

---

**inspur 浪潮**



# Inspur Physical Infrastructure Manager V6.0.0 User Manual

Version **V1.1**

Release Date **2020-10-30**

## Legal Notice

Copyright © Inspur 2017. All rights reserved

No part of this document may be reproduced or modified or transmitted in any form or by any means without prior written consent.

Note: The products, services or features you purchase should be subject to Inspur Group's commercial contracts and terms. All or part of the products, services, or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Inspur Group makes no express or implied statement or warranty on the contents of this document. The content of this document may be updated from time to time due to product version upgrades or other reasons. Unless otherwise agreed, this document is intended as a guide only, and all statements, information, and recommendations in this document do not constitute any express or implied warranty. Inspur retains ownership of the software and all related intellectual property rights. Any entity that obtains or uses the software shall respect and protect Inspur and related rights holders to the software and related intellectual property rights in accordance with the provisions of laws and regulations and in accordance with the provisions of legal agreements. The respect and protection of the rights shall not be less than the obligations of Inspur to other rights holders.

“Inspur” is a registered trademark of Inspur Group.

“Windows” is a registered trademark of Microsoft Corporation.

“Intel” and “Xeon” are registered trademarks of Intel Corporation.

Other trademarks belong to their respective registered companies.

Service Phone: 4008600011  
Address: Inspur Electronic Information Industry Co.,  
Ltd., 1036 Inspur Road, Jinan, China  
Postcode: 250101

# Foreword

## Overview

This document introduces Inspur Physical Infrastructure Management Platform (hereinafter referred to as “ISPIM”) product introduction, basic operations, main functions, answers to frequently asked questions, etc.

## Audience

This document is intended for the following engineers:

- Technical Support Engineer
- Maintenance Engineer

## Security Statement

1. The product you purchased may obtain or use certain personal data of the user (such as account number, phone number, email address, user IP address, etc.) in the course of business operation or fault location. Therefore, you are obligated to comply with the laws of the applicable country or region and formulate necessary user privacy policies and take sufficient measures to ensure that users' personal data are fully protected.






2. This product needs to apply to the customer and obtain the customer's authorization to collect customer network data, and only collect data within the scope of the customer's authorization during the collection process. Before the customer network data is transmitted out of the customer network, it needs to apply to the customer and obtain the customer's authorization, and at the same time, comply with local laws and regulations. Customer network data transfer operations must strictly comply with the purpose authorized by the customer, and the transferred data is only used to provide services to the customer.

3. Before the product version upgrade or patch installation, it is recommended that you check the product hash value or digital signature, verify the legitimacy of the upgraded software, and avoid illegal tampering or replacement of the software, which may bring security risks to users.

4. Inspur has established a comprehensive emergency response and handling mechanism for product security vulnerabilities to ensure that product security issues are dealt with as soon as possible. If you find any security issues during the use of this product, or seek necessary support for product security vulnerabilities, please contact Inspur customer service personnel directly.

## Symbol Conventions

The following symbols may appear in the text, and their meanings are as follows:

Symbol	Description
 Danger	Warning inevitable dangerous situation that could cause death or serious bodily injury, or serious damage to the server.
 Warning	Warning of potentially dangerous situations which, if not avoided, may result in death, serious personal injury, or server damage.
 Careful	Used to warn of potentially dangerous situations which, if not avoided, may lead to moderate, minor personal injury, or a server failure.
 Notice	Transmitting device or environmental safety warning information, if not avoided, may lead to device damage, data loss, degradation of equipment performance or other unpredictable results, "Attention" does not involve personal injury.
 NOTE	For highlighting important/key information, best practices, tips, etc., "Instructions" is not a safety warning information, does not involve personal, equipment and environmental injuries.

## Revision History

Version	Date	Description
V1.1	2020-10-30	<ul style="list-style-type: none"> <li>● Second release</li> <li>● Added log management, monitoring tasks, network topology, service &amp; support, repository management</li> </ul>



---

Version	Date	Description
		functions
V1.0	2020-03-30	First release

# Table of Contents

FOREWORD .....	III
OVERVIEW .....	III
AUDIENCE .....	III
SECURITY STATEMENT .....	III
SYMBOL CONVENTIONS .....	IV
REVISION HISTORY .....	IV
TABLE OF CONTENTS .....	VI
1 DOCUMENTATION GUIDE .....	1
2 OVERVIEW .....	2
2.1 INTRODUCTION .....	2
2.2 TERMS AND DEFINITIONS .....	2
2.2.1 Related Terms .....	2
2.2.2 Role Definition .....	3
2.3 SYSTEM ICON DESCRIPTION .....	4
3 BASIC OPERATION .....	5
3.1 LOG IN TO ISPIM .....	5
3.2 MODIFY PASSWORD .....	5
3.3 SIGN OUT .....	5
3.4 SHORTCUT TOOL .....	6
4 QUICK GUIDE .....	7
4.1 REQUIREMENTS .....	7
4.2 QUICK START .....	7
5 HOMEPAGE .....	9
5.1 CUSTOM HOMEPAGE .....	10
5.2 ADD SERVERS .....	11
5.3 ADD ALARM RULES .....	11
6 ASSET MANAGEMENT .....	12
6.1 EQUIPMENT MANAGEMENT INSTRUCTIONS .....	12
6.1.1 Equipment Type .....	12
6.1.2 Equipment Management Protocol .....	13
6.1.3 Equipment Number and License Capacity .....	14
6.2 SERVER MANAGEMENT .....	14
6.2.1 Add Servers .....	15
6.2.2 View Server List .....	18
6.2.3 View Server Detail .....	19
6.3 CABINET MANAGEMENT .....	29
6.4 BLADE MANAGEMENT .....	29
6.4.1 Add Blade .....	30
6.4.2 View Blade List .....	31
6.4.3 View Blade Detail .....	32
6.5 ALL-IN-ONE DEVICE MANAGEMENT .....	34

6.5.1 Add All-in-one Device.....	34
6.5.2 View All-in-one Device List.....	36
6.5.3 View All-in-one Device Detail .....	37
6.6 EDGE DEVICE MANAGEMENT .....	41
6.6.1 Add Edge Device .....	41
6.6.2 View Edge Device List.....	44
6.6.3 View Edge Device Detail .....	44
6.7 STORAGE MANAGEMENT .....	49
6.7.1 Add Storage Device.....	49
6.7.2 View Storage Device List.....	52
6.7.3 View Storage Detail.....	53
6.7.4 View Disk Array Detail .....	59
6.8 NETWORK DEVICE MANAGEMENT .....	64
6.8.1 Add Network Device.....	64
6.8.2 View Network Device List .....	66
6.8.3 View Switch Detail.....	67
6.8.4 View Router Detail.....	72
6.8.5 View SDN Device Detail.....	72
6.9 SECURITY DEVICE MANAGEMENT .....	76
6.9.1 Add Security Device.....	76
6.9.2 View Security Device List.....	78
6.9.3 View Firewall Device Detail .....	79
6.9.4 View IDS/IPS Device List.....	83
6.10 GENERAL OPERATION OF EQUIPMENT .....	83
6.11 DATA CENTER MANAGEMENT .....	88
6.11.1 Create Data Center .....	89
6.11.2 Data Center Management .....	92
6.11.3 View Data Center.....	94
6.11.4 Power Consumption Management .....	98
6.11.5 Power Consumption Optimization .....	100
6.12 DEVICE GROUPING .....	106
6.12.1 Custom Group .....	106
6.12.2 Conditional Group.....	107
7 MONITORING .....	108
7.1 LOGICAL CLASSIFICATION OF MONITORING ITEMS .....	108
7.2 ALARM MANAGEMENT .....	109
7.2.1 Current Alarm.....	110
7.2.2 Historical Alarm .....	114
7.2.3 Masked Alarm .....	115
7.3 EVENT .....	116
7.3.1 Event Introduction.....	116
7.3.2 Event Operation.....	117
7.4 LOG MANAGEMENT.....	117
7.5 NOTIFICATION RECORDS .....	118

7.6 REPAIR RECORDS .....	119
7.7 MONITORING SETTINGS.....	120
7.7.1 Alarm Rules .....	120
7.7.2 Notification Rules.....	123
7.7.3 Masking Rules.....	127
7.7.4 Repair Rules .....	129
7.7.5 Redefine Rules .....	131
7.7.6 Notification Template .....	133
7.7.7 Southbound Trap Settings .....	134
7.7.8 Monitoring Tasks.....	135
8 CONTROL MANAGEMENT .....	137
8.1 REPOSITORY .....	137
8.1.1 OS Image Library .....	138
8.1.2 Firmware File Library .....	139
8.1.3 Bundle Management.....	141
8.2 FIRMWARE UPGRADE .....	142
8.2.1 Read Before Upgrading.....	143
8.2.2 BMC/BIOS Upgrade .....	144
8.2.3 Other Firmware Upgrade.....	145
8.2.4 Check After Upgrade.....	148
8.3 FIRMWARE CONFIGURE .....	149
8.3.1 BIOS Configure.....	149
8.3.2 BMC Configure.....	150
8.3.3 RAID Configure.....	152
8.4 POWER MANAGEMENT .....	154
8.5 OS DEPLOYMENT .....	154
8.5.1 Requirements.....	154
8.5.2 OS Deployment .....	155
8.6 BASELINE MANAGEMENT.....	156
8.6.1 Baseline Template .....	157
8.6.2 Baseline Strategy .....	159
9 TOPOLOGY MANAGEMENT.....	162
9.1 VIEW DATA CENTER TOPO .....	162
9.2 3D ROOM MANAGEMENT.....	163
9.2.1 Edit Room Layout .....	164
9.2.2 View Room Information.....	165
9.2.3 View Cabinet Detail .....	167
9.3 NETWORK TOPOLOGY .....	168
10 REPORTS MANAGEMENT.....	172
10.1 MAINTENANCES MANAGEMENT.....	172
10.2 ALERTS MANANGEMENT.....	173
10.3 ASSETS MANAGEMENT .....	174
11 SYSTEM MANAGEMENT .....	176
11.1 USER MANAGEMENT .....	176

11.1.1 Role Management.....	176
11.1.2 User Management.....	178
11.1.3 User Group Management.....	181
11.2 LOG MANAGEMENT.....	182
11.3 TASK.....	182
11.4 LICENSE MANAGEMENT .....	183
11.4.1 Activate the License .....	183
11.4.2 License Version Description .....	184
11.5 NORTHBOUND MANAGEMENT.....	186
11.5.1 Alert Forwarding .....	186
11.5.2 NFV .....	188
11.6 SERVICE&SUPPORT .....	188
11.7 SYSTEM SETTINGS.....	190
11.7.1 Set System Params .....	190
11.7.2 Services Management.....	191
11.7.3 Certificate Management .....	197
11.7.4 Proxy Servers.....	197
11.7.5 NOTE Servers .....	198
11.7.6 ISFM Config.....	200
11.7.7 Authentication Server .....	201
11.7.8 Model Mappers.....	201
11.7.9 Collector Settings .....	202
12 FAQ.....	208
12.1 ISPIM CANNOT LOG IN SUCCESSFULLY, HOW TO SOLVE IT? .....	208
12.2 AFTER ISPIM IS REINSTALLED DUE TO A FAILURE, DO I NEED TO REACTIVATE IT? .....	208
12.3 DOES THE MANAGED DEVICE OCCUPY THE LICENSE CAPACITY IF IT IS REINSTALLED DUE TO A FAULT?.....	208
12.4 WHAT EQUIPMENT DOES ISPIM SUPPORT? .....	209
12.5 HOW TO CHECK SNMP TRAP SETTINGS?.....	212
A GETTING HELP.....	212
A.1 COLLECTING FAULT INFORMATION .....	212
A.2 USING PRODUCT DOCUMENTATION .....	213
A.3 OBTAINING TECHNICAL SUPPORT.....	213

# 1 Documentation Guide

**Table 1-1 Documentation Guide**

Type	Type	Description	Document
Product Overview	Product White Paper	This document describes the architecture, positioning, features, functions of ISPIM.	<a href="#">《Inspur Physical Infrastructure Manager(ISPIM) V6.0.0 Product White Paper》</a>
Installation and Commissioning	Deploy Guide	This document describes how to install ISPIM and provides common operations and troubleshooting methods.	<a href="#">《Inspur Physical Infrastructure Manager(ISPIM) V6.0.0 Deploy Guide》</a>
Operation	User Manual	This document describes how to configure and manage ISPIM and provides specification operation instructions.	<a href="#">《Inspur Physical Infrastructure Manager(ISPIM) V6.0.0 User Manual》</a>

## 2 Overview

### 2.1 Introduction

Inspur Physical Infrastructure Manager (hereinafter referred to as “ISPIM”) is a hardware intelligent operation and maintenance management platform for industry data centers. The platform has functions such as resource management, fault monitoring, performance monitoring, energy consumption management, report statistics, topology display, server fault diagnosis, automatic repair, firmware upgrade/configuration, and OS deployment.

With the help of the ISPIM platform, users can realize the unified management of servers, cabinets, blades, all-in-one devices, edge devices, network equipment, security equipment, storage and other equipment, which truly promotes the intelligent management of data centers. ISPIM can help users build unattended data centers, help companies improve operation and maintenance efficiency, reduce operation and maintenance costs, and ensure the safe, reliable, and stable operation of data centers.

ISPIM can be widely used in public clouds, private clouds, data centers, operators, and enterprise customers. ISPIM can be deployed in multiple scenarios such as AI, HPC, Internet, and smart cities. It also provides interfaces such as Restful and SNMP to facilitate user integration and docking.

### 2.2 Terms and Definitions

#### 2.2.1 Related Terms

To facilitate users to understand the related concepts of the ISPIM, the basic terminology is shown in Table 2-1.

Table 2-1 Terms

Term	Description	Explanation
IPMI	Intelligent Platform Management Interface	ISPIM discovers the server through the IPMI protocol and polls the server regularly to realize active monitoring. In addition, IPMI commands can also be used for server firmware configuration, power operation and other functions.

Term	Description	Explanation
SNMP	Simple Network Management Protocol	ISPIM receives server Trap through the SNMP protocol to realize passive monitoring. In addition, the SNMP protocol is also used to collect some server information, such as asset information and performance data.
SMIS	Storage Management Initiative Specification	ISPIM discovers storage devices through the SMIS protocol and polls the storage devices regularly to realize active monitoring.

## 2.2.2 Role Definition

ISPIM includes three types of users: super administrators, operation and maintenance administrators, and general users. The maximum operation authority of each role function is shown in Figure 2-2.

Figure 2-2 Role Permissions

Role	Permissions
Super Administrator	<b>Home page, assets</b> (servers, cabinets, blades, all-in-one devices, edge devices, storage, network equipment, security equipment, data centers, groups), <b>monitoring</b> (alarms, events, logs, notification records, repair orders, settings), <b>control</b> (operation, baseline, repository), <b>topology</b> (3D view, network topology), <b>large screen, reports</b> (maintenance, alarms, assets), <b>system</b> (user, log, job, license, northbound, service & support, settings)
O&M Administrator	<b>Home page, assets</b> (servers, cabinets, blades, all-in-one devices, edge devices, storage, network equipment, security equipment, data centers, groups), <b>monitoring</b> (alarms, events, logs, notification records, repair orders, settings), <b>control</b> (operation, baseline, repository), <b>large screen, reports</b> (maintenance, alarms, assets), <b>system</b> (license)
General User	<b>Home page, assets</b> (servers, cabinets, blades, all-in-one devices, edge devices, storage, network equipment, security equipment, data centers, groups), <b>monitoring</b> (alarms, events, logs, notification records, repair orders, settings), <b>control</b> (operation,



	baseline, repository), <b>large screen, reports</b> (maintenance, alarms, assets), <b>system</b> (license)
--	--



## NOTE

- Users in different roles have access and operation permissions to different functions, as shown in Figure 2-2.
- Unless there are special instructions for the login user in this manual, the default super administrator user (admin/Inspur1!) login is used as an example to introduce functions.

## 2.3 System Icon Description

The description of some icons in ISPIM is shown in Figure 2-3.

Figure 2-3 Icon Description

Icon	Description
	Indicates that the current job or task is running.
	Indicates that the job or task has been executed.
	Indicates that the current device network connection is normal.
	Indicates that the current device network connection is unknown.
	Indicates that the user is enabled.
	Indicates that the user is disabled.
	Indicates that the backup task is being executed.

## 3 Basic Operation

### 3.1 Log in to ISPIM

After ISPIM is successfully installed, enter the following URL in the browser address bar: <host IP> to log in to the platform. Where <Host IP> is the IP address of the server where ISPIM is deployed. The system default user (admin/Inspur1!) can be used to log in to the system when logging in for the first time.



#### NOTE

- When logging in to ISPIM, the browser mandatory requirements for accessing ISPIM are: Chrome57, Firefox52 and above.
- After the ISPIM login fails, you can enter the correct user name, password, and verification code and try to log in again.
- If the password is incorrect for 5 consecutive times, the user will be locked out. The lock time is 30 minutes; if the current user is locked and cannot log in, you can contact the super administrator to unlock it.






### 3.2 Modify Password

After the login is successful, select the <Modify Password> tab in the drop-down box of the logged-in current user in the upper right corner, and the password modification window will pop up. The old password, new password and confirmed password will be displayed in the window, and the user can submit it after modifying the password. To improve account security, it is recommended that users modify their login passwords periodically.

### 3.3 Sign Out

After successful login, select <Sign out> in the drop-down box of the current user at the upper right corner to log out of the system.

## 3.4 Shortcut Tool

Tool	Description
Search	In the navigation bar at the top of ISPIM, click the  icon and enter the device or alarm keywords to fuzzy search related devices.
Favorites	In the navigation bar at the top of ISPIM, click the  icon to quickly view the current user's favorite server list. For details on how to bookmark the server, please refer to <a href="#">Equipment Collection</a> .
Big screen display	In the navigation bar at the top of ISPIM, click the  icon to enter the large screen of ISPIM to view system alarm information, resource view, alarm information and other overview information.
View running jobs	In the navigation bar at the top of ISPIM, click the  icon, and a list of jobs currently running in the system will appear at the bottom of the page. User can view job name, job status, job progress and other information.
View alarm details	In the top navigation bar of ISPIM, hover the mouse over the  icon in the top navigation bar to view the alarm status of the system, including alarm level statistics, alarm content, etc. Click <More> to enter the alarm management page to view alarms related information.

# 4 Quick Guide

## 4.1 Requirements

- **Activate ISPIM:** After accessing ISPIM for the first time, user need to enter the [System] -> [License] page to activate ISPIM. For details on how to activate ISPIM, please refer to “Inspur Physical Infrastructure Management Platform (ISPIM) V6.0.0 Deployment Manual-20201030”.
- **Collector Setting:** Before using the ISPIM, it is recommended to enter the [System] -> [Settings] -> [Collection Settings] page to check the relevant configuration of the collectors:
  - If ISPIM is deployed in a single-node solution: After logging in, it is recommended that the user check whether the IP of the system default collector “Local collector” is “127.0.0.1”.
  - If the user additionally deploys other collectors: After logging in to ISPIM, the user also needs to add and configure the collectors. For detail, see 11.7.9 Collector Settings.

## 4.2 Quick Start

ISPIM can realize the full life cycle management of the managed equipment, including adding equipment, monitoring equipment, configuring equipment, installing operating system, firmware upgrading, intelligent asset management, etc. The quick use instructions of some functions of ISPIM are shown in Figure 4-1.

Figure 4-1 ISPIM Quick Use Instructions

Function	Description	Reference Section
Add Device	The ISPIM supports two ways to manage servers through automatic discovery and batch import.	6.2.1 Add Servers
Monitoring	After the server is successfully managed, ISPIM will automatically collect and monitor relevant information about the server. After a period of time, the system may generate corresponding alarm data.	7 Monitoring

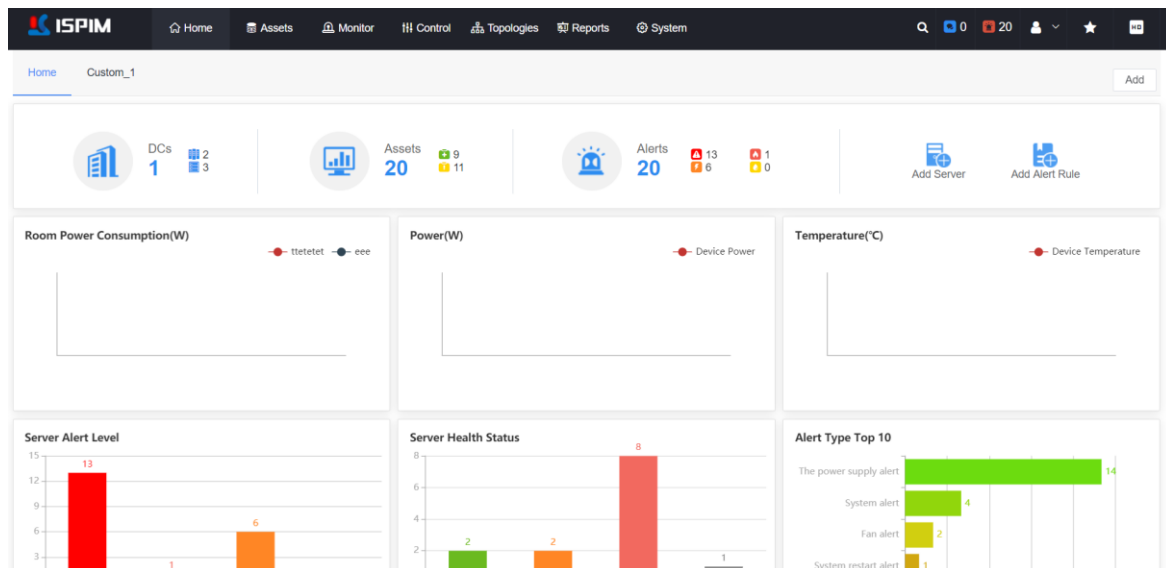
Function	Description	Reference Section
	Users can view equipment alarm information in real time.	
Configure Firmware	According to actual needs, users can configure BIOS, BMC, RAID and other firmware.	8.3 Firmware Configure
OS Deployment	According to actual needs, users can upload the OS image and deploy it to the corresponding device.	8.5 OS Deployment
Upgrade Firmware	ISPIM supports batch upgrade of BMC, BIOS and other firmware.	8.2 Firmware Upgrade
Asset Management	ISPIM supports the information management of the entire life cycle of data center assets, including asset maintenance, exporting asset reports, etc., which is convenient for users to inventory data center assets.	6 Asset Management

# 5 Homepage

Select the “Home” tab in the top navigation bar of ISPIM to enter the home page, as shown in figure Figure 5-1. On the home page, user can view asset statistics, and perform operations such as customizing the home page, adding servers, and adding alarm rules. On the system default homepage, user can view the following content:


- Platform overview information: Support to view global overview information such as data center, asset statistics, alarm statistics in the ISPIM platform. Click the statistics corresponding to the data center, asset statistics or alarm statistics to jump to the corresponding management page to view related detailed information
- Asset usage: Support to view information such as power consumption statistics, power consumption trend statistics, temperature trend statistics, and server alarm statistics in the ISPIM platform. Hover the mouse on each trend graph, user can view the details of the power consumption, temperature, alarms and other indicators of the room at a specified time.

Figure 5-1 Home Page



## NOTE

The descriptions of the alarm status icons are as follows:

-  : Critical alarm, indicating that the device is in a high-risk state and needs to be dealt with immediately.

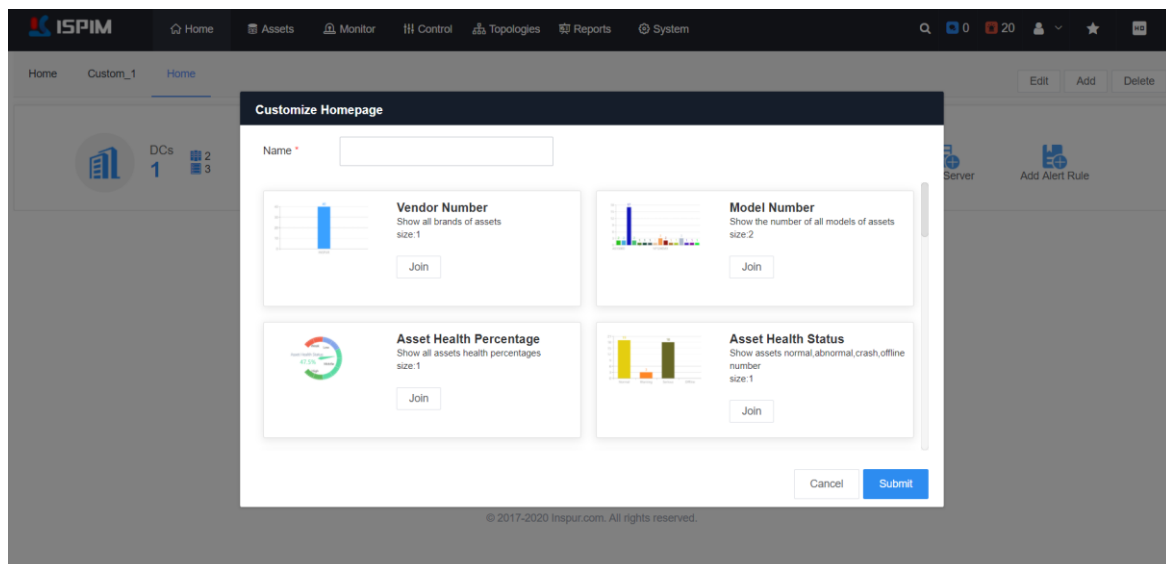
- 🔥 : Serious alarm, indicating that the device is in a dangerous state and needs to be dealt with as soon as possible.
- ⚡ : Moderate alarm, this level of alarm will not have a major impact on the equipment, but it is recommended to take timely measures to prevent fault escalation.
- 🟡 : Minor alarms, alarms of this level can usually be ignored.

## 5.1 Custom Homepage

On the homepage, click the <Add> button in the upper right corner, and the home page window will pop up, as shown in Figure 5-2. Enter the customized home page name in, select each module and click its corresponding <Join> button, and then click <Submit> to add the selected modules to the customized home page.

The statistical modules that can be added to the custom home page are: vendor number statistics, model number statistics, asset health percentage, asset health status, asset usage status, alert severity statistics, brand and status statistics, component alert number statistics, alert type top 10, data center overview statistics.

Figure 5-2 Custom Homepage



### NOTE

- After the custom homepage is added, select the corresponding custom homepage tab to enter

the corresponding custom homepage page.

- Customized homepage: Click the <Edit>, <Add> or <Delete> button above the customized homepage to edit, add or delete the customized homepage.
  - For the system default homepage: only supports viewing, and cannot be edited or deleted.
- 

## 5.2 Add Servers

On the homepage, click the <Add Server> button to enter the server page where user can add servers.

For details about adding servers, see 6.2.1Add Servers.

## 5.3 Add Alarm Rules

On the home page, click the <Add Alert Rule> button to enter the alarm rule page, where user can add alarm rules. For details about alarm rules, see 1Add Alarm Rules.



# 6 Asset Management

In the navigation bar at the top of ISPIM, select the “Assets” tab to enter the asset management module, as shown in Figure 6-1. The asset management module mainly includes equipment management (servers, cabinets, blades, edge devices, all-in-one devices, storage, network equipment, security equipment, etc.), data center management, and equipment grouping functions. Through equipment management, a variety of heterogeneous equipment can be centrally managed on the ISPIM.

Figure 6-1 Asset Management

Name	BMC IP	OS IP	Status	Serial Num...	Asset St...	Vendor	Model	Room	Cabinet	Operation
Inspur_100.2.39.121	100.2.39.121	---	Serious	219300399	Used	Inspur	NF5280M5	---	---	[Icons]
Inspur_100.7.34.39	100.7.34.39	---	Offline	222	Used	Inspur	NF5280M4	---	---	[Icons]
Inspur_100.7.34.40	100.7.34.40	---	Serious	817234660	Used	Inspur	NF5280M4	---	---	[Icons]
Inspur_100.7.34.45	100.7.34.45	---	Warning	215208622	Used	Inspur	NF5280M4	---	---	[Icons]
Inspur_100.7.34.47	100.7.34.47	---	Normal	00001	Used	Inspur	SA5248	---	---	[Icons]
Inspur_100.7.34.51	100.7.34.51	---	Serious	817238829	Used	Inspur	NF5280M4	---	---	[Icons]
Inspur_100.7.34.61	100.7.34.61	---	Serious	218397134	Used	Inspur	NF8480M5	---	---	[Icons]
Inspur_100.7.34.72	100.7.34.72	---	Serious	217379168	Used	Inspur	AS13000-M5	---	---	[Icons]
Inspur_100.7.34.131	100.7.34.131	---	Serious	218613264	Used	Inspur	NF8480M5	eee	444	[Icons]
Inspur_100.7.34.132	100.7.34.132	---	Serious	218584178	Used	Inspur	NF8480M5	---	---	[Icons]

## 6.1 Equipment Management Instructions

### 6.1.1 Equipment Type

The devices supported by the ISPIM platform include: servers, cabinets, blades, all-in-one devices, edge devices, storage devices, network devices, and security devices.



The scope of ISPIM asset management equipment management includes: Inspur's full range of products (including general servers, AI intelligent servers, blade servers, all-in-ones and other high-end server products) and third-party equipment.

## 6.1.2 Equipment Management Protocol

The process of adding different types of equipment is similar, the only difference lies in the authentication protocol type and protocol configuration parameters. For details, please refer to the actual page. The parameter configuration descriptions of different protocols are shown in Table 6-1.

Table 6-1 Parameter Instructions for Different Protocols

Protocol	Parameter Instruction
IPMI	<ul style="list-style-type: none"> <li>● Servers, cabinets and blades support IPMI protocol.</li> <li>● Need to configure IPMI username/password. For the Inspur server, the username and password of the IPMI protocol is the username and password of BMC, and the default is admin/admin.</li> </ul>
SNMP	<ul style="list-style-type: none"> <li>● Servers, blades, storage devices, switches, routers, firewalls and IDS/IPS devices support SNMP protocol.</li> <li>● Need to configure the SNMP version and related parameters of the corresponding version. <ul style="list-style-type: none"> <li>- For V2c, only the community name needs to be configured.</li> <li>- For V3, user need to configure protocol parameters such as username, authentication key, authentication level, authentication algorithm, privacy algorithm, and privacy key.</li> </ul> </li> </ul>
Redfish	<ul style="list-style-type: none"> <li>● Only the server supports the Redfish protocol.</li> <li>● Protocol parameters such as protocol, port, redfish username and password need to be configured.</li> </ul>
SSH	<ul style="list-style-type: none"> <li>● Only the server supports the SSH protocol.</li> <li>● User need to configure protocol parameters such as username, password, and port.</li> </ul>
SMIS	<ul style="list-style-type: none"> <li>● Only storage devices support the SMIS protocol.</li> <li>● Need to configure SMI-S user name, password, port number, access protocol (http/https), namespace, IP.</li> </ul>
HTTP	<ul style="list-style-type: none"> <li>● All-in-one servers, edge devices, distributed storage and SDNs devices support the HTTP protocol.</li> </ul>

---

Protocol	Parameter Instruction
	<ul style="list-style-type: none"><li>It is necessary to configure parameters such as protocol (http/https), port, user name, and password.</li></ul>

---

**NOTE**

ISPIM supports the collection of in-band performance data of equipment through the in-band agent software-Inspur management driver software (ISMD), so as to achieve more comprehensive equipment information collection and monitoring. For ISMD products, please refer to “Inspur Management Driver Software (ISMD) User Manual” for details.

---

### 6.1.3 Equipment Number and License Capacity

The ISPIM managed device number is limited by the license capacity. Each time a device is added to the ISPIM platform, it will occupy a license capacity. For license management, see 11.4 License Management for details.

---

**NOTE**

ISPIM manages the number of licenses based on the device SN. Even if the managed device is deleted, the device still occupies one license capacity.

---

## 6.2 Server Management

The types of ISPIM managed servers include the full range of Inspur products, such as general-purpose servers, AI smart servers, blade servers, and third-party servers. For third-party equipment, please refer to the “ISPIM Specification List”. On the server management page, user can perform operations such as adding, bookmarking, resetting monitoring rules, resetting protocols, editing, and deleting servers.

## 6.2.1 Add Servers

In the ISPIM platform, there are two ways to add servers: “auto discovery” and “batch import”:

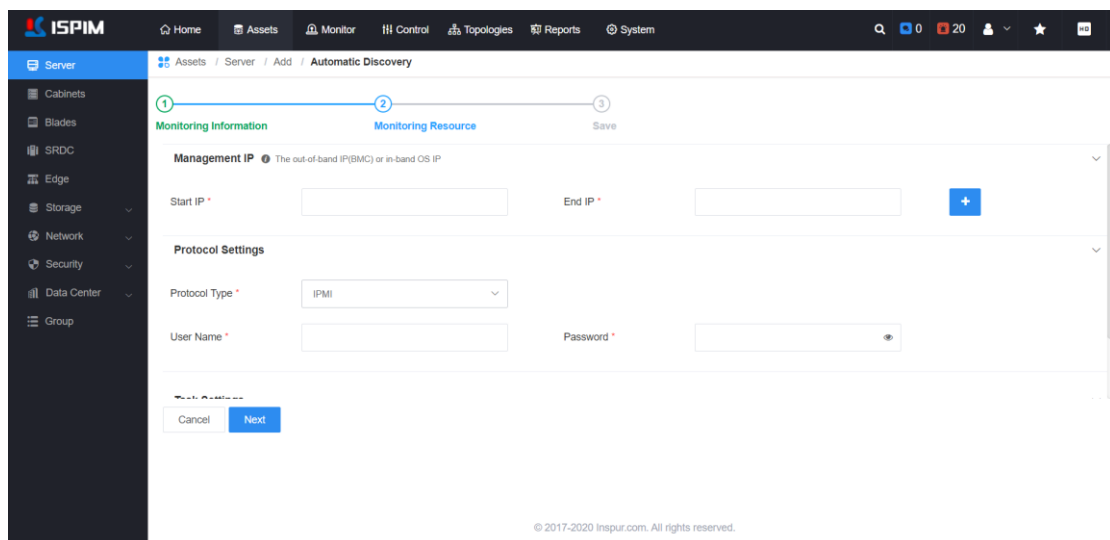
- Automatic discovery: The server can be automatically discovered by specifying the IP range of the device, and the discovery task can be executed periodically.
- Batch import: User can add devices in batches by using an excel template containing device management protocol information. When importing servers in batches, their data center and room cabinet information will also be imported automatically. Support importing 1000+ devices at a time.

### 1. Automatic Discovery


To add a server in ISPIM using “auto discovery” mode, the operation is as follows:

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** Click <Add>, select “Auto Discovery” in the drop-down box, and enter the automatic discovery server configuration page, as shown in the figure below.



**Step 3** Input information such as the IP address, protocol parameters, and task type.

- Configure the server IP range: When adding multiple servers at the same time, the first three parts of the server's starting IP and ending IP must be the same (ISPIM defaults to 255.255.255.0 as the subnet mask); if the server is located in a different network segment, click the  icon to add multiple IP ranges. To add a single device, enter the same start IP and end IP.

- Protocol Parameters: Select the protocol type and configure the relevant parameters of the protocol.
- Task Type: Select task category.
  - When selecting “Auto Discovery”, user needs to configure the task name, task frequency, and start time, and the subsequent steps will not be triggered. After that, user can view the task execution status in the task center. For details about the task center, please refer to 11.3Task.
  - When selecting “Immediate Discovery”, user needs to click <Next> to enter the asset scanning step and start scanning the server.

**Step 4** After the scan is complete, click <Next>, configure the trap switch settings and click <Submit>.

- “Trap Switch Settings” is selected as “Open”.
  - For Inspur servers, ISPIM will automatically set the BMC Trap report address of the server to the ISPIM IP.
  - For servers from other vendors, after the device is added, user needs to manually modify the device’s BMC trap report address to the ISPIM IP.
- When "Trap Switch Setting" is selected as "Off", ISPIM will not set the server's BMC trap report address as the ISPIM IP. ISPIM will not receive trap alarm related information. It is not recommended to set "Trap Switch Setting" to "Off".

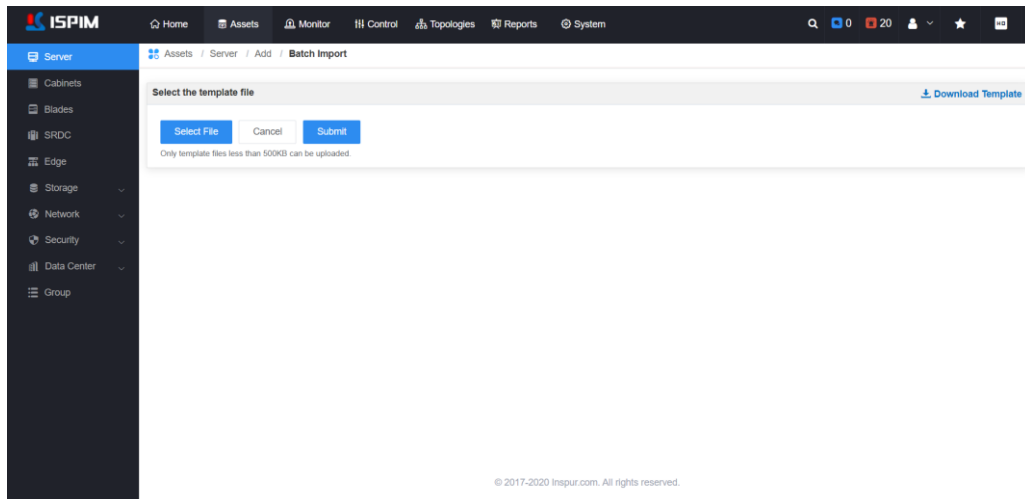
---End

## 2. Batch Import

To add servers in ISPIM by "Batch Import", the operation is as follows:

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** Click <Add> and select "Batch Import" in the drop-down box to enter the batch import page, as shown in the figure below.



**Step 3** Click <Download Template>, edit the downloaded template and configure server related information.

- The fields identified by "\*" in the template are required information, such as asset name, BMC IP address, and IPMI protocol authentication information.
- For Inspur series servers, SNMP protocol information can be omitted.
- If there is data center, room, cabinet, and contact email information in the template, ISPIM will automatically create it and associate it with the server.

**Step 4** After editing the template, click <Select File> to upload the edited template file, and click the <Submit> button to start scanning the servers.

**Step 5** After the scan is complete, click <Next>, configure the trap switch settings and click <Submit>.

- "Trap Switch Settings" is selected as "Open".
  - For Inspur servers, ISPIM will automatically set the BMC Trap report address of the server to the ISPIM IP.
  - For servers from other vendors, after the device is added, user needs to manually modify the device's BMC trap report address to the ISPIM IP.
- When "Trap Switch Setting" is selected as "Off", ISPIM will not set the server's BMC trap report address as the ISPIM IP. ISPIM will not receive trap alarm related information. It is not recommended to set "Trap Switch Setting" to "Off".

----End

## 6.2.2 View Server List

After adding the server device, user can view the managed server information in the server list, as shown in Figure 6-2. In the server list, user can view the server name, BMC IP, server status, serial number, asset status, model, cabinet and other related information.

- Server name: The default format is "vendor\_management IP". Click the server name to view the server details.
- BMC IP: Click to jump to the login page of the device BMC. For the Inspur server, the user name and password for BMC login is admin/admin by default.
- Room/cabinet: The information is empty by default and needs to be specified during batch import or manually.

Table 6-2 Server List Operations






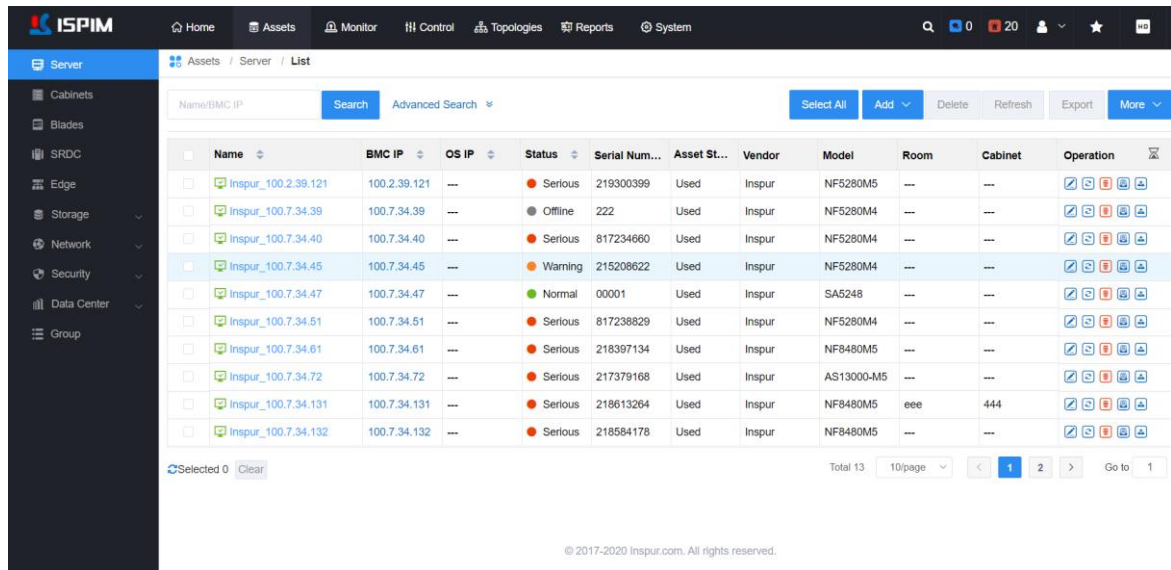
Operation	Description
	Click this icon to edit the basic information and protocol configuration of the server.
	When component asset changes occur to the server (such as hard disk addition/replacement), click this icon to manually synchronize hardware information once.
	Click the icon and confirm in the pop-up window to delete the corresponding server.
	Click this icon to enter the KVM management page. KVM related parameters can be set as needed to achieve the purpose of remotely managing equipment.
	Click this icon to export the corresponding server log.

Figure 6-2 Server List Page



NOTE

User can click the icon to customize the server parameters displayed in the server list.

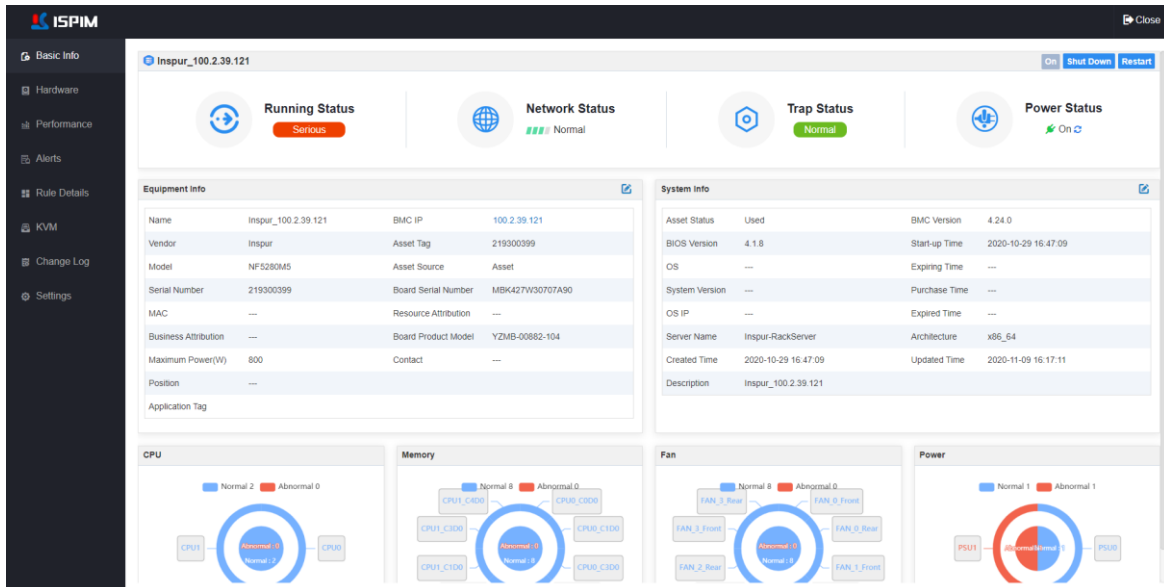
### 6.2.3 View Server Detail

In the server list, click on a server name to enter the server details page, as shown in Figure 6-3. In the server details page, user can view the basic information, hardware information, performance data, alarm list, rule details, KVM, change records, and server settings of the server.

- Network status: It is used to indicate the network connectivity between ISPIM and the server. When the status is weak, it is recommended to check the network connection.
- Trap status: It is used to indicate whether the ISPIM and server SNMP trap are configured normally. When the status is abnormal, ISPIM will not be able to receive traps from the server correctly.

Figure 6-3 Server Detail Page






## 1. Basic Info


On the basic information page, user can view the server's operating status, network status, trap status, power status, device details, system information and other information.

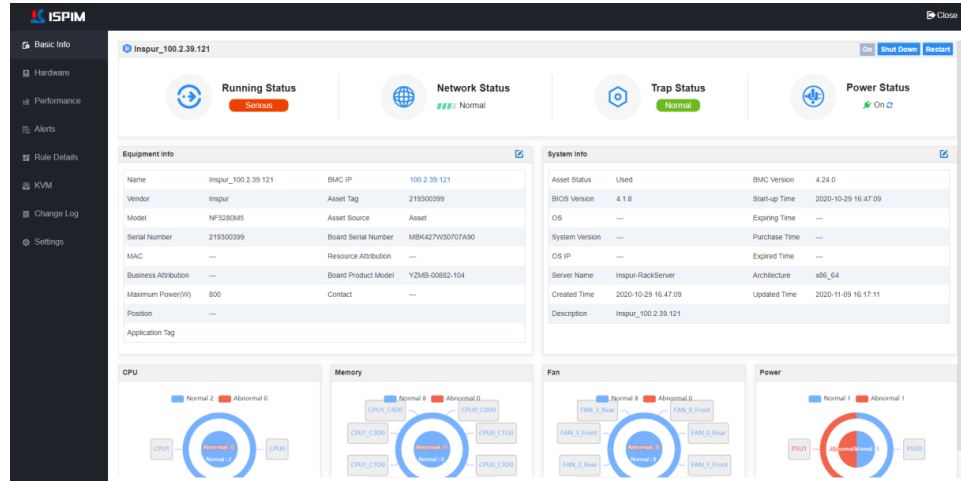
### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page. Click a server name in the server list to enter the server details page.

**Step 2** Select [Basic Info] in the left navigation bar to enter the basic information page, as shown in the figure below. User can view/edit device information and asset information on this page.

- Edit device information: Click the  icon in the upper right corner of the equipment information to edit the device information. Including asset source, application tag, MAC address, resource attribution, business attribution and other information.
  - Asset Source: Contains assets, borrowed or customized.
  - Application Tag: Contains computer node, control node, storage node, bare metal, etc.

- Edit device system information: Click the  icon in the upper right corner of the system information to edit the asset system information, including asset status and created time.



----End

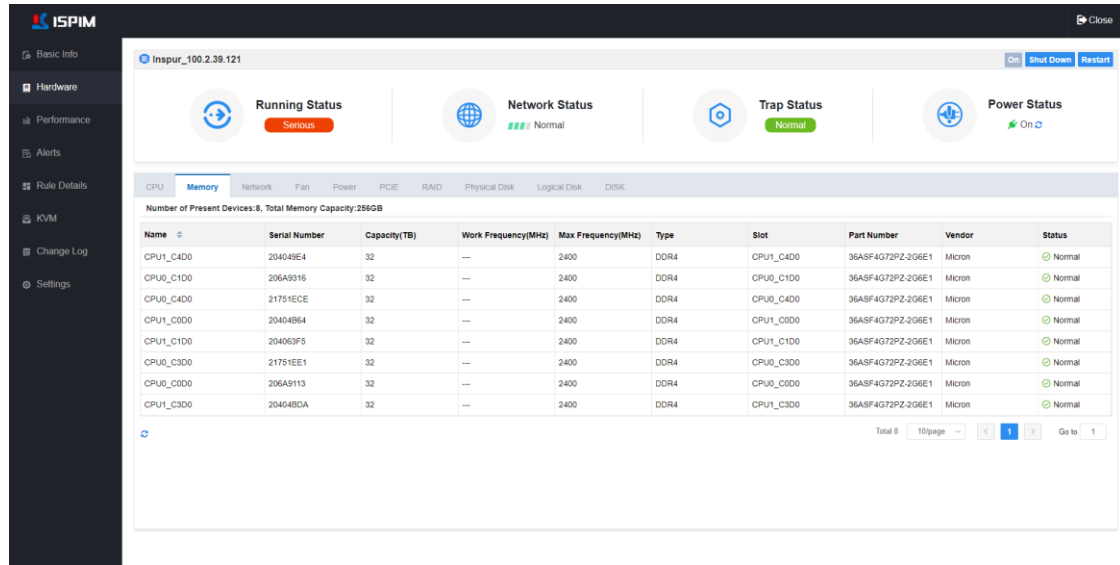
## 2. Hardware Info

In the hardware information page, user can view the hardware information of the server, including CPU, memory, network, fan, power supply, RAID, physical disk, logical disk and other information.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page. Click a server name in the server list to enter the server details page.

**Step 2** Select [Hardware Info] in the left navigation bar to enter the hardware information page, as shown in the figure below. User can view the server hardware information on this page. Including: CPU, memory, network, fan, power supply, RAID, physical disk, logical disk and other information. Select different tabs such as "CPU", "Memory", "Network", "Fan", and "Power" to switch the page and view the corresponding hardware information.



----End

Table 6-3 Hardware Info Description

Type	Fields
CPU	Name, serial number, type, architecture, hyper-threading, main frequency, cores/threads, slot, model, manufacturer, L1 cache, L2 cache, L3 cache, status
Memory	Name, serial number, capacity, working frequency, maximum frequency, type, slot, part number, manufacturer, status
Network	<ul style="list-style-type: none"> <li>● BMC adapter: name, MAC address and IP</li> <li>● System network adapter: location, serial number, vendor, model, port, port status, port MAC address, presence status</li> </ul>
Fan	Name, speed, speed percentage, slot, mode, status
Power	Name, model, rated power, status, slot, mode
PCIE	Name, status, vendor, slot, description
RAID	Name, serial number, firmware version, model, status
Physical Disk	Name, device ID, slot, interface type, capacity, firmware status
Logical Disk	Device ID, name, capacity, status
Disk	<ul style="list-style-type: none"> <li>● Backplane: Backplane number, status, front/rear, CPLD version, port number, hard disk number, temperature.</li> </ul>

Type	Fields
	<ul style="list-style-type: none"> <li>● Backplane Hard Disk: number, status, front/rear, back panel serial number, NVME, NVME firmware version.</li> <li>● OnBoard HDD: number, status, capacity, SN</li> </ul>

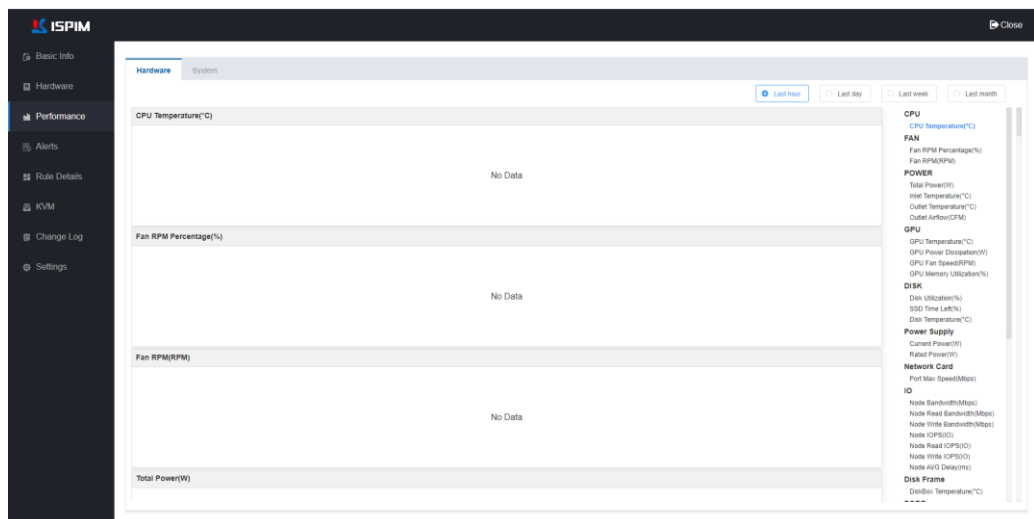
### 3. Performance Data

On the performance data page, user can view the server performance curve, including hardware indicators and system indicators, which can monitor the server's in-band and out-of-band performance in seconds.

#### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page. Click a server name in the server list to enter the server details page.

**Step 2** Select [Performance] in the left navigation bar to enter the performance data page, as shown in the figure below. On this page, user can view the performance data change curve of server hardware indicators and system indicators.



**Step 3** In the indicator tree on the right side of the page, click on an indicator item, and the related graph of the indicator item will be displayed on the left side of the page. The indicator options include CPU, GPU, hard disk, fan, memory, power supply, network card, system I/O Wait, etc.

---End



Click "Last hour", "Last day", "Last week" and "Last month" in the upper right corner of the page to view the changes in the indicator curve within the corresponding time range.

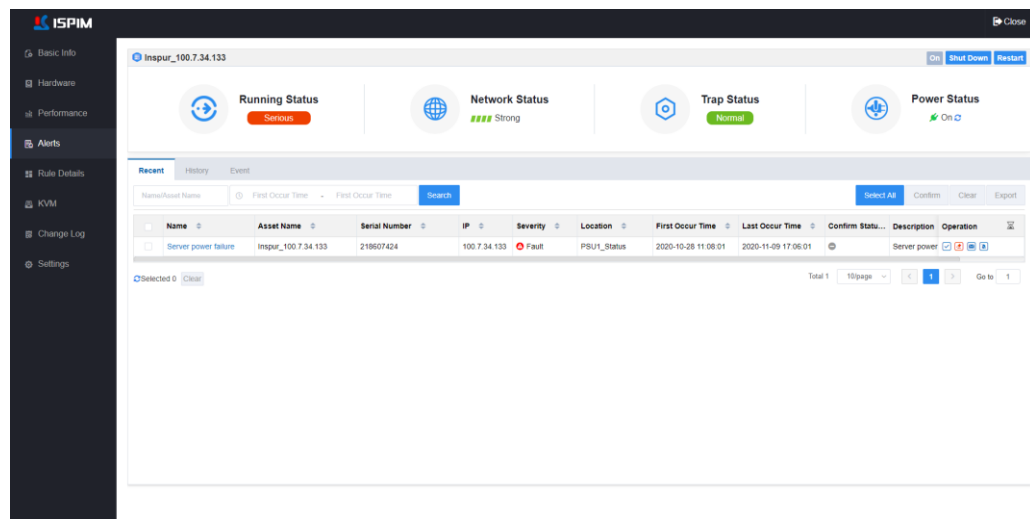
## 4. Alarm List

On the alarm list page, user can view server alarm related information, including real-time, history, and events.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page. Click a server name in the server list to enter the server details page.

**Step 2** Select [Alerts] in the left navigation bar to enter the alarm list page, as shown in the figure below. On this page, user can view the alarm-related information of the server, including real-time alarms, historical alarms, and events.



---End

## 5. Rule Details

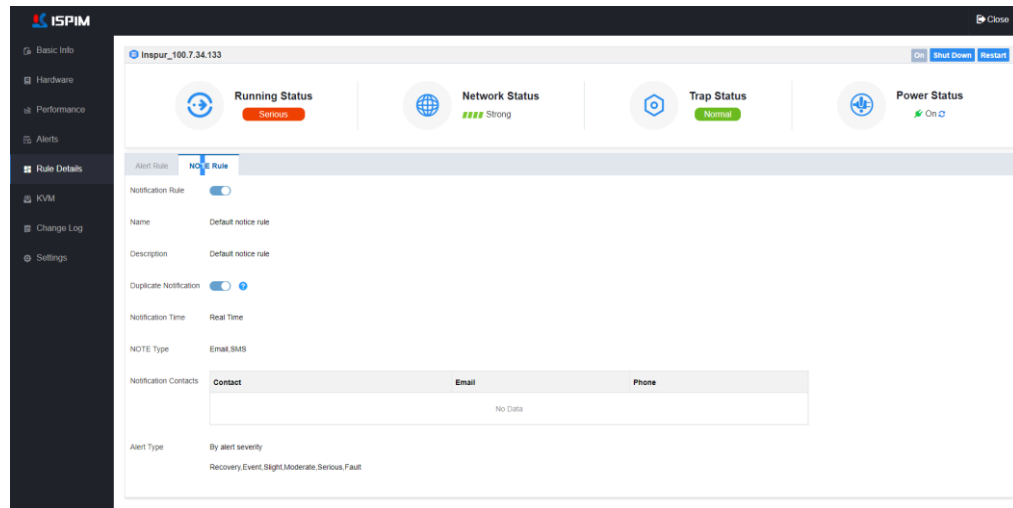
On the rule details page, user can view device alarm rules and notification rules.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page. Click a server name in the server

list to enter the server details page.

**Step 2** Select [Rule Details] in the left navigation bar to enter the rule details page, as shown in the figure below. You can view the alarm rules and notification rules of the server on this page.



**Step 3** Select the "Alarm Rules" or "Notification Rules" tab as needed to view the corresponding alarm rules or notification rule information.

--End



NOTE  
On the rule details page, only the alarm rules can be viewed, and cannot be set or modified.

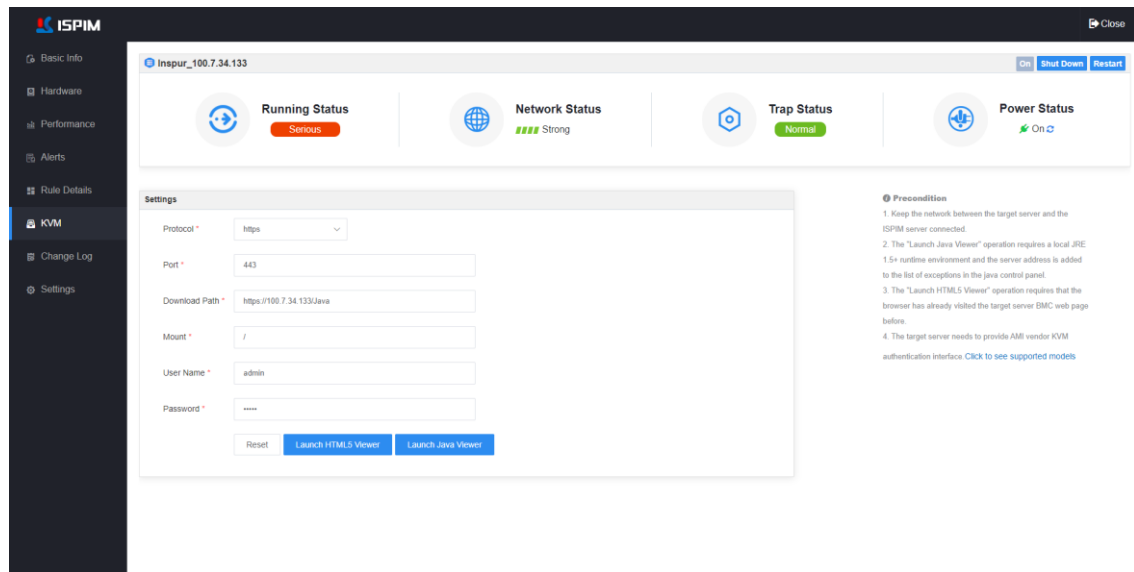
## 6. KVM

ISPIM supports the KVM function of Inspur server and other third-party servers, including Launch Java Viewer and Launch HTML5 Viewer. KVM remote management allows operation and maintenance personnel to directly access the device locally without logging in to the management interface of the corresponding device, facilitating remote device management.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page. Click a server name in the server list to enter the server details page.

**Step 2** Select [KVM] in the left navigation bar to enter the device KVM page, as shown in the figure below.



**Step 3** Configure the protocol, port, download path, mount path, user name, and password parameters.

- Protocol: Support http, https, and the default is https.
- Port: The default is 443.
- Mount path: The default is "/".
- User name/password: The default of each is admin.

**Step 4** When using the Java Viewer to access KVM, user need to click the <Launch Java Viewer> button, and then click the downloaded jviewer\_ip.jnlp file and run it to open the KVM window.

**Step 5** When using HTML5 to access KVM, user can directly click <Launch HTML5 Viewer> to log in to KVM.

--End



#### NOTE

- For the Launch Java Viewer method, the JRE1.5+ operating environment is required locally, and the location of the target server is added to the "Exception Sites" list of the Java control panel, and the target server also needs to provide the AMI vendor KVM authentication interface, regarding compatible devices List, see Table 6-4.
- For the Launch HTML5 Viewer method, the user needs to have visited the BMC page of the target server in this browser.

Table 6-4 KVM Compatibility List

Vendor	Model	Java Viewer	HTML5
DELL	PowerEdge R720	Supported	Unsupported
DELL	PowerEdge R730	Supported	Unsupported
DELL	PowerEdge R920	Supported	Unsupported
DELL	PowerEdge R930	Supported	Unsupported
HP	ProLiant DL580 G7	Supported	Unsupported
HP	ProLiant DL680 G7	Supported	Unsupported
HP	ProLiant DL580 G5	Supported	Unsupported
Huawei	RH2288 V3	Supported	Unsupported
Huawei	RH5885H V3	Supported	Unsupported
Huawei	RH5885 V3	Supported	Unsupported
Inspur	M4 Series Servers	Supported	Unsupported
Inspur	M5 Series Servers	Supported	Supported
Sugon	G20 I620	Supported	Unsupported
Sugon	G20 I840	Supported	Unsupported
Sugon	G30 I620	Supported	Unsupported

## 7. Change Log

On the change record page, user can view the change records of the server and its components in the whole life cycle according to the timeline. The equipment and components can be displayed according to the complete machine and component change events (equipment on-shelf, off-shelf, component replacement, component failure, version change, etc.) The detailed data of the component change, including the change time, change type, name, SN, type, location and change description, etc., realizes the traceability function of the whole life cycle component change of Inspur server.

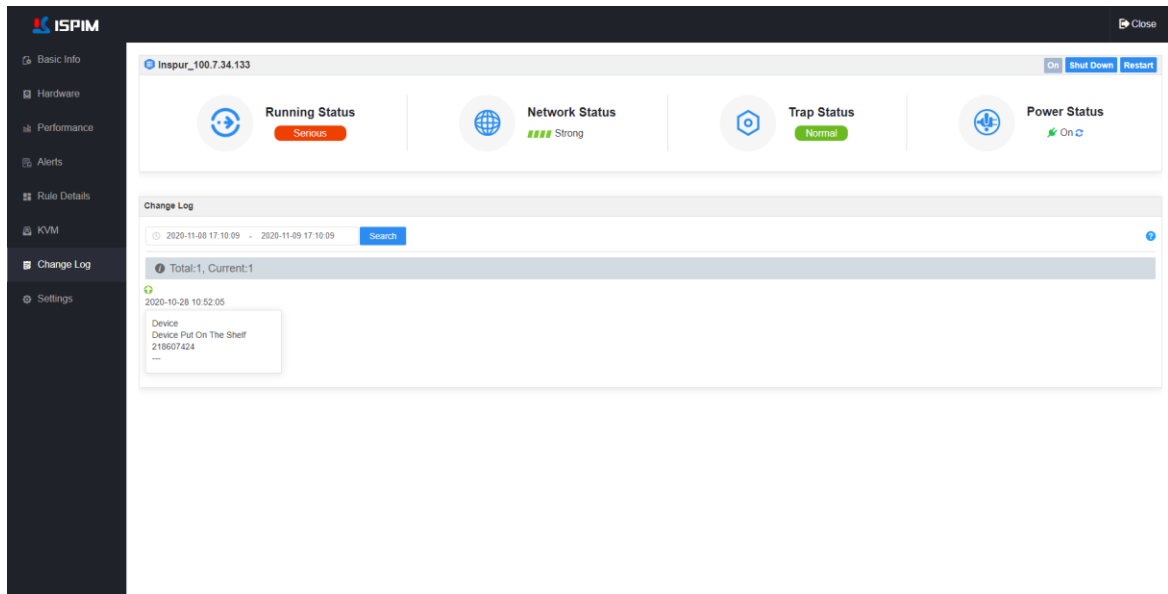
## Procedure

**Step 1** Click [Assets] -> [Servers] in turn to enter the server page. Click a server name in the server list to enter the server details page.

**Step 2** Select [Change Log] in the left navigation bar to enter the change history page, as



shown in the figure below.



**Step 3** Click the time search box in the upper left corner of the page, select the time range and click <Search> to view the change record information of the server in the selected time range.

----End

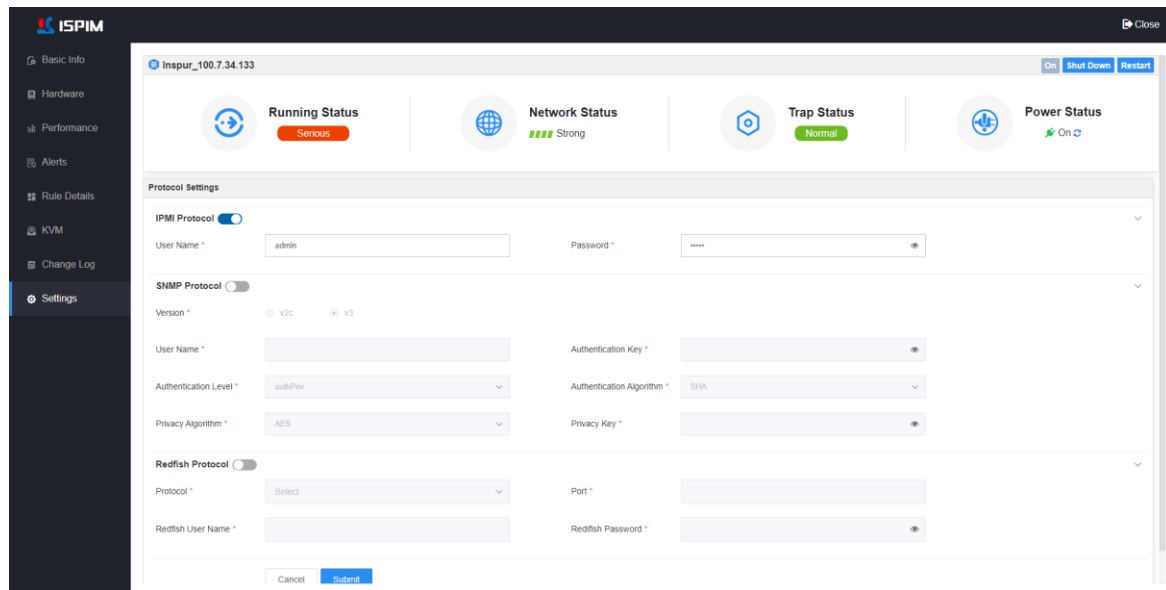
## 8. Settings

User can view or modify its protocol configuration on the server settings page, including IPMI protocol, SNMP protocol and Redfish protocol.

### Procedure

**Step 1** Click [Assets] -> [Servers] in turn to enter the server page. Click a server name in the server list to enter the server details page.

**Step 2** Select [Settings] in the left navigation bar to enter the protocol setting page, as shown in the figure below.



**Step 3** Configure the relevant parameters of the IPMI/SNMP/Redfish protocol as needed, and click the <Submit> button.

----End



#### NOTE

In the protocol setting page, only the authentication information stored in ISPIM can be modified, but the real protocol information of the device, such as BMC user name and password, will not be modified. If user needs to modify the protocol information of the device synchronously, please refer to 8.3.2 Configure BMC.

## 6.3 Cabinet Management

The Smart Rack management function is similar to the server management operation. For details, please refer to the actual page. For server management functions.

## 6.4 Blade Management

ISPIM supports automatic scanning of the blade box CMC to obtain the blade BMC information. Through the blade BMC, the unified management of the blade node can be realized, and the tool box can be edited, deleted, collected, and viewed for details.

## 6.4.1 Add Blade

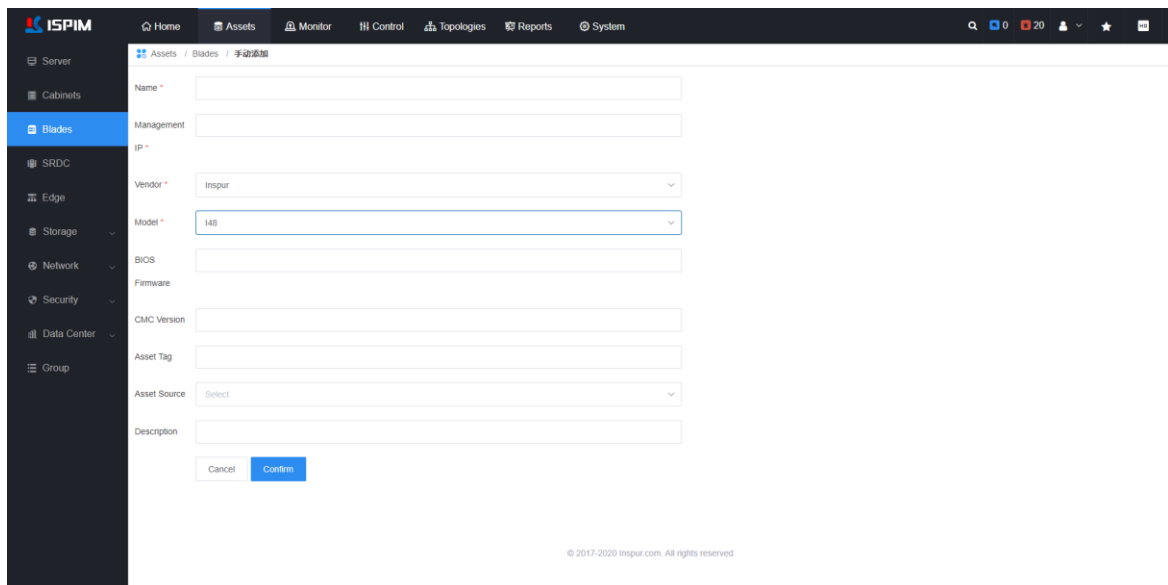
There are three ways to add blade box in ISPIM: "auto discovery", "batch import" and "add manually". Users can choose one of them according to their needs.

### 1. Add Manually

The operation of adding blade box equipment in ISPIM by "manual addition" is as follows:

**Step 1** Click [Assets] -> [Blades] to enter the blade equipment page.

**Step 2** Click <Add>, select "Add Manually" in the drop-down box, and enter the manual add server page, as shown in the figure below.



The screenshot shows the 'Add Manually' form in the ISPIM interface. The form is titled 'Assets / Blades / 手动添加'. It contains the following fields and controls:

- Name \* (text input)
- Management (text input)
- IP \* (text input)
- Vendor \* (dropdown menu, currently showing 'Inspur')
- Model \* (dropdown menu, currently showing 'I48')
- BIOS (text input)
- Firmware (text input)
- CMC Version (text input)
- Asset Tag (text input)
- Asset Source (dropdown menu, currently showing 'Select')
- Description (text input)
- Buttons: 'Cancel' and 'Confirm'

At the bottom right of the form, there is a small copyright notice: '© 2017-2020 Inspur.com. All rights reserved.'

**Step 3** Configure the relevant parameters of the blade device as needed, including name, management IP, manufacturer, model, BIOS firmware, CMC version, etc.

**Step 4** Click <Confirm> to continue.

----End

### 2. Automatic Discovery / Batch Import Blade

The operation process of automatic discovery/batch import of blades is similar to that of server equipment. The only difference is that the authentication protocol is different. For details, please refer to the actual page.

## 6.4.2 View Blade List

After adding the blade box, user can view the information of the blade box that has been managed, as shown in Figure 6-4. In the list, user can view the name, management IP, status, serial number, model, cabinet and other related information

- Name: Click the name of the blade box to view the detail.
- IP: Click to jump to the login page of the device manager.
- Room/Cabinet: The information is empty by default, and needs to be specified during batch import or manually.

Table 6-5 Blade List Operations






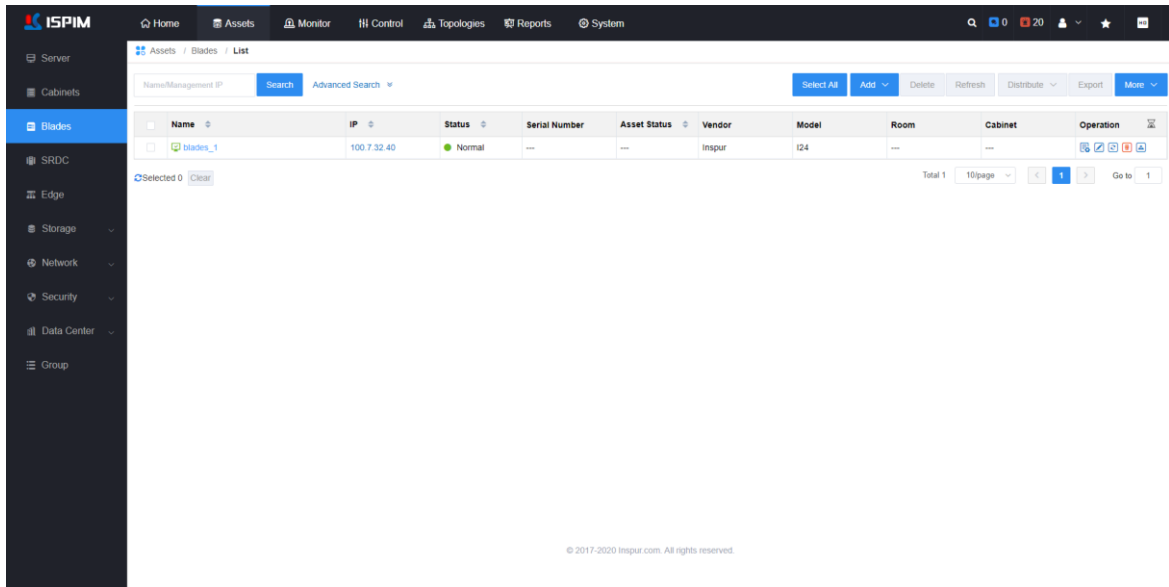
Operation	Description
	Click this icon, in the pop-up associated asset window, user can configure the related assets information.
	Click this icon, and according to the prompts on the page, user can edit the basic information and protocol of the blade box.
	When component asset changes occur, click this icon to manually synchronize hardware information.
	Click this icon and confirm in the pop-up window to delete the corresponding device.
	Click this icon to export the corresponding blade box log.

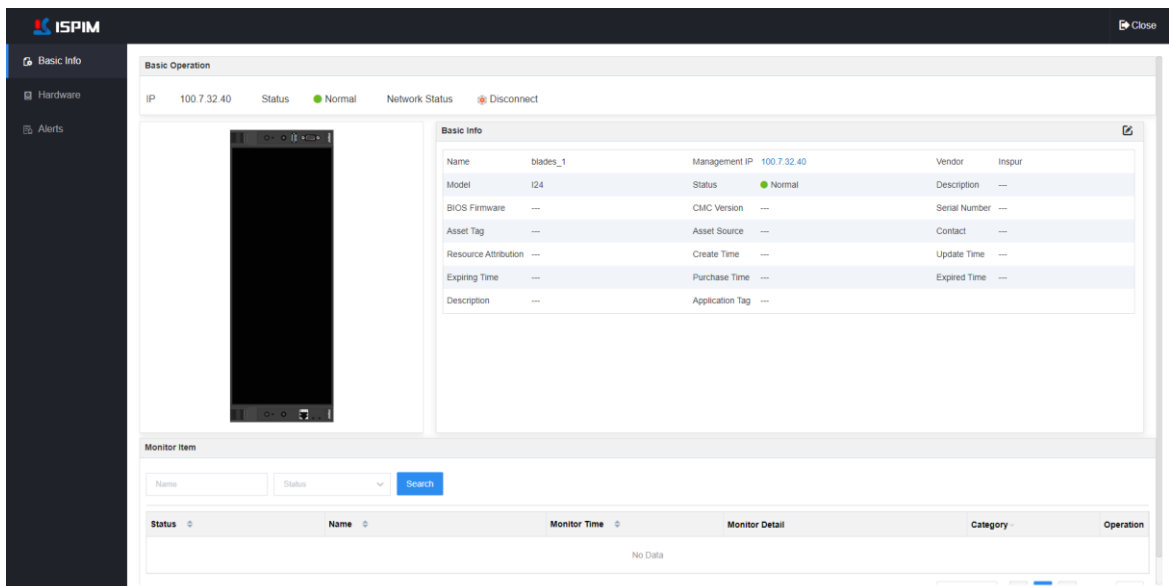
Figure 6-4 Blade List



### 6.4.3 View Blade Detail


In the toolbox list, click on a blade box name to enter the device details page, as shown in Figure 6-3. On the device details page, user can view the basic information, hardware information, and alarm list of the blade box.

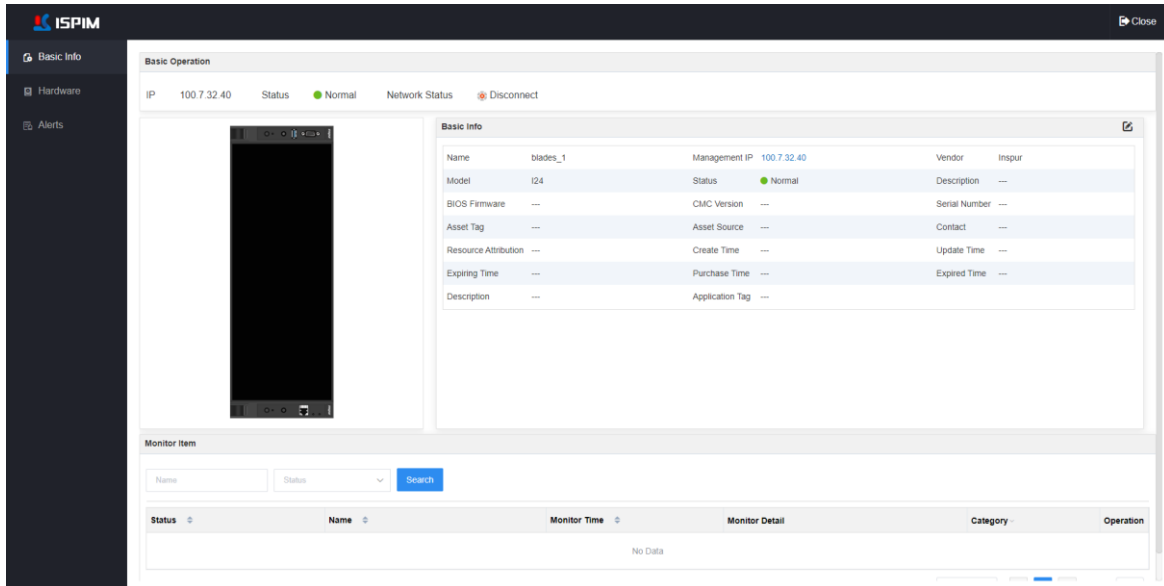
Figure 6-5 Blade Box Detail Page



#### 1. Basic Info

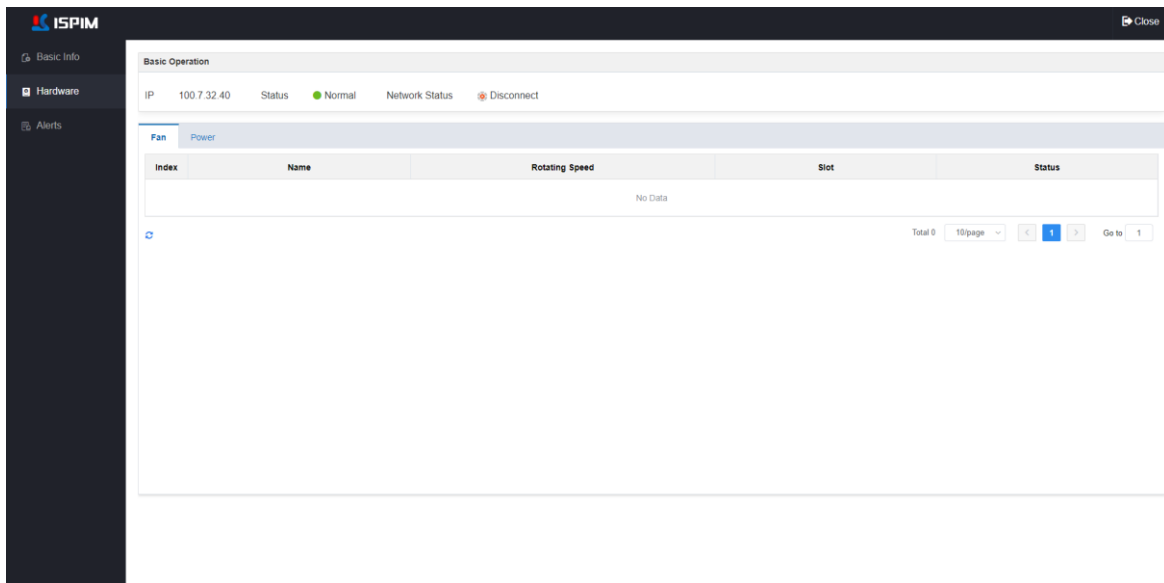
In the device details page, select [Basic Info] in the left navigation tree, user can enter the basic

information page, as shown in the figure below. On the basic information page, user can view the detailed information of the blade box and edit the basic information of the device. Click the  icon in the upper right corner of the basic info can edit the device information of the device, including asset source, application tag, resource attribution, business attribution and other information.



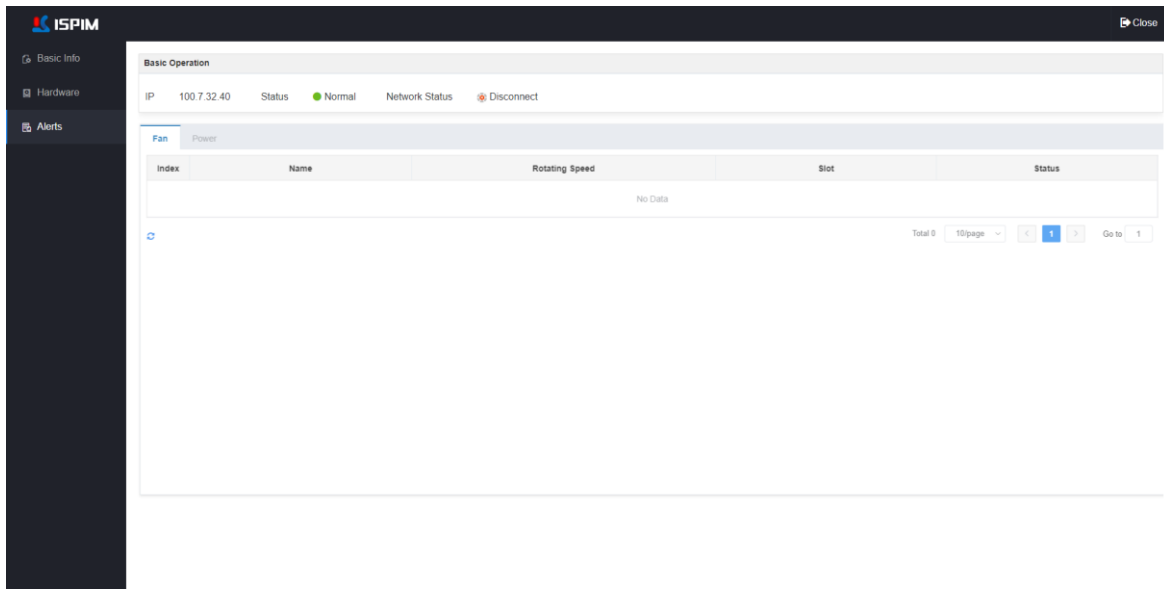
## 2. Hardware Info

Select [Hardware] in the left navigation tree, user can enter the hardware information page, as shown in the figure below. On the hardware information page, user can view the fan and power supply information of the knife box.



### 3. Alarm List

Select [Alerts] in the left navigation tree, user can enter the alarm list page, as shown in the figure below. On the alarm list page, user can view the alarm information of the device, including real-time, history and events.



## 6.5 All-in-one Device Management

ISPIM supports the scanning and management of the Inspur all-in-one device. Through the HTTP management protocol, the management of the internal servers, switches, and storage devices of the all-in-one device can be realized. At the same time, it supports the detection of the temperature, humidity, smoke sensor and other sensors of the all-in-one device. Before adding to the ISPIM, user needs to deploy the ISPIM-XX-SR-A1 management platform in the all-in-one "management box".

### 6.5.1 Add All-in-one Device

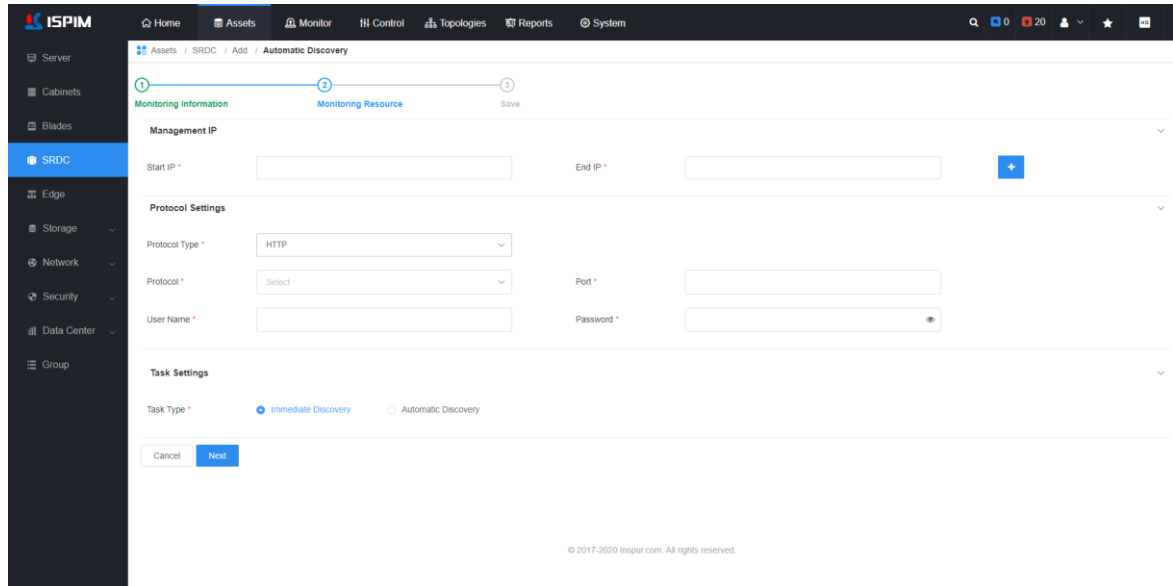
ISPIM supports adding all-in-one device in the way of "auto discovery" or "batch import".

#### 1. Automatic Discovery


The operation of adding an all-in-one device in the way of "auto discovery" is as follows:

**Step 1** Click [Assets] -> [SRDC] to enter the all-in-one device management page.

**Step 2** Click <Add>, select "Automatic Discovery" in the drop-down box to enter the configuration page, as shown in the figure below.



**Step 3** Configure parameters such as IP address, protocol information and task type.

- IP: Configure the all-in-one IP range. When adding multiple all-in-one devices at the same time, the first three parts of the all-in-one's starting IP and ending IP must be the same (ISIPM defaults to 255.255.255.0 as the subnet mask). User can click the  icon to add multiple IP ranges. To add a single device, just enter the same start IP and end IP.
- Protocol: Select the protocol type and configure the relevant parameters.
- Task Type: Select task category.
  - When selecting "Auto Discovery", user needs to configure the task name, task frequency, and start time, and the subsequent steps will not be triggered. After that, user can view the task execution status in the task center.
  - When selecting "Immediate Discovery", user needs to click <Next> to enter the asset scanning step and start scanning the server.

**Step 4** After the scan is completed, click <Next> to enter the device save page, the successfully scanned devices are displayed in the list, and click the <Submit> button to add the device to ISIPM.

----End

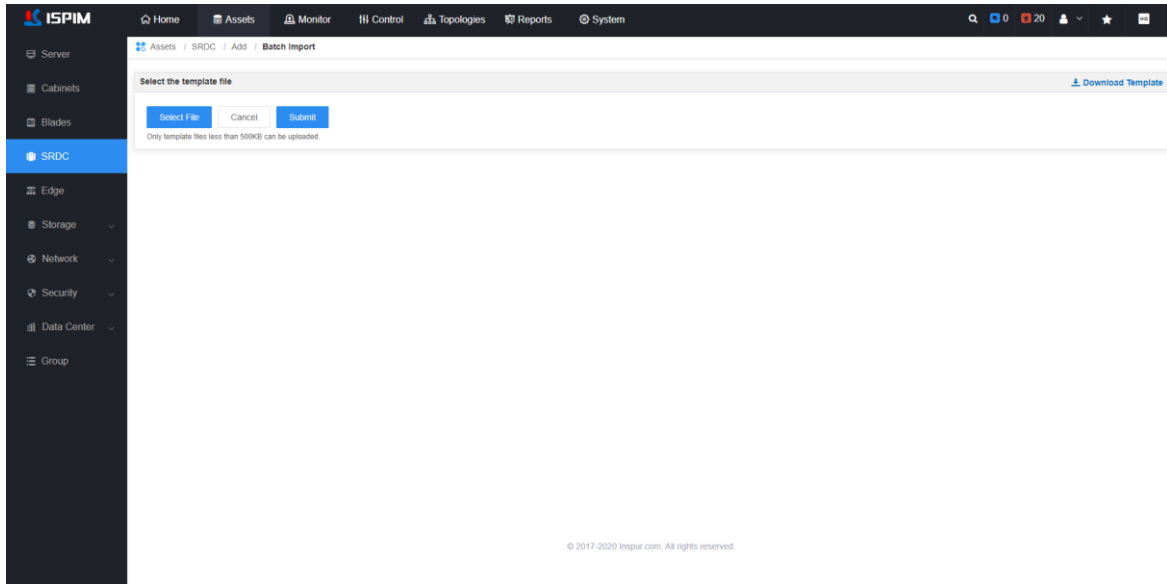


## 2. Batch Import

The operation of adding all-in-one devices in ISPIM in the way of "batch import" is as follows:

**Step 1** Click [Assets] -> [SRDC] to enter the all-in-one device management page.

**Step 2** Click <Add>, select "Batch Import" in the drop-down box, and enter the batch import page, as shown in the figure below.



**Step 3** Click <Download Template>, edit the downloaded template and configure the relevant information. Among them, the field marked with "\*" in the template is required.

**Step 4** After editing the template, click <Select File> to upload the edited template file, and click the <Submit> button to start scanning the device.

**Step 5** After the scan is completed, click <Next> to enter the device save page. The successfully scanned devices are displayed in the list. Click the <Submit> button to add multiple devices to ISPIM in batches.

----End

### 6.5.2 View All-in-one Device List

After the all-in-one device is added, user can view the information of the all-in-one that has been managed in the all-in-one list, as shown in Figure 6-6. In the all-in-one device list, hover the mouse over a device to view the device's information name, IP, status, serial number, model, manufacturer and other

related information. Click on the IP in the upper left corner of the all-in-one device to enter the all-in-one details page.

Table 6-6 All-in-one Device Operations





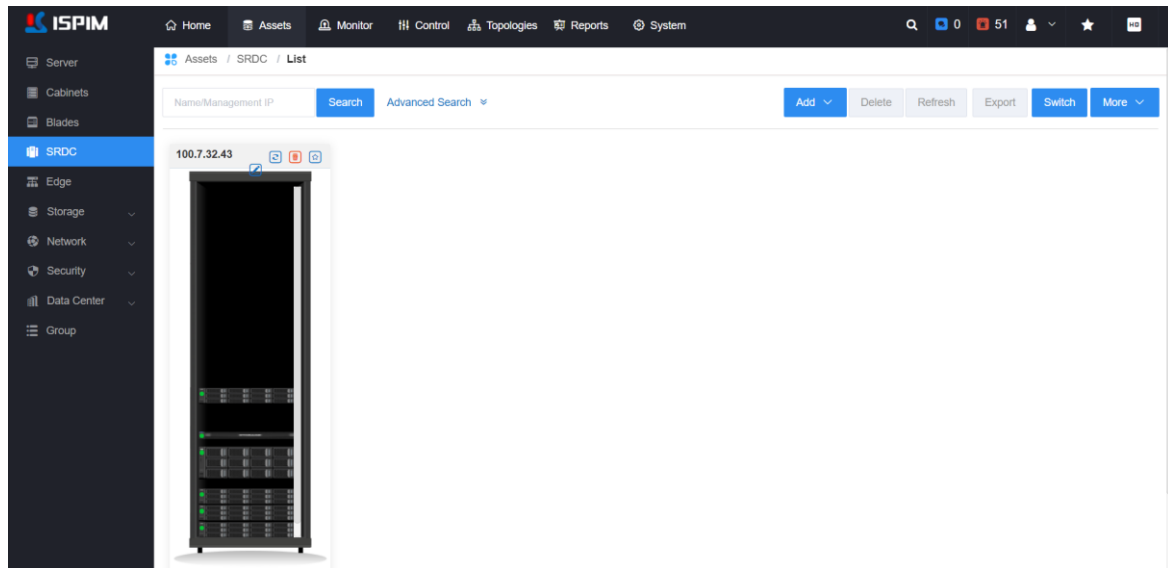
Operation	Description
	Click the icon and follow the prompts on the page to edit the basic information and protocol parameters.
	When components change in a certain device, click this icon to manually synchronize the hardware information.
	Click the icon and confirm in the pop-up window to delete the corresponding device.
	Click this icon to quickly bookmark the device.

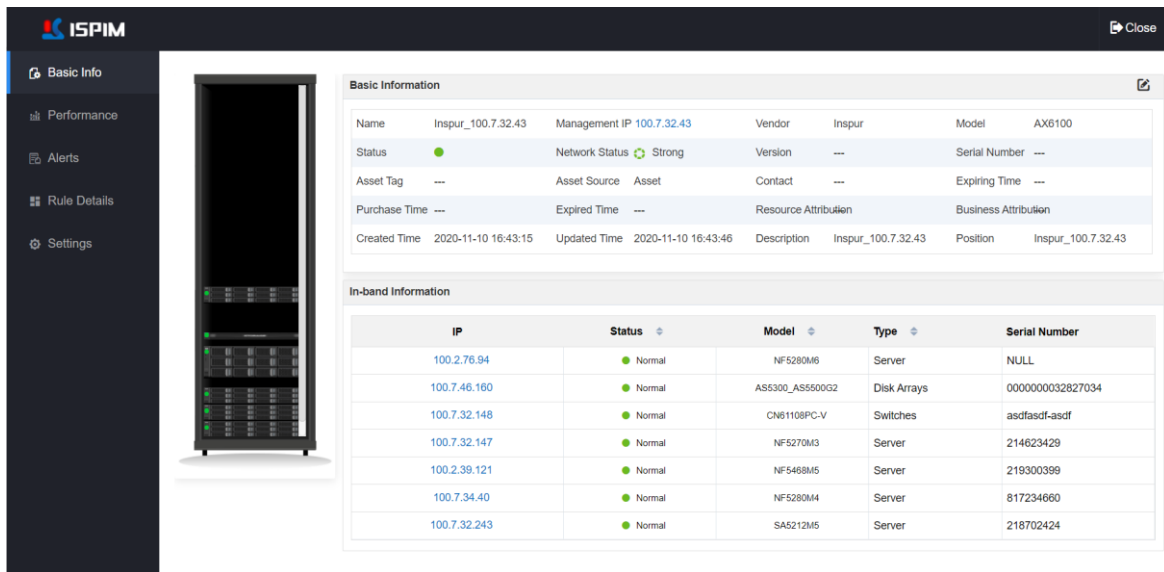
Figure 6-6 All-in-one Device List



### 6.5.3 View All-in-one Device Detail

In the all-in-one list, click the IP in the upper left corner of the device to enter the device details page, as shown in Figure 6-7. On this page, user can view and manage the basic information, performance data, alarm list, rule details, and settings information.

Figure 6-7 All-in-one Device List



The screenshot displays the 'Basic Info' page in the ISPIM interface. On the left is a dark navigation menu with options: Basic Info (selected), Performance, Alerts, Rule Details, and Settings. The main content area features a server rack image on the left and two data tables on the right.

**Basic Information**


Name	Inspur_100.7.32.43	Management IP	100.7.32.43	Vendor	Inspur	Model	AX6100
Status	●	Network Status	● Strong	Version	---	Serial Number	---
Asset Tag	---	Asset Source	Asset	Contact	---	Expiring Time	---
Purchase Time	---	Expired Time	---	Resource Attribution	Business Attribution		
Created Time	2020-11-10 16:43:15	Updated Time	2020-11-10 16:43:46	Description	Inspur_100.7.32.43	Position	Inspur_100.7.32.43

**In-band Information**

IP	Status	Model	Type	Serial Number
100.2.76.94	● Normal	NF5280M6	Server	NULL
100.7.46.160	● Normal	AS5300_AS5500G2	Disk Arrays	000000032827034
100.7.32.146	● Normal	CN61108PC-V	Switches	asdfasd-asdf
100.7.32.147	● Normal	NF5270M3	Server	214623429
100.2.39.121	● Normal	NF5468M5	Server	219300399
100.7.34.40	● Normal	NF5280M4	Server	817234660
100.7.32.243	● Normal	SA5212M5	Server	218702424

## 1. Basic Info

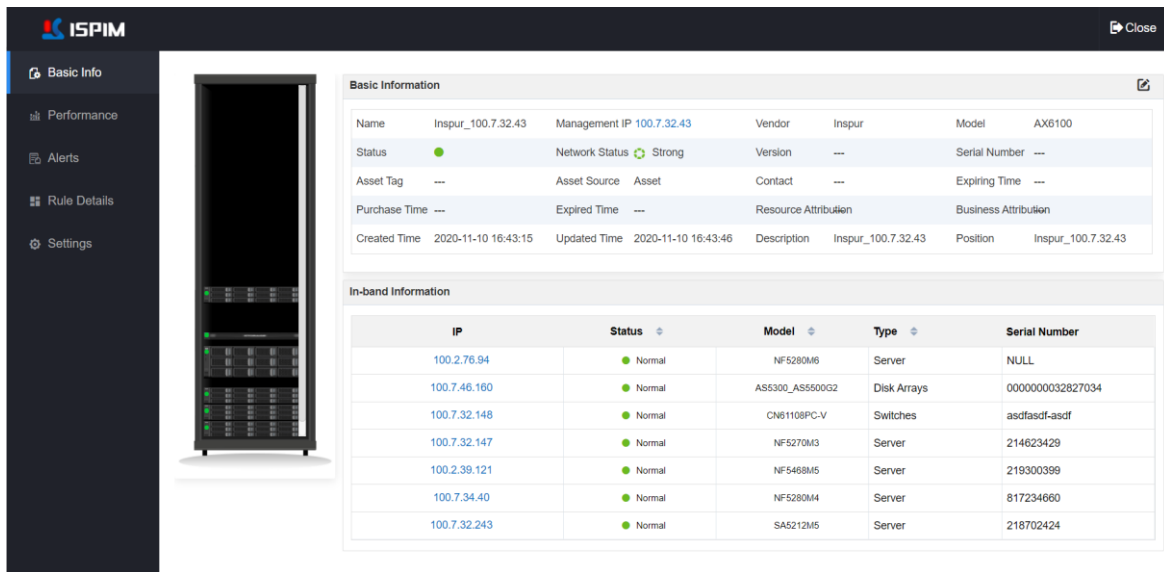
In the device details module, select [Basic Info] in the left navigation tree, user can enter the basic information page, as shown in Figure 6-8. In the basic info page, user can view the basic information and in-band information of the all-in-one, and support editing equipment information and view in-band details.

- Edit device information: Click the  icon in the upper right corner of the basic information operation bar, user can modify the asset name, asset source, asset status and other information in the basic information window that pops up.
- View in-band detailed information: In the in-band information list, click a device IP, user can view the CPU, memory, disk and network information corresponding to the device.

### NOTE

- Asset sources include: assets, borrow, custom.
- Asset status includes: used, unused, unavailable, lost, deleted.

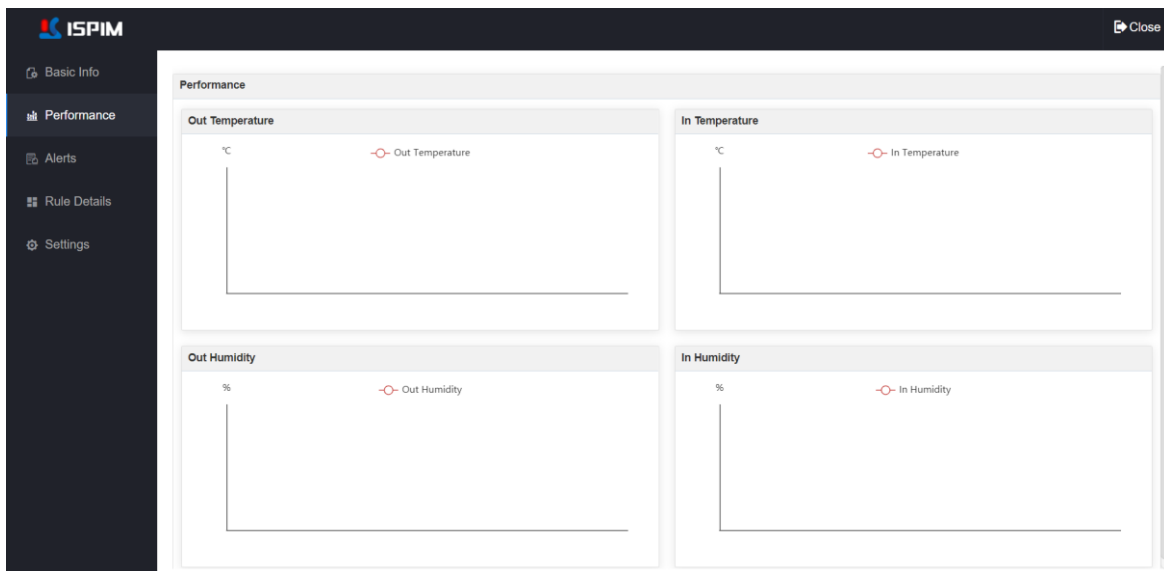
Figure 6-8 Basic Info



## 2. Performance Data

In the device details module, select [Performance] in the left navigation tree, user can enter the performance data page. On the performance data information page, you can view the performance data of the all-in-one machine, including outlet temperature, inlet temperature, Outlet humidity and inlet humidity.

Figure 6-9 Performance Data

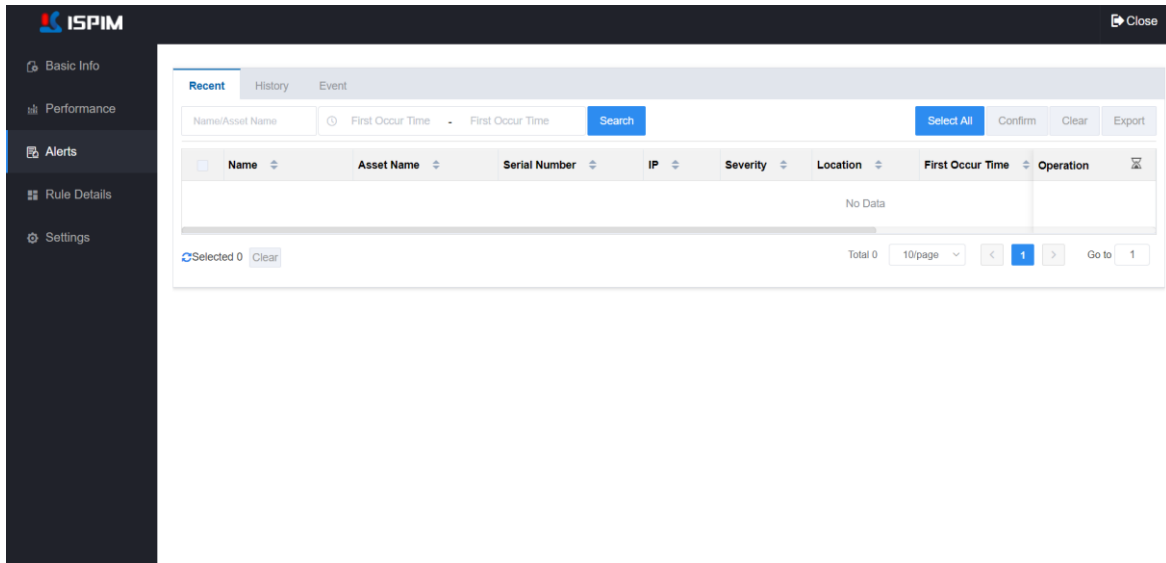


## 3. Alarm List

On the alarm list page, user can view server alarm related information, including real-time, history,

and events.

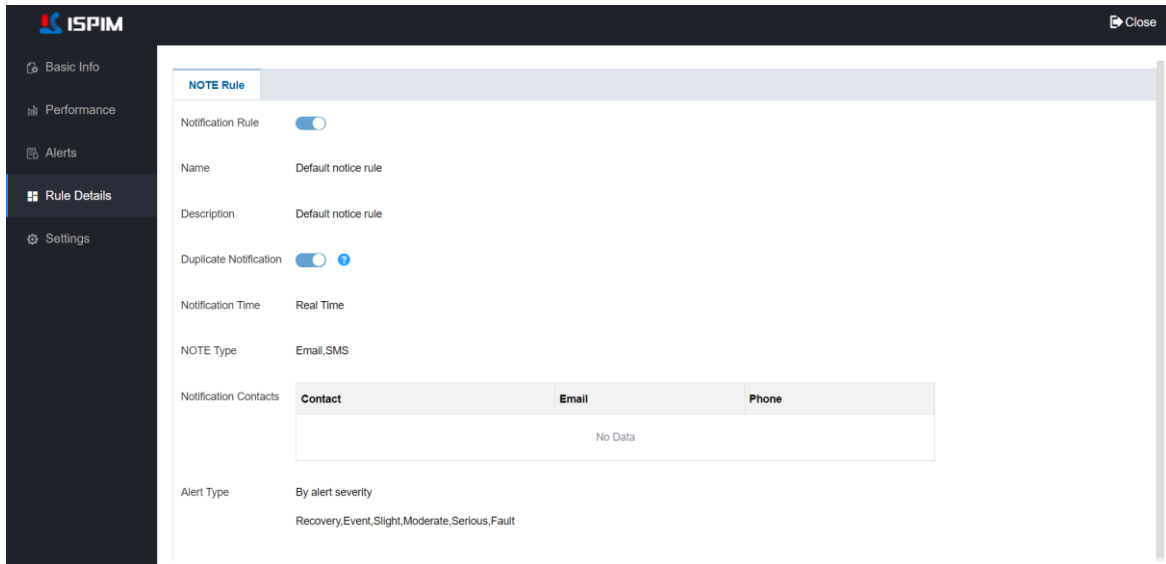
Figure 6-10 Alarm List



## 4. Rule Details

In the device details page, select [Rule Details] in the left navigation tree, user can enter the rule details page. In the rule details page, user can view the alarm notification rules.

Figure 6-11 Rule Details



## 5. Protocol Settings

In the device details page, select [Settings] in the left navigation tree, user can enter the protocol

setting page. In the device protocol setting page, user can view and modify the relevant protocol configuration.

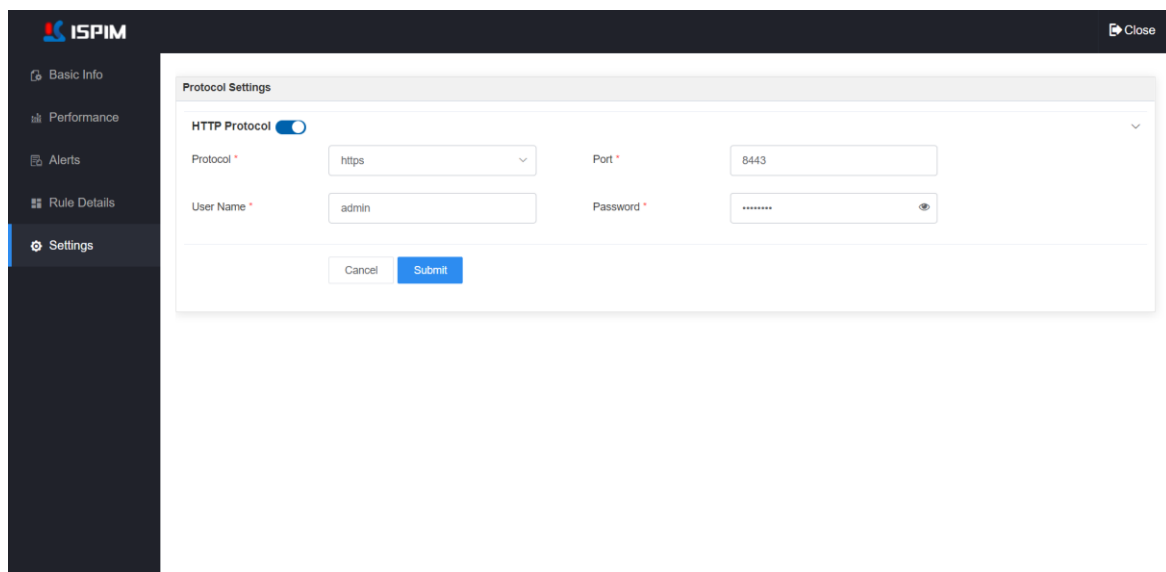
---

 NOTE

- The ISPIM supported management protocol for all-in-one device is HTTP.
- In the protocol setting page, only the authentication information stored in ISPIM can be modified, but the real protocol information of the device will not be modified.

---

Figure 6-12 Protocol Settings



## 6.6 Edge Device Management

ISPIM supports centralized management of Inspur edge devices using HTTP protocol. Before managing the edge devices, user needs to deploy the edge management system on the edge devices in advance, and set the IP and user name/password of the edge system. Then add the edge devices into ISPIM.

### 6.6.1 Add Edege Device

ISPIM supports adding edge devices in the way of "automatic discovery" or "batch import".


## 1. Automatic Discovery

To add an edge device in ISPIM using “automatic discovery” mode, the operation is as follows:

**Step 1** Click [Asset]->[Edge] to enter the edge device management page.

**Step 2** Click <Add>, and select "Automatic Discovery" in the drop-down box to enter the automatic discovery page, as shown in the figure below.

**Step 3** Configure parameters such as IP address, protocol information and task type.

- Configure the devices IP range: When adding multiple devices at the same time, the first three parts of the devices' starting IP and ending IP must be the same (ISPIM defaults to 255.255.255.0 as the subnet mask); if the device is located in a different network segment, click the  icon to add multiple IP ranges. To add a single device, enter the same start IP and end IP.
- Protocol Parameters: Select the protocol type and configure the relevant parameters of the protocol.
- Task Type: Select task category.
  - When selecting “Automatic Discovery”, user needs to configure the task name, task frequency, and start time, and the subsequent steps will not be triggered. After that, user can view the task execution status in the task center. For details about the task center, please refer to 11.3Task.
  - When selecting “Immediate Discovery”, user needs to click <Next> to enter the

asset scanning step and start scanning the server.

**Step 4** After the scan is completed, click <Next> to enter the device save page, the successfully scanned devices are displayed in the list, and click the <Submit> button to add the device to ISPIM.

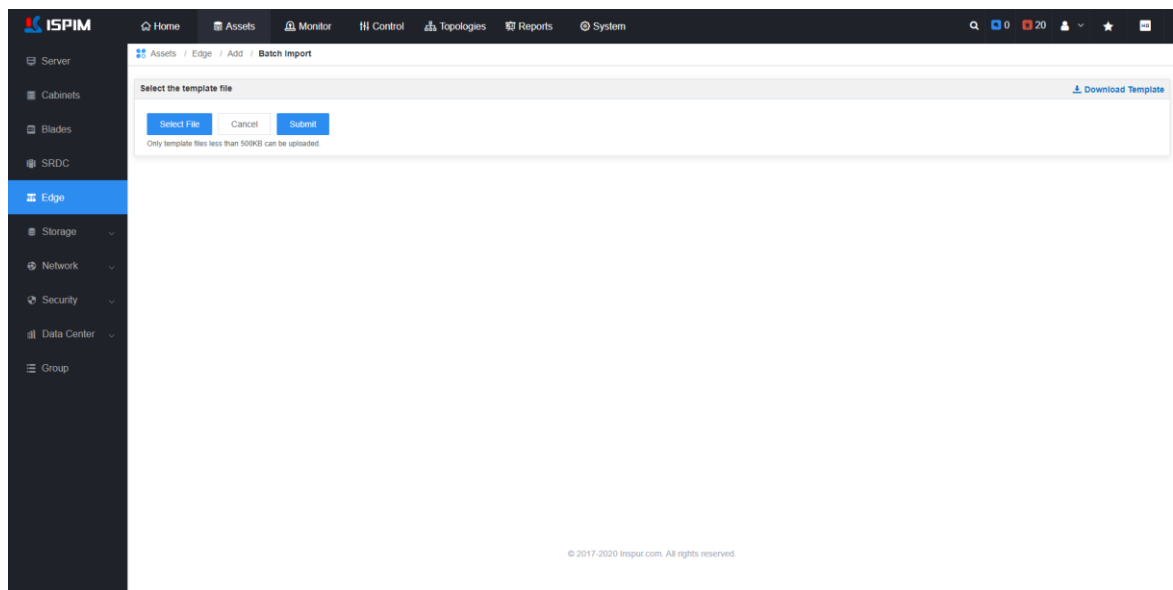
----End

## 2. Batch Import

The operation of adding edge devices in ISPIM in the way of "batch import" is as follows:

**Step 1** Click [Assets] -> [Edge] to enter the edge device management page.

**Step 2** Click <Add>, select "Batch Import" in the drop-down box, and enter the batch import page, as shown in the figure below.



**Step 3** Click <Download Template>, edit the downloaded template and configure the relevant information. Among them, the field marked with "\*" in the template is required.

**Step 4** After editing the template, click <Select File> to upload the edited template file, and click the <Submit> button to start scanning the device.

**Step 5** After the scan is completed, click <Next> to enter the device save page. The successfully scanned devices are displayed in the list. Click the <Submit> button to add multiple devices to ISPIM in batches.

----End



## 6.6.2 View Edge Device List

After the edge device is added, user can view the managed edge device information in the edge device list. In the edge device list, user can view the edge device name, management IP, device status, serial number, model, manufacturer and other related information.

- Device name: Click on the device name to view device details.
- Manage IP: Click to jump to the login page of the device manager.

Table 6-7 Edge Device Operations





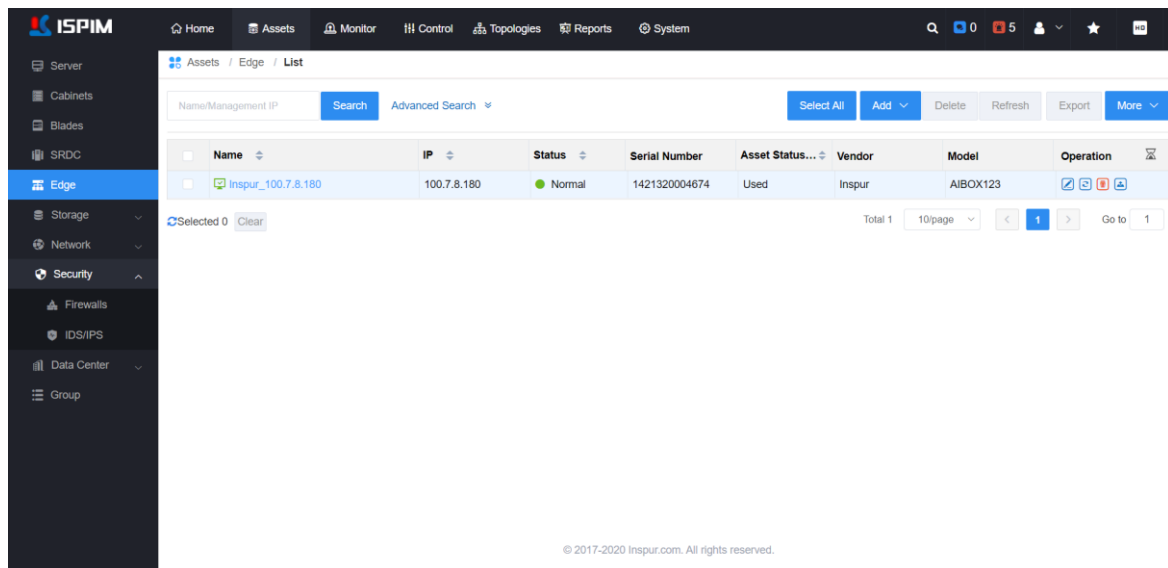
Operation	Description
	Edit the basic information and protocol configuration of the device.
	When asset changes occur to the components of the device, click this icon to manually synchronize hardware information.
	Click the icon and confirm in the pop-up window to delete the corresponding device.
	Export device logs.

Figure 6-13 Edge Device List

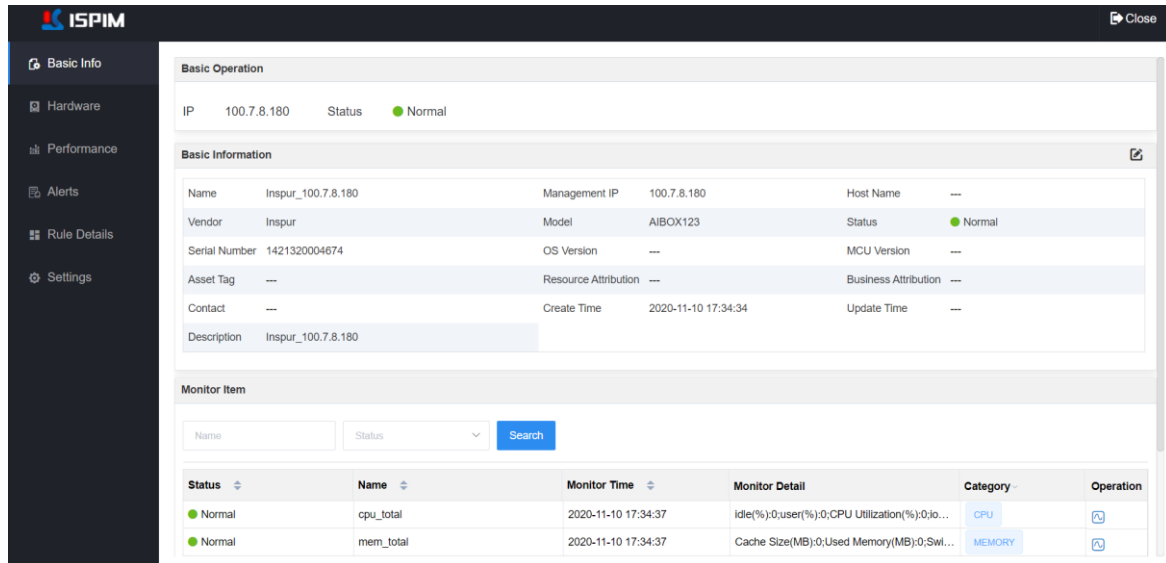


## 6.6.3 View Edge Device Detail

In the edge device list, click on the name of an edge device to enter the edge device details module, as shown in Figure 6-14. On this page, user can view and manage the basic information, hardware

information, performance data, and alarm list of the all-in-one devices, rules details and settings.

Figure 6-14 Edge Device Detail Page





## 1. Basic Info

In the device details page, select [Basic Info] in the left navigation list, user can enter the basic information page, as shown in Asset sources include: assets, borrow, custom.

- Asset status includes: used, unused, unavailable, lost, deleted.

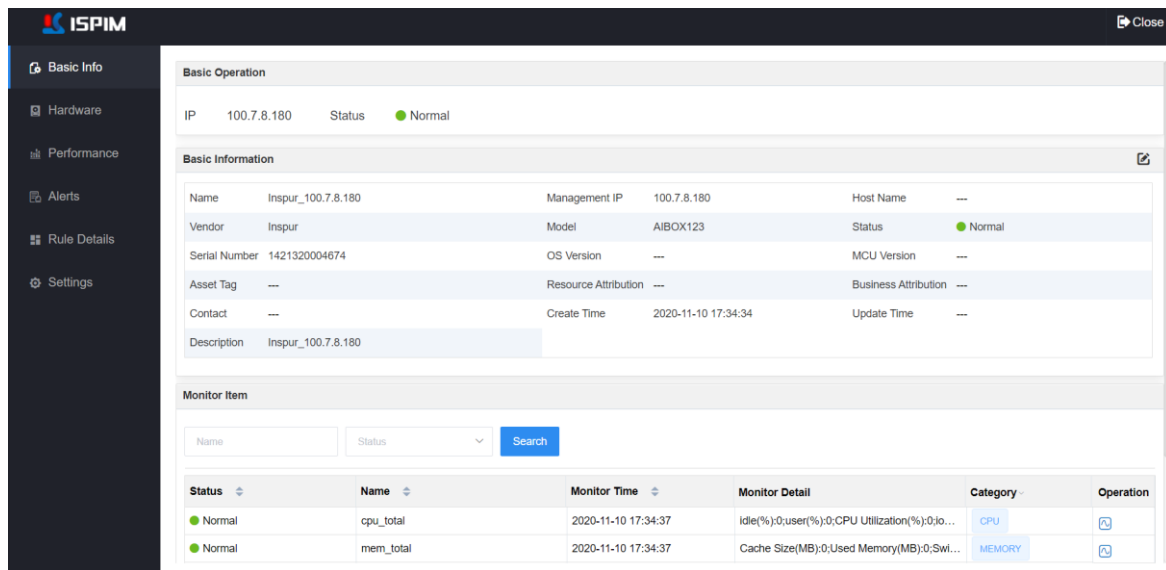
Figure 6-15. On the basic information page, user can view the basic information, monitoring indicators and other information of the edge device. User can edit device information and view historical curves of monitoring indicators.

- Edit device information: Click the  icon in the upper right corner of the basic information operation bar, and user can modify the asset name, asset source, asset status and other information in the basic information window that pops up.
- View the historical curve of monitoring indicators: In the operation area of the monitoring item list, click the  icon corresponding to an indicator, and user can view the historical curve change trend graph of the monitoring item in the pop-up window.

### NOTE

- Asset sources include: assets, borrow, custom.
- Asset status includes: used, unused, unavailable, lost, deleted.

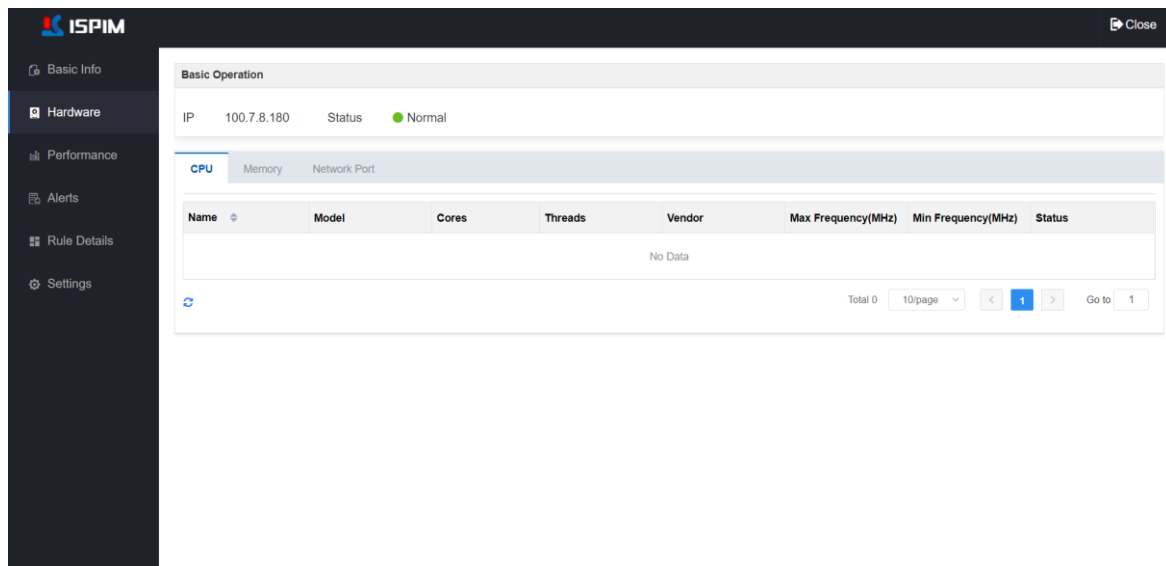
Figure 6-15 Basic Info



## 2. Hardware Info

In the device details page, select [Hardware Info] in the left navigation list, user can enter the hardware information page, as shown in Figure 6-16. In the hardware information page, user can view the hardware information of the edge device. Including: CPU, memory and network port.

Figure 6-16 Hardware Info

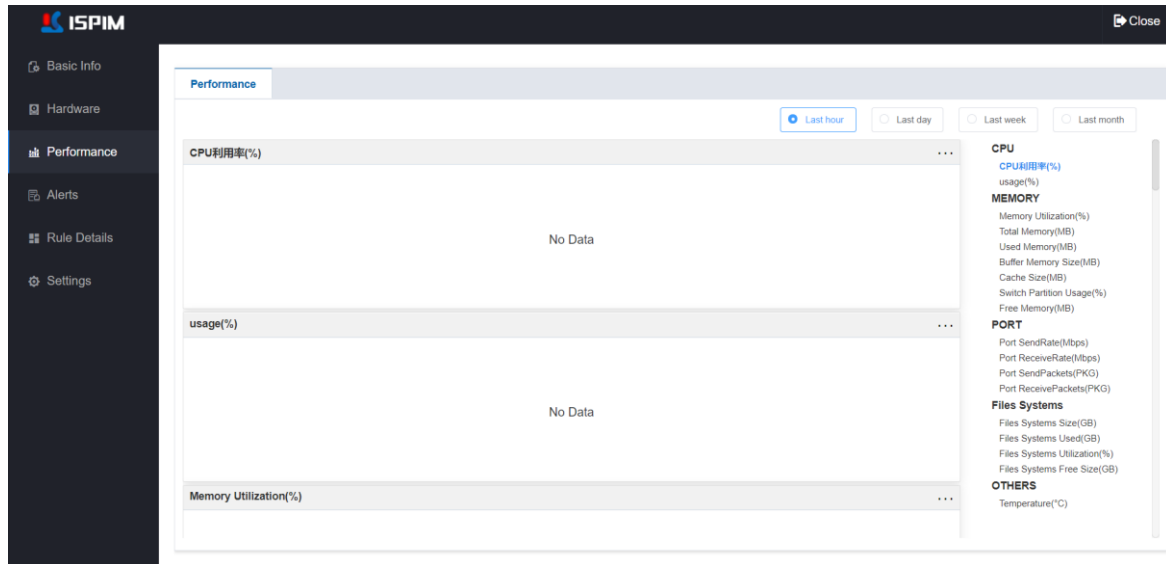


## 3. Performance Data

In the device details page, select [Performance Data] in the left navigation list to enter the

performance data page, as shown in Figure 6-17. On the performance data information page, user can view the performance data of the edge device, including CPU, memory, port, File system and other information. Click the performance index item on the right side of the page to view the data of the corresponding performance index.

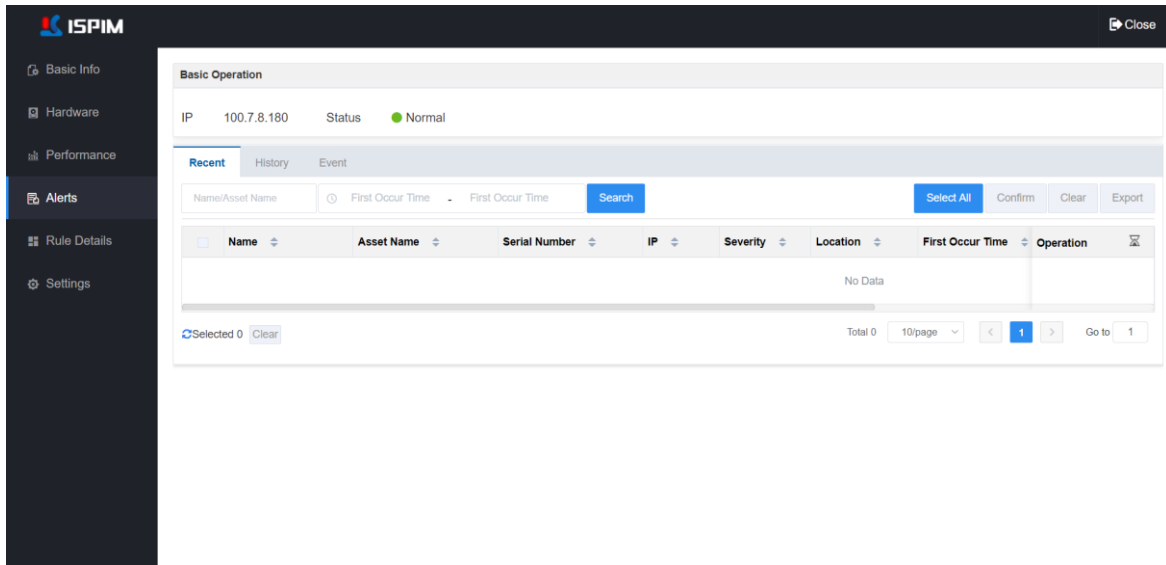
Figure 6-17 Performance Data



## 4. Alarm List

In the device details module, select [Alarms] in the navigation list on the left to enter the alarm list page. On the alarm list page, user can view equipment alarm related information, including real-time, history and events.

Figure 6-18 Alarm List



## 5. Rule Details

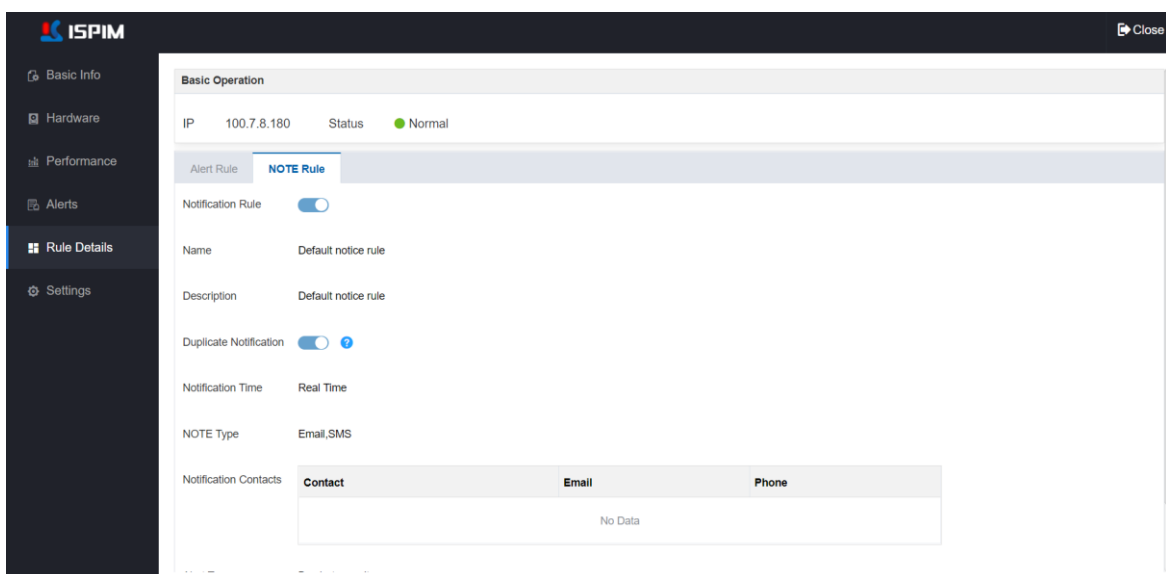
In the device details page, select [Rule Details] in the left navigation list, user can enter the rule details page, as shown in On the rule details page, the rules can only be viewed but cannot be set.

Figure 6-19. In the rule details page, user can view the device alarm rules and notification rules. Select different tabs to view the corresponding details of the rules.



On the rule details page, the rules can only be viewed but cannot be set.

Figure 6-19 Rule Details



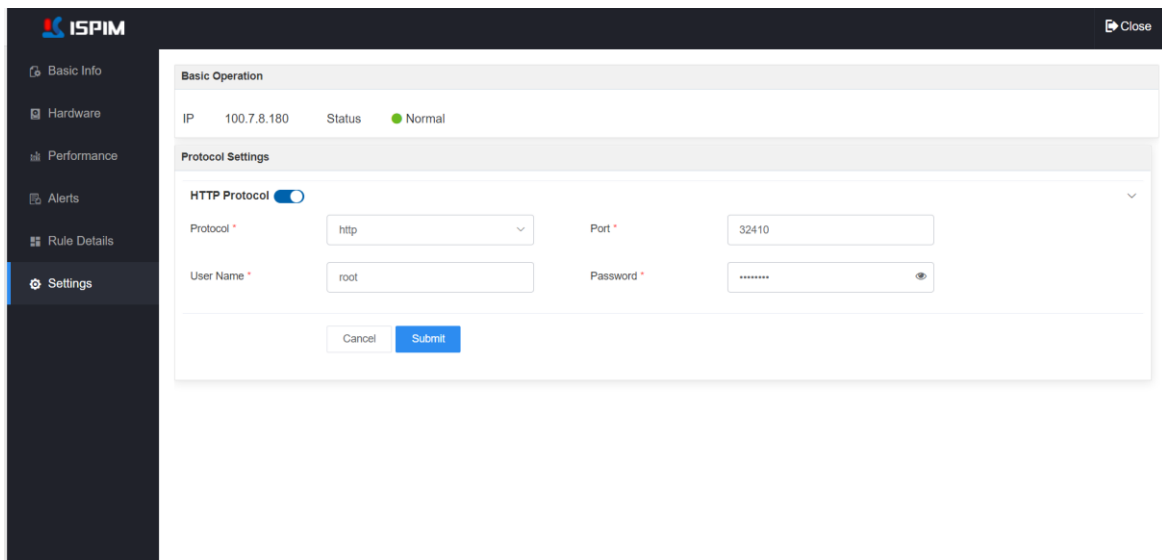
## 6. Settings

In the device details module, select [Settings] in the left navigation list, user can enter the protocol setting page, as shown in Figure 6-20. In the device protocol setting page, user can view and modify the relevant protocol configuration information.

### NOTE

- For edge device, the supported protocol is HTTP.
- Note: The protocol settings modified on this page only modify the authentication parameters stored in ISPIM, and will not modify the protocol information of the device.

Figure 6-20 Settings



## 6.7 Storage Management

In ISPIM, user can add general disk arrays and distributed storage devices through "auto-discovery" or "batch import", and perform operations such as collection, reset rules, reset protocols, edit, delete, etc. on them. ISPIM supports centralized management of general storage and distributed storage software of Inspur, Lenovo, Huawei, Sugon, ZTE, etc.

### 6.7.1 Add Storage Device

The processes of adding distributed storage or disk array are similar. The only difference is the

authentication protocol type and protocol related parameters. The storage device type and protocol parameters description are shown in Table 6-1. This chapter will take adding "distributed storage" as an example to introduce the process of adding storage devices.

## 1. Automatic Discovery

The operation of adding distributed storage in ISPIM by "auto discovery" is as follows:


**Step 1** Click [Assets] -> [Storage] -> [DSs] to enter the distributed storage management page.

**Step 2** Click <Add>, and select "Auto Discovery" in the drop-down box to enter the automatic discovery storage configuration page, as shown in the figure below.

The screenshot shows the 'Automatic Discovery' configuration page in the ISPIM interface. The page is organized into several sections:

- Monitoring Information:** Includes a progress indicator and a 'Save' button.
- Monitoring Resource:** Contains 'Start IP' and 'End IP' input fields, with a blue '+' icon to add multiple IP ranges.
- Protocol Settings:** Includes 'Protocol Type' (set to HTTP), 'Protocol', 'Port', 'User Name', and 'Password' fields.
- Management Information:** Includes 'Protocol', 'IP', 'Port', and 'User Name' fields.
- Task Settings:** Includes 'Task Type' with radio buttons for 'Immediate Discovery' (selected) and 'Automatic Discovery'.

**Step 3** Configure discovery related parameters such as IP address, protocol information and task type.

- Set the storage device IP range. The first three parts of the storage device's start IP and end IP must be the same (ISPIM defaults to 255.255.255.0 as the subnet mask). If the storage devices are located in different networks, user can click the  icon to add multiple IP ranges. To add a single device, enter the same start IP and end IP.
- Protocol configuration: Select the protocol related parameters.
- Task Type: Select task category.
  - When selecting "Automatic Discovery", user needs to configure the task name, task frequency, and start time, and the subsequent steps will not be triggered. After that, user can view the task execution status in the task center. For details about the task

center, please refer to 11.3Task.

- When selecting “Immediate Discovery”, user needs to click <Next> to enter the asset scanning step and start scanning the server.

**Step 4** After the scan is completed, click <Next> to enter the device save page, the successfully scanned devices are displayed in the list, and click the <Submit> button to add the devices to ISPIM.

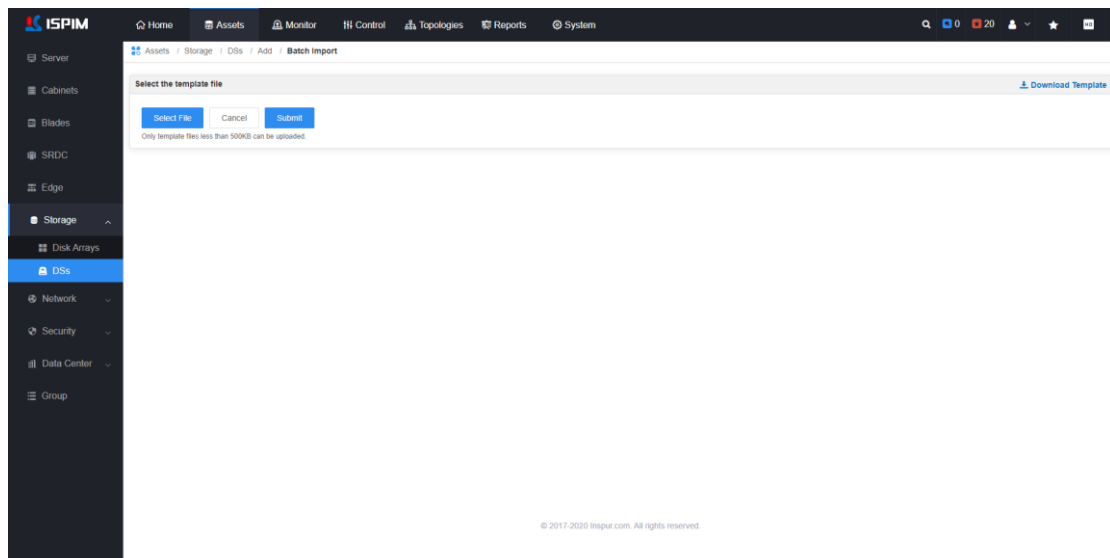
----End

## 2. Batch Import

The operation of adding storage devices in ISPIM in the way of "batch import" is as follows:

**Step 1** Click [Assets] -> [Storage] -> [DSs] to enter the edge device management page.

**Step 2** Click <Add>, select "Batch Import" in the drop-down box, and enter the batch import page, as shown in the figure below.



**Step 3** Click <Download Template>, edit the downloaded template and configure the relevant information. Among them, the field marked with "\*" in the template is required.

**Step 4** After editing the template, click <Select File> to upload the edited template file, and click the <Submit> button to start scanning the device.

**Step 5** After the scan is completed, click <Next> to enter the device save page. The successfully scanned devices are displayed in the list. Click the <Submit> button to add multiple devices to ISPIM in batches.








---End

## 6.7.2 View Storage Device List

After adding the storage array or distributed storage device, user can view the managed storage devices information in the storage list, as shown in Figure 6-21. In the distributed storage list, user can view the device name, status, model, manufacturer, number of nodes, and can perform editing, refreshing, collection and other operations.

Table 6-8 Device Operations List

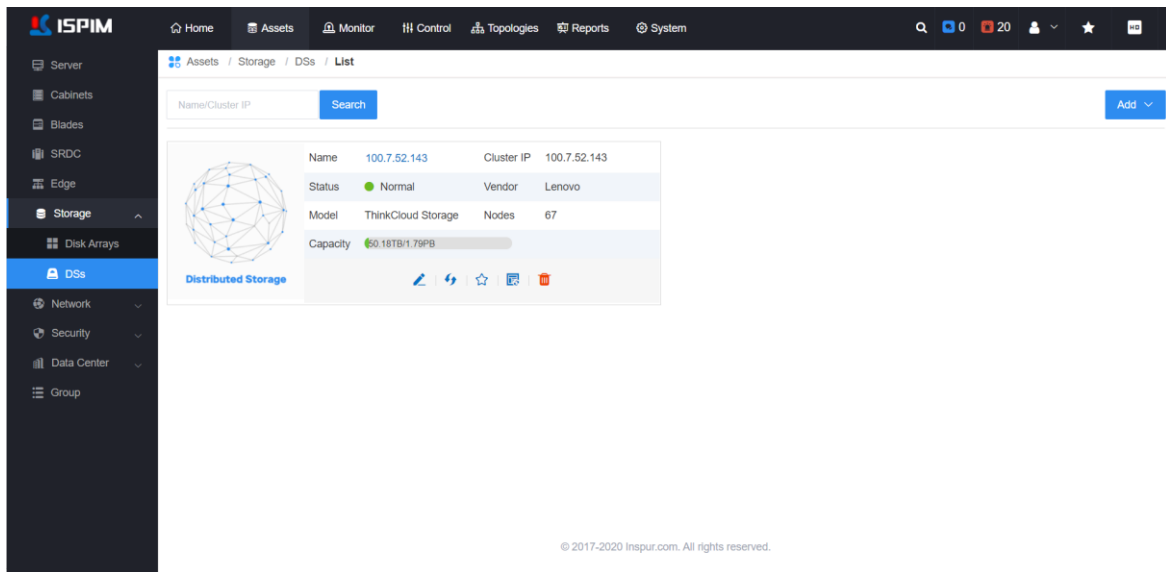
Operation	Detail
	Edit the device basic info and protocol info.
	Click this icon to trigger the collection of device hardware information and refresh.
	Click this icon to bookmark the corresponding device.
	Click the icon to delete the corresponding device.
	Click this icon to reset the monitoring rules and notification rules of this device.
View Detail	Click on a device name to enter the device details page.



### NOTE

The operation of viewing the disk array storage device list is similar to that of viewing the distributed storage list, please refer to the actual page.

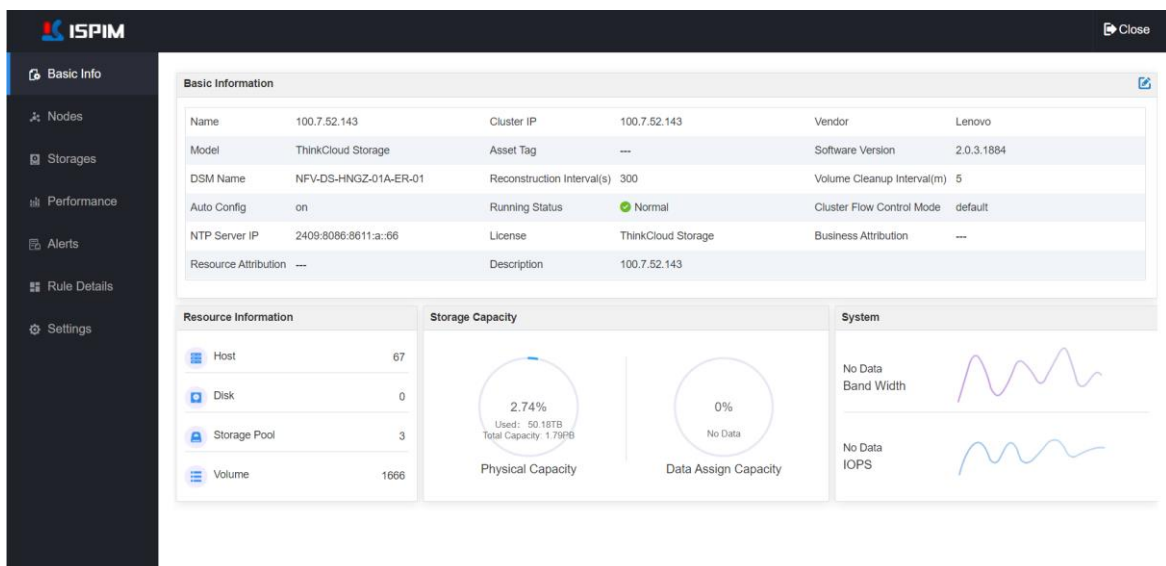
Figure 6-21 Distributed Storage List



### 6.7.3 View Storage Detail

In the list of distributed storage devices, click on a device name to enter the device details page, as shown in Figure 6-22. On this page, user can view the basic information, performance data, alarm list, rule details of the device, and perform node management, storage management.

Figure 6-22 Device Detail



#### 1. Basic Info

In the device details page, select [Basic Information] tab, user can enter the basic information page, as shown in Figure 6-23. In the basic information page, user can view the basic information of the


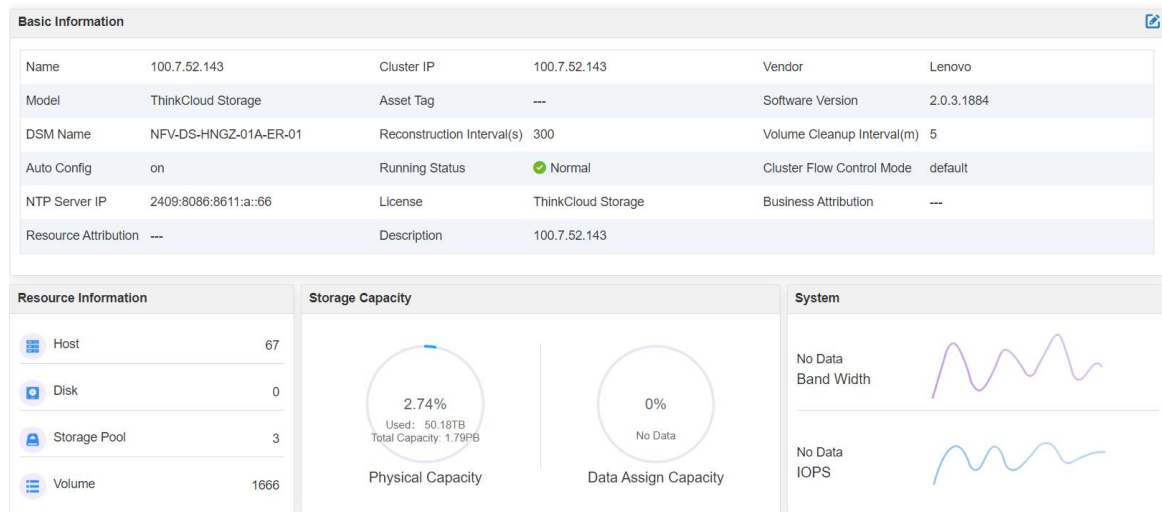
distributed storage (name, cluster IP, manufacturer, model, software version, etc.), resource information, storage capacity, system resources and other information. Click the  icon in the upper right corner of the page, in the basic information window that pops up, user can edit the basic information of the storage device.

Figure 6-23 Basic Info



## 2. Nodes Management

In the device details page, select [Nodes] tab, user can enter the node management page, as shown in Figure 6-24. In the node management page, user can view the node list information of distributed storage. The table shows the node name, serial number, RAID firmware version, business IP, management IP, asset name, running status.



### NOTE



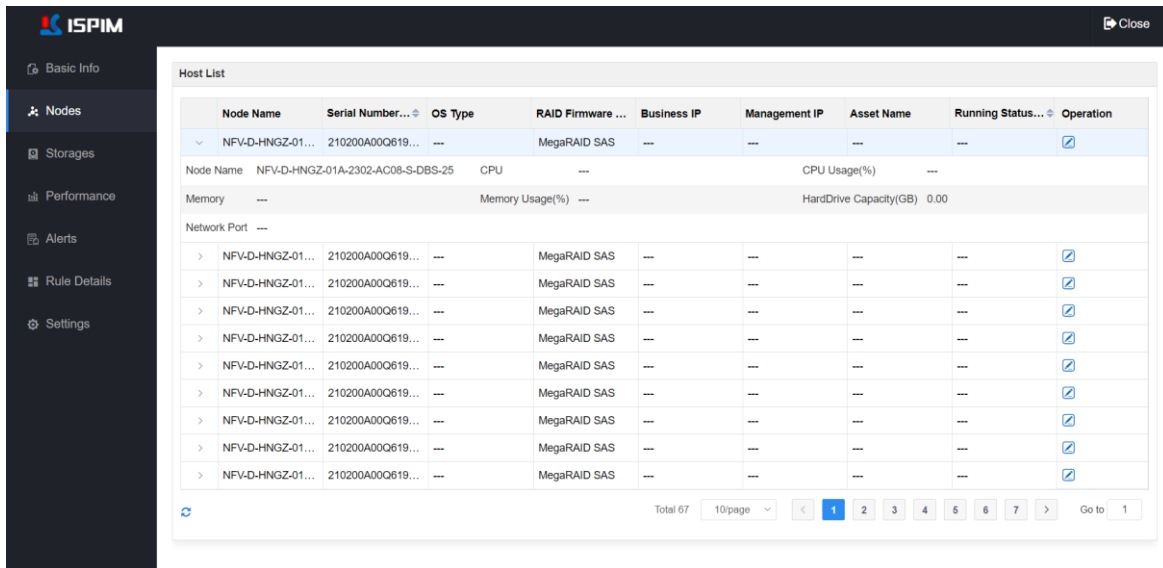
- In the node list, click the  icon corresponding to a node. In the pop-up window, user can edit the node IPMI protocol info, including IPMI IP, IPMI username, IPMI password, driver. When the node's BMC user and password change, user can sync them here.
- Click the  icon on the left side of the node name, user can view node details, including CPU utilization, memory utilization, hard disk capacity, etc.

Figure 6-24 Node Management



### 3. Device Storage Management

In the device details page, select [Storages] in the left navigation tree, user can enter the storage management page, as shown in Figure 6-25. In the storage management page, user can view the storage pool, volume, and snapshot information of the distributed storage. Select a different tab to view the corresponding content.

Figure 6-25 Device Storage Management

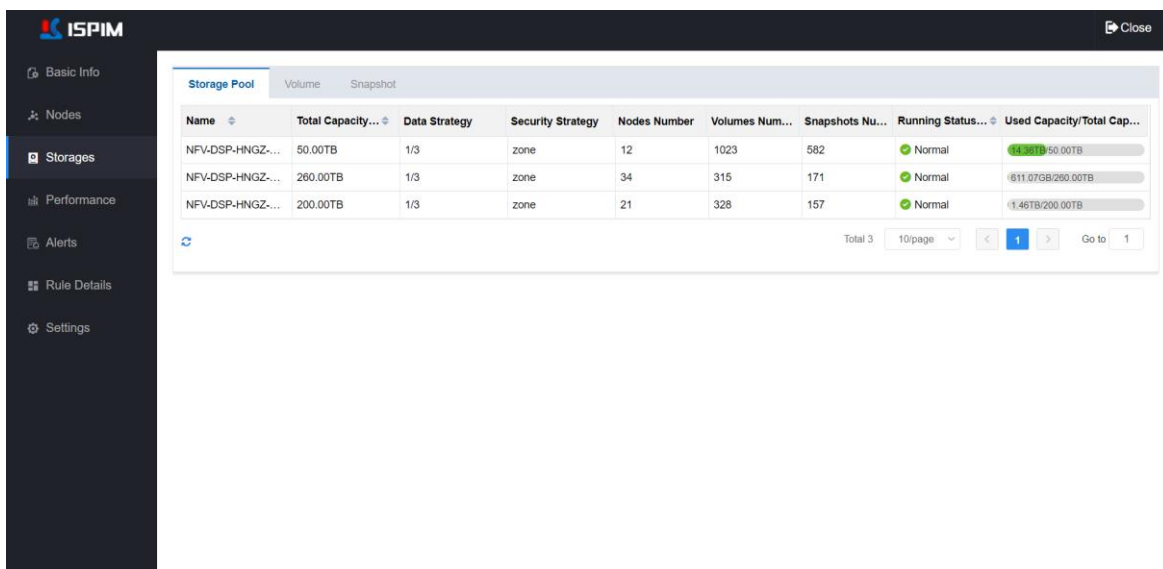


Table 6-9 Device Storage Description

Category	Items
Storage Pool	Name, total capacity, data strategy, security strategy, nodes number, volumes

	number, snapshots number, running status, used capacity/total capacity
Volume	Name, volume capacity, QOS list, creation time, running status, storage pool belonging
Snapshot	Name, volumes, dirty data capacity(GB), creation time, storage pool belonging

## 4. Performance Data

In the device details page, select [Performance] in the left navigation tree, user can enter the performance data page, as shown in Figure 6-26 . In the performance data page, user can view multiple performance statistics curves of the storage device.


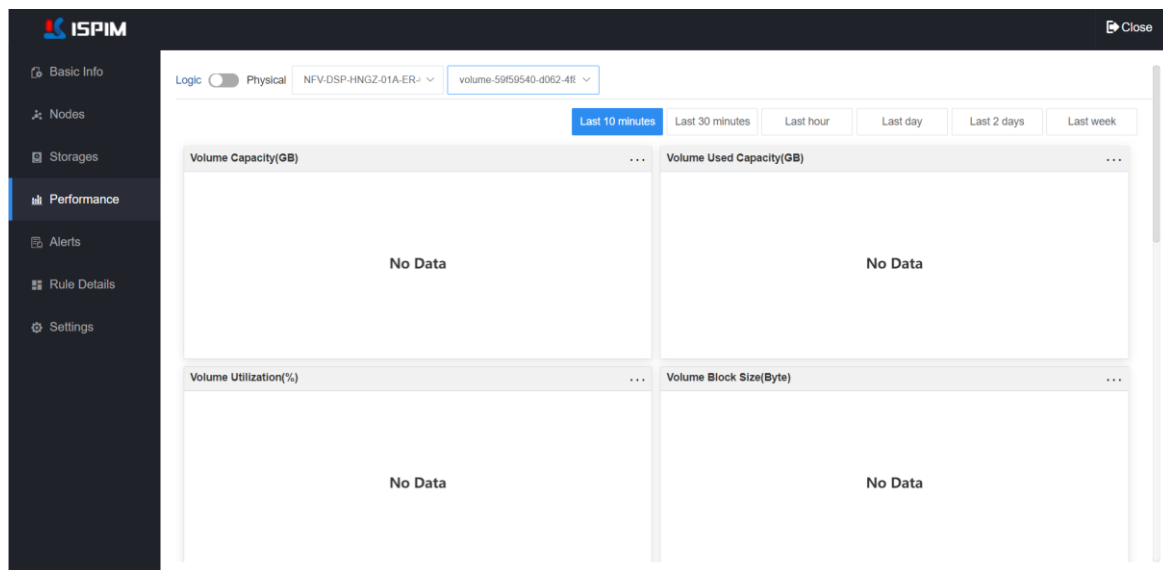
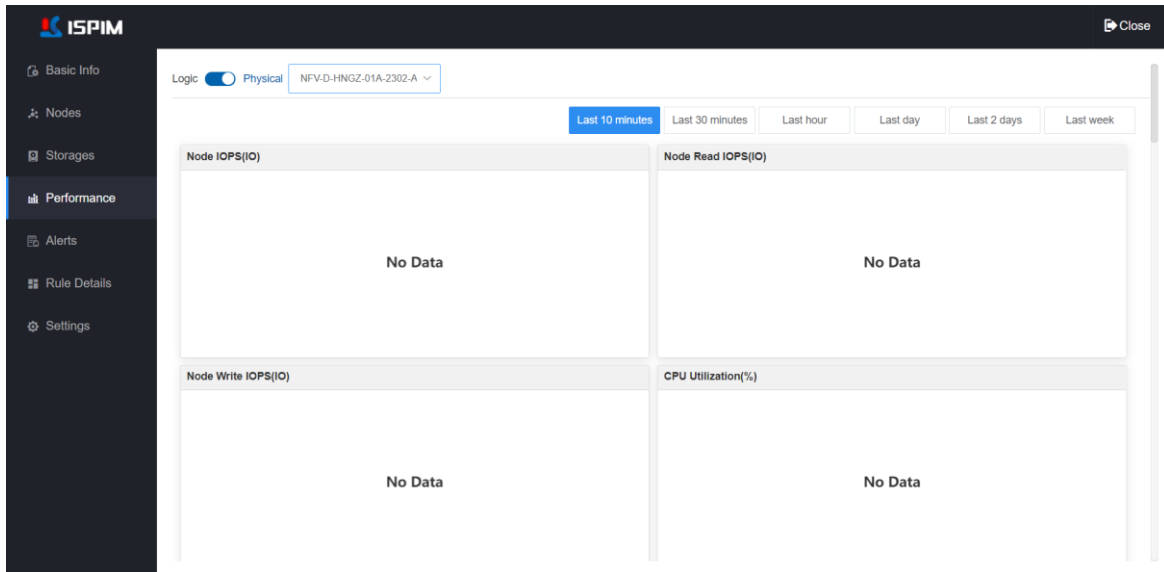
- Select "logical" or "physical" resource information display diagram: click the  icon, user can choose to switch performance data display information.
  - When selecting "Logical", user can drop down to select the resource pool name or volume name to view performance data in different dimensions.
  - When selecting "Physical", user can drop down to select the name of the physical node to view its corresponding node performance data.
- Select the time range: Click the <Last 10 minutes>, <Last 30 minutes>, <Last 1 hour> buttons at the top right of the page to view the device performance data within the corresponding time range.

Figure 6-26 Performance Data

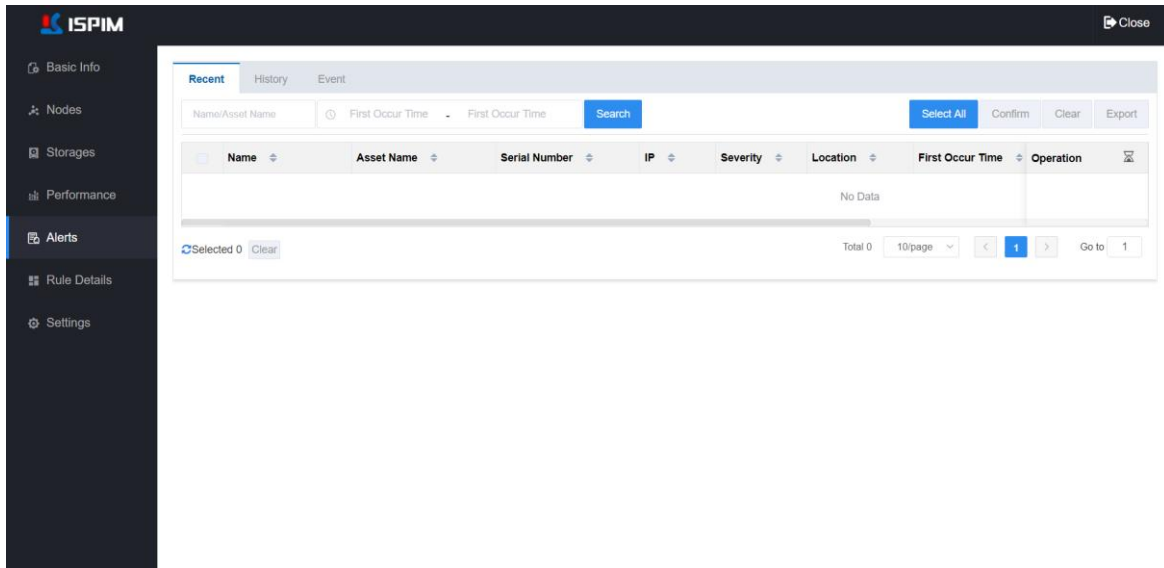




## 5. Alarm List

On the alarm list page, user can view the real-time, history, and event information of the device, as shown in Figure 6-27:

Figure 6-27 Alarm List



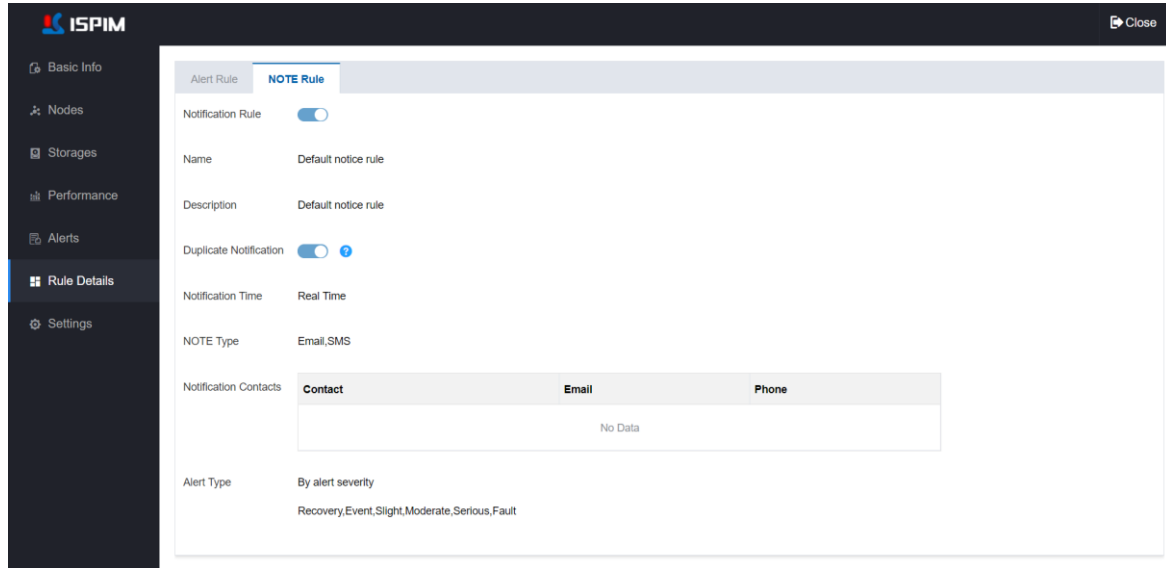
## 6. Rule Details

In the device details module, select [Rule Details] in the left navigation tree, user can enter the rule details page, as shown in Figure 6-28. In the rule details page, user can view storage device alarm rules and notification rules. Select different tabs to view corresponding rule details.



On the rule details page, the rules can only be viewed but cannot be set.

Figure 6-28 Rule Details



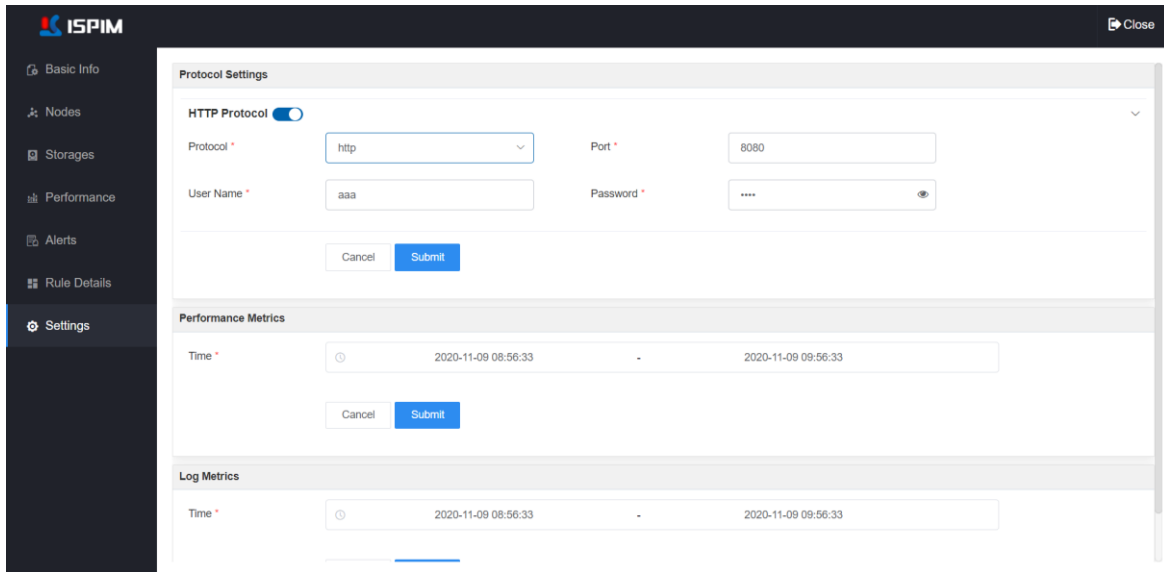
## 7. Settings

In the device details page, select [Settings] in the left navigation list, user can enter the device management page, as shown in Figure 6-29. In the device protocol settings page, user can view and modify the related protocol settings.



- For distributed storage, the supported protocol is HTTP.
- Note: The protocol settings modified on this page only modify the authentication parameters stored in ISIPM, and will not modify the protocol information of the device.

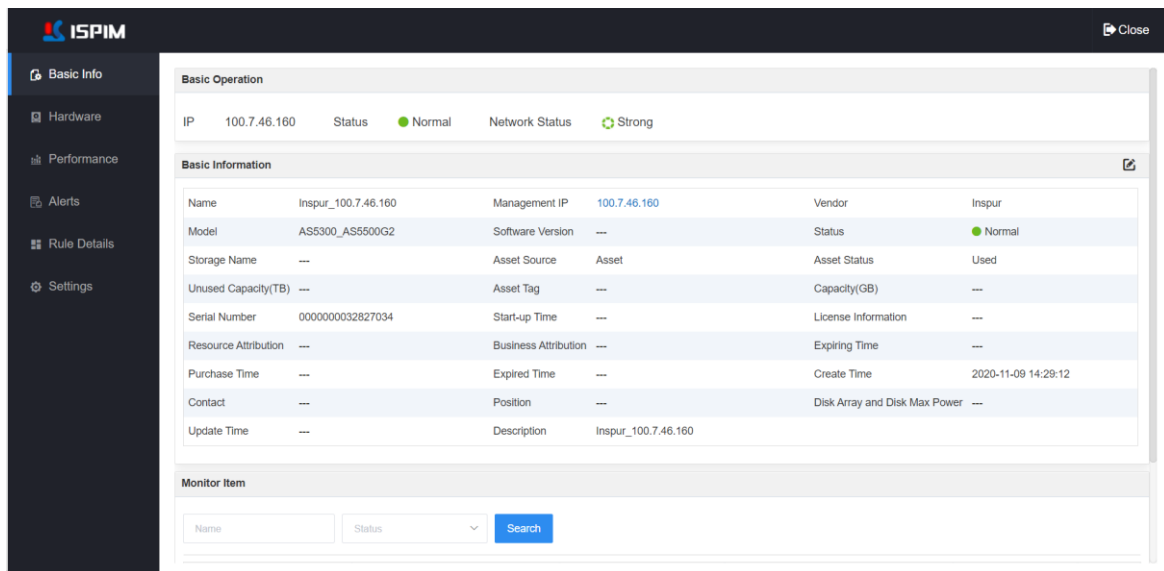
Figure 6-29 Setting Page



## 6.7.4 View Disk Array Detail

In the disk array storage device list, click on a device name, and user will enter the device details page, as shown in Figure 6-30. On this page, user can view and manage the basic information, hardware information, performance data, and alarm list, rules details and settings information.

Figure 6-30 Disk Array Detail




### 1. Basic Info

In the device details page, select [Basic Info] in the left navigation list, user can enter the basic information page, as shown in Figure 6-31. On the basic information page, user can view the basic



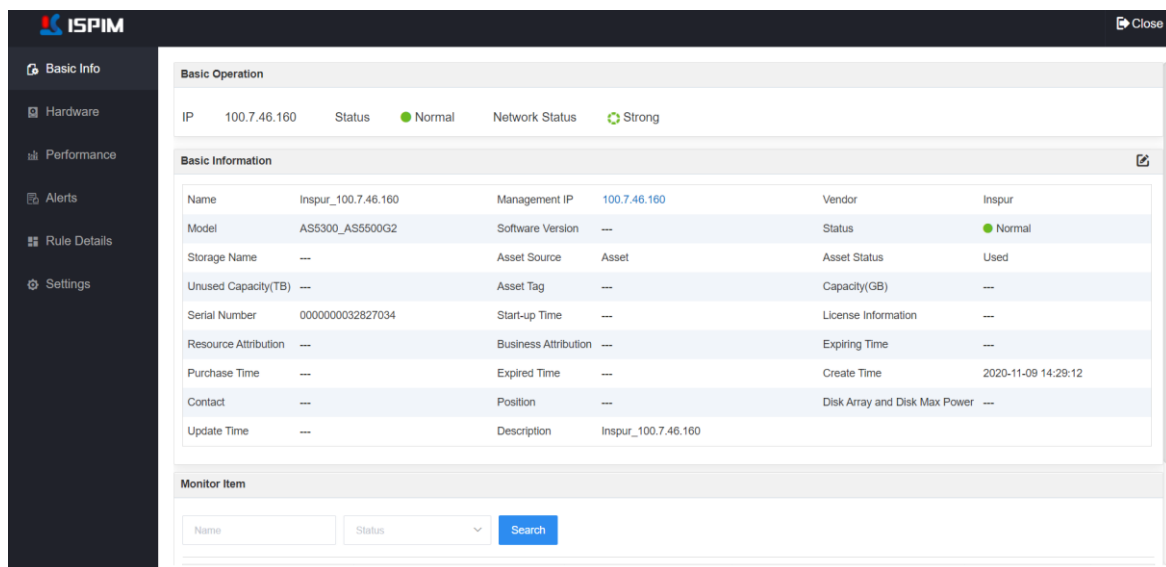
information, monitoring indicators and other information of the disk array. User can also edit device information and view historical curves of monitoring indicators.

- Edit device information: Click the icon in the upper right corner of the basic information operation bar, user can modify the asset name, asset source, asset status and other information in the basic information window that pops up.
- View the historical curve of monitoring items: In the operation area of the monitoring item list, click the  icon corresponding to an indicator, user can view the historical curve change trend graph of the monitoring item in the pop-up window.

 NOTE

- Asset sources include: assets, borrow, custom.
- Asset status includes: used, unused, unavailable, lost, deleted.

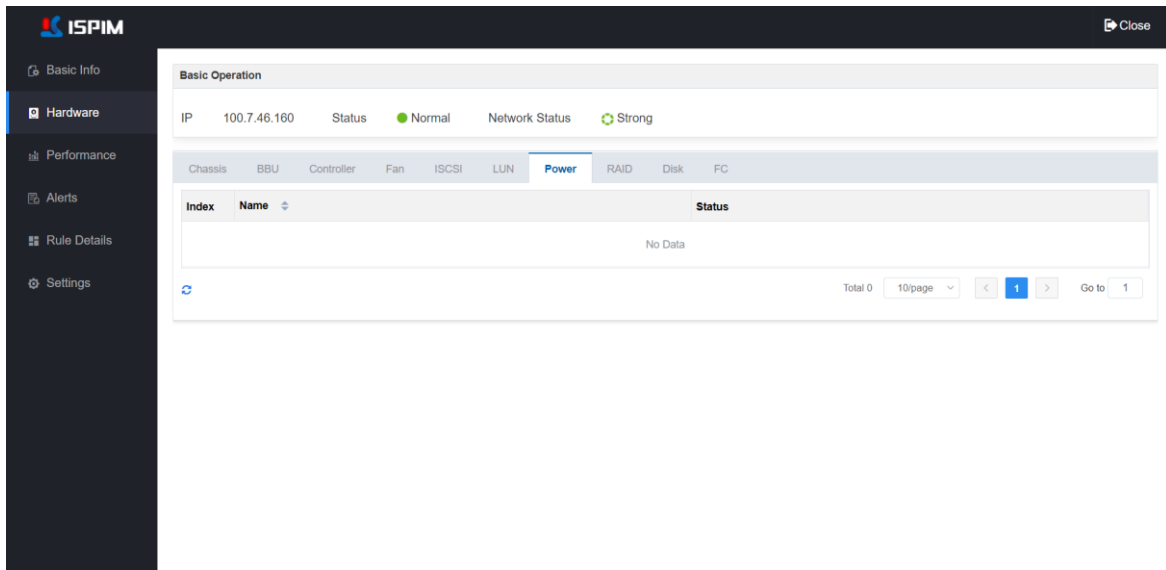
Figure 6-31 Basic Info



## 2. Hardware Info

In the device details page, select [Hardware] in the left navigation list, user can enter the hardware information page, as shown in Figure 6-32. On the hardware information page, user can view the hardware information of the disk array device. Including: Chassis, BBU, controller, fan, ISCSI, LUN, power, RAID, disk and FC information.

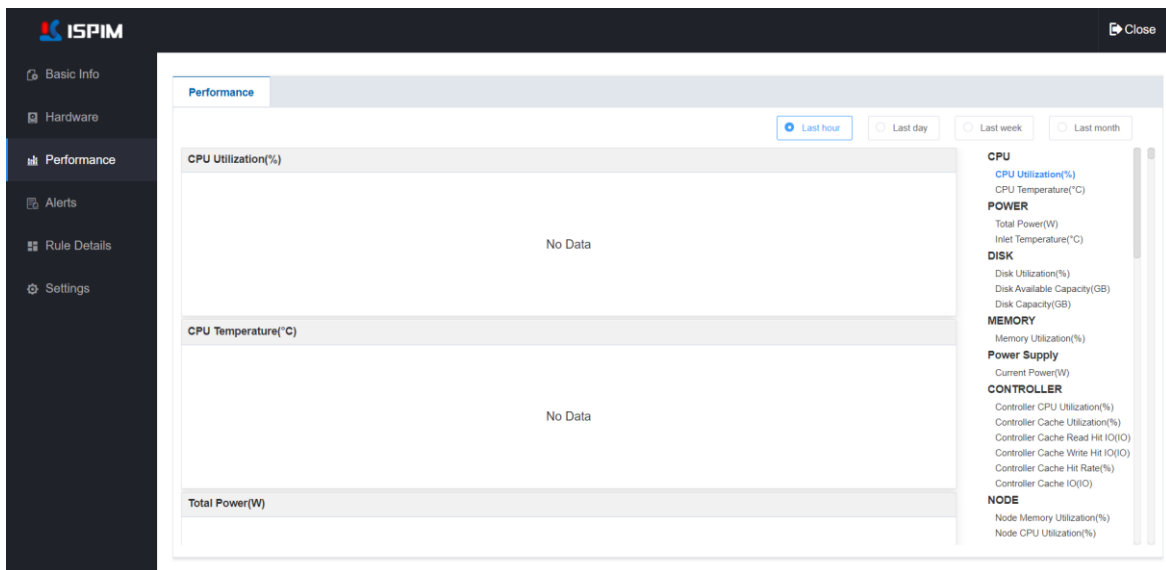
Figure 6-32 Hardware Info



### 3. Performance Data

In the device details page, select [Performance] in the left navigation list, user can enter the performance data page, as shown in Figure 6-33. In the performance data information page, user can view the performance data of the disk array, including CPU, power consumption, disk, memory, power supply, controller, node and other information. Click on the performance item on the right side of the page to view the corresponding performance index data.

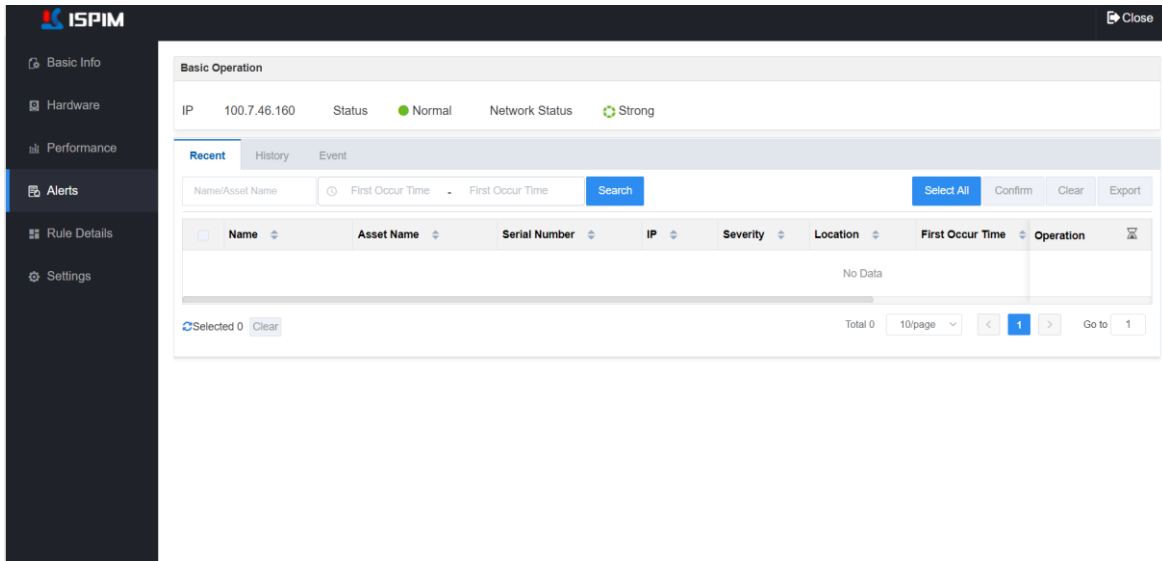
Figure 6-33 Performance Data



## 4. Alarm List

In the device details module, select [Alarms] in the navigation list on the left to enter the alarm list page. On the alarm list page, user can view equipment alarm related information, including real-time, history and events.

Figure 6-34 Alarm List Page



## 5. Rule Details

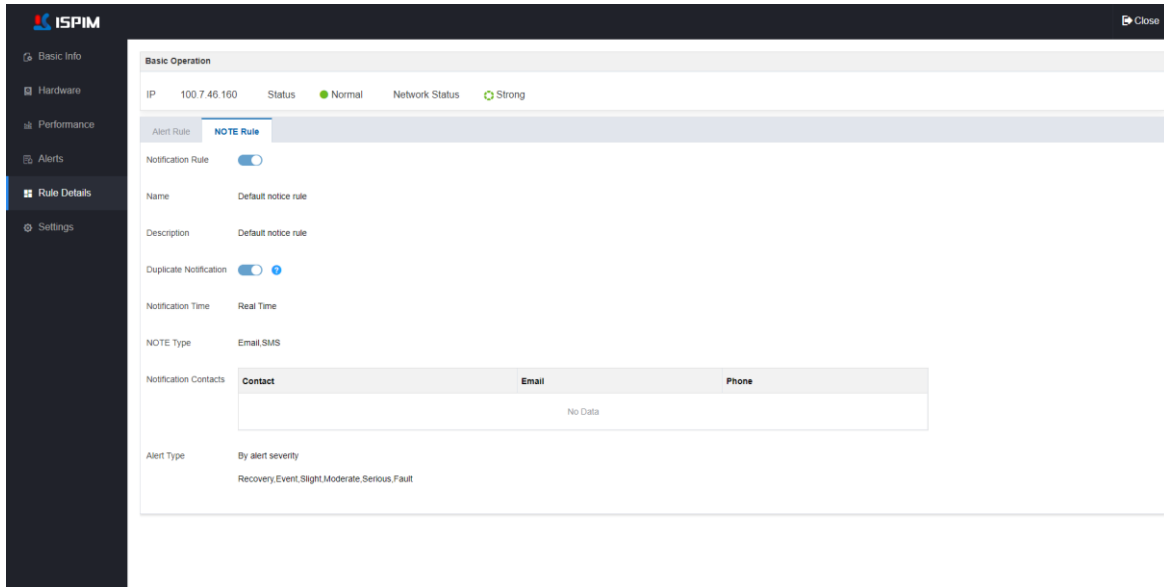
In the device details page, select [Rule Details] in the left navigation list, user can enter the rule details page, as shown in Figure 6-35.

In the rule details page, user can view the device alarm rule and notification rule. Select different tabs to view the corresponding rule details.

### NOTE

On the rule details page, the rules can only be viewed but cannot be set.

Figure 6-35 Rule Details



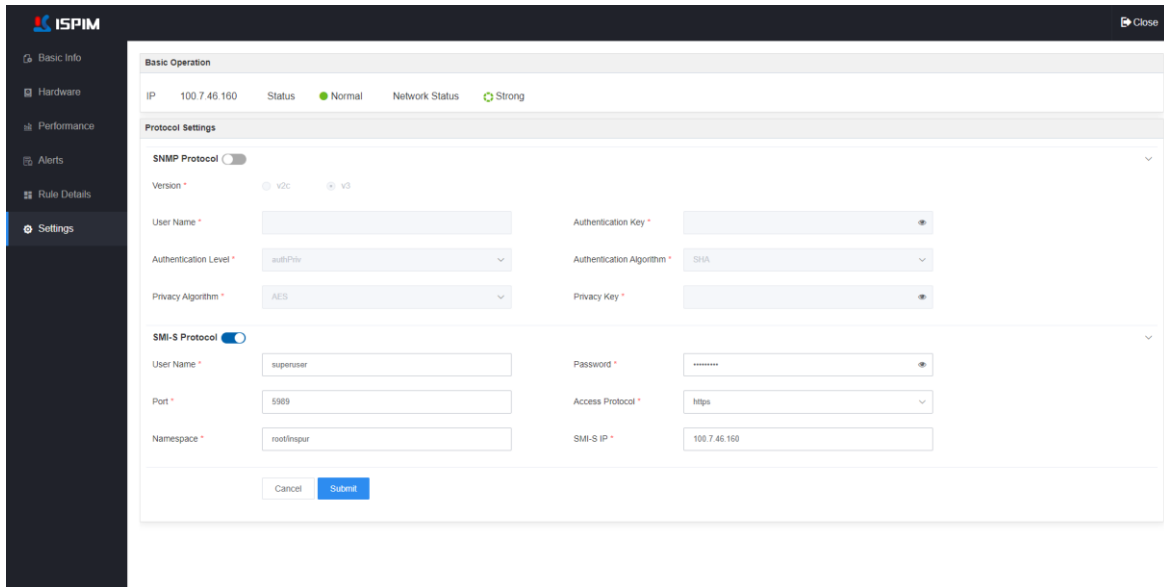
## 6. Settings

In the device details page, select [Settings] in the left navigation list, user can enter the protocol setting page, as shown in Figure 6-36. In the device protocol setting page, user can view and modify the relevant protocol information.

### NOTE

- For disk array, the supported protocols are SNMP and SMI-S.
- Note: The protocol settings modified on this page only modify the authentication parameters stored in ISIPM, and will not modify the protocol information of the device.

Figure 6-36 Protocol Settings



## 6.8 Network Device Management

In ISIPM supports adding switches, routers, SDN devices through "auto discovery" or "batch import". User can perform operations such as bookmarking, resetting rules, resetting protocols, editing, and deleting.

### 6.8.1 Add Network Device

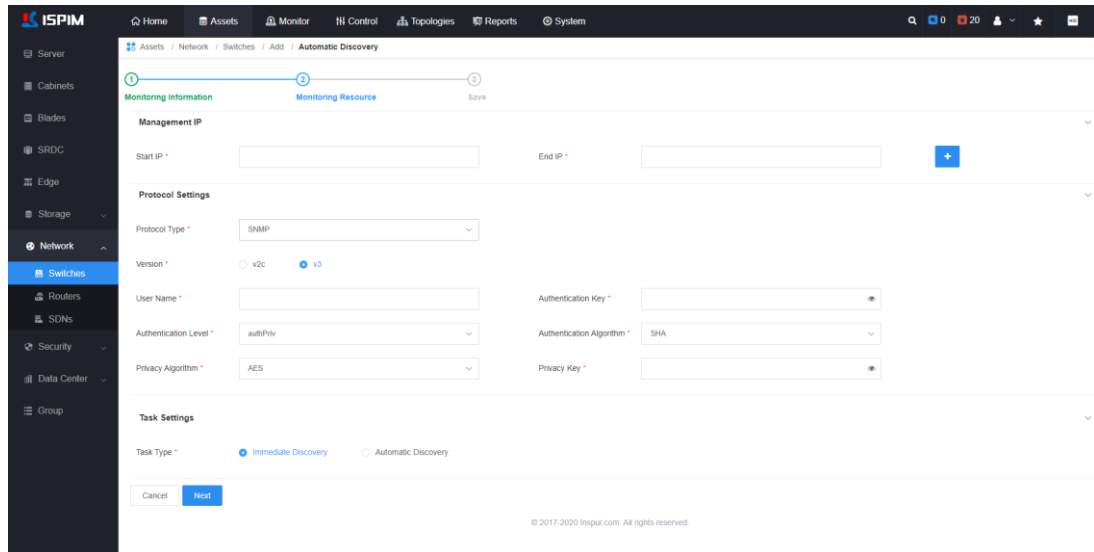
The process of adding different types of network devices is similar. The difference is only in the authentication protocol type and parameters. For each network device type and protocol type, the description is shown in Table 6-1. This chapter uses adding switch devices as an example to introduce the process of adding network equipment.

#### 1. Automatic Discovery


To add a switch device in ISIPM using "auto discovery" mode, the operation is as follows:

**Step 1** Click [Assets] -> [Network] -> [Switches] to enter the switch page.

**Step 2** Click <Add>, select "Auto Discovery" in the drop-down box, and enter the automatic discovery configuration page, as shown in the figure below.



**Step 3** Configure discovery related parameters such as IP address, protocol information and task type.

- Set the device IP range. The first three parts of the device's start IP and end IP must be the same (ISPIM defaults to 255.255.255.0 as the subnet mask). If the devices are located in different networks, user can click the  icon to add multiple IP ranges. To add a single device, enter the same start IP and end IP.
- Protocol configuration: Select the protocol related parameters.
- Task Type: Select task category.
  - When selecting “Automatic Discovery”, user needs to configure the task name, task frequency, and start time, and the subsequent steps will not be triggered. After that, user can view the task execution status in the task center. For details about the task center, please refer to 11.3Task.
  - When selecting “Immediate Discovery”, user needs to click <Next> to enter the asset scanning step and start scanning the server.

**Step 4** After the scan is completed, click <Next> to enter the device save page, the successfully scanned devices are displayed in the list, and click the <Submit> button to add the devices to ISPIM.

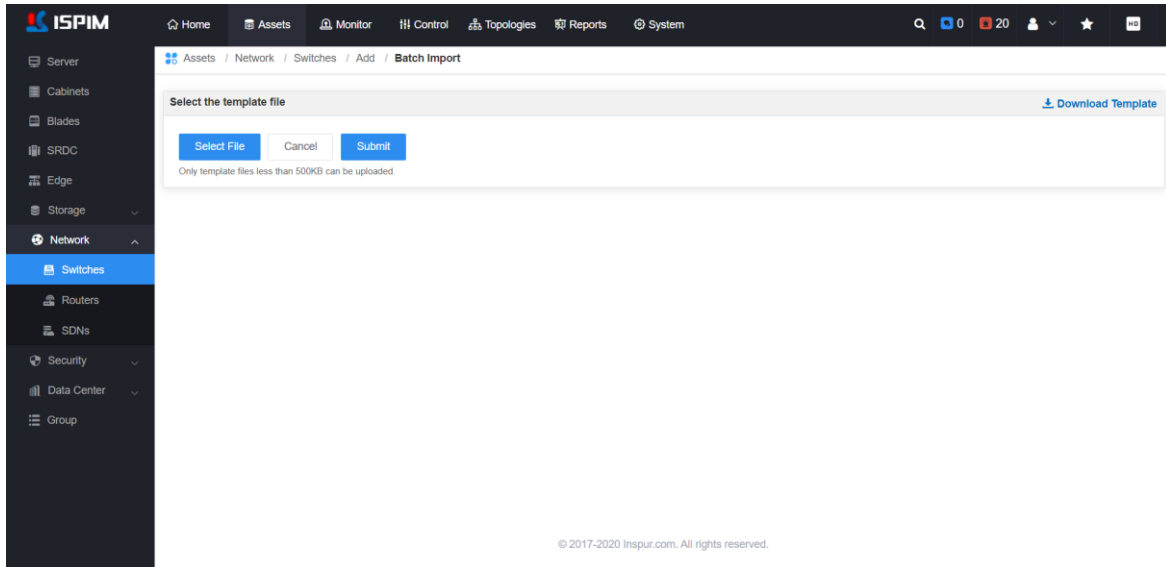
----End

## 2. Batch Import

The operation of adding edge devices in ISPIM in the way of "batch import" is as follows:

**Step 1** Click [Assets] -> [Network] -> [Switches] to enter the switch page.

**Step 2** Click <Add>, select "Batch Import" in the drop-down box, and enter the batch import page, as shown in the figure below.



**Step 3** Click <Download Template>, edit the downloaded template and configure the relevant information. Among them, the field marked with "\*" in the template is required.

**Step 4** After editing the template, click <Select File> to upload the edited template file, and click the <Submit> button to start scanning the device.


**Step 5** After the scan is completed, click <Next> to enter the device save page. The successfully scanned devices are displayed in the list. Click the <Submit> button to add multiple devices to ISIPM in batches.

----End

## 6.8.2 View Network Device List

After the switch, router or SDN network device is added, user can view the managed switch information in the network device list, as shown in Figure 6-37. User can view the device name, status, model, manufacturer, and serial number and other information in the switch list. User can edit, refresh, delete the device.

Table 6-10 Network Device Operations

Operation	Description
	Click this icon to edit the basic information and protocol parameters of the switch.



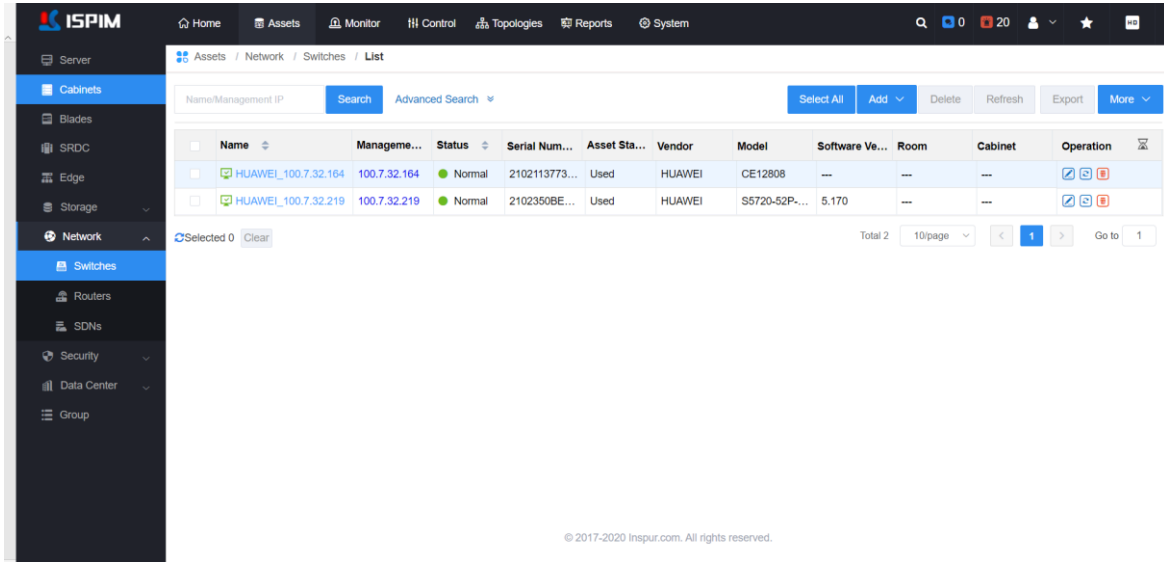
	Click this icon to trigger the collection of switch hardware information and refresh.
	Click the icon and confirm, user can delete the corresponding switch.

Figure 6-37 Switches List



 NOTE

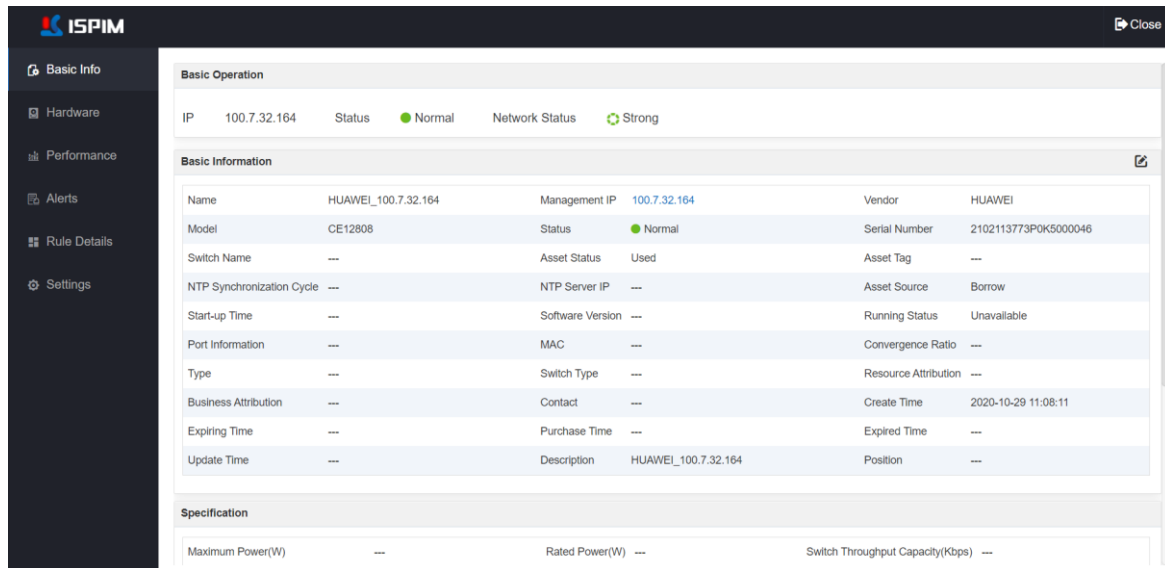
The operation of viewing the router and SDN device list is similar to that of viewing the switch list. For details, please refer to the actual page.

### 6.8.3 View Switch Detail

In the switch device list, click on a device name to enter the device details page, as shown in Figure 6-38. On this page, user can view the basic information, hardware information, performance data, alarm list, rule details and settings of the device.

Figure 6-38 Device Detail





## 1. Basic Info


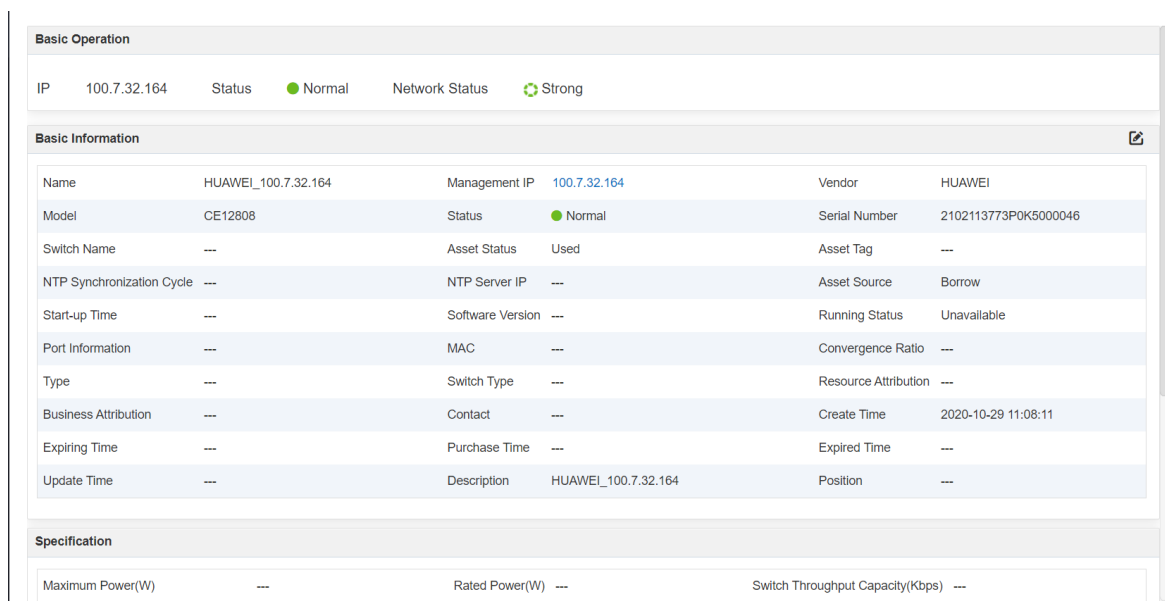
In the device details page, select [Basic Info] in the left navigation list, user can enter the basic information page, as shown in Figure 6-39. In the basic information page, user can view the basic information of the switch device (name, management IP, manufacturer, port Information, location, ownership, etc.), specification information, monitoring items. Click the  icon of the basic information module, in the basic information window that pops up, user can edit the basic information of the switch.

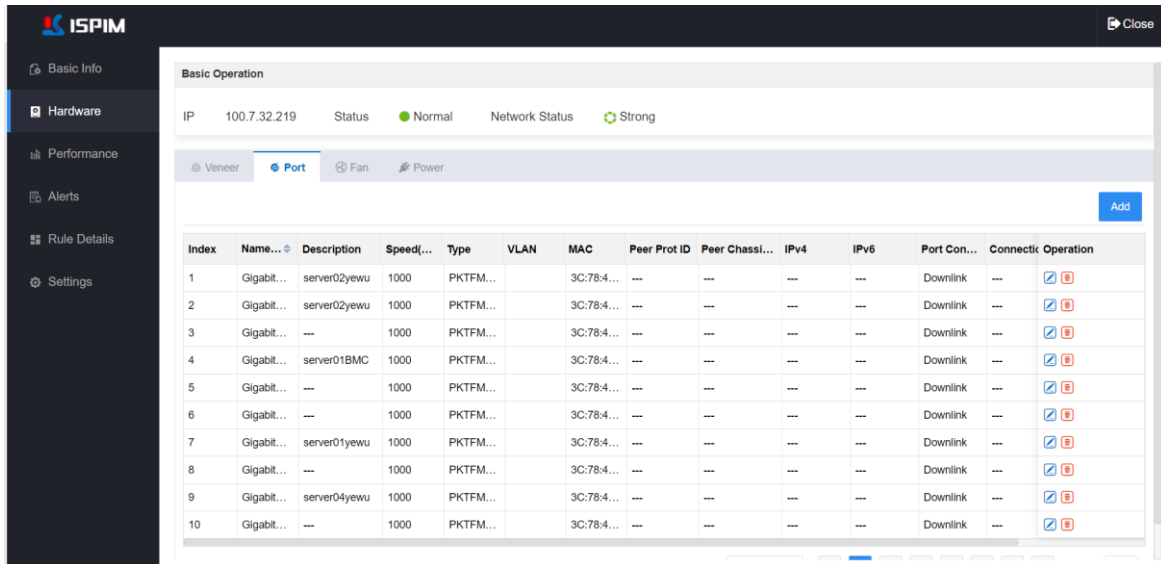
Figure 6-39 Basic Info



## Hardware Info

In the device details module, select [Hardware] in the left navigation list, user can enter the hardware information page, as shown in Figure 6-40. On the hardware information page, user can view the hardware information of the switch, including: board info, port, fan, power.

Figure 6-40 Hardware Info

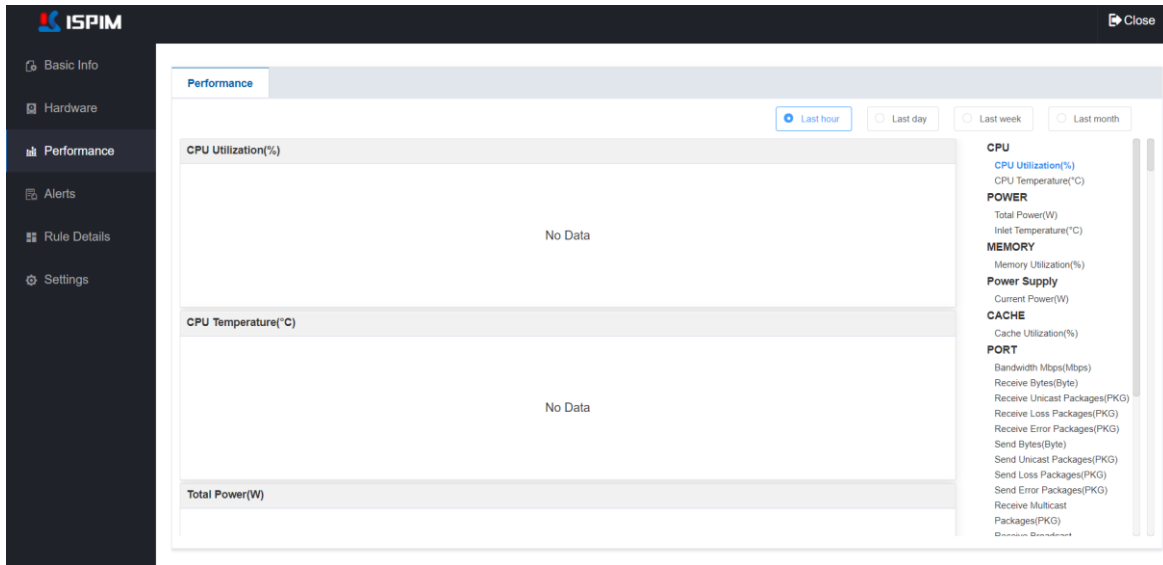


## 2. Performance Data

In the device details module, select [Performance] in the left navigation list, user can enter the performance data page, as shown in Figure 6-41. In the performance data page, user can view the performance statistics curve statistics of the switch device.

- Select the time range: Click the <Last 10 minutes>, <Last 30 minutes>, <Last 1 hour> buttons at the top right of the page to view the device performance data within the corresponding time range.
- Select performance items: In the items list on the right side of the performance data page, click the corresponding index item to view the performance curve statistics of the corresponding item.

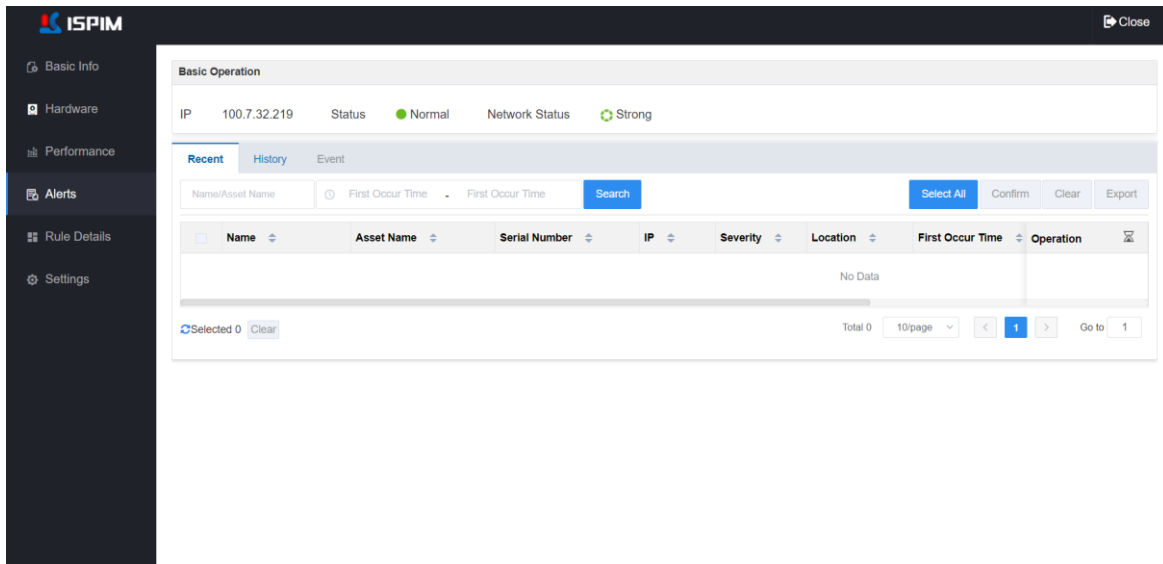
Figure 6-41 Performance Data



### 3. Alarm List

In the device details page, select [Alarms] in the left navigation list, user can enter the alarms page. On the alarm list page, user can view the real-time, history, and event information of the device.

Figure 6-42 Alarm List



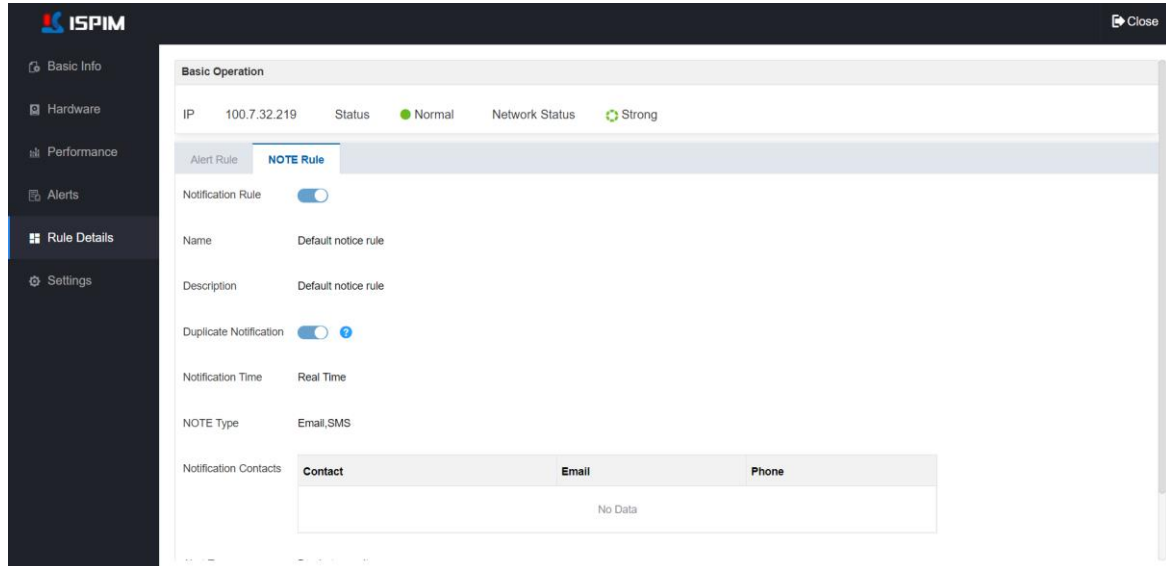
### 4. Rule Details

In the device details page, select [Rule Details] in the left navigation list, user can enter the rule details page. In the rule details page, user can view the device alarm rules and notification rules. Select a different tab to view the corresponding rule details.



On the rule details page, the rules can only be viewed but cannot be set.

Figure 6-43 Rule Details



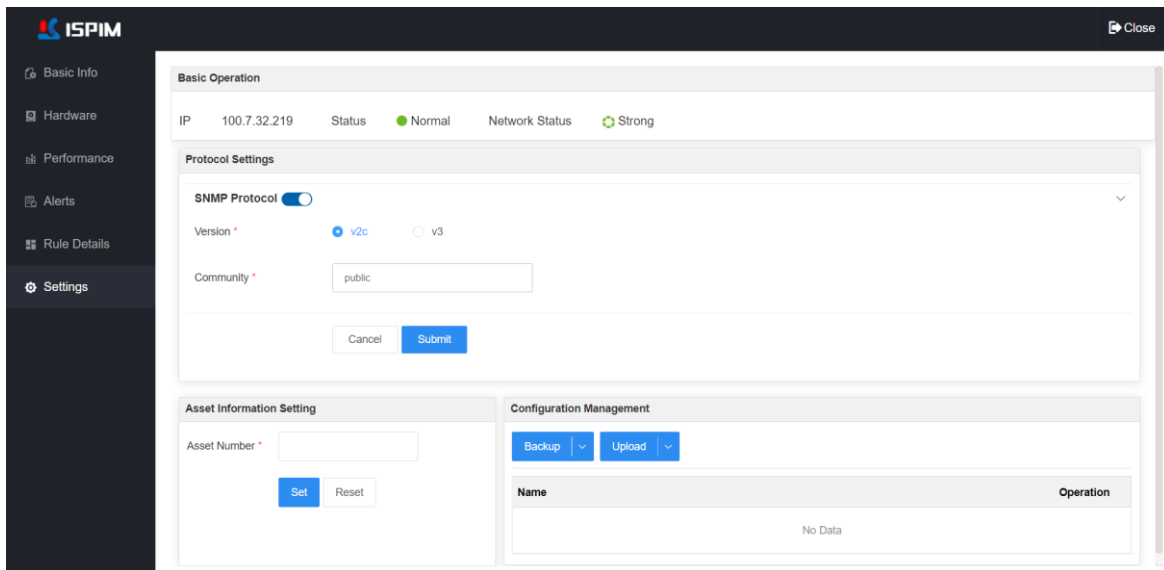
## 5. Settings

In the device details page, select [Settings] in the left navigation list, user can enter the settings page, as shown in Figure 6-44. In the device protocol settings page, user can view and modify the related settings.



- For switch device, the supported protocol is SNMP.
- Note: The protocol settings modified on this page only modify the authentication parameters stored in ISIPM, and will not modify the protocol information of the device.

Figure 6-44 Settings Page



## 6.8.4 View Router Detail

Viewing router device details is similar to viewing switch device details, please refer to the actual page for details.

## 6.8.5 View SDN Device Detail

### 1. Basic Info


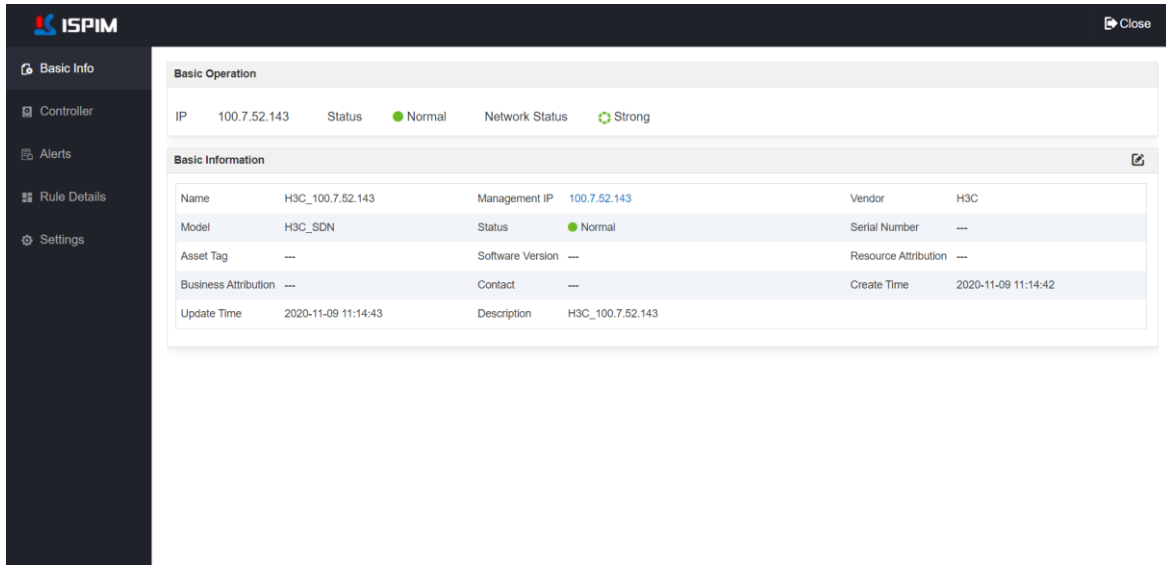
In the device details page, select [Basic Info] in the left navigation list to enter the basic information page, as shown in Figure 6-45. In the basic information page, user can view the basic information of the SDN device (name, management IP, manufacturer, model). Click the  icon, in the basic information window that pops up, user can edit the basic information of the SDN device.

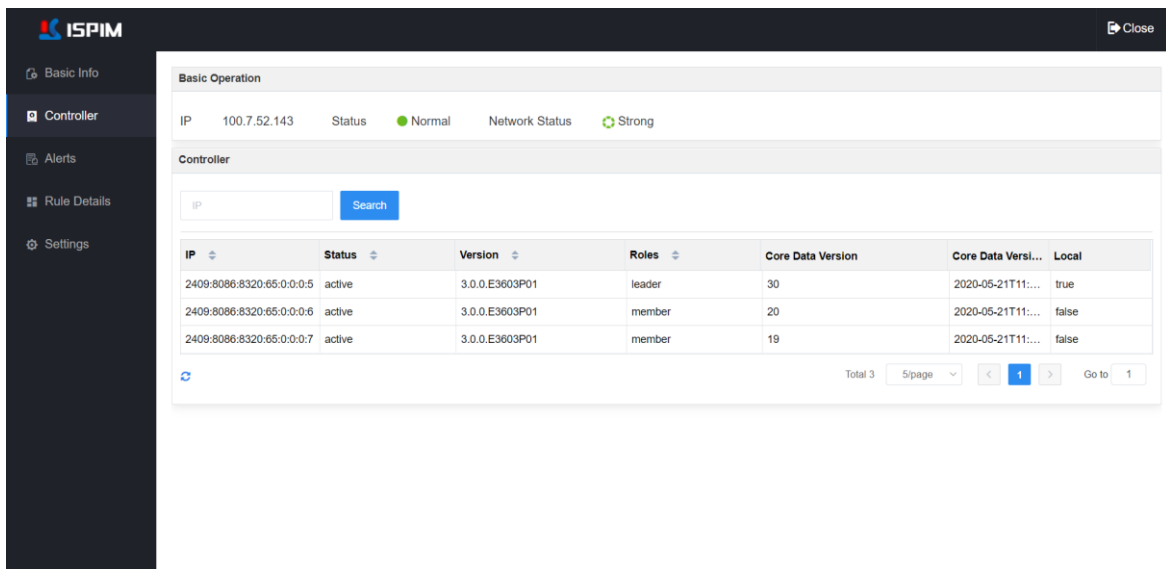
Figure 6-45 Basic Info



## 2. Controller Info

In the device details page, select [Controller] in the left navigation list, user can enter the controller page, as shown in Figure 6-46. On the controller page, user can view the SDN device controller information, including IP address, status, version, role, core data version.

Figure 6-46 Controller Info

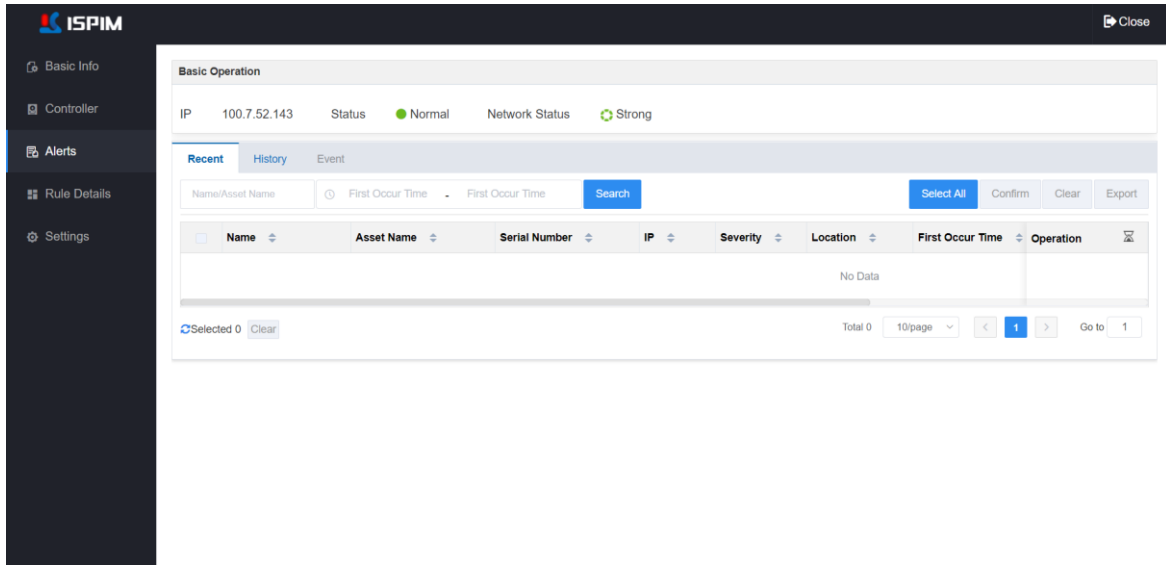


## 3. Alarm List

In the device details page, select [Alarms] in the left navigation list, user can enter the alarm list page, as shown in Figure 6-47, on the alarm list page user can view the real-time, history, and event

information of the device.

Figure 6-47 Alarm List



## 4. Rule Details

In the device details page, select [Rule Details] in the left navigation list, user can enter the rule details page, as shown in On the rule details page, the rules can only be viewed but cannot be set.

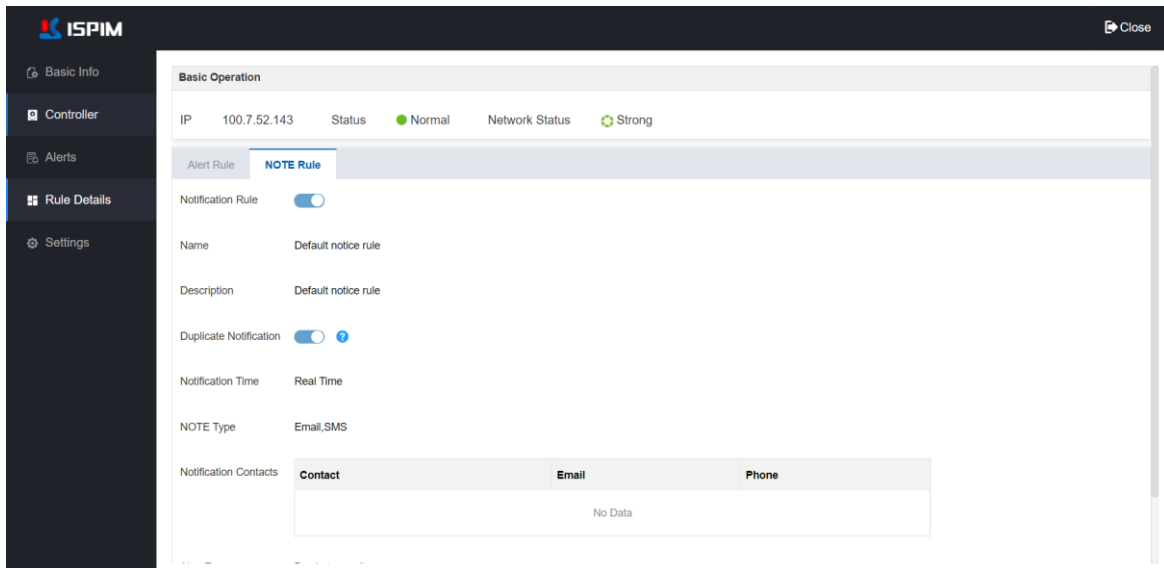
Figure 6-48. In the rule details page, user can view the device alarm rules and notification rules. Select different tabs to view details of the rules.



### NOTE

On the rule details page, the rules can only be viewed but cannot be set.

Figure 6-48 Rule Details



## 5. Settings

In the device details page, select [Settings] in the left navigation list, user can enter the settings page, as shown in For switch device, the supported protocol is SNMP.

- Note: The protocol settings modified on this page only modify the authentication parameters stored in ISIPM, and will not modify the protocol information of the device.

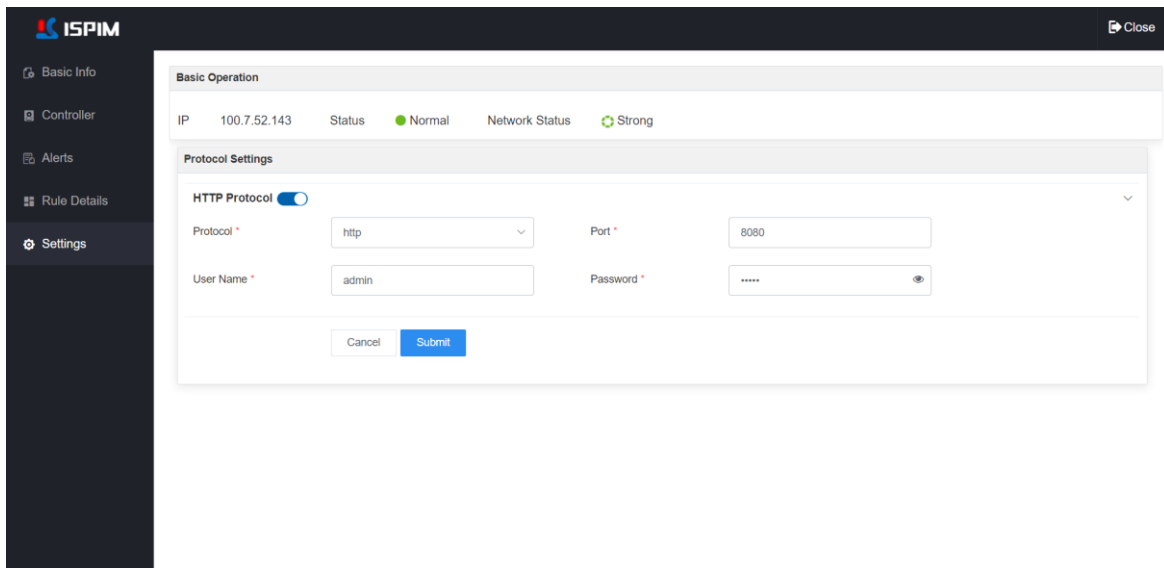
Figure 6-49. In the device protocol settings page, user can view and modify the related settings.

### NOTE

- For switch device, the supported protocol is SNMP.
- Note: The protocol settings modified on this page only modify the authentication parameters stored in ISIPM, and will not modify the protocol information of the device.

Figure 6-49 Settings





## 6.9 Security Device Management

In ISIPM supports adding firewalls and IDS/IPS security devices through "auto discovery" or "batch import", and user can perform operations such as bookmarking, resetting rules, resetting protocols, editing, and deleting.

### 6.9.1 Add Security Device

The process of adding different types of security devices is similar. For details, please refer to the actual page. The protocol descriptions of various devices are shown in the Table 6-1. This chapter uses adding "firewall" as an example to introduce the process of adding security devices.

#### 1. Automatic Discovery

The operation of adding a firewall in ISIPM by "auto discovery" is as follows:

**Step 1** Click [Assets] -> [Security] -> [Firewall] to enter the firewall management page.


**Step 2** Click <Add>, and select "Auto Discovery" to enter the auto discovery firewall configuration page, as shown in the figure below.

The screenshot shows the 'Protocol Configuration' step of the automatic discovery process. It includes the following fields and options:

- IP Address:** Start IP and End IP input fields with a '+' icon to add multiple ranges.
- Protocol Configuration:**
  - Protocol Type: SNMP
  - Version: v2c (radio), v3 (radio)
  - Username: [input field]
  - Authentication Method: SHA
  - Authentication Key: [input field]
  - Authentication Level: MD5Priv
  - Encryption Method: AES
  - Encryption Key: [input field]
- Task Settings:**
  - Task Type: Immediate Discovery (selected), Automatic Discovery

Buttons at the bottom include 'Cancel' and 'Next Step'.

**Step 3** Configure discovery related parameters such as IP address, protocol information and task type.

- Set the device IP range. The first three parts of the device's start IP and end IP must be the same (ISPIM defaults to 255.255.255.0 as the subnet mask). If the devices are located in different networks, user can click the  icon to add multiple IP ranges. To add a single device, enter the same start IP and end IP.
- Protocol configuration: Select the protocol related parameters.
- Task Type: Select task category.
  - When selecting “Automatic Discovery”, user needs to configure the task name, task frequency, and start time, and the subsequent steps will not be triggered. After that, user can view the task execution status in the task center.
  - When selecting “Immediate Discovery”, user needs to click <Next> to enter the asset scanning step and start scanning the server.

**Step 4** After the scan is completed, click <Next> to enter the device save page, the successfully scanned devices are displayed in the list, and click the <Submit> button to add the devices to ISPIM.

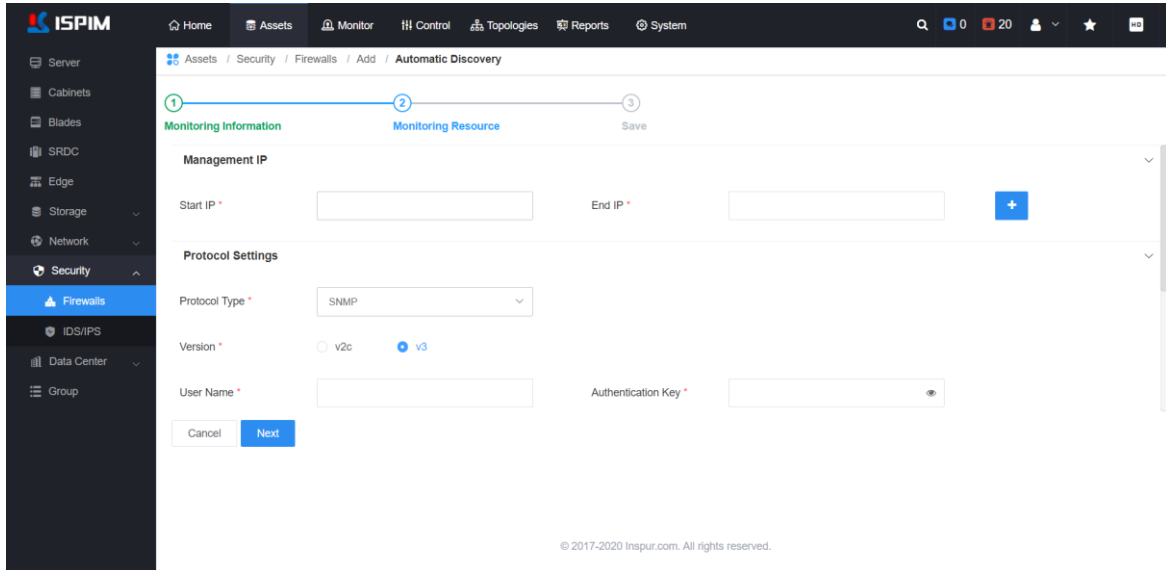
----End

## 2. Batch Import

The operation of adding firewall devices in ISPIM in the way of "batch import" is as follows:

**Step 1** Click [Assets] -> [Network] -> [Switches] to enter the switch page.

**Step 2** Click <Add>, select "Batch Import" in the drop-down box, and enter the batch import page, as shown in the figure below.



**Step 3** Click <Download Template>, edit the downloaded template and configure the relevant information. Among them, the field marked with "\*" in the template is required.

**Step 4** After editing the template, click <Select File> to upload the edited template file, and click the <Submit> button to start scanning the device.



**Step 5** After the scan is completed, click <Next> to enter the device save page. The successfully scanned devices are displayed in the list. Click the <Submit> button to add multiple devices to ISPIPM in batches.

----End

## 6.9.2 View Security Device List

After the firewall or ISD/IPS security device is added, user can view the managed security device information in the security device list. User can view the device name, management IP, serial number, manufacturer, model info. User can edit, refresh, delete the device.

Table 6-11 Security Device Operations

Operation	Description
	Click this icon to edit the basic information and protocol parameters of the device.
	Click this icon to trigger the collection of device hardware information and refresh.



Click the icon and confirm, user can delete the corresponding device.



#### NOTE

The operation of viewing the IDS/IPS device list is similar to the that of viewing the firewall list.

Please refer to the actual page for details.

## 6.9.3 View Firewall Device Detail

### 1. Basic Info

In the device details page, select [Basic Info] in the left navigation list, user can enter the basic information page, as shown in Figure 6-50. In the basic information page, user can view the device related information, such as basic information (name, management IP, manufacturer, model), specification information (maximum power, rated power, throughput, number of concurrent connections, etc.), monitoring items.



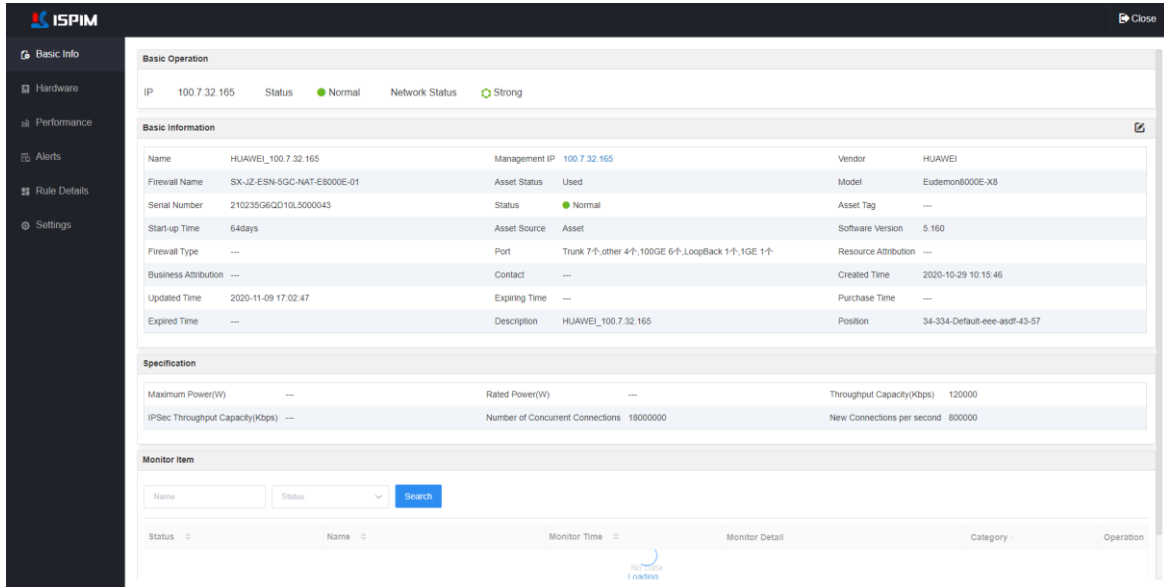
- On the basic information page, click the  icon, and in the basic information window that pops up, user can edit the basic information of the firewall device.
- On the monitoring item page, click the  icon corresponding to the monitoring item, and in the pop-up historical curve graph, user can view the historical curve change graph of the monitoring item.

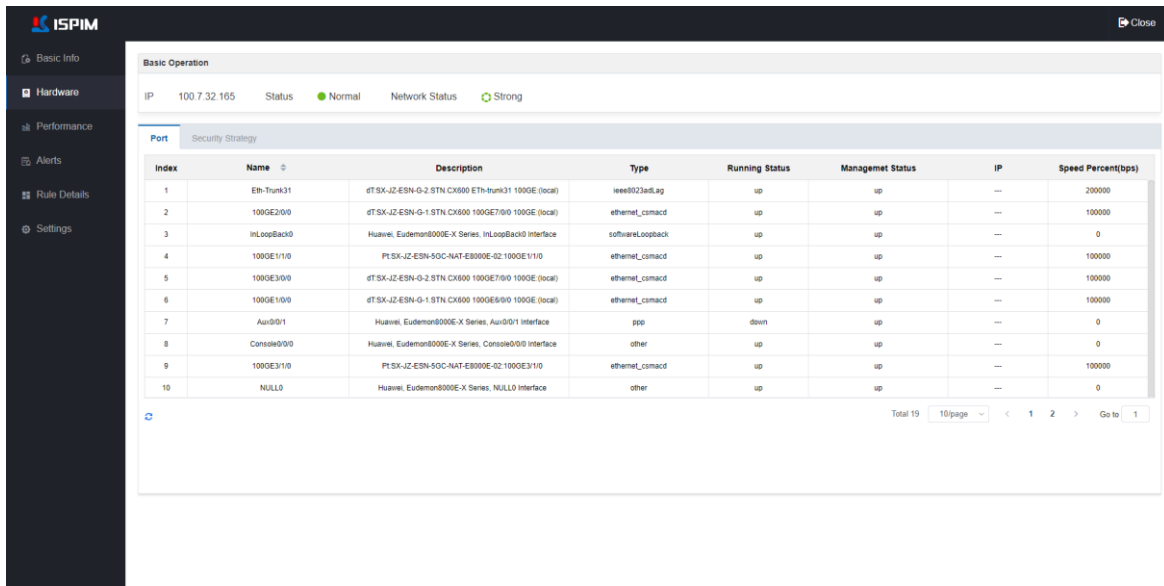
Figure 6-50 Basic Info



## 2. Hardware Info

In the device details module, select [Hardware] in the left navigation list, user can enter the hardware information page, as shown in Figure 6-51. On the hardware information page, user can view the hardware information of the firewall device, such as port and security policy.

Figure 6-51 Hardware Info



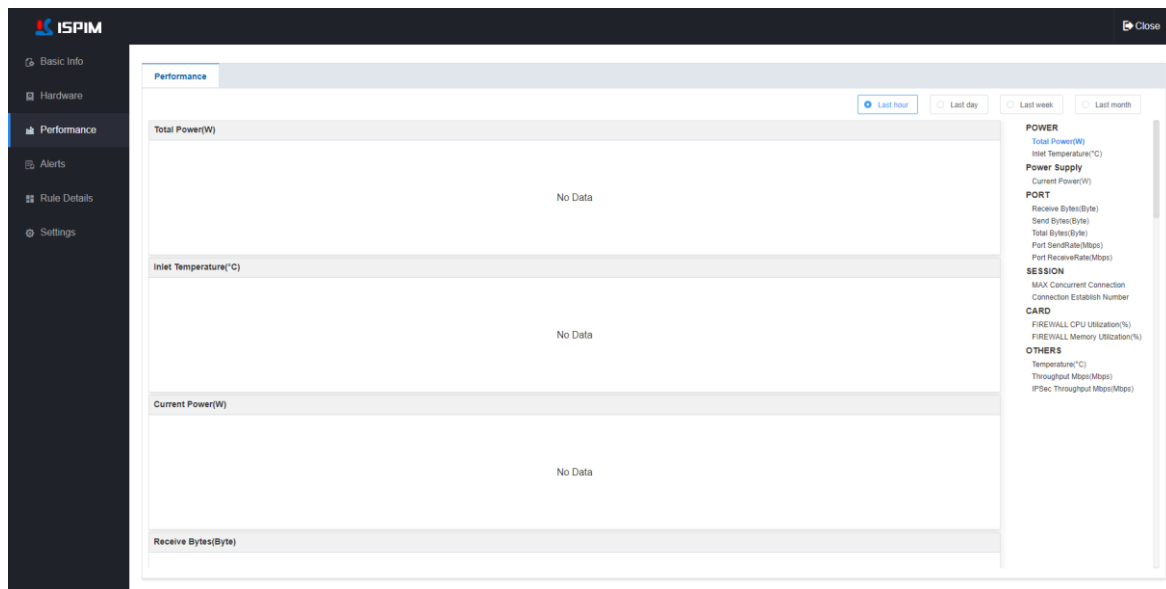
## 3. Performance Data

In the device details page, select [Performance] in the left navigation list, user can enter the

performance data page, as shown in Figure 6-52. On the performance data page, user can view the performance statistics curve statistics of the switch device.

- Select the time range: Click the <Last 10 minutes>, <Last 30 minutes>, <Last 1 hour> buttons at the top right of the page to view the device performance data within the corresponding time range.
- Select performance items: In the items list on the right side of the performance data page, click the corresponding index item to view the performance curve statistics of the corresponding item.

Figure 6-52 Performance Data



## 4. Alarm List

In the device details page, select [Alarms] in the navigation list. In the alarm list page, user can view the real-time, history, and event information of the device.

## 5. Rule Details

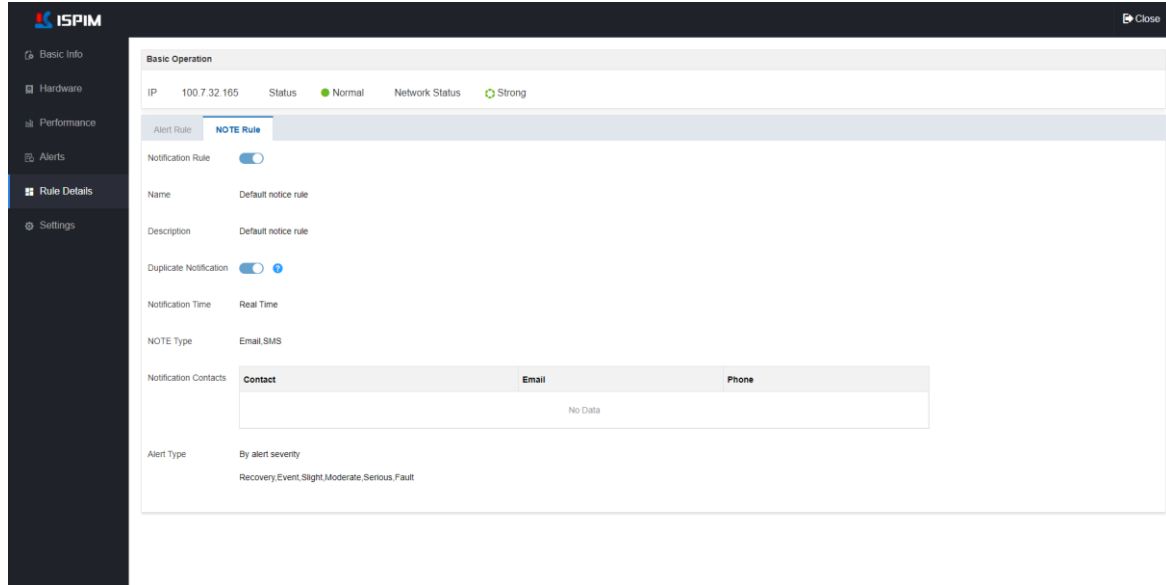
In the device details module, select [Rule Details] in the left navigation list, user can enter the rule details page, as shown in Figure 6-53. In the rule details page, user can view the device alarm rules and notification rules. Select different tabs to view the corresponding rules.



## NOTE

On the rule details page, the rules can only be viewed but cannot be set.

Figure 6-53 Rule Detail



## 6. Settings

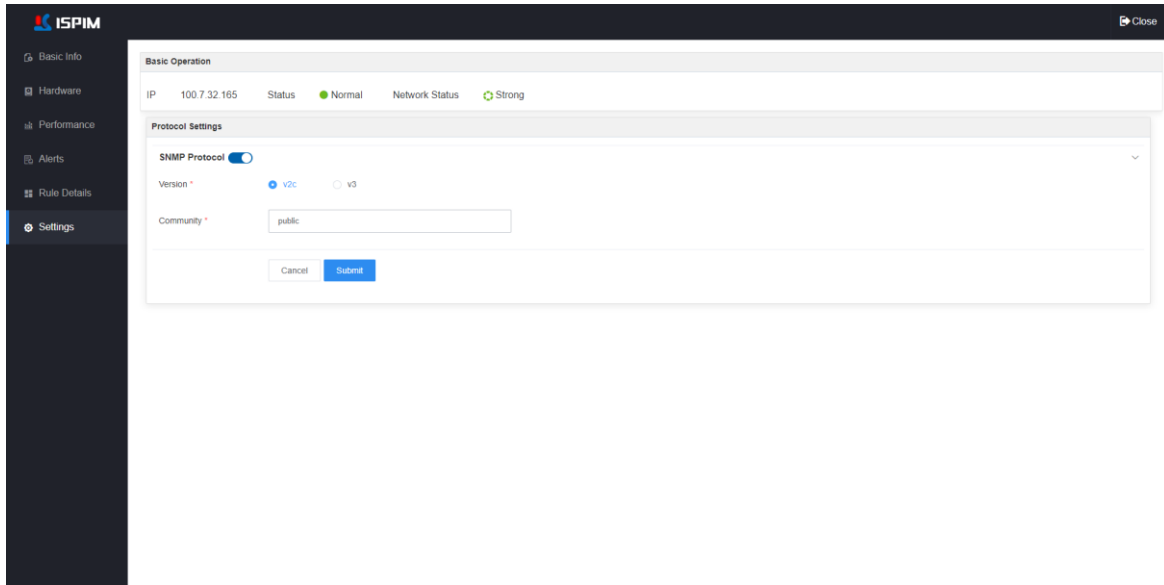
In the device details page, select [Settings] in the left navigation list, user can enter the settings page, as shown in Figure 6-54. In the device protocol settings page, user can view and modify the related settings.



## NOTE

- For firewall device, the supported protocol is SNMP.
- Note: The protocol settings modified on this page only modify the authentication parameters stored in ISPM, and will not modify the protocol information of the device.

Figure 6-54 Settings



## 6.9.4 View IDS/IPS Device List

Viewing IDS/IPS device details is similar to viewing firewall device details, please refer to the actual page for content details.

## 6.10 General Operation of Equipment

In the ISIPM platform, user can perform operations such as querying, collecting, assigning, and resetting protocols on the managed equipment (including servers, cabinets, blades, edge devices, all-in-one devices, storage, network equipment, security equipment, etc.). This chapter take the server as an example to introduce the general operation of the device.

### 1. Search

In ISIPM, it is supported to use keywords such as manufacturer, serial number, room, cabinet, etc. to perform fuzzy query on the managed equipment.

### Procedure

**Step 1** Click [Assets] -> [Server] in turn to enter the server page

**Step 2** At the top of the asset list, click <Advanced Search>, enter or select the corresponding search criteria in the search box on display, and click the <Search> button.



The asset list will correspondingly display a list of devices that meet the search criteria.

----End


## 2. Equipment Collection

Users can choose to add managed devices to favorites to quickly access the favorite devices. The process of device collection is similar. This section takes the server as an example to introduce the process of device collection.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2.** In the server list, select the server to be favorited, and click [More] -> [Collect] to favorite the selected server.

**Step 3** After the device is successfully saved, click the  icon in the navigation bar at the top of ISPIM to quickly view the favorite server.

----End

## 3. Equipment Allocation

Users in ISPIM have different permissions, and each user manages their own devices (servers, storage, network devices, etc.). Only the super administrator can view all devices, and other users can only see their own devices in ISPIM. According to needs, the super administrator can assign servers to other users.

The operation of allocating equipment is similar. This section takes the super administrator as an example to introduce the process of allocating machine servers.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** In the server list, select the server to be assigned, click <More> -> <Distribute User>, and in the pop-up user list, after selecting the user to be assigned, click <Submit> to assign the selected server to corresponding user.

**Step 3** Use the assigned user to log in to ISPIM and check whether there is an assigned

device in the device list.

----End



#### NOTE

- Users with super administrator rights will not appear in the list of users to be assigned.
  - Super administrators can assign devices to other non-super administrators.
  - The operation and maintenance administrator can assign the device to other ordinary users.
- 

## 4. Reset Rule

Users can reset the alarm rules and alarm notification rules of the server.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** In the server list, after selecting the server, click <More/Reset Rule>, and in the reset rules window that pops up, reselect the notification rules and alarm rules, and click <Submit>.

----End



#### NOTE

- Alarm rules: ISPIM uses the default alarm rules. At the same time, users can customize the monitoring template to specify monitoring items and alarm conditions.
  - Notification rules: When an alarm message is generated, the notification rules specify the scope of the notification user and the notification form.
  - Assign contact: Assign the person who receives the alarm information. Please note: Although the notification rule contains contact information, in order to improve the reusability of the notification rule, the notification rule can only include the necessary public Contact (such as the admin user), and then assign other contacts individually through this operation.
-

## 5. Enable/Disable Rules

According to needs, users can enable/disable the server's alarm rule or notification rule.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** In the server list, after selecting the server whose rule status is to be reset, click <More /Reset Rule Status>, and the reset rule status window will pop up.

**Step 3** Check the rules that need to be set, and select enable/disable, and then click <Submit>.

---End

## 6. Reset Protocol

When the IPMI/SNMP protocol of the server is changed, the authentication information saved in ISPIM can be updated through the "Reset Protocol" operation. The reset protocol supports batch operations. This section takes the server as an example to introduce the reset protocol operation.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** In the server list, after selecting the server whose protocol is to be reset, click <More/Reset Protocol>, and the protocol reset window will pop up.

**Step 3** After setting the protocol parameters, click <Submit>.

----End



#### NOTE

- The common scenario for resetting the protocol is: the user does not use the ISPIM platform, directly changes the BMC user name/password or SNMP authentication information, but ISPIM does not synchronize the related information, which causes the server to lose connection; or the information cannot be obtained normally, user can synchronize by resetting the protocol.

- ISPIM supports direct batch modification of BMC usernames and passwords, see 8.3.2 BMC for details. When BMC usernames and passwords are directly modified on the ISPIM platform, there is no need to perform the protocol reset operation again.
- 

## 7. Edit Warranty Info

By editing asset maintenance information, users can be notified in time that the asset maintenance is about to expire or has expired.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** In the server list, select the server to be edited and click <More/Edit Warranty Information>, and the related window will pop up.

**Step 3** Edit the purchase time, expiring time, expired time in the window, and click the <Submit> button.

----End

## 8. Import Warranty Information

User can import asset maintenance information in batches to facilitate the management of asset maintenance information.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** Click <More/Import Warranty Information>, and the import maintenance information window will pop up.

**Step 3** Click <Download Template>, edit the downloaded template, and fill in the asset maintenance related information.

**Step 4** After editing the template, click <Select File> to upload the template file edited in the above steps, and click the <Submit> button to import maintenance information in batches.


---End

## 9. Refresh Server

Server hardware information usually does not change frequently. ISPIM will synchronize hardware information regularly every day by default. When server component assets change (such as hard disk addition/replacement), user can manually refresh the server to synchronize hardware information.

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** In the server list, click the  icon corresponding to a server, ISPIM will re-collect the hardware information of the server; When needing to refresh servers in batches, user can select multiple servers in the server list and click <Refresh > button at the top of the server list.

---End

## 10. Export Asset Report

ISPIM can export asset reports to facilitate user management of asset information

### Procedure

**Step 1** Click [Assets] -> [Server] to enter the server page.

**Step 2** In the server list, select the server to be exported as required, and click the <Export> button above the list to export the selected server information to the local.

**Step 3** After the download is complete, user can view the exported excel file and view server-related information.

--End

## 6.11 Data Center Management

ISPIM data center management functions includes three parts: data center, power consumption

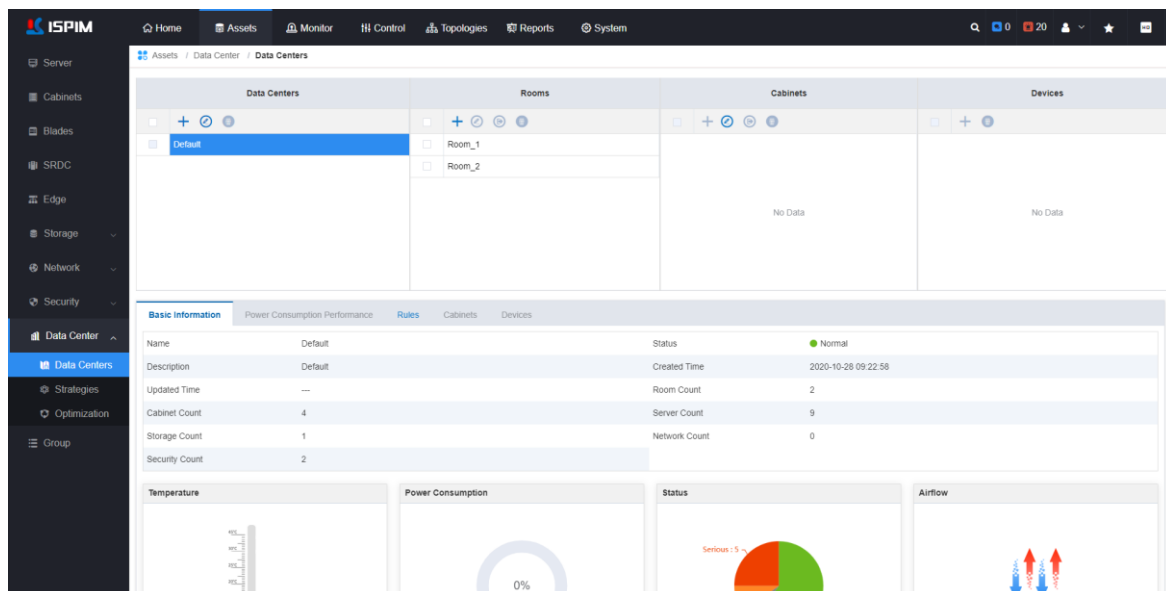
strategy and power optimization. ISPIM supports operations such as creating and modifying data centers, setting power consumption strategies, viewing function performance, and viewing energy optimization suggestions.

## 6.11.1 Create Data Center

ISPIM provides data center logic and 3D views. Users can easily build data center models to achieve efficient operation and maintenance of data centers. Click [Assets] -> [Data Center] to enter the data center page, as shown in Figure 6-55. In the data center page, user can perform operations such as creating data centers, adding rooms, adding cabinets, and adding equipment, and user can view basic data center information, functional performance, notification rules, and alarm rules. The relationship between each facility in the data center is described as follows:

- Room: A data center can contain multiple rooms.
- Cabinet: The room can contain multiple cabinets.
- Device: The cabinet can contain multiple devices.


Figure 6-55 Data Center



### 1. Add Data Center

## Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.

**Step 2** Click the  icon under the data center column, enter the name and description of the data center in the pop-up window, and click <Submit> to create a data center.


----End

## 2. Add Room to the Data Center

### Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.

**Step 2** In the data center field, click to select the data center that needs to add rooms.

**Step 3** Click the  icon under the room column, and select manual import/batch import to add the rooms.

- **Manual Import:** Select manual import, input the name, number, length and width of the room and other parameters in the pop-up window, and click <Submit>.
- **Batch Import:** Select batch import, in the pop-up window, click the <Template Download> button to download and edit the information in the template, then click <Select File>, upload the edited template and click the <Submit> button to batch import rooms.

----End



Please fill in the length and width of the room according to the actual situation, in order to facilitate the construction of real topology mapping.

---


## 3. Add Cabinet to Room

### Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.

**Step 2** In the data center field, click and select a data center.

**Step 3** In the room field, click and select a room.

**Step 4** Click the  icon in the cabinet column, select manual import, batch import or existing cabinet method to add cabinets to the room.

- **Manual Import:** Select manual import, input the name, number, height and other parameters of cabinet in the pop-up window, and click <Submit>.
- **Batch Import:** Select batch import, after downloading and editing the room template in the pop-up window, click <Select File> to upload the edited template and click the <Submit> button to import cabinet information in batches.
- **Existing cabinet:** Select an existing cabinet. In the pop-up window, select an existing cabinet and click <Submit>.

---End



#### NOTE

- To facilitate the use of the 3D room function, please fill in the actual value for the height of the cabinet.
- To facilitate the use of the power management function, please fill in the actual value for the rated power consumption of the cabinet.

## 4. Add Device to Cabinet


### Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.

**Step 2** In the data center field, click and select a data center.

**Step 3** In the room field, click and select a room.

**Step 4** In the cabinet column, click and select a cabinet.

**Step 5** In the device field, click the  icon, and the add device window will pop up. After checking the devices to be added in the device list on the right side of the window, the devices will be automatically added to the "Unallocated Resources" area.

**Step 6** Click the device in the "Unallocated Resources" area, and the device will be automatically added to the "Cabinet" area on the left. In the "Cabinet" area, user can drag the device to the specified location with the left mouse button.



**Step 7** After setting the location of all devices, click the <Submit> button.

---End



#### NOTE



- When dragging the device position in the "cabinet" area, keep the left mouse button pressed.
  - In the "cabinet" area, user can use <ctrl+arrow keys> to move the cabinet up and down.
  - In the "cabinet" area, user can use <ctrl+mouse wheel> to zoom the cabinet.
- 

## 6.11.2 Data Center Management

After the data center is created, user can modify the data center configuration or delete the data center related facilities as needed.

### 1. Edit/Delete Data Center

User can delete or edit data center information.

- **Edit Data Center:** In the data center column, click and select a data center, click the  icon, and in the pop-up edit data center window, user can modify the name and description of the data center.
  - **Delete Data Center:** In the data center field, click and select one or more data centers, click the  icon and confirm in the pop-up window to delete the selected data center.
- 






#### NOTE

- When deleting a data center, the room and cabinets under the data center will be deleted.
  - The default data center cannot be deleted.
- 

### 2. Edit/Delete/Move Room

User can edit, delete or move the room.




- **Edit Room:** In the room field, click and select a room, click the  icon, in the pop-up window, user can modify the room name, number, length and width and other parameters.
- **Delete Room:** In the room field, click and select one or more rooms, click the  icon and confirm in the pop-up window to delete the selected rooms.
- **Move Room:** In the room field, click and select one or more rooms, click  the icon, and select the destination data center in the drop-down box of the window that pops up, and click <Submit> to move the selected room to the corresponding data center.

**NOTE**

When the size of the room is modified, all the original cabinet layout information in the 3D room will be cleared and need to be re-edited. For details about the 3D room function, please refer to 9.2 3D.

### 3. Edit/Delete/Move Cabinet


User can edit, delete or move cabinet.

- **Edit Cabinet:** In the cabinet column, click and select a cabinet, click the  icon, and in the pop-up window, user can modify the cabinet name, number, height and other parameters.
- **Delete Cabinet:** In the cabinet column, click and select one or more cabinets, click the  icon and confirm in the pop-up window to delete the selected cabinets.
- **Move Cabinet:** In the cabinet column, click and select one or more cabinets, click the  icon, and select the destination room in the drop-down box of the window that pops up, and click <Submit> to move the selected cabinet to the corresponding room.

**NOTE**

When editing a cabinet, if there are already equipment in the cabinet and the new height of the cabinet cannot accommodate the existing equipment, the editing will fail.

### 4. Delete Device

User can delete the equipment in the cabinet. In the cabinet column, click and select one or more equipment, click the  icon, and confirm in the pop-up window to delete the selected equipment.

## 6.11.3 View Data Center

On the data center page, user can view data center related information, such as energy consumption statistics of different dimensions, such as data center, room, cabinet and equipment.

### 1. View Data Center Detail

#### Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.

**Step 2** In the data center column, click and select a data center. The bottom of the page will display the detailed information of the data center, including basic information, power consumption performance, rules, cabinets, devices. Select the "Basic Information" tab, user can view the basic information of the data center:

- Temperature: Display the highest temperature of all equipment in the data center.
- Power Consumption: Show the sum of power consumption of all equipment in the data center.
- Status: Display the distribution of the number of alarms for each device in the data center.
- Airflow: Display the average airflow information of all equipment in the data center.

**Step 3** Select the "Power Consumption Performance" tab to view the data center's air inlet temperature, air outlet temperature, power consumption and other curves.

- User can select different time buttons in the upper right corner to switch the statistical time of the graph.
- Select the "Max/Average/Min" tab on the upper right corner of the graph to hide/show the curve.

**Step 4** Select the "Rules" tab to set the alarm notification rules and monitoring rules of the data center.

**Step 5** Select the "Cabinet" tab, user can view the cabinet information under the data center, including name, location, available capacity, power consumption, temperature,

airflow.

**Step 6** Select the "Devices" tab to view the device information in the data center, including name, IP, model, derated power, power control ability, power consumption, temperature, and airflow.

--End

## 2. View Room Info and Layout

### Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.

**Step 2** In the room column, click and select a room, and the detailed information of the room will be displayed at the bottom of the page, including basic information, power consumption performance, rules, cabinets, devices and power strategy. Select "Basic information" tab, user can view the basic information, temperature, power consumption and other information of the room.

- Temperature: Display the highest temperature of all equipment in the room.
- Power Consumption: Show the sum of power consumption of all equipment in the room.
- Status: Display the distribution of the number of alarms for each device in the room.
- Airflow: Display the average airflow information of all equipment in the room.

[NOTE] Click the <Layout> button to enter the 3D room page. For details about the 3D room, please refer to 9.23D.

**Step 3** Select the "Power Consumption Performance" tab to view the data center's air inlet temperature, air outlet temperature, power consumption and other curves.:

- User can select different time buttons in the upper right corner to switch the statistical time of the graph.
- Select the "Max/Average/Min" tab on the upper right corner of the graph to hide/show the curve.

**Step 4** Select the "Rules" tab to set the alarm notification rules and monitoring rules of the data center.

**Step 5** Select the "Cabinet" tab, user can view the cabinet information under the data center, including name, location, available capacity, power consumption, temperature, airflow.

**Step 6** Select the "Devices" tab to view the device information in the data center, including name, IP, model, derated power, power control ability, power consumption, temperature, and airflow.

**Step 7** Select the "Power Strategy" tab, user can view the power policy of the room, and perform operations such as adding, deleting, enabling or disabling the power policy.

--End

### 3. View Cabinet Info and Layout

#### Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.


**Step 2** In the cabinet column, click and select a cabinet, the bottom of the page will display the detailed information of the cabinet, including basic information, layout, power consumption performance, rules, equipment and power consumption strategy. Select "Basic Information" tab, user can view the basic information, temperature, power consumption and other information of the cabinet.

- Temperature: Display the highest temperature of all equipment in the cabinet.
- Power Consumption: Show the sum of power consumption of all equipment in the cabinet.
- Status: Display the distribution of the number of alarms for each device in the cabinet.
- Airflow: Display the average airflow information of all equipment in the cabinet.

**Step 3** Select the "Layout" tab, user can view the basic layout, temperature, airflow layout of the cabinet.

- **View Device Detail:** Click the device icon in the cabinet to view the device details

- **View Temperature Airflow Layout:** Click the <Temperature Airflow Layout> button above the cabinet to view the temperature airflow layout of the device.

- **Edit Cabinet Layout:** Click the  icon to edit the device layout in the cabinet. User can drag the device position up and down in the cabinet area.

**Step 4** Select the "Power Consumption Performance" tab, user can view the cabinet's air inlet temperature, air outlet temperature, power consumption and other curves.

- User can select different time buttons in the upper right corner to switch the statistical time of the graph.
- Select the "Max/Average/Min" tab on the upper right corner of the graph to hide/show the curve.

**Step 5** Select the "Cabinet" tab, user can view the cabinet information under the data center, including name, location, available capacity, power consumption, temperature, airflow.

**Step 6** Select the "Devices" tab to view the device information in the data center, including name, IP, model, derated power, power control ability, power consumption, temperature, and airflow.

**Step 7** Select the "Power Strategy" tab, user can view the power policy of the room, and perform operations such as adding, deleting, enabling or disabling the power policy.

--End

## 4. View Device Info

### Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.

**Step 2** In the device field, click and select a device, the bottom of the page will display the detailed information of the device, including basic information, power consumption performance, rules and power strategy. Select the "Basic Information" tab, user can view basic information, temperature, power consumption and other information of the device.

- **Temperature:** Display the current temperature of the device.

- Power consumption: Shows the power consumption of the current device.
- Airflow: Display the airflow information of the current device.
- Calculation Usage: Display the current device's CPU utilization, memory utilization, and I/O utilization.

**Step 3** Select the "Power Consumption Performance" tab, user can view the device's air inlet temperature, air outlet temperature, power consumption and other curves.

- User can select different time buttons in the upper right corner to switch the statistical time of the graph.
- Select the "Max/Average/Min" tab on the upper right corner of the graph to hide/show the curve.

**Step 5** Select the "Cabinet" tab, user can view the cabinet information under the data center, including name, location, available capacity, power consumption, temperature, airflow.

**Step 6** Select the "Devices" tab to view the device information in the data center, including name, IP, model, derated power, power control ability, power consumption, temperature, and airflow.

**Step 7** Select the "Power Strategy" tab, user can view the power policy of the room, and perform operations such as adding, deleting, enabling or disabling the power policy.

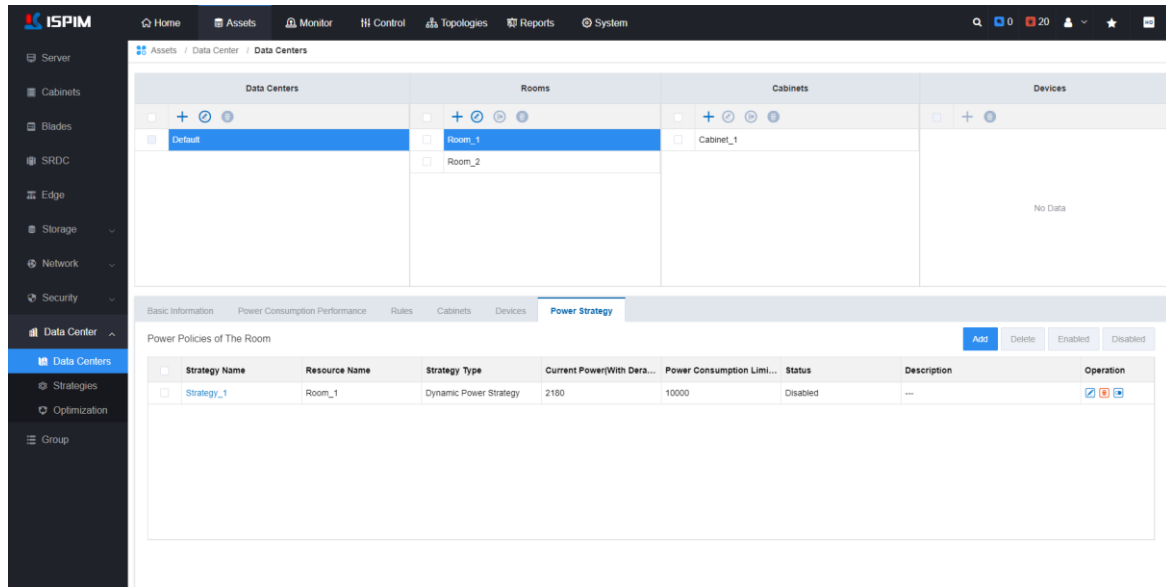
---End

## 6.11.4 Power Consumption Management

In the top navigation bar of ISPIM, select the "Assets" tab to enter the asset management page. In the left navigation tree of asset management, select [Data Center/Strategy] to enter the power consumption strategy page, as shown in Figure 6-56. User can edit, delete, disable, and enable the power strategy.

ISPIM supports setting power consumption strategies for Inspur M4 and M5 series servers to realize automated power management. When the power consumption of the device is higher than the set value, ISPIM will automatically reduce the power consumption of the device through commands.

Figure 6-56 Power Consumption Strategy Page



## 1. Add Power Consumption Strategy

According to needs, users can customize the power consumption strategy of the rooms cabinets and equipment to limit the maximum power consumption of the servers and realize automatic power management.

### Procedure

**Step 1** Click [Assets] -> [Data Center] to enter the data center page.

**Step 2** According to needs, user choose to set the power consumption strategy of the room, cabinet or equipment. After selecting the room, cabinet or equipment, select the "Power Strategy" tab at the bottom of the page.

**Step 3** Click the <Add> button, and the window for adding a power consumption strategy will pop up. After configuring the name, type, power consumption limit and other parameters as needed, click <Submit>.

- Dynamic power strategy: Set the expected power consumption strategy of the device. When the power consumption of the device is higher than this value, ISPM will automatically reduce the power consumption of the device.
- Lowest power strategy: ISPM uses commands to set the device to run at the lowest power consumption. Please note: Using the lowest power consumption strategy may limit the performance of the device, and **it is recommended to use it with caution.**



- Time: The effective time of the strategy. "Always Effective" means that the power consumption strategy is always effective; "Loop" can be used to set the effective date and time period of the power consumption strategy.

**Step 4** The created power consumption strategy will be displayed in the list, click the strategy name to view the detailed information of the power consumption strategy.

---End



## 2. Power Consumption Strategy Management


After the power strategy is added, user can view, edit, enable or disable the strategy on the power strategy page.

### Procedure

**Step 1** Click [Assets] -> [Data Center] -> [Strategy] to enter the power consumption strategy page.

**Step 2** Click the name in the power consumption strategy list to view the detailed information.

**Step 3** Click the  icon corresponding to a power consumption strategy to edit the power consumption strategy. Click the  icon to delete the power consumption strategy.

Click the  icon to disable/enable the power consumption policy.

**Step 4** After selecting multiple power consumption strategies in the list, click the <Delete>, <Enable> and <Disable> buttons above the list to delete/enable/disable in batches.

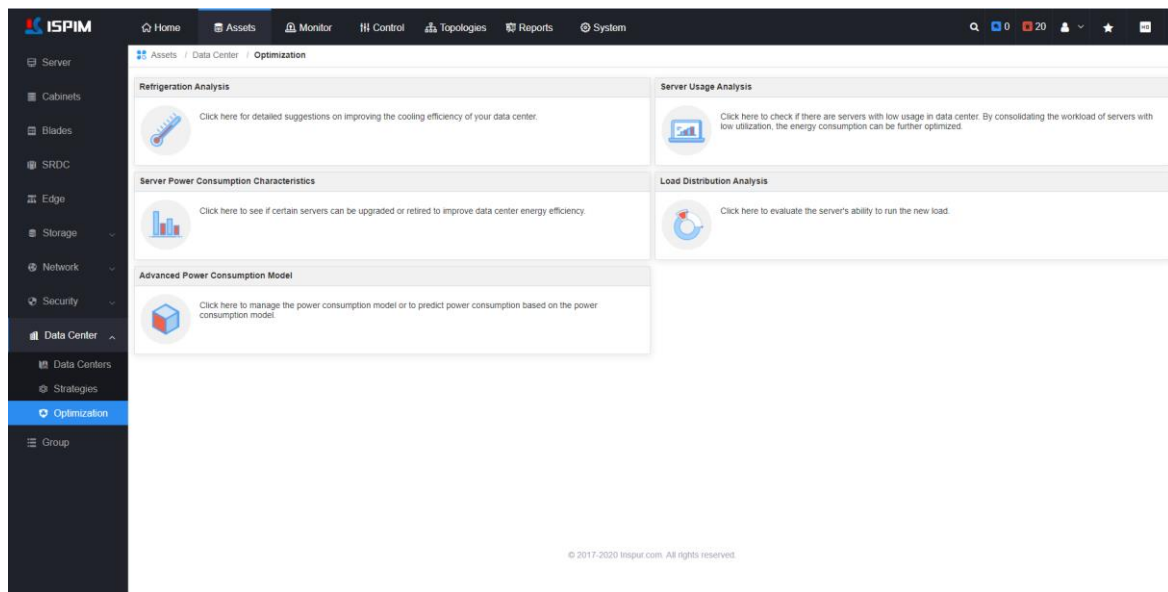
---End

### 6.11.5 Power Consumption Optimization

In the top navigation bar of ISPIM, select the "Assets" tab to enter the asset management page. In the left navigation tree of asset management, select [Data Center/Optimization] to enter the energy optimization page, as shown in Figure 6-57.

Based on the collected energy consumption data, ISPIM can display the power consumption, temperature and CUPS data of various dimensions from the data center to the equipment, and carry out data integration on this basis, providing room cooling, load distribution, energy consumption control, etc. Optimization suggestions. At the same time, it can provide detailed power consumption management to a single device to assist operation and maintenance personnel to manage the energy consumption of the room.

Figure 6-57 Power Consumption Optimization



## 1. Refrigeration Analysis

ISPIM takes the standard refrigeration specification as a reference, performs intelligent analysis based on the temperature distribution curve of the room, and gives the evaluation results and repair suggestions for the cooling of the room. Refrigeration analysis is to analyze the temperature of the equipment in the room, display the temperature distribution in the room, and list the high-temperature hotspots inside the room and give reasonable refrigeration suggestions. According to actual needs, users can choose three refrigeration specifications referenced by ISPIM, as shown in Table 6-12.

Table 6-12 Refrigeration Specification

Specification	Description
ASHREA Recommended	18°C- 27°C
ASHREA Class 1 Allowable	15°C- 32°C

ASHREA Class 2 Allowable	10°C- 35°C
--------------------------	------------

## Procedure

**Step 1** Click [Assets] -> [Data Center] -> [Optimization] -> [Refrigeration Analysis] to enter the cooling analysis page.

**Step 2** In the room list on the left, select a room, and select the cooling specification in the cooling specification drop-down list in the upper right corner. The cooling analysis page will automatically refresh the temperature distribution curve of the equipment in the room. At the same time, the evaluation, level, risk equipment, advice and operation plan will be displayed at the bottom of the page.

---End



### NOTE

Click the <Refresh> button above the temperature distribution graph to refresh the refrigeration analysis in real time.

---

## 2. Server Usage Analysis

Server utilization analysis uses power consumption data or CUPS to evaluate server utilization, finds "zombie devices" with low utilization, and displays average utilization estimates and 99% time utilization to predict power consumption trends. User can view the server usage analysis results and suggestions.

## Procedure

**Step 1** Click [Assets] -> [Data Center] -> [Optimization] -> [Server Usage Analysis] to enter the server utilization page.

**Step 2** Click the <Analysis> button in the upper right corner of the page, ISPIM will automatically collect and analyze the usage of the device, and list the devices with lower usage.

**Step 3** After the analysis is complete, user can view the average server usage, 99% time usage, and estimated energy savings in the list.

**Step 4** At the bottom of the page, ISPIM will list the daily usage mode of the device based on the historical data of the device, so that the user can view the usage distribution of the device at each time period in a day.

---End



#### NOTE

ISPIM needs to collect enough equipment history data to be able to analyze. To ensure the accuracy of the analysis, it is recommended that users add resources to ISPIM for at least 2 days before performing analysis operations.

---

### 3. Server Power Consumption Characteristics

ISPIM calculates the upper and lower limits of power consumption of different types of servers to form a distribution map of server power consumption characteristics, which is convenient for users to compare the energy consumption of different types of servers to optimize the equipment structure of the data center. In this way, users can view the power consumption range of each type of server, and the high power consumption server models can be found in time.

Applicable scenarios: For example, the user's same services are running on different models of servers, and the most suitable service carrier can be selected by comparing energy consumption.

#### Procedure

**Step 1** Click [Asset] -> [Data Center] -> [Optimization] -> [Server Power Consumption Characteristics] to enter the server power consumption characteristics page.

**Step 2** In the server power consumption characteristic distribution graph, click the bar graph of a server, and a distribution window will pop up. In this window, user can view the upper/lower power consumption histogram of the server, which is convenient for viewing the power consumption distribution of this model of server.

---End

## 4. Load Distribution and Migration

ISPIM can intelligently analyze server load and can help users allocate or migrate services.

- Load Distribution: According to the calculation utilization (CPU, IO and memory bandwidth utilization) required by the user, evaluate the server's carrying capacity and list the server's carrying capacity score.
  - a. Click [Assets] -> [Data Center] -> [Optimization] -> [Load Distribution Analysis] to enter the load distribution analysis page.
  - b. Select the "Load Distribution" tab, enter the expected CPU utilization, IO calculation utilization, and memory calculation utilization of the service, click the <Seek> button, and the list of devices that meet the search criteria will be arranged according to the score on the right. It is recommended that users choose devices with higher scores to carry new business loads.
- Load Migration: According to the device selected by the user to be moved out of the load, the carrying capacity of other servers is evaluated, and the server carrying capacity score is listed.
  - a. Click [Asset] -> [Data Center] -> [Optimization] -> [Load Distribution Analysis] to enter the load distribution analysis page.
  - b. Select the "Load Migration" tab, click the <Select> button, select the server where the business to be migrated is located in the pop-up server list, and click <Submit>. The list on the right will display the list of devices that meet the business migration conditions in order of score. It is recommended that users select devices with higher scores for load migration.

## 5. Advanced Power Consumption Model

ISPIM supports the creation of device power management models and power consumption predictions: According to the device CUPS and power consumption, the device power consumption can be analyzed through AI algorithms, and advanced power consumption models can be established.


The model supports the prediction of device power consumption from the three dimensions of CPU, IO and memory bandwidth utilization.

- Model Management

ISPIM can establish a power consumption model based on the relationship between the device's historical CUPS data (CPU utilization, memory bandwidth utilization, I/O bandwidth utilization) and historical power consumption.

- a. Click [Asset] -> [Data Center] -> [Optimization] -> [Advanced Power Consumption Model] to enter the advanced power consumption model page.
- b. Select the "Model" tab, click the <Add> button, in the pop-up Add Model window, configure the model name and select the device to be built, and then click <Submit>.
- c. After the addition is successful, user can view the created power consumption model in the management model list.

**NOTE**

- If the CUPS data or historical power consumption data of the device are incomplete, the model will not be created. Please wait for a while and try again, or choose another similar device to create the model.
- The device list supports query operations, and the query conditions include: data center, room, cabinet, and device name.
- Click the  icon corresponding to a power consumption model and confirm in the pop-up window to delete the model.

---

- Power Consumption Prediction

The operation of power consumption prediction is as follows:

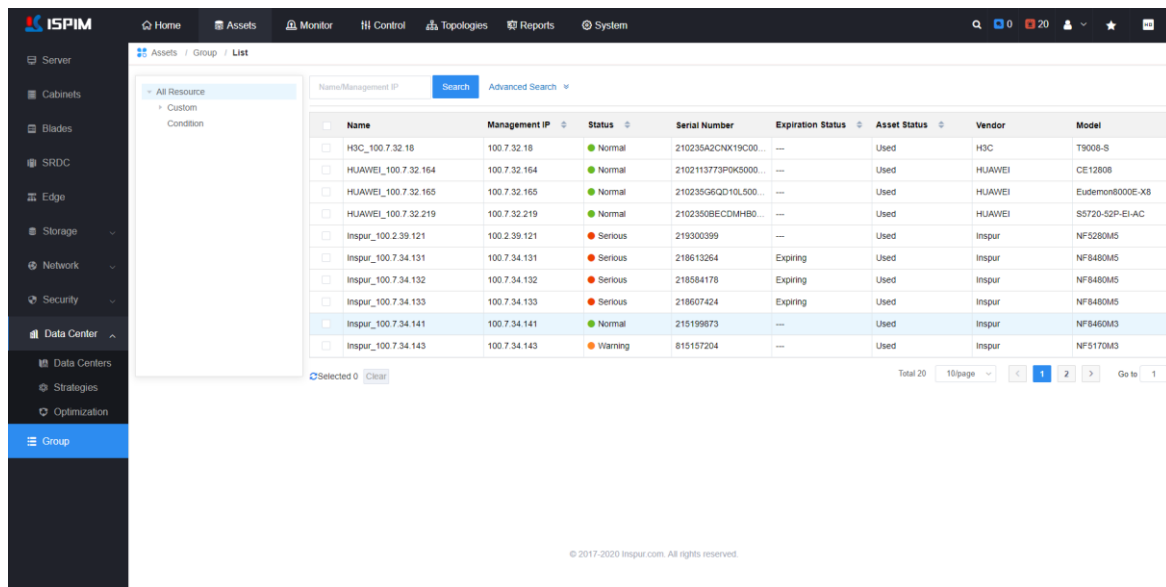
- a. Click [Asset] -> [Data Center] -> [Optimization] -> [Advanced Function Model] to enter the advanced power consumption model page.
- b. Select the "Predicted Power Consumption" tab, click in the list on the left and select the created power consumption model, enter the estimated CPU calculation utilization rate and memory calculation utilization rate, and click the <Predict> button to predict power consumption according to the model.

## 6.12 Device Grouping

In the navigation bar at the top of ISPIM, select the "Assets" tab to enter the asset management page. Select [Group] in the left navigation tree of asset management to enter the group list page, as shown in Figure 6-58. The device grouping function is convenient for operation and maintenance personnel to group devices according to actual business scenarios. The ISPIM platform includes two types of groups: custom groups and condition groups.

- Custom Group: Support users to create custom groups, and manually add devices to the group.
- Conditional Group: Support users to create conditional groupings. By filtering conditions, ISPIM will automatically add qualified devices to the grouping.

Figure 6-58 Device Grouping Page




### 6.12.1 Custom Group

On the device grouping page, user can create, edit and delete custom groups.

#### Procedure

**Step 1** Click [Asset] -> [Group] -> to enter the device group page.



**Step 2** Hover the mouse on the custom group, the  icon will appear. Click the icon to enter the custom group page.

**Step 3** Enter the group name, click the <Add> button, and select the corresponding device in the device list, click the <Submit> button to add the devices to the created group.

--End



#### NOTE

- Click the  icon to the right of a custom group name to edit the group name and the devices in the group.
- Click the  icon to the right of a custom group name to delete the custom group.


---

## 6.12.2 Conditional Group

On the device grouping page, user can create, edit and delete conditional groups.

### Procedure

**Step 1** Click [Asset] -> [Group] -> to enter the device group page.



**Step 2** Hover the mouse on the conditional group, the  icon will appear. Click the icon to enter the conditional group page.

**Step 3** Enter the group name, click the <Select> button, in the pop-up window, edit the filter conditions such as IP, vendor, model, etc., and click the <Submit> button to add the eligible devices to the condition group.

--End



#### NOTE

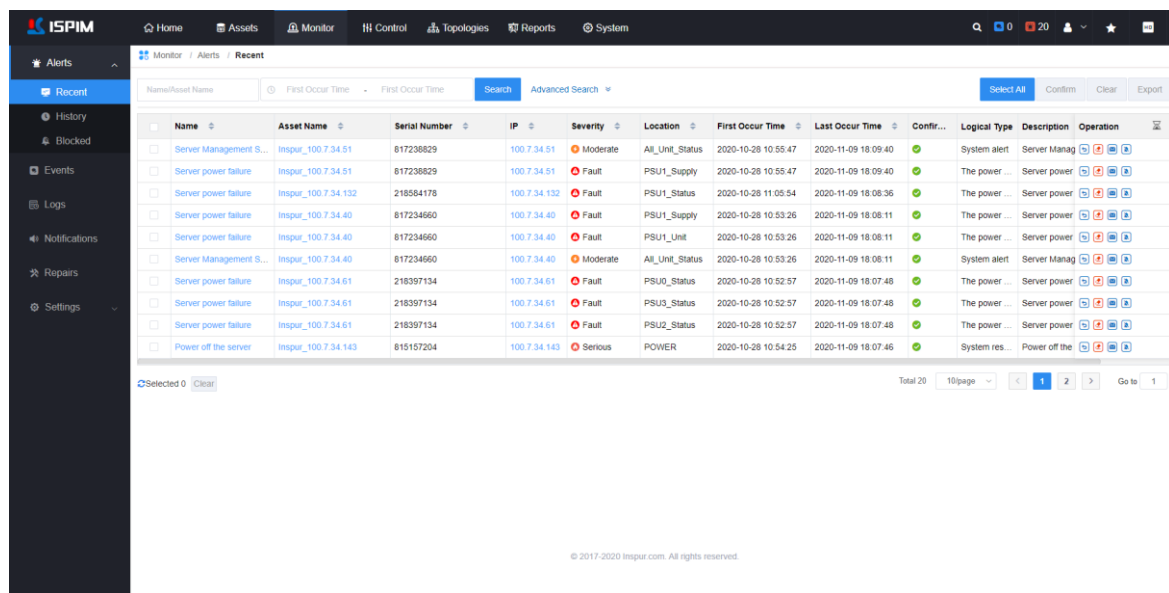
- If multiple filter conditions are added, the union of each filter condition is taken.
- Click the  icon to the right of a custom group name to edit the group name and the devices in the group.
- Click the  icon to the right of a custom group name to delete the condition group.



# 7 Monitoring

In the navigation bar at the top of ISPIM, select the "Monitor" tab to enter the monitoring management module, as shown in Figure 7-1. The monitoring management module mainly includes alarm management, event management, log management, notification records, repair work orders, and alarm settings functions.

Figure 7-1 Monitoring Management



NOTE

Users can use the system default alarm, notification or blocking rules, or customize these rules.

## 7.1 Logical Classification of Monitoring Items

The ISPIM platform divides monitoring items into seven categories, and their descriptions are shown in table Table 7-1.

Table 7-1 Logical Classification of Monitoring Items

Category	Sub Category
Business Process	Disaster tolerance problem, bureau data problem, routing failure, VFN alarm, synchronization clock failure, communication alarm, process alarm
Dynamic	Power alarm, fan alarm, humidity alarm, temperature alarm and airflow alarm

Category	Sub Category
Environment	
Performance	Storage performance alarm, CPU performance alarm, memory occupancy alarm, hard disk occupancy alarm, device performance alarm, GPU performance alarm, network port performance alarm
Security	Security log alarm, security event alarm, login event
System	System alarm, system switching alarm, system log alarm, system hint alarm, system abnormal alarm and system restart alarm
Hardware	Main control board alarm, clock board alarm, function expansion module alarm, CPU hardware alarm, hard disk hardware alarm, memory hardware alarm, controller hardware alarm, GPU hardware alarm, device hardware alarm
Connectivity	Service link fully blocked, link status abnormal, connectivity alarm



## NOTE

In the alarm list, click an alarm name to view the details of the logical classification corresponding to the alarm.

## 7.2 Alarm Management

ISPIM provides a variety of standard management protocols and uses a combination of active and passive alarm methods to realize real-time monitoring and fault analysis of equipment. For all kinds of information collected, ISPIM can perform internal intelligent alarm analysis and notify users of alarm information in time. The alarm related data collection methods are shown in Table 7-2.

Table 7-2 Alarm Related Data Collection Methods

Monitoring Method	Description
IPMI active collection	Polling the server's sensor information regularly through the IPMI protocol
SNMP active collection	Collect server information regularly through the SNMP protocol, such

Monitoring Method	Description
	as monitoring Huawei servers
SNMP trap reception	Passively receive and analyze server SNMP trap information
Log collection and analysis	For the Inspur server, it can actively collect the server's out-of-band logs and analyze them

**NOTE**

The setting instructions for SNMP trap reception are as follows:

- Inspur server: When adding a server, ISPIM can automatically set the server's BMC trap address to ISPIM IP.
- Servers, storage, network, security devices of other manufacturers: User needs to manually set the device's BMC trap address to the ISPIM IP before the ISPIM platform can receive the device's trap alarm.

## 7.2.1 Current Alarm

Current alarms are currently occurring alarms, which mainly include alarms of the equipment managed by the ISPIM and the alarms of the ISPIM system itself (such as ISPIM sub-service abnormal). Click [Monitor] -> [Alerts] -> [Recent], user can enter the current alarm page, as shown in Figure 7-2. On the current alarm page, user can view the real-time alarm list, perform confirmation, block, and clear operations.

Figure 7-2 Current Alarm Page

Name	Asset Name	Serial Number	IP	Severity	Location	First Occur Time	Last Occur Time	Confir...	Logical Type	Description	Operation
Server Management S...	Inspur_100 7.34.51	817238829	100 7.34.51	Moderate	All_Unit_Status	2020-10-28 10:55:47	2020-11-09 18:09:40		System alert	Server Manag	[Icons]
Server power failure	Inspur_100 7.34.51	817238829	100 7.34.51	Fault	PSU1_Supply	2020-10-28 10:55:47	2020-11-09 18:09:40		The power ...	Server power	[Icons]
Server power failure	Inspur_100 7.34.132	218584178	100 7.34.132	Fault	PSU1_Status	2020-10-28 11:05:54	2020-11-09 18:08:36		The power ...	Server power	[Icons]
Server power failure	Inspur_100 7.34.40	817234660	100 7.34.40	Fault	PSU1_Supply	2020-10-28 10:53:26	2020-11-09 18:08:11		The power ...	Server power	[Icons]
Server power failure	Inspur_100 7.34.40	817234660	100 7.34.40	Fault	PSU1_Unit	2020-10-28 10:53:26	2020-11-09 18:08:11		The power ...	Server power	[Icons]
Server Management S...	Inspur_100 7.34.40	817234660	100 7.34.40	Moderate	All_Unit_Status	2020-10-28 10:53:26	2020-11-09 18:08:11		System alert	Server Manag	[Icons]
Server power failure	Inspur_100 7.34.61	218397134	100 7.34.61	Fault	PSU0_Status	2020-10-28 10:52:57	2020-11-09 18:07:48		The power ...	Server power	[Icons]
Server power failure	Inspur_100 7.34.61	218397134	100 7.34.61	Fault	PSU2_Status	2020-10-28 10:52:57	2020-11-09 18:07:48		The power ...	Server power	[Icons]
Server power failure	Inspur_100 7.34.61	218397134	100 7.34.61	Fault	PSU2_Status	2020-10-28 10:52:57	2020-11-09 18:07:48		The power ...	Server power	[Icons]
Power off the server	Inspur_100 7.34.143	815157204	100 7.34.143	Serious	POWER	2020-10-28 10:54:25	2020-11-09 18:07:46		System res.	Power off the	[Icons]

### Current Alarm Operations

In the real-time alarm list, user can view the alarm details, alarm source details, device IP, etc.

- **View alarm details:** In the alarm list, click an alarm name to view the details of the alarm. ISPM can perform intelligent analysis on the alarm, and provide reference information such as "possible cause" and "repair suggestions" in the alarm information window.
- **View the details of the alarm source:** In the alarm list, click the name of the alarm source in the alarm list to enter the server details page corresponding to the alarm source.
- **Access device IP:** In the alarm list, click the "IP" corresponding to an alarm, it will link to the login page of the device manager, and for the Inspur server, it will jump to the login page of BMC.
- **Location:** In the alarm list, the "Location" column is used to display the location of the device's alarm source.

### NOTE

The sources of real-time alarms in the ISPM platform include the following three:

- Generate alarms based on alarm rules: Users can set the alarm duration in the ISPM alarm rules. When ISPM is in the process of active data collection and finds that the value of the monitored item exceeds the threshold within the duration, a real-time alarm will be generated.
- Passively receive trap alarms: ISPM receives trap alarms sent by the device and generates real-time alarms through internal intelligent analysis.


- Active monitoring method: ISPIM actively collects hardware logs of each device and generates real-time alarms through intelligent fault analysis.
- 

## 6. Confirm Current Alarm

User can confirm the alarm operation in the real-time alarm list. After the confirmation operation is performed, ISPIM will tag the confirmed alarm with a "confirmed" label, which is convenient for users to classify and filter the alarm information. After the alarm is confirmed, it is recommended that the user handle it in time. When the device returns to normal, under normal circumstances, the real-time alarm will be automatically restored and moved to the historical alarm. User can also delete the alarm manually without waiting for the alarm to recover.

### Procedure

**Step 1** Click [Monitor] -> [Alarm] -> [Recent] to enter the real-time alarm page. If user needs to confirm one by one, please execute Step 2; if user needs to confirm in batches, please execute Step 3.


**Step 2:** In the real-time alarm list, click the  icon corresponding to an alarm and confirm in the pop-up window to perform the confirmation operation.

**Step 3:** In the real-time alarm list, select multiple real-time alarms to be confirmed, click the <Confirm> button above the list, and confirm in the pop-up window to perform batch confirmation operations.

--End



#### NOTE

To deconfirm the confirmed alarms, user can click the  icon corresponding to an alarm in the real-time alarm list.

---


## 7. Clear Current Alarm

In the real-time alarm list, user can clear the alarm, and the cleared alarm will be displayed in the historical alarm list. Clearing the real-time alarm does not mean masking the alarm. If the device is still

in a fault state, the current alarm will continue to be generated.

## Procedure

**Step 1** Click [Monitor] -> [Alarm] -> [Recent] to enter the real-time alarm page. If user needs to clear one by one, please execute Step 2; if user needs to clear in batches, please execute Step 3.

**Step 2** In the real-time alarm list, click the  icon corresponding to a real-time alarm to clear the alarm.

**Step 3** In the real-time alarm list, select multiple real-time alarms to be cleared, click the <Clear> button above the list to clear the confirmation operations in batches.


----End

## 8. Mask Alarm

When the user believes that a certain alarm is a false alarm or does not need this alarm, the mask operation can be performed. The masked alarm will be displayed on the masked alarm page, and a new mask rule will be generated on the mask rule page.

## Procedure

**Step 1** Click [Monitor] -> [Alarm] -> [Recent] to enter the real-time alarm page.

**Step 2** In the real-time alarm list, click the  icon corresponding to an alarm and enter the reason for blocking in the pop-up window to block the alarm.

----End



### NOTE

The operation of masking alarms will create a mask rule. User can also mask alarms by creating a mask rule.

---


## 9. Alarm Notification

In the real-time alarm list, user can choose to notify the corresponding contact of the alarm. When an alarm occurs, ISPIM can automatically notify the user by email, or the user can manually trigger the

alarm notification.

## Procedure

**Step 1** Click [Monitor] -> [Alarm] -> [Recent] to enter the real-time alarm page.

**Step 2** In the real-time alarm list, click the  icon of an alarm to notify the corresponding contact.

---End



### NOTE

Before using the alarm notification function, user needs to pre-set the mail server, the contact person to receive the alarm notification and other related information on the [NOTE Rules] page.

---

## 10. Export Current Alarm

In the current alarm list, user can export real-time alarms as needed, and the exported file format is Excel.

## Procedure

**Step 1** Click [Monitor] -> [Alarm] -> [Recent] to enter the real-time alarm page.

**Step 2** In the current alarm list, after selecting the alarm to be exported (multiple selection is supported), click the <Export> button above the list to export the selected alarm information.

---End

## 7.2.2 Historical Alarm

Click [Monitor] -> [Alarm] -> [History] to enter the historical alarm page, as shown in Figure 7-3. On the historical alarm page, user can view historical alarms and perform delete operations.

If ISPIM detects that an alarm is no longer continuing, or receives trap and knows that an alarm is no longer continuing, it will automatically trigger alarm recovery and convert real-time alarms to historical alarms. The historical alarm page mainly displays historical alarms in the system, or real-time alarms cleared by the user, which is convenient for users to query and trace.



The deleted historical alarms will be permanently deleted, please operate with caution.

Figure 7-3 Historical Alarm Page

Name	Asset Name	Serial Number	IP	Severity	Location	Alert Time	Recovery Time	Clear Type	Logical Type	Descrj Operation
Server network comm...	inspur_100.7.34.133	218607424	100.7.34.133	Fault	Net-Ping	2020-11-09 15:46:57	2020-11-09 15:51:50	Automatic Clear	Alert for abnor...	Server   [X]
Server hard disk not in...	inspur_100.7.34.133	218607424	100.7.34.133	Serious	DISK3_Status	2020-11-09 11:01:12	2020-11-09 11:06:07	Automatic Clear	Hard disk hard...	Server   [X]
Server hard disk not in...	inspur_100.7.34.133	218607424	100.7.34.133	Serious	DISK1_Status	2020-11-09 11:01:12	2020-11-09 11:06:07	Automatic Clear	Hard disk hard...	Server   [X]
Server hard disk not in...	inspur_100.7.34.133	218607424	100.7.34.133	Serious	DISK4_Status	2020-11-09 11:01:12	2020-11-09 11:06:07	Automatic Clear	Hard disk hard...	Server   [X]
Server hard disk not in...	inspur_100.7.34.133	218607424	100.7.34.133	Serious	DISK5_Status	2020-11-09 11:01:12	2020-11-09 11:06:07	Automatic Clear	Hard disk hard...	Server   [X]
Server hard disk not in...	inspur_100.7.34.133	218607424	100.7.34.133	Serious	DISK2_Status	2020-11-09 11:01:12	2020-11-09 11:06:07	Automatic Clear	Hard disk hard...	Server   [X]
Server hard disk not in...	inspur_100.7.34.133	218607424	100.7.34.133	Serious	DISK0_Status	2020-11-09 11:01:12	2020-11-09 11:06:07	Automatic Clear	Hard disk hard...	Server   [X]
Power off the server	inspur_100.7.34.132	218584178	100.7.34.132	Serious	POWER	2020-11-09 09:13:43	2020-11-09 09:39:14	Automatic Clear	System restart...	Power   [X]
Power off the server	inspur_100.7.34.133	218607424	100.7.34.133	Serious	POWER	2020-11-09 09:05:52	2020-11-09 09:16:02	Automatic Clear	System restart...	Power   [X]
Server network comm...	inspur_100.7.34.132	218584178	100.7.34.132	Fault	Net-Ping	2020-11-09 06:01:57	2020-11-09 06:06:58	Automatic Clear	Alert for abnor...	Server   [X]

## 7.2.3 Masked Alarm

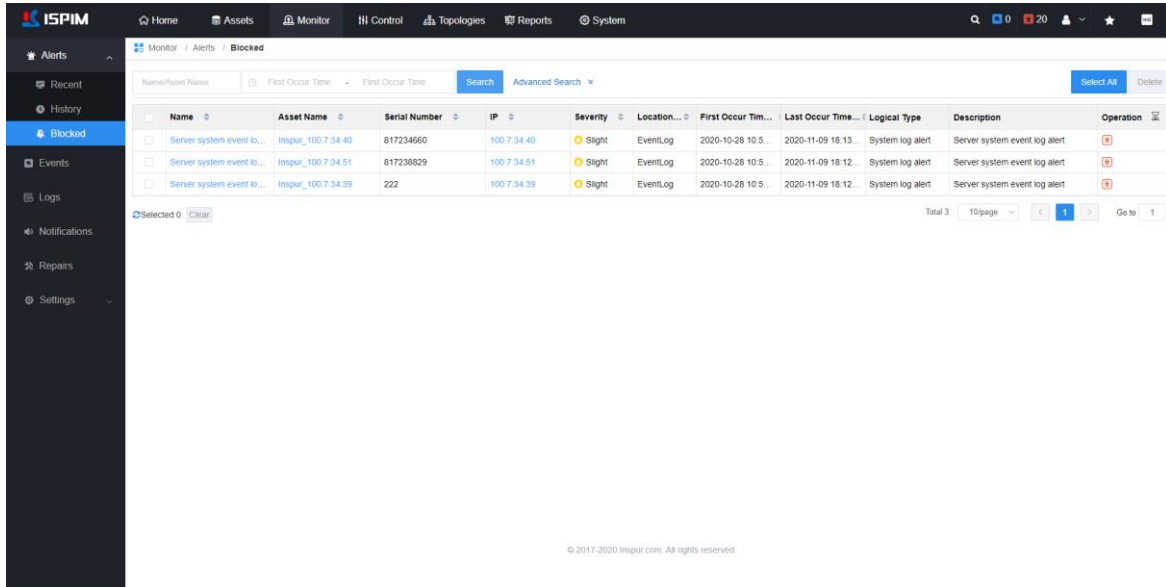
Click [Monitor]->[Alarms]->[Blocked] in turn to enter the masked alarm page, as shown in Figure 7-4. On the masked alarm page, user can view the list of blocked alarms, delete, search for alarms.



- The list of masked alarms shows the alarms that have been made by the user. After an alarm is made, if there is still alarm information of this type, it will be directly displayed in the masked alarm list.
- Delete operation will cause the masked alarm to be permanently deleted, please operate with caution.

Figure 7-4 Masked Alarm Page

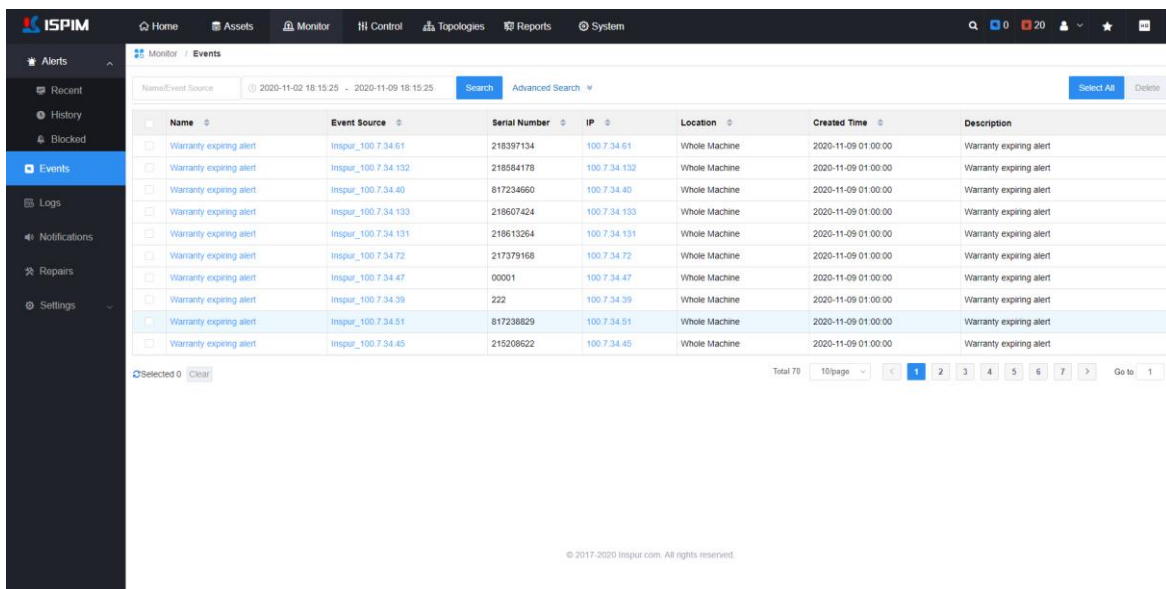




## 7.3 Event

Click [Monitor] -> [Event] to enter the event page, as shown in Figure 7-5. On the event page, user can view the event list, delete, and search for events.

Figure 7-5 Event Page



### 7.3.1 Event Introduction

Events refer to general notification information in ISIPM. This information will be generated when a specific action occurs on the device. The description of the event is shown in Table 7-3.

Table 7-3 Event Type

Category	Events
System	System configuration, system detection, server watchdog, system power, server power on
Hard disk	Hard drive insertion, hard drive detection
Processor	CPU detection event
Other	FRU event, maintenance is about to expire, trap test, battery charging, switch hot start, switch cold start, firewall record

## 7.3.2 Event Operation

In the event list, user can view the event details, event source server details, device IP, etc.

- **View event details:** In the event list, click an event name, and user can view the event details in the event information window that pops up on the right.
- **View event source server details:** In the event list, click an event source name in the event list to enter the server details page.
- **Access device:** In the event list, click the "IP" corresponding to an event, it will link to the device access page, and for the Inspur server, it will jump to the BMC login page.
- **Delete event:** In the time list, select the event to be deleted as required, click the <Delete> button above the list, and confirm in the pop-up window to delete the selected event.



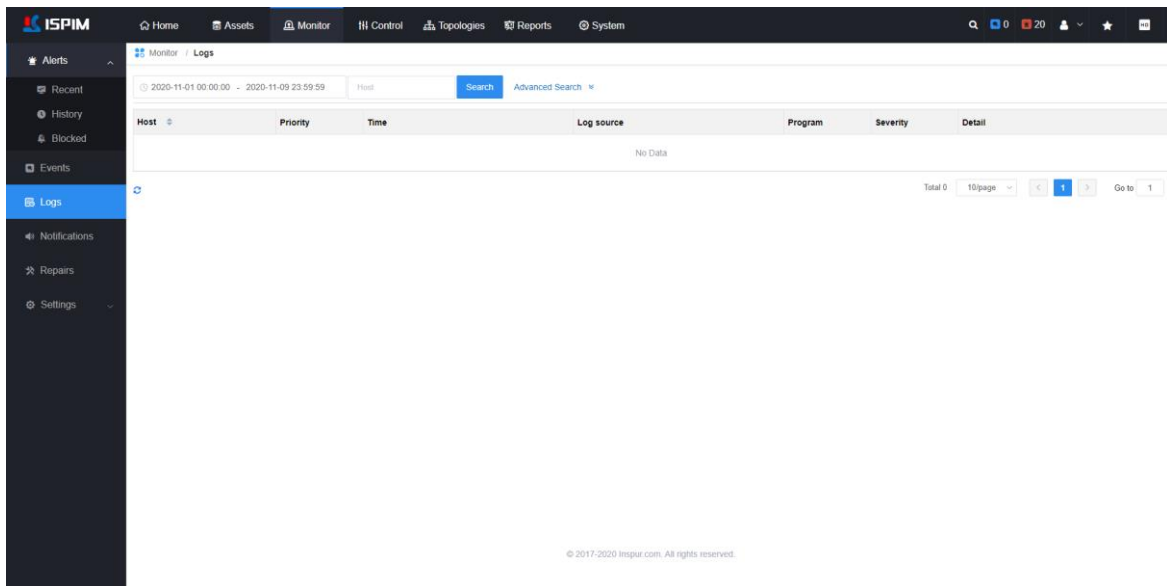
### NOTE

Deleted events cannot be recovered, please exercise caution.

## 7.4 Log Management

Click [Monitor] -> [Log] to enter the log management page, as shown in Figure 7-6. User can view syslog on this page. Syslog can be used for auditing, helping users find system problems in time, and ensure the stable operation of the system.

Figure 7-6 Log Management



## 7.5 Notification Records

Click [Monitor] -> [Notifications] to enter the notification record page, as shown in Figure 7-7. This page mainly records the alarm notification history, including resource name, notification type, notification method, recipients, etc. In the notification record page, user can view the notification details, perform delete or search operations.


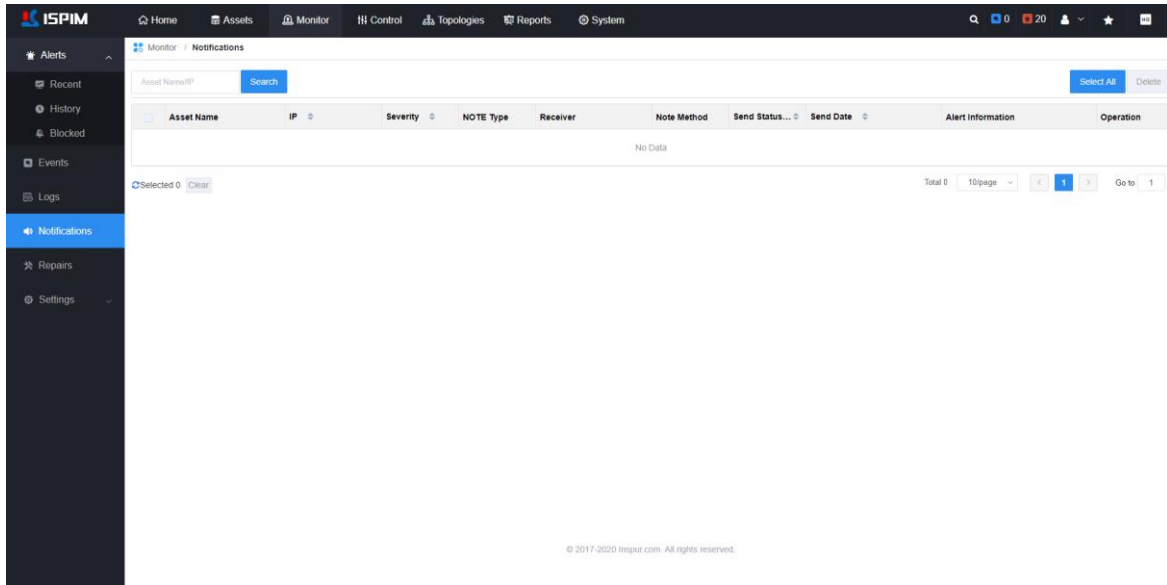
- **View notification details:** In the notification record list, click the alarm information corresponding to a resource, and user can view the detailed content of the alarm notification in the pop-up alarm information window.
- **Delete notification:** In the notification record list, click the  button corresponding to a resource to delete the notification record. After selecting multiple notification records in the list, click the <Delete> button above the list to delete the selected notification records in batches.
- **Search notification:** Enter the resource name or IP information in the search box to search notification records.

Figure 7-7 Notification Records Page



## 7.6 Repair Records




### NOTE

- Before using the repair work order function, user needs to set the repair rules and the related information about repair service & support.
- The rule for generating the repair work order is: user has enabled the repair rule, and an alarm corresponding to the repair rule is generated in ISPM, and ISPM sends the repair request to Inspur customer service. At this time, the system will automatically generate a repair order.

Click [Monitor] -> [Repairs] to enter the repair request form page. The repair request form page mainly records the system repair job order status, including: repair report number, resource name, equipment IP, alarm details, Recipient, sending status and other information, so that users can view and trace the details of the repair work order. On this page, you can view and execute the delete or search repair work order operations.

Click [Monitor] -> [Repairs] to enter the repair request form page. The content of the repair form list includes: number, resource name, equipment IP, alarm details, recipient, sending status and other information. On this page, user can view and execute delete or search operation.

- **Delete record:** In the list of repair orders, click the  icon corresponding to a certain order to delete the repair order; or after selecting multiple repair orders in the list, click the <Delete>

button above the list to delete all repair orders in batches.

- **Search record:** Enter the order number or IP information in the search box, user can search the repair order.

## 7.7 Monitoring Settings

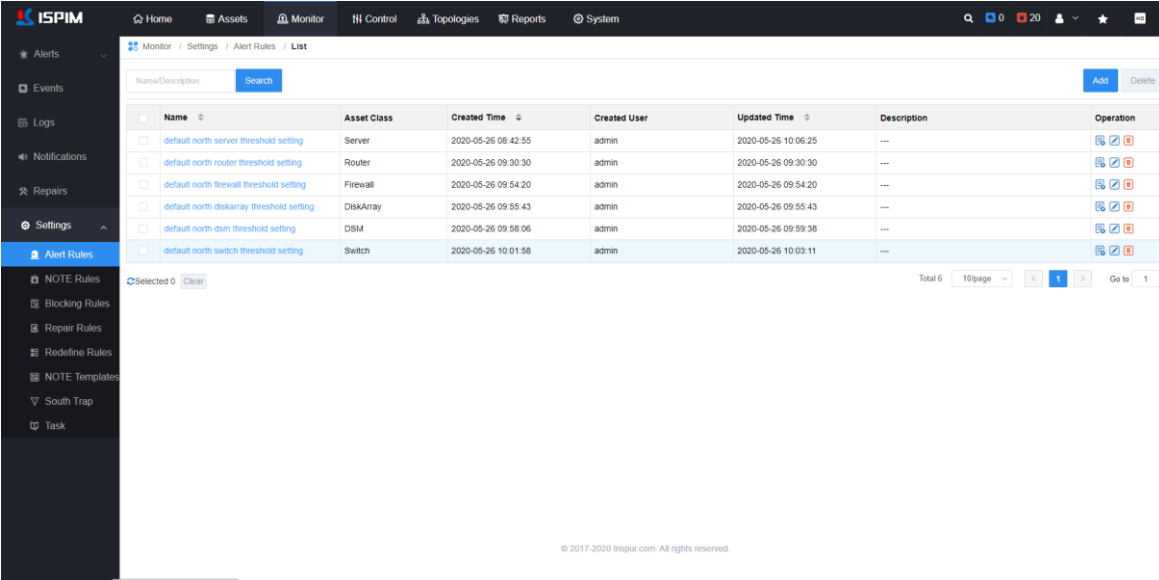
In the monitoring setting module, users can flexibly customize alarm rules, notification rules, masking rules, repair rules, and alarm redefine rules.

### 7.7.1 Alarm Rules

ISPIM can generate alarms based on alarm rules. ISPIM provides default alarm rules, including default server thresholds, default router thresholds, default firewall thresholds, default diskarray thresholds, default distributed storage thresholds, and default switch thresholds.

Users can also customize the alarm rules. Click [Monitor] -> [Settings] -> [Alarm Rules] to enter the alarm rules page, as shown in Figure 7-8. On the alarm rules page, user can add custom alarm rules, perform operations such as editing, deleting, applying, and viewing alarm rules.

Figure 7-8 Alarm Rules Page



The screenshot displays the 'Alert Rules' page in the ISPIM interface. The page features a navigation menu on the left with options like Alerts, Events, Logs, Notifications, Repairs, and Settings. The 'Alert Rules' section is active, showing a list of default rules. The table below contains the following data:

Name	Asset Class	Created Time	Created User	Updated Time	Description	Operation
default north server threshold setting	Server	2020-05-26 08:42:55	admin	2020-05-26 10:06:25	---	[Edit] [Delete]
default north router threshold setting	Router	2020-05-26 09:30:30	admin	2020-05-26 09:30:30	---	[Edit] [Delete]
default north firewall threshold setting	Firewall	2020-05-26 09:54:20	admin	2020-05-26 09:54:20	---	[Edit] [Delete]
default north diskarray threshold setting	DiskArray	2020-05-26 09:55:43	admin	2020-05-26 09:55:43	---	[Edit] [Delete]
default north dsm threshold setting	DSM	2020-05-26 09:58:06	admin	2020-05-26 09:59:38	---	[Edit] [Delete]
default north switch threshold setting	Switch	2020-05-26 10:01:58	admin	2020-05-26 10:03:11	---	[Edit] [Delete]

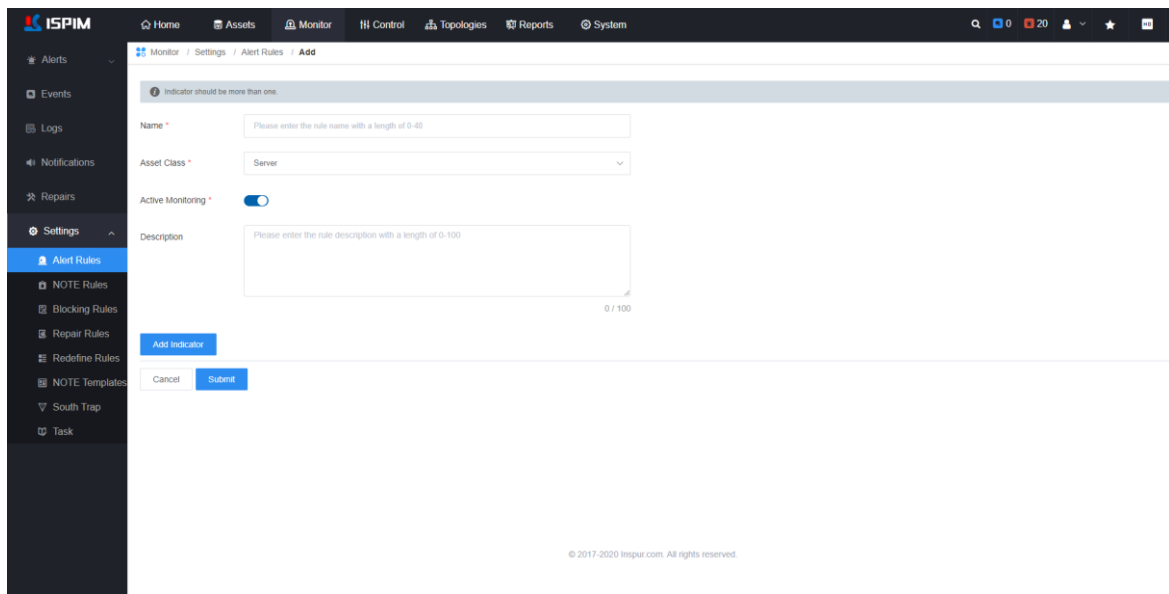
At the bottom of the table, it indicates 'Total 6' items and '10/page' for pagination. The page footer includes the copyright notice: '© 2017-2020 Inspur.com. All rights reserved.'

## 1. Add Alarm Rules

Users can add custom alarm rules

### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Alarm Rules] to enter the alarm rules page. Click the <Add> button at the upper right corner of the page to enter the add alarm rules page, as shown in the figure below.



**Step 2** Set the rule name, resource type, active monitoring and other parameters.

- **Resource type:** Including servers, disk arrays, distributed storage, switches, firewalls, routers, load balancers, waf, anti-DDOS, IDS/IPS, power environment, SDN, facilities (data centers, rooms, cabinets, which have the same monitoring indicators).
- **Active monitoring:** Choose whether ISPIM actively polls resources to collect relevant data. If it is not enabled, it means that ISPIM will passively accept trap alarms from the device. If it is enabled, it means that ISPIM actively polls.

**Step 3** Click the <Add> button, and in the pop-up window, user can view and select the performance monitoring items of each resource, and click the <Submit> button after selection.

**Step 4** After the monitoring items are submitted, the page will return to the page for

adding alarm rules. At this time, the selected monitoring items will be displayed in the items area. Click the item name to configure the alarm threshold and duration of each monitoring item.

- Duration: When ISPIM finds that the value of the monitoring item exceeds the set threshold, and the time exceeds the set duration, an alarm will be triggered. The duration is at least 5 minutes, and the maximum is 30 minutes.
- Threshold: Set at least one threshold: fault, serious, moderate, slight.

**Step 5** Click the <Submit> button to complete the creation of the alarm rule.


---End

## 2. Apply Alarm Rules

For the created alarm rules, they need to be associated with the corresponding devices to take effect.

### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Alarm Rules] to enter the alarm rules page.

**Step 2** In the alarm rule list, click the  icon corresponding to an alarm rule to enter the alarm asset setting page.

**Step 3** Click the <Device List> button, in the device list that pops up on the right, select the devices to which the alarm rule is applied, and click the <Add> button, the selected devices will be added to the device list.

**Step 4** Click the <Submit> button to complete the application of the alarm rule.


---End


## 3. Edit/Delete Alarm Rules

Alarm rules support edit and delete operations.

### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Alarm Rules] to enter the alarm rules page.

**Step 2** In the alarm rule list, click the  icon of an alarm rule to enter the edit alarm rule page, where user can edit the alarm rule name, monitoring indicators and other parameters.

**Step 3** In the alarm rule list, click the  icon corresponding to an alarm rule and confirm in the pop-up window to delete the alarm rule. To delete in batches, user can select multiple alarm rules and click <Delete> button at the top of the list.

---End

## 4. View Alarm Rule Detail

User can view the detailed information of the alarm rule.

### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Alarm Rules] to enter the alarm rules page.

**Step 2** In the alarm rule list, click the name of a rule to enter the alarm rule details page, where user can view the details of the alarm rule, including the name, resource type, creator, and thresholds.

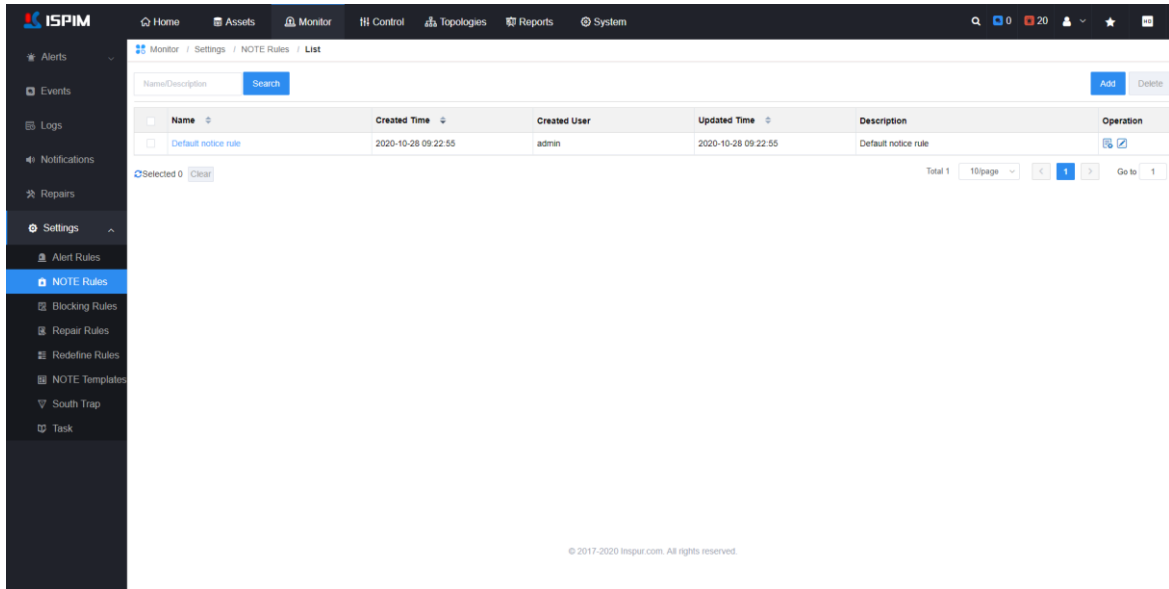
---End

## 7.7.2 Notification Rules

ISPIM will notify relevant personnel of alarms according to the notification rules. ISPIM provides default notification rules. Click [Monitor] -> [Settings] -> [NOTE Rules] to enter the notification rules page, as shown in Figure 7-9. Notification rules page, user can customize notification rules, perform editing, deleting, applying, viewing details operations.

Figure 7-9 Notification Rules





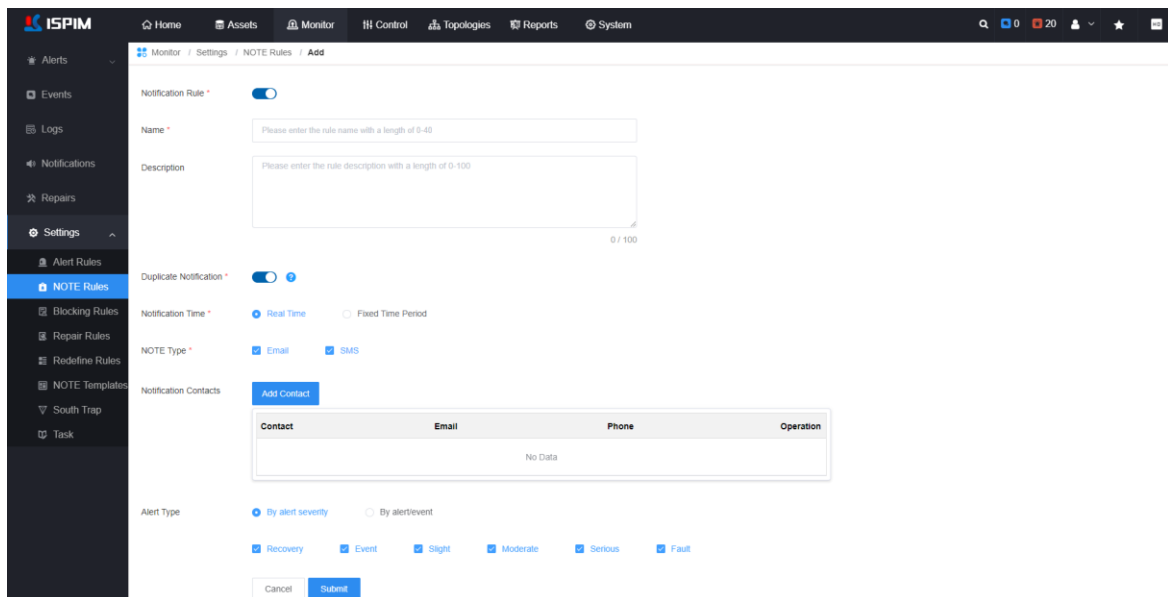
## 1. Add Notification Rules

Users can add custom alarm notification rules.

### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [NOTE Rules] to enter the notification rules page.

**Step 2** Click the <Add> button in the upper right corner to enter the page for adding notification rules, as shown in the figure below.



**Step 3** Set the notification rule name, notification time, notification method and other parameters.

- **Notification Rule:** Enable/disable this rule .
- **Duplicate Notification:** All alarms that are not cleared within 24 hours will be automatically scanned at 08:00 every day, and alarm notifications will be sent again.
- **Notification Time:** User can choose to "send alarms in real time" or send alarms in a fixed time period,
- **Notification Type:** User can choose to notify the contact by "email" or "SMS".

**【NOTE】** To use "Email" or "Short Message" notification, users need to enter the [System] -> [Settings] -> [NOTE Servers] page to configure their own mail server, short message server or other notification servers.

- **Notification Contacts:** Click <Add Contact>, in the pop-up contact management window, user can add, submit or delete contacts.
- **Alarm Type:** Select the trigger condition of the alarm notification: send the notification according to the specified alarm level, or only send the specific alarms notification.

**Step 4** After the above related notification parameters are configured, click the <Submit> button to complete the creation of the notification rule.


--End

## 2. Apply Notification Rules

For the new created notification rules, they need to be associated with devices before taking effect.

### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [NOTE Rules] to enter the notification rules page.

**Step 2** In the notification rule list, click the  icon of a notification rule to enter the corresponding assets page.

**Step 3** Click the <Device List> button, in the pop-up device list on the right, select the device to which the notification rule needs to be applied, and click the <Add> button, the selected device will be added to the device list.

**Step 4** Click the <Submit> button to complete the application of the notification rule.

---End

### 3. View Notification Rule Detail

User can view the details of notification rule.

#### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [NOTE Rules] to enter the notification rules page.

**Step 2** In the notification rule list, click a rule name to enter the notification rule details page, where user can view the rule details, including the name, notification contact, notification method and other information.


---End


### 4. Edit/Delete Notification Rule

User can edit or delete notification rules.

#### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [NOTE Rules] to enter the notification rules page.

**Step 2** In the notification rule list, click the  icon corresponding to a notification rule to enter the edit notification rule page. User can edit the rule name, notification type, contact and other parameters as needed.

**Step 3** In the notification rule list, click the  icon corresponding to a notification rule and confirm in the pop-up window to delete the notification rule. To delete in batches, user can select multiple notification rules and click <Delete> button at the top of the list.

---End



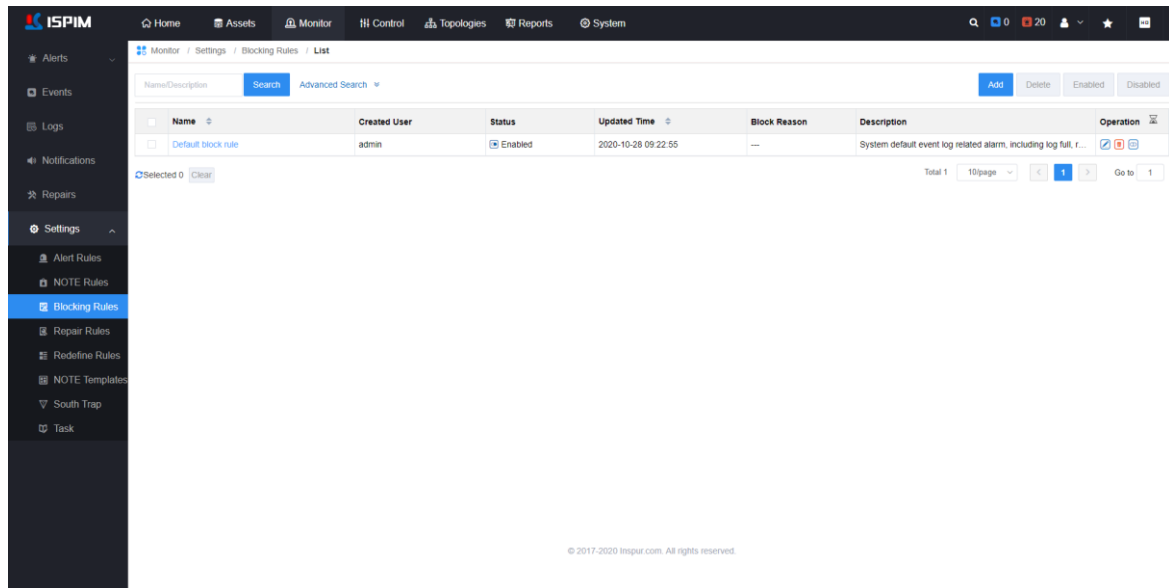
#### NOTE

- Unless the device has corresponding user-defined notification rules, the default notification rules built in ISPIM will be used.
- User can not delete default notification rule.

## 7.7.3 Masking Rules

ISPIM can mask alarm according to the mask rules. Click [Monitor] -> [Settings] -> [Blocking Rules] to enter the masking rules page, as shown in Figure 7-10. In the rules page, user can customize masking rules, perform editing, delete, and enable/disable operations.

Figure 7-10 Masking Rule Page



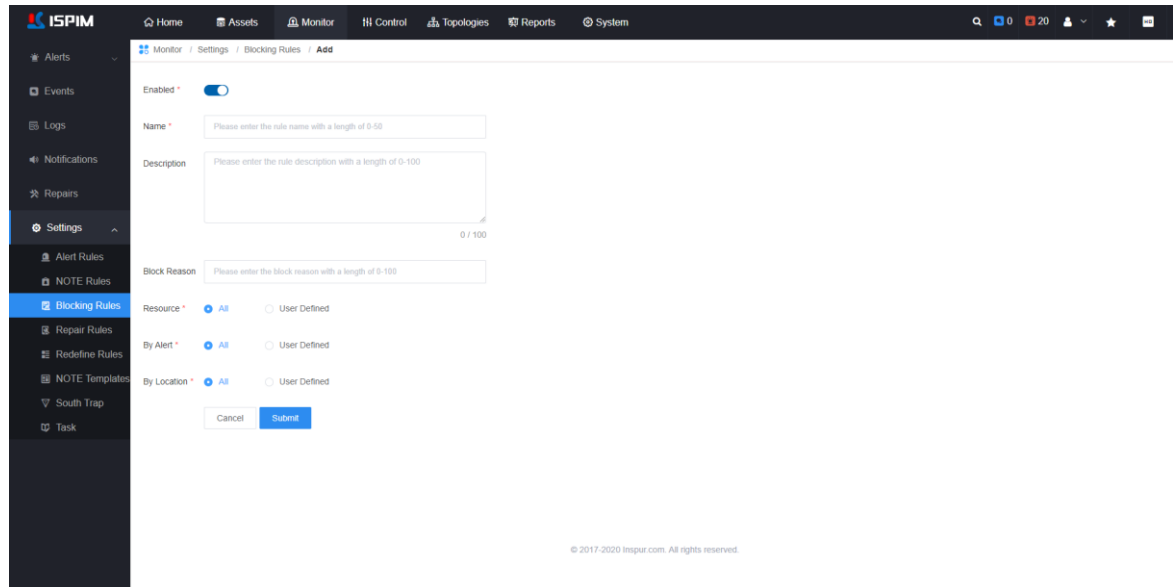
### 1. Create Masking Rules

ISPIM provides default masking rule. Users can also customize alarm masking rules.

#### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Blocking Rules] to enter the blocking rules page.

**Step 2** Click the <Add> button above the list of masking rules to enter the page for adding masking rules, as shown in the figure below.



### Step 3 Configure rules related parameters:

- Related Resource: Selecting "All" means that the rule applies to all devices. Select "Custom" to apply to specific devices.
- Masked Alarm Type: Select "All" to block all types of alarms, select "Custom" to block specific alarms.
- Mask Alarm by Location: Select the location of the component to be masked. Select "All" to mask the alarms of all component locations, select "Custom" to specify the alarm locations.

### Step 5 Click the <Submit> button to complete the creation of the masking rule.

----End

#### NOTE

When the alarm is masked by location, the location list only contains the the Inspur server BMC sensors. To add a custom location, user can click the <Add Location> button to manually add the location.

## 2. Manage Masking Rules


User can edit, delete, enable/disable masking rules.


### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Blocking Rules] to enter the masking rules page.

**Step 2** In the masking rule list, click the  icon of a masking rule to enter the edit page.

User can modify the rule name, source, and location parameters as needed.

**Step 3** In the rule list, click the  icon of a rule, and confirm in the pop-up window to delete the rule. To delete in batches, user can check multiple rules and click <Delete> button at the top of the list.

**Step 4** In the list of masking rules, click the  icon of a rule to enable or disable the rule. For batch operation, checking mutiple rules, click the <Enable/Disable> button above the list.

----End

### 3. View Masking Rule Detail

Users can view detailed information about masking rules

#### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Blocking Rules] to enter the masking rules page.

**Step 2** In the list of masking rules, click a rule name, and user can view the details of the rule in the pop-up window on the right

----End

### 7.7.4 Repair Rules

For the Inspur server, the user can choose to enable the automatic repair report function: when a corresponding alarm occurs on the device, the ISPIM platform will automatically notify the Inspur customer service staff of this alarm.

Click [Monitor] -> [Settings] -> [Repair Rules] to enter the repair rules page, as shown in Figure 7-11. On this page, user can manage the repair rules.



Figure 7-11 Repair Rules Page

Name	Severity	Automatic Repair Status	Operation
Warranty expiring alert	Event	On	Repair
Unplug the server hard disk	Serious	Off	Repair
Total server power consumption threshold alert	Slight	On	Repair
Total server power consumption threshold alert	Moderate	Off	Repair
Total server power consumption threshold alert	Serious	Off	Repair
Total server power consumption threshold alert	Fault	Off	Repair
The server failed to start the device.	Moderate	Off	Repair
The server detected that the device power cord is not connected	Serious	Off	Repair
The server detected an abnormal PCIe card	Moderate	Off	Repair
The server detected a memory failure	Fault	On	Repair

## 1. Enable Repair Rules



- Before enabling the repair rule, the user must first enter the [Service & Support] page to configure the relevant information, including the repair email, order prefix, customer company and other information.
- After the repair rule is enabled, when the device generates a corresponding alarm, ISPM will report the alarm to Inspur customer service staff and automatically generate a repair order.
- The repair rules are built in the system, and the user can only choose to turn on or off a repair rule, and cannot add or edit the repair rule.

- **Enable Single Repair Rule:** In the list of repair rules, click the  or  icon of an alarm to turn on or off the repair of this alarm.
- **Batch Enable Repair Rules:** In the list of repair rules, select multiple alarm items to be triggered, click the <Repair> button above the list, and confirm in the pop-up window to enable the selected repair rules in batches.

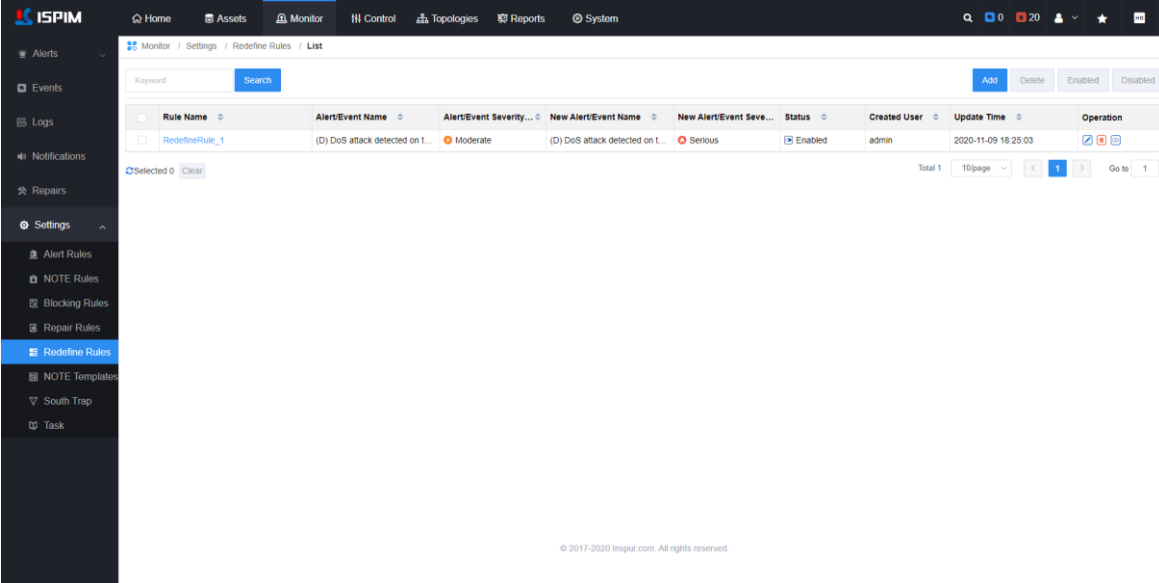
## 2. Search Repair Rules

- Basic query: In the upper left corner of the repair rule page, enter the rule name, and click the <Search> button to fuzzy query.
- Advanced query: Click <Advanced Search>, select the alarm level or status, the repair list will automatically refresh and display the result. Click <Reset > button, user can reset the query condition.

## 7.7.5 Redefine Rules

Click [Monitor] -> [Settings] -> [Redefine Rules] to enter the redefine rule page, as shown in Figure 7-12. On this page users can add, delete, enable/disable, edit rules. User can redefine the alarm name, alarm level, and equipment to which the rules apply

Figure 7-12 Redefinition Rules Page



Rule Name	Alert/Event Name	Alert/Event Severity	New Alert/Event Name	New Alert/Event Severity	Status	Created User	Update Time	Operation
RedefineRule_1	(D) DoS attack detected on t...	Moderate	(D) DoS attack detected on t...	Serious	Enabled	admin	2020-11-09 16:25:03	[Edit] [Delete]

### NOTE

- Each rule can only contain one type of alarm/event, and each type of alarm/event can only be redefined once.



## 1. Add Redefinition Rules


User can add redefinition rules.

### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Redefine Rules] to enter the redefine rules page.

**Step 2** Click the <Add> button above the list to enter the add redefinition rule page, as shown in the figure below.

**Step 3** Set rules name, original alarm/event, new alarm/event name, related resources, new alarm severity, etc.

- Alert/Event: Click the  icon, in the alarm/event list that pops up on the right, select the original alarm/event to be redefined, and click the <Add> button.
- Name Redefine: Set the new alert/event name.
- Severity Redefine:
  - Alert/Event Source: Selecting "All" means it will take effect for all devices. Select "Custom" to specify the effective device.
  - New Alert/Event Severity: New level of alarms/events, including: event, slight, moderate, serious, fault.

**Step 4** Click the <Submit> button to complete the creation.


----End


## 2. Manage Redefinition Rules


User can edit, delete, enable/disable redefinition rules.

### Procedure

**Step 1** Click [Monitor] -> [Settings] -> [Redefine Rules] to enter the redefine rules page.

**Step 2** In the list, click the  icon of a redefinition rule to enter the edit page, where user can modify the relevant parameters of the rule.

**Step 3** Click the  icon of a rule to delete the rule. If user wants to delete in batches, select multiple items and click the <Delete> button above the list.

**Step 4** Click the  icon of the rule to choose to enable/disable the rule. User can also check the rule and click the <Enable/Disable> button above the list to enable/disable the rule.

----End

## 3. View Redefinition Rule Detail

Users can view the details of the redefinition rules.

### Procedure

**Step 1** Click [Monitoring] -> [Settings] -> [Redefine Rules] to enter the redefinition rule page.

**Step 2** In the redefinition rule list, click a rule name, and user can view the detailed information of the rule in the pop-up details page on the right.

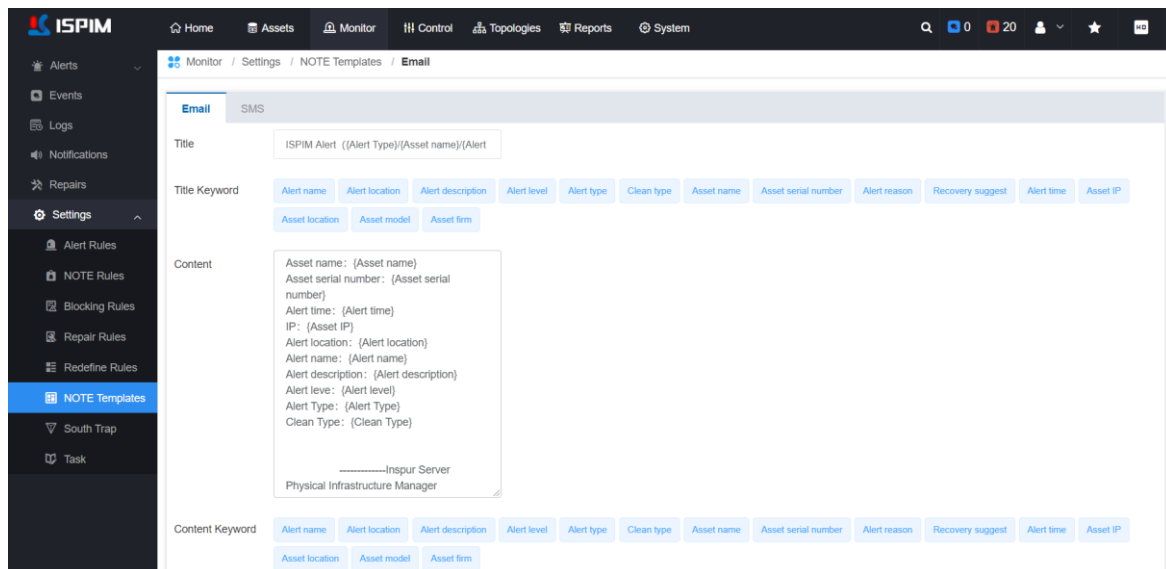
----End

## 7.7.6 Notification Template

Click [Monitor] -> [Settings] -> [Note Template] to enter the notification content template setting page, as shown in Figure 7-13. On this page, user can set the email or SMS alert notification content template, including the title, content keywords, etc.

- Email content template settings: Select the "Email" tab, user can set the subject and content format of the mail as needed.
  - Title keywords: Click the title keyword to add it to the email title.
  - Content keywords: Click the content keyword to add it to the email content.
- Short message content template settings: Select the "SMS" tab, edit the content keywords as needed, and click <Submit>.


Figure 7-13 Notification Template




## 7.7.7 Southbound Trap Settings

Click [Monitor] -> [Settings] -> [South Trap], enter the southbound trap setting page, as shown in Figure 7-14. User can set the device's trap receiving destination address to ISPIM IP.

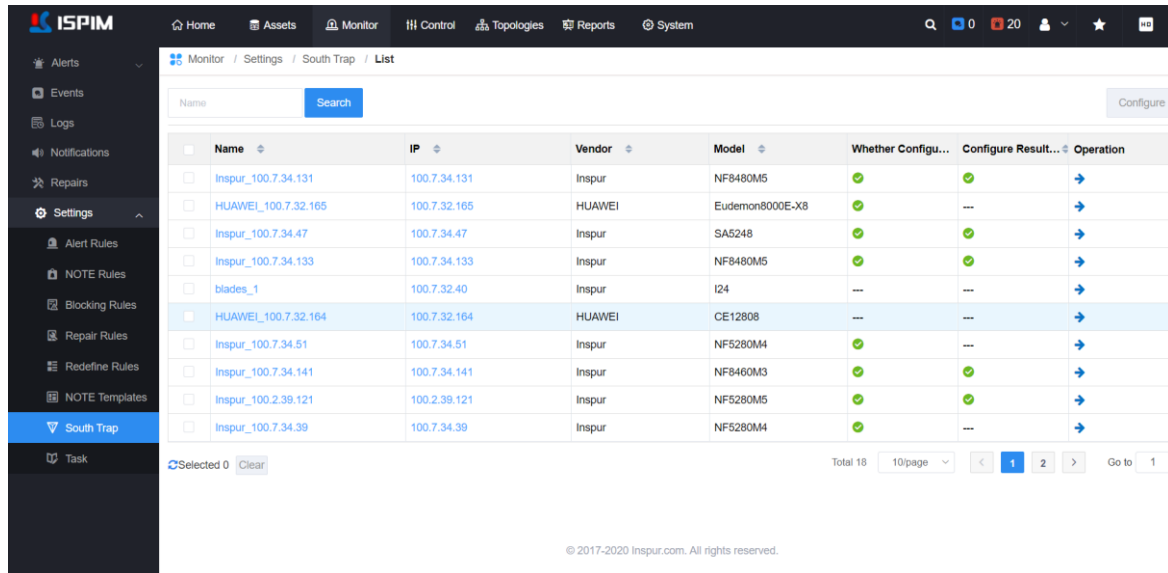
On the southbound trap settings page, it also provides links to quick access device details page and device management page.

- **Visit device detail page:** Clicking on a device name will enter the device details page. View server details for details.
- **Visit device management page:** Click the IP of a device to enter the device management page, such as the BMC WebUI page of the Inspur server.
- **Config trap destination:**
  - **Single node config:** In the device list, click the  icon of a device to perform the southbound trap configuration operation. After the configuration is successful, user can

click the  icon in the lower left corner of the list to refresh and check the result.

- **Batch config:** Check multiple devices and click the <Configure> button above the list to configure batches.

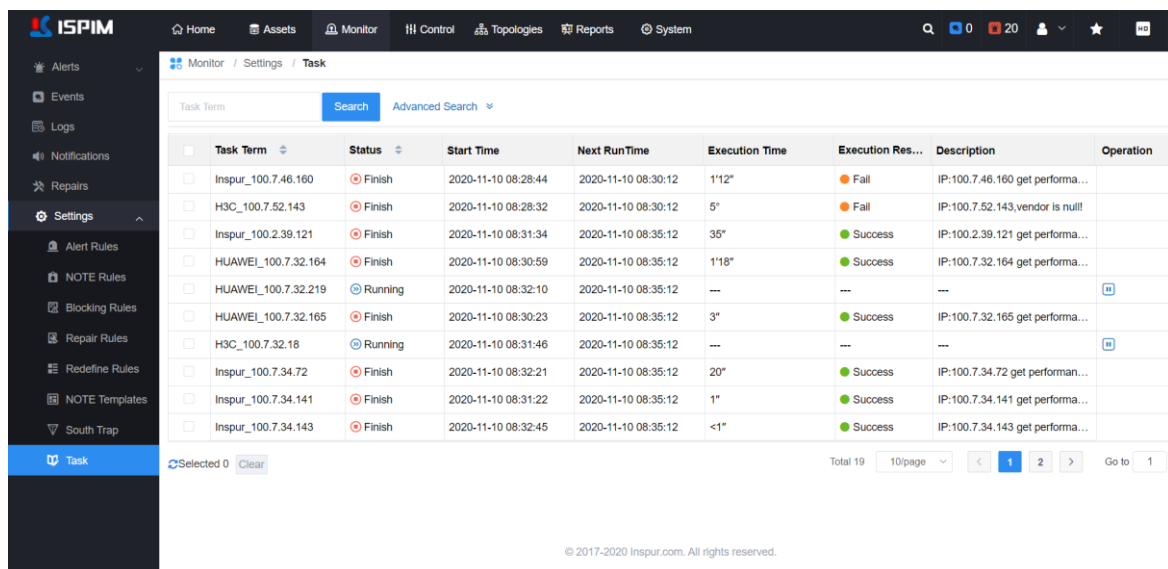
Figure 7-14 Southbound Trap Settings



## 7.7.8 Monitoring Tasks


Click [Monitoring] -> [Settings] -> [Tasks] to enter the monitoring task page. As shown in Figure 7-15. In the monitoring task page, user can view the details of the monitoring tasks for all devices, including: task status, execution time, start time, end time, execution result, task description.

Figure 7-15 Monitoring Tasks





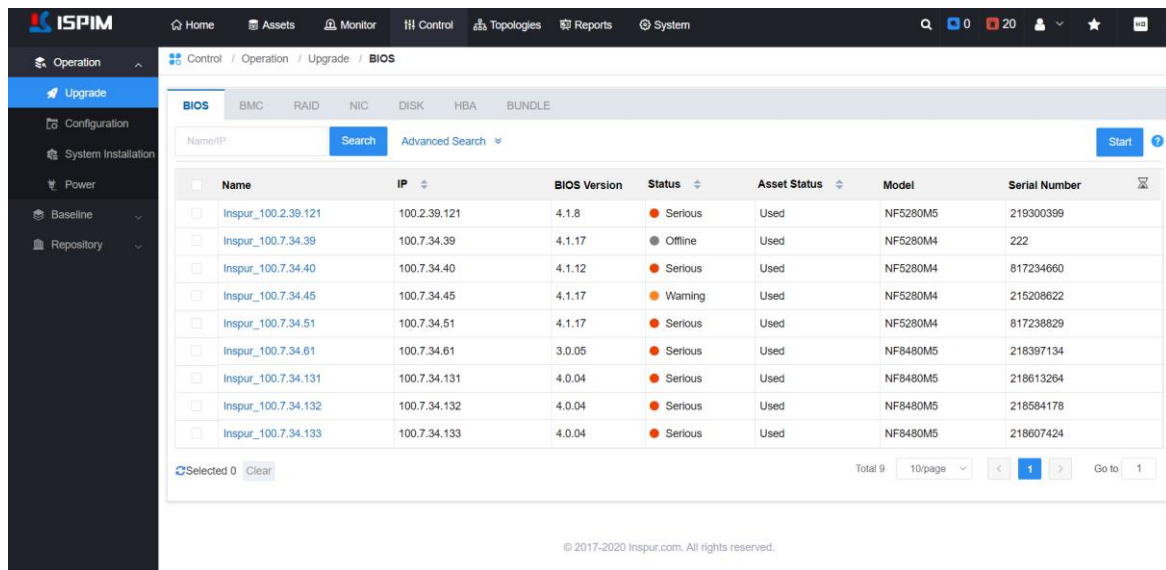
NOTE

- For a task whose task status is "running", user can click its  icon to pause the task.
  - The monitoring task frequency can be set on the [System] page.
  - Task list supports query operation.
-

# 8 Control Management

In the top navigation bar of ISPIM, select the "Control" tab, user can enter the control management module, as shown in Figure 8-1. The control management module mainly includes firmware upgrade, firmware configuration, system installation, power management, baseline management and image repository management. It can realize batch deployment and configuration of Inspur servers, which is convenient for users to quickly put servers into use and improve operation and maintenance efficiency.

Figure 8-1 Control Management



## 8.1 Repository

Image repository management can perform unified management of operating system images, firmware upgrade files (BIOS, BMC, RAID, NIC, DISK, HBA, BUNDLE), and software bundles. At the same time, unified repository management is also the basis of baseline management.

### NOTE

- For OS and firmware upgrade files, currently only supports local uploading.
- For bundles, both local upload and remote synchronization are supported.

## 8.1.1 OS Image Library

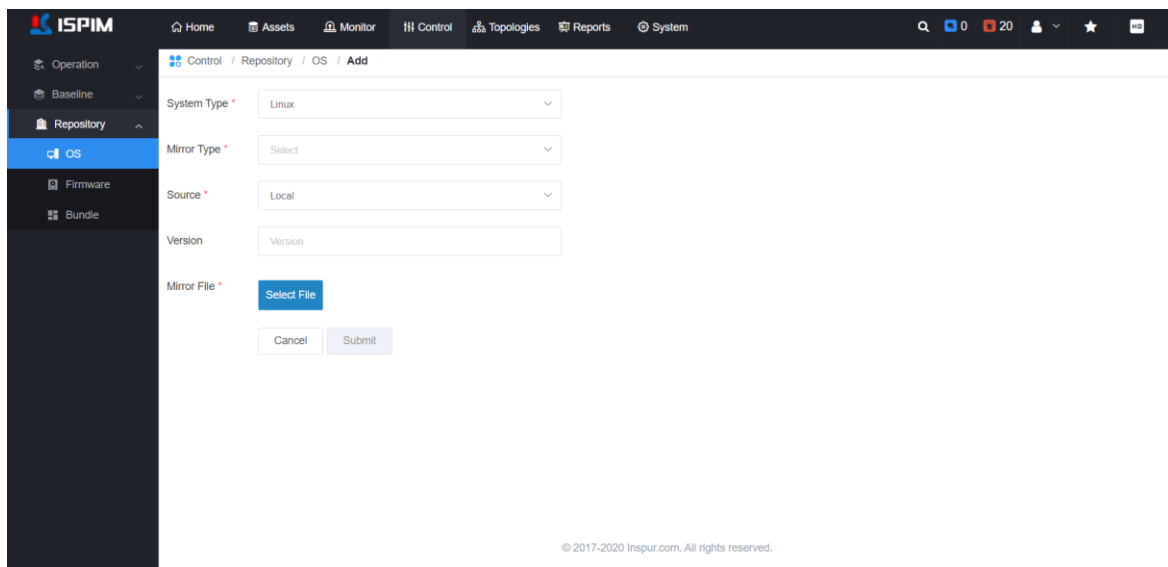
OS library management can perform unified version management on OS images. User can view the OS list, perform operations such as adding, searching or deleting OS images.

### 1. Add OS Image

#### Procedure

**Step 1** Click [Control] -> [Repository] -> [OS] to enter the OS library management page.

**Step 2** Click the <Add> button to enter the add mirror page, as shown in the figure below.




**Step 3** Set the system type, mirror type, source, version of the OS mirror file, click the <select mirror> button to upload.

**Step 4** Click the <Submit> button to upload the selected OS image to the ISPIM platform.

--End

### 2. Delete OS Images

- Delete a single mirror: In the mirror list, click the  icon corresponding to a mirror, and confirm in the pop-up window to delete the mirror.
- Batch delete mirrors: In the mirror list, after selecting multiple mirrors in batch, click the <Delete> button above the list, and confirm in the pop-up window to delete multiple mirrors

in batch.

### 3. Search OS Images

Enter the file name in the search box to search for the OS mirror. Click <Advanced Search> to search for the OS mirror according to the system type or mirror type.

## 8.1.2 Firmware File Library

Firmware library management is mainly to manage the files used in the firmware upgrade process such as BMC, BIOS, RAID, HBA, DISK. On the firmware library management page, user can view the file list, perform operations such as adding, searching or deleting.

### 1. Add Firmware File



#### NOTE

The naming requirements for the firmware file are as follows

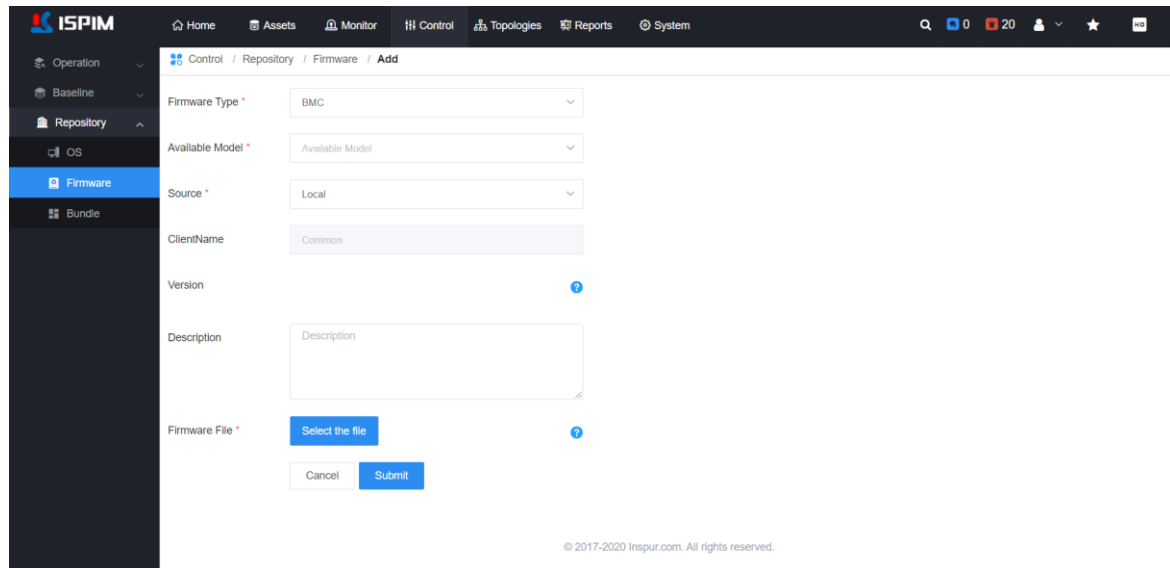
- BMC: Server Model\_BMC\_Customer Name\_Version\_Release Date
  - BIOS: Server Model\_BIOS\_Customer Name\_Version\_Release Date
  - RAID: isma\_raid\_Model\_Version\_Release Date
  - HBA: isma\_hba\_Model\_Version\_Release Date
  - NIC: isma\_nic\_Model\_Version\_Release Date
  - DISK: isma\_disk\_Model\_Version\_Release Date
- 

## Procedure


**Step 1** Click [Control] -> [Repository] -> [Firmware] to enter the firmware library management page.

**Step 2** Click the <Add> button to enter the page for adding firmware files, as shown below






**Step 3** Set the firmware file related parameters such as firmware type, available model, source, then click “Select the file” button to upload the firmware file.

- Firmware Type: Including BMC, BIOS, RAID, HBA, NIC and DISK.
- Available Model: Select the applicable server model.
- File Source: The default is "local", which means that only local uploads are supported
- Firmware file: Click <Select the file> to upload a firmware file that meets the naming convention. Click the  icon to view the naming requirements for the firmware file.

**Step 4** Click the <Submit> button to upload the selected firmware file to the ISPIM platform.

--End

## 2. Delete Firmware File

- Delete a single firmware file: In the image list, click the  icon of a firmware file and confirm in the pop-up window to delete the firmware file.
- Delete firmware files in batch: In the firmware file list, after selecting multiple firmware files in batch, click the <Delete> button above the list, and confirm in the pop-up window to delete multiple firmware files in batch.

### 3. Search Firmware File

ISPIM support query operation of firmware files. Including fuzzy query and advanced query.

## 8.1.3 Bundle Management

Bundle management is to package and manage the firmware files of BIOS, BMC, RAID, NIC, DISK, HBA in a unified way. Through the bundle management function, one-click upgrade of BIOS, BMC, RAID, NIC, DISK, HBA firmware can be realized.

### 1. Add Bundle File

User can upload local bundle file to ISPIM.

#### Procedure

**Step 1** Click [Control] -> [Repository] -> [Bundle] to enter the package management page.

**Step 2** Click the <Add> button to enter the upload bundle file page.

**Step 3** Click <Select File>, select the local bundle file, and click <Submit> to upload the selected package file to the ISPIM platform.

--End

### 2. Synchronize Bundle File

The package files can be synchronized remotely as needed.

#### Requirements

The ISFM account has been configured in the ISPIM platform.

#### Procedure

**Step 1** Click [Control] -> [Repository] -> [Bundle] to enter the bundle management page.


**Step 2** Click the <Synchronize> button at the top right of the list to enter the bundle synchronization page.

**Step 3** Click the <Full Sync> button in the list operation bar to upload the image file.

To synchronize a single file, user can click the <Select Sync> button in the list operation bar, select the firmware to be synchronized, and then click <Sync>.

--End

### 3. Delete Bundle File

- Delete a single bundle file: In the file list, click the  icon of a bundle file, and confirm in the pop-up window to delete the bundle file.
- Batch delete bundle files: In the bundle file list, after selecting multiple files in batches, click the <Delete> button above the list, and confirm in the pop-up window.

### 4. Search Bundle File

ISPIM support query operation of firmware files. Including fuzzy query and advanced query.

The bundle files supports two acquisition methods: automatic synchronization and local upload

- Automatic synchronization: In the case that ISPIM can link to the Inspur official mirror library website, it supports automatic synchronization of firmware upgrade packages from the official mirror library.
- Local upload: When ISPIM cannot link to the Inspur official mirror library website, it supports uploading the upgrade package from the local to ISPIM.

## 8.2 Firmware Upgrade

ISPIM supports calling BMC's out-of-band HTTP interface to upgrade server BIOS and BM. At the same time, it supports the upgrade of RAID, NIC, DISK, and HBA through ISQP in-band way.

## 8.2.1 Read Before Upgrading

### 1. Server Number Limit in Batch Upgrade

When creating an upgrade task, there is no restriction on the number of devices. However, in the actual upgrade process, the system will upgrade the devices in batches, and each batch supports up to 50 devices (the network bandwidth requirement is at least 800Mbps).

### 2. Requirements

- The effective bandwidth required by ISPIM for equipment batch upgrades is at least 800Mbps and above.
- When the effective bandwidth is satisfied, the update file distribution time to the server is about 1 minute. When the effective bandwidth is insufficient, the file delivery time will increase or even the distribution will fail.
- After the upgrade is complete, the device firmware image will take about 2 minutes to reload and effect.
- The upgrade time for a single device is about: file distribution time + upgrade execution time + firmware image reload time = about 5 minutes.

### 3. Precautions

- **File preparation:** Before firmware upgrade, user needs to upload the corresponding firmware file on the [Control] -> [Repository]> [Firmware] page.
- **Evaluation before upgrade:** As the firmware upgrade involves the distribution of image files, please make sure that the BMC network connection of the current device is normal before the upgrade, and ensure that the network bandwidth is sufficient and stable. Please refer to "Batch Upgrade Performance Constraints" to learn more about performance evaluation Details.
- **Upgrade test:** Before performing the batch upgrade, be sure to upgrade one device first, and then perform the batch upgrade after verifying that there is no problem.

- **Batch upgrade requirements:** The upgrade task only supports the same server model. You can use the advanced query function at the top left of the list to filter the devices of the same model.


## 8.2.2 BMC/BIOS Upgrade

The process of creating a BMS/BIOS upgrade task is similar. Here uses the BMC upgrade task as an example to introduce the upgrade process.

### Procedure

**Step 1 Enter the BMC upgrade page.** Click [Control] -> [Operation] -> [Upgrade] to enter the firmware upgrade page, select the "BMC" tab, and user will enter the BMC firmware upgrade page.

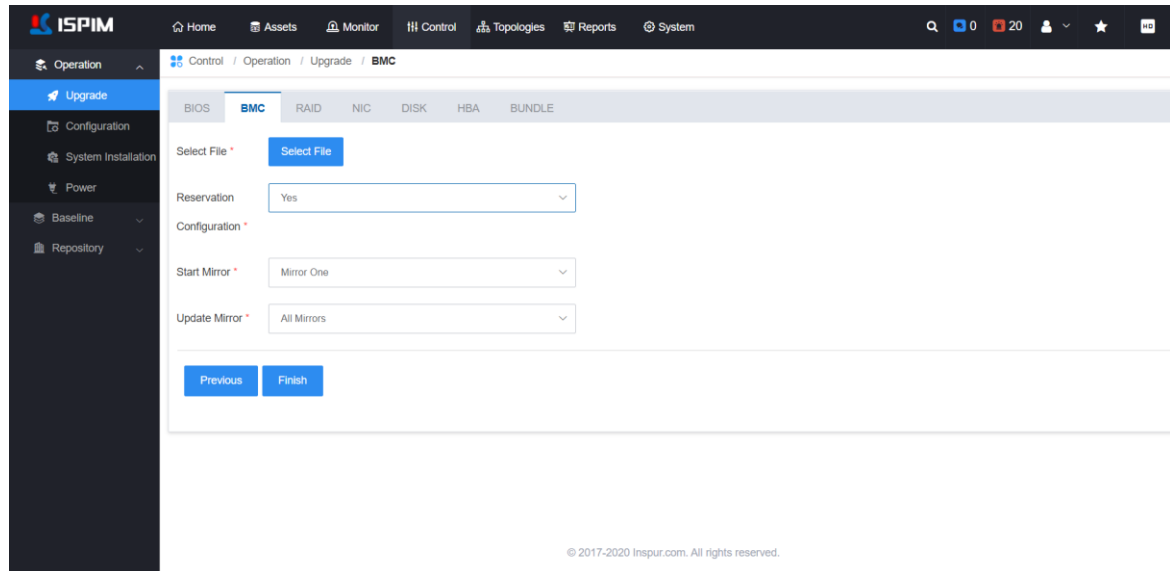
**Step 2 Select the device to be upgraded.** In the device list, user can check the devices to be upgraded in batches.

- Server model requirements: BMC batch upgrade tasks only support the same server model. User can use the advanced query function at the top left of the list to filter the devices of the same model.
- Supported models: hover the mouse over the  icon at the top of the list to view the device models supported by the BMC upgrade.

**Step 3 Configure upgrade parameters.** After the devices are selected, click the <Start> button at the top right of the list, and user will enter the BMC upgrade settings page, as shown in the figure below. User needs to configure the upgrade related parameters such as upgrade mirror file, whether to keep the BMC settings, BMC start mirror.


- Select Mirror: Click <Select File>, select the mirror file that needs to be uploaded in the list that pops up on the right, and click <Add> to select the mirror file. Please note that the upgrade file must have been uploaded to the mirror library.
- Keep configuration: whether keep the BMC settings in upgrade progress.
- Start mirroring: The BMC of Inspur M5 series servers contains active and standby dual mirrors. This parameter is used to set the mirror from which the BMC starts.

- Upgrade mirror: The BMC of the Inspur M5 series server adopts the main and standby dual mirror settings, this parameter is used to set which mirror of the BMC will be upgraded.



**Step 4** After the parameter configuration is completed, click the <Finish> button to complete the creation of the BMC upgrade task.

**Step 5** Check the execution of the upgrade task. There are two ways:

- Method 1: Click [System] -> [Task], user can enter the task center to view the details of each task in the ISIPM platform, including: task name, type, status, start time, completion time and other information. Click the task name, user can also view the execution of the subtasks of the nodes in the job.
- Method 2: In the top navigation bar of ISIPM, click the  icon to view the task list information that is running in the system, including task name, status, progress and other information.

---End

## 8.2.3 Other Firmware Upgrade

### NOTE

For the firmware upgrade of RAID, NIC, DISK, HBA, all rely on Inspur software ISQP. For details, please refer to "Inspur Server Quick Provisioning (ISQP) V6.0 0 User Manual"

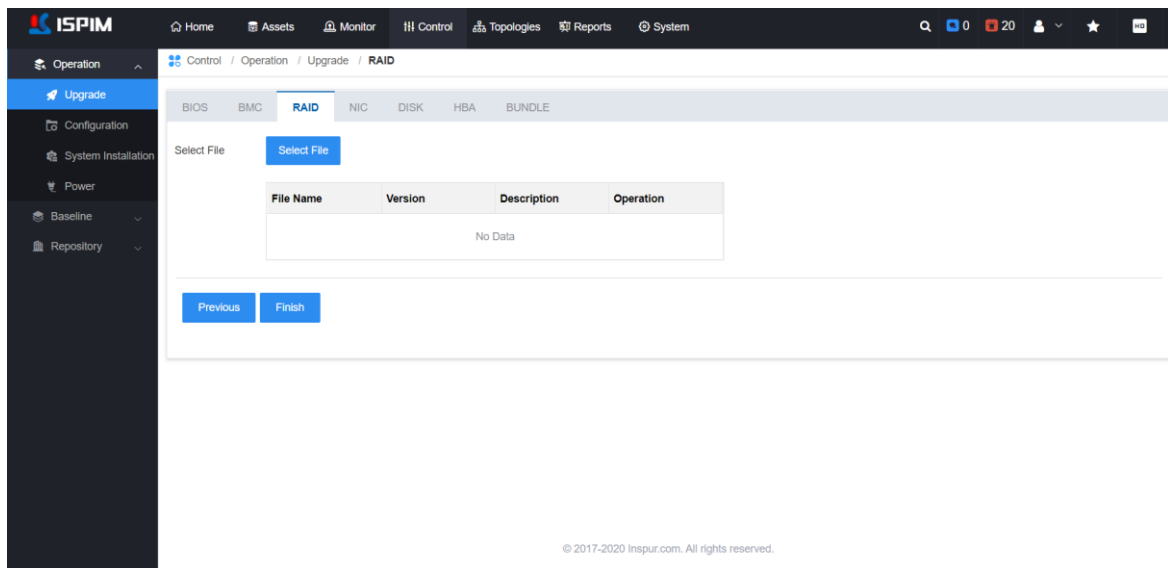
## 1. Single Firmware Upgrade

The upgrade operations of RAID, NIC, DISK, and HBA are similar. This chapter takes RAID upgrade as an example to introduce the single firmware upgrade process.

### Procedure

**Step 1 Enter the RAID upgrade page.** Click [Control] -> [Operation] -> [Upgrade] to enter the firmware upgrade page, select the "RAID" tab, and user will enter the RAID firmware upgrade page.


**Step 2 Select the devices to be upgraded.** In the device list, check the devices to be upgraded, and then click the <Start> button to enter the RAID upgrade configuration page, as shown in the figure below.



**Step 3 Select the mirror file.** Click the <Select File> button, in the file list that pops up on the right, select the mirror file, and click the <Add> button. Please note that the upgrade file must have been uploaded to the ISPIM repository.

**Step 4 Start the upgrade task.** Click the <Finish> button to complete the creation of the RAID upgrade task.

**Step 5 Check the execution of the upgrade task.** There are two ways:

- Method 1: Click [System] -> [Task], user can enter the task center to view the details of each task in the ISPIM platform, including: task name, type, status, start time, completion time and other information. Click the task name, user can also view the execution of the subtasks of the nodes in the job.
- Method 2: In the top navigation bar of ISPIM, click the  icon to view the task list information that is running in the system, including task name, status, progress and other information.

----End

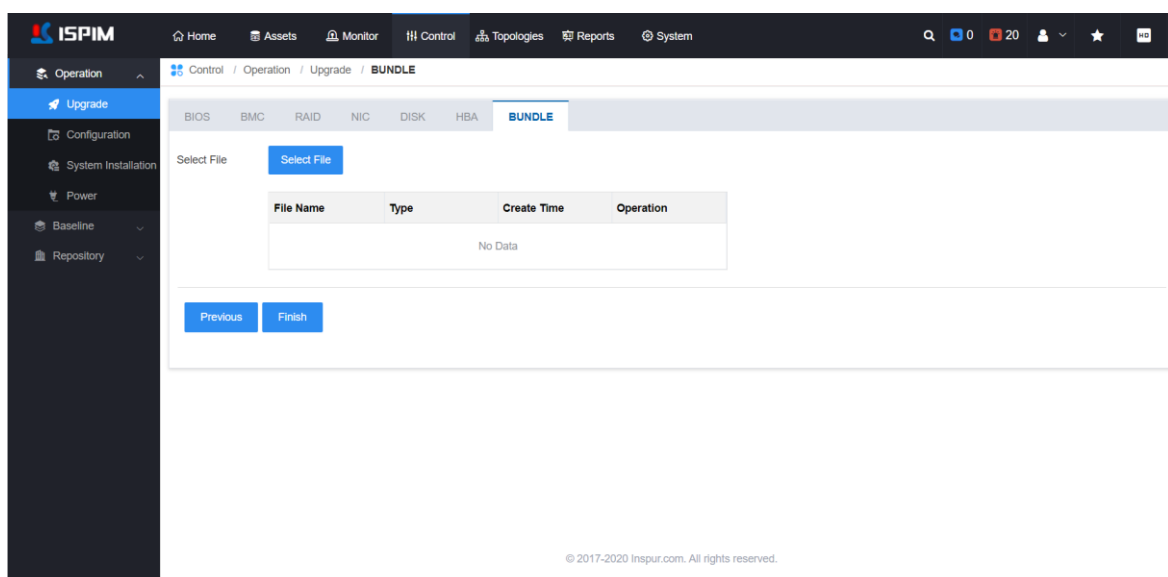
## 2. BUNDLE Upgrade

Through the BUNDLE upgrade function, one-click unified upgrade of BIOS, BMC, RAID, NIC, DISK and HBA firmware can be achieved.

### Procedure

**Step 1 Enter the upgrade page.** Click [Control] -> [Operation] -> [Upgrade], user can enter the firmware upgrade page, select the "BUNDLE" tab, and user will enter the BUNDLE firmware upgrade page.

**Step 2 Select the devices.** In the device list, tick the devices that needs to be upgraded, and click the <Start> button to enter the BUNDLE upgrade page, as shown in the figure below.






**Step 3 Bundle file settings.** Click the <Select File> button, in the file list that pops up on the right, select the bundle file, and click the <Add> button to select the corresponding upgrade file.

- The files in the file list that pops up on the right are: repository bundle packages filtered according to the selected model.
- With the mouse hovering over a file name, user can view the firmware type in the bundle file, and click the expansion icon to view the detailed information of each bundle file.

**Step 4 Start the upgrade task.** Click the <Finish> button to complete the creation of the bundle upgrade task.

**Step 5** Check the execution of the upgrade task. There are two ways:

- Method 1: Click [System] -> [Task], user can enter the task center to view the details of each task in the ISPIM platform, including: task name, type, status, start time, completion time and other information. Click the task name, user can also view the execution of the subtasks of the nodes in the job.
- Method 2: In the top navigation bar of ISPIM, click the  icon to view the task list information that is running in the system, including task name, status, progress and other information.

---End

## 8.2.4 Check After Upgrade

After the firmware upgrade is completed, it is recommended to check whether each firmware has been upgraded successfully. Different firmware has different checking methods:

- For BMC/BIOS: After the upgrade is complete, user can log in to the BMC WebUI interface of the device, and check whether the BMC and BIOS versions have been updated on the home page (the BIOS version changing may need more time before the system restart). User can also enter the asset details page, check whether the BMC and BIOS versions have been updated.
- For RAID, NIC, DISK, HBA type firmware upgrades, user can log in to the operating system to check them.

## 8.3 Firmware Configure

ISPIM supports batch firmware configuration for Inspur servers, and the configuration method is based on the BMC out-of-band management network.


### 8.3.1 BIOS Configure

ISPIM supports BIOS configuration operation.

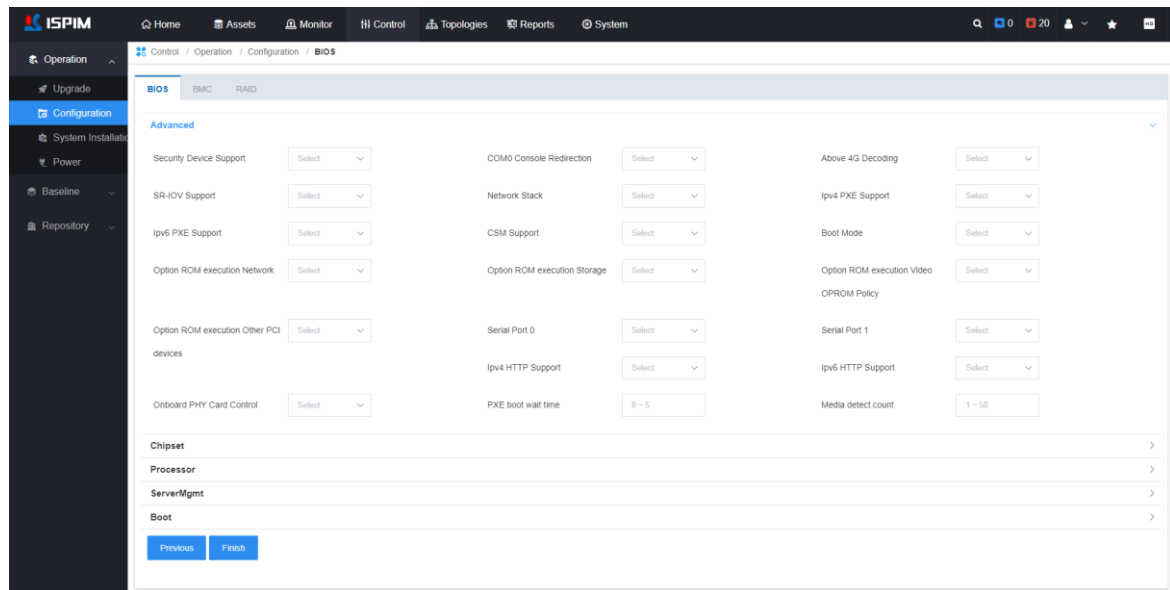
#### Procedure

**Step 1 Enter the BIOS configuration page.** Click [Control] -> [Operation] -> [Configuration] to enter the firmware configuration page, and select the "BIOS" tab to enter the BIOS configuration page.

**Step 2 Select the device to be configured.** In the device list, user can check the devices to be configured in batches.


- Model requirements: Each BIOS batch configuration tasks can only contains the same server model. User can use the search function at the top left of the list to filter devices of the same model.
- Supported models: Hover the mouse over the  icon at the top of the list to view the device models supported by the BIOS configuration.

**Step 3 Select configuration items.** After the device selection is complete, click the <Start> button at the top right of the list, and user will enter the BIOS configuration items page, as shown in the figure below. User can choose to set the items related to Advanced, Chipset, Processor, Server Management and Boot and other categories.



**Step 4 Configure each item value.** Configure the parameters of the selected items. After the configuration is complete, click the <Finish> button to start the BIOS configuration task.

**Step 5 Check the execution status of the task.**

- Method 1: Click [System] -> [Task], user can enter the task center to view the details of each task in the ISPM platform, including: task name, type, status, start time, completion time and other information. Click the task name, user can also view the execution of the subtasks of the nodes in the job.
- Method 2: In the top navigation bar of ISPM, click the  icon to view the task list information that is running in the system, including task name, status, progress and other information.

---End

## 8.3.2 BMC Configure


ISPM supports BIOS configuration operation.

### Procedure

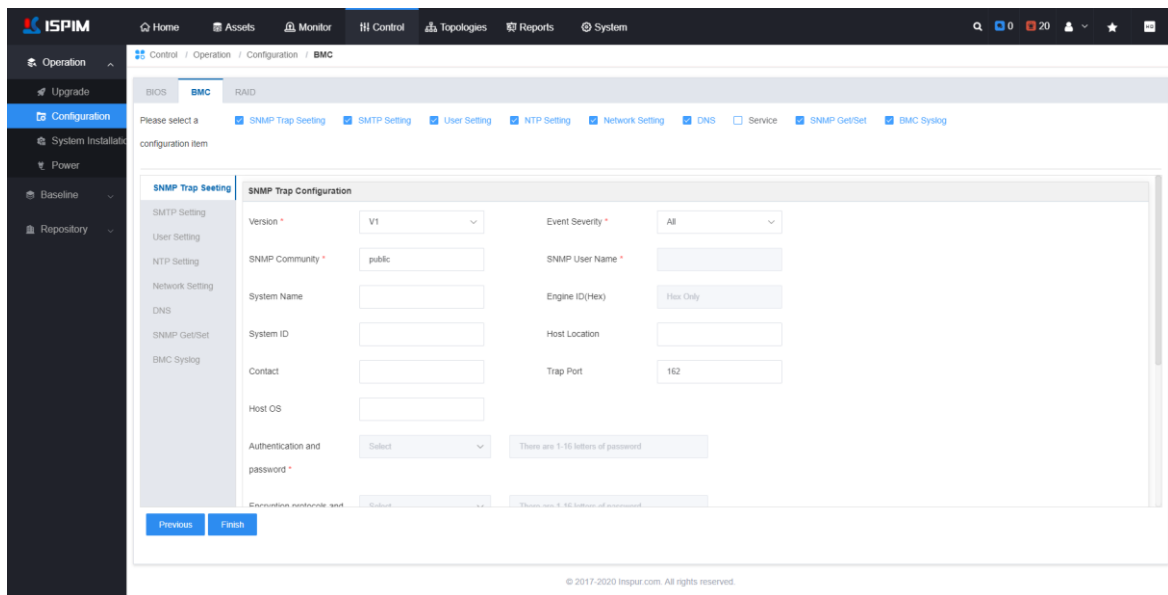
**Step 1 Enter the BMC configuration page.** Click [Control] -> [Operation] -> [Configuration] to enter the firmware configuration page, select the "BMC" tab, and user

will enter the BMC configuration page.

**Step 2 Select the device to be configured.** In the device list, user can check the devices to be configured in batches.

- Server model requirements: BMC batch configure tasks only support the same server model. User can use the advanced query function at the top left of the list to filter the devices of the same model.
- Supported models: hover the mouse over the  icon at the top of the list to view the device models supported by the BMC configure.


**Step 3 Select the configuration items.** After the devices are selected, click the <Start> button at the top right of the list, and user will enter the BMC configuration items page, as shown in the figure below. User can select setting items related to SNMP, SMTP, user, NTP, network, DNS, service, etc.



**Step 4 Configure each parameter item.** Set value of the selected items. After the configuration is completed, click the <Finish> button to start the BMC configuration task.

**Step 5 Check the execution status of the task.**

- Method 1: Click [System] -> [Task], user can enter the task center to view the details of each task in the ISPM platform, including: task name, type, status, start time, completion time and other information. Click the task name, user can also view the execution of the subtasks of the nodes in the job.

- Method 2: In the top navigation bar of ISPIM, click the  icon to view the task list information that is running in the system, including task name, status, progress and other information.

---End

### 8.3.3 RAID Configure

ISPIM supports the use of out-of-band or in-band configuration of RAID, which can flexibly meet the needs of users.

- Out-of-band mode: Configure the RAID card through the device BMC out-of-band HTTP management interface.
- In-band mode: Boot the operating system in the memory through the BMC, use the command line tool of the RAID manufacturer to realize the raid configuration
- In-band TF: Through the TF card on the server, execute the configuration script to complete the RAID configuration.


#### 1. Requirements

When performing RAID configuration in batches, user needs to specify a device as a template. ISPIM will read the configuration information of this device, construct corresponding configuration parameters, and apply them to other devices. Therefore, when configuring batches, the RAID and hard disk specifications of all devices must be the same. Otherwise, please configure in batches.

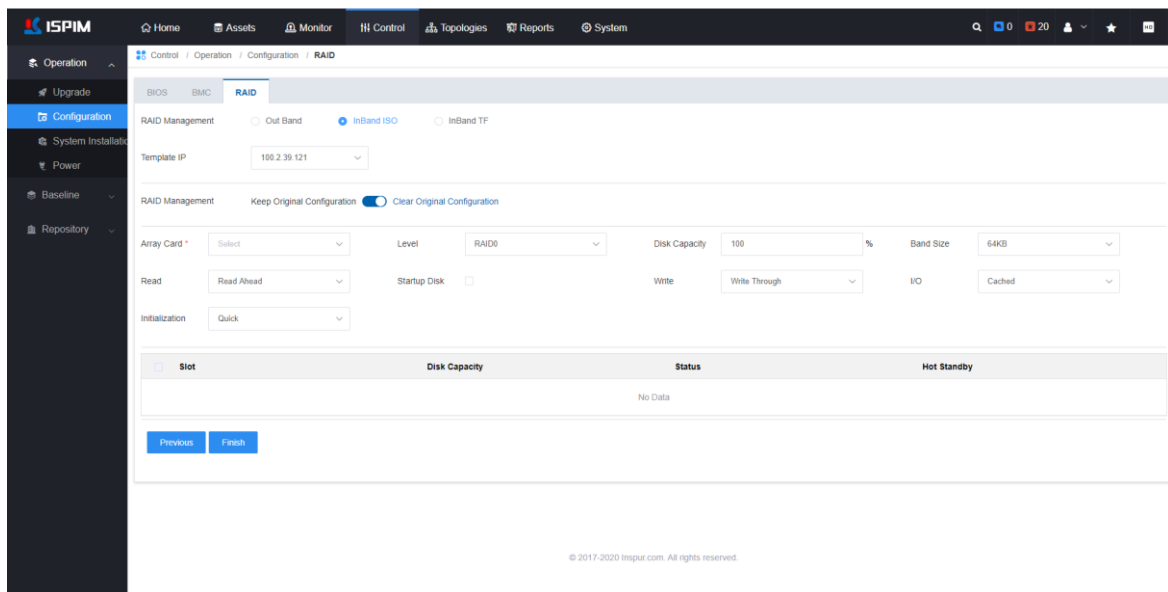
#### 2. Procedure

**Step 1 Enter the RAID configuration page.** Click [Control] -> [Operation] -> [Configuration] to enter the firmware configuration page, select the "RAID" tab, and user will enter the BMC configuration page.

**Step 2 Select the device to be configured.** In the device list, user can check the devices to be configured in batches.

- Server model requirements: RAID batch configure tasks only support the same server model. User can use the advanced query function at the top left of the list to filter the devices of the same model.
- Supported models: hover the mouse over the  icon at the top of the list to view the device models supported by the RAID batch configure.


**Step 3 Configure each parameter item.** After the devices are selected, click the <Start> button at the top right of the list, and user will enter the RAID configuration selection page, as shown in the figure below.



- RAID Management: Choose the method to configure RAID, which includes out-of-band, in-band OS, in-band TF.
- Template device IP: User can drop down to select the template device IP. The system will read the controller information and hard disk information of this device, and determine that the hard disk configuration of other devices is the same as this device.
- RAID Configuration: User can choose to keep the original configuration or clear the original configuration.

After the above parameter configuration is completed, click the <Finish> button to start the RAID configuration task.

**Step 5 Check the execution status of the task.**

- Method 1: Click [System] -> [Task], user can enter the task center to view the details of each task in the ISPIM platform, including: task name, type, status, start time, completion time and other information. Click the task name, user can also view the execution of the subtasks of the nodes in the job.
- Method 2: In the top navigation bar of ISPIM, click the  icon to view the task list information that is running in the system, including task name, status, progress and other information.


----End



## 8.4 Power Management

ISPIM supports single or batch power operations on the equipment, such as power on, power off, soft power off, restart.

### Procedure

**Step 1** Click [Control] -> [Operation] -> [Power] to enter the power management page.

**Step 2** In the device list, the "Status" column displays the current power status of the device. Click the  icon corresponding to a device to refresh the power status.

**Step 3** In the device list, click the  or  icon corresponding to a device to perform power-on/off operations on a single device. To perform power operations in batches, please select multiple devices and click <Power on>, <Power off>, <Soft shutdown> or <Restart> button at the top of the list.

----End

## 8.5 OS Deployment

### 8.5.1 Requirements

Before performing the operating system installation, pay attention to the following items:

- **Server model and configuration requirements:** Currently, only Inspur M5 series servers are supported, and the disk configuration of batch operation nodes must be consistent.

[Note] The installation of the operating system will format the disk, please make a data backup

in advance!

- **Repository management:** Before deploying the operating system, user needs to upload the operating system image in advance in Repository->OS.
- **OS type and version:** The supported OS types and versions are described in Table 8-1.

Table 8-1 OS type and version description

OS Type	Version
RedHat	RHEL7U3, RHEL7U4, RHEL7U5
VMware	ESXi6.0, ESXi6.5, ESXi6.7
CentOS	CentOS7U3, CentOS7U4, CentOS7U5

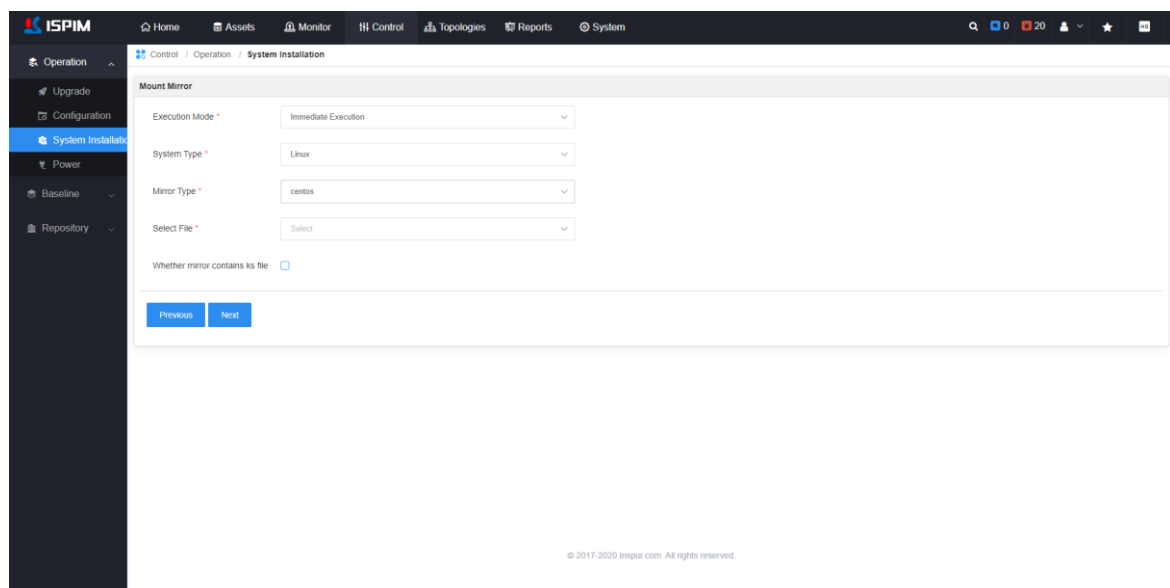
## 8.5.2 OS Deployment

After the prerequisites for installing the OS, user can start to install the operating system.

### Procedure

**Step 1** Click [Control] -> [Operation] -> [System Installation] to enter the system installation page. In the device list, check the devices to be deployed with the OS.

**Step 2** Click the <Start> button above the list, and user will enter the OS mirror file page, as shown in the figure below.



**Step 3** Configure the parameters of the OS installation task:



- The image contains the KS file: If the image contains the KS file, ISPIM will perform various configurations in the deployment process according to its KS file. It is suitable for scenarios where the KS file of the image has been edited.
- The image does not contain the KS file: If user chooses not to include the KS file, user can configure the relevant parameters of the system deployment in the subsequent steps, including: password, language, disk partition, IP, host name. ISPIM will automatically generate the KS file control according to its configuration in deployment process.

【NOTE】 Some models may have the problem of IP configuration failure. The common reason is that the image file lacks the driver of the device network card. When this problem occurs, please contact the hardware engineer of the corresponding device.

**Step 4** If the image contains the KS file, just click the <Finish> button, without the following steps. If the image does not contain the KS file, user needs to click <Next> to configure the system, and then click the <Finish> button.

**Step 5** After the operating system deployment task starts, user can click [System] -> [Task] to enter the task management page and view the task execution details, including: name, type, status, start time, completion time, etc.

---End

## 8.6 Baseline Management

### 1. Feature Introduction

The ISPIM platform provides a unified baseline management function, including two parts: baseline template and baseline strategy:

- **Baseline template:** The baseline template contains information such as the firmware version and firmware configuration for the Inspur server. Through the baseline template, the optimal configuration of a specific type of Inspur server can be set as the baseline template. It provides a basis for subsequent automatic correction.
- **Baseline strategy:** Through the baseline strategy, devices that deviate from the baseline

template can be processed, for example: whether to automatically update the firmware according to the baseline template, and whether to generate an alarm that deviates from the baseline.

**NOTE**

The baseline management module will periodically collect the firmware version, firmware configuration information of each server, and compare the collected information to the baseline template. For devices that deviate from the baseline, ISPIM will automatically perform the baseline calibration operation.

---

## 2. Science

Different types of equipment have the optimal firmware version and parameter configuration to meet different business needs. During the operation of the equipment, its configuration may be artificially modified or may be changed due to firmware upgrades. Using the baseline management function, automatic baseline comparison, baseline warning and automatic calibration can be achieved.

### 8.6.1 Baseline Template

The role of the baseline template is as follows:

- The baseline template can provide a firmware configuration basis for automatic correction.
- Users can set the optimal configuration of a certain model of Inspur server as a template.

#### 1. Add Baseline Template

Users can add baseline templates as needed.

---

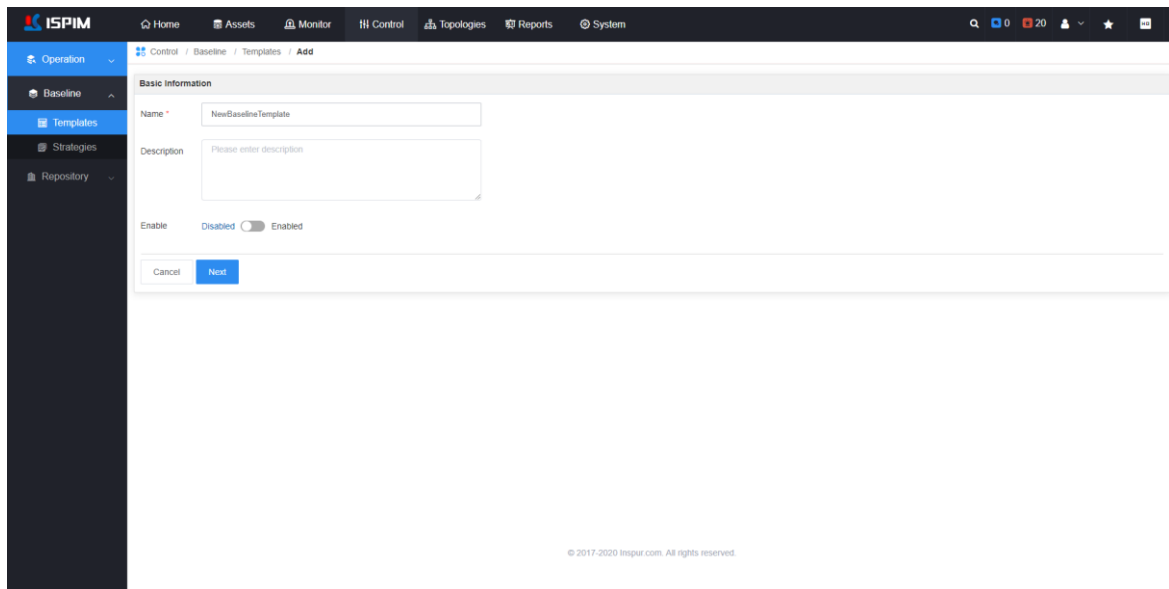
**NOTE**

- Before configuring the baseline template, user needs to upload the firmware files of BMC and BIOS on the Repository -> Firmware page in advance.
  - The baseline template can contain both the BMC and BIOS baselines.
-

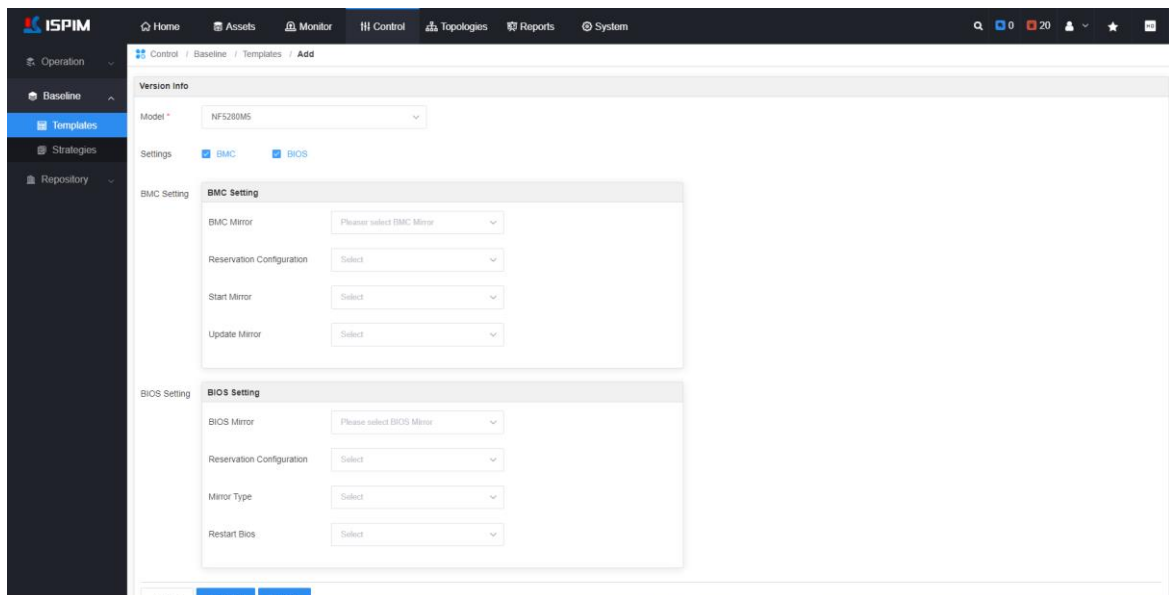
## Procedure

**Step 1** Click [Control] -> [Baseline] -> [Template] to enter the baseline template page.

**Step 2** Click the <Add> button in the upper right corner of the page to enter the add baseline template page, as shown in the figure below.



**Step 3** Set the parameters such as template name, description, enable status, etc., click <Next> to enter the template configuration page, as shown in the figure below.



**Step 4** Set the server related firmware settings of BMC and BIOS.

**Step 5** Click the <Submit> button to complete the creation of the baseline template.

---End



## 2. Baseline Template Operation


The baseline template can be enabled, disabled or deleted.

### Procedure

**Step 1** Click [Control] -> [Baseline] -> [Template] to enter the baseline template page.

**Step 2** In the baseline template list, click the name of a baseline template to view the details of the baseline template.

**Step 3** In the baseline template list, click the  or  icon corresponding to a baseline template to enable/disable the baseline template.

**Step 4** In the list of baseline templates, click the  icon corresponding to a baseline template to modify the baseline template.

**Step 5** In the baseline template list, click the <Delete> button of a template to delete the template. To delete templates in batches, click the <Delete> button above the list after checking multiple templates.

--End

## 8.6.2 Baseline Strategy

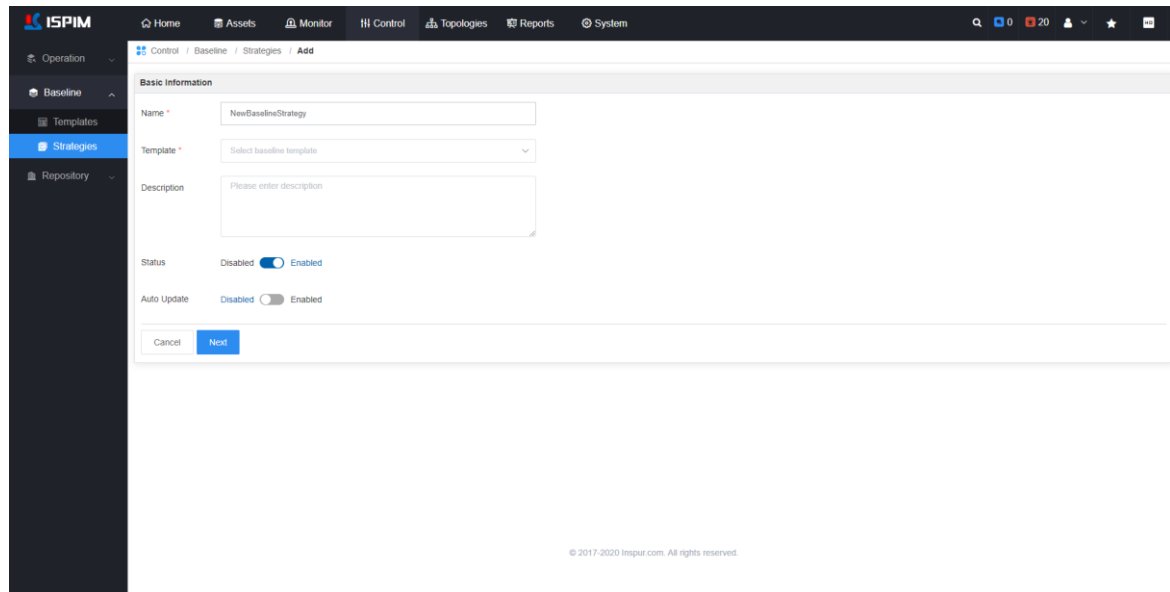
The baseline strategy can deal with devices that deviate from the baseline, such as whether to update the firmware according to the baseline template, and whether to generate corresponding alarms.

### 7.6.2.1 Add Baseline Strategy

#### Procedure

**Step 1** Click [Control] -> [Baseline] -> [Strategy] to enter the baseline strategy page.

**Step 2** Click the <Add> button in the upper right corner of the page to enter the “Add Baseline Strategy” page, as shown in the figure below



**Step 3** Set the parameters of the baseline strategy. Among them: "Auto Update" means whether to automatically trigger the alignment operation when the configuration of the associated device is inconsistent with the baseline strategy. **It is recommended that users choose this operation carefully. So as not to affect the normal operation of the business.**

**Step 4** After the parameter configuration is completed, click <Next> to enter the select nodes page. Click the <Add Node> button, select the devices associated with the baseline policy in the right slide bar, and click <Submit > button to complete the creation of the strategy.


---End



## 7.6.2.2 Baseline Strategy Operation


### Procedure

**Step 1** Click [Control] -> [Baseline] -> [Strategy] to enter the baseline strategy page.

**Step 2** In the baseline strategy list, click the name of a baseline strategy to view the details of the baseline strategy.

**Step 3** In the baseline strategy list, click the  icon in the operation field to edit the baseline strategy.

**Step 4** In the baseline strategy list, click the  or  icon to enable/disable the baseline strategy.

**Step 5** In the baseline strategy list, click the  icon of a baseline strategy operation column to delete the baseline strategy. Click the <Delete> button at the upper right of the list can do batch deletion after selecting multiple baseline strategies.

---End

# 9 Topology Management

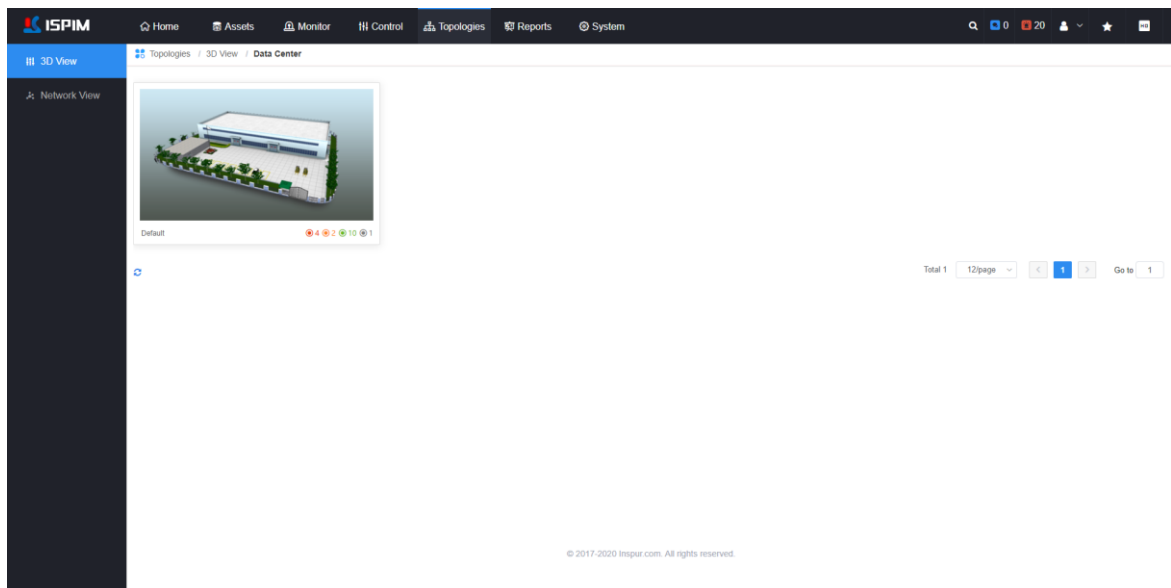
In the navigation bar at the top of ISPIM, select the "Topologies" tab, user will enter the topology management page. The topology management module includes two parts: network topology and 3D view.

## 9.1 View Data Center Topo

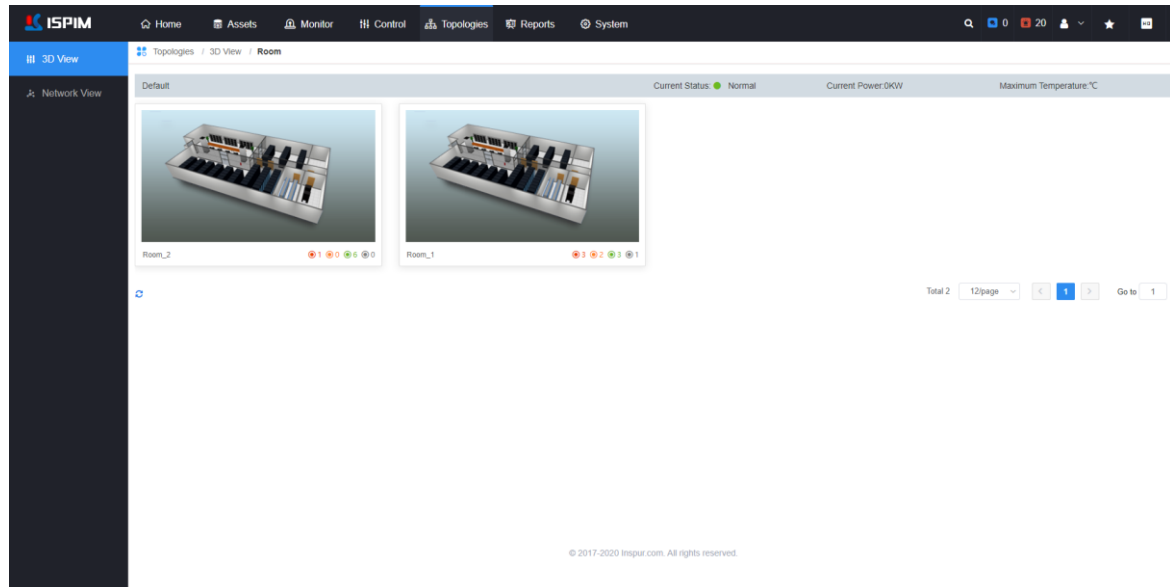
In the topology management module, user can view the data center topology details.

### Procedure

**Step 1** In the top navigation bar of ISPIM, select the "Topologies" tab to enter the data center page. As shown in the figure below. In the lower right corner of each data center diagram, user can view the status statistics of each data center device, including: the number of critical alarm devices, the number of minor alarm devices, the number of normal devices and the number of offline devices.



**Step 2** Click a data center icon, user can enter the room page, view the data center's room list, as shown in the figure below. In the upper right corner of the room page, user can also view the current data center operating status, power consumption and maximum temperature and other information.



---End

## 9.2 3D Room Management

ISPIM provides a 3D view of the data center. Users can build a data center model to achieve efficient operation and maintenance of the data center. On the 3D view page, user can view and edit 3D room information.

### Procedure

**Step 1** In the navigation bar at the top of ISPIM, select the "Topologies" tab to enter the data center page.

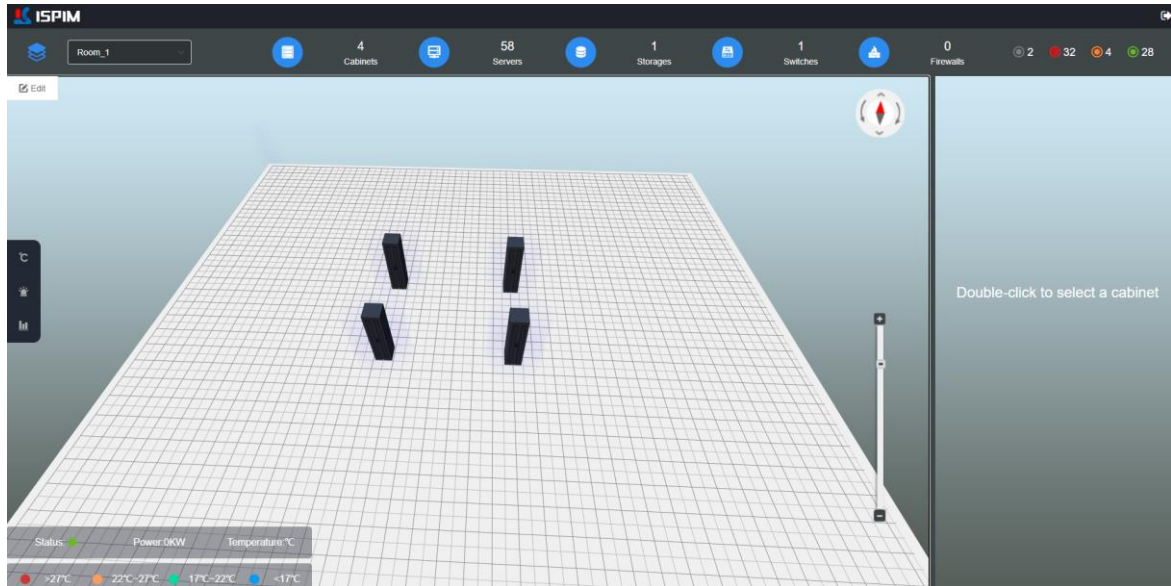
**Step 2** Click the icon of a data center to enter the room list of the data centers.

**Step 3** Click the icon of a room, user will enter the 3D view page of the room, as shown in the figure below.

- **Edit the room layout:** When user enters the 3D room page for the first time, the cabinets layout in the room is empty, and user needs to manually edit the room layout.
- **Switch room:** In the drop-down selection box in the upper left corner of the page, user can choose to switch between different rooms under the data center.
- **View statistics of the room:** At the top of the page, user can view information about the equipment and alarms in the room.



- **Zoom/rotate the 3D view:** Use the mouse wheel to zoom the 3D room view. Press the left mouse button, user can also rotate the room angle. Click the compass icon in the upper right corner of the room to restore to the original 3D view.



----End


## 9.2.1 Edit Room Layout



User can edit the 3D room layout.

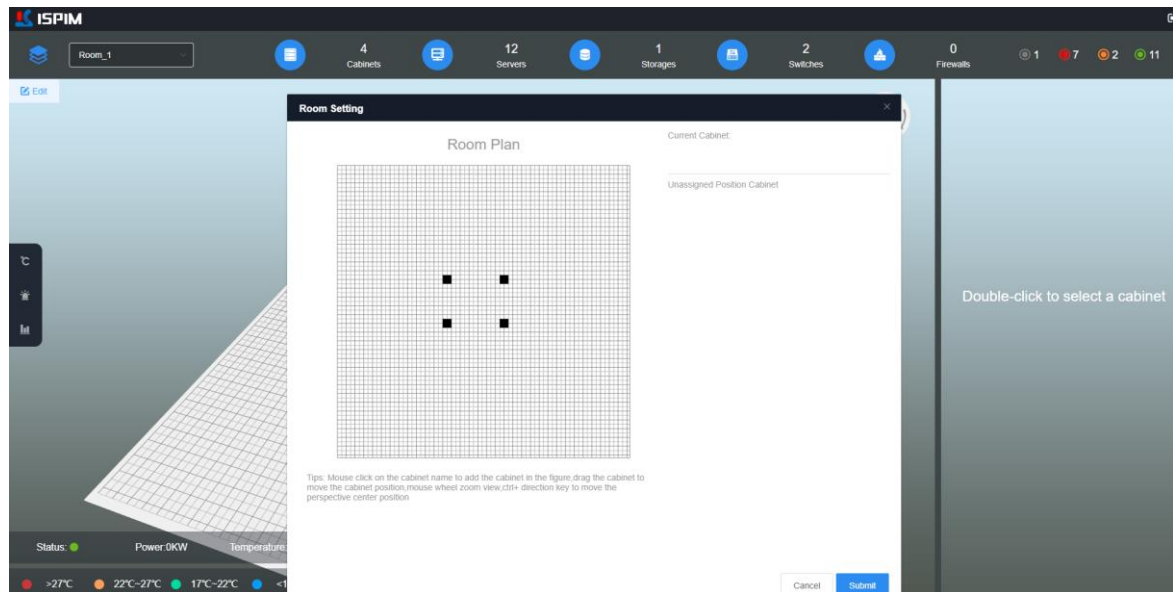
### Procedure

**Step 1** In the navigation bar at the top of ISPIM, select the "Topologies" tab to enter the data center page.

**Step 2** Click a data center icon to enter the room list page of a data center.

**Step 3** Click the  icon in the upper left corner of the 3D room, and the room settings window will pop up. As shown below:

- The cabinets with unallocated locations in the room will be displayed in the right list. Click the unassigned cabinets, and the cabinet will be added to the upper left corner of the room panel and displayed as an  icon.
- Press the left mouse button to drag the cabinet  icon to move the position, or drag the cabinet to the unallocated area on the right.



**Step 2** After editing the cabinet layout, click the <Submit> button, the room layout will be saved, and the page will automatically refresh and load.

----End

## 9.2.2 View Room Information

### 1. Room Temperature View


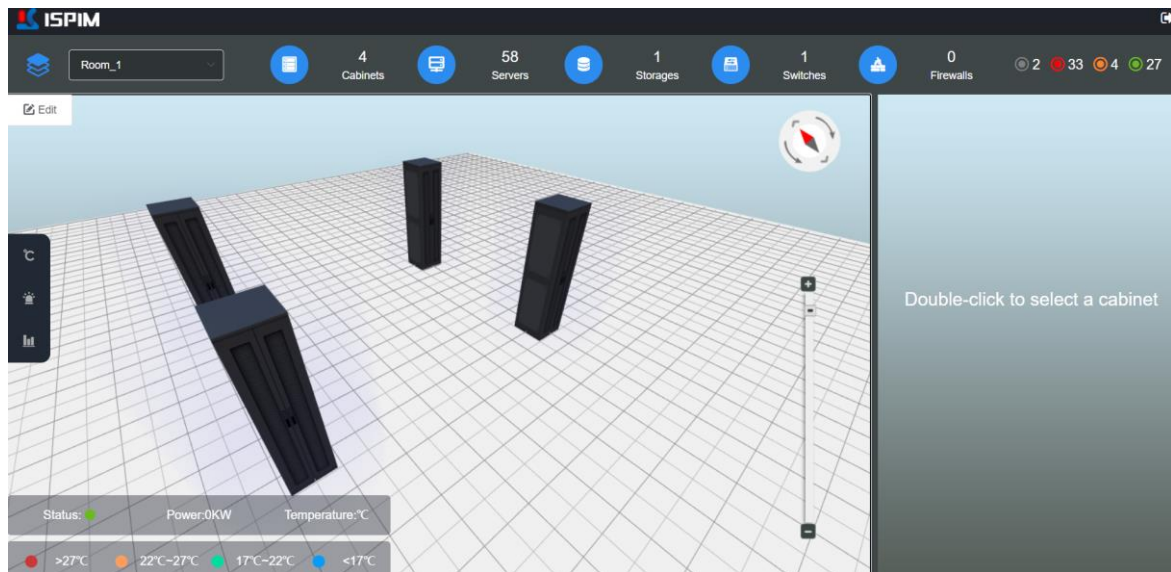
Click the  icon on the left side of the 3D room to view the temperature distribution of the cabinets in the room, which is convenient for users to adjust the cooling of the room, as shown in Figure 9-1. The division of the temperature range of the room will be displayed in the lower left corner of the view.

Figure 9-1 Room Temperature View



## 2. Room Alarm View


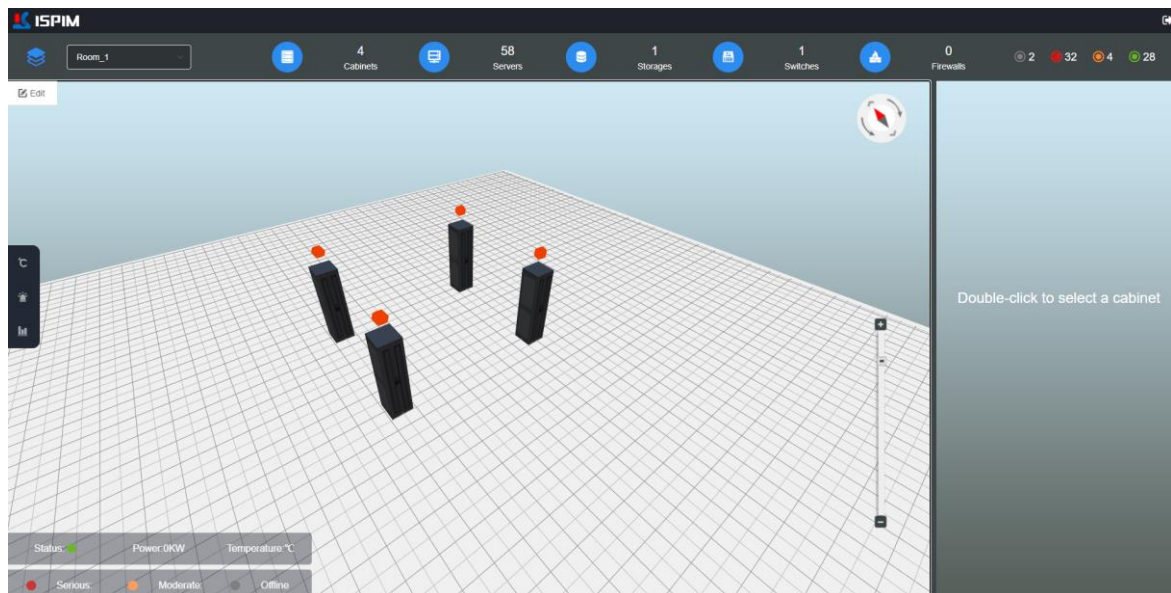
Click the  icon on the left side of the 3D room to view the alarm distribution of the cabinets, as shown in Figure 9-2. In the lower left corner of the view, user can view the alarm identification information, including: serious, moderate, offline.

Figure 9-2 Room Alarm View



### 3. Room Power Consumption View


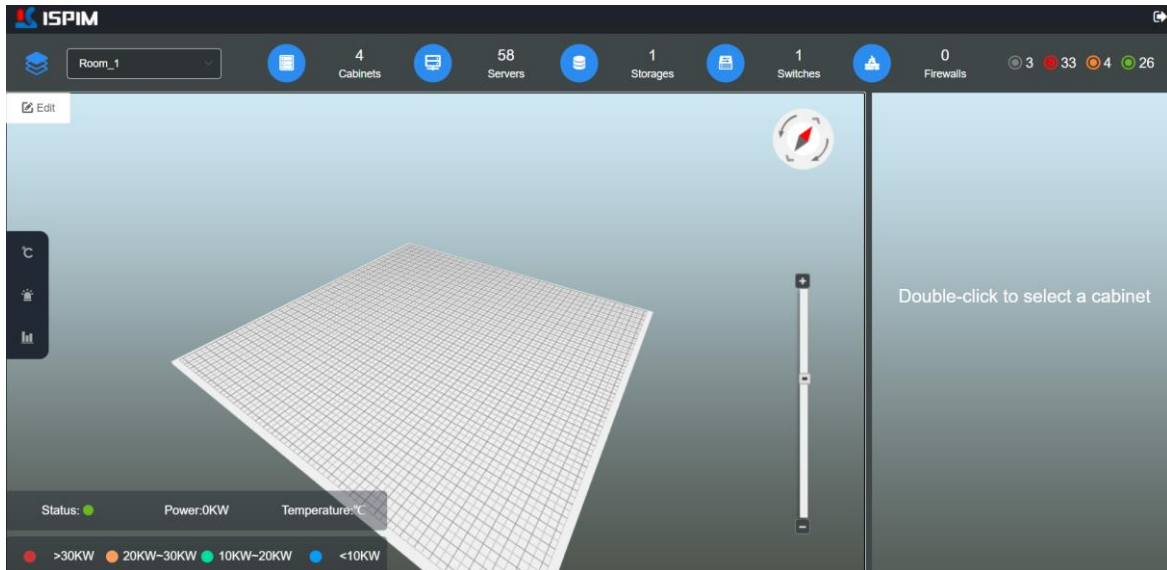
Click the  icon on the left side of the 3D room to view the power consumption distribution of the cabinets, as shown in Figure 9-3, the division of power consumption intervals will be displayed in the lower left corner of the view.

Figure 9-3 Room Power Consumption View

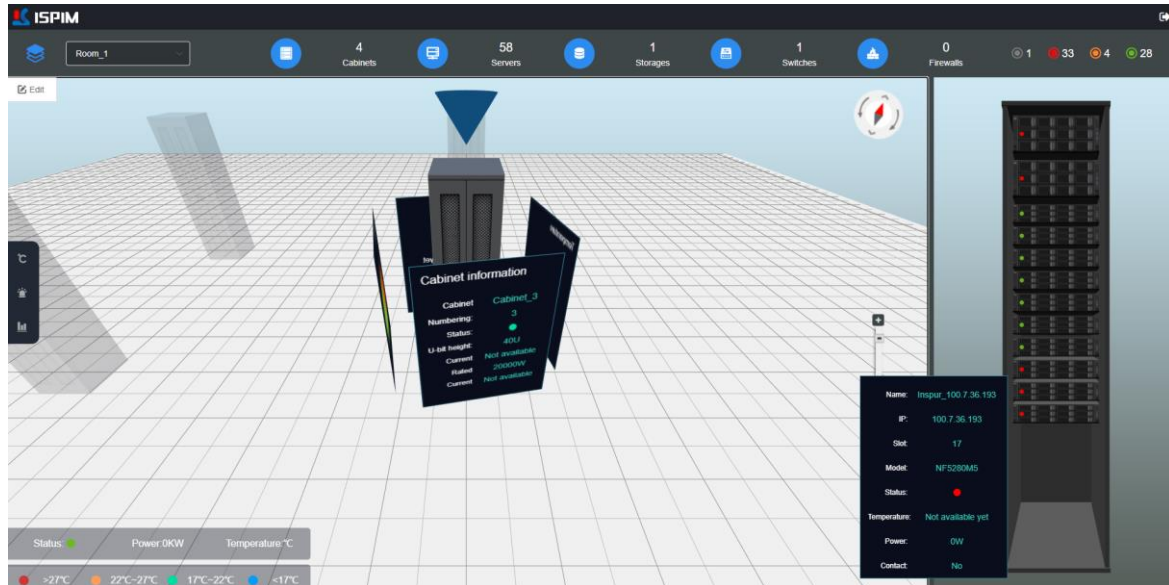


#### 9.2.3 View Cabinet Detail

Double-click the cabinet in the room to view the detailed information of the cabinet, as shown in Figure 9-4.

- The four panels around the cabinet respectively display the cabinet details: status, power consumption, and temperature information.
- Hover the mouse on a device in the cabinet on the right to view the detailed information of the device.

Figure 9-4 Cabinet Detail Page

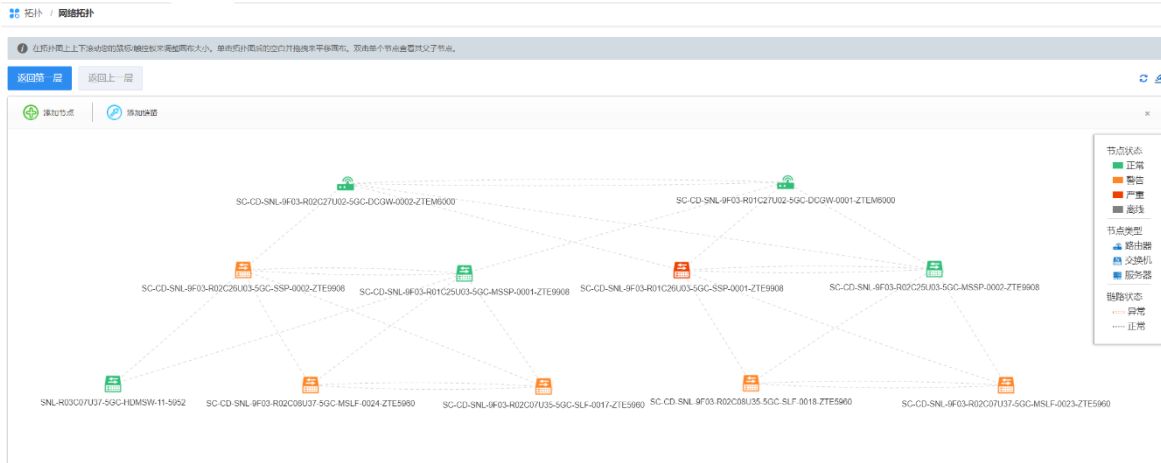


## 9.3 Network Topology

In the top navigation bar of ISPIM, select the "Topologies" tab to enter the topo page. In the navigation tree on the left side of the data center page, select [Network View] to enter the network topology page, as shown in Figure 9-5. User can perform operations such as adding nodes, adding links, and regenerating topology.

- Automatic topology generation: The physical link network topology can be automatically generated according to the physical links of the devices currently managed by ISPIM.
- Manual topology drawing: User can manually draw the network topology as needed.
- Modify network topology: Support to modify the physical connection relationships of the devices.

Figure 9-5 Network Topology

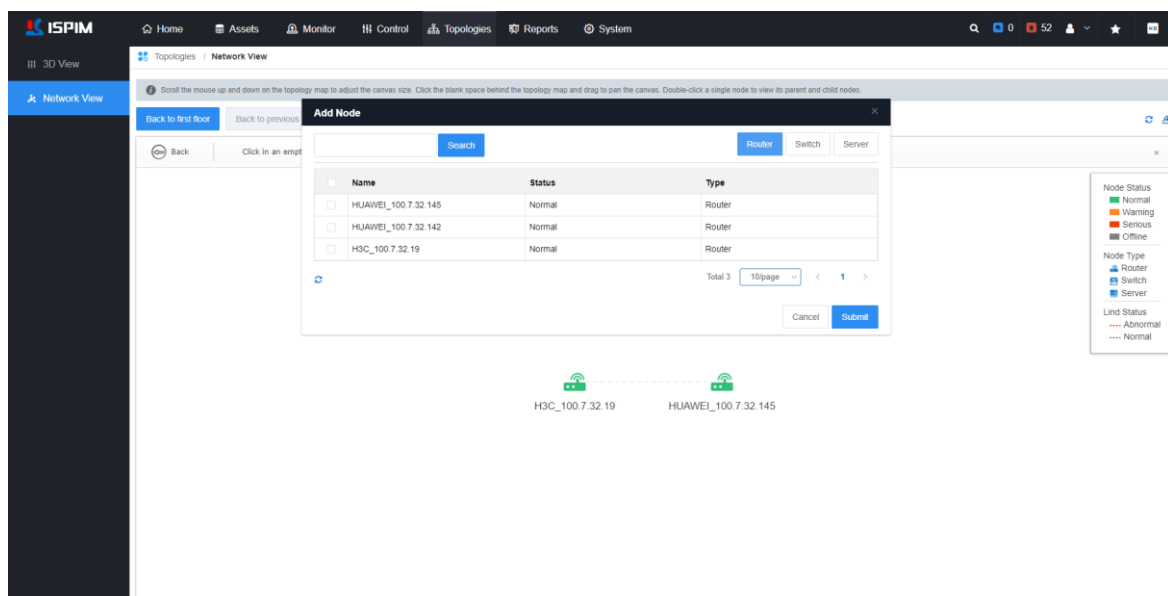


## 1. Add Node

User can add nodes to the network topology.

### Procedure

**Step 1** In the network topology page, after clicking the <Add Node> button in the topology panel, click any blank space, the “Add Node window” will pop up , as shown in the figure below.



**Step 2** In the add node window, click "router", "switch" or "server" as needed to select the added node devices (user can select "router", "switch" or "server" multiple devices at the same time). After the selection, click “Submit” to add the selected device to the topology panel.

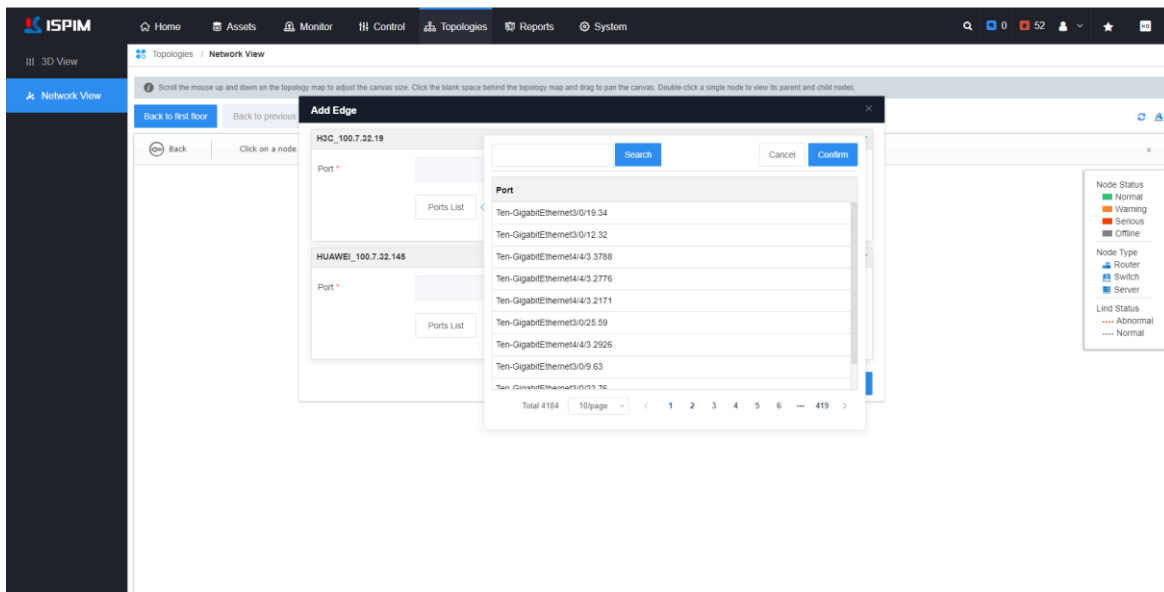
--End

## 2. Add Link

User can edit links between devices

### Procedure

**Step 1** On the network topology page, after clicking the <Add Edge> button in the topology, click a node device and drag the mouse to another node, a window for adding a link will pop up, as shown in the figure below.





**Step 2** In the adding link window, configure the device port type, port name, port MAC and other information according to the page prompts.

**Step 3** After the configuration is completed, click the <Submit> button to establish a link connection between the devices.

--End


### NOTE

Click a link connection line, and the functions of editing link and deleting link will appear:


- Click the  icon, according to the page prompt, user can modify the link nodes info.
- Click the  icon and confirm in the pop-up window to delete a link.



### 3. Regenerate Topology

Click the  icon to redraw the topology.

### 4. Refresh Topology

Click the  icon to manually refresh the network topology, the system will automatically render the current network topology.



#### NOTE

The outer layer of the network topology displays the topology diagram of the switches and routers. Double-click a switch or router to enter the next layer and view the specific nodes and link status connected to the switch or router.

---

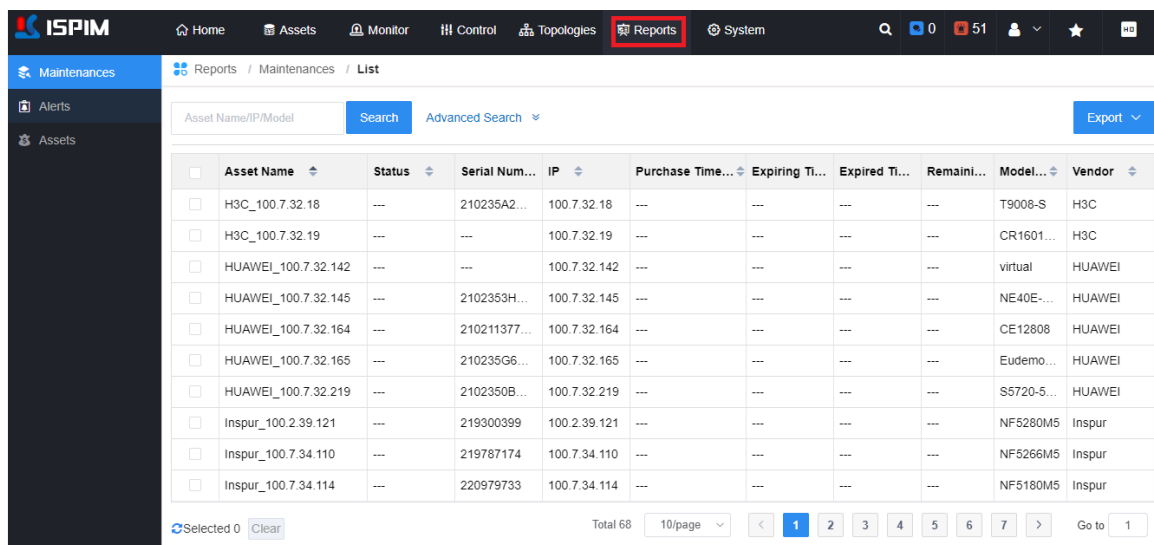


# 10 Reports Management

Click the "Reports" tab in the top navigation bar of ISPIM to enter the reports management module. As shown in Figure 10-1. Report management includes three parts: maintenances management, alarms management and assets management.

The report management module provides functions such as automated asset export, asset inventory, and asset visualization. ISPIM connects to the SR cabinet management RMC through the REST interface to realize intelligent asset management, improve management efficiency, and reduce management costs.

Figure 10-1 Reports Management



	Asset Name	Status	Serial Num...	IP	Purchase Time...	Expiring Ti...	Expired Ti...	Remains...	Model...	Vendor
<input type="checkbox"/>	H3C_100.7.32.18	---	210235A2...	100.7.32.18	---	---	---	---	T9008-S	H3C
<input type="checkbox"/>	H3C_100.7.32.19	---	---	100.7.32.19	---	---	---	---	CR1601...	H3C
<input type="checkbox"/>	HUAWEI_100.7.32.142	---	---	100.7.32.142	---	---	---	---	virtual	HUAWEI
<input type="checkbox"/>	HUAWEI_100.7.32.145	---	2102353H...	100.7.32.145	---	---	---	---	NE40E-...	HUAWEI
<input type="checkbox"/>	HUAWEI_100.7.32.164	---	210211377...	100.7.32.164	---	---	---	---	CE12808	HUAWEI
<input type="checkbox"/>	HUAWEI_100.7.32.165	---	210235G6...	100.7.32.165	---	---	---	---	Eudemo...	HUAWEI
<input type="checkbox"/>	HUAWEI_100.7.32.219	---	2102350B...	100.7.32.219	---	---	---	---	S5720-5...	HUAWEI
<input type="checkbox"/>	Inspur_100.2.39.121	---	219300399	100.2.39.121	---	---	---	---	NF5280M5	Inspur
<input type="checkbox"/>	Inspur_100.7.34.110	---	219787174	100.7.34.110	---	---	---	---	NF5266M5	Inspur
<input type="checkbox"/>	Inspur_100.7.34.114	---	220979733	100.7.34.114	---	---	---	---	NF5180M5	Inspur

## 10.1 Maintenances Management

In the navigation tree on the left side of the report management module, select [Maintenances] to enter the maintenances management page. On this page, you can view asset maintenance information, perform operations such as searching or exporting the maintenance list, which is convenient for users to manage asset maintenance information.

### Procedure

**Step 1** Click [Reports] -> [Maintenances] in turn to enter the maintenances management page, as shown in the figure below

Reports / Maintenances / List

Asset Name/IP/Model  Search [Advanced Search](#) [Export](#)

<input type="checkbox"/>	Asset Name	Status	Serial Num...	IP	Purchase Time...	Expiring Ti...	Expired Ti...	Remaini...	Model...	Vendor
<input type="checkbox"/>	Inspur_100.7.32.120	---	0	100.7.32.120	---	---	---	---	AS1300...	Inspur
<input type="checkbox"/>	Inspur_100.7.32.147	---	214623429	100.7.32.147	---	---	---	---	NF5270M3	Inspur
<input type="checkbox"/>	Inspur_100.7.32.210	---	216389594	100.7.32.210	---	---	---	---	AS13000	Inspur
<input type="checkbox"/>	Inspur_100.7.32.218	---	214623431	100.7.32.218	---	---	---	---	NF5270M3	Inspur
<input type="checkbox"/>	Inspur_100.7.32.231	---	00001	100.7.32.231	---	---	---	---	SA5248	Inspur
<input type="checkbox"/>	Inspur_100.7.32.248	---	215291206...	100.7.32.248	---	---	---	---	SN6116...	Inspur
<input type="checkbox"/>	Inspur_100.7.32.251	---	275012152	100.7.32.251	---	---	---	---	AS1300...	Inspur
<input type="checkbox"/>	Inspur_100.7.32.31	---	202003271...	100.7.32.31	---	---	---	---	NF5280M5	Inspur
<input type="checkbox"/>	Inspur_100.7.32.32	---	202003271...	100.7.32.32	---	---	---	---	NS5162...	Inspur
<input type="checkbox"/>	Inspur_100.7.32.41	---	213072056	100.7.32.41	---	---	---	---	NF5240M3	Inspur

Selected 0 [Clear](#) Total 11 10/page < 1 2 > Go to 1

**Step 2** In the search box, enter the asset name/IP/model to fuzzy query the maintenance report; click <Advanced Search>, you can also use the maintenance status, model, and remaining days to search for the maintenance report.

**Step 3** In the maintenance list, after choosing the maintenance information, click the <Export/Selected> button above the list to export the selected maintenance report; click <Export/Filtered> to export the maintenance report that meets the search criteria .

---End

## NOTE

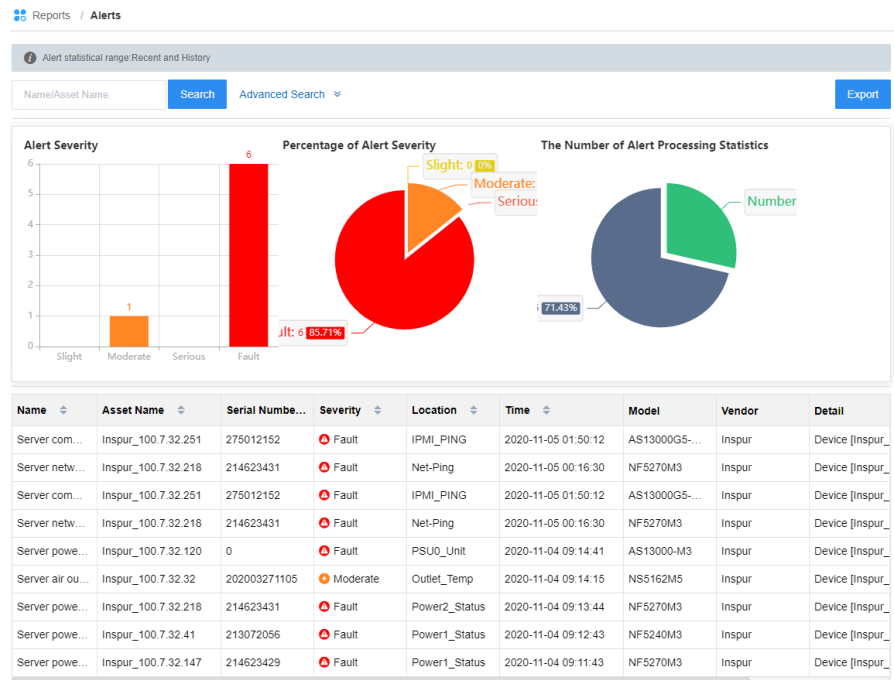
When the equipment maintenance is about to expire, ISPIM will send a maintenance expiration reminder. If necessary, you can edit the maintenance information. For details, see 7 Edit Maintenance Information.

## 10.2 Alerts Management

In the navigation tree on the left side of the report management module, select [Alerts] to enter the alert management page. On the alarm management page, you can view alarm severity, percentage of alert severity, the number of alert processing statistics, and support exporting alarm statistics information.

### Procedure

**Step 1** In the navigation tree on the left side of the report management module, select [Alerts] to enter the alarm management page. On the alarm management page, you can view alarm severity, percentage of alert severity, the number of alert processing statistics, and support exporting alarm statistics information.



**Step 2** Enter the device name or alarm source in the search box, you can fuzzy search the alarm report; click <Advanced Search>, support the use of serial number, date range and alarm level to query the alarm report.

**Step 3** Click the <Export> button above the list to export the alarm report with one click.

----End

## 10.3 Assets Management

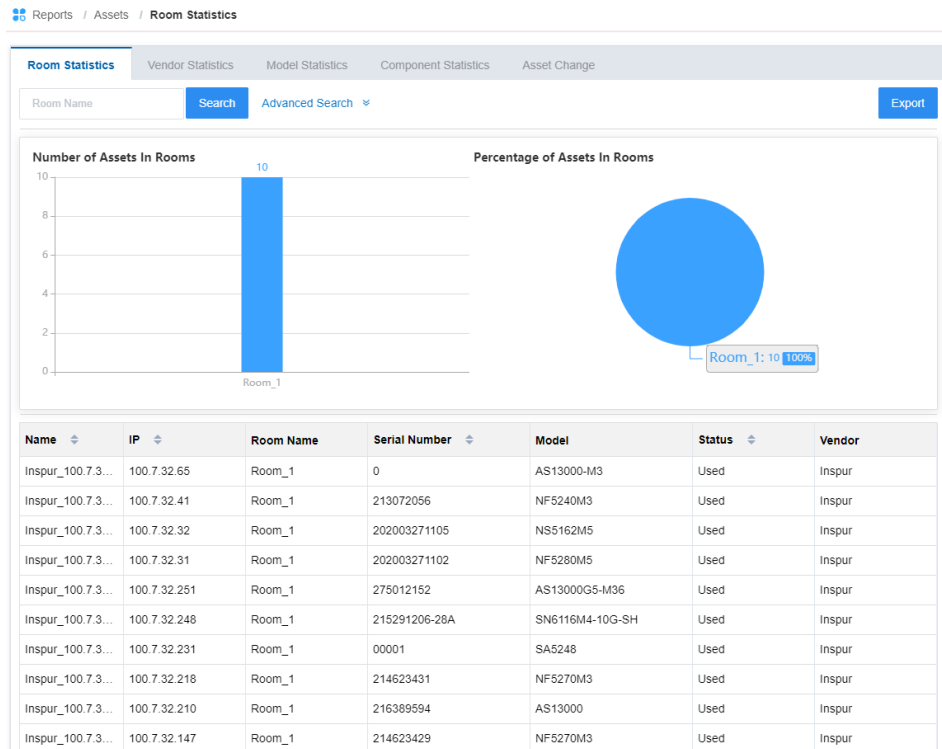
In the navigation tree on the left side of the report management module, select [Assets] to enter the asset report page. On the asset report page, you can view room statistics, vendor statistics, model statistics, component statistics and asset change information, and support exporting statistics lists of different dimensions. It is convenient for users to maintain asset information.

The operation of exporting asset report statistics of different dimensions is similar. This chapter takes the export of component statistics list as an example to introduce the export of asset reports. The component-level asset statistics function allows equipment component information to be clear at a glance, which can assist administrators in fine-grained control of asset data.

### Procedure

**Step 1** Click [Reports] -> [Assets] in turn to enter the asset report page, as shown in the

figure below.



**Step 2** Select the "Component Statistics" tab to enter the component statistics page. On this page, you can view asset and equipment parts details, realize the part-level classification and statistics functions, and also support exporting reports. The parts statistics list shows the parts statistics of each device Information. Including: CPU, RAID, disk, network port, fan, memory, network card, PCIE, power supply, number of logical disks, etc.

**Step 3** In the search box, enter the name or IP to fuzzy query the asset report; click <Advanced Search> to use the serial number, model or vendor to fuzzy query the asset report.

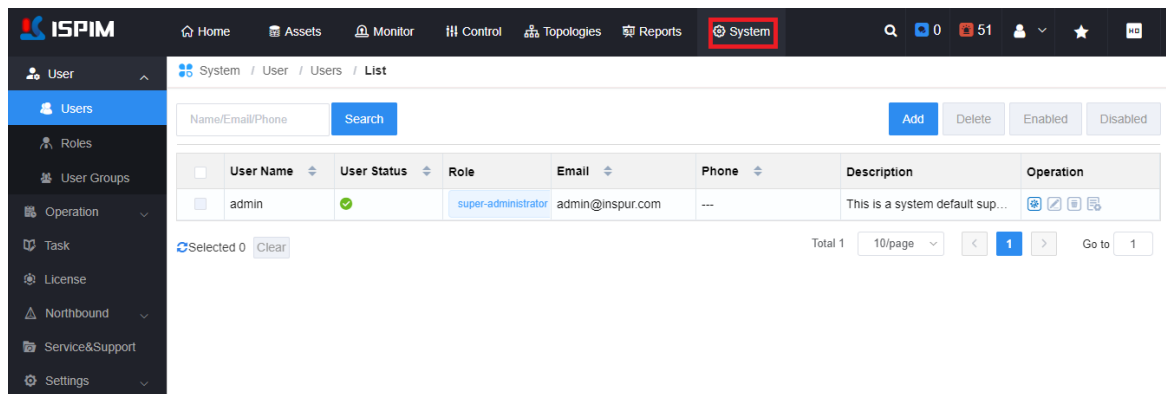
**Step 4** Click the <Export> button above the list to export the asset report with one click.

----End

# 11 System Management

In the navigation bar at the top of ISPIM, select the "System" tab to enter the system management module. The system management module mainly includes user management, log management, system operation management, license management, northbound management, service & support, system settings, etc.

Figure 11-1 System Management



## 11.1 User Management

The user management module mainly includes three parts: role management, user management and user group management. You can perform operations such as adding, editing, and deleting roles/users/user groups as needed.

### 11.1.1 Role Management

Different roles on the ISPIM platform have different operating permissions.

Table 11-1 Role description

Role	Description	Remarks
admin	admin has system management function, can view and allocate all resources.	The system default admin user is the admin role
operator	operator can only access their own resources.	
user	user can only view their own resources	

## 1. Add Roles

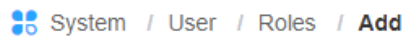
ISPIM supports custom roles to achieve more flexible division of permissions, and roles can be added as needed.

### Procedure

**Step 1** Click [System] -> [User] -> [Roles] to enter the role management page.

**Step 2** Click the <Add> button to enter the add role page, as shown in the figure below.

Set the role name, role type and description, etc. After the role type is selected, the role permissions tree will pop up on the right side, and you can check the corresponding permissions for the new role as needed

 System / User / Roles / Add

---

Name \*

Type \*  Admin  Operator  User

Description

**Step 3** After the role setting is completed, click the <Submit> button to complete the creation of the role.

---End



#### NOTE

- Only users with corresponding permissions can access the corresponding pages.
- After the role is added, you can select the role when creating a user.

## 2. View Roles

### Procedure

**Step 1** Click [System] -> [User] -> [Roles] to enter the role management page.

**Step 2** On the role management page, you can view role information, including role name, role type and description

**Step 3** In the role list, click the role name, and you can view the permissions of the role in the pop-up window on the right.


---End


## 3. Role Operation

You can edit or delete roles as needed.

### Procedure

**Step 1** Click [System] -> [User] -> [Roles] to enter the role management page.

**Step 2** In the role list, click the  icon corresponding to a role to enter the edit role page, where you can modify the role information and permissions as needed.

**Step 3** In the role list, click the  icon corresponding to a role to delete a single role. After selecting multiple roles in the list, click the <Delete> button at the top of the list to delete the selected roles in batches.

--End



#### NOTE

User cannot edit and delete built-in roles in the system.

---

## 11.1.2 User Management

On the user management page, you can perform operations such as creating, editing, enabling/disabling, and deleting users.

## 1. Add User

### Procedure

**Step 1** Click [System] -> [User] -> [Users] to enter the user management page.

**Step 2** Click the <Add> button to enter the add user page, as shown below. Set the user name, user password, role, full name, email and other parameters as required.

System / User / Users / Add

User Name \*

Password \*

Confirm \*

Role \*

User Status \* Disabled  Enabled

Full Name \*

Email \*

Phone \*

Description

© 2017-2020 Inspur.com. All rights reserved.

**Step 3** After setting the parameters, click the <Submit> button to complete the user creation.

--End

Table 11-2 Parameter Description

Parameter	Description	Remarks
User Nmae	username	-
Password	User password	At least 8 digits and contain letters, numbers and special characters
Confirm	Confirm password	Confirm that the password is consistent with the above user password settings




Parameter	Description	Remarks
Role	User role	When a user has multiple roles, its permission is the union of multiple roles
User Status	User status	Choose to enable or disable this user
Full name	User's full name	-


## 2. Manage users


According to needs, you can edit, delete, enable/disable, change password, unlock, etc.


### Procedure


**Step 1** Click [System] -> [User] -> [Users] to enter the user management page.

**Step 2** In the user list, click the  icon corresponding to a user, and in the pop-up change password window, enter the old password, the new password and confirm the password, and then the user password can be changed.

**Step 3** In the user list, click the  icon corresponding to a user to enter the edit user page. You can modify the user name, role, phone number, etc

**Step 4** In the user list, click the  icon corresponding to a user to delete the user; select multiple users in the user list, and click the <Delete> button above the list to delete the selected users in batches.

**Step 5** In the user list, click the  icon corresponding to a user to enter the device page. On this page, you can edit the user's asset information and assign asset devices to the user.

**Step 6** In the user list, click the  icon corresponding to a user to unlock the user. This operation is suitable for scenarios where the password needs to be unlocked due to continuous incorrect password input.

**Step 7** In the user list, after selecting a user, click the <Enable/Disable> button above the list to enable or disable the user.

--End



For the built-in admin user in the system, you can only modify the password, and cannot edit, delete, or allocate assets.

---

### 11.1.3 User Group Management

A user group is a logical collection of roles and users, and supports the management of custom roles and users. Through user groups, a large number of users and roles can be centrally managed.

#### 1. Add User Groups

You can add user groups as needed.

##### Procedure

**Step 1** Click [System] -> [User] -> [User Groups] to enter the user groups page.

**Step 2** Click the <Add> button to enter the page for adding a user group. According needs, set basic information, select roles and other parameters, and then click the <Submit> button to complete the creation of the user group.


--End


#### 2. User group operation

You can edit and delete user groups as needed.

##### Procedure

**Step 1** Click [System] -> [User] -> [User Groups] to enter the user groups page.

**Step 2** In the user group list, click the  icon corresponding to the user group to enter the edit user group page, where you can modify the related information of the user group

**Step 3** In the user group list, click the  icon corresponding to the user group to delete the user group. Select multiple users in the user group list, and click the <Delete> button above the list to delete the selected user groups in batches.

-- end



## NOTE

In the user group list, click the name of a user group, and in the right window you can view the detailed information of the user group, including basic information, roles and users in the group.

## 11.2 Log Management

The log management module records the system operation log in detail, which is convenient for users to audit and trace. On the log management page, you can view the log operation time, operator and other information, and you can perform operations such as deleting or exporting the log.

### Procedure

**Step 1** Click the [System] -> [Operation] -> [Operation Log] to enter the log management page, as shown in the figure below. On this page, you can view system operation log information, and support query operation log based on time, operator or operation IP.

System / Operation / Operation Log / Log List

2020-11-05 15:08:34 - 2020-11-06 15:08:34 - Operator or IP Search Export Delete

Time	Operator	IP	Result	Type	Level	Detail
2020-11-06 11:17:50	admin	100.7.32.20	✓	Operation Log	Medium	User admin login
2020-11-06 08:47:06	admin	100.7.32.20	✓	Operation Log	Medium	User admin login

Total 2 10/page 1 Go to 1

**Step 2** Click the <Export> button at the top of the list to export the log. According to your needs, you can choose to export all the logs or export some of the logs.

**Step 3** Click the <Delete> button above the list, and the log manual deletion window will pop up. Select the log time range in the window to delete the log within the selected time

-- end

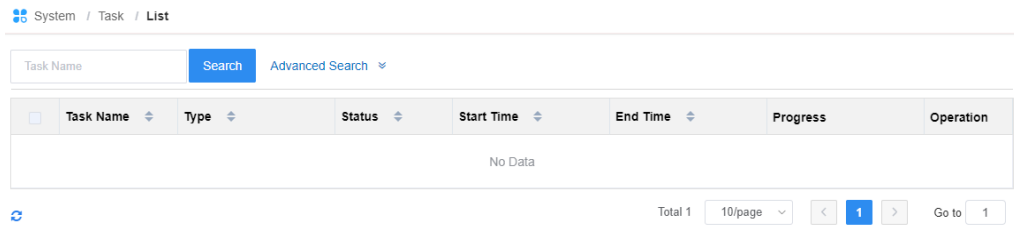
## 11.3 Task

ISPIM provides a unified job management portal, and jobs created in the system can be managed and traced on the job center page.


### Procedure

**Step 1** Click the [System]->[Task] in turn to enter the task management page, as shown

in the figure below. You can view task information on this page, including: task name, task type, status, start time, end time, etc.,



**Step 2** In the task list, click a task name to enter the task details page. In the task details page, you can view the task details, including: task item name, execution status, start time, execution time, execution result, description information In the task details page, click the

 icon corresponding to the job to view the log information of the task

--End

## 11.4 License Management

### 11.4.1 Activate the License

When you log in to ISPIM for the first time, the system will only display the license page by default.

After activation, you can use all the ISPIM functions.



When using ISPIM for the first time, you can apply for a trial version license. After the trial version license expires, you can contact Inspur customer service and choose to upgrade to the enterprise version or standard version and continue to use it.

### Procedure

**Step 1** Click the [System] -> [License] to enter the License Management page, as shown in the figure below. The Activation code is an important certificate for applying for a license. The user needs to provide the Activation code to Inspur customer service to apply for a license. Click the <Copy> button next to the Activation code to copy the Activation code.

System / License / List

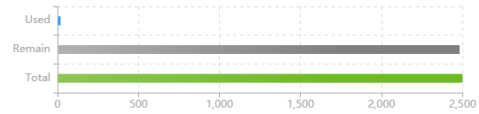
Machine Code: 0A214A5B7EABRBYRV [Copy](#)

**i** User can apply for a trial license to activate ISPIM. When the trial licenses have expired, please upgrade to standard or enterprise edition. If the license capacity is less than the added resources number, please manually delete some existing resources until the resources number matches the license capacity and activate again.

Activation Code \*

Activate

License Usage



License	Version	Activation Time	Resources Capacity	Remaining Days
3A5UA-*****N4-8X-W26	EnterpriseVersion	2020-11-05 10:24:42	2000	+∞
XJ5NE-*****MY-37-B24	EnterpriseVersion	2020-11-05 10:25:32	500	+∞



**Step 2** After receiving the activation code, paste the activation code into the activation code field, and click the <Activate> button to activate ISPIM.

**Step 3** After activation is complete, you can view the usage of the license on the License page, including: used number, remaining number and total number of authorizations. At the same time, the bottom of the page also displays the version of the license, activation time, number of supported resources and remaining days.

-- End



NOTE

- The calculation rules of the license depend on the number of resources it manages. If the number of added resources is greater than the authorized number, you need to manually delete some resources to the supported amount of the license and activate it again.
- After activation, the system will automatically log out the current user, and you need to log in ISPIM again.

## 11.4.2 License Version Description

The license is divided into two versions: Standard Edition and Enterprise Edition. The function descriptions supported by the Standard Edition and Enterprise Edition are shown in Table 11-3.

Table 11-3 License Version Description

Functions	Standard Edition	Enterprise Edition
Automatically discover resources	Y	Y
Server / storage / network equipment / security equipment list configuration	Y	Y
Unified monitoring alarms, custom alarm rules, email, SMS notification Server remote KVM	Y	Y
Data center, room, cabinet management	Y	Y
Large visual screen, custom homepage	Y	Y
Access control	Y	Y
Standardized baseline management	Y	Y
Smart energy management	NO	Y
Server batch power management	NO	Y
Support custom static grouping of resources, automatic grouping management of dynamic rules	NO	Y
Server fault diagnosis, automatic repair	NO	Y
Server inspection management	NO	Y
Server firmware batch upgrade and configuration; batch installation of out-of-band operating system	NO	Y
Multidimensional report	NO	Y
Unified management of multiple data centers, 3D room	NO	Y
Standardized northbound interface, TRAP push alerts	NO	Y
high availability, secure access	NO	Y
Support 100,000 scale monitoring	NO	Y

# 11.5 Northbound Management

## 11.5.1 Alert Forwarding

Through alarm forwarding, Trap alarms received by the ISPIM platform can be forwarded to a third-party management platform to facilitate user integration.

### 1. Trap Setting

#### Procedure

**Step 1** Click the [System] -> [Northbound] -> [Alert Forwarding] to enter the Trap forwarding setting page by default.

**Step 2** According to your needs, set the protocol version and parameters of the alarm forwarding. After setting, click <Submit>.

-- End

### 2. Trap Strategies

#### Procedure

**Step 1** Click the [System] -> [Northbound] -> [Alert Forwarding] -> [Trap Strategies] to enter the Trap forwarding strategies setting page.

**Step 2** Click the <Add> button to enter the Add Trap Forwarding Strategies page, as shown in the figure below.

System / Northbound / Alert Forwarding / Trap Strategies / Add

Trap Setting   **Trap Strategies**   Trap Histories

IP \*

Port \*

Trap Subscribe \*




OID	Name	Operation
No Data		

**Step 3** Set the forwarding destination IP and destination port parameters as needed, click the <Add> button next to the Trap subscribe, and in the pop-up list on the right, select the Trap OID that needs to be forwarded and click the <Add> button to add the selected OID Add to the list.

**Step 4** After setting, click the <Submit> button to complete the addition of the Trap forwarding strategy.

--End

#### NOTE

- In the Trap forwarding strategy, click the  icon corresponding to a strategy to modify the related information of the strategy; click the  icon to delete the strategy.
- Click the  icon to test whether the forwarding strategy is set successfully.

## 3. Trap Histories

### Procedure

**Step 1** Click [System] -> [Northbound] -> [Alert Forwarding] -> [Trap Histories] to enter the Trap Forwarding History page

**Step 2** In the forwarding histories list, you can view the IP, Target IP, location, send time, description, etc.



-- end

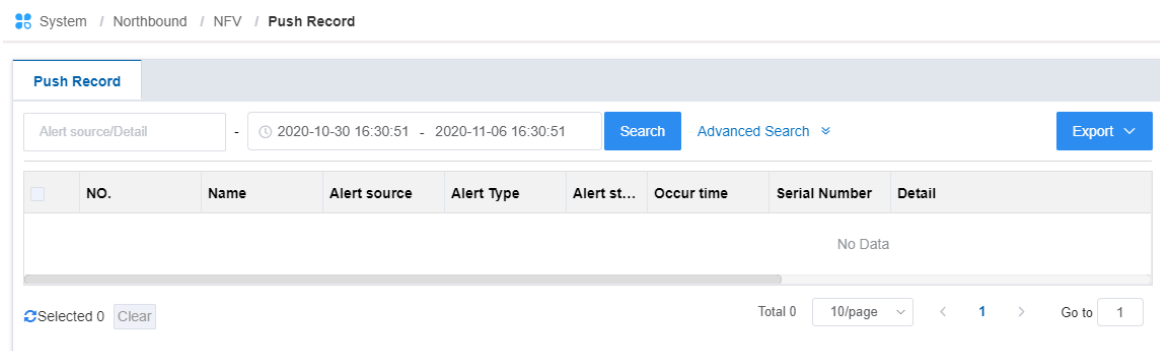
## 11.5.2 NFV

The prerequisites for using NFV are: The third-party management platform has successfully subscribed to ISPIM through NFV. NFV alarm push can push the alarm information of the ISPIM platform to the third-party management platform.

Click [System] -> [Northbound] -> [NFV], you can enter the NFV push record page, as shown in Figure 11-2. On this page, you can view all push records, perform searches, export push records, etc.

- **View the list of push records:** In the NFV push record list, you can view historical push record information, including: alert source, alert type, alert status, occur time, serial number, etc.
- **Search push records:** In the search box, enter the alarm source or alarm details to fuzzy search push records; click the search time box, select the time range in the pop-up time range window, and view the push records within the selected time range; click <advanced query> Button, you can drop down to select the reporting status, data type, level, etc. to view the push records of the corresponding conditions.
- **Export push records:** Click the <Export> button, and select <Today>, <Filter> or < Selected> according to actual needs to export the corresponding push records.

Figure 11-2 NVF



## 11.6 Service&Support

Click [System] -> [Service & Support] to enter the service & support page. On this page, you can set the related information of automatic repair, including repair email, Odd Prefix, company, address, email server, etc. When the device generates an alarm, ISPIM will automatically send an alarm repair

email to the repair mailbox.

## Procedure

**Step 1** Click [System] -> [Service & Support] to enter the service & support page, as shown in the figure below.

System / Service & Support

Status \*

Email \*

Odd Prefix \*

Company \*

Address \*

Email Server [Customize](#)

Resident Contact \* [Add](#)

Name	Email	Telephone	Phone	Oper
No Data				

[Cancel](#) [Submit](#)

© 2017-2020 Inspur.com. All rights reserved.

**Step 2** According to the needs, set the repair mail parameters. Including: Status, Email, Odd prefix, company, address, Email Server, etc.

- Status: Choose whether to enable this setting
- Email: Set the email address for receiving repair notice.
- Odd prefix: Inspur service's repair order number prefix.
- Email Server: Click < Customize> to pop up the custom mailbox server window. According to your needs, set the related parameters of the mailbox server that sends the repair mail.
- Resident Contact: Set the resident contact of the data center in the repair mail, so that Inspur customer service can communicate with them. Click the <Add> button, and in the pop-up Add Contact window, set the name, phone number, and email of the resident contact.

**Step 3** After the parameter setting is completed, click the <Submit> button to complete

the repair notification setting.

--End

## 11.7 System Settings

According to actual needs, users can customize the system configuration.

### 11.7.1 Set System Params

According to needs, users can customize parameters such as Asset Acquisition Frequency, System Monitoring Acquisition Frequency, Log Automatic Delete, and Inspect Log Expiration Setting

#### Procedure

**Step 1** Click [System] -> [Settings] -> [System Parameters] to enter the system parameter setting page, as shown in the figure below.

System / Settings / System Params

<b>Session Timeout Setting</b> Time(min) * <input type="text" value="-1"/> -1 means never expire <input type="button" value="Cancel"/> <input type="button" value="Submit"/>	<b>Asset Acquisition Frequency</b> Time(h) <input type="text" value="1"/> <input type="button" value="Cancel"/> <input type="button" value="Submit"/>
<b>Monitor Acquisition Frequency</b> Time(min) * <input type="text" value="5"/> <input type="button" value="Cancel"/> <input type="button" value="Submit"/>	<b>Log Automatic Delete</b> Retention Time <input type="text" value="1 Month"/> <input type="button" value="Cancel"/> <input type="button" value="Submit"/>
<b>Inspect Log Expiration Setting</b> Time(d) * <input type="text" value="30"/> <input type="button" value="Cancel"/> <input type="button" value="Submit"/>	

**Step 2** Set session timeout, monitor acquisition frequency, log automatic delete and other parameters.

- Session timeout: Set the timeout period for the user to log in to the system. If it expires, you need to log in to the system again. The default is 15 minutes; when set to -1, it will never time out.
- Asset Acquisition Frequency: The system actively collects equipment hardware

information, the default is 1 hour.

- **Monitor Acquisition Frequency:** The time interval for the system to actively collect each monitoring indicator item of the device, the default is 5 minutes.
- **Log Automatic Delete:** The time for the system to keep the operation log, you can drop down to select "Permanent", "1 week", "1 month", "3 months".
- **Inspect Log Expiration Setting:** Set the retention time of device hardware logs collected by the system, the default is 30 days.

--End

## 11.7.2 Services Management

Click [System] -> [Settings] -> [Services] to enter the services management page. On the service management page, you can view the operation condition of ISPIM nodes, microservices and components, and perform node alarm threshold setting, database backup, and adding FTP server operations.

Figure 11-3 Service Management

System / Settings / Services / Node / List

The screenshot displays the 'Node List' and 'Current Alert' sections of the service management page. The 'Node List' section contains a table with the following data:

Name	IP	Status
ispim	127.0.0.1	● Normal


The 'Current Alert' section contains a table with the following headers:

Name	Severity	First Occur Time	Last Occur Time	Detail
No Data				

At the bottom right of the page, there is a pagination control showing 'Total 0', '10/page', and 'Go to 1'.

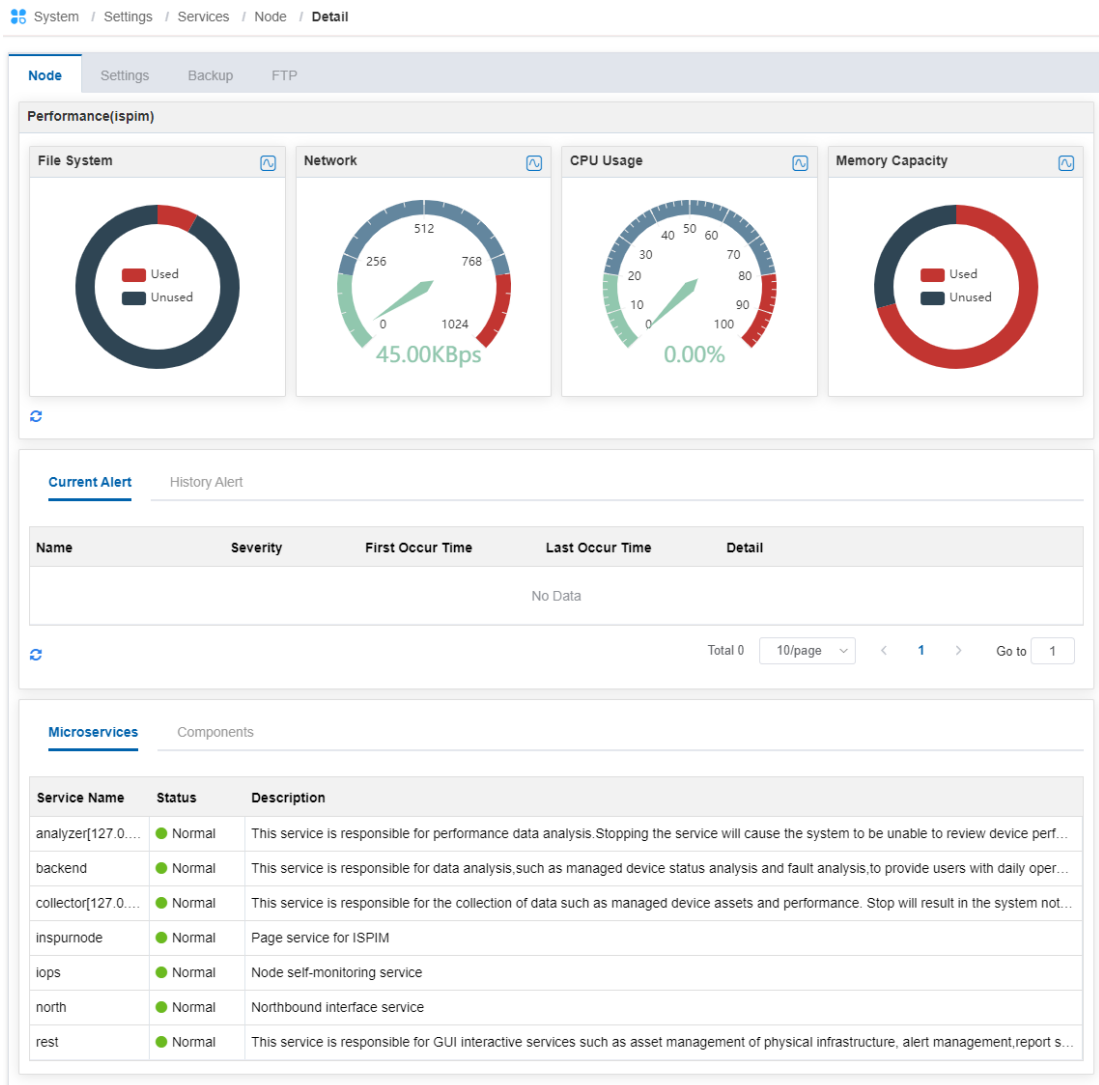
### 1. Node Management

On the service management page, select the "Node" tab to enter the node management page. You can view the ISPIM node list and real-time alarm list on this page.

- **Refresh list information:** Click the  icon in the lower left corner of the page to manually refresh the node list and current alarm list information


- **View node monitoring details:** In the node list, click on a node name to enter the node monitoring details page.

Figure 11-4 Monitoring Details



© 2017-2020 Inspur.com. All rights reserved.

On the node monitoring details page, you can view detailed node information, including: performance data usage, current alert and history alert lists of the node, microservices and component status and other related information.

- **Performance:** Display node file system, network, CPU usage and memory capacity usage. Click the  icon to view the performance history curve of corresponding performance.
- **Current/History Alarm:** Shows the current or historical alarm information that occurred on the node device, including: name, level, alarm first occur time, last occur time and node alarm details

- **Microservices:** This page shows the running status and description information of each ISPIM microservice.
- **Components:** This page displays the operating status and description information of ISPIM third-party components.

## 2. Node Settings

On the service management page, select the "Settings" tab to enter the node settings page. On this page, you can modify the alarm threshold, node refresh frequency and performance refresh frequency of ISPIM node indicators.


- **Modify threshold settings:** In the threshold setting list, click the  icon of an indicator item. In the pop-up modify threshold rule window, you can choose to modify the monitoring indicator item and its threshold. When the device indicator item exceeds the set threshold, the system will generate an alarm.
- **Modify node refresh frequency:** In the node refresh frequency input box, enter the time frequency, and click the <Submit> button to modify the node refresh frequency. The node refresh frequency is: ISPIM node interworking test frequency.
- **Modify performance refresh frequency:** In the performance refresh frequency input box, enter the time frequency and click <Submit> to modify the performance refresh frequency. The performance refresh frequency is: the node performance data collection frequency.

Figure 11-5 Node Settings

System / Settings / Services / Settings

Node Settings Backup FTP

Threshold Setting >

Monitoring Frequency v

Node Refresh Frequency Setting

Time(min) \* 5

Cancel Submit

Performance Refresh Frequency Setting

Time(min) \* 1

Cancel Submit

© 2017-2020 Inspur.com. All rights reserved.

### 3. FTP Management

On the service management page, select the "FTP" tab to enter the FTP management page. On this page, you can view the FTP list, perform operations such as adding, editing, and deleting FTP.

- **Add FTP:** click the <Add> button, and you will enter the FTP add page, as shown in the figure below. After setting the FTP URL, username and password parameters on this page, click <Submit> to add FTP.

System / Settings / Services / FTP / Add

Node Settings Backup FTP

URL \* For example:ftp://127.0.0.1:21/opt/ispim/backup/

User Name

Password

Cancel Submit



- **Edit FTP:** In the FTP list, click an FTP  icon, you can modify the FTP URL, user Name or Password.
- **Delete FTP:** In the FTP list, click the  icon of an FTP to delete the FTP.

Figure 11-6 FTP Management

System / Settings / Services / FTP / List

Node	Settings	Backup	FTP
<input type="text" value="URL"/> <input type="button" value="Search"/> <input type="button" value="Add"/>			
URL	User Name	Password	Operation
ftp://100.7.32.100	admin	***	
		Total 1    10/page    < 1 >    Go to 1	

## 4. System Backup/Restore

On the service management page, select the "Backup" tab to enter the backup page. On this page, you can view the historical backup list, perform operations such as backing up ISPIM configuration files, backing up the database, and restoring the system.



The system backup/restore function can ensure the security of users' data, and also help to ensure the consistency of data between ISPIM nodes in a high-availability environment. It is recommended that users perform data backup operations on a regular basis.

Figure 11-7 Backup

System / Settings / Services / Backup

Node	Settings	Backup	FTP
<b>Config Backup</b>			
<input type="button" value="Start Backup"/>		This function backs up the cluster or node configuration to facilitate management of configuration files	
Serial Number	Create Time	File Path	Operation
1	2020-11-09 14:24:26	ftp://100.7.32.100/config_20201109142426.tar.gz	
<b>Database Backup</b>			
<input type="button" value="Start Backup"/>		This function backs up the database to facilitate management of configuration files	
Serial Number	Create Time	File Path	Operation
No Data			

© 2017-2020 Inspur.com. All rights reserved.



## (1). Backup

According to needs, you can back up the ISPIM configuration file or back up the database.


- **Config Backup:** Click the corresponding <Start Backup> button, you can choose to back up the ISPIM configuration file and Redis component configuration file to the FTP server or local server.
- **Database Backup:** Click the corresponding <Start Backup> button, you can choose to backup the MySQL database to an FTP server or a local server. ISPIM supports backup and restoration of the system database to ensure user data security.



If you choose to back up data to an FTP server, you need to add FTP in the FTP management page first.

---

## (2). System Restore

Through system restore, you can restore system-related settings to the configuration data at the backup time. In the configuration backup list or database backup list, click the  icon and confirm in the pop-up window, the system will automatically perform the restore operation.

---

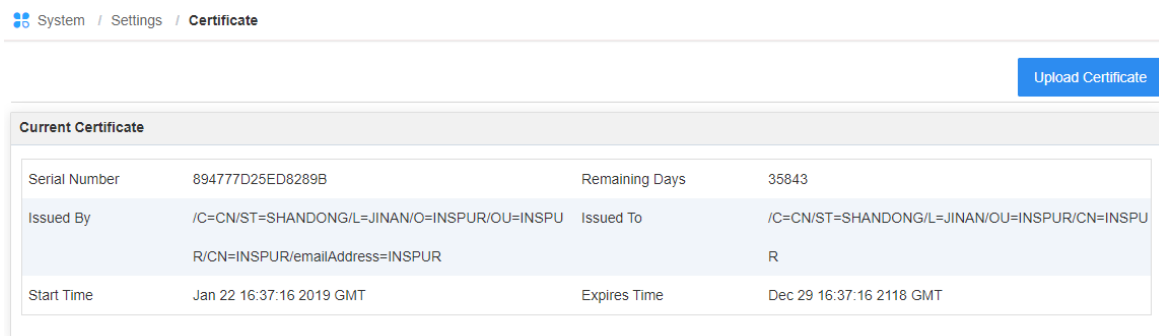


- System restore has risks, please operate with caution.
  - It may be necessary to restart some dependent components of the system after system restoration.
  - The system restore operation cannot be undone. If it is terminated forcibly, the system may become unusable. Before proceeding, please save the key data and close all system-related operations.
  - After the system restore is executed, the currently logged-in user will be logged out by default and needs to log in again.
-

## 11.7.3 Certificate Management

Click [System] -> [Settings] -> [Certificate] to enter the certificate management page. On this page, you can view the currently used SSL certificate. By default, users can use the default SSL certificate provided by Inspur. According to needs, users can also click the < Upload Certificate > button to upload the SSL certificate file.

Figure 11-8 Certificate Management



## 11.7.4 Proxy Servers

Users can use a proxy server to access ISPIM. The supported proxy types are as follows:

- HTTP: HTTP protocol proxy settings.
- Security: HTTPS protocol proxy settings.
- FTP: FTP protocol proxy settings.
- Socket: Socket level proxy settings.

### Procedure

**Step 1** Click [System] -> [Settings] -> [Certificate] to enter the certificate management page.

**Step 2** Select and tick the "Enable" column of the proxy type, then you can edit the server address and port of the proxy.

**Step 3** After the setting is completed, click the <Submit> button to complete the proxy server setting.

---End



## NOTE

Socket proxy has the highest priority.

---

## 11.7.5 NOTE Servers

Before setting the alarm notification rules, you need to set the notification server. ISPIM supports the settings of email server, SMS, SMS modem and SMS gateway server.

### 1. Email Servers Setting

#### Procedure

**Step 1** Click [System] -> [Settings] -> [NOTE Servers] to enter the notification servers setting page.

**Step 2** Select the "Email Servers" tab to set the SMTP Port, SMTP server, user name, password, security type and other parameters of the mailbox server.

**Step 3** Click the <Test> button to test whether the email server is successfully configured; click the <Submit> button to complete the email server settings.

---End

### 2. SMS Setting

#### Procedure

**Step 1** Click [System] -> [Settings] -> [NOTE Servers] to enter the notification servers setting page.

**Step 2** Select the "Short Message Server" tab to set the relevant parameters of the short message server.

- Enabled Status: Choose whether to enable the SMS
- Encode Protocol: Drop down to select the encoding protocol
- User Name: Username of the SMS
- Password: Password of the SMS

- Calling Phone Number: Mobile phone number for sending SMS
- Test Phone Number: SMS receiving test mobile phone number
- Open Proxy: Choose whether to send SMS through proxy

**Step 3** Click the <Test> button to send a short message to test whether the SMS is set successfully; click the <Submit> button to complete the SMS setting.

---End

### 3. SMS Modem

By setting the connection parameters between ISPIM and SMS modem, the communication between the two can be established. In daily monitoring, O&M personnel receive alarm notifications through short messages to achieve the purpose of monitoring equipment status.

#### Procedure

**Step 1** Click [System] -> [Settings] -> [Notification Server] to enter the notification servers setting page.

**Step 2** Select the "SMS modem" tab to set the relevant parameters of the SMS modem

- Enabled Status: Choose whether to enable the SMS modem server
- Network Standard: Drop down to select the network standard
- Baud Rate: Drop down to select the baud rate of the SMS modem
- Test Phone Number: Test mobile phone number for receiving SMS

**Step 3** Click the <Test> button to send a short message to test whether the SMS modem server is set successfully; click the <Submit> button to complete the SMS modem server settings.

---End

### 4. SMS Gateway

By setting the connection parameters between ISPIM and SMS gateway server, the communication between the two can be established.

#### Procedure

**Step 1** Click [System] -> [Settings] -> [Notification Server] to enter the notification servers setting page.

**Step 2** Select the "SMS gateway" tab to configure the relevant parameters of the SMS gateway server.

- Enabled Status: Choose whether to enable the SMS gateway server
- Protocol: Drop down to select the SMS gateway protocol type
- Request Method: Drop down to select the delivery method
- Encode Type: Drop down to select encoding method
- Crop ID: The name and value of the company ID
- Open Proxy: Choose whether to send SMS through SMS gateway server proxy

**Step 3** Click the <Test Send> button to send an SMS to test whether the gateway server is set successfully; click the <Submit> button to complete the SMS gateway server settings.

---End

## 11.7.6 ISFM Config

Click [System] -> [Settings] -> [ISFM Config] to enter the ISFM config page. Enter the ISFM login user name, password and domain name on this page, and click <Submit> to configure ISFM. For ISFM, please refer to the relevant manuals of ISFM products.

Figure 11-9ISFMConfig

System / Settings / ISFM Config

### ISFM Config

User Name \*

Password \*

Domain \*



## NOTE

By configuring ISFM, you can remotely synchronize the firmware package. About the firmware package file, for details, see `2Synchronize Bundle File`.

---

## 11.7.7 Authentication Server

You can use the user in the authentication server to log in to ISPIM.

### Procedure

**Step 1** Click [System] -> [Settings] -> [AS] to enter the authentication server page.

**Step 2** Set the relevant parameters of the authentication server as needed.

**Step 3** Click the <Test> button to test whether the authentication server is successfully configured; click the <Submit> button to save and submit the authentication server settings.

---End

## 11.7.8 Model Mappers

Through model mapping, the device model can be mapped to an ISPIM compatible device model to solve the problem of device incompatibility.

### Procedure

**Step 1** Click [System] -> [Settings] -> [Model Mappers] to enter the model mappers page

**Step 2** Click the <Add> button to enter the add model mapping page, as shown in the figure below. Enter the real device model, and select the mapped model from the drop-down list of mapper model. Click <Submit>.



System / Settings / Model Mappers / Add

Real Model \*

Mapper Model \*

---End

 NOTE

In the model mapping list, click the  icon corresponding to a model to edit the model mapping information; click the  icon corresponding to a model to delete the model mapping information.

### 11.7.9 Collector Settings




ISPIM supports distributed deployment, and can load balance system tasks to different collectors according to resource binding. At the same time, ISPIM can group collectors through proxy groups, and collectors under the same group share a load balancing strategy.

#### 1. Collector Settings

Click [System] -> [Settings] -> [Collector Settings] to enter the collector settings page. Select the "Proxy Clents" tab to enter the collector settings page. On this page, you can view the collector list, and perform operations such as adding, editing, and deleting collectors.

Figure 11-10 Collector Settings

System / Settings / Collector Settings / Proxy Clients / List

Proxy Clients		Proxy Groups					
Name/IP		Search		Add		Delete	
Name	IP	Type	Connect St...	CPU Usage(%)	Memory Usage(%)...	Resource ...	Operation
<input type="checkbox"/>	Local collector	Data Collector	Normal	2%	73%	69	  

Selected 0  Total 1 10/page < 1 > Go to 1



## NOTE

- Click the name of a collector, and you can view the details of the collector in the slide bar on the right.
- Click the resource number of a collector to view the details of the resources associated with the collector.

- **Add Collector**

## Prerequisite

According to the <Inspur Physical Infrastructure Manager (ISPIM) V6.0.0 Installation Guide-20201030.docx>, the ISPIM collection and analysis cluster has been deployed, and the collector system IP and related settings have been completed.

## Procedure

**Step 1** Click [System] -> [Settings] -> [Collector Settings] to enter the collector settings page.

**Step 2** Select the "Proxy Clients" tab and click the <Add> button to enter the add collector page, as shown in the figure below.

System / Settings / Collector Settings / Proxy Clients / Add

**Proxy Clients** Proxy Groups

Name \*

IP \*  ?

Network Card IP

Type	IP	Operation
No Data		

Type \*

Proxy Group \*

Description

© 2017-2020 Inspur.com. All rights reserved.

**Step 3** After setting the collector name, IP, Network Card IP, Collector type, Proxy Group



and other parameters, click the <Submit> button to complete the addition of the collector.


- Name: Custom collector name
- IP: The IP address used by the collector when reporting information to the ISPIM master node.
- Network Card IP: For network cards of different network segments, different IPs can be configured.
- Type: The default is the data collector.
- Proxy Group: Drop down to select the proxy group. Collectors in the same proxy group will use the same load balancing strategy. The system provides a default "centralized agent group", users can also create a custom agent group on the agent group page in advance. For details, see 2Proxy Group.

---End

● Collector associated resources

### Procedure

**Step 1** Click [System] -> [Settings] -> [Collector Settings] to enter the collector settings page.

**Step 2** Select the "Proxy Clients" tab, in the collector list, click the  icon corresponding to an Proxy, and the associated resource window will pop up, as shown in the figure below.

**Associated Resource**

Available Resource

Please Search

<input type="checkbox"/>	Resource Na...	IP	Type	Room
No Data				


Total 0

Already Associated Resource

Resource N...	IP	Type	Room	Operation
Inspur_100...	100.7.8.180	In Band	---	<input type="button" value="✖"/>
Inspur_100...	100.7.34.47	Out Band	Room_1	<input type="button" value="✖"/>
Inspur_100...	100.7.34.141	Out Band	Room_1	<input type="button" value="✖"/>
Inspur_100...	100.7.34.72	Out Band	Room_1	<input type="button" value="✖"/>
Inspur_100...	100.7.34.45	Out Band	Room_1	<input type="button" value="✖"/>
Inspur_100...	100.7.34.133	Out Band	Room_1	<input type="button" value="✖"/>
Inspur_100...	100.7.34.40	Out Band	Room_1	<input type="button" value="✖"/>
Inspur_100...	100.7.34.39	Out Band	Room_1	<input type="button" value="✖"/>
Inspur_100...	100.7.34.51	Out Band	Room_1	<input type="button" value="✖"/>
Inspur_100...	100.7.34.132	Out Band	Room_1	<input type="button" value="✖"/>

Total 69

**Step 3** In the "Associable Resources" list on the left, check the resources, and click the

<Add> button to move the selected resources to the "Already Associated Resource" list on the right. Click in the "Already Associated Resources" column The <Select Invert> button can move all selected associated resources to the "Associable Resources" list; in the "Already Associated Resources" list, click the  icon corresponding to a resource to move it to the "Associable Resources" list in.

**Step 4** Click the <Save> button to complete the association operation between the collector and the resource device.


---End


## ● Collector Management


According to needs, you can edit, delete or modify the collector.

### Procedure

**Step 1** Click [System] -> [Settings] -> [Collector Settings] to enter the collector settings page.

**Step 2** Select the "Proxy Clients" tab, In the proxy list, click the  icon corresponding to a proxy to edit the relevant information of the proxy, including name, IP, network card IP and other information.

**Step 3** In the proxy list, click the  icon corresponding to an proxy to delete the proxy. Select multiple proxies in the list, and click the <Delete> button above the list to delete the selected proxies in batches.

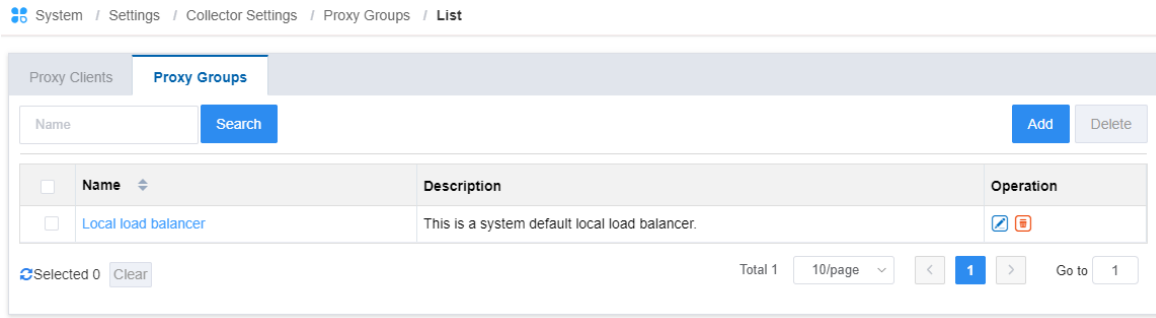
**Step 4** In the proxy list, click the  icon corresponding to a proxy to modify the resources associated with the proxy.

---End

## 2. Proxy Group

Click [System] -> [Settings] -> [Collector Settings] to enter the collector settings page. Select the "Proxy Group" tab to enter the proxy group management page. On this page, you can view the load balancer list, and perform operations such as adding, editing, and deleting load balancers.

Figure 11-11 Proxy Groups



 NOTE

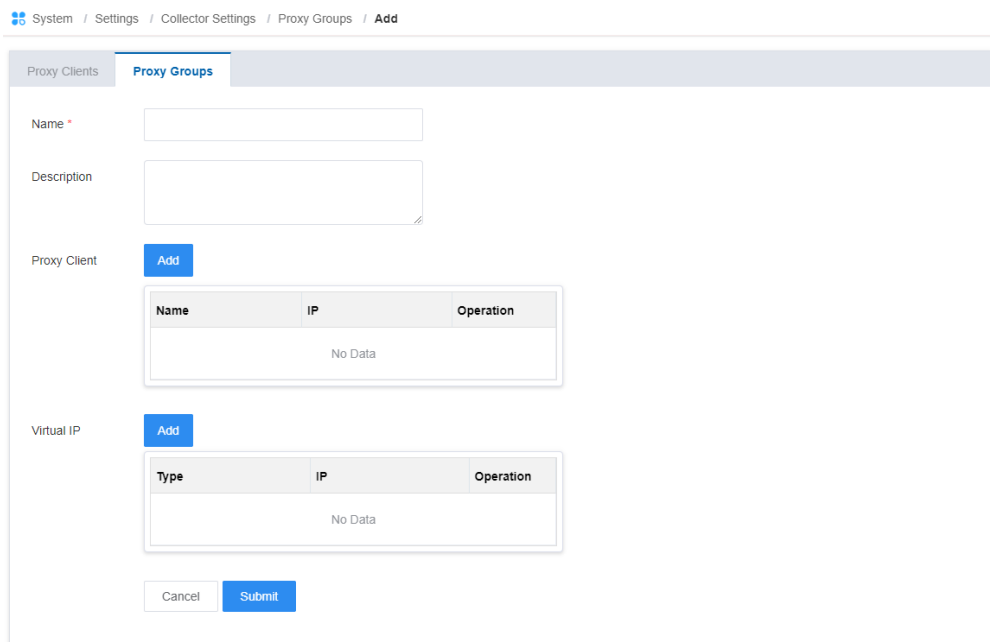
Click the name of a collector, and you can view the details of the collector on the right side sliding bar.

● Add Load Balancer

Procedure

**Step 1.** Click [System] -> [Settings] -> [Collector Settings] to enter the collector settings page.

**Step 2** Select the "Proxy Group" tab and click the <Add> button to enter the Add Load Balancer page, as shown in the figure below.



© 2017-2020 Inspur.com. All rights reserved.

**Step 3** Set the related parameters of the load balancer.

**Step 4** After setting the parameters, click the <Submit> button to complete the creation of the load balancer.

---End



#### NOTE

The system provides "Local load balancer" by default.


---


## ● Proxy Groups Management

You can edit and delete the load balancer as needed.

## Procedure

**Step 1** Click [System] -> [Settings] -> [Collector Settings] to enter the collector settings page.

**Step 2** Select the "Proxy Group" tab to enter the load balancer page. In the load balancer list, click the  icon corresponding to a load balancer to modify the related information of the load balancer.

**Step 3** In the load balancer list, click the  icon corresponding to a load balancer to delete the load balancer. In the load balancer list, after selecting multiple load balancers, click the <Delete> button above the list Delete selected load balancers in bulk.

---End

## 12 FAQ

### 12.1 ISPIM cannot log in successfully, how to solve it?

**[Phenomenon]:**After the ISPIM installation is complete, when logging in with the username/password, it prompts that the login failed.

**[Reason]:** ①Since ISPIM has just completed the deployment, the back-end service has not been fully started. ②The hardware configuration of the device where ISPIM is located does not meet the minimum configuration requirements for its deployment.

**[Solution]:**①, Please be patient and try to log in again after 5 minutes.②, Please follow the upgrade ISPIM platform to deploy the node hardware configuration.

### 12.2 After ISPIM is reinstalled due to a failure, do I need to reactivate it?

- If you reinstall ISPIM on other machines, the original activation code is no longer valid, you need to prepare the order number and the new machine code, and contact Inspur customer service again to obtain the new activation code.
- If ISPIM is reinstalled on the same machine, the generated machine code will not change, the original activation code is still valid, just reactivate.

### 12.3 Does the managed device occupy the license capacity if it is reinstalled due to a fault?

**[Phenomenon]:** The managed device is reinstalled due to a failure, and the IP address and other information has changed. Will adding it to ISPIM again occupy the license capacity?

**[Analysis]:** ISPIM manages the number of licenses based on the device SN. Usually SN will not reset the BMC IP address due to reinstalling the system. The specific situation depends on different

scenarios, such as:

- Scene 1: When the SN of the device is the same, please delete the old device record in ISPIM first, and add the new device. At this time, only one license capacity is still occupied.
- Scene 2: When the SN numbers of the new and old devices are inconsistent, ISPIM will consider the new and old devices to be different devices. At this time, two license capacity will be occupied.

## 12.4 What equipment does ISPIM support?

The devices supported by the ISPIM platform are listed in the following table.

Type	Manufacturer	Model
Server	Inspur	M4
		M5
		M6
		NF5488A5
		Chunxiao Model (NF2180M3)
	Huawei	RH2288 V3
		RH2288H V3
		RH2288H V5
		RH2288V5
		RH5885 V2
		RH5885V3
		RH5885H V3
		RH8100 V3
		CH121 V3
		CH242 V3
		2488H V5
		E9000
		X6800
		Taishan 2280
	Taishan 5280	
	ZTE	R5300G3
		R5300G4
		R5300 G4-12LFF
	H3C	UniServer R4900 G3

Type	Manufacturer	Model
	Sugon	I620-G20
		I620-G30
		I840-G20
		W720-G20
		W720-G30
		H620-G30
	HP	DL360G8, DL360G9
		DL380G8, DL360G9
	DELL	PowerEdge R630
		PowerEdge R720
		PowerEdge R730
		PowerEdge R740
		PowerEdge R920
		PowerEdge R930
	FiberHome	Fit Server R1200V5
Storage device	Inspur	AS1000 G2
		AS2200G2, AS2600G2, AS5300G2
		AS520EM1
		AS5300G2, AS5500G2
		AS5500G2F
		MNGRAS5300
		ASMANAGERCM12
		AS13000
	Huawei	OceanStor 2600V3
		OceanStor 5500V5
		OceanStor 5600V3
		OceanStor 9000V5
	DELL	SC5020
	Nvidia	SFA200
SFA7900		
Network Equipment	Inspur	CN61108PC-V
		S6850-24XS
		N6100
	Cisco	N7700, N7710, N6000
		N5672UP
	DELL	S4148-ON
		S3048-ON
	Huawei	CE6856-48S6Q-HI
		CE6856HI
		CE6851-48S6Q-HI
CE12808		
S5720-56-EI-AC		

Type	Manufacturer	Model
		NE40E-X16A
		V200R002
		CE6881-48S6CQ
		16808
		S5720-52P-EI-AC
		NE40E-X8C
	H3C	S5560-54C
		S5820V2-48S
		S5820V2-54QS-GE
		S6820-56HF
		S6900-4F
		S6900-54QF
		SA12508X-AF
		SR6608-X
		SR8805-F
		S12516F-AF
		S12508F-AF
		S6900-54QF-F
		S6860-54HF
		M9008
	ZTE	ZXR10 5252E
		ZXR10 5960-64DL
		ZXR10 5960-65DL
		ZXR10 5960-66DL
		ZXR10 5960-72DL
		ZXR10 M6000-8S/18S
		ZXR10 9908
		ZTE_5960-52TM
		ZXR10 5952D
	Juniper	QFX5100
QFX5200		
Maipu	S4320-56TC	
FiberHome	S5700-52T-X	
Mellanox	MCS7520	
Firewall	H3C	F5000-C, M9008-S
	Huawei	E8000E-X16
		EUDEMON8000E-X16
NSFOCUS	NX3P1000B	



## 12.5 How to check SNMP Trap settings?

This chapter takes the Inspur NF5280M5 server as an example to introduce how to view the Trap target address of the server in the BMC WebUI page.

### Procedure

**Step 1** In the browser address bar, enter the BMC IP address and click Enter, or in the server list, click the BMC IP of the server to enter the BMC login page of the device. For the Inspur server, you can use (admin/admin) Log in to the BMC management page.

**Step 2** On the BMC management page, select [BMC Settings/Alarm Management] in the navigation tree on the left to enter the alarm management page.

**Step 3** On the alarm management page, in the "Alarm Policy Settings" column in the list below, you can view the information about the alarm policy settings, including: whether it is enabled, LAN channel, alarm type, and alarm target.

**Step 4** Check whether the IP of the "alarm target" has been set as the access IP of ISPIM.

--end



#### NOTE

BMC supports up to three alarm strategies.

---

## A Getting Help

### A.1 Collecting Fault Information

Before troubleshooting, obtain the following information:

- Customer company and address.
- Contact person and telephone number.
- Time when the fault occurred.
- Detailed fault symptom.
- Device type and software version.
- Any measures taken and effects.

- Fault severity and expected rectification deadline.

## A.2 Using Product Documentation

Inspur provides the documents delivered with the equipment. This document provides guidance for users to solve common problems that occur during routine maintenance or troubleshooting.

To better rectify the fault, users are advised to use the guide before contacting Inspur technical support engineers.

## A.3 Obtaining Technical Support

Inspur's timely and efficient response is available from local branch offices, telephone support, remote support, onsite support.

The technical support system of Inspur Electronic Information Industry Co., Ltd. includes:

- Customer service center: (+86)400-860-0011; (+86)800-860-0011.
- Enterprise business website (<https://www.inspur.com>).