Mode	Access Location	Access Time	Account	Group	Creation Time	Enable Identification	Description	Operation
☐	1	sdsdsds	MAC Authenticat···		Permanent			2022-04-21 10:39:23	Enable		Modify Delete

Figure 8.1.1.2 Identification policy diagram

- Add policies

Add anew identification policy, as follows:



* Policy Name: Identification Policy1

* Priority: 1

Note: larger means higher priority, 1-9999

Enable Identification: Enable

Figure 8.1.1.3 Add a identification policy

Policy name: Name the policy name. The maximum length is 32 characters.

Priority: Configure the priority of the policy. If other conditions are met, the policy with higher priority will be matched first. The digital range of 1-9999 can be configured.

Access method: used to select the access method of the terminal. If it is not selected, this item will not be matched.

Access location: used to select the access location of the terminal online. As shown in the following figure, the pop-up box displays the organization on the left and two lists on the right. Each line of the list displays the access location, access device, access port and description information.

The list in the upper part shows all access positions under the organization. The lower part of the list displays the current selected access location. Click the **Delete** button on the right to delete the selected data. Click **OK** to return to the selected data. Press **Cancel** to cancel the operation of selecting the access location.

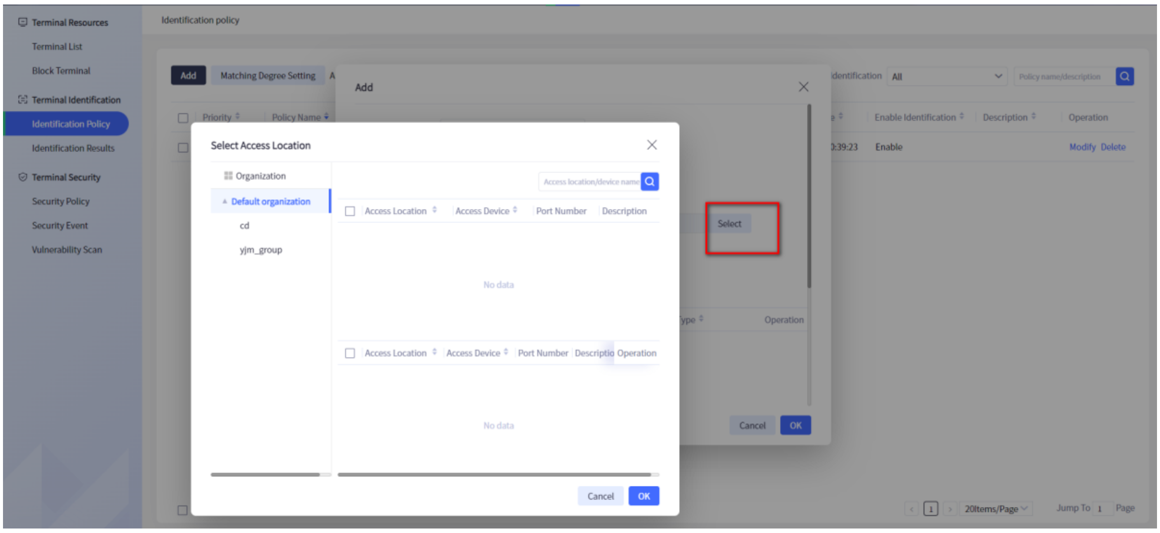
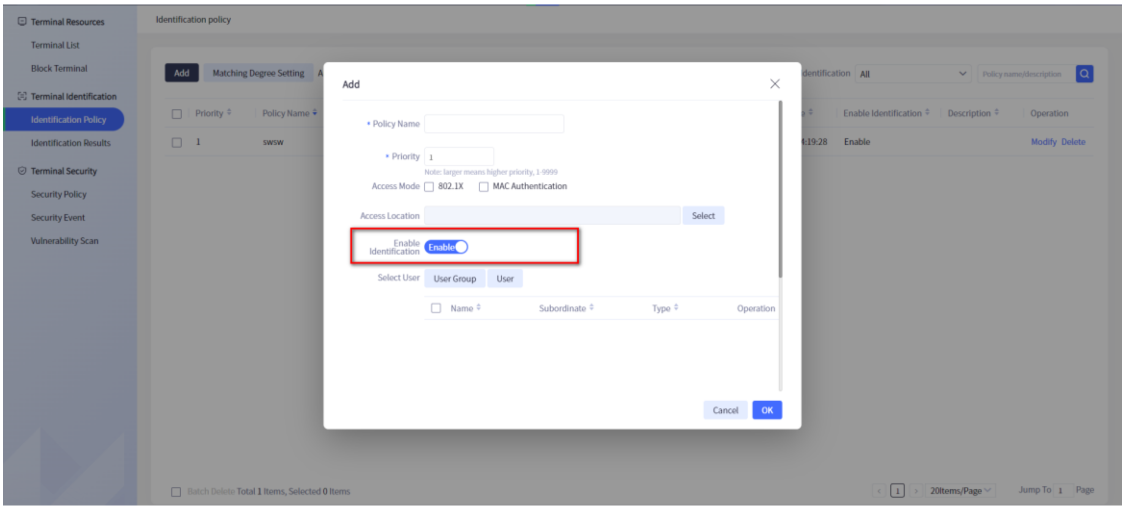


Figure 8.1.1.4 Add access location

Enable identification: You can select Enable/Disable. When enabled, the policy will be matched when the terminal goes online. When disabled, the policy will not be matched, as shown in the following figure:



Select User: You can select the user group and user matching the policy. It is used to select the matching user group or user when the terminal goes online. As shown in the following figure, the user group pop-up box displays the organization on the left and two lists on the right. Each line of the list displays the group name and its organization. The left side of the user pop-up box displays the organization, and the right side displays two lists. Each line of the list displays the user account, name, status, maximum number of online terminals, and the group to which they belong.

The upper part displays the user group or user information under the organization, and the lower part displays the user group or user selected by the user. Click **Delete** to delete the selected data.

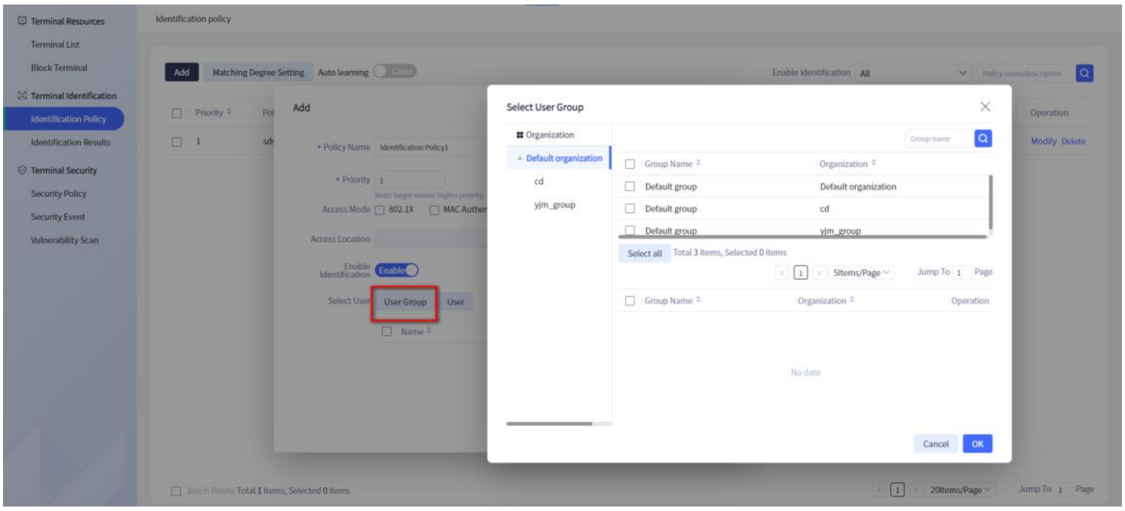


Figure 8.1.1.5 Select the user group

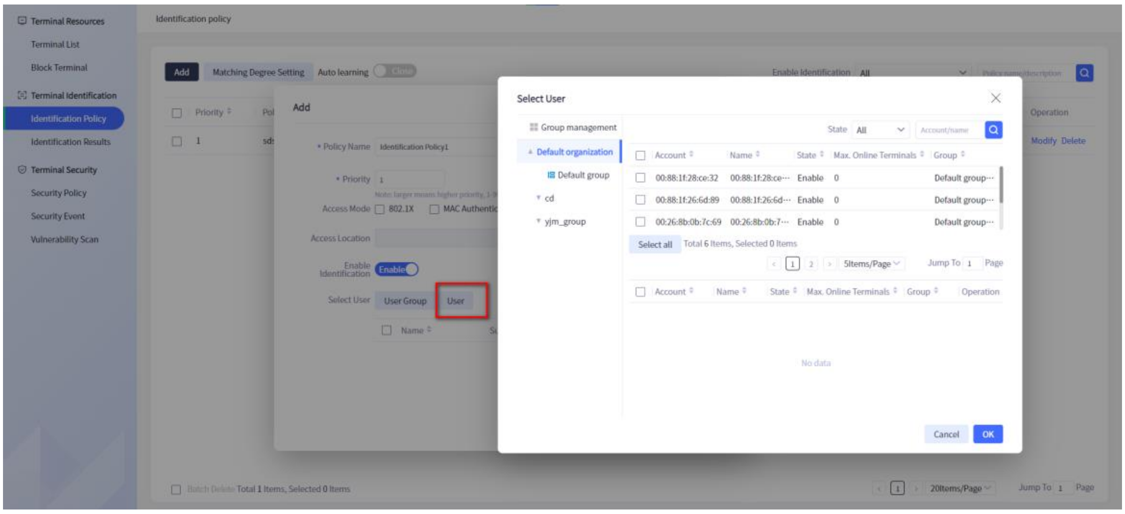
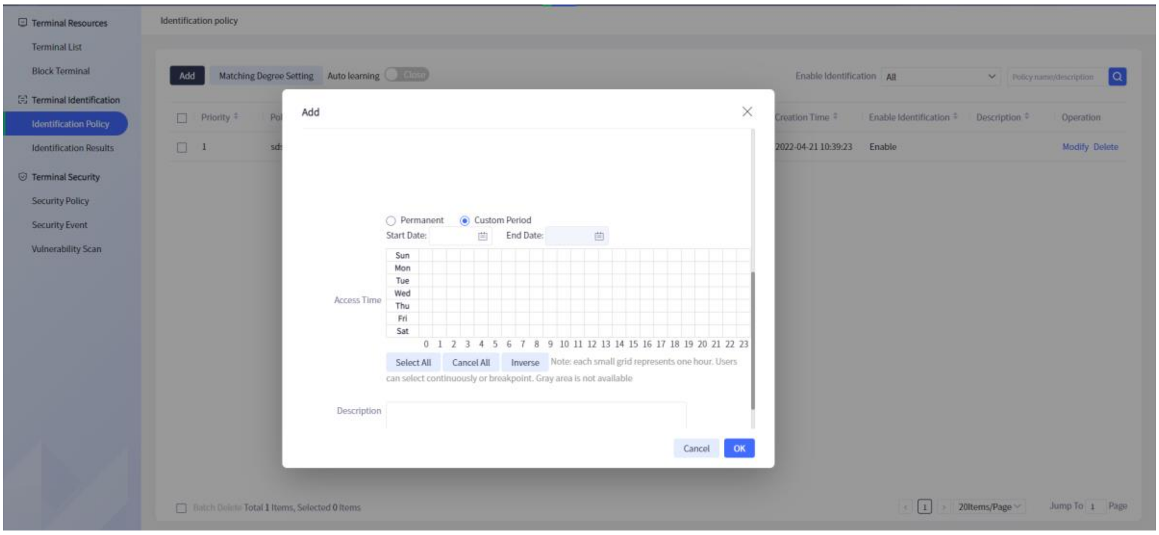


Figure 8.1.1.6 Select the user

Access time: permanent/custom period can be selected. If permanent, the terminal access time is unlimited. If custom period is selected, the terminal that is online in this time period will match this policy. If the terminal is online in the other time period, it will not match this policy. The blue box indicates the time allowed for terminal access. At the same time, **Select all** can be selected/none can be selected/the reverse selection can be performed according to the time selected at this time.



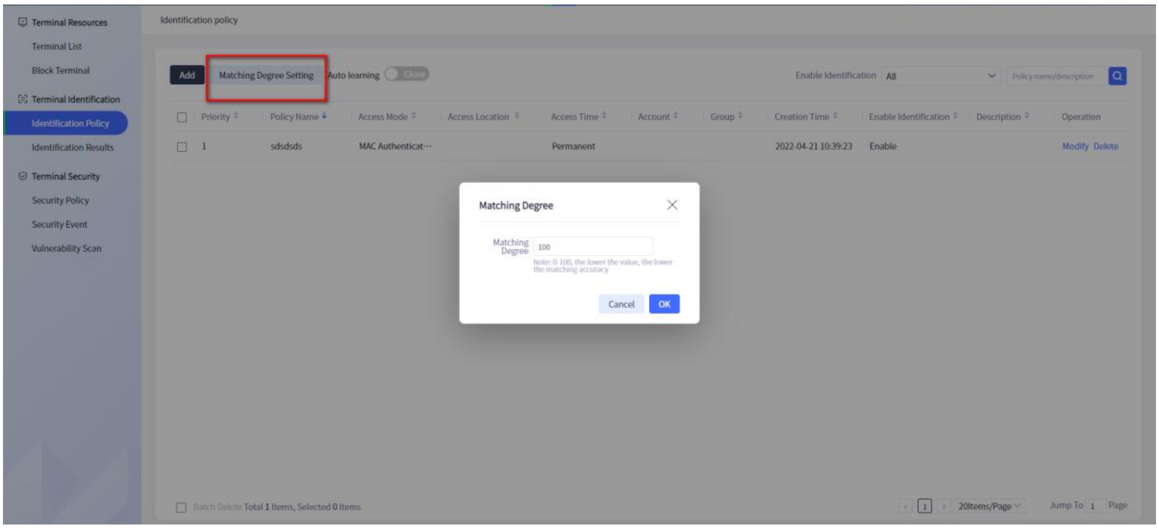
Note: each small grid represents one hour. Users can select continuously or breakpoint. Gray area is not available

Figure 8.1.1.7 Select the access time

Description: The description information of this policy. It cannot exceed 255 characters.

- Matching degree setting

Set the global matching degree. After setting the matching degree, as long as the terminal feature matching rate is greater than this value, it will be considered as successful matching, that is, successful recognition. The matching degree setting is shown in the following figure:



Enable Identification: All

Priority	Policy Name	Access Mode	Access Location	Access Time	Account	Group	Creation Time	Enable Identification	Description	Operation
1	sdsdsds	MAC Authenticat···		Permanent			2022-04-21 10:39:23	Enable		Modify Delete

Matching Degree

Matching Degree: 100

Note: 0-100, the lower the value, the lower the matching accuracy

Total 1 Items, Selected 0 Items

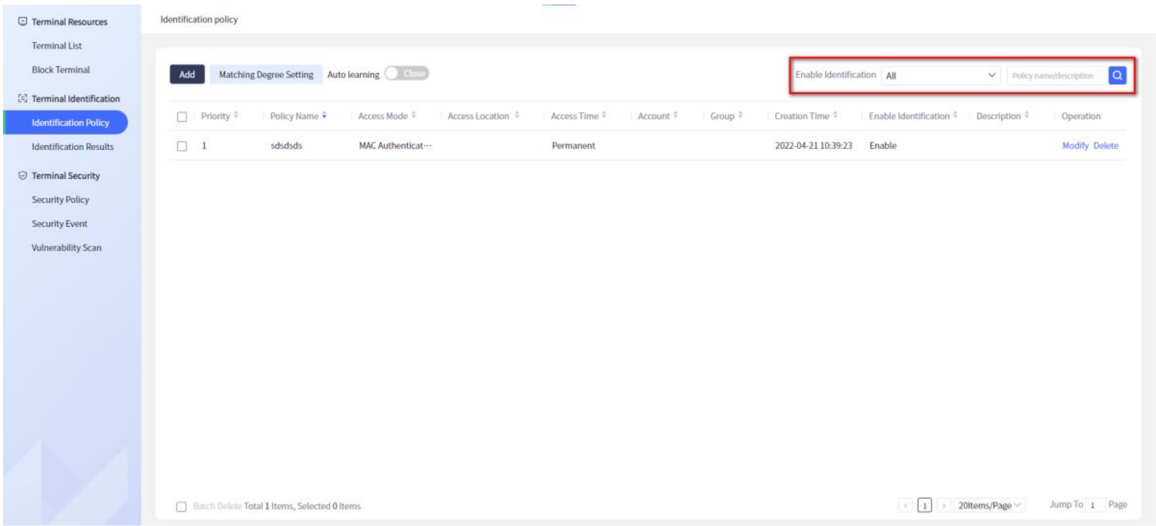
Figure 8.1.1.8 Matching degree setting

- Auto learning switch

  It is used to enable/disable the auto learning function. When this function is enabled, no security event will be generated. The system will automatically learn the characteristics of the terminals that are successfully scanned but not successfully identified (i.e., not matched), and automatically upgrade the terminal fingerprints that are successfully learned to the terminal fingerprint library. When the auto learning function is disabled, the unmatched terminal features will not be automatically learned.

- Query policy

  As shown in the following figure, the upper right of the interface is the query area, which can be queried according to the enabling status of the policy, and fuzzy query fields are supported.



Enable Identification: All

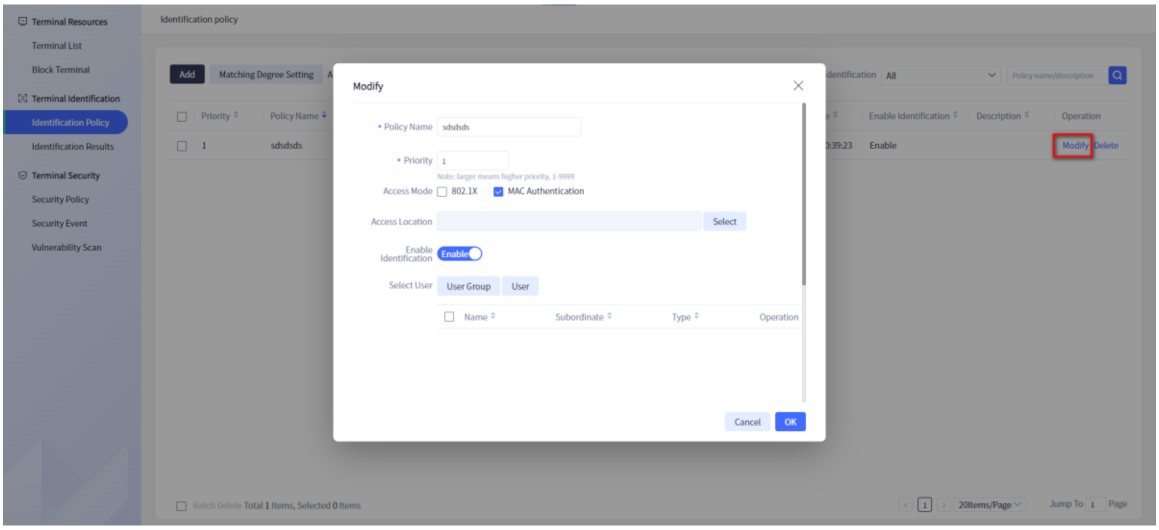
Priority	Policy Name	Access Mode	Access Location	Access Time	Account	Group	Creation Time	Enable Identification	Description	Operation
1	sdsdsds	MAC Authenticat···		Permanent			2022-04-21 10:39:23	Enable		Modify Delete

Total 1 Items, Selected 0 Items

Figure 8.1.1.9 Query identification policy

- Edit policy

  You can edit the identification policy, and modify the policy name, priority, access method, access position, identification switch, access time and description information.



Modify

* Policy Name: sdsdsds

* Priority: 1

Note: larger means higher priority, 1-9999

Access Mode: ☐ 802.1X ☑ MAC Authentication

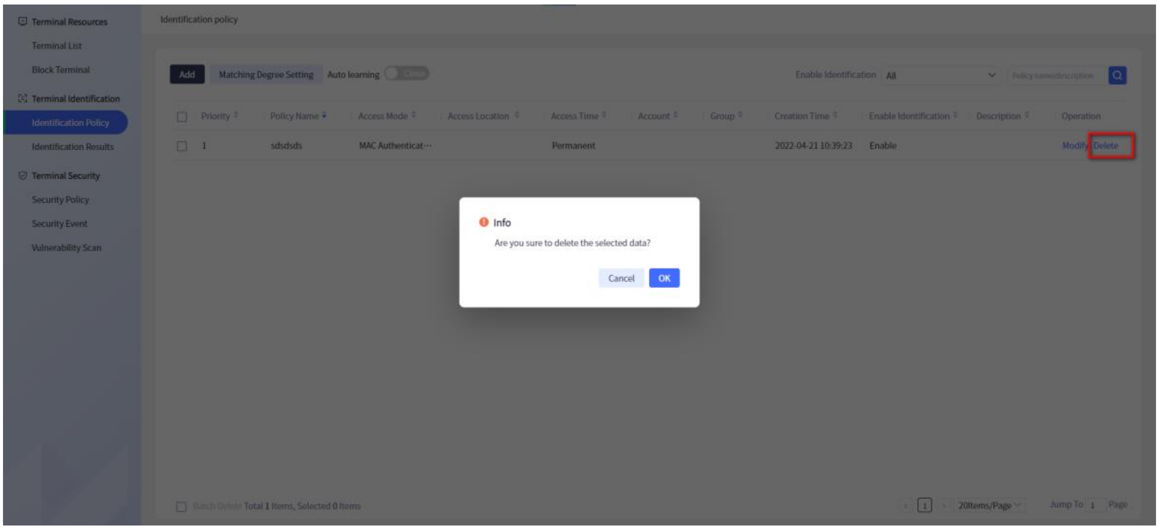
Access Location:

Enable Identification: Enable

Figure 8.1.1.10 Edit the identification policy

- Delete the policy

As shown in the following figure, you can delete a single policy and batch delete policies.



Priority	Policy Name	Access Mode	Access Location	Access Time	Account	Group	Creation Time	Enable Identification	Description	Operation
1	sdsdsds	MAC Authenticat···		Permanent			2022-04-21 10:39:23	Enable		Modify Delete

Info

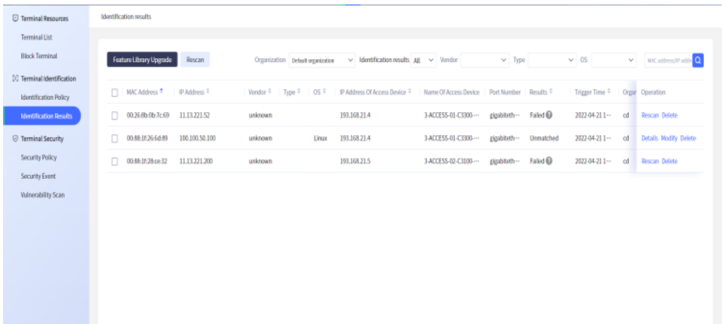
Are you sure to delete the selected data?

Cancel OK

Figure 8.1.1.11 Delete the identification policy

8.2.2 Identification Results

Open the identification result interface by clicking the menu "Terminal Protection" > "Identification Result". The identification result interface is used to display all terminal identification results, and can perform functions, such as feature library upgrade, rescan, edit, and delete.

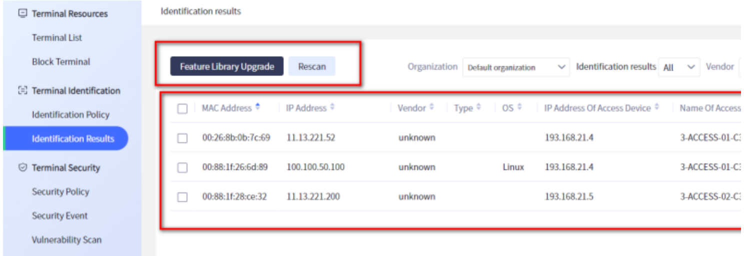


MAC Address	IP Address	Vendor	Type	OS	IP Address Of Access Device	Name Of Access Device	Port Number	Results	Trigger Time	Orga	Operation
00:26:8b:0b:7c:69	11.13.221.52	unknown			193.168.21.4	3-ACCESS-01-C3300-···	gigabiteth···	Failed	2022-04-21 1···	cd	Rescan Delete
00:88:1f:26:6d:89	100.100.50.100	unknown		Linux	193.168.21.4	3-ACCESS-01-C3300-···	gigabiteth···	Unmatched	2022-04-21 1···	cd	Details Modify Delete
00:88:1f:28:ce:32	11.13.221.200	unknown			193.168.21.5	3-ACCESS-02-C3100-···	gigabiteth···	Failed	2022-04-21 1···	cd	Rescan Delete

Figure 8.1.2.1 Identification result

- Identification result interface

  The identification result interface is divided into three parts. The left side is a sub menu, which shows the sub menu structure of terminal security. The upper right is the function area, including the feature library upgrade button, rescan button, and condition query button. The lower right is the identification result display area, including terminal MAC address, IP address, manufacturer, type, operating system, access device IP, access device name, access port, identification result, identification time, organization, and view details, edit, and delete buttons for a single identification result.

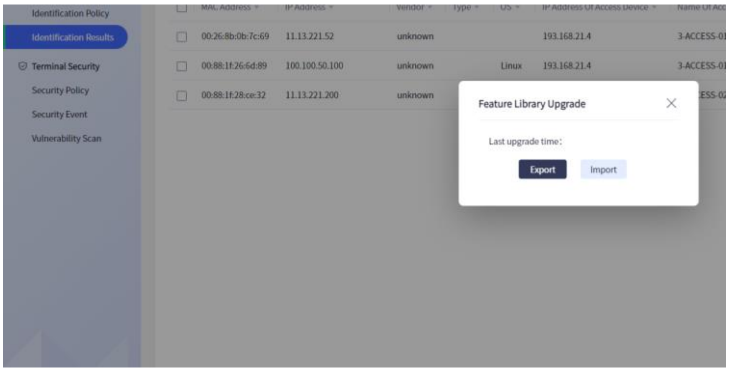


☐	MAC Address	IP Address	Vendor	Type	OS	IP Address Of Access Device	Name Of Access
☐	00:26:8b:0b:7c:69	11.13.221.52	unknown			193.168.21.4	3-ACCESS-01-C
☐	00:88:1f:26:6d:89	100.100.50.100	unknown		Linux	193.168.21.4	3-ACCESS-01-C
☐	00:88:1f:28:ce:32	11.13.221.200	unknown			193.168.21.5	3-ACCESS-02-C

Figure 8.1.2.2 Identification result interface

- Feature library upgrade

  The following figure shows the import and export buttons. Import can supplement the feature library, and export can export the encrypted feature group information.



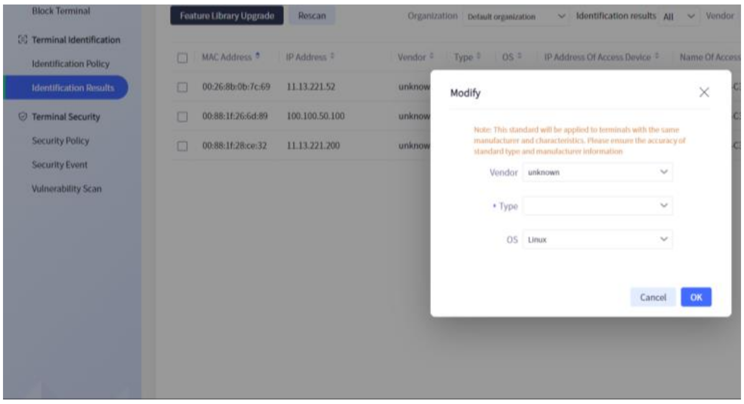
Feature Library Upgrade

Last upgrade time:

Figure 8.1.2.3 Feature library upgrade

- Edit identification result

  Edit the manufacturer, type and operating system information, and update the above information to the fingerprint database for the next identification match.



Modify

Note: This standard will be applied to terminals with the same manufacturer and characteristics. Please ensure the accuracy of standard type and manufacturer information

Vendor: unknown

* Type:

OS: Linux

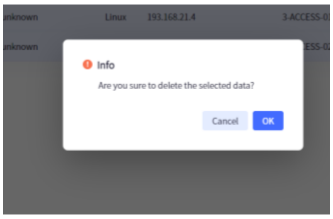
Figure 8.1.2.4 Edit identification result

  After the terminal is successfully identified, it can also be edited. During editing, the user can choose whether to synchronize this modification to the fingerprint database

- Delete identification result

  Delete this terminal identification result. Single deletion and batch deletion are supported.

Click **OK** to execute the deletion operation, as shown in the following figure:



Are you sure to delete the selected data?

Figure 8.1.2.6 Delete the identification result

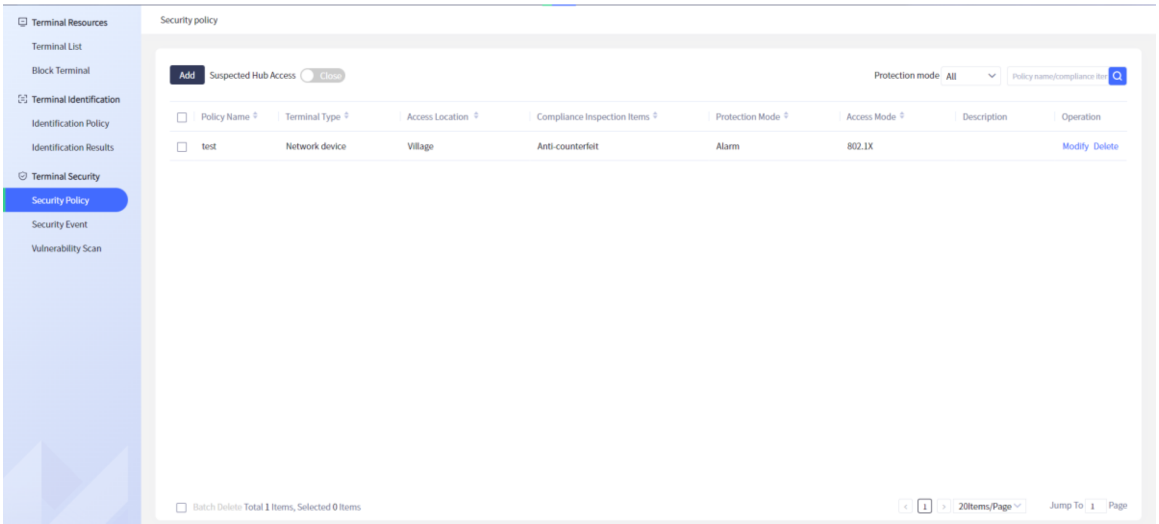
8.3 Terminal Security

8.3.1 Security Policy

The security policy interface displays all terminal security policy data, and provides functions such as query, add, modify, delete, and batch delete.

- Security policy interface

The security policy interface is divided into two parts: the upper part is the function area, including query input box, query button and add button; The lower part on the right is the display list of security policies.



☐	Policy Name	Terminal Type	Access Location	Compliance Inspection Items	Protection Mode	Access Mode	Description	Operation
☐	test	Network device	Village	Anti-counterfeit	Alarm	802.1X		Modify Delete

Total 1 Items, Selected 0 Items

Figure 8.2.1.1 Security policy interface

- Security policy function area

Add button: You can add a security policy, as shown in figure 8.2.1.2.

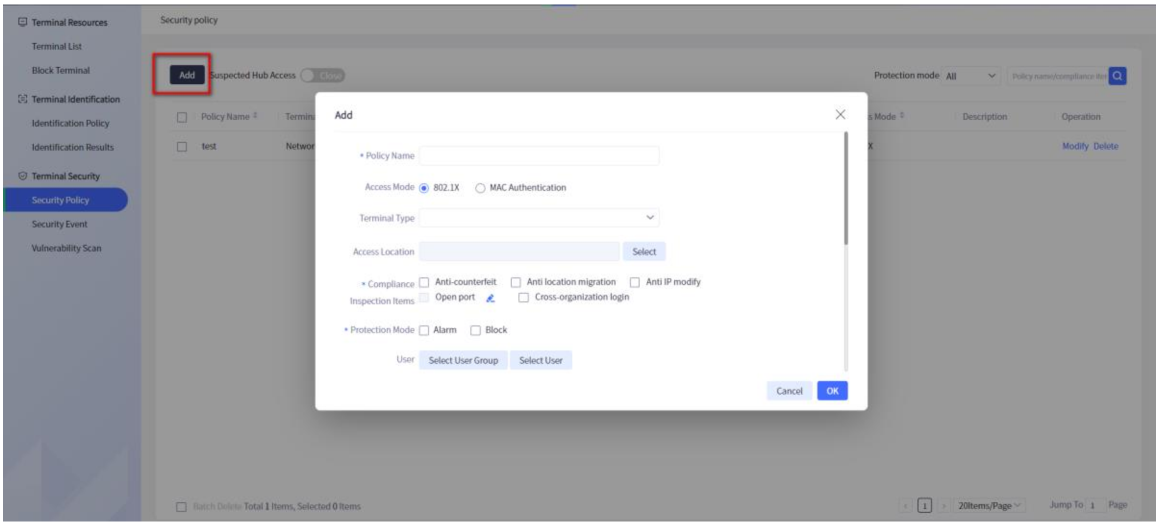
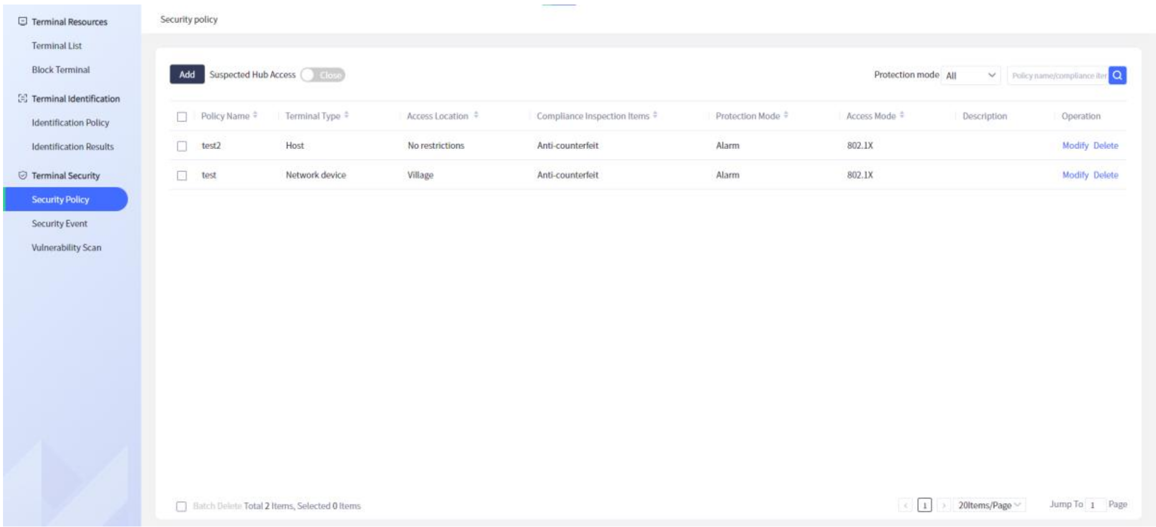


Figure 8.2.1.2 Add security policy

Query button: Query security policy data according to query criteria.

- Security policy list

The security policy list displays the policy name, terminal type, access location, compliance check items, protection method, description and operation; If the terminal type and access location are not selected, the display is unlimited.

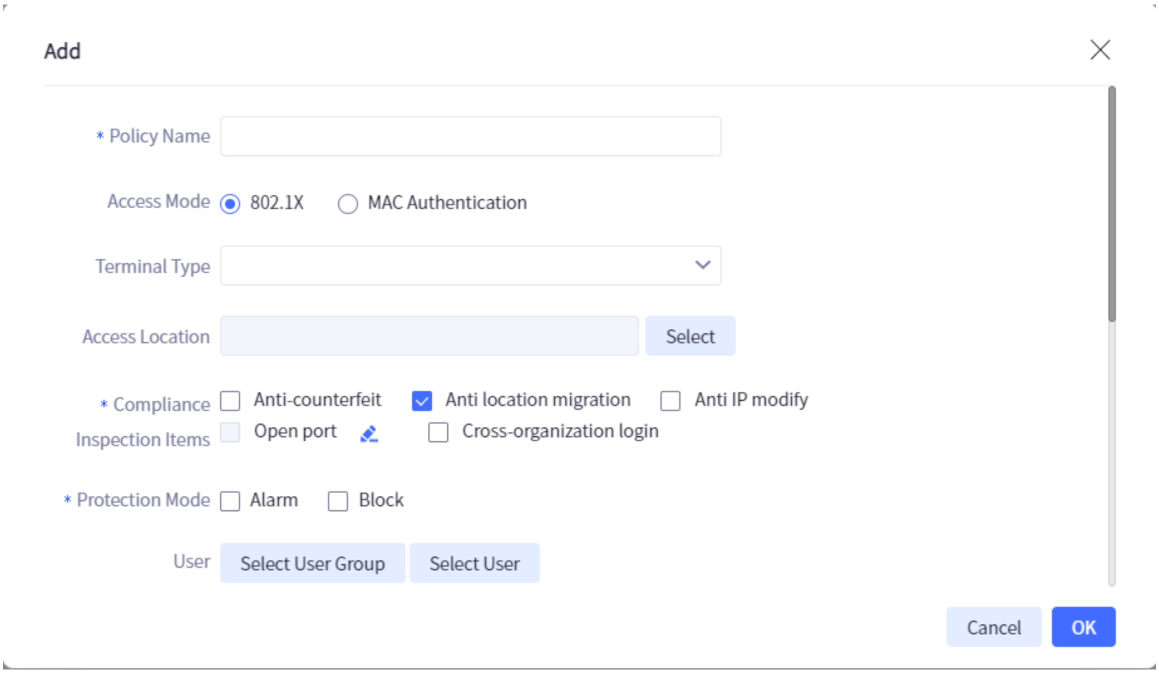


☐	Policy Name	Terminal Type	Access Location	Compliance Inspection Items	Protection Mode	Access Mode	Description	Operation
☐	test2	Host	No restrictions	Anti-counterfeit	Alarm	802.1X		Modify Delete
☐	test	Network device	Village	Anti-counterfeit	Alarm	802.1X		Modify Delete

Figure 8.2.1.3 Security policy list

- Add security policy

Click the **Add** button to display the “Add” pop-up box. The user needs to enter the policy name, terminal type, access location, and select compliance inspection items and protection methods, as shown in Figure 8.2.1.4 below.



* Policy Name

Access Mode ● 802.1X ○ MAC Authentication

Terminal Type

Access Location

* Compliance Inspection Items ☐ Anti-counterfeit ☑ Anti location migration ☐ Anti IP modify ☐ Open port ☐ Cross-organization login

* Protection Mode ☐ Alarm ☐ Block

User

Figure 8.2.1.4 Add security policy

Policy name: required item and cannot be greater than 32 characters.

Access mode: required. You can choose either MA authentication or 802.1x. The default is 802.1x.

Terminal type: optional; if it is not selected, it is unlimited by default.

Access location: optional; if it is not selected, it is unlimited by default.

Compliance inspection items (check at least one):

Anti-counterfeit: If anti-counterfeit is checked, the MAC, terminal type and operating system of the terminal will be checked. If there is any inconsistency with the baseline, a counterfeiting event will occur.

Anti location migration: If anti-location migration is checked, the access location of the terminal will be checked. If the location is changed, a security event of location change will occur.

Anti IP modify: If anti IP modify is checked, the IP of the terminal will be checked. If the IP is changed, a security event of IP change will occur.

Open port: To open port, you need to fill in "open port" or "close port" (both can be filled in at the same time). The port number filled in will be scanned after the terminal matches the policy. In the scanned result, the port number will be checked to see if it contains the open port number and does not contain the close port number. Otherwise, a port exception event will be generated. See figure 8.2.1.5 below.

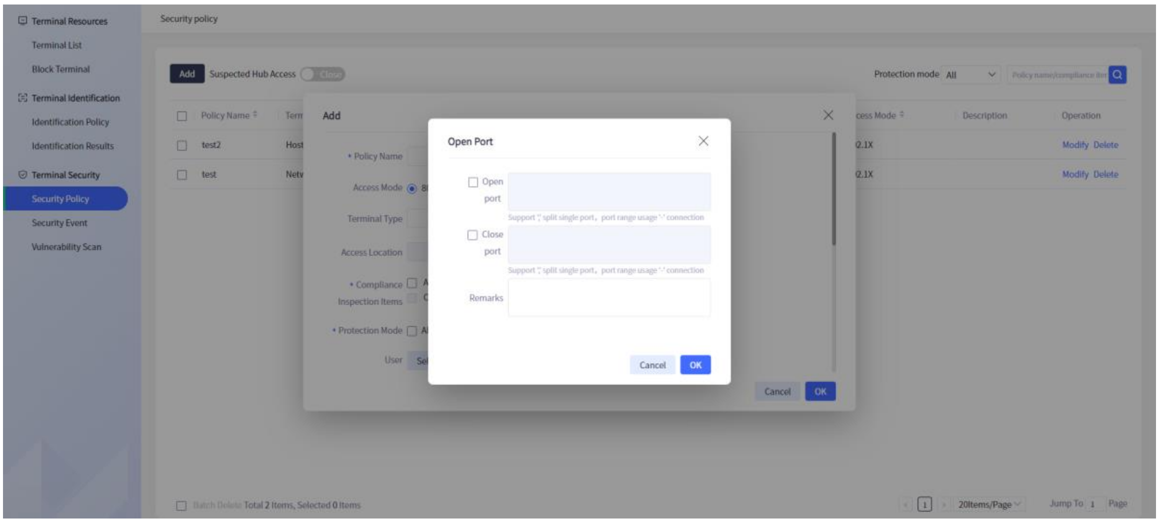


Figure 8.2.1.5 Open ports

Protection mode: check at least one item for alarm and block. When alarm generates an event, send alarm information. If selecting block, the MAC of the terminal will be added to the blacklist. The terminal will be directly refused during the next authentication.

User: You can select user/user group.

When a user/user group is selected, the online terminals of the user/user group will become one of the matching items of the policy.

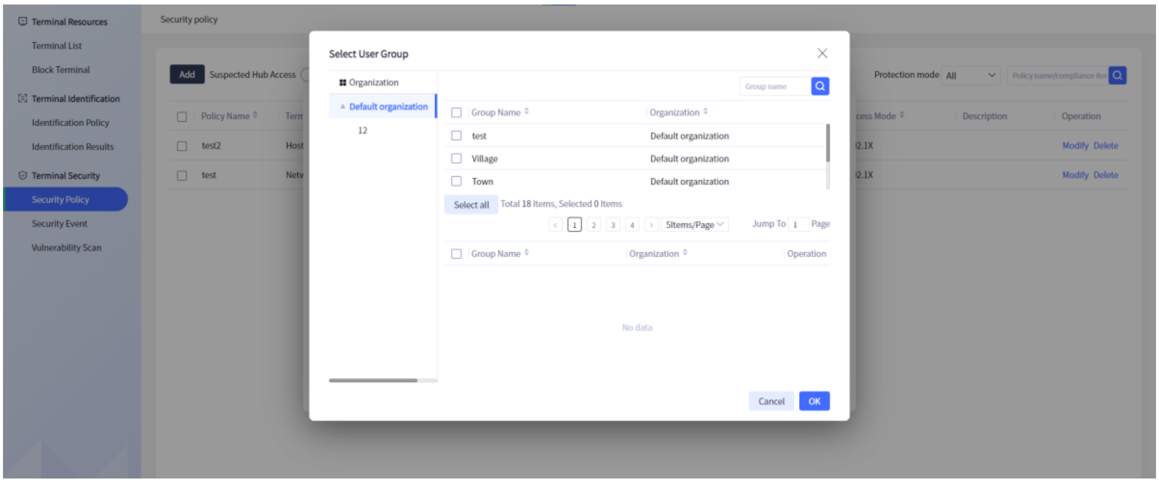
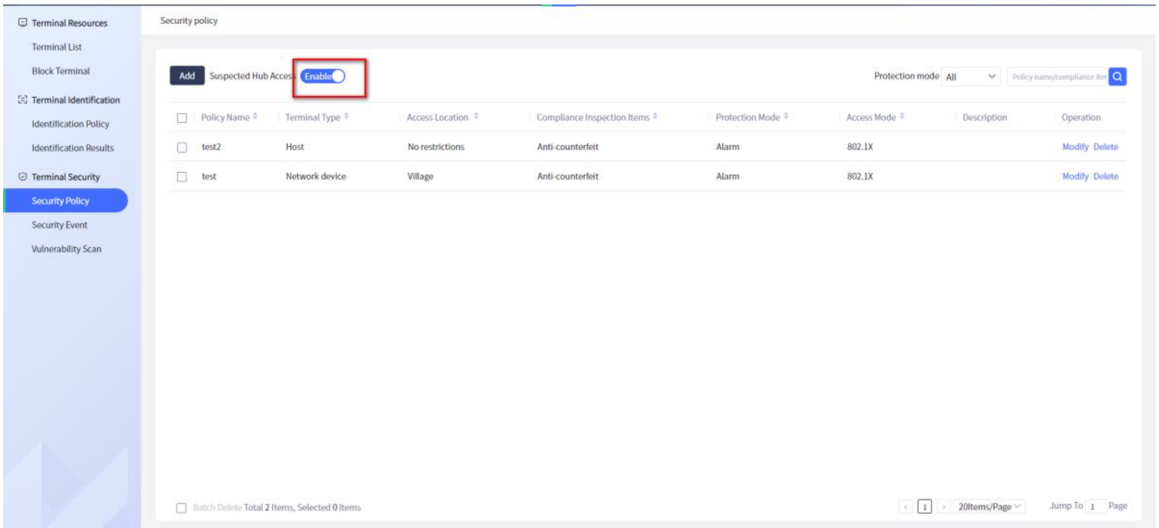


Figure 8.2.1.6 Select user/user group

- Suspected hub access

The suspected hub access is off by default. When you click the marked button in the figure below, the suspected hub access check will be enabled. When two or more terminals access the same device and port in the same access mode, a security event of suspected hub access will be generated (as shown in figure 8.2.2.1), and the corresponding alarm information will be sent.



☐	Policy Name	Terminal Type	Access Location	Compliance Inspection Items	Protection Mode	Access Mode	Description	Operation
☐	test2	Host	No restrictions	Anti-counterfeit	Alarm	802.1X		Modify Delete
☐	test	Network device	Village	Anti-counterfeit	Alarm	802.1X		Modify Delete

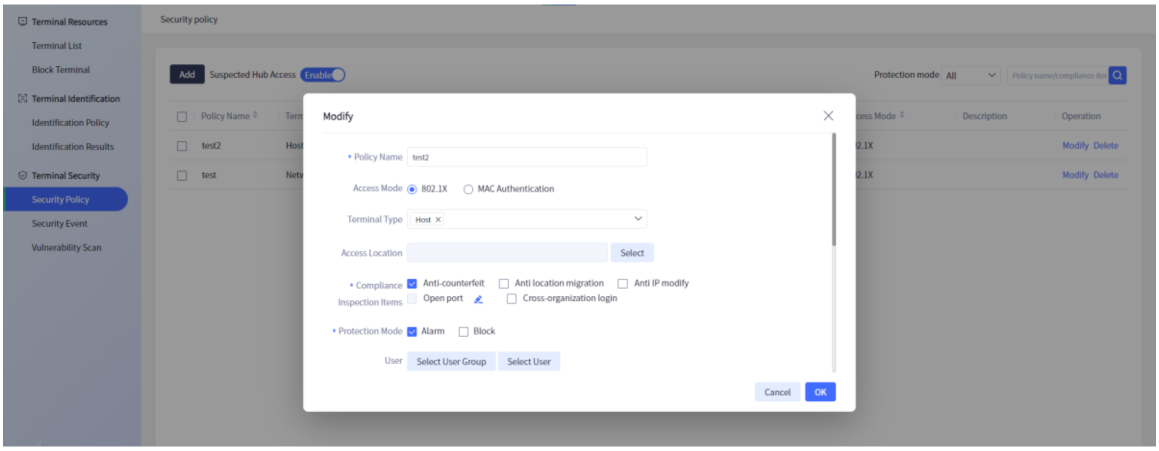
Figure 8.2.1.7 Enable/disable suspected hub access

Caution

- When the terminal goes online, matches the policy, and compliance check items check the corresponding items, compare according to the baseline in terminal resource monitoring. When the item in the baseline is empty, the item will not be checked accordingly.

- Modify security policy

Click the desired policy to display the **Modify** pop-up box. Users can modify all information as required. See figure 8.2.1.6 below.



* Policy Name: test2

Access Mode: ● 802.1X ○ MAC Authentication

Terminal Type: Host ×

Access Location:

* Compliance Inspection Items: ☑ Anti-counterfeit ☐ Anti location migration ☐ Anti IP modify ☐ Open port ☐ Cross-organization login

* Protection Mode: ☑ Alarm ☐ Block

User:

Figure 8.2.1.8 Modify security policy

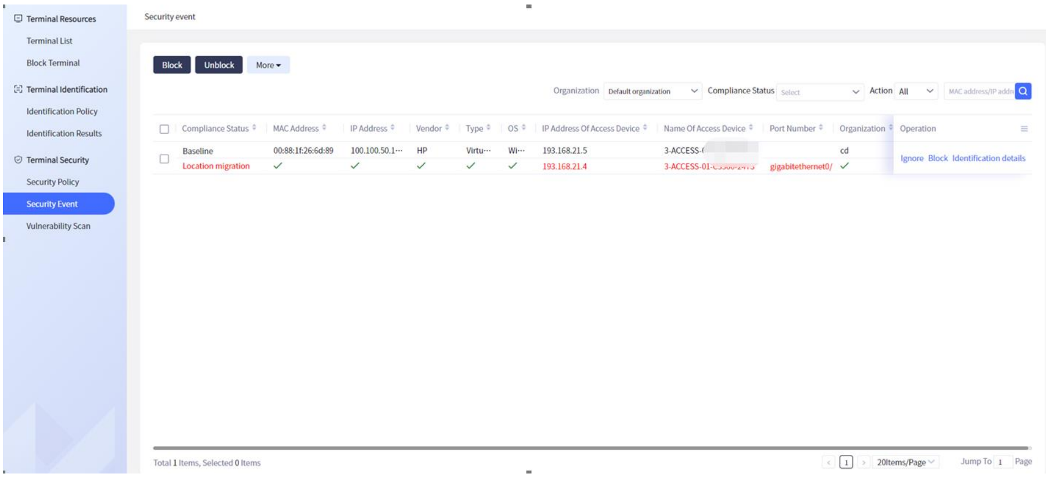
- Delete: deletes a single security policy.
- Batch delete: deletes the selected security policies in batch.

8.3.2 Security Event

In the security event interface, the terminal goes online, matches the security policy, compares the terminal information scanned by the terminal with the baseline information, and generates the corresponding security event data according to the matched policy information; The page displays all terminal security event data, and provides functions, such as querying, blocking, unblocking, ignoring, and resetting the baseline.

- Security event interface

The security event interface is divided into three parts. The organization tree on the left supports filtering the security events corresponding to the terminal by organization; The upper part of the right is the function area, including block, unblock, ignore, reset baseline, compliance status filtering, processing status, query input box and query button; The lower part on the right is the display list of security events. See figure 8.2.2.1 below.



Organization: Default organization
Compliance Status: Select
Action: All

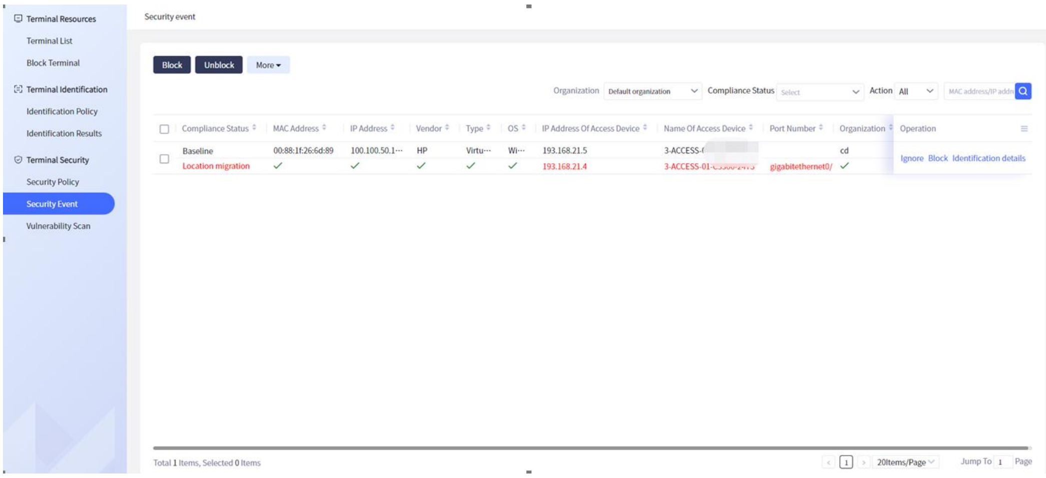
Compliance Status	MAC Address	IP Address	Vendor	Type	OS	IP Address Of Access Device	Name Of Access Device	Port Number	Organization
Baseline	00:88:1f:26:6d:89	100.100.50.1···	HP	Virtu···	Wi···	193.168.21.5	3-ACCESS-[redacted]		cd
Location migration	✓	✓	✓	✓	✓	193.168.21.4	3-ACCESS-01-[redacted]	gigabitethernet0/	✓

Total 1 Items, Selected 0 Items

Figure 8.2.2.1 Security event interface

- Security event list

The compliance status, MAC address, IP address, manufacturer, type, operating system, access device IP, access device name, access port, organization, processing status and operation are displayed in the security policy list; One event consists of two terminal messages, the baseline terminal message above and the terminal message generating the security event below. A green "tick" indicates that the message is consistent with the baseline message, as shown in figure 8.2.2.2.



Organization: Default organization
Compliance Status: Select
Action: All

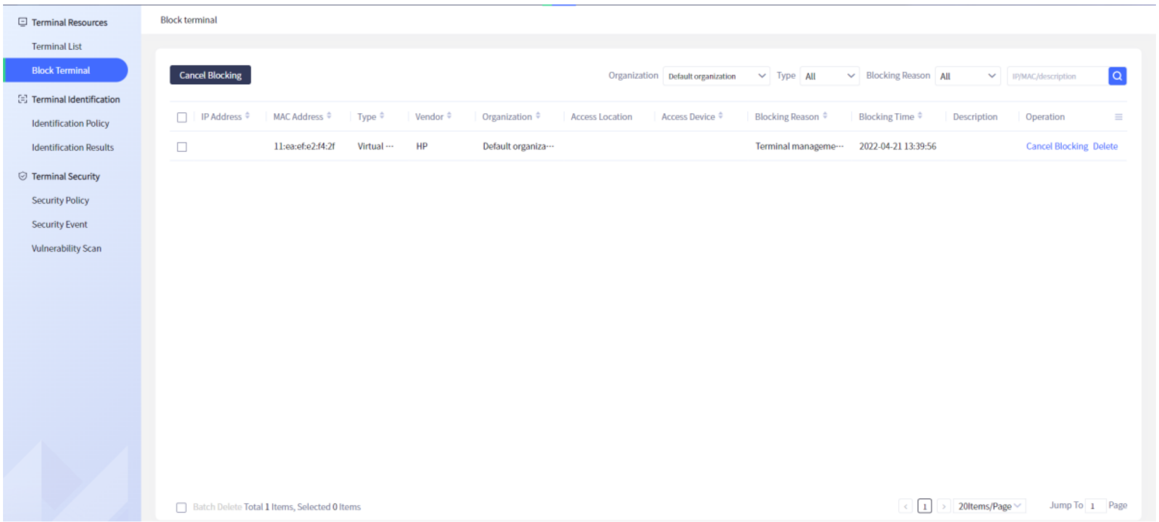
Compliance Status	MAC Address	IP Address	Vendor	Type	OS	IP Address Of Access Device	Name Of Access Device	Port Number	Organization
Baseline	00:88:1f:26:6d:89	100.100.50.1···	HP	Virtu···	Wi···	193.168.21.5	3-ACCESS-[redacted]		cd
Location migration	✓	✓	✓	✓	✓	193.168.21.4	3-ACCESS-01-[redacted]	gigabitethernet0/	✓

Total 1 Items, Selected 0 Items

Figure 8.2.2.2 Security event list

- Security event function area

Block: add the counterfeit terminal to the terminal resource / block terminal, and send an alarm. The corresponding security event is displayed as blocked, as shown in figure 8.2.2.3.



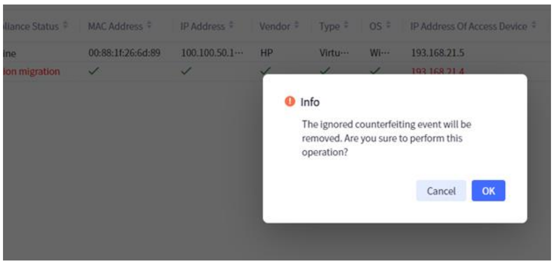
☐	IP Address	MAC Address	Type	Vendor	Organization	Access Location	Access Device	Blocking Reason	Blocking Time	Description	Operation
☐		11:ea:ef:e2:f4:2f	Virtual ···	HP	Default organiza···			Terminal manageme···	2022-04-21 13:39:56		Cancel Blocking Delete

☐ Batch Delete Total 1 Items, Selected 0 Items

Figure 8.2.2.3 MAC blacklist interface

Unblock: Remove the counterfeit terminal from the blocked terminal, and at the same time, clear the alarm. The corresponding security event is displayed as recovered.

Ignore: click **More** to ignore the security event. When the terminal is blocked, it will be removed from the blocked terminal synchronously; And clear the alarm and delete the event, as shown in figure 8.2.2.4.



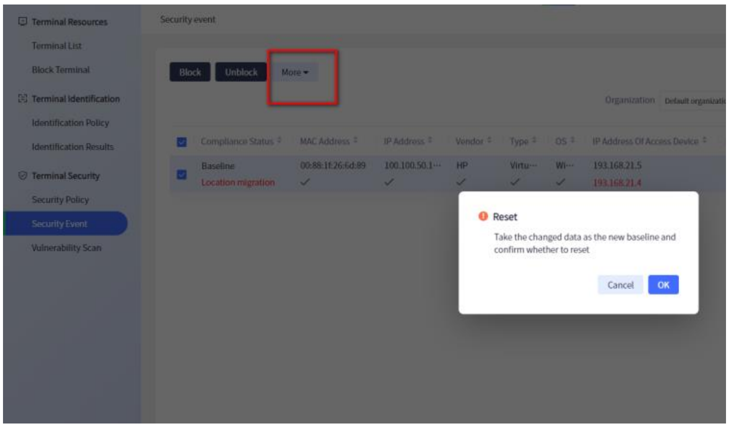
lliance Status	MAC Address	IP Address	Vendor	Type	OS	IP Address Of Access Device
ine	00:88:1f:26:6d:89	100.100.50.1···	HP	Virtu···	Wi···	193.168.21.5
ion migration	✓	✓	✓	✓	✓	193.168.21.4

Info

The ignored counterfeiting event will be removed. Are you sure to perform this operation?

Figure 8.2.2.4 Ignore event

Reset baseline: click **More** to reset the baseline and replace the original baseline with a counterfeit terminal. If the reset event is blocked, the MAC blacklist will be removed synchronously and the alarm will be relieved, as shown in figure 8.2.2.5.



☑	Compliance Status	MAC Address	IP Address	Vendor	Type	OS	IP Address Of Access Device
☑	Baseline Location migration	00:88:1f:26:6d:89 ✓	100.100.50.1··· ✓	HP ✓	Virtu··· ✓	Wi··· ✓	193.168.21.5 193.168.21.4

Reset

Take the changed data as the new baseline and confirm whether to reset

Figure 8.2.2.5 Reset baseline

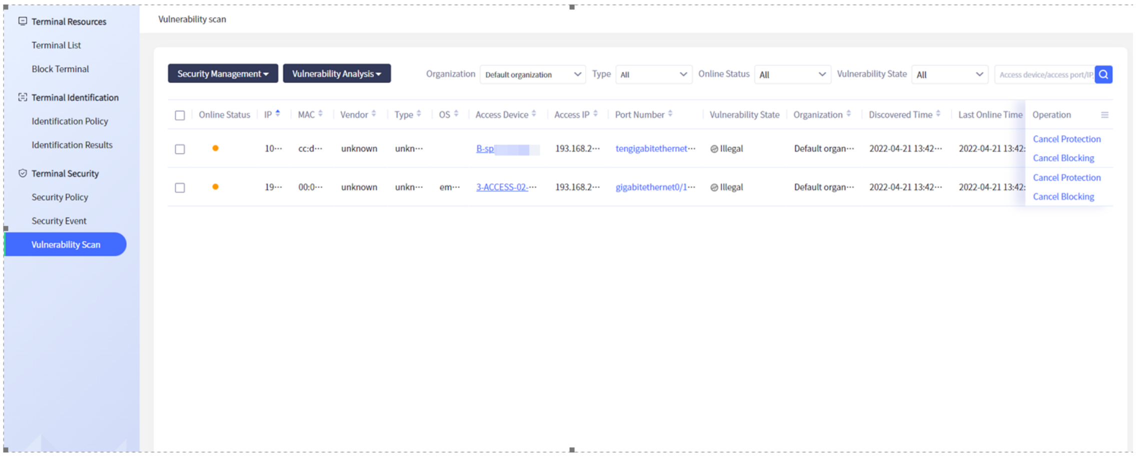
Caution

- By default, the terminal IP address is unique. If the MAC addresses are different and IP addresses are the same, it will also be considered as counterfeit. You can turn off the unique IP switch in the configuration file.

- For the security events of suspected hub access, you cannot perform the operations of resetting baseline, block or unblock, but can only ignore it.

8.4 Vulnerability Scan

Click the above menu **Terminal Protection** > **Terminal Security** > **Vulnerability Scan** to enter the vulnerability scan function interface.

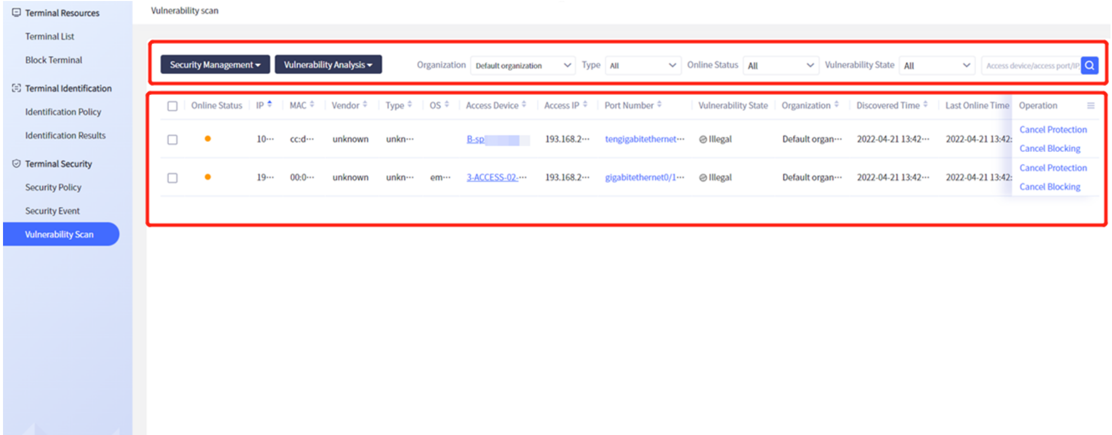


Organization: Default organization; Type: All; Online Status: All; Vulnerability State: All; Access device/access port/IP

☐	Online Status	IP	MAC	Vendor	Type	OS	Access Device	Access IP	Port Number	Vulnerability State	Organization	Discovered Time	Last Online Time	Operation
☐	●	10···	cc:d···	unknown	unkn···		B-sp[redacted]	193.168.2···	tengigabitethernet···	⊘ Illegal	Default organ···	2022-04-21 13:42···	2022-04-21 13:42:	Cancel Protection Cancel Blocking
☐	●	19···	00:0···	unknown	unkn···	em···	3-ACCESS-02-···	193.168.2···	gigabitethernet0/1···	⊘ Illegal	Default organ···	2022-04-21 13:42···	2022-04-21 13:42:	Cancel Protection Cancel Blocking

Figure 8.4.1 Vulnerability scan

Vulnerability scan is divided into three areas: the upper part is the main functional area, the middle part is the information display area, and the lower part is the basic functional area.

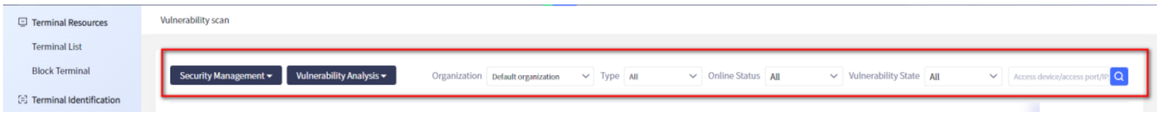


Organization: Default organization; Type: All; Online Status: All; Vulnerability State: All; Access device/access port/IP

☐	Online Status	IP	MAC	Vendor	Type	OS	Access Device	Access IP	Port Number	Vulnerability State	Organization	Discovered Time	Last Online Time	Operation
☐	●	10···	cc:d···	unknown	unkn···		B-sp[redacted]	193.168.2···	tengigabitethernet···	⊘ Illegal	Default organ···	2022-04-21 13:42···	2022-04-21 13:42:	Cancel Protection Cancel Blocking
☐	●	19···	00:0···	unknown	unkn···	em···	3-ACCESS-02-···	193.168.2···	gigabitethernet0/1···	⊘ Illegal	Default organ···	2022-04-21 13:42···	2022-04-21 13:42:	Cancel Protection Cancel Blocking

Figure 8.4.2 Vulnerability scan

The upper part is the main functional area, including security management and vulnerability analysis.



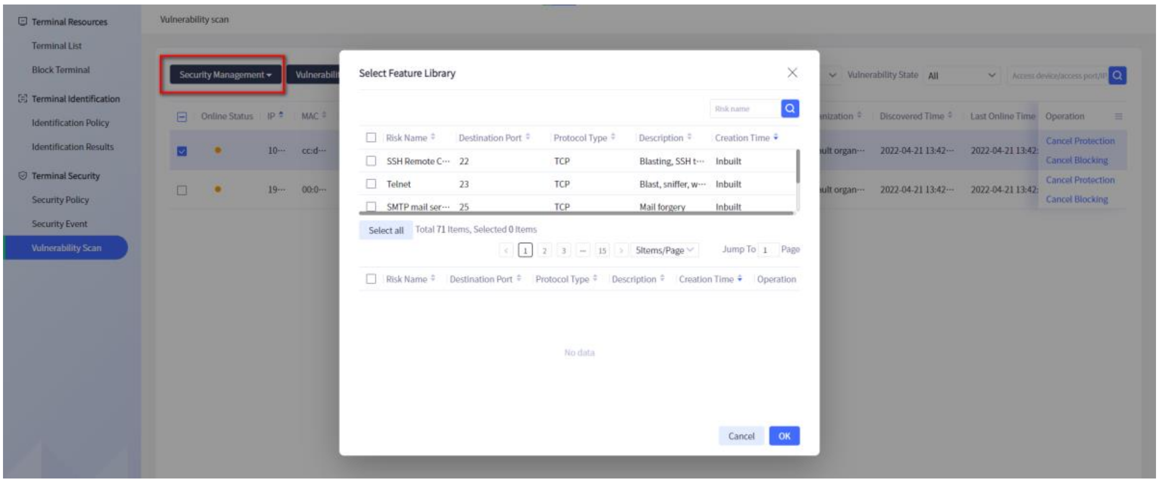
Organization: Default organization; Type: All; Online Status: All; Vulnerability State: All; Access device/access port/IP

Figure 8.4.3 Top function area

Security management includes protect, cancel protection, block, cancel blocking and historical records button.

- Protect: select the terminal, click **Security Management** > **Protect**, display the **Select Feature**

Library window, and the user can select the feature information for protection.



Select Feature Library

☐	Risk Name	Destination Port	Protocol Type	Description	Creation Time
☐	SSH Remote C···	22	TCP	Blasting, SSH t···	Inbuilt
☐	Telnet	23	TCP	Blast, sniffer, w···	Inbuilt
☐	SMTP mail ser···	25	TCP	Mail forgery	Inbuilt

Select all Total 71 Items, Selected 0 Items

Figure 8.4.4 Select feature library

- Cancel protection: select a terminal and click **Security Management** > **Cancel Protection** to unprotect the terminal.
- Block: select a terminal and click **Security Management** > **Block** to block this terminal.
- Cancel Blocking: select a terminal and click **Security Management** > **Cancel Blocking** to unblock this terminal.
- Historical Records: record the protection/blocking history.

Vulnerability analysis includes analysis setting and vulnerability feature library.

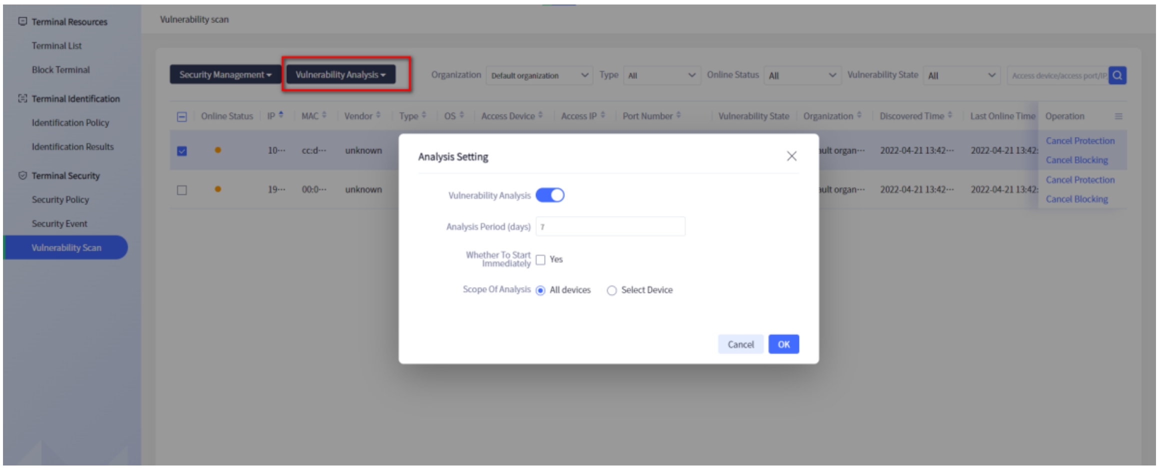
Analysis settings: set the parameters of vulnerability analysis, including the switch of vulnerability analysis, analysis period, whether to start immediately, and analysis range.

The vulnerability analysis switch is used to configure whether to enable vulnerability analysis.

The analysis period is used to configure the time interval for vulnerability analysis.

Whether to start immediately is used to configure whether to execute the setting result immediately.

Scope of Analysis includes **All devices** and **Select Device**. If selecting **All devices**, the terminals of all devices will be scanned by default. If selecting **Select Device**, the required devices will be selected according to user needs for vulnerability analysis.



Analysis Setting

Vulnerability Analysis: on

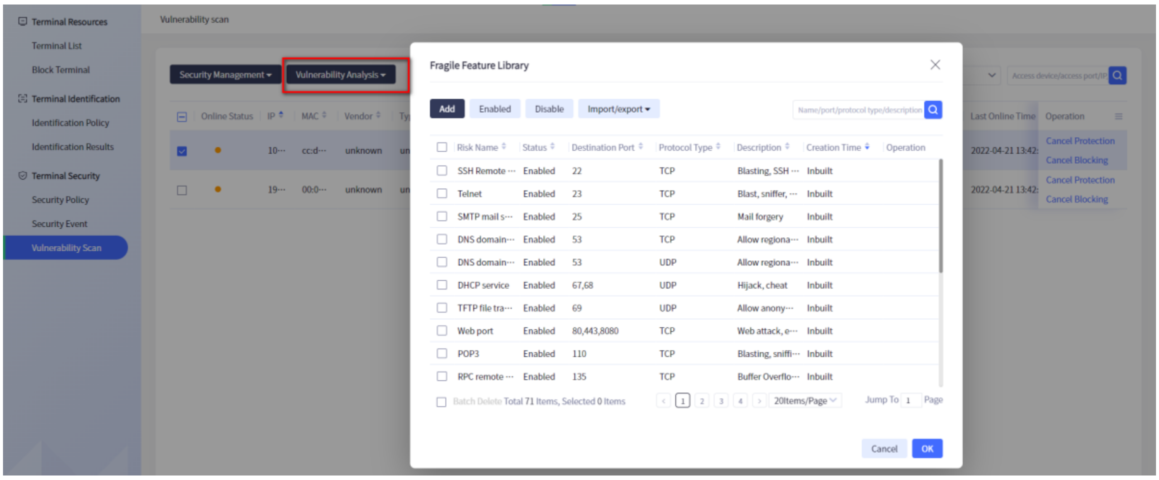
Analysis Period (days): 7

Whether To Start Immediately: ☐ Yes

Scope Of Analysis: ● All devices ○ Select Device

Figure 8.4.5 Analysis setting

- Fragile feature library: Provide the functions of adding, enabling, disabling, importing, exporting and fuzzy searching at the top of the fragile feature library interface. The middle part provides the risk name, status, destination port, protocol type, description, creation time and operation function of the vulnerability feature library. The following provides the functions of batch deletion and paging setting for the terminals.

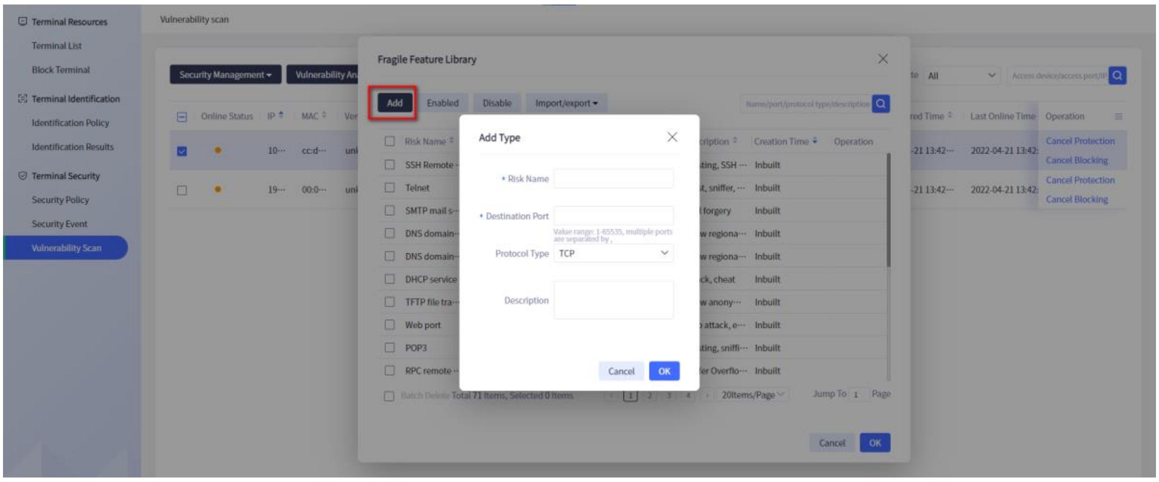


☐	Risk Name	Status	Destination Port	Protocol Type	Description	Creation Time	Operation
☐	SSH Remote ···	Enabled	22	TCP	Blasting, SSH ···	Inbuilt	
☐	Telnet	Enabled	23	TCP	Blast, sniffer, ···	Inbuilt	
☐	SMTP mail s···	Enabled	25	TCP	Mail forgery	Inbuilt	
☐	DNS domain···	Enabled	53	TCP	Allow regiona···	Inbuilt	
☐	DNS domain···	Enabled	53	UDP	Allow regiona···	Inbuilt	
☐	DHCP service	Enabled	67,68	UDP	Hijack, cheat	Inbuilt	
☐	TFTP file tra···	Enabled	69	UDP	Allow anony···	Inbuilt	
☐	Web port	Enabled	80,443,8080	TCP	Web attack, e···	Inbuilt	
☐	POP3	Enabled	110	TCP	Blasting, sniffi···	Inbuilt	
☐	RPC remote ···	Enabled	135	TCP	Buffer Overflo···	Inbuilt	

☐ Batch Delete Total 71 Items, Selected 0 Items

Figure 8.4.6 Fragile feature library

Add: You can add new vulnerability feature types, including risk name, destination port, protocol type and description.



* Risk Name

* Destination Port

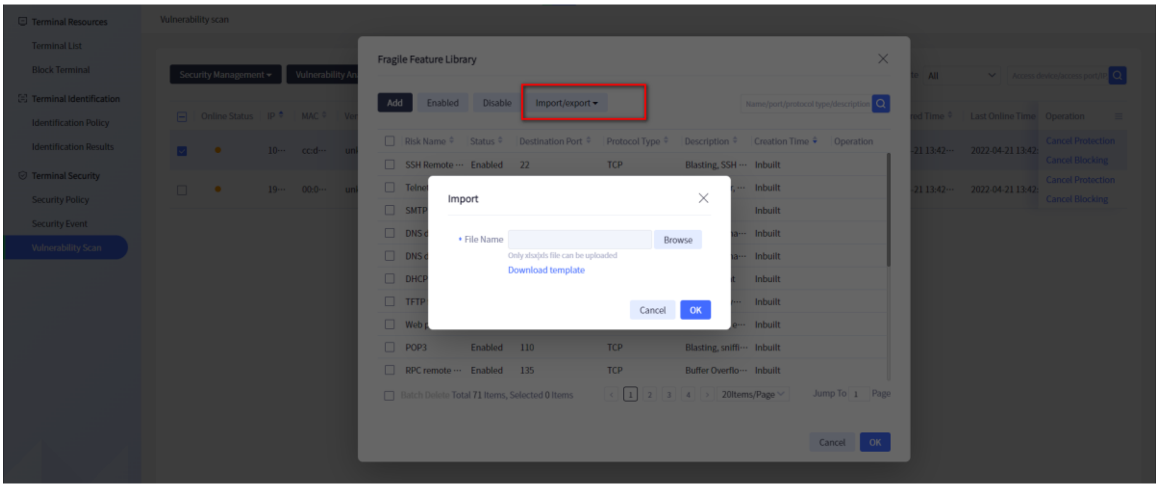
Value range: 1-65535, multiple ports are separated by ,

Protocol Type TCP

Description

Figure 8.4.7 Add fragile feature

Import: Click to download the template and fill in the corresponding information. After importing the edited file, you can modify and add the vulnerability information in batches.

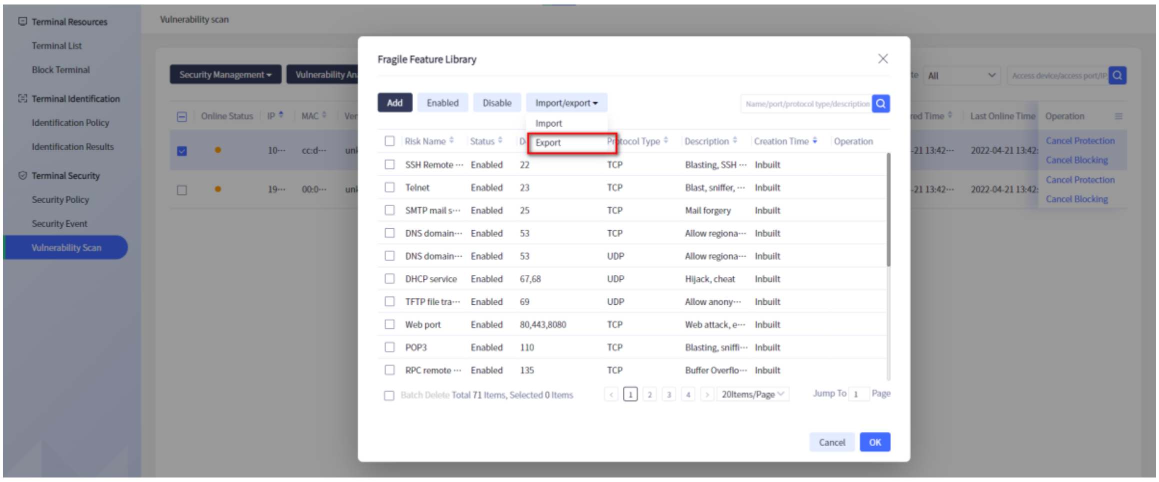


* File Name

Only xls/xlsx file can be uploaded

Figure 8.4.8 Import fragile features

Export: click **Export** to export the fragile feature library information.

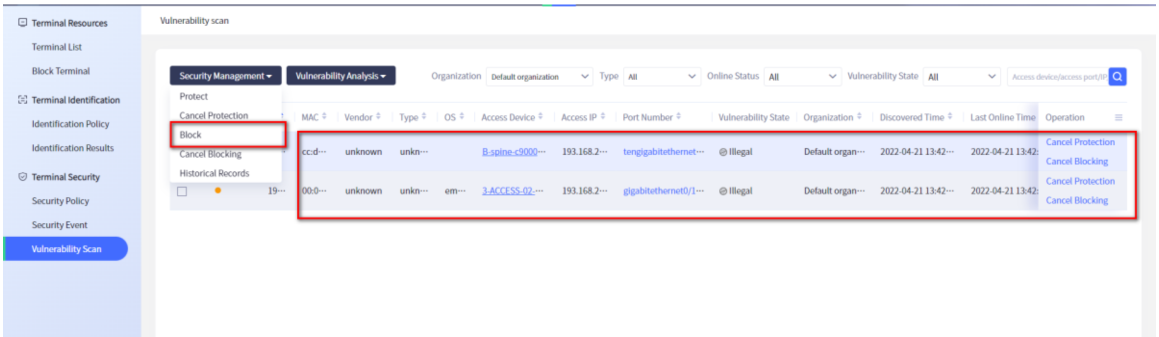


☐	Risk Name	Status	D	Protocol Type	Description	Creation Time	Operation
☐	SSH Remote ···	Enabled	22	TCP	Blasting, SSH ···	Inbuilt	
☐	Telnet	Enabled	23	TCP	Blast, sniffer, ···	Inbuilt	
☐	SMTP mail s···	Enabled	25	TCP	Mail forgery	Inbuilt	
☐	DNS domain···	Enabled	53	TCP	Allow regiona···	Inbuilt	
☐	DNS domain···	Enabled	53	UDP	Allow regiona···	Inbuilt	
☐	DHCP service	Enabled	67,68	UDP	Hijack, cheat	Inbuilt	
☐	TFTP file tra···	Enabled	69	UDP	Allow anony···	Inbuilt	
☐	Web port	Enabled	80,443,8080	TCP	Web attack, e···	Inbuilt	
☐	POP3	Enabled	110	TCP	Blasting, sniffi···	Inbuilt	
☐	RPC remote ···	Enabled	135	TCP	Buffer Overflo···	Inbuilt	

☐ Batch Delete Total 71 Items, Selected 0 Items ‹ 1 2 3 4 › 20Items/Page Jump To 1 Page

Figure 8.4.9 Export fragile feature

The middle area is the information display area. The display information includes IP, MAC, manufacturer, online status, type, operating system, access device, access IP, access port, security status, organization, discovery time and the latest online time. After each terminal message, it provides the operations of cancelling protection and cancelling block for a single message.

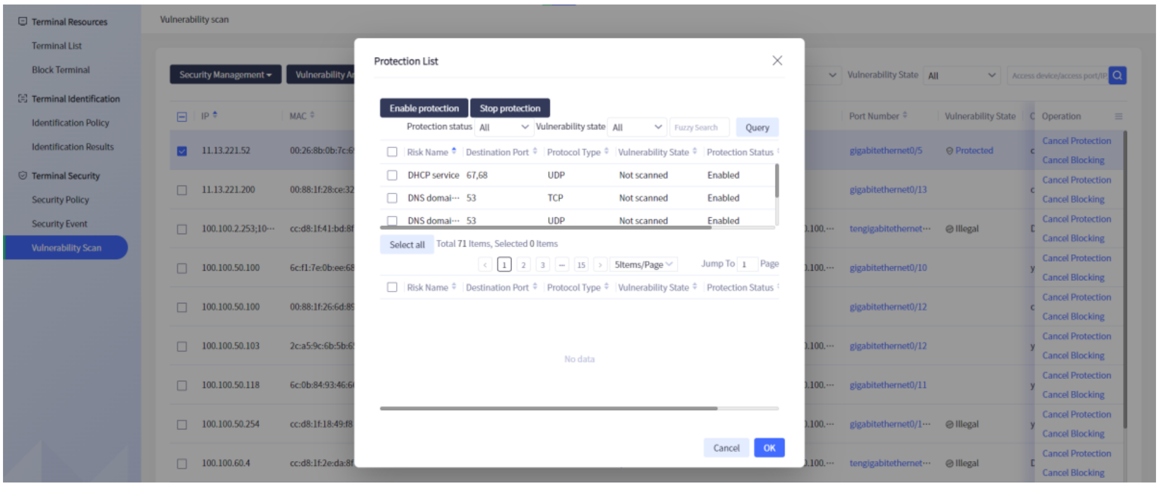


Organization: Default organization; Type: All; Online Status: All; Vulnerability State: All

MAC	Vendor	Type	OS	Access Device	Access IP	Port Number	Vulnerability State	Organization	Discovered Time	Last Online Time	Operation
cc:d···	unknown	unkn···		B-spine-c9000···	193.168.2···	tengigabitethernet···	Illegal	Default organ···	2022-04-21 13:42···	2022-04-21 13:42:	Cancel Protection Cancel Blocking
00:0···	unknown	unkn···	em···	3-ACCESS-02-···	193.168.2···	gigabitethernet0/1···	Illegal	Default organ···	2022-04-21 13:42···	2022-04-21 13:42:	Cancel Protection Cancel Blocking

Figure 8.4.10 Middle information display area

Click the **Weak** button on the fragile terminal to view the fragile port protection list and enable or disable the protection function for the fragile features.



Protection status: All; Vulnerability state: All

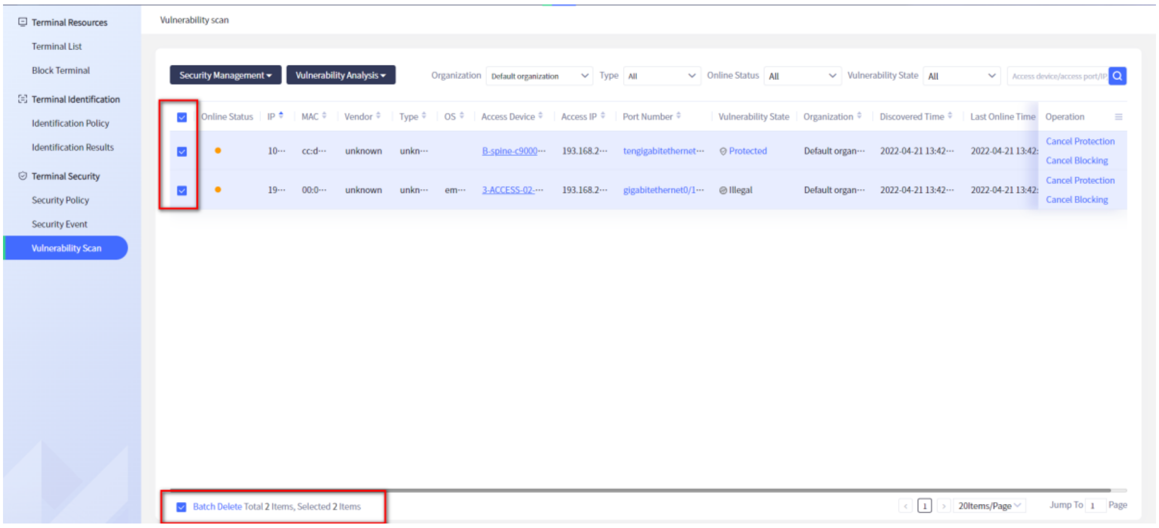
☐	Risk Name	Destination Port	Protocol Type	Vulnerability State	Protection Status
☐	DHCP service	67,68	UDP	Not scanned	Enabled
☐	DNS domai···	53	TCP	Not scanned	Enabled
☐	DNS domai···	53	UDP	Not scanned	Enabled

Total 71 Items, Selected 0 Items ‹ 1 2 3 ··· 15 › 5Items/Page Jump To 1 Page

☐	Risk Name	Destination Port	Protocol Type	Vulnerability State	Protection Status

Figure 8.4.11 Protection list

The bottom area provides the setting function of batch deletion and paging.



Organization: Default organization; Type: All; Online Status: All; Vulnerability State: All

☑	Online Status	IP	MAC	Vendor	Type	OS	Access Device	Access IP	Port Number	Vulnerability State	Organization	Discovered Time	Last Online Time	Operation
☑	●	10···	cc:d···	unknown	unkn···		B-spine-c9000···	193.168.2···	tengigabitethernet···	Protected	Default organ···	2022-04-21 13:42···	2022-04-21 13:42:	Cancel Protection Cancel Blocking
☑	●	19···	00:0···	unknown	unkn···	em···	3-ACCESS-02-···	193.168.2···	gigabitethernet0/1···	Illegal	Default organ···	2022-04-21 13:42···	2022-04-21 13:42:	Cancel Protection Cancel Blocking

☑ Batch Delete Total 2 Items, Selected 2 Items

< 1 > 20Items/Page Jump To 1 Page

Figure 8.4.12 Bottom function area

9 Network Maintenance

Configuration management mainly manages the related configurations of devices, including four functions: software package management, configuration file management, configuration command distribution, and policy object management. Click "Maintenance" > "Configuration Management" on the navigation bar at the top of the system to enter the corresponding sub module for operation.

9.1 Configuration Management

9.1.1 Device Configuration Management

The device configuration management module provides the management of device configuration tasks in the system and the query of device configuration;

Click "Maintenance" > "Configuration Management" > "Device Configuration " on the navigation bar at the top of the system to open the "Device Configuration " page, as follows:

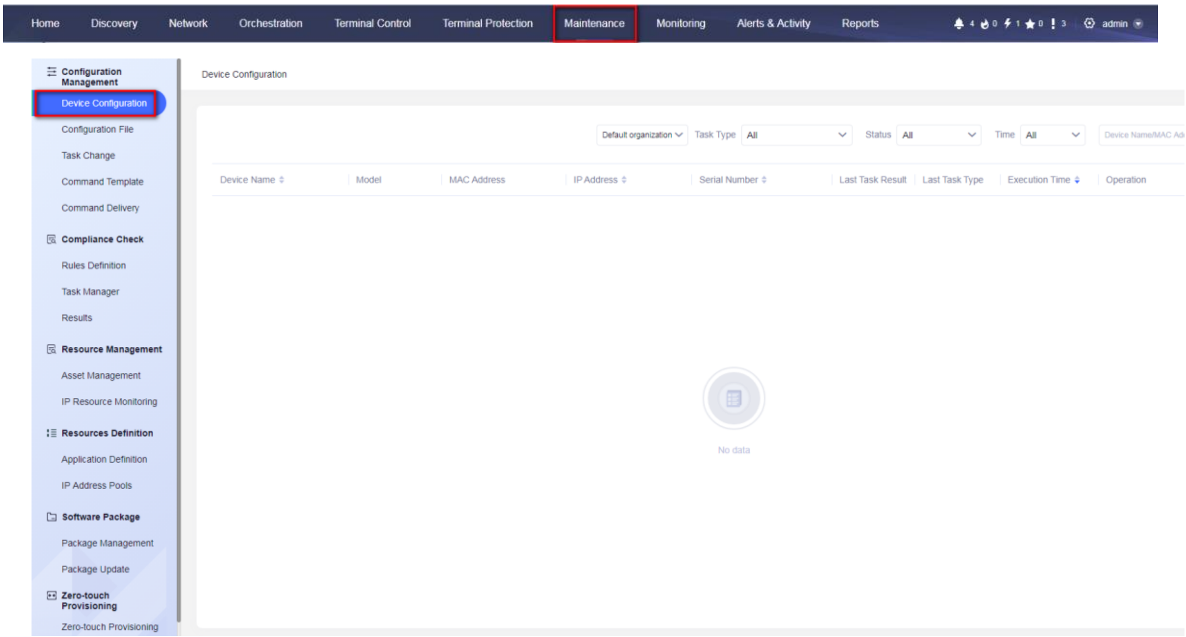
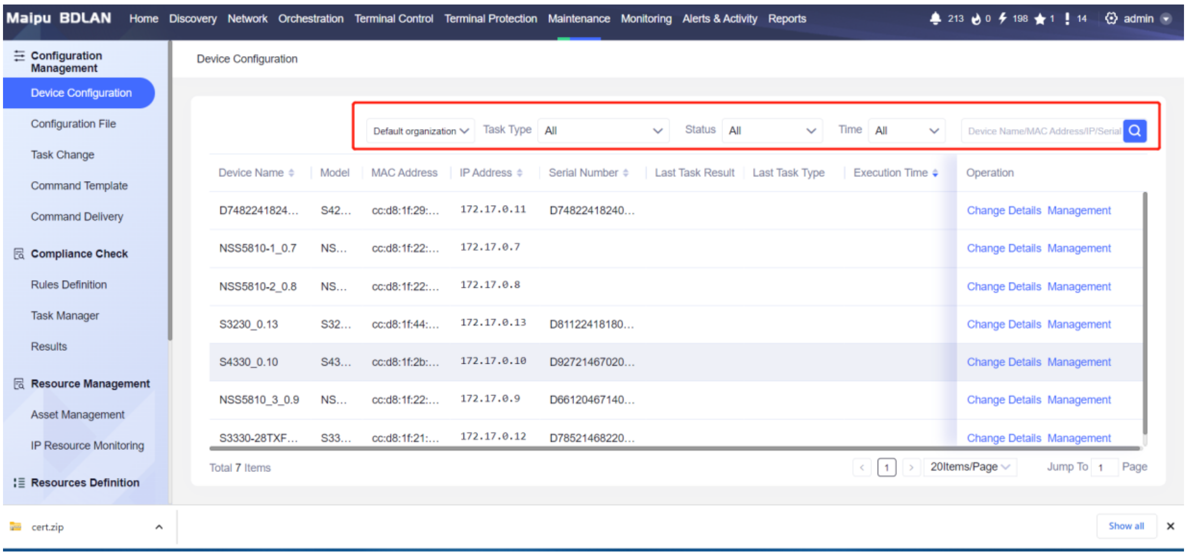


Figure 9.1.1.1Device configuration management

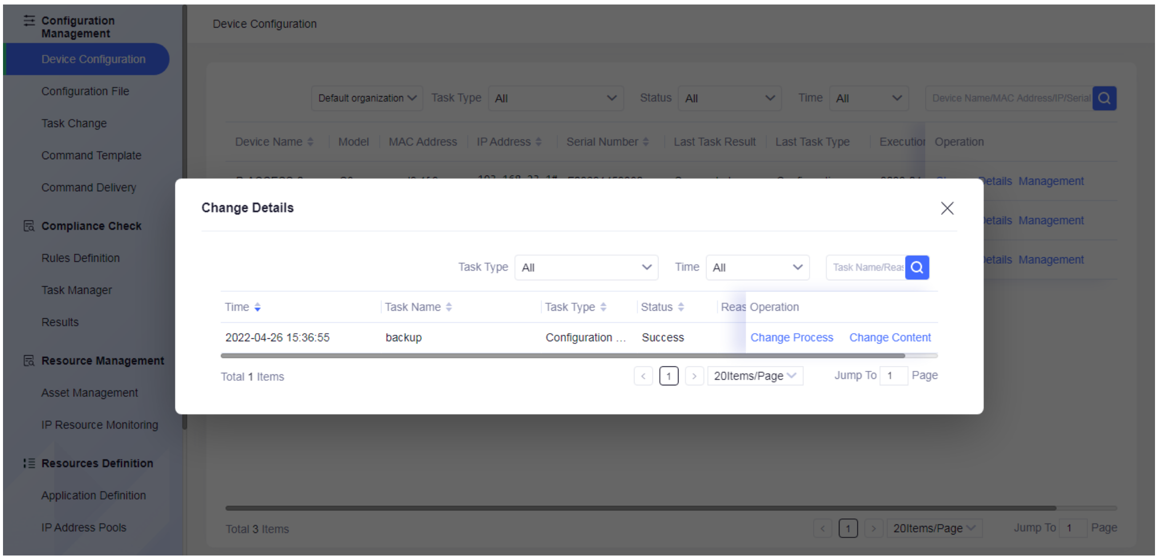
Users can accurately query by task type, change status, time, etc., and fuzzy query by device name, device MAC, device IP, device model, and serial number.



Device Name	Model	MAC Address	IP Address	Serial Number	Last Task Result	Last Task Type	Execution Time	Operation
D7482241824…	S42…	cc:d8:1f:29:…	172.17.0.11	D74822418240…				Change Details Management
NSS5810-1_0.7	NS…	cc:d8:1f:22:…	172.17.0.7					Change Details Management
NSS5810-2_0.8	NS…	cc:d8:1f:22:…	172.17.0.8					Change Details Management
S3230_0.13	S32…	cc:d8:1f:44:…	172.17.0.13	D81122418180…				Change Details Management
S4330_0.10	S43…	cc:d8:1f:2b:…	172.17.0.10	D92721467020…				Change Details Management
NSS5810_3_0.9	NS…	cc:d8:1f:22:…	172.17.0.9	D66120467140…				Change Details Management
S3330-28TXF…	S33…	cc:d8:1f:21:…	172.17.0.12	D78521468220…				Change Details Management

Figure 9.1.1.2 Query by conditions

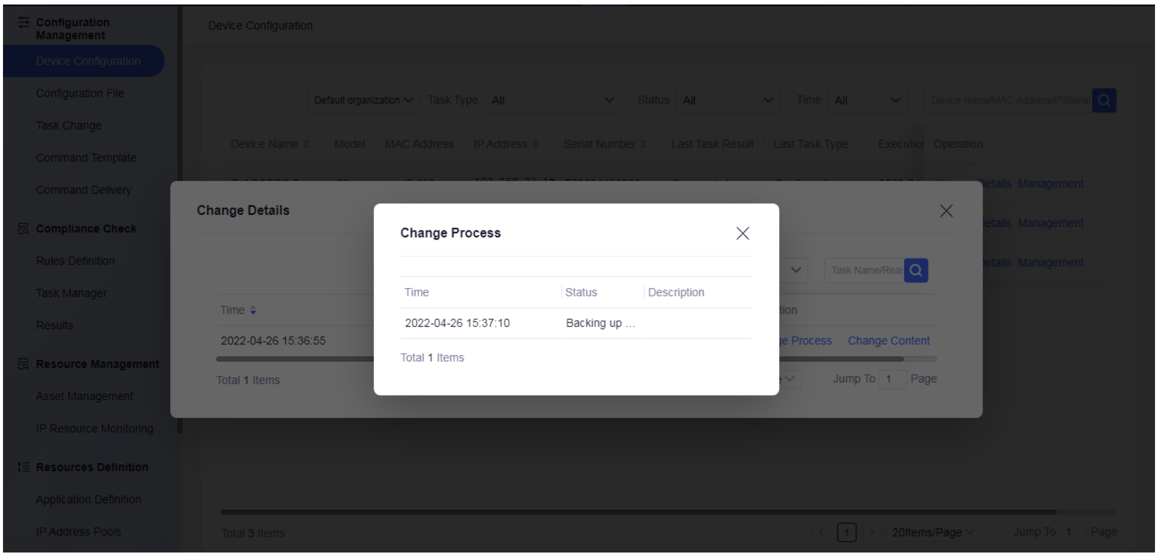
For change details, you can view the change time, task name, task type, task status, failure reason, change process and content. It provides precise query by task type and time, and fuzzy query by task name and failure reason.



Time	Task Name	Task Type	Status	Reas	Operation
2022-04-26 15:36:55	backup	Configuration …	Success		Change Process Change Content

Figure 9.1.1.3 Change details

For the change process, you can view the detailed steps:



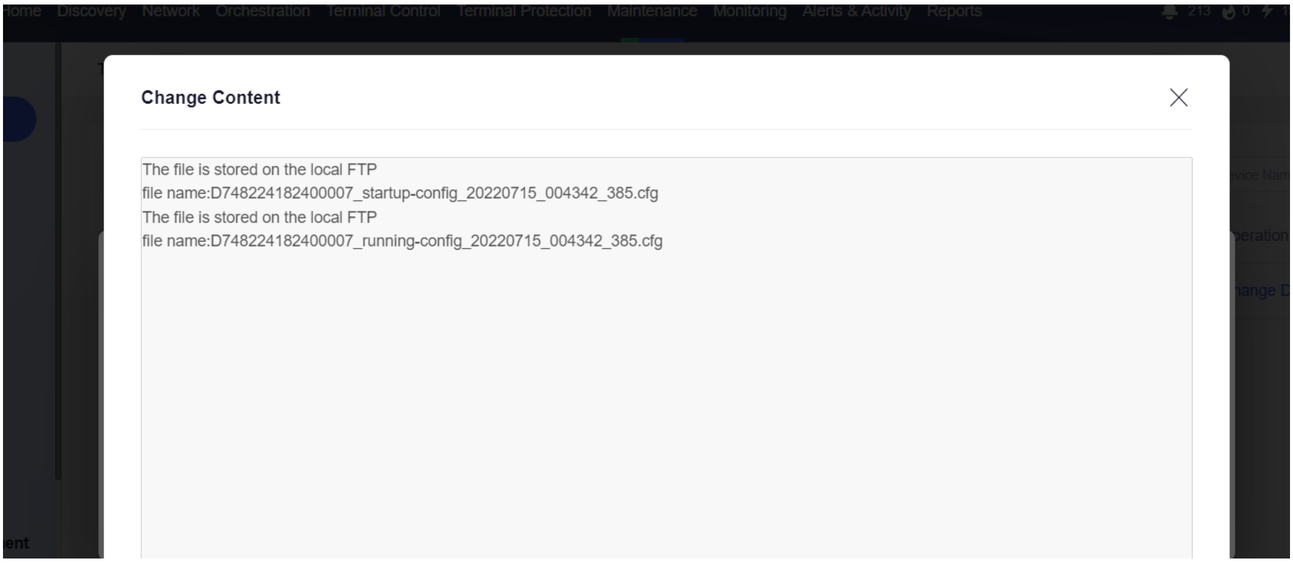
Change Process

Time	Status	Description
2022-04-26 15:37:10	Backing up ...	

Total 1 Items

Figure 9.1.1.4 Change process

Change content: You can view the backup path and other information.

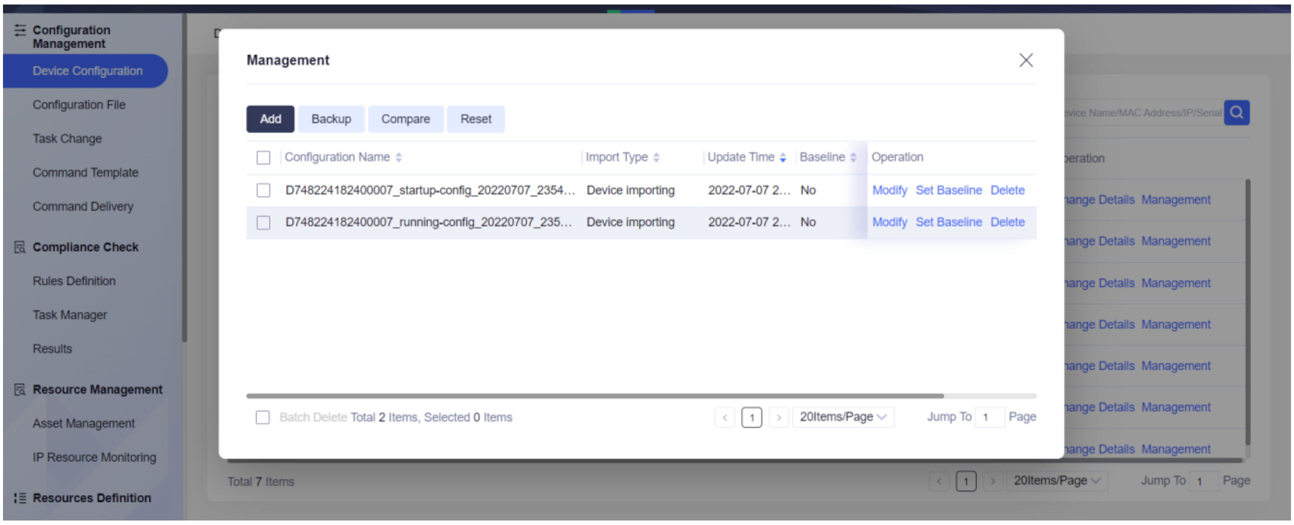


Change Content

The file is stored on the local FTP
file name:D748224182400007_startup-config_20220715_004342_385.cfg
The file is stored on the local FTP
file name:D748224182400007_running-config_20220715_004342_385.cfg

Figure 9.1.1.5 Change content

Operation > **Management** (you can quickly backup and restore devices, set baselines, modify, add, delete configuration file, reset configuration file, etc.)



Management

☐	Configuration Name	Import Type	Update Time	Baseline	Operation
☐	D748224182400007_startup-config_20220707_2354…	Device importing	2022-07-07 2…	No	Modify Set Baseline Delete
☐	D748224182400007_running-config_20220707_235…	Device importing	2022-07-07 2…	No	Modify Set Baseline Delete

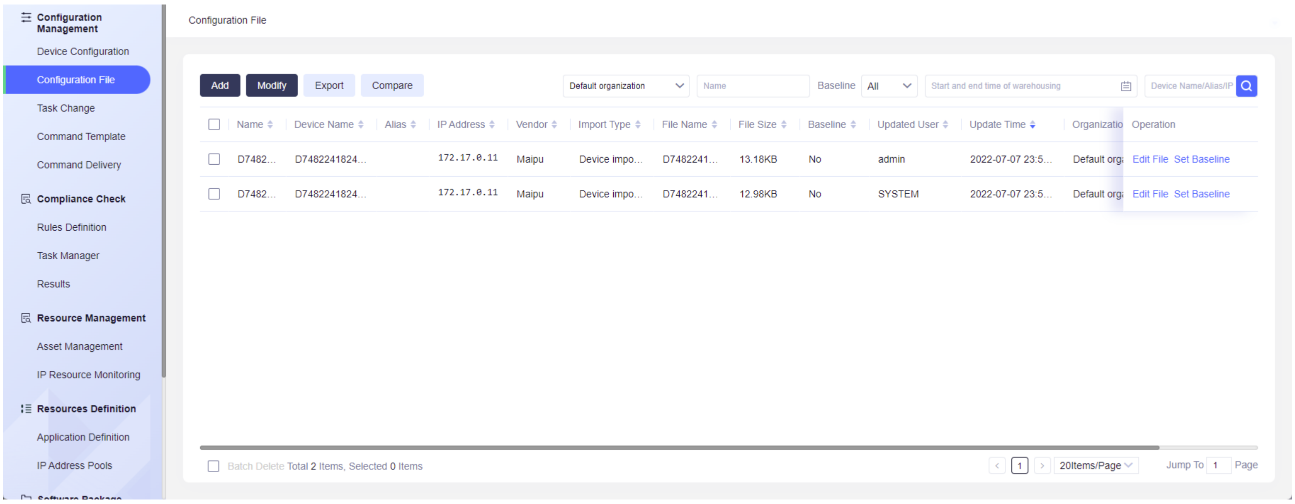
☐ Batch Delete Total 2 Items, Selected 0 Items

Figure 9.1.1.6 Change details

9.1.2 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 "Maintenance" > "Configuration Management" > "Configuration File " on the navigation bar at the top of the system to open the "Configuration File " page, as follows:



☐	Name	Device Name	Alias	IP Address	Vendor	Import Type	File Name	File Size	Baseline	Updated User	Update Time	Organizatio	Operation
☐	D7482...	D7482241824...		172.17.0.11	Maipu	Device impo...	D7482241...	13.18KB	No	admin	2022-07-07 23:5...	Default orga	Edit File Set Baseline
☐	D7482...	D7482241824...		172.17.0.11	Maipu	Device impo...	D7482241...	12.98KB	No	SYSTEM	2022-07-07 23:5...	Default orga	Edit File Set Baseline

Total 2 Items, Selected 0 Items

1 20Items/Page 1

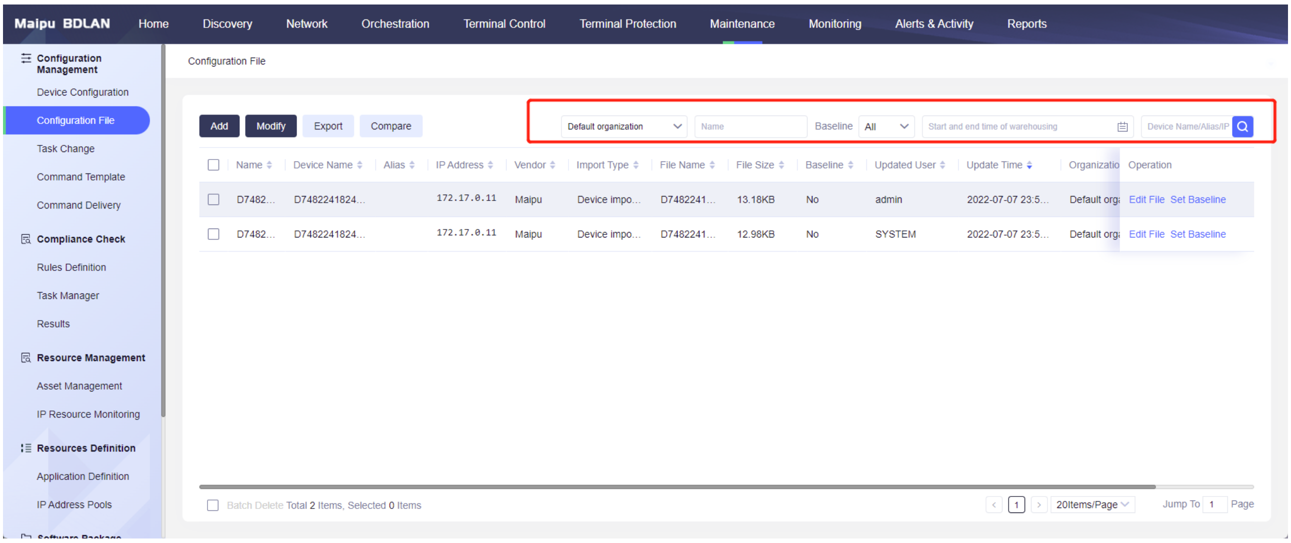
Figure 9.1.2.1 Configuration file management

Configuration file list:

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

This page provides various query criteria to query specific configuration files conveniently and quickly. Enter the corresponding query criteria in the configuration file query panel, and then click the **Query** button to query all configuration files according to the name, device (name/alias/ip), whether it is baseline, warehousing start time, warehousing end time and other fields; Click the fields in the header of the configuration file list to sort the configuration files according to the corresponding fields.

As shown in the following figure, all configuration files with the name "test" and the device IP "130.255.7.156" are found and sorted according to the names of the configuration files:



☐	Name	Device Name	Alias	IP Address	Vendor	Import Type	File Name	File Size	Baseline	Updated User	Update Time	Organizatio	Operation
☐	D7482...	D7482241824...		172.17.0.11	Maipu	Device impo...	D7482241...	13.18KB	No	admin	2022-07-07 23:5...	Default orga	Edit File Set Baseline
☐	D7482...	D7482241824...		172.17.0.11	Maipu	Device impo...	D7482241...	12.98KB	No	SYSTEM	2022-07-07 23:5...	Default orga	Edit File Set Baseline

☐ Batch Delete Total 2 Items, Selected 0 Items

Figure 9.1.2.2 Query and sort the configuration files

Caution

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

Add/Modify configuration file:

Click the **Add** button on the configuration file list panel to open the "Add" window, select the device and configuration file, and fill in the name and description of the configuration file, as shown in the following figure:

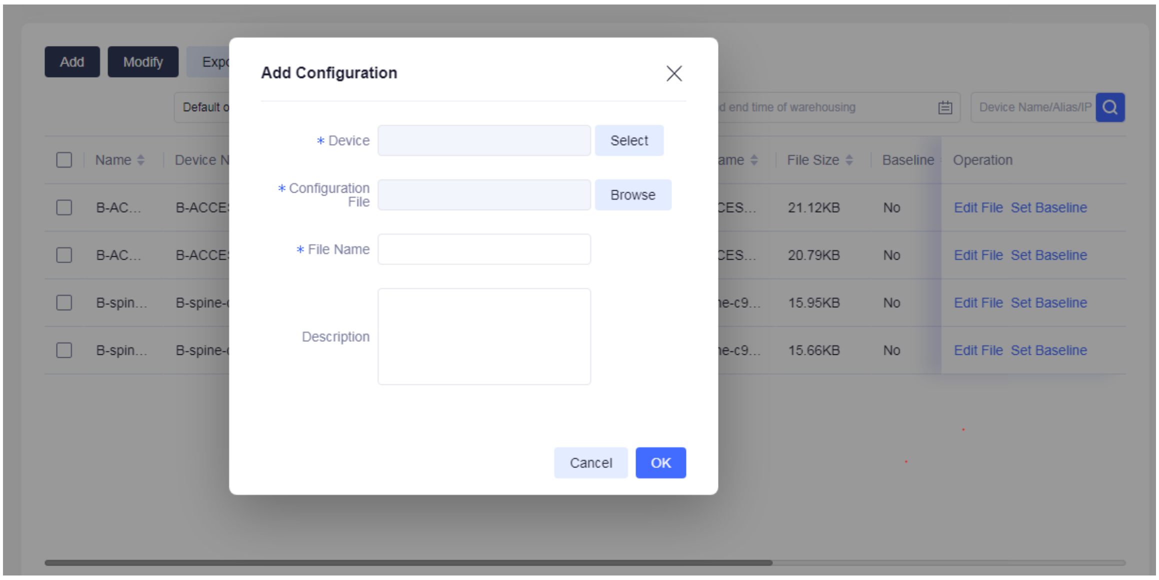


Figure 9.1.2.3 Add configuration file

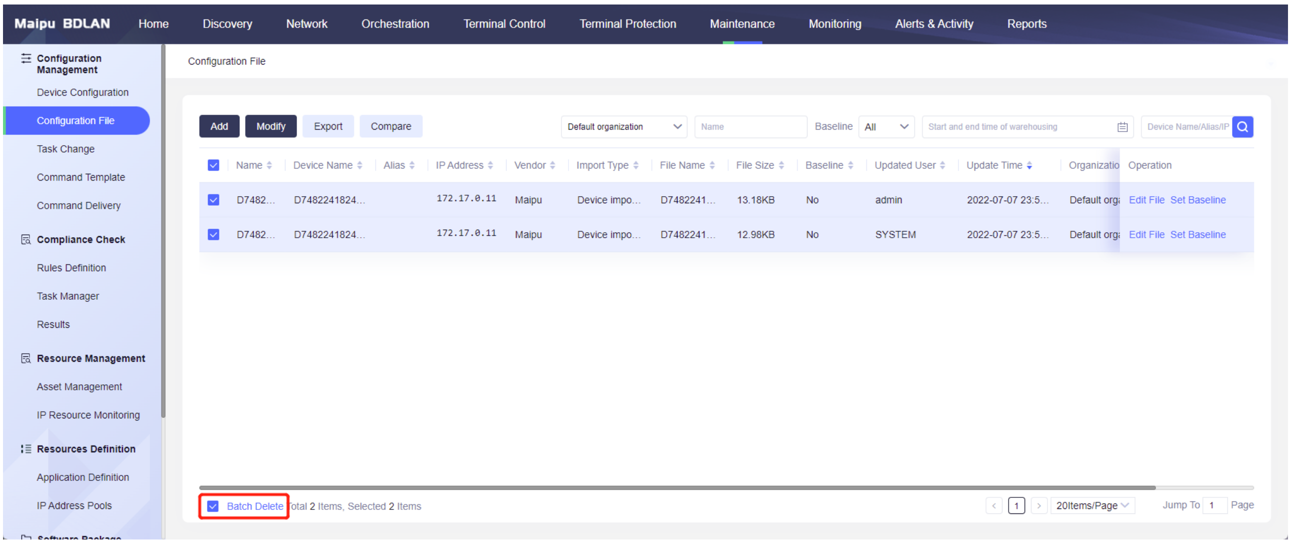
Click **OK** to add the configuration file. The process of modifying the configuration file is the same as above. Select the desired configuration file in the configuration file management list and click **Modify**.

Export configuration file:

Select the desired configuration file in the configuration file management list and click **Export**.

Delete configuration file:

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



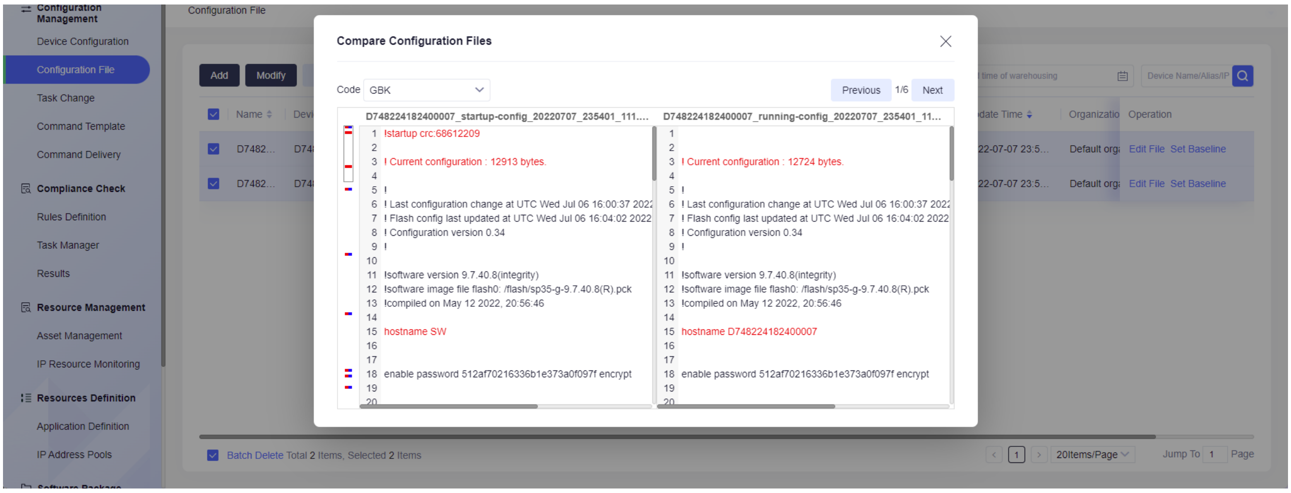
☑	Name	Device Name	Alias	IP Address	Vendor	Import Type	File Name	File Size	Baseline	Updated User	Update Time	Organizatio	Operation
☑	D7482…	D7482241824…		172.17.0.11	Maipu	Device impo…	D7482241…	13.18KB	No	admin	2022-07-07 23:5…	Default orga	Edit File Set Baseline
☑	D7482…	D7482241824…		172.17.0.11	Maipu	Device impo…	D7482241…	12.98KB	No	SYSTEM	2022-07-07 23:5…	Default orga	Edit File Set Baseline

☑ Batch Delete Total 2 Items, Selected 2 Items

Figure 9.1.2.4 Delete configuration file

Compare configuration file:

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



D748224182400007_startup-config_20220707_235401_111....

```
!startup crc:68612209

! Current configuration : 12913 bytes.

!
! Last configuration change at UTC Wed Jul 06 16:00:37 2022
! Flash config last updated at UTC Wed Jul 06 16:04:02 2022
! Configuration version 0.34
!

!software version 9.7.40.8(integrity)
!software image file flash0: /flash/sp35-g-9.7.40.8(R).pck
!compiled on May 12 2022, 20:56:46

hostname SW


enable password 512af70216336b1e373a0f097f encrypt
```

D748224182400007_running-config_20220707_235401_11...

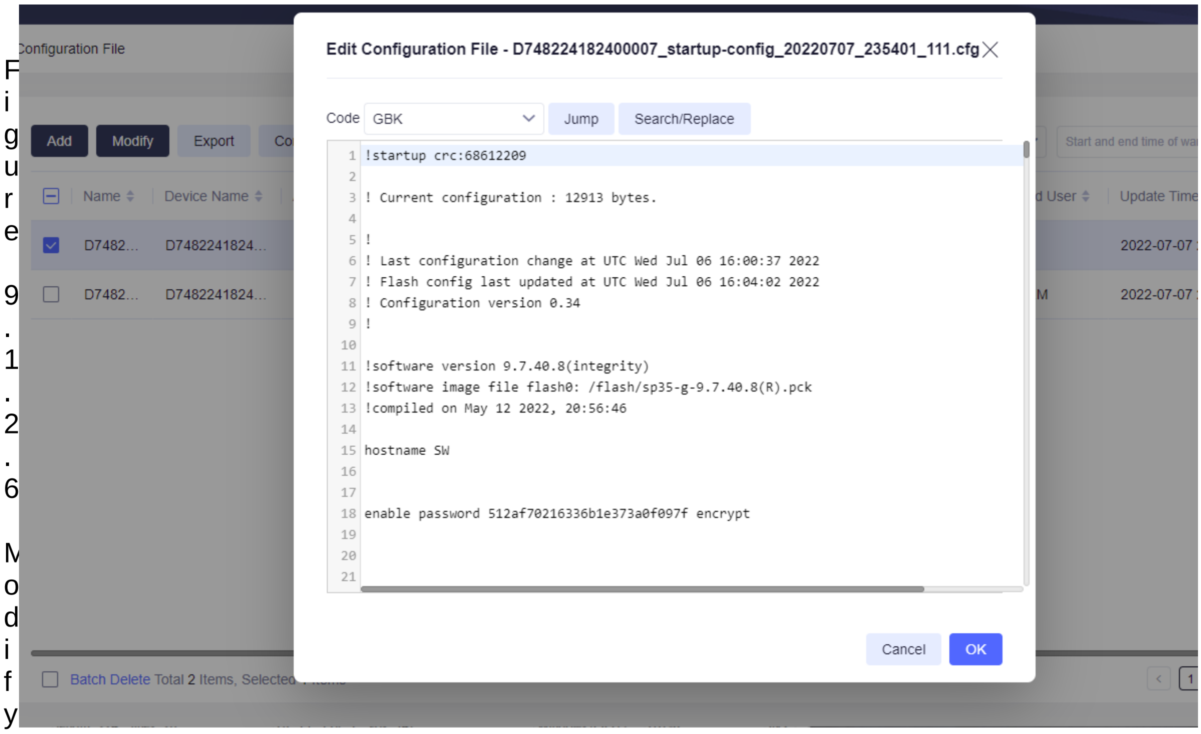
```


! Current configuration : 12724 bytes.

!
! Last configuration change at UTC Wed Jul 06 16:00:37 2022
! Flash config last updated at UTC Wed Jul 06 16:04:02 2022
! Configuration version 0.34
!

!software version 9.7.40.8(integrity)
!software image file flash0: /flash/sp35-g-9.7.40.8(R).pck
!compiled on May 12 2022, 20:56:46

hostname D748224182400007


enable password 512af70216336b1e373a0f097f encrypt
```

☑ Batch Delete Total 2 Items, Selected 2 Items

Figure 9.1.2.5 Compare configuration files

Modify configuration file:

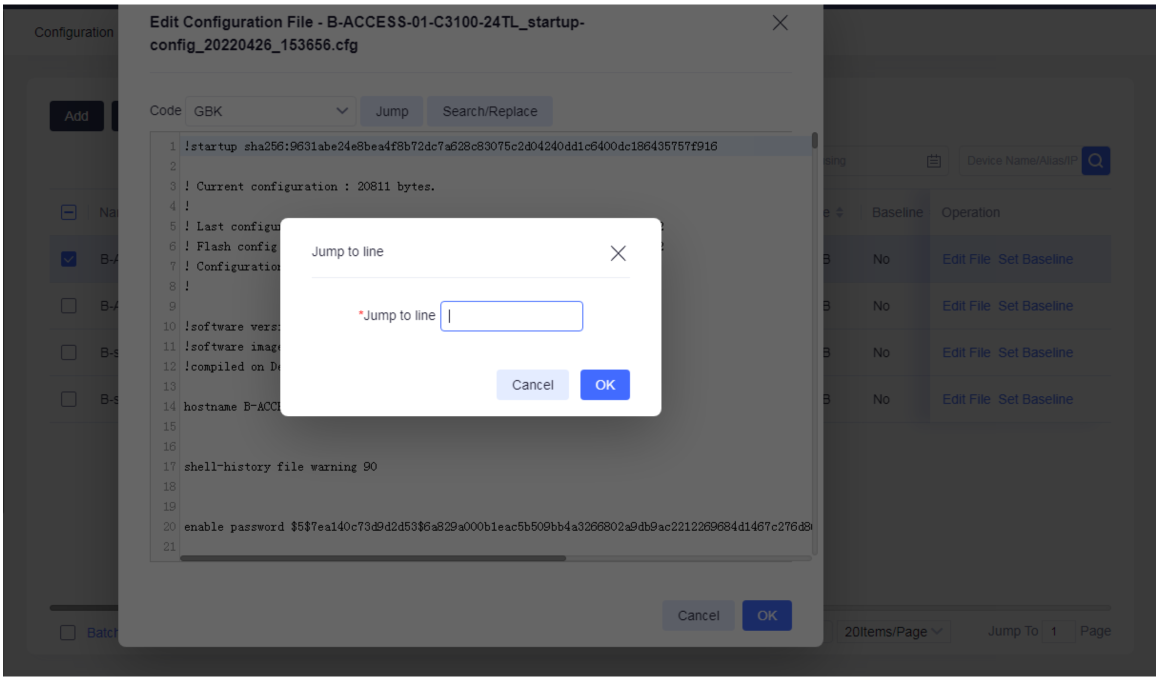
Select the desired configuration file in the configuration file list, and click the **Edit** button. You can enter the **Edit Configuration File** page, as shown in the following figure:



```
!startup crc:68612209

! Current configuration : 12913 bytes.

!
! Last configuration change at UTC Wed Jul 06 16:00:37 2022
! Flash config last updated at UTC Wed Jul 06 16:04:02 2022
! Configuration version 0.34
!

!software version 9.7.40.8(integrity)
!software image file flash0: /flash/sp35-g-9.7.40.8(R).pck
!compiled on May 12 2022, 20:56:46

hostname SW


enable password 512af70216336b1e373a0f097f encrypt


```

Figure 9.1.2.6 Modify configuration file

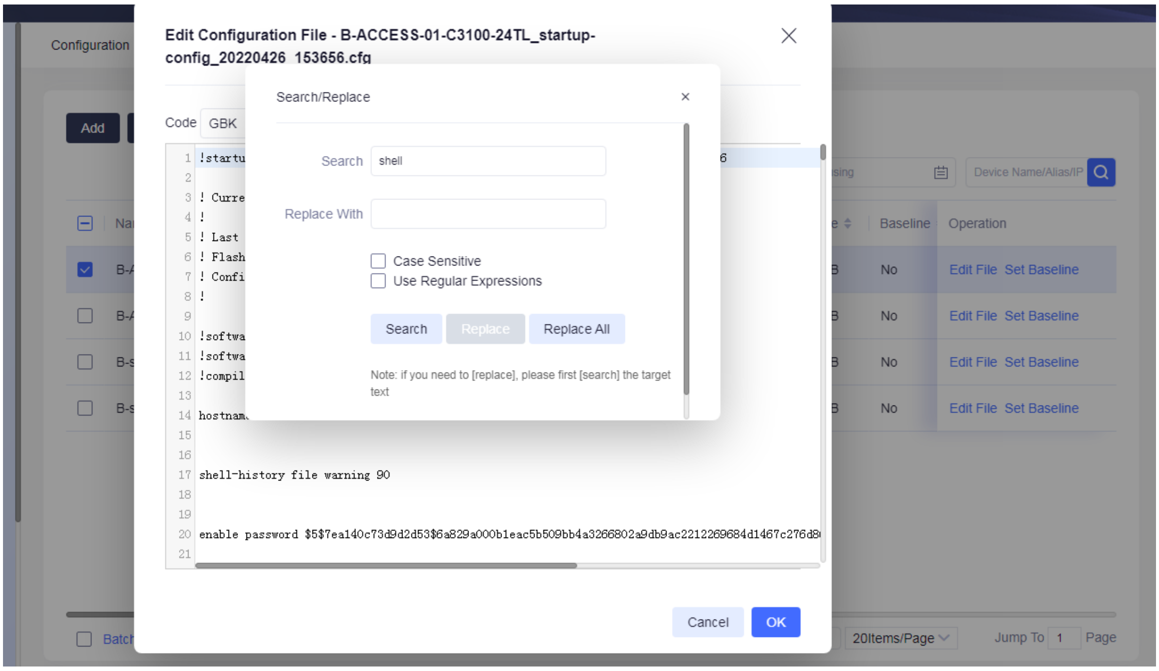
Click the "Jump" button to jump to the corresponding configuration line, as shown in the following figure.



```
!startup sha256:9631abe24e8bea4f8b72dc7a628c83075c2d04240dd1c6400dc186435757f916

! Current configuration : 20811 bytes.
!
! Last configu
! Flash config
! Configuratio
!

!software vers
!software image
!compiled on De

hostname B-ACCE


shell-history file warning 90


enable password $5$7ea140c73d9d2d53$6a829a000b1eac5b509bb4a3266802a9db9ac2212269684d1467c276d8

```

Figure 9.1.2.7 Jump to the specified line

Click the **Search/Replace** button to find and replace the configuration file. At the same time, you can select whether to distinguish cases and whether to use regular expression, as shown in the following figure:

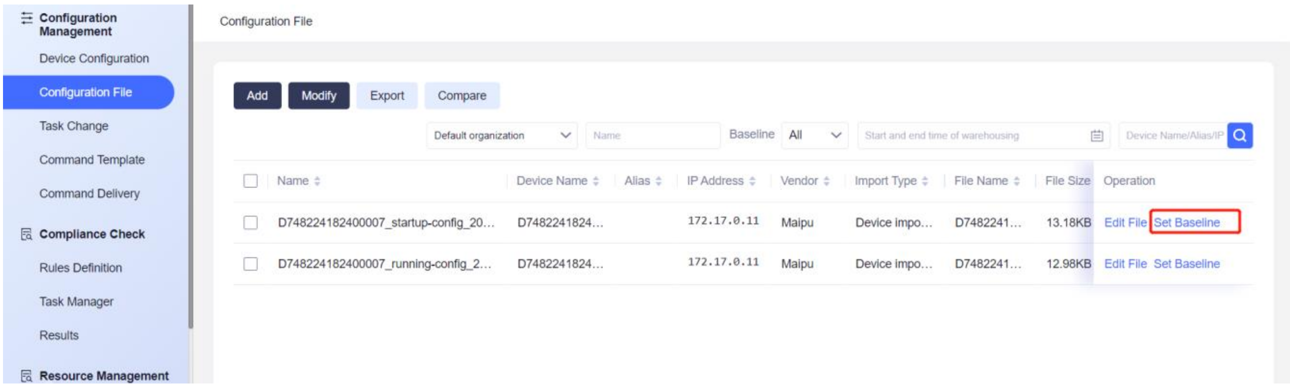


```
!startu

! Curre
!
! Last
! Flash
! Confi
!

!softwa
!softwa
!compil

hostnam


shell-history file warning 90


enable password $5$7ea140c73d9d2d53$6a829a000b1eac5b509bb4a3266802a9db9ac2212269684d1467c276d8
```

Figure 9.1.2.8 Search/replace configuration files

Set baseline:

Select the desired configuration file in the configuration file list, and click the **Set Baseline** button. You can set the file as the baseline file, as shown in the following figure:

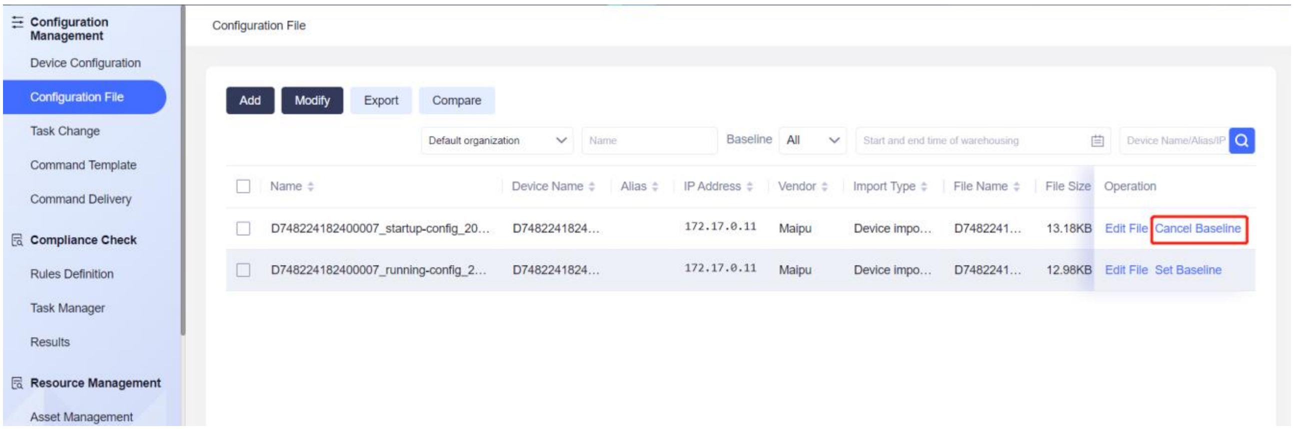


☐	Name	Device Name	Alias	IP Address	Vendor	Import Type	File Name	File Size	Operation
☐	D748224182400007_startup-config_20…	D7482241824…		172.17.0.11	Maipu	Device impo…	D7482241…	13.18KB	Edit File Set Baseline
☐	D748224182400007_running-config_2…	D7482241824…		172.17.0.11	Maipu	Device impo…	D7482241…	12.98KB	Edit File Set Baseline

Figure 9.1.2.9 Set the file as the baseline

Cancel baseline

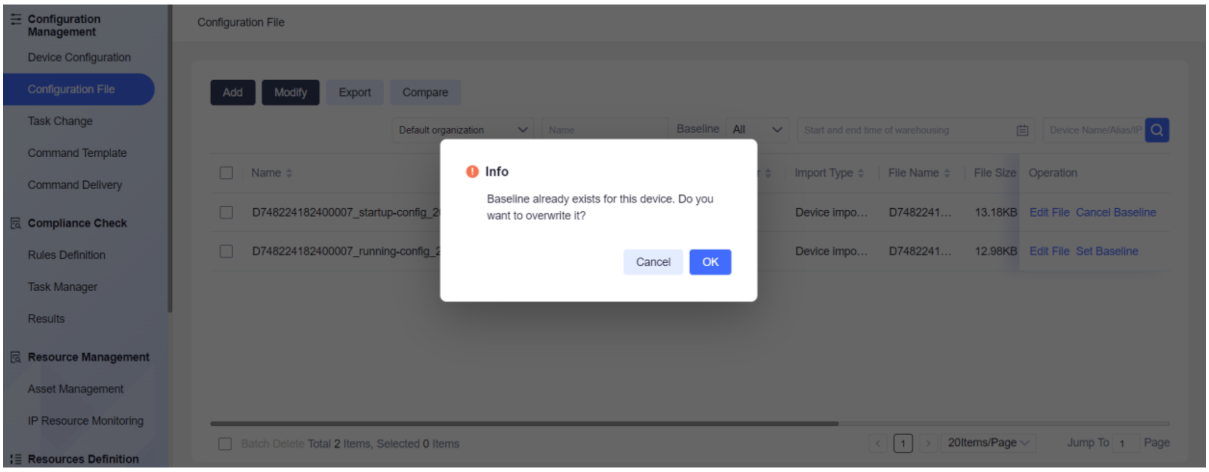
Select the desired configuration file in the configuration file list, and click the **Cancel Baseline** button, as shown in the following figure:



☐	Name	Device Name	Alias	IP Address	Vendor	Import Type	File Name	File Size	Operation
☐	D748224182400007_startup-config_20…	D7482241824…		172.17.0.11	Maipu	Device impo…	D7482241…	13.18KB	Edit File Cancel Baseline
☐	D748224182400007_running-config_2…	D7482241824…		172.17.0.11	Maipu	Device impo…	D7482241…	12.98KB	Edit File Set Baseline

Figure 9.1.2.10 Cancel baseline

A device can only have one baseline file. If a baseline file already exists for the device, a prompt will be given for repeated settings, as shown in the following figure:



Info

Baseline already exists for this device. Do you want to overwrite it?

Name	Import Type	File Name	File Size	Operation
D748224182400007_startup-config_2	Device impo…	D7482241…	13.18KB	Edit File Cancel Baseline
D748224182400007_running-config_2	Device impo…	D7482241…	12.98KB	Edit File Set Baseline

Batch Delete Total 2 Items, Selected 0 Items

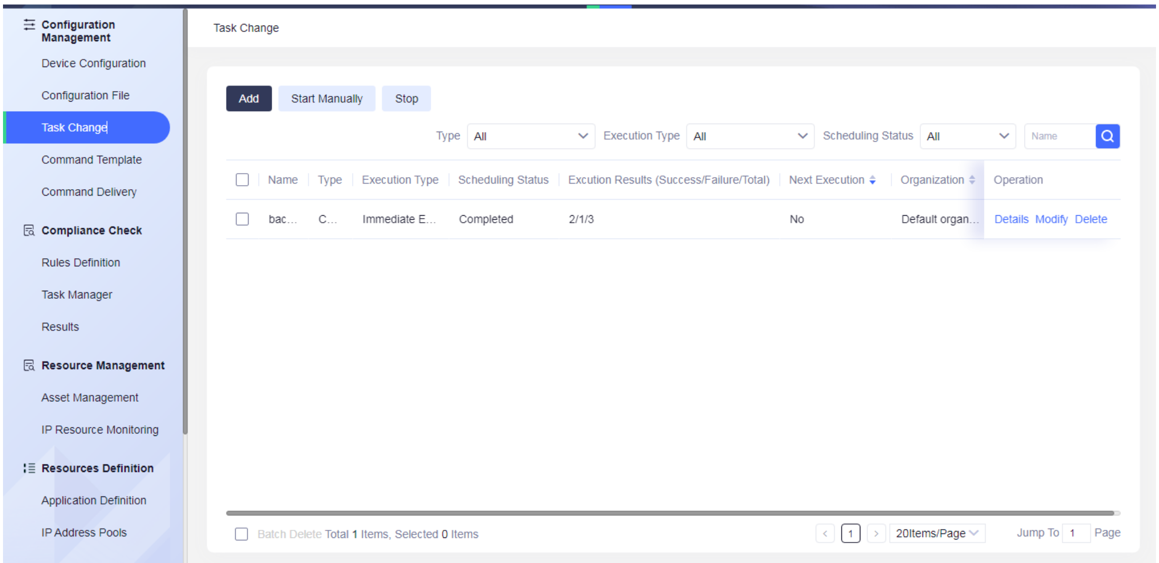
Figure 9.1.2.11 Set baseline repeatedly

Click **OK** to overwrite the previous set baseline. Click **Cancel** to not overwrite it.

9.1.3 Configuration Change Task

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

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



Name	Type	Execution Type	Scheduling Status	Excution Results (Success/Failure/Total)	Next Execution	Organization	Operation
bac…	C…	Immediate E…	Completed	2/1/3	No	Default organ…	Details Modify Delete

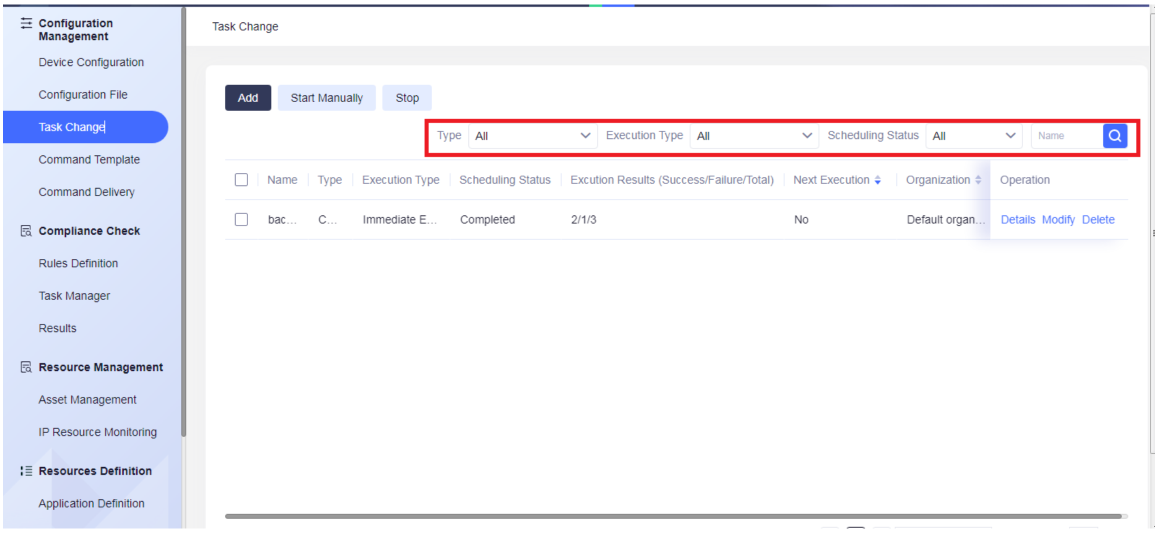
Batch Delete Total 1 Items, Selected 0 Items

Figure 9.1.3.1 Configuration change task management

Task list:

Open the "Task Change" interface to display all configuration change tasks in the system in pages by default, showing the name, type, scheduling type, scheduling status, scheduling result, next start time, organization, operation and other information of each task.

This page provides various query criteria to query specific tasks conveniently and quickly. Enter the corresponding query criteria, and then click **Query** to query all tasks by name, type, scheduling type, scheduling status and other fields; You can click the "Organization" in the header of the task list and the next scheduling time field to sort;



Type: All | Execution Type: All | Scheduling Status: All

☐	Name	Type	Execution Type	Scheduling Status	Excution Results (Success/Failure/Total)	Next Execution	Organization	Operation
☐	bac...	C...	Immediate E...	Completed	2/1/3	No	Default organ...	Details Modify Delete

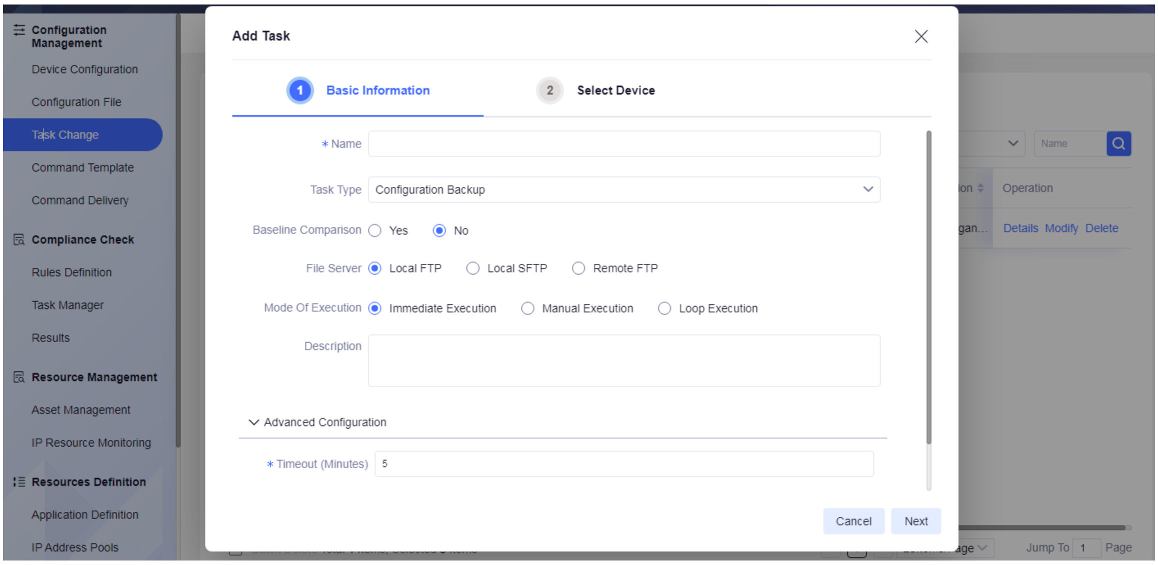
Figure 9.1.3.2 Query configuration change task

Caution

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

Add/modify a configuration backup task:

Click the **Add** button on the task panel to open the "Add" window, as shown in the following figure. Fill in the task name, select the task type, baseline comparison, file server, execution mode and description. Select the **Advanced Configuration** option, and you can set the timeout parameter and whether to support VRF.



* Name
Task Type: Configuration Backup
Baseline Comparison: ○ Yes ● No
File Server: ● Local FTP ○ Local SFTP ○ Remote FTP
Mode Of Execution: ● Immediate Execution ○ Manual Execution ○ Loop Execution
Description
* Timeout (Minutes): 5

Figure 9.1.3.3 Step 1 of adding configuration backup task

Caution

- The device concurrency of the current single task in the configuration change task is 10, and the task concurrency is 3

- Default timeout is 5 minutes
- Do not support VRF by default.

Baseline comparison: only tasks whose type is "Configuration Backup" can have the baseline comparison option; Select "Yes". If the device has not set a baseline file, the backup startup file will be automatically set as the baseline file. If the device has set a baseline file, the backup startup file and the baseline file will be used for comparison. If they are different from the baseline file, an alarm will be sent; Select **No** to neither compare with the baseline file nor set the backup startup file as the baseline file.

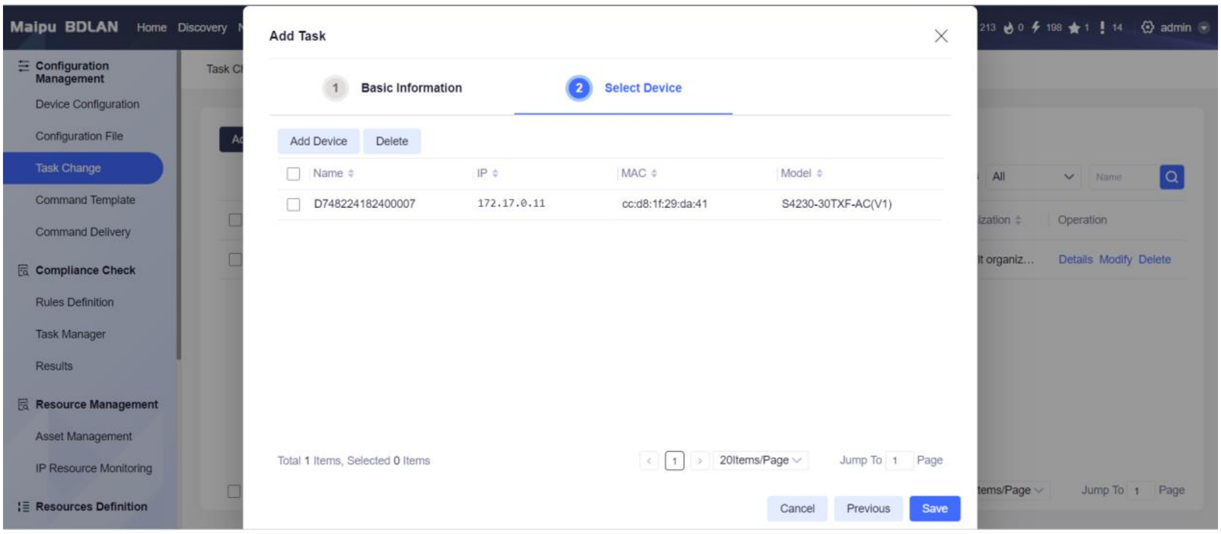
File server: Configuration change uses the FTP server for file transfer by default. FTP has a default password. Users do not need to enter the FTP password (if necessary, the FTP password can be modified). You can also use a remote FTP server for upgrading. When selecting a remote FTP server, you need to enter the FTP address, user name and password.

Execution mode: When **Immediate Execution** is selected, the task can be executed immediately after the task information is configured; Select **Manual Execution** to execute the task after the set time period; Select **Loop Execution** to start execution in a fixed time period within a fixed time period.

Timeout: when a task is executed, the task execution fails when the response time of the device exceeds the set timeout.

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

Click **Next** to enter the "Select Device" window, as shown in the following figure

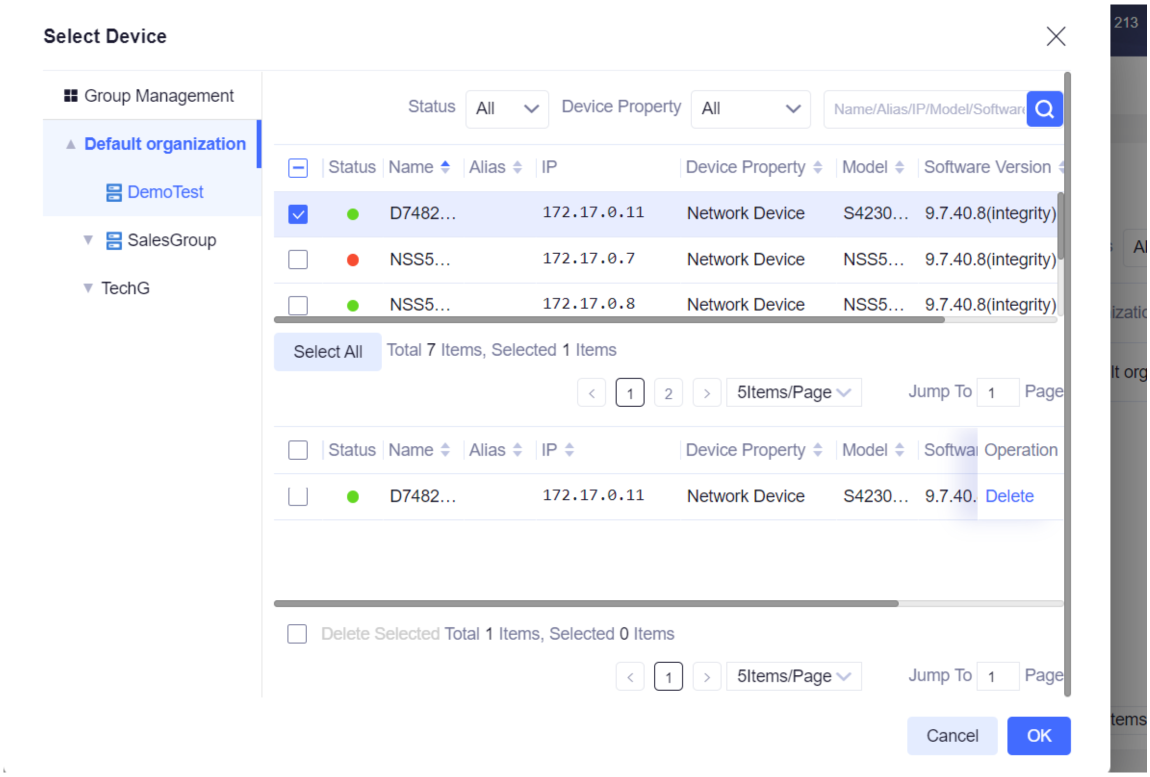


☐	Name	IP	MAC	Model
☐	D748224182400007	172.17.0.11	cc:d8:1f:29:da:41	S4230-30TXF-AC(V1)

Total 1 Items, Selected 0 Items 1 20Items/Page Jump To 1 Page

Figure 9.1.3.4 Step 2 of adding configuration backup task

Click "Add Device", support multiple choices. Select the corresponding device for the task and enter the "Select Device" window, as shown in the following figure

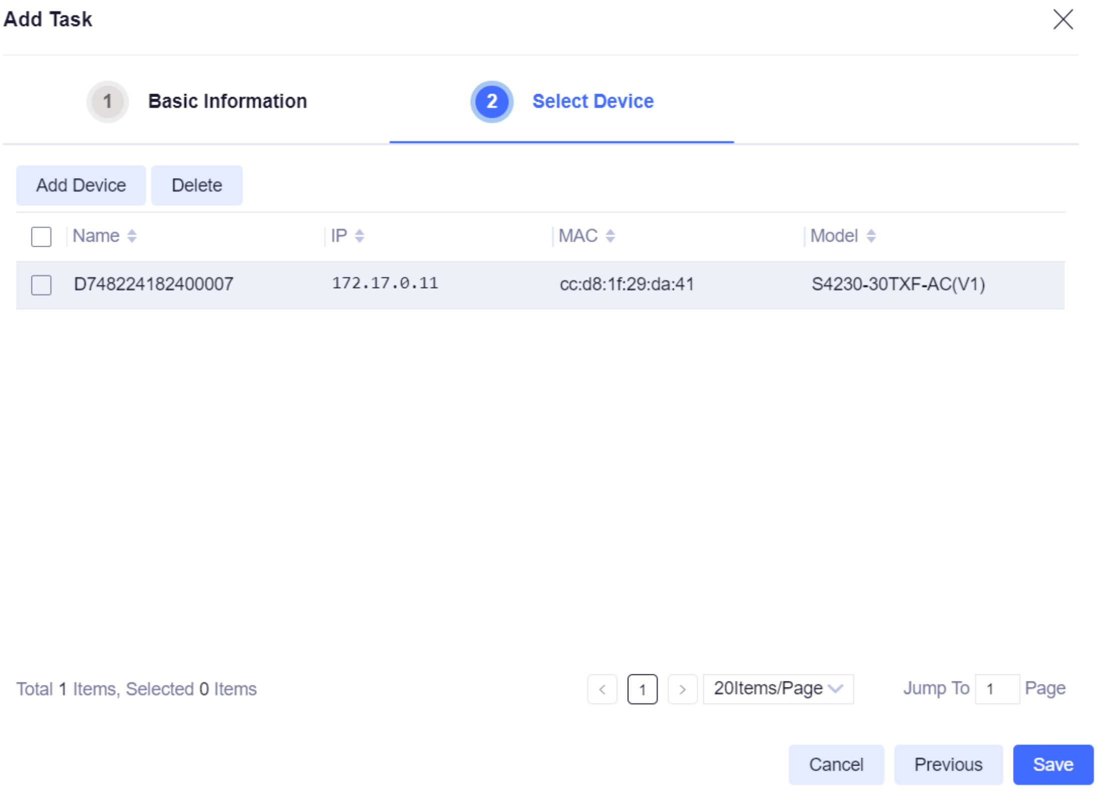


	Status	Name	Alias	IP	Device Property	Model	Software Version
☑	●	D7482…		172.17.0.11	Network Device	S4230…	9.7.40.8(integrity)
☐	●	NSS5…		172.17.0.7	Network Device	NSS5…	9.7.40.8(integrity)
☐	●	NSS5…		172.17.0.8	Network Device	NSS5…	9.7.40.8(integrity)

	Status	Name	Alias	IP	Device Property	Model	Softwa	Operation
☐	●	D7482…		172.17.0.11	Network Device	S4230…	9.7.40.	Delete

Figure 9.1.3.5 Select devices

Select a device and click **OK** to select a device for the configuration backup task, as shown in the following figure:



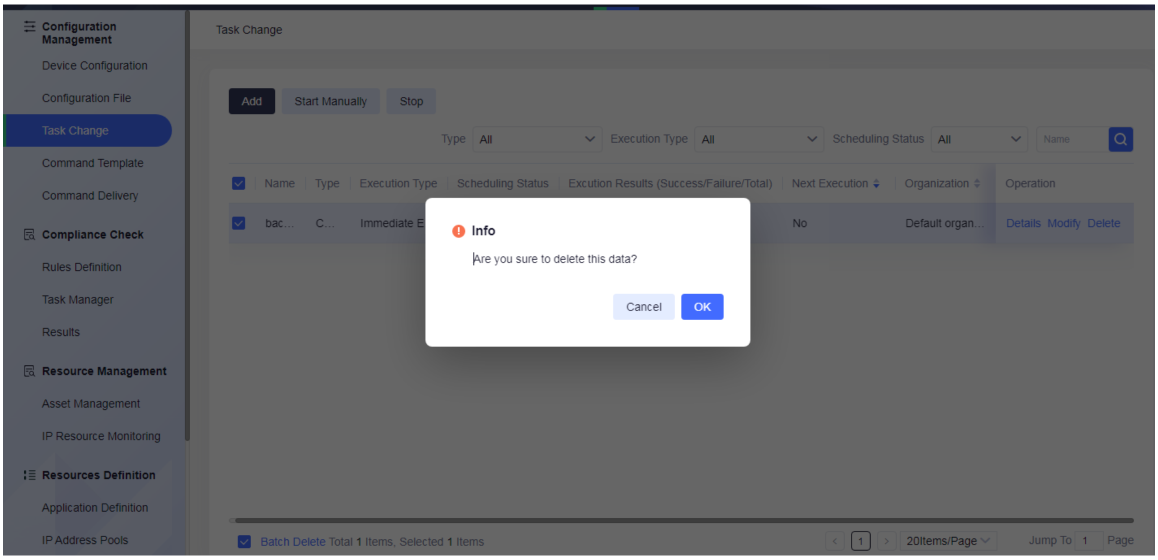
	Name	IP	MAC	Model
☐	D748224182400007	172.17.0.11	cc:d8:1f:29:da:41	S4230-30TXF-AC(V1)

Figure 9.1.3.6 Last step of adding the configuration backup task

Click the **Save** button, add the configuration backup task, and the device starts the configuration backup task. The process of modification task is the same as above. Select the desired task in the task list and click **Modify**.

Delete task:

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



Info

Are you sure to delete this data?

Batch Delete Total 1 Items, Selected 1 Items

Figure 9.1.3.12 Delete the task information

Note

- Tasks in progress cannot be deleted or modified.

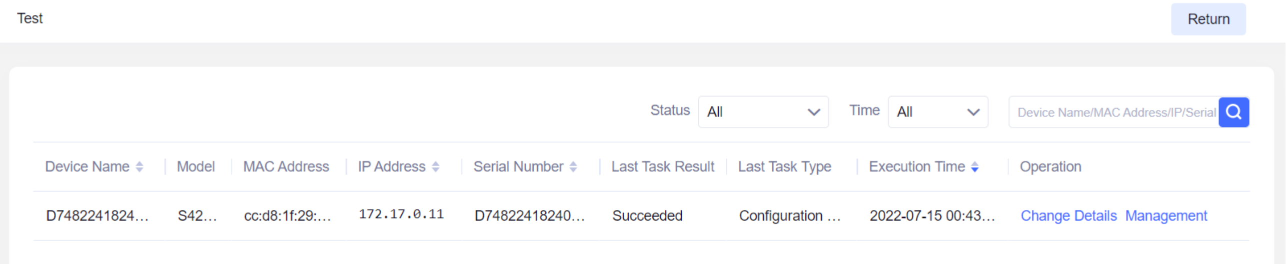
Manually start/stop task:

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

Select a stopped task and click the **Start Manually** button. The task can start running again from the beginning. At this time, the status of the task will change to "In progress".

View task details:

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



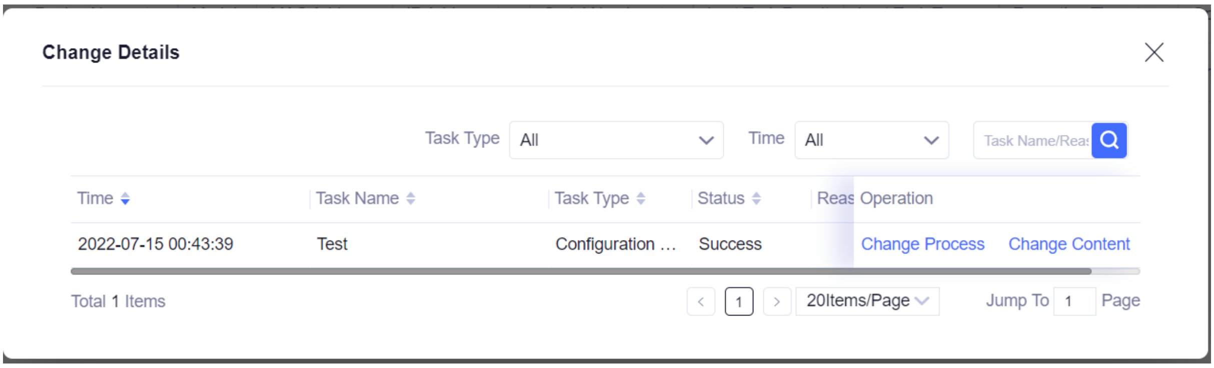
Status: All | Time: All

Device Name	Model	MAC Address	IP Address	Serial Number	Last Task Result	Last Task Type	Execution Time	Operation
D7482241824…	S42…	cc:d8:1f:29:…	172.17.0.11	D74822418240…	Succeeded	Configuration …	2022-07-15 00:43…	Change Details Management

Figure 9.1.3.13 Task details

The "Change Details" interface displays different devices under the same task in pages, showing the device name, model, MAC, IP, serial number, latest change status, latest change task type, change time, operation and other information of the device configuration.

Click **Details** of any configuration task in the change details list to open the "Change Details" window of the device, showing the detailed process of configuration file backup, as shown below:



Change Details

Task Type: All　Time: All　Task Name/Reas

Time	Task Name	Task Type	Status	Reas	Operation
2022-07-15 00:43:39	Test	Configuration ...	Success		Change Process Change Content

Total 1 Items　1　20Items/Page　Jump To 1 Page

Figure 9.1.3.14 Execution details of configuration backup

The cases that the task execution may fail:

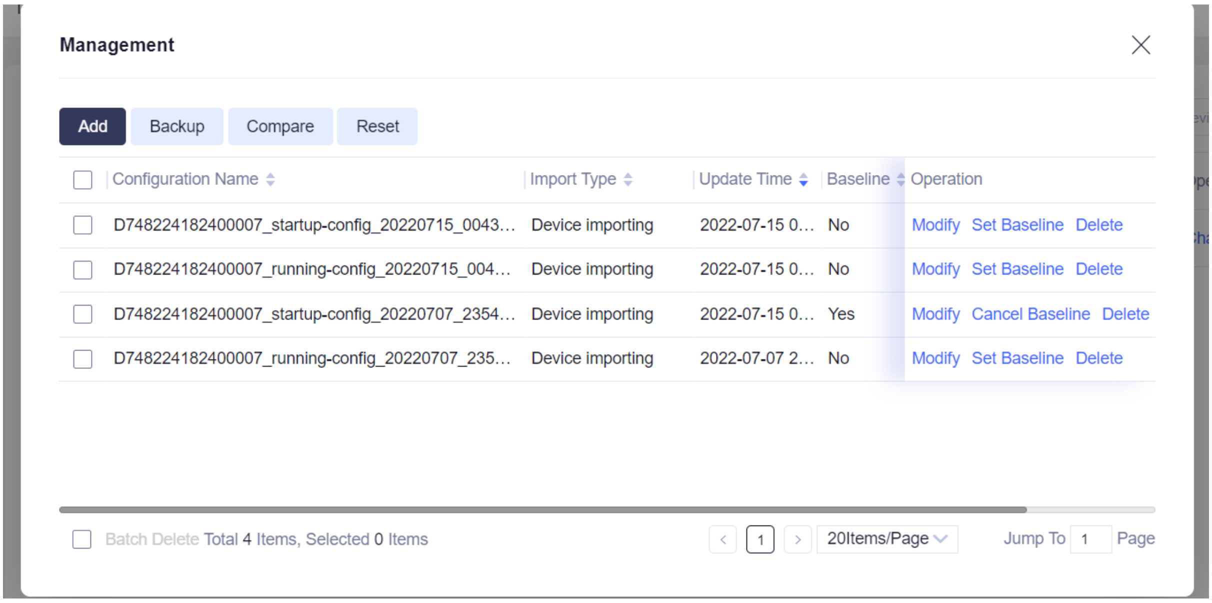
Note

- Task execution failed. **connect/transfer timeout** is reported in the details
- Cause: When a device is found, it is found through the device management address that the management address of the network management server and the device is reachable, but it is not reachable with the default routing egress interface address of the device. The task selects FTP and SFTP servers. When the device downloads a file as a client, it communicates through the default routing egress interface address, and the file transmission will fail.
- Judgment method: log in to the device and ping the address of the network management server on the device. The Ping fails; The ping can succeed when the management address serves as the source address
- Solution: specify the source address of ftp/sftp transmission on the device as the address accessible to the network management server. For example, configure the following commands 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
```

The "Management" interface also provides the operations such as backup, comparison, adding, editing, recovery, baseline setting and deleting of configuration files, as shown in the figure



☐	Configuration Name	Import Type	Update Time	Baseline	Operation
☐	D748224182400007_startup-config_20220715_0043…	Device importing	2022-07-15 0…	No	Modify Set Baseline Delete
☐	D748224182400007_running-config_20220715_004…	Device importing	2022-07-15 0…	No	Modify Set Baseline Delete
☐	D748224182400007_startup-config_20220707_2354…	Device importing	2022-07-15 0…	Yes	Modify Cancel Baseline Delete
☐	D748224182400007_running-config_20220707_235…	Device importing	2022-07-07 2…	No	Modify Set Baseline Delete

☐ Batch Delete Total 4 Items, Selected 0 Items

Figure 9.1.3.15 Management

9.1.4 Command Template Management

The command template management module provides management of the configuration command templates delivered to the device, including adding, importing, modifying, deleting command templates, and querying command templates.

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

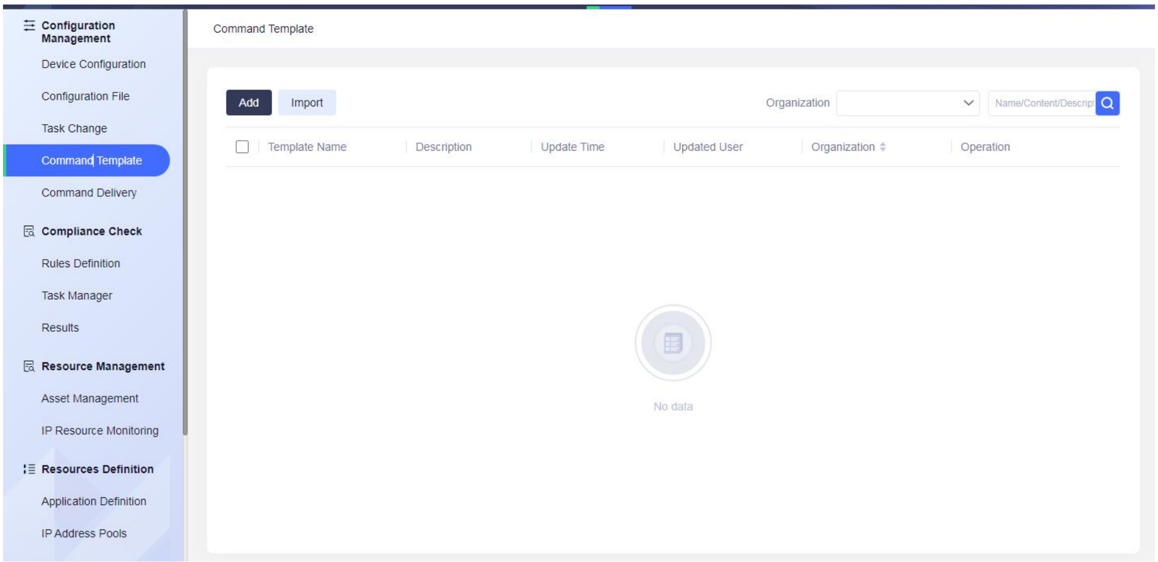


Figure 9.1.4.1 Command template management

List of command templates:

Open the "Command Template " interface to display all command templates in the system by default in pages, showing the name, description, update time, update user, organization, view content and other information of each command template by column; This page provides various query criteria to query specific command templates conveniently and quickly.

In the command template query panel, you can query the corresponding template according to the organization and advanced query. In advanced query, you can query according to the template name, content and description; Enter the corresponding query criteria, and then click **Query** to find the matching template; Click each field in the header of the command template list to sort the command templates according to the corresponding fields.

As shown in the following figure, the command template whose organization is "default organization" and advanced query is "test" is found:

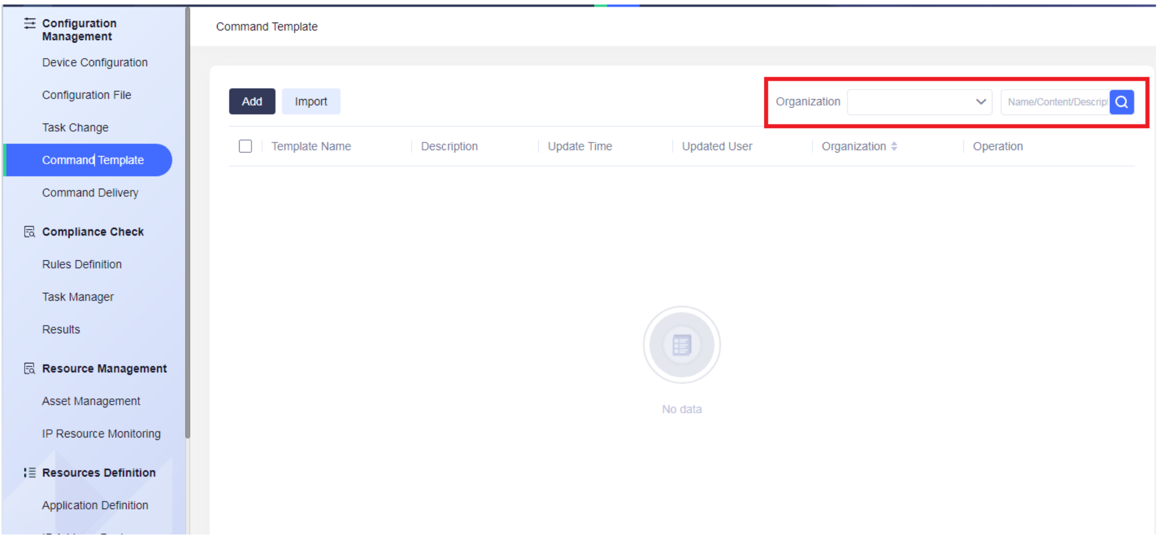


Figure 9.1.4.2 Query command template

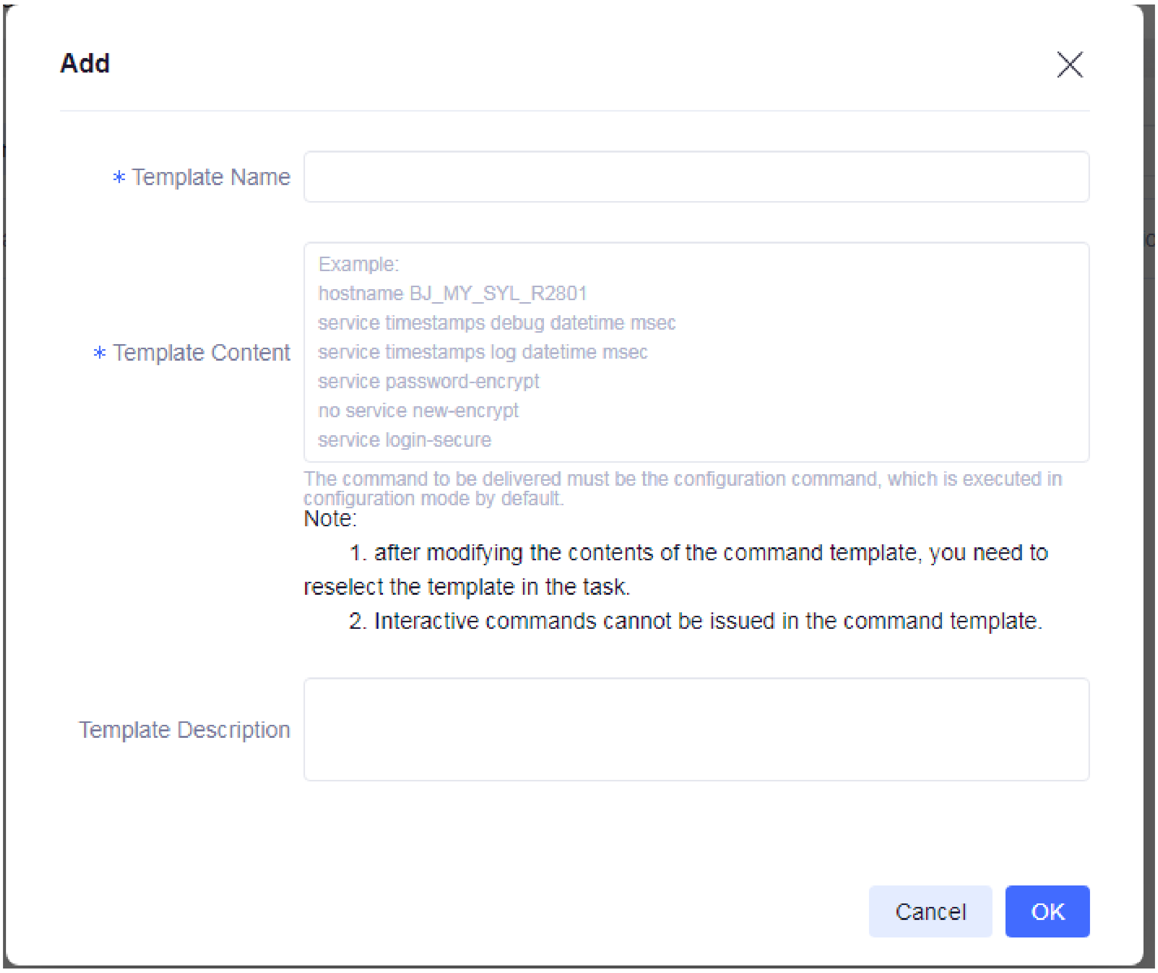
Caution

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

---

Add command template:

Click the **Add** button on 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:



```
Example:
hostname BJ_MY_SYL_R2801
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encrypt
no service new-encrypt
service login-secure
```

The command to be delivered must be the configuration command, which is executed in configuration mode by default.

Note:

1. after modifying the contents of the command template, you need to reselect the template in the task.
2. Interactive commands cannot be issued in the command template.

Figure 9. 1.4.3 Add command template

Click **OK** to add the command template. The process of modifying a command template is the same as above. Select a desired command template in the command template management list and click **Modify**.

Caution

- The command to be issued must be a configuration command, which will be executed in the configuration mode by default
- After modifying the command template, you need to re-select the template in the task

Import command template:

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

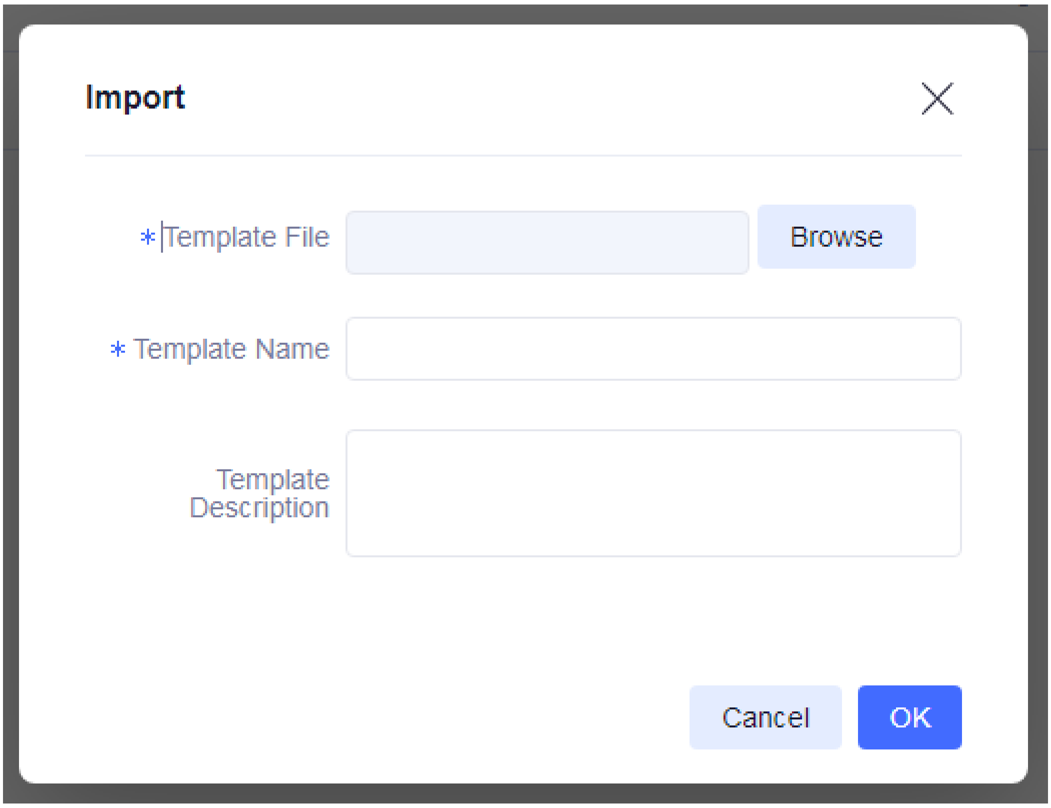
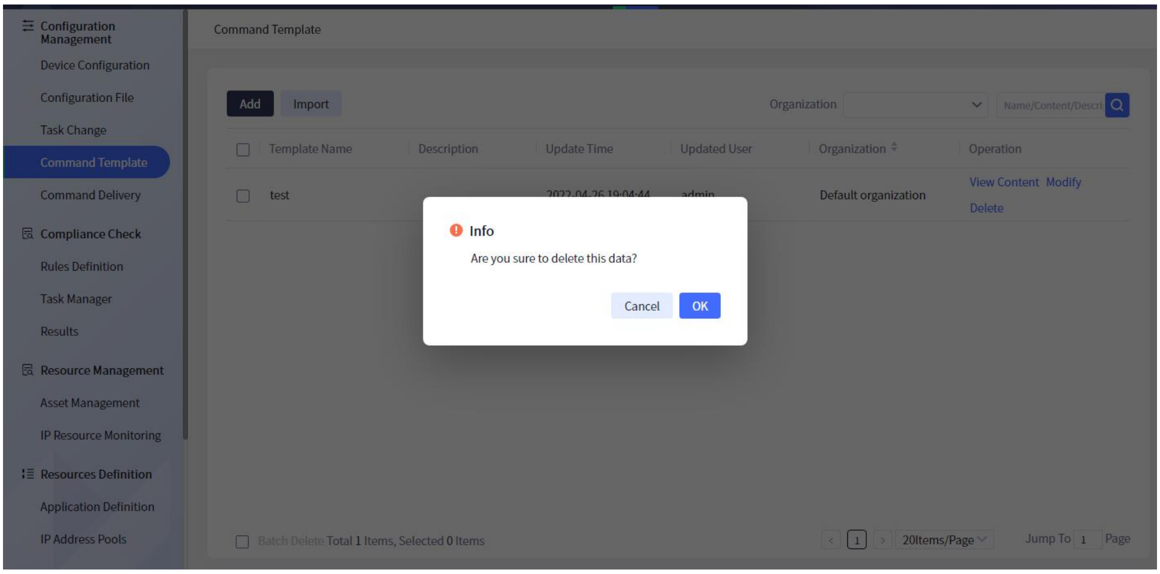


Figure 9. 1.4.4 Import the command template

Click **OK** to finish importing the command template.

Delete a command template:

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



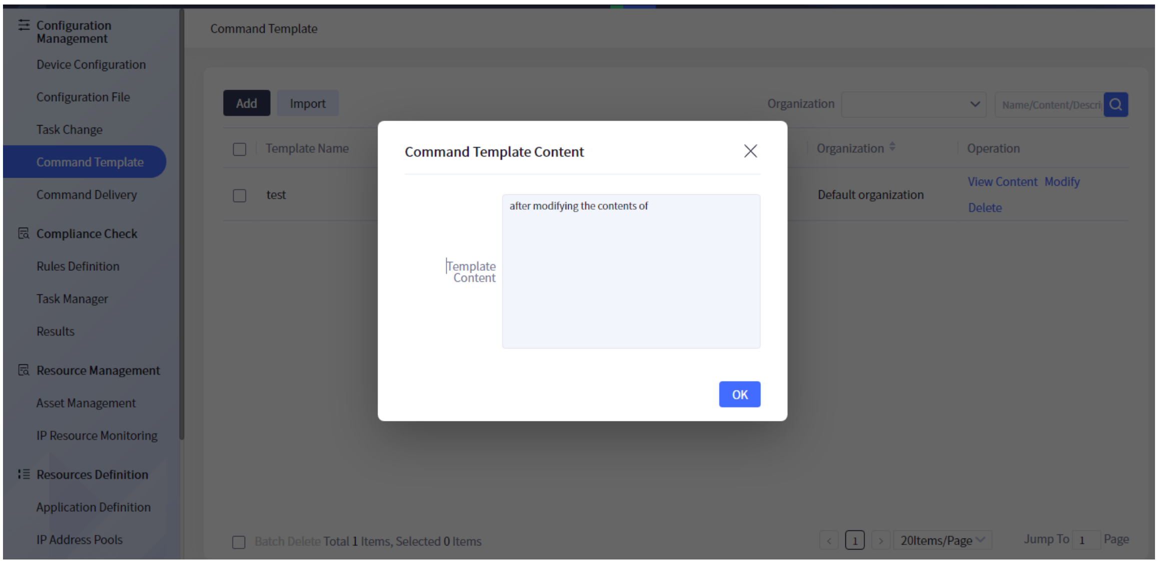
☐	Template Name	Description	Update Time	Updated User	Organization	Operation
☐	test		2022-04-26 19:04:44	admin	Default organization	View Content Modify Delete

Total 1 Items, Selected 0 Items

Info

Are you sure to delete this data?

Figure 9. 1.4.5 Delete the command template



Template Content: after modifying the contents of

Template Name	Organization	Operation
test	Default organization	View Content Modify Delete

Total 1 Items, Selected 0 Items

Figure 9. 1.4.6 View command template

9.1.5 Command Delivery Task

The command delivery task management module can issue configuration commands to the specified devices, including the addition, modification, deletion, manual start, stop, refresh and other operations of the configuration command delivery task, as well as the query of the command delivery task.

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

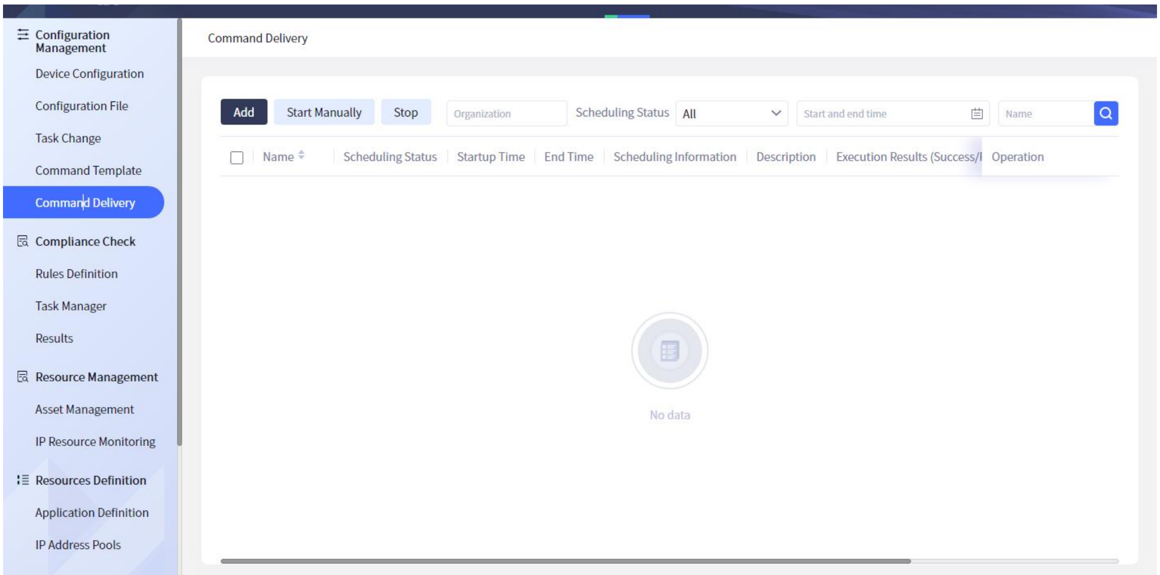


Figure 9. 1.5.1 Command delivery task management

Task list:

Open the "Command Delivery" interface to display all the tasks in the system in pages by default, showing the name, status, last start time, last end time, scheduling information, description, recent execution, update user, organization and operation of each task by column.

This page provides various query criteria to query specific tasks conveniently and quickly. Enter the corresponding query criteria, and then click **Query** to query all tasks by name, organization, status, start time, end time and other fields; Click the "Organization" and name fields at the head of the task list to sort by organization and name.

As shown in the following figure, all tasks with the name of "test" and the organization of "default organization" are found:

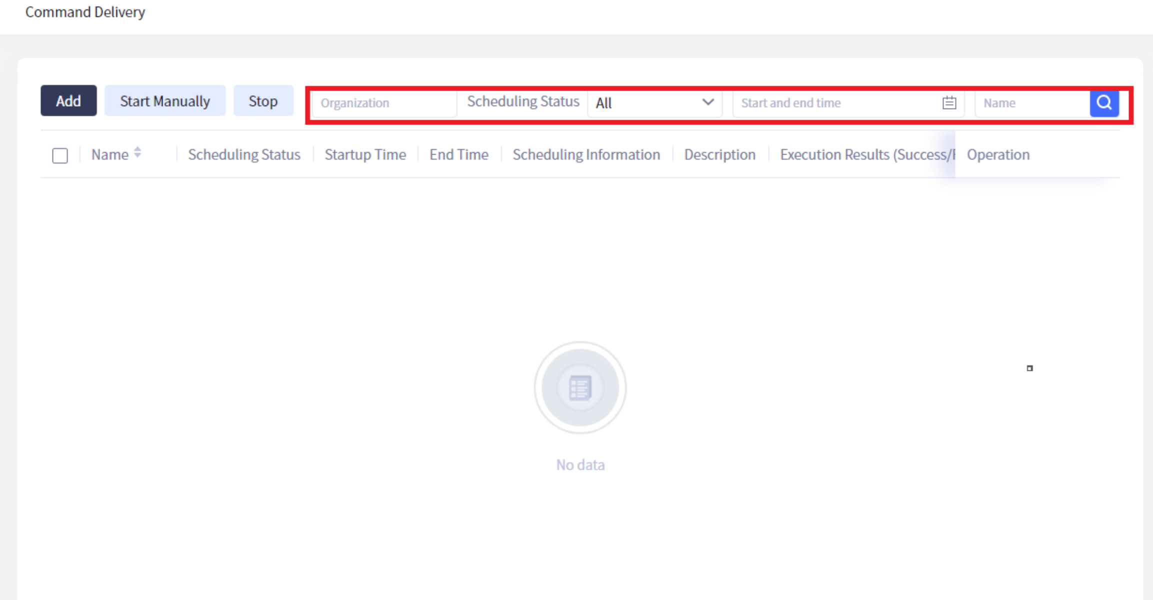


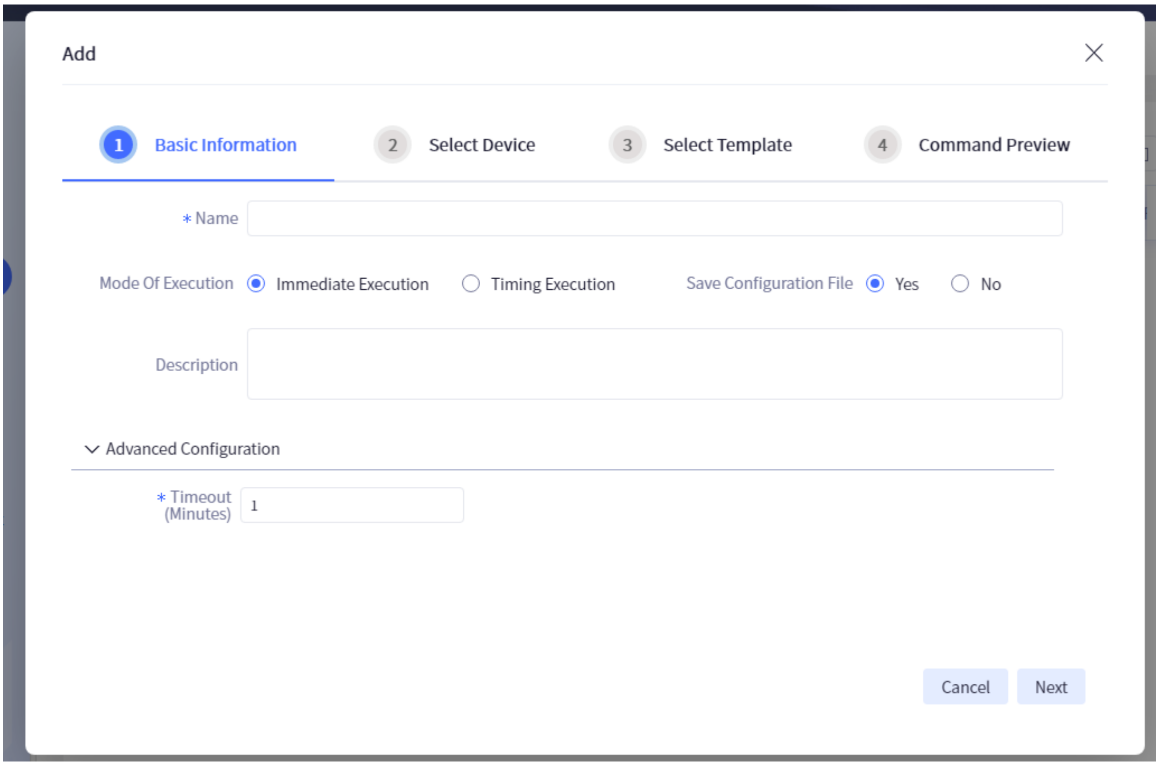
Figure 9. 1.5.2 Query command delivery task

Caution

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

Add task:

Click the **Add** button on the task panel to open the "Add" window, fill in the task name, execution mode, whether to save the configuration file, description and other information, and select the "Advanced Configuration" option to set the timeout, as shown in the following figure:



* Name

Mode Of Execution ● Immediate Execution ○ Timing Execution

Save Configuration File ● Yes ○ No

* Timeout (Minutes) 1

Figure 9. 1.5.3 Step 1 of adding the task information

Caution

- The device concurrency of the current single task in the command delivery task is 3, and the task concurrency is 3
- Default timeout is 2 minutes

Execution mode: When **Immediate Execution** is selected, the task can be executed immediately after the task information is configured; Select **Timing Execution** to display a “Appointed Time” text box. You can set a time and execute the task after the set time period.

Auto retry times: If the process of adding a task fails, the program will automatically retry according to the given number of times.

Timeout: When a task is executed, the task execution fails when the response time of the device exceeds the set timeout.

Click **Next** to enter the "Select Device" window, as shown in the following figure:

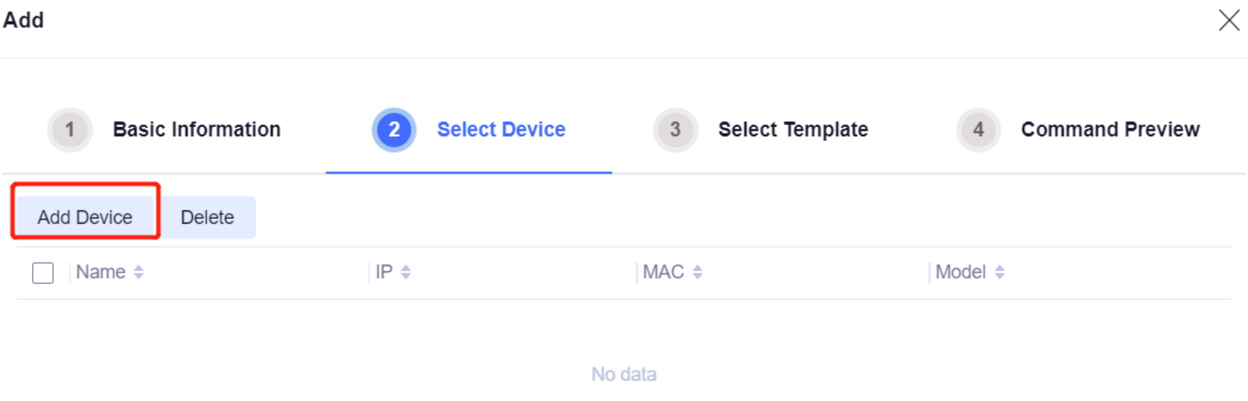
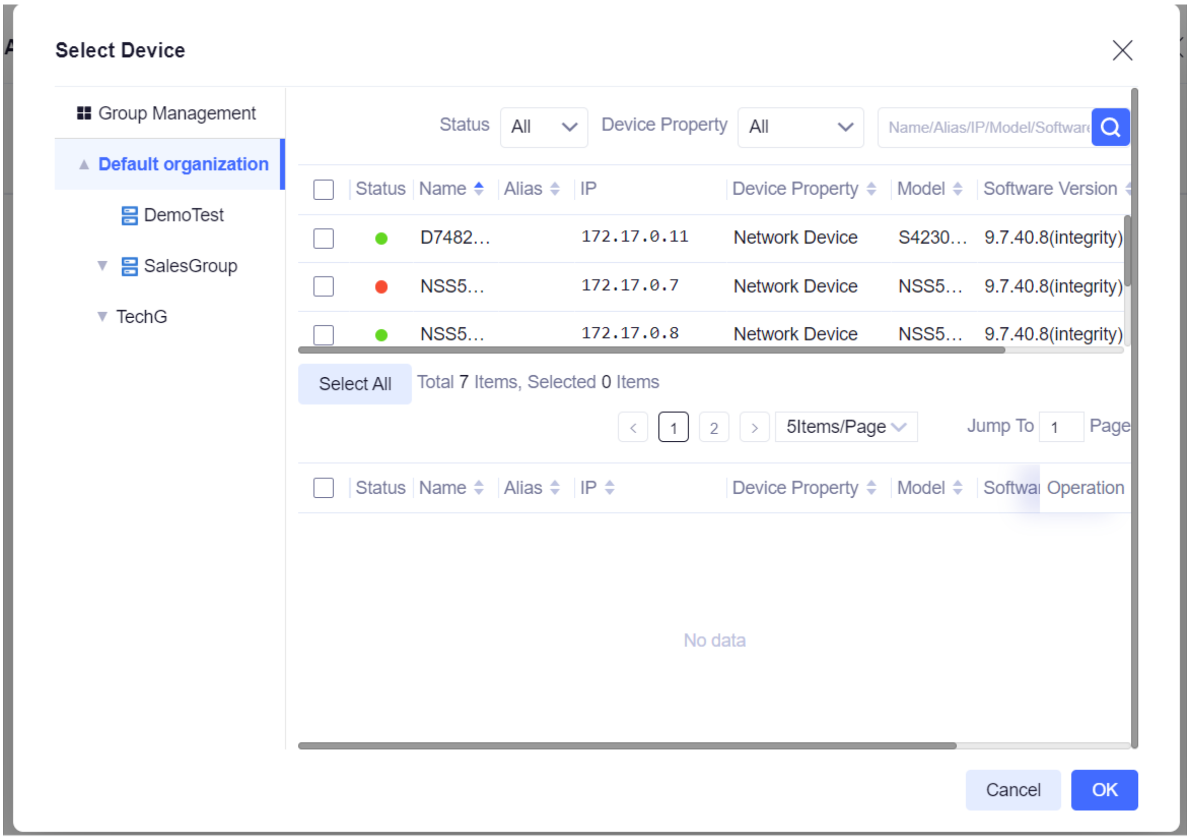


Figure 9.2.2.4 Step 2 of adding task information

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



Status: All · Device Property: All · Name/Alias/IP/Model/Software

☐	Status	Name	Alias	IP	Device Property	Model	Software Version
☐	●	D7482…		172.17.0.11	Network Device	S4230…	9.7.40.8(integrity)
☐	●	NSS5…		172.17.0.7	Network Device	NSS5…	9.7.40.8(integrity)
☐	●	NSS5…		172.17.0.8	Network Device	NSS5…	9.7.40.8(integrity)

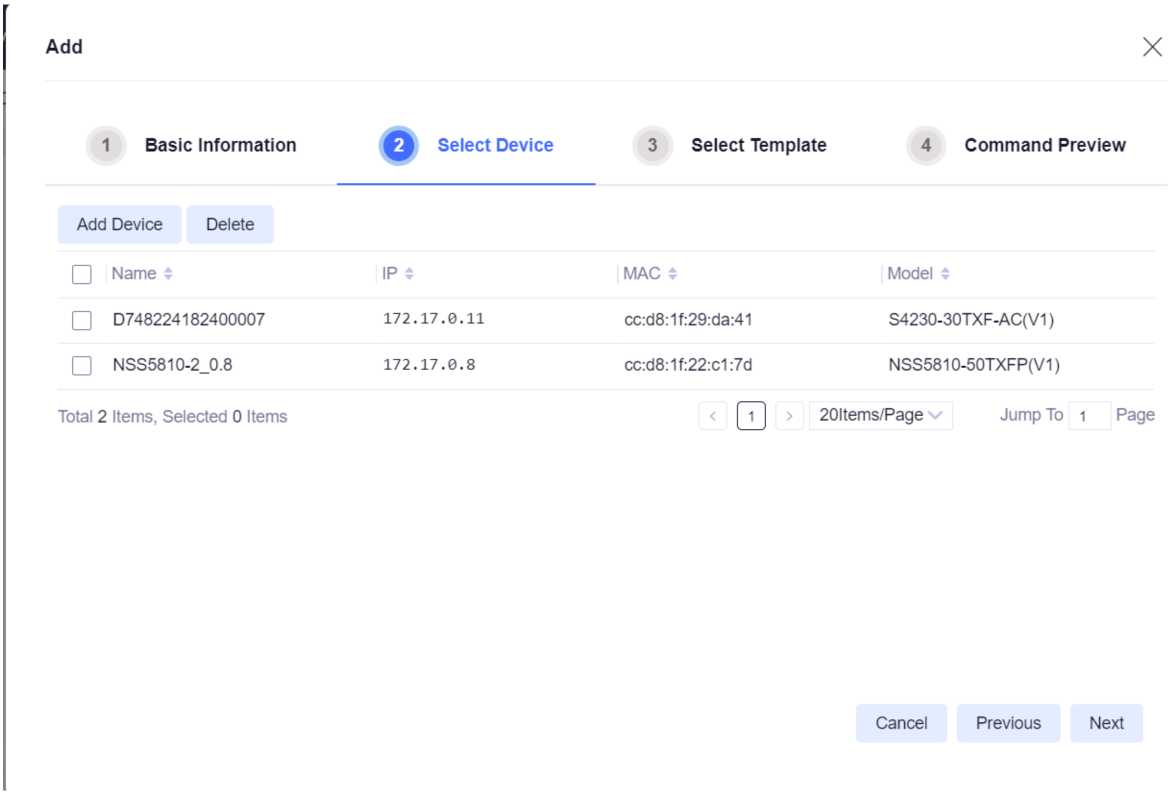
Total 7 Items, Selected 0 Items · 5Items/Page · Jump To 1 Page

☐	Status	Name	Alias	IP	Device Property	Model	Softwa	Operation

No data

Figure 9. 1.5.5 Select the device

Select a device. Support multiple choices. Click **OK** to select a device for the command delivery task, as shown in the following figure:

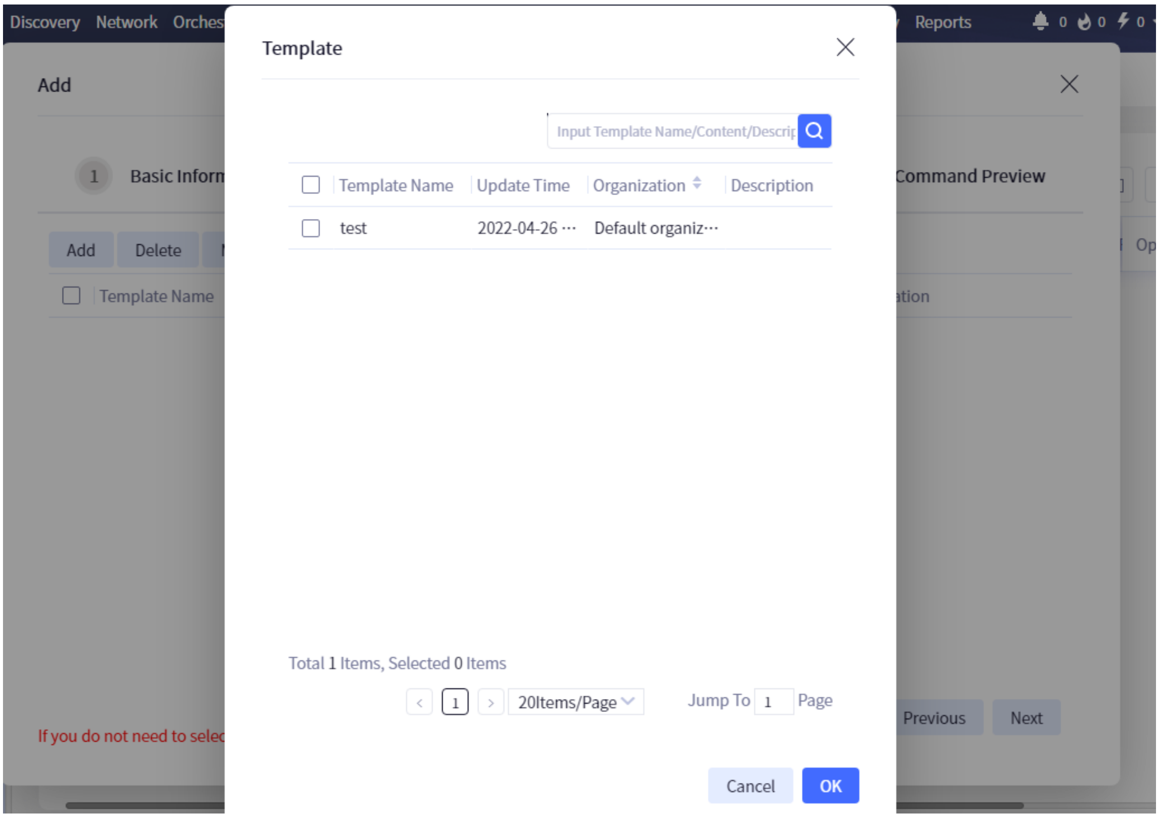


☐	Name	IP	MAC	Model
☐	D748224182400007	172.17.0.11	cc:d8:1f:29:da:41	S4230-30TXF-AC(V1)
☐	NSS5810-2_0.8	172.17.0.8	cc:d8:1f:22:c1:7d	NSS5810-50TXFP(V1)

Total 2 Items, Selected 0 Items · 20Items/Page · Jump To 1 Page

Figure 9. 1.5.6 Step 2 of adding task information

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



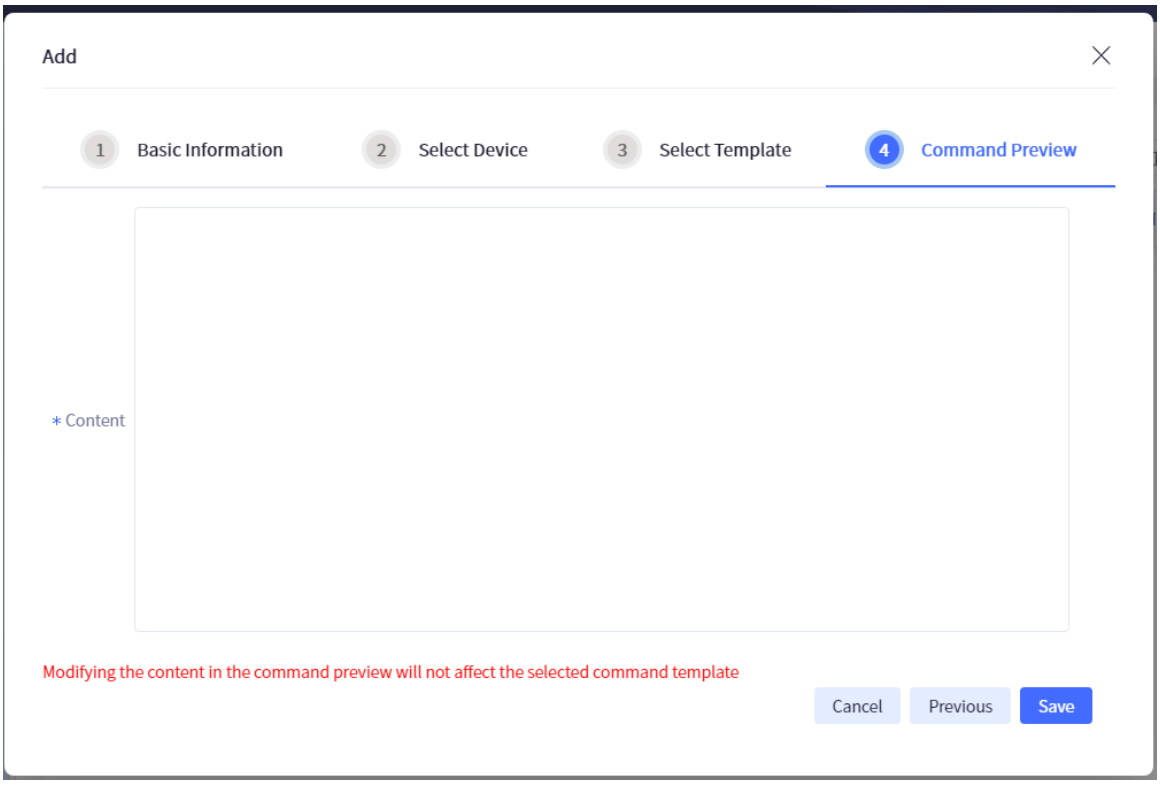
☐	Template Name	Update Time	Organization	Description
☐	test	2022-04-26 ···	Default organiz···	

Total 1 Items, Selected 0 Items

Figure 9. 1.5.7 Step 3 of adding task information

In the “Template” window, you can select a template in the command template list, and provide advanced query function to fuzzy query the template name, content and description. You can select multiple templates at the same time, and click **OK** to select the templates successfully.

Select a single template and click **Move Down** or **Move Up** to sort the templates. The order of templates determines the order of command preview and command delivery, Then click **Next** to preview the command in the selected template (you can modify the command to be delivered in the command preview window. Finally, the command in the command preview will prevail). Click **Save** to finish adding the configuration command delivery task. And then, the configuration command will be delivered.



Modifying the content in the command preview will not affect the selected command template

Figure 9. 1.5.8 Step 4 of adding the task information

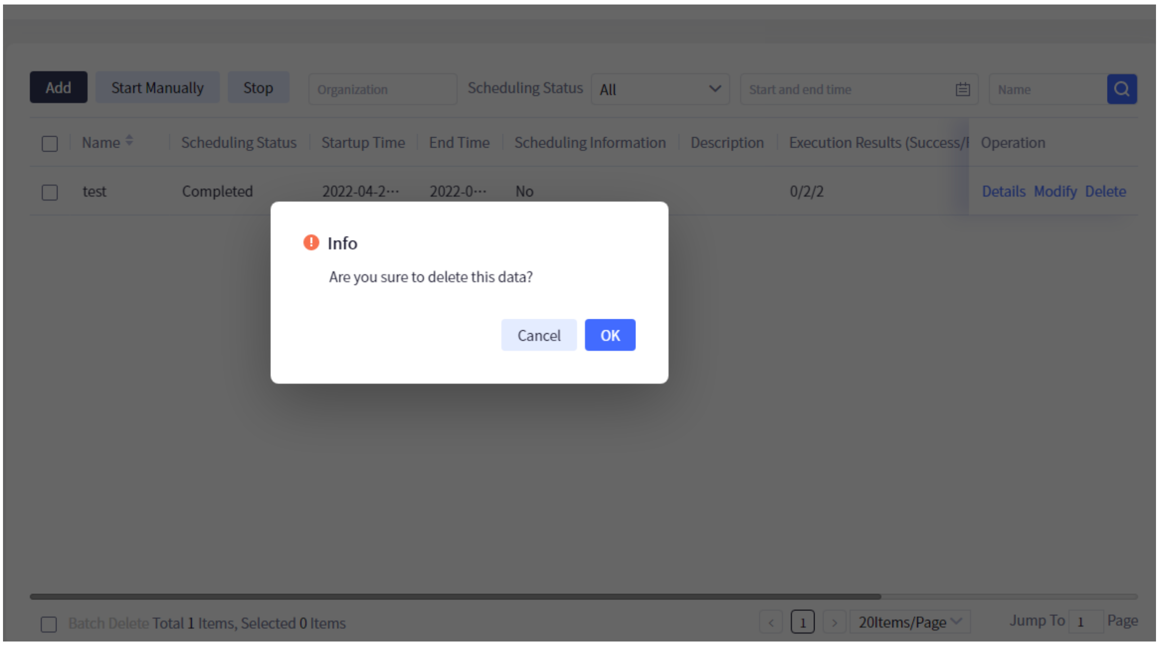
The process of modifying the task is the same as above. Select a desired task in the task list and click **Modify** to modify the task information.

Note

- No template can be selected in the “Template” interface. Commands can be entered directly in the command preview text box

Delete task:

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



☐	Name	Scheduling Status	Startup Time	End Time	Scheduling Information	Description	Execution Results (Success/I	Operation
☐	test	Completed	2022-04-2···	2022-0···	No		0/2/2	Details Modify Delete

Info

Are you sure to delete this data?

Total 1 Items, Selected 0 Items

Figure 9. 1.5.9 Delete the task information

Note

- The tasks in progress cannot be deleted or modified.

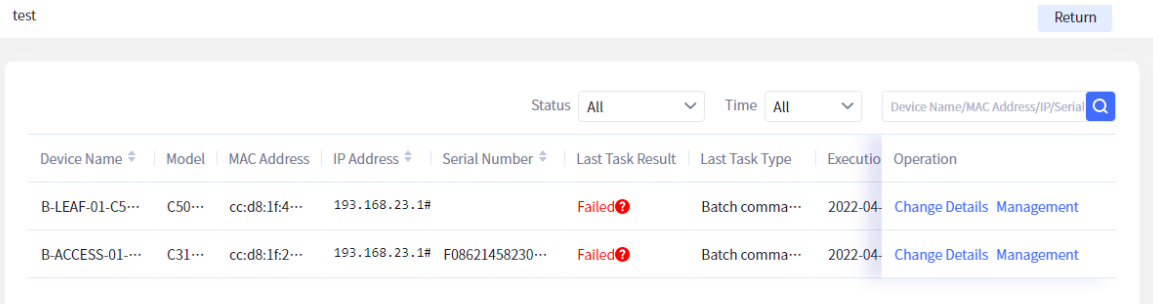
Manually start/stop task:

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

Select a stopped task and click the **Start Manually** button. The task can start running again from the beginning. At this time, the status of the task will change to "In progress".

View task details:

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

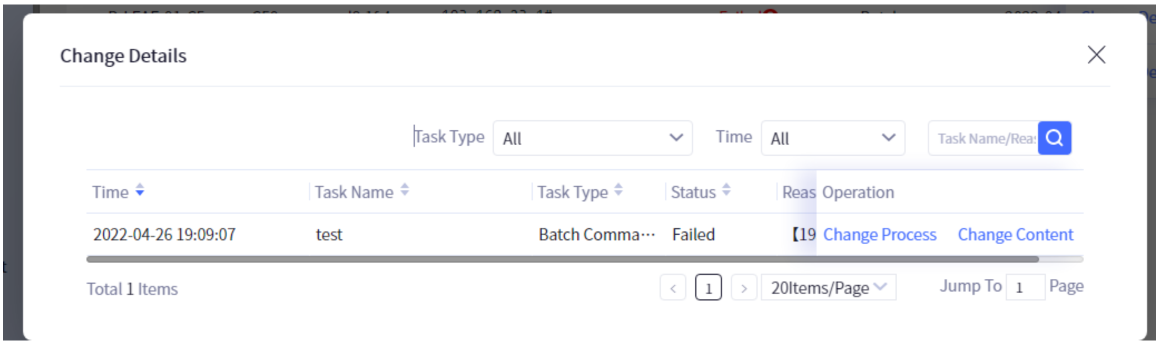


Device Name	Model	MAC Address	IP Address	Serial Number	Last Task Result	Last Task Type	Executio	Operation
B-LEAF-01-C5···	C50···	cc:d8:1f:4···	193.168.23.1#		Failed	Batch comma···	2022-04-	Change Details Management
B-ACCESS-01-···	C31···	cc:d8:1f:2···	193.168.23.1#	F08621458230···	Failed	Batch comma···	2022-04-	Change Details Management

Figure 9. 1.5.10 Task details

The "Task Details" interface displays different devices under the same task in pages, showing the device name, model, MAC, device IP, serial number, latest change status, latest change task type, change time, operation and other information of the command delivery.

View change details:

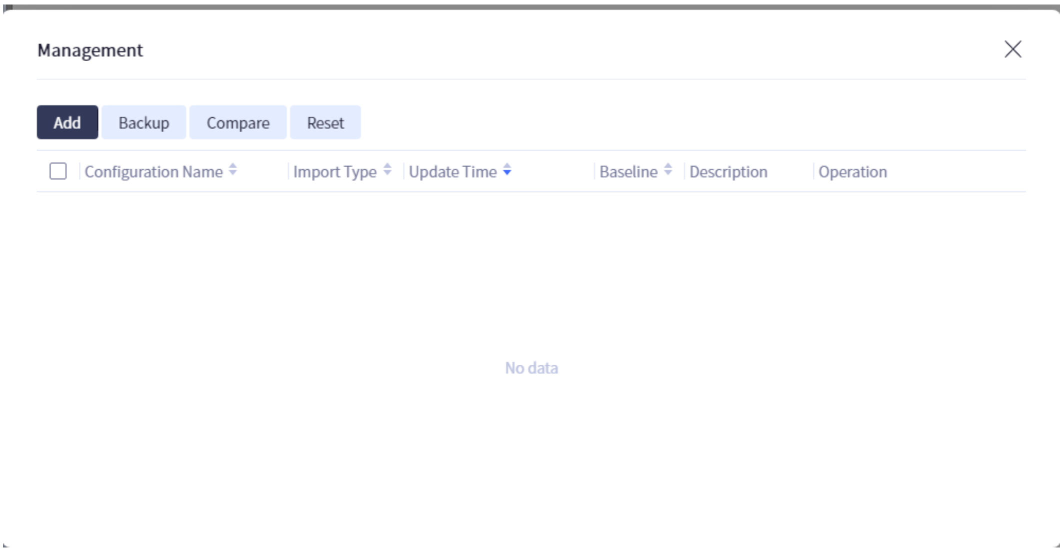


Time	Task Name	Task Type	Status	Reas	Operation
2022-04-26 19:09:07	test	Batch Comma···	Failed	【19	Change Process Change Content

Figure 9. 1.5.11 Change details

Management:

The "Management" interface also provides operations such as backup, comparison, addition, editing, recovery, baseline setting and deletion of configuration files, as shown in the figure:



☐	Configuration Name	Import Type	Update Time	Baseline	Description	Operation

Figure 9. 1.5.12 Management

9.2 Compliance Check

9.2.1 Rule Definition

Click "Maintenance" in the menu bar above, and select "Rules Definition" in the selection column on the left side of the page to enter the compliance rule definition page, as shown in the following figure:

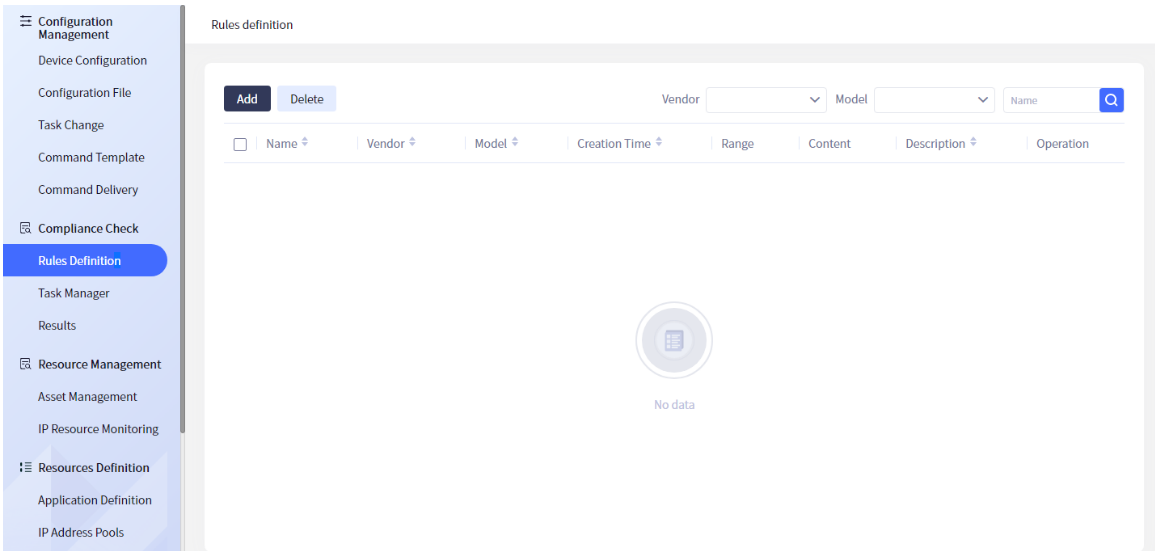


Figure 9. 2.1.1 Compliance rule definition

This page provides various query criteria to query specific tasks conveniently and quickly. Enter the corresponding query criteria, and then click **Query** to query the data according to the name, equipment manufacturer and model fields; You can click "Name", "Vendor", "Model" and other fields in the header of the list to sort, as shown below:

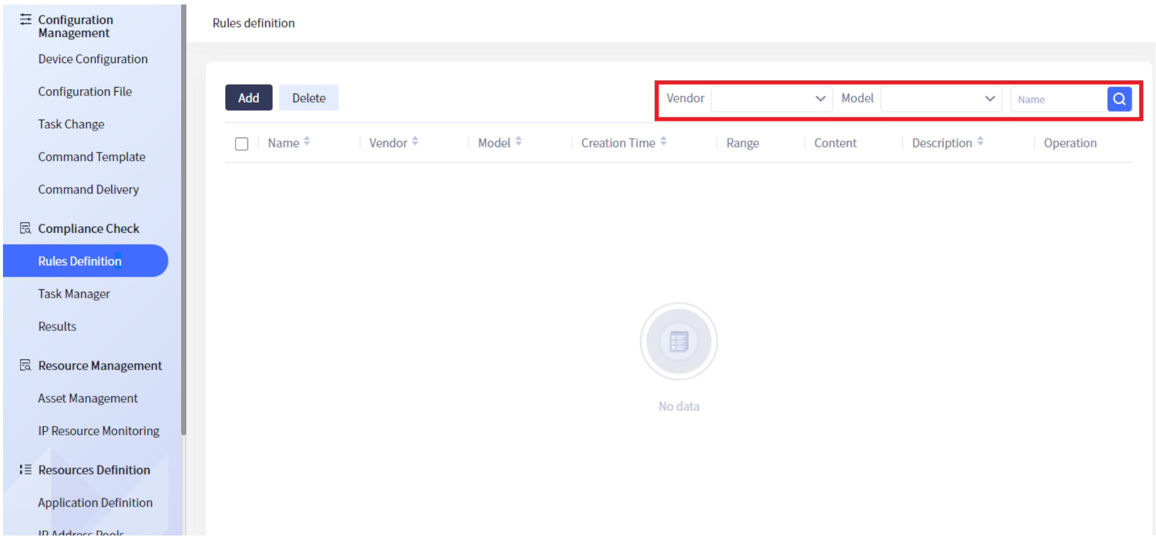


Figure 9. 2.1.2 Query compliance rules

Add rules:

Click **Add** to open the dialog box, fill in relevant parameters, and click **OK** to save the new rule, as shown below:

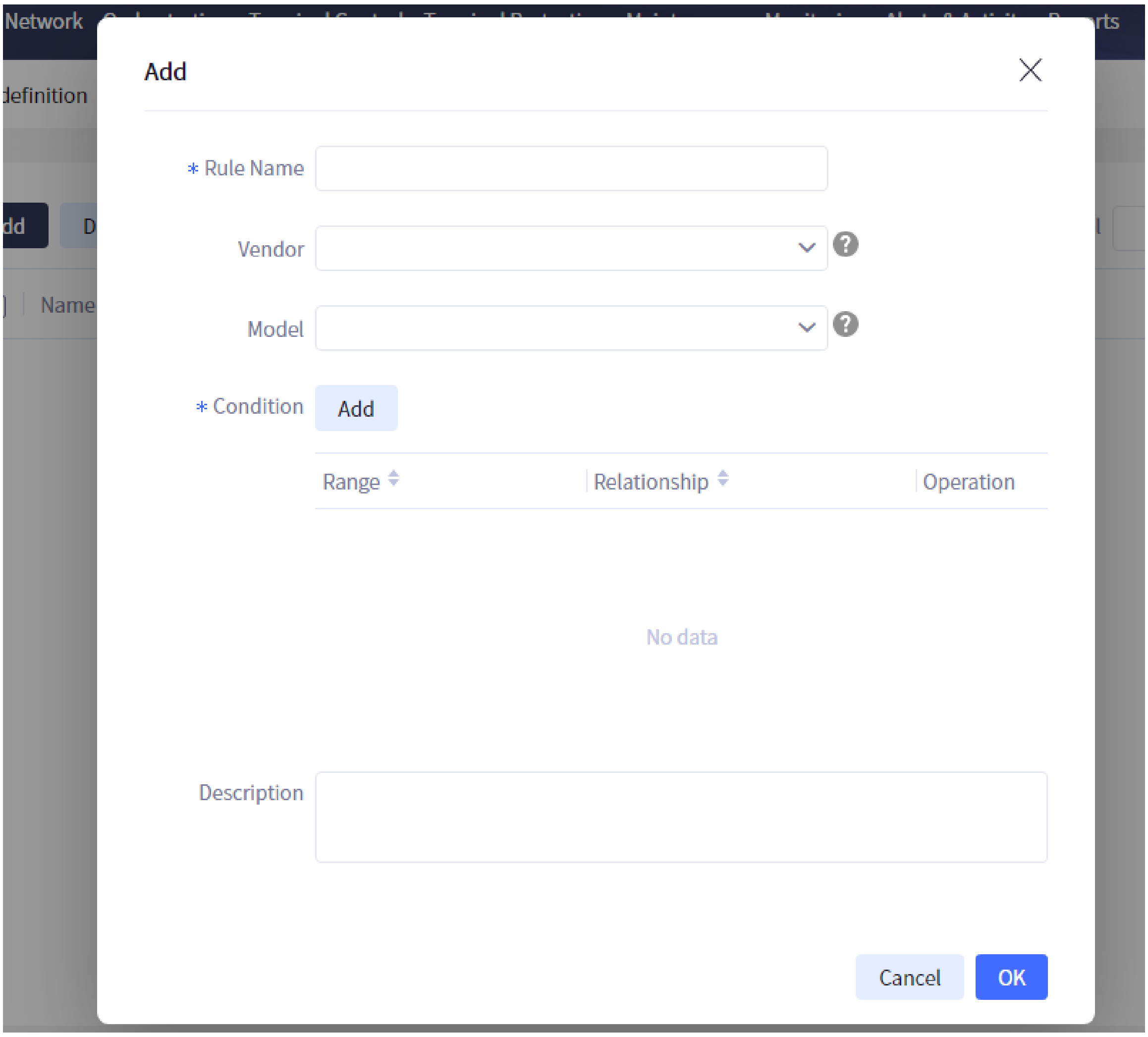


Figure 9. 2.1.3 Add compliance rule

To add a rule condition, click **Add**, as shown in the figure:

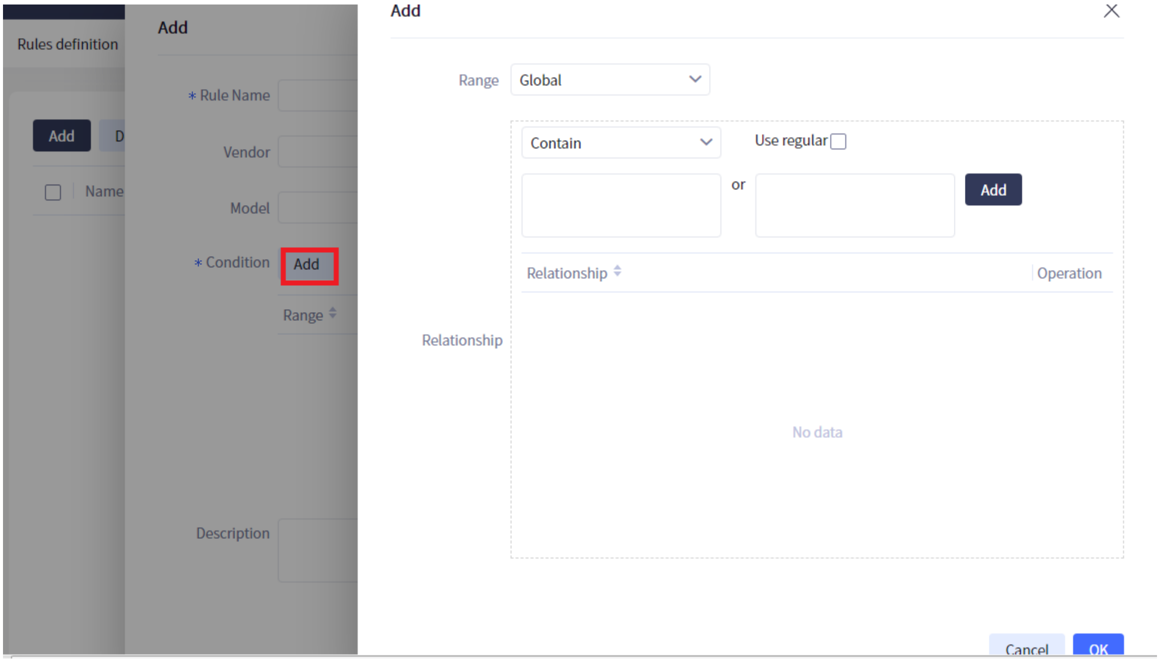
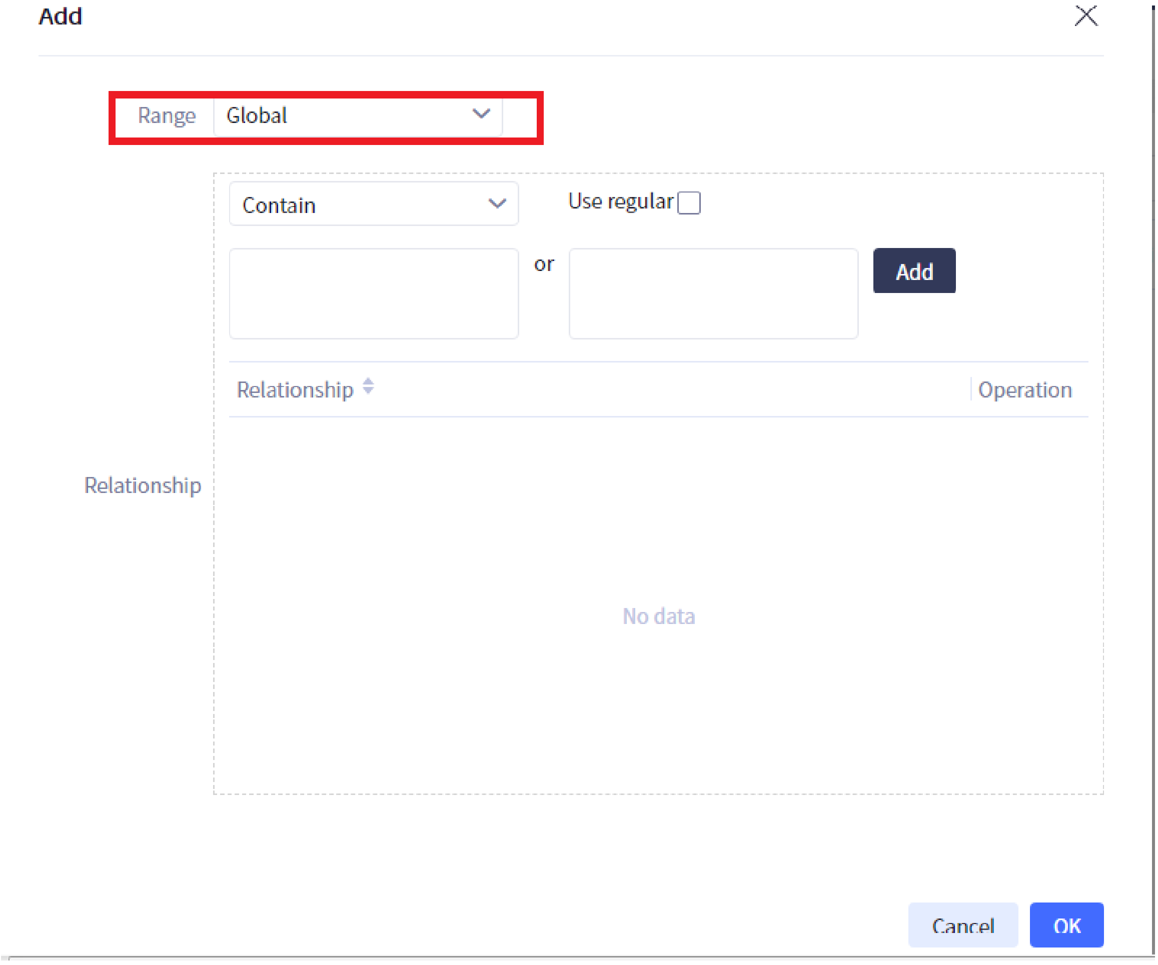


Figure 9. 2.1.4 Add rule conditions

Range supports global and port. **Relationship** includes **Contain** and **Does Not Contain**. It supports the use of regular, as shown below:



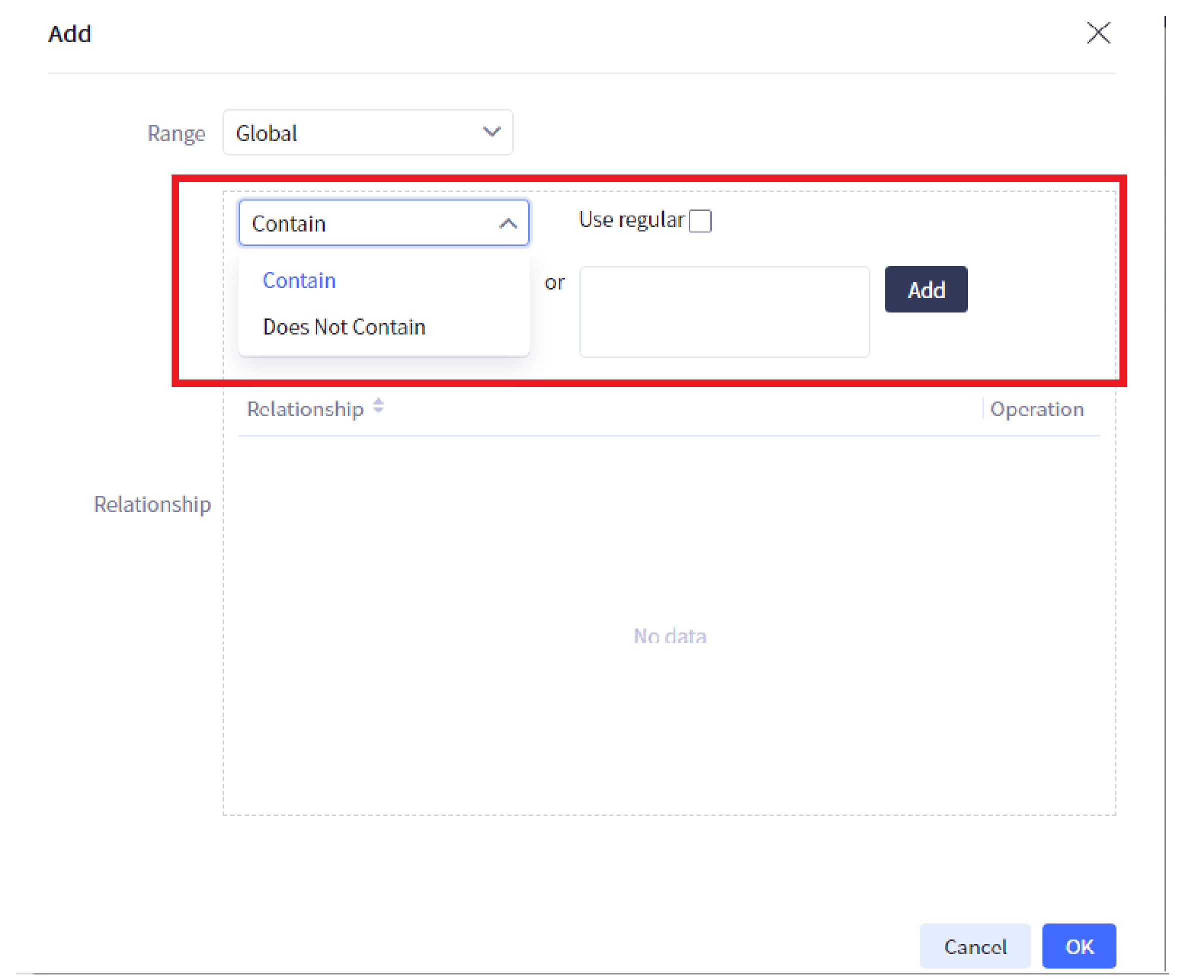


Figure 9. 2.1.5 Rule condition range

You can add and delete the **Contain** or **Does not Contain** relationship. After adding, click **OK** to save, as shown below:

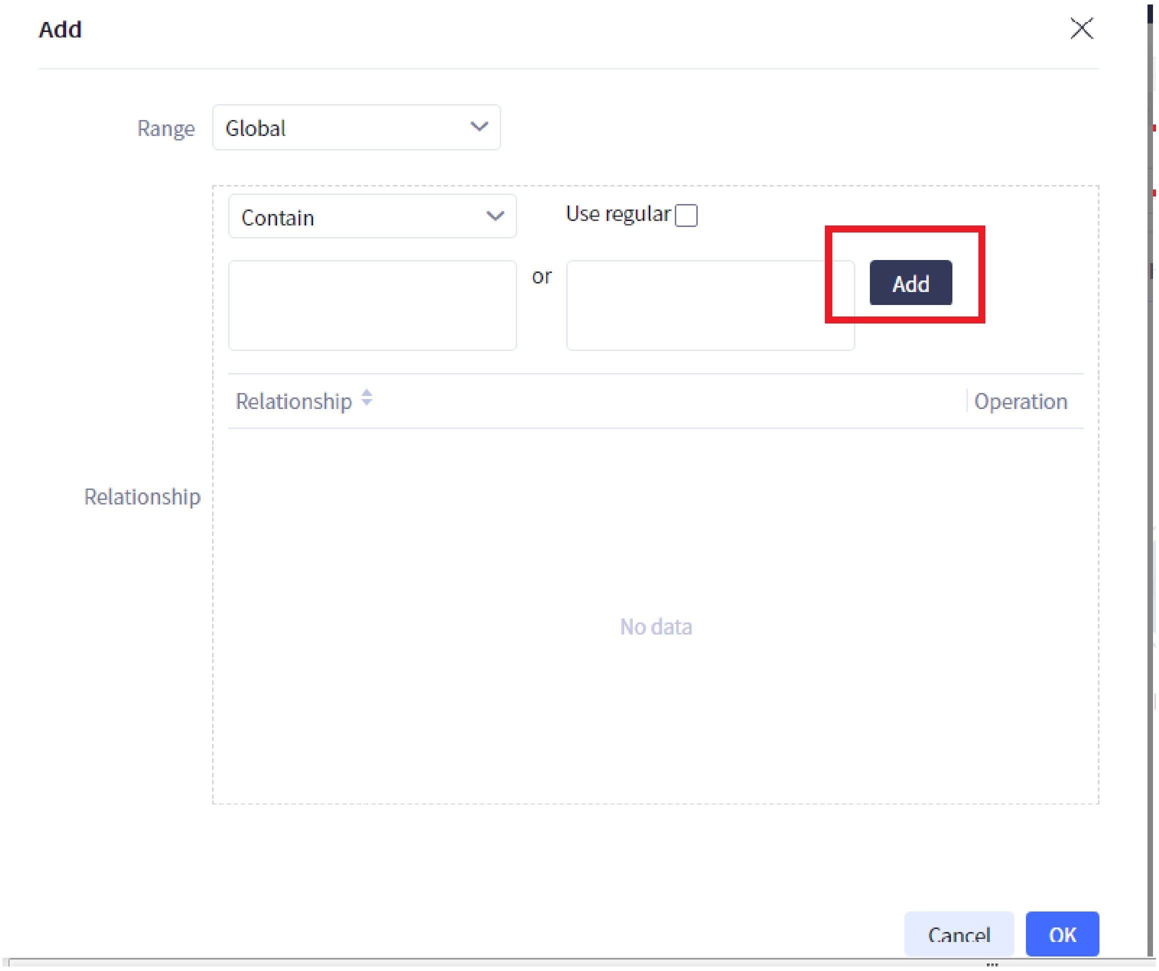
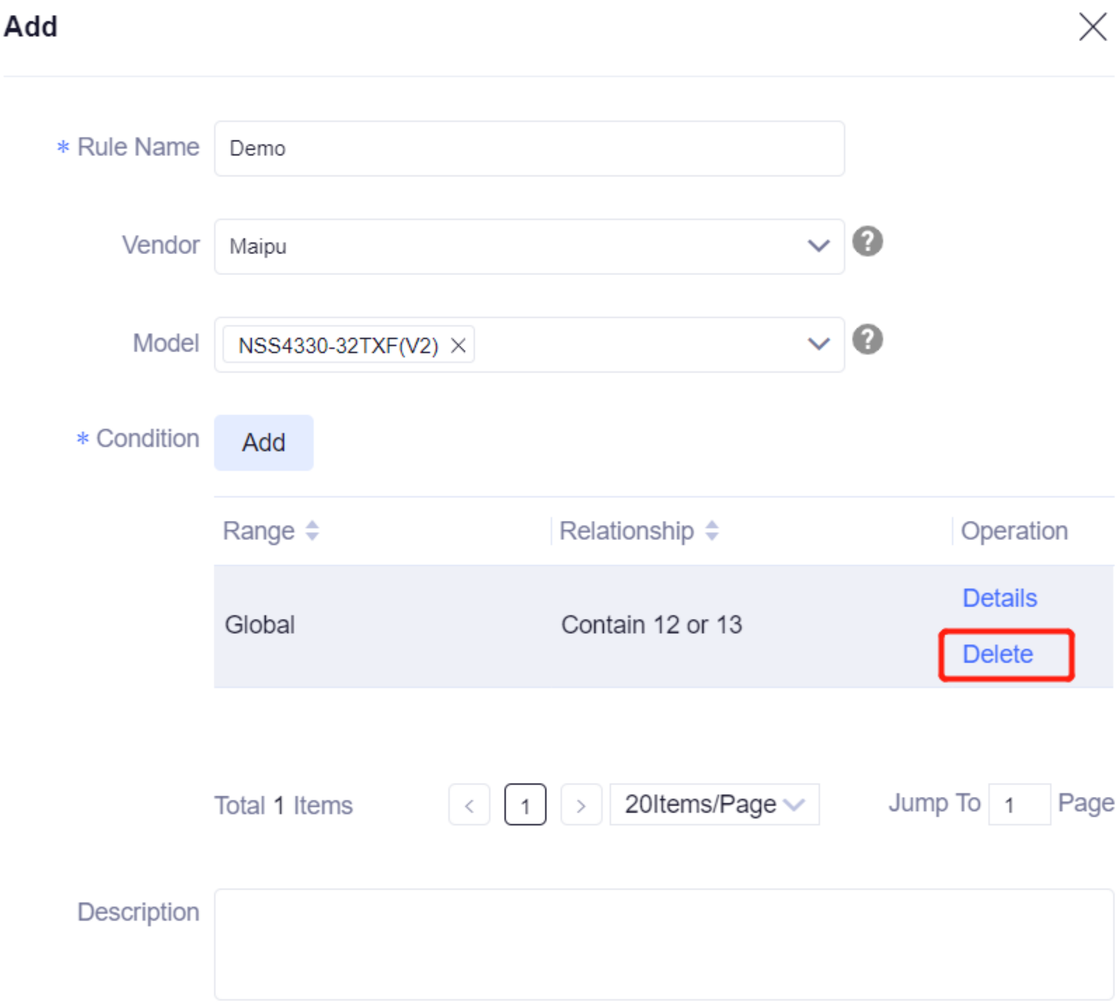


Figure 9. 2.1.6 Add rule condition relationship

After adding a rule condition, you can view the details and delete the rule condition, as shown below:



Add

* Rule Name: Demo

Vendor: Maipu

Model: NSS4330-32TXF(V2)

* Condition

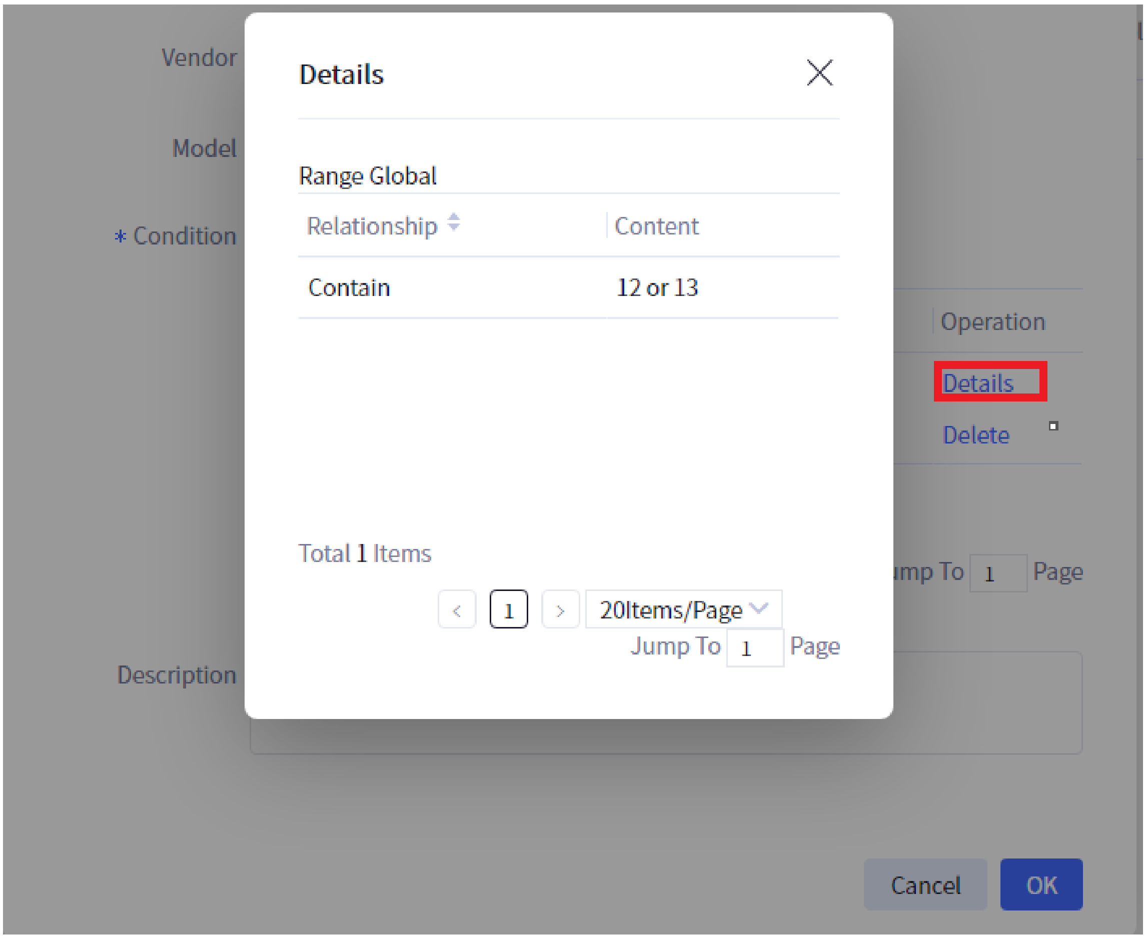
Range	Relationship	Operation
Global	Contain 12 or 13	Details Delete

Total 1 Items

Jump To 1 Page

Description

Figure 9. 2.1.7 Delete the rule condition


Details

Range Global

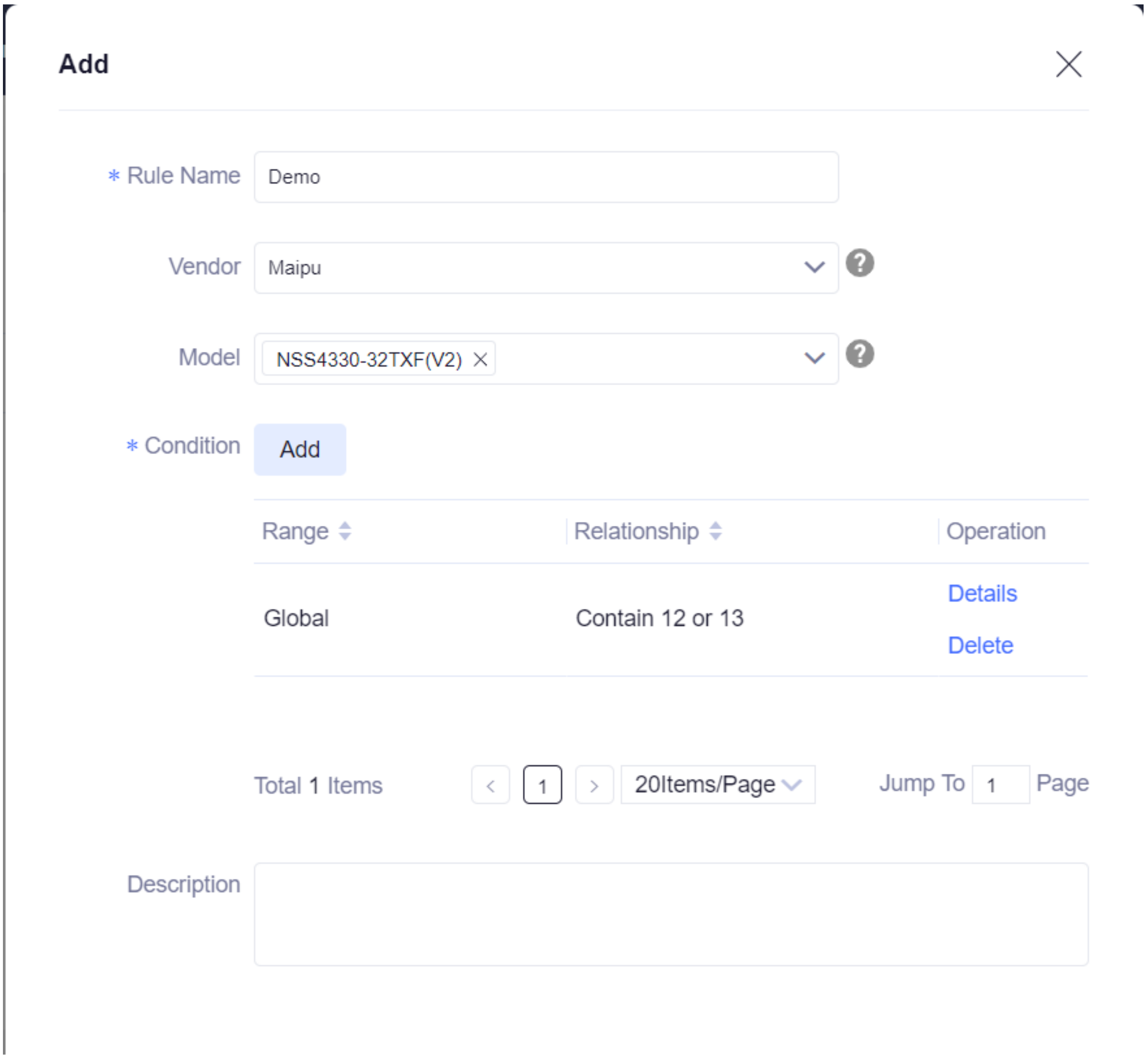
Relationship	Content
Contain	12 or 13

Total 1 Items

Figure 9. 2.1.8 Rule condition details

Modify rule:

Select a desired rule in the page, click **Modify** to open the “Modify” dialog box, where you can modify the details of the rule, and click **OK** to save the modified rule, as shown below:



Add

* Rule Name: Demo

Vendor: Maipu

Model: NSS4330-32TXF(V2)

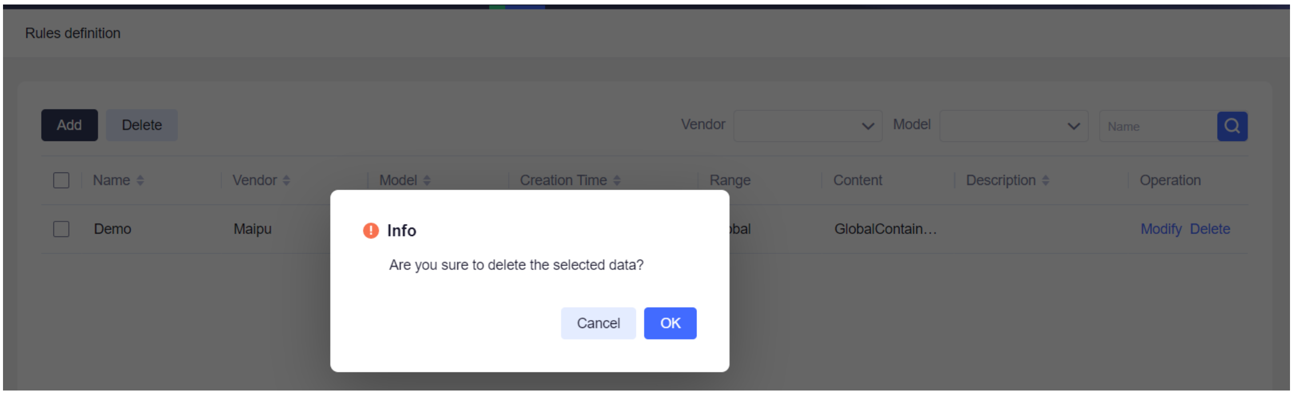
* Condition

Range	Relationship	Operation
Global	Contain 12 or 13	Details Delete

Figure 9. 2.1.9 Modify the rule

Delete rules:

Select the desired rule in the page, click **Delete**, click **OK** in the confirmation dialog box to delete the selected configuration, and click **Cancel** to abort the deletion, as shown below:



Name	Vendor	Model	Creation Time	Range	Content	Description	Operation
Demo	Maipu			bal	GlobalContain…		Modify Delete

Info

Are you sure to delete the selected data?

Figure 9. 2.1.10 Delete the rule

9.2.2 Compliance Task Management

Click "Maintenance" > "Compliance Check" > "Task Manager" in the menu bar to open the "Task Manager" page, as shown below.

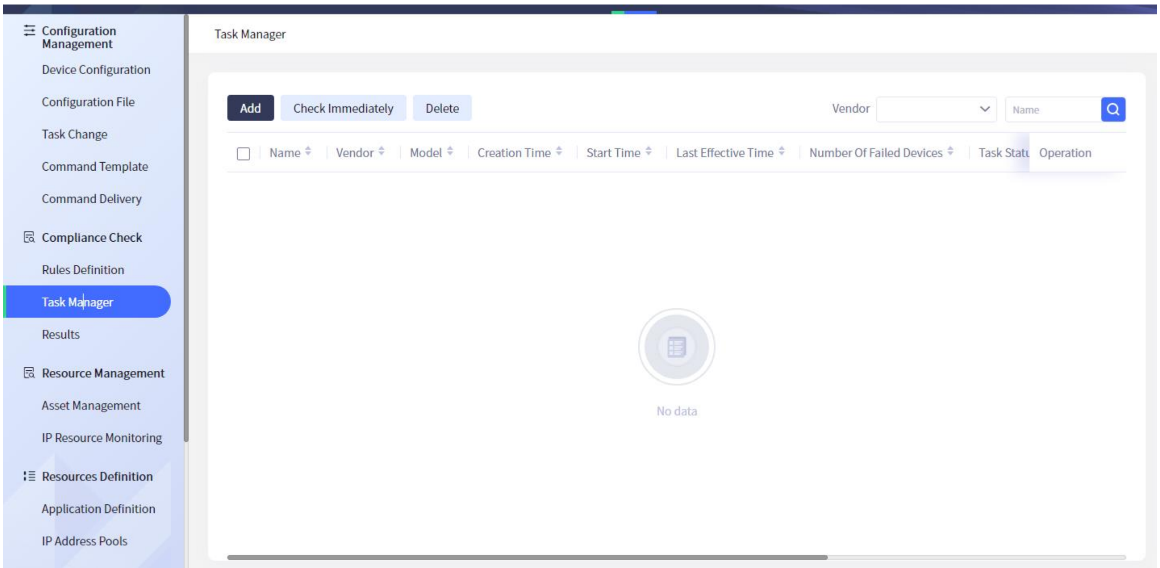


Figure 9. 2.2.1 Compliance task management

Condition query

Compliance task management supports fuzzy query and filtering by vendor and name, as shown in the following figure:

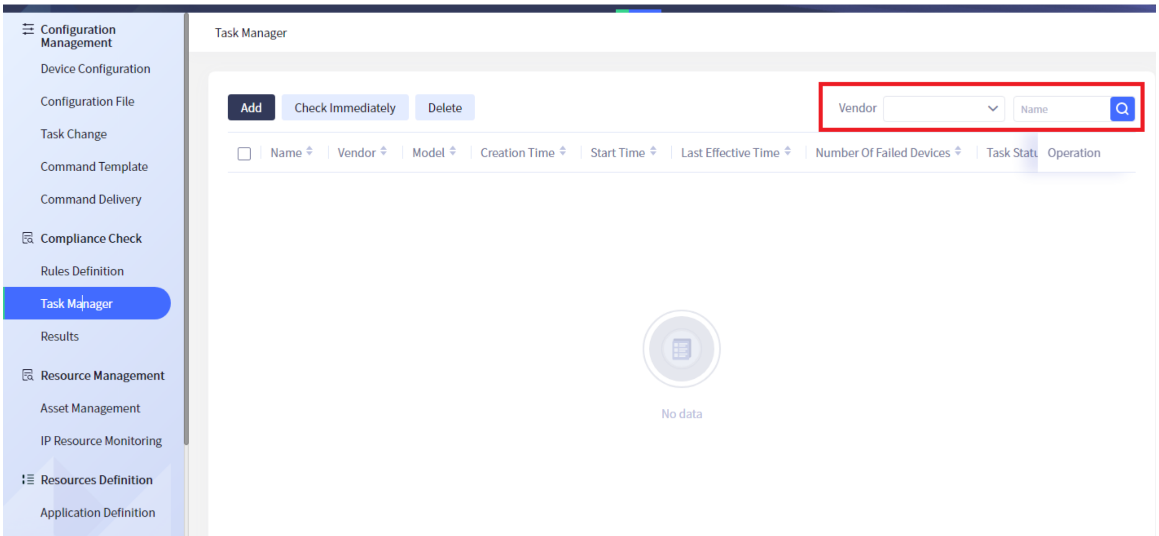


Figure 9. 2.2.2 Query compliance task

Add/modify task:

Click the **Add** button in the task list, or select a task and click the **Modify** button to open the "Add" window as shown in the following figure, and select the vendor information, model and organization.

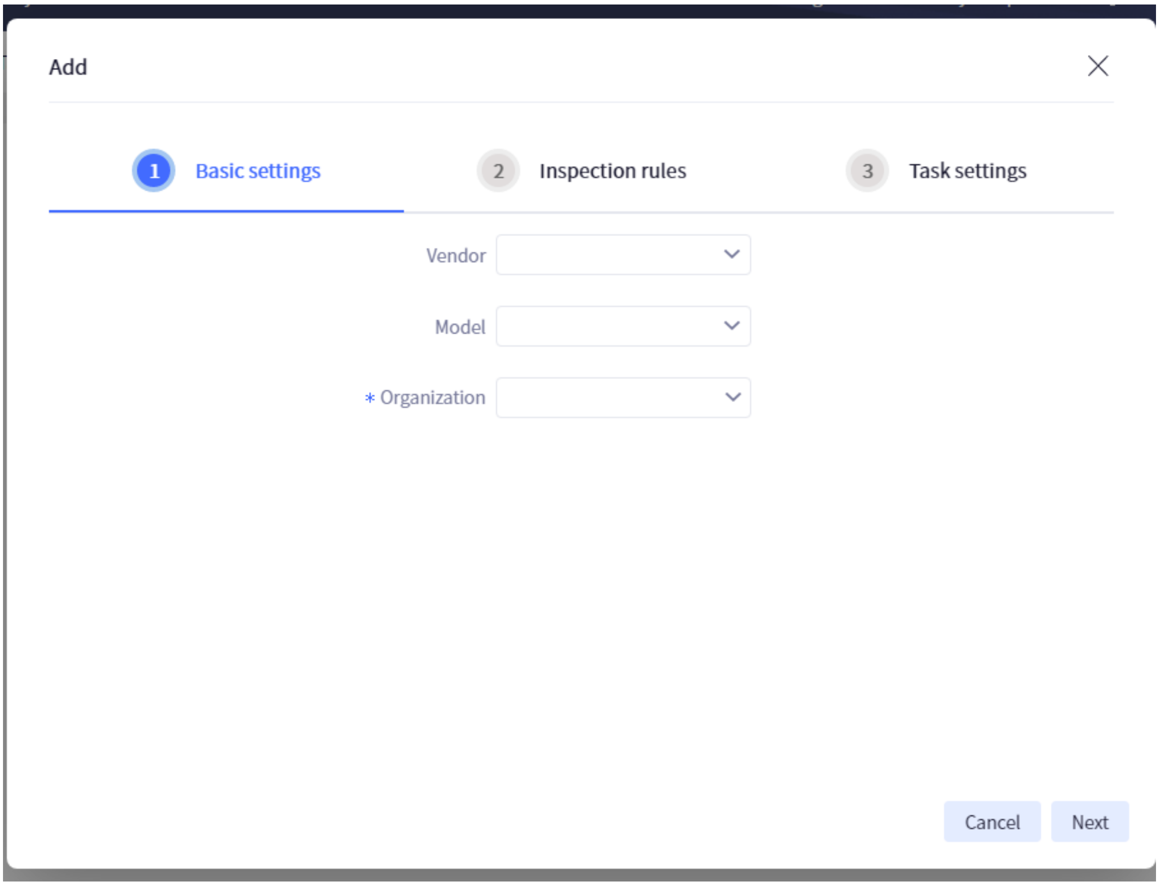
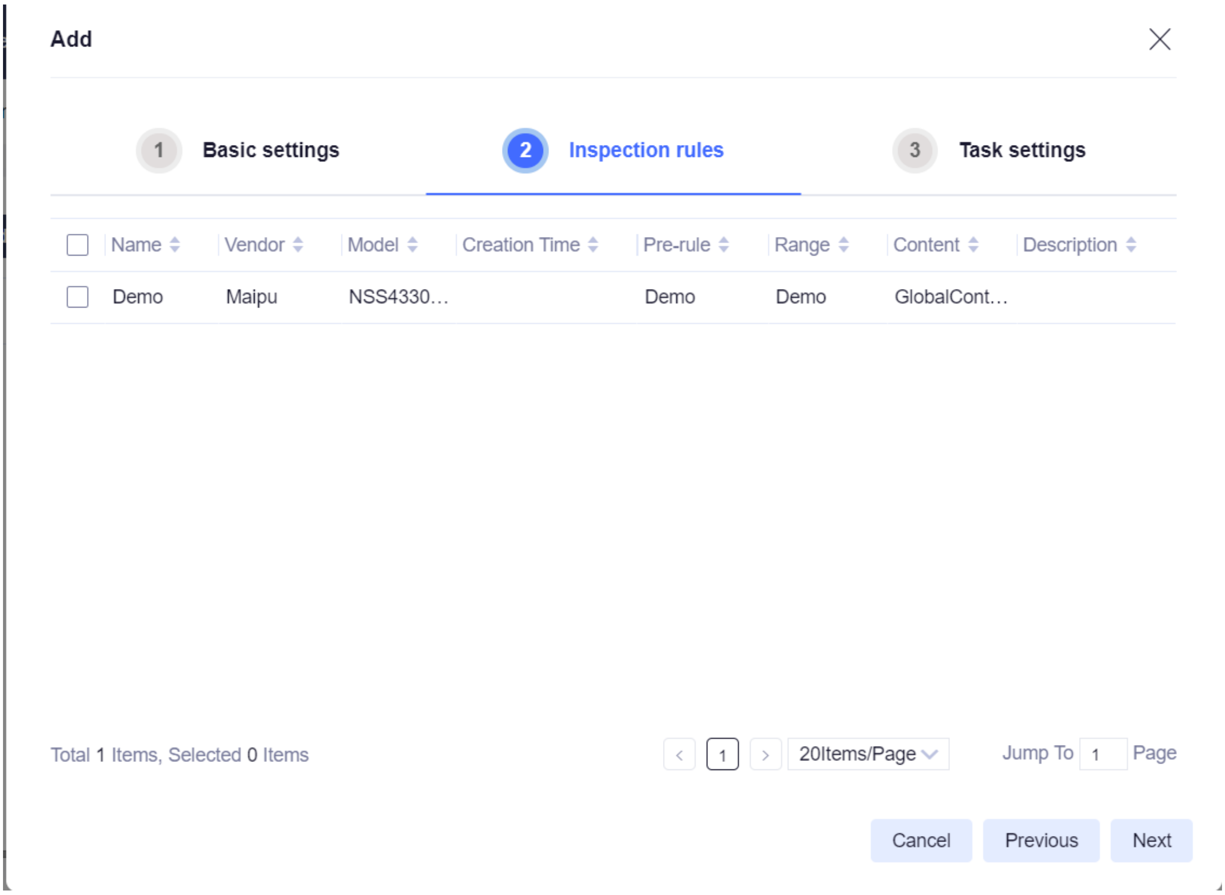


Figure 9. 2.2.3 Step 1 of adding/modifying the task information

Click “Next” to enter the “Inspection rules” window, as shown in the following figure:



☐	Name	Vendor	Model	Creation Time	Pre-rule	Range	Content	Description
☐	Demo	Maipu	NSS4330…		Demo	Demo	GlobalCont…	

Total 1 Items, Selected 0 Items

Figure 9. 2.2.4 Step 2 of adding/modifying the task information

Select the rule information and click **Next** to enter the **Task Settings** window, as shown in the following figure:

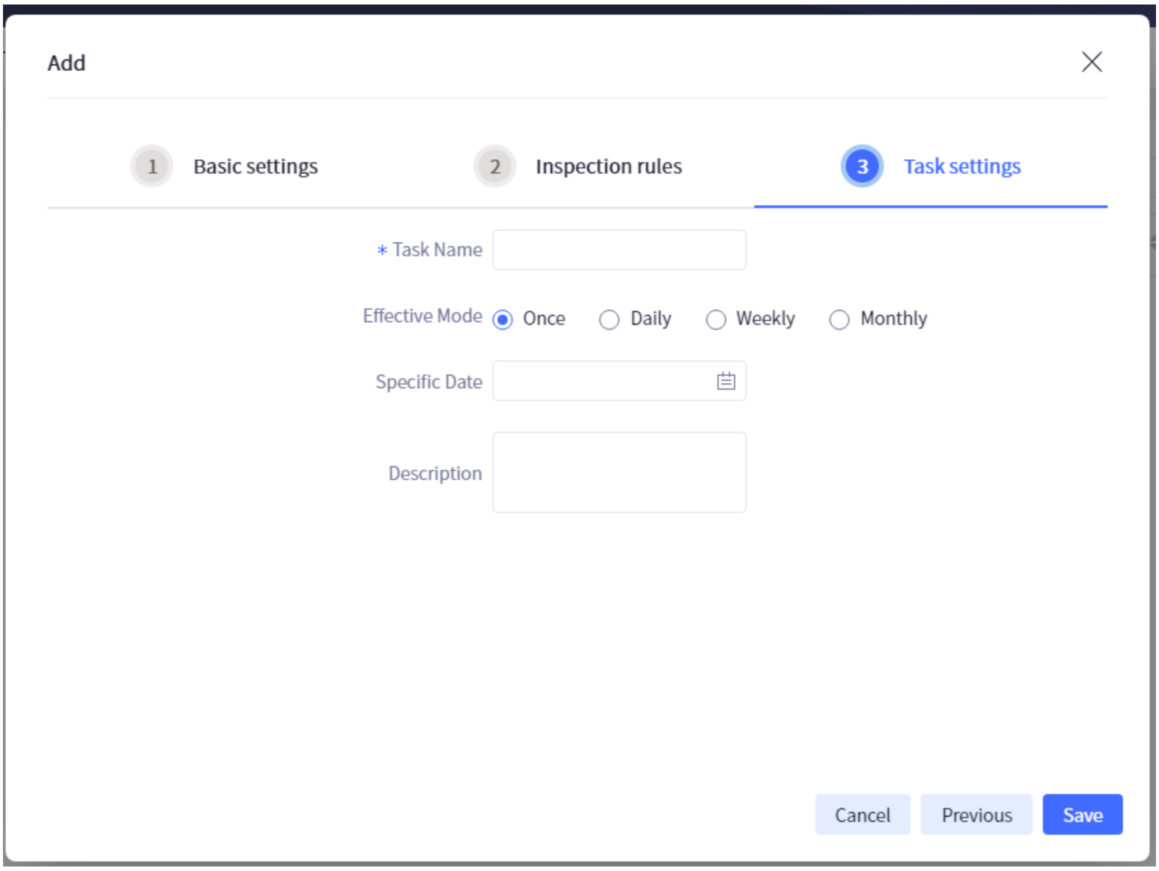
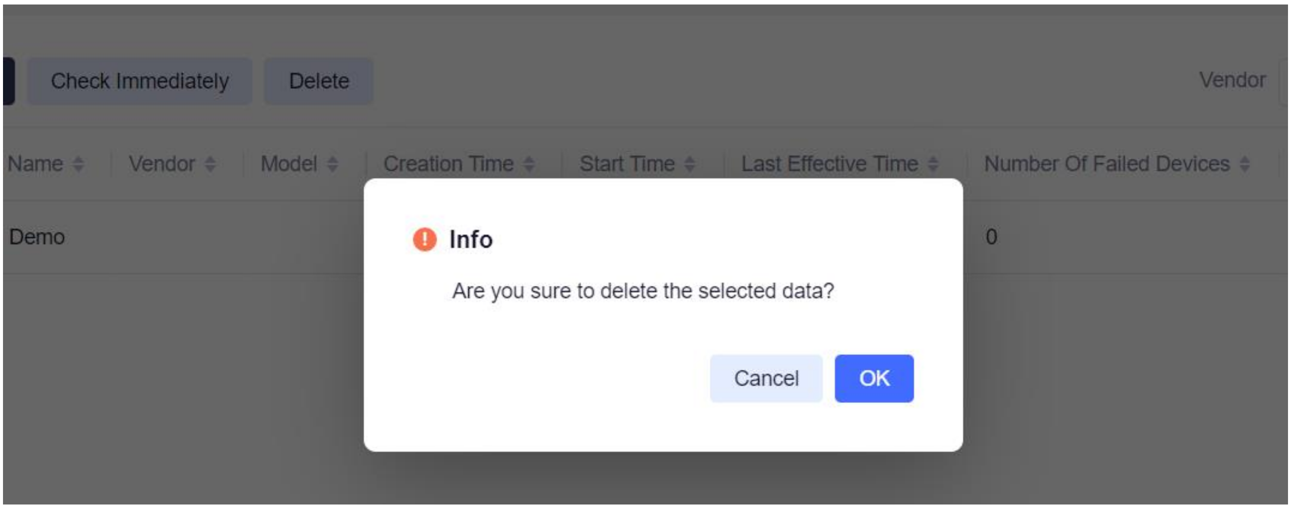


Figure 9. 2.2.5 Step 3 of adding/modifying the task information

Click **Save** to finish adding the compliance task. The process of task modification is the same as above. Select a desired task in the task list and click **Modify** to modify the task information.

Delete a task:

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

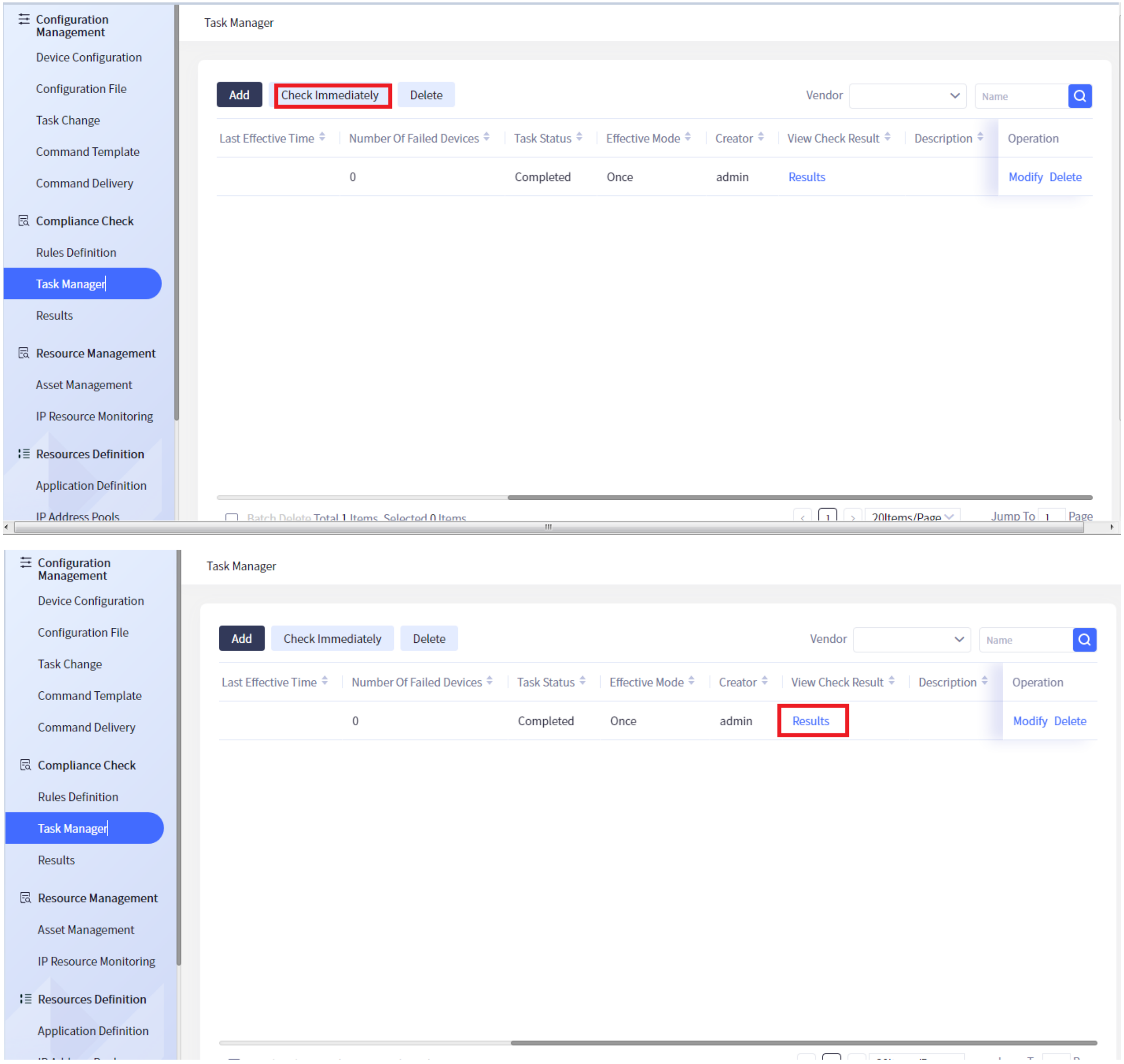


Are you sure to delete the selected data?

Figure 9. 2.2.6 Delete the task information

Check immediately:

Check the selected compliance task immediately, and you can view the inspection results, as shown in the following figure:

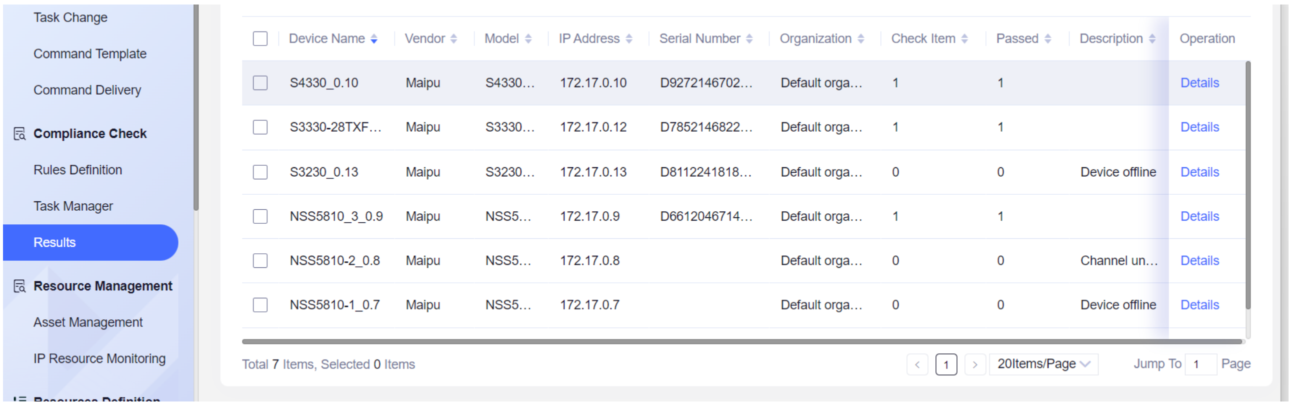


Last Effective Time	Number Of Failed Devices	Task Status	Effective Mode	Creator	View Check Result	Description	Operation
	0	Completed	Once	admin	Results		Modify Delete

Total 1 Items, Selected 0 Items

Figure 9. 2.2.7 Check task

Click **Results** to jump to the "Results" page, as shown below:



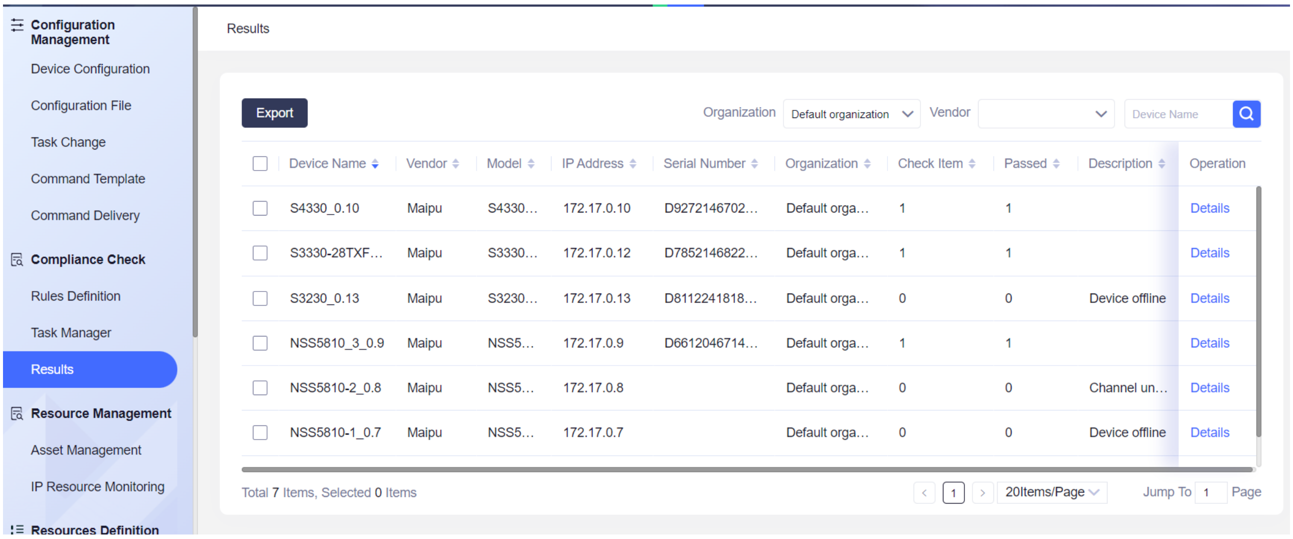
☐	Device Name	Vendor	Model	IP Address	Serial Number	Organization	Check Item	Passed	Description	Operation
☐	S4330_0.10	Maipu	S4330…	172.17.0.10	D9272146702…	Default orga…	1	1		Details
☐	S3330-28TXF…	Maipu	S3330…	172.17.0.12	D7852146822…	Default orga…	1	1		Details
☐	S3230_0.13	Maipu	S3230…	172.17.0.13	D8112241818…	Default orga…	0	0	Device offline	Details
☐	NSS5810_3_0.9	Maipu	NSS5…	172.17.0.9	D6612046714…	Default orga…	1	1		Details
☐	NSS5810-2_0.8	Maipu	NSS5…	172.17.0.8		Default orga…	0	0	Channel un…	Details
☐	NSS5810-1_0.7	Maipu	NSS5…	172.17.0.7		Default orga…	0	0	Device offline	Details

Total 7 Items, Selected 0 Items

Figure 9. 2.2.8 Check result

9.2.3 Check Result

Click "Maintenance" > "Compliance Check" - > "Results" in the menu bar to open the "Results" page, as shown below.



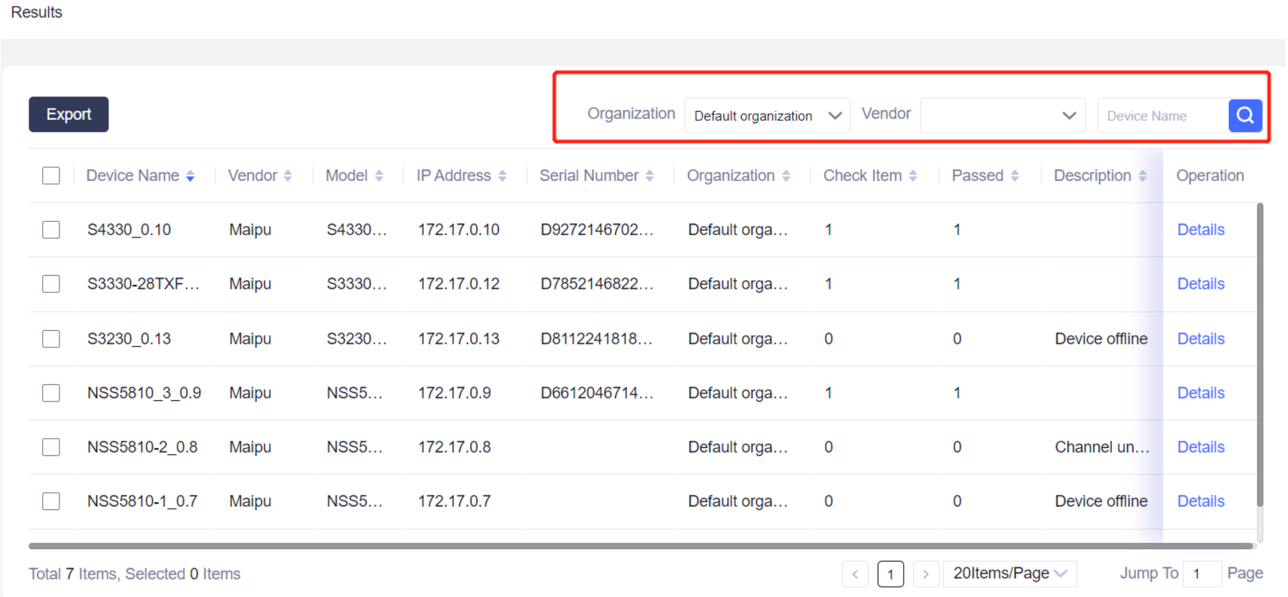
☐	Device Name	Vendor	Model	IP Address	Serial Number	Organization	Check Item	Passed	Description	Operation
☐	S4330_0.10	Maipu	S4330…	172.17.0.10	D9272146702…	Default orga…	1	1		Details
☐	S3330-28TXF…	Maipu	S3330…	172.17.0.12	D7852146822…	Default orga…	1	1		Details
☐	S3230_0.13	Maipu	S3230…	172.17.0.13	D8112241818…	Default orga…	0	0	Device offline	Details
☐	NSS5810_3_0.9	Maipu	NSS5…	172.17.0.9	D6612046714…	Default orga…	1	1		Details
☐	NSS5810-2_0.8	Maipu	NSS5…	172.17.0.8		Default orga…	0	0	Channel un…	Details
☐	NSS5810-1_0.7	Maipu	NSS5…	172.17.0.7		Default orga…	0	0	Device offline	Details

Total 7 Items, Selected 0 Items

Figure 9. 2.3.8 Check results

Condition query:

The check results support fuzzy query and filtering by the organization, vendor and device name, as shown in the following figure:



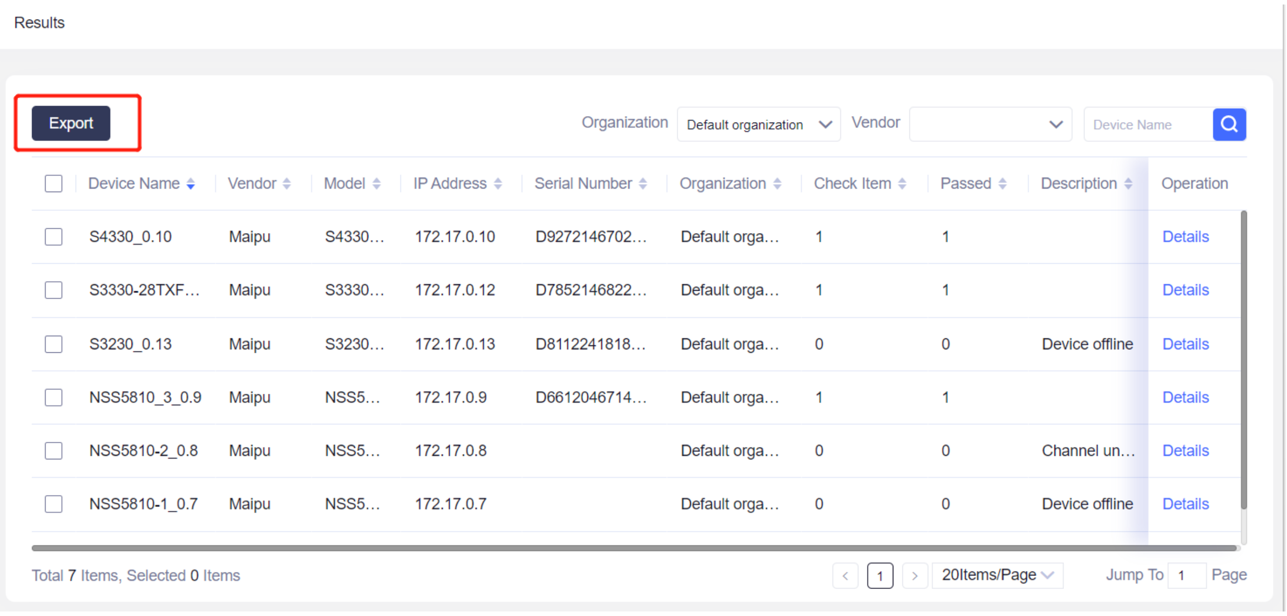
☐	Device Name	Vendor	Model	IP Address	Serial Number	Organization	Check Item	Passed	Description	Operation
☐	S4330_0.10	Maipu	S4330…	172.17.0.10	D9272146702…	Default orga…	1	1		Details
☐	S3330-28TXF…	Maipu	S3330…	172.17.0.12	D7852146822…	Default orga…	1	1		Details
☐	S3230_0.13	Maipu	S3230…	172.17.0.13	D8112241818…	Default orga…	0	0	Device offline	Details
☐	NSS5810_3_0.9	Maipu	NSS5…	172.17.0.9	D6612046714…	Default orga…	1	1		Details
☐	NSS5810-2_0.8	Maipu	NSS5…	172.17.0.8		Default orga…	0	0	Channel un…	Details
☐	NSS5810-1_0.7	Maipu	NSS5…	172.17.0.7		Default orga…	0	0	Device offline	Details

Total 7 Items, Selected 0 Items

Figure 9. 2.3.9 Check results

Export results:

Click the **Export** button to export and generate an excel file, as shown in the following figure:

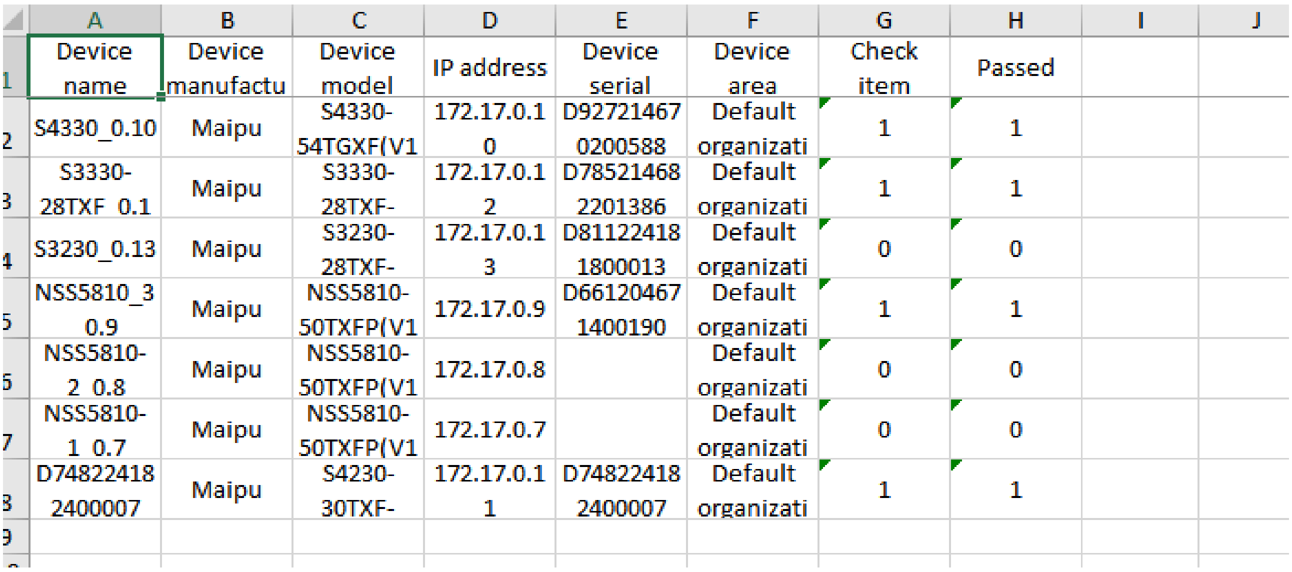


Results

☐	Device Name	Vendor	Model	IP Address	Serial Number	Organization	Check Item	Passed	Description	Operation
☐	S4330_0.10	Maipu	S4330…	172.17.0.10	D9272146702…	Default orga…	1	1		Details
☐	S3330-28TXF…	Maipu	S3330…	172.17.0.12	D7852146822…	Default orga…	1	1		Details
☐	S3230_0.13	Maipu	S3230…	172.17.0.13	D8112241818…	Default orga…	0	0	Device offline	Details
☐	NSS5810_3_0.9	Maipu	NSS5…	172.17.0.9	D6612046714…	Default orga…	1	1		Details
☐	NSS5810-2_0.8	Maipu	NSS5…	172.17.0.8		Default orga…	0	0	Channel un…	Details
☐	NSS5810-1_0.7	Maipu	NSS5…	172.17.0.7		Default orga…	0	0	Device offline	Details

Total 7 Items, Selected 0 Items

Figure 9. 2.3.10 Export check results

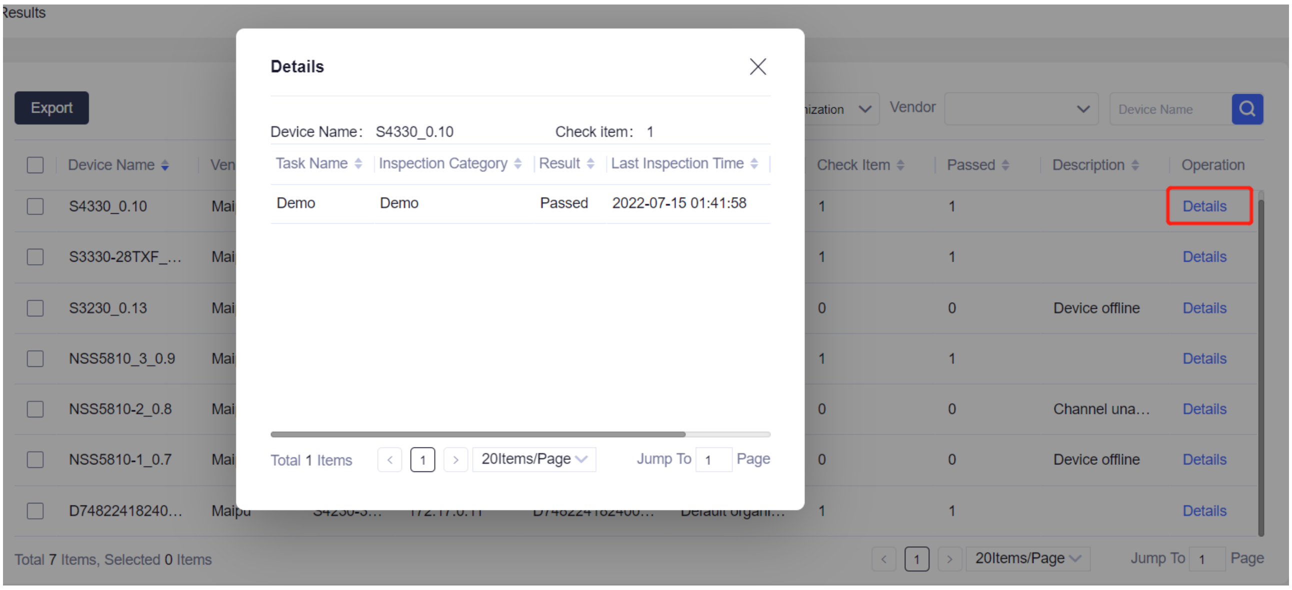


	A	B	C	D	E	F	G	H	I	J
1	Device name	Device manufactu	Device model	IP address	Device serial	Device area	Check item	Passed		
2	S4330_0.10	Maipu	S4330-54TGXF(V1	172.17.0.10	D927214670200588	Default organizati	1	1		
3	S3330-28TXF 0.1	Maipu	S3330-28TXF-	172.17.0.12	D785214682201386	Default organizati	1	1		
4	S3230_0.13	Maipu	S3230-28TXF-	172.17.0.13	D811224181800013	Default organizati	0	0		
5	NSS5810_3 0.9	Maipu	NSS5810-50TXFP(V1	172.17.0.9	D661204671400190	Default organizati	1	1		
6	NSS5810-2 0.8	Maipu	NSS5810-50TXFP(V1	172.17.0.8		Default organizati	0	0		
7	NSS5810-1 0.7	Maipu	NSS5810-50TXFP(V1	172.17.0.7		Default organizati	0	0		
8	D748224182400007	Maipu	S4230-30TXF-	172.17.0.11	D748224182400007	Default organizati	1	1		
9										

Figure 9. 2.3.11 Exported files

Details of check results:

Click the **Details** button to view the details of the corresponding check results, as shown in the following figure:



Device Name: S4330_0.10   Check item: 1

Task Name	Inspection Category	Result	Last Inspection Time
Demo	Demo	Passed	2022-07-15 01:41:58

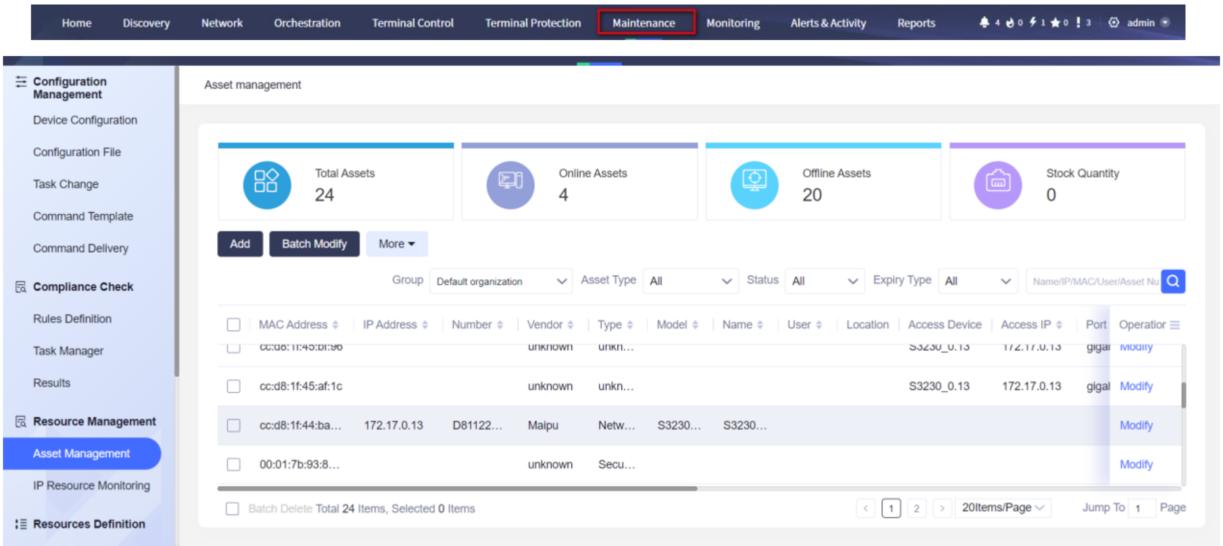
Device Name	Check Item	Passed	Description	Operation
S4330_0.10	1	1		Details
S3330-28TXF_...	1	1		Details
S3230_0.13	0	0	Device offline	Details
NSS5810_3_0.9	1	1		Details
NSS5810-2_0.8	0	0	Channel una...	Details
NSS5810-1_0.7	0	0	Device offline	Details
D74822418240...	1	1		Details

Figure 9. 2.3.12 Check result details

9.3 Resource Management

9.3.1 Asset Management

Click "Maintenance" in the menu bar above, and select "Asset Management" in the left side of the page to enter the **Asset Management** panel, as shown in the following figure:



Total Assets 24
Online Assets 4
Offline Assets 20
Stock Quantity 0

Group: Default organization Asset Type: All Status: All Expiry Type: All

MAC Address	IP Address	Number	Vendor	Type	Model	Name	User	Location	Access Device	Access IP	Port	Operation
cc:d8:1f:45:af:1c			unknown	unkn...					S3230_0.13	172.17.0.13	gigal	Modify
cc:d8:1f:44:ba...	172.17.0.13	D81122...	Maipu	Netw...	S3230...	S3230...						Modify
00:01:7b:93:8...			unknown	Secu...								Modify

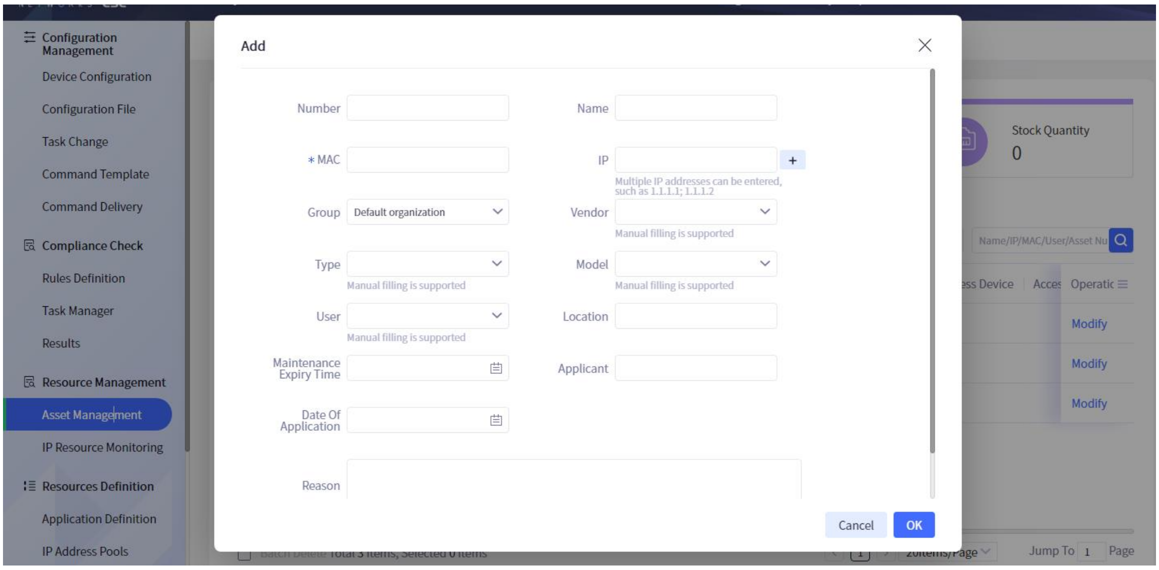
Total 24 Items, Selected 0 Items

Figure 9.3.1.1 Enter the asset management

The user can view the current total assets, online assets, offline assets, stock quantity and the details of each asset through the page.

Add assets

Click **Add** to open the **Add** dialog box, fill in the asset number, name, MAC address, IP address, organization, and other details, and click **OK** to save the new asset.

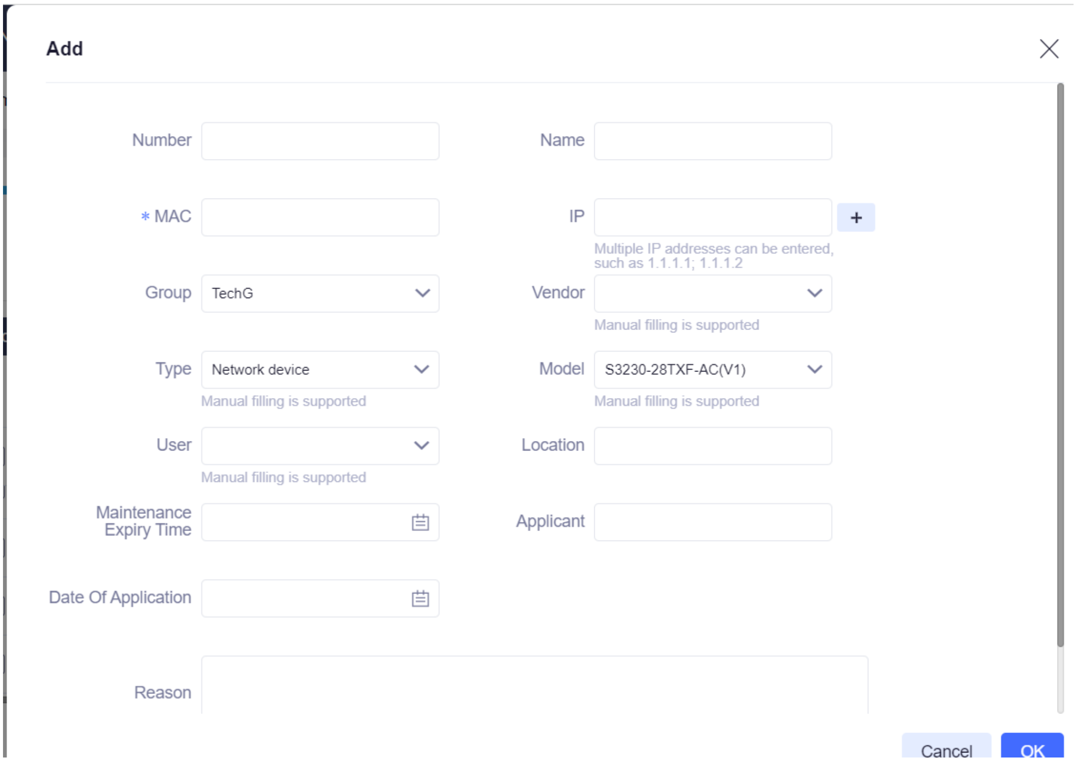


Group: Default organization

Figure 9.3.1.2 Add assets

Modify asset

Select the desired asset in the page, click **Modify** to open the **Modify** dialog box, where you can modify the details of the asset, and click **OK** to save the modified asset.


Add
Number
Name
* MAC
IP
+
Multiple IP addresses can be entered, such as 1.1.1.1; 1.1.1.2
Vendor
Manual filling is supported
Manual filling is supported
Manual filling is supported
User
Manual filling is supported
Location
Maintenance Expiry Time
Applicant
Date Of Application
Reason
Cancel
OK

Group: TechG

Type: Network device

Model: S3230-28TXF-AC(V1)

Figure 9.3.1.3 Modify assets

Batch modify assets

Select the desired asset in batch on the page, click **Batch Modify** to open the **Batch Modify** dialog box, where you can modify the details of the assets, and click **OK** to save all the modified assets.

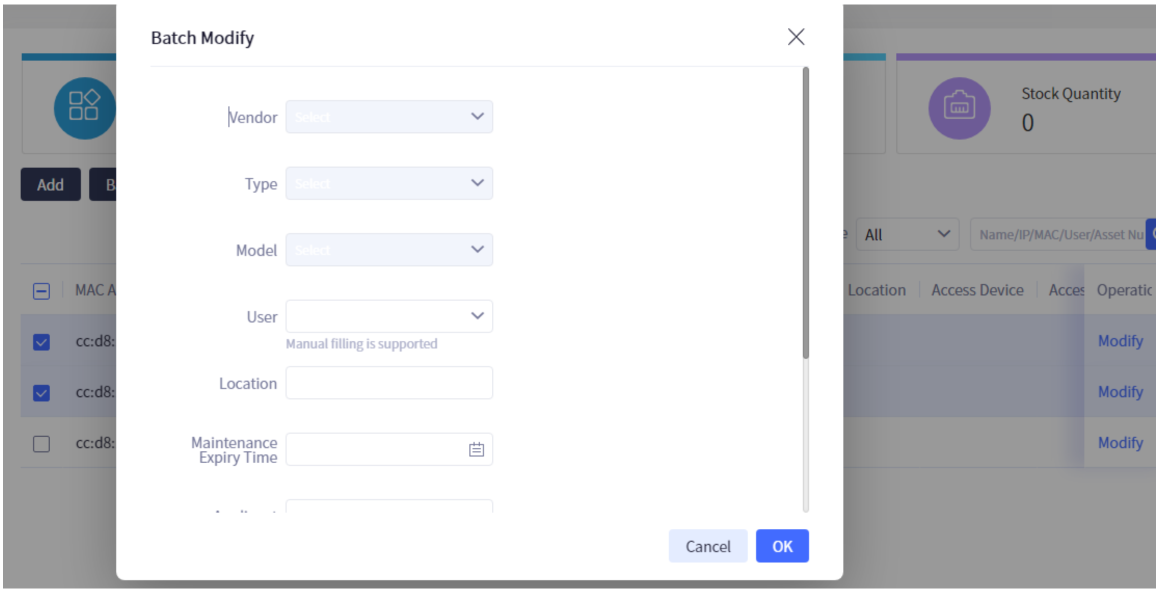


Figure 9.3.1.4 Batch modify assets

Import assets

Click **More** to open the drop-down box, and click **Import** to open the **Import** dialog box, as shown in the following figure:

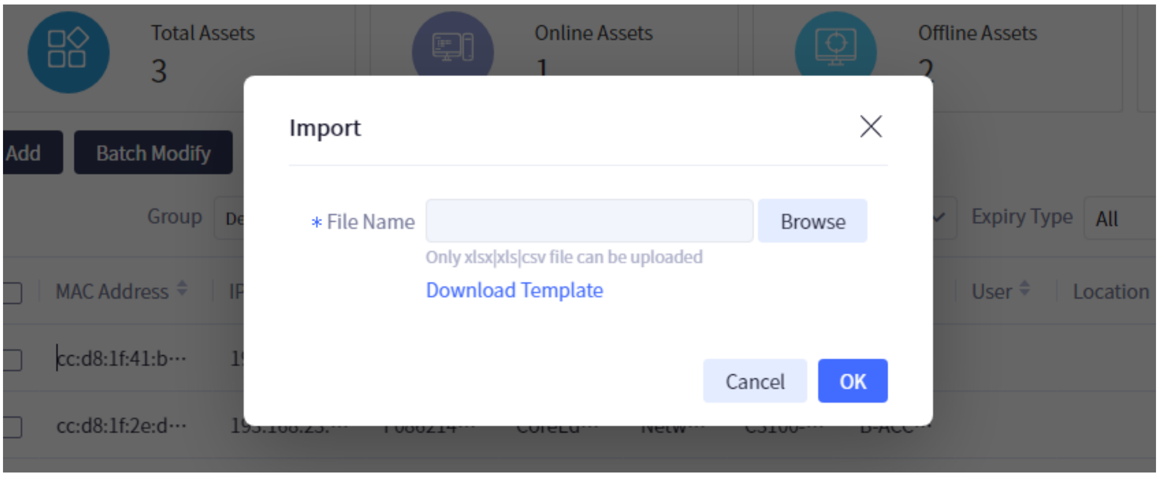
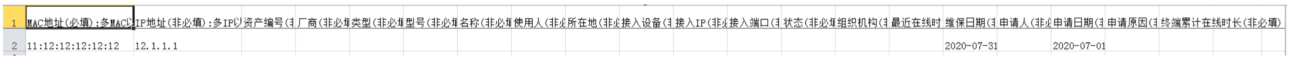


Figure 9.3.1.5 Import assets

Click the **Download Template** button to download the import template, as shown in the following figure.

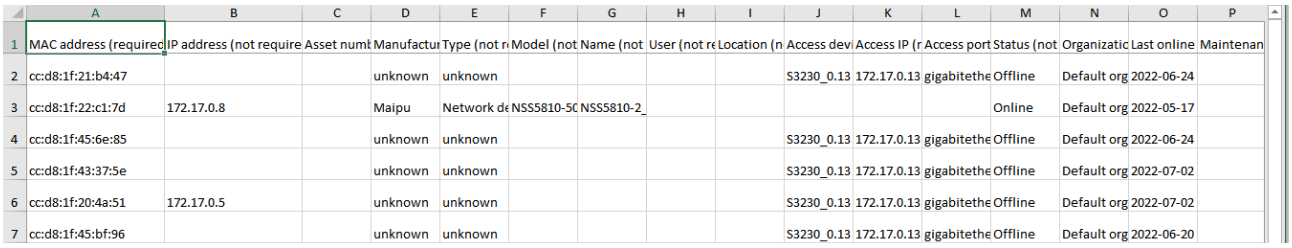


1	MAC地址(必填):多MAC以	IP地址(非必填):多IP以	资产编号(	厂商(非必填	类型(非必填	型号(非必填	名称(非必填	使用人(非必	所在地(非必	接入设备(	接入IP(非必	接入端口(	状态(非必填	组织机构(	最近在线时	维保日期(	申请人(非必	申请日期(	申请原因(	终端累计在线时长(非必填)
2	11:12:12:12:12:12	12.1.1.1														2020-07-31		2020-07-01		

Figure 9.3.1.6 Download import asset template

Export assets

Click **More** to open the drop-down box, and click **Export** to export and generate the table file, as shown in the following figure:



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	MAC address (required	IP address (not require	Asset numb	Manufactur	Type (not r	Model (not	Name (not	User (not re	Location (n	Access devi	Access IP (r	Access port	Status (not	Organizatic	Last online	Maintenan
2	cc:d8:1f:21:b4:47			unknown	unknown					S3230_0.13	172.17.0.13	gigabitethe	Offline	Default org	2022-06-24	
3	cc:d8:1f:22:c1:7d	172.17.0.8		Maipu	Network de	NSS5810-5C	NSS5810-2_						Online	Default org	2022-05-17	
4	cc:d8:1f:45:6e:85			unknown	unknown					S3230_0.13	172.17.0.13	gigabitethe	Offline	Default org	2022-06-24	
5	cc:d8:1f:43:37:5e			unknown	unknown					S3230_0.13	172.17.0.13	gigabitethe	Offline	Default org	2022-07-02	
6	cc:d8:1f:20:4a:51	172.17.0.5		unknown	unknown					S3230_0.13	172.17.0.13	gigabitethe	Offline	Default org	2022-07-02	
7	cc:d8:1f:45:bf:96			unknown	unknown					S3230_0.13	172.17.0.13	gigabitethe	Offline	Default org	2022-06-20	

Figure 9.3.1.7 Export assets

Custom properties

Click **More** to open the drop-down box, click **Custom Properties** to generate a **Custom Properties** dialog box, as shown in the following figure:

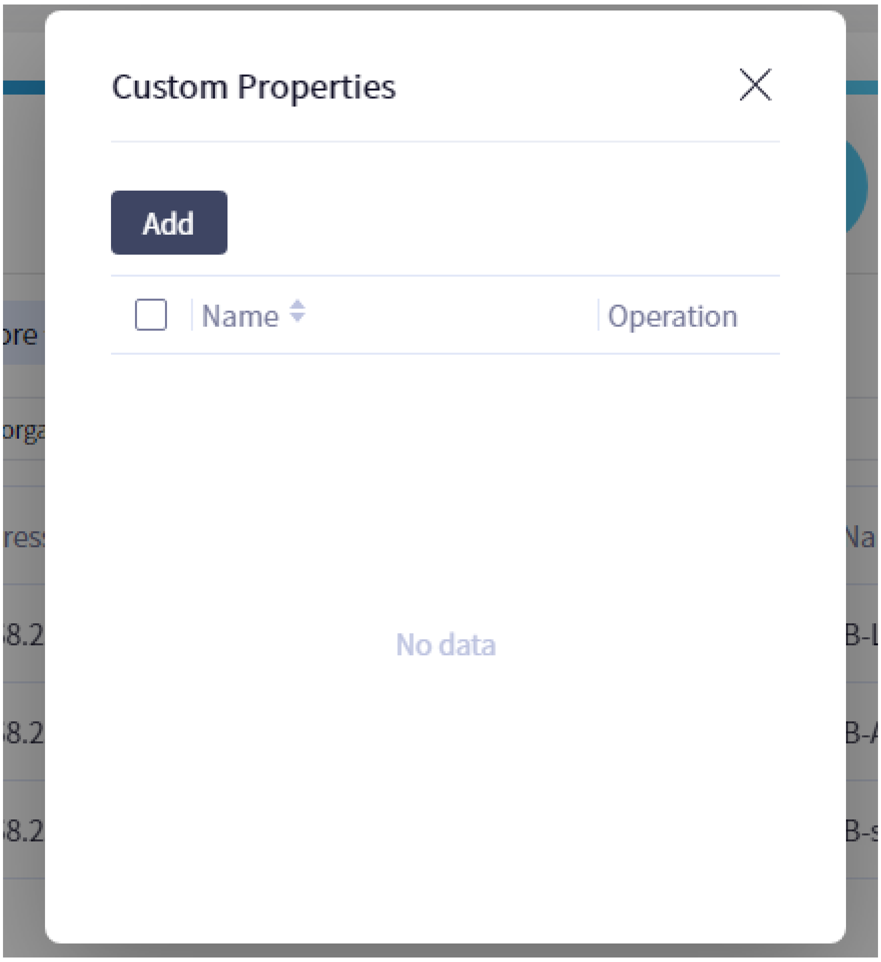
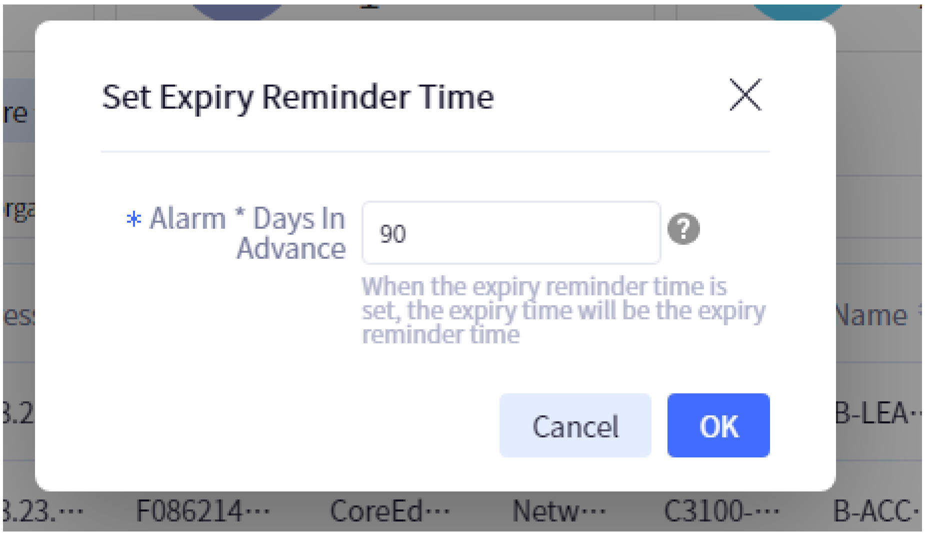


Figure 9.3.1.8 Custom properties

Set the expiry reminder time

Click the **More** button to open the drop-down box, click the **Set Expiry Reminder Time** button to generate the **Set Expiry Reminder Time** window, and then set the expiry time, as shown in the following figure:



Alarm * Days In Advance: 90

When the expiry reminder time is set, the expiry time will be the expiry reminder time

Figure 9.3.1.9 Set the expiry reminder time

Terminal MAC Merging

Select at least two desired assets, click **More** to open the drop-down box, and click **Terminal MAC Merging** to generate terminal MAC merging of assets, as shown in the following figure:

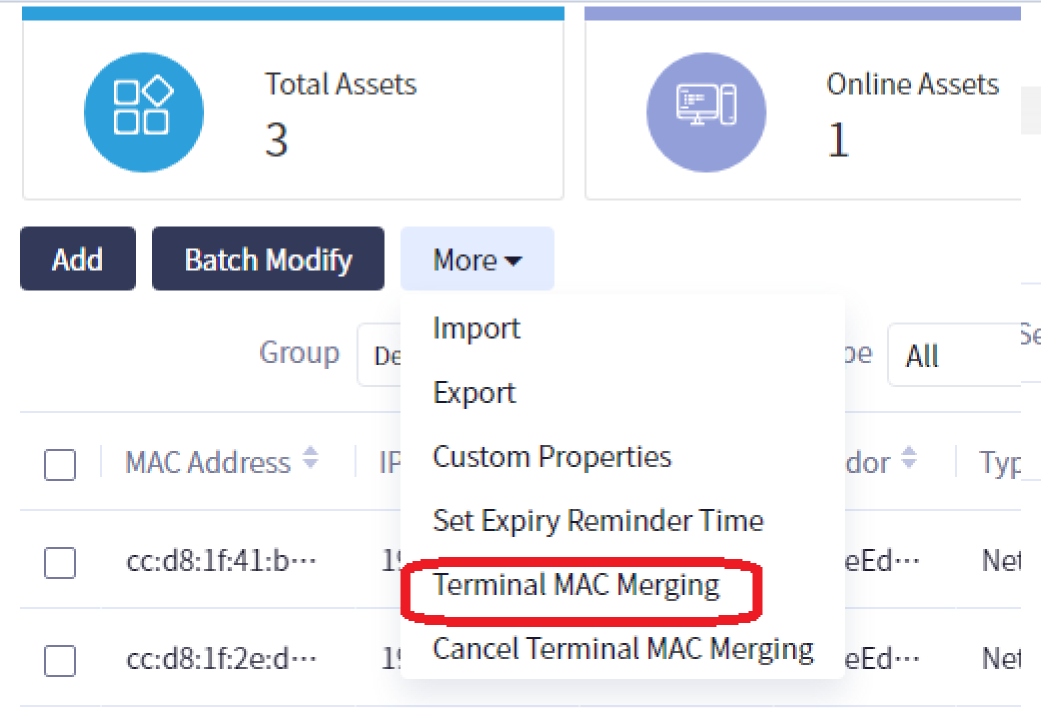


Figure 9.3.1.10 Terminal mac merging

Cancel terminal MAC merging

Select at least two desired assets, click **More** to open the drop-down box, and click **Cancel Terminal MAC Merging** to cancel terminal MAC consolidation of assets, as shown in the following figure:

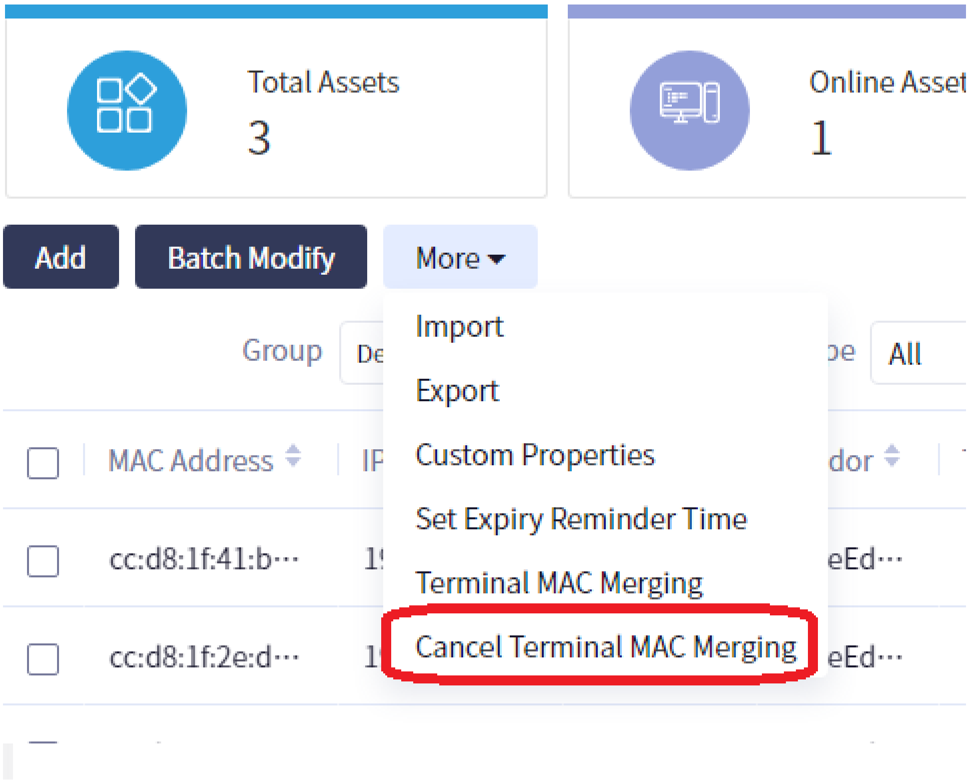
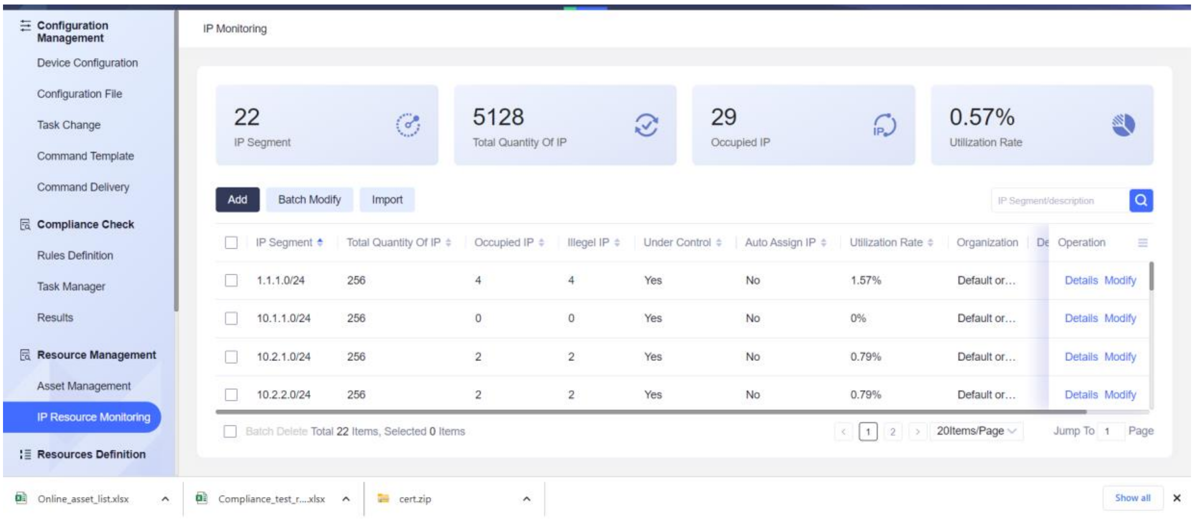


Figure 9.3.1.11 Cancel terminal MAC merging

9.3.2 IP Resource Monitoring

Click "Maintenance" in the menu bar above, and select "IP Resource Monitoring" on the left side of the page to enter the **IP Monitoring** panel, as shown in the following figure:



22 IP Segment | 5128 Total Quantity Of IP | 29 Occupied IP | 0.57% Utilization Rate

☐	IP Segment	Total Quantity Of IP	Occupied IP	Illegel IP	Under Control	Auto Assign IP	Utilization Rate	Organization	De	Operation
☐	1.1.1.0/24	256	4	4	Yes	No	1.57%	Default or...		Details Modify
☐	10.1.1.0/24	256	0	0	Yes	No	0%	Default or...		Details Modify
☐	10.2.1.0/24	256	2	2	Yes	No	0.79%	Default or...		Details Modify
☐	10.2.2.0/24	256	2	2	Yes	No	0.79%	Default or...		Details Modify

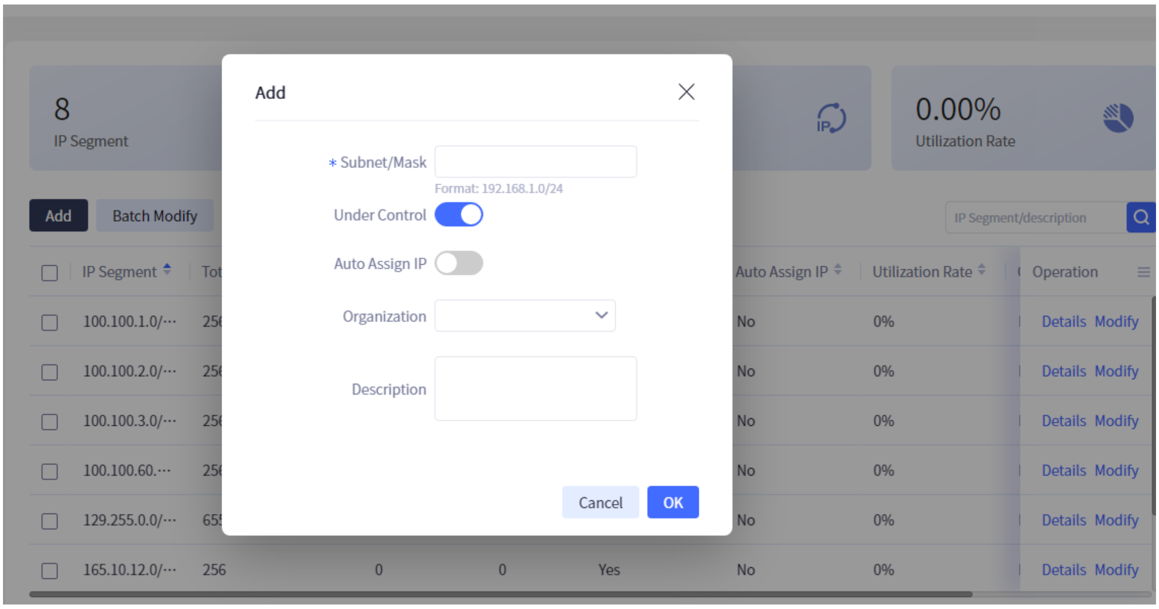
☐ Batch Delete Total 22 Items, Selected 0 Items ‹ 1 2 › 20Items/Page Jump To 1 Page

Figure 9.3.2.1 Enter IP resource monitoring

You can view the current total number of IP network segments, the total number of IP addresses, the number of used IPs, and the IP utilization rate, as well as the details of each IP segment.

Add IP segment

Click **Add** to open the **Add** dialog box, fill in the subnet/mask, add a description, and click **OK** to save the new IP network segment.

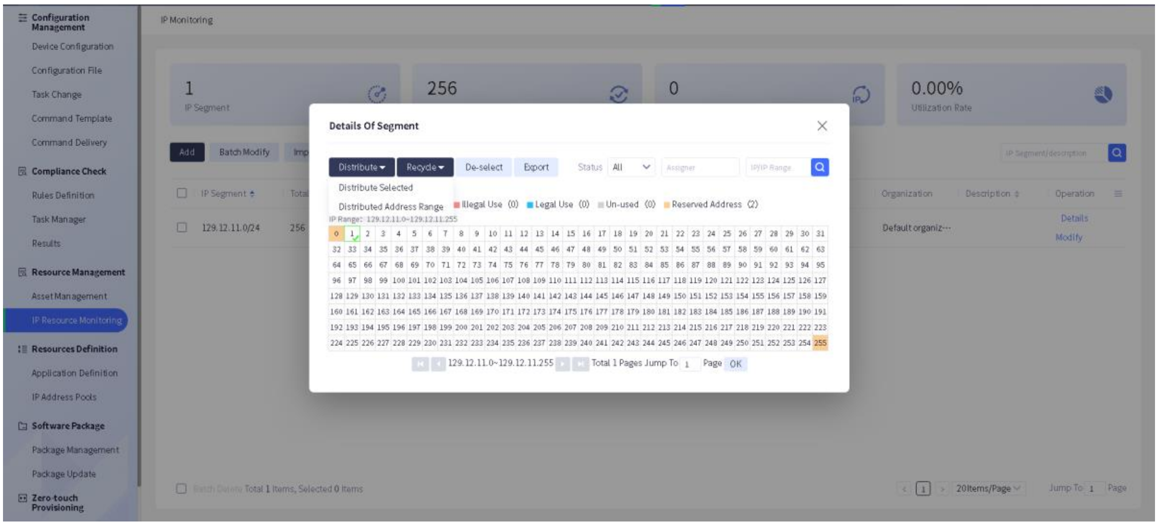


Add

* Subnet/Mask
Format: 192.168.1.0/24
Under Control ●
Auto Assign IP ○
Organization
Description

Figure 9.3.2.2 Add IP resource

Since the IPs assigned to the service network segment address pool does not include the service gateway IP, the terminal scanning will use the gateway IP as the source address for scanning, which conflicts with the IP address of the device network. Therefore, you need to click **Details** here to select the corresponding gateway address, as shown in the following figure:



1 IP Segment

256

0

0.00% Utilization Rate

IP Segment	Total	Organization	Description	Operation
129.12.11.0/24	256	Default organiz···		Details Modify

Total 1 Items, Selected 0 Items

Status: All

IP Range: 129.12.11.0~129.12.11.255

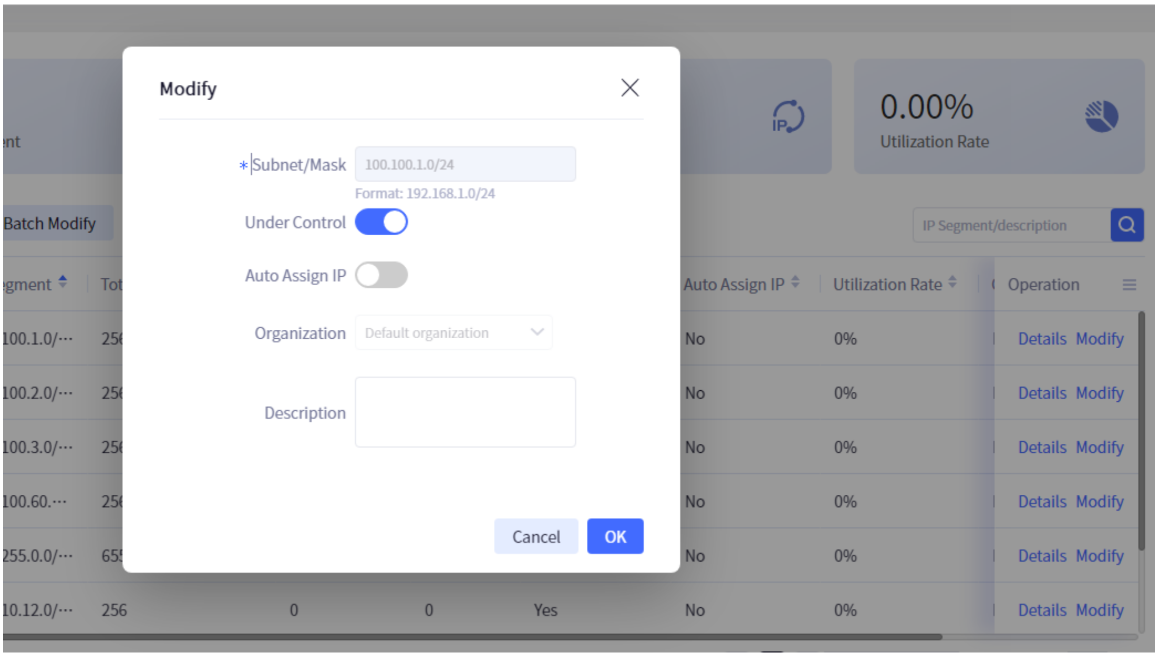
0	1 ✓	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60	61	62	63
64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95
96	97	98	99	100	101	102	103	104	105	106	107	108	109	110	111	112	113	114	115	116	117	118	119	120	121	122	123	124	125	126	127
128	129	130	131	132	133	134	135	136	137	138	139	140	141	142	143	144	145	146	147	148	149	150	151	152	153	154	155	156	157	158	159
160	161	162	163	164	165	166	167	168	169	170	171	172	173	174	175	176	177	178	179	180	181	182	183	184	185	186	187	188	189	190	191
192	193	194	195	196	197	198	199	200	201	202	203	204	205	206	207	208	209	210	211	212	213	214	215	216	217	218	219	220	221	222	223
224	225	226	227	228	229	230	231	232	233	234	235	236	237	238	239	240	241	242	243	244	245	246	247	248	249	250	251	252	253	254	255

129.12.11.0~129.12.11.255 Total 1 Pages Jump To 1 Page OK

Select the corresponding gateway address and click **Distribute Selected**.

Modify an IP segment

Select the desired IP segment on the page, click **Modify** to open the **Modify** dialog box, where you can modify the details of the IP segment, and click **OK** to save the modified IP segment.



0.00% Utilization Rate

*Subnet/Mask: 100.100.1.0/24

Format: 192.168.1.0/24

Under Control: on

Auto Assign IP: off

Organization: Default organization

Description:

gment	Tot				Auto Assign IP	Utilization Rate	Operation
100.1.0/···	25				No	0%	Details Modify
100.2.0/···	25				No	0%	Details Modify
100.3.0/···	25				No	0%	Details Modify
100.60.···	25				No	0%	Details Modify
255.0.0/···	65				No	0%	Details Modify
10.12.0/···	256	0	0	Yes	No	0%	Details Modify

Figure 9.3.2.3 Modify IP segment

Import IP segment

Click the **Import** button to open the **Import** dialog box, as shown in the following figure

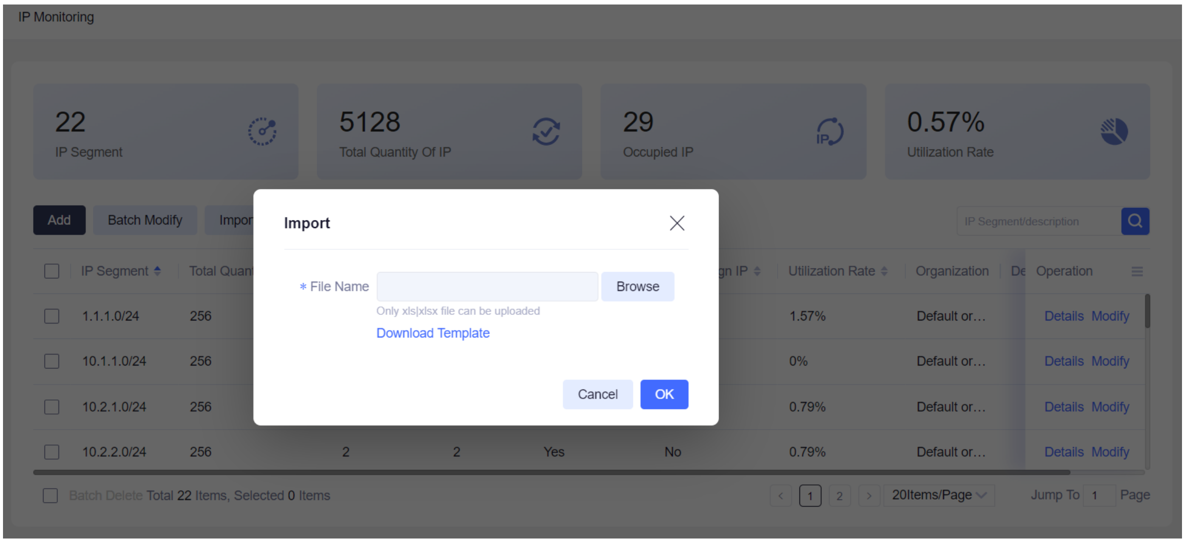
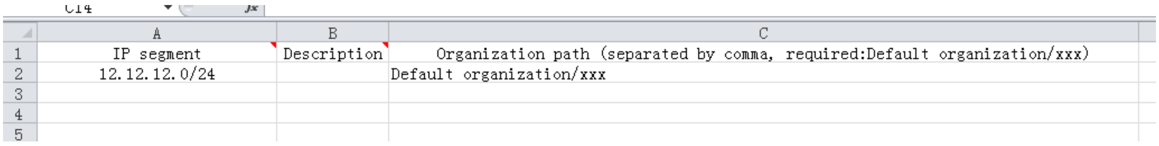

IP Monitoring
22
IP Segment
5128
Total Quantity Of IP
29
Occupied IP
0.57%
Utilization Rate
Add
Batch Modify
Impor
IP Segment/description
Import
* File Name
Browse
Only xls|xlsx file can be uploaded
Download Template
Cancel
OK
IP Segment
Total Quan
gn IP
Utilization Rate
Organization
De
Operation
1.1.1.0/24 256 1.57% Default or… Details Modify
10.1.1.0/24 256 0% Default or… Details Modify
10.2.1.0/24 256 0.79% Default or… Details Modify
10.2.2.0/24 256 2 2 Yes No 0.79% Default or… Details Modify
Batch Delete Total 22 Items, Selected 0 Items
1
2
20Items/Page
Jump To
1
Page

Figure 9.3.2.4 Import IP segment

Click the **Download Template** button to download the import template, as shown in the following figure.

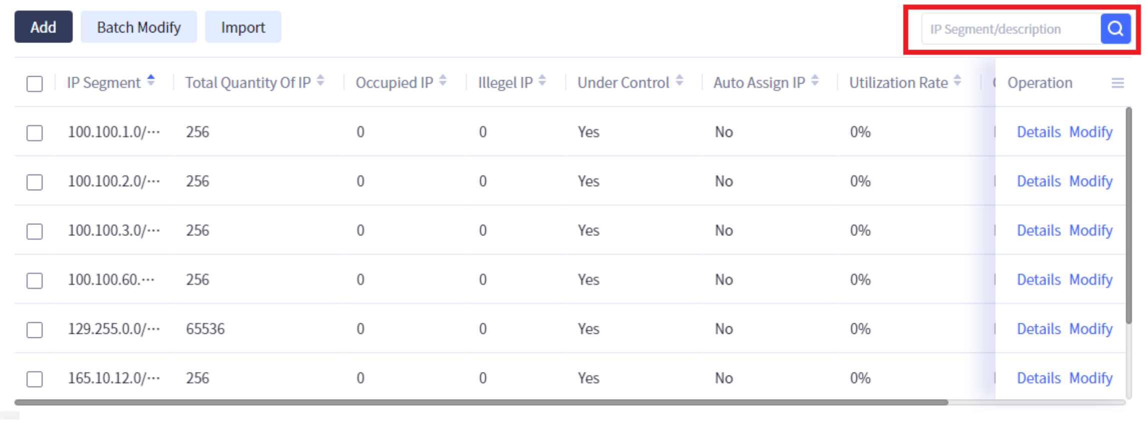


	A	B	C
1	IP segment	Description	Organization path (separated by comma, required:Default organization/xxx)
2	12.12.12.0/24		Default organization/xxx
3			
4			
5			

Figure 9.3.2.5 Download IP segment import template

Query IP segment

At the top of the IP segment management view is the IP segment query module, as shown in the following figure. You can query according to the name/description of the IP segment. The query content will be displayed in the organization list below, as shown in the following figure.



☐	IP Segment	Total Quantity Of IP	Occupied IP	Illegal IP	Under Control	Auto Assign IP	Utilization Rate	Operation
☐	100.100.1.0/···	256	0	0	Yes	No	0%	Details Modify
☐	100.100.2.0/···	256	0	0	Yes	No	0%	Details Modify
☐	100.100.3.0/···	256	0	0	Yes	No	0%	Details Modify
☐	100.100.60.···	256	0	0	Yes	No	0%	Details Modify
☐	129.255.0.0/···	65536	0	0	Yes	No	0%	Details Modify
☐	165.10.12.0/···	256	0	0	Yes	No	0%	Details Modify

Figure 9.3.2.6 Query IP segment

9.4 Software Package

9.4.1 Software Package Management

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

"Package Management" page, as follows:

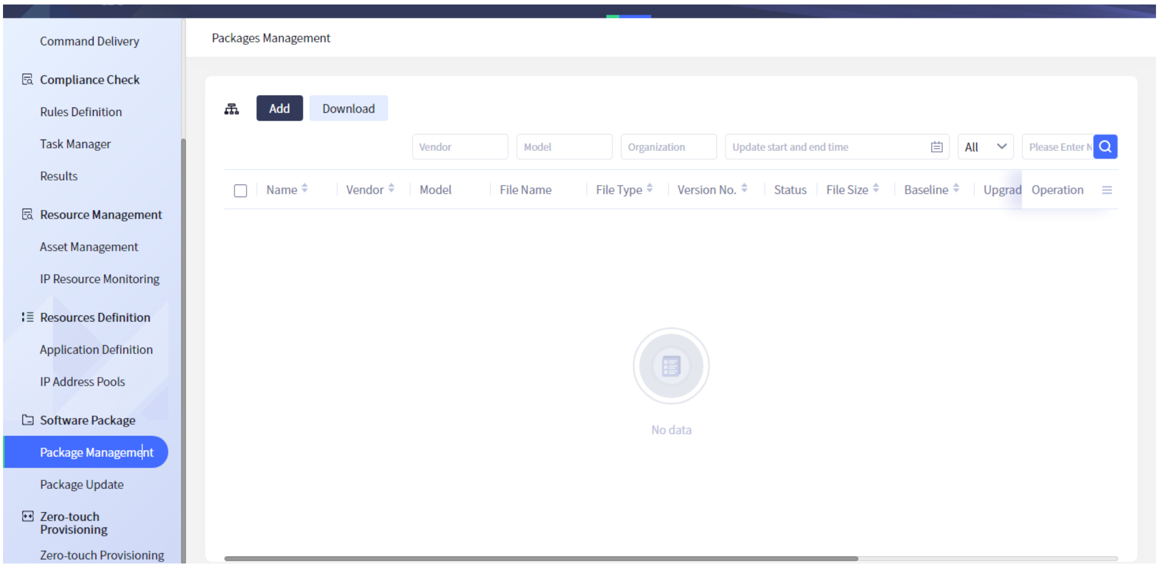


Figure 9.4.1.1 Software package management

Package list:

Open the "Package Management" interface to display all software packages in the system by default, and display the name, vendor, 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 various query criteria to query specific software packages conveniently and quickly. Enter the corresponding query criteria in the "Package Query" panel, and then click the **Query** button to query all software packages according to the vendor information, device model, affiliated organization, advanced query, update start time, update end time and other fields; Advanced query can be performed 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 following figure, all software package information with the vendor information of "Maipu", device model of "SM4120", affiliated organization of the headquarters, and the name of "test" are found, and sorted according to the software package name:

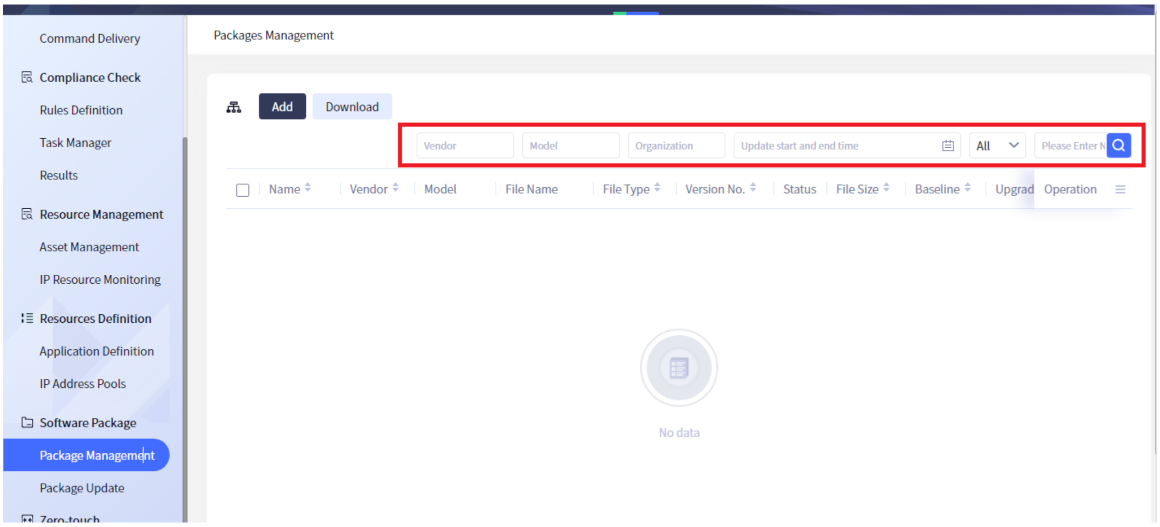


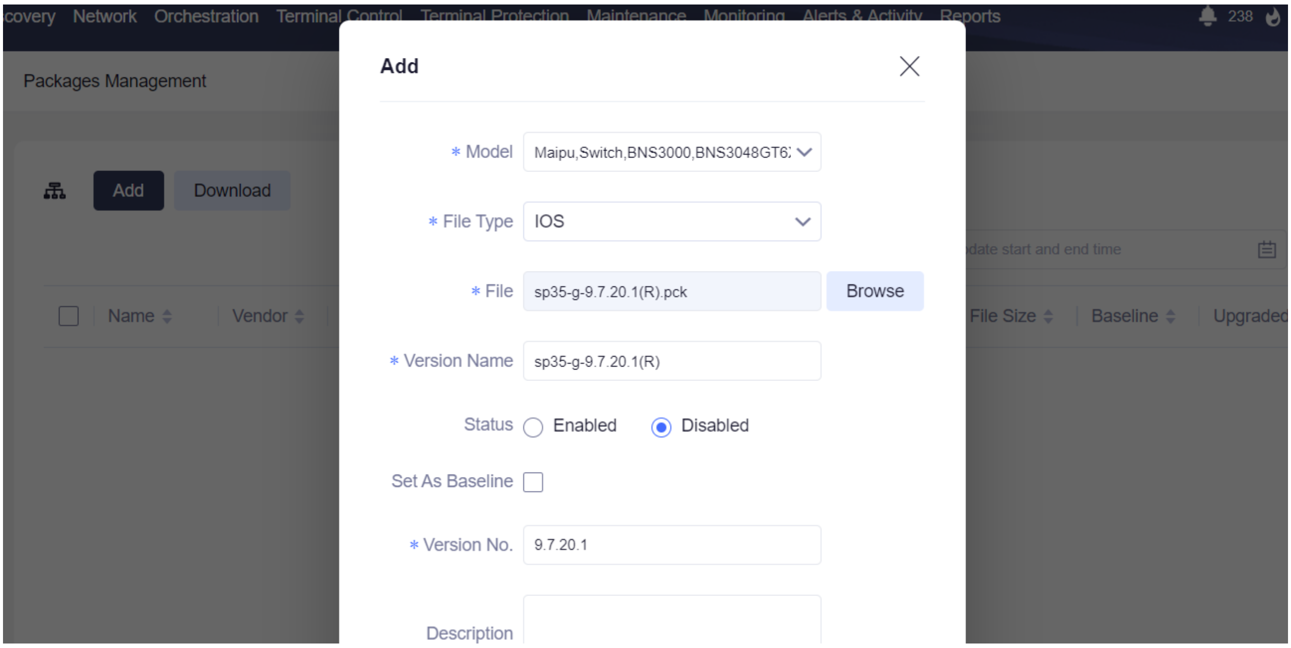
Figure 9.4.1.2 Package query and sorting

Caution

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

Add package:

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



* Model: Maipu,Switch,BNS3000,BNS3048GT6

* File Type: IOS

* File: sp35-g-9.7.20.1(R).pck

* Version Name: sp35-g-9.7.20.1(R)

Status: ○ Enabled ● Disabled

Set As Baseline ☐

* Version No.: 9.7.20.1

Description:

Figure 9.4.1.3 Add package

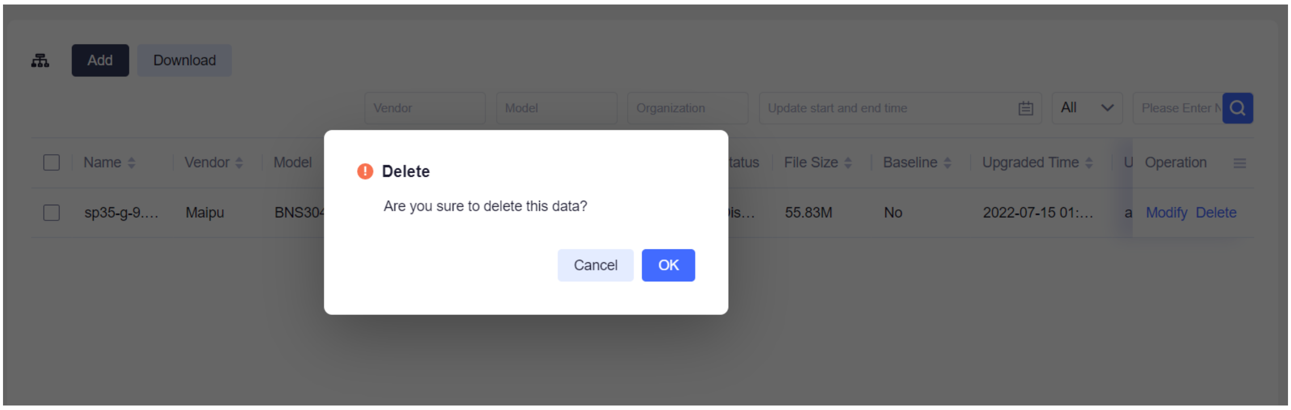
Click **OK** to finish adding the software package. The process of modifying the software package is the same as above. Select the desired software package in the software package management list and click the **Modify** button.

Note

- Status: Enabled: the software package can be selected in the "Package Update" task; Disabled: the package cannot be selected in the "Package Update" task.
- When selecting a model for a new software package, you cannot select a model across vendors.
- At present, only ios and pkg support setting the baseline version. When the baseline set by the added device ios and pkg software package is inconsistent with the current software version of the device, a baseline inconsistency alarm will be sent. When upgrading the device software version, the alarm before it is consistent with the baseline will be eliminated.

Delete a package:

Select the desired software package in the software package management list, click the **Delete** button, and click **OK** to delete the software package that is no longer in use.



Delete

Are you sure to delete this data?

☐	Name	Vendor	Model	…tatus	File Size	Baseline	Upgraded Time	U	Operation
☐	sp35-g-9.…	Maipu	BNS304	…is…	55.83M	No	2022-07-15 01:…	a	Modify Delete

Figure 9.4.1.4 Delete package

Download package:

Select the desired package from the package management list, and then click the **Download** button to download the selected package.

9.4.2 Package Update

The package update management module can update software packages for specified devices, including adding, modifying, deleting, manually starting, stopping and refreshing software package update tasks, and querying software package update tasks.

Click "Maintenance" > "Software Package" > "Package Update" on the navigation bar at the top of the system to open the "Package Update " page, as follows:

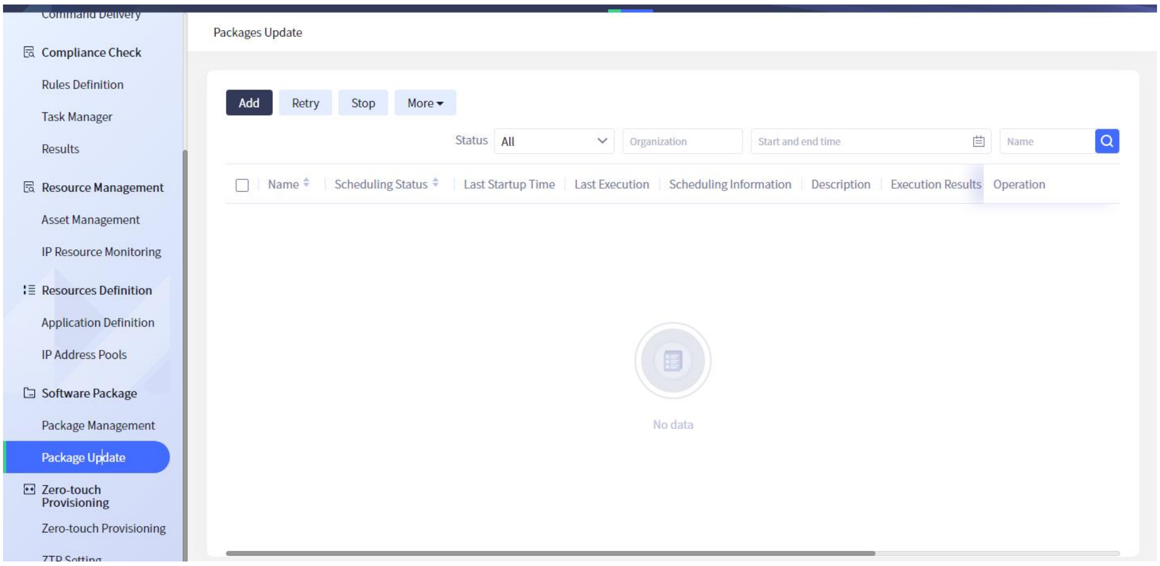


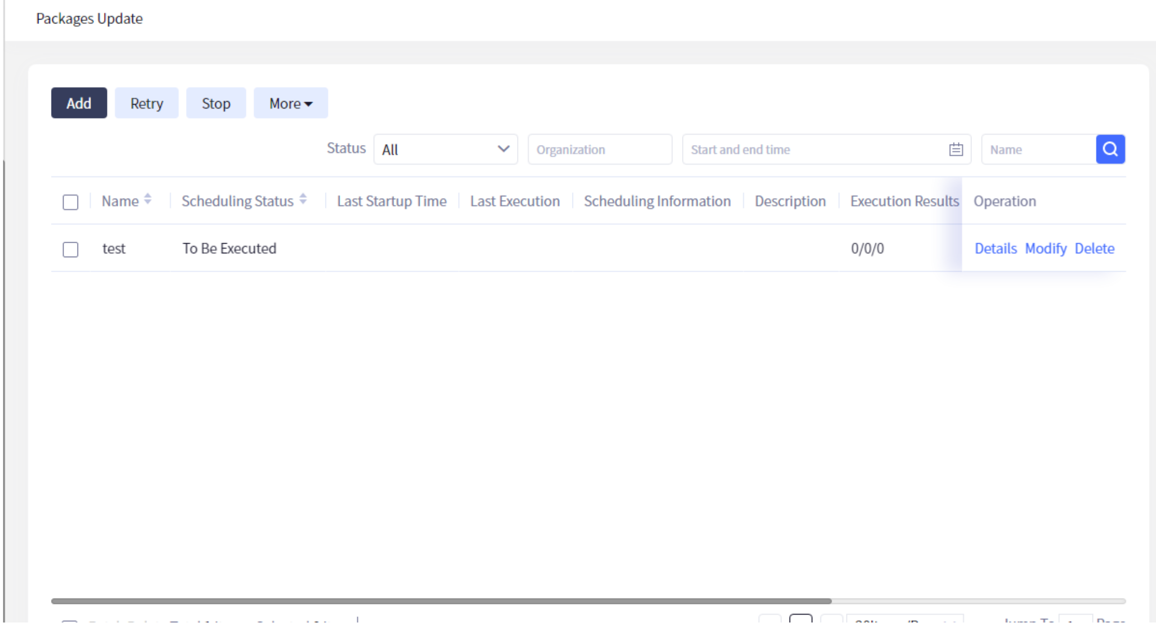
Figure 9.4.2.1 Package update task management

Task list:

Open the "Package Update" interface to display all software package update tasks in the system by default in pages, showing the name, status, last start time, last end time, scheduling information, description, recent execution, update user, organization, details, history and other information of each task.

This page provides various query criteria to query specific tasks conveniently and quickly. Enter the corresponding query criteria, and then click **Query** to query all tasks by name, status, organization, start time, end time and other fields. Click the "Organization" field at the head of the task list to sort the list data.

As shown in the following figure, all tasks with the name of "test" and the organization of "default organization" are found:



☐	Name	Scheduling Status	Last Startup Time	Last Execution	Scheduling Information	Description	Execution Results	Operation
☐	test	To Be Executed					0/0/0	Details Modify Delete

Figure 9.4.2.2 Query package update task

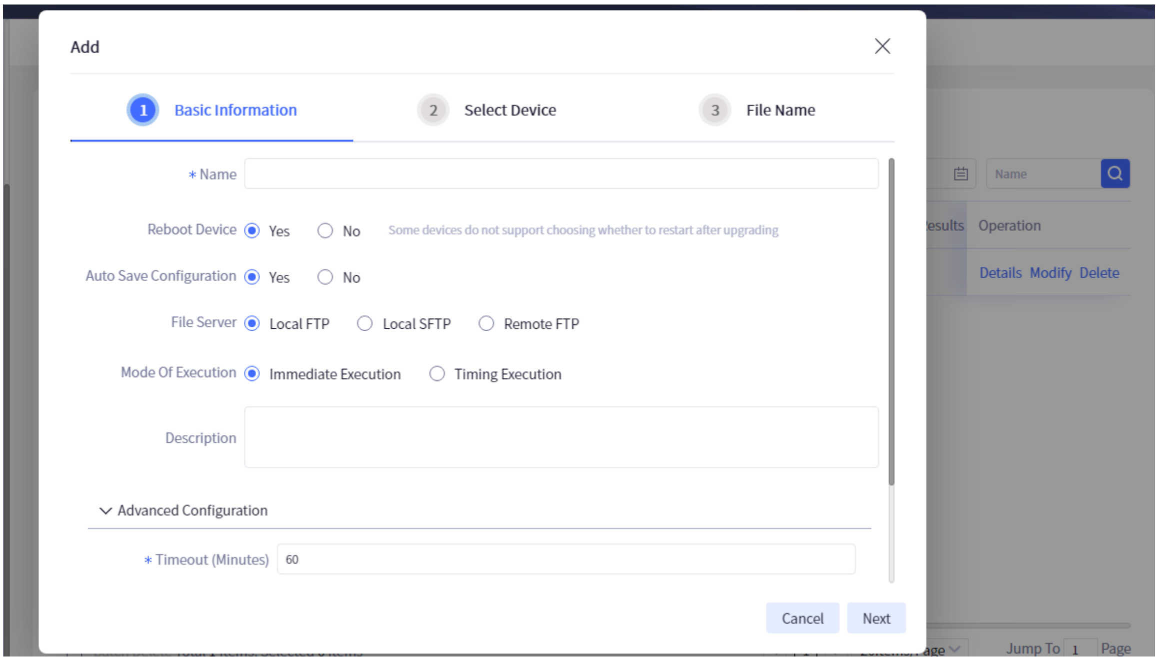
Caution

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

---

Add/modify task:

Click the **Add** button in the task list, or select a task and click the **Modify** button to open the "Add" window as shown in the following figure, fill in the task name and description, select whether to restart the device, select the file server, and select the execution mode. Select **Advanced Configuration** to set the timeout time, and select whether to delete files, whether to support VRF and other information.



* Name:

Reboot Device: ● Yes ○ No — Some devices do not support choosing whether to restart after upgrading

Auto Save Configuration: ● Yes ○ No

File Server: ● Local FTP ○ Local SFTP ○ Remote FTP

Mode Of Execution: ● Immediate Execution ○ Timing Execution

Description:

* Timeout (Minutes): 60

Figure 9.4.2.3 Step 1 of adding/modifying the task information

Caution

- The device concurrency of the current single task in the package update task is 5, and the task concurrency is 10.
- Default timeout is 60 minutes.
- By default, do not support VRF.

Auto delete file: The default value is "Yes". If the device storage space is insufficient, delete the existing package automatically and start to update the package. If "No" is selected, do not delete the file, but return an error message.

Reboot device: If this option is checked, the device will be restarted after the device software package is successfully updated. If the update fails, record the error message and do not restart the device.

File server: Configuration change uses the local FTP server for file transfer by default (the FTP password is the default value).

You can also use the remote FTP server for upgrading. When selecting the remote FTP server, you need to enter the FTP address, file name, file type (IOS, monitor, uboot, traitlibrary, package), user name and password.

Execution mode: When **Immediate Execution** is selected, the task can be executed immediately after the task information is configured; When timing execution is selected, execute the task after the set time period.

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

Timeout: When a task is executed, the task execution fails when the response time of the device exceeds the set timeout.

Support VRF: The default value is No. VRF is the VPN routing forwarding table. It is a special entity established and maintained by PE for directly connected sites.

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

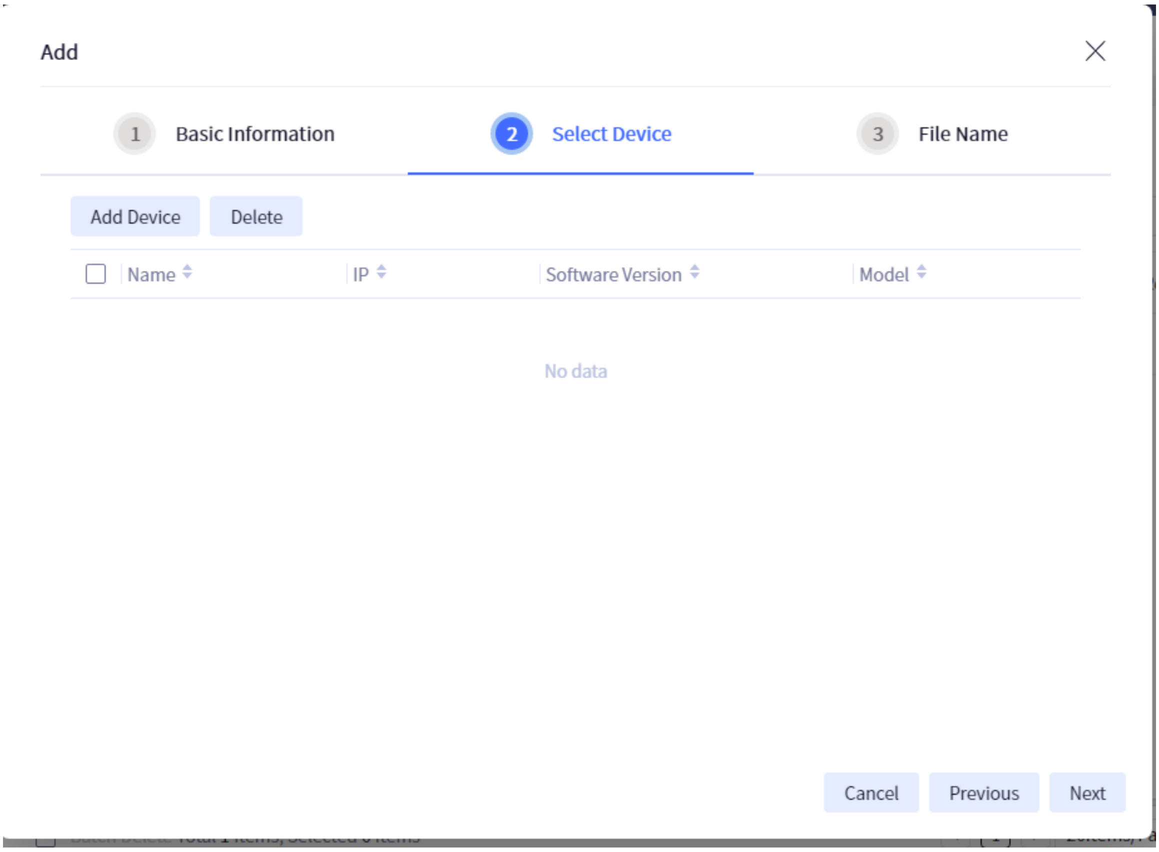
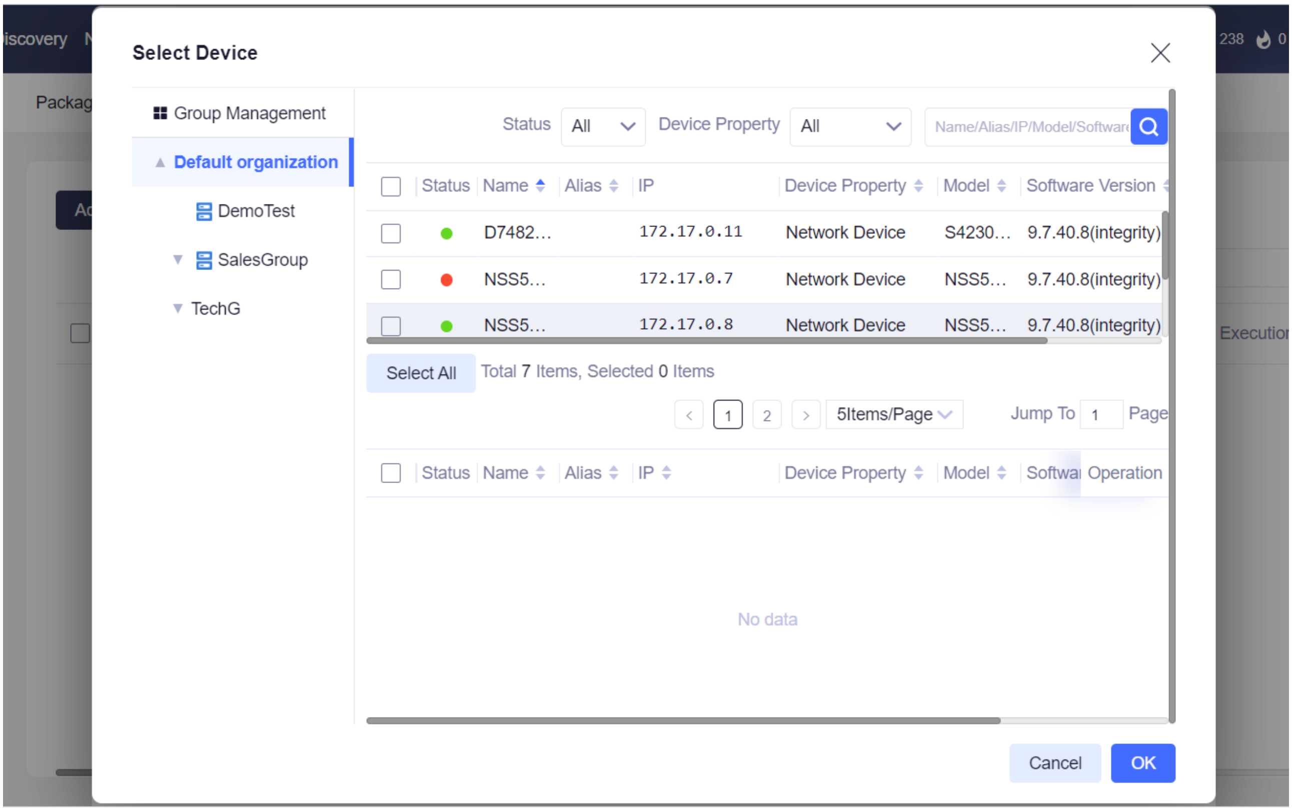


Figure 9.4.2.4 Step 2 of adding/modifying the task information

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



☐	Status	Name	Alias	IP	Device Property	Model	Software Version
☐	●	D7482…		172.17.0.11	Network Device	S4230…	9.7.40.8(integrity)
☐	●	NSS5…		172.17.0.7	Network Device	NSS5…	9.7.40.8(integrity)
☐	●	NSS5…		172.17.0.8	Network Device	NSS5…	9.7.40.8(integrity)

Total 7 Items, Selected 0 Items

‹ 1 2 › 5Items/Page Jump To 1 Page

☐	Status	Name	Alias	IP	Device Property	Model	Softwa	Operation

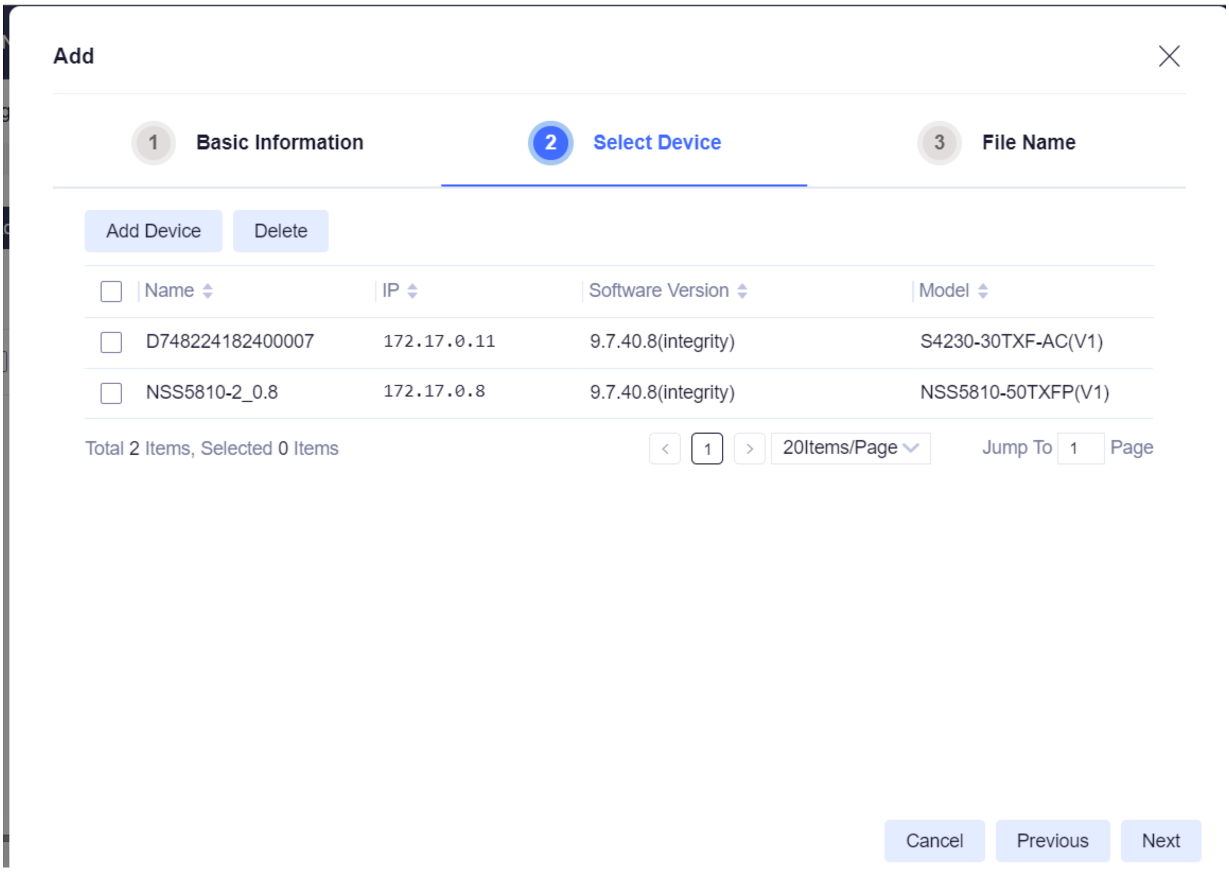
No data

Figure 9.4.2.5 Select devices

Note

- The selected devices have common software packages in software package management. Otherwise, the system cannot select a unified software upgrade package for them, and the software upgrade package will not be found in the "Select File " step.

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

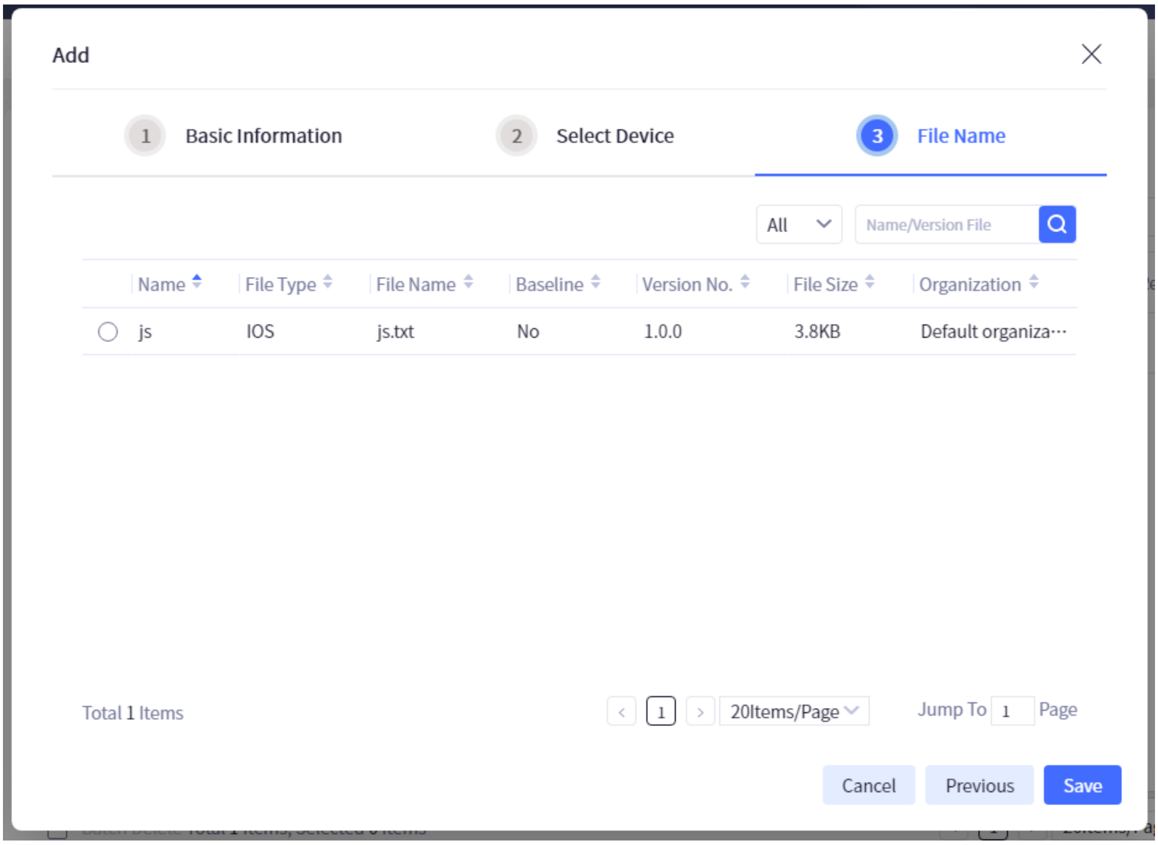


☐	Name	IP	Software Version	Model
☐	D748224182400007	172.17.0.11	9.7.40.8(integrity)	S4230-30TXF-AC(V1)
☐	NSS5810-2_0.8	172.17.0.8	9.7.40.8(integrity)	NSS5810-50TXFP(V1)

Total 2 Items, Selected 0 Items

Figure 9.4.2.6 Add/modify the task information

Click "Next" to enter the "Select file" window, as shown in the following figure:



	Name	File Type	File Name	Baseline	Version No.	File Size	Organization
○	js	IOS	js.txt	No	1.0.0	3.8KB	Default organiza···

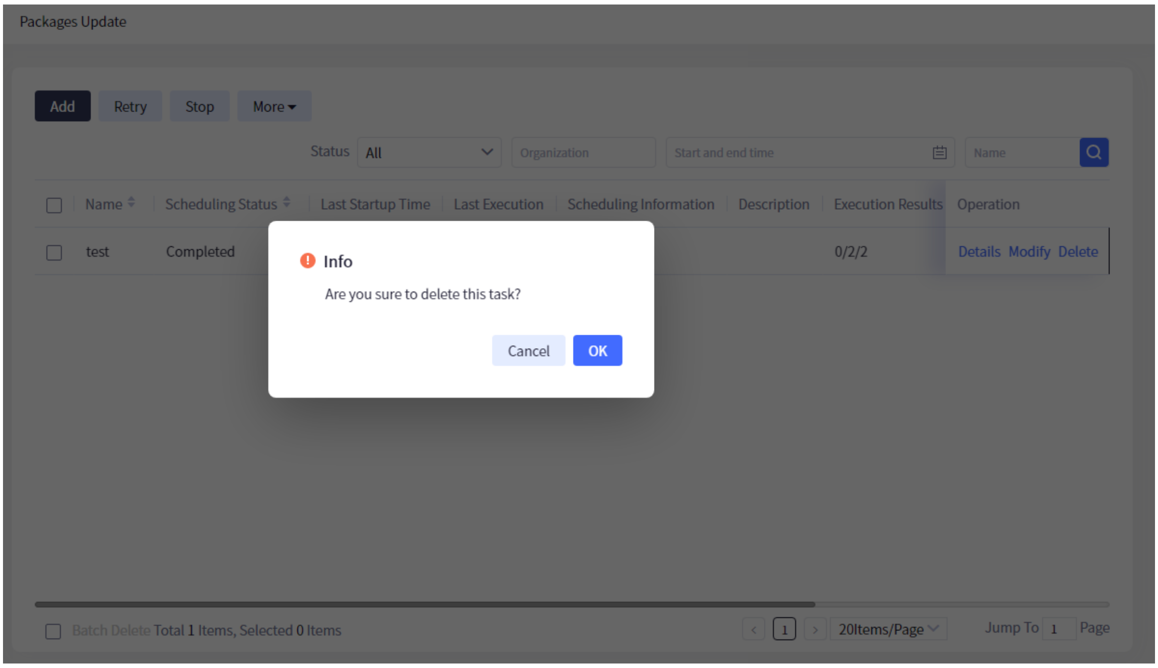
Figure 9.4.2.7 Add files

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

Click **Save** to complete the task of adding software package update, and the device starts to update the software package. The process of modification task is the same as above. Select the desired task in the task list and click **Modify** to modify the task information.

Delete task:

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



☐	Name	Scheduling Status	Last Startup Time	Last Execution	Scheduling Information	Description	Execution Results	Operation
☐	test	Completed					0/2/2	Details Modify Delete

Info

Are you sure to delete this task?

Figure 9.4.2.8 Delete the task information

Note

- The tasks in progress cannot be deleted or modified.

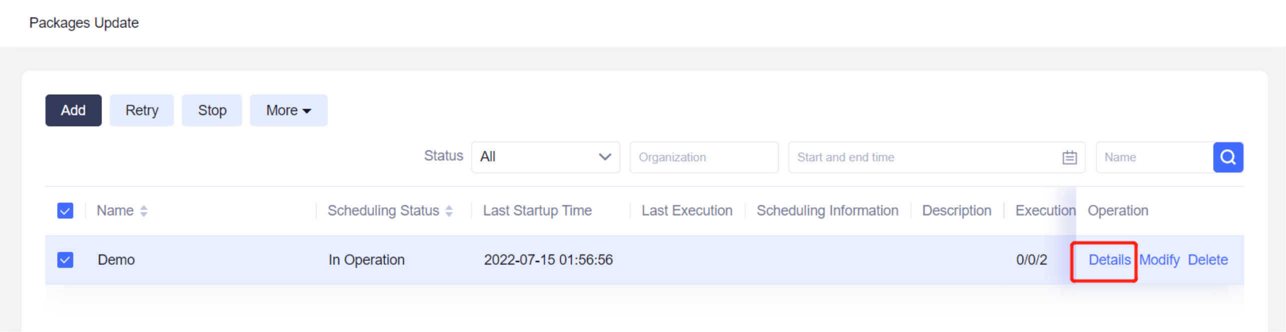
Manually start/stop task:

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

Select a stopped task and click the **Start Manually** button. The task can start running again from the beginning. At this time, the status of the task will change to "In progress".

View task details:

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

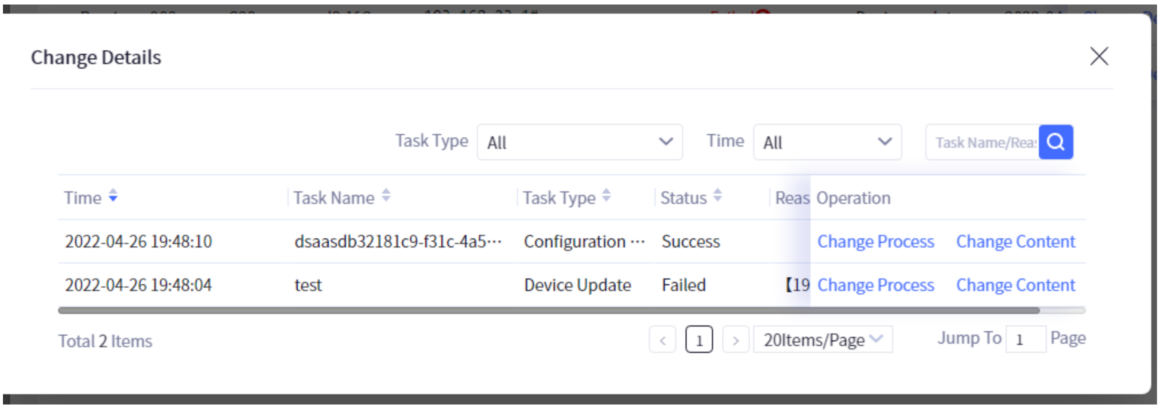


☑	Name	Scheduling Status	Last Startup Time	Last Execution	Scheduling Information	Description	Execution	Operation
☑	Demo	In Operation	2022-07-15 01:56:56				0/0/2	Details Modify Delete

Figure 9.4.2.9 Task details

The "Task Details" interface displays different devices under the same task in pages, showing the device name, scheduling status, start time, end time, scheduling information, description, scheduling results, update user, organization, operation and other information.

Click "Details" of any device update in the task details list to open the "Execution Details" window of the device, showing the detailed process of the device update, as shown below:



Time	Task Name	Task Type	Status	Reas	Operation
2022-04-26 19:48:10	dsaasdb32181c9-f31c-4a5···	Configuration ···	Success		Change Process Change Content
2022-04-26 19:48:04	test	Device Update	Failed	[19	Change Process Change Content

Figure 9.4.2.10 Execution details of the device update

The "Management" interface also provides operations such as backup, comparison, addition, editing, recovery, baseline setting and deletion of configuration files, as shown in the figure

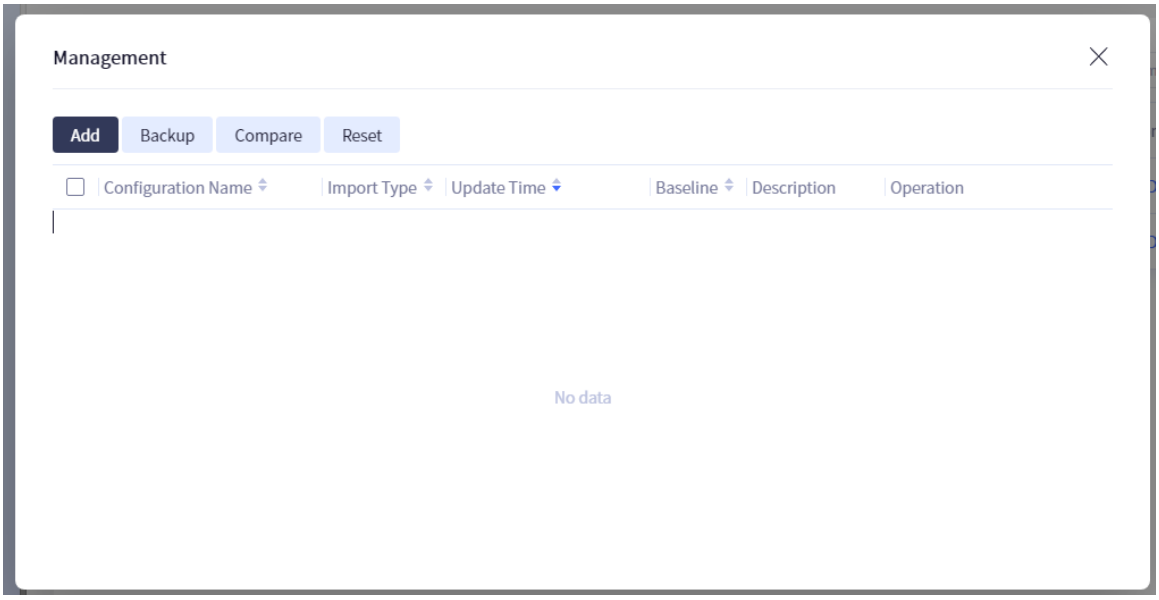


Figure 9.4.2.11 Management

Possible package update failures:

Note

- Task execution failed. **connect/transfer timeout** is reported in the details.
- Cause: When discovering the device, it is discovered through the device management address that the management address of the network management server and the device is reachable, but it is not reachable with the default routing egress interface address of the device. The task selects FTP and SFTP servers. When the device downloads a file as a client, it communicates through the default routing egress interface address, and the file transmission will fail.
- Judgment method: log in to the device and ping the address of the network management server on the device. The Ping fails; The ping can succeed when the management address serves as the source address
- Solution: specify the source address of ftp/sftp transmission on the device as the address accessible to the network management server. For example, configure the following commands 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
```

9.5 Zero-touch Provisioning

The provisioning settings are divided into DHCP and mail provisioning settings.

9.5.1 DHCP Provisioning Setting

Before DHCP provisioning, you need to set the DHCP provisioning address pool on the DHCP server configuration page. Click "Maintenance" > "Zero-Touch Provisioning" - > "ZTP Setting" > "Add" on the navigation bar at the top of the system.

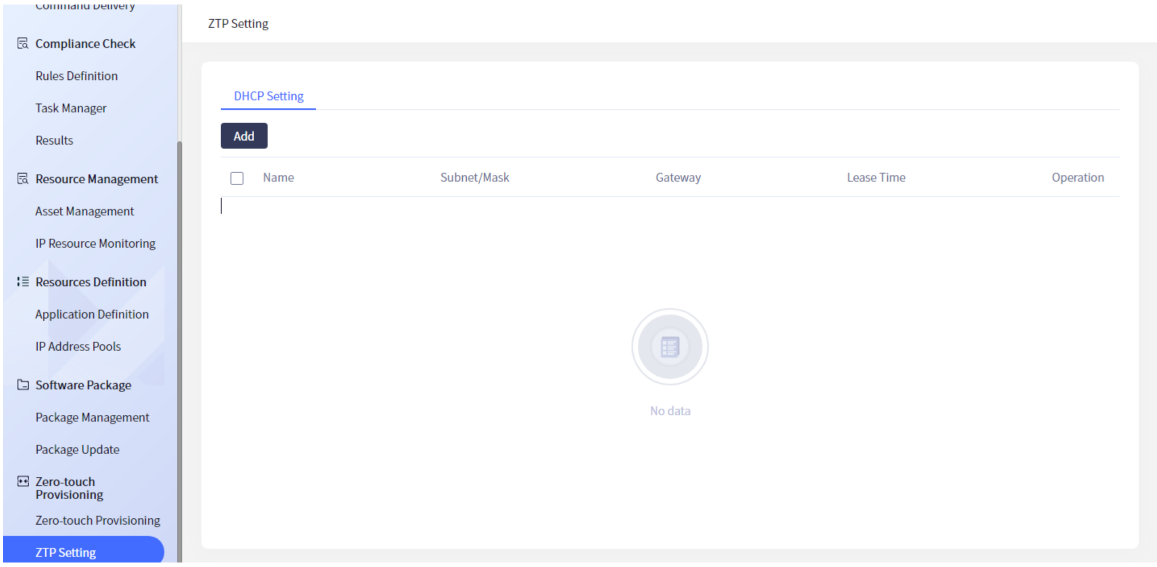


Figure 9.5.2.1 DHCP provisioning setting interface

Click "Add" to open the following interface, where you can enter the name, subnet/mask, address range, gateway and fixed term. The DHCP address pool must be set to a fixed term for DHCP provisioning. Gateway cannot be included in the address range.

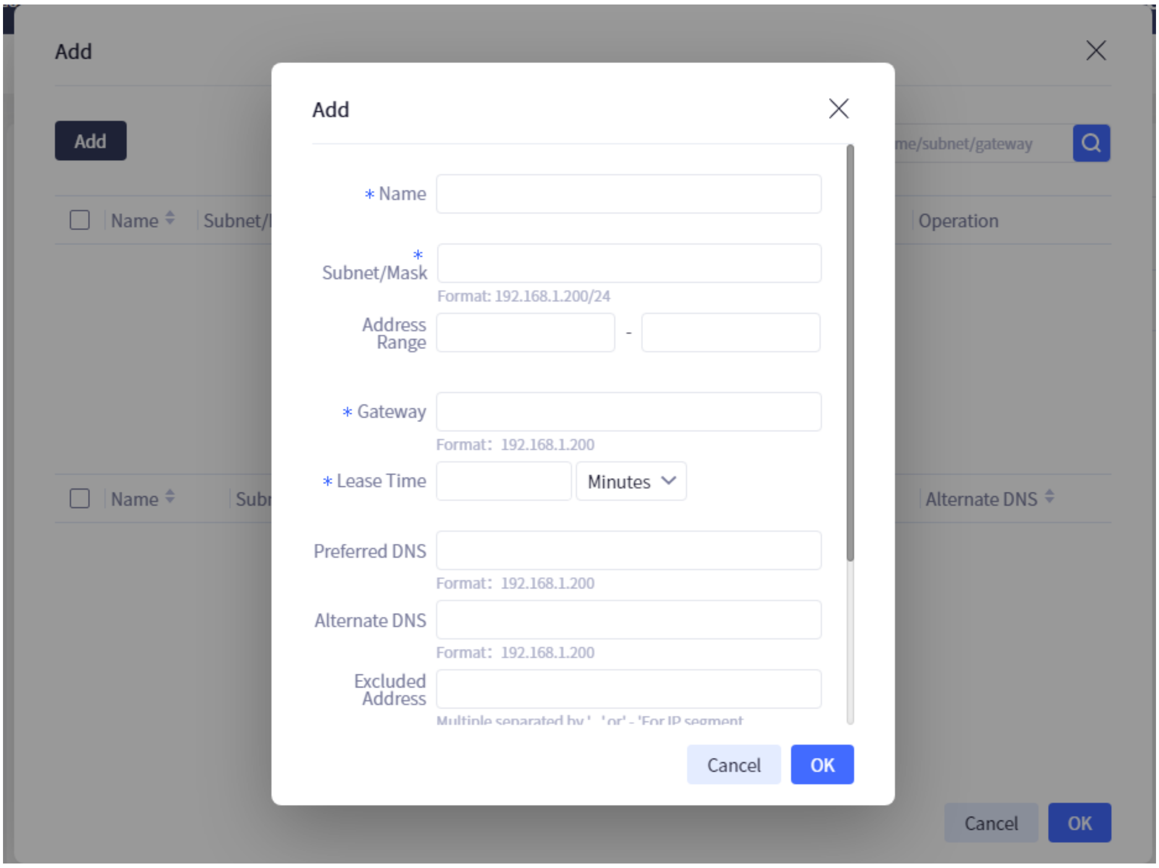
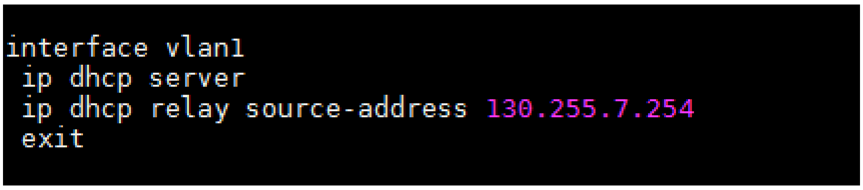


Figure 9.5.2.2 The “Add” interface

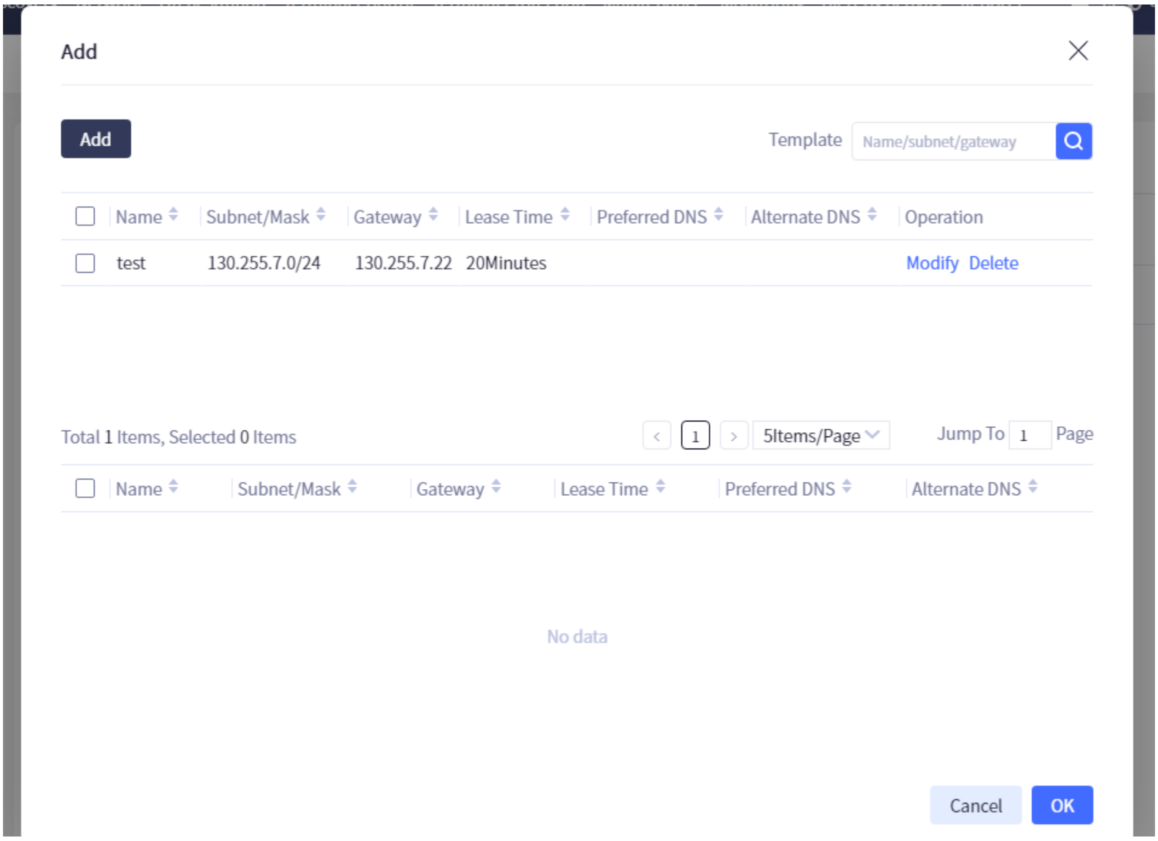
After setting successfully, as shown in the following figure, the gateway content needs to be configured in DHCP RELAY on the device side. Note: the DHCP relay configuration of different devices may be different. Please refer to the device configuration for specific settings, as shown in the following figure.



```
interface vlan1
 ip dhcp server
 ip dhcp relay source-address 130.255.7.254
 exit
```

Figure 9.5.2.3

Add the address pool set in the DHCP server to the DHCP provisioning setting, and the DHCP provisioning setting is completed, as shown in the following figure.



☐	Name	Subnet/Mask	Gateway	Lease Time	Preferred DNS	Alternate DNS	Operation
☐	test	130.255.7.0/24	130.255.7.22	20Minutes			Modify Delete

Total 1 Items, Selected 0 Items

☐	Name	Subnet/Mask	Gateway	Lease Time	Preferred DNS	Alternate DNS

No data

Figure 9.5.2.4

9.6 Provisioning Template

Click "Maintenance" - > "Zero-Touch Provisioning" - > "Zero-Touch Provisioning" on the navigation bar at the top of the system, as shown in the following figure

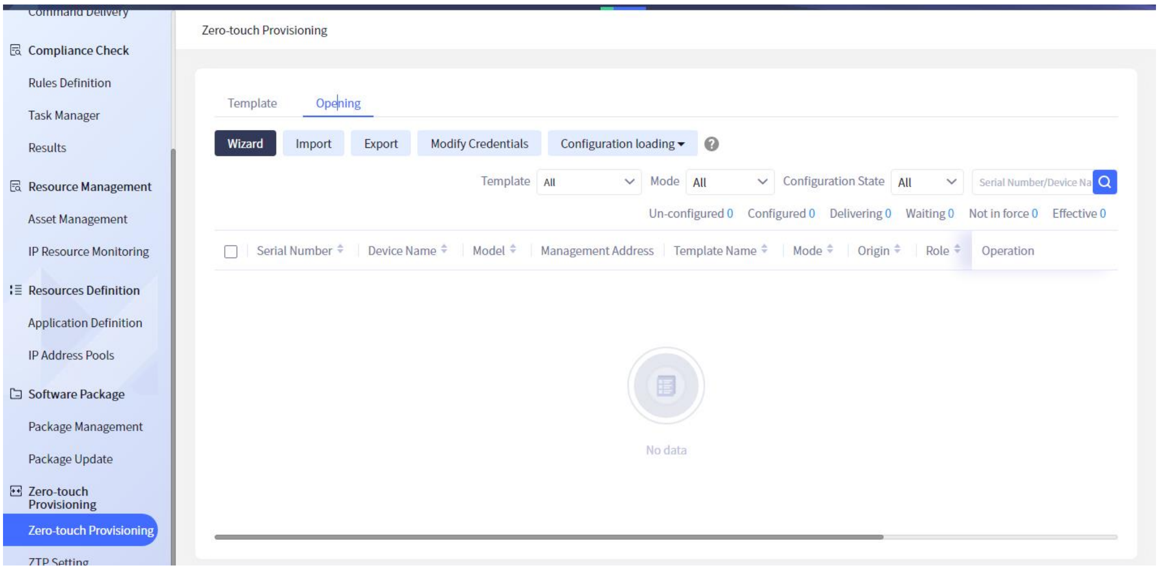
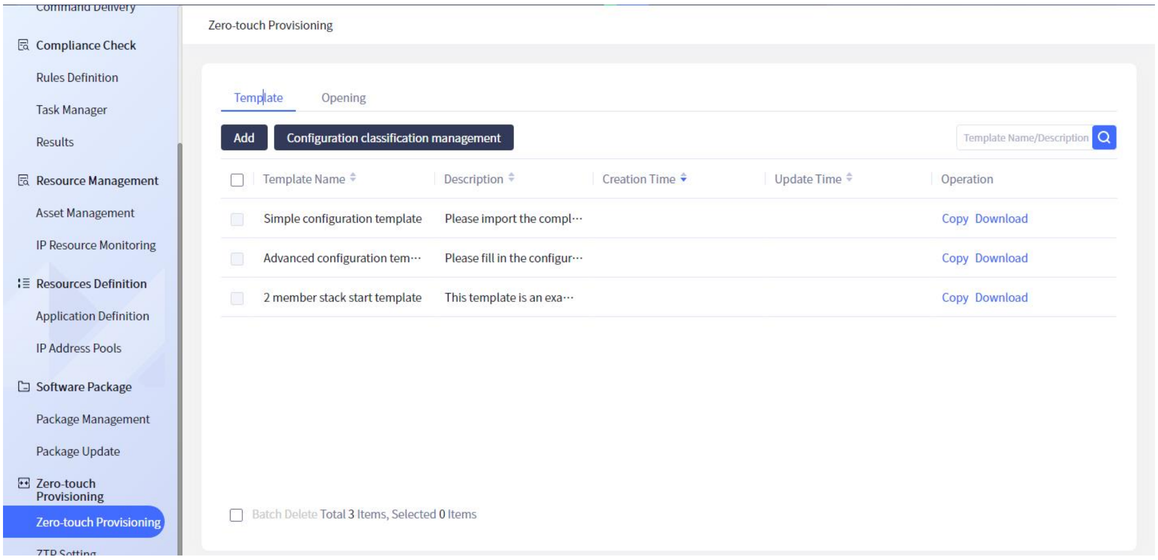


Figure 9.6.1.

Click **Template** to open the template setting interface, where you can modify and add templates.



☐	Template Name	Description	Creation Time	Update Time	Operation
☐	Simple configuration template	Please import the compl···			Copy Download
☐	Advanced configuration tem···	Please fill in the configur···			Copy Download
☐	2 member stack start template	This template is an exa···			Copy Download

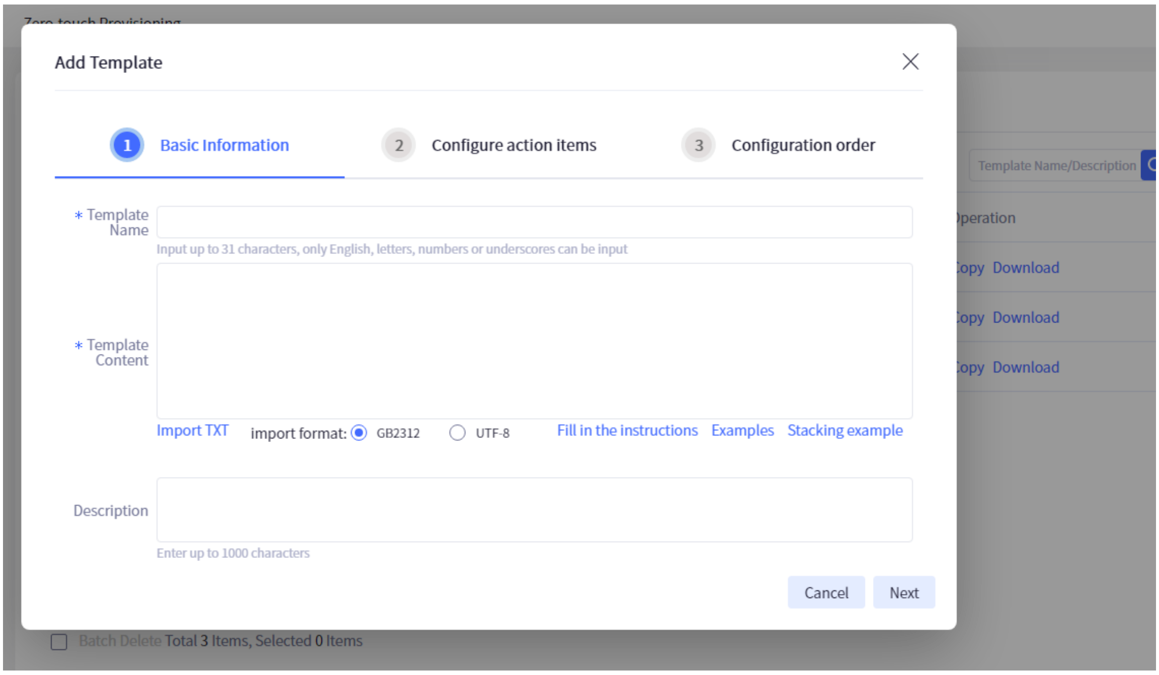
☐ Batch Delete Total 3 Items, Selected 0 Items

Figure 9.6.2

For the device configuration that needs to be started, you need to add a template or copy a template first. Note that when copying advanced templates and stacked templates, if the configuration items are different, but the same variable name needs to be used, you can fill in the same configuration name. In this way, it will only appear once in the start wizard and excel list. Then download the template file. The file is an excel file. The ${xxx} in the template will be mapped to the header in Excel. After filling in Excel, you can import the configuration of the corresponding device.

Examples are as follows:

Add a configuration template and fill in the template information.


Add Template

* Template Name

Input up to 31 characters, only English, letters, numbers or underscores can be input

* Template Content

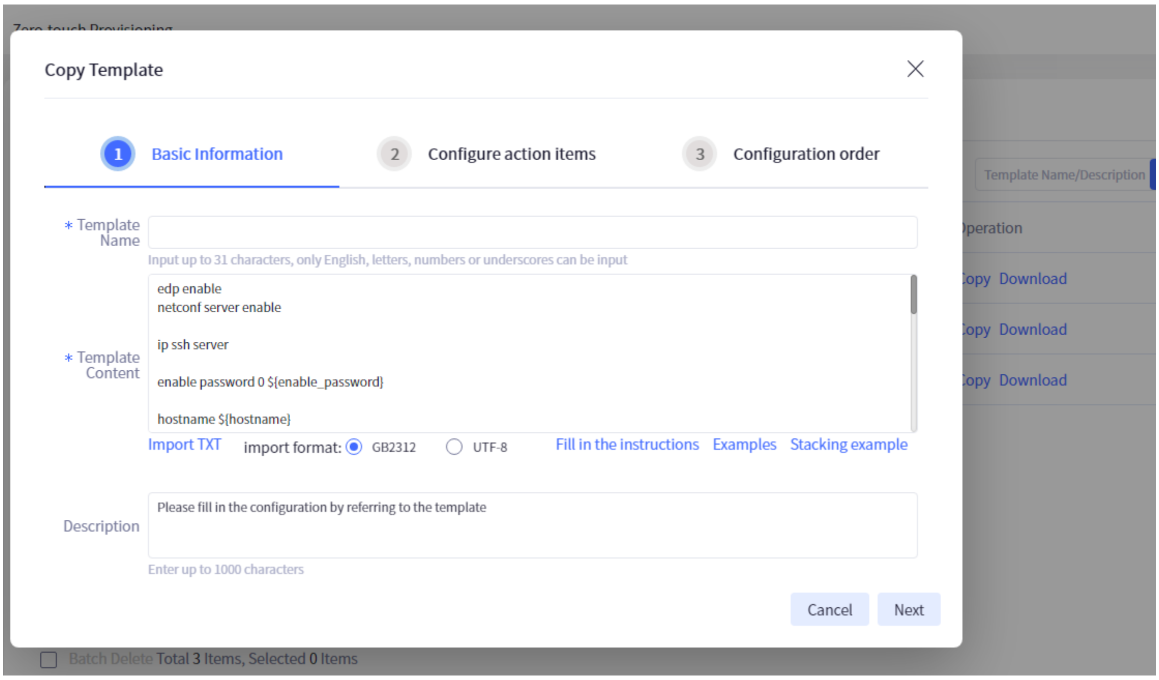
import format: ● GB2312 ○ UTF-8

Description

Enter up to 1000 characters

Figure 9.6.3

Copy the advanced template, add a configuration template, and fill in the template information.


Copy Template

* Template Name

Input up to 31 characters, only English, letters, numbers or underscores can be input

* Template Content

```
edp enable
netconf server enable

ip ssh server

enable password 0 ${enable_password}

hostname ${hostname}
```

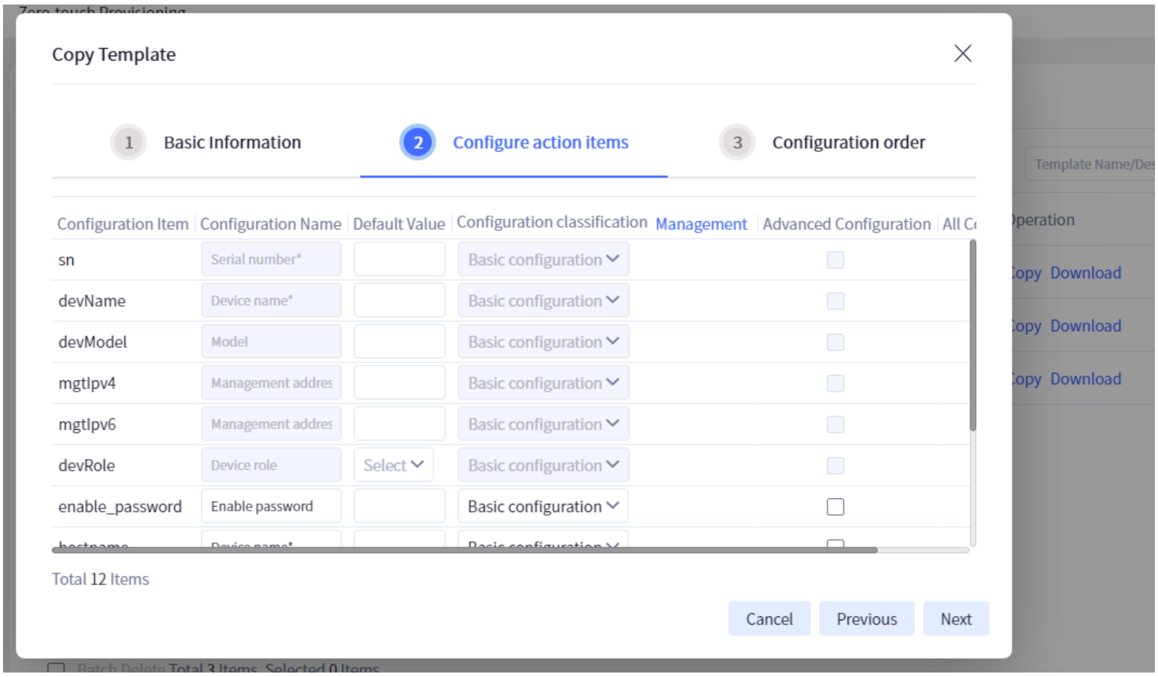
import format: ● GB2312 ○ UTF-8

Description: Please fill in the configuration by referring to the template

Enter up to 1000 characters

Figure 9.6.4

When configuring operation items, set the configuration names of the configuration items devName and hostname to be the same, so that they will only appear once in the start wizard and excel list.


Copy Template

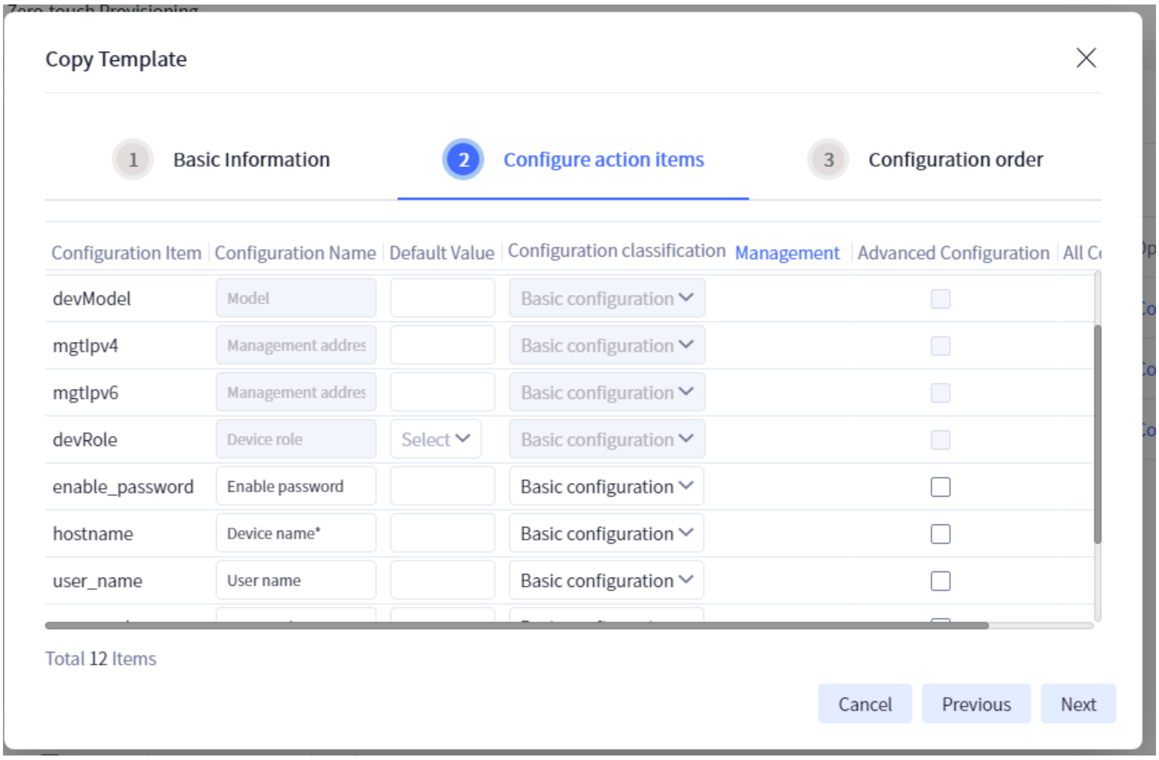
1 Basic Information　2 Configure action items　3 Configuration order

Configuration Item	Configuration Name	Default Value	Configuration classification	Management	Advanced Configuration
sn	Serial number*		Basic configuration		☐
devName	Device name*		Basic configuration		☐
devModel	Model		Basic configuration		☐
mgtIpv4	Management addres		Basic configuration		☐
mgtIpv6	Management addres		Basic configuration		☐
devRole	Device role	Select	Basic configuration		☐
enable_password	Enable password		Basic configuration		☐
hostname	Device name*		Basic configuration		☐

Total 12 Items

Figure 9.6.5

When configuring operation items, set the configuration names of the configuration items devName and hostname to be different, so that the configuration names displayed in the start wizard and excel list are different.


Copy Template

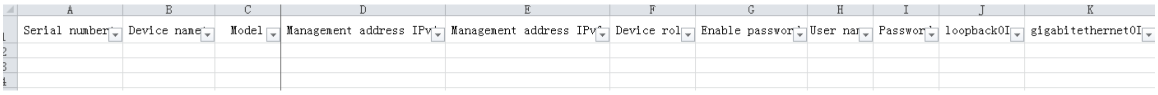
1 Basic Information　2 Configure action items　3 Configuration order

Configuration Item	Configuration Name	Default Value	Configuration classification	Management	Advanced Configuration
devModel	Model		Basic configuration		☐
mgtIpv4	Management addres		Basic configuration		☐
mgtIpv6	Management addres		Basic configuration		☐
devRole	Device role	Select	Basic configuration		☐
enable_password	Enable password		Basic configuration		☐
hostname	Device name*		Basic configuration		☐
user_name	User name		Basic configuration		☐

Total 12 Items

Figure 9.6.6

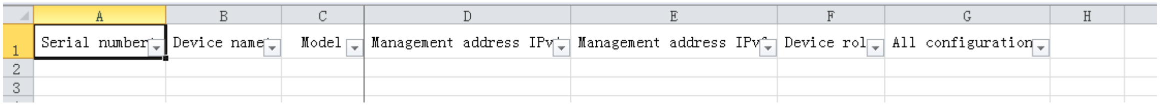
Compare the Excel files generated in figure 9.6.5 and figure 9.6.6, and you can see the difference.



	A	B	C	D	E	F	G	H	I	J	K
1	Serial number	Device name	Model	Management address IPv	Management address IPv	Device rol	Enable passwor	User nar	Passwor	loopback0I	gigabitethernet0I
2											
3											
4											

Figure 9.6.7

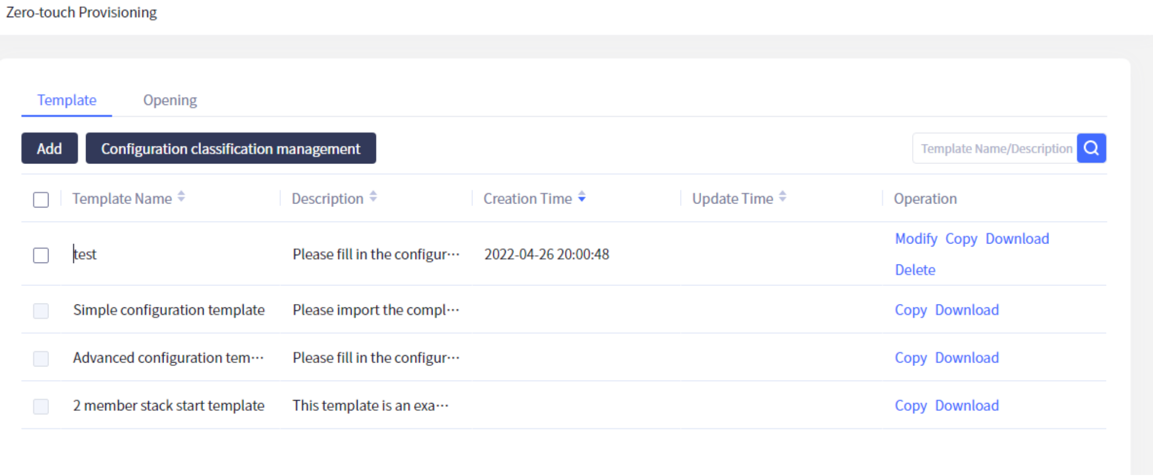
The excel file generated in figure 8.5.5 does not have the header field corresponding to the configuration item hostname, because the configuration name corresponding to the configuration item devname and the configuration item hostname are duplicate. The excel file generated in figure 8.5.6 has the header field "hostname name" corresponding to the configuration item hostname.



A	B	C	D	E	F	G	H
Serial number	Device name	Model	Management address IPv	Management address IPv	Device rol	All configuration	

Figure 9.6.8

Click "Template", select the new template "test", and click the "Download" button.



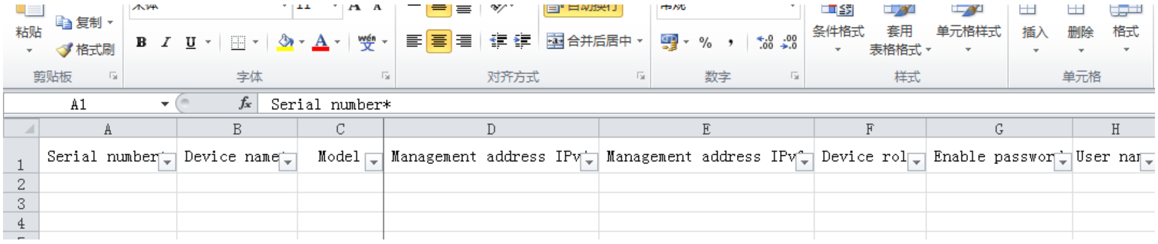
Zero-touch Provisioning

Template
Opening
Add
Configuration classification management
Template Name/Description

☐	Template Name	Description	Creation Time	Update Time	Operation
☐	test	Please fill in the configur···	2022-04-26 20:00:48		Modify Copy Download Delete
☐	Simple configuration template	Please import the compl···			Copy Download
☐	Advanced configuration tem···	Please fill in the configur···			Copy Download
☐	2 member stack start template	This template is an exa···			Copy Download

Figure 9.6.9

Download the excel file. You can see that the ${XXX} variable corresponds to the header field.



Serial number*

A	B	C	D	E	F	G	H
Serial number	Device name	Model	Management address IPv	Management address IPv	Device rol	Enable passwor	User nar

Figure 9.6.10

The first sheet at the bottom left is the template name and cannot be modified. Otherwise, the corresponding template cannot be found.

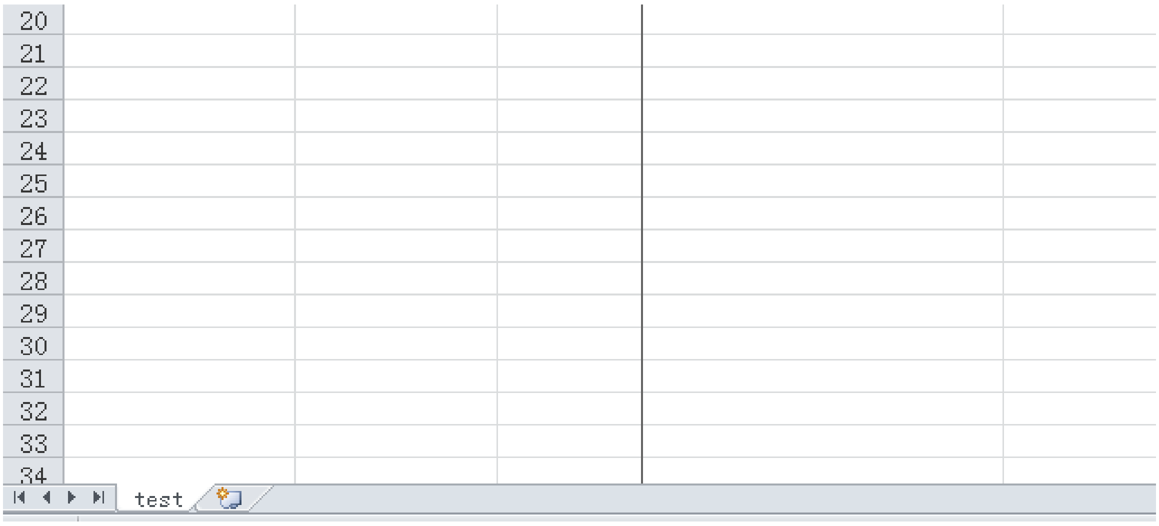
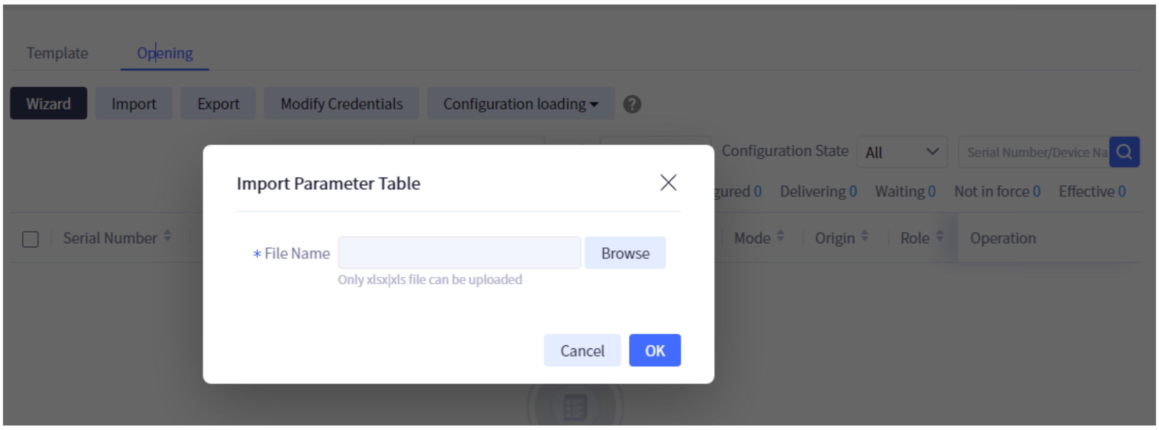


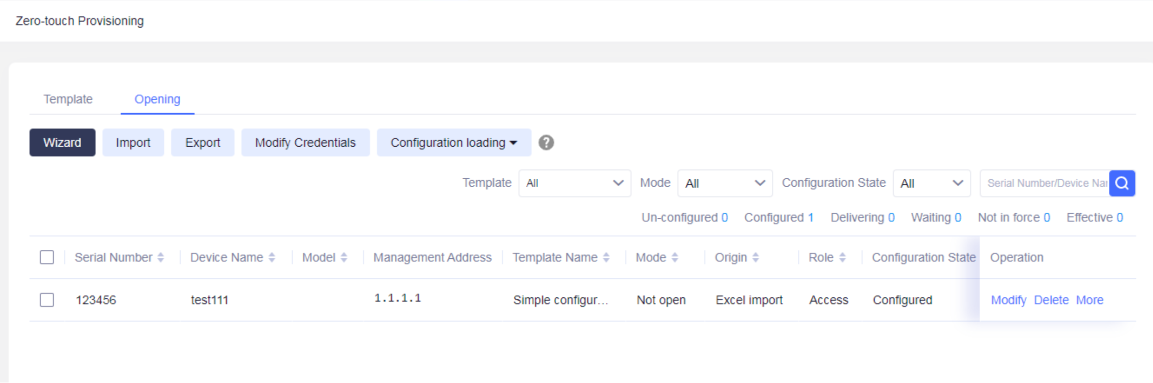
Figure 9.6.11



Only xlsx|xls file can be uploaded

Figure 9.6.12

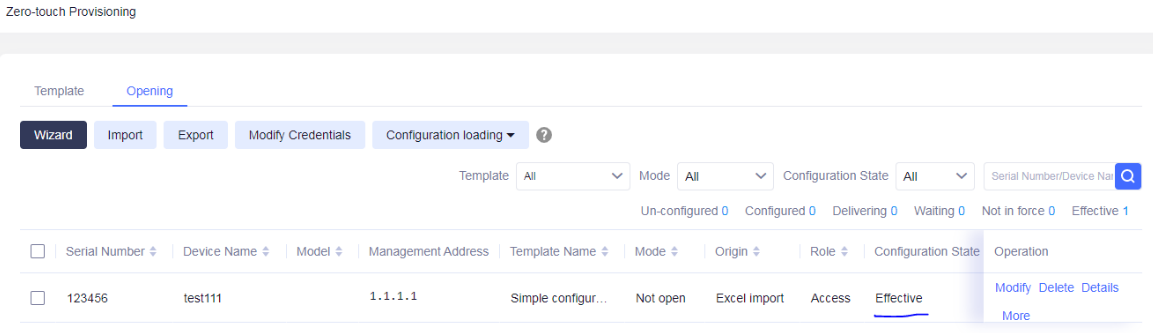
After importing successfully, it is shown in the following figure:



☐	Serial Number	Device Name	Model	Management Address	Template Name	Mode	Origin	Role	Configuration State	Operation
☐	123456	test111		1.1.1.1	Simple configur...	Not open	Excel import	Access	Configured	Modify Delete More

Figure 9.6.13

Select the desired device, click "Configure Loading" -> select the required loading method to load. During loading, the configuration status is "Being distributed". After loading successfully, the configuration status is "Effective".



☐	Serial Number	Device Name	Model	Management Address	Template Name	Mode	Origin	Role	Configuration State	Operation
☐	123456	test111		1.1.1.1	Simple configur...	Not open	Excel import	Access	Effective	Modify Delete Details More

Figure 9.6.14

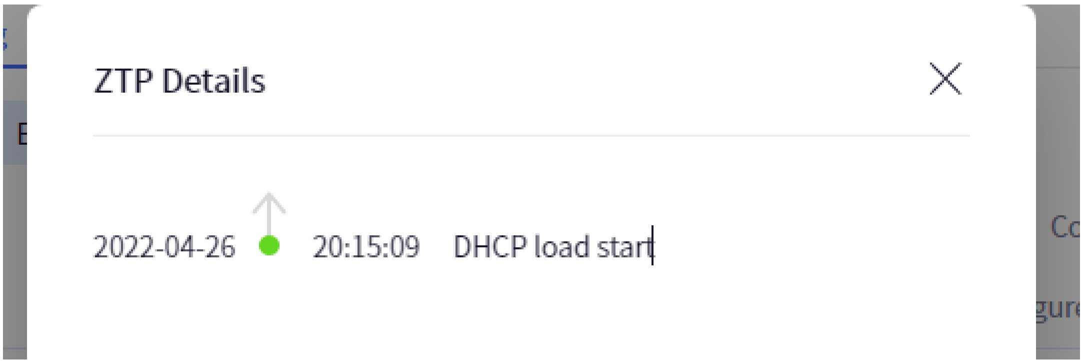
9.7 Loading Modes

The loading modes include DHCP loading and U-disk loading.

9.7.1 DHCP Loading

After setting the DHCP server, select DHCP loading, and you can perform DHCP provisioning.

Click "Details", and you can view the provisioning details, as shown below:



ZTP Details

2022-04-26 ● 20:15:09 DHCP load start

Figure 9.7.2.1

Device-side operation

If the device is brand new (it supports DHCP starting, the device version is correct, and the factory configuration), the device will automatically obtain the configuration file and restart to make the configuration effective.

If it is a configured device or a new device but fails to start, you need to connect to the device to trigger the start manually. The following is the start process of DHCP stacking devices:

Currently, only one member is opened in the cluster version stacking device, and the remaining members need to be added to the stacking device through manual commands.

According to the requirements of stacking topology, the stacking devices can be connected first, and the line connection relationship does not need to be modified later.

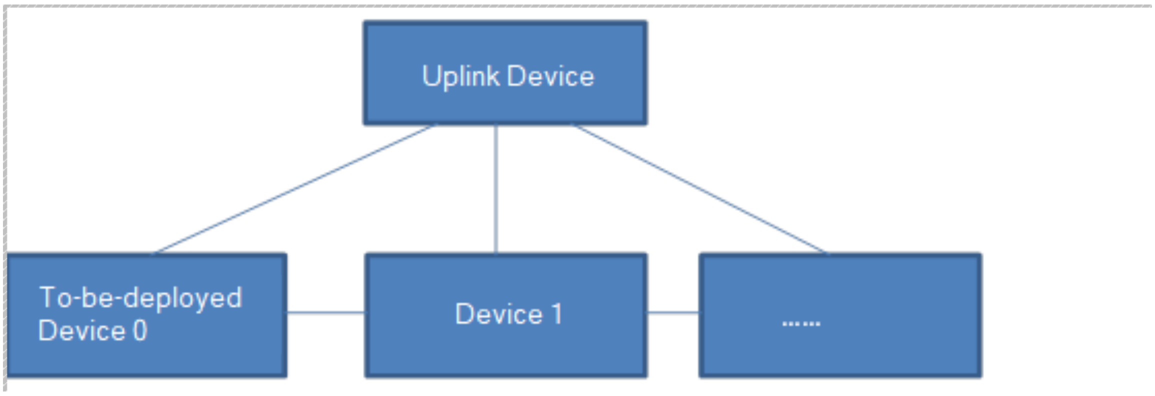


Figure 9.7.2.2

Enter the controller start interface to perform the necessary configuration for the start of stack member 0. The specific configuration can use "example template for stack start", "single variable template" or self-defined template. However, some configurations are necessary for the start of stacking. The details are as follows: red indicates that the fixed configuration cannot be modified:

```
! Current configuration
! startup vst mode                 Stacking mode
! Configuration version
hostname vst-leaf1-NSS5810-50TXFP(V1)
enable password 0 admin1234
local-user admin123 class manager
service-type telnet console ssh ftp netconf
password 0 admin1234
exit
link-aggregation 1 mode manual
```

```
vlan 1
exit
vlan 13
name Up-to-spine2
exit
vlan 100
name fast-hello
exit
lldp run
!PORT_CONFIG_BEGIN                    Slot number flag
!slot  0/0                                                  Member  configuration  flag.  Multiple
members need to modify the template to add
interface gigabitethernet0/0/11
switchport mode trunk
switchport trunk allowed vlan add 100
switchport trunk pvid vlan 1
no spanning-tree enable
dhcp-snooping trust
lldp enable
mad fast-hello vlan 100
exit
interface gigabitethernet0/0/24
link-aggregation 1 manual
exit
!end
!slot 1/0
interface gigabitethernet1/0/11
switchport mode trunk
switchport trunk allowed vlan add 100
switchport trunk pvid vlan 1
no spanning-tree enable
dhcp-snooping trust
lldp enable
mad fast-hello vlan 100
exit
interface gigabitethernet1/0/24
link-aggregation 1 manual
exit
!end
!PORT_CONFIG_END                      Slot number configuration end
```

```
interface link-aggregation1
description Up-to-spine3
switchport mode trunk
switchport trunk allowed vlan add 1,13
switchport trunk pvid vlan 1
exit
interface dc0
exit
interface loopback0
ip address 11.26.103.2 255.255.255.255
exit
interface vlan13
description Up-to-spine3
ip address 11.26.13.1 255.255.255.0
exit
interface null0
exit
router ospf 1
router-id 11.26.103.2
network 11.26.13.0 0.0.0.255 area 0
network 11.26.103.2 0.0.0.0 area 0
exit

ip ssh server
netconf server enable

!VST_CONFIG_BEGIN                    Stacking configuration flag. Without this flag, you will not
enter the stacking mode after the start
!vst_config
!mode member information
switch mode virtual
switch virtual member 0
domain 10
exit
!mode member end
!mode vsl information
vsl-channel 0/1
exit
vsl-channel 1/1
exit
```

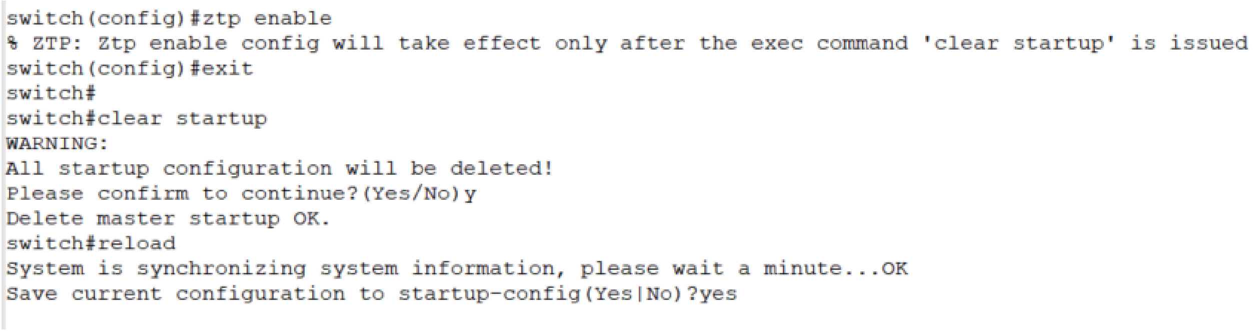
```
!mode vsl end
!PORT_CONFIG_BEGIN
!vsl   mode
!slot 0/0
interface tengigabitethernet0/0/25
vsl-channel 0/1 mode on
exit
interface tengigabitethernet0/0/27
vsl-channel 0/1 mode on
exit
!end
!slot_1/0_NSS5810-50TXFP(V1)
!vsl   mode
!slot 1/0
interface tengigabitethernet1/0/25
vsl-channel 1/1 mode on
exit
interface tengigabitethernet1/0/27
vsl-channel 1/1 mode on
exit
!end
!vst_end
!VST_CONFIG_END                Stacking configuration tag end
```

The device that needs to be started enters the ZTP mode for starting. The command for manually entering the starting mode at the device side is as follows:

Enter config mode and enter **ZTP enable**;

Exit the config mode, enter **clear startup**, and enter **yes** as prompted;

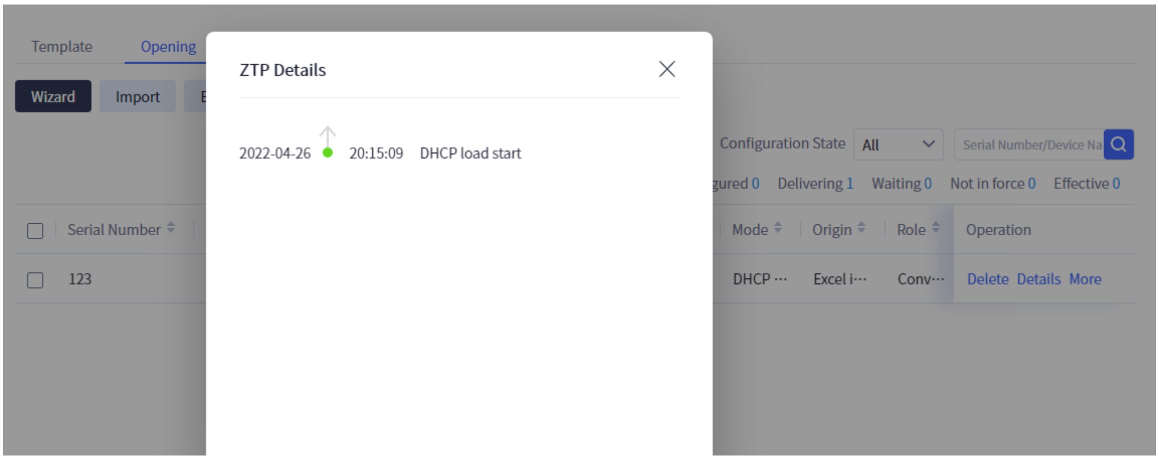
Then restart the device and enter **reload**; Enter **n**, **y** as prompted.



```
switch(config)#ztp enable
% ZTP: Ztp enable config will take effect only after the exec command 'clear startup' is issued
switch(config)#exit
switch#
switch#clear startup
WARNING:
All startup configuration will be deleted!
Please confirm to continue?(Yes/No)y
Delete master startup OK.
switch#reload
System is synchronizing system information, please wait a minute...OK
Save current configuration to startup-config(Yes|No)?yes
```

Figure 9.7.2.3

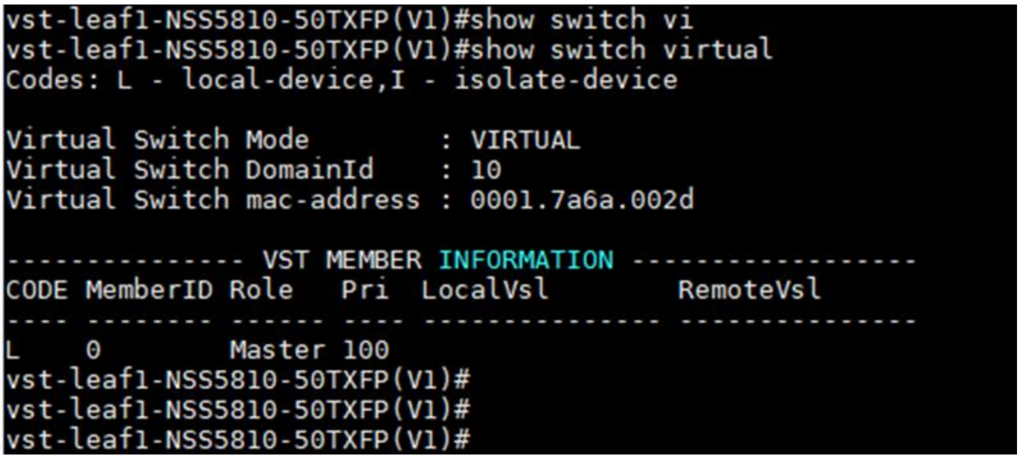
The devices that need to be started enter the ZTP mode to start. After a successful start, IP connection detection succeeds. You can view via the details of the start on the zero-touch start page, as shown in the following figure:



```
2022-04-26    20:15:09    DHCP load start
```

Figure 9.7.2.4

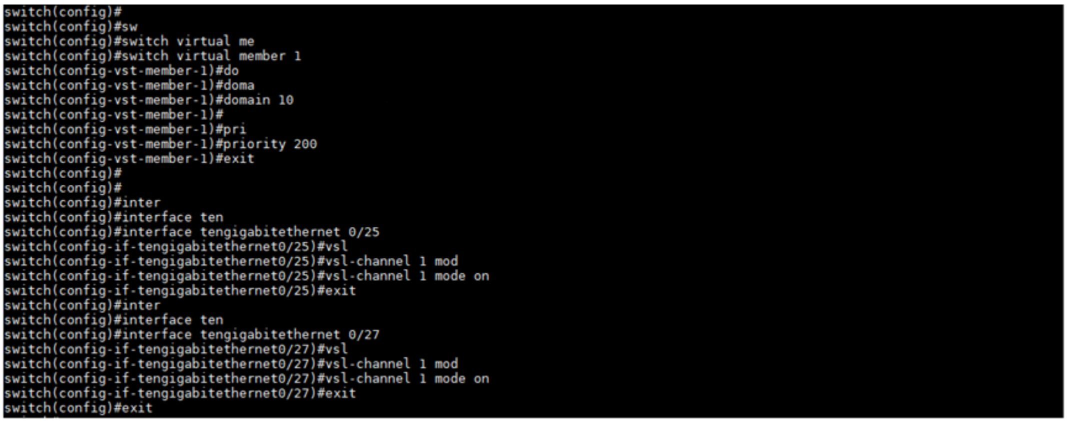
At this time, you can enter the member 0 device to view it. It is found that the stacking mode has been entered, and the member has only himself, as shown in the following figure.



```
vst-leaf1-NSS5810-50TXFP(V1)#show switch vi
vst-leaf1-NSS5810-50TXFP(V1)#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode          : VIRTUAL
Virtual Switch DomainId      : 10
Virtual Switch mac-address : 0001.7a6a.002d

--------------- VST MEMBER INFORMATION ------------------
CODE MemberID Role   Pri  LocalVsl         RemoteVsl
---- -------- ------ ---- --------------- ---------------
L    0        Master 100
vst-leaf1-NSS5810-50TXFP(V1)#
vst-leaf1-NSS5810-50TXFP(V1)#
vst-leaf1-NSS5810-50TXFP(V1)#
```

Figure 9.7.2.5

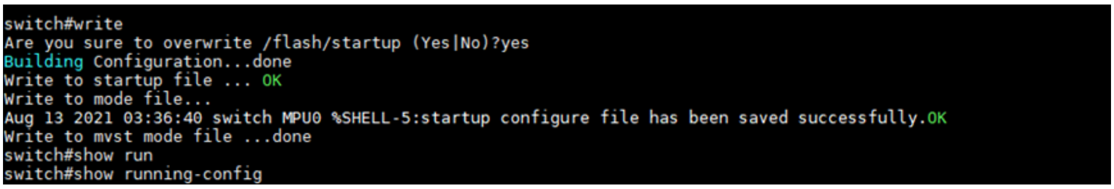
Then, enter the devices of other members through the console port, enter the stacking command, and join the stacking device members of the starting, as shown in the following figure.



```
switch(config)#
switch(config)#sw
switch(config)#switch virtual me
switch(config)#switch virtual member 1
switch(config-vst-member-1)#do
switch(config-vst-member-1)#doma
switch(config-vst-member-1)#domain 10
switch(config-vst-member-1)#
switch(config-vst-member-1)#pri
switch(config-vst-member-1)#priority 200
switch(config-vst-member-1)#exit
switch(config)#
switch(config)#
switch(config)#inter
switch(config)#interface ten
switch(config)#interface tengigabitethernet 0/25
switch(config-if-tengigabitethernet0/25)#vsl
switch(config-if-tengigabitethernet0/25)#vsl-channel 1 mod
switch(config-if-tengigabitethernet0/25)#vsl-channel 1 mode on
switch(config-if-tengigabitethernet0/25)#exit
switch(config)#inter
switch(config)#interface ten
switch(config)#interface tengigabitethernet 0/27
switch(config-if-tengigabitethernet0/27)#vsl
switch(config-if-tengigabitethernet0/27)#vsl-channel 1 mod
switch(config-if-tengigabitethernet0/27)#vsl-channel 1 mode on
switch(config-if-tengigabitethernet0/27)#exit
switch(config)#exit
```

Figure 9.7.2.6

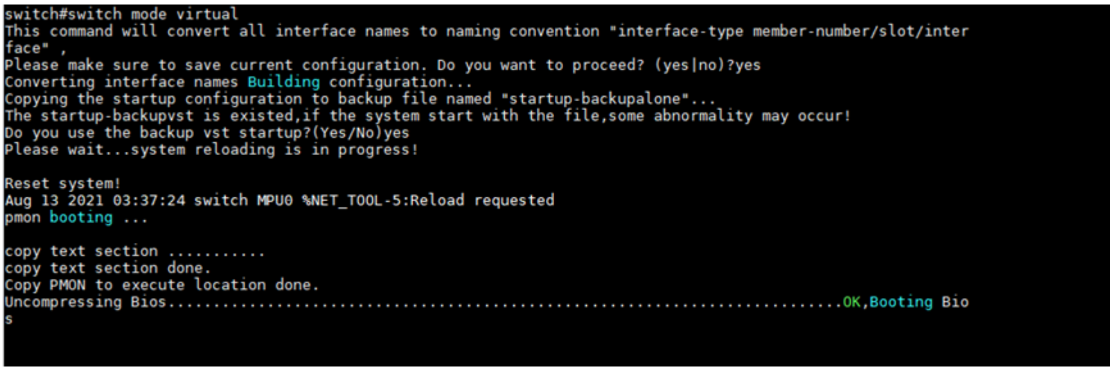
Enter the command **write** to write the configuration, as shown in the following figure.



```
switch#write
Are you sure to overwrite /flash/startup (Yes|No)?yes
Building Configuration...done
Write to startup file ... OK
Write to mode file...
Aug 13 2021 03:36:40 switch MPU0 %SHELL-5:startup configure file has been saved successfully.OK
Write to mvst mode file ...done
switch#show run
switch#show running-config
```

Figure 9.7.2.7

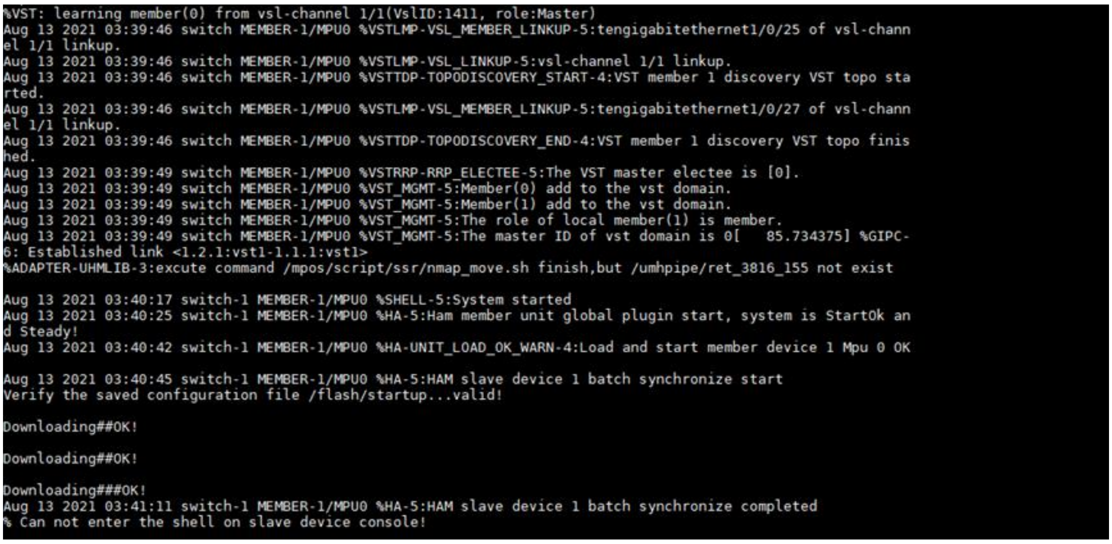
Use the command **switch mode virtual** to switch to the stacking mode, as shown in the following figure.



```
switch#switch mode virtual
This command will convert all interface names to naming convention "interface-type member-number/slot/inter
face" ,
Please make sure to save current configuration. Do you want to proceed? (yes|no)?yes
Converting interface names Building configuration...
Copying the startup configuration to backup file named "startup-backupalone"...
The startup-backupvst is existed,if the system start with the file,some abnormality may occur!
Do you use the backup vst startup?(Yes/No)yes
Please wait...system reloading is in progress!

Reset system!
Aug 13 2021 03:37:24 switch MPU0 %NET_TOOL-5:Reload requested
pmon booting ...

copy text section ..........
copy text section done.
Copy PMON to execute location done.
Uncompressing Bios..............................................................................OK,Booting Bio
s
```

Figure 9.7.2.8

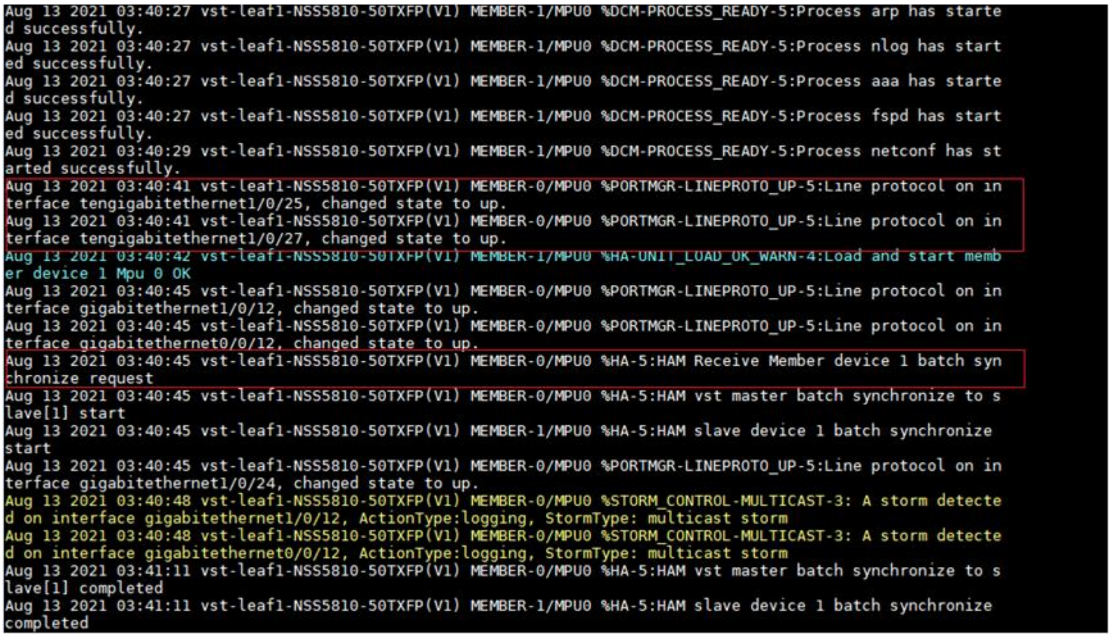
If the current member 1 device is successfully added to the stack, it cannot be accessed through the console port, as shown in the following figure,



```
%VST: learning member(0) from vsl-channel 1/1(VslID:1411, role:Master)
Aug 13 2021 03:39:46 switch MEMBER-1/MPU0 %VSTLMP-VSL_MEMBER_LINKUP-5:tengigabitethernet1/0/25 of vsl-chann
el 1/1 linkup.
Aug 13 2021 03:39:46 switch MEMBER-1/MPU0 %VSTLMP-VSL_LINKUP-5:vsl-channel 1/1 linkup.
Aug 13 2021 03:39:46 switch MEMBER-1/MPU0 %VSTTDP-TOPODISCOVERY_START-4:VST member 1 discovery VST topo sta
rted.
Aug 13 2021 03:39:46 switch MEMBER-1/MPU0 %VSTLMP-VSL_MEMBER_LINKUP-5:tengigabitethernet1/0/27 of vsl-chann
el 1/1 linkup.
Aug 13 2021 03:39:46 switch MEMBER-1/MPU0 %VSTTDP-TOPODISCOVERY_END-4:VST member 1 discovery VST topo finis
hed.
Aug 13 2021 03:39:49 switch MEMBER-1/MPU0 %VSTRRP-RRP_ELECTEE-5:The VST master electee is [0].
Aug 13 2021 03:39:49 switch MEMBER-1/MPU0 %VST_MGMT-5:Member(0) add to the vst domain.
Aug 13 2021 03:39:49 switch MEMBER-1/MPU0 %VST_MGMT-5:Member(1) add to the vst domain.
Aug 13 2021 03:39:49 switch MEMBER-1/MPU0 %VST_MGMT-5:The role of local member(1) is member.
Aug 13 2021 03:39:49 switch MEMBER-1/MPU0 %VST_MGMT-5:The master ID of vst domain is 0[   85.734375] %GIPC-
6: Established link <1.2.1:vst1-1.1.1:vst1>
%ADAPTER-UHMLIB-3:excute command /mpos/script/ssr/nmap_move.sh finish,but /umhpipe/ret_3816_155 not exist

Aug 13 2021 03:40:17 switch-1 MEMBER-1/MPU0 %SHELL-5:System started
Aug 13 2021 03:40:25 switch-1 MEMBER-1/MPU0 %HA-5:Ham member unit global plugin start, system is StartOk an
d Steady!
Aug 13 2021 03:40:42 switch-1 MEMBER-1/MPU0 %HA-UNIT_LOAD_OK_WARN-4:Load and start member device 1 Mpu 0 OK

Aug 13 2021 03:40:45 switch-1 MEMBER-1/MPU0 %HA-5:HAM slave device 1 batch synchronize start
Verify the saved configuration file /flash/startup...valid!

Downloading##OK!

Downloading##OK!

Downloading###OK!
Aug 13 2021 03:41:11 switch-1 MEMBER-1/MPU0 %HA-5:HAM slave device 1 batch synchronize completed
% Can not enter the shell on slave device console!
```

Figure 9.7.2.9

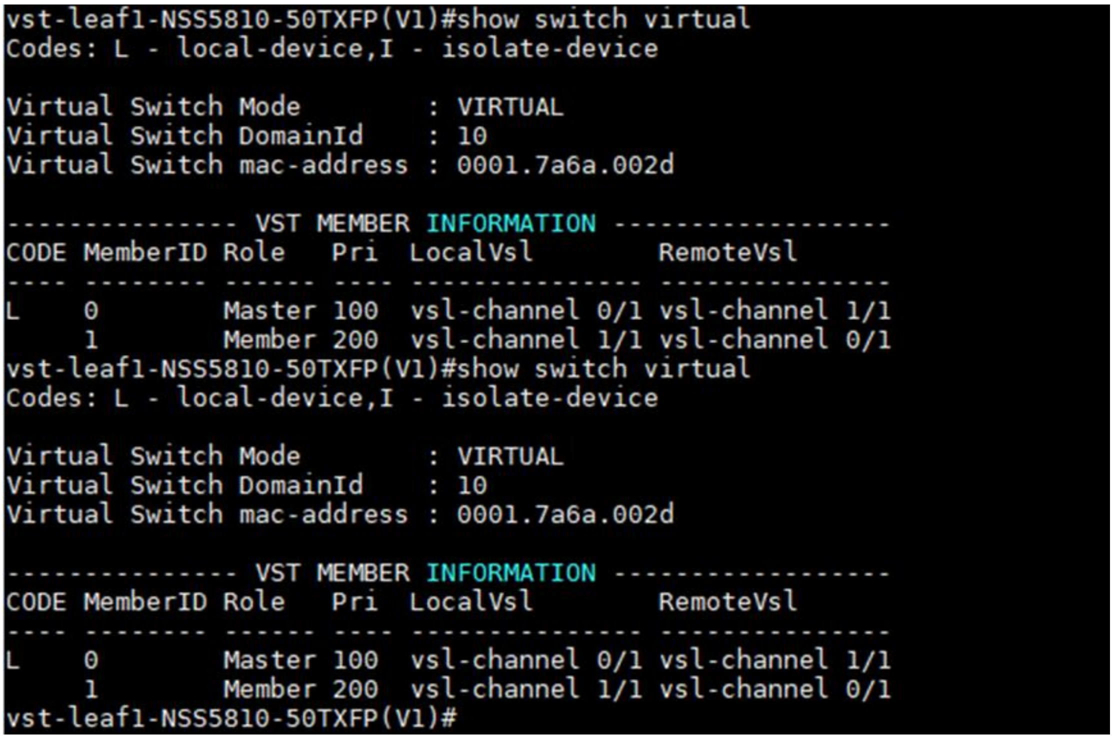
At this time, if there is a console port of member 0, enter the device, and member 0 will print the relevant logs of accessing member 1, as shown in the following figure.



```
Aug 13 2021 03:40:27 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-1/MPU0 %DCM-PROCESS_READY-5:Process arp has starte
d successfully.
Aug 13 2021 03:40:27 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-1/MPU0 %DCM-PROCESS_READY-5:Process nlog has start
ed successfully.
Aug 13 2021 03:40:27 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-1/MPU0 %DCM-PROCESS_READY-5:Process aaa has starte
d successfully.
Aug 13 2021 03:40:27 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-1/MPU0 %DCM-PROCESS_READY-5:Process fspd has start
ed successfully.
Aug 13 2021 03:40:29 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-1/MPU0 %DCM-PROCESS_READY-5:Process netconf has st
arted successfully.
Aug 13 2021 03:40:41 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %PORTMGR-LINEPROTO_UP-5:Line protocol on in
terface tengigabitethernet1/0/25, changed state to up.
Aug 13 2021 03:40:41 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %PORTMGR-LINEPROTO_UP-5:Line protocol on in
terface tengigabitethernet1/0/27, changed state to up.
Aug 13 2021 03:40:42 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-1/MPU0 %HA-UNIT_LOAD_OK_WARN-4:Load and start memb
er device 1 Mpu 0 OK
Aug 13 2021 03:40:45 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %PORTMGR-LINEPROTO_UP-5:Line protocol on in
terface gigabitethernet1/0/12, changed state to up.
Aug 13 2021 03:40:45 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %PORTMGR-LINEPROTO_UP-5:Line protocol on in
terface gigabitethernet0/0/12, changed state to up.
Aug 13 2021 03:40:45 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %HA-5:HAM Receive Member device 1 batch syn
chronize request
Aug 13 2021 03:40:45 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %HA-5:HAM vst master batch synchronize to s
lave[1] start
Aug 13 2021 03:40:45 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-1/MPU0 %HA-5:HAM slave device 1 batch synchronize
start
Aug 13 2021 03:40:45 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %PORTMGR-LINEPROTO_UP-5:Line protocol on in
terface gigabitethernet1/0/24, changed state to up.
Aug 13 2021 03:40:48 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %STORM_CONTROL-MULTICAST-3: A storm detecte
d on interface gigabitethernet1/0/12, ActionType:logging, StormType: multicast storm
Aug 13 2021 03:40:48 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %STORM_CONTROL-MULTICAST-3: A storm detecte
d on interface gigabitethernet0/0/12, ActionType:logging, StormType: multicast storm
Aug 13 2021 03:41:11 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-0/MPU0 %HA-5:HAM vst master batch synchronize to s
lave[1] completed
Aug 13 2021 03:41:11 vst-leaf1-NSS5810-50TXFP(V1) MEMBER-1/MPU0 %HA-5:HAM slave device 1 batch synchronize
completed
```

Figure 9.7.2.10

Looking at the stacked members of member 0 again, you can find that member 1 has been added to the stack, as shown in the following figure. At this point, the DHCP start of the stacking device is completed.



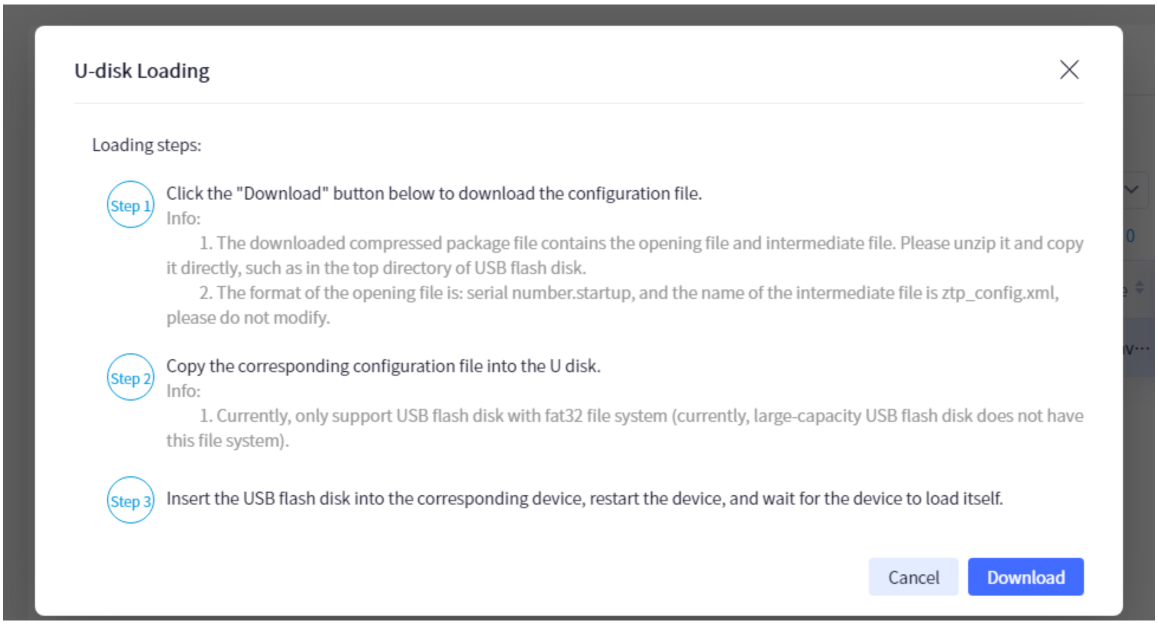
```
vst-leaf1-NSS5810-50TXFP(V1)#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode        : VIRTUAL
Virtual Switch DomainId    : 10
Virtual Switch mac-address : 0001.7a6a.002d

--------------- VST MEMBER INFORMATION ------------------
CODE MemberID Role   Pri  LocalVsl        RemoteVsl
---- -------- ------ ---- --------------- ---------------
L    0        Master 100  vsl-channel 0/1 vsl-channel 1/1
     1        Member 200  vsl-channel 1/1 vsl-channel 0/1
vst-leaf1-NSS5810-50TXFP(V1)#show switch virtual
Codes: L - local-device,I - isolate-device

Virtual Switch Mode        : VIRTUAL
Virtual Switch DomainId    : 10
Virtual Switch mac-address : 0001.7a6a.002d

--------------- VST MEMBER INFORMATION ------------------
CODE MemberID Role   Pri  LocalVsl        RemoteVsl
---- -------- ------ ---- --------------- ---------------
L    0        Master 100  vsl-channel 0/1 vsl-channel 1/1
     1        Member 200  vsl-channel 1/1 vsl-channel 0/1
vst-leaf1-NSS5810-50TXFP(V1)#
```

Figure 9.7.2.11

Check the opening details after the opening. If succeeded, you can click connection detection. If the connection succeeds, it is proved that the opening is successful. If the connection fails, repeat the above steps to restart.

9.7.2 U-disk Loading

Click the U-disk loading, the following prompt page will appear. Click the **Download** button to download xxx.zip file. After de-compressing, copy the unzipped file to the U disk. Then insert the U disk into the device to start.



Loading steps:

Step 1 Click the "Download" button below to download the configuration file.

Info:

1. The downloaded compressed package file contains the opening file and intermediate file. Please unzip it and copy it directly, such as in the top directory of USB flash disk.
2. The format of the opening file is: serial number.startup, and the name of the intermediate file is ztp_config.xml, please do not modify.

Step 2 Copy the corresponding configuration file into the U disk.

Info:

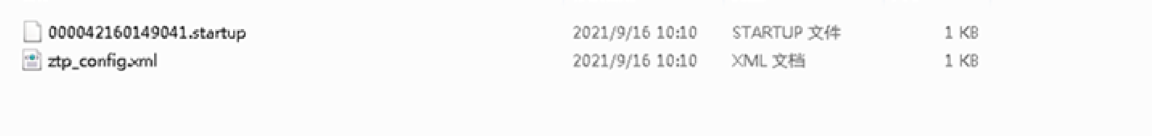
1. Currently, only support USB flash disk with fat32 file system (currently, large-capacity USB flash disk does not have this file system).

Step 3 Insert the USB flash disk into the corresponding device, restart the device, and wait for the device to load itself.

Figure 9.7.4.1

The U-disk opening process downloads the compressed package of startup file + intermediate file, which needs to be unzipped and copied into the top-level template of U-disk. The new U-disk supports slot labels.

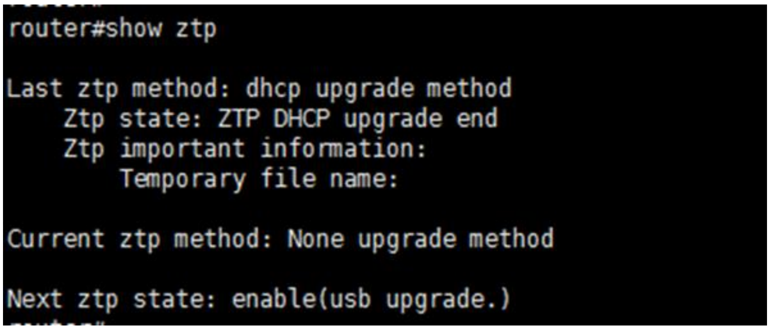
The compressed package name is startup_the number of opening files. The screenshot after decompression is as follows.



000042160149041.startup	2021/9/16 10:10	STARTUP 文件	1 KB
ztp_config.xml	2021/9/16 10:10	XML 文档	1 KB

Figure 9.7.4.2

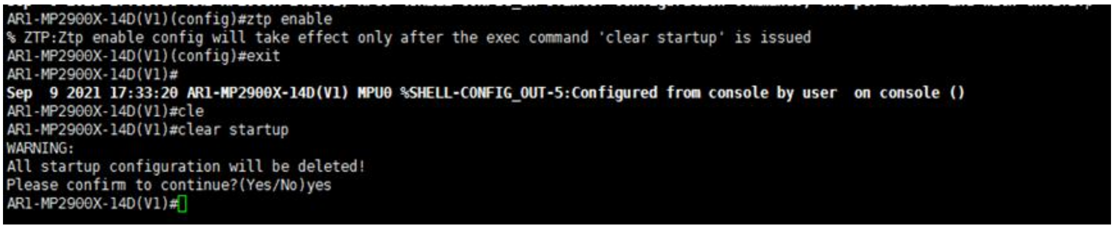
Insert the U-disk into the device, check the U-disk attached to the following directory on the device side, and enter the command: **show ztp**. The following figure indicates that the next time will uses the USB mode in ztp to start. If the U-disk is not recognized successfully, the next restart will not enter the U-disk start mode.



```
router#show ztp

Last ztp method: dhcp upgrade method
    Ztp state: ZTP DHCP upgrade end
    Ztp important information:
        Temporary file name:

Current ztp method: None upgrade method

Next ztp state: enable(usb upgrade.)
```

Figure 9.7.4.3

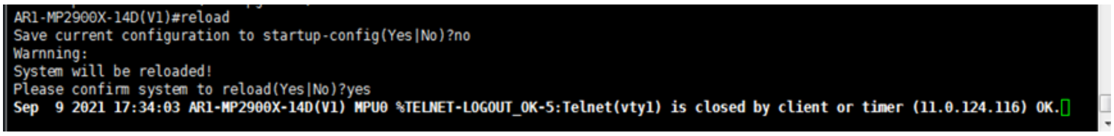
Next, clear the device configuration.



```
AR1-MP2900X-14D(V1)(config)#ztp enable
% ZTP:Ztp enable config will take effect only after the exec command 'clear startup' is issued
AR1-MP2900X-14D(V1)(config)#exit
AR1-MP2900X-14D(V1)#
Sep  9 2021 17:33:20 AR1-MP2900X-14D(V1) MPU0 %SHELL-CONFIG_OUT-5:Configured from console by user  on console ()
AR1-MP2900X-14D(V1)#cle
AR1-MP2900X-14D(V1)#clear startup
WARNING:
All startup configuration will be deleted!
Please confirm to continue?(Yes/No)yes
AR1-MP2900X-14D(V1)#
```

Figure 9.7.4.4

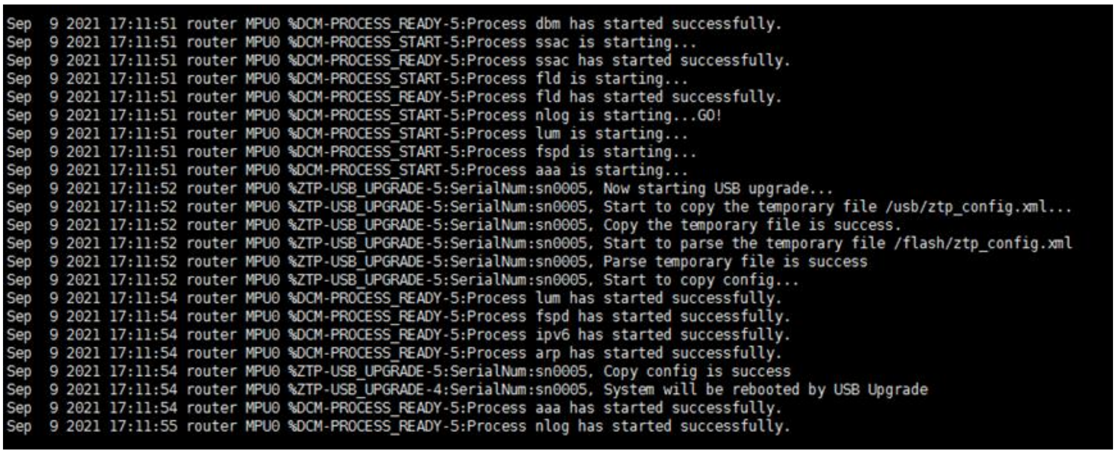
Restart the device.



```
AR1-MP2900X-14D(V1)#reload
Save current configuration to startup-config(Yes|No)?no
Warnning:
System will be reloaded!
Please confirm system to reload(Yes|No)?yes
Sep  9 2021 17:34:03 AR1-MP2900X-14D(V1) MPU0 %TELNET-LOGOUT_OK-5:Telnet(vty1) is closed by client or timer (11.0.124.116) OK.
```

Figure 9.7.4.5

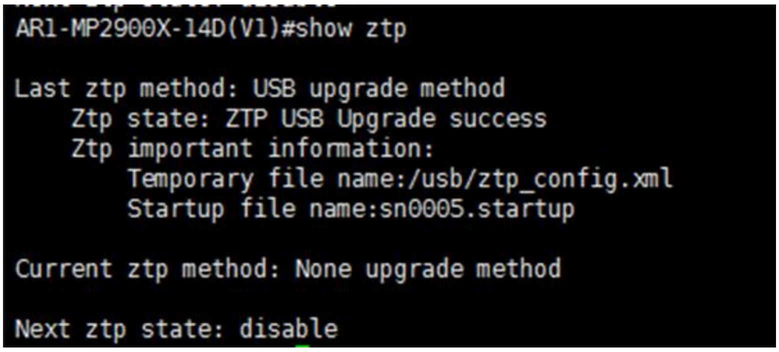
Print the following log, indicating entering the U-disk starting.



```
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_READY-5:Process dbm has started successfully.
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_START-5:Process ssac is starting...
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_READY-5:Process ssac has started successfully.
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_START-5:Process fld is starting...
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_READY-5:Process fld has started successfully.
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_START-5:Process nlog is starting...GO!
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_START-5:Process lum is starting...
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_START-5:Process fspd is starting...
Sep  9 2021 17:11:51 router MPU0 %DCM-PROCESS_START-5:Process aaa is starting...
Sep  9 2021 17:11:52 router MPU0 %ZTP-USB_UPGRADE-5:SerialNum:sn0005, Now starting USB upgrade...
Sep  9 2021 17:11:52 router MPU0 %ZTP-USB_UPGRADE-5:SerialNum:sn0005, Start to copy the temporary file /usb/ztp_config.xml...
Sep  9 2021 17:11:52 router MPU0 %ZTP-USB_UPGRADE-5:SerialNum:sn0005, Copy the temporary file is success.
Sep  9 2021 17:11:52 router MPU0 %ZTP-USB_UPGRADE-5:SerialNum:sn0005, Start to parse the temporary file /flash/ztp_config.xml
Sep  9 2021 17:11:52 router MPU0 %ZTP-USB_UPGRADE-5:SerialNum:sn0005, Parse temporary file is success
Sep  9 2021 17:11:52 router MPU0 %ZTP-USB_UPGRADE-5:SerialNum:sn0005, Start to copy config...
Sep  9 2021 17:11:54 router MPU0 %DCM-PROCESS_READY-5:Process lum has started successfully.
Sep  9 2021 17:11:54 router MPU0 %DCM-PROCESS_READY-5:Process fspd has started successfully.
Sep  9 2021 17:11:54 router MPU0 %DCM-PROCESS_READY-5:Process ipv6 has started successfully.
Sep  9 2021 17:11:54 router MPU0 %DCM-PROCESS_READY-5:Process arp has started successfully.
Sep  9 2021 17:11:54 router MPU0 %ZTP-USB_UPGRADE-5:SerialNum:sn0005, Copy config is success
Sep  9 2021 17:11:54 router MPU0 %ZTP-USB_UPGRADE-4:SerialNum:sn0005, System will be rebooted by USB Upgrade
Sep  9 2021 17:11:54 router MPU0 %DCM-PROCESS_READY-5:Process aaa has started successfully.
Sep  9 2021 17:11:55 router MPU0 %DCM-PROCESS_READY-5:Process nlog has started successfully.
```

Figure 9.7.4.6

After a successful start, enter the **show ztp** command again, and you can view the details of the last start.



```
AR1-MP2900X-14D(V1)#show ztp

Last ztp method: USB upgrade method
    Ztp state: ZTP USB Upgrade success
    Ztp important information:
        Temporary file name:/usb/ztp_config.xml
        Startup file name:sn0005.startup

Current ztp method: None upgrade method

Next ztp state: disable
```

Figure 9.7.4.7

10 Services Visible

10.1 Dashboard

The system operation status can be displayed visually in the dashboard. Click **Monitoring** > **Dashboard** to enter the dashboard interface, as shown in the following figure.

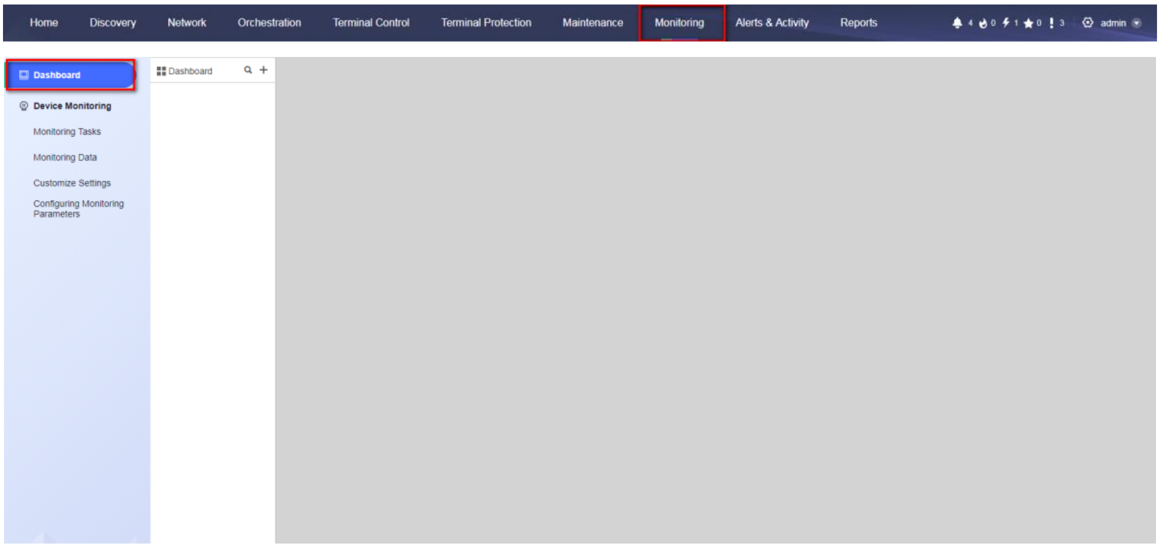
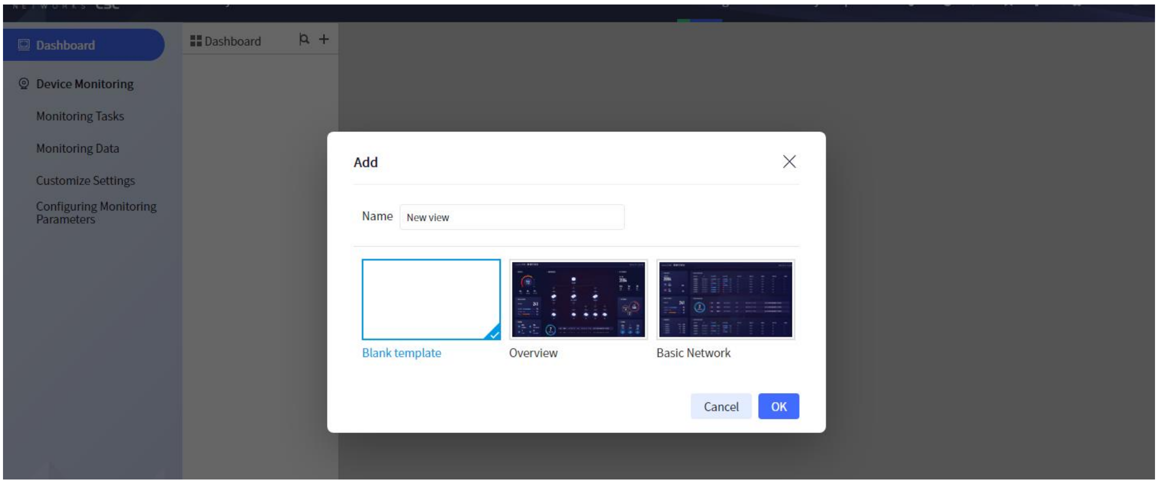


Figure 10.1.1 Enter the dashboard

Click the + sign to create a dashboard. You can select to create blank template, overview, and basic network, as shown in the following figure.



Name: New view

Figure 10.1.2 Create dashboard template

Blank template:

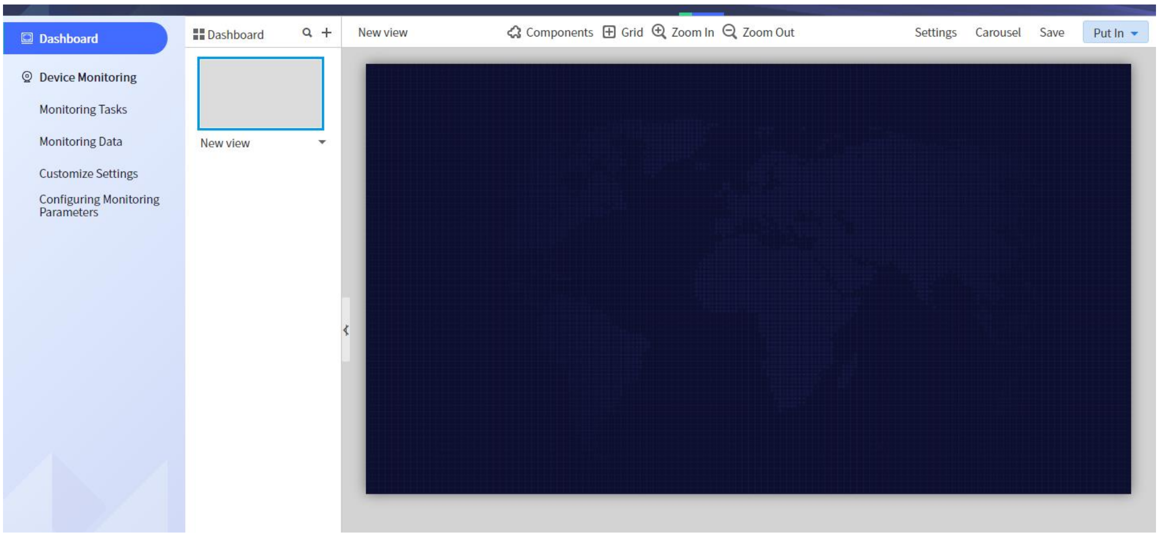


Figure 10.1.3 Blank template

Asset overview:

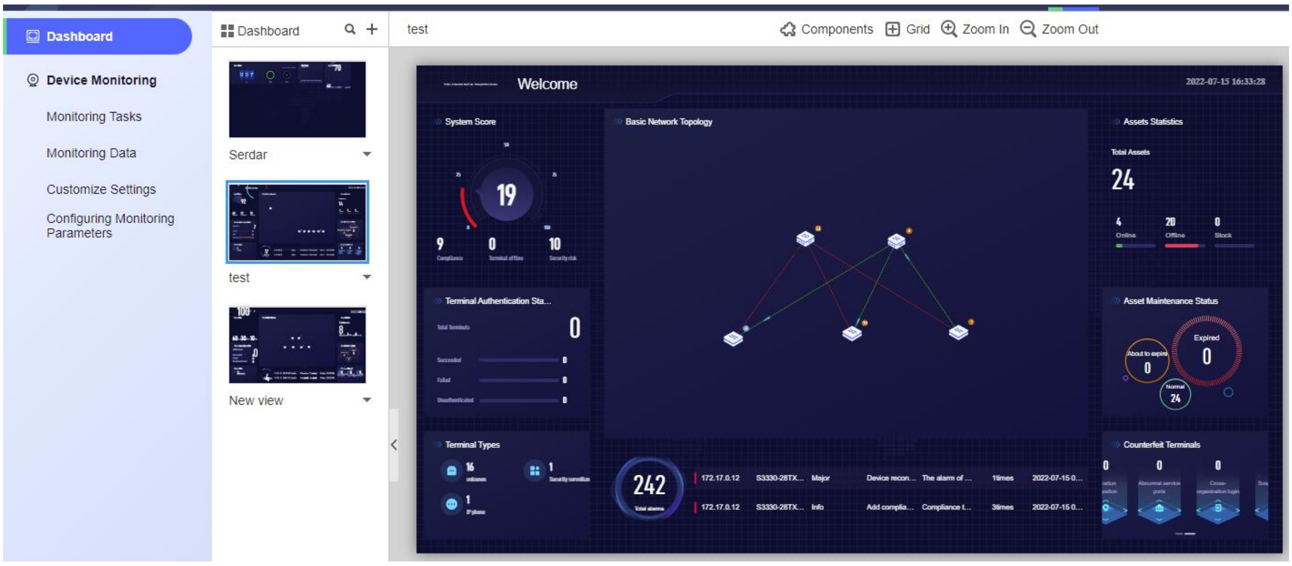
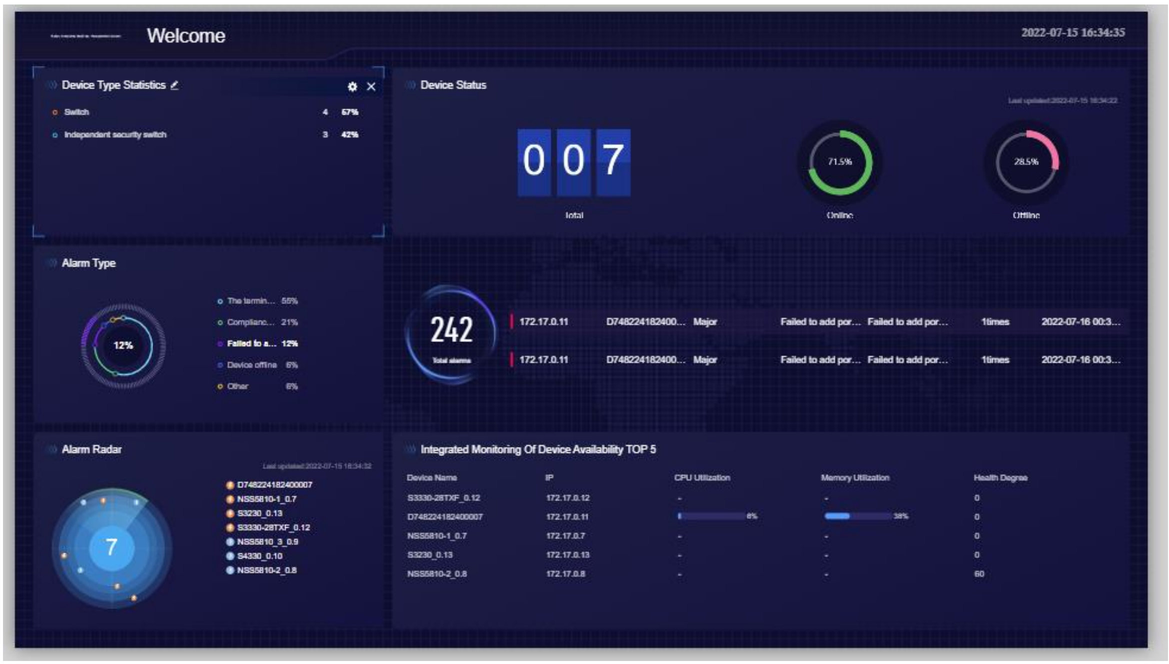


Figure 10.1.4 Asset overview

Basic network:



172.17.0.11 D748224182400... Major Failed to add por... Failed to add por... 1times 2022-07-16 00:3...

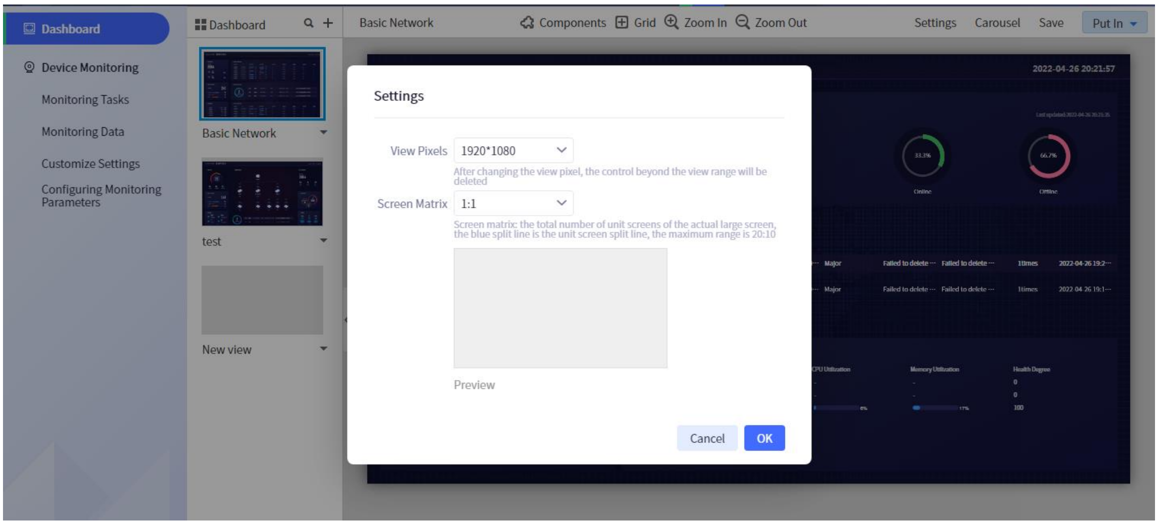
172.17.0.11 D748224182400... Major Failed to add por... Failed to add por... 1times 2022-07-16 00:3...

Integrated Monitoring Of Device Availability TOP 5

Device Name	IP	CPU Utilization	Memory Utilization	Health Degree
S3330-28TXF_0.12	172.17.0.12	-	-	0
D748224182400007	172.17.0.11	6%	38%	0
NSS5810-1_0.7	172.17.0.7	-	-	0
S3230_0.13	172.17.0.13	-	-	0
NSS5810-2_0.8	172.17.0.8	-	-	60

Figure 10.1.5 Basic network

Click the **Settings** button, and you can set the dashboard configuration, as shown in the following figure.



Settings

View Pixels: 1920*1080

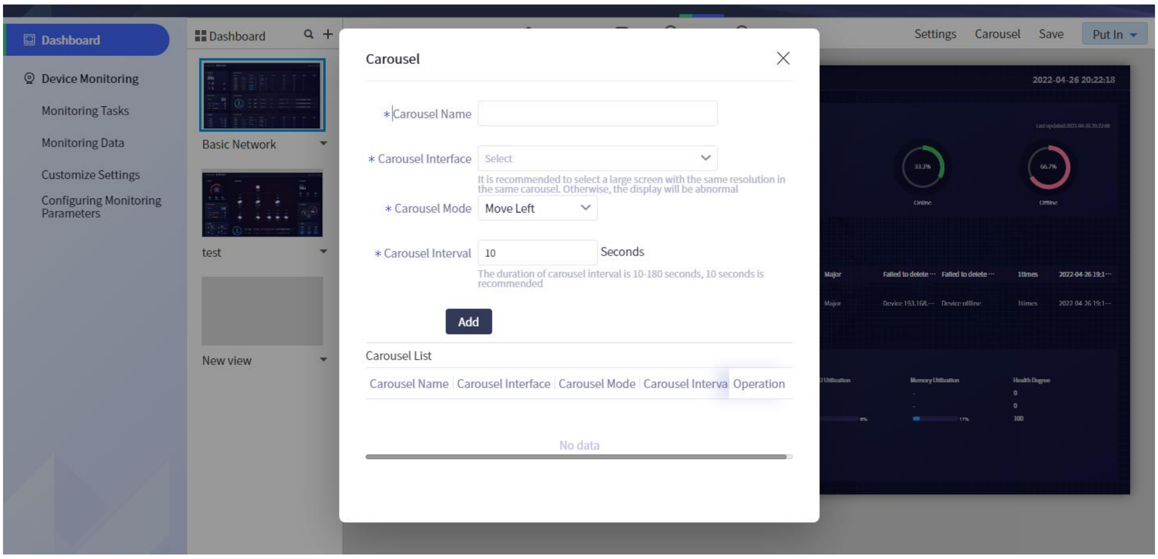
After changing the view pixel, the control beyond the view range will be deleted

Screen Matrix: 1:1

Screen matrix: the total number of unit screens of the actual large screen, the blue split line is the unit screen split line, the maximum range is 20:10

Figure 10.1.6 Dashboard setting

Click the **Carousel** button, and you can set all the current dashboards for carousel, as shown in the following figure.



Carousel

* Carousel Name
* Carousel Interface: Select

It is recommended to select a large screen with the same resolution in the same carousel. Otherwise, the display will be abnormal

* Carousel Mode: Move Left
* Carousel Interval: 10 Seconds

The duration of carousel interval is 10-180 seconds, 10 seconds is recommended

Add

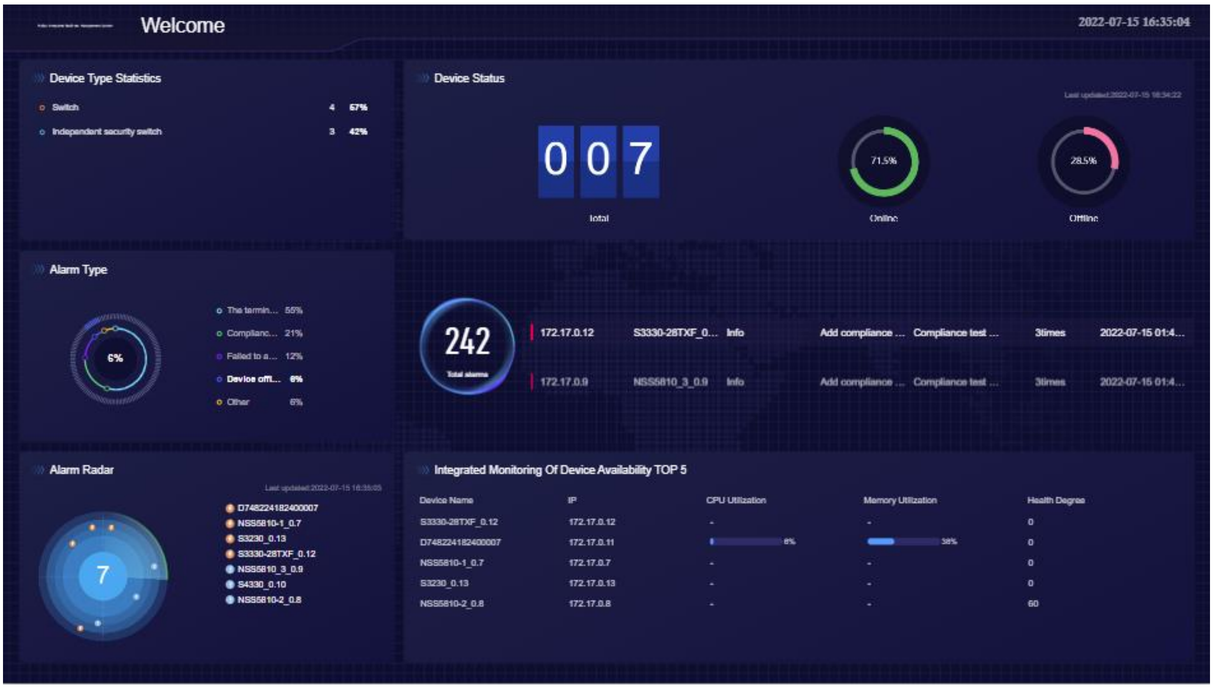
Carousel List

Carousel Name	Carousel Interface	Carousel Mode	Carousel Interval	Operation

No data

Figure 10.1.7 Dashboard carousel setting

The user can choose to put in the dashboard, and the effect is as follows.



172.17.0.12 S3330-28TXF_0... Info Add compliance ... Compliance test ... 3times 2022-07-15 01:4...

172.17.0.9 NSS5810_3_0.9 Info Add compliance ... Compliance test ... 3times 2022-07-15 01:4...

Integrated Monitoring Of Device Availability TOP 5

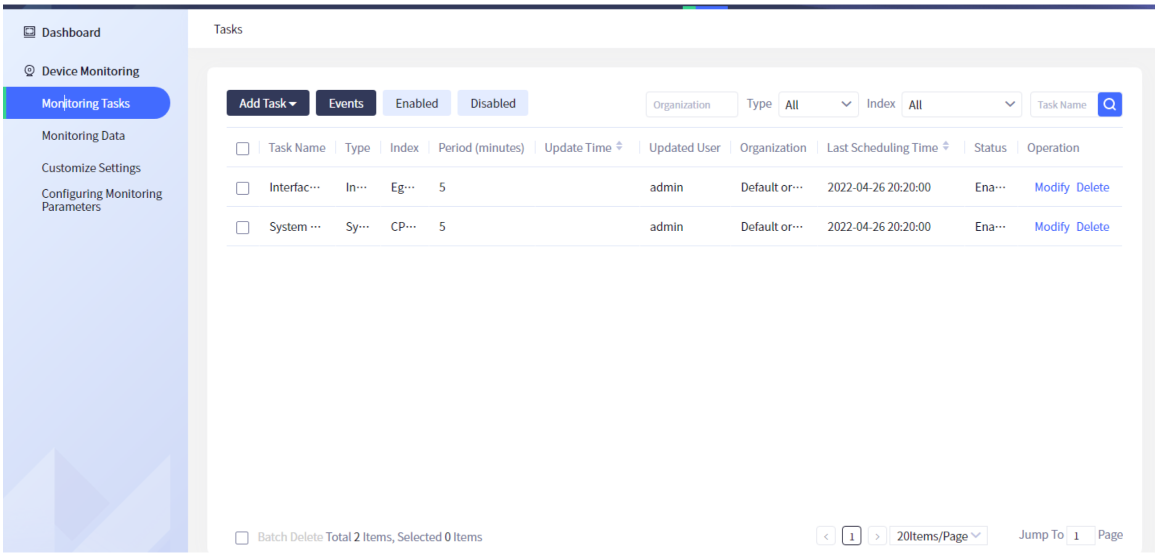
Device Name	IP	CPU Utilization	Memory Utilization	Health Degree
S3330-28TXF_0.12	172.17.0.12	-	-	0
D7482241824000007	172.17.0.11	6%	38%	0
NSS5810-1_0.7	172.17.0.7	-	-	0
S3230_0.13	172.17.0.13	-	-	0
NSS5810-2_0.8	172.17.0.8	-	-	60

Figure 10.1.8 The effect of putting in dashboard

10.2 Device Monitoring

10.2.1 Monitoring Task

Click **Monitoring** > **Monitoring Tasks** to enter the monitoring task page, as shown in the following figure.



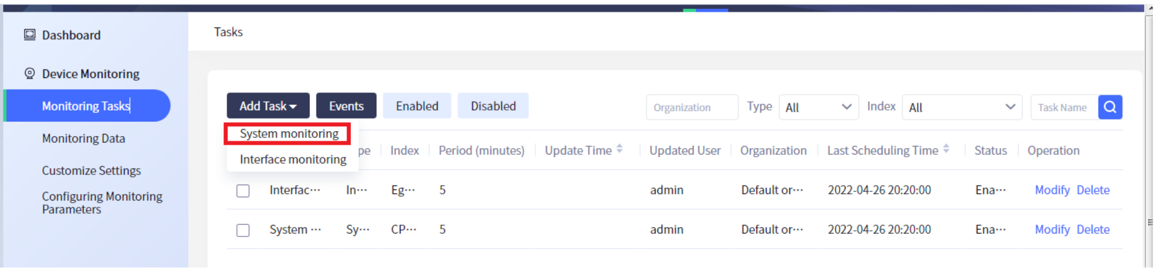
☐	Task Name	Type	Index	Period (minutes)	Update Time	Updated User	Organization	Last Scheduling Time	Status	Operation
☐	Interfac···	In···	Eg···	5		admin	Default or···	2022-04-26 20:20:00	Ena···	Modify Delete
☐	System ···	Sy···	CP···	5		admin	Default or···	2022-04-26 20:20:00	Ena···	Modify Delete

Total 2 Items, Selected 0 Items

Figure 10.2.1.1 Monitoring task button

To create a monitoring task, you can select whether to create system monitoring or interface monitoring, as shown in the following figure.

System monitoring:



☐	Task Name	pe	Index	Period (minutes)	Update Time	Updated User	Organization	Last Scheduling Time	Status	Operation
☐	Interfac···	In···	Eg···	5		admin	Default or···	2022-04-26 20:20:00	Ena···	Modify Delete
☐	System ···	Sy···	CP···	5		admin	Default or···	2022-04-26 20:20:00	Ena···	Modify Delete

Figure 10.2.1.2 System monitoring button

Fill in task name, collection period, indexes, resources, etc. to create system monitoring tasks, as shown in the following figure.

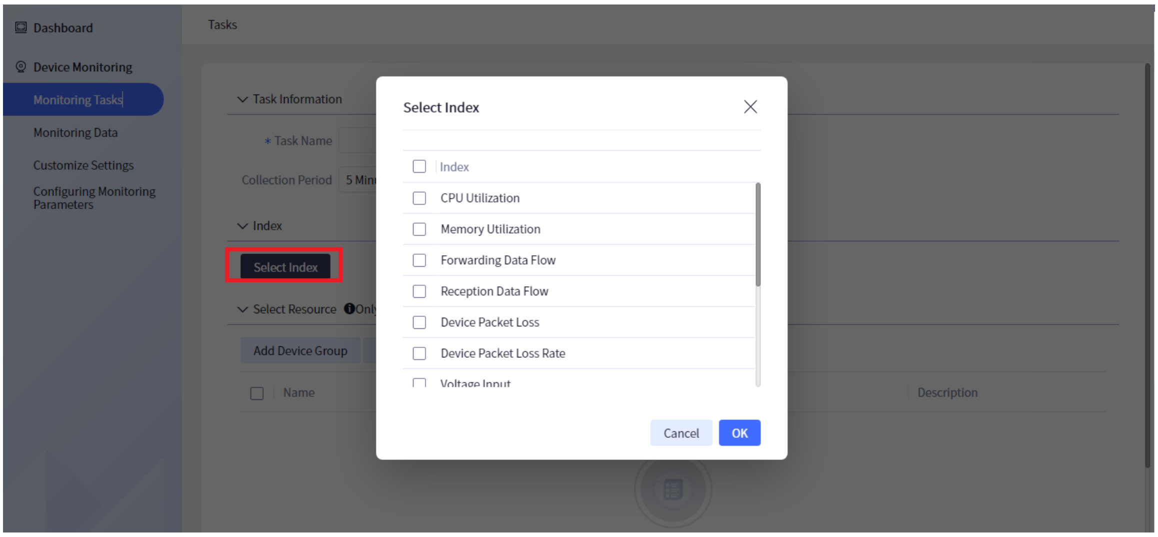
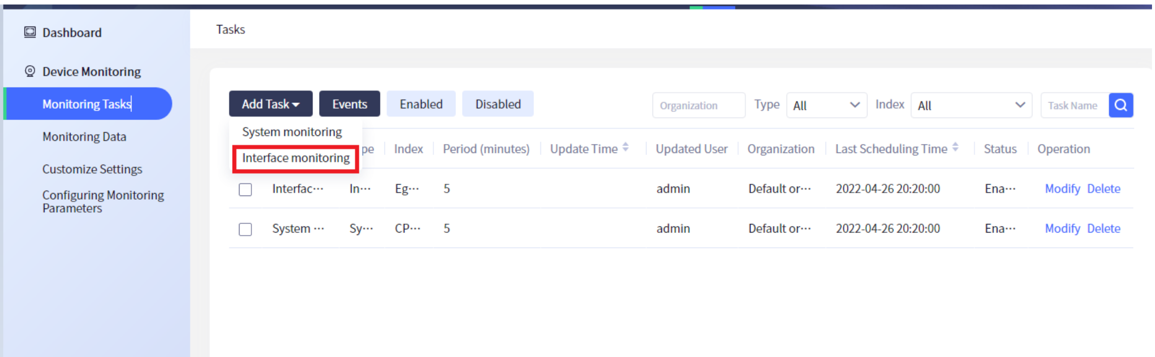


Figure 10.2.1.3 Create system monitoring task

Interface monitoring:



☐	...pe	Index	Period (minutes)	Update Time	Updated User	Organization	Last Scheduling Time	Status	Operation
☐ Interfac···	In···	Eg···	5		admin	Default or···	2022-04-26 20:20:00	Ena···	Modify Delete
☐ System ···	Sy···	CP···	5		admin	Default or···	2022-04-26 20:20:00	Ena···	Modify Delete

Figure 10.2.1.4 Interface monitoring button

Fill in task name, collection period, indexes, resources, etc. to create interface monitoring tasks, as shown in the following figure.

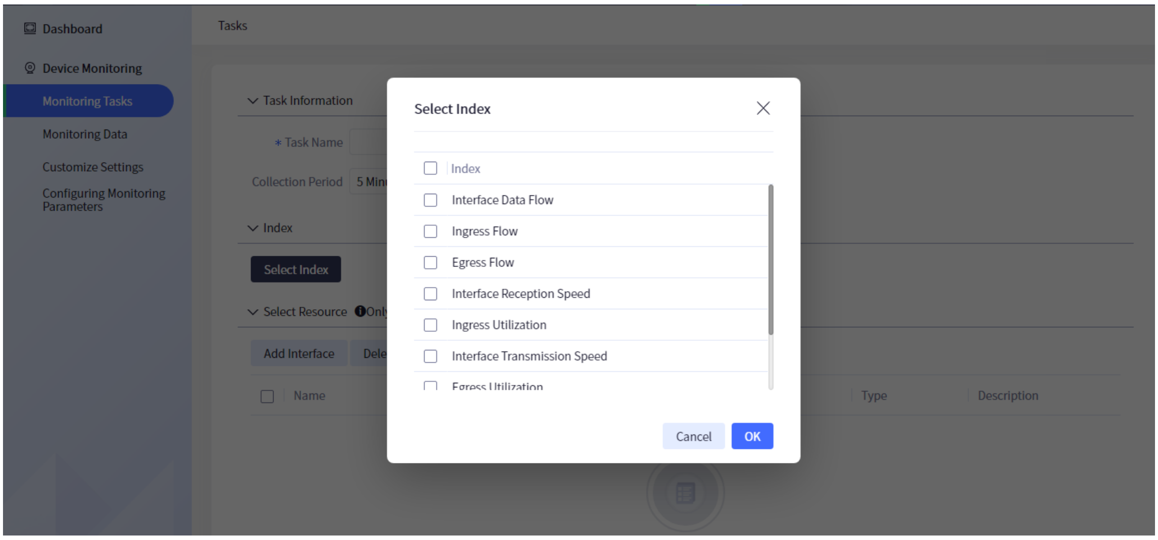
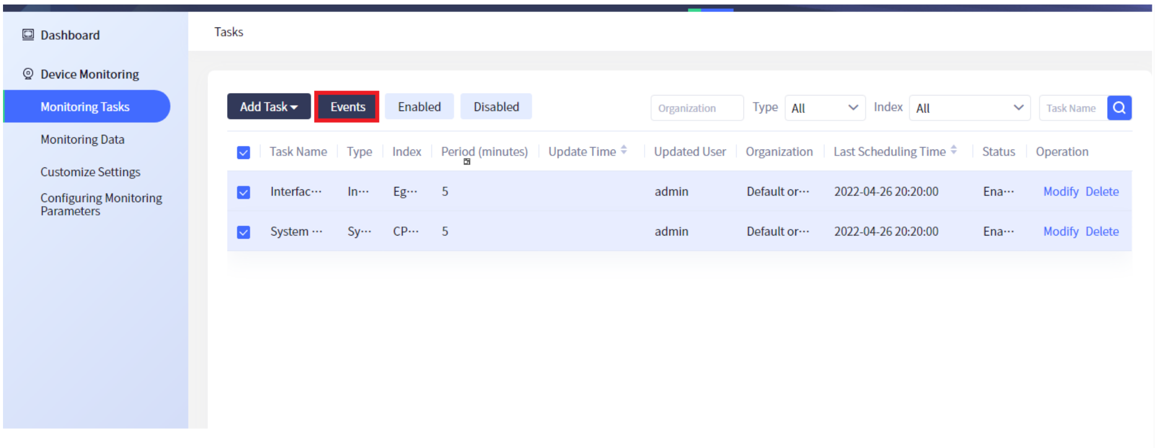


Figure 10.2.1.5 Interface monitoring task

After creating the monitoring task, click **Enabled** and **Disabled** to start or end monitoring. After selecting the monitoring task data, click the **Monitoring Data** button to jump to the monitoring data page to view the specific monitoring data (see the monitoring data page for details).

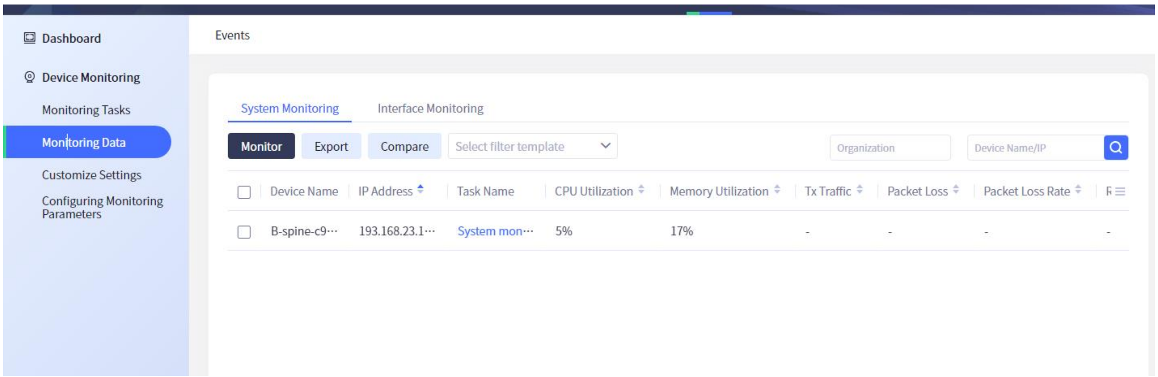


☑ Task Name	Type	Index	Period (minutes)	Update Time	Updated User	Organization	Last Scheduling Time	Status	Operation
☑ Interfac···	In···	Eg···	5		admin	Default or···	2022-04-26 20:20:00	Ena···	Modify Delete
☑ System ···	Sy···	CP···	5		admin	Default or···	2022-04-26 20:20:00	Ena···	Modify Delete

Figure 10.2.1.6 Monitoring task data

10.2.2 Monitoring Data

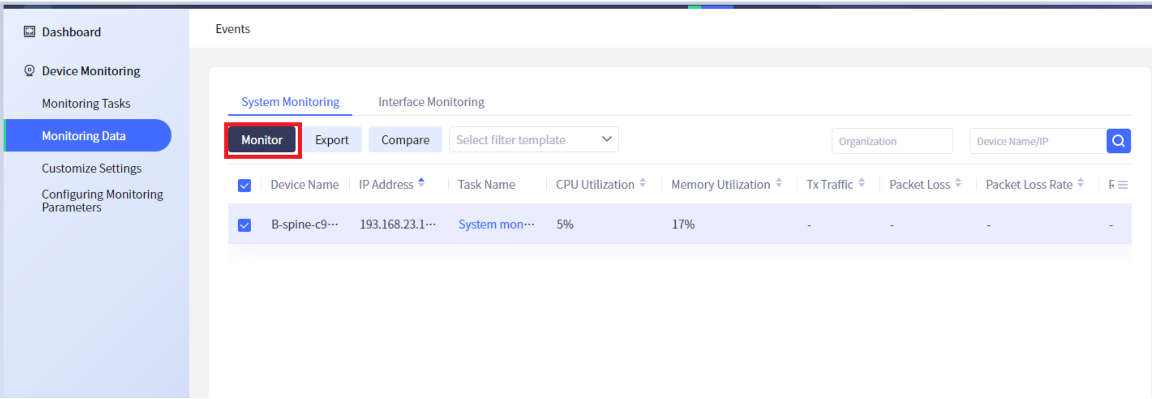
Click **Monitoring** > **Monitoring Data** to enter the monitoring data page, which visually presents the data monitored by the monitoring task, as shown in the following figure.



☐	Device Name	IP Address	Task Name	CPU Utilization	Memory Utilization	Tx Traffic	Packet Loss	Packet Loss Rate	R
☐	B-spine-c9···	193.168.23.1···	System mon···	5%	17%	-	-	-	-

Figure 10.2.2.1 Montioring data button

Select the data and click the **Monitor** button to view the monitoring details, as shown in the following figure.



☑	Device Name	IP Address	Task Name	CPU Utilization	Memory Utilization	Tx Traffic	Packet Loss	Packet Loss Rate	R
☑	B-spine-c9···	193.168.23.1···	System mon···	5%	17%	-	-	-	-

Figure 10.2.2.2 Monitor data

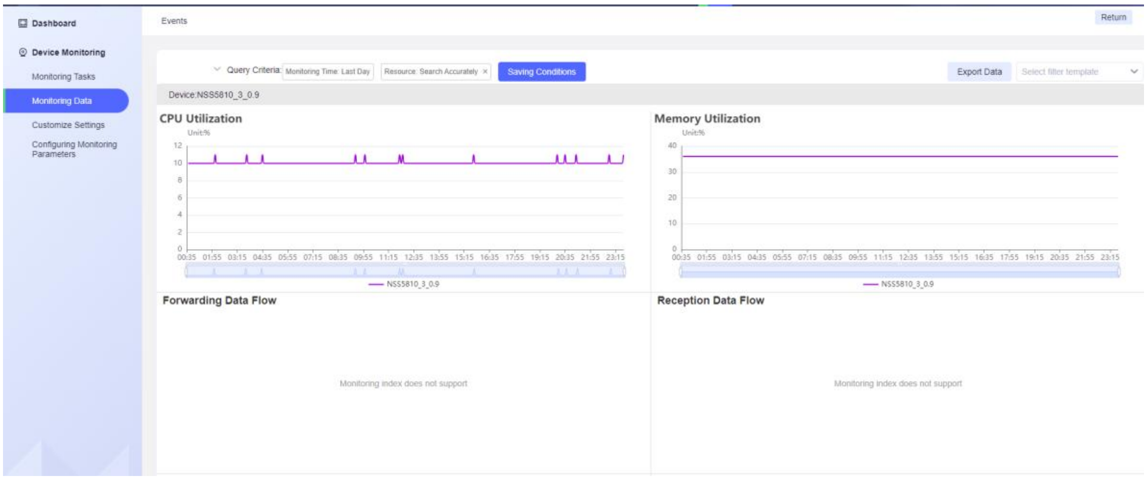
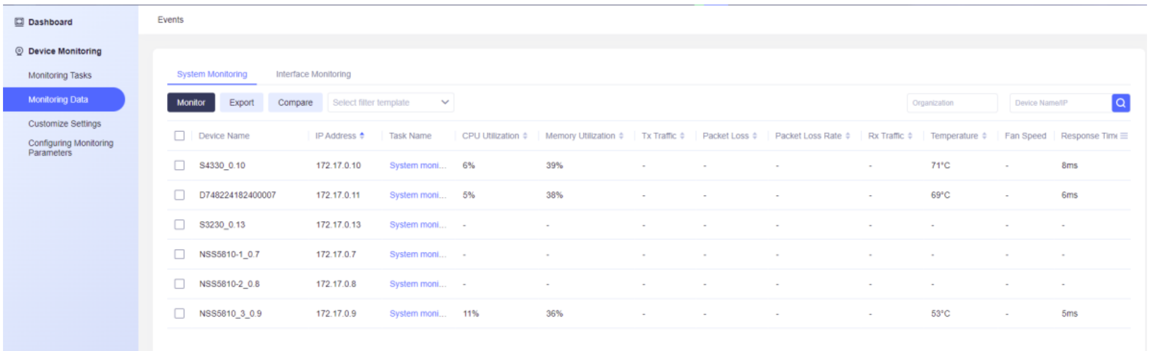


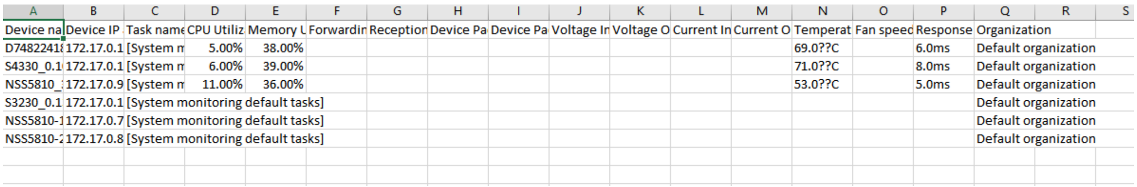
Figure 10.2.2.3 Monitoring data details

You can select to export monitoring data. Click the **Export** button directly to export all data. After selecting data, click **Export** to export only the selected data, as shown in the following figure.



☐	Device Name	IP Address	Task Name	CPU Utilization	Memory Utilization	Tx Traffic	Packet Loss	Packet Loss Rate	Rx Traffic	Temperature	Fan Speed	Response Time
☐	S4330_0.10	172.17.0.10	System moni...	6%	39%	-	-	-	-	71°C	-	8ms
☐	D748224182400007	172.17.0.11	System moni...	5%	38%	-	-	-	-	69°C	-	6ms
☐	S3230_0.13	172.17.0.13	System moni...	-	-	-	-	-	-	-	-	-
☐	NSS5810-1_0.7	172.17.0.7	System moni...	-	-	-	-	-	-	-	-	-
☐	NSS5810-2_0.8	172.17.0.8	System moni...	-	-	-	-	-	-	-	-	-
☐	NSS5810_3_0.9	172.17.0.9	System moni...	11%	36%	-	-	-	-	53°C	-	5ms

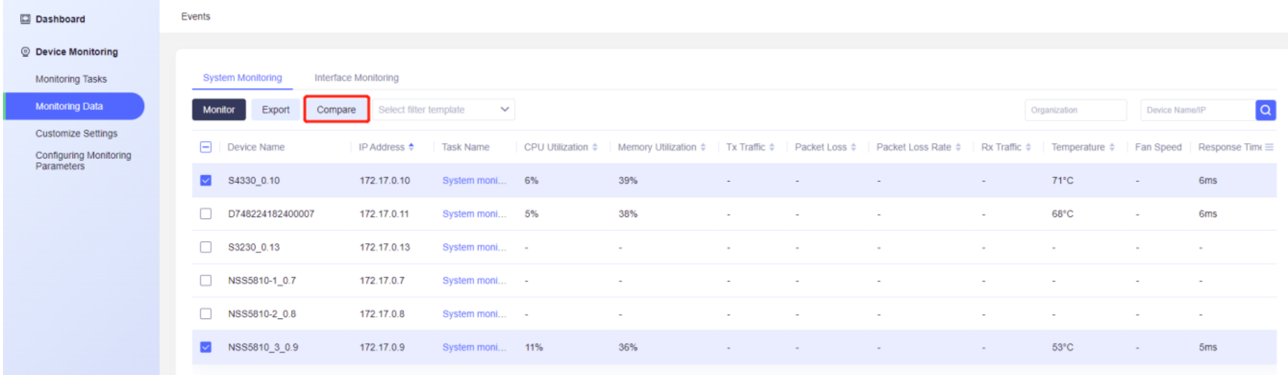
Figure 10.2.2.4 Export monitoring data



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Device na	Device IP	Task name	CPU Utiliz	Memory U	Forwardin	Reception	Device Pa	Device Pa	Voltage In	Voltage O	Current In	Current O	Temperat	Fan speed	Response	Organization		
D74822418	172.17.0.1	[System m	5.00%	38.00%									69.0??C		6.0ms	Default organization		
S4330_0.1	172.17.0.1	[System m	6.00%	39.00%									71.0??C		8.0ms	Default organization		
NSS5810_3	172.17.0.9	[System m	11.00%	36.00%									53.0??C		5.0ms	Default organization		
S3230_0.1	172.17.0.1	[System monitoring default tasks]														Default organization		
NSS5810-1	172.17.0.7	[System monitoring default tasks]														Default organization		
NSS5810-2	172.17.0.8	[System monitoring default tasks]														Default organization		

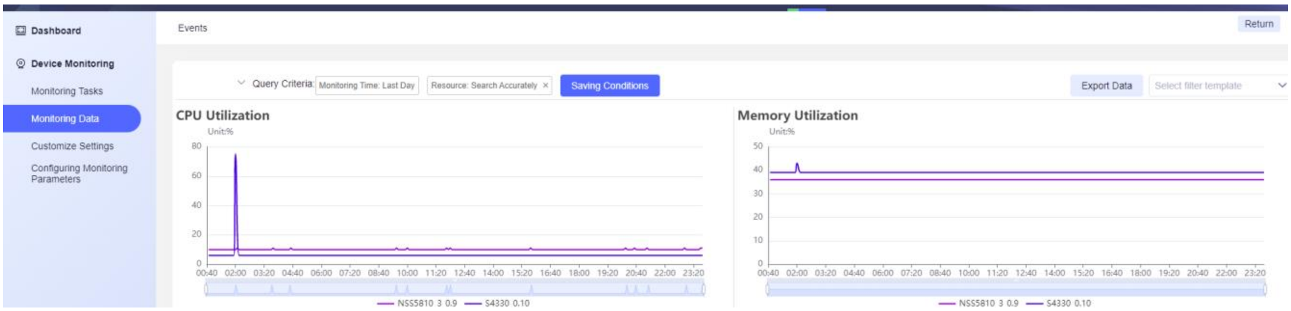
Figure 10.2.2.5 Exported monitoring data excel

Users can select multiple monitoring data for comparison, as shown in the following figure.



☐	Device Name	IP Address	Task Name	CPU Utilization	Memory Utilization	Tx Traffic	Packet Loss	Packet Loss Rate	Rx Traffic	Temperature	Fan Speed	Response Time
☑	S4330_0.10	172.17.0.10	System moni...	6%	39%	-	-	-	-	71°C	-	6ms
☐	D748224182400007	172.17.0.11	System moni...	5%	38%	-	-	-	-	68°C	-	6ms
☐	S3230_0.13	172.17.0.13	System moni...	-	-	-	-	-	-	-	-	-
☐	NSS5810-1_0.7	172.17.0.7	System moni...	-	-	-	-	-	-	-	-	-
☐	NSS5810-2_0.8	172.17.0.8	System moni...	-	-	-	-	-	-	-	-	-
☑	NSS5810_3_0.9	172.17.0.9	System moni...	11%	36%	-	-	-	-	53°C	-	5ms

Figure 10.2.2.6 Compare the monitoring data



Query Criteria: Monitoring Time: Last Day | Resource: Search Accurately

Figure 10.2.2.7 Comparing result of monitoring data

10.2.3 Customize Monitoring Indexes

You can customize monitoring indexes. Click **Monitoring** > **Customize Settings**, as shown in the following figure.

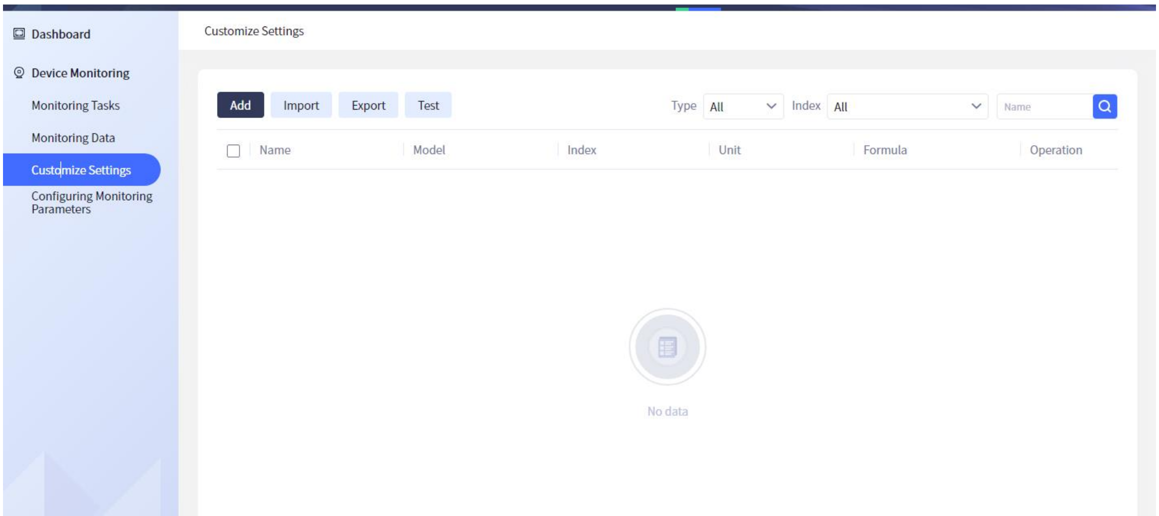
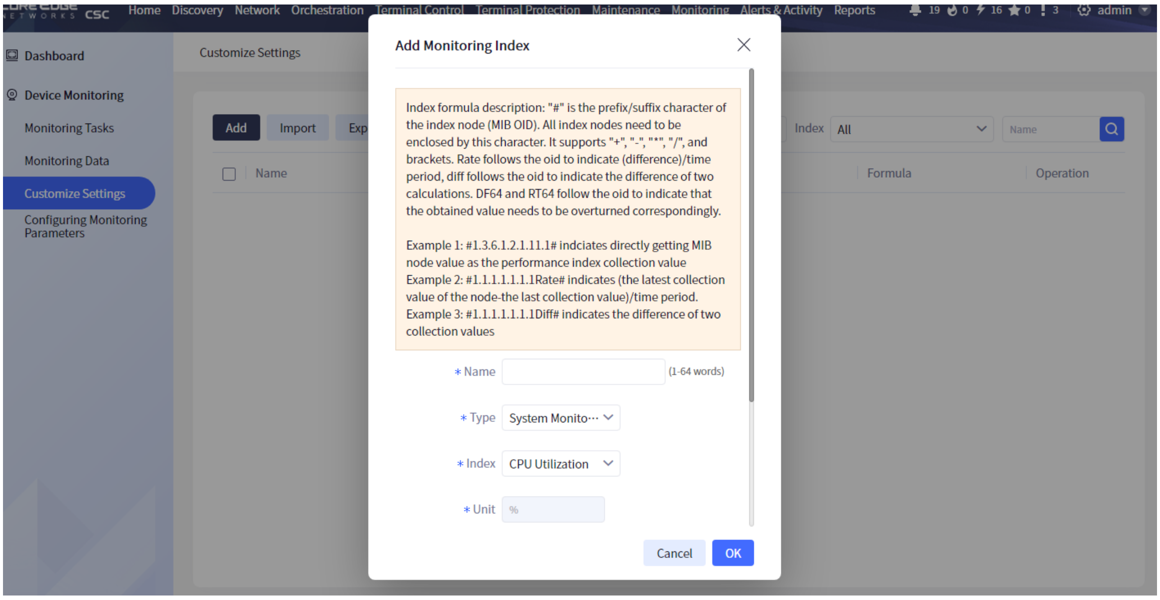


Figure 10.2.3.1 Customize monitoring



Index formula description: "#" is the prefix/suffix character of the index node (MIB OID). All index nodes need to be enclosed by this character. It supports "+", "-", "*", "/", and brackets. Rate follows the oid to indicate (difference)/time period, diff follows the oid to indicate the difference of two calculations. DF64 and RT64 follow the oid to indicate that the obtained value needs to be overturned correspondingly.

Example 1: #1.3.6.1.2.1.11.1# indciates directly getting MIB node value as the performance index collection value
Example 2: #1.1.1.1.1.1.1Rate# indicates (the latest collection value of the node-the last collection value)/time period.
Example 3: #1.1.1.1.1.1.1Diff# indicates the difference of two collection values

* Name (1-64 words)
* Type System Monito···
* Index CPU Utilization
* Unit %

Figure 10.2.3.2 Add monitoring indexes

Click the **Import** and **Export** buttons to customize the import or export of data, as shown in the following figure.

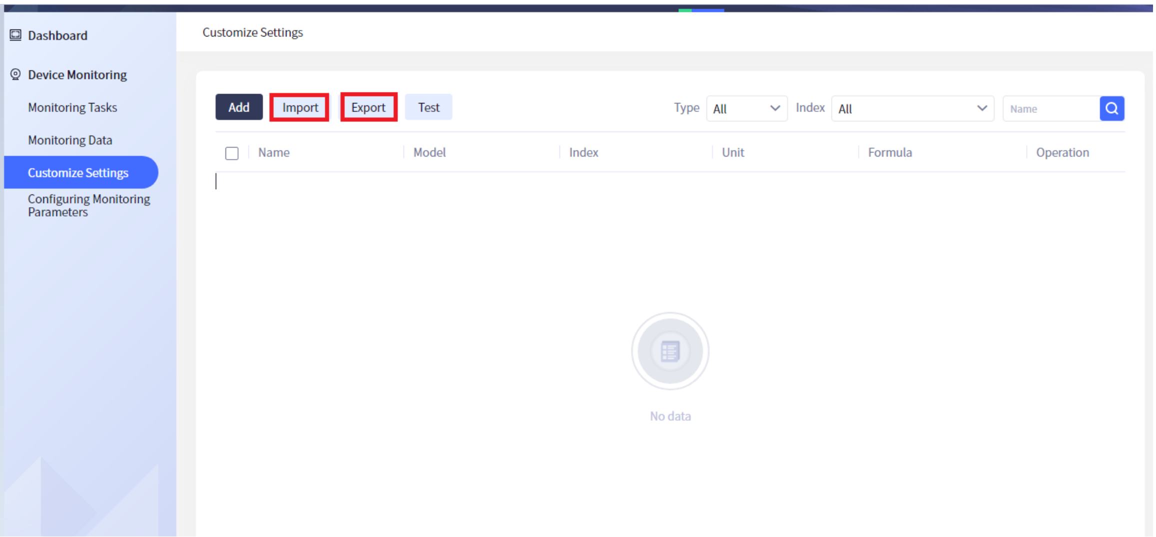
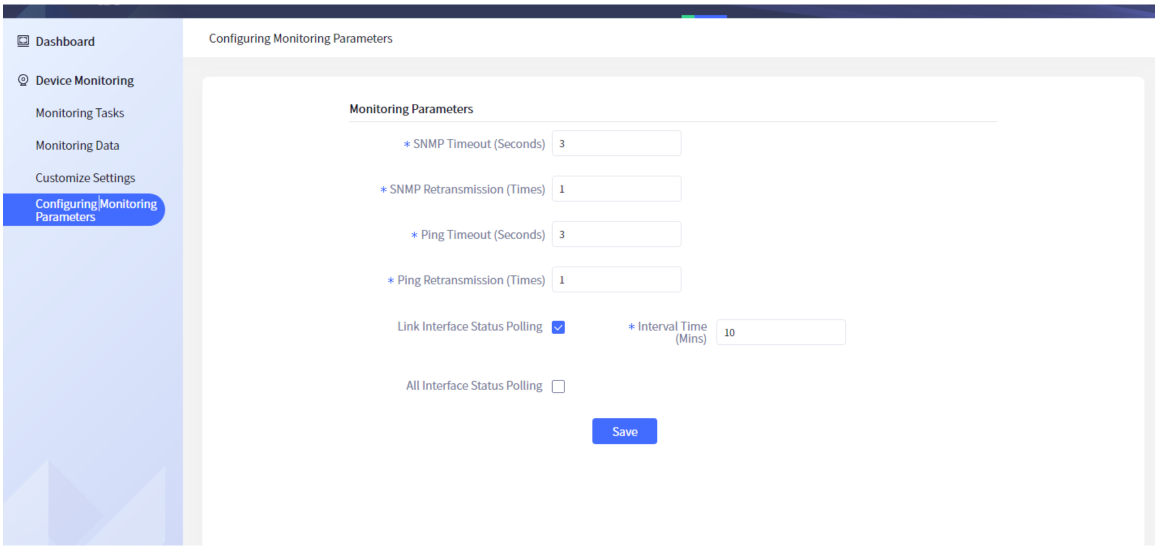


Figure 10.2.3.3 Customize the import and export of monitoring indexes

Click the **Test** button to test the selected monitoring indexes.

10.2.4 Status Monitoring Configuration

Click **Monitoring** > **Configuring Monitoring Parameters** to enter the status monitoring configuration page. You can customize the SNMP timeout, SNMP retransmission, Ping timeout, Ping retransmission, link interface status polling, interval time, all interface status polling and other indexes, as shown in the following figure.



* SNMP Timeout (Seconds) 3

* SNMP Retransmission (Times) 1

* Ping Timeout (Seconds) 3

* Ping Retransmission (Times) 1

Link Interface Status Polling ☑ * Interval Time (Mins) 10

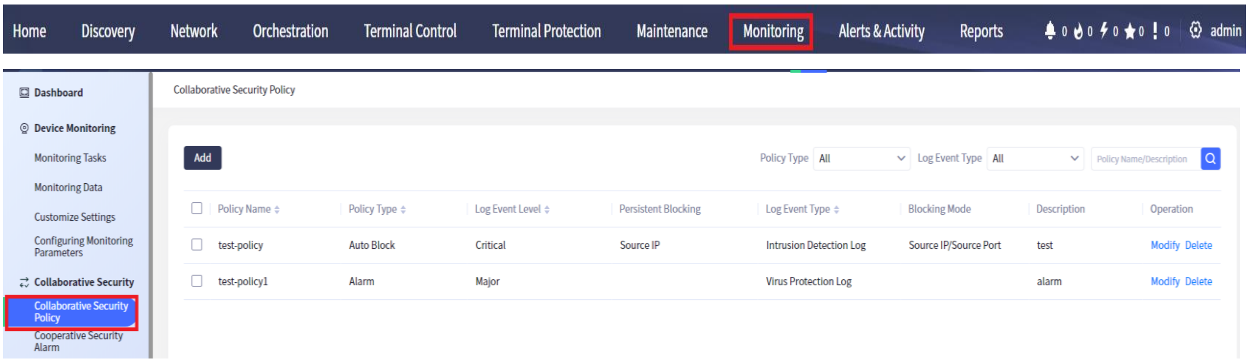
All Interface Status Polling ☐

Figure 10.2.4.1 Status monitoring configuration

10.3 Collaborative Security

10.3.1 Collaborative Security Policy

Click **Monitoring** > **Collaborative Security Policy** to enter the **Collaborative Security Policy** page, as shown in the following figure:

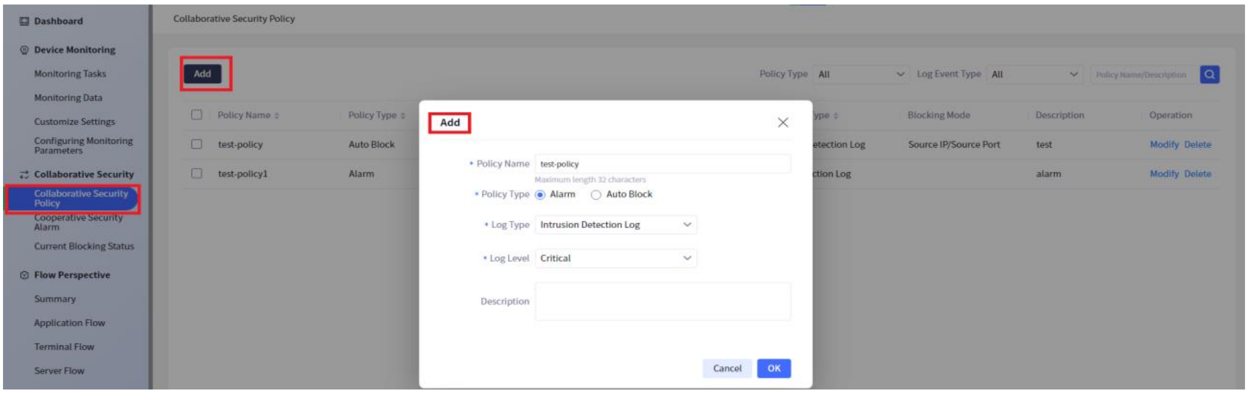


Policy Type All Log Event Type All

☐	Policy Name	Policy Type	Log Event Level	Persistent Blocking	Log Event Type	Blocking Mode	Description	Operation
☐	test-policy	Auto Block	Critical	Source IP	Intrusion Detection Log	Source IP/Source Port	test	Modify Delete
☐	test-policy1	Alarm	Major		Virus Protection Log		alarm	Modify Delete

Figure 10.3.1.1 Collaborative security policy

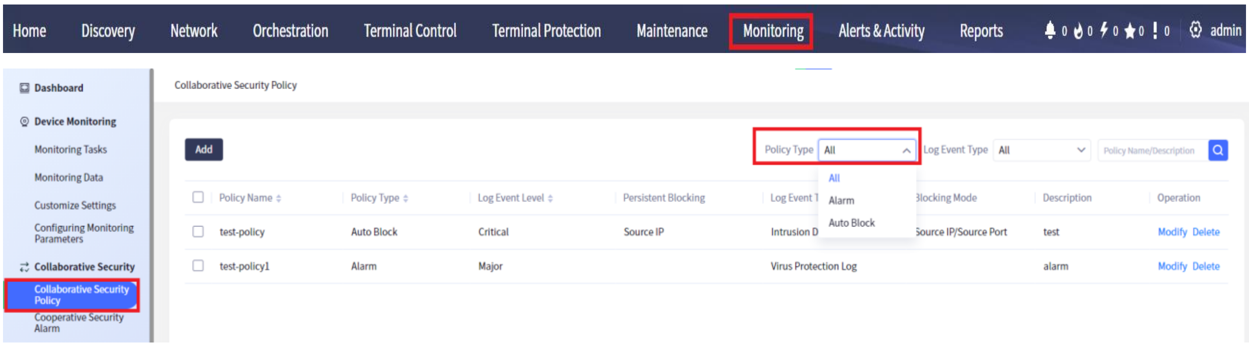
Click **Add** in the upper left corner of the list to open the **Add** interface, where you can add corresponding security policies, as shown in the following figure. You can select different log types and log levels, or describe security policies.



* Policy Name: test-policy
Maximum length 32 characters
* Policy Type: ● Alarm ○ Auto Block
* Log Type: Intrusion Detection Log
* Log Level: Critical
Description:

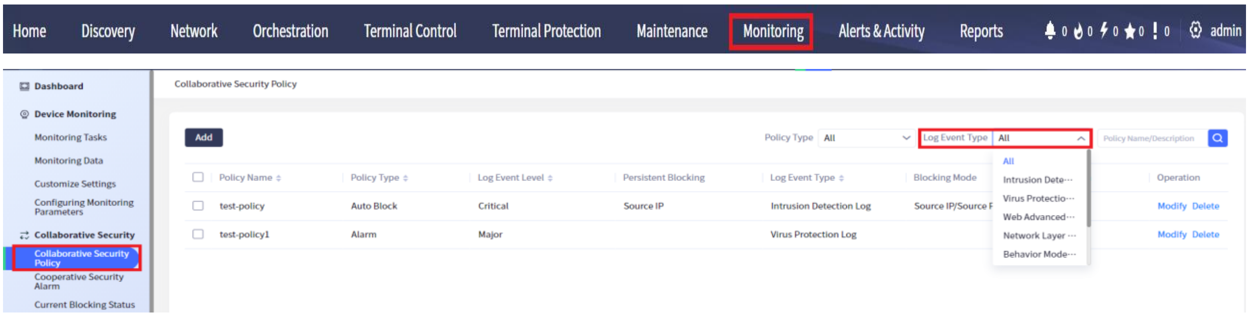
Figure 10.3.1.2 Add collaborative security policy

The user can query the security policy according to the policy type and log event type, or fuzzy query by filling in the policy name and description. The effect is shown in the figure.



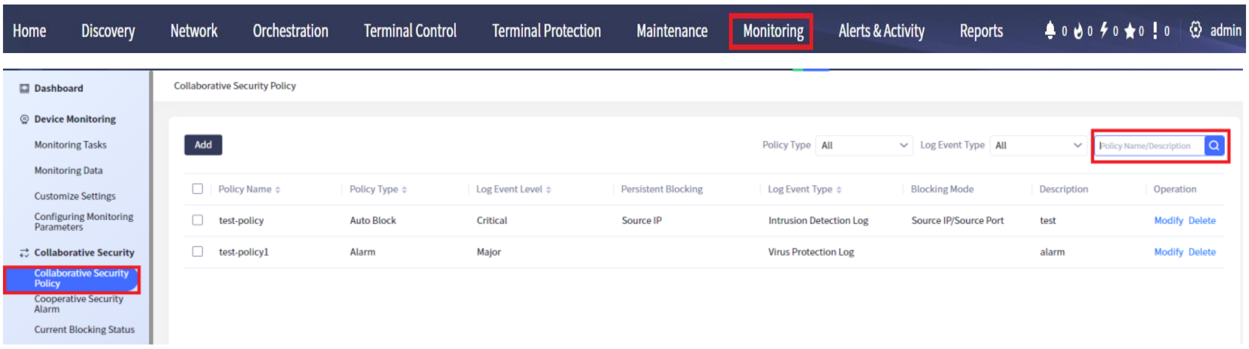
☐	Policy Name	Policy Type	Log Event Level	Persistent Blocking	Log Event T	Blocking Mode	Description	Operation
☐	test-policy	Auto Block	Critical	Source IP	Intrusion D	Source IP/Source Port	test	Modify Delete
☐	test-policy1	Alarm	Major		Virus Protection Log		alarm	Modify Delete

Figure 10.3.1.3 Query the collaborative security policy by policy type



☐	Policy Name	Policy Type	Log Event Level	Persistent Blocking	Log Event Type	Blocking Mode	Operation
☐	test-policy	Auto Block	Critical	Source IP	Intrusion Detection Log	Source IP/Source F	Modify Delete
☐	test-policy1	Alarm	Major		Virus Protection Log		Modify Delete

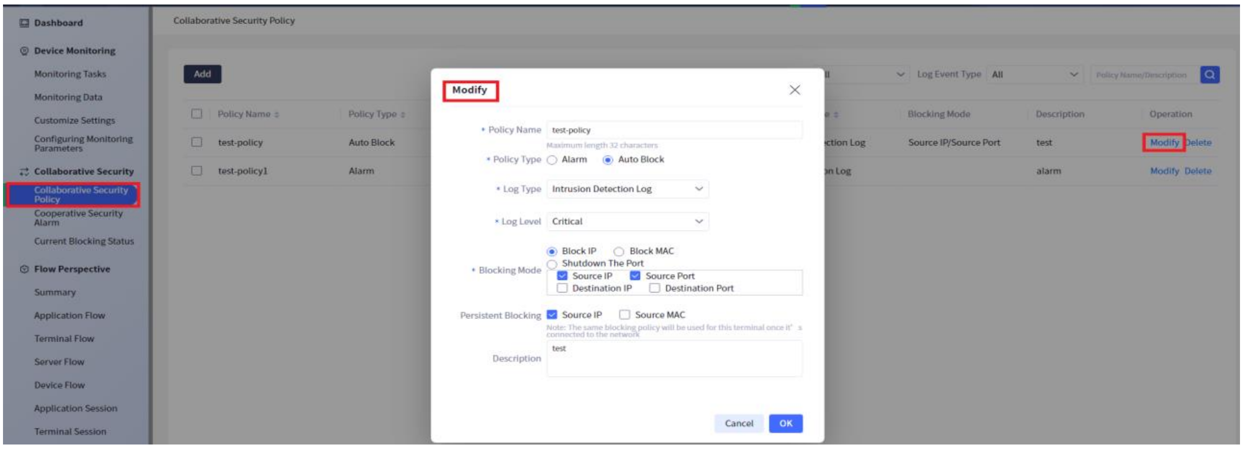
Figure 10.3.1.4 Query the collaborative security policy by log event type



☐	Policy Name	Policy Type	Log Event Level	Persistent Blocking	Log Event Type	Blocking Mode	Description	Operation
☐	test-policy	Auto Block	Critical	Source IP	Intrusion Detection Log	Source IP/Source Port	test	Modify Delete
☐	test-policy1	Alarm	Major		Virus Protection Log		alarm	Modify Delete

Figure 10.3.1.5 Query the collaborative security policy by policy name or description

Click the **Modify** button of a security policy to modify the policy name, policy type, log type and other information. The effect is shown in the figure:



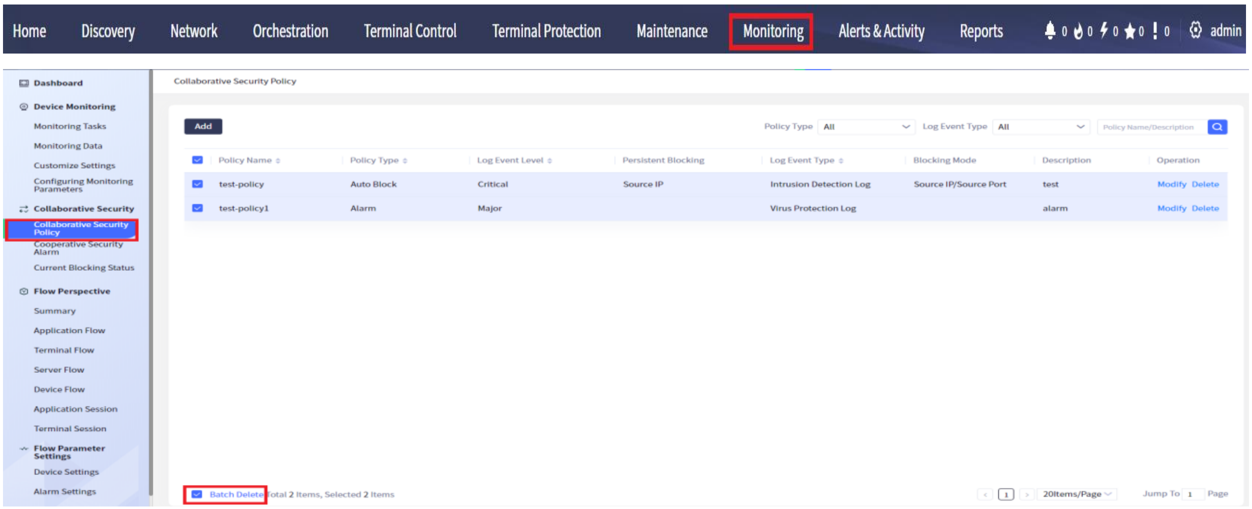
Modify

- Policy Name: test-policy (Maximum length 32 characters)
- Policy Type: ○ Alarm ● Auto Block
- Log Type: Intrusion Detection Log
- Log Level: Critical
- Blocking Mode: ● Block IP ○ Block MAC ○ Shutdown The Port
  - ☑ Source IP ☑ Source Port
  - ☐ Destination IP ☐ Destination Port
- Persistent Blocking: ☑ Source IP ☐ Source MAC (Note: The same blocking policy will be used for this terminal once it' s connected to the network)
- Description: test

Figure 10.3.1.6 Modify the collaborative security policy

Users can delete the selected security policy. Deletion is divided into batch deletion and single deletion.

Batch delete: Select the desired security policies, and click **Batch delete** under the added security policy list to delete all the selected security policy information, as shown in the figure.

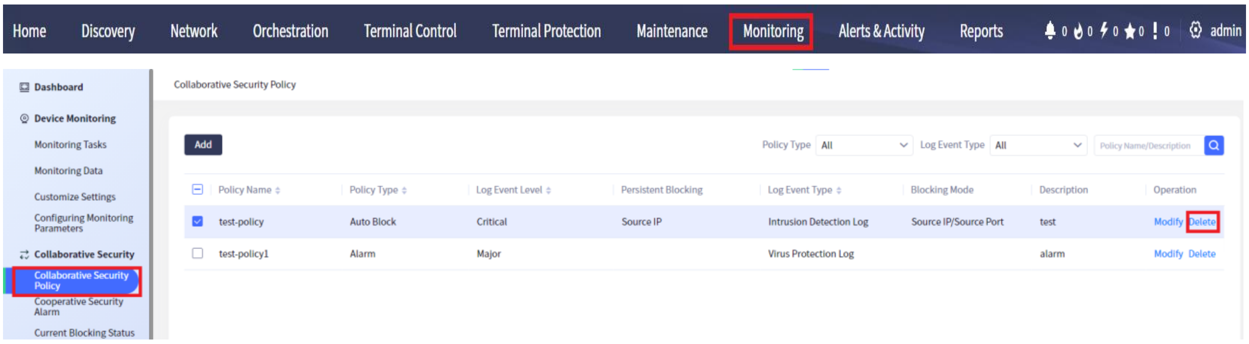


☑	Policy Name	Policy Type	Log Event Level	Persistent Blocking	Log Event Type	Blocking Mode	Description	Operation
☑	test-policy	Auto Block	Critical	Source IP	Intrusion Detection Log	Source IP/Source Port	test	Modify Delete
☑	test-policy1	Alarm	Major		Virus Protection Log		alarm	Modify Delete

Total 2 Items, Selected 2 Items

Figure 10.3.1.7 Batch delete collaborative security policies

Click the **Delete** button of a security policy to delete the security policy. The effect is shown in the figure:

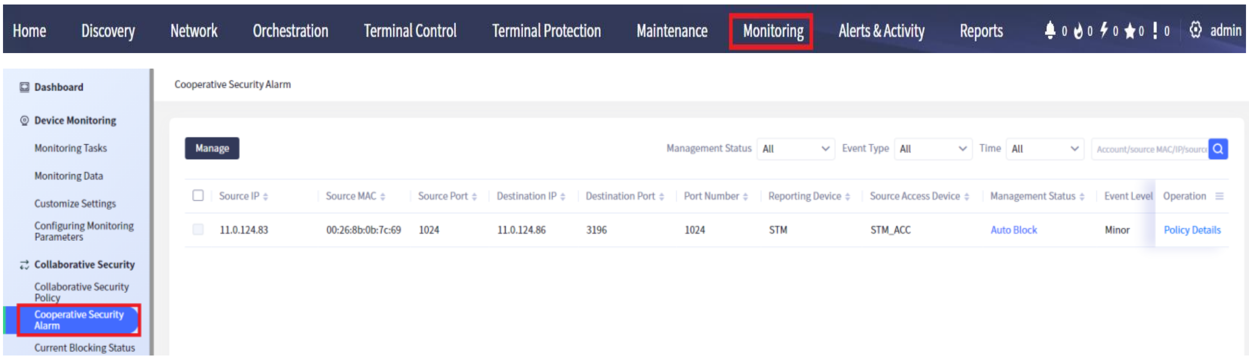


☐	Policy Name	Policy Type	Log Event Level	Persistent Blocking	Log Event Type	Blocking Mode	Description	Operation
☑	test-policy	Auto Block	Critical	Source IP	Intrusion Detection Log	Source IP/Source Port	test	Modify Delete
☐	test-policy1	Alarm	Major		Virus Protection Log		alarm	Modify Delete

Figure 10.3.1.8 Delete a single collaborative security policy

10.3.2 Collaborative Security Alarms

Click **Monitoring** > **Collaborative Security Policy Alarm** to enter the **Collaborative Security Alarm** page, as shown in the following figure:



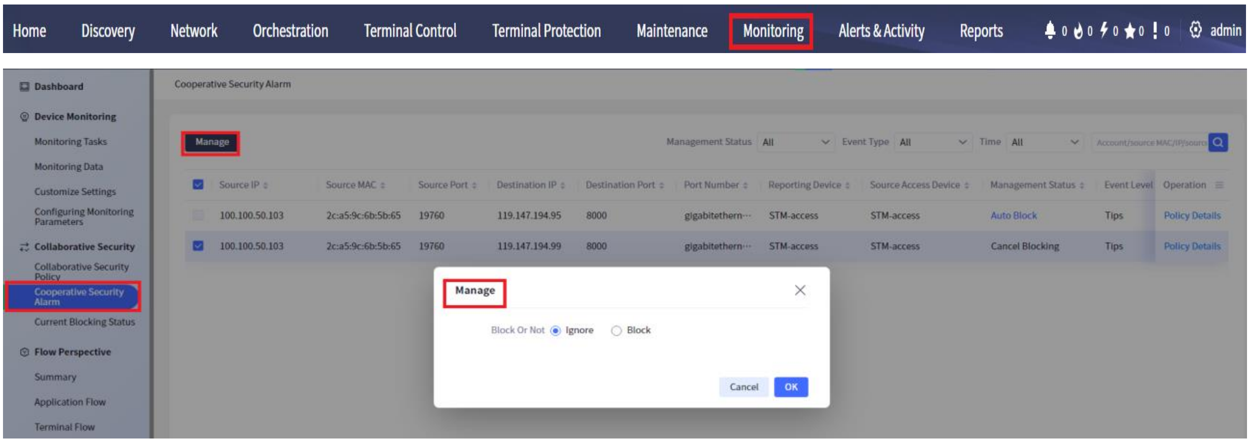
Cooperative Security Alarm

Management Status: All; Event Type: All; Time: All

☐	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Port Number	Reporting Device	Source Access Device	Management Status	Event Level	Operation
☐	11.0.124.83	00:26:8b:0b:7c:69	1024	11.0.124.86	3196	1024	STM	STM_ACC	Auto Block	Minor	Policy Details

Figure 10.3.2.1 Display collaborative security alarm list

Click the **Manage** button in the upper left corner of a list to process the selected collaborative security events. One is **Ignore**, that is, ignore the collaborative security event alarm. The other is **Block**, and you can select the block mode, **Block MAC** or **Block IP**. For the block mode, you can select to block the source IP and source port, or destination IP and destination port, or configure **Persistent Blocking**, and the corresponding options are source IP and source MAC, as shown in the following figure.



Cooperative Security Alarm

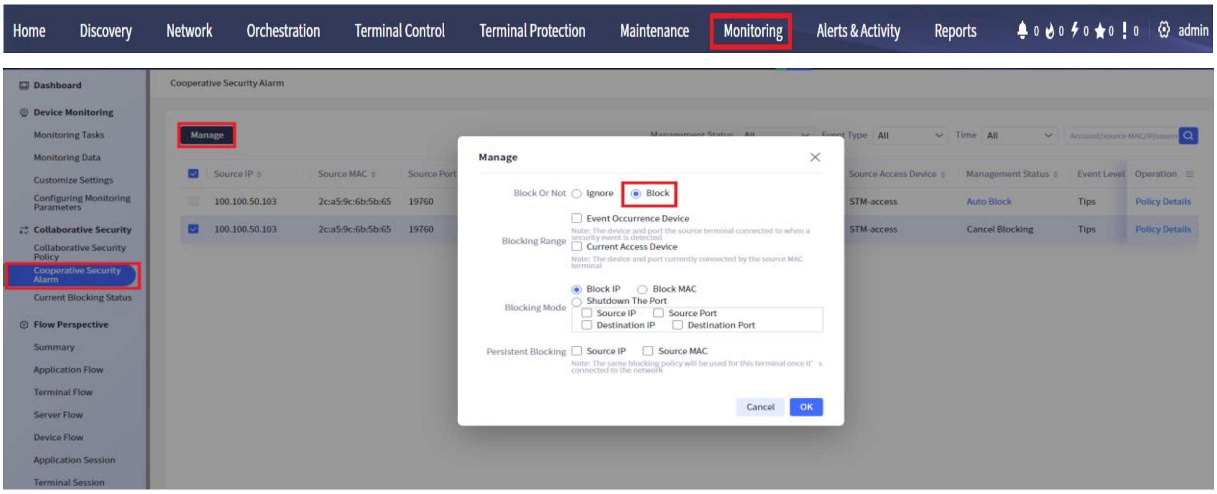
Management Status: All; Event Type: All; Time: All

☑	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Port Number	Reporting Device	Source Access Device	Management Status	Event Level	Operation
☐	100.100.50.103	2c:a5:9c:6b:5b:65	19760	119.147.194.95	8000	gigabitethern···	STM-access	STM-access	Auto Block	Tips	Policy Details
☑	100.100.50.103	2c:a5:9c:6b:5b:65	19760	119.147.194.99	8000	gigabitethern···	STM-access	STM-access	Cancel Blocking	Tips	Policy Details

Manage

Block Or Not ● Ignore ○ Block

Figure 10.3.2.2 Ignore collaborative security alarm event



Cooperative Security Alarm

☑	Source IP	Source MAC	Source Port	Source Access Device	Management Status	Event Level	Operation
☐	100.100.50.103	2c:a5:9c:6b:5b:65	19760	STM-access	Auto Block	Tips	Policy Details
☑	100.100.50.103	2c:a5:9c:6b:5b:65	19760	STM-access	Cancel Blocking	Tips	Policy Details

Manage

Block Or Not ○ Ignore ● Block

Blocking Range ☐ Event Occurrence Device

Note: The device and port the source terminal connected to when a security event is detected

☐ Current Access Device

Note: The device and port currently connected by the source MAC terminal

Blocking Mode ● Block IP ○ Block MAC

○ Shutdown The Port

☐ Source IP ☐ Source Port

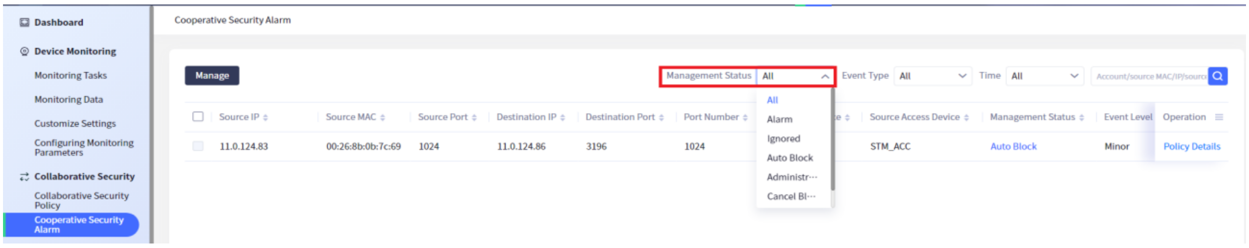
☐ Destination IP ☐ Destination Port

Persistent Blocking ☐ Source IP ☐ Source MAC

Note: The same blocking policy will be used for this terminal once it' s connected to the network

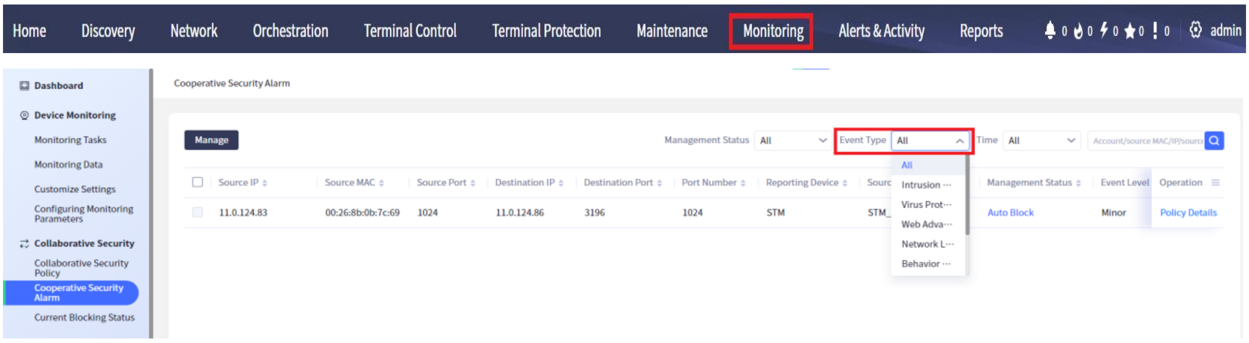
Figure 10.3.2.3 Set blocking

The user can query according to the management status, event type and time, or fuzzy query through account, source MAC, access device, etc. and the effect is shown in the figure.



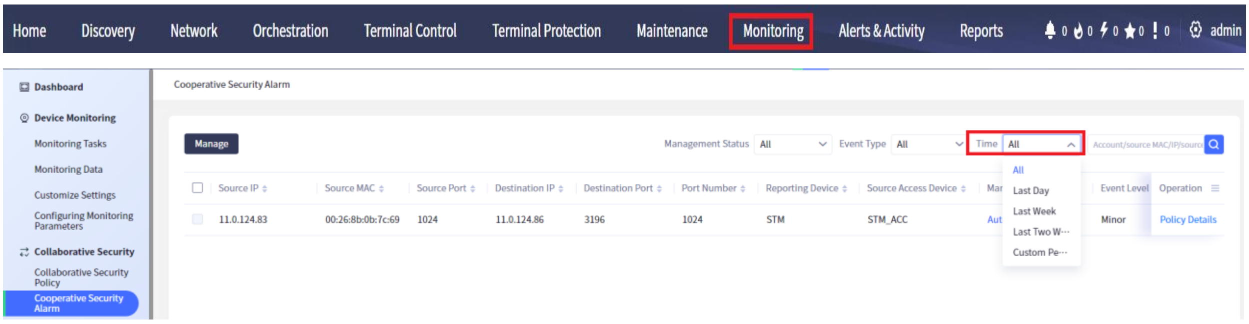
☐	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Port Number	Source Access Device	Management Status	Event Level	Operation
☐	11.0.124.83	00:26:8b:0b:7c:69	1024	11.0.124.86	3196	1024	STM_ACC	Auto Block	Minor	Policy Details

Figure 10.3.2.4 Query by management status



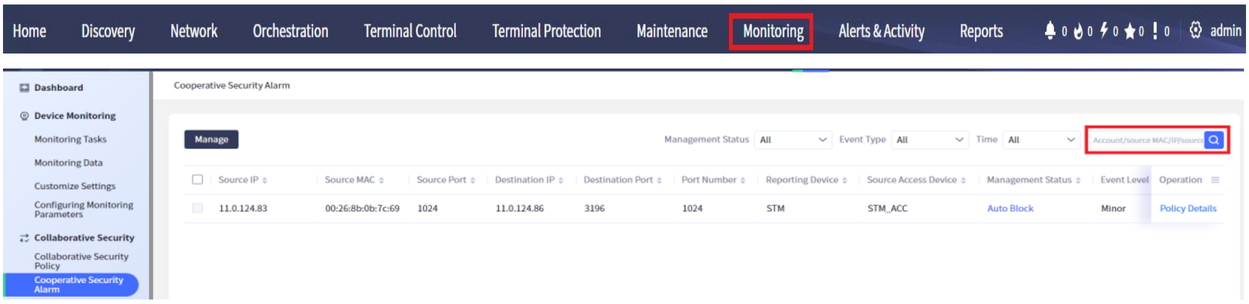
☐	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Port Number	Reporting Device	Sourc	Management Status	Event Level	Operation
☐	11.0.124.83	00:26:8b:0b:7c:69	1024	11.0.124.86	3196	1024	STM	STM_	Auto Block	Minor	Policy Details

Figure 10.3.2.5 Query by event type



☐	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Port Number	Reporting Device	Source Access Device	Mar	Event Level	Operation
☐	11.0.124.83	00:26:8b:0b:7c:69	1024	11.0.124.86	3196	1024	STM	STM_ACC	Aut	Minor	Policy Details

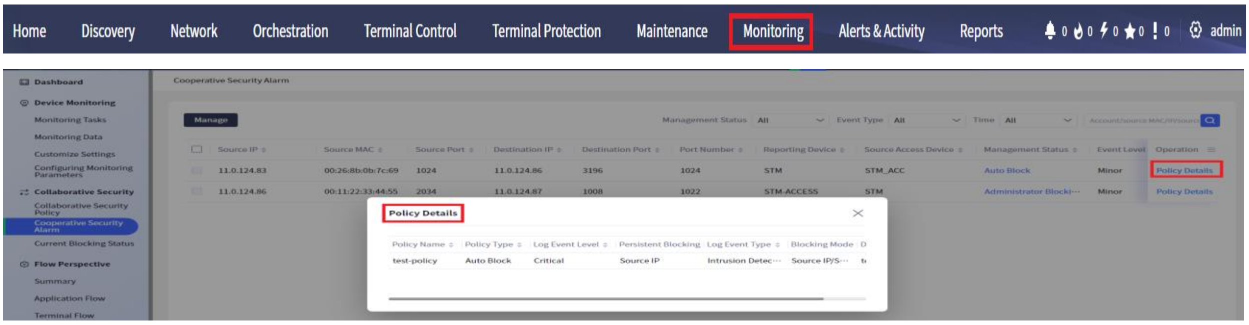
Figure 10.3.2.6 Query by time



☐	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Port Number	Reporting Device	Source Access Device	Management Status	Event Level	Operation
☐	11.0.124.83	00:26:8b:0b:7c:69	1024	11.0.124.86	3196	1024	STM	STM_ACC	Auto Block	Minor	Policy Details

Figure 10.3.2.7 Fuzzy query

The user can click the **Policy Details** button of the security alarm event to view the details of the alarm event, and the effect is shown in the figure:



☐	Source IP	Source MAC	Source Port	Destination IP	Destination Port	Port Number	Reporting Device	Source Access Device	Management Status	Event Level	Operation
☐	11.0.124.83	00:26:8b:0b:7c:69	1024	11.0.124.86	3196	1024	STM	STM_ACC	Auto Block	Minor	Policy Details
☐	11.0.124.86	00:11:22:33:44:55	2034	11.0.124.87	1008	1022	STM-ACCESS	STM	Administrator Blocki···	Minor	Policy Details

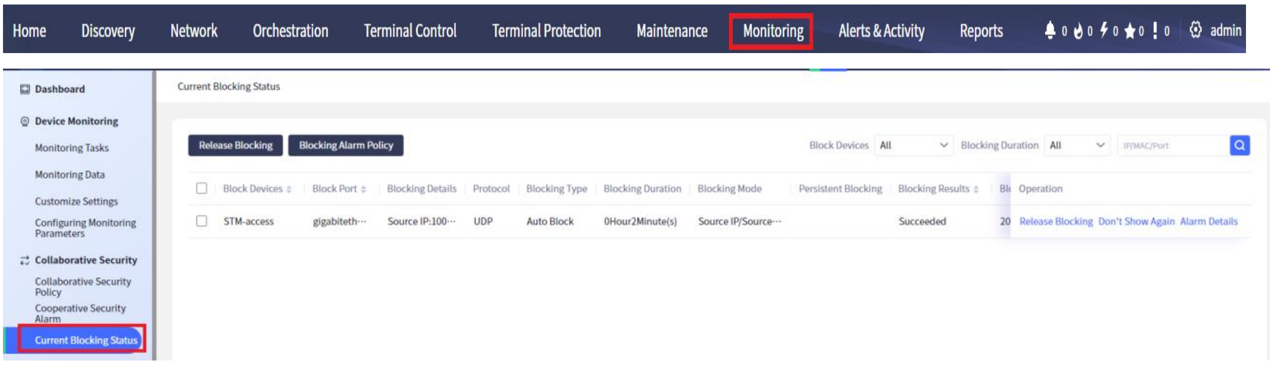
Policy Details

Policy Name	Policy Type	Log Event Level	Persistent Blocking	Log Event Type	Blocking Mode	D
test-policy	Auto Block	Critical	Source IP	Intrusion Detec···	Source IP/S···	t

Figure 10.3.2.8 View the alarm event details

10.3.3 Current Blocking Status

Click **Monitoring** > **Current Blocking Status** to enter the current blocking status page, as shown in the following figure



Current Blocking Status

☐	Block Devices	Block Port	Blocking Details	Protocol	Blocking Type	Blocking Duration	Blocking Mode	Persistent Blocking	Blocking Results	Bl	Operation
☐	STM-access	gigabiteth···	Source IP:100···	UDP	Auto Block	0Hour2Minute(s)	Source IP/Source···		Succeeded	20	Release Blocking Don't Show Again Alarm Details

Figure 10.3.3.1 Current blocking status list

Click the **Release Blocking** button in the upper left corner of the page to unblock the selected blocking event, and the effect is as shown in the figure:

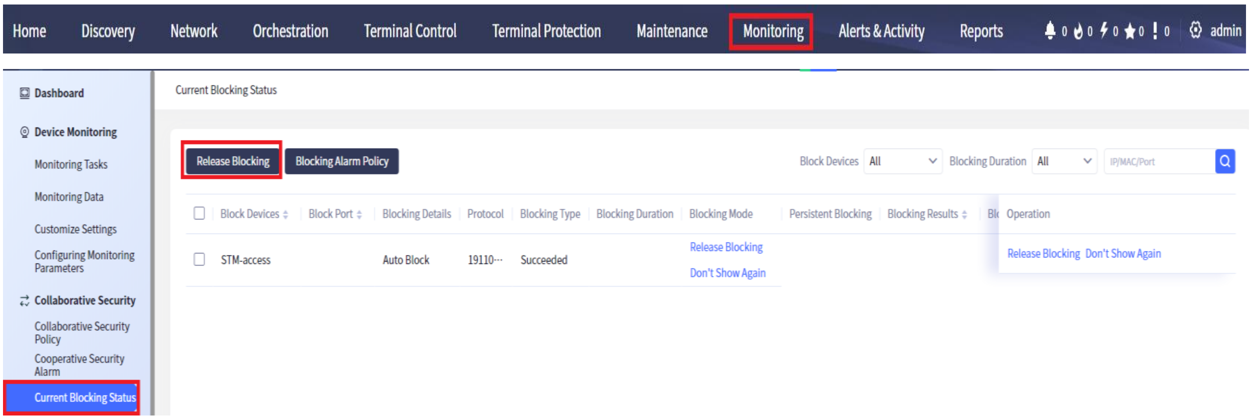
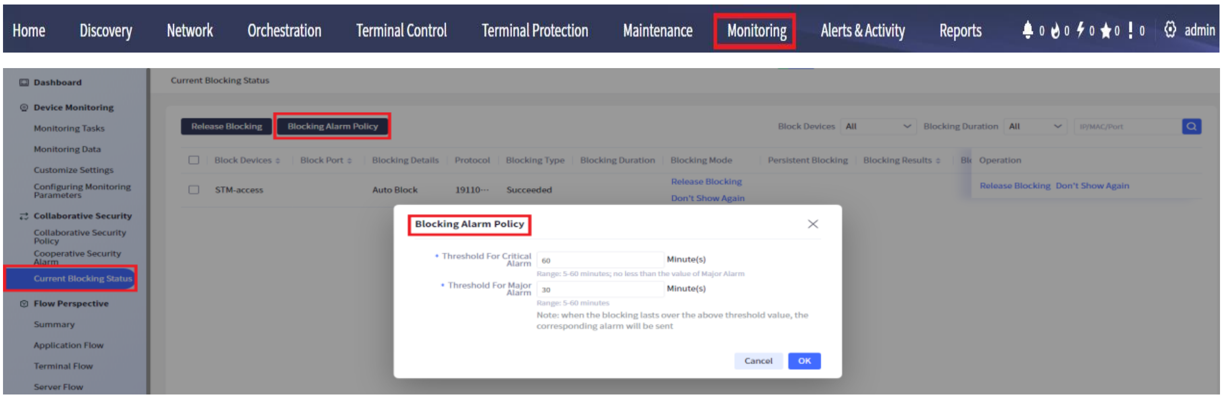


Figure 10.3.3.2 Release blocking

Click the **Blocking Alarm Policy** button in the upper left corner of the page to set **Blocking Alarm Policy**, and the effect is shown in the figure:



Blocking Alarm Policy

* Threshold For Critical Alarm: 60 Minute(s)
Range: 5-60 minutes; no less than the value of Major Alarm

* Threshold For Major Alarm: 30 Minute(s)
Range: 5-60 minutes

Note: when the blocking lasts over the above threshold value, the corresponding alarm will be sent

Figure 10.3.3.3 Set blocking alarm policy

The user can query according to the blocking device and blocking duration, or fuzzy query through IP, MAC, port, etc. and the effect is shown in the figure.

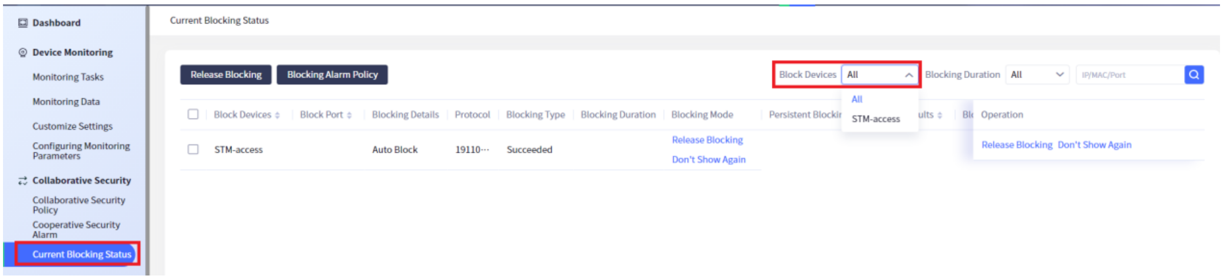


Figure 10.3.3.4 Query by blocking device

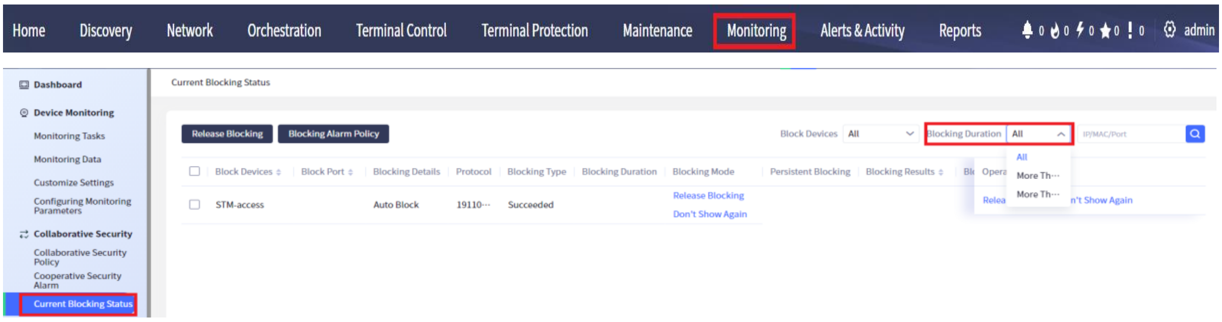


Figure 10.3.3.5 Query by blocking duration

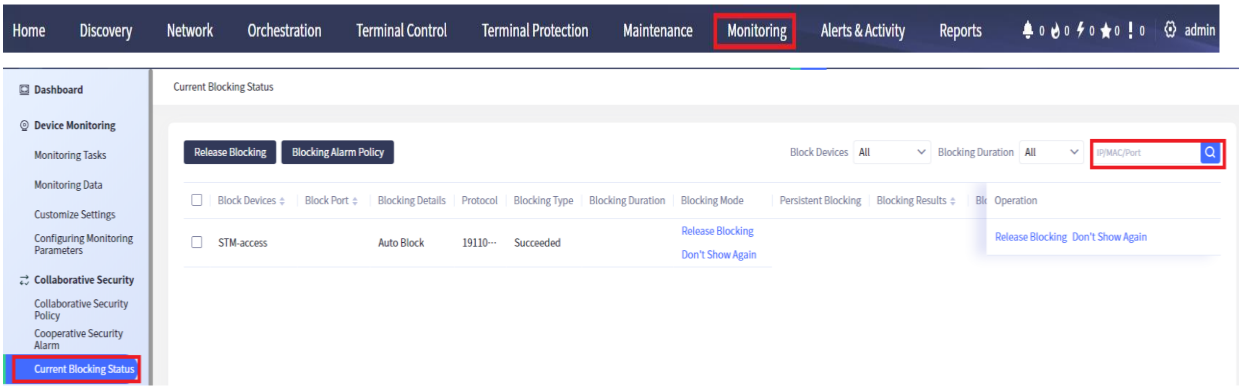
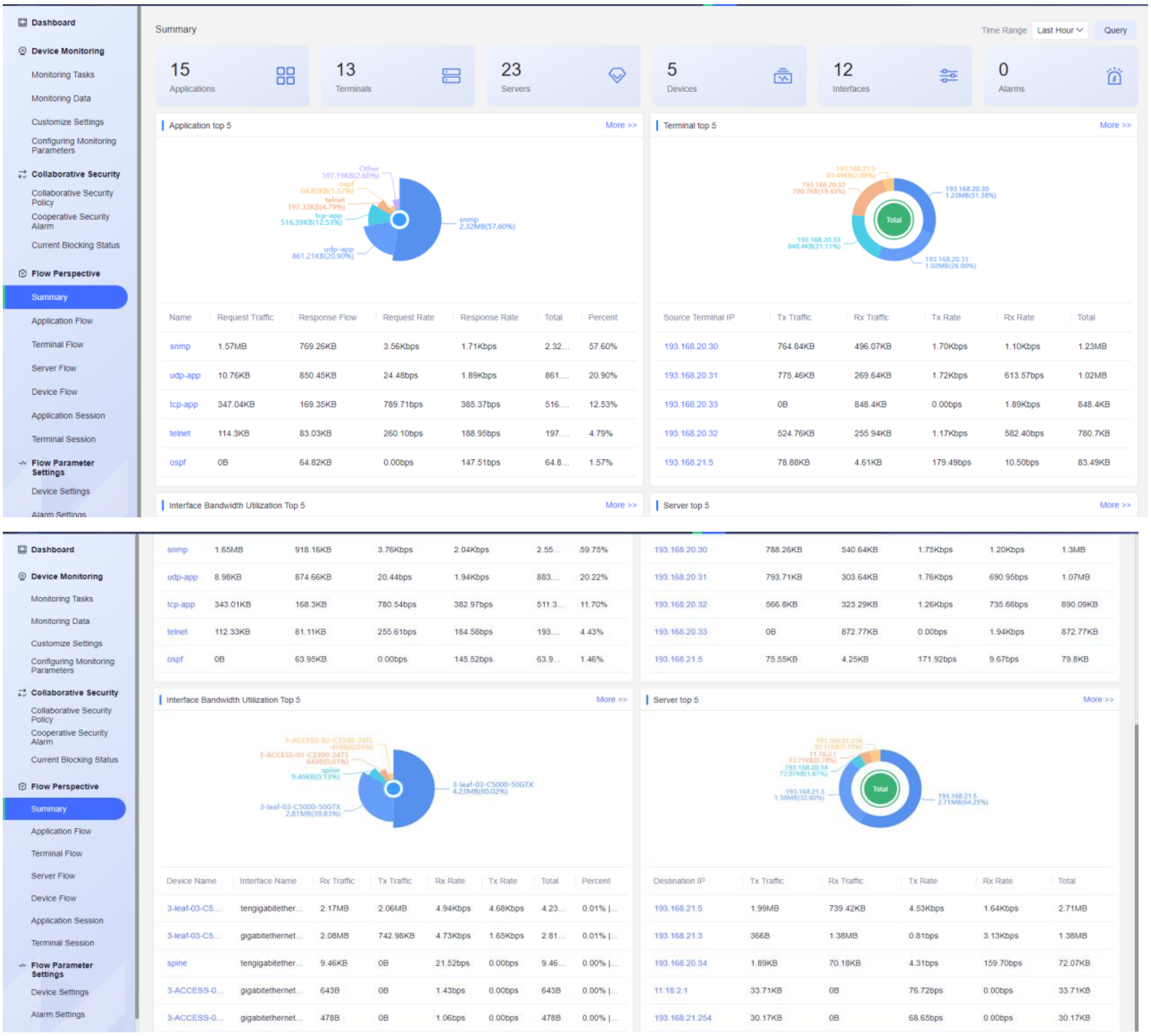


Figure 10.3.3.6 Fuzzy query

10.4 Flow Perspective

10.4.1 Flow Summary

Click **Monitoring** > **Summary** to enter the **Summary** interface, as shown in figure 10.4.1.1 below. In the traffic overview interface, you can visually see the number of applications, terminals, servers, collection devices, traffic alarms, as well as the sector chart of top5 data and the top5 data occupied by the bandwidth of applications, terminals, servers and interfaces. By default, the page displays the data of the last hour, Support viewing the data in different time periods (last hour, last day, last week, last month, custom).



Name	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Percent
snmp	1.57MB	769.26KB	3.56Kbps	1.71Kbps	2.32…	57.60%
udp-app	10.76KB	850.45KB	24.48bps	1.89Kbps	861.…	20.90%
tcp-app	347.04KB	169.35KB	789.71bps	385.37bps	516.…	12.53%
telnet	114.3KB	83.03KB	260.10bps	188.95bps	197.…	4.79%
ospf	0B	64.82KB	0.00bps	147.51bps	64.8…	1.57%

Source Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.20.30	764.84KB	496.07KB	1.70Kbps	1.10Kbps	1.23MB
193.168.20.31	775.46KB	269.64KB	1.72Kbps	613.57bps	1.02MB
193.168.20.33	0B	848.4KB	0.00bps	1.89Kbps	848.4KB
193.168.20.32	524.76KB	255.94KB	1.17Kbps	582.40bps	780.7KB
193.168.21.5	78.88KB	4.61KB	179.49bps	10.50bps	83.49KB

snmp	1.65MB	918.16KB	3.76Kbps	2.04Kbps	2.55…	59.75%
udp-app	8.98KB	874.66KB	20.44bps	1.94Kbps	883.…	20.22%
tcp-app	343.01KB	168.3KB	780.54bps	382.97bps	511.3…	11.70%
telnet	112.33KB	81.11KB	255.61bps	184.58bps	193.…	4.43%
ospf	0B	63.95KB	0.00bps	145.52bps	63.9…	1.46%

193.168.20.30	788.26KB	540.64KB	1.75Kbps	1.20Kbps	1.3MB
193.168.20.31	793.71KB	303.64KB	1.76Kbps	690.95bps	1.07MB
193.168.20.32	566.8KB	323.29KB	1.26Kbps	735.66bps	890.09KB
193.168.20.33	0B	872.77KB	0.00bps	1.94Kbps	872.77KB
193.168.21.5	75.55KB	4.25KB	171.92bps	9.67bps	79.8KB

Device Name	Interface Name	Rx Traffic	Tx Traffic	Rx Rate	Tx Rate	Total	Percent
3-leaf-03-C5…	tengigabitether…	2.17MB	2.06MB	4.94Kbps	4.68Kbps	4.23…	0.01% |…
3-leaf-03-C5…	gigabitethernet…	2.08MB	742.98KB	4.73Kbps	1.65Kbps	2.81…	0.01% |…
spine	tengigabitether…	9.46KB	0B	21.52bps	0.00bps	9.46…	0.00% |…
3-ACCESS-0…	gigabitethernet…	643B	0B	1.43bps	0.00bps	643B	0.00% |…
3-ACCESS-0…	gigabitethernet…	478B	0B	1.06bps	0.00bps	478B	0.00% |…

Destination IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.21.5	1.99MB	739.42KB	4.53Kbps	1.64Kbps	2.71MB
193.168.21.3	366B	1.38MB	0.81bps	3.13Kbps	1.38MB
193.168.20.34	1.89KB	70.18KB	4.31bps	159.70bps	72.07KB
11.18.2.1	33.71KB	0B	76.72bps	0.00bps	33.71KB
193.168.21.254	30.17KB	0B	68.65bps	0.00bps	30.17KB

Figure 10.4.1.1 Flow summary

The user can click the quantity block diagram of the **Summary** interface, as shown in figure 10.4.1.2 below, to jump to the corresponding interface. Jumping from the application number to the application flow interface, see 10.4.2 Application Flow in the manual. Jumping from the terminal number to the terminal flow interface, see 10.4.3 Terminal Flow in the manual. Jumping from the service number to the service flow interface, see 10.4.4 Service Flow in the manual. Jumping from the collection device number and collection interface number to the device flow interface, see 10.4.5 Device Flow in the manual. Jumping from flow alarm to the log alarm interface. See manual 11 Log Alarm.

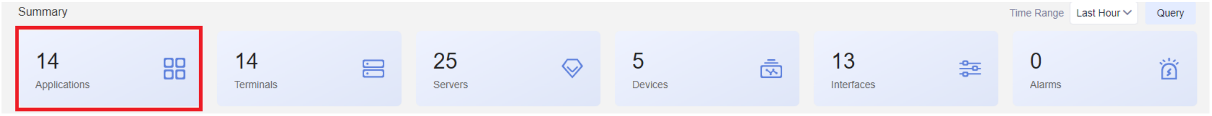
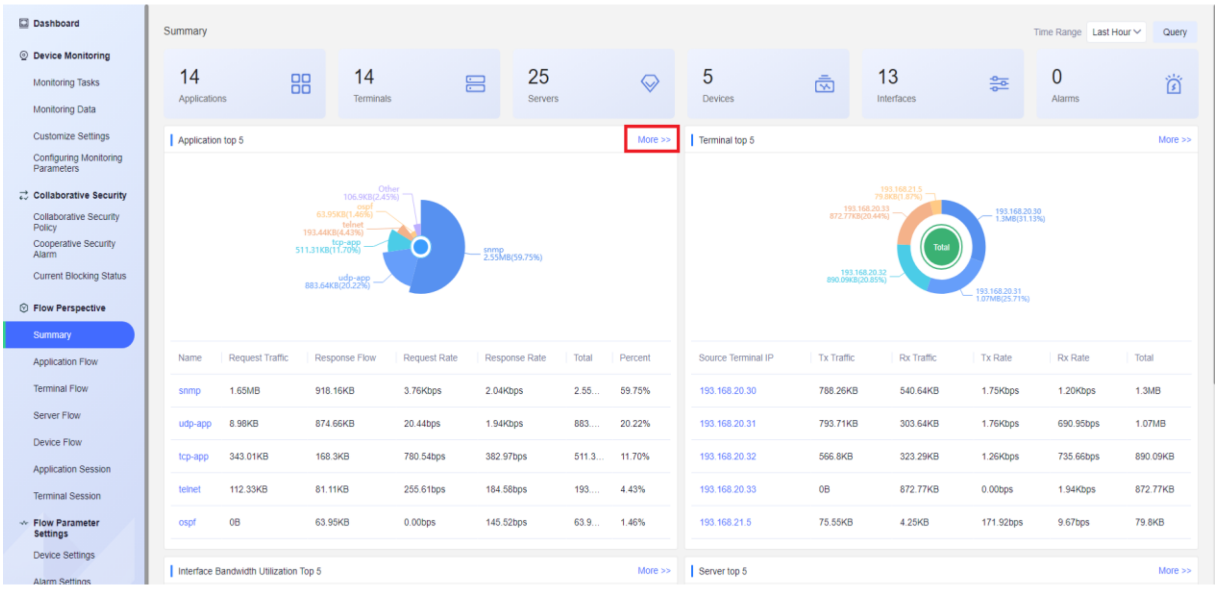


Figure 10.4.1.2 Applications

Users can click **More** in the upper right corner of top data of a module to display all traffic data of the module, as shown in figure 10.4.1.3.

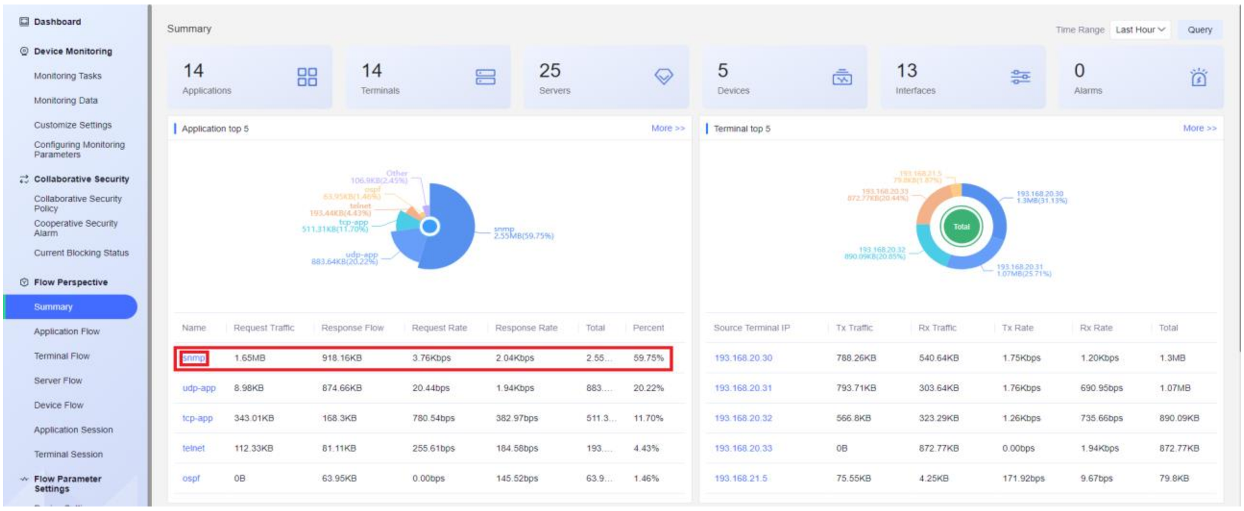


Name	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Percent
snmp	1.65MB	918.16KB	3.76Kbps	2.04Kbps	2.55…	59.75%
udp-app	8.98KB	874.66KB	20.44bps	1.94Kbps	883.…	20.22%
tcp-app	343.01KB	168.3KB	780.54bps	382.97bps	511.3…	11.70%
telnet	112.33KB	81.11KB	255.61bps	184.58bps	193.…	4.43%
ospf	0B	63.95KB	0.00bps	145.52bps	63.9…	1.46%

Source Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.20.30	788.26KB	540.64KB	1.75Kbps	1.20Kbps	1.3MB
193.168.20.31	793.71KB	303.64KB	1.76Kbps	690.95bps	1.07MB
193.168.20.32	566.8KB	323.29KB	1.26Kbps	735.66bps	890.09KB
193.168.20.33	0B	872.77KB	0.00bps	1.94Kbps	872.77KB
193.168.21.5	75.55KB	4.25KB	171.92bps	9.67bps	79.8KB

Figure 10.4.1.3 Click **More**

Users can click a piece of data in each top module to enter the details interface of the data. For example, click the blue words in the data of accessing EIP in top5, as shown in 10.4.1.4. The same is true for other top modules. See 10.4.2 Application Flow in the manual for the application details interface, 10.4.3 Terminal Flow in the manual for the terminal details interface, 10.4.4 Service Flow in the manual for the details of the server, and 10.4.5 Device Flow in the manual for details of the proportion of interface bandwidth.

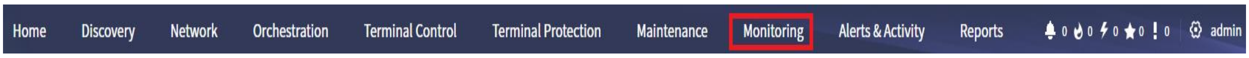

Name	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Percent
snmp	1.65MB	918.16KB	3.76Kbps	2.04Kbps	2.55…	59.75%
udp-app	8.98KB	874.66KB	20.44bps	1.94Kbps	883.…	20.22%
tcp-app	343.01KB	168.3KB	780.54bps	382.97bps	511.3…	11.70%
telnet	112.33KB	81.11KB	255.61bps	184.58bps	193.…	4.43%
ospf	0B	63.95KB	0.00bps	145.52bps	63.9…	1.46%

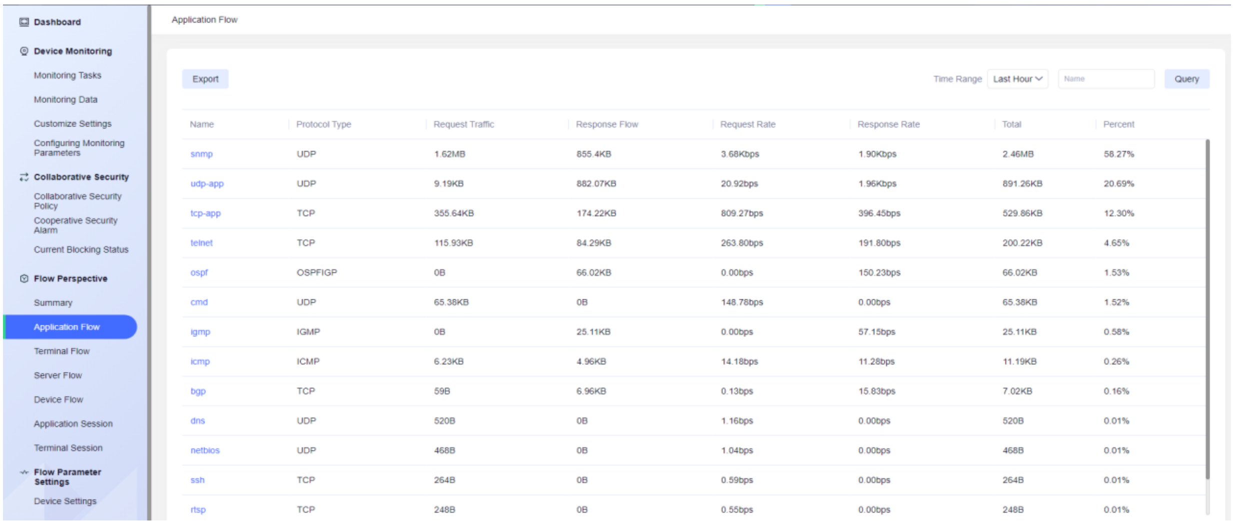
Source Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.20.30	788.26KB	540.64KB	1.75Kbps	1.20Kbps	1.3MB
193.168.20.31	793.71KB	303.64KB	1.76Kbps	690.95bps	1.07MB
193.168.20.32	566.8KB	323.29KB	1.26Kbps	735.66bps	890.09KB
193.168.20.33	0B	872.77KB	0.00bps	1.94Kbps	872.77KB
193.168.21.5	75.55KB	4.25KB	171.92bps	9.67bps	79.8KB

Figure 10.4.1.4 View details

10.4.2 Application Flow

Click **Monitoring** > **Application Flow** to enter the **Application Flow** interface, as shown in figure 10.4.2.1 below. The flow data displays the latest hour by default. It supports viewing data of different time periods (the latest hour, the latest day, the latest week, the latest month/custom), which is displayed in descending order by total traffic volume. It supports the precise search function by application name, and supports exporting the application traffic data of the current page to excel tables, Click the **Export** button in the upper left corner, as shown in figure 10.4.2.1.



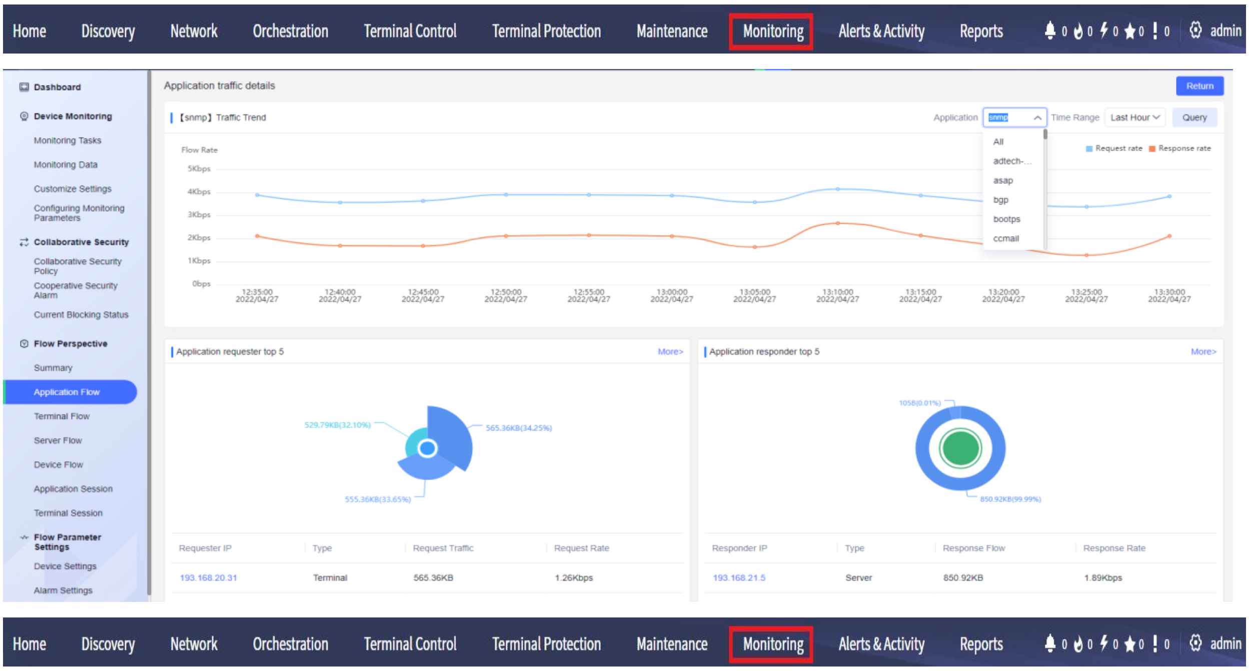


Application Flow

Name	Protocol Type	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Percent
snmp	UDP	1.62MB	855.4KB	3.68Kbps	1.90Kbps	2.46MB	58.27%
udp-app	UDP	9.19KB	882.07KB	20.92bps	1.96Kbps	891.26KB	20.69%
tcp-app	TCP	355.64KB	174.22KB	809.27bps	396.45bps	529.86KB	12.30%
telnet	TCP	115.93KB	84.29KB	263.80bps	191.80bps	200.22KB	4.65%
ospf	OSPFIGP	0B	66.02KB	0.00bps	150.23bps	66.02KB	1.53%
cmd	UDP	65.38KB	0B	148.78bps	0.00bps	65.38KB	1.52%
igmp	IGMP	0B	25.11KB	0.00bps	57.15bps	25.11KB	0.58%
icmp	ICMP	6.23KB	4.96KB	14.18bps	11.28bps	11.19KB	0.26%
bgp	TCP	59B	6.96KB	0.13bps	15.83bps	7.02KB	0.16%
dns	UDP	520B	0B	1.16bps	0.00bps	520B	0.01%
netbios	UDP	468B	0B	1.04bps	0.00bps	468B	0.01%
ssh	TCP	264B	0B	0.59bps	0.00bps	264B	0.01%
rtsp	TCP	248B	0B	0.55bps	0.00bps	248B	0.01%

Figure 10.4.2.1 Application flow

The user can click the application name of a single piece of data to jump to the application details interface to display the traffic trend chart of the application, the top5 data at the application requesting end and responding end and the circular proportion chart of the data under the application. In the **Details** interface, you can also change the application to view the details of other applications. Since the Details interface only displays the top5 data at the application requesting end and responding end, the **More** interfaces are set respectively, Click the **More** button to view all the data. At the same time, it also supports accurate IP search, as shown in figure 10.4.2.2.



Application traffic details

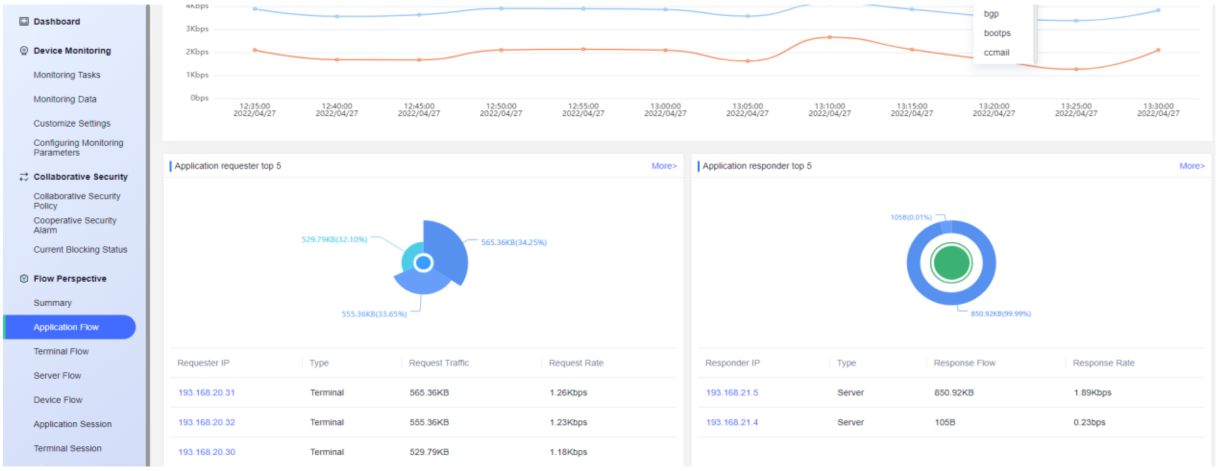
【snmp】Traffic Trend

Application requester top 5

Requester IP	Type	Request Traffic	Request Rate
193.168.20.31	Terminal	565.36KB	1.26Kbps

Application responder top 5

Responder IP	Type	Response Flow	Response Rate
193.168.21.5	Server	850.92KB	1.89Kbps



Requester IP	Type	Request Traffic	Request Rate
193.168.20.31	Terminal	565.36KB	1.26Kbps
193.168.20.32	Terminal	555.36KB	1.23Kbps
193.168.20.30	Terminal	529.79KB	1.18Kbps

Responder IP	Type	Response Flow	Response Rate
193.168.21.5	Server	850.92KB	1.89Kbps
193.168.21.4	Server	105B	0.23bps

Figure 10.4.2.2 Application flow details

The user can click the IP of a single piece of data in the **Details** interface to view the traffic trend chart of the data. The **Details** interface is the same as the **More** interfaces, as shown in figure 10.4.2.3.

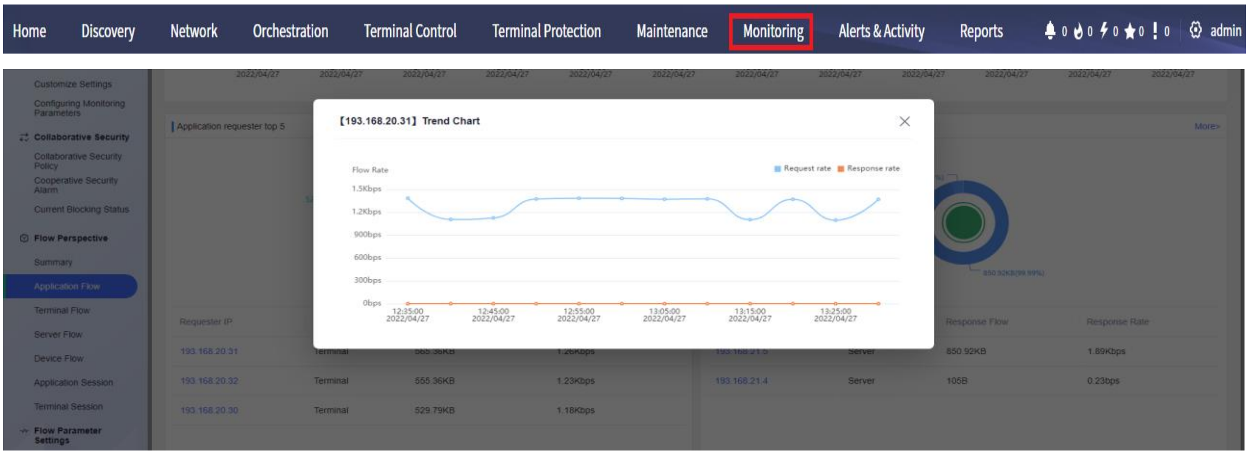
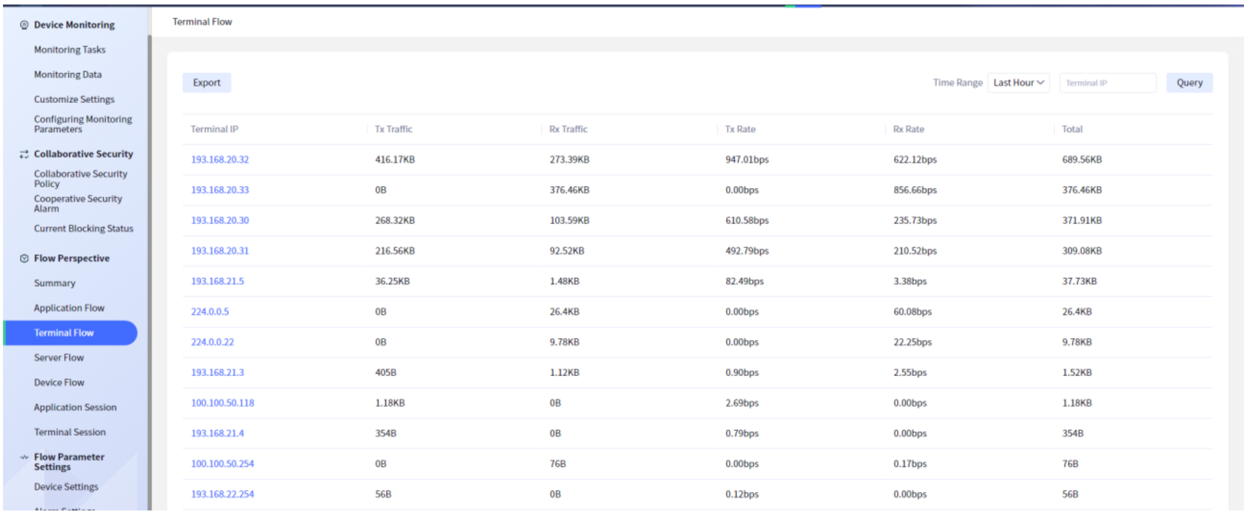


Figure 10.4.2.3 Flow trend chart

10.4.3 Terminal Flow

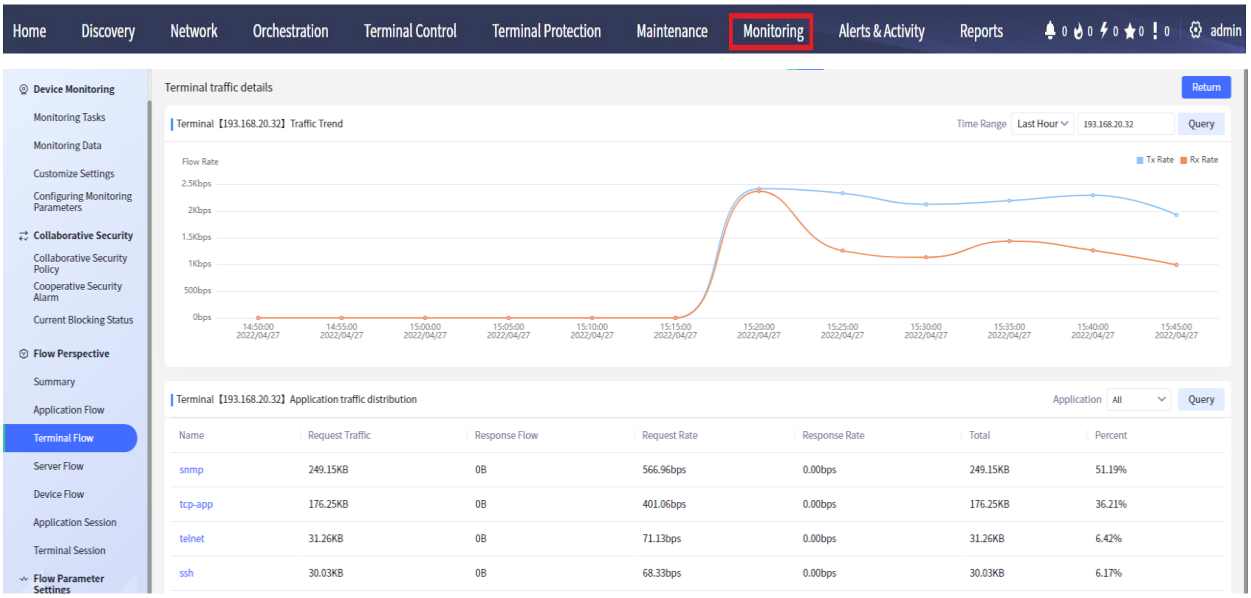
Click **Monitoring** > **Terminal Flow** to enter the **Terminal Flow** interface, which displays all terminal traffic data, as shown in figure 10.4.3.1 below. By default, the latest hour is displayed. It supports viewing data of different time periods (the latest hour, the latest day, the latest week, and the latest month, custom), which is displayed in descending order by total traffic. It supports the function of precise IP search by terminal. It also supports exporting the terminal traffic data of the current page to excel tables, Click the **Export** button in the upper left corner, as shown in figure 10.4.3.1.



Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.20.32	416.17KB	273.39KB	947.01bps	622.12bps	689.56KB
193.168.20.33	0B	376.46KB	0.00bps	856.66bps	376.46KB
193.168.20.30	268.32KB	103.59KB	610.58bps	235.73bps	371.91KB
193.168.20.31	216.56KB	92.52KB	492.79bps	210.52bps	309.08KB
193.168.21.5	36.25KB	1.48KB	82.49bps	3.38bps	37.73KB
224.0.0.5	0B	26.4KB	0.00bps	60.08bps	26.4KB
224.0.0.22	0B	9.78KB	0.00bps	22.25bps	9.78KB
193.168.21.3	405B	1.12KB	0.90bps	2.55bps	1.52KB
100.100.50.118	1.18KB	0B	2.69bps	0.00bps	1.18KB
193.168.21.4	354B	0B	0.79bps	0.00bps	354B
100.100.50.254	0B	76B	0.00bps	0.17bps	76B
193.168.22.254	56B	0B	0.12bps	0.00bps	56B

Figure 10.4.3.1 Terminal Flow

The user can click the terminal IP of a single piece of data to jump to the details interface of the terminal to display the traffic trend diagram of the terminal. At the same time, the **Details** interface supports accurate IP search of the terminal and terminal application traffic distribution. By default, all application traffic data belonging to the terminal are displayed. You can also select an application to view individual application traffic data, as shown in figure 10.4.3.2.



Name	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Percent
snmp	249.15KB	0B	566.96bps	0.00bps	249.15KB	51.19%
tcp-app	176.25KB	0B	401.06bps	0.00bps	176.25KB	36.21%
telnet	31.26KB	0B	71.13bps	0.00bps	31.26KB	6.42%
ssh	30.03KB	0B	68.33bps	0.00bps	30.03KB	6.17%

Figure 10.4.3.2 Terminal flow details

Users can click the application name of a single application traffic data to view the traffic trend chart of the data, as shown in figure 10.4.3.3:

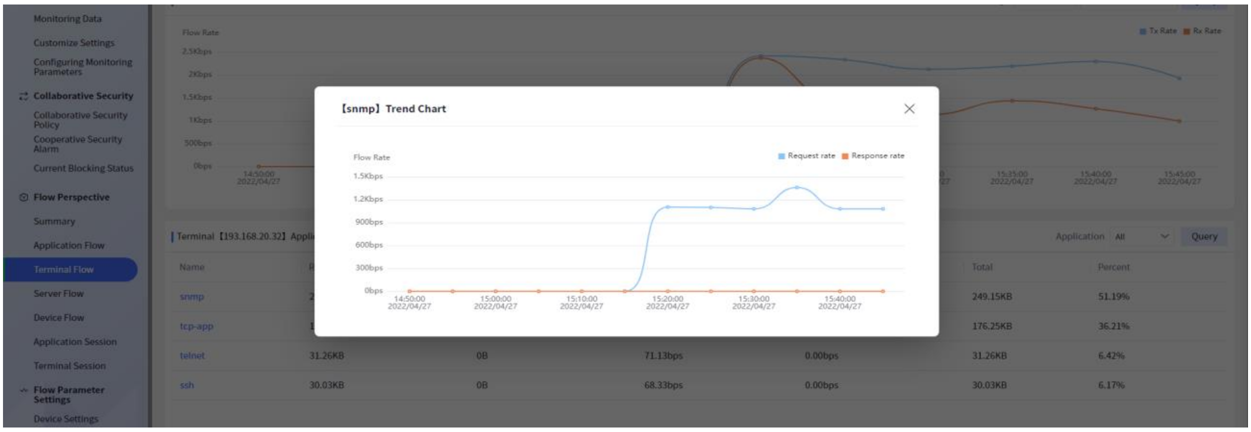
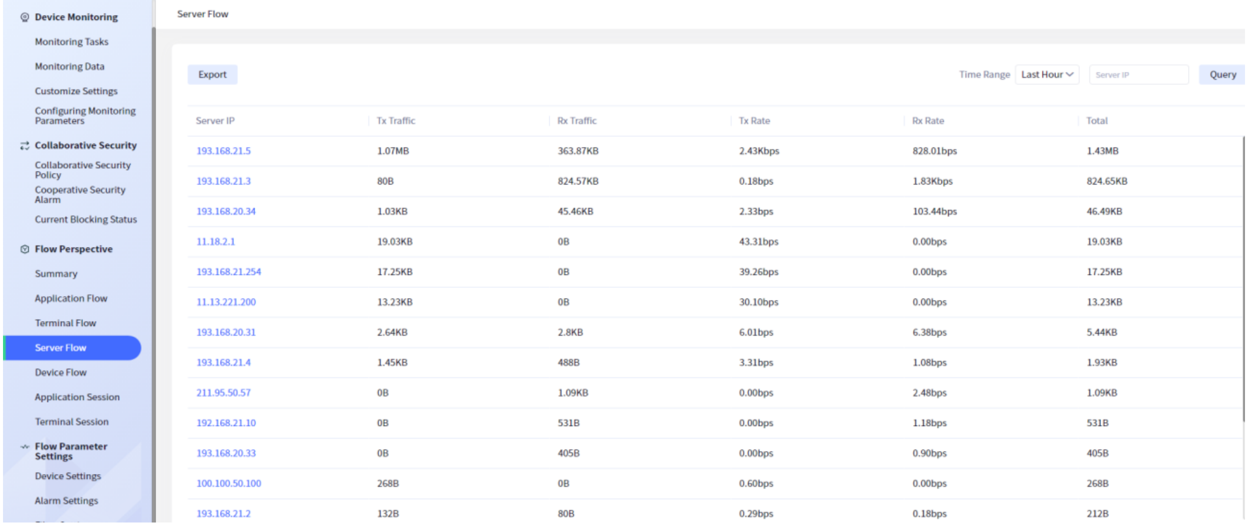


Figure 10.4.3.3 Flow trend chart

10.4.4 Server Flow

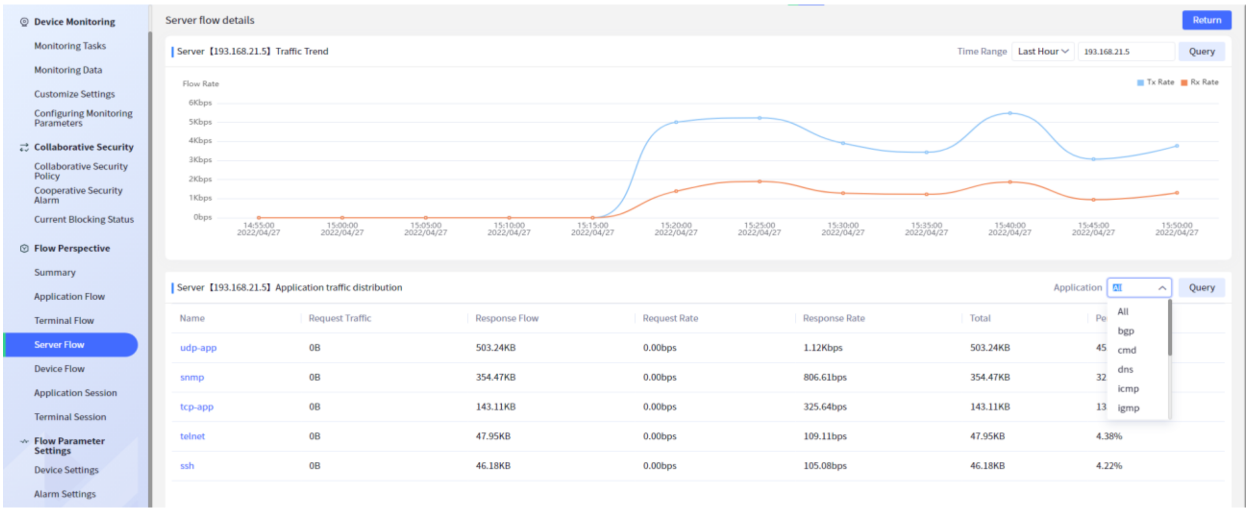
Click **Monitoring** > **Terminal Flow** to enter the **Terminal Flow** interface, which displays all server traffic data, as shown in figure 10.4.4.1 below. By default, the last hour is displayed. You can view data in different time periods (the last hour, the last day, the last week, and the latest month custom), which is displayed in descending order by total traffic, and support the precise IP search function by server, At the same time, the server traffic data of the current page can be exported to excel. Click the **Export** button in the upper left corner, as shown in figure 10.4.4.1.



Server IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.21.5	1.07MB	363.87KB	2.43Kbps	828.01bps	1.43MB
193.168.21.3	80B	824.57KB	0.18bps	1.83Kbps	824.65KB
193.168.20.34	1.03KB	45.46KB	2.33bps	103.44bps	46.49KB
11.18.2.1	19.03KB	0B	43.31bps	0.00bps	19.03KB
193.168.21.254	17.25KB	0B	39.26bps	0.00bps	17.25KB
11.13.221.200	13.23KB	0B	30.10bps	0.00bps	13.23KB
193.168.20.31	2.64KB	2.8KB	6.01bps	6.38bps	5.44KB
193.168.21.4	1.45KB	488B	3.31bps	1.08bps	1.93KB
211.95.50.57	0B	1.09KB	0.00bps	2.48bps	1.09KB
192.168.21.10	0B	531B	0.00bps	1.18bps	531B
193.168.20.33	0B	405B	0.00bps	0.90bps	405B
100.100.50.100	268B	0B	0.60bps	0.00bps	268B
193.168.21.2	132B	80B	0.29bps	0.18bps	212B

Figure 10.4.4.1 Server flow

The user can click the server IP of a single piece of data to jump to the **Details** interface of the terminal to display the traffic trend graph of the terminal. At the same time, the **Details** interface supports the precise IP search of the server and the application traffic distribution of the server. By default, all the application traffic data of the server are displayed. You can also select an application to view the individual application traffic data, as shown in figure 10.4.3.2.

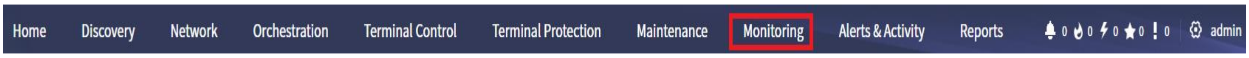


Server【193.168.21.5】Application traffic distribution

Name	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Pe
udp-app	0B	503.24KB	0.00bps	1.12Kbps	503.24KB	45
snmp	0B	354.47KB	0.00bps	806.61bps	354.47KB	32
tcp-app	0B	143.11KB	0.00bps	325.64bps	143.11KB	13
telnet	0B	47.95KB	0.00bps	109.11bps	47.95KB	4.38%
ssh	0B	46.18KB	0.00bps	105.08bps	46.18KB	4.22%

Figure 10.4.4.2 Server flow details

Users can click the application name of a single application flow data to view the flow trend chart of the data, as shown in figure 10.4.3.3.



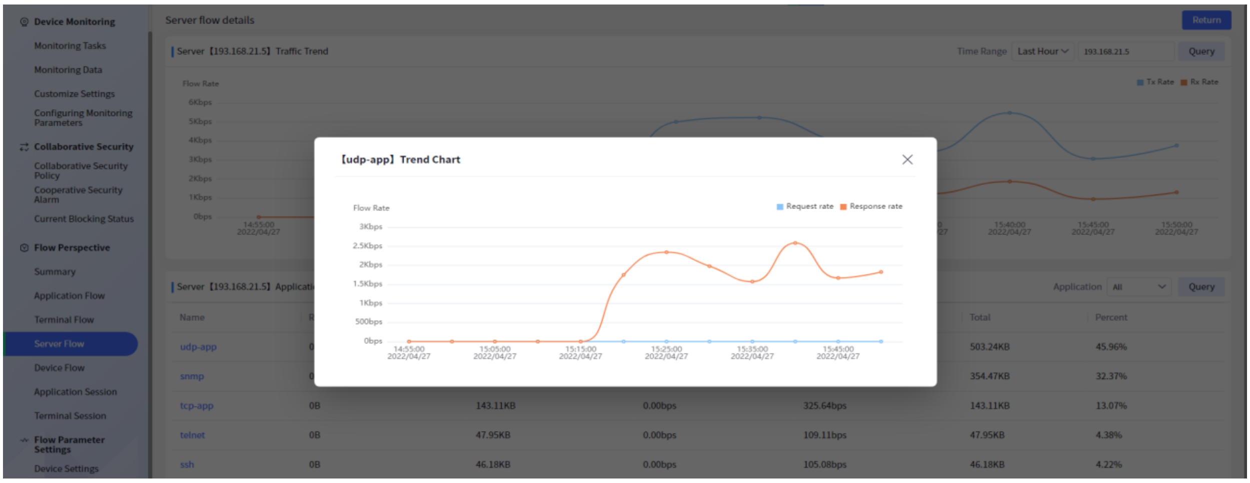
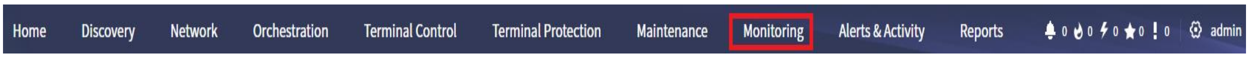
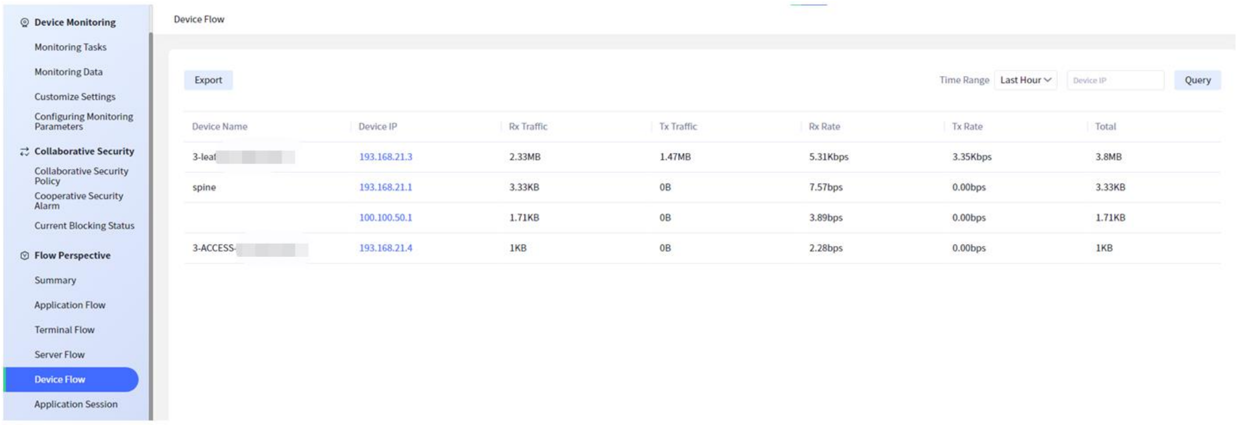


Figure 10.4.4.3 Flow trend chart

10.4.5 Device Flow

Click **Monitoring** > **Device Flow** to enter the **Device Flow** interface, which displays the traffic data of all devices. By default, the latest hour is displayed. You can view the data of different time periods (last hour, last day, last week, last month, custom), which is displayed in descending order by total traffic. You can search the device IP precisely by device, and export the device traffic data of the current page to excel, Click the **Export** button in the upper left corner, as shown in figure 10.4.5.1.

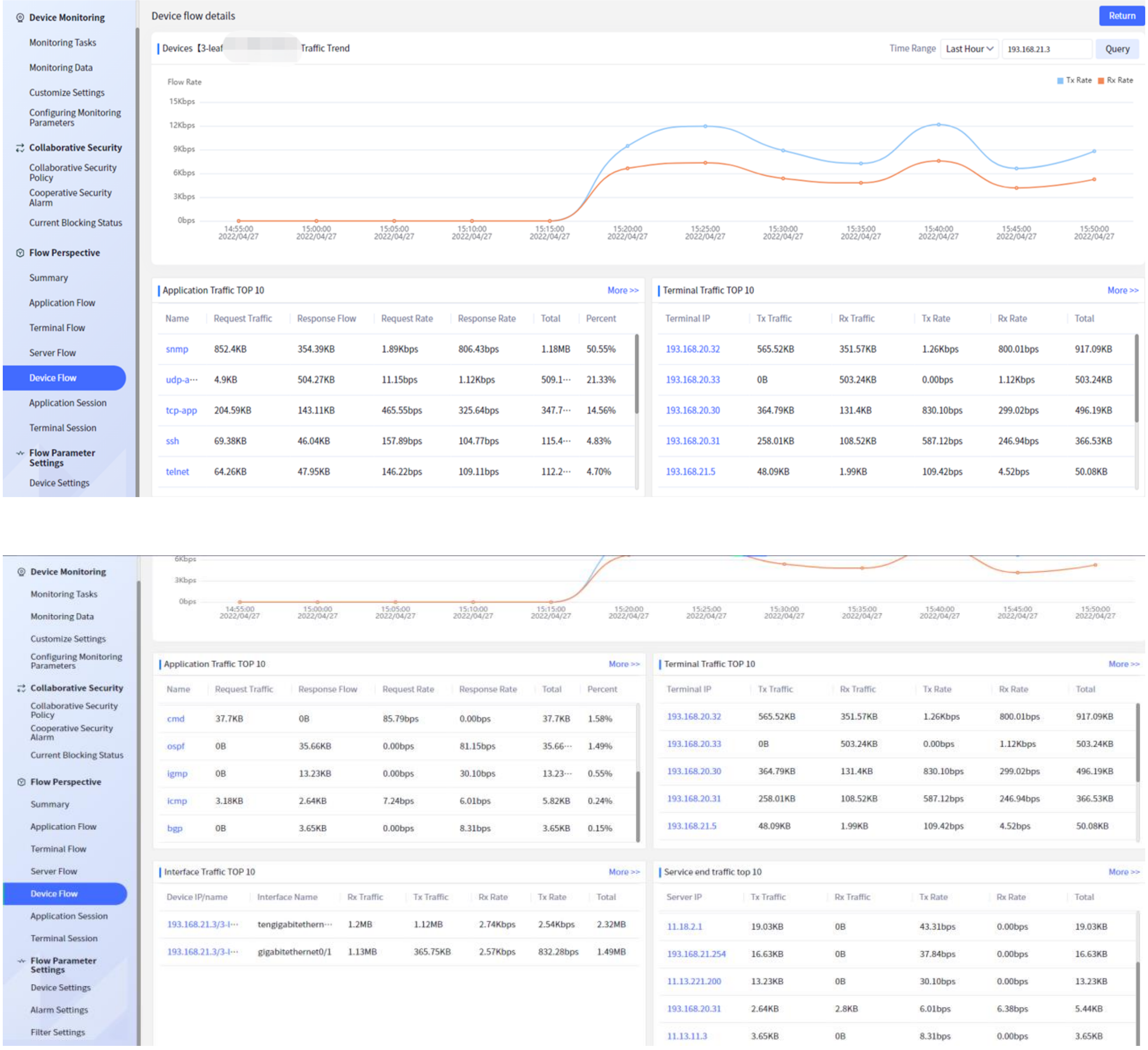




Device Name	Device IP	Rx Traffic	Tx Traffic	Rx Rate	Tx Rate	Total
3-leaf[redacted]	193.168.21.3	2.33MB	1.47MB	5.31Kbps	3.35Kbps	3.8MB
spine	193.168.21.1	3.33KB	0B	7.57bps	0.00bps	3.33KB
	100.100.50.1	1.71KB	0B	3.89bps	0.00bps	1.71KB
3-ACCESS-[redacted]	193.168.21.4	1KB	0B	2.28bps	0.00bps	1KB

Figure 10.4.5.1 Device flow

You can click the device IP of a single piece of data to jump to the details interface of the device to display the traffic trend diagram of the device, the name of the collection device and the top10 data of the application, terminal, interface and service traffic under the collection device. At the same time, the **Details** interface also supports precise IP search by device, as shown in figure 10.4.5.2



Application Traffic TOP 10

Name	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Percent
snmp	852.4KB	354.39KB	1.89Kbps	806.43bps	1.18MB	50.55%
udp-a···	4.9KB	504.27KB	11.15bps	1.12Kbps	509.1···	21.33%
tcp-app	204.59KB	143.11KB	465.55bps	325.64bps	347.7···	14.56%
ssh	69.38KB	46.04KB	157.89bps	104.77bps	115.4···	4.83%
telnet	64.26KB	47.95KB	146.22bps	109.11bps	112.2···	4.70%

Terminal Traffic TOP 10

Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.20.32	565.52KB	351.57KB	1.26Kbps	800.01bps	917.09KB
193.168.20.33	0B	503.24KB	0.00bps	1.12Kbps	503.24KB
193.168.20.30	364.79KB	131.4KB	830.10bps	299.02bps	496.19KB
193.168.20.31	258.01KB	108.52KB	587.12bps	246.94bps	366.53KB
193.168.21.5	48.09KB	1.99KB	109.42bps	4.52bps	50.08KB

Application Traffic TOP 10

Name	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Percent
cmd	37.7KB	0B	85.79bps	0.00bps	37.7KB	1.58%
ospf	0B	35.66KB	0.00bps	81.15bps	35.66···	1.49%
igmp	0B	13.23KB	0.00bps	30.10bps	13.23···	0.55%
icmp	3.18KB	2.64KB	7.24bps	6.01bps	5.82KB	0.24%
bgp	0B	3.65KB	0.00bps	8.31bps	3.65KB	0.15%

Terminal Traffic TOP 10

Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.20.32	565.52KB	351.57KB	1.26Kbps	800.01bps	917.09KB
193.168.20.33	0B	503.24KB	0.00bps	1.12Kbps	503.24KB
193.168.20.30	364.79KB	131.4KB	830.10bps	299.02bps	496.19KB
193.168.20.31	258.01KB	108.52KB	587.12bps	246.94bps	366.53KB
193.168.21.5	48.09KB	1.99KB	109.42bps	4.52bps	50.08KB

Interface Traffic TOP 10

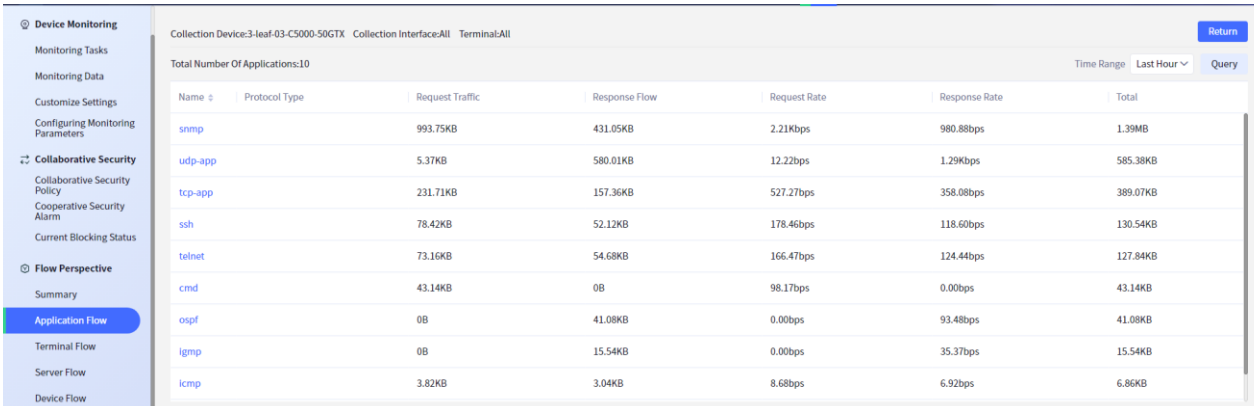
Device IP/name	Interface Name	Rx Traffic	Tx Traffic	Rx Rate	Tx Rate	Total
193.168.21.3/3-l···	tengigabitethern···	1.2MB	1.12MB	2.74Kbps	2.54Kbps	2.32MB
193.168.21.3/3-l···	gigabitethernet0/1	1.13MB	365.75KB	2.57Kbps	832.28bps	1.49MB

Service end traffic top 10

Server IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
11.18.2.1	19.03KB	0B	43.31bps	0.00bps	19.03KB
193.168.21.254	16.63KB	0B	37.84bps	0.00bps	16.63KB
11.13.221.200	13.23KB	0B	30.10bps	0.00bps	13.23KB
193.168.20.31	2.64KB	2.8KB	6.01bps	6.38bps	5.44KB
11.13.11.3	3.65KB	0B	8.31bps	0.00bps	3.65KB

Figure 10.4.5.2 Device flow details

At the same time, the **More** interfaces of the four TOP10 are provided respectively. Users can click **More** in the upper right corner to jump to the corresponding **More** interfaces to display all the corresponding data of the collection device. The effect diagram is as follows:



Collection Device:3-leaf-03-C5000-50GTX Collection Interface:All Terminal:All

Total Number Of Applications:10

Name	Protocol Type	Request Traffic	Response Flow	Request Rate	Response Rate	Total
snmp		993.75KB	431.05KB	2.21Kbps	980.88bps	1.39MB
udp-app		5.37KB	580.01KB	12.22bps	1.29Kbps	585.38KB
tcp-app		231.71KB	157.36KB	527.27bps	358.08bps	389.07KB
ssh		78.42KB	52.12KB	178.46bps	118.60bps	130.54KB
telnet		73.16KB	54.68KB	166.47bps	124.44bps	127.84KB
cmd		43.14KB	0B	98.17bps	0.00bps	43.14KB
ospf		0B	41.08KB	0.00bps	93.48bps	41.08KB
igmp		0B	15.54KB	0.00bps	35.37bps	15.54KB
icmp		3.82KB	3.04KB	8.68bps	6.92bps	6.86KB

Figure 10.4.5.3 More interface

Note

- The **More** interfaces of application flow TOP10 and interface flow TOP10 do not support the search function, and the **More** interfaces of terminal and server flow support accurate query by IP.

In the **Details** interface, users can click the IP of a single piece of data in the top module to view the flow trend chart. The same is true for the **More** interfaces, as shown in figure 10.3.5.4.

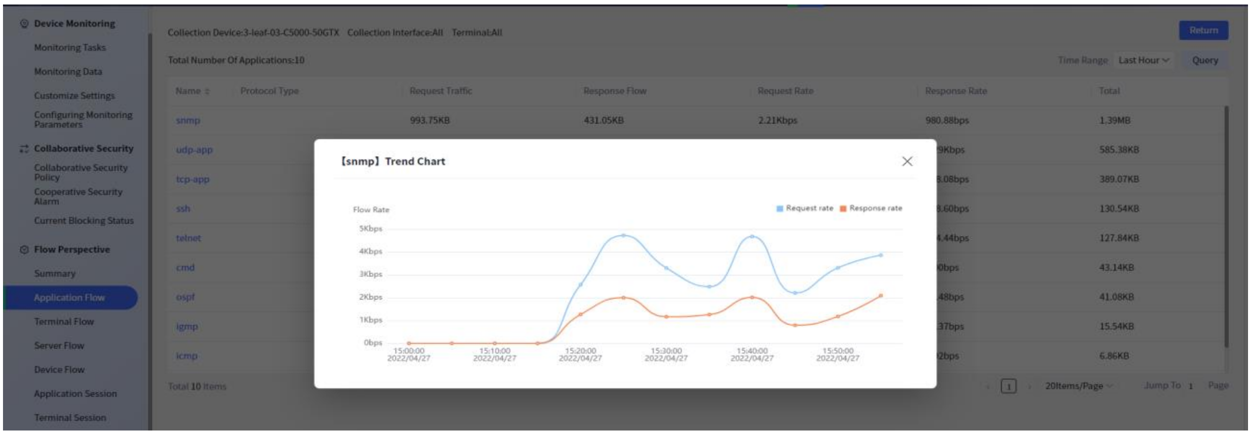
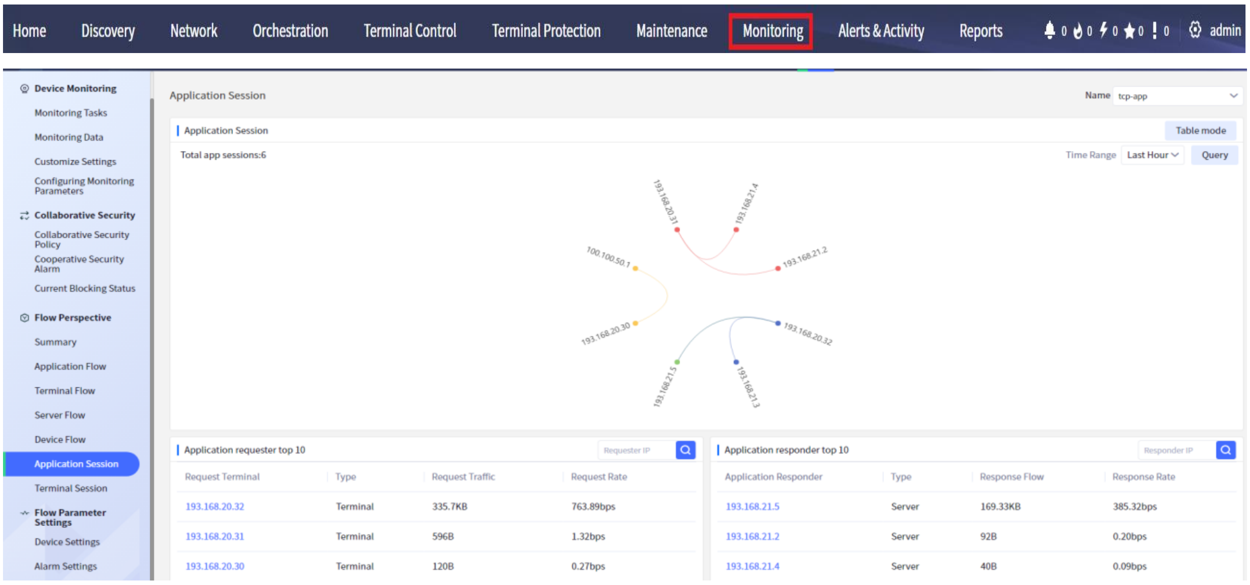


Figure 10.4.5.4 Flow trend chart

10.4.6 Application Session

Click **Monitoring** > **Application Session** to enter the **Application Session** interface, which displays the application session data, TOP10 data at the application request end and TOP10 data at the application response end. By default, the application session data with the largest total traffic in the last hour is displayed. It supports viewing data of different time periods (last hour, last day, last week, last month, custom). In the upper right corner, you can select to view different application session data according to the application name. The application name displays all application names with traffic data in descending order according to the total traffic. In the application session area, display the total number of application sessions and the graphical mode of application sessions, as shown in figure 10.4.6.1. At the same time, support the table mode of application sessions, that is, display the specific data of application sessions, as shown in figure 10.4.6.2.



Application Session

Name: tcp-app

Application Session

Total app sessions:6

Time Range: Last Hour

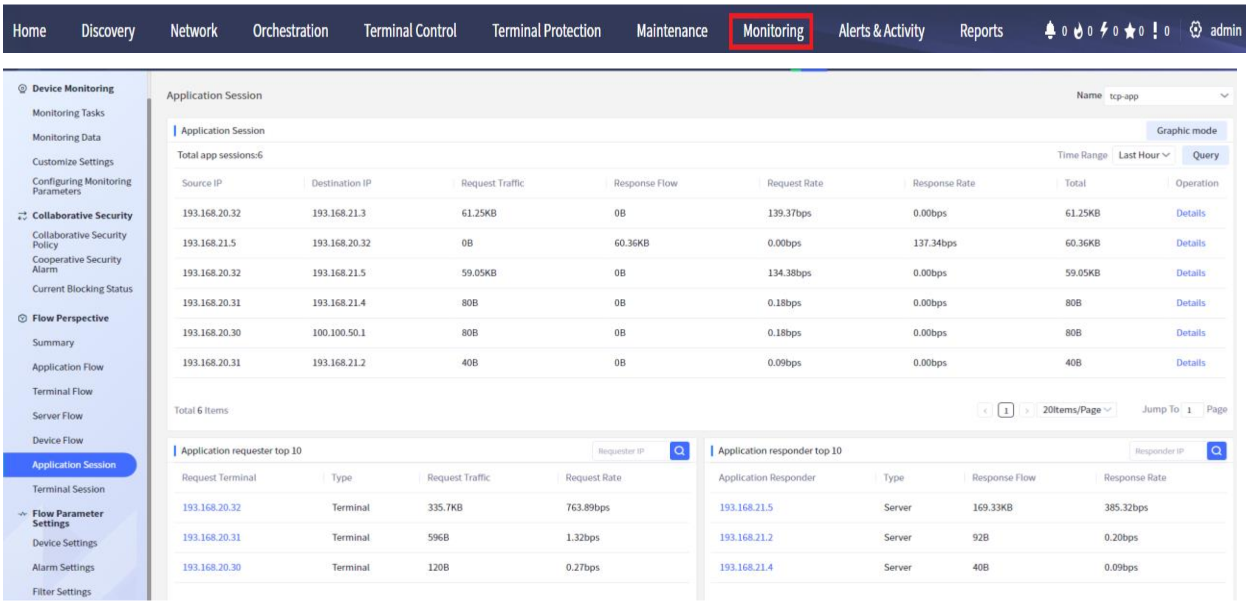
Application requester top 10

Request Terminal	Type	Request Traffic	Request Rate
193.168.20.32	Terminal	335.7KB	763.89bps
193.168.20.31	Terminal	596B	1.32bps
193.168.20.30	Terminal	120B	0.27bps

Application responder top 10

Application Responder	Type	Response Flow	Response Rate
193.168.21.5	Server	169.33KB	385.32bps
193.168.21.2	Server	92B	0.20bps
193.168.21.4	Server	40B	0.09bps

Figure 10.4.6.1 Graphical mode of the application sessions



Application Session

Name: tcp-app

Application Session

Total app sessions:6

Time Range: Last Hour

Source IP	Destination IP	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Operation
193.168.20.32	193.168.21.3	61.25KB	0B	139.37bps	0.00bps	61.25KB	Details
193.168.21.5	193.168.20.32	0B	60.36KB	0.00bps	137.34bps	60.36KB	Details
193.168.20.32	193.168.21.5	59.05KB	0B	134.38bps	0.00bps	59.05KB	Details
193.168.20.31	193.168.21.4	80B	0B	0.18bps	0.00bps	80B	Details
193.168.20.30	100.100.50.1	80B	0B	0.18bps	0.00bps	80B	Details
193.168.20.31	193.168.21.2	40B	0B	0.09bps	0.00bps	40B	Details

Total 6 Items 1 20Items/Page Jump To 1 Page

Application requester top 10

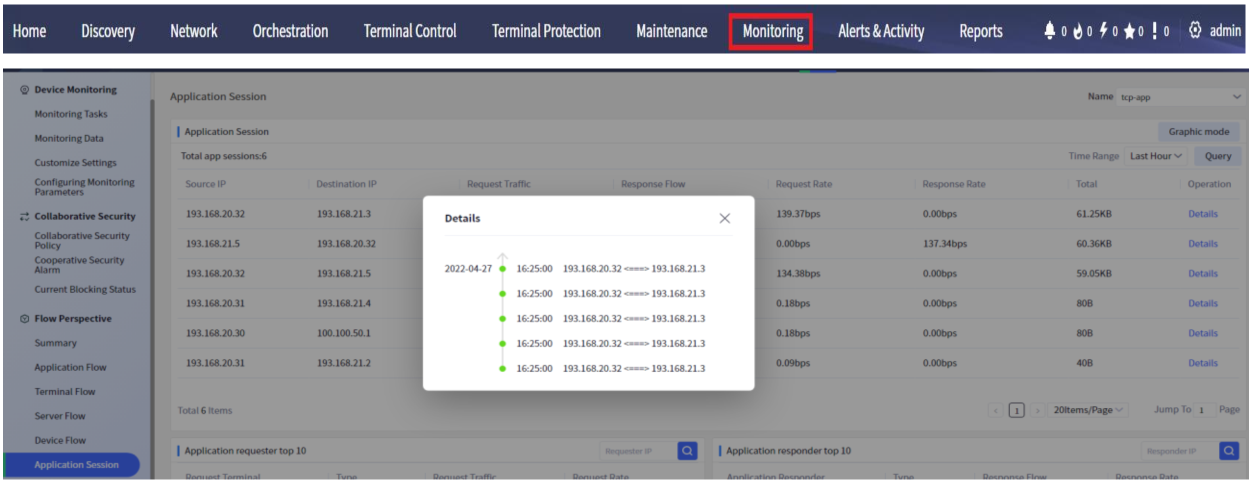
Request Terminal	Type	Request Traffic	Request Rate
193.168.20.32	Terminal	335.7KB	763.89bps
193.168.20.31	Terminal	596B	1.32bps
193.168.20.30	Terminal	120B	0.27bps

Application responder top 10

Application Responder	Type	Response Flow	Response Rate
193.168.21.5	Server	169.33KB	385.32bps
193.168.21.2	Server	92B	0.20bps
193.168.21.4	Server	40B	0.09bps

Figure 10.4.6.2 Table mode of the application sessions

In the table mode, the user can click the **Details** of a session data to view the details of the session, as shown in figure 10.4.6.3.



Details

2022-04-27
16:25:00 193.168.20.32 <===> 193.168.21.3
16:25:00 193.168.20.32 <===> 193.168.21.3
16:25:00 193.168.20.32 <===> 193.168.21.3
16:25:00 193.168.20.32 <===> 193.168.21.3
16:25:00 193.168.20.32 <===> 193.168.21.3

Figure 10.4.6.3 The details of application session table mode

Support precise IP search in the upper right corner of the top data. At the same time, users can click the IP of a data to view the session graphic mode or table mode of the IP, as shown in figure 10.4.6.4.

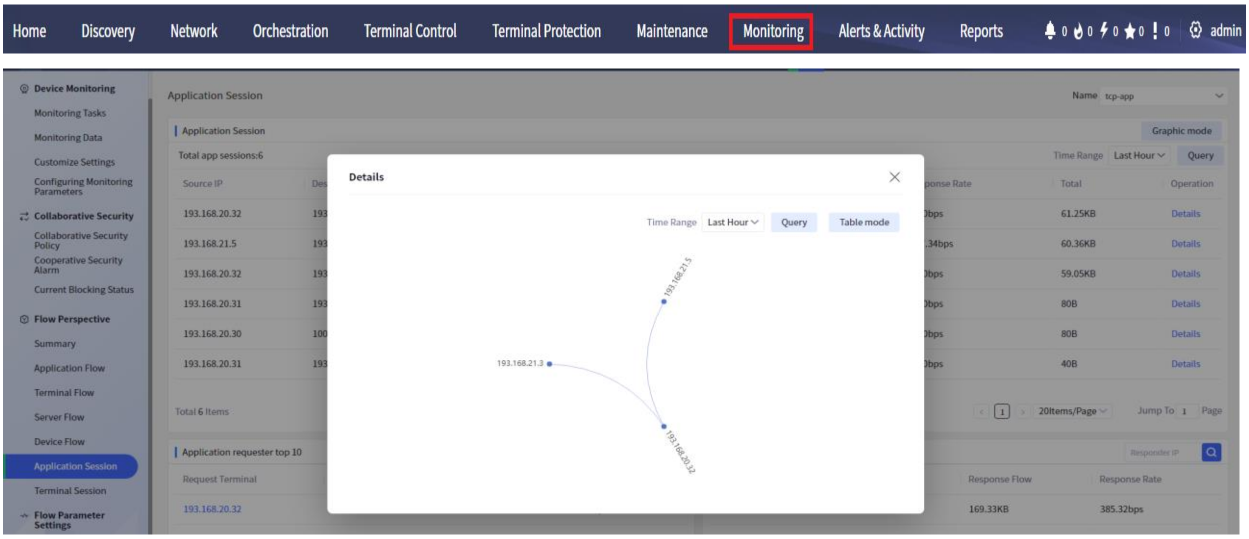
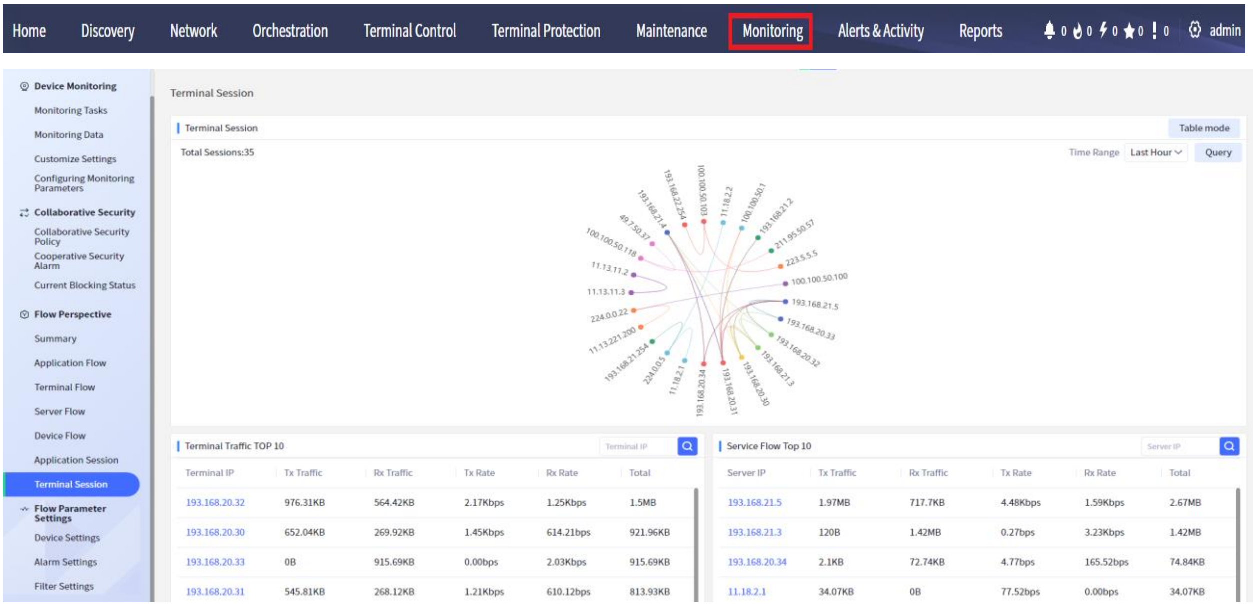


Figure 10.4.6.4 Details of application session data

10.4.7 Terminal Session

Click **Monitoring** > **Terminal Session** to enter the **Terminal Session** interface, which displays the terminal session data, terminal traffic TOP10 data and service traffic TOP10 data. By default, it displays the last hour. It supports viewing data of different time periods (last hour, last day, last week, last month, custom). The total number of terminal sessions and the graphical mode of terminal sessions will be displayed in the terminal session area, as shown in figure 10.4.7.1, At the same time, it supports the table mode of the terminal session, that is, to display the specific data of the application session, as shown in figure 10.4.7.2.



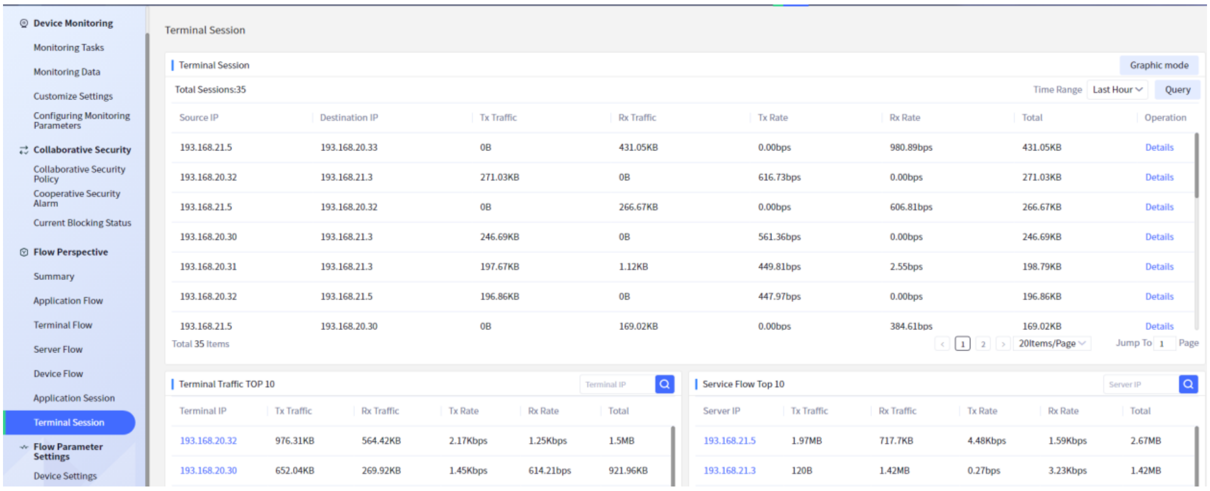
Terminal Traffic TOP 10

Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.20.32	976.31KB	564.42KB	2.17Kbps	1.25Kbps	1.5MB
193.168.20.30	652.04KB	269.92KB	1.45Kbps	614.21bps	921.96KB
193.168.20.33	0B	915.69KB	0.00bps	2.03Kbps	915.69KB
193.168.20.31	545.81KB	268.12KB	1.21Kbps	610.12bps	813.93KB

Service Flow Top 10

Server IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.21.5	1.97MB	717.7KB	4.48Kbps	1.59Kbps	2.67MB
193.168.21.3	120B	1.42MB	0.27bps	3.23Kbps	1.42MB
193.168.20.34	2.1KB	72.74KB	4.77bps	165.52bps	74.84KB
11.18.2.1	34.07KB	0B	77.52bps	0.00bps	34.07KB

Figure 10.4.7.1 Terminal sessions



Terminal Session

Terminal Session

Total Sessions:35

Source IP	Destination IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total	Operation
193.168.21.5	193.168.20.33	0B	431.05KB	0.00bps	980.89bps	431.05KB	Details
193.168.20.32	193.168.21.3	271.03KB	0B	616.73bps	0.00bps	271.03KB	Details
193.168.21.5	193.168.20.32	0B	266.67KB	0.00bps	606.81bps	266.67KB	Details
193.168.20.30	193.168.21.3	246.69KB	0B	561.36bps	0.00bps	246.69KB	Details
193.168.20.31	193.168.21.3	197.67KB	1.12KB	449.81bps	2.55bps	198.79KB	Details
193.168.20.32	193.168.21.5	196.86KB	0B	447.97bps	0.00bps	196.86KB	Details
193.168.21.5	193.168.20.30	0B	169.02KB	0.00bps	384.61bps	169.02KB	Details

Total 35 Items 1 2 20Items/Page Jump To 1 Page

Terminal Traffic TOP 10

Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.20.32	976.31KB	564.42KB	2.17Kbps	1.25Kbps	1.5MB
193.168.20.30	652.04KB	269.92KB	1.45Kbps	614.21bps	921.96KB

Service Flow Top 10

Server IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.21.5	1.97MB	717.7KB	4.48Kbps	1.59Kbps	2.67MB
193.168.21.3	120B	1.42MB	0.27bps	3.23Kbps	1.42MB

Figure 10.4.7.2 Table mode of the terminal sessions

In the table mode, the user can click the **Details** of a session data to view the details of the session, as shown in figure 10.4.7.3.

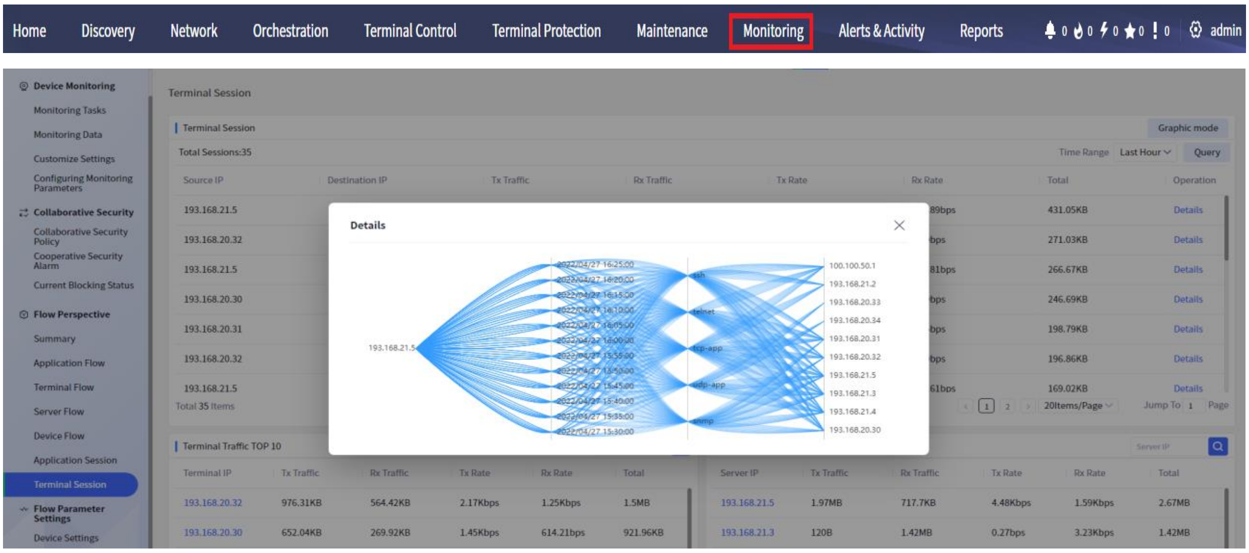


Figure 10.4.7.3 Details of terminal session table mode

Support precise IP search in the upper right corner of the top data. At the same time, users can click the IP of a data to view the session graphic mode or table mode of the IP, as shown in figure 10.4.7.4.

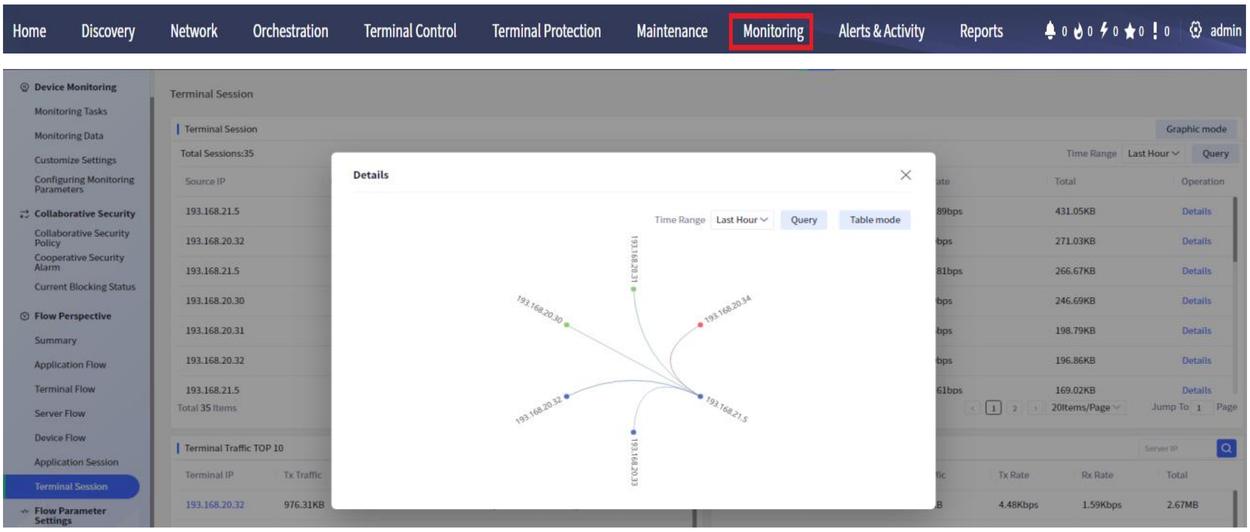


Figure 10.4.7.4 Details of terminal session data

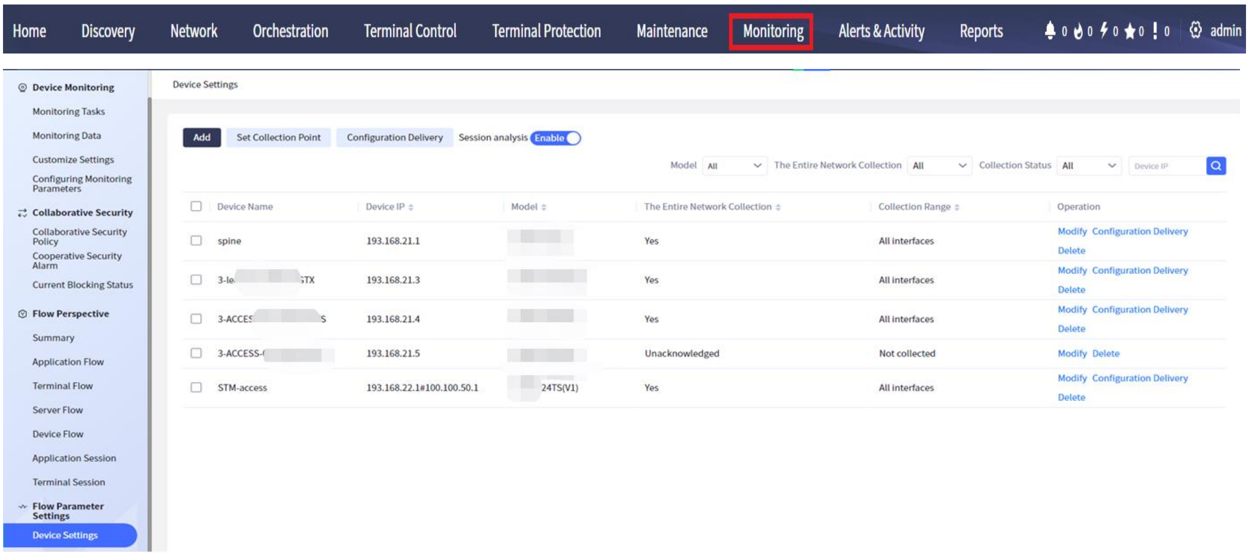
Note

- To use the application session and terminal session functions, you need to enable session analysis in the collection configuration. See 10.4.1 Collection Configuration in the manual.
- The graphics mode of the terminal session and application session can display up to 500 pieces of data.

10.5 Flow Configuration

10.5.1 Collection Configuration

Click **Monitoring** > **Device Settings** to enter the **Device Settings** page, where the device name, device IP, model, the entire network collection point and collection range information are displayed, as shown in the following figure.



Device Settings

Session analysis Enable

Model All | The Entire Network Collection All | Collection Status All | Device IP

☐	Device Name	Device IP	Model	The Entire Network Collection	Collection Range	Operation
☐	spine	193.168.21.1	[redacted]	Yes	All interfaces	Modify Configuration Delivery Delete
☐	3-le[redacted]TX	193.168.21.3	[redacted]	Yes	All interfaces	Modify Configuration Delivery Delete
☐	3-ACCES[redacted]S	193.168.21.4	[redacted]	Yes	All interfaces	Modify Configuration Delivery Delete
☐	3-ACCESS-[redacted]	193.168.21.5	[redacted]	Unacknowledged	Not collected	Modify Delete
☐	STM-access	193.168.22.1#100.100.50.1	[redacted]24TS(V1)	Yes	All interfaces	Modify Configuration Delivery Delete

Figure 10.5.1.1 Collection configuration

Click the **Add** button in the upper left corner of the list to open an **Add** interface. On this page, click the **Add Device** button to pop up a **Device** page. On the **Device** page, the user can click the box in front of a device or directly click the device to add, or click the box in the upper left corner of the device list or the **Select all** button to add all devices. The effect is shown in the figure.

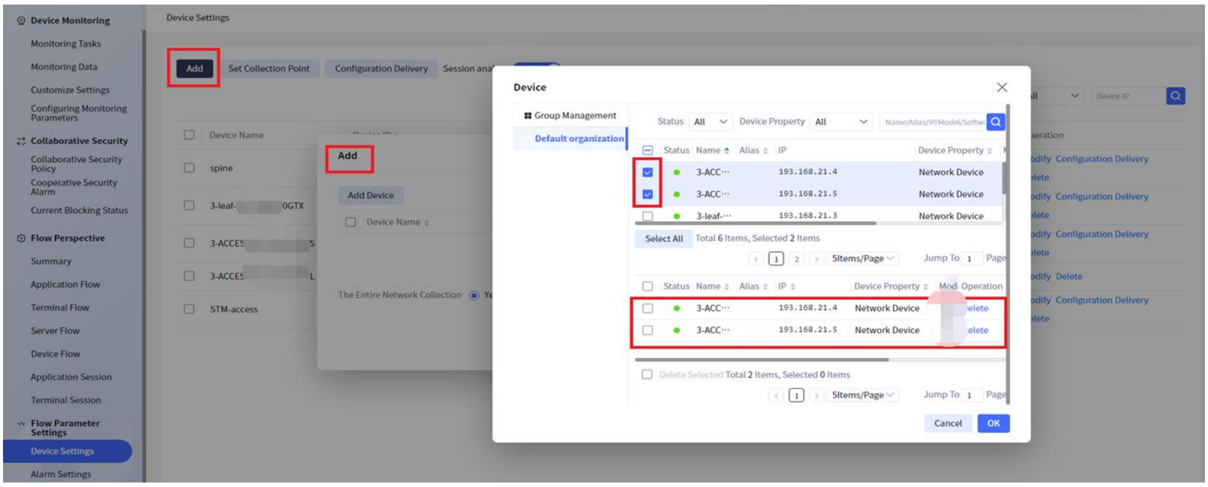


Figure 10.5.1.2 Add collection configuration-1

After selecting the device on the **Device** page, the added device will be displayed. On the **Add** interface, you can set whether the device is **The Entire Network Collection**, and the effect is as shown in the figure.

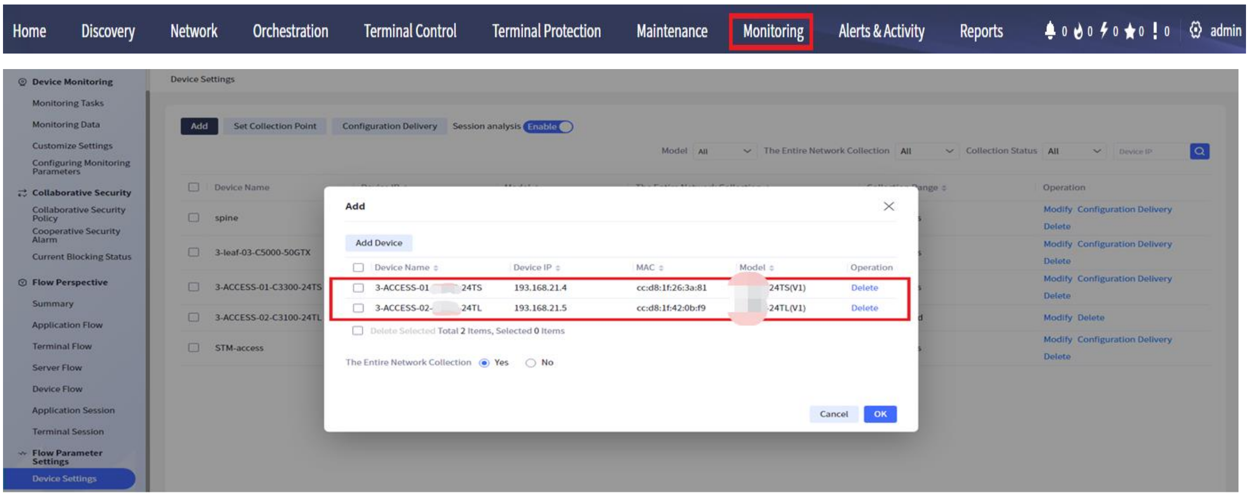


Figure 10.5.1.3 Add collection configuration-2

You can delete the pre-selected devices in the **Device** interface. You can click **Delete Selected** to delete multiple devices, or select a device and click **Delete** to delete it. The effect is shown in the figure.

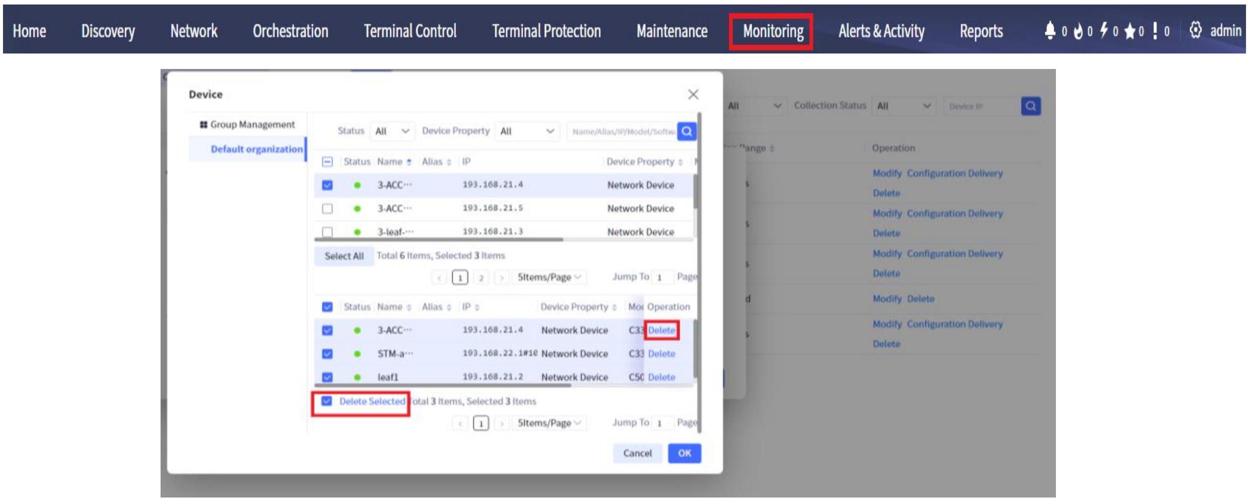


Figure 10.5.1.4 Delete the selected devices

The user can accurately query the devices according to the status and device attributes, or fuzzy query by filling in the name, alias, IP, model and software version. The effect is shown in the figure.

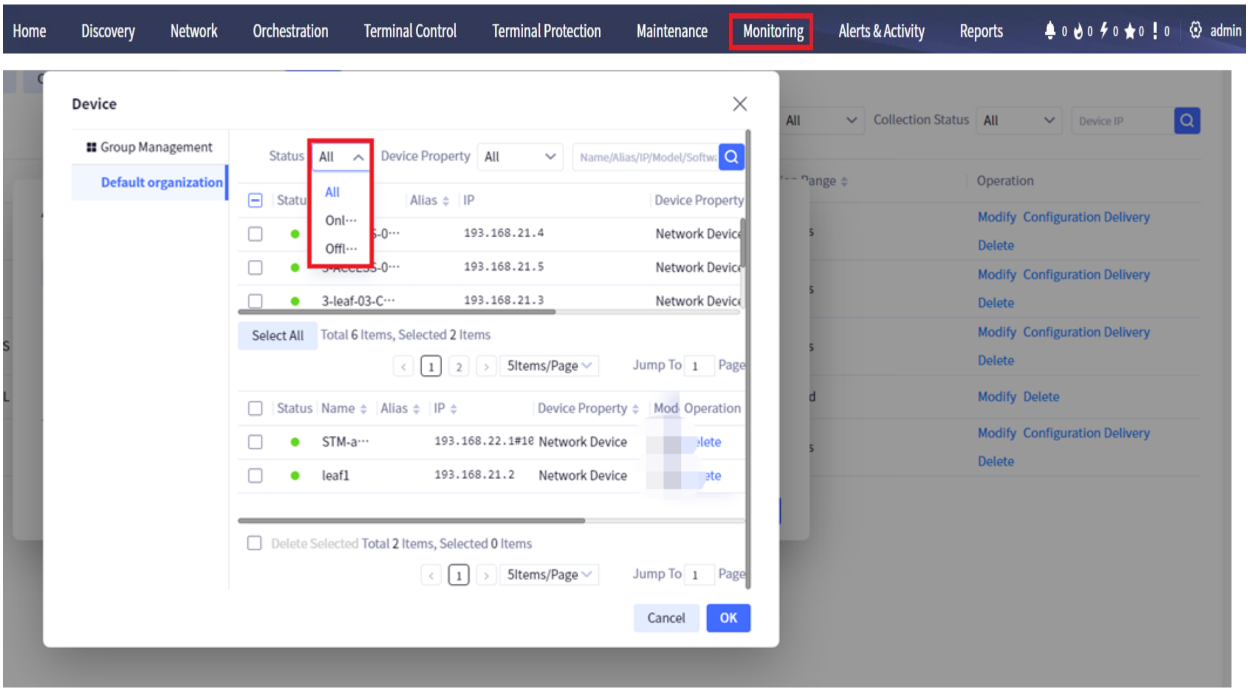


Figure 10.5.1.5 Query by the device status

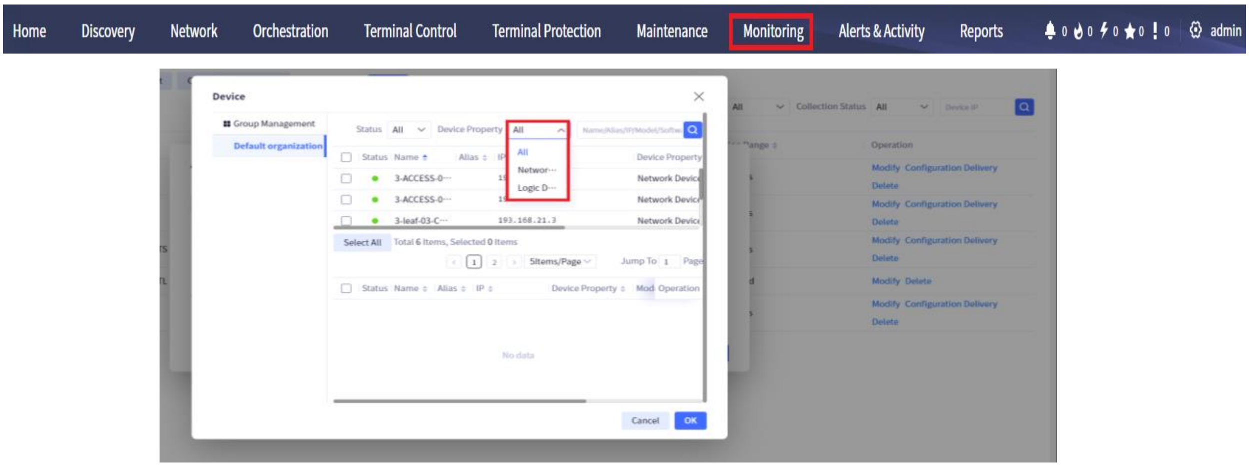
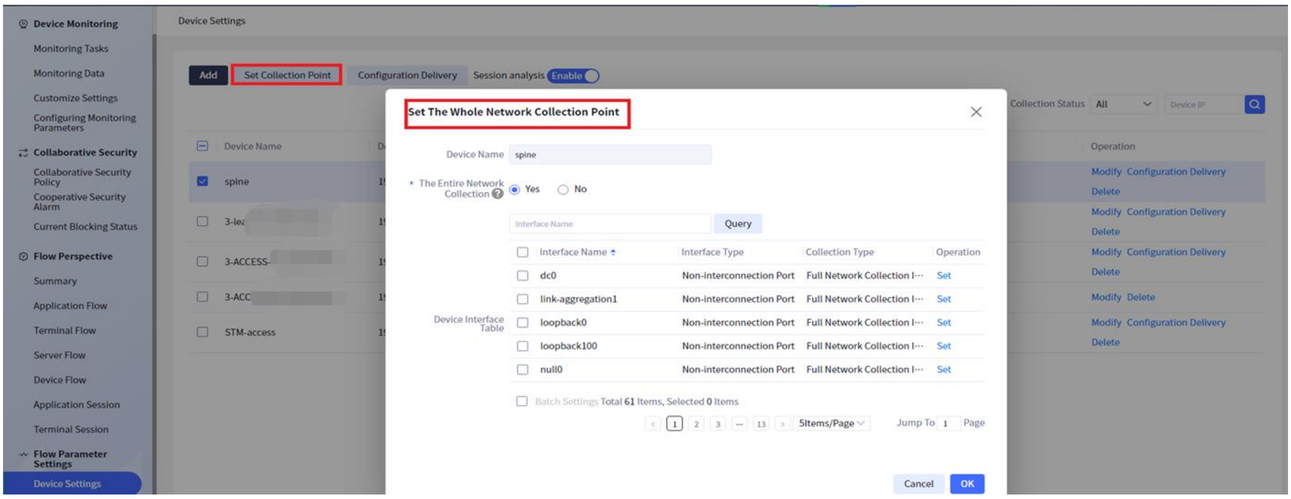


Figure 10.5.1.6 Query by device attributes

Select a device in the device list and click the **Set Collection Point** button in the upper left corner of the list to open a new page for setting the collection point of the whole network. On this page, you can modify whether the device is a collection point of the whole network. The effect is shown in the figure. Click the **Set** button of an interface to set the collection type of the interface as the whole network collection interface or the non-whole network collection interface, and the effect is shown in the figure. On this page, you can also fill in the interface name and click **Query**. The effect is shown in the figure.



Set The Whole Network Collection Point

Device Name spine

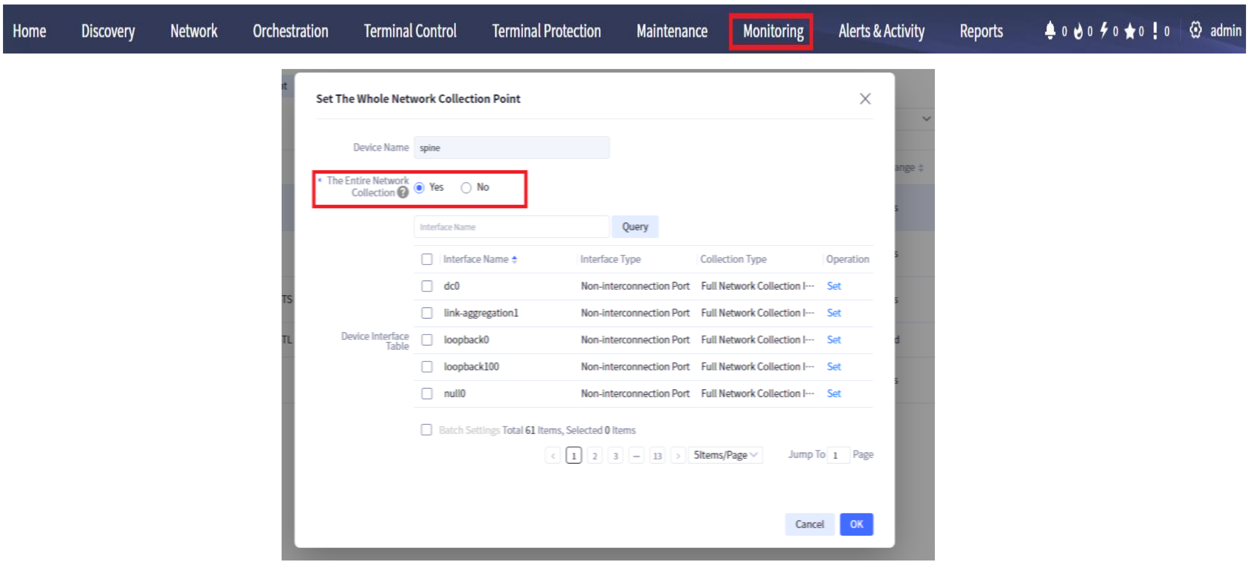
* The Entire Network Collection ● Yes ○ No

Device Interface Table

☐	Interface Name	Interface Type	Collection Type	Operation
☐	dc0	Non-interconnection Port	Full Network Collection I···	Set
☐	link-aggregation1	Non-interconnection Port	Full Network Collection I···	Set
☐	loopback0	Non-interconnection Port	Full Network Collection I···	Set
☐	loopback100	Non-interconnection Port	Full Network Collection I···	Set
☐	null0	Non-interconnection Port	Full Network Collection I···	Set

☐ Batch Settings Total 61 Items, Selected 0 Items

Figure 10.5.1.7 Set the collection point



Set The Whole Network Collection Point

Device Name spine

* The Entire Network Collection ● Yes ○ No

Device Interface Table

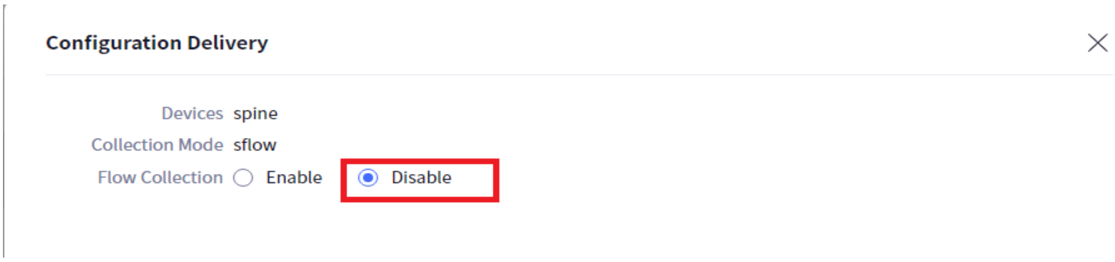
☐	Interface Name	Interface Type	Collection Type	Operation
☐	dc0	Non-interconnection Port	Full Network Collection I···	Set
☐	link-aggregation1	Non-interconnection Port	Full Network Collection I···	Set
☐	loopback0	Non-interconnection Port	Full Network Collection I···	Set
☐	loopback100	Non-interconnection Port	Full Network Collection I···	Set
☐	null0	Non-interconnection Port	Full Network Collection I···	Set

☐ Batch Settings Total 61 Items, Selected 0 Items

Figure 10.5.1.8 Set the collection port of the whole network

Click the **Configuration Delivery** button in the upper left corner to perform single delivery or batch delivery.

If a device is selected, it is the single delivery. Click the **Configuration Delivery** button to pop up a new page for configuration delivery, which displays the device name, collection mode and flow collection. It is disabled by default.



Configuration Delivery

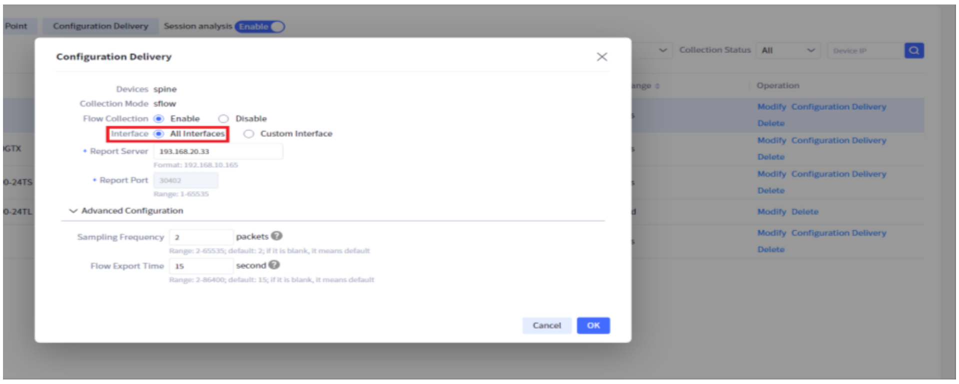
Devices spine

Collection Mode sflow

Flow Collection ○ Enable ● Disable

Figure 10.5.1.9 Configuration delivery interface

When flow collection is selected as **Enable**, if the original device is not collected, select all interfaces by default. The user needs to fill in the report server, sampling frequency and flow export time information, and then click **OK** to deliver a configuration task. After the configuration task is completed, the collection status of the device is displayed as **All Interfaces**.


Configuration Delivery

Devices spine

Collection Mode sflow

Flow Collection ● Enable ○ Disable

Interface ● All Interfaces ○ Custom Interface

* Report Server 193.168.20.33

Format: 192.168.10.165

* Report Port 30402

Range: 1-65535

Advanced Configuration

Sampling Frequency 2 packets

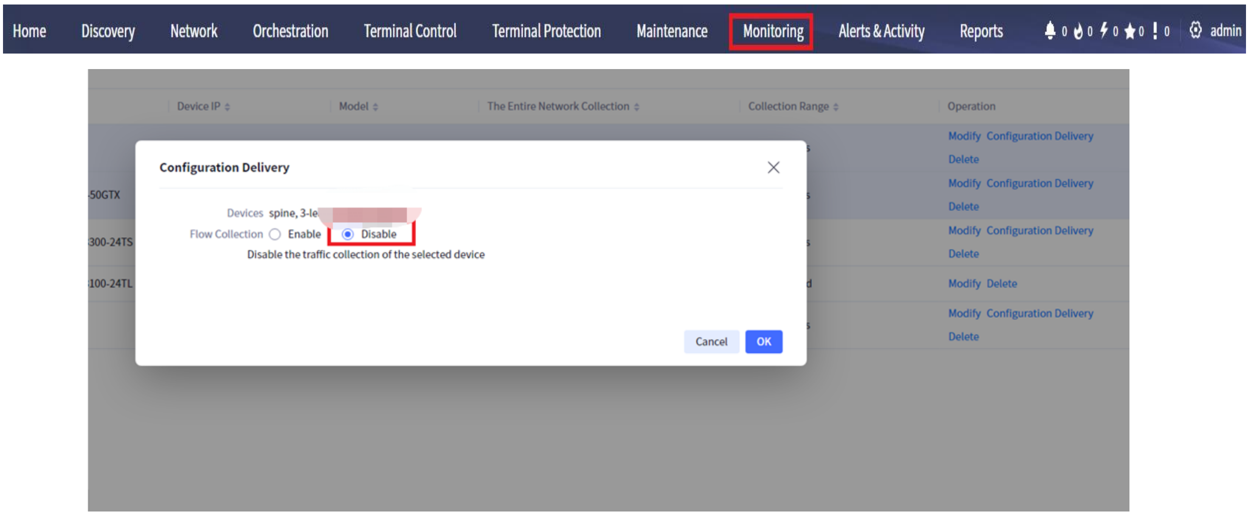
Range: 2-65535; default: 2; if it is blank, it means default

Flow Export Time 15 second

Range: 2-86400; default: 15; if it is blank, it means default

Figure 10.5.1.10 All interface configuration delivery

If multiple devices are selected, they are distributed in batch. Click the **Configuration Delivery** button to pop up a new page for configuration delivery, which displays the device name, collection mode and flow collection. It is closed by default.


Configuration Delivery

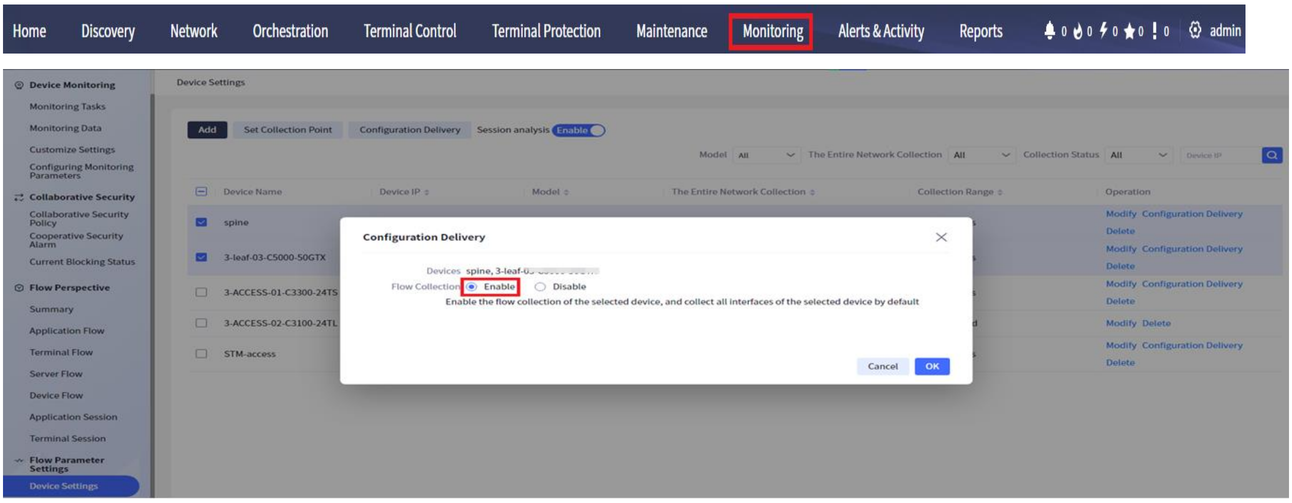
Devices spine, 3-le[redacted]

Flow Collection ○ Enable ● Disable

Disable the traffic collection of the selected device

Figure 10.5.1.11 Disable batch configuration

If multiple devices are selected, click the **Configuration Delivery** button to pop up a **Configuration Delivery** page. If the flow collection status is enabled, it is batch configuration delivery.


Configuration Delivery

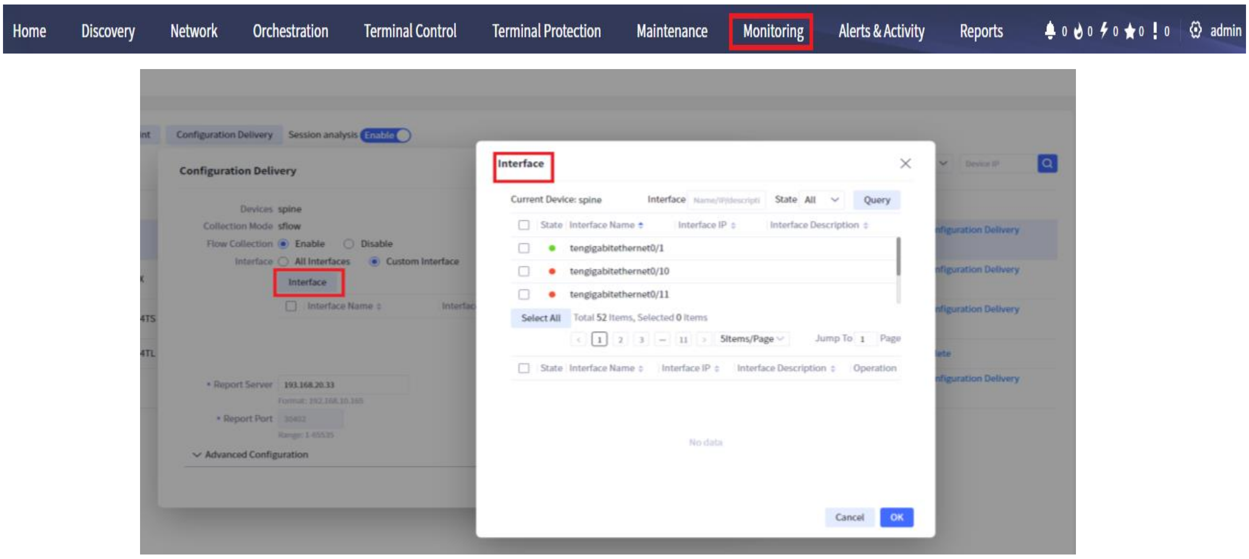
Devices spine, 3-leaf-0[redacted]

Flow Collection ● Enable ○ Disable

Enable the flow collection of the selected device, and collect all interfaces of the selected device by default

Figure 10.5.1.12 Enable batch configuration

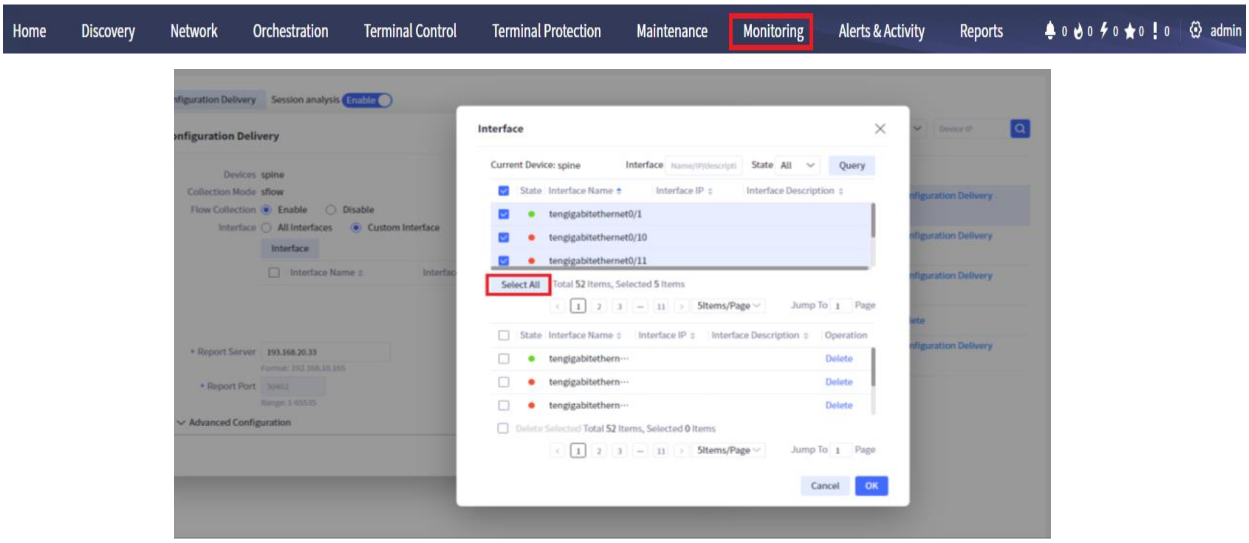
When flow collection is selected as **Enable** and some interfaces are selected for delivery, click **Interface** to open an interface for selecting interfaces. All interfaces corresponding to the device will be displayed in pages. The user selects some interfaces and fills in the report server, sampling frequency and flow export time information. Then click **OK** to deliver a configuration task. After the configuration task is completed. The collection status of the device is displayed as some interfaces, and the effect is shown in the figure.



Devices: spine
Collection Mode: sflow
Flow Collection: ● Enable ○ Disable
Interface: ○ All Interfaces ● Custom Interface
Report Server: 193.168.20.33
Total 52 Items, Selected 0 Items

Figure 10.5.1.13 Some interface configuration delivery

On the **Interface** page, the user can click the box in front of an interface or directly click the interface to add, or click the box in the upper left corner of the device list or the **Select all** button to add all devices. The effect is shown in the figure.



Total 52 Items, Selected 5 Items

Figure 10.5.1.14 Select the interface

You can delete the selected interface. Deletion is divided into batch deletion and single deletion.

Batch delete: select the desired devices, and click **Delete Selected** under the added device list to delete all the selected interfaces, as shown in the figure.

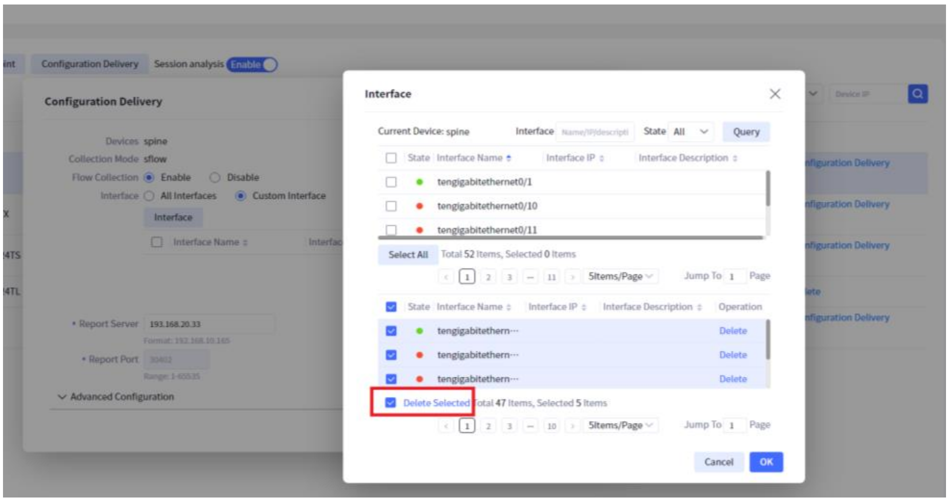
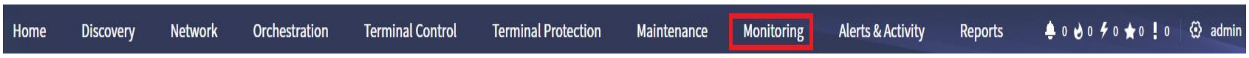


Figure 10.5.1.15 Batch device interfaces

Single delete: Select a desired interface, and then click **Delete** to delete the selected interface, as shown in the figure.

When flow collection is selected as **Disable**, a configuration task will be delivered. After the configuration task is completed, the collection status of the device will be displayed as **Configuration Disabled**.



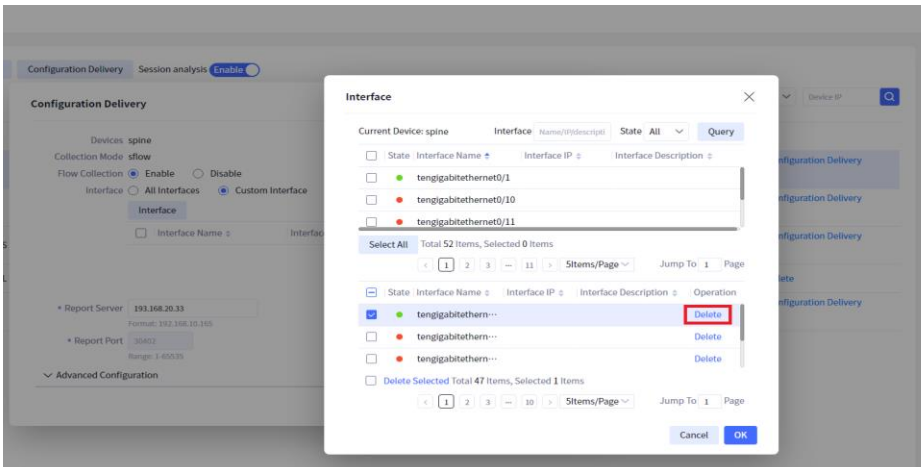
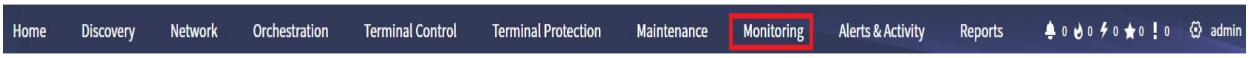


Figure 10.5.1.16 Delete a single interface

Click the **Modify** button of a device to pop up a new page for setting the whole network collection point. On this page, you can modify whether the device is a whole network collection point. The effect is shown in the figure. Click the **Set** button of an interface to set it as an entire network or non-entire network collection interface. The effect is shown in the figure. On this page, you can also fill in the interface name and click **Query**. The effect is shown in the figure.



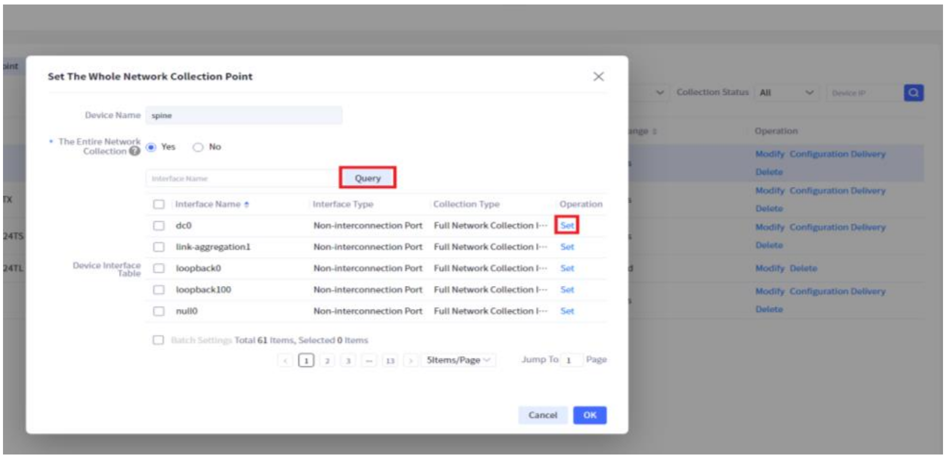


Figure 10.5.1.17 Modify collection configuration

You can delete the collection configuration. Deletion is divided into batch deletion and single deletion.

Batch delete: Select the desired collection configuration rules, click the **Batch Delete** button below, a prompt box will appear, and then click the **OK** button. The effect is shown in the figure.

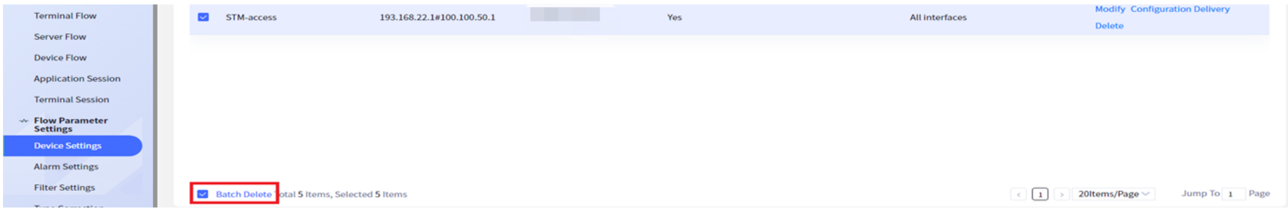


Figure 10.5.1.18 Batch delete collection configurations

Single deletion: Select a collection configuration rule, and then click the **Delete** button. A prompt box will appear, and click **OK** button. The effect is shown in the figure.

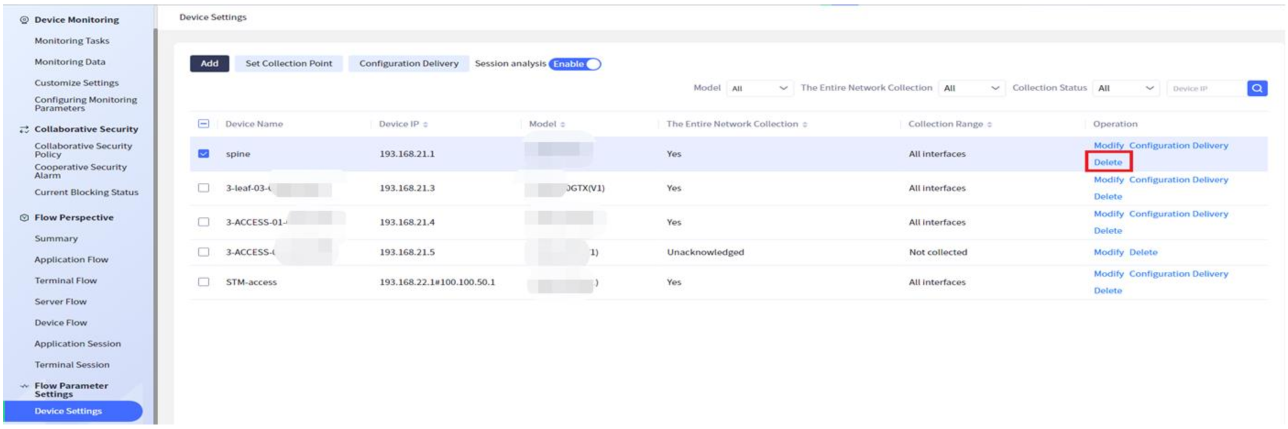


Figure 10.5.1.19 Delete a single collection configuration

The user can accurately query the collection configuration according to the device model, whether to collect the whole network, and the collection status, and can also accurately or vaguely query according to the device IP.

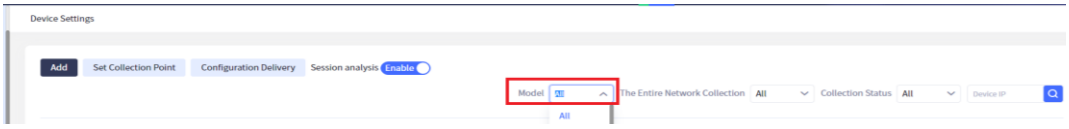


Figure 10.5.1.20 Query by device model

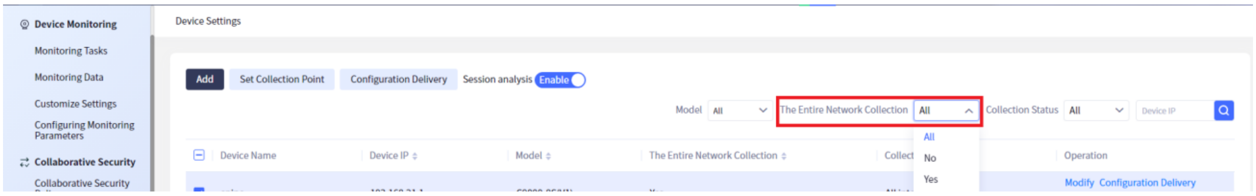


Figure 10.5.1.21 Query by whether to collect the entire network

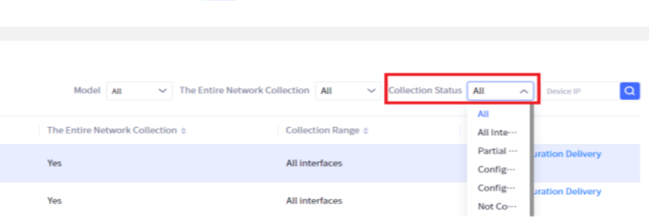
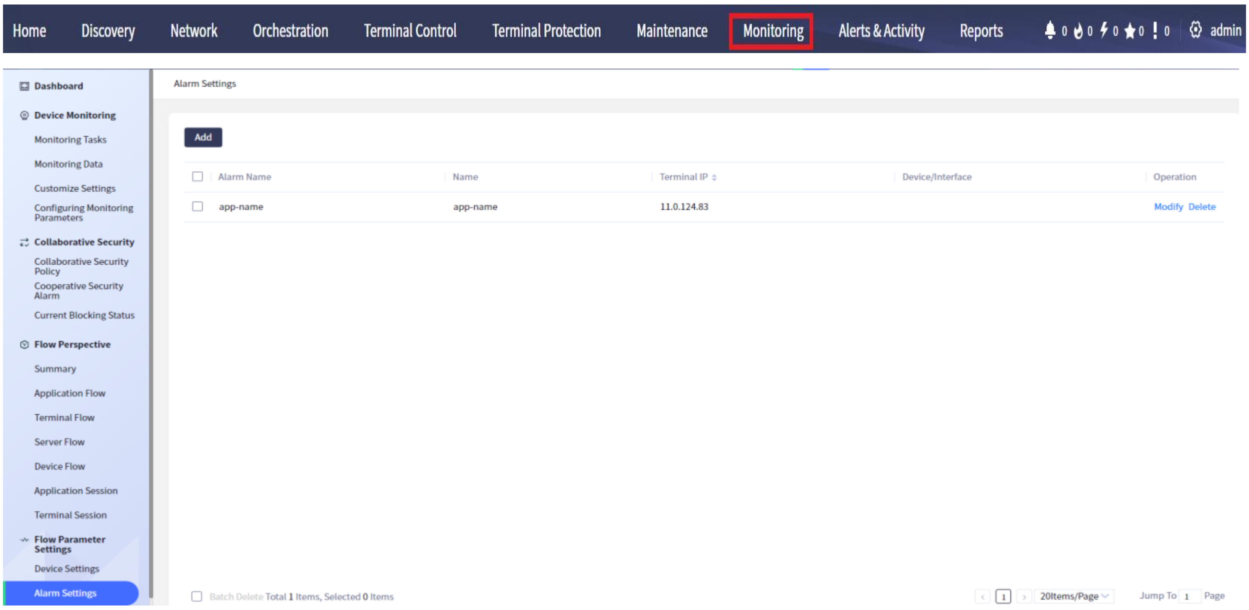


Figure 10.5.1.22 Query by collection status

10.5.2 Alarm Configuration

Click **Monitoring** > **Alarm Settings** to enter the **Alarm Settings** page, where the alarm name, application name, terminal IP and device/interface information are displayed. The effect is shown in the following figure.

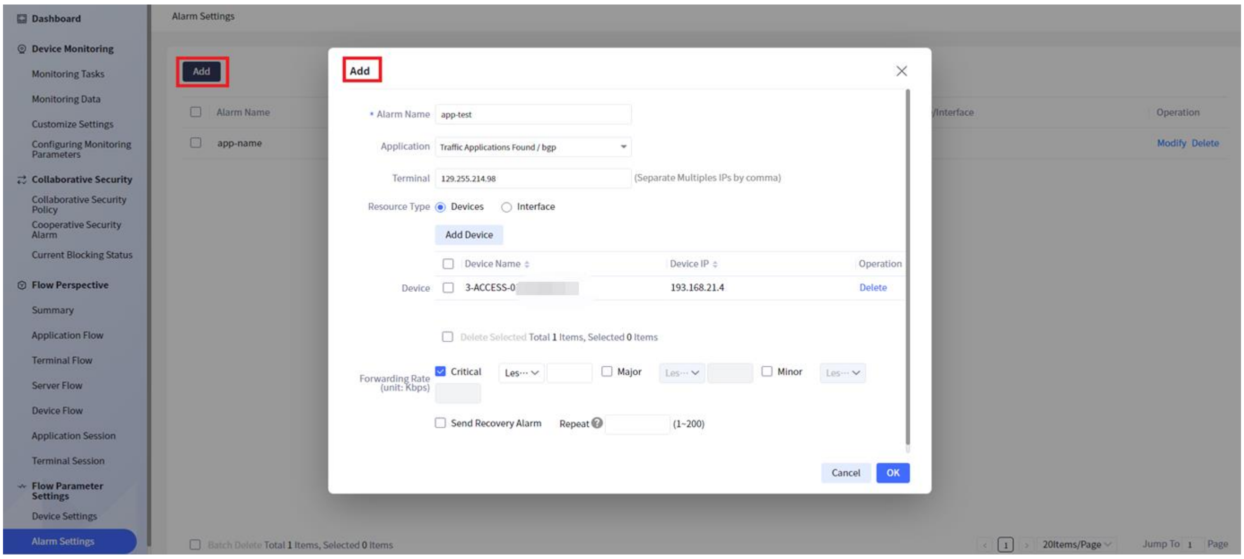


☐	Alarm Name	Name	Terminal IP	Device/Interface	Operation
☐	app-name	app-name	11.0.124.83		Modify Delete

Total 1 Items, Selected 0 Items

Figure 10.5.2.1 Alarm configuration display

Click the **Add** button in the upper left corner of the list to open an interface for adding alarm setting rules. The user needs to fill in the alarm name. When selecting an application, click the drop-down box to display the discovered traffic applications, all custom applications and all built-in applications. Click one of them to select the corresponding application name. The user also needs to enter the terminal IP. Multiple IPs are separated by commas. Select the resource type as device or interface, Select the forwarding rate, whether to send the reply alarm and the number of repetitions. The effect is shown in the figure.



Add

* Alarm Name: app-test

Application: Traffic Applications Found / bgp

Terminal: 129.255.214.98 (Separate Multiples IPs by comma)

Resource Type: ● Devices ○ Interface

	Device Name	Device IP	Operation
☐	3-ACCESS-0[redacted]	193.168.21.4	Delete

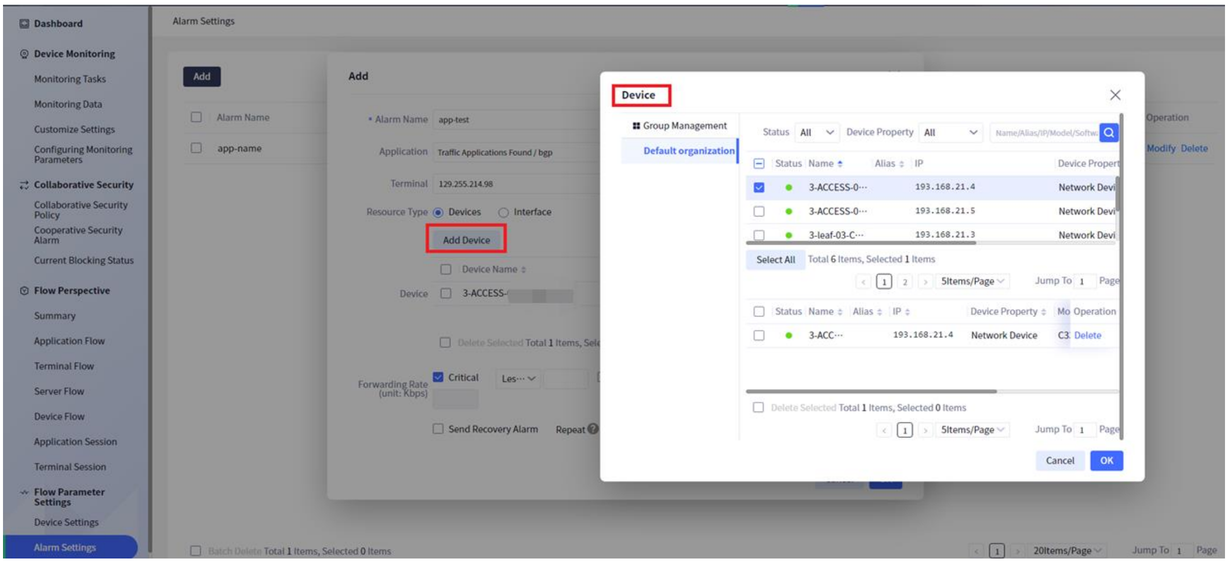
☐ Delete Selected Total 1 Items, Selected 0 Items

Forwarding Rate (unit: Kbps): ☑ Critical Les··· ☐ Major Les··· ☐ Minor Les···

☐ Send Recovery Alarm Repeat (1~200)

Figure 10.5.2.2 Add alarm configuration

When the resource type is selected as device, click **Add Device** to open the page of selecting the device. By default, all devices will be displayed, as shown in the figure.



Status: All Device Property: All

	Status	Name	Alias	IP	Device Property
☑	●	3-ACCESS-0···		193.168.21.4	Network Devi
☐	●	3-ACCESS-0···		193.168.21.5	Network Devi
☐	●	3-leaf-03-C···		193.168.21.3	Network Devi

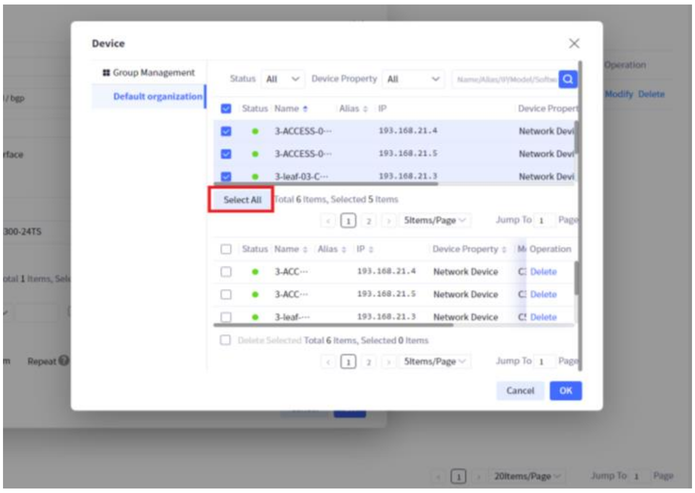
Select All Total 6 Items, Selected 1 Items

	Status	Name	Alias	IP	Device Property	Mo	Operation
☐	●	3-ACC···		193.168.21.4	Network Device	C3	Delete

☐ Delete Selected Total 1 Items, Selected 0 Items

Figure 10.5.2.3 Select the device

On the page of selecting the device, the user can click the box in front of a device or directly click the device to add, or click the box in the upper left corner of the device list or the **Select All** button to add all devices. The effect is shown in the figure.



Status: All Device Property: All

	Status	Name	Alias	IP	Device Property
☑	●	3-ACCESS-0···		193.168.21.4	Network Devi
☑	●	3-ACCESS-0···		193.168.21.5	Network Devi
☑	●	3-leaf-03-C···		193.168.21.3	Network Devi

Select All Total 6 Items, Selected 5 Items

	Status	Name	Alias	IP	Device Property	M	Operation
☐	●	3-ACC···		193.168.21.4	Network Device	C	Delete
☐	●	3-ACC···		193.168.21.5	Network Device	C	Delete
☐	●	3-leaf-···		193.168.21.3	Network Device	C	Delete

☐ Delete Selected Total 6 Items, Selected 0 Items

Figure 10.5.2.4 Add the device

You can delete the selected device. Deletion is divided into batch deletion and single deletion.

Batch delete: Select the desired devices, and click **Delete** under the added device list to delete all the selected devices, as shown in the figure.

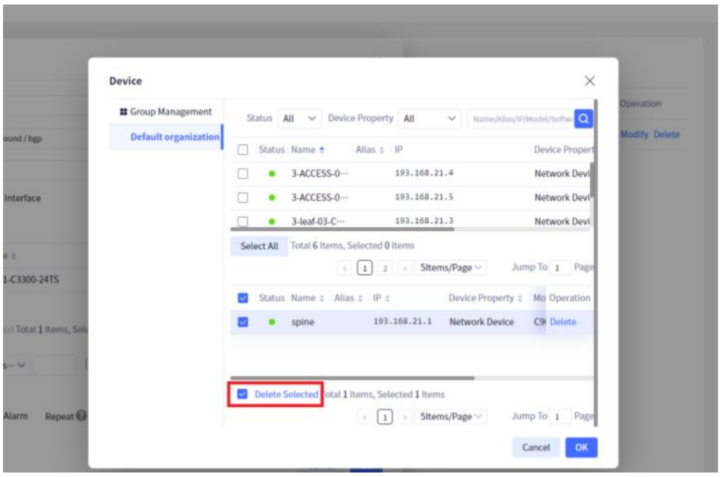


Figure 10.5.2.5 Batch delete devices

Single delete: select a desired device, and then click **Delete** to delete the selected device. The effect is as shown in the figure.

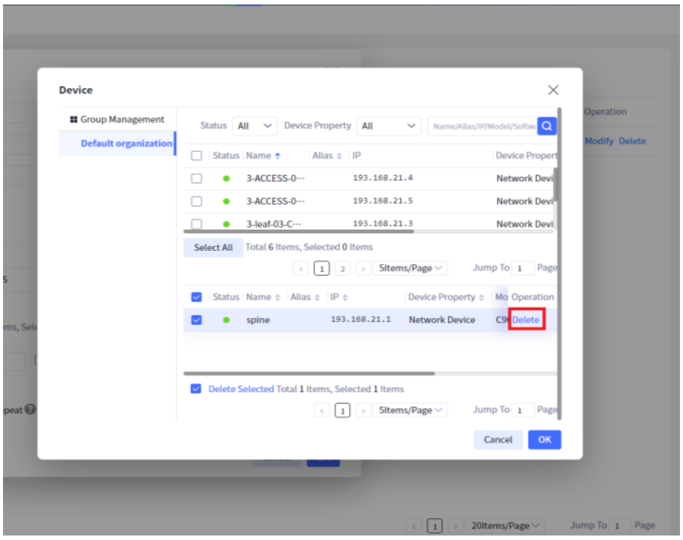


Figure 10.5.2.6 Delete a single device

The user can accurately query the device according to the status and device attributes, or fuzzy query by filling in the name, alias, IP, model and software version. The effect is shown in the figure.

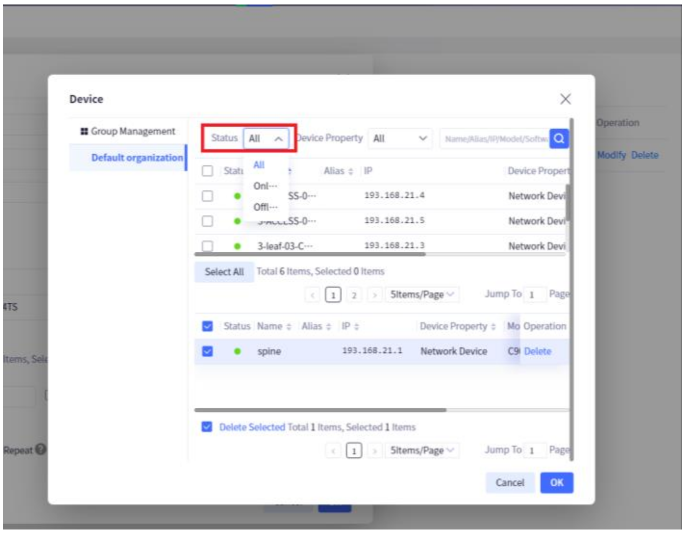


Figure 10.5.2.7 Query by the status

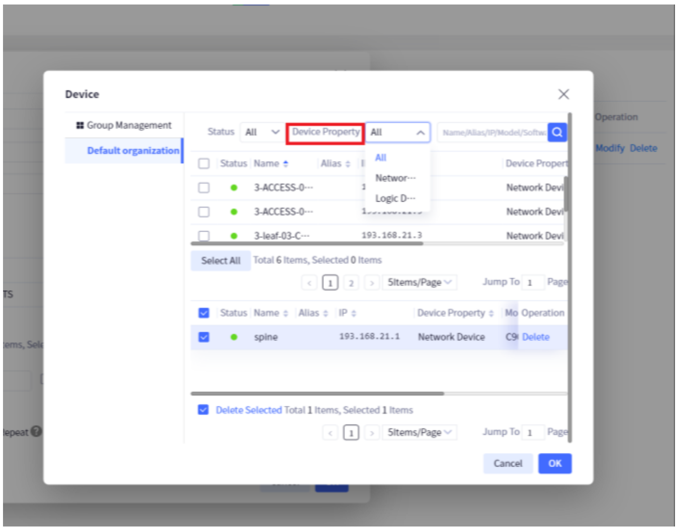


Figure 10.4.5.8 Query by the device attributes

When the resource type is selected as interface, click **Add Interface** to open the page of selecting the device, which displays all interfaces by default, as shown in the figure.

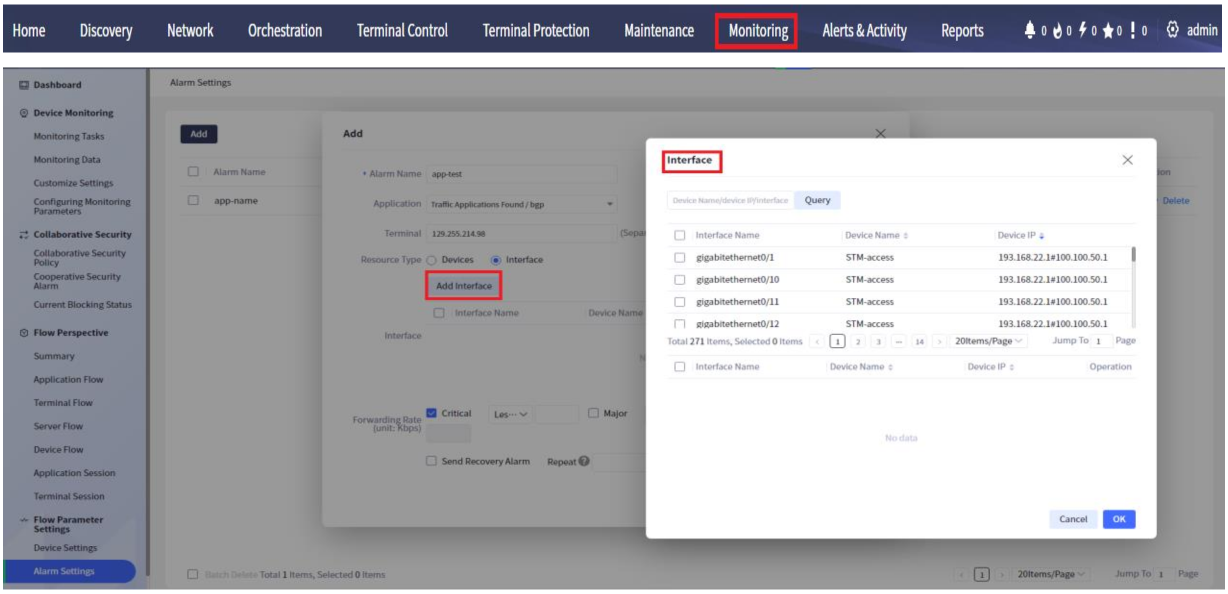
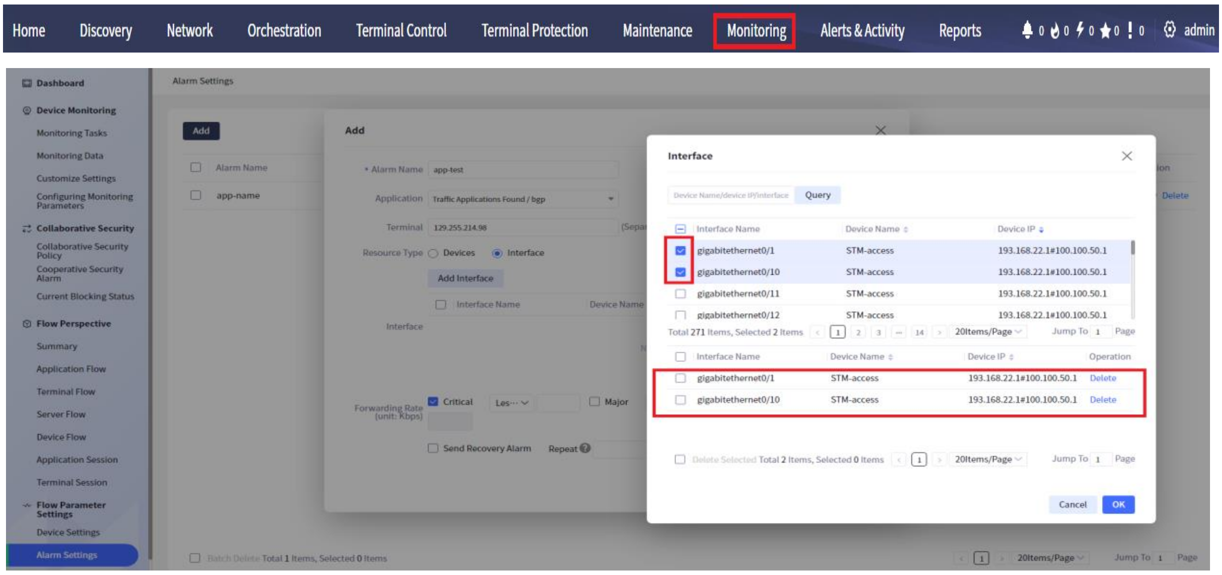


Figure 10.5.2.9 Select the interface

On the page of selecting the interface, the user can click the box in front of an interface or directly click the interface to add, or click the box in the upper left corner of the device list to add all interfaces. The effect is shown in the figure.



Alarm Name: app-test

Application: Traffic Applications Found / bgp

Terminal: 129.255.214.98

Resource Type: ○ Devices ● Interface

☐ Interface Name	Device Name	Device IP
☑ gigabitethernet0/1	STM-access	193.168.22.1#100.100.50.1
☑ gigabitethernet0/10	STM-access	193.168.22.1#100.100.50.1
☐ gigabitethernet0/11	STM-access	193.168.22.1#100.100.50.1
☐ gigabitethernet0/12	STM-access	193.168.22.1#100.100.50.1

Total 271 Items, Selected 2 Items

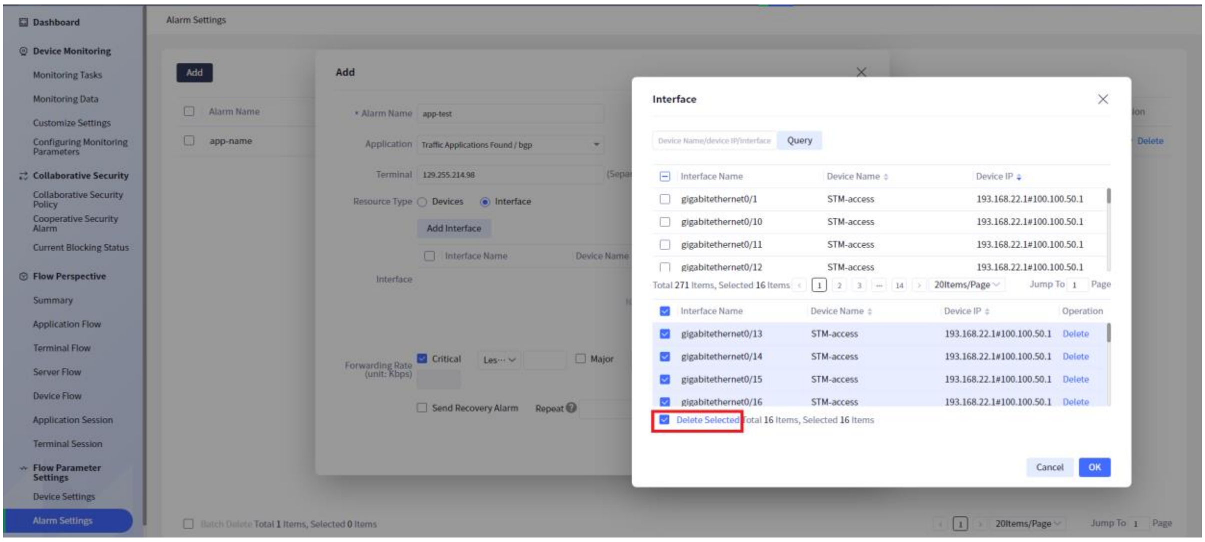
☐ Interface Name	Device Name	Device IP	Operation
☐ gigabitethernet0/1	STM-access	193.168.22.1#100.100.50.1	Delete
☐ gigabitethernet0/10	STM-access	193.168.22.1#100.100.50.1	Delete

Delete Selected Total 2 Items, Selected 0 Items

Figure 10.5.2.10 Add the interface

You can delete the selected interface. Deletion is divided into batch deletion and single deletion.

Batch delete: Select the desired interfaces, and click **Delete** under the added interface list to delete all the selected interfaces, as shown in the figure.



☐ Interface Name	Device Name	Device IP
☐ gigabitethernet0/1	STM-access	193.168.22.1#100.100.50.1
☐ gigabitethernet0/10	STM-access	193.168.22.1#100.100.50.1
☐ gigabitethernet0/11	STM-access	193.168.22.1#100.100.50.1
☐ gigabitethernet0/12	STM-access	193.168.22.1#100.100.50.1

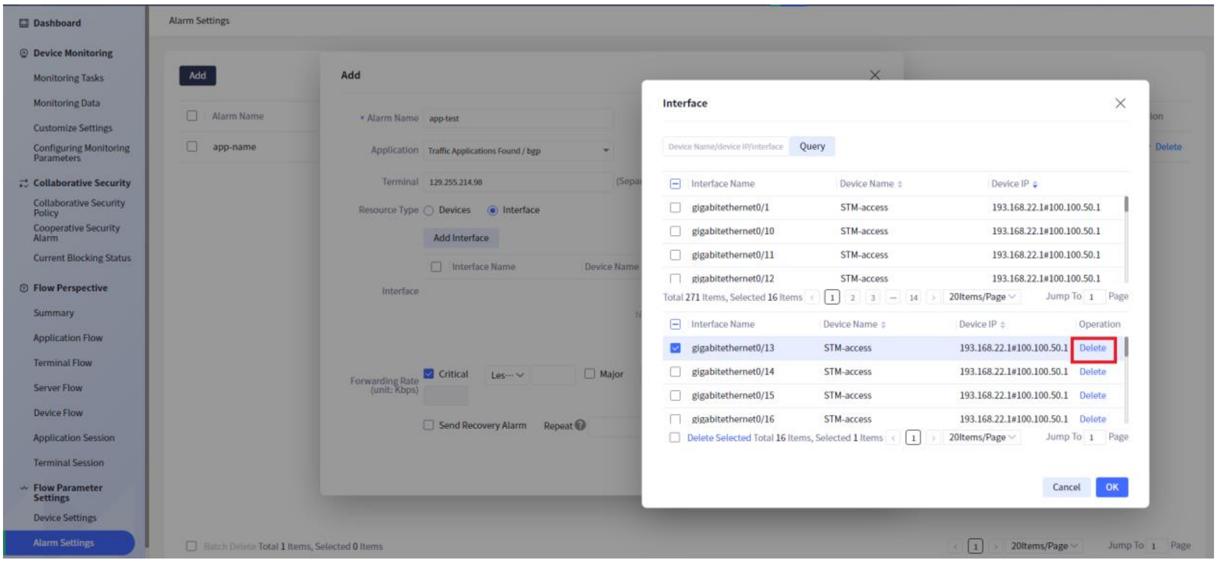
Total 271 Items, Selected 16 Items

☑ Interface Name	Device Name	Device IP	Operation
☑ gigabitethernet0/13	STM-access	193.168.22.1#100.100.50.1	Delete
☑ gigabitethernet0/14	STM-access	193.168.22.1#100.100.50.1	Delete
☑ gigabitethernet0/15	STM-access	193.168.22.1#100.100.50.1	Delete
☑ gigabitethernet0/16	STM-access	193.168.22.1#100.100.50.1	Delete

☑ Delete Selected Total 16 Items, Selected 16 Items

Figure 10.5.2.11 Batch delete interfaces

Single delete: Select a desired interface, and then click **Delete** to delete the selected interface, as shown in the figure.



Alarm Name: app-test

Application: Traffic Applications Found / bgp

Terminal: 129.255.214.98

Resource Type: ○ Devices ● Interface

☐ Interface Name	Device Name	Device IP
☐ gigabitethernet0/1	STM-access	193.168.22.1#100.100.50.1
☐ gigabitethernet0/10	STM-access	193.168.22.1#100.100.50.1
☐ gigabitethernet0/11	STM-access	193.168.22.1#100.100.50.1
☐ gigabitethernet0/12	STM-access	193.168.22.1#100.100.50.1

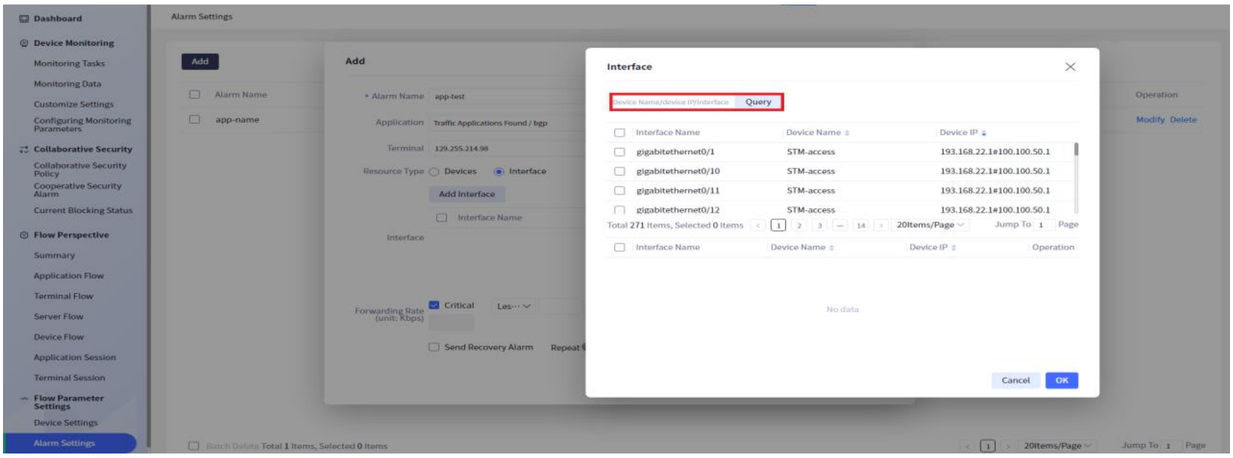
Total 271 Items, Selected 16 Items

☐ Interface Name	Device Name	Device IP	Operation
☑ gigabitethernet0/13	STM-access	193.168.22.1#100.100.50.1	Delete
☐ gigabitethernet0/14	STM-access	193.168.22.1#100.100.50.1	Delete
☐ gigabitethernet0/15	STM-access	193.168.22.1#100.100.50.1	Delete
☐ gigabitethernet0/16	STM-access	193.168.22.1#100.100.50.1	Delete

Delete Selected Total 16 Items, Selected 1 Items

Figure 10.5.2.12 Delete a single interface

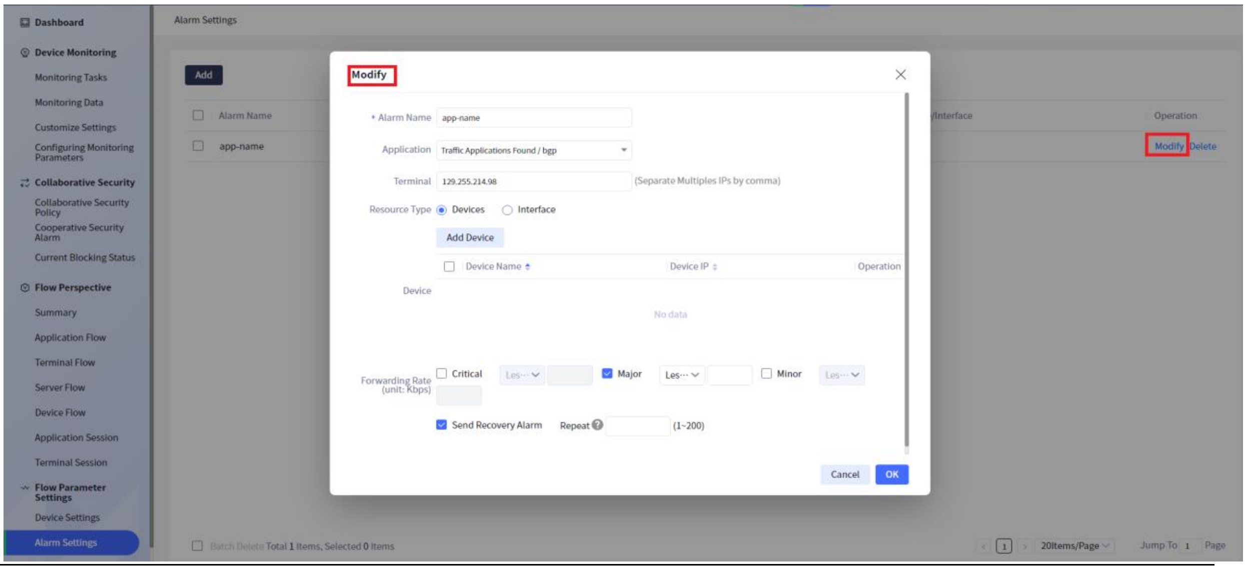
Users can accurately query according to the filled interface name, device IP and device name.



Total 271 Items, Selected 0 Items

Figure 10.5.2.13 Query by device name, IP, interface

Users can modify alarm configuration rules. Select an alarm configuration rule and click **Modify**. The user can modify the alarm name, the originally selected application and the terminal in the rule. At the same time, the resource types in the original rules can be added or deleted. The user can also modify the forwarding rate, whether to restore alarms, alarm times, etc. After the modification, click **OK**. The effect is shown in the figure.



Alarm Name: app-name

Application: Traffic Applications Found / bgp

Terminal: 129.255.214.98 (Separate Multiples IPs by comma)

Resource Type: ● Devices ○ Interface

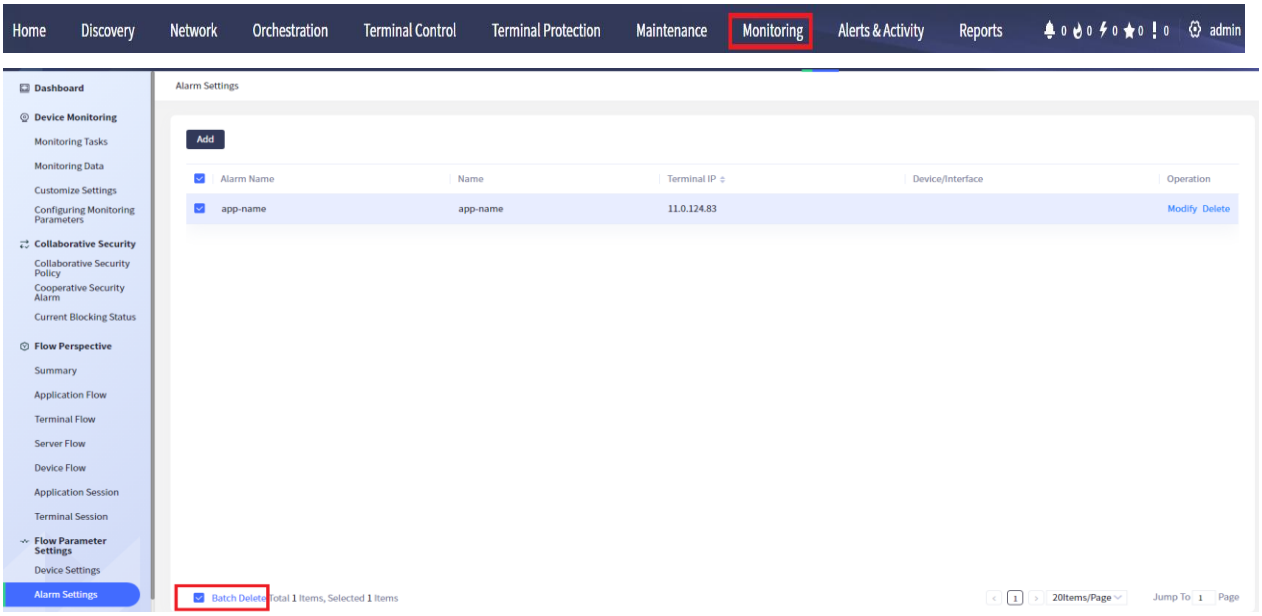
Forwarding Rate (unit: Kbps): ☐ Critical ☑ Major ☐ Minor

☑ Send Recovery Alarm Repeat (1~200)

Figure 10.5.2.14 Modify alarm configuration rule

Users can delete alarm configuration rules. Deletion is divided into batch deletion and single deletion.

Batch delete: Select the desired alarm configuration rules, click the **Batch Delete** button below, a prompt box will appear, and then click the **OK** button in the prompt box. The effect is shown in the figure.

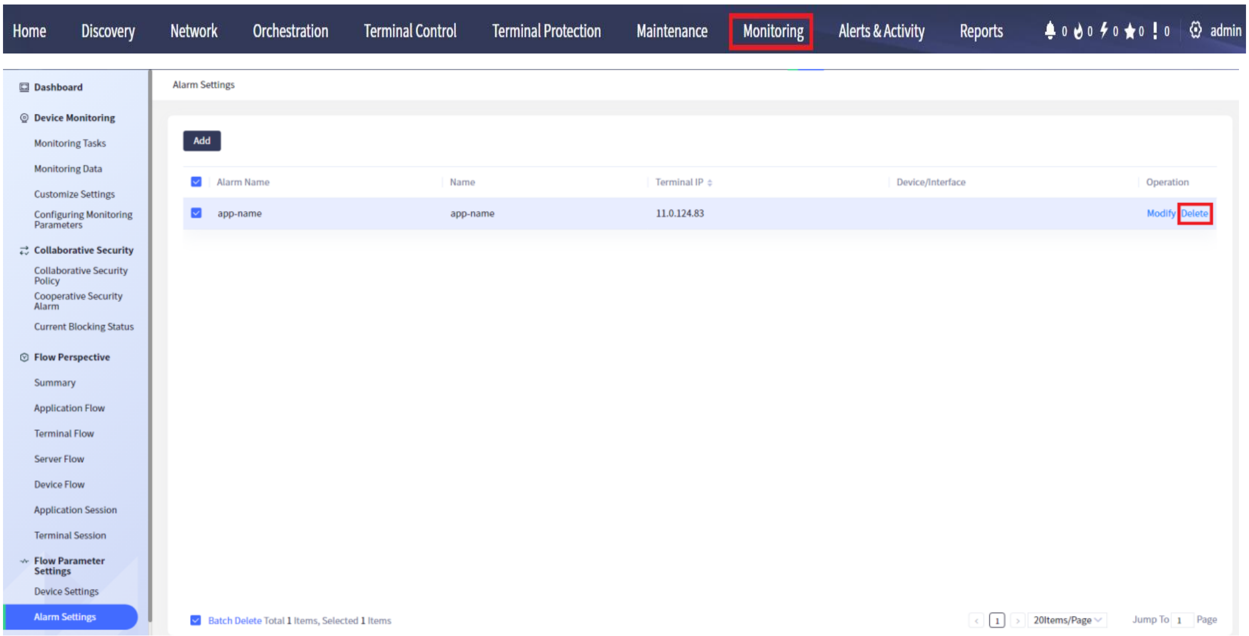


☑	Alarm Name	Name	Terminal IP	Device/Interface	Operation
☑	app-name	app-name	11.0.124.83		Modify Delete

☑ Batch Delete Total 1 Items, Selected 1 Items

Figure 10.5.2.15 Batch delete alarm configurations

Single deletion: Select a server identification rule and click **Delete** to display a prompt box. Click **OK** in the prompt box. The effect is shown in the figure.



☑	Alarm Name	Name	Terminal IP	Device/Interface	Operation
☑	app-name	app-name	11.0.124.83		Modify Delete

☑ Batch Delete Total 1 Items, Selected 1 Items

Figure 10.5.2.16 Delete a single alarm configuration

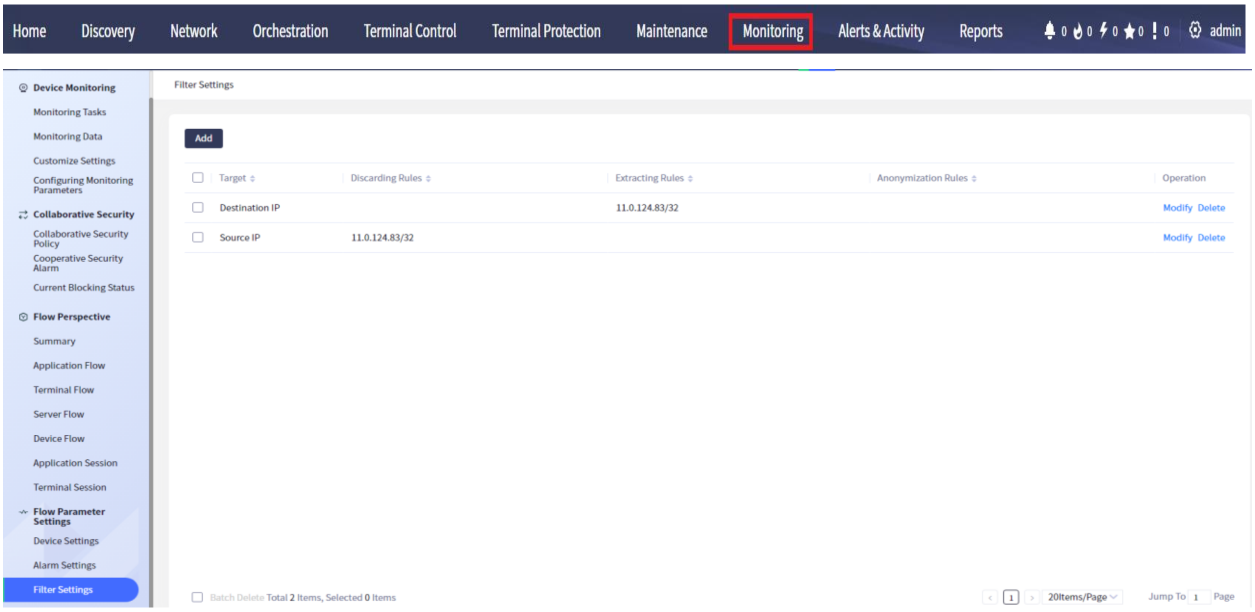
Note

- Multiple terminal IPs entered on the Add page are separated by commas

- Only when the times of continuously exceeding the threshold meets the number of repetitions, can the index be confirmed to be abnormal and an alarm of exceeding the threshold is sent.
- Only when the times of continuously not exceeding the threshold value meets the number of repetitions, can the index be confirmed to return to normal and a recovery alarm be sent.

10.5.3 Filter Configuration

Click **Monitoring** > **Filter Settings** to enter the **Filter Settings** page, where the configuration object (source IP or destination IP), discarding rule, extraction rule and anonymization rule are displayed. The effect is shown in the following figure:

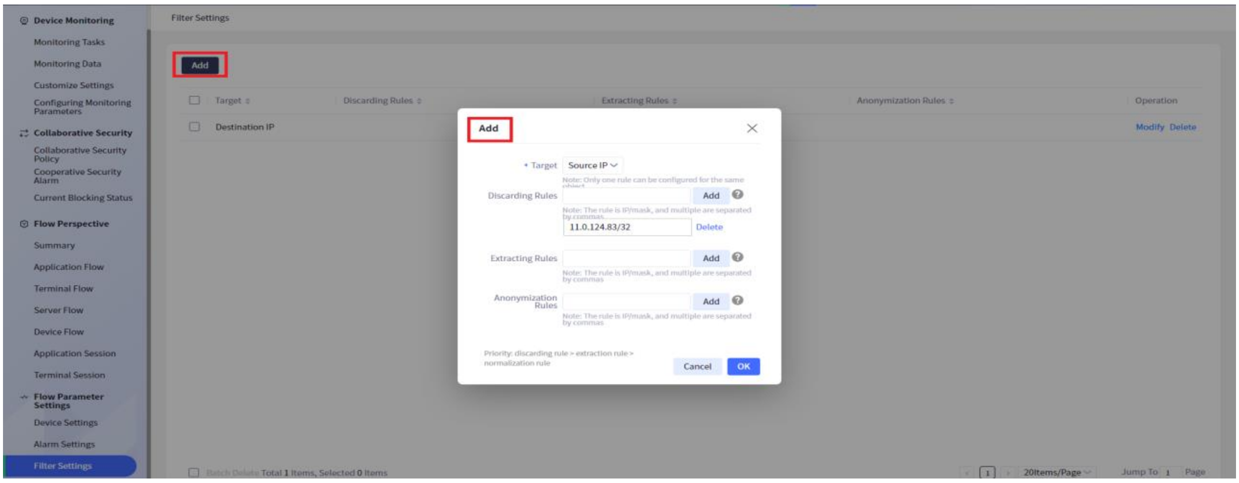


☐	Target	Discarding Rules	Extracting Rules	Anonymization Rules	Operation
☐	Destination IP		11.0.124.83/32		Modify Delete
☐	Source IP	11.0.124.83/32			Modify Delete

Total 2 Items, Selected 0 Items

Figure 10.5.3.1 Filter settings display

Click **Add** in the upper left corner of the list to open the interface for adding filter configuration rules. You need to select whether the object of the filter rule is the source IP or the destination IP. You need to fill in the rule information according to the rule requirements. The pre-added rule information can be deleted by clicking **Delete** on the left. After filling in, click **OK** to complete the addition of filter configuration content.



Note: Only one rule can be configured for the same object

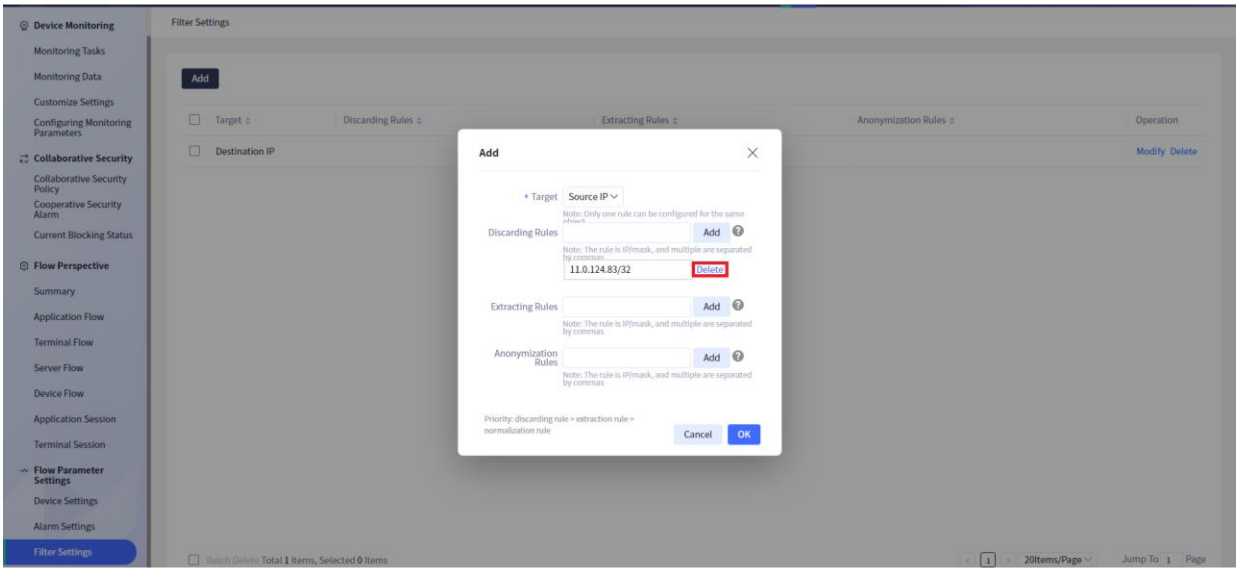
Note: The rule is IP/mask, and multiple are separated by commas

11.0.124.83/32

Priority: discarding rule > extraction rule > normalization rule

Total 1 Items, Selected 0 Items

Figure 10.5.3.2 Add filter configuration



Note: Only one rule can be configured for the same object

Note: The rule is IP/mask, and multiple are separated by commas

11.0.124.83/32

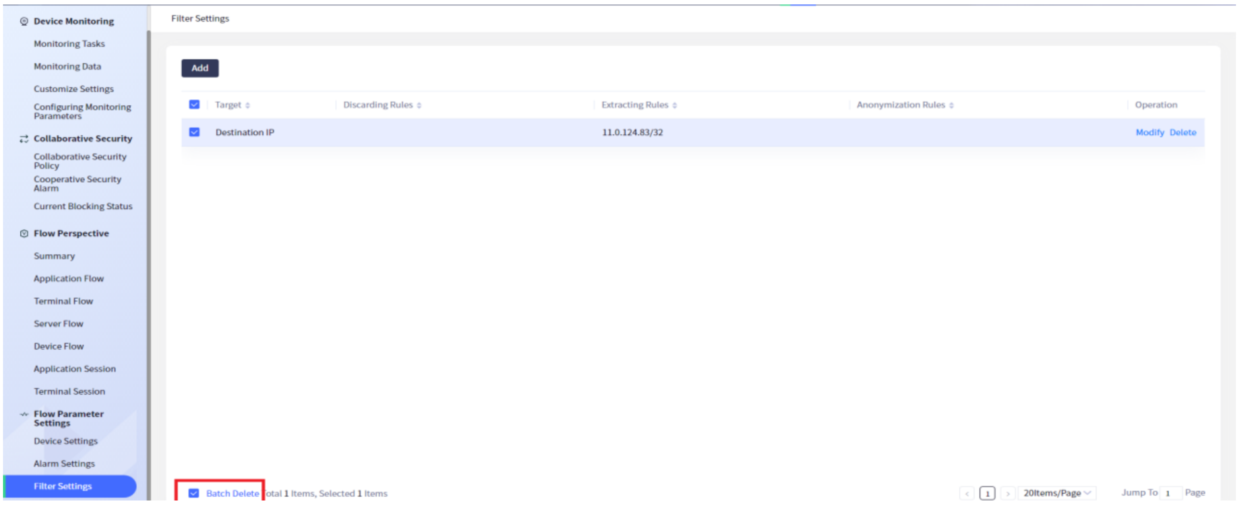
Priority: discarding rule > extraction rule > normalization rule

Total 1 Items, Selected 0 Items

Figure 10.5.3.3 Delete the pre-added filter configuration

Users can delete filter configuration rules. Deletion is divided into batch deletion and single deletion.

Batch delete: Select the desired filter configuration rules, click **Batch delete** below to display a prompt box, and then click **OK** in the prompt box. The effect is as shown in the figure.



Target	Discarding Rules	Extracting Rules	Anonymization Rules	Operation
Destination IP		11.0.124.83/32		Modify Delete

Total 1 Items, Selected 1 Items

Figure 10.5.3.4 Batch delete filter configurations

Single deletion: Select a server identification rule and click **Delete** to display a prompt box. Click **OK** in the prompt box. The effect is shown in the figure.

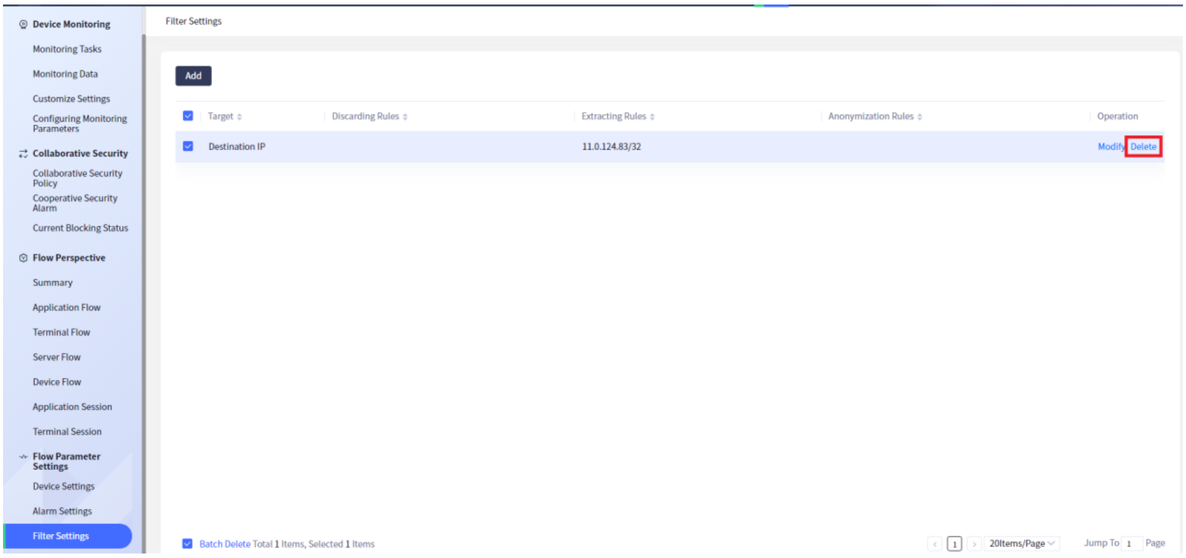


Figure 10.5.3.5 Delete a single filter configuration

Users can modify the filter configuration rule. Select a filter configuration rule and click **Modify**. Users can modify the objects in the rule and the originally configured rule information. At the same time, you can click **Delete** on the right of the rule to delete the rule information, or you can click **Add** to add a new filter rule based on the original filter configuration rule information. Multiple IP addresses of the same rule are separated by commas. After modification, click the **OK** button, and the effect is as shown in the figure.

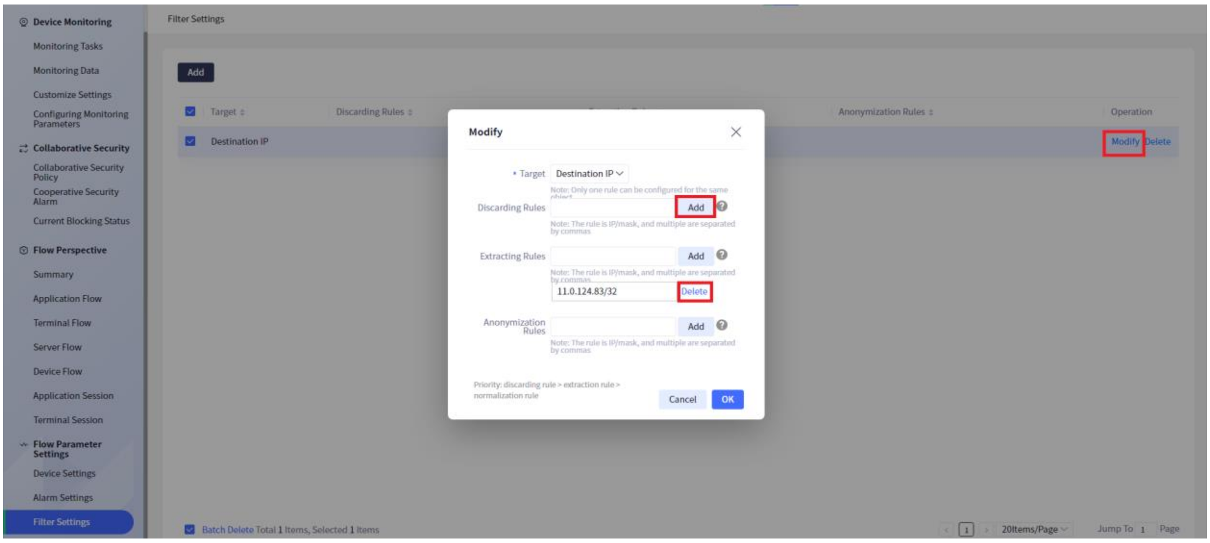

Filter Settings
Add
Target
Discarding Rules
Anonymization Rules
Operation
Destination IP
Modify
Delete
Modify
* Target
Destination IP
Note: Only one rule can be configured for the same object
Discarding Rules
Add
Note: The rule is IP/mask, and multiple are separated by commas
Extracting Rules
Add
Note: The rule is IP/mask, and multiple are separated by commas
11.0.124.83/32
Delete
Anonymization Rules
Add
Note: The rule is IP/mask, and multiple are separated by commas
Priority: discarding rule > extraction rule > normalization rule
Cancel
OK
Batch Delete Total 1 Items, Selected 1 Items
20Items/Page
Jump To
Page

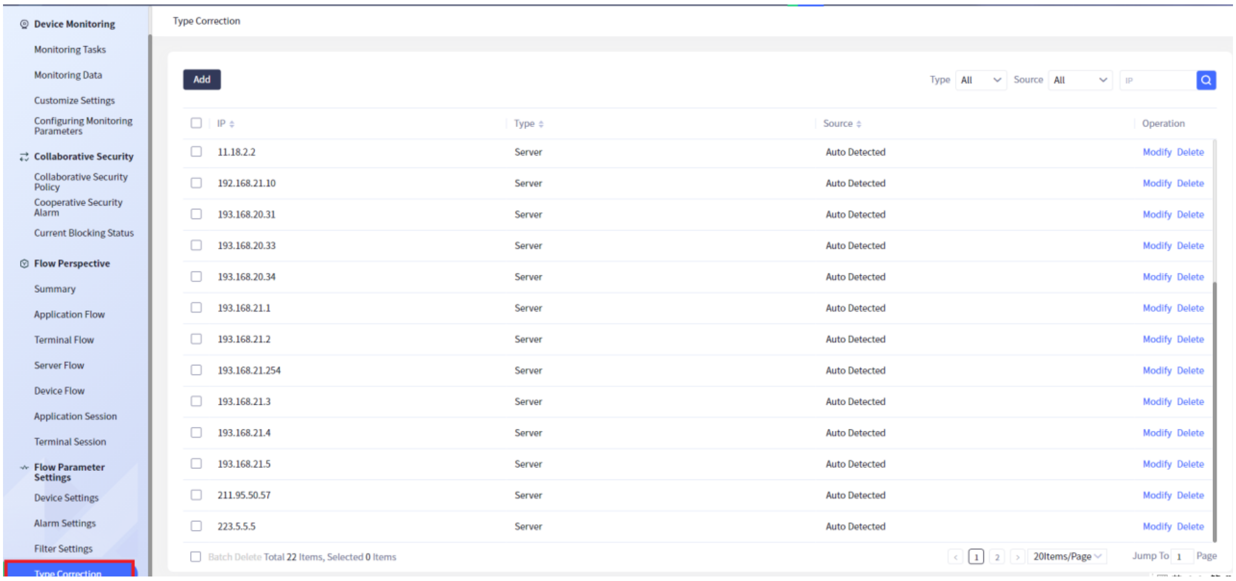
Figure 10.5.3.6 Modify the filter configuration

Note

- Only one rule can be configured for the same object.
- The rules are in IP/MASK mode, and multiple are separated by commas.
- Rule priority: discard rule > extract rule > anonymization rule.

10.5.4 Type Correction

Click **Monitoring** > **Type Correction** to enter the **Type Correction** page, where the IP address, type (terminal or server) and source (auto detected or manual detected) are displayed. The effect is shown in the following figure.



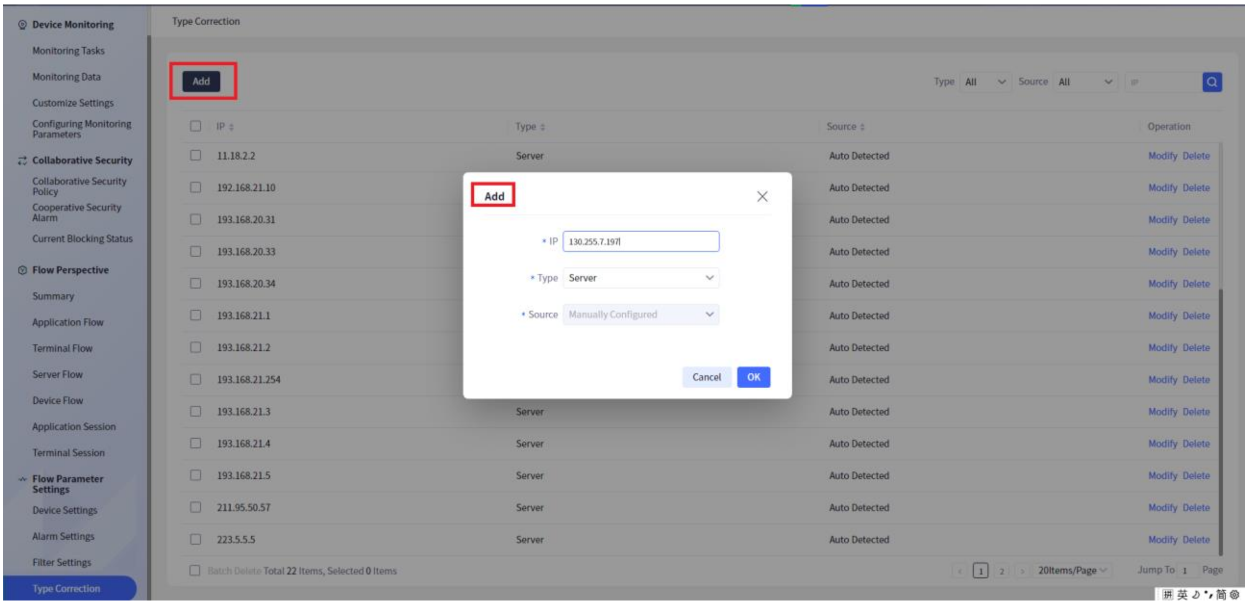
☐ IP	Type	Source	Operation
☐ 11.18.2.2	Server	Auto Detected	Modify Delete
☐ 192.168.21.10	Server	Auto Detected	Modify Delete
☐ 193.168.20.31	Server	Auto Detected	Modify Delete
☐ 193.168.20.33	Server	Auto Detected	Modify Delete
☐ 193.168.20.34	Server	Auto Detected	Modify Delete
☐ 193.168.21.1	Server	Auto Detected	Modify Delete
☐ 193.168.21.2	Server	Auto Detected	Modify Delete
☐ 193.168.21.254	Server	Auto Detected	Modify Delete
☐ 193.168.21.3	Server	Auto Detected	Modify Delete
☐ 193.168.21.4	Server	Auto Detected	Modify Delete
☐ 193.168.21.5	Server	Auto Detected	Modify Delete
☐ 211.95.50.57	Server	Auto Detected	Modify Delete
☐ 223.5.5.5	Server	Auto Detected	Modify Delete

☐ Batch Delete Total 22 Items, Selected 0 Items

< 1 2 > 20Items/Page Jump To 1 Page

Figure 10.5.4.1 Type correction display

Click the **Add** button in the upper left corner of the list to open an interface for adding type correction. The user needs to fill in the IP and select the type, which is divided into terminal and server. After filling in, click **OK** to complete the addition of type correction content.



* IP: 130.255.7.197

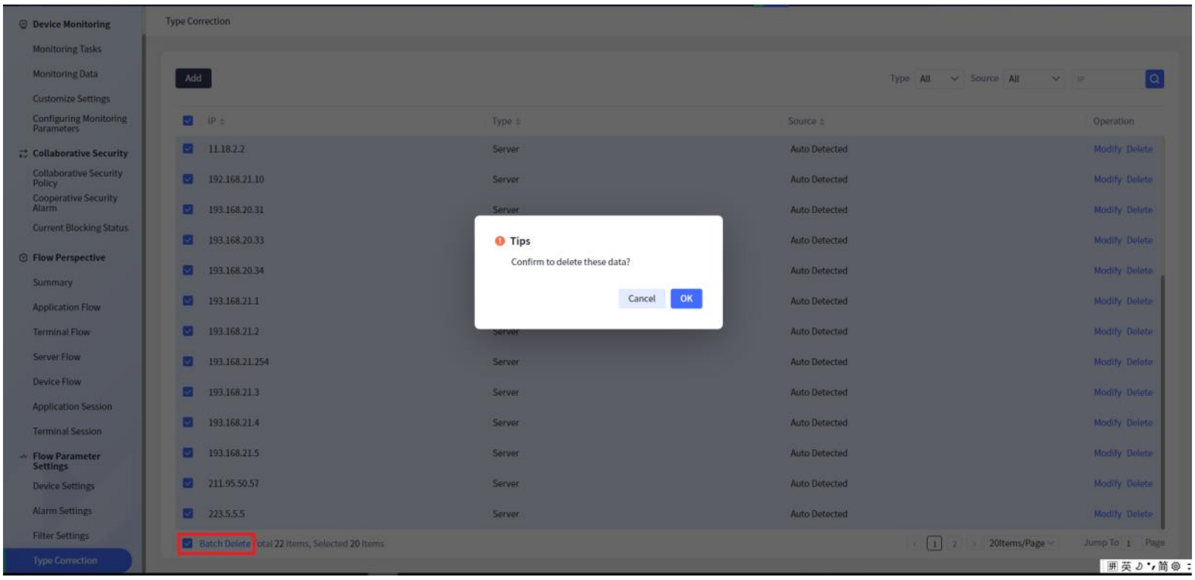
* Type: Server

* Source: Manually Configured

Figure 10.5.4.2 Add type correction rule

Users can delete the type correction rules. Deletion is divided into batch deletion and single deletion.

Batch delete: Select a desired type correction rule, click **Batch Delete** below, a prompt box will appear, and then click **OK** in the prompt box. The effect is as shown in the figure.



☑	IP	Type	Source	Operation
☑	11.18.2.2	Server	Auto Detected	Modify Delete
☑	192.168.21.10	Server	Auto Detected	Modify Delete
☑	193.168.20.31	Server	Auto Detected	Modify Delete
☑	193.168.20.33		Auto Detected	Modify Delete
☑	193.168.20.34		Auto Detected	Modify Delete
☑	193.168.21.1		Auto Detected	Modify Delete
☑	193.168.21.2	Server	Auto Detected	Modify Delete
☑	193.168.21.254	Server	Auto Detected	Modify Delete
☑	193.168.21.3	Server	Auto Detected	Modify Delete
☑	193.168.21.4	Server	Auto Detected	Modify Delete
☑	193.168.21.5	Server	Auto Detected	Modify Delete
☑	211.95.50.57	Server	Auto Detected	Modify Delete
☑	223.5.5.5	Server	Auto Detected	Modify Delete

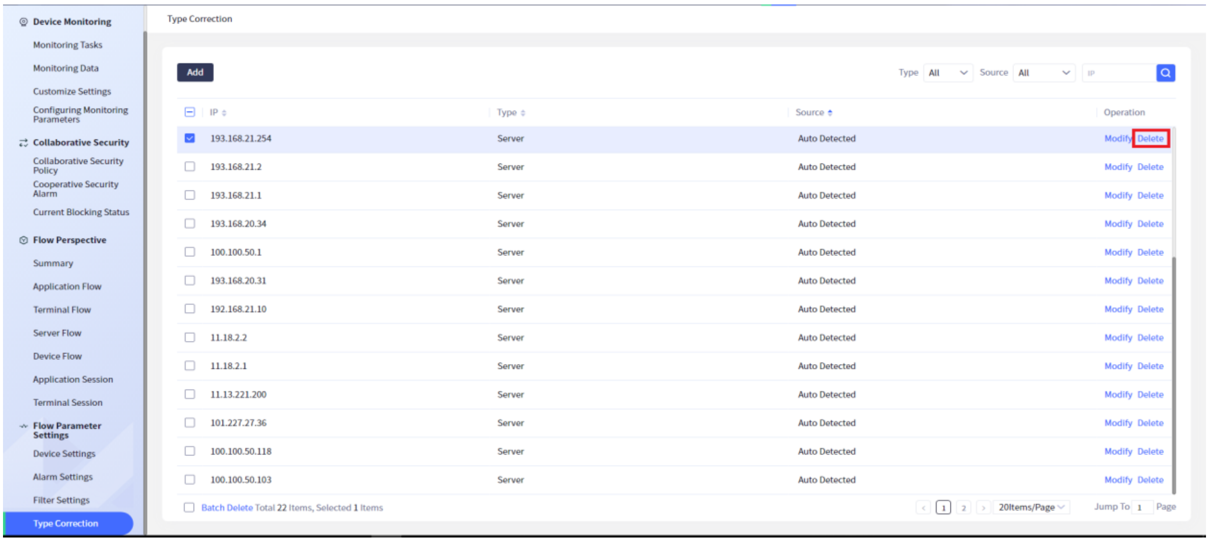
☑ Batch Delete otal 22 Items, Selected 20 Items

Tips

Confirm to delete these data?

Figure 10.5.4.3 Batch delete type correction rules

Single deletion: Select a type correction rule, and then click **Delete**. A prompt box will appear, and then click **OK** in the prompt box. The effect is as shown in the figure.

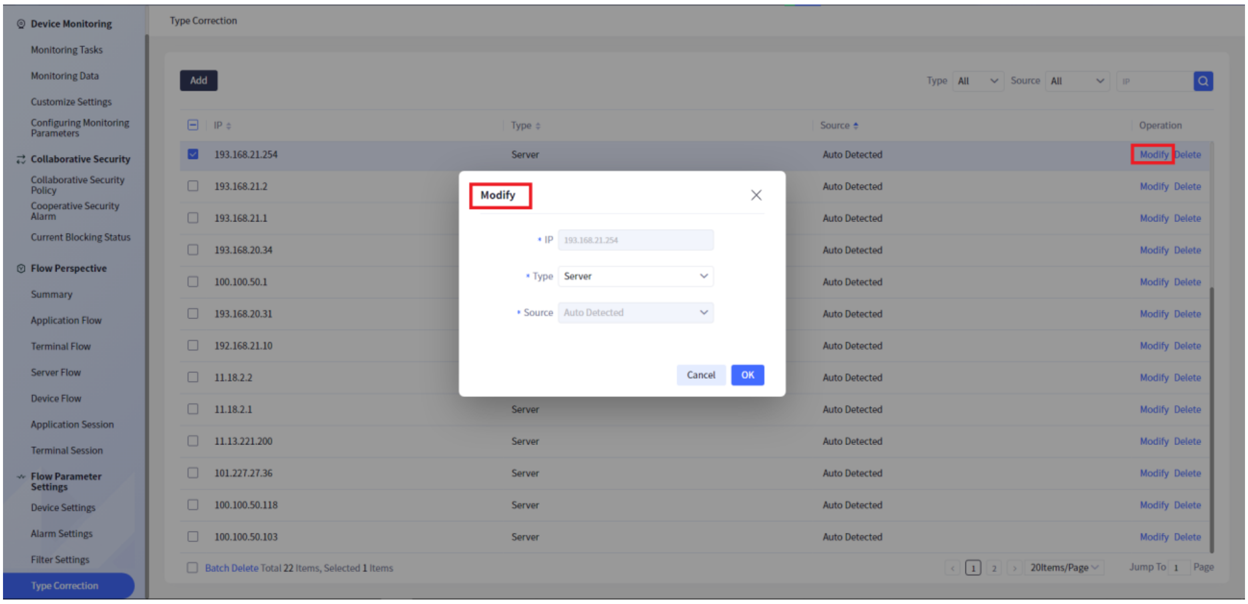


⊟	IP	Type	Source	Operation
☑	193.168.21.254	Server	Auto Detected	Modify Delete
☐	193.168.21.2	Server	Auto Detected	Modify Delete
☐	193.168.21.1	Server	Auto Detected	Modify Delete
☐	193.168.20.34	Server	Auto Detected	Modify Delete
☐	100.100.50.1	Server	Auto Detected	Modify Delete
☐	193.168.20.31	Server	Auto Detected	Modify Delete
☐	192.168.21.10	Server	Auto Detected	Modify Delete
☐	11.18.2.2	Server	Auto Detected	Modify Delete
☐	11.18.2.1	Server	Auto Detected	Modify Delete
☐	11.13.221.200	Server	Auto Detected	Modify Delete
☐	101.227.27.36	Server	Auto Detected	Modify Delete
☐	100.100.50.118	Server	Auto Detected	Modify Delete
☐	100.100.50.103	Server	Auto Detected	Modify Delete

☐ Batch Delete Total 22 Items, Selected 1 Items

Figure 10.5.4.4 Delete a single type correction rule

Users can modify the type correction rules. Select a server identification rule and click **Modify**. You can only modify the type. After modification, click **OK**. The effect is as shown in the figure.



Modify

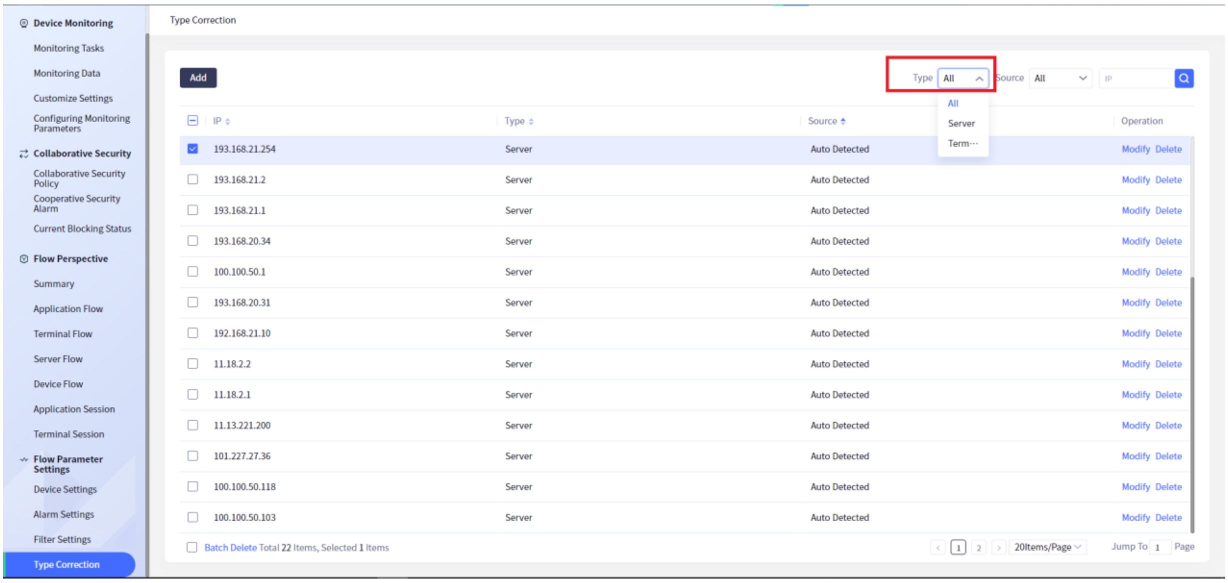
- IP: 193.168.21.254
- Type: Server
- Source: Auto Detected

☐	IP	Type	Source	Operation
☑	193.168.21.254	Server	Auto Detected	Modify Delete
☐	193.168.21.2		Auto Detected	Modify Delete
☐	193.168.21.1		Auto Detected	Modify Delete
☐	193.168.20.34		Auto Detected	Modify Delete
☐	100.100.50.1		Auto Detected	Modify Delete
☐	193.168.20.31		Auto Detected	Modify Delete
☐	192.168.21.10		Auto Detected	Modify Delete
☐	11.18.2.2		Auto Detected	Modify Delete
☐	11.18.2.1	Server	Auto Detected	Modify Delete
☐	11.13.221.200	Server	Auto Detected	Modify Delete
☐	101.227.27.36	Server	Auto Detected	Modify Delete
☐	100.100.50.118	Server	Auto Detected	Modify Delete
☐	100.100.50.103	Server	Auto Detected	Modify Delete

Total 22 Items, Selected 1 Items

Figure 10.5.4.5 Modify type correction rules

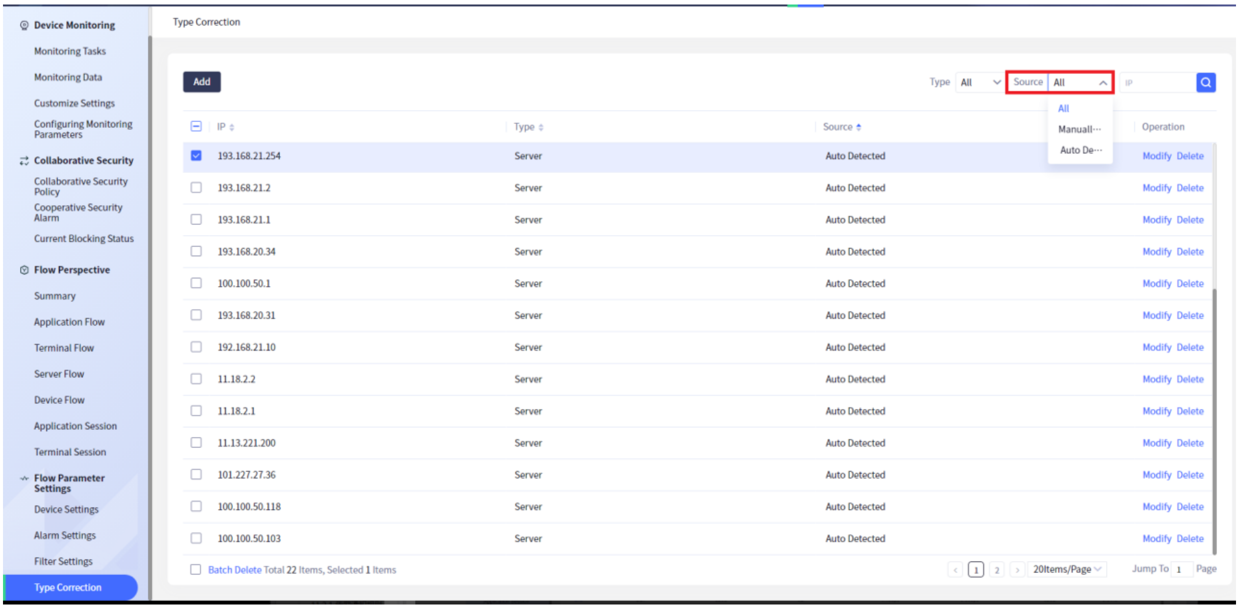
The current type correction rule presents the user with unprocessed rule information. In the current type correction rule interface, users can accurately query by type, source and IP, or fuzzy query by IP. The effect is shown in the figure.



☐	IP	Type	Source	Operation
☑	193.168.21.254	Server	Auto Detected	Modify Delete
☐	193.168.21.2	Server	Auto Detected	Modify Delete
☐	193.168.21.1	Server	Auto Detected	Modify Delete
☐	193.168.20.34	Server	Auto Detected	Modify Delete
☐	100.100.50.1	Server	Auto Detected	Modify Delete
☐	193.168.20.31	Server	Auto Detected	Modify Delete
☐	192.168.21.10	Server	Auto Detected	Modify Delete
☐	11.18.2.2	Server	Auto Detected	Modify Delete
☐	11.18.2.1	Server	Auto Detected	Modify Delete
☐	11.13.221.200	Server	Auto Detected	Modify Delete
☐	101.227.27.36	Server	Auto Detected	Modify Delete
☐	100.100.50.118	Server	Auto Detected	Modify Delete
☐	100.100.50.103	Server	Auto Detected	Modify Delete

Total 22 Items, Selected 1 Items

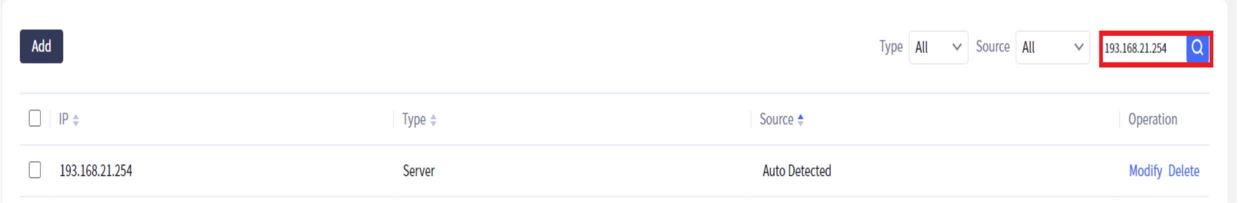
Figure 10.5.4.6 Query by type



☐	IP	Type	Source	Operation
☑	193.168.21.254	Server	Auto Detected	Modify Delete
☐	193.168.21.2	Server	Auto Detected	Modify Delete
☐	193.168.21.1	Server	Auto Detected	Modify Delete
☐	193.168.20.34	Server	Auto Detected	Modify Delete
☐	100.100.50.1	Server	Auto Detected	Modify Delete
☐	193.168.20.31	Server	Auto Detected	Modify Delete
☐	192.168.21.10	Server	Auto Detected	Modify Delete
☐	11.18.2.2	Server	Auto Detected	Modify Delete
☐	11.18.2.1	Server	Auto Detected	Modify Delete
☐	11.13.221.200	Server	Auto Detected	Modify Delete
☐	101.227.27.36	Server	Auto Detected	Modify Delete
☐	100.100.50.118	Server	Auto Detected	Modify Delete
☐	100.100.50.103	Server	Auto Detected	Modify Delete

☐ Batch Delete Total 22 Items, Selected 1 Items

Figure 10.5.4.7 Query by source



☐	IP	Type	Source	Operation
☐	193.168.21.254	Server	Auto Detected	Modify Delete

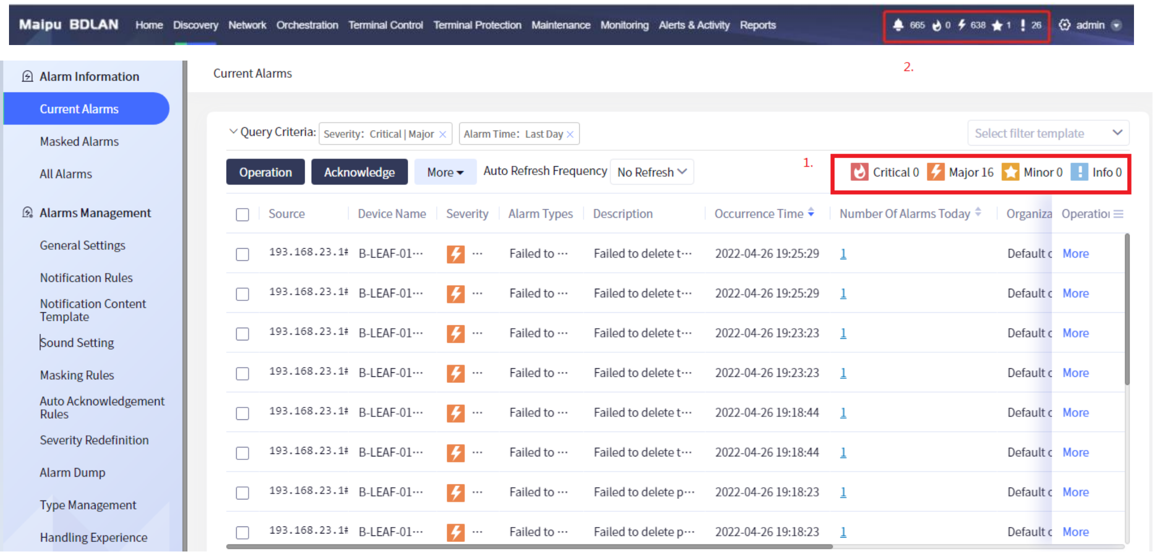
Figure 10.5.4.8 Query by IP

11 Log Alarms

The alarm module is responsible for storing the alarm information generated by the device and other modules, and providing it to the user for viewing in the interface. In addition, the alarm module also provides various configurations, such as alarm notification configuration, alarm shielding configuration, alarm level redefinition, etc. Among them, the alarm notification configuration can encapsulate some important messages in the controller (such as device offline, excessive device load, etc.) or messages concerned by the administrator into alarm information and actively send it to the administrator in the form of SMS and e-mail, so that the network administrator can timely and dynamically understand the network operation, perceive possible network problems in advance, and improve the management efficiency and early warning ability.

11.1 Alarm Information

Click "Alerts&Activity" > "Current Alarms" in the menu bar to open the **Current Alarms** page. The left navigation of the **Current Alarms** interface includes current alarms, masked alarms and all alarms. The alarm events triggered by all components can be found in the alarm event view. The effect is as shown in the figure: current alarms, masked alarms and all alarms pages. The statistics of alarms at each level can be seen in Part 1 of the figure. Click the icon to filter out the alarms at this level. The alarm overview in the upper right corner of the page indicates the alarm information counted by level of the current alarm. Click to jump to the current alarm page and filter out the alarms of the selected alarm level. The alarm probability icon in the upper right corner of the page is the same as the bell. If the alarm sound is playing, you can click the icon to stop playing



Query Criteria: Severity: Critical | Major ✕ Alarm Time: Last Day ✕

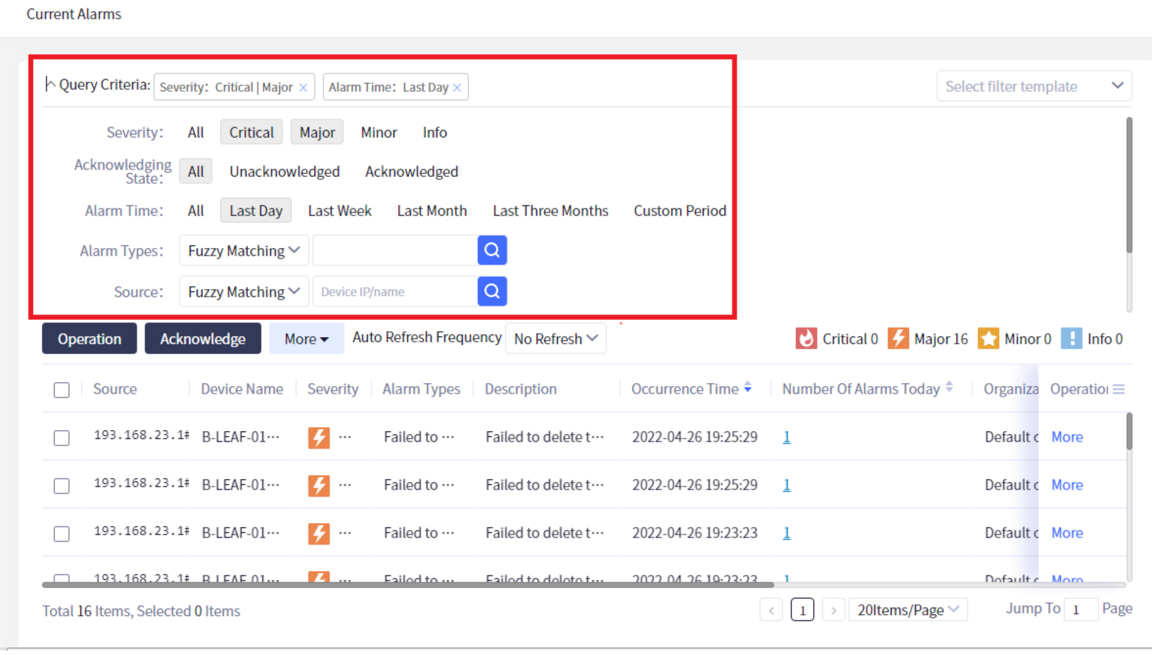
Auto Refresh Frequency: No Refresh

☐	Source	Device Name	Severity	Alarm Types	Description	Occurrence Time	Number Of Alarms Today	Organiza	Operatio
☐	193.168.23.1	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:18:44	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:18:44	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete p···	2022-04-26 19:18:23	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete p···	2022-04-26 19:18:23	1	Default c	More

Figure 11.1.1 Alarm information

Current Alarms

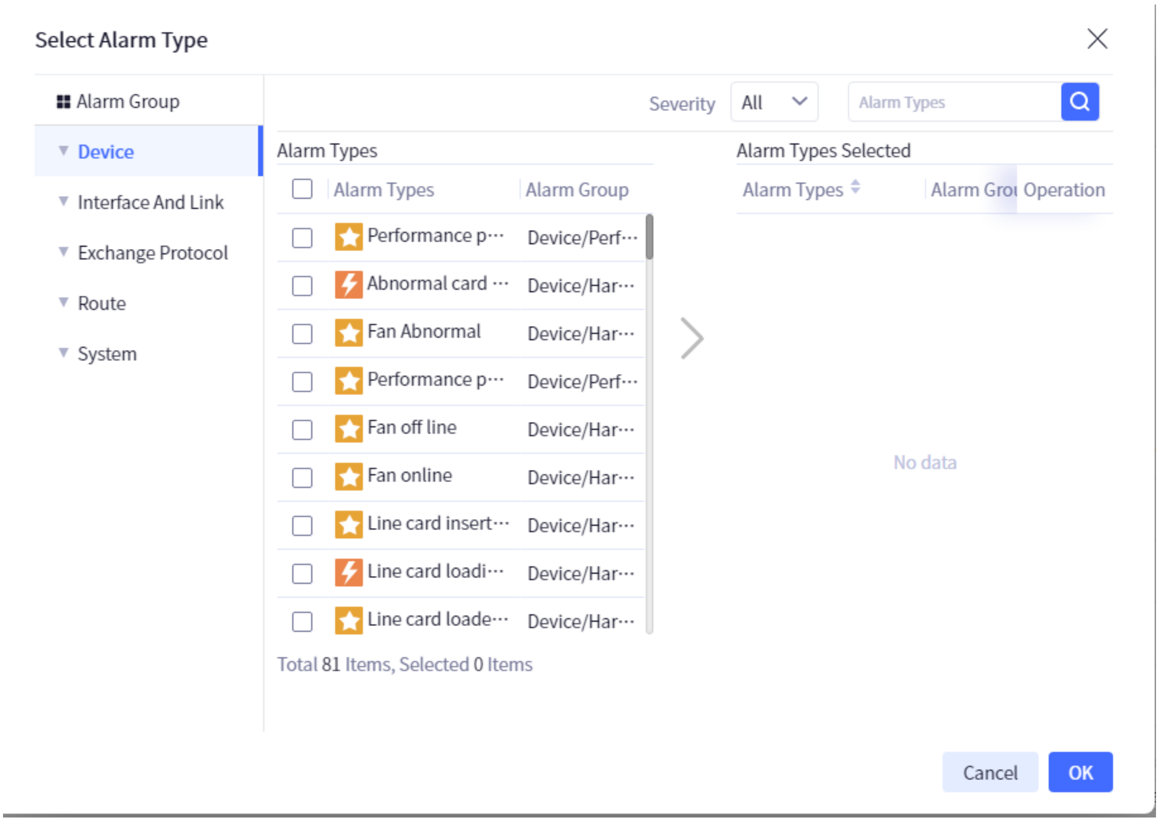
Current Alarms presents the user with unprocessed alarm information. In the current alarm interface, users can accurately query by the alarm level, confirmation status and alarm time, and can also fuzzy query by the alarm source, alarm type and description. At the same time, users can also accurately query by the alarm type and alarm source. The effect is shown in the figure.


Current Alarms
Query Criteria:
Severity: Critical | Major ×
Alarm Time: Last Day ×
Select filter template
Severity: All Critical Major Minor Info
Acknowledging State: All Unacknowledged Acknowledged
Alarm Time: All Last Day Last Week Last Month Last Three Months Custom Period
Alarm Types: Fuzzy Matching
Source: Fuzzy Matching
Device IP/name
Operation
Acknowledge
More
Auto Refresh Frequency
No Refresh
Critical 0
Major 16
Minor 0
Info 0

☐	Source	Device Name	Severity	Alarm Types	Description	Occurrence Time	Number Of Alarms Today	Organiza	Operatio
☐	193.168.23.1#	B-LEAF-01···	···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	1	Default c	More
☐	193.168.23.1#	B-LEAF-01···	···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	1	Default c	More
☐	193.168.23.1#	B-LEAF-01···	···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	1	Default c	More
☐	193.168.23.1#	B-LEAF-01···	···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	1	Default c	More

Figure 11.1.2 Current alarms

Users can accurately query by alarm type. First, select the alarm type to match accurately, then click the **Select** button on the right, and then the **Select Alarm Type** dialog box will appear. The user can add the alarm type, and finally click the **OK** button to query accurately according to the alarm type. The effect is as shown in the figure



☐	Alarm Types	Alarm Group
☐	Performance p···	Device/Perf···
☐	Abnormal card ···	Device/Har···
☐	Fan Abnormal	Device/Har···
☐	Performance p···	Device/Perf···
☐	Fan off line	Device/Har···
☐	Fan online	Device/Har···
☐	Line card insert···	Device/Har···
☐	Line card loadi···	Device/Har···
☐	Line card loade···	Device/Har···

Figure 11.1.3 Query accurately by alarm type

Users can also accurately query through the alarm source. First, select the accurate matching of alarm sources, then click the **Select** button on the right, and then the **Select Alarm Source** dialog box will appear. Users can add alarm sources by adding device groups, adding devices, adding interface groups, and adding local network management. Finally, click the **OK** button to accurately query by alarm source. The effect is shown in the figure.

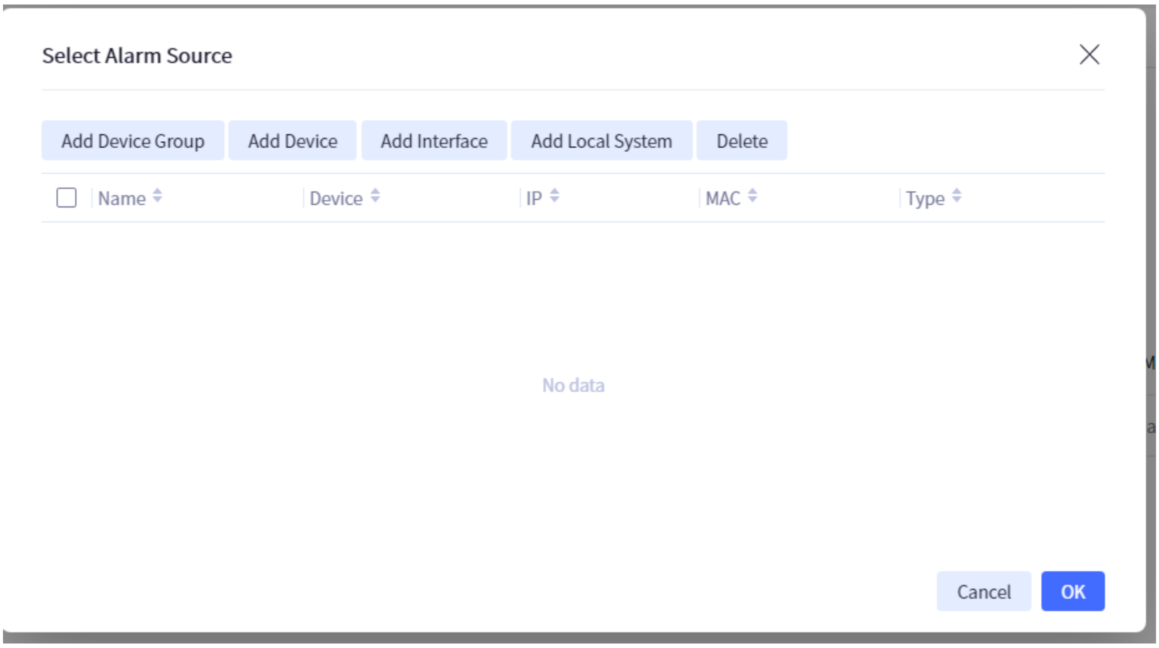


Figure 11.1.4 Query by alarm source

In addition, users can process, confirm, cancel confirmation and export alarm information. Support batch operations for processing, confirming, and canceling confirmation.

Select the desired alarm event then click the **Process** button in the current alarm interface, and a pop-up box will appear. The user needs to fill in the handling comments in the pop-up box (required), and finally click the **OK** button (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 display.

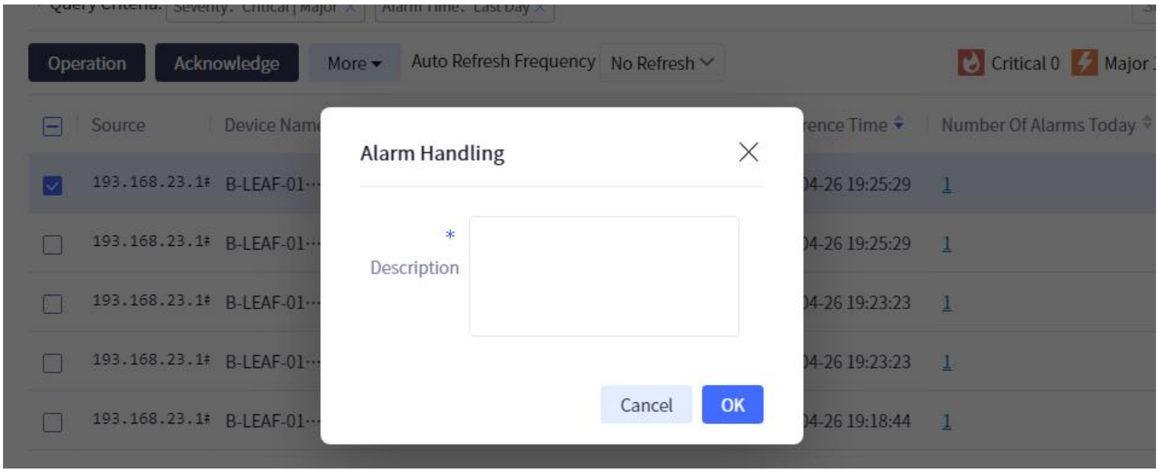


Figure 11.1.5 Process alarm events

Select the desired alarm event (not including the confirmed alarm event), then click **Acknowledge** in the current alarm interface, and a pop-up box will appear. The user needs to fill in the confirmation comments in the pop-up box (not required), and finally click **OK** (see the figure below) to confirm the selected alarm event:

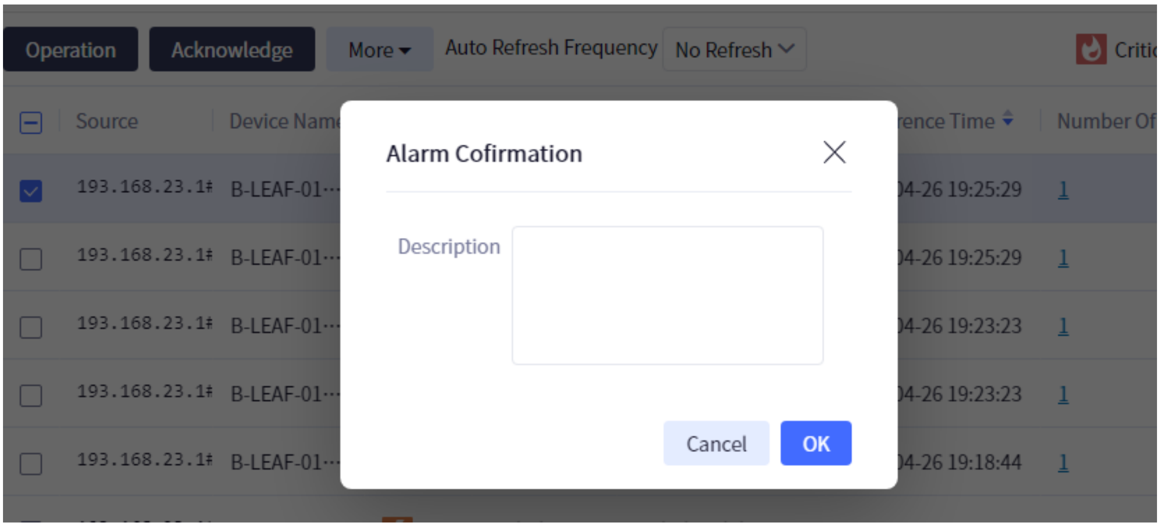
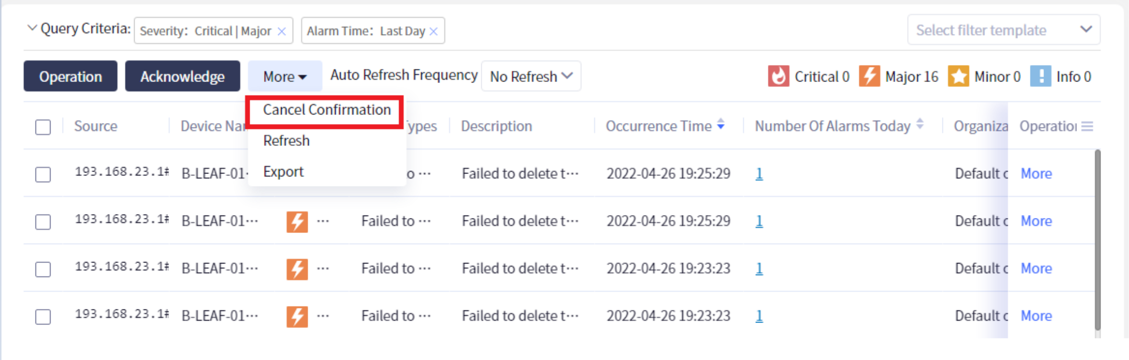


Figure 11.1.6 Confirm the alarm event

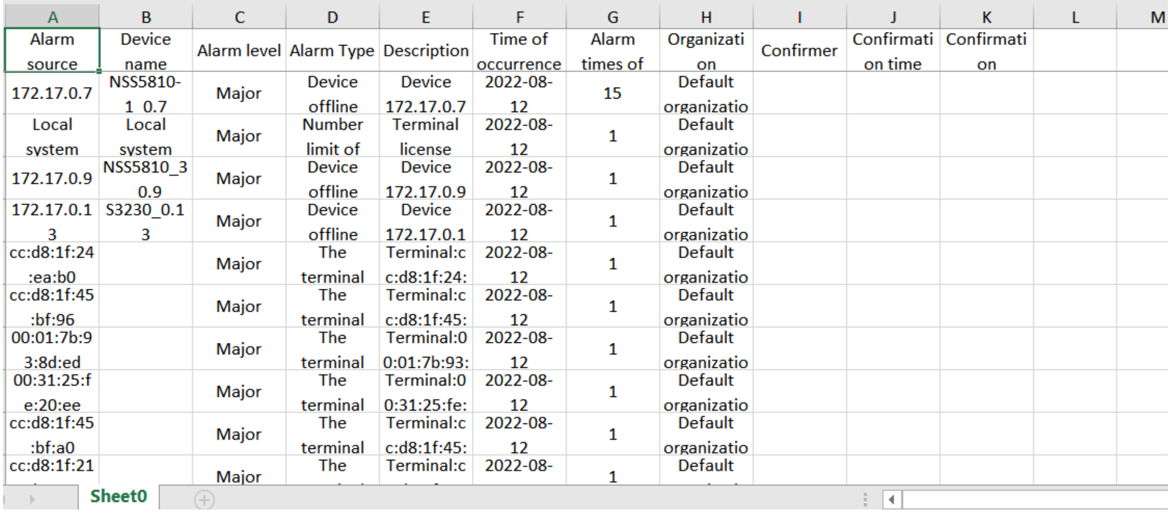
Select the desired alarm event (not including the un-confirmed alarm event), then click the **Cancel Confirmation** button in the current alarm interface, and a pop-up box will appear. Then click the **OK** button (see the figure below) to cancel the confirmation of the selected alarm event.



☐	Source	Device Na			ypes	Description	Occurrence Time	Number Of Alarms Today	Organiza	Operatio
☐	193.168.23.1	B-LEAF-01·			o ···	Failed to delete t···	2022-04-26 19:25:29	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡	···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡	···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	1	Default c	More
☐	193.168.23.1	B-LEAF-01···	⚡	···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	1	Default c	More

Figure 11.1.7 Cancel confirming the alarm event

The user can also export all alarm events, as shown in the following figure:



Alarm source	Device name	Alarm level	Alarm Type	Description	Time of occurrence	Alarm times of	Organization	Confirmer	Confirmation time	Confirmation		
172.17.0.7	NSS5810-1_0.7	Major	Device offline	Device 172.17.0.7	2022-08-12	15	Default organizatio					
Local system	Local system	Major	Number limit of	Terminal license	2022-08-12	1	Default organizatio					
172.17.0.9	NSS5810_3 0.9	Major	Device offline	Device 172.17.0.9	2022-08-12	1	Default organizatio					
172.17.0.13	S3230_0.13	Major	Device offline	Device 172.17.0.1	2022-08-12	1	Default organizatio					
cc:d8:1f:24:ea:b0		Major	The terminal	Terminal:cc:d8:1f:24:	2022-08-12	1	Default organizatio					
cc:d8:1f:45:bf:96		Major	The terminal	Terminal:cc:d8:1f:45:	2022-08-12	1	Default organizatio					
00:01:7b:93:8d:ed		Major	The terminal	Terminal:00:01:7b:93:	2022-08-12	1	Default organizatio					
00:31:25:fe:20:ee		Major	The terminal	Terminal:00:31:25:fe:	2022-08-12	1	Default organizatio					
cc:d8:1f:45:bf:a0		Major	The terminal	Terminal:cc:d8:1f:45:	2022-08-12	1	Default organizatio					
cc:d8:1f:21		Major	The	Terminal:c	2022-08-	1	Default					

Figure 11.1.8 Export the alarm event

Users can save their own filter criteria. After selecting the filter criteria in the interface, click the **Saving Conditions** button, and a pop-up box will appear. You need to fill in the condition name in the pop-up box, and then you can see it in selecting the filter template (see the following figure).

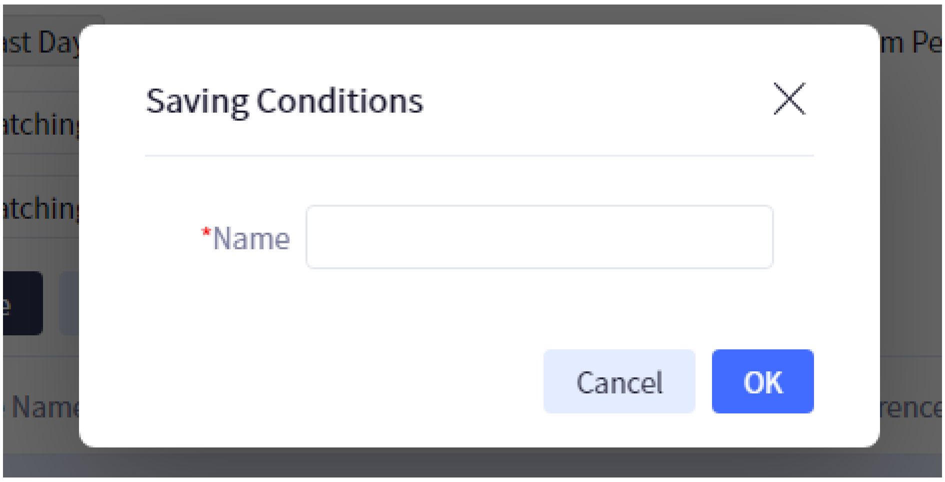
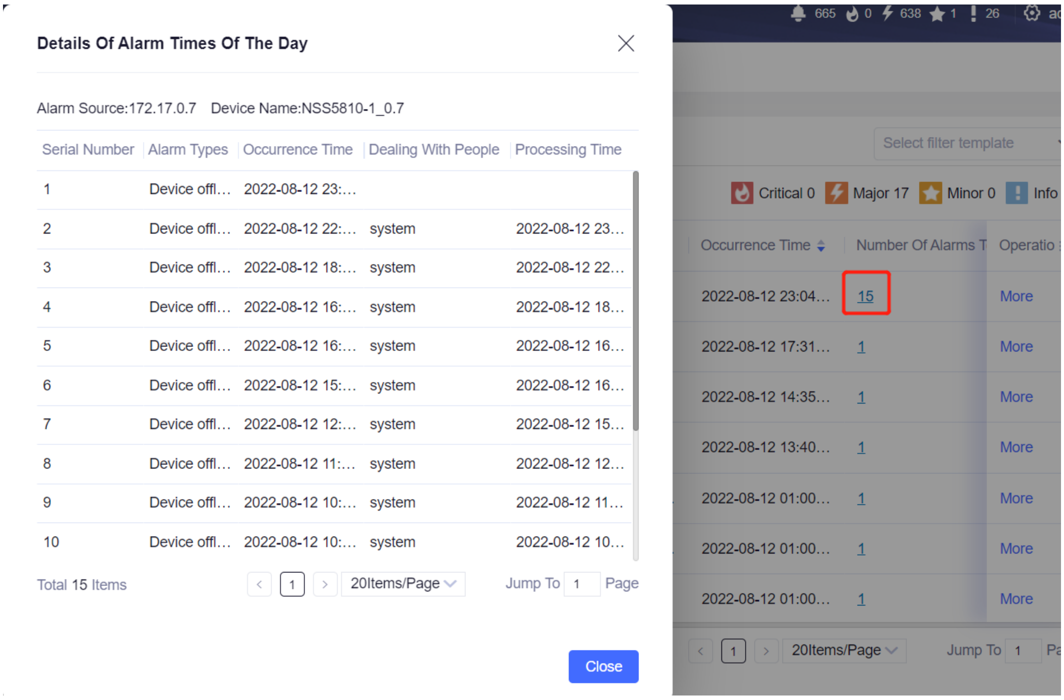


Figure 11.1.9 Save conditions

In addition, in the current alarms, the user can also view the repetition times of an alarm message. The number of alarms will not count the masked alarms.

The effect is shown in the figure.



Alarm Source:172.17.0.7 Device Name:NSS5810-1_0.7

Serial Number	Alarm Types	Occurrence Time	Dealing With People	Processing Time
1	Device offl…	2022-08-12 23:…		
2	Device offl…	2022-08-12 22:…	system	2022-08-12 23…
3	Device offl…	2022-08-12 18:…	system	2022-08-12 22…
4	Device offl…	2022-08-12 16:…	system	2022-08-12 18…
5	Device offl…	2022-08-12 16:…	system	2022-08-12 16…
6	Device offl…	2022-08-12 15:…	system	2022-08-12 16…
7	Device offl…	2022-08-12 12:…	system	2022-08-12 15…
8	Device offl…	2022-08-12 11:…	system	2022-08-12 12…
9	Device offl…	2022-08-12 10:…	system	2022-08-12 11…
10	Device offl…	2022-08-12 10:…	system	2022-08-12 10…

Total 15 Items 1 20Items/Page Jump To 1 Page

Occurrence Time	Number Of Alarms T	Operatio
2022-08-12 23:04…	15	More
2022-08-12 17:31…	1	More
2022-08-12 14:35…	1	More
2022-08-12 13:40…	1	More
2022-08-12 01:00…	1	More
2022-08-12 01:00…	1	More
2022-08-12 01:00…	1	More

1 20Items/Page Jump To 1 Pa

Figure 11.1.10 Alarm repetition times

Masked alarms

The masked alarm presents the masked alarm information to the user. On the **Masked Alarms** interface, users can accurately query by the alarm level and time, and can also fuzzy query by the alarm source, alarm type, organization and description. At the same time, users can also accurately query by the alarm type and alarm source. The effect is shown in the following figure.

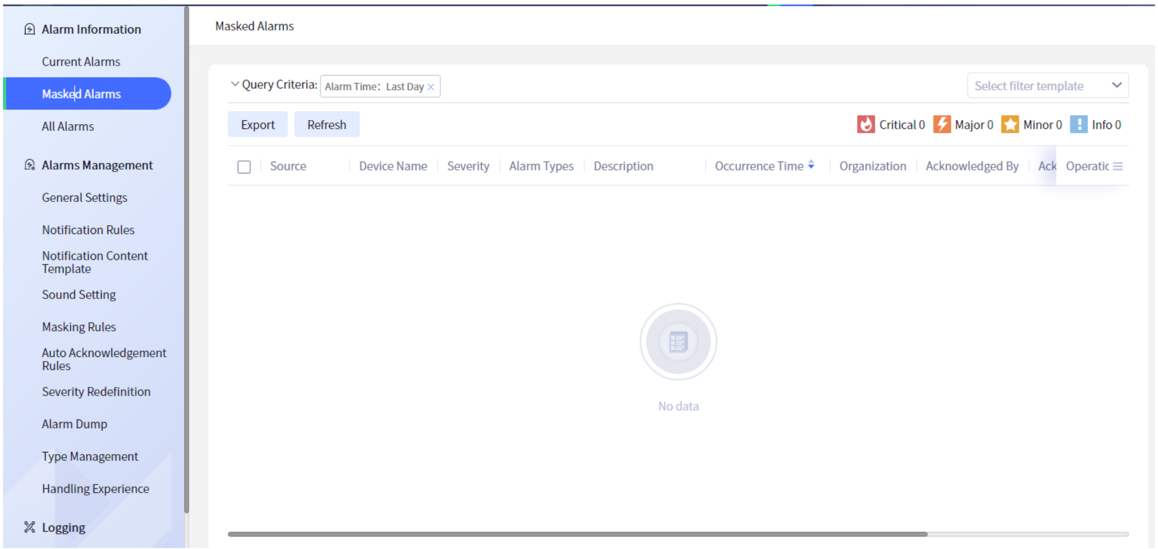
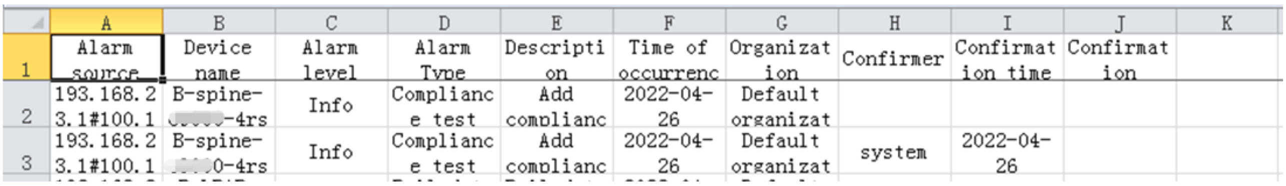


Figure 11.1.11 Masked alarms

After querying the desired masked alarm information, click the **Export** button, and you can export all masked alarm events (including paged masked alarm events) in the list.



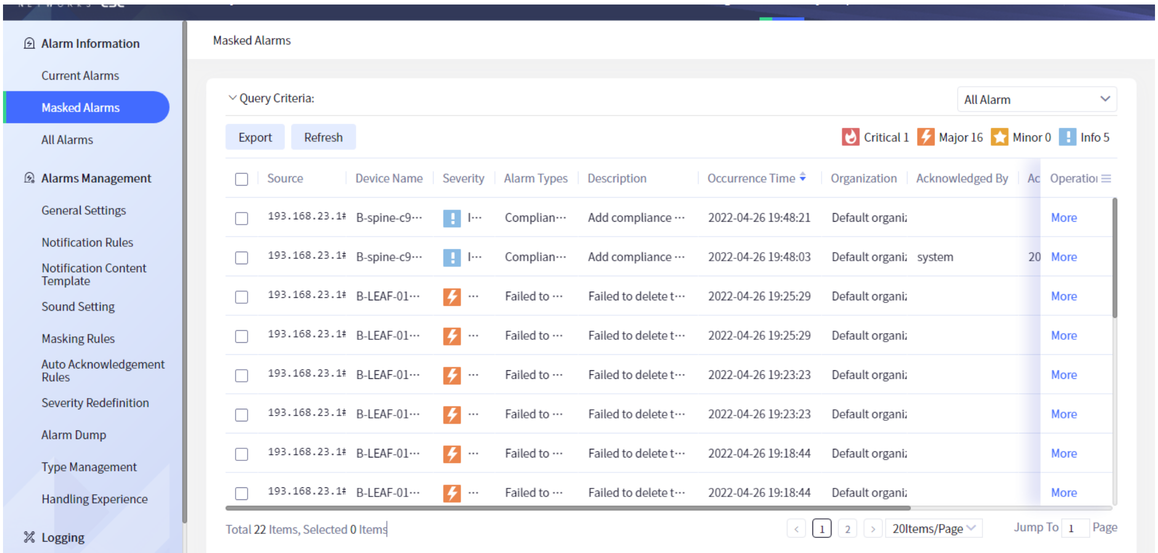
	A	B	C	D	E	F	G	H	I	J	K
1	Alarm source	Device name	Alarm level	Alarm Type	Description	Time of occurrence	Organization	Confirmer	Confirmation time	Confirmation	
2	193.168.23.1#100.1	B-spine-[redacted]-4rs	Info	Compliance test	Add complianc	2022-04-26	Default organizat				
3	193.168.23.1#100.1	B-spine-[redacted]0-4rs	Info	Compliance test	Add complianc	2022-04-26	Default organizat	system	2022-04-26		

Figure 11.1.12 Export masked alarm information

Similarly, the function of saving filter conditions is also supported on the **Masked Alarms** interface, and will not be repeated here.

All Alarms

The **All Alarms** module presents the current alarms, masked alarms, processed alarms, and auto recovery, auto processing, and duplicate cleared alarms to the user. The user can accurately query by the alarm level, processing status, confirmation status, masking status and alarm time on **All Alarms** interface, and can also fuzzy query by the alarm source, alarm type, affiliated organization and description. At the same time, the user can also accurately query by the alarm type and alarm source.

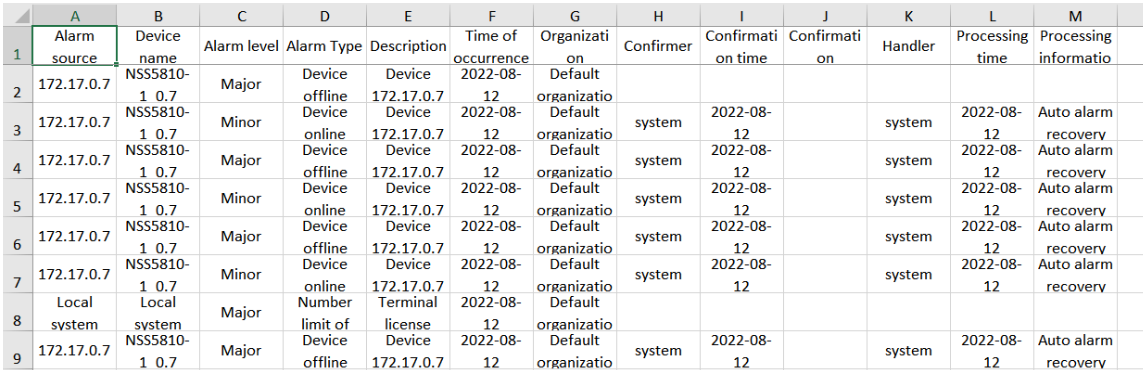


☐	Source	Device Name	Severity	Alarm Types	Description	Occurrence Time	Organization	Acknowledged By	Ac	Operatioı
☐	193.168.23.1‡	B-spine-c9···	! I···	Complian···	Add compliance ···	2022-04-26 19:48:21	Default organi:			More
☐	193.168.23.1‡	B-spine-c9···	! I···	Complian···	Add compliance ···	2022-04-26 19:48:03	Default organi:	system	20	More
☐	193.168.23.1‡	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	Default organi:			More
☐	193.168.23.1‡	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	Default organi:			More
☐	193.168.23.1‡	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	Default organi:			More
☐	193.168.23.1‡	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	Default organi:			More
☐	193.168.23.1‡	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:18:44	Default organi:			More
☐	193.168.23.1‡	B-LEAF-01···	⚡ ···	Failed to ···	Failed to delete t···	2022-04-26 19:18:44	Default organi:			More

Total 22 Items, Selected 0 Items

Figure 11.1.13 All alarms

After querying the desired alarm information, click the **Export** button, and you can export all alarm events (including paged alarm events) in the list.

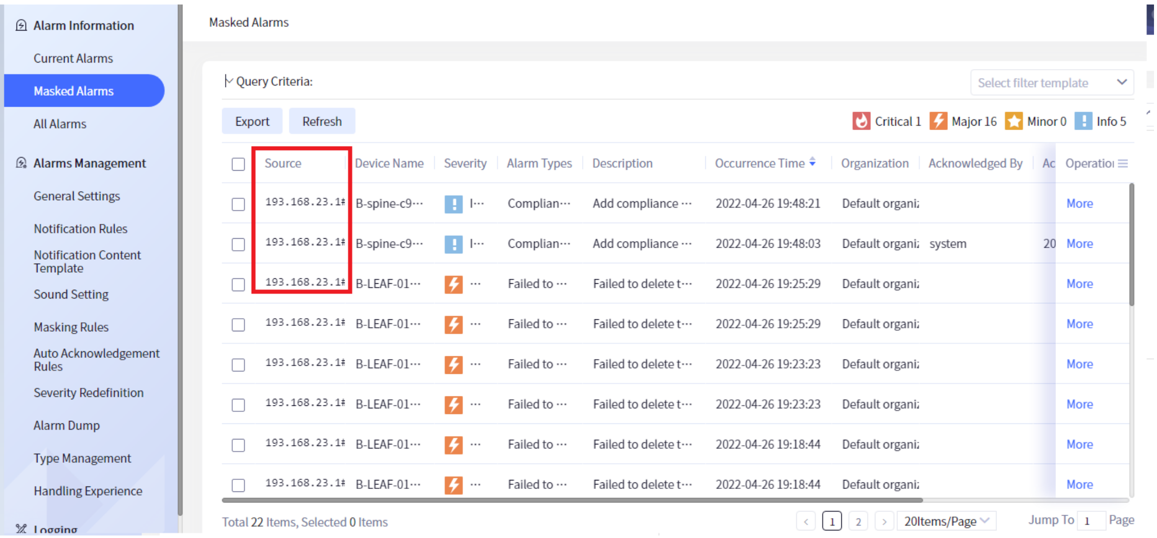


	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Alarm source	Device name	Alarm level	Alarm Type	Description	Time of occurrence	Organization	Confirmer	Confirmation time	Confirmation	Handler	Processing time	Processing informatio
2	172.17.0.7	NSS5810-1 0.7	Major	Device offline	Device 172.17.0.7	2022-08-12	Default organizatio						
3	172.17.0.7	NSS5810-1 0.7	Minor	Device online	Device 172.17.0.7	2022-08-12	Default organizatio	system	2022-08-12		system	2022-08-12	Auto alarm recovery
4	172.17.0.7	NSS5810-1 0.7	Major	Device offline	Device 172.17.0.7	2022-08-12	Default organizatio	system	2022-08-12		system	2022-08-12	Auto alarm recovery
5	172.17.0.7	NSS5810-1 0.7	Minor	Device online	Device 172.17.0.7	2022-08-12	Default organizatio	system	2022-08-12		system	2022-08-12	Auto alarm recovery
6	172.17.0.7	NSS5810-1 0.7	Major	Device offline	Device 172.17.0.7	2022-08-12	Default organizatio	system	2022-08-12		system	2022-08-12	Auto alarm recovery
7	172.17.0.7	NSS5810-1 0.7	Minor	Device online	Device 172.17.0.7	2022-08-12	Default organizatio	system	2022-08-12		system	2022-08-12	Auto alarm recovery
8	Local system	Local system	Major	Number limit of	Terminal license	2022-08-12	Default organizatio						
9	172.17.0.7	NSS5810-1 0.7	Major	Device offline	Device 172.17.0.7	2022-08-12	Default organizatio	system	2022-08-12		system	2022-08-12	Auto alarm recovery

Figure 11.1.14 Export all alarm information

The function of saving filter conditions is also supported on the **All Alarms** interface, and will not be repeated here.

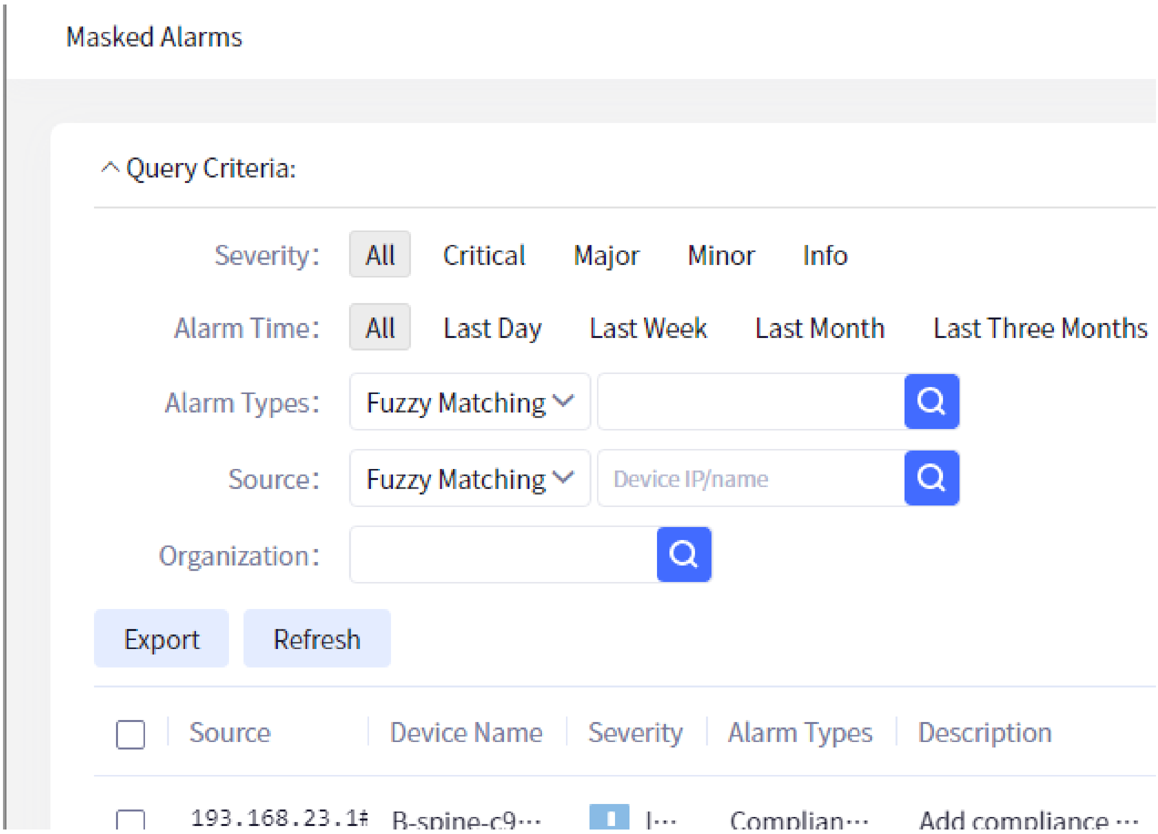
Current alarms, masked alarms and all alarms support clicking the alarm source IP to view all alarm information generated by the alarm source; Click the alarm level statistics icon to view the alarm information of all the same alarm levels. The effect is shown in the figure.



☐	Source	Device Name	Severity	Alarm Types	Description	Occurrence Time	Organization	Acknowledged By	Ac	Operatio
☐	193.168.23.1	B-spine-c9···	! I···	Complian···	Add compliance ···	2022-04-26 19:48:21	Default organi:			More
☐	193.168.23.1	B-spine-c9···	! I···	Complian···	Add compliance ···	2022-04-26 19:48:03	Default organi:	system	20	More
☐	193.168.23.1	B-LEAF-01···	ϟ ···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	Default organi:			More
☐	193.168.23.1	B-LEAF-01···	ϟ ···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	Default organi:			More
☐	193.168.23.1	B-LEAF-01···	ϟ ···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	Default organi:			More
☐	193.168.23.1	B-LEAF-01···	ϟ ···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	Default organi:			More
☐	193.168.23.1	B-LEAF-01···	ϟ ···	Failed to ···	Failed to delete t···	2022-04-26 19:18:44	Default organi:			More
☐	193.168.23.1	B-LEAF-01···	ϟ ···	Failed to ···	Failed to delete t···	2022-04-26 19:18:44	Default organi:			More

Total 22 Items, Selected 0 Items

Figure 11.1.15 Query by alarm source



Masked Alarms

Query Criteria:

Severity: All | Critical | Major | Minor | Info

Alarm Time: All | Last Day | Last Week | Last Month | Last Three Months

Alarm Types: Fuzzy Matching

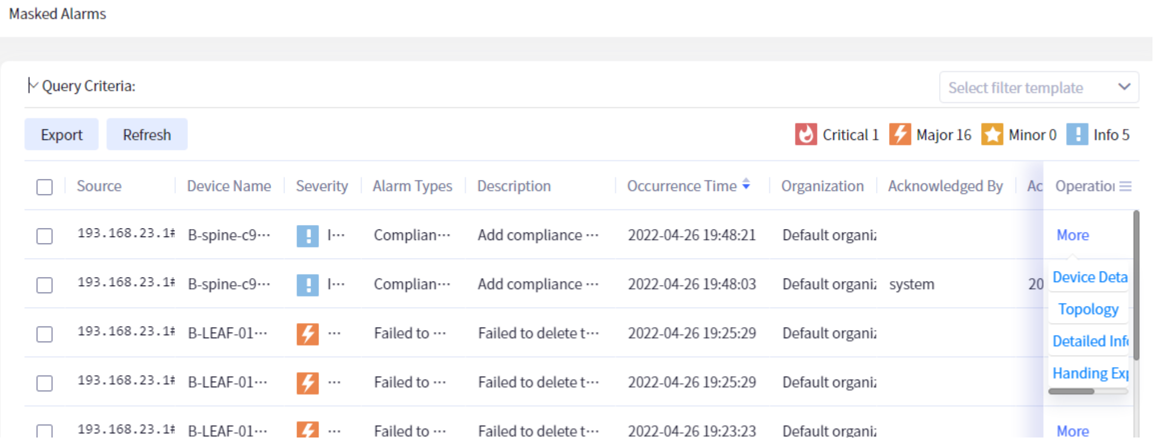
Source: Fuzzy Matching | Device IP/name

Organization:

☐	Source	Device Name	Severity	Alarm Types	Description
☐	193.168.23.1#	B-spine-c9···	I···	Complian···	Add compliance ···

Figure 11.1.16 Query by alarm level

In the current alarms, masked alarms and all alarms, **Locate to Device** supports jumping to topology and **Locate to Topology**, and the effect is shown in the figure.



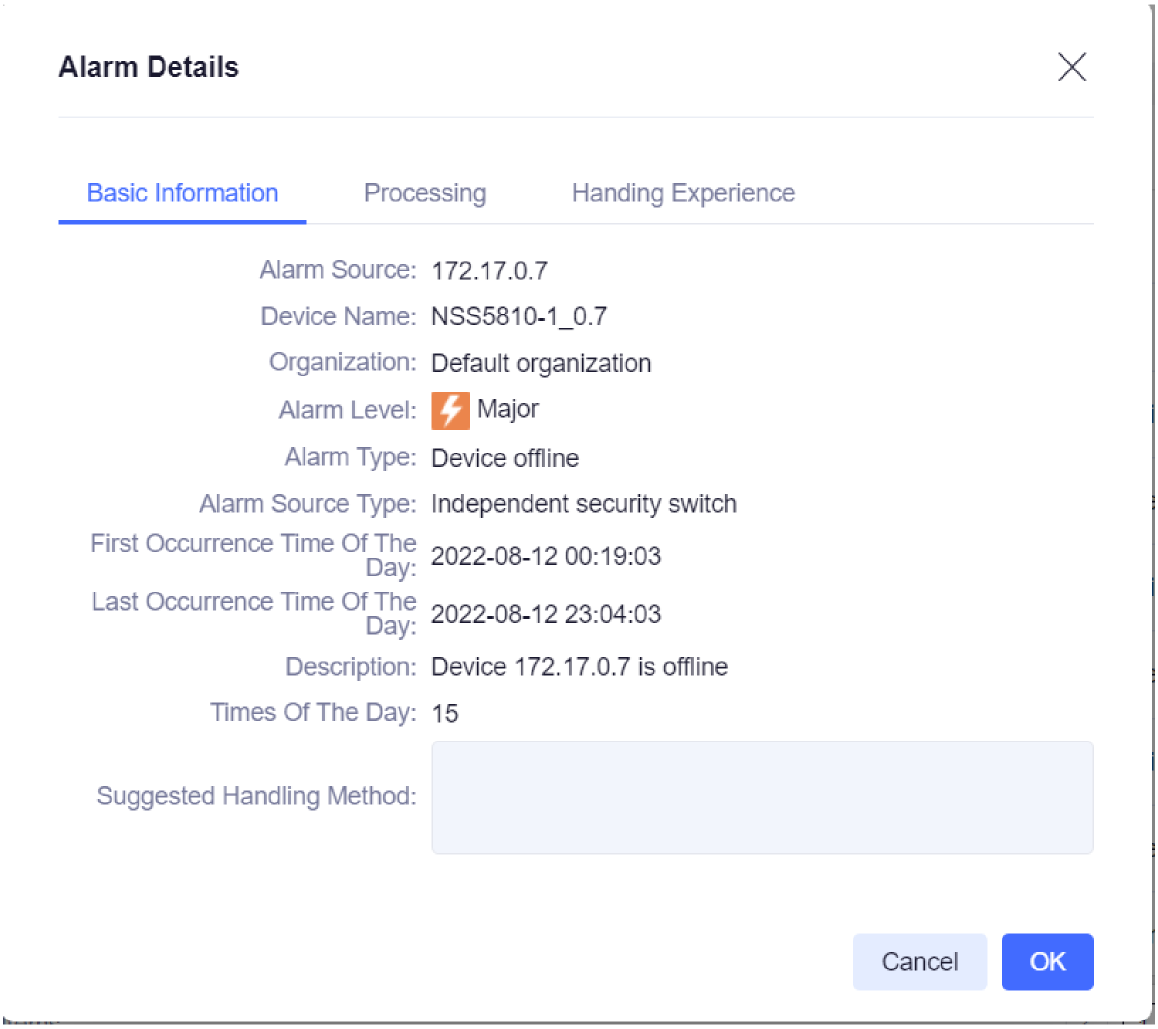
Masked Alarms

Query Criteria:

☐	Source	Device Name	Severity	Alarm Types	Description	Occurrence Time	Organization	Acknowledged By	Ac	Operatio
☐	193.168.23.1#	B-spine-c9···	I···	Complian···	Add compliance ···	2022-04-26 19:48:21	Default organi:			More
☐	193.168.23.1#	B-spine-c9···	I···	Complian···	Add compliance ···	2022-04-26 19:48:03	Default organi:	system	20	Device Deta Topology Detailed Inf Handing Ex
☐	193.168.23.1#	B-LEAF-01···	···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	Default organi:			
☐	193.168.23.1#	B-LEAF-01···	···	Failed to ···	Failed to delete t···	2022-04-26 19:25:29	Default organi:			
☐	193.168.23.1#	B-LEAF-01···	···	Failed to ···	Failed to delete t···	2022-04-26 19:23:23	Default organi:			More

Figure 11.1.17 Locate to the device and topology

In the current alarms, masked alarms and all alarms, you can view the alarm **Details**, and the effect is shown in the figure.



Alarm Source: 172.17.0.7
Device Name: NSS5810-1_0.7
Organization: Default organization
Alarm Level: ⚡ Major
Alarm Type: Device offline
Alarm Source Type: Independent security switch
First Occurrence Time Of The Day: 2022-08-12 00:19:03
Last Occurrence Time Of The Day: 2022-08-12 23:04:03
Description: Device 172.17.0.7 is offline
Times Of The Day: 15
Suggested Handling Method:

Figure 11.1.18 Alarm details information

In the current alarms, masked alarms and all alarms, support adding alarm maintenance experience for alarms. The effect is shown in the figure.

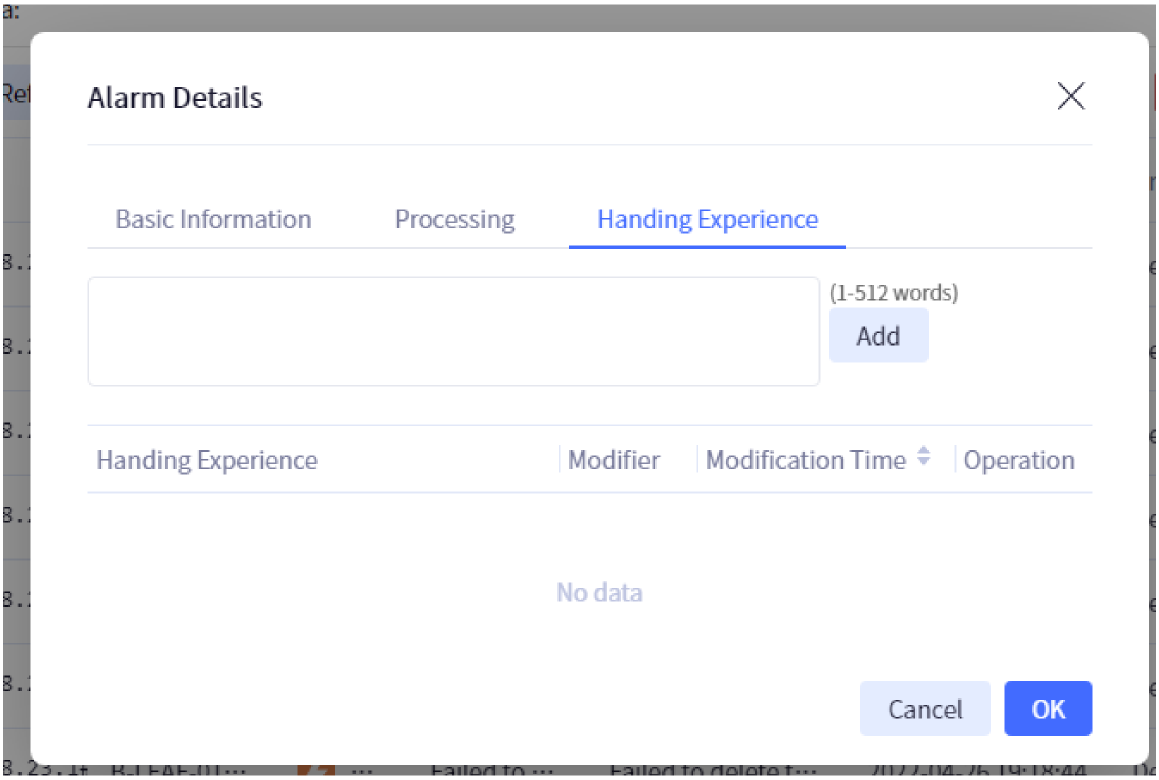


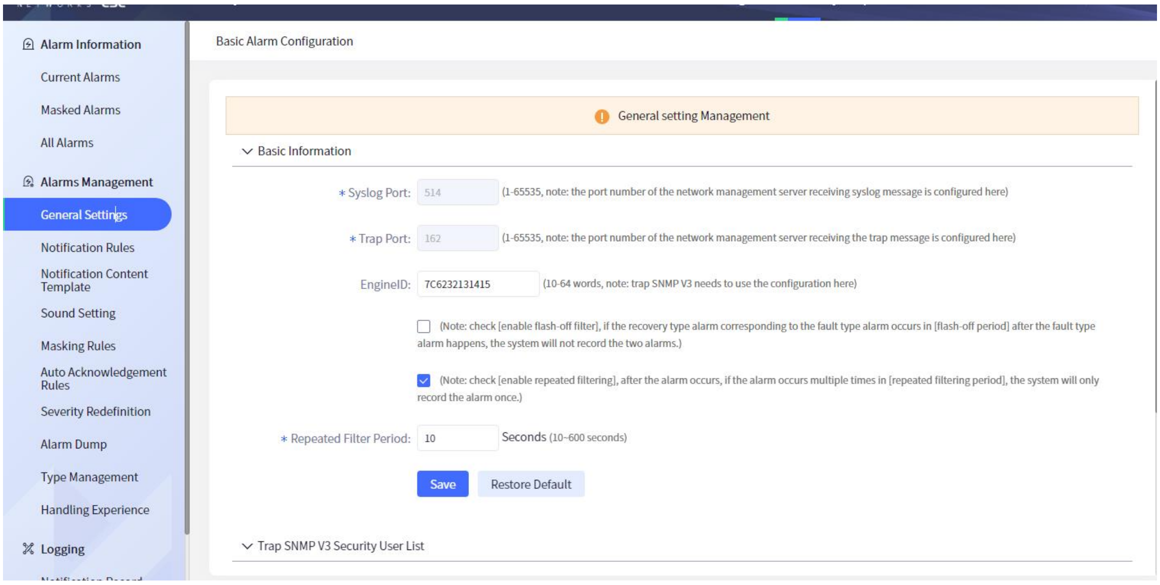
Figure 11.1.19 Add alarm maintenance experiences

Note

- In the current alarms, masked alarms and all alarms, do not support the function of locating the alarm information whose device name is the local system to the device and to the topology.
- After the device adds an interface, the alarm generated when the device does not refresh this interface can only be queried by the interface information and alarm description information, but cannot be accurately queried through the interface.

11.2 Alarm Configuration

Click "Alerts&Activity" in the menu bar to open the "Basic Alarm Configuration" page. The left navigation of the "Basic Alarm Configuration" interface includes general settings, alarm notification rules, notification content template, sound setting, masking rules, auto acknowledge rules, severity redefinition, alarm dump, type management and handling experience. The results are shown in the figure.



∗ Syslog Port: 514 (1-65535, note: the port number of the network management server receiving syslog message is configured here)

∗ Trap Port: 162 (1-65535, note: the port number of the network management server receiving the trap message is configured here)

EngineID: 7C6232131415 (10-64 words, note: trap SNMP V3 needs to use the configuration here)

☐ (Note: check [enable flash-off filter], if the recovery type alarm corresponding to the fault type alarm occurs in [flash-off period] after the fault type alarm happens, the system will not record the two alarms.)

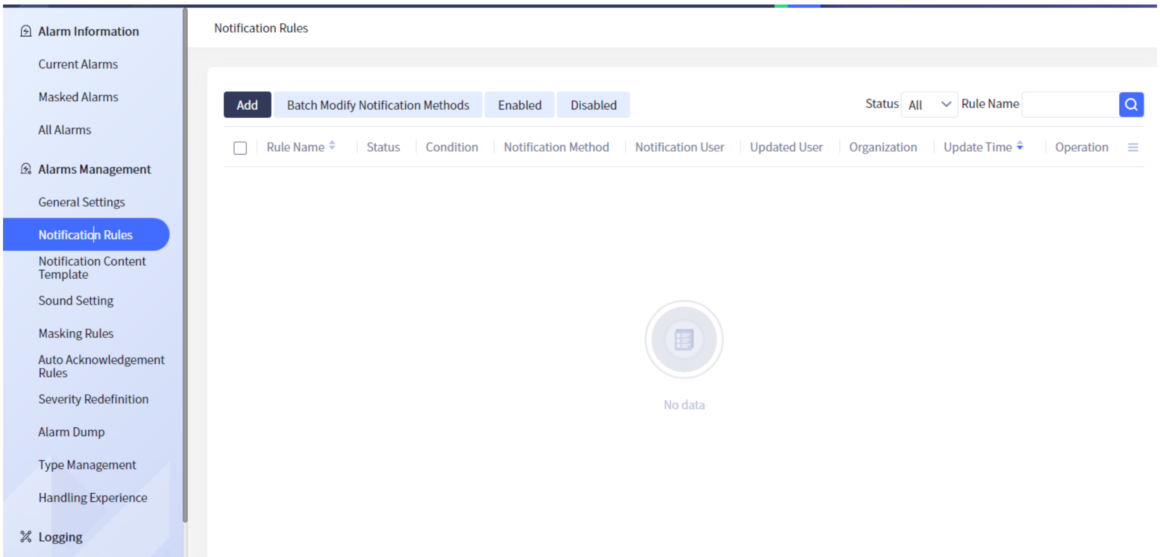
☑ (Note: check [enable repeated filtering], after the alarm occurs, if the alarm occurs multiple times in [repeated filtering period], the system will only record the alarm once.)

∗ Repeated Filter Period: 10 Seconds (10~600 seconds)

Figure 11.2.1 Alarm configuration

11.2.1 Alarm Notification Rules

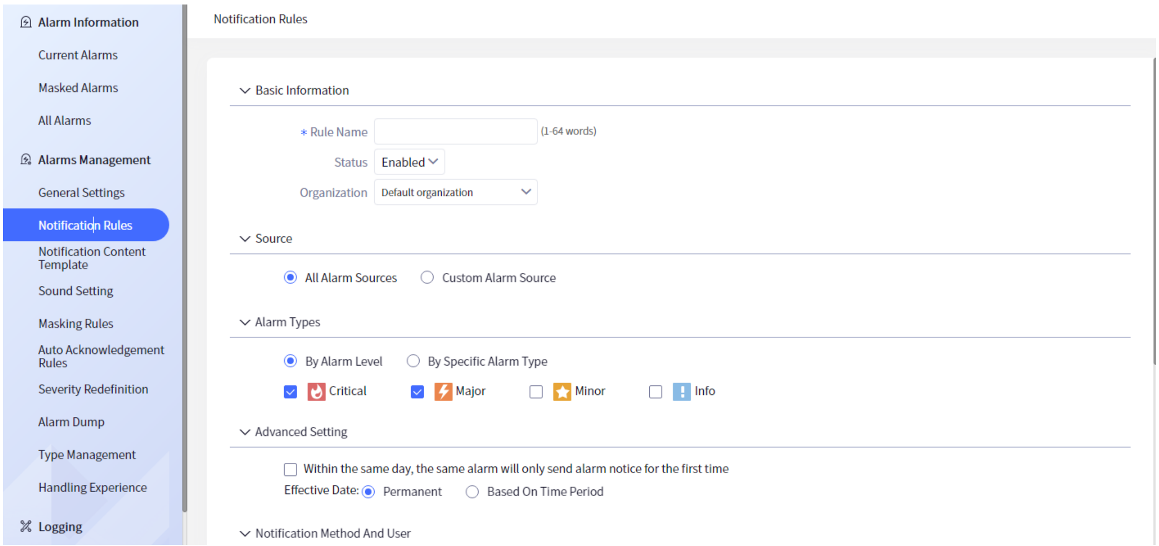
Alarm notification rules are used to configure alarm information to be notified to users by email, SMS and voice. The alarm information of which alarm source or type can be configured, and which notification method can be used to notify the user. In the **Notification Rules** interface, the user can query the notification rules vaguely through the rule name, and can also query the notification rules accurately for the enabling status. The effect is shown in the figure.



☐	Rule Name	Status	Condition	Notification Method	Notification User	Updated User	Organization	Update Time	Operation

Figure 11.2.1.1 Alarm notification rules

The user can click the **Add** button to add one alarm notification rule, and the effect is as follows:



Notification Rules

Basic Information

* Rule Name (1-64 words)

Status: Enabled

Organization: Default organization

Source

● All Alarm Sources ○ Custom Alarm Source

Alarm Types

● By Alarm Level ○ By Specific Alarm Type

☑ Critical ☑ Major ☐ Minor ☐ Info

Advanced Setting

☐ Within the same day, the same alarm will only send alarm notice for the first time

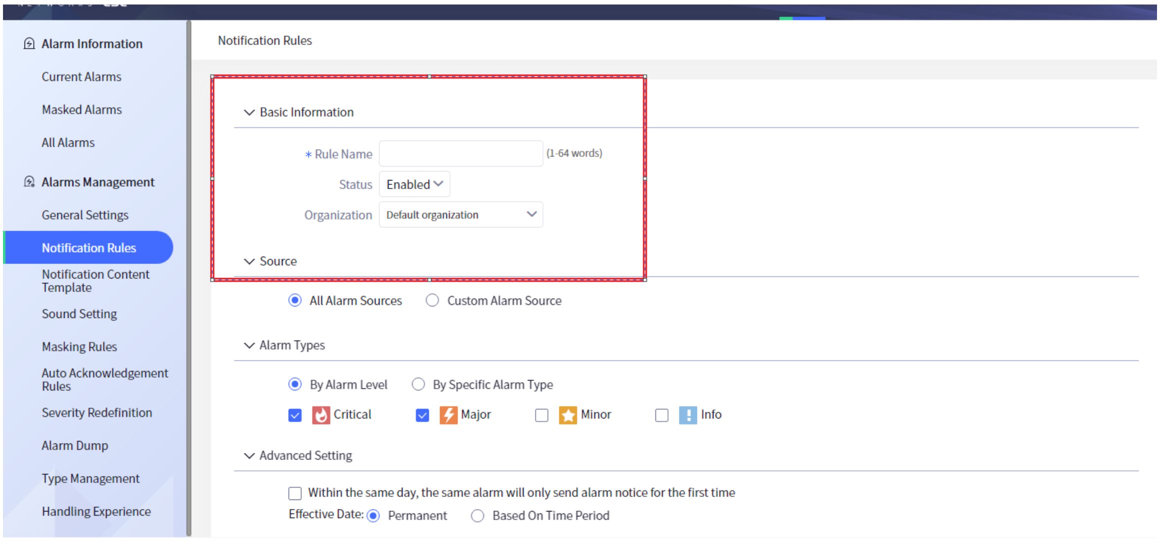
Effective Date: ● Permanent ○ Based On Time Period

Notification Method And User

Figure 12.2.1.2 Add alarm notification rules

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 of the rule (the alarm notification rule configured by the lower level can only be seen by the administrators at the same level and the upper level). The effect is shown in the figure.



Notification Rules

Basic Information

* Rule Name (1-64 words)

Status: Enabled

Organization: Default organization

Source

● All Alarm Sources ○ Custom Alarm Source

Alarm Types

● By Alarm Level ○ By Specific Alarm Type

☑ Critical ☑ Major ☐ Minor ☐ Info

Advanced Setting

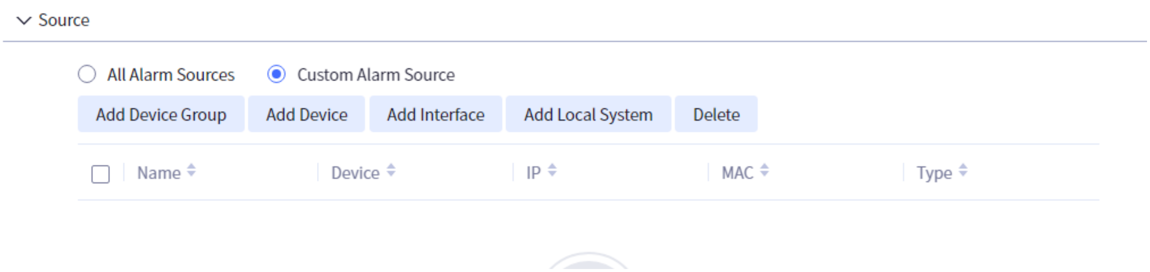
☐ Within the same day, the same alarm will only send alarm notice for the first time

Effective Date: ● Permanent ○ Based On Time Period

Figure 11.2.1.3 Configure the basic information 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 subordinate 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 current level and subordinate organizations will send alarm notifications. 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 the **Custom Alarm Source** button to select a specific alarm source. The effect is shown in the figure.



Source

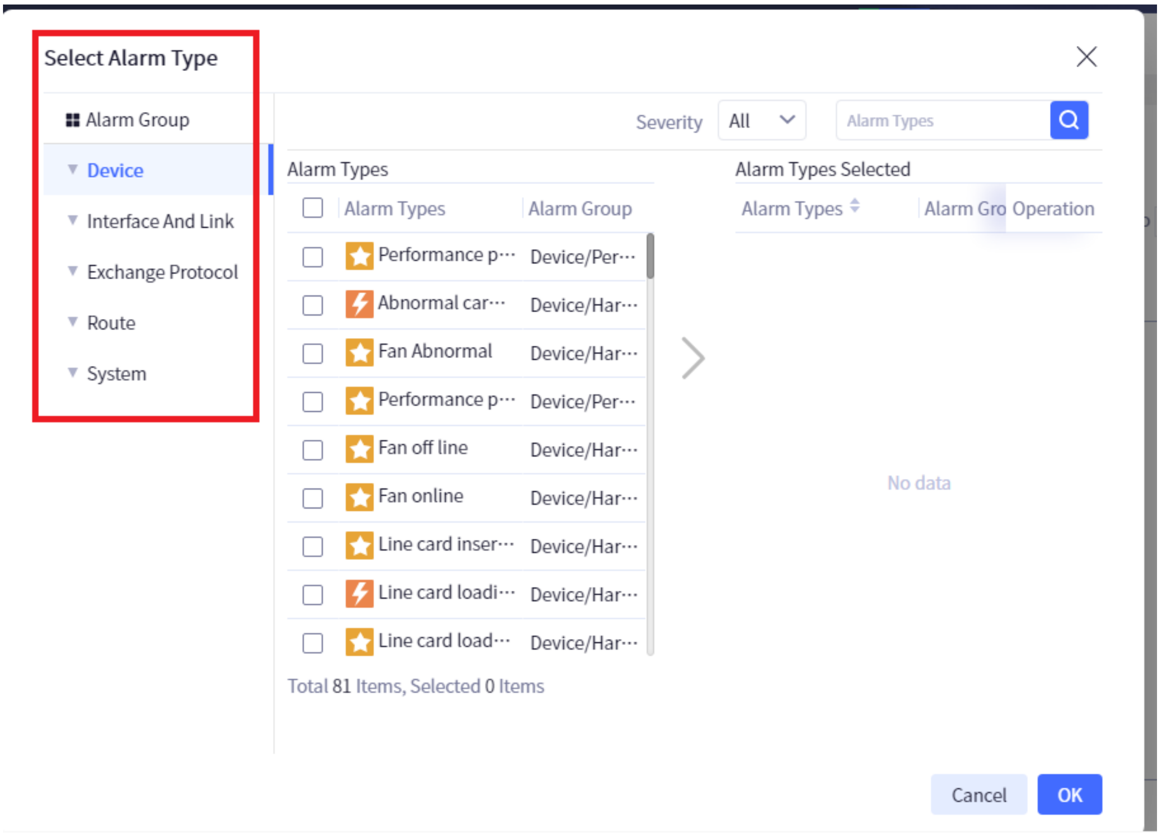
○ All Alarm Sources ● Custom Alarm Source

☐	Name	Device	IP	MAC	Type

Figure 11.2.1.4 Configure alarm source

Alarm type management:

Alarm type management is used to determine which type of alarm information needs to be notified. 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 you select a specific alarm type, a list will appear. Click "Add Alarm Type" to customize the specific alarm type. The effect is shown in the figure.



Select Alarm Type

Severity All

Alarm Types

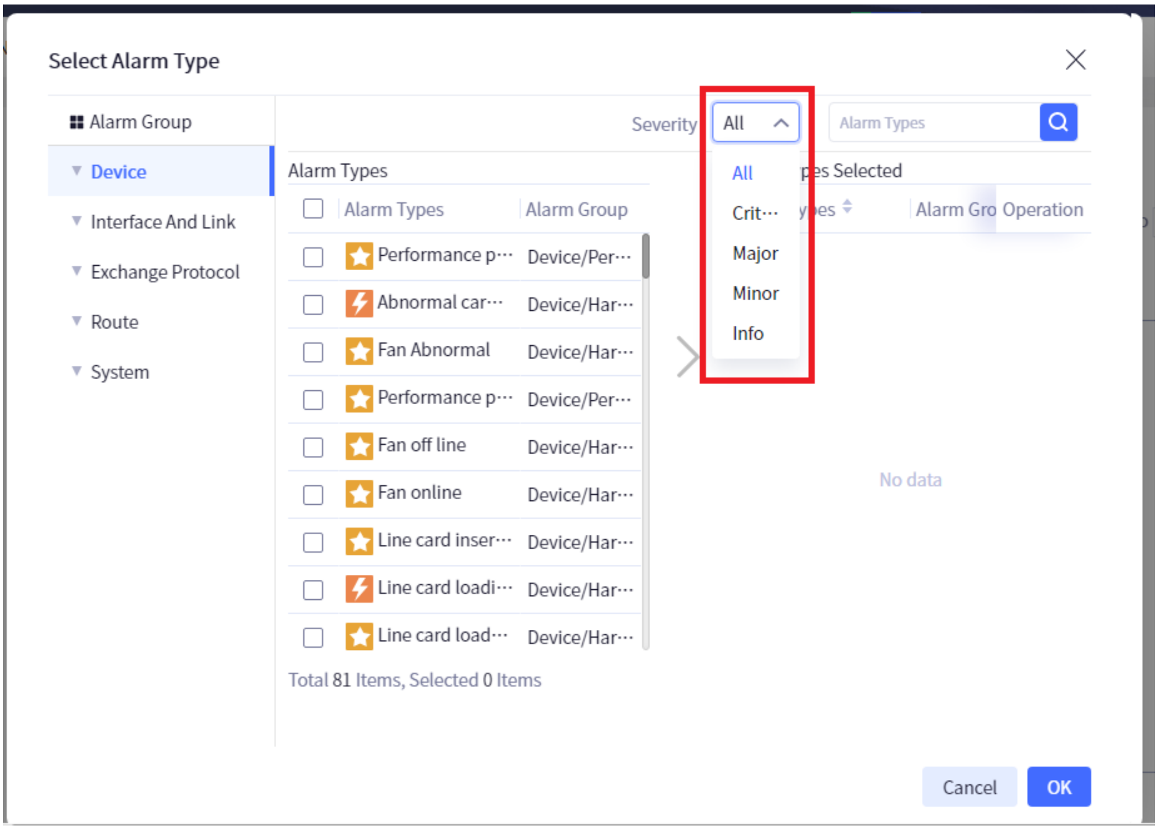
☐	Alarm Types	Alarm Group
☐	Performance p···	Device/Per···
☐	Abnormal car···	Device/Har···
☐	Fan Abnormal	Device/Har···
☐	Performance p···	Device/Per···
☐	Fan off line	Device/Har···
☐	Fan online	Device/Har···
☐	Line card inser···	Device/Har···
☐	Line card loadi···	Device/Har···
☐	Line card load···	Device/Har···

Total 81 Items, Selected 0 Items

Alarm Types Selected

Alarm Types	Alarm Gro	Operation

No data



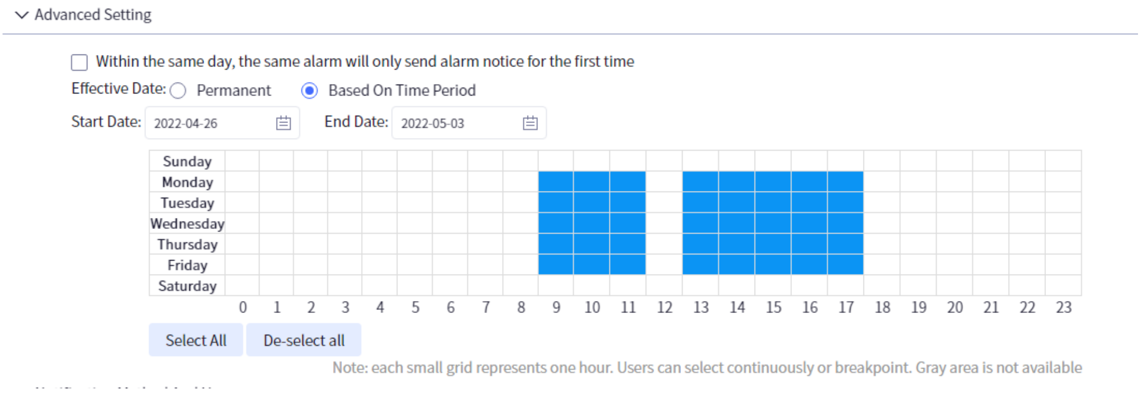
☐	Alarm Types	Alarm Group
☐	Performance p···	Device/Per···
☐	Abnormal car···	Device/Har···
☐	Fan Abnormal	Device/Har···
☐	Performance p···	Device/Per···
☐	Fan off line	Device/Har···
☐	Fan online	Device/Har···
☐	Line card inser···	Device/Har···
☐	Line card loadi···	Device/Har···
☐	Line card load···	Device/Har···

Total 81 Items, Selected 0 Items

Figure 11.2.1.5 Configure alarm type

Advanced configuration:

The advanced configuration includes two configurations, namely, in the same day, the same alarm will only send the alarm notice for the first time and the effective date of the rule. The effective date includes permanent and based on time period. If you select **Based On Time Period**, a time list will appear. You can select a time in the time list (the vertical coordinate represents the date, and the horizontal coordinate represents the time scale). The effect is as shown in the figure.



☐ Within the same day, the same alarm will only send alarm notice for the first time

Effective Date: ○ Permanent ● Based On Time Period

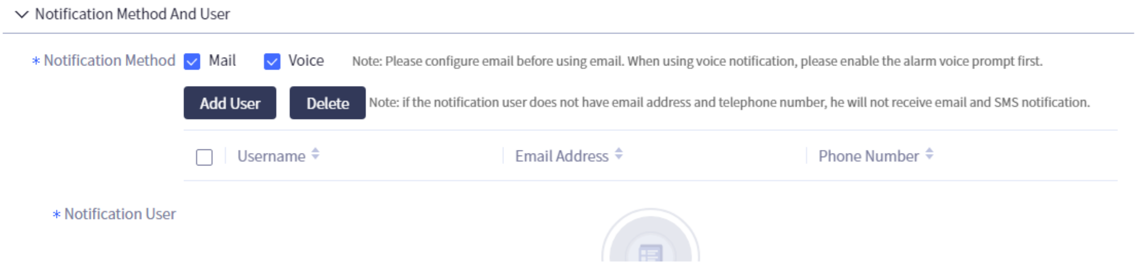
Start Date: 2022-04-26 End Date: 2022-05-03

Note: each small grid represents one hour. Users can select continuously or breakpoint. Gray area is not available

Figure 11.2.1.6 Advanced configuration

Notification method and user:

Notification methods include email, SMS and voice. If SMS is selected, a SMS Gateway must be selected. The gateway user can click the button to select the user to be notified (the user can only select the users of the current level and subordinate organizations of the organization to which the rule belongs, and the user must have the authorities of the alarm source before sending the alarm notification). The effect is shown in the figure.

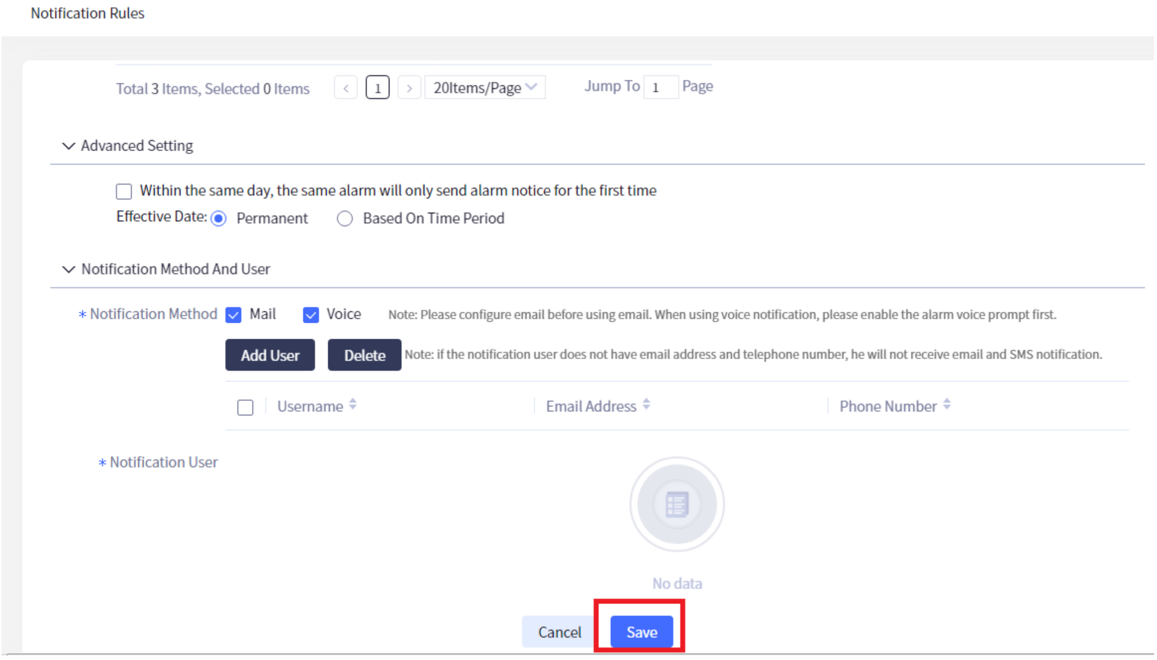


Note: Please configure email before using email. When using voice notification, please enable the alarm voice prompt first.

Note: if the notification user does not have email address and telephone number, he will not receive email and SMS notification.

Figure 11.2.1.7 Configure notification mode and user

Users can modify the alarm notification rules. Select an alarm notification rule and click **Modify**. The basic information can only be modified to the enabled status, but the alarm source, alarm type, advanced settings, notification method and user can all be modified. After modification, click the **Save** button, and the effect is shown in the figure.



☐ Within the same day, the same alarm will only send alarm notice for the first time

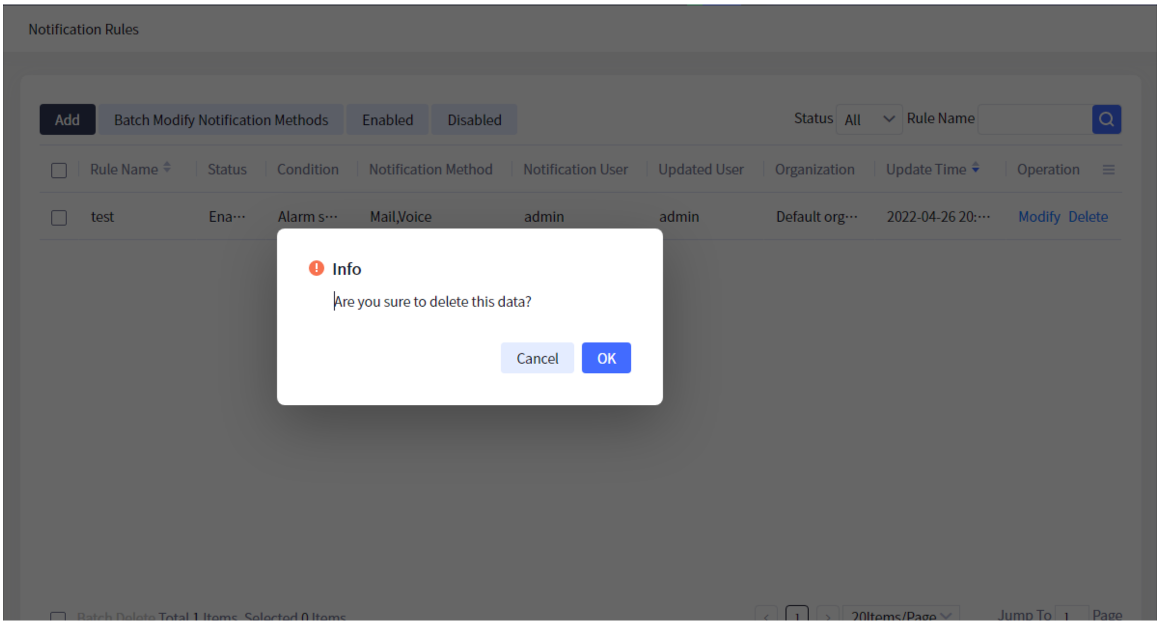
Effective Date: ● Permanent ○ Based On Time Period

Note: Please configure email before using email. When using voice notification, please enable the alarm voice prompt first.

Note: if the notification user does not have email address and telephone number, he will not receive email and SMS notification.

Figure 11.2.1.8 Modify alarm notification rules

Users can delete alarm notification rules. Select an alarm notification rule and click **Delete** to display a prompt box. Then click **OK** in the prompt box. The effect is as shown in the figure.



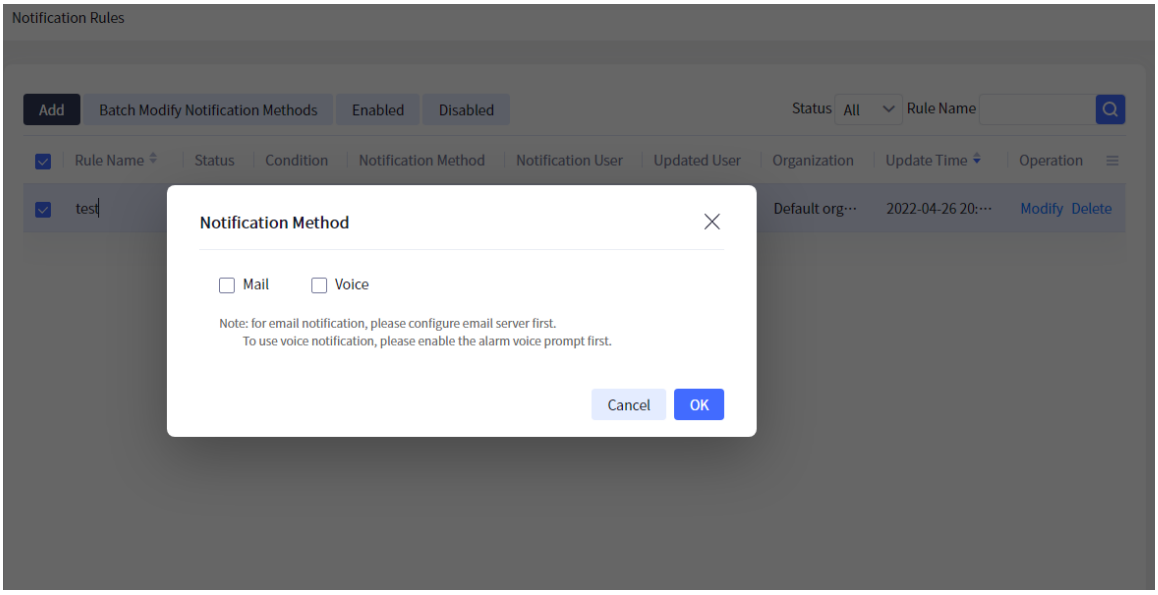
☐	Rule Name	Status	Condition	Notification Method	Notification User	Updated User	Organization	Update Time	Operation
☐	test	Ena···	Alarm s···	Mail,Voice	admin	admin	Default org···	2022-04-26 20:···	Modify Delete

Are you sure to delete this data?

Total 1 Items, Selected 0 Items

Figure 11.2.1.9 Delete the alarm notification rule

The user can modify the alarm notification rules in batch. The user can select one or more alarm notification rules, and then click the button **Batch Modify Notification Methods** to open the **Notification Method** dialog box. The user selects the appropriate notification method in the dialog box, and then click the **OK** button. The effect is shown in the figure.



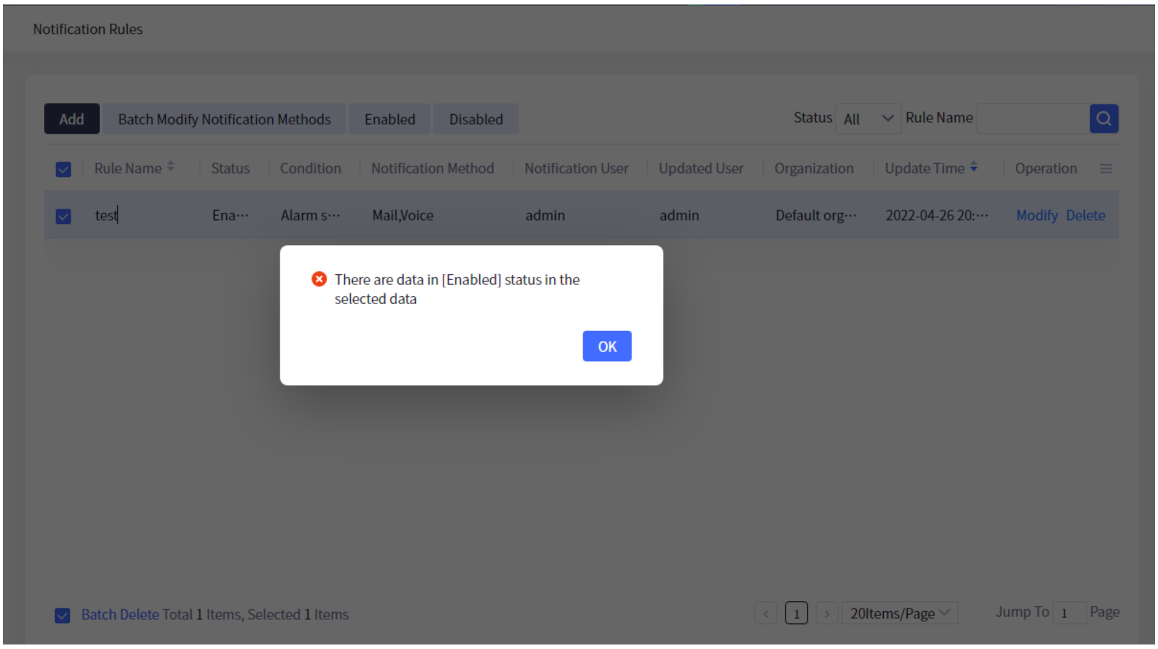
☑	Rule Name	Status	Condition	Notification Method	Notification User	Updated User	Organization	Update Time	Operation
☑	test						Default org···	2022-04-26 20:···	Modify Delete

☐ Mail ☐ Voice

Note: for email notification, please configure email server first.
To use voice notification, please enable the alarm voice prompt first.

Figure 11.2.1.10 Batch modify notification methods

Users can enable alarm notification rules (support batch operation). The user can select one or more alarm notification rules (only in disabled state) on the interface, then click **Enabled** to open a dialog box, and then click **OK** on the dialog box. The effect is shown in the figure.



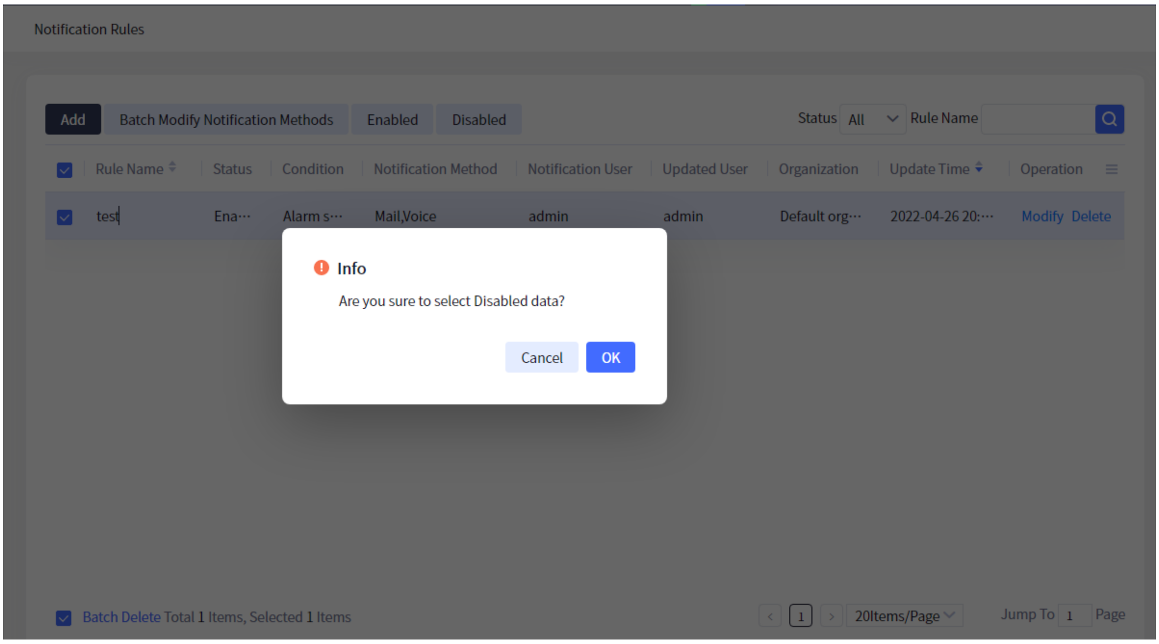
☑	Rule Name	Status	Condition	Notification Method	Notification User	Updated User	Organization	Update Time	Operation
☑	test	Ena···	Alarm s···	Mail,Voice	admin	admin	Default org···	2022-04-26 20:···	Modify Delete

There are data in [Enabled] status in the selected data

☑ Batch Delete Total 1 Items, Selected 1 Items

Figure 11.2.1.11 Enable alarm notification rules

You can disable the alarm notification rule (support batch operation). The user can select one or more alarm notification rules (only in enabled state) on the interface, then click **Disabled** to open a dialog box, and then click **OK** on the dialog box. The effect is shown in the figure.



☑	Rule Name	Status	Condition	Notification Method	Notification User	Updated User	Organization	Update Time	Operation
☑	test	Ena···	Alarm s···	Mail,Voice	admin	admin	Default org···	2022-04-26 20:···	Modify Delete

Info

Are you sure to select Disabled data?

Total 1 Items, Selected 1 Items

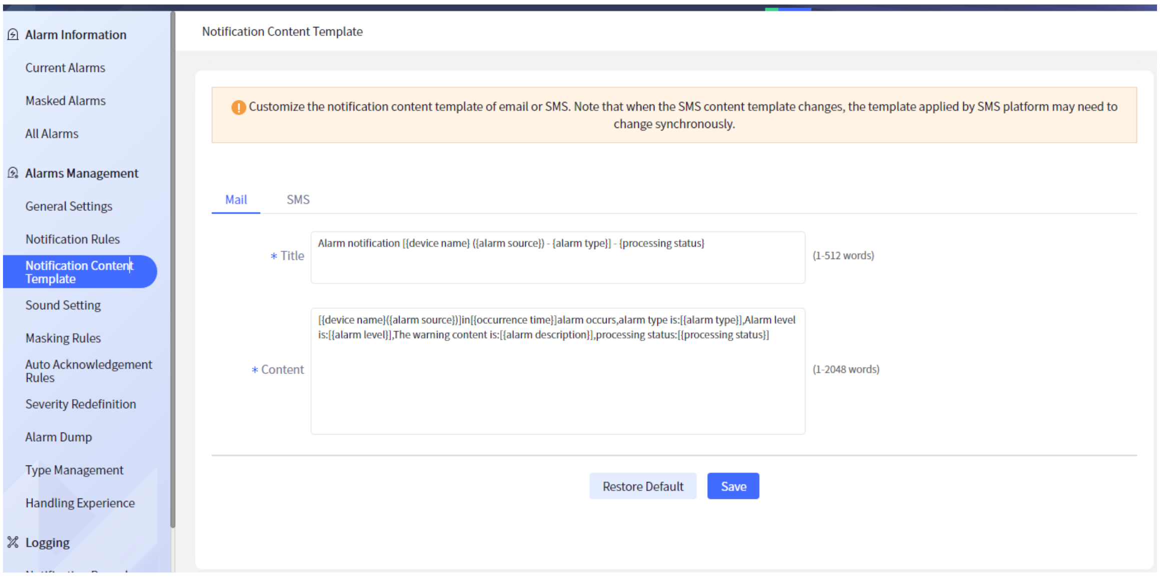
Figure 11.2.1.12 Disable the alarm notification rule

Note

- In an alarm push period (3 seconds), only one round of the highest level sound will be played.
- The email and SMS notification information and notification status (success or failure) can be viewed in the alarm notification record.
- Mail sending requires the correct mail server to be configured.
- The sound notification takes effect only when it is enabled in the alarm sound configuration.
- Rules cannot be disabled and enabled repeatedly.
- Mailbox and mobile number must be configured. Otherwise, there will be no notification record.

11.2.2 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 the development of content templates for e-mail and SMS. The left side of the tab is email and the right side is SMS. The effect is shown in the figure.



Customize the notification content template of email or SMS. Note that when the SMS content template changes, the template applied by SMS platform may need to change synchronously.

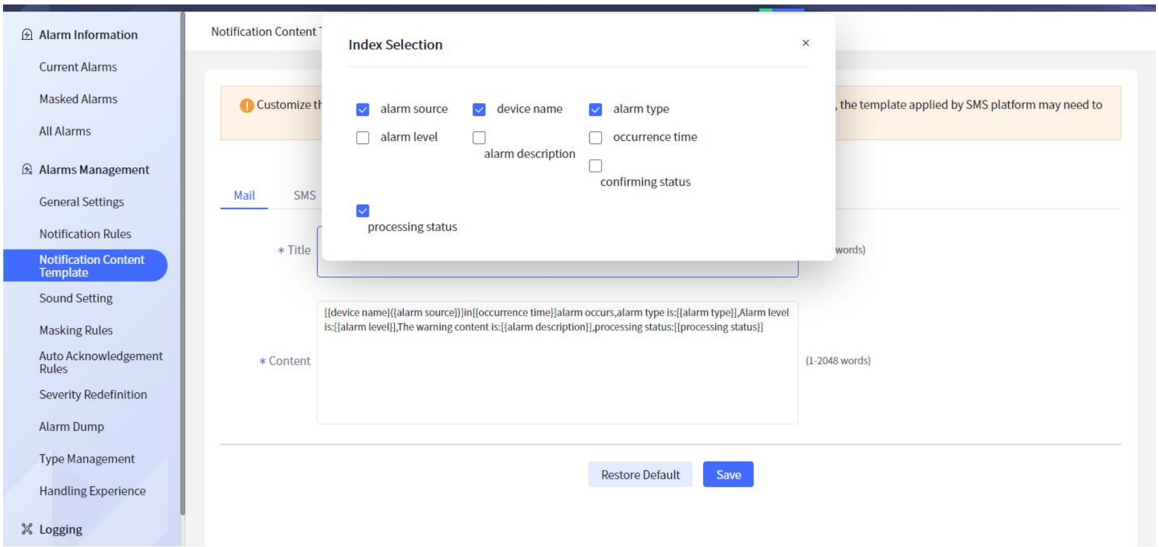
* Title: Alarm notification [{device name} ({alarm source}) - {alarm type}] - {processing status} (1-512 words)

* Content: [{device name}({alarm source})]in[{occurrence time}]alarm occurs,alarm type is:[{alarm type}],Alarm level is:[{alarm level}],The warning content is:[{alarm description}],processing status:[{processing status}] (1-2048 words)

Figure 11.2.2.1 Notification content template

Mail:

Users can make templates for mail. When the user clicks the edit box, a dialog box will appear. The user can select the required options in the dialog box or remove the unnecessary options. At the same time, users can fill in the title manually by filling in the title edit box. The email content is the same as the email title. You can also select the content. At the same time, you can also enter it manually. After selecting it, click **Save**. The effect is shown in the figure.



☑ alarm source ☑ device name ☑ alarm type
☐ alarm level ☐ alarm description ☐ occurrence time
☐ confirming status
☑ processing status

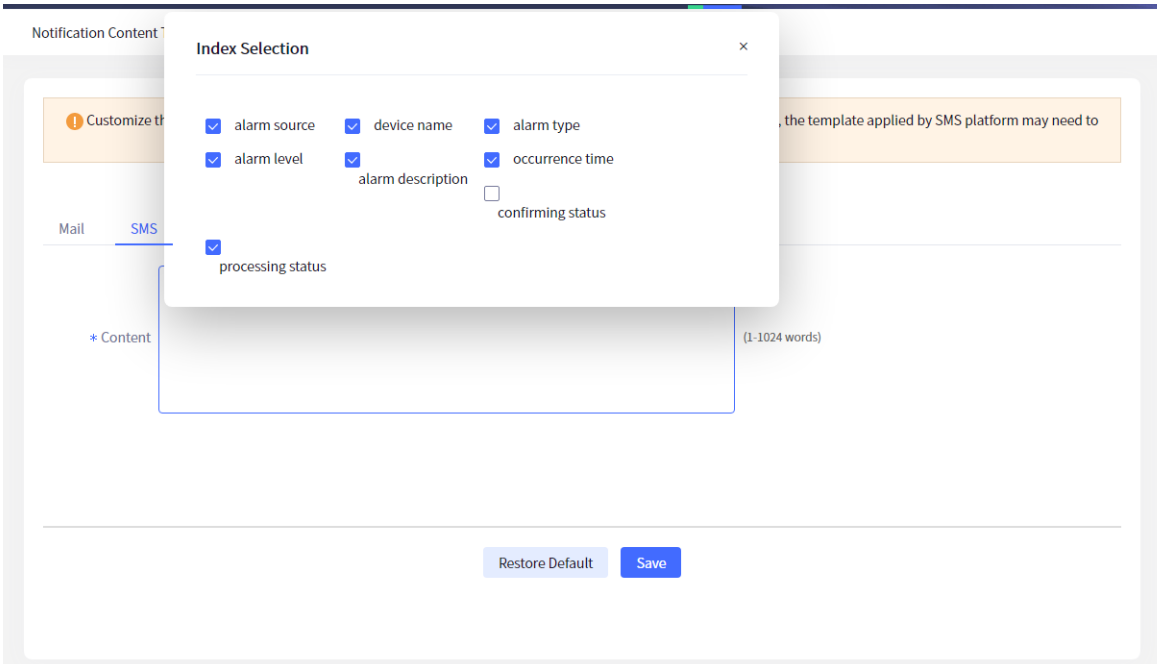
* Title (words)

* Content: [{device name}({alarm source})]in[{occurrence time}]alarm occurs,alarm type is:[{alarm type}],Alarm level is:[{alarm level}],The warning content is:[{alarm description}],processing status:[{processing status}] (1-2048 words)

Figure 11.2.2.2 Mail 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 in the dialog box or remove the unnecessary options. At the same time, users can fill in the SMS content manually, just filling in the content edit box, and click **Save** after selecting it. The effect is shown in the figure.



Index Selection

☑ alarm source
☑ device name
☑ alarm type
☑ alarm level
☑ alarm description
☑ occurrence time
☐ confirming status
☑ processing status

∗ Content (1-1024 words)

Figure 11.2.2.3 SMS template

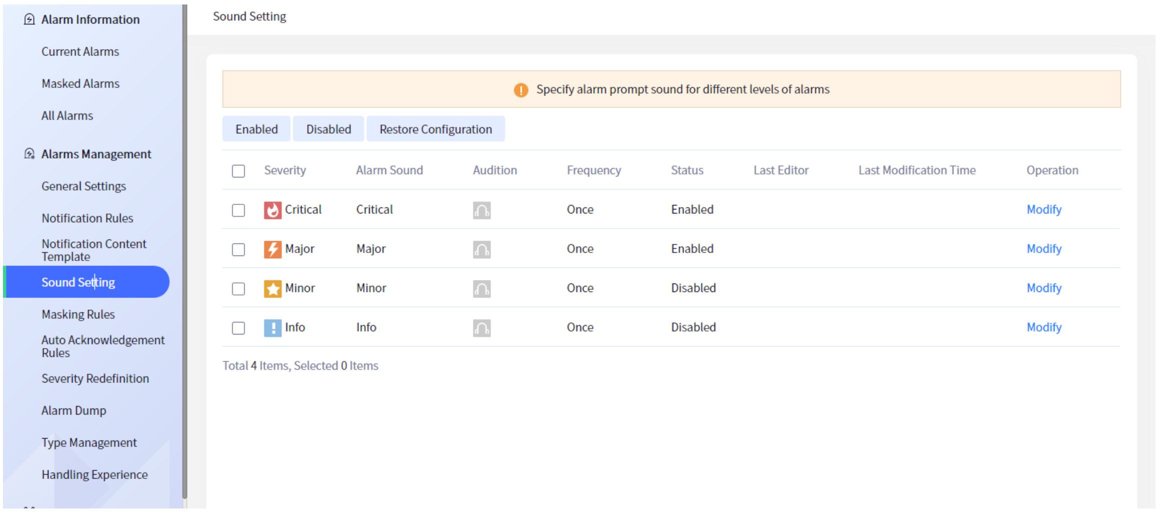
Users can also restore the default configuration of e-mail and SMS content templates by clicking the **Restore Default** button.

Note

- Customize the notification content template of e-mail or SMS. Note that when the SMS content template changes, the template applied by the SMS platform may need to be changed synchronously.

11.2.3 Alarm Sound Configuration

The alarm sound configuration is used to play the prompt sound when the alarm information is notified to the user. Two different prompt sounds are provided for different alarm levels, and the effect is shown in the figure.



Specify alarm prompt sound for different levels of alarms

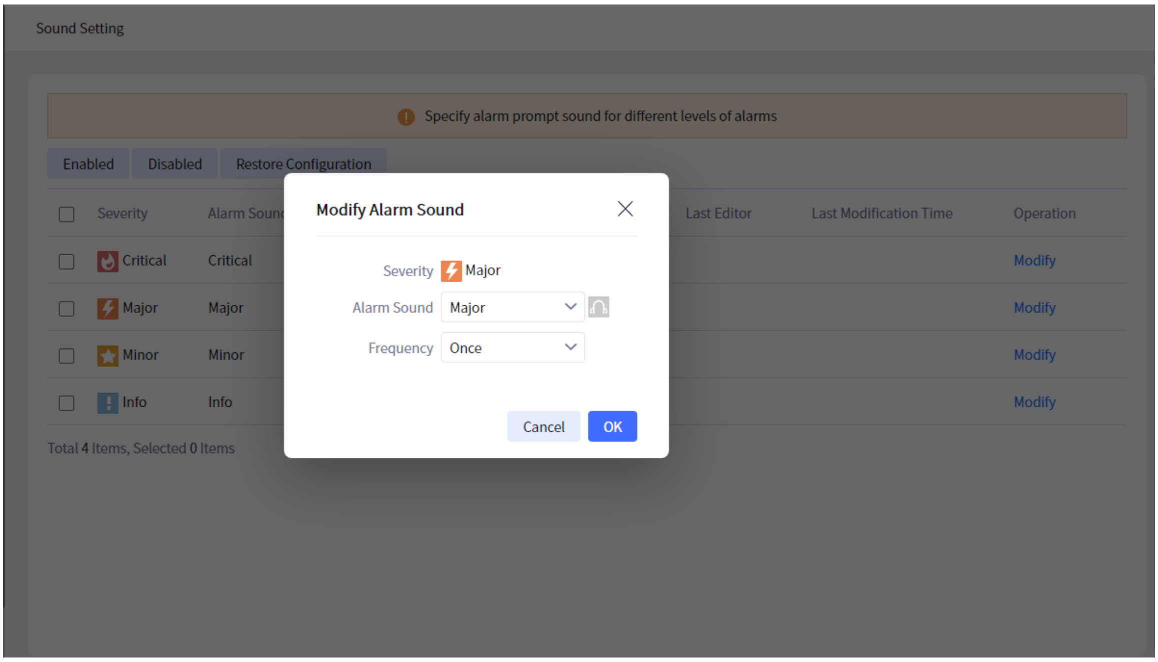
☐	Severity	Alarm Sound	Audition	Frequency	Status	Last Editor	Last Modification Time	Operation
☐	Critical	Critical		Once	Enabled			Modify
☐	Major	Major		Once	Enabled			Modify
☐	Minor	Minor		Once	Disabled			Modify
☐	Info	Info		Once	Disabled			Modify

Total 4 Items, Selected 0 Items

Figure 11.2.3.1 Alarm sound configuration

Users can modify the sound configuration. Select an alarm level on the interface, and then click

Modify to open the **Modify Alarm Sound** dialog box. In this dialog box, there are the **Alarm Sound** and **Frequency** drop-down boxes. There are two kinds of alarm sounds for users to choose. Users can also click the button to listen to the sound. You can click to modify, and the playback times can be once, three times, and cycle all the time for the user to select. After selection, click the **OK** button, and the effect is as shown in the figure.

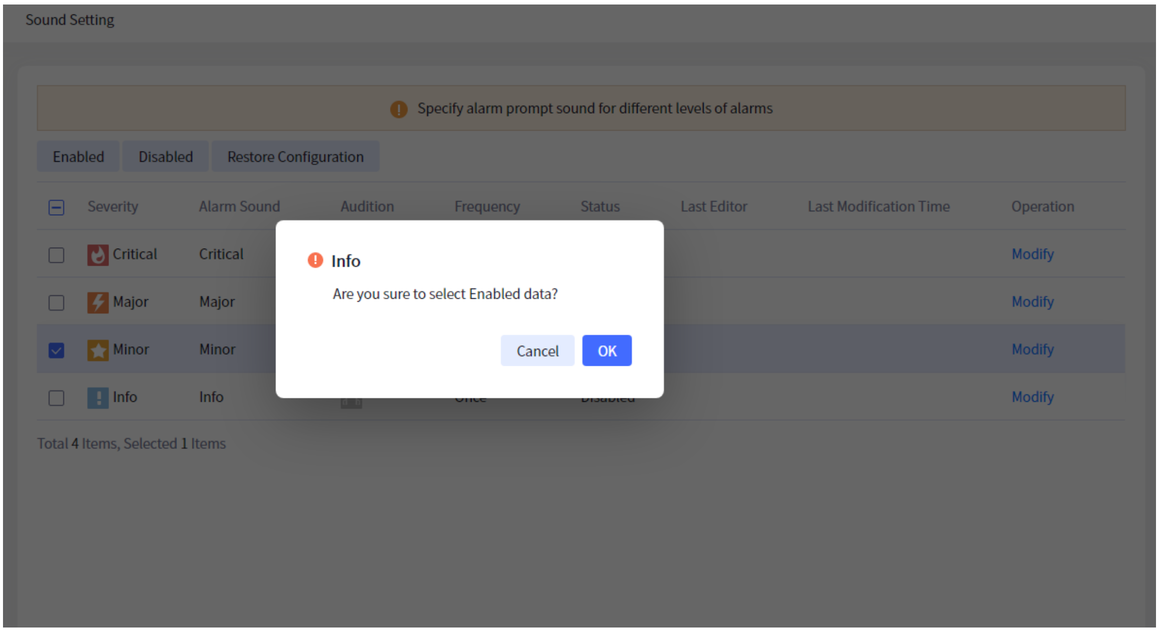


Modify Alarm Sound

Severity: Major
Alarm Sound: Major
Frequency: Once

Figure 11.2.3.2 Modify alarm sound configuration

The user can enable the alarm sounds in batch. Select one or more alarm levels on the interface (only in the inactive state), and then click the **Enable** button. A prompt dialog box will appear. Click the **OK** button. The effect is shown in the figure.

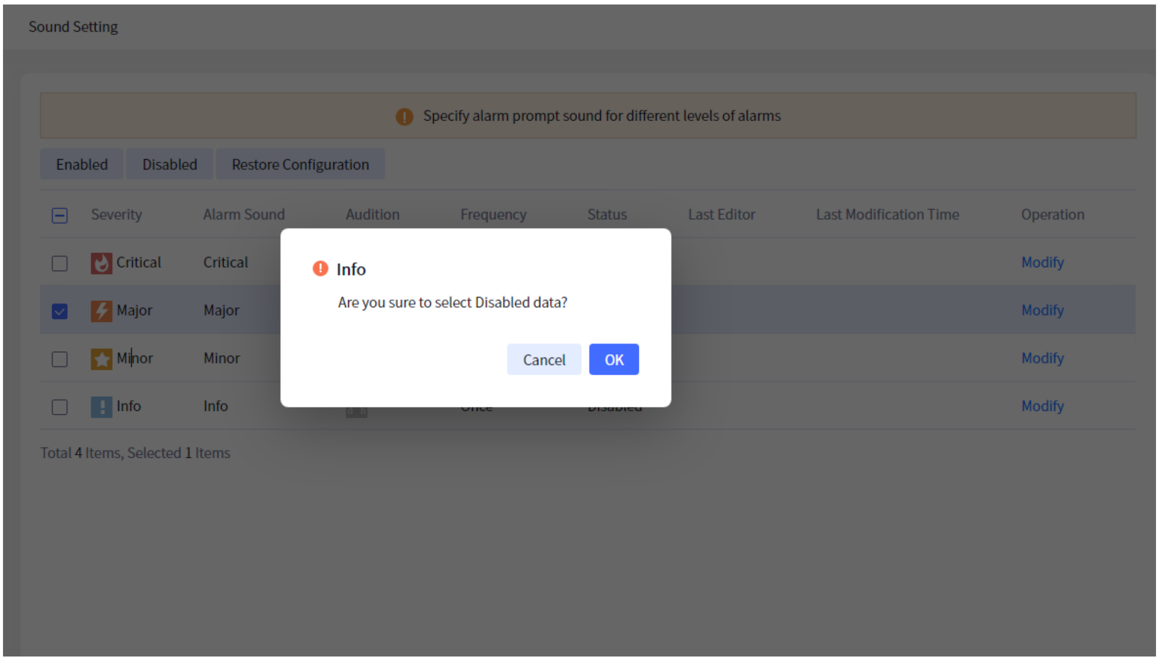


Info

Are you sure to select Enabled data?

Figure 11.2.3.3 Enable alarm sound configuration

The user can disable the alarm sounds in batch. Select one or more alarm levels (only in enabled status) on the interface, and then click the **Disable** button to display a prompt dialog box. Click the **OK** button, and the effect is as shown in the figure.



Sound Setting

Specify alarm prompt sound for different levels of alarms

☐	Severity	Alarm Sound	Audition	Frequency	Status	Last Editor	Last Modification Time	Operation
☐	Critical	Critical						Modify
☑	Major	Major						Modify
☐	Minor	Minor						Modify
☐	Info	Info						Modify

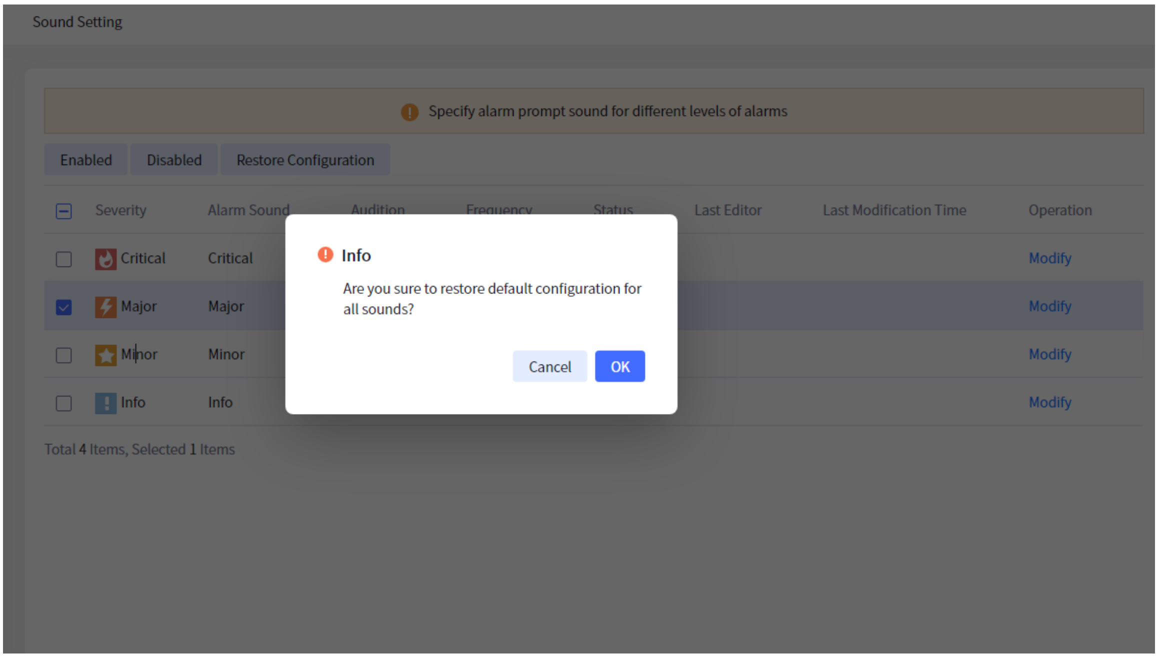
Total 4 Items, Selected 1 Items

Info

Are you sure to select Disabled data?

Figure 11.2.3.4 Disable alarm sound configuration

The user can restore the default configuration of the alarm sound in batches. Click the **Restore Configuration** button on the interface, and a prompt dialog box will appear. Click the **OK** button, and the effect is as shown in the figure.



Sound Setting

Specify alarm prompt sound for different levels of alarms

☐	Severity	Alarm Sound	Audition	Frequency	Status	Last Editor	Last Modification Time	Operation
☐	Critical	Critical						Modify
☑	Major	Major						Modify
☐	Minor	Minor						Modify
☐	Info	Info						Modify

Total 4 Items, Selected 1 Items

Info

Are you sure to restore default configuration for all sounds?

Figure 11.2.3.5 Restore default configuration

11.2.4 Alarm Masking Rules

The alarm masking rule is used to configure how alarm information is processed. The processing methods include shield, reject and receive. The alarm information of which alarm source or type of alarm information can be configured, and in which time period it is processed. In the **Masking Rules** interface, users can fuzzy query the shielding rules by rule name, and can also query the masking rules accurately by enabling status and masking method. The effect is shown in the figure.

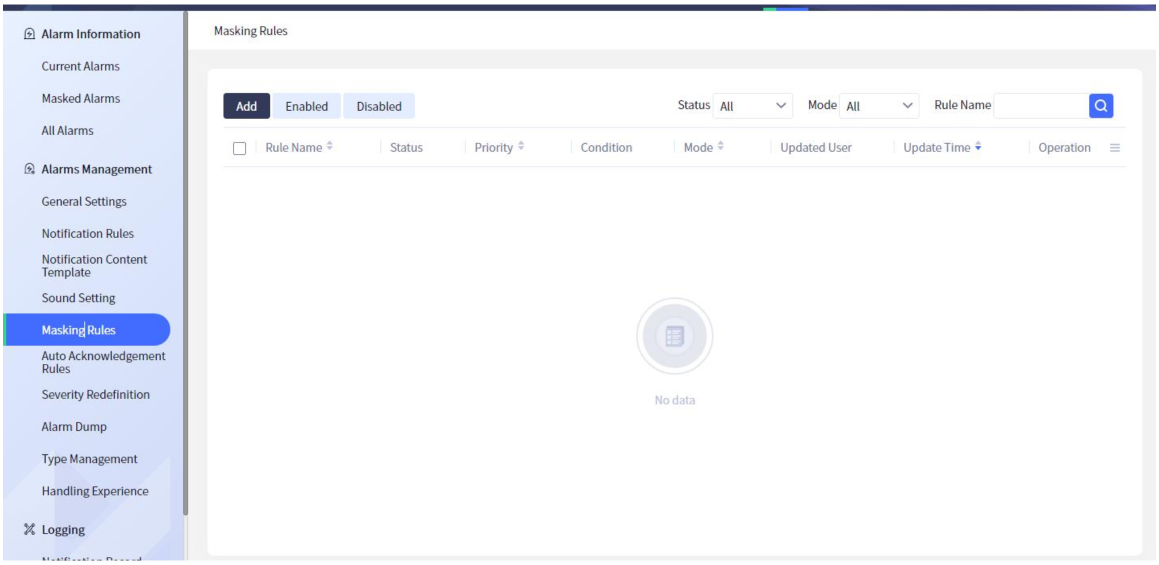
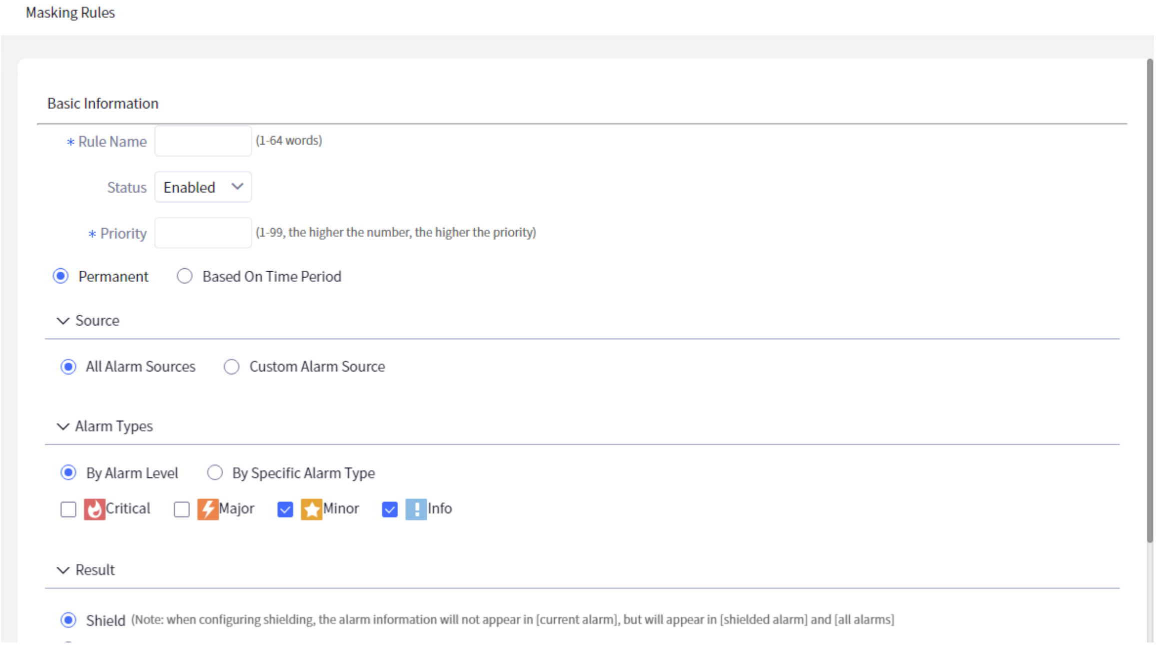


Figure 11.2.4.1 Alarm masking rules

The user can click the **Add** button to add an alarm shielding rule, and the effect is shown in the figure.



* Rule Name (1-64 words)

Status: Enabled

* Priority (1-99, the higher the number, the higher the priority)

● Permanent ○ Based On Time Period

● All Alarm Sources ○ Custom Alarm Source

● By Alarm Level ○ By Specific Alarm Type

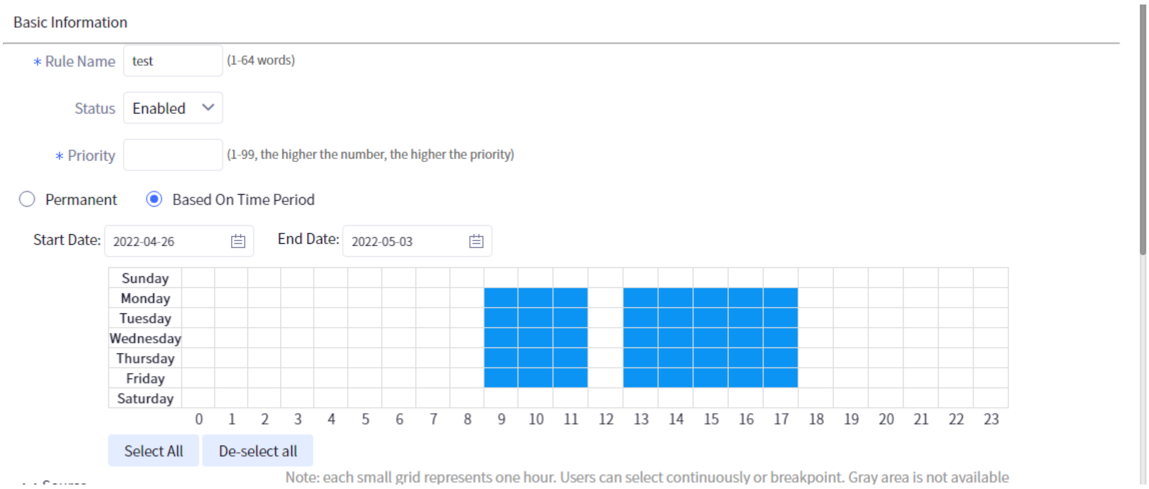
☐ Critical ☐ Major ☑ Minor ☑ Info

● Shield (Note: when configuring shielding, the alarm information will not appear in [current alarm], but will appear in [shielded alarm] and [all alarms]

Figure 11.2.4.2 Add the alarm shielding rule

Basic information:

The basic information is used to configure the name of the alarm shielding rule (required), the enabling status of the rule, the priority of the rule (required, the larger the value, the higher the priority) and the effective time of the rule. The effect is shown in the figure.



Basic Information

* Rule Name: test (1-64 words)

Status: Enabled

* Priority: (1-99, the higher the number, the higher the priority)

○ Permanent ● Based On Time Period

Start Date: 2022-04-26 End Date: 2022-05-03

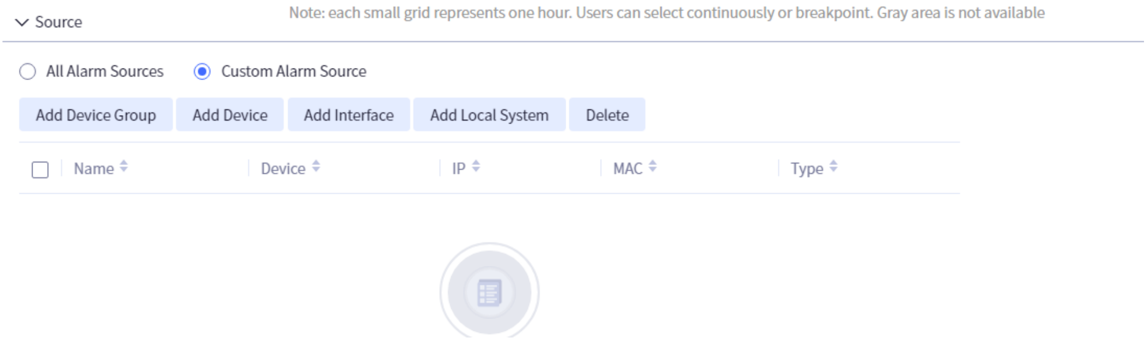
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday																								
Monday										■	■	■		■	■	■	■	■						
Tuesday										■	■	■		■	■	■	■	■						
Wednesday										■	■	■		■	■	■	■	■						
Thursday										■	■	■		■	■	■	■	■						
Friday										■	■	■		■	■	■	■	■						
Saturday																								

Note: each small grid represents one hour. Users can select continuously or breakpoint. Gray area is not available

Figure 11.2.4.3 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 a custom alarm source, a list will appear. The user can click the **Add Alarm Source** button to select a specific alarm source. The effect is shown in the figure.



Note: each small grid represents one hour. Users can select continuously or breakpoint. Gray area is not available

Source

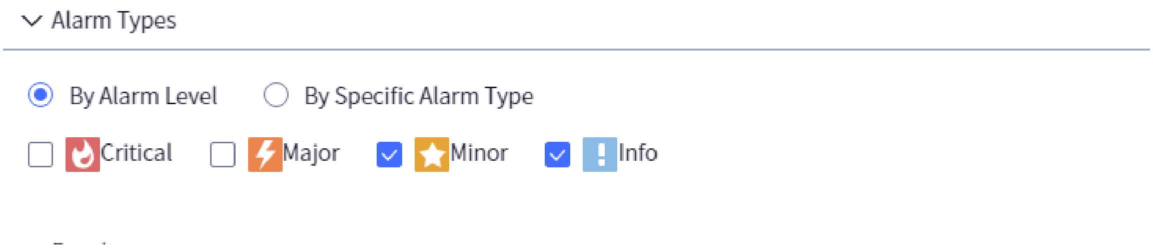
○ All Alarm Sources ● Custom Alarm Source

☐	Name	Device	IP	MAC	Type

Figure 11.2.4.4 Configure alarm source

Alarm type:

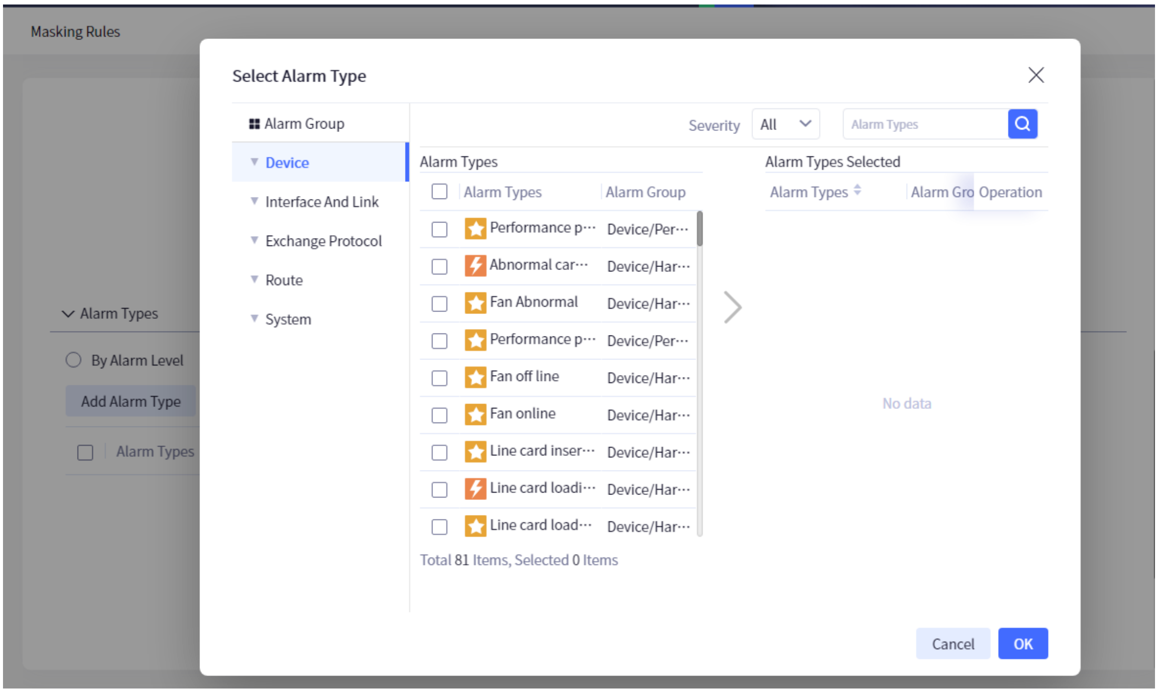
The alarm type is used to determine which type of alarm information needs to be processed. Alarm type rules include by alarm level and by specific alarm type. If the user selects the alarm level, there will be four alarm levels for the user to select. If you select a specific alarm type, a list will appear. You can click the **Add Alarm Type** button to select a specific alarm type. The effect is shown in the figure.



Alarm Types

● By Alarm Level ○ By Specific Alarm Type

☐ Critical ☐ Major ☑ Minor ☑ Info



☐	Alarm Types	Alarm Group
☐	Performance p···	Device/Per···
☐	Abnormal car···	Device/Har···
☐	Fan Abnormal	Device/Har···
☐	Performance p···	Device/Per···
☐	Fan off line	Device/Har···
☐	Fan online	Device/Har···
☐	Line card inser···	Device/Har···
☐	Line card loadi···	Device/Har···
☐	Line card load···	Device/Har···

Total 81 Items, Selected 0 Items

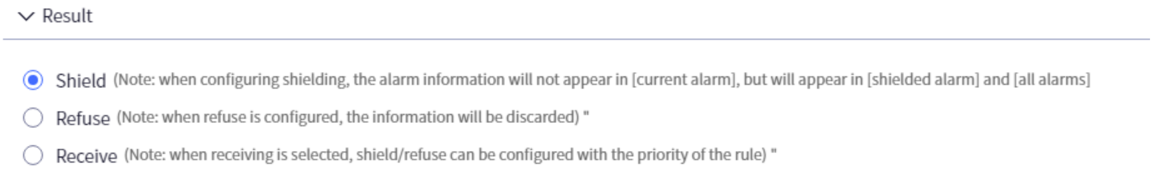
Alarm Types	Alarm Gro	Operation

No data

Figure 11.2.4.5 Configure the alarm type

Result configuration:

Advanced configuration includes three configurations: shield, reject, and receive. **Shield** is to shield the alarm information, and the user can view it in the shielded alarm and all alarm information; **Reject** is to discard the alarm information directly; **Receive** is to store the alarm information. When selecting **Receive**, combine with the rule priority, and you can perform the exception configuration of shield/reject. The effect is shown in figure 10.2.4.6.



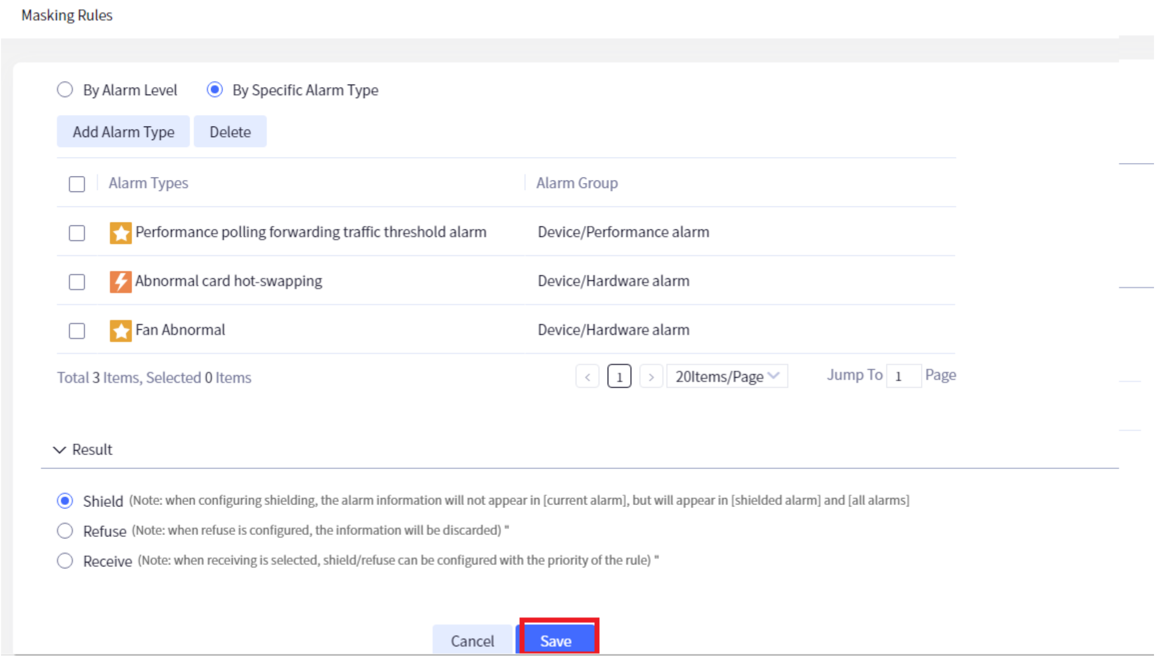
● Shield (Note: when configuring shielding, the alarm information will not appear in [current alarm], but will appear in [shielded alarm] and [all alarms]

○ Refuse (Note: when refuse is configured, the information will be discarded) "

○ Receive (Note: when receiving is selected, shield/refuse can be configured with the priority of the rule) "

Figure 11.2.4.6 Result configuration

Users can modify the alarm shielding rules. Select an alarm shielding rule and click **Modify**. Only the enabling status and priority can be modified for the basic information, while the alarm source, alarm type and result settings can be modified. After modification, click the **Save** button, and the effect is as shown in the figure.



○ By Alarm Level ● By Specific Alarm Type

☐	Alarm Types	Alarm Group
☐	Performance polling forwarding traffic threshold alarm	Device/Performance alarm
☐	Abnormal card hot-swapping	Device/Hardware alarm
☐	Fan Abnormal	Device/Hardware alarm

Total 3 Items, Selected 0 Items   1   20Items/Page   Jump To 1 Page

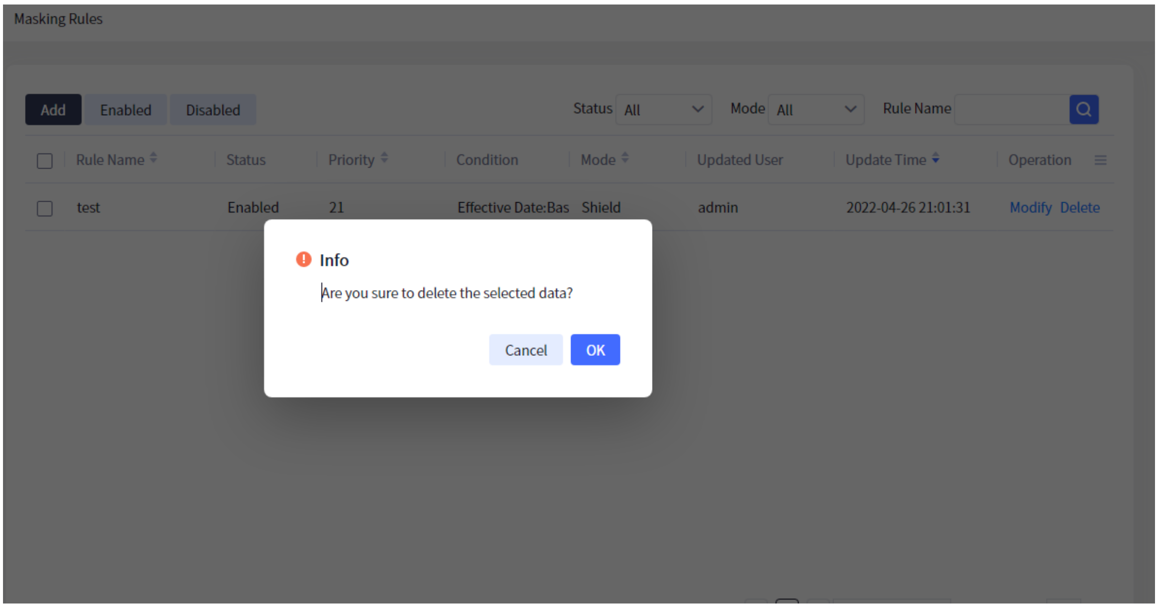
● Shield (Note: when configuring shielding, the alarm information will not appear in [current alarm], but will appear in [shielded alarm] and [all alarms]

○ Refuse (Note: when refuse is configured, the information will be discarded) "

○ Receive (Note: when receiving is selected, shield/refuse can be configured with the priority of the rule) "

Figure 11.2.4.7 Modify the alarm masking rule

You can delete the alarm masking rule. Select an alarm masking rule, and then click the **Delete** button. A prompt box will appear, and then click the **OK** button in the prompt box. The effect is as shown in the figure.



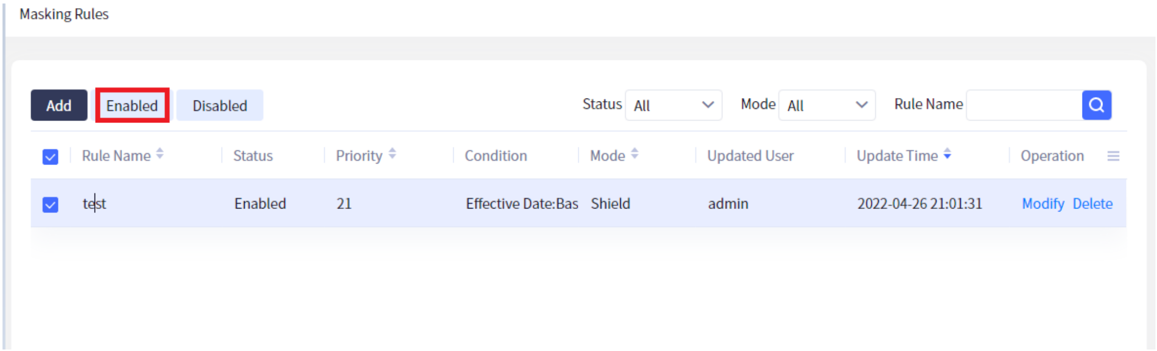
☐	Rule Name	Status	Priority	Condition	Mode	Updated User	Update Time	Operation
☐	test	Enabled	21	Effective Date:Bas	Shield	admin	2022-04-26 21:01:31	Modify Delete

Info

Are you sure to delete the selected data?

Figure 11.2.4.8 Delete the alarm masking rule

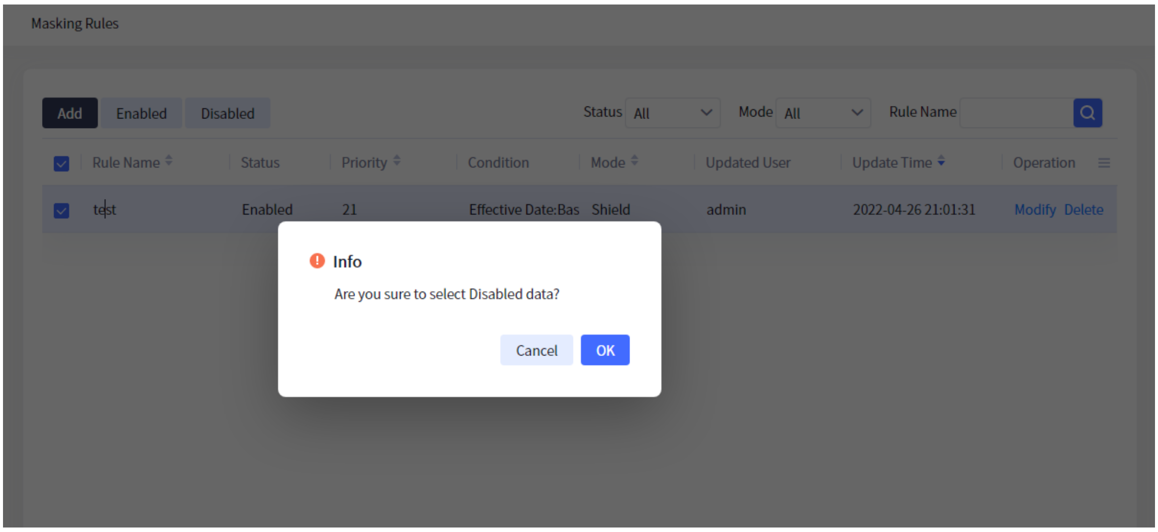
The user can enable the alarm masking rules (support batch operation). On the interface, the user selects one or more alarm masking rules (only in the disabled state), and then clicks the **Enable** button to open a dialog box. Then click the **OK** button on the dialog box. The effect is shown in the figure.



☑	Rule Name	Status	Priority	Condition	Mode	Updated User	Update Time	Operation
☑	test	Enabled	21	Effective Date:Bas	Shield	admin	2022-04-26 21:01:31	Modify Delete

Figure 11.2.4.9 Enable the alarm masking rule

You can disable the alarm masking rule (support batch operation). The user can select one or more alarm masking rules (only in enabled state) on the interface, then click **Disable** to open a dialog box, and then click **OK** on the dialog box. The effect is shown in the figure.



☑	Rule Name	Status	Priority	Condition	Mode	Updated User	Update Time	Operation
☑	test	Enabled	21	Effective Date:Bas	Shield	admin	2022-04-26 21:01:31	Modify Delete

Info

Are you sure to select Disabled data?

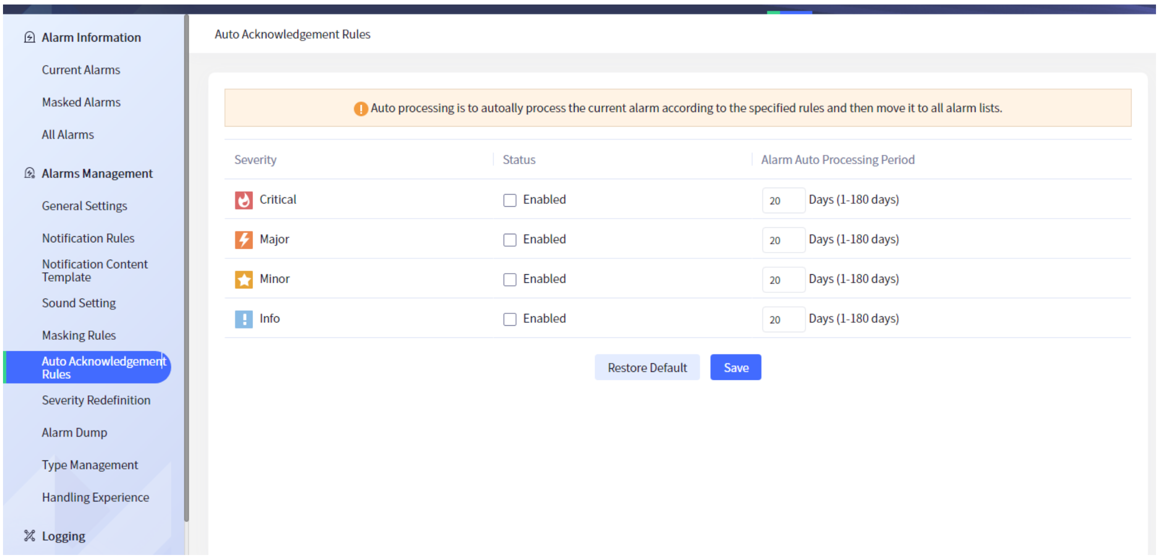
Figure 11.2.4.10 Disable the alarm masking rule

Note

- The alarm matches only one masking rule at a time. The rule with higher priority is prior. When the priorities are the same, the rule with the latest time is prior. When the priority and time are the same, match according to the rule ID
- You cannot repeatedly disable and enable the masking rule.

11.2.5 Auto Processing Rules of Alarms

The auto alarm processing rule is used to configure the alarm information (the alarm information that has not been processed, and the auto processing time is 2 a.m. every day) to be automatically processed by the system within a certain period. Different alarm levels can be configured with different auto processing periods. Different alarm levels can be configured with different auto processing periods. The effect is shown in the figure.

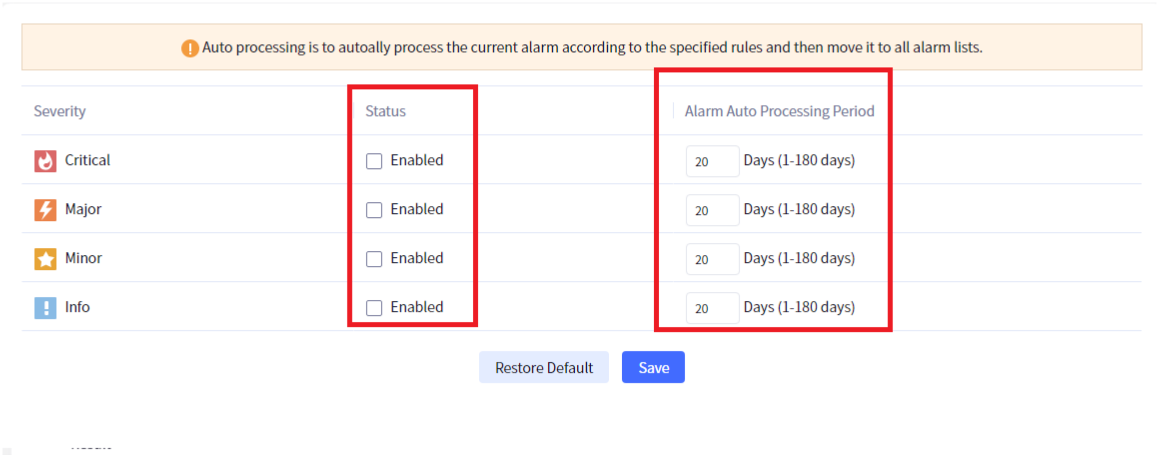


Auto processing is to autoally process the current alarm according to the specified rules and then move it to all alarm lists.

Severity	Status	Alarm Auto Processing Period
Critical	☐ Enabled	20 Days (1-180 days)
Major	☐ Enabled	20 Days (1-180 days)
Minor	☐ Enabled	20 Days (1-180 days)
Info	☐ Enabled	20 Days (1-180 days)

Figure 11.2.5.1 Auto alarm processing rule

The user can configure the enabling status (enabled, not enabled) and auto alarm processing cycle for different alarm types on the **Auto Acknowledge Rules** interface. The user can also restore the default for the auto alarm processing rule, and the effect is shown in the figure.



Auto processing is to autoally process the current alarm according to the specified rules and then move it to all alarm lists.

Severity	Status	Alarm Auto Processing Period
Critical	☐ Enabled	20 Days (1-180 days)
Major	☐ Enabled	20 Days (1-180 days)
Minor	☐ Enabled	20 Days (1-180 days)
Info	☐ Enabled	20 Days (1-180 days)

Figure 11.2.5.2 Configure the auto alarm processing rule

11.2.6 Severity Re-definition

Alarm level redefinition is used to configure how the level of alarm information is redefined. The processing methods include level redefinition and level auto upgrade. The alarm information of which alarm source can be configured or the level of which type of alarm information can be redefined. In the **Severity Redefinition** interface, you can use the rule name to fuzzy query rules, and you can also accurately query rules by the enabling state and rule type. The effect is shown in the figure.

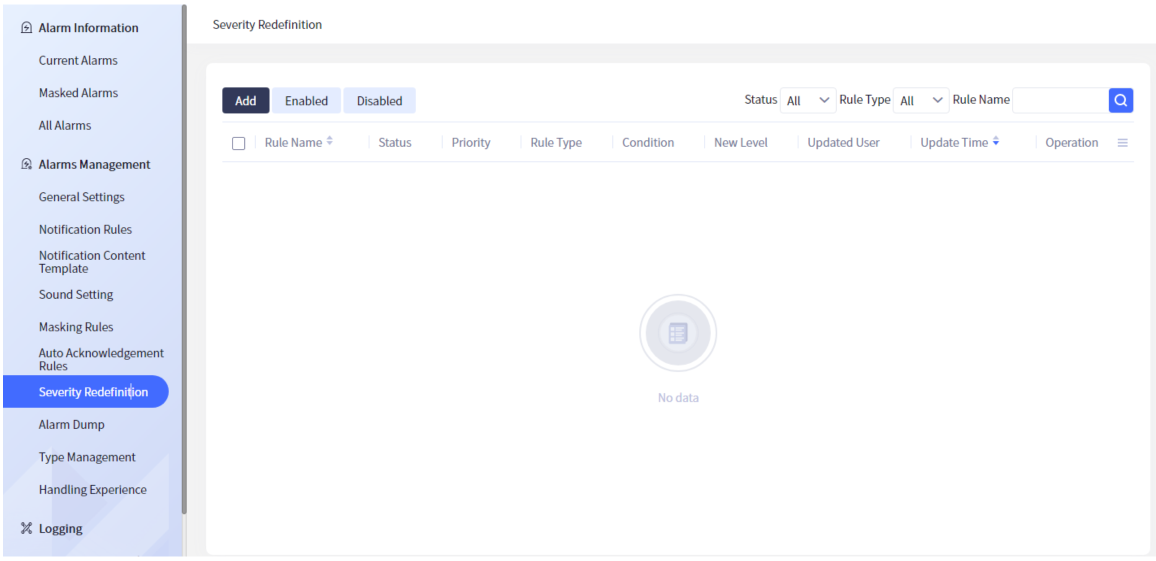
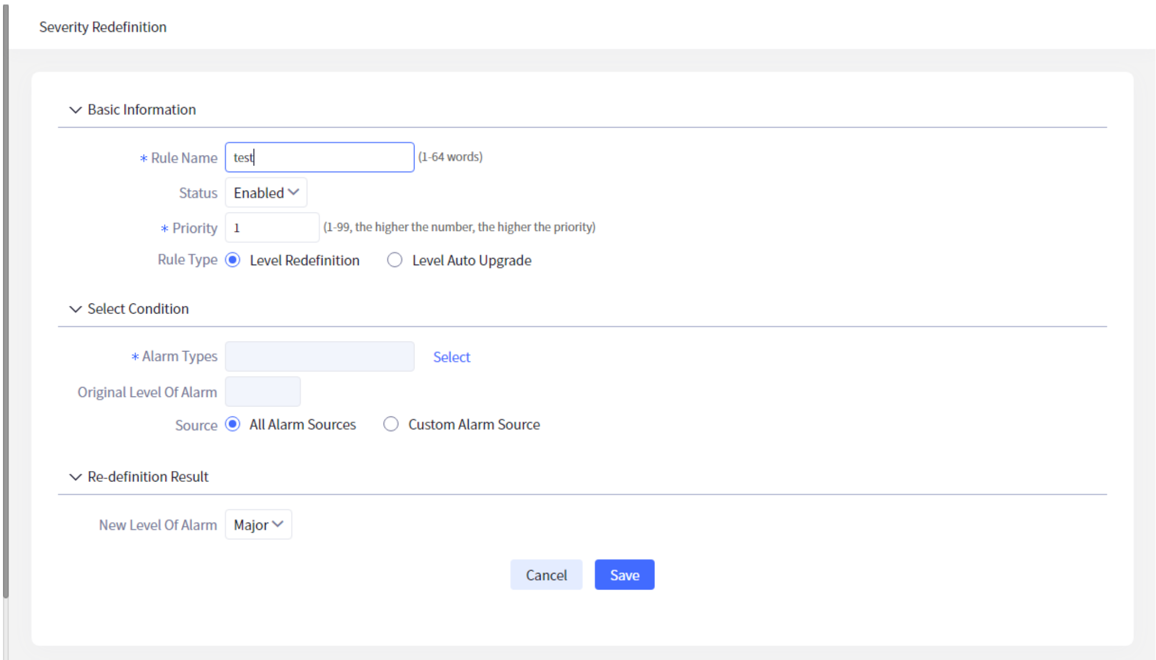


Figure 11.2.6.1 Severity re-definition

The user can click the **Add** button to add an alarm level redefinition, and the effect is shown in the figure.



* Rule Name: test (1-64 words)

Status: Enabled

* Priority: 1 (1-99, the higher the number, the higher the priority)

Rule Type: ● Level Redefinition ○ Level Auto Upgrade

* Alarm Types:

Original Level Of Alarm:

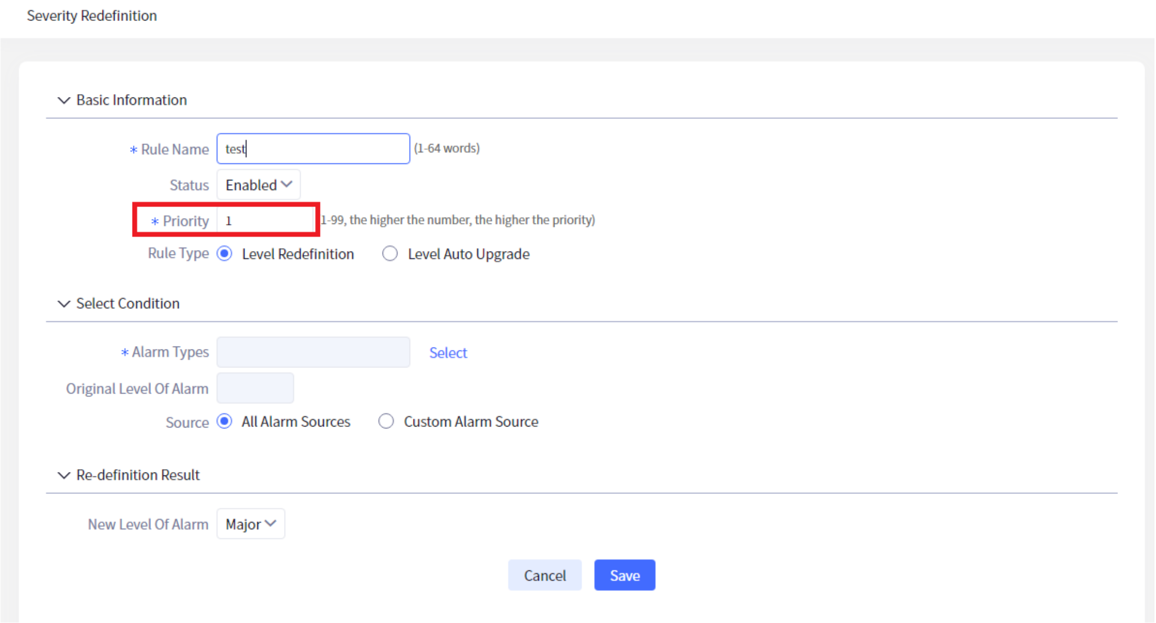
Source: ● All Alarm Sources ○ Custom Alarm Source

New Level Of Alarm: Major

Figure 11.2.6.2 Add the alarm severity re-definition rule

Basic information:

The basic information is used to configure the severity re-definition rule name (required), the enabling status of the rule, the priority of the rule (required, the larger the value, the higher the priority) and the rule type. The effect is shown in the figure.



Severity Redefinition

Basic Information

* Rule Name: test (1-64 words)

Status: Enabled

* Priority: 1 (1-99, the higher the number, the higher the priority)

Rule Type: ● Level Redefinition ○ Level Auto Upgrade

Select Condition

* Alarm Types: Select

Original Level Of Alarm:

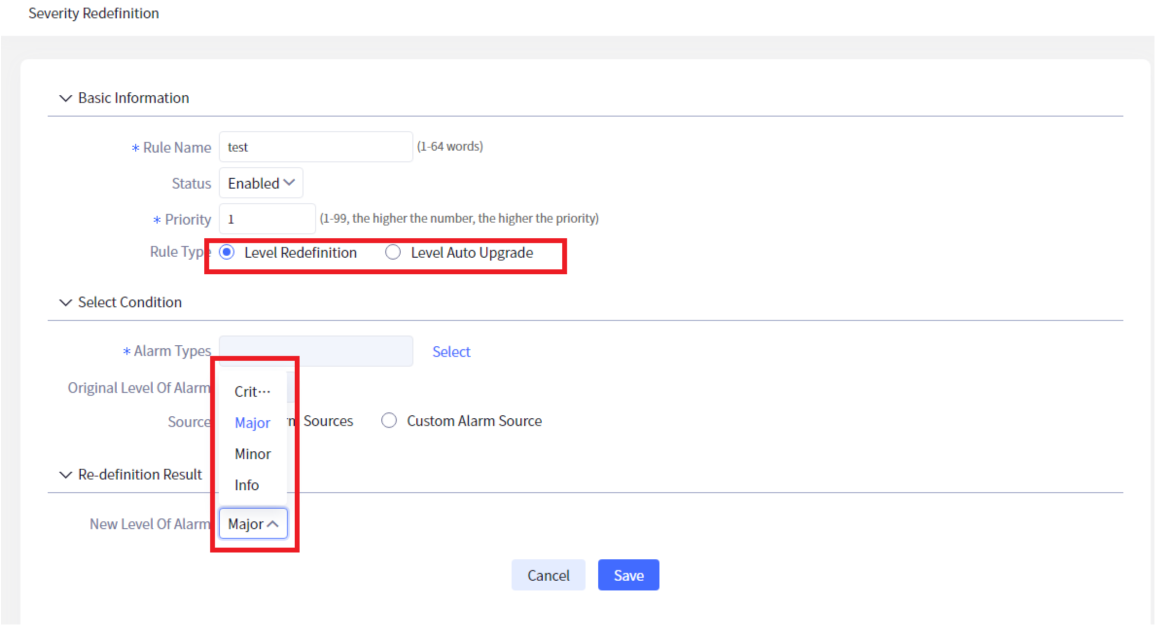
Source: ● All Alarm Sources ○ Custom Alarm Source

Re-definition Result

New Level Of Alarm: Major

Figure 11.2.6.3 Configure the basic information of the severity re-definition

If selecting **Level Redefinition**, you need to configure the redefinition results. If selecting **Level Auto Upgrade**, you need to configure policy settings. The effect is shown in the figure.



Severity Redefinition

Basic Information

* Rule Name: test (1-64 words)

Status: Enabled

* Priority: 1 (1-99, the higher the number, the higher the priority)

Rule Typ ● Level Redefinition ○ Level Auto Upgrade

Select Condition

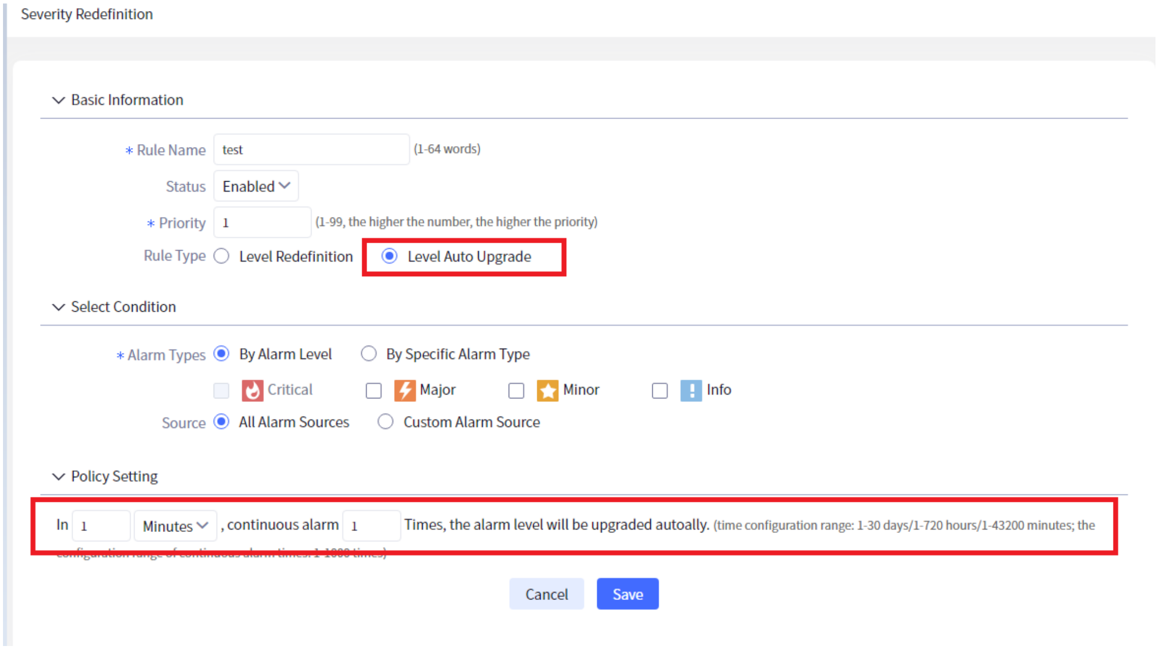
* Alarm Types: Select

Original Level Of Alarm

Source ... Sources ○ Custom Alarm Source

Re-definition Result

New Level Of Alarm: Major



* Rule Name: test (1-64 words)

Status: Enabled

* Priority: 1 (1-99, the higher the number, the higher the priority)

Rule Type: ○ Level Redefinition ● Level Auto Upgrade

* Alarm Types: ● By Alarm Level ○ By Specific Alarm Type

☐ Critical ☐ Major ☐ Minor ☐ Info

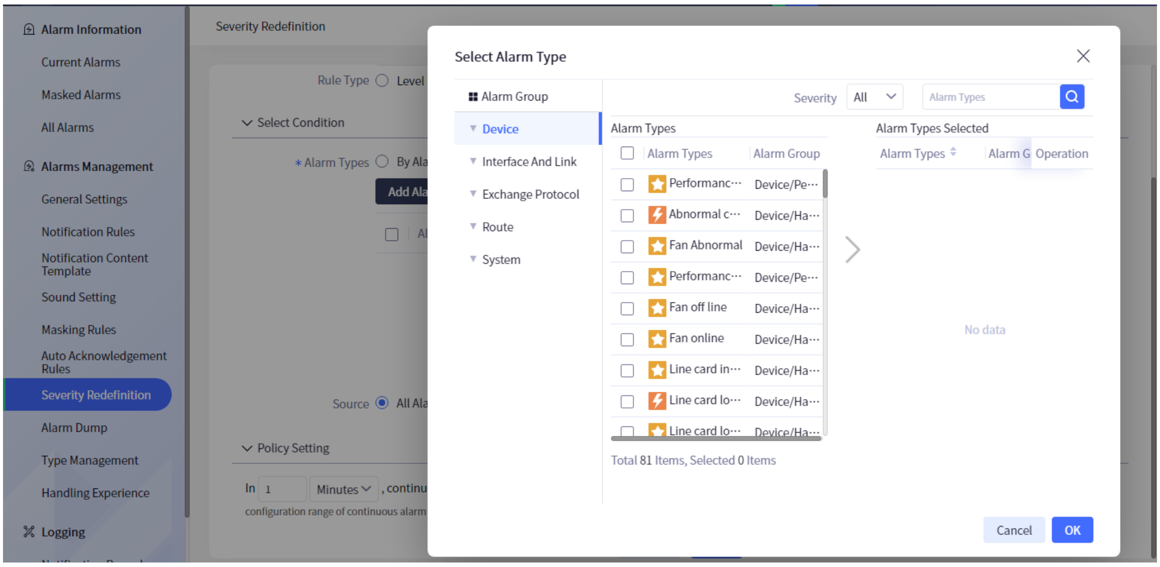
Source: ● All Alarm Sources ○ Custom Alarm Source

In 1 Minutes , continuous alarm 1 Times, the alarm level will be upgraded autoally. (time configuration range: 1-30 days/1-720 hours/1-43200 minutes; the configuration range of continuous alarm times: 1-1000 times)

Figure 11.2.6.4 Configure the rule type

Condition selection:

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, and then the user clicks the button **Add Alarm Type** to select the specific alarm type. The effect is shown in the figure.



☐	Alarm Types	Alarm Group
☐	Performanc···	Device/Pe···
☐	Abnormal c···	Device/Ha···
☐	Fan Abnormal	Device/Ha···
☐	Performanc···	Device/Pe···
☐	Fan off line	Device/Ha···
☐	Fan online	Device/Ha···
☐	Line card in···	Device/Ha···
☐	Line card lo···	Device/Ha···
☐	Line card lo···	Device/Ha···

Total 81 Items, Selected 0 Items

Figure 11.2.6.5 Configure the alarm type

The alarm source is used to determine which alarm information needs to be redefined. Alarm source rules include **All Alarm Sources** and **Custom Alarm Source**. When the user selects **Custom Alarm Source**, a list will appear. The user can click the button **Alarm Source** to select a specific alarm source. The effect is shown in the figure.

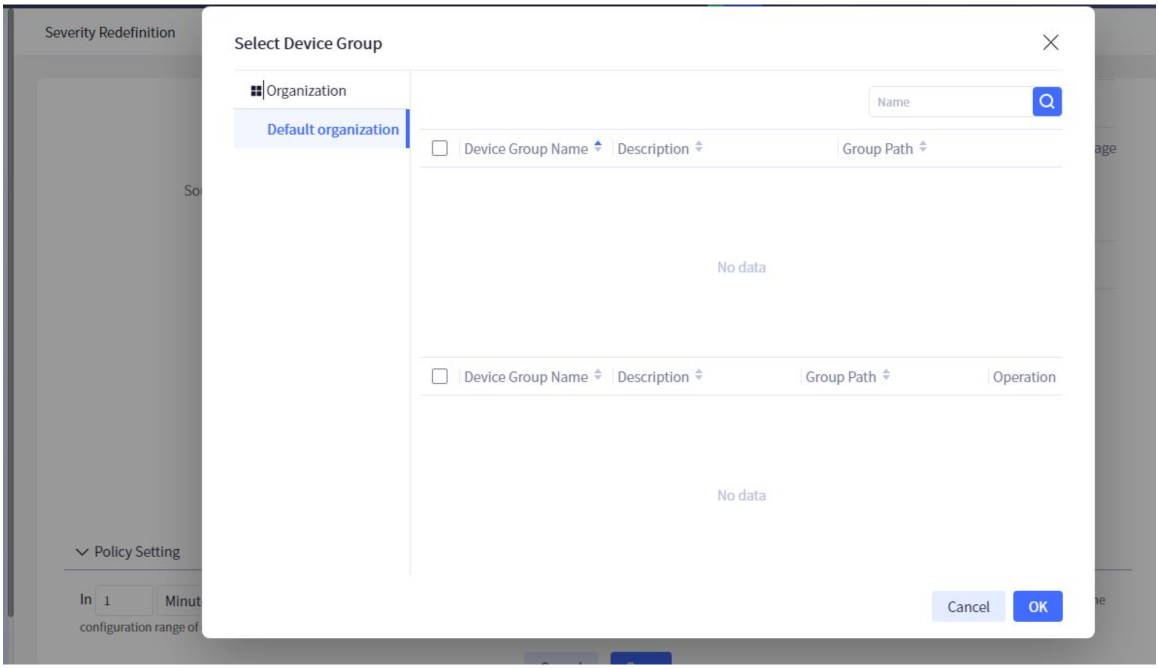
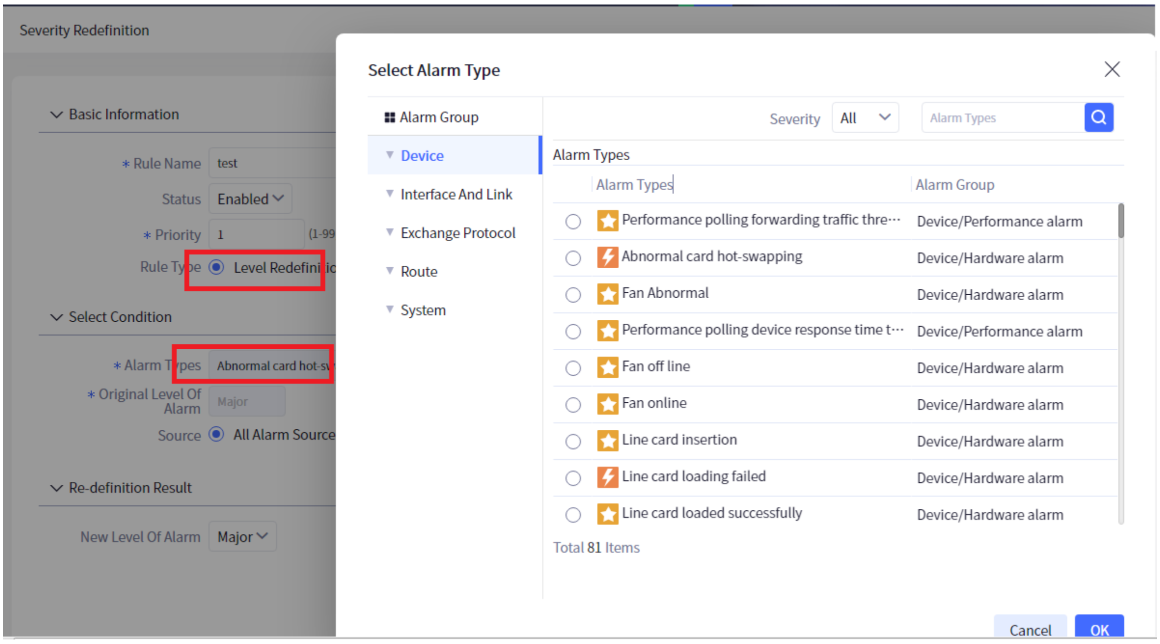


Figure 11.2.6.6 Configure the alarm source

Redefine result configuration:

If the rule type is selected as level redefinition, you need to configure the level of the alarm, including four levels: critical, major, minor, and info. If the rule type is level auto upgrade, you need to configure the policy, and the effect is shown in the figure.



* Rule Name: test

Status: Enabled

* Priority: 1 (1-99

Rule Type: ● Level Redefini

* Alarm Types: Abnormal card hot-s

* Original Level Of Alarm: Major

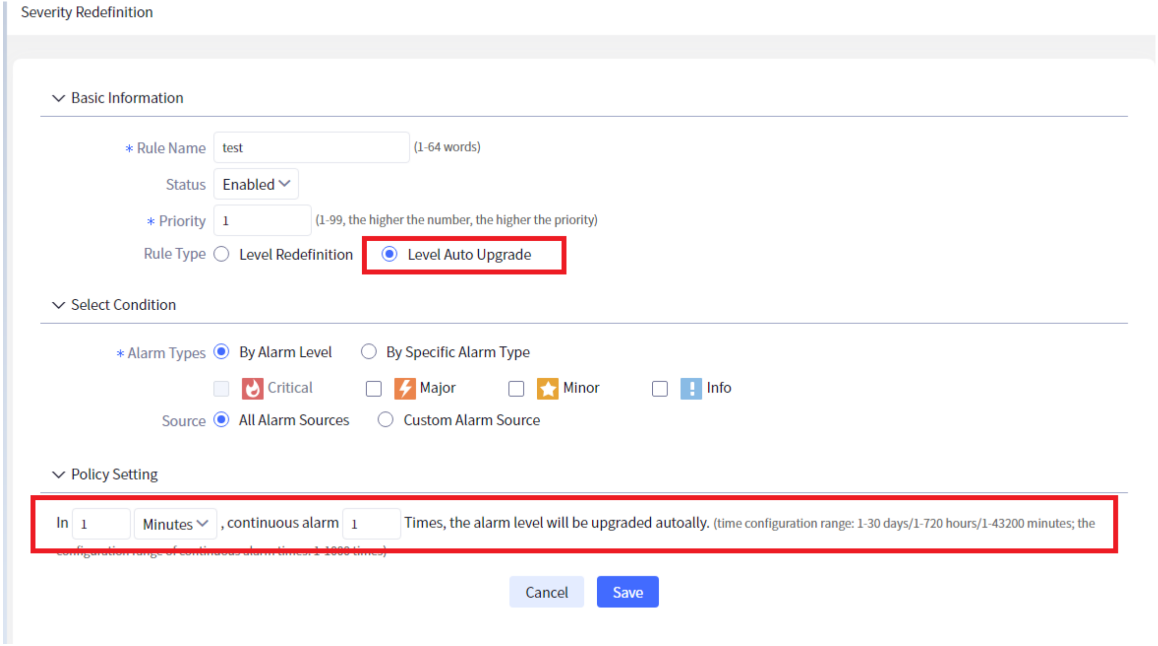
Source: ● All Alarm Source

New Level Of Alarm: Major

Alarm Types

	Alarm Types	Alarm Group
○	Performance polling forwarding traffic thre···	Device/Performance alarm
○	Abnormal card hot-swapping	Device/Hardware alarm
○	Fan Abnormal	Device/Hardware alarm
○	Performance polling device response time t···	Device/Performance alarm
○	Fan off line	Device/Hardware alarm
○	Fan online	Device/Hardware alarm
○	Line card insertion	Device/Hardware alarm
○	Line card loading failed	Device/Hardware alarm
○	Line card loaded successfully	Device/Hardware alarm

Total 81 Items



Severity Redefinition

Basic Information

* Rule Name: test (1-64 words)

Status: Enabled

* Priority: 1 (1-99, the higher the number, the higher the priority)

Rule Type: ○ Level Redefinition ● Level Auto Upgrade

Select Condition

* Alarm Types: ● By Alarm Level ○ By Specific Alarm Type

☐ Critical ☐ Major ☐ Minor ☐ Info

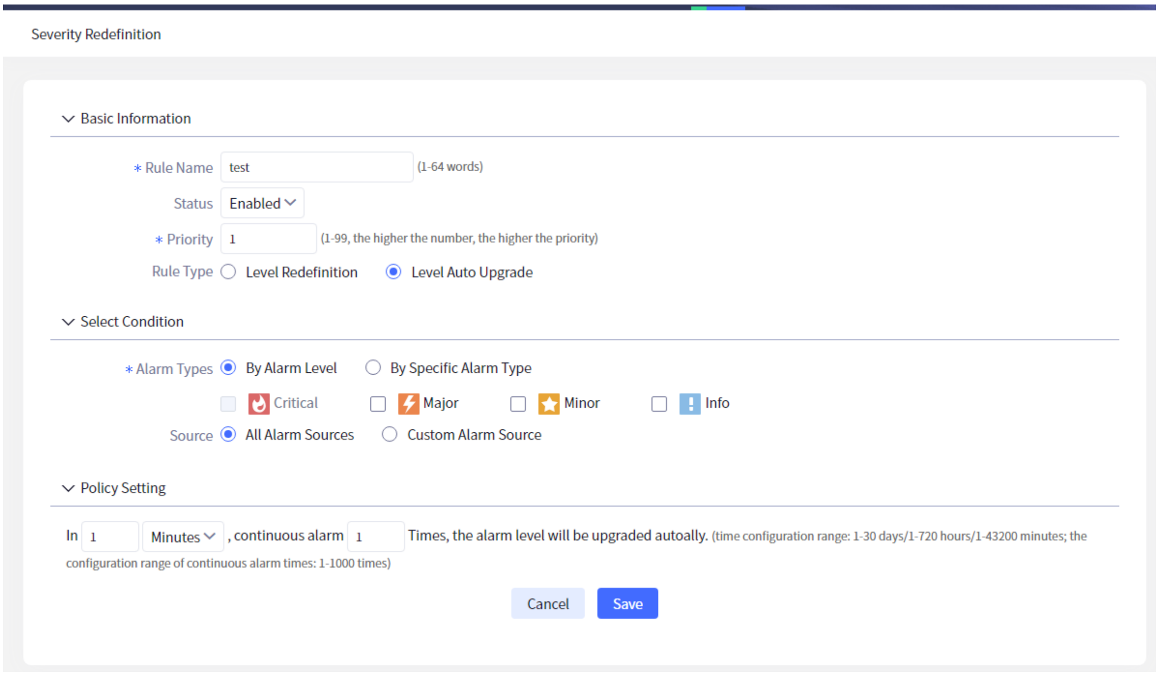
Source: ● All Alarm Sources ○ Custom Alarm Source

Policy Setting

In 1 Minutes , continuous alarm 1 Times, the alarm level will be upgraded autoally. (time configuration range: 1-30 days/1-720 hours/1-43200 minutes; the

Figure 11.2.6.7 Result configuration

The user can modify the severity redefinition. Select a severity redefinition rule and click **Modify**. Only the enabling status and priority can be modified for the basic information, while the alarm source, alarm type and result settings can be modified. After modification, click the **Save** button, and the effect is as shown in the figure.



Severity Redefinition

Basic Information

* Rule Name: test (1-64 words)

Status: Enabled

* Priority: 1 (1-99, the higher the number, the higher the priority)

Rule Type: ○ Level Redefinition ● Level Auto Upgrade

Select Condition

* Alarm Types: ● By Alarm Level ○ By Specific Alarm Type

☐ Critical ☐ Major ☐ Minor ☐ Info

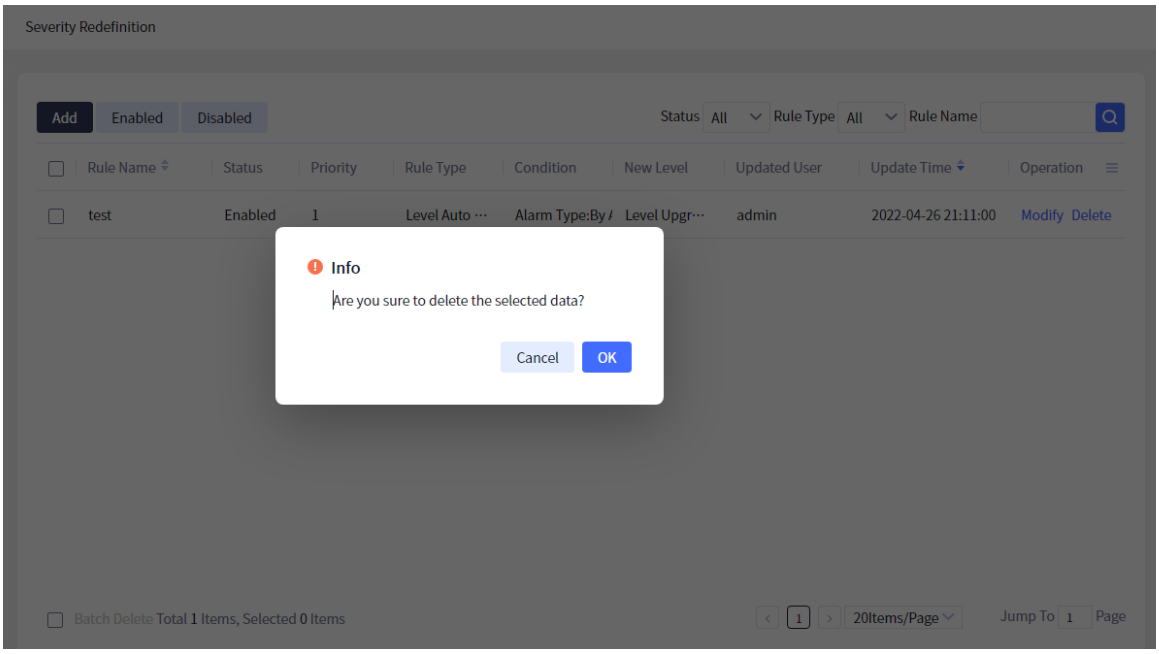
Source: ● All Alarm Sources ○ Custom Alarm Source

Policy Setting

In 1 Minutes , continuous alarm 1 Times, the alarm level will be upgraded autoally. (time configuration range: 1-30 days/1-720 hours/1-43200 minutes; the configuration range of continuous alarm times: 1-1000 times)

Figure 11.2.6.8 Modify the severity re-definition

The user can delete the severity redefinition. Select a severity redefinition rule, and then click **Delete** to display a prompt box. Then click **OK** in the prompt box, and the effect is as shown in the figure.



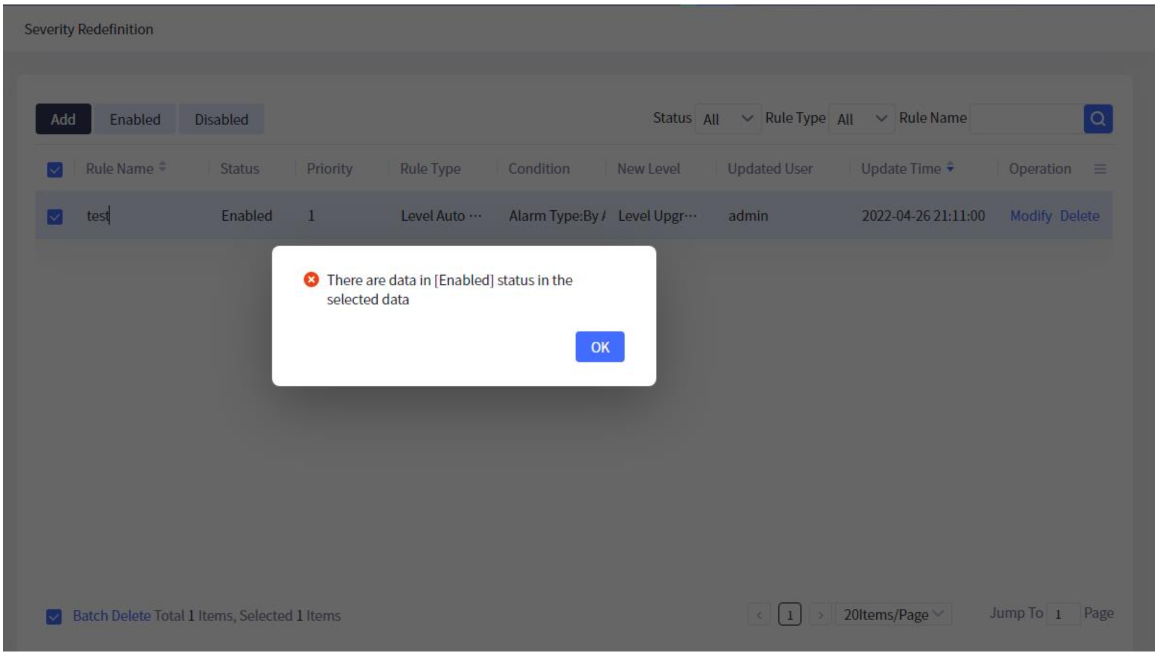
☐	Rule Name	Status	Priority	Rule Type	Condition	New Level	Updated User	Update Time	Operation
☐	test	Enabled	1	Level Auto ···	Alarm Type:By /	Level Upgr···	admin	2022-04-26 21:11:00	Modify Delete

Info

Are you sure to delete the selected data?

Figure 11.2.6.9 Delete the severity redefinition rule

The user can enable the severity redefinition rule (support batch operation). On the interface, the user selects one or more severity redefinition rules (only in the disabled state), and then clicks the **Enable** button to pop up a dialog box. Then click the **OK** button on the dialog box. The effect is shown in the figure.

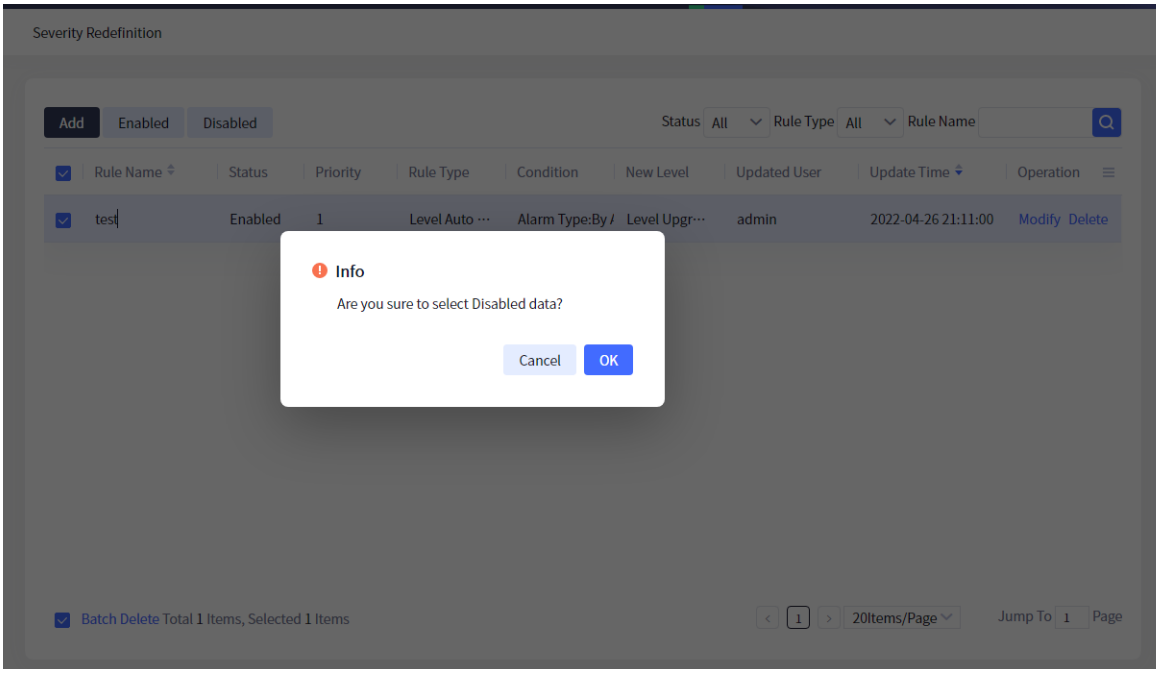


☑	Rule Name	Status	Priority	Rule Type	Condition	New Level	Updated User	Update Time	Operation
☑	test	Enabled	1	Level Auto ···	Alarm Type:By /	Level Upgr···	admin	2022-04-26 21:11:00	Modify Delete

There are data in [Enabled] status in the selected data

Figure 11.2.6.10 Enable the severity redefinition rule

You can disable the severity redefinition rule (support batch operation). The user can select one or more severity redefinition rules (only in enabled state) on the interface, then click **Disable** to open a dialog box, and then click **OK** on the dialog box. The effect is shown in the figure.



☑	Rule Name	Status	Priority	Rule Type	Condition	New Level	Updated User	Update Time	Operation
☑	test	Enabled	1	Level Auto ···	Alarm Type:By /	Level Upgr···	admin	2022-04-26 21:11:00	Modify Delete

Total 1 Items, Selected 1 Items

Info

Are you sure to select Disabled data?

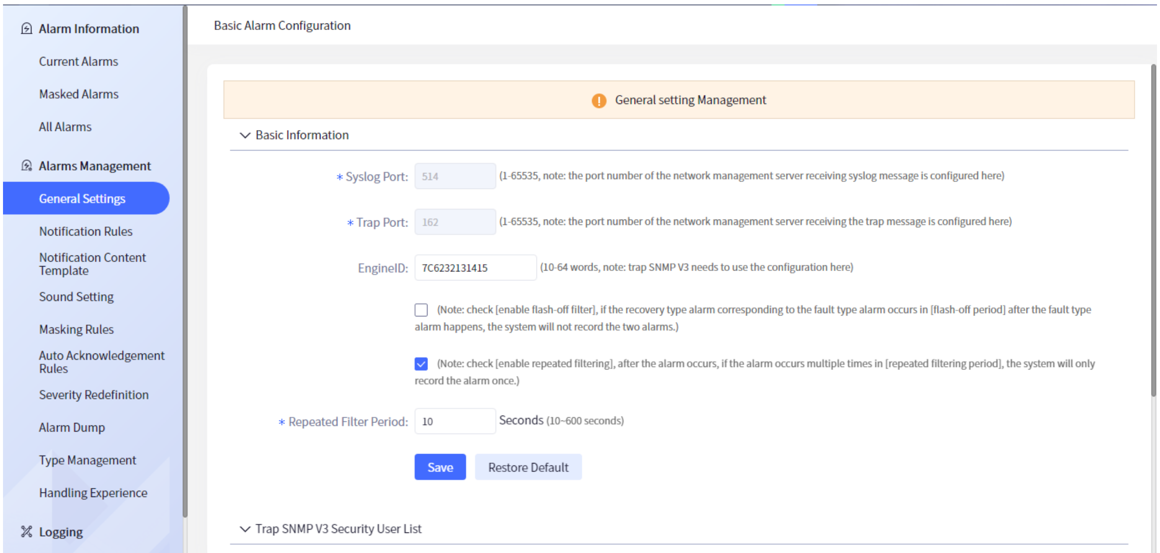
Figure 11.2.6.11 Disable the severity redefinition rule

Note

- It is necessary to select an effective alarm source.
- The alarm information matches only one rule at a time. The rule with higher priority is prior. When the priorities are the same, the rule with the latest time is prior. When the priority and time are the same time, match by the rule ID.

11.2.7 General Configuration of Alarms

The basic alarm configuration is used to configure the SYSLOG port, trap port, EngineID, whether to enable the alarm flash-off filter and repeated filter. If enabled, the flash-off filter and repeated filter periods need to be configured. In addition, users can add, modify and delete TRAP SNMP V3 security users. The effect is shown in the figure.



* Syslog Port: 514 (1-65535, note: the port number of the network management server receiving syslog message is configured here)

* Trap Port: 162 (1-65535, note: the port number of the network management server receiving the trap message is configured here)

EngineID: 7C6232131415 (10-64 words, note: trap SNMP V3 needs to use the configuration here)

☐ (Note: check [enable flash-off filter], if the recovery type alarm corresponding to the fault type alarm occurs in [flash-off period] after the fault type alarm happens, the system will not record the two alarms.)

☑ (Note: check [enable repeated filtering], after the alarm occurs, if the alarm occurs multiple times in [repeated filtering period], the system will only record the alarm once.)

* Repeated Filter Period: 10 Seconds (10~600 seconds)

Figure 11.2.7.1 General settings of the alarm

Basic configuration:

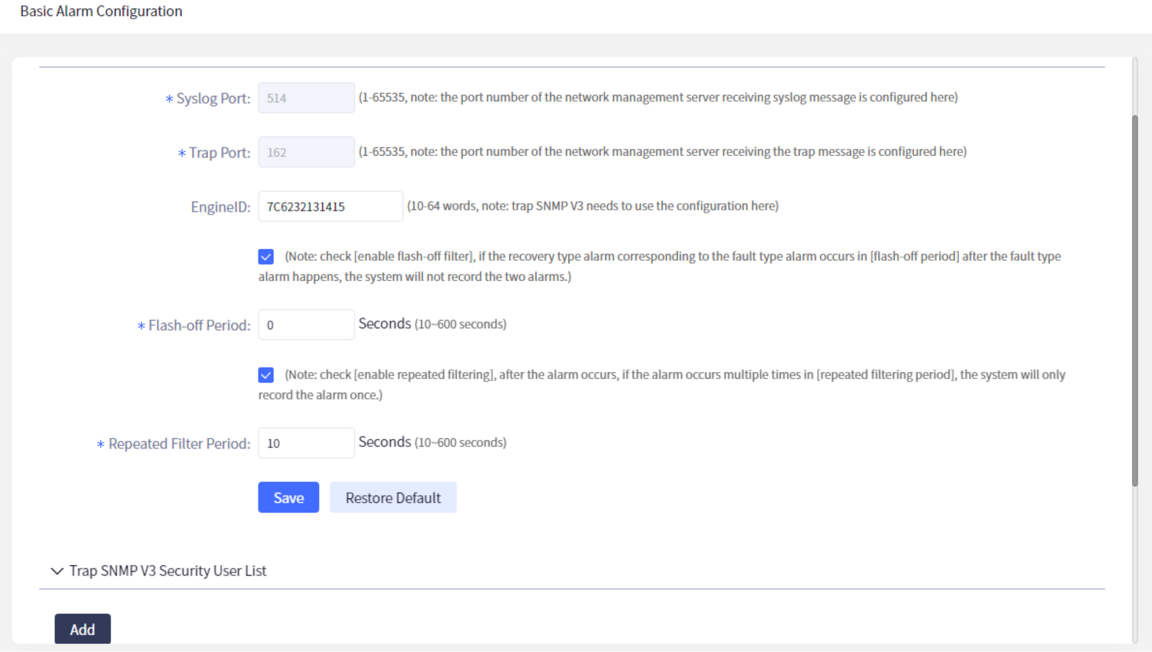
Syslog port is the port number used by the network management server to receive syslog messages. The port number here is required.

Trap port is the port number used by the NMS server to receive trap messages. The port number here is required.

The flash-off filter is used to prevent the network management server from recording the two alarm messages if a fault alarm occurs and then a recovery alarm corresponding to the fault alarm occurs within a flash-off period. If the flash-off filter is enabled, the flash-off period must be configured.

Repeated filter is used to record an alarm only once after an alarm occurs and the alarm occurs many times during the repeated filter period. If the flash-off filter is enabled, the repeated filtering period must be configured.

After the above parameters are configured, click the **Save** button, and the effect is shown in the figure.



Basic Alarm Configuration

∗ Syslog Port: 514 (1-65535, note: the port number of the network management server receiving syslog message is configured here)

∗ Trap Port: 162 (1-65535, note: the port number of the network management server receiving the trap message is configured here)

EngineID: 7C6232131415 (10-64 words, note: trap SNMP V3 needs to use the configuration here)

☑ (Note: check [enable flash-off filter], if the recovery type alarm corresponding to the fault type alarm occurs in [flash-off period] after the fault type alarm happens, the system will not record the two alarms.)

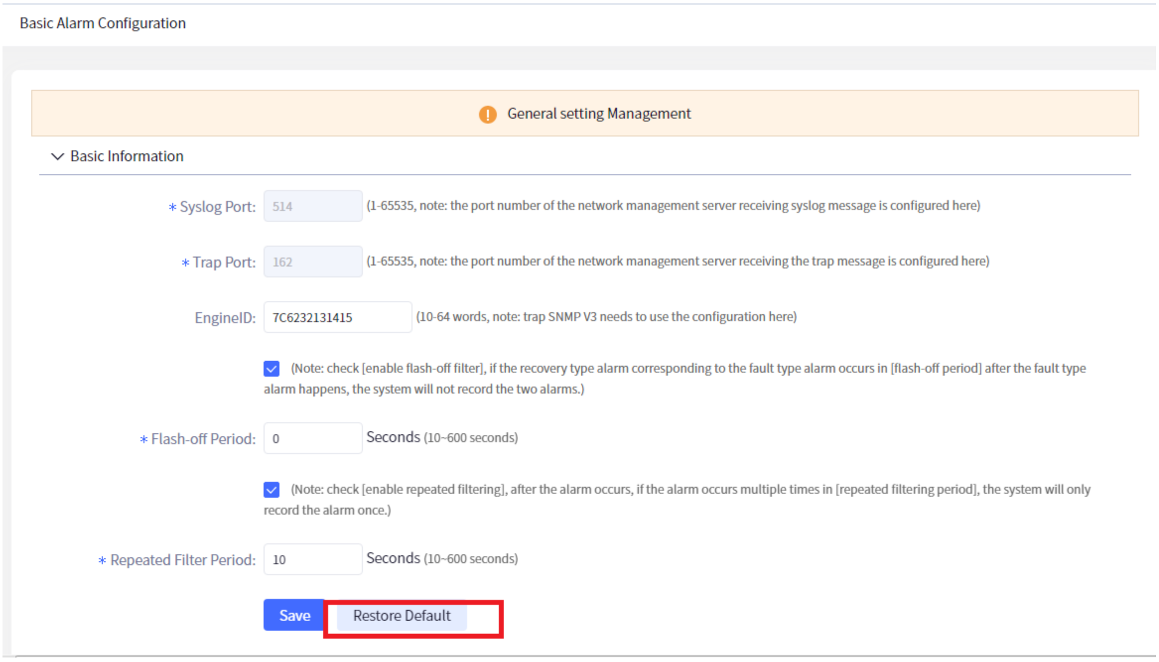
∗ Flash-off Period: 0 Seconds (10~600 seconds)

☑ (Note: check [enable repeated filtering], after the alarm occurs, if the alarm occurs multiple times in [repeated filtering period], the system will only record the alarm once.)

∗ Repeated Filter Period: 10 Seconds (10~600 seconds)

Figure 11.2.7.2 Basic configuration

To restore the basic configuration, just click **Restore Default**. The SYSLOG port number is 514, the TRAP port number is 162, the flash-off filter is not enabled by default, the repeated filter is enabled by default, and the repeated filter period is 10 seconds. The effect is shown in the figure.


Basic Alarm Configuration

General setting Management

Basic Information

* Syslog Port: 514 (1-65535, note: the port number of the network management server receiving syslog message is configured here)

* Trap Port: 162 (1-65535, note: the port number of the network management server receiving the trap message is configured here)

EngineID: 7C6232131415 (10-64 words, note: trap SNMP V3 needs to use the configuration here)

☑ (Note: check [enable flash-off filter], if the recovery type alarm corresponding to the fault type alarm occurs in [flash-off period] after the fault type alarm happens, the system will not record the two alarms.)

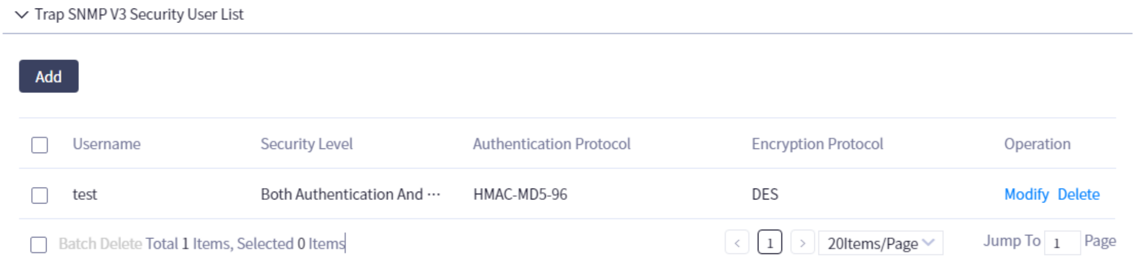
* Flash-off Period: 0 Seconds (10~600 seconds)

☑ (Note: check [enable repeated filtering], after the alarm occurs, if the alarm occurs multiple times in [repeated filtering period], the system will only record the alarm once.)

* Repeated Filter Period: 10 Seconds (10~600 seconds)

Figure 11.2.7.3 Restore default basic configuration

The trap SNMP V3 security user is used to add, modify and delete SNMP V3 users. The effect is shown in the figure.


Trap SNMP V3 Security User List

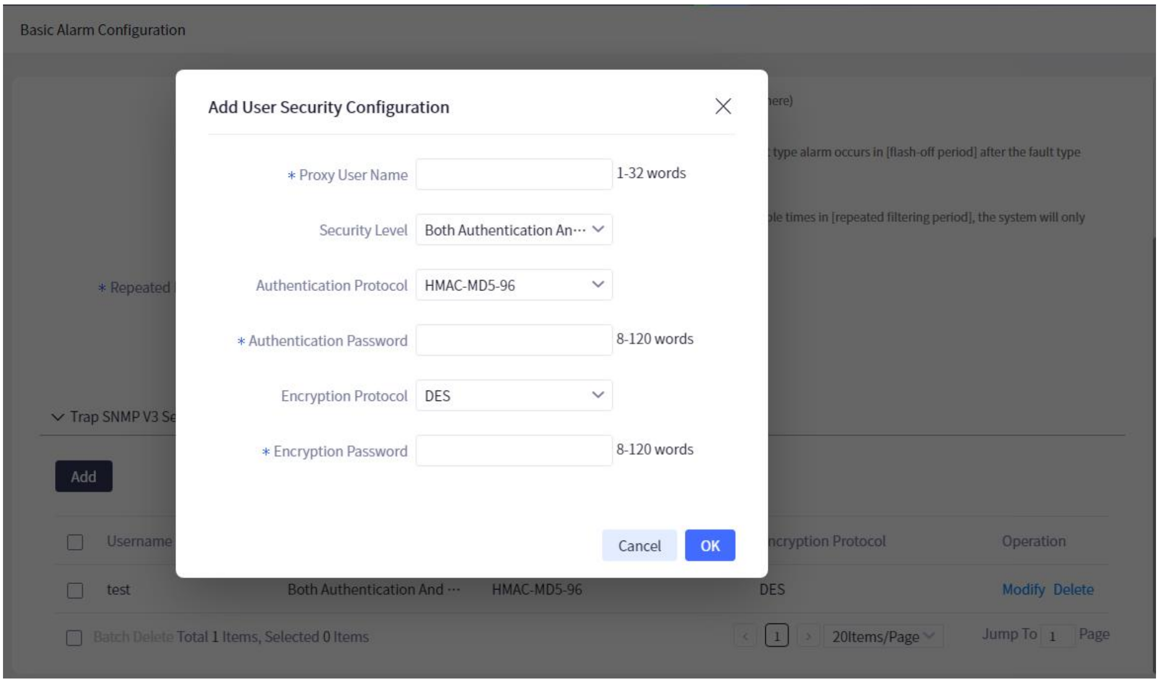
☐	Username	Security Level	Authentication Protocol	Encryption Protocol	Operation
☐	test	Both Authentication And ···	HMAC-MD5-96	DES	Modify Delete

☐ Batch Delete Total 1 Items, Selected 0 Items

Figure 11.2.7.4 Security user list

Add security users:

First, click the **Add** button in the upper left corner of the trap SNMP V3 security user list to open a **Add User Security Configuration** interface. The user needs to fill in the proxy user name and select the security level. If you select both authentication and encryption for the security level, you need to select the authentication protocol, fill in the authentication password, select the encryption protocol, and fill in the encryption password. If only authentication without encryption is selected for the security level, you need to select the authentication protocol and fill in the authentication password. If the user selects no authentication and no encryption, click **OK**, and the effect is shown in the figure.

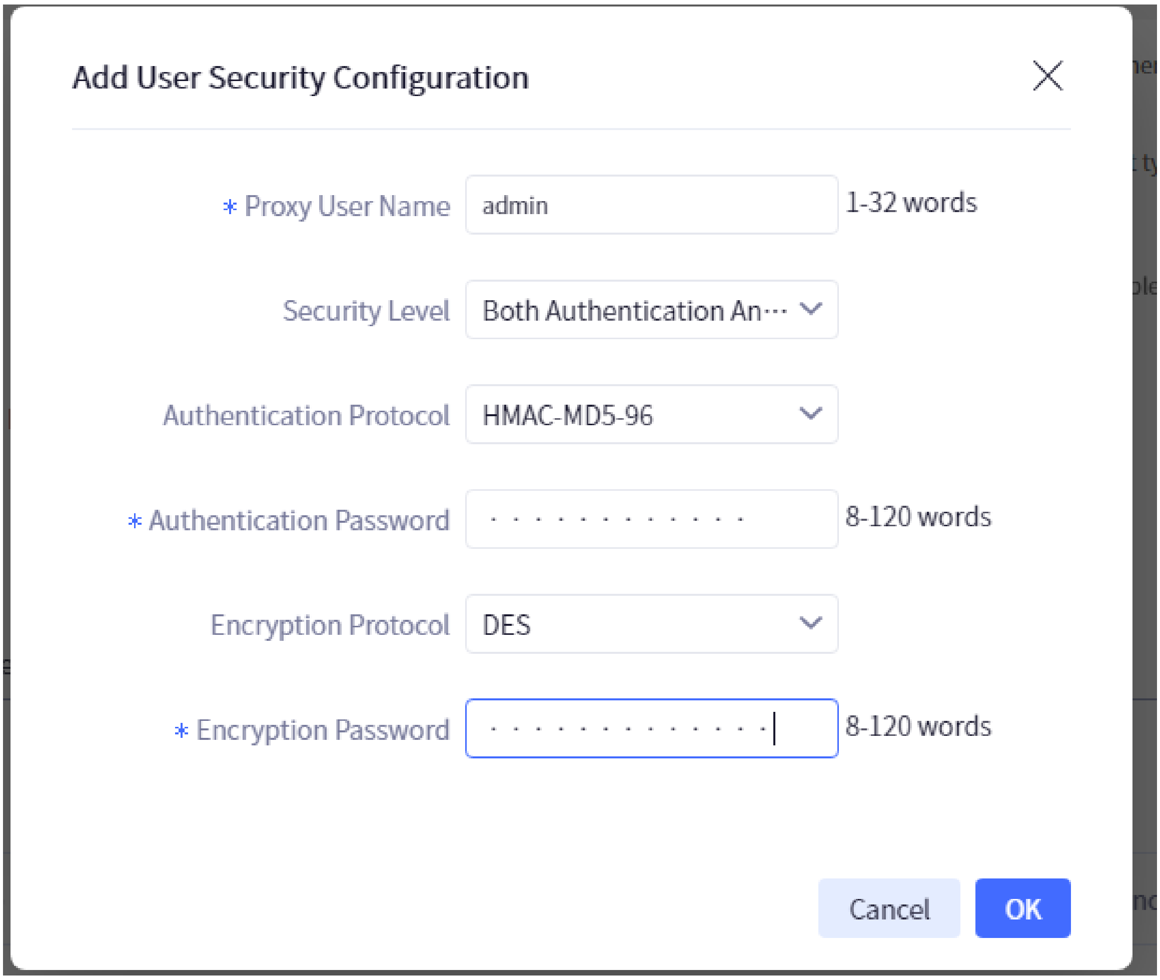

Basic Alarm Configuration
here)
type alarm occurs in [flash-off period] after the fault type
le times in [repeated filtering period], the system will only
* Repeated
Trap SNMP V3 Se
Add
Cancel
OK

Add User Security Configuration

* Proxy User Name: (empty) 1-32 words
Security Level: Both Authentication An···
Authentication Protocol: HMAC-MD5-96
* Authentication Password: (empty) 8-120 words
Encryption Protocol: DES
* Encryption Password: (empty) 8-120 words

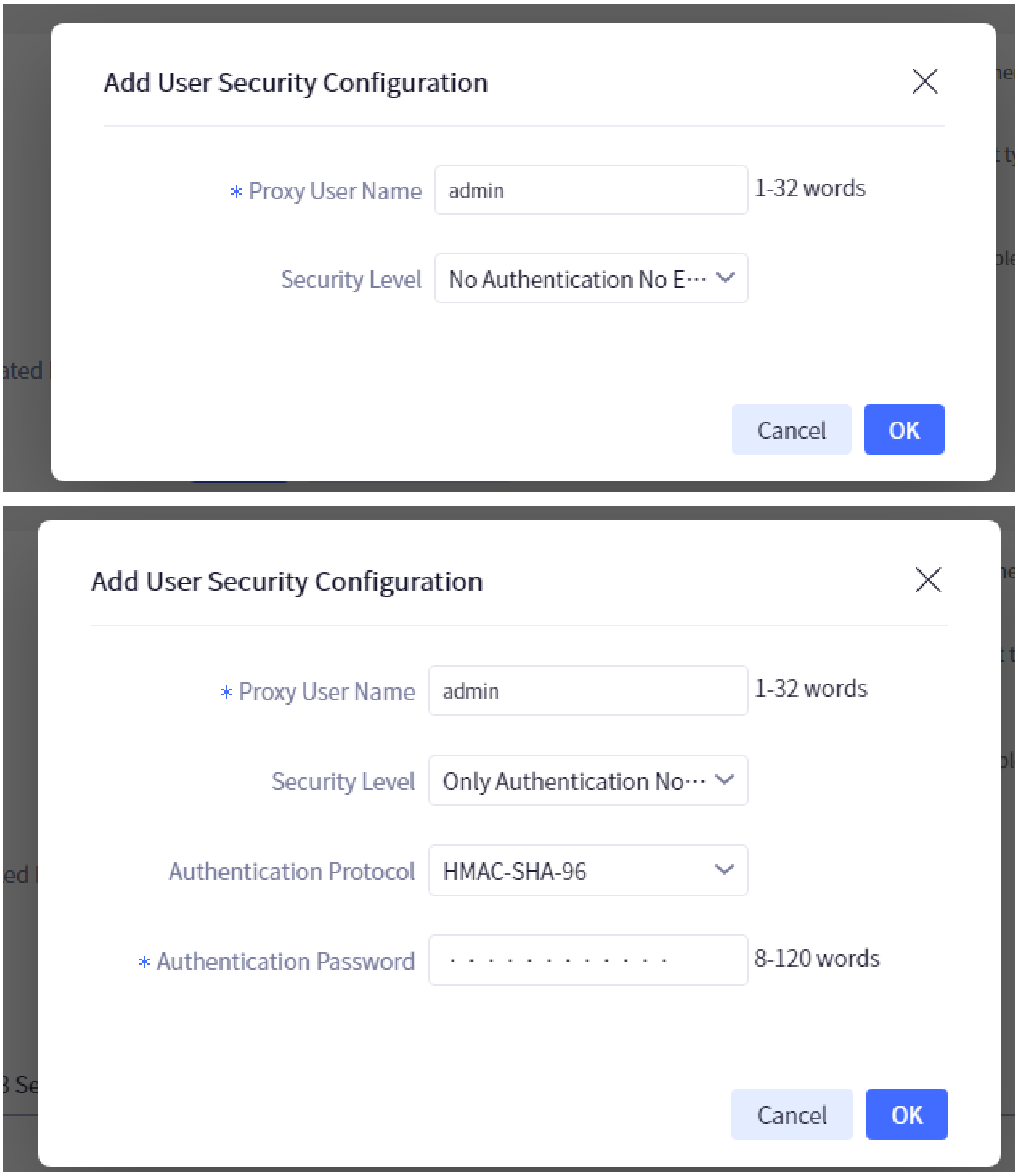
☐	Username			ncryption Protocol	Operation
☐	test	Both Authentication And ···	HMAC-MD5-96	DES	Modify Delete

☐ Batch Delete Total 1 Items, Selected 0 Items ‹ 1 › 20Items/Page Jump To 1 Page



Add User Security Configuration

* Proxy User Name: admin 1-32 words
Security Level: Both Authentication An···
Authentication Protocol: HMAC-MD5-96
* Authentication Password: · · · · · · · · · · · · 8-120 words
Encryption Protocol: DES
* Encryption Password: · · · · · · · · · · · · · 8-120 words



Add User Security Configuration

* Proxy User Name: admin (1-32 words)

Security Level: No Authentication No E···

Add User Security Configuration

* Proxy User Name: admin (1-32 words)

Security Level: Only Authentication No···

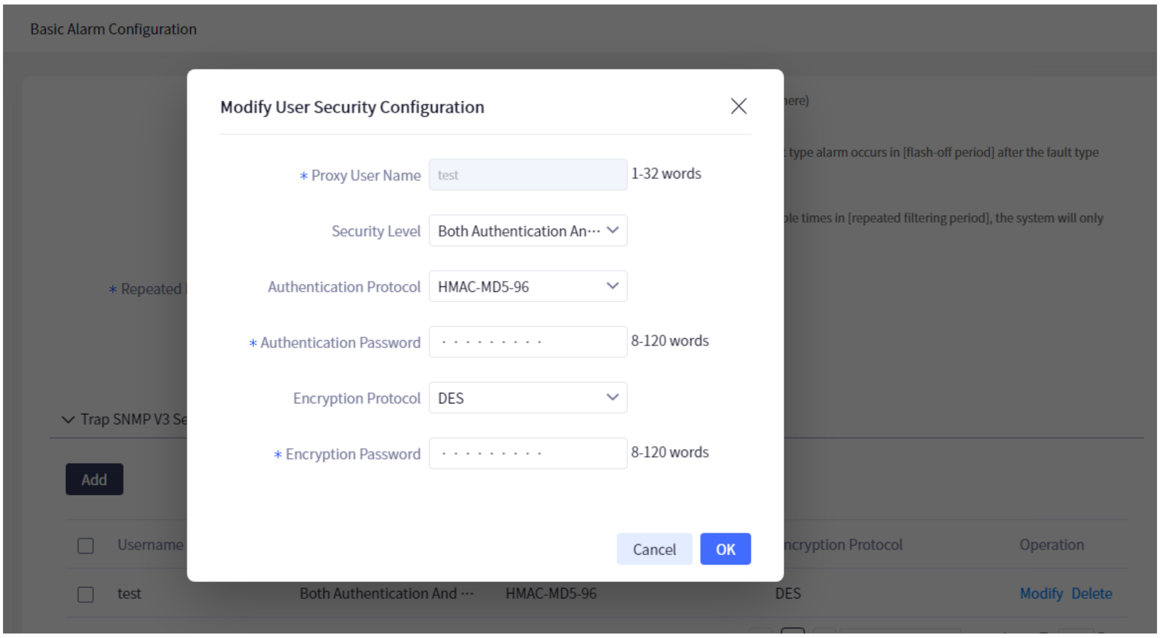
Authentication Protocol: HMAC-SHA-96

* Authentication Password: · · · · · · · · · · · · (8-120 words)

Figure 11.2.7.5 Add security users

Edit security user:

First, select a security user in the trap SNMP V3 security user list, and then click the **Modify** button in the upper left corner of the user list to open the **Modify User Security Configuration** interface. Users can modify the user configuration according to their own needs. Only the proxy user name cannot be modified. The effect is shown in the figure.



Basic Alarm Configuration

Modify User Security Configuration

* Proxy User Name: test (1-32 words)

Security Level: Both Authentication An···

Authentication Protocol: HMAC-MD5-96

* Authentication Password: ········· (8-120 words)

Encryption Protocol: DES

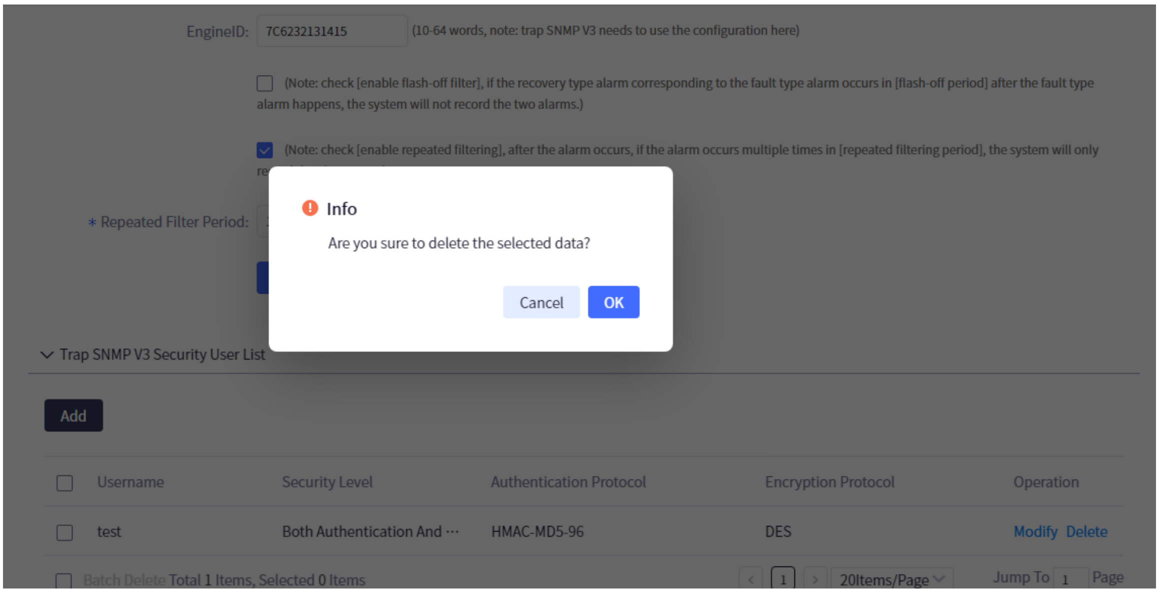
* Encryption Password: ········· (8-120 words)

☐	Username	Security Level	Authentication Protocol	Encryption Protocol	Operation
☐	test	Both Authentication And ···	HMAC-MD5-96	DES	Modify Delete

Figure 11.2.7.6 Modify the security user

Delete a security user:

First, select one or more security users in the TRAP SNMP V3 security user list, then click the **Delete** button in the upper left corner of the user list to pop up a prompt box, and then click the **OK** button in the prompt box. The effect is shown in the figure.



EngineID: 7C6232131415 (10-64 words, note: trap SNMP V3 needs to use the configuration here)

☐ (Note: check [enable flash-off filter], if the recovery type alarm corresponding to the fault type alarm occurs in [flash-off period] after the fault type alarm happens, the system will not record the two alarms.)

☑ (Note: check [enable repeated filtering], after the alarm occurs, if the alarm occurs multiple times in [repeated filtering period], the system will only

* Repeated Filter Period:

Info

Are you sure to delete the selected data?

Trap SNMP V3 Security User List

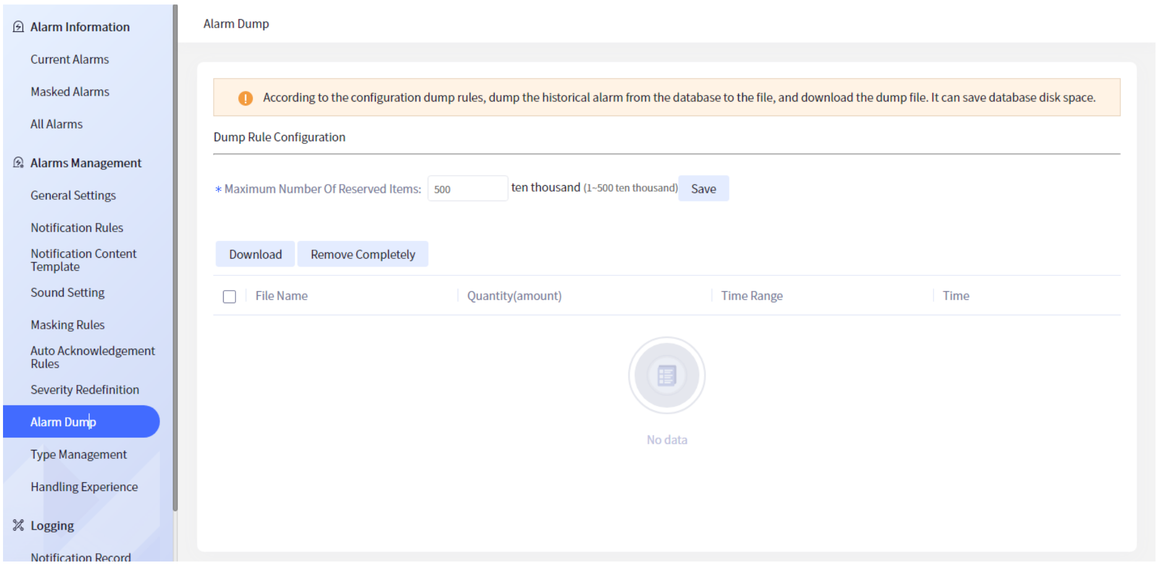
☐	Username	Security Level	Authentication Protocol	Encryption Protocol	Operation
☐	test	Both Authentication And ···	HMAC-MD5-96	DES	Modify Delete

☐ Batch Delete Total 1 Items, Selected 0 Items

Figure 11.2.7.7 Delete the security user

11.2.8 Alarm Dump

Alarm dump is used to configure the conditions that trigger alarm dump operations. Only one parameter **Maximum Number of Reserved Items** needs to be configured. If it is not modified, the default value is 5million. When the alarm data exceeds 5million, the alarm dump operation will be triggered, and the dumped files 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 the figure. (unit of dump: day)



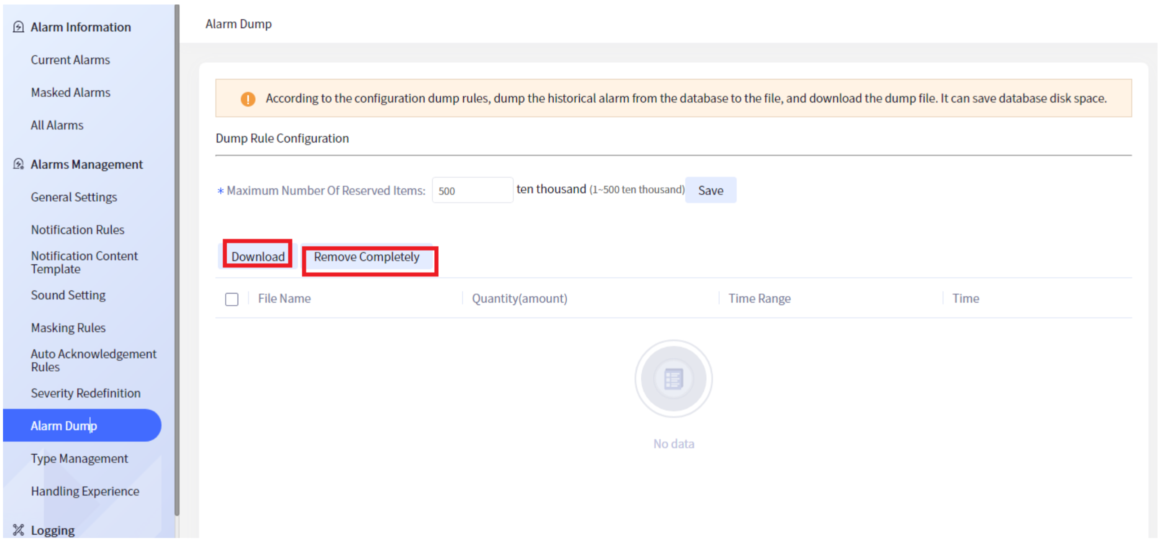
According to the configuration dump rules, dump the historical alarm from the database to the file, and download the dump file. It can save database disk space.

* Maximum Number Of Reserved Items: 500 ten thousand (1~500 ten thousand)

Figure 11.2.8.1 Alarm dump

Users can also download and completely delete dumped files on the interface.

The user selects one or more files in the dump list, and then clicks the **Download** button to download the dumped files. The user selects one or more files, and then clicks the **Remove Completely** button to delete the selected dumped file. The effect is as shown in the figure.



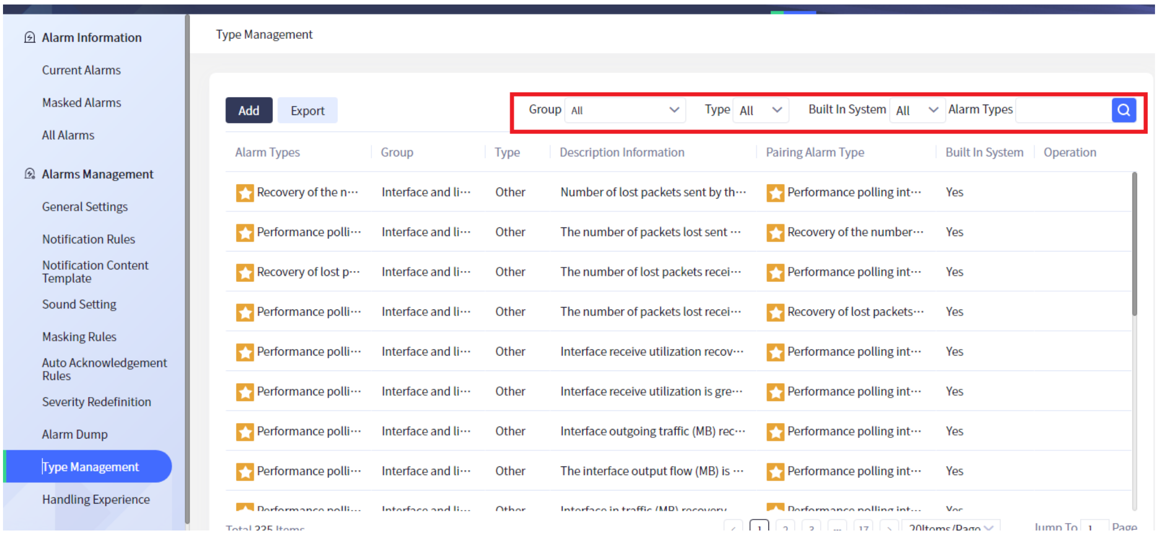
According to the configuration dump rules, dump the historical alarm from the database to the file, and download the dump file. It can save database disk space.

* Maximum Number Of Reserved Items: 500 ten thousand (1~500 ten thousand)

Figure 11.2.8.2 Download/delete the alarm dump file

11.2.9 Alarm Type Management

Alarm type management is used to manage alarm types. Users can query, add, edit, delete and export alarm types (only new alarm types can be edited and deleted, and built-in alarm types cannot be edited and deleted). In the **Type Management** interface, the user can fuzzy query the alarm type by the name of the alarm type, or select the group of the alarm type, and the type and whether it is a built-in condition to accurately query the alarm type. The effect is shown in the figure.

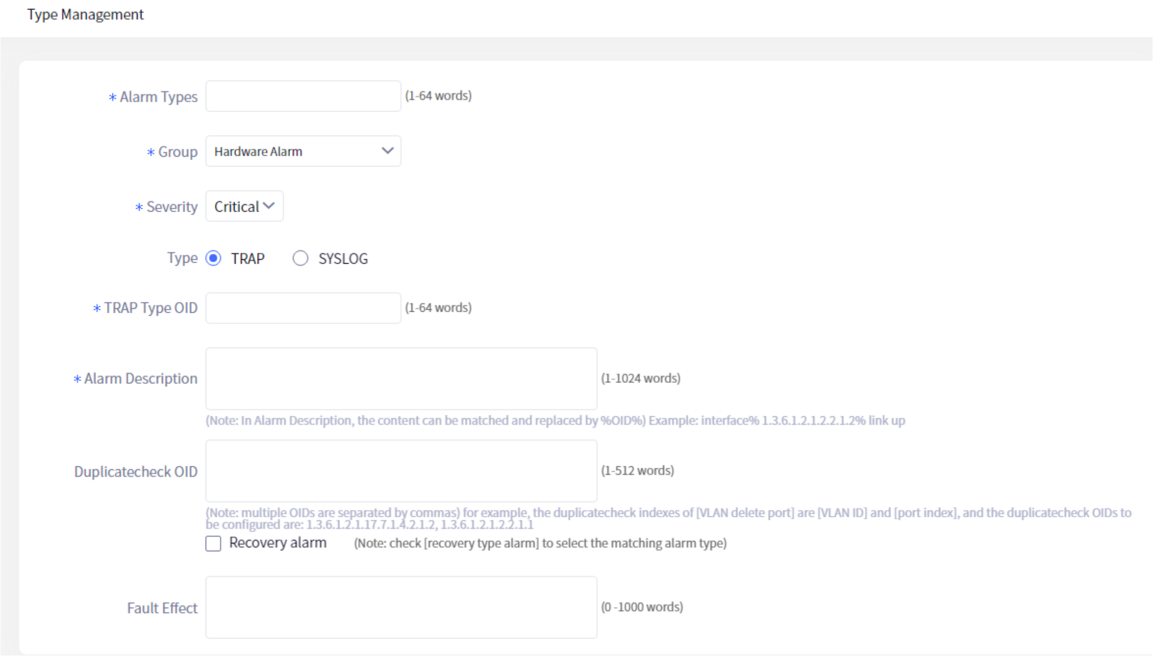


Group All Type All Built In System All Alarm Types

Alarm Types	Group	Type	Description Information	Pairing Alarm Type	Built In System	Operation
Recovery of the n···	Interface and li···	Other	Number of lost packets sent by th···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	The number of packets lost sent ···	Recovery of the number···	Yes	
Recovery of lost p···	Interface and li···	Other	The number of lost packets recei···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	The number of packets lost recei···	Recovery of lost packets···	Yes	
Performance polli···	Interface and li···	Other	Interface receive utilization recov···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	Interface receive utilization is gre···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	Interface outgoing traffic (MB) rec···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	The interface output flow (MB) is ···	Performance polling int···	Yes	

Figure 11.2.9.1 Alarm type management

The user can click the **Add** button to add an alarm type. The information to be filled in is the alarm type name, the group and the severity. Thee information is required items, and the effect is shown in the figure.


Type Management

∗ Alarm Types (1-64 words)

∗ Group: Hardware Alarm

∗ Severity: Critical

Type ● TRAP ○ SYSLOG

∗ TRAP Type OID (1-64 words)

∗ Alarm Description (1-1024 words)

(Note: In Alarm Description, the content can be matched and replaced by %OID%) Example: interface% 1.3.6.1.2.1.2.2.1.2% link up

Duplicatecheck OID (1-512 words)

(Note: multiple OIDs are separated by commas) for example, the duplicatecheck indexes of [VLAN delete port] are [VLAN ID] and [port index], and the duplicatecheck OIDs to be configured are: 1.3.6.1.2.1.17.7.1.4.2.1.2, 1.3.6.1.2.1.2.2.1.1

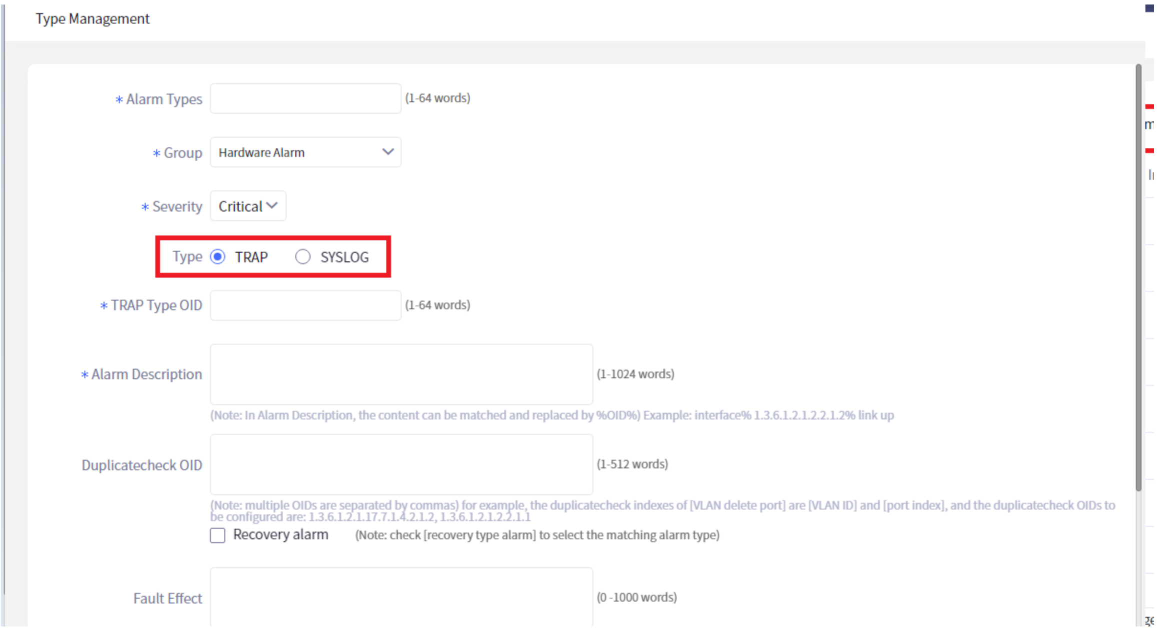
☐ Recovery alarm (Note: check [recovery type alarm] to select the matching alarm type)

Fault Effect (0 -1000 words)

Figure 11.2.9.2 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 type oid (required), alarm description (required), duplicate check oid, fault effect, fault cause and processing suggestions. The effect is shown in the figure.



Type Management

* Alarm Types (1-64 words)

* Group: Hardware Alarm

* Severity: Critical

Type: ● TRAP ○ SYSLOG

* TRAP Type OID (1-64 words)

* Alarm Description (1-1024 words)

(Note: In Alarm Description, the content can be matched and replaced by %OID%) Example: interface% 1.3.6.1.2.1.2.2.1.2% link up

Duplicatecheck OID (1-512 words)

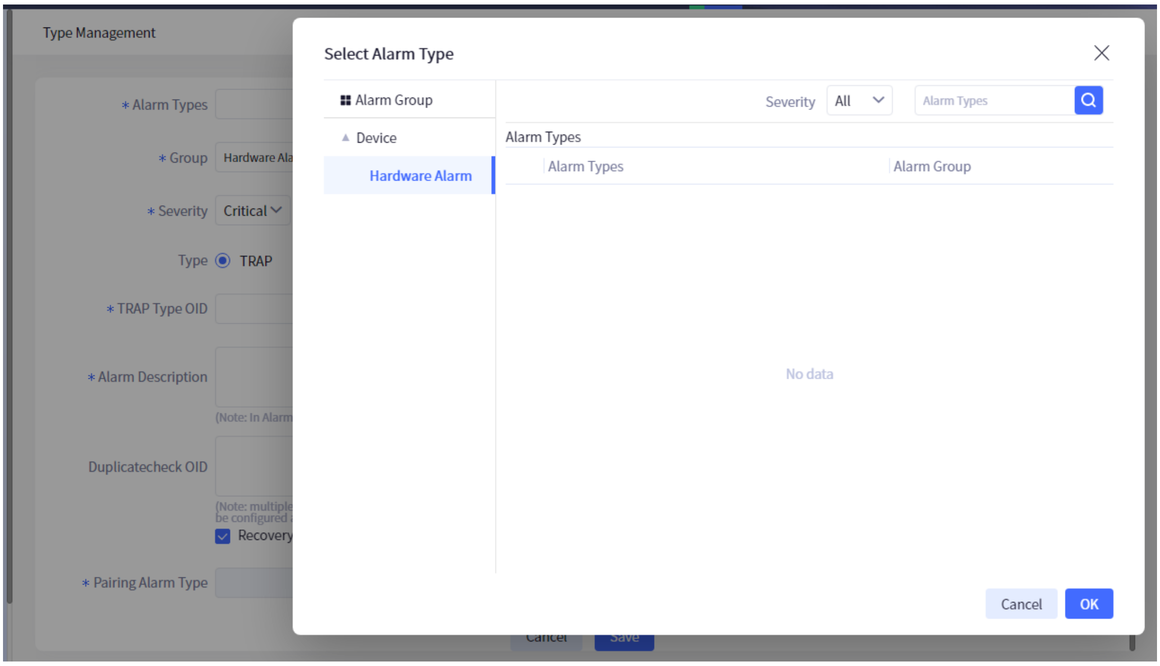
(Note: multiple OIDs are separated by commas) for example, the duplicatecheck indexes of [VLAN delete port] are [VLAN ID] and [port index], and the duplicatecheck OIDs to be configured are: 1.3.6.1.2.1.17.7.1.4.2.1.2, 1.3.6.1.2.1.2.2.1.1

☐ Recovery alarm (Note: check [recovery type alarm] to select the matching alarm type)

Fault Effect (0 -1000 words)

Figure 11.2.9.3 Add TRAP alarm type

If the user selects **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 the figure.



Select Alarm Type

Alarm Group

- Device
  - Hardware Alarm

Severity: All

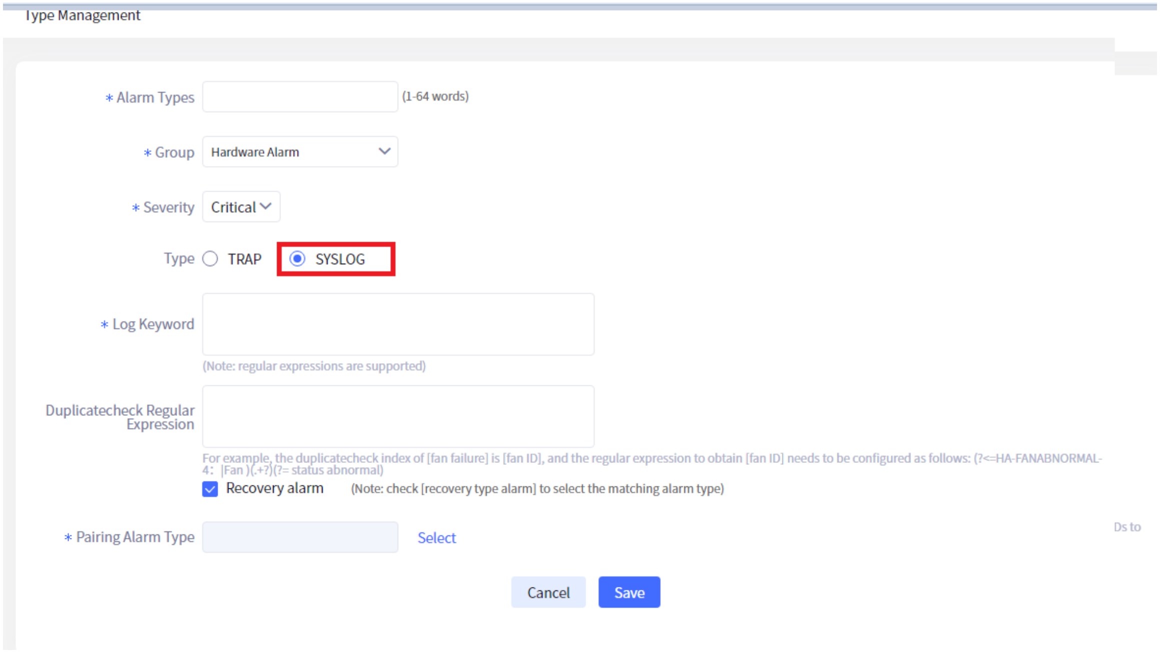
Alarm Types

Alarm Types	Alarm Group

No data

Figure 11.2.9.4 Pair TRAP alarm types

If the user selects syslog, the information to be filled in is the log keyword (required), the re duplicatecheck regular expression, the fault impact, the fault cause and the processing suggestions. The effect is shown in the figure.



∗ Alarm Types (1-64 words)

∗ Group: Hardware Alarm

∗ Severity: Critical

Type ○ TRAP ● SYSLOG

∗ Log Keyword

(Note: regular expressions are supported)

Duplicatecheck Regular Expression

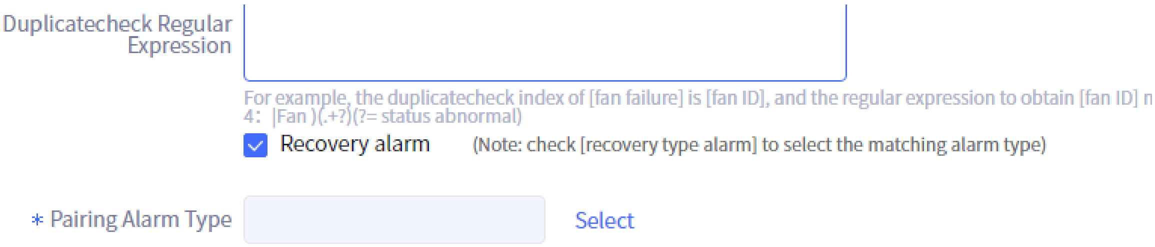
For example, the duplicatecheck index of [fan failure] is [fan ID], and the regular expression to obtain [fan ID] needs to be configured as follows: (?<=HA-FANABNORMAL-4： |Fan)(.+?)(?= status abnormal)

☑ Recovery alarm (Note: check [recovery type alarm] to select the matching alarm type)

∗ Pairing Alarm Type

Figure 11.2.9.5 Add SYSLOG alarm type

If the user selects **Recovery alarm,** the new alarm type is paired with the selected alarm type, and the effect is shown in the figure.



Duplicatecheck Regular Expression

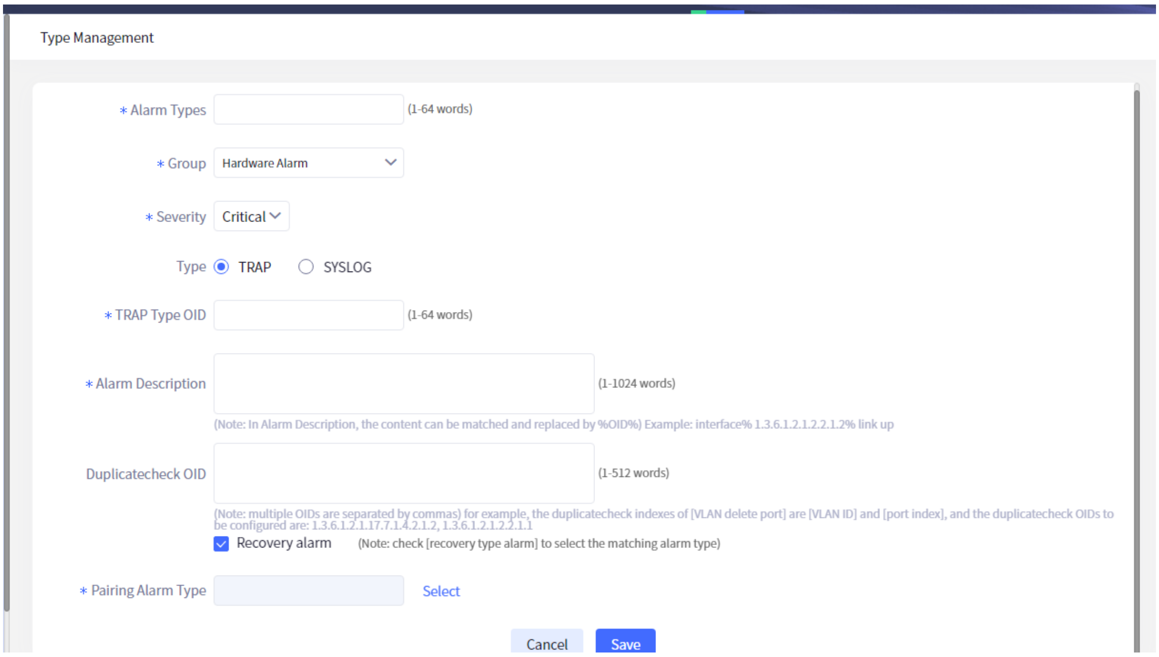
For example, the duplicatecheck index of [fan failure] is [fan ID], and the regular expression to obtain [fan ID] n
4： |Fan)(.+?)(?= status abnormal)

☑ Recovery alarm (Note: check [recovery type alarm] to select the matching alarm type)

∗ Pairing Alarm Type

Figure 11.2.9.6 Pair the SYSLOG alarm types

You can modify the alarm type (new alarm type). Find the desired alarm type, and then click the **Modify** button. The names of the two alarm types cannot be modified. The trap type oid of the trap alarm type cannot be modified, and the others can be modified (the paired alarm type cannot modify its group). When modifying the alarm type, the option "Recovery alarm" cannot be modified, and the effect is shown in the figure.


Type Management

* Alarm Types (1-64 words)

* Group: Hardware Alarm

* Severity: Critical

Type ● TRAP ○ SYSLOG

* TRAP Type OID (1-64 words)

* Alarm Description (1-1024 words)

(Note: In Alarm Description, the content can be matched and replaced by %OID%) Example: interface% 1.3.6.1.2.1.2.2.1.2% link up

Duplicatecheck OID (1-512 words)

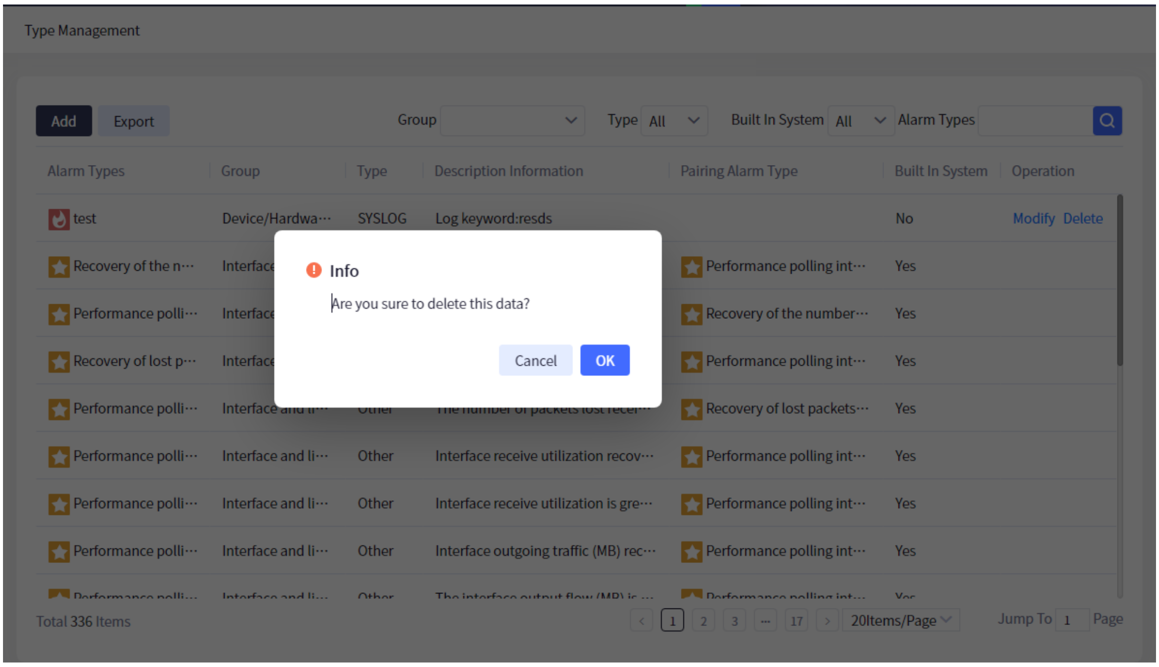
(Note: multiple OIDs are separated by commas) for example, the duplicatecheck indexes of [VLAN delete port] are [VLAN ID] and [port index], and the duplicatecheck OIDs to be configured are: 1.3.6.1.2.1.17.7.1.4.2.1.2, 1.3.6.1.2.1.2.2.1.1

☑ Recovery alarm (Note: check [recovery type alarm] to select the matching alarm type)

* Pairing Alarm Type

Figure 11.2.9.7 Modify the alarm type

You can delete the alarm type (new alarm type). Find the desired alarm type, and then click **Delete** button. A prompt box will appear, and then click the **OK** button in the prompt box. The effect is as shown in the figure.


Type Management

Group: Type: All Built In System: All Alarm Types:

Alarm Types	Group	Type	Description Information	Pairing Alarm Type	Built In System	Operation
test	Device/Hardwa···	SYSLOG	Log keyword:resds		No	Modify Delete
Recovery of the n···	Interface			Performance polling int···	Yes	
Performance polli···	Interface			Recovery of the number···	Yes	
Recovery of lost p···	Interface			Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	The number of packets lost recei···	Recovery of lost packets···	Yes	
Performance polli···	Interface and li···	Other	Interface receive utilization recov···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	Interface receive utilization is gre···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	Interface outgoing traffic (MB) rec···	Performance polling int···	Yes	

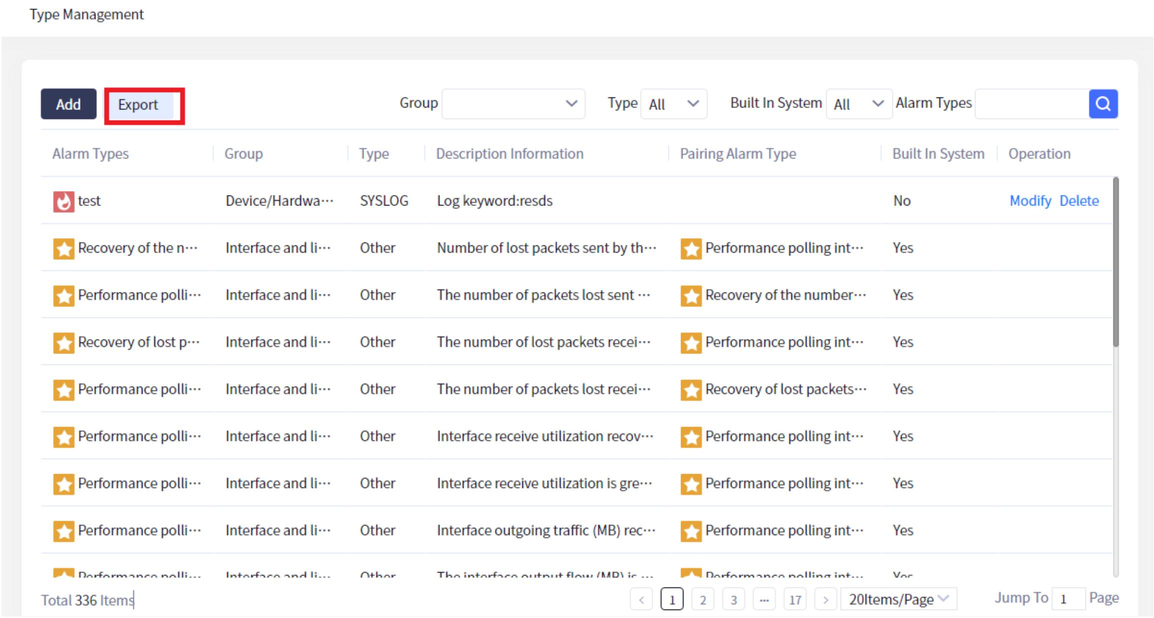
Info

Are you sure to delete this data?

Total 336 Items

Figure 11.2.9.8 Delete the alarm type

Users can export alarm types. Click **Export** on the interface. The exported content is the query content.

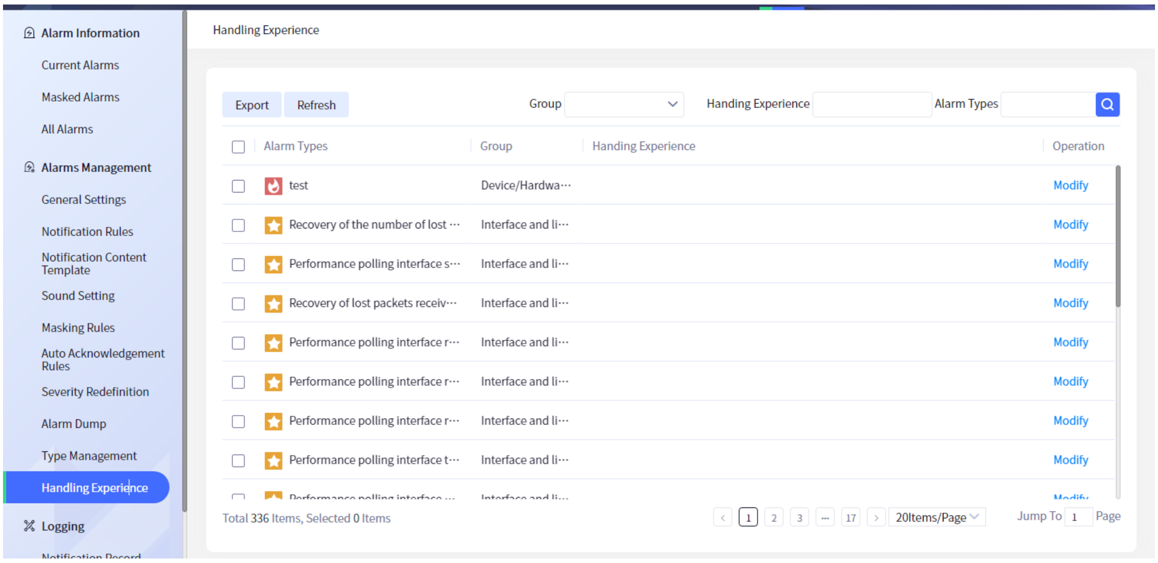


Alarm Types	Group	Type	Description Information	Pairing Alarm Type	Built In System	Operation
test	Device/Hardwa···	SYSLOG	Log keyword:resds		No	Modify Delete
Recovery of the n···	Interface and li···	Other	Number of lost packets sent by th···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	The number of packets lost sent ···	Recovery of the number···	Yes	
Recovery of lost p···	Interface and li···	Other	The number of lost packets recei···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	The number of packets lost recei···	Recovery of lost packets···	Yes	
Performance polli···	Interface and li···	Other	Interface receive utilization recov···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	Interface receive utilization is gre···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	Interface outgoing traffic (MB) rec···	Performance polling int···	Yes	
Performance polli···	Interface and li···	Other	The interface output flow (MB) is ···	Performance polling int···	Yes	

Figure 10.2.9.9 Export alarm types

11.2.10 Handling Experience Management

Handling experience is used to add maintenance experience to alarm types. Users can query, edit, delete and export alarm maintenance experience. In the **Handling Experience** interface, the user can fuzzy query the alarm type by the alarm type name and handling experience, or select the group condition of the alarm type to accurately query the alarm type. The effect is shown in the figure.



☐	Alarm Types	Group	Handing Experience	Operation
☐	test	Device/Hardwa···		Modify
☐	Recovery of the number of lost ···	Interface and li···		Modify
☐	Performance polling interface s···	Interface and li···		Modify
☐	Recovery of lost packets receiv···	Interface and li···		Modify
☐	Performance polling interface r···	Interface and li···		Modify
☐	Performance polling interface r···	Interface and li···		Modify
☐	Performance polling interface r···	Interface and li···		Modify
☐	Performance polling interface t···	Interface and li···		Modify
☐	Performance polling interface ···	Interface and li···		Modify

Figure 11.2.10.1 Handling experience management

The user can select an alarm type on the interface, and then click the **Modify** button to add handling experience to the alarm type. The information to be filled in is alarm maintenance experience (required), and the effect is shown in the figure.

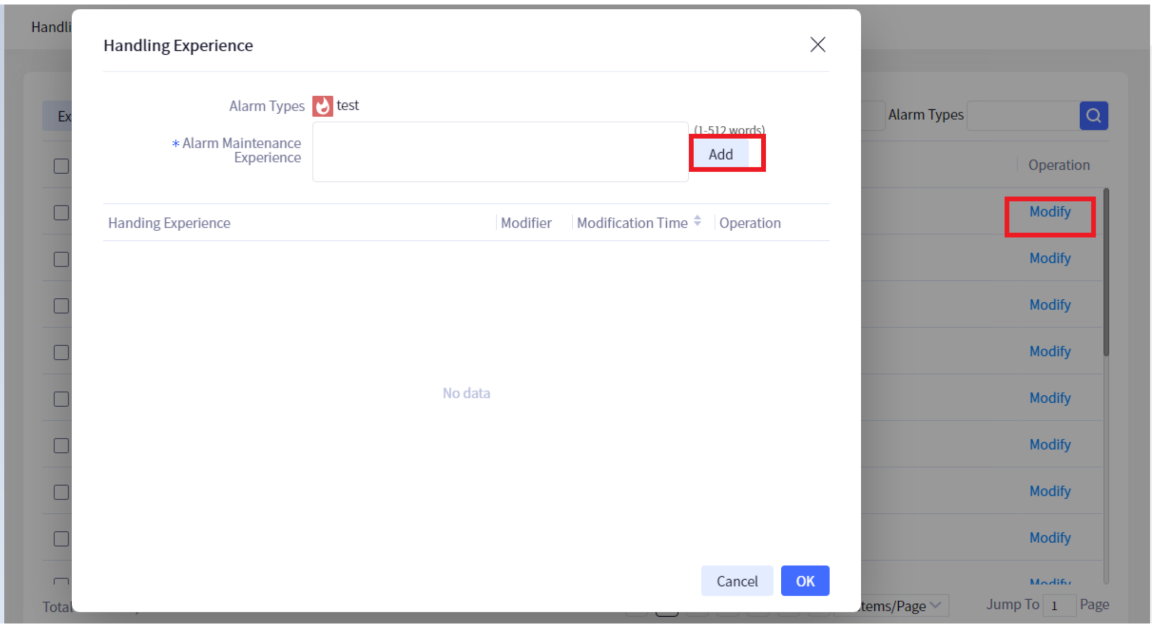
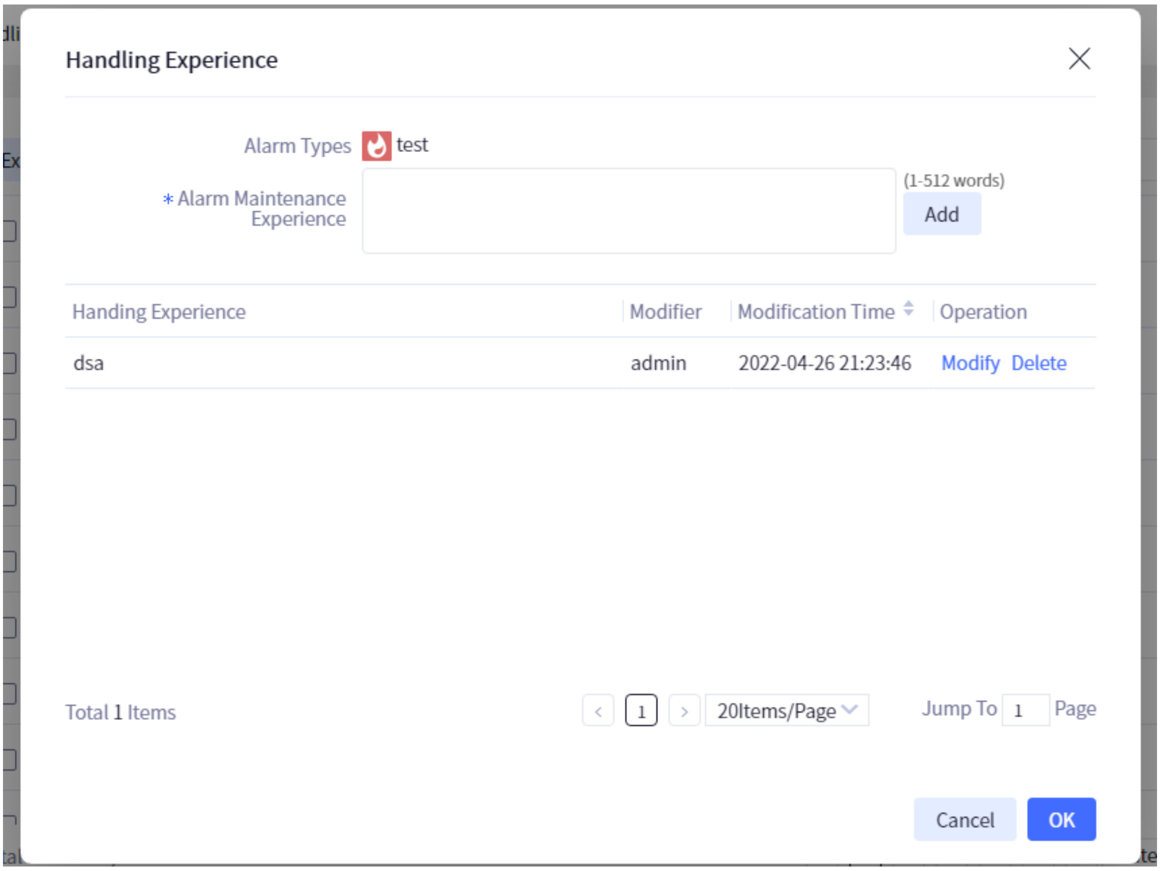


Figure 11.2.10.2 Add alarm maintenance experience

You can modify the alarm handling experience by clicking the **Modify** button. You can also click the **Delete** button to delete the alarm handling experience. One alarm type can correspond to multiple alarm handling experiences, and the effect is shown in the figure.



Handing Experience	Modifier	Modification Time	Operation
dsa	admin	2022-04-26 21:23:46	Modify Delete

Figure 11.2.10.3 Edit/modify the alarm maintenance experience

The user can export the alarm maintenance experience. Click **Export** on the interface.

11.3 Log Records

11.3.1 Notification Records

Click "Alarts&Activity" in the menu bar to open the "Notification Record" page. The email and SMS notified to users can be queried in the notification record module. In the alarm notification interface, users can accurately query by the alarm level, notification status, notification method and notification time, and can also fuzzy query by the alarm source, alarm type and notification user. At the same time, users can also accurately query by the alarm type and alarm source. The effect is shown in the figure.

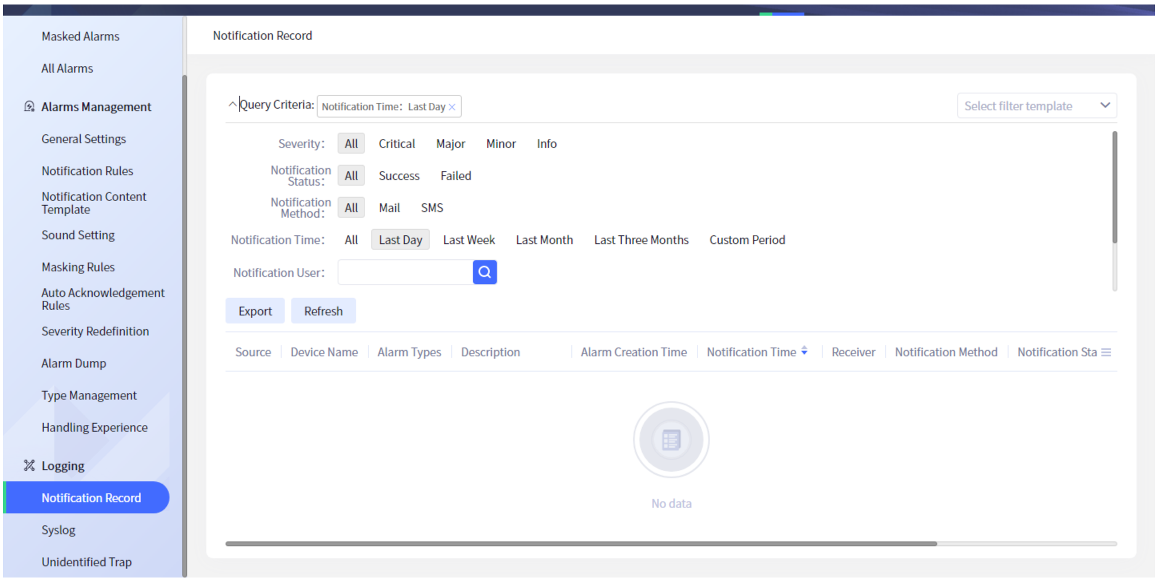
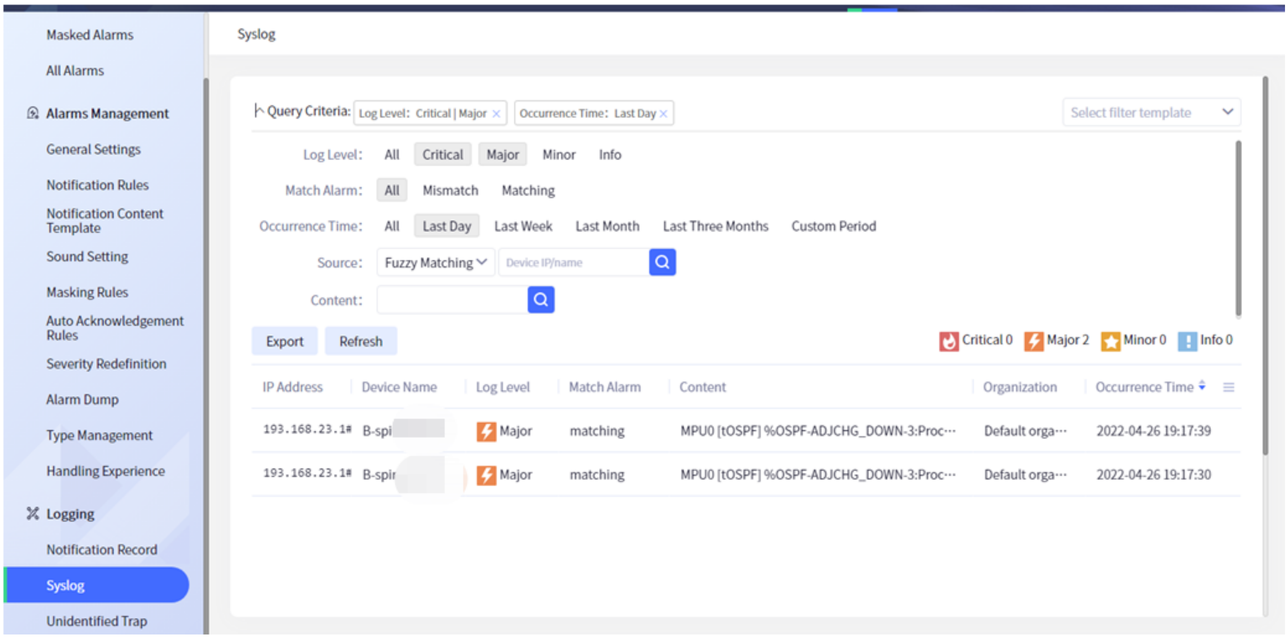


Figure 11.3.1 Notification records

After querying the desired alarm notification records, click **Export** to export the alarm notification records in the list (including paged notification records, which are exported as queried contents).

11.3.2 Syslog Logs

Click "Alerts&Activity" in the menu bar to open the "Syslog" page. In the Syslog log interface, users can accurately query by the log level, matching alarm and occurrence time, and can also fuzzy query the devices and content. At the same time, users can also accurately query the devices. The effect is shown in the figure.



Query Criteria: Log Level: Critical | Major × Occurrence Time: Last Day ×

Log Level: All Critical Major Minor Info

Match Alarm: All Mismatch Matching

Occurrence Time: All Last Day Last Week Last Month Last Three Months Custom Period

Source: Fuzzy Matching Device IP/name

Content:

IP Address	Device Name	Log Level	Match Alarm	Content	Organization	Occurrence Time
193.168.23.1#	B-spi[redacted]	Major	matching	MPU0 [tOSPF] %OSPF-ADJCHG_DOWN-3:Proc···	Default orga···	2022-04-26 19:17:39
193.168.23.1#	B-spir[redacted]	Major	matching	MPU0 [tOSPF] %OSPF-ADJCHG_DOWN-3:Proc···	Default orga···	2022-04-26 19:17:30

Figure 11.3.2.1 .1 Syslog logs

Users can also accurately query through devices. First, select the accurate matching of alarm sources, then click the **Select** button on the right, and then the **Select Device** dialog box will appear. The user can add devices by adding device groups, adding devices, and adding local network management. Finally, click the **OK** button to accurately query by the device. The effect is shown in the figure.

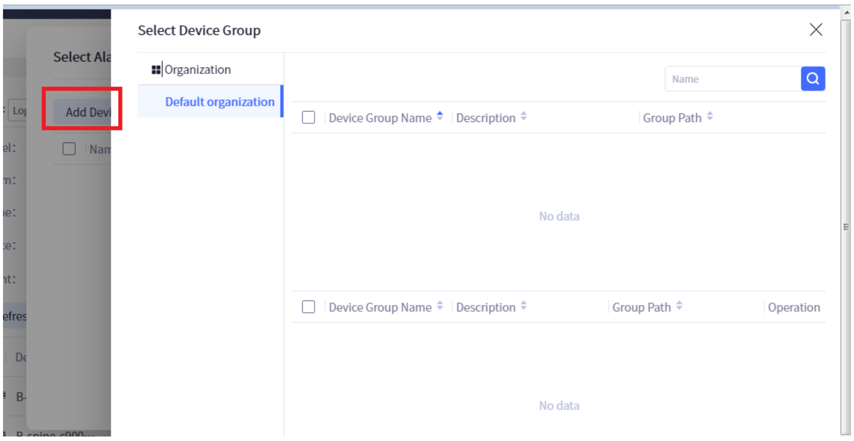
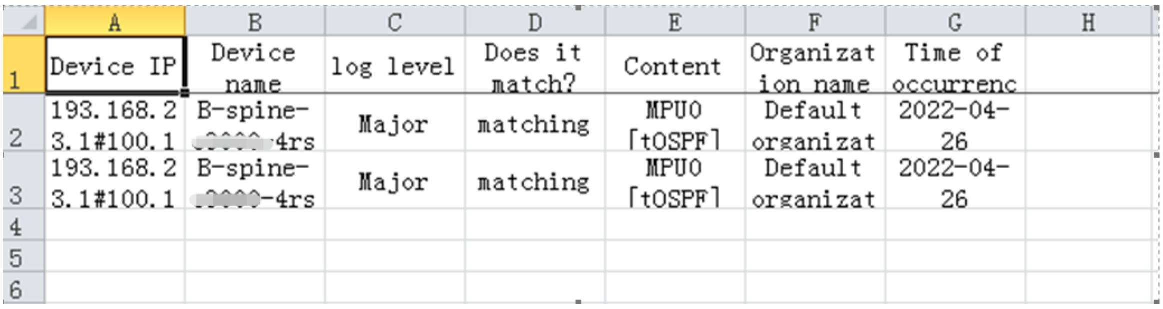


Figure 11. 3.2.2 Query by devices accurately

After querying the desired syslog, click **Export** to export the syslog in the list (including the paged syslog, which is exported as the queried content)



	A	B	C	D	E	F	G	H
1	Device IP	Device name	log level	Does it match?	Content	Organization name	Time of occurrenc	
2	193.168.23.1#100.1	B-spine-[redacted]4rs	Major	matching	MPU0 [tOSPF]	Default organizat	2022-04-26	
3	193.168.23.1#100.1	B-spine-[redacted]-4rs	Major	matching	MPU0 [tOSPF]	Default organizat	2022-04-26	
4								
5								
6								

Figure 11.3..2.3 Export Syslog logs

11.3.3 Un-identified Trap

Click "Alerts&Activity" in the menu bar to open the "Unidentified Trap" page. In the unidentified Trap interface, you can accurately query by the occurrence time, fuzzy query by the device and type oid, and also support the accurate query of the device. The effect is shown in the figure.

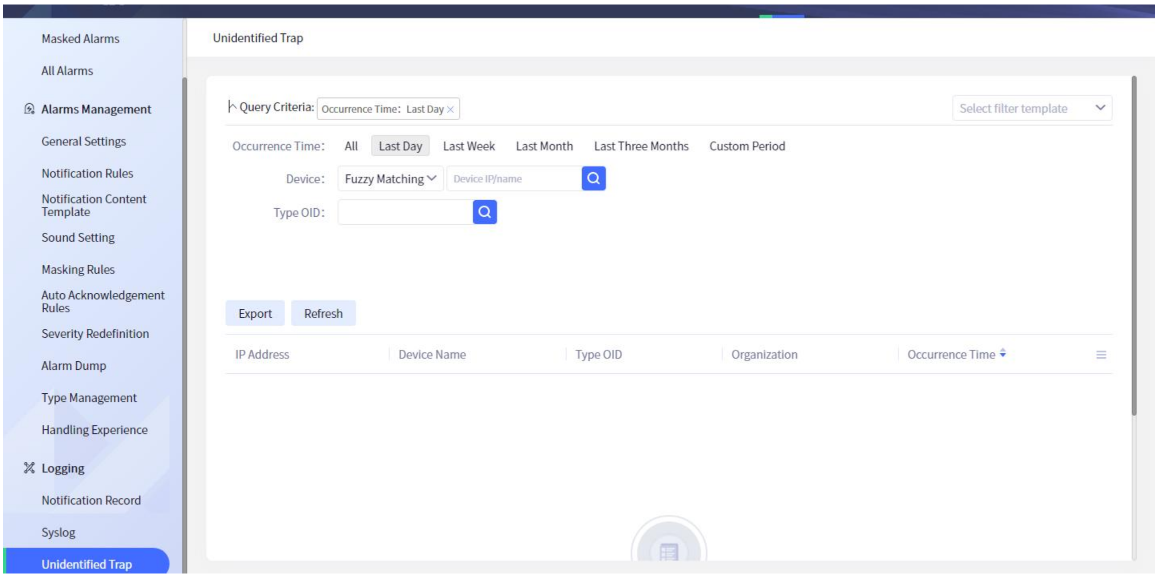


Figure 11.3.3.1 Unidentified Trap

Users can also accurately query through devices. First, select the accurate matching of alarm sources, then click the **Select** button on the right, and then the **Select Device** dialog box will appear. The user can add devices by adding device groups, adding devices, and adding local network management. Finally, click the **OK** button to accurately query by the device. The effect is shown in the figure.

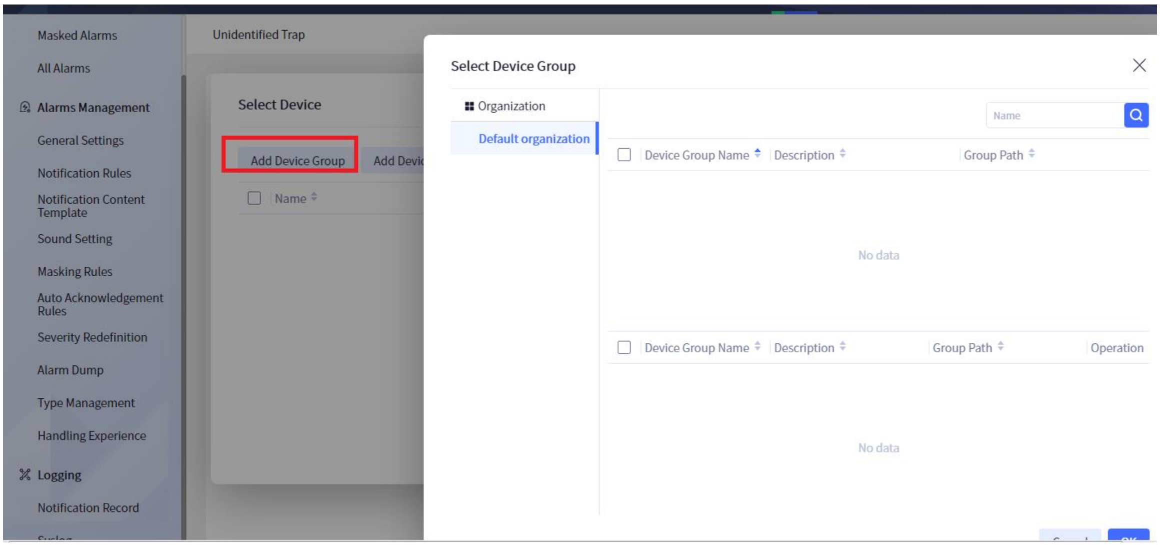


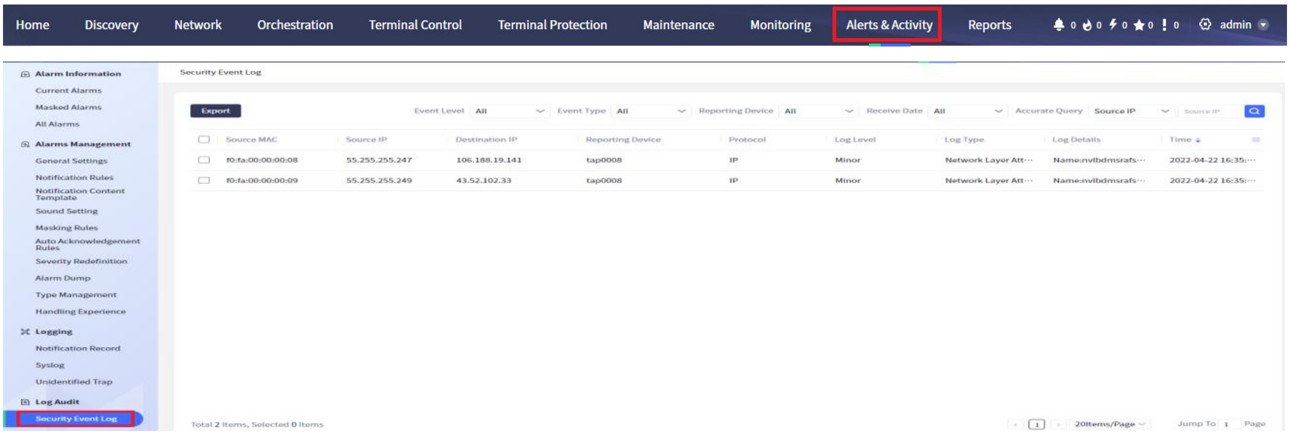
Figure 11.3.3.2 Accurate query by the device

After finding the desired unidentified Trap information, click **Export** to export the unidentified Trap information in the list (including the paged unidentified Trap information).

Log Audit

11.3.4 Security Event Log

Click **Log Alarm** > **Security Event Log** to enter the **Security Event Log** interface, as shown in figure 11.4.1.1 below, to display the details of the security event log, including source MAC, source IP, destination IP and other related information.



Security Event Log

Event Level: All; Event Type: All; Reporting Device: All; Receive Date: All; Accurate Query: Source IP

	Source MAC	Source IP	Destination IP	Reporting Device	Protocol	Log Level	Log Type	Log Details	Time
☐	f0:fa:00:00:00:08	55.255.255.247	106.188.19.141	tap0008	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···
☐	f0:fa:00:00:00:09	55.255.255.249	43.52.102.33	tap0008	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···

Figure 11.4.1.1 Display the security log event

In the current **Security Event Log** interface, users can perform fuzzy query by event level, event type, reporting device and receiving date, and can also perform accurate query by IP. The effect is shown in the figure.

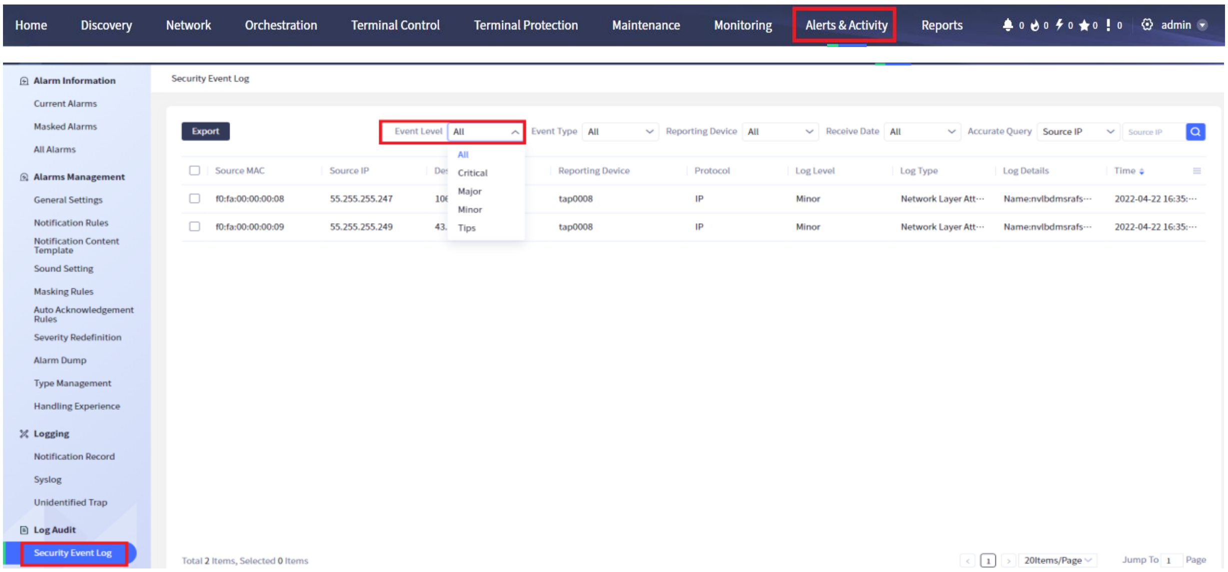
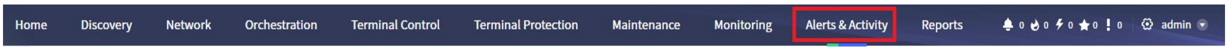
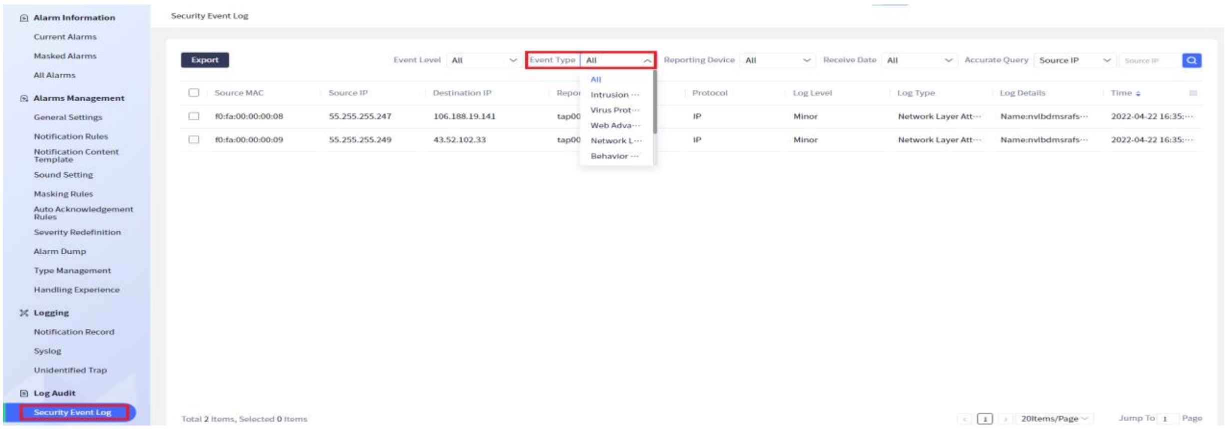


Figure 11.4.1.2 Query security log event by event level

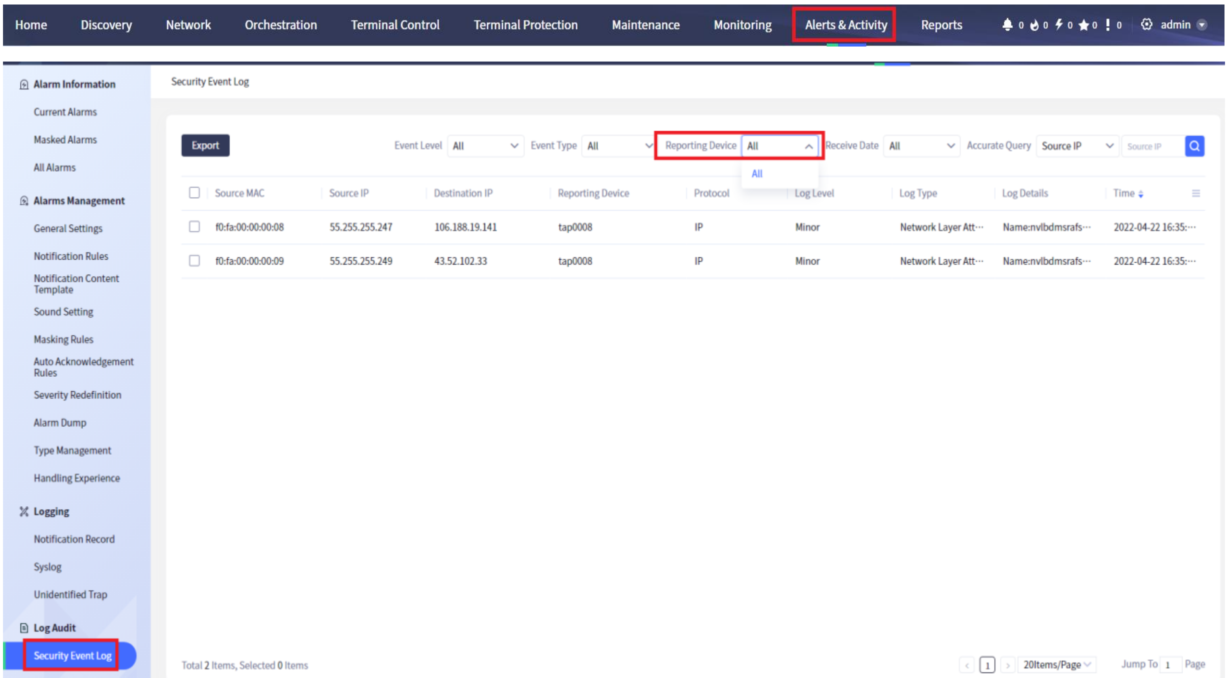




☐	Source MAC	Source IP	Destination IP	Repor	Protocol	Log Level	Log Type	Log Details	Time
☐	f0:fa:00:00:00:08	55.255.255.247	106.188.19.141	tap00	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···
☐	f0:fa:00:00:00:09	55.255.255.249	43.52.102.33	tap00	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···

Total 2 Items, Selected 0 Items

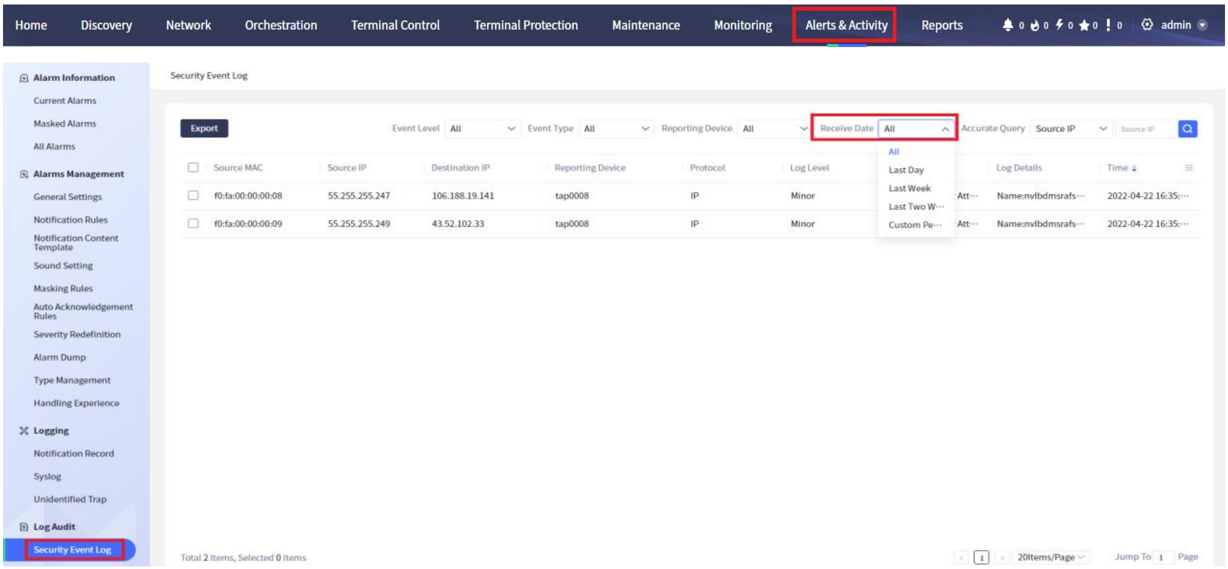
Figure 11.4.1.3 Query security log event by event type



☐	Source MAC	Source IP	Destination IP	Reporting Device	Protocol	Log Level	Log Type	Log Details	Time
☐	f0:fa:00:00:00:08	55.255.255.247	106.188.19.141	tap0008	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···
☐	f0:fa:00:00:00:09	55.255.255.249	43.52.102.33	tap0008	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···

Total 2 Items, Selected 0 Items

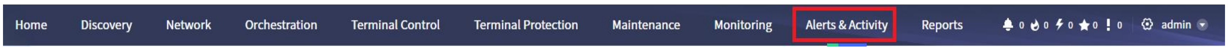
Figure 11.4.1.4 Query security log event by reporting device

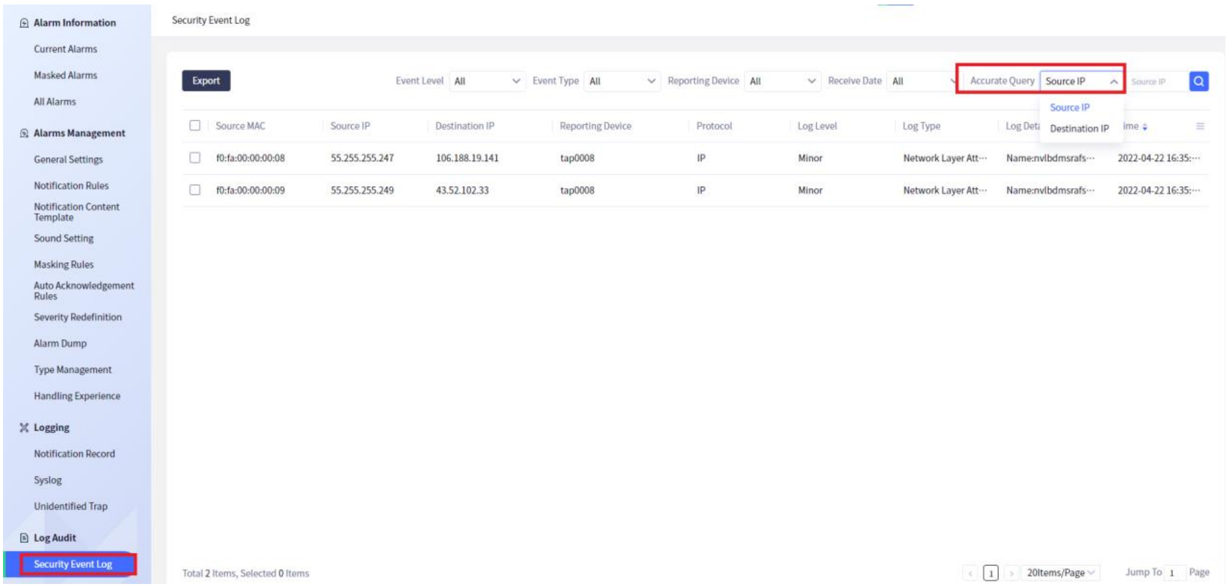


☐	Source MAC	Source IP	Destination IP	Reporting Device	Protocol	Log Level		Log Details	Time
☐	f0:fa:00:00:00:08	55.255.255.247	106.188.19.141	tap0008	IP	Minor	Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···
☐	f0:fa:00:00:00:09	55.255.255.249	43.52.102.33	tap0008	IP	Minor	Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···

Total 2 Items, Selected 0 Items

Figure 11.4.1.5 Query security log event by receiving date



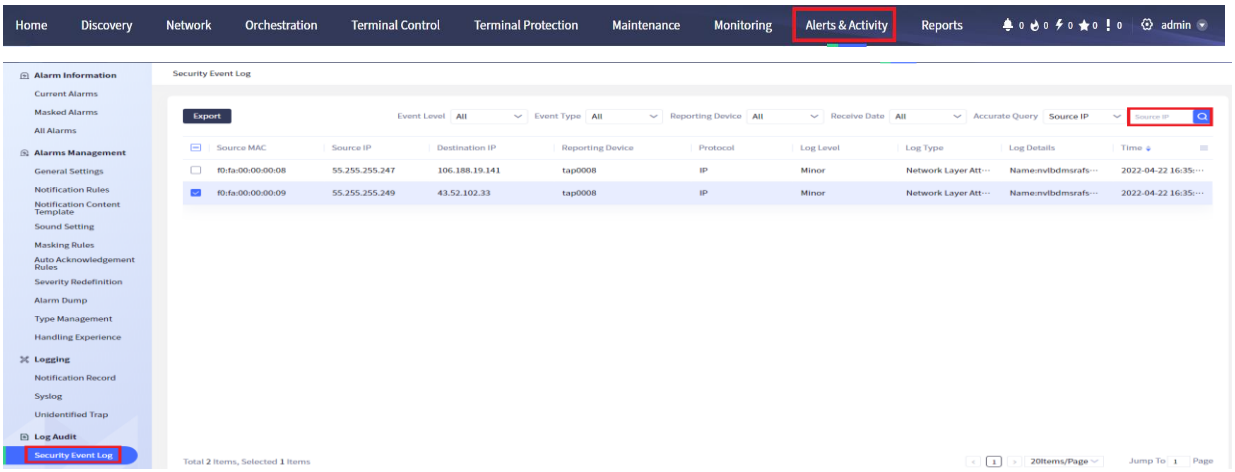


Event Level: All | Event Type: All | Reporting Device: All | Receive Date: All | Accurate Query: Source IP

☐	Source MAC	Source IP	Destination IP	Reporting Device	Protocol	Log Level	Log Type	Log Deta…	…ime
☐	f0:fa:00:00:00:08	55.255.255.247	106.188.19.141	tap0008	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···
☐	f0:fa:00:00:00:09	55.255.255.249	43.52.102.33	tap0008	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···

Total 2 Items, Selected 0 Items

Figure 11.4.1.6 Query security log event by event IP



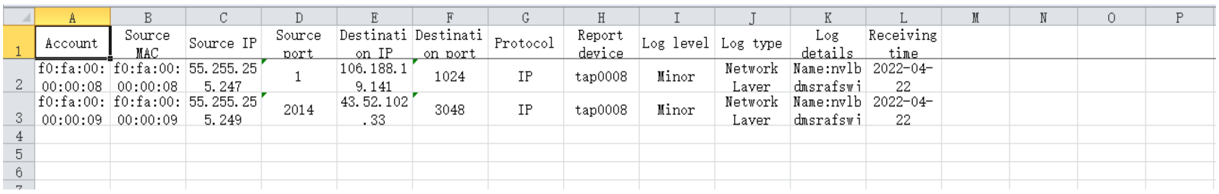
Event Level: All | Event Type: All | Reporting Device: All | Receive Date: All | Accurate Query: Source IP

☐	Source MAC	Source IP	Destination IP	Reporting Device	Protocol	Log Level	Log Type	Log Details	Time
☐	f0:fa:00:00:00:08	55.255.255.247	106.188.19.141	tap0008	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···
☑	f0:fa:00:00:00:09	55.255.255.249	43.52.102.33	tap0008	IP	Minor	Network Layer Att···	Name:nvlbdmsrafs···	2022-04-22 16:35:···

Total 2 Items, Selected 1 Items

Figure 11.4.1.7 Query security log event by source IP

According to the query criteria, click the **Export** button in the upper left corner of the page to export the security events. The exported data is as shown in the figure:

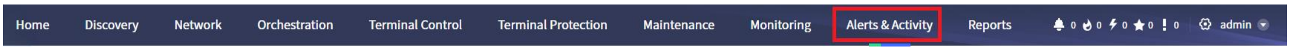


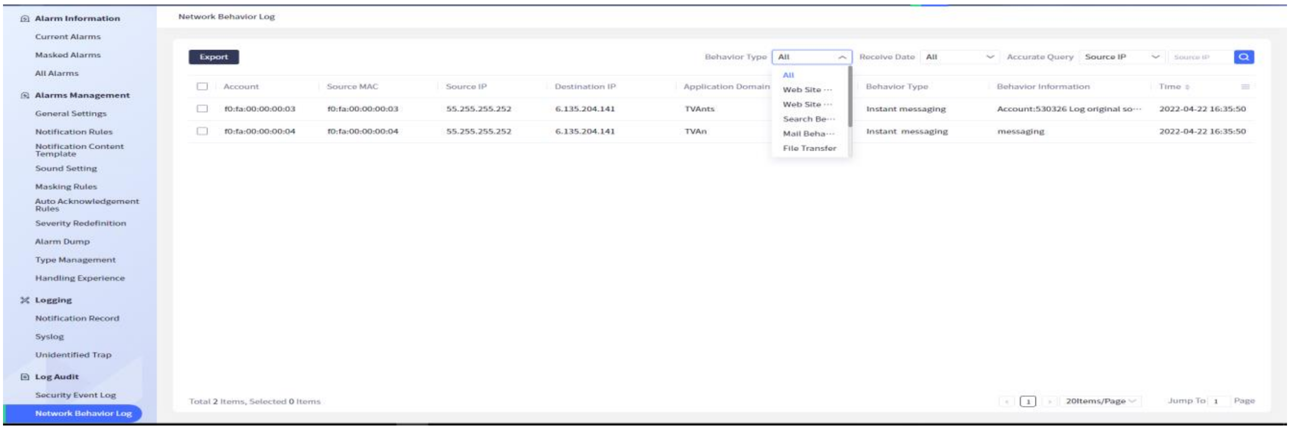
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	Account	Source MAC	Source IP	Source port	Destination IP	Destination port	Protocol	Report device	Log level	Log type	Log details	Receiving time				
2	f0:fa:00:00:00:08	f0:fa:00:00:00:08	55.255.255.247	1	106.188.19.141	1024	IP	tap0008	Minor	Network Laver	Name:nvlbdmsrafswi	2022-04-22				
3	f0:fa:00:00:00:09	f0:fa:00:00:00:09	55.255.255.249	2014	43.52.102.33	3048	IP	tap0008	Minor	Network Laver	Name:nvlbdmsrafswi	2022-04-22				
4																
5																
6																

Figure 11.4.1.8 Export security log events

11.3.5 Network Behavior Log

Click **Alerts&Activity** > **Network Behavior Log** to enter the **Network Behavior Log** interface, as shown in figure 11.4.2.1 below, to display the details of the network behavior log, including user account, source MAC, source IP, destination IP and other related information.



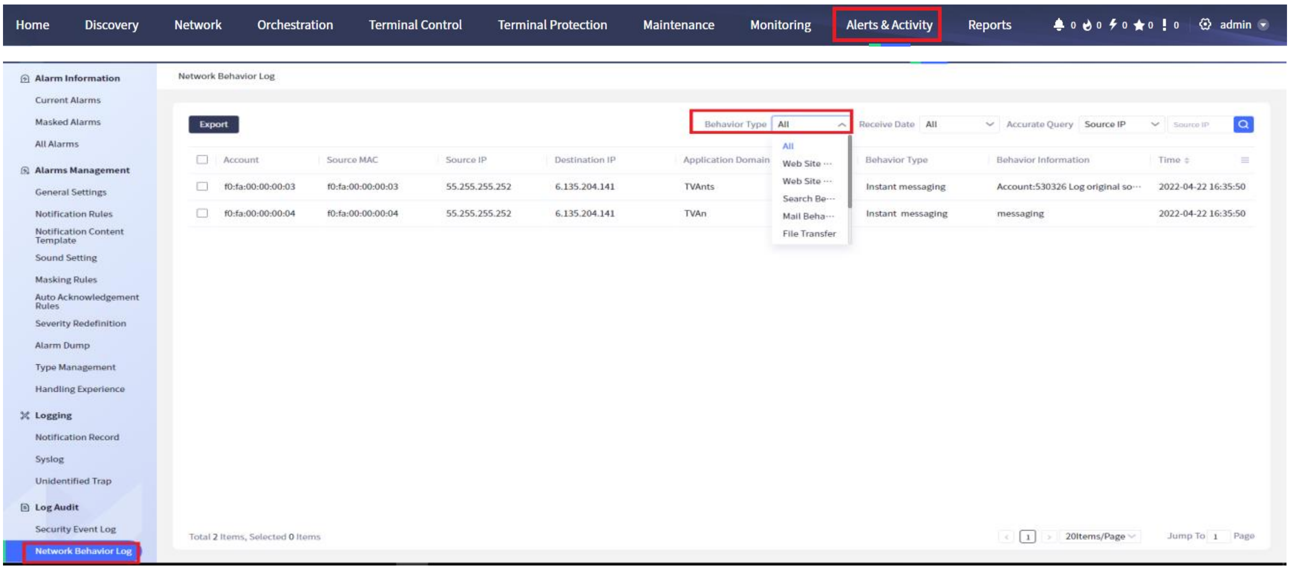


Network Behavior Log

☐	Account	Source MAC	Source IP	Destination IP	Application Domain	Behavior Type	Behavior Information	Time
☐	f0:fa:00:00:00:03	f0:fa:00:00:00:03	55.255.255.252	6.135.204.141	TVAnts	Instant messaging	Account:530326 Log original so···	2022-04-22 16:35:50
☐	f0:fa:00:00:00:04	f0:fa:00:00:00:04	55.255.255.252	6.135.204.141	TVAn	Instant messaging	messaging	2022-04-22 16:35:50

Figure 11.4.2.1 Display the network behavior log

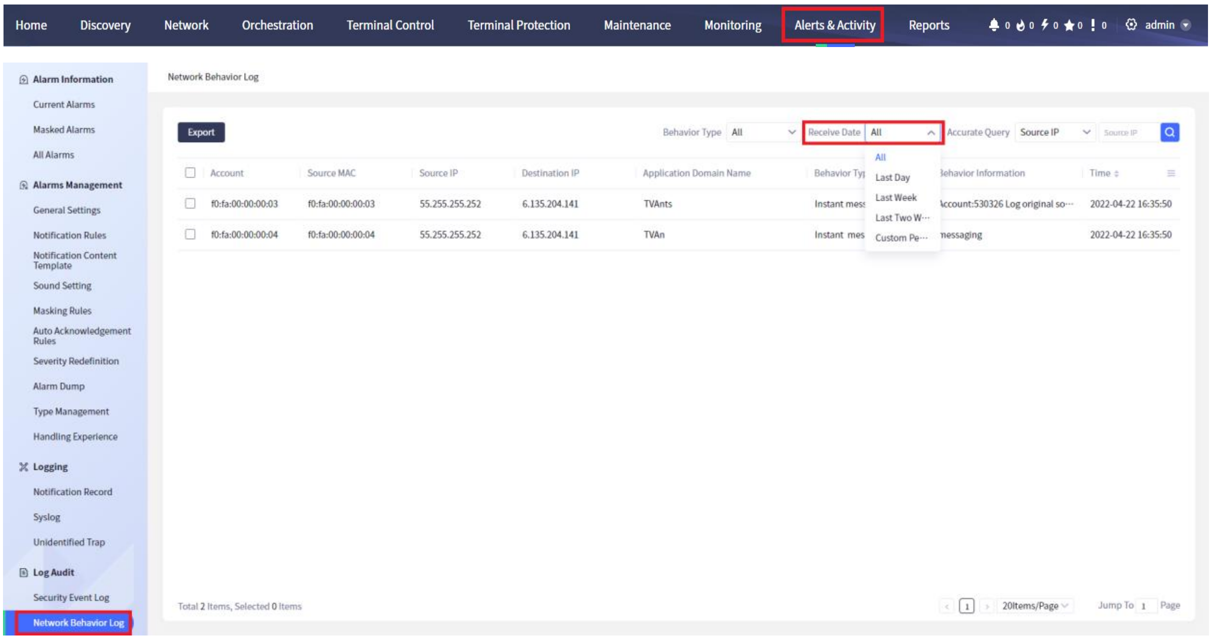
In the current **Network Behavior Log** interface, users can perform fuzzy query by behavior type and receiving date, and can also perform accurate query by IP. The effect is shown in the figure.



Network Behavior Log

☐	Account	Source MAC	Source IP	Destination IP	Application Domain	Behavior Type	Behavior Information	Time
☐	f0:fa:00:00:00:03	f0:fa:00:00:00:03	55.255.255.252	6.135.204.141	TVAnts	Instant messaging	Account:530326 Log original so···	2022-04-22 16:35:50
☐	f0:fa:00:00:00:04	f0:fa:00:00:00:04	55.255.255.252	6.135.204.141	TVAn	Instant messaging	messaging	2022-04-22 16:35:50

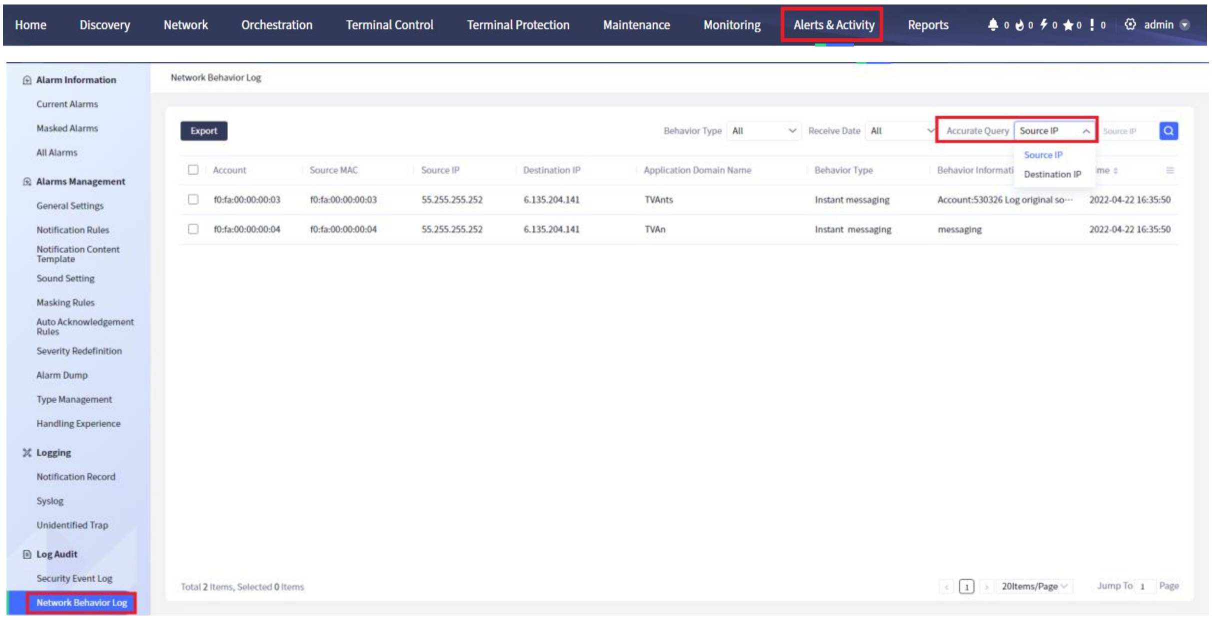
Figure 11.4.2.2 Query network behavior log by behavior type



Network Behavior Log

☐	Account	Source MAC	Source IP	Destination IP	Application Domain Name	Behavior Typ	ehavior Information	Time
☐	f0:fa:00:00:00:03	f0:fa:00:00:00:03	55.255.255.252	6.135.204.141	TVAnts	Instant mes	ccount:530326 Log original so···	2022-04-22 16:35:50
☐	f0:fa:00:00:00:04	f0:fa:00:00:00:04	55.255.255.252	6.135.204.141	TVAn	Instant mes	messaging	2022-04-22 16:35:50

Figure 11.4.2.3 Query network behavior log by receiving date

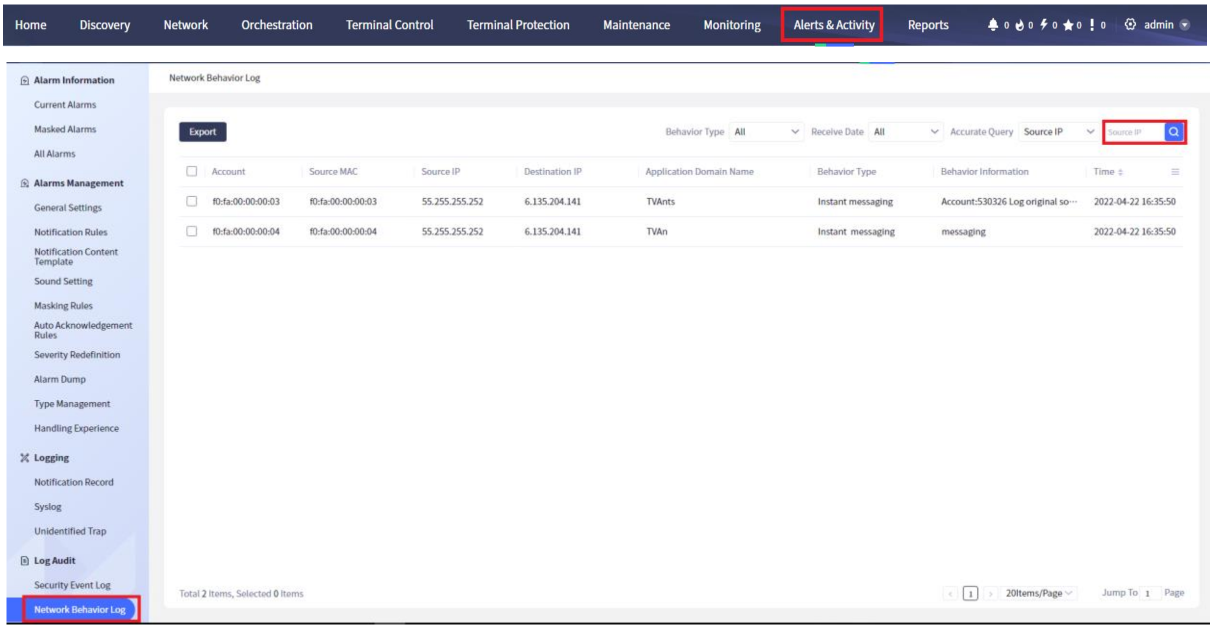


Behavior Type: All; Receive Date: All; Accurate Query: Source IP

Account	Source MAC	Source IP	Destination IP	Application Domain Name	Behavior Type	Behavior Informati	ime
f0:fa:00:00:00:03	f0:fa:00:00:00:03	55.255.255.252	6.135.204.141	TVAnts	Instant messaging	Account:530326 Log original so···	2022-04-22 16:35:50
f0:fa:00:00:00:04	f0:fa:00:00:00:04	55.255.255.252	6.135.204.141	TVAn	Instant messaging	messaging	2022-04-22 16:35:50

Total 2 Items, Selected 0 Items

Figure 11.4.2.3 Accurately query the network behavior log by IP



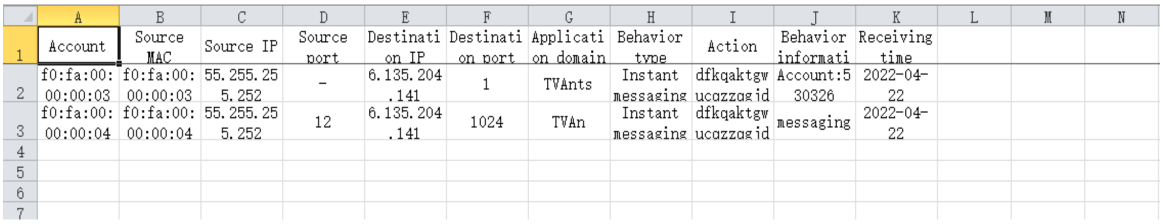
Behavior Type: All; Receive Date: All; Accurate Query: Source IP

Account	Source MAC	Source IP	Destination IP	Application Domain Name	Behavior Type	Behavior Information	Time
f0:fa:00:00:00:03	f0:fa:00:00:00:03	55.255.255.252	6.135.204.141	TVAnts	Instant messaging	Account:530326 Log original so···	2022-04-22 16:35:50
f0:fa:00:00:00:04	f0:fa:00:00:00:04	55.255.255.252	6.135.204.141	TVAn	Instant messaging	messaging	2022-04-22 16:35:50

Total 2 Items, Selected 0 Items

Figure 11.4.2.4 Fuzzy query the network behavior log by IP

According to the query criteria, click the **Export** button in the upper left corner of the page to export the security events. The exported data are as follows:



Account	Source MAC	Source IP	Source port	Destination IP	Destination port	Application domain	Behavior type	Action	Behavior informati	Receiving time
f0:fa:00:00:00:03	f0:fa:00:00:00:03	55.255.255.252	-	6.135.204.141	1	TVAnts	Instant messaging	dfkqaktgwucqzzqgid	Account:530326	2022-04-22
f0:fa:00:00:00:04	f0:fa:00:00:00:04	55.255.255.252	12	6.135.204.141	1024	TVAn	Instant messaging	dfkqaktgwucqzzqgid	messaging	2022-04-22

Figure 11.4.2.5 Export the network behavior log

12 Report Center

12.1 Compliance Statistics Report

Click **Reports** > **Compliance Statistics** to enter the compliance statistics report page. The compliance statistics report is used for device compliance statistics, regional compliance device statistics, etc. The user can filter by the current day, last week, last month and custom time period, as shown in the following figure.

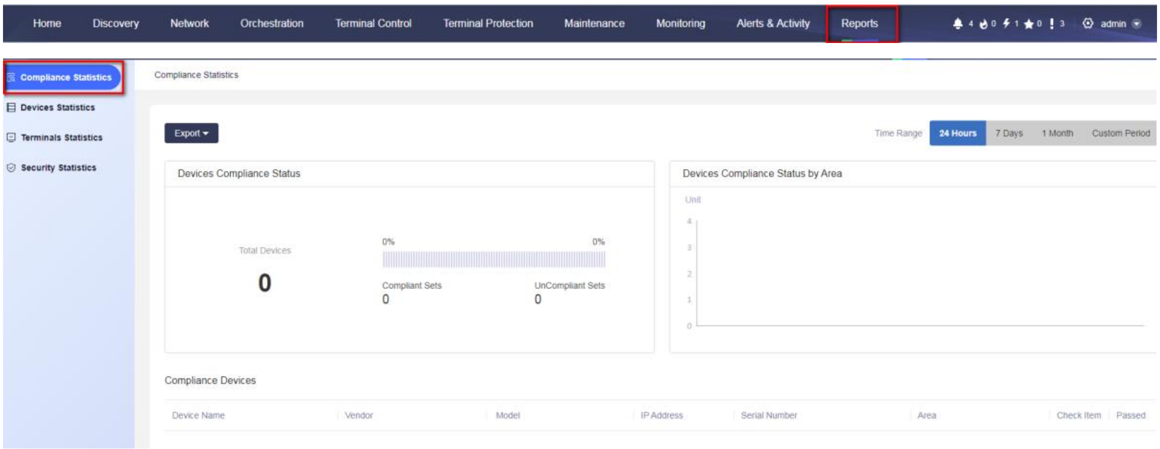


Figure 12.1.1 Enter compliance statistics report

Click the **Export** button, the user can select to export the page data, which can be divided into HTML and Excel according to the export form, as shown below.

HTML export:

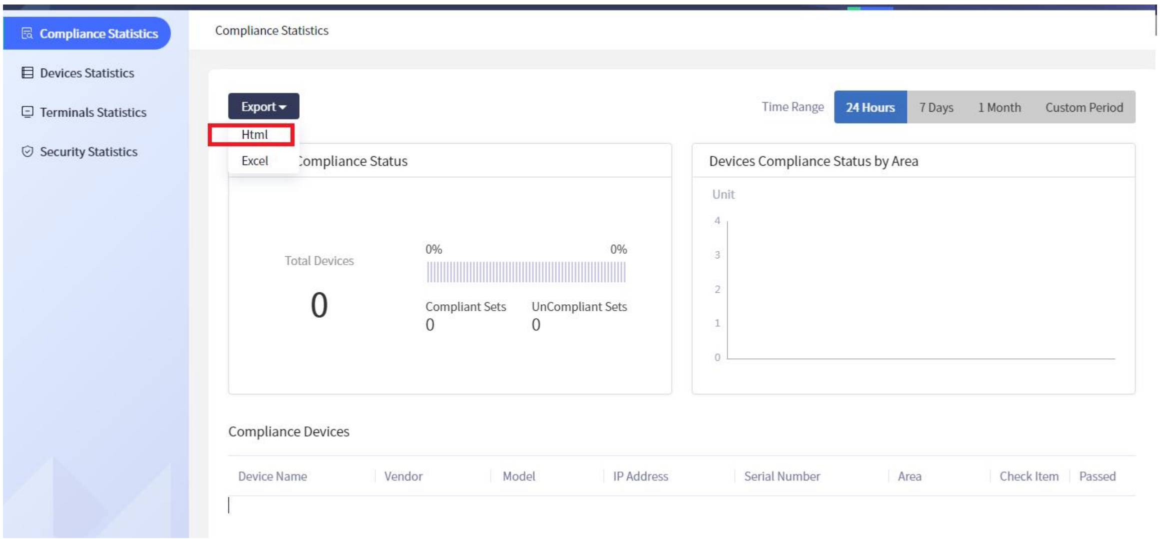


Figure 12.1.2 html export button

Excel export report:

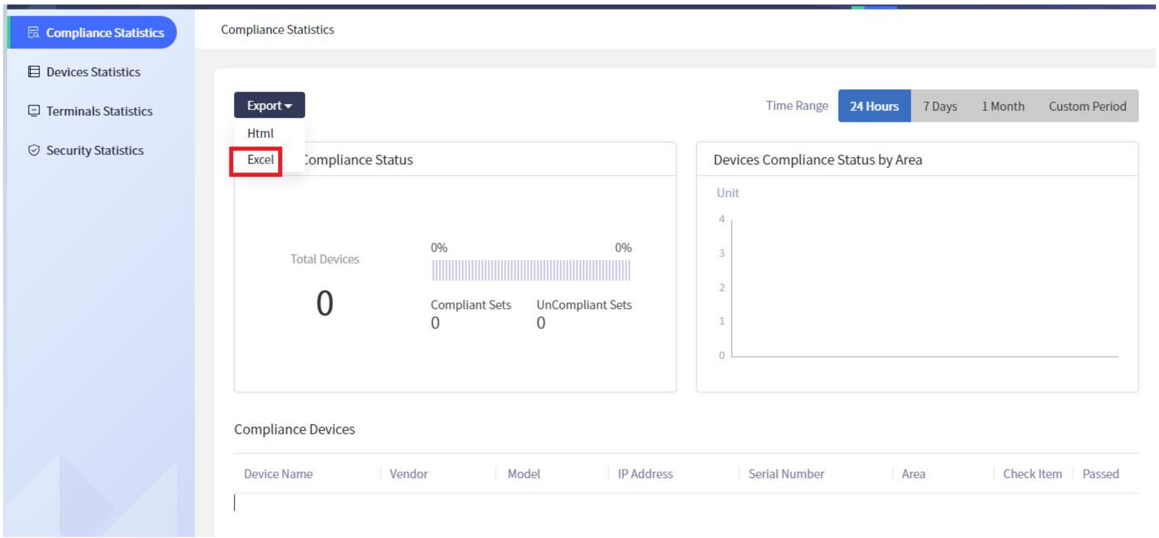


Figure 12.1.3 excel export report button

12.2 Device Statistics Report

Click **Reports** > Device Statistics to enter the **Device Statistics** page. The device statistics report is used to make statistics on the status, distribution and details of the device. You can filter by the current day, last week, last month and custom time period, as shown in the following figure.

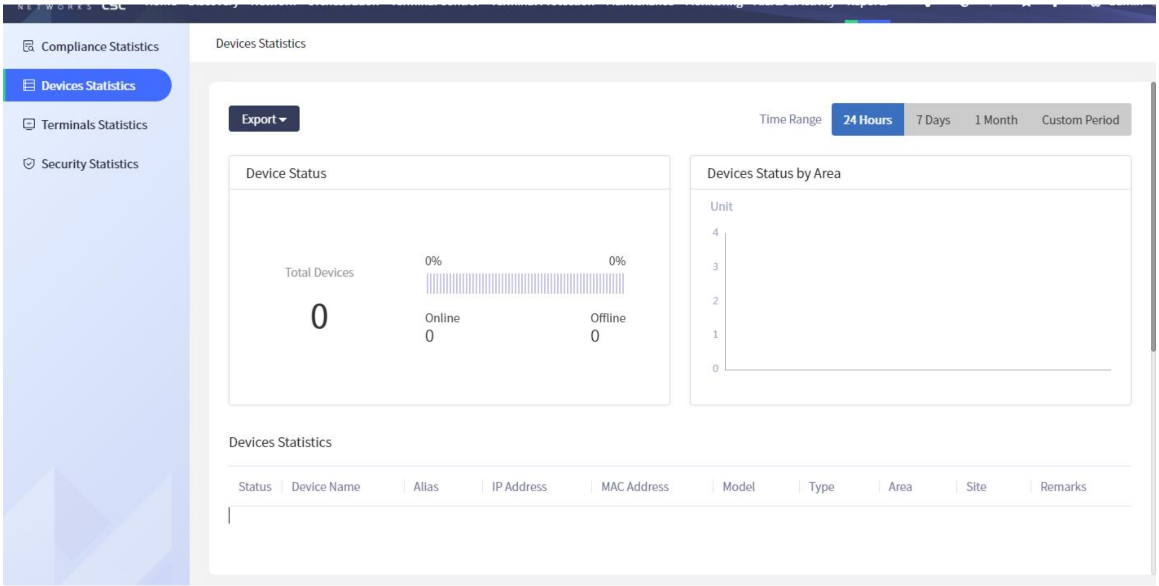


Figure 12.2.1 Enter device statistics report

Click the **Export** button, the user can select to export the page data, which can be divided into HTML and Excel according to the export form. The export is shown below.

HTML export:

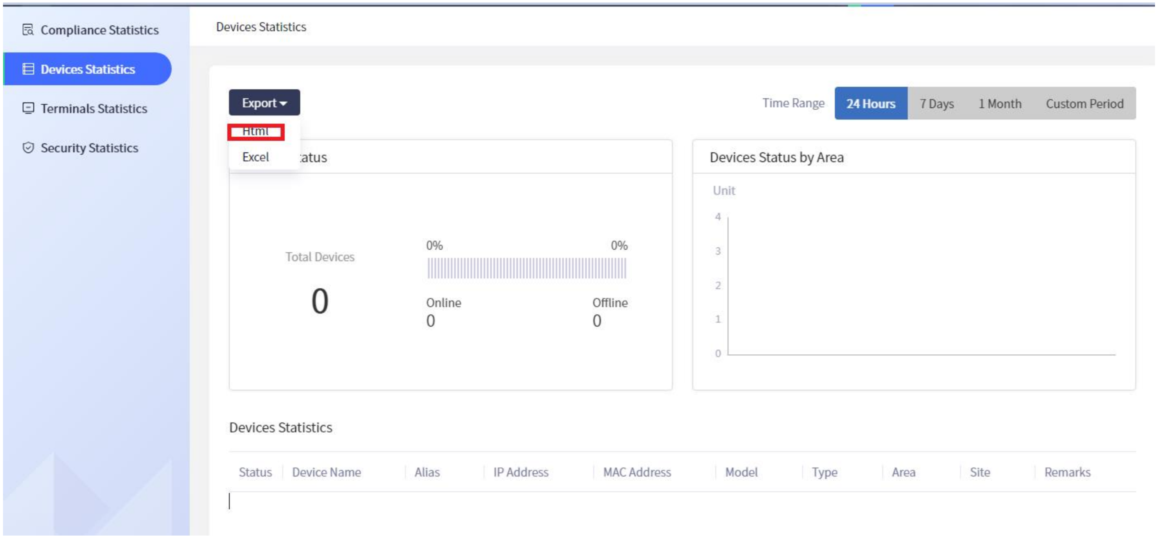


Figure 12.2.2 html export button

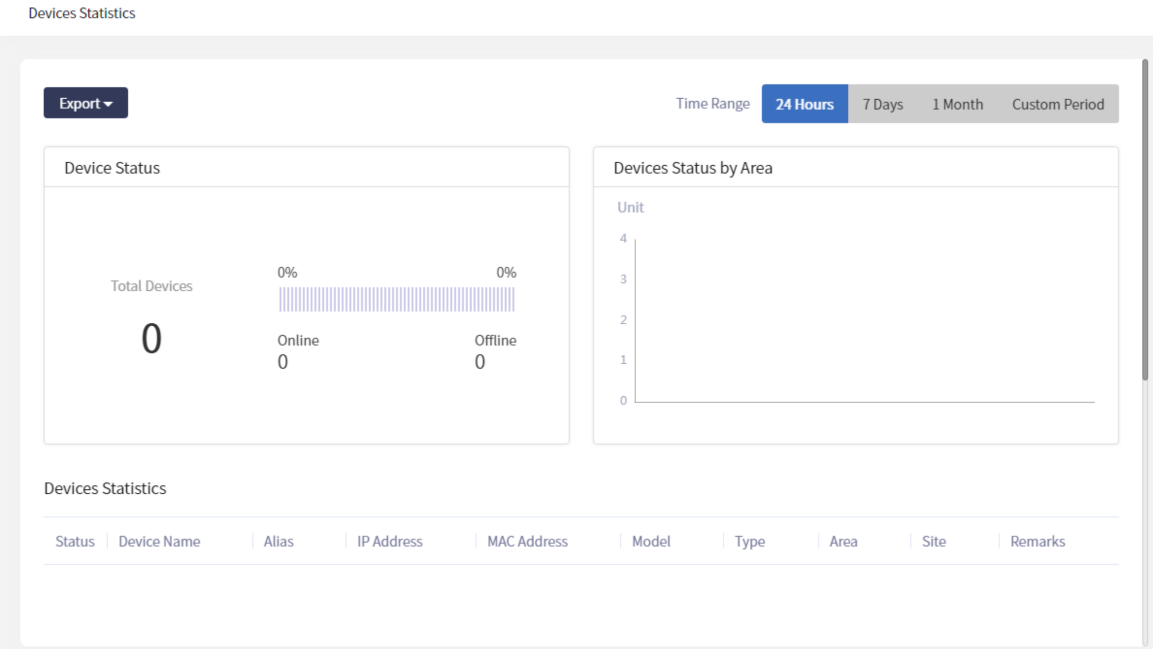


Figure 12.2.3 html export report

Excel export report:

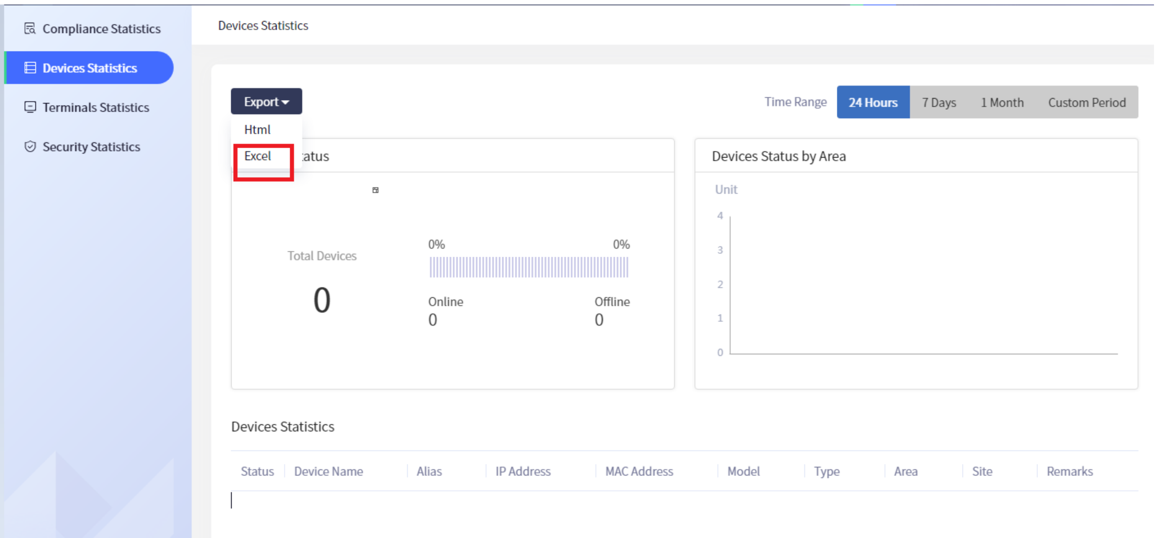
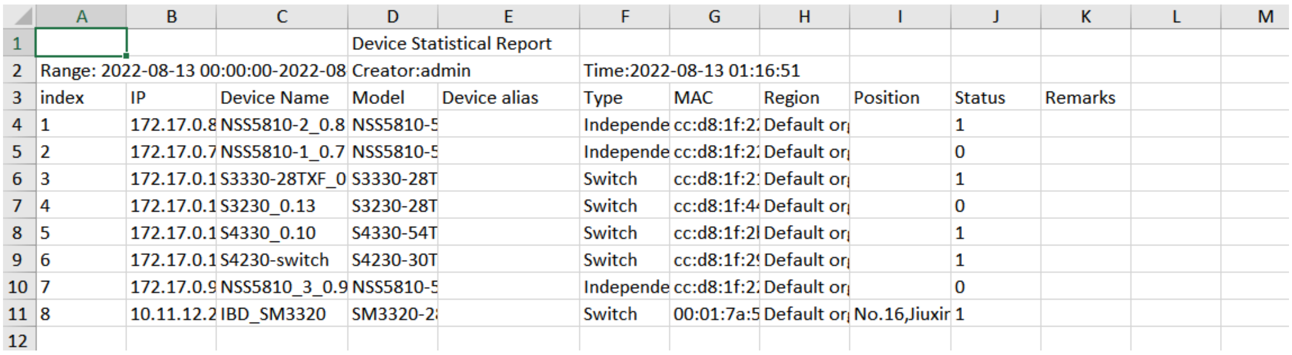


Figure 12.2.4 excel export report button



	A	B	C	D	E	F	G	H	I	J	K	L	M
1				Device Statistical Report									
2	Range: 2022-08-13 00:00:00-2022-08			Creator:admin		Time:2022-08-13 01:16:51							
3	index	IP	Device Name	Model	Device alias	Type	MAC	Region	Position	Status	Remarks		
4	1	172.17.0.8	NSS5810-2_0.8	NSS5810-5		Independe	cc:d8:1f:2	Default or		1			
5	2	172.17.0.7	NSS5810-1_0.7	NSS5810-5		Independe	cc:d8:1f:2	Default or		0			
6	3	172.17.0.1	S3330-28TXF_0	S3330-28T		Switch	cc:d8:1f:2	Default or		1			
7	4	172.17.0.1	S3230_0.13	S3230-28T		Switch	cc:d8:1f:4	Default or		0			
8	5	172.17.0.1	S4330_0.10	S4330-54T		Switch	cc:d8:1f:2	Default or		1			
9	6	172.17.0.1	S4230-switch	S4230-30T		Switch	cc:d8:1f:2	Default or		1			
10	7	172.17.0.9	NSS5810_3_0.9	NSS5810-5		Independe	cc:d8:1f:2	Default or		0			
11	8	10.11.12.2	IBD_SM3320	SM3320-2		Switch	00:01:7a:5	Default or	No.16,Jiuxir	1			
12													

Figure 12.2.5 excel export report

12.3 Terminal Statistics Report

Click "Reports" > "Terminal Statistics" in the menu bar, and the page is as follows:

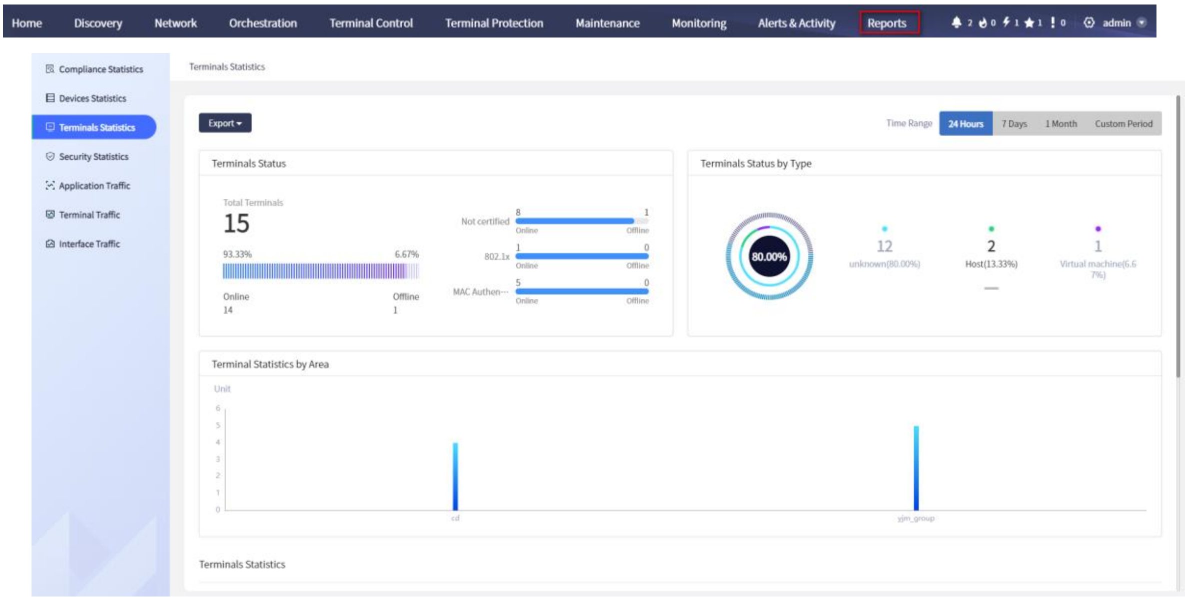


Figure 12.3.1 Terminal statistics report

This page provides the report export function and statistical time selection, and realizes data analysis, data statistics and data presentation in the form of charts and lists.

12.3.1 Select Statistics Time

After entering the terminal statistical report, the default statistical time is the current day, and an optional time range is provided on the right side of the page:

- ➢ 24 hours: the data within the time range of taking the current query time as the end time (find all data earlier than the end time).
- ➢ 7 days: the data within the time range of taking 24:00 p.m. of the last weekend as the end time (find out all data earlier than the end time).
- ➢ 1 month: the data within the time range of taking 24:00 p.m. on the last day of the last month as end time (find out all data earlier than the end time).
- ➢ Custom Period: the data within the time range of selecting 24:00 p.m. of a certain date as the end time (find out all data earlier than the end time).

After selecting and clicking the corresponding statistical time button, generate the statistical data in combination with the region of the current login user.

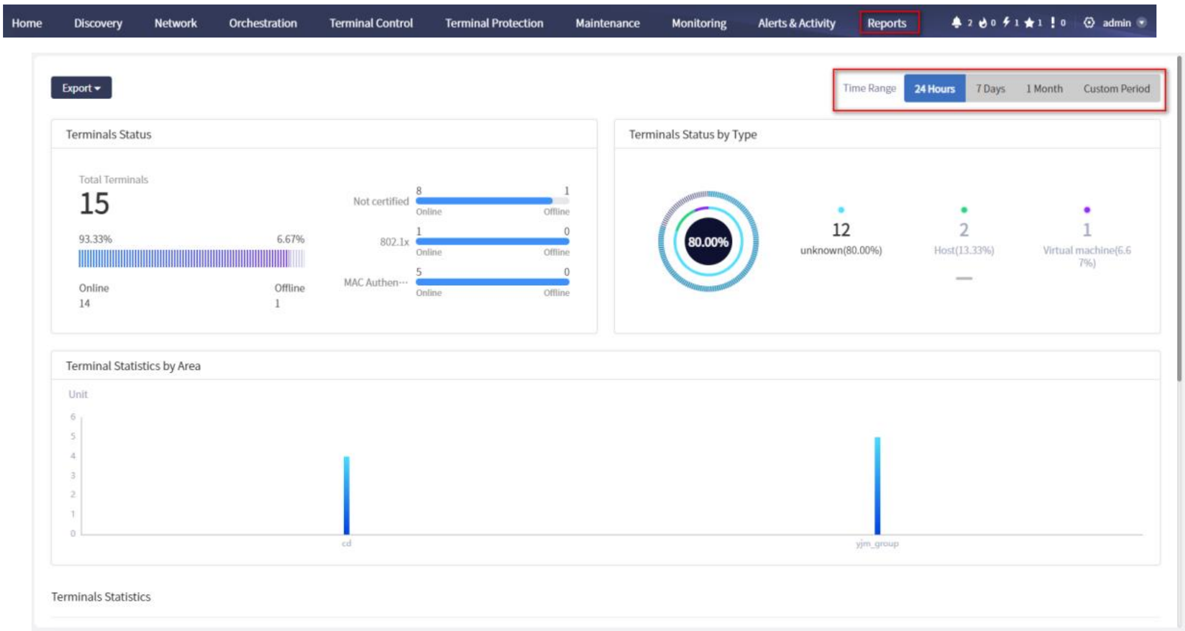


Figure 12.3.1.1 Select statistics time

12.3.2 Select Report Export

After selecting the required statistical time, click **Export** on the left side of the page to open the box of selecting the export format, as follows:

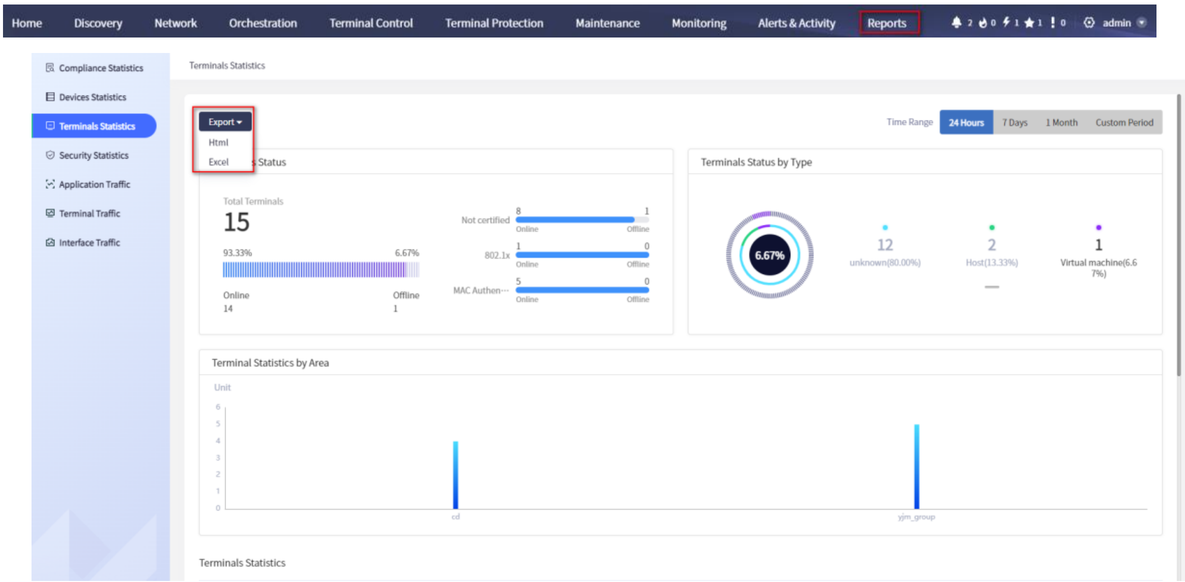


Figure 12.3.2.1 Select the report export format

For report export, you can select web page format (HTML file) and Excel file format. Click the desired file format to start exporting. After normal export, the excel file format can be opened immediately for viewing. After the web page format is exported, it is a zip package. You need to unzip and select the index.html in the corresponding unzipped file to open for viewing.

12.3.3 Terminal Status Statistics

Terminal status statistics: count the corresponding total number of terminals, online and offline terminals, MAC authentication, 1x authentication and unauthenticated terminals according to the selected statistical time point and the region of the current login user.

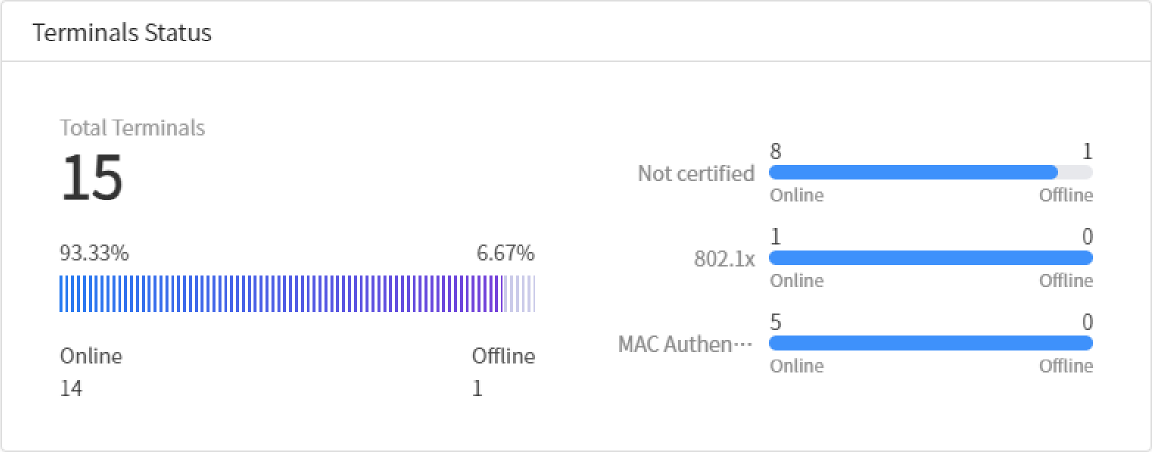


Figure 12.3.3.1 Terminal status statistics

12.3.4 Terminal Type Statistics

Terminal type statistics: According to the selected statistical time point and the region of the currently log in user, count the corresponding terminal type, and the percentage of the terminal type corresponding to the carousel of the pie chart on the left.

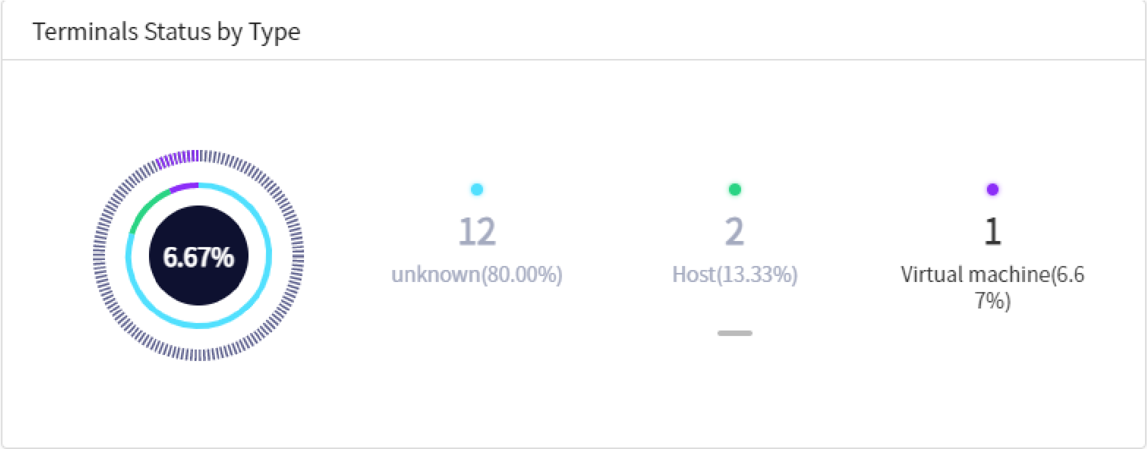


Figure 12.3.4.1 Terminal type statistics

12.3.5 Terminal Area Distribution Statistics

Terminal area distribution statistics: the number of terminals according to the selected statistical time period and the subordinate area of the area of the current login user (if there is no subordinate area, display the current area).

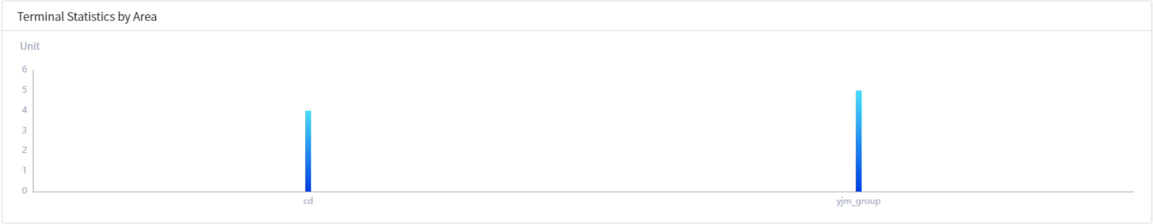
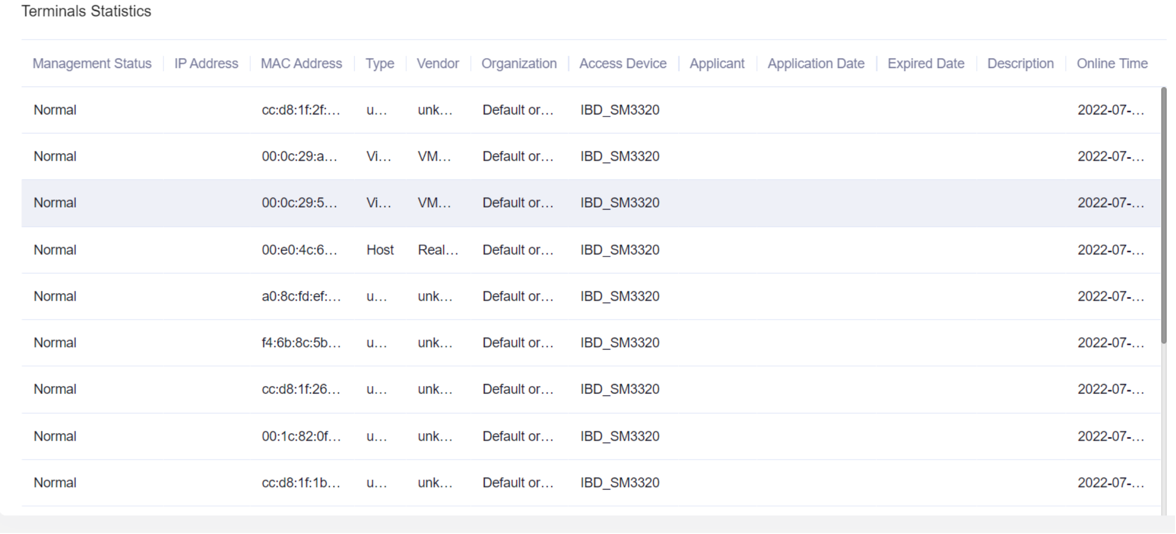


Figure 12.3.5.1 Terminal area distribution statistics

12.3.6 Terminal Statistics List

Terminal statistical list: Display the terminal information in pages according to the area of the current login user and the selected statistical time point. By default, the current page has 20 pieces. You can select the number of pieces to display per page as required.

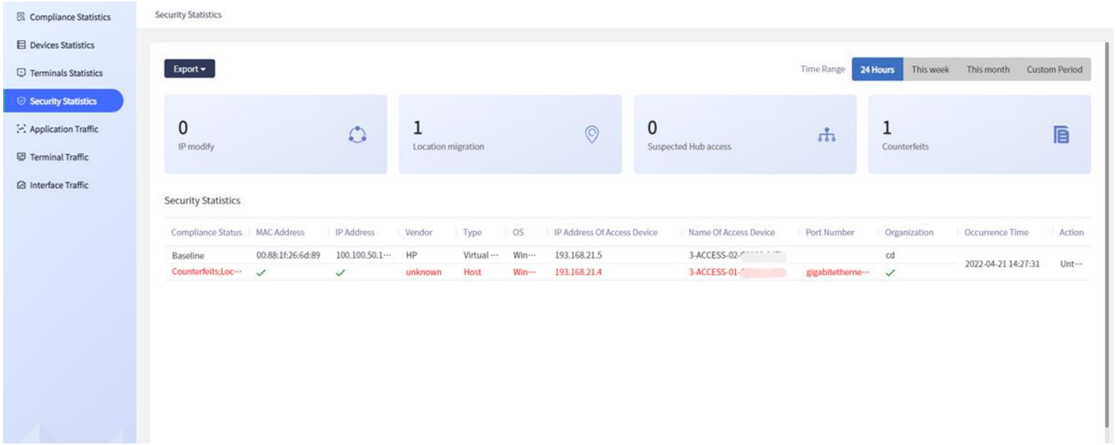


Terminals Statistics

Management Status	IP Address	MAC Address	Type	Vendor	Organization	Access Device	Applicant	Application Date	Expired Date	Description	Online Time
Normal		cc:d8:1f:2f:…	u…	unk…	Default or…	IBD_SM3320					2022-07-…
Normal		00:0c:29:a…	Vi…	VM…	Default or…	IBD_SM3320					2022-07-…
Normal		00:0c:29:5…	Vi…	VM…	Default or…	IBD_SM3320					2022-07-…
Normal		00:e0:4c:6…	Host	Real…	Default or…	IBD_SM3320					2022-07-…
Normal		a0:8c:fd:ef:…	u…	unk…	Default or…	IBD_SM3320					2022-07-…
Normal		f4:6b:8c:5b…	u…	unk…	Default or…	IBD_SM3320					2022-07-…
Normal		cc:d8:1f:26…	u…	unk…	Default or…	IBD_SM3320					2022-07-…
Normal		00:1c:82:0f…	u…	unk…	Default or…	IBD_SM3320					2022-07-…
Normal		cc:d8:1f:1b…	u…	unk…	Default or…	IBD_SM3320					2022-07-…

Figure 12.3.6.1 Terminal statistics list

Click "Reports" > "Security Statistics " in the menu bar, and the page is as follows:



0 IP modify

1 Location migration

0 Suspected Hub access

1 Counterfeits

Security Statistics

Compliance Status	MAC Address	IP Address	Vendor	Type	OS	IP Address Of Access Device	Name Of Access Device	Port Number	Organization	Occurrence Time	Action
Baseline	00:88:1f:26:6d:89	100.100.50.1···	HP	Virtual ···	Win···	193.168.21.5	3-ACCESS-02-[redacted]		cd	2022-04-21 14:27:31	Unt···
Counterfeits;Loc···	✓	✓	unknown	Host	Win···	193.168.21.4	3-ACCESS-01-[redacted]	gigabitetherne···	✓		

Figure 12.4 Security statistics list

This page provides report export function and statistical time selection, and realizes data analysis, data statistics and data presentation in the form of charts and lists.

12.3.7 Select Statistics Time

After entering the security statistics report, the default statistics time is the current day, and an optional time range is provided on the right side of the page:

- 24 hours: the data from the early morning of the current day to the current query time.
- This week: the data from the early morning of this Monday to the current query time.
- This month: the data from the early morning of the first day of this month to the current query time.
- Custom: the historical data within the time range from one day to another day (for example,

from March 13, 2021 to June 15, 2021). Support 6 months at most.

After selecting and clicking the corresponding statistical time button, generate the statistical data in combination with the area of the current login user.

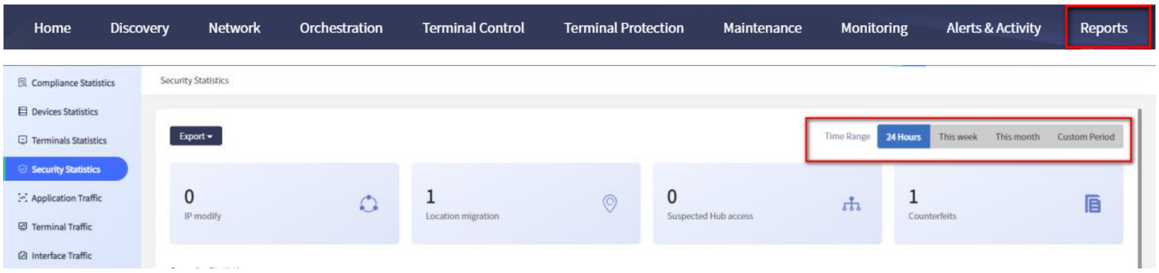


Figure 12.4.1 Select statistics time

12.3.8 Select Report Export

After selecting the required statistical time, click **Export** on the left side of the page to open the box of selecting the export format, as follows:

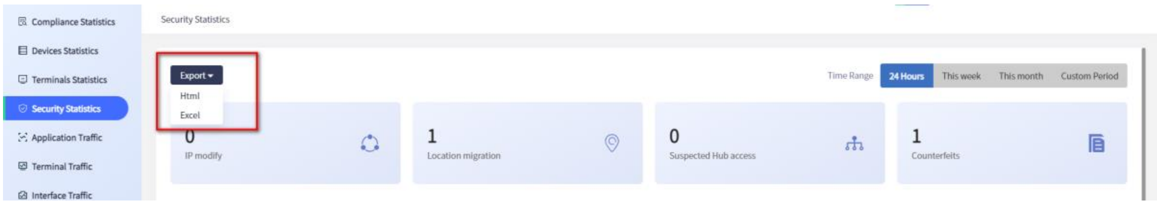


Figure 12.4.2 Select report export

For report export, you can select web page format (HTML file) and excel file format. Click the desired file format to start exporting. After normal export, the excel file format can be opened immediately for viewing. After the web page format is exported, it is a zip package. You need to unzip and select the index.html in the corresponding unzipped file to open for viewing.

12.3.9 Security Event Statistics

Security event statistics: The total number of IP changes, location movements, suspected hub access, and counterfeits according to the selected statistical time point and the area of the current login user.

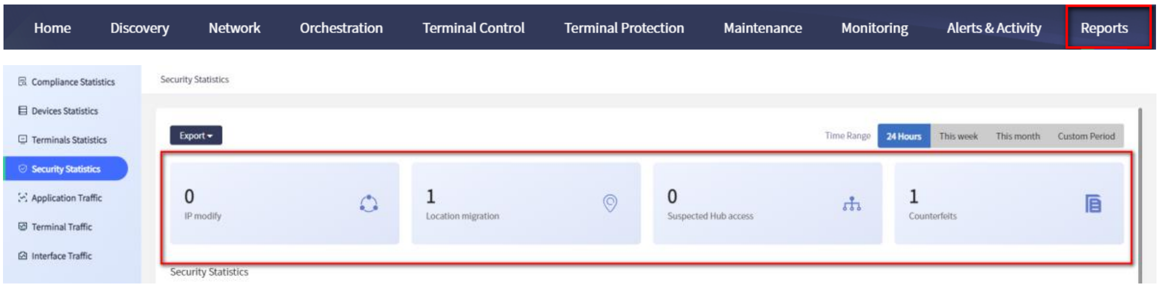
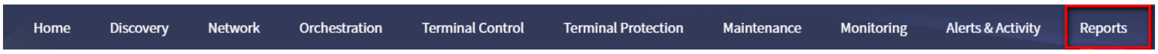
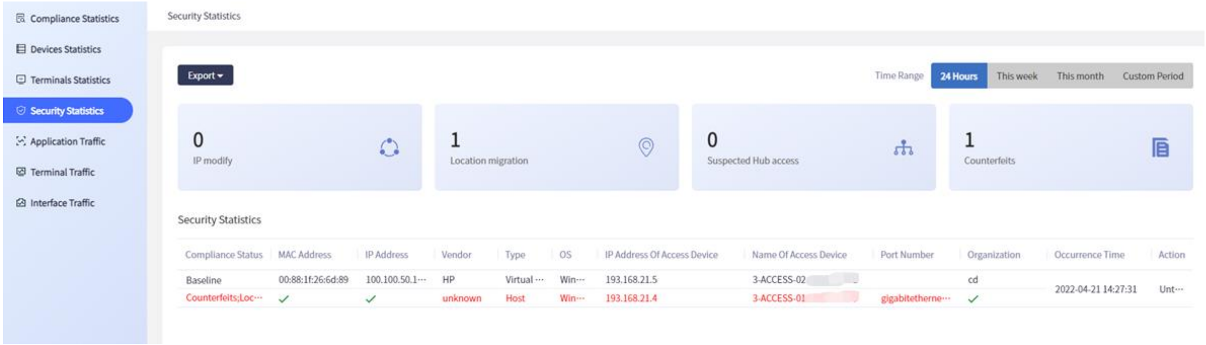


Figure 12.4.3 Security Event Statistics

12.3.10 Security Statistics List

Security statistical list: Display the security event information in pages according to the area of the current login user and the selected statistical time point. By default, the current page has 20 pieces. You can select the number of pieces to display per page as required.





0 IP modify

1 Location migration

0 Suspected Hub access

1 Counterfeits

Security Statistics

Compliance Status	MAC Address	IP Address	Vendor	Type	OS	IP Address Of Access Device	Name Of Access Device	Port Number	Organization	Occurrence Time	Action
Baseline	00:88:1f:26:6d:89	100.100.50.1···	HP	Virtual ···	Win···	193.168.21.5	3-ACCESS-02 [redacted]		cd	2022-04-21 14:27:31	Unt···
Counterfeits;Loc···	✓	✓	unknown	Host	Win···	193.168.21.4	3-ACCESS-01 [redacted]	gigabitetherne···	✓		

Figure 12.4.4 Security Statistics List

12.4 Application Flow Report

Click "Reports" > "Application Traffic" in the menu bar, and the page is as follows:

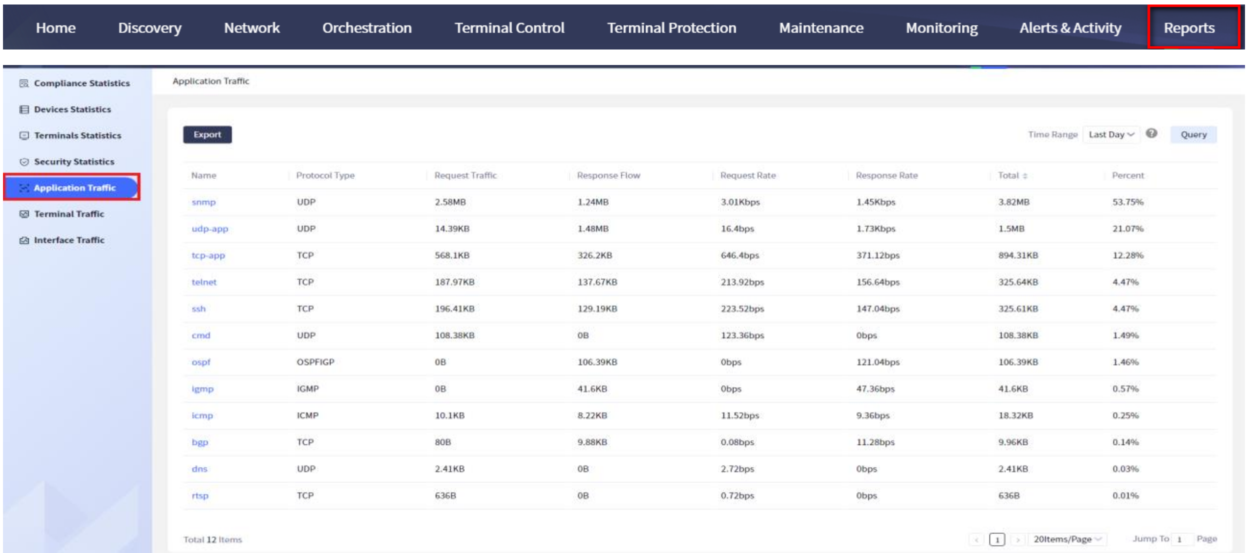
This page provides the report export function and data presentation function in the form of list.

12.4.1 Select Query Time

After entering the application traffic report, the default statistical time is the last hour, and display 1000 pieces of data at most. At the same time, an optional time range is provided on the right side of the page:

- Last hour: the data in the time rang from the current time of the last hour to the current query time.
- Last day: the data in the time rang from the current time of the last day to the current query time.
- Last week: the data in the time rang from the current time of the last week to the current query time.
- Last month: the data in the time rang from the current time of the last month to the current query time.
- Custom: the historical data in the time range from one day to another day; The query interval cannot be greater than 30 days.

Click the **Search** button after selecting the corresponding time to display the data within the specified time range.



Time Range Last Day

Name	Protocol Type	Request Traffic	Response Flow	Request Rate	Response Rate	Total	Percent
snmp	UDP	2.58MB	1.24MB	3.01Kbps	1.45Kbps	3.82MB	53.75%
udp-app	UDP	14.39KB	1.48MB	16.4bps	1.73Kbps	1.5MB	21.07%
tcp-app	TCP	568.1KB	326.2KB	646.4bps	371.12bps	894.31KB	12.28%
telnet	TCP	187.97KB	137.67KB	213.92bps	156.64bps	325.64KB	4.47%
ssh	TCP	196.41KB	129.19KB	223.52bps	147.04bps	325.61KB	4.47%
cmd	UDP	108.38KB	0B	123.36bps	0bps	108.38KB	1.49%
ospf	OSPFIGP	0B	106.39KB	0bps	121.04bps	106.39KB	1.46%
igmp	IGMP	0B	41.6KB	0bps	47.36bps	41.6KB	0.57%
icmp	ICMP	10.1KB	8.22KB	11.52bps	9.36bps	18.32KB	0.25%
bgp	TCP	80B	9.88KB	0.08bps	11.28bps	9.96KB	0.14%
dns	UDP	2.41KB	0B	2.72bps	0bps	2.41KB	0.03%
rtsp	TCP	636B	0B	0.72bps	0bps	636B	0.01%

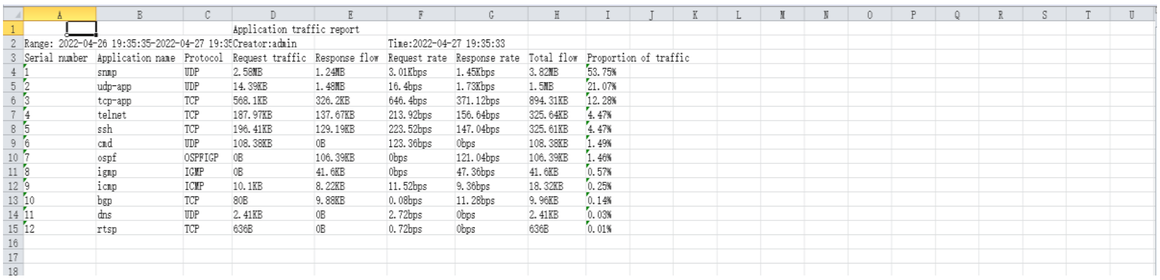
Total 12 Items

1 20Items/Page Jump To 1 Page

Figure 12.4.1 Application traffic report

12.4.2 Report Export

After selecting the required query time, click the **Export** button on the left side of the page to export the data, as shown in the figure below:



Application traffic report

Range: 2022-04-26 19:35:35-2022-04-27 19:35 Creator:admin Time:2022-04-27 19:35:33

Serial number	Application name	Protocol	Request traffic	Response flow	Request rate	Response rate	Total flow	Proportion of traffic
1	snmp	UDP	2.58MB	1.24MB	3.01Kbps	1.45Kbps	3.82MB	53.75%
2	udp-app	UDP	14.39KB	1.48MB	16.4bps	1.73Kbps	1.5MB	21.07%
3	tcp-app	TCP	568.1KB	326.2KB	646.4bps	371.12bps	894.31KB	12.28%
4	telnet	TCP	187.97KB	137.67KB	213.92bps	156.64bps	325.64KB	4.47%
5	ssh	TCP	196.41KB	129.19KB	223.52bps	147.04bps	325.61KB	4.47%
6	cmd	UDP	108.38KB	0B	123.36bps	0bps	108.38KB	1.49%
7	ospf	OSPFIGP	0B	106.39KB	0bps	121.04bps	106.39KB	1.46%
8	igmp	IGMP	0B	41.6KB	0bps	47.36bps	41.6KB	0.57%
9	icmp	ICMP	10.1KB	8.22KB	11.52bps	9.36bps	18.32KB	0.25%
10	bgp	TCP	80B	9.88KB	0.08bps	11.28bps	9.96KB	0.14%
11	dns	UDP	2.41KB	0B	2.72bps	0bps	2.41KB	0.03%
12	rtsp	TCP	636B	0B	0.72bps	0bps	636B	0.01%

Figure 12.4.2 Exported file of application reports

After exporting normally, the Excel file format can be opened immediately for viewing.

12.5 Terminal Traffic Report

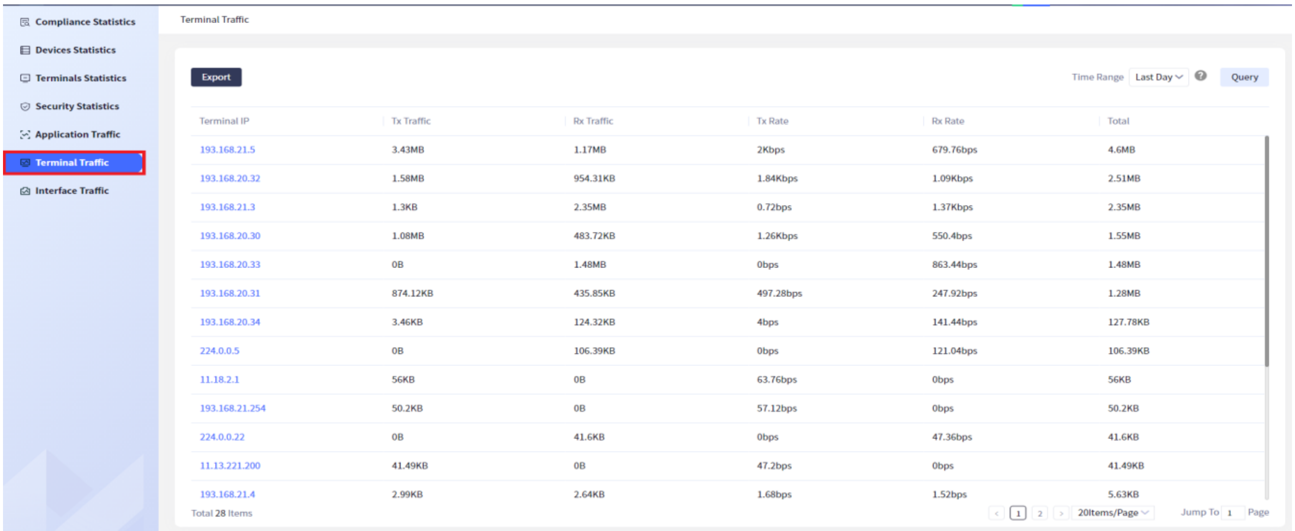
Click **Reports** > **Terminal Traffic** in the menu bar, as shown in the following figure:

12.5.1 Select Query Time

After entering the terminal traffic report, the default statistical time is the last hour, and display 1000 pieces of data at most. At the same time, an optional time range is provided on the right side of the page:

- Last hour: the data in the time rang from the current time of the last hour to the current query time.
- Last day: the data in the time rang from the current time of the last day to the current query time.
- Last week: the data in the time rang from the current time of the last week to the current query time.
- Last month: the data in the time rang from the current time of the last month to the current query time.
- Custom: the historical data in the time range from one day to another day; The query interval cannot be greater than 30 days.

Click the **Search** button after selecting the corresponding time to display the data within the specified time range.



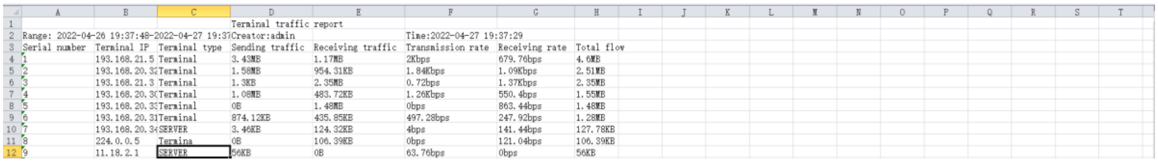
Terminal IP	Tx Traffic	Rx Traffic	Tx Rate	Rx Rate	Total
193.168.21.5	3.43MB	1.17MB	2Kbps	679.76bps	4.6MB
193.168.20.32	1.58MB	954.31KB	1.84Kbps	1.09Kbps	2.51MB
193.168.21.3	1.3KB	2.35MB	0.72bps	1.37Kbps	2.35MB
193.168.20.30	1.08MB	483.72KB	1.26Kbps	550.4bps	1.55MB
193.168.20.33	0B	1.48MB	0bps	863.44bps	1.48MB
193.168.20.31	874.12KB	435.85KB	497.28bps	247.92bps	1.28MB
193.168.20.34	3.46KB	124.32KB	4bps	141.44bps	127.78KB
224.0.0.5	0B	106.39KB	0bps	121.04bps	106.39KB
11.18.2.1	56KB	0B	63.76bps	0bps	56KB
193.168.21.254	50.2KB	0B	57.12bps	0bps	50.2KB
224.0.0.22	0B	41.6KB	0bps	47.36bps	41.6KB
11.13.221.200	41.49KB	0B	47.2bps	0bps	41.49KB
193.168.21.4	2.99KB	2.64KB	1.68bps	1.52bps	5.63KB

Total 28 Items

Figure 12.5.1 Terminal traffic report

12.5.2 Report Export

After selecting the required query time, click the **Export** button on the left side of the page to export the data, as shown in the figure below:



	A	B	C	D	E	F	G	H
1				Terminal traffic report				
2	Range: 2022-04-26 19:37:48-2022-04-27 19:37			Creator:admin		Time:2022-04-27 19:37:29		
3	Serial number	Terminal IP	Terminal type	Sending traffic	Receiving traffic	Transmission rate	Receiving rate	Total flow
4	1	193.168.21.5	Terminal	3.43MB	1.17MB	2Kbps	679.76bps	4.6MB
5	2	193.168.20.3	Terminal	1.58MB	954.31KB	1.84Kbps	1.09Kbps	2.51MB
6	3	193.168.21.3	Terminal	1.3KB	2.35MB	0.72bps	1.37Kbps	2.35MB
7	4	193.168.20.3	Terminal	1.08MB	483.72KB	1.26Kbps	550.4bps	1.55MB
8	5	193.168.20.3	Terminal	0B	1.48MB	0bps	863.44bps	1.48MB
9	6	193.168.20.31	Terminal	874.12KB	435.85KB	497.28bps	247.92bps	1.28MB
10	7	193.168.20.3	SERVER	3.46KB	124.32KB	4bps	141.44bps	127.78KB
11	8	224.0.0.5	Termina	0B	106.39KB	0bps	121.04bps	106.39KB
12	9	11.18.2.1	SERVER	56KB	0B	63.76bps	0bps	56KB

Figure 12.5.2 Exported file of the reports

After exporting normally, the Excel file format can be opened immediately for viewing. Export all data in the query time range.

12.6 Interface Traffic Report

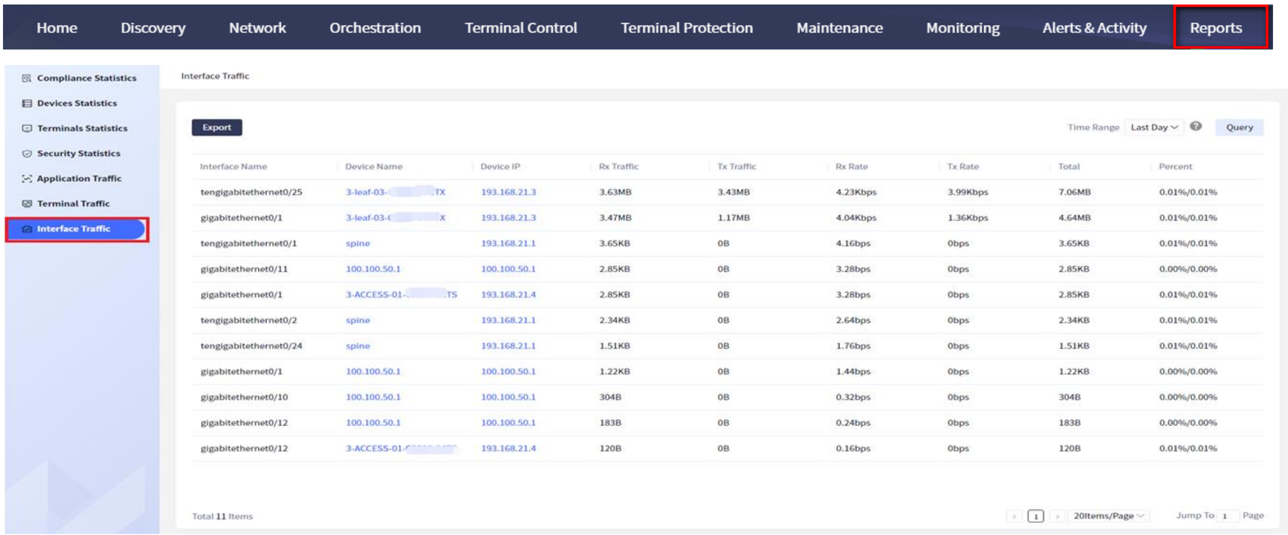
Click **Reports** > **Interface Traffic** in the menu bar, as shown in the following figure:

12.6.1 Select Query Time

After entering the interface traffic report, the default statistical time is the last hour, and display 1000 pieces of data at most. At the same time, an optional time range is provided on the right side of the page:

- Last hour: the data in the time rang from the current time of the last hour to the current query time.
- Last day: the data in the time rang from the current time of the last day to the current query time.
- Last week: the data in the time rang from the current time of the last week to the current query time.
- Last month: the data in the time rang from the current time of the last month to the current query time.
- Custom: the historical data in the time range from one day to another day; The query interval cannot be greater than 30 days.

Click the **Search** button after selecting the corresponding time to display the data within the specified time range.



Interface Traffic

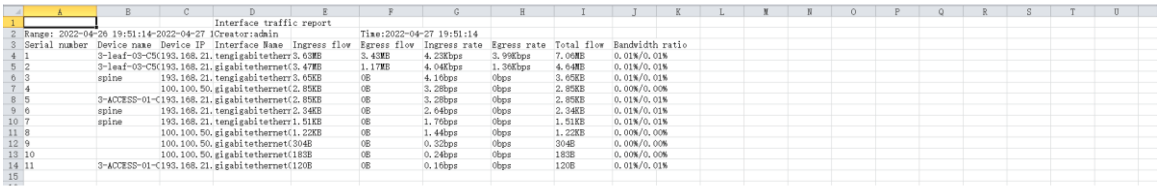
Interface Name	Device Name	Device IP	Rx Traffic	Tx Traffic	Rx Rate	Tx Rate	Total	Percent
tengigabitethernet0/25	3-leaf-03-[redacted]TX	193.168.21.3	3.63MB	3.43MB	4.23Kbps	3.99Kbps	7.06MB	0.01%/0.01%
gigabitethernet0/1	3-leaf-03-[redacted]X	193.168.21.3	3.47MB	1.17MB	4.04Kbps	1.36Kbps	4.64MB	0.01%/0.01%
tengigabitethernet0/1	spine	193.168.21.1	3.65KB	0B	4.16bps	0bps	3.65KB	0.01%/0.01%
gigabitethernet0/11	100.100.50.1	100.100.50.1	2.85KB	0B	3.28bps	0bps	2.85KB	0.00%/0.00%
gigabitethernet0/1	3-ACCESS-01-[redacted]TS	193.168.21.4	2.85KB	0B	3.28bps	0bps	2.85KB	0.01%/0.01%
tengigabitethernet0/2	spine	193.168.21.1	2.34KB	0B	2.64bps	0bps	2.34KB	0.01%/0.01%
tengigabitethernet0/24	spine	193.168.21.1	1.51KB	0B	1.76bps	0bps	1.51KB	0.01%/0.01%
gigabitethernet0/1	100.100.50.1	100.100.50.1	1.22KB	0B	1.44bps	0bps	1.22KB	0.00%/0.00%
gigabitethernet0/10	100.100.50.1	100.100.50.1	304B	0B	0.32bps	0bps	304B	0.00%/0.00%
gigabitethernet0/12	100.100.50.1	100.100.50.1	183B	0B	0.24bps	0bps	183B	0.00%/0.00%
gigabitethernet0/12	3-ACCESS-01-[redacted]	193.168.21.4	120B	0B	0.16bps	0bps	120B	0.01%/0.01%

Total 11 Items

Figure 12.6.1 Interface traffic report

12.6.2 Report Export

After selecting the required query time, click the **Export** button on the left side of the page to export the data, as shown in the figure below:



	A	B	C	D	E	F	G	H	I	J
1				Interface traffic report						
2	Range: 2022-04-26 19:51:14-2022-04-27 1			Creator:admin		Time:2022-04-27 19:51:14				
3	Serial number	Device name	Device IP	Interface Name	Ingress flow	Egress flow	Ingress rate	Egress rate	Total flow	Bandwidth ratio
4	1	3-leaf-03-C5(	193.168.21.	tengigabitetherr	3.63MB	3.43MB	4.23Kbps	3.99Kbps	7.06MB	0.01%/0.01%
5	2	3-leaf-03-C5(	193.168.21.	gigabitethernet(	3.47MB	1.17MB	4.04Kbps	1.36Kbps	4.64MB	0.01%/0.01%
6	3	spine	193.168.21.	tengigabitetherr	3.65KB	0B	4.16bps	0bps	3.65KB	0.01%/0.01%
7	4		100.100.50.	gigabitethernet(	2.85KB	0B	3.28bps	0bps	2.85KB	0.00%/0.00%
8	5	3-ACCESS-01-C	193.168.21.	gigabitethernet(	2.85KB	0B	3.28bps	0bps	2.85KB	0.01%/0.01%
9	6	spine	193.168.21.	tengigabitetherr	2.34KB	0B	2.64bps	0bps	2.34KB	0.01%/0.01%
10	7	spine	193.168.21.	tengigabitetherr	1.51KB	0B	1.76bps	0bps	1.51KB	0.01%/0.01%
11	8		100.100.50.	gigabitethernet(	1.22KB	0B	1.44bps	0bps	1.22KB	0.00%/0.00%
12	9		100.100.50.	gigabitethernet(	304B	0B	0.32bps	0bps	304B	0.00%/0.00%
13	10		100.100.50.	gigabitethernet(	183B	0B	0.24bps	0bps	183B	0.00%/0.00%
14	11	3-ACCESS-01-C	193.168.21.	gigabitethernet(	120B	0B	0.16bps	0bps	120B	0.01%/0.01%
15										

Figure 12.6.2 Exported file of the interface report

After exporting normally, the Excel file format can be opened immediately for viewing.

Caution

- The data of application traffic report, terminal traffic report and interface traffic report is not stored in real time. The data is calculated once an hour. The data may not be found in the last hour.

13 System Management

13.1 Organization Management

Organization management provides the management of enterprise organizations or the division of device areas. Click the "Settings" icon > **Organization Management** in the top menu bar to open the "Organization Management" page. It provides functions such as organization query, adding, modifying, deleting, importing, exporting, and downloading import templates.

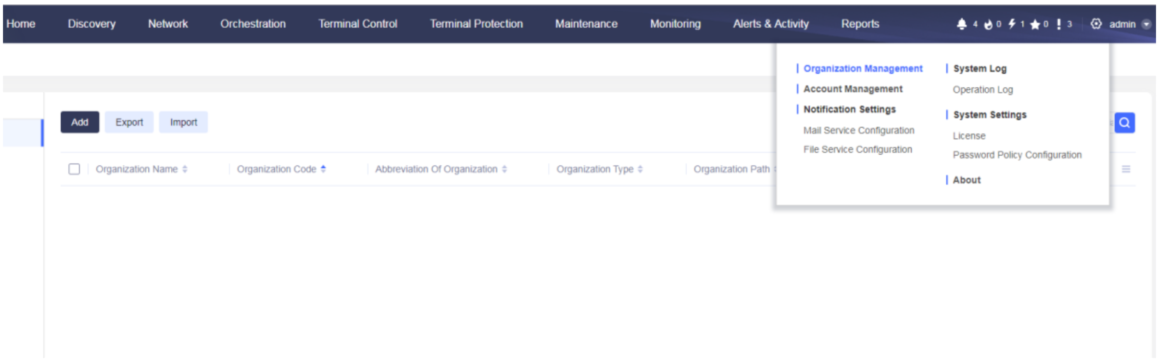


Figure 13.1.1 Organization

Query organization

At the top of the **Organization Management** view is the organization query module, as shown in the following figure. You can query by organization name, organization code, and organization abbreviation. The query content will be displayed in the organization list below, as shown in the following figure.

Figure 13.1.2 Query the organization

When querying the organization, click **Search** without entering conditions, the default organization will appear, as shown in the following figure. You can modify the area, description, code, name and other information of the default organization.

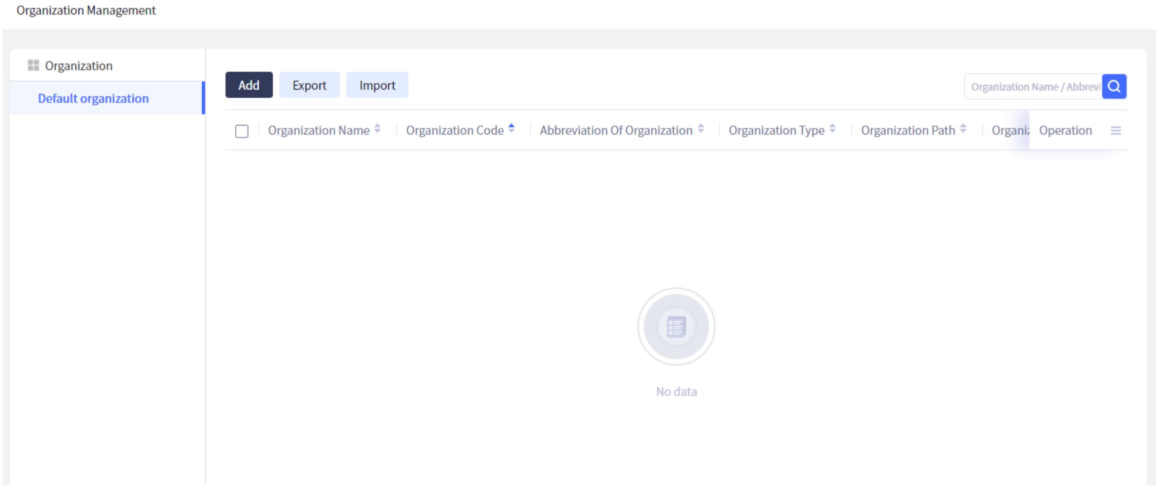
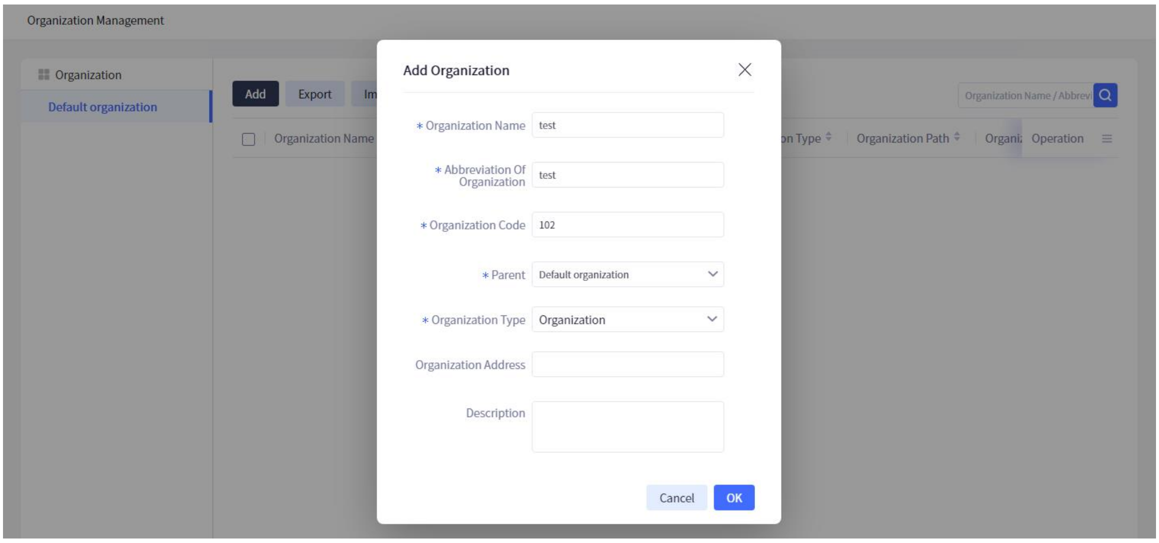


Figure 13.1.3 Query the organization

Add organization

Click **Add** to open the **Add Organization** dialog box. Fill in the organization name, organization abbreviation, organization code, organization type, organization address and description information. Select the parent and click **OK** to save the new organization.



* Organization Name: test
* Abbreviation Of Organization: test
* Organization Code: 102
* Parent: Default organization
* Organization Type: Organization

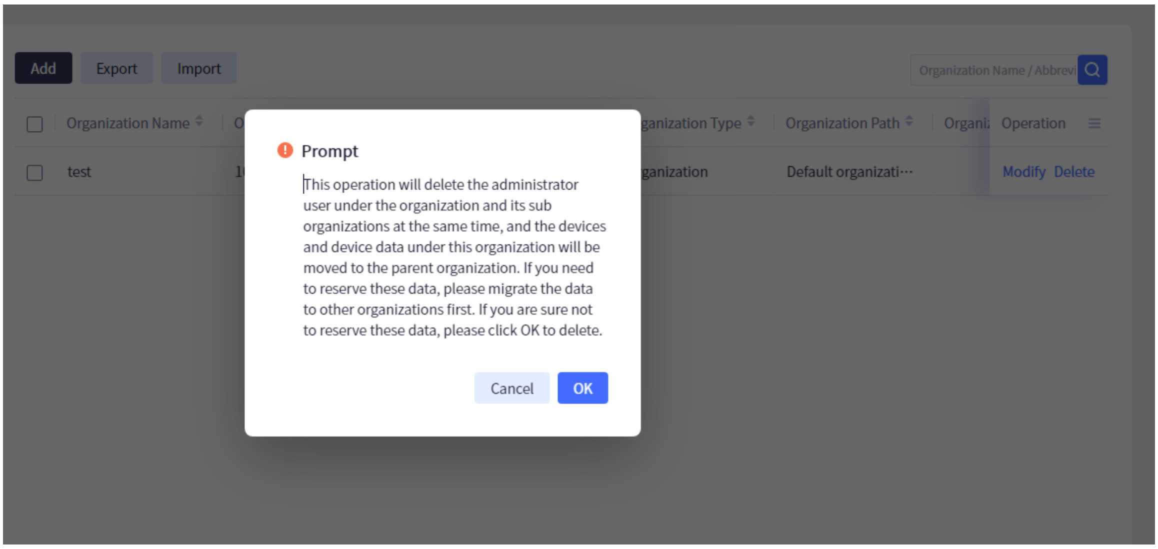
Figure 13.1.4 Add an organization

Modify organization

Select a desired organization in the organization list (only one organization can be modified at the same time), and click **Modify** in the menu bar to open the **Modify** dialog box (see the above figure), where you can modify all the information of the organization in the dialog box. After modification, click **OK** to save the modification information.

Delete organization

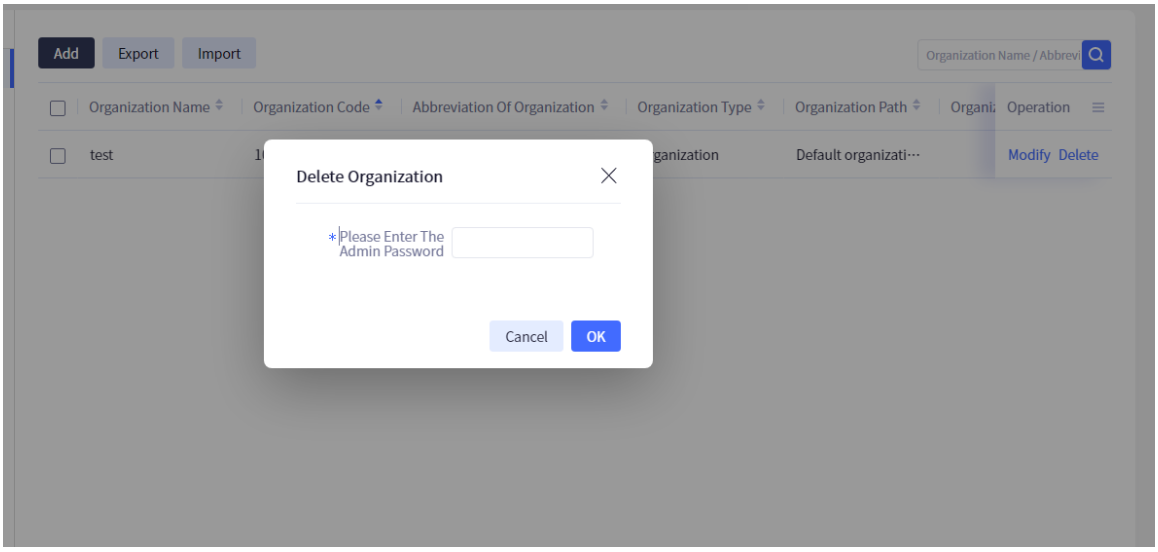
Select a desired organization in the organization list (multiple organizations can be selected), click **Delete** in the menu bar, click **OK** in the pop-up dialog box, enter the login user password to verify identity, and delete the selected organization.



Prompt

This operation will delete the administrator user under the organization and its sub organizations at the same time, and the devices and device data under this organization will be moved to the parent organization. If you need to reserve these data, please migrate the data to other organizations first. If you are sure not to reserve these data, please click OK to delete.

Figure 13.1.5 Delete the organization



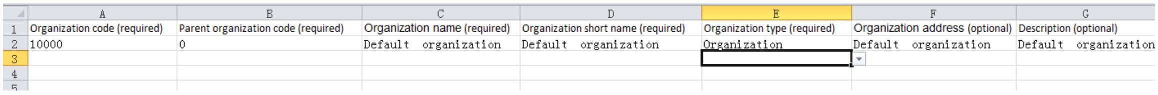
Delete Organization

*Please Enter The Admin Password

Figure 13.1.6 Verify the login password when deleting the organization

Import Organization

Click **Download Template** to download the import template, as shown in the following figure:



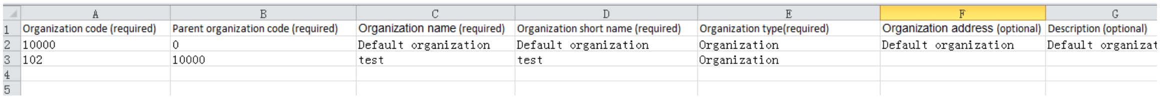
	A	B	C	D	E	F	G
1	Organization code (required)	Parent organization code (required)	Organization name (required)	Organization short name (required)	Organization type (required)	Organization address (optional)	Description (optional)
2	10000	0	Default organization	Default organization	Organization	Default organization	Default organization
3							
4							
5							

Figure 13.1.7 Download the import template

Click **Import**, select the desired organization file, and click **Submit**, as shown in the following figure. After importing successfully, the new imported organization can be queried in the **Organization Management** interface

Export organization

Click **Export** to export all current organizations and save as xlsx format files, as shown in the following figure.

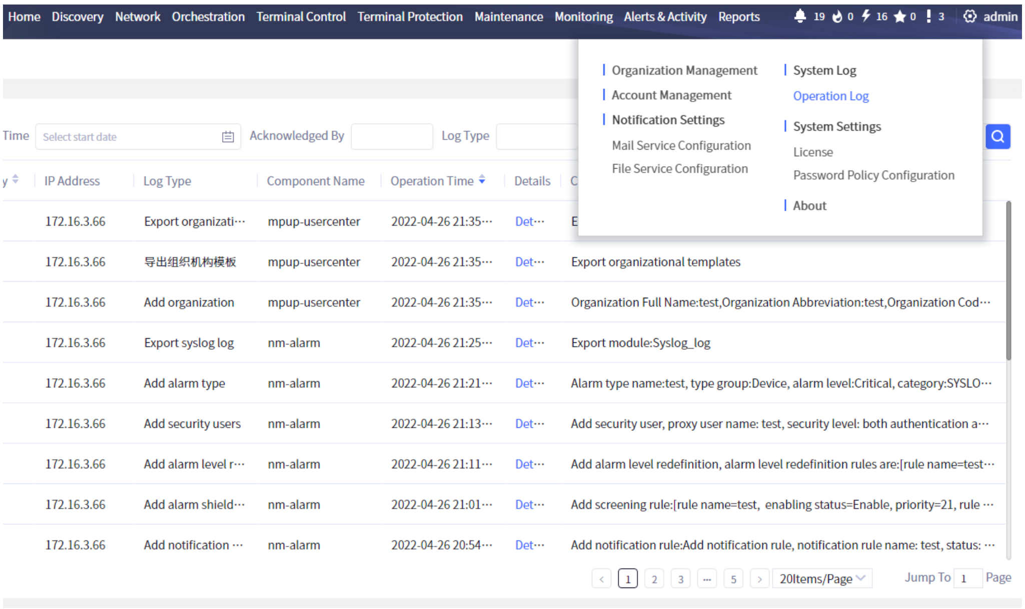


	A	B	C	D	E	F	G
1	Organization code (required)	Parent organization code (required)	Organization name (required)	Organization short name (required)	Organization type(required)	Organization address (optional)	Description (optional)
2	10000	0	Default organization	Default organization	Organization	Default organization	Default organizat
3	102	10000	test	test	Organization		
4							
5							

Figure 13.1.8 Export the organization

13.2 Operation Logs

The operation log module records the addition, modification, deletion, export and other operations of all users in the system. This module provides the functions of querying and exporting log information. You can find the desired log information by operation user, start time, end time, log type and content. Fuzzy query by user name, log type and content is supported. Click "Settings" > "Operation Log" in the menu bar to open the "Operation Log" page.

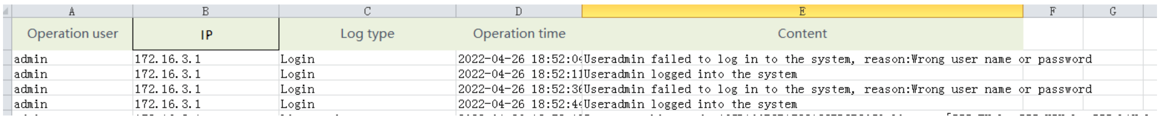


IP Address	Log Type	Component Name	Operation Time	Details	C
172.16.3.66	Export organizati···	mpup-usercenter	2022-04-26 21:35···	Det···	E
172.16.3.66	导出组织机构模板	mpup-usercenter	2022-04-26 21:35···	Det···	Export organizational templates
172.16.3.66	Add organization	mpup-usercenter	2022-04-26 21:35···	Det···	Organization Full Name:test,Organization Abbreviation:test,Organization Cod···
172.16.3.66	Export syslog log	nm-alarm	2022-04-26 21:25···	Det···	Export module:Syslog_log
172.16.3.66	Add alarm type	nm-alarm	2022-04-26 21:21···	Det···	Alarm type name:test, type group:Device, alarm level:Critical, category:SYSLO···
172.16.3.66	Add security users	nm-alarm	2022-04-26 21:13···	Det···	Add security user, proxy user name: test, security level: both authentication a···
172.16.3.66	Add alarm level r···	nm-alarm	2022-04-26 21:11···	Det···	Add alarm level redefinition, alarm level redefinition rules are:[rule name=test···
172.16.3.66	Add alarm shield···	nm-alarm	2022-04-26 21:01···	Det···	Add screening rule:[rule name=test, enabling status=Enable, priority=21, rule ···
172.16.3.66	Add notification ···	nm-alarm	2022-04-26 20:54···	Det···	Add notification rule:Add notification rule, notification rule name: test, status: ···

Figure 13.2.1 Log management

Export log

Click the **Export Log** button in the log list to export the log information in the list to a file in Excel format.

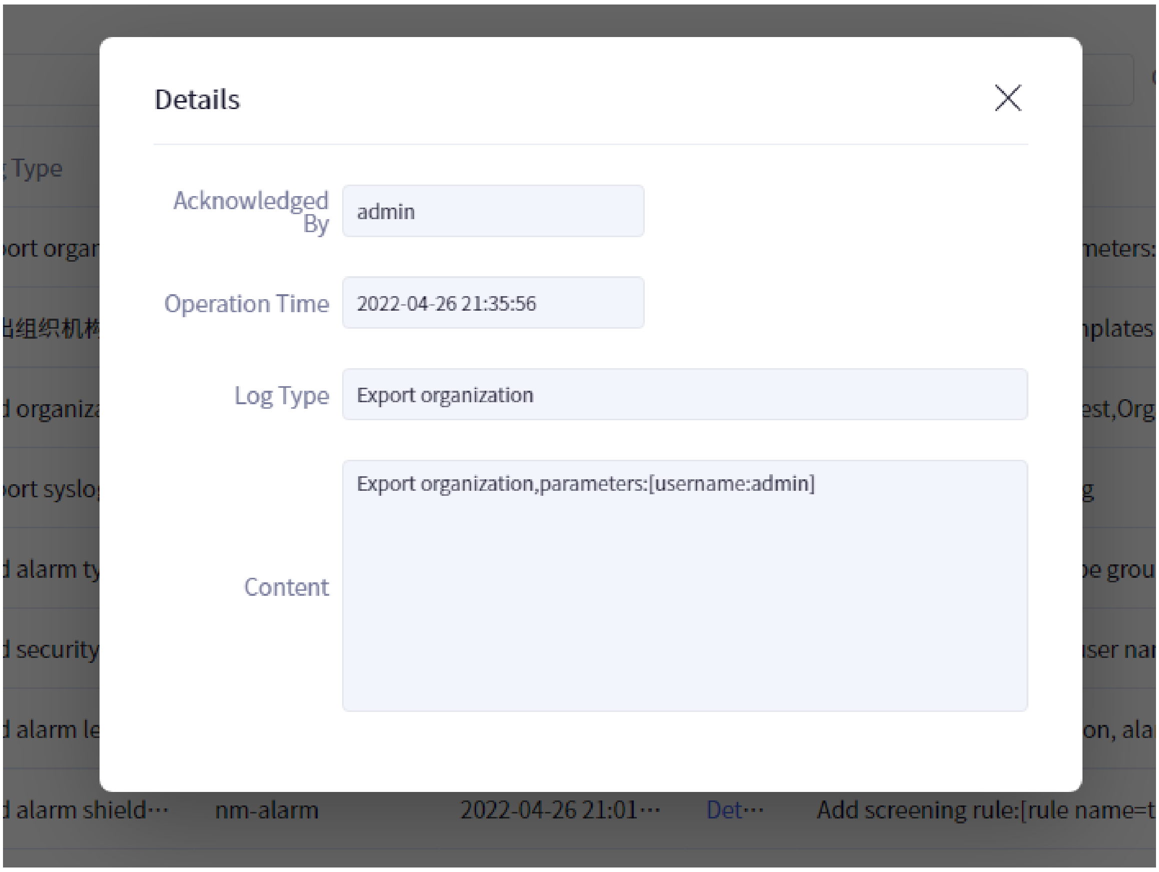


Operation user	IP	Log type	Operation time	Content
admin	172.16.3.1	Login	2022-04-26 18:52:0	Useradmin failed to log in to the system, reason:Wrong user name or password
admin	172.16.3.1	Login	2022-04-26 18:52:1	Useradmin logged into the system
admin	172.16.3.1	Login	2022-04-26 18:52:3	Useradmin failed to log in to the system, reason:Wrong user name or password
admin	172.16.3.1	Login	2022-04-26 18:52:4	Useradmin logged into the system

Figure 13.2.2 Log excel file

Log details

Click the "Details" field in the log list to open the **Details** dialog box, as shown in the following figure. You can get the operation user, log type, operation time and details of the log.



Acknowledged By: admin

Operation Time: 2022-04-26 21:35:56

Log Type: Export organization

Content: Export organization,parameters:[username:admin]

Figure 13.2.3 Log details

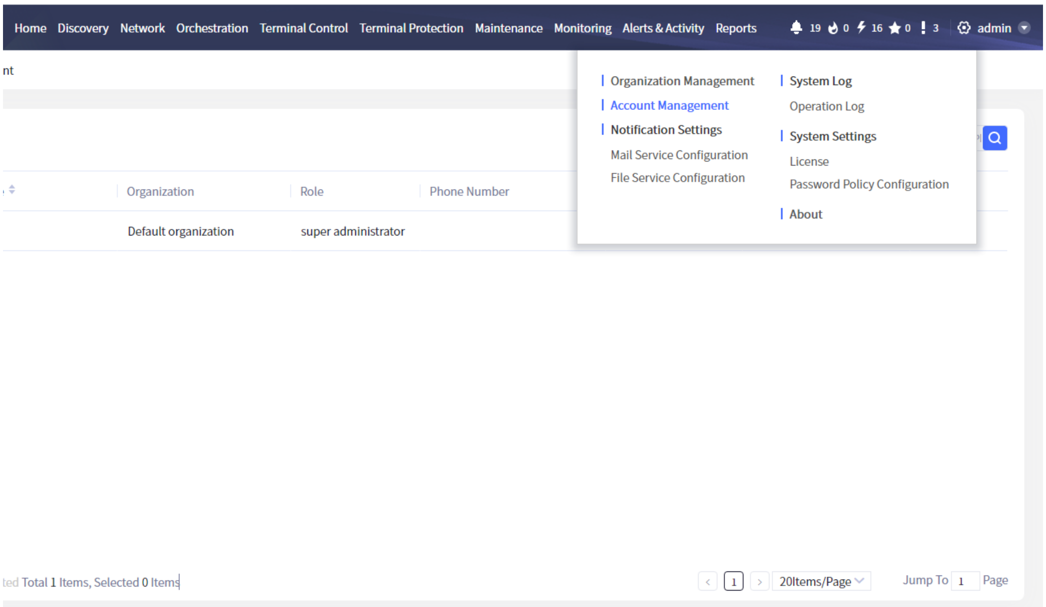
13.3 Administrator

13.3.1 User Management

Introduction to user management

The controller platform adopts matrix authority management, and users need to have the role authority and management area authority. User and authority management provides centralized management for users and their authorities.

Click "Settings" > "Account Management" in the menu bar to open the "Account Management" interface.



Organization	Role	Phone Number
Default organization	super administrator	

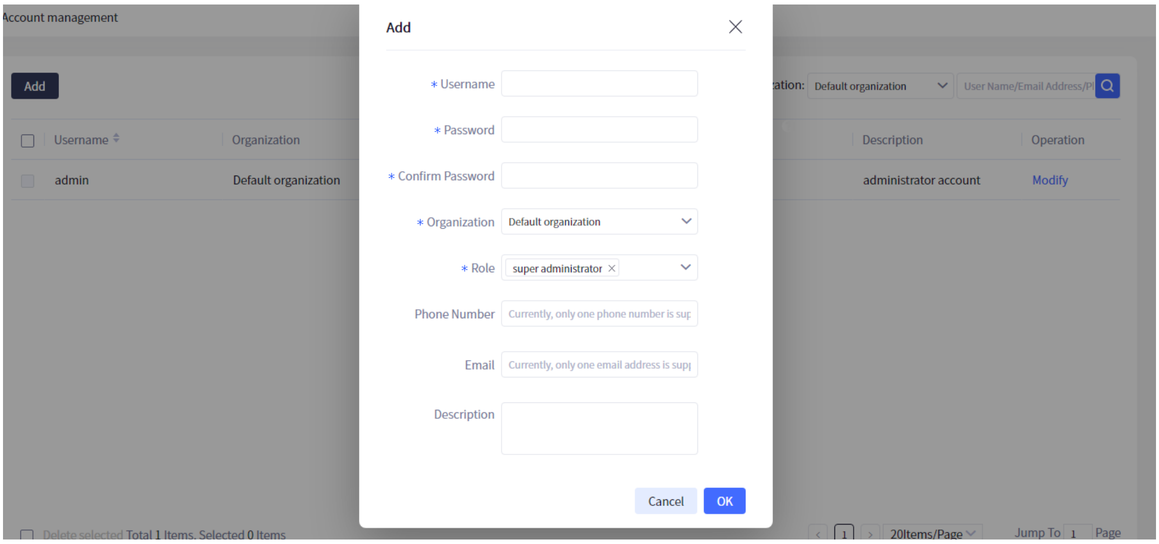
Total 1 Items, Selected 0 Items

20Items/Page

Figure 13.3.1.1 User Management

Add user

Click **Add** to open the **Add** dialog box. Fill in the user name, password, contact information, email address and description, and select the organization and role. Click **OK** to add a user successfully.



Username	Organization	Description	Operation
admin	Default organization	administrator account	Modify

* Username

* Password

* Confirm Password

* Organization: Default organization

* Role: super administrator

Phone Number: Currently, only one phone number is sup

Email: Currently, only one email address is sup

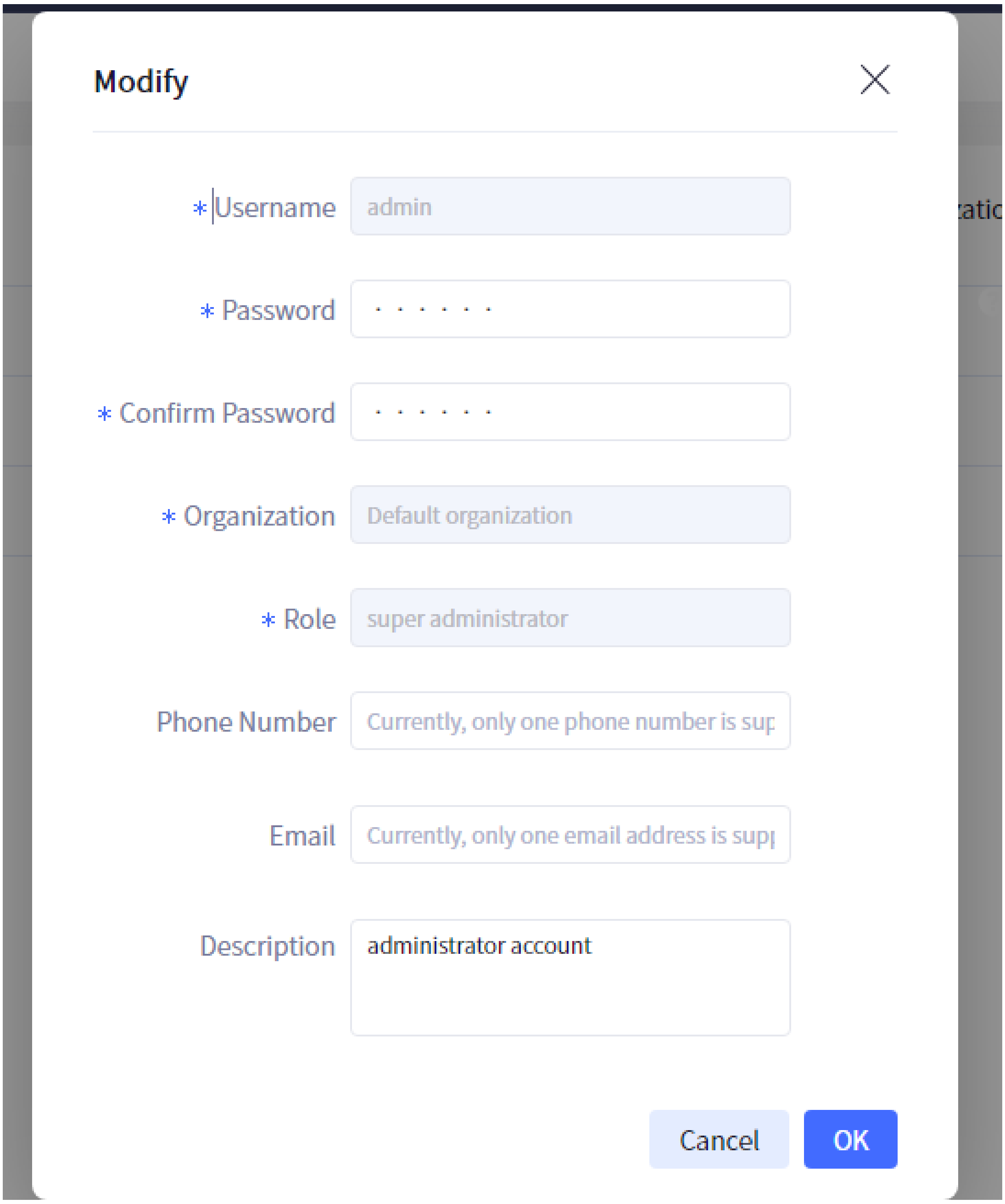
Description

Delete selected Total 1 Items, Selected 0 Items

Figure 13.3.1.2 Add a user

Edit user

Select a desired user and click **Modify** to open the **Modify** dialog box, where you can modify all parameters. After modification, click **OK** to complete the modification.



*Username admin

*Password ·······

*Confirm Password ·······

*Organization Default organization

*Role super administrator

Phone Number Currently, only one phone number is sup

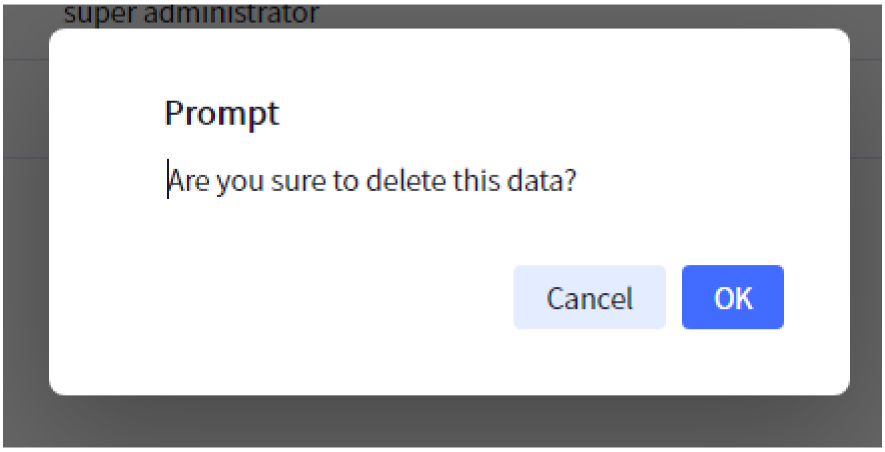
Email Currently, only one email address is sup

Description administrator account

Figure 13.3.1.3 Modify a user

Delete user

Select a desired user and click **Delete** to open the confirmation dialog box. Click **OK** to delete the user successfully. The system built-in user (admin) cannot be deleted.



super administrator

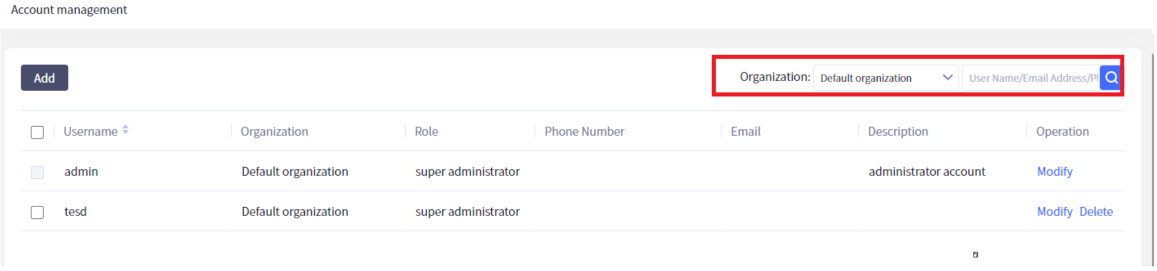
Prompt

Are you sure to delete this data?

Figure 13.3.1.4 Delete a user

Query users

This page provides the query operation for users. You can fuzzy query the user information by entering keywords in the user query criteria section, as shown in the following figure:



Account management

Organization: Default organization

☐	Username	Organization	Role	Phone Number	Email	Description	Operation
☐	admin	Default organization	super administrator			administrator account	Modify
☐	tesd	Default organization	super administrator				Modify Delete

Figure 13.3.1.5 Query users

Click the organization section on the left, and the user list on the right will display the list of all users belonging to the organization in pages.

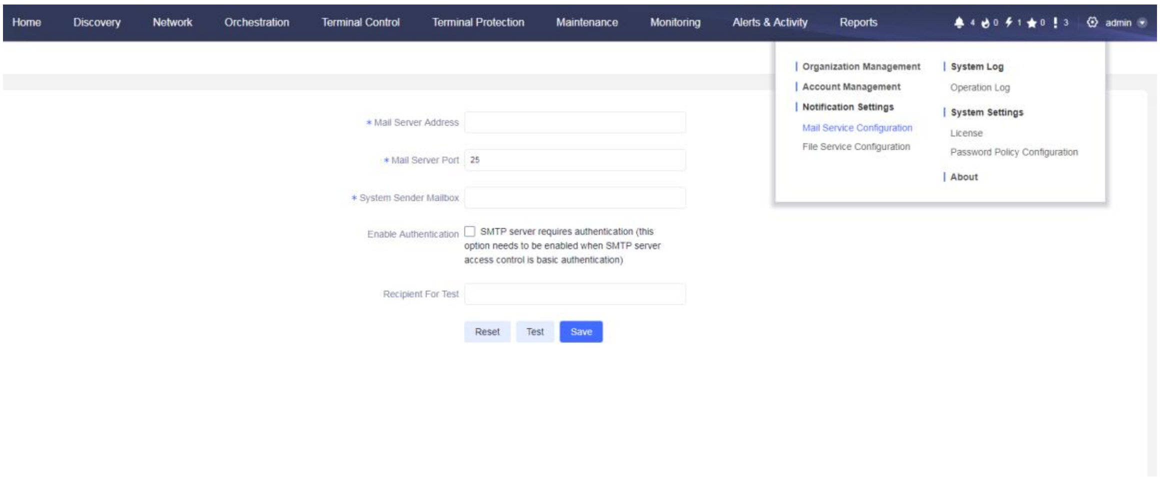
13.4 Notification Settings

This module is mainly used to configure some basic data and configurations of the system, including SMS gateway configuration and mailbox service configuration.

13.4.1 Mail Service Configuration

Mailbox sending is used for all components of Maipu BD-LAN Controller. Before use, it is necessary to configure the relevant parameters of the mail server, such as mail server address (support domain name configuration, the domain name needs to be configured with DNS server or corresponding domain name resolution), mail server port, system sender email address, whether to enable authentication, verify user name, verify password, test recipient, etc.

Click "Settings" > "Notification Settings" > "Mail Service Configuration" in the menu bar to enter the "Mail service configuration" interface.



* Mail Server Address

* Mail Server Port 25

* System Sender Mailbox

Enable Authentication ☐ SMTP server requires authentication (this option needs to be enabled when SMTP server access control is basic authentication)

Recipient For Test

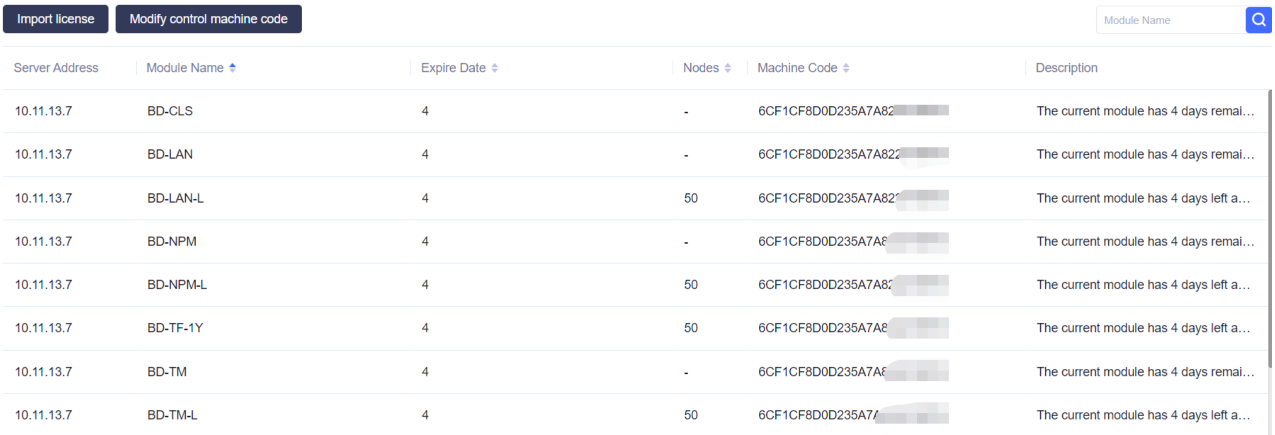
Figure 13.4.2.1 Mail setting

13.5 System Settings

13.5.1 License

License is used to manage the licenses of all components of Maipu BD-LAN Controller. Using this function, you can view the relevant license information and machine code

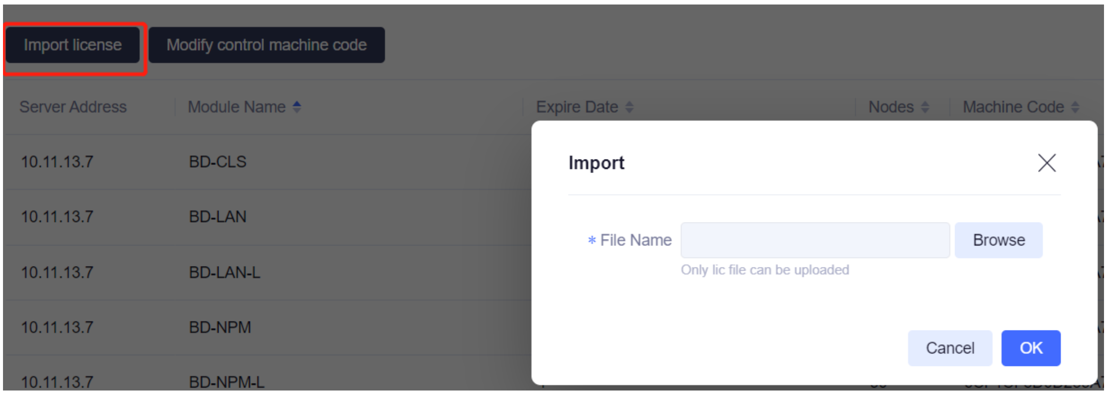
Click "Settings" > "System Settings" > "License" in the menu bar to enter the "License Management" interface.



Server Address	Module Name	Expire Date	Nodes	Machine Code	Description
10.11.13.7	BD-CLS	4	-	6CF1CF8D0D235A7A82[redacted]	The current module has 4 days remai...
10.11.13.7	BD-LAN	4	-	6CF1CF8D0D235A7A822[redacted]	The current module has 4 days remai...
10.11.13.7	BD-LAN-L	4	50	6CF1CF8D0D235A7A82[redacted]	The current module has 4 days left a...
10.11.13.7	BD-NPM	4	-	6CF1CF8D0D235A7A[redacted]	The current module has 4 days remai...
10.11.13.7	BD-NPM-L	4	50	6CF1CF8D0D235A7A8[redacted]	The current module has 4 days left a...
10.11.13.7	BD-TF-1Y	4	50	6CF1CF8D0D235A7A[redacted]	The current module has 4 days left a...
10.11.13.7	BD-TM	4	-	6CF1CF8D0D235A7A[redacted]	The current module has 4 days remai...
10.11.13.7	BD-TM-L	4	50	6CF1CF8D0D235A7[redacted]	The current module has 4 days left a...

Figure 13.5.1.1 License management

By default, all current licenses are displayed in the license list, including server address, module name, expire date, number of nodes, machine code and description information. Click **Import License**, select the desired file, and click **Import** to import the license.



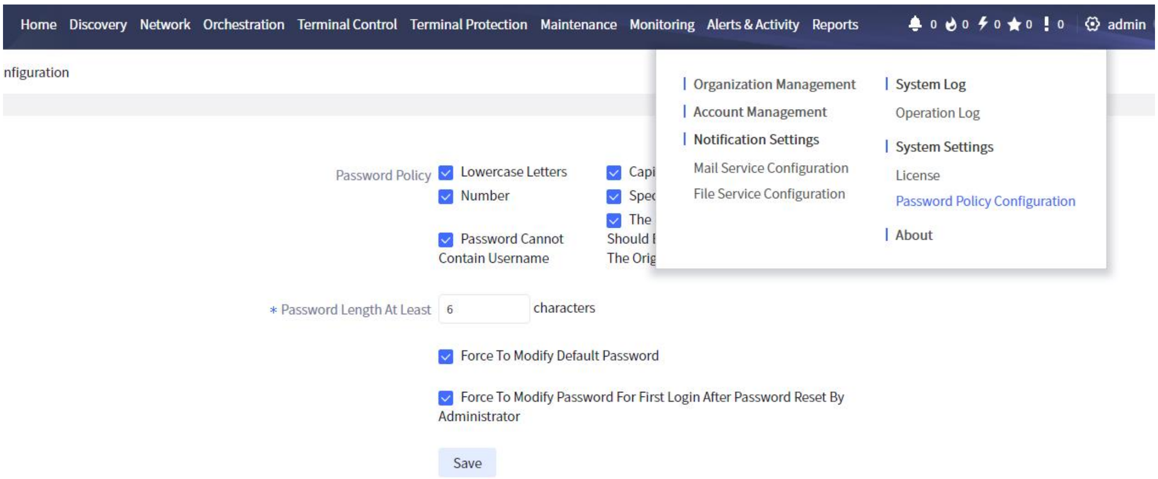
Only lic file can be uploaded

Figure 13.5.1.2 Import license

13.5.2 Password Policy Configuration

Password policy configuration is used to configure the complexity, minimum length, and whether to force the modification of the initial password.

Click "Settings" > "System Settings" > "Password Policy Configuration" in the menu bar to enter the "Password Policy Configuration" page.



Password Policy ☑ Lowercase Letters ☑ Capi ☑ Number ☑ Spec ☑ The ☑ Password Cannot Contain Username · Should I The Orig

* Password Length At Least 6 characters

☑ Force To Modify Default Password

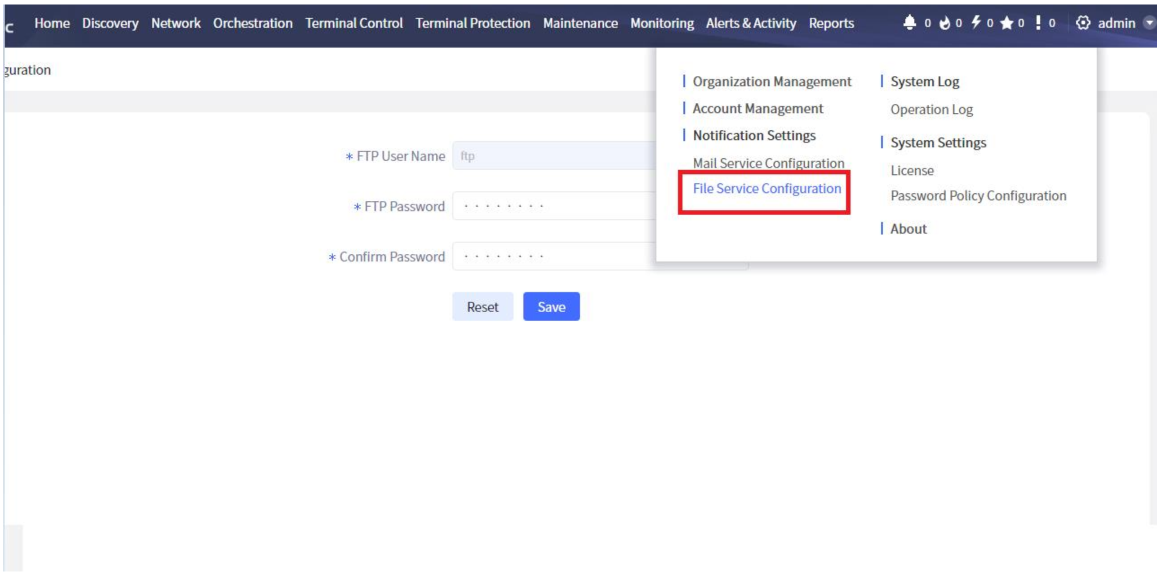
☑ Force To Modify Password For First Login After Password Reset By Administrator

Figure 13.5.2.1 Password policy configuration

13.6 File Service Configuration

Click "Settings" > "Notification Settings" > "File Service Configuration" in the menu bar to enter the "File service configuration" interface.

You can modify the user name and password of FTP file transfer



∗ FTP User Name ftp

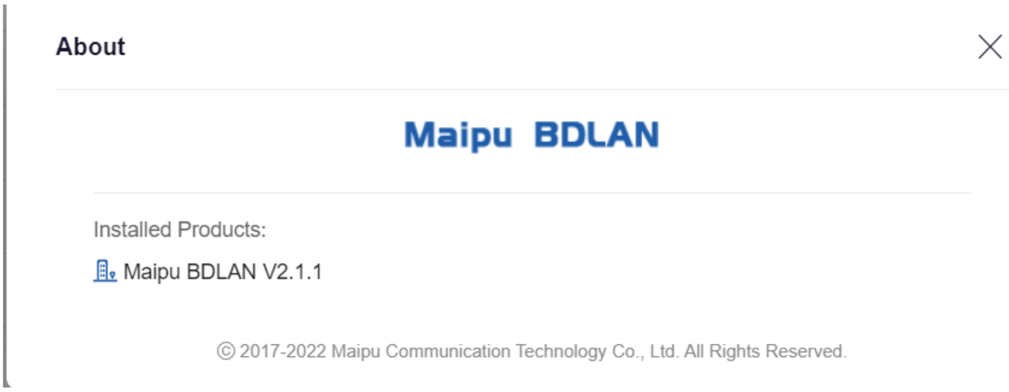
∗ FTP Password · · · · · · · ·

∗ Confirm Password · · · · · · · ·

Figure 13.6.1 File service configuration interface

13.7 About

Click "Settings" > "About" in the menu bar to enter the " MAIPU-BDSTM Overview" page.



About

Maipu BDLAN

Installed Products:

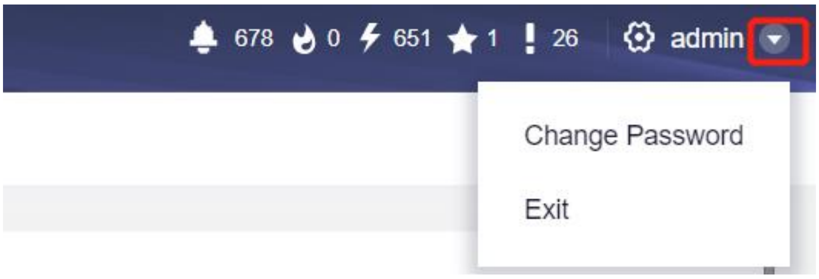
Maipu BDLAN V2.1.1

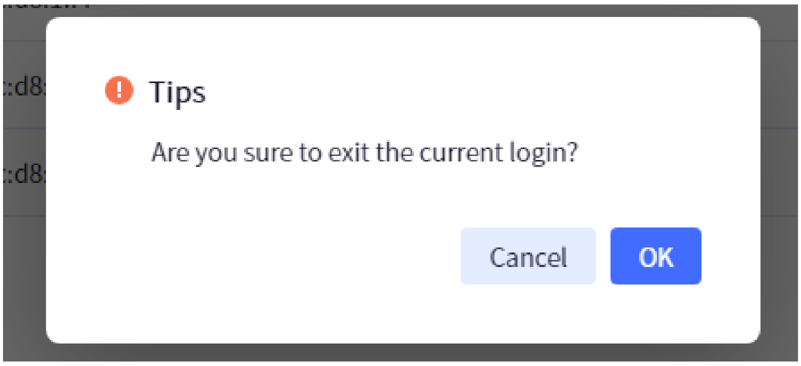
© 2017-2022 Maipu Communication Technology Co., Ltd. All Rights Reserved.

Figure 13.7.1 About

13.8 Log out

Click **Exit** in the upper right corner of the menu bar to open the exit prompt box. Click **OK** to exit and jump to the login interface.





Tips

Are you sure to exit the current login?

Figure 13.8.1 Log out