VANTAGEO Server

BMC User Guide (for BMC Version 3)

Version: R1.5

VANTAGEO PRIVATE LIMITED
Corporate Address: 617, Lodha Supremus II,
Road No. 22, Wagle Estate,
Thane - 400604
URL: https://vantageo.com
E-mail: support@vantageo.com
Helpdesk - +91 18002669898

LEGAL INFORMATION

This document is provided as is, and all express, implied, or statutory warranties, representations or conditions are disclaimed, including without limitation any implied warranty of merchantability, fitness for a particular purpose, title or non-infringement. VANTAGEO PRIVATE LIMITED and its licensors shall not be liable for damages resulting from the use of or reliance on the information contained herein.

VANTAGEO PRIVATE LIMITED or its licensors may have current or pending intellectual property rights or applications covering the subject matter of this document. Except as expressly provided in any written license between VANTAGEO PRIVATE LIMITED and its licensee, the user of this document shall not acquire any license to the subject matter herein.

VANTAGEO PRIVATE LIMITED reserves the right to upgrade or make technical change to this product without further notice.

Users may visit the VANTAGEO technical support website https://www.vantageo.com/support to inquire for related information.

The ultimate right to interpret this product resides in VANTAGEO PRIVATE LIMITED.

Statement on the Use of Third-Party Embedded Software:

If third-party embedded software such as Oracle, Sybase/SAP, Veritas, Microsoft, VMware, and Redhat is delivered together with this product of VANTAGEO, the embedded software must be used as only a component of this product. If this product is discarded, the licenses for the embedded software must be void either and must not be transferred. VANTAGEO will provide technical support for the embedded software of this product.

Revision History

Revision No.	Revision Date	Revision Reason
R1.5	2024-11-27	Full-text update.
R1.4	2023-12-12	Full-text update.
R1.3	2023-09-08	Full-text update.
R1.2	2022-11-17	Full-text update.
R1.1	2022-06-27	Full-text update.
R1.0	2021-09-09	First edition.

Serial Number: VT20230301

Publishing Date: 2024-11-27 (R1.5)

Contents

About This Manual

Purpose

This manual describes the BMC management software of VANTAGEO servers to provide guidance on BMC configuration and management.

Intended Audience

This manual is intended for:

- Network planning engineers
- Configuration engineers
- Maintenance engineers

What Is in This Manual

This manual contains the following chapters.

Chapter 1, BMC Overview	Describes the operating principle and functions of the BMC, software security and operation interfaces.
Chapter 2, Performing Client Commissioning	Describes the debugging operations on the BMC Web portal logged in through a Client.
Chapter 3, BMC Web Operations	Describes the operations on the BMC Web portal.
Chapter 4, Common Operations	Describes common operations in the BMC.
Chapter 5, Reference: Default Passwords	Describes the default passwords that are used to log in to the BMCs in VANTAGEO servers of different models.
Chapter 6, Reference: Accessing Documents	Describes the steps for accessing documents.

Conventions

This manual uses the following conventions.

❗	Notice: indicates equipment or environment safety information. Failure to comply can result in equipment damage, data loss, equipment performance degradation, environmental contamination, or other unpredictable results.

📚	Note: provides additional information about a topic.

Chapter 1

BMC Overview

Table of Contents

The BMC is the management system of a VANTAGEO server, which monitors and manages server hardware, and provides a Web portal for operation and maintenance, achieving the purposes of software and hardware configuration, fault diagnosis, operating system installation, and operations on the server.

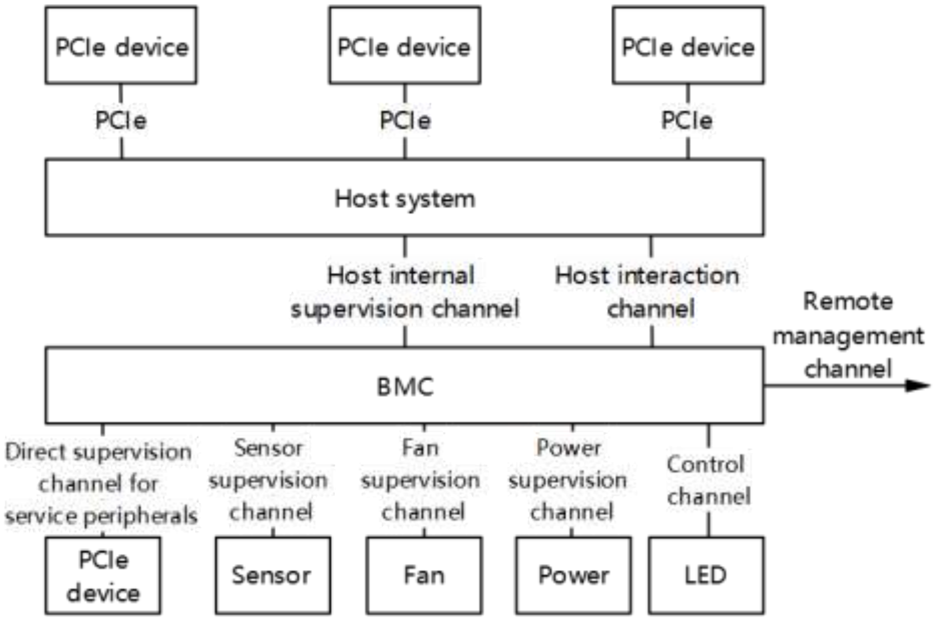
1.1 Operating Principle

The BMC consists of a dedicated management chip and the management software operating on the chip.

- Dedicated management chip

  The server-dedicated management chip provides abundant hardware interfaces and functions. For the hardware interfaces of the BMC, see Figure 1-1.

Figure 1-1 BMC Hardware Interfaces


PCIe device
PCIe device
PCIe device
PCIe
PCIe
PCIe
Host system
Host internal supervision channel
Host interaction channel
Remote management channel
BMC
Direct supervision channel for service peripherals
Sensor supervision channel
Fan supervision channel
Power supervision channel
Control channel
PCIe device
Sensor
Fan
Power
LED

For a description of the BMC channels, refer to Table 1-1.

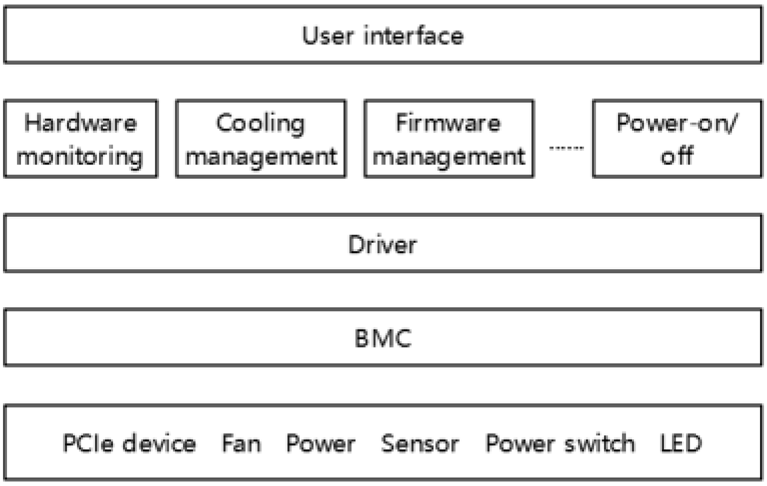
Table 1-1 BMC Hardware Channel Descriptions

Channel	Typical Physical Link	Typical Management Object or Function
Service peripheral supervision channel	PCIe and SMBUS	PCIe devices of a server
Host internal supervision channel	SMBUS and PECI	Internal functional units of the CPU or bridge chip
Host interaction channel	PCIe, USB, LPC, KCS, and SMBUS	Supports KVM, virtual media function, and host serial port functions, and the IPMI protocol
Direct supervision channel for service peripherals	SMBUS and NC-SI	PCIe devices of a server
Sensor supervision channel	SMBUS, GPIO, and A/D	Temperature sensor, voltage sensor, current sensor, and presence sensor
Fan supervision channel	PWM	Fan
Power supervision channel	SMBUS	CRPS, and PMBUS power supply
Control channel	GPIO and SGPIO	Power-on, power-off, and indicator on/off
Remote management channel	Ethernet	Accesses the BMC management server

- Management software

  The BMC management software communicates with hardware devices through the management channels to monitor and manage hardware. For the architecture of the BMC management software, see Figure 1-2.

Figure 1-2 BMC Management Software Architecture



1.2 Functions

The BMC is a the management system of a server. It provides abundant management functions.

- Server health status management: Checks the operational status of a server, analyzes historical data and actual monitoring data, and helps users to find and solve problems in advance, ensuring the highly reliable operation of the server.
  - The 80-code recording function provides sufficient information for analyzing startup failures.
  - When the system crashes, the last-screen capture function records the on-site scenario for analyzing system crashes.
  - Screen snapshots and screen recording on preventive maintenance and operation processes facilitate follow-up audits.
  - The alarm function supports precise fault diagnosis based on components, facilitating component fault locating and replacement.
  - The CrashDump function facilitates further analysis of system errors.
  - The BMC supports Syslog, SNMP Trap, e-mails and Redfish subscription functions to report alarms, so that the NMS can collect server fault information easily.
  - The BMC supports direct display of the server health status through the alarm indicator.
- Host system maintenance

  - → Supports virtual KVM and virtual media functions for remote maintenance of the host system.
  - → Supports out-of-band monitoring and management of RAIDs, so that RAIDs can be monitored without depending on the host system, and the storage devices in the host system can be configured, which improves configuration efficiency and management capability.
  - → Supports OS installation through PXE, which improves the efficiency of remote installation of operating systems in batches.
- ● Device firmware management
  - → Dual BMCs are supported to ensure the reliable operation.
  - → Dual BIOSs are supported to improve the reliability of BIOS upgrade and operation.
  - → The firmware (for example, the FRU and EPLD) upgrade function is supported.
- ● System cooling
  - → Monitors the temperature of important components on the server, and performs different cooling controls based on different hardware thermal characteristics.
  - → Supports the over-temperature power-off function to ensure that the server hardware is not damaged, extending the service life of components.
- ● Intelligent power consumption management
  - → The BMC supports the power capping technology, and provides the standard DCMI for centralized control by the NMS, improving the deployment density of servers.
  - → Energy-saving design reduces the operating costs of a server.
- ● BMC self-management
  - → Supports synchronizing the BMC time through the network and the host, meeting the requirements in different scenarios.
  - → Supports multiple authentication modes, which simplifies server management.
  - → Supports DHCP and DNS, which simplifies server deployment and management.
- ● Diversified management interfaces

  The BMC meets the requirements of various system integration interfaces by providing the following:
  - → Standard DCMI1.5/IPMI2.0/Redfish interfaces
  - → Remote command line interfaces and Web management interfaces
  - → SNMPv1, SNMPv2 and SNMPv3 interfaces

1.3 Software Security

Security Measures for Function Invocation

- ● Complete security design: Uses threat modeling for security design.
- ● Encrypted KVM access: Supports encrypted KVM access.

- HTTPS access with a high encryption security level: Provides an HTTPS trusted path between the server and users to protect local or remote users when they log in to the system through the Web page and prevent communication data from being modified or leaked.
- SSH access with a high encryption security level: Provides an SSH trusted path between the server and users, and between servers and other devices to protect local or remote users when they log in to the system and prevent communication data from being modified or leaked.
- SNMPv3 protocol with a high encryption security level: Supports the SNMPv3 communication security protocol, SHA, and AES.
- IPMI 2.0 protocol with a high encryption security level: Supports the IPMI 2.0 communication protocol, and provides the encryption security technology with a higher level.
- Redfish interface with a high encryption security level: Supports the next-generation standard shelf management interface, with the encryption level higher than the IPMI protocol.
- Protocol and port anti-attack: Disables unused network services and high-risk ports as well as insecure protocols by default, including RMCP, Telnet.

Security Measures for User Permissions

- User role management: User permissions are allocated to logged-in users, and multiple management user roles can be allocated. Roles can be divided into different levels. By associating roles, the functional permissions of each user can be restricted to prevent unauthorized operations.
- User account security enhancement: Weak password detection, default strong password, password complexity configuration, password validity period configuration, and forbidding repeated use of the latest three historical passwords during password modification are supported.
- Authentication service: The BMC supports both local authentication access and remote authentication access. Remote access supports authentication through LDAP, and account locking upon login authentication failures. The number of login failures can be configured.
- User access restriction: User access can be restricted by port, source IP address, and MAC whitelist. The system supports the functions such as maximum number of sessions, forced exit after session timeout, configurable session expiration, multi-session concurrent restriction for a single user, online user management, and forced logout.
- Intrusion alarm: The BMC supports the chassis cover opening alarm to improve system security.
- Certificate service: The BMC supports certificate encryption and import services, which can only be operated by the administrator.

Security Measures for Log Management

- Log recording: All key system events can be recorded, including the date, time, user, event description, event result, and other related information. The BMC supports recording of component replacement logs.
- Log category: The BMC supports different log categories, including operation logs, system logs, and login logs.
- Log query: The BMC provides log information query permissions for authorized users, and supports allocating log file read permissions by account to prevent log files from being accessed illegally.
- Log protection: Logs are saved in non-volatile storage media. Log information that has been stored cannot be deleted without authorization to prevent modifying the stored log information. Logs are saved for 90 days or longer.
- Centralized alarm management: The BMC supports centralized alarm management for the faults that occur during device operation, allows authorized users to export alarms, and supports alarm reporting through SNMP Trap in a centralized manner.
- Centralized log management: The BMC allows authorized users to export logs, and supports log through Syslog in a centralized manner.
- Reliable timestamp: The BMC supports local time modification and NTP to ensure the time accuracy of system logs and alarms.

Security Measures for Data Security

- Encrypted data storage: Supports data protection, encrypted data storage, and database password authentication.
- Encrypted data transmission: Supports communication protocols with high encryption security levels such as IPMI 2.0/SNMP V3/SSH/Redfish/HTTPS and the KVM encryption function to ensure data transmission security.
- Data integrity: Supports data integrity check to ensure data verification, storage and transmission.

Security Measures for Version Management

- Version integrity check: When the server system loads software, the BMC checks the integrity of the software to prevent version confusion or malicious modification caused by error codes during transmission.
- Software upgrade permission control: The BMC records software version and firmware version information. Only the administrator has the permission to upgrade software and firmware and record related operations in logs.

- Version rollback: When an error occurs during the version upgrade process, the version can be rolled back.
- Venerability-free release of software: Before the product software is released, it passes the security scan by the security tools such as NSFOCUS, NESSUS, and WebInspect, and passes the source code scan for vulnerabilities. In addition, the product software passes several rounds of penetration tests to ensure no vulnerability.
- Redundancy: The BMC supports active/standby BMC boots, BMC versions and BMC management ports.
- Strict version release control process: The BMC supports security evaluation of the third-party software and plug-ins used. Before a version is released, the BMC scans it by using mainstream anti-virus software. SHA256 check codes are released to prevent version tempering.
- Secure and controllable BMC source code: The BMC source code passes the 100% code walkthrough and the Klocwork and Coverity white box security checks and tests, so that the potential security vulnerabilities are eliminated and the security is reinforced.

1.4 Operation Interfaces

The BMC supports common batch deployment operation interfaces and server management interfaces.

- The batch deployment operation interfaces include:
  - The IPMI is a standard server interface. It is used for interconnection with the upper-layer NMS or the monitoring software at the host side to implement the functions specified by the IPMI2.0.
  - The Redfish interface is a standard server interface. It is used for interconnection with the upper-layer NMS to monitor and manage a server.
  - The SNMP interface is a non-standard server interface. It is used for interconnection with the upper-layer NMS to monitor and manage a server.
- The server management interfaces include:
  - Web interface
  - KVM interface
  - Remote CLI

Chapter 2
Performing Client Commissioning

Abstract

In most cases, a client (namely, PC) logs in to the Web portal of the BMC through a server's iSAC management network port. Before logging in for the first time, you must debug the iSAC management network port to ensure that the communication with the client is proper.

Prerequisite

- All the needed tools are ready:
  - → A client PC
  - → Network cables
- One of the following browsers is already installed on the client PC:
  - → Google Chrome 59 or later versions
  - → Firefox 54 or later versions
  - → Microsoft IE 11 or later versions

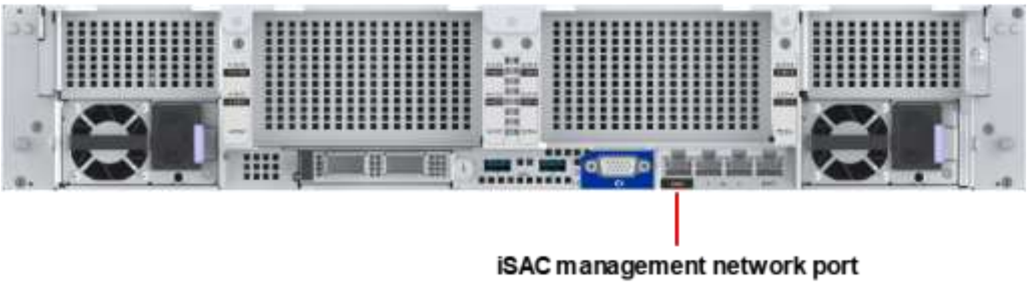
  Note

  Google Chrome 59 and later versions are recommended.
- The server is powered on.

Context

For the position of the iSAC management network port on the rear panel, see Figure 2-1.

Figure 2-1 Position of the iSAC Management Network Port



Note

The positions of the iSAC management network ports on the rear panels of the servers are basically the same. This procedure uses the position of the iSAC management network port on the rear panel of an 2230-RE server as an example.

Steps

1. Connect the client PC to the iSAC management network port on the rear panel of the server through a network cable.
2. On the client PC, change the IP address of the client PC to an IP address in the same network segment as 192.168.5.7, for example, 192.168.5.8.

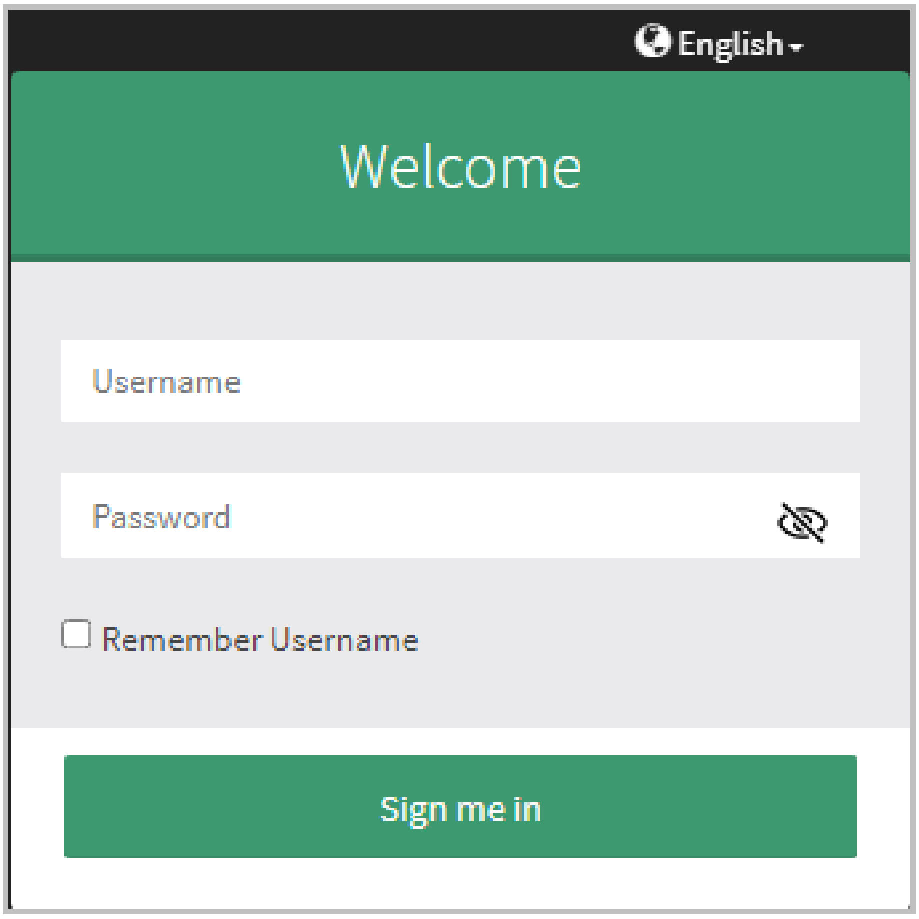
   Note

   The default IP address of the iSAC management network port of the server is 192.168.5.7.
3. On the client PC, start the browser.

   Note

   The browsers supported include Google Chrome 59, Firefox 54, Microsoft IE 11 and later versions. Google Chrome 59 and later versions are recommended.
4. In the address bar of your browser, enter *https://192.168.5.7* and press **Enter**. The **Welcome** page is displayed, see Figure 2-2.

Figure 2-2 Welcome Page



English

Welcome

Username

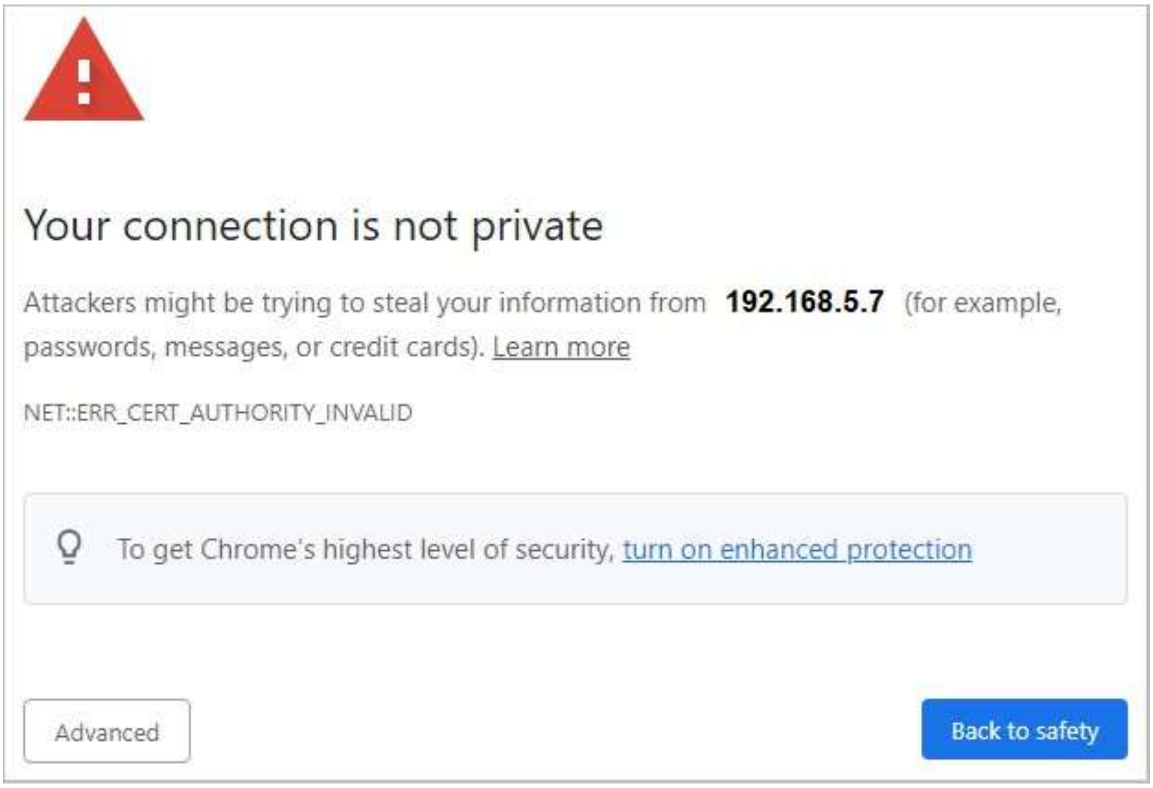
Password

□ Remember Username

Sign me in

If the following information is displayed before the **Welcome** page is displayed, click **Advanced** and select **Proceed to**. The **Welcome** page is displayed.

Figure 2-3 Security Alarm



Your connection is not private

Attackers might be trying to steal your information from **192.168.5.7** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

To get Chrome's highest level of security, turn on enhanced protection

5. Enter your username and password.

Note

The default username and password are as follows:

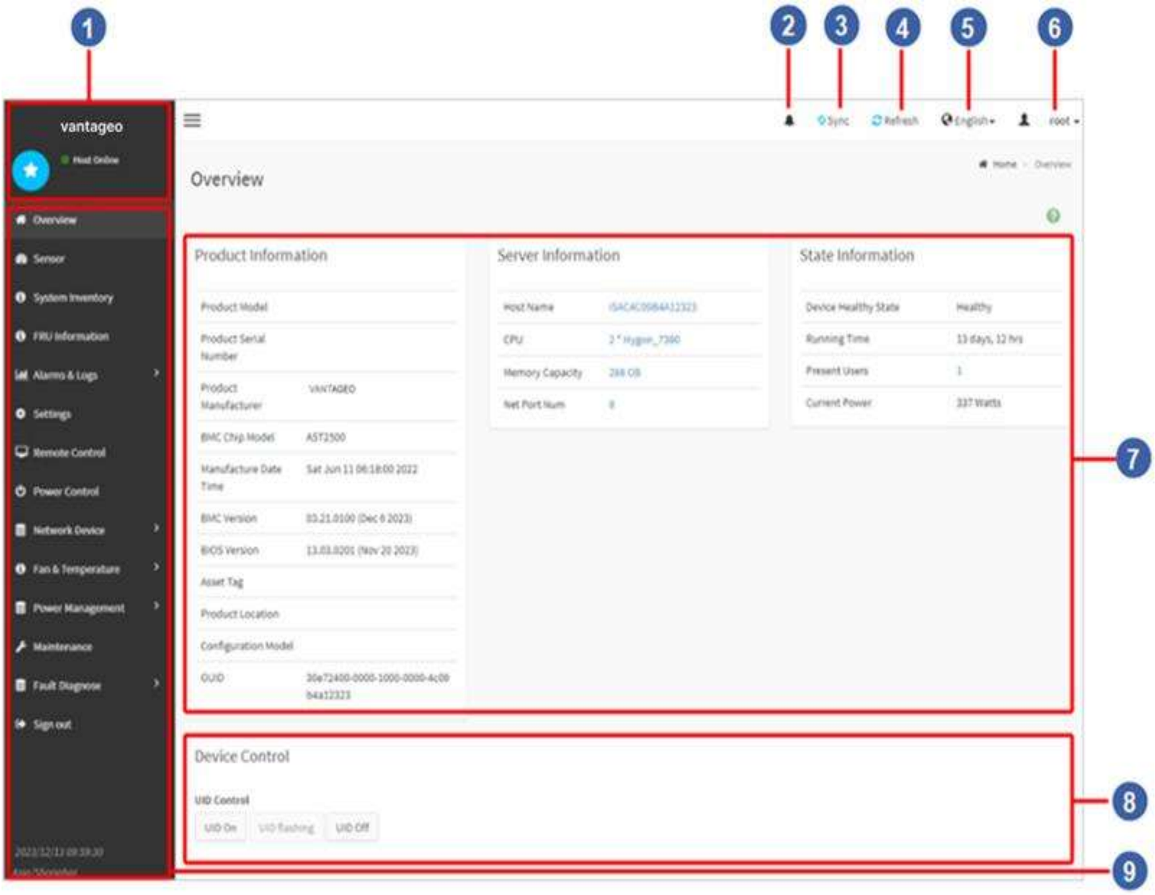
- Username: root
- Password: Superuser9!

Note

After you log in to the BMC Web portal by using the default password, you must change the default password immediately. It is recommended that you change the default password to a strong password.

6. (Optional) To remember the username, select **Remember Username**.
7. Click **Sign me in**. The home page of the Web portal of the BMC is displayed, see Figure 2-4 .

Figure 2-4 Home Page



Overview

Product Information

Product Model	
Product Serial Number	
Product Manufacturer	VANTAGEO
BMC Chip Model	AST2500
Manufacture Date Time	Sat Jun 11 06:18:00 2022
BMC Version	03.21.0100 (Dec 6 2023)
BIOS Version	13.03.0201 (Nov 20 2023)
Asset Tag	
Product Location	
Configuration Model	
OUID	30e72400-0000-1000-0000-4c09b4a12323

Server Information

Host Name	iSACAC0984A12323
CPU	2 * Hygon_7380
Memory Capacity	288 GB
Net Port Num	8

State Information

Device Healthy State	Healthy
Running Time	13 days, 12 hrs
Present Users	1
Current Power	337 Watts

Device Control

UID Control

UID On | UID Flashing | UID Off

1. Host online status
2. Alarm button
3. Synchronization button
4. Refresh button
5. Language button
6. Current user
7. Overview
8. Device control area
9. Menu bar

8. Set the IP address of the iSAC management network port as planned, for example, 10.235.53.84.

   For details, refer to "3.7.8 Configuring IP Settings".
9. Record the IP address of the iSAC management network port.
10. Connect the iSAC management network port to a switch through a network cable.
11. On the client PC, change the IP address of the client PC to one that is in the same network segment as that of the iSAC management network port, for example, 10.235.53.85.
12. Connect the client PC to the switch through a network cable.
13. Run the `ping` command in the command line on the client PC to test the connection between the client PC and the iSAC management network port.

Chapter 3

BMC Web Operations

Table of Contents

3.1 Logging In to the Web Portal of the BMC

Abstract

You can log in to the server BMC Web portal through the specified browser. On this portal, you can configure and manage the server, view server and user information, and perform KVM-based remote control.

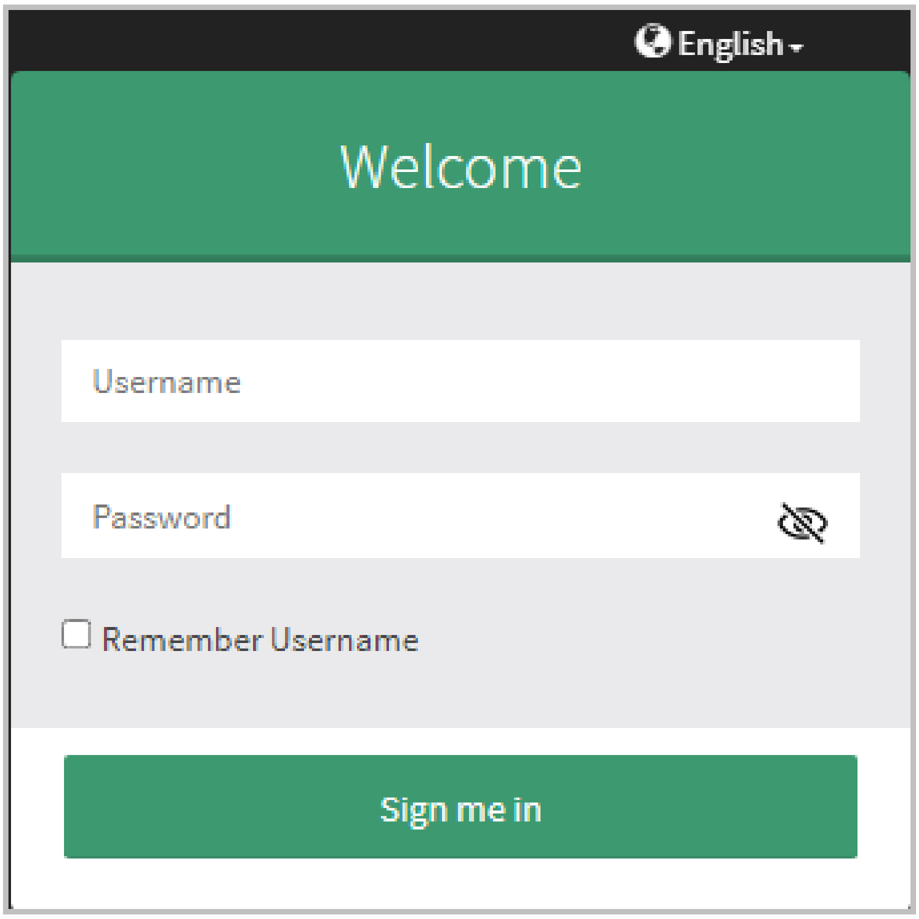
Prerequisite

The IP address of the iSAC management network port is obtained.

Steps

1. In the address bar of your browser, enter the address of the BMC Web portal, and press **Enter**. The **Welcome** page is displayed, see Figure 3-1.

Figure 3-1 Welcome Page



Note

The address format of the BMC Web portal is as follows: `https://IP`. "IP" is the IP address of the iSAC management network port.

2. Enter **Username** and **Password**.

Note

The default username and password are as follows:

- Username: root
- Password: Superuser9!

Note

After you log in to the BMC Web portal by using the default password, you must change the default password immediately. It is recommended that you change the default password to a strong password.

3. (Optional) To save the login username, select **Remember Username**.

4. Click **Sign me in**. The home page of the BMC Web portal is displayed.

Related Tasks

Log out the current user through either of the following ways:

- From the menu bar in the left pane, select **Sign Out**.
- In the upper right corner of the page, click the current user. In the displayed menu, select **Sign Out**.

3.2 Basic Operations

For the basic operations that can be performed on the BMC Web portal, refer to Table 3-1.

Table 3-1 Basic Operation Descriptions

Action	Description
View the server overview	From the menu bar in the left pane, select **Overview**. The **Overview** page displays the product information, server information and BMC status information.
View firmware version information	In the **Product Information** area on the **Overview** page, view the BMC and BIOS firmware version information.
View the online help	Click ? in the upper right corner of the page. The help information of the current page is displayed.
View the current user information	After you log in to the BMC Web portal, the current user is displayed in the upper right corner of the page. Click the current user. On the displayed page, click **My Profile**. The **My Profile** page is displayed.
Modify the current user information	1. In the upper right corner of the page, click the current user. On the displayed page, click **My Profile**. The **My Profile** page is displayed. 2. Select **Change Password** and change the password. 3. In the **Email ID** text box, enter your e-mail address. 4. Click **Save**.
Sign out the current user	In the upper right corner of the page, click the current user. On the displayed page, click **Sign Out**.
Control the UID indicator	From the menu bar in the left pane, select **Overview**. In the **Device Control** area in the lower part of the **Overview** page, you can control the UID indicator on the server panel. ● Click **UID On**. The UID indicator is turned on. ● Click **UID flashing**. The UID indicator flashes, indicating that the administrator is operating the BMC.

Action	Description
	The UID light flashes automatically when the administrator uses the BMC management backend, Web portal, KVM, and virtual media. ● Click **UID Off**. The UID indicator is turned off. An inactive button indicates the current state of the UID indicator. For example: If the **UID flashing** button is inactive, it indicates that the UID indicator is flashing.
Check alarms	Click 🔔 in the upper right corner of the page. All the alarm information received is displayed.
Synchronize sensor information and event logs	Click Sync in the upper right corner of the page. The sensor information and event logs are synchronized.
Refresh the current page	Click Refresh in the upper right corner of the page. The current page is refreshed.
Switch languages	Click the language button in the upper-right corner to change the GUI language.

3.3 Querying Sensor Information

Abstract

By querying sensor information, you can learn about the names, actual values, and operational statuses of all available sensors on the server to help understand server indicators.

Sensor types include:

- Discrete sensor: a sensor used to monitor the presence of components such as hard disks, CPUs, fans, or power supplies.
- Normal sensor: a sensor used to monitor KPIs such as temperature, voltage, fan rotation speed, or power.

Note

The **Sensor Reading** page includes the following areas:

- **Critical Sensors**
- **Discrete Sensor States**
- **Normal Sensors**
- **Disabled Sensors**

When the actual value of a normal sensor reaches or exceeds the corresponding threshold, the sensor information is displayed in the **Critical Sensors** area. When a sensor is disabled, the sensor information is displayed in the **Disabled Sensors** area.

Context

For a description of common sensors, refer to Table 3-2.

Table 3-2 Sensor Descriptions

Sensor Name	Test Object
CPU1(/2)_PCORE	Core power voltage of CPU1 or CPU2
CPU1(/2)_PSOC	SOC power voltage of CPU1 or CPU2
CPU1(/2)_VDDQ_01(/02)	01 or 02 channel memory voltage of CPU1 or CPU2
CPU1(/2)_VCC1V8	1.8 V power voltage of CPU1 or CPU2
CPU1(/2)_VCC0V9S5	0.9 V power voltage of CPU1 or CPU2
CPU1(/2)_VCC1V8S5	1.8 V power voltage of CPU1 or CPU2
BD_VCC3V3	3.3V management power voltage of the mainboard
BAT_VOLTS	CMOS battery voltage of the mainboard
INPUT_TEMP	Intake temperature of the server
OUTPUT_TEMP	Outlet temperature of the server
SYS_TEMP_01	Mainboard temperature of the server
CPU_TEMP_01(/02)	Core temperature of CPU1 or CPU2
CPU_STATUS_01(/02)	Presence status of CPU1 or CPU2
PSU_STATUS_01(/02)	Presence status of the server power module 1 or 2
MEM_TEMP_*1	Surface temperature of each memory bar of the server
FAN_SPEED_01F(/01R/02F/02R/03F/03R/04F/04R)	Actual rotation speed of each fan on the server Only 8056 fans support FAN_SPEED_01R/02R/03R/04R.
FAN_STATUS_01(/02/03/04)	Presence status of each fan on the server
POWER_WATTS	Overall power consumption of the server
INPUT_VOLTS_01(/02)	Input voltage of the server power module 1 or 2
OUTPUT_VOLTS_01(/02)	Working voltage input to the mainboard by the server power module 1 or 2
CPU_VOLTS_01(/02)	Core voltage output by the power supply chip of CPU1 or CPU2
MEM_VOLTS_*1	Power voltage output by the power supply chip of the memory bar on the mainboard

Sensor Name	Test Object
VCORE_TEMP01(/02)	Temperature of the power supply chip for the VCORE voltage of CPU1 or CPU2
PSOC_TEMP_01(/02)	Temperature of the power supply chip for the SOC voltage of CPU1 or CPU2
VDDQ_TEMP_01(/02)_1(/2)	Temperature of the power supply chip for the 01 or 02 channel memory voltage of CPU1 or CPU2
INTRUSION	Cover opening intrusion protection alarm of the server
MEM_STATUS_*1	Presence status of each memory bar on the server

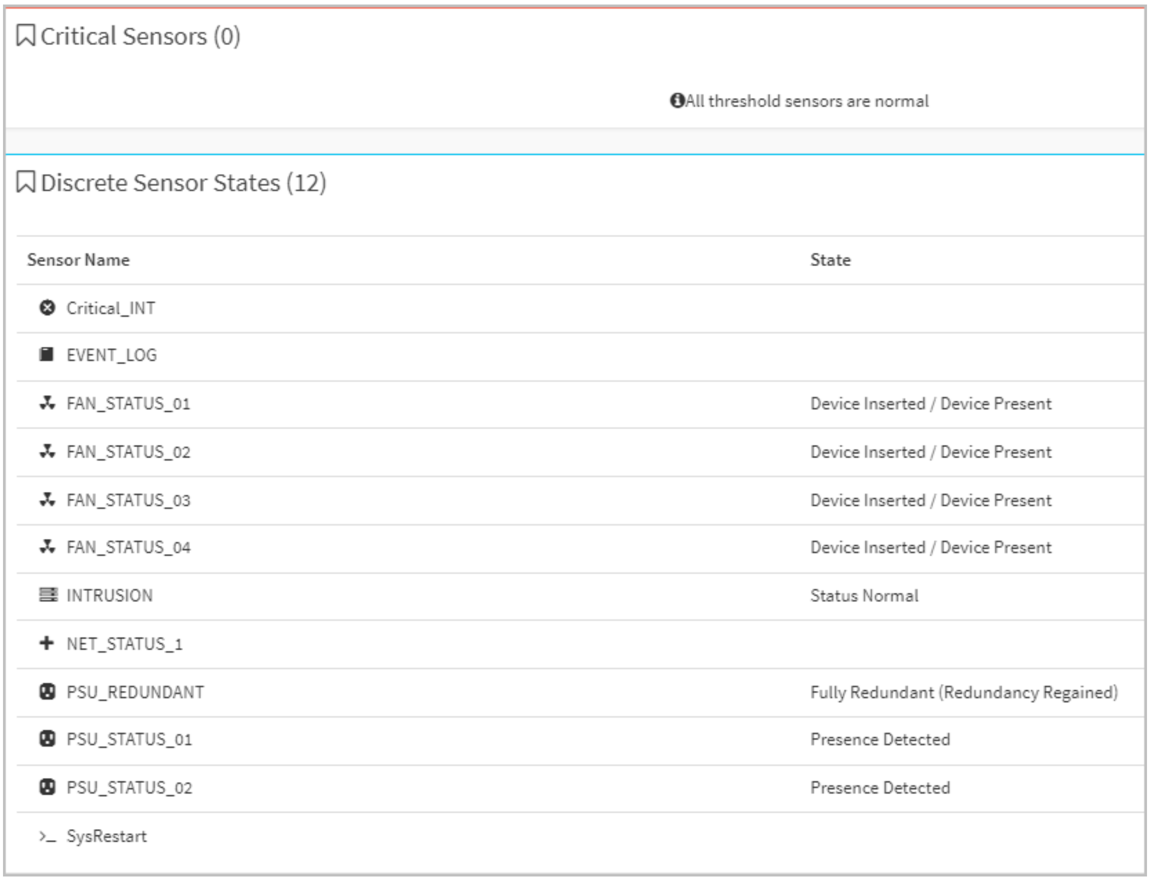
Note

***1** is the 32 memory bars represented by 1A1–2H2.

Steps

1. From the menu bar in the left pane, select **Sensor**. The **Sensor Reading** page is displayed, see Figure 3-2.

Figure 3-2 Sensor Reading Page



Critical Sensors (0)

All threshold sensors are normal

Discrete Sensor States (12)

Sensor Name	State
Critical_INT	
EVENT_LOG	
FAN_STATUS_01	Device Inserted / Device Present
FAN_STATUS_02	Device Inserted / Device Present
FAN_STATUS_03	Device Inserted / Device Present
FAN_STATUS_04	Device Inserted / Device Present
INTRUSION	Status Normal
NET_STATUS_1	
PSU_REDUNDANT	Fully Redundant (Redundancy Regained)
PSU_STATUS_01	Presence Detected
PSU_STATUS_02	Presence Detected
SysRestart	

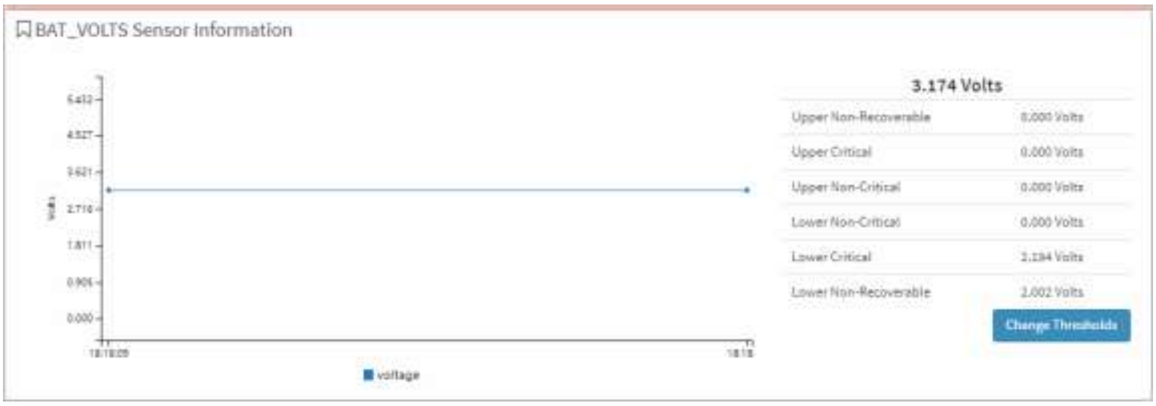
Note

The **Sensor Reading** page is long, so only a part of it is displayed here.

2. (Optional) Click the icon or name of the sensor whose detailed information is to be viewed.

   The **Sensor Detail** page is displayed, see Figure 3-3.

Figure 3-3 Sensor Detail Page



BAT_VOLTS Sensor Information

3.174 Volts

Upper Non-Recoverable	0.000 Volts
Upper Critical	0.000 Volts
Upper Non-Critical	0.000 Volts
Lower Non-Critical	0.000 Volts
Lower Critical	2.134 Volts
Lower Non-Recoverable	2.002 Volts

3. (Optional) Click **Change Thresholds** to change the alarm thresholds for the sensor.

Note

Thresholds can be changed for only **Normal Sensors**.

3.4 Querying System Inventory

Abstract

By querying the system inventory, you can learn about the status and details of the CPU and memory of the server.

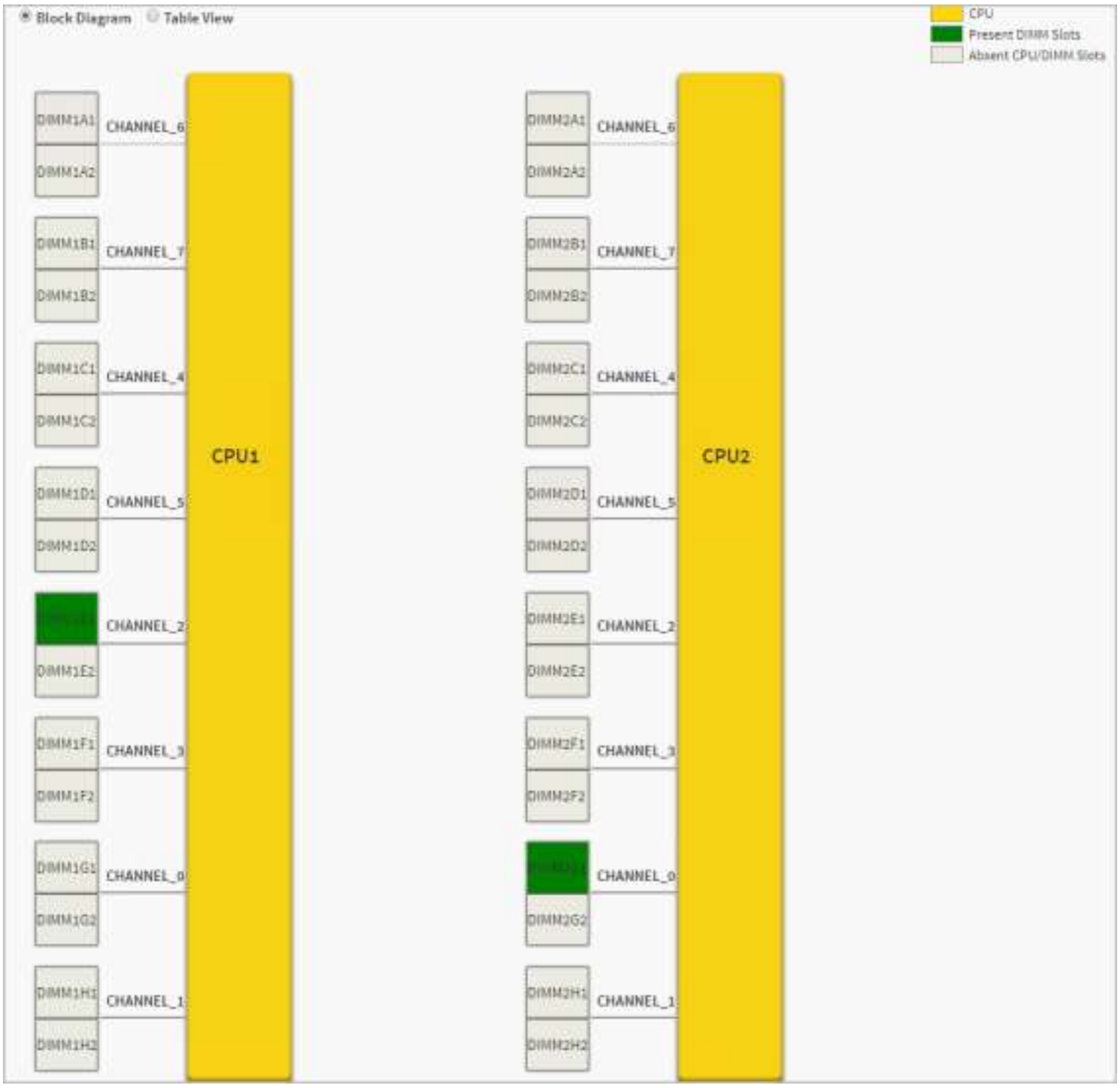
Note

The CPU, memory, and their corresponding relationships can be displayed in a block diagram or tabular form.

Steps

1. From the menu bar in the left pane, select **System Inventory**. The **System Inventory** page is displayed, see Figure 3-4.

Figure 3-4 System Inventory—Block Diagram



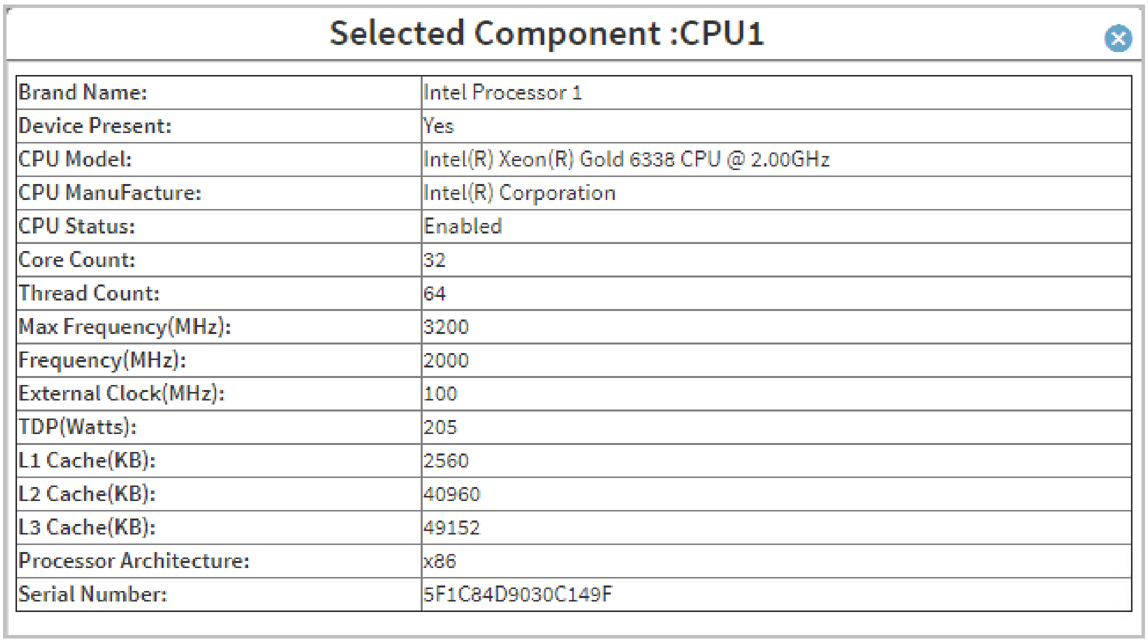
Note

The colors in the device block diagram have the following meanings:

- Yellow: The CPU is present.
- Green: The memory is present.
- Grey: The memory is not present.

2. (Optional) To view the details of a component present, click the component. For example, click any area of **CPU1**, the details of CPU1 are displayed, see Figure 3-5.

Figure 3-5 CPU1 Details Page

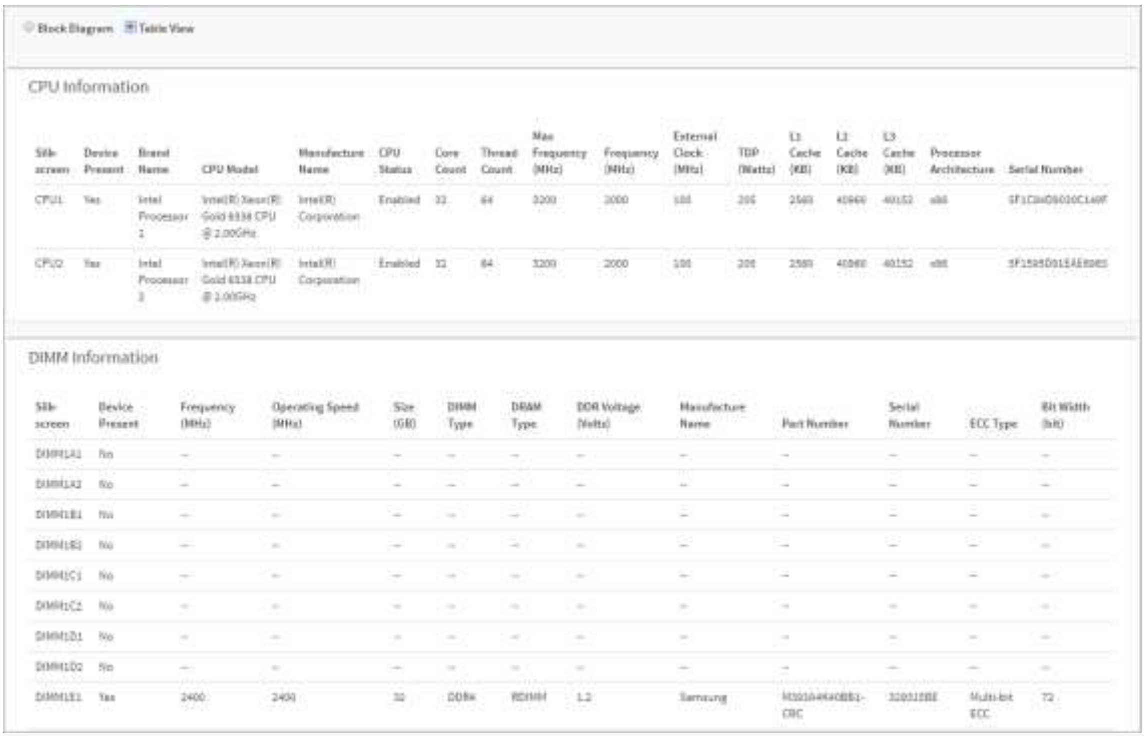


Selected Component :CPU1

Brand Name:	Intel Processor 1
Device Present:	Yes
CPU Model:	Intel(R) Xeon(R) Gold 6338 CPU @ 2.00GHz
CPU ManuFacture:	Intel(R) Corporation
CPU Status:	Enabled
Core Count:	32
Thread Count:	64
Max Frequency(MHz):	3200
Frequency(MHz):	2000
External Clock(MHz):	100
TDP(Watts):	205
L1 Cache(KB):	2560
L2 Cache(KB):	40960
L3 Cache(KB):	49152
Processor Architecture:	x86
Serial Number:	5F1C84D9030C149F

3. (Optional) On the **System Inventory** page, select **Table View**. The system inventory is displayed in a tabular form, see Figure 3-6.

Figure 3-6 System Inventory—Table



CPU Information

Silk-screen	Device Present	Brand Name	CPU Model	Manufacture Name	CPU Status	Core Count	Thread Count	Max Frequency (MHz)	Frequency (MHz)	External Clock (MHz)	TDP (Watts)	L1 Cache (KB)	L2 Cache (KB)	L3 Cache (KB)	Processor Architecture	Serial Number
CPU1	Yes	Intel Processor 1	Intel(R) Xeon(R) Gold 6338 CPU @ 2.00GHz	Intel(R) Corporation	Enabled	32	64	3200	2000	100	205	2560	40960	49152	x86	5F1C84D9030C149F
CPU2	Yes	Intel Processor 2	Intel(R) Xeon(R) Gold 6338 CPU @ 2.00GHz	Intel(R) Corporation	Enabled	32	64	3200	2000	100	205	2560	40960	49152	x86	5F1585D015AE8065

DIMM Information

Silk-screen	Device Present	Frequency (MHz)	Operating Speed (MHz)	Size (GB)	DIMM Type	DRAM Type	DDR Voltage (Volts)	Manufacture Name	Part Number	Serial Number	ECC Type	Bit Width (bit)
DIMM1A1	No	--	--	--	--	--	--	--	--	--	--	--
DIMM1A2	No	--	--	--	--	--	--	--	--	--	--	--
DIMM1B1	No	--	--	--	--	--	--	--	--	--	--	--
DIMM1B2	No	--	--	--	--	--	--	--	--	--	--	--
DIMM1C1	No	--	--	--	--	--	--	--	--	--	--	--
DIMM1C2	No	--	--	--	--	--	--	--	--	--	--	--
DIMM1D1	No	--	--	--	--	--	--	--	--	--	--	--
DIMM1D2	No	--	--	--	--	--	--	--	--	--	--	--
DIMM1E1	Yes	2400	2400	32	DDR4	RDIMM	1.2	Samsung	M393A4K40BB1-CRC	320312BE	Multi-bit ECC	72

Note

The **System Inventory** page is long, so only a part of it is displayed here.

3.5 Querying FRU Information

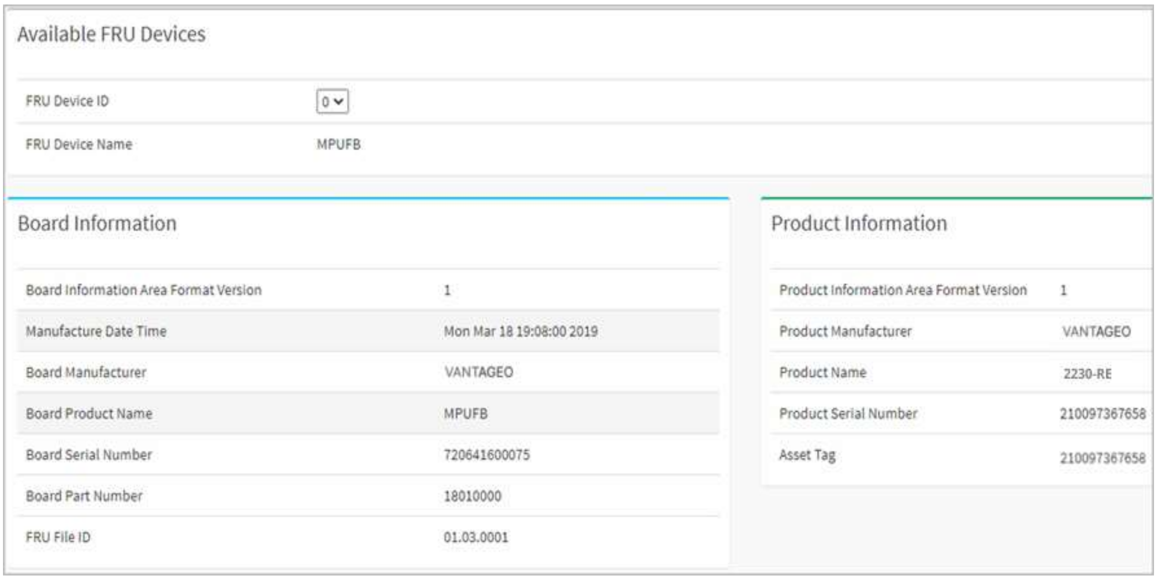
Abstract

FRUs include the mainboard, backplane, and cards that can be replaced on site. Before replacement, you must query the FRU information to learn about the details of the replaceable unit to be replaced.

Steps

1. From the menu bar in the left pane, select **FRU Information**. The **FRU** page is displayed, see Figure 3-7.

   Figure 3-7 FRU Page

   Available FRU Devices

FRU Device ID	0
FRU Device Name	MPUFB

   Board Information

Board Information Area Format Version	1
Manufacture Date Time	Mon Mar 18 19:08:00 2019
Board Manufacturer	VANTAGEO
Board Product Name	MPUFB
Board Serial Number	720641600075
Board Part Number	18010000
FRU File ID	01.03.0001

   Product Information

Product Information Area Format Version	1
Product Manufacturer	VANTAGEO
Product Name	2230-RE
Product Serial Number	210097367658
Asset Tag	210097367658

2. From the **FRU Device ID** list, select the slot number of the FRU device. The detailed information of the FRU device is displayed in the lower part of the page.

3.6 Alarm and Log Query

3.6.1 Querying Alarms

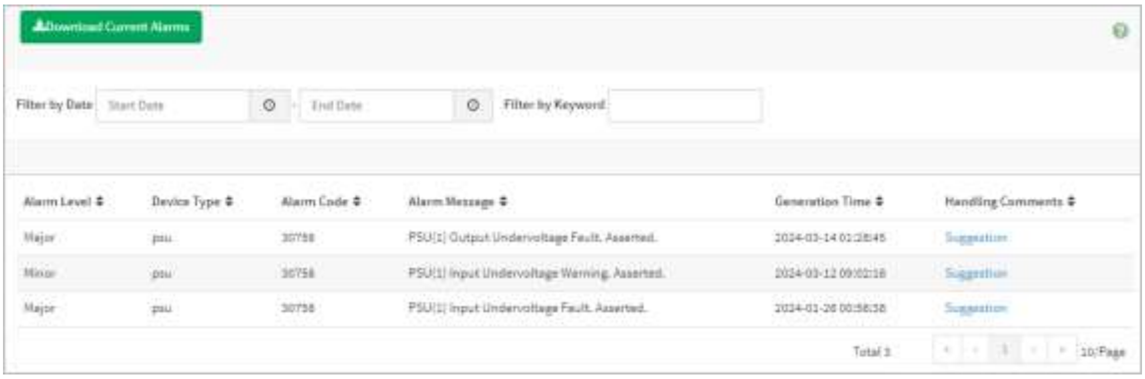
Abstract

By querying alarms, you can learn about the alarm information of the actual system events on the server.

Steps

1. From the menu bar in the left pane, select **Alarms & Logs > Current Alarm**. The **Current Alarm** page is displayed, see Figure 3-8.

Figure 3-8 Current Alarm Page



Alarm Level	Device Type	Alarm Code	Alarm Message	Generation Time	Handling Comments
Major	psu	30758	PSU[1] Output Undervoltage Fault. Asserted.	2024-03-14 01:28:45	Suggestion
Minor	psu	30758	PSU[1] Input Undervoltage Warning. Asserted.	2024-03-12 09:02:18	Suggestion
Major	psu	30758	PSU[1] Input Undervoltage Fault. Asserted.	2024-01-28 00:58:38	Suggestion

Total 3 1 10/Page

2. Perform the following operations as required.

To...	Do...
Filter alarms by date	Click 🕘 in the **Filter by Date** area and set the start date and end date for querying operation alarms.
Filter alarms by keyword	a. In the **Filter by Keyword** text box, enter a keyword. b. Press **Enter**. The results filtered by the keyword are displayed on the page.
Save the alarm information to the local PC	Click **Download Current Alarms** and save the alarm information to the local PC.

3.6.2 Querying Login Logs

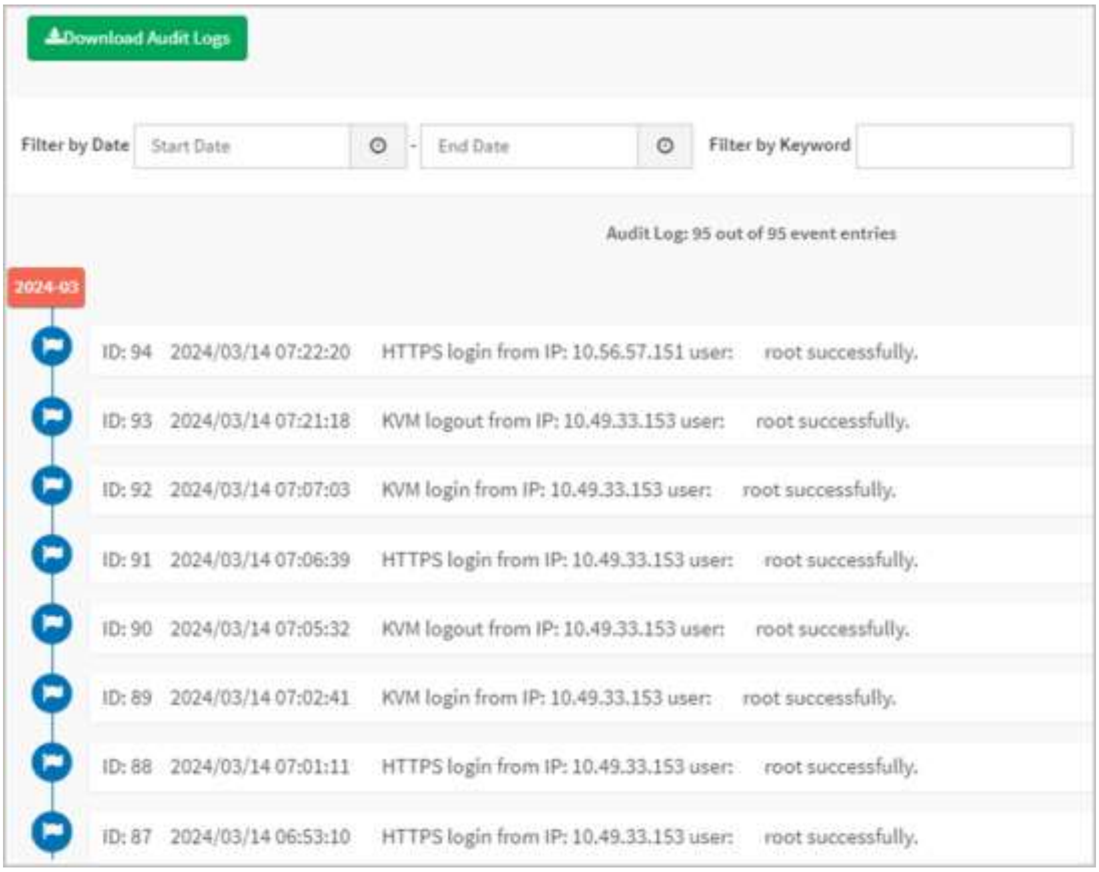
Abstract

Login logs record user logins and logouts of the BMC Web portal, BMC command lines, and KVM information.

Steps

1. From the menu bar in the left pane, select **Alarms & Logs > Audit Log**. The **Audit Log** page is displayed, see Figure 3-9.

Figure 3-9 Audit Log Page



Audit Log: 95 out of 95 event entries

```
ID: 94   2024/03/14 07:22:20   HTTPS login from IP: 10.56.57.151 user:   root successfully.
ID: 93   2024/03/14 07:21:18   KVM logout from IP: 10.49.33.153 user:   root successfully.
ID: 92   2024/03/14 07:07:03   KVM login from IP: 10.49.33.153 user:   root successfully.
ID: 91   2024/03/14 07:06:39   HTTPS login from IP: 10.49.33.153 user:   root successfully.
ID: 90   2024/03/14 07:05:32   KVM logout from IP: 10.49.33.153 user:   root successfully.
ID: 89   2024/03/14 07:02:41   KVM login from IP: 10.49.33.153 user:   root successfully.
ID: 88   2024/03/14 07:01:11   HTTPS login from IP: 10.49.33.153 user:   root successfully.
ID: 87   2024/03/14 06:53:10   HTTPS login from IP: 10.49.33.153 user:   root successfully.
```

2. Perform the following operations as required.

To...	Do...
Filter logs by date	Click 🕘 in the **Filter by Date** area and set the start date and end date for querying login logs.
Filter logs by keyword	a. In the **Filter by Keyword** text box, enter a keyword. b. Press **Enter**. The results filtered by the keyword are displayed on the page.
Save logs to the local PC	Click **Download Audit Logs** and save the login logs to the local PC.

3.6.3 Querying Operation Logs

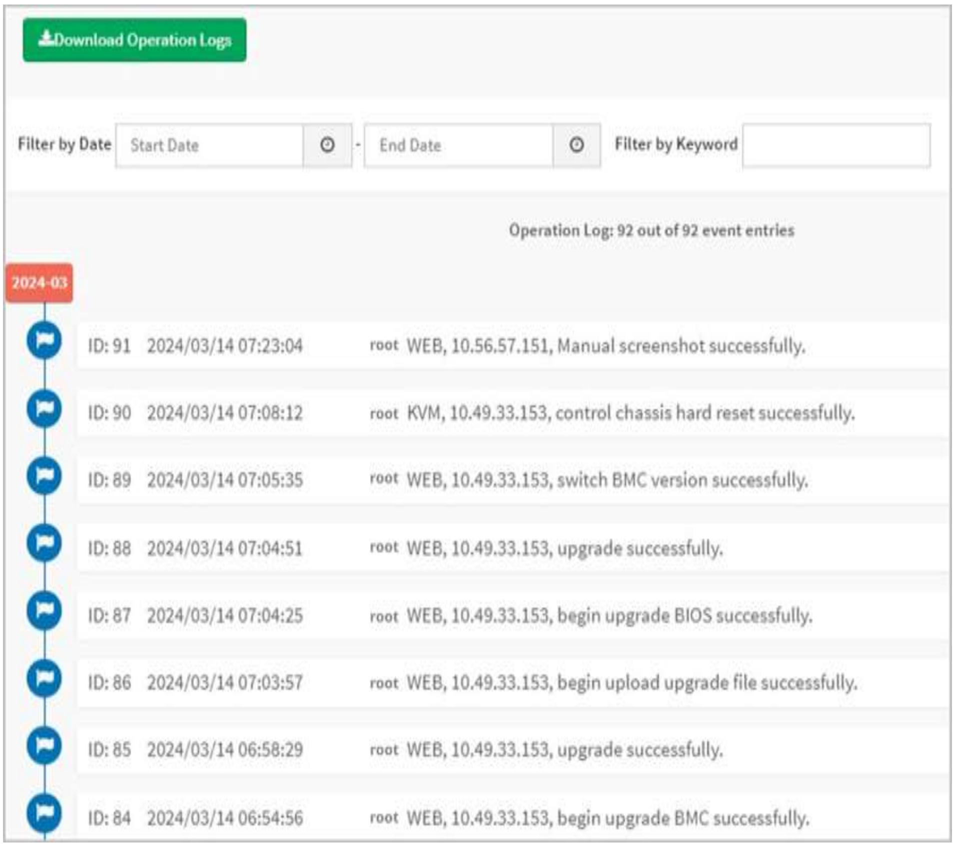
Abstract

Operation logs record the information about users' operations on the server, including manual server operations and remote server operations.

Steps

1. From the menu bar in the left pane, select **Alarms & Logs > Operation Log**. The **Operation Log** page is displayed, see Figure 3-10.

Figure 3-10 Operation Log Page



Operation Log: 92 out of 92 event entries

```
ID: 91   2024/03/14 07:23:04   root  WEB, 10.56.57.151, Manual screenshot successfully.
ID: 90   2024/03/14 07:08:12   root  KVM, 10.49.33.153, control chassis hard reset successfully.
ID: 89   2024/03/14 07:05:35   root  WEB, 10.49.33.153, switch BMC version successfully.
ID: 88   2024/03/14 07:04:51   root  WEB, 10.49.33.153, upgrade successfully.
ID: 87   2024/03/14 07:04:25   root  WEB, 10.49.33.153, begin upgrade BIOS successfully.
ID: 86   2024/03/14 07:03:57   root  WEB, 10.49.33.153, begin upload upgrade file successfully.
ID: 85   2024/03/14 06:58:29   root  WEB, 10.49.33.153, upgrade successfully.
ID: 84   2024/03/14 06:54:56   root  WEB, 10.49.33.153, begin upgrade BMC successfully.
```

2. Perform the following operations as required.

To...	Do...
Filter logs by date	Click 🕘 in the **Filter by Date** area and set the start date and end date for querying operation logs.
Filter logs by keyword	a. In the **Filter by Keyword** text box, enter a keyword. b. Press **Enter**. The results filtered by the keyword are displayed on the page.
Save logs to the local PC	Click **Download Operation Logs** and save the operation logs to the local PC.

3.6.4 Querying System Logs

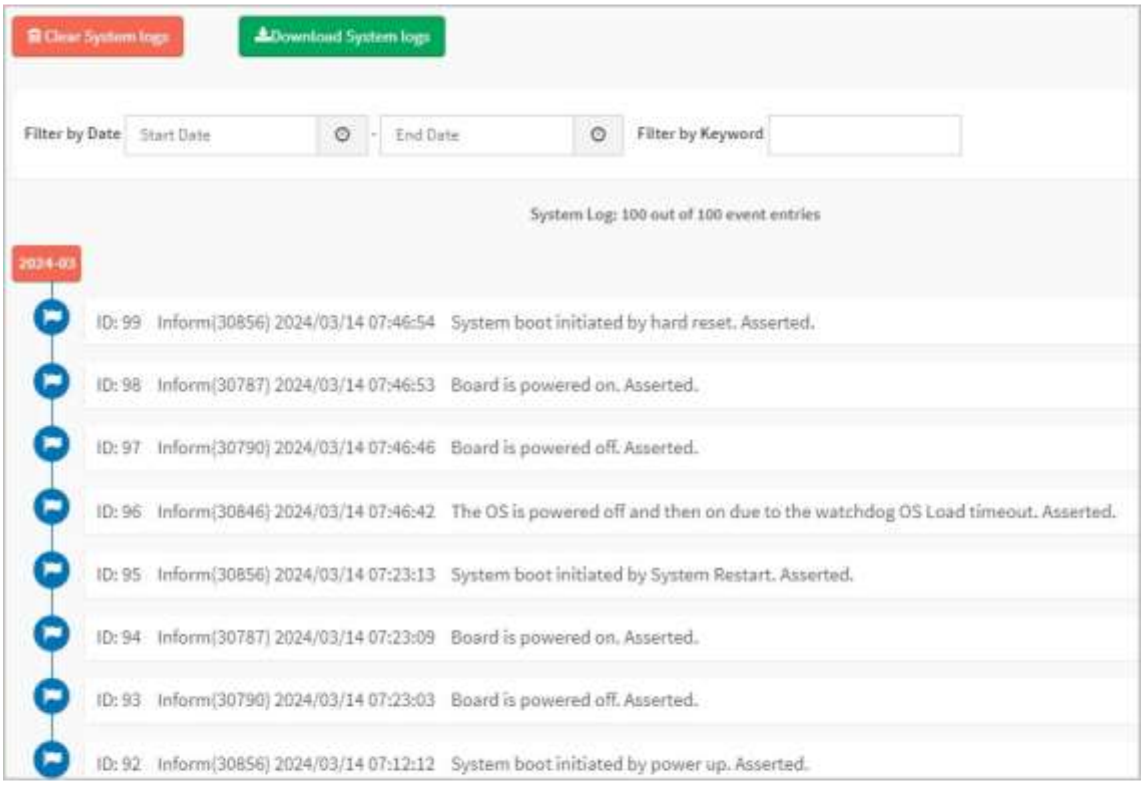
Abstract

System logs record log and alarm information generated during the operation of the server.

Steps

1. From the menu bar in the left pane, select **Alarms & Logs > System Log**. The **System Log** page is displayed, see Figure 3-11.

Figure 3-11 System Log Page



System Log: 100 out of 100 event entries

```
ID: 99   Inform(30856) 2024/03/14 07:46:54   System boot initiated by hard reset. Asserted.
ID: 98   Inform(30787) 2024/03/14 07:46:53   Board is powered on. Asserted.
ID: 97   Inform(30790) 2024/03/14 07:46:46   Board is powered off. Asserted.
ID: 96   Inform(30846) 2024/03/14 07:46:42   The OS is powered off and then on due to the watchdog OS Load timeout. Asserted.
ID: 95   Inform(30856) 2024/03/14 07:23:13   System boot initiated by System Restart. Asserted.
ID: 94   Inform(30787) 2024/03/14 07:23:09   Board is powered on. Asserted.
ID: 93   Inform(30790) 2024/03/14 07:23:03   Board is powered off. Asserted.
ID: 92   Inform(30856) 2024/03/14 07:12:12   System boot initiated by power up. Asserted.
```

2. Perform the following operations as required.

To...	Do...
Filter logs by date	Click 🕘 in the **Filter by Date** area and set the start date and end date for querying system logs.
Filter logs by keyword	a. In the **Filter by Keyword** text box, enter a keyword. b. Press **Enter**. The results filtered by the keyword are displayed on the page.
Save logs to the local PC	Click **Download System Logs** and save the system logs to the local PC.
Clear logs	Click **Clear System Logs** to clear logs.

3.6.5 Querying Event Logs

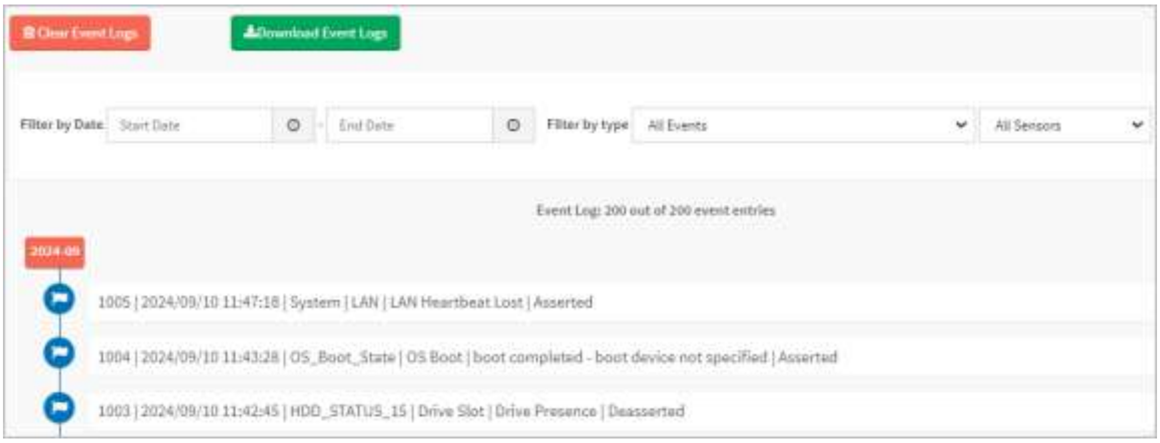
Abstract

Event logs record event information generated during the operation of the server.

Steps

1. From the menu bar in the left pane, select **Alarms & Logs > Event Log**. The **Event Log** page is displayed, see Figure 3-12.

Figure 3-12 Event Log Page



Event Log: 200 out of 200 event entries

```
1005 | 2024/09/10 11:47:18 | System | LAN | LAN Heartbeat Lost | Asserted
1004 | 2024/09/10 11:43:28 | OS_Boot_State | OS Boot | boot completed - boot device not specified | Asserted
1003 | 2024/09/10 11:42:45 | HDD_STATUS_15 | Drive Slot | Drive Presence | Deasserted
```

2. Perform the following operations as required.

To...	Do...
Filter logs by date	Click ◷ in the **Filter by Date** area and set the start date and end date for querying system logs.
Filter logs by event type	From the **Filter by type** list, select the event log type to be queried.
Filter logs by sensor	From the Sensor list, select the sensor to be queried.
Save logs to the local PC	Click **Download Event Logs** and save the event logs to the local PC.
Clear logs	Click **Clear Event Logs** to clear logs.

3.6.6 Querying Video Logs

Abstract

Video logs record the contents displayed on the screen before a server crashes, restarts, or is powered off.

Prerequisite

The video recording function is enabled. For details, refer to "3.7.25 Configuring Screen Recording Parameters".

Steps

1. From the menu bar in the left pane, select **Alarms & Logs > Video Log**. The **Video Log** page is displayed.
2. Perform the following operations as required.

To...	Do...
Filter logs by date	Click 🕘 in the **Filter by Date** area and set the start date and end date for querying video logs.
Play video logs	In the log list, click the details of the video logs that you want to play. A dialog box for playing videos is displayed.
Clear logs	Click ⊗ on the right side of the logs that you want to clear.

3.7 Configuration Management

3.7.1 Configuring the Time Synchronization Mode

Abstract

This procedure describes how to configure the time synchronization mode so that the BMC can obtain the correct time.

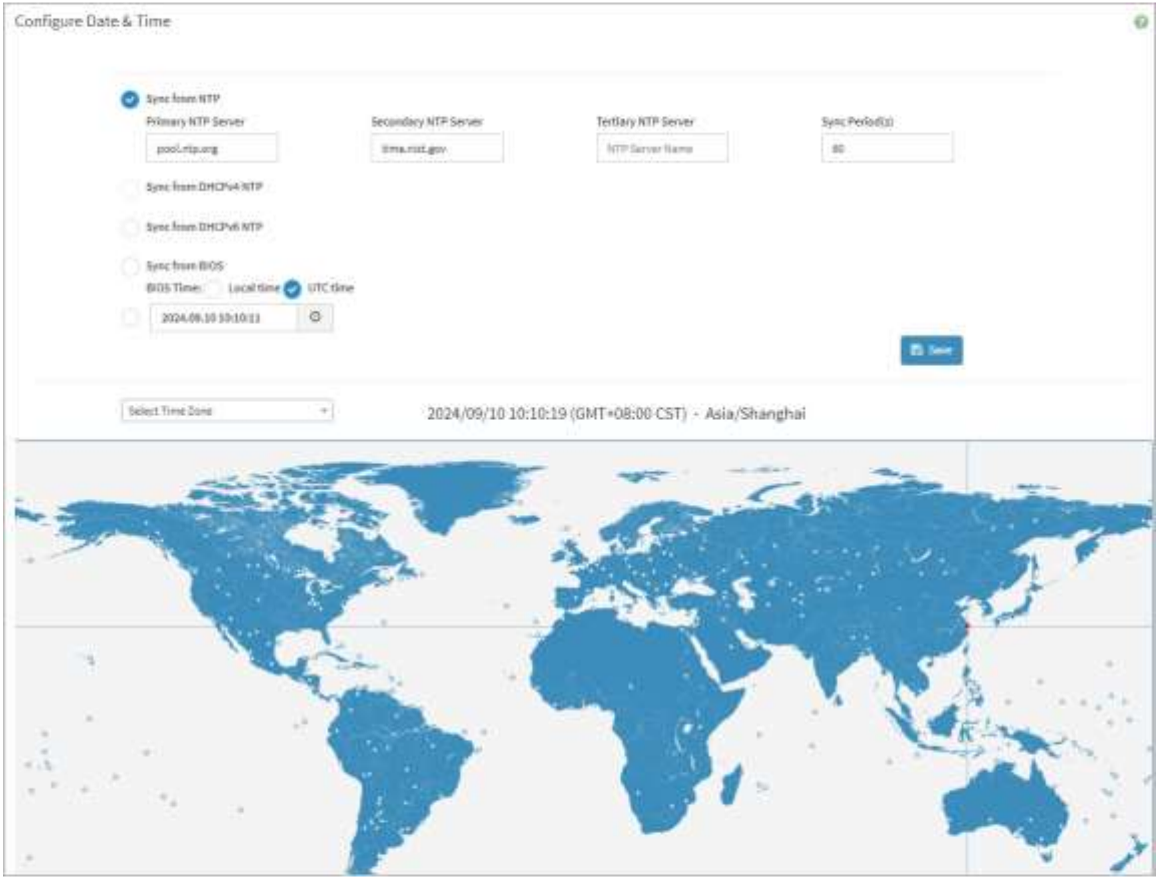
Prerequisite

To select **Sync from DHCPv4 NTP** or **Sync from DHCPv6 NTP**, you must enable the DHCP function on the management network port or shared network port. For details, refer to "3.7.8 Configuring IP Settings".

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Date & Time**. The **Date & Time** page is displayed, see Figure 3-13.

Figure 3-13 Date & Time Page



Configure Date & Time

● Sync from NTP

Primary NTP Server: pool.ntp.org

Secondary NTP Server: time.nist.gov

Tertiary NTP Server: NTP Server Name

Sync Period(s): 60

○ Sync from DHCPv4 NTP

○ Sync from DHCPv6 NTP

○ Sync from BIOS

BIOS Time: ○ Local time ● UTC time

□ 2024.09.10 10:10:11

2024/09/10 10:10:19 (GMT+08:00 CST) - Asia/Shanghai

3. Select the BMC time synchronization mode and configure the corresponding parameters.

To...	Do...
Perform NTP-based synchronization	a. Select **Syn from NTP**. b. Configure the following parameters: ● Primary NTP Server: Enter the IP address or FQDN of the primary NTP server, with the length not exceeding 127 characters. This parameter is required. ● Secondary NTP Server: Enter the IP address or FQDN of the secondary NTP server, with the length not exceeding 127 characters. The parameter is optional. ● Tertiarydary NTP Server: Enter the IP address or FQDN of the tertiary NTP server, with the length not exceeding 127 characters. The parameter is optional. ● Sync Period(s): Enter the time synchronization period in seconds, range: 60–65535. The parameters of the three NTP servers cannot be the same.
Perform DHCPv4 NTP–based synchronization	Select **Sync from DHCPv4 NTP**.

To...	Do...
Perform DHCPv6 NTP–based synchronization	Select **Sync from DHCPv6 NTP**.
Perform BIOS-based synchronization	a. Select **Syn from BIOS**. b. Configure **BIOS Time**: ● If the server runs the Linux operating system, select either **Local time** or **UTC time**, and configure the time zone the same as that of the server. ● If the server runs the Windows operating system and the operating system uses UTC time, select either **Local time** or **UTC time**, and configure the time zone to **0**. ● If the server runs the Windows operating system and the operating system uses local time, select **Local time**, and configure the time zone the same as that of the server. UTC time is the universal time coordinated (UTC time = local time - time zone difference). For example, if Beijing time is 08:00, the UTC time is 00:00.

Note

If **Sync from NTP** is selected as the time synchronization mode, the BMC synchronizes with **Primary NTP Server** first. If the synchronization fails, the BMC will synchronize time with **Secondary NTP Server** and **Tertiarydary NTP Server** in turn.

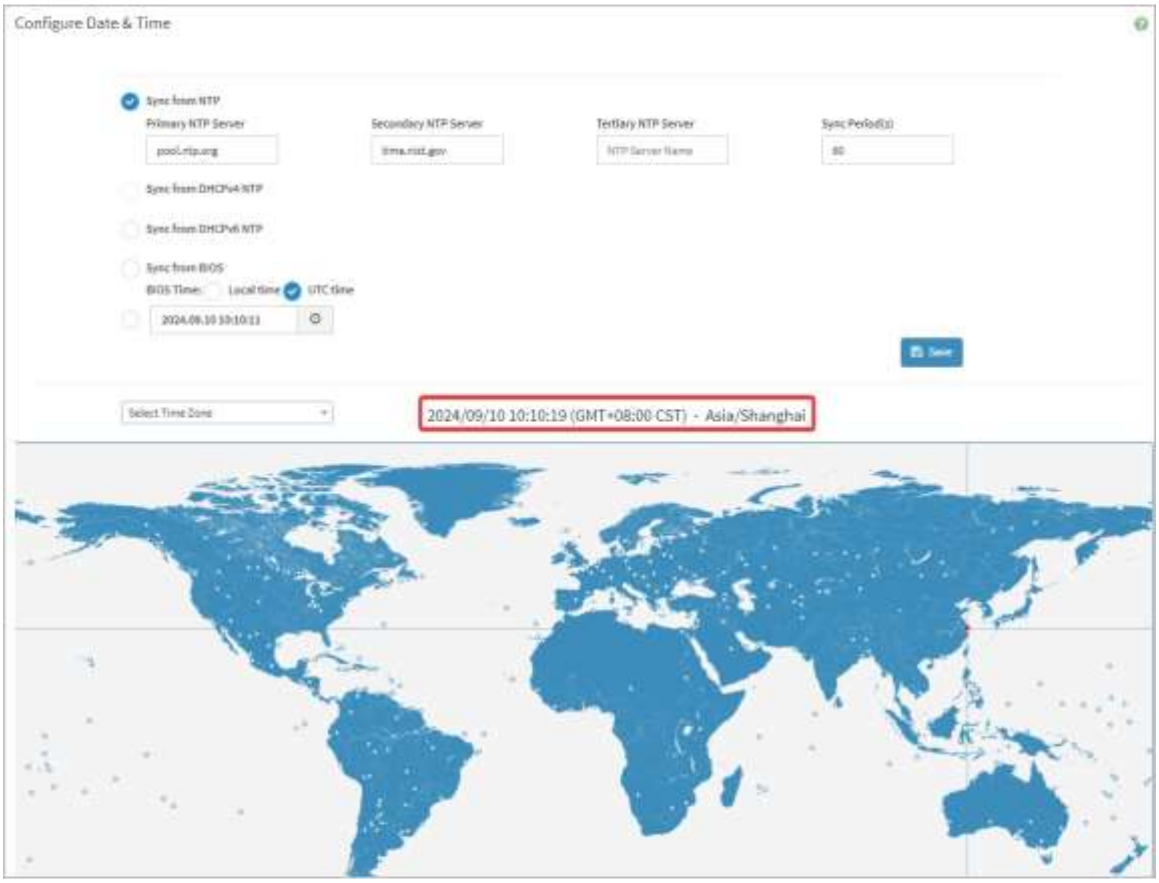
4. Click **Save.**

Verification

If **Sync from NTP** is selected, perform the following operations to check time consistency:

1. Check the date and time on the **Configure Date & Time** page, see Figure 3-14.

Figure 3-14 Configure Date & Time Page



Configure Date & Time

● Sync from NTP

Primary NTP Server: pool.ntp.org

Secondary NTP Server: time.nist.gov

Tertiary NTP Server: NTP Server Name

Sync Period(s): 80

○ Sync from DHCPv4 NTP

○ Sync from DHCPv6 NTP

○ Sync from BIOS

BIOS Time: ○ Local time ● UTC time

○ 2024.09.10 10:10:11

2024/09/10 10:10:19 (GMT+08:00 CST) - Asia/Shanghai

2. Check the NTP server to see if the time is consistent with the time of the BMC.

3.7.2 Configuring Authentication Parameters for External Users

Abstract

To authenticate external users through the LDAP server or AD server, you must configure authentication parameters for external users.

Note

External users refer to non-BMC users.

Prerequisite

The following parameters of the LDAP server or AD server are obtained:

- LDAP server
  - → Server address
  - → Port
  - → Bound identity name
  - → Password

- → Search base
- → User login attribute
- → CA file
- → Certificate file
- → Private key
- → Group name
- → Group domain

Note

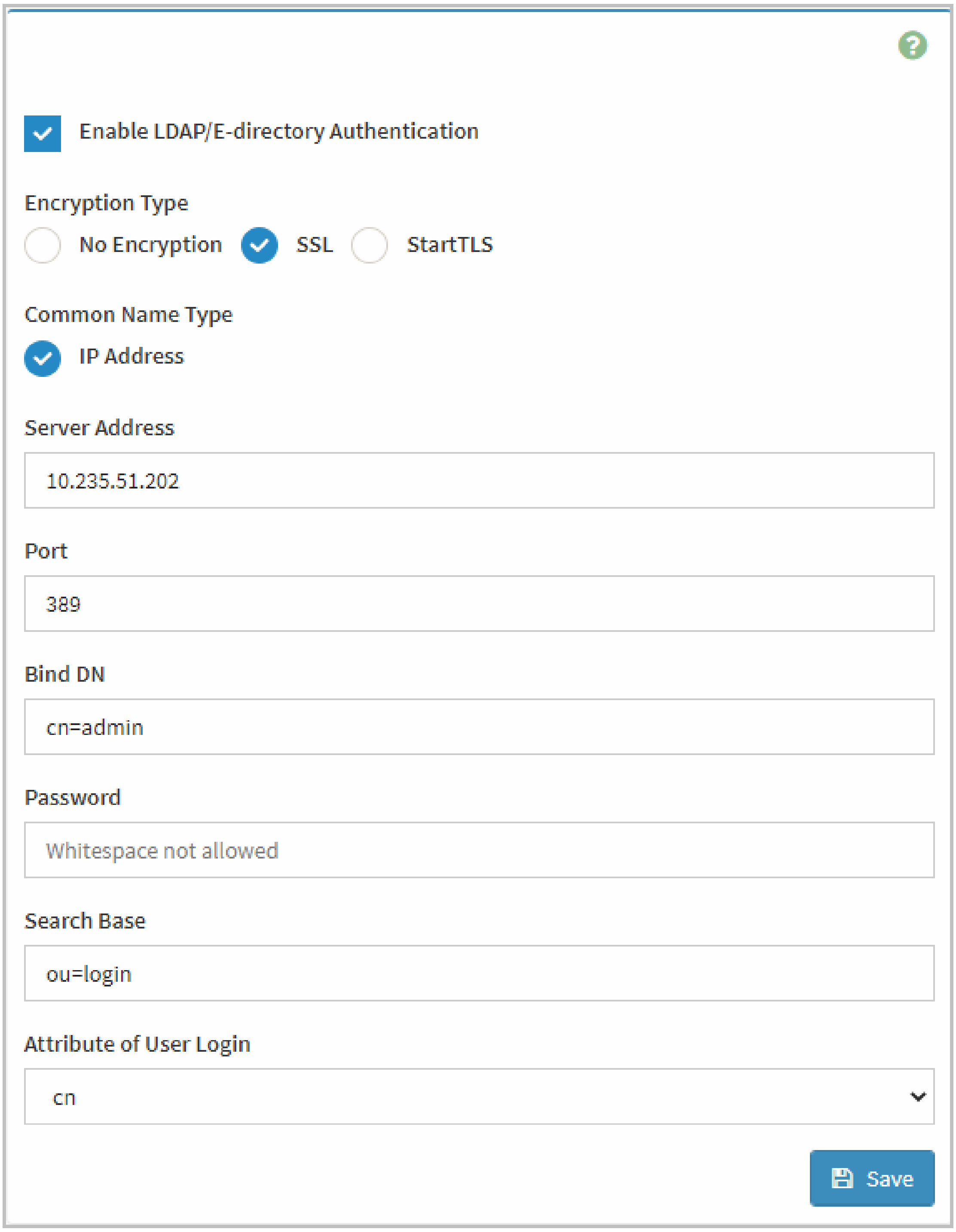
If **Encryption Type** is set to **StarTLS**, the following parameters are needed:
- → CA file
- → Certificate file
- → Private key

- AD server
  - → Username
  - → Password
  - → User's domain name
  - → Server address of the domain controller
  - → Group name
  - → Group domain

Steps

- Configuring LDAP Server Authentication Parameters
  1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
  2. Click **External User Services**. The **External User Services** page is displayed.
  3. Click **LDAP/E-directory Settings**. The **LDAP/E-directory Settings** page is displayed.
  4. Click **General Settings**. The **General LDAP Settings** page is displayed, see Figure 3-15.

Figure 3-15 General LDAP Settings Page



☑ Enable LDAP/E-directory Authentication

Encryption Type

○ No Encryption ● SSL ○ StartTLS

Common Name Type

● IP Address

Server Address

10.235.51.202

Port

389

Bind DN

cn=admin

Password

Whitespace not allowed

Search Base

ou=login

Attribute of User Login

cn

5. Configure the parameters. For a description of the parameters, refer to Table 3-3.

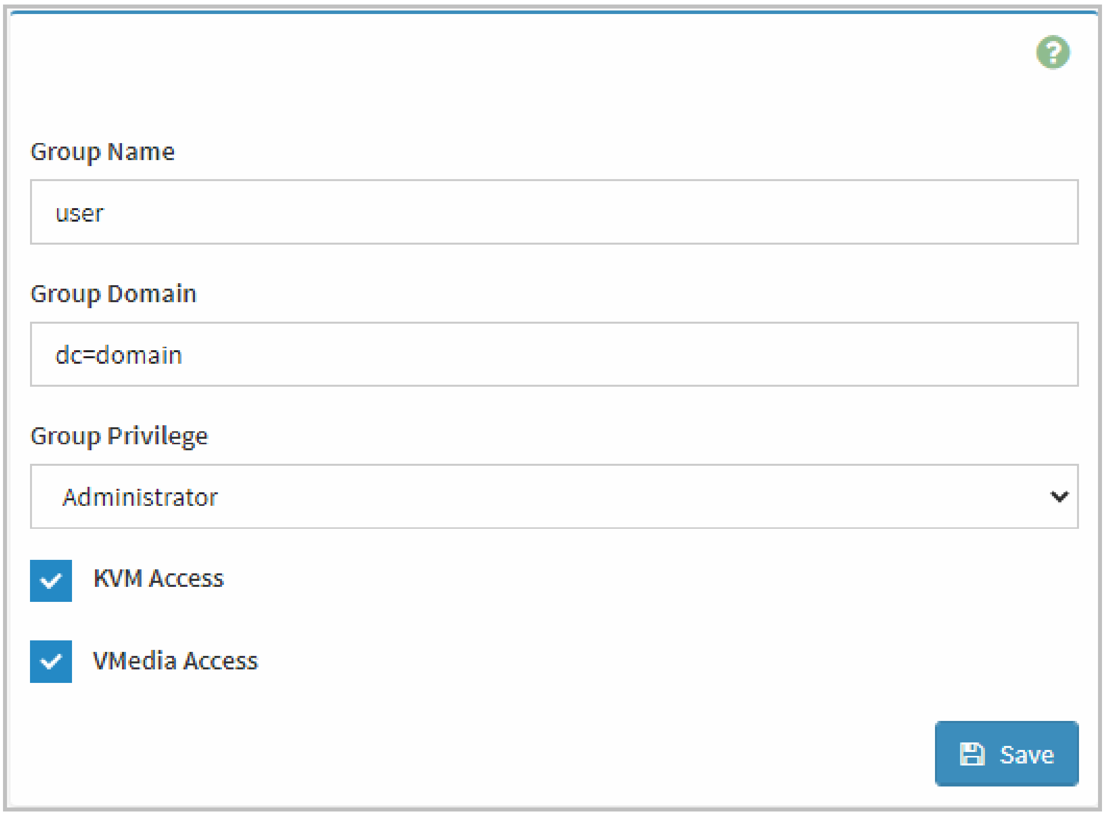
Table 3-3 Parameter Descriptions for the General LDAP Settings

Parameter	Description	Setting
Enable LDAP/E-directory Authentication	Whether to enable LDAP authentication.	→ Select **Enable LDAP/E-directory Authentication** to enable LDAP authentication.

Parameter	Description	Setting
		→ Clear **Enable LDAP/E-directory Authentication** to disable LDAP authentication.
Encryption Type	LDAP encryption type.	Select the corresponding encryption type: → **No Encryption**: No encryption. → **SSL**: The SSL is used for encryption. → **StarTLS**: The StarTLS is used for encryption.
Common Name Type	Address type of the LDAP server.	Select the corresponding name type: → **IP Address**: The LDAP server address is identified in IP format. → **FQDN**: The LDAP server address is identified in FQDN format. The **FQDN** option is available only when **Encryption Type** is set to **StarTLS**.
Server Address	Address of the LDAP server.	→ If **Common Name Type** is set to **IP Address**, enter the IP address of the LDAP server, which supports the IPv4 and IPv6 formats. → If **Common Name Type** is set to **FQDN**, enter the FQDN address of the LDAP server.
Port	Port number of the LDAP server.	Enter the port number, with a range of 1–65535. The default port number is 389. If **Encryption Type** is set to **SSL**, enter the port number *636*.
Bind DN	Identity name used to log in to the LDAP server.	Enter the bound identity name, for example, *cn=manager,ou=login, dc=domain,dc=com*.
Password	Password used to log in to the LDAP server.	Enter the password. It cannot be left blank. Range of password length: 1–48 characters.
Search Base	Directory where external user information is stored on the LDAP server.	Enter the search base, for example, *ou=login,dc=domain,dc=com*.
Attribute of User Login	User login attribute.	Select the corresponding attribute of user login.
CA certificate file	-	The CA file needs to be uploaded only when **Encryption Type** is set to **StarTLS**.
Certificate File	-	The certificate file needs to be uploaded only when **Encryption Type** is set to **StarTLS**.
Private Key	-	The private key file needs to be uploaded only when **Encryption Type** is set to **StarTLS**.

6. Click **Save**.
7. On the **LDAP/E-directory Settings** page, click **Role Groups**. The **Role Groups** page is displayed.
8. Click the icon for the new role group. The **Role Groups** page is displayed, see Figure 3-16.

Figure 3-16 Role Groups Page



Group Name

user

Group Domain

dc=domain

Group Privilege

Administrator

☑ KVM Access

☑ VMedia Access

9. Configure the parameters. For a description of the parameters, refer to Table 3-4.

Table 3-4 Role Groups Parameter Descriptions

Parameter	Description	Setting
Group Name	Name of the role group.	Enter the group name.
Group Domain	Domain where the role group is located.	Enter the group domain.
Group Privilege	Permissions of the role group on the BMC.	Select a permission for the role group: → **Administrator**: administrator permission → **Operator**: operator permission → **User**: viewer permission → **None**: no permission
KVM Access	Whether the role group can access the KVM.	→ Select **KVM Access**. The role group can access the KVM.

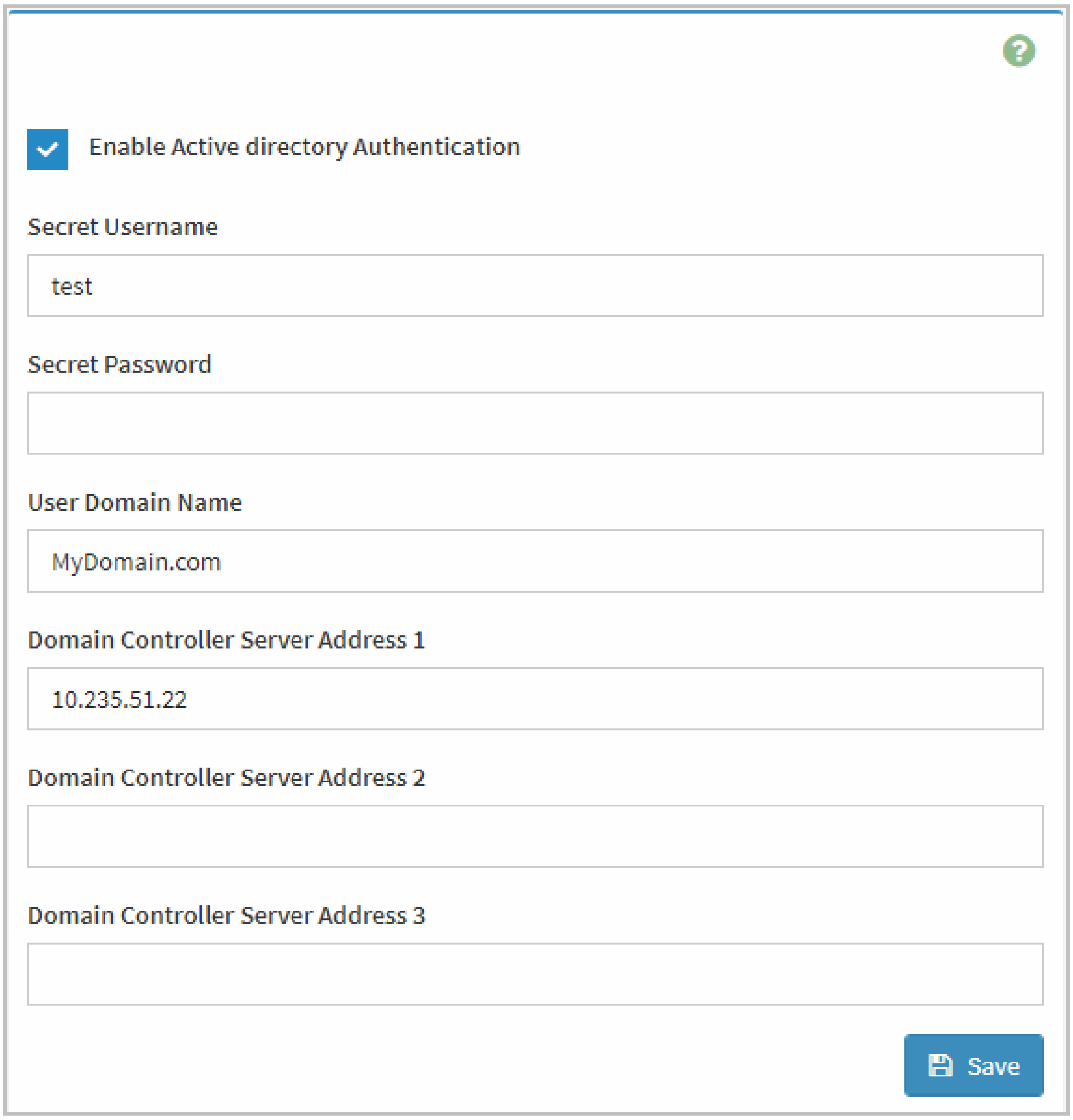
Parameter	Description	Setting
		→ Clear **KVM Access**. The role group cannot access the KVM.
VMedia Access	Whether the role group can access the VMedia.	→ Select **VMedia Access**. The role group cannot access the VMedia. → Clear **VMedia Access**. The role group cannot access the VMedia.

10. Click **Save**.

- Configuring AD Server Authentication Parameters

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **External User Services**. The **External User Services** page is displayed.
3. Click **Active Directory Settings**. The **Active Directory Settings** page is displayed.
4. Click **General Settings**. The **General Active Directory Settings** page is displayed, see Figure 3-17.

Figure 3-17 General Active Directory Settings Page



☑ Enable Active directory Authentication

Secret Username: test

Secret Password:

User Domain Name: MyDomain.com

Domain Controller Server Address 1: 10.235.51.22

Domain Controller Server Address 2:

Domain Controller Server Address 3:

5. Configure the parameters. For a description of the parameters, refer to Table 3-5.

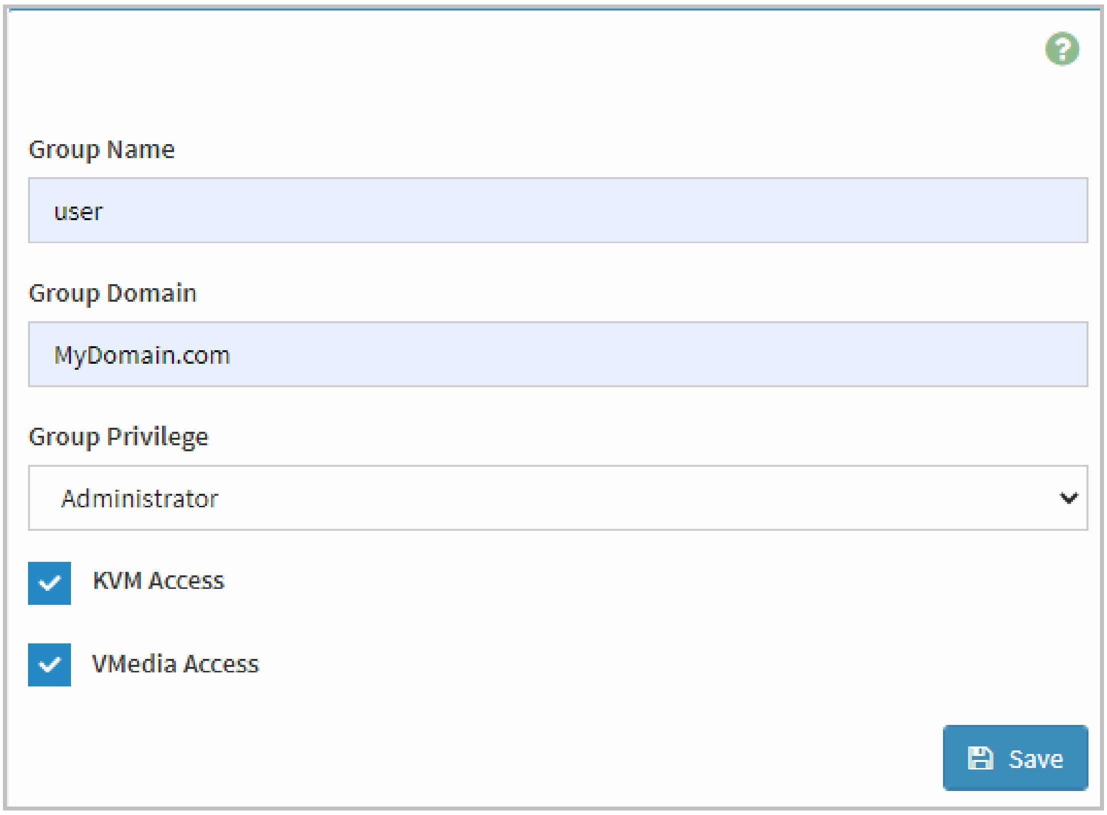
Table 3-5 Parameter Descriptions for the General Active Directory Settings

Parameter	Description	Setting
Enable Active directory Authentication	Whether to enable AD authentication.	→ Select **Enable Active Directory Authentication** to enable AD authentication. → Clear **Enable Active Directory Authentication** to disable AD authentication.
Secret Username	Username for logging in to the AD server.	Enter the username consisting of 1–64 letters or digits. If the username and password are not required, leave this parameter blank.

Parameter	Description	Setting
Secret Password	Password for logging in to the AD server.	Enter the password consisting of 6–127 characters. If the username and password are not required, leave this parameter blank.
User Domain Name	Domain name of the AD server.	Enter the domain name of the user, for example, *MyDomain.com*.
Domain Controller Server Address 1	Address 1 of the AD server.	Enter the IP address 1 of the AD server, which supports IPv4 and IPv6, and is required.
Domain Controller Server Address 2	Address 2 of the AD server.	Enter the IP address 2 of the AD server, which supports IPv4 and IPv6, and is optional.
Domain Controller Server Address 3	Address 3 of the AD server.	Enter the IP address 3 of the AD server, which supports IPv4 and IPv6, and is optional.

6. Click **Save**.
7. On the **Active Directory Settings** page, click **Role Groups**. The **Role Groups** page is displayed.
8. Click the icon for the new role group. The **Role Groups** page is displayed, see Figure 3-18.

Figure 3-18 Role Groups Page



Group Name

user

Group Domain

MyDomain.com

Group Privilege

Administrator

☑ KVM Access

☑ VMedia Access

9. Configure the parameters. For a description of the parameters, refer to Table 3-6.

Table 3-6 Role Groups Parameter Descriptions

Parameter	Description	Setting
Group Name	Name of the role group.	Enter the group name.
Group Domain	Domain where the role group is located.	Enter the group domain.
Group Privilege	Permissions of the role group on the BMC.	Select a permission for the role group: → **Administrator**: administrator permission → **Operator**: operator permission → **User**: viewer permission → **None**: no permission
KVM Access	Whether the role group can access the KVM.	→ Select **KVM Access**. The role group can access the KVM. → Clear **KVM Access**. The role group cannot access the KVM.
VMedia Access	Whether the role group can access the VMedia.	→ Select **VMedia Access**. The role group cannot access the VMedia. → Clear **VMedia Access**. The role group cannot access the VMedia.

10. Click **Save**.

Verification

- If the LDAP server authentication parameters are configured, log in to the BMC Web portal on the LDAP server to check whether the login is successful.
- If the AD server authentication parameters are configured, log in to the BMC Web portal on the AD server to check whether the login is successful.

3.7.3 Configuring a KVM Mouse Mode

Abstract

This procedure describes how to configure the mouse mode used during remote control based on personal habits.

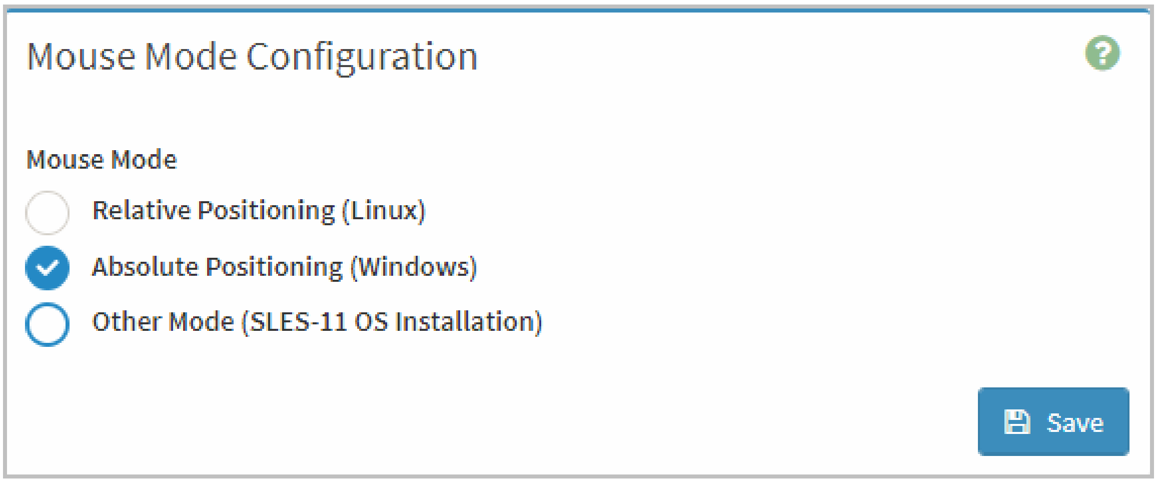
Note

In addition to the BMC Web portal, the mouse mode can also be configured in the KVM. The mouse mode configured on the BMC Web portal and that configured in the KVM are automatically synchronized. The latest configured mouse mode shall prevail.
For a description of the mouse mode configurations in the KVM, refer to "3.8 Remotely Controlling a Server".

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **KVM Mouse Settings**. The **KVM Mouse Settings** page is displayed, seeFigure 3-19.

Figure 3-19 KVM Mouse Settings Page



Mouse Mode Configuration

Mouse Mode

○ Relative Positioning (Linux)

● Absolute Positioning (Windows)

○ Other Mode (SLES-11 OS Installation)

3. Select a mouse mode as required. For a description of the mouse modes, refer to Table 3-7.

Table 3-7 Mouse Mode Descriptions

Mouse Mode	Description
Relative Positioning (Linux)	Calculates the displacement of the local mouse relative to the server mouse, and transfers it to the server to make the mouse on the server move.
Absolute Positioning (Windows)	Transfers the absolute position of the local mouse to the server to make the mouse on the server move.
Other Mode (SLES-11 OS Installation)	Calculates the displacement of the local mouse relative to the center position, and transfers it to the server to make the mouse on the server move.

4. Click **Save**.

3.7.4 Configuring Remote Log Parameters

Abstract

This procedure describes how to configure remote log parameters to upload local logs (including login logs, operation logs, and system logs) to a remote log server.

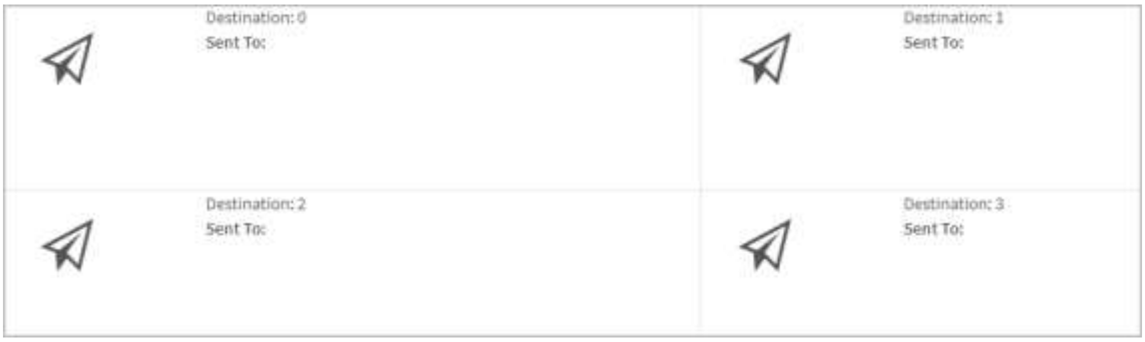
Steps

Configuring a Remote Log Destination

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.

2. Click **Log Settings**. The **Log Settings** page is displayed.
3. Click **Remote Log Settings**. The **Remote Log Settings** page is displayed, see Figure 3-20.

Figure 3-20 Remote Log Settings Page



Destination: 0
Sent To:

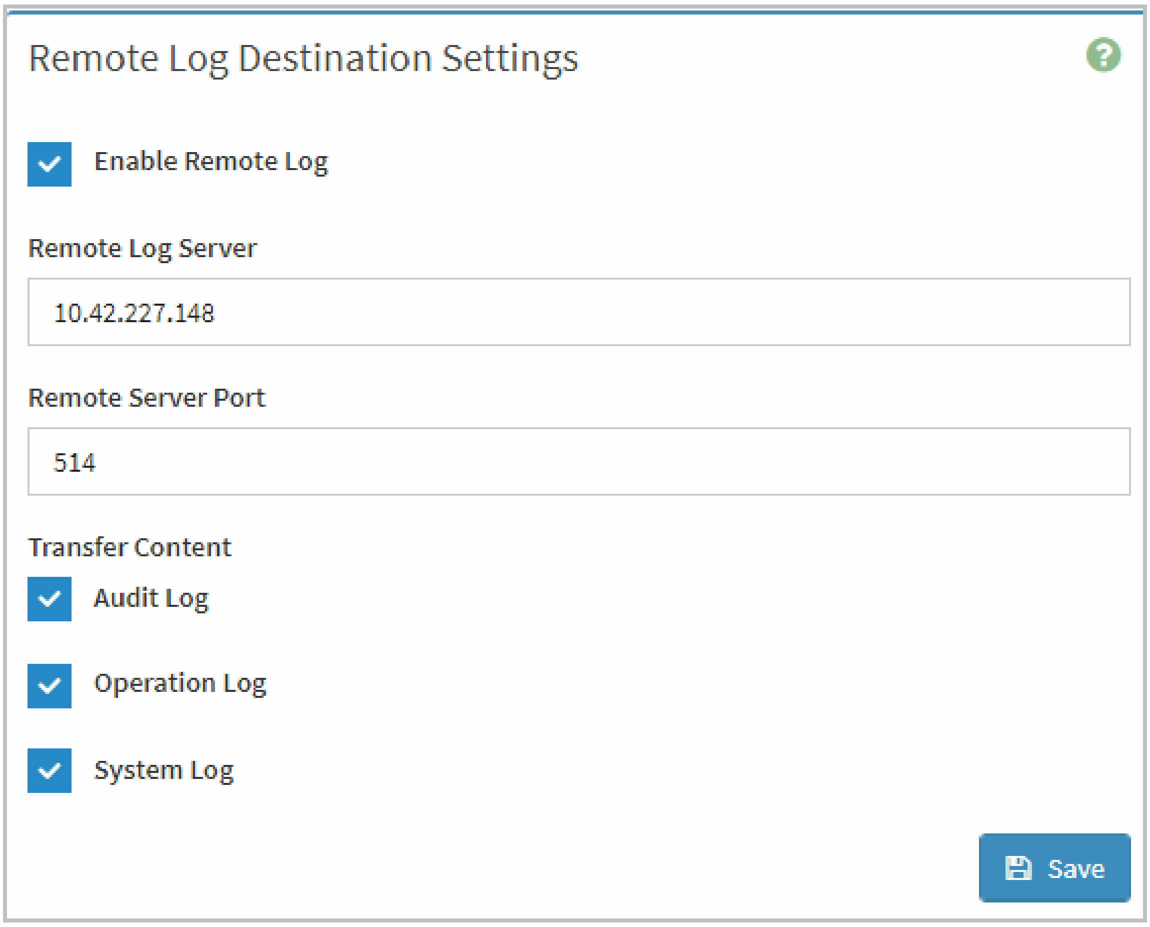
Destination: 1
Sent To:

Destination: 2
Sent To:

Destination: 3
Sent To:

4. Click any **Destination**. The **Remote Log Destination Settings** page is displayed, see Figure 3-21.

Figure 3-21 Remote Log Destination Settings Page



Remote Log Destination Settings

☑ Enable Remote Log

Remote Log Server

10.42.227.148

Remote Server Port

514

Transfer Content

☑ Audit Log

☑ Operation Log

☑ System Log

5. Configure the parameters. For a description of the parameters, refer to Table 3-8.

Table 3-8 Parameter Descriptions for the Remote Log Destination

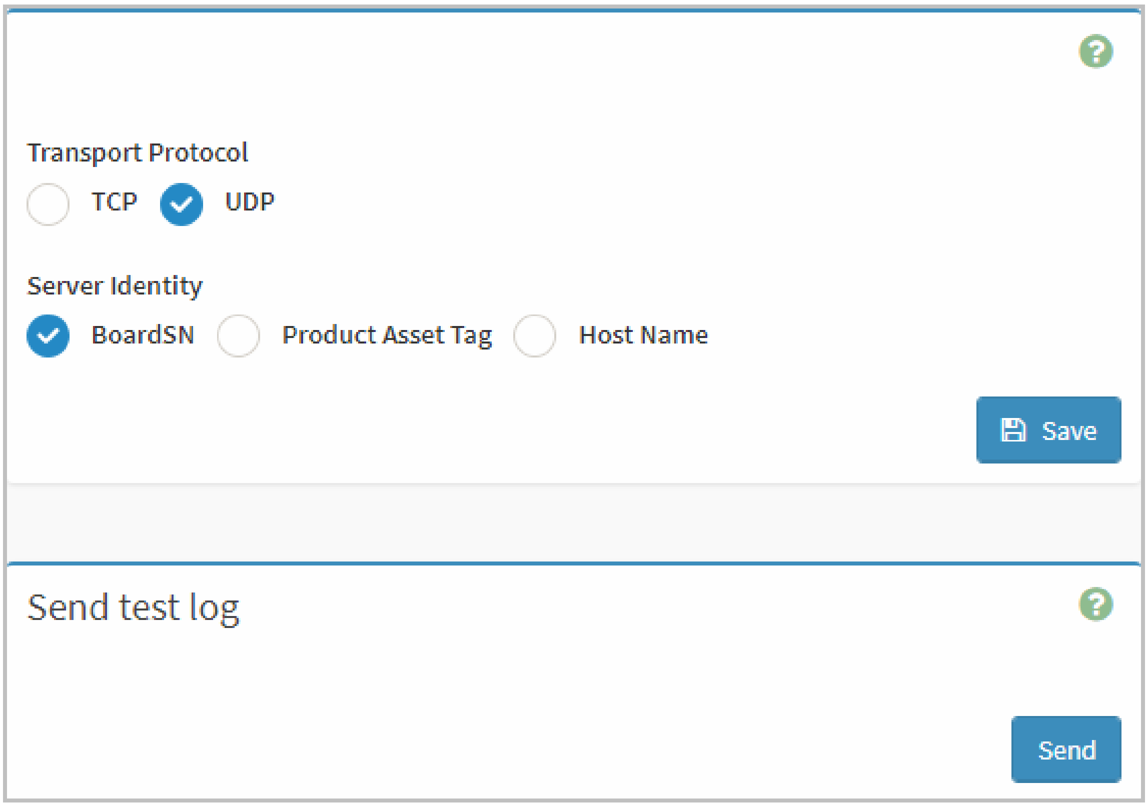
Parameter	Description	Setting
Enable Remote Log	Whether to upload local logs to a remote log server.	Select **Enable Remote Log**.
Remote Log Server	IP address or host name of the remote log server.	Enter the IP address or host name of the remote log server. ● The IP address supports the IPv4 and IPv6 formats. ● The host name must comply with the FQDN format, with a maximum length of 255 characters.
Remote Server Port	Port number of the remote server.	Enter the port number of the remote server. Port number range: 1–65535, 514 by default.
Transfer Content	Log type for remote transmission: ● Audit log: Records user logins and logouts of the BMC Web portal, BMC command lines, and KVM information. ● Operation log: Records the information about users' operations on the server, including manual operations and remote operations. ● System log: Records log and alarm information generated during the operation of the server.	Select the type(s) of logs to be transmitted remotely.

6. Click **Save**.

Configuring a Remote Log Policy

7. On the **Log Settings** page, click **Remote Log Policy**. The **Remote Log Policy** page is displayed, see Figure 3-22.

Figure 3-22 Remote Log Policy Page



Transport Protocol

○ TCP ● UDP

Server Identity

● BoardSN ○ Product Asset Tag ○ Host Name

Send test log

8. Configure the parameters. For a description of the parameters, refer to Table 3-9.

Table 3-9 Parameter Descriptions for the Remote Log Policy

Parameter	Description	Setting
Transport Protocol	Protocol used to upload remote logs.	Select a transport protocol.
Server Identity	Server identity type.	Select the type to identify the host.

9. Click **Save**.
10. (Optional) In the **Send test log** area, click **Send**. The Syslog test log is sent to the remote log server.

Verification

1. Log in to or log out of the BMC Web portal.

Note

When configuring parameters in the **Transfer Content** area in Step 5, make sure **Audit Log** is selected. Otherwise, the login log generated from logging in/out the BMC Web portal will not be uploaded to the remote log server.

2. Check the remote log server to see if the newly generated login log is received.

3.7.5 Configuring the Event Log Storage Policy

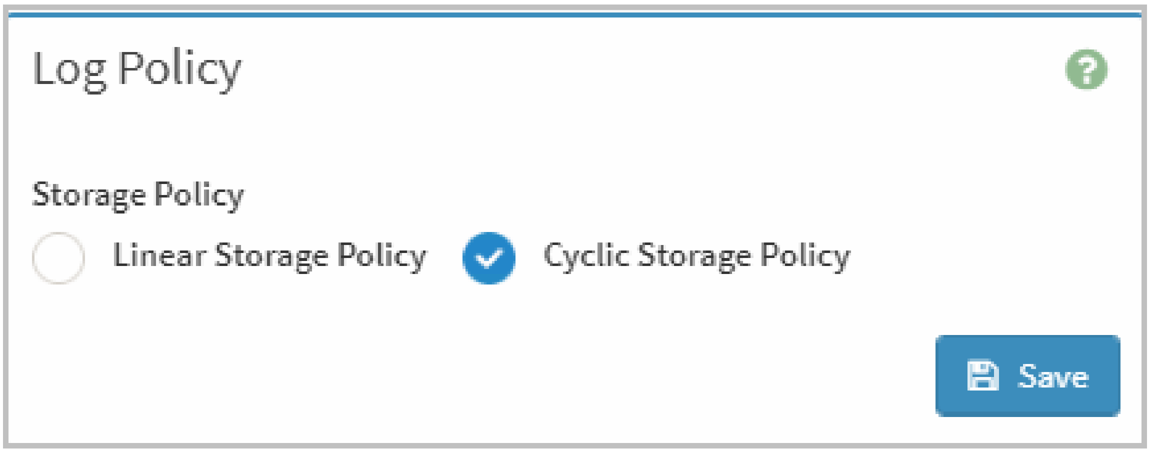
Abstract

Event logs are the records of the events that occur during the operation of the server. This procedure describes how to configure the event log storage policy.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Log Settings**. The **Log Settings** page is displayed.
3. Click **Log Policy**. The **Log Policy** page is displayed, as shown in Figure 3-23.

Figure 3-23 Log Policy Page



Log Policy

Storage Policy

○ Linear Storage Policy ● Cyclic Storage Policy

4. Select the desired event log storage policy.
   - **Linear Storage Policy**: After the hard disk for storing event logs is full, all old logs are cleared and then new logs are stored.
   - **Cyclic Storage Policy**: After the hard disk for storing event logs is full, the oldest event logs are overwritten by the newly generated event logs.
5. Click **Save**.

3.7.6 Configuring VMedia Instance Parameters

Abstract

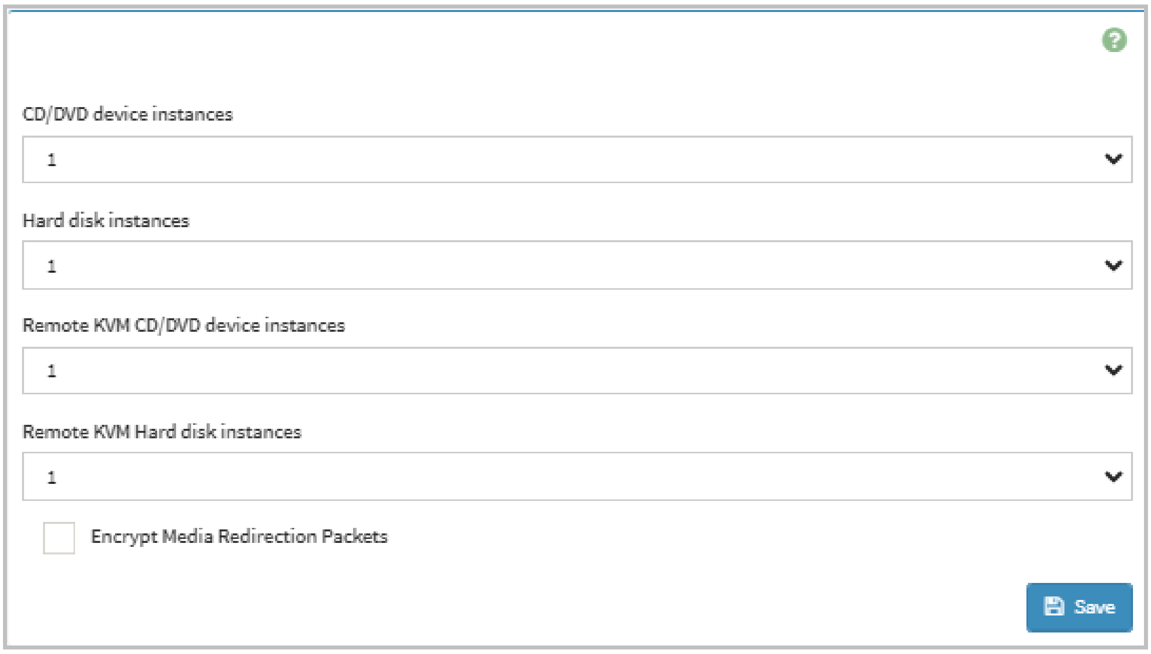
Before mounting a CD/DVD and HD on the KVM, you must configure the VMedia instance parameters.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Media Redirection Settings**. The **Media Redirection** page is displayed.

3. Click **VMedia Instance Settings**. The **VMedia Instance Settings** page is displayed, see Figure 3-24.

Figure 3-24 VMedia Instance Settings Page



CD/DVD device instances: 1

Hard disk instances: 1

Remote KVM CD/DVD device instances: 1

Remote KVM Hard disk instances: 1

□ Encrypt Media Redirection Packets

4. Configure the parameters. For a description of the parameters, refer to Table 3-10.

Table 3-10 Parameter Descriptions for the VMedia Instance Settings

Parameter	Description	Setting
CD/DVD device instances	Number of CDs/DVDs on the client PC.	Select **1** by default.
Hard disk instances	Number of HDs on the client PC.	Select **1** by default.
Remote KVM CD/DVD device instances	Number of CDs/DVDs mounted on the KVM.	Select **1** by default.
Remote KVM Hard disk instances	Number of HDs mounted on the KVM.	Select **1** by default.
Encrypt Media Redirection Packets	Whether to encrypt files when uploading them remotely.	Clear **Encrypt Media Redirection Packets**.

5. Click **Save**.

3.7.7 Configuring Remote Session Parameters

Abstract

Before controlling a server remotely, you must configure the remote session parameters.

The server can be remotely controlled in the following ways:

- KVM
- VNC

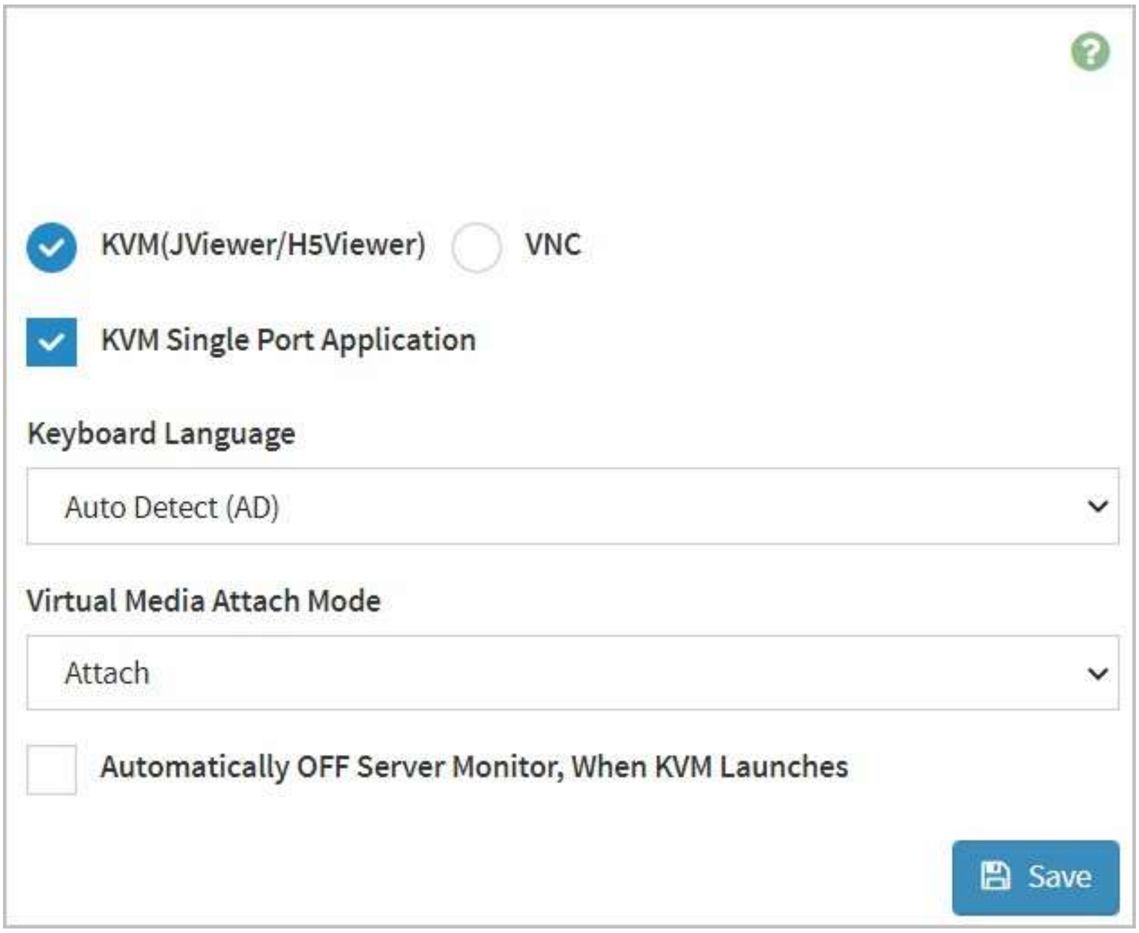
Note

You cannot remotely control the server through KVM and VNC simultaneously.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Media Redirection Settings**. The **Media Redirection** page is displayed.
3. Click **Remote Session**. The **Remote Session** page is displayed, see Figure 3-25 and Figure 3-26.

Figure 3-25 Remote Session Page-KVM



● KVM(JViewer/H5Viewer) ○ VNC

☑ KVM Single Port Application

Keyboard Language

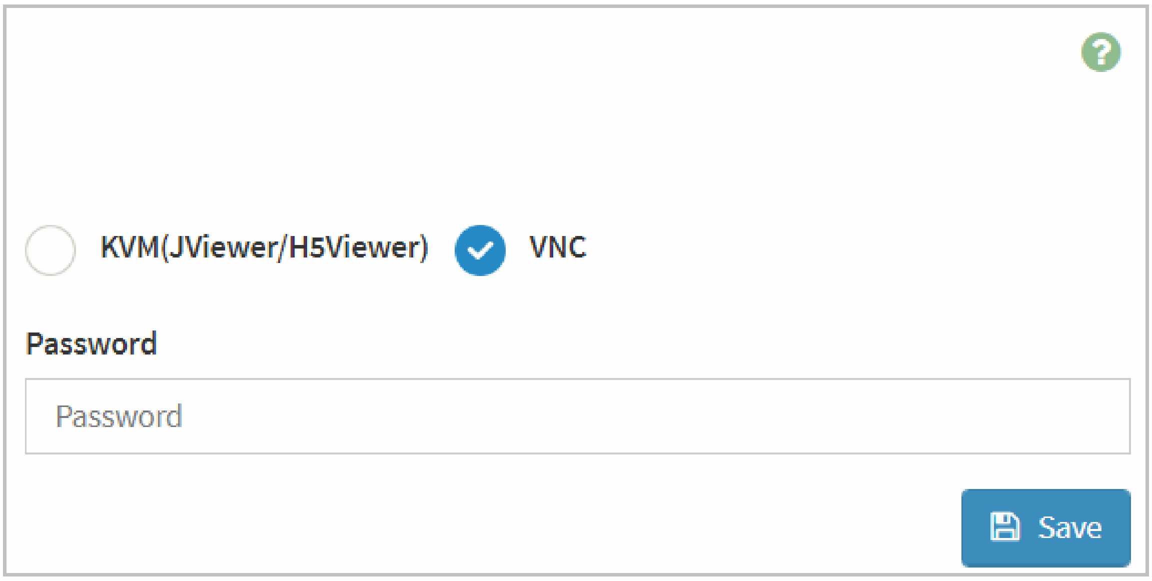
Auto Detect (AD)

Virtual Media Attach Mode

Attach

□ Automatically OFF Server Monitor, When KVM Launches

Figure 3-26 Remote Session Page-VNC



○ KVM(JViewer/H5Viewer) ● VNC

Password

Password

4. Set the parameters. For a description of the parameters, refer to Table 3-11 and Table 3-12.

Table 3-11 Parameter Descriptions for Remote Session-KVM

Parameter	Description	Setting
KVM (JViewer/H5Viewer)	Whether to remotely control the server through KVM.	Select **KVM (JViewer/H5Viewer)**.
VNC	Whether to remotely control the server through VNC.	Clear **VNC**.
KVM Single Port Application	Whether to use the **443** port when the KVM is started in HTML mode.	When **KVM Single Port Application** is selected, **Enable KVM Encryption** is not available.
Keyboard Language	Keyboard language used during remote KVM operations.	The **Auto Detect(AD)** parameter is selected by default.
Virtual Media Attach Mode	Whether to reconnect the virtual drive automatically when the network is disconnected.	Select a virtual media connection mode: ● **Attach**: not reconnected automatically. ● **Auto Attach**: reconnected automatically.
Automatically OFF Server Monitor When KVM Launches	Whether to automatically shut down the physical display during remote KVM operations.	The **Automatically OFF Server Monitor When KVM Launches** parameter is cleared by default.

Table 3-12 Parameter Descriptions for Remote Session-VNC

Parameter	Description	Setting
KVM (JViewer/H5Viewer)	Whether to remotely control the server through KVM.	Clear **KVM port number**.

Parameter	Description	Setting
VNC	Whether to remotely control the server through VNC.	Select **VNC**.
Password	Password used for remote server control through VNC.	The password consists of numbers, letters and special characters, and the length of the password does not exceed 8 digits. If the password is empty, the default password is used. The default password is **Supcnv9@**.

5. Click **Save**.

3.7.8 Configuring IP Settings

Abstract

To re-plan the IP settings of the iSAC management network port or shared network port of the server, you must configure the IP address, subnet mask, default gateway, and other related information.

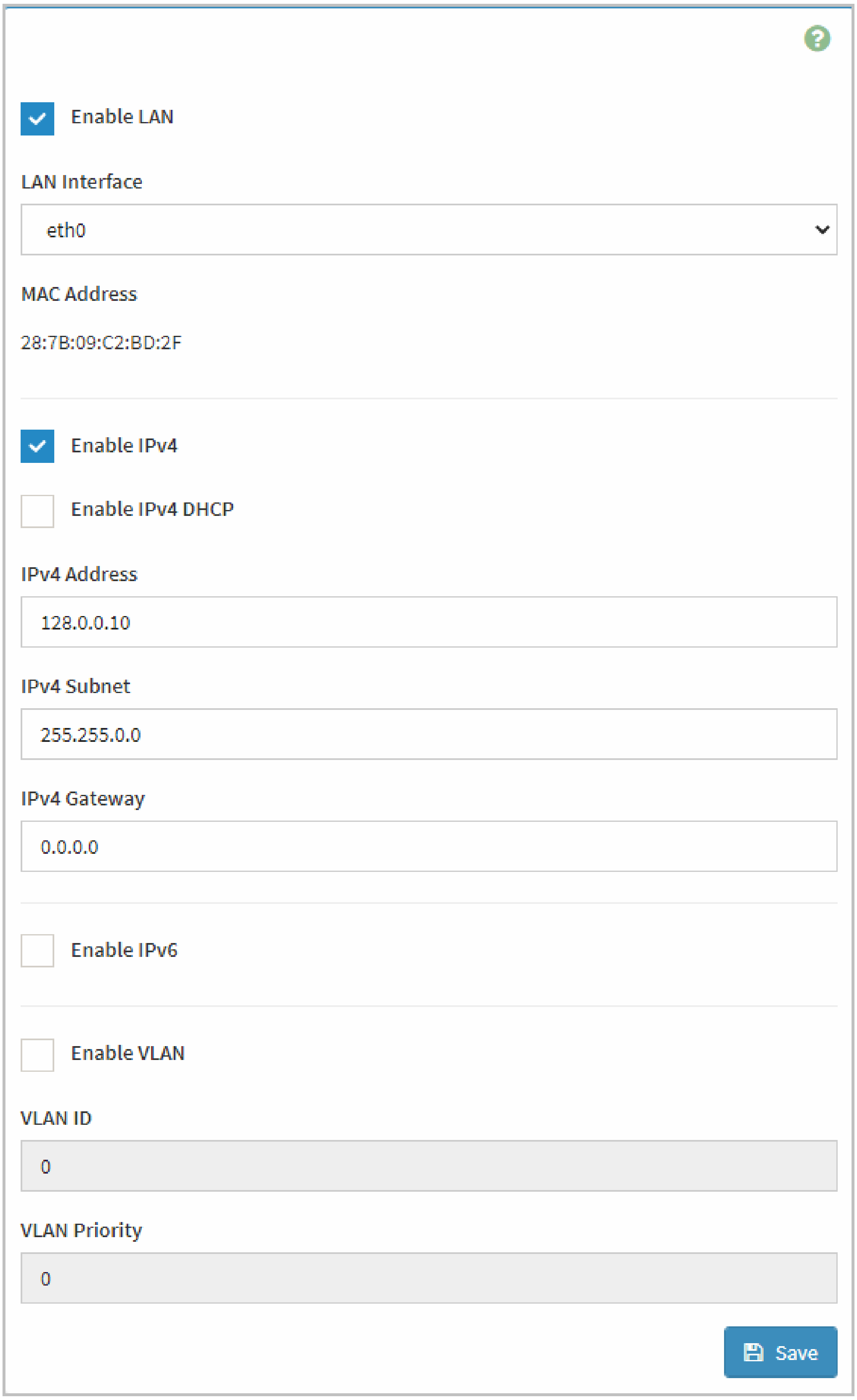
In most cases, **eth0** is the shared network port and **eth1** is the management network port.

The shared network port can be used as a service network port or management network port. If the management network port is abnormal, the shared network port can be used as the management network port.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Network Settings**. The **Network Settings** page is displayed.
3. Click **Network IP Settings**. The **Network IP Settings** page is displayed, see Figure 3-27 and Figure 3-28.

Figure 3-27 Network IP Settings Page (Shared Network Port)



☑ Enable LAN

LAN Interface

eth0

MAC Address

28:7B:09:C2:BD:2F

☑ Enable IPv4

□ Enable IPv4 DHCP

IPv4 Address

128.0.0.10

IPv4 Subnet

255.255.0.0

IPv4 Gateway

0.0.0.0

□ Enable IPv6

□ Enable VLAN

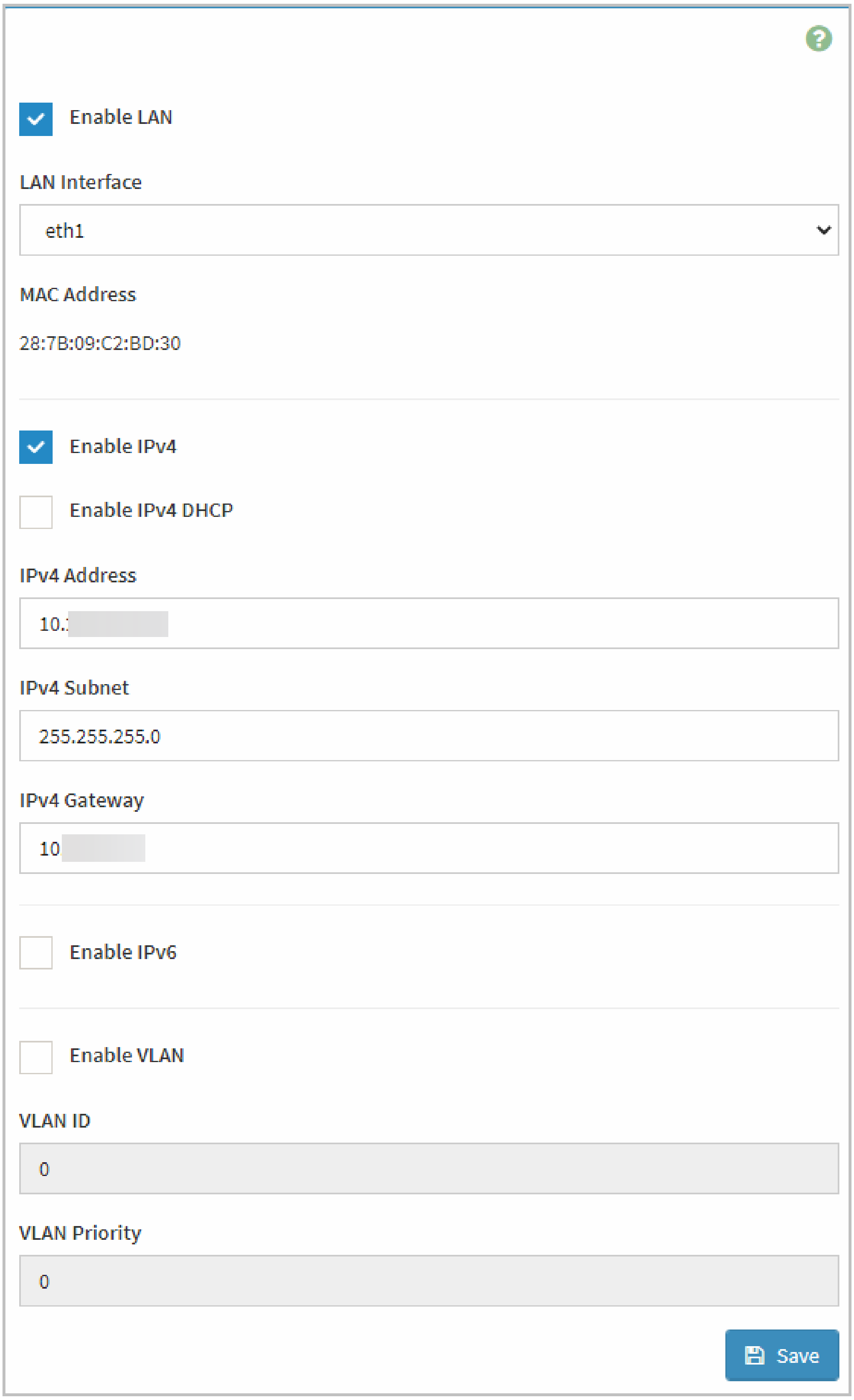
VLAN ID

0

VLAN Priority

0

Figure 3-28 Network IP Settings Page (Management Network Port)



☑ Enable LAN

LAN Interface

eth1

MAC Address

28:7B:09:C2:BD:30

☑ Enable IPv4

□ Enable IPv4 DHCP

IPv4 Address

10.[redacted]

IPv4 Subnet

255.255.255.0

IPv4 Gateway

10[redacted]

□ Enable IPv6

□ Enable VLAN

VLAN ID

0

VLAN Priority

0

4. Configure the parameters. For a description of the parameters, refer to Table 3-13.

Table 3-13 Parameter Descriptions for the Network IP Address Configuration

Parameter	Description	Setting
Enable LAN	Whether to enable the network port. The network port is selected from the **LAN Interface** list.	● Select **Enable LAN**. The network port is enabled. ● Deselect **Enable LAN**. The network port is disabled.
LAN Interface	Current network port.	● To configure the management network port, select **eth1**. ● To configure the shared network port, select **eth0**.
MAC Address	MAC address of the corresponding network port.	This parameter is displayed only and cannot be configured.
Enable IPv4	Whether the network port enables the IPv4 protocol.	● Select **Enable IPv4**. The IPv4 protocol is enabled. ● Clear **Enable IPv4**. The IPv4 protocol is disabled. The IPv4-related parameters can be configured only after **Enable IPv4** is selected. ● To automatically obtain the IP address, select **IPv4 DHCP**. ● To manually configure the IP address, deselect **IPv4 DHCP**, and manually configure **IPv4 Address**, **IPv4 Subnet** and **IPv4 Gateway**. The IP addresses of the management network port and the shared network port must not be in the same network segment.
Enable IPv6	Whether the network port enables the IPv6 protocol.	● Select **Enable IPv6**. The IPv6 protocol is enabled. ● Clear **Enable IPv6**. The IPv6 protocol is disabled. The IPv6-related parameters can be configured only after **Enable IPv6** is selected. ● To automatically obtain the IP address, select **IPv6 DHCP**. ● To manually configure the IP address, deselect **IPv6 DHCP**, and manually configure **IPv6 Address**, **Subnet Prefix Length** and **IPv6 Gateway**. The IP addresses of the management network port and the shared network port must not be in the same network segment.

Parameter	Description	Setting
Enable VLAN	Whether the network port enables VLAN.	● Select **Enable VLAN**. The network port can be added into a VLAN. ● Clear **Enable VLAN**. The network port cannot be added into a VLAN. The VLAN-related parameters can be configured only after **Enable VLAN** is selected. ● **VLAN ID**: 1–4094. ● **VLAN Priority**: 0–7, with 7 of the highest priority.

5. Click **Save**.

3.7.9 Configuring Network Bonding

Abstract

If the shared network port eth0 and the iSAC management network port eth1 are bonded, you can access the BMC through the IP address of either network ports even if only one of the two ports is connected.

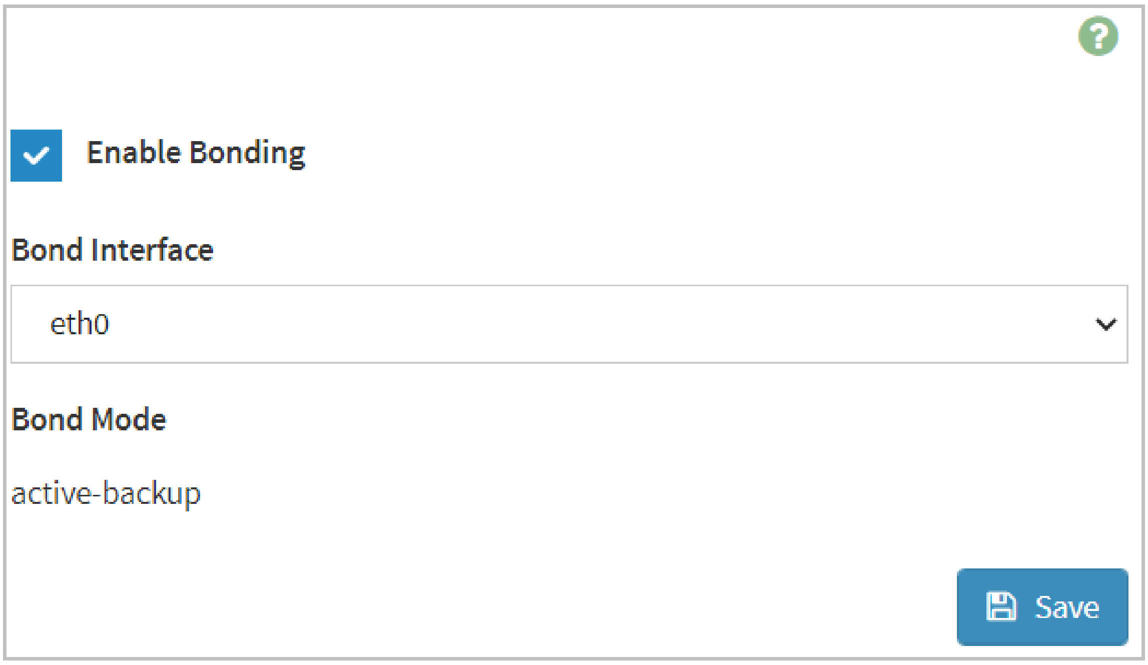
Prerequisite

The VLAN function of both the shared network port and the iSAC management network port has been disabled. For details, refer to "3.7.8 Configuring IP Settings".

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Network Settings**. The **Network Settings** page is displayed.
3. Click **Network Bond Configuration**. The **Network Bond Configuration** page is displayed, see Figure 3-29.

Figure 3-29 Network Bonding Configuration Page



☑ Enable Bonding

Bond Interface

eth0

Bond Mode

active-backup

4. Set the parameters. For a description of the parameters, refer to Table 3-14.

Table 3-14 Parameter Descriptions for Network Bonding

Parameter	Description	Setting
Enable Bonding	Whether to enable network bonding.	● If you select **Enable Bonding**, the network bonding function is enabled. ● If you clear **Enable Bonding**, the network bonding function is disabled.
Bond Interface	Select the network port that provides the external network service.	● If you select **eth0**, the shared network port **eth0** provides the external network service. ● if you select **eth1**, the iSAC management network port **eth1** provides the external network service.

5. Click **Save**.

3.7.10 Configuring the DNS

Abstract

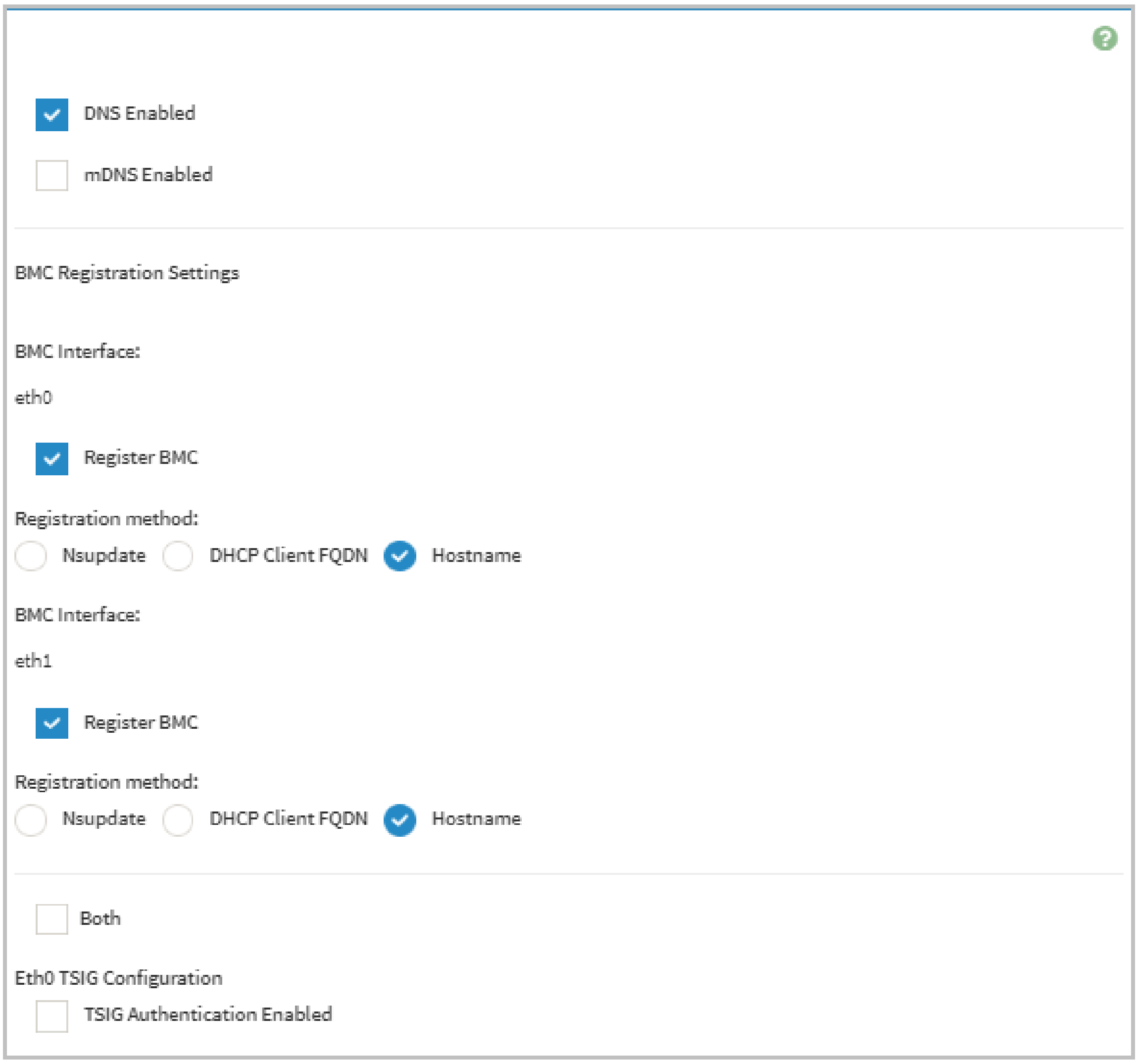
To access the BMC Web portal through FQDN, you must configure the DNS information for the management network port and shared network port of the server.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Network Settings**. The **Network Settings** page is displayed.

3. Click **DNS Configuration**. The **DNS Configuration** page is displayed, see Figure 3-30.

Figure 3-30 DNS Configuration Page



☑ DNS Enabled

□ mDNS Enabled

BMC Registration Settings

BMC Interface:

eth0

☑ Register BMC

Registration method:

○ Nsupdate ○ DHCP Client FQDN ● Hostname

BMC Interface:

eth1

☑ Register BMC

Registration method:

○ Nsupdate ○ DHCP Client FQDN ● Hostname

□ Both

Eth0 TSIG Configuration

□ TSIG Authentication Enabled

Note

The **DNS Configuration** page is long, so only a part of it is displayed here.

4. Configure the parameters. For a description of the parameters, refer to Table 3-15.

Table 3-15 DNS Configuration Parameter Descriptions

Parameter	Description	Setting
DNS Enabled	Whether to enable the DNS service.	● Select **DNS Enabled**. The DNS service is enabled. ● Clear **DNS Enabled**. The DNS service is disabled.

Parameter	Description	Setting
mDNS Enabled	Whether to enable the multicast DNS access.	● Select **mDNS Enabled**. The multicast DNS service is enabled. ● Clear **mDNS Enabled**. The multicast DNS service is disabled.
BMC Registration Settings	Whether to register DNS for eth1 (management network port) and eth0 (shared network port).	● Select **Register BMC** under eth0. The DNS is registered for eth0. ● Select **Register BMC** under eth1. The DNS is registered for eth1. The BMC registration methods include: ● **Nsupdate**: Uses a name server application to register on the DNS server. ● **DHCP Client FQDN**: Uses the DHCP option 81 to register on the DNS server. ● **Hostname**: Uses the DHCP option 12 to register on the DNS server. If the DHCP server does not support the DHCP option 81, select **Hostname**.
Domain Setting	Way to set the domain name.	● If **Automatic** is selected, the domain name is set automatically. ● If **Manual** is selected, you must set the domain name manually. The length of a domain name should not exceed 63 characters per label, and the length of the FQDN should not exceed 255 characters.
Domain Name Server Setting	Way to set the domain name server.	● If **Automatic** is selected, the DNS server information is obtained automatically. ● If **Manual** is selected, you must configure the DNS server information manually, and configure **Primary NTP Server**, **Secondary NTP Server** and **Tertiarydary NTP Server**. The **Primary NTP Server** parameter must be set, while others are optional. **Primary NTP Server**, **Secondary NTP Server** and **Tertiarydary NTP Server** cannot be set to the same value.

5. Click **Save**.

Verification

1. On the DNS server, check the registration information about the BMC, including the domain name and host name.

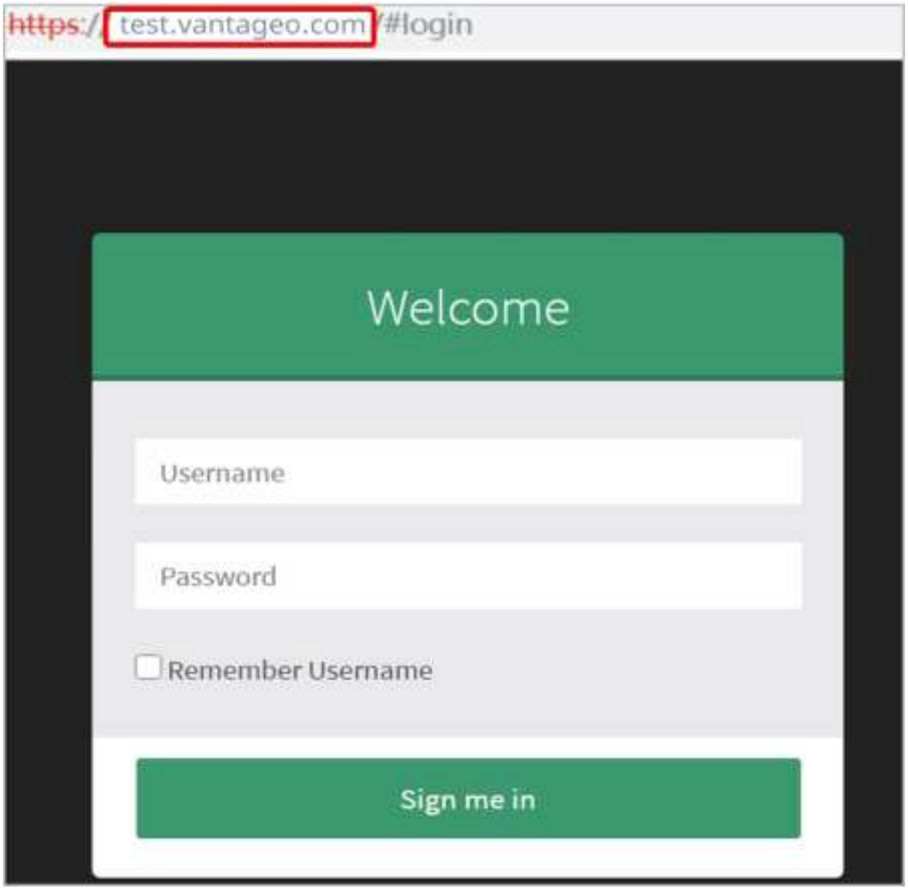
For example, if the parameters are configured as shown in Table 3-16 on the **DNS Configuration** page, the domain name is **vantageo.com** and the host name **test111**.

Table 3-16 Example of DNS Configuration Parameter

Parameter	Description
DNS Enabled	The **DNS Enabled** parameter is selected.
mDNS Enabled	The **mDNS Enabled** parameter is unselected.
BMC Registration Settings	The **Register BMC** parameter under eth1 is selected. The **Hostname** parameter is selected for **Registration Method**.
Domain Setting	The **Manual** parameter is selected, and the **Domain Name** parameter is set as **vantageo.com**
Domain Name Server Setting	The **Manual** parameter is selected and **Primary NTP Server** is configured. The IP address of **Primary NTP Server** must be in the same network segment as that of the management network port (eth1).

2. Visit the BMC Web portal through FQDN and check whether the **Welcome** page of the BMC Web portal is accessible, see Figure 3-31.

Figure 3-31 Welcome Page



3.7.11 Configuring a Hostname

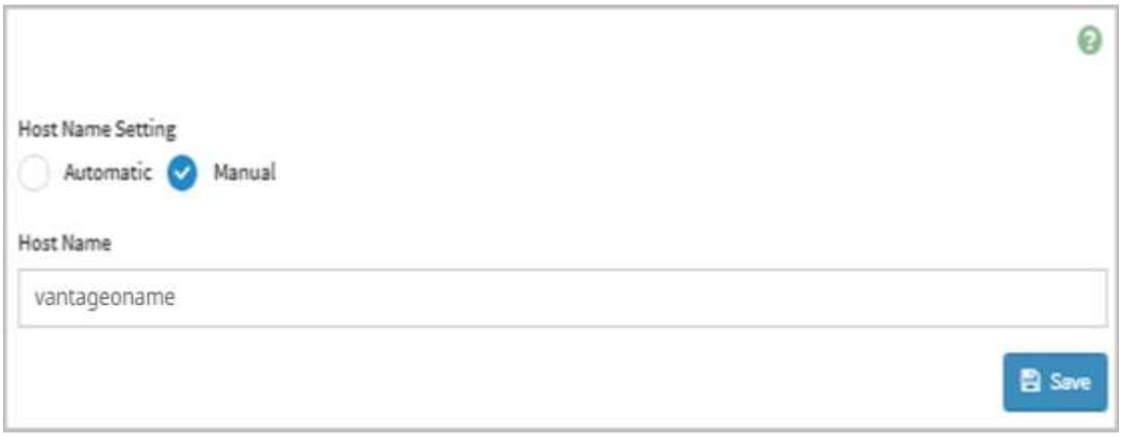
Abstract

A hostname is used to identify a server.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Network Settings**. The **Network Settings** page is displayed.
3. Click **Host Name Setting**. The **Host Name Setting** page is displayed, as shown in Figure 3-32.

Figure 3-32 Hostname Setting Page



Host Name Setting

○ Automatic ● Manual

Host Name

vantageoname

4. Set the parameters. For a description of the parameters, refer to Table 3-17.

Table 3-17 Hostname Parameter Descriptions

Parameter	Description	Setting
Host Name Setting	Sets the hostname setting mode.	● **Automatic**: A hostname is automatically set by the system. ● **Manual**: A hostname needs to be manually entered in the **Host Name** text box.
Host Name	Hostname of the server.	This parameter is required if **Host Name Settings** is set to **Manual**. Enter the hostname. A maximum of 63 characters can be entered, including digits, letters, hyphen (-), and underscores (_). It cannot contain spaces and is case insensitive. The first character must be a letter or digit, and the last character cannot be a hyphen (-).

5. Click **Save**.

3.7.12 Configuring NCSI

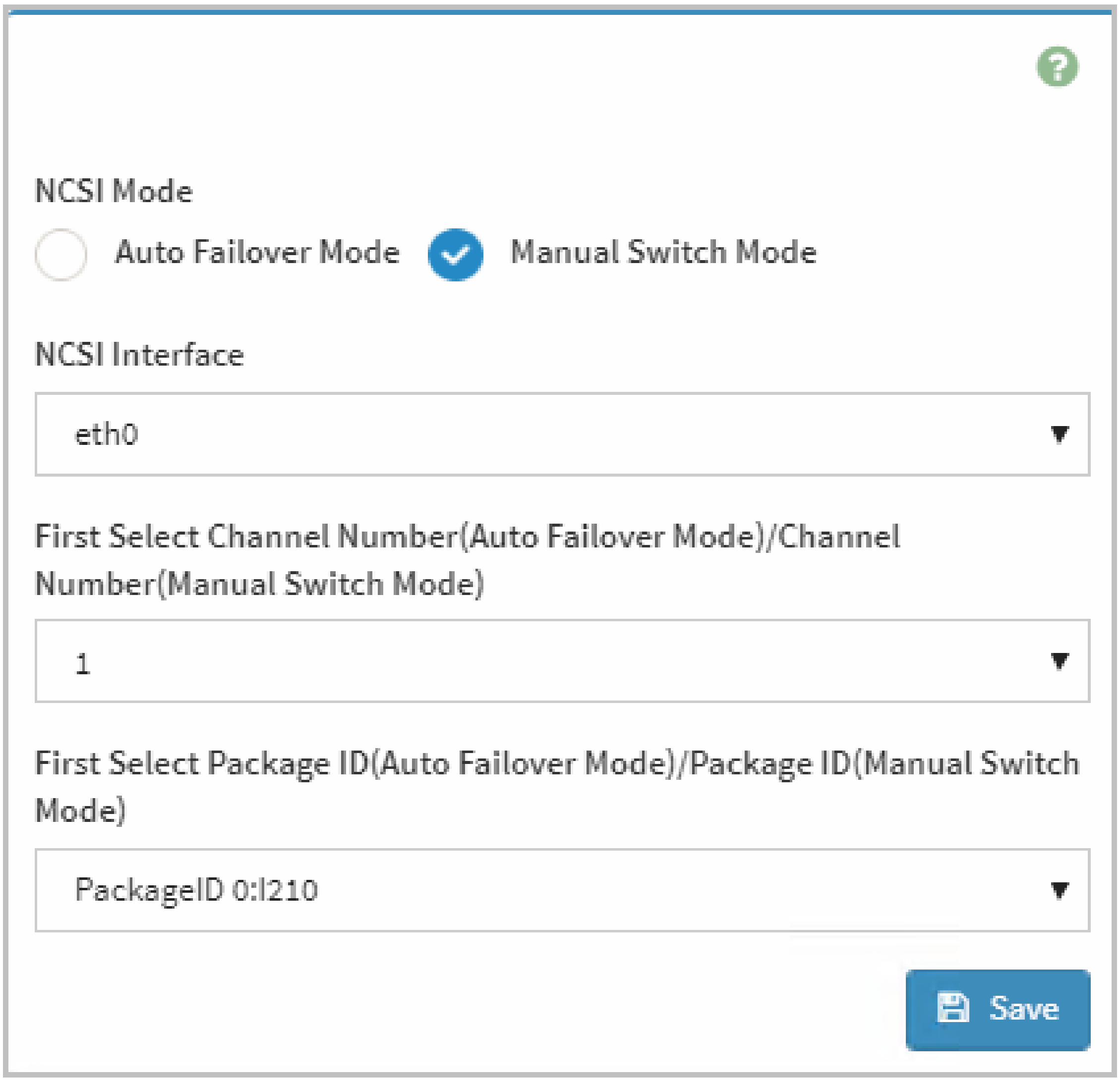
Abstract

You can specify a shared network port by configuring the NCSI.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Network Settings**. The **Network Settings** page is displayed.
3. Click **Sideband Interface (NC-SI)**. The **Sideband Interface (NC-SI)** page is displayed, see Figure 3-33.

Figure 3-33 Sideband Interface (NC-SI) Page



NCSI Mode

○ Auto Failover Mode ● Manual Switch Mode

NCSI Interface

eth0 ▼

First Select Channel Number(Auto Failover Mode)/Channel Number(Manual Switch Mode)

1 ▼

First Select Package ID(Auto Failover Mode)/Package ID(Manual Switch Mode)

PackageID 0:I210 ▼

4. Configure the parameters. For a description of the parameters, refer to Table 3-18.

Table 3-18 NCSI Configuration Parameter Descriptions

Parameter	Description	Setting
NCSI Mode	Way to specify a shared network port.	Select the NCSI mode: ● **Auto Failover Mode**: When the shared network port is abnormal, the server automatically switches to a network port in normal status as the shared network port. If **NCSI Mode** is set to **Auto Failover Mode**, you do not need to set any other parameters. ● **Manual Switch Mode**: You must manually specify a network port as the shared network port.

Parameter	Description	Setting
		If **NCSI Mode** is set to **Manual Switch Mode**, you must set **NCSI Interface**, **Channel Number** and **Package ID**.
NCSI Interface	Name of the NCSI.	Select **eth0** by default.
Channel Number	Network port number.	Select the number of the network port used as the shared network port.
Package ID	NIC ID.	Select the ID of the NIC where the shared network port is located.

5. Click **Save**.

3.7.13 Configuring Network Self-Adaptive Mode

Abstract

After the network self-adaptive mode is enabled, you can access the BMC through the IP address of the management network port regardless of whether the iSAC management network port or shared network port is in **UP** status.

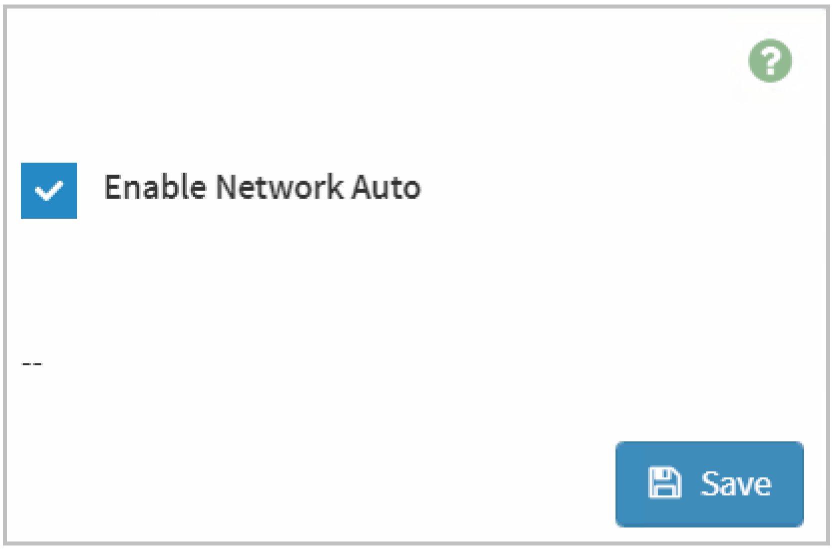
Prerequisite

The network bonding function has been disabled. For details, refer to "3.7.9 Configuring Network Bonding".

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Network Settings**. The **Network Settings** page is displayed.
3. Click **Network Adaptive Configuration**. The **Network Auto Settings** page is displayed, see Figure 3-34.

Figure 3-34 Network Auto Settings Page



☑ Enable Network Auto

--

4. Set the parameters. For a description of the parameters, refer to Table 3-19.

Table 3-19 Parameter Descriptions for Network Self-Adaptive Mode

Parameter	Description	Setting
Enable Network Auto	Whether to enable network self-adaptive mode.	● If you select **Enable Network Auto**, the network self-adaptive mode is enabled. ● If you clear **Enable Network Auto**, the network self-adaptive mode is disabled.

5. Click **Save**.

3.7.14 Configuring LLDP

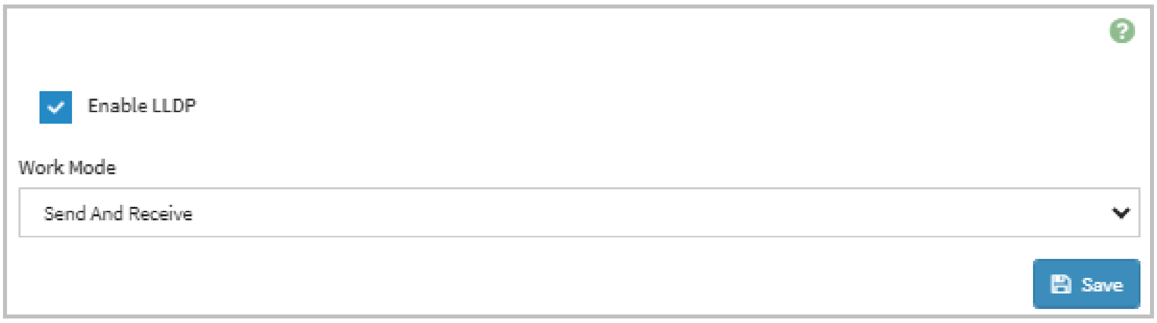
Abstract

After LLDP is enabled on a server, you can obtain the device information from adjacent network ports on the switch through LLDP packets.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Network Settings**. The **Network Settings** page is displayed.
3. Click **LLDP Configuration**. The **LLDP Configuration** page is displayed, as shown in Figure 3-35.

Figure 3-35 LLDP Configuration Page



☑ Enable LLDP

Work Mode

Send And Receive

4. Set the parameters. For a description of the parameters, refer to Table 3-20.

Table 3-20 LLDP Parameter Descriptions

Parameter	Description	Setting
Enable LLDP	Whether to enable LLDP.	● To enable LLDP, select **Enable LLDP**. ● To disable LLDP, deselect **Enable LLDP**.
Work Mode	LLDP working mode.	Select a LLDP working mode: ● **Receive**: only receives LLDP packets. ● **Send And Receive**: sends and receives LLDP packets.

5. Click **Save**.

3.7.15 Querying RAID Information

Abstract

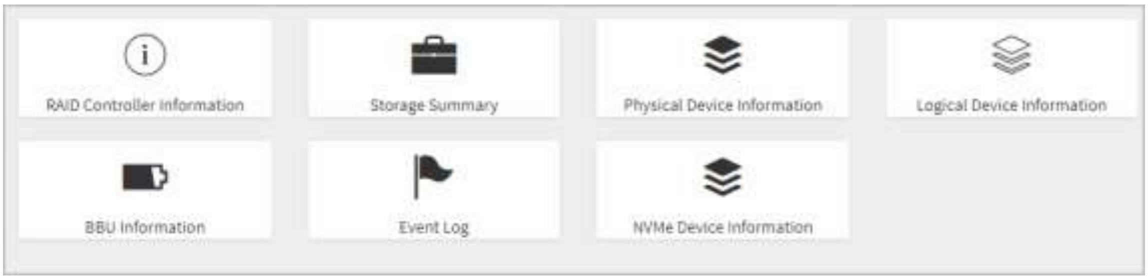
RAID information includes:

- Controller information: detailed information of the RAID controller, including the serial number, version number, and health status.
- Storage summary information: storage summary information of the RAID controller, including the number of physical devices, and that of logical devices.
- Physical device information: information of all the physical disks managed by the RAID controller.
- Logical device information: information of all the logical disks managed by the RAID controller.
- BBU information: battery information of the RAID controller.
- Event record: event list of the RAID controller.
- NVMe device information: NVMe device information.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **RAID Management**. The **RAID Management** page is displayed, see Figure 3-36.

Figure 3-36 RAID Management Page


RAID Controller Information
Storage Summary
Physical Device Information
Logical Device Information
BBU Information
Event Log
NVMe Device Information

3. Perform the following operations as required.

To...	Do...
Query RAID controller information	a. Click **RAID Controller Information**. The **RAID Controller Information** page is displayed. b. From the **RAID Controller** list, select the RAID controller you want to query. The information about the selected RAID controller is displayed in the lower part of the page. c. (Optional) In the **RAID Event Log Statistics** area, click **Details**. The **Event Log** page is displayed, where you can view the event logs of the RAID controller.
Query storage summary	a. Click **Storage Summary**. The **Storage Summary** page is displayed. b. From the **RAID Controller** list, select the RAID controller you want to query. The storage summary of the selected RAID controller is displayed in the lower part of the page. The storage summary of the RAID controller is described as follows: ● Number of physical devices: number of physical hard disks. ● Number of logical devices: number of logical disks. ● Number of global hot spare disks: number of physical hard disks used as global hot spare disks. ● Number of local hot spare disks: number of physical hard disks used as local hot spare disks.
Query physical device information	a. Click **Physical Devices Information**. The **Physical Devices Information** page is displayed. b. From the **Select the RAID Controller** list, select the RAID controller you want to query. The information about all the physical disks managed by the selected RAID controller is displayed in the lower part of the page. The **State** information in the physical disk information is described as follows: ● Online: The member disk of the logical disk is online. ● Missing: The member disk of the logical disk is removed. ● Offline: The member disk of the logical disk is offline. ● Rebuild: Rebuild. The hard disk is rebuilding data to ensure data redundancy and integrity of the logical disk.

To...	Do...
	● Shield State: Protected. Temporary status of the diagnosis operation. ● Hotspare: Hot spare disk. ● Copyback: Copyback. A new disk is replacing a faulty member disk. ● Bootable: Boot disk. ● Unconfigured_good: Not configured, and the hard disk is available. ● Unconfigured_bad: Not configured, and the hard disk is not available. ● PredictiveFailure: Failure. The hard disk is unavailable. ● ExposedToOS: Pass-through disk. This state is displayed when the RAID controller card is set to pass-through mode or set to mixed mode but no RAID controller card is created. c. (Optional) Click ⊞ on the right of the physical hard disk. More action options are displayed.
Query logical device information	a. Click **Logical Device Information**. The **Logical Device Information** page is displayed. b. From the **Select the RAID Controller** list, select the RAID controller you want to query. The information about all the logical disks managed by the selected RAID controller is displayed in the lower part of the page. The **State** information in the logical disk information is described as follows: ● Optimal: Optimization. ● Degraded: Degraded. ● Rebuilt: Rebuilt. ● Initialization: Initialization. ● Offline: Offline. c. (Optional) Click ⊞ on the right of the physical hard disk. More actions are displayed. d. (Optional) Click **Create Virtual Device**. A logical disk is created.
Query BBU information	a. Click **BBU Information**. The **BBU Information** page is displayed. b. From the **RAID Controller** list, select the RAID controller you want to be query. The BBU information of the selected RAID controller is displayed in the lower part of the page.
View event logs	a. Click **Event Log**. The **Event Log** page is displayed. b. From the **Select the RAID Controller** list, select the RAID controller you want to query. The event logs of the selected RAID controller are displayed in the lower part of the page.

To...	Do...
Query the NVMe device information	Click **NVMe Device Information**. The **NVMe Device Information** page is displayed, showing the NVMe device information below. In the NVMe device list, you can turn on the UID indicator of an NVMe device.

3.7.16 Querying SAS IT Information

Abstract

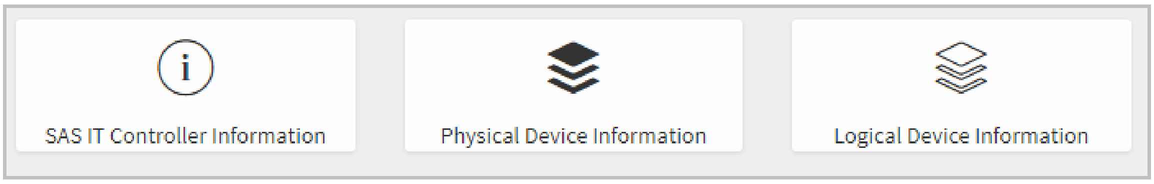
SAS IT information includes:

- Controller information: detailed information of the SAS IT controller, including the serial number, version number, and health status. The SAS IT controller usually includes the LSI HBA card and SDLSA card.
- Physical device information: information of all the physical disks managed by the SAS IT controller.
- Logical device information: Information of all the logical disks managed by the SAS IT controller.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **SAS IT Management**. The **SAS IT Management** page is displayed, see Figure 3-37.

Figure 3-37 SAS IT Management Page


SAS IT Controller Information
Physical Device Information
Logical Device Information

3. Perform the following operations as required.

To–	Do–
Query SAS IT controller information	a. Click **SAS IT Controller Information**. The **SAS IT Controller Information** page is displayed. b. From the **SAS IT Controller** list, select the SAS IT controller you want to query. The information about the selected SAS IT controller is displayed in the lower part of the page.
Query physical device information	a. Click **Physical Device Information**. The **Physical Device Information** page is displayed. b. From the **Select the SAS IT Controller** list, select the SAS IT controller you want to query. The information about all the physical disks

To–	Do–
	managed by the selected SAS IT controller is displayed in the lower part of the page.
Query logical device information	a. Click **Logical Device Information**. The **Logical Device Information** page is displayed. b. From the **Select the SAS IT Controller** list, select the SAS IT controller you want to query. The information about all the logical disks managed by the selected SAS IT controller is displayed in the lower part of the page.

3.7.17 Configuring Services

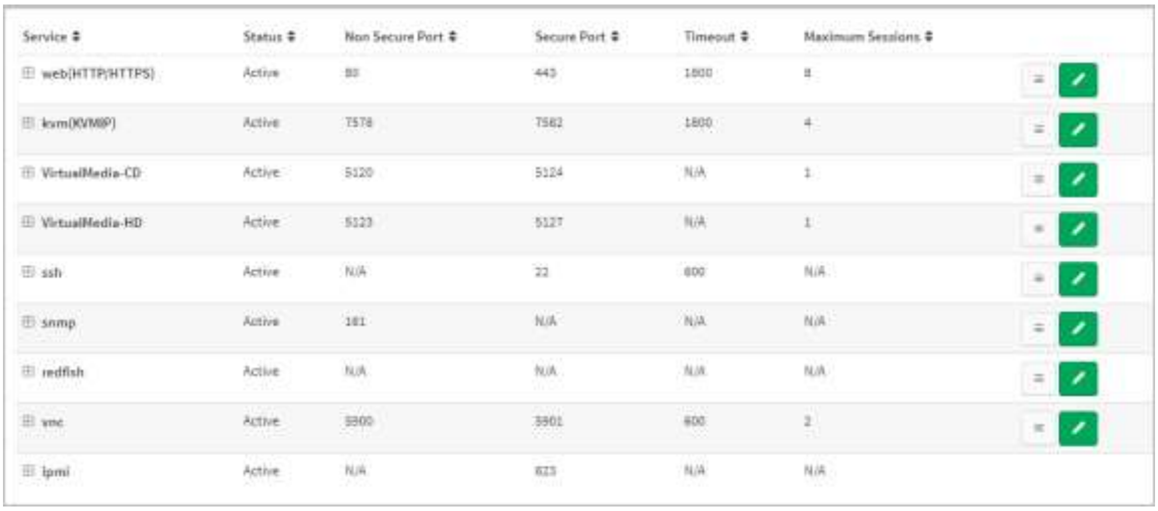
Abstract

This procedure describes how to configure the status, secure port, non-secure port, and timeout for a service of the BMC.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Services**. The **Services** page is displayed, see Figure 3-38.

Figure 3-38 Services Page



Service ⬍	Status ⬍	Non Secure Port ⬍	Secure Port ⬍	Timeout ⬍	Maximum Sessions ⬍
⊞ web(HTTP/HTTPS)	Active	80	443	1800	8
⊞ kvm(KVMIP)	Active	7578	7582	1800	4
⊞ VirtualMedia-CD	Active	5120	5124	N/A	1
⊞ VirtualMedia-HD	Active	5123	5127	N/A	1
⊞ ssh	Active	N/A	22	600	N/A
⊞ snmp	Active	161	N/A	N/A	N/A
⊞ redfish	Active	N/A	N/A	N/A	N/A
⊞ vnc	Active	5900	5901	600	2
⊞ ipmi	Active	N/A	623	N/A	N/A

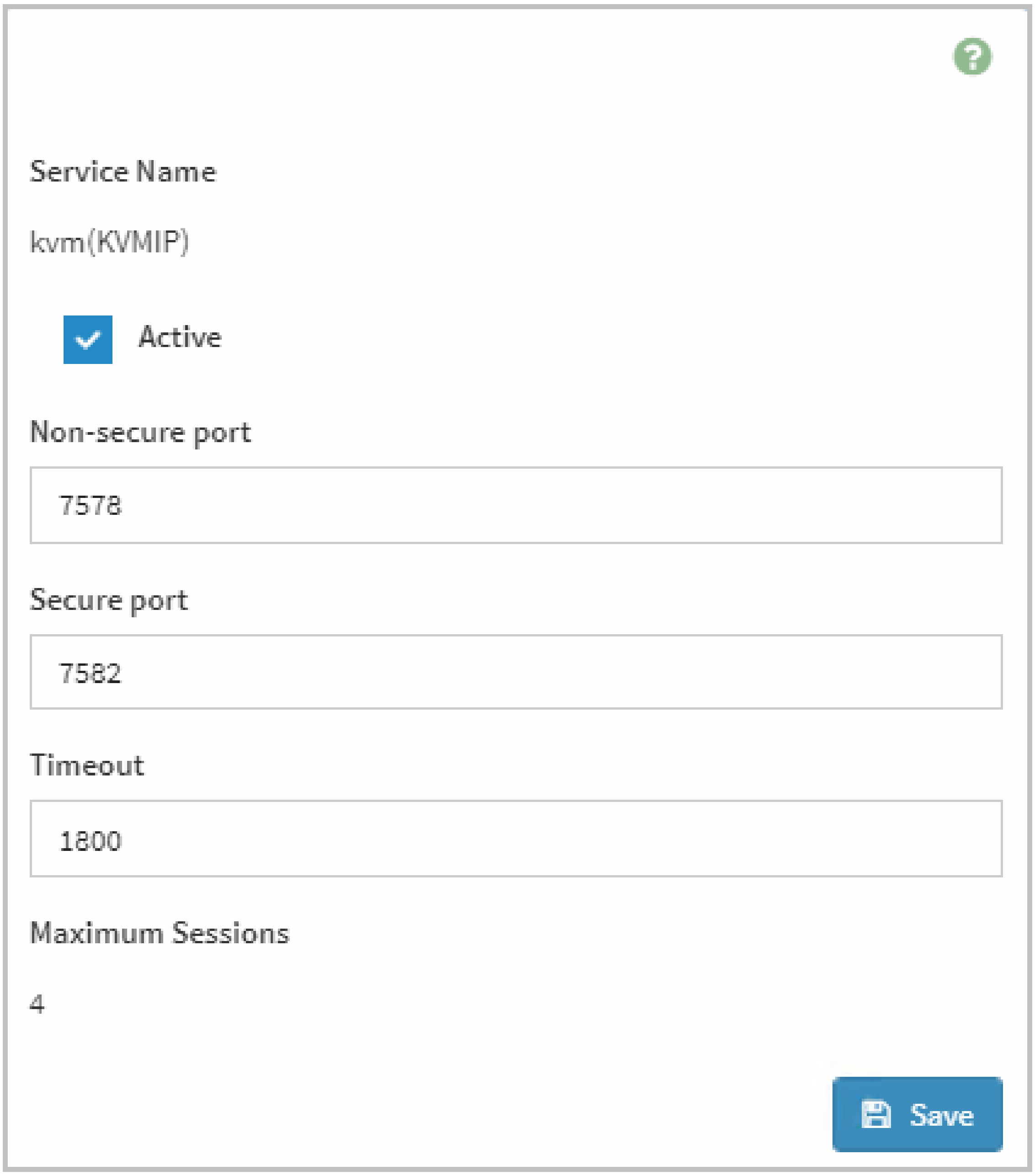
Note

Redfish is a server management specification. Based on the extensible platform management API, it uses the semantic RESTful interface to access the data defined in the model format for out-of-band system management. Redfish is applicable to the management and deployment of large-scale server cloud environment.

For a detailed description of Redfish, refer to the *VANTAGEO Server Redfish Interface Description*. For detailed steps to access the *VANTAGEO Server Redfish Interface Description*, refer to "6 Reference: Accessing Documents".

3. Click ✎ for the service to be configured. The **Service Configuration** page is displayed, see Figure 3-39.

Figure 3-39 Service Configuration Page



Service Name

kvm(KVMIP)

☑ Active

Non-secure port

7578

Secure port

7582

Timeout

1800

Maximum Sessions

4

Note

This procedure uses the KVM service as an example. The operations for configuring other services are similar.

4. Configure the parameters. For a description of the parameters, refer to Table 3-21.

Table 3-21 Service Parameter Descriptions

Parameter	Description	Setting
Active	Whether to enable the service.	● Select **Active**. The service is available. ● Deselect **Active**. The service is not available.
Non-secure port	Non-secure port number of the service.	● Default non-secure port number of the Web service: 80. ● Default non-secure port number of the KVM service: 7578. ● Default non-secure port number of the CD media service: 5120. ● Default non-secure port number of the HD media service: 5123. ● The SSH service does not support non-secure ports. ● Default non-secure port number of the SNMP service: 161. Range of the non-secure port number: 1 – 65535.
Secure port	Secure port number of the service.	● Default secure port number of the Web service: 443. ● Default secure port number of the KVM service: 7582. ● Default non-secure port number of the CD media service: 5124. ● Default non-secure port number of the HD media service: 5127. ● Default secure port number of the SSH service: 22. Range of the secure port number: 1–65535.
Timeout	Timeout period after which the service exits if no operation is performed.	● The timeout period of the Web service and KVM service ranges from 300 through 1800 seconds.

Parameter	Description	Setting
		● The timeout period of the SSH service ranges from 60 through 1800 seconds. The timeout period must be a multiple of 60.

5. Click **Save**.

Verification

- Set the status of the Redfish service to **Active** to enable query and configuration of the BMC through the Redfish interface.
  For a detailed description of Redfish, refer to the *VANTAGEO Server Redfish Interface Description*. For detailed steps to access the *VANTAGEO Server Redfish Interface Description*, refer to "6 Reference: Accessing Documents".
- Set the status of the SNMP service to **Active** and configure the correct **Non Secure Port** to enable query and configuration of the BMC through the SNMP interface.
  For a detailed description of SNMP, refer to the *VANTAGEO Server SNMP Interface Description*. For detailed steps to access the *VANTAGEO Server SNMP Interface Description*, refer to "6 Reference: Accessing Documents".

3.7.18 Configuring an Alarm Mailbox

Abstract

To send the alarm information of the server to a specified mailbox, you must configure the alarm mailbox.

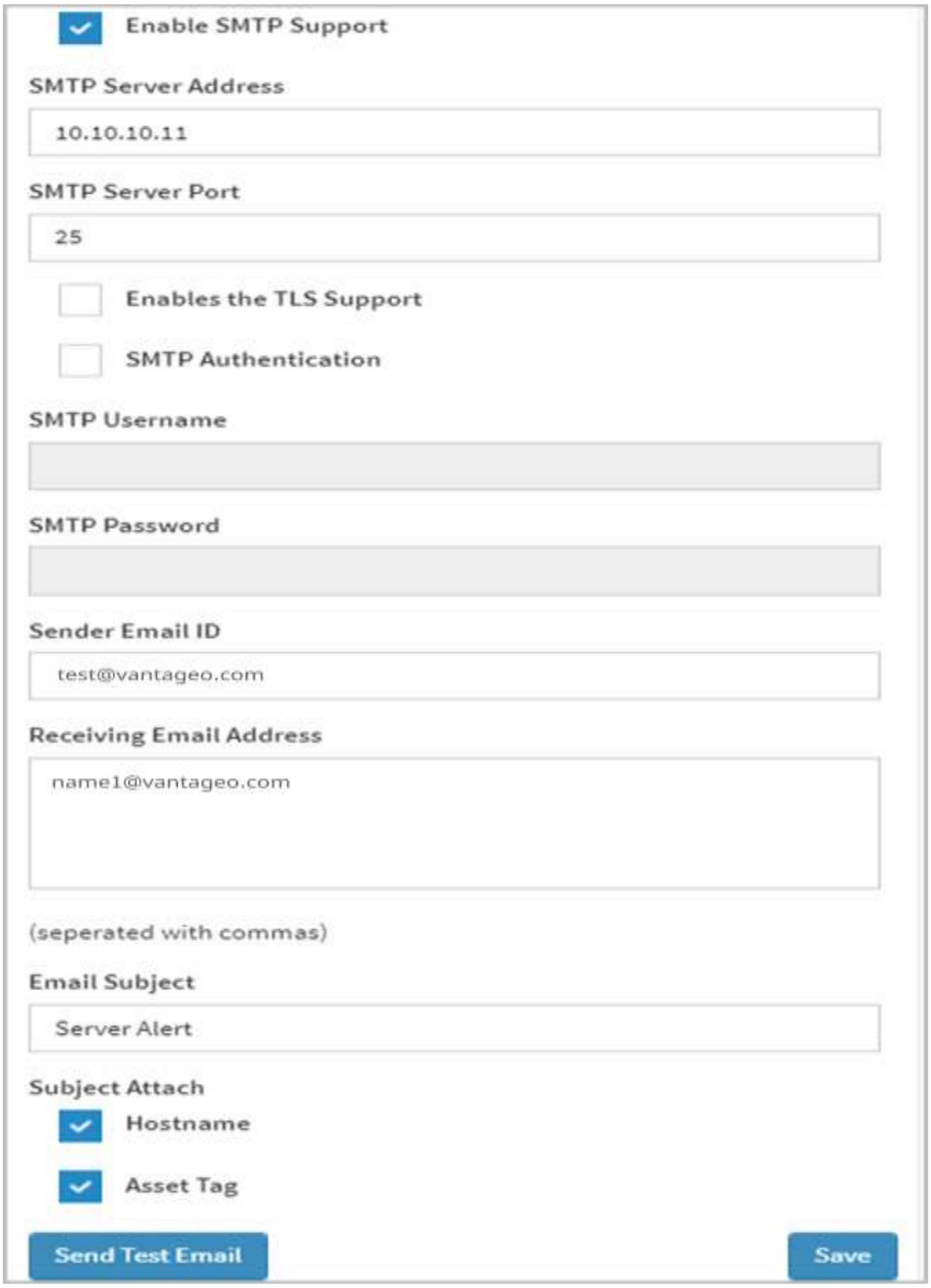
Prerequisite

The SMTP server is configured. For details, refer to "4.12 Configuring the SMTP Server".

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **SMTP Settings**. The **SMTP Settings** page is displayed, see Figure 3-40.

Figure 3-40 SMTP Settings Page



☑ Enable SMTP Support

SMTP Server Address

10.10.10.11

SMTP Server Port

25

□ Enables the TLS Support

□ SMTP Authentication

SMTP Username

SMTP Password

Sender Email ID

test@vantageo.com

Receiving Email Address

name1@vantageo.com

(seperated with commas)

Email Subject

Server Alert

Subject Attach

☑ Hostname

☑ Asset Tag

3. Configure the parameters. For a description of the parameters, refer to Table 3-22.

Table 3-22 Parameter Descriptions for the Alarm Box Configuration

Parameter	Description	Setting
Enable SMTP Support	Whether to send alarms to a specified mailbox.	Select **Enable SMTP Support**.
SMTP Server Address	IP address of the SMTP server.	Enter the IP address of the SMTP server.
SMTP Server Port	Port number of the SMTP server.	The port number range is 1–65535, and the default port number is 25.
Enables the TLS Support	Whether to enable TLS encryption.	To enable TLS encryption, select **Enables the TLS Support**.
SMTP Authentication	Whether to enable SMTP authentication.	To enable SMTP authentication, select **SMTP Authentication**, and set **SMTP Username** and **SMTP Password**.
Sender Email ID	Email address of the sender.	Enter the email address of the sender.
Receiving Email Address	Email address of a recipient.	Enter the email addresses of the recipients, which are separated with commas.
Email Subject	Subject of the alarm email.	Enter the subject of the alarm email.
Subject Attach	Whether to attach **Hostname** and **Asset Tag** to the subject.	Select the information to be attached.

4. Click **Save**.

Verification

1. Click the **Send Test Mail** button on the **SMTP Settings** page.
2. Check on the SMTP server whether a testing email is received.

3.7.19 Configuring SSL

Abstract

To make a link to access the BMC Web portal to be a secure link, you must configure SSL.

You can perform the following operations to configure SSL:

1. Upload the SSL certificate in your browser
2. Upload the SSL certificate on the BMC Web portal

Prerequisite

The certificate file and private key file of the `pem` type are obtained.

Steps

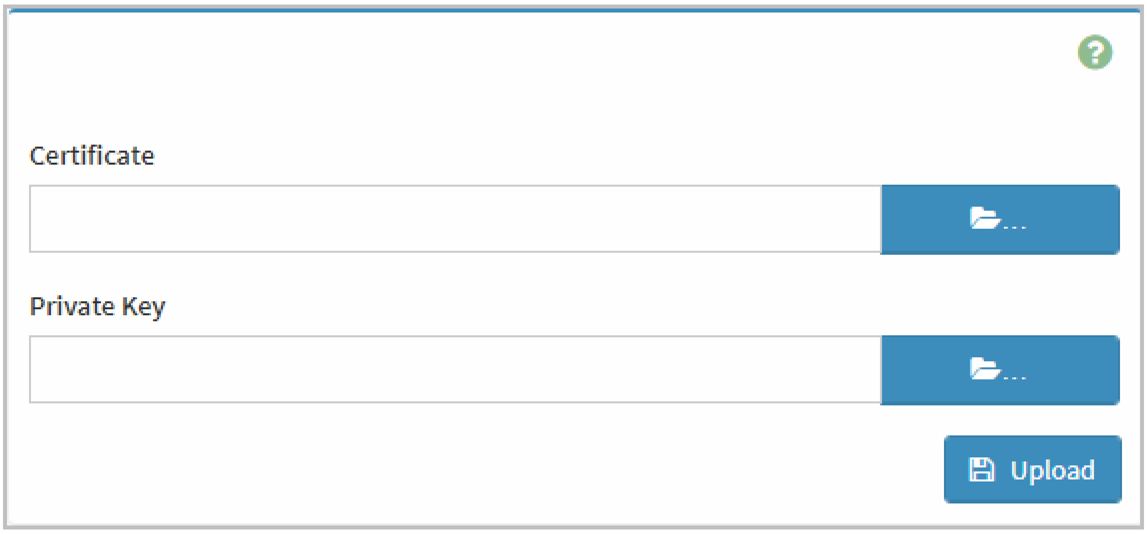
Uploading the SSL Certificate in Your Browser

1. On the **Settings** page of the browser (for example, Chrome) on the client PC, select **Privacy and security**. The **Privacy and security** page is displayed.
2. Click ↗ on the right of **Manage certificates** and upload the SSL certificate.

Uploading the SSL Certificate on the BMC Web Portal

3. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
4. Click **SSL Settings**. The **SSL Settings** page is displayed.
5. Click **Upload SSL certificate**. The page for uploading the SSL certificate is displayed, see Figure 3-41.

Figure 3-41 Uploading the SSL Certificate

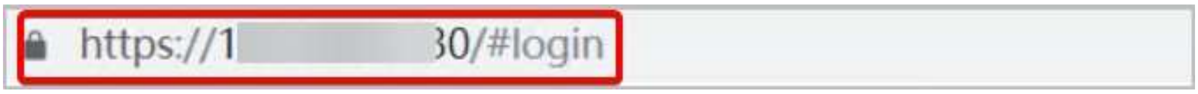


6. Select the prepared certificate file and private key file.
7. Click **Upload**.

Verification

In the address bar of your browser, enter the address of the BMC Web portal, and press **Enter**. Check whether the **Welcome** page is displayed and the address bar of the browser does not prompt "Not secure", see Figure 3-42.

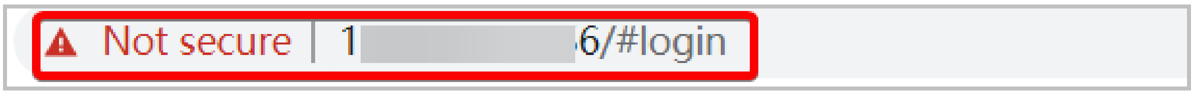
Figure 3-42 Welcome Page



https://1[redacted]30/#login

Figure 3-43 shows the page where the address bar of the browser prompts "Not secure".

Figure 3-43 Not Secure Connection Page



Not secure | 1[redacted]6/#login

3.7.20 Configuring the Default Firewall Policy

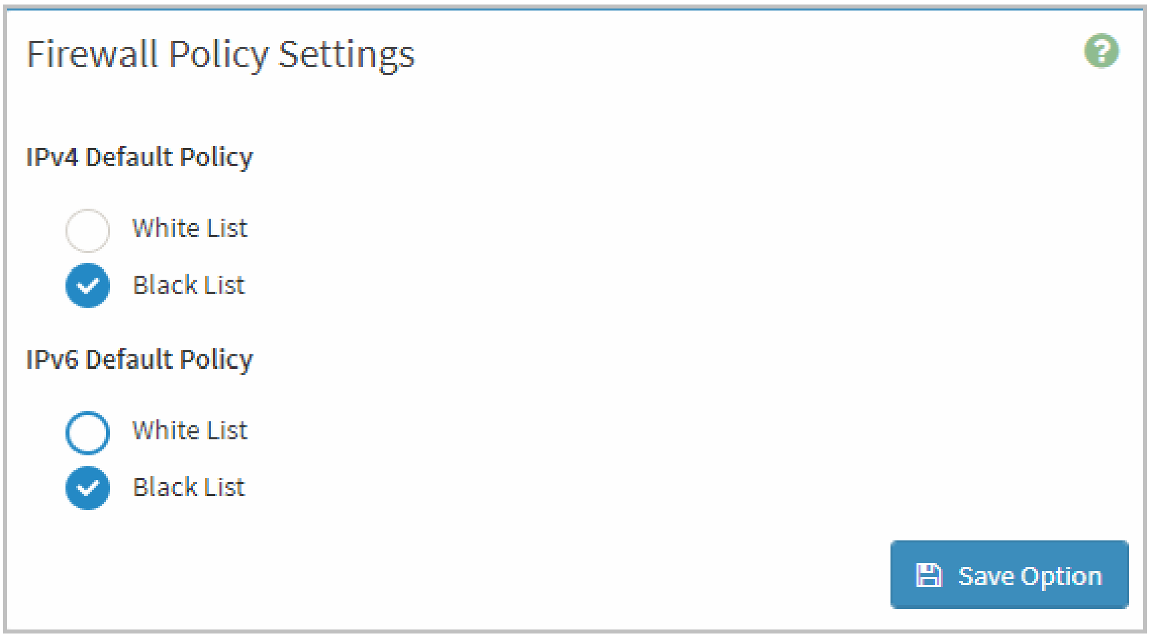
Abstract

If the existing firewall rules do not match, a server uses the default firewall policy.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **System Firewall**. The **System Firewall** page is displayed.
3. Click **Firewall Policy Settings**. The **Firewall Policy Settings** page is displayed, see Figure 3-44.

Figure 3-44 Firewall Policy Settings Page



Firewall Policy Settings

IPv4 Default Policy

○ White List

✓ Black List

IPv6 Default Policy

○ White List

✓ Black List

4. Select **White List** or **Black List**.
   - **White List**: The users in the whitelist are allowed to access the server.
     If **White List** is enabled, you must configure an **Allow** rule first.
     The **Allow** rule can be any one or more of the IP address firewall rule, MAC address firewall rule or port firewall rule.
   - **Black List**: The users in the blacklist are not allowed to access the server.
5. Click **Save Option**.

3.7.21 Configuring an IP Address Firewall Rule

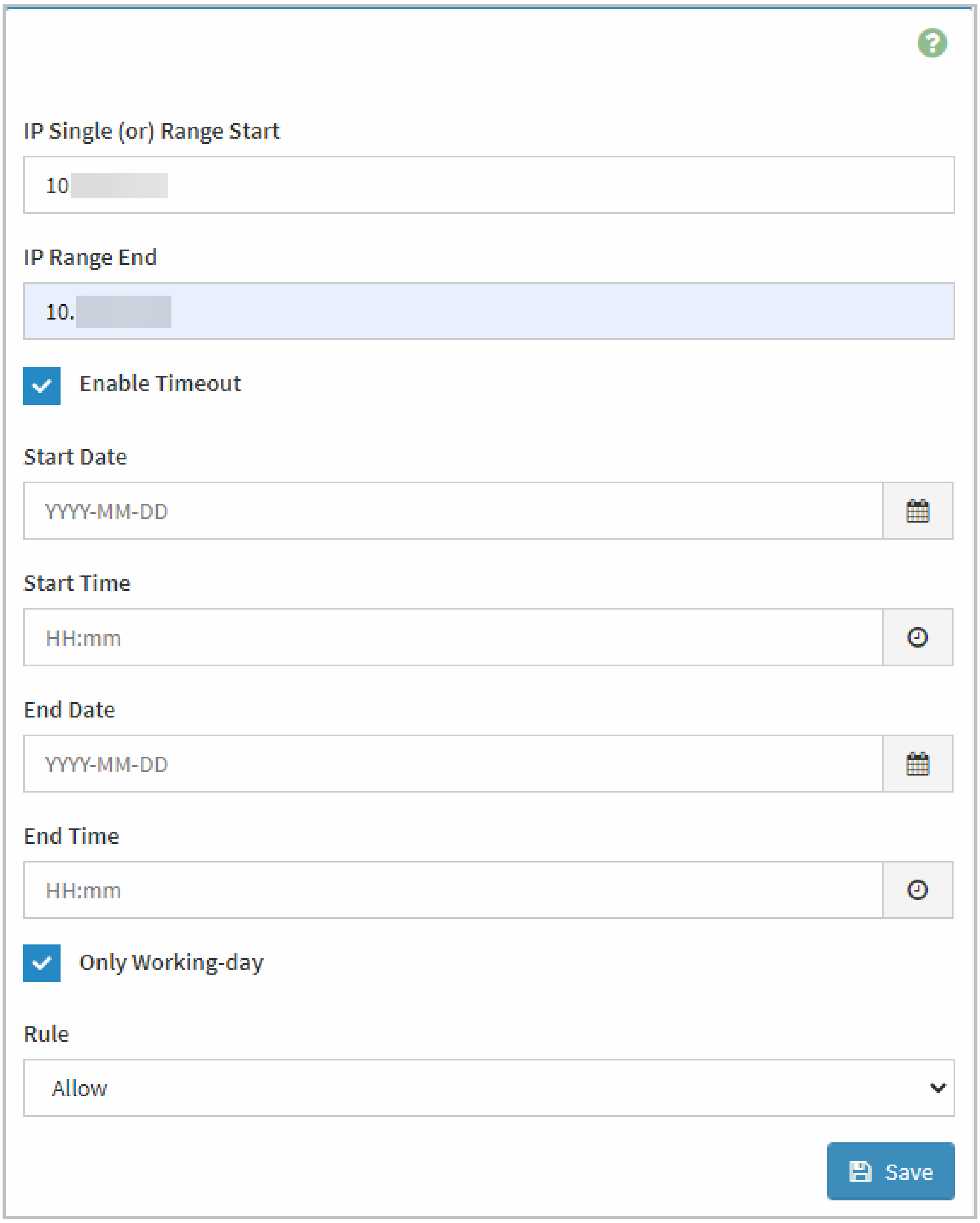
Abstract

This procedure describes how to configure an IP address firewall rule to allow or disallow the devices with the specified IP addresses to access the server.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **System Firewall**. The **System Firewall** page is displayed.
3. Click **IP Address Firewall Rules**. The **IP Firewall Rules** page is displayed.
4. Click **Add New IP Rule**. The **Add IP Rule** page is displayed, see Figure 3-45.

Figure 3-45 Add IP Rule Page



IP Single (or) Range Start

10[redacted]

IP Range End

10.[redacted]

☑ Enable Timeout

Start Date

YYYY-MM-DD

Start Time

HH:mm

End Date

YYYY-MM-DD

End Time

HH:mm

☑ Only Working-day

Rule

Allow

5. Configure the parameters. For a description of the parameters, refer to Table 3-23.

Table 3-23 Parameter Descriptions for the IP Address Firewall Rule

Parameter	Description	Setting
IP Single (or) Range Start	Single IP address or the start address of an IP address segment.	● For a single IP address, enter this address. ● For an IP address segment, enter the start address.

Parameter	Description	Setting
IP Range End	End address of the IP address segment. This parameter is optional.	For an IP address segment, enter the end address.
Enable Timeout	Whether to enable the firewall timeout rule.	● Select **Enable Timeout**. The firewall rule is valid in a specified time period. The time period can be set in **Start Date**, **Start Time**, **End Date** and **End Time**. You can also select **Only Working-day**, so that the firewall rule is effective on working days. ● If you do not select **Enable Timeout**, the firewall rule becomes valid immediately.
Rule	**Allow** or **Block**.	Select the type of firewall rule: ● **Allow**: Allows the devices with the specified IP addresses to access the server. ● **Block**: Blocks the devices with the specified IP addresses from accessing the server.

6. Click **Save.**

3.7.22 Configuring a MAC Address Firewall Rule

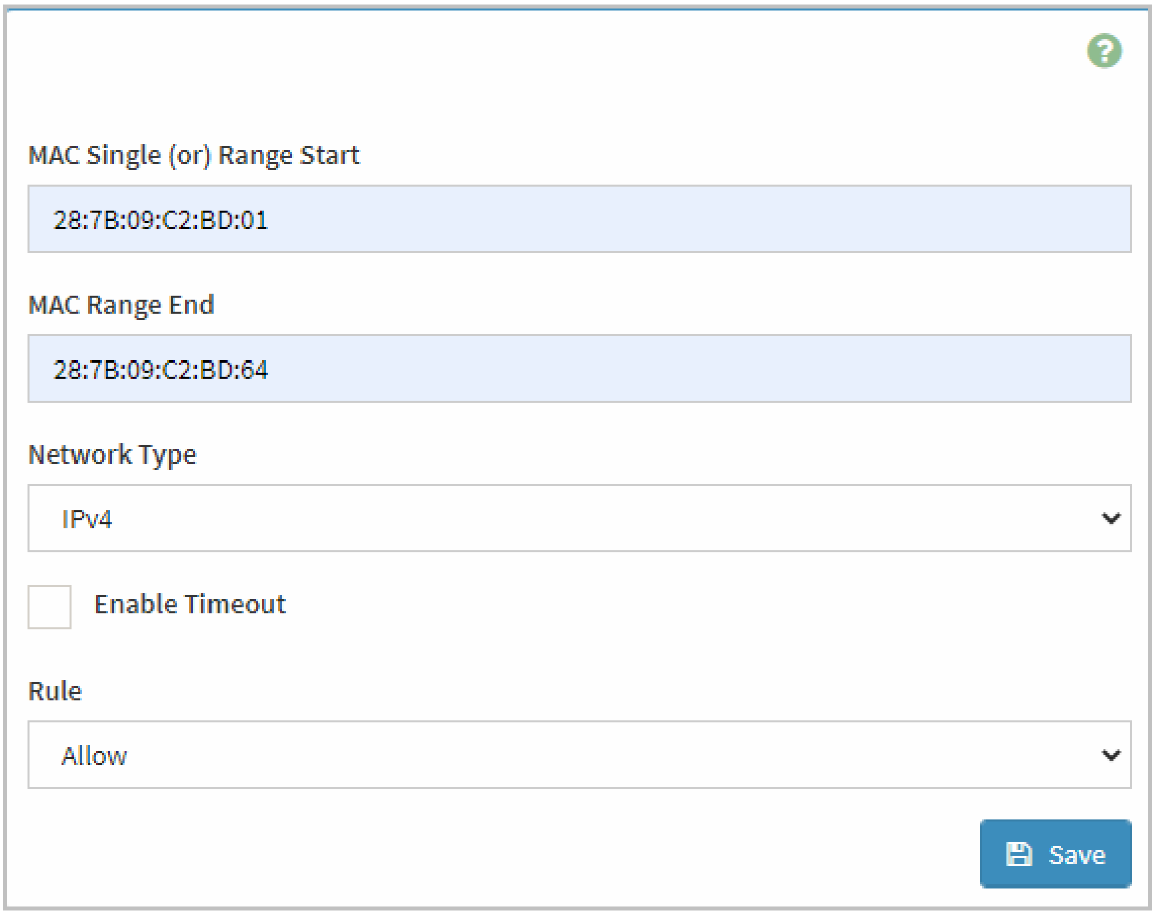
Abstract

This procedure describes how to configure a MAC address firewall rule to allow or disallow the devices with the specified MAC addresses to access a server.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **System Firewall**. The **System Firewall** page is displayed.
3. Click **MAC Firewall Rules**. The **MAC Firewall Rules** page is displayed.
4. Click **Add New MAC Rule**. The **Add New MAC Rule** page is displayed, see Figure 3-46.

Figure 3-46 Add New MAC Rule Page



MAC Single (or) Range Start

28:7B:09:C2:BD:01

MAC Range End

28:7B:09:C2:BD:64

Network Type

IPv4

□ Enable Timeout

Rule

Allow

5. Configure the parameters. For a description of the parameters, refer to Table 3-24.

Table 3-24 Parameter Descriptions for the MAC Address Firewall Rule

Parameter	Description	Setting
MAC Single (or) Range Start	Single MAC address or the start address of a MAC address segment.	● For a single MAC address, enter this address. ● For a MAC address segment, enter the start address.
MAC Range End	End address of a MAC address segment. This parameter is optional.	For a MAC address segment, enter the end address. Only the last byte of the end MAC address can be different from the start MAC address, and a maximum of 64 MAC addresses are allowed between the end MAC address and the start MAC address.
Network Type	**IPv4**, **IPv6** or **Both**.	Select the corresponding network type.
Enable Timeout	Whether to enable the firewall timeout rule.	● Select **Enable Timeout**. The firewall rule is valid in a specified time period. The time period can be set in **Start Date**, **Start Time**, **End Date** and **End Time**.

Parameter	Description	Setting
		You can also select **Only Working-day**, so that the firewall rule is effective on working days. ● If you do not select **Enable Timeout**, the firewall rule becomes valid immediately.
Rule	**Allow** or **Block**.	Select the type of firewall rule: ● **Allow**: Allows the devices with the specified MAC addresses to access the server. ● **Block**: Blocks the devices with the specified MAC addresses from accessing the server.

6. Click **Save**.

3.7.23 Configuring a Port Firewall Rule

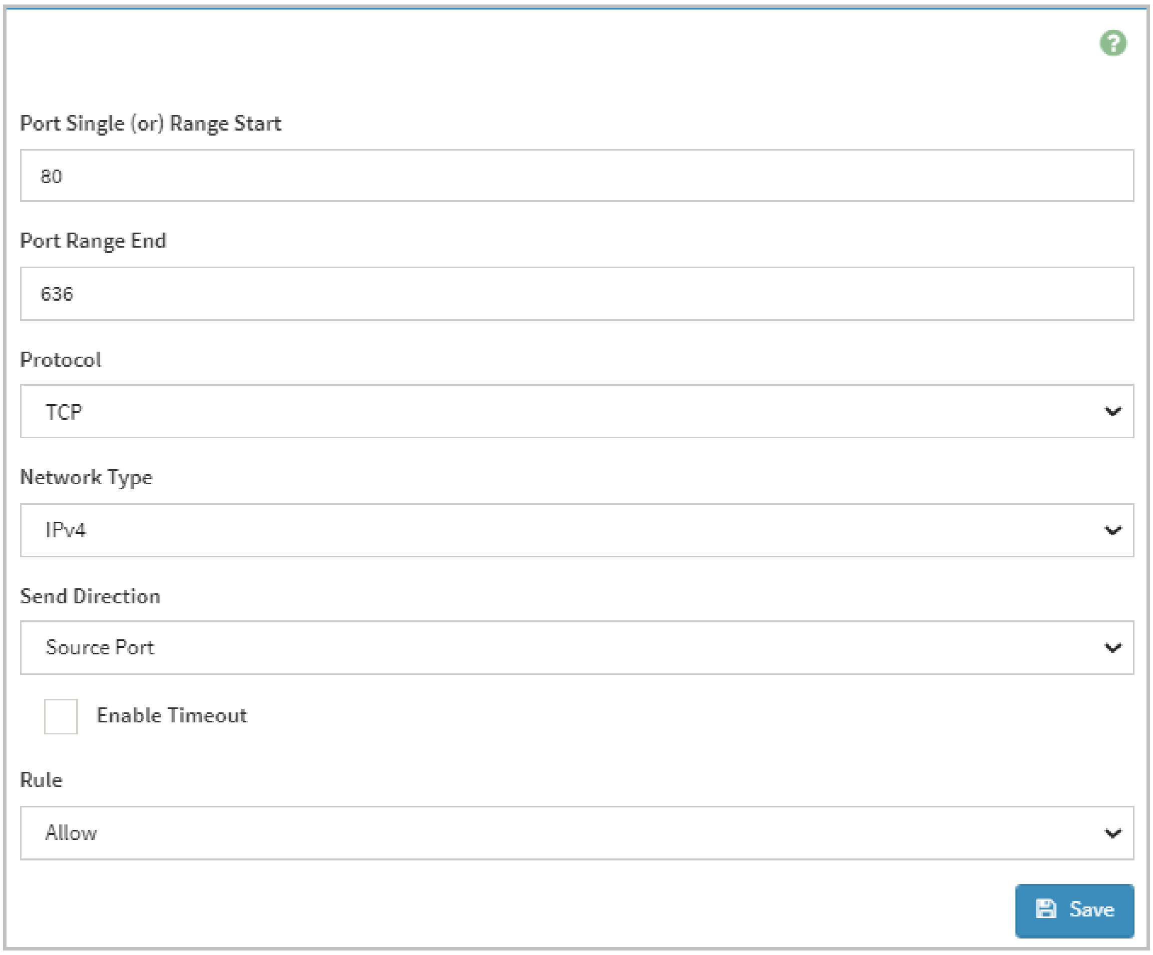
Abstract

This procedure describes how to configure a port firewall rule to allow or disallow a device to access the server through a specified port.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **System Firewall**. The **System Firewall** page is displayed.
3. Click **Port Firewall Rules**. The **Port Firewall Rules** page is displayed.
4. Click **Add New Port Rule**. The **Add New Port Rule** page is displayed, see Figure 3-47.

Figure 3-47 Add New Port Rule Page



Port Single (or) Range Start

80

Port Range End

636

Protocol

TCP

Network Type

IPv4

Send Direction

Source Port

□ Enable Timeout

Rule

Allow

5. Configure the parameters. For a description of the parameters, refer to Table 3-25.

Table 3-25 Port Rule Parameter Descriptions

Parameter	Description	Setting
Port Single (or) Range Start	Single port or the start port of a port range.	● For a single port, enter the port number. ● For a port range, enter the start port number. Port range: 1–65535.
Port Range End	End port. This parameter is optional.	For a port range, enter the end port number. Port range: 1–65535.
Protocol	Protocol type.	Select the corresponding protocol type.
Network Type	**IPv4**, **IPv6** or **Both**.	Select the corresponding network type.
Send Direction	**Source Port** or **Destination port**.	Select the corresponding sending direction.
Enable Timeout	Whether to enable the firewall timeout rule.	● Select **Enable Timeout**. The firewall rule is valid in a specified time period. The time period can be set in **Start Date**, **Start Time**, **End Date** and **End Time**.

Parameter	Description	Setting
		● If you do not select **Enable Timeout**, the firewall rule becomes valid immediately.
Rule	**Allow** or **Block**.	Select the type of firewall rule: ● **Allow**: Allows to access the server through the specified port. ● **Block**: Blocks accessing the server through the specified port.

6. Click **Save**.

3.7.24 Creating a User

Abstract

This procedure describes how to create a BMC user by using the user group management and user management functions.

To create a user, perform the following steps:

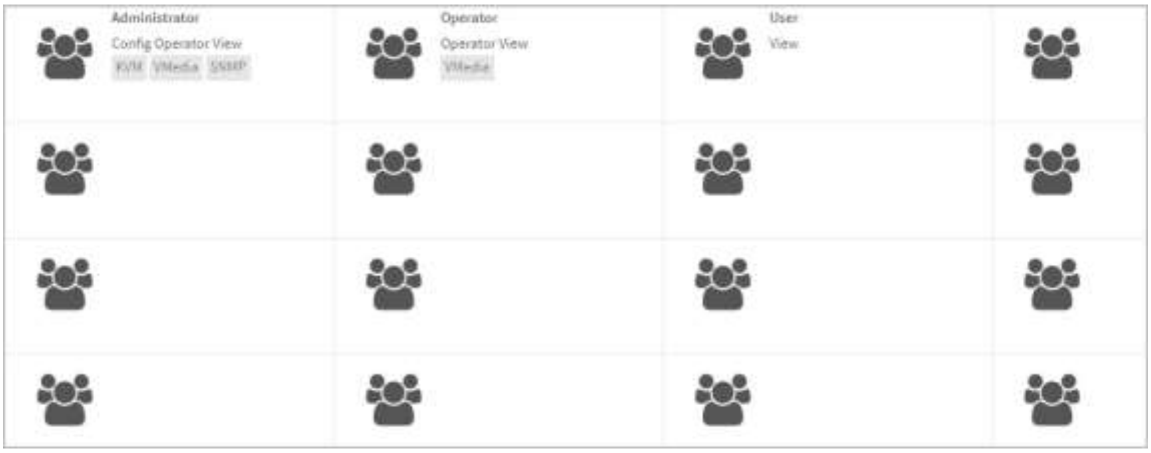
1. Add a user group
2. Add a user

Steps

Adding a User Group

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Group Management**. The **Group Management** page is displayed, see Figure 3-48.

Figure 3-48 Group Management Page

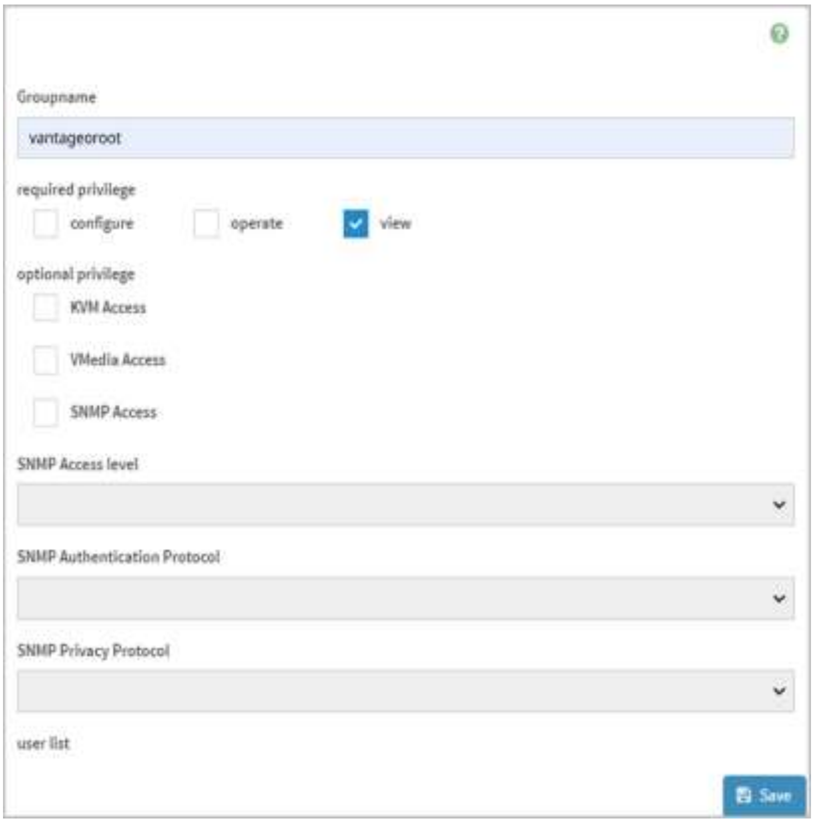


Note

The existing user group has a group name on the right of the user group icon, and the new user group has no group name. To add a user group, click the new user group icon.

3. Click the icon for the new user group. The **Group Management Configuration** page is displayed, see Figure 3-49.

Figure 3-49 Group Management Configuration Page



Groupname
vantageoroot

required privilege
□ configure □ operate ☑ view

optional privilege
□ KVM Access
□ VMedia Access
□ SNMP Access

SNMP Access level

SNMP Authentication Protocol

SNMP Privacy Protocol

user list

4. Configure the parameters. For a description of the parameters, refer to Table 3-26.

Table 3-26 Group Parameter Descriptions

Parameter	Description	Setting
Groupname	Name of the user group.	Enter a user group name. ● The group name is a string composed of 4–16 letters, digits, " - " , " _ " or " @ " , which must start with a letter. ● Letters are case-sensitive.

Parameter	Description	Setting
required privilege/optional privilege	Operation permissions of the users in the user group.	The permissions are divided into required permissions and optional permissions. ● Required permission: Select at least one of the following permissions: → **configure** → **operate** → **view** In most cases, the required permissions for the user group of each role are as follows: → Administrator: **configure**, **operate**, and **view** → Operator: **operate** and **view** → Viewer: **view** ● Optional permission: Select one of the following permissions as needed. → **KVM Access** → **VMedia Access** → **SNMP Access** In most cases, the optional permissions of each role user group are as follows: → Administrator: **KVM Access**, **VMedia Access**, and **SNMP Access** → Operator: **SNMP Access** → Viewer: not applicable
SNMP Access level	SNMP access level.	When **SNMP Access** is selected for **optional privilege**, you must configure this parameter. Select an SNMP access level, including: ● Read Only ● Read Write
SNMP Authentication Protocol	SNMP authentication protocol.	When **SNMP Access** is selected for **optional privilege**, you must configure this parameter. Select an SNMP authentication protocol, including: ● NONE ● SHA ● MD5 ● SHA256 ● SHA384 ● SHA512
SNMP Privacy Protocol	SNMP encryption mode.	When **SNMP Access** is selected for **optional privilege**, you must configure this parameter. Select an SNMP encryption mode, including: ● NONE

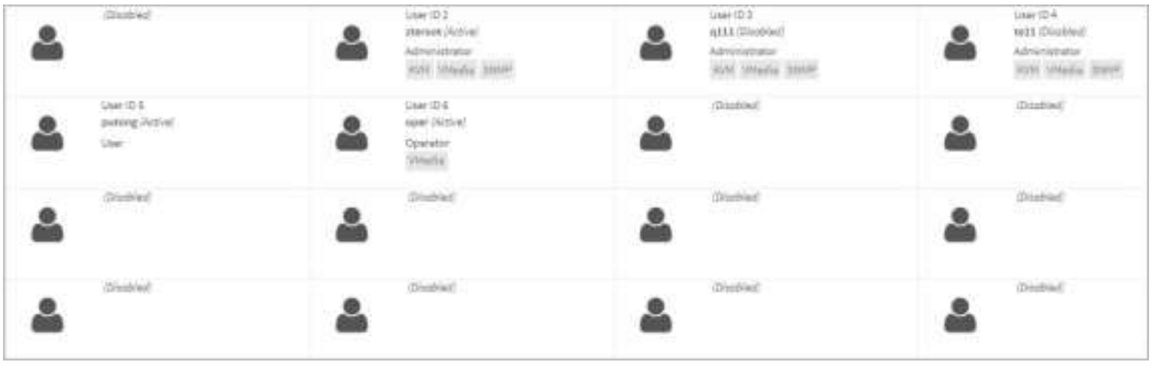
Parameter	Description	Setting
		● DES ● AES ● AES256 If **SNMP Authentication Protocol** is set to **NONE**, **SNMP Privacy Protocol** can only be set to **NONE**. **AES256** can be used together with only **SHA256**, **SHA384**, or **SHA512**.

5. Click **Save**.

Adding a User

6. On the **Settings** page, click **User Management**. The **User Management** page is displayed, see Figure 3-50.

Figure 3-50 User Management Page

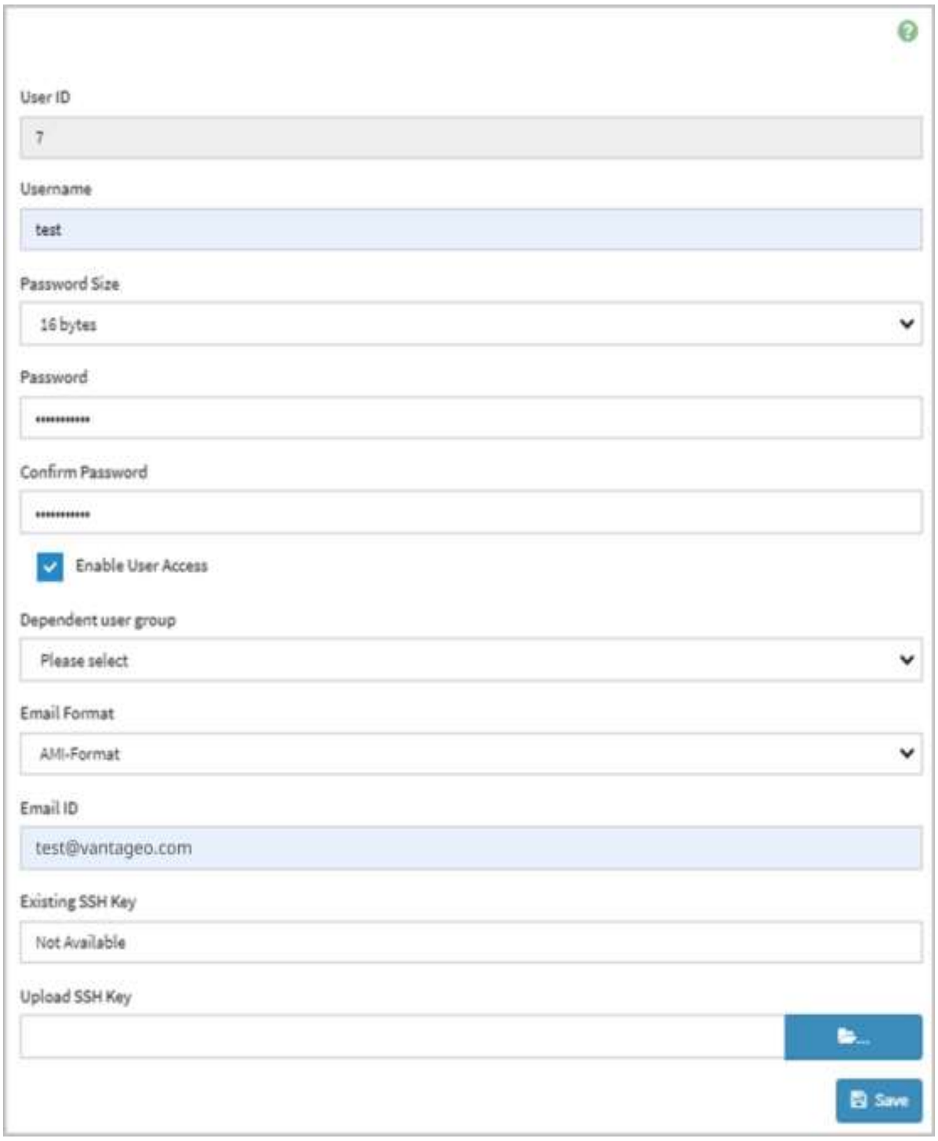


Note

The existing user has a user name on the right of the user icon, and the new user has no user name. To add a user, click the new user icon. The first user in the upper left corner is reserved and cannot be created or modified.

7. Click the icon for the new user. The **User Management Configuration** page is displayed, see Figure 3-51.

Figure 3-51 User Management Configuration Page



User ID

7

Username

test

Password Size

16 bytes

Password

•••••••••••

Confirm Password

•••••••••••

☑ Enable User Access

Dependent user group

Please select

Email Format

AMI-Format

Email ID

test@vantageo.com

Existing SSH Key

Not Available

Upload SSH Key

8. Configure the parameters. For a description of the parameters, refer to Table 3-27.

Table 3-27 User Parameter Descriptions

Parameter	Description	Setting
User ID	User ID.	Generated by the system automatically and cannot be configured.
Username	User name.	Enter a username. ● The username is a string composed of 4–16 letters, digits, " - " , " _ " or " @ " , which must start with a letter. ● Letters are case-sensitive.

Parameter	Description	Setting
		● It is not allowed to use anonymous, root, admin, users, nobody, username, or sysadmin as the username, and the username and password must not be the same.
Password Size	Length of the password to be entered in **Password**/**Confirm Password**.	Select a password length.
Password	User password.	Enter the user password. It is allowed to enter letters, digits, and symbols. Letters are case-sensitive. ● The password must not contain spaces or tabs. ● If a strong password is enabled, the password must contain four types of characters (upper-case letters, lower-case letters, digits, and symbols).
Confirm Password	Confirm the user password.	Enter the password for confirmation, which must be the same as **Password**.
Enable User Access	Whether to enable the user immediately.	The added user can take effect only after this option is selected.
Dependent user group	User group that the user belongs to.	Select a user group for the user. The user inherits the permissions of the user group that the user belongs to.
Email Format	Format of emails sent by the BMC to the user.	Select an email format: ● **AMI-Format**: The email title format is " Alert from (host address) " . The emails in this format display sensor information, for example, sensor types and descriptions. ● **FixedSubject-Format**: The emails in this format display messages in accordance with user settings. The user must specify the email subject and messages in advance.
Email ID	Email address of the user.	Enter an email address.
Existing SSH Key	Displays the SSH key uploaded by the user.	-
Upload SSH Key	Uploads a public SSH key to the server. The file size cannot exceed 4 KB.	Click 📂... and select a key file.

9. Click **Save**.

3.7.25 Configuring Screen Recording Parameters

Abstract

By configuring screen recording parameters, you can specify the events that trigger screen recording and the recording duration.

The recorded videos can be viewed on the **Video Log** page.

Prerequisite

To enable the screen recording function, you need to enable the KVM service. For details, refer to "3.7.17 Configuring Services".

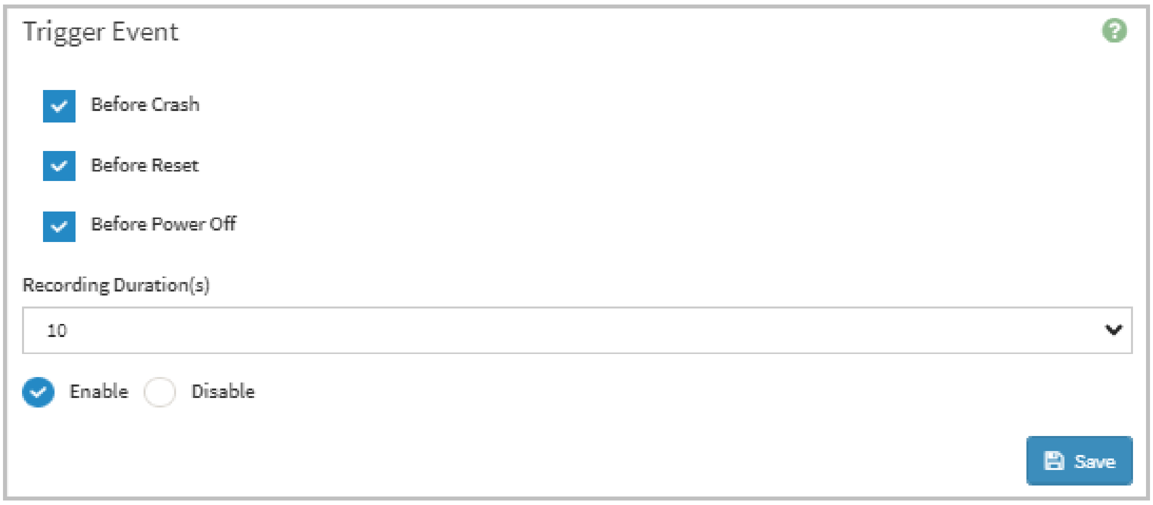
Note

The launch of a KVM or VNC session temporarily disables recording. After the KVM or VNC session is closed, recording is automatically resumed.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Video Trigger Settings**. The **Video Trigger Settings** page is displayed, as shown in Figure 3-52.

Figure 3-52 Video Trigger Settings Page



Trigger Event

☑ Before Crash

☑ Before Reset

☑ Before Power Off

Recording Duration(s)

10

● Enable ○ Disable

3. Set the parameters. For a description of the parameters, refer to Table 3-28.

Table 3-28 Screen Recording Parameter Descriptions

Parameter	Description	Setting
Before Crash/Before Reset/Before Power Off	Select the events that trigger screen recording.	Select the events that trigger screen recording.
Recording Duration(s)	Select a recording duration.	Select a recording duration. Range: 10–60 seconds.
Enable/Disable	Whether to enable the screen recording function.	Select whether to enable the screen recording function.

4. Click **Save**.

3.7.26 Configuring a Boot Mode

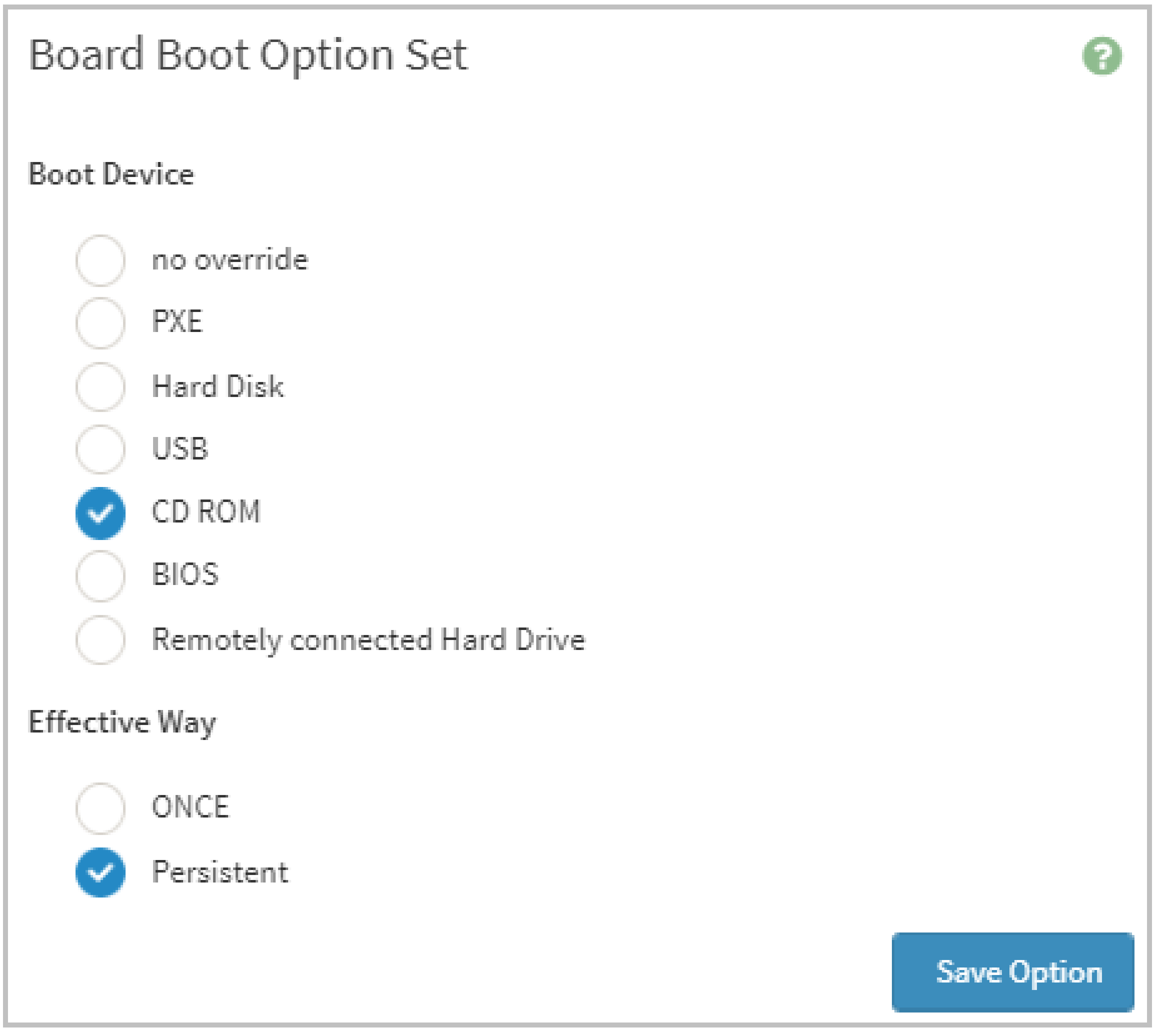
Abstract

This procedure describes how to configure a boot mode, including the boot device and the application mode of the server.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Boot Option Settings**. The **Boot Option** page is displayed, see Figure 3-53.

Figure 3-53 Boot Option Page



Board Boot Option Set

Boot Device

○ no override
○ PXE
○ Hard Disk
○ USB
● CD ROM
○ BIOS
○ Remotely connected Hard Drive

Effective Way

○ ONCE
● Persistent

3. Configure the parameters. For a description of the parameters, refer to Table 3-29.

Table 3-29 Boot Option Parameter Descriptions

Parameter	Description
Boot Device	Hardware device used to boot the server system. ● **no override**: The first boot device is not set. The default boot mode set in BIOS prevails, which is not controlled by the BMC. ● **PXE**: The system is forcibly started through the network. ● **Hard Disk**: The system is booted forcibly through the hard disk. ● **USB**: The system is forcibly booted through USB. ● **CD ROM**: The system is forcibly booted through the CD-ROM drive. ● **BIOS**: After the server is booted, the BIOS menu is displayed. ● **Remotely connected Hard Drive**: The system is forcibly started through the remote hard disk.
Effective Way	Whether the reconfigured server boot is applied only once. ● **ONCE**: only effective for this restart.

Parameter	Description
	● **Persistent**: permanently effective.

4. Click **Save Option**.

3.7.27 Modifying BIOS Parameters

Abstract

This procedure describes how to modify BIOS parameters on the Web portal of the BMC.

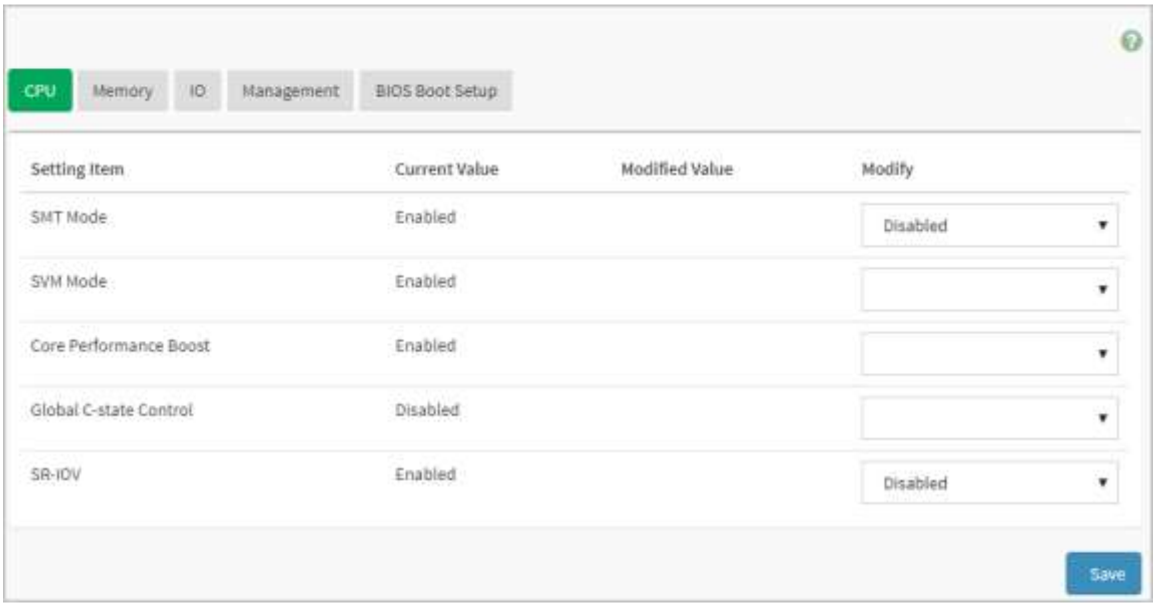
Note

This function is applicable to only server models developed based the Hygon platform.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **BIOS Setting**. The **BIOS Setting** page is displayed, as shown in Figure 3-54.

Figure 3-54 BIOS Setting Page



Setting Item	Current Value	Modified Value	Modify
SMT Mode	Enabled		Disabled ▾
SVM Mode	Enabled		▾
Core Performance Boost	Enabled		▾
Global C-state Control	Disabled		▾
SR-IOV	Enabled		Disabled ▾

3. For the BIOS parameter that you want to modify, select the target value in the **Modify** column.
4. Click **Save**.

Note

After the modification is saved, the target value is displayed in the **Modified Value** column. The modification takes effect after the server is restarted.

3.7.28 Configuring Login Parameters

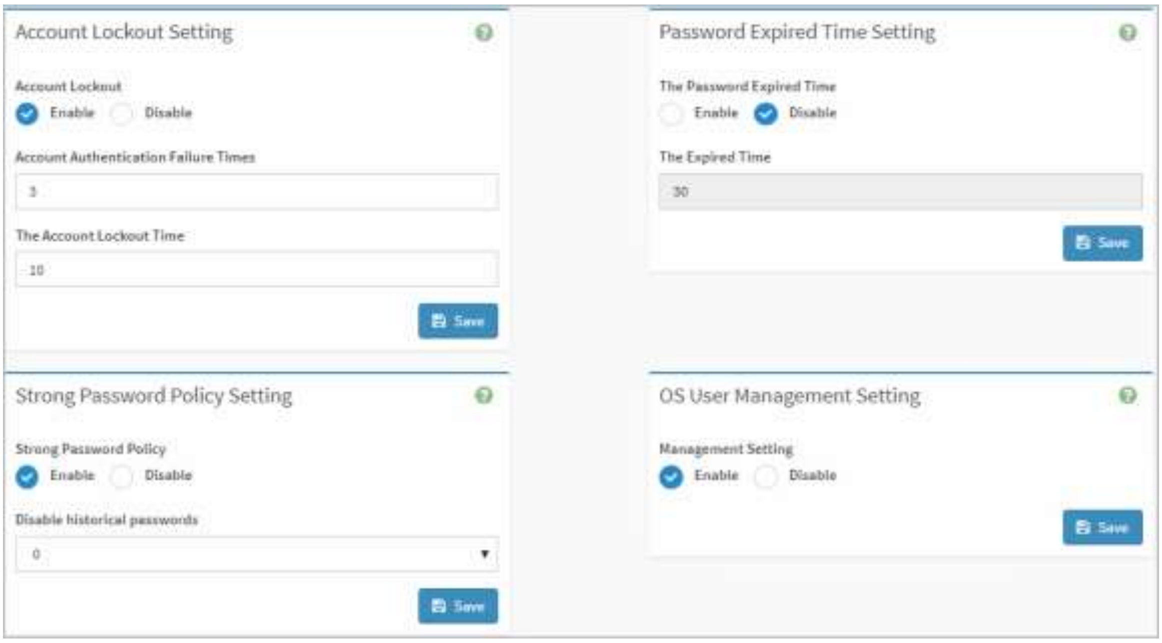
Abstract

To ensure user account security, you must configure the login parameters.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Login Settings**. The **Account Login Settings** page is displayed, see Figure 3-55.

Figure 3-55 Account Login Settings Page



Account Lockout Setting

Account Lockout

● Enable ○ Disable

Account Authentication Failure Times

3

The Account Lockout Time

10

Save

Password Expired Time Setting

The Password Expired Time

○ Enable ● Disable

The Expired Time

30

Save

Strong Password Policy Setting

Strong Password Policy

● Enable ○ Disable

Disable historical passwords

0

Save

OS User Management Setting

Management Setting

● Enable ○ Disable

Save

3. Configure the parameters. For a description of the parameters, refer to Table 3-30.

Table 3-30 Parameter Descriptions for the Account Login Settings

Parameter		Description	Setting
Account Lockout Setting	Account Lockout	Whether to lock a user account when the number of times that the user enters incorrect passwords reaches **Account Authentication Failure Times**.	Select whether to enable account lockout: ● Enable: locks the user account when the number of times that the user enters incorrect passwords reaches **Account Authentication Failure Times** . ● Enable: does not lock the user account when the number of times that the user enters incorrect passwords reaches **Account Authentication Failure Times**.

Parameter		Description	Setting
			When this parameter is set to **Enable**, you must configure **Account Authentication Failure Times** and **The Account Lockout Time**.
	Account Authentication Failure Times	Number of authentication failures caused by incorrect passwords.	Enter the number of account authentication failures. The range is 0–10.
	The Account Lockout Time	Length of time for which an account is locked. Unit: minutes.	Enter the length of time for which an account is locked. The range is 1–1440.
Password Expired Time Setting	The Password Expired Time	Whether to enable the password validity period.	After the password validity period is enabled, the account that expires fails to log in.
	The Expired Time	Validity period of the password in days.	Enter the validity period of the password, which ranges from 1 through 90.
Strong Password Policy Setting	Strong Password Policy	Whether to enable the strong password policy.	Select whether to enable the strong password policy. A strong password must contain at least eight characters, including uppercase and lowercase letters, digits, and symbols.
	Disable historical passwords	Number of historical passwords that cannot be used as the new password.	Range: 0–5. The values 1–5 indicate that the new password cannot be the same as the last 1 to 5 passwords. The value 0 indicates that the new password can be the same as any historical password.
OS User Management Setting	Management Setting	Whether to enable the user management configuration function on the service side. After the function is enabled, the BMC user information can be configured in the BIOS and OS.	Select whether to enable the user management configuration function on the service side.

4. Click **Save**.

3.7.29 Configuring Two-Factor Authentication

Abstract

Two-factor authentication requires another credential for access to the system in addition to a static password. It improves system security.

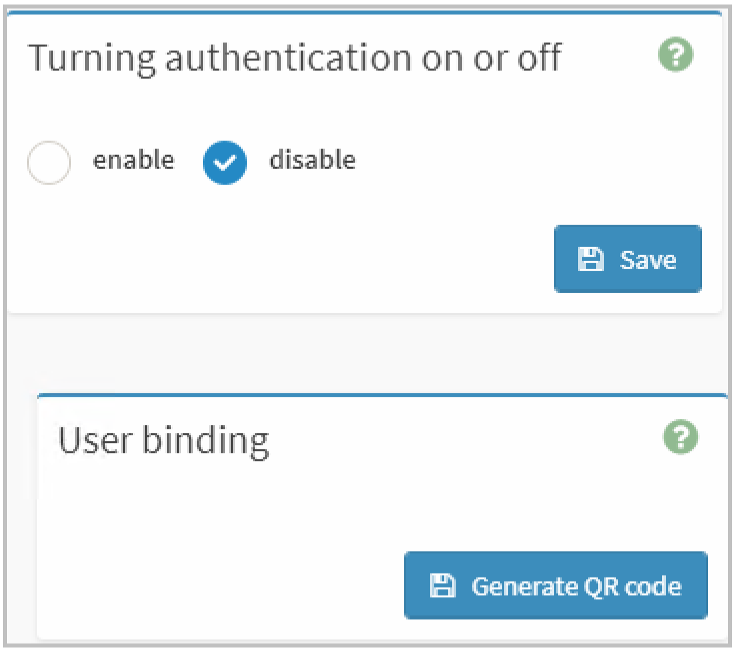
Note

This function is applicable to only server models developed based the Hygon platform.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Two-factor Authentication**. The **Two-factor Authentication** page is displayed, as shown in Figure 3-56.

Figure 3-56 Two-factor Authentication Page



Turning authentication on or off

○ enable ● disable

3. Select whether to enable two-factor authentication. Options:
   - **enable**: enables two-factor authentication.
   - **disable**: disables two-factor authentication.
4. Click **Save**.
5. (Optional) If two-factor authentication is enabled, click **Generate QR code**, and then scan the code and enter the correct token to bind your mobile number.

Note

The bound mobile number will be used as the other credential in addition to the static password. In addition, the BMC time must be the same as the Internet time. Otherwise, the verification fails.

3.7.30 Configuring SNMP Parameters

Abstract

SNMP parameters are used by the BMC to send alarms and notifications to a third-party NMS .

SNMP parameters include:

- SNMP Community: A community consists of SNMP and SNMP entities, and different communities are identified by community names. Community names can be used as the plain-text passwords between the management process and the agent process.
- SNMP Trap Configurations
- SNMP Trap Destinations: Destination address to which alarms and notifications are sent, including the IP address and port number.

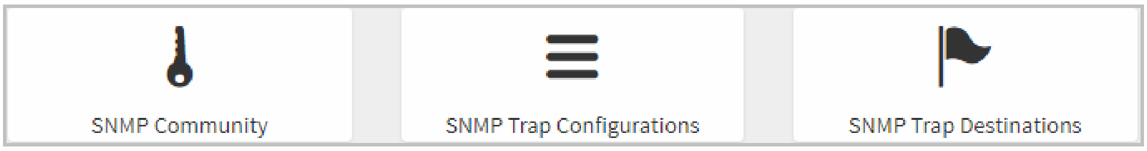
Note

SNMP parameters are provided by a third-party NMS.

Steps

1. From the menu bar in the left pane, select **Settings** . The **Settings** page is displayed.
2. Click **SNMP Settings** . The **SNMP Configurations** page is displayed, see Figure 3-57.

Figure 3-57 SNMP Configurations Page

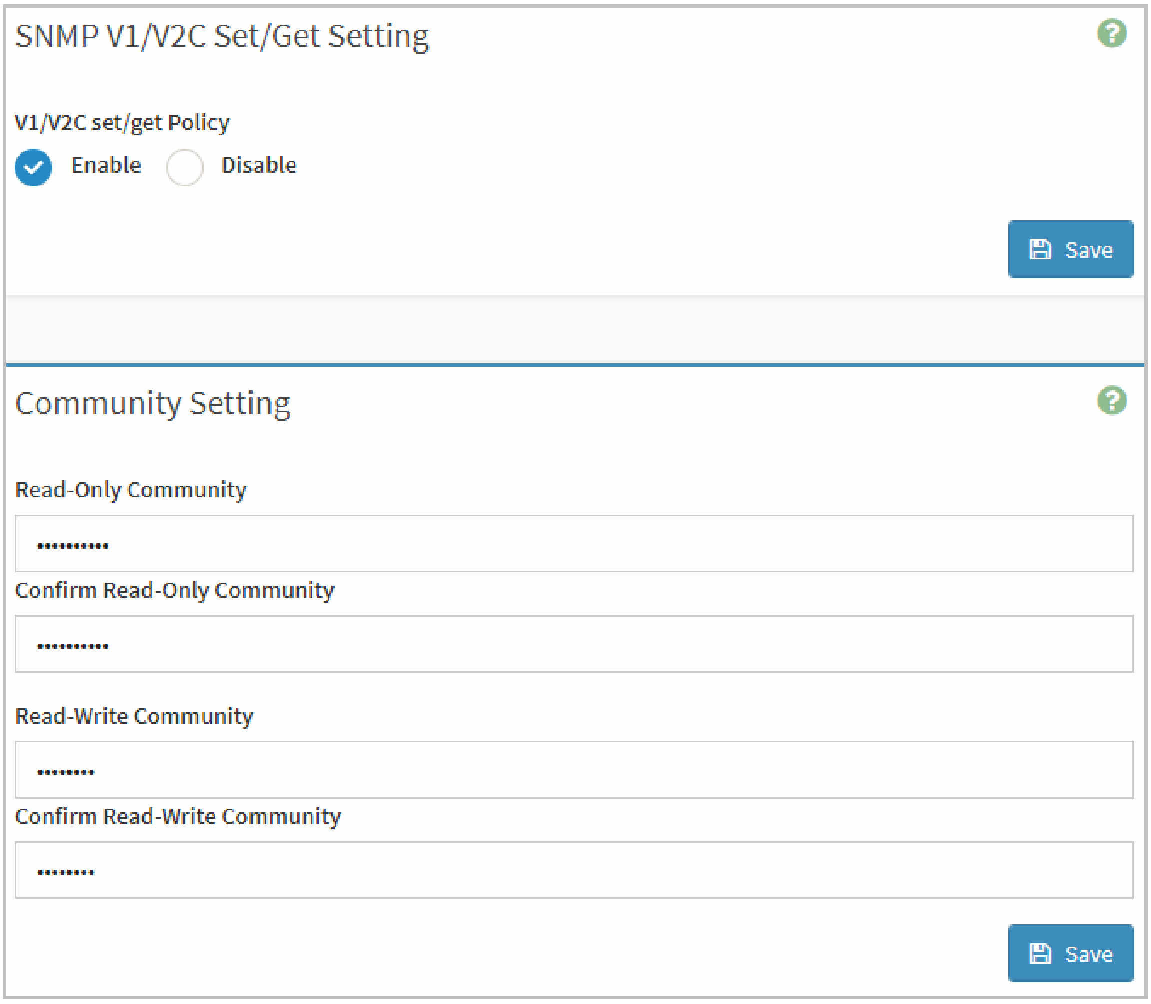


3. Perform the following operations as required.

To...	Do...
Configure the SNMP community	a. Click **SNMP Community** . The **SNMP Community** page is displayed, see Figure 3-58. b. Determine whether to enable the **V1/V2C set/get Policy** function. If the **V1/V2C set/get Policy** function is enabled, the Set and Get operations are allowed to be performed in accordance with SNMPv1 or SNMPv2c. c. Click **Save** in the **SNMP V1/V2C Set/Get Setting** area.

To...	Do...
	d. Set **Read-Only Community** , **Confirm Read-Only Community** , **Read-Write Community** , and **Confirm Read-Write Community** . In most cases, **Read-Only Community** is set to `vantageo_public` , and **Read-Write Community** is set to `platform` by default. e. Click **Save** in the **Community Setting** area.
Configure SNMP Trap	a. Click **SNMP Trap Configurations** . The **SNMP Trap Configurations** page is displayed, see Figure 3-59. b. Select **Enable** in the **SNMP Trap Setting** area. c. Select an alarm level from the **Alarm Sending Level** list. Alarm levels include: ● **Critical** : Alarms of critical level are sent only. ● **Major** : Alarms of major and critical levels are sent. ● **Minor** : Alarms of minor, major, and critical levels are sent. ● **Normal** : Alarms of normal, minor, major, and critical levels are sent. d. Select a mode from the **Module Trap Mode** list. Modes include: ● **Event OID Mode** : indicates that alarms are triggered by event. ● **Module OID Mode** : indicates that alarms are triggered by module. e. Click **Save** in the **SNMP Trap Setting** area. f. Enter a community name in the **Trap Community** text box and confirm it in the **Confirm Trap Community** text box in the **SNMP Trap Community Name Setting** area. g. Click **Save** in the **SNMP Trap Community Name Setting** area. h. Go back to the **SNMP Configurations** page. i. Click **SNMP Trap Destinations** . The **SNMP Trap Destinations** page is displayed. j. Click ⚑ . The **Trap Destination Configuration** page is displayed, see Figure 3-60. k. Configure the trap destination parameters. For a description of the parameters, refer to Table 3-31. l. Click **Save** .

Figure 3-58 SNMP Community Page



SNMP V1/V2C Set/Get Setting

V1/V2C set/get Policy

● Enable ○ Disable

Community Setting

Read-Only Community

••••••••••

Confirm Read-Only Community

••••••••••

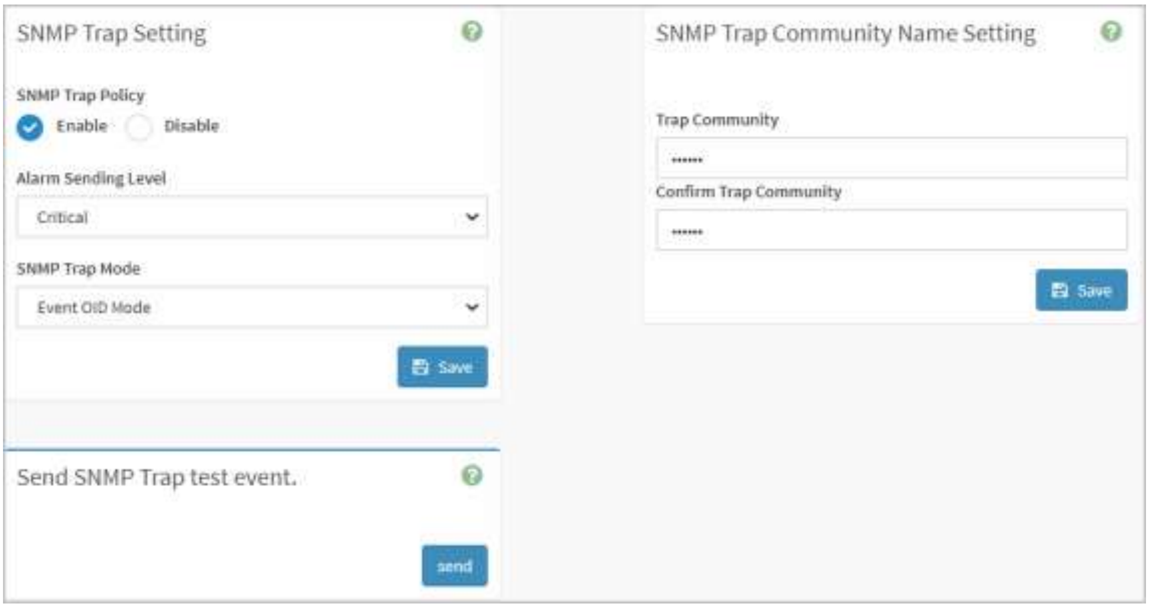
Read-Write Community

••••••••

Confirm Read-Write Community

••••••••

Figure 3-59 SNMP Trap Setting Page



SNMP Trap Setting

SNMP Trap Policy

● Enable ○ Disable

Alarm Sending Level

Critical

SNMP Trap Mode

Event OID Mode

SNMP Trap Community Name Setting

Trap Community

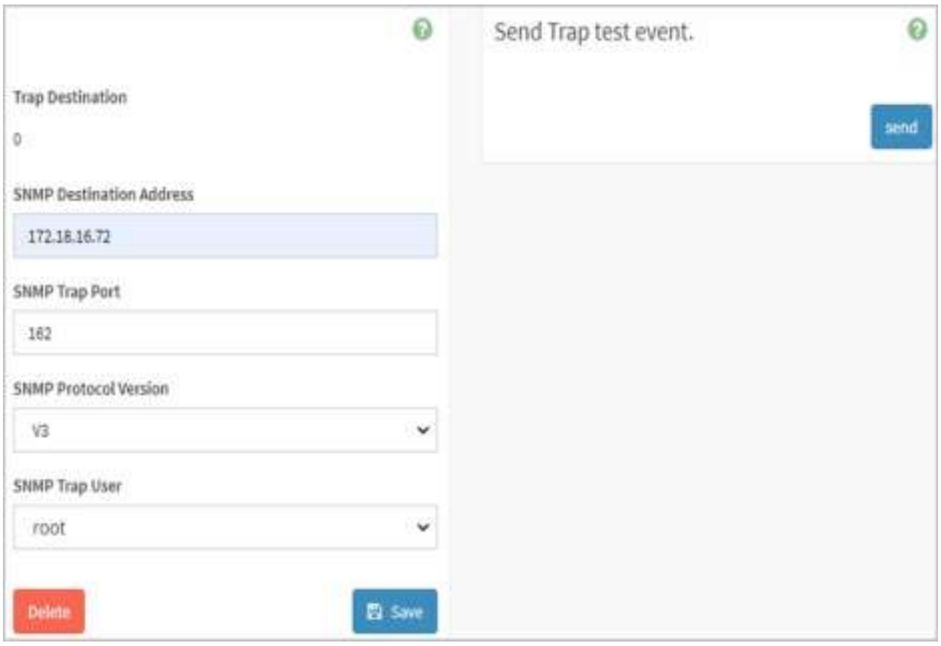
••••••

Confirm Trap Community

••••••

Send SNMP Trap test event.

Figure 3-60 Trap Destination Configuration Page



Trap Destination

0

SNMP Destination Address

172.18.16.72

SNMP Trap Port

162

SNMP Protocol Version

V3

SNMP Trap User

root

Send Trap test event.

Table 3-31 Trap Destination Parameter Descriptions

Parameter	Description	Setting
SNMP Destination Address	IP address of the server that receives alarms.	Enter the IP address in the IPv4 or IPv6 format.
SNMP Trap Port	Server port that receives alarms.	Enter the port number, with a range of 1–65535. If there is a default port number, provide it.
SNMP Protocol Version	SNMP protocol type used for sending alarms.	Select a protocol type.
SNMP Trap User	User used for sending alarms.	When **SNMP Protocol Version** is set to **V3** , you must select a user with the SNMP permissions as the alarm sender. For how to create a user with the SNMP permissions, refer to "4.20 Creating an SNMP User".

3.7.31 Configuring an Asset Tag

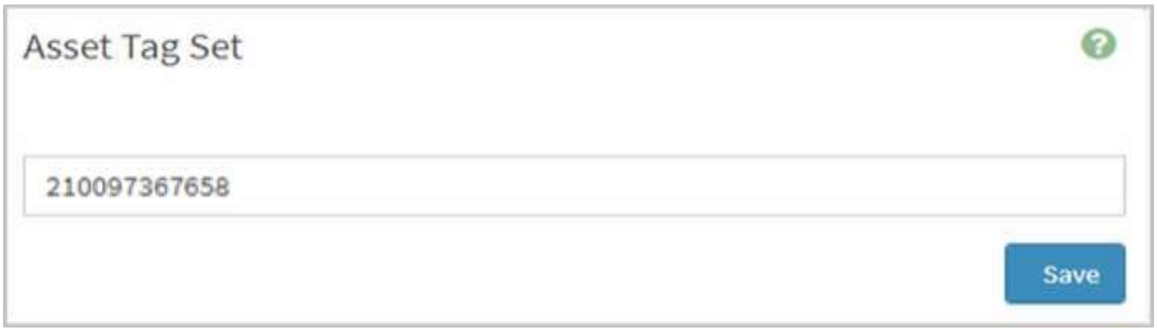
Abstract

This procedure describes how to modify the server asset tag when it needs to be updated.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Asset Tag Settings**. The **Asset Tag** page is displayed, see Figure 3-61.

Figure 3-61 Asset Tag Page



Asset Tag Set

210097367658

3. Enter the asset tag name with a maximum of 63 characters.
4. Click **Save**.

3.7.32 Configuring the Server Location

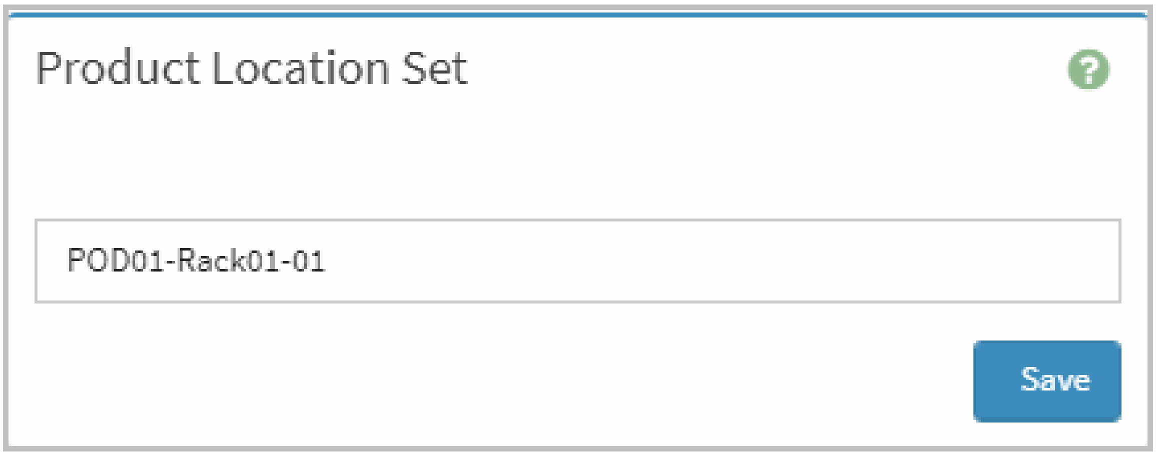
Abstract

This procedure describes how to configure the server location.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Product Location**. The **Product Location** page is displayed, as shown in Figure 3-62
   .

Figure 3-62 Product Location Page



Product Location Set

POD01-Rack01-01

3. Enter the server location. Range: 0–64 characters, which include digits, letters, and special characters.
4. Click **Save**.

3.7.33 Configuring Disk Alarm Thresholds

Abstract

This procedure describes how to configuring disk alarm thresholds by using the **Monitor info** function. Once the hard disk usage reaches a threshold, an alarm of the corresponding level is raised.

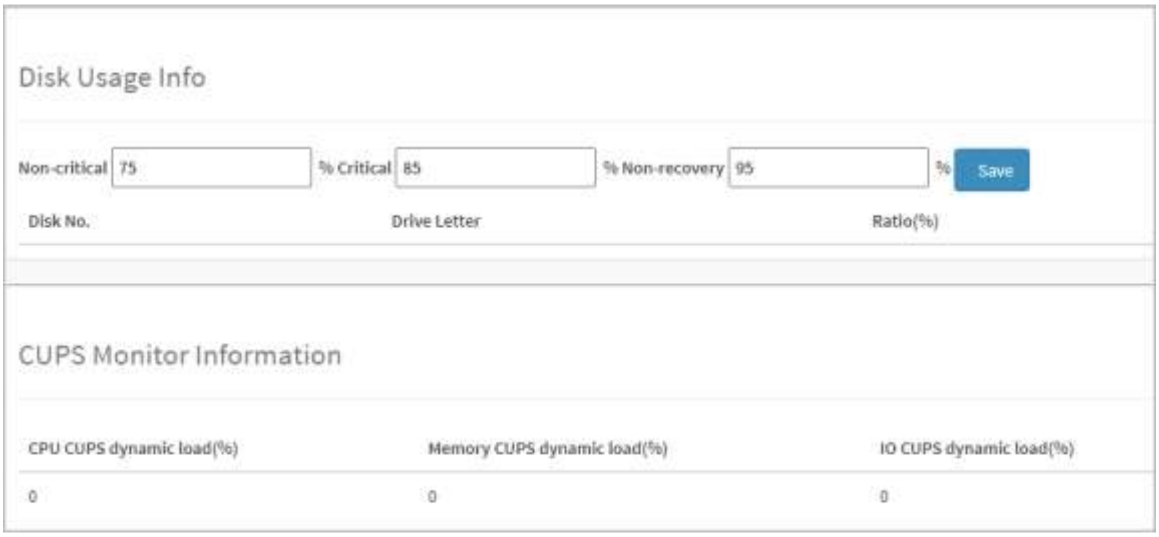
Note

The **Monitor Info** function is only provided for specific operating systems and monitoring tools.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Monitor info**. The **Monitor Information** page is displayed, see Figure 3-63.

Figure 3-63 Monitor Information Page



Disk Usage Info

Non-critical 75 % Critical 85 % Non-recovery 95 %

Disk No.	Drive Letter	Ratio(%)

CUPS Monitor Information

CPU CUPS dynamic load(%)	Memory CUPS dynamic load(%)	IO CUPS dynamic load(%)
0	0	0

3. Enter the three thresholds for hard disk monitoring.

   Generally, the three thresholds are 75%, 85%, and 95% from low to high.
4. Click **Save**.

Related Tasks

On the **Monitor Information** page, you can view the usage of each disk and the monitoring information of the CPU, memory and I/O.

- **CPU CUPS dynamic load(%)**: proportion of the used CPU resources to the server resources.
- **Memory CUPS dynamic load(%)**: proportion of the used memory resources to the server resources.

- **IO CUPS dynamic load(%)**: proportion of the used I/O resources to the server resources.

3.7.34 Configuring an Alarm Source

Abstract

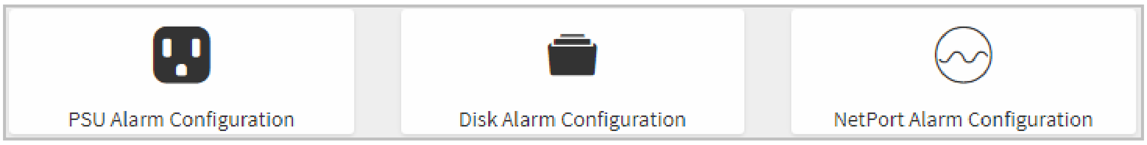
This procedure describes how to configure alarm sources by using the **Alarm Settings** function, including the PSU alarm, disk alarm and network port alarm.

- PSU alarm: When a power module is not present, an alarm is raised.
- Disk alarm: When a hard disk is not present, an alarm is raised.
- Net port alarm: When the network cable corresponding to the network port is removed or not properly connected, an alarm is raised.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Alarm Settings**. The **Alarm Configuration** page is displayed, see Figure 3-64.

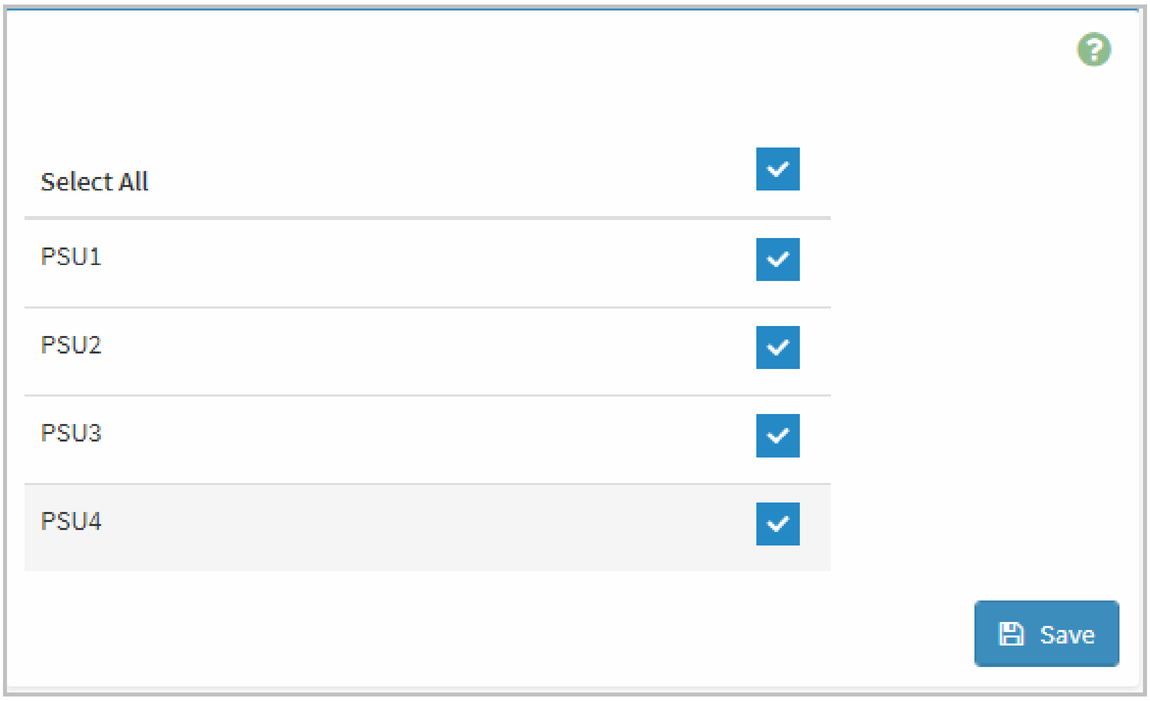
Figure 3-64 Alarm Configuration Page



3. Perform the following operations as required.

To...	Do...
Configure the PSU alarm	a. Click **PSU Alarm Configuration**. The **PSU Alarm Configuration** page is displayed, see Figure 3-65. b. Select the power supply whose alarms need to be reported. c. Click **Save**.
Configure the disk alarm	a. Click **Disk Alarm Configuration**. The **DISK Alarm Configuration** page is displayed, see Figure 3-66. b. Select the hard disk whose alarms need to be reported. c. Click **Save**.
Configure the network port alarm	a. Click **NetPort Alarm Configuration**. The **NetPort Alarm Configuration** page is displayed, see Figure 3-67. b. Select whether to enable the network port alarm. ● Select **NetPort** to enable the network port alarm. ● Deselect **NetPort** to disable the network port alarm. c. Click **Save**.

Figure 3-65 PSU Alarm Configuration Page



Select All ☑

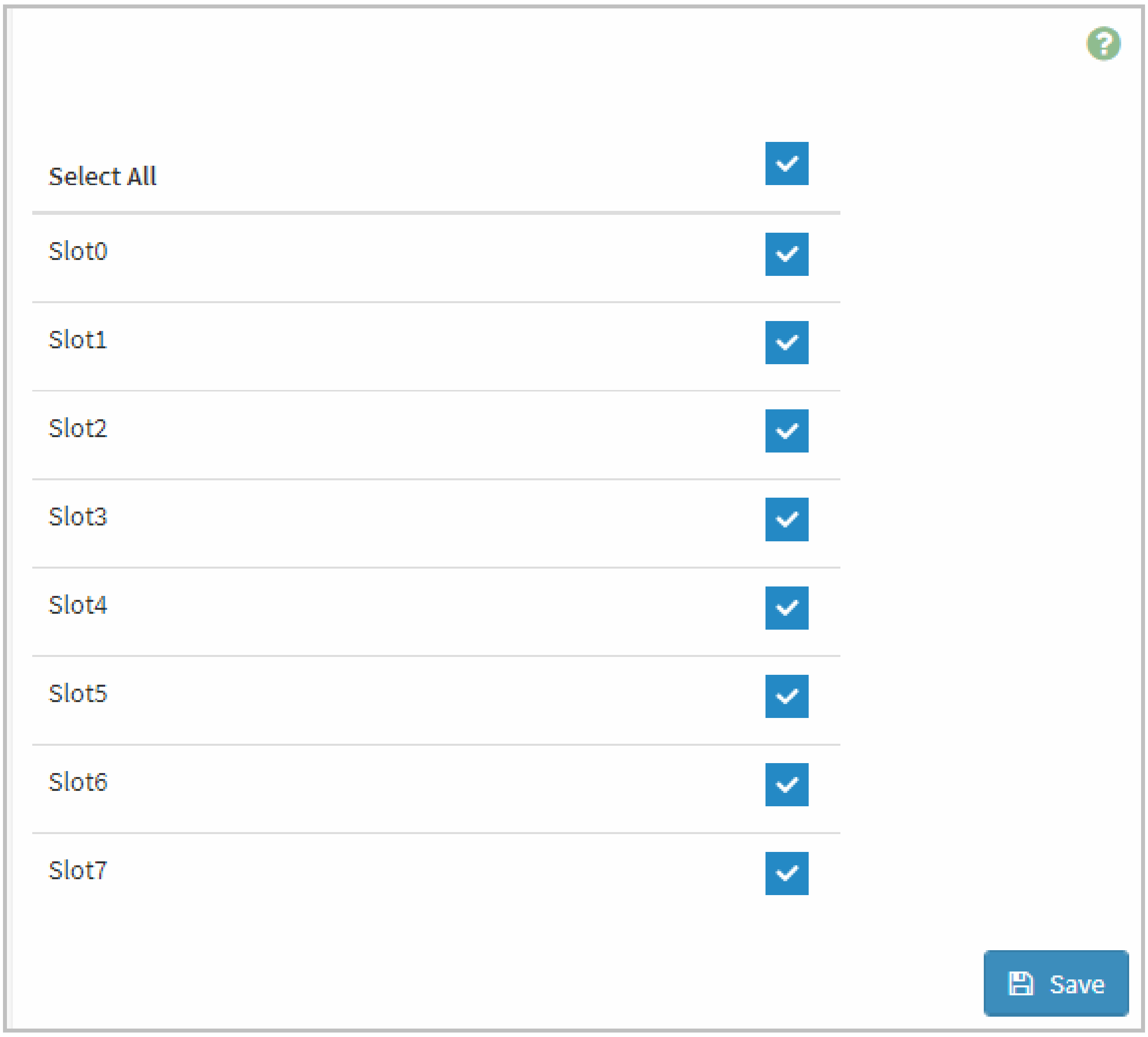
PSU1 ☑

PSU2 ☑

PSU3 ☑

PSU4 ☑

Figure 3-66 Disk Alarm Configuration Page



Select All ☑

Slot0 ☑

Slot1 ☑

Slot2 ☑

Slot3 ☑

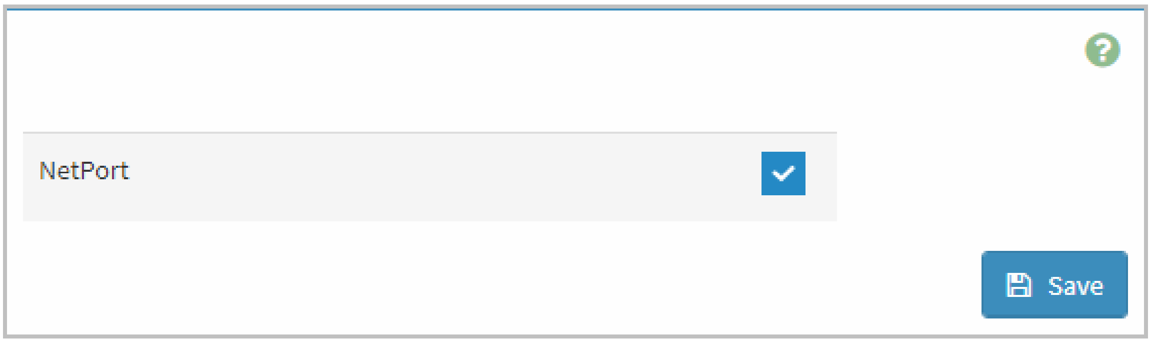
Slot4 ☑

Slot5 ☑

Slot6 ☑

Slot7 ☑

Figure 3-67 NetPort Alarm Configuration Page



NetPort ☑

3.7.35 Configuring a Serial Port Output Mode

Abstract

The serial port output modes on the panel include:

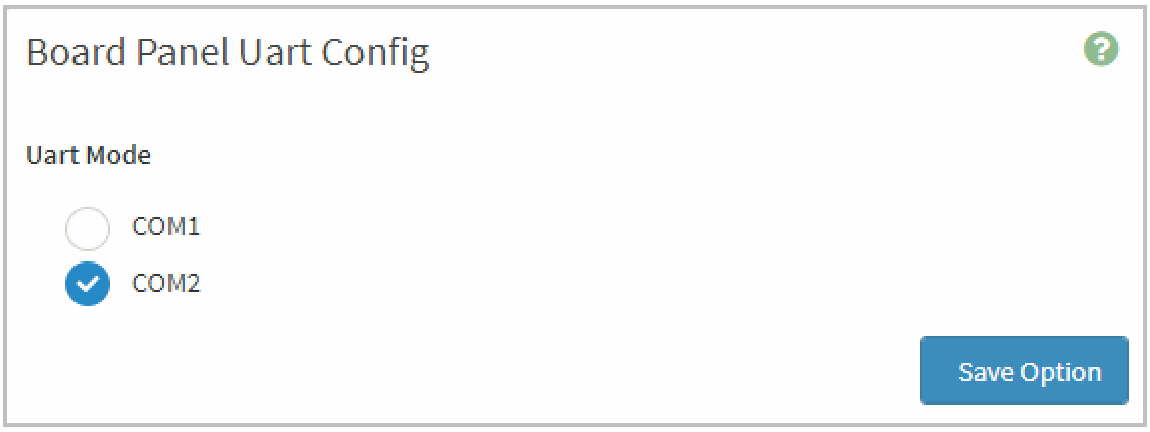
- COM1: The print information in the BIOS phase is output. The BIOS can be configured.

- COM2: There is no output in the BIOS phase and the system hot key cannot be responded. The print information in the OS phase is output.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Panel Uart Settings**. The **Panel Uart** page is displayed, see Figure 3-68.

Figure 3-68 Panel Uart Page



Board Panel Uart Config

Uart Mode

○ COM1

● COM2

3. Select a serial port output mode.
4. Click **Save Option**.

3.7.36 Configuring the Cooling Mode

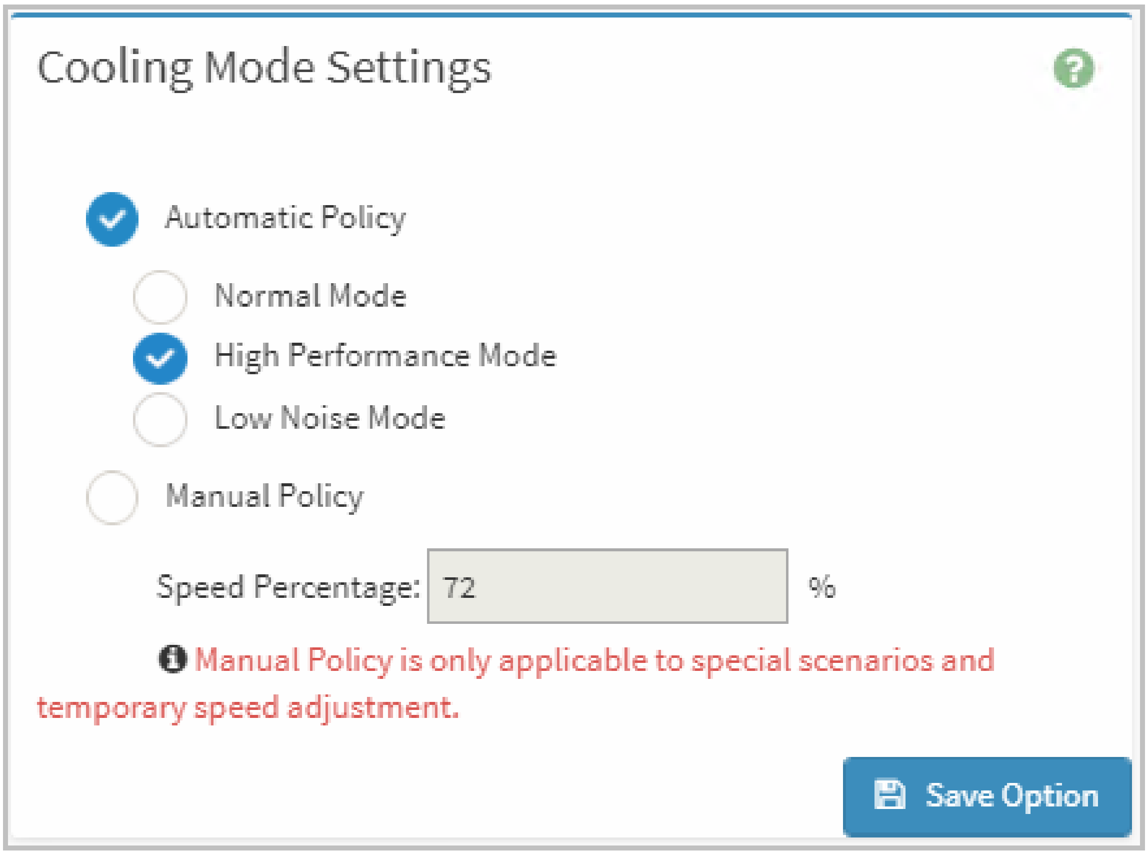
Abstract

This procedure describes how to set the cooling mode in accordance with the storage scenario of the server to improve the server performance.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Cooling Mode Management**. The **Cooling Mode Management** page is displayed, see Figure 3-69.

Figure 3-69 Cooling Mode Management Page



Cooling Mode Settings

● Automatic Policy

○ Normal Mode

● High Performance Mode

○ Low Noise Mode

○ Manual Policy

Speed Percentage: 72 %

Manual Policy is only applicable to special scenarios and temporary speed adjustment.

3. Select a cooling mode as required.

If...	Then...
There is space above the top surface of the server, and the server is insensitive to noise	Select **Normal Mode** under **Automatic Policy**.
Servers are stacked together, and there is no space between them	Select **High Performance Mode** under **Automatic Policy**.
The server is placed in an office or other areas that are sensitive to noise	Select **Low Noise Mode** under **Automatic Policy**, and leave some space above the top surface of the server.
The fan rotation speed needs to be set manually for the server	Select **Manual Policy** and enter **Speed Percentage**.

Note

Speed Percentage indicates the ratio of the current speed of the fan to its maximum speed.

Note

Manual Policy is applicable to only special scenarios and temporary adjustment. Use this function with care.

4. Click **Save Option**.

3.7.37 Querying GPU Information

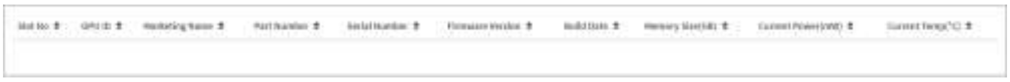
Abstract

By querying the GPU information, you can learn about the basic information of the GPU on the server, including the model and version number.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **GPU Information**. The **GPU Management** page is displayed, see Figure 3-70.

Figure 3-70 GPU Management Page



Slot No ⇕	GPU ID ⇕	Marketing Name ⇕	Part Number ⇕	Serial Number ⇕	Firmware Version ⇕	Build Date ⇕	Memory Size(GB) ⇕	Current Power(W) ⇕	Current Temp(°C) ⇕

3.7.38 Configuring a Power-On Policy

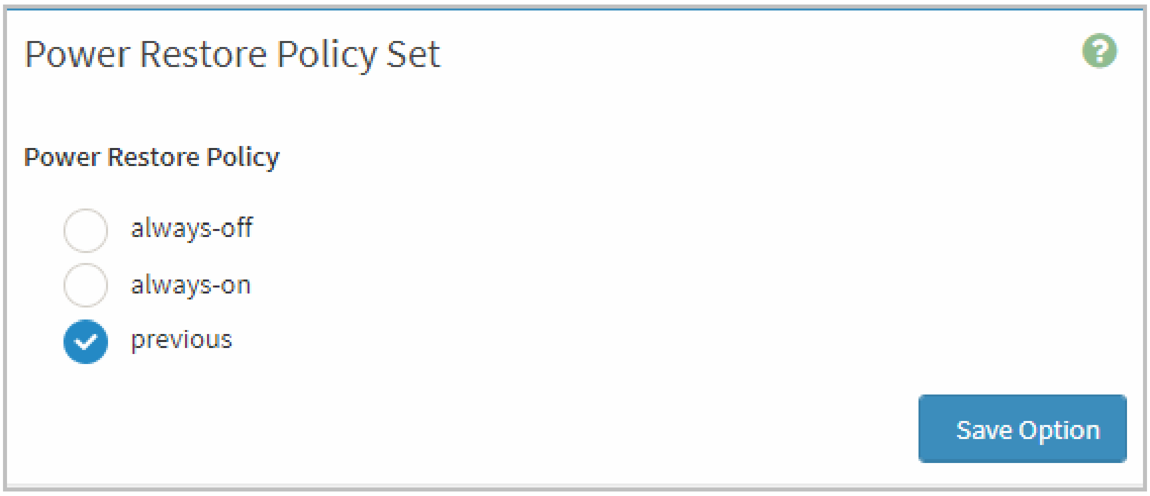
Abstract

By using the power-on restoration policy function, you can configure the power-on/power-off status of the host when the system is to restore its power after it is powered off.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Power Restore Policy**. The **Power Restore Policy** page is displayed, see Figure 3-71.

Figure 3-71 Power Restore Policy Page



Power Restore Policy Set

Power Restore Policy

○ always-off

○ always-on

☑ previous

3. Select a power-on policy.
   - always-off: When the system is powered off and then restores power, the host is in the power-off status.
   - always-on: When the system is powered off and then restores power, the host is in the power-on status.
   - previous: When the system is powered off and then restores power, the host is in the status the same as that before the power-off.
4. Click **Save Option**.

3.7.39 Configuring the VGA Output Mode

Abstract

VGA output modes include:

- Front: Signals are output from the front VGA interface.
- Rear: Signals are output from the rear VGA interface. The rear VGA interface is selected by default.

The front VGA interface cannot display the 80-code startup process. If debugging is required, you must connect the display to the rear VGA interface.

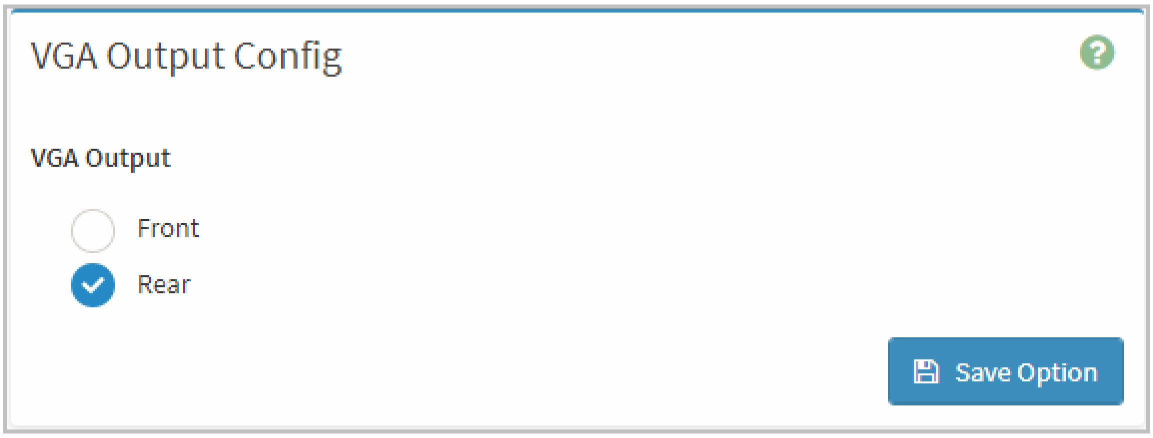
Note

The VGA output mode needs to be configured for only server models developed based the Hygon platform.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **VGA Output**. The **VGA Output Config** page is displayed, see Figure 3-72.

Figure 3-72 VGS Output Config Page



VGA Output Config

VGA Output

○ Front

● Rear

3. Select a VGA output mode.
4. Click **Save Option**.

3.7.40 Configuring Power-On Delay Parameters

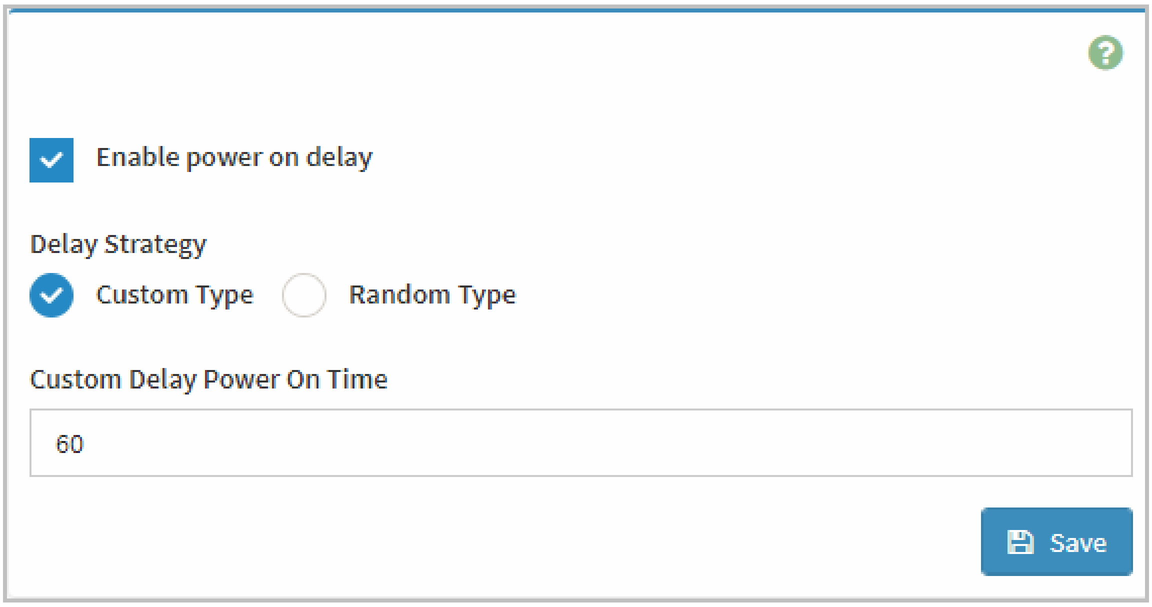
Abstract

This procedure describes how to configure power-on delay parameters for off-peak power-on.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Power On delay Settings**. The **Power On delay Settings** page is displayed, see Figure 3-73.

Figure 3-73 Power On Delay Settings Page



☑ Enable power on delay

Delay Strategy

● Custom Type ○ Random Type

Custom Delay Power On Time

60

3. Configure the parameters. For a description of the parameters, refer to Table 3-32.

Table 3-32 Parameter Descriptions for the Power-On Delay

Parameter	Description	Setting
Enable power on delay	Whether to enable the power-on delay function.	- Select **Enable power on delay**. The power-on delay function is enabled. - Deselect **Enable power on delay**. The power-on delay function is disabled.
Delay Strategy	Power-on delay mode.	Select the corresponding power-on delay mode: - **Custom Type**: The power-on delay time is user-defined. If **Custom Type** is selected, **Custom Delay Power On Time** is also required. **Custom Delay Power On Time** ranges from 1 through 120 seconds. - **Random Type**: The power-on delay time is generated by the system automatically.

4. Click **Save**.

3.7.41 Querying Pass-Through Disk Information

Abstract

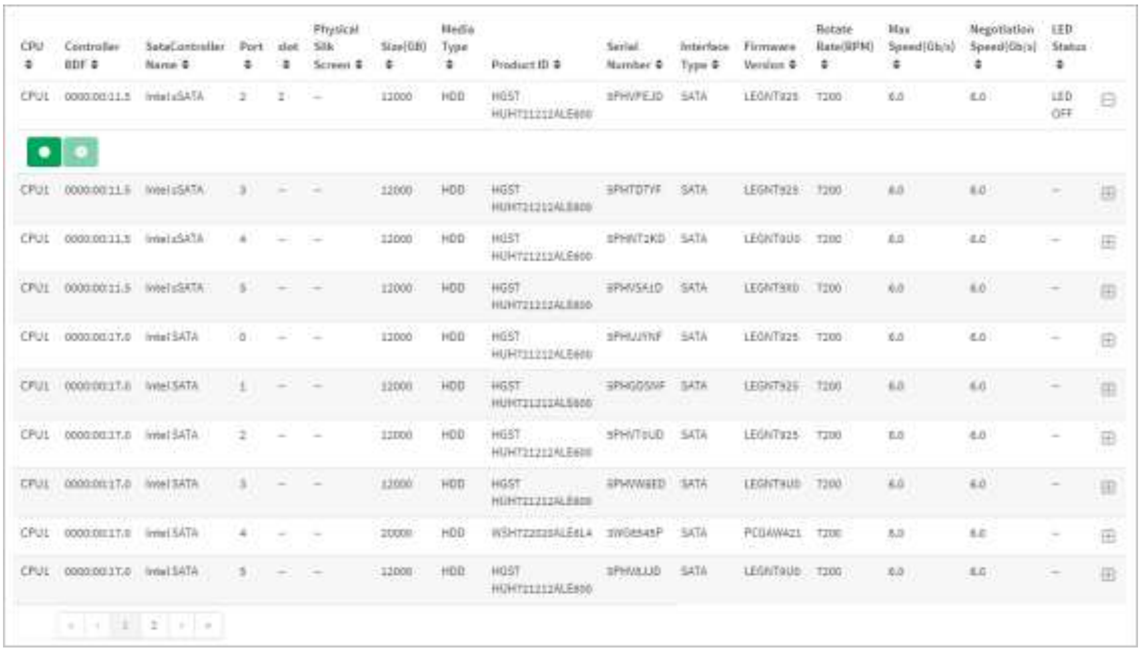
Pass-through disks are hard disks directly connected to the PCH or a CPU rather than a RAID controller card.

By querying the information about a pass-through disk, you can learn about the corresponding CPU, capacity, and model of the pass-through disk, and turn on the UID indicator of the pass-through disk.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Direct Harddisk Management**. The **Direct Harddisk Management** page is displayed, see Figure 3-74.

Figure 3-74 Direct Harddisk Management Page



CPU ⇕	Controller BDF ⇕	SataController Name ⇕	Port ⇕	slot ⇕	Physical Silk Screen ⇕	Size(GB) ⇕	Media Type ⇕	Product ID ⇕	Serial Number ⇕	Interface Type ⇕	Firmware Version ⇕	Rotate Rate(RPM) ⇕	Max Speed(Gb/s) ⇕	Negotiation Speed(Gb/s) ⇕	LED Status ⇕	
CPU1	0000:00:11.5	Intel sSATA	2	2	–	12000	HDD	HGST HUH721212ALE600	8PHVPEJD	SATA	LEGNT925	7200	6.0	6.0	LED OFF	⊟
● ●																
CPU1	0000:00:11.5	Intel sSATA	3	–	–	12000	HDD	HGST HUH721212ALE600	8PHTDTYF	SATA	LEGNT925	7200	6.0	6.0	–	⊞
CPU1	0000:00:11.5	Intel sSATA	4	–	–	12000	HDD	HGST HUH721212ALE600	8PHNT2KD	SATA	LEGNT9U0	7200	6.0	6.0	–	⊞
CPU1	0000:00:11.5	Intel sSATA	5	–	–	12000	HDD	HGST HUH721212ALE600	8PHVSA1D	SATA	LEGNT9X0	7200	6.0	6.0	–	⊞
CPU1	0000:00:17.0	Intel SATA	0	–	–	12000	HDD	HGST HUH721212ALE600	8PHUJYNF	SATA	LEGNT925	7200	6.0	6.0	–	⊞
CPU1	0000:00:17.0	Intel SATA	1	–	–	12000	HDD	HGST HUH721212ALE600	8PHGDSNF	SATA	LEGNT925	7200	6.0	6.0	–	⊞
CPU1	0000:00:17.0	Intel SATA	2	–	–	12000	HDD	HGST HUH721212ALE600	8PHVT0UD	SATA	LEGNT925	7200	6.0	6.0	–	⊞
CPU1	0000:00:17.0	Intel SATA	3	–	–	12000	HDD	HGST HUH721212ALE600	8PHWW8ED	SATA	LEGNT9U0	7200	6.0	6.0	–	⊞
CPU1	0000:00:17.0	Intel SATA	4	–	–	20000	HDD	WSH722020ALE6L4	3WG8545P	SATA	PCGAW421	7200	6.0	6.0	–	⊞
CPU1	0000:00:17.0	Intel SATA	5	–	–	12000	HDD	HGST HUH721212ALE600	8PHW8JJD	SATA	LEGNT9U0	7200	6.0	6.0	–	⊞

Note

Controller BDF is the controller of the PCH or CPU.

3. (Optional) To turn on the UID indicator, click ● for the corresponding hard disk.

Note

After the indicator is turned on, its status in the **LED Status** column is changed to **LED ON**, and the ⊗ button is activated. You can click ⊗ to turn off the UID indicator.

3.8 Remotely Controlling a Server

Abstract

If the server cannot be controlled on-site, you can control it remotely on the client PC.

Prerequisite

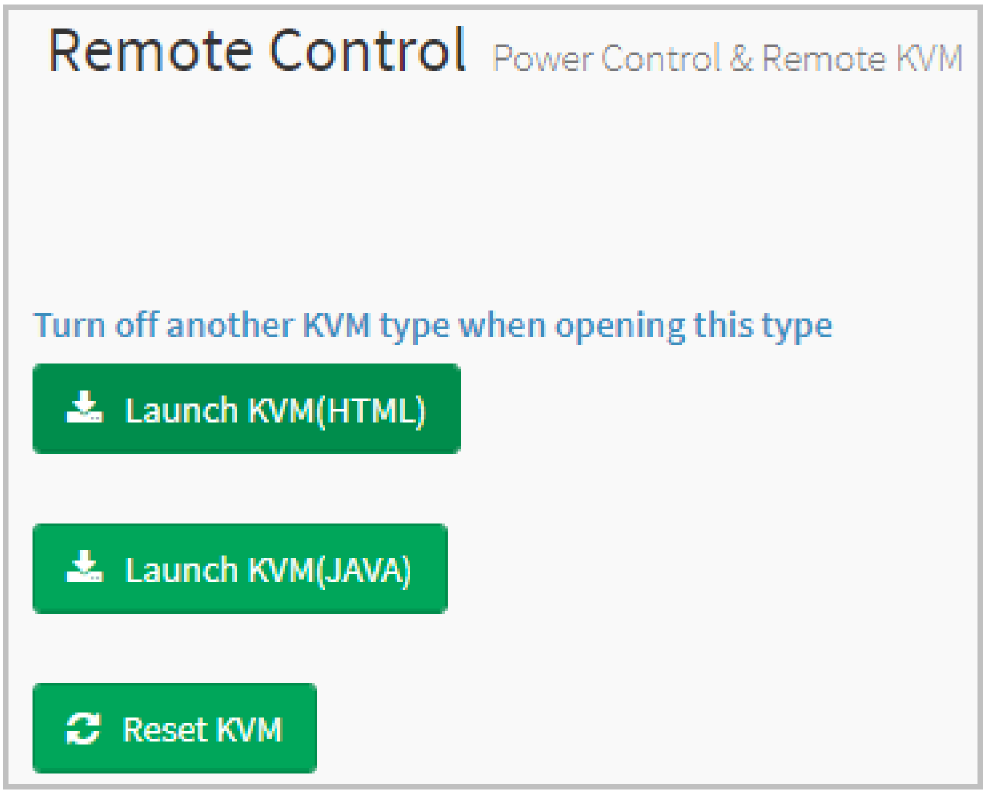
To start the KVM in JAVA mode, the JRE is installed on the client PC, for example, `jre-8u191`

.

Steps

1. From the menu bar in the left pane, select **Remote Control**. The **Remote Control** page is displayed, see Figure 3-75.

Figure 3-75 Remote Control Page


Remote Control Power Control & Remote KVM

Turn off another KVM type when opening this type

2. Perform the following operations as required.

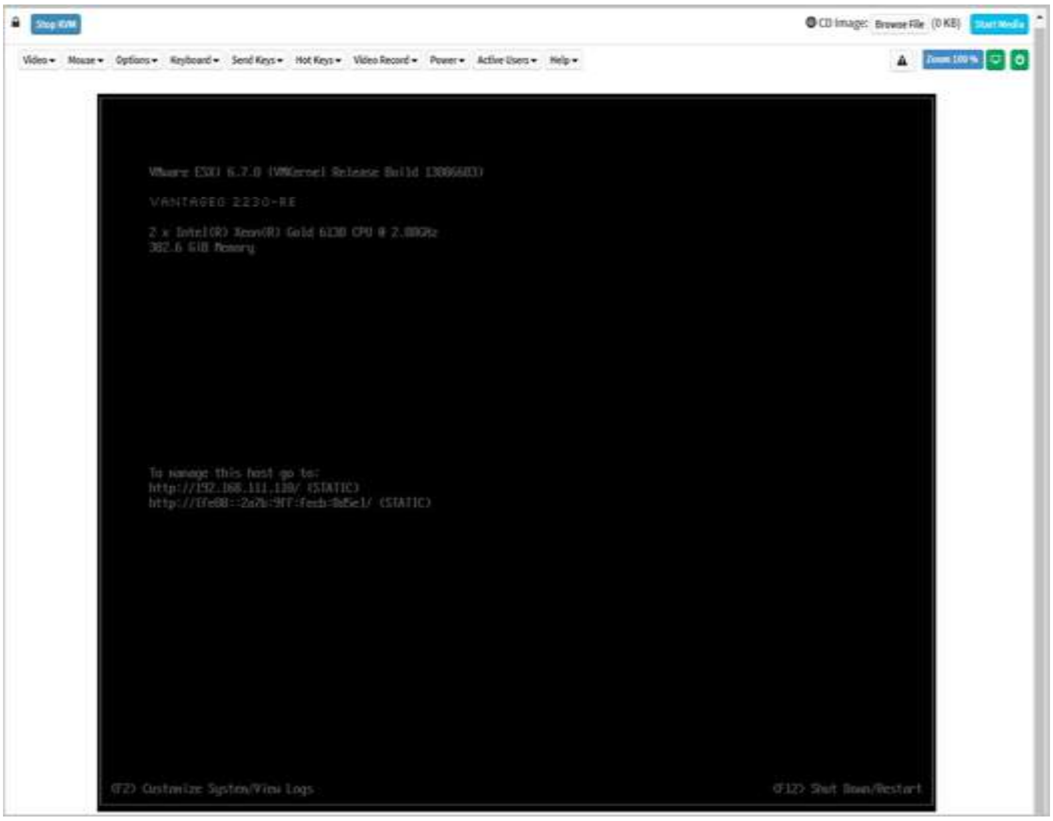
To...	Do...
Start the KVM in HTML mode	a. Click **Launch KVM (HTML)**. The **Remote KVM (HTML)** window is displayed, see Figure 3-76. b. Perform the operations as required. For a description of the operations, refer to Table 3-33.
Start the KVM in JAVA mode	a. In the search box in the lower left corner of the client PC, enter `Java`. b. In the search result, select **Java**. The **Java Control Panel** dialog box is displayed. c. Click **Security**. The **Security** window is displayed. d. Click **Edit Site List**. The **Exception Site List** dialog box is displayed. e. Click **Add** to add the address of the BMC Web portal. f. Click **OK** to return to the **Security** window. g. Click **OK**. h. On the **Remote Control** page of the BMC Web portal, click **Launch KVM (JAVA)**. A dialog box indicating whether to keep `jviewer.jnlp` is displayed. i. Click **Keep**. j. In the lower left corner of the browser, click `jviewer.jnlp`. A dialog box is displayed. k. Click **Continue**. The **Do you want to run this application?** dialog box is displayed.

To...	Do...
	l. Select **I accept the risk and want to run this app.** and click **Run**. The **Untrusted Connection** dialog box is displayed. m. Click **Yes**. The **Remote KVM (JAVA)** page is displayed, see Figure 3-77. n. Perform the operations as required. For a description of the operations, refer to Table 3-34.
Reset KVM	When the KVM is not smooth, click **Reset KVM** to reset the KVM. After resetting the KVM, you must wait for several seconds before starting the KVM.

Note

Before starting the KVM in one mode, you must disable the KVM in another mode. For example, before starting the KVM in JAVA mode, you must disable the KVM started in HTML mode.

Figure 3-76 Remote KVM (HTML) Window



```
VMware ESXi 6.7.0 (VMKernel Release Build 13006603)

VANTAGEO 2230-RE

2 x Intel(R) Xeon(R) Gold 6130 CPU @ 2.00GHz
382.6 GiB Memory


To manage this host go to:
http://192.168.111.130/ (STATIC)
http://[fe80::2a7b:9ff:fecb:8e5e1]/ (STATIC)

<F2> Customize System/View Logs                    <F12> Shut Down/Restart
```

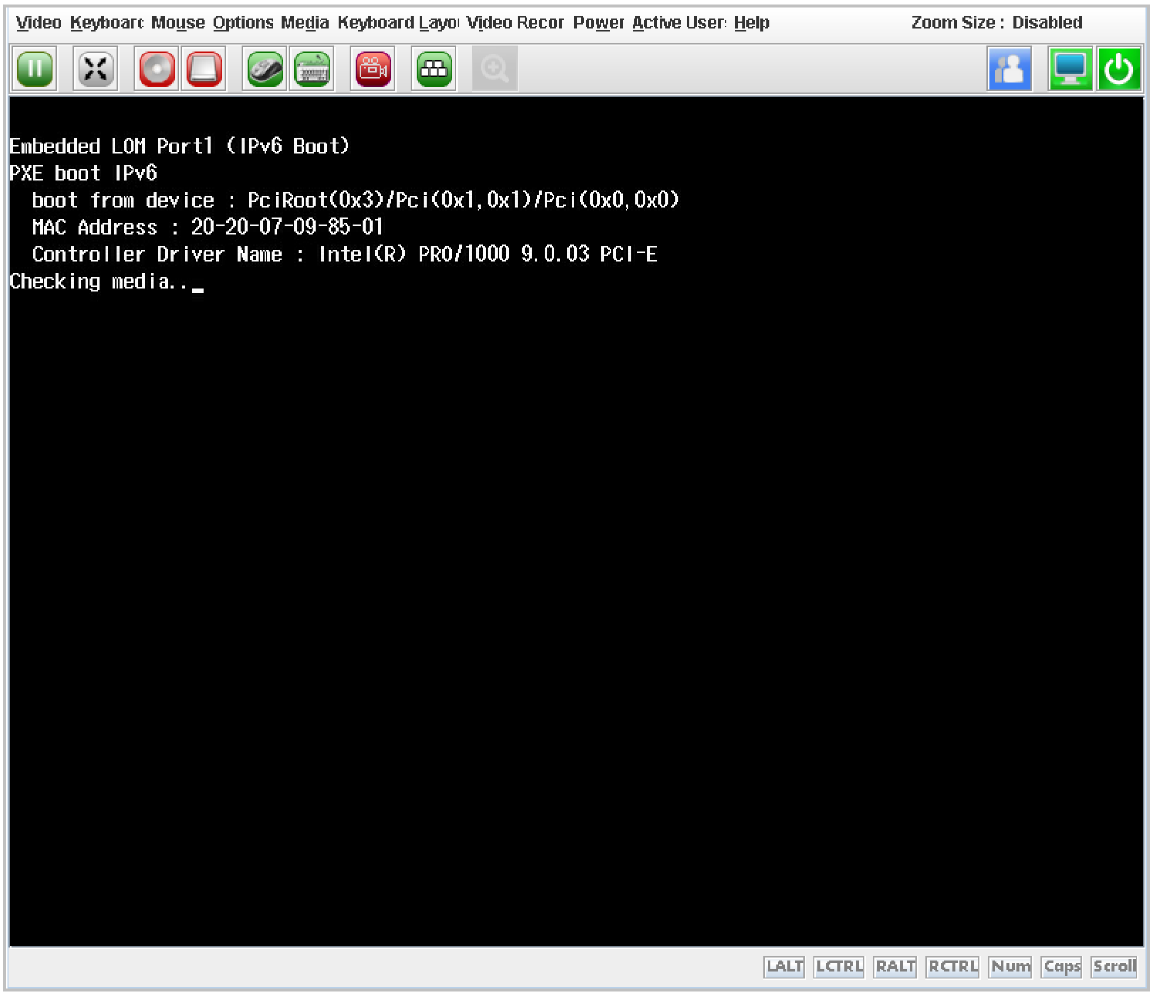
Table 3-33 Descriptions for the Remote KVM (HTML) Operations

Operation	Description
Stop KVM	Click **Stop KVM**. The **Remote KVM (HTML)** window is closed.
Mount a local ISO file	a. Click **Browse File** on the right of **CD Image**, and select the `ISO` file from the client PC.

Operation	Description
	b. Click **Start Media**.
Display the notifications received	Click ⚠ .
Lock the host display	Lock the host display through either of the following ways: - Click 🟩. - Select **Video > Display OFF**. After the host display is locked, if another user wants to view the host page, a permission request is sent. The user can view the host page only when being authorized by the current active user.
Unlock the host display	Unlock the host display through either of the following ways: - Click 🟥. - Select **Video > Display ON**. The 🟩 button is changed to 🟥.
Pause a remote control screen	Select **Video > Pause Video**.
Resume a remote control screen	Select **Video > Resume Video**.
Refresh a remote control screen	Select **Video > Refresh Video**.
Capture the current screen	Select **Video > Capture Screen**.
Set a video decoding mode	a. Select **Video > Compression Mode**. b. Select a video decoding mode from the displayed submenu.
Switch the mouse show mode on the client	- Show the cursor: Select **Mouse** and **Show Client Cursor**. - Hide the cursor: Select **Mouse** and deselect **Show Client Cursor**.
Set a mouse mode	- Set the absolute mouse mode: Select **Mouse** and then select **Absolute Mouse Mode**. In absolute mouse mode, the absolute position of the local mouse is transferred to the server to make the mouse on the server move. - Set the relative mouse mode: Select **Mouse** and then select **Relative Mouse Mode**. In relative mouse mode, the displacement of the local mouse relative to the server mouse is calculated and transferred to the server to make the mouse on the server move. - Set other mouse mode: Select **Mouse** and then select **Other Mouse Mode**.

Operation	Description
	In other mouse mode, the displacement of the local mouse relative to the center location is calculated and transferred to the server to make the mouse on the server move.
Set keyboard layout	a. Select **Keyboard**. b. In the displayed submenu, select the keyboard layout, including **English U.S**, **German** and **Japanese**. **English U.S** is selected by default.
Set a key sending mode	a. Select **Send Keys**. b. Select a key sending mode from the displayed submenu.
Set shortcut keys	a. Select **Hot Keys**. b. Select **Add Hot Keys** from the displayed submenu. c. In the displayed dialog box, add or clear shortcut keys.
Set video recording time length	a. Select **Video Record > Record Settings**. The **Record Settings** dialog box is displayed. b. Set the video recording time length with a range of 1–1800 seconds. c. Click **OK**.
Record a video	Select **Video Record > Record Video**.
Stop recording	Select **Video Record > Stop Recording**.
Shut down the server	Shut down the server through either of the following ways: ● Select **Power > Immediate shutdown**. ● Click ⏻.
Power on the server	Start the server through either of the following ways. ● Select **Power > Power On Server**. ● Click ⏻.
Perform a cold reboot	Select **Power > Power Cycle Server**. Cold reboot means that the server is started after it is shut down. During the restart, the server is offline.
Perform a warm reboot	Select **Power > Reset Power**. Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline.
Shut down the operating system of the server	Select **Power > Orderly shutdown**.
View the users using remote control	Select **Active Users**.

Figure 3-77 Remote KVM (JAVA) Window



```
Embedded LOM Port1 (IPv6 Boot)
PXE boot IPv6
  boot from device : PciRoot(0x3)/Pci(0x1,0x1)/Pci(0x0,0x0)
  MAC Address : 20-20-07-09-85-01
  Controller Driver Name : Intel(R) PRO/1000 9.0.03 PCI-E
Checking media.._
```

Table 3-34 Descriptions for the Remote KVM (JAVA) Operations

Operation	Description
Pause a remote control screen	Pause a remote control screen through one of the following ways: ● Select **Video > Pause Redirection**. ● Click ⏸. ● Press **Alt+P**.
Resume a remote control screen	Resume the remote control screen through one of the following ways: ● Select **Video > Resume Redirection**. ● Click ▶. ● Press **Alt+R**.
Refresh a remote control screen	Refresh the remote control screen through either of the following ways: ● Select **Video > Refresh Video**. ● Press **Alt+E**.
Switch the host screen display mode	● To display the remote screen on the host: Select **Video > Turn ON Host Display**.

Operation	Description
	● Not to display the remote screen on the host: Select **Video > Turn OFF Host Display**. Note: You can use either of the following methods to rapidly switch between the remote screen display modes of the host. ● Click 🖥. ● Press **Alt+N**.
Capture the current screen	Capture the current screen through either of the following ways: ● Select **Video > Capture Screen**. ● Press **Alt+S**.
Set a video decoding mode	a. Select **Video > Compression Mode**. b. Select a video decoding mode from the displayed submenu.
Set the video display quality	a. Select **Video > DCT Quantization Table**. b. Select the video display quality from the displayed submenu. Note: The video display quality is divided into eight levels from 0 through 7, with video quality degraded in turn.
Send a default key combination to the server	a. Select **Keyboard**. The **keyboard** submenu is displayed. b. Select the shortcut key to be sent. Note: There are two sending types of default shortcut keys by default: ● **Hold Down**: The corresponding shortcut key is always pressed until the selection of the shortcut key is canceled. You can also press the corresponding button in the lower right corner of the window. ● **Press and Release**: The corresponding shortcut key is sent once and released immediately.
Define a key combination	a. Select **Keyboard > Hot Keys > add Hot Keys**. The **User Defined Macros** page is displayed. b. Click **add**. The **Add Macros** page is displayed. c. Press and then release the user-defined key combination. d. Click **OK**.
Send a user-defined key combination to the server	a. Select **Keyboard > Hot Keys**. b. In the displayed submenu, select the self-defined keyboard shortcut to be sent.
Enable full keyboard support	● Enable full keyboard support: Select **Keyboard** and then select **Full Keyboard Support**. ● Disable full keyboard support: Select **Keyboard** and then deselect **Full Keyboard Support**.
Switch mouse show mode on the client	● Show the cursor: Select **Mouse** and then select **Show Cursor**. ● Hide the cursor: Select **Mouse** and then deselect **Show Cursor**. Note: You can use either of the following methods to rapidly switch between the mouse display modes on the client.

Operation	Description
	● Press **Alt+C**. ● Click 🖱.
Set a mouse mode	a. Select **Mouse > Mouse Mode**. b. Select a mouse mode from the displayed mouse mode submenu. ● **Absolute mouse mode**: transfers the absolute position of the local mouse to the server to make the mouse on the server move. ● **Relative mouse mode**: calculates the displacement of the local mouse relative to the server mouse, and transfers it to the server to make the mouse on the server move. ● **Other mouse mode**: calculates the displacement of the local mouse relative to the center position, and transfers it to the server to make the mouse on the server move.
Set the network bandwidth	a. Select **Options > Bandwidth**. b. Select the bandwidth from the displayed submenu.
Switch the encryption status of the mouse/keyboard	● Enable mouse/keyboard encryption: Select **Options** and then select **Keyboard/Mouse Encryption**. ● Disable mouse/keyboard encryption: Select **Options** and then deselect **Keyboard/Mouse Encryption**.
Set the scaling mode of a remote screen	a. Select **Options > Zoom**. b. In the displayed submenu, set the zoom scale of the remote screen. ● **Zoom In**: zooms in the remote screen. ● **Zoom Out**: zooms out the remote screen. ● **Actual Size**: displays the remote screen in the proportion of 100%. ● **Fit to Client Resolution**: displays the remote screen in the resolution of the local client system. ● **Fit to Host Resolution**: displays the remote screen in the resolution of the remote server system.
Send an IPMI command to the server	a. Select **Options > Send IPMI Command**. The **IPMI Command Dialog** window is displayed. b. Enter the IPMI command. c. Click **Send**. Note: The IPMI command supports hex format and ASCII format.
Set a GUI language	a. Select **Options > GUI Languages**. b. Select the GUI language from the displayed submenu. Only English is supported in the current version.
Set the privilege request mode	a. Select **Options > Block Privilege Request**. b. Select a privilege request block mode from the displayed submenu. ● **Allow only Video**: Privilege requests in the system are automatically granted access to video.

Operation	Description
	● **Deny Access**: Privilege requests in the system are blocked.
Request all permissions	Select **Options > Request Full Permission**.
Mount a local ISO file	a. Open the **Virtual Media** window through either of the following ways: ● Select **Media > Virtual Media Wizard...**, and switch to the **CD/DVD** tab. ● Click 💿. b. Click **Browse** and select a local ISO file. c. Click **Connect**.
Mount a local disk	a. Select **Media > Virtual Media Wizard...**, and switch to the **Hard Disk/USB** tab. b. Select a local disk drive letter or click **Browse** and then select the image file of the local disk. c. Click **Connect**.
Mount a local folder	a. Create a new ISO file on the client PC b. Open the **Virtual Media** window through either of the following ways: ● Select **Media > Virtual Media Wizard...**, and switch to the **Hard Disk/USB** tab. ● Click 🖴. c. Select **Physical Drive > Folder Path** or **Logical Drive > Folder Path** . d. Click **Browse** and select a local folder path. e. Set **Size** and **Image Path**. f. Click **Connect**. Note: **Size** must be the n-th power of 2, such as 2, 4 and 8. **Image Path** should be the same as the new ISO file path.
Set keyboard layout	a. Select **Keyboard Layout**. b. Select the keyboard layout from the displayed submenu.
Open the soft keyboard	Click ⌨.
Configure video recording	a. Select **Video Record > Settings**. The **Video Record** window is displayed. b. Set the video recording time length in seconds and the video storage position. c. Click **OK**. Note: The video recording time length ranges from 1 through 1800 seconds.
Record a video	a. Start recording a video through either of the following ways: ● Select **Video Record > Start Record**.

Operation	Description
	● Click 🎥. b. (Optional) Stop recording a video through either of the following ways: ● Select **Video Record > Stop Record**. ● Click 🎥. c. After the preset recording time length is reached or the recording is stopped manually, click **OK**. The recorded video file is saved to the `VideoCaptures` folder in the preset path.
Set the server power mode	a. Select **Power**. b. Select a server power option from the displayed submenu. The server power options are as follows: ● **Reset Server**: restarts the system without shutting down the power supply (warm reboot). ● **Immediate Shutdown**: shuts down the server immediately by shutting down the power supply. ● **Orderly Shutdown**: shuts down the server in order through program control. ● **Power On Server**: starts the server. ● **Power Cycle Server**: shuts down the server and restarts it (cold reboot).
Check active users	View the users using remote control through either of the following ways: ● Select **Active Users**. ● Click 👤.

3.9 Controlling the Server Power Supply

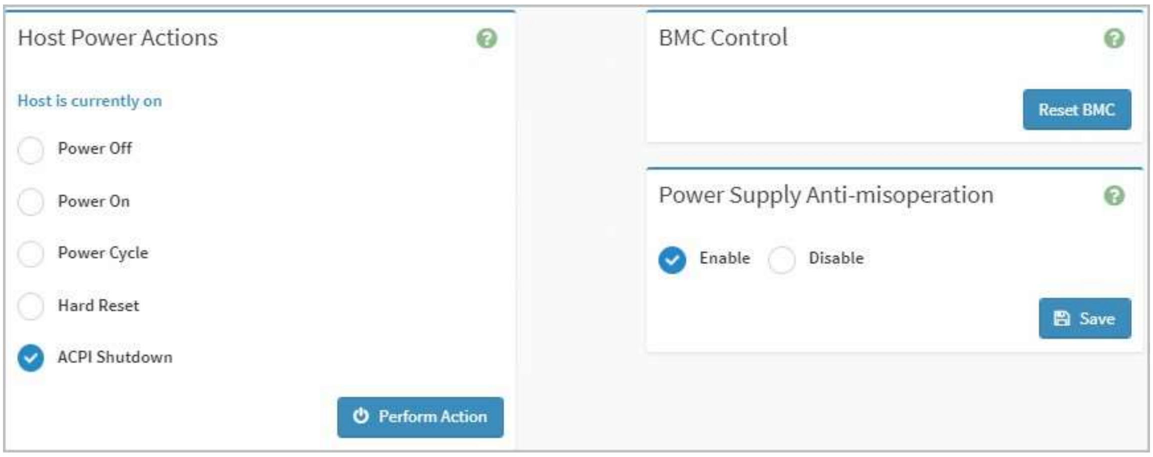
Abstract

If the server power supply cannot be controlled on-site, you can control the server remotely on the client PC for power-on, power-off, restart, and BMC resetting.

Steps

1. From the menu bar in the left pane, select **Power Control**. The **Power Control** page is displayed, see Figure 3-78.

Figure 3-78 Power Control Page



Host Power Actions

Host is currently on

○ Power Off

○ Power On

○ Power Cycle

○ Hard Reset

● ACPI Shutdown

BMC Control

Power Supply Anti-misoperation

● Enable ○ Disable

2. Perform the following operations as required.

To...	Do...
Shut down the server	a. Select **Power Off**. b. Click **Perform Action**.
Power on the server	a. Select **Power On**. b. Click **Perform Action**.
Perform a cold reboot	a. Select **Power Cycle**. b. Click **Perform Action**. Cold reboot means that the server is started after it is shut down. During the restart, the server is offline.
Perform a warm reboot	a. Select **Hard Reset**. b. Click **Perform Action**. Warm reboot means that the server is restarted when it is not shut down. During the restart, the server is not offline.
Shut down the operating system of the server	a. Select **ACPI Shutdown**. b. Click **Perform Action**. ACPI shutdown refers to the operation of simulating the shutdown button of the operating system to shut down the operating system.
Reset the BMC	Click **Reset BMC**. After the BMC is reset, you can log in to the Web portal again.
Enable the power supply anti-misoperation function	a. Select **Enable**. b. Click **Save**. After the function is enabled, the server that is in power-on state will not be powered off if the power button is pressed for a short period (within 10 seconds).
Disable the power supply anti-misoperation function	a. Select **Disable**. b. Click **Save**.

To...	Do...
	After the function is disabled, the power button takes effect immediately when it is pressed.

3.10 NIC Information Query

3.10.1 Querying Ethernet NIC Information

Abstract

By querying the Ethernet NIC information, you can learn about the detailed information about the NIC and its port on the server.

Context

The Ethernet NIC uses the IP protocol, and it is connected to an Ethernet switch through optical fibers or twisted pairs.

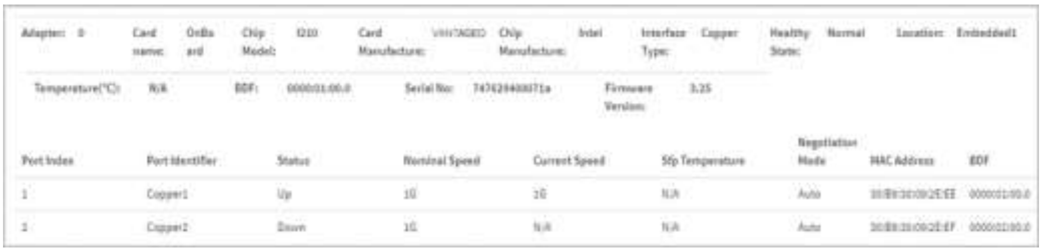
The Ethernet NIC has optical interfaces and electrical interfaces.

- Optical interface: Data is transmitted through optical fibers.
- Electrical interface: Data is transmitted through twisted pairs. The common interface type is RJ45.

Steps

1. From the menu bar in the left pane, select **Network Device > NIC Information**. The **NIC** page is displayed, see Figure 3-79.

Figure 3-79 NIC Page



Adapter: 0 Card name: OnBoard Chip Model: I210 Card Manufacture: VANTAGEO Chip Manufacture: Intel Interface Type: Copper Healthy State: Normal Location: Embedded1

Temperature(°C): N/A BDF: 0000:01:00.0 Serial No: 747629400871a Firmware Version: 3.25

Port Index	Port Identifier	Status	Nominal Speed	Current Speed	Sfp Temperature	Negotiation Mode	MAC Address	BDF
1	Copper1	Up	1G	1G	N/A	Auto	30:B8:30:09:2E:EE	0000:01:00.0
2	Copper2	Down	1G	N/A	N/A	Auto	30:B8:30:09:2E:EF	0000:01:00.0

Note

The rate of the onboard NIC cannot be self-adaptive.

3.10.2 Querying FC NIC Information

Abstract

By querying the FC NIC information, you can learn about the detailed information about the FC NIC and its port on the server.

Context

The FC NIC is also called fiber NIC, which uses the fiber channel protocol and is generally connected to a fiber channel switch through optical fibers.

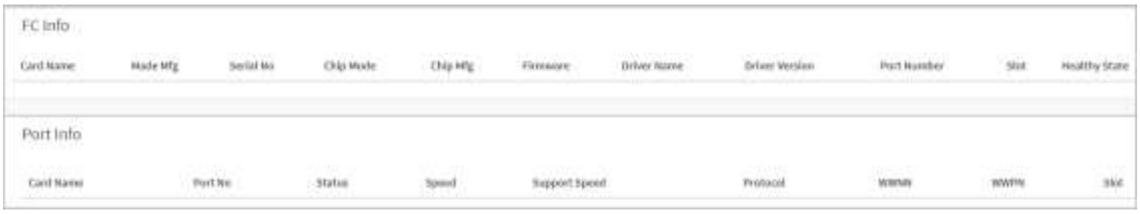
The FC NIC has optical interfaces and electrical interfaces:

- Optical interface: Data is transmitted through optical fibers.
- Electrical interface: Data is transmitted through twisted pairs. The common interface type is D89 or HSSDC.

Steps

1. From the menu bar in the left pane, select **Network Device > FC Information**. The **FC** page is displayed, see Figure 3-80.

Figure 3-80 FC Page



FC Info

Card Name	Made Mfg	Serial No	Chip Mode	Chip Mfg	Firmware	Driver Name	Driver Version	Port Number	Slot	Healthy State

Port Info

Card Name	Port No	Status	Speed	Support Speed	Protocol	WWNN	WWPN	Slot

Some of the parameters in the FC information are described as follows:

- **Healthy State**: indicates the health status of the FC NIC, including healthy and faulty.
- **Status**: indicates the connection status of the ports of the FC NIC, including connected and disconnected.
- WWNN: indicates the globally unique identifier of the FC NIC.
- WWPN: indicates the globally unique identifier of the port of the FC NIC.

Note

→ A single-port FC NIC has one WWNN and one WWPN.
→ A dual-port FC NIC has one WWNN and two WWPNs.

3.11 Fan Information and Air Intake Temperature Query

3.11.1 Querying Fan Information

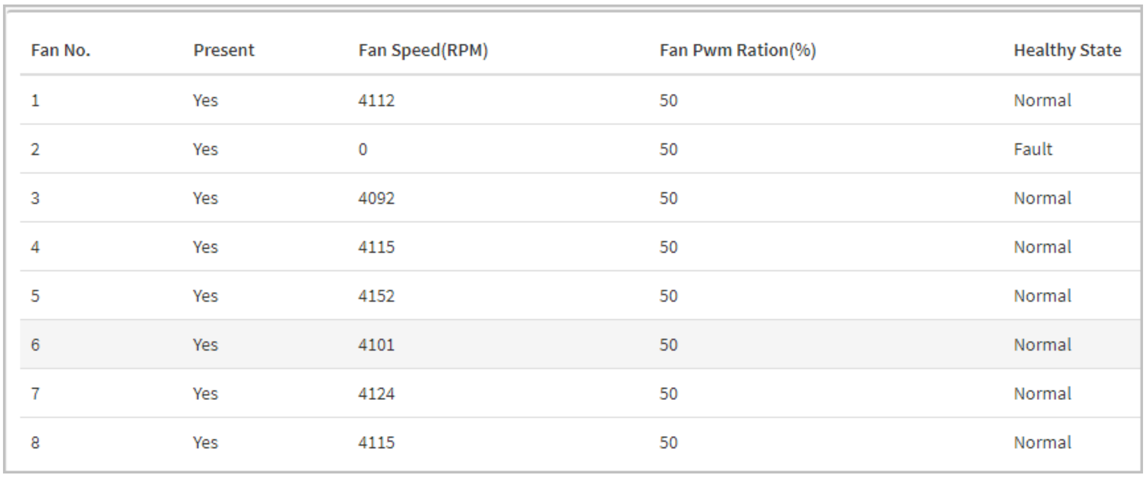
Abstract

By querying fan information, you can learn about internal fans of the server.

Steps

1. From the menu bar in the left pane, select **Fan&Temperature > Fan Information**. The **Fan Information** page is displayed, see Figure 3-81.

Figure 3-81 Fan Information Page



Fan No.	Present	Fan Speed(RPM)	Fan Pwm Ration(%)	Healthy State
1	Yes	4112	50	Normal
2	Yes	0	50	Fault
3	Yes	4092	50	Normal
4	Yes	4115	50	Normal
5	Yes	4152	50	Normal
6	Yes	4101	50	Normal
7	Yes	4124	50	Normal
8	Yes	4115	50	Normal

Note

- The **Fan Speed(RPM)** column displays the current speed of each fan.
- The **Fan Pwm Ratio(%)** column displays the ratio of the current speed of a fan to the maximum speed of the fan.

3.11.2 Querying Air Intake Temperatures

Abstract

This procedure describes how to query air intake temperatures to learn about the air intake temperature changes of the server.

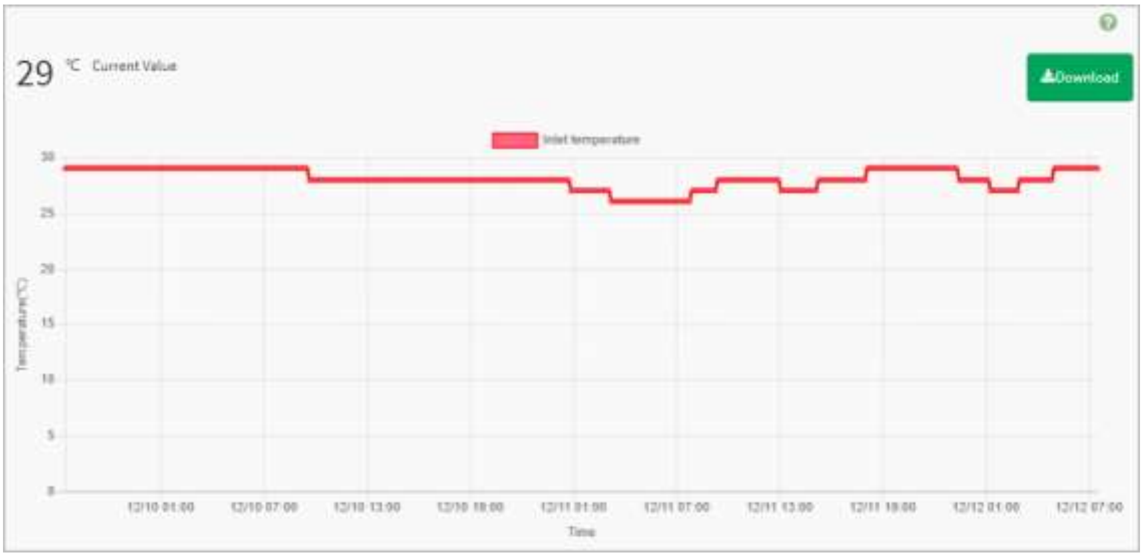
Note

The server supports the high-temperature power-off function. If this function is enabled, the server is powered off after the air inlet temperature reaches the preset threshold, avoiding damages to the server hardware. To ensure service operation stability, it is recommended to disable this function.

Steps

1. From the menu bar in the left pane, select **Fan&Temperature > Inlet Temperature**. The **Inlet Temperature** page is displayed, as shown in Figure 3-82.

Figure 3-82 Inlet Temperature Page



2. (Optional) To save the temperature statistics (which are stored for a maximum of 60 hours on the BMC) to the local PC, click **Download**.

3.12 Power Supply Management

3.12.1 Configuring System Power Control Parameters

Abstract

System power includes:

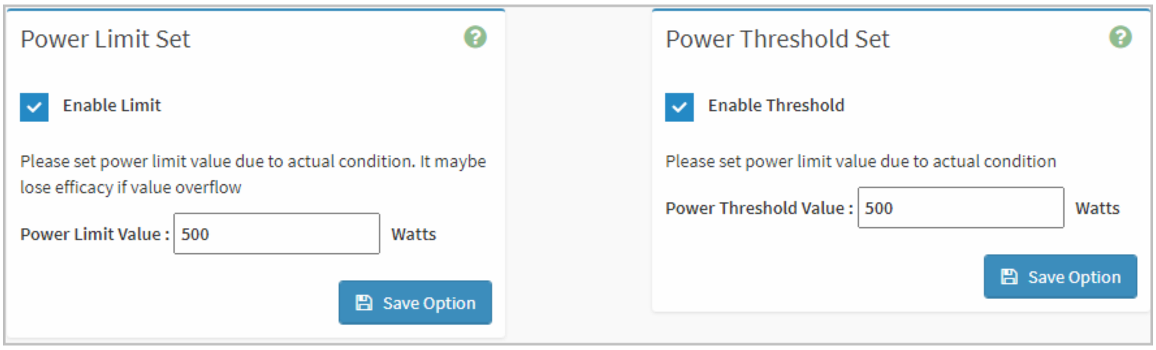
- **Capped power**: Peak power of the server.
- **Threshold power**: An alarm is raised when the power of the server exceeds the threshold.

By configuring system power control parameters, you can set the capped power and threshold power.

Steps

1. From the menu bar in the left pane, select **Power Management > System Power Limit**. The **System Power Limit** page is displayed, see Figure 3-83.

Figure 3-83 System Power Limit Page



Power Limit Set

☑ Enable Limit

Please set power limit value due to actual condition. It maybe lose efficacy if value overflow

Power Limit Value : 500 Watts

Save Option

Power Threshold Set

☑ Enable Threshold

Please set power limit value due to actual condition

Power Threshold Value : 500 Watts

Save Option

2. Perform the following operations as required.

To...	Do...
Set the capped power	a. In the **Power Limit Set** area, select **Enable Limit**. b. In the **Power Limit Value** text box, enter the capped power, with a range of 1–32767. c. Click **Save Option** in the **Power Limit Set** area.
Set the threshold power	a. In the **Power Limit Set** area, select **Enable Threshold**. b. In the **Power Threshold Value** text box, enter the threshold power, with a range of 5–32767. c. Click **Save Option** in the **Power Threshold Set** area.

3.12.2 Collecting System Power Statistics

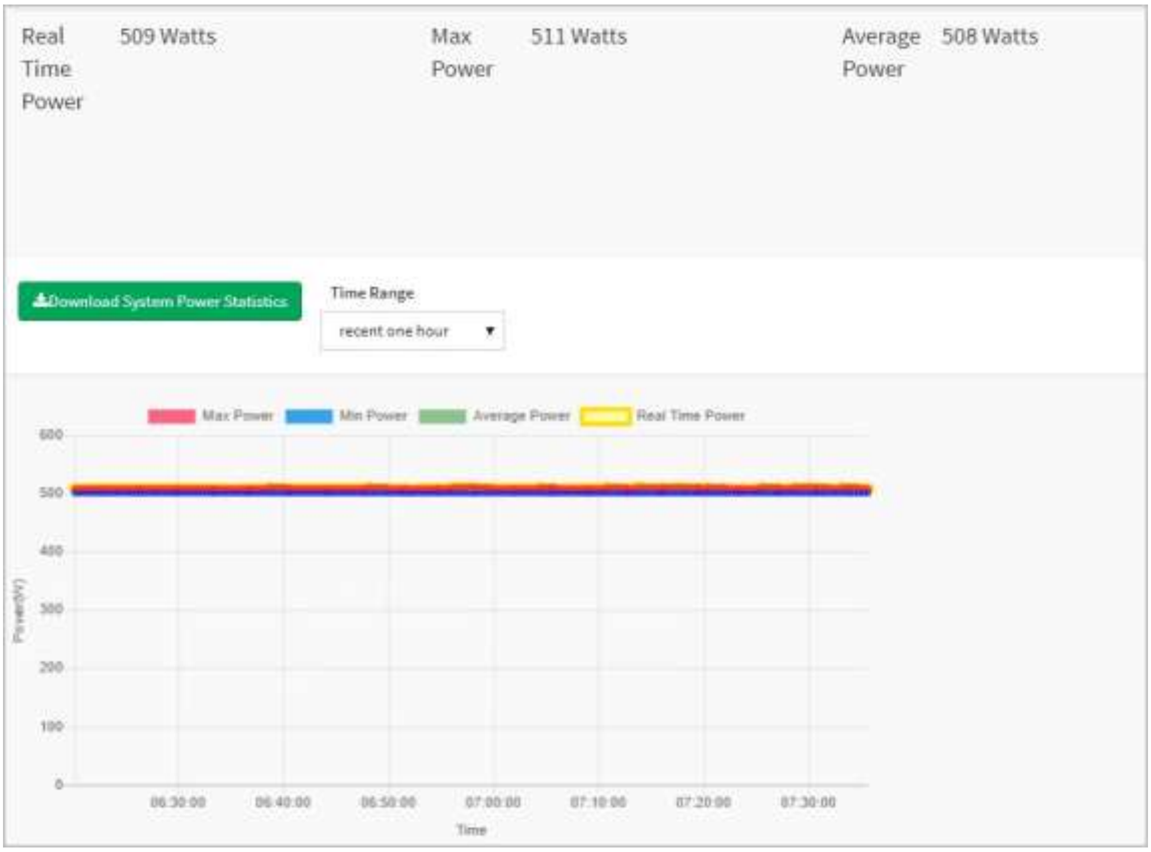
Abstract

System power statistics show the fluctuations of system power in a designated period of time.

Steps

1. From the menu bar in the left pane, select **Power Management > System Power Statistics**. The **System Power Statistics** page is displayed, see Figure 3-84.

Figure 3-84 System Power Statistics Page



Real Time Power 509 Watts

Max Power 511 Watts

Average Power 508 Watts

Download System Power Statistics

Time Range: recent one hour

2. From the **Time Range** list, select a time range. A page is displayed, showing the system power statistics in the selected time range.
3. (Optional) To download historical data to the local PC, click **Download System Power Statistics**.

3.12.3 Querying Power Supply Information

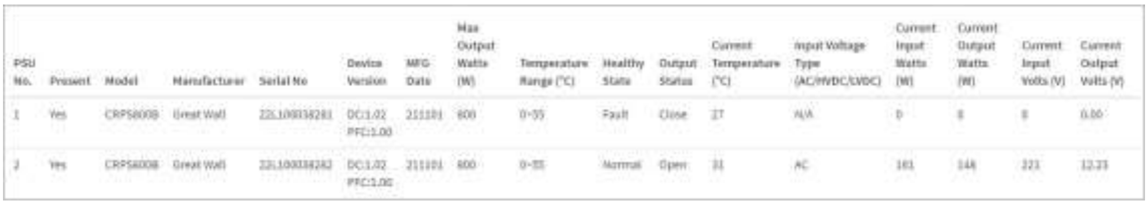
Abstract

By querying power supply information, you can learn about the power supplies of the server.

Steps

1. From the menu bar in the left pane, select **Power Management > Power Information**. The **Power Information** page is displayed, see Figure 3-85.

Figure 3-85 Power Information Page



PSU No.	Present	Model	Manufacturer	Serial No	Device Version	MFG Date	Max Output Watts (W)	Temperature Range (°C)	Healthy State	Output Status	Current Temperature (°C)	Input Voltage Type (AC/HVDC/LVDC)	Current Input Watts (W)	Current Output Watts (W)	Current Input Volts (V)	Current Output Volts (V)
1	Yes	CRPS800B	Great Wall	22L100038281	DC:1.02 PFC:1.00	211101	800	0~55	Fault	Close	27	N/A	0	0	0	0.00
2	Yes	CRPS800B	Great Wall	22L100038282	DC:1.02 PFC:1.00	211101	800	0~55	Normal	Open	31	AC	181	148	221	12.23

Note

Power supply input types include:

- AC
- HVDC
- LVDC

3.12.4 Setting the Power Mode

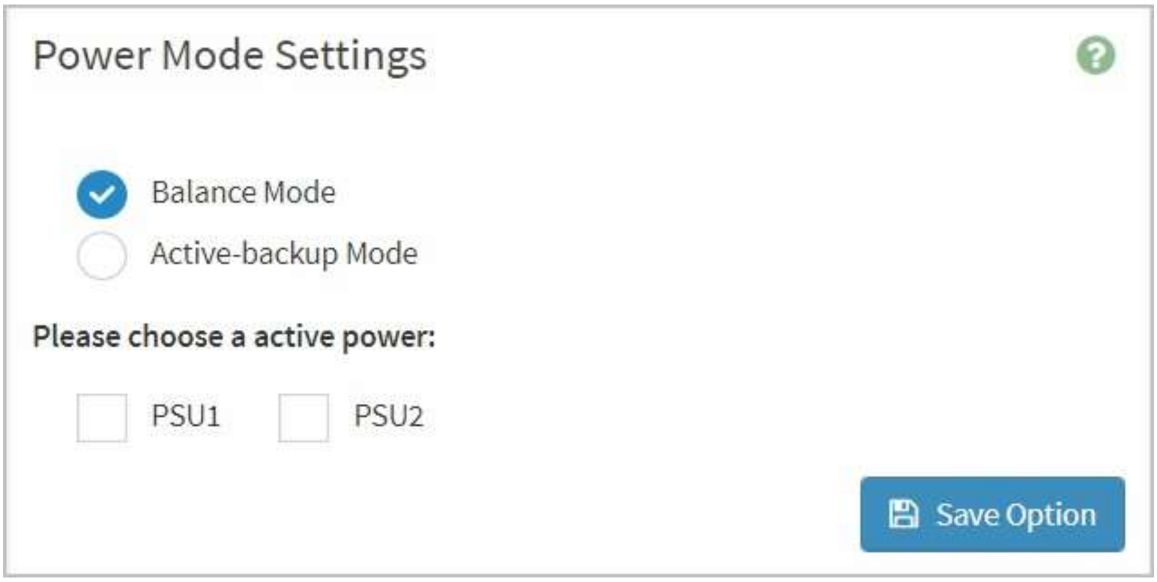
Abstract

If all the power supplies are configured for a server and the power supply models are the same, the power mode can be set on the Web portal of the BMC. In other cases, you can set the power mode only through the CLI of the BMC.

Steps

1. From the menu bar in the left pane, select **Power Management > Power Mode**. The **Power Mode Settings** page is displayed, see Figure 3-86.

Figure 3-86 Power Mode Settings Page



Power Mode Settings

● Balance Mode
○ Active-backup Mode

Please choose a active power:

□ PSU1 □ PSU2

2. Set the parameters. For a description of the parameters, refer to Table 3-35.

Table 3-35 Parameter Descriptions for Power Supply Mode

Parameter	Description	Setting
Balance Mode	Whether the power modules supply power in load balancing mode.	- If you select **Balance Mode**, the power modules supply power in load balancing mode. - If you clear **Balance Mode**, the power modules do not supply power in load balancing mode.

Parameter	Description	Setting
Active-standby Mode	Whether the power modules supply power in active-standby mode.	● If you select **Active-standby Mode**, the power modules supply power in active-standby mode, and the active power supply must be specified. ● If you clear **Active-standby Mode**, the power modules do not supply power in active-standby mode.

3. Click **Save**.

3.13 Querying KPIs

Abstract

KPIs include the following:

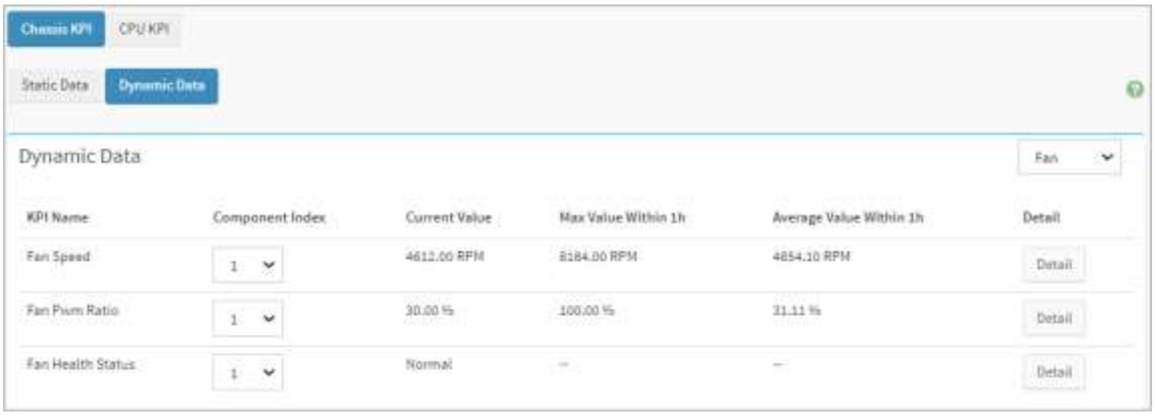
- Chassis KPIs
  - → Static data: chassis health status.
  - → Dynamic data: includes the air inlet temperature, air outlet temperature, power input voltage, and power output voltage.
- CPU KPIs
  - → Static data: CPU details, including the number of CPU cores, maximum frequency, and model.
  - → Dynamic data: includes CPU temperature, total power, and dynamic load.

By querying the KPIs, you can learn about the operational status of the server.

Steps

1. From the menu bar in the left pane, select **Key Performance**. The **KPI Overview** page is displayed, as shown in Figure 3-87.

Figure 3-87 KPI Overview Page



Dynamic Data

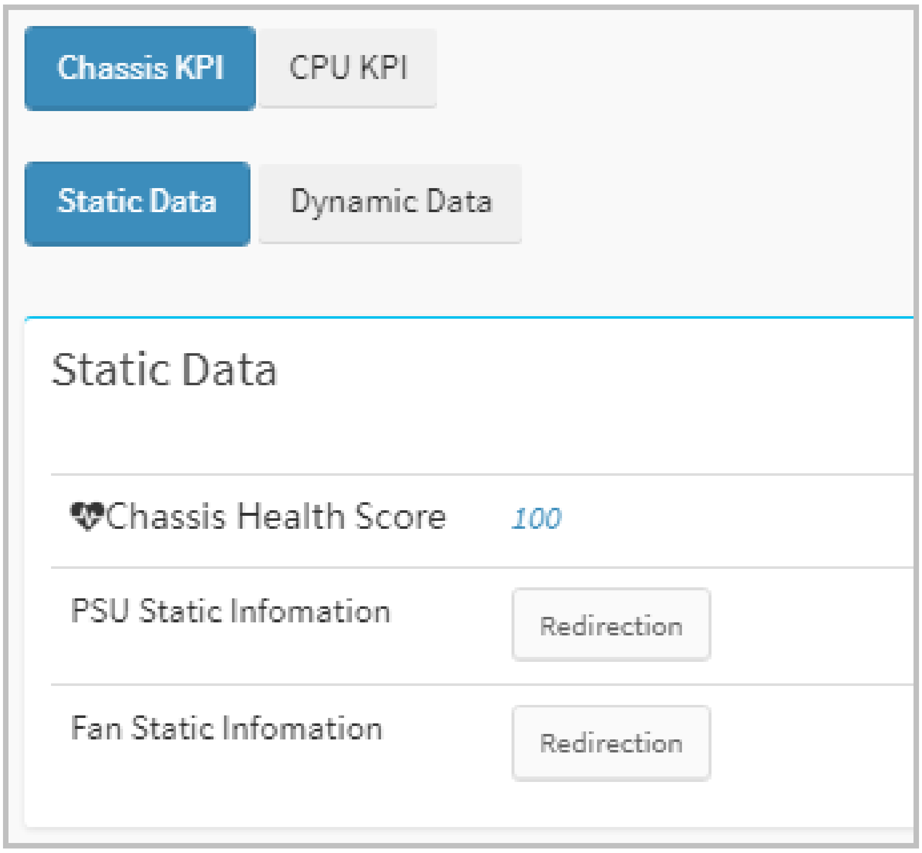
Fan

KPI Name	Component Index	Current Value	Max Value Within 1h	Average Value Within 1h	Detail
Fan Speed	1	4612.00 RPM	8184.00 RPM	4654.10 RPM	Detail
Fan Pwm Ratio	1	30.00 %	100.00 %	31.11 %	Detail
Fan Health Status	1	Normal	--	--	Detail

2. Perform the following operations as required.

To...	Do...
Query the static data of chassis KPIs	a. In the upper area, click **Chassis KPI** and then **Static Data**. The static data of chassis KPIs is displayed, as shown in Figure 3-88. b. (Optional) If the value of **Chassis Health Score** is not **100**, click the score to view the detailed score deduction items.
Query the dynamic data of chassis KPIs	a. In the upper area, click **Chassis KPI** and then **Dynamic Data**. The dynamic data of chassis KPIs is displayed, as shown in Figure 3-87. b. Click **Detail** for an indicator to check the indicator details.
Query the static data of CPU KPIs	a. In the upper area, click **CPU KPI** and then **Static Data**. The static data of CPU KPIs is displayed, as shown in Figure 3-89. b. Check CPU details.
Query the dynamic data of CPU KPIs	a. In the upper area, click **CPU KPI** and then **Dynamic Data**. The dynamic data of CPU KPIs is displayed, as shown in Figure 3-90. b. Click **Detail** for an indicator to check the indicator details.

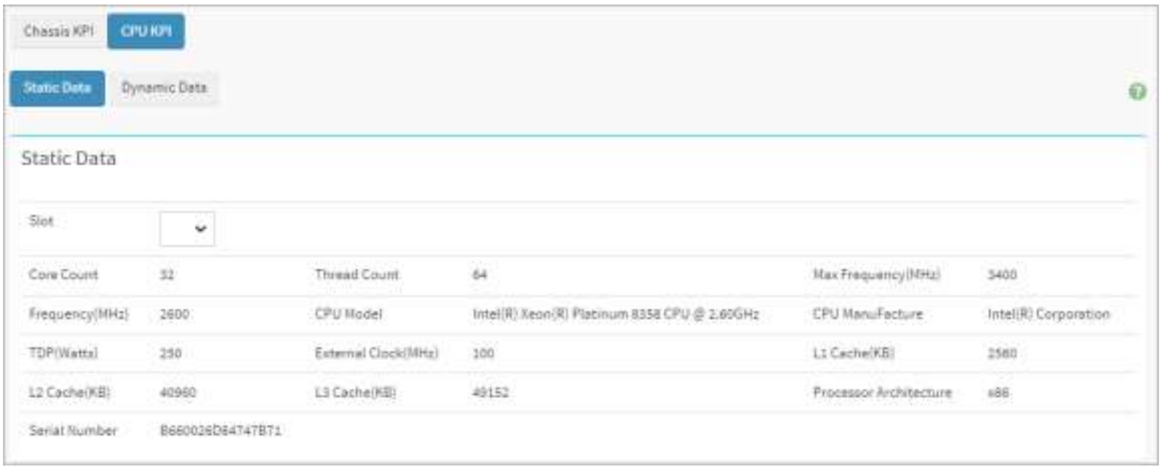
Figure 3-88 Static Data of Chassis KPIs



Static Data

Chassis Health Score	100
PSU Static Infomation	Redirection
Fan Static Infomation	Redirection

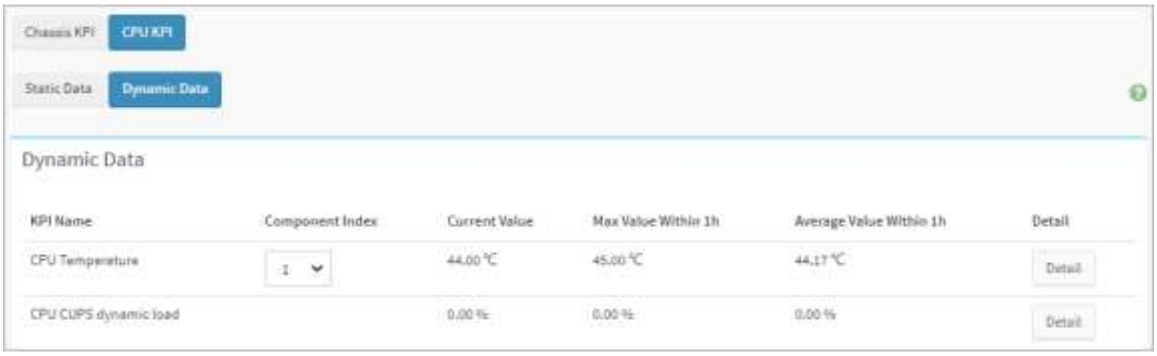
Figure 3-89 Static Data of CPU KPIs



Static Data

Slot					
Core Count	32	Thread Count	64	Max Frequency(MHz)	3400
Frequency(MHz)	2600	CPU Model	Intel(R) Xeon(R) Platinum 8358 CPU @ 2.60GHz	CPU ManuFacture	Intel(R) Corporation
TDP(Watts)	250	External Clock(MHz)	100	L1 Cache(KB)	2560
L2 Cache(KB)	40960	L3 Cache(KB)	49152	Processor Architecture	x86
Serial Number	B660026D64747B71				

Figure 3-90 Dynamic Data of CPU KPIs



Dynamic Data

KPI Name	Component Index	Current Value	Max Value Within 1h	Average Value Within 1h	Detail
CPU Temperature	1	44.00 ℃	45.00 ℃	44.17 ℃	Detail
CPU CUPS dynamic load		0.00 %	0.00 %	0.00 %	Detail

3.14 Maintenance Management

3.14.1 Querying Firmware Information

Abstract

By querying the firmware information, you can learn about the firmware version of each board on the server. If a firmware version is low and there are upgrade files for higher version, you can upgrade the firmware of the corresponding board.

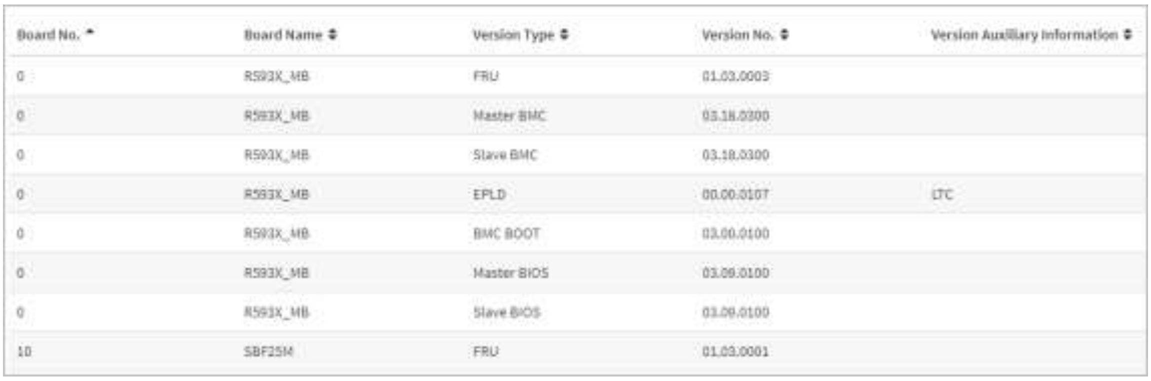
Context

The board firmware versions include EPLD, BMC, FRU and BIOS.

Steps

1. From the menu bar in the left pane, select **Maintenance**. The **Maintenance** page is displayed.
2. Click **Firmware Information**. The **Firmware Information** page is displayed, see Figure 3-91.

Figure 3-91 Firmware Information Page



Board No. ▲	Board Name ⇕	Version Type ⇕	Version No. ⇕	Version Auxiliary Information ⇕
0	R593X_MB	FRU	01.03.0003	
0	R593X_MB	Master BMC	03.18.0300	
0	R593X_MB	Slave BMC	03.18.0300	
0	R593X_MB	EPLD	00.00.0107	LTC
0	R593X_MB	BMC BOOT	03.00.0100	
0	R593X_MB	Master BIOS	03.09.0100	
0	R593X_MB	Slave BIOS	03.09.0100	
10	SBF25M	FRU	01.03.0001	

Note

If **LTC** is displayed in the **Version Auxiliary Information**, the manufacturer of the EPLD on the mainboard is the Lattice Semiconductor Corporation.

3.14.2 Restoring Factory Defaults

Abstract

By restoring factory defaults, you can restore the server configuration items (for example, the network, user, SNMP configuration and startup mode) to factory defaults.

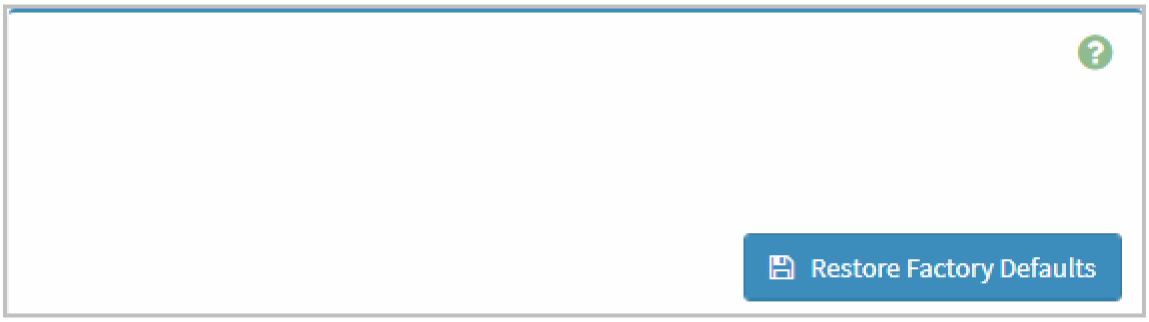
Note

Do not perform any operation during restoration.
After factory defaults are restored, the server is restarted.

Steps

1. From the menu bar in the left pane, select **Maintenance** . The **Maintenance** page is displayed.
2. Click **Restore Factory Defaults** . The **Restore Factory Defaults** page is displayed, see Figure 3-92.

Figure 3-92 Restore Factory Defaults Page



3. Click **Restore Factory Defaults**.

3.14.3 Configuring a System Administrator

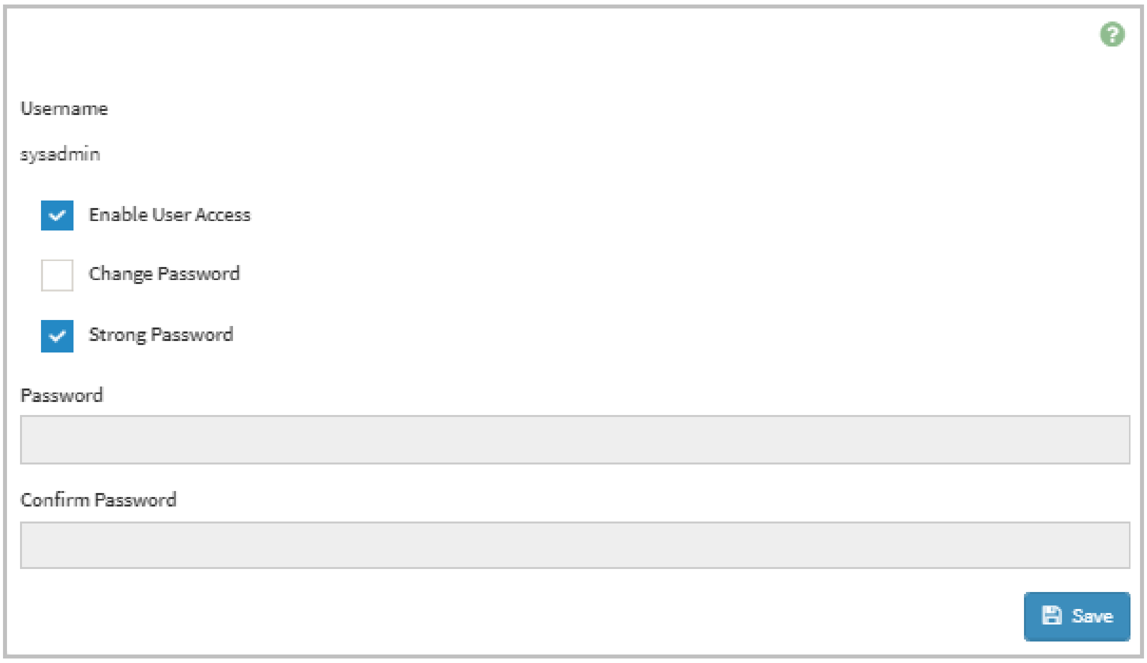
Abstract

By configuring a system administrator, you can enable or disable the system administrator to access the BMC backend command line system and configure the password for the system administrator to log in to the BMC backend command line system.

Steps

1. From the menu bar in the left pane, select **Maintenance** . The **Maintenance** page is displayed.
2. Click **System Administrator** . The **System Administrator** page is displayed, see Figure 3-93.

Figure 3-93 System Administrator Page



Username

sysadmin

☑ Enable User Access

□ Change Password

☑ Strong Password

Password

Confirm Password

3. Configure the system administrator parameters. For a description of the parameters, refer to Table 3-36.

Table 3-36 System Administrator Parameter Descriptions

Parameter	Description	Setting
Username	Username used to log in to the BMC backend command line system.	This parameter is read only, and you do not need to configure it.

Parameter	Description	Setting
Enable User Access	Whether to enable the system administrator to access the BMC back-end command line system.	● To enable the system administrator to access the BMC back-end command line system, select **Enable User Access** . ● To disable the system administrator to access the BMC back-end command line system, deselect **Enable User Access** .
Change Password	Whether to change the login password of the system administrator. The default passwords depend on the server models and BMC versions. For details, refer to 5 Reference: Default Passwords.	● To change the login password for the system administrator, select **Change Password** , and enter **Password** and **Confirm Password** . Range of password length: 8–64 characters. ● If the login password for the system administrator does not need to be changed, deselect **Change Password** .
Strong Password	Whether to enable the strong password policy.	The password must contain four types of characters (uppercase letters, lowercase letters, digits, and symbols). ● To enable the strong password policy, select **Strong Password**. ● To disable the strong password policy, deselect **Strong Password**.

4. Click **Save**.

3.14.4 Upgrading Firmware

Abstract

If the firmware on the mainboard of a server needs an upgrade, you can upload the firmware online for upgrade.

If multiple firmware versions need an upgrade, the following sequence is recommended:

1. FRU firmware

   After the FRU firmware is upgraded, the BMC is automatically restarted to apply the new version.

2. BMC firmware

   The Web portal of the BMC temporarily supports the upgrade of the active BMC firmware only. After the active BMC firmware is upgraded, the BMC is automatically restarted to apply it.

3. EPLD firmware

After the EPLD firmware is upgraded, the new version takes effect only after the server is restarted. Therefore, it is recommended that you stop the services running on the server before the upgrade.

4. BIOS firmware

   After the BIOS firmware is upgraded, the new version takes effect only after the server is restarted. Therefore, it is recommended that you stop the services running on the server before the upgrade.

   - If the BIOS firmware is upgraded when the server is powered off, the upgraded BIOS firmware takes effect directly.
   - If the BIOS firmware is upgraded when the server is powered on, the upgraded BIOS firmware is displayed as a standby version on the Web portal and takes effect automatically after the server is powered off and restarted. It takes time for the new version to take effect automatically. During this period, firmware upgrade is not allowed.

5. VR firmware

Note

If a firmware version fails to be upgraded during version upgrade, you must upgrade it again.

Prerequisite

You have obtained the version upgrading files.

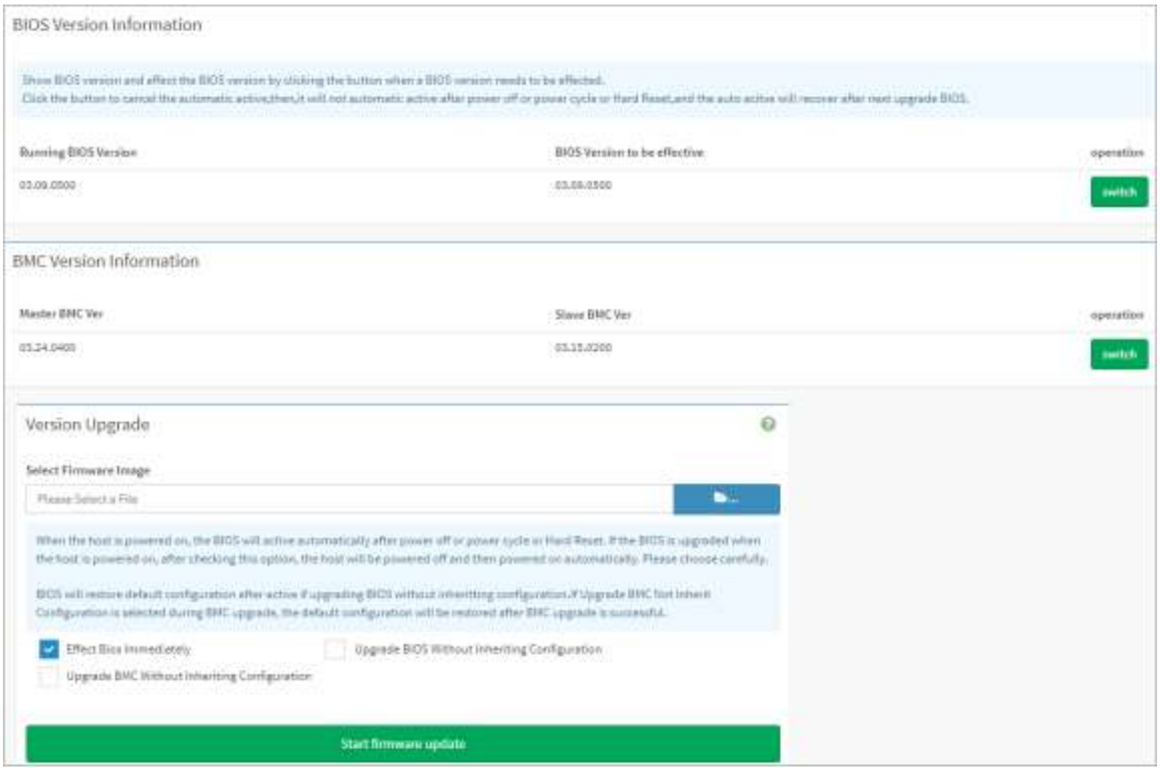
Note

The firmware upgrade files can be downloaded on the Web portal (https://vantageo.com) of the servers.

Steps

1. From the menu bar in the left pane, select **Maintenance**. The **Maintenance** page is displayed.
2. Click **Firmware Update**. The **Firmware Update** page is displayed, see Figure 3-94.

Figure 3-94 Firmware Update Page



BIOS Version Information

Show BIOS version and affect the BIOS version by clicking the button when a BIOS version needs to be affected.
Click the button to cancel the automatic active,then,it will not automatic active after power off or power cycle or Hard Reset,and the auto active will recover after next upgrade BIOS.

Running BIOS Version	BIOS Version to be effective	operation
03.09.0500	03.08.0500	switch

BMC Version Information

Master BMC Ver	Slave BMC Ver	operation
03.24.0400	03.15.0200	switch

Version Upgrade

Select Firmware Image

Please Select a File

When the host is powered on, the BIOS will active automatically after power off or power cycle or Hard Reset. If the BIOS is upgraded when the host is powered on, after checking this option, the host will be powered off and then powered on automatically. Please choose carefully.

BIOS will restore default configuration after active if upgrading BIOS without inheriting configuration.If Upgrade BMC Not Inherit Configuration is selected during BMC upgrade, the default configuration will be restored after BMC upgrade is successful.

☑ Effect Bios Immediately ☐ Upgrade BIOS Without Inheriting Configuration
☐ Upgrade BMC Without Inheriting Configuration

3. In the **Version Upgrade** area, click 📂.... In the displayed dialog box, select a version file.

Note

Only one version file can be selected at a time. When the firmware version is updated, the firmware type is automatically matched.

4. (Optional) Select the following check box as needed if the BIOS firmware is upgraded.
   - **Effect Bios Immediately**: When the server is powered on and the BIOS firmware is upgraded, the server is automatically powered off and then powered on to make the upgraded firmware take effect.
   - **Upgrade BIOS Without Inheriting Configuration**: After the upgraded BIOS firmware takes effect, the default BIOS configuration is restored.
   - **Upgrade BIOS Without Inheriting Configuration**: After the upgraded BIOS firmware takes effect, the default BIOS configuration is restored.

Note

When the server is powered on, the upgraded BIOS firmware takes effect after the server is powered off, power cycled, or hard rebooted.

5. Click **Start firmware update.** The firmware upgrade progress is displayed below.

Notice

During the version upgrade process, it is not allowed to switch to another page. Otherwise, the version upgrade process is interrupted.

Note

After the BIOS firmware and BMC firmware are upgraded, the **Other Firmware Update** page is refreshed as follows:

- BIOS firmware: When the server is powered on, the firmware version number generated after upgrade is displayed in the **BIOS Version to be effective** column, and **Active** is displayed in the **operation** column. When the server is powered off, the firmware version number generated after upgrade is displayed in the **Running BIOS Version**, and **switch** is displayed in the **operation** column.
- BMC firmware: The firmware version number generated after upgrade is displayed in the **Master BMC Ver** column, and the version number originally displayed in the **Master BMC Ver** column is displayed in the **Slave BMC Ver** column.

6. (Optional) When the BIOS firmware is upgraded, and **Effect Bios Immediately** is not selected, click **Active** in the **operation** column of the **BIOS Version Information**.

Note

The server is powered off and then powered on automatically to make the upgraded firmware take effect.

Related Tasks

Perform the following operations as required.

To...	Do...
Perform a switchover between the running BIOS version and the BIOS version to be effective	In the **BIOS Version Information** area, click **switch**.
Perform a switchover between the active and standby BMC versions	In the **BMC Version Information** area, click **switch**.

Note

- After the switchover between the running BIOS version and the BIOS version to be effective, the server is automatically restarted.
- After the switchover between the active and standby BMC versions, the BMC is automatically restarted.

3.14.5 Exporting Data in One Click

Abstract

By exporting data in one click, you can export the log data of the BMC to the local PC. The exported log file name is *bmcinfo_SN.tar.gz*, which is stored in the default download directory of the browser.

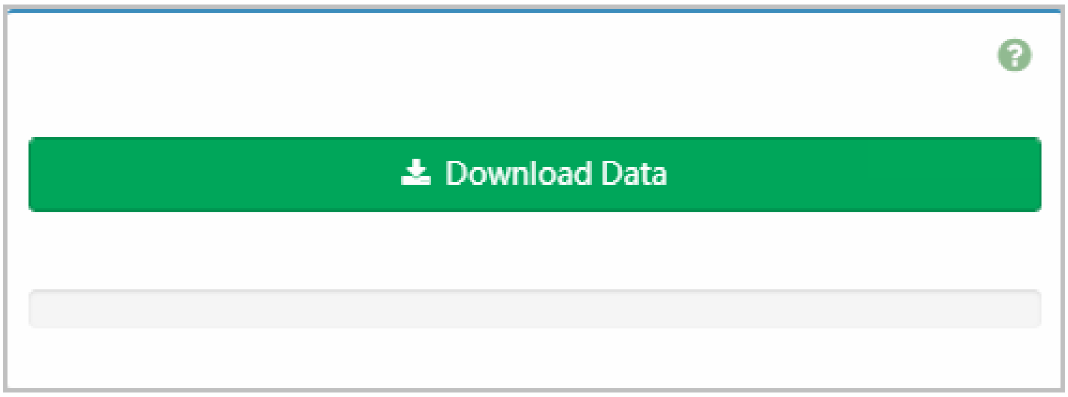
Note

If the SN of the server cannot be queried, the name of the exported log file is *bmcinfo_UnknownProductSN.tar.gz*.

Steps

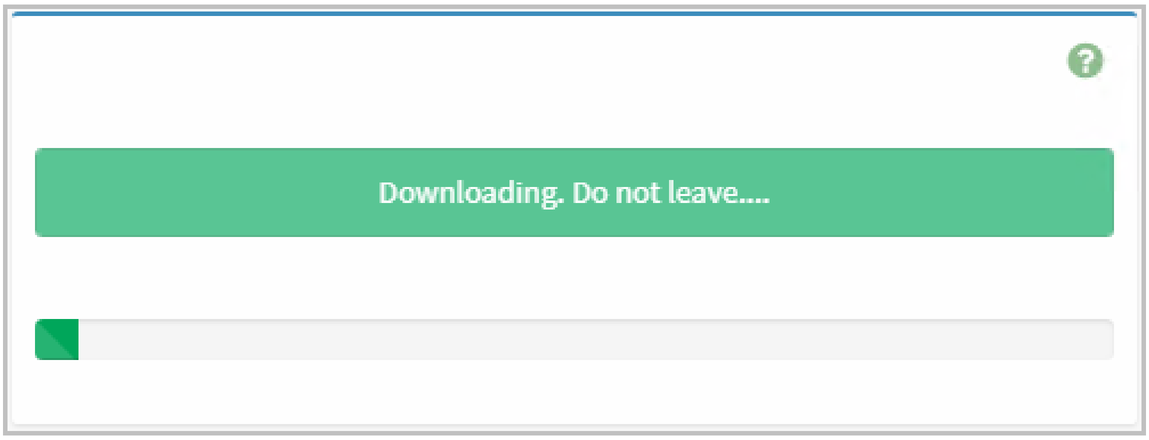
1. From the menu bar in the left pane, select **Maintenance**. The **Maintenance** page is displayed.
2. Click **Expert Data**. The **Download Expert Data** page is displayed, see Figure 3-95.

Figure 3-95 Download Expert Data Page



3. Click **Download Data**. The download progress is displayed, see Figure 3-96.

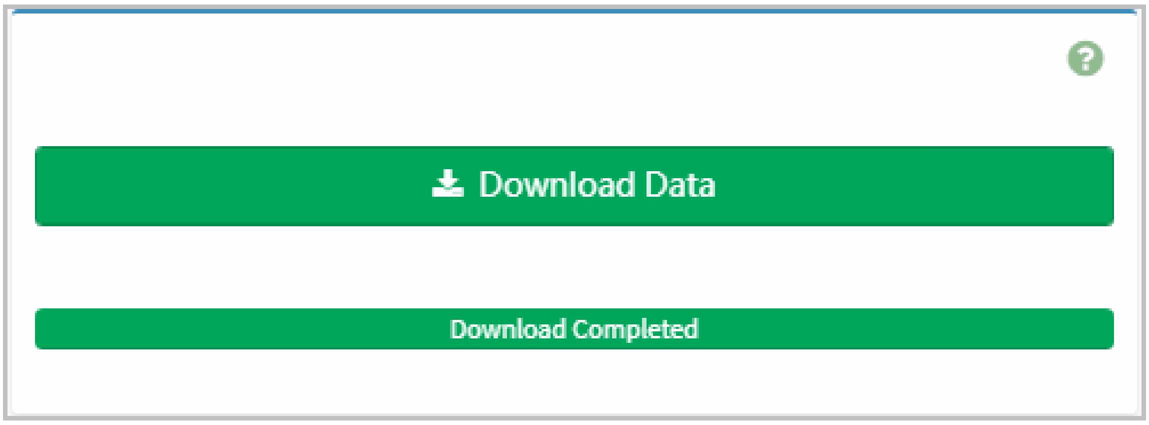
Figure 3-96 Download Progress Page



Downloading. Do not leave....

Figure 3-97 shows the downloaded page.

Figure 3-97 Download Completed Page



Download Data

Download Completed

3.14.6 Backing Up BMC Configurations

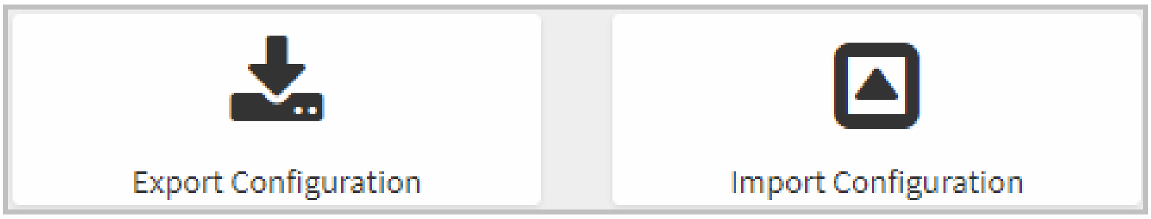
Abstract

Before replacing the mainboard of the server, you must export the BMC configurations. After the mainboard is replaced, you can import the BMC configurations.

Steps

1. Select **Maintenance**. The **Maintenance** page is displayed.
2. Click **Backup Configuration**. The **Backup Configuration** page is displayed, see Figure 3-98.

Figure 3-98 Backup Configuration Page



3. Perform the following operations as required.

To...	Do...
Export configurations	a. Click **Export Configuration**. The **Export Configuration** page is displayed. b. Click **Download Configuration**.
Import configurations	a. Click **Import Configuration**. The **Import Configuration** page is displayed. b. Click 📂..., and select the exported configuration file. c. Click **Upload Configuration**.

3.14.7 Updating PCIe Topology

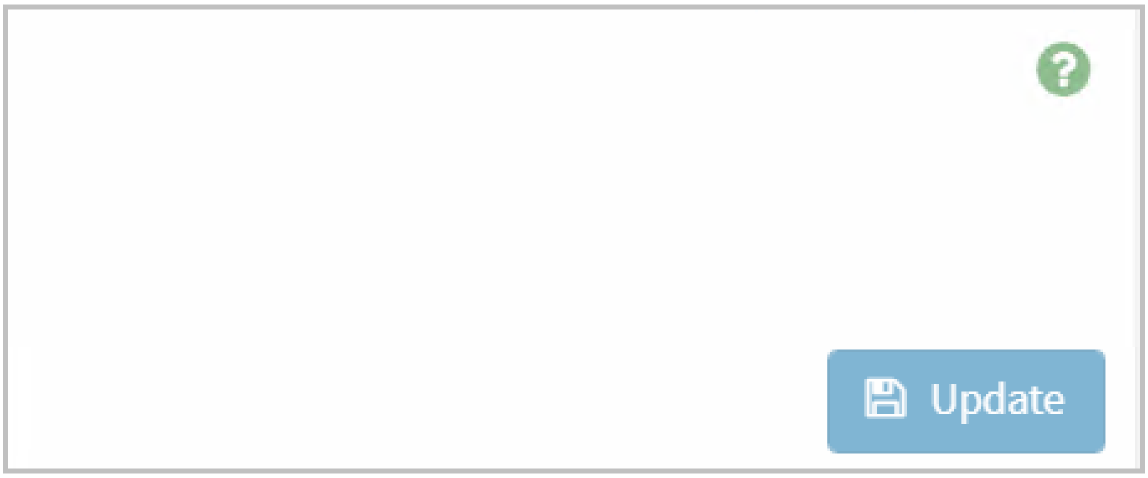
Abstract

If there are changes on the hardware configuration on a server, such as unplugging and plugging the Riser card, changing the NVMe wiring, the PCIe slot topology information assigned by the BMC changes accordingly. Once the PCIe topology changes, the BMC Web portal will report the **30840** alarm, at which point the PCIe topology needs to be updated.

Steps

1. From the menu bar in the left pane, select **Maintenance**. The **Maintenance** page is displayed.
2. Click **PCIe Topology Update**. The **PCIe Topology Update** page is displayed, see Figure 3-99.

Figure 3-99 PCIe Topology Update Page



3. Click **Update**.

3.15 Fault Diagnosis Management

3.15.1 Triggering an NMI

Abstract

When the server is faulty, you can try to trigger an NMI by using the **NMI Control** function and then perform fault diagnosis.

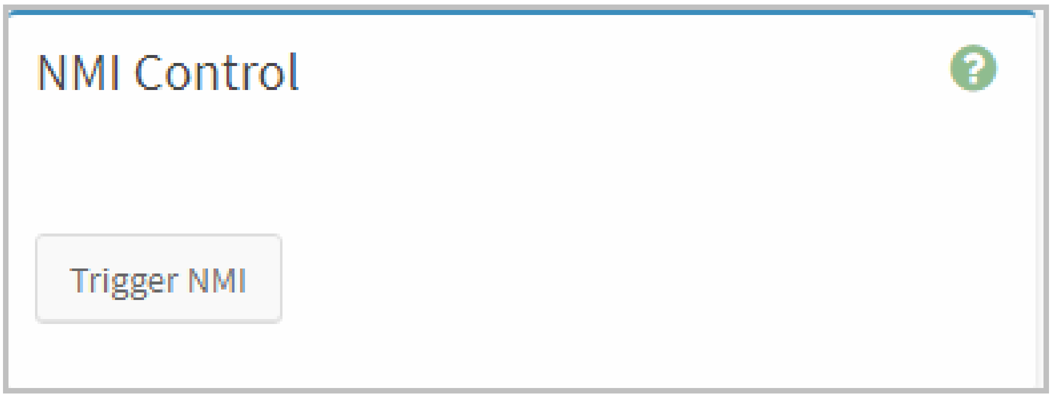
Note

The **NMI Control** function is used when the server operating system cannot be used. This function is disabled when a server is operating properly.

Steps

1. From the menu bar in the left pane, select **Fault Diagnose > NMI Control**. The **NMI Control** page is displayed, see Figure 3-100.

Figure 3-100 NMI Control Page



2. Click **Trigger NMI**.

3.15.2 Enabling Auto-Capture

Abstract

This procedure describes how to enable the last-screen capture function for the server for fault diagnosis.

Screenshots are captured automatically when the following conditions are met:

- The server restarts after a fatal error (for example, a CPU fault) occurs.
- The BMC triggers **Hard Reset**.
- The BMC triggers **Power Cycle**.
- The BMC triggers **Power Off**.

For a description of the power supply-related operations triggered by the BMC, refer to "3.9 Controlling the Server Power Supply".

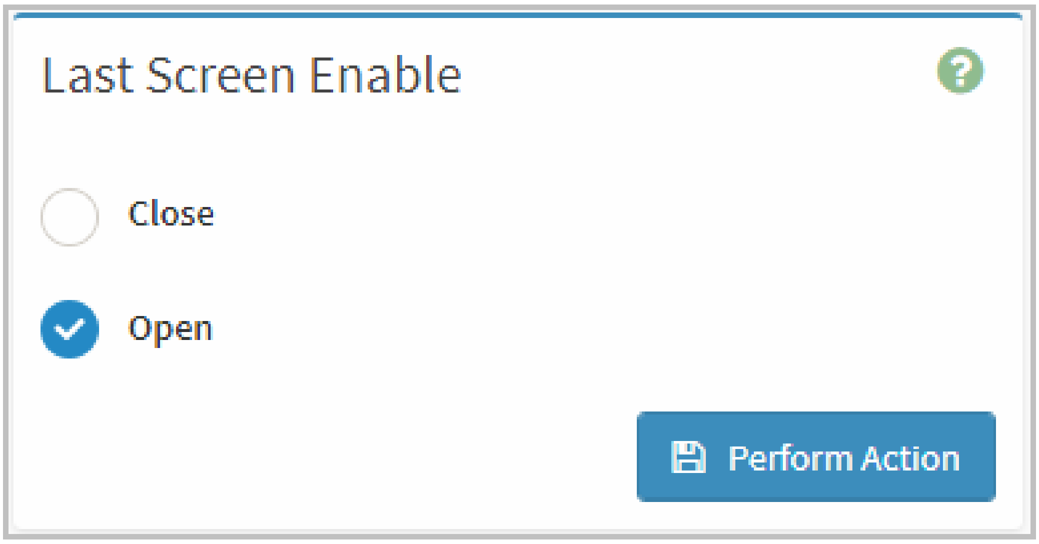
Note

If the KVM operates, the auto-capture function becomes invalid. Therefore, you must disable the KVM before using this function.

Steps

1. From the menu bar in the left pane, select **Fault Diagnose > Screenshots**. The **Screen Captured** page is displayed, see Figure 3-101.

Figure 3-101 Screen Captured Page



Last Screen Enable

○ Close

● Open

2. Select whether to enable the automatic last-screen capture function.
   - Close: Not captured automatically.

- Open: When the triggering conditions are met, the last screen of the server is automatically captured and displayed in the lower part of the page.

3. Click **Perform Action**.

3.15.3 Manually Capturing Screenshots

Abstract

This procedure describes how to capture the current screen of the server for fault diagnosis.

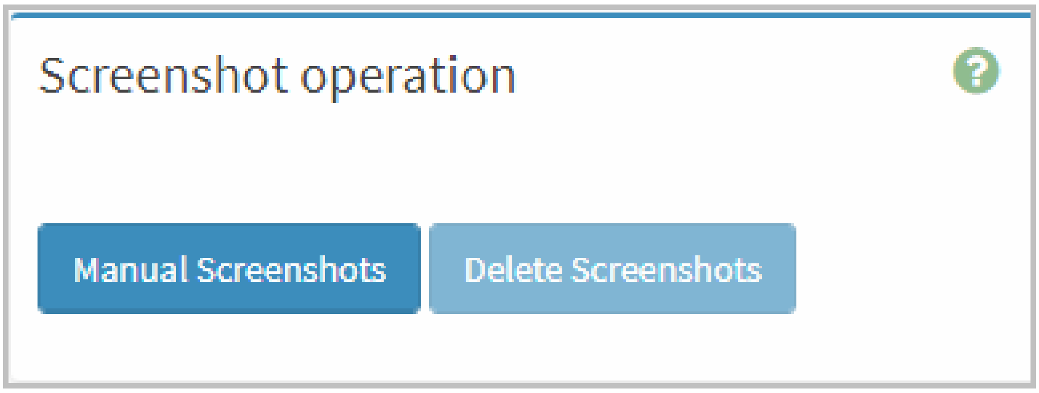
Note

If the KVM operates, the manual screenshot capture function becomes invalid. Therefore, you must disable the KVM before using this function.

Steps

1. From the menu bar in the left pane, select **Fault Diagnose > Manual Screenshots**. The **Manual Screenshots** page is displayed, see Figure 3-102.

Figure 3-102 Manual Screenshots Page



2. Perform the following operations as required.

To...	Do...
Capture a screenshot of the current screen	Click **Manual Screenshots**. The screenshot of the current screen is displayed in the lower part of the page.
Delete a captured screenshot	Click **Delete Screenshots**.

3.15.4 Querying POST Codes

Abstract

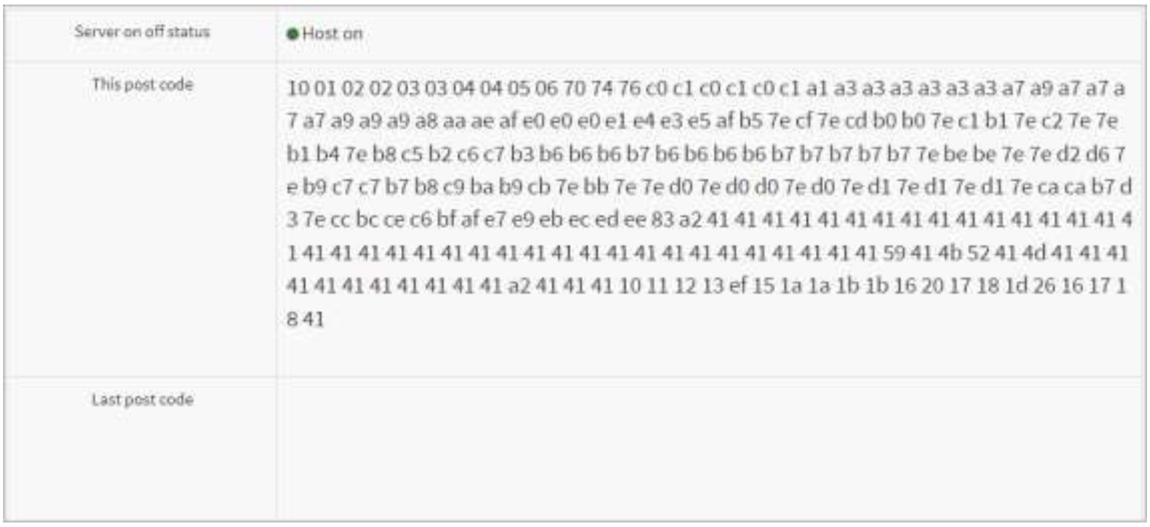
POST codes record the status of the server during power-on.

This procedure describes how to check POST codes for fault diagnosis.

Steps

1. From the menu bar in the left pane, select **Fault Diagnose > PostCode**. The **System post code** page is displayed, as shown in Figure 3-103.

Figure 3-103 System post code Page



Server on off status: ● Host on

This post code:

```
10 01 02 02 03 03 04 04 05 06 70 74 76 c0 c1 c0 c1 c0 c1 a1 a3 a3 a3 a3 a3 a3 a7 a9 a7 a7 a
7 a7 a9 a9 a9 a8 aa ae af e0 e0 e0 e1 e4 e3 e5 af b5 7e cf 7e cd b0 b0 7e c1 b1 7e c2 7e 7e
b1 b4 7e b8 c5 b2 c6 c7 b3 b6 b6 b6 b7 b6 b6 b6 b6 b7 b7 b7 b7 b7 7e be be 7e 7e d2 d6 7
e b9 c7 c7 b7 b8 c9 ba b9 cb 7e bb 7e 7e d0 7e d0 d0 7e d0 7e d1 7e d1 7e d1 7e ca ca b7 d
3 7e cc bc ce c6 bf af e7 e9 eb ec ed ee 83 a2 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 4
1 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 59 41 4b 52 41 4d 41 41 41
41 41 41 41 41 41 41 41 a2 41 41 41 10 11 12 13 ef 15 1a 1a 1b 1b 16 20 17 18 1d 26 16 17 1
8 41
```

Last post code:

2. Check **Server on off status**, **This post code**, and **Last post code**.

3.15.5 Downloading Host Logs

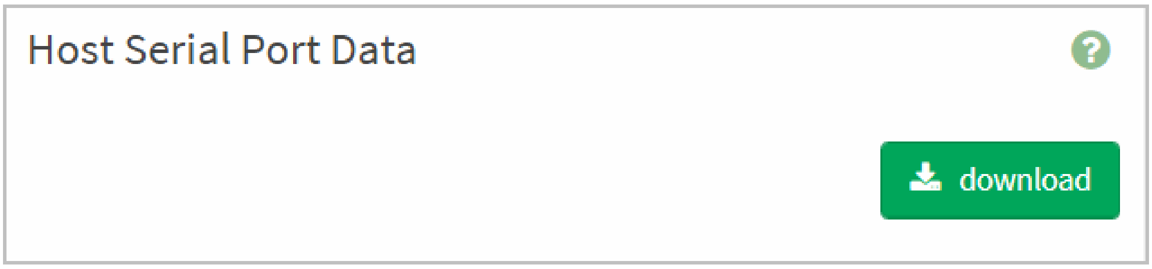
Abstract

If there is a fault, the serial port prints host logs. You can download these logs for troubleshooting.

Steps

1. From the menu bar in the left pane, select **Fault Diagnose > Host Log**. The **Host Log** page is displayed, see Figure 3-104.

Figure 3-104 Host Log Page



2. Click **download**.

Chapter 4
Common Operations

Table of Contents

4.1 Logging In to the BMC Management Backend in SSH Mode

Abstract

You can log in to the BMC management backend in SSH mode to configure the BMC.

Prerequisite

The client PC is installed with the SSH software, for example, *PuTTY*.

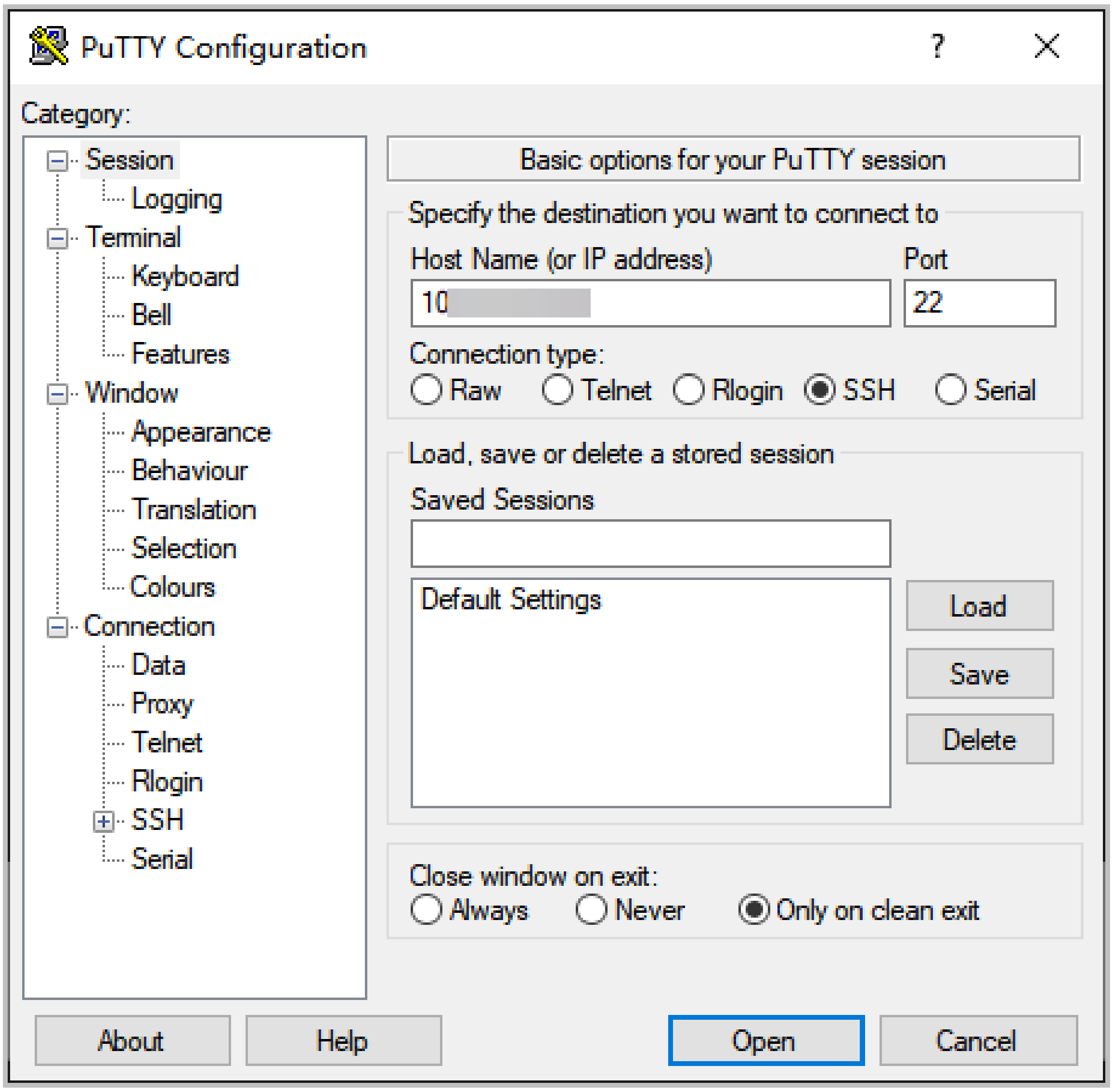
Note

The operations for different SSH software are similar. This procedure describes how to configure the *PuTTY* software.

Steps

1. On the client PC, open the *PuTTY* software. The **PuTTY Configuration** dialog box is displayed, see Figure 4-1.

Figure 4-1 PuTTY Configuration Dialog Box



PuTTY Configuration ? ×

Category:

- Session
  - Logging
- Terminal
  - Keyboard
  - Bell
  - Features
- Window
  - Appearance
  - Behaviour
  - Translation
  - Selection
  - Colours
- Connection
  - Data
  - Proxy
  - Telnet
  - Rlogin
  - SSH
  - Serial

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10[redacted]

Port: 22

Connection type:
○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Load Save Delete

Close window on exit:
○ Always ○ Never ● Only on clean exit

About Help Open Cancel

2. Configure the parameters. For a description of the parameters, refer to Table 4-1.

Table 4-1 PuTTY Configuration Parameter Descriptions

Parameter	Description	Setting
Category	Operation type.	Select **Session**.
Host Name (or IP address)	Host name or IP address.	Enter the IP address of the iSAC management network port or shared network port.
Port	Port number.	Enter *22*.
Connection type	Connection type.	Select **SSH**.

3. Click **Open**. The command line window is displayed.
4. Enter the account and password of the administrator.

Note

The default administrator username is *sysadmin*. The default administrator password depends on server models and BMC versions. For details, refer to 5 Reference: Default Passwords.

5. Press **Enter** to log in to the management backend of the BMC.

4.2 Logging In to the BMC Management Backend Through the Serial Port

Abstract

When neither the iSAC management network port nor the shared network port can access the BMC, you can log in to the BMC management backend through the serial port to configure the BMC.

Prerequisite

- The client PC is installed with SSH software, for example, *PuTTY*.

Note

The operations for different SSH software are similar. This procedure describes how configure the *PuTTY* software.

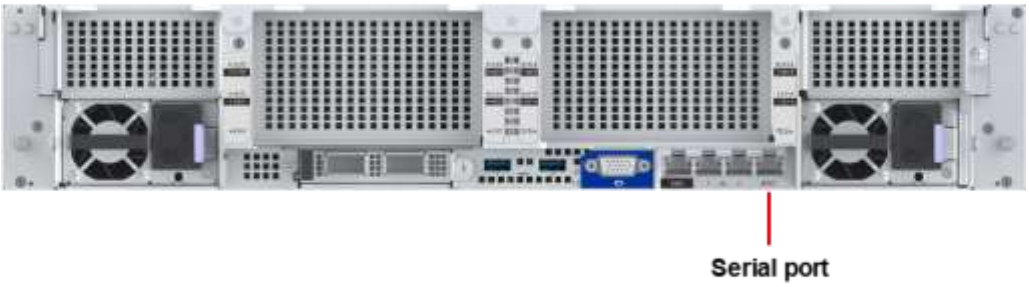
- If the client PC converts the serial port through the USB port, the driver for converting the serial port through the USB port must be installed.
- A serial cable is available.

Steps

1. Connect the client PC to the serial port on the rear panel of the server through a serial cable.

   For the position of the serial port on the rear panel, refer to Figure 4-2.

   Figure 4-2 Position of the Serial Port

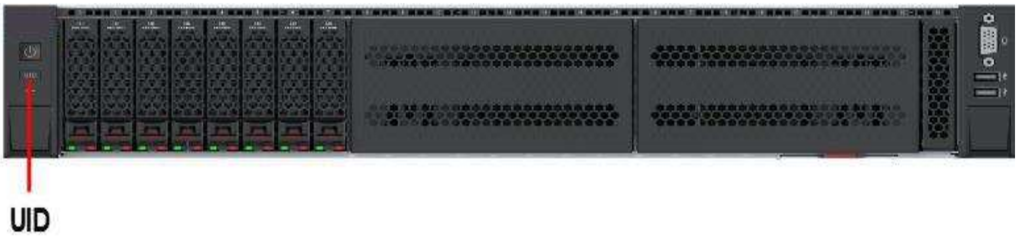
   Note

   The positions of the serial ports on the rear panels of servers are basically the same. This procedure uses the position of the serial port on the rear panel of an 2230-RE server as an example.

2. Press and hold the UID indicator on the front panel of the server for eight seconds. The serial port is switched to the BMC debugging serial port mode.

   For the position of the UID indicator on the front panel, see Figure 4-3.

   Figure 4-3 Position of the UID Indicator

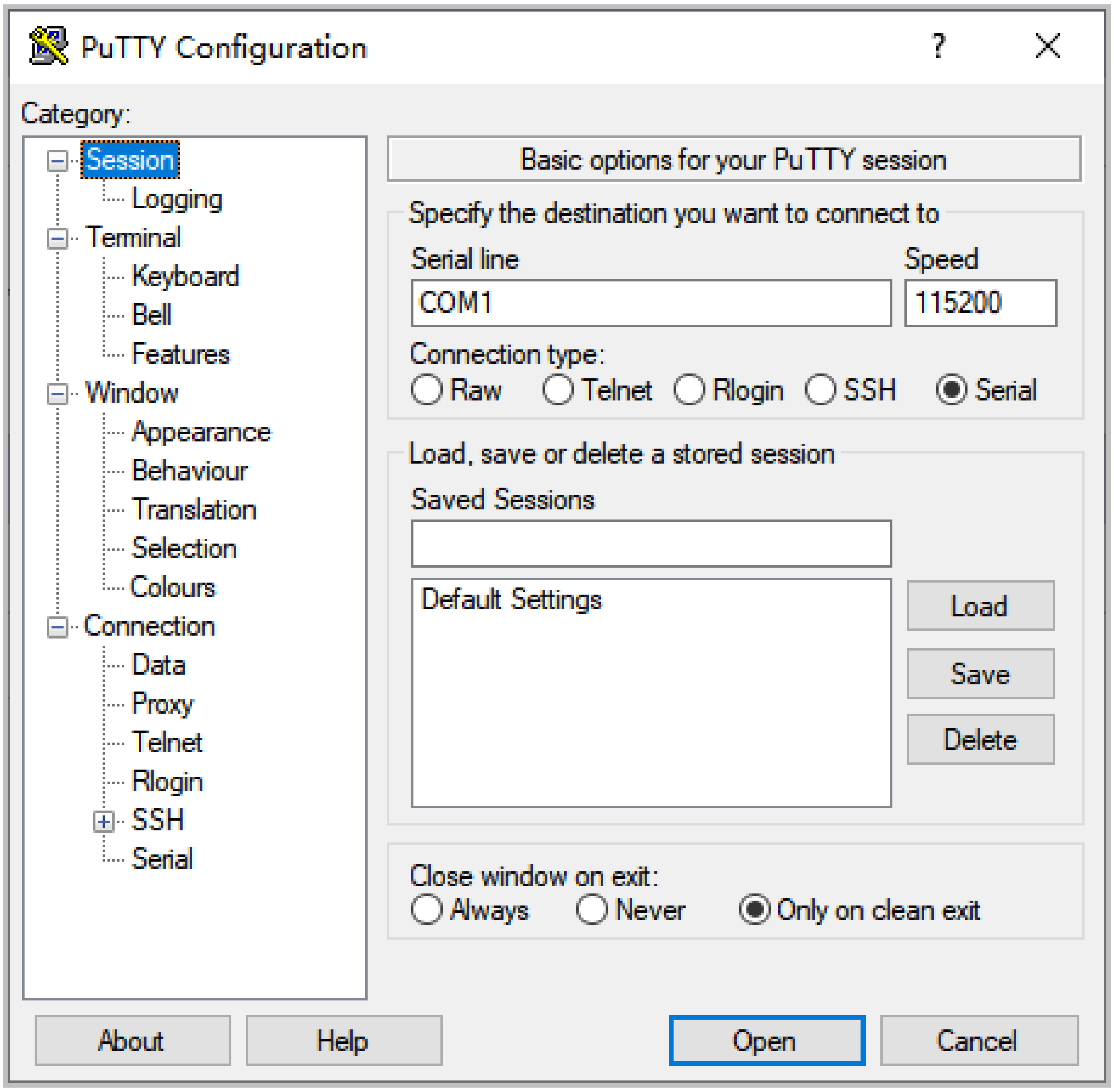
   

   Note

   The positions of the UID indicators on the front panels of servers are basically the same. This procedure uses the position of the UID indicator on the front panel of an 2230-RE server as an example.

3. On the **Device Manager** page on the client PC, query the serial port connected with the serial cable.
4. On the client PC, open the *PuTTY* software. The **PuTTY Configuration** dialog box is displayed, see Figure 4-4.

Figure 4-4 PuTTY Configuration Dialog Box



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Serial line: COM1

Speed: 115200

Connection type: ○ Raw ○ Telnet ○ Rlogin ○ SSH ● Serial

Load, save or delete a stored session

Saved Sessions

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

5. Configure the parameters. For a description of the parameters, refer to Table 4-2.

Table 4-2 PuTTY Configuration Parameter Descriptions

Parameter	Description	Setting
Category	Operation type.	Select **Session**.
Serial line	Serial port.	Enter the serial port queried in Step 3.
Speed	Speed.	Enter `115200`.
Connection type	Connection type.	Select **Serial**.

6. Click **Open**. The command line window is displayed.

7. Enter the account and password of the administrator.

Note

The default administrator username is `sysadmin`. The default administrator password depends on server models and BMC versions. For details, refer to 5 Reference: Default Passwords.

8. Press **Enter** to log in to the management backend of the BMC.

4.3 Logging In to the Web Portal of the BMC Through the Shared Network Port

Abstract

In addition to the iSAC management network port, you can also log in to the Web portal of the BMC through the shared network port.

Steps

1. Perform the following operations as required.

To...	Do...
Modify the network configuration of the shared network port through the Web portal of the BMC	a. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed. b. Click **Network Settings**. The **Network Settings** page is displayed. c. Click **Sideband Interface (NC-SI)**. The **Sideband Interface (NC-SI)** page is displayed. d. Configure the following parameters: ● **NCSI Mode**: Select **Manual Switch Mode**. ● **NCSI Interface**: Select **eth0**. e. Click **Save**. f. On the **Network Settings** page, click **Network IP Settings**. The **Network IP Settings** page is displayed. g. Configure the following parameters: ● **Enable LAN**: Select **Enable LAN**. ● **LAN Interface**: Select **eth0**. ● Select **Enable IPv4**, and configure **IPv4 Address**, **IPv4 Subnet** and **IPv4 Gateway**. h. Click **Save**.
Modify the network configuration of the shared network port through BIOS	a. In the BIOS window, select **iSAC > BMC Network Configuration**. The **BMC Network Configuration** window is displayed. b. Configure the gateway-related parameters in the **NIC (Shared)** area. c. Press **F4** to save the configuration and exit.

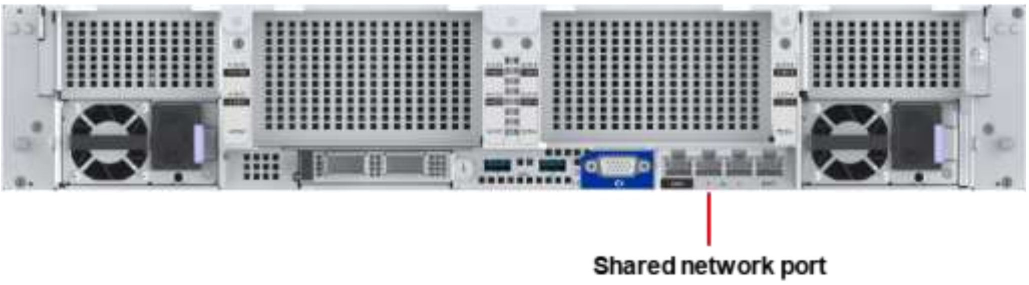
2. Connect the shared network port to the client PC through a network cable.

Note

The shared network port can be connected to the client PC directly through a network cable or a network device.

In most cases, the onboard service port marked as **1** is the shared port. For the position of the shared port on the rear panel, see Figure 4-5.

Figure 4-5 Position of the Shared Port



Note

The positions of the shared ports on the rear panels of servers are basically the same. This procedure uses the position of the shared port on the rear panel of an 2230-RE server as an example.

3. Log in to the Web portal of the BMC on the client PC.

   For details, refer to "3.1 Logging In to the Web Portal of the BMC".

4.4 Modifying the BMC Address

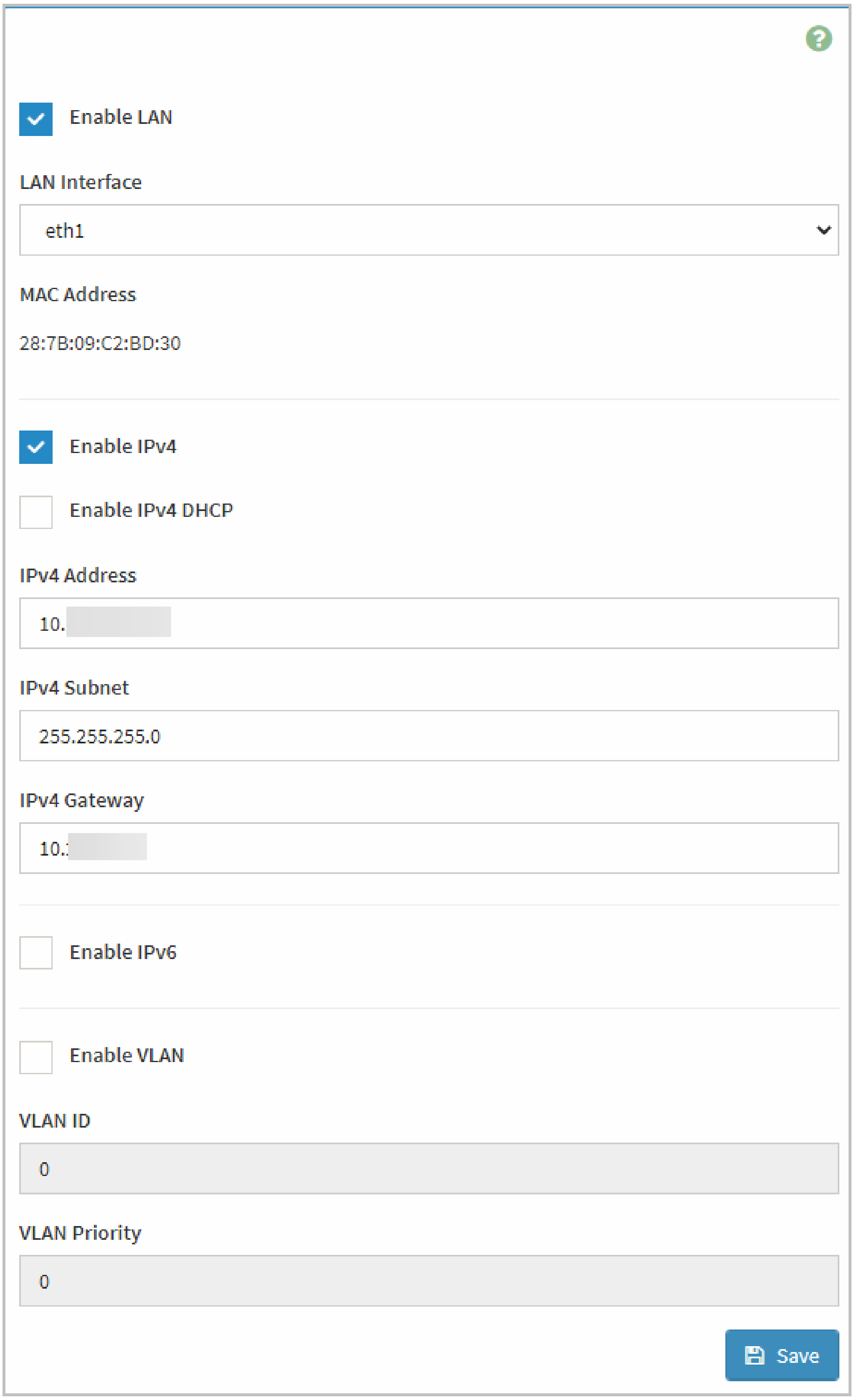
Abstract

To re-plan the BMC address of the server, you must modify the IP address, subnet mask and default gateway of the iSAC management network port or shared network port.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Network Settings**. The **Network Settings** page is displayed.
3. Click **Network IP Settings**. The **Network IP Settings** page is displayed, see Figure 4-6.

Figure 4-6 Network IP Settings Page



☑ Enable LAN

LAN Interface

eth1

MAC Address

28:7B:09:C2:BD:30

☑ Enable IPv4

☐ Enable IPv4 DHCP

IPv4 Address

10.[redacted]

IPv4 Subnet

255.255.255.0

IPv4 Gateway

10.[redacted]

☐ Enable IPv6

☐ Enable VLAN

VLAN ID

0

VLAN Priority

0

4. Configure the parameters. For a description of the parameters, refer to Table 4-3.

Table 4-3 Parameter Descriptions for the Network IP Address Configuration

Parameter	Description	Setting
Enable LAN	Whether to enable the network port. The network port is selected from the **LAN Interface** list.	Select **Enable LAN**. The network port is enabled.
LAN Interface	Current network port.	● To configure the management network port, select **eth1**. ● To configure the shared network port, select **eth0**.
MAC Address	MAC address of the corresponding network port.	This parameter is displayed only and cannot be configured.
Enable IPv4	Whether the network port enables the IPv4 protocol.	● Select **Enable IPv4**. The IPv4 protocol is enabled. ● Clear **Enable IPv4**. The IPv4 protocol is disabled. The IPv4-related parameters can be configured only after **Enable IPv4** is selected. ● To automatically obtain the IP address, select **IPv4 DHCP**. ● To manually configure the IP address, deselect **IPv4 DHCP**, and manually configure **IPv4 Address**, **IPv4 Subnet** and **IPv4 Gateway**.
Enable IPv6	Whether the network port enables the IPv6 protocol.	● Select **Enable IPv6**. The IPv6 protocol is enabled. ● Clear **Enable IPv6**. The IPv6 protocol is disabled. The IPv6-related parameters can be configured only after **Enable IPv6** is selected. ● To automatically obtain the IP address, select **IPv6 DHCP**. ● To manually configure the IP address, deselect **IPv6 DHCP**, and manually configure **IPv6 Index**, **IPv6 Address**, **Subnet Prefix Length** and **IPv6 Gateway**.
Enable VLAN	Whether the network port enables VLAN.	● Select **Enable VLAN**. The network port can be added into a VLAN. ● Clear **Enable VLAN**. The network port cannot be added into a VLAN. The VLAN-related parameters can be configured only after **Enable VLAN** is selected.

Parameter	Description	Setting
		● **VLAN ID**: 1–4094. ● **VLAN Priority**: 0–7, with 7 of the highest priority.

5. Click **Save**.

4.5 Querying Server Information

Abstract

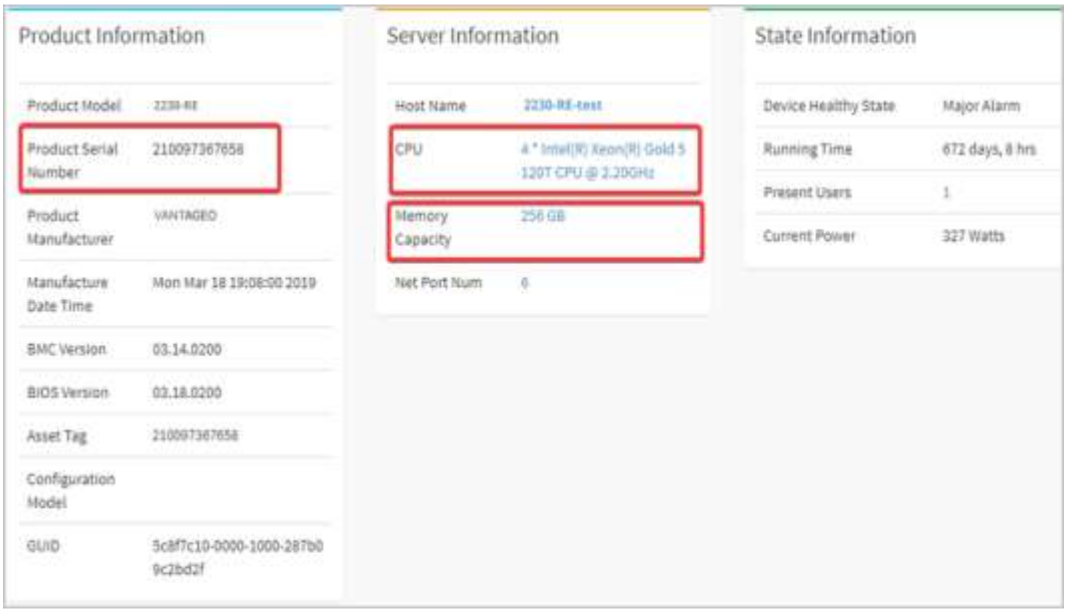
Before reporting a fault or replace the corresponding hardware, a user must query the server information, including:

- Serial No.
- CPU
- Memory
- NIC

Steps

1. From the menu bar in the left pane, select **Overview**. The **Overview** page is displayed, see Figure 4-7.

Figure 4-7 Overview Page



Product Information

Product Model 2230-RE
Product Serial Number 210097367658
Product Manufacturer VANTAGEO
Manufacture Date Time Mon Mar 18 19:08:00 2019
BMC Version 03.14.0200
BIOS Version 03.18.0200
Asset Tag 210097367658
Configuration Model
GUID 5c8f7c10-0000-1000-287b09c2bd2f

Server Information

Host Name 2230-RE-test
CPU 4 * Intel(R) Xeon(R) Gold 5120T CPU @ 2.20GHz
Memory Capacity 256 GB
Net Port Num 6

State Information

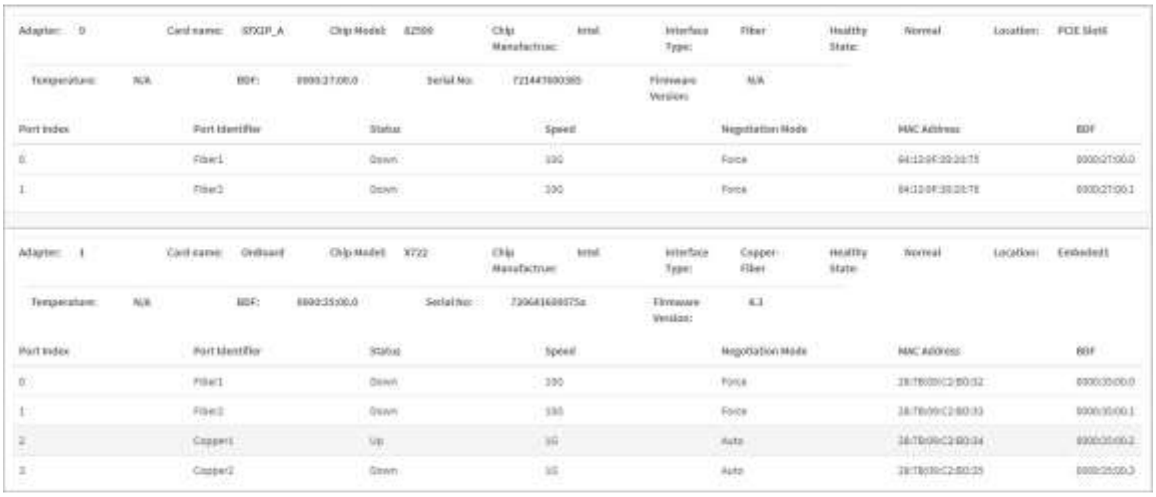
Device Healthy State Major Alarm
Running Time 672 days, 8 hrs
Present Users 1
Current Power 327 Watts

Note

On the **Overview** page, you can view **Product Serial Number**, **CPU** and **Memory Capacity**.

2. From the menu bar in the left pane, select **Network Device > NIC Information**. The **NIC** page is displayed, see Figure 4-8.

Figure 4-8 NIC Page



Adapter:	0	Card name:	SFXIP_A	Chip Model:	82599	Chip Manufacturer:	Intel	Interface Type:	Fiber	Healthy State:	Normal
Location:	PCIE Slot6										
Temperature:	N/A	BDF:	0000:27:00.0	Serial No:	721447000385	Firmware Version:	N/A				

Port Index	Port Identifier	Status	Speed	Negotiation Mode	MAC Address	BDF
0	Fiber1	Down	10G	Force	64:12:9F:39:20:75	0000:27:00.0
1	Fiber2	Down	10G	Force	64:12:9F:39:20:78	0000:27:00.1

Adapter:	1	Card name:	Onboard	Chip Model:	X722	Chip Manufacturer:	Intel	Interface Type:	Copper-Fiber	Healthy State:	Normal
Location:	Embedded1										
Temperature:	N/A	BDF:	0000:35:00.0	Serial No:	720641600075a	Firmware Version:	4.3				

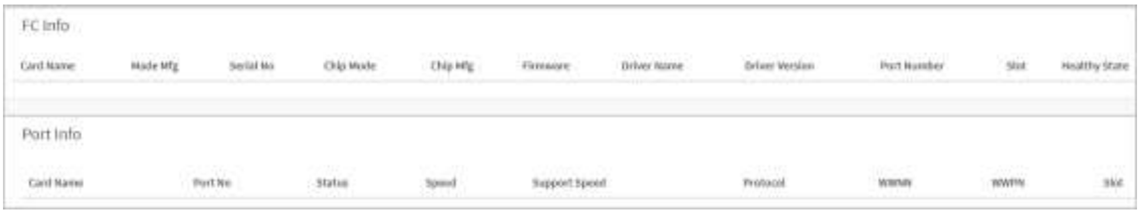
Port Index	Port Identifier	Status	Speed	Negotiation Mode	MAC Address	BDF
0	Fiber1	Down	10G	Force	28:7B:09:C2:B0:32	0000:35:00.0
1	Fiber2	Down	10G	Force	28:7B:09:C2:B0:33	0000:35:00.1
2	Copper1	Up	1G	Auto	28:7B:09:C2:B0:34	0000:35:00.2
3	Copper2	Down	1G	Auto	28:7B:09:C2:B0:35	0000:35:00.3

Note

On the **NIC** page, you can view the Ethernet NIC information.

3. From the menu bar in the left pane, select **Network Device > FC Information**. The **FC** page is displayed, see Figure 4-9.

Figure 4-9 FC Page



FC Info

Card Name	Made Mfg	Serial No	Chip Mode	Chip Mfg	Firmware	Driver Name	Driver Version	Port Number	Slot	Healthy State

Port Info

Card Name	Port No	Status	Speed	Support Speed	Protocol	WWNN	WWPN	Slot

Note

On the **FC** page, you can view the FC NIC information.

4.6 Managing RAIDs

Abstract

You can perform the following common operations to manage RAIDs:

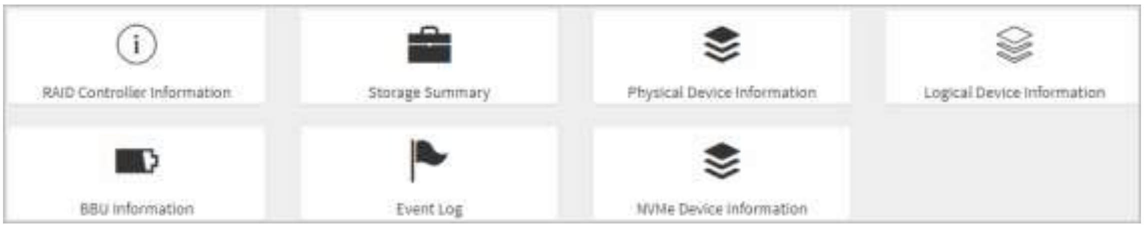
- Querying the RAID controller information
- Querying the physical device information

- Creating a RAID
- Setting a RAID as the boot disk

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **RAID Management**. The **RAID Management** page is displayed, see Figure 4-10.

Figure 4-10 RAID Management Page

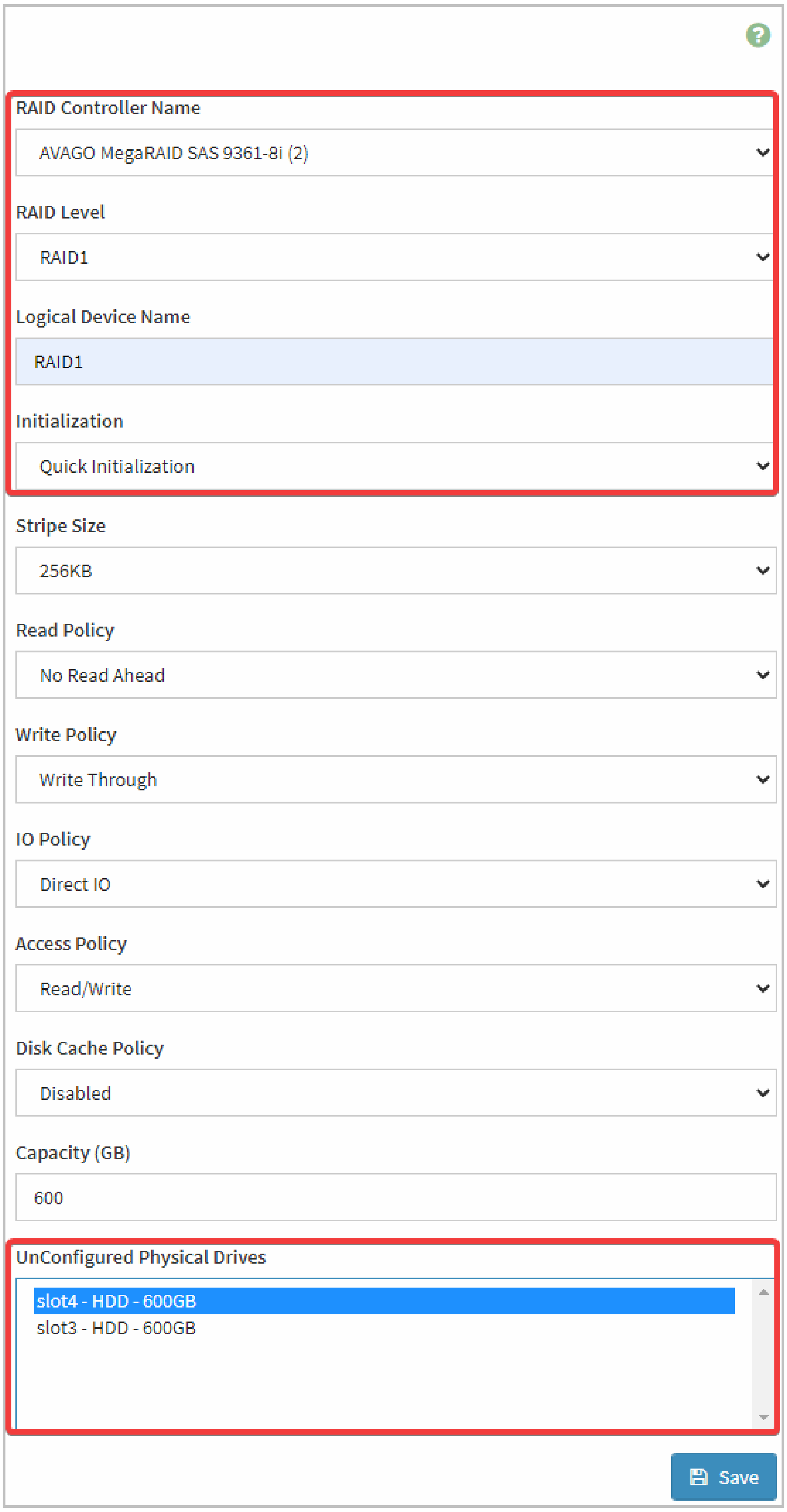

RAID Controller Information
Storage Summary
Physical Device Information
Logical Device Information
BBU Information
Event Log
NVMe Device Information

3. Perform the following operations as required.

To...	Do...
Query the RAID controller information	a. Click **RAID Controller Information**. The **RAID Controller Information** page is displayed. b. From the **Select the RAID Controller** list, select the RAID controller you want to query. The information about the selected RAID controller is displayed in the lower part of the page. c. (Optional) In the **RAID Event Log Statistics** area, click **Details**. The **Event Log** page is displayed, where you can view the event logs of the RAID controller.
Query the physical device information	a. Click **Physical Device Information**. The **Physical Device Information** page is displayed. b. From the **Select the RAID Controller** list, select the RAID controller you want to query. The information about all the physical disks managed by the selected RAID controller is displayed in the lower part of the page. The **State** information in the physical disk information is described as follows: ● Online: The member disk of the logical disk is online. ● Missing: The member disk of the logical disk is removed. ● Offline: The member disk of the logical disk is offline. ● Rebuild: Rebuild. The hard disk is rebuilding data to ensure data redundancy and integrity of the logical disk. ● Shield State: Protected. Temporary status of the diagnosis operation. ● Hotspare: Hot spare disk. ● Copyback: Copyback. A new disk is replacing a faulty member disk.

To...	Do...
	● Bootable: Boot disk. ● Unconfigured_good: Not configured, and the hard disk is available. ● Unconfigured_bad: Not configured, and the hard disk is not available. ● PredictiveFailure: Failure. The hard disk is unavailable. ● ExposedToOS: Pass-through disk. This state is displayed when the RAID controller card is set to pass-through mode or set to mixed mode but no RAID controller card is created. c. (Optional) Click ⊞ on the right of the physical hard disk. More actions are displayed.
Create a RAID	a. Click **Logical Device Information**. The **Logical Device Information** page is displayed. b. From the **Select the RAID Controller** list, select the controller to which the RAID to be created belongs. c. Click **Create Virtual Device**. The **Create Virtual Device** page is displayed, see Figure 4-11. d. Configure the following key parameters: ● RAID Controller Name: Select the controller to which the RAID to be created belongs. ● RAID Level: Select the corresponding RAID level. ● Logical Device Name: Enter the RAID name. ● Initialization: Select **Quick Initialization**. ● UnConfigured Physical Drives: Select the disk required to create a RAID. The other parameters are set to the default values. e. Click **Save**.
Set a RAID as the boot disk	a. Click **Logical Device Information**. The **Logical Device Information** page is displayed. b. From the **Select the RAID Controller** list, select the controller that the RAID belongs to. c. Click ⊞ for the RAID that you want to set as the boot disk. d. Click ✓.

Figure 4-11 Create Virtual Device Page



RAID Controller Name

AVAGO MegaRAID SAS 9361-8i (2)

RAID Level

RAID1

Logical Device Name

RAID1

Initialization

Quick Initialization

Stripe Size

256KB

Read Policy

No Read Ahead

Write Policy

Write Through

IO Policy

Direct IO

Access Policy

Read/Write

Disk Cache Policy

Disabled

Capacity (GB)

600

UnConfigured Physical Drives

slot4 - HDD - 600GB

slot3 - HDD - 600GB

4.7 Installing the Operating System Remotely

Abstract

If the operating system cannot be installed on-site, you can install it remotely on the client PC.

The operations for remote OS installation include:

1. Disable media redirection configurations
2. Configure a boot mode
3. Install the operating system

Prerequisite

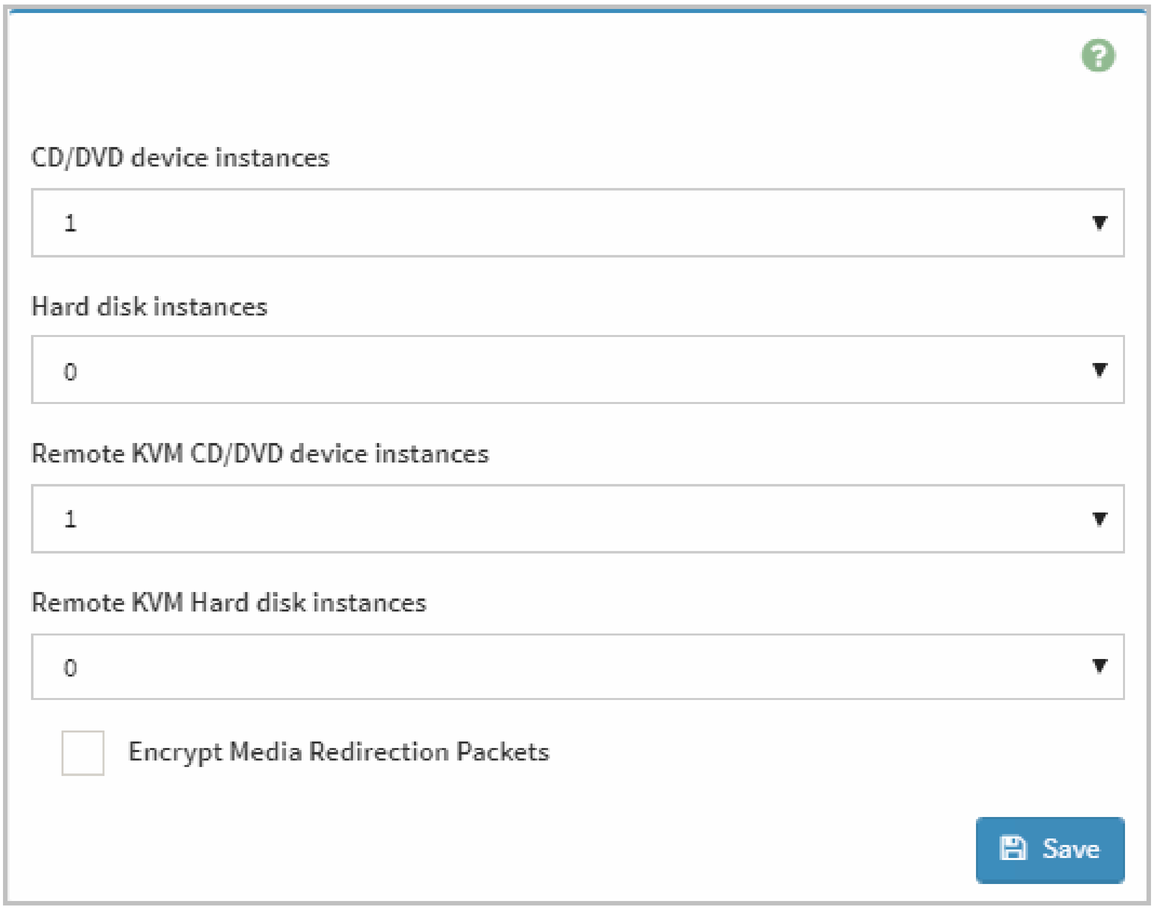
- The *ISO* image file of the operating system is obtained.
- The RAID configuration of the system disk of the server is completed.
- If the KVM is started in JAVA mode, the JRE is installed on the client PC, for example, *jre-8u191*.

Steps

Disabling Media Redirection Configurations

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Media Redirection Settings**. The **Media Redirection** page is displayed.
3. Click **VMedia Instance Settings**. The **VMedia Instance Settings** page is displayed, see Figure 4-12.

Figure 4-12 VMedia Instance Settings Page



CD/DVD device instances

1 ▼

Hard disk instances

0 ▼

Remote KVM CD/DVD device instances

1 ▼

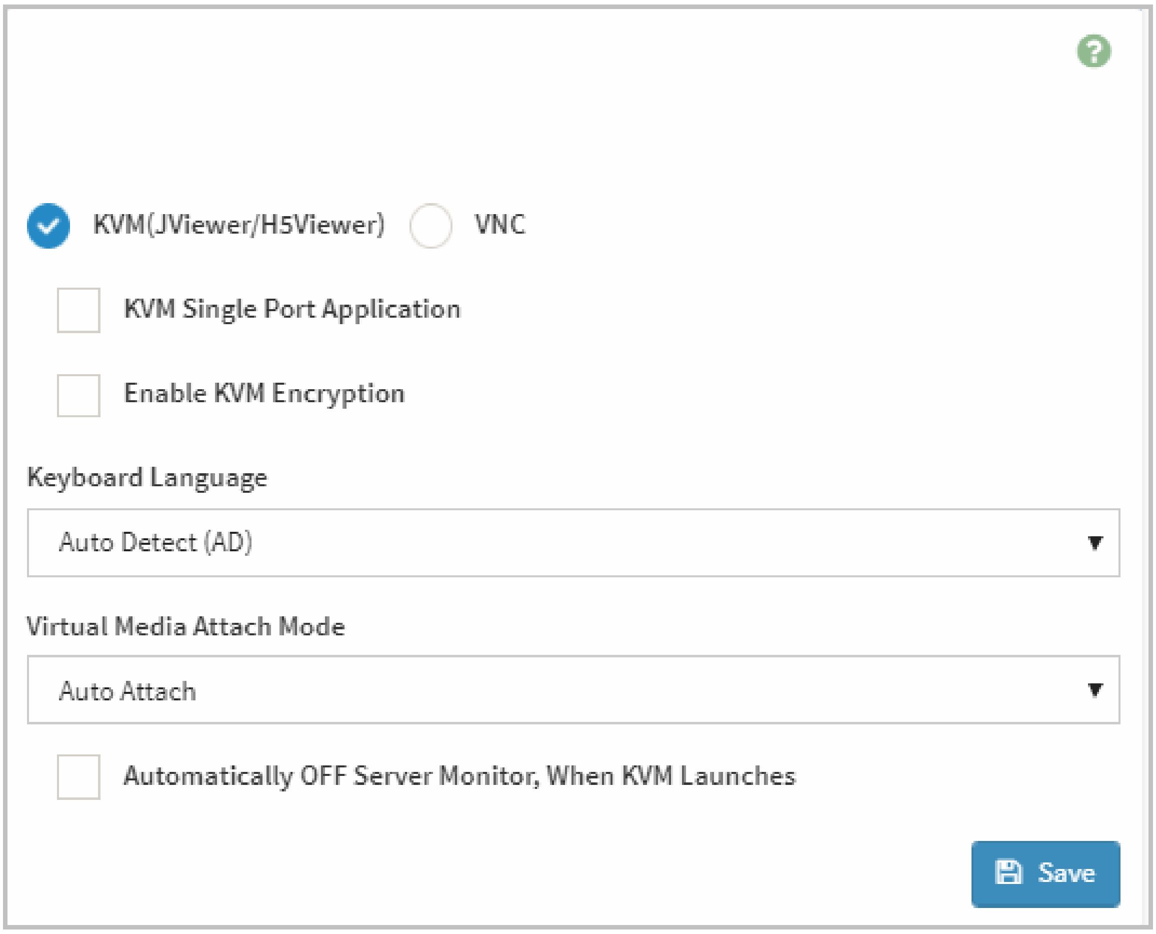
Remote KVM Hard disk instances

0 ▼

□ Encrypt Media Redirection Packets

4. Deselect **Encrypt Media Redirection Packets**.
5. Click **Save**.
6. On the **Media Redirection** page, click **Remote Session**. The **Remote Session** page is displayed, see Figure 4-13.

Figure 4-13 Remote Session Page



● KVM(JViewer/H5Viewer) ○ VNC

□ KVM Single Port Application

□ Enable KVM Encryption

Keyboard Language: Auto Detect (AD)

Virtual Media Attach Mode: Auto Attach

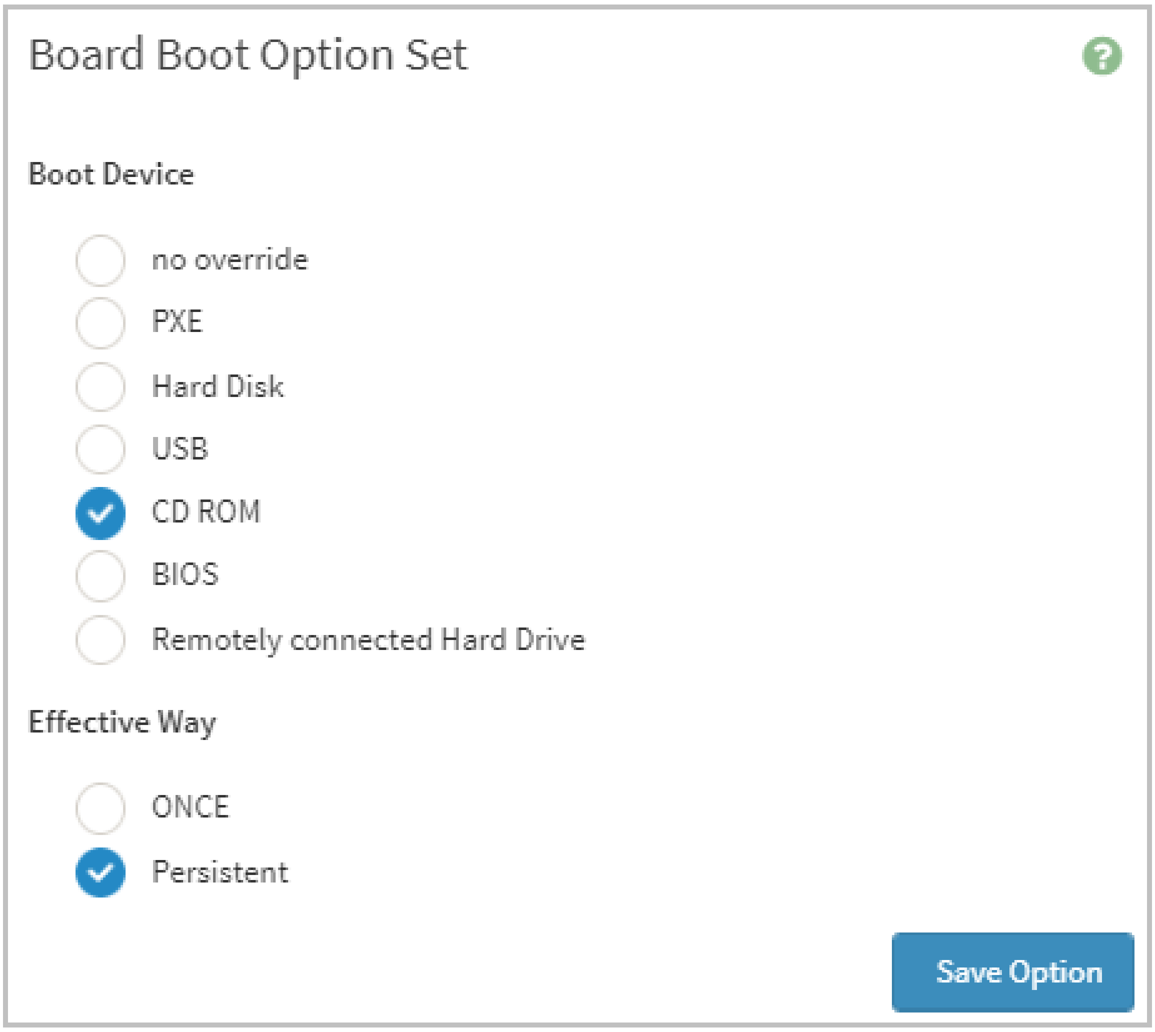
□ Automatically OFF Server Monitor, When KVM Launches

7. Deselect **Enable KVM Encryption**.
8. Click **Save**.

Configuring a Boot Mode

9. On the **Settings** page, click **Boot Option Settings**. The **Boot Option** page is displayed, see Figure 4-14.

Figure 4-14 Boot Option Page



Board Boot Option Set

Boot Device

○ no override
○ PXE
○ Hard Disk
○ USB
● CD ROM
○ BIOS
○ Remotely connected Hard Drive

Effective Way

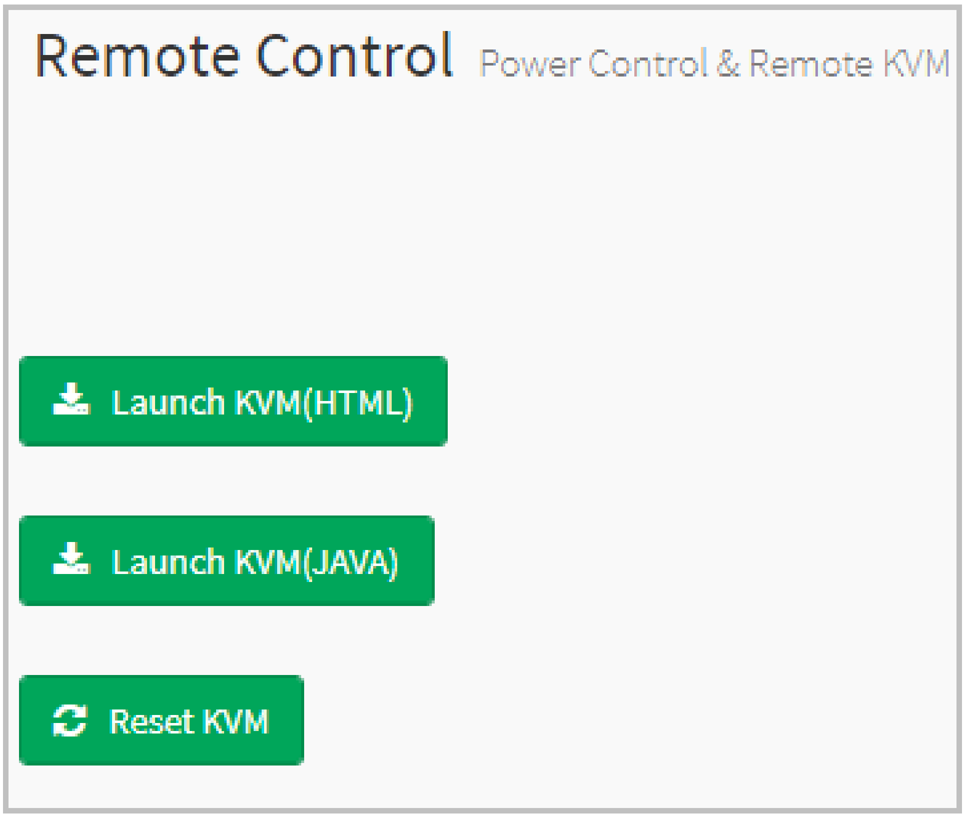
○ ONCE
● Persistent

10. Select **CD ROM** and **Persistent**.
11. Click **Save Option**.

Installing the Operating System

12. From the menu bar in the left pane, select **Remote Control**. The **Remote Control** page is displayed, see Figure 4-15.

Figure 4-15 Remote Control Page



13. Perform the following operations as required.

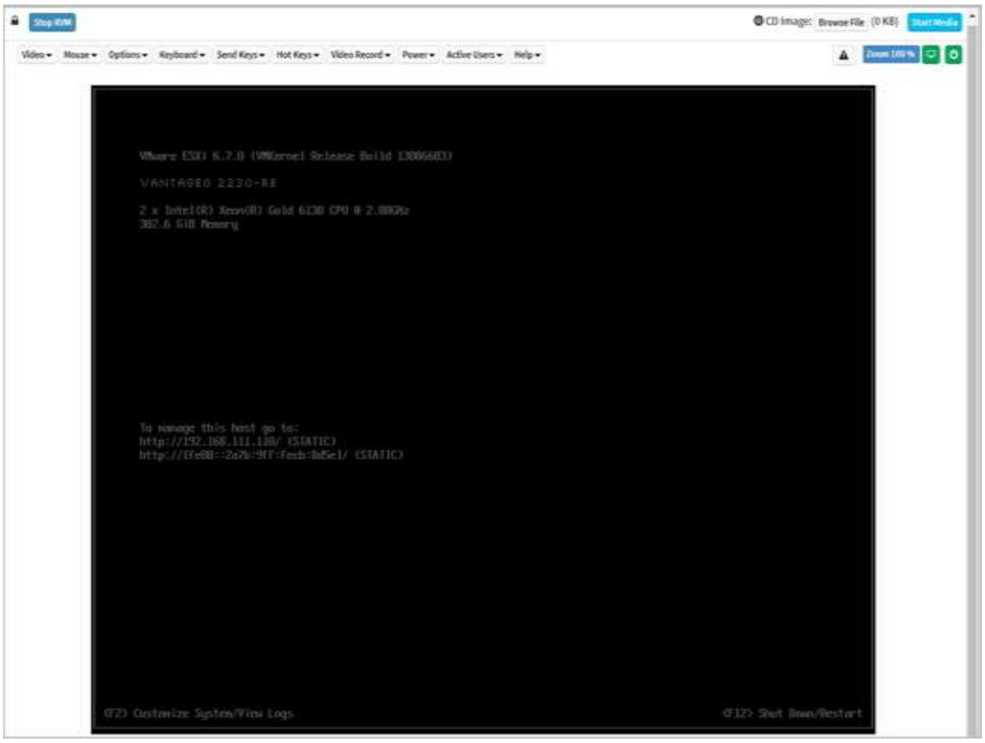
To...	Do...
Start the KVM in HTML mode	a. Click **Launch KVM (HTML)**. The **Remote KVM (HTML)** window is displayed, see Figure 4-16. b. Click **Browse File** on the right of **CD Image**, and select the `ISO` image file from the client PC. c. Click **Start Media** and load the `ISO` image file. d. Select **Power > Reset Server** and restart the server. The page for installing the operating system is displayed.
Start the KVM in JAVA mode	a. In the search box in the lower left corner of the client PC, enter `Java`. b. In the search result, select **Java**. The **Java Control Panel** dialog box is displayed. c. Click **Security**. The **Security** window is displayed. d. Click **Edit Site List**. The **Exception Site List** dialog box is displayed. e. Click **Add** to add the address of the BMC Web portal. f. Click **OK** to return to the **Security** window. g. Click **OK**. h. On the **Remote Control** page of the BMC Web portal, click **Launch KVM (JAVA)**. A dialog box indicating whether to keep `jviewer.jnlp` is displayed. i. Click **Keep**.

To...	Do...
	j. In the lower left corner of your browser, click `jviewer.jnlp`. A dialog box is displayed. k. Click **Continue**. The **Do you want to run this application?** dialog box is displayed. l. Select **I accept the risk and want to run this app.** and click **Run**. The **Untrusted Connection** dialog box is displayed. m. Click **Yes**. The **Remote KVM (JAVA)** page is displayed, see Figure 4-17. n. Select **Media > Virtual Media Wizard...**, and switch to the **CD/DVD** tab. o. Click **Browse** and select the *ISO* image file from the client PC. p. Click **Connect**. q. Select **Power > Reset Server** and restart the server. The page for installing the operating system is displayed.

Note

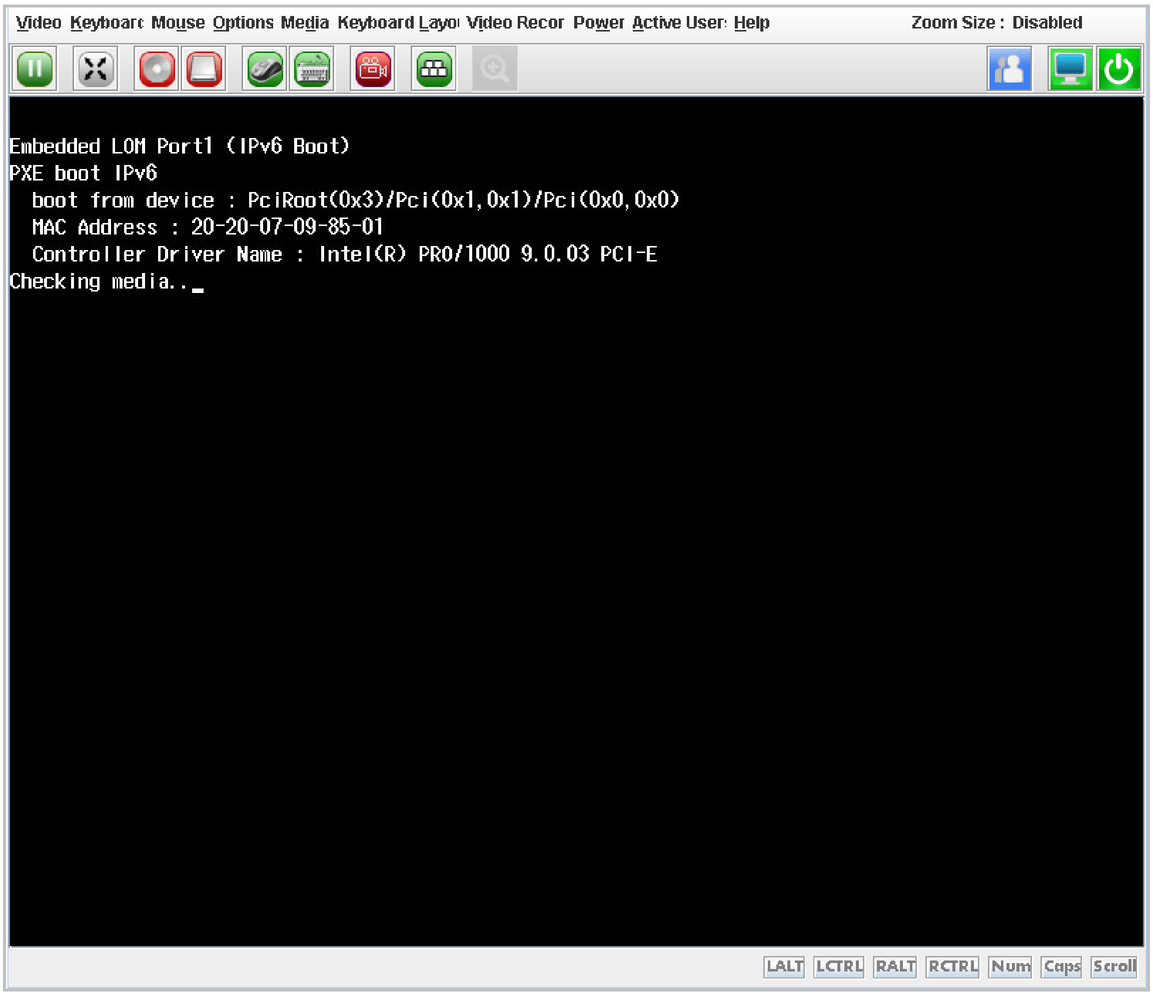
Before starting the KVM in one mode, you must disable the KVM in another mode. For example, before starting the KVM in JAVA mode, you must disable the KVM started in HTML mode.

Figure 4-16 Remote KVM (HTML) Window



```
VMware ESXi 6.7.0 (VMKernel Release Build 13006603)

VANTAGEO 2230-RE

2 x Intel(R) Xeon(R) Gold 6138 CPU @ 2.00GHz
382.6 GiB Memory


To manage this host go to:
http://192.168.111.139/ (STATIC)
http://[fe80::2a7b:9ff:fecb:9d5e]/ (STATIC)


<F2> Customize System/View Logs                    <F12> Shut Down/Restart
```

Figure 4-17 Remote KVM (JAVA) Window



Video Keyboarc Mouse Options Media Keyboard Layo Video Recor Power Active User Help
Zoom Size : Disabled
LALT LCTRL RALT RCTRL Num Caps Scroll

```
Embedded LOM Port1 (IPv6 Boot)
PXE boot IPv6
  boot from device : PciRoot(0x3)/Pci(0x1,0x1)/Pci(0x0,0x0)
  MAC Address : 20-20-07-09-85-01
  Controller Driver Name : Intel(R) PRO/1000 9.0.03 PCI-E
Checking media.._
```

4.8 Resetting the BMC

Abstract

If you cannot log in to the BMC Web portal, you must reset the BMC.

You can reset the BMC through one of the following ways:

- Reset the BMC by logging in to the server
- Reset the BMC by using a SSH tool (for example, PuTTY)
- Reset the BMC by using the ipmitool
- Reset the BMC by powering off the server

Prerequisite

- If the BMC is reset by using the ipmitool, the port number of the **ipmi** service is set to **623**.
- If the BMC is reset by using the ipmitool, the BMC address is successfully pinged with the ipmitool.

Steps

- Reset the BMC by logging in to the server
  1. Log in to the server as the `root` user.
  2. Run the following commands to reset the BMC:

     ```
     # modprobe ipmi_si
     # modprobe ipmi_devintf
     # ipmitool mc reset cold
     ```
- Reset the BMC by using a SSH tool
  1. Log in to the BMC management backend by using the SSH tool.

     Enter the following parameters for login:

     → Host Address: BMC address

     → Username: sysadmin

     → Password: refer to 5 Reference: Default Passwords

     → Port: 22
  2. Run the following command to reset the BMC:

     ```
     # reboot
     ```
- Reset the BMC by using the ipmitool
  1. In the ipmitool, run the following command to reset the BMC:

     → Warm boot: `ipmitool -I lan -H 10.43.211.200 -U root -P Superuser9! mc reset warm Sent warm reset command to MC`

     → Cold reboot: `ipmitool -I lan -H 10.43.211.200 -U root -P Superuser9! mc reset cold Sent cold reset command to MC`

     The parameters in the command are described as follows:

     → **10.43.211.200**: BMC address

     → **root**: username

     → **Superuser9!**: password
- Reset the BMC by powering off the server
  1. Power off the server without services.
  2. Power on the server.

4.9 Querying and Configuring a Temperature Policy

Abstract

A temperature policy refers to the policy of whether to shut down a server after the server temperature reaches a specified threshold.

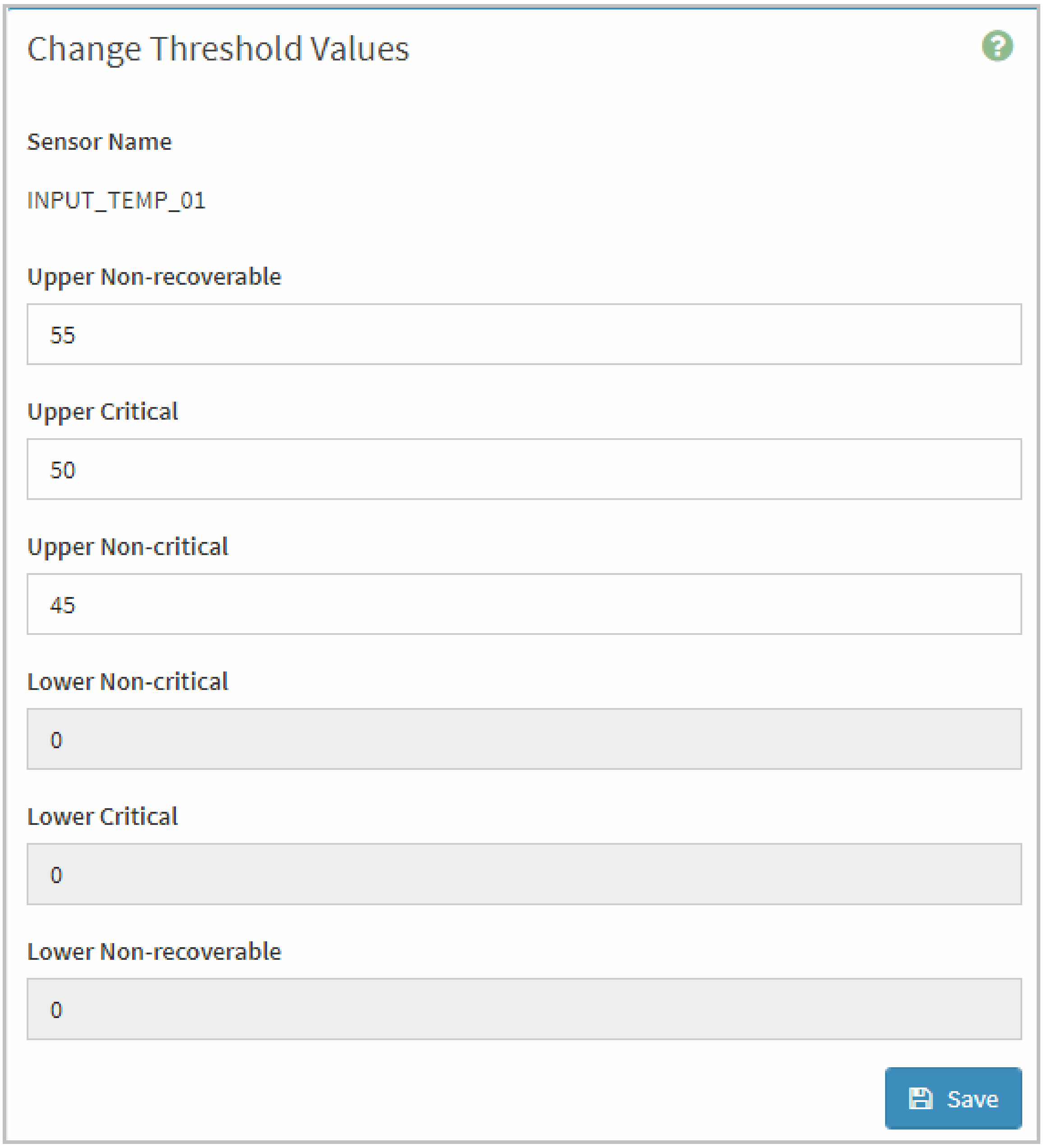
You can set the temperature thresholds on the BMC Web portal, and query and configure a temperature policy by using the ipmitool.

Steps

Setting Temperature Thresholds

1. From the menu bar in the left pane, select **Sensor**. The **Sensor Reading** page is displayed.
2. In the **Normal Sensors** area, click the sensor with the keyword **INPUT_TEMP** in its name. The **Sensor detail** page is displayed.
3. Click **Change Thresholds**. The **Sensor Thresholds** page is displayed, see Figure 4-18.

Figure 4-18 Sensor Thresholds Page



Change Threshold Values

Sensor Name

INPUT_TEMP_01

Upper Non-recoverable

55

Upper Critical

50

Upper Non-critical

45

Lower Non-critical

0

Lower Critical

0

Lower Non-recoverable

0

4. Configure the parameters. For a description of the parameters, refer to Table 4-4.

Table 4-4 Temperature Threshold Descriptions

Parameter	Description	Setting
Upper Non-recoverable	A fatal alarm is raised when the temperature reaches the threshold.	It is set to `55` by default.
Upper Critical	A critical alarm is raised when the temperature reaches the threshold.	It is set to `50` by default.
Upper Non-critical	A minor alarm is raised when the temperature reaches the threshold.	It is set to `45` by default.

Note

When the threshold specified in **Upper Critical** is reached, the server is shut down.

5. Click **Save**.

Querying and Configuring a Temperature Policy

6. In the ipmitool tool, run the following command to query the temperature policy:

```
ipmitool -I lan -H 10.43.211.200 -U root -P Superuser9! raw 0x2e 0xd6
0x3e 0x0f 0
```

The parameters in the command are described as follows:

- **10.43.211.200**: BMC address
- **root**: username
- **Superuser9!**: password

The values returned after the command is run are described as follows:

- **1**: indicates that the over-temperature shutdown policy is enabled.
- **0**: indicates that the over-temperature shutdown policy is disabled.

7. (Optional) To adjust the temperature policy, run the following command to configure the temperature policy:

```
ipmitool -I lan -H 10.43.211.200 -U root -P Superuser9! raw 0x2e 0xd6
0x3e 0x0f 0 1
```

The last byte in the command is described as follows:

- **1**: indicates that the over-temperature shutdown policy is enabled.
- **0**: indicates that the over-temperature shutdown policy is disabled.

4.10 Querying and Configuring Services

Abstract

By default, the BMC provides the following services:

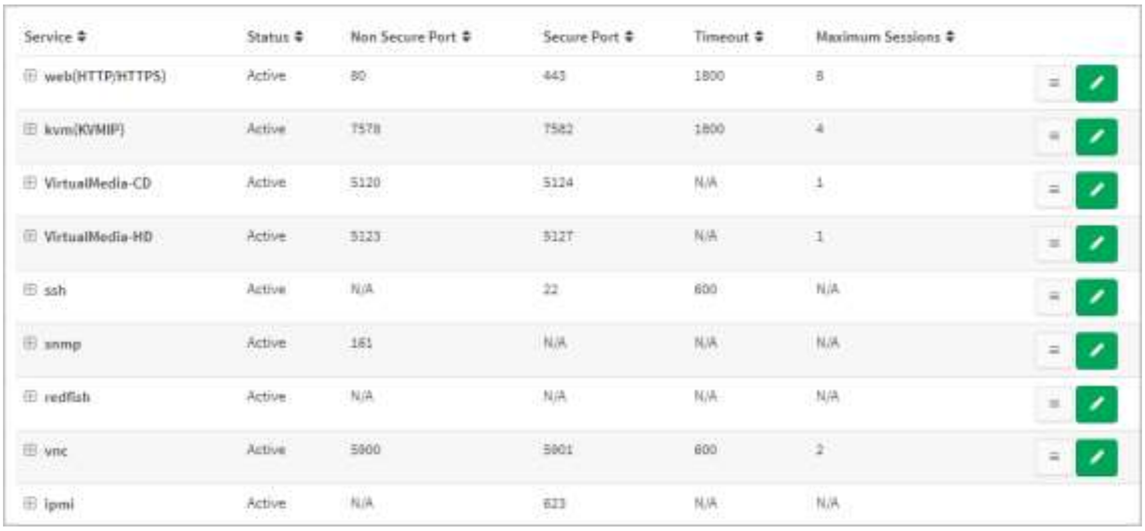
- **web**
- **kvm**
- **VirtualMedia-CD**
- **VirtualMedia-HD**
- **ssh**
- **snmp**
- **redfish**
- **vnc**
- **ipmi**

To query or modify the parameters of the services above, you can query and configure services.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Services**. The **Services** page is displayed, see Figure 4-19.

Figure 4-19 Services Page



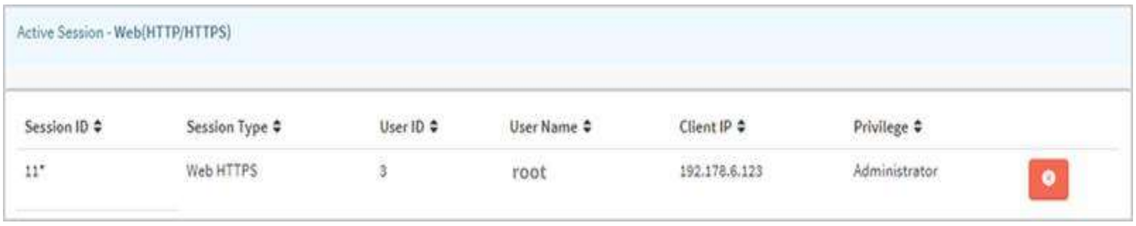
Service ⇕	Status ⇕	Non Secure Port ⇕	Secure Port ⇕	Timeout ⇕	Maximum Sessions ⇕
⊞ web(HTTP/HTTPS)	Active	80	443	1800	8
⊞ kvm(KVMIP)	Active	7578	7582	1800	4
⊞ VirtualMedia-CD	Active	5120	5124	N/A	1
⊞ VirtualMedia-HD	Active	5123	5127	N/A	1
⊞ ssh	Active	N/A	22	600	N/A
⊞ snmp	Active	161	N/A	N/A	N/A
⊞ redfish	Active	N/A	N/A	N/A	N/A
⊞ vnc	Active	5900	5901	600	2
⊞ ipmi	Active	N/A	623	N/A	N/A

3. Perform the following operations as required.

To...	Do...
View the active sessions of a service	a. Click ⊞ on the left of a service. The number of the active sessions is expanded under this service.

To...	Do...
	b. Click ≡ on the right of the service. The **Service Sessions** page is displayed, see Figure 4-20. On the **Service Sessions** page, you can view the detailed information of the active sessions. c. (Optional) To terminate a session, click ⊗ for the session.
Set parameters for a service	a. Click ✎ on the right of a service. The **Service Configuration** page is displayed, see Figure 4-21. This procedure uses the KVM service as an example. The operations for configuring other services are similar. b. Configure the parameters. For a description of the parameters, refer to Table 4-5. c. Click **Save**.

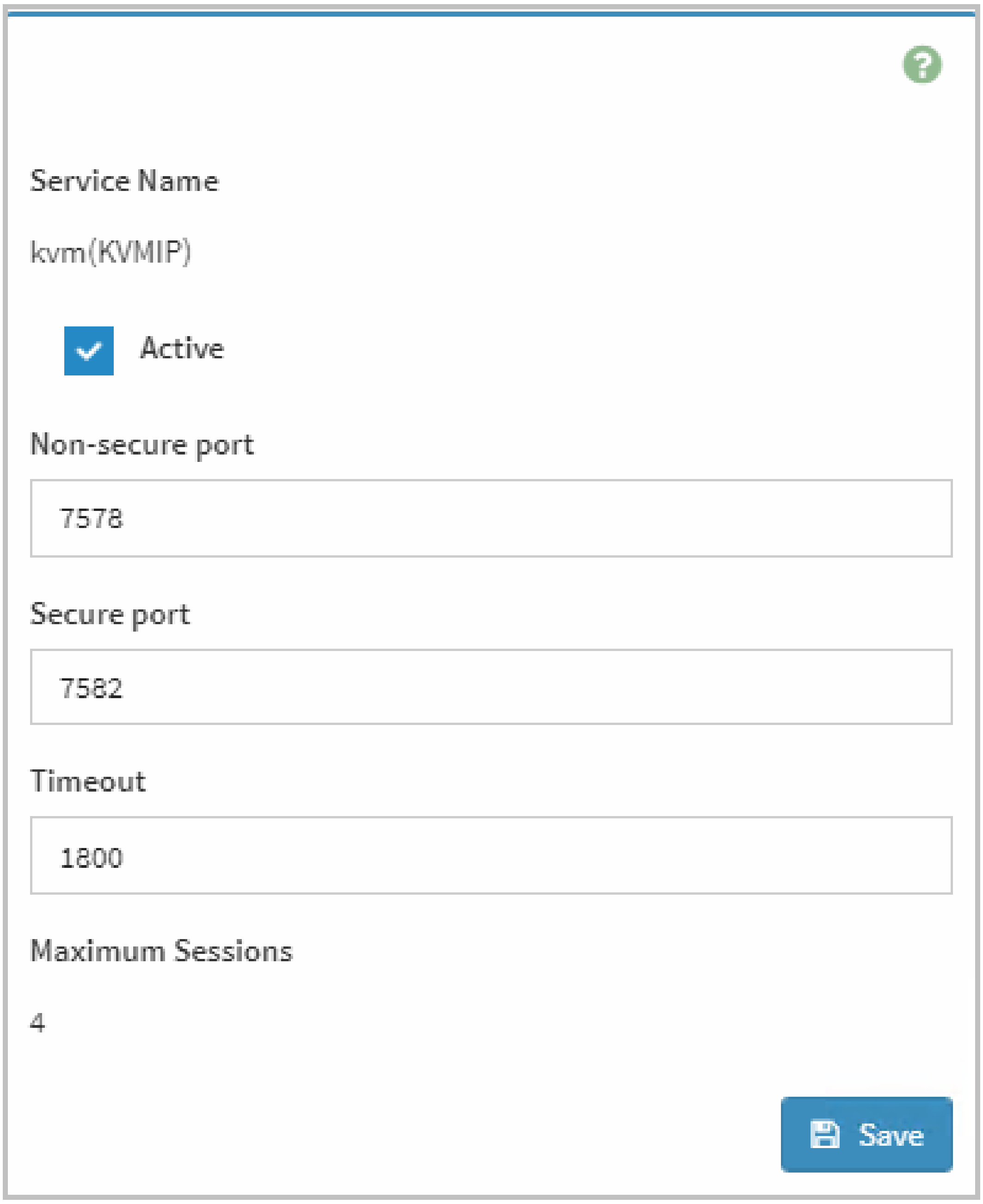
Figure 4-20 Service Sessions Page



Active Session - Web(HTTP/HTTPS)

Session ID ⇕	Session Type ⇕	User ID ⇕	User Name ⇕	Client IP ⇕	Privilege ⇕	
11*	Web HTTPS	3	root	192.178.6.123	Administrator	⊗

Figure 4-21 Service Configuration Page



Service Name

kvm(KVMIP)

☑ Active

Non-secure port

7578

Secure port

7582

Timeout

1800

Maximum Sessions

4

Table 4-5 Service Parameter Descriptions

Parameter	Description	Setting
Active	Whether to enable the service.	● Select **Active**. The service is available. ● Deselect **Active**. The service is not available.
Non-secure port	Non-secure port number of the service.	● Default non-secure port number of the Web service: 80.

Parameter	Description	Setting
		● Default non-secure port number of the KVM service: 7578. ● Default non-secure port number of the CD media service: 5120. ● Default non-secure port number of the HD media service: 5123. ● The SSH service does not support non-secure ports. ● Default non-secure port number of the SNMP service: 161. ● Default non-secure port of the VNC service: 5900. Range of the non-secure port number: 1 – 65535.
Secure port	Secure port number of the service.	● Default secure port number of the Web service: 443. ● Default secure port number of the KVM service: 7582. ● Default non-secure port number of the CD media service: 5124. ● Default non-secure port number of the HD media service: 5127. ● Default secure port number of the SSH service: 22. ● Default secure port number of the VNC service: 5901. Range of the secure port number: 1–65535.
Timeout	Timeout period after which the service exits if no operation is performed.	● The timeout period of the Web service and KVM service ranges from 300 through 1800 seconds. ● The timeout period of the SSH service ranges from 60 through 1800 seconds. The timeout period must be a multiple of 60.

4.11 Configuring the NTP Server

Abstract

The time on the BMC is synchronized from the NTP server.

The operations for configuring the NTP server include:

1. Enable the NTP service: Provides the NTP service for the devices whose time needs to be synchronized.
2. Modify the registry: Modifies the registry parameters related to the NTP service.
3. Restart the NTP service: Applies the modified registry parameters.

Note

This procedure describes how to perform the operations on a PC with the Windows 10 operating system.

Steps

Enabling the NTP Service

1. Right-click **This PC** on the desktop, and then select **Manage** from the shortcut menu. The **Computer Management** window is displayed.
2. From the navigation tree in the left pane, select **Services and Applications > Services**. The **Services** window is displayed.
3. In the service list, right-click **Windows Time** and select **Start** from the shortcut menu.

Modifying the Registry

4. Press **Windows+R**. The **Run** dialog box is displayed.
5. In the **Open** text box, enter *regedit*, and click **OK**. The **Registry Editor** window is displayed.
6. Modify the registry parameters. For a description of the parameters, refer to Table 4-6.

Table 4-6 Registry Parameter Descriptions

Registry Path	Parameter	Value
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config	AnnounceFlags	5
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\TimeProviders\NtpServer	Enabled	1

Restarting the NTP Service

7. In the **Open** text box in the **Run** dialog box, enter *cmd*, and click **OK**. The command line window is displayed.
8. Run the following command to stop the NTP service:

```
C:\> net stop w32time
```

9. Run the following command to start the NTP service:

```
C:\> net start w32time
```

10. Run the following command to verify that the NTP server is configured successfully:

    `C:\> w32tm /stripchart /computer:127.0.0.1`

    If the output time is displayed after the command is run, it indicates that the configuration is successful.

4.12 Configuring the SMTP Server

Abstract

The SMTP server receives alarm emails from the BMC.

The operations for configuring the SMTP server include:

1. Install the SMTP server: Provides the SMTP service for the BMC.
2. Configure the IP address and port number: After the same IP address and port number are configured on the Web page of the BMC, the alarm emails (if any) are sent to the default path *`C:\inetpub\mailroot\Drop`* on the SMTP server.

Note

This procedure describes how to perform the operations on a PC with the Windows Server 2012 R2 operating system. The operations for other Windows Server operating systems are similar.

Steps

Installing the SMTP Server

1. Press **Windows+R**. The **Run** dialog box is displayed.
2. In the **Open** text box, enter *`servermanager`*, and click **OK**. The **Server Manager** window is displayed.
3. Click **Add Roles and Features**. The **Add Roles and Features Wizard** window is displayed.
4. Select **Role-based or feature-based installation**.
5. Click **Next**.
6. Select **Select a server from the server pool**, and then select the server from **Server Pool**.
7. Click **Next** until the **Features** step in **Add Roles and Features Wizard** is displayed.
8. Select **SMTP Server**.
9. Click **Install**.

Configuring the IP Address and Port Number

10. In **Control Panel > System and Security > Administrative Tools**, double-click **Internet Information Services (IIS) 6.0 Manager**.
11. Right-click **SMTP Virtual Server #1**, and select **Properties** from the shortcut menu. The **[SMTP Virtual Server #1] Properties** dialog box is displayed.

12. From the **IP address** list, select the corresponding IP address.

Note

The selected IP address is that of the server selected in Step 6.

13. Switch to the **Delivery** tab.
14. Click **Outbound connections**. The **Outbound Connections** dialog box is displayed.
15. In the **TCP port** text box, enter `25`.
16. Click **OK**.

4.13 Configuring SNMP Trap

Abstract

SNMP Trap parameters are used by the BMC to send alarms and notifications to a third-party NMS.

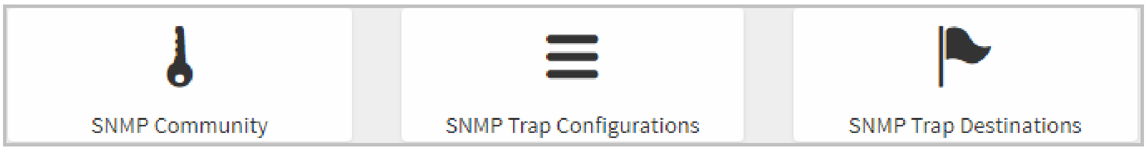
Note

SNMP Trap parameters are provided by a third-party NMS.

Steps

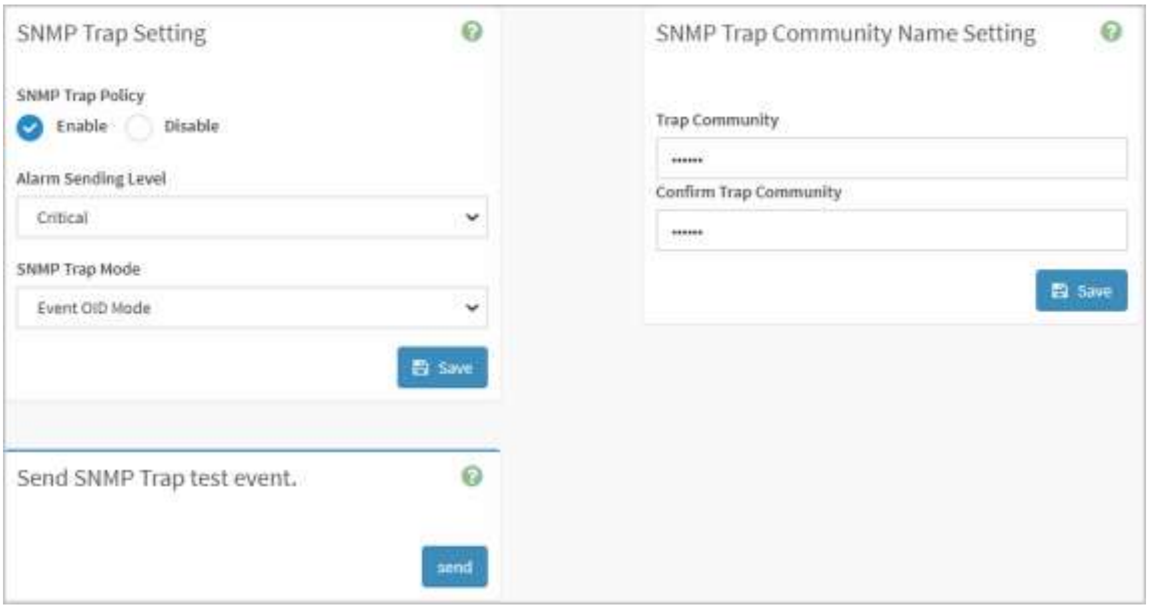
1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **SNMP Settings**. The **SNMP Settings** page is displayed, see Figure 4-22.

Figure 4-22 SNMP Settings Page



3. Click **SNMP Trap Configurations**. The **SNMP Trap Configurations** page is displayed, see Figure 4-23.

Figure 4-23 SNMP Trap Configurations Page



SNMP Trap Setting

SNMP Trap Policy

● Enable ○ Disable

Alarm Sending Level: Critical

SNMP Trap Mode: Event OID Mode

Send SNMP Trap test event.

SNMP Trap Community Name Setting

Trap Community: ******

Confirm Trap Community: ******

4. Select **Enable** in the **SNMP Trap policy** area.
5. Select an alarm level from the **Alarm Sending Level** list.

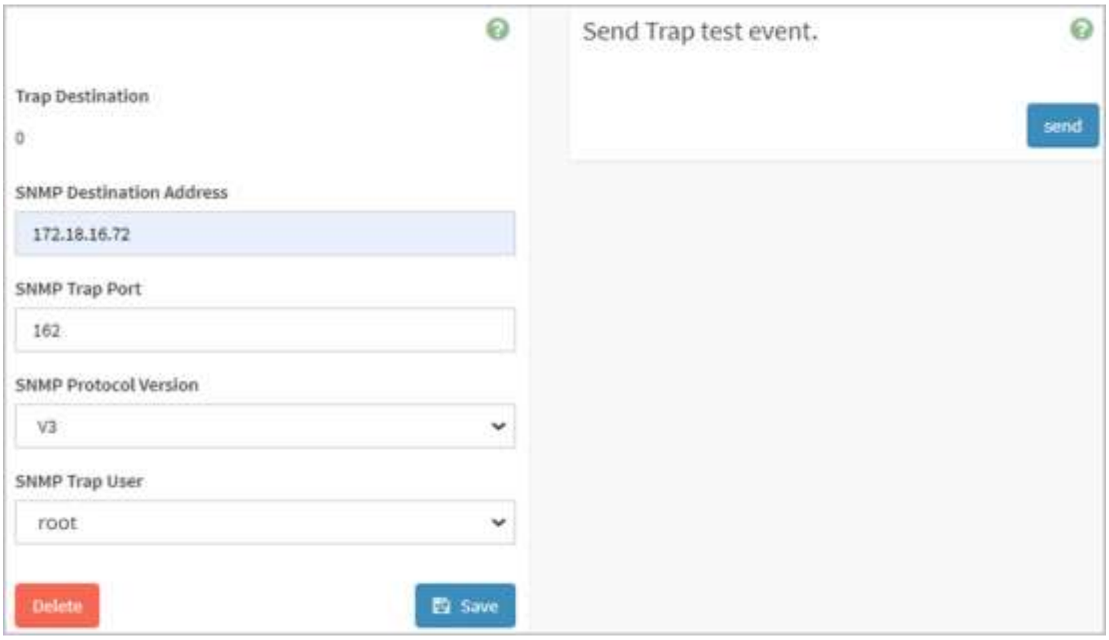
   Alarm levels include:

   - **Critical**: Alarms of critical level are sent only.
   - **Major**: Alarms of major and critical levels are sent.
   - **Minor**: Alarms of minor, major, and critical levels are sent.
   - **Normal**: Alarms of normal, minor, major, and critical levels are sent.
6. Select a mode from the **Module Trap Mode** list.

   Modes include:

   - **Event OID Mode**: indicates that alarms are triggered by event.
   - **Module OID Mode**: indicates that alarms are triggered by module.
7. Click **Save** in the **SNMP Trap Setting** area.
8. Enter a community name in the **Trap Community** text box and confirm it in the **Confirm Trap Community** text box in the **SNMP Trap Community Name Setting** area.
9. Click **Save** in the **SNMP Trap Community Name Setting** area.
10. Return to the **SNMP Settings** page.
11. Click **SNMP Trap Destinations**. The **SNMP Trap Destinations** page is displayed.
12. Click ⚑. The **Trap Destination Configuration** page is displayed, see Figure 4-24.

Figure 4-24 Trap Destination Configuration Page



Trap Destination

0

SNMP Destination Address: 172.18.16.72

SNMP Trap Port: 162

SNMP Protocol Version: V3

SNMP Trap User: root

Send Trap test event.

13. Configure the parameters. For a description of the parameters, refer to Table 4-7.

Table 4-7 Trap Destination Parameter Descriptions

Parameter	Description	Setting
SNMP Destination Address	IP address of the server that receives alarms.	Enter the IP address in the IPv4 or IPv6 format.
SNMP Trap Port	Server port that receives alarms.	Enter the port number, with a range of 1–65535. If there is a default port number, provide it.
SNMP Protocol Version	SNMP protocol used for sending alarms.	Select a protocol version.
SNMP Trap User	User used for sending alarms.	When **SNMP Protocol Version** is set to **V3**, you must select a user with the SNMP permissions as the alarm sender. For a description of the authentication protocol and private protocol, refer to "3.7.24 Creating a User".

14. (Optional) Click **send** in the **Send Trap test event** area. A test event is sent to the Trap destination.

Note

If the information indicating "sent successfully" is displayed on the page, it indicates that the SNMP Trap function is normal.

15. Click **Save**.

4.14 Handling Network Port Alarms

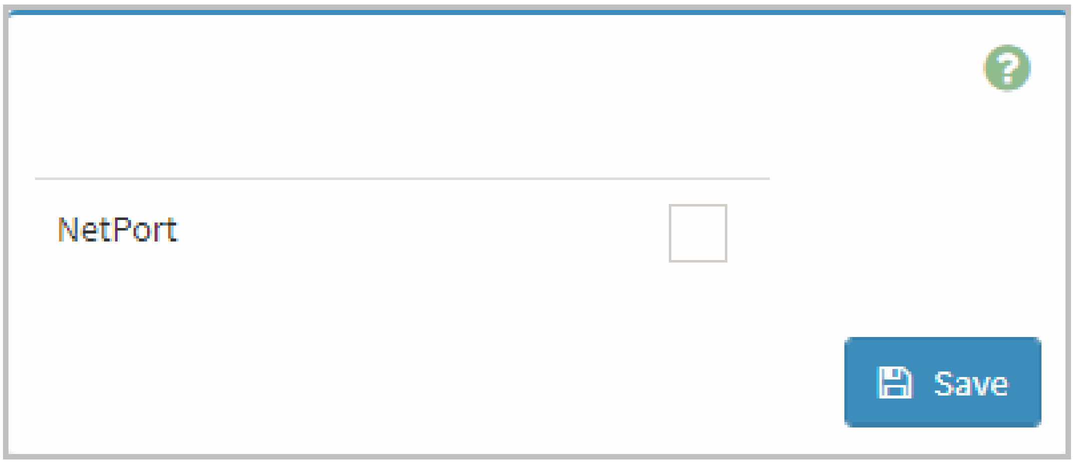
Abstract

If the network port is not connected with a network cable, a net port alarm is reported, indicating "NetPort Down or Cable Disconnected". Network port alarms can be handled through the **NetPort Alarm Configuration** function.

Steps

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Alarm Settings**. The **Alarm Settings** page is displayed.
3. Click **NetPort Alarm Configuration**. The **NetPort Alarm Configuration** page is displayed, see Figure 4-25.

Figure 4-25 NetPort Alarm Configuration Page



NetPort □

4. Deselect **NetPort** to disable network port alarms.
5. Click **Save**.

4.15 Exporting BMC Logs

You can export BMC logs through the following ways:

- Export BMC logs in one click. For details refer to "4.15.1 Exporting Data in One Click".
- Export BMC logs by category. For details, refer to "4.15.2 Exporting BMC Logs by Category".
- Export logs through the SSH command line (SSH). For details, refer to "4.15.3 Exporting Logs Through the Command Line (SSH)".
- Export logs through the command line (serial port). For details, refer to "4.15.4 Exporting Logs Through the Command Line (Serial Port)".

4.15.1 Exporting Data in One Click

Abstract

By exporting data in one click, you can export the log data of the BMC to the local PC. The exported log file name is *bmcinfo_SN.tar.gz*, which is stored in the default download directory of the browser.

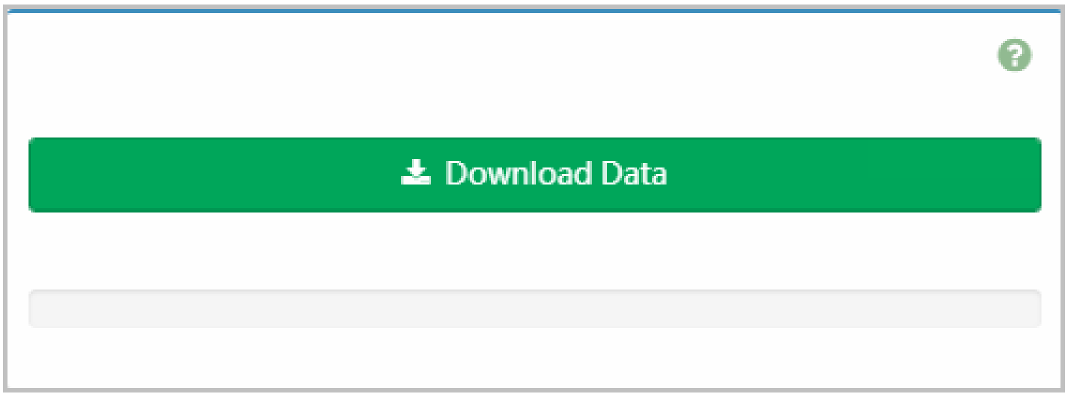
Note

If the SN of the server cannot be queried, the name of the exported log file is *bmcinfo_UnknownProductSN.tar.gz*.

Steps

1. From the menu bar in the left pane, select **Maintenance**. The **Maintenance** page is displayed.
2. Click **Expert Data**. The **Download Expert Data** page is displayed, see Figure 4-26.

Figure 4-26 Download Expert Data Page



3. Click **Download Data**. The download progress is displayed, see Figure 4-27.

Figure 4-27 Download Progress Page

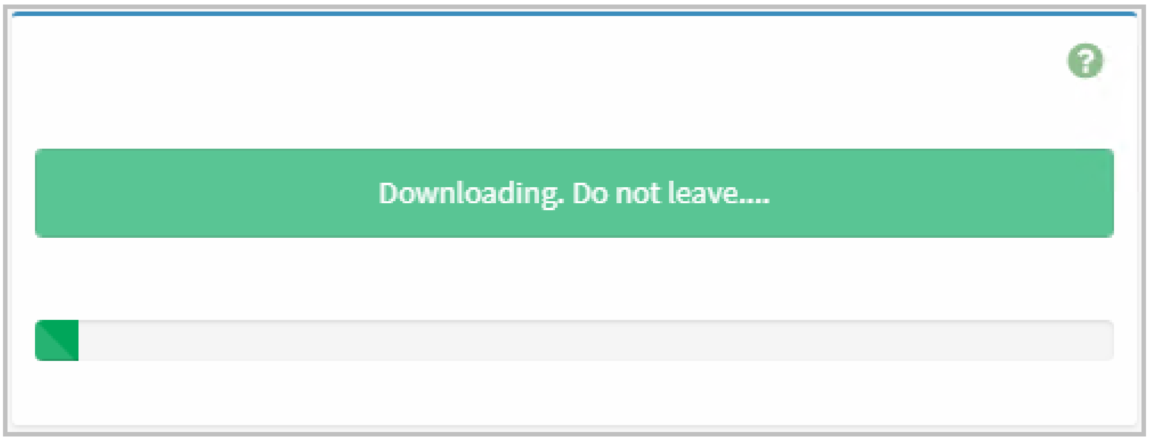
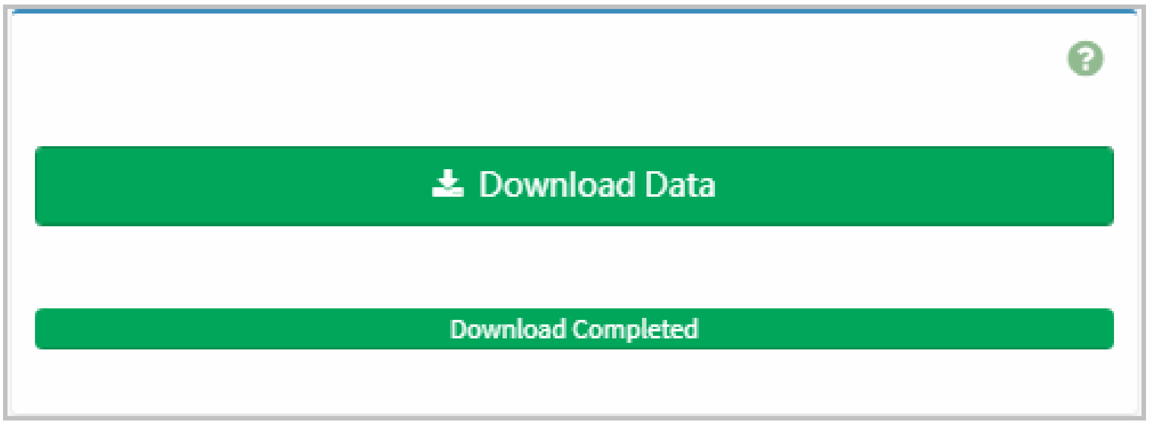


Figure 4-28 shows the downloaded page.

Figure 4-28 Download Completed Page



4.15.2 Exporting BMC Logs by Category

Abstract

BMC logs include:

- Login log: records user login and logout information.
- Operation log: records users' operations.
- System log: records log and historical alarm information generated during the operation of the server.
- Event log: records events generated during the operation of the server.

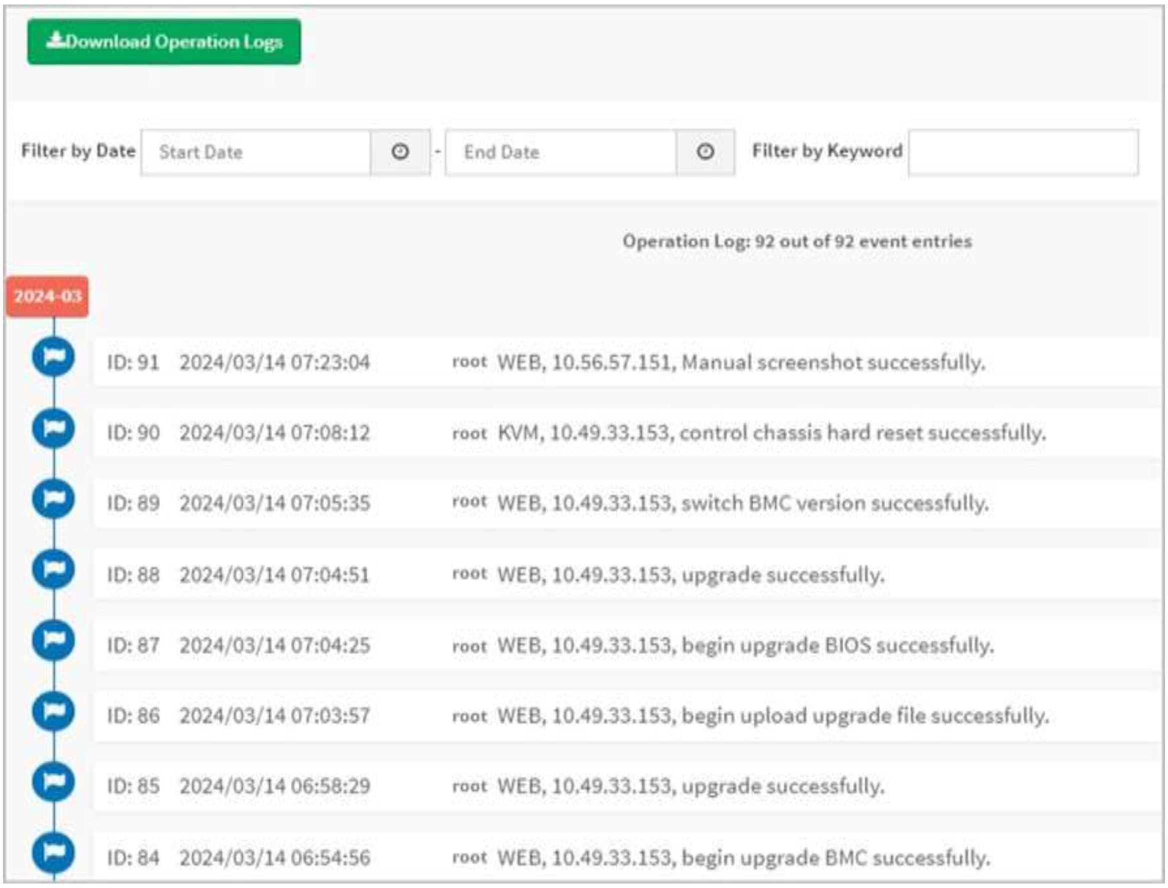
Note

The operations for exporting logs of the above categories are similar. This procedure describes how to export operation logs.

Steps

1. From the menu bar in the left pane, select **Alarms & Logs > Operation Log**. The **Operation Log** page is displayed, see Figure 4-29.

Figure 4-29 Operation Log Page



Operation Log: 92 out of 92 event entries

```
ID: 91  2024/03/14 07:23:04  root WEB, 10.56.57.151, Manual screenshot successfully.
ID: 90  2024/03/14 07:08:12  root KVM, 10.49.33.153, control chassis hard reset successfully.
ID: 89  2024/03/14 07:05:35  root WEB, 10.49.33.153, switch BMC version successfully.
ID: 88  2024/03/14 07:04:51  root WEB, 10.49.33.153, upgrade successfully.
ID: 87  2024/03/14 07:04:25  root WEB, 10.49.33.153, begin upgrade BIOS successfully.
ID: 86  2024/03/14 07:03:57  root WEB, 10.49.33.153, begin upload upgrade file successfully.
ID: 85  2024/03/14 06:58:29  root WEB, 10.49.33.153, upgrade successfully.
ID: 84  2024/03/14 06:54:56  root WEB, 10.49.33.153, begin upgrade BMC successfully.
```

2. Perform the following operations as required.

To...	Do...
Filter logs by date	Click 🕘 in the **Filter by Date** area and set the start date and end date for querying operation logs.
Filter logs by keyword	a. In the **Filter by Keyword** text box, enter a keyword. b. Press **Enter**. The results filtered by the keyword are displayed on the page.
Save logs to the local PC	Click **Download Operation Logs** and save the operation logs to the local PC.

4.15.3 Exporting Logs Through the Command Line (SSH)

Abstract

If the BMC Web portal is faulty, you can connect to the BMC remotely through SSH and export logs in one click in command line mode.

Steps

1. Connect to the BMC by using the SSH tool.
2. Run the following commands in the command line to export logs:

```
# cd /etc/init.d/
# ./expert_data.sh
```

Note

After the logs are exported, they are stored in the */var/video/bmcinfo.tar.gz* directory.

3. Download the log file to the local PC by using the SFTP function.
4. Run the following commands in the command line to delete the BMC log file:

```
# cd /var/video
# rm bmcinfo.tar.gz
```

4.15.4 Exporting Logs Through the Command Line (Serial Port)

Abstract

If the network is abnormal and cannot be connected to the BMC, you can export logs through the serial port.

Steps

1. Connect the serial port of the BMC by using a DB9 serial port cable.
2. Press and hold the UID indicator on the server panel for eight seconds until the indicator flashes blue.
3. Use a serial port tool to connect to the serial port of the BMC.
4. After the connection is established, log in to the serial port with the account and password.
5. Run the following commands in the command line to export logs:

```
# cd /etc/init.d/
# ./expert_data.sh
```

Note

After the logs are exported, they are stored in the */var/video/bmcinfo.tar.gz* directory.

6. Run the following command to back up the log file to the */mnt/nandflash0/* directory:

```
# cp /var/video/bmcinfo.tar.gz /mnt/nandflash0/
```

Note

You can download log files to the local PC by using the SFTP function after the network is restored.

4.16 Upgrading the BMC Version

Abstract

To upgrade the firmware version of the BMC, you can load the version file online for firmware upgrade.

Note

- After the BMC firmware is upgraded, the BMC is reset automatically.
- During the upgrade process, in case of any upgrade failure, you must upgrade the version again.

Prerequisite

The version upgrade file for the BMC is obtained.

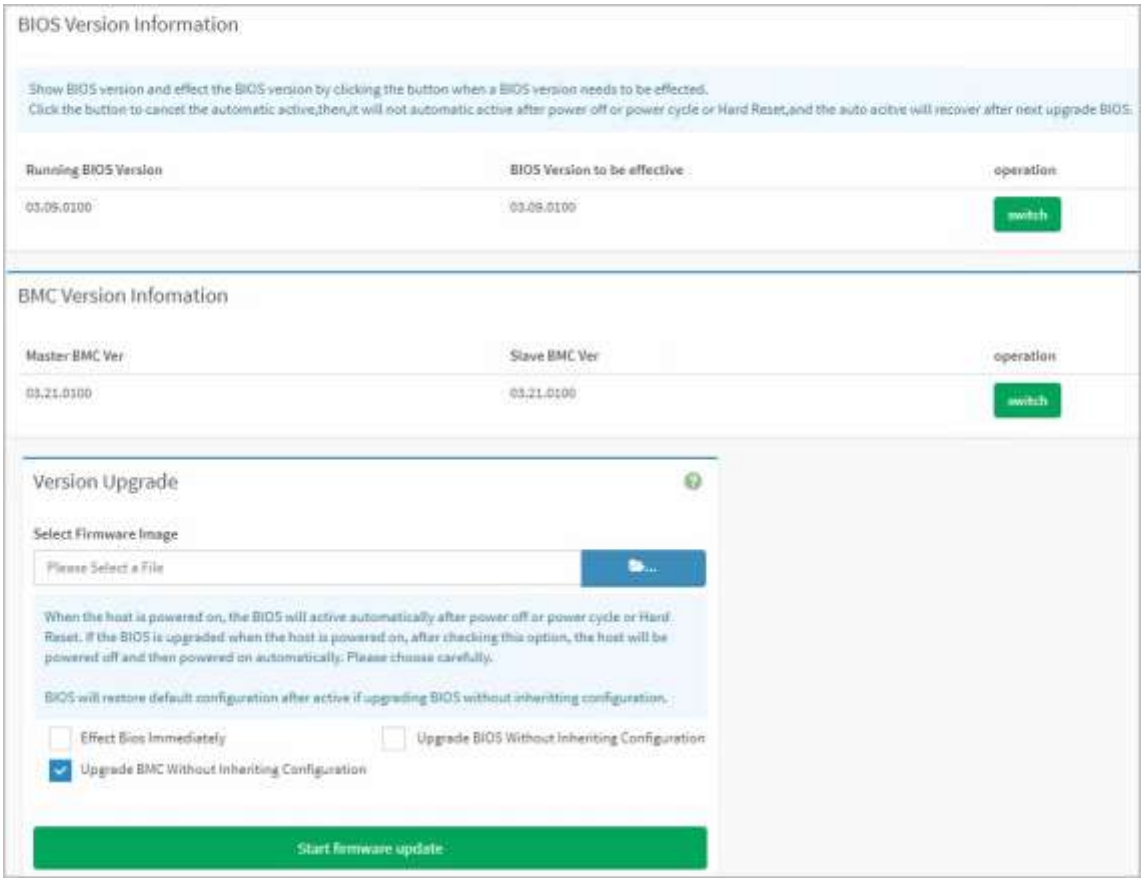
Note

The firmware upgrade files can be downloaded on the **Software Download** page on the Web portal (https://vantageo.com) of the servers and storage products.

Steps

1. From the menu bar in the left pane, select **Maintenance**. The **Maintenance** page is displayed.
2. Click **Firmware Update**. The **Other Firmware Update** page is displayed, see Figure 4-30.

Figure 4-30 Other Firmware Update Page



BIOS Version Information

Show BIOS version and effect the BIOS version by clicking the button when a BIOS version needs to be effected.
Click the button to cancel the automatic active,then,it will not automatic active after power off or power cycle or Hard Reset,and the auto acitve will recover after next upgrade BIOS.

Running BIOS Version	BIOS Version to be effective	operation
03.05.0100	03.08.0100	switch

BMC Version Infomation

Master BMC Ver	Slave BMC Ver	operation
03.21.0100	03.21.0100	switch

Version Upgrade

Select Firmware Image

Please Select a File

When the host is powered on, the BIOS will active automatically after power off or power cycle or Hard Reset. If the BIOS is upgraded when the host is powered on, after checking this option, the host will be powered off and then powered on automatically. Please choose carefully.

BIOS will restore default configuration after active if upgrading BIOS without inheriting configuration.

□ Effect Bios Immediately

□ Upgrade BIOS Without Inheriting Configuration

☑ Upgrade BMC Without Inheriting Configuration

3. In the **Version Upgrade** area, click 📂... . In the displayed dialog box, select a BMC version file.

Note

Only one version file can be selected at a time. When the firmware version is updated, the firmware type is automatically matched.

4. Click **Start firmware update**. The firmware upgrade progress is displayed below.

Notice

During the version upgrade process, it is not allowed to switch to another page. Otherwise, the version upgrade process is interrupted.

Note

The firmware version number generated after upgrade is displayed in the **Master BMC Ver** column, and the version number originally displayed in the **Master BMC Ver** column is displayed in the **Slave BMC Ver** column.

Related Tasks

If the switchover between the active and standby BMC versions is required, click **switch** in the **BMC Version Information**.

4.17 Restoring Factory Defaults

Abstract

By restoring factory defaults, you can restore the server configuration items (for example, the network, user, SNMP configuration and startup mode) to factory defaults.

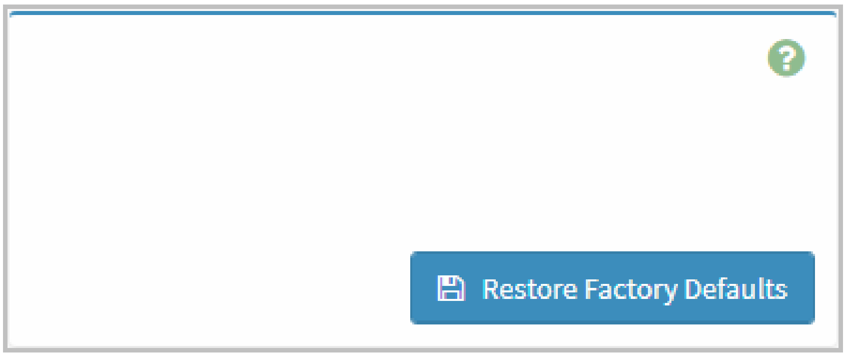
Note

Do not perform any operation during restoration.
After factory defaults are restored, the server is restarted.

Steps

1. From the menu bar in the left pane, select **Maintenance**. The **Maintenance** page is displayed.
2. Click **Restore Factory Defaults**. The **Restore Factory Defaults** page is displayed, see Figure 4-31.

Figure 4-31 Restore Factory Defaults Page



3. Click **Restore Factory Defaults**.

4.18 Backing Up BMC Configurations

Abstract

Before replacing the mainboard of a server, you must export the BMC configurations. After the mainboard is replaced, you can import the BMC configurations.

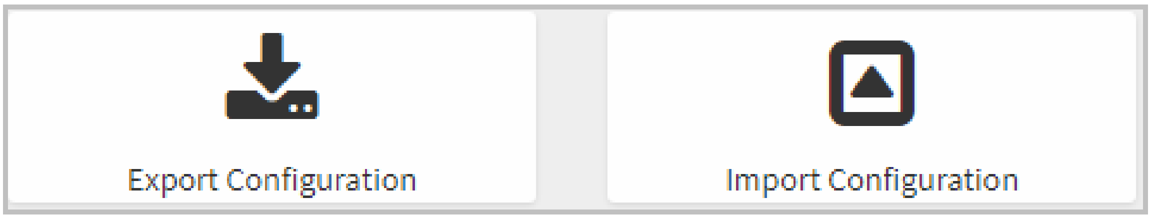
Note

Only product serial numbers can be exported in this version.

Steps

1. From the menu bar in the left pane of the BMC Web portal, select **Maintenance**. The **Maintenance** page is displayed.
2. Click **Backup Configuration**. The **Backup Configuration** page is displayed, see Figure 4-32.

Figure 4-32 Backup Configuration Page



3. Perform the following operations as required.

To...	Do...
Export configurations	a. Click **Export Configuration**. The **Export Configuration** page is displayed. b. Click **Download Configuration**.
Import configurations	a. Click **Import Configuration**. The **Import Configuration** page is displayed. b. Click 📂..., and select the exported configuration file. c. Click **Upload Configuration**.

4.19 Identifying a Liquid-Cooled Server

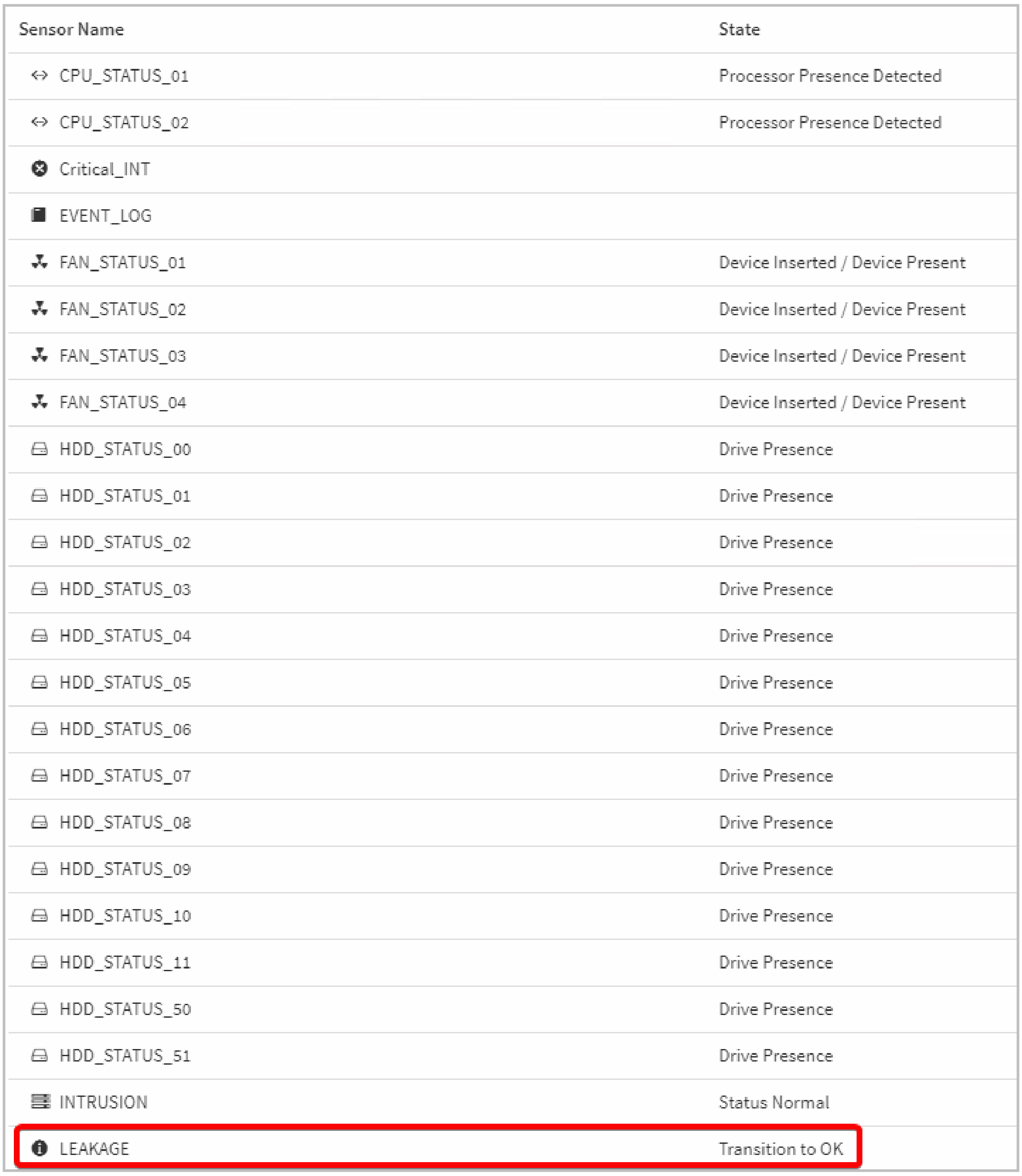
Abstract

A liquid-cooled server differs from a non-liquid-cooled server in that the former has a leakage (**LEAKAGE**) sensor.

Steps

1. From the menu bar in the left pane, select **Sensor**. The **Sensor Reading** page is displayed.
2. In the **Discrete Sensor States** area, check whether the **LEAKAGE** sensor exists, as shown in Figure 4-33.

Figure 4-33 Checking the LEAKAGE Sensor



Sensor Name	State
CPU_STATUS_01	Processor Presence Detected
CPU_STATUS_02	Processor Presence Detected
Critical_INT	
EVENT_LOG	
FAN_STATUS_01	Device Inserted / Device Present
FAN_STATUS_02	Device Inserted / Device Present
FAN_STATUS_03	Device Inserted / Device Present
FAN_STATUS_04	Device Inserted / Device Present
HDD_STATUS_00	Drive Presence
HDD_STATUS_01	Drive Presence
HDD_STATUS_02	Drive Presence
HDD_STATUS_03	Drive Presence
HDD_STATUS_04	Drive Presence
HDD_STATUS_05	Drive Presence
HDD_STATUS_06	Drive Presence
HDD_STATUS_07	Drive Presence
HDD_STATUS_08	Drive Presence
HDD_STATUS_09	Drive Presence
HDD_STATUS_10	Drive Presence
HDD_STATUS_11	Drive Presence
HDD_STATUS_50	Drive Presence
HDD_STATUS_51	Drive Presence
INTRUSION	Status Normal
LEAKAGE	Transition to OK

Note

If the **LEAKAGE** sensor exists, the server is a liquid-cooled server. The **State** column displays the state of the sensor.

4.20 Creating an SNMP User

Abstract

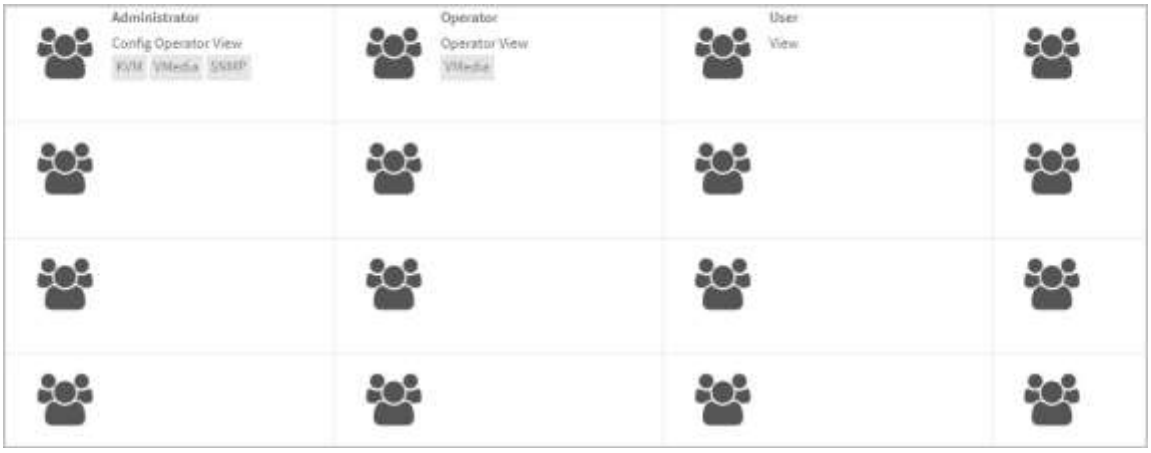
When configuring SNMP trap destinations, if SNMPv3 is used, you must select a user with the SNMP permissions as the alarm sender. This procedure describes how to create an SNMP user on the **Group Management** and **User Management** pages.

Steps

Adding a User Group

1. From the menu bar in the left pane, select **Settings**. The **Settings** page is displayed.
2. Click **Group Management**. The **Group Management** page is displayed, as shown in Figure 4-34.

Figure 4-34 Group Management Page

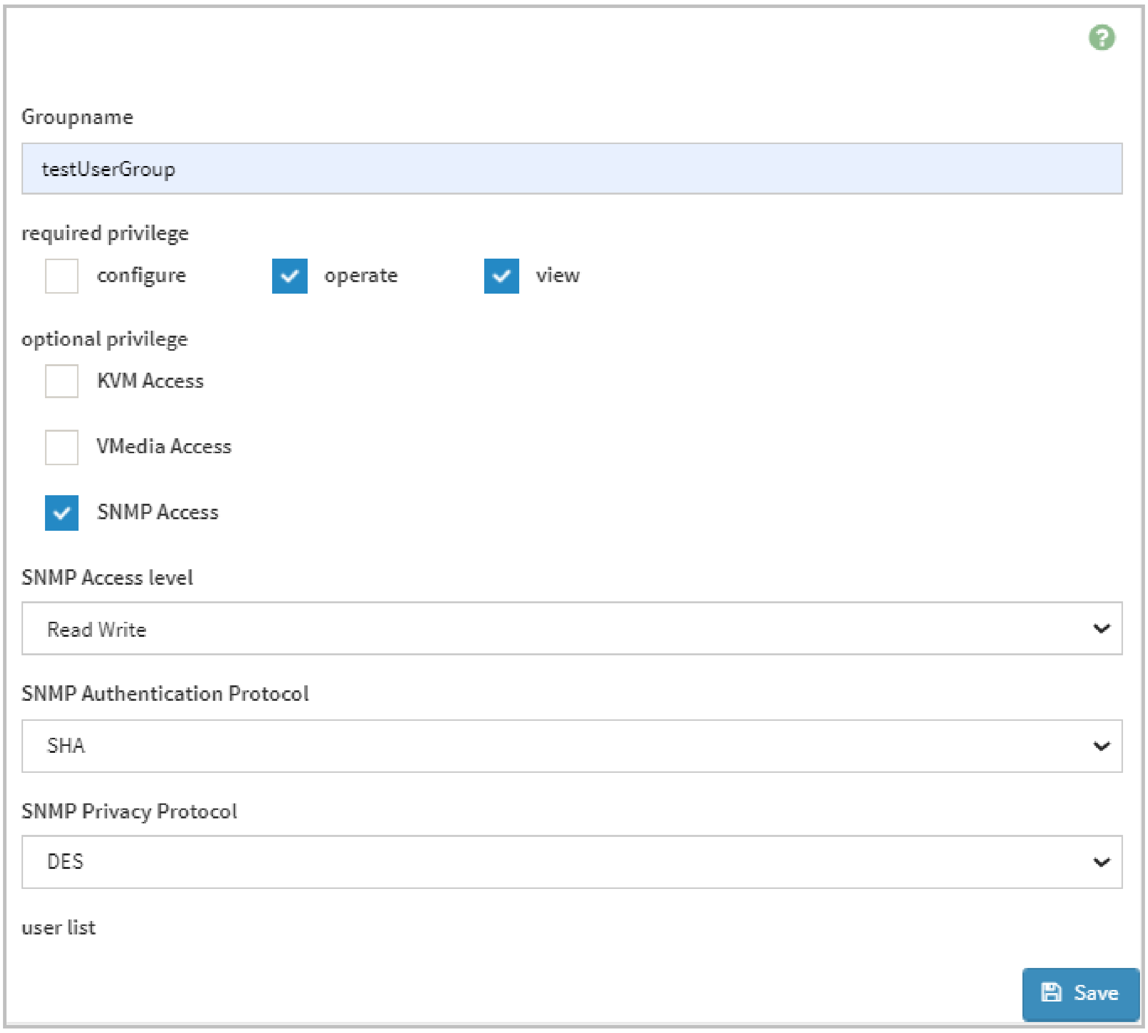


Note

A user group icon with a name on the right indicates an existing user group. A user group icon without a name is a placeholder for a new user group. To add a user group, click a user group icon without a name.

3. Click a user group icon without a name. The **Group Management Configuration** page is displayed, as shown in Figure 4-35.

Figure 4-35 Group Management Configuration Page



Groupname

testUserGroup

required privilege

□ configure ☑ operate ☑ view

optional privilege

□ KVM Access

□ VMedia Access

☑ SNMP Access

SNMP Access level

Read Write

SNMP Authentication Protocol

SHA

SNMP Privacy Protocol

DES

user list

4. Set the parameters. For a description of the parameters, refer to Table 4-8.

Table 4-8 User Group Parameter Descriptions

Parameter	Description	Setting
Groupname	Name of the user group.	Enter a user group name. ● The group name is a string composed of 4–16 letters, digits, " - " , " _ " or " @ " , which must start with a letter. ● Letters are case-sensitive.
required privilege/optional privilege	Operation permissions of the users in the user group.	The permissions are divided into required permissions and optional permissions. ● Required permissions: Select at least one of the following permissions: → **configure** → **operate** → **view**

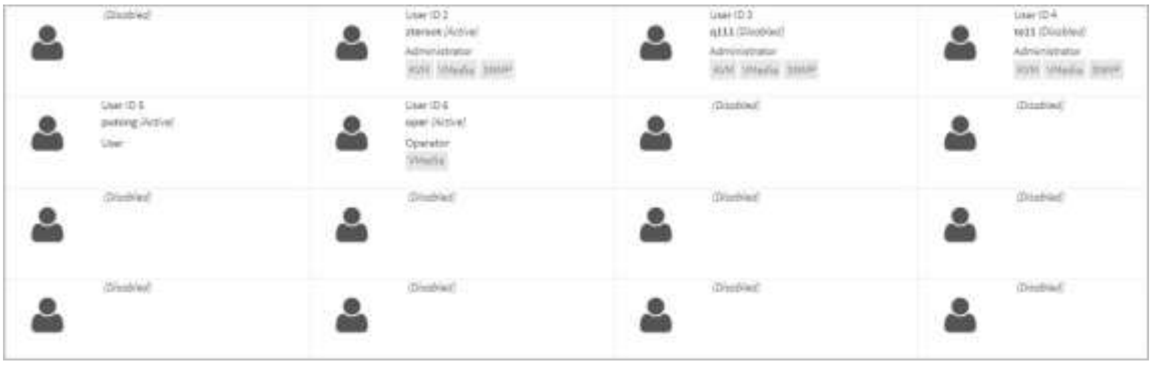
Parameter	Description	Setting
		In most cases, the required permissions for each user group are as follows: → Administrator: **configure**, **operate**, and **view** → Operator: **operate** and **view** → Viewer: **view** ● Optional permissions: Select one of the following permissions as needed. → **KVM Access** → **VMedia Access** → **SNMP Access** In most cases, the optional permissions for each user group are as follows: → Administrator: **KVM Access**, **VMedia Access**, and **SNMP Access** → Operator: **SNMP Access** → Viewer: not applicable
SNMP Access Level	SNMP access level.	Select an SNMP access level, including: ● Read Write ● Read Only
SNMP Authentication Protocol	SNMP authentication protocol.	Select an SNMP authentication protocol, including: ● NONE ● SHA ● MD5 ● SHA256 ● SHA384 ● SHA512
SNMP Privacy Protocol	SNMP encryption mode.	Select an SNMP encryption mode, including: ● NONE ● DES ● AES ● AES256 If **SNMP Authentication Protocol** is set to **NONE**, **SNMP Privacy Protocol** can only be set to **NONE**. **AES256** can be used together with only **SHA256**, **SHA384**, or **SHA512**.

5. Click **Save**.

Creating a User

6. On the **Settings** page, click **User Management**. The **User Management** page is displayed, as shown in Figure 4-36.

Figure 4-36 User Management Page



(Disabled)

User ID 2
zteroot (Active)
Administrator
KVM VMedia SNMP

User ID 3
q111 (Disabled)
Administrator
KVM VMedia SNMP

User ID 4
te11 (Disabled)
Administrator
KVM VMedia SNMP

User ID 5
pateing (Active)
User

User ID 6
oper (Active)
Operator
VMedia

(Disabled)

(Disabled)

(Disabled)

(Disabled)

(Disabled)

(Disabled)

(Disabled)

(Disabled)

(Disabled)

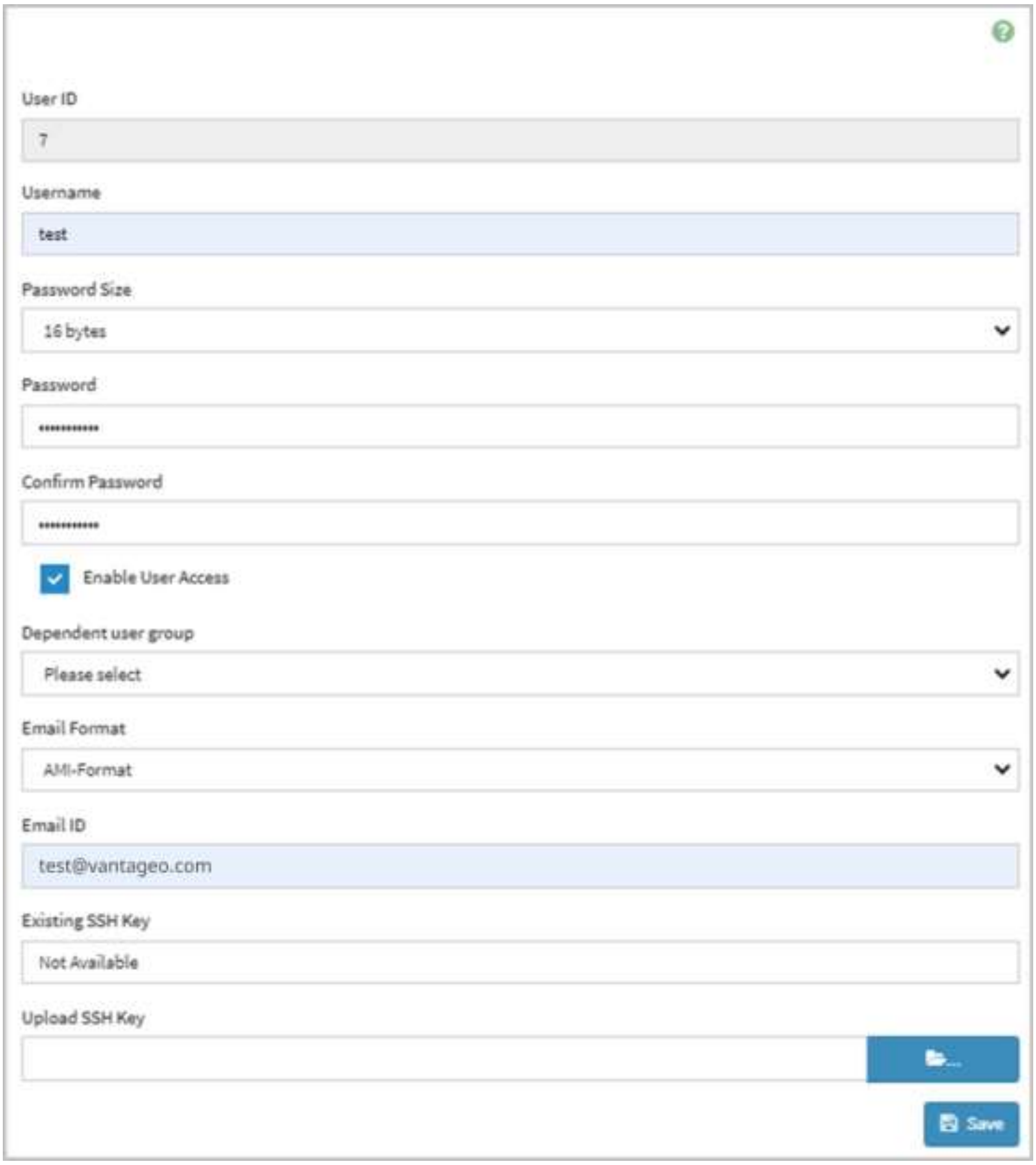
(Disabled)

Note

A user icon with a name on the right indicates an existing user. A user icon without a name is a placeholder for a new user. To add a user, click a user icon without a name. The first user icon in the upper left corner is reserved by the system and no user creation or modification operation can be performed.

7. Click a user icon without a name. The **User Management Configuration** page is displayed, as shown in Figure 4-37.

Figure 4-37 User Management Configuration Page



User ID

7

Username

test

Password Size

16 bytes

Password

•••••••••••

Confirm Password

•••••••••••

☑ Enable User Access

Dependent user group

Please select

Email Format

AMI-Format

Email ID

test@vantageo.com

Existing SSH Key

Not Available

Upload SSH Key

8. Set the parameters. For a description of the parameters, refer to Table 4-9.

Table 4-9 User Parameter Descriptions

Parameter	Description	Setting
User ID	User ID.	Generated by the system automatically and cannot be configured.
Username	User name.	Enter a username. ● The username is a string composed of 4–16 letters, digits, " - " , " _ " or " @ " , which must start with a letter. ● Letters are case-sensitive.

Parameter	Description	Setting
		● The username cannot be anonymous, root, admin, users, nobody, username, or sysadmin, and the username and password must not be the same.
Password Size	Length of the password to be entered in **Password**/**Confirm Password**.	Select a password length.
Password	User password.	Enter the user password. It is allowed to enter letters, digits, and symbols. Letters are case-sensitive. ● The password must not contain spaces or tabs. ● If a strong password is enabled, the password must contain four types of characters (upper-case letters, lower-case letters, digits, and symbols).
Confirm Password	Confirm the user password.	Enter the password for confirmation, which must be the same as **Password**.
Enable User Access	Whether to enable the user immediately.	The added user can take effect only after this option is selected.
Dependent user group	User group that the user belongs to.	Select a user group. For how to add a user group, refer to Adding a User Group. The user inherits the permissions of the user group that the user belongs to.
Email Format	Format of emails sent by the BMC to the user.	Select an email format: ● **AMI-Format**: The email title format is "Alert from (host address)". The emails in this format display sensor information, for example, sensor types and descriptions. ● **FixedSubject-Format**: The emails in this format display messages in accordance with user settings. The user must specify the email subject and messages in advance.
Email ID	Email address of the user.	Enter an email address.
Existing SSH Key	Displays the SSH key uploaded by the user.	-
Upload SSH Key	Uploads a public SSH key to the server. The file size cannot exceed 4 KB.	Click 📂… and select a key file.

9. Click **Save**.

Chapter 5
Reference: Default Passwords

The default administrator username for logging in to the BMC of a server is `sysadmin`. The default administrator password depends on server models and BMC versions. For details, refer to Table 5-1.

Table 5-1 Default Password Descriptions

Server Model	BMC Version	Default Password
2230-RE	Versions earlier than V03.20.01.10	superuser
	V03.20.01.10 and later	Superuser@123

Note

After logging in to the BMC by using the default password, you must change it immediately. It is recommended that you change the password to a strong password.

Chapter 6
Reference: Accessing Documents

Abstract

Documents are readily available at VANTAGEO

Note

This procedure takes *VANTAGEO Server SNMP Interface Description* as an example, and other documents can be accessed by similar steps.

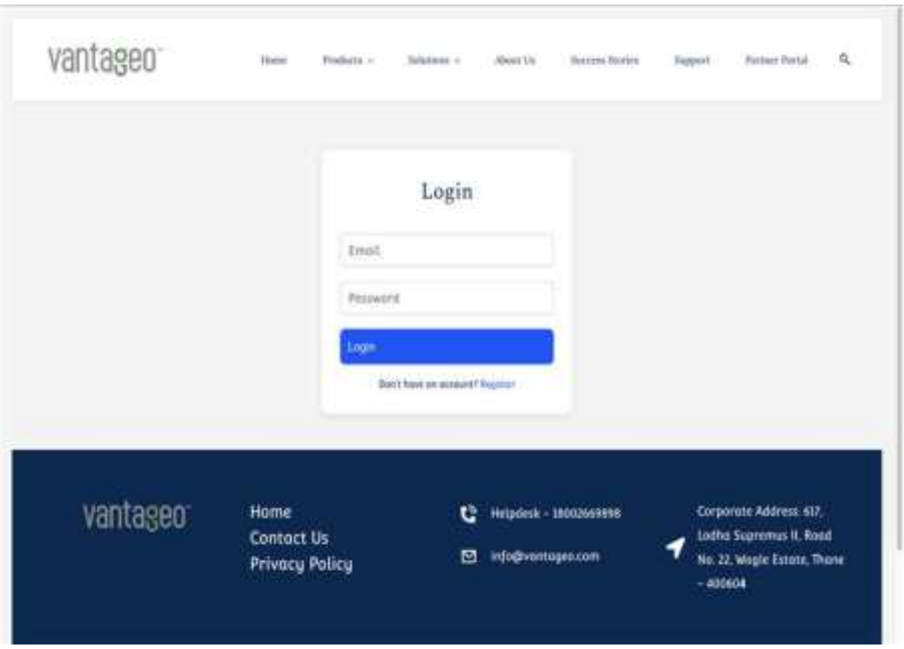
Prerequisite

You have registered successfully at VANTAGEO

Steps

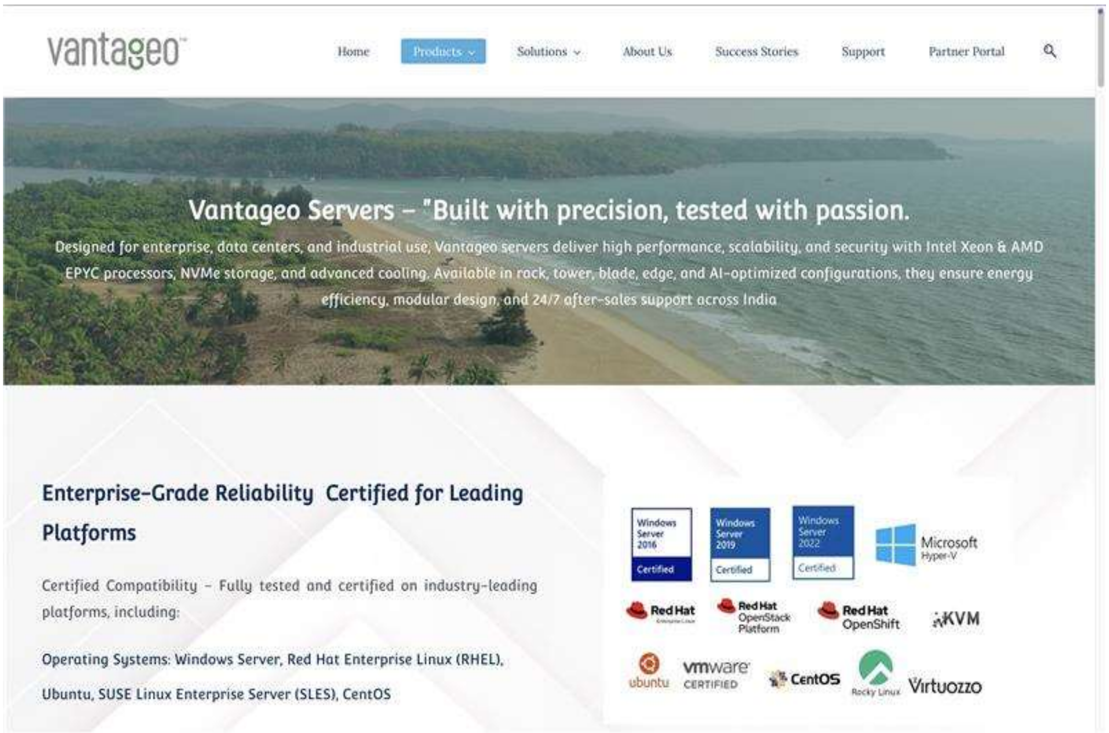
1. In the address bar of your browser, enter `https://vantageo.com` and press **Enter**. The home page is displayed.
2. Click **Login** in the upper right corner. The **User Login** page is displayed, see Figure 6-1.

Figure 6-1 User Login Page



3. Enter the username, password, and verification code.
4. Click **Login** to log in the VANTAGEO website.
5. Select **Products** on the menu. The **Products** page is displayed, see Figure 6-2.

Figure 6-2 Products Page



Vantageo Servers – "Built with precision, tested with passion.

Designed for enterprise, data centers, and industrial use, Vantageo servers deliver high performance, scalability, and security with Intel Xeon & AMD EPYC processors, NVMe storage, and advanced cooling. Available in rack, tower, blade, edge, and AI-optimized configurations, they ensure energy efficiency, modular design, and 24/7 after-sales support across India

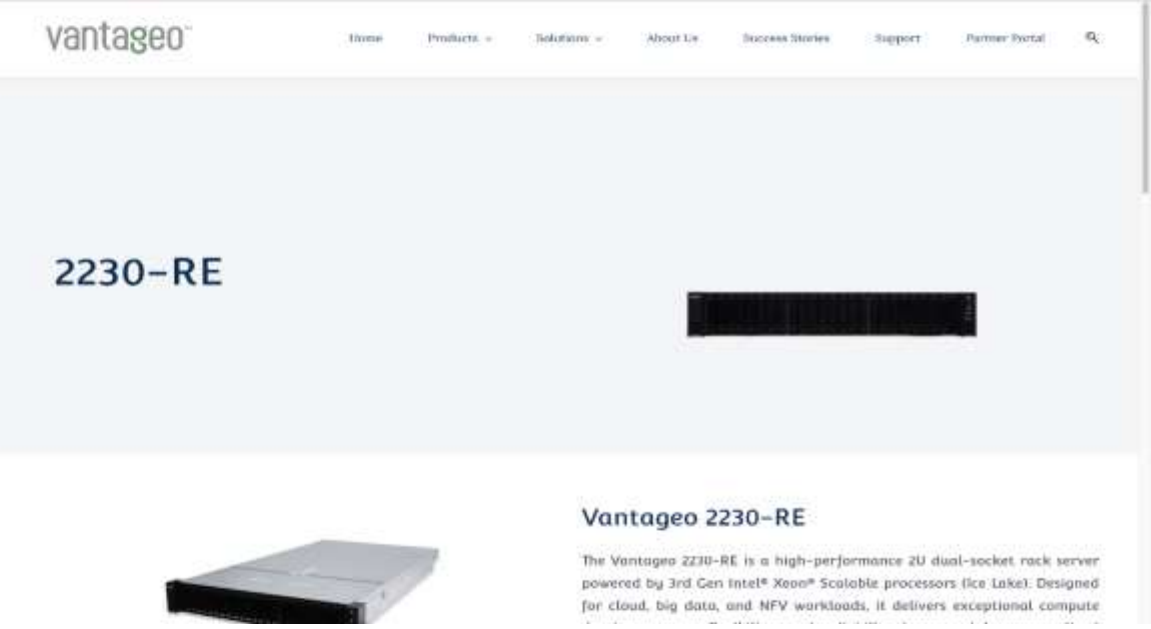
Enterprise-Grade Reliability Certified for Leading Platforms

Certified Compatibility – Fully tested and certified on industry-leading platforms, including:

Operating Systems: Windows Server, Red Hat Enterprise Linux (RHEL), Ubuntu, SUSE Linux Enterprise Server (SLES), CentOS

6. On the server list of servers at the lower part of the page, click the server that the document to be accessed is about, for example 2230-RE, and the **2230-RE** page is displayed, see Figure 6-3.

Figure 6-3 2230-RE Page



2230-RE

Vantageo 2230-RE

The Vantageo 2230-RE is a high-performance 2U dual-socket rack server powered by 3rd Gen Intel® Xeon® Scalable processors (Ice Lake). Designed for cloud, big data, and NFV workloads, it delivers exceptional compute

7. In the **document** list, select **Interface Description**, and all the documents about interface description are display on the right side of the page.
8. Click **Download** to the right of **Vantageo Server SNMP Interface Description**, and download the document.

Figures

Glossary

A/D

- Analog to Digital

AC

- Alternating Current

ACPI

- Advanced Configuration and Power Interface

AD

- Active Directory

AES

- Advanced Encryption Standard

API

- Application Programming Interface

ASCII

- American Standard Code for Information Interchange

BBU

- Battery Backup Unit

BIOS

- Basic Input/Output System

BMC

- Baseboard Management Controller

CA

- Certificate Authentication

CD

- Compact Disk

CLI

- Command Line Interface

CPU

- Central Processing Unit

CRPS

- Common Redundant Power Supplies

DCMI

- Data Center Manageability Interface

DES

- Data Encryption Standard

DHCP

- Dynamic Host Configuration Protocol

DNS

- Domain Name Server

DVD

- Digital Versatile Disc

EPLD

- Erasable Programmable Logic Device

FC

- Fiber Channel

FQDN

- Fully Qualified Domain Name

FRU

- Field Replaceable Unit

GPIO

- General Purpose Input Output

GPU

- Graphics Processing Unit

GUI

- Graphical User Interface

HBA

- Host Bus Adapter

HD

- Hard disk

HSSDC

- High Speed Serial Data Connector

HTML

- HyperText Markup Language

HTTPS

- Hypertext Transfer Protocol Secure

HVDC

- High-Voltage Direct Current

I/O

- Input/Output

ID

- Identification

IE

- Internet Explorer

IP

- Internet Protocol

IPMI

- Intelligent Platform Management Interface

IPv4

- Internet Protocol Version 4

IPv6

- Internet Protocol Version 6

ISO

- International Organization for Standardization

IT

- Information Technology

JRE

- Java Runtime Environment

KVM

- Keyboard, Video and Mouse

LAN

- Local Area Network

LDAP

- Lightweight Directory Access Protocol

LLDP

- Link Layer Discovery Protocol

LPC

- Lower order Path Connection

LSI

- Large Scale Integration

LVDC

- Low-Voltage Direct Current

MAC

- Media Access Control

MD5

- Message Digest 5 Algorithm

NCSI

- Network Controller Sideband Interface

NIC

- Network Interface Card

NMI

- Non-Maskable Interrupt

NMS

- Network Management System

NTP

- Network Time Protocol

NVMe

- Non-Volatile Memory Express

OS

- Operating System

PC

- Personal Computer

PCH

- Platform Controller Hub

PCIe

- Peripheral Component Interconnect Express

PECI

- Platform Environment Control Interface

PSU

- Power Supply Unit

PWM

- Pulse-Width Modulation

PXE

- Preboot eXecution Environment

RAID

- Redundant Array of Independent Disks

RMCP

- Remote Management Control Protocol

SAS

- Serial Attached SCSI

SFTP

- Secure File Transfer Protocol

SGPIO

- Serial GPIO

SHA

- Secure Hash Algorithm

SMBUS

- System Management BUS

SMTP

- Simple Mail Transfer Protocol

SN

- Serial Number

SNMP

- Simple Network Management Protocol

SOC

- System on Chip

SSH

- Secure Shell

SSL

- Secure Sockets Layer

TLS

- Transport Layer Security

UID

- Unit Identification Light

USB

- Universal Serial Bus

UTC

- Universal Time Coordinated

VGA

- Video Graphic Adapter

VLAN

- Virtual Local Area Network

VNC

- Virtual Network Computing

VNC

- Virtual Network Console

VR

- Voltage Regulator

WWNN

- World Wide Node Name

WWPN

- World Wide Port Name

iSAC

- Integrated Server Administrator Controller