

# ***UPM***

Unified Performance Management Solution

User Guide

Copyright © 2022 Colasoft. All rights reserved. Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form, or by any means, electronic or mechanical, including photocopying, for any purpose, without the express written permission of Colasoft.

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](mailto:sales@colasoft.com)

### **Technical Support**

[support@colasoft.com](mailto:support@colasoft.com)

### **Website**

<http://www.colasoft.com/>

# Contents

Contents .....	ii
1. Preface .....	1
2. Introduction .....	2
2.1. Components .....	2
2.2. Deployment .....	2
2.3. System Requirement .....	2
2.4. Listening Port .....	3
2.5. Technical Support .....	3
2.6. Monitor Port .....	4
2.7. Default Account .....	4
3. Basic Configuration .....	5
3.1. Connect UPM to nChronos .....	5
3.1.1. nChronos Configuration .....	5
3.1.2. Probe Configuration .....	5
3.2. Business Configuration .....	5
3.2.1. Application Configuration .....	6
3.2.2. Business Configuration .....	6
3.3. Transaction Configuration .....	6
3.3.1. Data Dictionary Configuration .....	6
3.3.2. Business Transaction Capture Configuration .....	7
3.3.3. Business Field Configuration .....	7
3.3.4. Business Transaction Metric Configuration .....	7
3.4. Home page configure .....	8
3.4.1. Features .....	8
3.4.2. Operation Guide .....	9
3.4.3. common problem .....	14
4. Other Configuration .....	15
4.1. Network Segment Configuration .....	15
4.2. Issue Strategy Configuration .....	15
4.3. Alarm Configuration .....	15
4.3.1. Abnormal Access Alarm Configuration .....	15
4.3.2. Abnormal Traffic Alarm Configuration .....	16
4.3.3. Email Alarm Configuration .....	17
4.3.4. Domain Alarm Configuration .....	18

4.3.5.	Signature Alarm .....	18
4.3.6.	Terminal Alarm Configuration .....	19
4.3.7.	Predefined Alarm Configuration .....	20
4.3.8.	Business Alarm Configuration .....	20
4.3.9.	Link Traffic Alarm Configuration .....	20
4.3.10.	Network Performance Alarm Configuration .....	21
4.3.11.	Network Topology Alarm Configuration .....	22
4.3.12.	System Alarm .....	22
4.3.13.	Alarm and Information Send Configuration .....	22
4.3.14.	Email Send Configuration .....	23
4.3.15.	Syslog Send Configuration .....	23
4.3.16.	SMS Send Configuration .....	24
4.3.17.	SMTP Server Configuration .....	24
4.4.	VoIP Terminal Management Configuration .....	25
4.5.	Name Table Configuration .....	25
4.6.	Agent Configuration .....	25
4.7.	Network Device Configuration .....	25
4.7.1.	Basic Configuration .....	26
4.7.2.	Monitor configuration .....	27
4.7.3.	Interface configuration .....	28
4.8.	OID Query Configuration .....	28
4.8.1.	.....	29
4.9.	Superior UPM Configuration .....	29
4.10.	Map Configuration .....	30
4.11.	Unit Conversion Configuration .....	30
4.12.	Kafka interface and task .....	31
4.12.1.	Kafka interface setting .....	31
4.12.2.	Task Push Configuration .....	32
4.13.	System Parameters configuration .....	33
4.14.	Configure report sending tasks .....	34
<b>5.</b>	<b>Discover .....</b>	<b>35</b>
5.1.	Application Discovery .....	35
5.1.1.	Interface Introduction .....	36
5.1.2.	Data Collection .....	38
5.1.3.	Create Applications .....	40
5.1.4.	Create Business .....	40
5.1.5.	Snapshot Comparison .....	41

5.1.6.	Generate snapshot report .....	42
5.1.7.	Custom Metric Discover .....	43
5.1.8.	Other Common Operations .....	44
5.2.	Network Path Discovery .....	49
5.2.1.	Interface Introduction .....	49
5.2.2.	Other Common Operations .....	50
5.3.	Conversion Path Carding .....	53
<b>6.</b>	<b>Business .....</b>	<b>56</b>
6.1.	Timeline .....	56
6.1.1.	Timeline Components .....	56
6.1.2.	Time Slice Operation .....	56
6.2.	Business Status .....	56
6.3.	Business Custom Monitoring .....	57
6.4.	Business Global Performance Monitoring .....	57
6.5.	Business Performance Analysis .....	58
6.6.	Business Metrics Analysis .....	59
6.7.	Business Multiple Analysis .....	61
6.8.	Business Alarm Configuration .....	61
6.9.	Business Report .....	62
<b>7.</b>	<b>Transaction .....</b>	<b>63</b>
7.1.	Transaction Custom Monitoring .....	63
7.2.	Transaction Performance Analysis .....	63
7.3.	Transaction Custom Query .....	63
7.3.1.	Add a New Custom Query Rule .....	64
7.3.2.	Perform Query Rule .....	65
7.3.3.	Task Management .....	66
7.4.	Transaction Alarm .....	66
7.5.	Transaction Report .....	66
<b>8.</b>	<b>Network .....</b>	<b>68</b>
8.1.	Network Performance Monitoring .....	68
8.1.1.	Define Monitor View .....	68
8.1.2.	Monitoring View .....	68
8.2.	Network Performance Analysis .....	68
8.2.1.	Group .....	69
8.2.2.	Ratio Analysis .....	69
8.2.3.	Comparison Analysis .....	69

8.2.4.	Trend Prediction Analysis	69
8.3.	Network Path Analysis	69
8.4.	Network Performance Alarm	70
8.5.	Network Performance Report	70
8.6.	Network Topology Monitoring	72
8.7.	Network Topology Alarm	72
<b>9.</b>	<b>Device</b>	<b>73</b>
9.1.	Device Performance Analysis	73
9.2.	SNMP Custom Monitoring	73
9.3.	SNMP Report	73
<b>10.</b>	<b>Link</b>	<b>74</b>
10.1.	Link Custom Analysis	74
10.2.	VoIP Custom Analysis	74
10.3.	Link Traffic Analysis	74
10.3.1.	Group	74
10.3.2.	Ratio Analysis	75
10.3.3.	Comparison Analysis	75
10.3.4.	Trend Prediction Analysis	75
10.3.5.	Packets Decoding	76
10.4.	Application Object Analysis	76
10.4.1.	Customize Application Object	76
10.5.	Link Traffic Alarm	76
10.6.	Link Report	76
10.7.	VoIP Report	77
<b>11.</b>	<b>Abnormal Activity</b>	<b>78</b>
11.1.	Abnormal Activity Monitoring	78
11.2.	Abnormal Activity Alarm	78
<b>12.</b>	<b>Terminal Monitoring</b>	<b>80</b>
12.1.	Terminal management	80
12.2.	Terminal Monitoring	82
12.2.1.	Create Monitoring View	82
12.2.2.	Real-Time Monitoring	85
12.3.	Terminal Analysis	86
12.4.	Terminal Alarm	87
<b>13.</b>	<b>Backup Monitoring</b>	<b>89</b>

13.1. Terminal Management.....	89
13.1.1. Add a Terminal Group.....	89
13.1.2. Add Terminal.....	90
13.1.3. Import/Export .....	91
13.2. Terminal Monitoring .....	92
13.2.1. Create Monitor Views .....	92
13.2.2. Metric Description .....	97
<b>14. Search and Download .....</b>	<b>99</b>
14.1. Search Packets.....	99
14.2. Download Packets.....	99
14.3. In-depth Analysis.....	100
14.4. Discover.....	100
14.5. Multi-segment Analysis.....	101
14.6. Trend Analysis .....	101
<b>15. Packet Signature Query .....</b>	<b>103</b>
15.1. Add Query Task .....	103
15.2. Check Query Result .....	104
<b>16. Log Analysis .....</b>	<b>105</b>
16.1. Log Analysis Configuration .....	105
16.1.1. Log Collection Configuration.....	105
16.1.2. Log Analysis Scene Configuration .....	106
16.2. Log Retrieval.....	107
<b>17. System Management.....</b>	<b>108</b>
17.1. User Group Management .....	108
17.2. User Account .....	108
17.3. Security Policy .....	108
17.4. Audit Logs.....	109
17.5. Import/Export Configurations.....	109
17.5.1. Import Configurations.....	110
17.5.2. Export Configurations .....	110
17.6. System Information.....	111
17.6.1. Server Information.....	111
17.6.2. License Information .....	112
17.7. Replace Certificate .....	112
<b>18. Network Topology monitoring.....</b>	<b>113</b>

18.1. View settings .....	113
18.1.1. Configuring Monitoring Indicators.....	116
18.1.2. Rectangle Setting .....	117
18.1.3. Text setting.....	117
18.1.4. Image Setting .....	118
18.1.5. Device Icon .....	118
18.1.6. Connecting Cables for Icon .....	119
18.2. View Group.....	122
18.2.1. Add new group.....	122
18.2.2. Edit Group .....	123
18.2.3. Delete Group.....	123
18.3. Template .....	123
18.3.1. Adding the Current View as a Template .....	123
18.3.2. Exporting the Current View as a Template .....	124
18.3.3. Template Management .....	124
18.4. Monitor and Analysis Module .....	125
<b>19. Custom indicator monitoring .....</b>	<b>126</b>
19.1. Function introduction.....	126
19.1.1. Terminology .....	126
19.1.2. Function Usage Scenarios .....	126
19.1.3. Value of functions .....	126
19.2. Operations Guide .....	127
19.2.1. View management .....	127
19.2.2. Template Management .....	132
19.2.3. View operation.....	133
19.2.4. Style setting.....	135
19.2.5. FAQ.....	142
<b>20. Session Tracking.....</b>	<b>144</b>
20.1. Introduction.....	144
20.1.1. Function Description .....	144
20.1.2. Application Scenarios.....	144
20.1.3. Function Value .....	144
20.2. Operation Guide.....	144
<b>20.2.1. Device Icon</b> .....	<b>145</b>
20.2.2. Select Session.....	148
<b>21. SRv6 Session Path Combing .....</b>	<b>149</b>
21.1. Introduction.....	149



21.1.1.	Terminology .....	149
21.1.2.	Function Description .....	149
21.1.3.	Scenario .....	149
21.1.4.	Value .....	150
21.2.	Operation Guide .....	150
21.2.1.	Configuring Network Devices .....	150
21.2.2.	Select Session .....	151
21.2.3.	Trend .....	151
21.3.	FAQ .....	185
<b>22.</b>	<b>SNMP .....</b>	<b>153</b>
22.1.	Features .....	153
22.1.1.	Technical background .....	153
22.1.2.	Functional structure .....	153
22.2.	Device configuration .....	155
22.2.1.	Network device configuration .....	155
22.2.2.	Basic configuration .....	155
22.2.3.	Monitoring configuration .....	156
22.3.	OID query configuration .....	157
22.3.1.	Query Template Configuration .....	158
22.3.2.	Metric group configuration .....	158
22.3.3.	Common indicator configuration .....	158
22.3.4.	Calculated indicator configuration .....	160
22.4.	Analyze .....	162
22.4.1.	Equipment performance analysis .....	162
<b>23.</b>	<b>Alerts .....</b>	<b>164</b>
23.1.	Function Introduction .....	164
23.1.1.	Function Description .....	164
23.1.2.	Functional scenarios .....	164
23.1.3.	Functional value .....	164
23.2.	Alarm display .....	165
23.2.1.	Alarm filtering .....	165
23.2.2.	Alarm Statistics .....	165
23.2.3.	Alarm Log .....	166
<b>24.</b>	<b>Smart Baseline .....</b>	<b>167</b>
24.1.	Features .....	167
24.1.1.	The term .....	167
24.1.2.	Functional background .....	167

24.1.3.	Functional value .....	167
24.1.4.	Function description .....	167
24.2.	Operation guide .....	167
24.2.1.	Connect with CSAIS .....	167
24.2.2.	Add monitoring object .....	168
24.2.3.	Monitor display and analysis .....	170
24.3.	Common problem .....	170
<b>25.</b>	<b>Kafka log collection .....</b>	<b>171</b>
25.1.	Features .....	171
25.1.1.	Function description .....	171
25.1.2.	Functional scene .....	171
25.1.3.	Function value .....	171
25.2.	Operation guide .....	171
25.2.1.	Kafka interface configuration .....	171
25.2.2.	Acquisition configuration .....	173
25.2.3.	Data usage .....	175

# 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

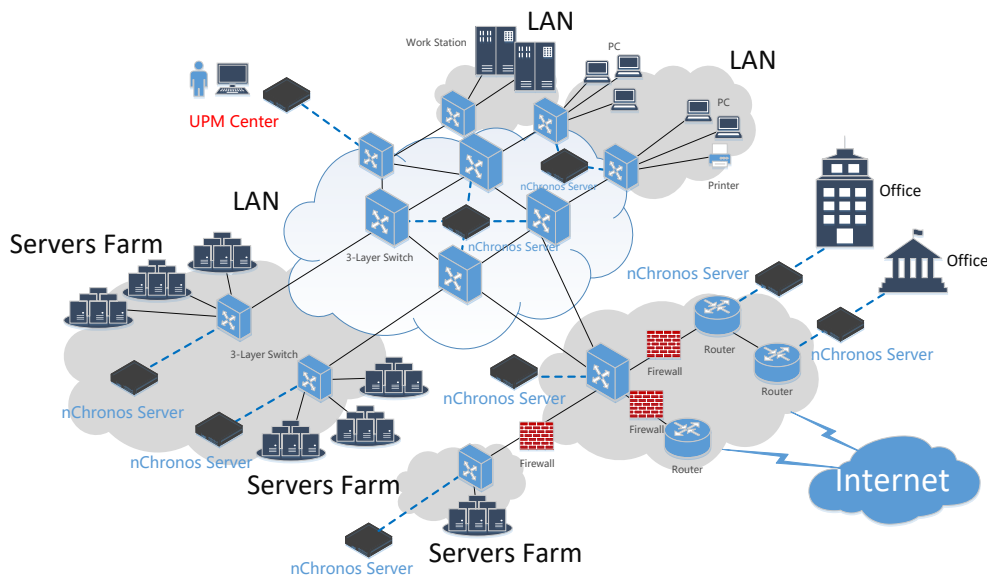
Colasoft UPM consists of nChronos Server and UPM Analysis Center (hereinafter referred to as “UPM Center”).

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 Minimum: 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](mailto: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

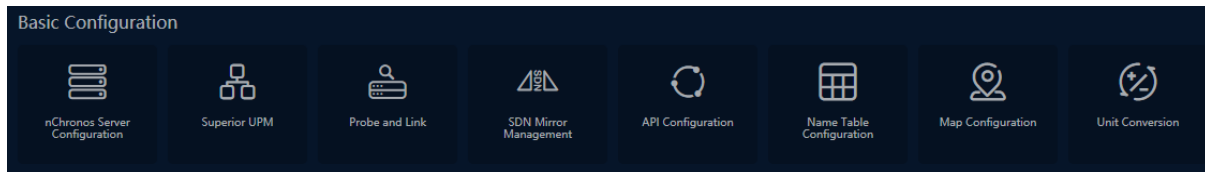
The default accounts provided by UPM are shown in the following table:

Number	User Name	Password	Explanation
1	csadmin	!CSUPM23	UPM web default login account
2	root	!ColosoftL23	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

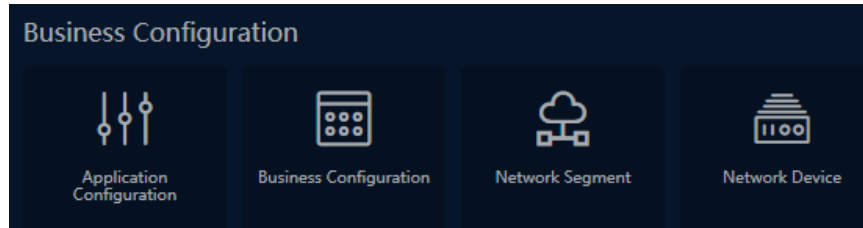
All analysis results on UPM are based on the data collected by probes. One probe indicates one data collection site. UPM probe corresponds to the network link on nChronos server.

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 20 records in the last 15 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

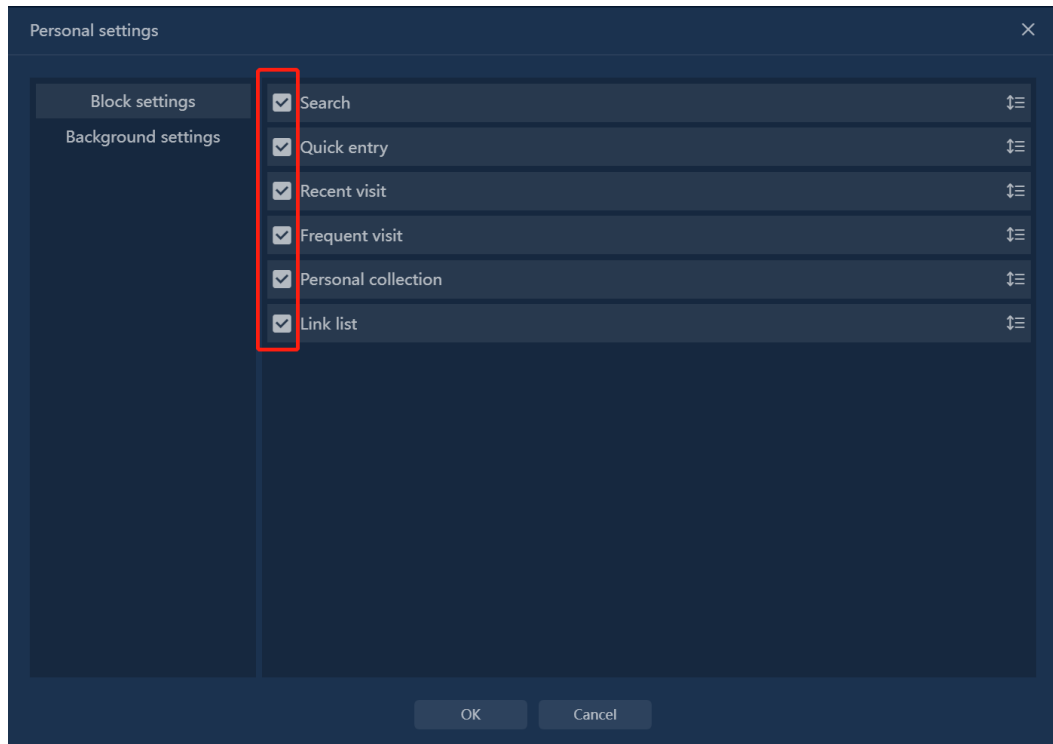
### 3.4.2.1 Show and hide blocks

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.

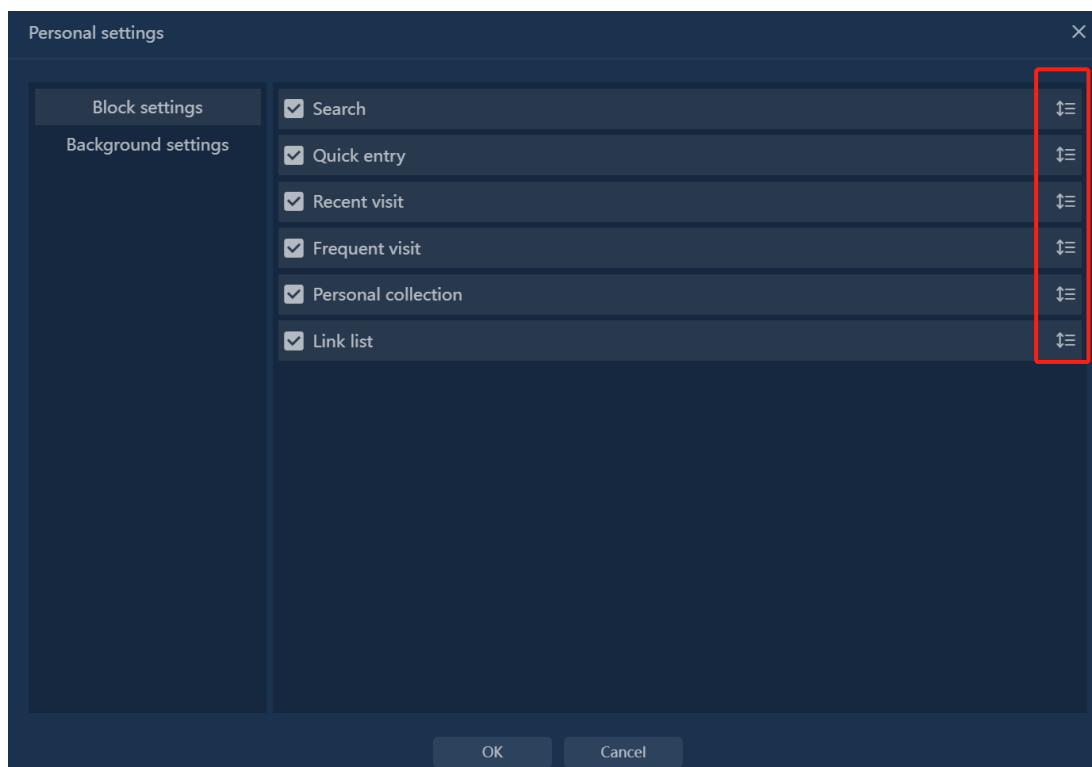


**Method 2:** In the lower right corner of the home page, there is a home page personality setting button " **Personal settings** ", click the button, and uncheck the checkbox to hide the block in the pop-up window.



### 3.4.2.2 Block display sorting

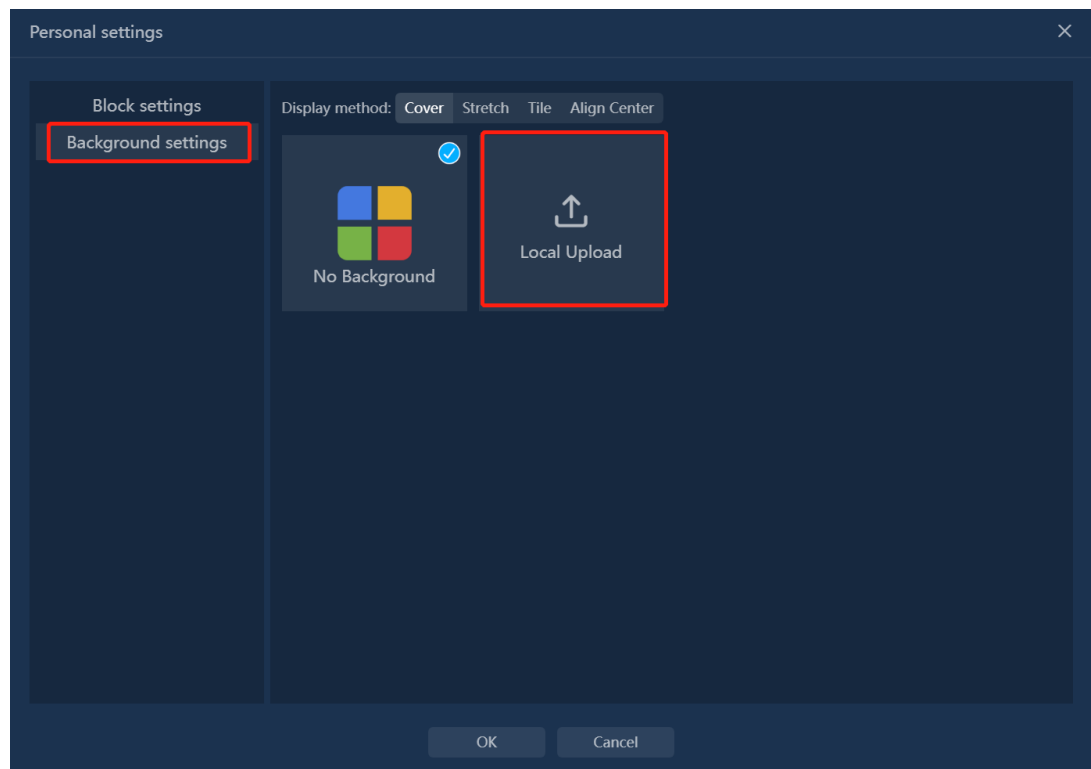
In the lower right corner of the home page, there is a home page personality setting button " **Personal settings** ", click the button and drag the mouse to adjust the display order of the blocks on the home page in the pop-up window.



### 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.

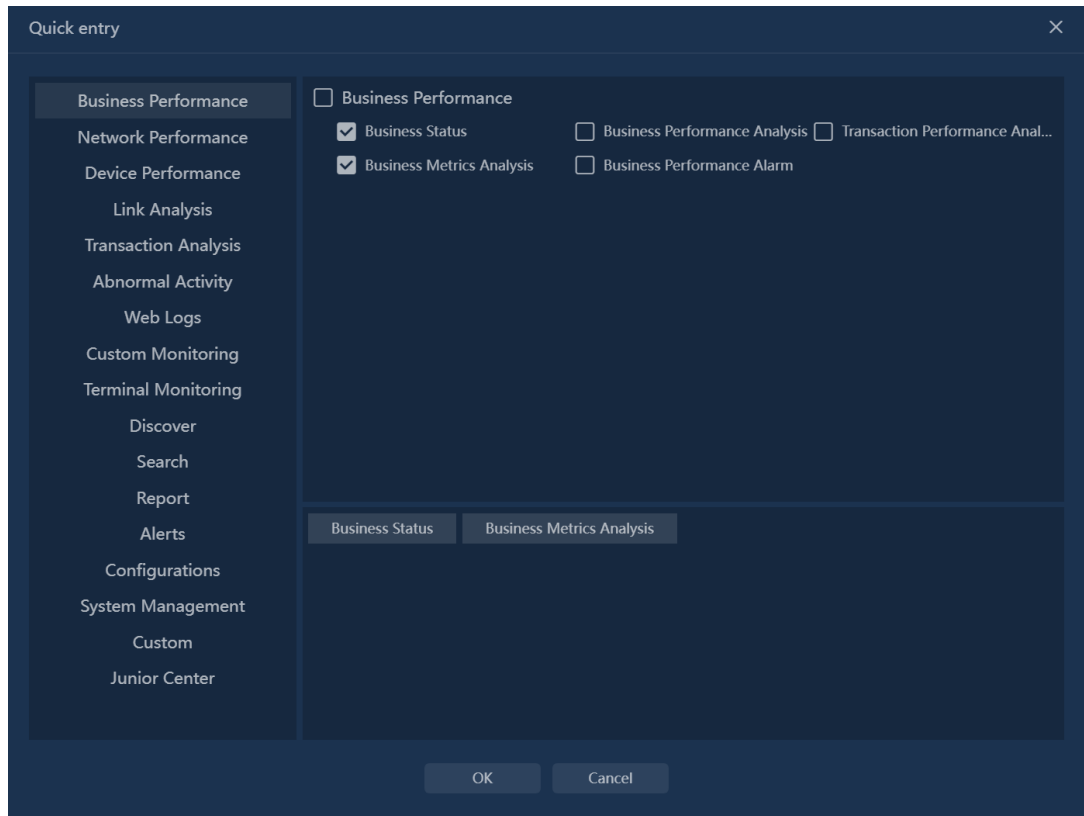


### 3.4.2.4 Edit Quick Entry

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.

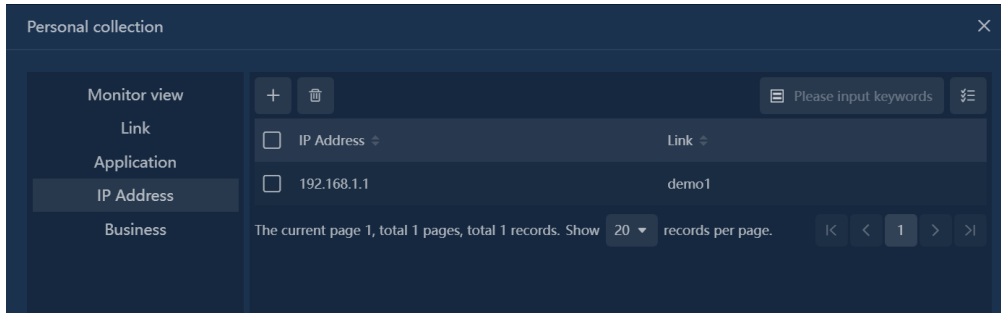
Supports collection of all types of links, aggregation, common, and sub-links.

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.

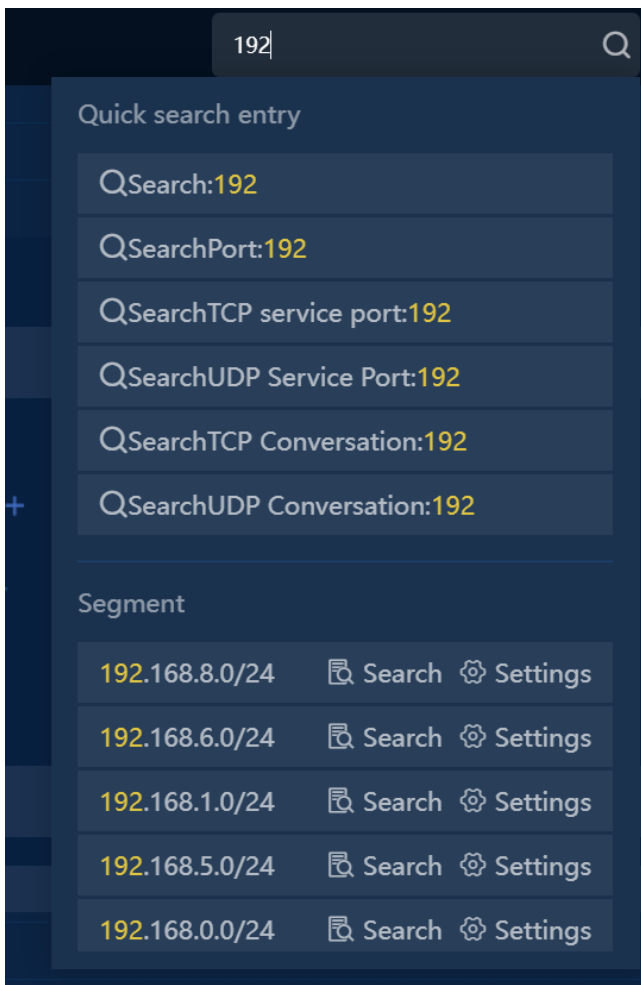




### 3.4.2.6 Associative search

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.



Configuration ID	Configuration Name	The Current Configuration	Range
homepageDataDeadline	Time for the retention of search records and recent access records on the homepage (unit: days)	15	1 - 60
indexSummaryLimit	Allowed Maximum Number of Home shortcut	6	1 - 20

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.

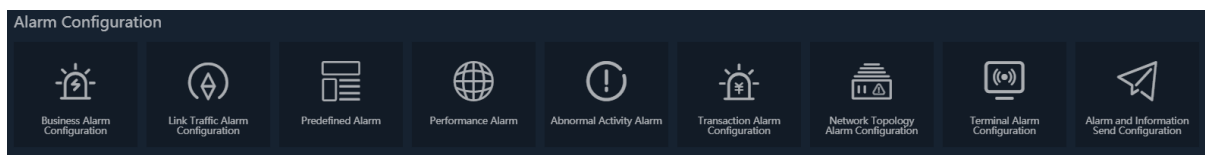
### 4.2. Issue Strategy Configuration

- 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.

The screenshot shows the 'Add Abnormal Access Alarm' dialog box with the 'Basic Configuration' tab selected. The fields are as follows:

- Alarm Name: Name
- Alarm Description: Description (optional)
- Level: Severe
- Link: test
- Creator: Creator
- Alarm Category: 333
- Alarm Type: Abnormal IP Access

Buttons: Next, Cancel

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

The screenshot shows the 'Add Rule' dialog box with the following configuration:

- Rule Group: No Option
- Src. Address: IP Address =
- Dest. Address: IP Address =
- Dest. Port: Port
- Application: System A... alpemix
- Protocol: System Pr... 0\_HOP
- Description: Describe the access relationship of rules (optional)
- Access Policy:  Allow  Reject
- Rule Priority:  Top  Bottom

Buttons: OK, Cancel

Rules have priority, and alarms are detected according to the priority of rules. An alarm is triggered when a rule is hit and the rule access policy is rejected.

Rules can be grouped by rules for merge management and priority sorting.

### 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.

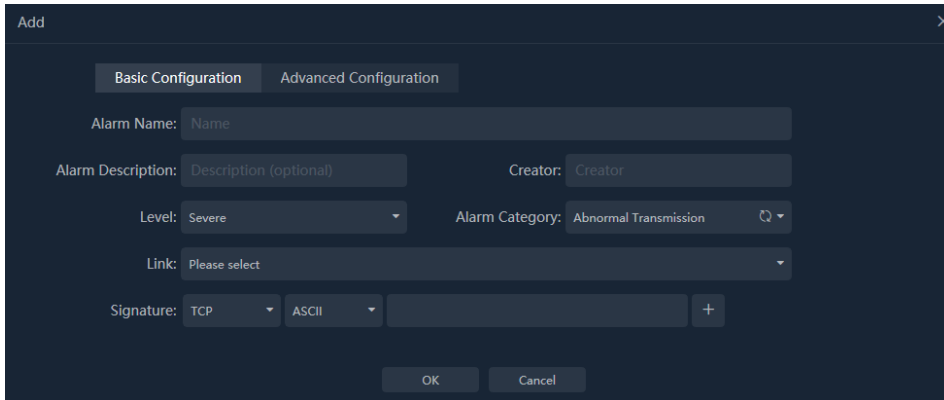
Click the menu Configuration-> Alarm Configuration -> Abnormal Activity Alarm to open the alarm configuration page. Enter the alarm basic information.

- 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.

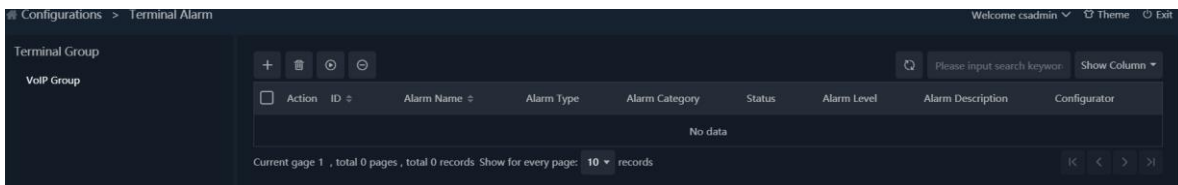


- Signature can be encoded in ASCII and hexadecimal.
- Multiple signature can be added to make the matching more accurate.


### 4.3.6. Terminal Alarm Configuration

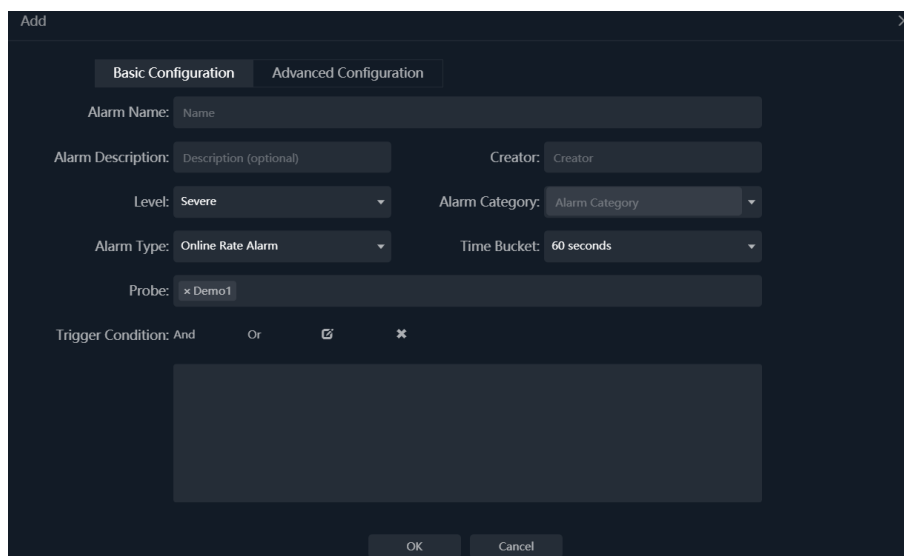
Users can go to the Terminal Alarm Configuration page via Configuration> Alarm Configuration -> Terminal Alarm Configuration.

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.

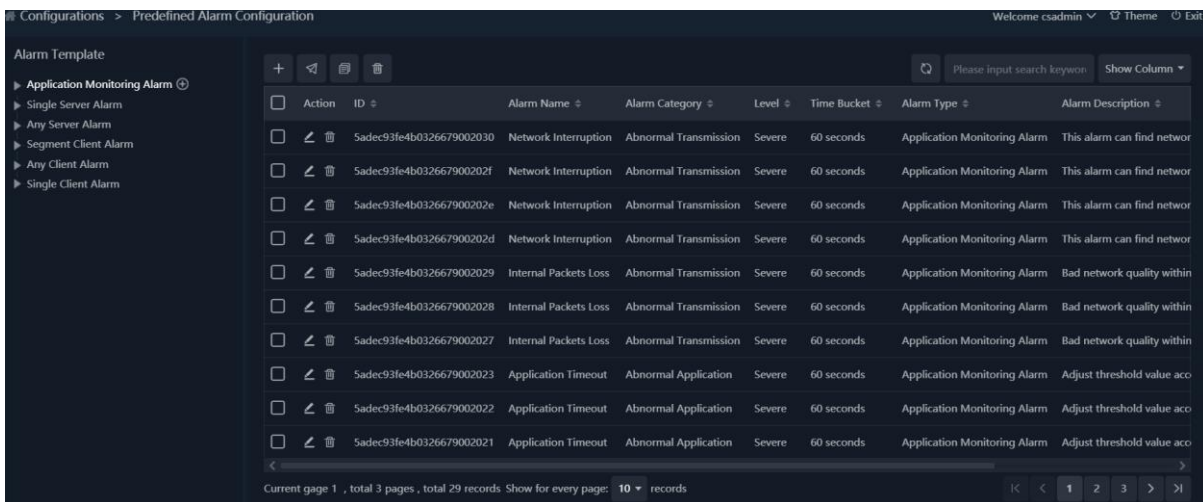
To add a terminal alarm ,users can click the button “” to enter the dialog box, as shown below:



- 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.

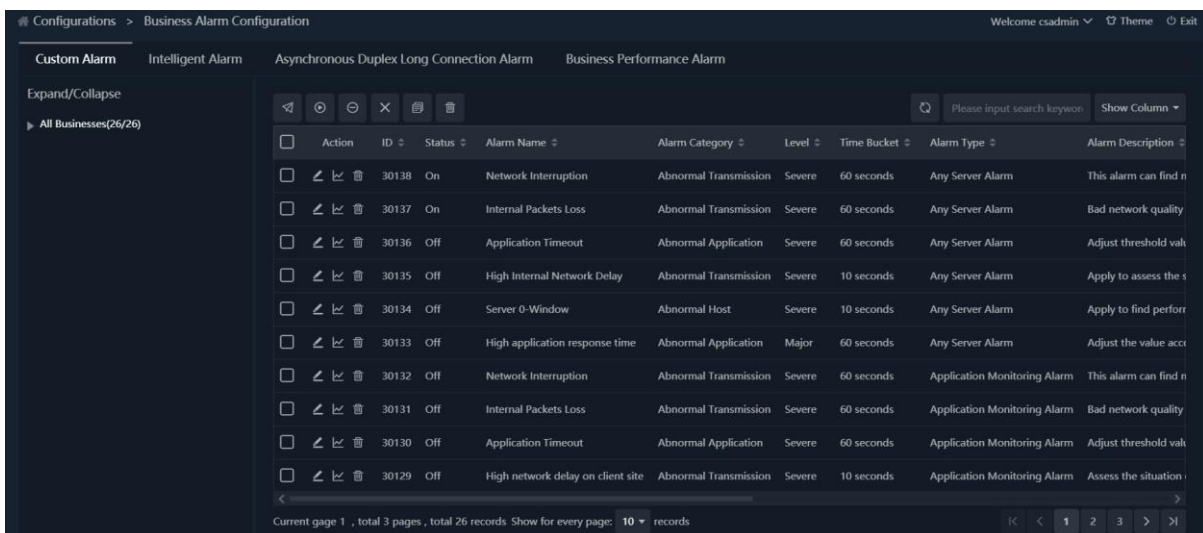
### 4.3.7. Predefined Alarm Configuration

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

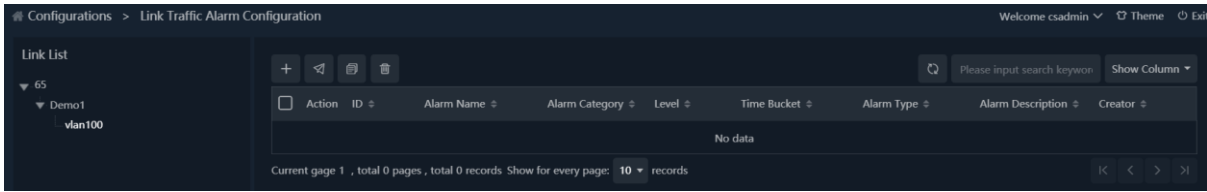
Click the menu Configurations -> Alarm Configuration -> Business Alarm Configuration to open the Business Alarm Configuration page, as the screenshot below:




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

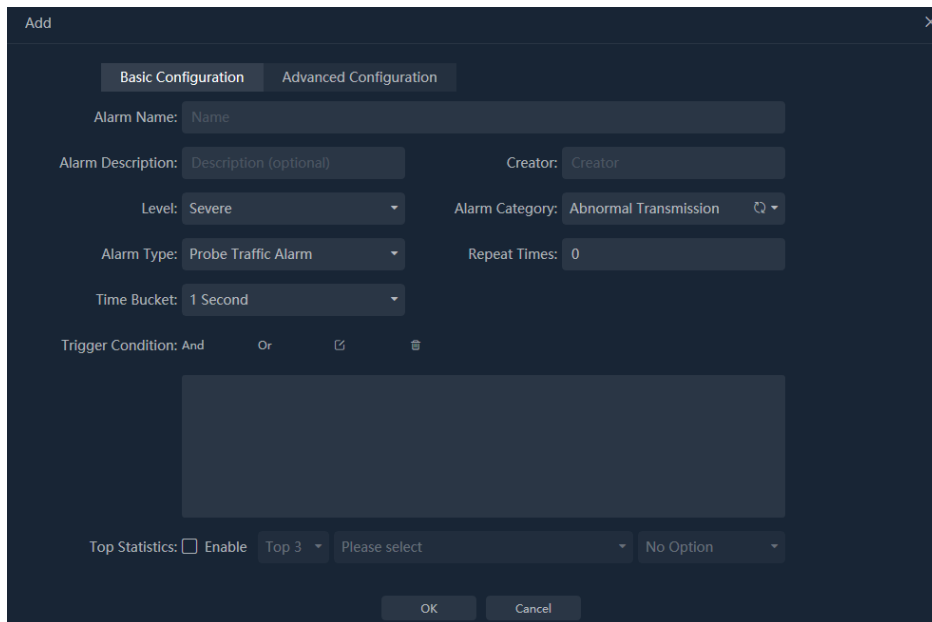
Click the menu Configurations -> Alarm Configuration -> Link Traffic Alarm Configuration to open the Link Traffic Alarm Configuration page, as the screenshot below:



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.

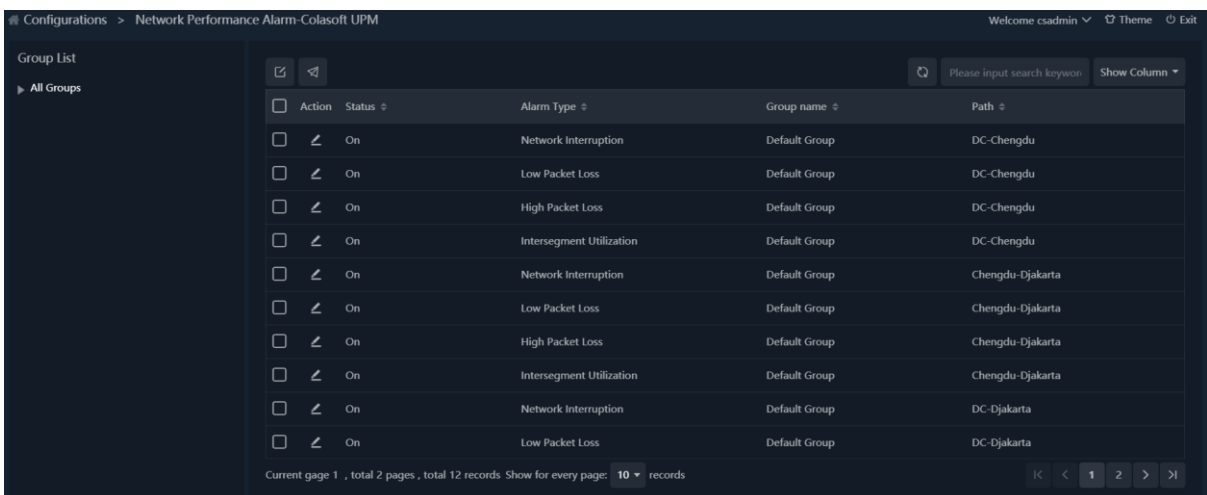
If the selected node is an nChronos server, then the added alarm will be forwarded to all links on that nChronos server; if the selected node is a link, then the added alarm will be only forwarded to that link.

The Add Alarm box shows as the screenshot below:



### 4.3.10. Network Performance Alarm Configuration

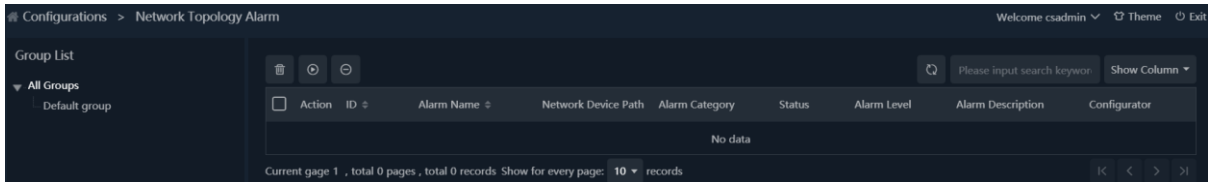
Click the menu Configuration -> Alarm Configuration -> Network Performance Alarm Configuration to open the Network Performance Alarm Configuration page, as the screenshot below:



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:

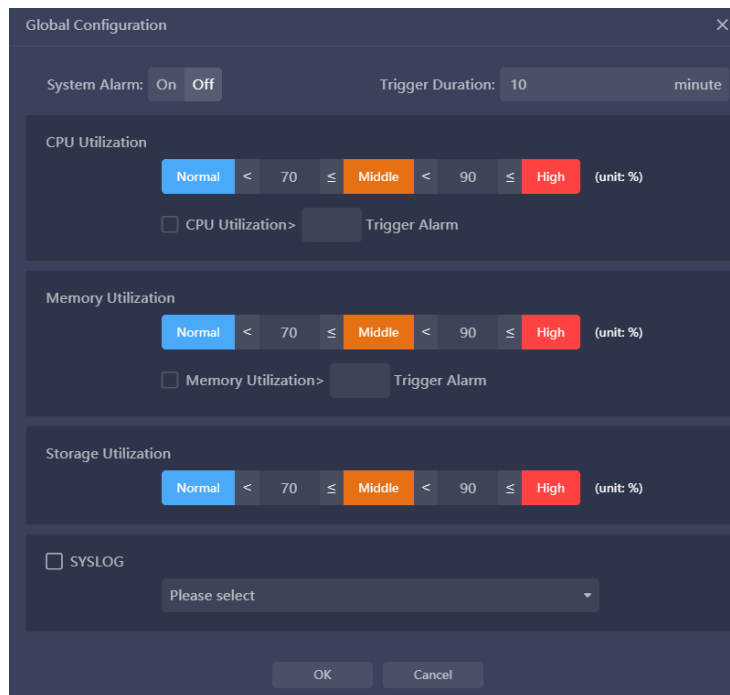


Network Topology Alarm Configuration is an alarm configuration for custom metric between network devices.

### 4.3.12. System Alarm

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

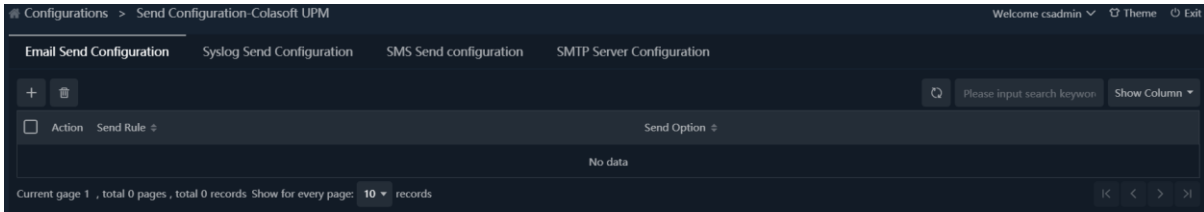
Click Configuration -> nChronos Server Configuration -> nChronos Server List to enter the front-end list page. Click to open the system alarm configuration window, as shown in the following figure:



### 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:

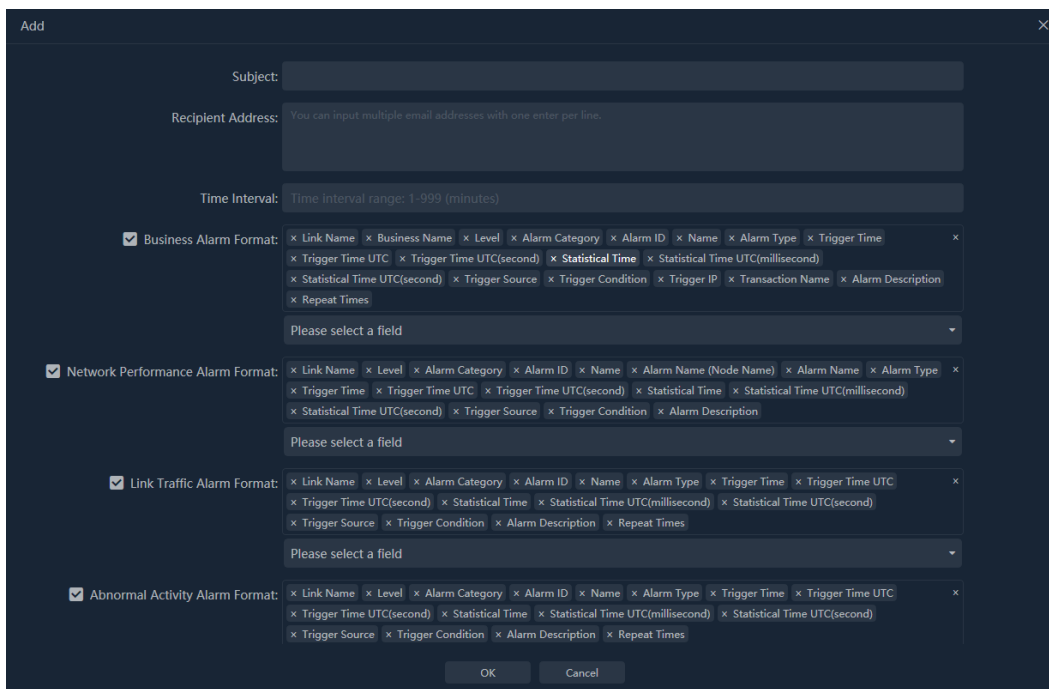




### 4.3.14. Email Send Configuration

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:

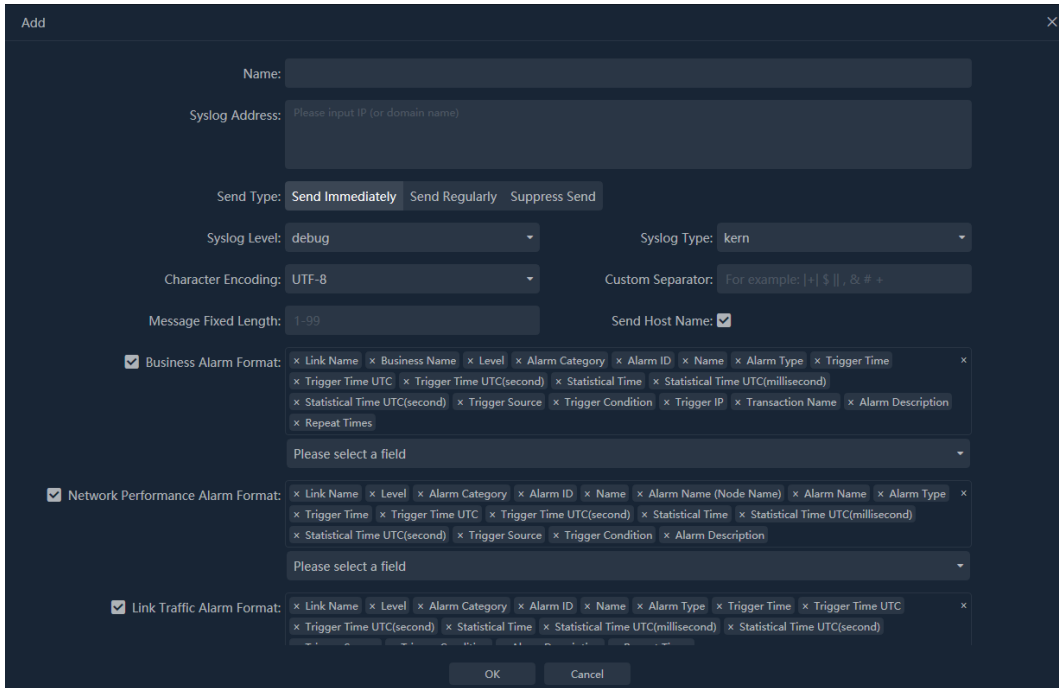


### 4.3.15. Syslog Send Configuration

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.

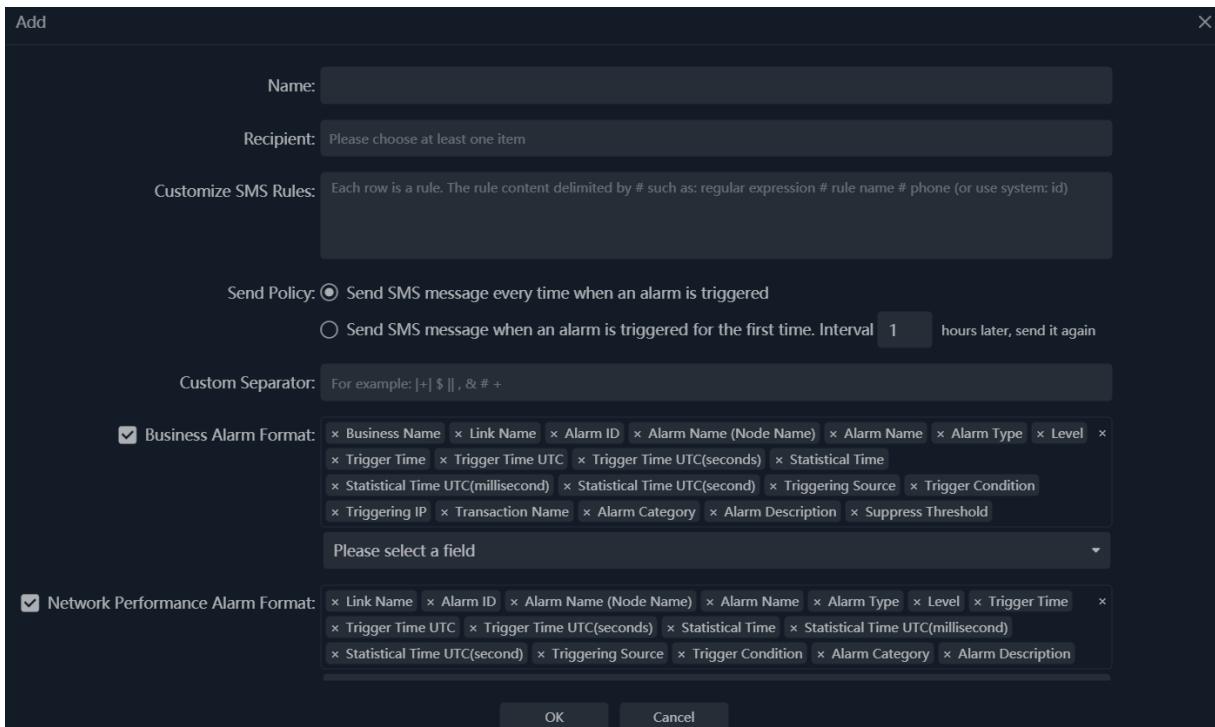
When setting syslog format, it is required to configure send format based on the alarm type (business alarm, network alarm, probe alarm) that the alarm category belongs to. If users don't configure send format for an alarm type, alarm logs of that alarm type will not be sent via syslog.

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.

The screenshot shows a configuration form with the following sections and fields:

- User Information:**
  - Name: [Text input field]
  - Email Address: [Text input field]
- Server Information:**
  - Mail Server: [Text input field]
  - Encryption: [Dropdown menu, currently set to 'No']
  - Port: [Text input field, currently set to '25']
- Logon Information:**
  - Username: [Text input field, placeholder: 'Enter username here']
  - Password: [Text input field, placeholder: 'Enter password here']

At the bottom, there are two buttons: 'Save' and 'Test'. Below the buttons is a note: 'Please first save the settings and then test.'

## 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.

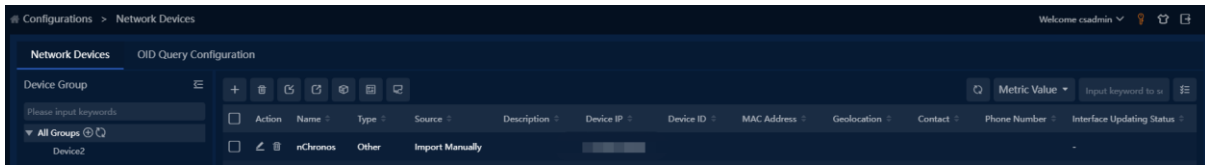
## 4.6. Agent Configuration

Please refer to the document **How to Configure Agent (linux)**.

## 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 from <a href="#">3.1.1 nChronos configuration</a> <a href="#">3.1.2 probe configuration</a>
	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.

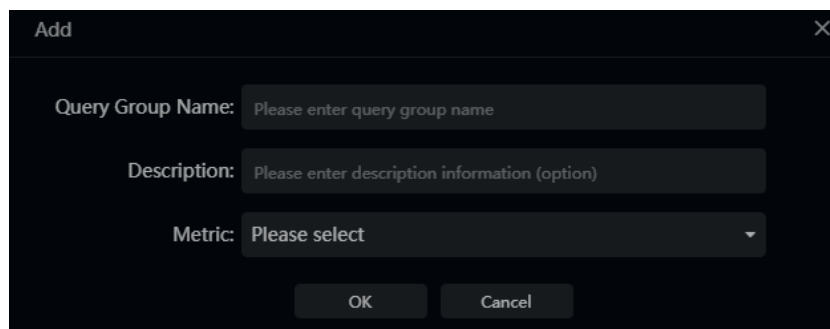
### 4.7.3. Interface configuration

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.

## 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:

**Add** [Close]

Metric Name:

Description:

OID:  +

Ask Type: GET ▾

Type: Text ▾

Unit: None ▾ No options found. ▾

Accuracy: 2

Trend Analysis:  Enable

OK Cancel

### 4.8.1.

## 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:

Configurations > Superior UPM

Frontend Name:

Center Address:

Center Port:

User Name:

Password:

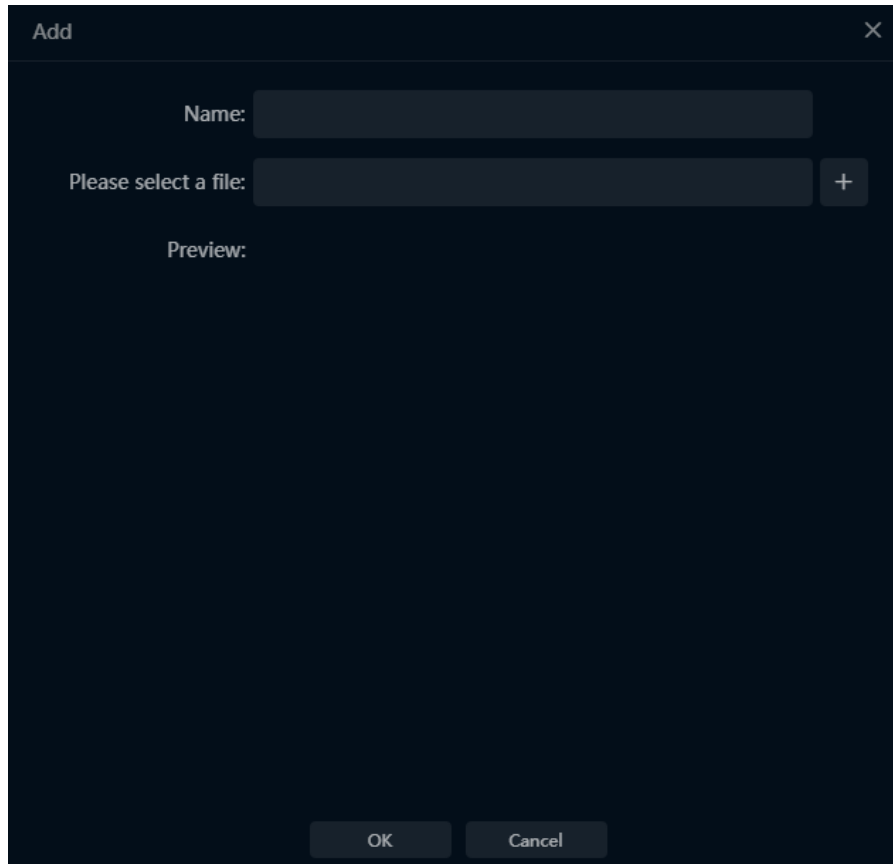
SSL:

Disconnected from UPM Center

Connect

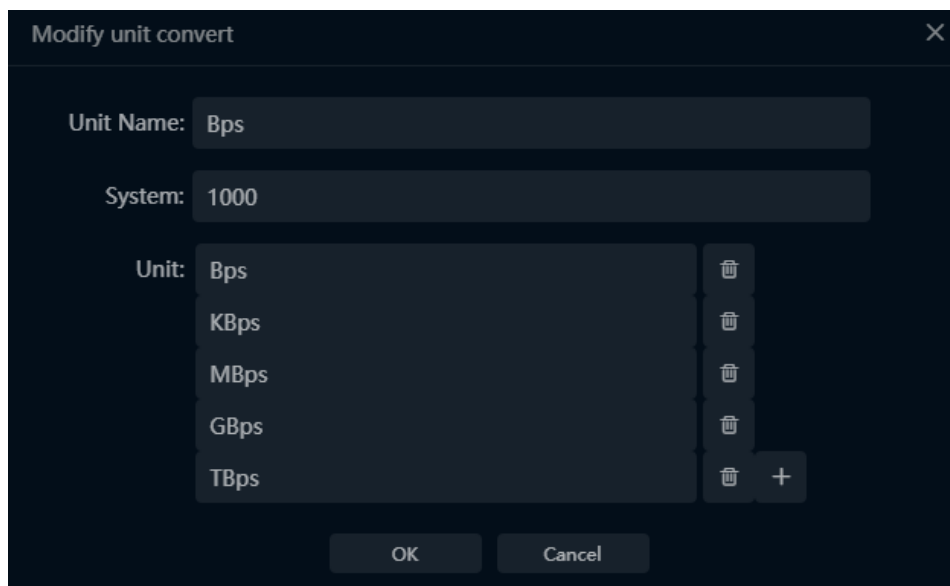
## 4.10. Map Configuration

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.

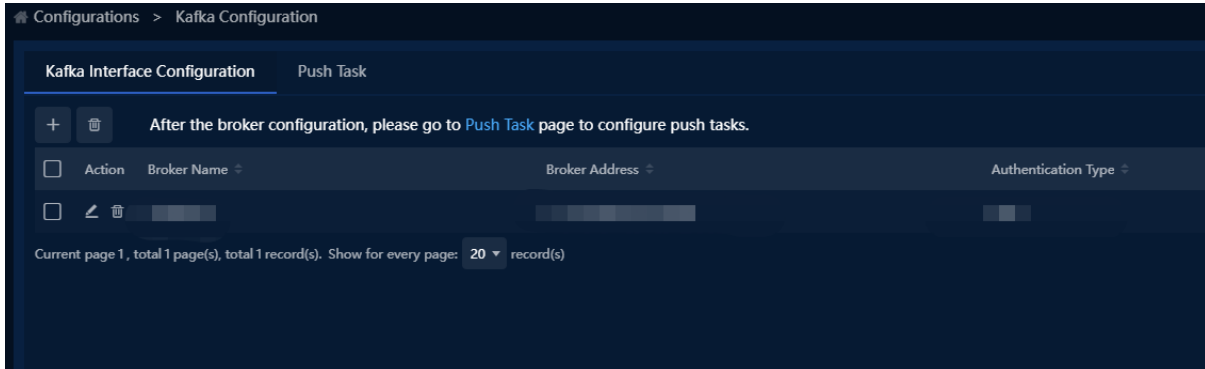




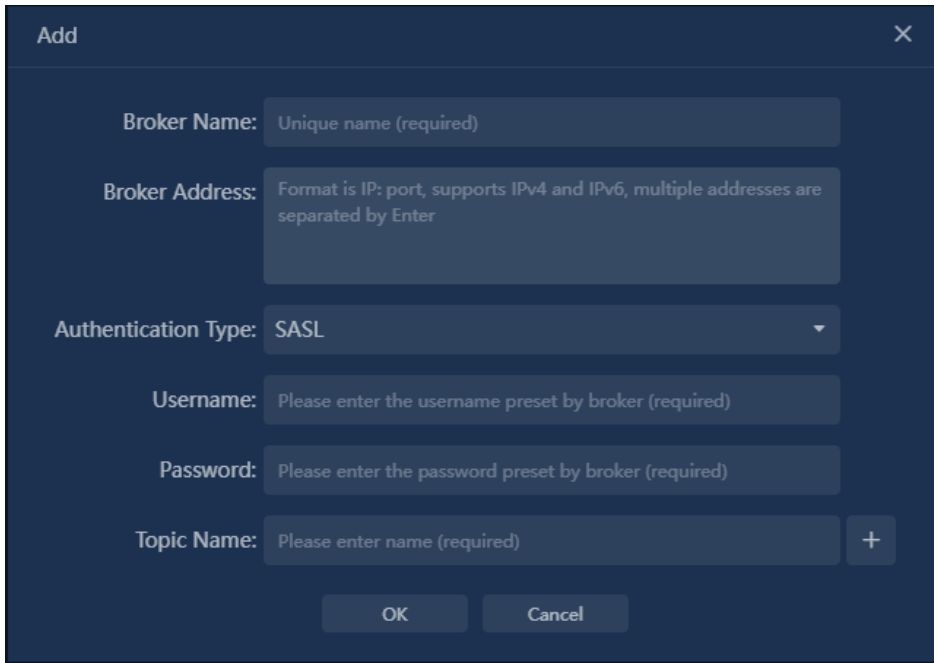
## 4.12. Kafka interface and task

### 4.12.1. 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	This parameter is mandatory. It is used to configure the

Name	Instruction
Type	Kafka authentication mode. SASL and no authentication can be selected.
Username	When SASL authentication is selected, configure the 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

## 4.12.2. 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 choice.
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	This parameter is mandatory. The format of the output

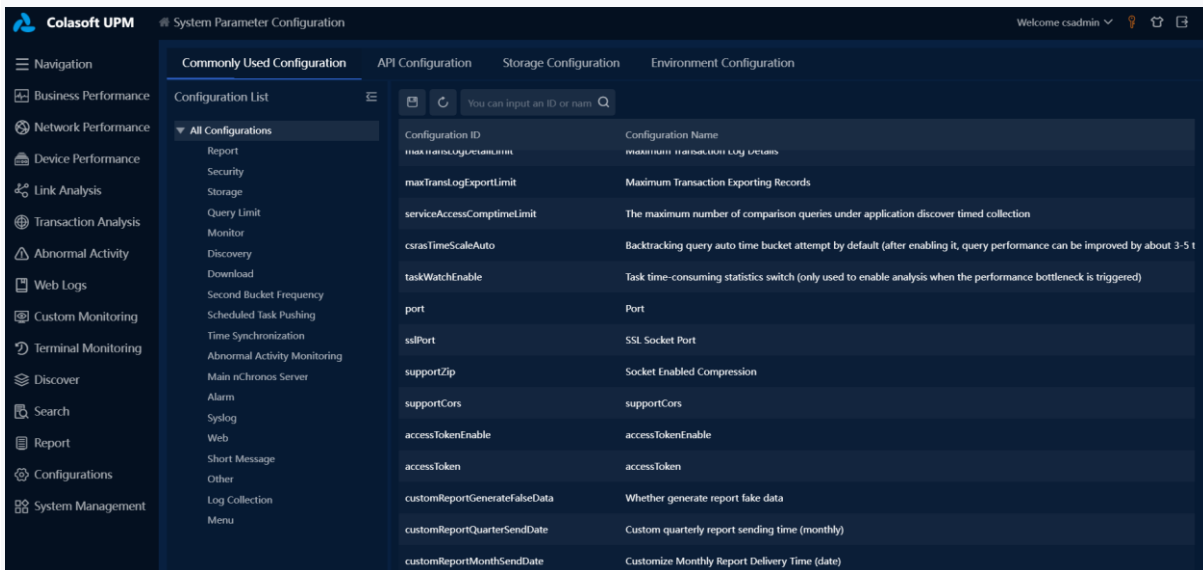
Name	Instruction
Format	data can be binary or JSON.

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

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

## 4.13. System Parameters configuration

Administrator in your browser URL bar type <https://upmip/system/parameter.html> or <https://upmip/syp> 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.

## 4.14. Configure report sending tasks

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

Operation	Name	Frequency of report delivery	Status	Schedule creation time	Number of generated reports	Report Name
<input type="checkbox"/>	test for report requirementReport sending schedule	Daily	Stopped	2022-08-01 11:08:36	10	test for report requirement
<input type="checkbox"/>	testKTReport sending schedule	Daily	Stopped	2022-07-01 10:35:22	42	testKT
<input type="checkbox"/>	Report - testReport sending schedule	Daily	Stopped	2022-06-10 20:19:48	60	Report - test
<input type="checkbox"/>	test for testReport sending schedule	Daily	Stopped	2022-05-05 11:09:48	99	test for test
<input type="checkbox"/>	Basic network reportReport sending schedule	Weekly	Stopped	2022-01-18 16:32:59	28	Basic network report
<input type="checkbox"/>	testReport sending schedule	Daily	Stopped	2021-11-30 20:51:40	251	test
<input type="checkbox"/>	TEST for AISReport sending schedule	Daily	Stopped	2021-11-16 15:44:17	261	TEST for AIS
<input type="checkbox"/>	DEMORepor sending schedule	Quarterly	Stopped	2020-02-21 17:15:24	3	DEMO
<input type="checkbox"/>	demo reportReport sending schedule	Quarterly	Stopped	2019-06-20 15:54:24	3	demo report

The current page 1, total 1 pages, total 9 records. Show 20 records per page.

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.

Add
✕

Report Setting
Email Settings
Sending settings

Plan Name:

Select Report: test for report requirement PDF +

LOGO:  + ↻

1. Image size supports below 100KB  
2. Image format supports \*. JPG, \*. PNG, \*. GIF, \*. BMP

OK
Cancel

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

**Add** [X]

Report Setting | **Email Settings** | Sending settings

Email Title: Colasoft Business Performance Management System Analysis Report

Email Body: This is the regular report from Colasoft business performance management system. Please check the attachment for the detailed report.

Recipient: You can input multiple email addresses with one enter per line.

CC: You can input multiple email addresses with one enter per line.

[OK] [Cancel]

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

**Add** [X]

Report Setting | Email Settings | **Sending settings**

Send way: Send Alone | Merge to Send

Send Period: Daily | Weekly | Monthly | Quarterly

Execute every day 01:00 [v]

Scale: 1-Minute Scale [v]

Business Period: All Period | Specified Period

Report Data: Last Cycle | Current Cycle

Compare:

[OK] [Cancel]

3. Click OK to complete the report sending task.

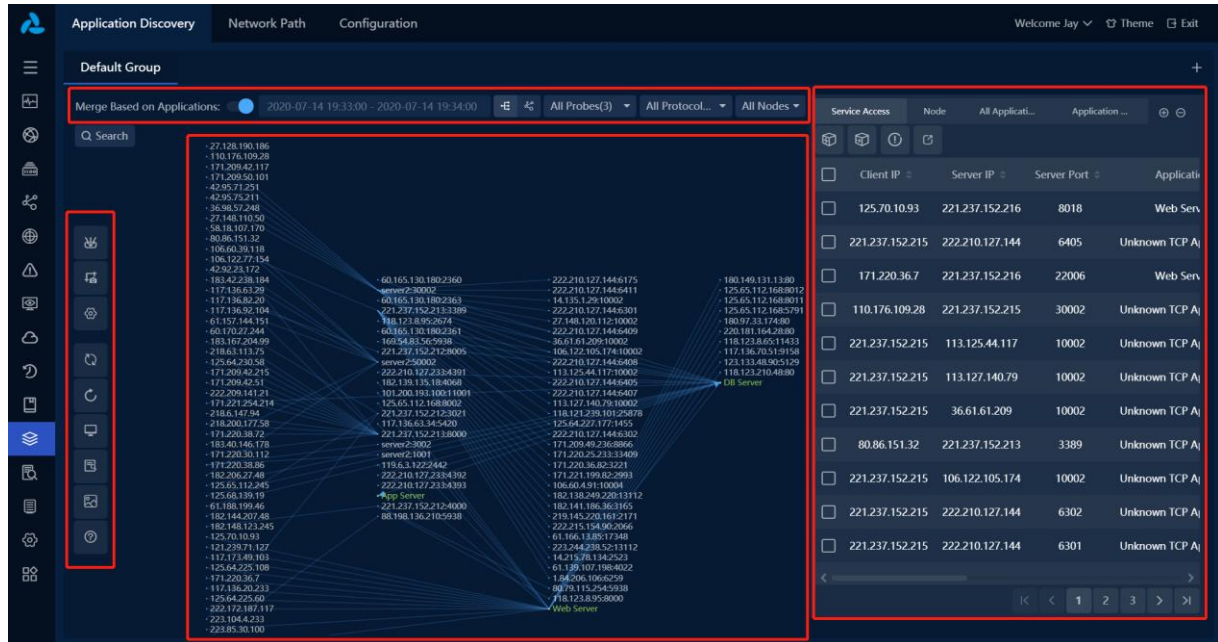
## 5. Discover

### 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.

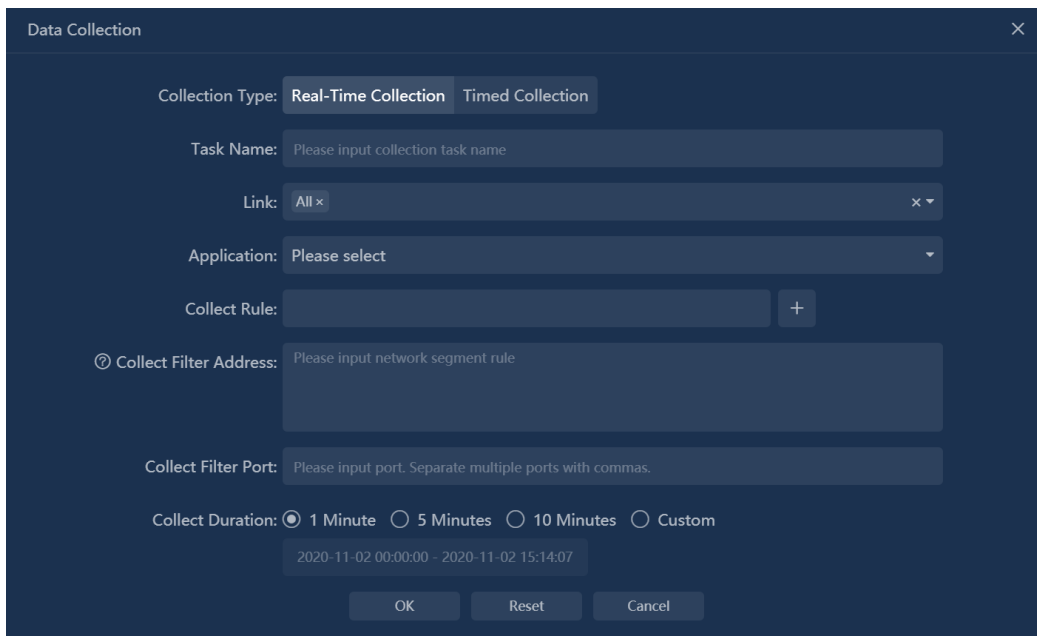
## 5.1.2. Data Collection

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:

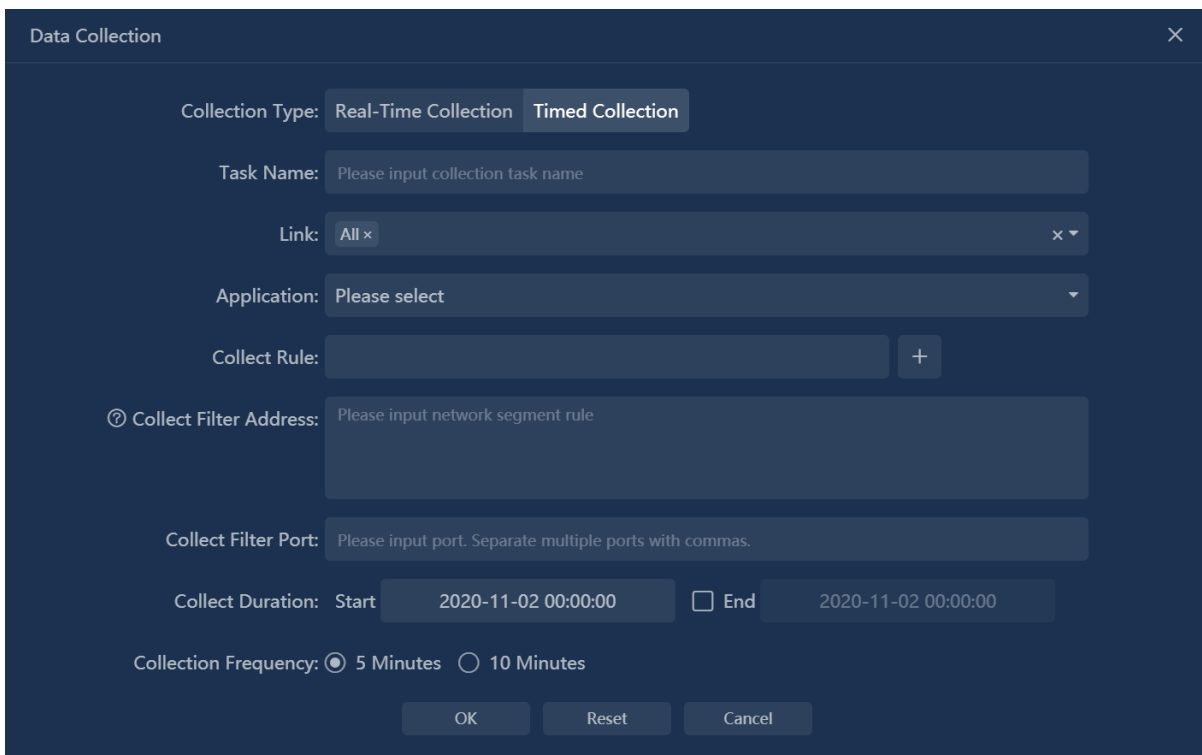
Setting Items	Description
Task Name	It is used to set the name of the collection task. When there are multiple collection tasks, it is recommended to set the name for each collection task to facilitate the distinction and search.
Link	It is used to set the data source for collection, that is, which link 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.

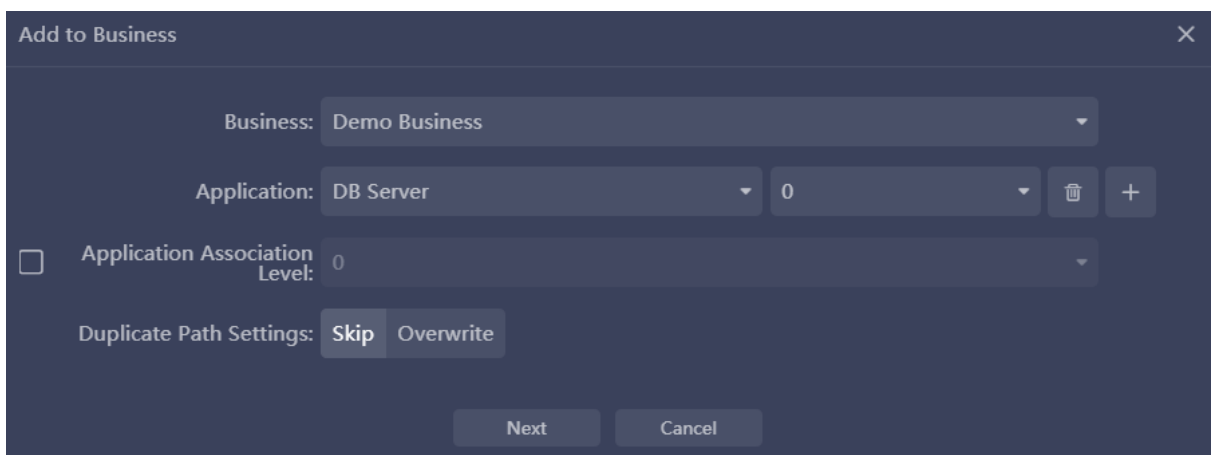
Method 3: In the "Node" list on the right, select one or more node(s) information and click "Add Application"  or "Add to Application"  icon at the top of the table to complete the creation of the application.

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.

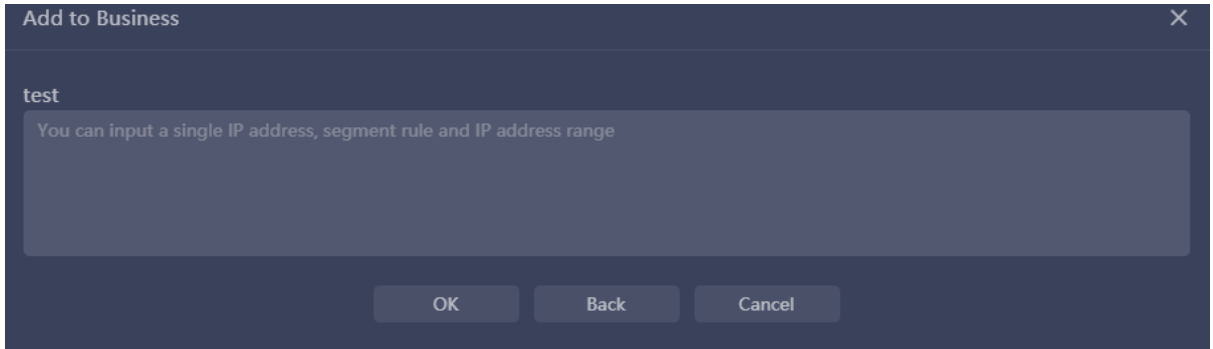
### 5.1.4. Create Business

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

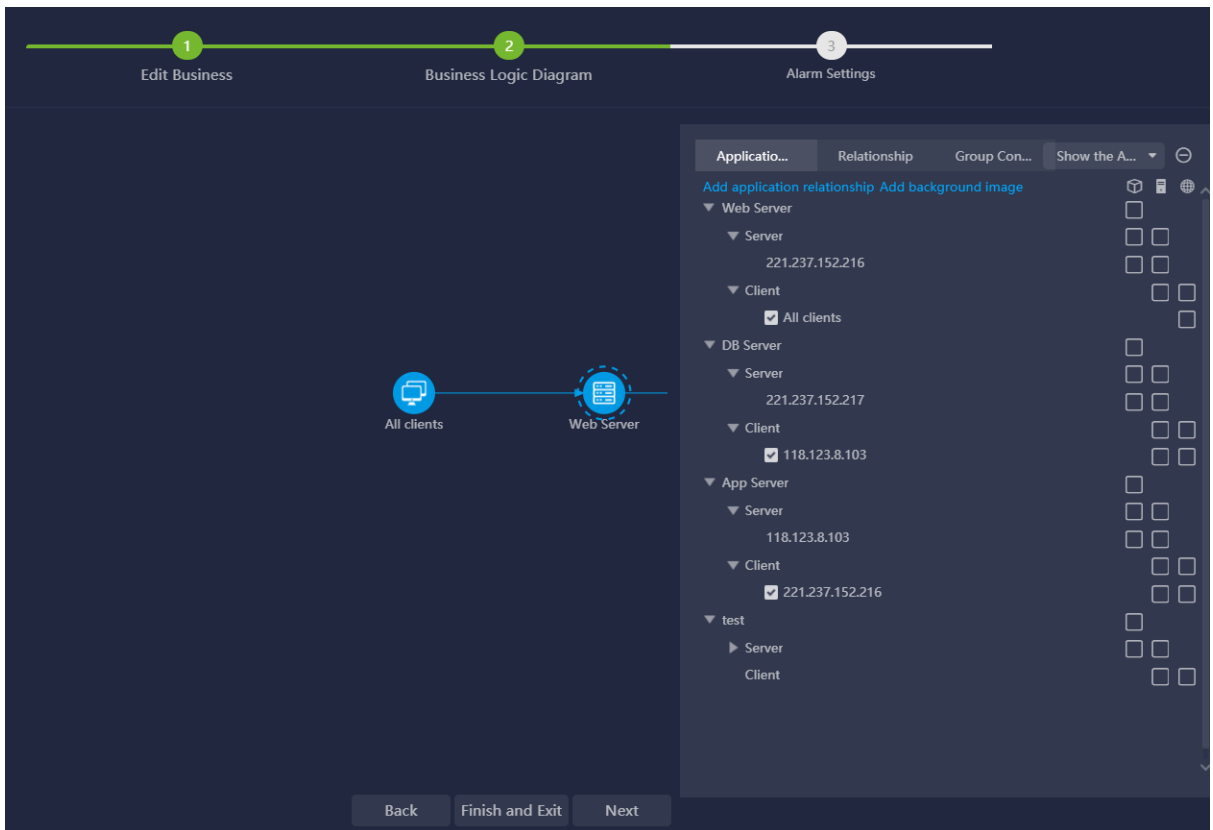
- Step1: In the "All Applications " list on the right, select one or more applications and click the  button at the top of the table to complete the creation of the business.



- 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:

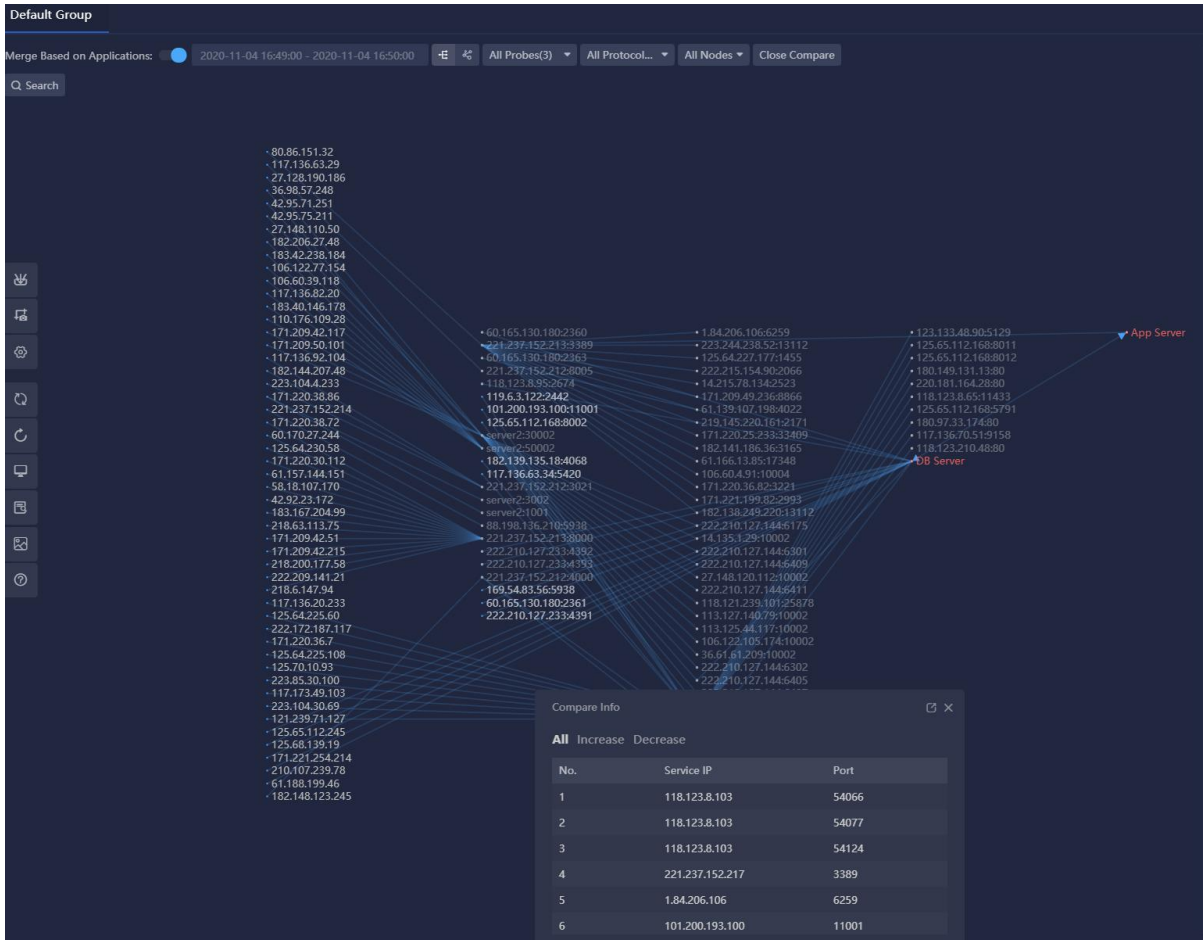


In the business logic diagram, the system will conduct the connection between nodes according to the service access relationship in the application discovery. For nodes that can find access relationship, automatic connection will be made. The probe on the connection is the probe that collects access 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.

### 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.

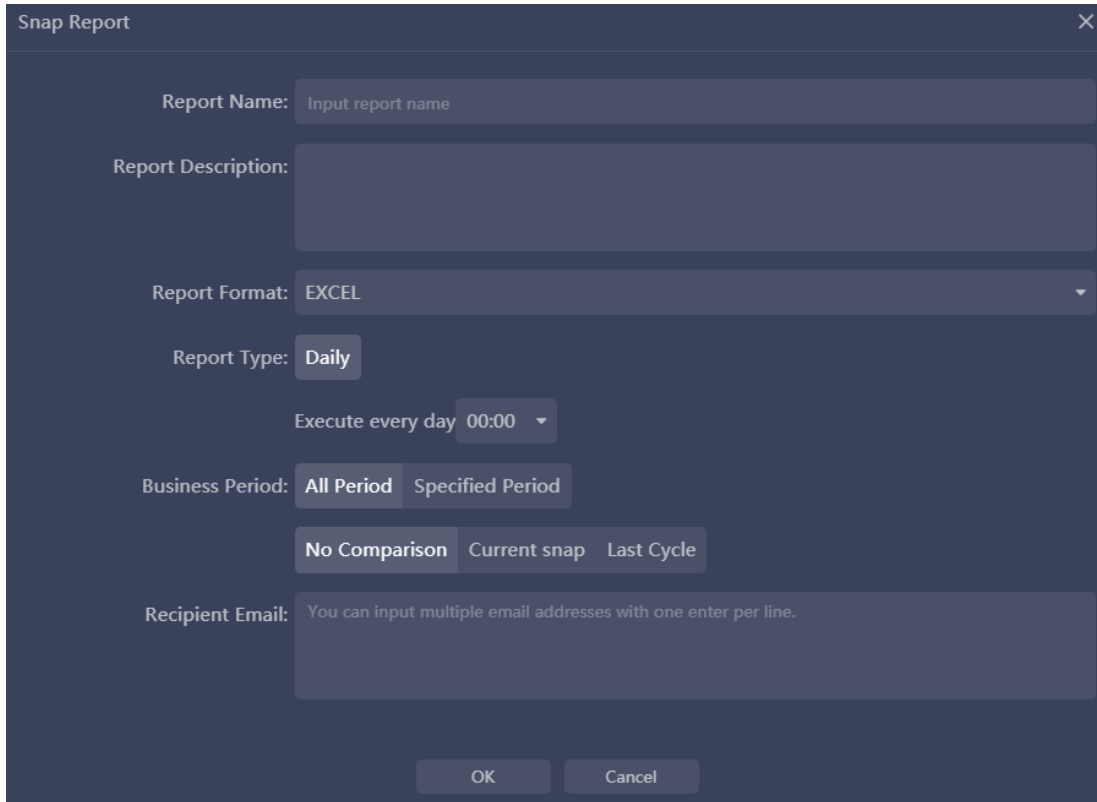
In the comparison diagram, the red text represents the increased IP nodes during the comparison, and the light color text represents the decreased IP nodes during the comparison.

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

## 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:



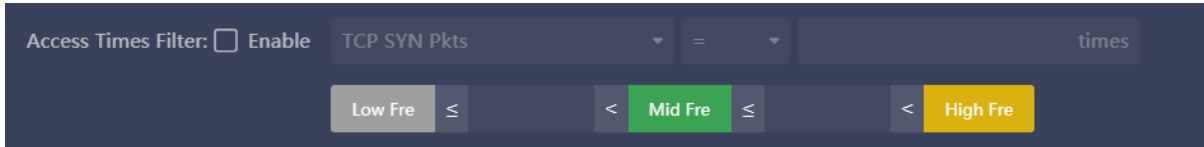
The description of each setting item in the generate snapshot report pop-up box is shown in the following table:

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.

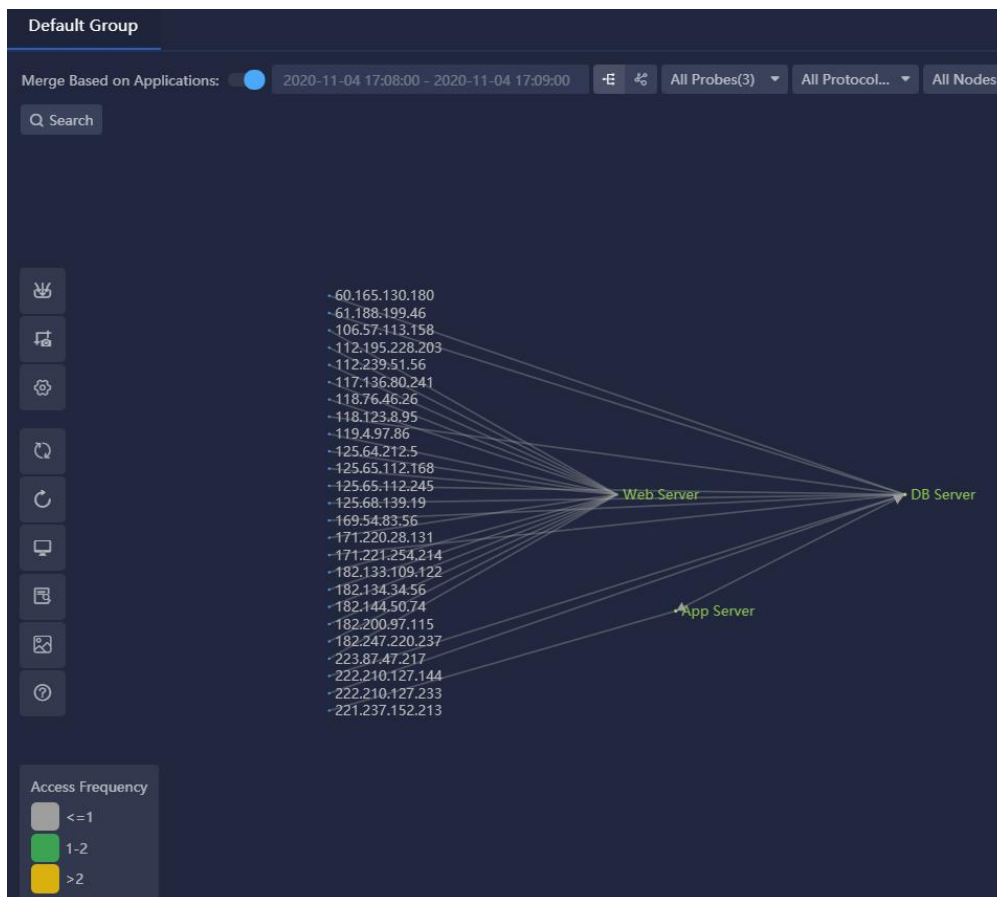
Enable access times filtering in the Display Configuration pop-up box, and set thresholds for filtering conditions and access frequency, as shown in the figure below.



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:




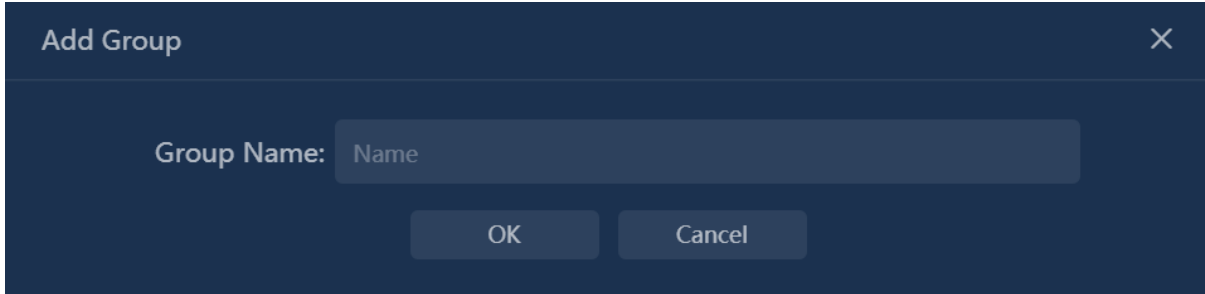
## 5.1.8. Other Common Operations

### Add Group

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

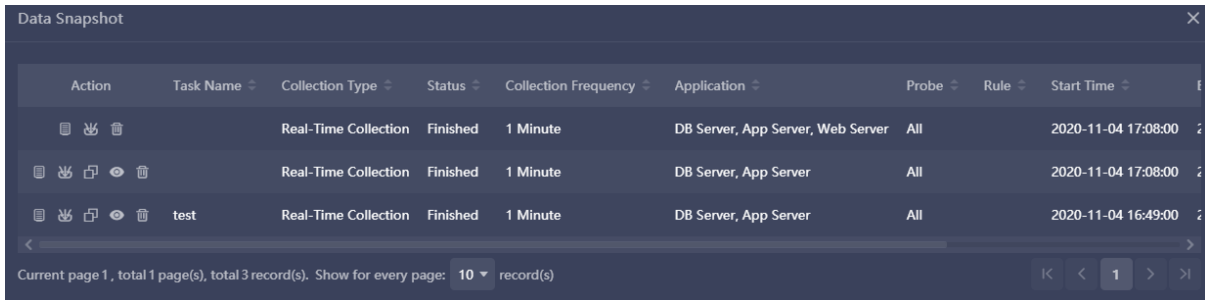
collecting task or the area of collecting data.

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:

**Display Configuration**

Top Clients for One Server Node:

Top Servers for One Client Node:

Client Segment:

Max. Lines:

Display Filter Address:

Display Filter Port:

Access Times Filter:  Enable    times

≤  <  ≤  <

Display Node as:  IP Address  Name  IP and Name

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.

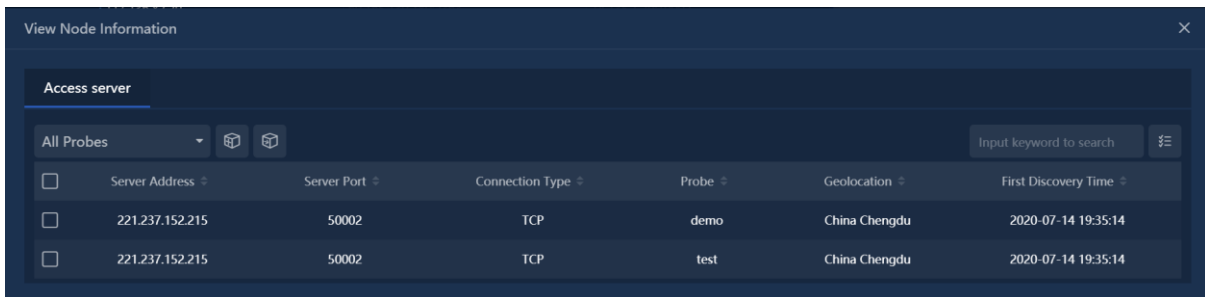
## View Node Information

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.

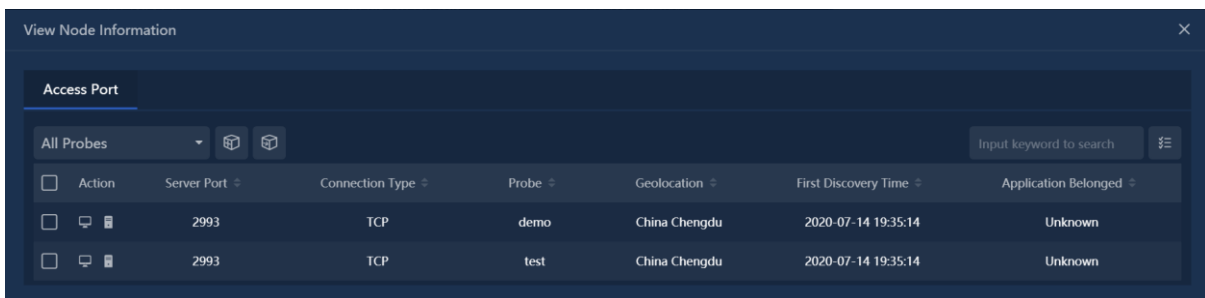
### Client Type Node

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:

Action	Server Port	Connection Type	Probe	Geolocation	First Discovery Time	Application Belonged
<input type="checkbox"/>	2361	TCP	test	China	2020-07-14 19:35:14	Unknown
<input type="checkbox"/>	2360	TCP	test	China	2020-07-14 19:35:14	Unknown
<input type="checkbox"/>	2363	TCP	test	China	2020-07-14 19:35:14	Unknown

## 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:

Server Address	Server Port	Connection Type	Probe	Business Belonged	Geolocation	First Discovery Time
118.123.8.103	52780	TCP	demo	Demo Business	China	2020-07-14 19:35:14
118.123.8.103	52781	TCP	demo	Demo Business	China	2020-07-14 19:35:14
118.123.8.103	52787	TCP	demo	Demo Business	China	2020-07-14 19:35:14
118.123.8.103	52806	TCP	demo	Demo Business	China	2020-07-14 19:35:14
118.123.8.103	52789	TCP	demo	Demo Business	China	2020-07-14 19:35:14

## 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

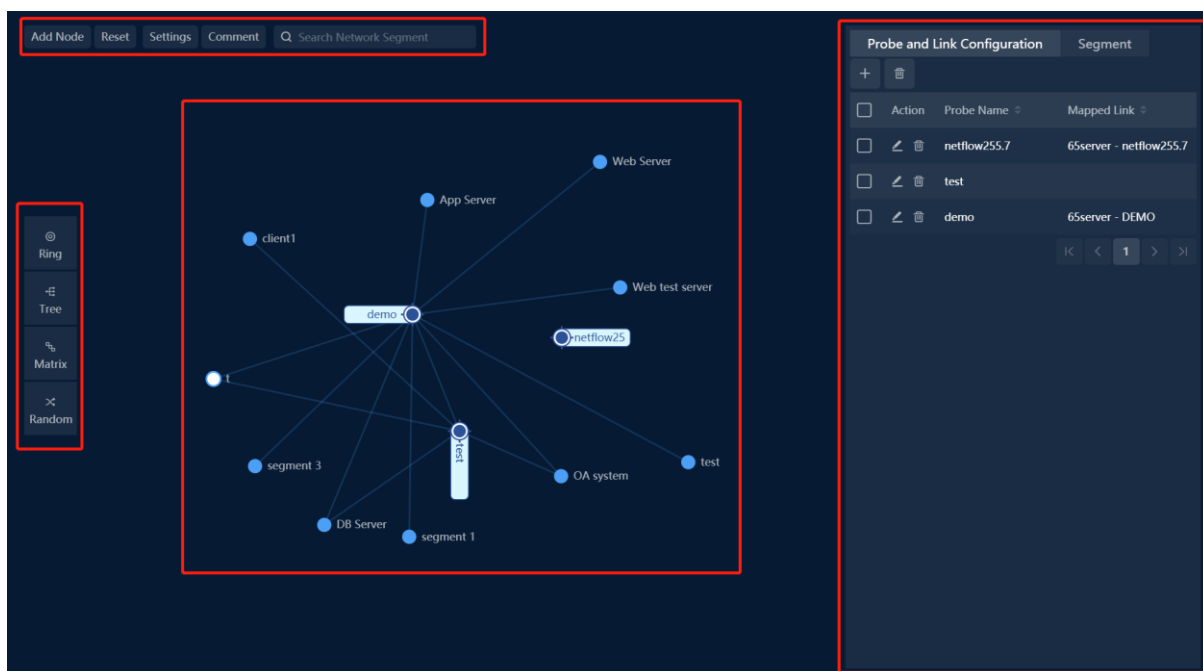
The system provides a "hide/show client" icon. By clicking the icon, users can hide and show client nodes in the application discover diagram.

## 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:

The screenshot shows a dark-themed dialog box titled "Add Node". It features a close button (X) in the top right corner. The dialog contains the following elements:

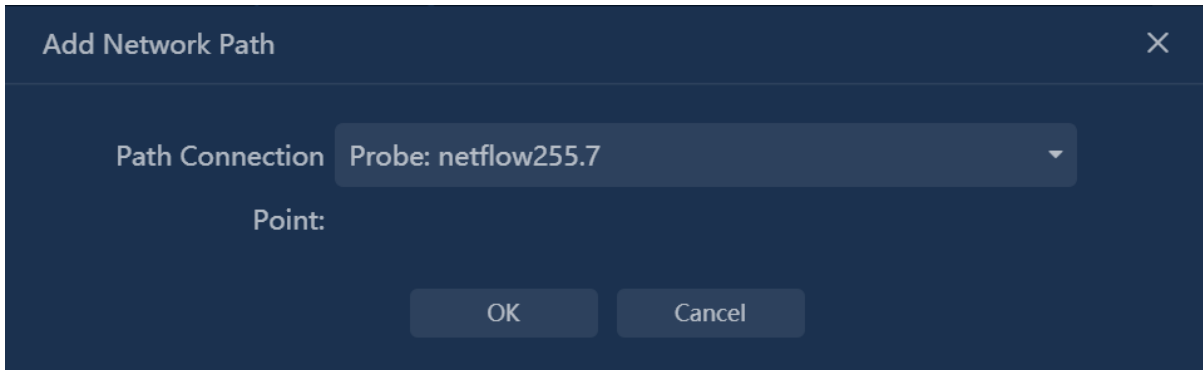
- Name:** A text input field with the placeholder text "Name".
- Type:** Two radio button options: "IP Address" (which is selected) and "Internet Client".
- Segment:** A dropdown menu with the text "Please select" and a downward arrow.
- Address:** A text area with the instruction "You can input a single IP address, segment rule and IP address range".
- Buttons:** "OK" and "Cancel" buttons at the bottom.

Network path nodes include two types:

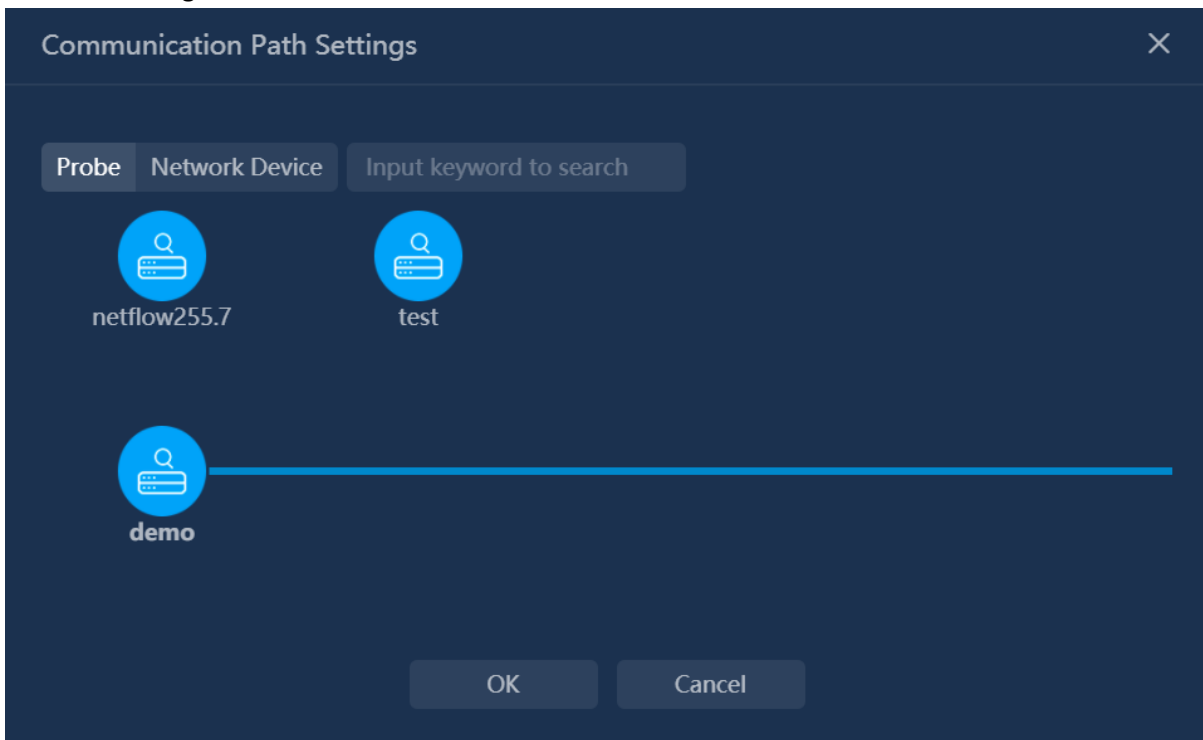
- IP address: users can choose the existing network segment or directly enter the IP address.
- Internet client: if users select the Internet client, it is only need to set the node name.

## 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:



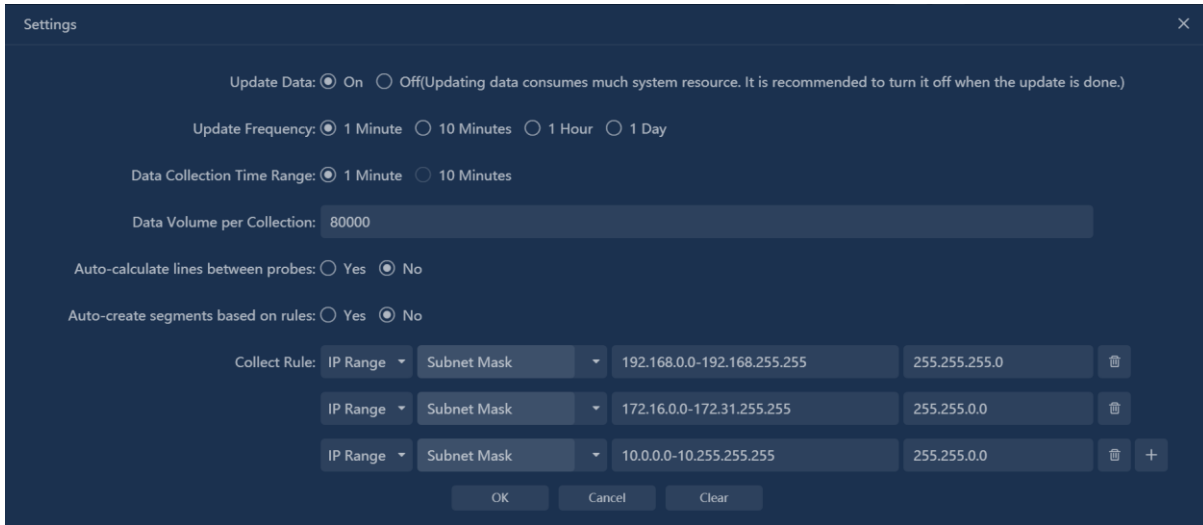
Select the probe in the drop-down list, and the selected probe in the list is the starting probe of the node. Click "OK" button to enter the "Communication Path Settings" and set the pop-up box, as shown in the figure below:



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

## Data Update Settings

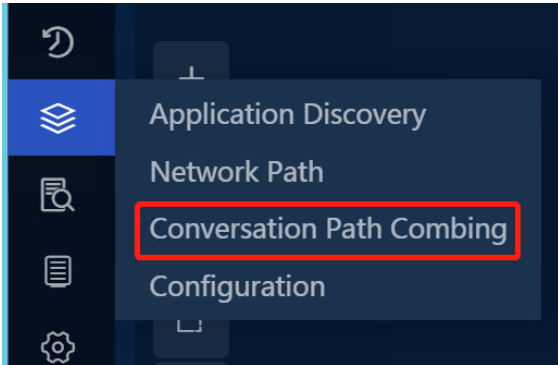
Data Update Settings is used to update the data source of network path discovery. Click the "Settings" button, and a pop-up box of data Update setting pops up, as shown in the figure below:



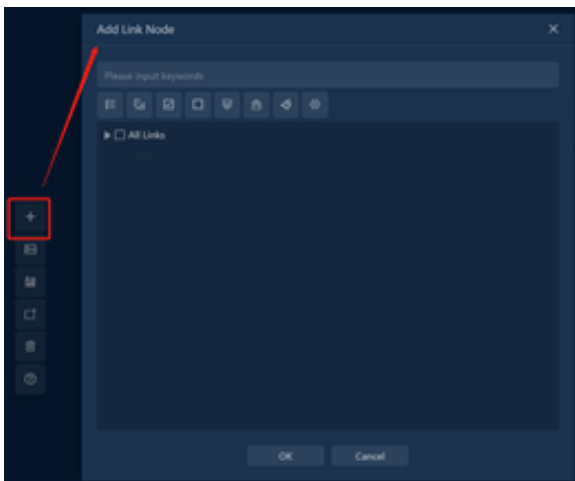
Data update task will take up more system resources, and it is recommended to close this task after network path combing is completed.

## 5.3. Conversion Path Carding

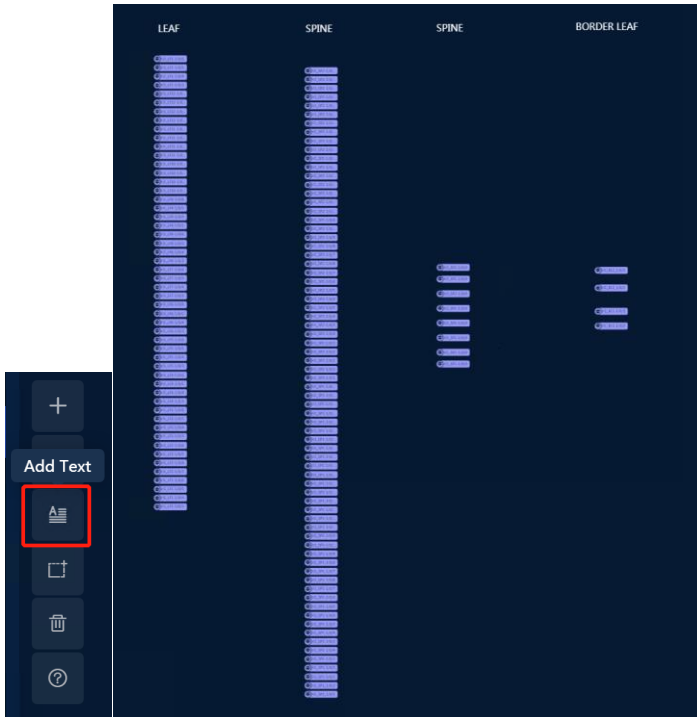
users can check the path of a specific conversation (TCP session) on UPM. Specify the IP address and port of the TCP conversation, input the date and time that will be searched, select conversation direction, then click Start, UPM can show the path of a TCP conversation.



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.

Application Discovery   Network Path   Conversation Path Combing   Configuration

Default Group   SILA-H1

2021-09-05 13:42:00 - 2021-09-05 13:43:00   10.156.131.5   : 54950   -   10.156.131.4   : 10599   Endpoint 2 -> ...   Start

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.

Link Tree   +   ☰   H1\_SP\_1D

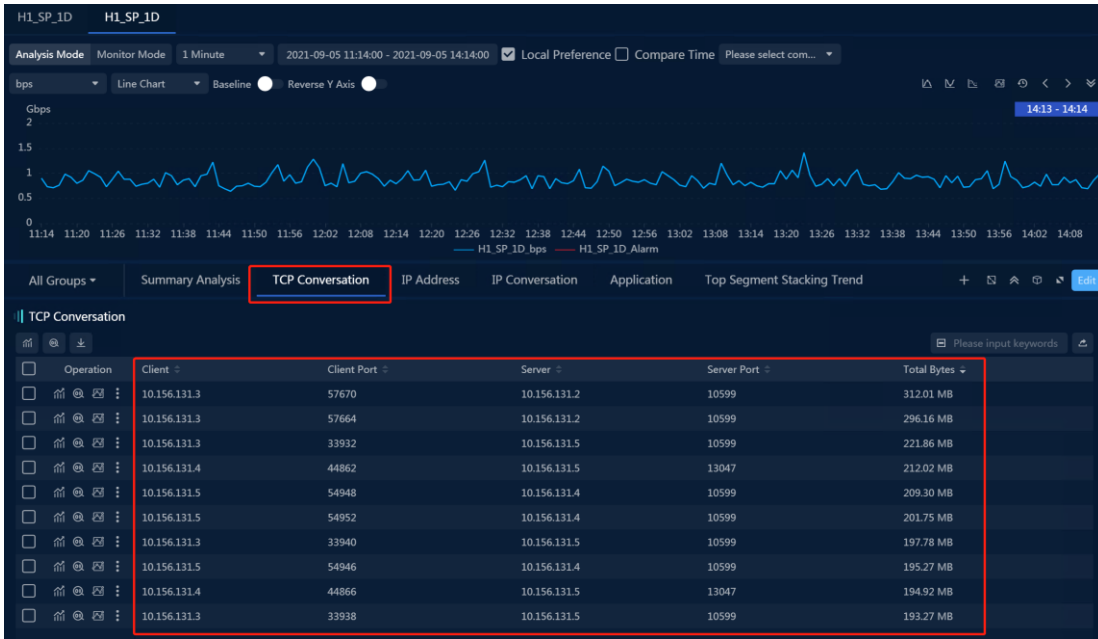
Please input keywords

▼ All Links

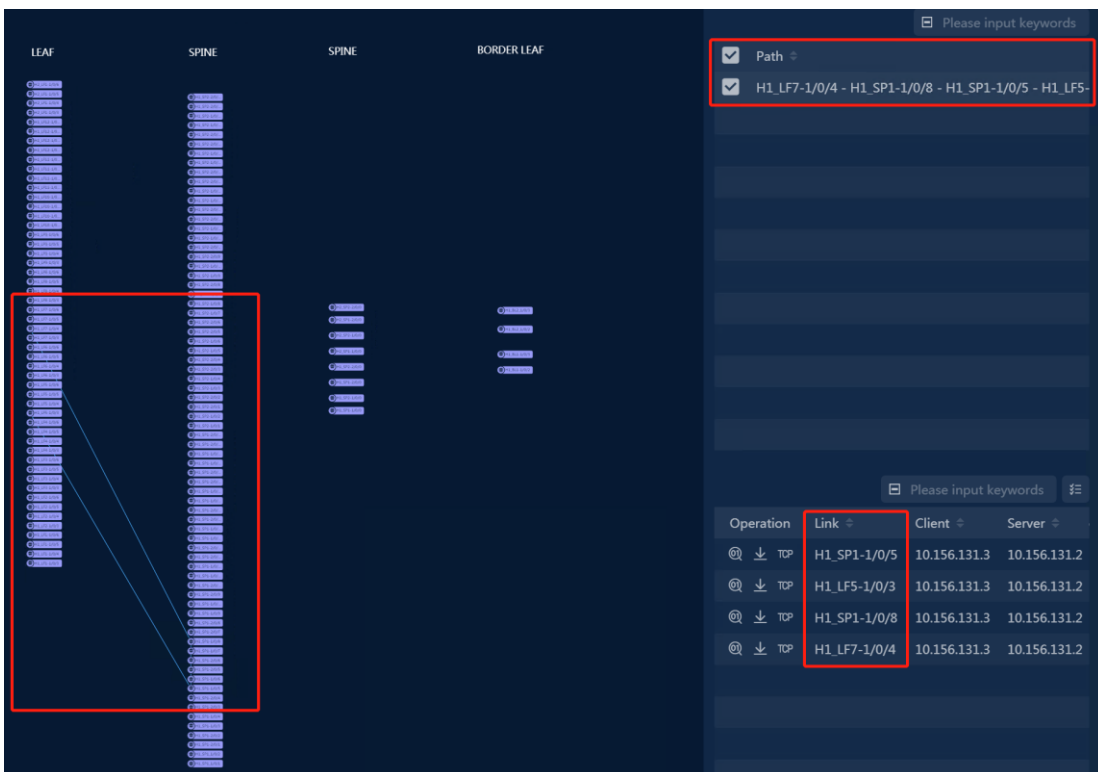
- ▶ H2\_SP\_1D
- ▶ H2\_SP\_2D
- ▶ H2\_BL\_02
- ▶ H2\_BL\_01
- ▶ H1\_SP\_2D
- ▶ **H1\_SP\_1D**
- ▶ H1\_LF\_1-12
- ▶ H1\_BL\_02
- ▶ H1\_BL\_01
- ▶ H1-2\_SP1-2\_U

Link	bps	Total Bytes	Total Pkts
<b>H1_SP_1D</b>	978.89 Mbps	6.84 GB	7266204
H1_SP1_1/0/1	293.64 Kbps	2.10 MB	9390
H1_SP1_1/0/2	210.23 Kbps	1.50 MB	7372
H1_SP1-2/0/1	380.88 Kbps	2.72 MB	10825
H1_SP1-2/0/2	146.89 Kbps	1.05 MB	3505
H1_SP1-1/0/3	467.99 Kbps	3.35 MB	12939





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.

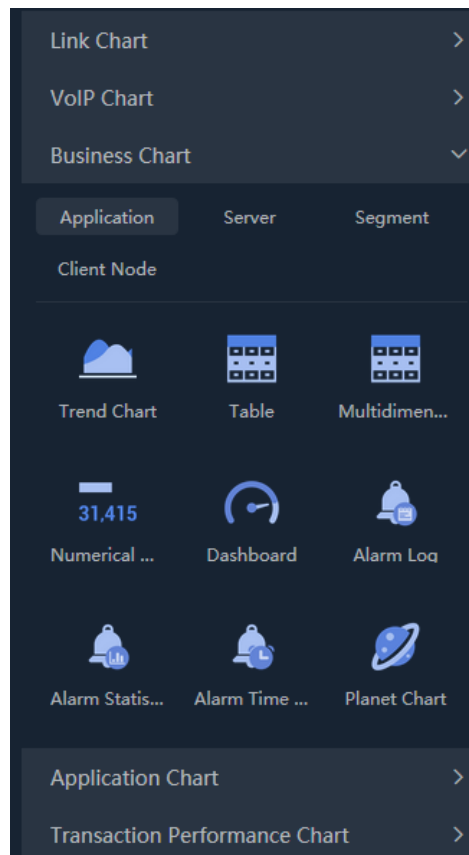
- Click the menu Business Performance -> Business Status to open the Business Status page.
- Click the button “ **Health Level** **Alarm** ” to set the health and alarm status information of the business to display.
- Users can add, edit and delete the business groups.
- Click the button “ **Fullscreen** ” 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:

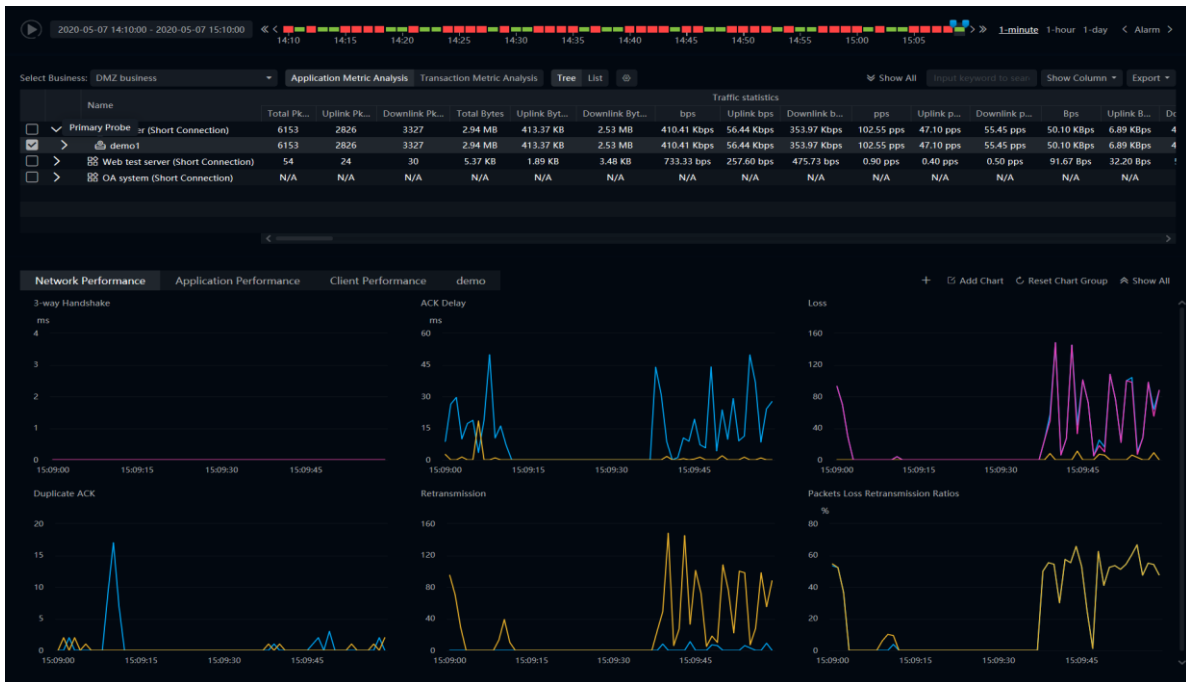


- Click the button “ **Configure Metrics** ” to set application node metrics, client line metrics and custom application node metrics. No more than three indicators per object. The types of indicators include TCP layer performance indicators and application transaction performance indicators.
- Click 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 “Tree List” 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.



## 6.7. Business Multiple 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.

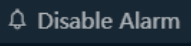


- Through the "business performance analysis" page, right click the line in the business logic diagram, and select "multi-segment analysis" from the pop-up menu to enter the multi-segment analysis page.
- Users can do analysis configurations:
  - select the application under the current business.
  - 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.


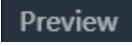

- Users can click the button “” to open the Disable Alarm page.
- Users can click the button “” to open the data downloading page.
- Users can click the button “” to download the packets automatically saved by the server to the local.

### 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 “” to preview the real chart.
- After completing the settings, click the button “” 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.

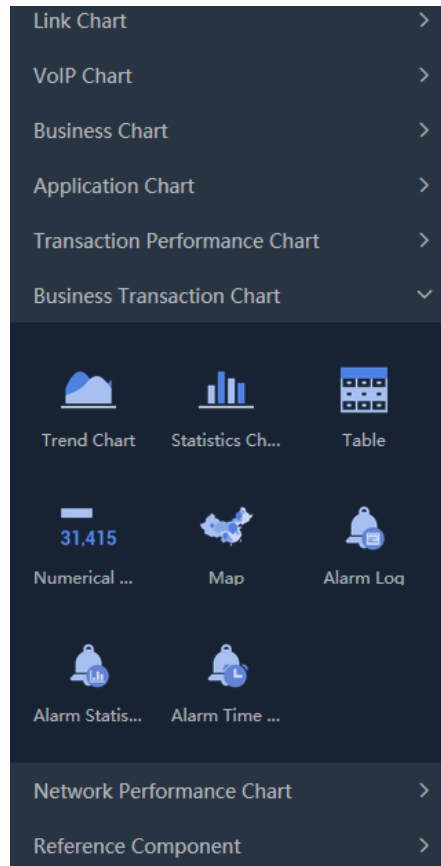
- In the report list page, users can also click the name of a report to enter the report log interface and view the historical reports generated by the report



## 7. Transaction

### 7.1. Transaction Custom Monitoring

Click the menu Custom Monitoring -> Custom Metric Monitoring to open the custom metric monitoring interface.




### 7.2. 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.

### 7.3. Transaction Custom Query

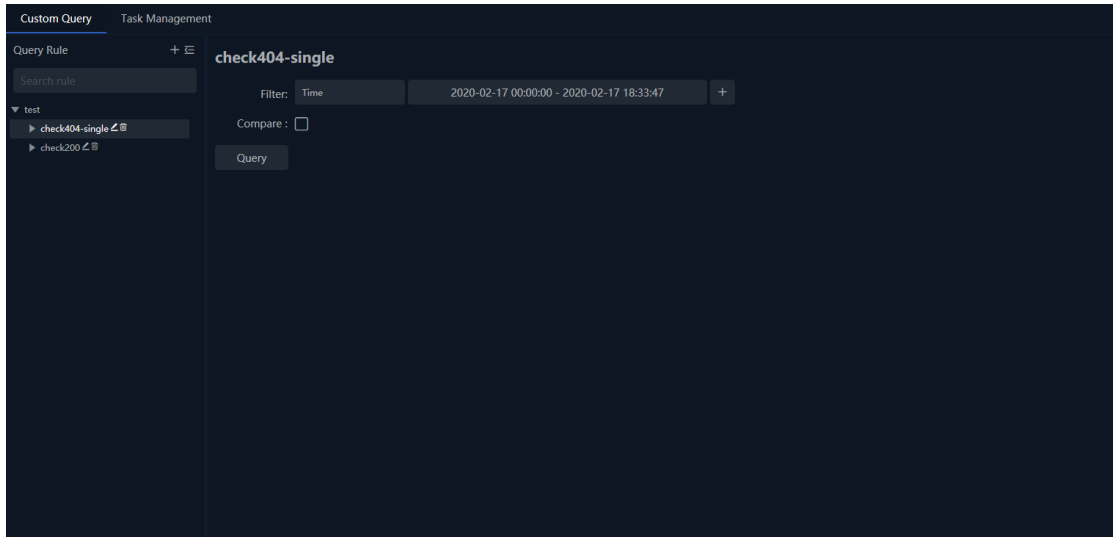
According to the needs of analysis, the system flexibly defines the query rules based on the configured business fields and trading metrics, and outputs the query results. Multiple query rules can be defined, and users can save and export query results


 **Note**

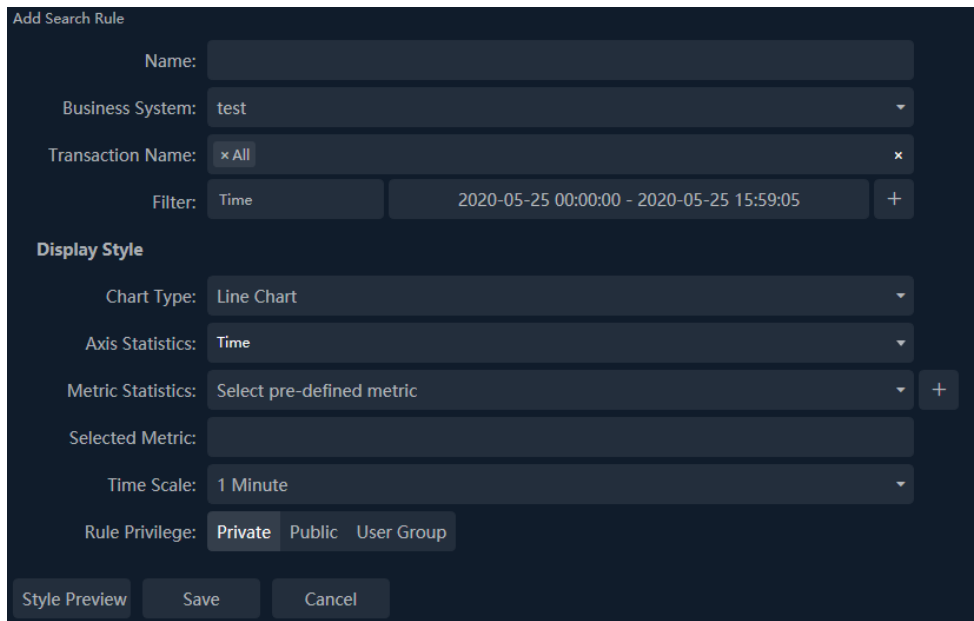
The system can only custom queries for transactions configured with business fields. All automatically identified transactions are processed as one type of transaction (transaction group).

## 7.3.1. 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:

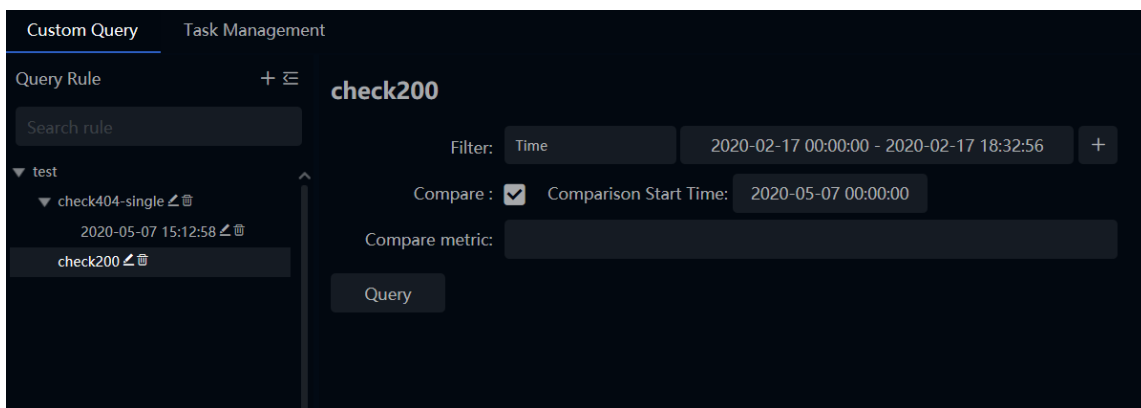


- Name: Doesn't allow duplicate names
- Business System: Choose a business system
- Transaction Name: Choose transaction names
- Filter: One or more filters can be added, where "transaction time" is the required filter. A filter is an enabled state field in the business field configuration of the selected 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.

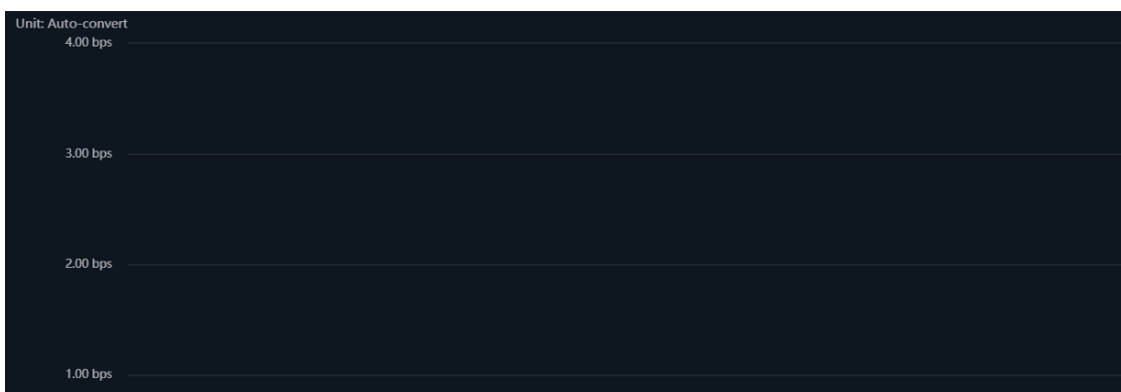
- Axis Statistics: User can select multiple field dimension for statistics when the table typed selected while only one filed can be selected when other chart types selected.
- Metric Statistics: Selected transaction metrics.
- Time Scale: Only valid when the time dimension selected.
- After entering 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.

### 7.3.2. 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.

### 7.3.3. 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.

Action	Task Name	Task Type	Progress	Create Time	Creator	Comments
	check404-single	Custom Transaction Query	Finished	2020-05-07 15:12:58	Administrator	Task runs successfully, query result has been saved.
	check200	Custom Transaction Query	Finished	2020-05-07 15:16:40	Administrator	Task runs successfully, query result has been saved.

Current page 1, total 1 page(s), total 2 record(s). Show for every page: 10 record(s)

**Note**

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

### 7.4. 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:

**Configurations Add**

Business System

- All Business System
  - Demo1
  - Demo

**Basic Configuration** | Advanced Configuration

Alarm Name:

Alarm Description:  Creator:

Level:  Alarm Category:

Alarm Type:  Time Bucket:

Filter:   +

Trigger Condition:

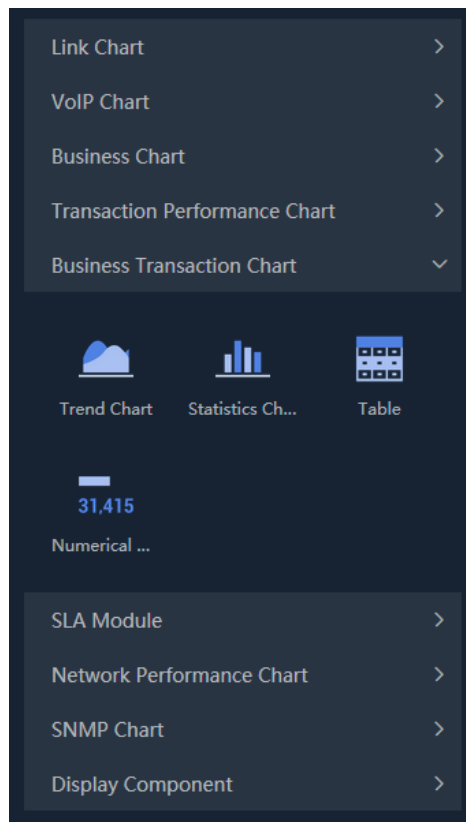
Additional information:  Enable  Latest...

OK Cancel

### 7.5. 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:






## 8. Network

### 8.1. 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.

#### 8.1.1. 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.

#### 8.1.2. 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.

### 8.2. 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.

### 8.2.1. 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.

### 8.2.2. 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.

### 8.2.3. Comparison Analysis

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

### 8.2.4. 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).

## 8.3. 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.


## 8.4. 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.

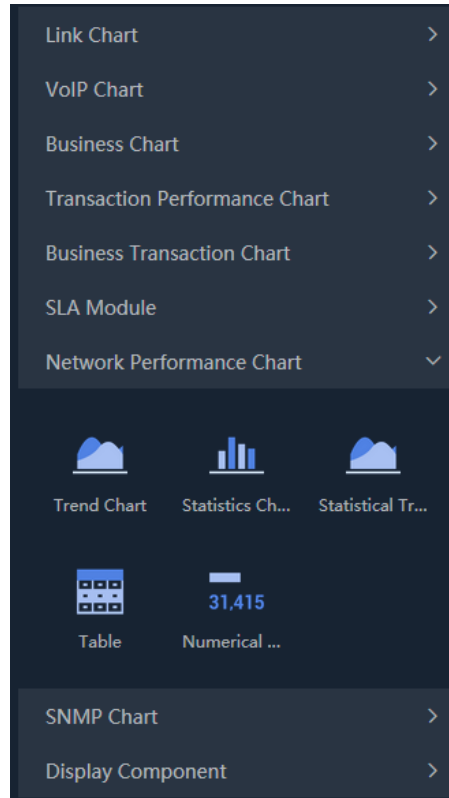
- Click the menu Network Performance ->Network Performance Alarm to open the Network Performance Alarm page.
- Click the button “” to record the alarm. When the same alarm is triggered later, users can view the previous log for quick troubleshooting.
- Click the button “” to view the previous log for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

## 8.5. 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.




## 8.6. 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.

## 8.7. 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

## 9. Device

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


### 9.1. 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.


### 9.2. 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.

### 9.3. 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.

## 10. Link


### 10.1. 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.

### 10.2. VoIP Custom Analysis

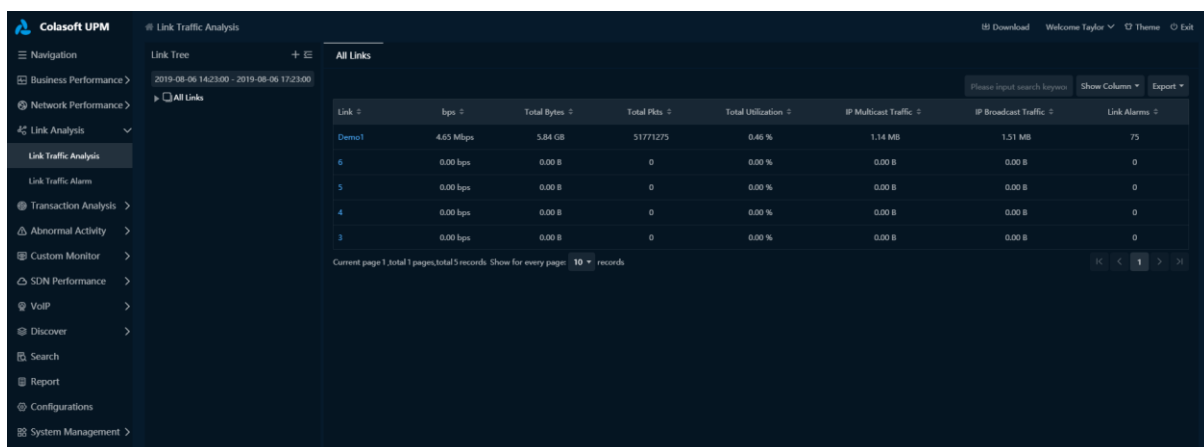
Users can customize the monitoring settings according to their needs.

- 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.

### 10.3. 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.

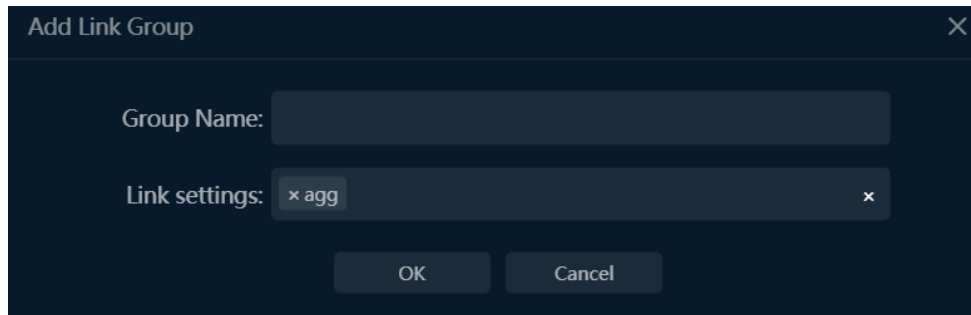


Link	bps	Total Bytes	Total Pkts	Total Utilization	IP Multicast Traffic	IP Broadcast Traffic	Link Alarms
Demo1	4.65 Mbps	5.84 GB	51771275	0.46 %	1.14 MB	1.51 MB	75
6	0.00 bps	0.00 B	0	0.00 %	0.00 B	0.00 B	0
5	0.00 bps	0.00 B	0	0.00 %	0.00 B	0.00 B	0
4	0.00 bps	0.00 B	0	0.00 %	0.00 B	0.00 B	0
3	0.00 bps	0.00 B	0	0.00 %	0.00 B	0.00 B	0




Current page 1, total 1 pages, total 5 records. Show for every page: 10 records

#### 10.3.1. Group

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



### 10.3.2. 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.

### 10.3.3. Comparison Analysis

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

Users can check  **Compare Time**, 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.

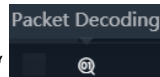
Last Month YoY: Compare the data over the same time range last month.

### 10.3.4. 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).

### 10.3.5. Packets Decoding



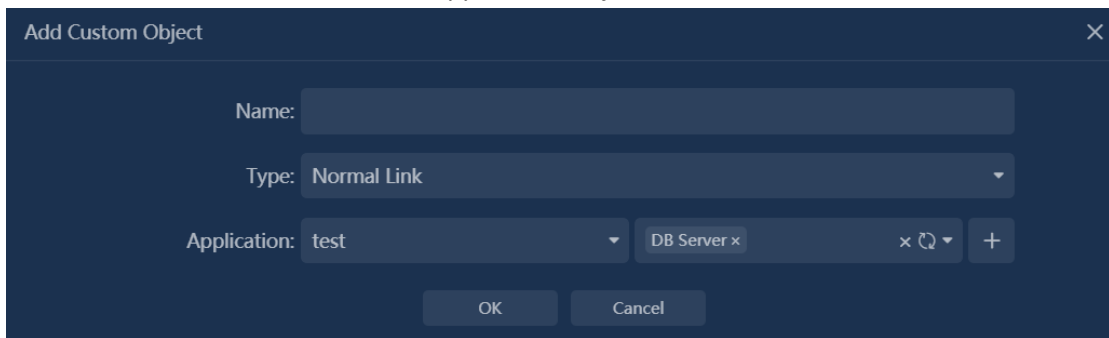
In the process of link analysis, click the button “” to view the decoding information of analysis object's packet online.

## 10.4. Application Object Analysis

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




### 10.4.1. Customize Application Object

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




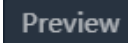

## 10.5. Link Traffic Alarm

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.

## 10.6. 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.

## 10.7. 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.

## 11. Abnormal Activity

### 11.1. Abnormal Activity Monitoring

Abnormal Activities Monitoring is provided by the UPM center. It's a function to monitor all abnormal access activities monitored by the system. Users can define abnormal activities in Abnormal Activity Alarm so as to monitor the abnormal activities.

Users can monitor abnormal activities via Abnormal Activity -> Abnormal Activity Monitoring. The latest anomaly information can be monitored in real time at a refresh rate of 1 minute.

- **Abnormal activity status diagram**

Abnormal activity state diagram is based on the application has been discovered. It shows the abnormal access of application. Including: abnormal access between applications, as well as illegal clients access the application, and use the flow arrow shows attack direction.

By default, only the application has been added in business will be displayed. Users can click

“  Filter “ button to check the application in the pop-up dialog box.

- **Attack source**

TOP 10 attack source IP addresses that trigger the abnormal activity alarm on the same day. Click the IP address and view the abnormal activity alarm.

- **Target IP**

TOP 10 target IP addresses that are attacked on the same day. Click the target IP addresses and view the abnormal activity alarm.

- **Type distribution**

The distribution of various abnormal access activities on the same day. Click on the distribution type and view the abnormal activity alarm.

- **TOP 10 applications**

TOP 10 applications that are attacked on the same day. Click the application and view the abnormal activity alarm.

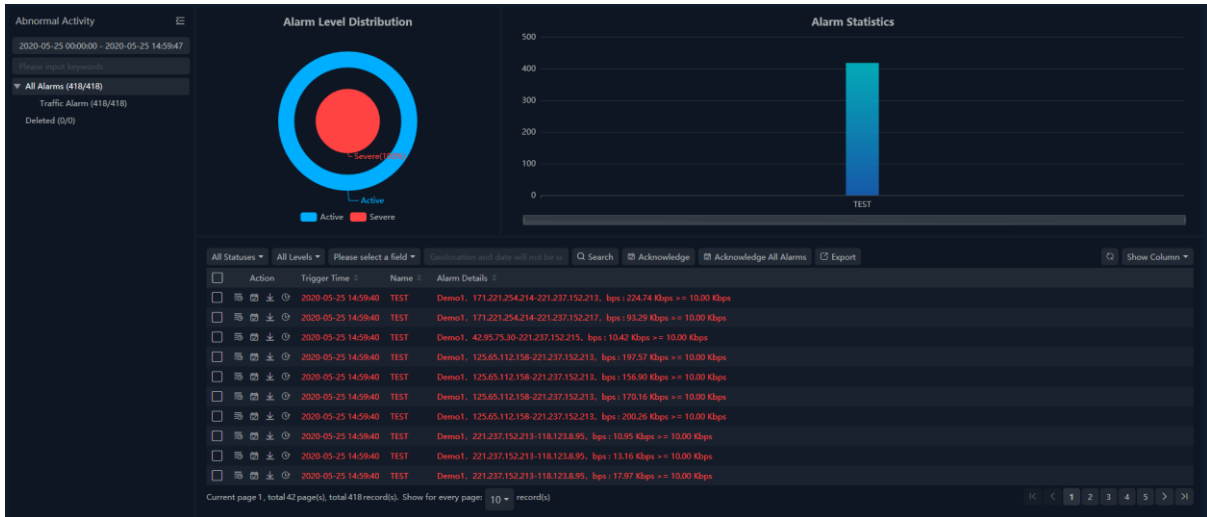
- **Alarm log**

Display all abnormal activity alarms triggered during the current monitoring period. Click to view the abnormal activity alarm

### 11.2. Abnormal Activity Alarm

Click the menu Abnormal Activity-> Abnormal Activity Alarm to open the Abnormal Activity Alarm page, which shows all triggered abnormal activity alarm logs, as the screenshot below:





By default, only all alert logs for the day are displayed and the alarm logs can be exported.

## 12. Terminal Monitoring

The terminal monitoring function is to monitor application client types in different scenarios. The main scenarios include:

- **VoIP terminal monitoring:** By monitoring video (voice) terminal jitter, delay, packet loss and other metrics, it can timely discover abnormal terminals and locate the cause of the problem.
- **Application client monitoring:** By analyzing the network performance metrics (latency, number of conversations, traffic, etc.) of the terminal accessing the business system, monitoring the application service status and network quality from the perspective of terminal experience, and quickly locating problems.
- **Backup monitoring:** Through statistical analysis of service data, monitor the service switching and recovery status of participating terminals in the drill.

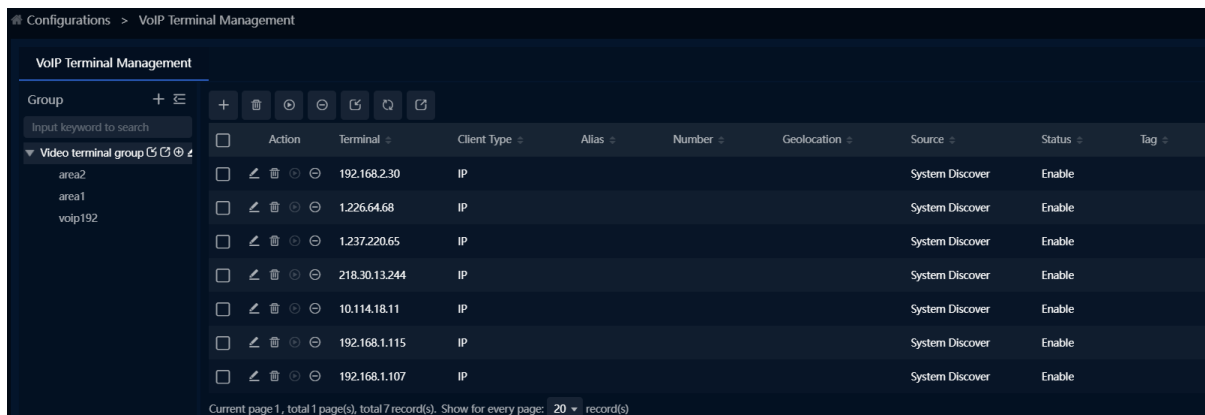
Main functions include:

- **Terminal management:** terminals used for maintenance and monitoring, 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 alerts.
- **Terminal alarm query:** query terminal alarm log.

### 12.1. Terminal management

Click the menu Terminal Monitoring -> Configuration -> Terminal Management to open the configuration page. Select different terminals for configuration according to the scenario, including backup terminal management, VoIP terminal management, and application client management.

The terminal configuration process is basically the same. Take the VoIP terminal configuration as an example, as shown in the following figure:



Terminals are managed in a group-level manner.

- Step 1: click the button “+” to add a group, as the screenshot below:

Dialog: Edit VoIP Terminal Group


Name: Video terminal group

Discover Terminal

Automatically:

Group Level:	Level	Name
	0	0
	1	1
	2	
	3	
	4	
	5	
	6	

Buttons: OK, Cancel

- Step 2: Click the button “” next to the group to add lower group. Multiple peer and subordinate groups can be added.

Dialog: Group

Group Level: 1

Group Name: area2

Probe: DEMO1

Note: Modification to father probe may cause that the sub-probe cannot capture data.

Group Number:

Correlated Network: Please select

Segment:

Geolocation:

Longitude:

Latitude:

Buttons: OK, Cancel

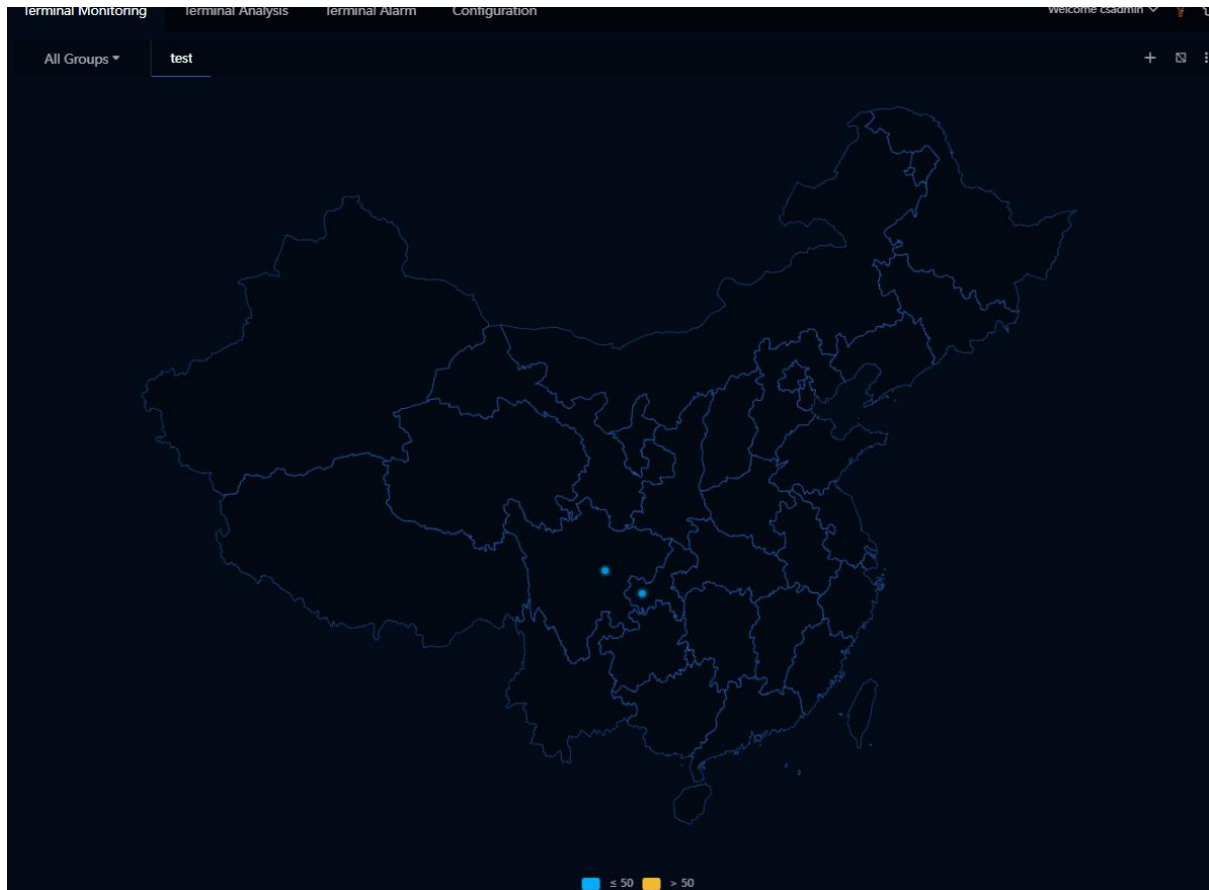
Terminal grouping needs to be associated with probes and network segments, which are used to indicate the data collection area and range of grouped terminals.

- Step 3: Add terminals. Select the node and add a single terminal or add batch terminals.

Note: The system can associate network segments according to the group, automatically discover the terminals within the range and add them to the terminal list.


## 12.2. Terminal Monitoring

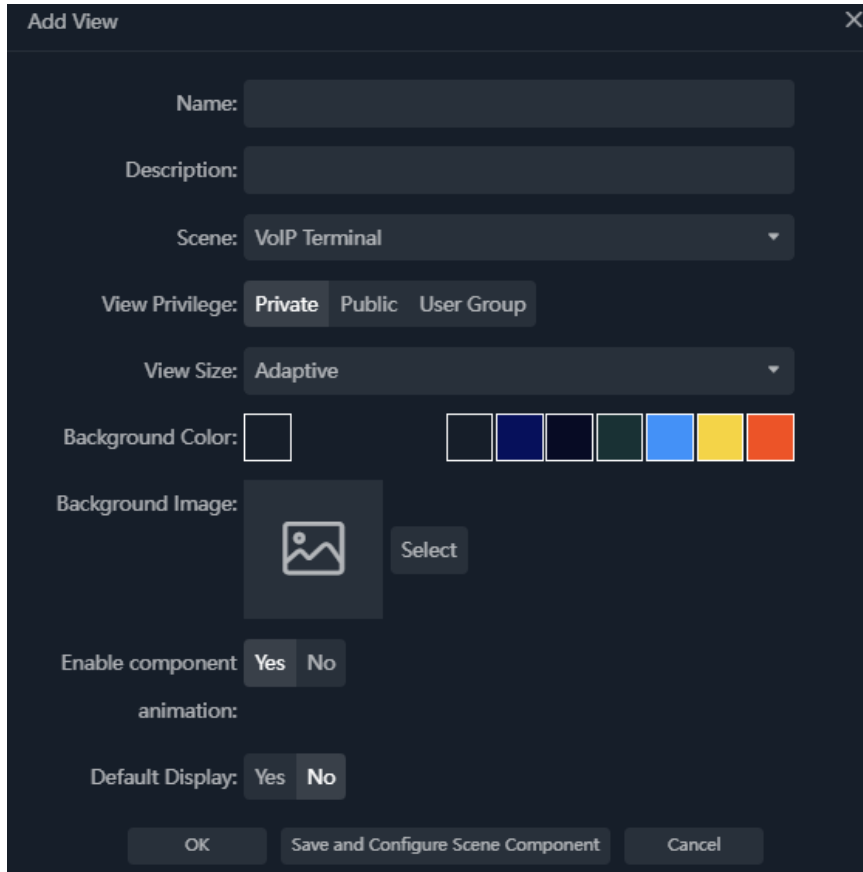
Click the menu Terminal Monitoring -> Terminal Monitoring to open the configuration page, as the screenshot below:



The terminal monitoring page includes monitoring view management and real-time monitoring. There is no monitoring view by default. So the first step is to create a monitoring view.

### 12.2.1. Create Monitoring View

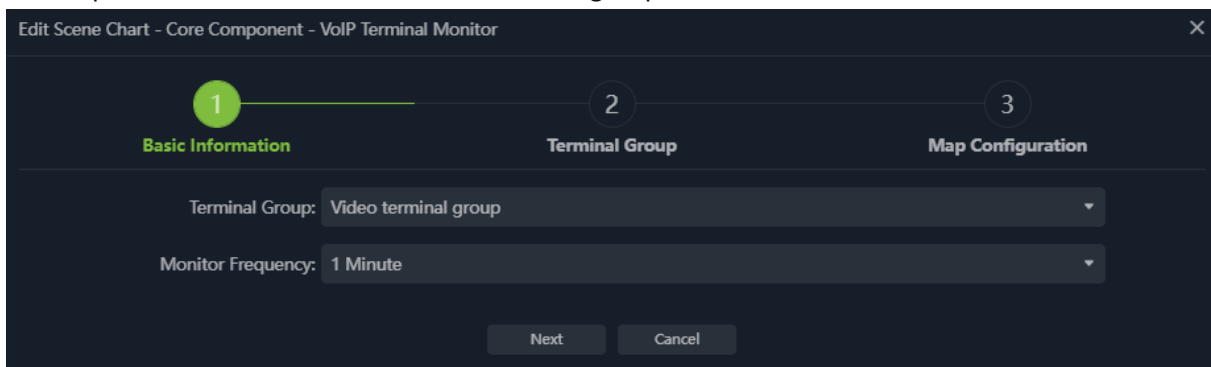
Click the button “” to add a monitoring view, the configuration is shown below:

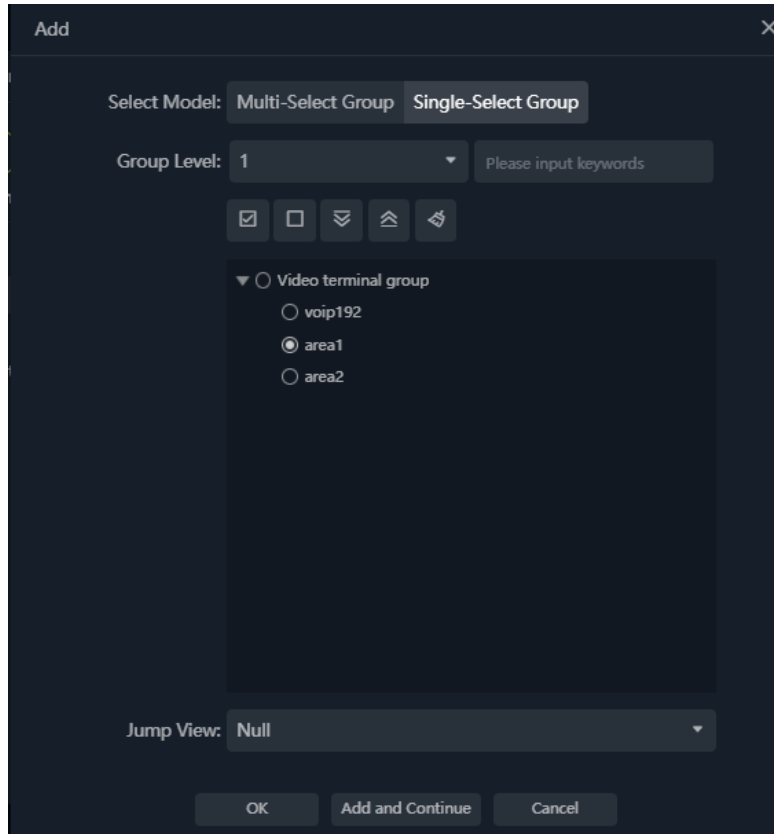


- Customize the group name, cannot be the same as other group names.
- Scene, that is, options for different monitoring scenarios. The default is the application client terminal monitoring. After selecting "VoIP terminal", it is the VoIP monitoring scenario. When adding a monitoring client, only the client type of the corresponding scenario can be selected, which corresponds to the type in the terminal management group.

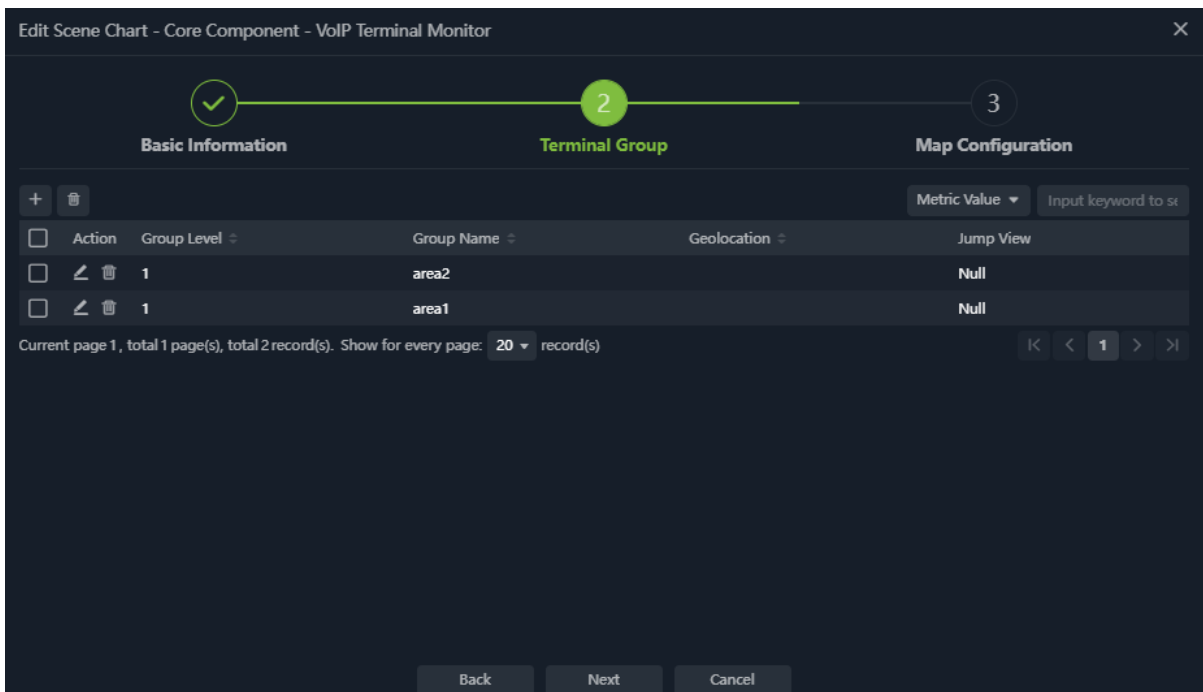
After entering the information, click the "OK" button, and an empty monitoring view will be generated. The monitoring component panel can be expanded on the left side of the view, and the monitoring view can be configured through the components in the panel. Users can also directly select "Save and configure scene components" to start configuring monitoring views.

- Step 1: select monitor terminal and terminal group.





- Support multiple selection.



After the selection is complete, click "Next" to configure the display map.

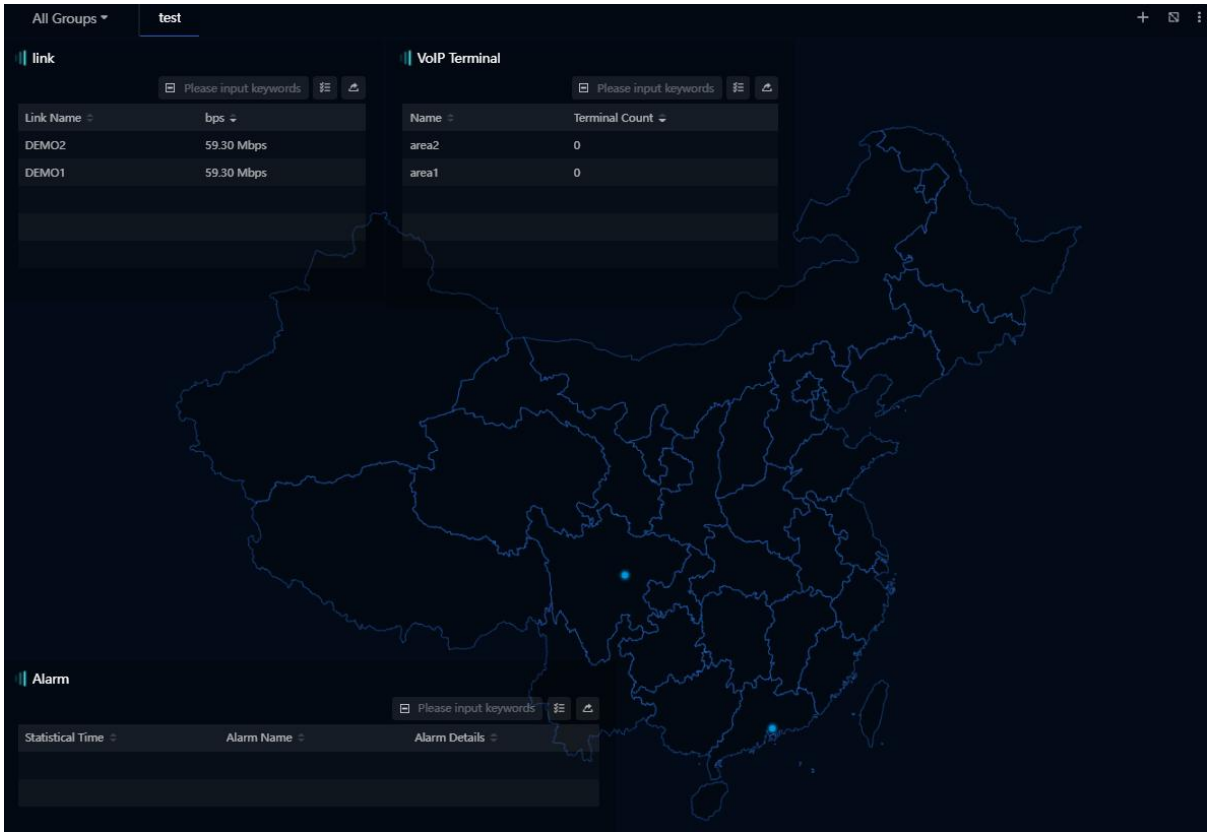


After completing all configurations, click the "OK" button to save and complete the view creation.

Note: When creating a monitoring view, the node geolocation will be automatically displayed on the map based on the group geolocation information (geographic location name or latitude and longitude). In addition, the node geolocation can be dragged with the left mouse button.

### 12.2.2. Real-Time Monitoring

The default refresh rate of the monitoring view is 1 minute, and the monitoring period is 1 minute.

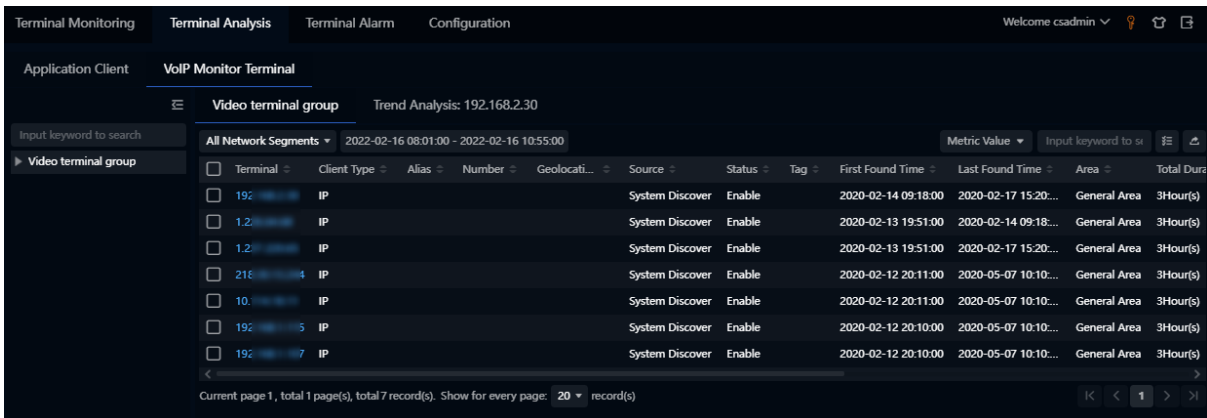


- The monitoring metrics support customization, and the node color changes through the metric value range.
- Right-click the monitoring node and click "Terminal Analysis" to enter the terminal analysis page.

### 12.3. Terminal Analysis

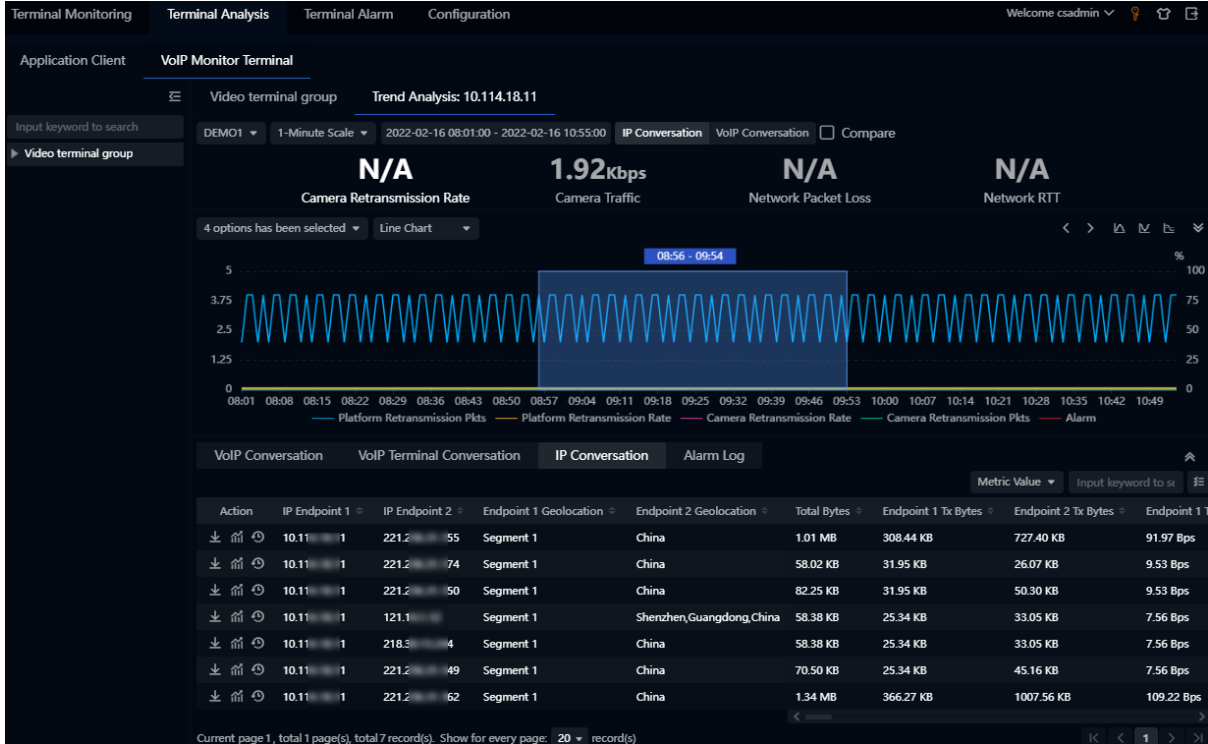
Terminal analysis is to analyze and locate problems through terminal indicators and provide judgment basis.

- Click the menu VoIP -> Terminal Analysis to open the Terminal Analysis page, as the screenshot below:



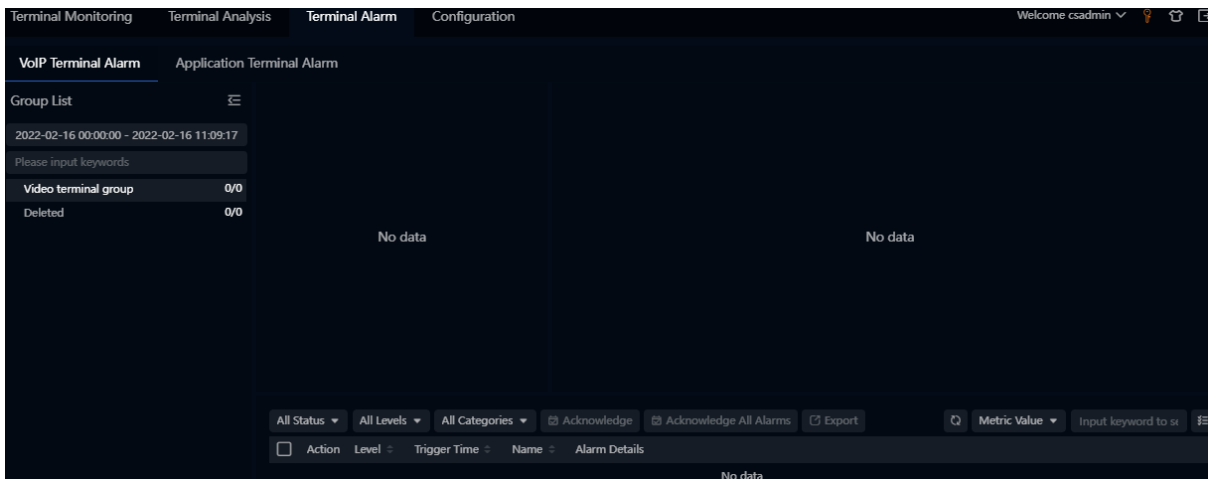


Through terminal grouping, users can quickly filter and locate terminals, and view terminal summary information. Click the terminal IP to enter the terminal metric analysis details page.



## 12.4. Terminal Alarm

Click the menu VoIP -> Terminal Alarm to open the Terminal Alarm page, as the screenshot below:



- By default, displays all alert logs for the day.
- Carry out alarm processing operations through “Acknowledge”;
- Support to export alarm log.



## 13. Backup Monitoring

Main functions include:

- Terminal management: mainly for centralized configuration management of organizational level and network terminals. Used for terminal grouping and client terminal resources. Support query, edit, delete, add, import and other functions.
- Backup monitoring: mainly displays the recovery status of each system business of each terminal group (such as province, city, and network node), and distinguishes the recovered and unrecovered status by color. Display the recovery time, the number of recovered outlets, the number of unrecovered outlets, and the business recovery status of each system. Support the creation of monitoring views on demand, define view names, maintain participating outlets and business types in the view, and display the recovery situation in the process of recovery switching by configuring predefined business recovery judgment conditions.
- Backup analysis: displaying business logs. Supports viewing business transaction log details by outlets and business types. Export to local is supported.

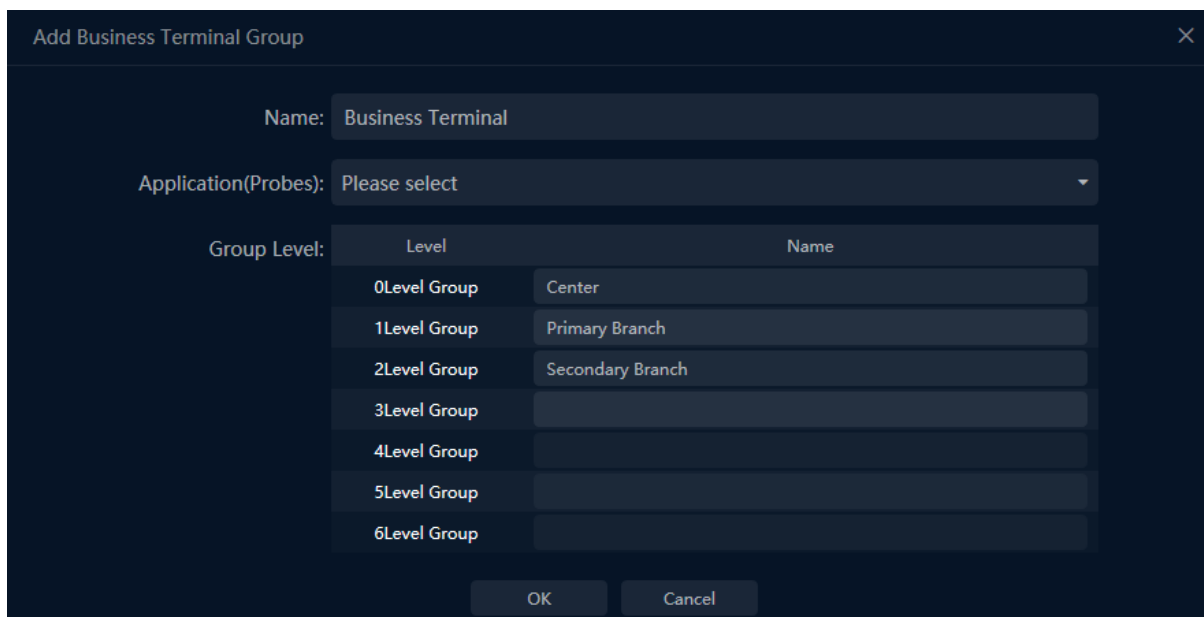
### 13.1. Terminal Management

Click the menu Configuration -> Backup Terminal Management to go to the Backup Terminal Management interface.

#### 13.1.1. Add a Terminal Group

On the left side of the page, click button “” to open the terminal group adding box.

- Complete the basic information.



**Add Business Terminal Group**

Name:

Application(Probes):

Group Level:	Level	Name
	0Level Group	Center
	1Level Group	Primary Branch
	2Level Group	Secondary Branch
	3Level Group	
	4Level Group	
	5Level Group	
	6Level Group	

OK Cancel

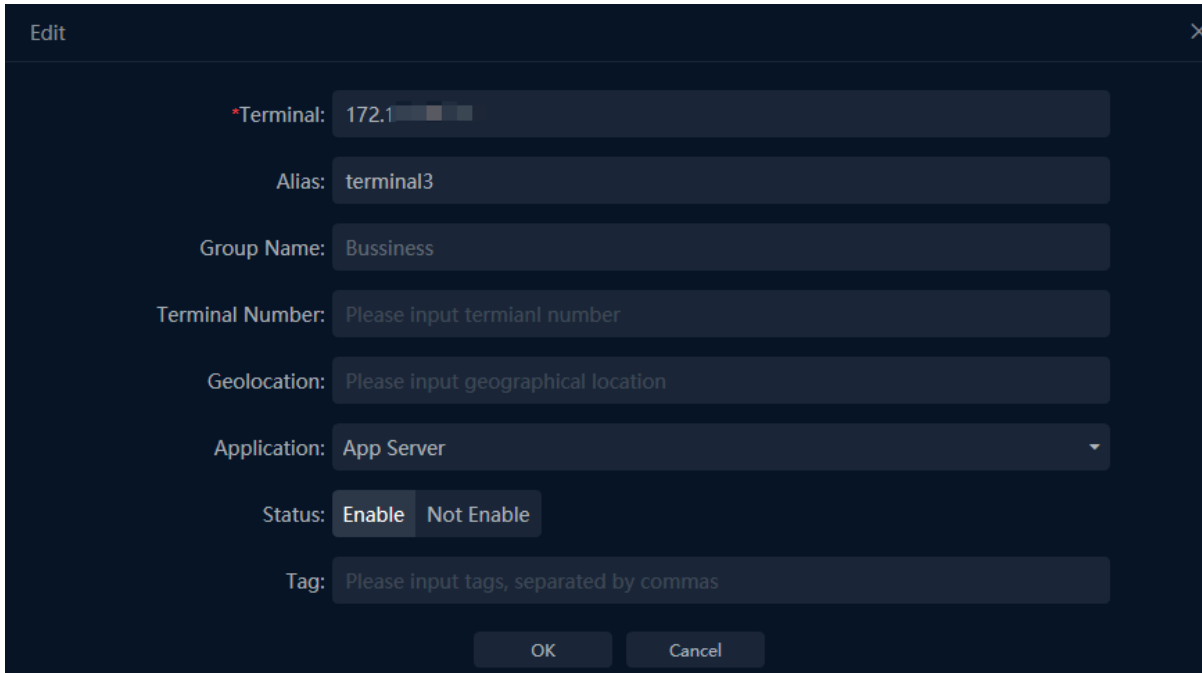
- Application(Probes): Only applications that bind to transaction groups within permissions are shown.
- Group Level: The purpose to define group level is to clear group level meaning. In terminal configuration, terminal monitor group component and alarm configuration, the group names can be displayed directly, which will be very convenient.
- Complete the Group Configuration

- Group Level: The drop-down option shows the six levels groups with their names.
- Geographical Position: It corresponds to the location information on the map.
- Longitude/Latitude: The longitude and latitude of the group on the map.

### 13.1.2. Add Terminal



To add a terminal, there are two modes: manually add and import a template.

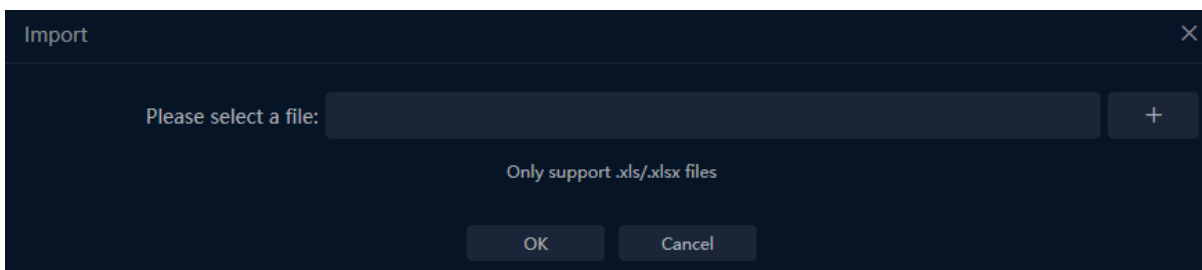
To manually add a terminal, click the button “” to open the adding box, as the screenshot below:



- Terminal: The Client IP which accesses the application,
- Terminal Number: The number of terminal. It's optional.
- Geolocation: Description of the terminal geolocation. It's optional.
- Tag: Keyword of terminal description. It's optional.

### 13.1.3. Import/Export

Click “” and “” to import and export the terminal configuration.



- Groups and terminals can be imported separately.
- Import rules:
  - Groups: Take the selected group in the left tree as the benchmark. When the imported group level is higher or the same as the selected group, the system will look up the higher level group successively and after that, create the new imported group under the high level group. When the imported group level is lower than the selected group, the new imported group will be created under the selected group.
  - Terminal: By default, the imported terminal information belongs to group in the imported template. When there is no group of the template, the terminal information belongs to the selected group.
- Only group and terminal information under selected group can be exported.

## 13.2. Terminal Monitoring

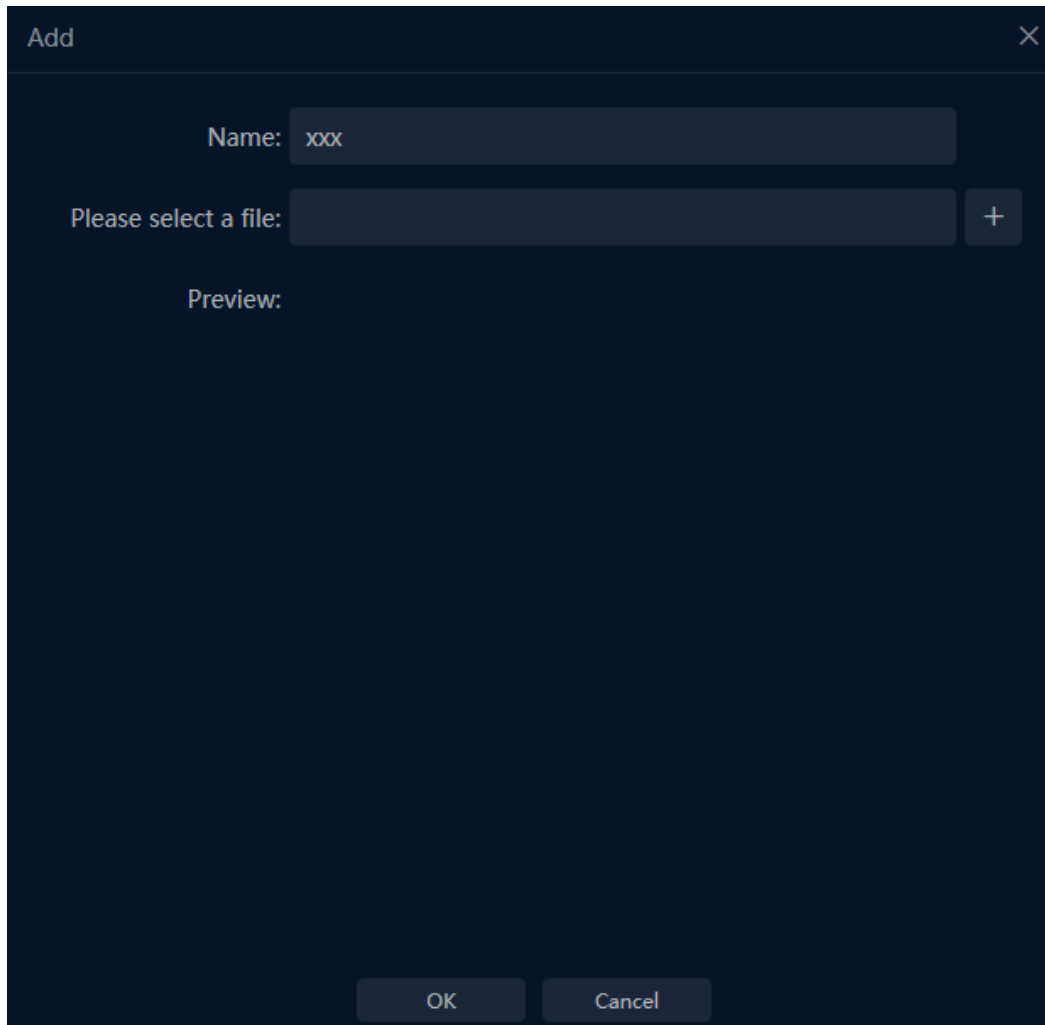
Terminal Monitoring displays the recovery status of each system's businesses of each terminal group, and distinguishes the recovered and unrecovered state by color. It can display the recovery time, the number of recovered nodes, the number of unrecovered nodes, etc.

In Terminal Monitoring, users can create a monitoring view, define the name of the view, and display the recovery status according needs and view the business recovery status by configuring the criteria for successful business recovery.

Click the menu Terminal Monitoring to go to the terminal monitor interface.

### 13.2.1. Create Monitor Views

Before the configuration of a scene chart, it's required to import map files in .json format. Go to menu Configurations -> Map Configuration. Click “+” to add map files.



After configuration of maps, follow below steps to configure a scene chart.

Click “+” to add a view.

- Complete the basic information. Then click “Save and Configure Path”.

**Add View** [Close]

Name:

Description:

View Permissions: **Private** Public User Group

Default Display:

[Save and Configure Path] [Cancel]

- Configure basic information.

**Add Scene Chart - Core Component - Terminal Monitor** [Close]

1 **Basic Information** 2 Transaction Verification Group 3 Participating Network 4 Map Configuration

Terminal Group:

Drill Start Time:

Monitor Frequency:

[Next] [Cancel]

- Add transaction groups and set transaction count.

**Add Scene Chart - Core Component - Terminal Monitor** [Close]

1 ✓ **Transaction Verification Group** 2 3 Participating Network 4 Map Configuration

Input Keyword to Search

✓	Action	Transaction Verification Group	Transaction Count	Transaction Verification Group
✓		group 2	11	A
✓		group 1	11	A

Current page 1, total 1 page(s), total 2 record(s). Show for every page: 10 record(s) [Page Navigation]

Add

Transaction Verification Group:

Action	Transaction Verification Group	Transaction Name	Transaction Count
<input type="button" value="🗑"/>	A	web4	<input type="text" value="10"/>
<input type="button" value="🗑"/>	A	WEB3	<input type="text" value="1"/>

Current page 1, total 1 page(s), total 2 record(s). Show for every page:  record(s)



- Select terminal groups.

Add Scene Chart - Core Component - Terminal Monitor

Progress: 1. Basic Information (✓) 2. Transaction Verification Group (✓) 3. Participating Network (3) 4. Map Configuration (4)

Action	Root Network	Network	Network Number	Terminal IP	Transaction Verification Group
<input checked="" type="checkbox"/>	Bussiness	Branches1		All	group 2

Current page 1, total 1 page(s), total 1 record(s). Show for every page: 10 record(s)

Buttons: Back, Next, Cancel

Add

Transaction Verification Group: group 2

Select Model: **Multi-Select Group** Single-Select Group

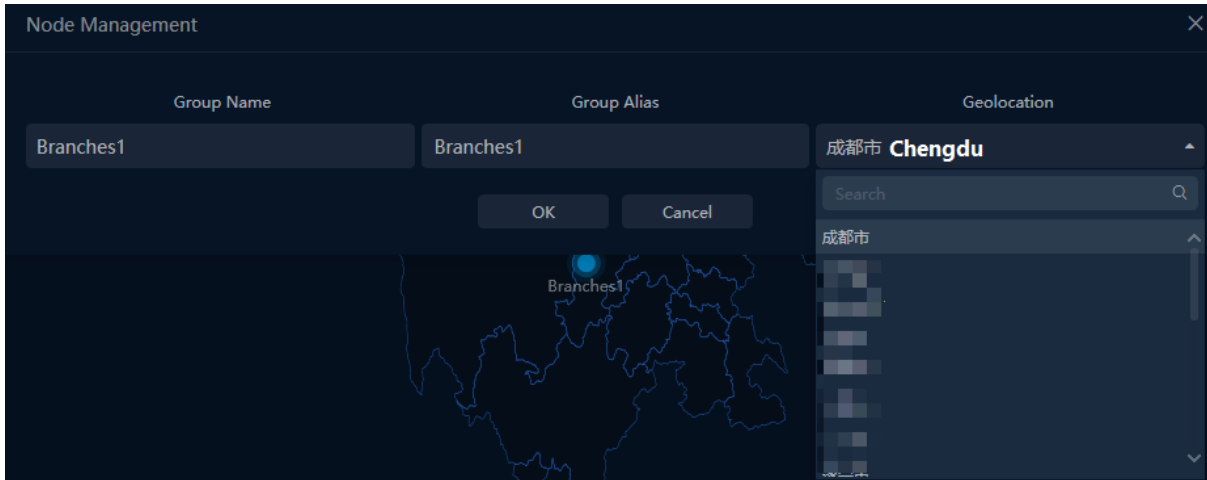
Group Level: Branches Please Input Keywords

- Bussiness
  - Branches1

Buttons: OK, Add and Continue, Cancel

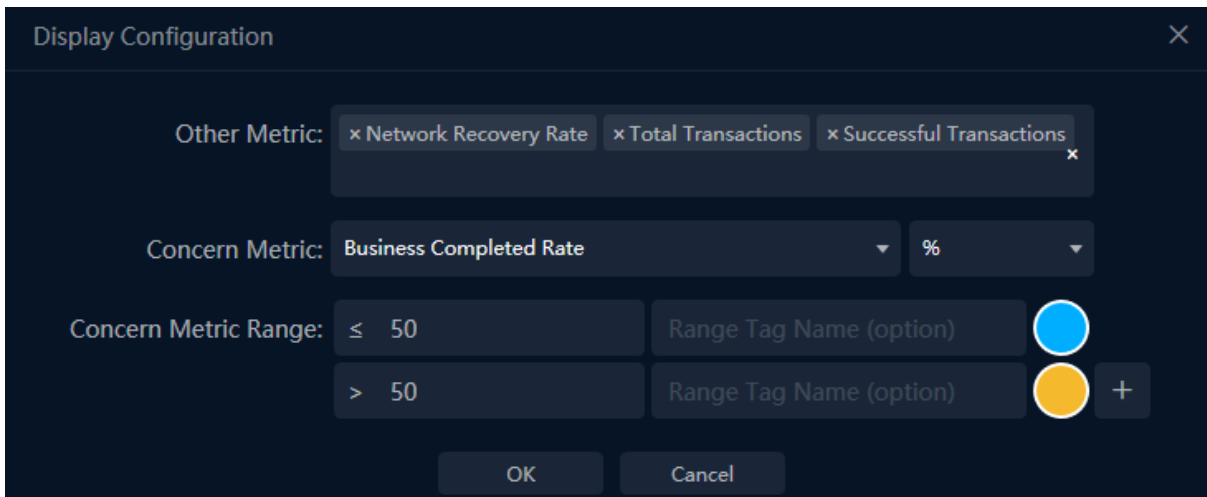
Both Multi-Select Group and Single-Select Group are supported.

Users can manage nodes manually. Take Chengdu for an example, click “**Node Management**” and map the node with Chengdu.



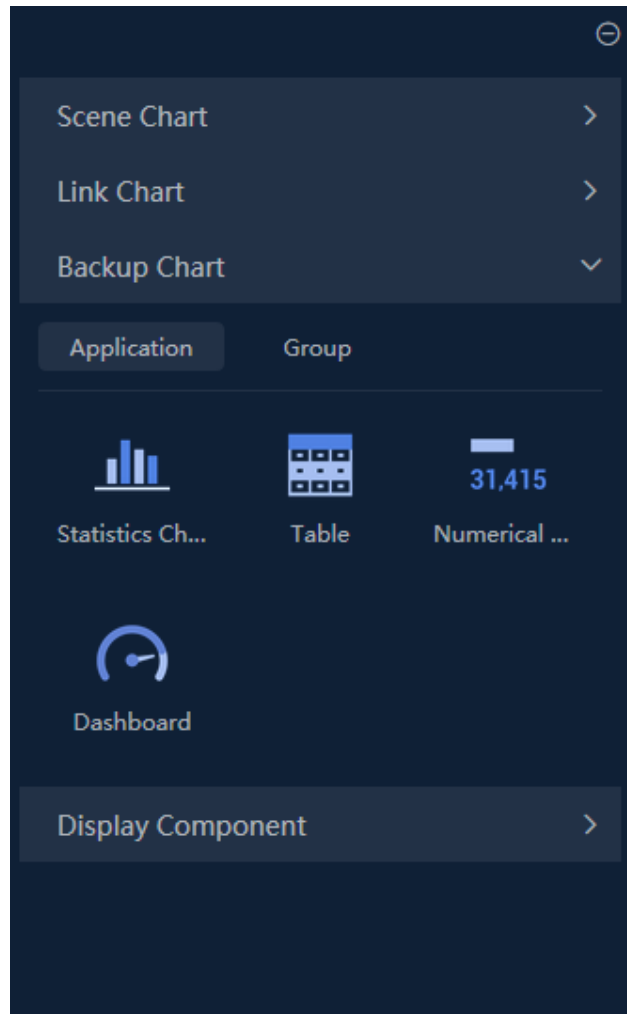
Also, the nodes can be automatically located in the right geolocation in the map if the geolocation names in terminal configuration match the location parameters in map files.

Then, click “**Show Configuration**” to complete the metric configuration.



Click OK to complete the configuration.

Also, there are some other metric components for users to monitor. Click “>” to open the component list on the left side of the page, as shown below:



## 13.2.2. Metric Description

- Group Metric
  - Business Completed Rate: Proportion of the number of completed businesses to the number of predefined businesses.  
Eg: The transaction group has four transaction names: A, B, C, D and E. Each transaction name has A predefined number of 2 transactions. When A completes 1 transaction, the completion rate is 10% and the number of completed trades is 1. When A completes 2 or more than 2 transactions (4), the completion rate is 20% and the number of completed transactions is 2. When A completes 2 or more transactions and B completes 4 transactions, the completion rate is 40% and the number of transactions completed is 4.
  - Network Recovery Rate: The proportion of the number of recovered terminals to the number of total terminals.
  - Drill Completion Time: Elapsed time from the beginning of the drill until the business completion rate =100%.
  - Predefined Transactions: Total predefined transaction count.
  - Completed Transactions: Total completed transaction count.

- Uncompleted Transactions: Total uncompleted transaction count.
  - Total Transactions: Total transaction count.
  - No-Response Transactions: Total no-response transaction count.
  - Transaction Response Count: Total responsive transaction count.
  - Successful Transactions: Total successful transaction count.
  - Failed Transactions: Total failed transaction count.
- Application Metric
    - Business Recover Rate: Proportion of the number of business types completed to the number of participating business types.  
Eg: For ATM, the participating types include A, B, C, D, E, 5 types. When the number of A is greater than 1 and the numbers of others are 0, the completion rate of ATM channel is 20%.
    - Predefined Transactions: Total predefined transaction count.
    - Total Transactions: Total transaction count.
    - No-Response Transactions: Total no-response transaction count.
    - Transaction Response Count: Total responsive transaction count.
    - Successful Transactions: Total successful transaction count.
    - Failed Transactions: Total failed transaction count.

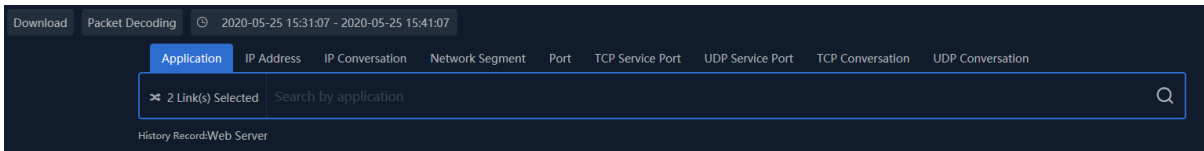
## 14. Search and Download


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.

### 14.1. Search Packets


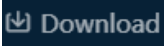
Search Packets allows user to use the application, IP address, IP session, network segment, port, TCP service port, UDP service port, TCP session, and UDP session as the entry, to search and download the packet.

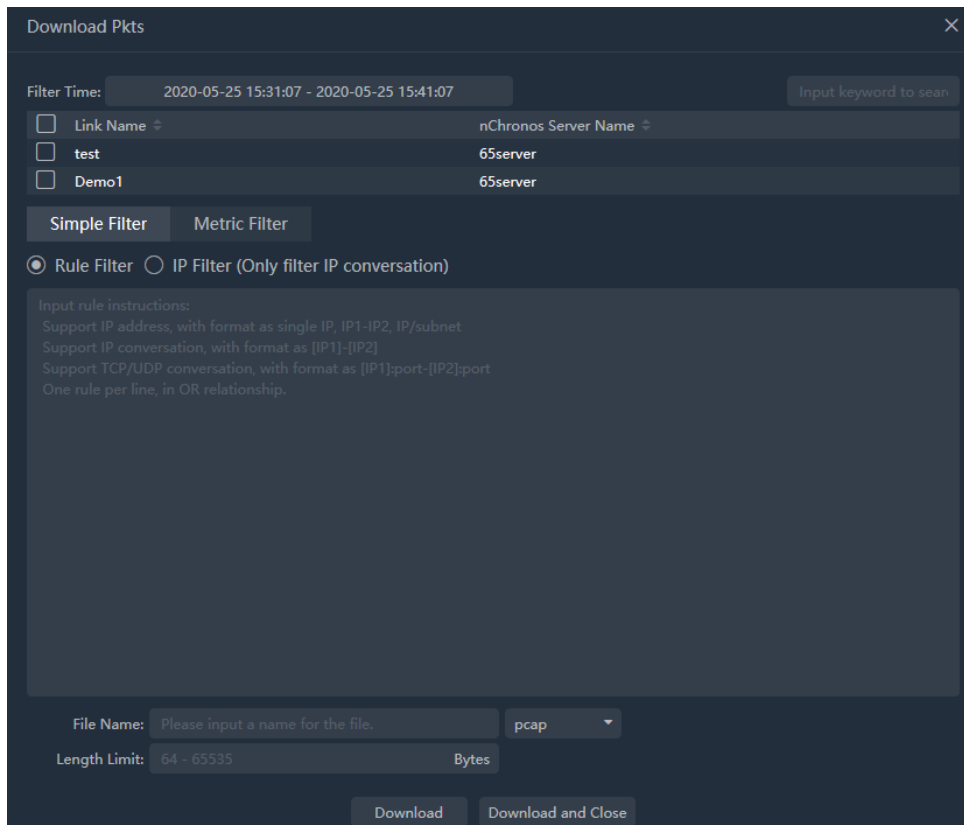
Click the menu Search to open the Search Packets page, as the screenshot below:



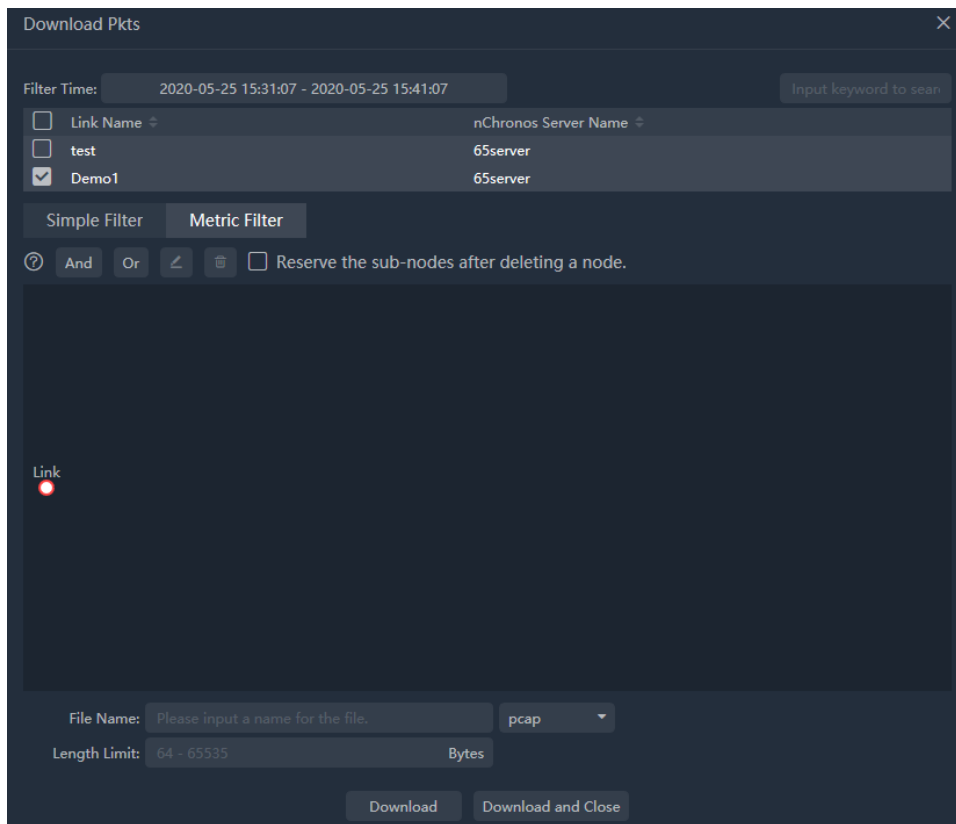
Enter the keywords for search and then click the button “”, the system will automatically search the communication data that matches the keyword.

### 14.2. Download Packets

Support simple filter and advanced filter. Users can click the button “” or “” to open the Download Packets box. Simple filter is shown below:



Metric filter supports filtering downloads for applications, sessions, intersegments, IP addresses, ports, segments, protocols, and virtual network identifiers, which is shown below:




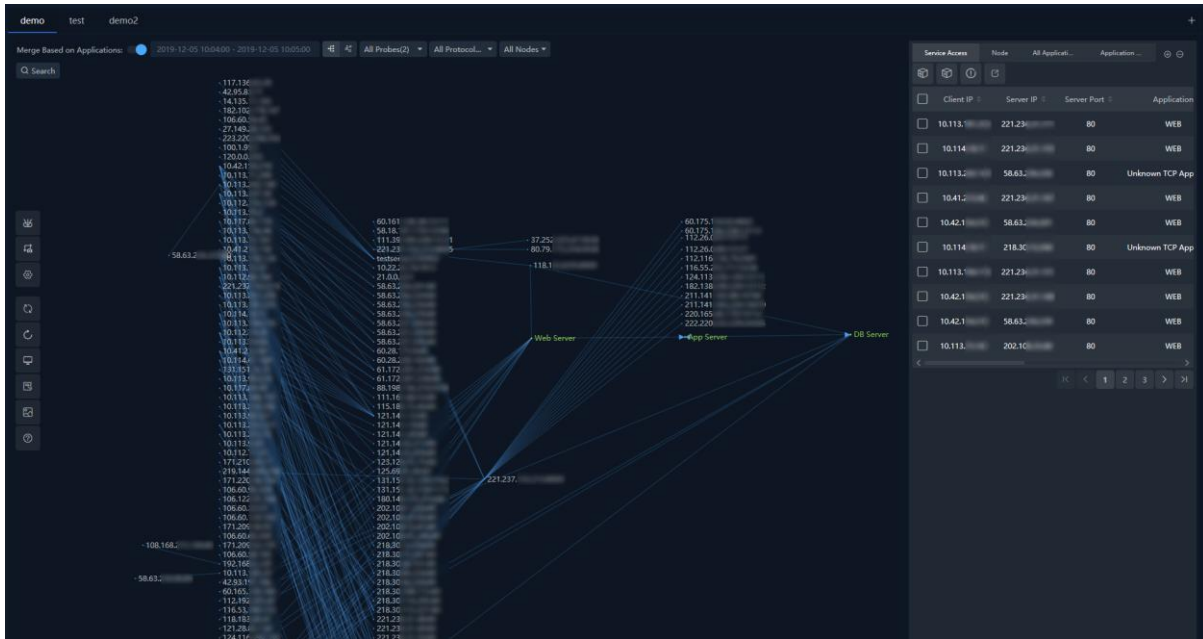
## 14.3. In-depth Analysis

Click the button “” to open the nChronos console to do in-depth analysis

## 14.4. Discover

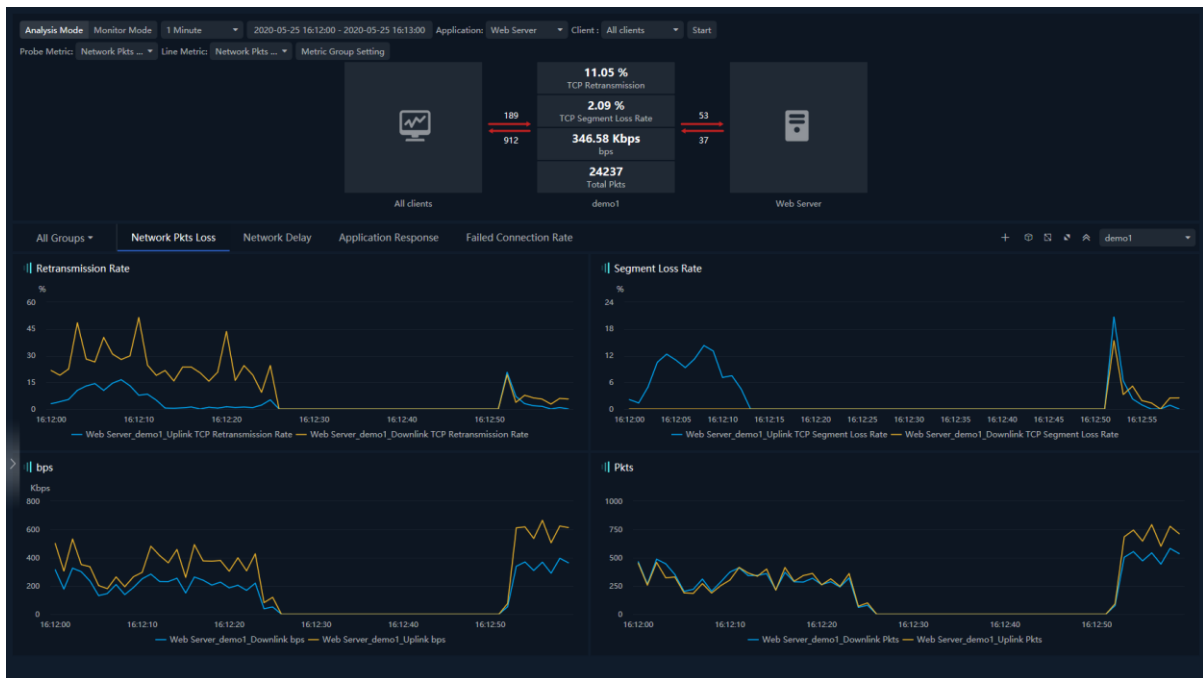
Users can discover the relationships between the IP addresses of searched objects.

Click the button “” to open the Discover page, as the screenshot below:




## 14.5. Multi-segment Analysis

When "merge by application" is not enabled, multi-segment analysis function is supported between IP relationships. Right-click a line and then click Multi-Segment Analysis to open the Multi-Segment Analysis page, as the screenshot below:



## 14.6. Trend Analysis

Users can click the button “” to do trend analysis, the page is shown below:





## 15. Packet Signature Query

UPM provides packet signature query feature. Users can create query tasks to query the source IP, destination IP, source port, destination port, source location, destination location, etc. related the signature rules.

Click Retrieve -> Signature Query to go to the signature query page.

Action	Query Task Name	Signature Alarms	Query Process	Query Status	Query to Time Point	Query Time Range	Link	Query Link	Created
<input type="checkbox"/>	test11	307378	100%	Finished	2020-10-23 00:10:00	2020-10-22 00:00:00 - 2020-10-23 00:10:00	Demo	ret5f928f8dc1e65a22ed23c4cd	taylo
<input type="checkbox"/>	test3	265193	100%	Finished	2020-10-19 00:00:00	2020-10-18 00:00:00 - 2020-10-19 00:00:00	Demo	ret5f8d4328c1e65a22edaaa104	taylo
<input type="checkbox"/>	test1	0	0%	Error		2020-10-18 00:00:00 - 2020-10-19 00:00:00	Demo	ret5f8d3a33c1e65a599f69ae5f	taylo

### 15.1. Add Query Task

Click the button “+” to add a new query task.

- Complete the information.

**Add**

Name: test5

Time Range: 2020-10-28 13:30:00 - 2020-10-28 14:30:00

Query Link: Demo x

Filter Condition: +

Packet Signature: Basic Signature | Signature Expression

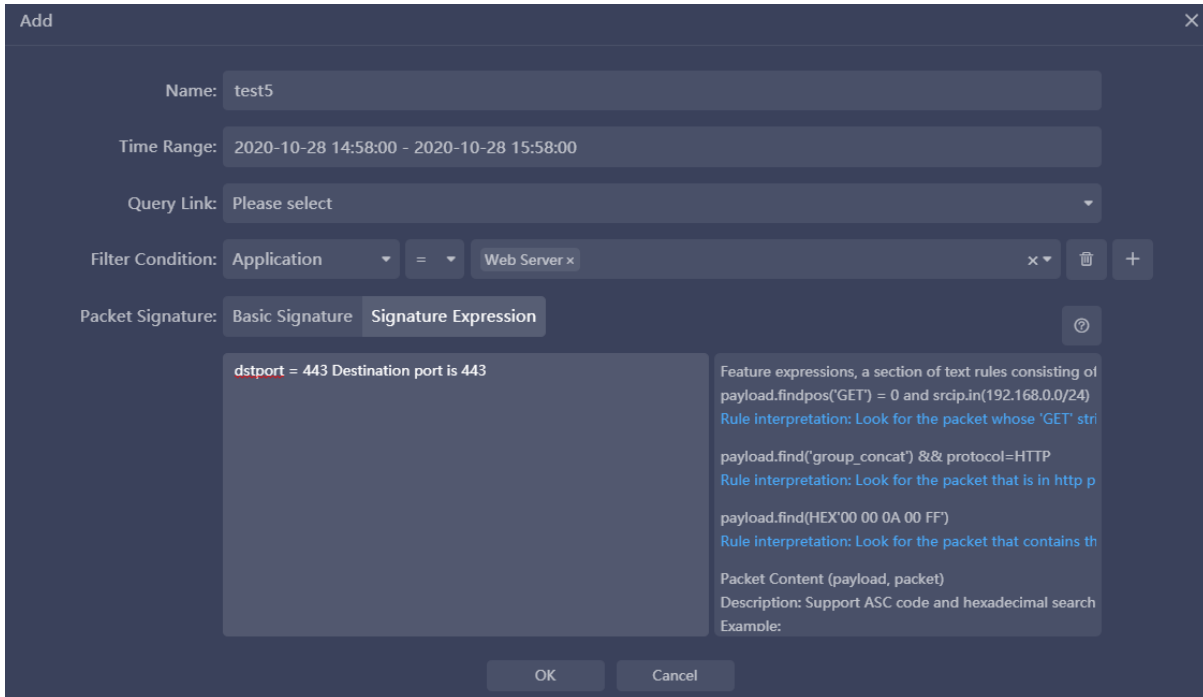
Content:  ASCII  HEX

123


OK Cancel

- Name: The name of the query task.
- Time Range: Users can query the tasks of in the specified time range.
- Query Link: Specify the link queries from. Support multiple links.
- Filter Condition: Support application, segment, IP, port and protocol.
- Packet Signature: The signature users need to query. Support basic signature

settings and signature expression. Users can click the button “?” to refer to user guide document. One signature per row, and they are in OR relation.



## 15.2. Check Query Result

After successful creation of a task, users can check query results during or after the query by clicking button “”.

Action	Signature Start Time	Trigger Condition	Src. IP	Src. IP Location	Src. Port	Dest. IP	Dest. IP Address Location	Dest. Port
<input type="checkbox"/>	2020-10-28 15:05:30	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:05:30	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:13:54	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:13:54	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:22:20	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:22:20	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:30:46	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:30:46	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:39:11	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686
<input type="checkbox"/>	2020-10-28 15:39:11	payload.find("123")	61.135.192.10	China Beijing	80	221.237.192.10	Beijing	49686

Current page 1, total 36 page(s), total 355 record(s). Show for every page: 10 record(s)

The query task supports stop, re-query, and delete operations


## 16. Log Analysis

UPM provides log analysis function for analyzing specified information in history logs.

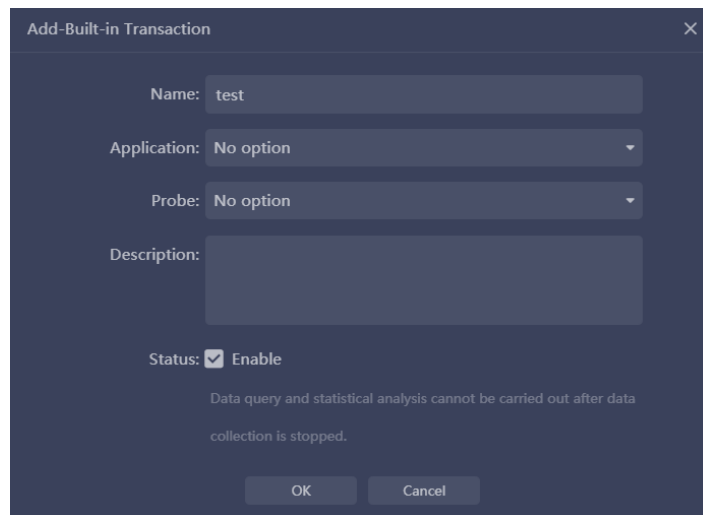
### 16.1. Log Analysis Configuration

#### 16.1.1. Log Collection Configuration

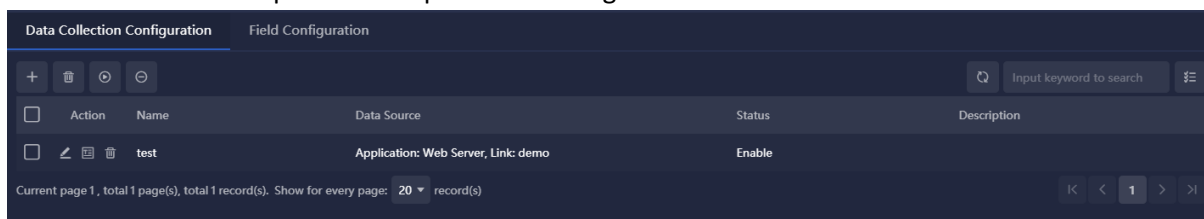
Click Configuration -> Log Analysis Configuration -> Log Analysis Collection Configuration to go to the log analysis collection configuration page.



Click button “” to add a new log collection item.

- Complete the information:

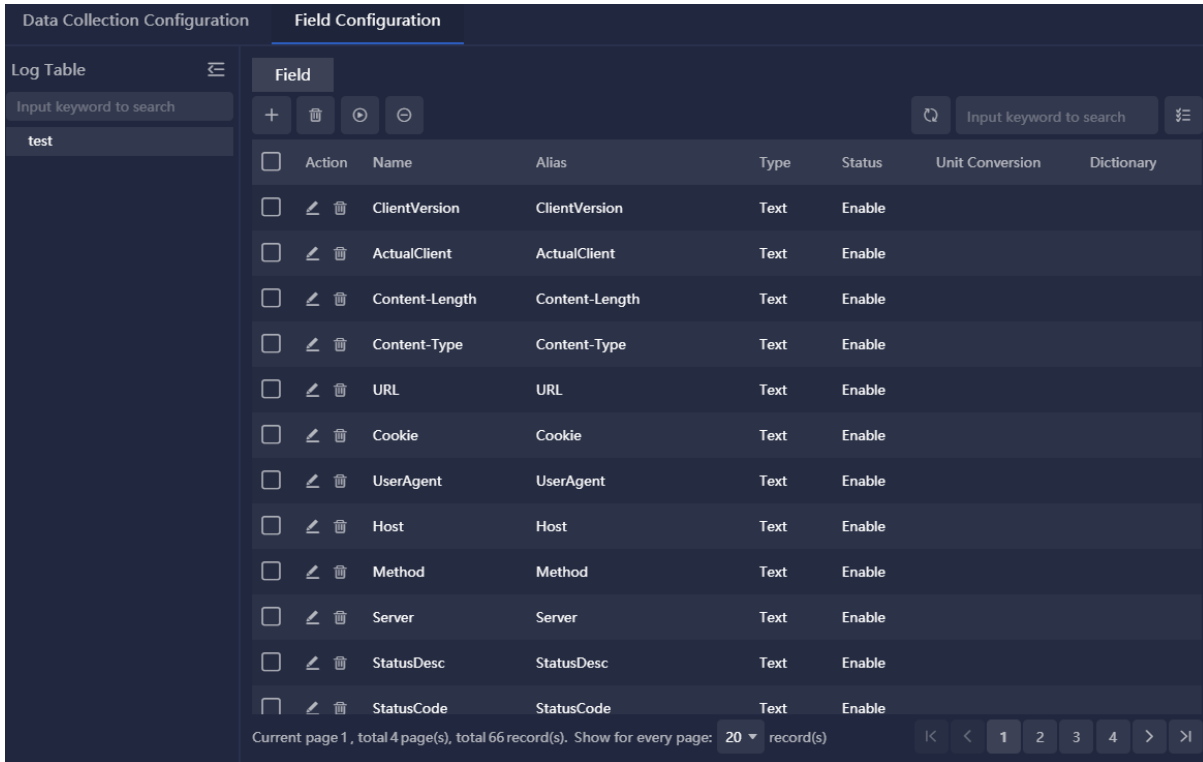


- Name: The name of the transaction log collection item.
- Application: Specify the application for collecting transaction log.
- Probe: Specify the link for collecting transaction log.
- Description: Description for the log collection item.




Action	Name	Data Source	Status	Description
 	test	Application: Web Server, Link: demo	Enable	

The built-in fields are all enable by default. Users also can custom fields.



### 16.1.2. Log Analysis Scene Configuration

This function only supports the configuration of account association scene.

Click button “” -> PPPoE Account Analysis Scene to add an analysis scene.

- Complete the information:

**Add-Analysis Scene**

Name:

Collect Log:

Account Correlated:

Field:

IP Correlated Field:

Analysis Link:

Note:

OK Cancel


- Name: The name of the analysis scene.

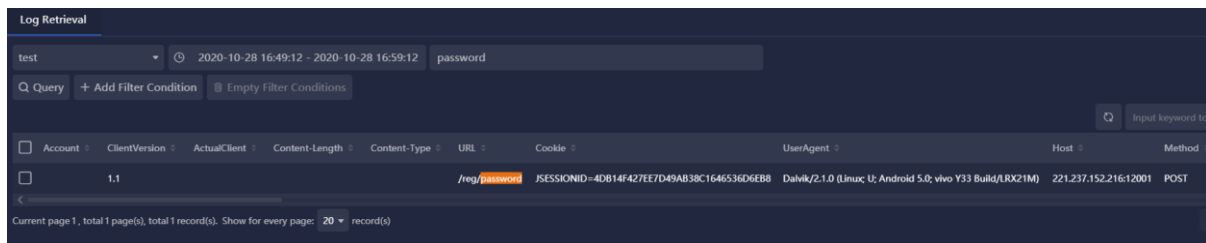
- Collect Log: Specify the log for the scene.
- Account Correlated Field: The field of account that need to be correlated with the IP field.
- IP Correlated Field: The field of IP that need to be correlated with the account field.
- Analysis Link: Specify the link for the scene.
- Note: Note for the scene.

## 16.2. Log Retrieval


In log retrieval function, users can search specified keywords in logs.

Click Log Analysis -> Log Retrieval to go to the log retrieval page.

Select a log, set the time range, input the keyword and click button “” to begin the retrieval.



Support full field retrieval and support any keyword, wildcard, field, etc.

Users can click button “” to export the retrieval result as a file in .csv format.

## 17. System Management

### 17.1. 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.

### 17.2. User Account

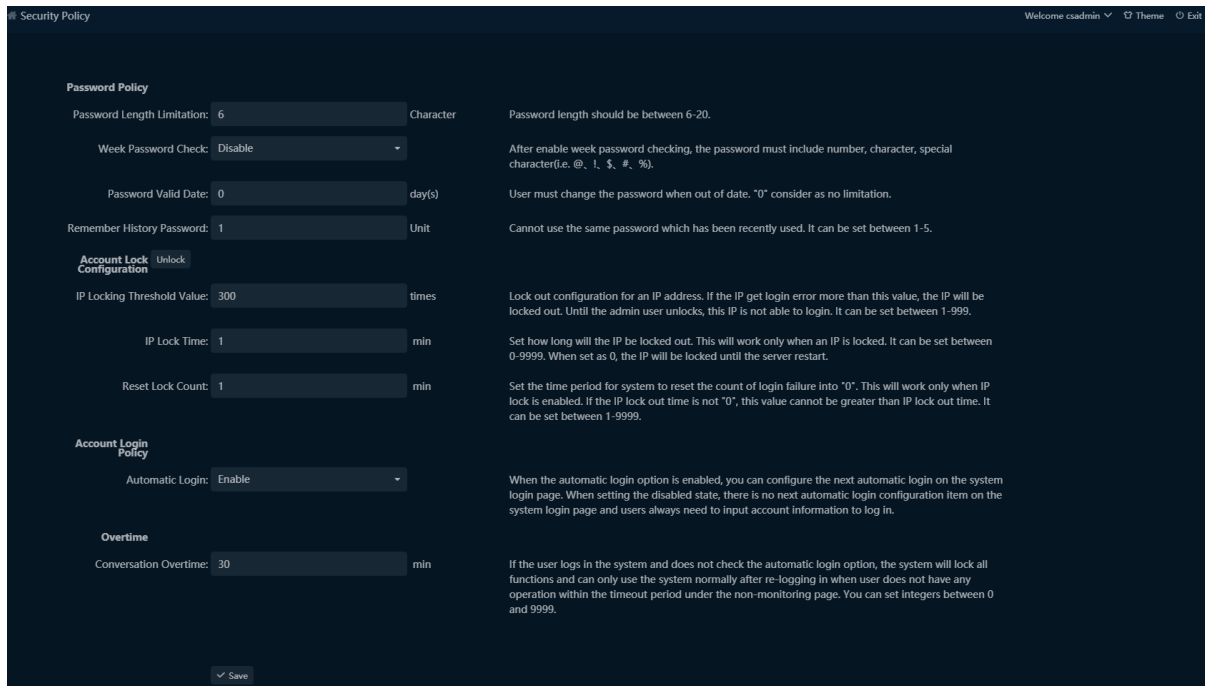
User management includes two tabs, user management and authentication configuration. User management carries out unified maintenance for system users. In Authentication configuration, users can configure Radius and LDAP server information.

- 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.

### 17.3. Security Policy

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

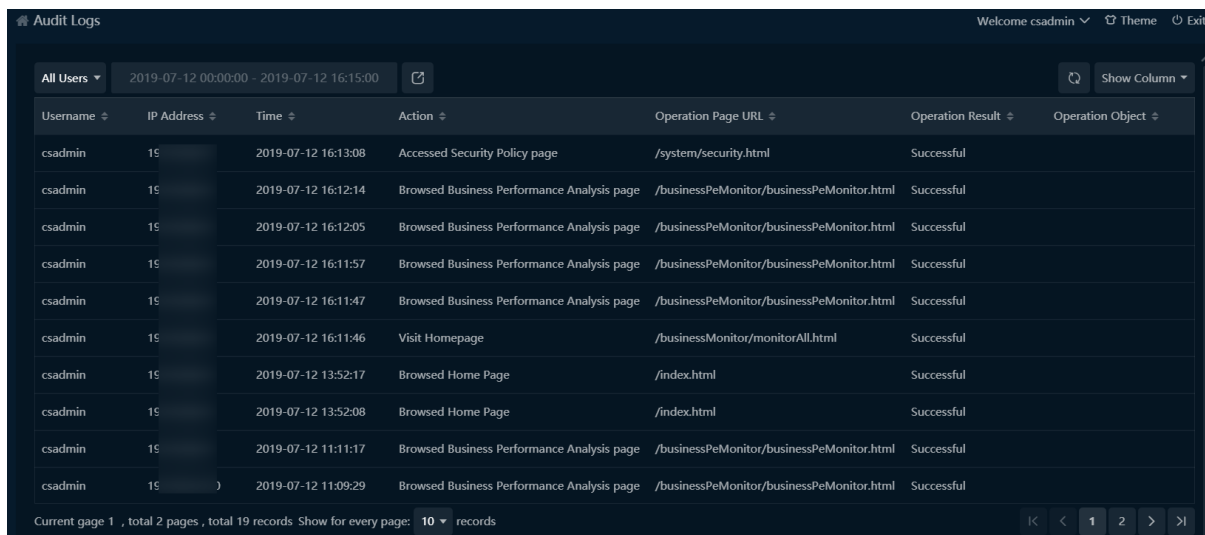
The security policy page is used to configure the password policy, account lock policy (including account unlock) and overtime policy.



## 17.4. 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.

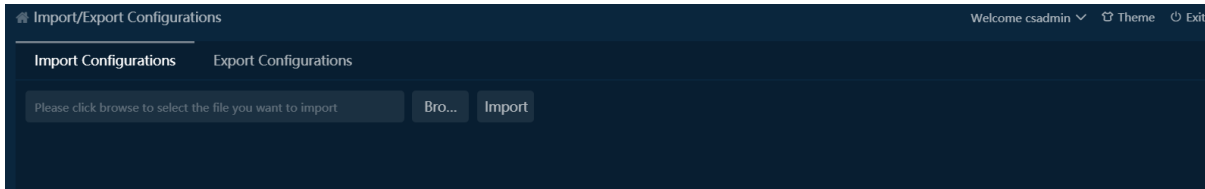
## 17.5. Import/Export Configurations

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.

## 17.5.1. Import Configurations

The Import Configurations page shows as the screenshot below:



To import configurations:

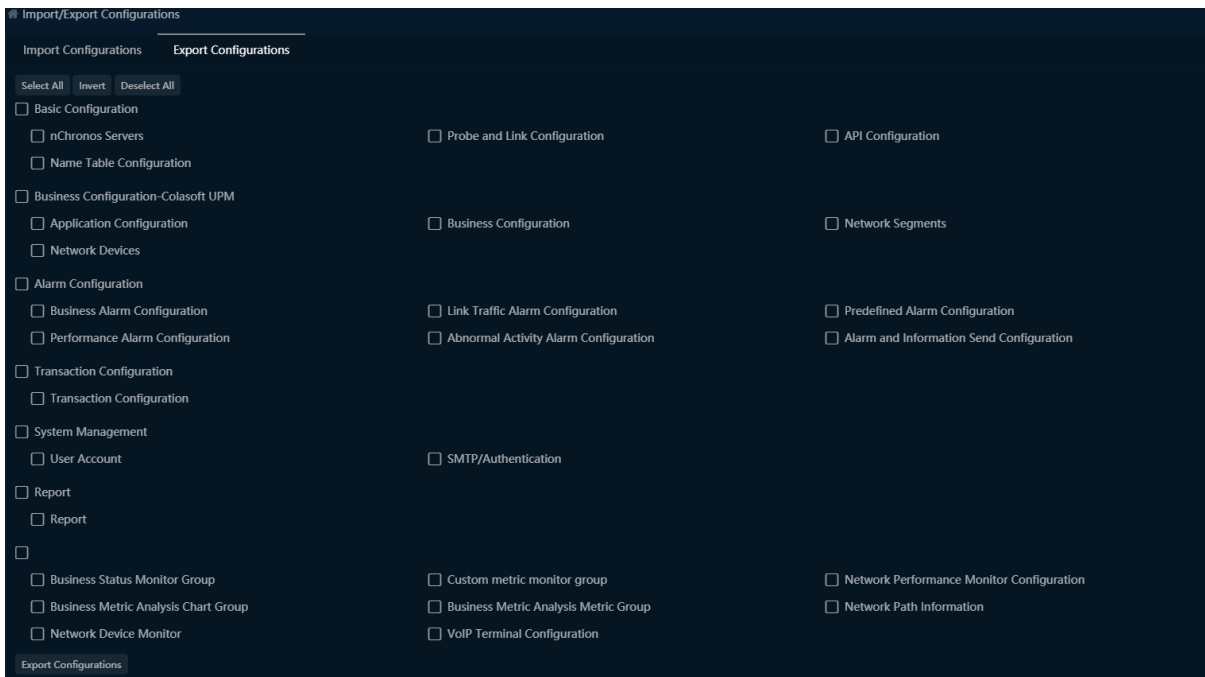
1. Select the file to be imported. For Google Chrome, users can drag the file to the box.
2. Click Start Uploading to upload it.
3. When the configurations conflict, users can choose to skip, overlap or cancel the import.

### Note

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

## 17.5.2. 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).



## 17.6. 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.

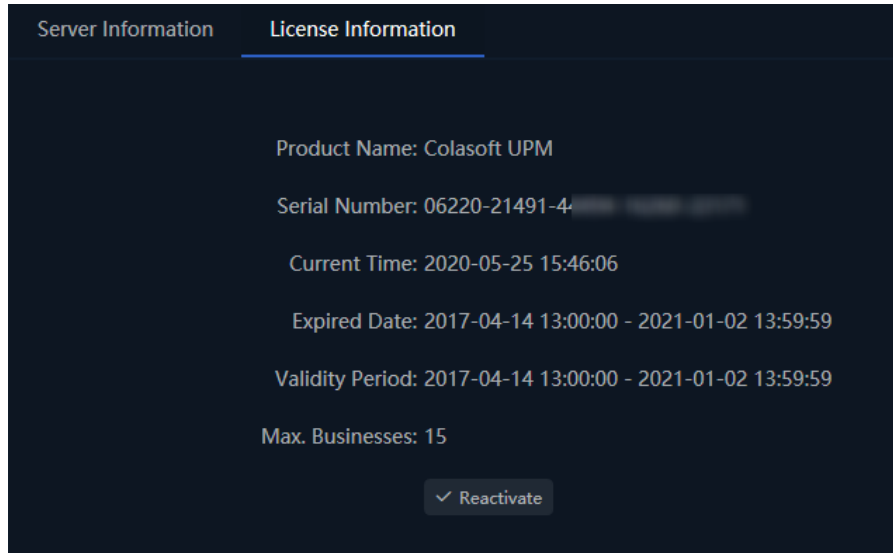
### 17.6.1. Server Information

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

Server Information	License Information
OS Name: Linux	
OS Architecture: amd64	
OS Version: 2.6.32-504.el6.x86_64	
Total Memory (JVM): 8.76GB	
Available Memory (JVM): 3.03GB	
Maximum Available Memory (JVM): 8.76GB	
Total Memory (physical memory): 15.41GB	
Available Memory (physical memory): 156.22MB	
Java Version: 1.8.0_191	
MongoDB Version: 3.2.0	
Current Time: 2020-05-25 15:46:06	
Boot Time: 2020-05-13 17:36:25	
Monitor Port: 22000,22100	

## 17.6.2. 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.

## 17.7. Replace Certificate

Users can update digital certificates and socket certificates.

## 18. Network Topology monitoring

The main features of network topology monitoring are as follows:

- View configuration

Establish a network topology diagram based on the actual network environment, and configure network nodes, links, indicators, and alarms.

- View group

When the network structure is complex and cannot be displayed in one view, you can draw multiple views. Views are divided into different view groups based on regions and groups.

- Template

Reuse topology to reduce user configuration workload.

- Monitoring and analysis mode

Monitors the latest network status in real time and supports retrospective analysis in a customized historical time.

### 18.1. View settings

Click on the menu "Network Performance" -> Network Topology Monitoring, access the network Topology Monitoring page.

Click " " to add a view, as shown below:

Add View
✕

Name:

Description:

View Privilege: Private Public User Group

Clone View Configuration: None ▾

Label:

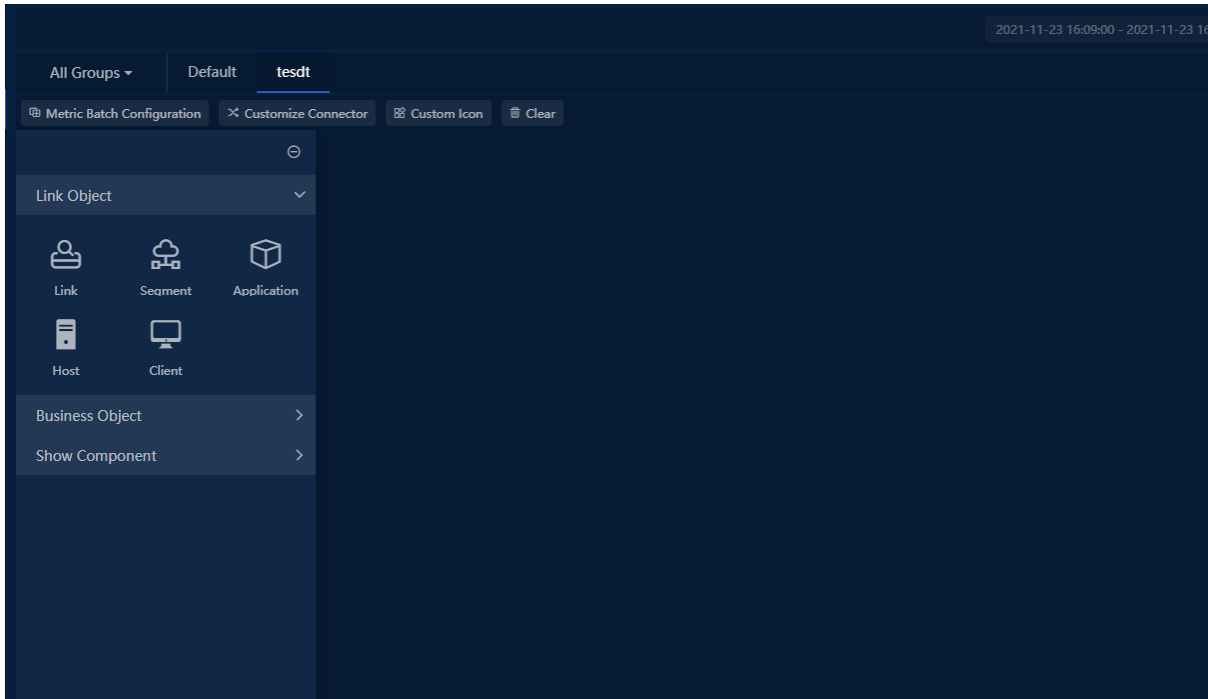
Default Display:

OK Cancel

Add view configuration:

Field Name	Description
Name	View name
Description	View description
View Privilege	Select one of Private, Public, User Group
Clone View Configuration	Clone the existing view configuration.
Label	The label is the horizontal menu bar - > Options in the view drop-down list.
Default Display	Access the network topology monitoring view displayed by default.

Click to enter editing mode, as shown below:



A view in Edit mode consists of the top operation bar, the left configuration panel, and the view display area.

- The top operation bar offers the following functions:
  - Metric Batch configuration
  - Customizes connector
  - Custom icon
  - Clear
  - Save
  - Cancel

- The left configuration panel provides the following configurable objects:
  - Link Object

Configure monitoring indicators based on links, network segments, applications, hosts, and clients.

- Business Object

Configure monitoring indicators for service, application, host, and client objects.

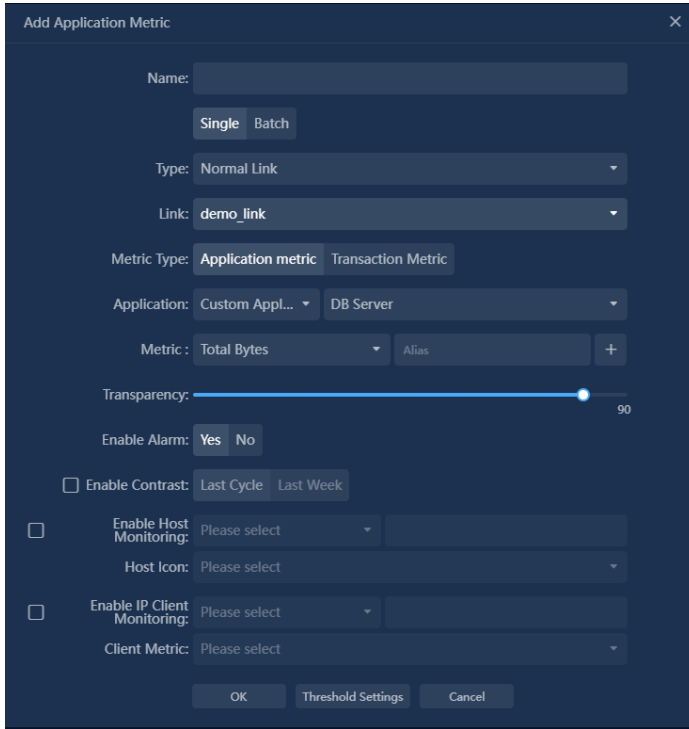
- Show Component

Configure rectangles, texts, pictures, and device ICONS.

**Note:** Select an object and drag it to the function pane. If you deselect an object, the object configuration window is displayed for you to configure.

## 18.1.1. Configuring Monitoring Indicators

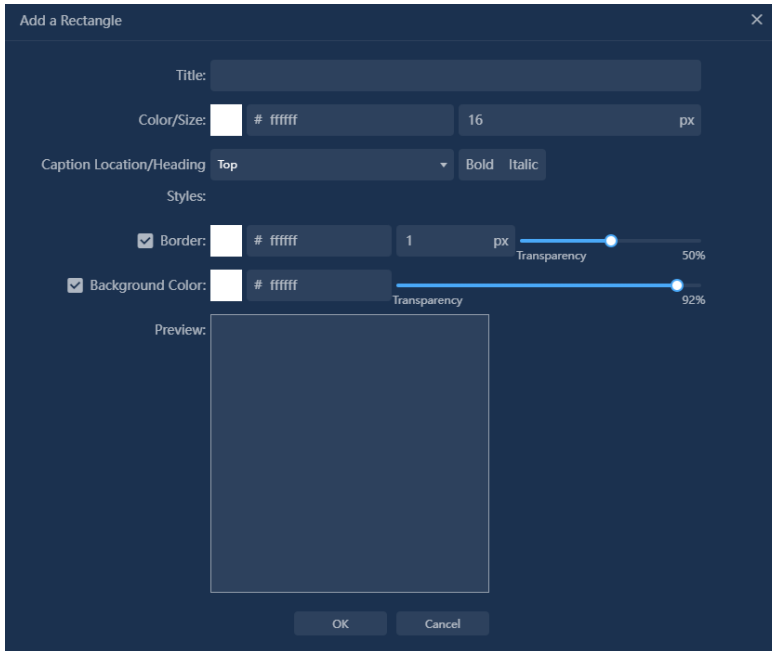
You can configure link object monitoring indicators and service object monitoring indicators, using link object -> application as an example, you can add in batches or in a single instance. The following figure shows the configuration for a single:



Field	Description
Name	Chart name
Add	Single or Batch
Type	Can select either a common link, an aggregate link, a sublink, a virtual interface sublink, a NetFlow sublink, or a MAC address sublink.
Link	Link options. Add Mode If single link is selected, the link options can be selected in one mode. Add Mode If batch is selected, you can select multiple links.
Metric Type	Choose Application Metric or Transaction Metric
Application	Customize application, system application, or single option
Metric	Maximum of 4 items can be configured
Transparency	Figure background Transparent background configuration.
Enable Alarm	The chart shows the alert number configuration, shown by default.
Enable Contrast	Indicators can be compared with the previous period or the last cycle. The comparison function is disabled by default.
Enable Host Monitoring	Supports application host monitoring. You can configure the host range and host monitoring indicators. After the configuration, click the chart to view the traffic status of the host. This function is disabled by default.
Enable IP Client Monitoring	Supports application host monitoring. You can configure the host range and host monitoring indicators. After the configuration, click the chart to view the traffic status of the host. This function is disabled by default.
Threshold Setting	Configures the display color of indicators in different value ranges.

## 18.1.2. Rectangle Setting

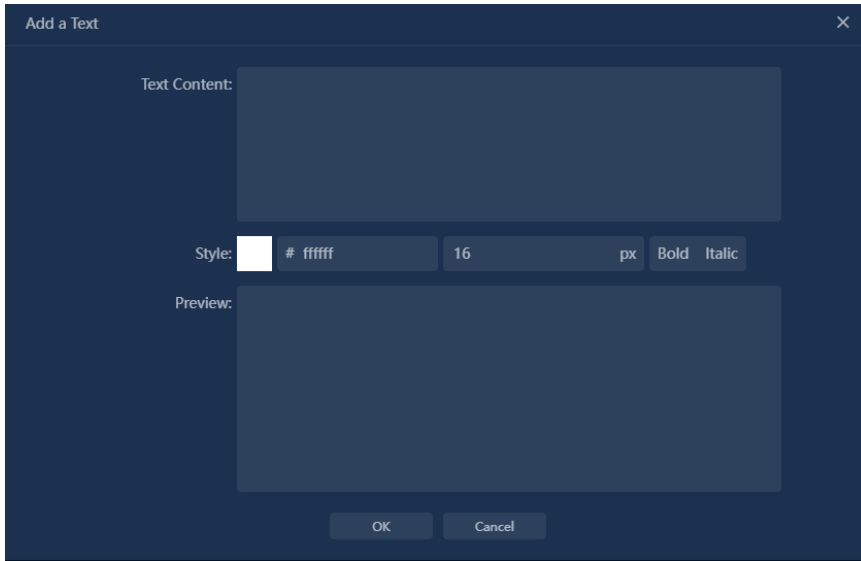
Show component -> Rectangle:



字段名称	描述
Title	Rectangle title
Color/Size	Title font color and size Settings
Caption Location/Heading	Title font color and size Settings
Border	Rectangle border display Settings, border style Settings
Background Color	Rectangle fill color with transparency Settings
Preview	Preview rectangles

## 18.1.3. Text setting

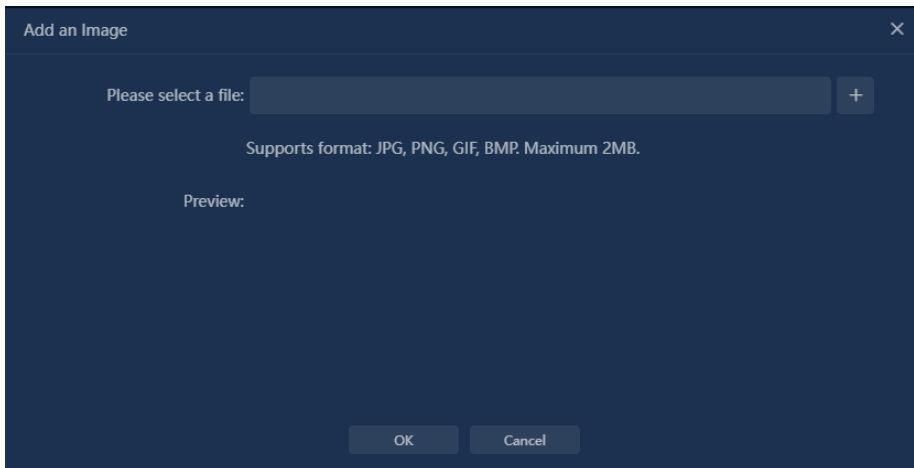
Show component-> Text



Field name	Description
Text Content	Text content
Style	Text color, size, bold italic style Settings.
Preview	Preview text renderings.

## 18.1.4. Image Setting

Show component-> Image

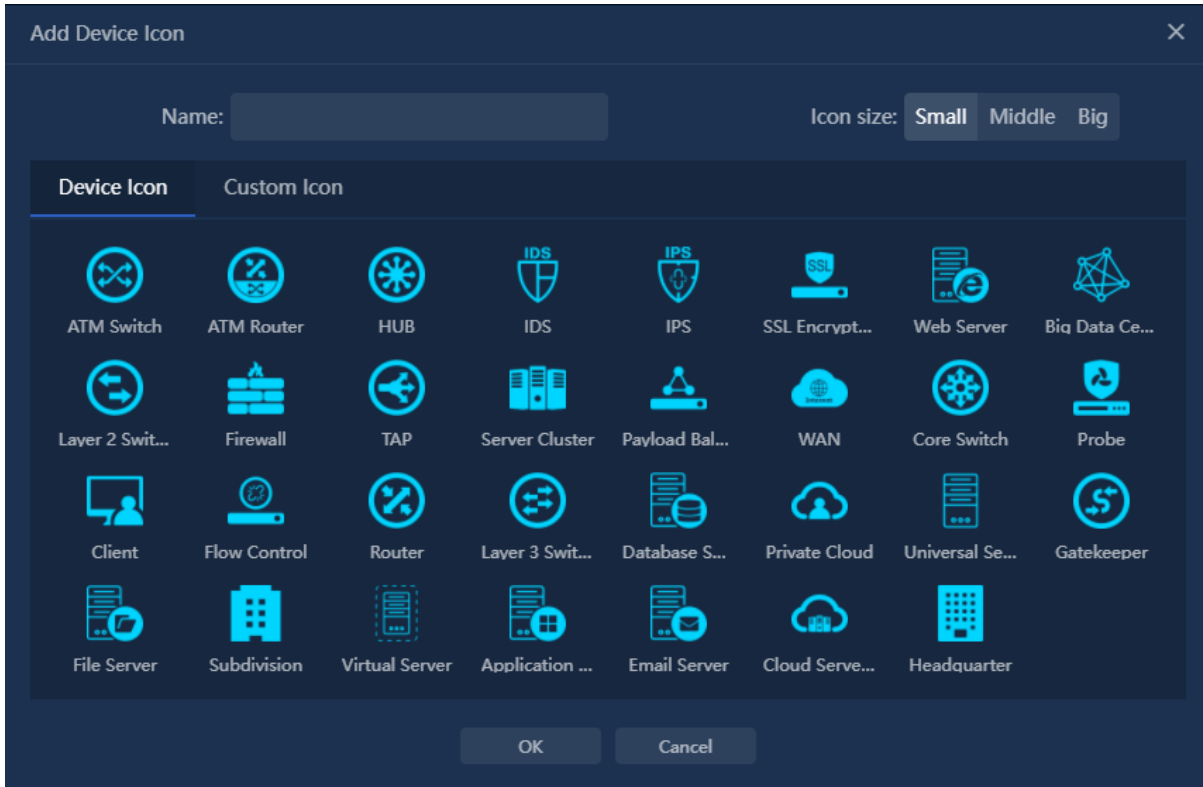


Field name	Description
Please select a file	Can upload image files in JPG, PNG, GIF, and BMP formats with a maximum of 2MB.
Preview	Preview the picture.

## 18.1.5. Device Icon

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





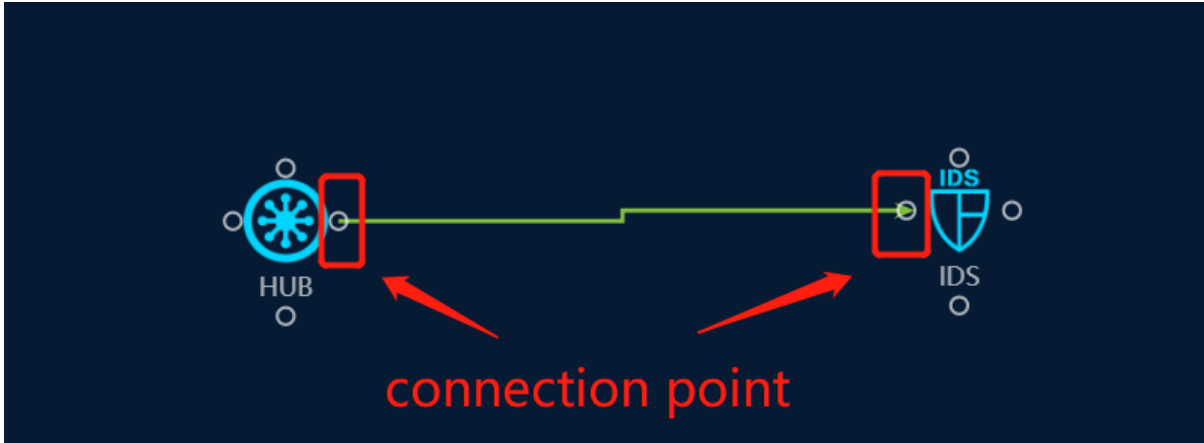
Field Name	Description
Name	This parameter is mandatory
Icon Size	Large: 80x80, medium: 60x60, small: 40x40 three icon sizes
Icon	Preview the picture

### 18.1.6. Connecting Cables for Icon

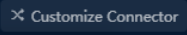
There are two configuration modes of connection: connection point connector and custom connection.


#### Connecting point

Click two connection points of the icons, the line would connect them automatically.



## Customize Connector

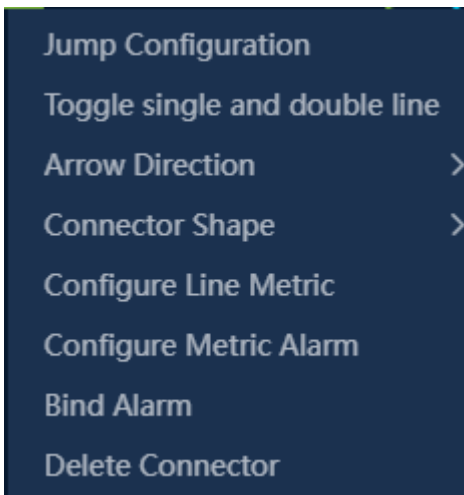
Click , the customize connection mode is displayed. Click with the left mouse to draw a broken path. Right-click to finish the current polyline drawing.

Click , quit the customize connection mode.

## Connection properties

Support for configuring wiring styles, wiring metrics, wiring alerts, and wiring interaction properties.

Right-click on the line to call out the menu.

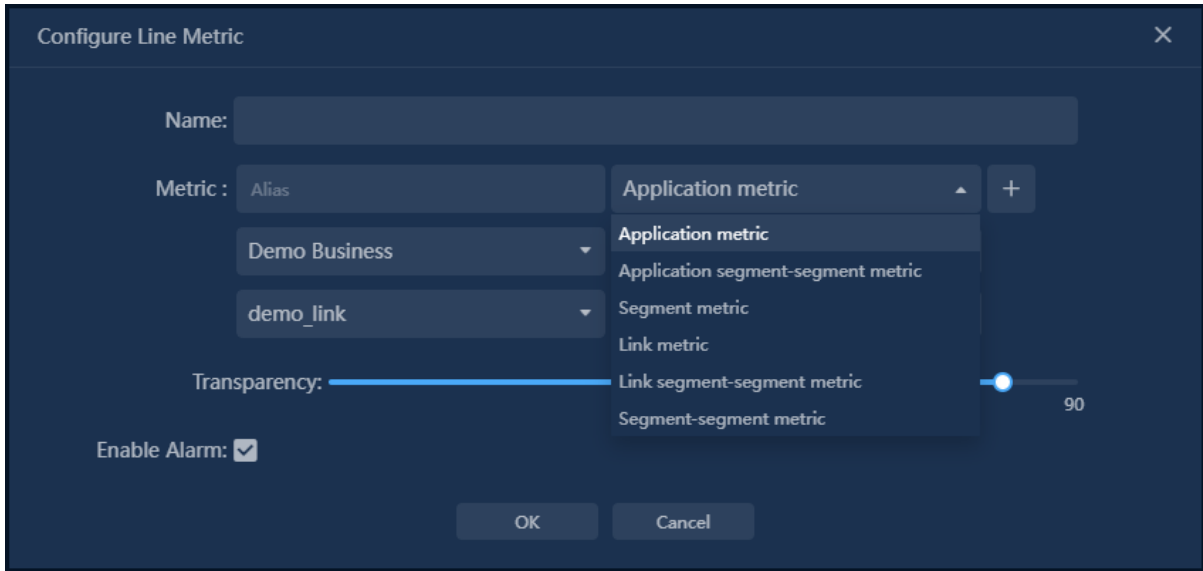


- Connection Style
  - Toggle single and double line
  - Arrow direction:
    - no arrow point-to-point
    - Start Point-to-End Double-Arrow
  - Connector Shape
  - Elbow straight curve

- Configure Line Metric

You can set application metric, application segment-segment metric, segment metric, link metric, link segment-segment metric, segment-segment metric. The inter-segment index value is the difference between two links.

A maximum of four indicators can be configured for one cable.



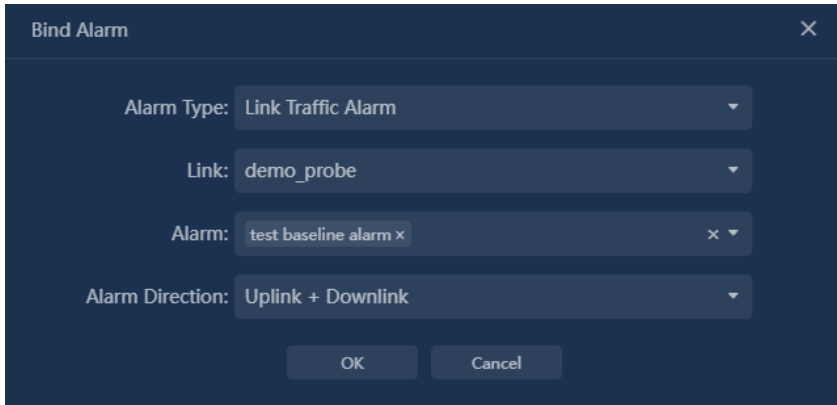
Field Name	Description
Name	Name
Metric	Support application metric, application segment-segment metric, segment metric, link metric, link segment-segment metric, segment-segment metric. The inter-segment index value is the mean value of the two links.
Transparency	Figure background Transparent background configuration.
Enable Alarm	The chart shows the alert number configuration, shown by default.

- Alarm
- Configure metric alert

Click Configure metric alert, a prompt dialog box will pop up. Click OK to jump to the network topology monitoring alarm configuration page.

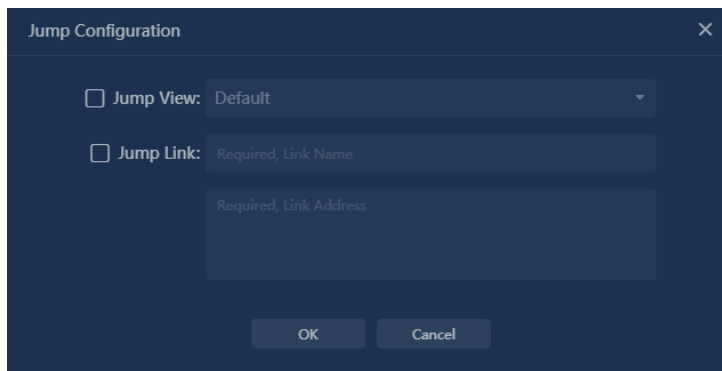
- Bind alarm

Supports binding link traffic alarm and service alarm.



Field Name	Description
Alarm type	Supports binding link traffic alarm and service alarm.
Link	Single choice
Alarm	Multi choice
Alarm direction	Uplink + Downlink, Uplink, Downlink

- Jump configuration



Field Name	Description
Jump View	Select the topology monitoring view.
Jump Link	Set the link name and link address.

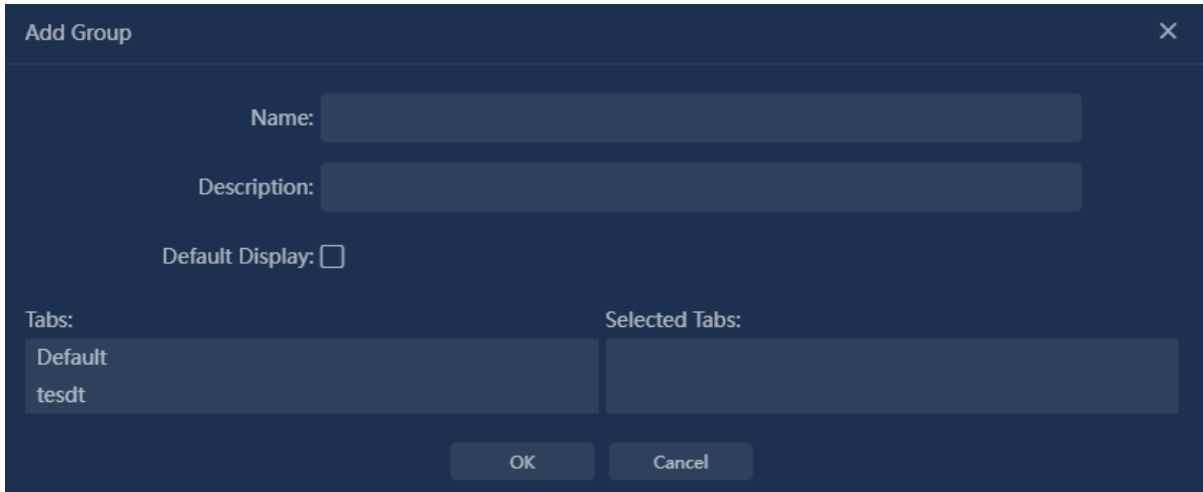
In monitoring mode, right-click the line to display the jump menu.

## 18.2. View Group

View group management allows you to add, edit, and delete groups, and hide and display empty groups

### 18.2.1. Add new group

Click "Add Group" as shown below. Set the view that the group needs to include by clicking the view name in the Optional view or selected View module.



### 18.2.2. Edit Group

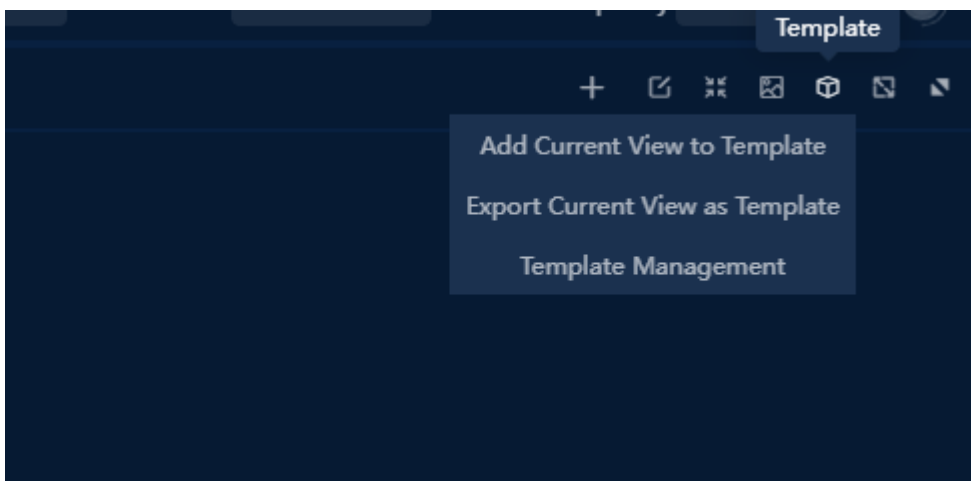
Click "✎", the "Edit Group" window pops up. You can update the group name, description, and membership view.

### 18.2.3. Delete Group

Click "🗑️", the "Delete Group" confirmation dialog box pops up. After the user confirms the deletion, the group will be deleted.

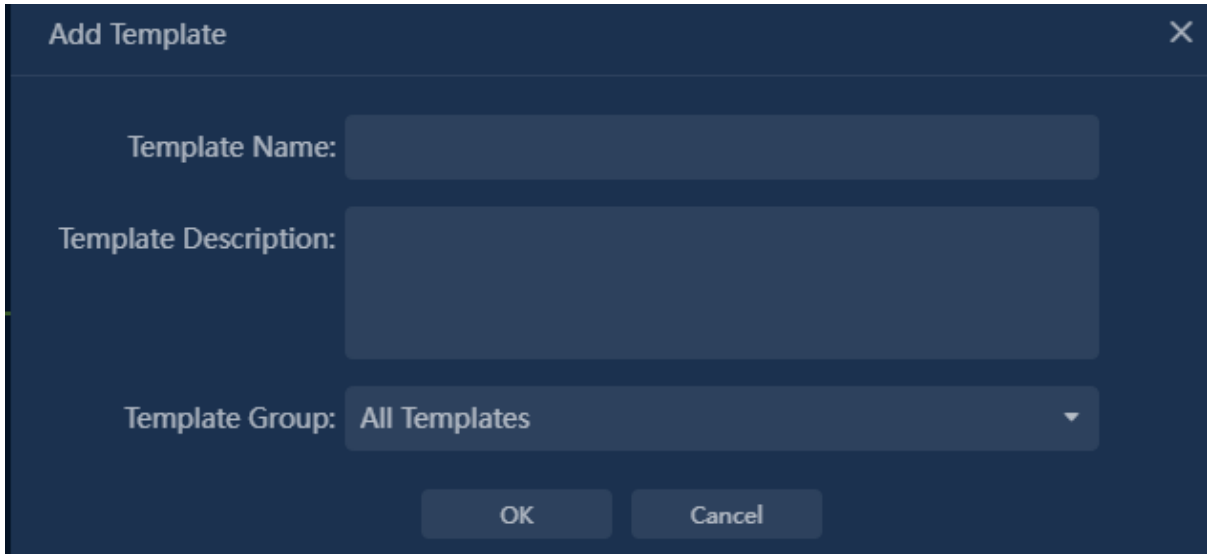
## 18.3. Template

You can add the current view as a template, export the current view as a template, and manage templates. Click "📄", as shown below:



### 18.3.1. Adding the Current View as a Template

Click "Add Current View as template". The Add Template window is displayed. You can configure the name, description, and template group. As shown below:

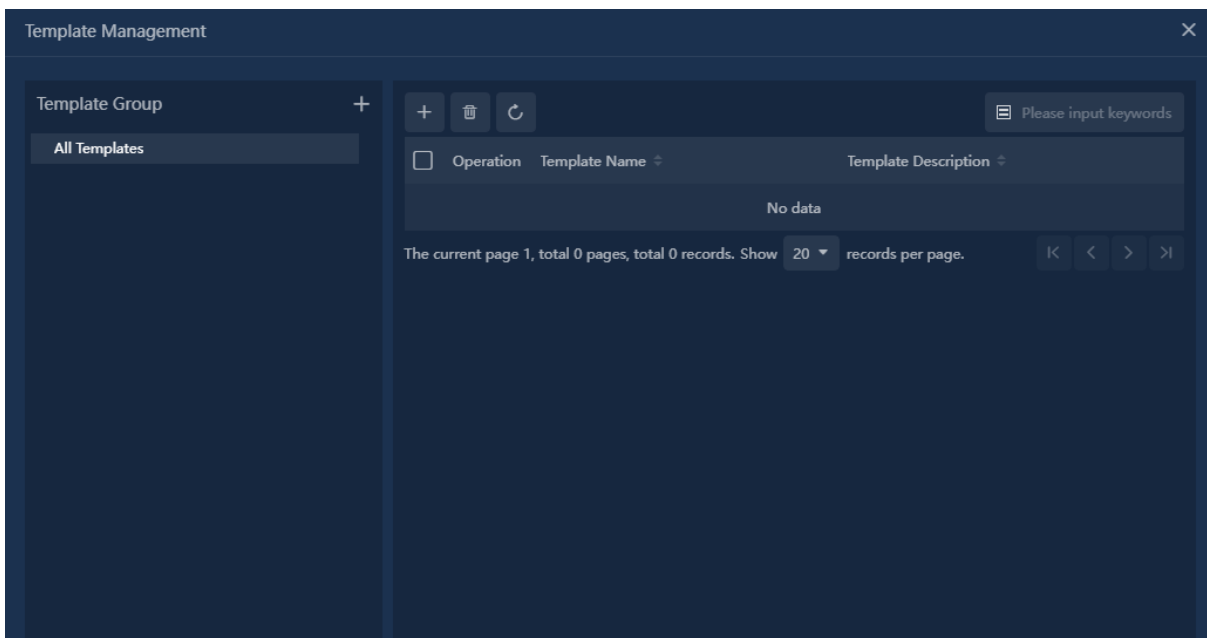


### 18.3.2. Exporting the Current View as a Template

Click Export Current View as template to save the view file in .cmt format.

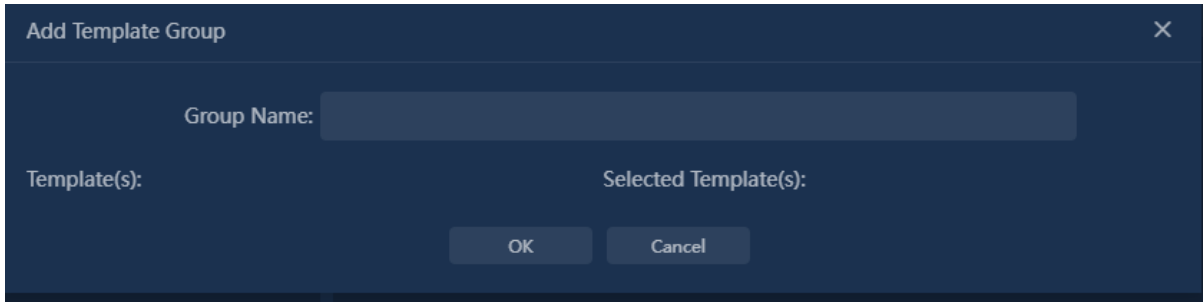
### 18.3.3. Template Management

Click Template Management. The Template Management window is displayed. You can add, delete, or modify a template group, export a template, or apply a template. As shown below:




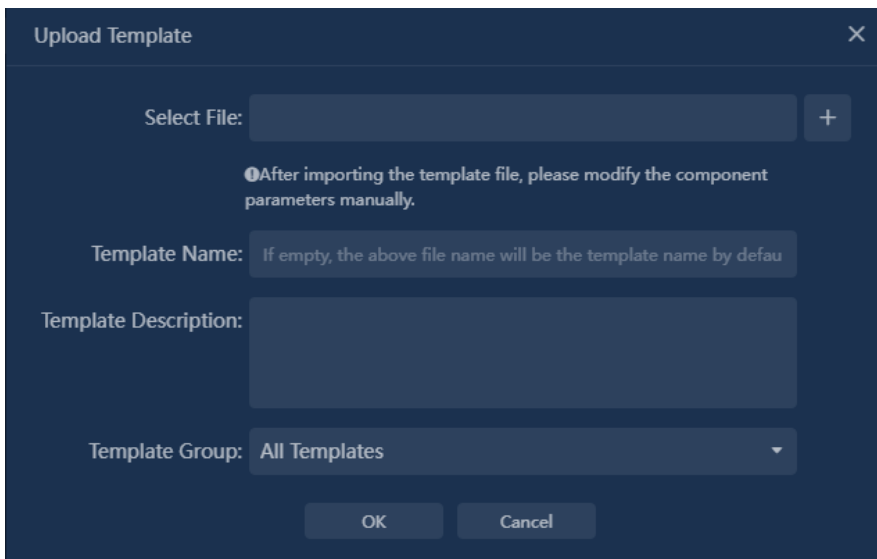
- Adds a template group

Click "+", as shown below. Set the view that the group needs to include by clicking the view name in the optional template or selected template module.




- Add a Template

Click "", the "Add Template" window is displayed. Users can select a template. cmt file import. As shown below:



- Apply the template

Click "". A dialog box is displayed asking you to apply the template. After the user confirms the application, the current view is overwritten.

## 18.4. Monitor and Analysis Module

When the view is in monitoring mode, you can configure the monitoring period and frequency.

If the view is in analysis mode, you can configure the analysis time range.

Click the indicator and exhale the drawer panel at the bottom of the page to display the indicator trend chart and drill-down object statistics.

## 19. Custom indicator monitoring

### 19.1. Function introduction

#### 19.1.1. Terminology

##### View

A view consists of one or more components that represent the monitoring of a particular object or scenario.

##### Object

Object Indicates the object to be monitored. The system supports monitoring of multiple objects, such as links, services, applications, and transactions.

##### Component

A component is the smallest data display unit. The system supports a variety of components, such as trend charts, tables, values, pictures, and texts.

##### Empty packet

or the current login user, if no view can be viewed in a view group, the view is called an empty group. Users can set to show/hide empty groups.

#### 19.1.2. Function Usage Scenarios

Data visualization is about instantly show the business relationships and potential problems that lie behind massive amounts of data in a more vivid and user-friendly form. Interaction with the monitoring view helps technical personnel find and troubleshoot service problems.

The user-defined indicator monitoring function meets the following scenarios:

- As a large screen for daily monitoring services, which monitors real-time traffic information of services.
- As a unified monitoring platform, the screens of other monitoring modules, such as terminal monitoring and network topology monitoring, are displayed in a centralized manner.
- The system monitors the real-time status of network devices, including the CPU, memory, and online status.
- Monitor VoIP communication quality, including call status, network latency, TOP communication, alarms, and more.

#### 19.1.3. Value of functions

The user-defined indicator monitoring function has the following value:

- The system provides built-in scenario templates to simplify user configuration.
- Support multiple icon components, allowing users to mix and free collocation.



- A component lends itself to a personalized style set to meet the monitoring needs of different users.
- Lent The view supports a customized resolution and can be adapted to various large monitoring screens.

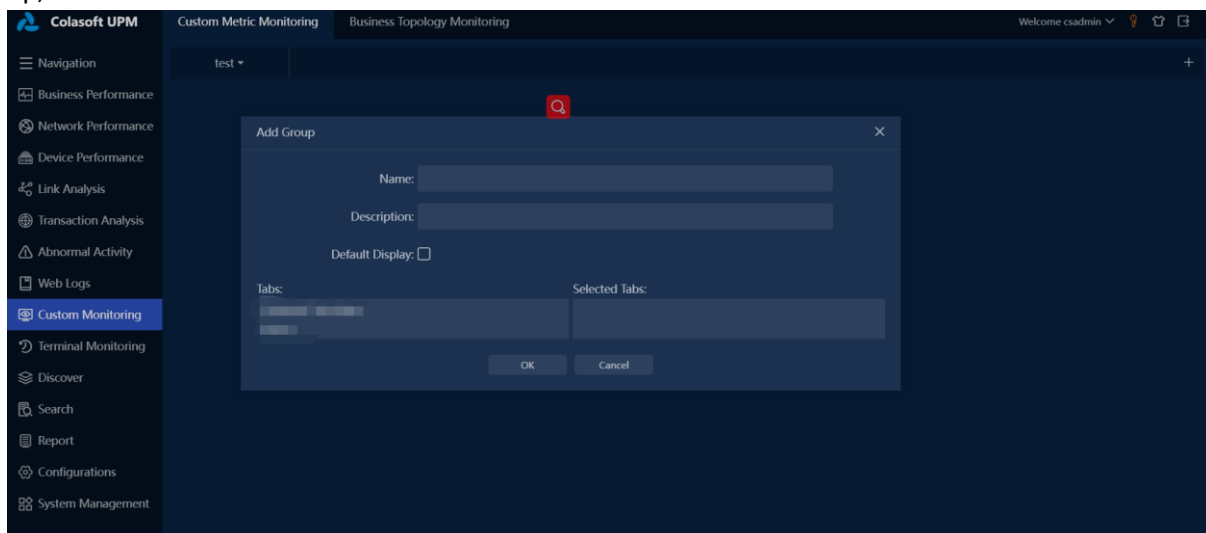
## 19.2. Operations Guide

### 19.2.1. View management

#### View group

User can group views by department, service, and region, etc.

Click the "Add Group" button in the drop-down list of view, and the Add Group pop-up box will pop up, as shown below:



Set the name and description of a view group, and select a view to be included in the group.

If you want to display the view group by default, select the "Default display" check box. That view can be added to multiple view groups

#### View properties

Click the  button to pop up the Add View box, as shown below.

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

Field Name	Description
Name	Set the name of the view. The view name must be unique.
Description	This parameter is optional. It is used to set the description of a view.
View privilege	Use to set the permissions of a view.  Private: Create a view that is visible only to myself. Public: The view created is visible to all.

Field Name	Description
	User group: The created view is visible to the specified user group.
View template	This parameter is optional. It is used to select a referenced view to quickly create a view.
View size	This command is used to set the size of the view to facilitate the display of various large screens. The system provides a variety of common sizes for selection, users can also directly enter a custom size.
Background color	This is an optional configuration item that is used to set the background color of the view.
Background image	This is an optional configuration item for setting the background image of a view. The background image can be adaptive, tiled, stretched, filled, original size, or original size center play. The background image is not used by default.
Enable component animation	Used to set whether component animation is enabled for the view, enabled by default.
Label	This configuration item is optional. You can add one or more labels to a view. The system supports view filtering based on labels.
Default display	Used to set whether the view is displayed, not selected by default.


Note: The default view displayed in the monitoring of user-defined indicators is: The default view displayed in the default view group.

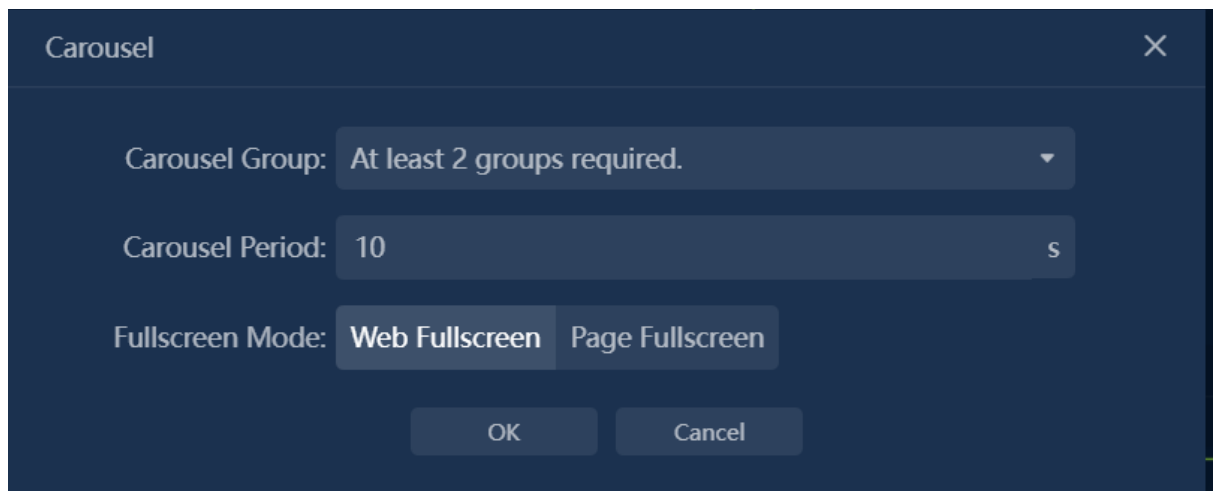
## View operation

### Page Fullscreen:

View supports browser full-screen display, which is generally used for screen casting.

### Carousel:


Select "carousel" in , and the round seeding setting dialog box pops up, as shown in the following figure.

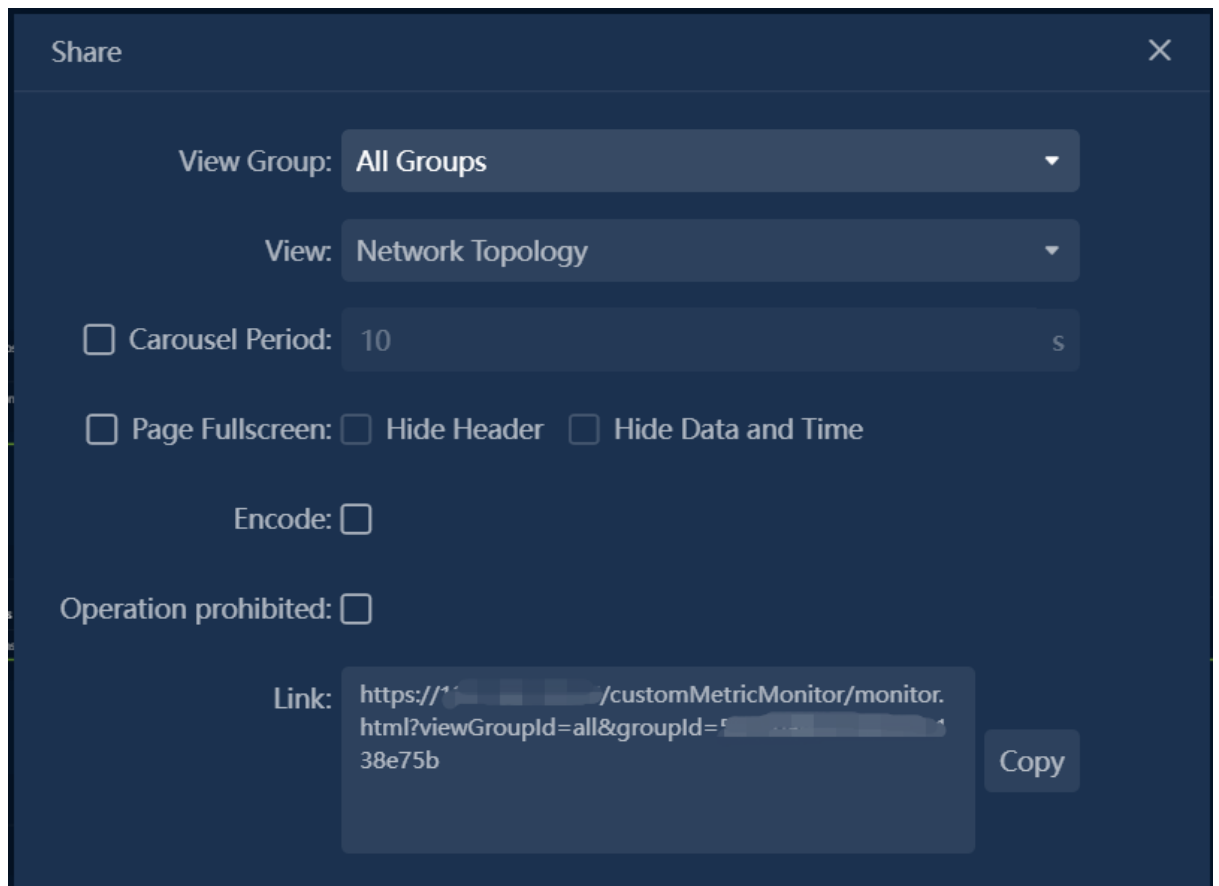


The following table describes the configuration fields in the dialog box.

Field Name	Description
Carousel Group	This parameter is used to set the views to be broadcasted. You need to select two or more views.
Carousel Period	Set the interval between views.
Fullscreen mode	The system supports full-screen browser and full-screen page modes. The default mode is full-screen browser.

### Share:

Select "Share" in , and the share setting dialog box is displayed, as shown in the following figure.

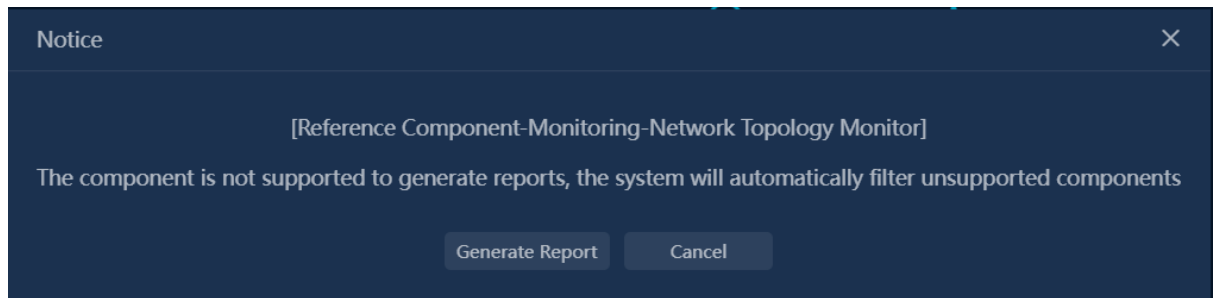


Field Name	Description
View group	This parameter is used to select a view group.
View	Used to select shared views. If you select "Carousel Period", you need to select two or more views.
Carousel Period	This parameter is optional. It is used to set the interval between carousel views.
Page Fullscreen	This parameter is optional. It is used to set the display mode of the shared view. When "Page Fullscreen" is selected, you can set whether to hide the top bar and whether to hide the time and date.
Encode	This configuration item is optional. It is used to encode special characters in share links.

Field Name	Description
Operation Prohibited	This configuration item is optional. If “Operation Prohibited” is selected, all jumps in the shared view become invalid.
Link	Share the URL of the link. Other logged in users can access the corresponding view through this URL.


### Generate report:

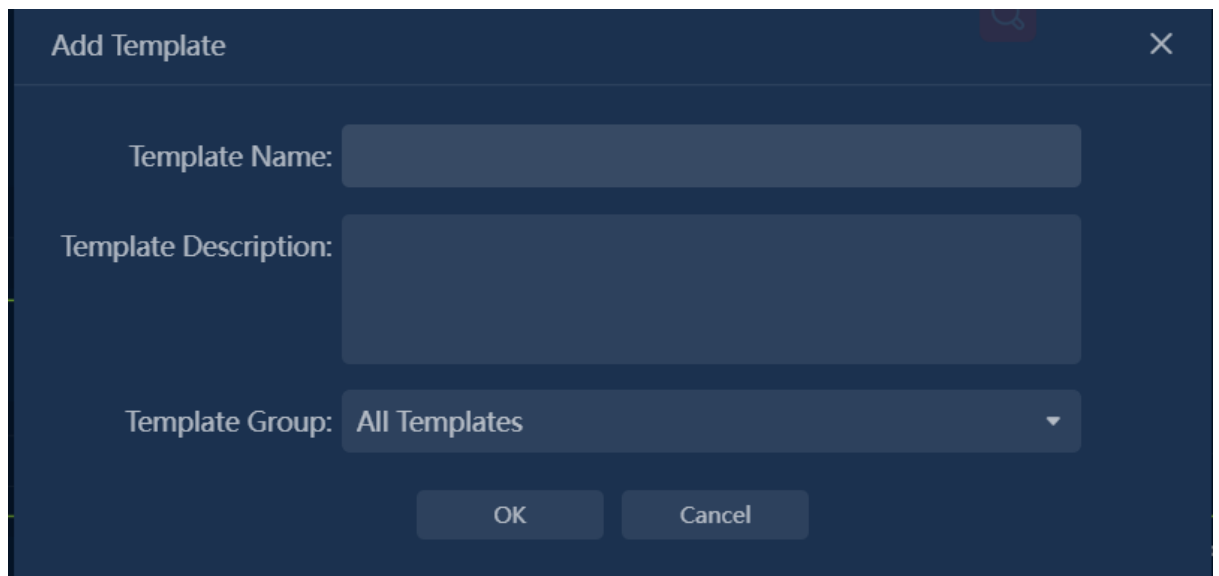
You can directly generate reports in system view. Select “Generate Report”, and a dialog box is displayed, as shown in the following figure



Click "Generate report" button to jump to the page of new report.


### Add the current view as a template

You can add a view as a template. Click this button  then click “add Current View to template”. The Add Template dialog box is displayed, as shown in the following figure.




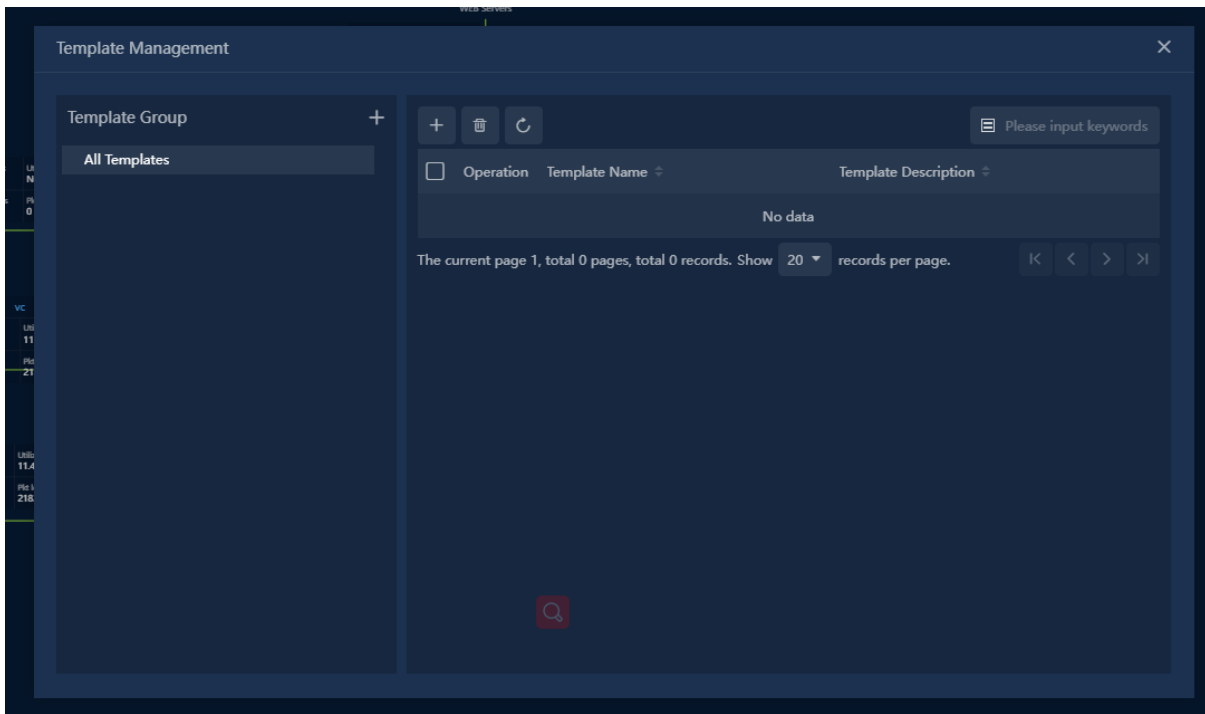
Set the template name and description, select a template group, and click OK to add the template.

### Example Export the current view as a template

You can export a view as a template file. You can select “Export Current View as a template” in  to export the view as a \*. CMT template file. In template management, you can upload template files directly.


## 19.2.2. Template Management

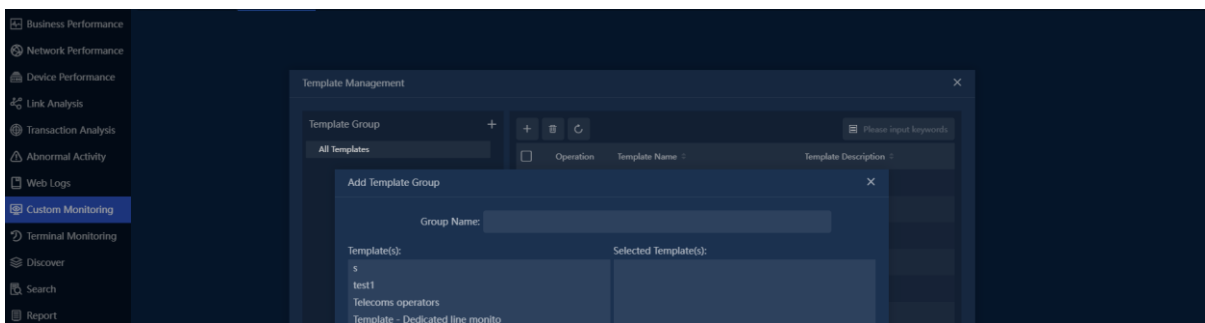
Select “Template Management” in , the template management dialog box is displayed, as shown in the following figure.



### Template group


You can group templates based on user-defined maintenance.

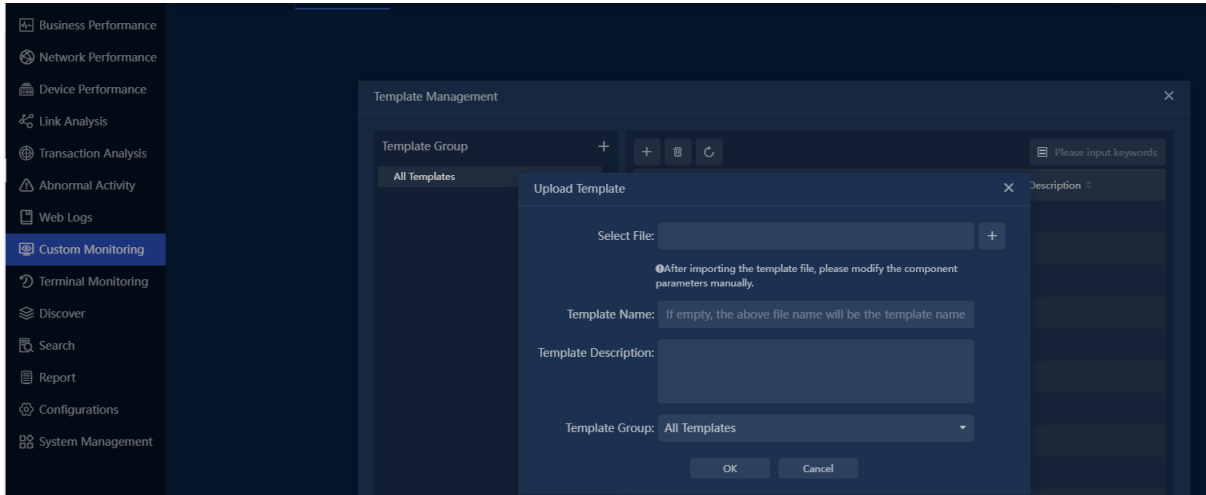
Click on the  right of “Template group” , the add Template group pop-up box will pop up, as shown below.



### Upload template


To upload a template, import a \*. CMT template file to the system.

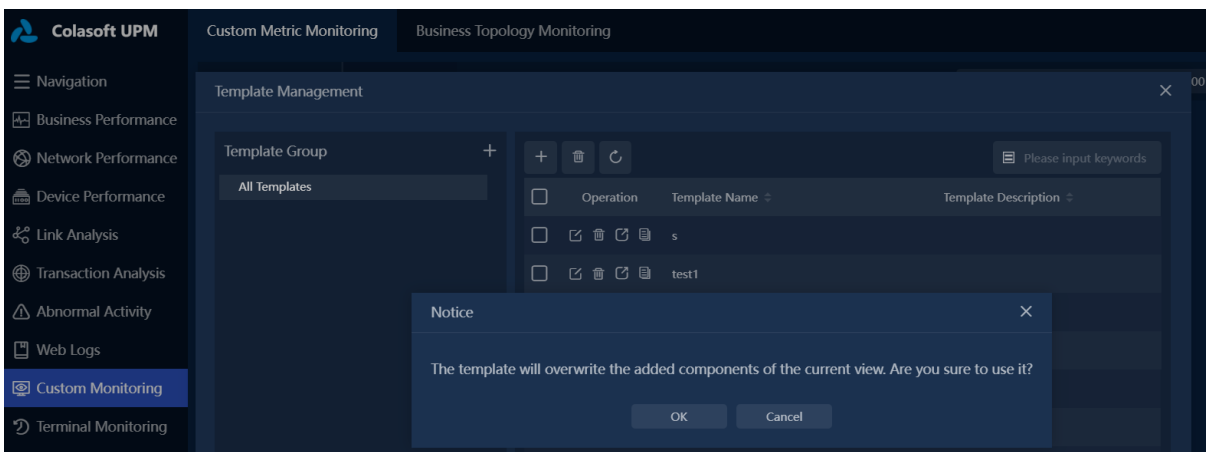
Click  on the template list, and the Upload Template dialog box is displayed. In the dialog box, select a template file, set the template name and description, and select the template group to which the template belongs, as shown in the following figure.



## Template reference

A template reference applies the selected template to the current view.

Click  in the operation column of the template list, and a prompt box will pop up, as shown in the picture below.



### 19.2.3. View operation

#### Component selection

You can select multiple components in the following three ways:

- Queue to select multiple components in a view using Ctrl+ the left mouse button.
- A user directly screens several components in a view, allowing all components in the box range to be selected.
- At the same time, you press Ctrl+ the left mouse button to select multiple components.

## Component copy

Components support single replication and batch replication.

- Automatically adds a component to the bottom of the view during a single replication.
- Bulk replication, in which the copied component is added next to the component being copied.

## Component delete

Components can be deleted one by one or in batches. You can delete components in either of the following ways:

- After selecting a component, right-click the component and choose Delete Component.
- After selecting a component, press the Del key.

## Layer set

In a view, a component is a layer. Layer Settings include top layer, bottom layer, up Layer, down layer.

Once the component is selected, layer Settings can be performed using the buttons in the toolbar at the top of the page or the right-click menu.

## Style brush

The size style brush can quickly set multiple components to the same size. The size style brush includes sync size, sync height, and sync width.

Select two or more components and click the size style brush button on the top toolbar. The system will synchronize the size of the selected component to the size of the first selected component according to the order of component selection.

## Component lock

After a component is locked, it cannot be edited or dragged. It can be unlocked in two ways:

- Directly clicking the lock icon above the locked component in the view.
- In the list of added components, click the unlock diagram of the locked component.

## Components are hidden

Component hiding is only hidden in edit mode, not in view monitoring.


For hidden components, you can reset them to display in the list of added components.



## 19.2.4. Style setting

In the custom indicator monitoring view, you can set styles for all components to meet the customization requirements.

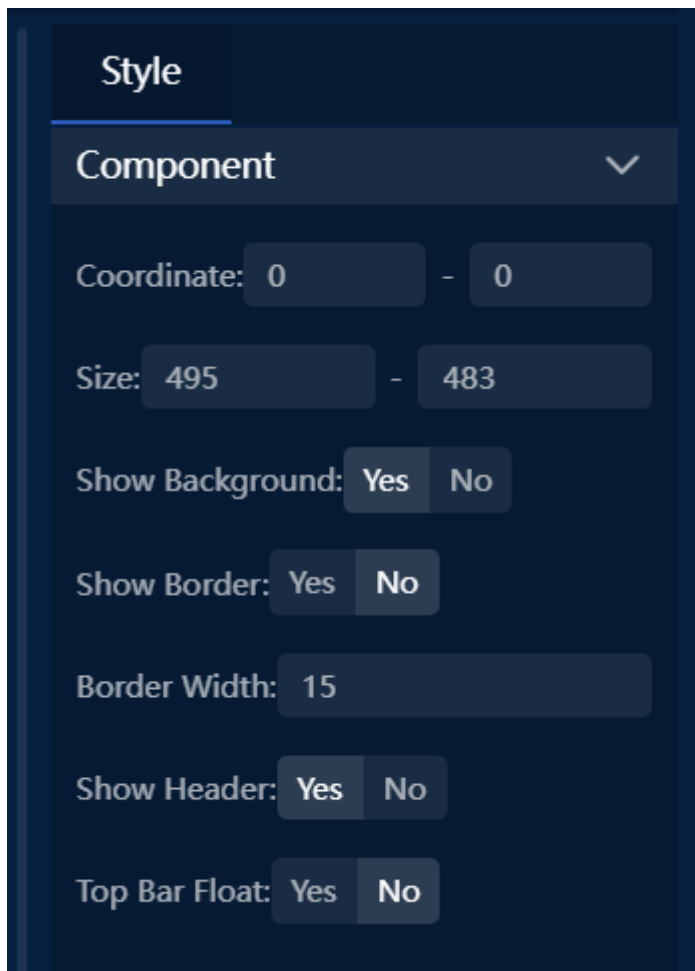
Users can access the component's styling page in two ways:

- 1: In editing mode, right-click a component, and choose Style Settings from the shortcut menu to expand the style setting bar.
- 2: In editing mode, tap the  icon in the upper left corner of your view to expand the style Settings bar.

All components support component Settings or title Settings.

## Component setting

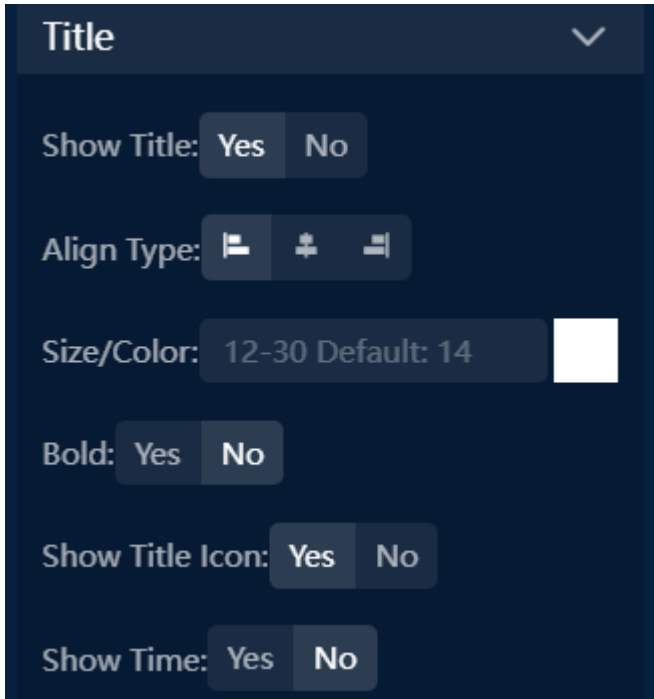
Component Settings are used to set the component's position, size, background, border style, top bar, and whether animation is enabled.



Tips: Component positions and dimensions can be manually dragged and dropped, but are more precise through component Settings.

## Title setting

Title Settings are used to set the content of the title bar of the component, including whether the title is displayed, alignment, font style, and display time.



## Trend chart style Setting

Trend chart style Settings include:

- Broken line

Sets the line width and point size for the line trend chart.

- Value setting

Set whether to display the value of each monitoring point in time, the peak value, valley value, and average value of the trend chart in the current monitoring period, and the font style to display the value on the trend chart.

- Sets the X axis

Sets whether to display the X-axis title, whether to display the split line, and the style of the split line.

- Sets the Y axis

Set the Y axis style. The system supports linear axis and logarithmic axis. The default is linear axis.

Sets whether the splitter line is displayed, and the style of the splitter line.

Set the maximum value of the Y-axis. If this is set, values beyond the maximum value will not be displayed on the graph.

- Sets the prompt

Sets whether to display the prompt and the font style of the prompt.

- Legend setting

Sets whether to display the legend.

Set the legend layout position. The system provides four positions: bottom, top, left, and right.

Set the legend height. To ensure the integrity of the example display, you can customize the legend height.

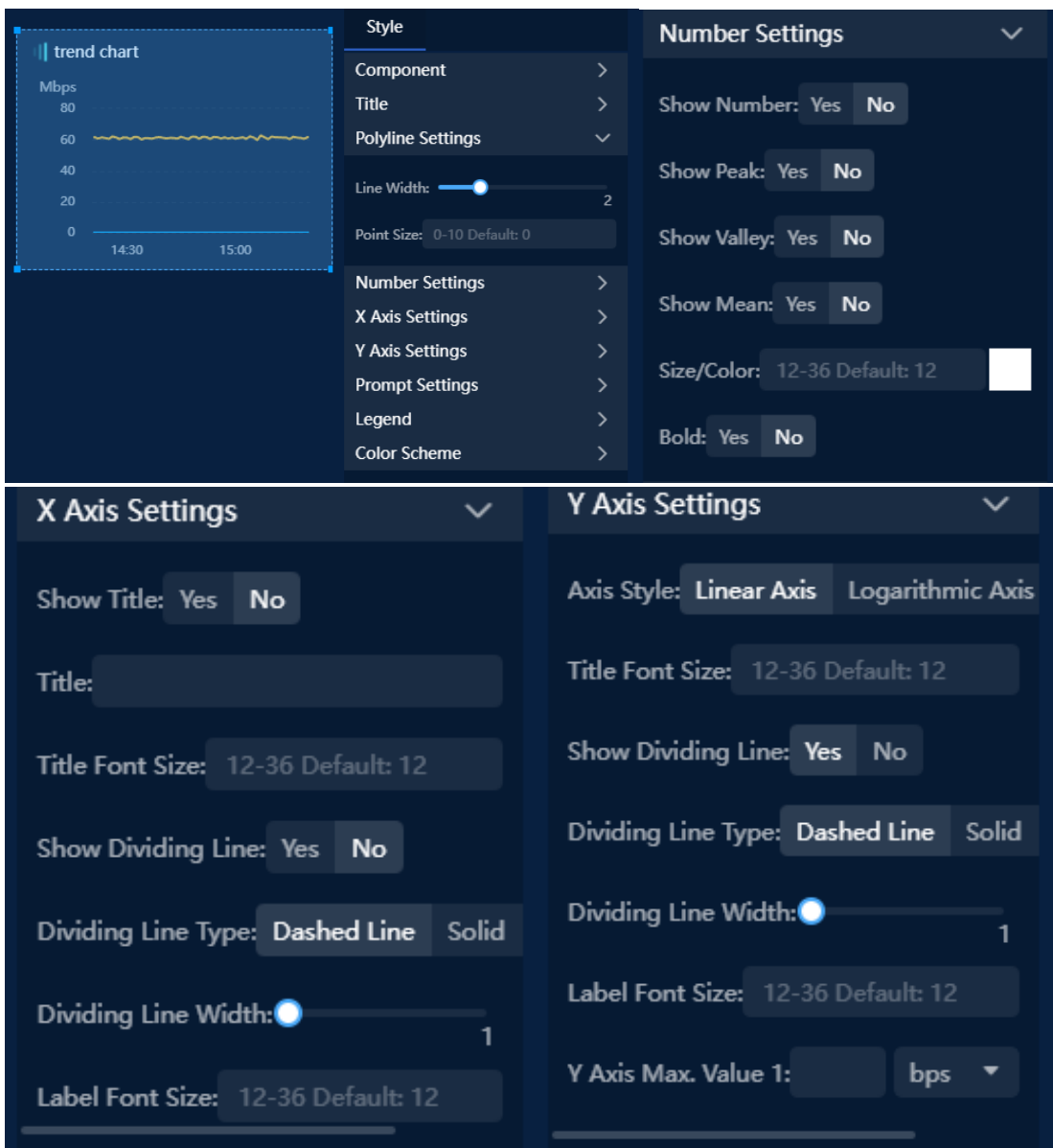
Set example width, support custom width and adaptive width. To ensure that the example display is complete, the user

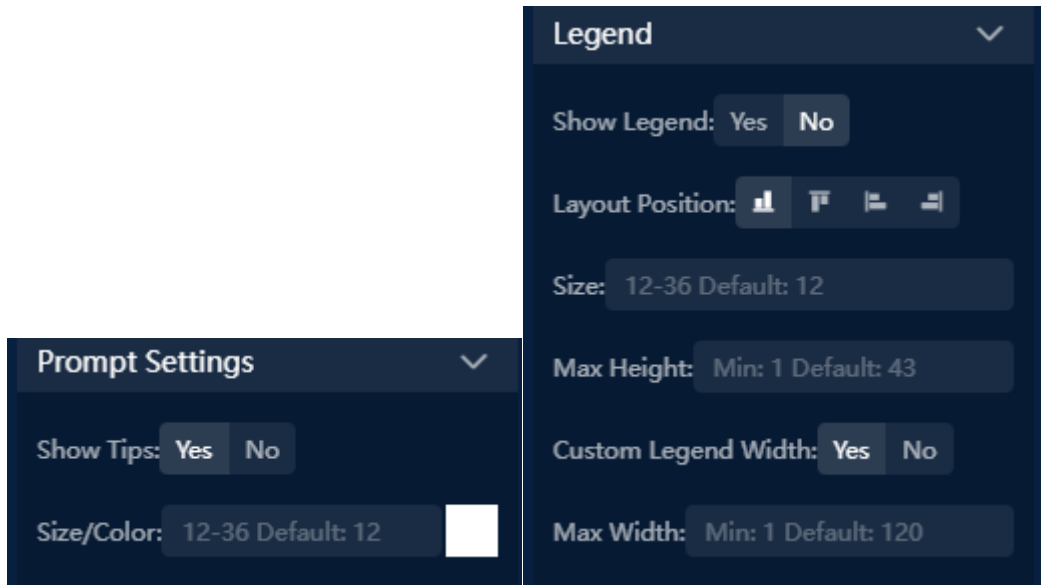
Custom example width is available.

- Color scheme Settings

Set the color of each example on the trend diagram.

The trend chart style setting interface is as follows:





## Statistics chart setting

Chart style Settings include:

- Value set

Sets whether a specific value is displayed on the column, and the font style for the value.

- Cylinder set

Set the width of the column and the radian of the fillet.

- The X axis is set

Sets whether to display the X-axis title, whether to display the split line, and the style of the split line.

- Virtual Gateway Sets the Y axis

Set the Y axis style. The system supports linear axis and logarithmic axis. The default is linear axis.

Sets whether the splitter line is displayed, and the style of the splitter line.

Set the maximum value of the Y-axis. If this is set, values beyond the maximum value will not be displayed on the graph.

- Prompt setting

Sets whether to display the prompt and the font style of the prompt.

- Legend set

Sets whether legend is displayed.

Set the legend layout position. The system provides four positions: bottom, top, left, and right.

Set the legend height. To ensure the integrity of the legend display, you can customize the legend height.

Set legend width, support custom width and adaptive width. To ensure that the legend display is complete, the user

Custom legend width is available.

- Color scheme Set

Set the color of Top N in the bar chart.

The setting interface of statistical graph style is as follows:

### Column Settings

Column Width: Min: 1 Default: Adapt

Radius: 0-10 Default: 0

### Number Settings

Show Number: Yes No

Size/Color: 12-36 Default: 12  

Font Bold: Yes No

### Legend

Show Legend: Yes No

Layout Position: | | | |

Size: 12-36 Default: 12

Max Height: Min: 1 Default: 44

Custom Legend Width: Yes No

Max Width: Min: 1 Default: 120

### X Axis Settings

Show Title: Yes No

Title:

Title Font Size: 12-36 Default: 12

Show Dividing Line: Yes No

Dividing Line Type: Dashed Line Solid

Dividing Line Width:  1

Label Font Size: 12-36 Default: 12

### Y Axis Settings

Title Font Size: 12-36 Default: 12

Show Dividing Line: Yes No

Dividing Line Type: Dashed Line Solid

Dividing Line Width:  1

Label Font Size: 12-36 Default: 12

Y Axis Max. Value:  bps ▼

## Table style Setting

Table style Settings include:

- Value set

You can set the display styles for indicators such as percentage in the table. The system provides two styles: value and progress bar. By default, the value is displayed.

Set whether values in the table are displayed in thousandths. By default, values are not displayed in thousandths.

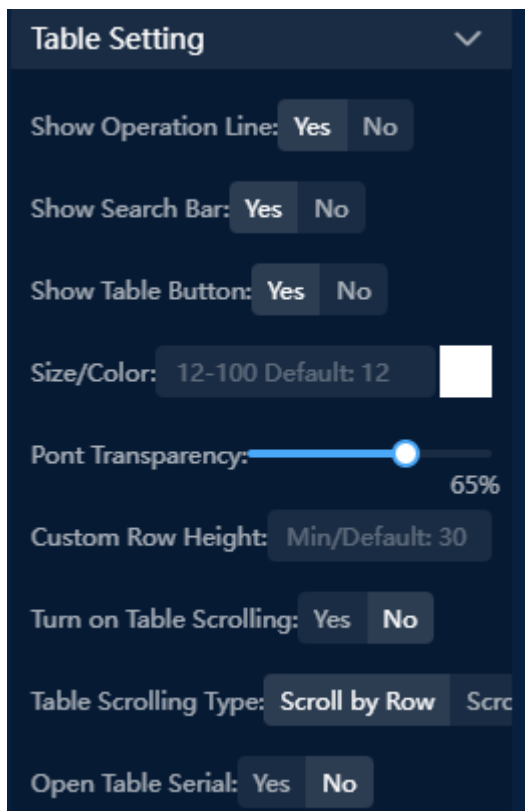
- Table Settings

Sets whether the table displays the action column, search bar, table button, and table sequence number.

Set the font color, size, and row height for the table.

Set the scrolling mode of the table. The system provides two modes: row scrolling and page scrolling.

The table style setting interface is as follows:



## Numerical graph style Settings

Numerical graph style Settings include:

- Title Style Settings

Sets the text style for the title.

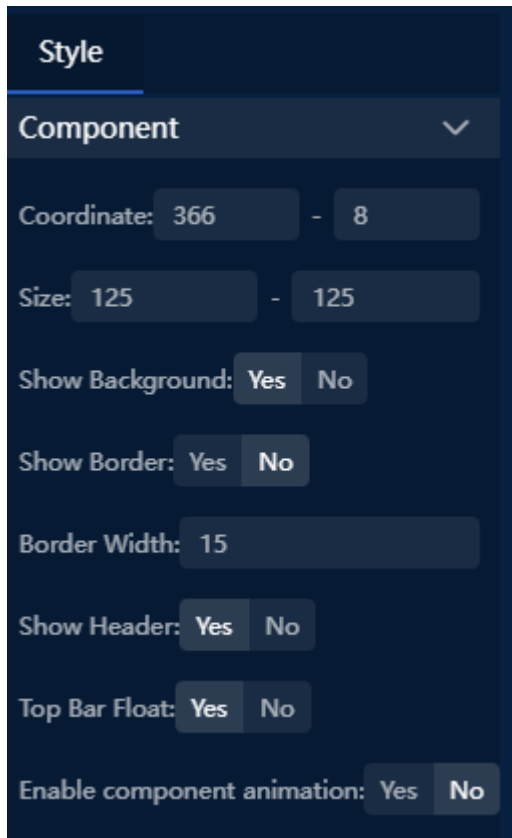
- Indicator Style Settings

Sets the text style of the indicator and whether to use a thousandth separator.

- Unit style Settings

Sets the text style of the unit.

The value diagram style setting interface is as follows:



## 19.2.5. FAQ

### Messy layout after referencing view templates

#### Problem description

When a view is created, the layout of the components in the view is inconsistent with that in the view template after the view template is referenced.

#### Possible reasons

The size of the new view is inconsistent with that of the view template.



## Solution

When creating a view, set the view size to the size of the view template.

## 20. Session Tracking

### 20.1. Introduction

#### 20.1.1. 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.

#### 20.1.2. 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.

#### 20.1.3. 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.

### 20.2. 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:

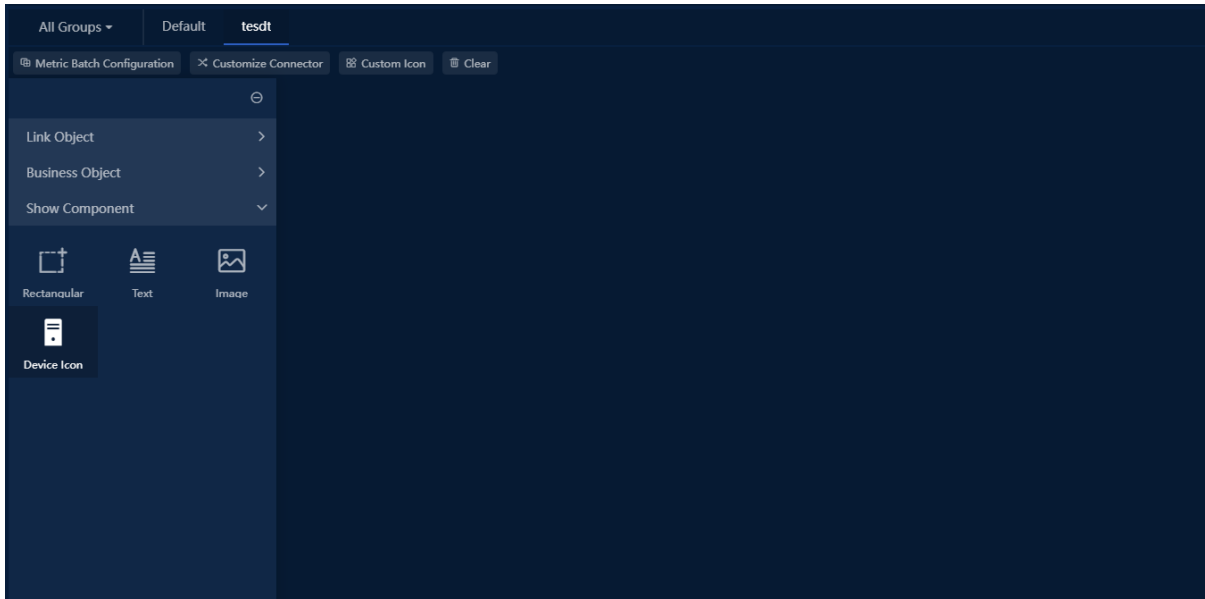
Add view configuration:

Field Name	Description
Name	View name
Description	View description
View Privilege	Select one of Private, Public, User Group
Clone View Configuration	Clone the existing view configuration.
Label	The label is the horizontal menu bar - > Options in the view drop-down list.
Default Display	Access the network topology monitoring view displayed by default.

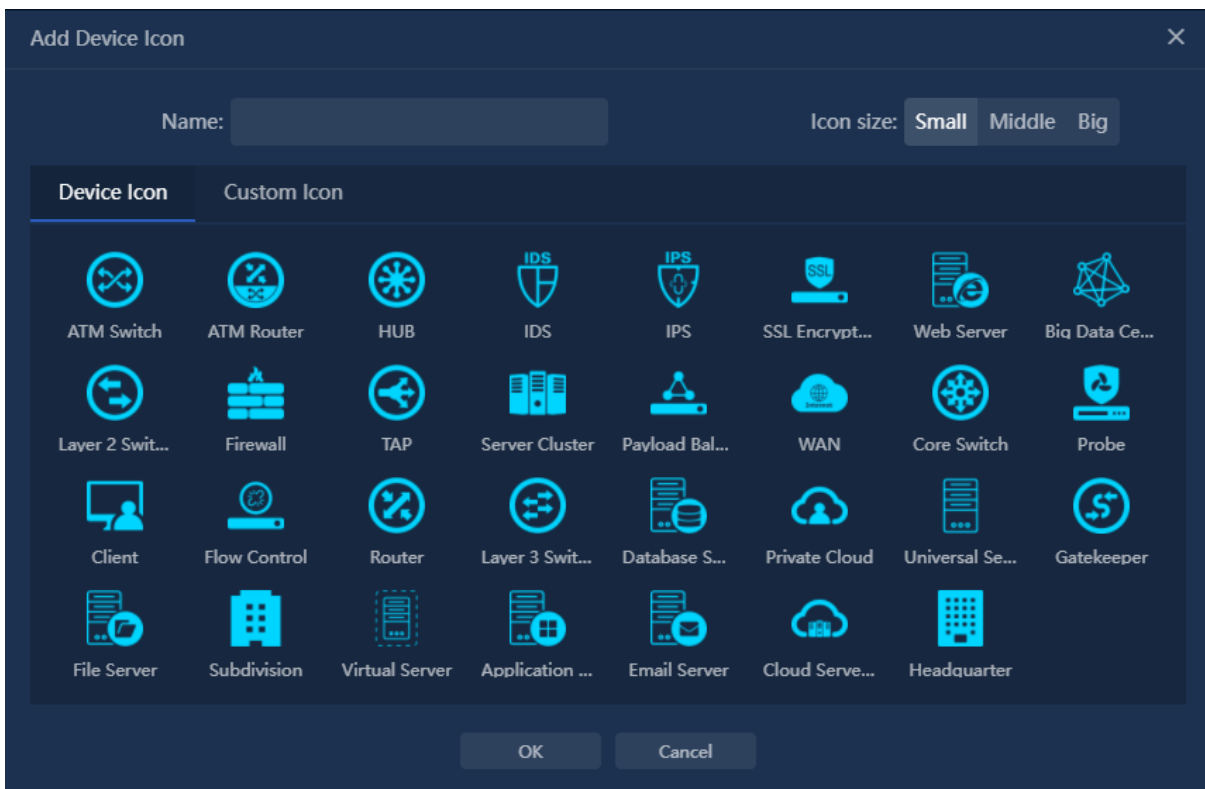
3, Click "OK", the basic information about a view is added. Then click "  " to enter editing mode, as shown below:

### 20.2.1. Device Icon

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

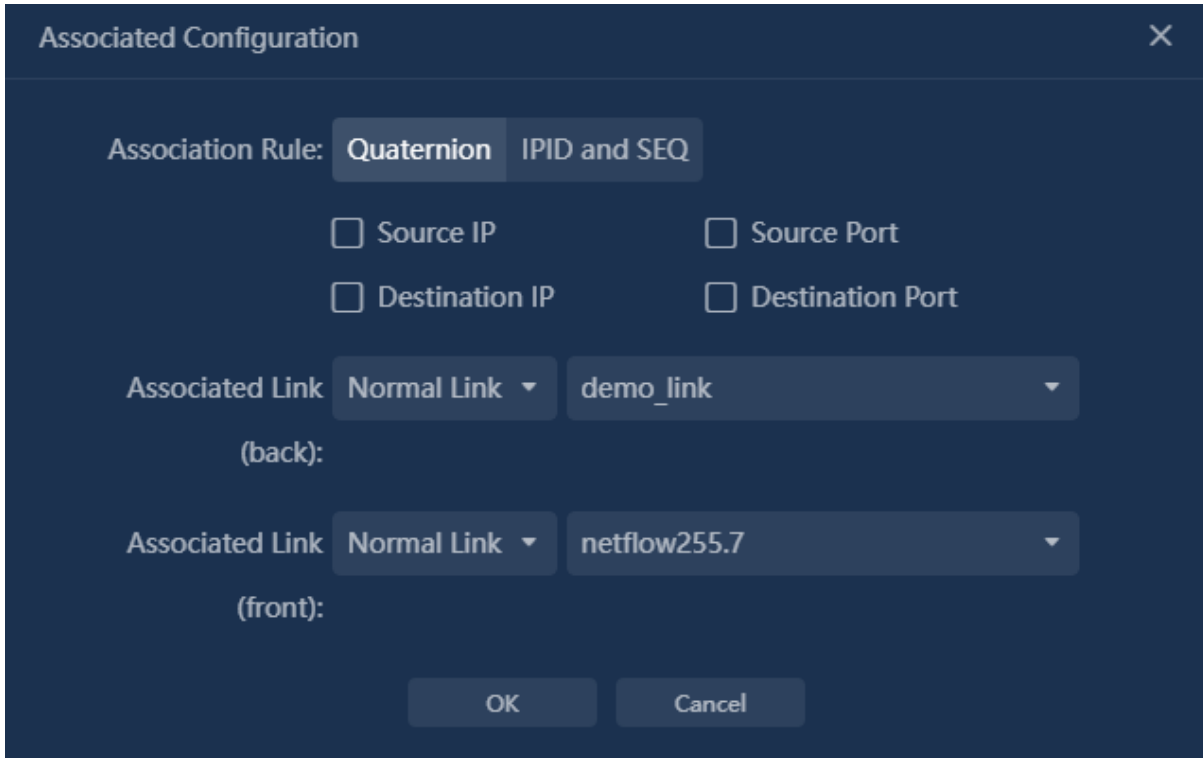


4, In Show Components on the left, select Device Icon and drag it to the canvas on the right. The Add device icon dialog box is displayed, as shown in the following figure.



5, Select the device icon, set the name and size of the icon, and click OK. The device icon is added.

6, 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.

7, 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.

8, To make the session access path more complete and intuitive, you can add links, lines, or other auxiliary ICONS.

## 20.2.2. 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:

The screenshot shows a network topology diagram at the top with nodes like Unicorn, LB, WEB FW, APP FW, Core Switch, SFI DS, and SFI DB. Below it is a 'Conversation List' table with the following data:

Operation	Application Name	Client	Client Port	Server	Server Port	Total Bytes	bps	Total Pkts
<input type="checkbox"/>	DB Server		50560		6433	61.49 MB	8.60 Mbps	65459
<input type="checkbox"/>	DB Server		37669		6433	25.53 MB	3.57 Mbps	51631
<input type="checkbox"/>	DB Server		35447		6433	9.47 MB	1.32 Mbps	35558
<input type="checkbox"/>	DB Server		13616		6433	8.10 MB	1.13 Mbps	30309

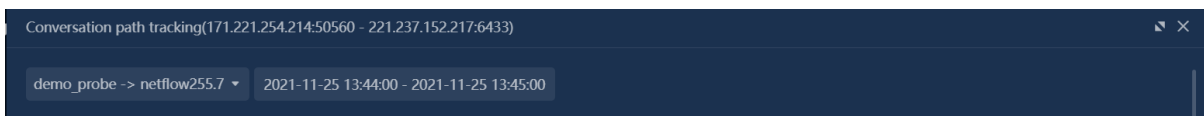
After you click the "Session Tracking" button, the session tracking dialog box is displayed.

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:



## 21. SRv6 Session Path Combing

### 21.1. Introduction

#### 21.1.1. 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.

#### 21.1.2. 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.

#### 21.1.3. 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.

## 21.1.4. Value

- Supports decoding of SRv6 network protocols.
- Automatically combs the real SRv6 session access path.

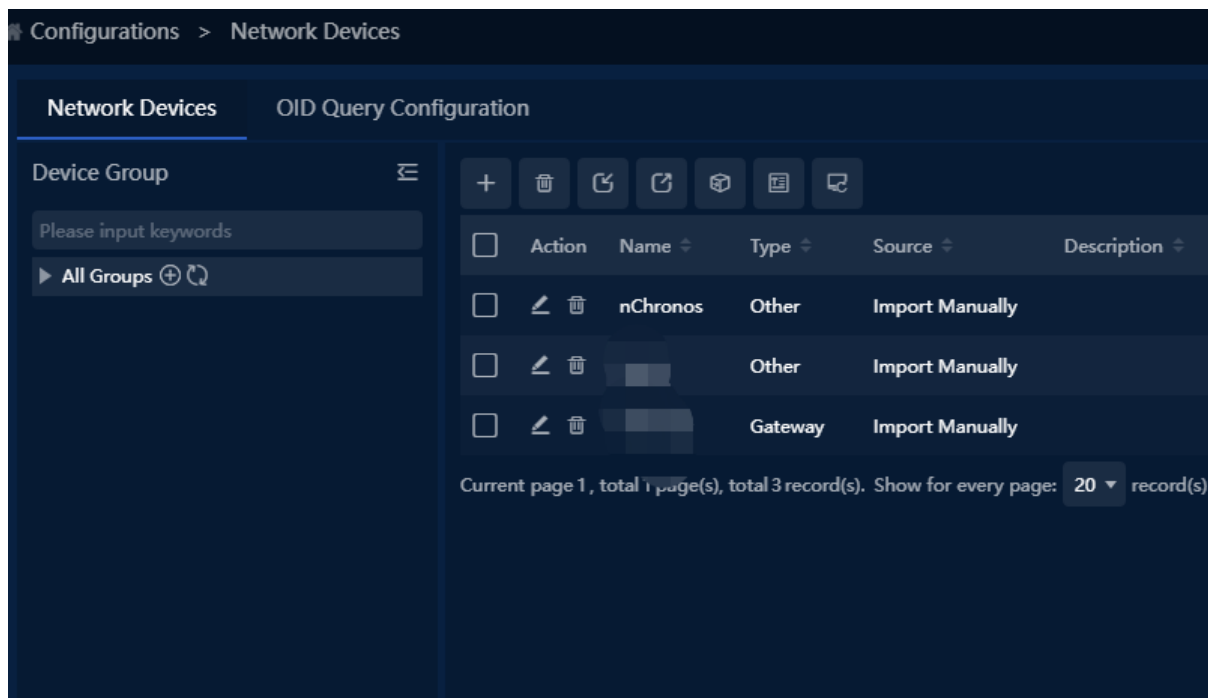
## 21.2. Operation Guide

### 21.2.1. 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.



Field Name	Description
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 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.

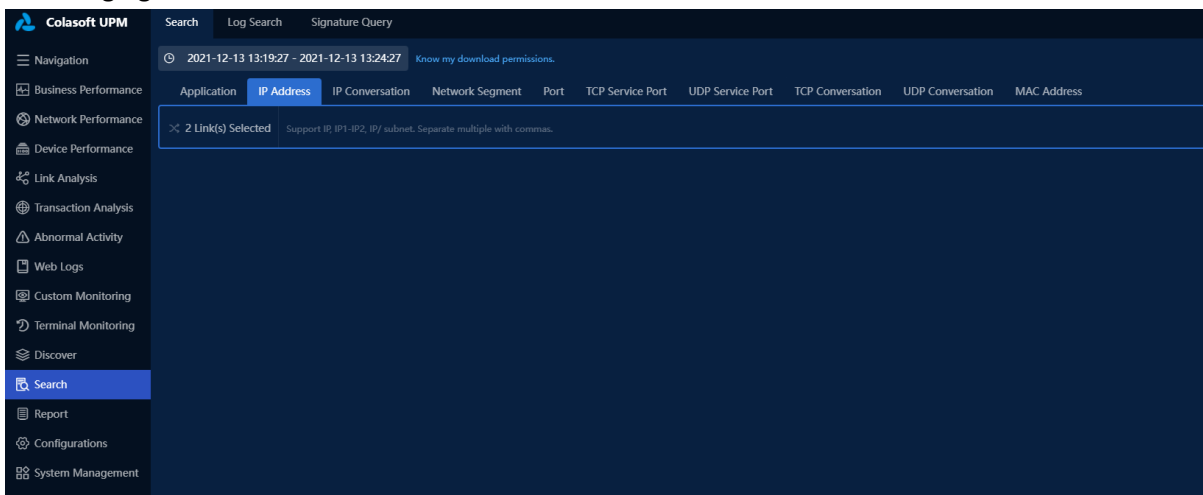
Notice: Not allow device ids configured on different network devices to cross; otherwise, unique network devices cannot be matched based on device ids.

3. Click OK to finish configuring the network device.

## 21.2.2. 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.



## 21.2.3. Trend

In the dialog box of "Session device Grooming", click the "Start grooming" button to view the grooming result, as shown below.

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.
- At the same time, multiple devices that are the same in a row are merged and only one network device is displayed.

## 22. SNMP

### 22.1. Features

#### 22.1.1. 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.

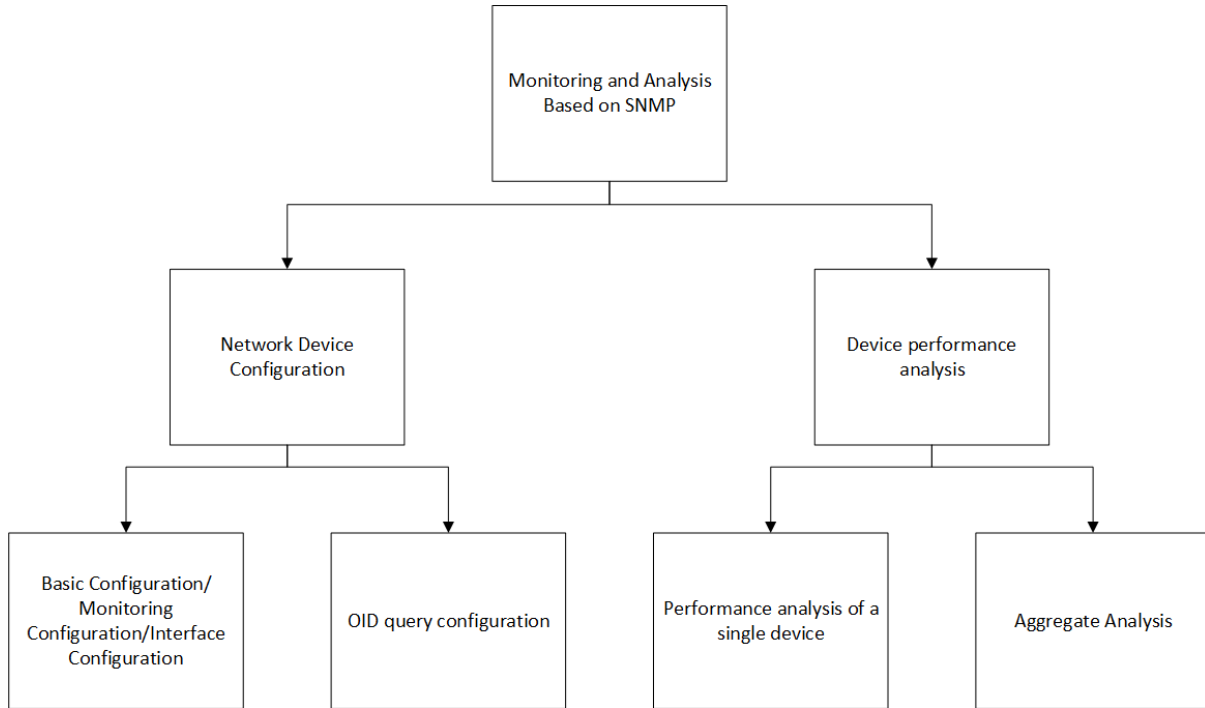
The NMS can send a request to the Agent to query or modify one or more specific parameter values. After the Agent receives the request information from the NMS, it completes the query or modification operation, and sends the operation result to the NMS to complete the response. MIB can also be regarded 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.

#### 22.1.2. 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.

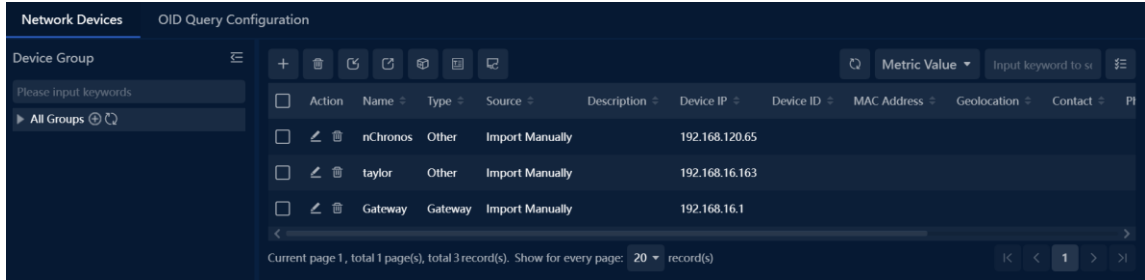
The functional structure is shown in the following figure:



## 22.2. Device configuration

### 22.2.1. 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 <a href="#">3.1.1 Basic Configuration</a> <a href="#">3.1.2 Monitoring configuration</a>
	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.

### 22.2.2. 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.

### 22.2.3. Monitoring configuration

Click  the button to add a network device. The monitoring configuration is shown in the following figure:

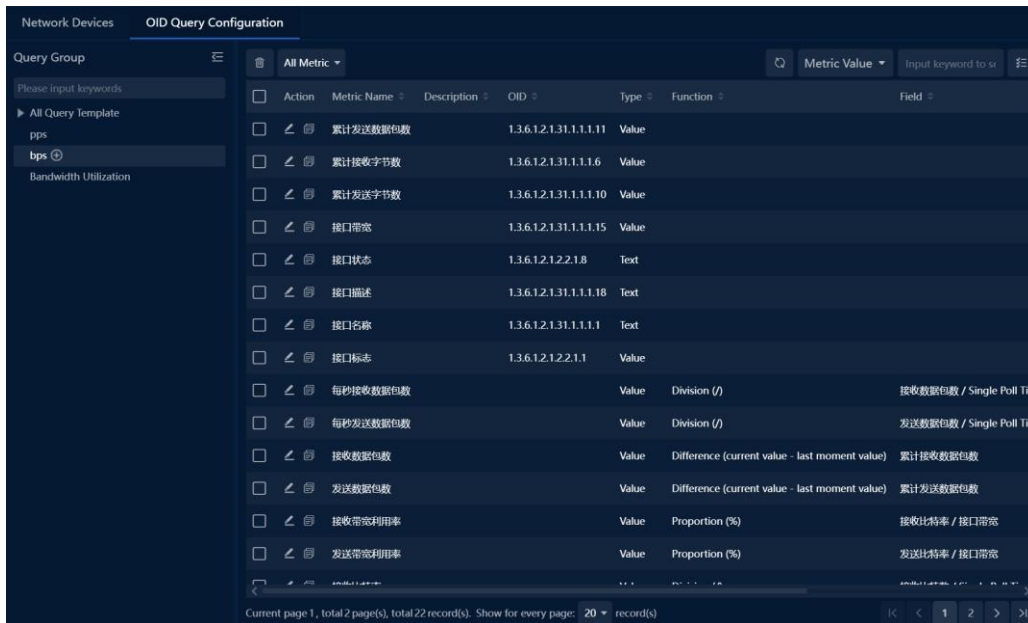
Monitoring status is not enabled by default. After enabling, configuration parameters are required, as shown in the following table:

operate	illustrate
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 .

## 22.3. 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 <a href="#">3.2.1 Query Template Configuration</a>
	Edit query template
	delete query template

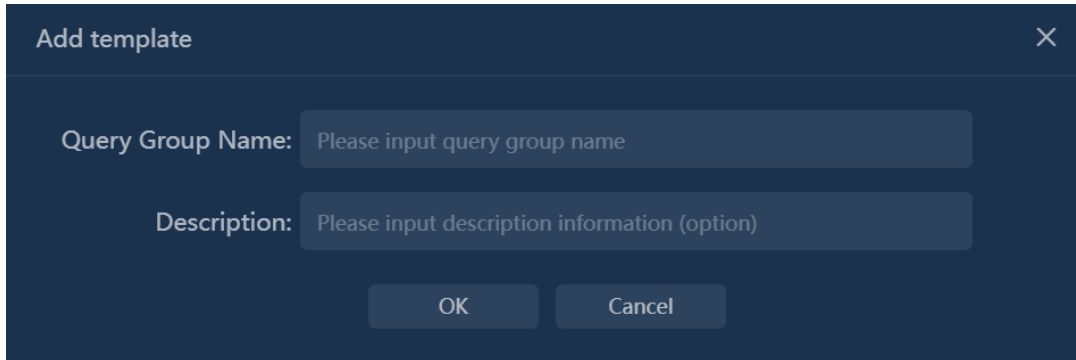
The functions of the action bar above the indicator list are shown in the table below:

operate	illustrate
	To add common indicators, please refer to <a href="#">3.2.3 Common Indicator Configuration</a>
	delete indicator
	Compile the MIB library and display the OID tree list.

Add calculated metrics	add calculation indicators, please refer to <a href="#">3.2.4 Configuration of calculation indicators</a>
Metric filtering	Filter options include: all indicators, common indicators, calculated indicators

### 22.3.1. 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:

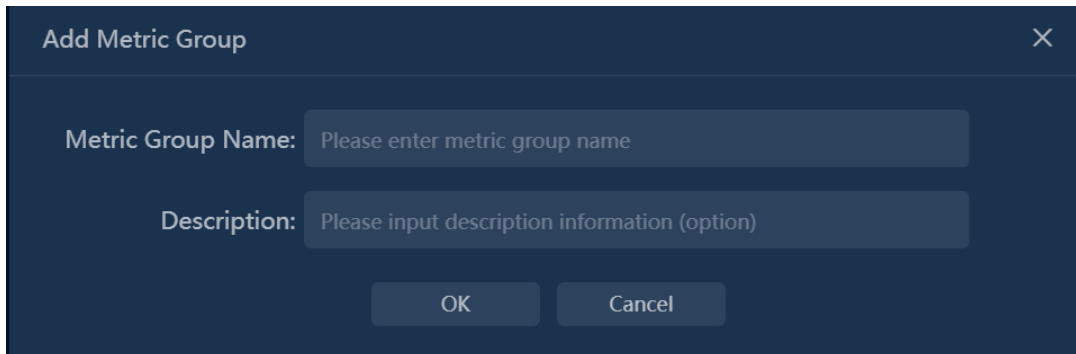


### 22.3.2. Metric group configuration

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:




### 22.3.3. Common indicator configuration

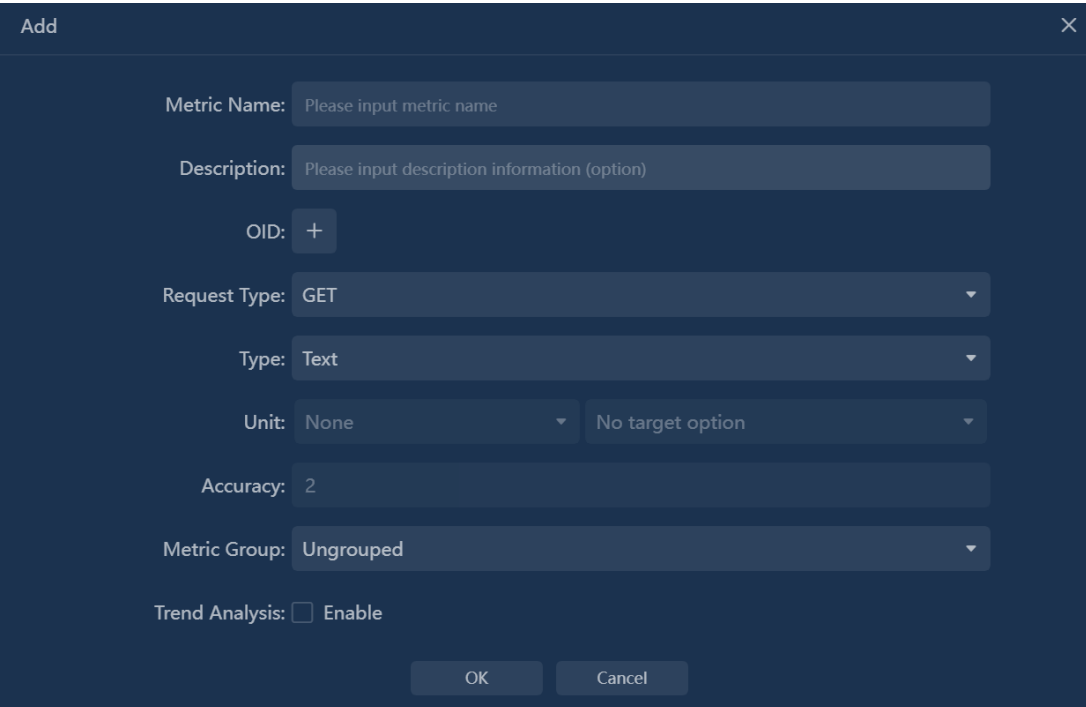
The system has built-in default common indicators, including:

- 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

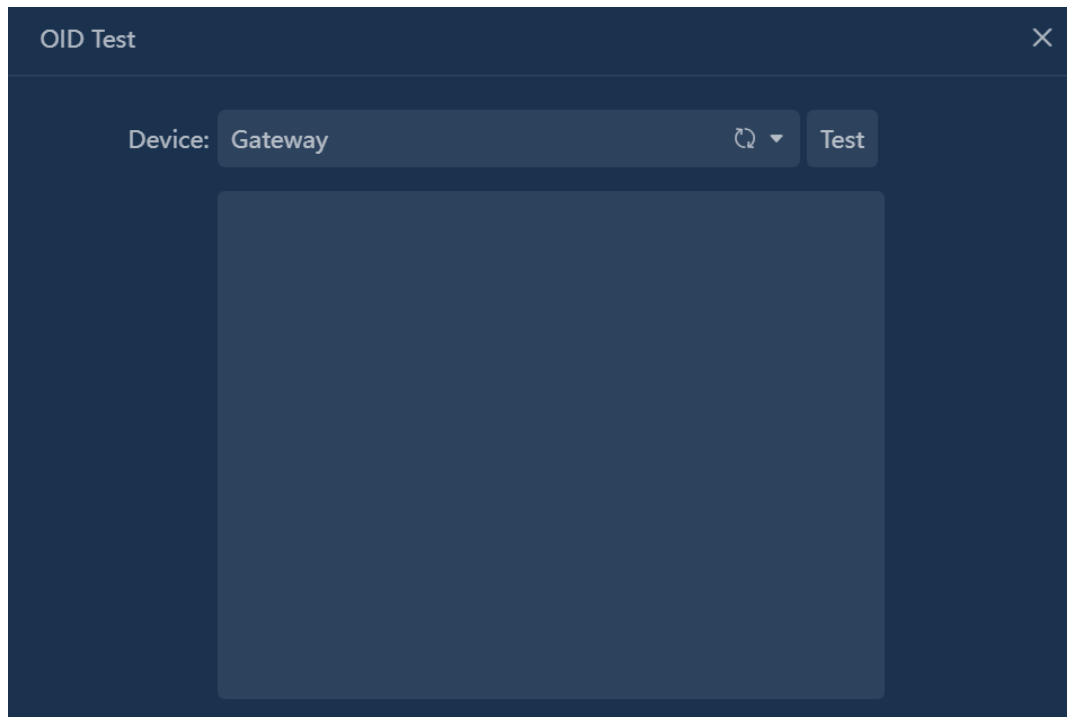
operate	illustrate
OID	Configure the OID query category and OID, and support the configuration of multiple OIDs. Support to quickly add OIDs and test OID availability .
request method	GET , WALK two ways.
value type	Text and numeric types
unit	
Preserve decimal places	
Indicator group	Configure the indicator 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:



### 22.3.4. 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:

Add Calculated Metric

Metric Name: Input name

Function: Difference (current value - last moment value)

Request Type: GET

Field: Single Poll Time

Accuracy: 2

Unit Format: None No target option

Metric Group: Ungrouped

Trend Analysis:  Enable

Absolute Value:  Enable

OK Cancel

Calculation functions support difference, percentage, and divide .

In the calculation field, you can select common indicators and calculated indicators.

## 22.4. Analyze

### 22.4.1. 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:

Action	Name	Current Time	IP Address	Type	Description	NetFlow Status	Rx bps	Tx bps	Interfaces	Poll Status
	Gateway		192.168.16.1	Gateway		netflow255.7	0.00 bps	0.00 bps		Failed
	taylor		192.168.16.163	Other		netflow255.7	0.00 bps	0.00 bps		Failed
	nChronos		192.168.120.65	Other		-	0.00 bps	0.00 bps		N/A


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:

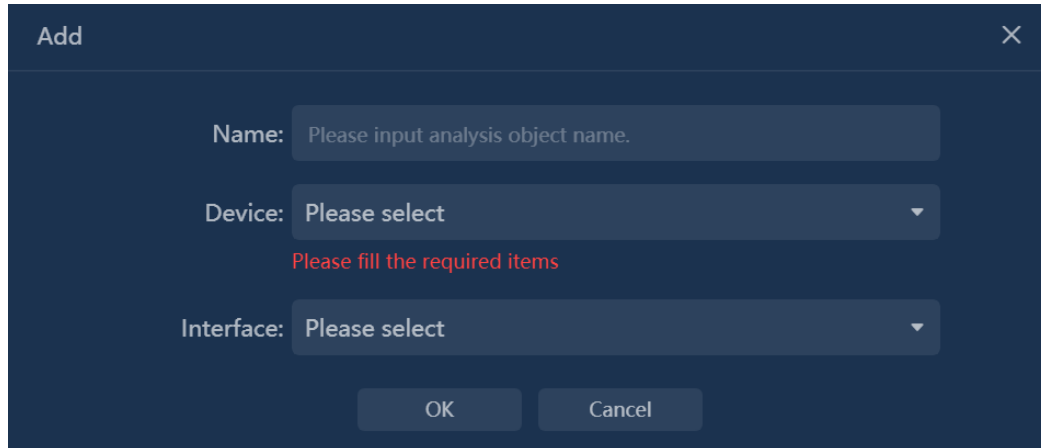
Device Name: nChronos		Device IP: 192.168.120.65		Device Type: Other	
Correlate Link: -		Last Upgrade Time:		Poll Status: N/A	
Interfaces:		Rx bps: 0.00 bps		Tx bps: 0.00 bps	

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.


## 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:



The screenshot shows a dark-themed 'Add' dialog box with a close button (X) in the top right corner. It contains three input fields: 'Name' with a text input field containing the placeholder 'Please input analysis object name.', 'Device' with a dropdown menu showing 'Please select', and 'Interface' with a dropdown menu showing 'Please select'. Below these fields is a red error message: 'Please fill the required items'. At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

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.

## 23. Alerts

### 23.1. Function Introduction

#### 23.1.1. 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.

#### 23.1.2. Functional scenarios

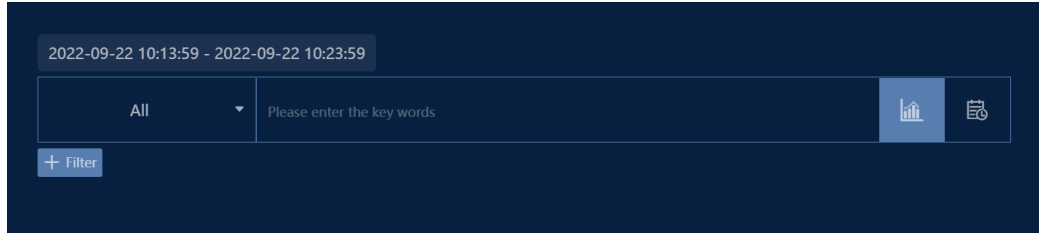
After UPM triggers an alarm, it is directly displayed centrally in the unified alarm log monitoring page, which is suitable for viewing the daily alarm log of UPM and statistical display of alarm information triggered by specific objects, so as to quickly view all relevant alarm information and improve troubleshooting efficiency.

#### 23.1.3. 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.



## 23.2. Alarm display

### 23.2.1. 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.

### 23.2.2. 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.

### 23.2.3. Alarm Log

2022-09-22 10:13:59 - 2022-09-22 10:23:59

All | Please enter the key words

+ Filter

Acknowledge | Please input keywords

Operation	Alarm Severity	Alarm module	Trigger Time	Alarm Name	Date	Link	Type	alarm details
⊕	Severe	Terminal Alarm	2022-09-22 10:23:00	test	2022-09-22 10:23:00	Demo	Terminal Group Alarm	area2, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:23:00	test	2022-09-22 10:23:00	Demo	Terminal Group Alarm	area1, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:23:00	test	2022-09-22 10:23:00	Demo	Terminal Group Alarm	voip192, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:23:00	test	2022-09-22 10:23:00	Demo	Terminal Group Alarm	area2, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:23:00	test	2022-09-22 10:23:00	Demo	Terminal Group Alarm	area1, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:23:00	test	2022-09-22 10:23:00	Demo	Terminal Group Alarm	voip192, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	area2, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	area1, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	voip192, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	area2, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	area1, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	voip192, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	area2, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	area1, Terminal Count0 == 0, Span1.0min
⊕	Severe	Terminal Alarm	2022-09-22 10:22:00	test	2022-09-22 10:22:00	Demo	Terminal Group Alarm	voip192, Terminal Count0 == 0, Span1.0min

The current page 1, total 2 pages, total 24 records. Show 20 records per page.

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.

2022-09-22 10:13:59 - 2022-09-22 10:23:59

All | Please enter the key words

+ Filter

Acknowledge | Please input keywords

Operation	Alarm Severity	Alarm module	Trigger Time	Alarm Name	Date	Link	Type	alarm details
⊖	Severe	Terminal Alarm	2022-09-22 10:23:00	test	2022-09-22 10:23:00	Demo	Terminal Group Alarm	area2, Terminal Count0 == 0, Span1.0min

Alarm Severity: Severe

Alarm module: Terminal Alarm

Trigger Time: 2022-09-22 10:23:00

Alarm Name: test

Date: 2022-09-22 10:23:00

Duration: 1.0min

Link: Demo

Category: Sensitive information

Type: Terminal Group Alarm

alarm details: area2, Terminal Count0 == 0, Span1.0min

Trigger Condition: Terminal Count0 == 0

Process Status: Active

The current page 1, total 2 pages, total 24 records. Show 20 records per page.

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.



## 24. Smart Baseline

### 24.1. Features

#### 24.1.1. The term

##### CSAIS

The abbreviation of Colasoft Artificial Intelligence Server is an intelligent baseline detection system independently developed by Colasoft.

#### 24.1.2. 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.

#### 24.1.3. 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.

#### 24.1.4. 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.

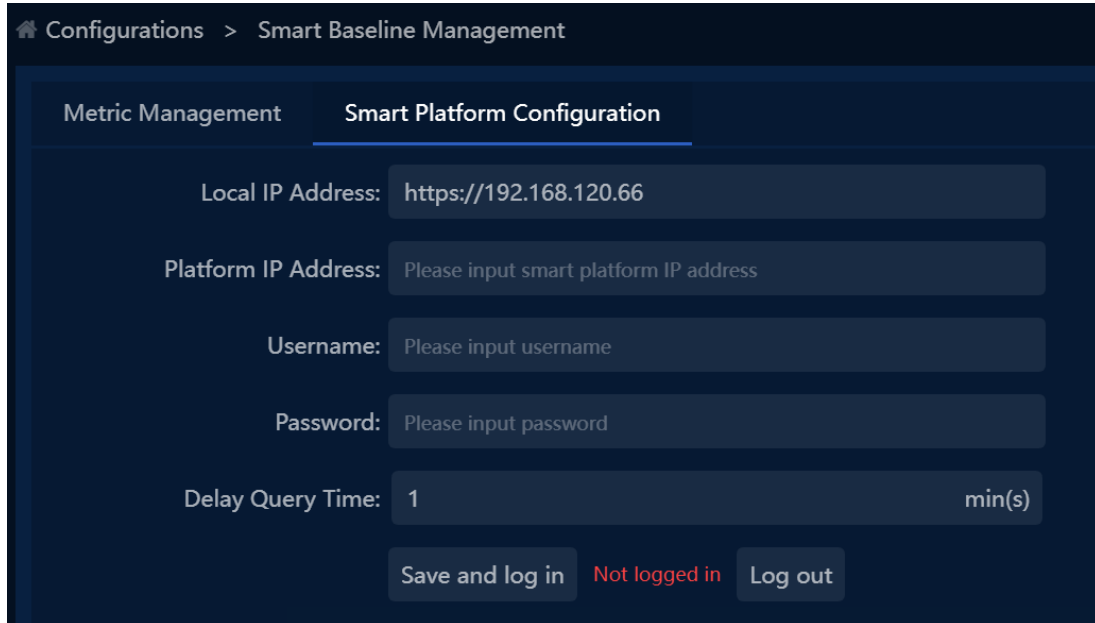
CSAIS is responsible for baseline data generation and anomaly detection, and transmits the results to UPM.

### 24.2. Operation guide

#### 24.2.1. 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.

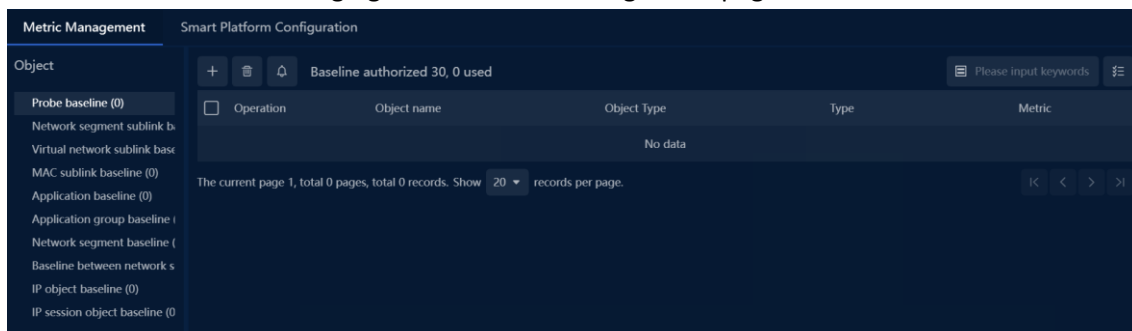
### 24.2.2. Add monitoring object

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

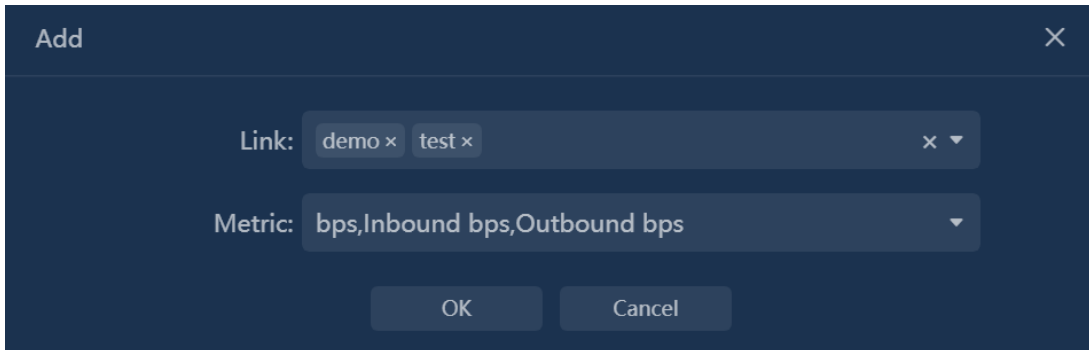
Click on the UPM menu navigation "Configuration" -> "Intelligent Baseline Management" -> "Metrics Management".

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.



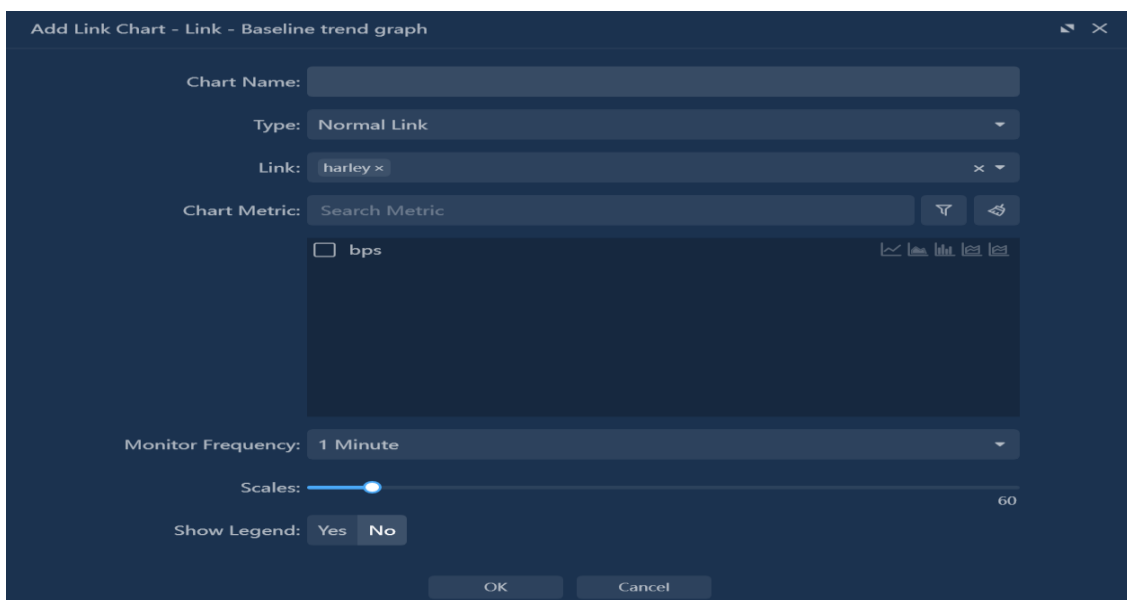
The table on the right: displays the monitored objects and indicators. The indicator names of the same objects are concatenated and displayed in the "Indicators" column.

- 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

In custom monitoring, trend graph components of common links, aggregated links, network segment sub-links, virtual interface sub-links, MAC sub-links, applications, application groups, network segments, network segments, IP, and IP sessions Baseline monitoring can be added directly.

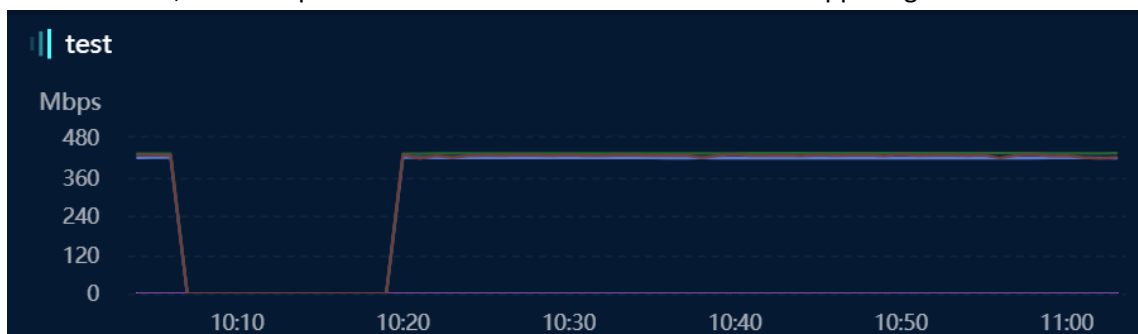
As shown in the figure below, when the monitoring frequency is selected as 1 minute, when the mouse moves over the indicator , select Smart Baseline to perform baseline monitoring of the indicator.



### 24.2.3. 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.



## 24.3. 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.

## 25. Kafka log collection

### 25.1. Features

#### 25.1.1. 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.

#### 25.1.2. Functional scene

1. Perspective monitoring and multi-dimensional perspective statistics of third-party data.
1. Retrieval viewing of third-party data.
2. Integrated collection of large amounts of third-party data.

#### 25.1.3. 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.

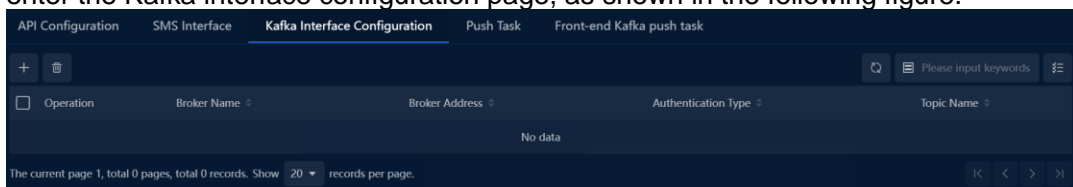
## 25.2. Operation guide

This section mainly introduces the configuration used for Kafka data consumption.

### 25.2.1. 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 screenshot shows a dark-themed 'Add' dialog box with a close button (X) in the top right corner. The fields are as follows:

- Broker Name:** Unique name (required)
- Broker Address:** Format is IP: port, supports IPv4 and IPv6, multiple addresses are separated by Enter
- Authentication Type:** SASL
- Username:** Please enter the username preset by broker (required)
- Password:** Please enter the password preset by broker (required)
- Compression format:** Null
- Send bytes:** 5000 (with a 'Byte' unit selector)
- Topic Name:** Please enter name (required) (with a '+' icon)

Buttons: OK, Cancel

The description of each configuration field in the pop-up box is shown in the following table.

Field Name	describe
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	describe
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**

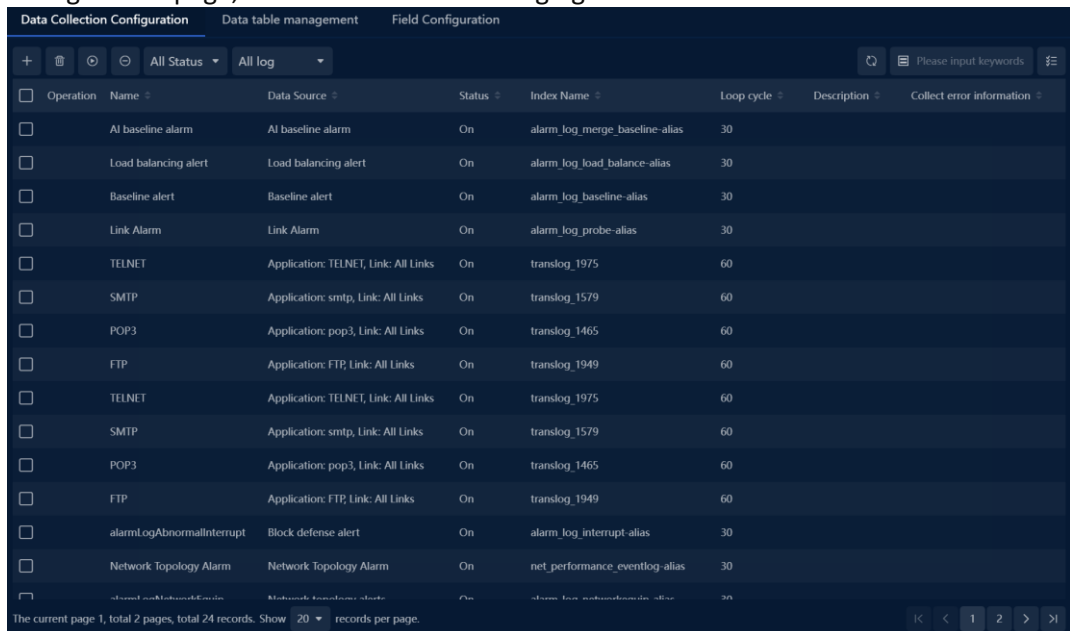
Kafka version should be at least a new version after 1.0.0 to avoid problems caused by version negotiation errors.

- Click the "OK" button to complete the configuration of the Kafka interface.

## 25.2.2. Acquisition configuration

The acquisition configuration steps are as follows:

- > "Data Collection Configuration" from the menu to enter the data collection configuration page, as shown in the following figure.



- 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.

Field Name	describe
name	Required. It is used to set the collection task name. Duplicates are not allowed.
Broker address	Required, single choice, you can choose the Broker that has been configured on the kafka interface.
Topic	Required, multiple choices, you can choose Topic that has been configured on the kafka interface .
data index name	Required, the index name used for configuration data retrieval in the database.
Data storage time	Required, the default is 60 days. Configure the length of time that the acquired data is stored in the database.
describe	Optional, describe the details of this task
Field parsing lua script	parsing script that requires special processing such as formats and fields .

**Note**

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.

### 25.2.3. 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".



## 26. ARP Log Analysis

### 26.1. 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.

#### 26.1.1. 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.

### 26.2. Operation Guide


#### 26.2.1. 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:

4. Choose Configuration > Log Analysis Collection Configuration from the menu. The log collection configuration page is displayed.

5. Click the Data Collection Configuration TAB.

6. Move the mouse pointer to , and choose DataSourceProtocol Log from the drop-down list box  
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.

Field Name	Description
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.

## 26.3. 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.

### 26.3.1. Data Dictionary Management

The data dictionary is mainly used to configure the corresponding relationship between field encoding and field display name.

Take the newly added gratuitous 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:

Configurations > Data Dictionary Management

Action	Status	Category	Value	Name
<input type="checkbox"/>	Enable	web dictionary	200	OK
<input type="checkbox"/>	Enable	web dictionary	404	Not found
<input type="checkbox"/>	Enable	web dictionary	500	Internal server error

Current page 1, total 1 page(s), total 3 record(s). Show for every page: 20 record(s)


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.

7, Click OK to complete the configuration of the protocol log collection task.

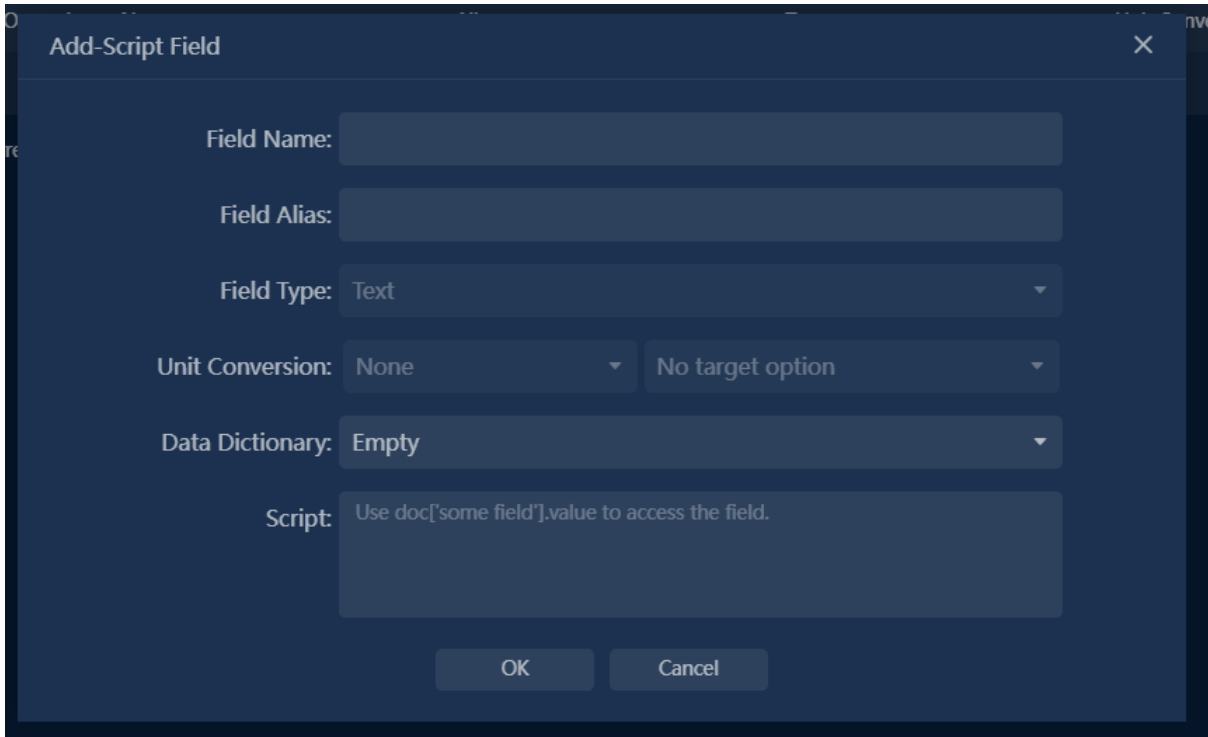
### 26.3.2. Filed Configuration

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.
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.

Click OK to complete the configuration of the protocol log collection task.

### 26.3.3. ARP log search

On the ARP log search page, you can perform statistical analysis on the collected ARP logs as follows:

13. Choose Search;The log search page is displayed.

14. Select the configured ARP log collection task from the log drop-down list box.
15. Select a time frame.
16. 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.
17. Click the "Query" button to view the matched ARP log.

#### **26.3.4. 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

A host that is suspected of initiating ARP spoofin

## 27. 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.