Colasoft
Maximize Network Value

UPM

Unified Performance Management Solution

User Guide

Colasoft reserves the right to make changes in the product design without reservation and without notification to its users.

Contact Us

Sales
sales@colasoft.com

Technical Support
support@colasoft.com

Website
http://www.colasoft.com/

Contents

1. Preface

Summary

This guide introduces the configurations, operations, and daily maintenance for Colasoft UPM.

Who should read this guide

This guide is written for all users of Colasoft UPM.

Glossary

The commonly used terms in this guide are described in the table below:

Term	Description
Probe	One probe indicates one data collection site, for collecting network packets. One probe corresponds to one network link on nChronos server.
Aggregation probe	One aggregation probe is mapped with two or more probes.
nChronos	nChronos Server, which is deployed at the critical links to capture, analyze and store network packets.
Access relationship	If two IP addresses are communicated, there is access relationship between them.
Access relationship diagram	Access relationship diagram consists of the access relationships among multiple IP addresses.
Business	A business means a specific transaction completed via network. One business can be done via one or more network applications.
Business logic diagram	A business logic diagram consists of the access relationships among server nodes and client nodes for the business.
Business transaction path	A business transaction path consists of server nodes and client nodes that are passed sequentially by to complete a specific task, such as balance inquiry, bank transfer.
Network node	Network communication endpoint, one IP address or a network segment can be taken as one network node.
Network path	Also called as communication path. A network path consists of probes and network devices passed sequentially by when two network nodes communicate.
Intelligent alarm	An advanced alarm triggered by UPM Center which automatically compares the packets difference, retransmission packets and probe data from two probes on one network path.
Asynchronous duplex long connection	One TCP connection method. Asynchronous duplex: when a program sends and receives data, there are two sub processes which send and receive data respectively. With long connection, one TCP connection can send multiple packets continuously. During the keep-live period of the TCP connection, if no packets are sent, both ends are required to send detection packets to keep the connection.

2. Introduction

Colasoft UPM is a network business oriented performance management system. By analyzing the network from service layer, application layer, down to network layer, Colasoft UPM combines network operation and maintenance with service performances, analyzes the performance, quality, fault, and security issues based on business, and thus provides the visibility to business performances. Colasoft UPM helps users promote business oriented, proactive network operational capability, ensure the running of businesses, and enhance troubleshooting efficiency.

2.1. Components

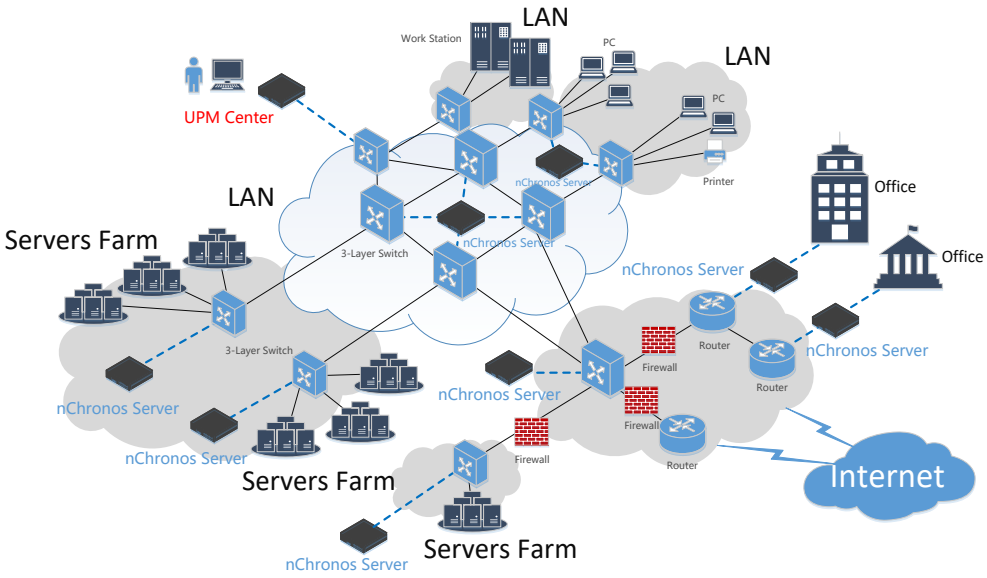
Colasoft UPM consists of nChronos Server and UPM Analysis Center (hereinafter referred to as “UPM Center”).

nChronos server can be deployed at the key nodes on the communication link for business system, and capture business communication data by switch port mirroring or network TAP. The nChronos server collects and analyzes the performance metric parameters and application alarm information in real-time, and uploads to UPM Center via the management interface for overall analysis.

UPM Center is deployed to converge nChronos servers, collect the business performance metrics and alarm information uploaded by nChronos servers, and display the analysis results.

2.2. Deployment

The deployment of UPM is visualized as the following figure:



2.3. System Requirement

Metrics of UPM client usage environment are shown in the following table:

Metric	Minimum
Browser	Google Chrome 50 or higher version Firefox 46 or higher version
Screen resolution	Suggest: 1920×1200 Mininum:1280×800

UPM central servers are available in two models, UPM3010 and UPM 3030.

2.4. Listening Port

Interface	Description
22000	The port for connecting nChronos server to UPM server. nChronos server pushes data to UPM server through this interface. This port should be always on.
22100	The encrypted port for connecting nChronos server to UPM server. nChronos server pushes data to UPM server through this interface after encrypting data with SSL. This port should be always on.
443	The port for accessing UPM webpage. This port should be always on. UPM server firewall will map 443 port to 8080 interface.
8080	The port for accessing UPM webpage. This port does not need to be on.
123	NTP time synchronization interface. If UPM is required to provide NTP service, it should be always on.
22	SSH remote accessing port. It's off by default.
27017	The port used by the MongoDB connection tool. It's off by default.
9200	The port used for internal startup of the ES, and it does not need to be provided to the outside. It's off by default.
9300	The port used for internal startup of the ES, and it does not need to be provided to the outside. It's off by default.
19527-19536	The port used by the UPM server to collect syslog logs. It's off by default.

2.5. Technical Support

Basically, we provide technical support to all users of our products, including commercial customers and freeware users, but please understand that commercial customers have priorities to get help and to be supported within one working day.

For common questions, users can find answers in our Knowledge Base.

Website support

In addition to up-to-date FAQs and glossary, there is version upgrade information and public resources available at http://www.colasoft.com.

Email support

Users are welcome to contact us at support@colasoft.com with technical questions at any time. We will reply users as quickly as possible. Users' email should include information about the serial number of the product, product version and edition, the version of operating system, detailed description of the problem and other relevant information.

Forum support

To get our support, provide users' suggestions and discuss our products with other users, please join our Support Forum.

2.6. Monitor Port

The legitimate monitor port used by UPM is shown in the following table:

Interface	Minimum

22000	nChronos' interface to connect to the UPM server. nChronos pushes data to UPM server through this interface, which should be opened all the time.
22100	NChronos' cryptographic interface to connect to the UPM interface. nChronos encrypts the data and pushes it to UPM server through this interface, which should be turned on all the time.
443	The interface on the UPM server for accessing the Web, which should be turned on all the time. The UPM server firewall will map interface 443 to interface 8080.
8080	The interface on the UPM server for accessing the Web, which doesn't need to be turned on.
123	NTP time synchronization interface. If UPM needs to provide NTP service, it needs to be turned on all the time.
22	SSH remote access interface, which is off by default.

2.7. Default Account

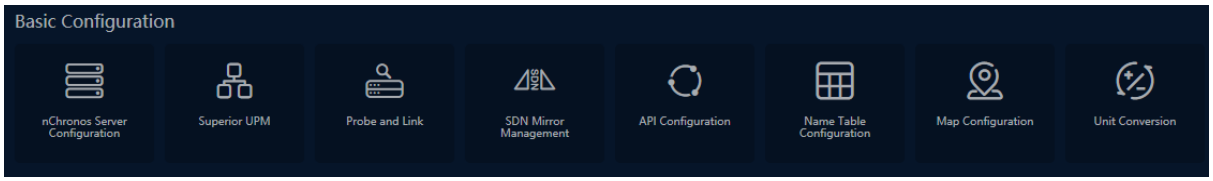
The default accounts provided by UPM are shown in the following table:

Number	User Name	Password	Explanation
1	csadmin	!CSUPM23	UPM web default login account
2	root	!ColasoftL23	UPM server default login account
3	-	ah(G26h@	HTTPS certificate password
4	-	(t*4RE$J	Socket certificate password
5	upm	Y6*(T^7d	Database login password

3. Basic Configuration

Colasoft UPM does the entire monitor and analysis job by analyzing the data from nChronos servers. Therefore, before using UPM to monitor network businesses, it is required to do some basic configurations.

Go to Configuration ->Basic Configurations to enter the Basic Configuration page, as the screenshot below:



Note

The SDN mirror image configuration and API configuration features are only available for specific users.

3.1. Connect UPM to nChronos

The monitoring and analysis of the UPM center relies on the data captured by the front end at various data collection points. Users need to connect the front end to the UPM center.

3.1.1. nChronos Configuration

nChronos is responsible for data collection, analysis, statistics and regular data reporting to UPM center

- Go to Configuration -> nChronos Server Configuration to enter the nChronos server configuration page.
- Access the nChronos server web configuration page -> Analysis Center to connect UPM center.
- View the detail of UPM Center -> nChronos Configuration -> nChronos Server List to check if nChronos server is connected successfully and the connection status is online.

3.1.2. Probe Configuration

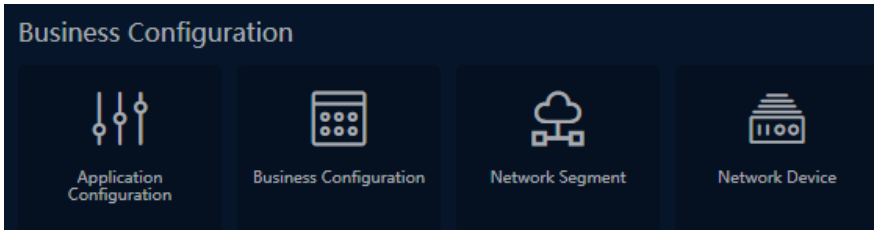
All analysis results on UPM are based on the data collected by probes. One probe indicates one data collection site. UPM probe corresponds to the network link on nChronos server.

Click the menu Configuration -> Probe and Link to open the probe and link configuration page, and click the button “ + “ to open the Add Probe box.

3.2. Business Configuration

Business configuration is the unified entry for business-related configuration items.

Click the menu Configuration -> Business Configuration to open the Business Configuration page.



3.2.1. Application Configuration

Application configuration supports three application categories, standard applications, eigenvalue applications, and WEB applications, among which the standard applications support three application types, short connection, asynchronous double foreman connection and long connection.

Click the menu Configuration -> Business Configuration -> Application Configuration and users will go to the Applications

Note

The configured application will issue to nChronos servers of the central connection, and recognition will be enabled by default.

3.2.2. Business Configuration

Business configuration supports business logic diagrams, business performance evaluation alerts, business performance alerts, and other configurations

- Click the menu Configuration -> Business Configuration -> Business Configuration to open the Business Configuration page. Users can configure business infrastructure information, business logic diagrams, business paths, and business alerts.
- In the business logic diagram configuration, click the “Add Application Relationship” button open the “Add Application Relationship” window and add the required applications. Users can also edit the communication path of the client by adding the application client in the “Application Structure” window.

Note

After the application is added to the business, nChronos server releases the application to enable critical application analysis. Service performance alerts are issued to links mapped by probes on the service path.

3.3. Transaction Configuration

Users can enter the transaction configuration entry interface through the "Configuration> Transaction Configuration" menu.

3.3.1. Data Dictionary Configuration

The data dictionary configuration matches the collected code with the description of the actual business, which facilitates the system to parse the identified code into the information that the user can understand.

Click the menu Configuration -> Transaction Configuration -> Data Dictionary Configuration to open the data dictionary configuration page. Users can add data dictionaries either individually or in bulk. The dictionary codes and dictionary names are unique within each dictionary

Note

When the state of the data dictionary is not enabled and the business field configures the data dictionary property, it is not displayed for selection when the business field values are subsequently set.

3.3.2. Business Transaction Capture Configuration

The configuration of business transaction capturing points is the basis of business transaction analysis. The business field information of the transaction can be automatically obtained after the configuration is completed.

Click the menu Configuration -> Transaction Configuration -> Business Transaction Capture to add capturing points. The applications and probes of different points may be different.

Note

Only applications that have transaction groups mounted on nChronos server show up in the list of applications.

If the status of a collection point is not enabled, the collection point will not be shown in the business transaction metrics configuration and the transaction alarm page.

3.3.3. Business Field Configuration

Business field configuration is mainly about configuring the association relationship between business field and data dictionary, as well as the basic definition of the field, so as to facilitate subsequent analysis and statistics. The system obtains the corresponding business fields according to the configured acquisition points in the configuration of business transaction acquisition points.

- Click the menu Configuration -> Transaction Configuration -> Business Field to set business field properties.
- Click the button  to open the “View Transaction” page. Users can view the probes, transaction groups and transaction information which to the business field belongs.

Note

Users only can configure the captured field, and cannot add fields.

Set the common business fields as query field to improve later data query efficiency.

Only the business fields that are set to query fields can be used in business transaction metrics and transaction alarms.

3.3.4. Business Transaction Metric Configuration

Business Transaction Metric Configuration Configures the business metrics that need to be monitored and analyzed. When configuring, it needs to be associated with business systems and transactions.

Click the menu Configuration -> Transaction Configuration -> Business Transaction Metric to add transaction metrics.

Note

The filter conditions and calculate fields must be enable business fields. The calculate fields must be business fields of numeric type.

3.4. Home page configure

3.4.1. Features

3.4.1.1 Terminology

Blocks

A relatively independent display area or page module in the page.

3.4.1.2 Functional Background

There are many system function menus. After users enter the system, it is not easy to find and quickly enter the required function page.

Most of the cases when users analyze problems are based on specific objects (applications, IPs, sessions, etc.)

For analysis, it is necessary to guide users to find objects quickly.

3.4.1.3. Functional value

Guide users to quickly find the object to be analyzed (application, IP, session, etc.), and the monitoring or analysis view to be viewed.

3.4.1.4 Functional Description

The home page is the entrance to quickly help users obtain the target object of analysis.

The home page is divided into several display blocks, namely: Search, Quick Entry, Personal Collection, Recent Visits, Frequent Visits, and Link List.

Retrieval: Perform associative matching on the input keywords to help users quickly obtain the target object for analysis and perform the next retrieval or analysis operation.

Quick Entry: Support users to add frequently used function pages as shortcut entries, which is convenient to quickly open the function pages. The initial state of the system will default to some shortcut function entries.

Personal Collection: Allows users to add defined monitoring views, analysis views and specific objects (such as links, IPs, applications, services) to their personal collection, as commonly used or special attention analysis objects, to facilitate quick selection of views each time or objects for viewing and analysis.

Recent visits: Display the monitoring view page or analysis page that the user has recently visited, and display the last 20 records

Frequent visits: Displays monitoring view pages or analysis pages that are frequently visited by users, and displays the top 2 0 records in the last 1 5 days by default.

Link List: Displays the data link list, which is convenient to directly search for links for link analysis.

3.4.2. Operation guide

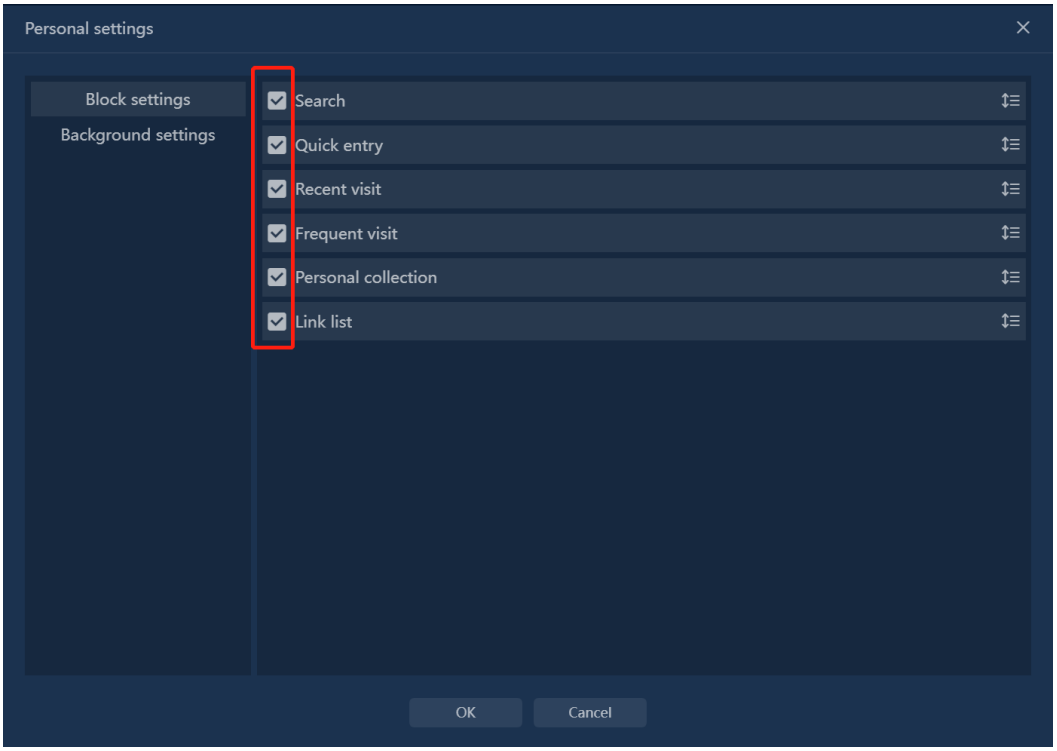
3.4.2.1 Show and hide blocks

Each display block supports hiding and showing, the method of hiding the block:

Method 1: Move the mouse to the right side of the block title, an icon with three dots will appear, click the icon to display the hide button, and click the hide button to hide the block.

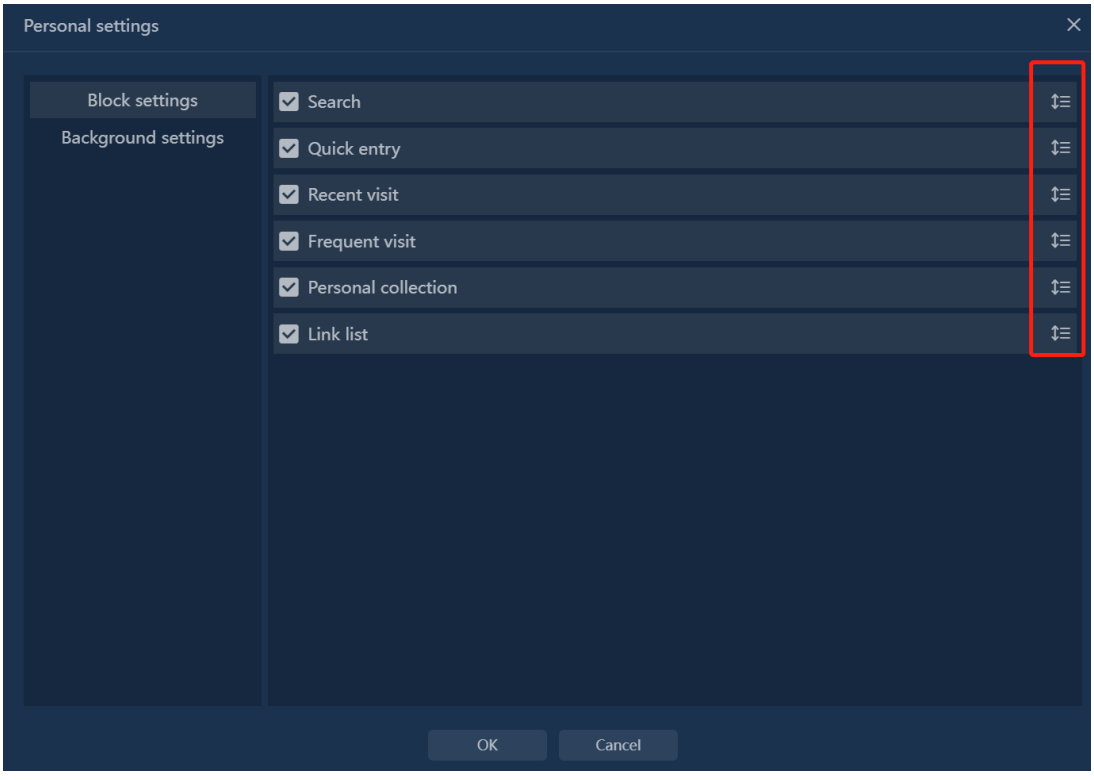
Method 2: In the lower right corner of the home page, there is a home page personality setting button " 

", click the button, and uncheck the checkbox to hide the block in the pop-up window.



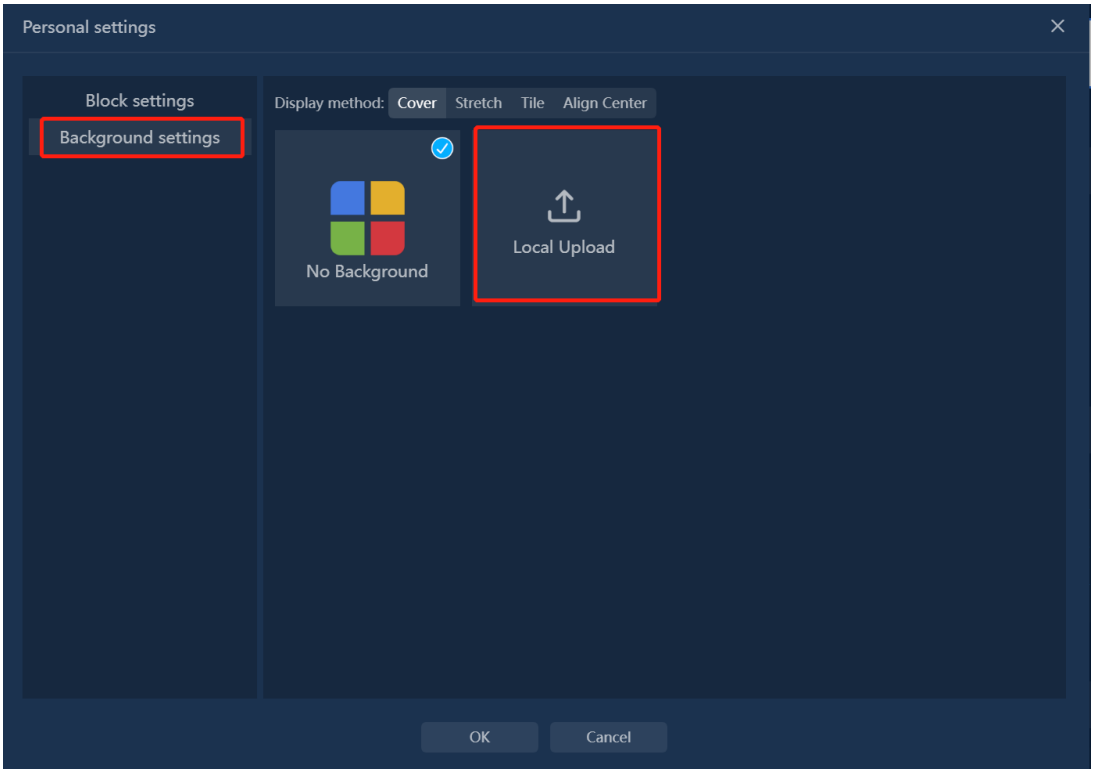
3.4.2.2 Block display sorting

In the lower right corner of the home page, there is a home page personality setting button "Personal settings", click the button and drag the mouse to adjust the display order of the blocks on the home page in the pop-up window.



3.4.2.3 Set the homepage background

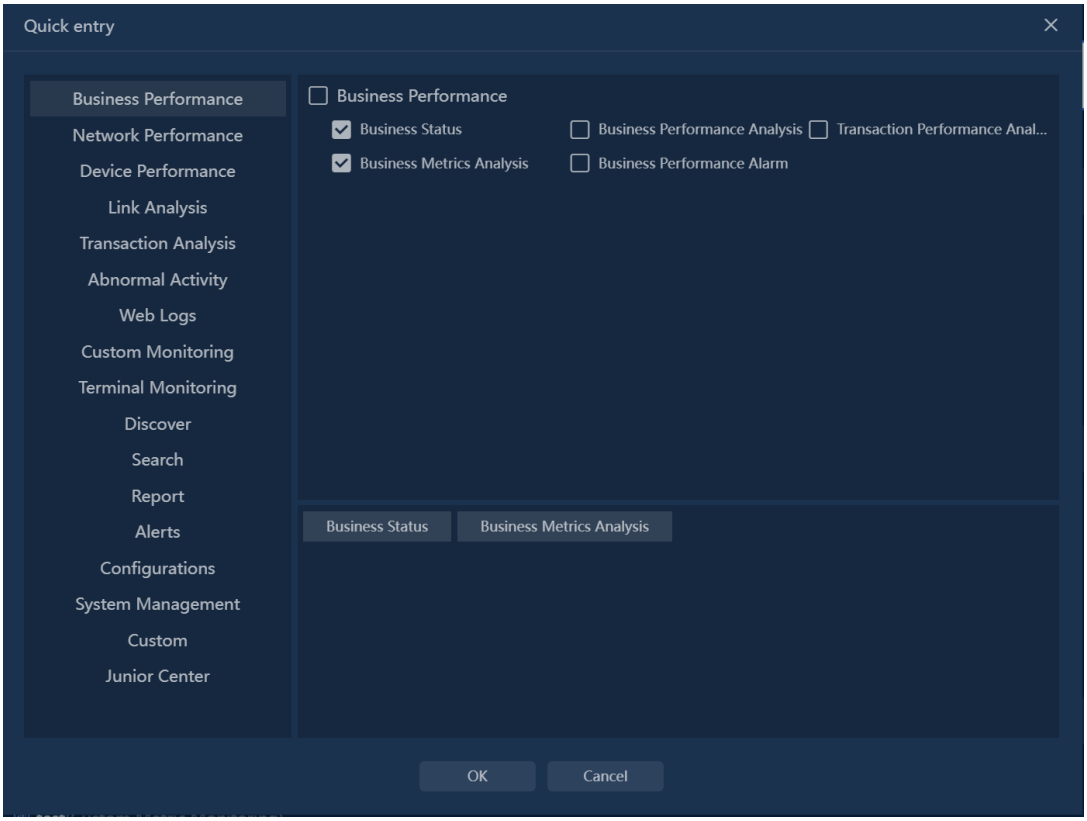
In the lower right corner of the home page, there is a home page personality setting button "Personal settings", click the button and select the background setting in the pop-up window. Supports switching background images, and supports uploading background images.



3.4.2.4 Edit Quick Entry

System default quick entry: business performance monitoring, link traffic analysis, custom indicator monitoring, retrieval, reporting, and configuration.

Allows users to customize quick entries. Move the mouse to the right side of the block title, an icon of three dots will appear, click the icon to display the edit button, click the edit button, the function menu checked in the pop-up window will be displayed in the quick entry block.



3.4.2.5 Edit collection

Supports adding monitoring views, links, applications, IPs, and services to personal collections as commonly used and special attention analysis objects.

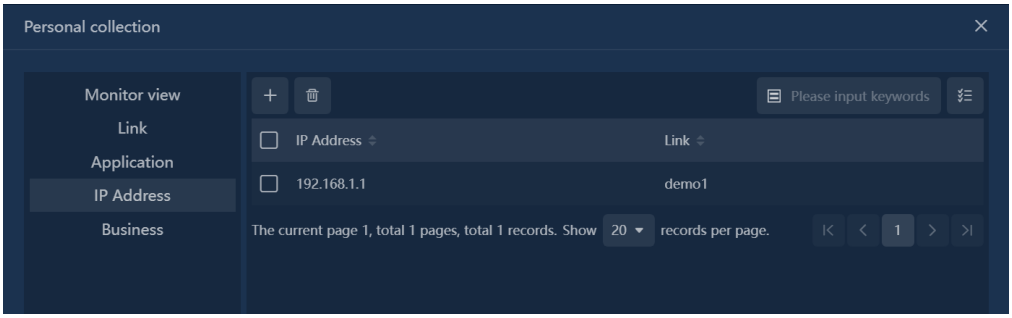
Views that can be saved include: custom monitoring view, custom monitoring large-screen view, network performance monitoring view, network topology monitoring view, scene analysis view, and terminal monitoring view.

Supports collection of all types of links, aggregation, common, and sub-links.

Supports collected application objects and IP objects. When adding, you need to specify the link at the same time.

Support the collection of business, click the business to directly enter the business performance analysis page.

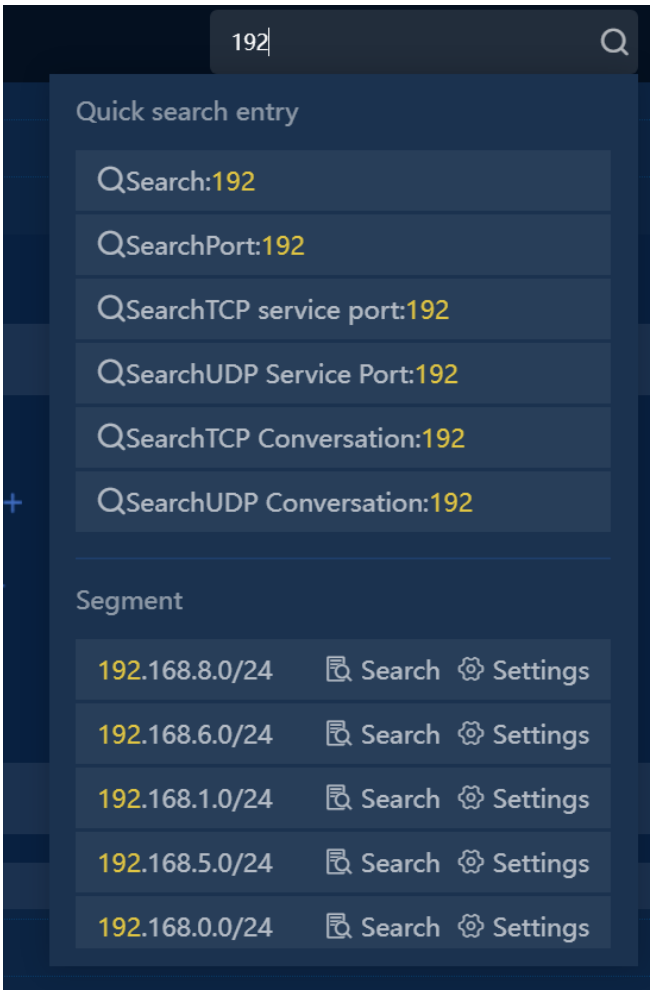
Move the mouse to the right side of the title of the personal collection block, an icon of three dots will appear, click the icon to display the edit button, click the edit button, and add and delete the collected objects according to the object type in the pop-up window. When adding, it only supports adding views and links within user permissions.



3.4.2.6 Associative search

When a user types a keyword in the search input box, the system will automatically perform real-time associative matching and display based on the keyword. The associated range includes: function menu, monitoring view, link, service, network segment, application and other configurations. Appropriate search suggestions are also given.

As shown in the following example: Enter an IP address, the system will recognize it as an IP, and provide retrieval suggestions, and will also show which configurations the IP exists in.



3.4.3. common problem

1. **Whether the content displayed on the home page is bound to the logged-in user one by one**

Problem Description

Are the homepage display blocks and block content bound to the logged-in user, and different users have different homepages?

Question answer

The home page display block and block content are bound one by one with the logged-in user, and different users have different home pages.

When a user logs in to the homepage, the search records, personal favorites, quick entries, and access records they see are all related to the current user.

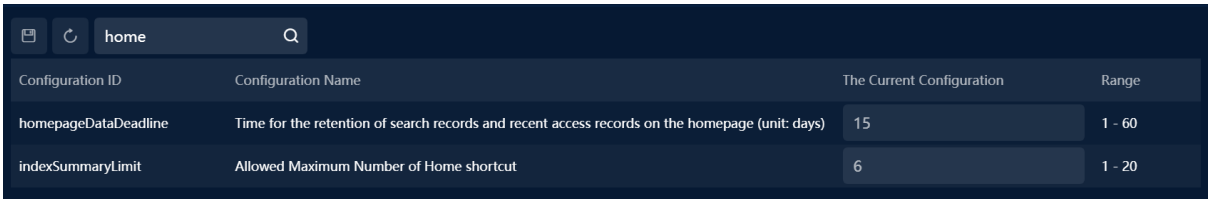
2. **Whether the retrieval records and recent access records are always kept**

Problem Description

Are home page search records and recent visits records always kept?

Question answer

15 days records will be saved by default. The saving time can be adjusted by modifying the system parameters.



3. **Why do I sometimes do a search operation but don't see the search record?**

Problem Description

Why do I sometimes do a search operation and enter a keyword, but I don't see the search record?

Question answer

The system will only log retrievals for:

Case 1: After entering the keyword, press Enter directly on the keyboard to jump to the global search page;

Case 2: After entering the keyword, in the Lenovo drop-down window, select a specific object, click it, and jump to the page.

4. Other Configuration

4.1. Network Segment Configuration

- Click the menu Configuration -> Business Configuration -> Network Segment to open the network segment configuration page.
- Single addition and batch export of network segments are supported.
- remote update of network segment via FTP is supported. Click the button "  " to configure remote update.

Note

The configuration function is consistent with the network path combing, and the network segment information of the two pages after adding/editing network segments will be updated at the same time.

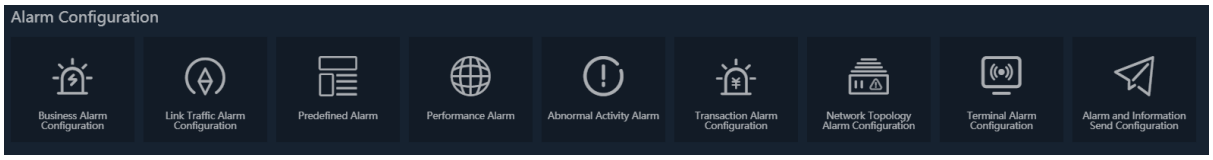
4.2. Issue Strategy Configuration

- Click the menu Configuration -> Business Configuration -> Issue Strategy to open the issue strategy configuration page.
- Click button  to open the issue strategy adding window.
- When configuring applications and network segments, please select the expected issue strategy. When no issue is specified, the application and network segment configuration will be issued to all links.

4.3. Alarm Configuration

The Alarm configuration menu is a unified entry for all system alarms configuration.

Users can go to the alarm configuration portal through the Configuration> Alarm Configuration menu, as shown in the following figure:

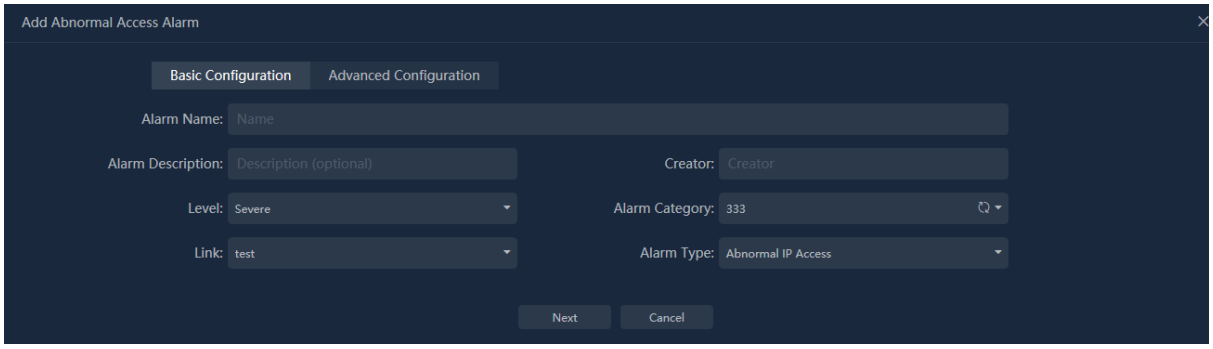


4.3.1. Abnormal Access Alarm Configuration

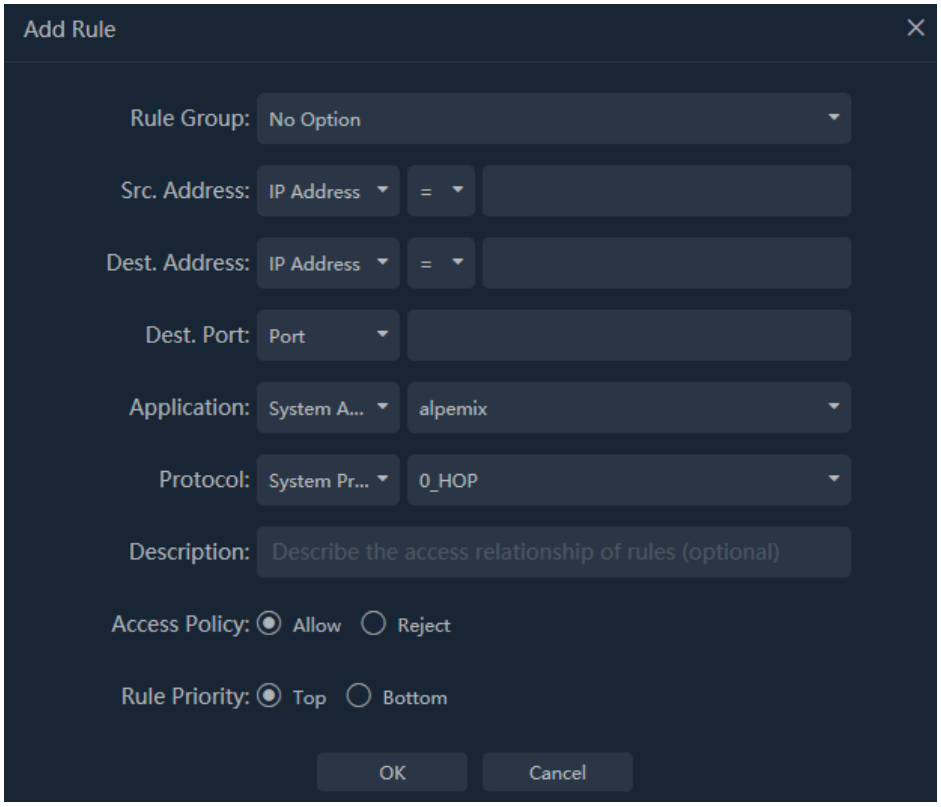
Abnormal Access Alarm Configuration is used to find out illegal or abnormal network access activities.

Click the menu Configuration -> Alarm Configuration -> Abnormal Activity Alarm to open the alarm configuration page.

- Step 1: Enter the alarm basic information and select a link.



- Step 2: Configure access trigger rules. The elements of each rule include source IP, target IP, target port, application and protocol.



  - Each rule consists of elements such as source IP address, destination IP address, destination port, application, and protocol.
  - Rules have priorities. When detecting alarms, they are checked in the order of rule priorities. When a rule is hit and the rule access policy is set to deny, an alarm is triggered.
  - Rules can be managed and prioritized by rule groups.

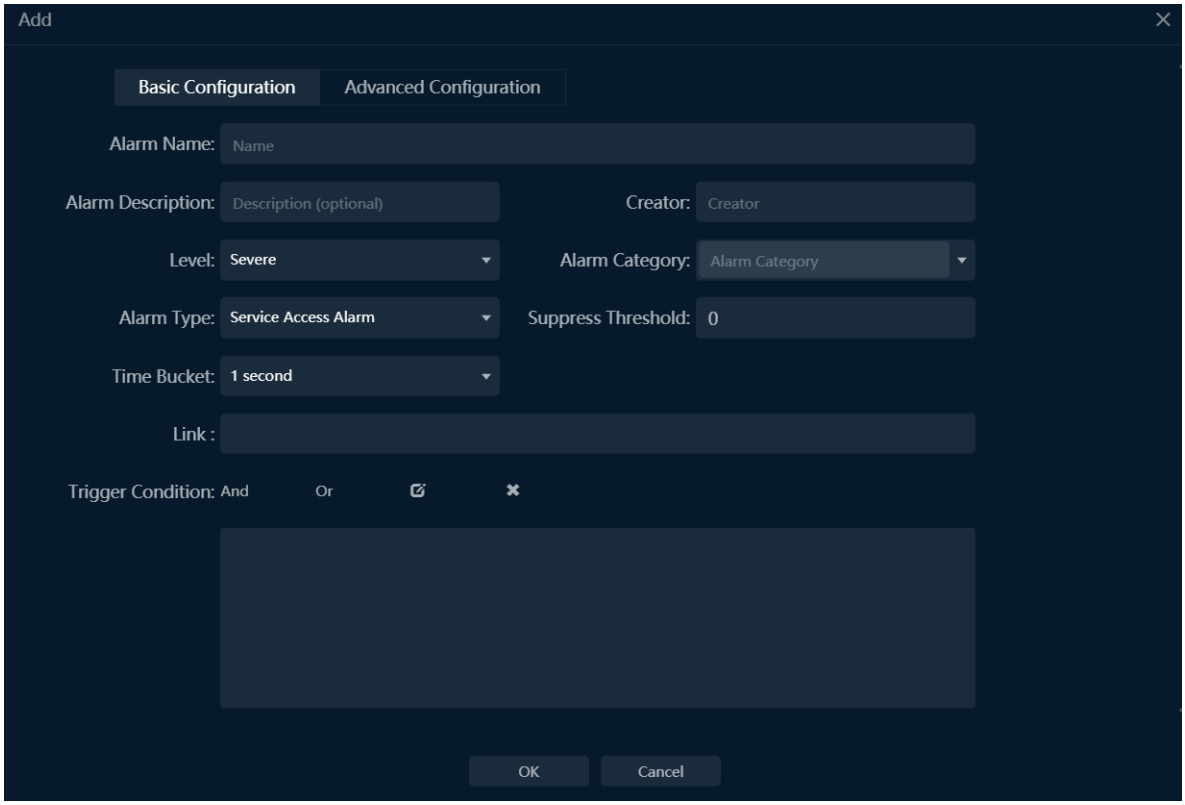
MAC abnormal access rules:.

  - Each rule consists of elements including MAC address, alias, and description.
  - Configured MAC addresses are whitelisted. When detecting alarms, if a MAC address is not in the rules, an alarm is triggered.
  - Rules can be managed by rule groups.

4.3.2. Abnormal Traffic Alarm Configuration

Abnormal Traffic Alarm Configuration is used to find out the conversations with abnormal traffic metrics in the network.

Click the menu Configuration-> Alarm Configuration -> Abnormal Activity Alarm to open the alarm configuration page. Enter the alarm basic information.

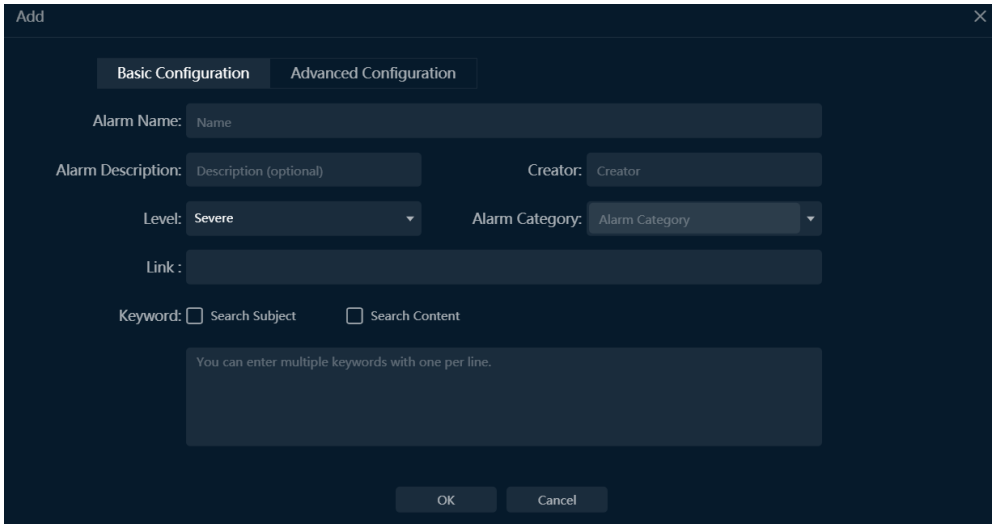


- Alarm Type: IP address, IP conversation, network segment, application, segment-segment, VLAN and so on.
- Time Bucket: The time cycle unit for judging if the trigger condition is met.
- Suppress Threshold: When the value is greater than 0, N consecutive time buckets (time units) simultaneously meet the trigger conditions.
- Link: The data range for alarm detection.

4.3.3. Email Alarm Configuration

Email Alarm Configuration is used to find out if a particular keyword information exists in the header or the body of an email in the network.

Click the menu Configuration-> Alarm Configuration -> Abnormal Activity Alarm to open the alarm configuration page. Enter the alarm basic information.

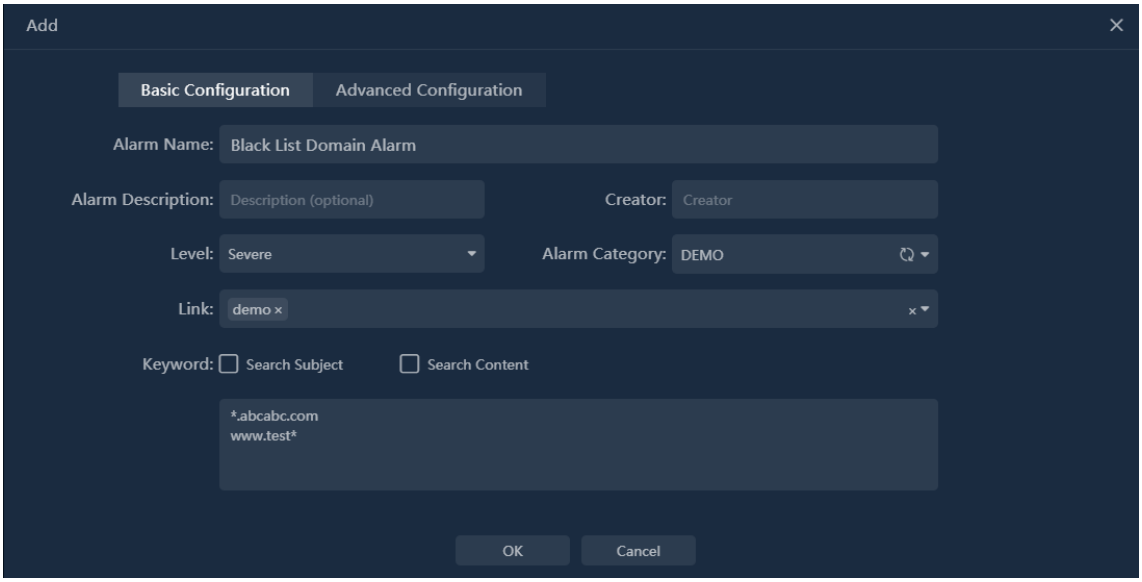


Multiple feature keywords are separated by “Enter”.

4.3.4. Domain Alarm Configuration

Domain Alarm Configuration is used to find out the activities of accessing specified domain and IP address in the network.

Click the menu Configuration-> Alarm Configuration -> Abnormal Activity Alarm to open the alarm configuration page. Enter the alarm basic information.

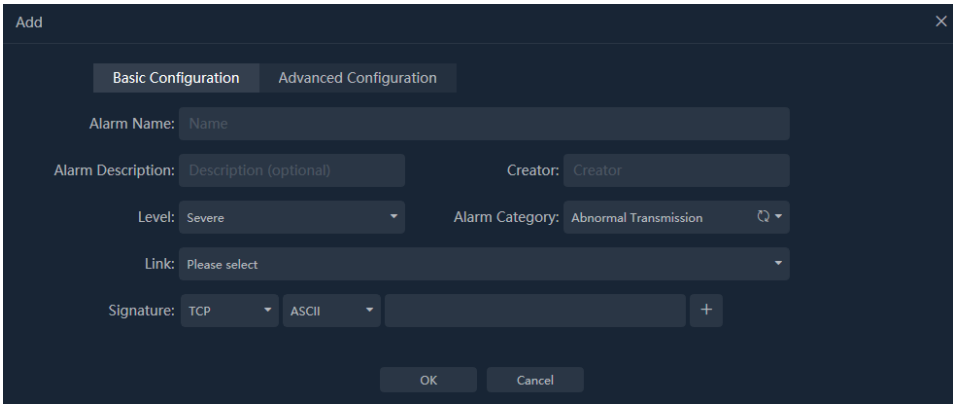


- Multiple IP or domain names are separated by “Enter”.
- Fuzzy matching is supported and the “*” is a wildcard.

4.3.5. Signature Alarm

Signature Alarm Configuration is used to find out characteristic keywords specified in network conversation transmission packets, such as Trojan characteristics.

Click the menu Configuration-> Alarm Configuration -> Abnormal Activity Alarm to open the alarm configuration page. Enter the alarm basic information.

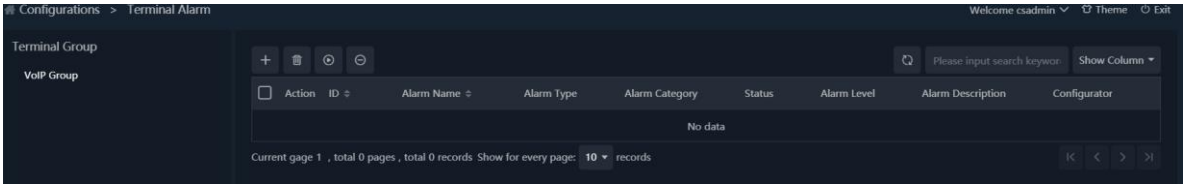


- Signature can be encoded in ASCII and hexadecimal.
- Multiple signature can be added to make the matching more accurate.

4.3.6. Terminal Alarm Configuration

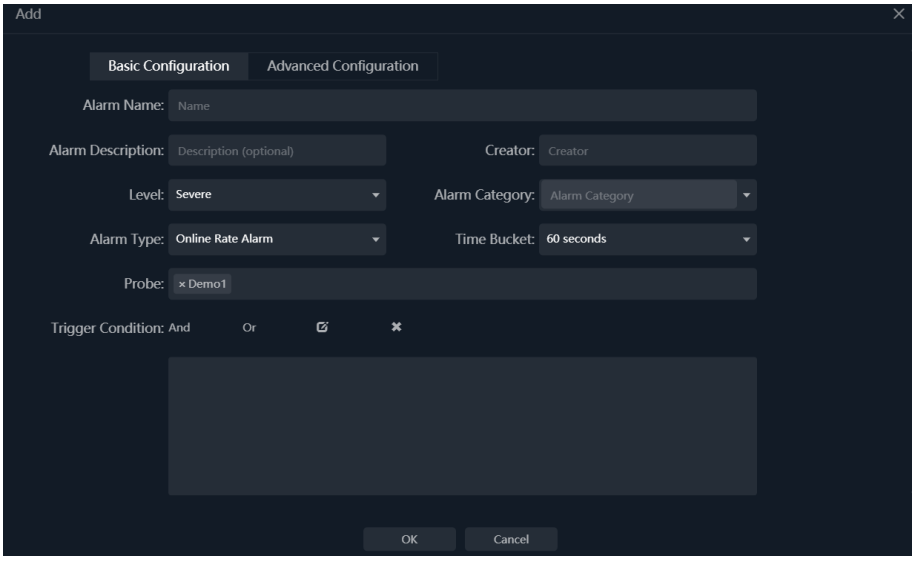
Users can go to the Terminal Alarm Configuration page via Configuration> Alarm Configuration -> Terminal Alarm Configuration.

Terminal alarm configuration page as shown below:



On the left side of the page is the terminal grouping (level 1 nodes). Alarms are configured by group, and the alarms are only valid for the terminals under the corresponding group.

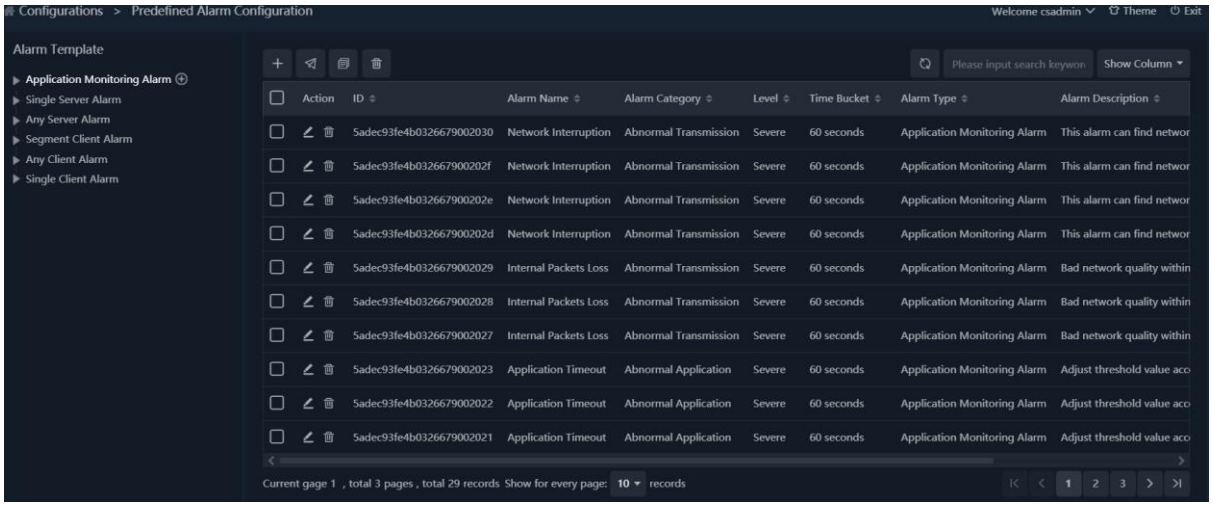
To add a terminal alarm, users can click the button “ + ” to enter the dialog box, as shown below:



- Choose different types of alarms depending on users’ needs.
- In the advanced configuration, we mainly configure the effective time period and the way of sending the alarm.

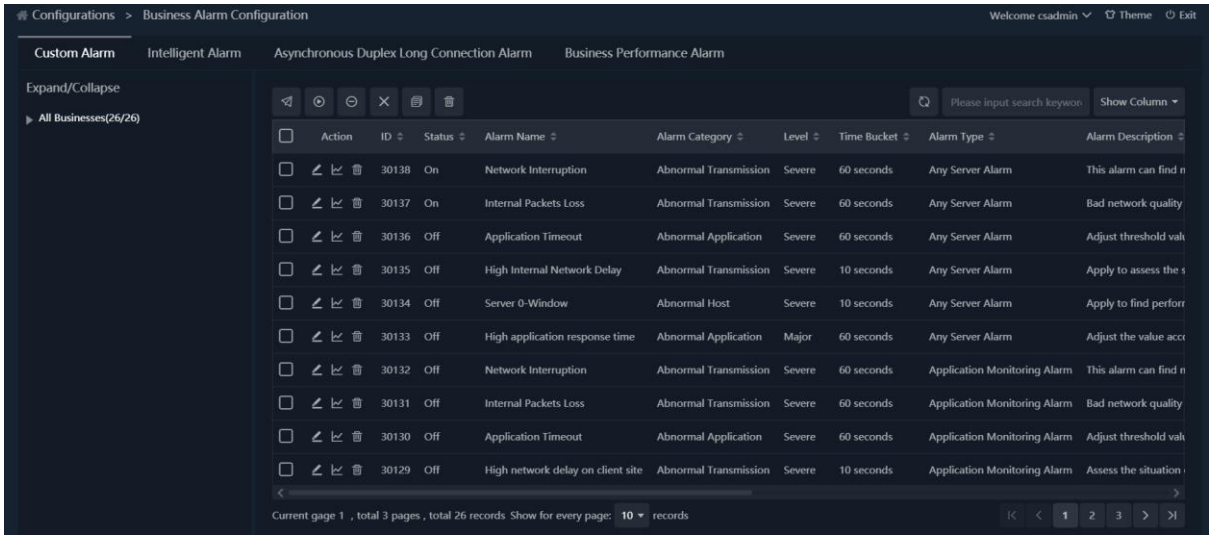
4.3.7. Predefined Alarm Configuration

UPM Center provides predefined alarm template feature. When defining a business, users can select predefined alarm template. By default, system provides six alarm types: Application Monitoring Alarm, Single Server Alarm, Any Server Alarm, Segment Client Alarm, Any Client Alarm, and Single Client Alarm. For each alarm type, users can define corresponding type of alarm, as the screenshot below:



4.3.8. Business Alarm Configuration

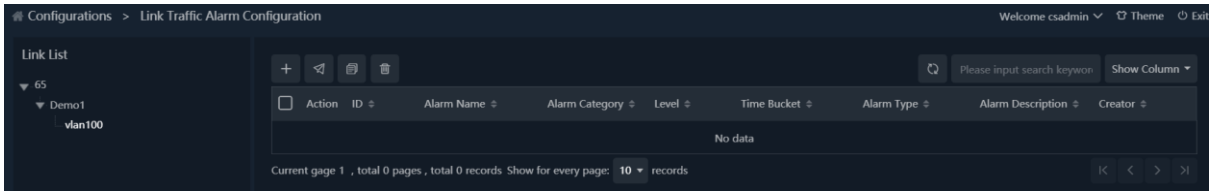
Click the menu Configurations -> Alarm Configuration -> Business Alarm Configuration to open the Business Alarm Configuration page, as the screenshot below:



On the Business Alarm Configuration page, users can manage and configure all business alarms. There are three types of business alarms: Customized Alarm, Intelligent Alarm, and Asynchronous Duplex Long Connection Alarm.

4.3.9. Link Traffic Alarm Configuration

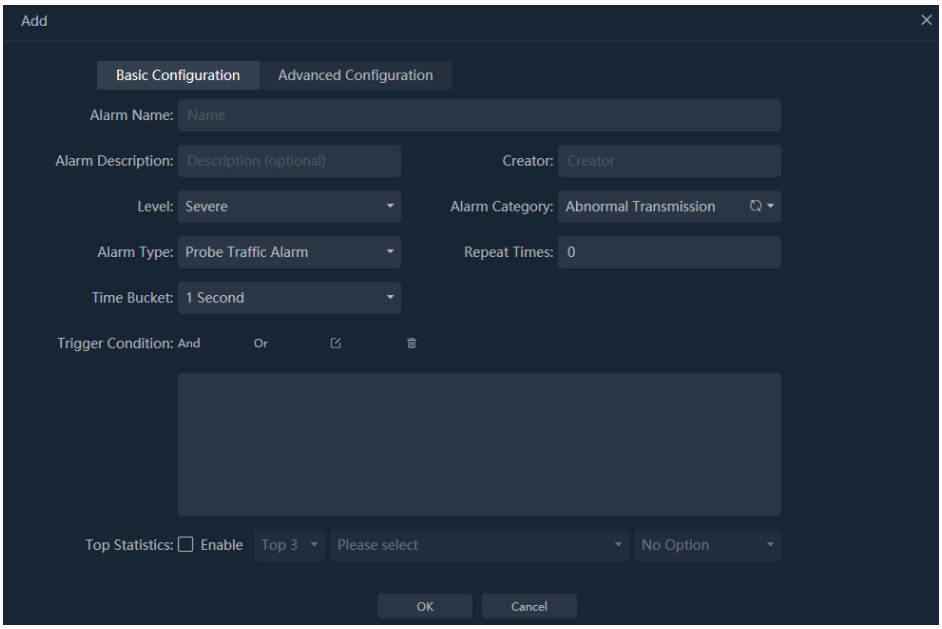
Click the menu Configurations -> Alarm Configuration -> Link Traffic Alarm Configuration to open the Link Traffic Alarm Configuration page, as the screenshot below:



The link List displays all nChronos servers connected UPM Center and the links for each nChronos server. Select a node and then click the button " + " to add an alarm.

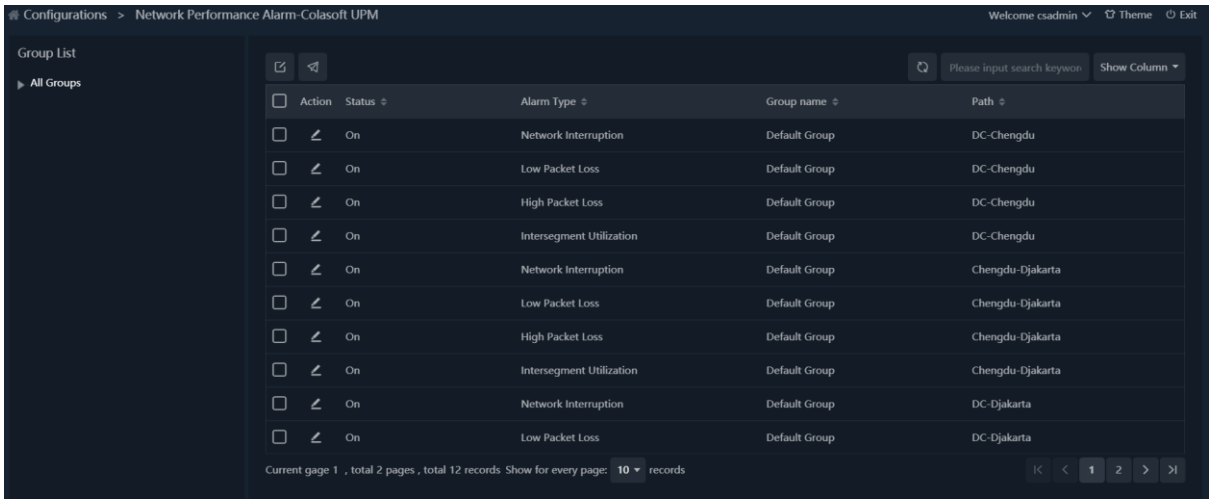
If the selected node is an nChronos server, then the added alarm will be forwarded to all links on that nChronos server; if the selected node is a link, then the added alarm will be only forwarded to that link.

The Add Alarm box shows as the screenshot below:



4.3.10. Network Performance Alarm Configuration

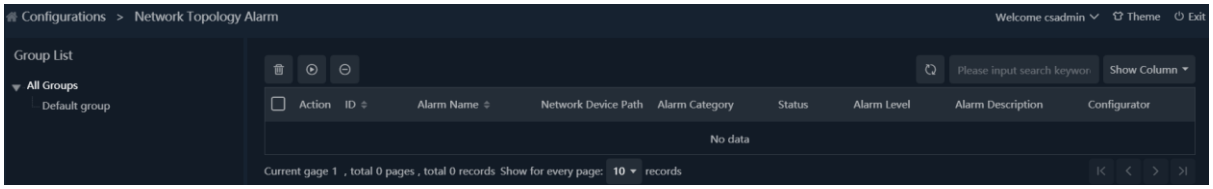
Click the menu Configuration -> Alarm Configuration -> Network Performance Alarm Configuration to open the Network Performance Alarm Configuration page, as the screenshot below:



UPM Center will generate Network Performance Alarm automatically according to the intelligent analysis for network path. Network Performance Alarm includes Network Interruption, Packet Loss, etc.

4.3.11. Network Topology Alarm Configuration

Click the menu Configuration -> Alarm Configuration -> Network Topology Alarm Configuration to open the Network Topology Alarm Configuration page, as the screenshot below:

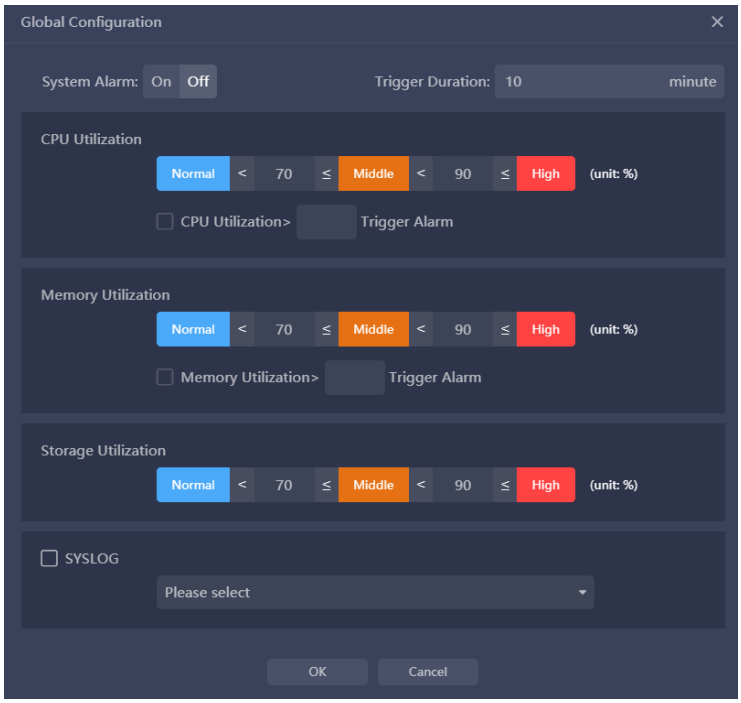


Network Topology Alarm Configuration is an alarm configuration for custom metric between network devices.

4.3.12. System Alarm

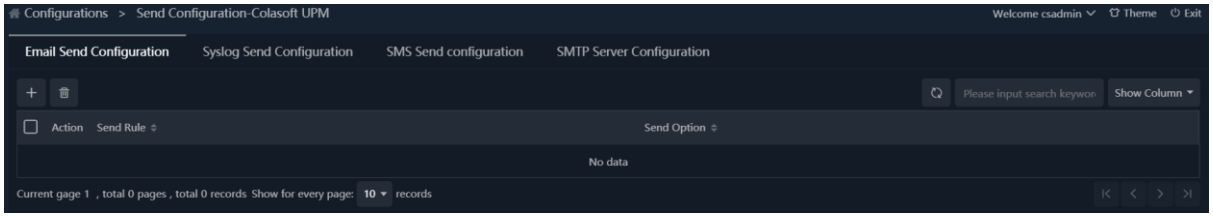
System alarm is to alarm CPU, memory and online status.

Click Configuration -> nChronos Server Configuration -> nChronos Server List to enter the front-end list page. Click to open the system alarm configuration window, as shown in the following figure:



4.3.13. Alarm and Information Send Configuration

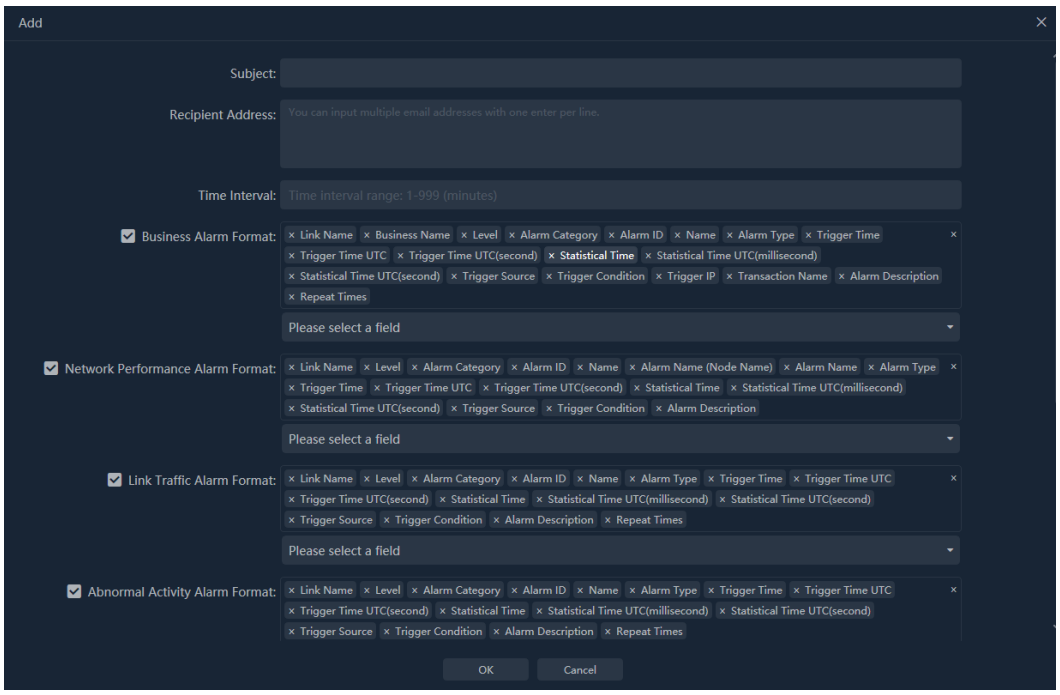
Click the menu Configuration -> Alarm Configuration -> Alarm and Information Send Configuration page, which includes Email Send Configuration tab, Syslog Send Configuration tab, SMS Send Configuration tab and SMTP Server Configuration tab, as the screenshot below:



4.3.14. Email Send Configuration

The alert sending page is used to set the subject of the message, the recipient of the alarm, and the interval between when the alarm is sent.

To add a send rule, click the button " + " to open the Add Send Rule box, as the screenshot below:

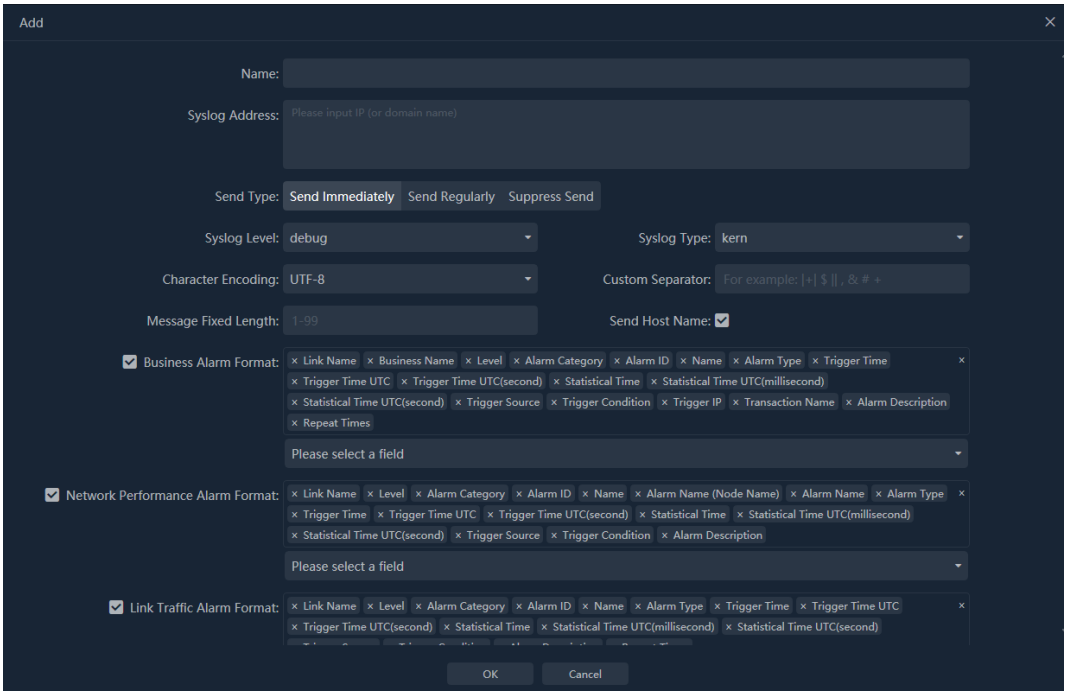


4.3.15. Syslog Send Configuration

The Syslog Send Configuration tab is for setting syslog server address, send method and syslog format. The syslog send rule is related to alarm category, users can set one send rule for multiple categories, and users can also set one send rule for one category.

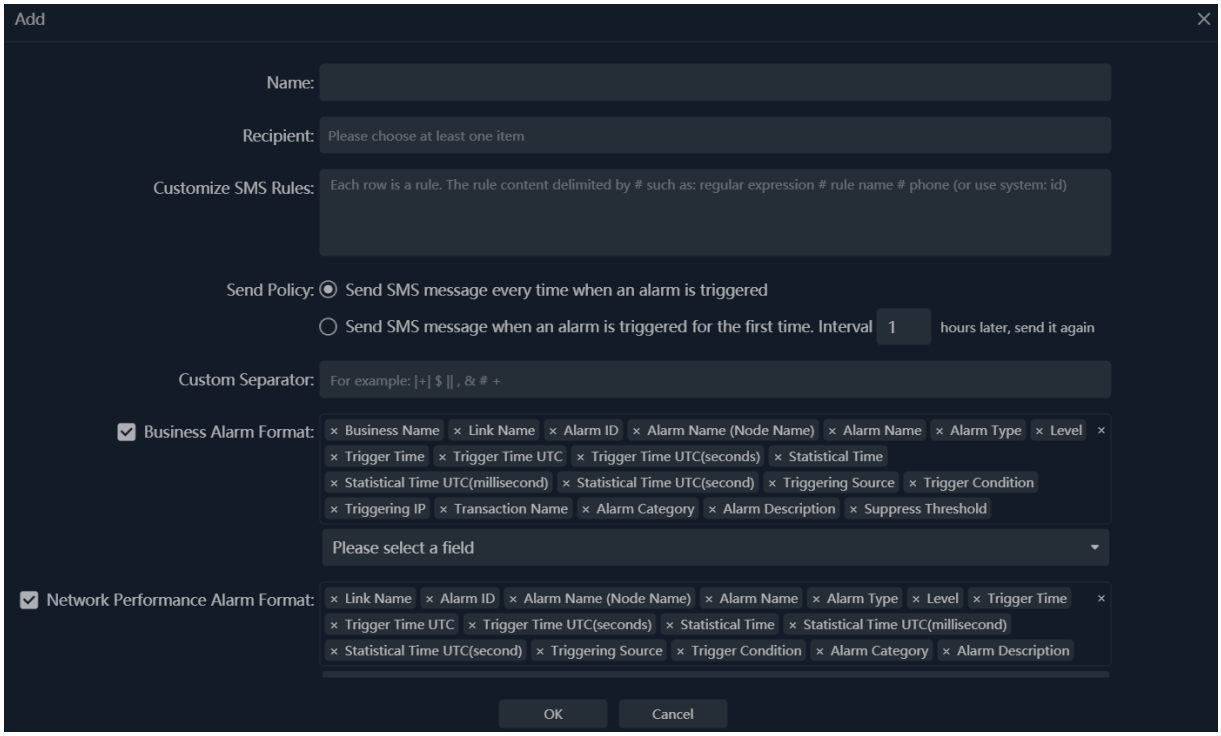
When setting syslog format, it is required to configure send format based on the alarm type (business alarm, network alarm, probe alarm) that the alarm category belongs to. If users don't configure send format for an alarm type, alarm logs of that alarm type will not be sent via syslog.

To configure a syslog send rule, click the button " + " to open the Add Send Rule box, as the screenshot below:



4.3.16. SMS Send Configuration

The SMS Send Configuration is used to set the recipient of SMS message, the sending policy and the SMS message format.



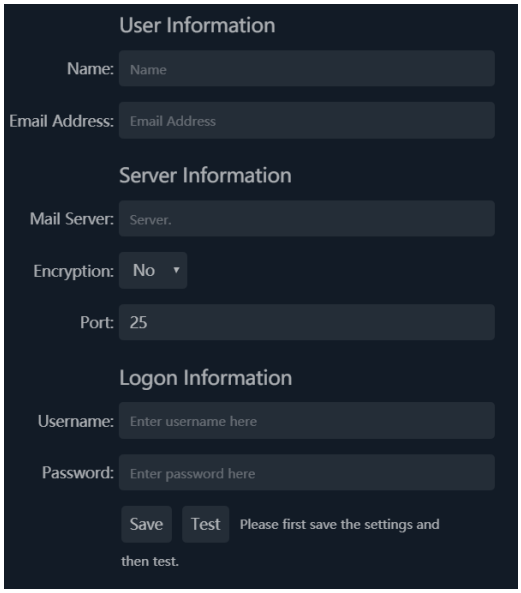
4.3.17. SMTP Server Configuration

To successfully send alarm logs and SLA reports to email inbox, users have to configure SMTP server settings correctly.

The setting options are described as below:

- Name: The name of the sender.
- Email Address: The email address of the sender.
- Mail Server: The address of the email server.
- Encryption: The encryption connection type of email server.
- Port: The port number for the encryption connection.
- Username: The user name of the sender to logon the email server.
- Password: The password for the sender address.

After the configuration, users can click Test to check it.



Parameter Name	Parameter Description
Name	The name of the sender.
Email Address	The email address of the sender.
Mail Server	The address of the mail server.
Encryption	The encryption method supported by the system is SSL.
Port	The port of the mail server. If encryption is not selected, the default port is 25; If SSL is selected as the encryption method, the default port is 465.
Username	Sender's email.
Password	Sender's email password. When configuring system support, user authentication is not required, which means the password can be left empty.

4.4. VoIP Terminal Management Configuration

Please refer to 11.1 **Terminal Management**.

4.5. Name Table Configuration

In the name table configuration, users can customize aliases for IPv4 address, IPv6 address, MAC address, IP address, VLAN ID, MPLS VPN ID, DSCP ID, ISL VLAN ID, VXLAN ID and Netflow ID for easy identification and management of network Settings.

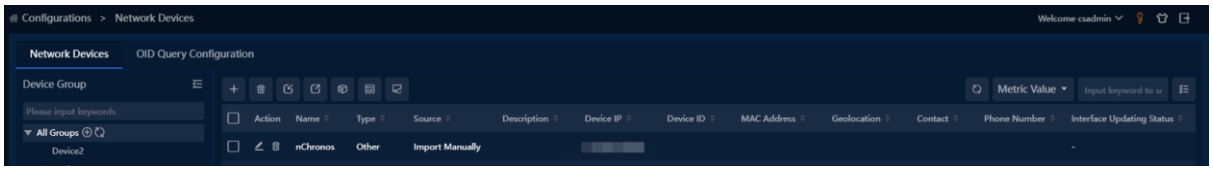
4.6. API Configuration

Please refer to the API document.

4.7. Network Device Configuration

Network device Configuration You can add existing network devices, such as switches, routers, and firewalls, to the system. The configuration page consists of the device group tree list and device list, as shown in the following figure:

Network device configuration page



The following table describes the functions supported by the root node and device group node in the device group tree list:

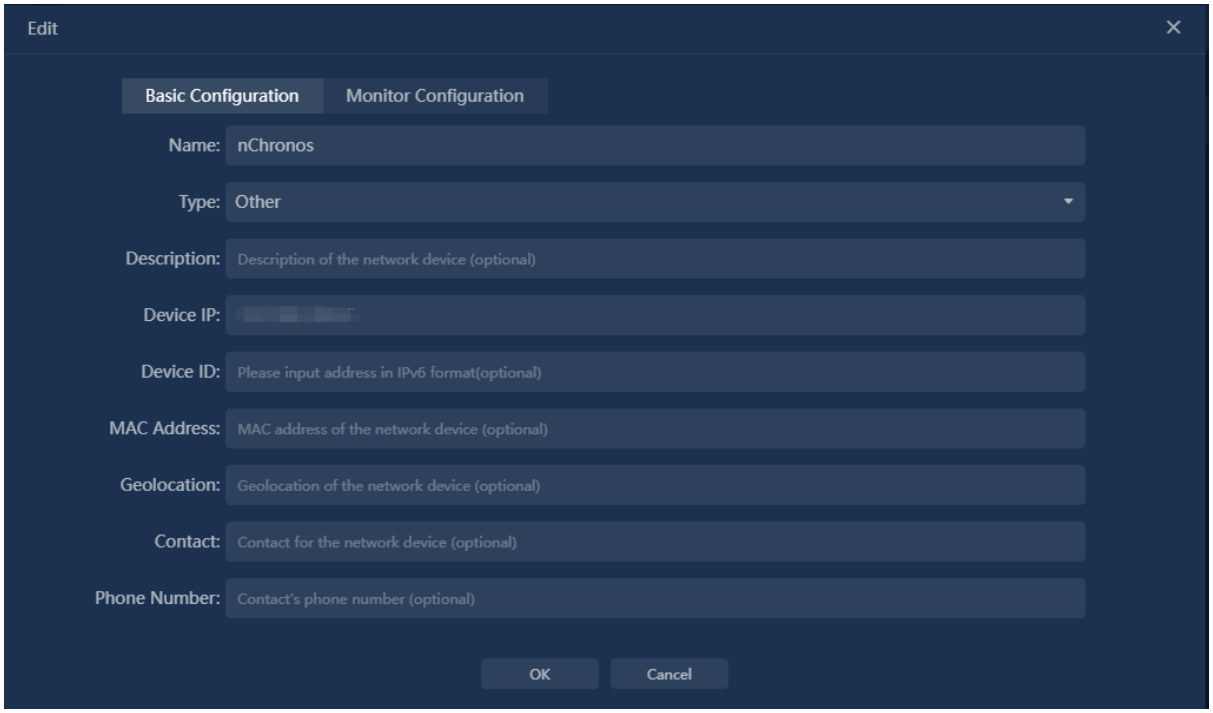
Operation	Instruction
	Add subgroups
	Edit current group
	Delete current group
	Refresh interface information

The following table describes the functions of the operation bar on the top of the device list:

Operation	Instruction
	Add network devices, please refer from3.1.1 nChronos configuration 3.1.2 probe configuration
	Delete network device
	Export network device configurations
	Inport network device configurations
	Mobile network configuration
	Batch set query templates
	You can configure the frequency of automatic interface updates and synchronize the interface names to the enabled/disabled status of the name list.

4.7.1. Basic Configuration

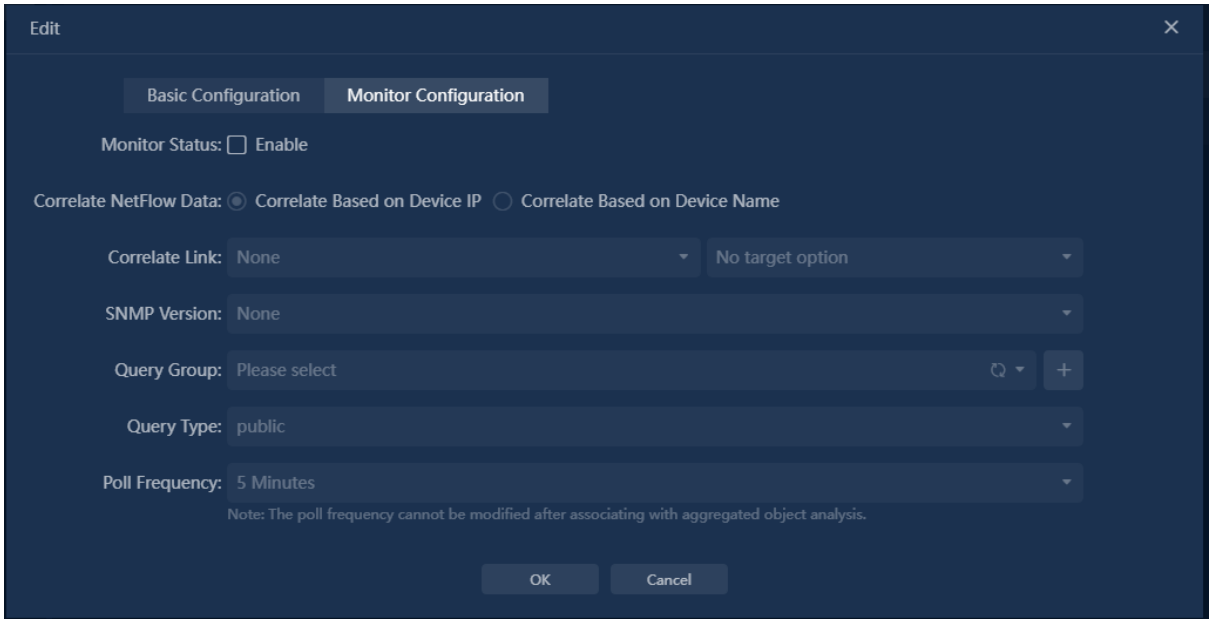
Click , add network devices, Basic Configuration setting as shown in the following figure:



Name and Device IP address in basic configuration This parameter is mandatory. The Device IP address is used as the proxy IP address for SNMP monitoring.

4.7.2. Monitor configuration

Click , add network devices, Monitor Configuration setting as shown in the following figure:



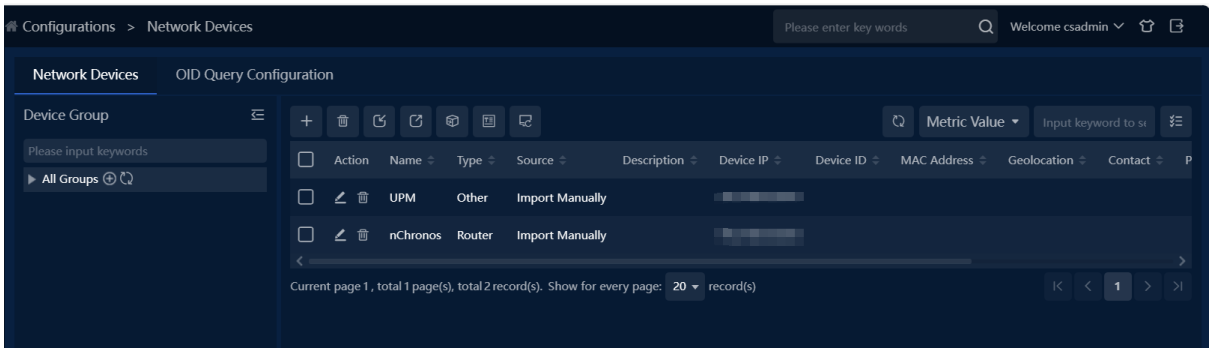
Monitoring status is disabled by default. After enabling the function, you need to set the following parameters:

Operation	Instruction
Correlate NetFlow Data	Automatically associate backtracking NetFlow links based on device proxy IP or name
SNMP Version	Support SNMPv1、SNMPv2、SNMPv3
SNMP Community	Select SNMPv1 or SNMPv2 need to set community. If select SNMPv3, no need to set community, but security parameters are necessary.
Poll Frequency	Five frequency are supported: 5 sec、10 sec、30 sec、1 min、5 min. One or five minute frequencies are recommended.
Query Type	The default category public is selected. You can switch to a custom category. The category determines which OID is used for device polling.

Note：The Query Type corresponds to the OID Query Type configured, helping the device determine which OID in the indicator configuration is used for query.

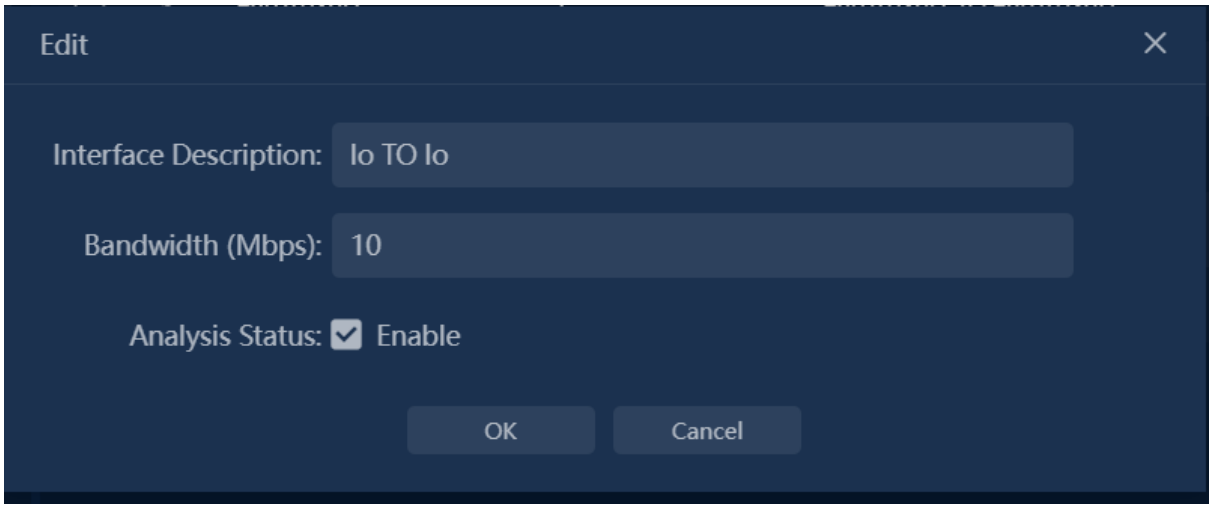
4.7.3. Interface configuration

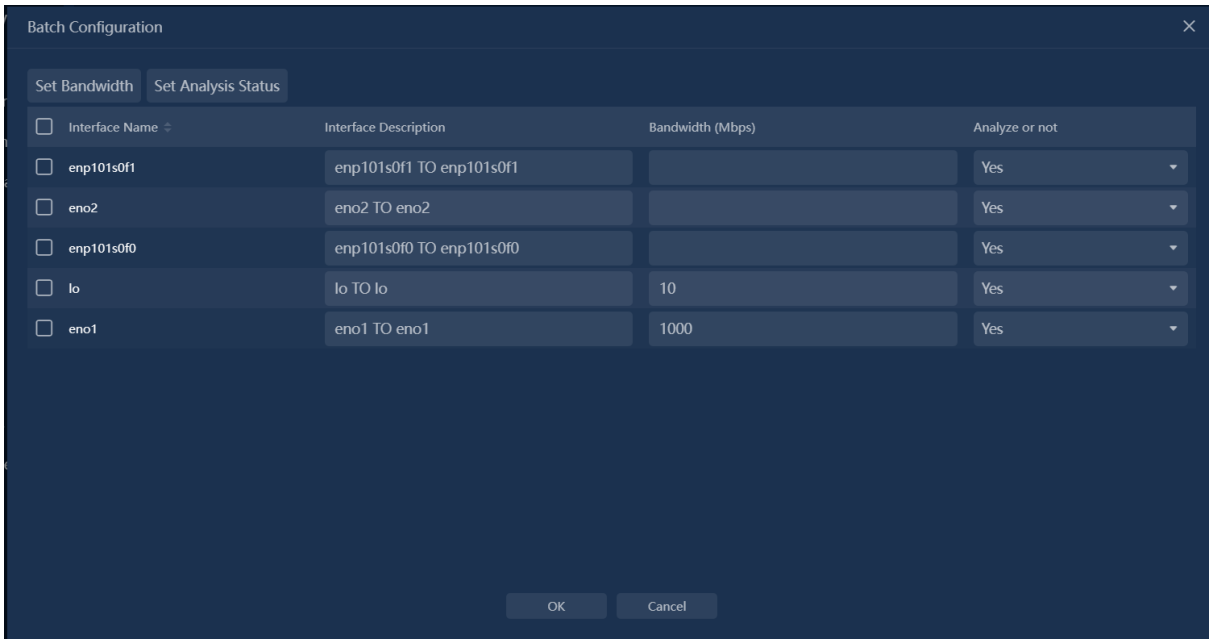
After the device monitoring configuration is complete, the interface information is automatically obtained. Click the device name node in the tree to view the list of interfaces.



Operation	Description
	Batch edit interfaces, support configuring interface description, interface bandwidth, and enabling interface trend analysis.
	Delete Network Device
	Export Network Device Configuration

Individual interface configuration and batch interface configuration. As shown in the following figure:

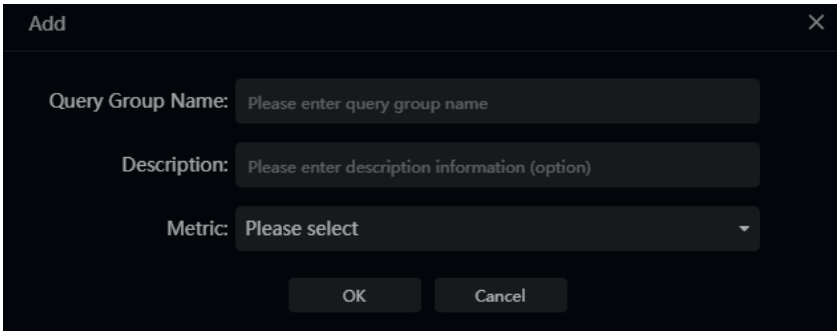




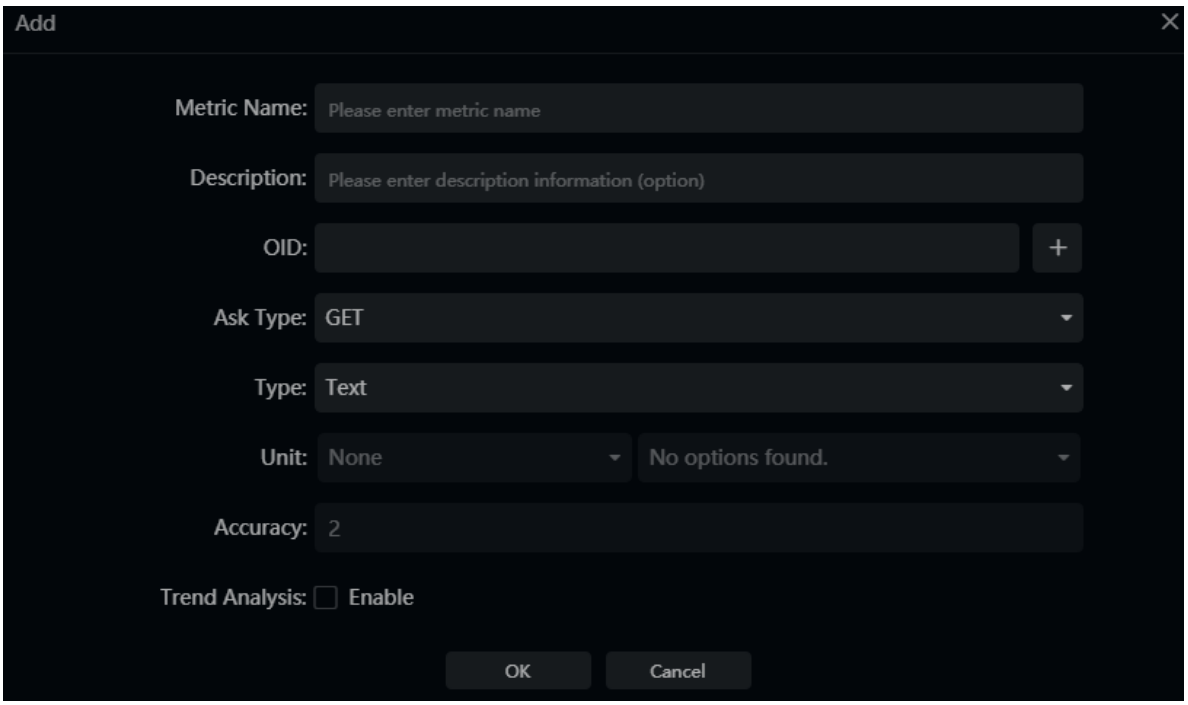
4.8. OID Query Configuration

OID Query configuration used to configure and manage monitoring indicators (including common indicator configuration and computing indicator configuration), indicator groups, and query templates. The OID query configuration page consists of a query template tree list and an indicator list

go to Configuration -> OID Query Configuration. Click the Add button “ + ” to open the Add Query Group box, as the screenshot below:

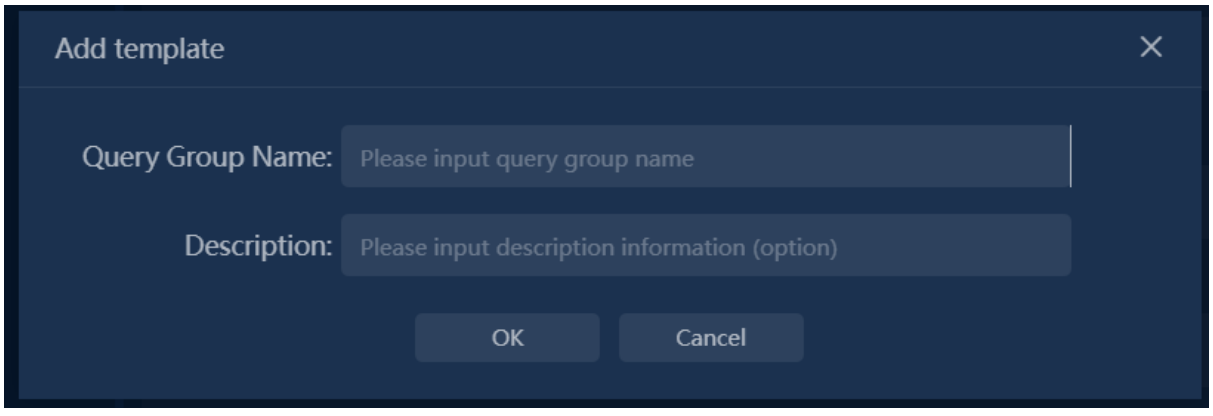


Click the Add button " + " to open the Add Metric Configuration box, as the screenshot below:



4.8.1. Query Template Configuration

The system has built-in default templates. Users can click the button on the right side of all query template nodes to add custom query templates, as shown in the following figure:



Operation	Description
	To add a query template, please refer to 3.2.1 Query Template Configuration
	Edit Query Template
	Delete Query Template

Operation	Description
	To add a regular index, please refer to 3.2.3 Regular Index Configuration
	Delete Index
	Compile MIB library and display OID tree list.
Add Calculation Index	To add a calculation index, please refer to 3.2.4 Calculation Index Configuration
Index Filtering	Filter options include: All Indexes, Regular Indexes, Calculation Indexes

4.8.2. Metric Group Configuration

Metrics of the same group will be displayed on the same trend chart in device performance analysis. The system has built-in three default metric groups, including:

- Packets per second, including metrics for packets received per second and packets sent per second.
- Bit rate, including metrics for received bit rate and sent bit rate.
- Bandwidth utilization, including metrics for received utilization and sent utilization.

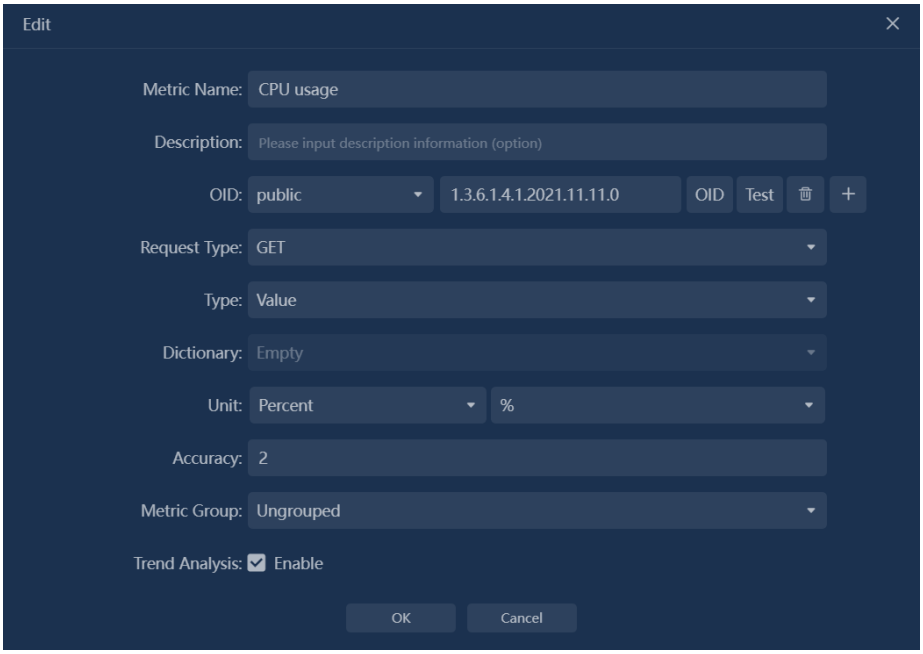
 Users can click the button on the right side of the template node to add custom metric groups

4.8.3. General Indicator Configuration

The system has built-in default general indicators, including:

- Total number of sent packets
- Total number of received packets
- Total number of received bytes
- Total number of sent bytes
- Interface bandwidth
- Interface status
- Interface description
- Interface name
- Interface identifier
- Number of interfaces

Users can click the  button to add custom general indicators, as shown in the following figure:



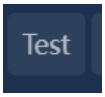
Monitoring indicators need to configure metric name, OID, OID dictionary, request type, value type, unit, and trend analysis enable status.

The configuration is explained in the following table:

Operation	Description
OID	Configure OID query category and OID, supports configuring multiple OID. Support quick addition of OID, testOIDavailability.
Request Method	GETand WALK methods.
Value Type	Text and Numeric types
Unit	
Decimal Places	
Metric Group	Configure the associated metric group
Trend Analysis	Enable/Disable the analysis configuration

Units can be configured in 'Settings' -> 'Unit Conversion'.

OIDs can be quickly added through MIB compilation. After compilation, select the desired OID and click 'OK' to automatically fill in the OID input box in the metric configuration.

OIDs can be tested to verify their availability. Click the button: 

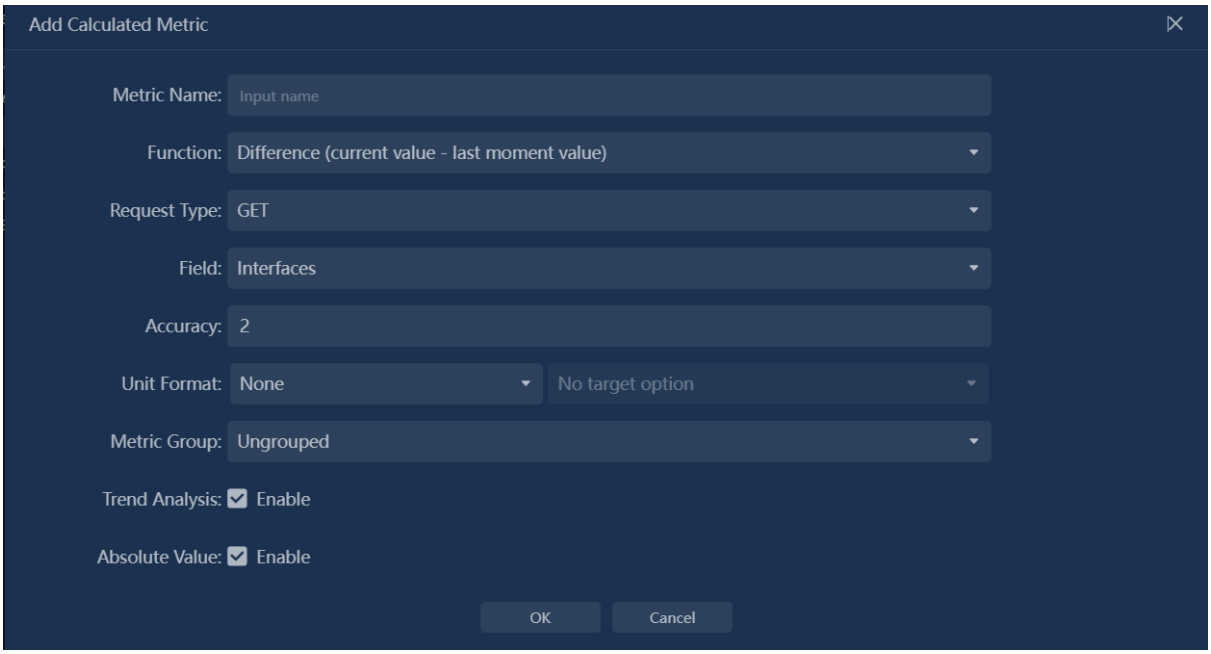
4.8.4. Computed Metric Configuration

The system has built-in computed metrics, including:

- Received Packets
- Sent Packets
- Received Bit Rate

- Sent Bit Rate
- Received Byte Count
- Bytes Sent
- Packets Received per Second
- Packets Sent per Second
- Receive Utilization
- Send Utilization

Users can click the button Add Calculated Metric to add custom calculation metrics, as shown in the figure below:



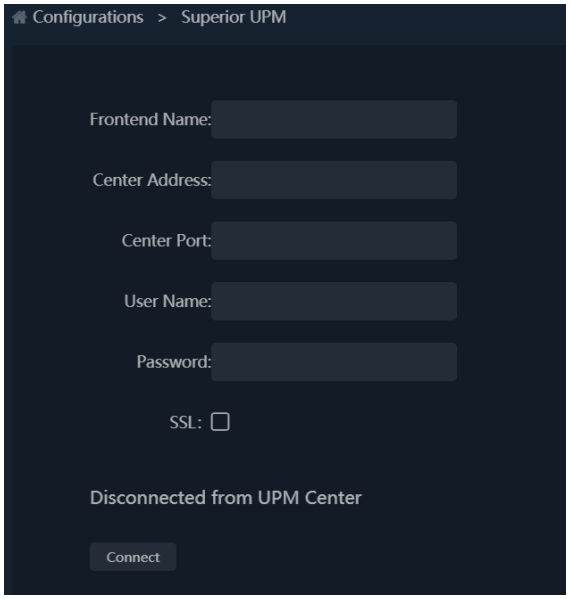
The calculation function supports difference, percentage, and division.

The calculation field can select normal metrics or calculation metrics.

4.9. Superior UPM Configuration

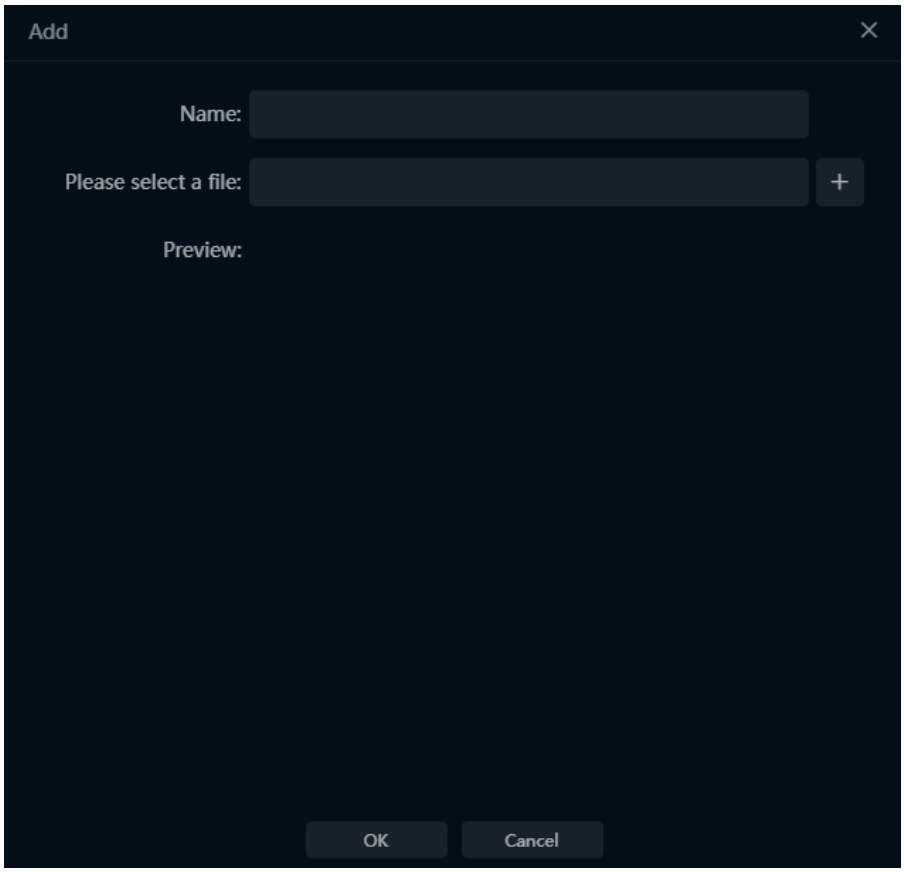
The distributed architecture of UPM adopts multi-stage deployment, hierarchical management and distributed data collection. It monitors and analyzes the nChronos data collected by UPM centers in various physical networks. The superior UPM center has the data authority of the probe and link of the subordinate UPM center. The subordinate UPM cannot access the superior UPM center data. Each subordinate UPM is relatively independent.

To configure a Superior UPM, Click the menu Configuration -> Superior UPM to open Superior UPM Configuration page, as the screenshot below:



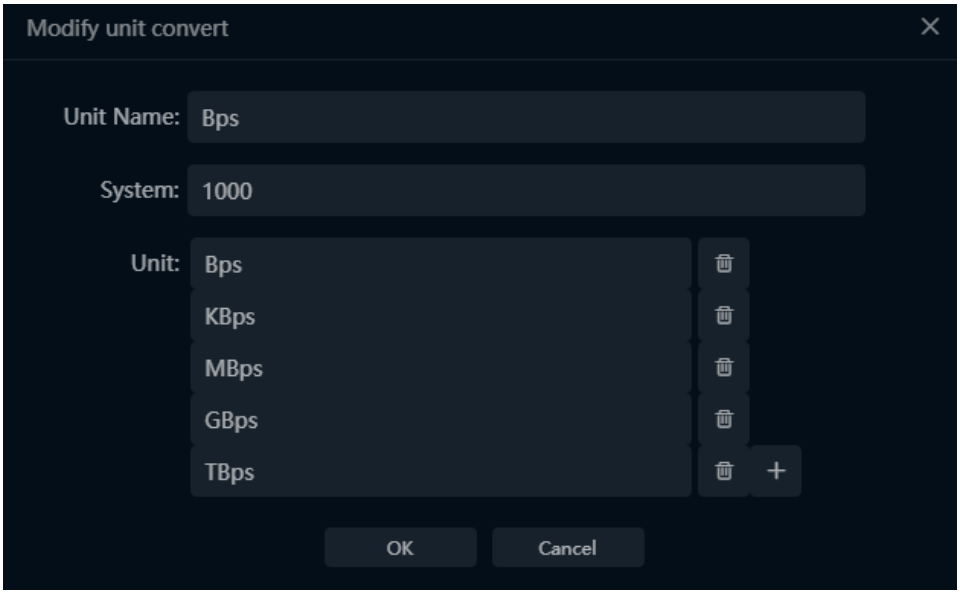
4.10. Map Configuration

Map configuration is the unified management of maps supported by the map component in the monitor views. By default, maps of Chinese provinces are built into the system.



4.11. Unit Conversion Configuration

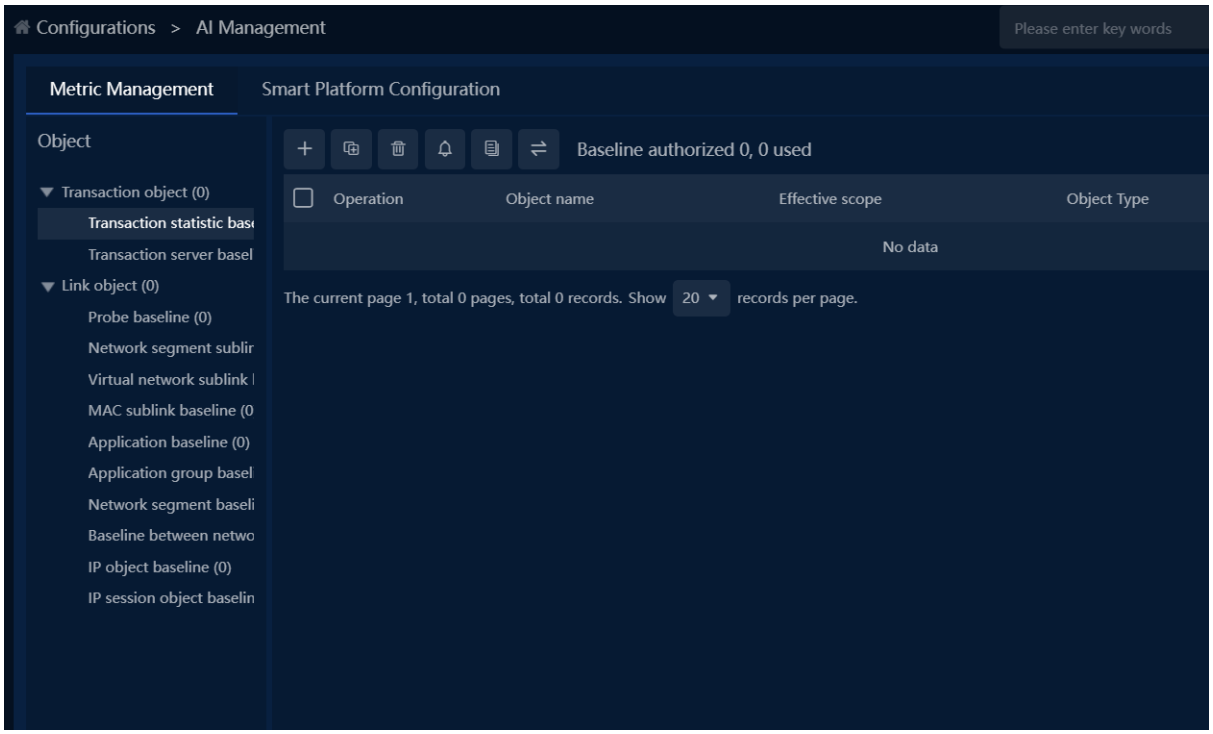
Unit conversion configuration is the unified management of the unit information needed for business field, transaction metric configuration and OID configuration.



4.12. Configure AI management of intelligent baselines

AI management calculate key indicators that users are concerned about and can trigger corresponding intelligent baseline alerts. The system supports intelligent monitoring of link indicators, business indicators, application indicators, VoIP indicators, network performance indicators, transaction performance indicators, and business transaction indicators.

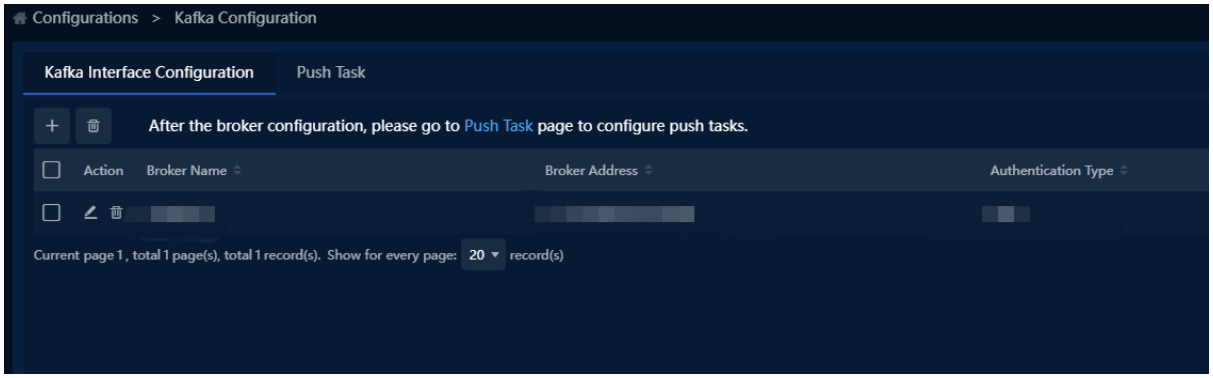
The indicator management interface of intelligent baselines is shown in the following figure:



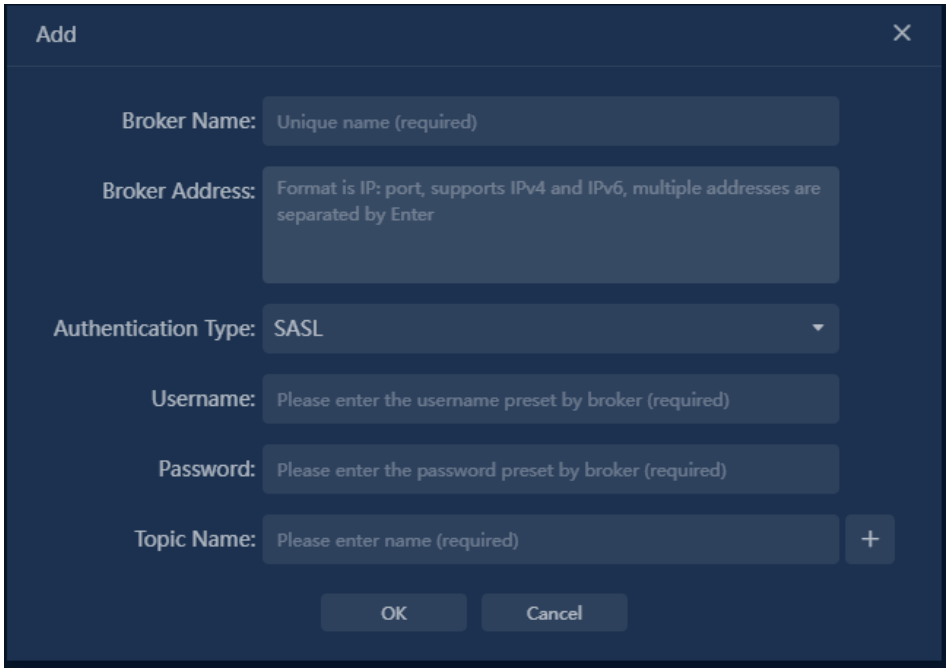
4.13. Kafka interface and task

4.13.1. Kafka interface setting

Select Kafka Configuration from the configuration menu and click Kafka Interface Configuration to enter the Kafka interface.



Click +, The Add Interface configuration dialog box is displayed



The following table describes the configuration fields in the dialog box.

Name	Instruction
Broker Name	This parameter is mandatory. It is used to set the Broker name. The Broker name must be unique
Broker Address	This parameter is mandatory. It is used to set the address of the Broker. The format is IP: port. This supports IPv4 and IPv6, Multiple addresses are separated by Enter.
Authentication Type	This parameter is mandatory. It is used to configure the Kafka authentication mode. SASL and no authentication can be selected.
Username	When SASL authentication is selected, configure the

Name	Instruction
	Kafka authentication account.
Password	When SASL authentication is selected, configure the Kafka authentication password.
Topic Name	This parameter is mandatory. This parameter is used to set the name of the interface Topic. Multiple Topic names can be created at the same time.

Note：Kafka version must be later than 1.0.0 to avoid problems caused by version negotiation errors

Click OK to complete the configuration of the Kafka interface

4.13.2. Task Push Configuration

Select Kafka configuration from the configuration menu and click Push Task to enter the push task configuration screen.

Click the add push task pop-up box is displayed.

The following table describes the configuration fields in the dialog box.

Name	Instruction
Task Name	Mandatory. The task name must be unique.
Broker Name	Mandatory, select the Broker configured in the Kafka interface configuration.
Topic Name	Mandatory. Topic name can selects a Topic that is pre-configured in the Broker.
Link	Mandatory. Configure the link for pushing tasks to obtain data. Can choose more than one.
Data Table	Mandatory. Select the data table type to be pushed. You can select the data table contained in the selected link.
Filter Condition	Optional: Sets the filter criteria for pushing data. You can configure the logical configuration of and, or.
Query Field	Mandatory. Configure the data fields to be pushed. The optional fields are included in the selected data table.
Sort Field	This parameter is mandatory. You can select the fields in the query fields to sort pushed data. Single choise.
Key-value field	Mandatory. You can set the statistical range of data to be pushed.
Sort Type	Mandatory. You can set the sorting mode for pushing data. The sorting mode can be none, ascending, or descending.
Sort TOP	Mandatory. The default value is 2000.
Execute Frequency	Mandatory. Set the execution frequency of the push task. The value can be 1 second, 10 seconds, 1 minute, 10 minutes, 1 hour, or 1 day.
Automatic Data Formatting	Mandatory. Whether to automatically format data. The value can be Yes or no.
Data display Format	This parameter is mandatory. You can select value, alias, or value + alias.
Data Output Format	This parameter is mandatory. The format of the output data can be binary or JSON.

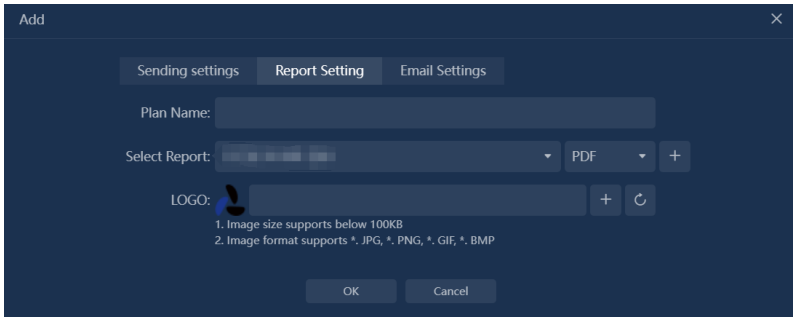
- Notice: Configure the Kafka interface before creating a push task.

Click "OK" to complete the configuration of push task.

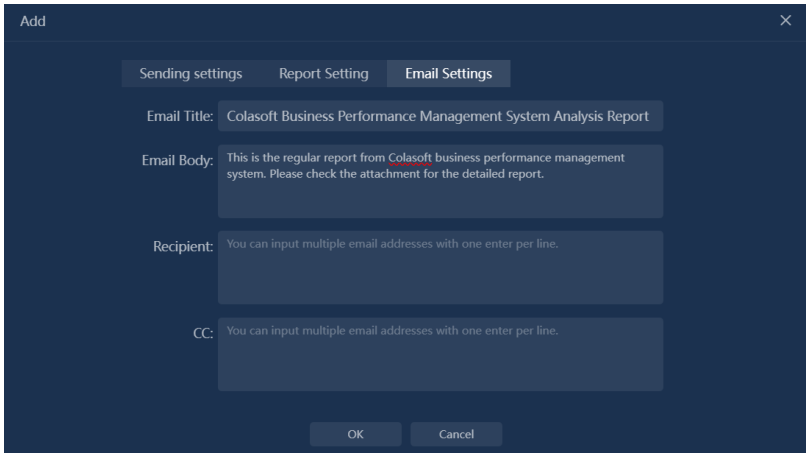
4.13.3. Report sending task

1. Report Sending Configuration to enter the configuration page
2. Click +, a sending configuration popup will appear

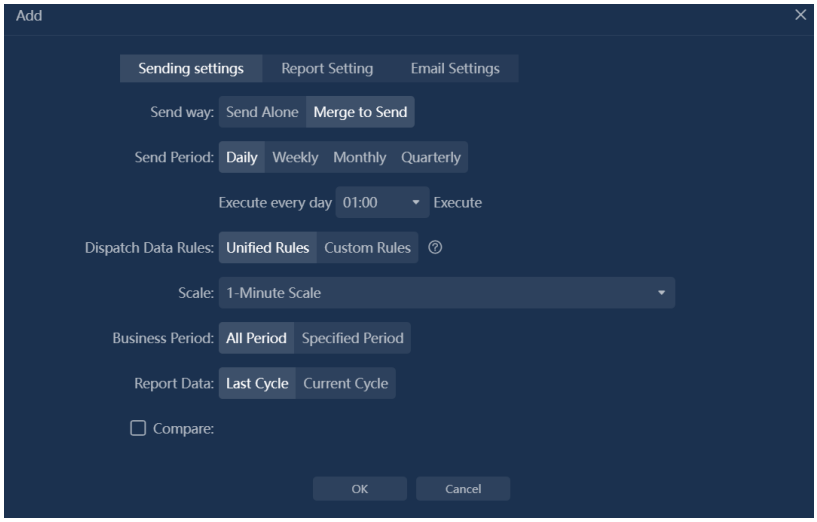
（1） Report Seting: Configure the name, LOGO, included reports and their corresponding formats for this sending plan.



（2） Email Sending: Configure the subject, body, recipients, and CC recipients for this sending.



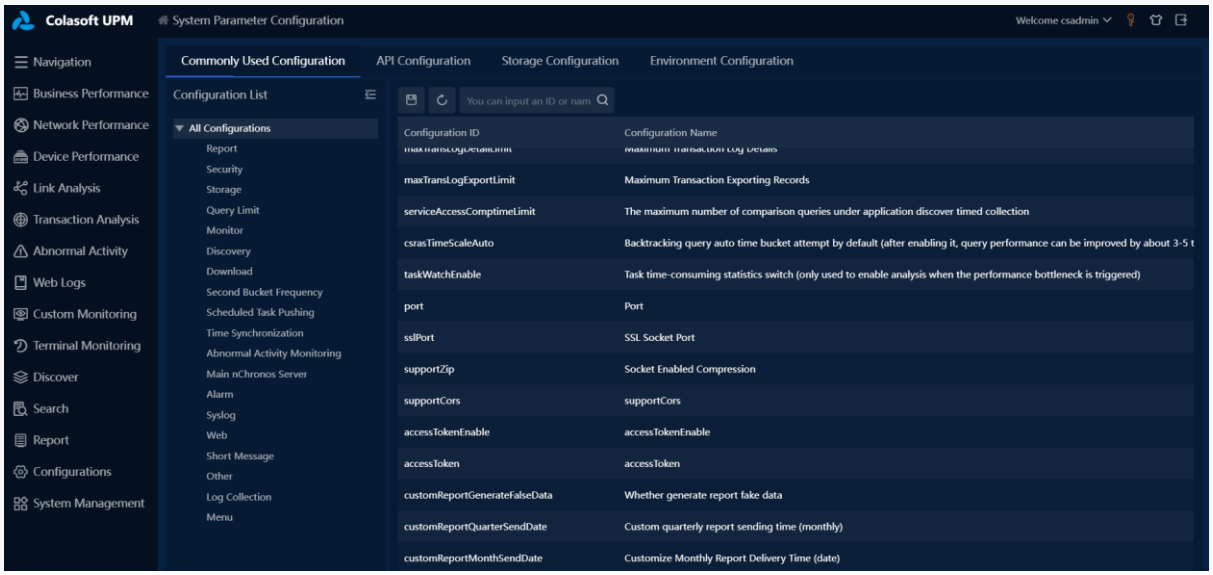
（3） Sending Settings: Configure the sending method, frequency, and relevant content of report data for this scheduled sending task.



3. Click OK to complete the report sending task.

4.14. System Parameters configuration

Administrator in your browser URL bar type https://upmip/system/parameter.html or https://upmip /sysp access UPM parameters configuration page.



Commonly used setting

The common configuration page is used to configure variables for code execution. For example, maxLimit indicates the maximum value of a data query, the default value is 22000. If your environment needs to increase the maximum number of queries, modify the corresponding parameters and save.

Third-party Interface Configuration

The third-party interface configuration page is used to configure third-party interface system parameters, such as the IP address and version.

Storage configuration

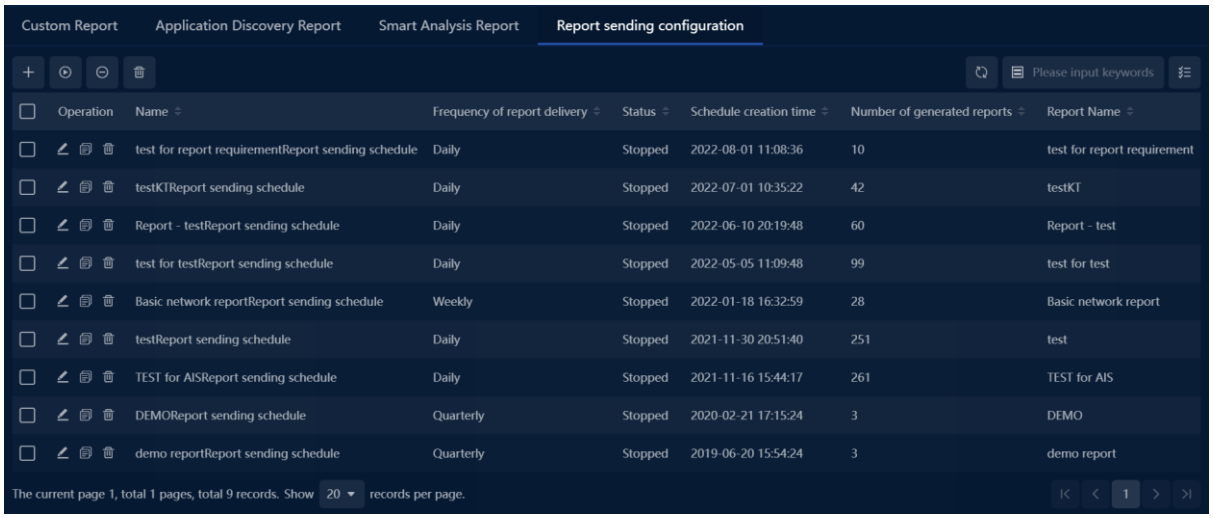
On the storage configuration page, you can monitor UPM data and check the usage of MongoDB and ElasticSearch in real time

Environment configuration

The environment configuration page is used to configure some parameters for system startup, such as MongoDB connection address and password, which can be modified on this page. If the modification is incorrect, the system fails to start, you can delete the Linux /data/upm/custom properties files, let the MongoDB password to the initial state, then can be successfully started.

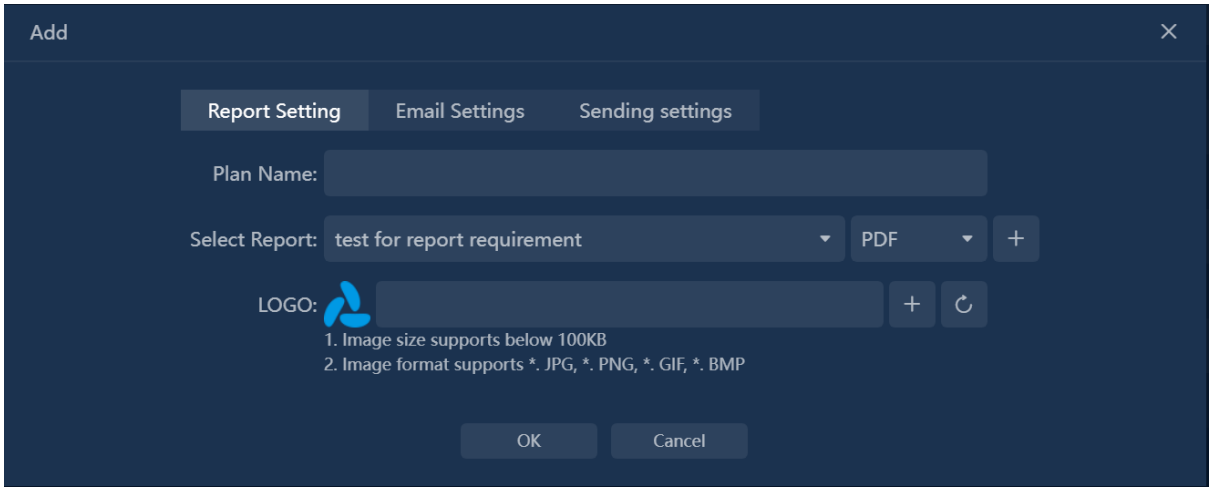
4.15. Configure report sending tasks

1. Click Report - > Report Sending Configuration to enter the sending configuration page, as shown in the following figure

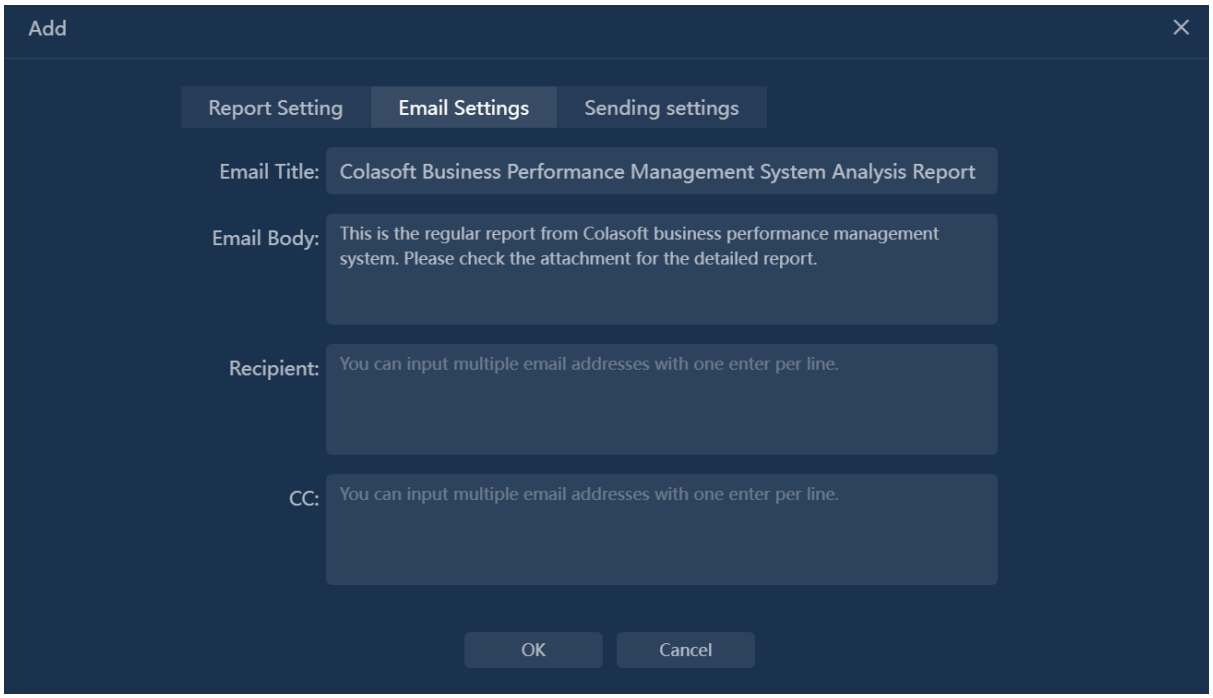


2. Click to pop up the send configuration pop-up window

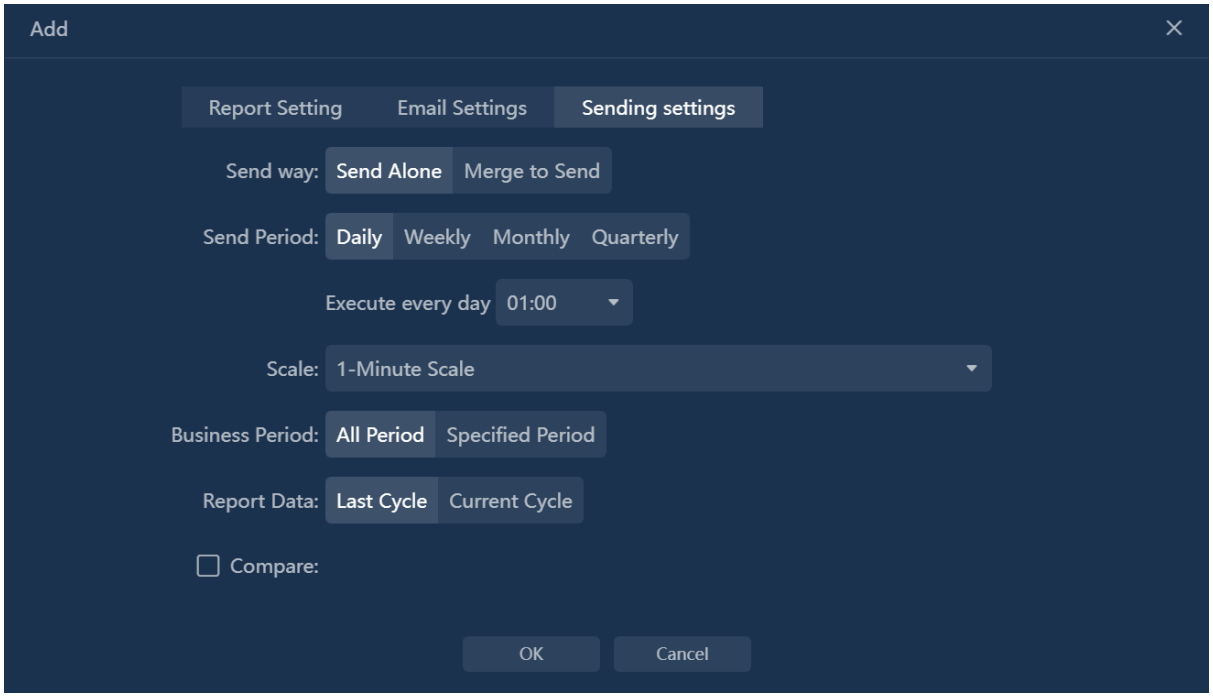
（1） Report configuration: configure the name, logo , included reports and corresponding formats of this sending plan.



（2） Email configuration: configure the subject, body, recipient and cc of this sending.



（3） Sending configuration: Configure the sending method, frequency and report data content of this scheduled sending task.



3. Click OK to complete the report sending task.

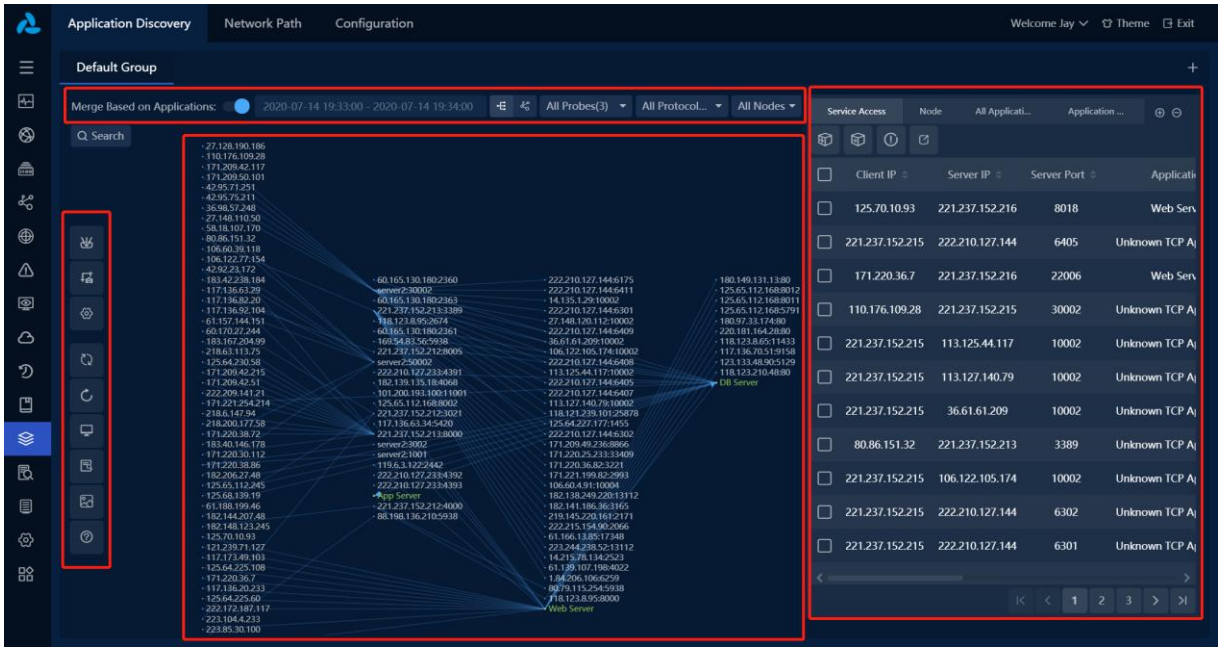
5. Discover

5.1. Application Discovery

Application discovery means to discover the access relationship between applications according to the service access data collected by the probe(s). Users can create applications, create business and make fast comparisons based on the results of application discovery.

5.1.1. Interface Introduction

The application discovery interface includes the top filter bar, the left toolbar, the discovery diagram and the list area, as shown in the figure below:



Top Filter Bar

The top filter bar is used to filter and display the contents shown in the discovery diagram. The filtering modes include:

- Merge based on applications: This mode is used to set the diagram of the node according to the application. If it is open, all the same application server nodes will be merged into one point.
- Filtering based on probes: This mode is used to filter the data of diagram according to probes. Only the selected nodes will be displayed in the diagram.
- Filtering based on protocols: This mode is used to filter the data of diagram according to protocols. Only the selected nodes will be displayed in the diagram.
- Filtering based on node types: The node types include TCP, UDP and all. Only the selected nodes will be displayed in the diagram.
- Filtering based on search: This mode is used to filter data according to the input search condition.

Left Toolbar

The left toolbar is used to manage the data acquisition task and set the display settings of the discovery diagram. The options in the toolbar include:

- Data Collection: This option is to create the data acquisition task. All data in the diagram

come from the data acquisition task.

- Data Snapshot: This option is used to manage data acquisition task. Snapshot data can be compared to generate into reports.
- Display Configuration: This option is to set the diagram display content.
- Refresh: This option is to refresh data in a diagram.
- Reset: This option is to reset the position of each node in the diagram.
- Hide Clients: This option is to hide all the clients in the diagram.
- View Hidden Nodes: This option is to view the hidden node(s). Users can hide node(s) by right-click the node(s) in the diagram.
- Add Background Image: This option is used to add background image to diagram.
- Help: This option is to view the marginal data of the diagram.

Discovery Diagram

Discovery diagram is the result display of data acquisition task and provides two display styles: carding diagram and mechanical diagram. The options in the discovery diagram include:

- Modifying the name of the node(s)
- Checking node(s) information
- Checking the connection between the two nodes
- Displaying or not displaying node(s) connected to the selected one
- Hiding or not hiding node(s) connected to the selected node
- Adding the selected server node(s) to be a new application
- Adding the selected server node(s) into an existing application
- Modifying the application configuration information
- Adding the selected node(s) to be a new business
- Displaying all the other nodes connecting to the selected one

List Area

The options in list area include:

- Service Access: It shows the service access relationship that was collected. Users can add applications, add to applications, add exception access rules, and export.

- Node: It shows all server nodes were collected. Users can add applications, add to the application, view client(s) and delete node(s).
- All Applications: It shows all the customized application(s) in the system. Application(s) can be added to group, modified, copied or deleted, and also be added to business.
- Application Access: It shows all applications imported through a third party platform or synchronized to the system. Users need to manually define the applications synchronized into the system as customized applications.

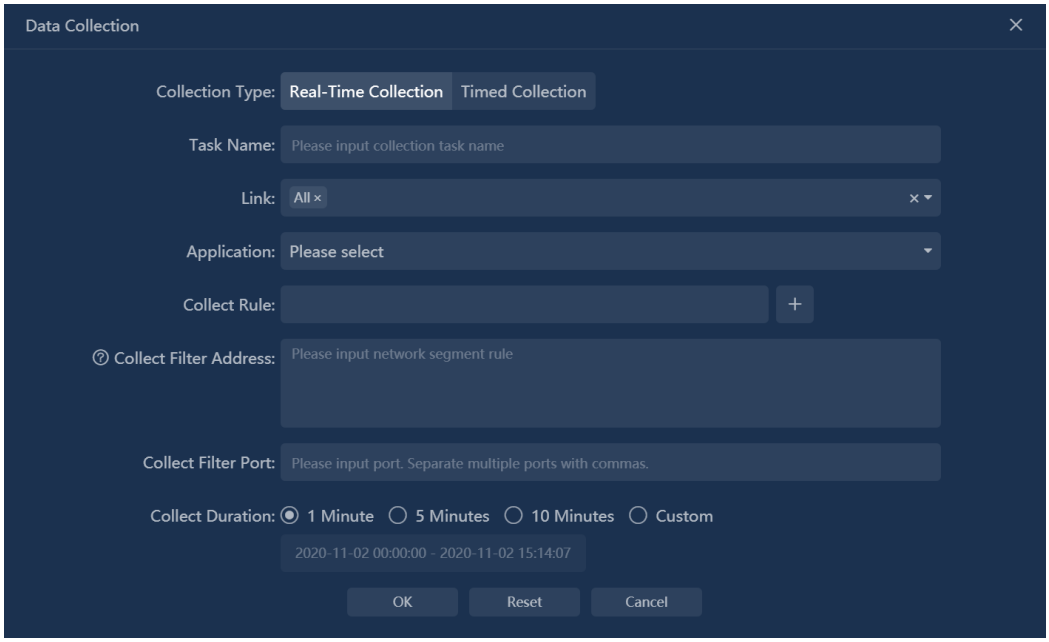
5.1.2. Data Collection

Data collection is the basis of application discovery. UPM conducts application relationship carding according to collected service access data.

Data collection includes two modes: real-time collection and timed collection.

Real-time Collection

Click the button of "Data Collection", a data collection box pops up, and select the “Real-time Collection”, as shown in the figure below:



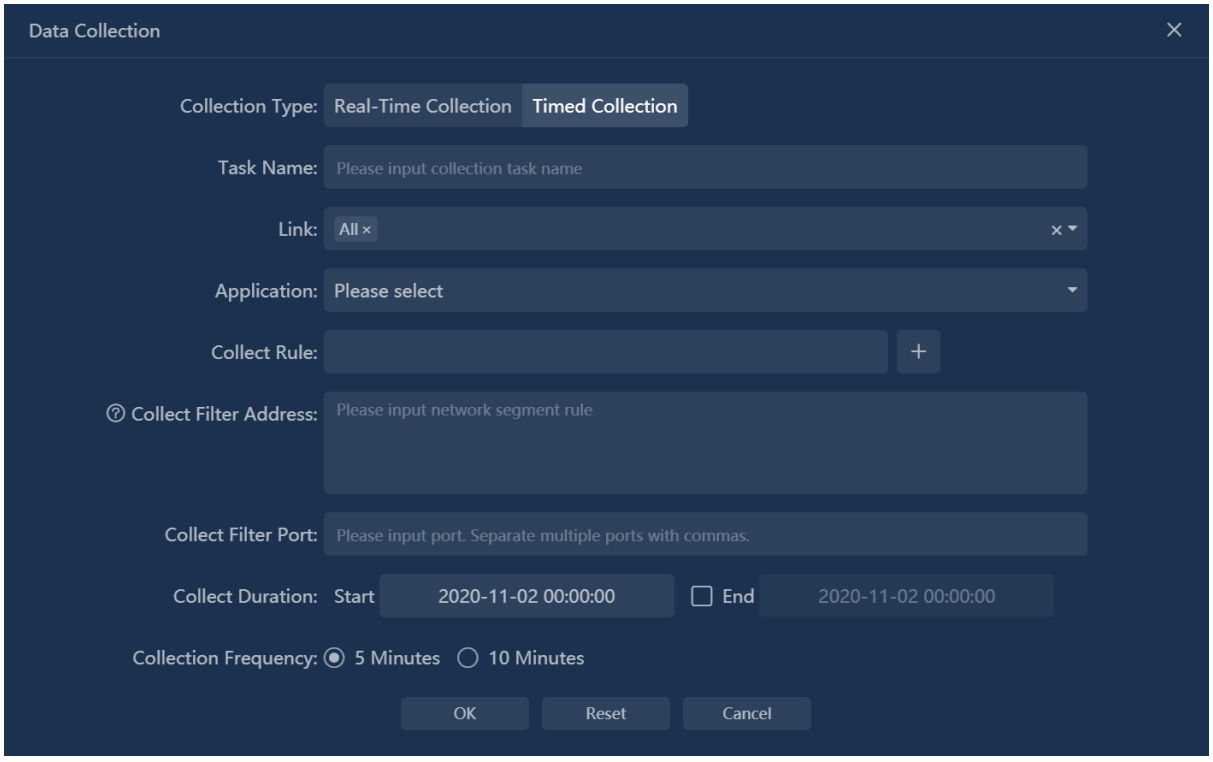
Description of setting items in the “Data Collection” box is shown in the following table:

Setting Items	Description
Task Name	It is used to set the name of the collection task. When there are multiple collection tasks, it is recommended to set the name for each collection task to facilitate the distinction and search.
Link	It is used to set the data source for collection, that is, which link data needs to be collected, supporting multiple selection.
Application	It is used to collect data only for the specified application(s), supporting multiple selection. If no application is specified, data from all applications will be collected.

Collect Rule	It is used to set collection rules. One rule is composed of server IP address and port. It supports setting multiple acquisition rules. If a rule is set, only data that conforms to the collection rule will be collected.
Collect Filter Address	It is used to set the IP address that needs to be filtered out when collecting data.
Collect Filter Port	It is used to set the server port(s) that needs to be filtered out when collecting data.
Collect Duration	The system provides 1-minute, 5-minute, and 10-minute time ranges for setting up data collection. It also supports customized time ranges. The default time ranges is 1-minute.

Timed Collection

Click the button of "Data Collection", a data acquisition box pops up, and select the “Timed Collection”, as shown in the figure below:



The difference between Timed Collection and Real-time Collection is that the ending time of Timed

Collection can be set to a future time. If the ending time is not set, the collection task will continue until the task is finished manually. The collection frequency includes 5 minutes and 10 minutes, and the default collection frequency is 5 minutes.

Operation Suggestions

Since data collection will have a certain impact on system performance, the following operation Suggestions are made when data collection is carried out:

- The data collection duration should not be too long.
- Too much Timed Collection tasks are not recommended.
- By setting the collection filter conditions, users can reduce the amount of data collected and shorten the time of data collection.

5.1.3. Create Applications

There are many ways to create server nodes as applications.

Method 1: Select the server node in the application carding diagram, right-click, and select Add Application or Add to Application in the popup right-click menu.

- Add Application: Selecting a server node and add it as a new application. Users need to select classification, application type, and then set the basic information of the application.
- Add to Application: Selecting a server node as an application rule and add it to an existing application. Users only need to select an application in the drop-down list.

Method 2: In the "Service Access" list on the right, select one or more service access records, and click "Add Application"  or "Add to Application"  icon at the top of the table to complete the creation of the application.

Method 3: In the "Node" list on the right, select one or more node(s) information and click "Add Application"  or "Add to Application"  icon at the top of the table to complete the creation of the application.

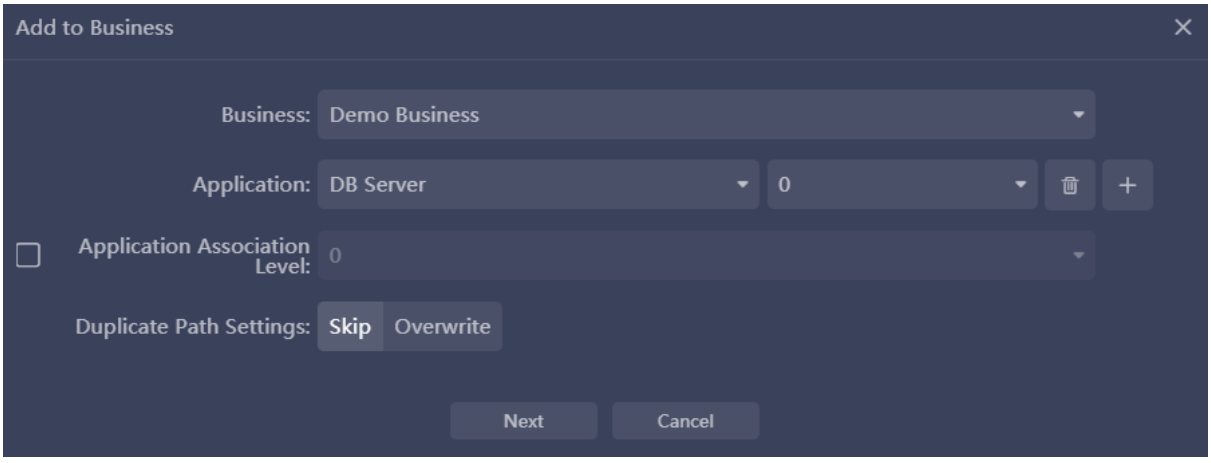
Method 4: In the "View Node Information" pop-up box, select “Access Server” or “Access Port”, and click “Add Application”  or “Add to Application”  icon at the top of the table to complete the creation of the application.

5.1.4. Create Business

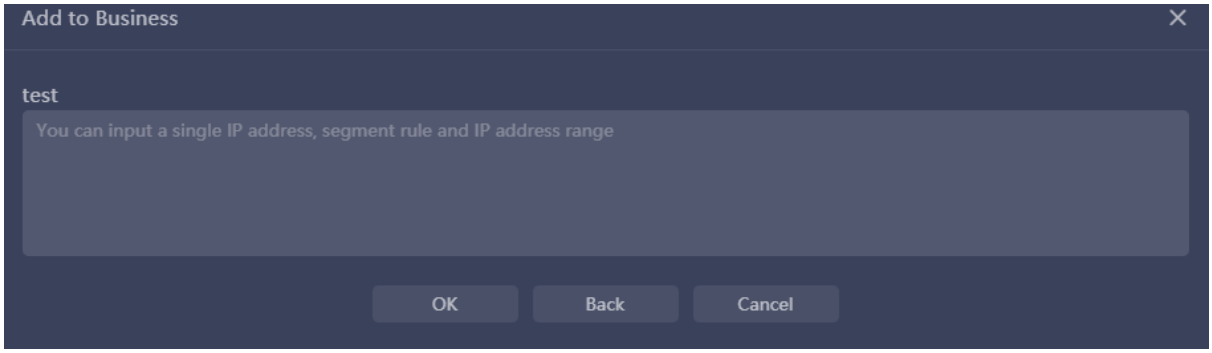
In the application carding diagram, one or more of the selected applications can be quickly created as businesses for applications that have been discovered.

Method 1: Create business through application relationship diagram

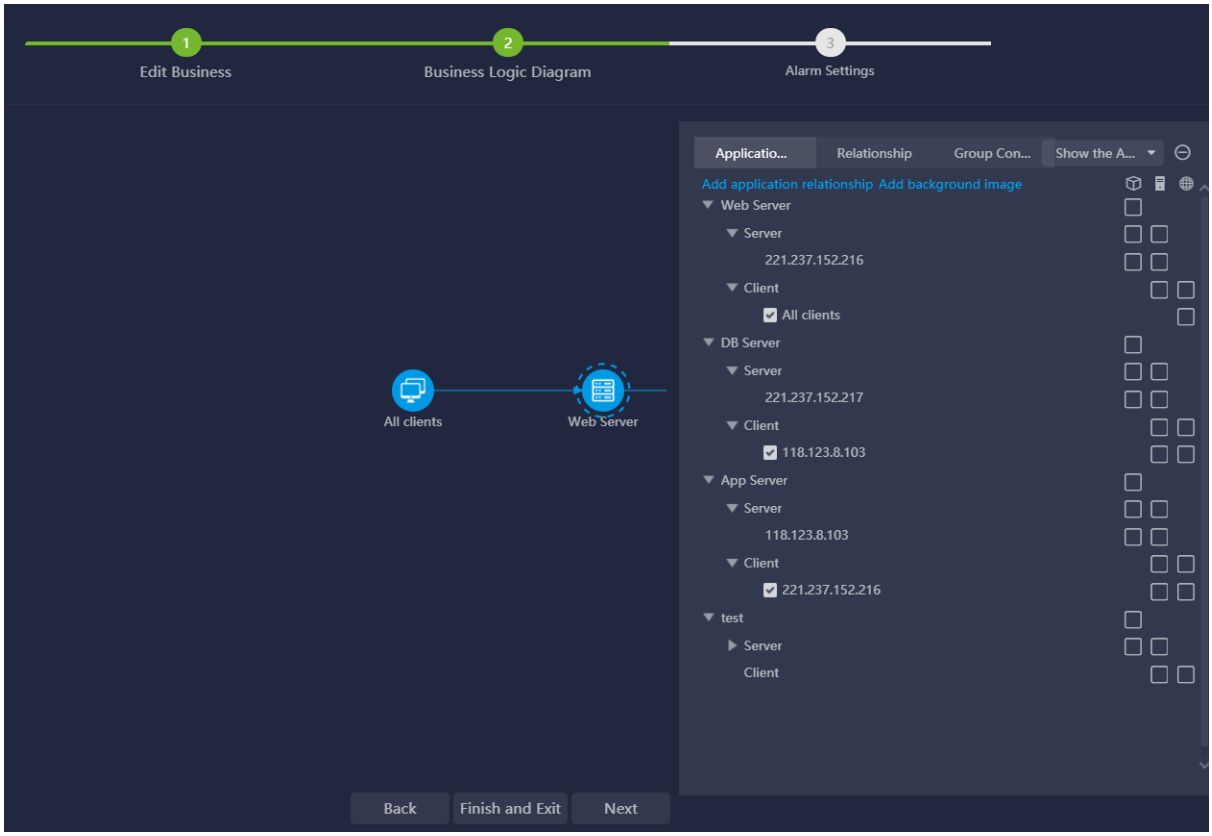
- Step1: In the "All Applications " list on the right, select one or more applications and click the  button at the top of the table to complete the creation of the business.



- Step 3: Click the "Next" button to set the client, as shown in the figure below:



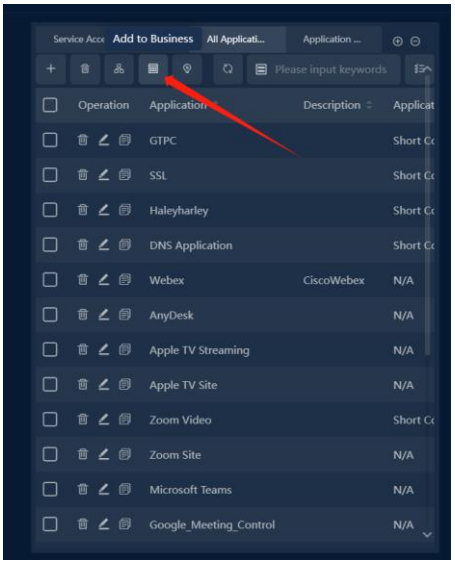
- Step 4: Click the "OK" button to jump to Business Logic Diagram page, as shown in the figure below:



In the business logic diagram, the system will conduct the connection between nodes according to the service access relationship in the application discovery. For nodes that can find access relationship, automatic connection will be made. The probe on the connection is the probe that collects access relationship of this service. If the corresponding access relationship cannot be found, the user needs to connect manually, and when connected, the user needs to manually specify the probe on the path.

Method 2: Create through the entrance above the 'All Applications' list

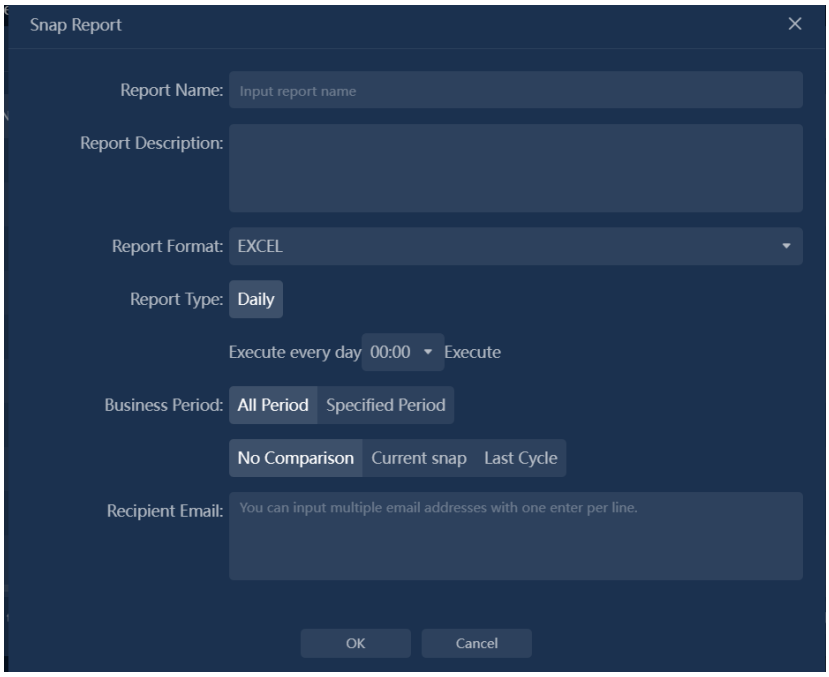
In the right 'All' list, select one or more applications, click the 'Add to Business' icon above the table to complete the business creation.



5.1.5. Snapshot Comparison

The data snapshot function is mainly used to compare the difference of data collected by different data collection tasks.

In the data snapshot list, select the snapshot comparison icon in the collection task operation column to compare the collection results of the selected collection task with the snapshot showing the collection task in the current view. The comparison results of snapshots are shown in the figure below:



In the snapshot comparison information, all nodes increased and reduced are displayed by tab. Click the export button in the upper right corner of the "Comparison Information" pop-up box to export the comparison information to a FILE in CSV format.

In the comparison diagram, the red text represents the increased IP nodes during the comparison, and the light color text represents the decreased IP nodes during the comparison.

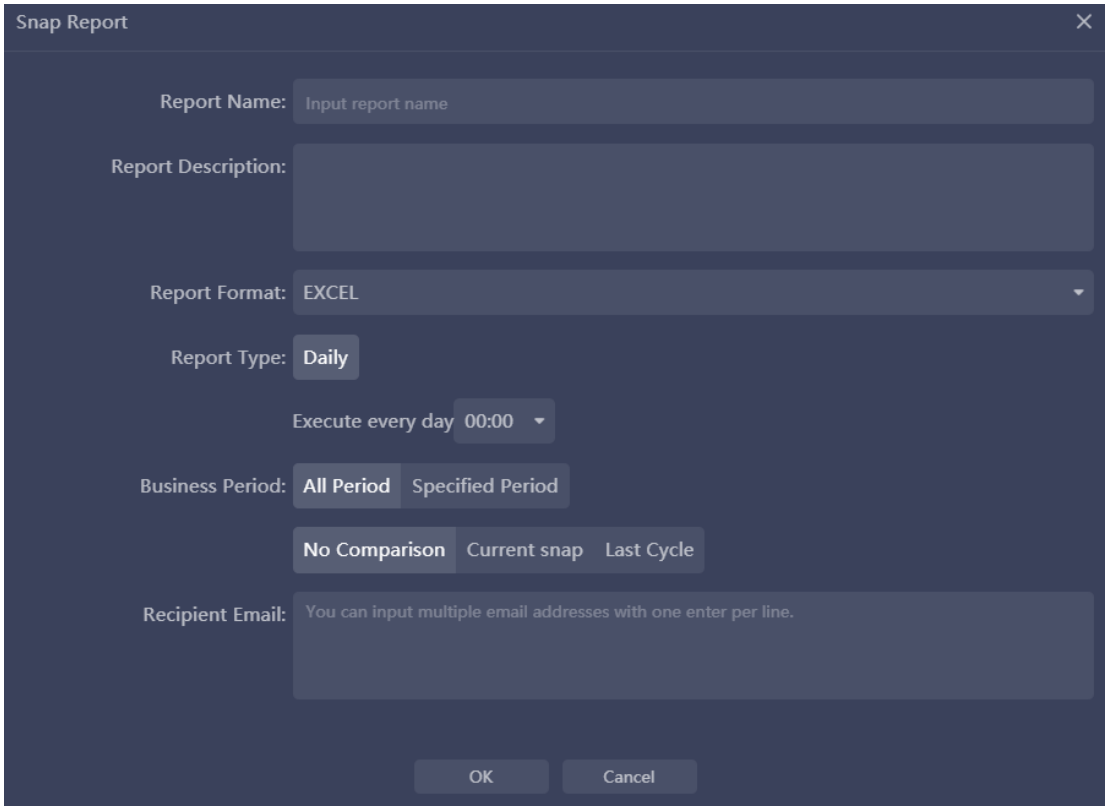
Click the "Close Comparison" button in the top bar to exit snapshot comparison mode.

Settings	Description
Report name	Used to set the name of the snapshot report.
Report Description	Used to set the description information for snapshot reports, optional configuration item.
Report Format	Used to set the format of the report, currently supports Excel format.
Report Type	Used to set the type of the report, currently supports daily report. The system supports setting the generation time of the report, default execution at 0:00 every day.
Business Period	Used to set the time range for data collection in the report, the system defaults to collecting data for the whole day. Used to set whether the report is compared, the system provides 3 options: ● No Comparison: The report only includes the data collection results for the current day, and the system defaults to no comparison. ● Current Snapshot: The report will use the currently displayed snapshot in the system as the base report, and each generated report will be compared with the currently displayed snapshot. ● Last cycle: The report will compare the report of the day with the snapshot generated in the previous report cycle.
Recipient Email	Used to set the email address to receive the report. Please separate multiple addresses with line breaks.

5.1.6. Generate snapshot report

The snapshot report function mainly generates reports according to the specified period of data collected by the collection task and sends them to the specified mailbox.

In the data snapshot list, select the snapshot report  icon in the collection task operation column to generate a report of the collection results of the selected collection task. Generate snapshot report pop-up box as shown in the figure below:



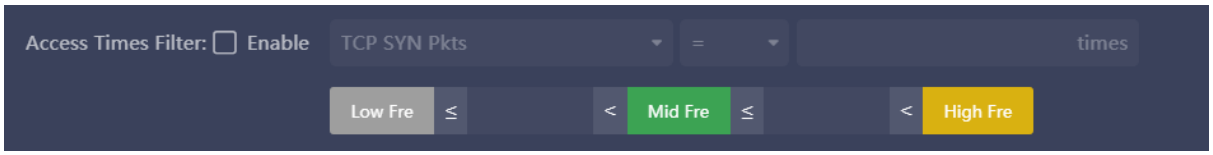
The description of each setting item in the generate snapshot report pop-up box is shown in the following table:

Setting Items	Description
Report Name	It is used to set the name of the snapshot report.
Report Description	It is used to set the snapshot report as an optional configuration item.
Report Format	Excel format is currently supported.
Report Type	It is used to set the type of report. Daily report is currently supported. The system supports setting the generating time of the report. By default, the report will be executed at 0 o 'clock every day.
Business Period	It is used to set the time range of data collection in the report. The default of the system is to collect the data of the whole day.
Recipient Email	It is used to set the mailbox address to receive the report. Please use separators between email addresses.

5.1.7. Custom Metric Discover

In the application of carding, the system supports filtering access relations according to user-defined indicators, and displays them in different colors in the carding diagram according to the access frequency of indicators.

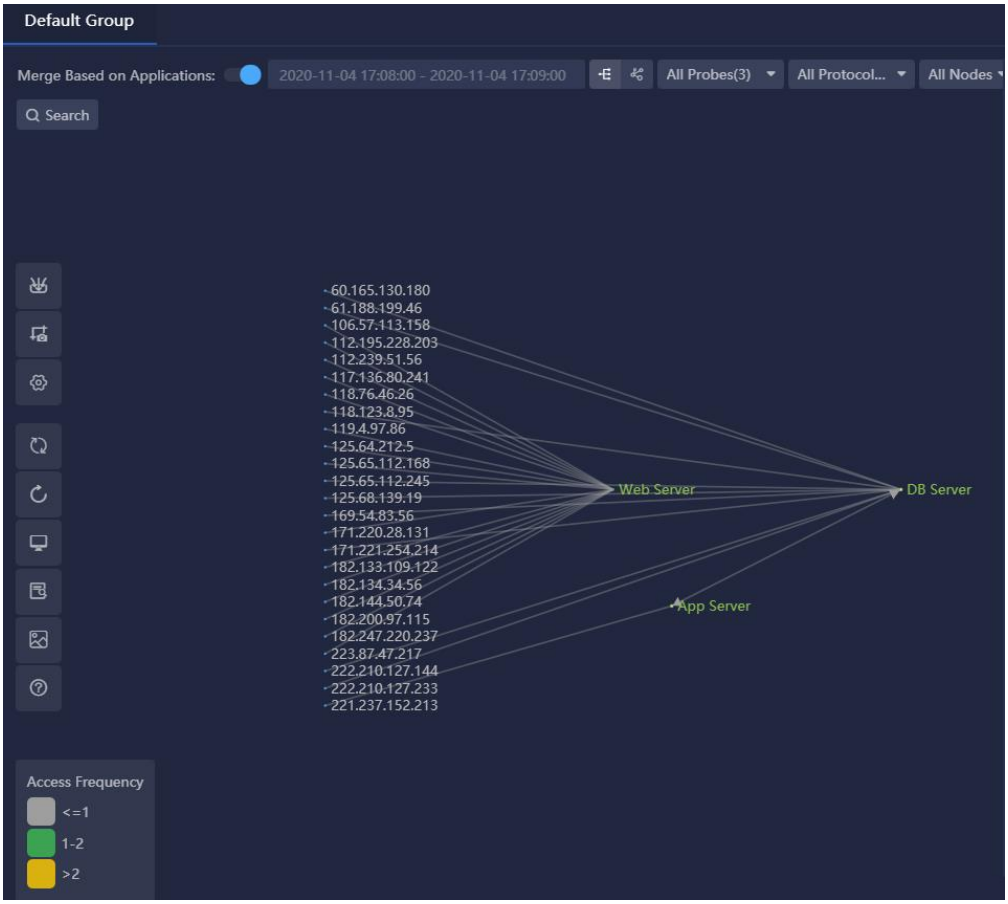
Enable access times filtering in the Display Configuration pop-up box, and set thresholds for filtering conditions and access frequency, as shown in the figure below.



The metrics supported by access count filtering include TCP synchronization packets, total number of connection requests, three handshakes, and connection failures. For example, setting TCP synchronization packet > 1 means that among the collected service access records, only the records of TCP synchronization packet > 1 will be displayed in the carding diagram.

The system supports setting the color of low frequency access, medium frequency access and high frequency access. In the carding diagram, the line between nodes will be displayed according to the color of set frequency.

After the display setting is completed, the filter condition and frequency color set by the user will be displayed in the carding diagram, as shown in the figure below:



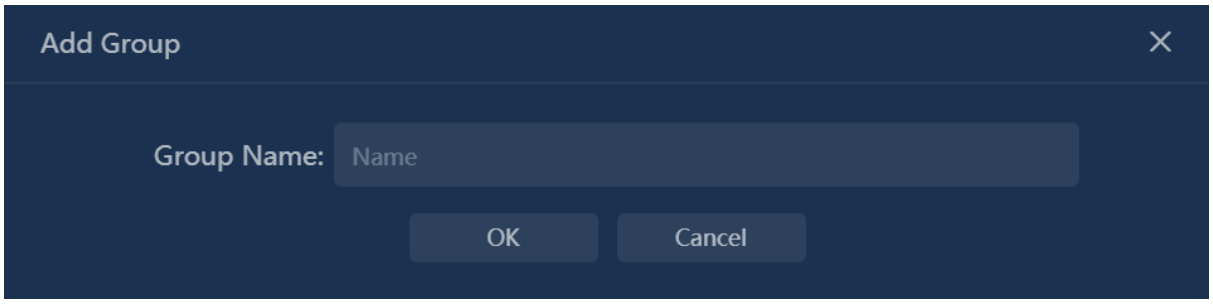
5.1.8. Other Common Operations

Add Group

UPM provides view grouping function, and users can group and manage according to the type of

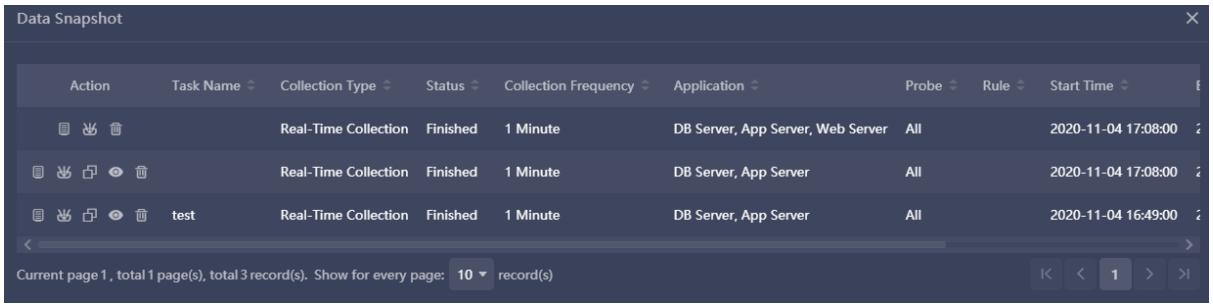
collecting task or the area of collecting data.

Click the button to the right of the view title bar, and the add Group dialog box pops up, as shown in the figure below:



Data Snapshot

The data snapshot list shows all the data acquisition tasks created within the current view group, as shown in the figure below:

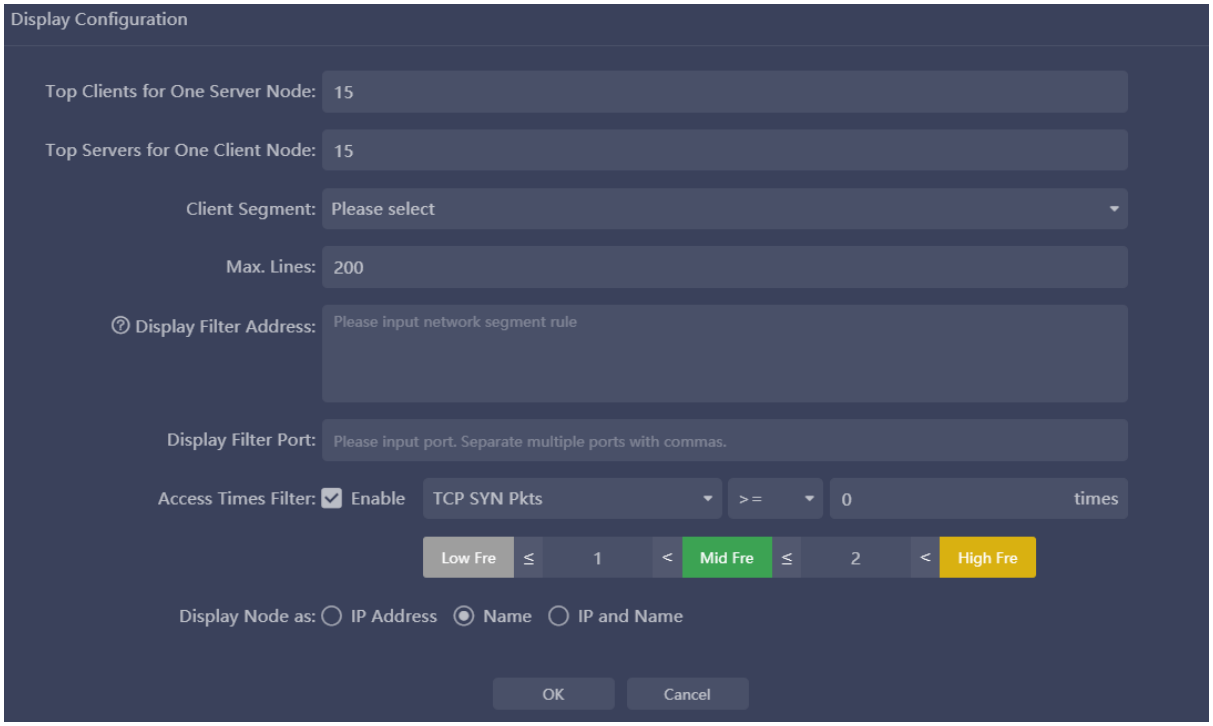


The operations provided by the operations column in the data snapshot list include:

- Snapshot report: to choose a snapshot of the generate reports on a regular basis, sent to the specified email.
- Collect again: to bring up this snapshot of the data collection configuration dialog, the user can modify the acquisition conditions, start data collection.
- Compare: compare the snapshot and shows a snapshot of the current.If the snapshot was already in the display state, the comparison icon would not appear in the action column.
- Show: set the snapshot to display status. If the snapshot is already in the display state, the display icon does not appear in the action column.
- Delete: delete selected snapshot.

Display Configuration

Display Configuration is mainly used to display the results of application discovery, as shown in the figure below:



Descriptions of each setting items are shown in the following table:

Setting Items	Description
Top Clients for One Server Node	It is used to set the maximum number of clients a server node can connect to. The number of clients is set to a range of 1-500 and the default is 15.
Top Servers for One Client Node	It is used to set the maximum number of servers a customer node can connect to. The number of clients is set to a range of 1-500 and the default is 15.
Client Segment	It is used to set the client segment that the user is concerned with, only the nodes associated with the client segment selected by the user are included in the application carding diagram.
Max. Lines	It is used to set the client network segment that users are concerned about. Only the number of node lines selected by users will be included in the carding diagram, and the range is 1-3000, and the default is 200.
Display Filter Address	It is used to set the IP address to be filtered out, the node set in the filter address will not be shown in the carding diagram.
Display Filter Port	It is used to set the server ports that need to be filtered out, the nodes associated with the filtered ports are not shown in the application carding diagram.
Access Times Filter	By setting the access times, the collected service access relationships can be filtered, and only the access relationships that meet the filtering conditions can be displayed.Metrics that

	support filtering include TCP synchronization packets, total number of connection requests, number of three handshakes, and number of connection failures.According to the number of visits, it can be divided into low frequency access, intermediate frequency access and high frequency access. Users can customize the threshold and color.The colors of the lines in the application carding diagram are displayed according to the user-defined colors.
Display Node as	It is used to set the name that the node displays, which can be an IP address, alias, IP address, and alias. The system defaults to alias.

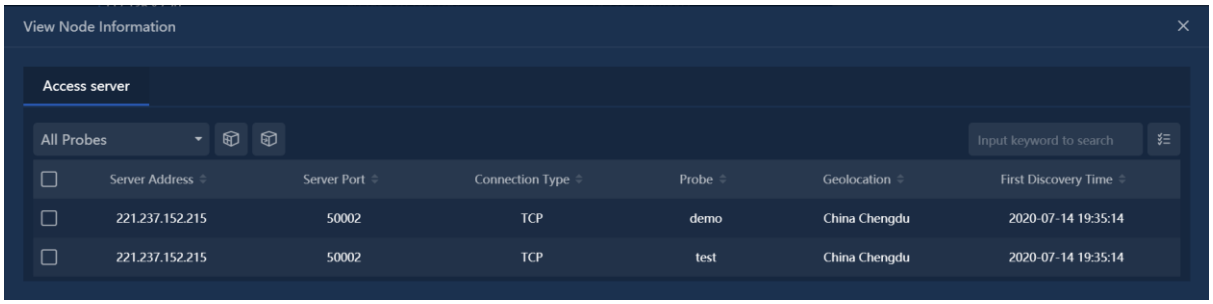
View Node Information

After selecting the node in the carding diagram, right-click and select "View Node Information" from the right-click menu to pop up the "View Node Information" pop-up box.

The application discover diagram includes multiple types of nodes, each with different node information.

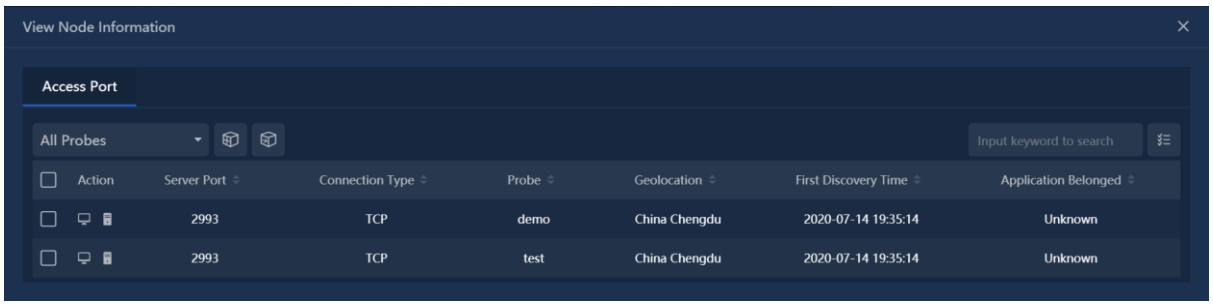
Client Type Node

Node information shows all server information accessed by the client. Users can select one or more server information as application rules to quickly add to the application, as shown in the figure below:



Server Type Node

All access port information provided by the server is shown in the node information, as shown in the figure below:



For each server port record, you can select the client and select the same port host operation.

- Choose client: playing box display visited the client IP address of the server port.

- Choose same port host: playing box display provides the same server port server IP address.

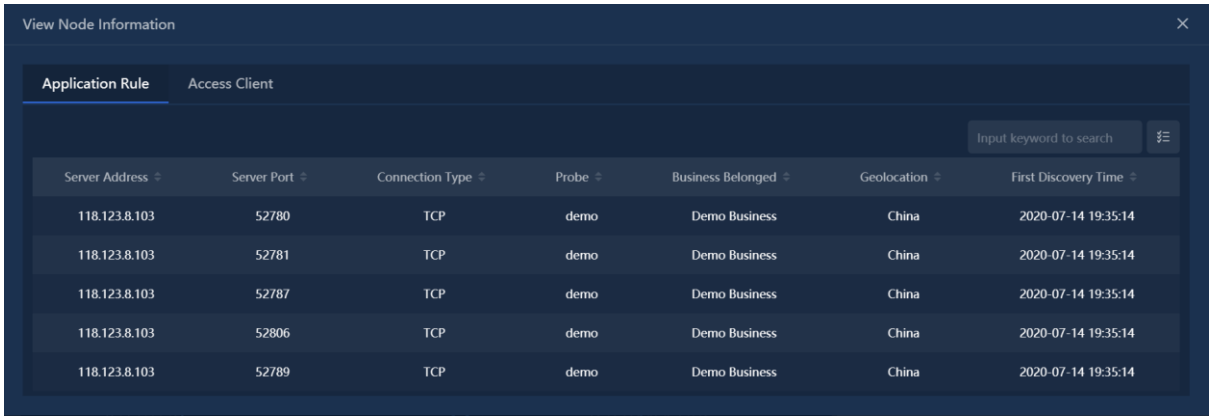
Users can add selected clients and servers to the application as application rules.

Client and Server Type Node

The node information shows all access port information provided by the node as a server and which servers are accessed as clients, as shown in the figure below:

Application Type Node

The node information shows the application rules and access client information actually collected by the application, as shown in the figure below:



Merge Based on Applications

The system supports merging the nodes according to the application before displaying. When the "Merge Based on Application" switch is turned on, nodes belonging to the same application are combined in the application discover diagram and presented as application nodes.

Filtering

When there are too many nodes, it can be filtered through nodes to show only the specified nodes. UPM supports probe filtering, protocol filtering, type filtering and search filtering.

- Probe filtering: the user can through the probe of the comb filter application diagram node, list box, click the probe in the pop-up drop-down list Settings need to filter the probe, the drop-down list includes only acquisition task, select the probe.
- Protocol filtering: the user can through the agreement of comb filter application diagram node, list box, click the agreement in the pop-up drop-down list Settings need to filter the agreement, the agreement from the drop-down list to service access.
- Type filtering: application of carding diagram, the type of connection between nodes may be

a TCP or UDP, the user can set the node connection types, see only the TCP or UDP type of connection. The system displays all TCP and UDP connections by default.

- Search filtering: system provides the search bar, users can search application, host or port directly, at the same time support level of the specified search.

Hide/Show Client

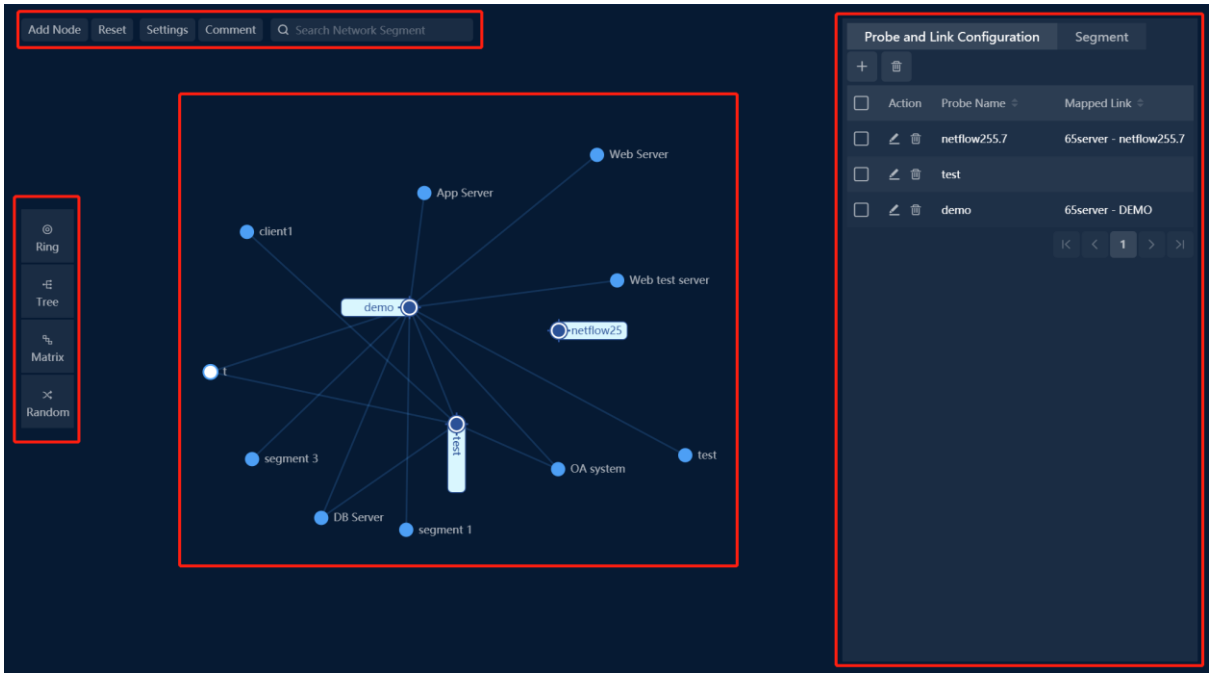
The system provides a "hide/show client" icon. By clicking the icon, users can hide and show client nodes in the application discover diagram.

5.2. Network Path Discovery

Network path discovery is centered on the probe, which combs the access relationship between the probe and the probe, and between the probe and the network node.

5.2.1. Interface Introduction

The network path discovery interface includes the top bar, the left toolbar, the discovery diagram and the list area, as shown in the figure below:



Top Bar

Features provided in the top bar include:

- Add Node: used to add network path node, in view of the network path node to add, you can set the node after the probe.
- Reset: the network path diagram to restore to the default sort.
- Settings: used to set the data acquisition task.
- Comment: displays information about the relevant illustration comb network path diagram.
- Search Network Segment: input keyword to search network path node in the diagram.

Left Toolbar

The network path discovery diagram supports four display styles; which users can switch through the left style bar. The four styles are ring, tree, rectangle and random, and the default display is ring.

Discovery Diagram

The discovery diagram shows the results of network discovery. Users select nodes in the discovery diagram and can add network paths, edit nodes and delete nodes.

List Area

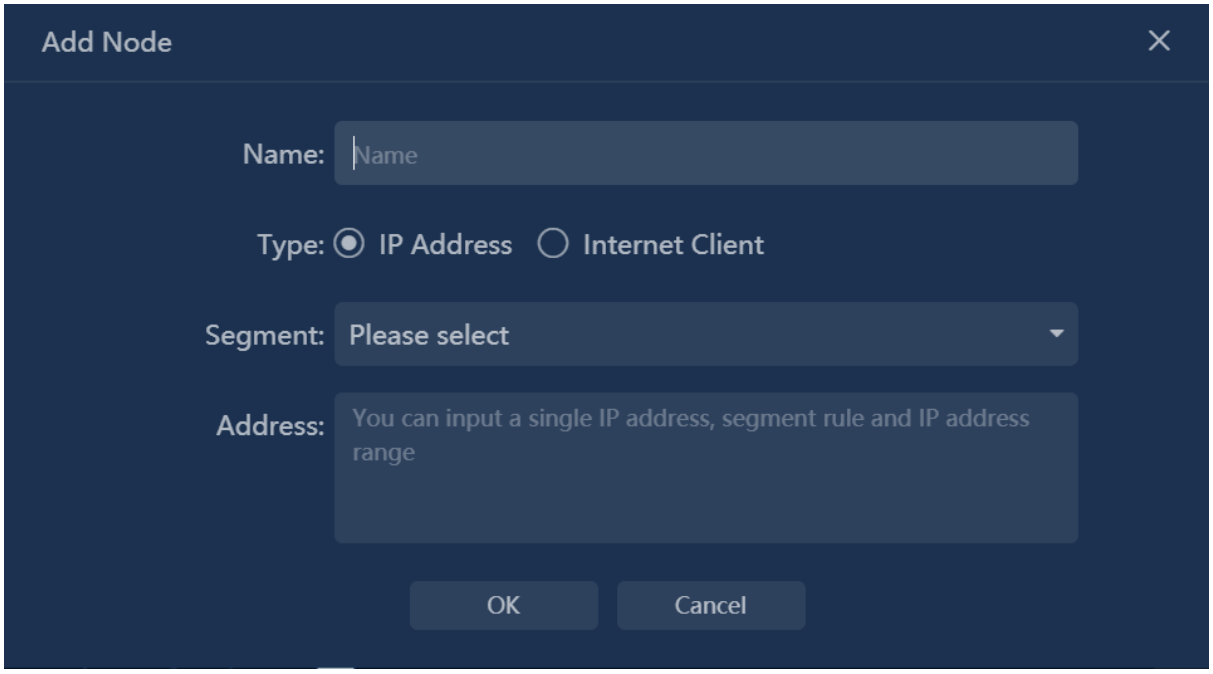
The lists in the area includes:

- Probe and Link Configuration: used for the management of the probe, including new, modify, and delete probe operation.
- Segment: used for the management of the network segment, including adding a network segment, added to the network segment, modify, delete, specify, add issued, the issuance of the import operation.

5.2.2. Other Common Operations

Add Node

Click the "Add Node" button, and the "Add Node" dialog box pops up, as shown in the figure below:

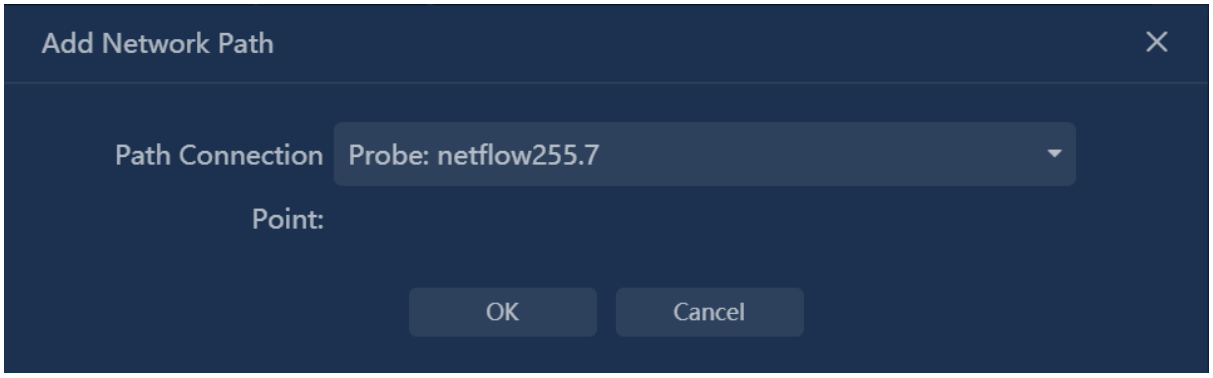


Network path nodes include two types:

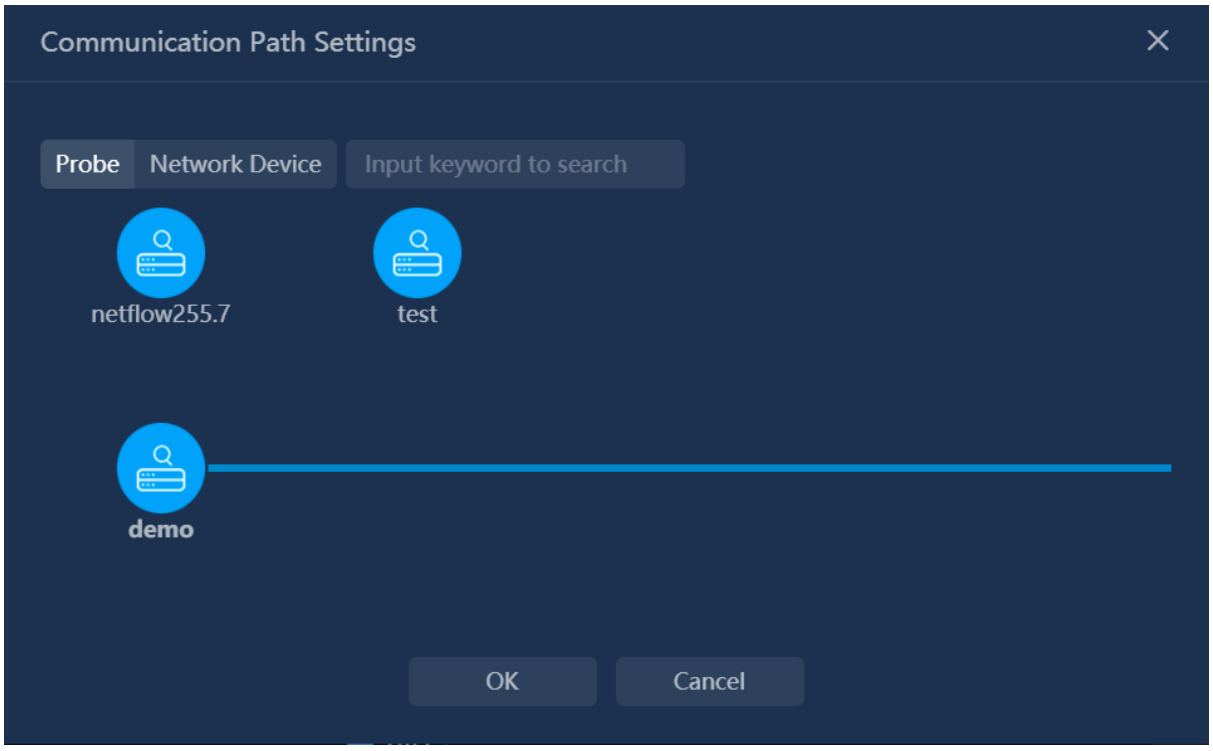
- IP address: users can choose the existing network segment or directly enter the IP address.
- Internet client: if users select the Internet client, it is only need to set the node name.

Add Network Path

After selecting the node, right-click and select "Add Network Path" in the popup right-click menu. The "Add Network Path" pop-up box appears, as shown in the figure below:



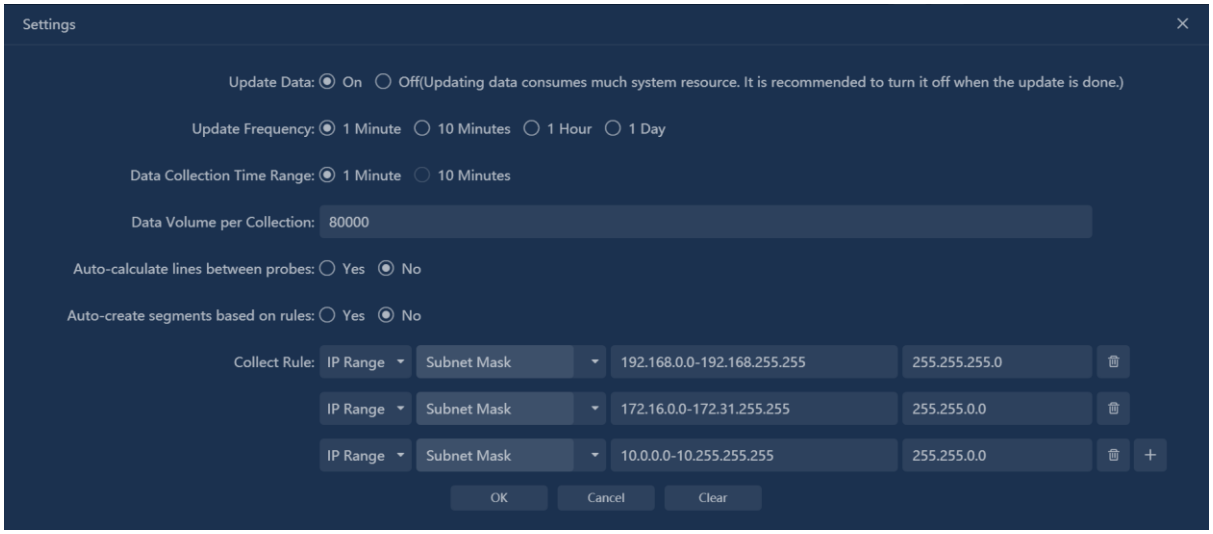
Select the probe in the drop-down list, and the selected probe in the list is the starting probe of the node. Click "OK" button to enter the “Communication Path Settings” and set the pop-up box, as shown in the figure below:



In the “Communication Path Settings” pop-up box, select the other probes that the node passes through.

Data Update Settings

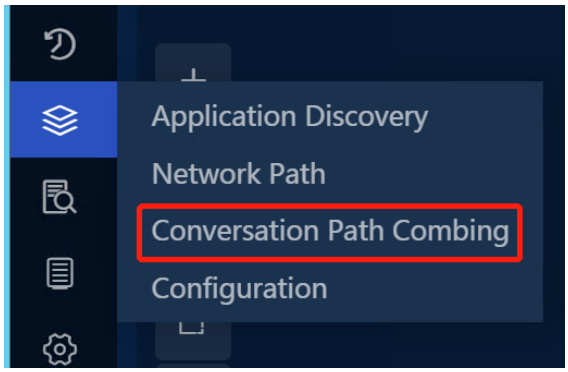
Data Update Settings is used to update the data source of network path discovery. Click the "Settings" button, and a pop-up box of data Update setting pops up, as shown in the figure below:



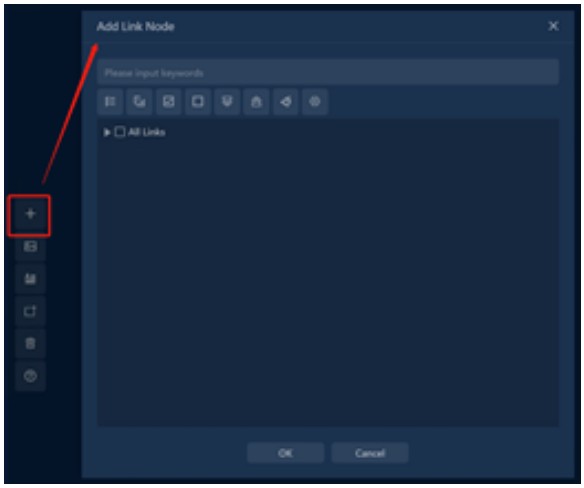
Data update task will take up more system resources, and it is recommended to close this task after network path combing is completed.

5.3. Conversion Path Combing

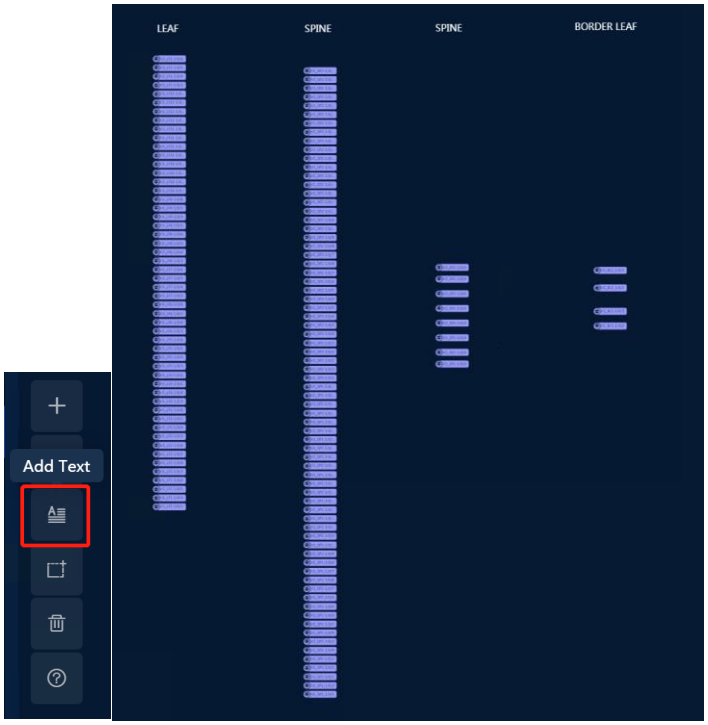
Users can check the path of a specific conversation (TCP session) on UPM. Specify the IP address and port of the TCP conversation, input the date and time that will be searched, select conversation direction, then click Start, UPM can show the path of a TCP conversation.



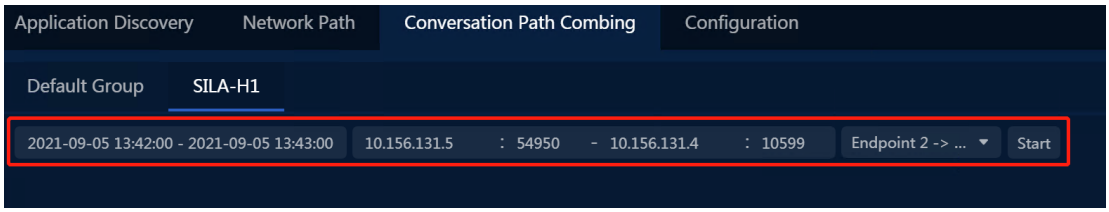
Click Add Link Node to add the links that will search in. Then, click the link to expand its sub-links.



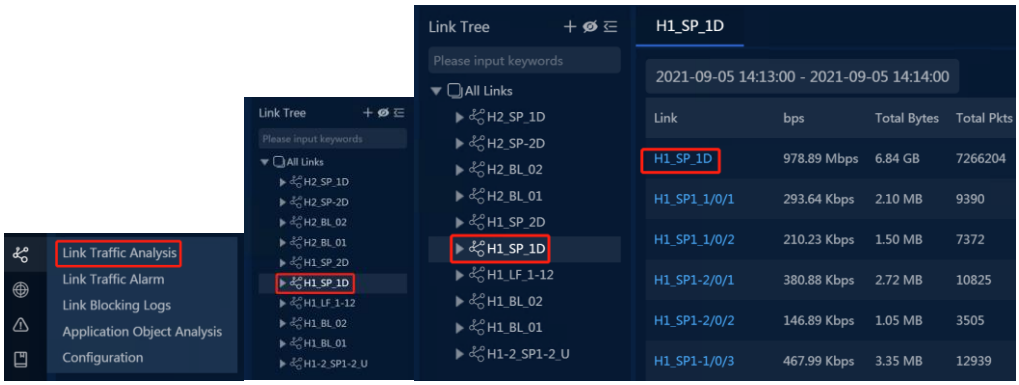
Add text to mark what kinds of sublinks they are.

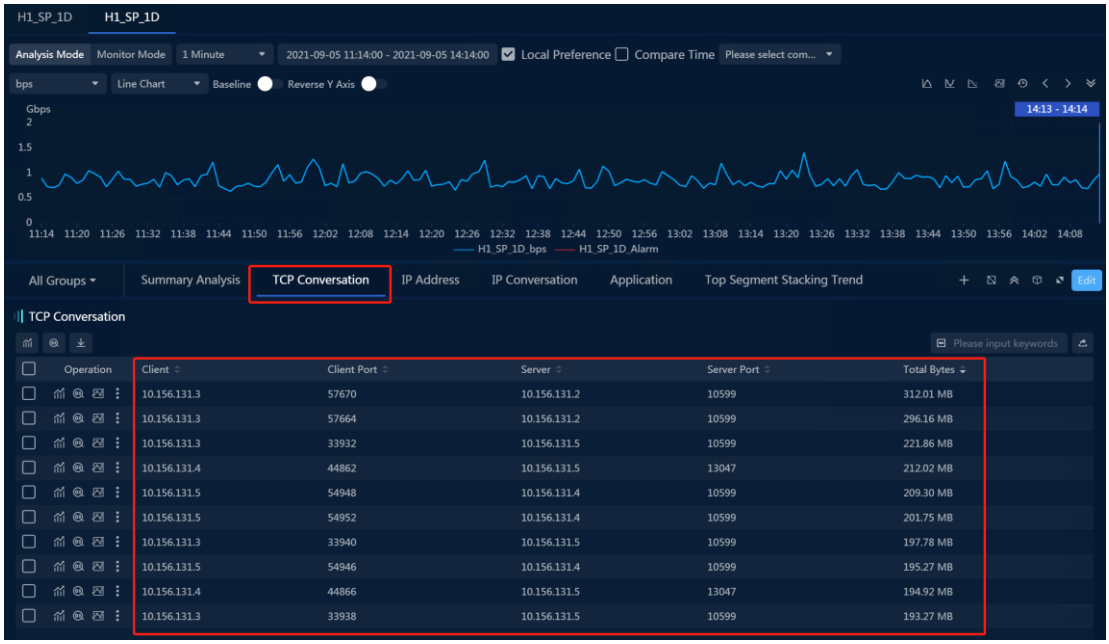


Input the date/time, the ip address and port of the conversation, select the direction, then click Start to search the path. For the time item, we suggest that don't input the second selection.

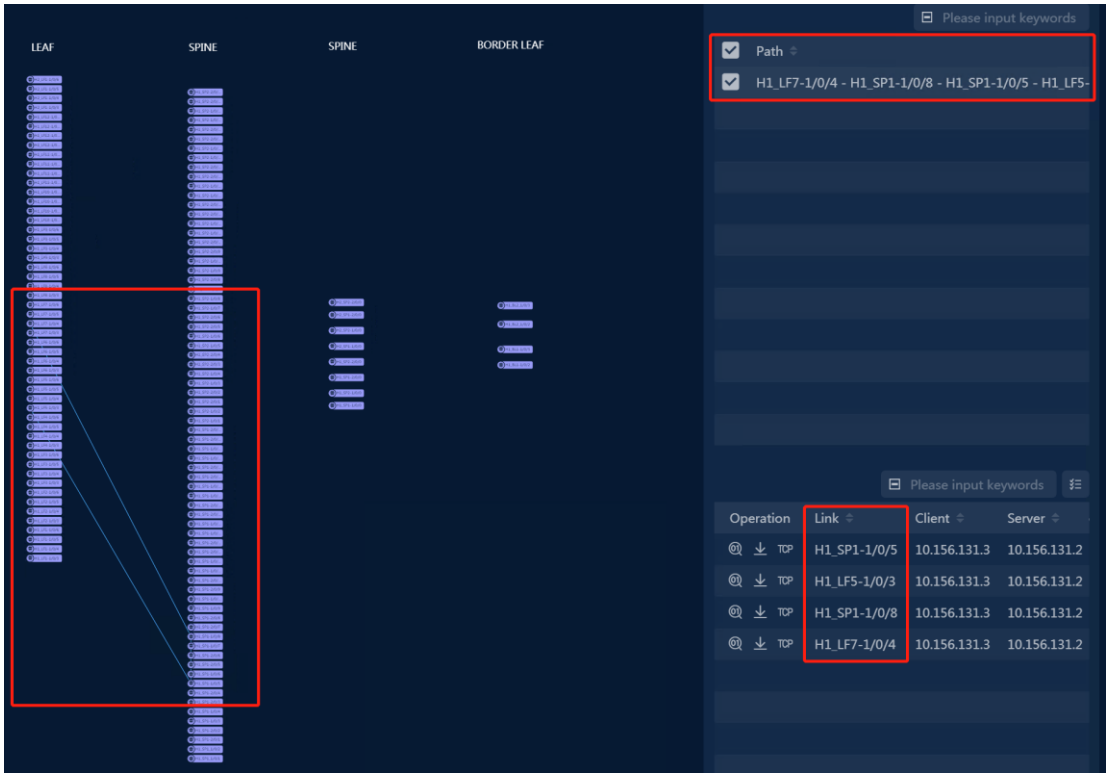


Click Link Traffic Analysis, select a link (here we selected H1_SP_1D), and click this link on the right panel, then all the TopN of the TCP conversations will be displayed in the new panel.





Check in the Path button on the right column, then the conversation path will be displayed. In the lower right corner, the interfaces that this TCP conversation went through are also displayed.



6. Business

6.1. Timeline

On most business monitor and analysis pages, UPM Center uses timeline to display the status of monitored businesses, as the figure below:

6.1.1. Timeline Components

The timeline consists of following components:

- Timeline: consisting of multiple time slices, with a time slice indicating one status. On real-time monitor page, users can click one time slice to open the corresponding time analysis page. On the analysis pages, users can click one time slice to filter data based on that time slice. The time slices can be shown in four colors:
  - Green: no alarms are triggered.
  - Red: there are severe alarms triggered.
  - Orange: there are major alarms triggered.
  - Yellow: there are minor alarms triggered.
- Time Range: the start and end time of the timeline. On analysis pages, users can click it to choose any interested time range.
- Time Slice: the time range of a time slice.
- Selected Time: the time range that is currently selected.

6.1.2. Time Slice Operation

The following list describes the operations on time slices:

 : click to select the previous time slice.

 : click to select the next time slice.

: click to select the previous time slice that has alarms triggered.

: click to select the next time slice that has alarms triggered.

 : click to skip to previous time range.

 : click to skip to next time range.

6.2. Business Status

Business status is a unified monitoring of the running state of all businesses.

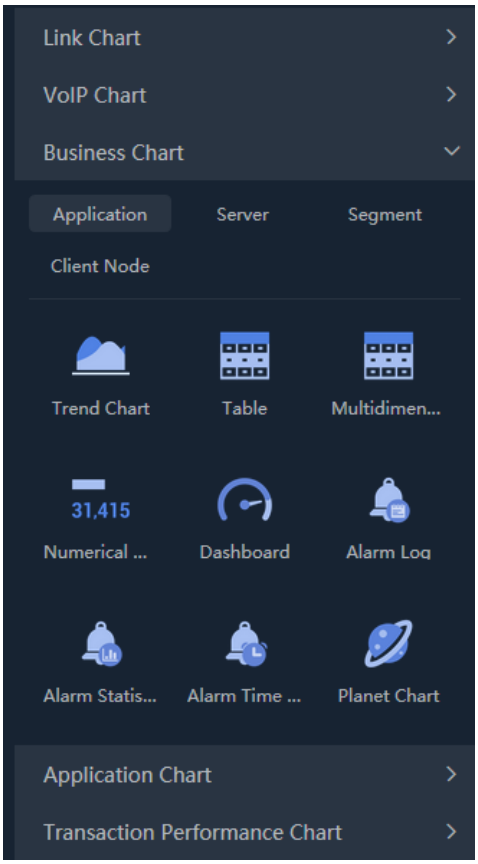
- Click the menu Business Performance -> Business Status to open the Business Status page.
- Click the button " Health Level Alarm " to set the health and alarm status information of the business to display.
- Users can add, edit and delete the business groups.
- Click the button " Fullscreen " to display the monitoring page in full screen.
- Remain users' mouse on the business module and click the button " Analyze "or " Query " to enter into the business performance page or business metric page.
- Click the time slice in the business module or click the alarm number to enter into the Corresponding alarm query page.

6.3. Business Custom Monitoring

Users can customize the monitoring content based on needs.

Click the menu Custom Monitoring -> Custom Metric Monitoring to open the custom Metric Monitoring page. Click the button " " to display the left sidebar and add monitoring graphs.

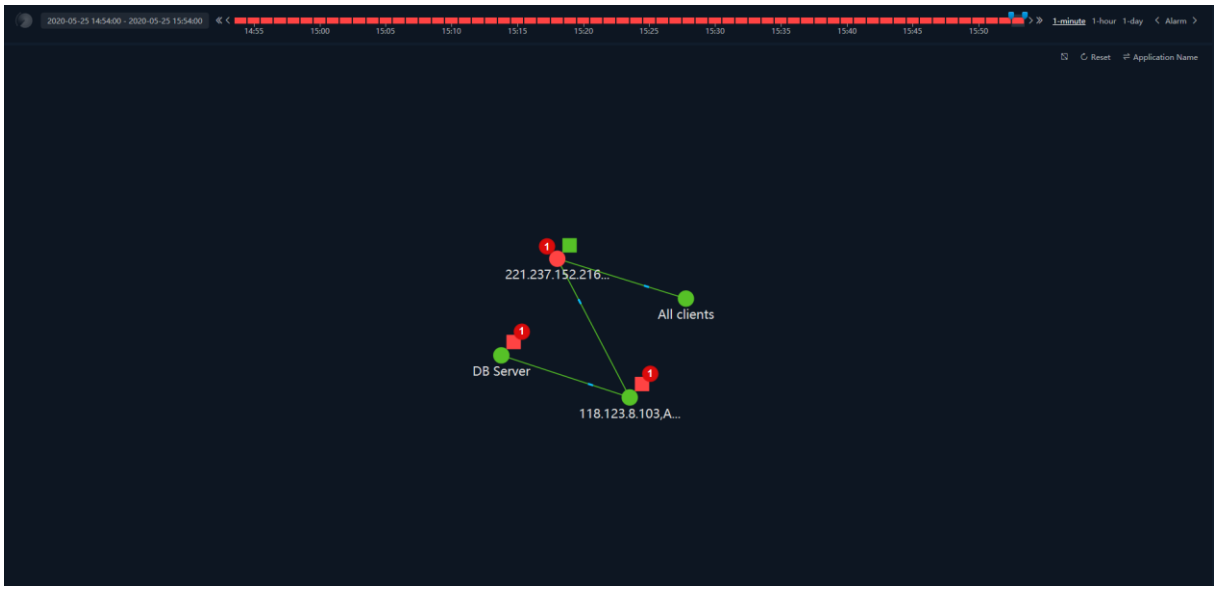
Select the objects and chart type under the business chart to add a new chart.



6.4. Business Global Performance Monitoring

Business global performance monitoring shows the status and alerts of all business nodes.

- Click the menu Custom Monitor -> Business Topology Monitoring to open the global performance monitoring page, as the screenshot below:



- Click the alarm number on the node to jump to the business performance alert page.
- Right-click the node and jump to the business performance analysis page.
- Right-click the link and jump to the page of packet download, multi-segment analysis and business indicator analysis.
- Click the button " ⇌ Application Name " or " ⇌ Alias " to toggles the type of text that the node displays.

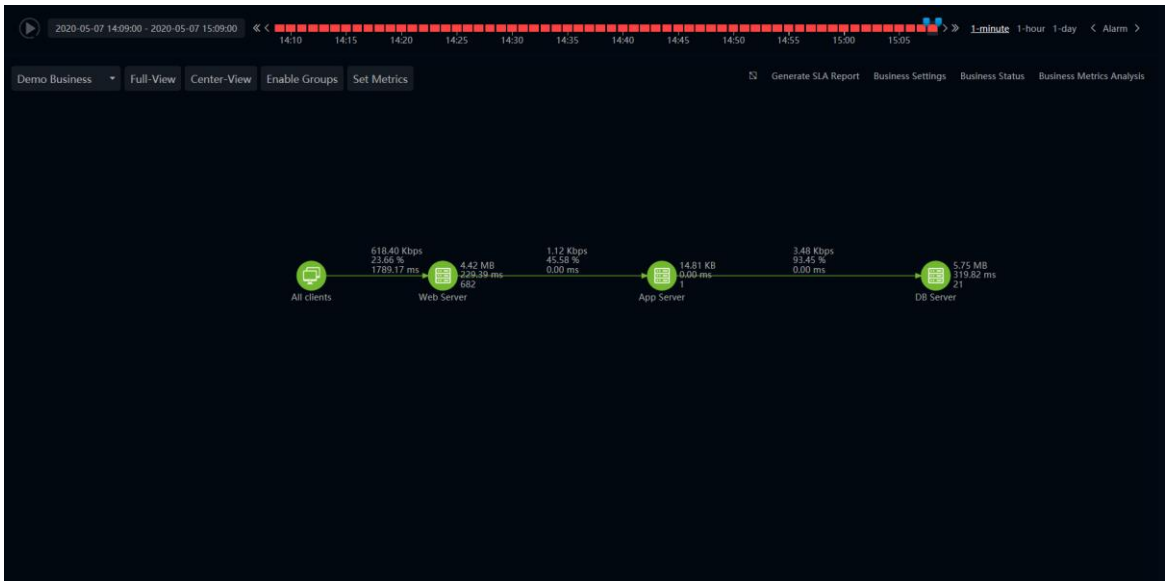
Note

A line means a network path. A circle means a host, a square means an application. And a solid one means a single, a hollow one means multiple.

6.5. Business Performance Analysis

Business performance analysis provides an overall performance analysis of the business, showing business logic relationships and business operation status.

- Click the menu Business Performance -> Business Performance to open the Business Performance analysis page, as the screenshot below:

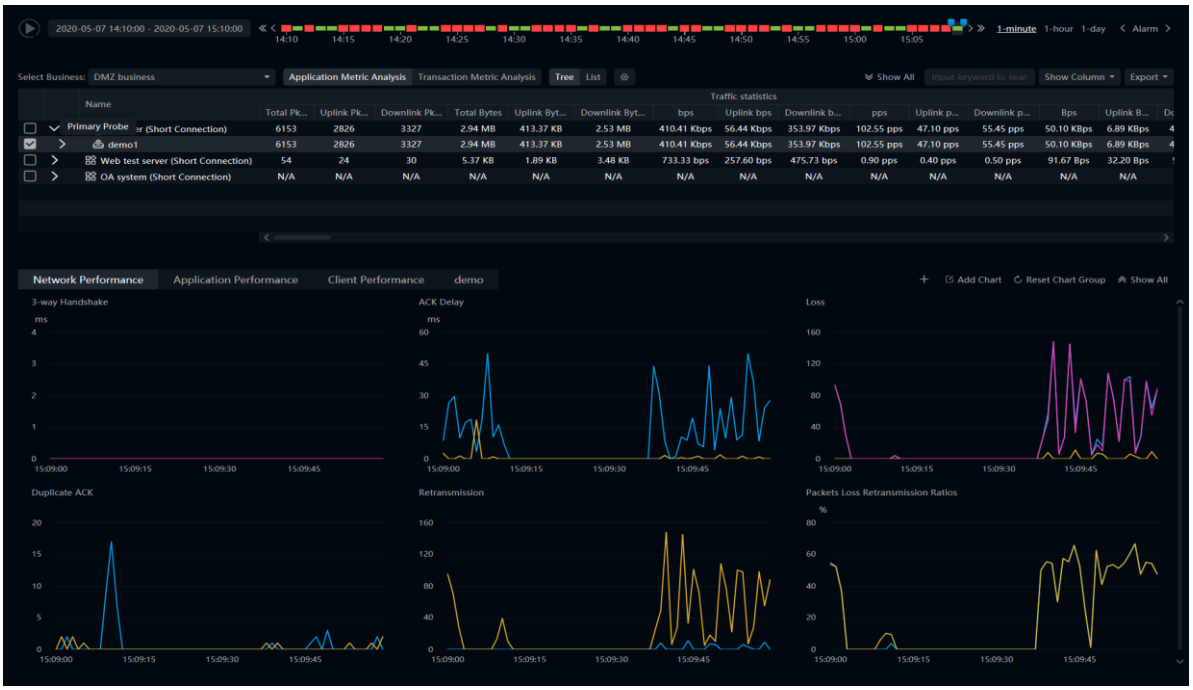


- Click the button “ Configure Metrics “ to set application node metrics, client line metrics and custom application node metrics. No more than three indicators per object. The types of indicators include TCP layer performance indicators and application transaction performance indicators.
- Click the application nodes to open the Summary interface. In the interface users can view application performance, transaction performance, host performance and alarm log performance.
- Click the number of the alarm to view clients alarm information in the Summary interface.
- Right-click the line to jump to packets downloading interface, multiple-segments analysis interface, business metrics analysis interface and transaction performance analysis interface.
- Click these buttons “ Generate SLA Report Business Settings Business Status Business Metrics “ to jump to report interface, business configuration interface, business status interface and business metrics interface.

6.6. Business Metrics Analysis

Business metrics analysis includes application metrics analysis and transaction metrics analysis, which can provide comparison query and graphical display between metrics.

- Click the menu Business Performance -> Business Metrics to open the Business Metric analysis page, as the screenshot below:



- By default, the page displays the metric analysis results of the first business in alphabetical order. Users can click the drop-down list on the top left to choose an interested business.
- Users can view the indicators under application indicator analysis and trading indicator analysis. For the query results of metrics, the system supports two ways of displaying, namely list and tree. Click the button "  " to switch the Display mode.
- Click the button "  " to grouping the metrics and display the status configuration.
- Users can view the system default metric trend charts.

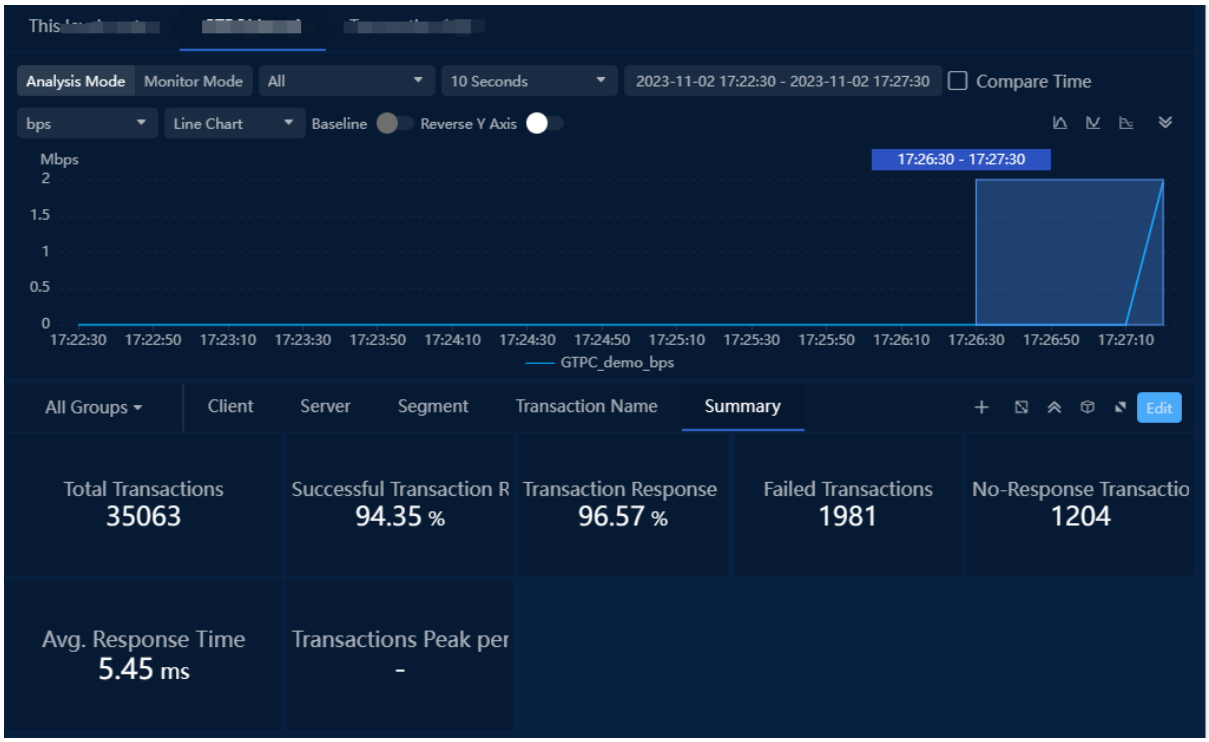
  In the application metric analysis, system provides three metric trend chart groups by default:

  - Network Performance: three handshakes, ACK delay, packet loss, repeated ACK, retransmission, packet loss retransmission ratio.
  - Application Performance: response time, timeout ratio, response time distribution, Apdex metric, number of transactions, transaction response rate.
  - Host Performance: Number of conversations, connection status, server window size, client window size.

  In the transaction analysis, system provides one metric trend chart group by default:

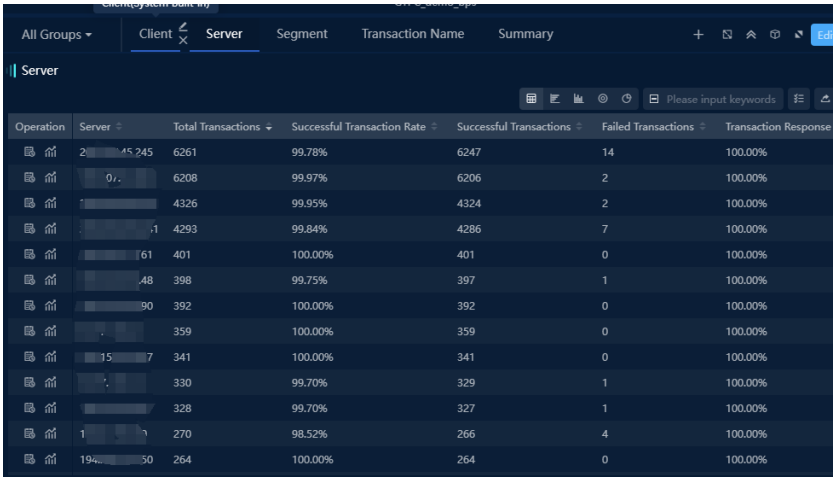
  - Metric chart: number of transactions, response rate, success rate, response time, Apdex value.
- It's supported to customize chart groups and their contents.

6.6.1. Summary



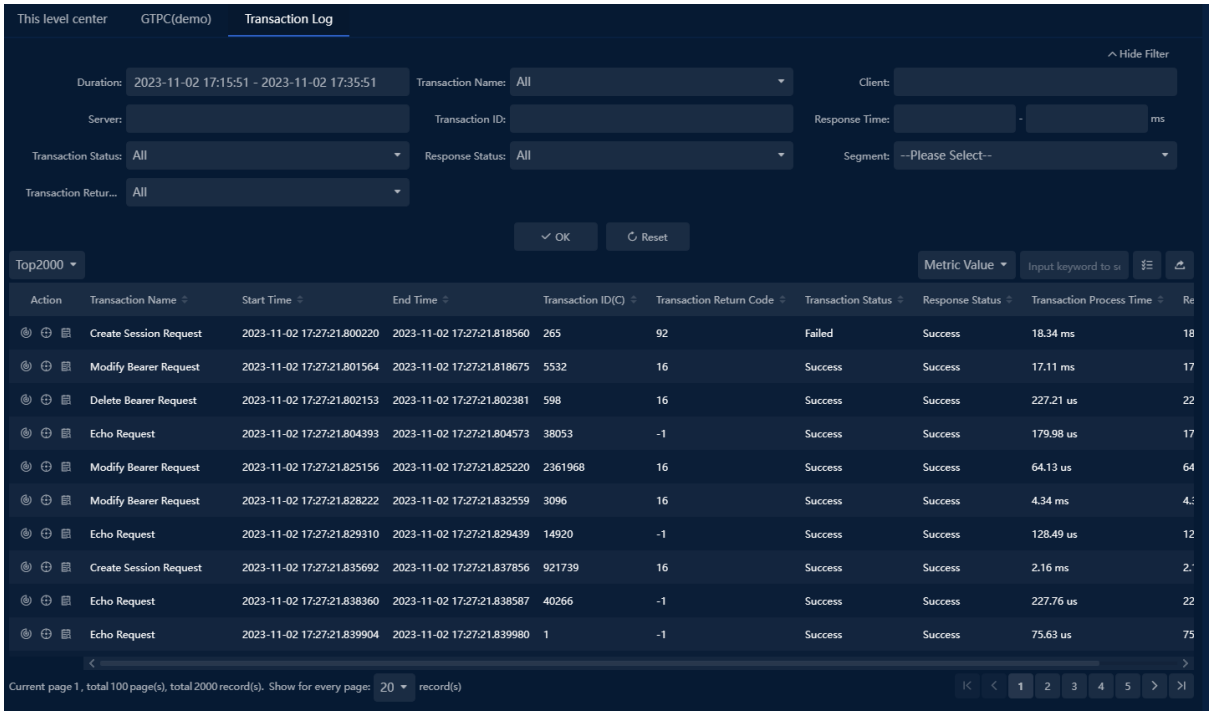
- Supports Analysis mode and Monitor mode. When monitoring mode is enabled, chart data will automatically update according to the refresh rate;
- Supports time comparison. When time comparison is enabled, the trend chart adds a comparison period indicator curve, and the chart below the trend chart is displayed in a vertical stacked manner;
- Table and other components support drill-down analysis, directly entering the transaction query page, or further analyzing and mining trends based on transaction name, server, client, and other dimensions. Multiple analysis pages can be opened.

Detail analysis:



6.6.2. Transaction log

Transaction log analysis page, as shown in the figure below:



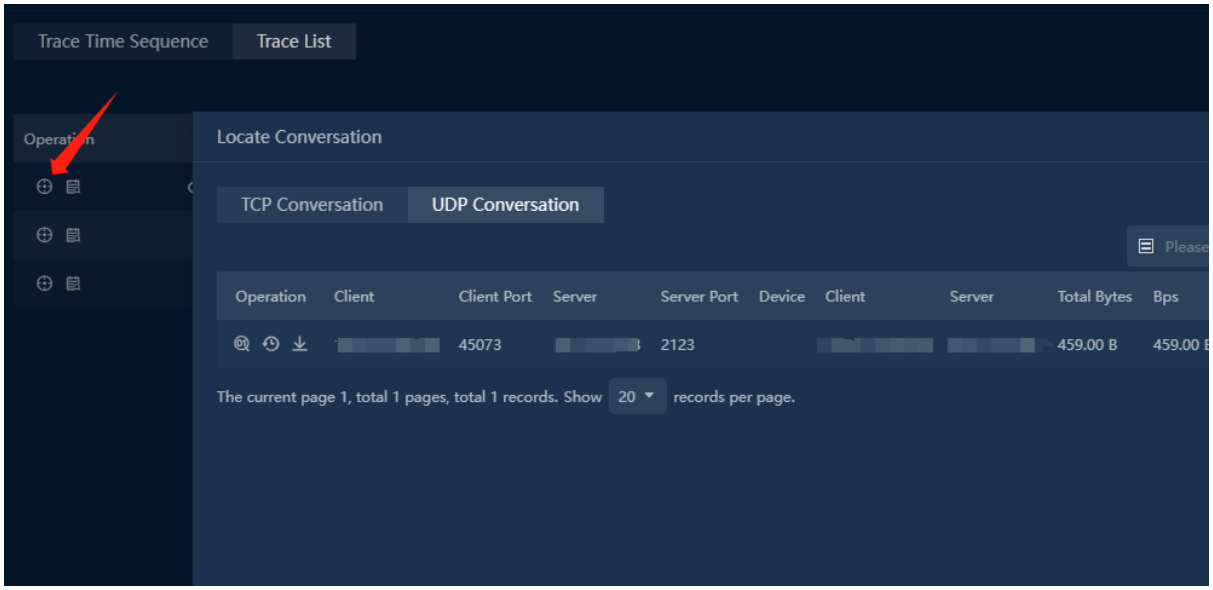
Users can set filtering conditions to filter transaction logs.

6.6.3. Transaction Trace

Select a specific transaction log from the transaction log list to jump to the transaction trace page, as shown in the following figure:

The transaction trace page graphically displays the duration of the entire transaction process, transaction status, and other information. You can quickly find nodes with long durations.

In addition, it supports locating sessions from transaction logs for further viewing of network metrics, host metrics, and problem analysis.



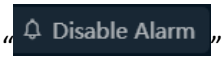
6.7. Business Multiple Segment Analysis

Multi-segment analysis is for comparing and analyzing the data of one application from different probes to identify the segment loss or retransmission issues and the time delay issue.

- Through the "business performance analysis" page, right click the line in the business logic diagram, and select "multi-segment analysis" from the pop-up menu to enter the multi-segment analysis page.
- Users can do analysis configurations:
  - select the application under the current business.
  - select the client in the current application. Different clients correspond to different application paths. When the client is switched, the system will automatically switch paths. If an application is configured with only one client node, the client node is selected by default.
  - set time range: the default time range of the system is consistent with the business performance analysis interface, and users can customize it.
- Users can view the network device information in the communication path.
- Users can view the default indicator trend chart of the system, and check the probe object to be viewed.
  - Select the network packet loss metric, and the metric trend chart shows four metric trend charts by default, retransmission rate, bit rate, segmented loss rate and packet number.
  - Select the network delay, and the indicator trend graph shows four indicator trend graphs by default, namely, RTT of the three-shake client, RTT of the three-shake server, ACK delay of the client and ACK delay of the server.
  - Select the connection failure rate indicator, and the indicator trend chart shows four indicator trend charts by default: synchronization packet, connection failure rate, connection unresponsive times and connection reset times.
  - Select the application response metric, and the metric trend graph default application performance metric, response time, TCP transaction proportion of timeout and TCP transaction request times.

6.8. Business Alarm Configuration

Business alarm management provides unified management of all alarms triggered by business within a certain period of time. In business alarms, users can view all the alarms that have been triggered by the system during the week, and users can acknowledge the alerts as well.

- Click the menu Business Performance -> Business Performance Alarm to open the Business Performance Alarm page.
- Users can view the alarm level distribution diagram, alarm statistics diagram and alarm list.
- Users can click the button “  ” to acknowledge the alarms. After acknowledging alarms, the system will automatically generate a log for this alarm. When the same alarm is triggered later, users can look at the previous log for quick troubleshooting.
- Users can click the button “  ” to look at the previous log for quick troubleshooting. In the logs, according to the history log of the alarm, the false alarm rate, the cause classification of the alarm and the top 10 hosts/network devices/paths that triggered the most alarms under this classification were counted.
- Users can click the button “ 

” to open the Disable Alarm page.
- Users can click the button "  " to disable the alert.
- Users can click the button "  " to cancel the disable of the alert.
- Users can click the button “  ” to open the data downloading page.
- Users can click the button “  ” to download the packets automatically saved by the server to the local.

Note

when configuring the alarm, users can only click the button to download a packet if users have enabled custom alerts for automatic packet download.

6.9. Business Report

The business report component produces individual business reports from a business perspective. Users can select an application analysis object for a business and select the diagram type.

- Click the menu Report to enter into the report management interface and click the button “  “ to add a new application chart.
- Click the button “ Preview “ to preview the real chart.
- After completing the settings, click the button “ OK “ to save settings. Set the report properties:
    - Report format: PDF, WORD, EXCEL and HTML, and users can choose one of them.
    - Report type: optional daily report, weekly report, monthly report and report generation time.
    - Business period: support the setting of business period, with the minimum accuracy to minutes for daily report, 10 minutes for weekly report and hours for monthly report.

- Comparison: support comparison with the previous period, the same period of last year, the same period of last week and the designated date when selecting the daily newspaper; When selecting a weekly report, support comparison with the previous period and the specified date; When selecting a monthly report, support comparisons with the previous cycle, the same period last year, and the specified date.
- Receiving mailbox: the receiving mailbox of the report. After filling in the email address, the system will regularly send the report to the designated mailbox.

Note

The SMTP server is configured correctly before the report can be sent successfully.

- In the report list page, users can also click the name of a report to enter the report log interface and view the historical reports generated by the report

7. Business configuration

7.1. Introduction

7.1.1. Description

The business monitoring and analysis function can comprehensively monitor the service quality of various links in the business system, quickly discover and locate issues that affect key business performance and stability. The business module is designed to maximize the operational efficiency and fault handling capability of the business network, and provides analysis functions such as supporting network environment analysis, real-time performance monitoring, and fast fault localization based on the customer's business network.

7.1.2. Functional scenarios

- In the centralized monitoring page of the business, the running status of each business is visually displayed in graphics, allowing users to quickly identify business with abnormal status.
- Analyze and locate different application nodes and network paths for individual businesses.
- Monitor and analyze the transaction performance of individual businesses. Analyze the running quality of business systems from a business perspective, achieving the goal of quickly analyzing and locating problems.

7.1.3. Value

The product focuses on business and actively organizes and analyzes traffic data from all nodes in the network, helping users quickly understand the access relationships and business logic relationships of key hosts and applications in the network from a business perspective, and presenting them in a graphical and visual way.

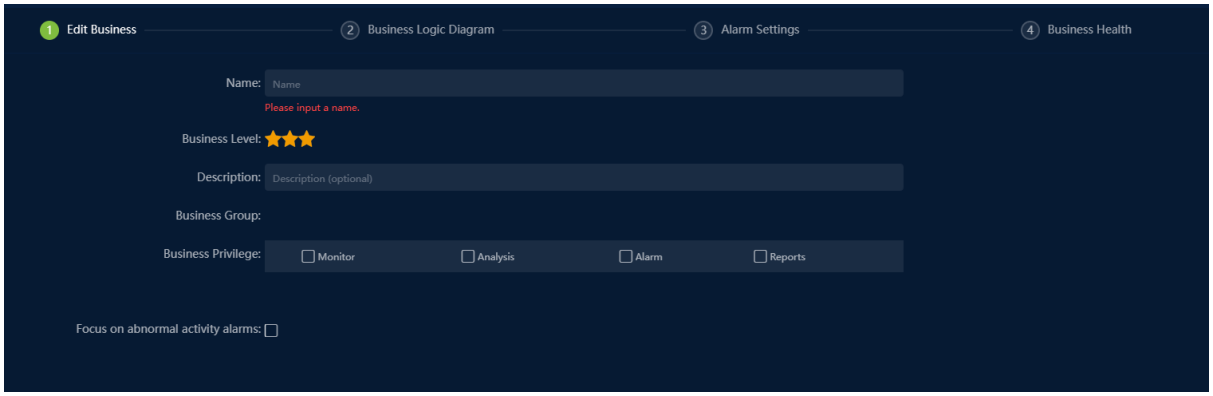
7.2. Guide

The content of business configuration includes edit basic business information, business logic diagram, alarm settings, and business health.

7.2.1. Edit Business

The main step of 'Edit business' is to configure the basic information of the business.

The configuration page of 'Edit business' is shown in the figure below.

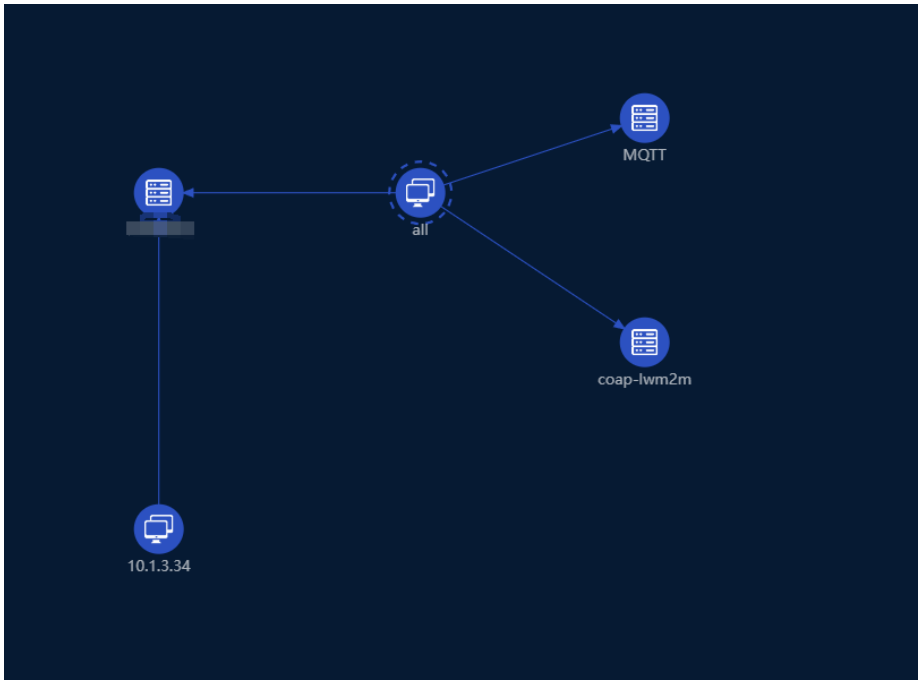


Field Name	Description
Name	Used to set the name of the business, and the business name cannot be duplicated.
Automatically defined through interfaces	Optional configuration item, supports synchronizing application and application group information to business configuration through interfaces.
Business level	Used to set the operation level of the business. The centralized monitoring page of the business supports sorting and filtering based on the operation level.
Description	Optional configuration item, used to describe relevant information of the business.
Business Group	Optional configuration item for setting the business group to which the business belongs. The business monitoring page supports business monitoring by business group.
Business Privilege	Optional configuration item for setting the permissions of users already configured in the system for adding new businesses, including monitoring, analysis, alert, and reporting permissions.
Whether to monitor abnormal behavior alerts	Optional configuration item for determining whether application-related abnormal behavior alerts are included in this business.

7.2.2. Business Logic Diagram

The 'Business Logic Diagram' step mainly sets the access relationships between applications within the business. The business logic diagram is the basis for subsequent business monitoring and analysis.

The completed business logic diagram is shown in the following figure.



The business logic diagram supports configuration through both new configuration and import.

Configuration

The basic elements involved in the business logic diagram configuration include:

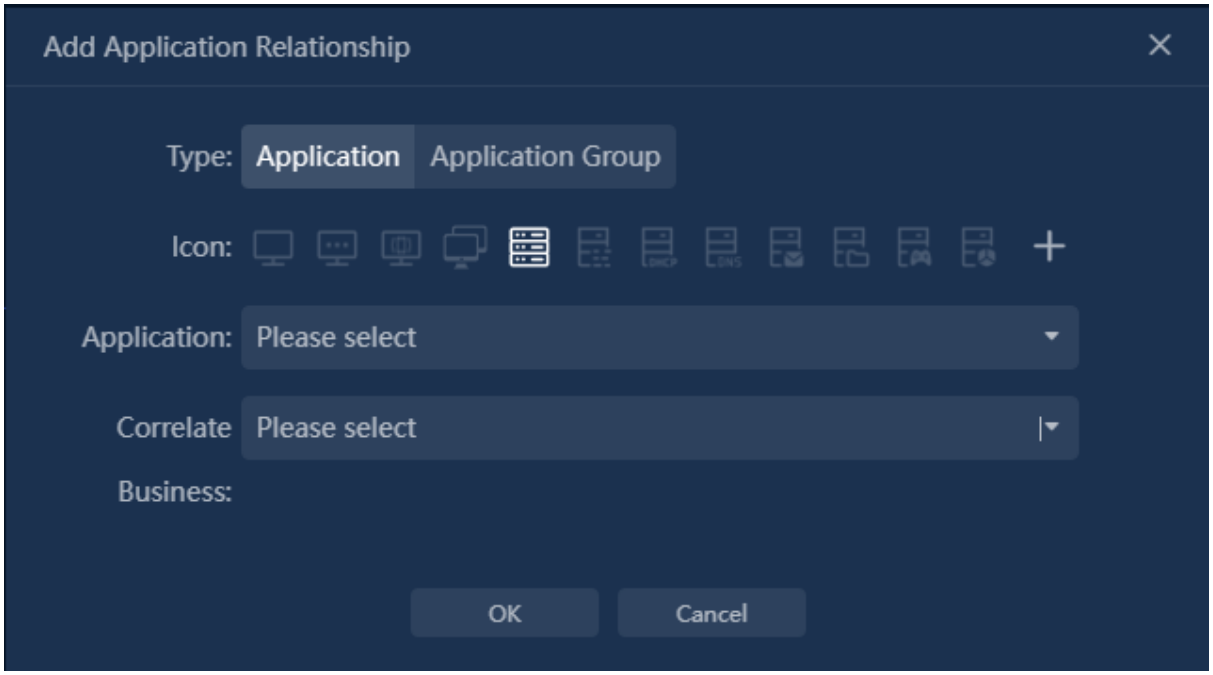
- Application node: represents an application or application group, through which applications or clients can be discovered and managed.
- Client node: can directly select clients in the application configuration, and also supports adding clients in the business logic diagram.
- Merge node: clients can be merged with client nodes or server nodes under certain conditions, and after merging, they will be displayed as one point.
- Connection: represents the communication path between applications and clients. Probes can be bound, intelligent alerts can be set, and network devices can be configured on the connection.

Add application node

Add application nodes through the following entry points:

- Right-click on the blank area of the page and select 'Add application relationship' from the pop-up context menu.
- Click on the 'Add application' icon in the upper left corner of the page.
- In the application structure tab on the right side of the page, click on 'Add application'.

The 'Add application' dialog box is shown in the following figure.



The configuration items in the dialog box are explained as follows:

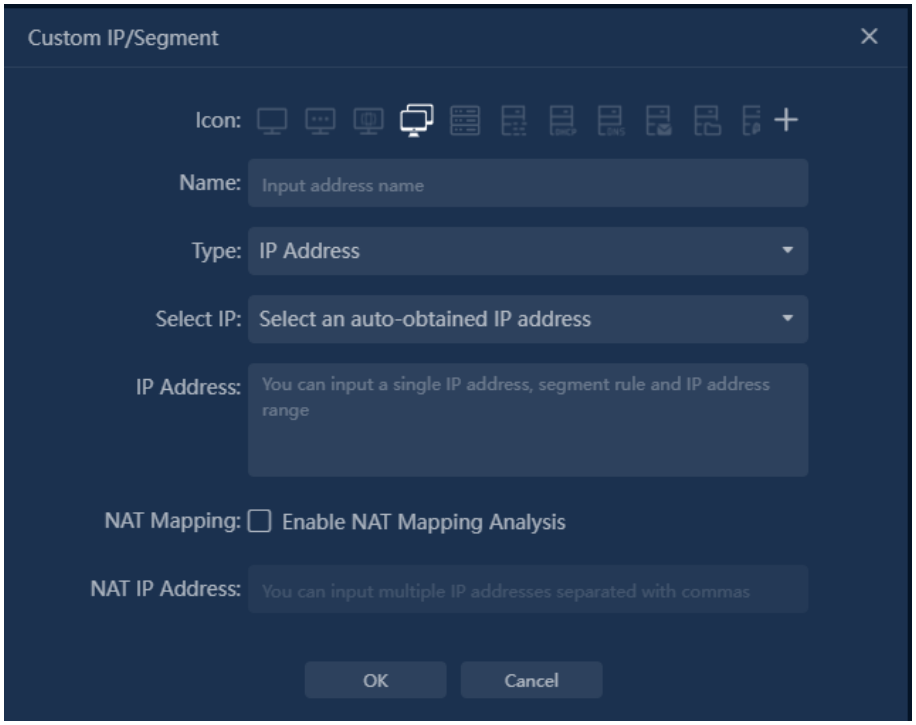
- Type: Used to set whether the added node is an application or an application group.
- Icon: Used to set the icon of the added node, and users can upload icons.
- Application: Used to select applications/application groups, supports multiple selections.
- Associated Business: Used to select associated businesses, supports multiple selections. If associated businesses are configured, clicking on the application node will jump to the associated business analysis page in the business performance analysis page.

Add client node

Add client node through the following entry:

- The "Add Client" icon in the upper left corner of the page. The icon is clickable only when an application node is selected in the logical diagram.
- After selecting the application node, right-click and choose "Discover Client" or "Add Client" from the pop-up context menu.
- On the right side of the page, click "Add" or "Discover" on the client node in the application structure tab.

The "Add Client" dialog box is shown in the following figure.



The configuration items in the dialog box are explained as follows:

- Icon: Used to set the icon of the added node, and users can upload icons.
- Name: Used to set the name of the added node.
- Type: Client node types include IP address, subnet, and all clients.
- IP Address: When selecting the IP address type, it is used to set the client's IP address, supporting single IP, subnet (mask method), and IP range.
- Subnet: When selecting the subnet type, it is used to select the configured subnets in the system. Only one subnet can be selected.
- NAT Mapping: Used to set whether to enable NAT mapping analysis. If enabled, the statistical data of NAT IP and the statistical data of the original client will be merged during data statistics.
- NAT IP Address: Used to set the IP address after NAT. The N AT IP address can only be configured when N AT mapping is enabled.

Discover Associated Applications

Discover Associated Applications is mainly used to discover other application nodes accessed by the selected node as a client node, that is, to discover the access relationship between applications.

The process of discovering associated applications: Use the server address of the application as the query condition to query the service access table in all probes for the past 1 minute. According to the query results, display them merged by application. If no application is matched, the server: port will be displayed directly. Users can define such nodes as applications or add them to existing application configurations.

After selecting the application node, right-click and select 'Discover Associated Applications' from the pop-up menu. The system will automatically perform a query for associated applications, and the query result dialog box is shown in the following figure.

The functional buttons in the 'Discover Related Applications' dialog box include 'Add Application' and 'Add to Application', which support filtering the data in the list based on status and whether the application is defined.

Explanation of 'Add to Business' field:

- 'Add to Business' includes 'Added' and 'Not Added', indicating whether the current application node has been added to the current business.
- When selecting a node that is not defined as an application, the operation of adding to the business cannot be performed.
- When selecting a node that is defined as an application, you can choose whether to add it to the business.

The fields in the list include checkboxes, 'Add to Business', application rules, connection type, path, and application.

- Application rules: Displayed in the format of server IP+ port, for defined applications, if there are multiple server IPs: ports, they need to be merged into one record.
- Path: If the traffic is only collected on one probe, just add that probe to the network path; If multiple probes collect the same traffic, the order between the probes needs to be determined. Probe order determination algorithm: Based on the serverRTTtime in the service access statistics table, the smaller the serverRTTtime, the closer it is to the server. For automatically generated network paths, customers are allowed to manually update them.

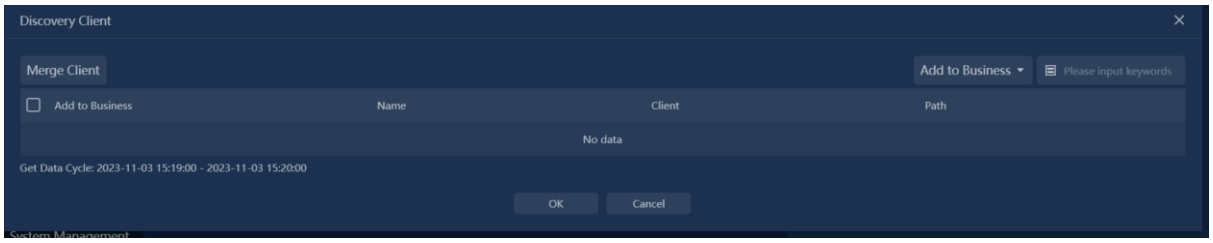
Note: When performing associated application discovery, the selected application's server addresses are added as subnets to the client nodes of the newly discovered application. After this processing, when the application's configuration changes, such as adding new server addresses, the client nodes of the newly discovered application do not need to be manually updated. The client information is automatically updated through the form of subnets.

Discover Clients

Discover Clients is mainly used to find out which clients are accessing the selected node as an application server. The number of automatically discovered clients varies greatly depending on different applications (such as intranet applications, internet applications). Discover Clients is mainly used to automatically discover clients for intranet applications.

Process of discovering clients: Use the server address of the application as the query condition and search the service access table in all probes for the past 1 minute. Use the retrieved sessions as basic data to organize the clients.

After selecting the application node, right-click and choose 'Discover Client' from the pop-up menu. The system will automatically perform client discovery. The client discovery dialog box is shown in the following figure.



In the client pop-up box, the functional buttons include merging clients and filtering data in the list by status. Merging clients means combining one or more clients into one client.

Adding to the business column allows you to add the selected clients to the business or not.

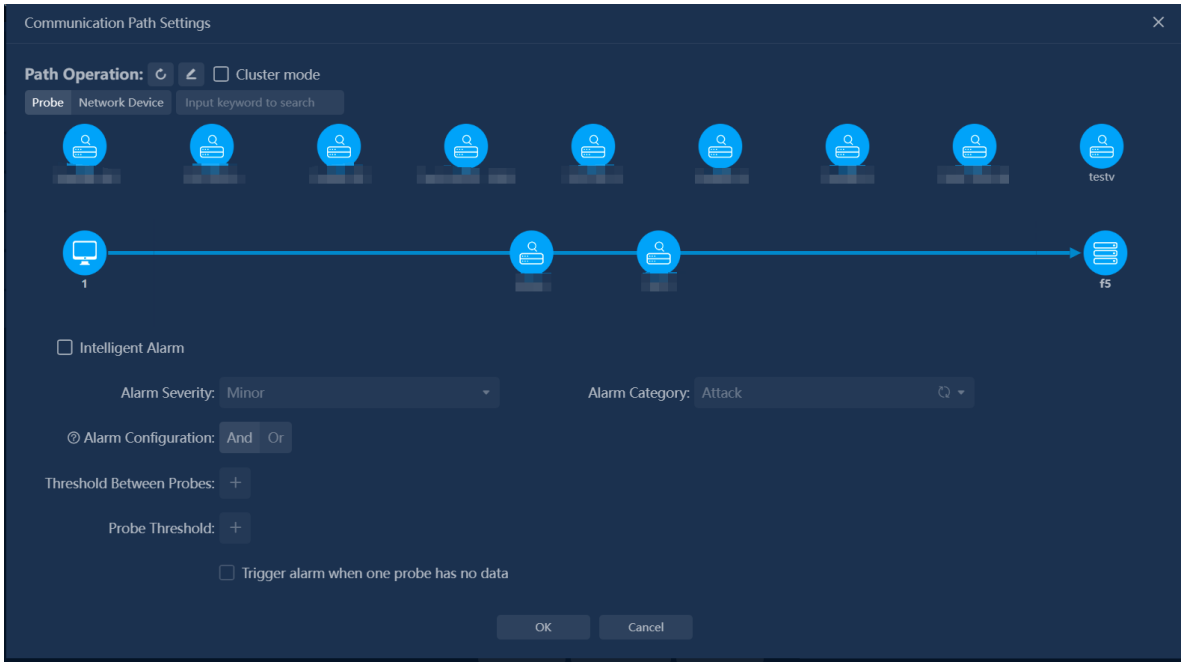
- Add to business: If set to add to business, it means that the corresponding application node will be added to the business logic diagram and application structure tree.
- Do not add to business: If set to not add to business, it means that the node will not appear in the business logic diagram and application structure tree.

The fields in the 'Client Discovery' list include checkboxes, add to business, name, client, and path.

- Name: Displays the automatically discovered clients by default and supports user modification. If it is a network segment, it will be displayed as the network segment name; If it is a single IP client, it will be displayed as the IP address.
- Client: According to the traffic data, if the discovered client belongs to the defined network segment, it needs to be merged into one record based on the network segment.
- Path: If the traffic is only collected on one probe, just add that probe to the network path; If multiple probes collect the same traffic, the order between the probes needs to be determined. Probe order determination algorithm: Based on the serverRTTtime in the service access statistics table, the smaller the serverRTTtime, the closer it is to the server. For automatically generated network paths, customers are allowed to manually update them.

Edit communication path

Click on the connection between the application node and the client node to open the 'Communication Path Settings' dialog box. Set the communication path in the dialog box as shown in the following figure.



The communication path can be set as curve, polyline, or straight line, with straight line as the default setting.

In the communication path configuration, support for probe cluster mode is available, which is suitable for application clusters or scenarios with primary and backup deployments. In cluster mode, when configuring, there is no need to separately set the aggregate probe. The system automatically aggregates data based on the selected probes.

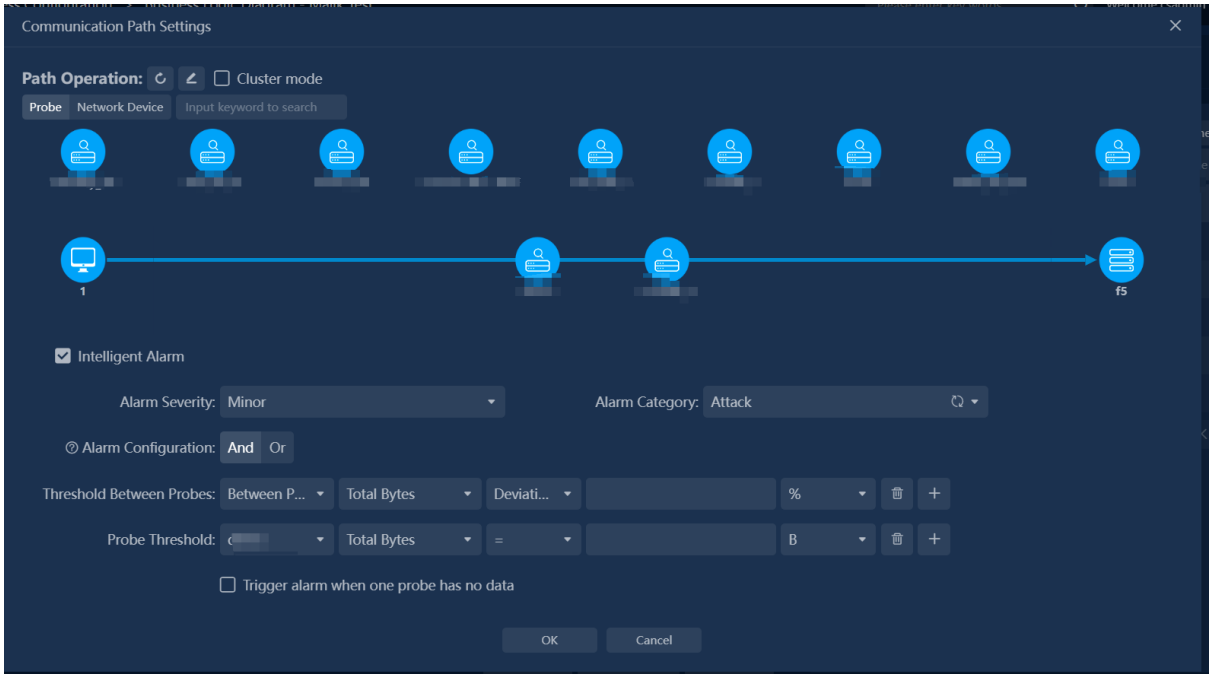
Import Access Relationships

By importing access relationships, you can simplify the configuration operation of the business logic diagram. Go to the 'Relationship' tab on the right side of the page and click the 'Import' button to import the pre-exported access relationship table. After the import is completed, you can edit the imported access relationships in the left view.

Note: When importing and exporting access relationships between different systems, please ensure that the applications in the access relationship file exist in different systems and have the same configuration, otherwise it may be impossible to import.

Intelligent alarm

In the communication path settings dialog box, when the number of probes added on the path is greater than or equal to 2, the intelligent alert configuration page will appear as shown in the following figure.

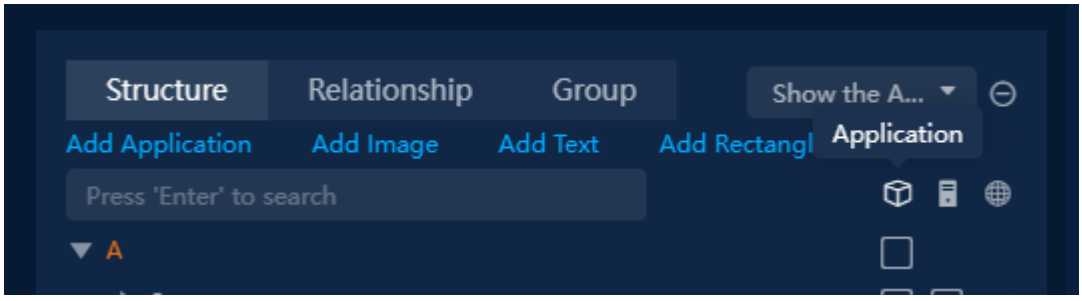


When configuring intelligent alarms, you can set the deviation between probes and specify the threshold for probe metrics. When the collected traffic meets the set threshold, an alarm will be triggered automatically.

The intelligent alarms enabled here can be managed on the 'Configuration > Business Alarm Configuration' page.

Application performance alarm

In the application structure tree, you can enable/disable business performance alarms as shown in the following figure.



Business performance alarms include application performance, host performance, and network performance 3 types.

- Application performance: application performance degradation, poor application performance, application service unresponsive, transaction performance poor, transaction performance degradation, transaction service unresponsive
- Host Performance: Server Unreachable, Server Unavailable, Server Transmission Performance Severely Degraded
- Network Performance: Few Packet Loss in Network, Severe Packet Loss in Network, Network Path Interruption

The enabled business performance alerts can be managed on the 'Configuration > Business Alarm Configuration' page.

Note: Business performance alerts are system-built alerts and do not support custom alert thresholds.

Application group

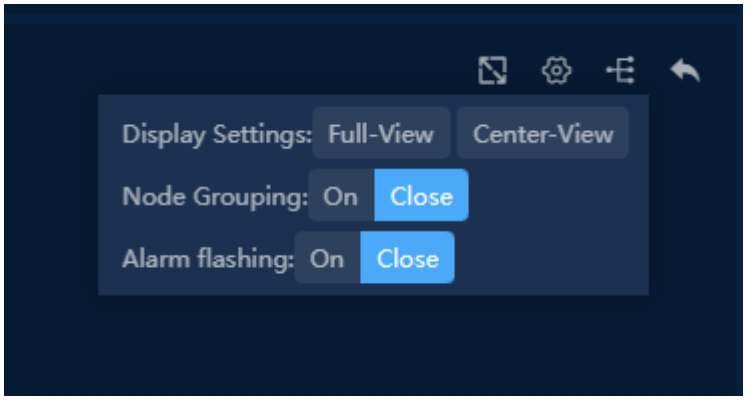
Group settings are used to group nodes in the business logic diagram. Nodes belonging to the same group can be displayed as one node when shown.

When setting up groups, 'Group Coordinates' indicate the node that serves as the base point for grouping when displaying.

Rules for group settings:

- Only nodes of the same type can be added to a group.
- The number of group nodes cannot be less than 2
- Currently, only 1 group is supported

On the 'Business Performance -> Business Performance Analysis' page, you can set whether nodes are displayed according to groups through the display settings button.

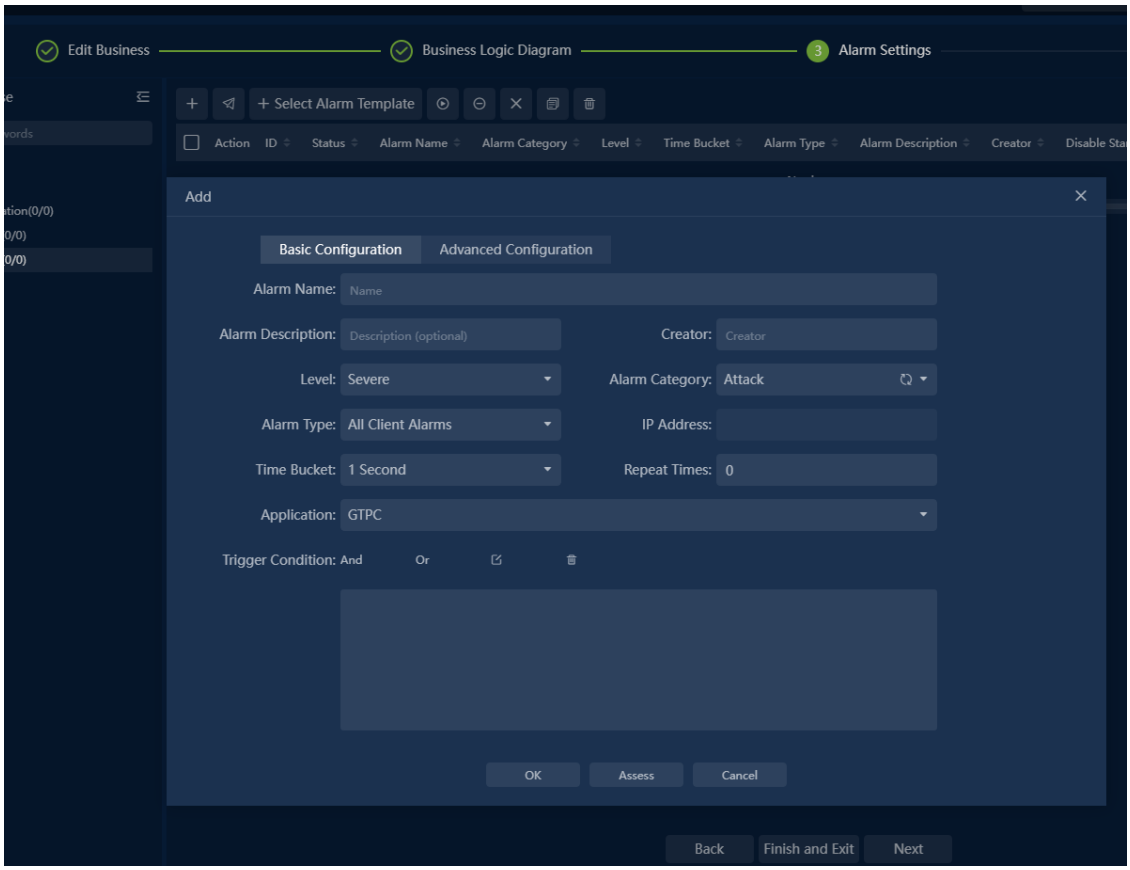


7.2.3. Alarm settings

The alarm settings page is used to configure alarms related to business, including custom alarms, intelligent alarms, asynchronous duplex long connection alarms, and business performance alarms.

Custom alarm configuration can be performed on the alarm settings page of business configuration. For configuration and management of other alarms, please operate on the 'Configuration > Business Alarm Configuration' page.

The alarm settings page is shown in the following figure.



Custom alarms are mainly configured for application nodes, server nodes, and client nodes in the business tree. The alarms that can be configured for various types of nodes are as follows.

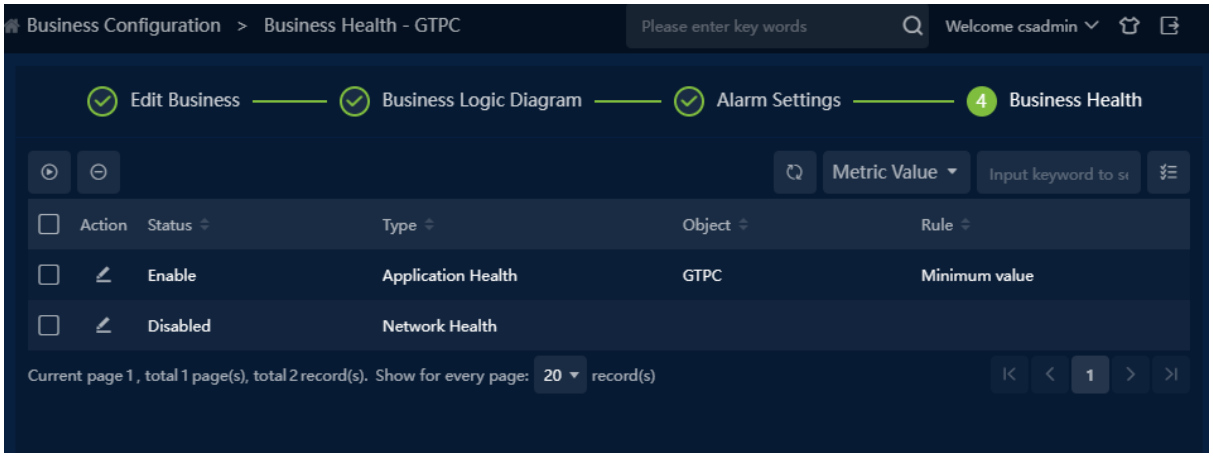
- Application Node: Application Monitoring Alert, Application Baseline Alert, Application Burst Alert, Application Transaction Burst Alert, Application Transaction Baseline Alert, IP Session Alert, TCP Session Alert, UDP Session Alert, Service Access Alert, TCP Service Port Alert, UDP Service Port Alert, Transaction Statistics Alert, Transaction Burst Alert, Transaction Baseline Alert, Transaction Log Alert
- Server Node: Single Server Alert, Single Server Burst Alert, Any Server Alert
- Subnet Client: Subnet Client Alert
- Any Client: Any Client Alert
- Single Client: Single Client Alert

Note: For transaction-related alerts in the application node, configuration is only supported if the application is mounted with transactions.

7.2.4. Business health

The Business Health page is used to set the application health and network health of the business.

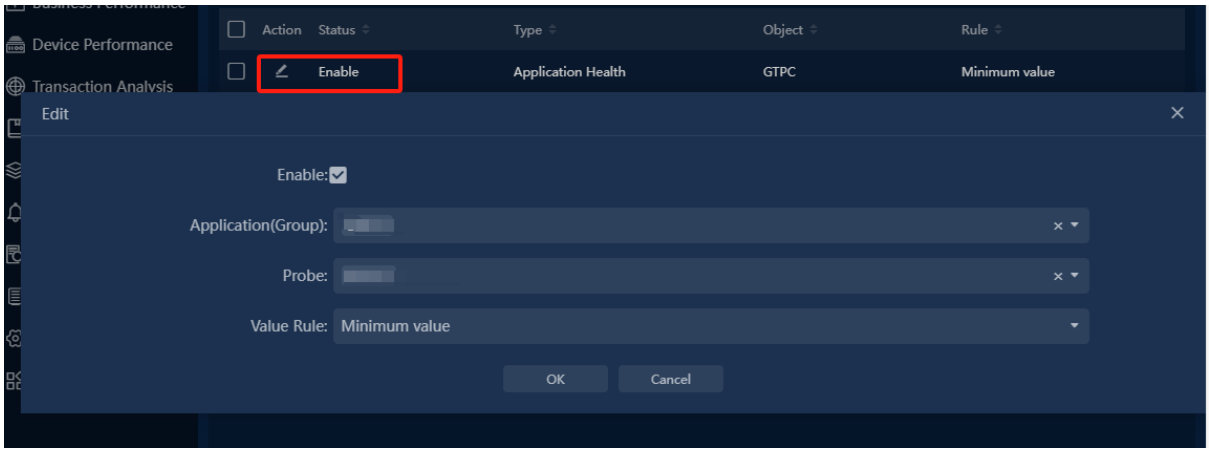
The Business Health Settings page is shown in the following figure.



7.2.5. Application health

Application Health is mainly used to evaluate the service quality of the business.

The Application Health Settings dialog box is shown in the following figure.

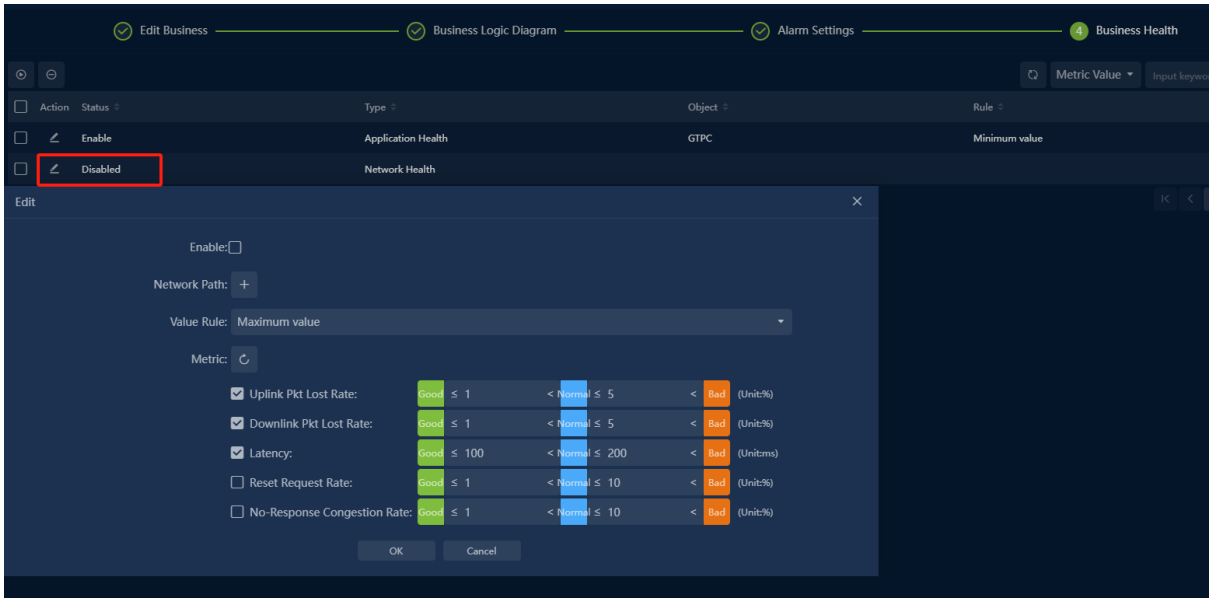


Calculation Explanation: When multiple applications or probes are selected, multiple application health values will be calculated. At this time, the system will calculate the application health of the business based on the value rules. Value rules include maximum value, minimum value, and average value. The system defaults to the minimum value.

7.2.6. Network Health

Network health is mainly used to evaluate the network quality of the business.

The network health settings dialog box is shown in the following figure.



Evaluate network health by specifying metrics in the network path.

When configuring the network path, you need to select the application, client, and probe. Among them, the application and client support single selection, while the probe supports multiple selection. Select which probe's data to use for health calculation from the probe list. If multiple probes are selected, the lowest score will be used as the network health of the business.

Supported metrics include upstream packet loss rate, downstream packet loss rate, network latency, connection request reset rate, and connection no response rate. Users can set the thresholds for good, normal, and poor for each metric based on the actual network conditions. If multiple metrics are selected, the health is calculated separately for each metric, and then the final network health is calculated based on the value rules.

When multiple network paths are configured, the system will calculate the health of each network path separately, and then calculate the network health of the business based on the user's set value rules. The value rules include maximum value, minimum value, and average value, and the system defaults to the minimum value.

> *Note:* The system defaults to not enable application health and network health statistics. The application health and network health of the business can be monitored on the business centralized monitoring page and the custom indicator monitoring page.

7.2.7. Common QA

1. Operation tips

When configuring the business logic diagram, you can refer to the following tips:

1. Right-click on the blank area to quickly add applications and batch set line shapes.
2. When dragging two nodes to overlap, you can merge the nodes.

3. Ctrl + click or Ctrl + select to select multiple nodes.
4. After selecting multiple nodes, you can quickly align, distribute evenly, and perform other operations through icons.
5. Click on the connection to set the network path.
6. By importing/exporting relationships, you can quickly define new businesses.

2. Node merge failed.

Problem Description

Failed to merge when dragging two nodes to overlapping positions.

Possible reasons

Does not comply with the rules for node merging.

Rules for node merging:

- Application nodes cannot be merged.
- The number of same-direction connections should not decrease when merging nodes.
- Nodes under group settings cannot be merged.

8. Transaction

8.1. Transaction Custom Monitoring

Click the menu Scene Center View -> 

-> Custom to open the custom metric monitoring interface.

8.2. Transaction Performance Analysis

Transaction performance analysis is a multidimensional analysis of the application of transaction processing performance, which is used to find out whether there are problems in the processing performance of business systems and analyze positioning problems.

Transaction performance analysis includes transaction summary analysis, transaction log analysis and transaction tracking analysis.

8.3. Transaction Custom Query

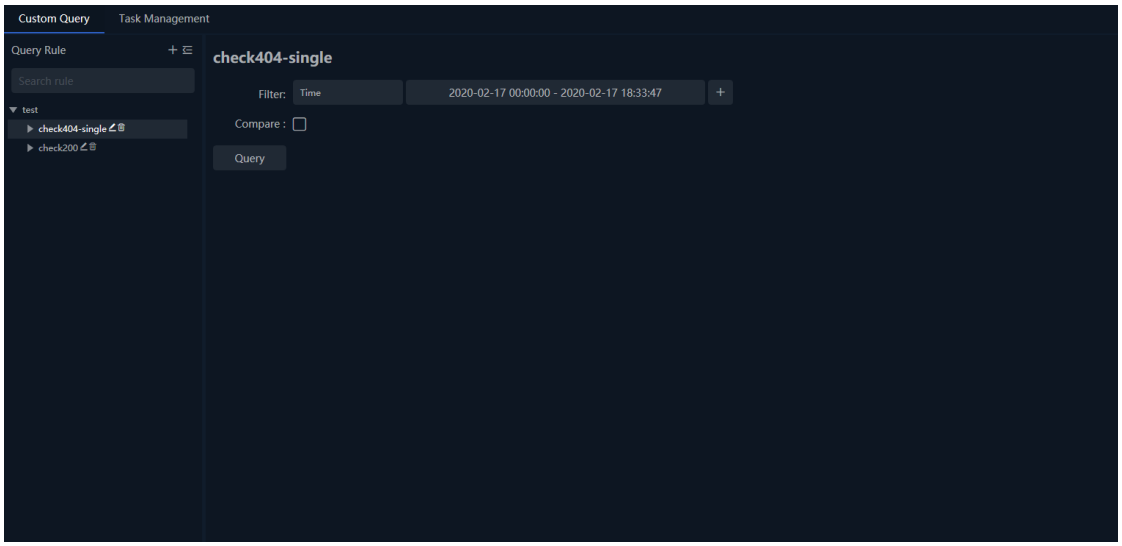
According to the needs of analysis, the system flexibly defines the query rules based on the configured business fields and trading metrics, and outputs the query results. Multiple query rules can be defined, and users can save and export query results

Note

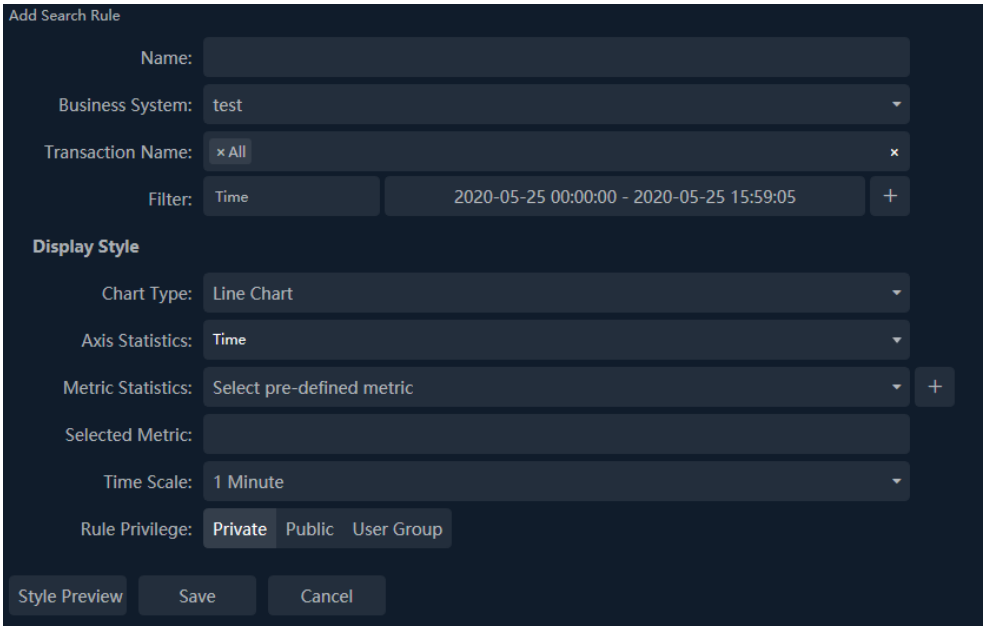
The system can only custom queries for transactions configured with business fields. All automatically identified transactions are processed as one type of transaction (transaction group).

8.3.1. Add a New Custom Query Rule

Click the menu Transaction Analysis -> Custom Querying to open the querying rule management interface. As the screenshot below:



Click the button “ + “ to open the Add Search Rule page, as the screenshot below:

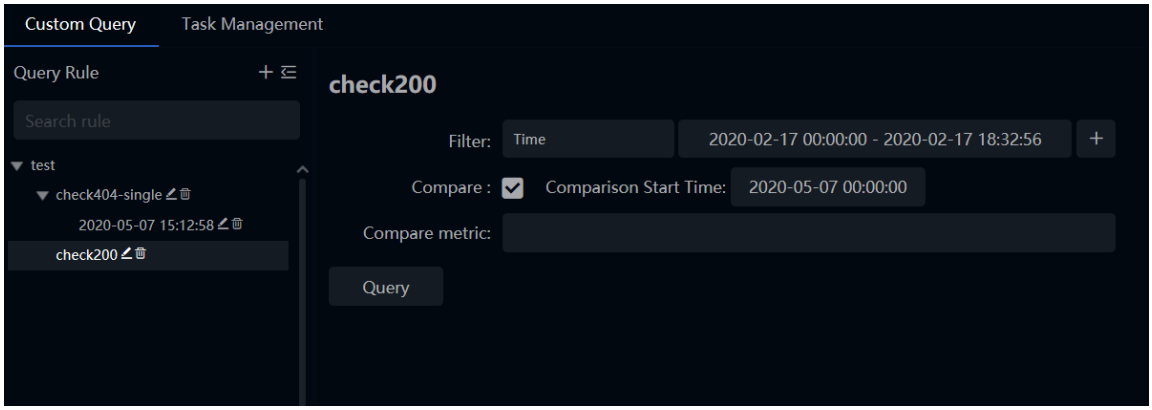


- Name: Doesn’t allow duplicate names
- Business System: Choose a business system
- Transaction Name: Choose transaction names
- Filter: One or more filters can be added, where "transaction time" is the required filter. A filter is an enabled state field in the business field configuration of the selected transaction name. When multiple transaction names are selected, the filter is the intersection of business fields in multiple transactions.
- Chart Type: Broken line chart, area chart, bar chart, pie chart, statistical table and detail table. When selecting bar chart, pie chart and statistical table, need to set the Top number and sort fields When selecting detail table, no need to set other fields.
- Axis Statistics: User can select multiple field dimension for statistics when the table typed selected while only one filed can be selected when other chart types selected.
- Metric Statistics: Selected transaction metrics.
- Time Scale: Only valid when the time dimension selected.

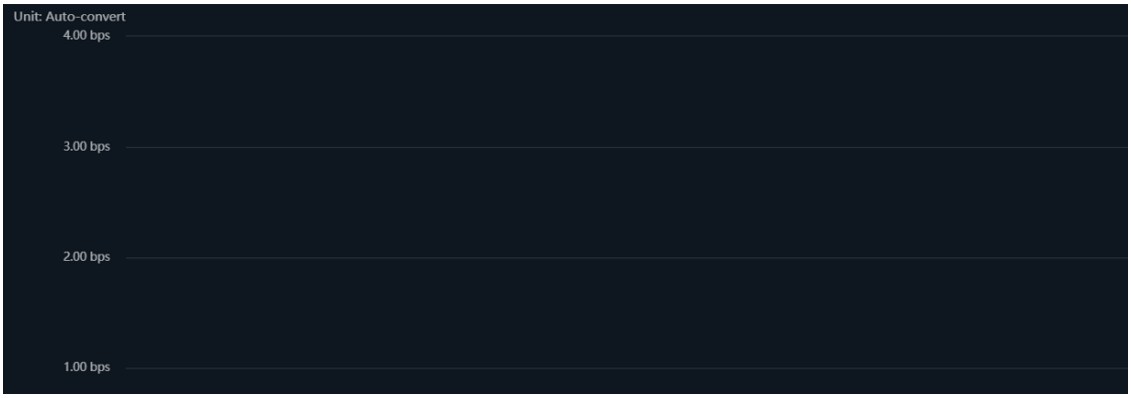
- After entering the rule, users can click the button “ Style Preview “ to view the result. The preview data is data randomly generated by the system instead of real one.
- Click the button “ Save “ to finish search rule adding.

8.3.2. Perform Query Rule

Select the query rule to perform, as the screenshot below:



- Click the button " + " to add more criteria for screening.
- Check the option " Compare : ☐ " to compare the data of different time ranges and show the comparison period data and growth rate.
- Click the button " Query " to start performing the query rule and the results will displayed on the page after finishing performing. As the screenshot below:



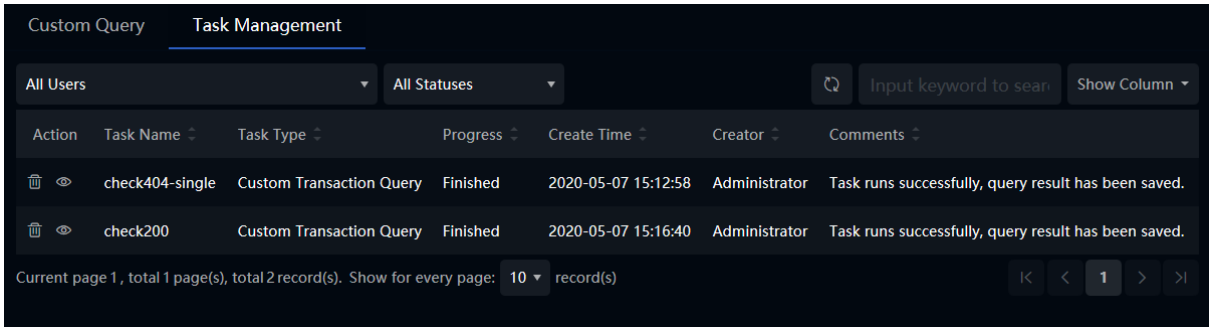
Note

A comparison query cannot be performed in the following cases

- Chart type is statistical table, bar chart or bar chart. And statistical maintenance is time type.
- Chart type is detail table or pie chart.

8.3.3. Task Management

When the query execution time exceeds 120 seconds or the query time range exceeds 1 day, the system will prompt whether to create the query task. After the query task is generated, even if the page is closed, the system still executes the query rules in the background until the query results are generated and automatically saved.



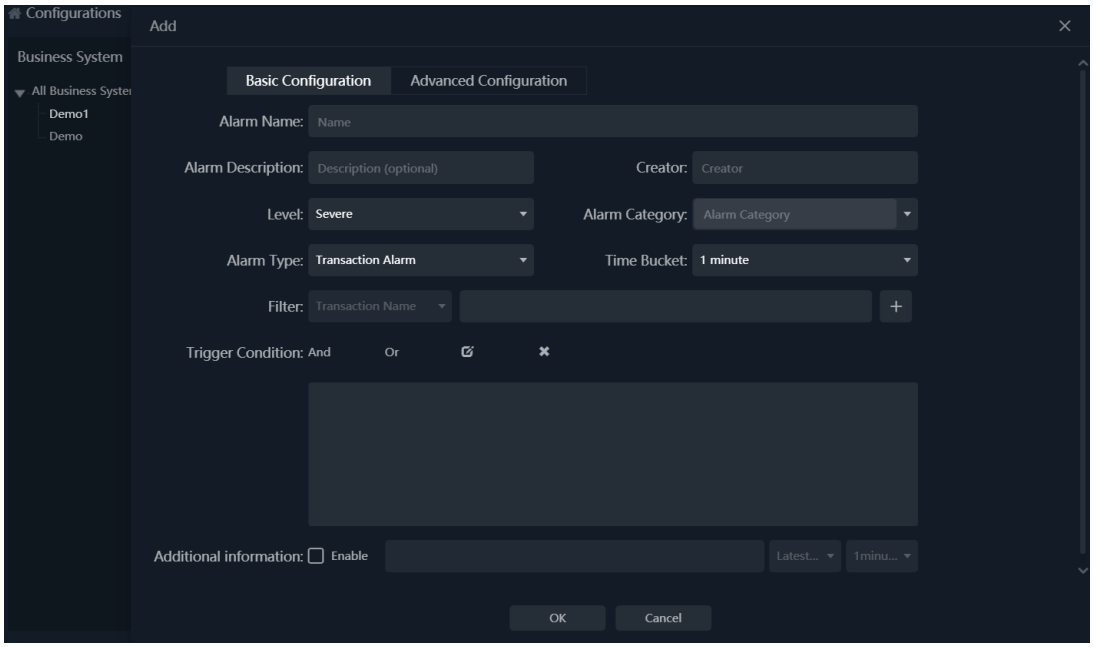
Note

The query task being executed can only be stopped, not paused. Stopped tasks can be restarted or deleted.

8.4. Transaction Alarm

Users can enter the transaction alarm configuration page via Configuration> Transaction Alarm Configuration.

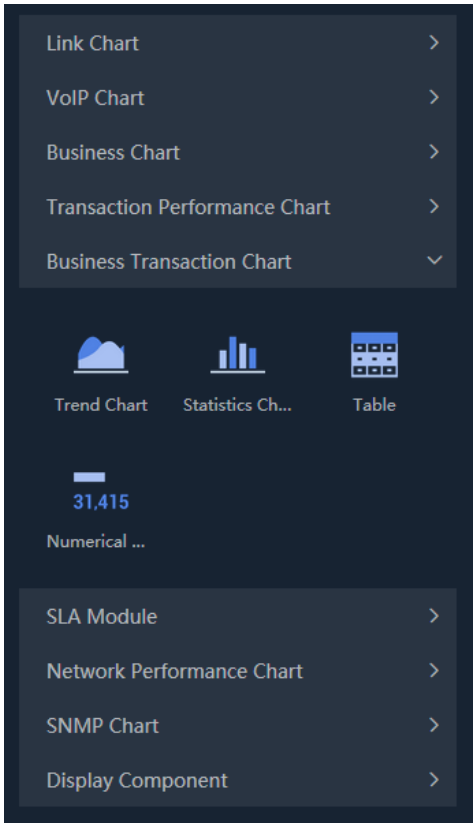
In the transaction alarm configuration, users can set an alarm for a single or multiple transactions, as shown in the following figure:



8.5. Transaction Report

The business report component is a report that produces a single business based on the business. Users can select an application analysis object for a business and select the diagram type.

Click the menu Report to enter into the report management interface and click the button " + " to add a new transaction report. As the screenshot below:



9. Network

9.1. Network Performance Monitoring

Network Performance Monitor is a customized monitor view. Users can customize multiple network nodes and network paths among the nodes to thereby monitor the communication among the nodes in real-time.

Click the menu Network Performance -> Network Performance Monitoring to open the Network Performance Monitoring page, which shows no data if no nodes or paths are defined.

9.1.1. Define Monitor View

- Users can delete, add, and edit the monitoring groups.
  - Group type: Both common type and VoIP type supports
  - Group permission type: Private, public, and user groups
  - Path width, path animation and font size in groups are configurable
- Click the button " Edit " to edit the view.
- In edit mode, users can click the button " " and set information of network nodes, network paths, bandwidth, congestion threshold and so on. Batch addition of intersegment relationships is supported.
- Users can add a single node or add batch nodes through the right-click menu.
- Users can set network evaluation alerts and network segment utilization alerts.
- Click the button "Change Background" to change the background.

9.1.2. Monitoring View

After adding network nodes and network paths, UPM system automatically evaluates each network path status. The evaluation results are listed as below:

- X: network interruption.
- Grey: no traffic.
- Green: there is traffic and the network performance is good.
- Red: there is traffic and the network performance is bad.
- Orange: there is traffic and the network performance is not good.

Users can select one network path and right-click to open the Path Analysis page.

9.2. Network Performance Analysis

In the Network Performance Analysis, traffic occupancy, comparative analysis and trend analysis are carried out according to the grouping of network segments.

Click the menu Network Performance -> Network Performance Analysis to open the network performance analysis page.

9.2.1. Group

There is only one default group for system. The hierarchical relationship is: monitoring group -> network segment -> probe. Users can click the button "  " to add a new group.

Note

The path scope of the custom group setting is the inter-segment relationship of monitoring groups.

A network segment relationship can only belong to one group.

9.2.2. Ratio Analysis

- Users can click the button "  " to set metric groups.
- Users can view metric trend graph and switching metric group and graph type are supported.
- Users can view the top table data of different network objects, and the display of list, pie chart and bar chart are supported.
- Users can click the button "  " to do trend analysis of the data.
- Users can click the button "  " to perform drilldown analysis.

9.2.3. Comparison Analysis

Comparison analysis refers to the comparative analysis of the same metric at different time points.

9.2.4. Trend Prediction Analysis

Trend prediction analysis simulates the running trend of the metric at the specified time point in the future, and provides a reference for the expansion or planning of the user network.

- Click the button "  " to set the trend prediction conditions and begin predict.
- Trend analysis supports daily and weekly analysis, and the system defaults to daily analysis.
    - Trend analysis by day: Users can select the data of the whole day or at a certain time as the historical data of trend analysis. According to certain algorithms, the system will use historical data to generate the trend graph of future specified time range (unit: day).
    - Trend analysis by week: Users can choose a day or a whole day of a week, or select a specific moment as the historical data of trend analysis. According to certain algorithms, the system will use historical data to generate the trend graph of the future specified time range (unit: week).

9.3. Network Path Analysis

Path analysis is to compare and analyze the data of different probes in the same network segment to find the network packet loss and network delay or VoIP intersegment Mos, packet loss and jitter issues.

- Through the "network performance monitoring" page, right click on the path and select "path analysis" from the pop-up menu to enter the network path analysis page.
- Users can set the time range: the default time range of the system is consistent with the

network performance monitoring interface, and users can customize it.

- Users can view the network device information in the communication path.
- Users can view the default indicator trend chart of the system, and check the probe object to be viewed.
    - Select the network packet loss metric, and the metric trend chart shows four metric trend charts by default: retransmission rate, bit rate, segmented loss rate and packet number.
    - Select the network delay, and the indicator trend graph shows four indicator trend graphs by default, namely, RTT of the three-shake client, RTT of the three-shake server, ACK delay of the client and ACK delay of the server.
    - Select the Mos metric, and the metric trend chart shows by default four metric trend charts, namely, uplink average video Mos, downlink average video Mos, average video Mos and code rate.
    - Select the metric of packet loss rate, and the metric trend chart shows four metric trend charts by default: uplink media packet loss rate, downward media packet loss rate, average media packet loss rate and code rate.
    - Select the metric of packet loss rate, and the metric trend chart shows four metric trend charts by default, namely, uprating average dithering, descending average dithering, average dithering and code rate.

9.4. Network Performance Alarm

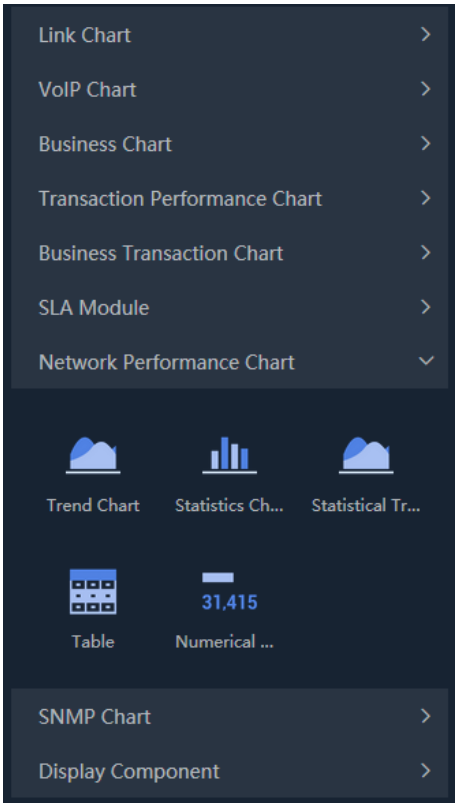
Network performance alarm management provides unified management of all network triggered alarms within a certain period of time. In network performance alarms, users can view all the alerts that have been triggered by the system during the week.

- Click the menu Network Performance ->Network Performance Alarm to open the Network Performance Alarm page.
- Click the button “  “ to record the alarm. When the same alarm is triggered later, users can view the previous log for quick troubleshooting.
- Click the button “  “ to view the previous log for quick troubleshooting.
- Click the button “  “ to jump to the data download page for data download.

9.5. Network Performance Report

Users can select network segment relationships in a network performance monitoring group as analysis objects and select chart types.

- Click the menu Report to open the report management page. Click the button “  “ to add a new report, as the screenshot below:



- After adding the chart, users can view the report presentation effect. At this point, the report graph is simulated data, not real data.
- Click the button " Preview " to preview the real data in the chart.
- After completing the settings, click the button " OK " to save settings.
    - Report format: PDF, WORD, EXCEL and HTML, and users can choose one of them.
    - Report type: optional daily report, weekly report, monthly report and report generation time.
    - Business period: support the setting of business period, with the minimum accuracy to minutes for daily report, 10 minutes for weekly report and hours for monthly report.
    - Comparison: support comparison with the previous period, the same period of last year, the same period of last week and the designated date when selecting the daily newspaper; When selecting a weekly report, support comparison with the previous period and the specified date; When selecting a monthly report, support comparisons with the previous cycle, the same period last year, and the specified date.
    - Receiving mailbox: the receiving mailbox of the report. After filling in the email address, the system will regularly send the report to the designated mailbox.

Note

The SMTP server is configured correctly before the report can be sent successfully.

- In the report list page, users can also click the name of a report to enter the report log interface and view the historical reports generated by the report.

9.6. Network Topology Monitoring

Network topology monitoring is provided by UPM center to monitor the whole network topology diagram from the network perspective.

- Click the menu Network Performance -> Network Topology Monitoring to open the network monitoring page.
- Click the button " Edit " to enter the editing state. Users can configure monitoring objects and network devices.
- The system provides the monitoring with six types objects, link, segment, business, application, host and client.
    - Link type: ordinary link, aggregate link, sub-link, and virtual connector link.
    - Network segment: the network segment under the link.
    - Business: summary of main probe data of each application under business.
    - Application: application on a certain probe under business.
    - Host: the host applied on a probe under business.
    - Client: client applied on a probe under business.
- Equipment monitoring supports setting monitoring cycle and monitoring frequency, and the monitoring page will display indicator information and alarm information.
- Right-click the line and click the line metric option. The feature supports five metrics, application metric, application segment-segment metric, segment metric, link metric and link segment-segment metric.
    - Application metric: summary of probe data of each application under business.
    - Intersegment metric: mean value of data between applied probes.
    - Network segment metric: network segment data under probe.
    - Link metric: probe metric data.
    - Link intersegment metric: mean value of data between probes of each network segment.
- Users can set the jump view of devices and wires. Click Edit Settings option from the right menu of the device, or click Jump View option from the right menu of the line.

9.7. Network Topology Alarm

The network topology alarm management provides unified management of the alarms triggered within a certain period of time. In network performance alarms, users can view all the alerts that have been triggered by the system during the week.

- Click the menu Network Performance ->Network Topology Alarm to open the Network Performance Alarm page.
- Users can view the alarm level distribution diagram, alarm statistics diagram and alarm list.
- Click the button "" to acknowledge the alarms. After acknowledging alarms, the system will automatically generate a log for this alarm. When the same alarm is triggered later, users can look at the previous log for quick troubleshooting.
- Click the button "  " to view the previous log for quick troubleshooting.
- Click the button "  " to jump to the data download page for data download

10. Device

Users can refer to the document *SNMP-Based Device Performance Analysis Manual*.

10.1. Device Performance Analysis

Device Performance Analysis is a data analysis function based on SNMP data source provided by UPM Center.

- Click the menu Network Performance> Device Performance Analysis to open the device performance analysis page.
- Users can view the summary information of the devices under the Group Tree, or click the button to query the device indicator trend chart and the related netflow data.
- Users can view the summary information of the interfaces under the device, or click the button to query the interface indicator trend chart and the related netflow data.
- Users can add aggregate interface objects to perform aggregation analysis.

10.2. SNMP Custom Monitoring

Users can customize the monitoring settings according to their needs.

- Click the menu Custom Monitoring -> Custom Metrics Monitoring to open the Custom Metrics Monitoring page. Click the button “  “ to displays the left sidebar for adding monitoring charts.
- Users can add a chart by selecting the objects and chart types under the SNMP chart.

10.3. SNMP Report

SNMP component supports report configuration for devices and interfaces.

Click the menu Report to enter into the Custom Report interface, click the button “  “ and select SNMP Chart to add a new SNMP report.

11. Link

11.1. Link Custom Analysis

Custom Metrics is one of the custom monitoring views provided by the UPM center. In the Custom Metrics, users can select different chart of link, application, transaction performance, transaction, etc. And put them in one interface so that users are able to view the charts they care about.

- Click the menu Custom Monitoring -> Custom Metrics Monitoring to open the Custom Metrics Monitoring page. Click the button "  " to displays the left sidebar for adding monitoring charts.
- Users can add a chart by selecting the objects and chart types under the link chart.

11.2. VoIP Custom Analysis

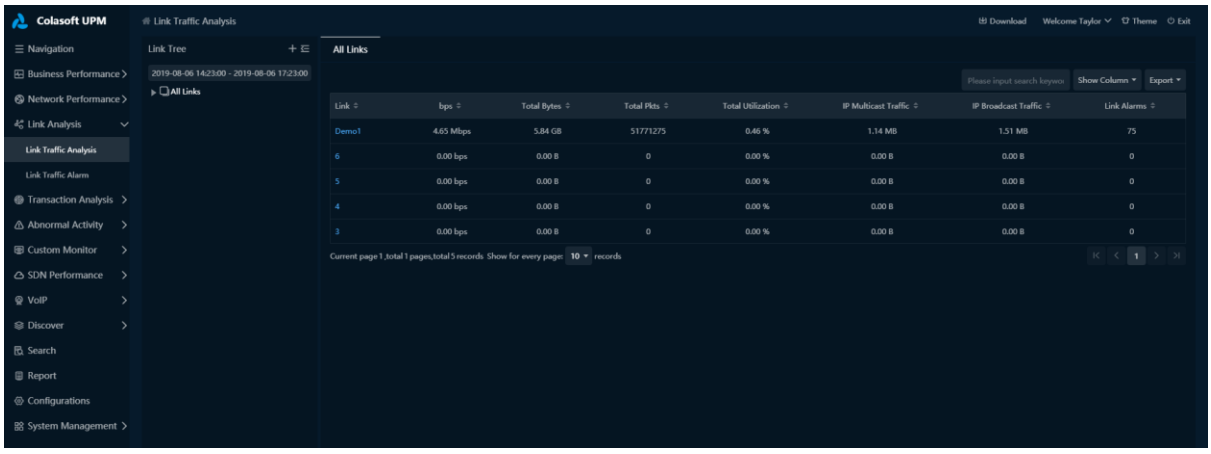
Users can customize the monitoring settings according to their needs.

- Click the menu Custom Monitoring -> Custom Metrics Monitoring to open the Custom Metrics Monitoring page. Click the button "  " to displays the left sidebar for adding monitoring charts.
- Users can add a chart by selecting the objects and chart types under the VoIP chart.

11.3. Link Traffic Analysis

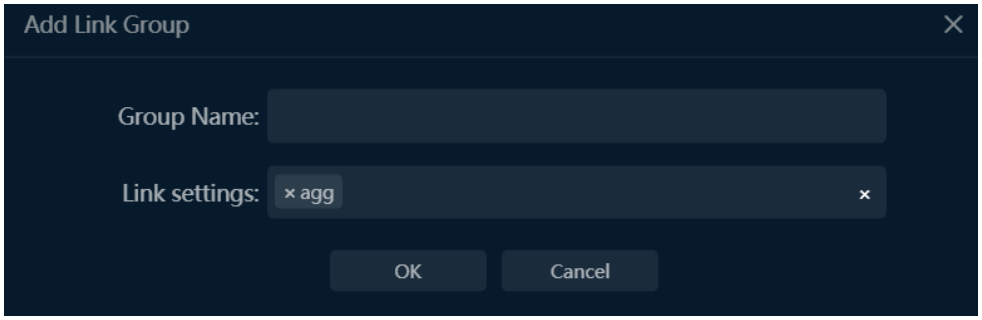
In the traffic analysis page, the traffic occupancy analysis, baseline analysis, comparative analysis and trend analysis of probes and their sub-probes are conducted according to the grouping of probes.

Click the menu Link Analysis -> Link Traffic Analysis to open the Link Traffic Analysis page.



11.3.1. Group

There is only one default group for system, and users can click the button "  " to add a new group, as the following screenshot:



11.3.2. Ratio Analysis

- Users can click the button "  " to set metric groups.
- Users can view metric trend graph and switching metric group and graph type are supported.
- Users can view the top table data of different network objects, and the display of list, pie chart and bar chart are supported.
- Users can click the button "  " to do trend analysis of the data.
- Users can click the button "  " to analyze data in a new window.

11.3.3. Comparison Analysis

Comparison analysis refers to the comparative analysis of the same metric at different time points.

Users can check 

, select Day on Day, Last Week YoY, Last Month YoY or Custom for comparative analysis.

Tips:

Day on Day: Compare the data over the same time range yesterday.

Last Week YoY: Compare the data over the same time range last week.

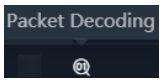
Last Month YoY: Compare the data over the same time range last month.

11.3.4. Trend Prediction Analysis

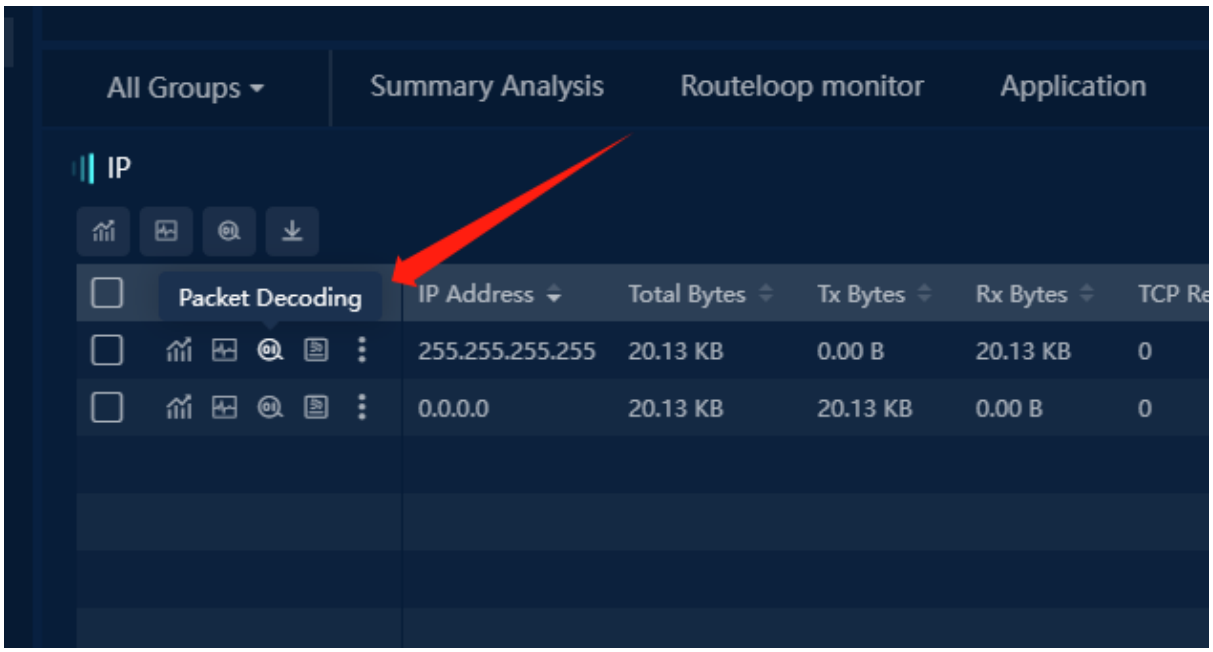
Trend prediction analysis simulates the running trend of the metric at the specified time point in the future, and provides a reference for the expansion or planning of the user network.

- Click the button "  " to set the trend prediction conditions and begin predict.
- Trend analysis supports daily and weekly analysis, and the system defaults to daily analysis.
    - Trend analysis by day: Users can select the data of the whole day or at a certain time as the historical data of trend analysis. According to certain algorithms, the system will use historical data to generate the trend graph of future specified time range (unit: day).
    - Trend analysis by week: Users can choose a day or a whole day of a week, or select a specific moment as the historical data of trend analysis. According to certain algorithms, the system will use historical data to generate the trend graph of the future specified time range (unit: week).

11.3.5. Packets Decoding

In the process of link analysis, click the button “ 

” to view the decoding information of analysis object's packet online.

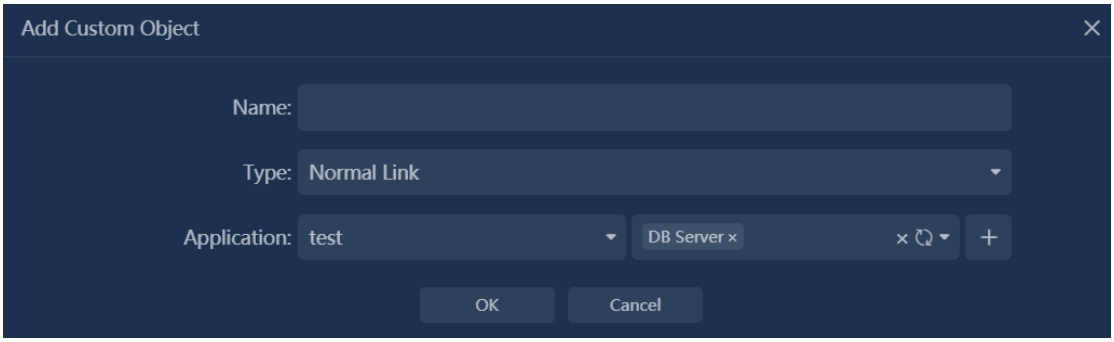


11.4. Application Object Analysis

Application Object Analysis supports custom application combinations for traffic analysis, baseline analysis, comparative analysis and trend analysis.

11.4.1. Customize Application Object

- Click the button “  ” to customize application object. As the screenshot below,



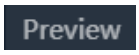
11.5. Link Traffic Alarm

Link traffic alarm management provides unified management of all network triggered alarms within a certain period of time. In link traffic alarm, users can view all the alerts that have been triggered by the system during the week.

- Click the menu Link Analysis -> Link Traffic Alarm to open the Link Traffic Alarm page.
- Users can view the alarm level distribution diagram, alarm statistics diagram and alarm list.
- Click the button "  " to acknowledge the alarms. After acknowledging alarms, the system will automatically generate a log for this alarm. When the same alarm is triggered later, users can look at the previous log for quick troubleshooting.
- Click the button "  " to view the previous log for quick troubleshooting.
- Click the button "  " to jump to the data download page for data download.

11.6. Link Report

Link components are link-based reports that generate reports based on normal links, aggregate links and sublinks. Users can select the analysis object for a link and select the chart type.

- Click the menu Report to enter into the report management interface and click the button "  " to add a new link chart.
- Click the button " 

" to preview the real chart.
- After completing the settings, click the button " 

" to save settings.
    - Report format: PDF, WORD, EXCEL and HTML, and users can choose one of them.
    - Report type: optional daily report, weekly report, monthly report and report generation time.
    - Business period: support the setting of business period, with the minimum accuracy to minutes for daily report, 10 minutes for weekly report and hours for monthly report.
    - Comparison: support comparison with the previous period, the same period of last year, the same period of last week and the designated date when selecting the daily newspaper; When selecting a weekly report, support comparison with the previous period and the specified date; When selecting a monthly report, support comparisons with the previous cycle, the same period last year, and the specified date.
    - Receiving mailbox: the receiving mailbox of the report. After filling in the email address, the system will regularly send the report to the designated mailbox.
- In the report list page, users can also click the name of a report to enter the report log interface and view the historical reports generated by the report.

11.7. VoIP Report

VoIP components support the configuration of reports for profiles, terminals, terminal conversations, conversations, segments and inter-segments. Report configurations can refer to 9.5 link report.

12. Search and Download

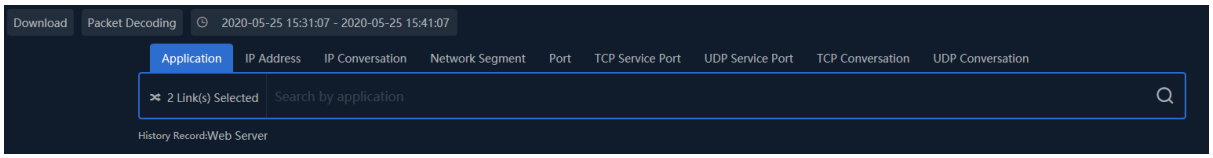
UPM provides packet search and packet download function. Packet search is supported by application, IP address, IP session, network segment, port, TCP service port, UDP service port, TCP session, and UDP session as the entry point for searching, and packet downloading, in-depth analysis, relationship combing and trend analysis are also supported for searching results.

12.1. Download packets

Search Packets allows user to use the application, IP address, IP session, network segment, port, TCP service port, UDP service port, TCP session, and UDP session as the entry, to search and download the packet.

Click the menu Search to open the Search Packets page, as the screenshot below:

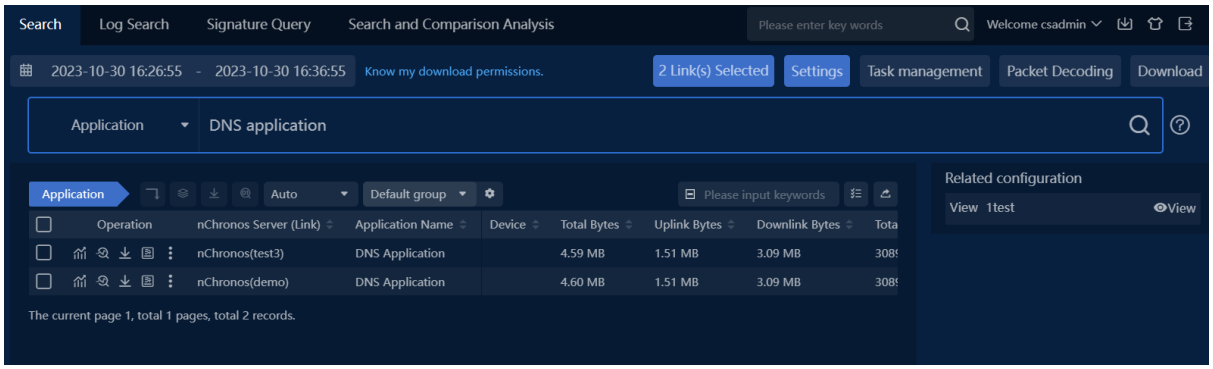
12.2. Search Packets



Enter the keywords for search and then click the button "  ", the system will automatically search the communication data that matches the keyword.

12.2.1. Search and drill down

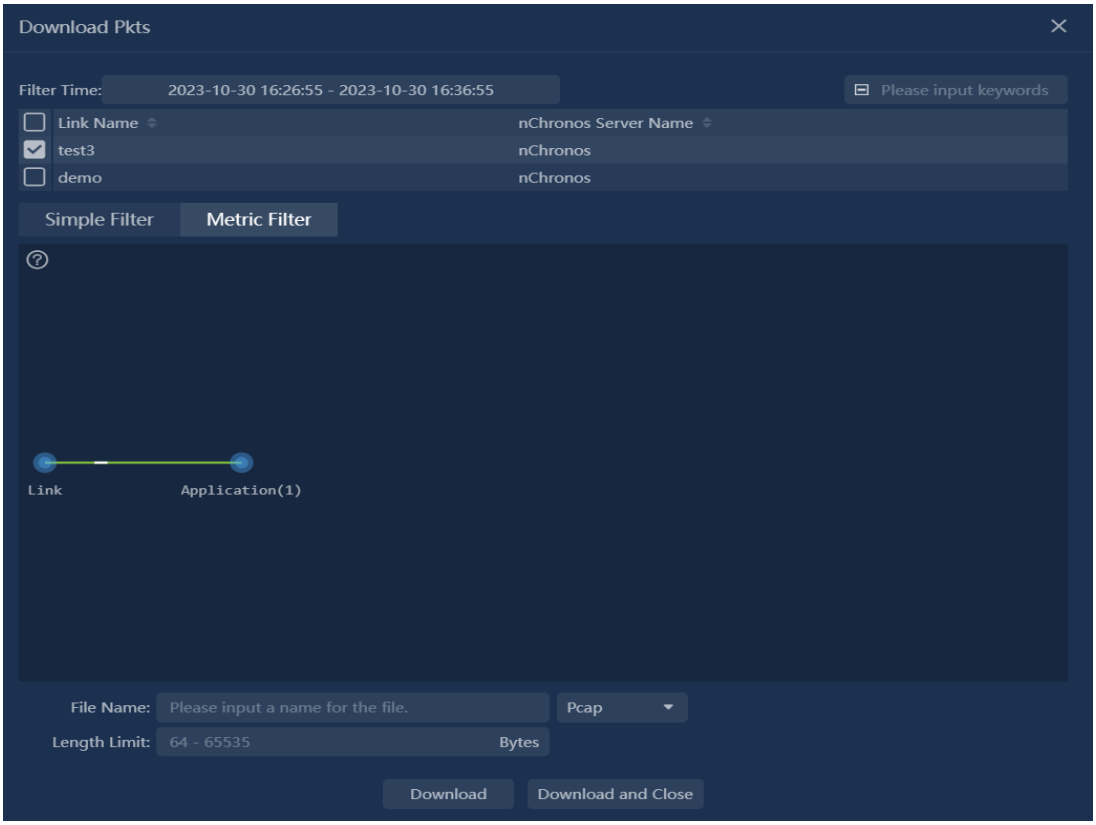
The retrieval result list is shown in the figure below:



In the retrieval result list, select at least one record, select the drill-down target object, and the system will automatically retrieve the drill-down data. Each entrance supports drill-down: application, IP session, TCP session, UDP session, client, server.

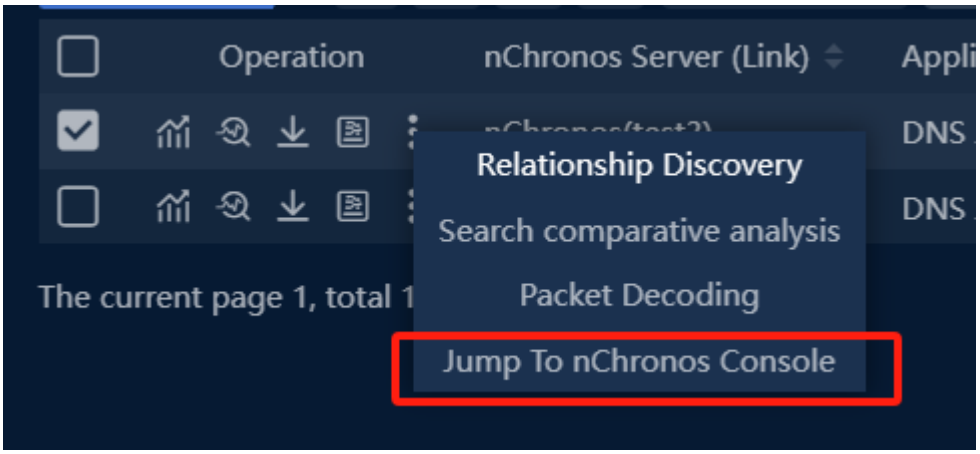
12.3. Packet Download

Support Simple Filtering and Advanced Filtering to download packets, click or button, pop up the "Packet Download" window, simple filtering as shown in the figure below :



12.4. Deep analysis

Click the button to call up the nChronos console for deep analysis.

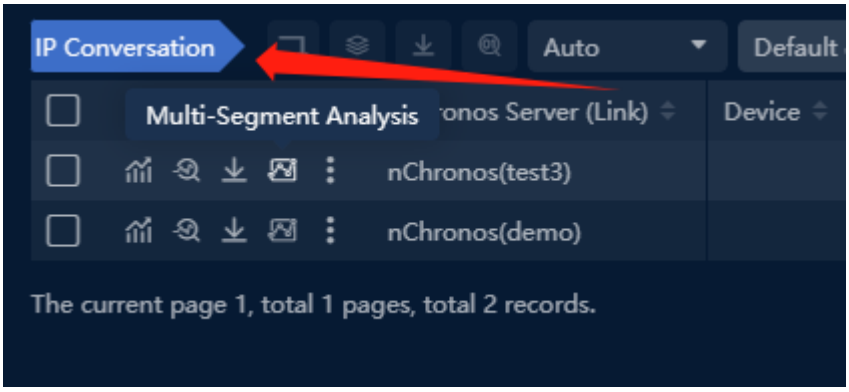


12.5. Relationship Discover

Support retrieving object IP address relationship analysis, click or button, pop up the "Relationship Discover" window, as shown in the figure below :

12.6. Multi-segment analysis

In the retrieved IP session, click on the 'Multi-segment Analysis' icon before the IP session to enter the multi-segment analysis page of the IP session, as shown in the figure below:



In the TCP conversation or UDP conversation view at the bottom of the page, select the TCP conversation or UDP conversation to directly enter the multi-segment analysis page of the selected session. In the multi-segment analysis page, you can view the packet loss situation of the data packets in the session through each probe.

12.7. Trend analysis

Click the button to open the 'Trend Analysis' window.

13. System Management

13.1. User Group Management

User group management, which represents a collection of users with the same functionality, is provided. The user group consists of five roles, administrator, creator, user, auditor and renter.

- Click the menu System Management -> User Group Management to access the page.
- Users can configure four roles.
  - Administrator: has all UPM permissions.
  - Configurator: can configure business and do downloading on the links.
  - Regular user: can configure the home page and do monitoring, analyzing, configuring alarms, configuring reports and downloading on the businesses, links and transactions.
  - Auditor: can configure audits.
  - Renter: can configure the home page and do monitoring, analyzing, configuring alarms, configuring reports and downloading on the businesses, links and transactions.

Note

- To delete the user group, users need to remove all associated users in the user group before deleting the user group.
- Once the user's roles in the user group is set, not allow to modify.
- The renter role is usually used in conjunction with renter link.

13.2. User Account

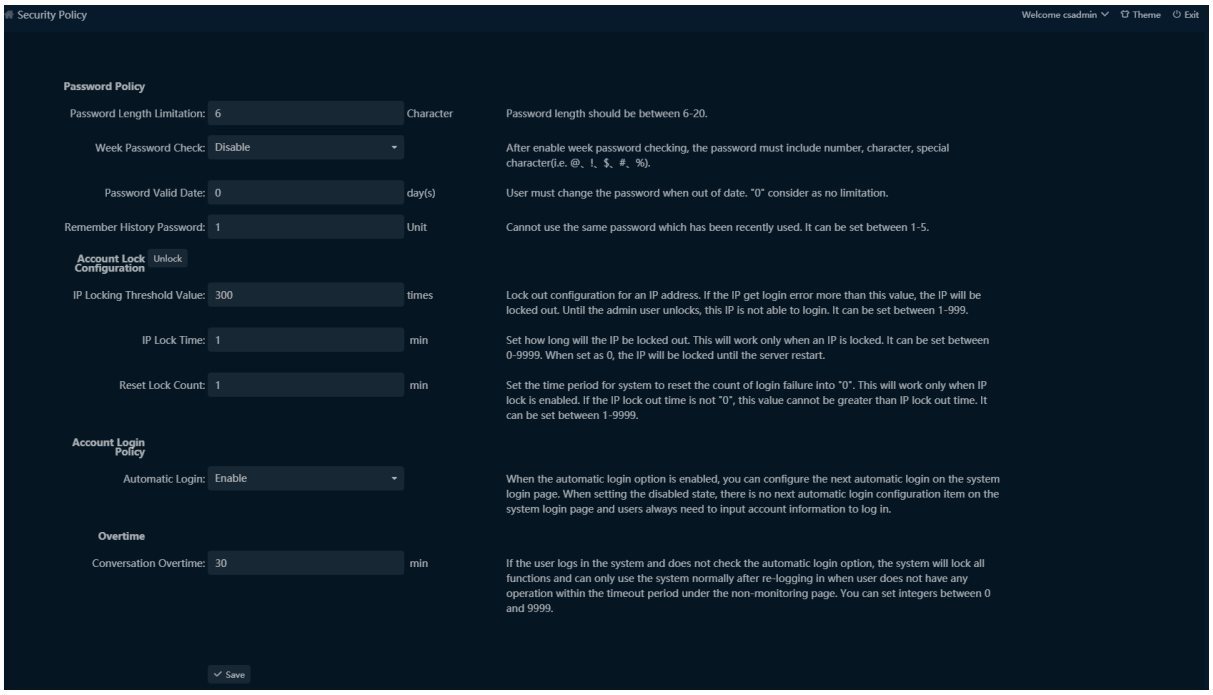
User management includes two tabs, user management and authentication configuration. User management carries out unified maintenance for system users. In Authentication configuration, users can configure Radius and LDAP server information.

- Administrator users can access through System Administration -> User Account.
- Users can add, modify and delete users, as well as can view the login time, login IP, login counts.

13.3. Security Policy

Click the menu System Management > Security Policy to open the security policy page.

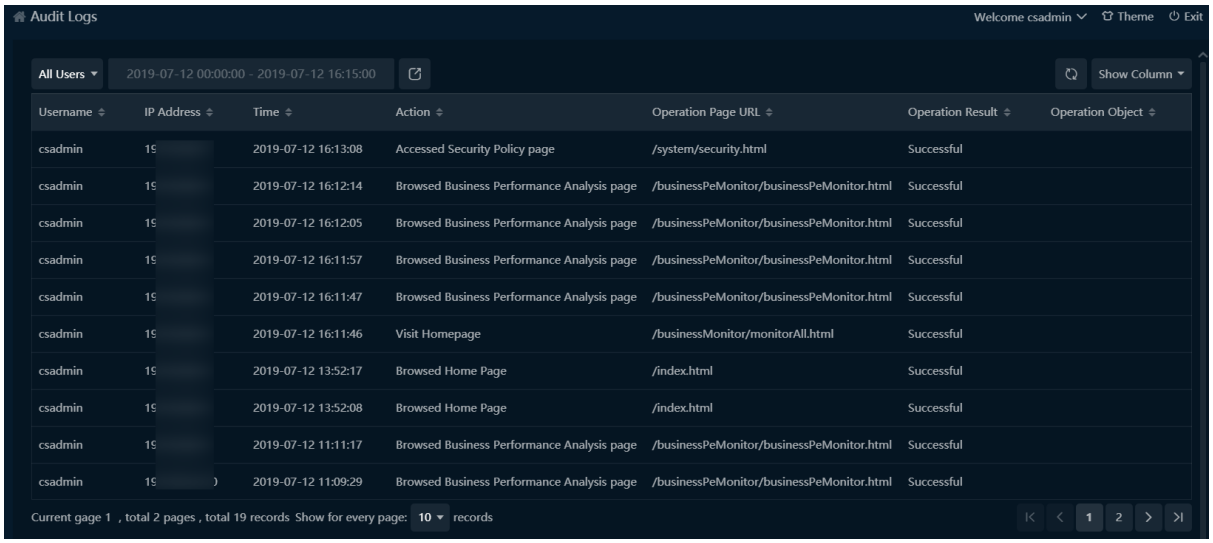
The security policy page is used to configure the password policy, account lock policy (including account unlock) and overtime policy.



13.4. Audit Logs

Click the menu System Management -> Audit Logs to open the Audit Logs page.

The Audit Logs page lists detailed operation log information. Users can view the operation logs of a specific user in a specified time range, as the screenshot below:



Users can click the button “  ” to export the filtered logs.

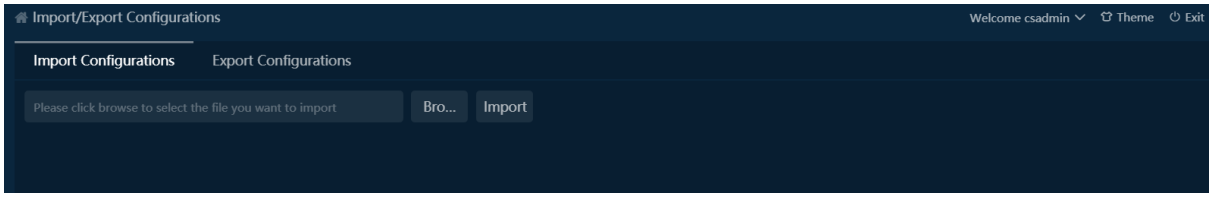
13.5. Import/Export Configurations

Click the menu System Management -> Import/Export Configurations to open the Import/Export Configurations page.

Users can export UPM configurations to local machine and import the configurations to UPM again.

13.5.1. Import Configurations

The Import Configurations page shows as the screenshot below:



To import configurations:

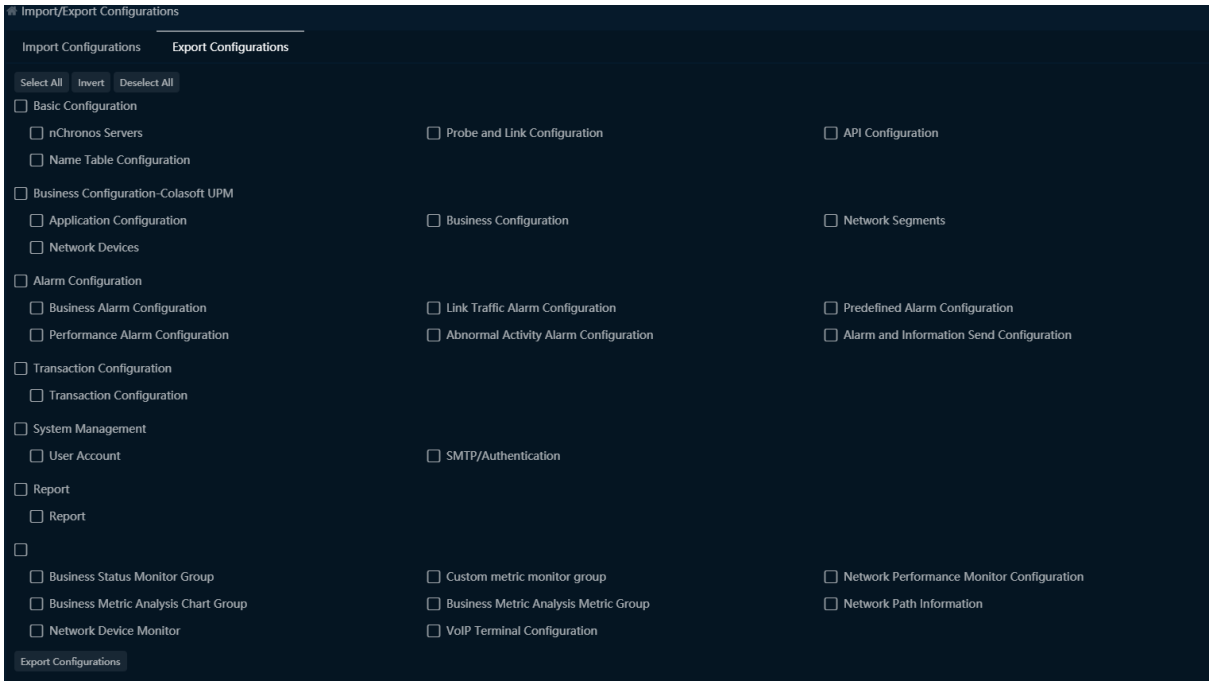
1. Select the file to be imported. For Google Chrome, users can drag the file to the box.
2. Click Start Uploading to upload it.
3. When the configurations conflict, users can choose to skip, overlap or cancel the import.

Note

Only file of UPM specific format (.csu) can be imported.

13.5.2. Export Configurations

The Export Configurations page shows as the screenshot below:



To export configurations, check the configurations to be exported and click the button Configurations Export.

Note

When exporting the configuration, the UPM center saves the configuration file in a specific format (.csu).

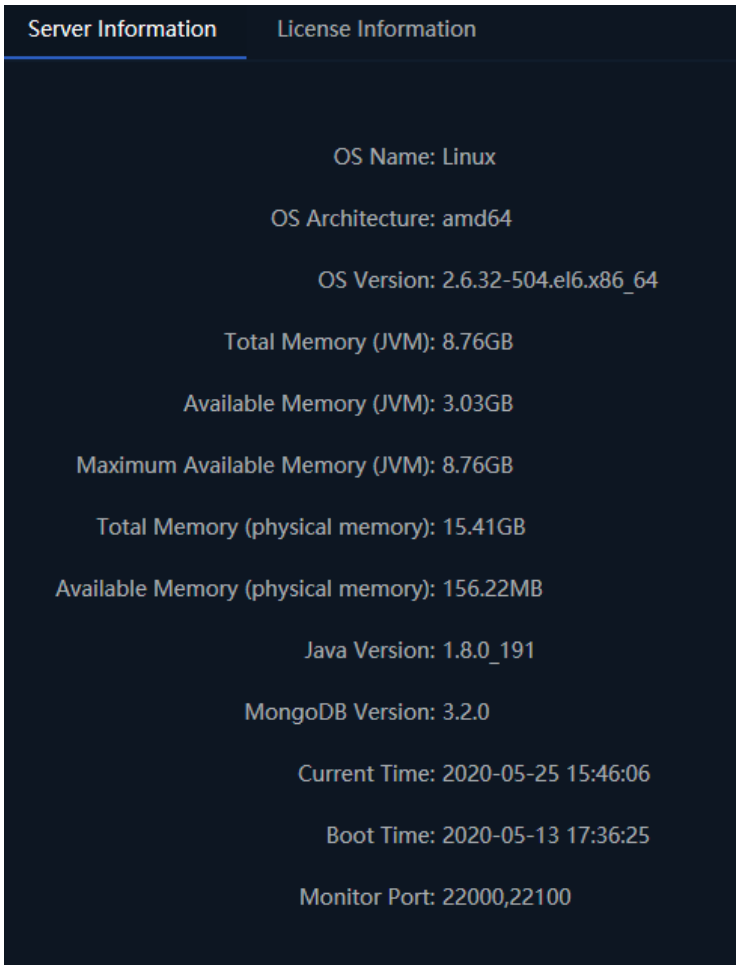
13.6. System Information

Click the menu System Management -> System Information to open the System Information page.

On the System Information page, users can check the license information and server information.

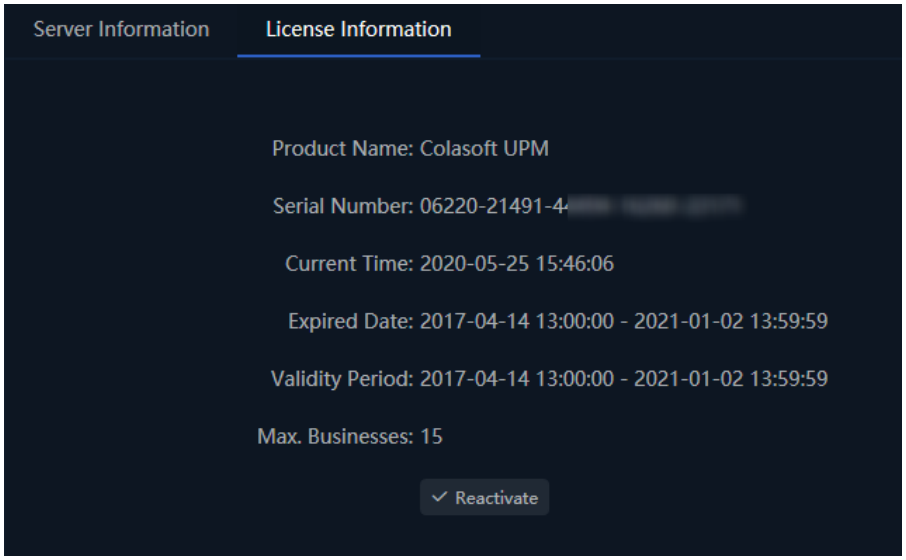
13.6.1. Server Information

On the server Information page, users can check the OS information, hard disk information and memory information, etc. as the screenshot below:



13.6.2. License Information

On the license Information page, users can check the license information, also can reactivate the product. As the screenshot below:



When the license changes, users can click the button Reactivate to renew the license.

13.7. Replace Certificate

Users can update digital certificates and socket certificates.

14. Scenario Center User Manual

14.1. Scenario Center Management

14.1.1. Functional background

1. Existing modules such as network performance monitoring, network topology monitoring, custom metric monitoring, scenario monitoring, scenario analysis, terminal monitoring, global business performance monitoring, and abnormal behavior monitoring are partial data views in the overall scenario from a business perspective. They are displayed as core modules on the product homepage, making the product 'bulky' and interfering with users' understanding of the product's functionality.

2. Users need to build monitoring views to visually and clearly present complex data, quickly understand the essence of the data behind complex business, help them and managers discover problems in a timely manner, and guide relevant decisions. However, when users create a large number of views (dozens or even hundreds), managing and building monitoring views with the existing module functions of the product is inefficient and difficult to conveniently and quickly locate the monitoring views.

14.1.2. Functional value

1. Reduce the number of modules on the product homepage and abstractly integrate and manage the reduced modules to make the product visually cleaner and easier to use.

2. Support previewing the actual content of templates, support built-in scene view covers or custom scene view thumbnails, making it easier to identify scene views and scene template content.

3. Support batch management of displayed scene views and batch settings for edited scene views, facilitating quick management and editing of scene views and scene templates.

4. The original product homepage had 17 primary modules, which have been reduced to 12, a reduction of 5. The 56 secondary module menus have been reduced to 35, a reduction of 21.

5. Enhanced and highlighted the product's proactive, intelligent, and efficient operation and maintenance monitoring capabilities for business-oriented scenarios. Manage various scene

views and scene templates in a one-stop and convenient manner through the [Scene Center].

14.1.3. Functional Terminology

Scene Center: A workstation for managing various visual scene views or scene templates.

14.1.4. Functional description

In the UPM 6.4.0 version, the [Scene Center] primary module is added, which aggregates the original functional modules and views such as network performance monitoring, network topology monitoring, custom metric monitoring, global business performance monitoring, backup terminal, application terminals, VoIP terminals, transaction terminals, abnormal behavior monitoring, scene analysis, and customized scene monitoring. Overall, the original product's 17 primary menus on the homepage have been reduced to 12, a decrease of 5; The 56 secondary menus have been reduced to 35, a decrease of 21.

The scene center module is mainly divided into management and display of scene views, and management and display of scene template functions.

Manage and display scene views

1. Support adding, deleting, modifying, and querying scene views, as well as adding, deleting, modifying, and querying scene view label groups.

2. Support waterfall layout browsing mode, support batch management of displayed scene views, batch setting of edited scene views, and facilitate quick management and editing of views.

3. Support built-in scene view cover and custom scene view thumbnails.

Manage and display scene templates

1. Support adding, deleting, modifying, and querying scene templates, as well as adding, deleting, modifying, and querying scene template label groups.

2. Support previewing the actual content of scene templates, making it easier to identify scene view and scene template content.

14.1.5. Operation Guide

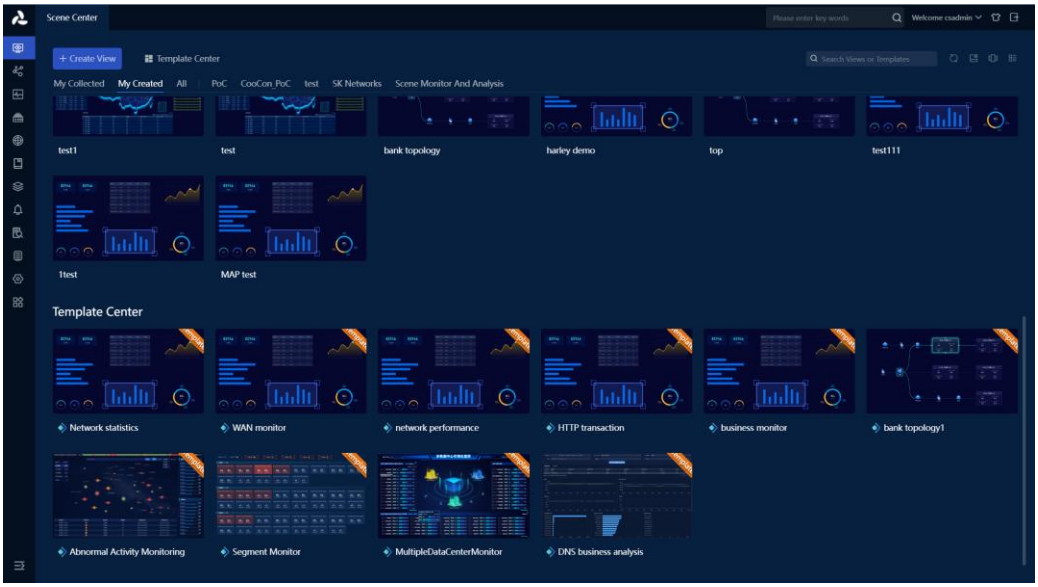
Add [Scenario Center] module in the left navigation of UPM. During initialization, built-in scenario views such as segment monitoring, DNS business analysis, route loop monitoring, IP address conflict, device performance monitoring, abnormal behavior monitoring, global business monitoring, and multi-data center visualization monitoring are provided. The template center includes scenario templates such as segment monitoring, DNS business analysis, abnormal behavior monitoring, and multi-data center visualization monitoring.

Create scenario view

[Scenario Center] provides the option to create a scenario view from scratch or using a scenario template.

1. Creating a scenario view from scratch

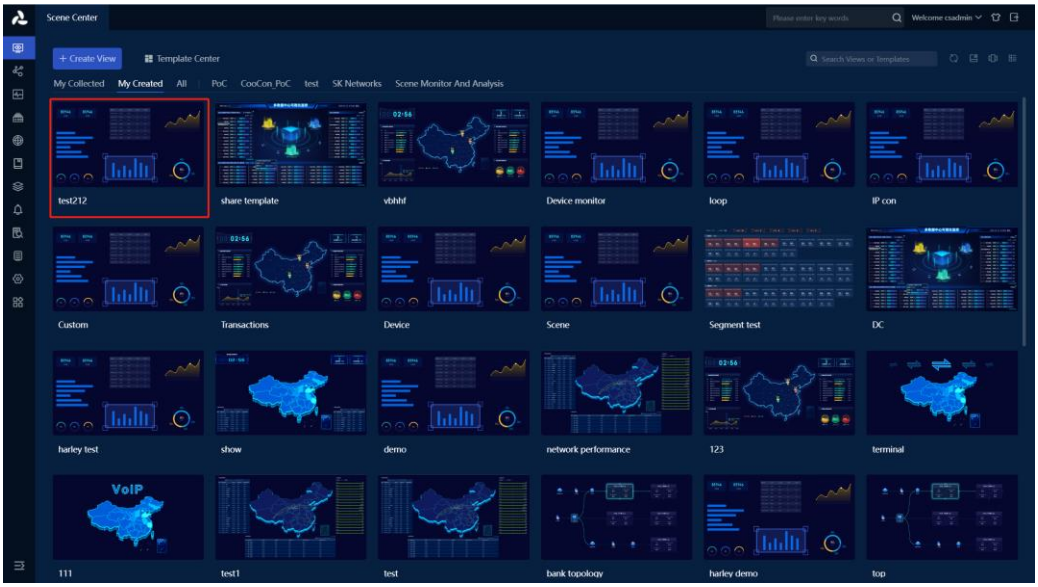
On the homepage of the Scenario Center, click [Create View] at the top left to open the Create View dialog box.



In the Create View dialog box, you can select types such as Custom, Network Performance Monitoring, Network Topology Monitoring, backup terminal, Application Terminals, VoIP Terminals, Transaction Terminals, etc. Enter the view name, view description, select view group, view permissions, and click [Create] to complete.

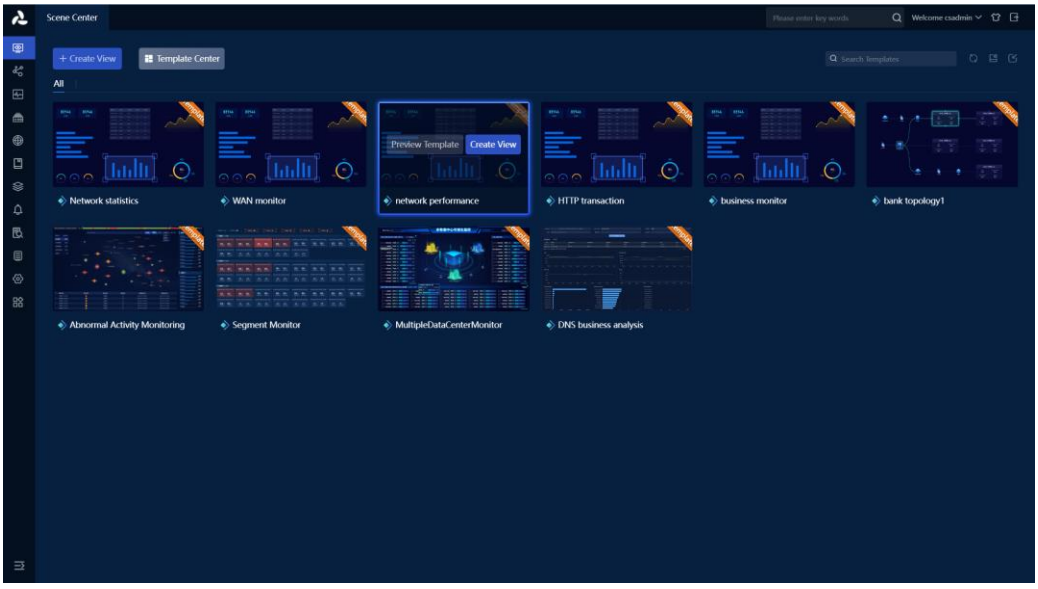
After clicking [Create], a new browser tab will open and enter the Edit View page state. You can drag components, bind data, and layout views (the function of building view content is consistent with history). After completion, click [Exit] to enter monitoring mode.

After creation, you can view the created scene view on the Scene Center homepage.

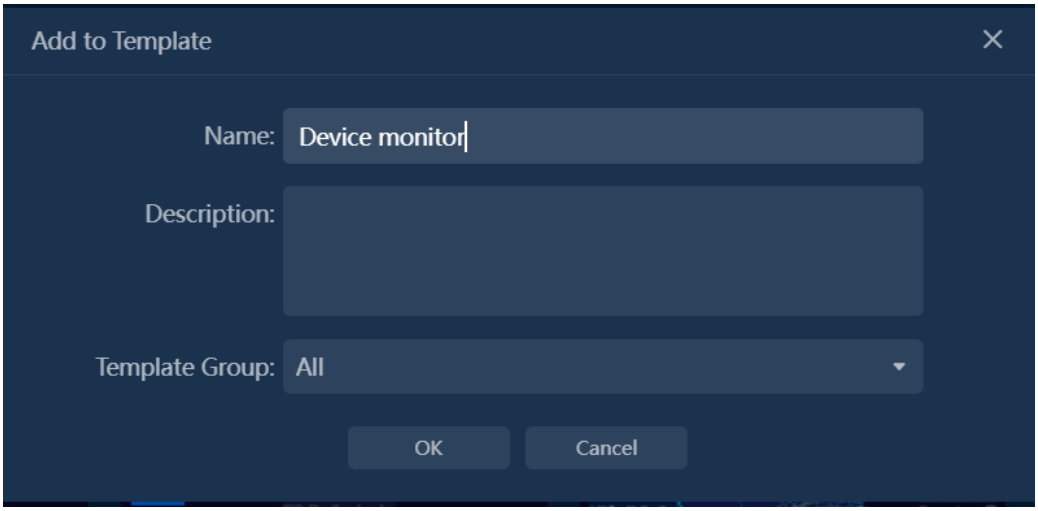


2. Create scene views using scene templates

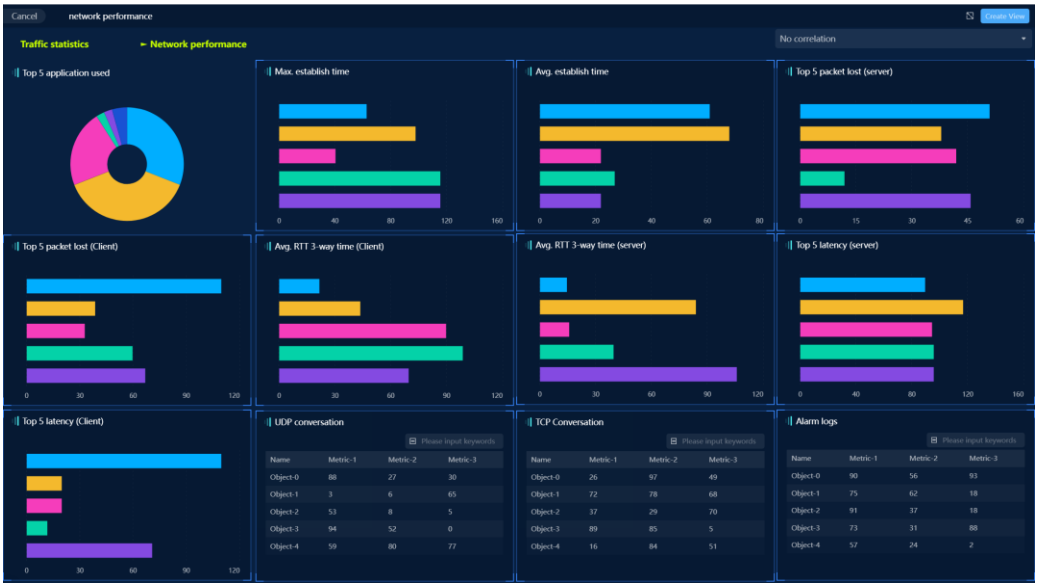
On the Scene Center homepage, scroll down to the Template Center area or click [Template Center] to view scene templates. Select the target scene template and click [Create View] to open the dialog box for creating xxxxxx as a view.



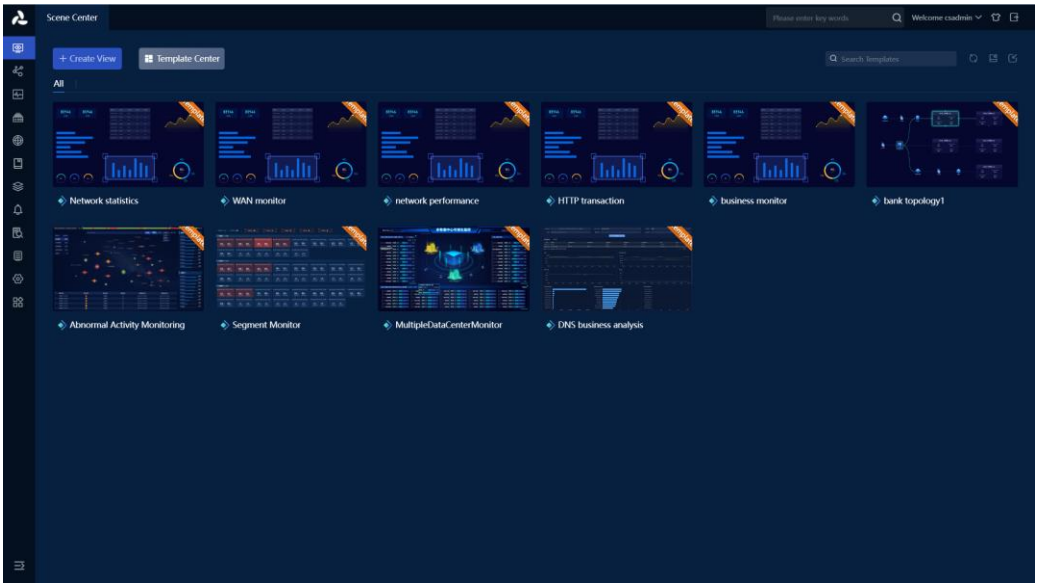
In the process of creating xxxxxx as a dialog box, enter the view name, view description, select the view group, view permissions, and click [OK] when finished.



After clicking [OK], a new browser tab will open and enter the edit view page state. You can modify or drag components, bind data, and layout views based on the existing content (the function of building view content is consistent with history). After completion, click [Exit] to enter monitoring mode.

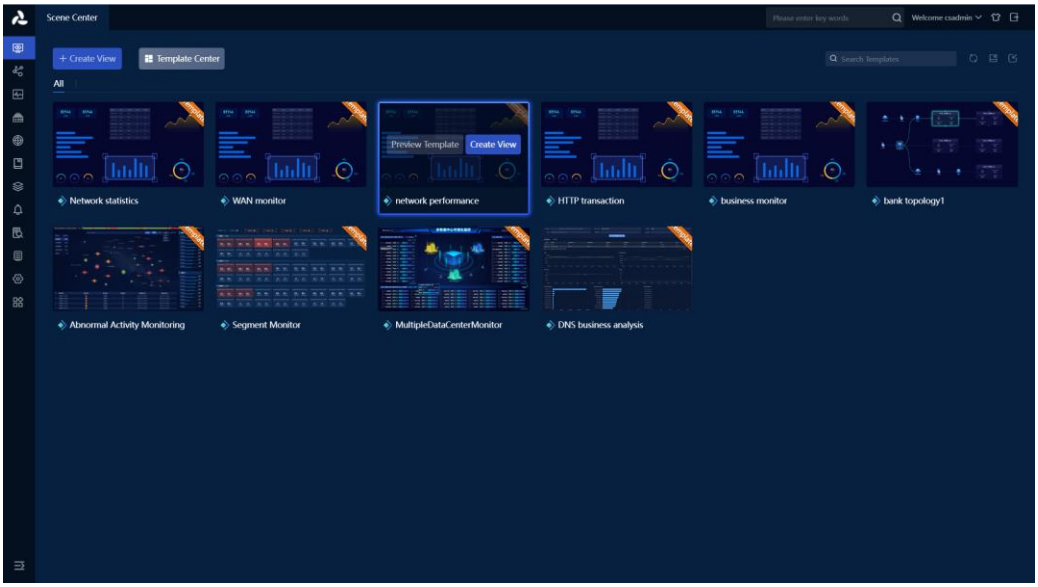


After creation, you can view the created scene view on the Scene Center homepage.

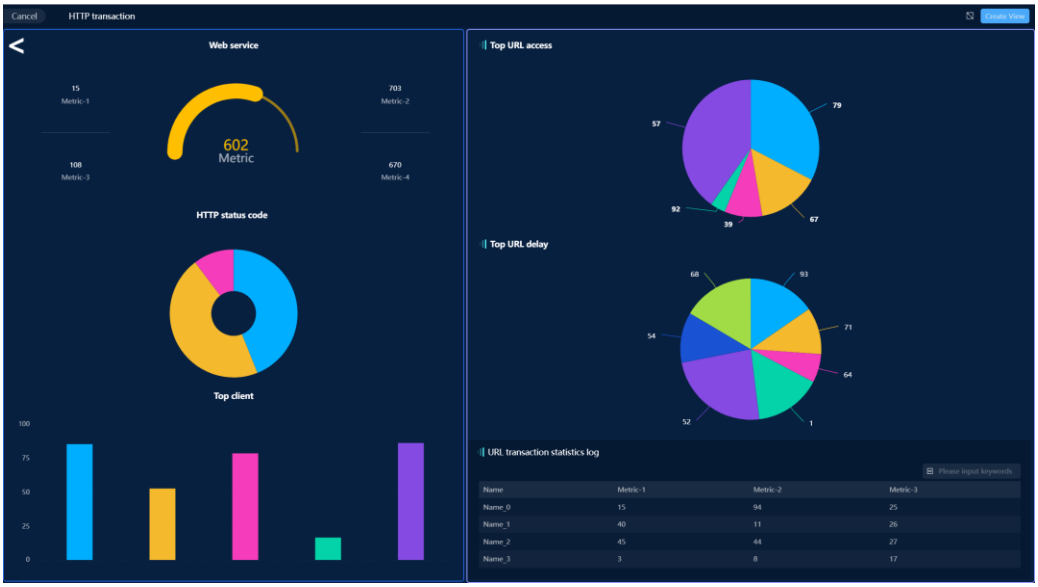


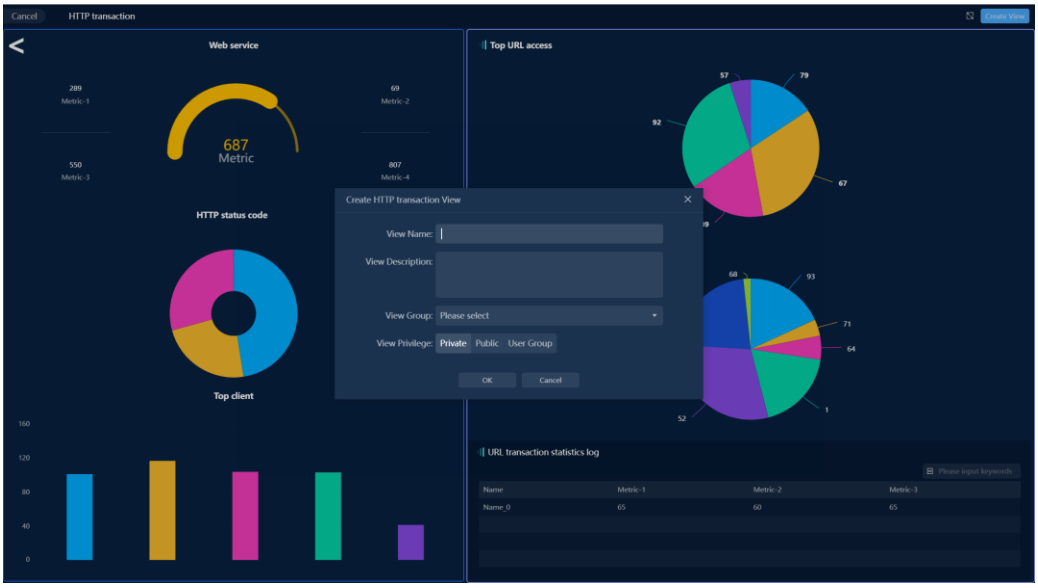
You can also preview the scene template before creating the scene view,

On the homepage of the scene center, scroll down to the template center area or click [Template Center] to view scene templates. Select the target scene template and click [Preview Template]. A new browser tab will open and enter the preview template page state.



In the template preview page, you can first globally view the display effect of the scene template to see if it meets the expected requirements. If it does, you can click on the [Create View] in the upper right corner to open the dialog box for creating xxxxxx as a view.





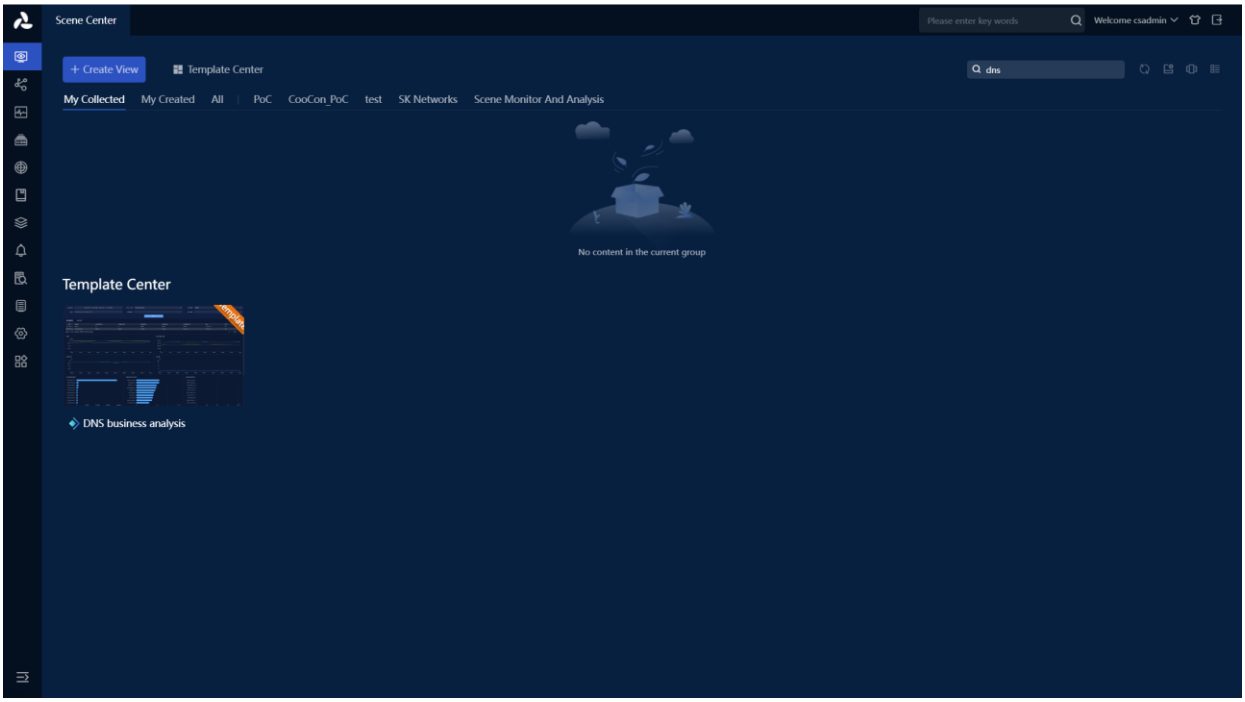
The subsequent operation steps are the same as the first method.

Quickly find scene views

1. **Search for scene views or scene templates**

On the homepage of the scene center, enter the content you need to search for in the top right corner, and it will filter and match scene views or scene templates with rules in real time.

Support fuzzy matching of typed numbers/English (case-insensitive)



2. List/Grid Scene View

14.1.6. Q&A

1. Where can I create and view modules under the historical version?

They are created and viewed in the scene center; Including views under modules such as historical version network performance monitoring, network topology monitoring, custom metric monitoring, scene monitoring, scene analysis, terminal monitoring, global business performance monitoring, and abnormal behavior monitoring.

2. Is there a limit to the number of scene views?

There is no limit to the number of scene views that can be created. When the network is connected normally and the speed is good, creating 200 scene views has a normal switching speed and the front-end page does not lag.

14.2. Tutorial for using custom metric monitoring

14.2.1. Function introduction

Terminology

- View

A view consists of one or more components, representing the monitoring of specific objects or specific scenes.

- Object

Object represents the target of monitoring in the system, and the system supports monitoring of various objects, such as links, businesses, applications, transactions, etc.

- Component

Component is the smallest unit of data presentation. The system supports various components, such as trend charts, tables, numerical graphs, images, text, etc.

- Empty Group

For the currently logged-in user, if there are no views that can be viewed in a certain view group, the view group is called an 'empty group'. Users can set to show/hide empty groups.

Functional scenarios

Data visualization is dedicated to presenting business relationships and potential issues hidden behind massive data in a more vivid and user-friendly form. It helps technical personnel discover and troubleshoot business issues through interaction with monitoring views.

The custom index monitoring function can meet the following scenarios:

- As a daily monitoring screen for business, monitor real-time traffic information of various businesses.
- As a unified monitoring platform, centrally display pages of other monitoring modules, such as terminal monitoring, network topology monitoring, etc.
- Monitor the real-time status of network devices, including CPU, memory, online status, etc.
- Monitor VoIP communication quality, including call status, network delay, TOP communication, alerts, etc.

Value

The custom index monitoring function includes the following functional values:

- The system provides various scenario templates to reduce user configuration difficulty.
- Support various icon components for users to freely match.
- The component provides personalized style settings to meet the monitoring needs of different users.
- The view supports custom resolutions, perfectly adapting to various monitoring screens.

14.3. Network Topology Monitoring

14.3.1. Functional background

When there is a network or business failure, single-point alarms cannot intuitively reflect the network location, lack understanding of network topology relationships, and cannot display the monitoring metrics of individual network nodes, affecting the efficiency of fault analysis.

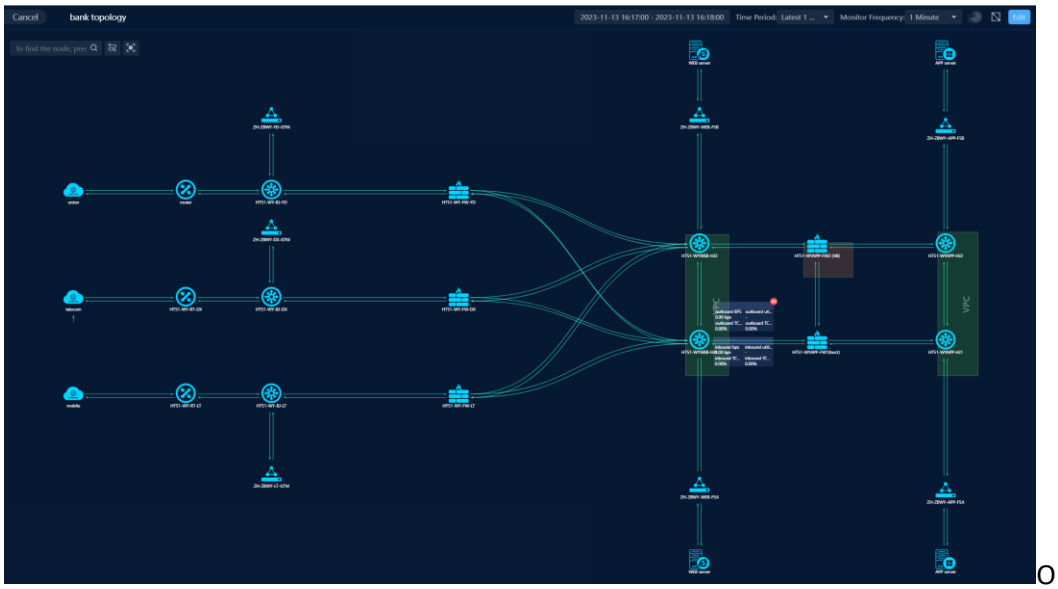
14.3.2. Value

To improve the efficiency of fault analysis, visually display the relationships between various nodes (devices, terminals, applications, etc.) in the network and key metrics through topology, locate root causes, and provide convenient analysis entry points.

Proactively monitor and analyze the overall network, provide real-time alerts, and promptly detect network anomalies.

14.3.3. Functional description

Support drawing and importing network topology views, associating network, host, application, and device entities, thereby enabling overall real-time monitoring and analysis of network links, application services, and device operations.

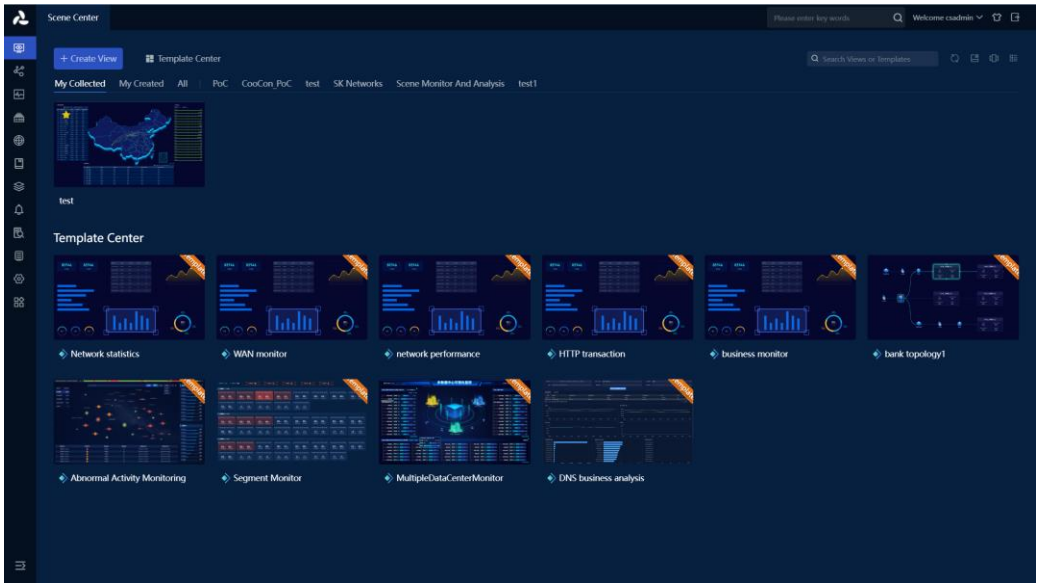


14.3.4. Guide

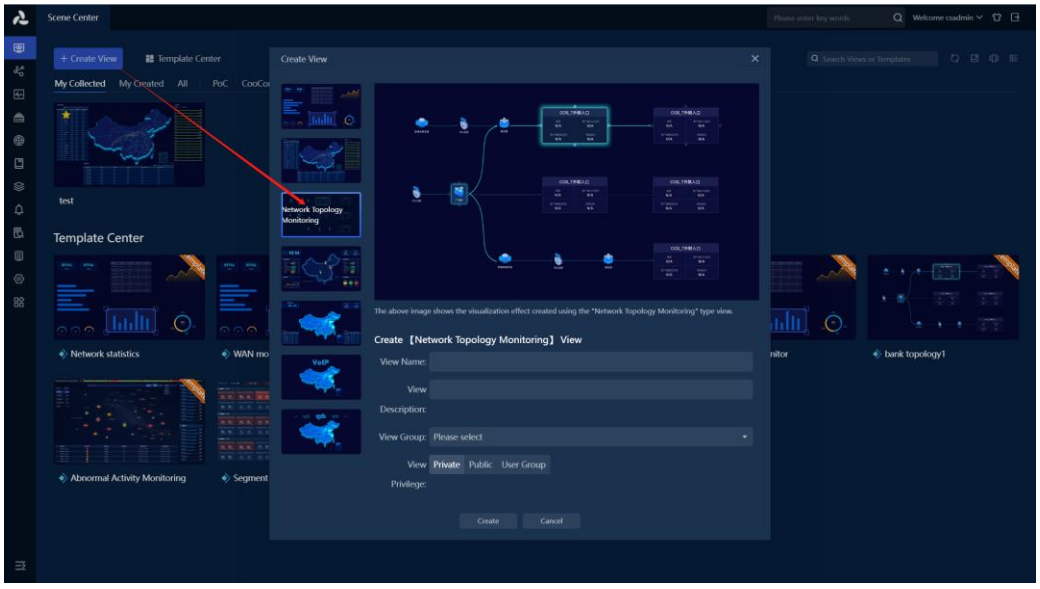
Create network topology monitoring scene views.

Create network topology monitoring scene views from scratch.

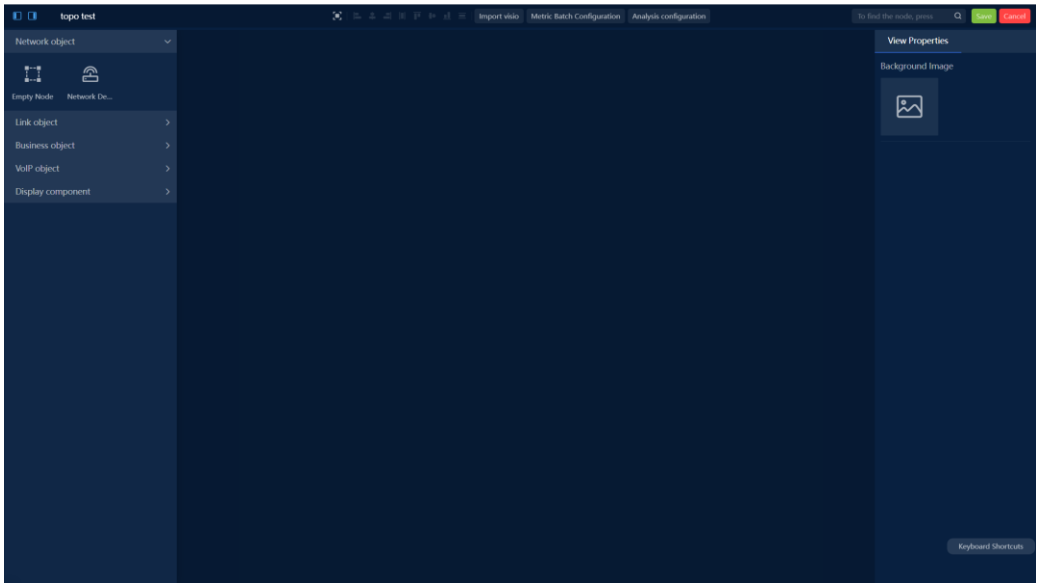
On the homepage of the Scenario Center, click [Create View] at the top left to open the Create View dialog box.

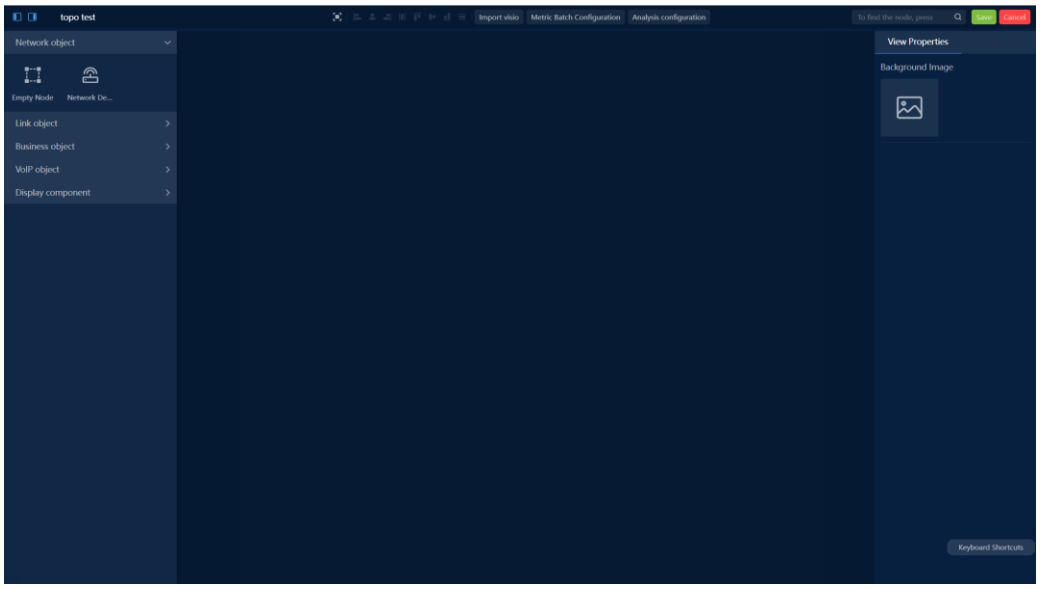


In the Create View dialog box, you can select the network topology monitoring type, enter the view name and description, select the view group and view permissions, and click [Create] when finished.

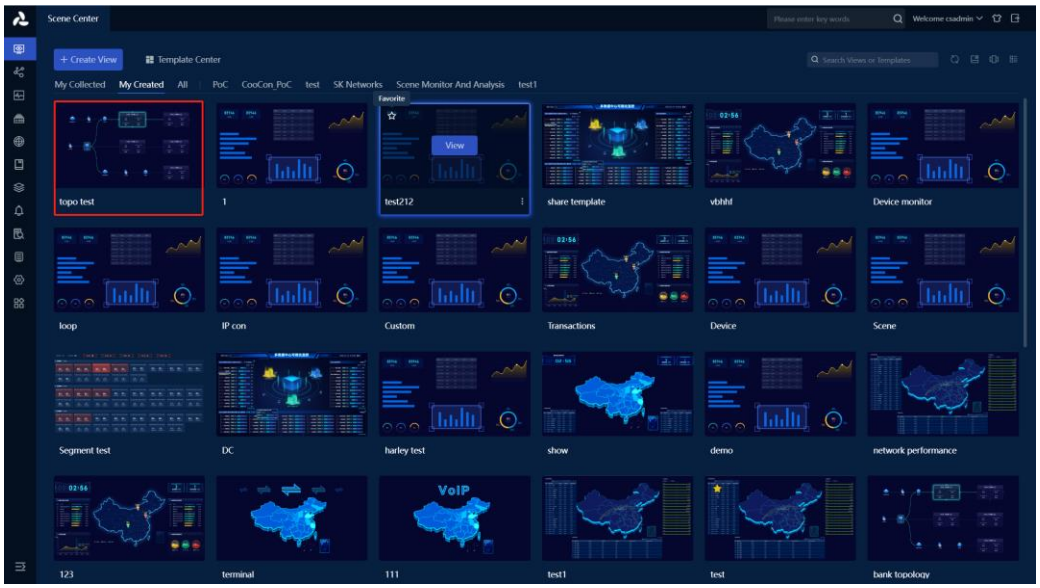


After clicking [Create], a new browser tab will open and enter the Edit View page state. You can drag components, bind data, and layout views (the function of building view content is consistent with history). After completion, click [Exit] to enter monitoring mode.



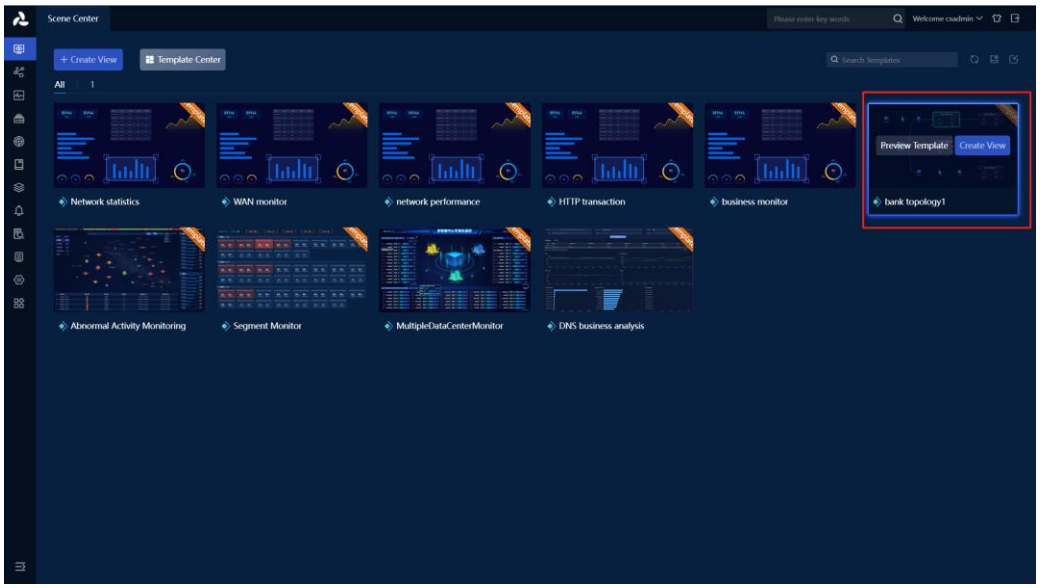


After creation, you can view the created scene view on the Scene Center homepage.

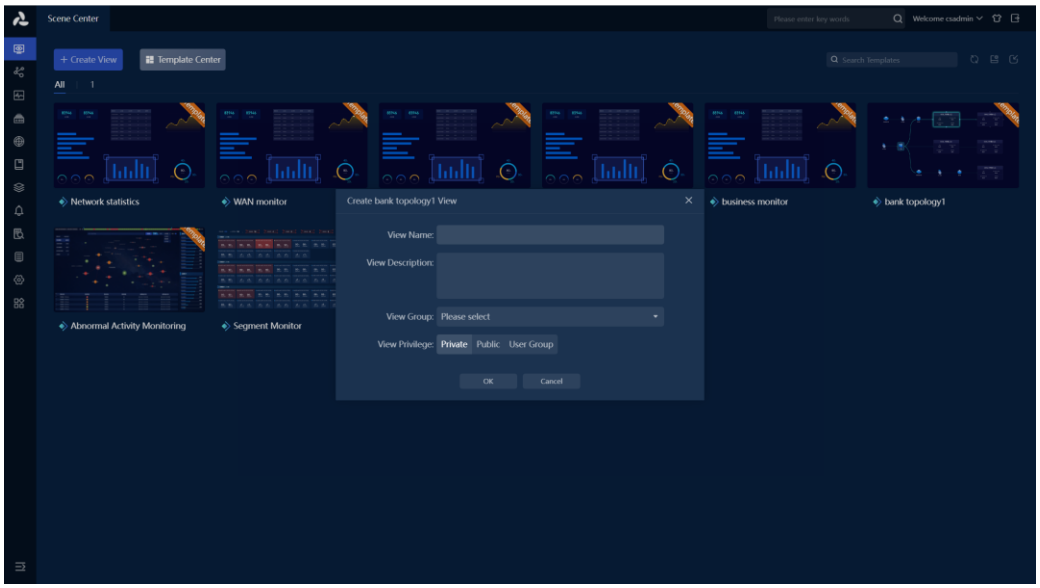


Create network topology monitoring scene views using scene templates.

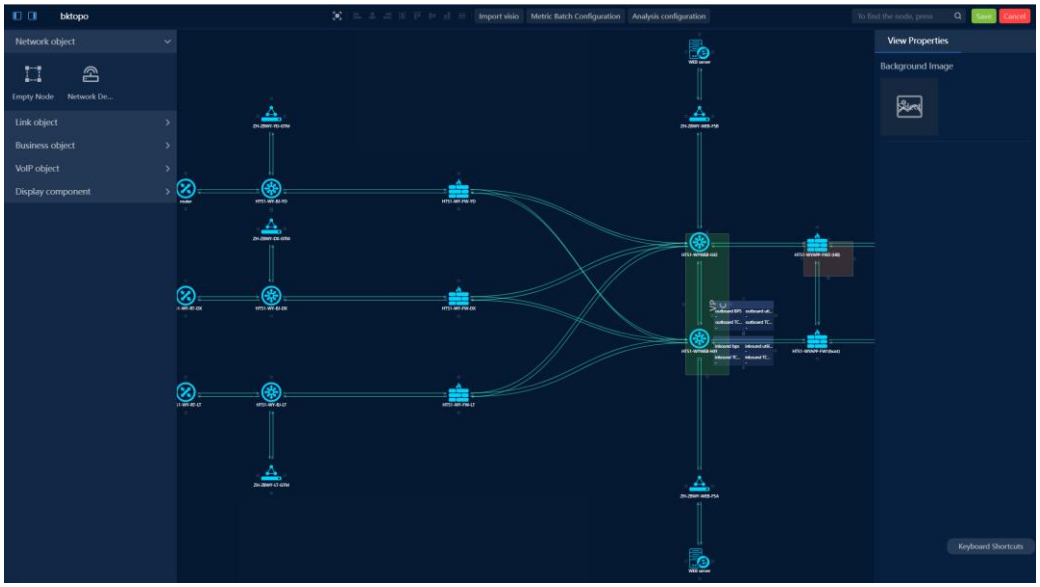
On the Scene Center homepage, scroll down to the Template Center area or click [Template Center] to view scene templates. Select the target scene template and click [Create View] to open the dialog box for creating xxx as a view.



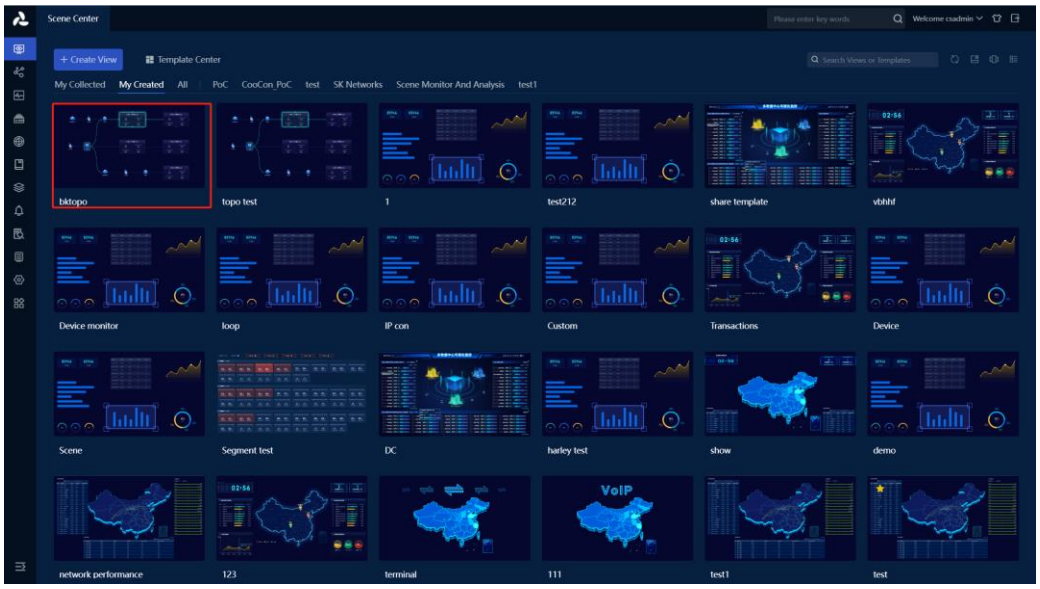
In the process of creating xxxxxx as a dialog box, enter the view name, view description, select the view group, view permissions, and click [OK] when finished.



After clicking [OK], a new browser tab will open and enter the edit view page state. You can modify or drag components, bind data, and layout views based on the existing content (the function of building view content is consistent with history). After completion, click [Exit] to enter monitoring mode.

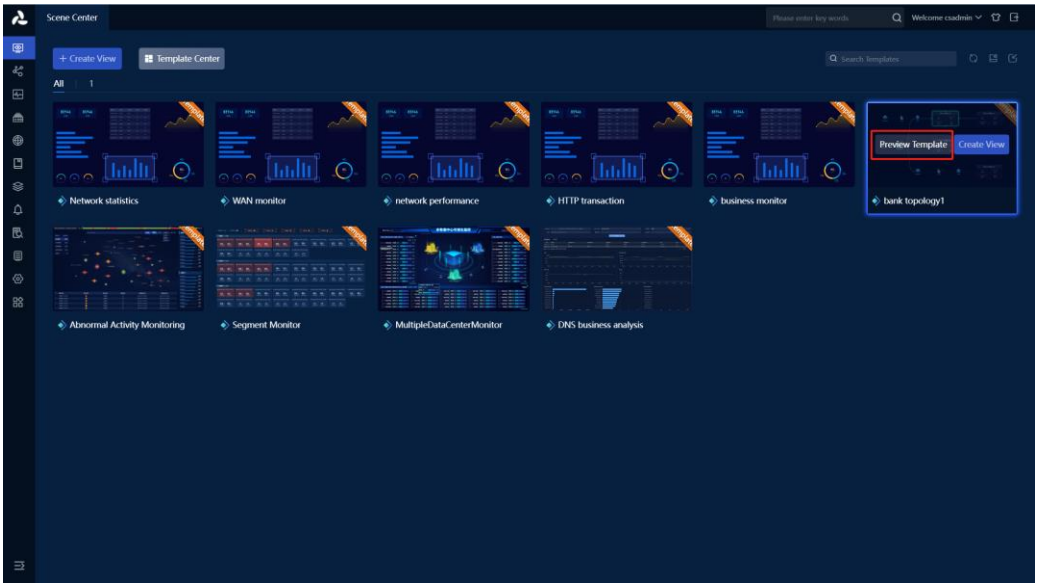


After creation, you can view the created scene view on the Scene Center homepage.

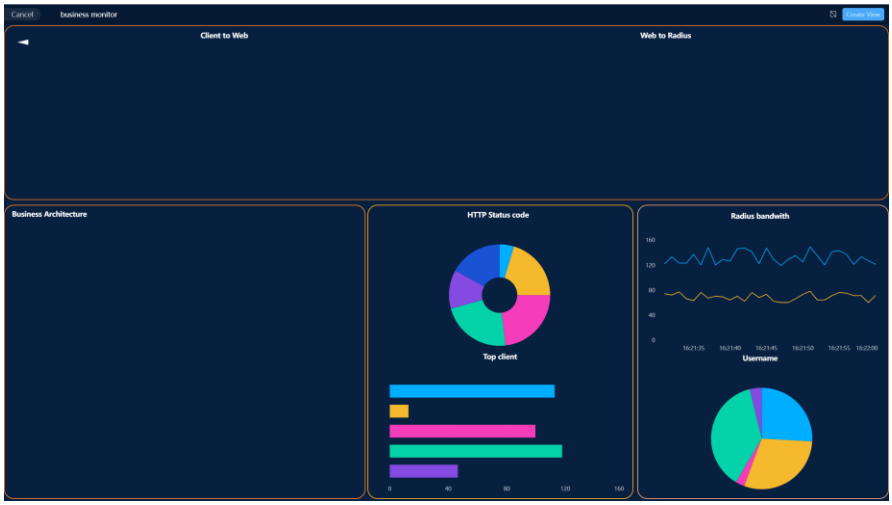


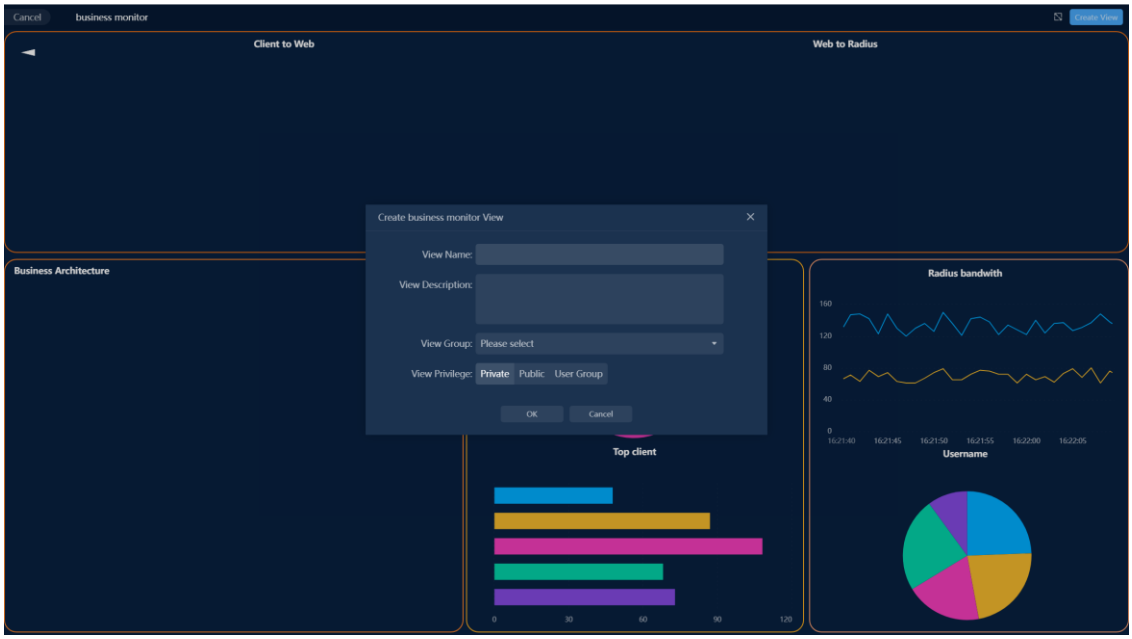
You can also preview the scene template before creating the scene view:

On the homepage of the scene center, scroll down to the template center area or click [Template Center] to view scene templates. Select the target scene template and click [Preview Template]. A new browser tab will open and enter the preview template page state.



In the template preview page, you can first globally view the display effect of the scene template to see if it meets the expected requirements. If it does, you can click on the [Create View] in the upper right corner to open the dialog box for creating xxx as a view.

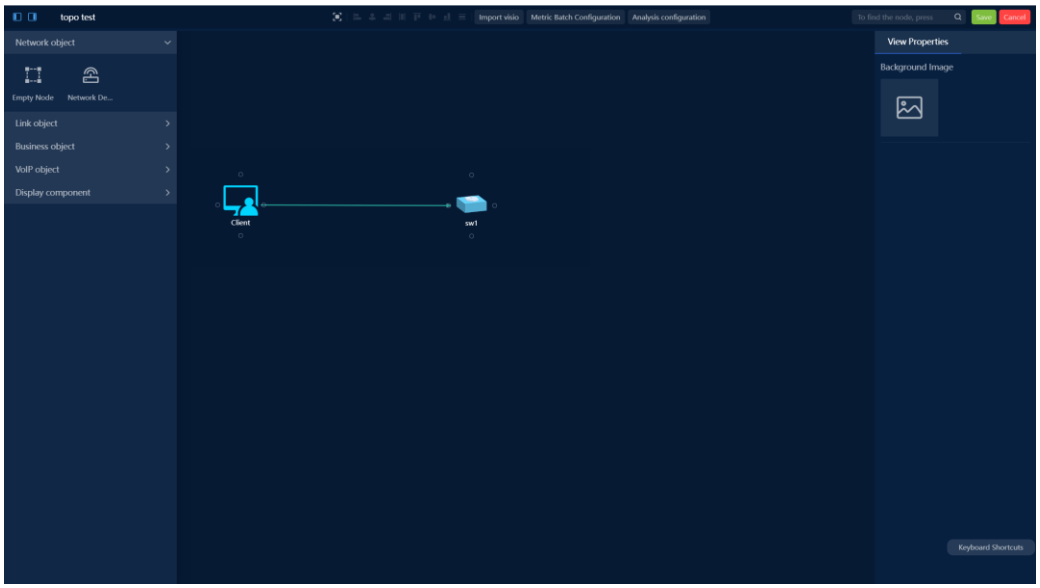




The subsequent operation steps are the same as the first method.

Draw topology

After creating a view, click the [Edit] button on the right side of the page to enter edit mode. In edit mode, the page layout consists of a top toolbar, a left component bar, and a right style bar.

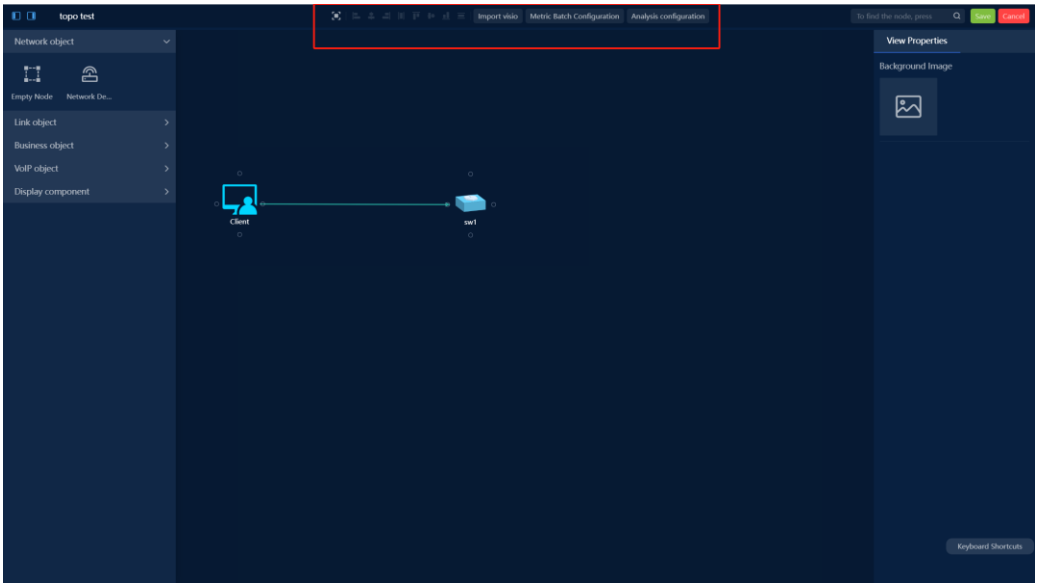


Top toolbar

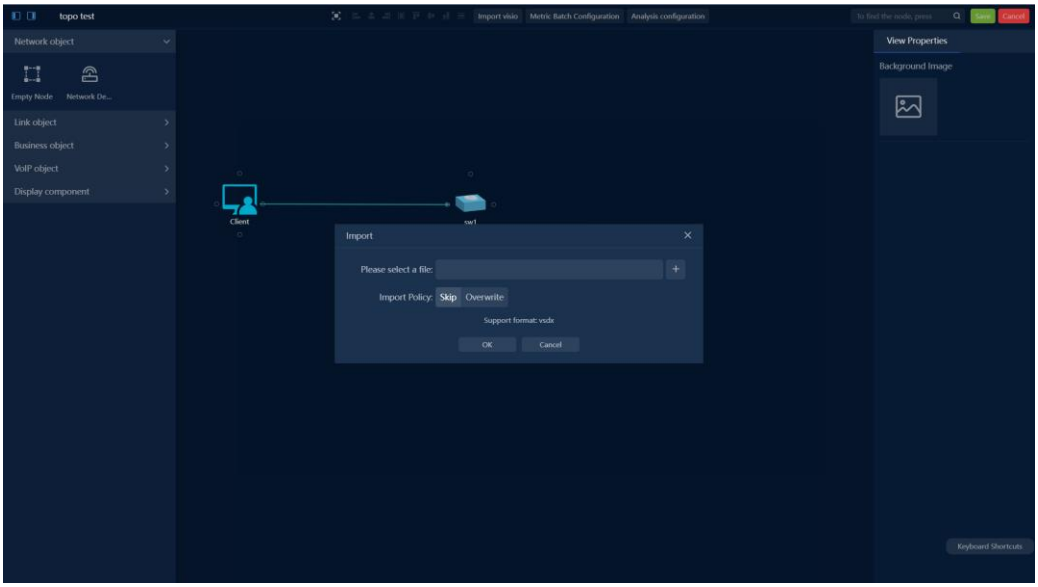
Clicking the Fit Canvas operation will center all content in the canvas.

When selecting two or more components by dragging a left mouse button, the left alignment/horizontal center alignment/right alignment/top alignment/vertical center

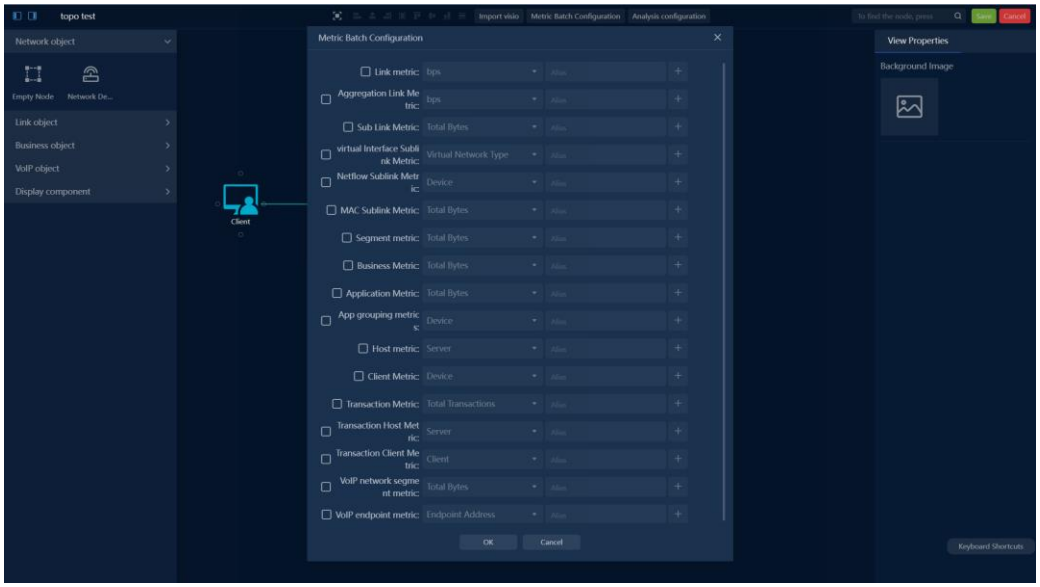
alignment/bottom alignment/horizontal equidistance/vertical equidistance functions in the top bar become available (not disabled), and you can then operate the left alignment/horizontal center alignment/right alignment/top alignment/vertical center alignment/bottom alignment/horizontal equidistance/vertical equidistance functions.



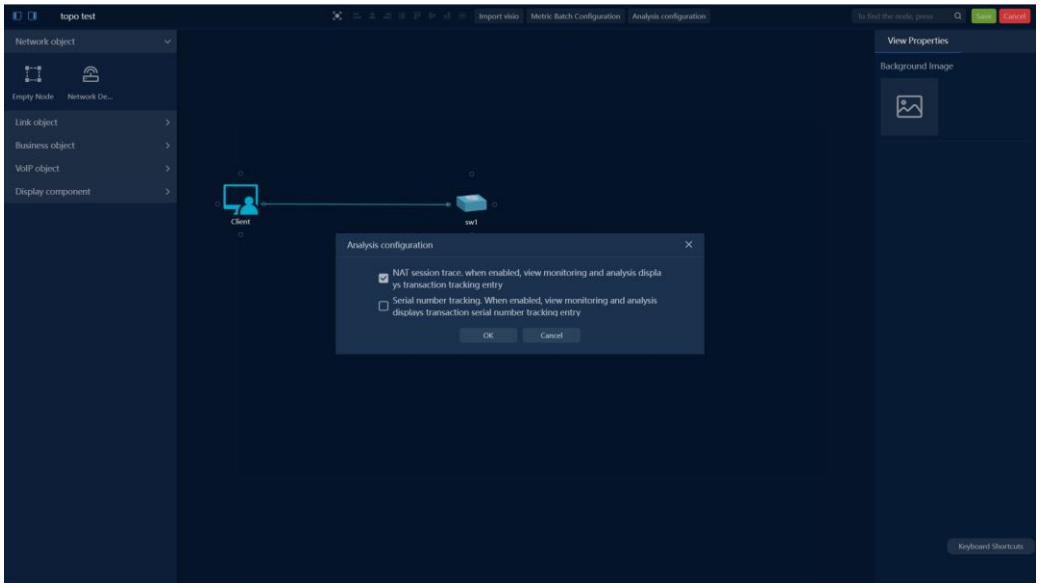
Support importing Visio files to generate topology.



Support batch setting of metrics.

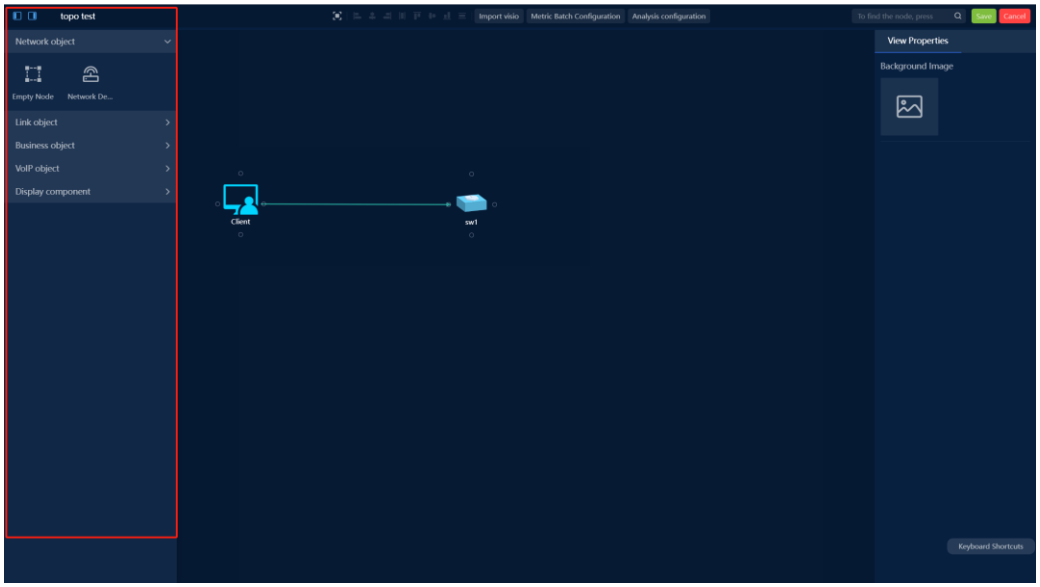


Support NAT tracking, transaction tracking analysis settings.



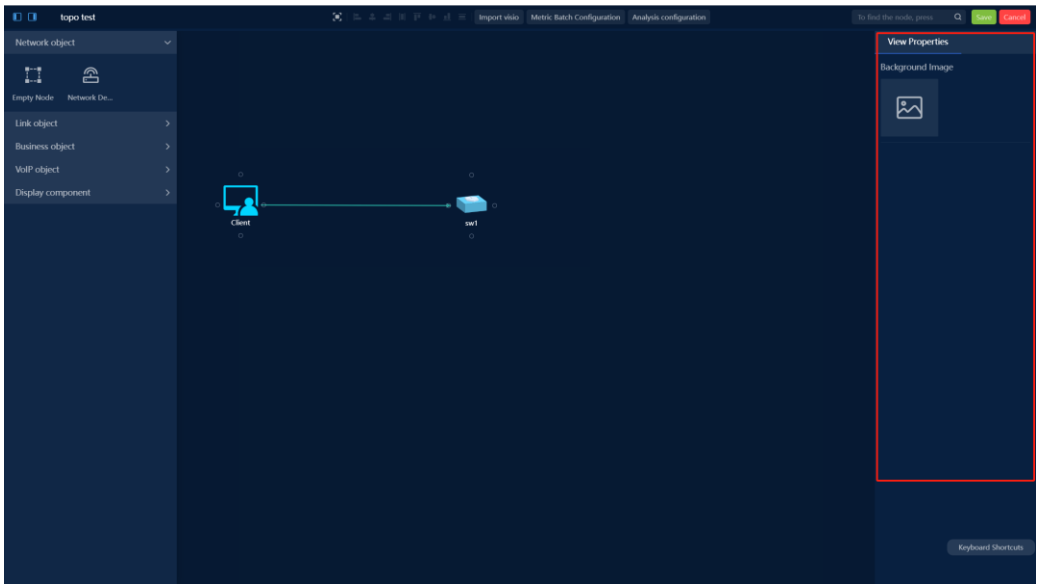
Left component bar

For various network objects and display components that can be placed in the topology diagram, including links, subnets, applications, network devices, images, and text. These components can be associated with corresponding data metrics. Hold down the left mouse button and drag it to the right to add it to the view.



Right style bar

Adjust the font size, color, background color, border style, line color animation, and other styles in the components.



Batch set the style of components:

- When selecting multiple components by dragging the left mouse button or selecting a single component by left-clicking, you can set the component parameters in the open right attribute panel state. For example, when selecting components under the link object, you can set the icon size, text, etc. in the open right attribute panel state.
- When selecting two or more components by dragging the left mouse button to select, you can set the component parameters while the properties panel on the right is open. If

components of the same type are selected, such as link objects, business objects, VoIP objects, you can set the icon size and text of the components while the properties panel on the right is open.

- If components of different types are selected, such as network objects, link objects, business objects, VoIP objects (including quadrants), rectangles, text, lines, you can set the text of the components while the properties panel on the right is open.

The shortcut operation bar on the lower right: You can use shortcuts to quickly operate the canvas and components. In edit mode, click the [Shortcut Key] operation to display the top layer. After clicking [Shortcut Key], the shortcut key panel will open. Click [Close] to hide the panel.

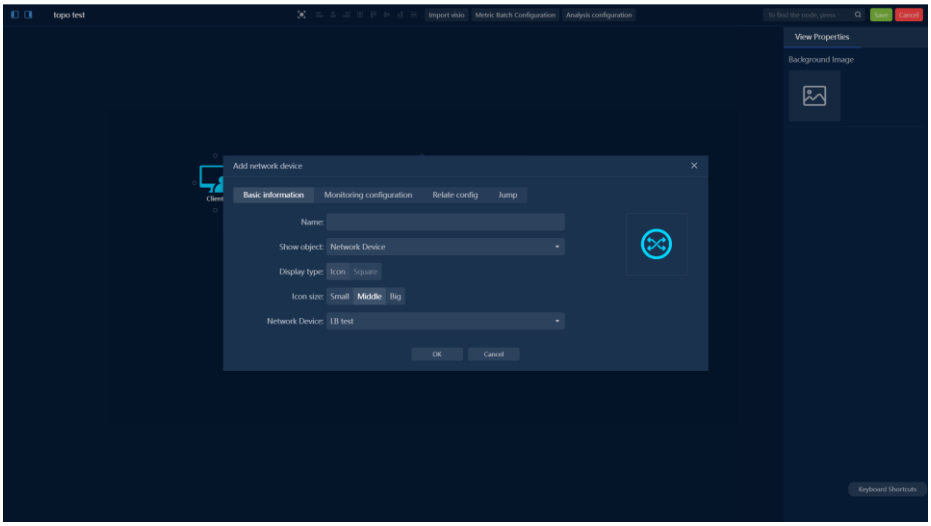
- Canvas editing shortcuts (regardless of editing status): Move: Drag right mouse button. Zoom in: Scroll down. Zoom out: Scroll up. Fit canvas: Ctrl + 1.
- Component editing shortcuts: Select: Drag left mouse button. Select all: Ctrl + A. Delete: Delete. Align left: Alt + A. Align right: Alt + D. Align top: Alt + W. Align bottom: Alt + S. Align horizontally center: Alt + Q. Align vertically center: Alt + E. Distribute horizontally: Alt + Shift + Q. Distribute vertically: Alt + Shift + E.

Topology drawing - Middle area

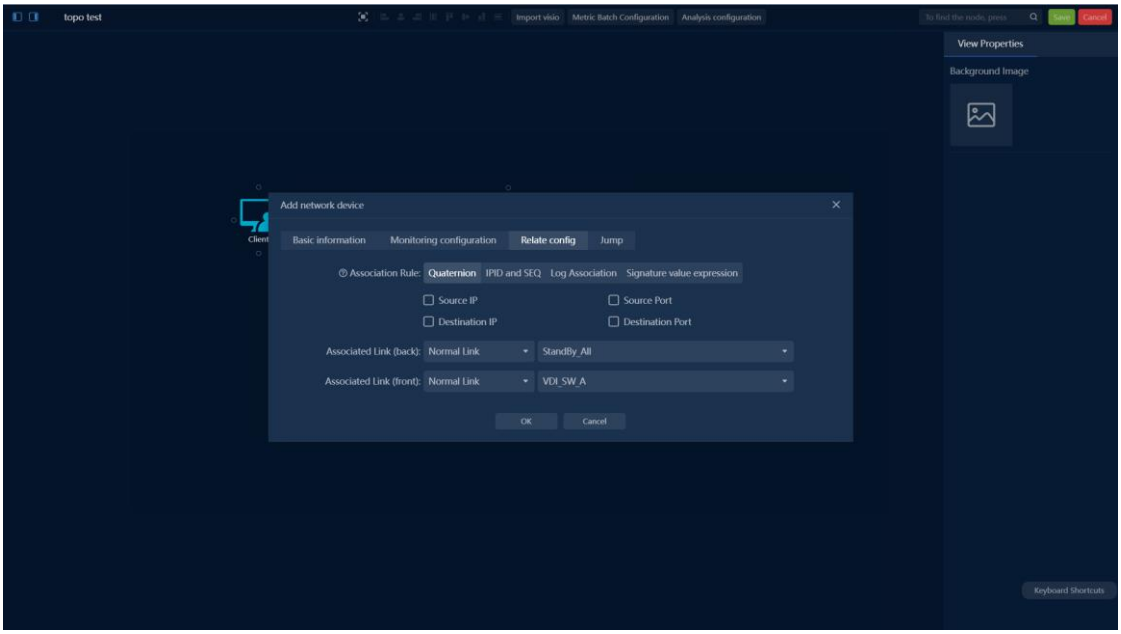
Topology Node Configuration

Node refers to any graphical component dragged into the view area as a topology node. Node configuration includes: basic information, monitoring configuration, association configuration, jump interaction.

- Basic information: configure the display name, display icon, specific display object, and indicators of the node. Selectable display objects include: devices, links, applications, subnets, hosts, etc., in a dropdown menu.
- Monitoring configuration: mainly configure the alarms for monitoring nodes and the threshold range for indicator display colors.



- Relate config: used for configuring session NAT tracking scenarios, how to associate the same session before and after passing through a device node, for session segmentation analysis and troubleshooting. When you need to perform NAT session tracking analysis through this topology view, you can configure this item.



- Jump: This configuration allows you to right-click on a node and quickly jump to the target view or specified URL page.

Connection Configuration

- In view editing mode, each node displays connection anchor points on all sides. Select an anchor point with the mouse and drag it to the target node's anchor point to complete the connection drawing.
- Select a connection and click on the right-side style panel to set the style of the connection, which will take effect in real-time. You can also right-click on the connection to configure connection

indicators and adjust the connection style.

- Supports setting connection style, connection indicator display settings, indicator name settings, and indicator settings.
- Connection Indicators
- Configure connection indicators, supporting the association of application indicators, application segment indicators, network segment indicators, link indicators, link segment indicators, and network segment-to-segment indicators to the connection. The segment-to-segment indicator value is the difference between the indicators of two links.
- In the 'Monitoring Configuration' of the connection indicators, you can define alarms for the connections.
- The configuration of the display position of indicators on the connections can be set to follow the connections and display above them in the style settings, or dragged to a specified position in a four-grid form.

Save view

After the topology is drawn, click the save button in the upper right corner of the view to complete the creation and editing of the view.

Node analysis

In the topology monitoring view, click on the node or connection associated with the relevant indicator, and the analysis view of the corresponding indicator will be displayed below the view, supporting the selection of any time period for analysis.

Find node

When there is a lot of content in the view and it is difficult to locate a node directly, you can use keywords to search and locate the node. The matched node will be highlighted and the node's position will be centered in the view. Both the node name and the name of the bound object support searching.

Path retrieval

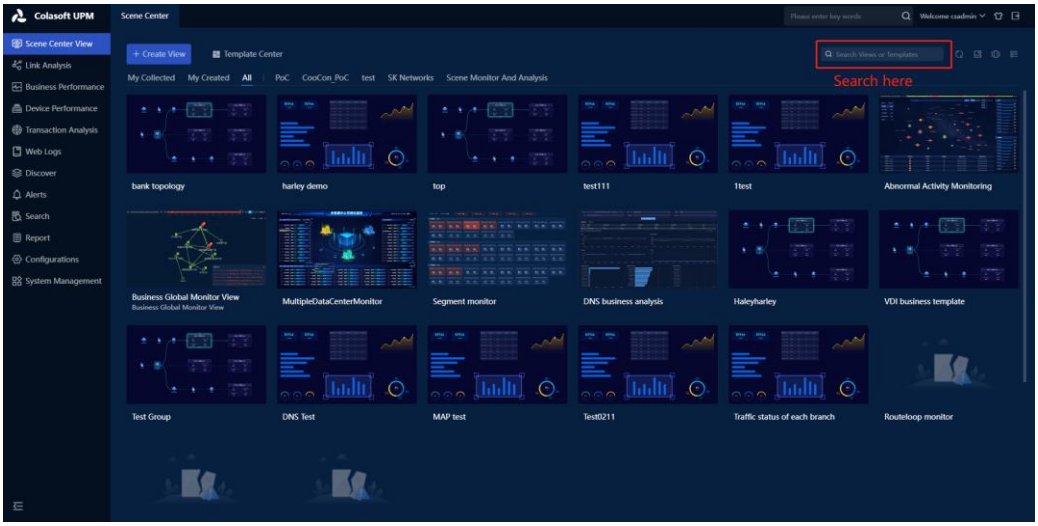
Supports path retrieval by entering IP sessions, applications, subnets, and IPs in the view.

For scenarios where the full path of a public network client IP needs to be located, highlight the nodes and connection paths that the IP passes through based on the selected time range and IP in the view, helping to quickly locate abnormal locations and improve response efficiency.

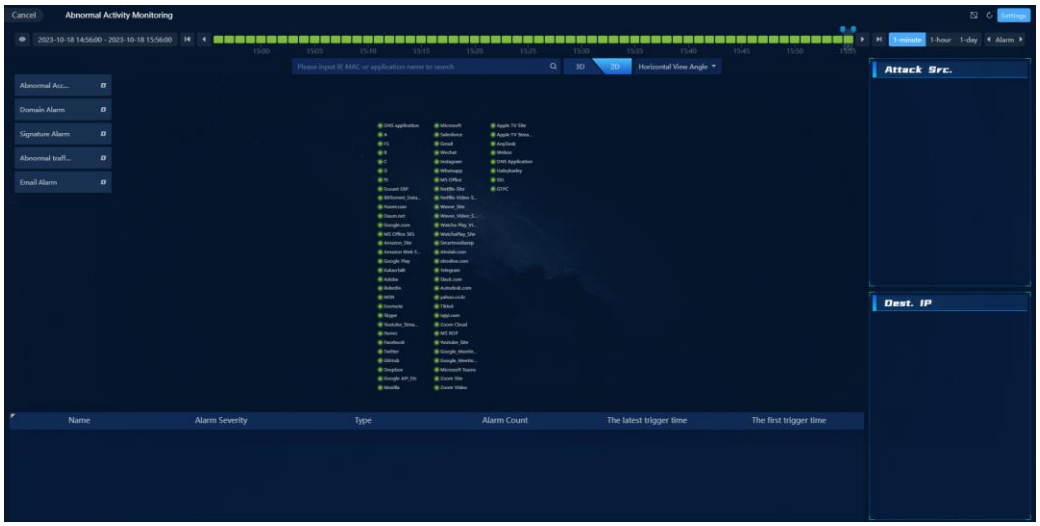
14.4. Abnormal Behavior Monitoring

Provides network security and business security monitoring based on network traffic analysis technology. Supports various types of abnormal behavior alerts, including abnormal access alerts, abnormal traffic alerts, email sensitive word alerts, suspicious domain alerts, and data flow characteristic alerts. For detailed alert configuration, please refer to section 4.3 Abnormal Behavior Alert Configuration.

Click on the navigation menu and select 'Scene Center'. In the all Views page, search for the Abnormal Behavior Monitoring View or search for the view using the keyword ' Abnormal Activity Monitoring'.



Click on View to open the view. The view displays the latest 1 minute of abnormal alarms by default.



Page content description:

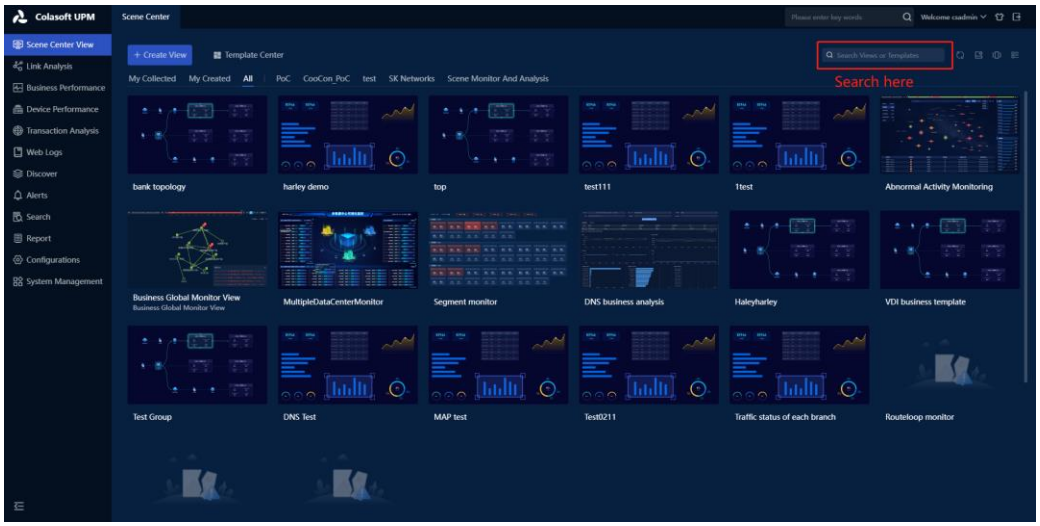
Access Relationship Diagram: In the middle of the page, the diagram shows the abnormal access situation of each application and host, with the application as the core. This includes abnormal access between applications and abnormal access by illegal clients to applications, represented by arrows indicating the direction of access.

 The icon node represents an application node,  and the icon node represents an IP node.

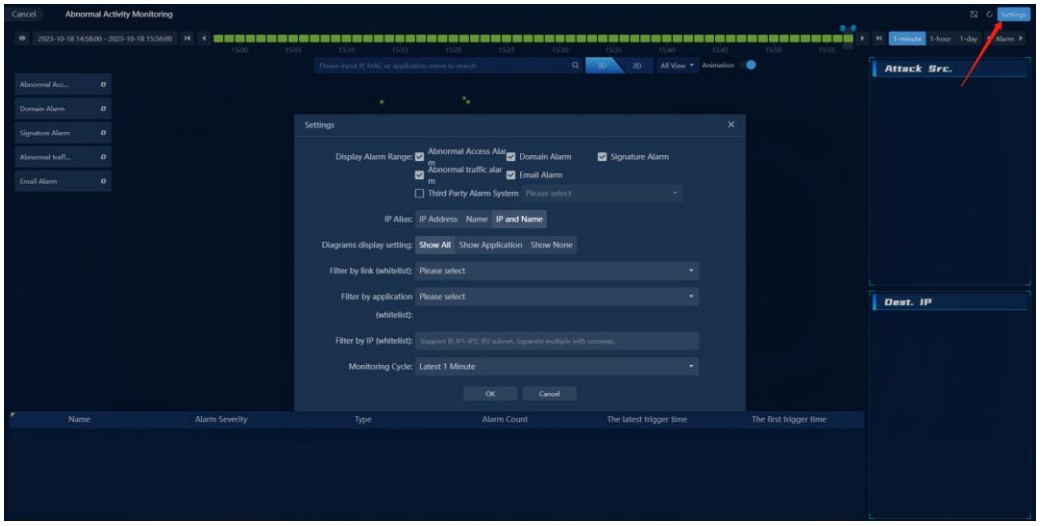
- **Source IP:** Displays the top 10 source IP addresses with the highest number of triggered alarms during the current monitoring or analysis period. Click on the source IP address to view alarm details.
- **Destination IP**: displays the top 10 destination IP addresses with the highest number of attacks during the current monitoring or analysis period. Click on the destination IP address to view alert details.
- **Type Statistics**: displays the number of alerts for each alert type during the current monitoring or analysis period. Click to filter and display alerts based on selected alert types in the current view.
- **Alert Statistics**: aggregates and displays alert information triggered during the monitoring period by alert name. Click on an alert to view its details.

14.4.1. Create a new abnormal behavior monitoring view

Click on the 'Scene Center View' in the navigation menu, and search for the template using the keyword 'Abnormal Activity Monitoring' in the all Views page or Template Center page. You can select a template to create a new view.

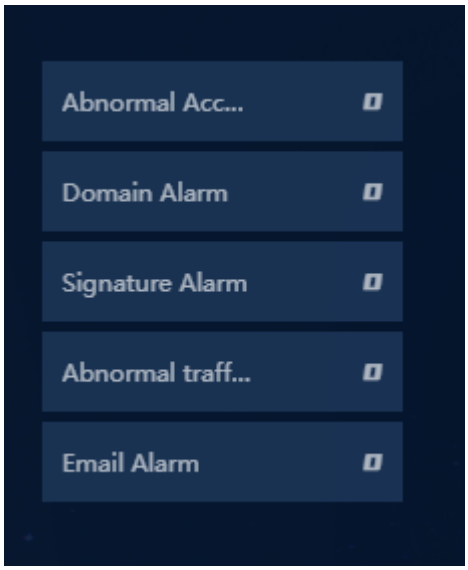


In the view, the content that can be filtered and displayed by link, application, IP, and alarm type is supported. As shown in the figure below, filter conditions can be set in the configuration. Different filter conditions for abnormal behavior views take effect independently.



14.4.2. Display of third-party system alarm logs

Third-party system alarms refer to alarms received by UPM through interfaces from third-party systems. Support display within the view. As shown in the figure below, only the number of alarms is displayed, and clicking on it will show the specific alarm details.



14.5. Network Monitoring

14.5.1. Network Performance Monitoring

Network performance monitoring is also a custom monitoring view provided by UPM Center. In network performance monitoring, you can customize multiple network nodes and the network paths between nodes to monitor the communication status between nodes in real time.

1. You can access "Network Performance" > "Network Performance Monitoring".

Define monitoring views

1. You can delete, add, edit monitoring views, view permissions support private, public, and user group.
2. Configure the core component of the view "Network Performance Monitoring".

    1） View types support network types and VoIP types.
    2） Configurablewhether data in the viewisfiltered.
    3） Configurable monitoring period and frequency of the view.
    4） Configure the relationship between network segments in the view.
    5） Configurethe metrics monitored in the view.
    6） Configure the display mode of the view, supporting line charts, scatter plots, and area charts.

3. Configure other monitoring components based on corecomponentsdata, supporting alert logs, path analysis, tables and application metric monitoring components.

Note

When adding network segment nodes, the system will automatically list all network segments that have been sorted out in the network path sorting, and you can choose one or more network segments from them.

Monitoring View

The system will automatically evaluate the status of each network path and identify the network paths differently based on the evaluation results.

The alert evaluation results of the network path are as follows:

1. X: Network interruption
2. Gray: No traffic
3. Green: There is traffic and the network performance of this path is good.
4. Orange: There is traffic but the network performance of this path is average.
5. Red: There is traffic but the network performance of this path is poor.

The congestion evaluation results of the network path are as follows:

1. X: Network interruption
2. Gray: No traffic
3. Green: Very idle
4. Blue: Idle
5. Orange: Moderate congestion
6. Red: Severe congestion

The evaluation results of the network path indicators are determined based on the user's custom indicator threshold color scale.

You can select a path, right-click, and enter the path analysis page, trend analysis page, or quick analysis page for detailed analysis.

14.5.2. Network performance analysis

In network performance analysis, analyze the traffic occupancy, comparison, and trend analysis between segments based on the packet situation between segments.

1. Access through "Network Performance" > "Network Performance Analysis". Users can see a list of data between all network segments, which displays key indicators.

Grouping

The grouping list is displayed by default based on network performance monitoring groups. The hierarchical relationship is: monitoring groups -> network segments -> probes.

1.  You can click the button to add groups and set the relationship between network segments within the group.

Note

Custom group settings path ranges from network segment relationship under monitoring groups.

A network segment relationship can only belong to one group.

Proportion Analysis

1.  You can click the button and set the metric group in the "Metric Group Configuration" popup window.
2. You can view the metric trend chart and switch between metric groups and chart types.
3. You can view the Top table data of different network objects, supporting list, pie chart, and bar chart display.
4.  You can click the button to further analyze the data trend.
5. You can click the button to analyze the data mining. 

Comparison Analysis

Compare the values of a same metric at different time points.

1. You can check the” comparison period” options to set the comparison time period for comparative analysis.

Trend prediction analysis

Simulate the trend of indicators at specified time points in the future period, providing reference for network capacity expansion or planning.

1. You can click  the button to open the 'Trend Prediction Settings' window and set the trend prediction conditions for prediction.
2. Trend analysis supports daily and weekly analysis, with the system defaulting to daily

analysis. When selecting daily or weekly analysis, the units for historical time range and trend time length will also be switched accordingly.

1) Trend analysis by day: You can choose the data for the whole day or a specific time as the historical data for trend analysis. The system will use a certain algorithm and historical data to generate trend charts for the specified time range (in days) in the future.
2) Trend analysis by week: You can choose each day or the whole day of a week, or a specific time data as the historical data for trend analysis. The system will use a certain algorithm and historical data to generate trend charts for the specified time range (in weeks) in the future.

14.5.3. Network Path Analysis

Path analysis is a comparative analysis of data from the same network segment between different probes to identify network packet loss and network latency issues between segments. Or VoIP segment Mos, packet loss and jitter issues.

1. On the 'Network Performance Monitoring' page, right-click on the path and select 'Path Analysis' from the pop-up menu to enter the network path analysis page.
2. You can set the time range: the system default time range is consistent with the network performance monitoring interface, and you can customize it.
3. You can view the network device information in the communication path.
4. You can view the default system's metric trend chart, and select the probe objects you need to view.

    1) When selecting the network packet loss metric, the metric trend chart defaults to displaying four metric trend charts: retransmission rate, bit rate, segment loss rate, and packet count.
    2) When selecting network latency, the metric trend chart defaults to displaying four metric trend charts: three-way handshake client RTT, three-way handshake server RTT, client ACK delay, and server ACK delay.
    3) Select the Mos indicator, and the indicator trend chart defaults to displaying the average video Mos for upstream, average video Mos for downstream, average video Mos, and bitrate 4 indicator trend charts.
    4) Select the packet loss indicator, the indicator trend chart defaults to display the upstream media packet loss rate, downstream media packet loss rate, average media packet loss rate, and bitrate 4 indicator trend charts.
    5) Select the packet loss indicator, the indicator trend chart defaults to display the upstream average jitter, downstream average jitter, average jitter, and bitrate 4 indicator trend charts.

14.5.4. Network Quick Analysis

Network Quick Analysis allows you to quickly view the trend of abnormal data, supports custom query configuration generation temporary charts, and performs comparative analysis and trend analysis between multiple network segments or multiple probes.

14.5.5. Network Performance Alert

In the Network Performance Alert Management, you can manage all alerts triggered by the network within a certain time period. In the Network Performance Alert, you can view all alerts triggered by the system within a week and process them for approval.

1. Access through 'Network Performance' > 'Network Performance Alert'.
2. You can view the distribution chart of alarm levels, alarm statistics chart, and alarm list.
3.  You can click the button to process the alarm. After the alarm is processed, the system will automatically generate a log of the alarm. When the same alarm is triggered again in the future, you can view the previous log to quickly trouble shoot.

Note

After selecting multiple alerts, you can batch sign the alerts. When signing multiple alerts triggered by different network paths, the segmented path in the fault type is unavailable.

4.  You can click the button to view the previous processing history of the alarm and quickly troubleshoot the cause of the fault. In the processing history, based on the historical processing logs of the alarm, the false positive rate of the alarm is calculated, and the top 10 hosts/network devices/paths that trigger the alarm the most under each cause category are listed. You can also view the detailed processing log.
5. You can click  the button to jump to the packet download page for data download.

14.5.6. Network Performance Reports

The network performance component generates individual network performance monitoring group reports based on network performance. You can select the relationship between network segments as the analysis object in a specific network performance monitoring group and choose the chart type.

1. You can access the report management page through the 'Reports' menu. Click on 'Add' to enter the new report page and add network performance charts. 
2. After adding the chart, you can view the report display effect. At this time, the report graph is simulated data, not real data.
3. You can click on the 'Preview' button to enter the report preview page and view the real report graph.
4. After completing the report settings, click the” Save” button to set report properties

   2） Report format: The system supports four formats: PDF, WORD, EXCEL, and HTML, and you can choose one of them.
   3） Report type: You can choose daily, weekly, monthly reports, and the report generation time.
   4） Business period: Supports setting the business period, with the minimum accuracy of minutes for daily reports, 10 minutes for weekly reports, and hours for monthly reports.
   5） Comparison: When selecting daily reports, you can compare with the previous period, the same period last year, the same period last week, and a specified date;

When selecting weekly reports, you can compare with the previous period and a specified date; When selecting monthly reports, you can compare with the previous period, the same period last year, and a specified date;

6） Recipient Email: The email address to receive the report. After filling in the email address, the system will send the report to the specified email address regularly.

Note

In order for the report to be successfully sent, the SMTP server configuration must be correct.

7） On the report list page, you can also click on the name of a report to enter the report log interface and view the generated historical reports for that report.

14.5.7. Network Topology Alert

The Network Topology Alert Management provides unified management for alerts triggered during a certain time period. In the Network Topology Alert, you can view all the alerts triggered by the system within a week and process the alerts for signing.

1. Access through "Network Performance" > "Network Topology Alert". The hierarchical relationship of the left grouping tree is: View Group -> Device Relationship.
2. You can view the distribution chart of alarm levels, alarm statistics chart, and alarm list.
3.  You can click the button to process the alarm. After the alarm is processed, the system will automatically generate a log of the alarm. When the same alarm is triggered again in the future, you can view the previous log to quickly troubleshoot.
4.  You can click the button to view the signing history before the alert to quickly troubleshoot the cause of the problem. In the signing history, you can view detailed signing logs.
5. You can click  the button to jump to the packet download page for data download.

14.6. Terminal Monitoring User Manual

Terminal monitoring is used to monitor different types of application client in various scenarios, including:

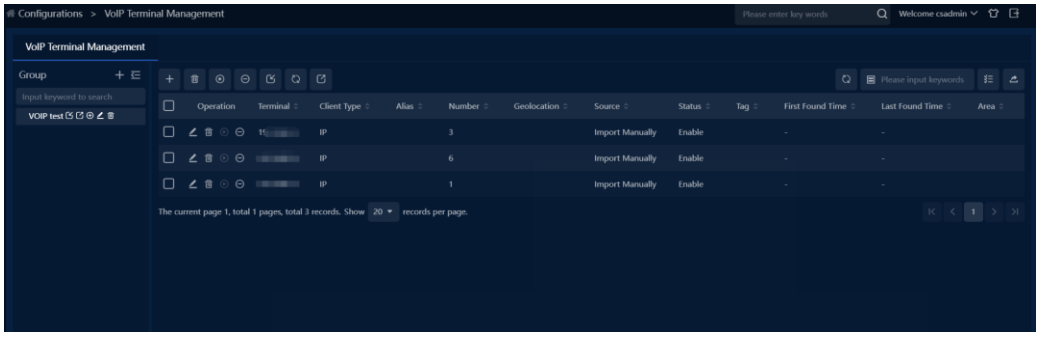
- VoIP terminal monitoring, by monitoring indicators such as jitter, delay, and packet loss of video (voice) terminals, abnormal terminals can be detected and the cause of the problem can be identified in a timely manner;
- Application client monitoring, by analyzing network performance indicators of terminal access to business systems (such as latency, number of sessions, and traffic), application service status and network quality can be monitored from the perspective of terminal experience, enabling quick problem identification.
- Business continuity exercise monitoring, by statistically analyzing business data, monitoring the status of business switch recovery for terminals participating in the exercise. For detailed functionality, please refer to the chapter on Backup Terminal monitoring.

The main functions include:

- Terminal Management: Used to maintain monitored terminals and terminal information (such as terminal type, alias, IP address).
- Terminal Monitoring: Define monitoring views as needed to monitor terminal status and alarm information in real time.
- Terminal Analysis: Analyze network performance and application performance from the perspective of terminals, and analyze and locate problems.
- Terminal Alarm Configuration: Define terminal alarms.
- Terminal Alarm Query: Query terminal alarm logs.

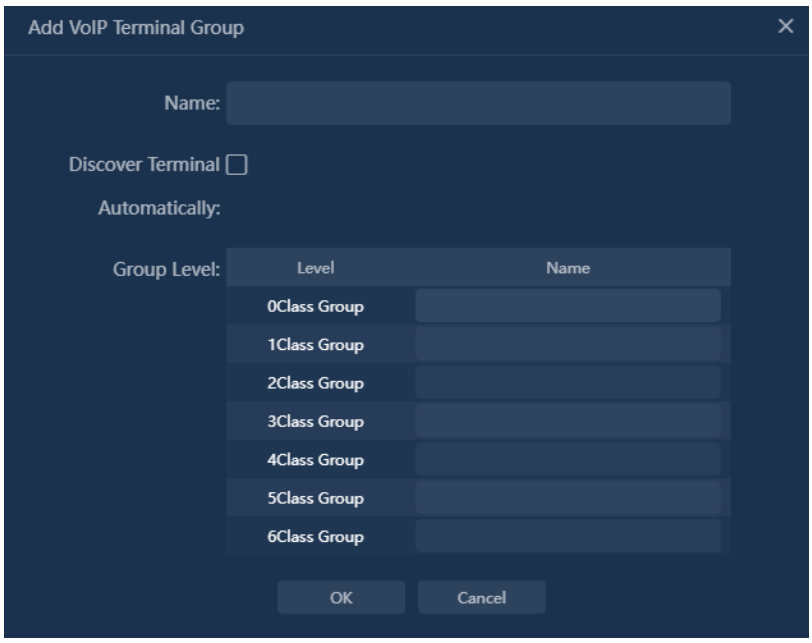
14.6.1. Terminal Management

Click on the navigation menu, go to 'Terminal Monitoring' -> 'Configuration' -> 'Terminal Management' to enter the configuration page, and configure different terminals based on the scenario. The types include: Backup terminal management, VoIP terminal management, application client management. The terminal configuration process is basically the same. Taking VOIP terminal configuration as an example, it is shown in the figure below:

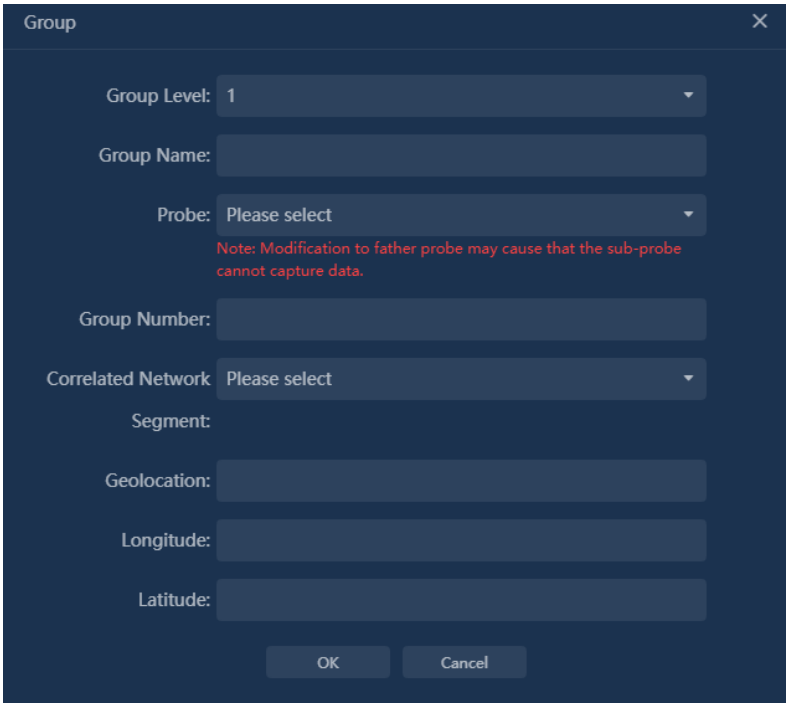


Terminals are managed using a hierarchical grouping method.

Step one, click on the '+' to add a group.



Step two, click on the icon next to the group '⊕ ' to add subgroups. Multiple subgroups can be added at the same level to complete the configuration of terminal group hierarchy.



Terminal groups need to be associated with probes and network segments to indicate the data collection area and scope of the group terminals.

Step three, add terminals. After selecting the group node, terminals can be added individually or in batches through import.

Note

The system can automatically discover terminals within the range based on the group-associated network segments and add them to the terminal list.

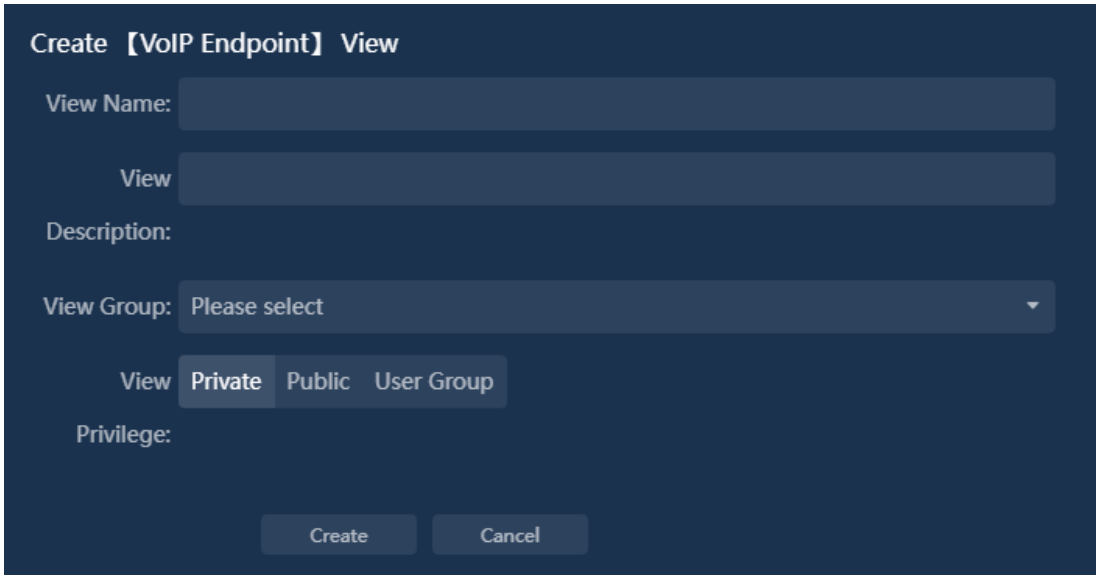
14.6.2. Terminal Monitoring

Click on the 'Terminal Monitoring' -> 'Terminal Monitoring' in the navigation menu to enter the monitoring page.

The terminal monitoring page includes the management and real-time monitoring of the monitoring view. By default, there is no monitoring view. The first step is to create a monitoring view.

Create a monitoring view

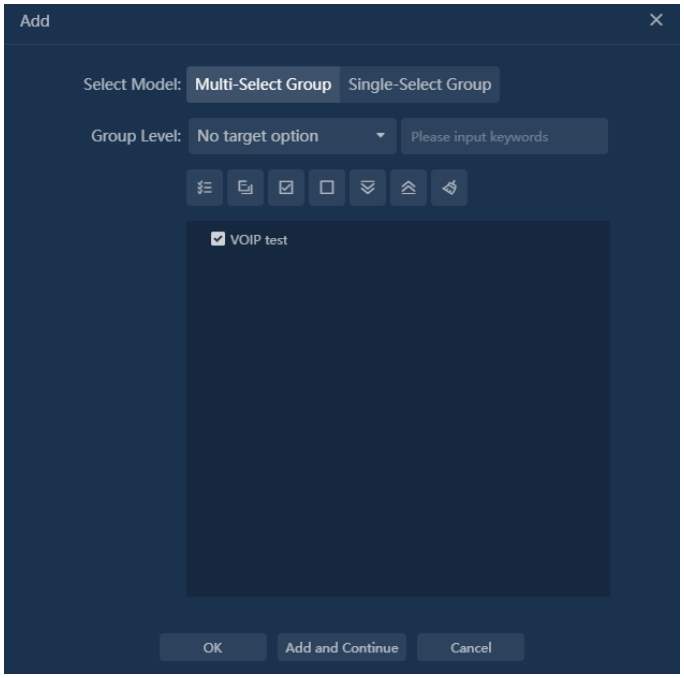
Click on the '+' icon to add a monitoring view, and a view configuration page will pop up, as shown below:



- Customize the input group name, the group name cannot be duplicated with other group names;
- Scene type, that is, different monitoring scene options. The default is application client terminal monitoring. After selecting 'VoIP terminal', it becomes VoIP monitoring scene. When adding monitoring clients, you can only select the corresponding client type for the scene, which corresponds one-to-one with the types in the terminal management group;

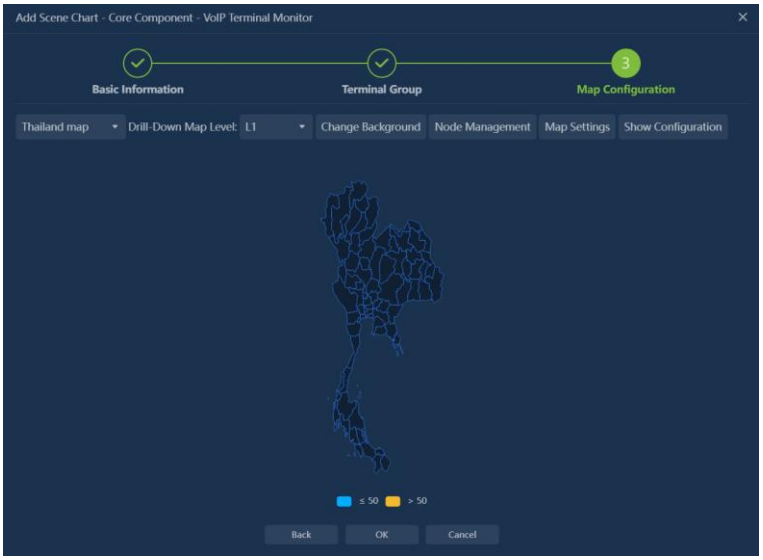
After entering the information, click the 'Create' button to generate an empty monitoring view. On the left side of the view, you can expand the monitoring component panel to configure the monitoring view through the components in the panel. You can also directly select 'Save and configure scene components' to start configuring the monitoring view.

Step 1, add monitoring terminals and select terminal groups.



- Supports multiple selections, add multiple at the same time
- For single selection, custom node names are supported;

After selecting, click 'OK' to configure the display map.



Finally, click the 'OK' button to save and complete the view creation.

Note

When creating a monitoring view, the node positions will be automatically displayed on the map based on the group's position information (geographical location name or latitude and longitude), and you can also drag the node positions with the left mouse button.

Real-time monitoring

The default refresh rate for the monitoring view is 1 minute, and the monitoring cycle is 1 minute.

- Monitoring indicators support customization, and node colors change based on the indicator value range.
- Right-click on the monitoring node, click on 'Terminal Analysis' to enter the terminal analysis page.

14.7. Backup Terminal monitoring User manual

Terminal monitoring is used to monitor different types of application client in various scenarios, including:

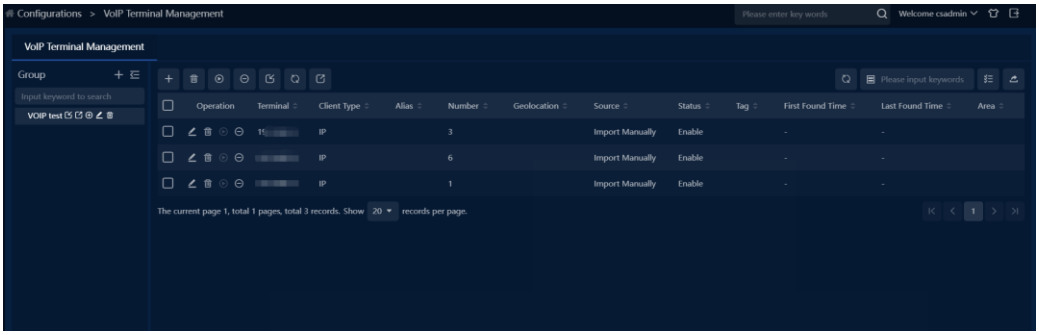
- VoIP terminal monitoring, by monitoring indicators such as jitter, delay, and packet loss of video (voice) terminals, abnormal terminals can be detected and the cause of the problem can be identified in a timely manner;
- Application client monitoring, by analyzing network performance indicators of terminal access to business systems (such as latency, number of sessions, and traffic), application service status and network quality can be monitored from the perspective of terminal experience, enabling quick problem identification.
- Business continuity exercise monitoring, by statistically analyzing business data, monitoring the status of business switch recovery for terminals participating in the exercise. For detailed functionality, please refer to the chapter on Backup Terminal monitoring.

The main functions include:

- Terminal Management: Used to maintain monitored terminals and terminal information (such as terminal type, alias, IP address).
- Terminal Monitoring: Define monitoring views as needed to monitor terminal status and alarm information in real time.
- Terminal Analysis: Analyze network performance and application performance from the perspective of terminals, and analyze and locate problems.
- Terminal Alarm Configuration: Define terminal alarms.
- Terminal Alarm Query: Query terminal alarm logs.

14.7.1. Terminal management

Click on the navigation menu, go to 'Terminal Monitoring' -> 'Configuration' -> 'Terminal Management' to enter the configuration page, and configure different terminals based on the scenario. The types include: Backup terminal management, VoIP terminal management, application client management. The terminal configuration process is basically the same. Taking VOIP terminal configuration as an example, it is shown in the figure below:

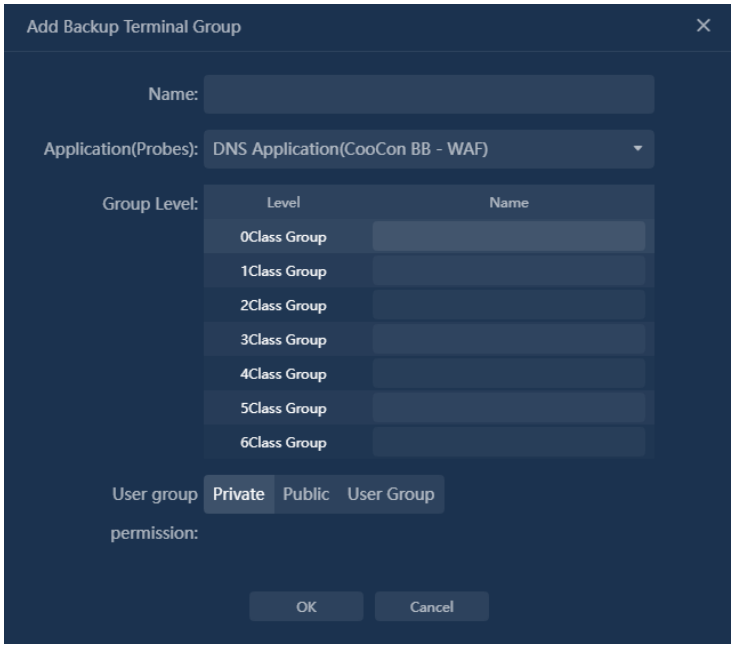


Add terminal group

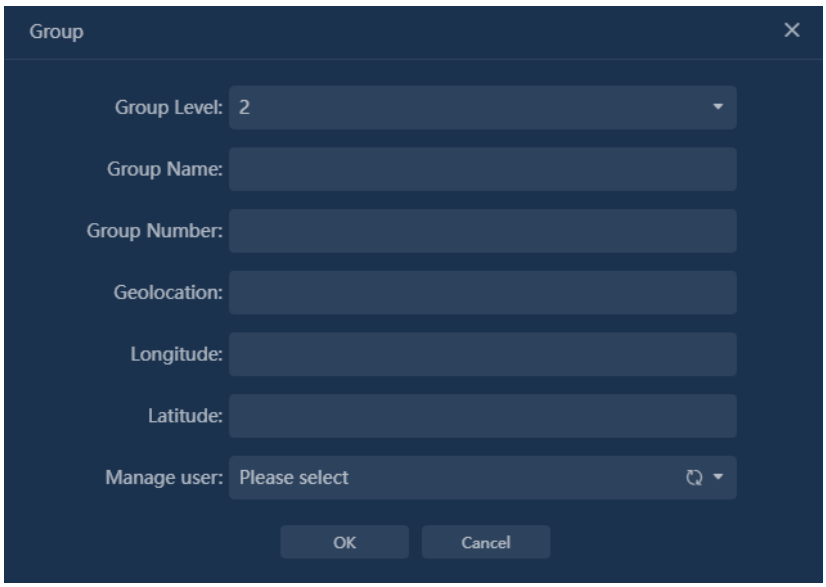
In the left tree view, click '+' to add terminal groups and define group levels. Operating steps:

Step one, fill in basic information.

Figure 14-1



- Applications (probes), only display applications bound to transaction groups within the authorized permissions, support multiple selections.
- Define group levels to clarify the meaning of group hierarchy. In terminal configuration, terminal monitoring group components, and alarm configuration, the group name can be directly displayed for a more intuitive and scenario-compliant experience.
- Supports up to 6 levels by default, with level names ranging from 1st group to 6th group.



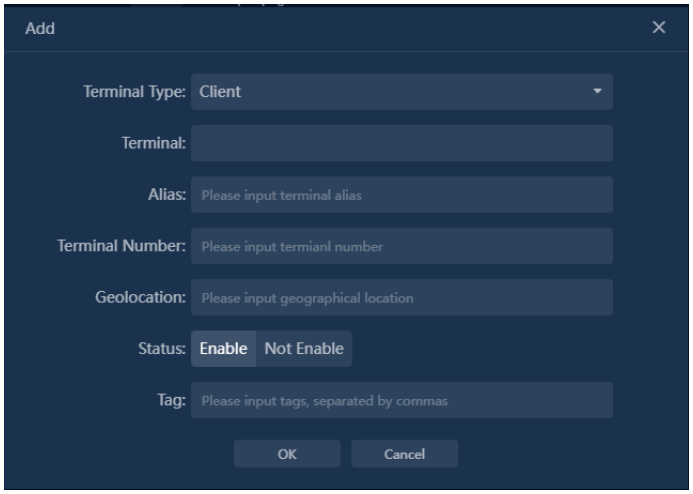
- Geographical location, corresponds to the location information on the map, from province to city to district. Built-in system, can be left blank
- Latitude and longitude, the latitude and longitude of the group on the map, can be left blank
- The purpose of geographical location and latitude and longitude is to automatically match the coordinates of the group based on the location and latitude and longitude when generating the map. When both location and latitude and longitude are filled in, latitude and longitude take priority in matching.

Add terminal

The ways to add terminals include manual form addition and template import.

The form addition method is as follows:

Figure 14-2

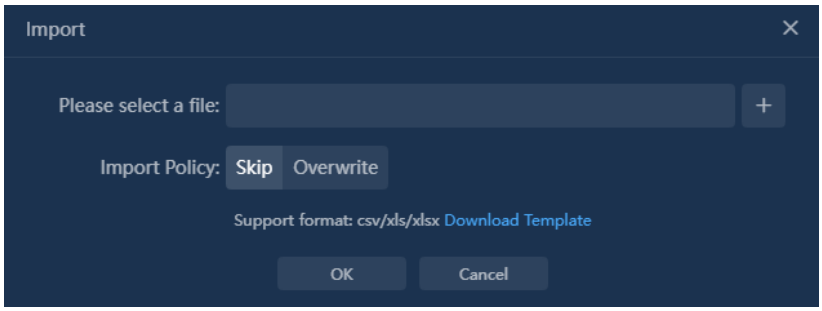


- *Terminal type, optional client IP, client subnet*
- Terminal Number, the number of the terminal, not required
- Geolocation, description of the final terminal location, not required
- Tag, keywords describing the terminal, multiple inputs allowed, not required.

Import/Export

Improve terminal and terminal group management efficiency through import.

Figure 14-3



- Support separate import for groups and terminals
- Export, only export groups and terminal information under selected groups.

14.7.2. Terminal Monitoring

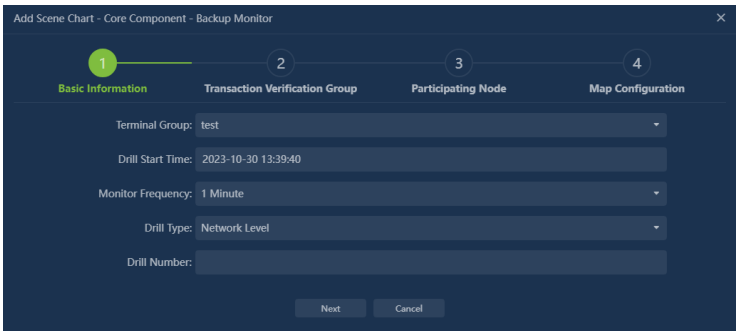
Click on the 'Terminal Monitoring' menu to enter the Backup Terminal monitoring page.

Create a monitoring view

Click the '  ' button to add a view.

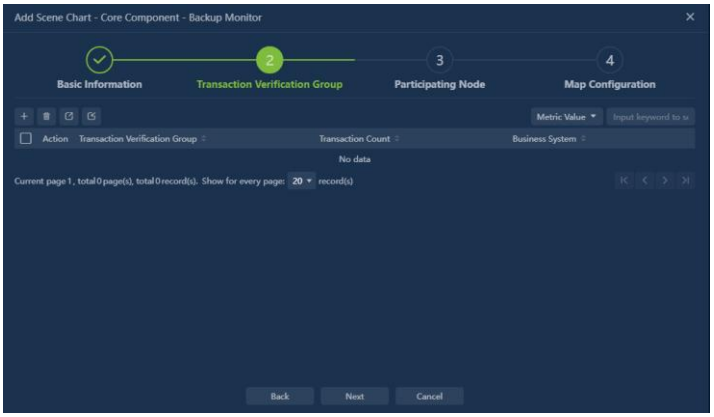
Step 1, Basic Information

Figure 14-4



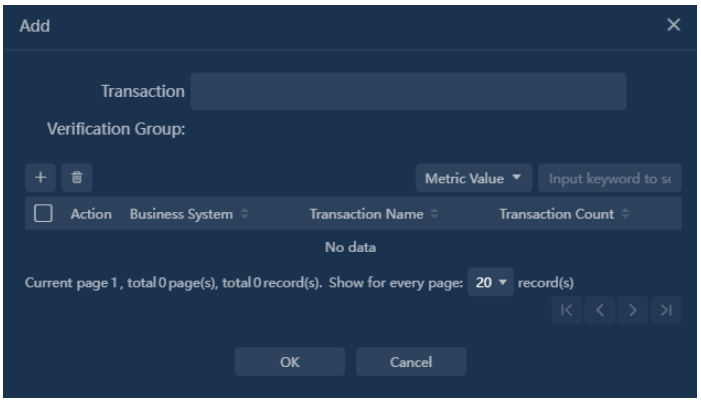
Step 2, configure transaction groups, determine transaction scope, and generate drill list.

Figure 14-5



- Add transaction group, select transactions (multiple selections), and display selected transactions in the list, and set transaction count for each transaction.

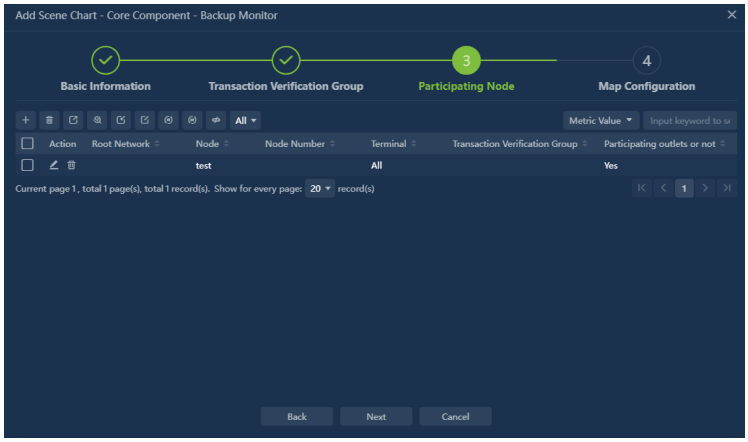
Figure 14-6



- Multiple transaction groups can be added, or imported quickly through templates.

Step three, configure participating Node, that is, select terminal groups.

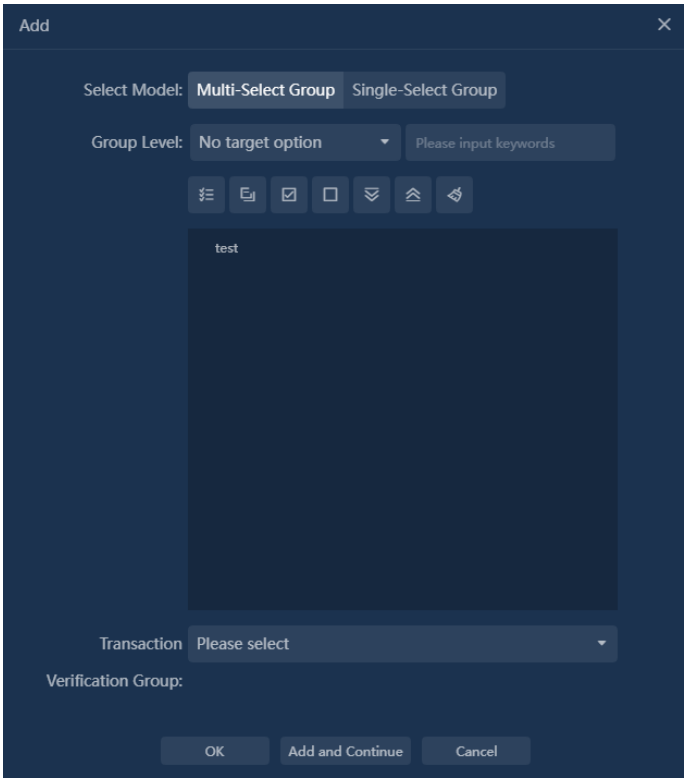
Figure 14-7



- Add, select participating branches

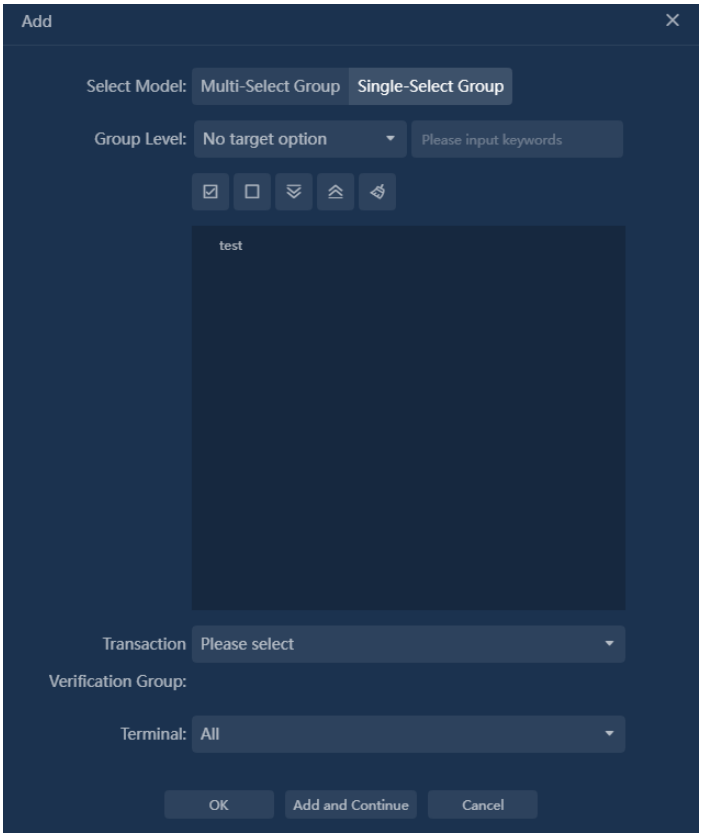
Multiple selection mode

Figure 14-8



Single selection mode

Figure 14-9



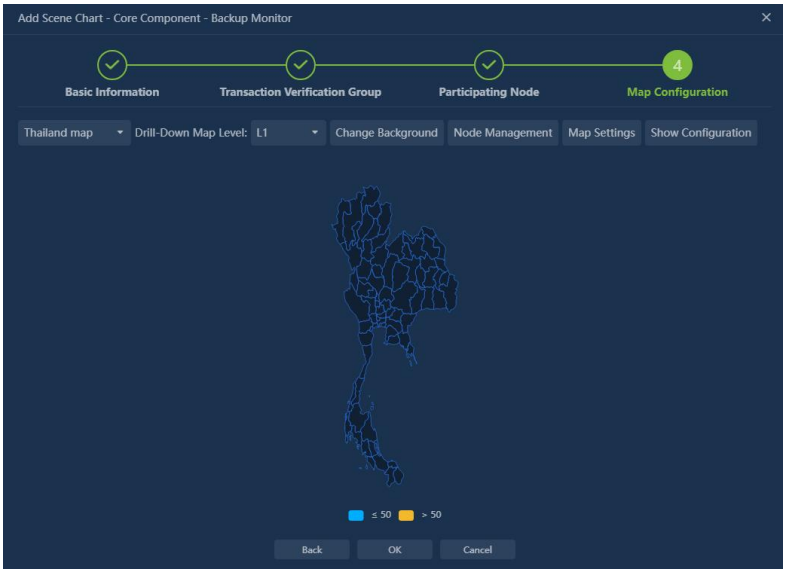
Enter terminal (i.e. terminal IP) at the same time, default to all terminals under the group when not entered.

Select associated transaction group.

- Participating branches can be quickly imported through templates.

Step four, configure the map

Figure 14-10



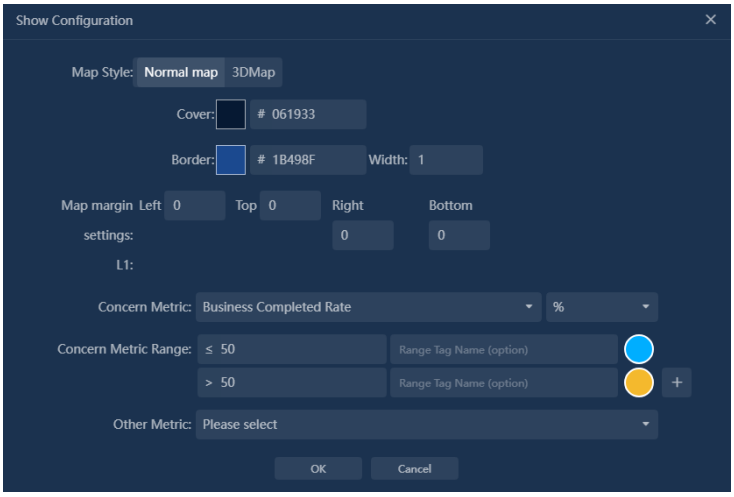
- Map, default to select national map. When not selecting a map, display the background image setting entry and upload background image. After selecting a map, the selected terminal groups are displayed on the map according to their geographical locations. If there is no location information (or when not selecting a map), they are randomly arranged in the upper left corner and support left mouse button dragging.

Dragging only changes the display position and does not change the actual configuration position information of the group.

When the map is opened for drilling, if the group location matches the drilling map location name, it will be displayed in the drilling map.

- Map drilling enables direct drilling into the map by clicking on the area on the map, supporting drilling down to the district level. For example, if the national map is clicked on Sichuan Province, it will drill down to the map of Sichuan Province.
- Click on 'Display Settings' to configure indicators and indicator color gradients.

Figure 14-11

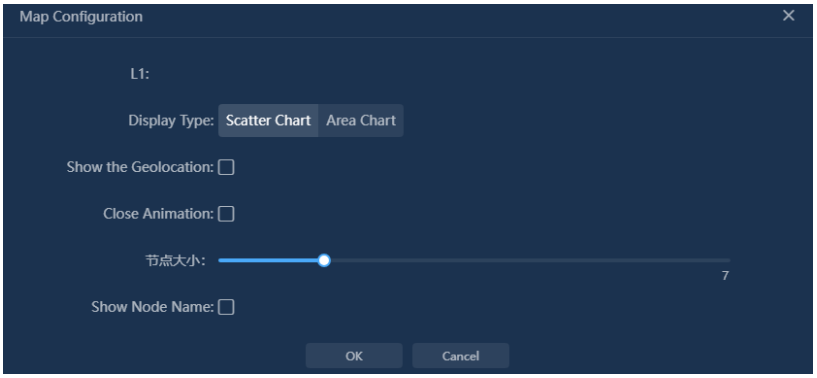


Pay attention to the indicators displayed in the grouped indicators and the color distribution of the map area, which are determined by the range of this indicator. Single selection

Attachment displays indicators, interactive indicators, and displays together with indicator items when the mouse is moved to a node or area. Multiple selection

- Map settings, configure map display type and effects

Figure 14-12



- Background image, including optional system-provided background images or uploaded background images

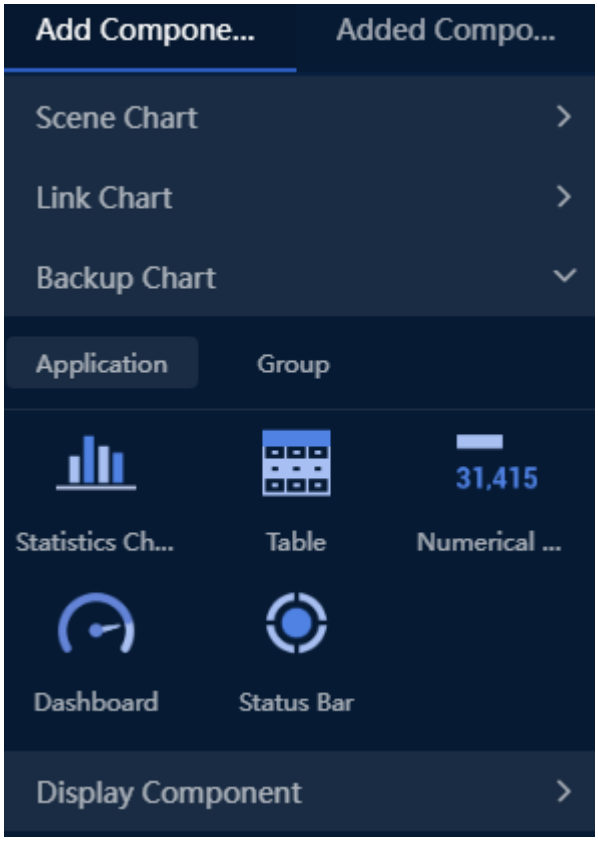
Step five, click OK to complete

- Configuration completed, generate monitoring view.

Figure 14-13

In the monitoring view, you can customize other view components. Click the left arrow on the view to expand the component list.

Figure 14-14

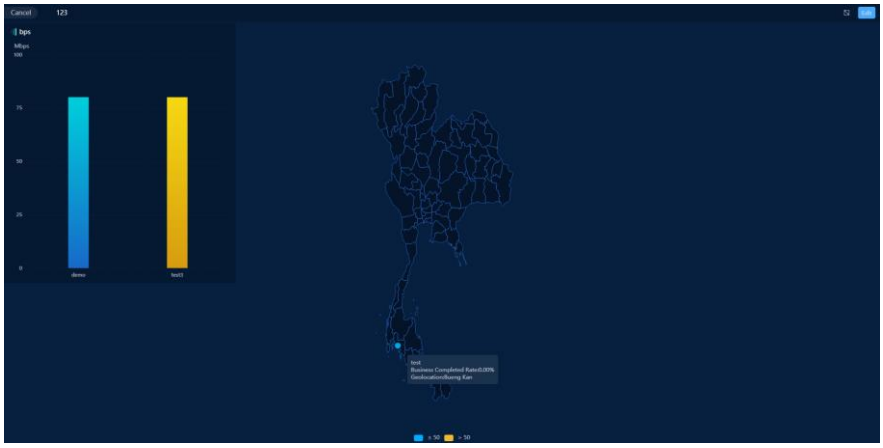


The component list includes link charts, application charts, terminal group charts, and display-type components. Click on the component chart to open the configuration window, add the chart component to the monitoring view, and the added component supports mouse dragging to change position and size.

Real-time monitoring

The refresh frequency of the monitoring view can be set to 10 seconds or one minute.

Figure 14-15



- Interactive Monitoring View

Interact on the map, move the mouse over the map area or node, and display the indicators in a tooltip manner. Right-click to analyze and jump to the terminal analysis view, and locate the group.

Figure 14-16

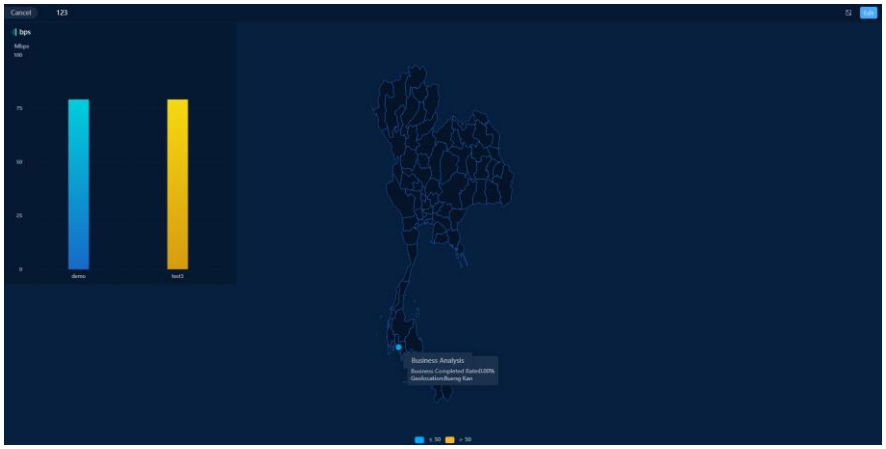
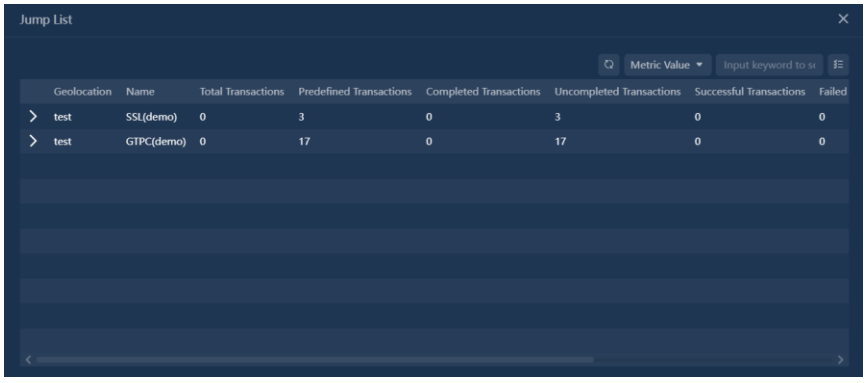
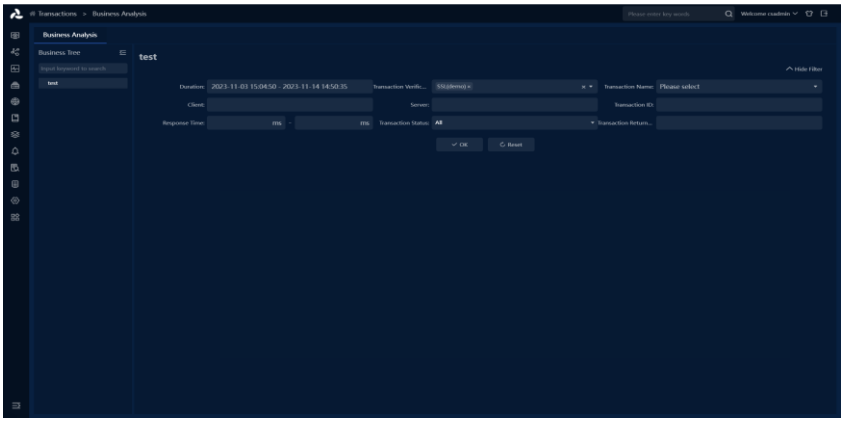


Figure 14-17



- List, click to jump to the terminal analysis view, and locate the group.

Figure 14-18



➢ Sticky interaction of bottom components

Click the button in the lower right corner to enable sticky interaction of bottom components. After enabling, the logic of the bottom components will be placed on top without changing the view effect. You can directly right-click on the bottom components at any position or any component layer to perform operations; After closing, it will be restored and only right-click operations can be performed on the bottom components.

Terminal Analysis

On the monitoring page, click on the nodes in the map and items in the list to enter the terminal analysis page. Display transaction details logs under corresponding conditions, support conditional queries.

Indicator

Grouped Indicators

Table 14-1

Indicator Name	Indicator Description
Business Completion Rate	The percentage of completed practice transactions in the predefined transaction count in the branch practice business list. If the transaction group has four transaction names: A, B, C, D, E, and each transaction name has a predefined transaction count of 2, when the completed transaction count of A is 1, the completion rate is 10%, and the completed transaction count is 1; When the completed transaction count of A is 2 or more (4), the completion rate is 20%, and the completed transaction count is 2; When the completed transaction count of A is 2 or more, and the completed transaction count of B is 4, the completion rate is 40%, and the completed transaction count is 4.
Time taken for completion of the drill	Duration from the start of the drill until the completion rate of the operation reaches 100%

Branch recovery rate	Proportion of recovered branches to the total number of participating branches Recovered branch count / Total branch count (Recovered branch refers to branches with an operation completion rate of 100%) Branch completion rate: Number of completed transactions / Total number of transactions
Predefined total number of transactions	Predefined total number of transactions in the business validation group
Total number of completed transactions	Total number of completed drill transactions
Total number of incomplete transactions	Total number of incomplete drill transactions
Total number of transactions	Actual total number of transactions
Number of transactions with no response	Actual number of transactions with no response, i.e., the number of transactions without a response message
Number of responsive transactions	Number of actual transactions with response, number of transactions with response messages
Number of successful transactions	Number of actual successful transactions, number of transactions with success return codes
Number of failed transactions	Number of actual failed transactions, number of transactions with failure return codes

Application Indicator

Table 14-2

Indicator Name	Indicator Description
Business recovery rate	The ratio of the number of business types that the business system completes transactions to the number of participating business types. For example, for ATM, the participating types include: A, B, C, D, E, 5 types. When the number of A transactions is greater than 1 and the number of other transactions is equal to 0, the completion rate of ATM channel is 20%
Predefined total number of transactions	Predefined total number of transactions in the business validation group

Total number of transactions	Actual total number of transactions
Number of transactions with no response	Actual number of transactions with no response, i.e., the number of transactions without a response message
Number of responsive transactions	Number of actual transactions with response, number of transactions with response messages
Number of successful transactions	Number of actual successful transactions, number of transactions with success return codes
Number of failed transactions	Number of actual failed transactions, number of transactions with failure return codes

15. Scenario Analysis Template

15.1. User manual for segment monitoring scenarios

15.1.1. Functional background

1. A dedicated network provided by communication operators to individual customers, making data transmission for customer business faster, more reliable, and more trustworthy. Due to the higher cost of segment compared to regular network fees, customers hope to monitor the quality and stability of the segment in real-time, accurately alert and resolve network failures, and ensure the availability of the segment; And assist in decision-making for expanding or reducing the bandwidth of the dedicated network, making the cost of using the segment more reasonable.
2. When congestion occurs in the segment, customers can only monitor the overall link traffic data KPI quality through the current product, resulting in poor monitoring effectiveness and difficulty in quickly analyzing and focusing on key KPIs for in-depth analysis.
3. Enhance the specialized monitoring and analysis capabilities for product incubation and promotion, and improve the competitiveness of the product.

15.1.2. Functional value

1. Support comprehensive quality monitoring of segments from dimensions such as network congestion, packet loss retransmission, session abnormalities, network latency, and traffic interruption. Support good monitoring display effects.
2. Support quick definition of segments for various data types and data, including physical links (including aggregated links), subnet sublinks, MAC sublinks, and virtual interface sublinks. Built-in multidimensional segments monitoring alarms, support customization of segments monitoring alarm trigger conditions, and support intelligent baseline alarms.
3. Support automatic localization of abnormal segments and display of alarm information. Support fast analysis and abnormal localization of alarm information from dimensions such as IP, IP session, application, and QoS.

15.1.3. Functional Terminology

Segment: A dedicated network provided by a communication operator to a customer, making the data transmission of customer's business faster, more reliable, and more trustworthy.

Segment Group: A group formed by multiple segments. In the business perspective, it is generally used for label management of head office segment and branch segment.

15.1.4. Functional description

The templates for segment monitoring scenarios mainly consist of three major functional features: segment management, real-time monitoring, and quick analysis.

Segment Management

1. Supports adding, deleting, modifying, and querying segment and adding, deleting, modifying, and querying segment groups.
2. Supports default alarm policies and built-in multidimensional segment monitoring alerts; Supports custom triggers for segment monitoring alerts and supports intelligent baseline alerts.
3. Support configuring corresponding physical links (including aggregated links), subnet sublinks, MAC sublinks, virtual interface sublinks, and other data types and data DSCP marking values and aliases; Support batch import of DSCP name table.

Real-time monitoring

1. Statistically and monitor the quantity, normal and abnormal conditions of segment in a visual way; Abnormal conditions can be subdivided into network congestion, packet loss retransmission, session abnormalities, network latency, and traffic interruption, etc., to comprehensively monitor the quality of segment.
2. Support monitoring and analysis modes; In monitoring mode, the monitoring cycle can reach minute-level accuracy, and in analysis mode, the data of the past week can be viewed.
3. Support fuzzy query of segment, matching based on line name and DSCP marking value.

Quick Analysis

1. Supports alert events through statistical abnormal lines, further analyze and locate the abnormal root cause based on the alert events from multiple dimensions such as QOS, IP, IP session, and application.
2. Normal lines support further viewing the operation status of the line from multiple dimensions such as QOS, IP, IP session, and application.

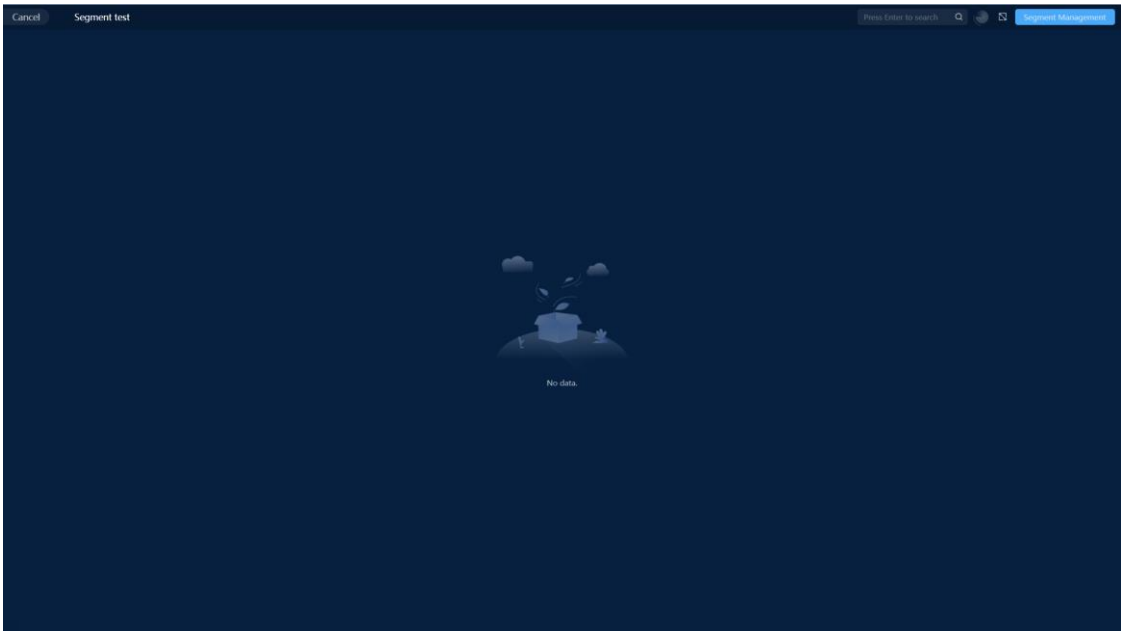
15.1.5. Operation Guide

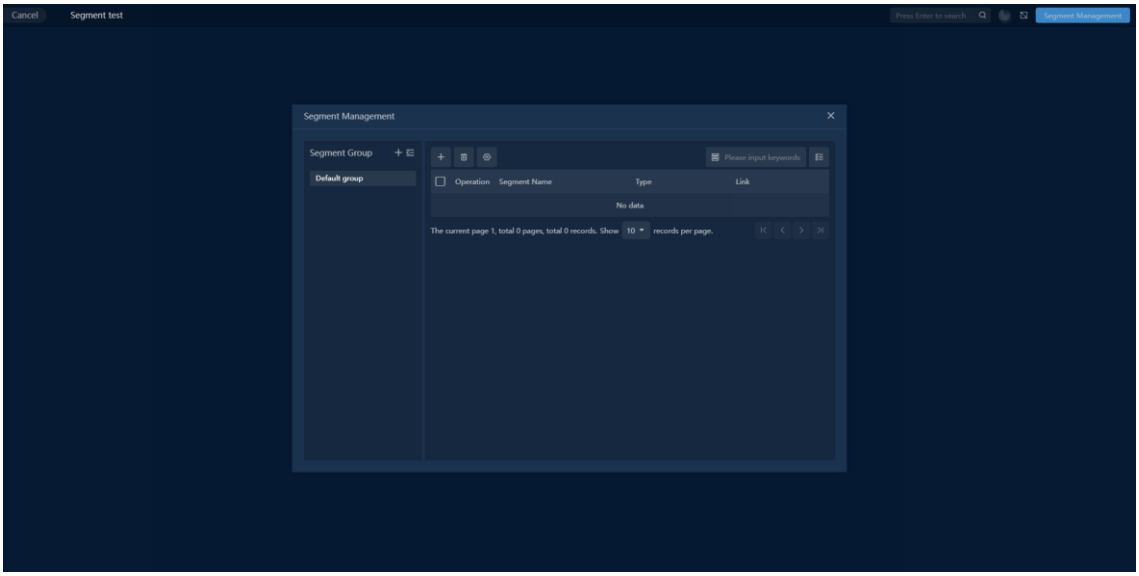
Built-in monitoring scene view in the UPM product's [Scene Center] module. Built-in line monitoring scene templates in the [Template Center], where one template can create multiple view instances.

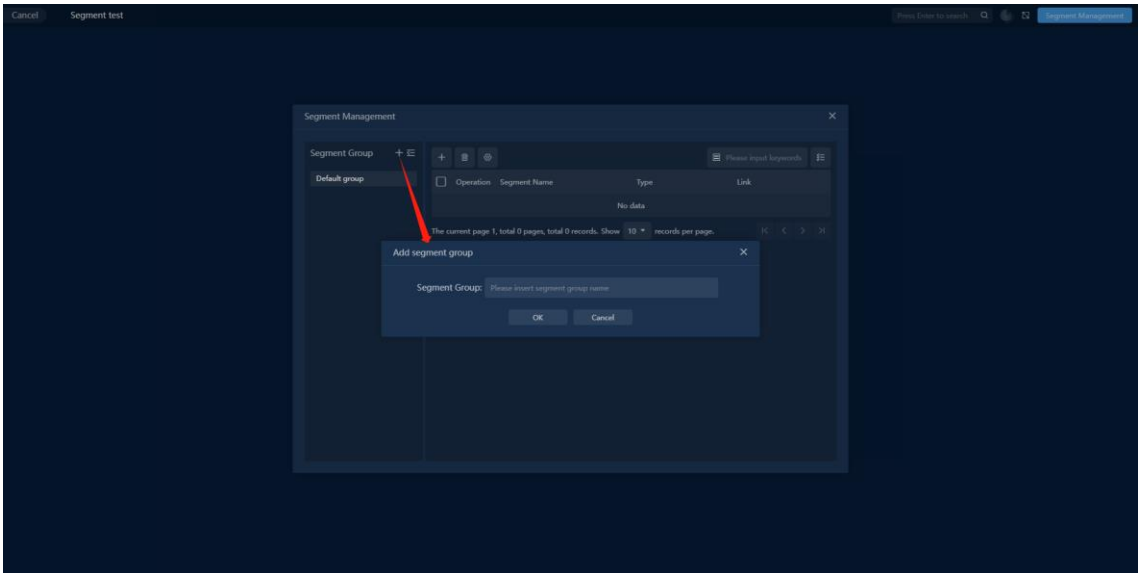
15.1.6. Add segment group

The segment management page can be opened by clicking on segment management on the [Segment Monitoring Scene View] home page, which by default has no line information. As shown in the following figure:

In the segment management page, click [Add] in the left [segment Group] list to open the Add Segment Group form dialog. Enter the group name and click OK to complete the creation of the segment group, as shown in the following figure:



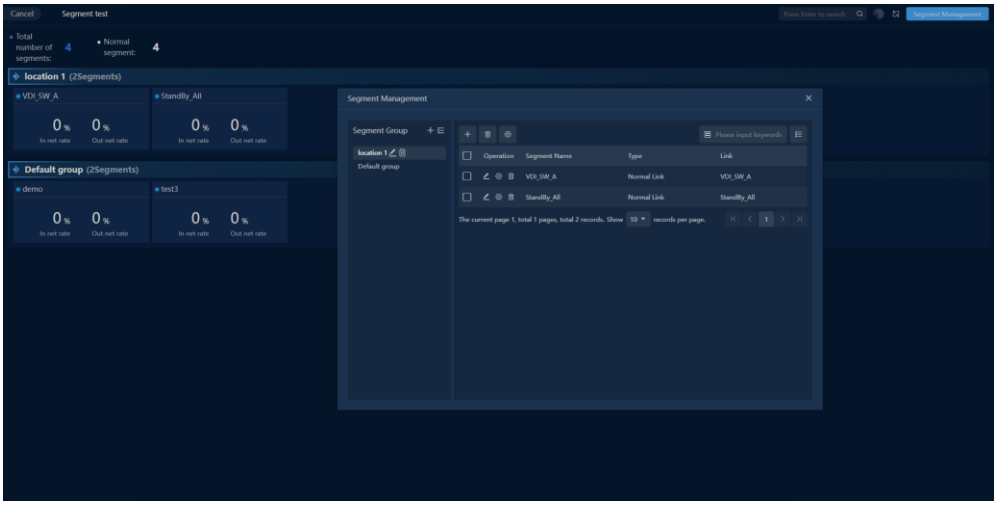


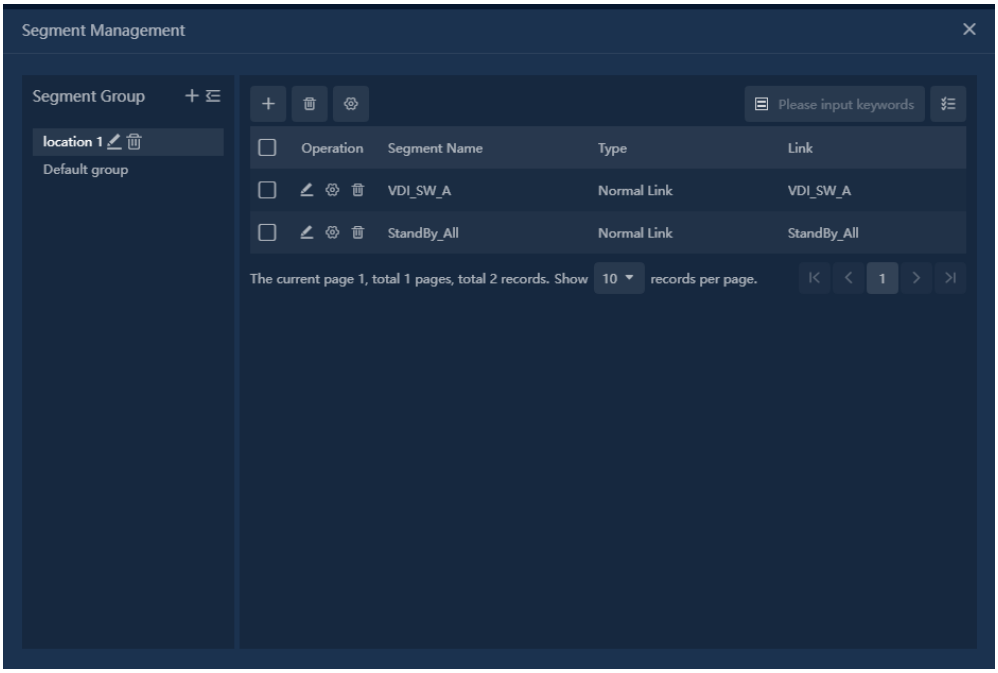


15.1.7. Add Segment

In the segment management page, select a segment group and click [Add] above the table on the right side to open the Add segment form dialog. Select the link type, link, enter the segment name, and select the segment group to add the segment.

The link type supports physical links (including aggregated links), subnet sublinks, MAC sublinks, virtual interface sublinks, etc., and supports multiple selections. The link supports functions such as search filtering before or after search filtering, reverse selection, clear selection, and display selected items. When the segment name is not entered, the link name is taken by default.



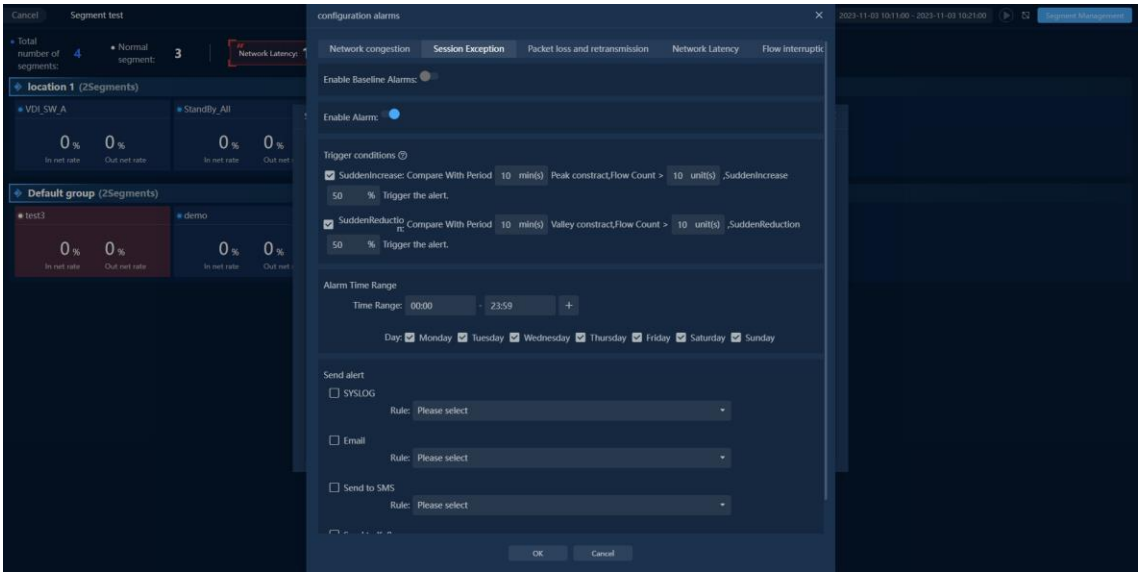


15.1.8. Configure segment alarm strategy

After adding a segment, you can configure the alarm strategy for the existing segment. The system will have a set of alarm rules built in. If you do not customize the alarm strategy, the built-in alarm strategy will be used.

In the segment management page, click on a segment [Configure Alarm] to open the Configure Alarm Strategy form dialog.

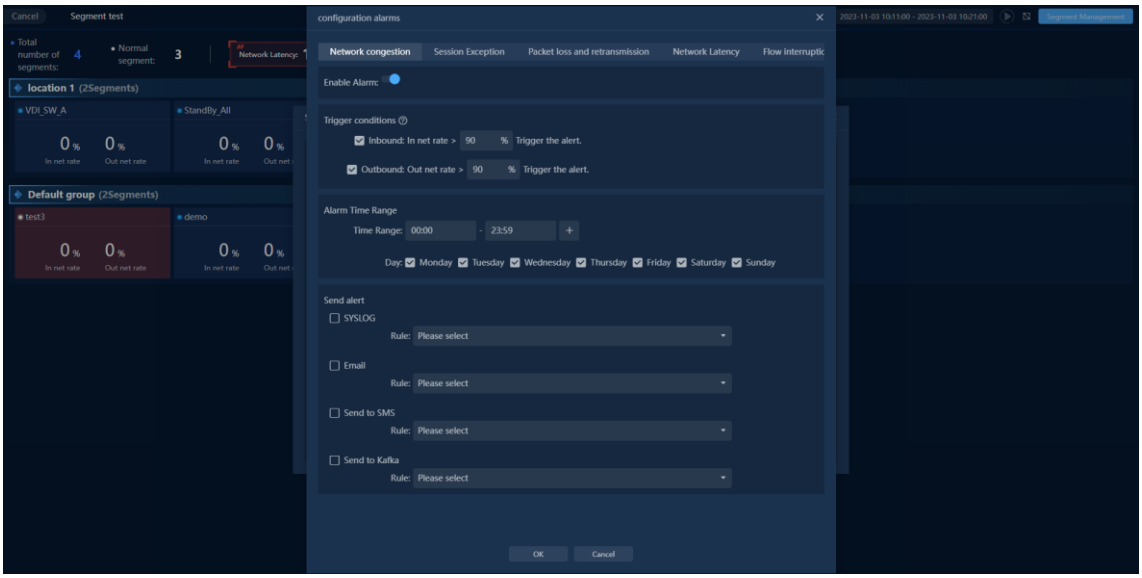
- Batch operations are also supported for configuring alarm strategies. After selecting multiple segments in the existing segment list, click [Batch Configure Alarm].



In the Configure Alarm Strategy form dialog, you can configure alarms for five dimensions: network congestion, session abnormality, packet loss retransmission, network delay, and

traffic interruption. In addition, session abnormality and network delay dimensions can be connected to the intelligent baseline platform and generate intelligent baseline alarms.

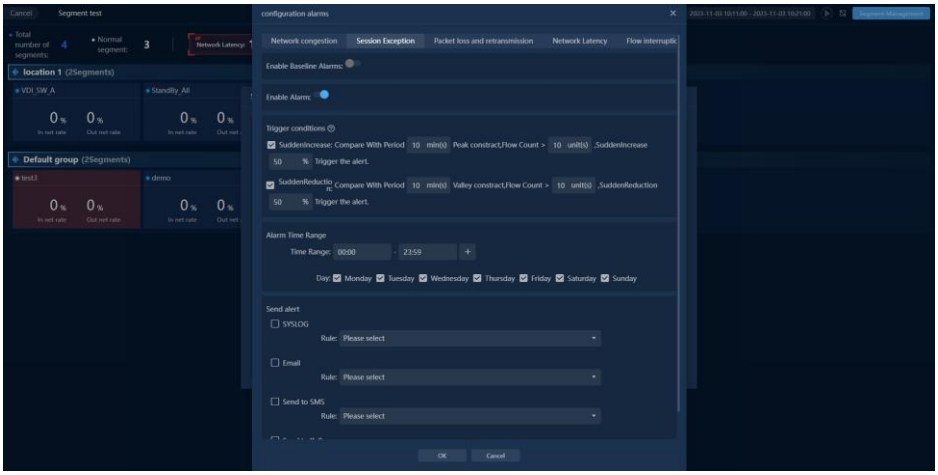
1. **Network congestion** Default enable alert, enter the threshold of inbound utilization rate in the inbound direction or outbound utilization rate in the outbound direction in the trigger condition area, select the alert period (time range, date range), configure the alert sending method (syslog, email, SMS, kafka), and click [OK] to complete the network congestion alert configuration. As shown in the figure below:



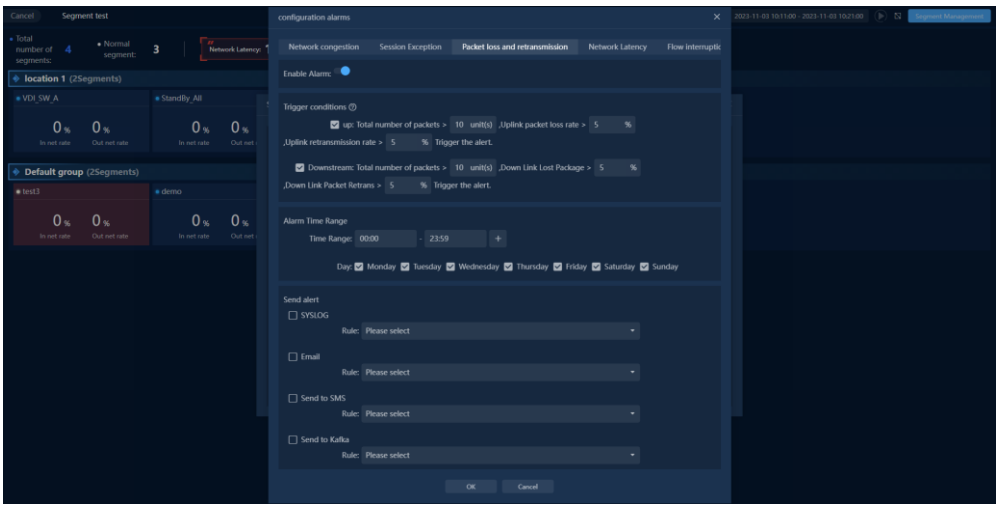
Alert trigger conditions: separate calculation for inbound and outbound (duration is calculated separately), the alert is not triggered outside the valid period. Alert description: xx, network congestion alert. Start time: year-month-day hour: minute, indicator > x%, duration, continuous status; Year-month-day hour: minute indicator = x%. Just triggered the alert without duration; The continuous trigger alert status is in progress (the indicator is based on the data of the past minute and keeps updating); After the continuous trigger alert ends, the status is set to finished (the indicator is based on the data at the end time).

2. **Session exception** Default enable alarm, disable intelligent baseline alarm. Enter the threshold values for minutes, total sessions, and increase value in the trigger condition area under the surge direction, or the threshold values for minutes, total sessions, and decrease value in the trigger condition area under the drop direction. Select the alarm period (time range, date range) and configure the alarm sending method (syslog, email, SMS, kafka). Click [OK] to complete the configuration of session abnormal alarm. As

shown in the figure below:



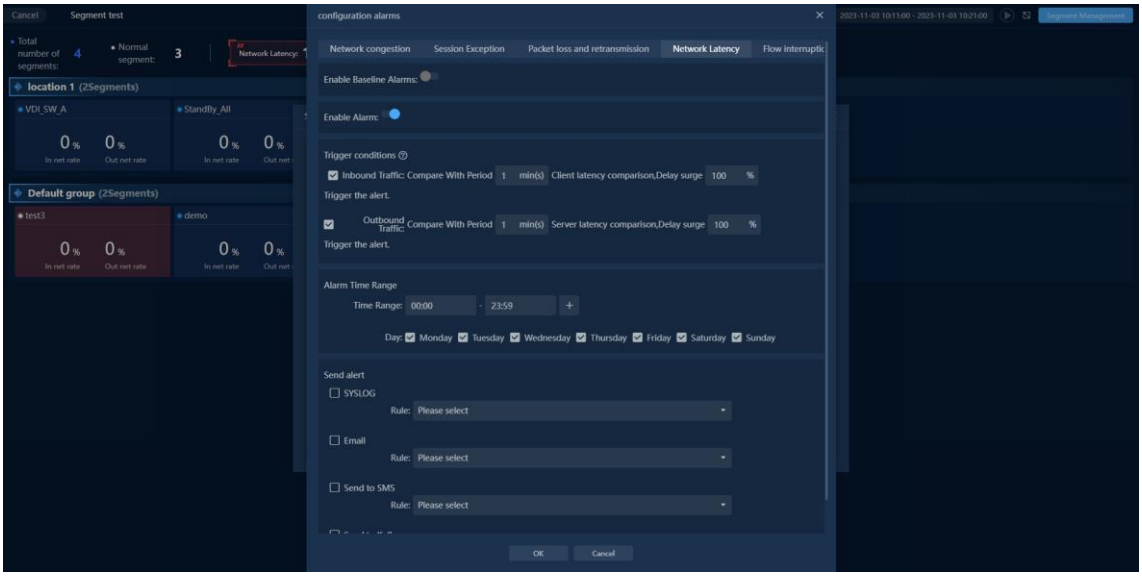
3. **Alarm trigger** conditions: separate calculation for surge and drop (duration is calculated separately), alarm is not triggered outside the valid period. Alarm description: xx, session abnormal alarm. Start time: year-month-day hour: minute, total sessions increase/decrease x%, duration, continuous status; year-month-day hour: minute index=x%. No duration for just triggered alarm; Continuous triggered alarm is in progress (the index is based on the data of the past minute and keeps updating); After the continuous triggered alarm ends, the status is set to finished (the index is based on the data at the end time).
4. **Packet Loss and Retransmission** Default enabled alert, enter the threshold values for total packets in the upstream direction, upstream packet loss rate, upstream retransmission rate, or total packets in the downstream direction, downstream packet loss rate, downstream retransmission rate in the trigger condition area. Select the alert period (time range, date range), configure the alert sending method (syslog, email, SMS, kafka), and click [OK] to complete the configuration of packet loss retransmission alert. As shown in the figure below:



Alert trigger conditions: separate calculation for upstream and downstream (duration is

calculated separately), the alert is not triggered outside the valid period. Alert description: xx, packet loss retransmission alert. Start time: Year-Month-Day Hour: Minute, indicator > x%, duration, continuous status; Year-Month-Day Hour: Minute indicator = x%. Just triggered the alert without duration; The continuous trigger alert is in progress (the indicator is based on the data of the past minute and keeps updating); After the continuous trigger alert ends, the status is set to finished (the indicator is based on the data at the end time).

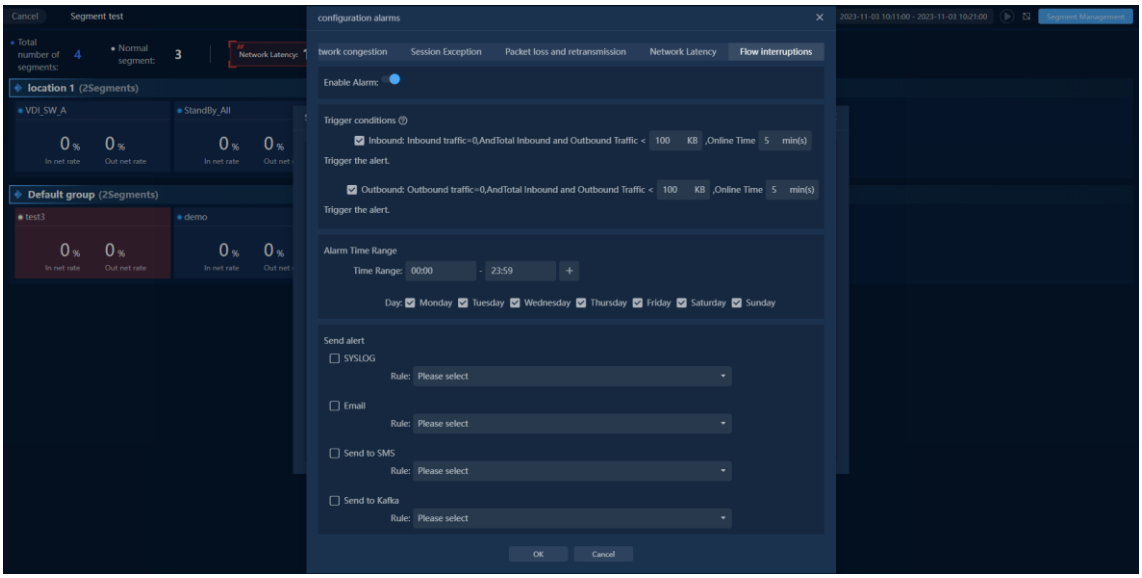
5. **Network Latency** Default enable alarm, disable intelligent baseline alarm. Enter the minutes, burst value, etc. threshold for the inbound direction or the minutes, burst value, etc. threshold for the outbound direction in the trigger condition area. Select the alarm period (time range, date range) and configure the alarm sending method (syslog, email, SMS, kafka). Click [OK] to complete the network latency alarm configuration. As shown in the figure below:



Alarm trigger condition: Separate calculation for client and server (duration is calculated separately), alarm is not triggered outside the valid period. Alarm description: xx, network latency alarm. Start time: Year-Month-Day Hour: Minute, metric burst x%, duration, continuous status; Year-Month-Day Hour: Minute metric = x ms. No duration for just triggered alarm; Continuous triggered alarm is in progress (the metric is the data of the past minute, continuously updated); After the continuous triggered alarm ends, the status is set to finished (the metric is the data at the end time point).

6. **Traffic Interruption** Enable default alerts, enter thresholds for total traffic and duration in the trigger condition area for inbound or outbound direction, select alert period (time range, date range), configure alert sending methods (syslog, email, SMS, kafka),

and click [OK] to complete the configuration of traffic interruption alerts. As shown in the figure below:



Alert trigger conditions: separate calculations for inbound and outbound (duration), alerts are not triggered outside the valid period. Alert description: xx, traffic interruption alert. Start time: year-month-day hour: minute, indicator=0, duration, continuous status. Continuous triggering alert status is ongoing; After continuous triggering alert ends, the status is finished.

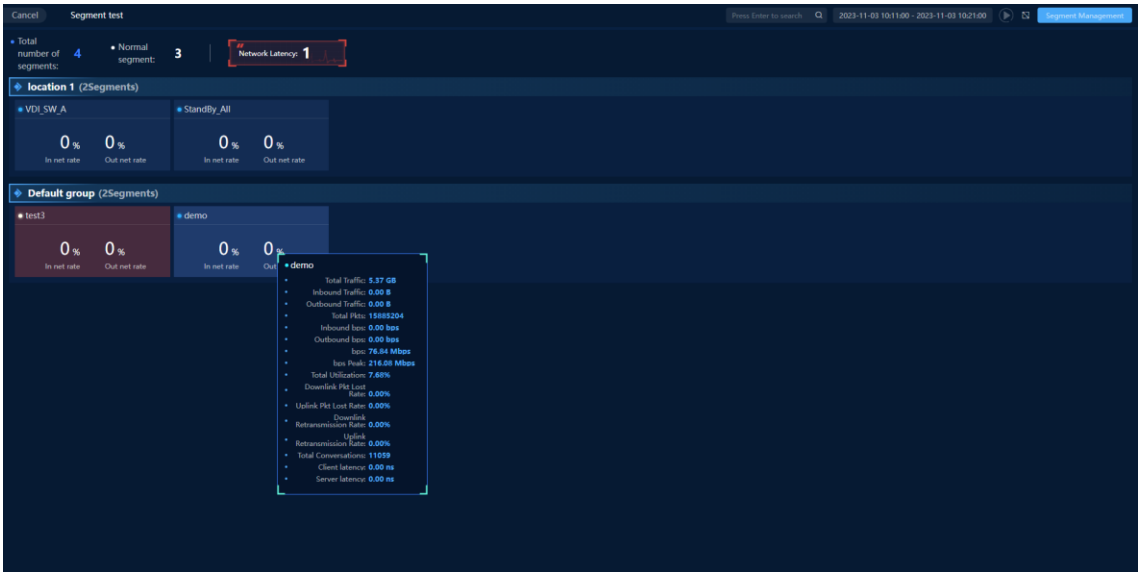
15.1.9. Monitoring segment

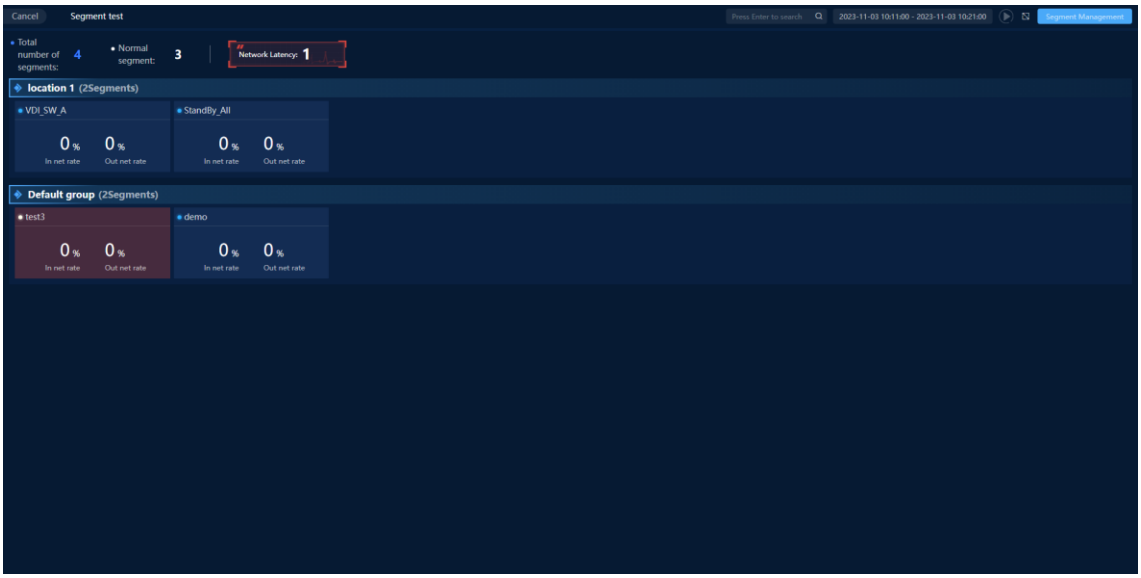
After completing the alarm strategy configuration, you can monitor and view the normal and abnormal status of the segment under each segment group in the segment monitoring scene view homepage. The default mode is monitoring mode: monitoring the status of the segment in the past 1 minute. Click the [Time Component] on the top right of the toolbar to switch to analysis mode. In analysis mode, you can view the historical data of the segment by selecting a time range of up to one week. When hovering over a specific segment, you can view the configuration indicators of that segment.

By default, it is sorted in descending order based on the highest inbound or outbound utilization rate under each group.

- When there is abnormal segment, the abnormal segment is sorted first, and the abnormal segment with the highest inbound or outbound utilization rate are sorted in descending order. The normal segment is sorted last, and the normal segment with the highest inbound or outbound utilization rate are sorted in descending order.

As shown in the following figure:





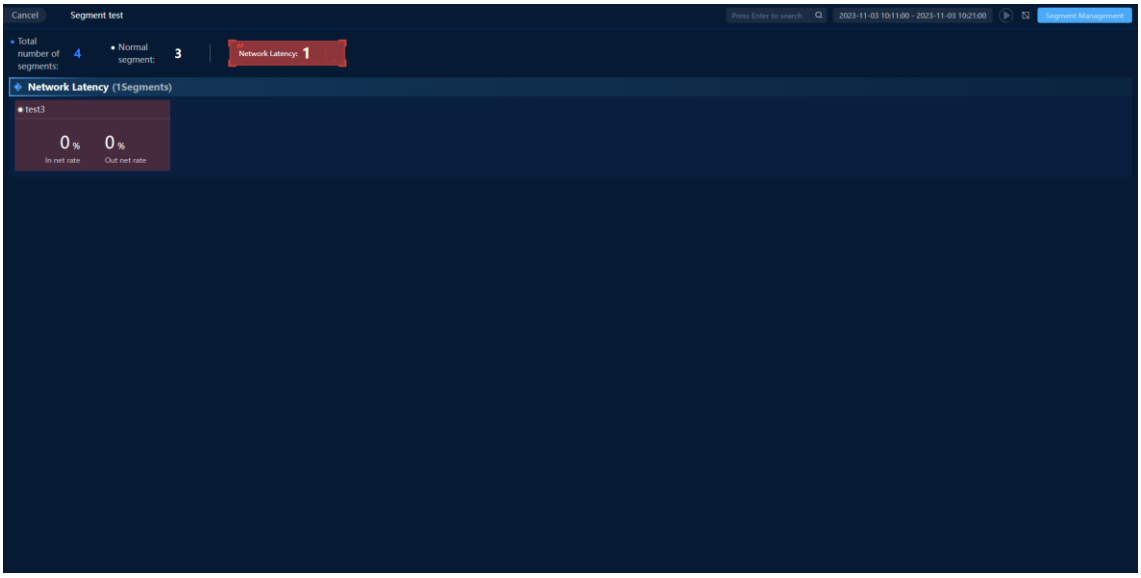
By default, the total number of segments, normal segment, network congestion/packet loss retransmission/session abnormality/network delay/traffic interruption content is not displayed. When there is segment data, the total number of segments, normal segment, network congestion/packet loss retransmission/session abnormality/network delay/traffic interruption statistics are displayed.

When there is abnormal segment data, you can filter the target alarm type data.

- Clicking on network congestion/packet loss retransmission/session abnormality/network delay/traffic interruption will display the abnormal data at the top below, hiding the original segment data. Clicking again will hide the abnormal data

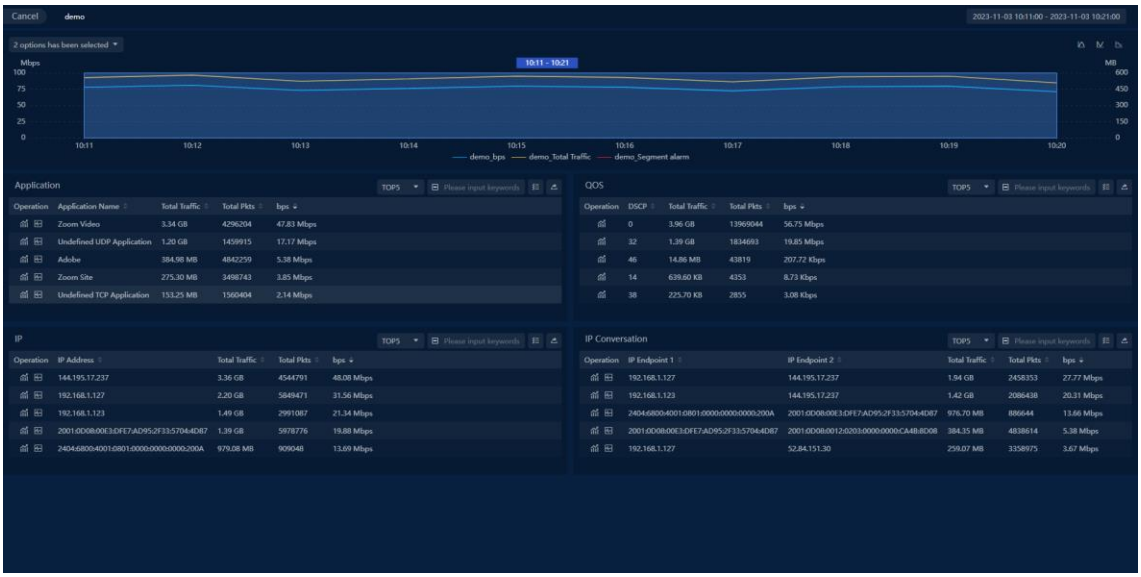
and display the original segment data. For example, at a certain moment, it shows network congestion 10. Clicking will display the abnormal data of 10 segment at the top below. Clicking again will hide it.

As shown in the following figure:



15.1.10.Analyze segment

In the home page monitoring mode and analysis mode, you can perform in-depth analysis on specific segment. Click on a specific segment to enter the analysis page of that line; If you click on an abnormal segment, the analysis page will display the alarm data for that abnormal segment. As shown in the following figure:



On the segment analysis page, it is mainly divided into segment alarms, trend chart display, application, QoS, IP, and IP session dimension statistics table areas. You can select a time period to view the data situation of each area within a certain time range.

Click on a specific alarm information in the segment alarm table to analyze that alarm and refresh the data in the trend chart indicators, trend chart time range, and application, QoS, IP, and IP session dimension statistics table. For example, for a traffic interruption alarm in the segment alarm, after clicking on [Analyze Alarm], the trend chart below will display the trend of inbound and outbound traffic indicators, and the application, QoS, IP, and IP session dimension statistics table will display the inbound and outbound traffic indicators in descending order of size. As shown in the following figure:

Trend Chart: Displays the historical trend of selected indicators for the segment within the selected time range. The time range selected will refresh the application, QoS, IP, and IP session dimension statistical table data in a linked manner.

Application, QoS, IP, and IP session dimension statistical table: By default, it displays the total byte count, total packet count, and bit rate indicator fields. When linked with analysis alerts, it will switch to indicators related to alert dimensions.

Session anomaly and network latency intelligent baseline alerts: If intelligent baselines are enabled in [Alert Configuration], you can view intelligent baseline alert log data in the segment alert table on the segment analysis page. Operation, start time, and alert type remain the same as the original field content. Alert Description: Fills in the alert details of intelligent baseline alerts.

15.1.11. Q&A

Does the segment support custom monitoring metrics?

All monitoring metrics in segment monitoring are associated with metrics in alarm policies and do not support separate customization of monitoring metrics.

How to enable and generate alerts for intelligent baseline alarms?

Session anomalies and network latency alarm functions support intelligent baselines and generate alerts. It is not enabled by default. After enabling intelligent baselines, collection logs are generated in the Intelligent Baseline Management and baseline tasks are started. When there is an alarm, alert logs need to be generated on the segment alarm page. Adding a baseline task for a certain link in the Intelligent Baseline Management does not automatically enable the intelligent baseline for the relevant link in the segment monitoring scene view template. Only when the intelligent baseline task in the segment monitoring scene view template is enabled, it will start.

- After connecting to the UPM on the Intelligent Baseline Platform and then disconnecting, the Intelligent Baseline switch in the segment monitoring is turned on normally, but no data is displayed.
- When the Intelligent Baseline Platform is not connected to the UPM, the Intelligent Baseline switch in the segment monitoring is disabled. Prompt: Not logged in to the Intelligent Baseline Platform, please log in to the Intelligent Baseline Management.
- The number of baseline indicators in the Intelligent Baseline Indicator Management has exceeded the authorized quantity. Enabling the Intelligent Baseline in the segment monitoring is unsuccessful. Prompt: The number of baseline authorizations has reached the limit. The authorized quantity is X, Y has been used, and Z will be added this time.
- The alarm sending configuration here is not related to the Intelligent Baseline. The Intelligent Baseline alarm function is not affected by the alarm switch.

15.2. IP Address Conflict Monitoring

15.2.1. Scenario Introduction

15.2.1.1 Scenario Background

IP address conflicts can cause abnormal communication between conflicting hosts, and in severe cases, it can slow down the entire network or even cause network failure. Therefore, network administrators hope to promptly detect IP address conflict issues in the network and quickly locate and resolve the problems.

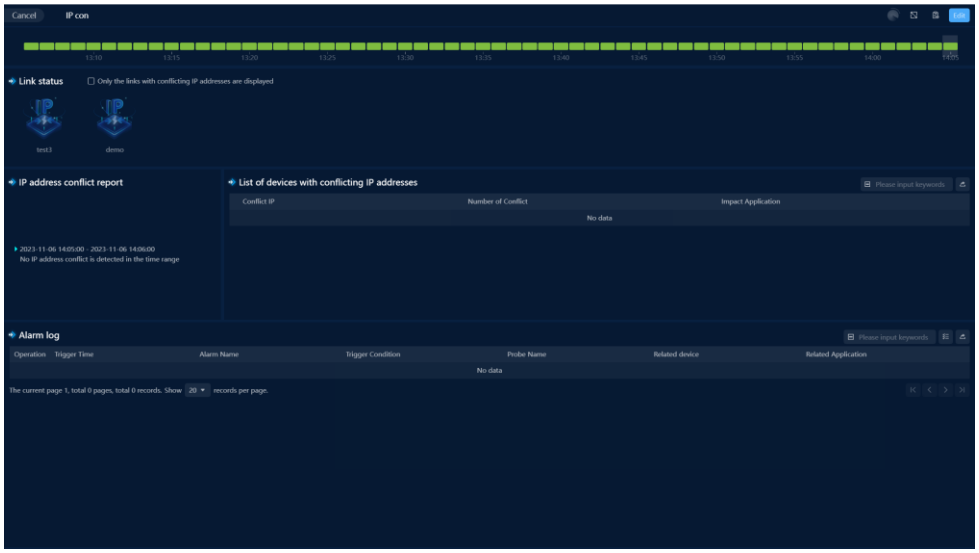
15.2.1.2 Scenario Value

- Used to monitor the occurrence of IP address conflicts in the network.
- When an IP address conflict occurs, it can notify network administrators in real-time through SMS or email.
- When an IP address conflict occurs, it can quickly locate the host where the conflict is happening.
- When there is an IP address conflict, it can quickly determine the scope of the conflict's impact on business/applications.

15.2.2. Analysis Guide

15.2.2.1 Scenario View

In the custom metric monitoring page, the system has built-in the 'Scenario Monitoring and Analysis' group, which includes the IP address conflict monitoring view. It is used to monitor and analyze IP address conflicts in the network. As shown in the following figure:



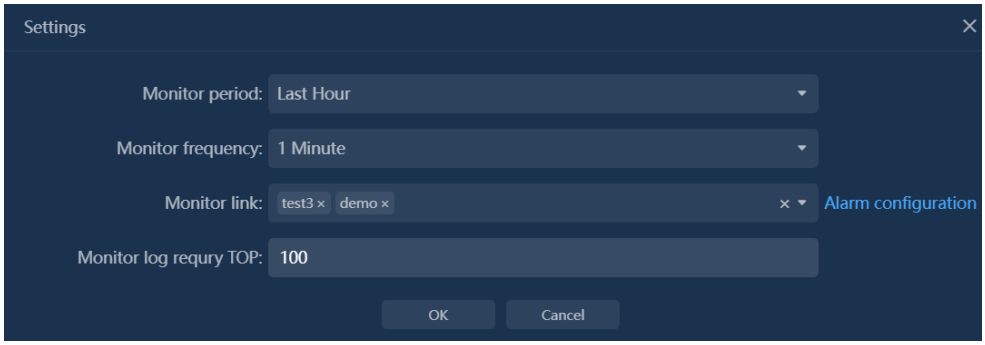
The IP address conflict view provides two modes: monitoring and analysis. By the status of the timeline, you can clearly see if there is an IP address conflict within the current time range. During the monitoring process, if an IP address conflict alarm is triggered, the alarm log details will be sent to the specified SMS, email, or syslog server. In analysis mode, by selecting a time range on the timeline, you can view the statistical information of the triggered alarms within the selected time range.

In the alarm log, you can directly see the scope of the impact of IP address conflicts, including the devices where the conflicts occur, as well as the affected applications or services, guiding users to perform subsequent troubleshooting operations. For a single alarm log, you can perform trend analysis, packet download, and packet decoding operations.

15.2.2.2 Scenario Configuration

When entering this view for the first time, you need to configure the monitoring range of the links. Please use the right-click menu in the view editing mode to configure the monitoring data.

The monitoring data configuration dialog box is shown in the following figure:



15.3. Route Loop Monitoring

15.3.1. Introduction

15.3.1.1 Background

When a loop occurs, there may be slow network and application access, network packet loss, or even the inability to provide services normally. Usually, locating and discovering network loops in large networks is quite difficult.

15.3.1.2 Scenario Value

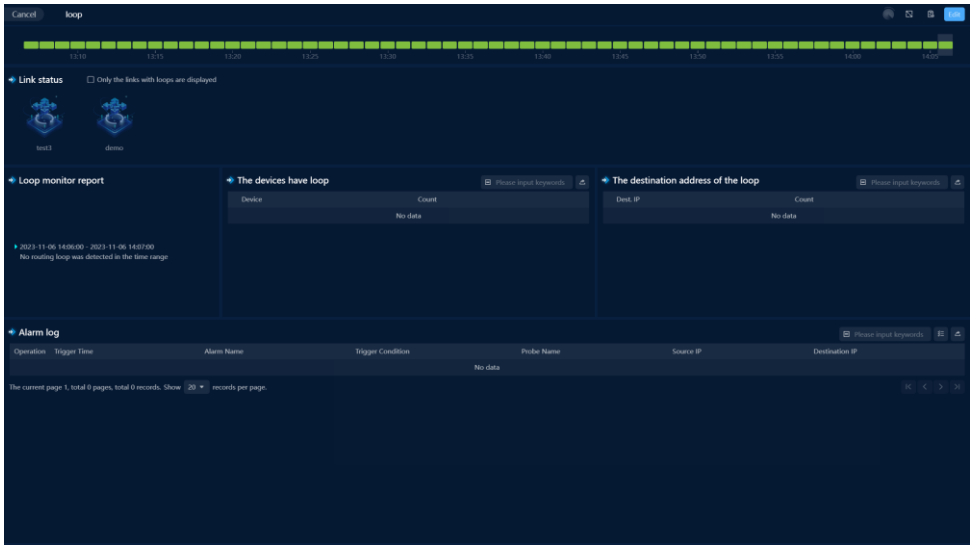
- Used to monitor routing loops in the network.

- When a loop occurs, it can notify the operation and maintenance personnel in real time through SMS or email.
- When a loop occurs, it can quickly locate the device where the loop occurs, as well as the affected target IP address.

15.3.2. Guide

15.3.2.1 Scenario View

In the custom metric monitoring page, the system has built-in the 'Scenario Monitoring and Analysis' group, which includes the routing loop monitoring view for monitoring and analyzing routing loop situations in the network. As shown in the following figure:



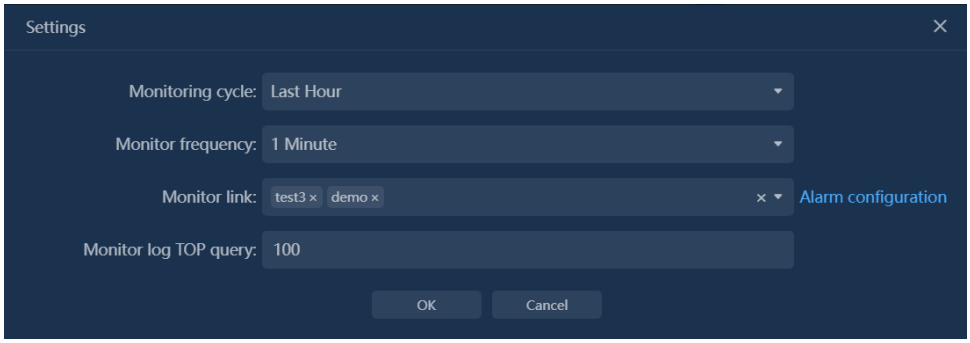
The routing loop monitoring view provides two modes: monitoring and analysis. By the status of the timeline, you can clearly see if there is a routing loop within the current time range. During the monitoring process, if a routing loop alarm is triggered, the alarm log details will be sent to the specified SMS, email, or syslog server. In analysis mode, by selecting a time range on the timeline, you can view the statistical information of the triggered alarms within the selected time range.

In the alarm log, you can directly see the devices that have routing loops and the affected destination IP addresses, guiding users to perform subsequent troubleshooting operations. For a single alarm log, you can perform trend analysis, packet download, and packet decoding operations.

15.3.2.2 Scenario Configuration

When entering this view for the first time, you need to configure the monitoring range of the links. Please use the right-click menu in the view editing mode to configure the monitoring data.

The monitoring data configuration dialog box is shown in the following figure:



15.4. Key device performance monitoring

15.4.1. Introduction

15.4.1.1 Background

Sometimes, business anomalies occur due to insufficient performance of a device (such as a firewall, load balancer, SSL device, WAF device) or policy configuration. In order to quickly discover device issues, it is necessary to actively monitor key devices (devices that are prone to problems). When a device is abnormal, you can quickly understand whether it affects the business and which businesses are affected. Is it a global impact or a local impact.

There are multiple devices, and an intuitive monitoring method is needed.

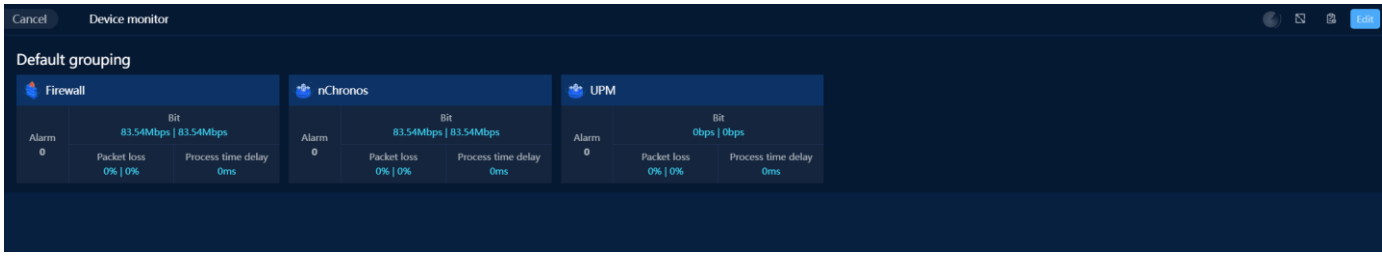
15.4.1.2 Value

- Efficiently identify which devices have abnormalities and promptly notify frontline monitoring personnel.
- When a device has an abnormality, it can quickly divide the event responsibility and locate the root cause from the perspective of device traffic monitoring.

15.4.2. Analysis guide

15.4.2.1 Scenario View

Through an overall monitoring view, you can see which devices are being monitored and which devices have issues. Support alarm notifications and device performance analysis.



The monitoring principle is to specify the front and back links of the device (i.e., traffic probes), and compare and analyze the network indicators and application performance

indicators of the front and back links to achieve performance anomaly monitoring of the device.

15.4.2.2 Scenario Configuration

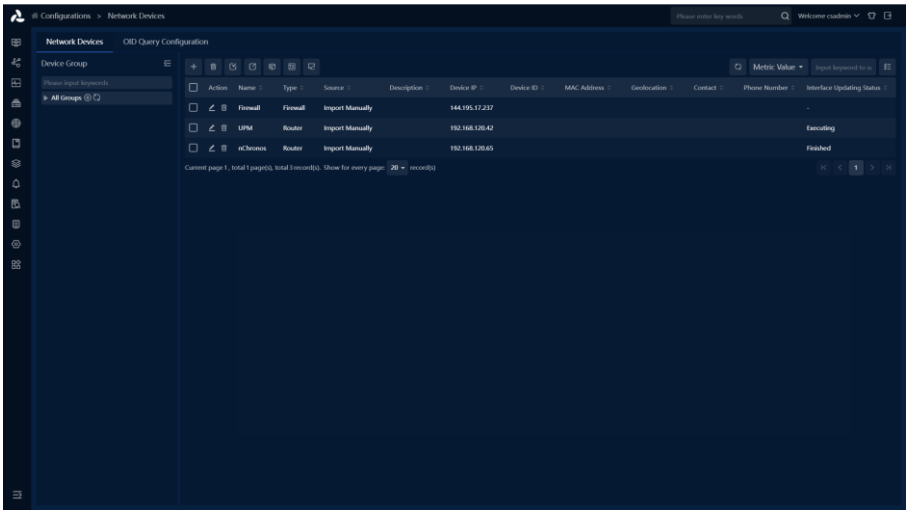
1. Add network devices

First, add the network devices that need to be monitored in the system, and after the device configuration is completed, select the devices for monitoring in the view.

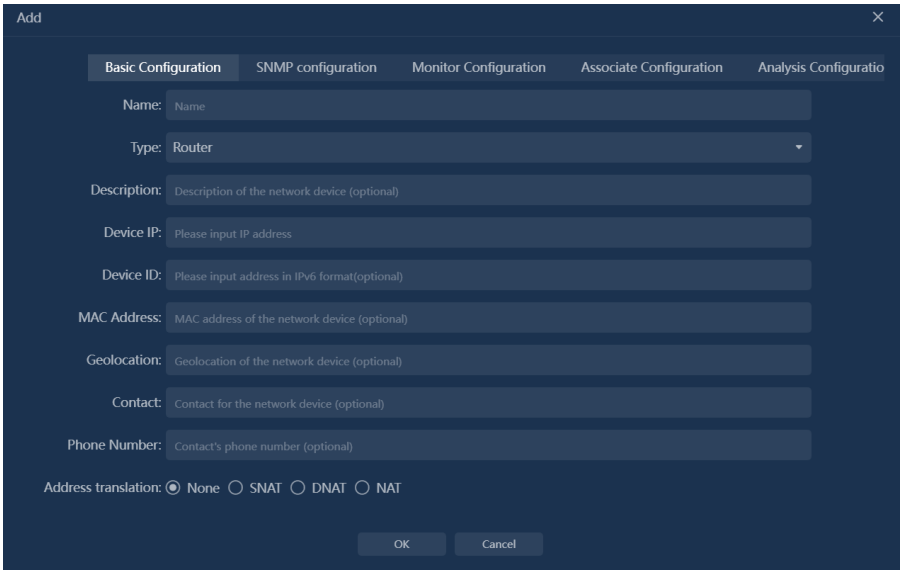
The steps for configuring network devices are as follows:

(1) Configuration entry: Select 'Configuration > Network Device Configuration' from the navigation menu.

Here you can see all the network device information configured in the system.



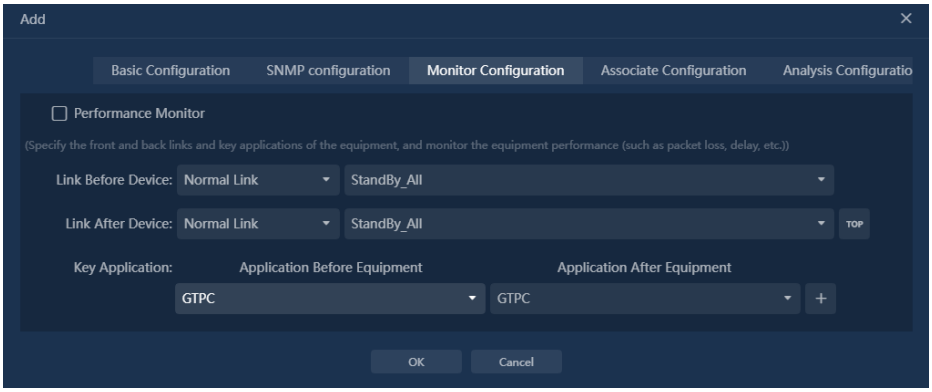
(2) Click the add button in the top left corner of the list '  ' to display the device configuration form.



Fill in the basic information of the device, with the required information being the name and device type.

Field Name	Description
Name*	Network device names cannot be duplicated.
Type*	Select the network device type, different types correspond to different display icons.

To enable device monitoring, switch to the 'Monitoring Configuration' tab, as shown below:



Check 'Monitoring Configuration' and specify the pre and post links and pre and post applications for the device.

The purpose of configuring pre and post links and pre and post applications is to analyze the network metrics and application metrics of the pre and post links, calculate packet loss and latency of the device, and perform monitoring.

Configure key applications:

a) Select up to 5 applications, click the 'top' button to get the top 5 applications in the link for the past 1 hour.
b) The configuration of the applications before and after, each line corresponds to each other.
c) For devices without NAT enabled, the applications before and after can remain the same.
d) For devices with NAT enabled, the applications before and after need to be manually specified as corresponding.

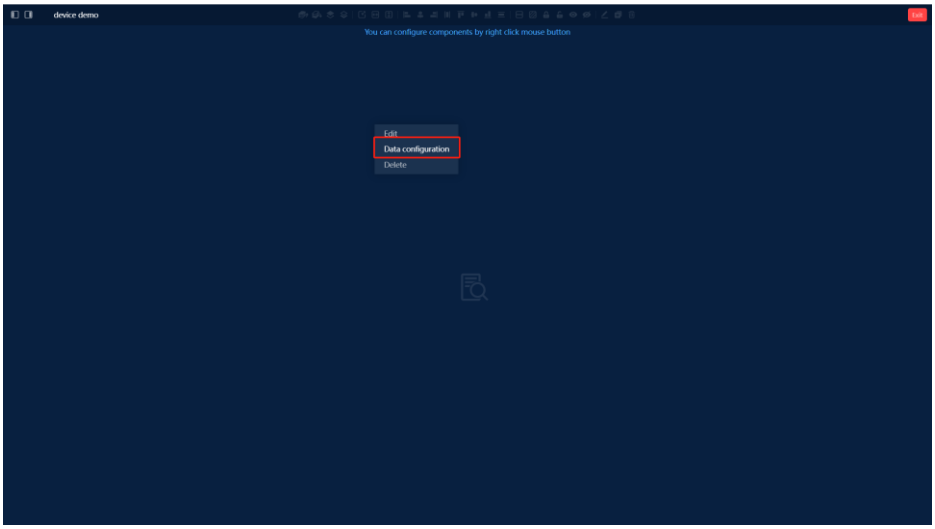
(3) Click the 'OK' button to complete the addition and monitoring configuration of the network devices.

2. Configure monitoring views

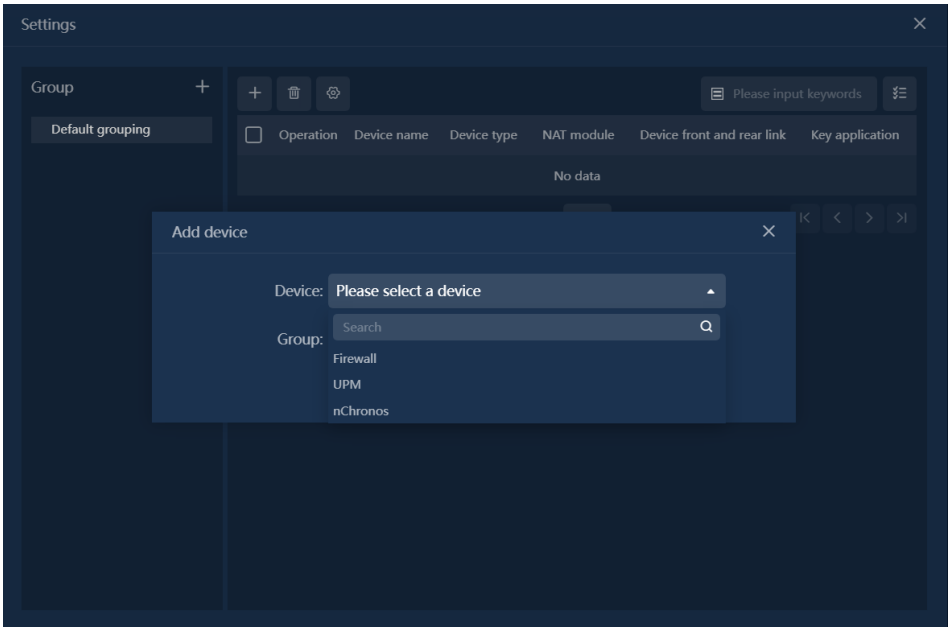
After configuring the network devices, define the display of monitoring views.

Configuration entry: Select 'Custom Monitoring' from the navigation menu

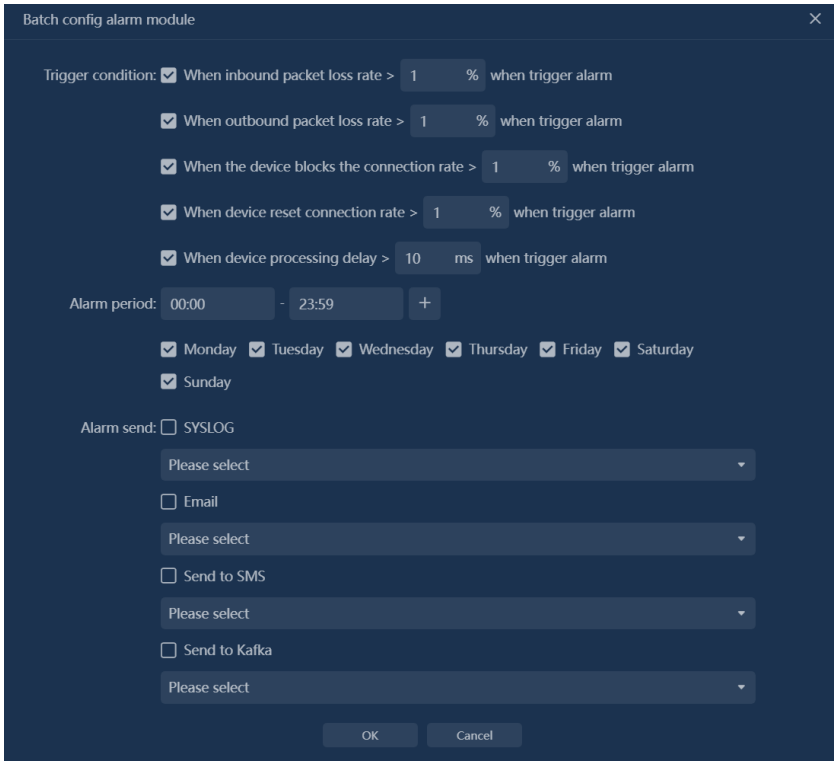
Find the 'Key Device Monitoring' view on the page and edit the view.



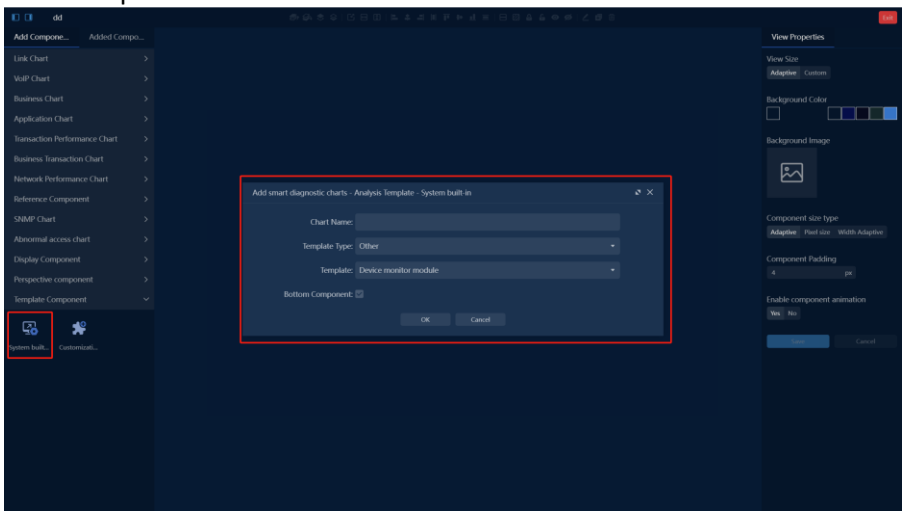
Right-click and select 'Data Configuration', select the device to add to the monitoring view in the pop-up window.



After adding the device, the system defaults to enable alarms. The alarm strategy is shown in the following figure and can be manually adjusted.



If not found, click the add button on the right side of the page  to add a new view. Add template components and select 'Device Monitoring '. After adding, follow the above step 2 to add devices to the view.



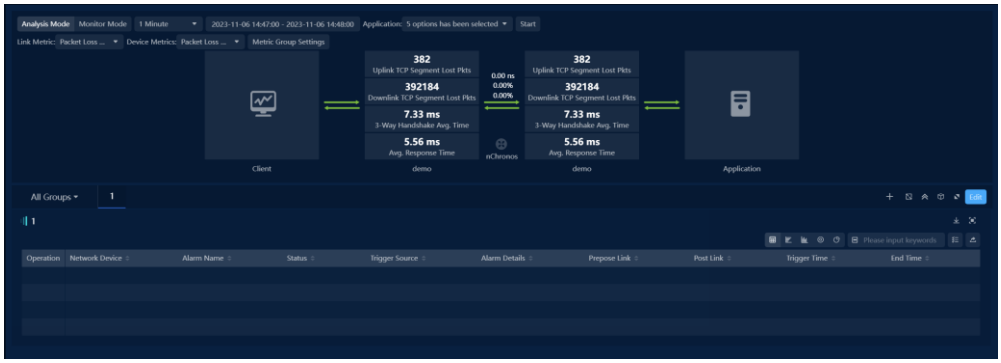
3. Device Analysis

On the device monitoring view page, select a single device and click to enter the device analysis page.

Use this page to view detailed pre and post indicators of the device, as well as device performance indicators, providing analysis basis.

Content displayed on the page:

(1) Device front and back link information, as well as device performance indicators.
(2) Device alarm information.
(3) Device packet loss, delay, and connection-related indicator analysis view.
(4) Device front and back traffic analysis view.



16. Session Tracking

16.1. Introduction

16.1.1. Function Description

Session tracing is a process in which associated sessions are matched in links based on the association rules configured by devices and session information (tuple or quad) is presented in the session access path.

16.1.2. Application Scenarios

During network access, the source IP address, destination IP address, source port, or destination port may change because multiple network devices pass through the network. In this case, users cannot perform association analysis on the session before and after the change or need to query the address port mapping table separately. The analysis process is tedious and the analysis result is not intuitive.

16.1.3. Function Value

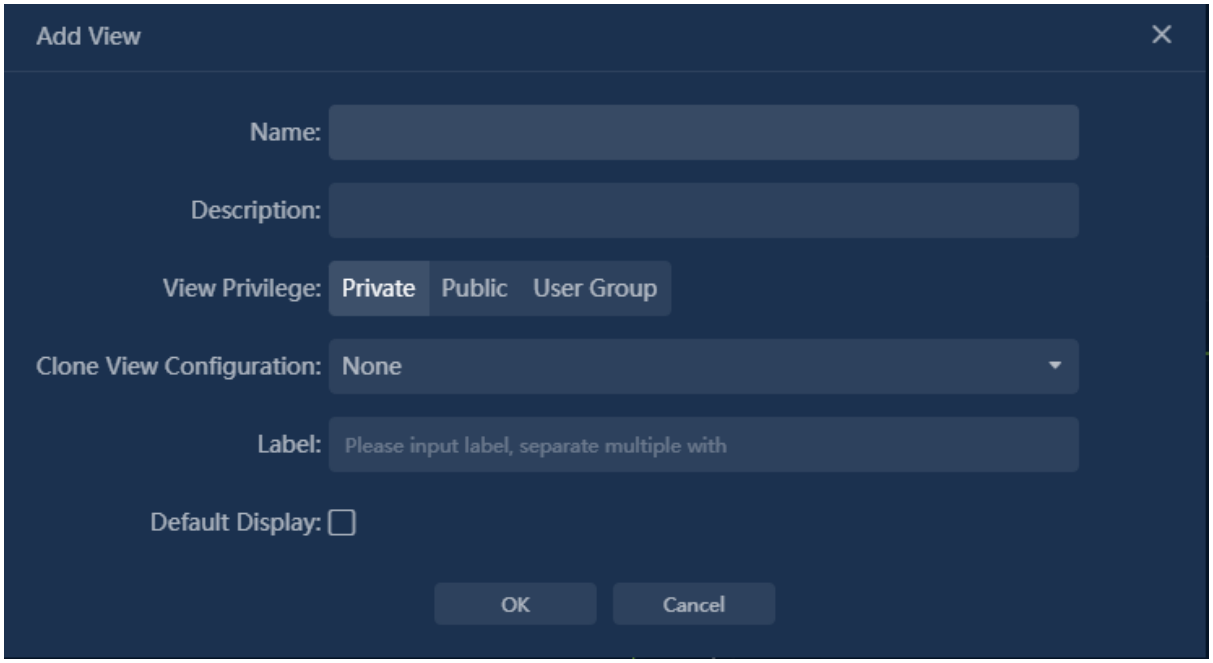
- Displays the IP address and port mapping before and after a session passes through the device.
- Automatically matches associated sessions on links.
- Functions costing a user to compare, download, decode, and export associated sessions.

16.2. Operation Guide

During session tracing, you need to select a session access path and search for associated sessions based on the association rules before and after devices in the access path. Session access paths are the basis for session tracing and need to be configured in advance. Different sessions can use the same path for session tracing.

Session access paths can be configured in the network topology monitoring. A network topology monitoring view can contain one or more session access paths. The configuration procedure is as follows:

1. Click on the menu "Network Performance" - > Network Topology Monitoring, access the network Topology Monitoring page.
2. Click "  " to add a view, as shown below:



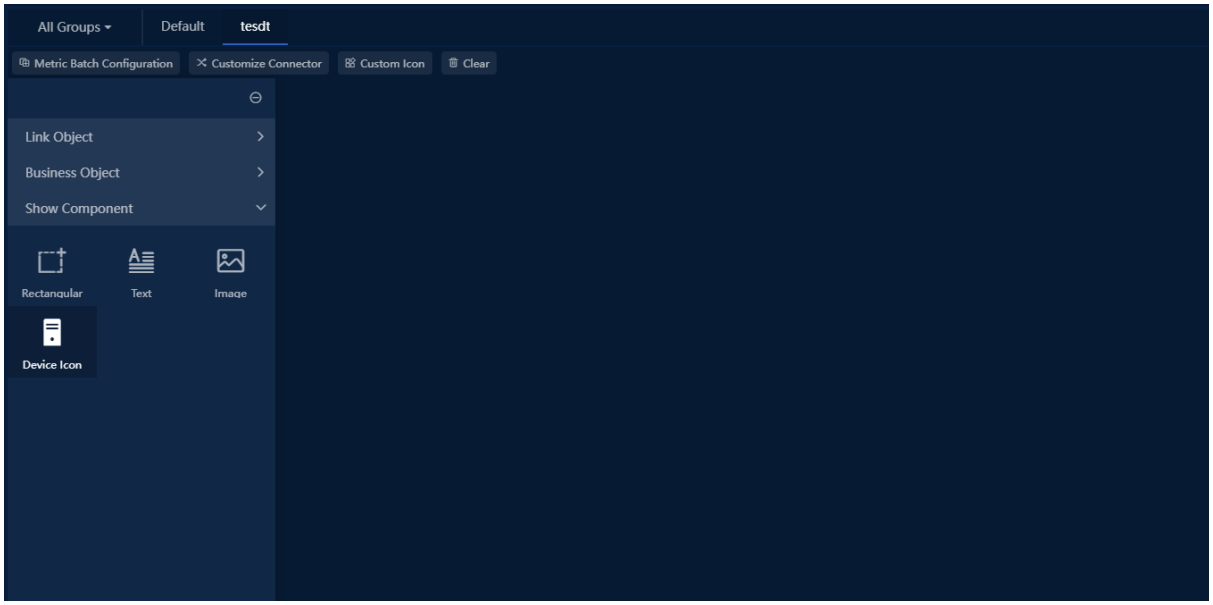
Add view configuration:

Field Name	Description
Name	Used to set the view name, the view name cannot be duplicated.
Description	Optional configuration item, used to set the description information of the view.
View Privilege	Used to set the permissions of the view. ● Private: The created view is only visible to oneself. ● Public: The created view is visible to everyone. User group: The created view is visible to the specified user group.
Clone view configuration	Optional configuration item for selecting the view to be cloned, enabling quick view creation.
Label	Optional configuration item for adding one or more tags to the view. The system supports filtering and displaying views based on tags.
Default display	Optional configuration item for setting whether the view is displayed by default. Not selected by default.

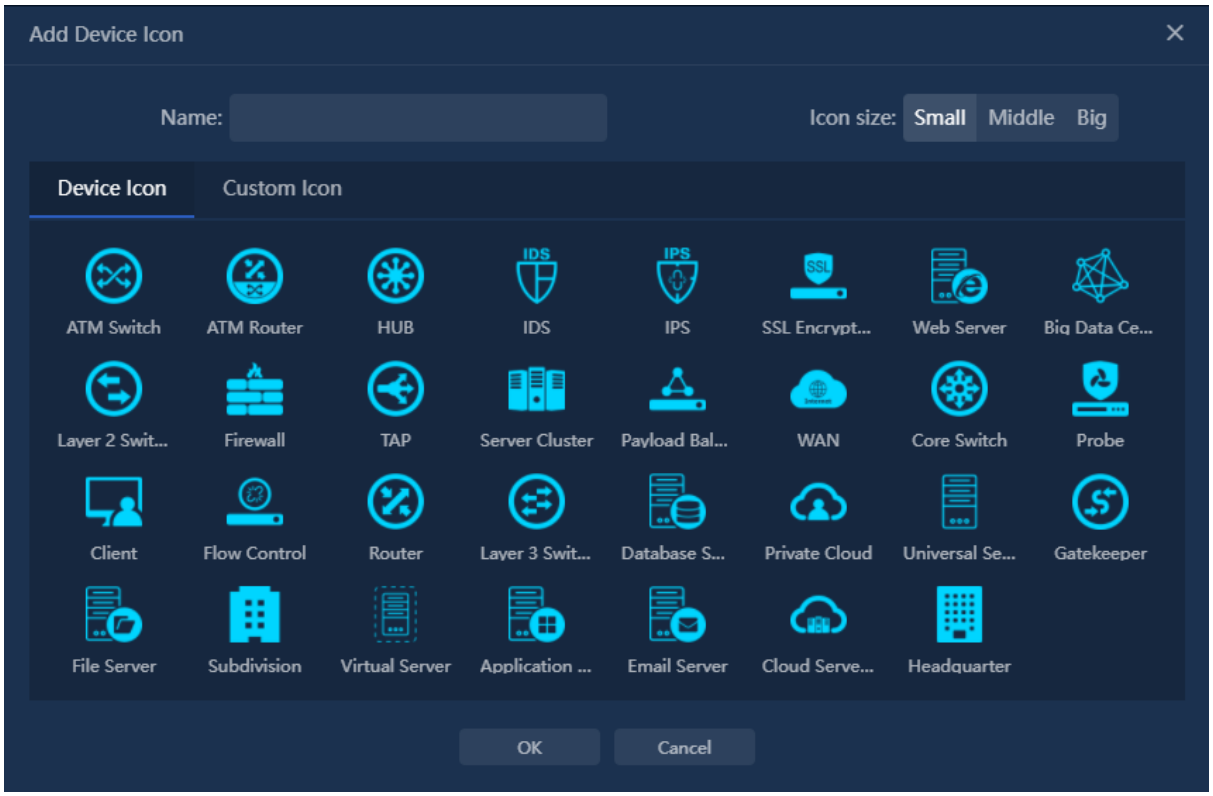
3. Click “OK”, the basic information about a view is added. Then click “ ” to enter editing mode, as shown below:

16.2.1. Device Icon

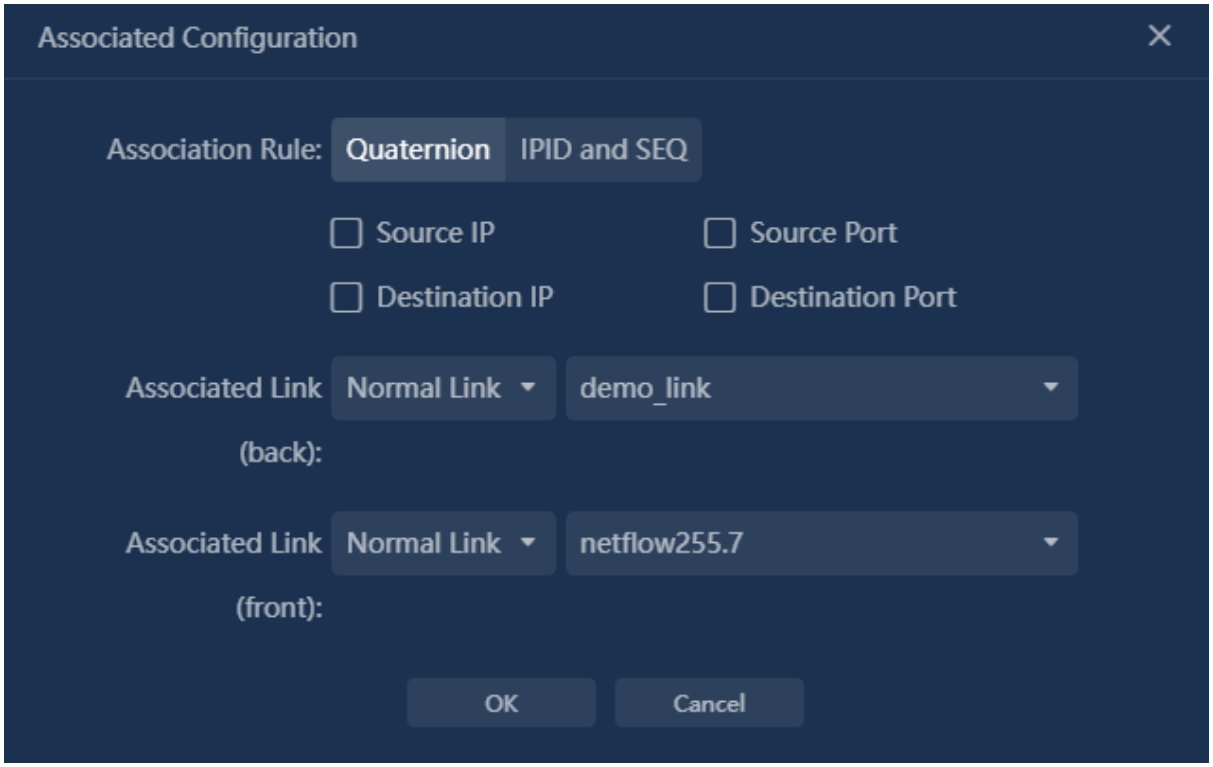
Show components - > Device Icon configuration You can select a default icon or a custom icon. As shown below:



1. In Show Components on the left, select Device Icon and drag it to the canvas on the right. The Add device icon dialog box is displayed, as shown in the following figure.



2. Select the device icon, set the name and size of the icon, and click OK. The device icon is added.
3. Right-click the icon of the added device and choose Associated Configuration from the shortcut menu. The Associate configuration dialog box is displayed, as shown in the following figure.



Field Name	Description
Association Rule	Select association rules. The system supports session association based on quad rules and IPID/SEQ rules.
Associated Link (back)	Set the link in front of the device in the session access path (client-server direction).
Associated Link (front)	Set the link behind the device in the session access path (client-server direction).

- Configures a quad association rule

Link sessions are associated with the front and rear devices using quads. Quads include source IP address, source port, destination IP address, and destination port. You can select one or more fields for session association.

- Association rule for IPID and SEQ

The IPID and Sequence Number are used to associate links between the front and rear devices. You can select one or more fields for session association.

Note

The IPID and SEQ association rules can only be used to trace TCP and UDP sessions.

4. Repeat the previous step to configure association rules for other network devices. The system automatically sorts out session access paths based on the links of added network devices. There may be one or more session access paths. During session tracing, users can select them as required.

5. To make the session access path more complete and intuitive, you can add links, lines, or other auxiliary ICONS.

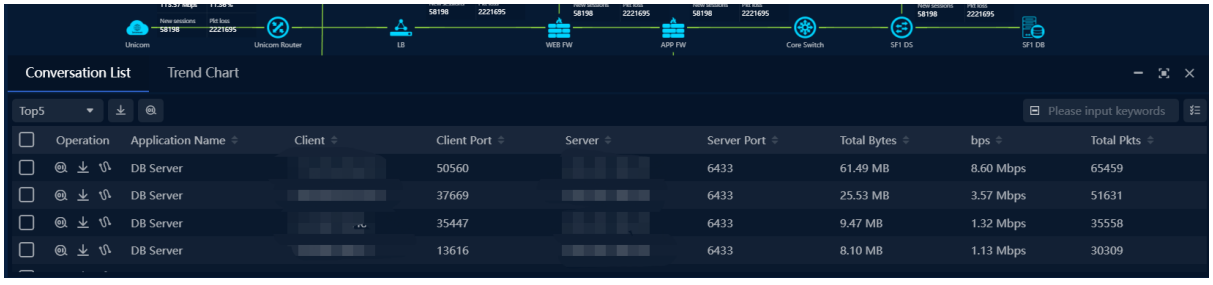
16.2.2. Select Session

The system provides an entry for session tracking in the network topology monitoring and retrieval page.

Session tracing in network topology monitoring

Prerequisites: Session access paths and application counters have been configured in the network topology monitoring view.

Click the four-grid of application indicator, and the session list will be displayed at the bottom of the page. Select the session to be tracked in the session list, and click "Session Tracking" in the operation column, as shown below:



After you click the "Session Tracking" button, the session tracking dialog box is displayed.

Note: Only TCP session tracing is supported in Network Topology Monitoring.

Retrieves session tracking from the page

Prerequisites: A session access path has been configured in the network topology monitoring view.

For the IP session, TCP session and UDP session retrieved in the search page, click the "Session Tracking" button in the operation column to pop up the session tracking pop-up box, as shown below:

Select the session access path, click 'OK' to trace the selected session.

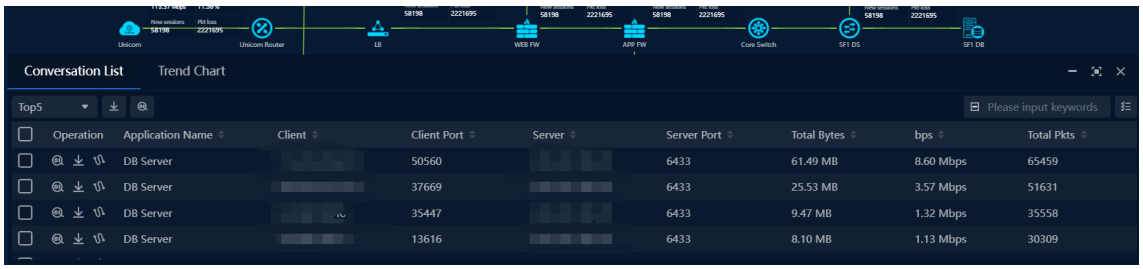
Note

When selecting the session access path, only the paths that include the link where the session is located will be displayed in the path list.

16.2.3. Session tracing result

IP session tracing

The session tracing result is shown in the following figure.



The session tracing result is explained as follows:

- The top of the pop-up box can switch the network topology monitoring view and select the session access path for tracing within the view.
- Below the link of the session tracing path, the associated sessions traced are displayed (showing session tuple information). If no associated sessions are traced on the link based on the association rules, it will display: Association failed.
- The session tracking list displays all tracked associated sessions. Users can download, decode, and export the tracked sessions.

16.3. Q&A

Failed to display association in session trace path

- **Problem Description**

In the session trace path, the link failed to trace the associated session, prompting association failure.

- **Possible reasons**

The association rule configuration is incorrect, resulting in the inability to establish an association relationship between the devices before and after.

- **Solution**

In the session access path configuration, check whether the association rules of the devices are configured correctly, and whether the selection of the devices before and after the link is consistent with the actual network deployment.

Unable to select network topology monitoring view during session trace in retrieval

- **Problem Description**

The network topology monitoring view list is empty in the pop-up box when performing session trace in retrieval.

- **Possible reasons**
  - No session access path is configured in the system.
  - The configured session access paths in the system do not include the link to which the selected session belongs.
- **Solution**
  - Configure session access paths in the network topology monitoring view.
  - Change the configured session access path and add the link belonging to the currently selected session to the path.

17. SRv6 Session Path Combing

17.1. Introduction

17.1.1. Terminology

SR

The core idea of the SR technology is to divide the packet forwarding path into different segments and insert segment information into the packet at the start point of the path. Intermediate nodes only need to forward the packet according to the segment information carried in the packet. Such path segments are called "segments" and identified by their SIDs. The key of SR technology lies in two points: Segment the path and sort and combine the path at the starting node to determine the travel path.

SRv6

SRv6 is a new generation protocol designed to forward IPv6 packets on the network based on the concept of source routing. SRv6, namely SR+IPv6, simplifies protocol types, has good scalability and programmability, and can meet diversified requirements of more new services.

SRH

SRH is a technology that implements SR based on the IPv6 forwarding plane, add the Segment Routing Header (SRH) in the IPv6 route extension Header. The SRH specifies an explicit IPv6 path and stores IPv6 Segment List information. Segment List is a forwarding path obtained by ordering segments and network nodes. During packet forwarding, Segments Left and Segment List fields jointly determine the IPv6 destination address (DA) information to guide packet forwarding paths and behaviors.

17.1.2. Function Description

By decoding the Segment Routing Header (SRH) of the SRv6 session packet, the Segment list is obtained, and the network devices passing through the access path of both sides of the session are sorted out according to the Segment list.

17.1.3. Scenario

With the expansion of the network scale and the arrival of the Cloud business, more and more types of network services have different requirements on networks. Traditional IP/MPLS networks face many challenges. SRv6 is an IPv6 forwarding based SR technology, which combines the advantages of SR source routing and the simplicity and expansibility of IPv6.

If SRv6 is used on the network, users can analyze the traffic passing through the device and optimize the network topology by combing the actual access paths of sessions on the network.

17.1.4. Value

- Supports decoding of SRv6 network protocols.
- Automatically combs the real SRv6 session access path.

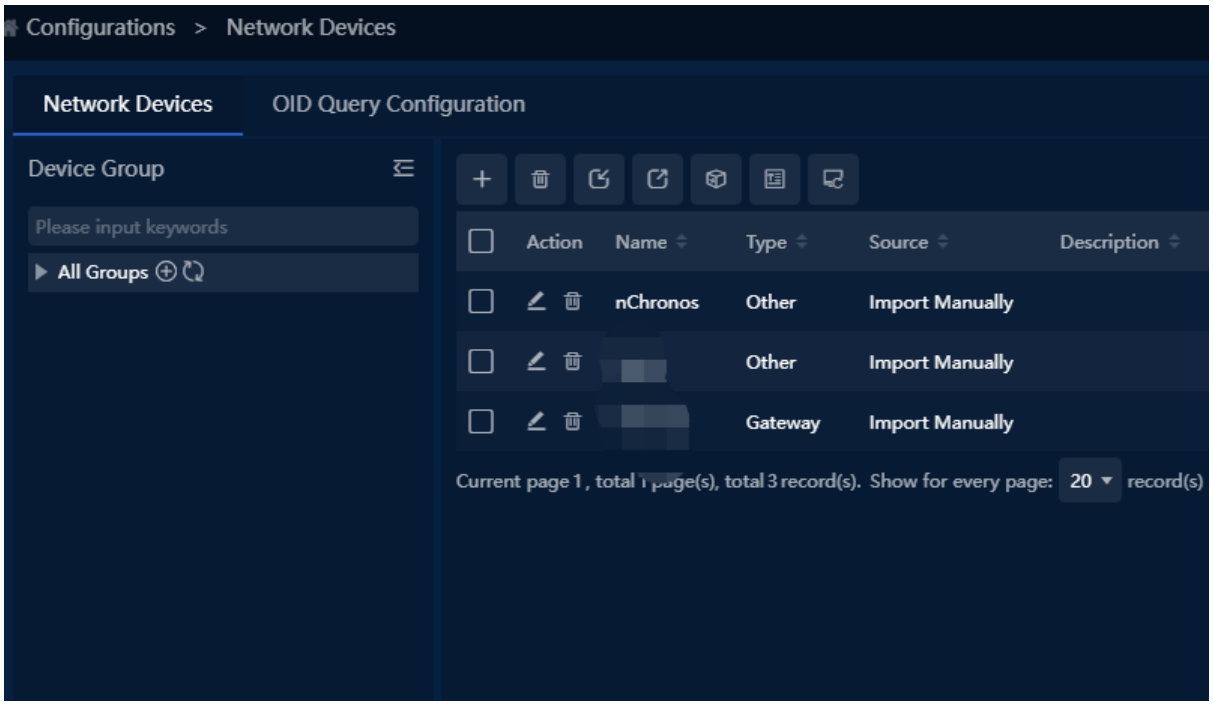
17.2. Operation Guide

17.2.1. Configuring Network Devices

Network Devices are optional. If no network device is configured, the id of the network device is displayed in device carding of the session path. If a network device is configured, it is displayed as the name of the network device based on the device ID.

The procedure for configuring network devices is as follows:

1. On the menu, choose Configuration > Business Configuration > Network Device, then the page is displayed, as shown in the following figure.



2, Click  , The “Add” dialog box is displayed, as shown in the following figure.

Field Name	Description
Name	This parameter is used to set the name of a network device. The network device name must be unique.
Type	This parameter is used to set the type of the network device. Different ICONS correspond to different types.
Description	This parameter is optional. It is used to set the description of the network device.
Device IP	This parameter is optional. It is used to set the IP address of the network device.
Device ID	This parameter is optional. It is used to set the network device ID. The device ID is in IPv6 format. You can set one IPv6 address, multiple IPv6 addresses, ranges, and network segments. For

Field Name	Description
	example: : 2404-440 ff00: FFFF: 203: : / 80
MAC Address	This parameter is optional. It is used to set the MAC address of a network device.
Geolocation	This parameter is optional. It is used to set the geographical location of the network device.
Contact	This parameter is optional. It is used to set contacts for network devices.
Phone Number	This parameter is optional. It is used to set the phone number of a network device.

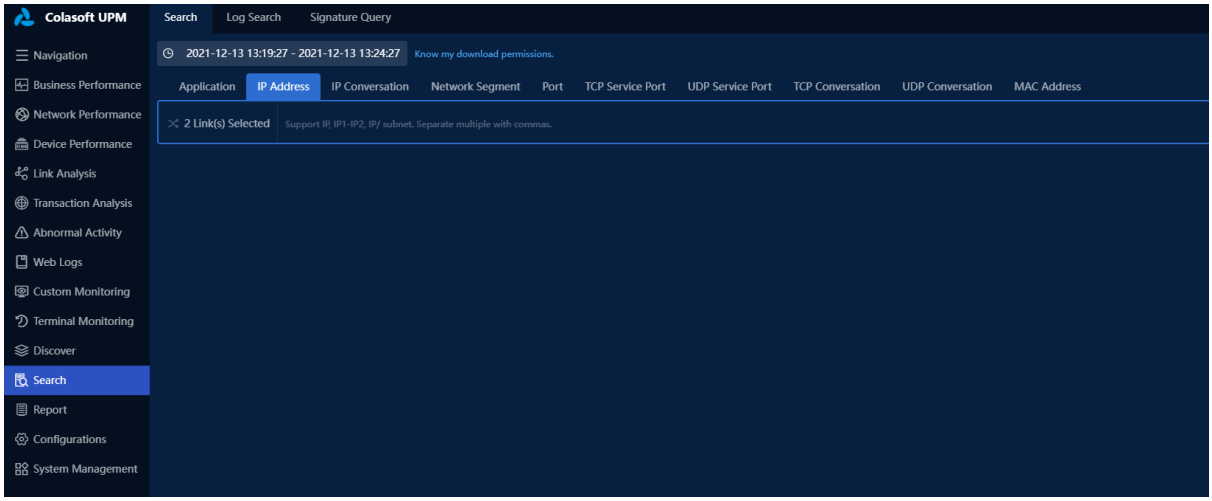
Notice: Not allow device ids configured on different network devices to cross; otherwise, unique network devices cannot be matched based on device ids.

3. Click OK to finish configuring the network device.

17.2.2. Select Session

The system supports device carding of TCP and UDP session paths.

On the search page, go to the TCP or UDP session list and click The "Session Device Comb" in the operation column to comb the network devices that pass through the session path, as shown in the following figure.



17.2.3. Session Path Analysis

In the 'Session Device Analysis' dialog box, click the 'Start Analysis' button to view the analysis results, as shown in the figure below.

Explanation of the session path device analysis results:

- Displays the network devices passed through in the client->server direction and server->client direction separately.
- For devices that cannot be matched in the network device configuration, the identification of the network device is directly displayed in the path.
- After modifying the time range or link, users can reorganize the session path device.
- In the same direction path, if there are multiple consecutive identical devices, they will be merged and only one network device will be displayed.

The result of session path device combing is described as follows:

- Displays network devices that pass through the client -> server - server -> client respectively.
- Automatically displays the network device's identity in the path if a device cannot be matched in a network device configuration.
- A user changes the time range or link to rearrange the session path device.

17.3. Q&A

Device not organized in the session path

- **Problem Description**

  Device information not organized in the session path, only server and client nodes.

- **Possible reasons**

  The selected session is not an SRv6session. There is no device information in the packet decoding information of the session, so the device cannot be organized.

Device name not displayed in the session path

- **Problem Description**

  The devices organized in the session path are directly displayed with device identification, and the device name is not displayed.

- **Possible reasons**

  The device identifier is not configured in the network device, so it cannot be matched to the corresponding device and can only be displayed directly.

- **Solution**

  In the 'Configuration > Business Configuration > Network Device' network device configuration page, pre-configure the network device identifier, and then reorganize the session path.

18. ARP Log Analysis

18.1. Introduction:

Based on ARP logs, you can analyze the ARP behavior of traffic in the network environment and discover ARP scanning and ARP spoofing Abnormal ARP behavior.

18.1.1. Functional value

- Detects a host that is suspected of an ARP scan.
- Detects a host that initiates an active reply exception.
- Detects a suspected faulty ARP server.
- Detects a host suspected of ARP spoofing.

18.2. Operation Guide

18.2.1. Configuring a Data Collection Task

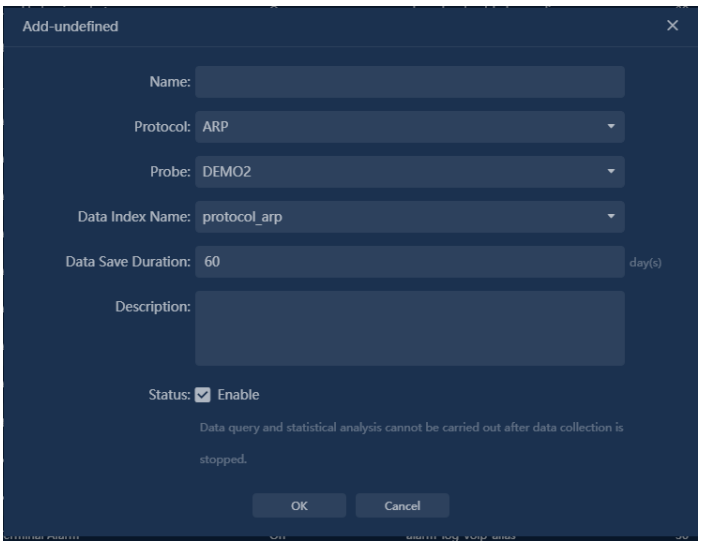
Before analyzing ARP logs, you need to collect ARP log data and configure ARP log collection

The steps are as follows:

1. Choose Configuration > Log Analysis Collection Configuration from the menu. The log collection configuration page is displayed.

2. Click the Data Collection Configuration TAB.

3. Move the mouse pointer to +, and choose DataSourceProtocol Log from the drop-down list box, as shown in the picture below,



Field Name	Description
Name	This parameter is used to set the name of a network device. The network device name must be unique.
Protocol	This parameter is used to set the log type of the collection protocol. Currently, only ARP is supported.
Probe	Probes used to set protocol log collection. Only common probes are supported. Sub-probes are not supported.
Data Index Name	This parameter is used to set the storage index of the collected data in ES, no need to add manually, use the default type is OK.
Data Save Duration	This parameter is used to set the duration for storing protocol logs.
MAC Address	This parameter is optional. It is used to set the MAC address of a network device.
Description	This parameter is optional. It is used to set the description of a collection task.
Status	This parameter is used to set the status of the collection task. If this parameter is disabled, the number of protocol logs will not be collected. It is enabled by default.

18.3. Field configuration

Customer can configure user-defined fields based on the fields collected in ARP logs. Custom fields and other collection fields in ARP logs are used in the same way and can be used in log retrieval and perspective components.

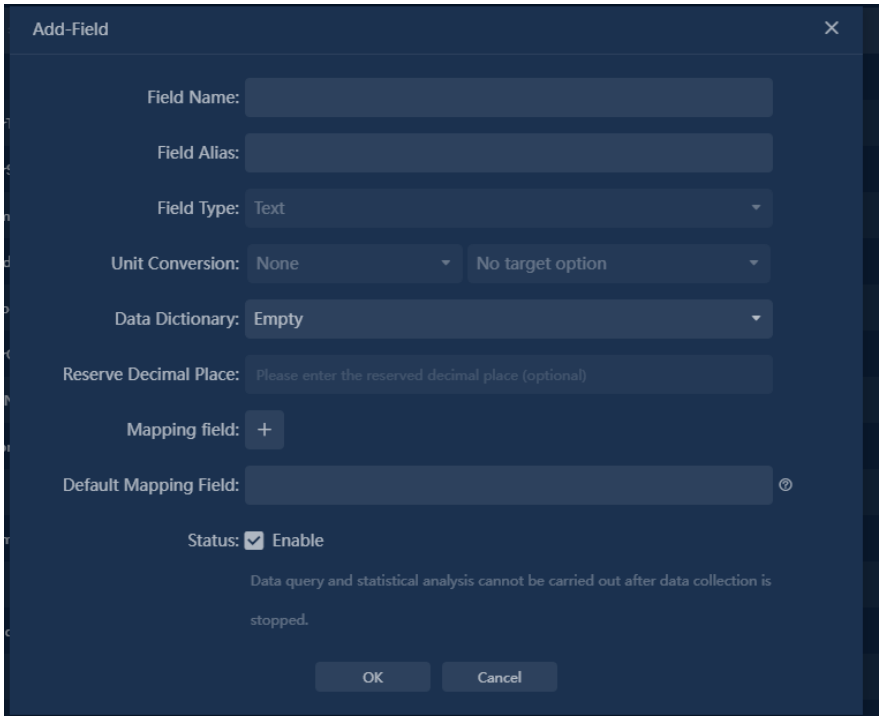
For example, to add a script field that identifies whether the log is a gratuitous ARP packet, the configuration procedure is as follows:

1. Choose Log Collection Configuration> Field Configuration from the menu. The Field configuration page is displayed.

2. Select the configured ARP log collection task from the log table on the left.

3. Click the Script Fields TAB. You can configure the script fields of ARP logs.

4. Click  to pop up the new script field dialog box, as shown in the picture below.



Field Name	Description
Field Name	This parameter is used to set the name of the field to be added. The name cannot be modified after being set.
Field Alias	Used to set the name of the new field to be displayed in usage, such as in log retrieval and perspective component analysis. The field alias can be changed.
Field Type	Used to set the type of the new field.
Data Dictionary	This parameter is used to set the duration for storing protocol logs.

18.3.1. Data Dictionary Management

The data dictionary is mainly used to configure the corresponding relationship between field encoding and field display name.

Take ARP packet identification field as an example. This field corresponds to two values. 0 indicates a non-ARP packet, and 1 indicates a non-ARP packet. For easy viewing and use, you can use the data dictionary to map 0 to no and map 1 as yes.

Choose Configuration > Transaction Configuration > Data Dictionary from the menu. The Data Dictionary configuration page is displayed. As shown below:

C

Field Name	Description
Name	Used to set the view name, the view name cannot be repeated.
Protocol	It is used to set the type of collected protocol logs. Currently, only ARP protocol is supported.
Probe	It is used to set the probe for collecting protocol logs. Only common probes are supported, and selector probes are not supported.
Data Index Name	It is used to set the storage index of the collected data in ES. You don't need to add it manually, just select the default type of the system.
Data Save Duration	Used to set the length of time protocol logs are saved.
Description	Optional configuration item, used to set the description information of the collection task.
Status	It is used to set the status of the collection task. If it is not enabled, the protocol log data will not be collected, and the system is enabled by default.

18.3.2. Filed Configuration

Users can configure custom fields based on the fields collected in the ARP log. Custom fields are used in the same way as other collected fields in ARP logs, and can be used in log retrieval and perspective components.

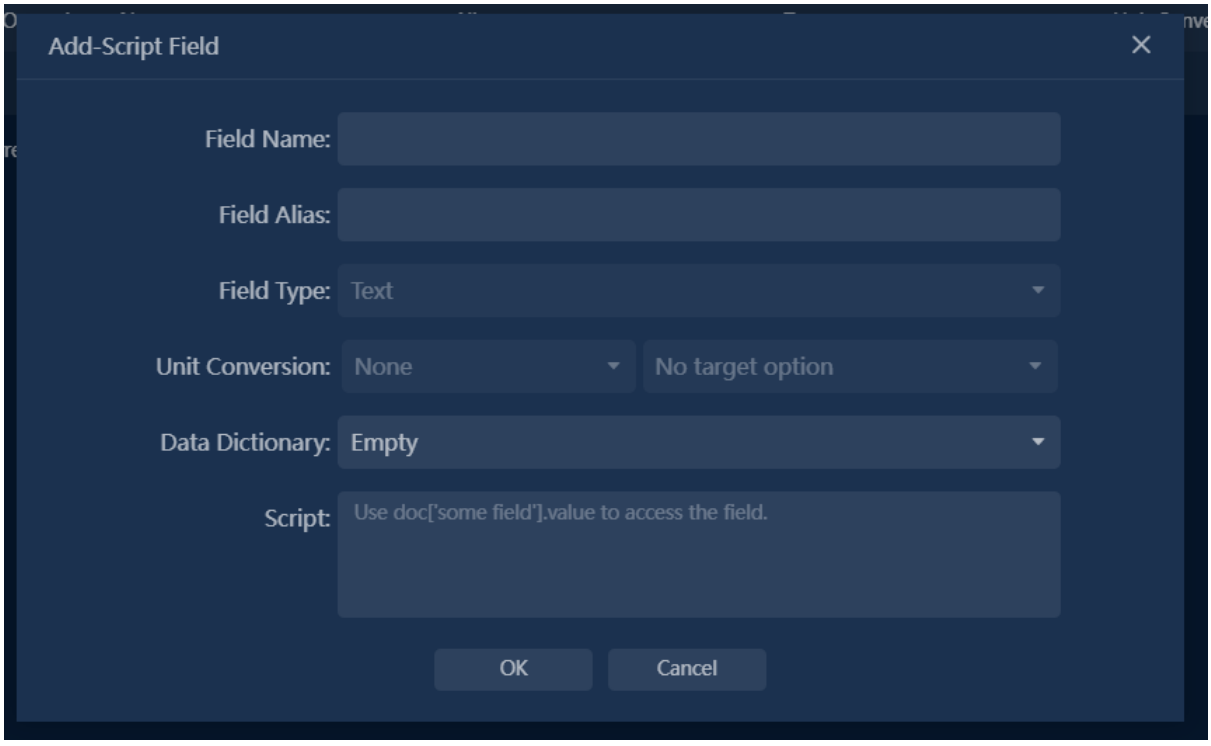
For example, add a script field to identify whether the log is a gratuitous ARP packet. The configuration steps are as follows:

1. Choose Log Collection Configuration > Field Configuration from the menu to enter the field configuration page.

2. Select the configured ARP log collection task in the log table on the left.

3. On the right, select the Script Fields tab to configure the script fields of the ARP log.

4. Click + to pop up the New Script Field pop-up box, as shown in the following figure.



Field Name	Description
Field Name	Used to set the name of the field to be added. The name cannot be modified after being set.

Field Name	Description
Filed Alias	Used to set the name of the new field to be displayed in usage, such as in log retrieval and perspective component analysis. The field alias can be changed.
Field Type	Used to set the type of the new field.
Data Dictionary	This parameter is optional. It is used to set the data dictionary referenced by the new field. The data dictionary needs to be configured separately.
Scrip	Script used to set the new fields. Take gratuitous ARP packets as an example. If the sender IP address is the same as the destination IP address, the packet is marked as a gratuitous ARP packet.

18.3.3. ARP log search

On the ARP log search page, you can perform statistical analysis on the collected ARP logs as follows:

1. Choose Search and log search page is displayed.

2. Select the configured ARP log collection task from the log drop-down list box.

3. Select a time frame.

4. Set filter criteria. Filter conditions including source MAC address, the source IP address, request destination MAC address, destination IP address, request the sender MAC address, the sender response target IP address, MAC address, destination IP address response, in response to the sender MAC address and respond to the sender IP address, protocol type, operation code, destination MAC address and destination IP Address.

5. Click the "Query" button to view the matched ARP log.

18.3.4. ARP analysis

You can use the perspective analysis function of collected ARP logs to discover abnormal ARP events on the network, such as:

- Hosts that make the most ARP requests, Top
- The host Top that initiates the most ARP responses
- Hosts that send the most gratuitous ARP entries

18.4. FAQ

No device is displayed in the session path

- **Problem description**

  The session path contains only two nodes, the server and the client, and no device information is displayed.

- **Possible reasons for**

  The selected session is not an SRv6 session, and the device information does not exist in the packet decoding information of the session. Therefore, the device cannot be sorted out.

The device name is not displayed in the session path

- **Problem description**

  The device ID is directly displayed in the session path, but the device name is not displayed.

- **Possible reasons for**

  The device ID is not configured on the network device. Therefore, the device ID cannot be matched and can only be displayed directly.

- **The solution**

  Choose Configuration > Service Configuration > Network Devices to configure the network device id, and then rearrange the session path.

19. Feature Value Alerts

19.1. Function introduction

19.1.1. Functional description

Feature value alerts mainly detect and match specific transmission content in network traffic, and provide alerts for matched traffic. Compared to other types of alerts, feature value alerts are more accurate and flexible, helping network analysts quickly identify traffic characteristics and enhance the product's detection capability for malicious threats.

19.1.2. Functional scenarios

1. Support counting statistics for features. During the statistical period, when the number of packets or sessions hitting the feature threshold is reached, trigger an alert.
2. For individual sessions, support feature context detection, trigger an alert when both request data and response data hit the feature at the same time.
3. For individual packets, when configuring feature values, for common protocols, it can quickly locate the decoding fields in the selected protocol.

19.1.3. Functional value

- Enhance the detection capability of unknown threats for the product.
- When configuring feature values, provide a configuration assistance interface to reduce user configuration difficulty and improve user experience.

19.2. Feature value alert classification

Based on different alert objects, feature value alerts include packet feature value alerts and session flow feature value alerts.

19.2.1. Packet feature value alerts

Packet feature value alerts are triggered by judging the feature values of the content transmitted in individual packets. By unpacking and analyzing each packet, compare whether the configured feature value information exists in the packet to trigger an alert.

- Single packet single match: According to single packet matching, each packet is detected separately, and an alarm is triggered when the preset feature is matched.
- Multiple packets counting match: Within an alarm cycle, feature detection is performed on single packets. When a single packet matches the feature, it is counted. An alarm is triggered when the number of feature matches in the alarm cycle reaches the threshold.

Example scenario: Detecting the situation where the number of SYN packets sent by host A to host B in the network environment exceeds 100 within 3 seconds and issuing a warning.

19.2.2. Session feature value alarm

Session flow feature value alarm takes the session as the triggering object, matches the features of the packets within the session, and also supports setting feature matching with contextual correlation of packets within the session.

Support HTTP protocol context correlation analysis, by distinguishing the requests and responses in the HTTP protocol session, to determine the correlation of the requests and responses, and to alert when there are attack characteristics in the request parameters or specific information in the response status, meeting various configuration requirements.

19.3. Operation Guide

This section mainly introduces the configuration of feature value alerts and the display of alert logs.

19.3.1. Alert object filtering

Feature value alerts can monitor all captured traffic for feature values, and can also be filtered by quadruples or TCP flags.

The filtering fields supported by the system include protocol, source IP, source port, destination IP, destination port, TCP flags, ICMP flags, and packet size.

- The protocol supports thousands of protocols on the network layers 2-7, and the protocol supports fuzzy search. Multiple protocols are connected by the OR relationship.
- IP address supports input of single, multiple, range, and mask.
- Port supports input of single, multiple, and range.
- Packet size supports setting a range.
- TCP flags include Urgent, Push, Acknowledgment, Reset, Synchronize, and Terminate.
- ICMP flags are shown in the table below.

Redirect for network	Request-Echo request (Ping request)	Host Unreachable
Unsupported length	Router advertisement	TTL equals 0 during transit
TTL equals 0 during reassembly	Required options missing	Destination network unknown
Redirect for TOS and network	IP header bad	Destination network administratively prohibited
Timestamp reply	Host precedence violation	Host unreachable for TOS
Net Unreachable	Reply-echo response (Ping response)	Protocol Unreachable
Timestamp request	Redirect for TOS and host	Communication administratively prohibited by filtering
Precedence cutoff in effect	Destination host administratively prohibited	Network unreachable for TOS
Destination host unknown	Route solicitation	Fragmentation needed but no frag. bit set
Redirect for host	Source routing failed	Port Unreachable

Note

To reduce system load, it is recommended to configure quadruple filtering information when making feature judgments for specific IP or port.

19.3.2. Feature value configuration

The system supports three formats for feature values: ASCII, HEX, and expression.

ASCII

Simply enter ASCII characters directly in the feature content input box.

HEX

Simply enter hexadecimal characters in the feature content input box.

Expression

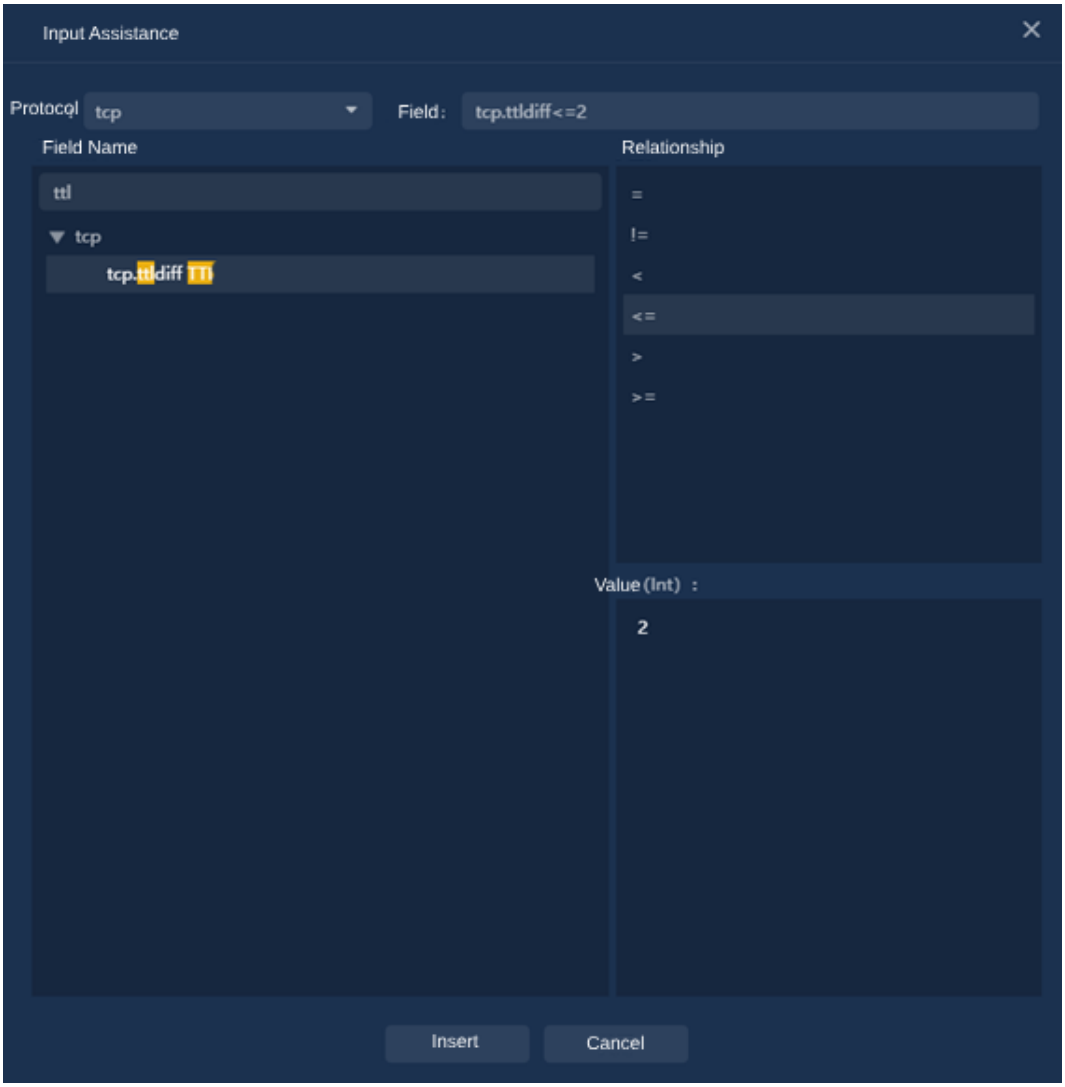
An expression consists of one or more rules, with logical OR relationships between multiple rules.

Expression for single packet

Method 1: Enter the expression directly in the text box and click  to view the help documentation for input rules.

Method 2: Configure through input assistance

1. Click the 'Input Assistance' button to open the input assistance dialog box.
2. Select the protocol, field, and logical relationship in the dialog box, and enter the condition value.
3. Click the 'Insert' button to insert the expression into the alarm configuration.



Expression configuration for session

1. The expression for a session includes request features and response features.
2. The content of the requested feature needs to be included in the request tag <request></request>, and the content of the response feature needs to be included in the response tag <response></response>.
3. A single line expression can only contain one request tag and one response tag, and there is a logical AND relationship between the request feature and the response feature in the same line.
4. The configuration method of the request and response features is consistent with the configuration method of a single packet expression.

For example: <request>http.payload.find('and 1=1')</request><response> http.status.find ('200ok')</response>

19.3.3. Alarm log

View triggered feature value alarms on the 'Abnormal Behavior > Abnormal Behavior Alarm' page.

In the alarm details column, you can view the quadruple information of the triggered feature, as well as the specific feature that was triggered.

20. Load Balancing Analysis

20.1. Function introduction

20.1.1. Functional description

By obtaining the configuration information of Load Balancing VS, Pool, and Member, real-time monitoring of the network performance of each node server in the load balancing system can be achieved. It can also automatically generate applications based on the configuration information for more professional and in-depth metric monitoring, and provide alert prompts when abnormal alarm information occurs. Improve work efficiency for the operations department, provide application quality evaluation for the business department, and provide data support for the security department.

20.1.2. Functional scenarios

In a network environment that uses load balancing, the distribution of business systems is complex. In general, a large amount of IP port information is configured in load balancing. V S, Pool, and Member can provide a simpler and faster way to identify business applications. Therefore, from an overall perspective, by directly monitoring the network metrics of business applications through the configuration information of V S, Pool, and Member, the manual configuration workload for users is greatly reduced.

20.1.3. Functional value

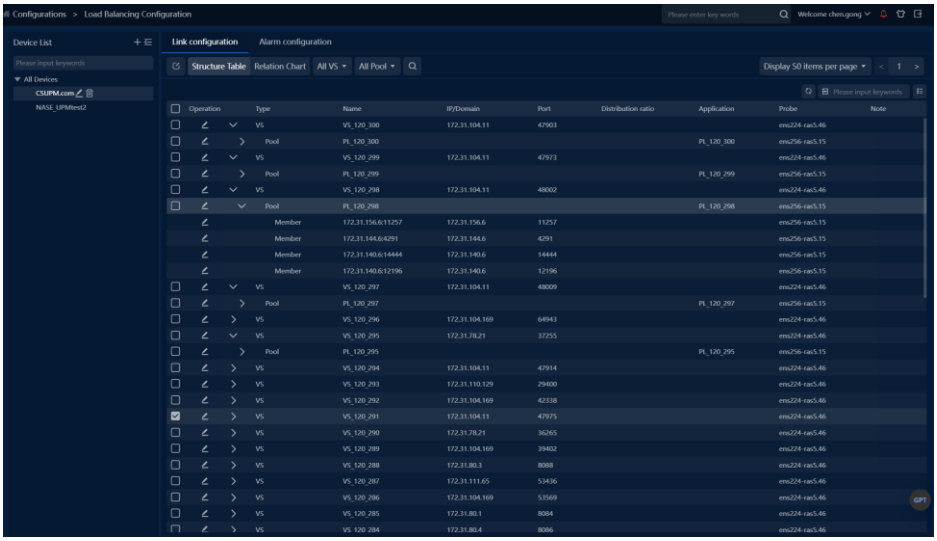
- Automated data updates, changing with the configuration changes on the load balancing side through interfaces, reducing the degree of manual involvement.
- Accurate metric data, achieved by collecting probes on V S, Pool, and Member configurations, enabling real-time data collection on the target IP port.
- Deeper analysis, fully utilizing the product's existing mining capabilities, directly digging into and analyzing query service access, client, TCP/UDP service ports, and other information through analysis data on VS, Pool, and Member.
- Precise triggering of alarms and timely alerts, based on the current powerful data collection capabilities, the system can discover abnormal situations and trigger alarms according to the configured trigger conditions, and send alert messages, emails, and other notifications to the operation and maintenance personnel for timely handling.

20.2. Operation Guide

20.2.1. Load Balancing Configuration

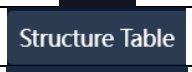
Click on Configuration -> Load Balancing Configuration  to enter the Load Balancing Configuration page, as shown in the figure below.

Figure 20-1 Load Balancing Configuration



The functions of the operation bar above the list are shown in the table below:

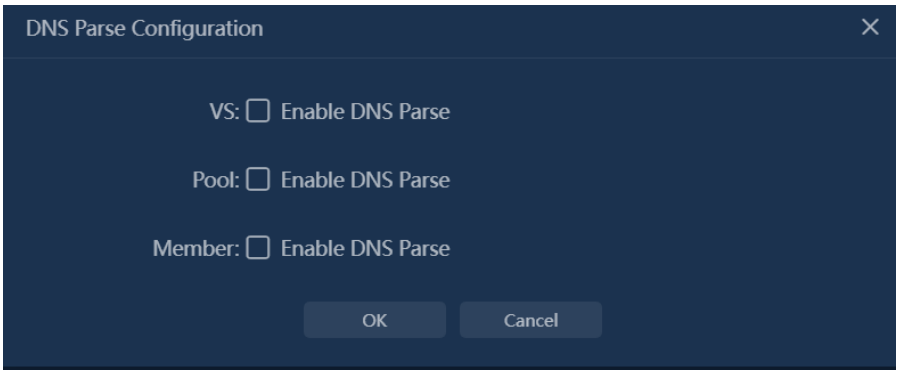
Table 20-1 Operation Instructions

Operation	Description
	Batch Link Probe Association
	View Structure Table
	View Relationship Diagram
	Filter and Select Nodes

20.2.1.1 Device Configuration

Click on the button  after the device name in the device list, and a "DNS Resolution Configuration" pop-up window will appear. When the application is automatically generated and successfully applied in the interface, and the corresponding application is mounted on the node in the console, you can use the DNS resolution switch to determine whether to collect and display DNS transaction metric data.

Figure 20-2 DNSResolution Configuration

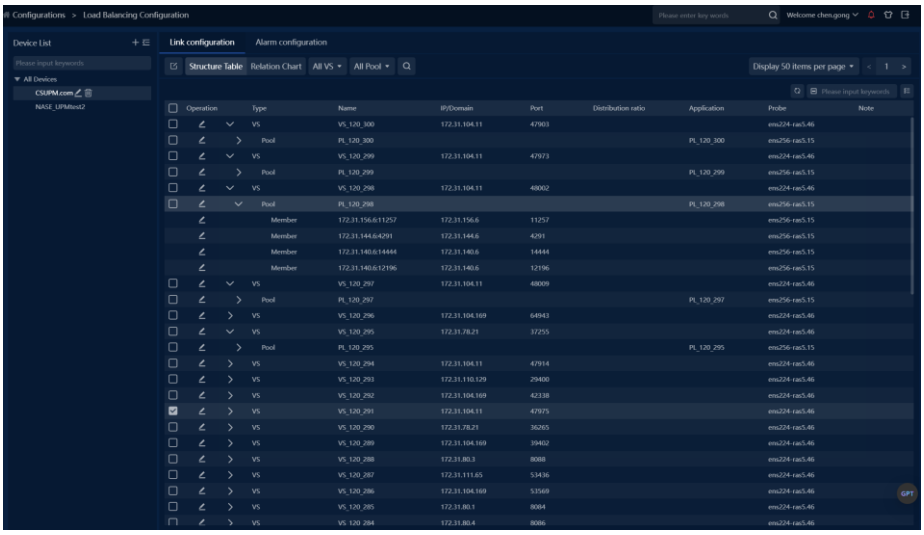


Click the button next to the device name in the device list to delete all information of this device and reacquire it by manually calling the interface.

20.2.1.2 Link Configuration

Select 'Configuration > Load Balancing Configuration > Link Configuration' in the menu to enter the load balancing link configuration page, as shown in the following figure.

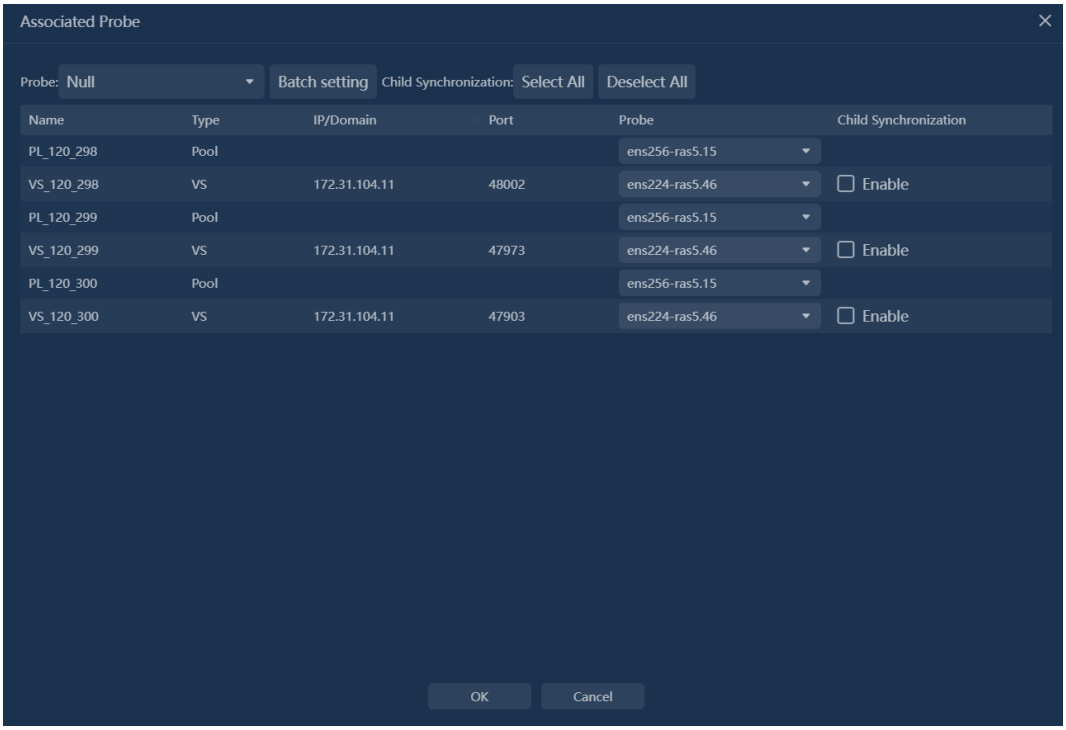
Figure 20-3 Link Configuration



Probe Batch Configuration

Check the nodes that need to configure probes in the structure table or click on the nodes that need to configure probes on the relationship diagram. The color of the nodes will change to to indicate that they have been selected. Click the button; The batch configuration interface will pop up. As shown in the following figure:

Figure 20-4 Probe Batch Configuration



Select the probe names that need to be configured, click on batch configuration, all nodes in the pop-up window will be configured with the same probe, and can also be modified individually.

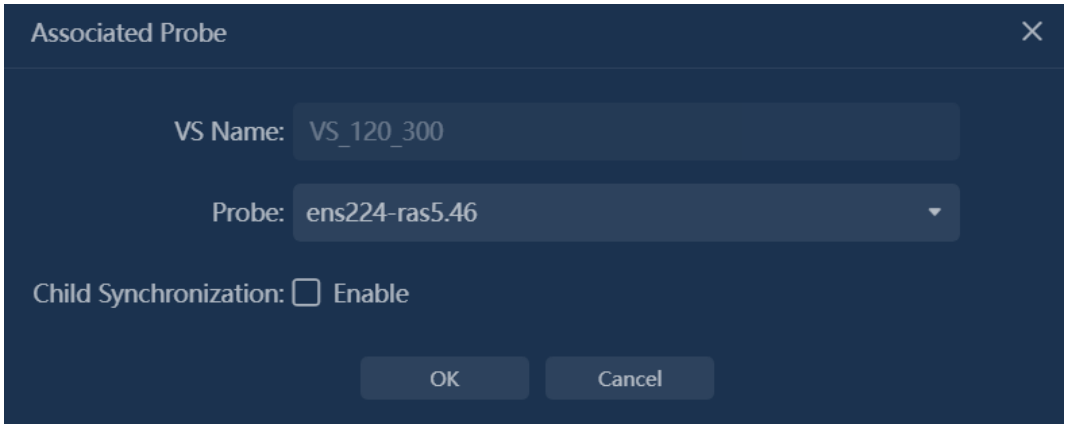
Sublevel synchronization: After clicking select all, all Pool and Member nodes under this VSnode will be set to the same probe as the VSnode.

Click the 'OK' button to complete the batch configuration of the probe.

Probe individual configuration

In the structure table, directly click the button or in the relationship diagram, move the mouse over the card area of the node that needs to be configured and then click the button to open the associated probe interface. As shown in the figure below:

Figure 20-5 Associated Probe



Select the probe name that needs to be configured.

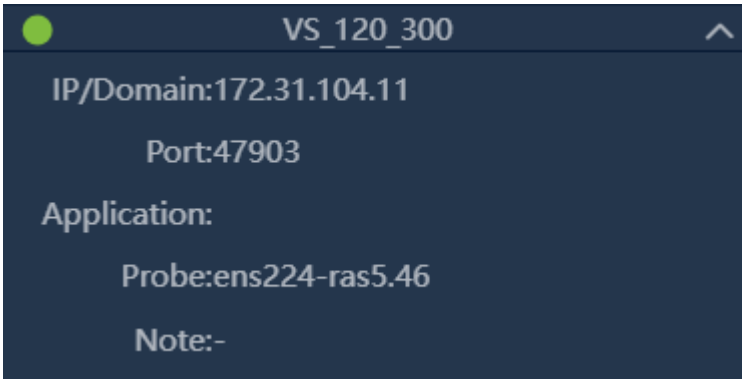
Sublevel synchronization: After checking, all Pool and Member nodes under this VSnode will be set to the same probe as the VSnode.

Click the 'OK' button to complete the batch configuration of the probe.

20.2.1.3 Relationship Diagram Configuration Information View

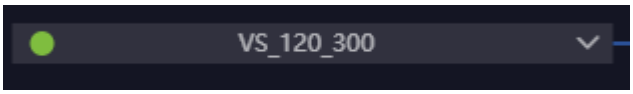
1.  Click the button on the card that needs to view the information to expand and view the detailed configuration attribute information of the current node.

Diagram 20-6 Card Expand



2. Click the button on the card that expands the information to hide the detailed information. 

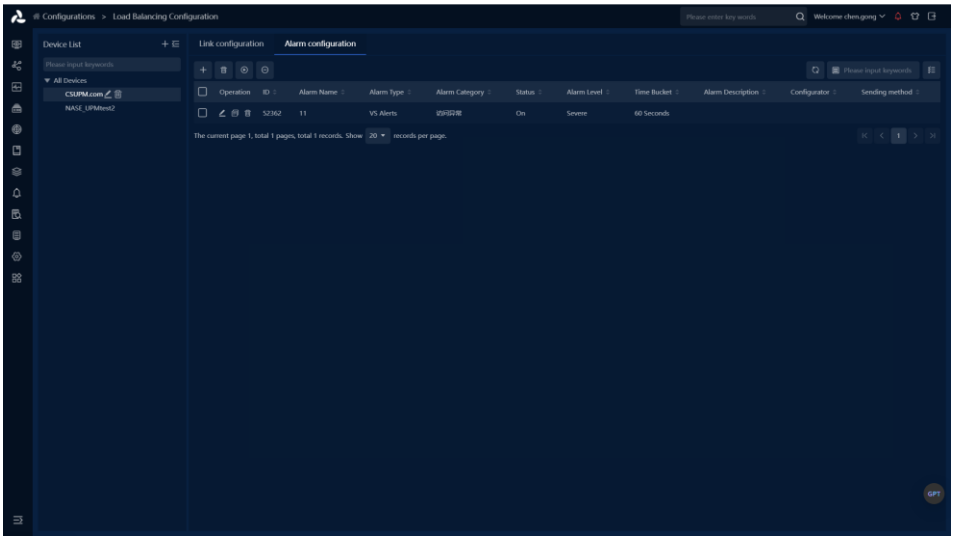
Diagram 20-7 Card Collapse



20.2.2. Alarm Configuration

Select 'Configuration > Load Balancing Configuration > Alarm Configuration' in the menu to enter the load balancing alarm configuration page, as shown in the following figure.

Diagram 20-8 Alarm List



The functions of the operation bar above the alarm list are shown in the table below:

Table 20-2 Operation Instructions

Operation	Description
	To add an alarm, please refer to 2.1.3.1 Alarm Creation
	Delete Alert
	Enable selected alerts.
	Disable selected alerts

20.2.2.1 Alert Creation

Click  to add load balancing alerts. The alert configuration is shown in the following figure:

Figure 20-9 Alert Creation

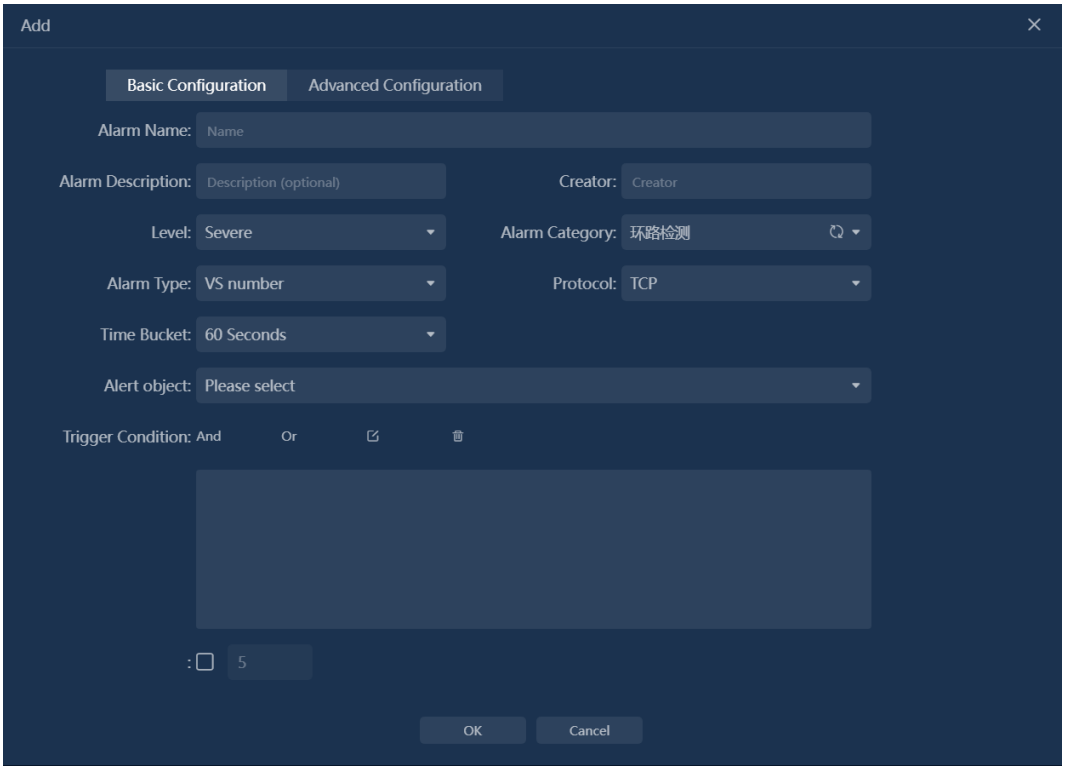


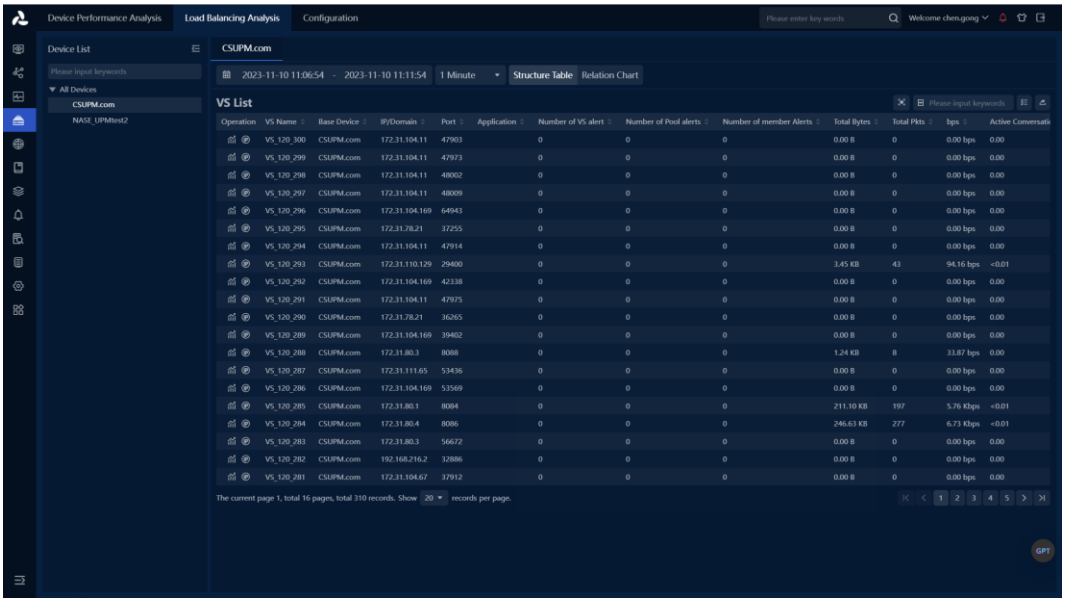
Table 20-3 Configuration Description

Operation	Description
Alarm Name	Configure the name of the alert for easy identification of the alert type that occurred
Alarm Description	Configure the description information related to the alert
Creator	Set the configuration staff for the alert
Level	The alert level is divided into high, medium, and low levels, configure the severity of the alert
Alarm Category	Configure the types of issues that trigger the alert
Alarm Type	Select to configureVSor Member triggered alerts
Protocol	Configure the data protocol types that trigger alarms
Time bucket	Configure the time bucket scale for triggering alarm data
Duration count	Configure the number of times the trigger condition needs to be met before an alarm is issued
Alert object	Configure the nodes that trigger VSor Member alarms
Trigger Condition	Configure the trigger conditions for related network metrics

20.2.3. Load balancing analysis

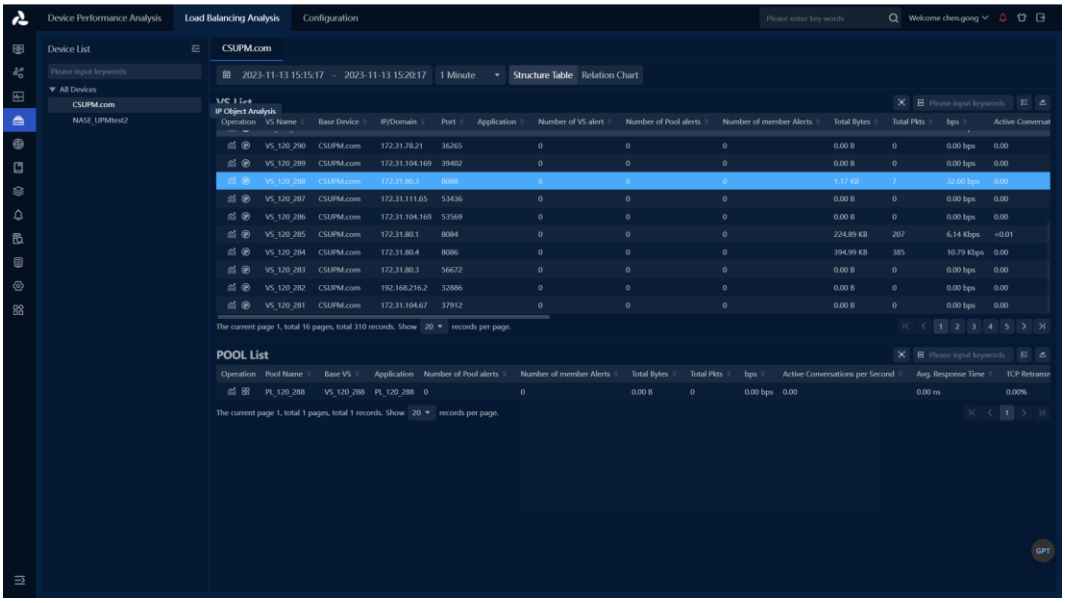
1. Load Balancing Analysis' in the menu to enter the load balancing analysis page, which initializes the display of VS indicator parameters, as shown in the figure below.

Figure 20-10 Load Balancing VS Analysis



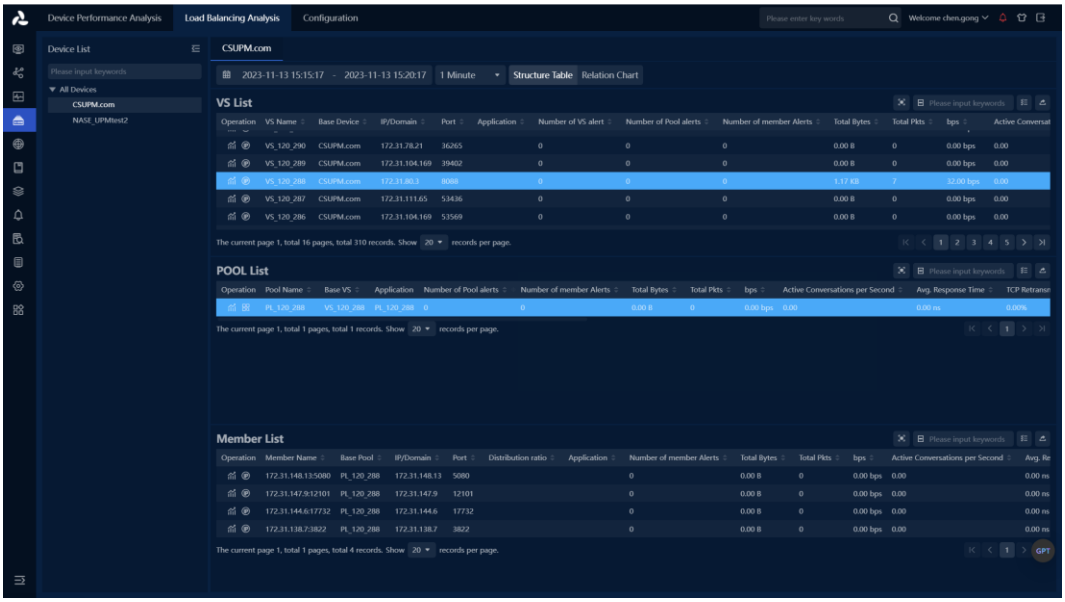
2. Click on the VSrow to expand and view the indicator parameters of the Pool included in that VS.

20-11Figure 26 11 Load Balancing Performance Analysis



3. Click on the Pool row to expand and view the metric parameters of the Members included in this Pool.

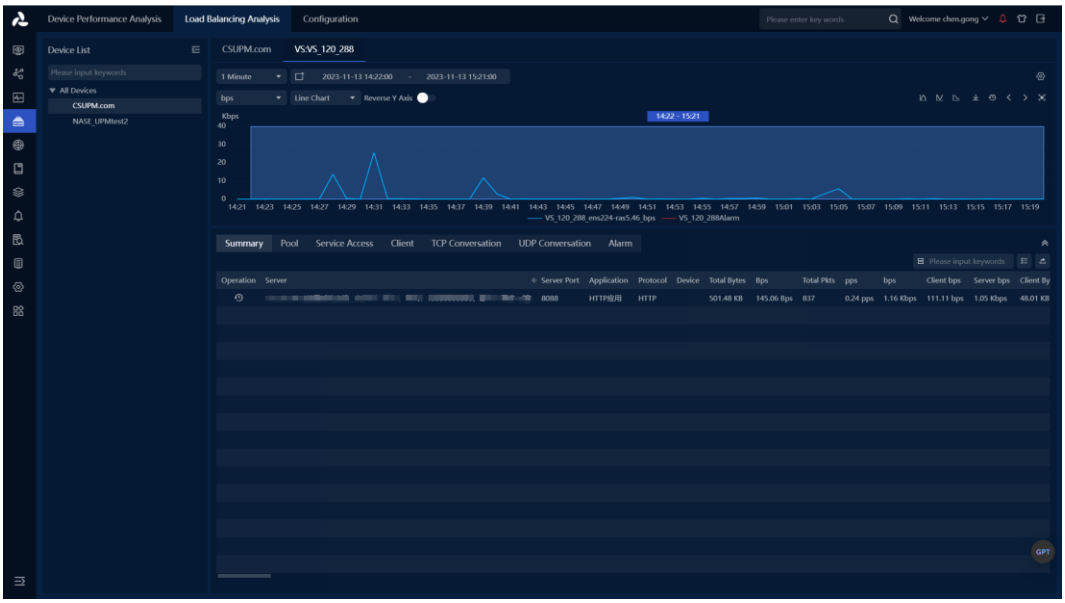
Figure 20-12 Load Balancing Member Analysis



20.2.3.1 Trend Analysis

 Click on the Trend Analysis button in the Operation column to enter the Trend Analysis page for this node, as shown in the following figure.

Figure 20-13 Trend Analysis



The operation of the Trend Analysis page is the same as the existing Trend Analysis function.

20.2.3.2 IP Object Analysis

 Click on the IP Object Analysis button in the Operation column to enter the IP Object Analysis page for this node.

The operation of the IP Object Analysis page is the same as the existing IP Object Analysis function.

20.2.3.3 Application Object Analysis

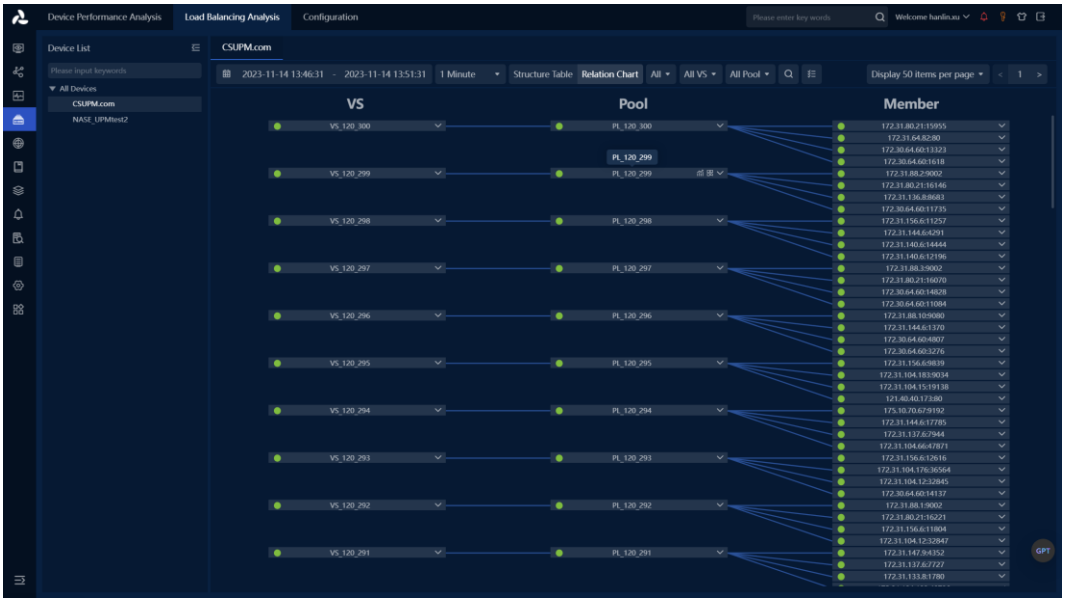
 Click the Application Object Analysis button in the operation column to enter the Application Object Analysis page of this node.

The operation of the Application Object Analysis page is the same as the existing Application Object Analysis function.

20.2.3.4 Relationship Graph Analysis

Click the button to enter the VS, Pool, Member Relationship Graph mode to view analysis data. You can switch to view all nodes or only view alarm nodes. Alarm nodes are displayed at the top. You can also directly perform trend analysis, IP Object Analysis, and Application Object Analysis on nodes. As shown in the following figure.

Figure 20-14 Relationship Diagram Analysis



Note

1. Before viewing network metric data and performing trend analysis, I P object analysis operations, you need to configure the probe first.
2. After successfully generating applications in the interface configuration for VS, Pool, and Member, you can perform application object analysis.

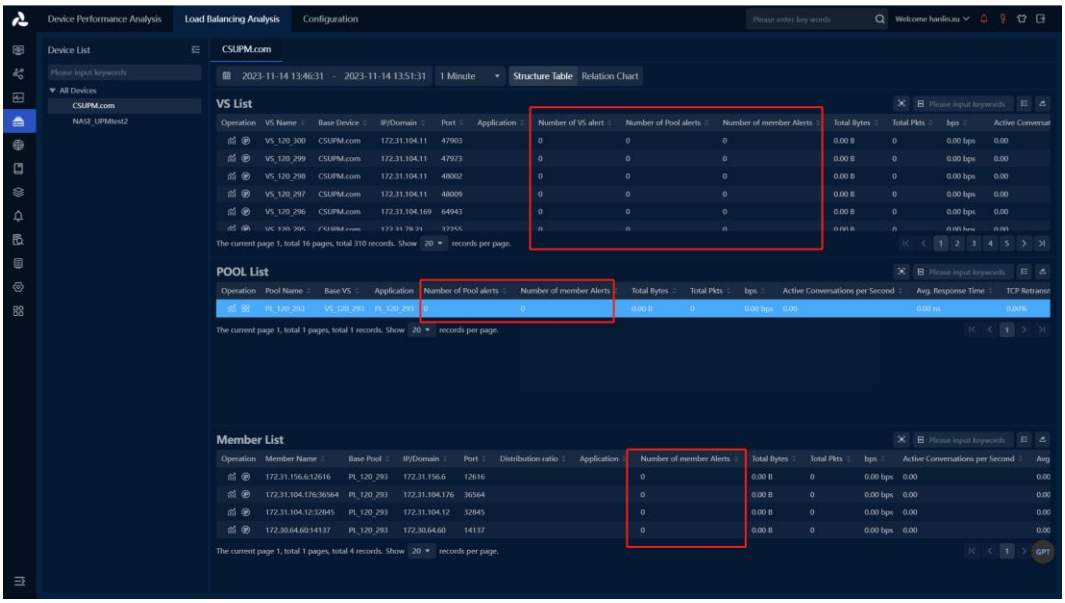
20.3. Load Balancing Alerts

In the load balancing analysis table, you can directly view the number of alerts for each node.

20.3.1. Alert Statistics

In the load balancing analysis structure table, VS can view the number of alerts triggered by itself and its subordinate Pool, Member; Pool can view the number of alerts triggered by itself and its subordinate Member; Member can view the number of alerts triggered by itself. As shown in the following figure.

Figure 20-15 Alarm Statistics



21. SNMP

21.1. Features

21.1.1. Technical background

SNMP is a communication protocol between a management process (NMS) and an agent process (Agent). It specifies a standardized management framework for monitoring and managing devices in a network environment, a common language for communication, and corresponding security and access control mechanisms. Network administrators can use the SNMP function to query device information, modify device parameter values, monitor device status, automatically discover network faults, and generate reports.

The network architecture consists of three parts: NMS, Agent and MIB.

- NMS: It is a system that uses SNMP protocol to manage and monitor network devices.
- Agent: It is an application module in the network device, which is used to maintain the information data of the managed device and respond to the request of the NMS.
- MIB: is a collection of managed objects.

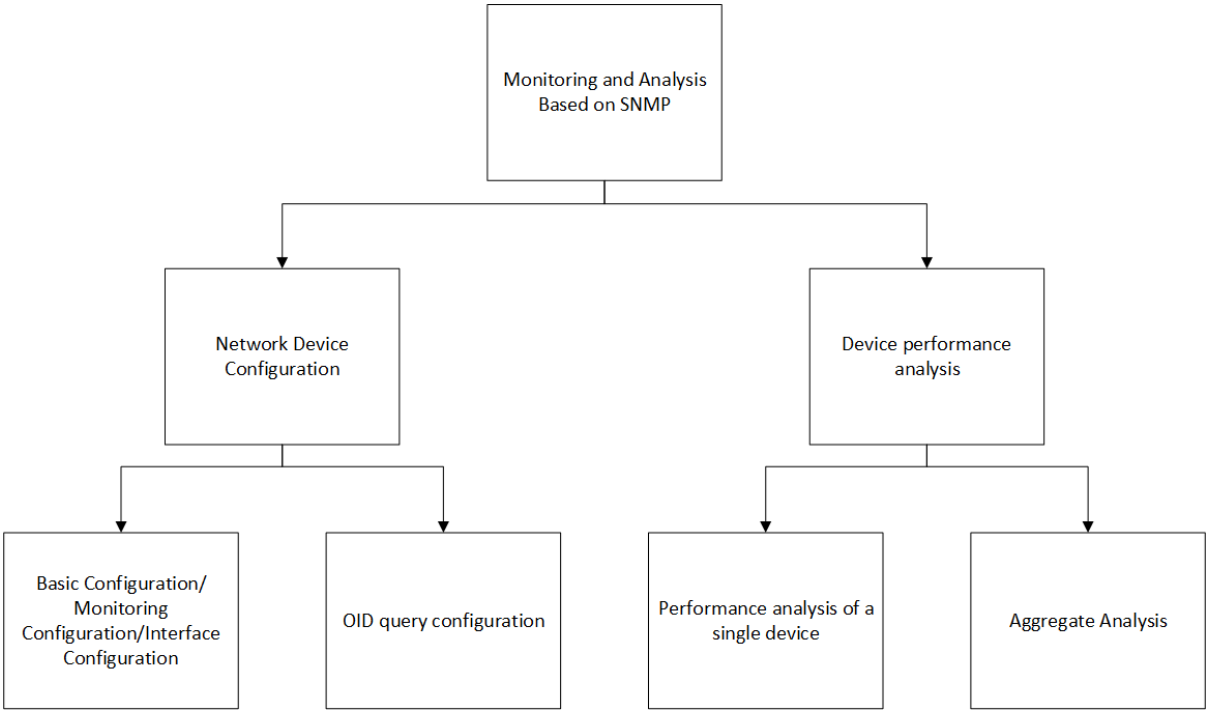
The NMS can send a request to the Agent to query or modify one or more specific parameter values. After the Agent receives the request information from the NMS, it completes the query or modification operation, and sends the operation result to the NMS to complete the response. MIB can also be regarded as an interface between NMS and Agent. Through this interface, NMS can perform read/write operations on each managed object in Agent, so as to achieve the purpose of managing and monitoring equipment.

21.1.2. Functional structure

SNMP-based performance analysis is mainly composed of two parts: network device configuration and device performance analysis.

- Network device configuration provides unified management of network devices, network device groups, interfaces, indicator items, indicator groups, and query templates.
- Device performance analysis provides a display platform for unified monitoring and analysis of SNMP data, and also integrates and displays NetFlow data, making up for the lack of traffic indicators and performance indicators supported by SNMP.

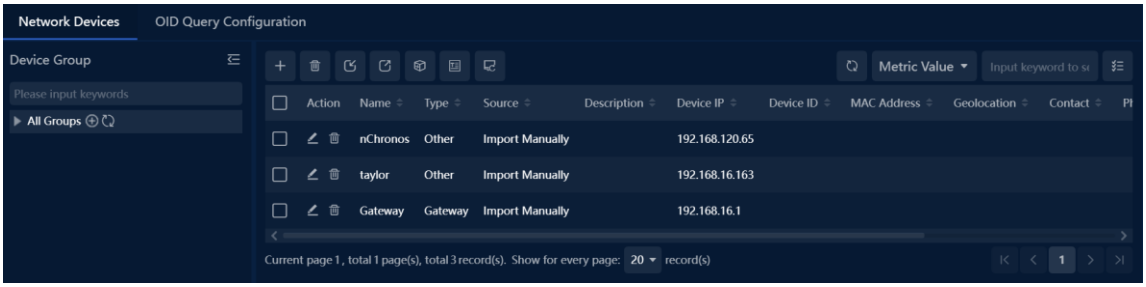
The functional structure is shown in the following figure:



21.2. Device configuration

21.2.1. Network device configuration

Network device configuration supports adding network devices such as switches, routers, and firewalls that exist in the network to the system. The configuration page consists of a device grouping tree list and a device list, as shown in the following figure:



The root node and device grouping node in the device grouping tree list support functions as shown in the following table:

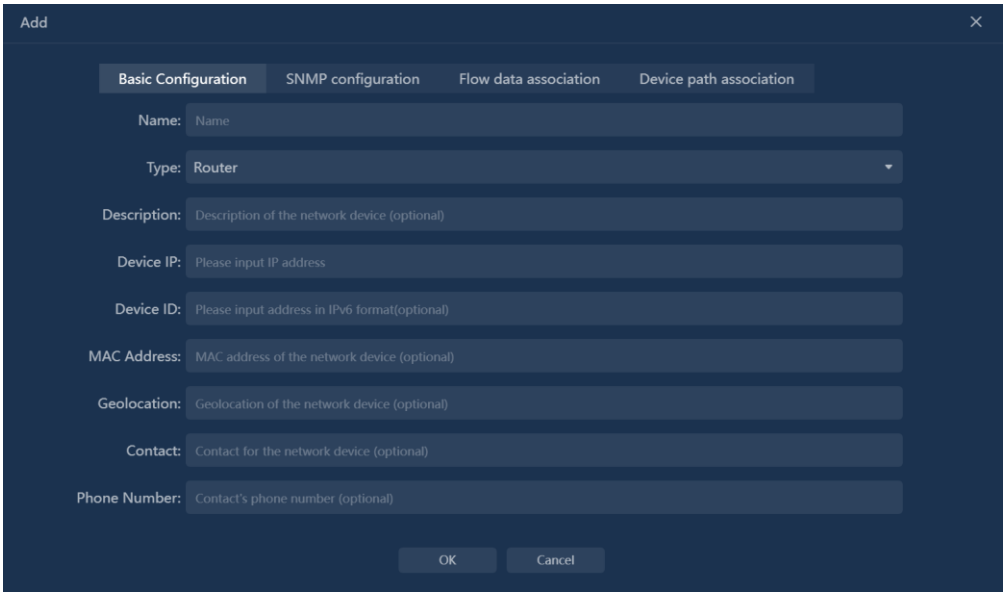
operate	illustrate
	Add subgroup
	Edit current group
	delete current group
	Update interface information

The functions of the action bar above the device list are shown in the table below:

operate	illustrate
	Add network devices, see 3.1.1 Basic Configuration 3.1.2 Monitoring configuration
	delete network device
	Export network device configuration
	Export network device configuration
	mobile network equipment
	Set query templates in batches
	Automatically update the interface configuration, support to configure the frequency of automatic interface update, support to configure the enabled/disabled state of the interface name that needs to be synchronized to the name table.

21.2.2. Basic configuration

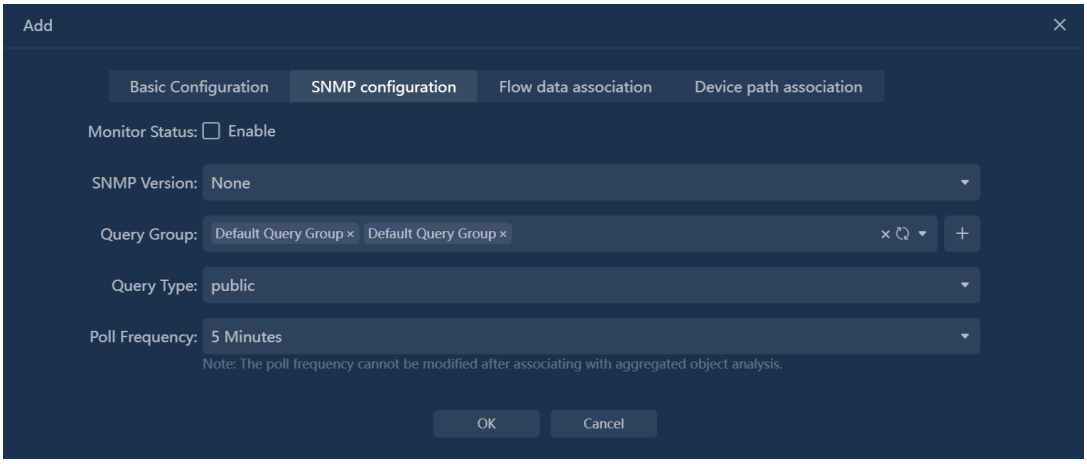
Click the button to add a network device. The basic configuration is shown in the following figure:



In the basic configuration, the device name and device IP address are required, and the device IP address is used as the proxy IP for SNMP monitoring.

21.2.3. Monitoring configuration

Click the button to add a network device. The monitoring configuration is shown in the following figure:



Monitoring status is not enabled by default. After enabling, configuration parameters are required, as shown in the following table:

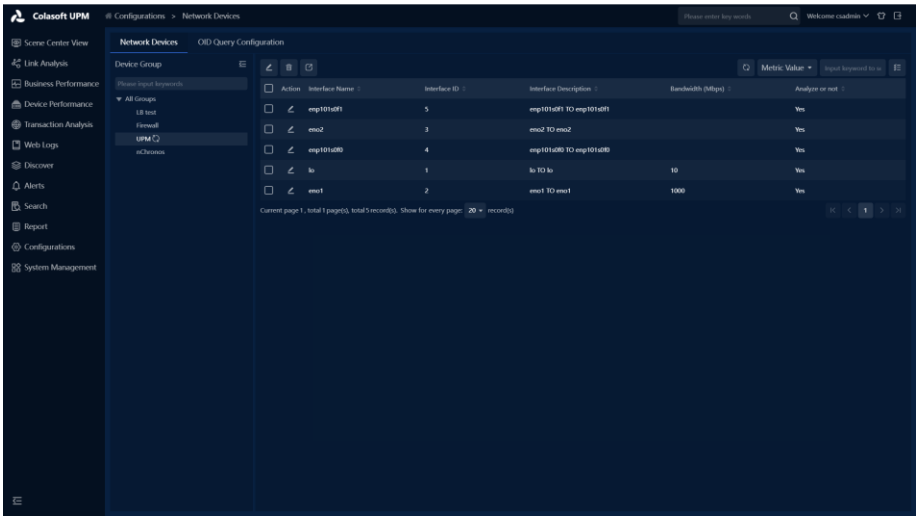
Operation	Description
Correlate NetFlow data	with backtracking NetFlow links based on device proxy IP or name
SNMP protocol version	Support SNMPv1 , SNMPv2 , SNMPv3 three protocols
Certification	select the SNMPv1 or SNMPv2 protocol version, you need to set the read community name . If you select the SNMPv3 protocol version, you do not need to set the read community name , but you need to set the SNMPv3 security parameters.

Monitoring frequency	Support 5 types of frequencies: 5 seconds, 10 seconds, 30 seconds, 1 minute, and 5 minutes . A frequency of 1 minute or 5 minutes is recommended .
Monitoring templates	The default template has been associated, and additional associated custom templates are supported. The scope of metrics monitored by the device is determined by the template.
Query category	default category public has been selected , and switching to a custom category is supported. It is the class that determines which class of OIDs the device uses when polling .

21.2.4. Interface configuration

After the device monitoring configuration is completed, the interface information will be automatically obtained once. Click on the device name node in the tree list to view the interface list. As shown in the following figure:

Figure 3.4 Interface List



The functions of the operation bar above the device list are shown in the following table:

Table 21-1 Operation Instructions

Operation	Description
	Batch edit interfaces, support configuring interface description, interface bandwidth, and enabling interface trend analysis.
	Delete Network Device
	Export Network Device Configuration

Individual interface configuration and batch interface configuration. As shown in the following figure:

Figure 21-2 Single Interface Configuration

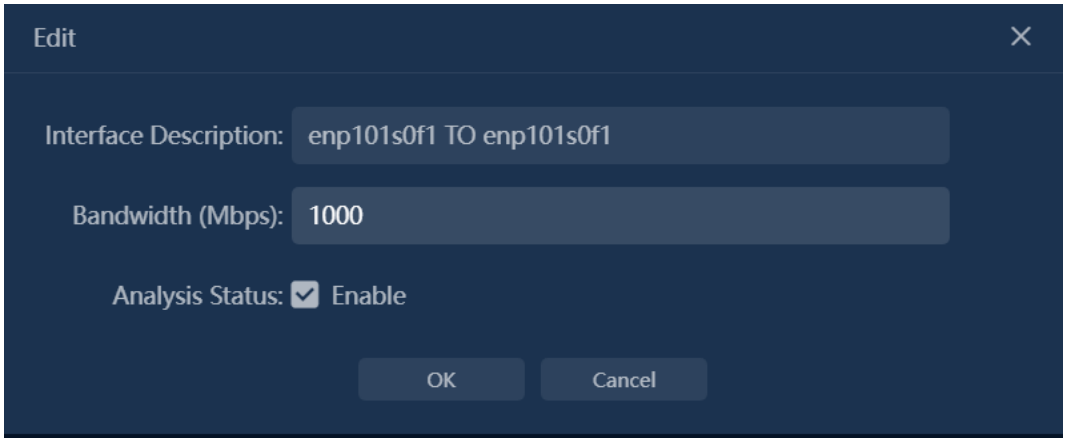
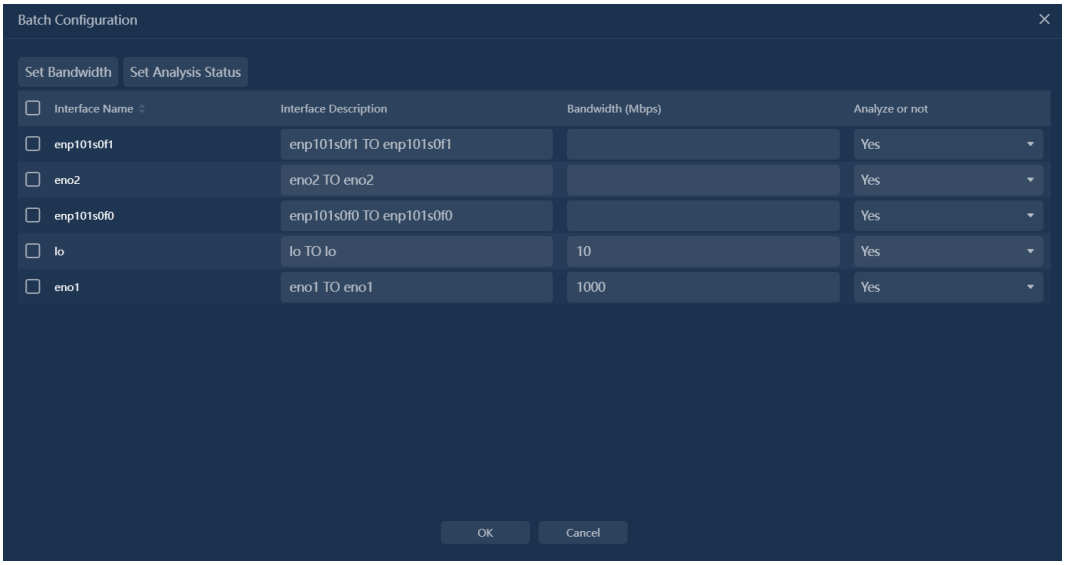


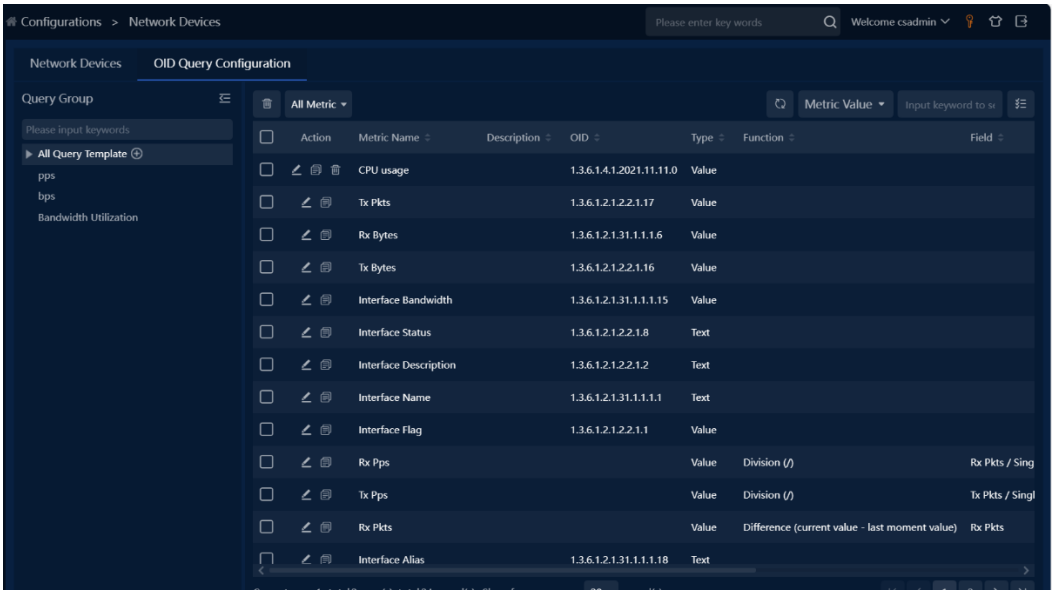
Figure21-3 Batch Interface Configuration



21.3. OID query configuration

The OID query configuration is used to configure and manage monitoring indicators (divided into common indicator configuration and calculation indicator configuration), indicator groups, and query templates. The OID query configuration page consists of a

query template tree list and an indicator list, as shown in the following figure:



The supported functions of the root node and template node in the query template tree list are shown in the following table:

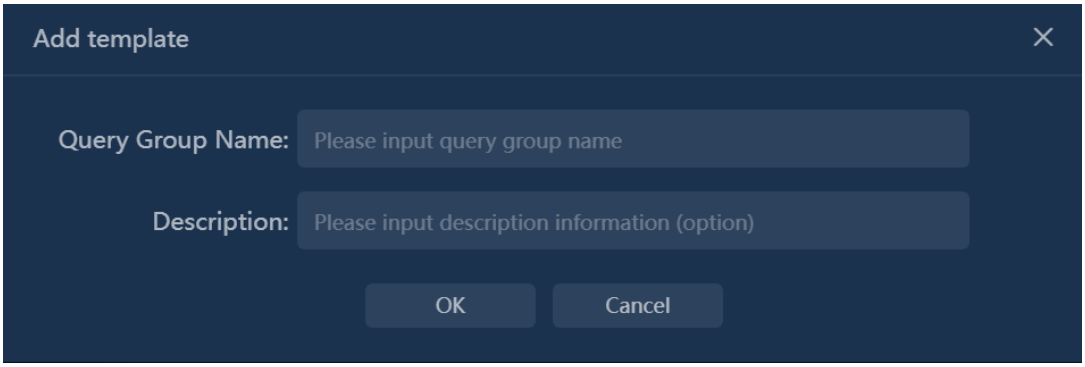
operate	illustrate
	To add a query template, see 3.2.1 Query Template Configuration
	Edit query template
	delete query template

The functions of the action bar above the indicator list are shown in the table below:

operate	illustrate
	To add common indicators, please refer to 3.2.3 Common Indicator Configuration
	delete indicator
	Compile the MIB library and display the OID tree list.
Add calculated metrics	add calculation indicators, please refer to 3.2.4 Configuration of calculation indicators
Metric filtering	Filter options include: all indicators, common indicators, calculated indicators

21.3.1. Query Template Configuration

The system has built-in default templates. Users can click the button on the right side of all query template nodes to add custom query templates, as shown in the following figure:

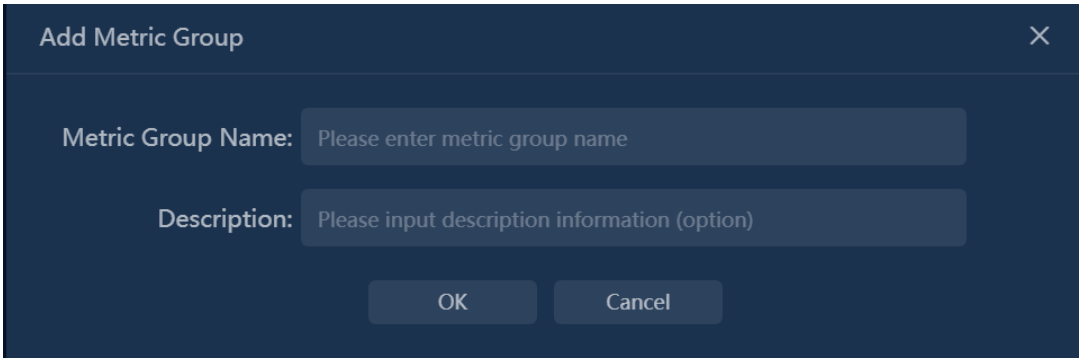


21.3.2. Metric group configuration

Indicators of the same indicator group will be displayed on the same trend graph in the device performance analysis. The system has built-in three default indicator groups, including:

- The number of packets per second, the indicators include the number of packets received per second, the number of packets sent per second.
- Bit rate, indicators include receive bit rate, send bit rate.
- Bandwidth utilization, indicators include receiving utilization and sending utilization.

Users can click the button on the right side of the template node to add a custom indicator group, as shown in the following figure:



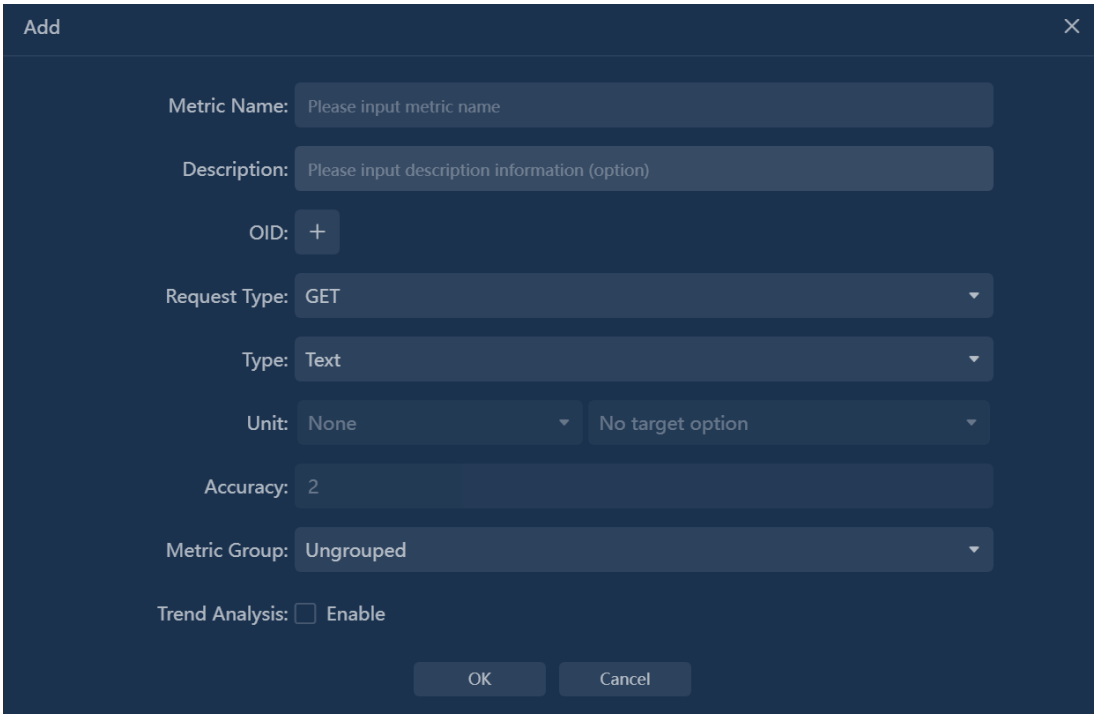
21.3.3. Common indicator configuration

The system has built-in default common indicators, including:

- The cumulative number of packets sent
- Accumulated number of received packets
- Accumulated number of bytes received
- Cumulative number of bytes sent
- interface bandwidth
- interface status
- Interface description

- interface name
- Interface ID
- Number of interfaces

Users can click the button to add custom common indicators, as shown in the following figure:



For monitoring indicators, you need to configure the indicator name, OID, OID category, request method, value type, unit, and trend analysis enabled status.

The configuration instructions are shown in the following table:

Table 3.7 _ Configuration instructions

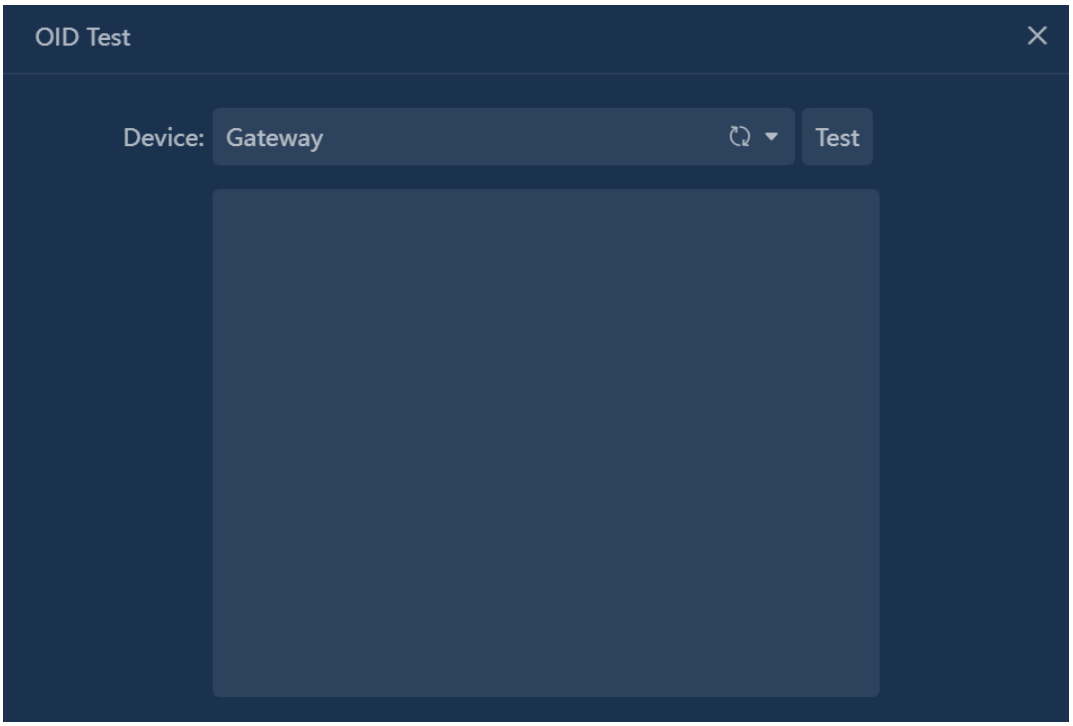
operate	illustrate
OID	Configure the OID query category and OID, and support the configuration of multiple OIDs. Support to quickly add OIDs and test OID availability .
request method	GET , WALK two ways.
value type	Text and numeric types
unit	
Preserve decimal places	
Indicator group	Configure the indicator group to which it belongs
trend analysis	Configure analytics enabled/disabled state

Note

Units can be configured in "Configuration" -> "Unit Conversion".

OID can be quickly added through MIB compilation. After compilation, select the OID to be used, and click OK to automatically backfill it into the OID input box of the indicator configuration.

OID can be tested to verify whether the OID is available, click the “Test” button, as shown in the following figure:

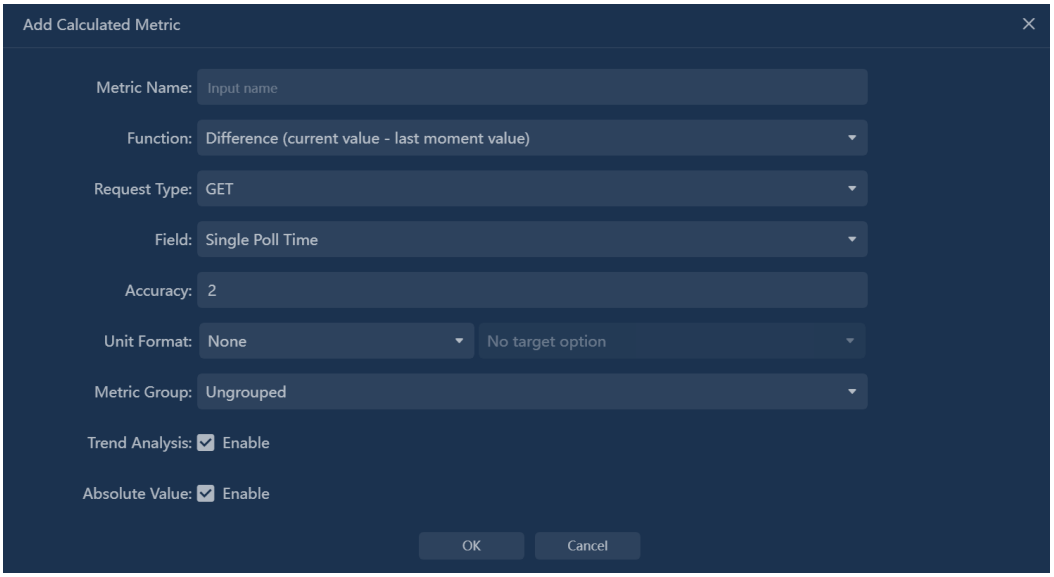


21.3.4. Calculated indicator configuration

The system has built-in calculation indicators, including:

- receive packets
- send packets
- Number of received bit rates
- send bit rate
- received bytes
- number of bytes sent
- Received packets per second
- Number of packets sent per second
- Receive utilization
- Send utilization

- Users can click Add Calculated Metric the button to add custom calculation indicators, as shown in the following figure:



Calculation functions support difference, percentage, and divide.

In the calculation field, you can select common indicators and calculated indicators.

21.4. Analyze

21.4.1. Equipment performance analysis

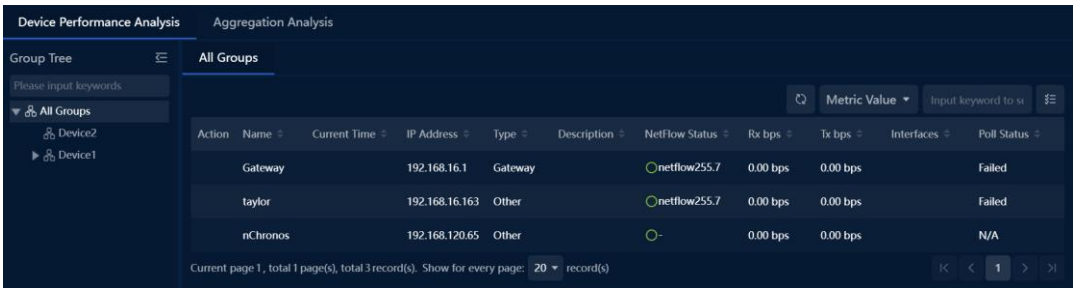
You can view the summary information of all devices in a group, and view the trend analysis of monitoring indicators of a single device.

You can view the summary information of the interfaces on the device and view the trend analysis of monitoring indicators of a single interface.

The device performance analysis page consists of a device grouping tree list and a data display area.

Equipment Analysis

Click the grouping node in the grouping list to view the device overview information. You can see the device name, device flow status, device SNMP indicator data and other information, as shown in the following figure:

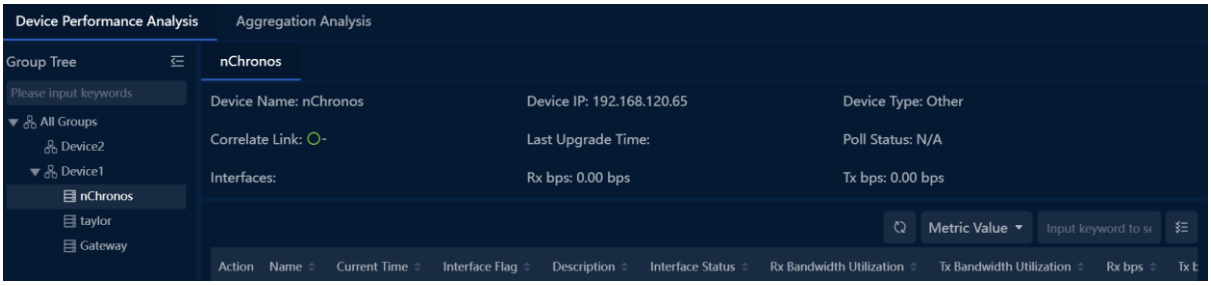


Click the trend analysis button in the operation column to view the trend analysis results of a single device. The trend graph displays SNMP data, and the list displays NetFlow data.

Click the Traffic Analysis button in the Action column to view the associated NetFlow traffic analysis results.

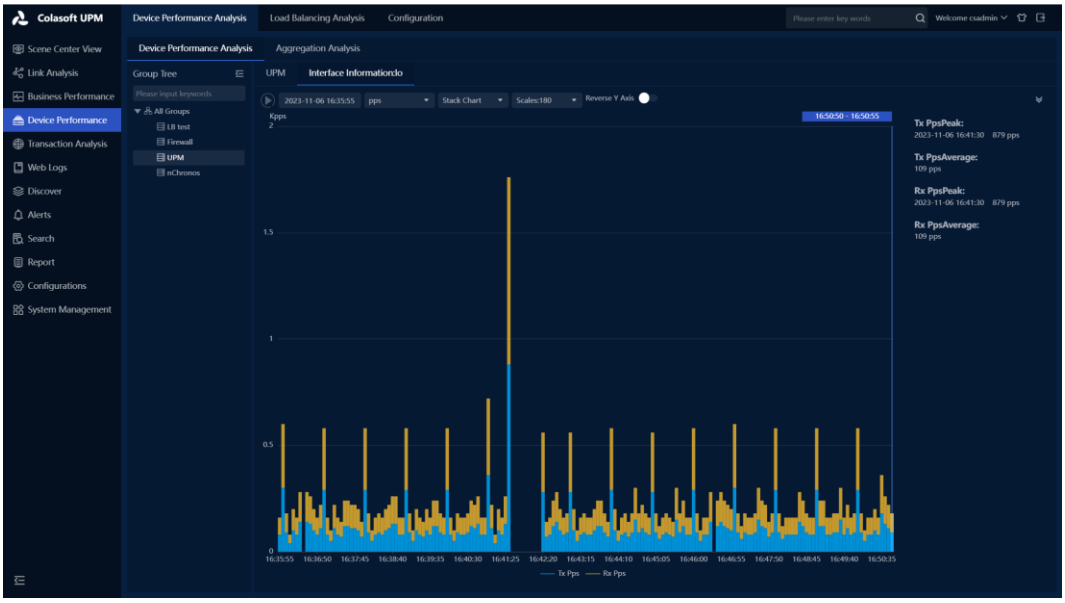
Interface Analysis

Click the device node in the group list to view the interface summary information. You can see the basic device information, interface name, interface flow status, and interface SNMP indicator data, as shown in the following figure:



Click the trend analysis button in the operation column to view the trend analysis results of a single interface. The trend graph displays SNMP data, and the list displays Net Flow data.

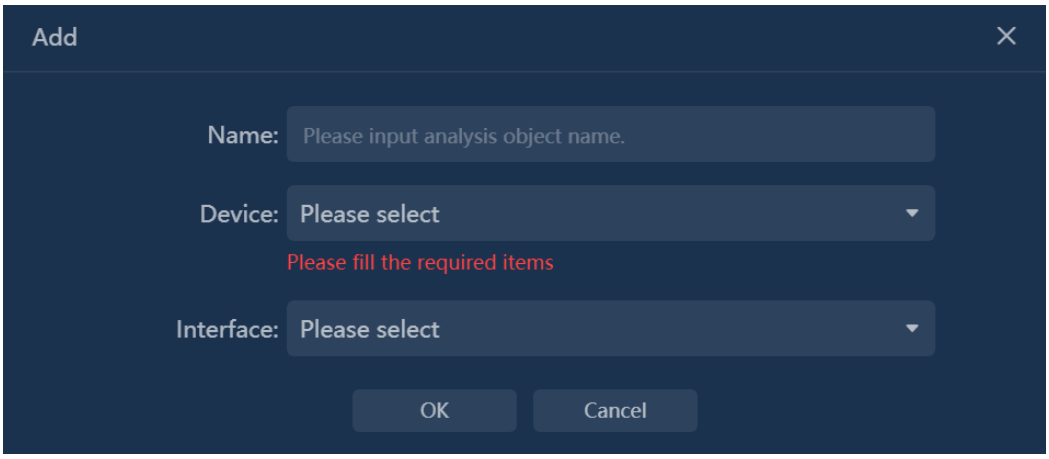
Figure 21-4 Interface Trend Analysis



Aggregate Analysis

Supports interface aggregation analysis across devices. First, the aggregation interface needs to be defined, and then trend analysis is performed.

Define the aggregation interface as shown in the following figure:



Click the Trend Analysis button in the operation column to view the trend analysis results of the aggregated objects. The trend graph displays SNMP data, and the list displays Net Flow data.

22. Alarm

22.1. Function Introduction

22.1.1. Function Description

Alerts is a centralized display of alarm log menus in the UPM system that are scattered in various functional modules, with various filter conditions set to facilitate precise location and quick search of alarm log details of related objects.

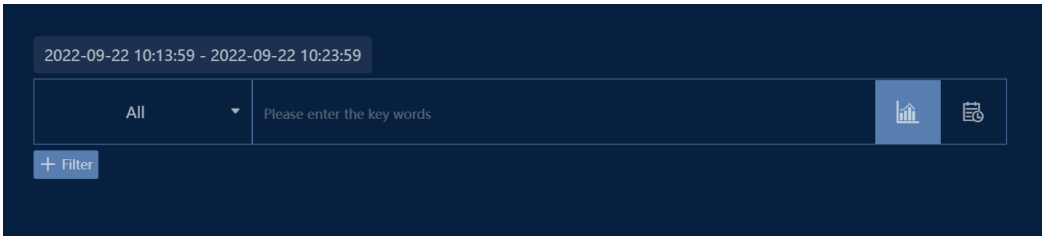
22.1.2. Functional scenarios

After UPM triggers an alarm, it is directly displayed centrally in the unified alarm log monitoring page, which is suitable for viewing the daily alarm log of UPM and statistical display of alarm information triggered by specific objects, so as to quickly view all relevant alarm information and improve troubleshooting efficiency.

22.1.3. Functional value

- Alarm logs are displayed in a unified and centralized manner, making it easy to view and locate problems as a whole.
- You can filter the alarm logs to view specific objects and contents, and quickly sort out the causes of problems.
- Multi-dimensional statistics on the number of alarms to provide a reference for optimal alarm configuration.
- Multiple alarm log filter dimensions and filter criteria to find the exact information you need.

22.1.4. Alarm filtering



The query filtering of alarms uses keyword fuzzy query and filtering condition exact query in two ways. Among them.

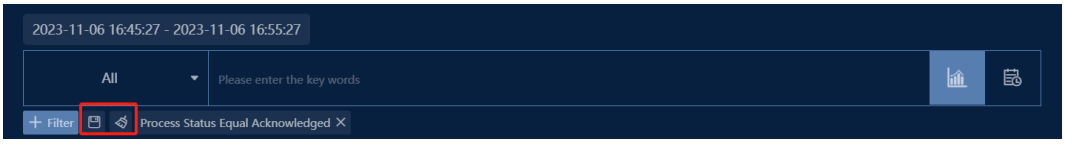
1. Fuzzy queries cover most of the fields in the alarm log, such as alarm name, alarm details, IP address, etc.

2. Filtering conditions cover most of the alarm attribute information, such as alarm name filtering, alarm level filtering, IP address filtering, port filtering, MAC address filtering, link filtering, alarm type filtering, transaction name filtering, etc.

Click  in the search bar to view the alarm log statistics calculated based on the filter criteria; click  in the search bar to view the filtered alarm log details. When you do not fill in the filter criteria statistics or view the logs, all the alarm information within the time period is automatically queried.

22.1.5. Filter Condition Save and Clear

Figure 22-1 Filter Condition Save

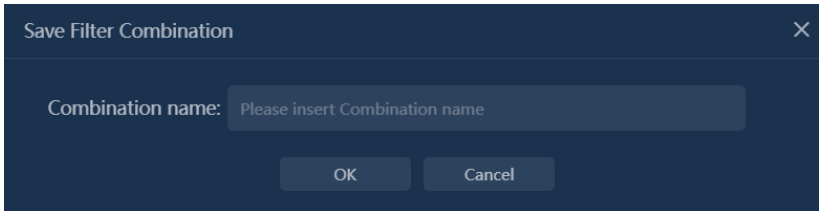


After adding filter conditions, the button  will be displayed.

1. Filter Condition Save

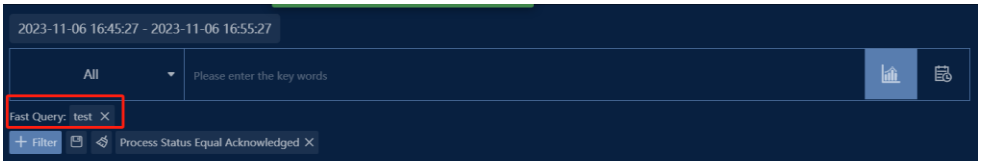
(1) After clicking the  button, a save dialog will pop up. Enter the combination name of the search conditions and click OK to save.

Figure 22-2 Filter Condition Save



(2) After saving, the saved combination names will be displayed below the search input box. Clicking on them will automatically fill in the filter conditions and complete the filtering. Additionally, you can instantly add or modify filter condition combinations.

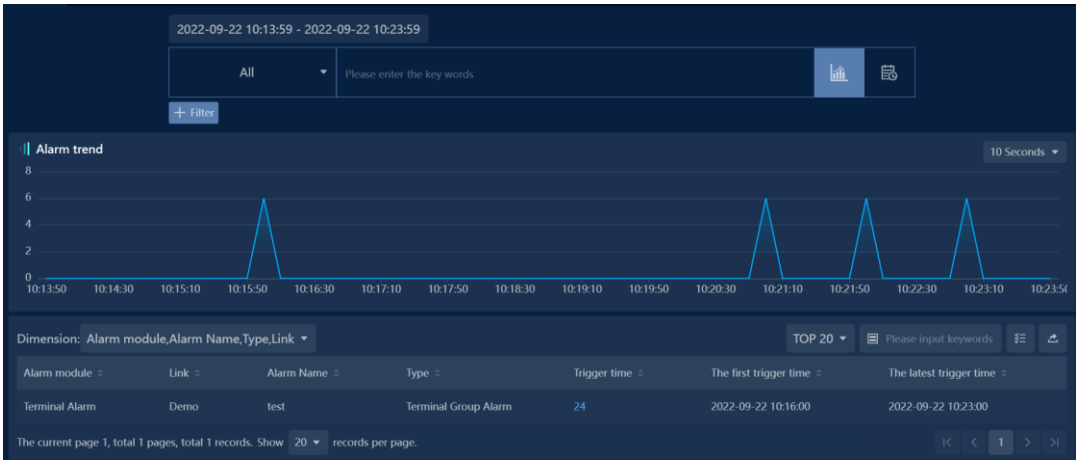
Figure 22-3 Filter Condition Save



2. Filter Condition Clear

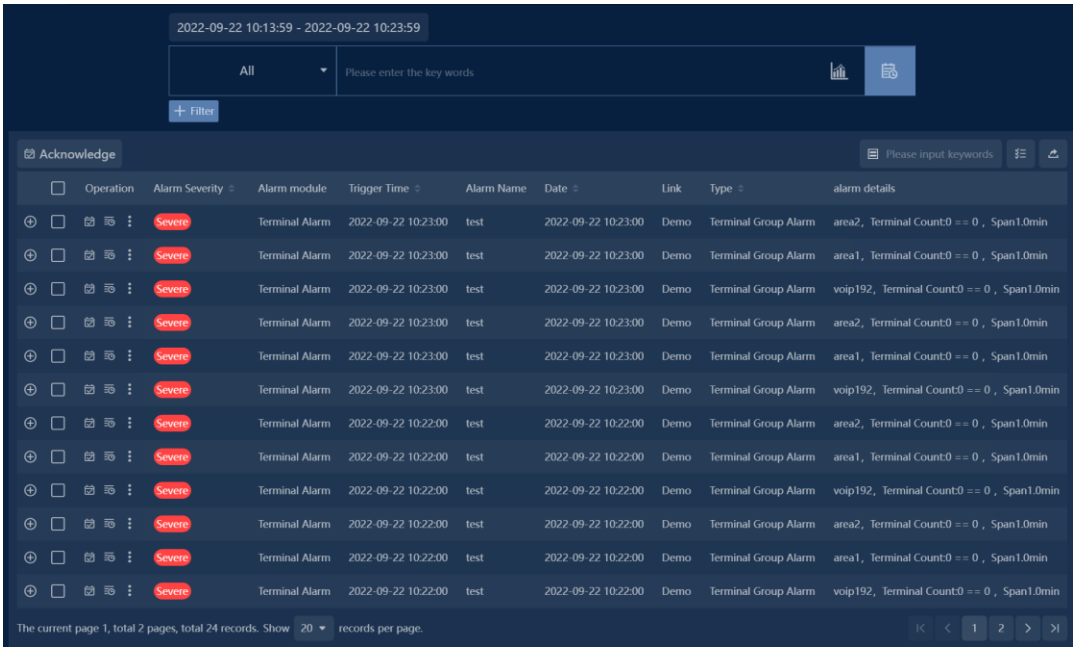
After selecting filter conditions to complete log filtering and needing to clear them for the next filtering search, click the  button to clear all conditions.

22.1.6. Alarm Statistics

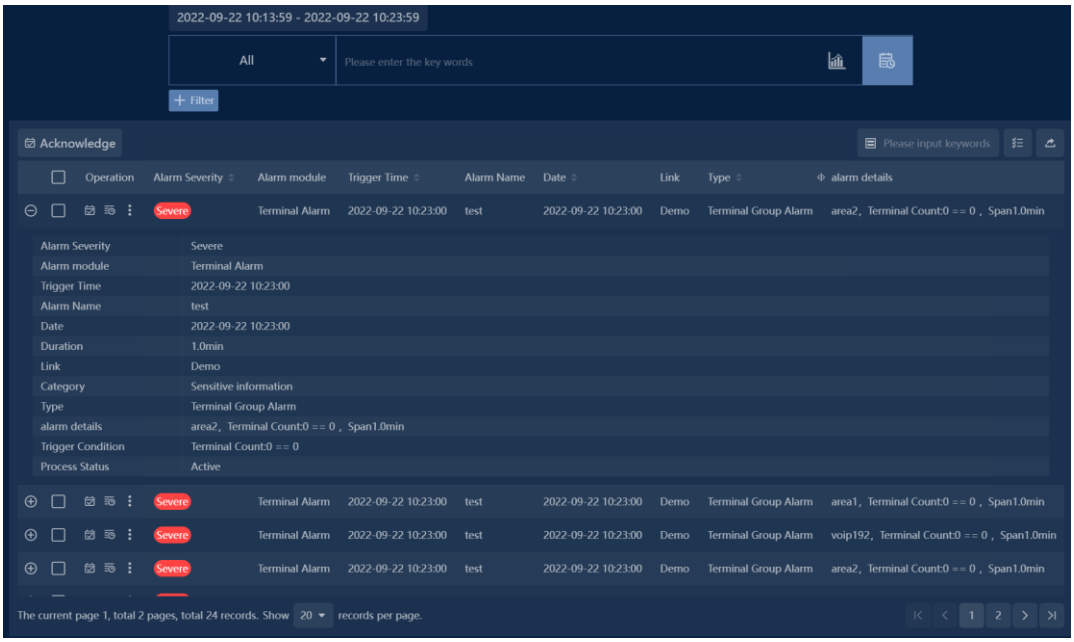


1. Alarm statistics to view a trend of the number of alarms triggered at each moment in the selected time range
2. Comprehensive statistics on the number of alarm triggers according to various dimensions are available, and you can jump to view the corresponding log details by clicking the trigger number.

22.1.7. Alarm Log



Alarm logs can be viewed according to filtering criteria, or all log details within a specified time period can be queried directly without setting any criteria.



The action buttons of the alarm log can be operated according to the log type. Click the plus sign to see the detailed information of this log.

23. Smart Baseline

23.1. Features

23.1.1. The term

CSAIS

The abbreviation of Colasoft Artificial Intelligence Server is an intelligent baseline detection system independently developed by Colasoft.

23.1.2. Functional background

It is impossible to judge whether the fluctuation is within the normal allowable range simply by the indicator trend, and it is impossible to compare and analyze the historical situation to evaluate the indicator status.

Users cannot explicitly set a reasonable fixed threshold, the alarm threshold is single, the false alarm rate and false alarm rate are high, and reliable alarm information cannot be provided for users.

The fixed alarm threshold cannot be updated with the actual situation, and manual operation is required. Especially in the case of frequent requirements, manual operations cannot respond quickly.

23.1.3. Functional value

Using the AI baseline engine automatic learning and intelligent algorithm technology, it monitors the key indicators of the specified objects, actively detects abnormalities and gives alarms, and graphically displays the abnormal period information.

Reduce the alarm false alarm rate and false alarm rate, improve the efficiency of operation and maintenance analysis, and improve the ability of product intelligent analysis.

23.1.4. Function description

UPM baseline monitoring needs to be used with CSAIS, and communication between UPM and CSAIS is through the interface.

UPM is responsible for baseline management and monitoring and presentation, and issues baseline tasks to CSAIS.

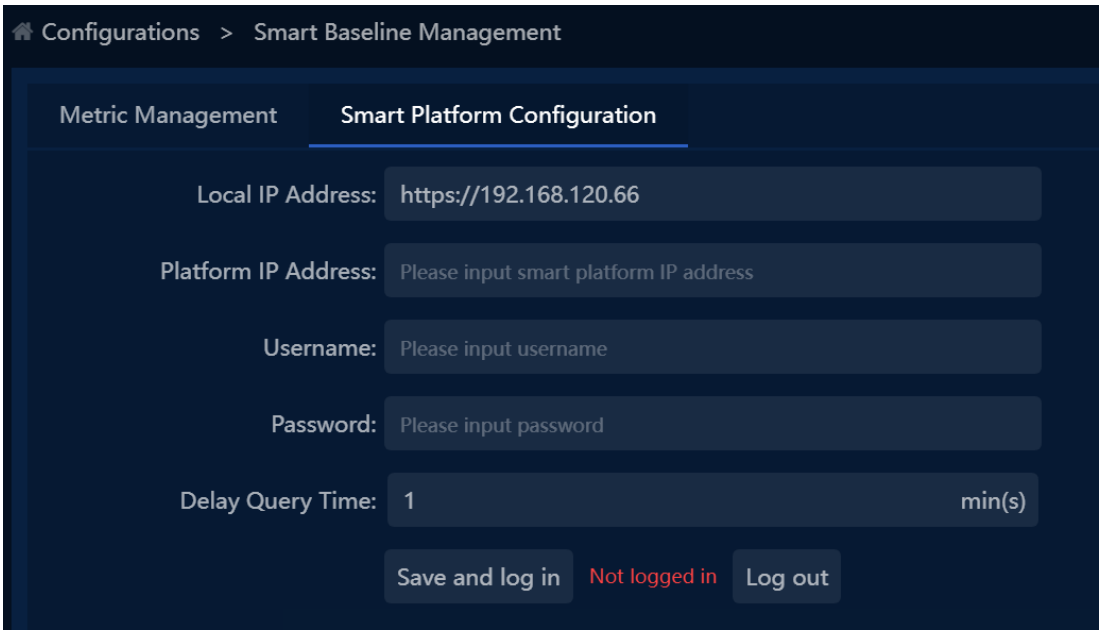
CSAIS is responsible for baseline data generation and anomaly detection, and transmits the results to UPM.

23.2. Operation guide

23.2.1. Connect with CSAIS

When performing intelligent baseline monitoring on UPM, it is necessary to establish a connection between UPM and CSAIS first.

Click the UPM menu navigation "Configuration" -> "Intelligent Baseline Management", after entering the page, switch to the "Intelligent Platform Configuration" page, as shown below:



Enter the platform IP address, user name and password information of CSAIS . The default query delay time is 1 minute. After inputting, click the "Save and Login" button. If it shows logged in, it means the connection is successful. If it fails, there will be a failure reason prompt.

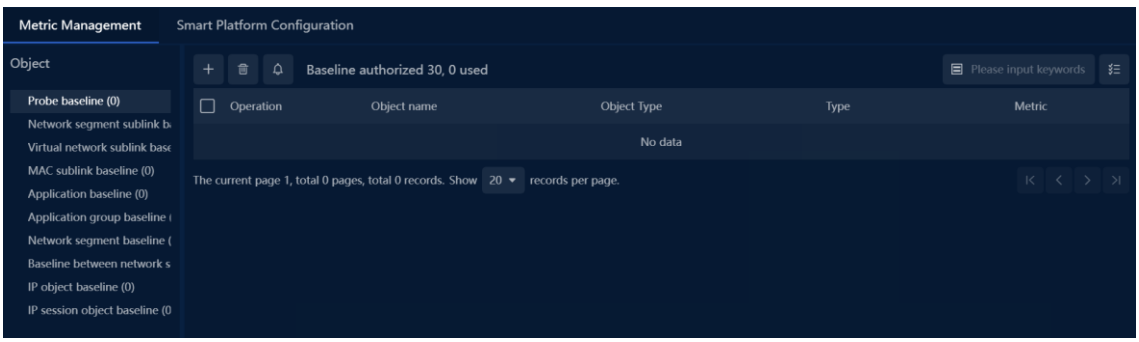
23.2.2. Add monitoring object

After the connection between UPM and CSAIS is successfully established, you need to manually add the objects to be monitored by the baseline. Currently, there are two ways to add them:

Method 1: Add through the indicator management function

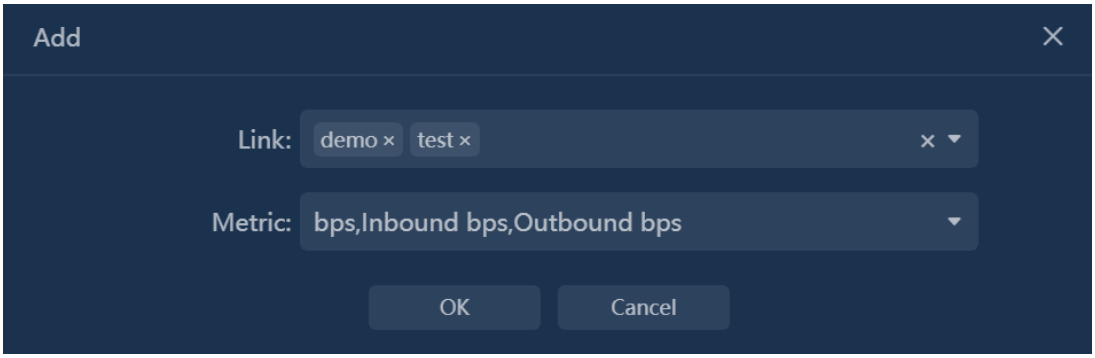
Click on the UPM menu navigation "Configuration" -> "Intelligent Baseline Management" -> "Metrics Management".

Supports baseline monitoring of all indicators of common links, aggregated links, network segment sub-links, virtual interface sub-links, MAC sub-links, applications, application groups, network segments, inter-network segments, IP, and IP sessions. Here you can manually add and delete in bulk. The following figure shows the management page:



- Add baseline monitoring objects and indicators: When adding, you can select multiple objects and indicators at the same time, and the system will combine the objects and indicators to add them.
- The following figure shows the baseline monitoring of the bit rate, total number of

sessions, TCP segment loss rate, incoming RTT, and outgoing RTT indicators of link ens161 and link-ens192. The number of added baselines is 10.



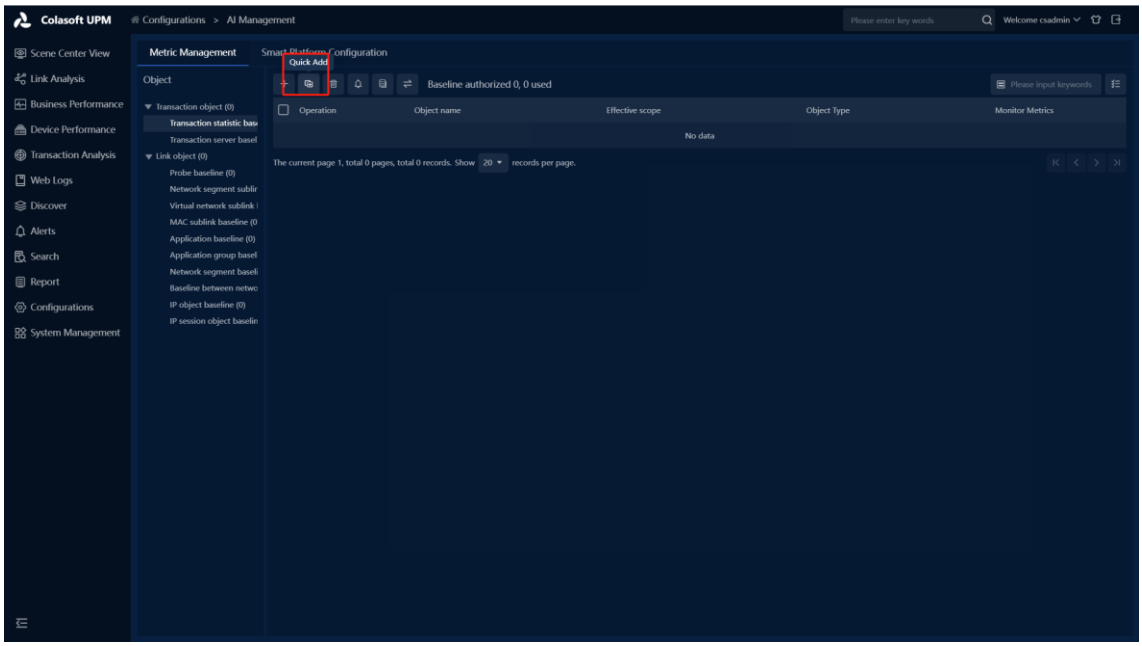
The table on the right: displays the monitored objects and indicators. The indicator names of the same objects are concatenated and displayed in the "Indicators" column.

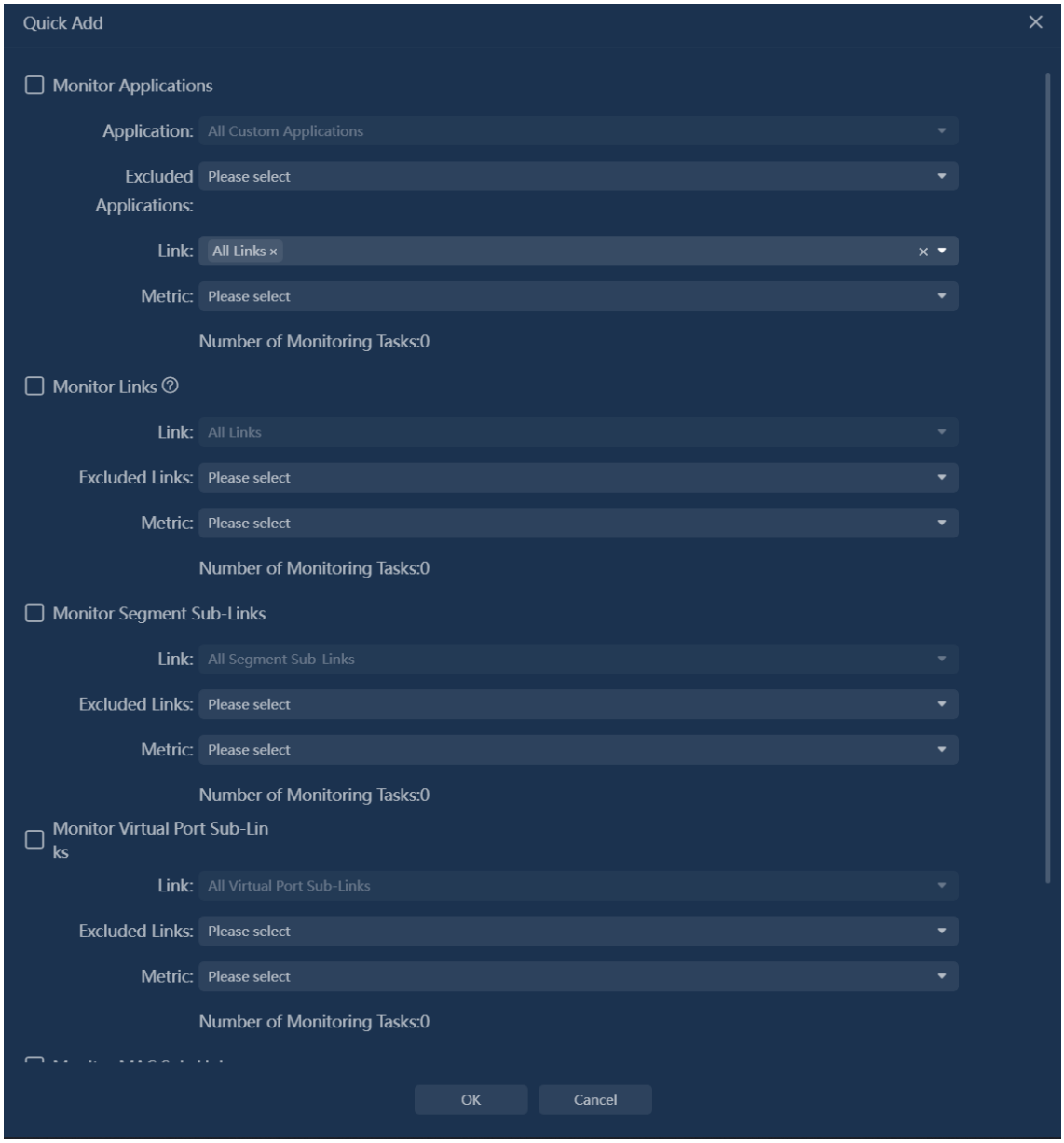
- Left tree: Displays currently supported monitoring objects and how many baselines are added to each object.
- Baseline authorizations: Refers to the number of baselines that can be monitored by the system, and cannot be added after the authorizations are exceeded.
- Alarm sending: For added indicator monitoring, the system will automatically perform baseline anomaly detection on indicators and generate alarm logs. If alarm notification is required, you can select the notification method through alarm sending.

Method 2: Add custom monitoring trend graph components

Click on the UPM menu navigation 'Configuration'-> 'Intelligent Baseline Management'-> 'Metric Management'.

Select and click the 'Quick Addition' button in the top operation bar of the table. This method can automatically perform baseline monitoring on the metrics defined in the system for links and applications. For example, when a new application or link is added to the system, the system will automatically add the link (or application) to the baseline monitoring based on this configuration.

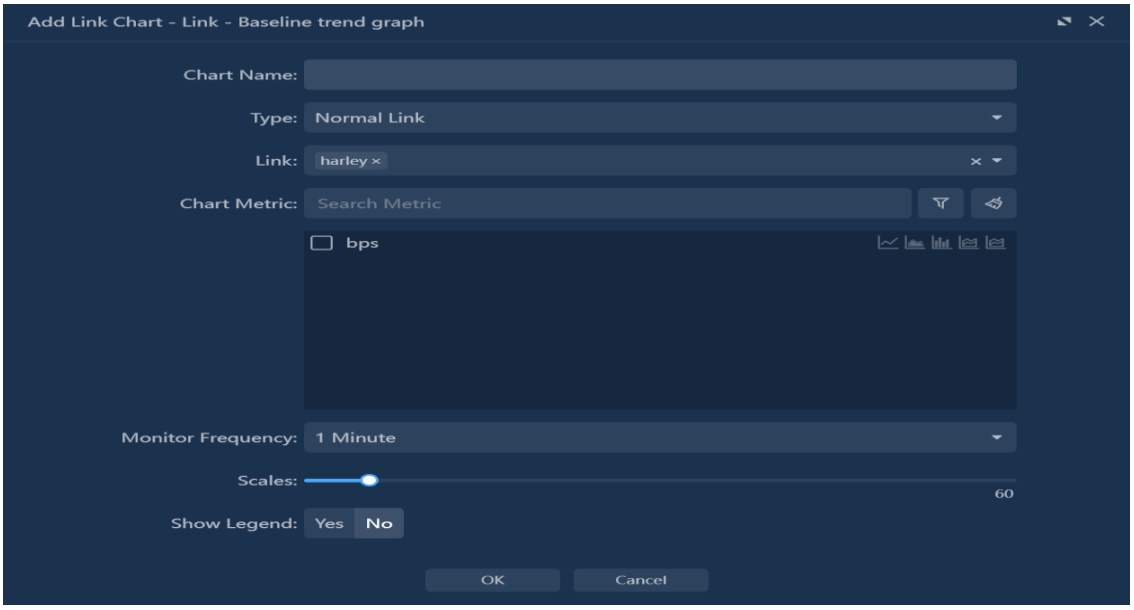




Method 3: Add custom monitoring trend chart component

In custom monitoring, trend chart components for regular links, aggregate links, subnet sublinks, virtual interface sublinks, MAC sublinks, applications, application groups, subnets, subnet interconnections, IP, and IP sessions can be directly added for baseline monitoring.

As shown in the following figure, when selecting a monitoring frequency of1minute, check the smart baseline when hovering over the indicator to enable baseline monitoring for that indicator.

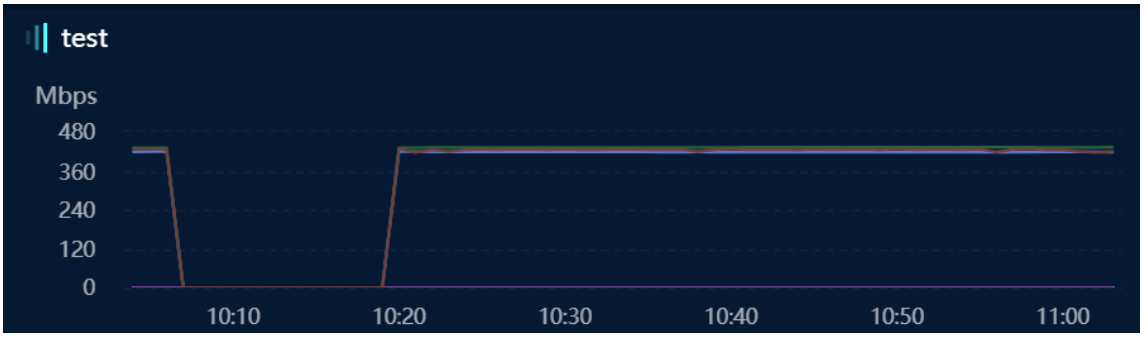


Refer to Chapter 1.2.3 Monitoring Display for the display effect.

23.2.3. Monitor display and analysis

The monitored indicators and change curves can be displayed in real time in the custom monitoring.

The monitoring effect is shown in the following figure, which shows the actual value and baseline value curve of the indicator. If there is an abnormality in the detection, it will be clearly marked in red, and the specific alarm content can be viewed in the upper right corner.



23.3. Common problem

1. About Metric Baseline Management

Problem Description

Baseline monitoring can be added to both custom monitoring and indicator management functions. How to manage?

Question answer

1、The monitoring indicators added in the custom monitoring will be viewed uniformly in

the indicator management function. The indicator management function is where all monitoring indicators are centrally managed.

2、 In the custom monitoring trend graph component, if the smart baseline is checked for the indicator, and then unchecked, the baseline monitoring of the indicator will not be deleted, and the system background will continue to monitor. To delete, you need to operate in the indicator management.

Question answer

The baseline alarm is inaccurate, how to manually optimize?

Problem Reply

1、 On the 'Intelligent Baseline Management' -> 'Metric Management' page, you can set monitoring strategies for metrics to manually optimize metric monitoring in this way.

In the edit metric operation, select metric monitoring parameters to optimize combinations from alarm direction, sensitivity, normal value range, and continuous count.
The normal value range refers to the range in which the metric does not generate alarms.

2、 The system also provides built-in metric monitoring parameter templates, which have default settings for some metric alarm parameters.

24. Kafka Log Collection

24.1. Features

24.1.1. Function description

the third-party system sends the data to Kafka in Json format, the system connects to Kafka as a consumer, consumes and uses the saved data in Kafka, analyzes it according to the field, and performs data perspective monitoring and analysis to improve the system's ability to respond to the first the ability to obtain third-party data.

24.1.2. Functional scene

1. Perspective monitoring and multi-dimensional perspective statistics of third-party data.

2.Retrieval viewing of third-party data.

3.Integrated collection of large amounts of third-party data.

24.1.3. Function value

- Improve the system's ability to obtain third-party data.
- Enhance the ability to combine third-party data with the product's own data.

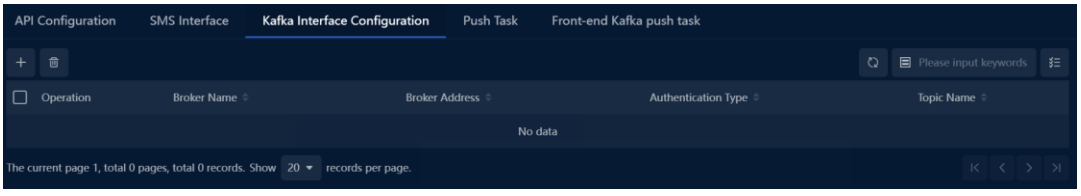
24.2. Operation guide

This section mainly introduces the configuration used for Kafka data consumption.

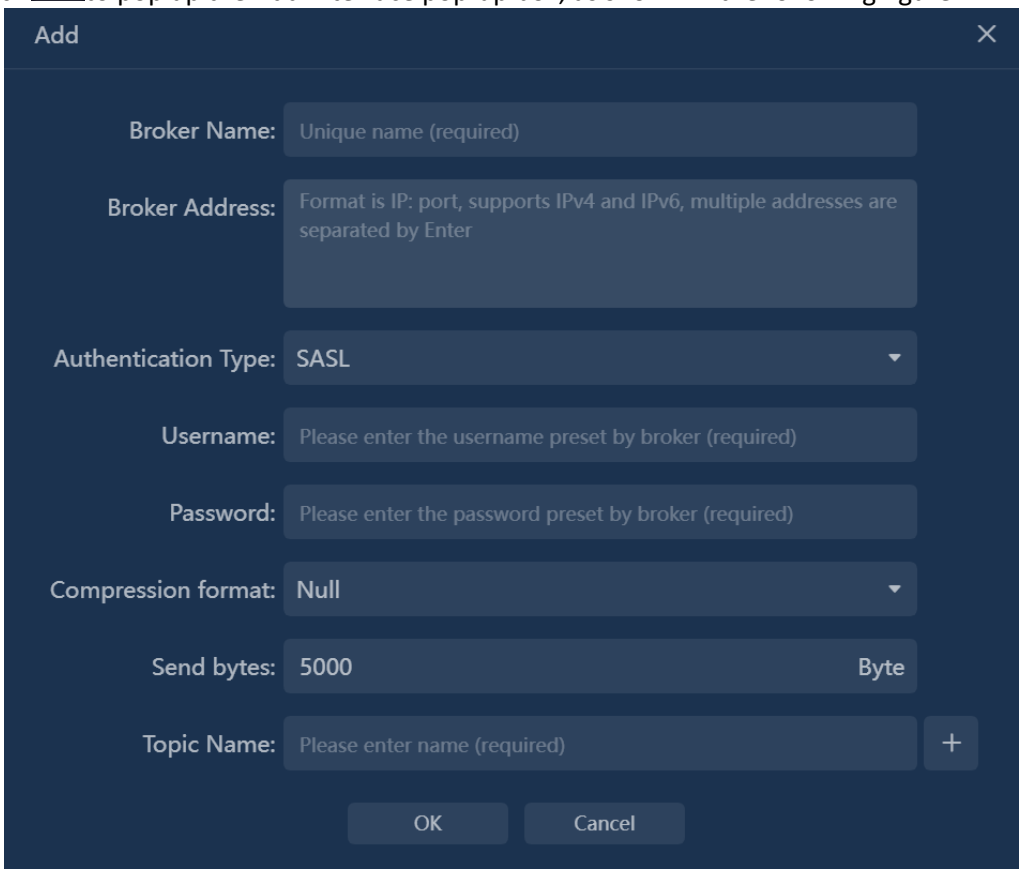
24.2.1. Kafka interface configuration

The Kafka interface configuration steps are as follows:

1.In the menu select "Configure > Third-party interface configuration > Kafka interface", enter the Kafka interface configuration page, as shown in the following figure.



2.Click + to pop up the Add Interface pop-up box, as shown in the following figure.



The description of each configuration field in the pop-up box is shown in the following table.

Field Name	Description
Broker name	Required. It is used to set the Broker name. Repeated Broker names are not allowed.
Broker address	Required, used to set the Broker's address. The format is IP: port, supports IPv4 and IPv6, and multiple addresses are separated by carriage return and line feed.
Verification method	Required, used to configure the authentication method of Kafka, you can choose S ASL , no authentication, kerberos
Username	When S ASL or Kerberos authentication is selected, configure the authentication account of Kafka.
Password	When S ASL authentication is selected, configure the authentication password of Kafka.
Service Name	When Kerberos authentication is selected, configure the authentication service address of Kafka.
K rb5 file	When Kerberos authentication is selected, configure the authentication file for Kafka.
Keytab file	When Kerberos authentication is selected, configure the authentication file for Kafka.
Compression format	Configure the compression format used for push data, you can choose Lz4, snappy, gzip
Send bytes	Used to limit the size of the amount of data sent, in bytes

Field Name	Description
Topic name	Required. It is used to set the name of the interface topic. Multiple topic names can be created at the same time.

Note

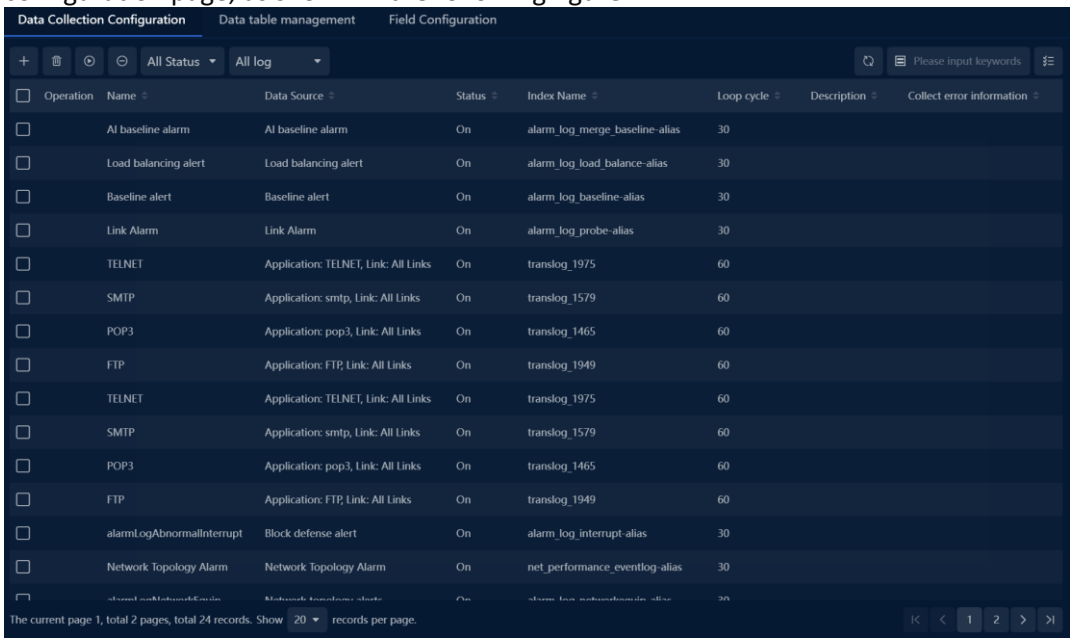
Kafka version should be at least a new version after 1.0.0 to avoid problems caused by version negotiation errors.

Click the "OK" button to complete the configuration of the Kafka interface.

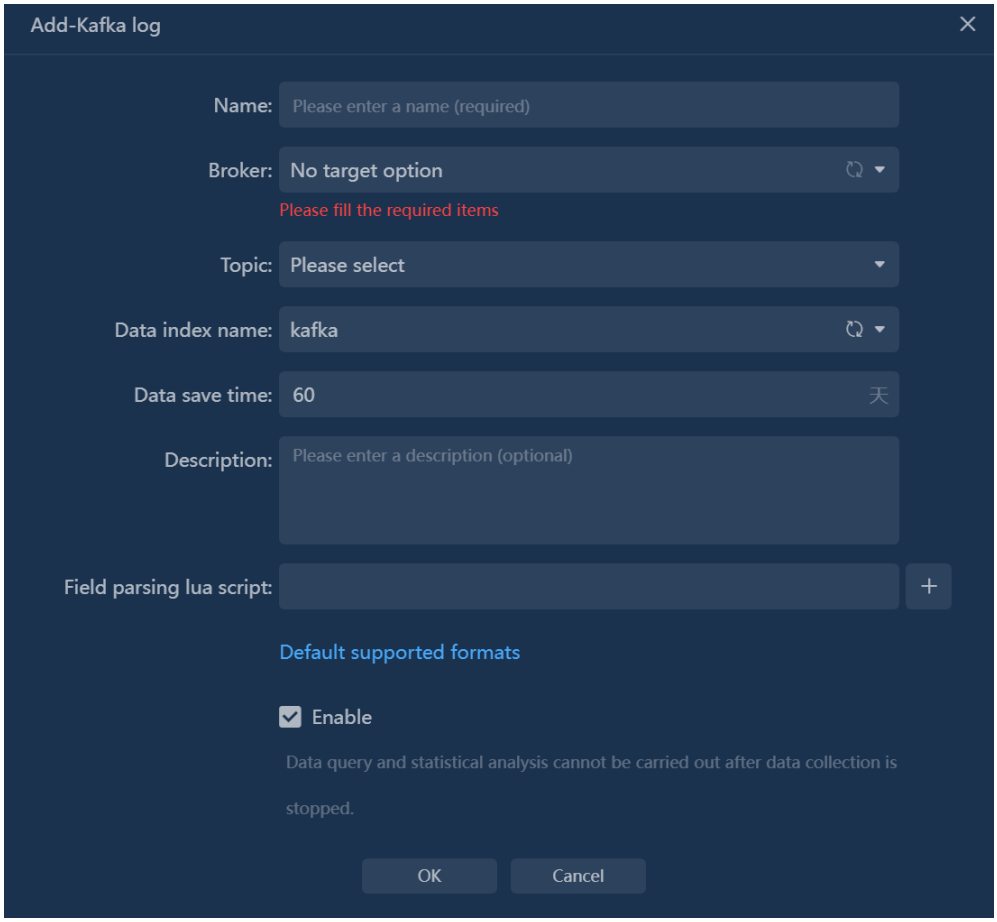
24.2.2. Acquisition configuration

The acquisition configuration steps are as follows:

1. > Data Collection Configuration" from the menu to enter the data collection configuration page, as shown in the following figure.



2. Click +, select Kafka log, and a pop-up collection configuration dialog box will pop up, as shown in the following figure.



The description of each configuration field in the pop-up box is shown in the following table.

Note

Field Name	Description
Name	Required. Used to set the collection task name, and it must be unique.
Broker	Required. Single selection. You can choose a Broker that has been configured in the Kafka interface.
Topic	Required. Multiple selection. You can choose aTopic that has been configured in the Kafka interface.
Data index name	Required, the index name used to retrieve configuration data from the database.
Data save time	Required, default 60 days, the duration for which the retrieved data is stored in the database.
Description	Optional, provides detailed information about this task.
Field parsing lua script	Optional, upload the corresponding parsing script for special formatting, fields, and other specific processing requirements.

The data format that can be automatically parsed supports a layer of JSON , for example:

- JSON object format: {"name":"test","id":"abcdefg","age":18}
- JSON array format: [{"name":"test","id":"abcdefg","age":18}]

Other complex types such as multi-level nesting need to use lua script for auxiliary parsing.

24.2.3. Data usage

After the collected data is configured with data tables and fields, it can be queried and used in "Log Retrieval" and "Pivot Component".

25. Segment Statistical Report

25.1. Function introduction

25.1.1. Functional description

The indicators supported by the segment statistical report include bandwidth utilization, peak traffic, peak TOP objects (sessions, applications, IP), congestion duration, interruption duration, etc., and provide expansion and speed limit suggestions based on decision algorithms.

25.2. Functional value

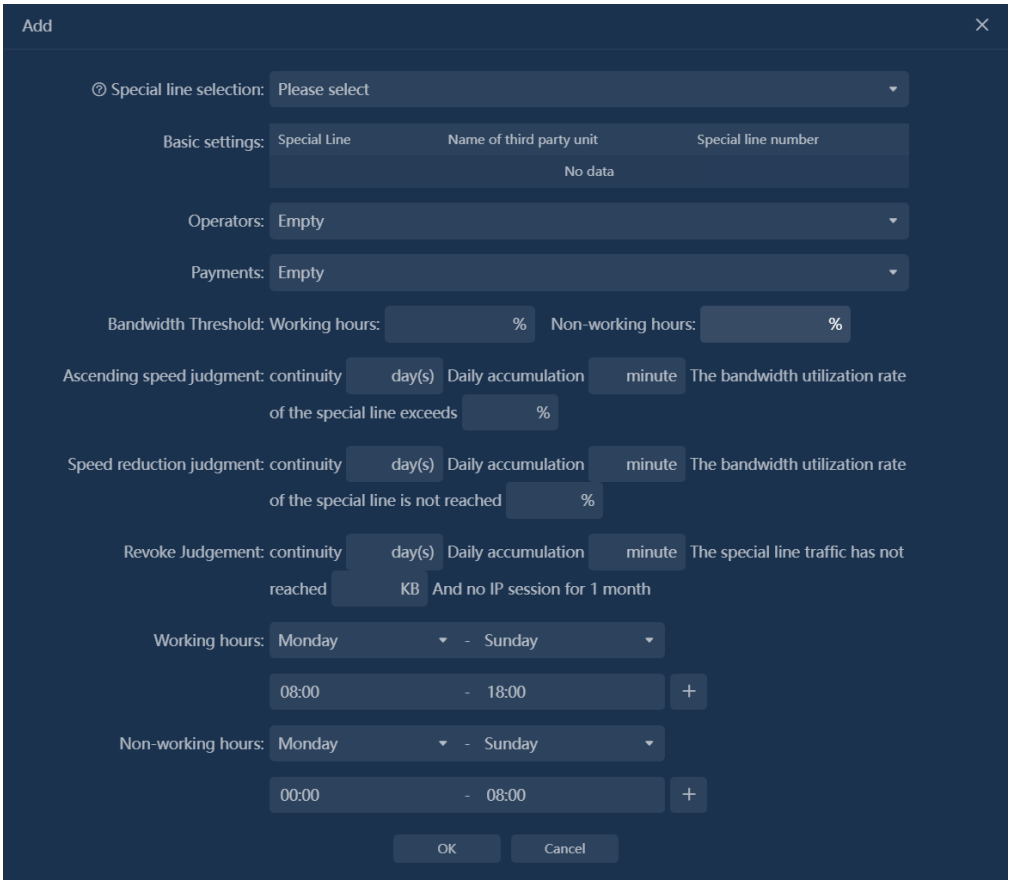
- Segment data statistics can be performed separately according to working and non-working periods, as well as inbound and outbound directions.
- The segment link types support regular links, aggregated links, and subnet sublinks.
- The segment statistical report types support daily, weekly, and monthly reports. In addition to weekly and monthly summary statistics, weekly and monthly reports can also support daily data statistics display.
- Reports can be regularly sent to designated recipients via email.

Operation Guide

Configure segment properties

Before configuring segment reports, you need to configure the properties of the segment. Follow the steps below:

1. Select "Reports > Segment Statistics Report" from the menu to enter the segment statistics report page.
2. Select the "Segment Configuration" tab.
3. Click + to open the Add Segment Configuration dialog box, as shown in the following figure.



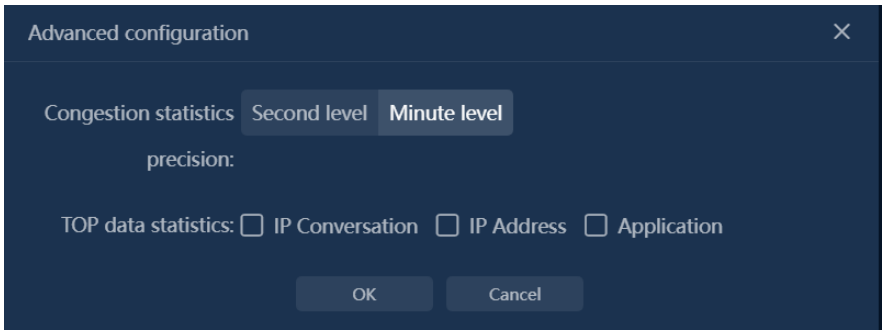
The configuration fields in the pop-up box are explained in the table below.

Field Name	Description
Segment Selection	Used to set the links that need to be defined as segment for report statistics in the system. The link types supported include regular links, aggregated links, subnet sublinks, M AC sublinks, and virtual interface sublinks.
Basic Settings	Configure the dedicated name and internal use number of the segment link
Congestion Threshold	Configure the inbound and outbound network utilization percentages for judging segment congestion during working and non-working periods.
Up speed judgment	Set the conditions for determining whether the segment bandwidth needs to be increased
Down speed judgment	Set the conditions for determining whether the segment bandwidth needs to be decreased
Cancellation judgment	Set the conditions for determining whether the segment needs to be canceled
Interrupt judgment	Set the conditions for determining whether the segment has a disconnection
Time period configuration	Set the time range for data statistics during working and non-working hours

4. Click the 'OK' button to complete the configuration of the segment properties.

Advanced configuration

After completing the configuration of the segment properties, click Advanced configuration to perform advanced configuration



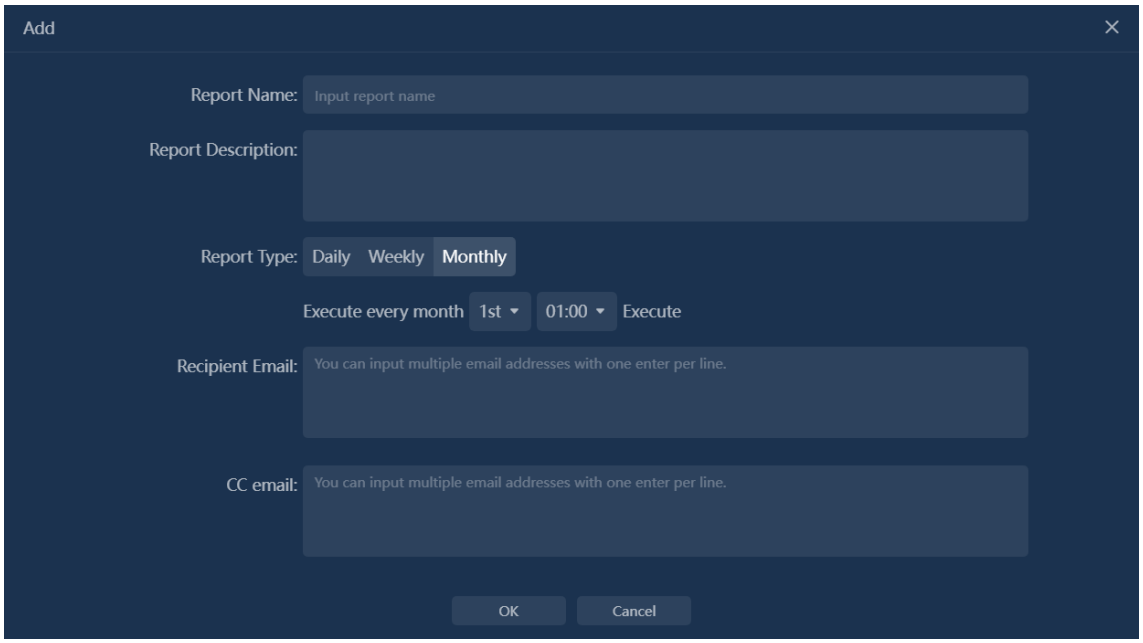
1. Congestion statistics accuracy: Configure whether the accuracy of congestion duration is in minutes or seconds
2. TOP data statistics: Configure whether the corresponding segment statistics include IP sessions, IP addresses, and applications' TOP5 data.

Note

When the accuracy is in seconds and the TOP statistics are enabled, the query pressure for backtracking is high. It is recommended to only enable the above configuration for a small number of key segment.

Add Report

1. Select the 'Segment statment' tab to add a report.
2. Click + to open the 'Add Report' dialog box, as shown in the following figure.



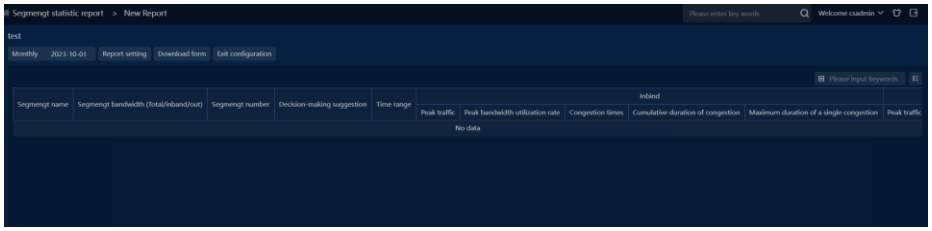
The configuration fields in the pop-up box are explained in the table below.

Field Name	Description
Report name	Configure the name of the report
Report Description	Configure the description of the report
Report Type	Select whether the report is a daily, weekly, or monthly report, and configure the report generation time
Recipient Email	Configure the receiving email after the report is sent
CC Email	Configure the CC email after the report is sent

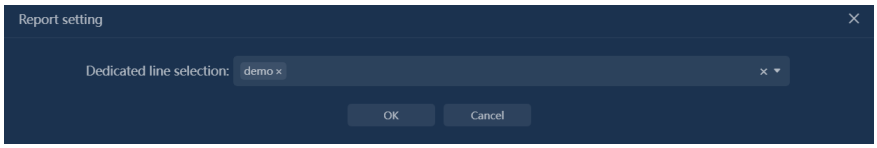
3. Click the 'OK' button to complete the configuration of adding a report.

Configure Report

After configuring the information for adding a new report, click the 'OK' button to enter the report configuration page. As shown in the following figure.

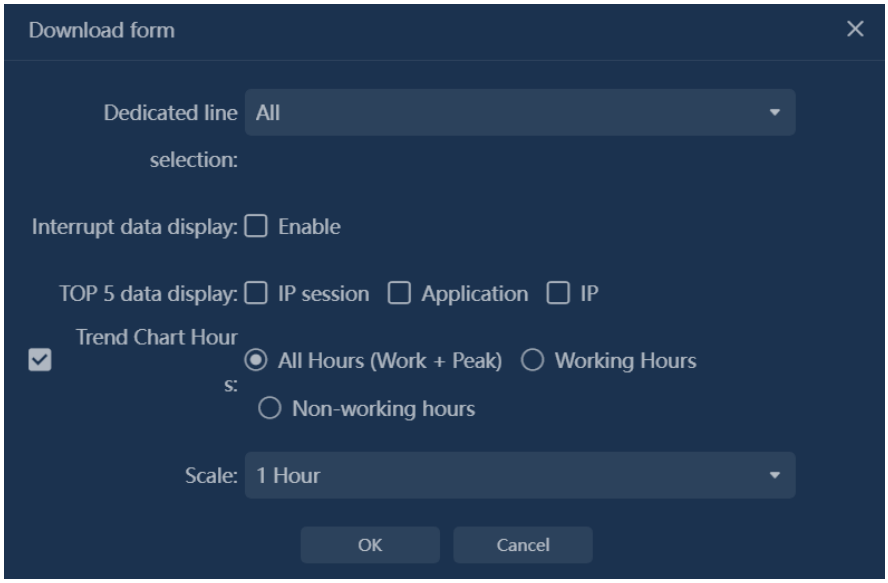


1. Click 'Report Setting' to enter the 'Add segment' pop-up window.



Segment can be selected with pre-configured judgment conditions.

2. Click on 'Download form' to enter the instant download report pop up.



(1) Select the specific segment object to be downloaded and viewed for this session.
(2) Interrupted data display: whether to display the interruption duration of the segment.
(3) TOP5 data display: configure whether to display the collected TOP5data.

(4) Trend chart period is used to select the period of the segment bit rate trend chart after downloading the report.

3. Click on the blue font to open the peak bit rate trend chart within the report period.

Note

1. Report data is counted from the configuration moment and does not perform historical data retrieval.
2. Reports cannot view data for the current day, only historical data from the previous cycle and earlier can be selected for viewing.
3. When configuring segment, only select links that have already been configured with bandwidth.